参考資料１

（第１回課長級会議（8/26）資料）

重要インフラサイバーセキュリティ対策推進会議
検討すべき論点等

令和７年８月26日
内閣官房国家サイバー統括室

検討の背景

サイバー攻撃の巧妙化・高度化及び国家を背景とした攻撃キャンペーンによる被害の深刻化

サイバーセキュリティ戦略本部第１回会合
（令和７年７月１日）資料

■ サイバー攻撃の巧妙化・高度化や国家を背景とした攻撃キャンペーン等により、政府機関・重要インフラ等を標的に、重要インフラサービスの停止や機微情報の流出等、**国民生活・経済活動及び安全保障に深刻かつ致命的な被害を及ぼす恐れが顕在化。**

■ 被害が生じる前に脅威を未然に排除することを含め、強固な官民連携・国際連携の下、民間事業者への情報提供、アトリビューション、アクセス無害化等、多様な手段の組み合わせによる**実効的な防止・抑止の実現が急務。**

有事を想定した重要インフラ等への事前侵入

- 2023年5月、米国は、中国を背景とするグループ「Volt Typhoon」が、事前のアクセス確保を通じた有事における米国内の重要インフラの機能不全を狙い、システム内寄生攻撃等を実施と公表。

国家背景アクターによる機微技術情報、金銭等資産等の窃取

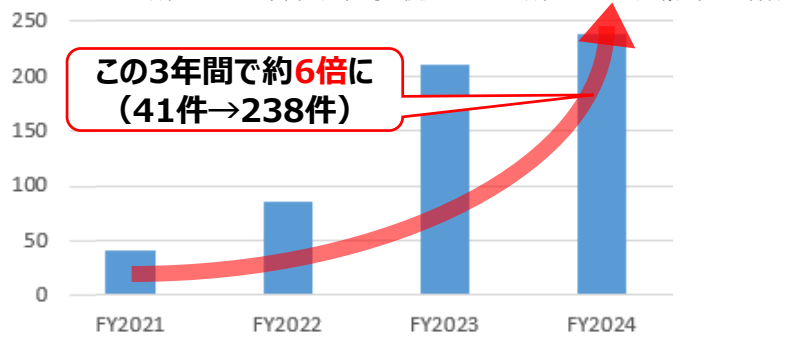
- 2019年以降、中国の関与が疑われるグループ「MirrorFace」が、日本の安全保障や先端技術に係る情報窃取を狙う攻撃キャンペーンを実行。
- 2024年5月、北朝鮮を背景とする攻撃グループ「TraderTraitor」が、暗号資産関連事業者から約482億円相当の暗号資産を窃取。

重要インフラの機能停止

- 2023年7月、名古屋港でランサムウェア攻撃によるシステム障害の発生により、業務が約3日間停止し、物流に大きな影響。
- 2024年から2025年の年末年始にかけて、航空事業者、金融機関、通信事業者等が相次いでDDoS攻撃を受け、サービス一時停止等の被害。

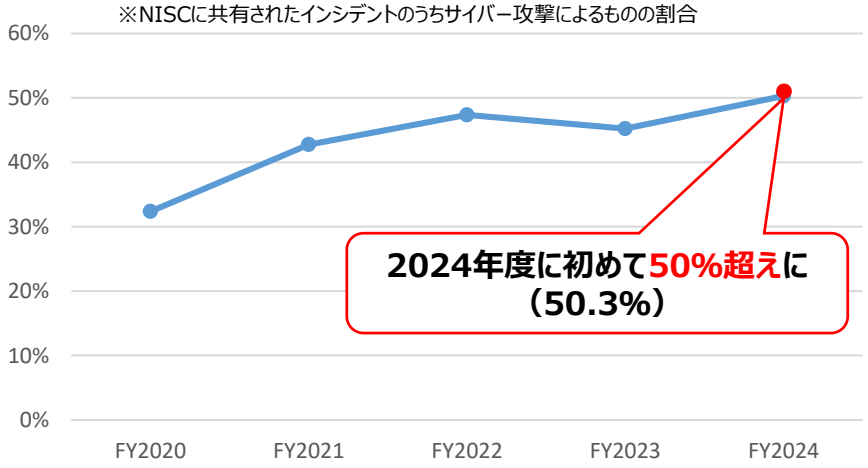
政府機関へのサイバー攻撃疑いの件数※

※NISCにおいて政府機関への不審な通信等を検知し、当該政府機関への通報を行った件数



重要インフラで発生したインシデントのうちサイバー攻撃の割合※

※NISCに共有されたインシデントのうちサイバー攻撃によるものの割合



サイバー対処能力強化法及び同整備法の制定

サイバー対処能力強化法※1及びサイバー対処能力強化法整備法※2の制定

※1　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
※2　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の施行に伴う関係法律の整備等に関する法律

- 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**、④**NISC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設置された「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」（令和６年６月７日～11月29日）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。

サイバー対処能力強化法整備法の内容（組織・体制整備等関係）

- 能動的サイバー防御を含む各種取組を実現・促進するため、司令塔たる内閣官房新組織の設置等、政府を挙げた取組を推進するための体制を整備
  （内閣官房（司令塔・総合調整）と内閣府（実施部門）が一体となって機能）

サイバーセキュリティ戦略本部の強化（サイバーセキュリティ基本法改正）

□ サイバーセキュリティ戦略本部の改組

サイバーセキュリティ戦略本部を次のとおり改組
（第28条、第30条）
- 本部長：内閣総理大臣
- 本部員：全ての国務大臣

※ 有識者から構成される「サイバーセキュリティ推進専門家会議」を設置

□ サイバーセキュリティ戦略本部の機能強化

サイバーセキュリティ戦略本部の所掌事務に次を追加（第26条）
- **重要インフラ事業者等のサイバーセキュリティの確保に関する国の施策の基準の作成**
- **国の行政機関等におけるサイバーセキュリティの確保の状況の評価**

サイバーセキュリティ基本法の改正による司令塔機能強化の一環として、サイバーセキュリティ（CS）戦略本部は、重要インフラ事業者等のサイバーセキュリティの確保に関する国の施策の基準の作成や施策評価を実施し、重要インフラのサイバーセキュリティ強化を進める。

- **武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入**する。そのために、**サイバー安全保障分野における情報収集・分析能力を強化**するとともに、**能動的サイバー防御の実施のための体制を整備**することとし、以下の(ア)から(ウ)までを含む必要な措置の実現に向け検討を進める。

  (ア) 重要インフラ分野を含め、**民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有**や、**政府から民間事業者等への対処調整、支援等の取組を強化**するなどの取組を進める。

  (イ) **国内の通信事業者が役務提供する通信に係る情報を活用**し、**攻撃者による悪用が疑われるサーバ等を検知**するために、所要の取組を進める。

  (ウ) **国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃**について、**可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与**されるようにする。

- 能動的サイバー防御を含むこれらの取組を実現・促進するために、**内閣官房サイバーセキュリティセンター（NISC）を発展的に改組**し、**サイバー安全保障分野を一元的に総合調整する新たな組織を設置**する。そして、**これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備**、運用の強化**を図る**。

