資料５

重要インフラサイバーセキュリティ対策推進会議
検討の背景等

令和７年８月４日
内閣官房国家サイバー統括室

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

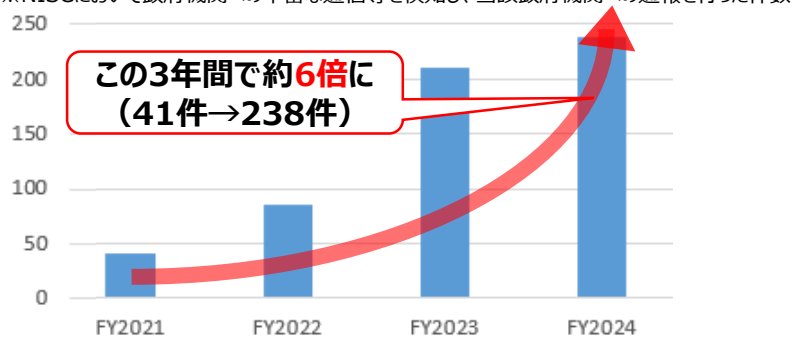
- 2019年以降、中国の関与が疑われるグループ「MirrorFace」が、日本の安全保障や先端技術に係る情報窃取を狙う攻撃キャンペーンを実行。
- 2024年5月、北朝鮮を背景とする攻撃グループ「TraderTraitor」が、暗号資産関連事業者から約482億円相当の暗号資産を窃取。

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。

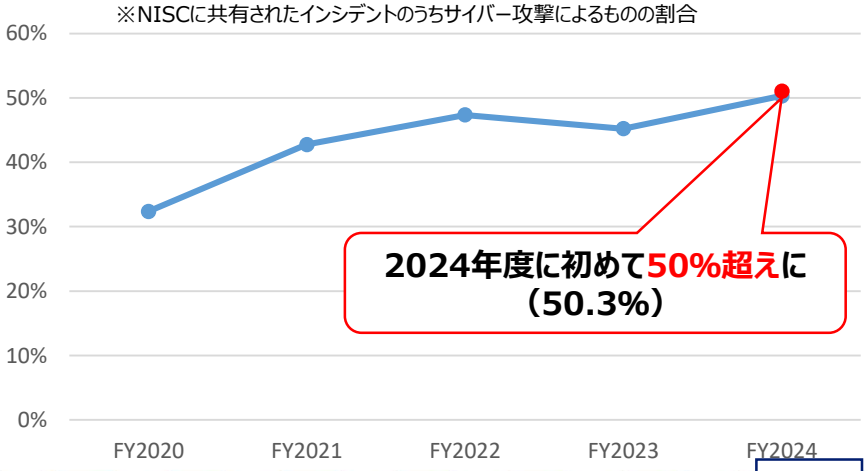
政府機関へのサイバー攻撃疑いの件数※

※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。

【参考】 国家安全保障戦略（抄） （令和４年12月16日閣議決定）

- **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〕

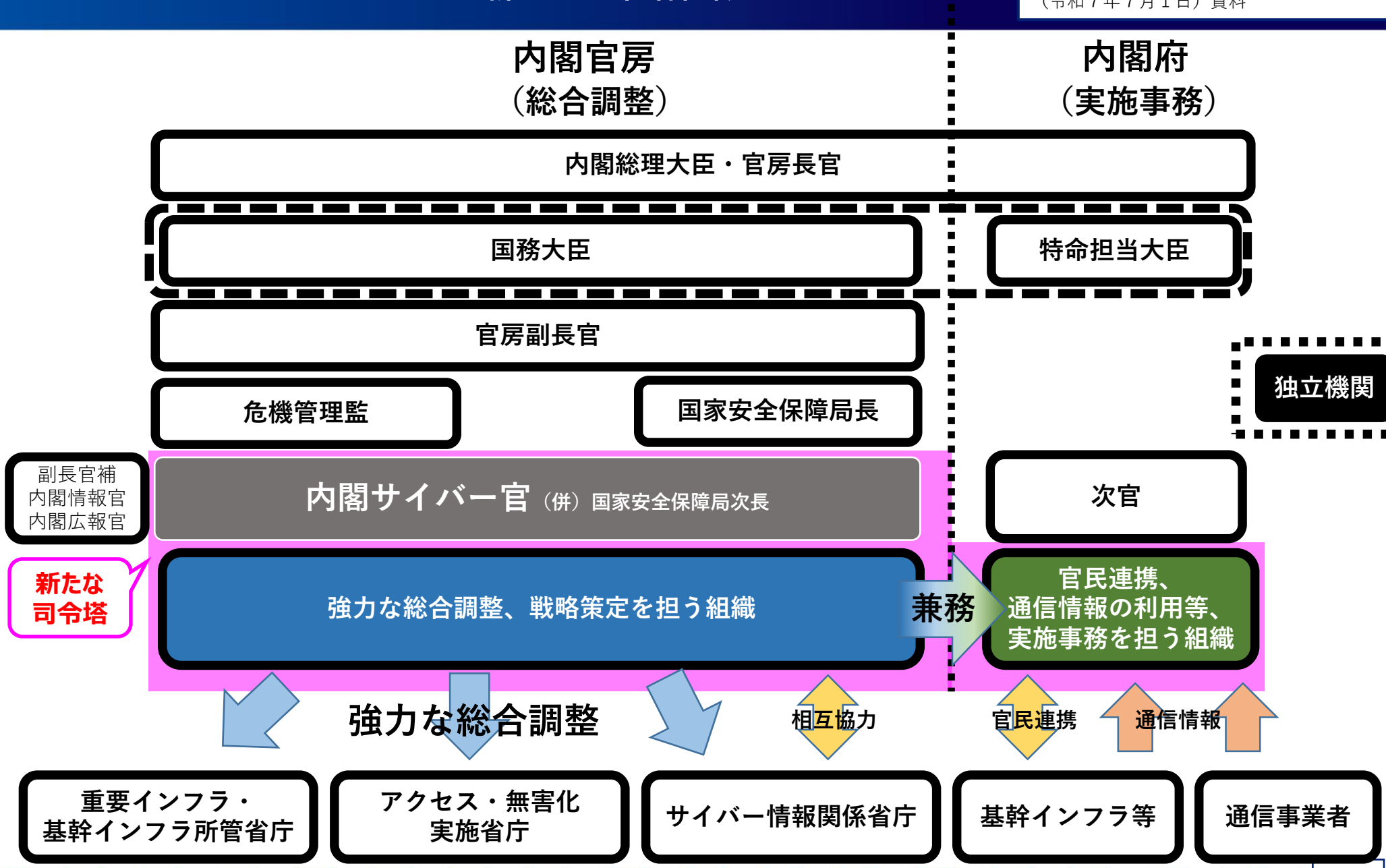
- 内閣府（経済安全保障）
- 警察庁（治安の確保）
- デジタル庁（デジタル社会形成）
- 総務省（通信・ネットワーク政策）
  - － NICT（(国研)情報通信研究機構）
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
  - － IPA（(独)情報処理推進機構）
- 防衛省（国の防衛）
- 文部科学省（セキュリティ教育）等