【参考】サイバーセキュリティ基本法の改正について（一部抜粋）

改正後	改正前
第四章　サイバーセキュリティ戦略本部	第四章　サイバーセキュリティ戦略本部
（所掌事務等）	（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。	第二十六条　本部は、次に掲げる事務をつかさどる。
一・二　（略）	一・二　（略）
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	（新設）
四　国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティの確保の状況の評価（情報システムに対する不正な活動であって情報通信ネットワーク又は電磁的記録媒体を通じて行われるものの監視及び分析並びにサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む。）を含む。）に関すること。	三　国の行政機関、独立行政法人又は指定法人で発生したサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む。）に関すること。
五・六　（略）	四・五　（略）
2　（略）	2　（略）
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。	（新設）
一　サイバーセキュリティ戦略の案を作成しようとするとき。	
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。	
4　（略）	3　（略）
（サイバーセキュリティ戦略本部長）	（サイバーセキュリティ戦略本部長）
第二十八条　本部の長は、サイバーセキュリティ戦略本部長（以下「本部長」という。）とし、内閣総理大臣をもって充てる。	第二十八条　本部の長は、サイバーセキュリティ戦略本部長（以下「本部長」という。）とし、内閣官房長官をもって充てる。
2～4　（略）	2～4　（略）
5　（削る）	5　（略）
（サイバーセキュリティ戦略本部員）	（サイバーセキュリティ戦略本部員）
第三十条　（略）	第三十条　本部に、サイバーセキュリティ戦略本部員（次項において「本部員」という。）を置く。
2　本部員は、本部長及び副本部長以外の全ての国務大臣をもって充てる。	2　本部員は、次に掲げる者（第一号から第六号までに掲げる者にあっては、副本部長に充てられたものを除く。）をもって充てる。
（削る）	一～五　（略）
（資料の提出その他の協力）	（資料の提出その他の協力）
第三十三条　（略）	第三十三条　（略）
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。	（新設）
3　本部は、その所掌事務を遂行するため特に必要があると認めるときは、前二項に規定する者以外の者に対しても、第一項の協力を依頼することができる。	

サイバーセキュリティ戦略推進体制

※令和７年７月１日時点（予定）

サイバーセキュリティ戦略本部第１回会合
（令和７年７月１日）資料

内 閣

重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針
（サイバー対処能力強化法第３条に基づき今後策定）

サイバーセキュリティ戦略
（令和３年９月28日閣議決定）

国家安全保障戦略
（令和４年12月16日国家安全保障会議・閣議決定）

サイバーセキュリティ推進専門家会議

意見聴取

サイバーセキュリティ戦略本部

本部長：内閣総理大臣
副本部長：内閣官房長官、サイバー安全保障担当大臣
本部員：全大臣

意見

国家安全保障会議（NSC）

内閣官房　国家サイバー統括室

内閣サイバー官（併）国家安全保障局次長

〔CS戦略本部事務局、総合調整〕

緊密連携

国家安全保障局（NSS）

総合調整

＜全府省庁＞

〔自組織・所管独立行政法人等のセキュリティ確保の推進〕

＜サイバーセキュリティ政策推進省庁＞

〔所掌に基づくサイバーセキュリティ施策の実施〕

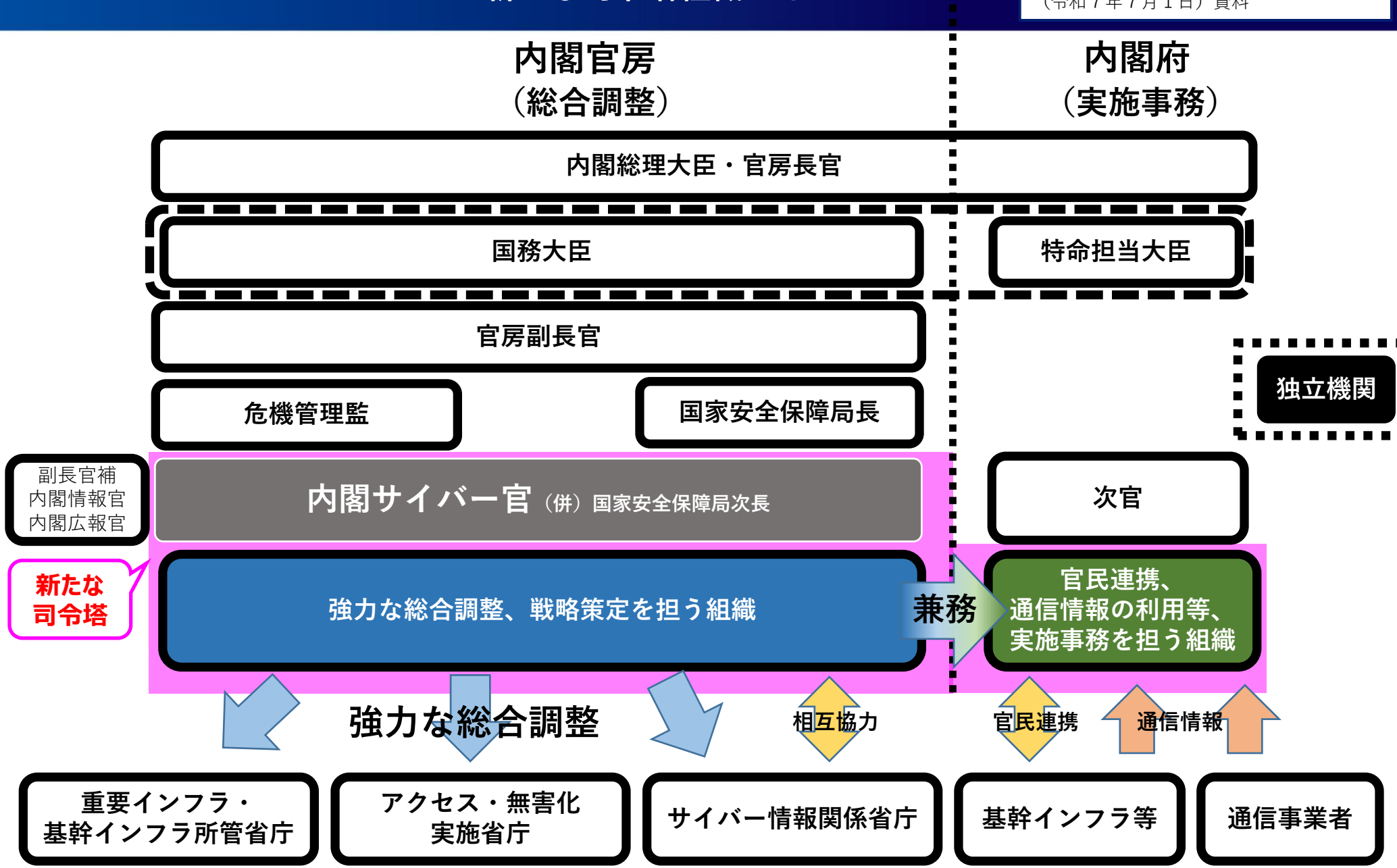
内閣府（経済安全保障）
警察庁（治安の確保）
デジタル庁（デジタル社会形成）
総務省（通信・ネットワーク政策）
　－ NICT（(国研)情報通信研究機構）
外務省（外交・安全保障）
経済産業省（情報政策）
　－ IPA（(独)情報処理推進機構）
防衛省（国の防衛）
文部科学省（セキュリティ教育）等

重要インフラ所管省庁

金融庁（金融）
総務省
（政府・行政サービス、情報通信）
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
（鉄道、航空、物流、水道、空港、港湾）

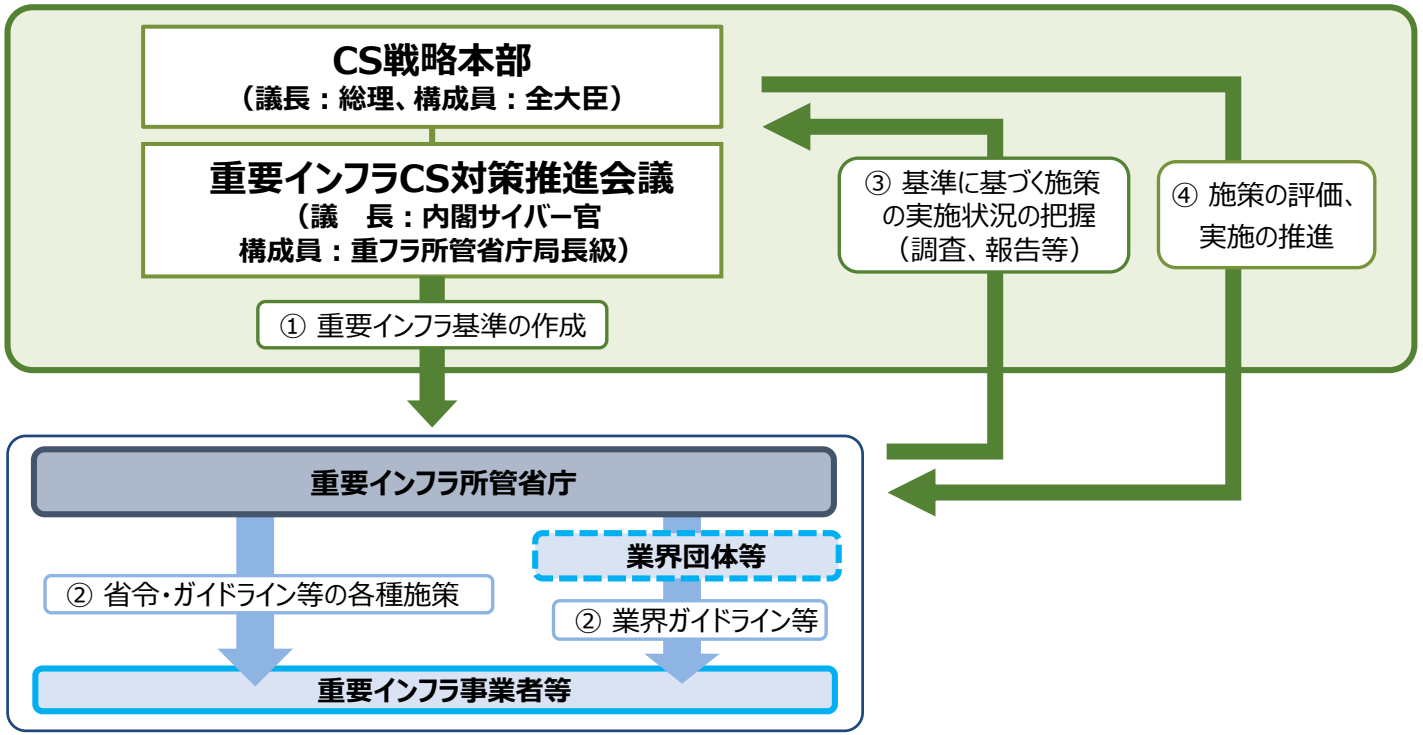
新たな司令塔組織のイメージ

サイバーセキュリティ戦略本部第１回会合
（令和７年７月１日）資料



重要インフラのサイバーセキュリティに係る施策の基準

- 改正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、CS戦略本部は、重要インフラのサイバーセキュリティ対策強化を図るため、重要インフラ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や、当該基準に基づく施策の評価を行う。



サイバーセキュリティ基本法
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。
六　前各号に掲げるもののほか、サイバーセキュリティに関する施策で重要なものの企画に関する調査審議、府省横断的な計画、関係行政機関の経費の見積りの方針及び施策の実施に関する指針の作成並びに施策の評価その他の当該施策の実施の推進並びに総合調整に関すること。

【参考】サイバーセキュリティ戦略本部の関連会議について

サイバーセキュリティ戦略本部第１回会合
（令和７年７月１日）資料

■ サイバー対処能力強化法整備法の一部施行による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戦略本部の下に以下の会議を設置する。

・**CS戦略推進会議**：我が国のサイバー対処能力の向上及びCSの確保に関し、関係省庁が情報交換・意見交換を行い、連携を図るとともに、総合的な施策を検討・推進する。

・**重要インフラCS対策推進会議**：CS基本法第26条第１項第３号等の規定を踏まえ、関係行政機関相互の緊密な連携の下、我が国全体の重要インフラ防護に資するCS対策の推進を図る。

関連会議

内　閣

CS戦略本部
議　長:内閣総理大臣
構成員:全閣僚

［CS基本法により設置］

CS推進専門家会議
議　長・構成員:有識者

［新設］

CS戦略推進会議
議　長:サイバー安全保障担当大臣
構成員:各省官房長級

［新設］

重要インフラCS対策推進会議
議　長:内閣サイバー官
構成員:重フラ所管省庁局長級

CS対策推進会議（CISO等連絡会議）
議　長:副長官(事務)
構成員:各省官房長級

CS対策推進専任審議官等会議（副CISO等連絡会議）
議　長:内閣サイバー官
構成員:各省審議官級

CS対策推進会議幹事会
議　長:国家サイバー統括室審議官
構成員:各省参事官級

検討すべき論点

（１）重要インフラ防護に資するサイバーセキュリティ対策の基本的枠組みについて

（２）重要インフラ防護に資するサイバーセキュリティ対策の推進について

（３）その他重要インフラ防護に資するサイバーセキュリティ対策に関し必要な事項について

うち当面検討すべき論点

（１）重要インフラ事業者等におけるサイバーセキュリティの確保に係る施策の基準等（主な観点、位置付け、関係制度との関係整理、重要インフラ防護対象の在り方、施策の評価方法等）

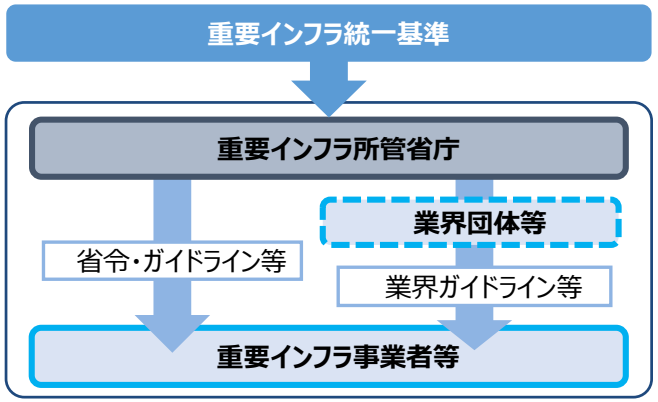
（２）上記を踏まえた「重要インフラのサイバーセキュリティに係る行動計画」の見直し

（３）その他

骨子（今後の取組方向性）をとりまとめ、新たな「サイバーセキュリティ戦略」へ反映

論点：重要インフラ統一基準の主な観点、位置付け

- 現在、各重要インフラ分野における取組の評価と改善につながるような具体的かつ統一的な基準はなく、サイバーセキュリティ確保の取組やその水準は分野・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、各分野における個々のサイバーセキュリティ対策のさらなる強化とともに、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）を徹底することにより、重要インフラにおけるサイバーセキュリティ水準の斉一的な引上げが求められる。
- 新たに作成する、重要インフラ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（以下「重要インフラ統一基準」という。）によって、重要インフラ事業者等において講ずべきベースラインとなる対策を明示しつつ、その徹底のため、どのように実効性を確保すべきか。



重要インフラ統一基準群（イメージ）

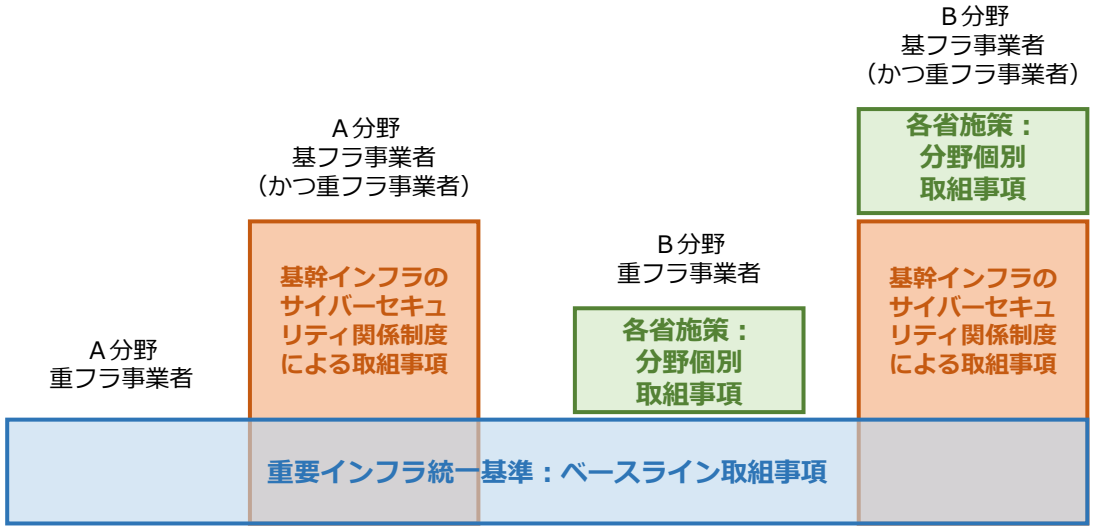
<統一基準>

1．総則
1.1 基準の目的
1.2 基準の適用対象
1.3 ・・・
2．重要インフラにおける取組の基本的枠組み
2.1 導入・計画
2.2 運用
2.3 ・・・
3．・・・