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）

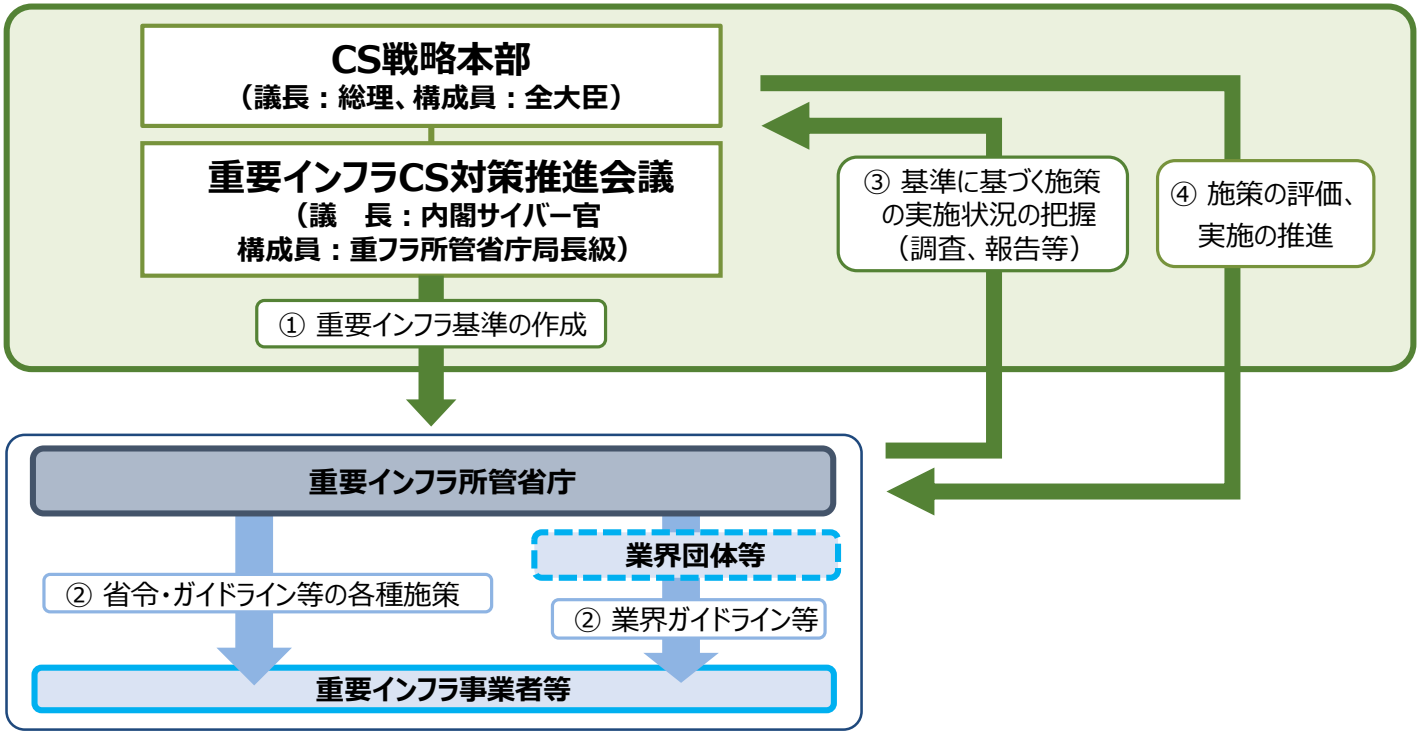
新たな司令塔組織のイメージ

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