<統一基準ガイドライン>

1．総則
1.1 基準の目的
1.2 基準の適用対象
1.3 ・・・
2．重要インフラにおける取組の基本的枠組み
2.1 導入・計画
2.2 運用
2.3 ・・・
3．・・・

■重要インフラ統一基準（ベースライン取組事項）＋関係取組事項



論点：重要インフラ統一基準作成に当たっての考慮事項

- 重要インフラ統一基準の作成に当たっては、安全基準等策定指針や政府統一基準といった現行制度、各重要インフラ分野における特性や実情、サイバー対処能力強化法や経済安全保障推進法に基づく基幹インフラのサイバーセキュリティ関係制度、国際標準や諸外国における取組、技術・脅威の動向等を考慮することが必要ではないか。

重要インフラにおける現状課題

- 各重要インフラ分野における取組の評価と改善につながるような具体的かつ統一的な基準はなく、サイバーセキュリティ確保の取組やその水準は分野・事業者によってばらつきが見られる。
- 他にも、次の現状課題あり。
  - ✓ 中小規模の重要インフラ事業者は組織的リソースに限りがあり、膨大な対策事項への対応が難しい。
  - ✓ 参照し得るガイドラインが膨大であり、対策すべき事項の優先順位等の判断が難しい。
  - ✓ 技術の変化にも関わらず、ITと接続したOTのリスクが見過ごされ十分なサイバーセキュリティ対策が講じられていない。

重要インフラにおける具体的かつ統一的な基準の検討

現行制度等の考慮

- 現行制度
  - ✓ 安全基準等策定指針
  - ✓ 政府統一基準　等
- 各重要インフラ分野における特性や実情

関係制度の考慮

- 基幹インフラのサイバーセキュリティ関係制度
  - ✓ サイバー対処能力強化法（資産届出、インシデント報告等）
  - ✓ 経済安全保障推進法（リスク管理措置等）

国際標準や諸外国における取組、技術・脅威の動向等の考慮

- 国際標準規格
  - ✓ ISO/IEC 27000シリーズ（情報セキュリティマネジメント）
  - ✓ ISO/IEC 62443（制御システムセキュリティ）　等
- 諸外国の取組
  - ✓ 米：NIST CSF※1（サイバーセキュリティフレームワーク）、NIST SP800シリーズ（対策の参考となるガイダンス群）、CISA CPGs※2（重要インフラの優先的対策事項）
  - ✓ 英：CAF※3（重要インフラ等の優先的対策事項及び評価）　等
- 技術・脅威の動向等
  - ✓ PQCやAI等の新興技術によるサイバーセキュリティ対策への影響　等

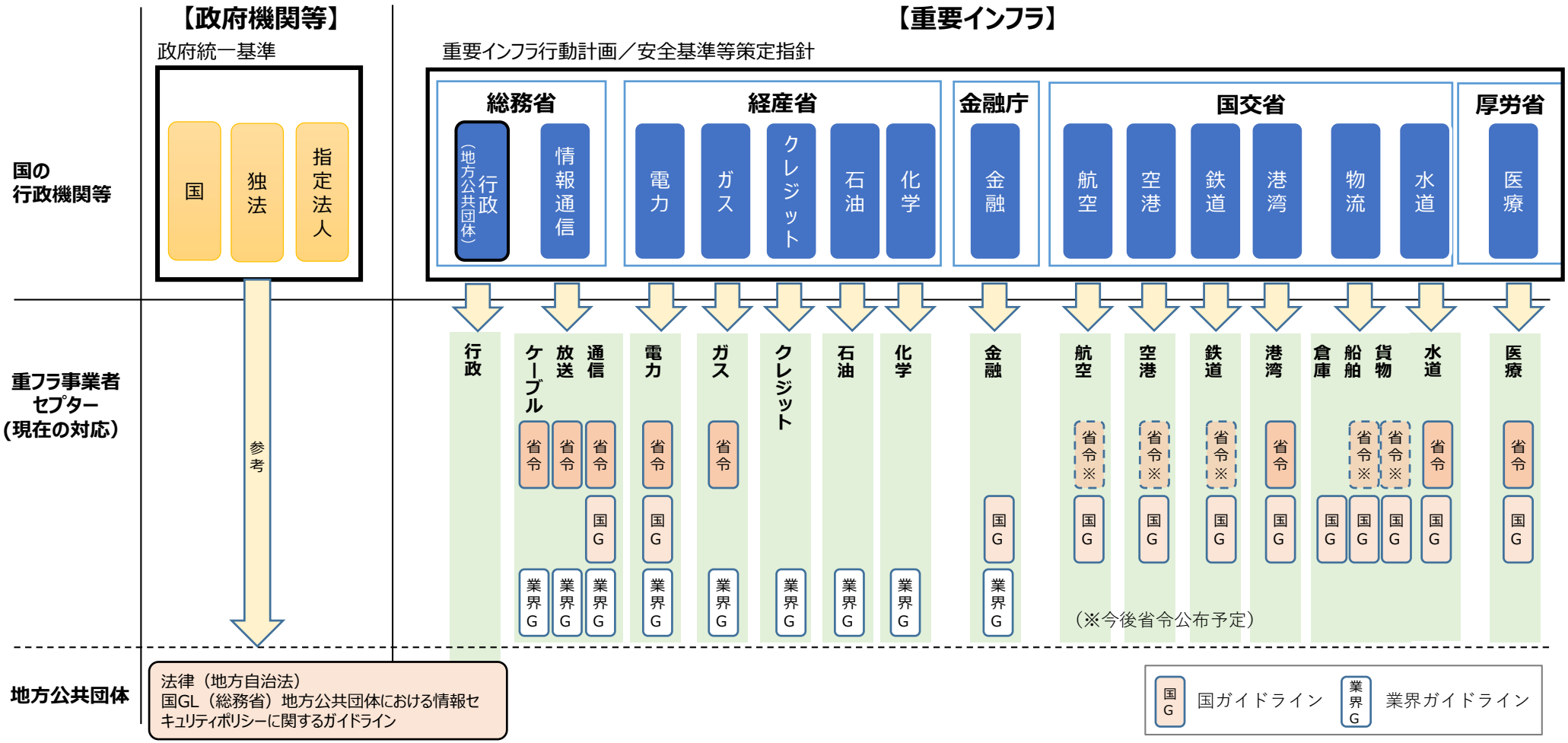
※1 CSF: Cybersecurity Framework
※2 CPGs: Cross-Sector Cybersecurity Performance Goals
※3 CAF: Cyber Assessment Framework

重要インフラ統一基準の作成

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）を徹底し
重要インフラにおけるサイバーセキュリティ水準を斉一的に引上げ

論点：重要インフラ統一基準作成に当たっての考慮事項（現行制度等）

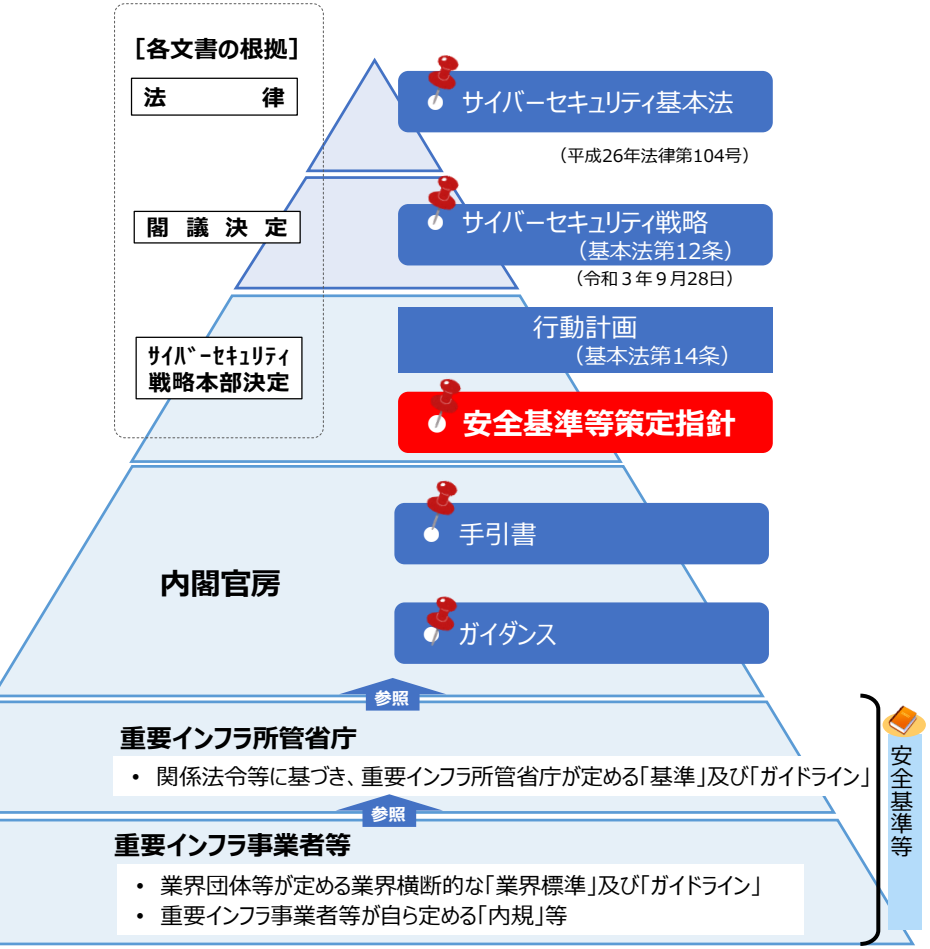
- 現在、重要インフラ事業者等のサイバーセキュリティ確保に係る必要な取組を示した安全基準等としては、各重要インフラ分野に関する法制度の下、安全基準等策定指針や政府統一基準等を踏まえ、国による基準やガイドライン、あるいは、業界団体等による業界標準やガイドライン等が定められている。
- 重要インフラ統一基準の作成に当たっては、これら現行制度に基づく各重要インフラ分野の取組状況、特性や実情を踏まえつつ、全体としてサイバーセキュリティ対策の強化を図ることができるような仕組みを検討すべきではないか。



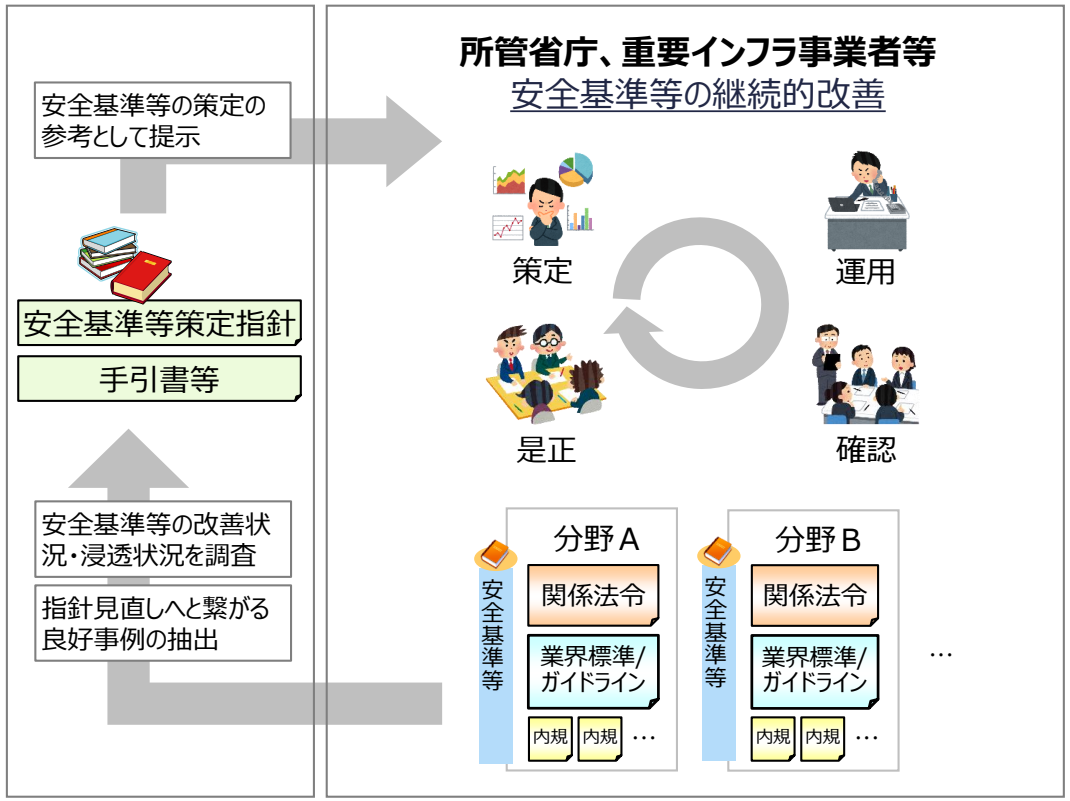
（参考）安全基準等策定指針

安全基準等策定指針※とは、重要インフラサービスの安全かつ持続的な提供を図る観点から、**安全基準等において規定が望まれる項目を整理・記載**し、重要インフラ事業者や重要インフラ所管省庁の「安全基準等」の策定・改定を支援することを目的とするもの。

※ 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指針（令和５年７月サイバーセキュリティ戦略本部決定、令和７年６月一部改定）



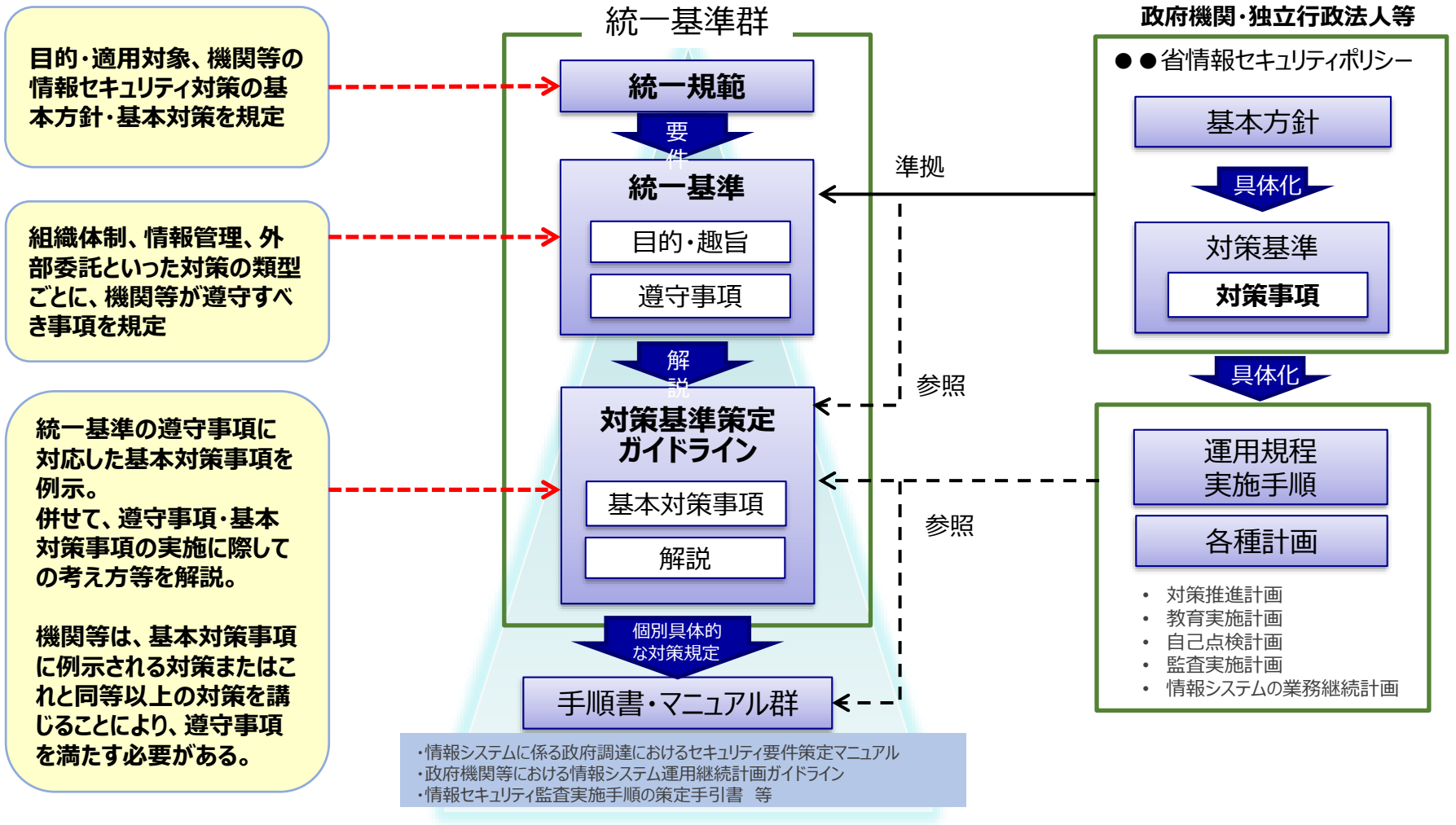
【安全基準等策定指針の活用方法】



（参考）政府統一基準

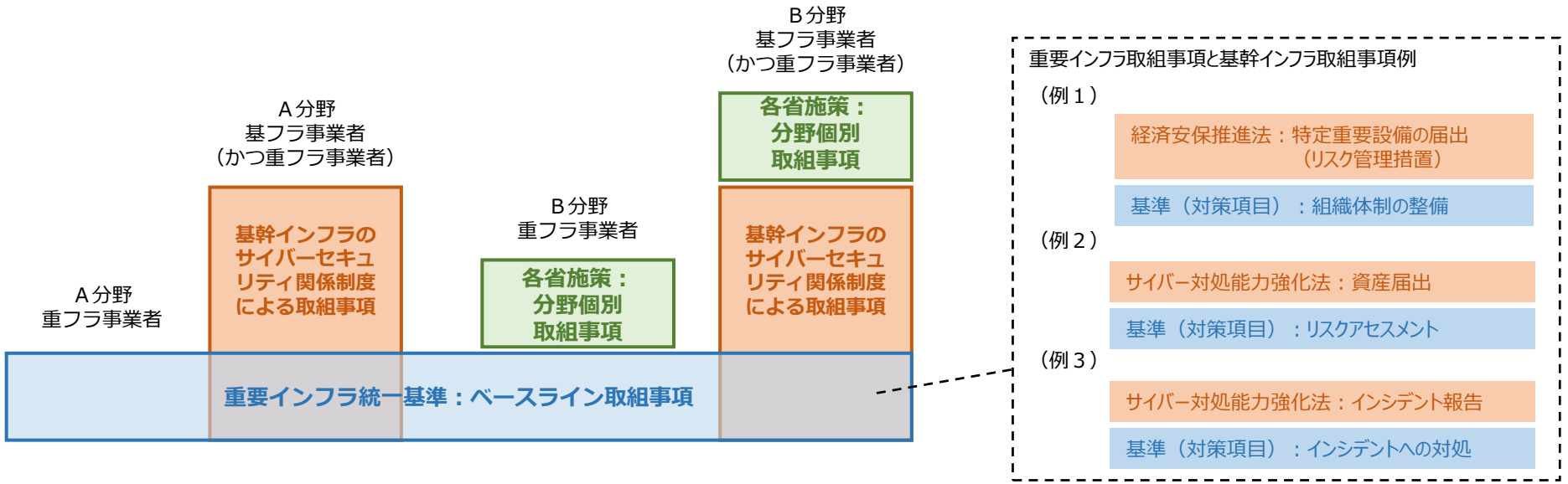
✓ 政府機関及び独立行政法人等は、**政府統一基準※に準拠**しつつ、組織及び取り扱う情報の特性等を踏まえ**各組織の情報セキュリティポリシーを策定。**

※ 政府機関等のサイバーセキュリティ対策のための統一基準（令和５年７月サイバーセキュリティ戦略本部決定、令和７年６月一部改定）



論点：重要インフラ統一基準作成に当たっての考慮事項（関係制度）

- 重要インフラ統一基準の作成に当たっては、サイバー対処能力強化法や経済安全保障推進法に基づく基幹インフラを対象としたサイバーセキュリティ確保の各種規定との整合や全体調和を考慮し、関係事業者にとって過度な負担にならないようにしつつ、関係制度間の構造を明確にし、関係事業者においてより効果的な取組がなされるようにすることが必要ではないか。



（参考）経済安全保障推進法における関連規定例
- 特定重要設備の届出（第52条）における特定妨害行為を防止するための措置（リスク管理措置）
  （例）製造等の過程における不正な変更の防止、役務提供の継続体制等

（参考）サイバー対処能力強化法における関連規定例
- 資産届出（第４条）
  基幹インフラ事業者は、特定重要電子計算機を導入したときは、その製品名等を事業所管大臣に届出
- インシデント報告（第５条）
  基幹インフラ事業者は、特定重要電子計算機のインシデント情報やその原因となり得る事象を認知したときは、事業所管大臣及び内閣総理大臣に報告
- 情報共有・対策のための協議会の設置（第９章）

（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）

論点：重要インフラ防護対象の在り方

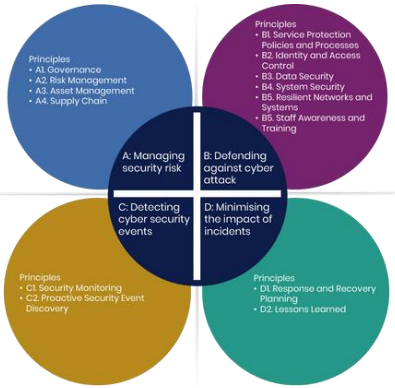
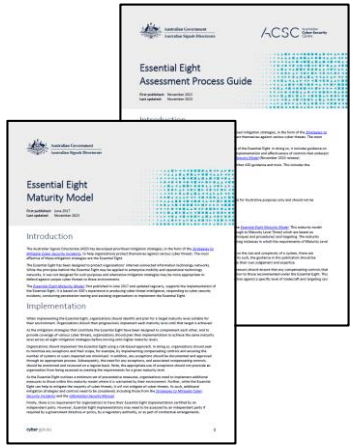
- 重要インフラ及び基幹インフラは、それぞれの根拠法令等に基づき分野・業種や事業者が指定されている。これにより両制度間での対象分野の違いや、同一の分野内でも、例えば基幹インフラ事業者だが重要インフラ事業者でない事業者等の存在が認められる。
- これら制度背景による差異は、関係制度の運用における複雑化の要因、また、分野・事業者による取組内容やその水準のばらつきの要因となり得るところ、全体調和の観点から、構造を整理すべく重要インフラ防護範囲の在り方を見直してはどうか。

重要インフラ対象分野等	基幹インフラ対象分野等
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）	—

（参考）重要インフラのサイバーセキュリティ対策強化（諸外国の取組）①

■ 諸外国では、**<u>レジリエンスの強化</u>**の観点から、中小規模の重要インフラ事業者を含め、基本的なサイバーセキュリティ対策の　重要性が認識される一方、**<u>対策強化の優先順位等の判断の困難性</u>**や、それによる**<u>成熟度のばらつき</u>**に課題があるとの認識

■ そのため、近年、各国では、**<u>特に重要な事項として</u>**、優先順位をつけて分野横断的な対策の**<u>ベースラインを明示</u>**

米（CISA）	英（NCSC）	豪（ACSC）	EU
Cross-Sector Cybersecurity Performance Goals (CPGs) （2022策定、2023更新）	Cyber Assessment Framework (CAF) （2019策定、2024最終更新）	Essential Eight Maturity Model （2017策定、2023最終更新）	NIS2指令 (Network and Information Systems Directive 2) （2022発表）
			
・NISTのCSF※に準拠し、「識別、防御、検知、対応、復旧」の段階ごとに、実装が容易でリスクの低減効果が大きいIT/OTのサイバーセキュリティ対策のベースライン、優先順位を明示。 ※CSF: Cyber Security Framework	・セクターを問わず共通の中核的原則として、サイバーセキュリティとレジリエンス強化に必要な14項目を明示。 ・構造化された指標(IGPs※) による組織の評価が可能。 ※IGPs:　Indicators of Good Practice	・特に取り組むべき優先度の高いサイバーセキュリティ対策８項目を明示。 ・成熟度レベルによる組織の評価が可能（自己評価／第三者評価）。	・サイバーセキュリティのリスク管理のため、EU各国でのサイバーセキュリティ対策の共通のベースラインを明示。 ・事業者等のリスクへの曝露の程度、組織の規模等に比例した措置とすることを規定。

（参考）重要インフラのサイバーセキュリティ対策強化（諸外国の取組）②

■ 諸外国では、分野横断的なサイバーセキュリティ対策のベースラインを明示。

■ 各国で共通する事項としては、「リスク管理（資産管理と脆弱性対策）」、「事業継続と復旧の計画」のほか、「サプライチェーン対策」などが規定されている。

	米（CISA）	英（NCSC）	豪（ACSC）	EU
基準名	Cross-Sector Cybersecurity Performance Goals (CPGs)	Cyber Assessment Framework (CAF)	Essential Eight Maturity Model	NIS2指令 （うちリスク管理措置）
適用対象	重要インフラ全体	国家重要インフラを含む民間事業者	重要インフラを含む様々な組織	基幹事業者及び重要事業者
主な内容	1．識別 資産インベントリ、ITとOTのサイバーセキュリティ関係の改善、既知の脆弱性の緩和、サプライチェーンでのインシデントの報告　等 2．防御 デフォルトパスワードの変更、ネットワークセグメンテーション、多要素認証、OTサイバーセキュリティトレーニング、強力でアジャイルな暗号化、マクロの無効化、システムのバックアップ、ログの収集、公衆インターネットへのOT接続の制限　等 3．検知 関連する脅威及びTPPの検知 4．対応 インシデント報告、脆弱性報告　等 5．復旧 インシデント計画及び準備	1．ガバナンス 2．リスク管理 3．資産管理 4．サプライチェーン 5．サービス保護の方針とプロセス 6．IDとアクセス制御 7．データ・セキュリティ 8．システム・セキュリティ（脆弱性管理等） 9．レジリエントなネットワークとシステム（バックアップ等） 10．スタッフの意識向上と研修 11．セキュリティ監視 12．プロアクティブなセキュリティ・イベントの発見 13．対応と復旧計画 14．教訓からの学習	1．資産管理と脆弱性スキャン 2．OSへのパッチ適用 3．多要素認証 4．特権アカウントの管理 5．アプリケーション制御 6．MS officeのマクロ制御 7．ウェブブラウザの制御 8．定期的なバックアップ	・リスク分析及び情報セキュリティに関する方針 ・インシデント対応 ・事業継続（バックアップ管理等） ・サプライチェーンセキュリティ ・ネットワークやシステムのセキュリティ（脆弱性対処等） ・リスク管理措置の有効性評価 ・サイバー衛生の実施及びサイバーセキュリティ研修 ・暗号の使用 ・人的セキュリティ（アクセス管理等）及び資産管理 ・多要素認証等の活用

※赤字は、各国で特に共通する事項

NIST CSF（重要インフラのサイバーセキュリティを向上させるためのフレームワーク）

- 業種や企業規模などに依存せず、サイバーセキュリティ対策の効果を数値で評価するための基準も含む体系的なガイドライン。
- 米国国立標準研究所（National Institute of Standards and Technology, NIST）が2014年に初版、2024年に第２版を公表。

➢ コア（Core）、ティア（Tier）、プロファイル（Profile）の３要素で構成

	概要
コア（Core）	組織の種類や規模を問わない共通のサイバーセキュリティ対策の一覧
ティア（Tier）	対策状況を数値化し、組織を評価する基準（成熟度評価基準（4段階））
プロファイル（Profile）	ティア等の評価基準を用いて、組織のサイバーセキュリティ対策の「現状」（as is）と「目標」（to be）をまとめたもの。

組織プロファイルを作成、ギャップを分析、行動計画により継続的に改善

対策を６種類に分類し、具体的な内容はNIST SP-800等を参照

	概要	カテゴリー
統治（GV）	組織のサイバーセキュリティリスクマネジメント戦略、期待、及びポリシーが確立、周知、監視されている。	• 組織の状況 • リスクマネジメント戦略 • 役割、責任、権限 • ポリシー • 監督 • サイバーセキュリティサプライチェーンリスクマネジメント
識別（ID）	組織の現在のサイバーセキュリティリスクが理解されている。	• 資産管理 • リスクアセスメント • 改善
防御（PR）	組織のサイバーセキュリティリスクを管理するための保護対策が使用されている。	• ID管理、認証、アクセス制御 • 意識向上とトレーニング • データセキュリティ • プラットフォームセキュリティ • 技術インフラのレジリエンス
検知（DE）	サイバーセキュリティ攻撃及び侵害の可能性が発見、分析されている。	• 継続的監視 • 有害事象の分析
対応（RS）	検知されたサイバーセキュリティインシデントに関する措置が講じられている。	• インシデント管理 • インシデント分析 • インシデント対応の報告とコミュニケーション • インシデントの軽減
復旧（RC）	サイバーセキュリティインシデントの影響を受けた資産及び業務の復旧が行われている。	• インシデント復旧計画の実行 • インシデント復旧のコミュニケーション

（参照）IPA翻訳文書（https://www.ipa.go.jp/security/reports/oversea/nist/about.html）

NIST SP800シリーズ

- SP800シリーズ(Special Publications 800 Series)は、連邦政府がセキュリティ対策を実施する際に参考文書として利用することを前提として、NISTのコンピュータセキュリティ課(CSD)により作成されるガイダンス群。

➢ 各トピックにおけるガイドライン例

リスクマネジメント	
SP800-18	連邦情報システムのためのセキュリティ計画作成ガイド
SP800-30	ITシステムのためのリスクマネジメントガイド
SP800-34	ITシステムのための緊急時対応計画ガイド
SP800-37	情報システムと組織のためのリスクマネジメントフレームワーク
SP800-53	連邦政府情報システムにおける推奨セキュリティ管理策
SP800-53B	組織と情報システムのための管理策ベースライン
SP800-60	情報及び情報システムのタイプとセキュリティ分類のマッピングガイド
SP800-70	IT製品のための国家的なチェックリストプログラム

事業継続	
SP800-34	ITシステムのための緊急時対応計画ガイド
SP800-61	コンピュータインシデント対応ガイド
SP800-83	不正プログラムインシデント防止・対応ガイド

制御システム	
SP800-82	産業用制御システム(ICS)セキュリティガイド

認証	
SP800-63	電子的認証に関するガイドライン

サイバー脅威インテリジェンス(CTI)共有	
SP800-137	連邦情報システム及び組織のための情報セキュリティ常時監視(ISCM)
SP800-150	サイバー脅威情報共有のガイド

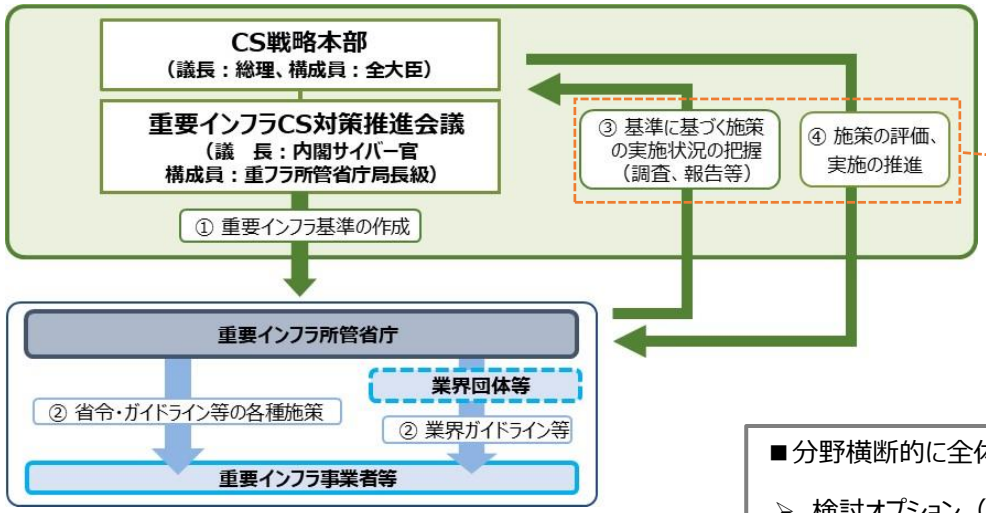
サプライチェーン	
SP800-161	システムと組織のためのサイバー・サプライチェーン・リスク管理の実践

管理すべき重要情報(CUI)保護	
SP800-171	連邦政府以外のシステムと組織における管理された非格付け情報の保護

ゼロトラスト	
SP800-207	ゼロトラストアーキテクチャ

論点：重要インフラ統一基準に基づく施策の評価及び改善

- 重要インフラ統一基準に基づく取組の評価は、年に１回を目途に、次のプロセスにおいて行うことが適当ではないか。
  - 内閣官房において、所管省庁を通じて、各分野の重要インフラ事業者等における取組の実施状況に対する専門的調査を実施
  - 所管省庁において、それら調査結果を踏まえ、施策の実施状況を取りまとめ
  - 所管省庁からサイバーセキュリティ戦略本部に取りまとめ結果を報告
  - サイバーセキュリティ戦略本部において、基準に基づく施策を評価
- 所管省庁が重要インフラ統一基準に基づき施策を実施するに当たり参照するための詳細事項については、別途ガイドラインにて定めることが考えられるが、本基準を通じて官民の間で共通理解を形成し、実効性のあるものとするためにはどのような点に留意すべきか。
- 特に、サイバーセキュリティ確保の取組やその水準は現状、分野・事業者によってばらつきが見られることを踏まえ、全体として対策の水準を上げられるような仕組みとしてどのようなものが考えられるか。



■重要インフラ統一基準に基づく施策の実施状況の把握と評価

（③ 基準に基づく施策の実施状況の把握）
- 内閣官房において、所管省庁を通じて、各分野の重要インフラ事業者等における取組の実施状況に対する専門的調査を実施
- 所管省庁において、それら調査結果を踏まえ、施策の実施状況を取りまとめ
- 所管省庁からサイバーセキュリティ戦略本部に取りまとめ結果を報告

（④ 施策の評価、実施の推進）
- サイバーセキュリティ戦略本部において、基準に基づく施策を評価

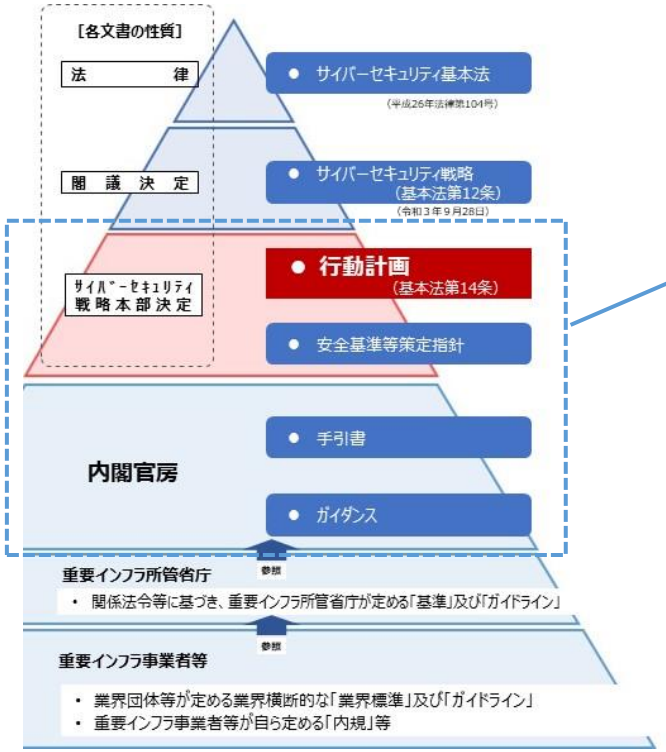
■分野横断的に全体として対策の水準を上げるための仕組みとしてどのようなものが考えられるか。

- 検討オプション（例）
① 「講ずべき対策事項」に加えて「講ずることが望ましい対策事項」を提示。
② ①をレベル別に提示。

		講ずべき対策事項		講ずることが望ましい対策事項
導入・運用	Lv.1	Lv.2	Lv.3
１．組織・体制の整備			
２．資産管理			
・・・			

論点：重要インフラのサイバーセキュリティに係る行動計画の見直し

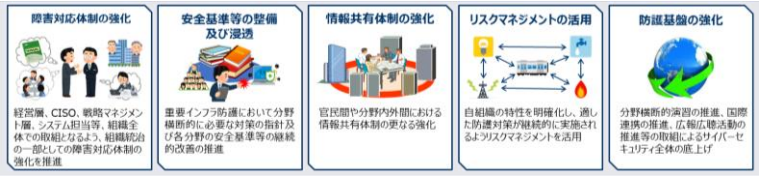
- 重要インフラ事業者等におけるサイバーセキュリティの確保に関して国の行政機関が実施すべき施策について具体的かつ統一的な基準を示す重要インフラ統一基準は、重要インフラのサイバーセキュリティ確保に関する政府と重要インフラ事業者等との共通の取組方向性を示した「重要インフラのサイバーセキュリティに係る行動計画」とは、目的や内容を異にするものと考えられる。
- 重要インフラ統一基準の作成に当たり、まずは当該基準と行動計画との関係を整理しつつ、基幹インフラ関係制度等の整備を含め制度的な環境変化を踏まえた行動計画の見直しを優先的に進め、その後に、技術・脅威の動向等、重要インフラを取り巻くサイバーセキュリティの環境変化を踏まえた行動計画の見直しを進めることが適当か。



■ 重要インフラのサイバーセキュリティに係る行動計画

（主な取組）

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



■ 関連指針及び手引書等

- 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指針
- 重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書
- 「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書　等

まずは①の見直しを優先的に進め、その後に②の見直しを実施。

① 制度的な環境変化を踏まえた行動計画の見直し
- 重要インフラ統一基準と行動計画との関係の整理
- 重要インフラ統一基準や基幹インフラ関係制度等の整備を踏まえ、重要インフラのサイバーセキュリティ確保に関する政府と重要インフラ事業者等の取組方向性の在り方の整理　等

② 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を踏まえた行動計画の見直し