

重要インフラサイバーセキュリティ研究会 検討の背景等

令和 7 年 11 月 5 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

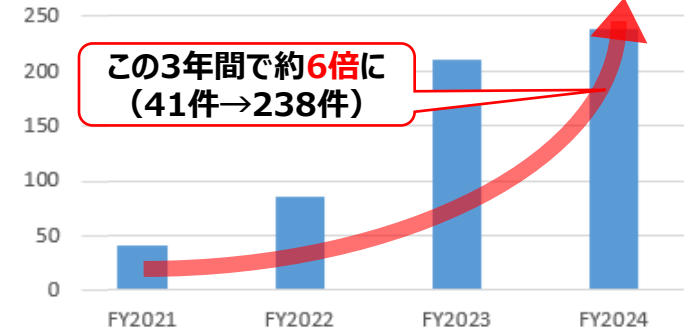
- 2019年以降、中国の関与が疑われるグループ「MirrorFace」が、日本の安全保障や先端技術に係る情報窃取を狙う攻撃キャンペーンを実行。
- 2024年5月、北朝鮮を背景とする攻撃グループ「TraderTraitor」が、暗号資産関連事業者から約482億円相当の暗号資産を窃取。

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※

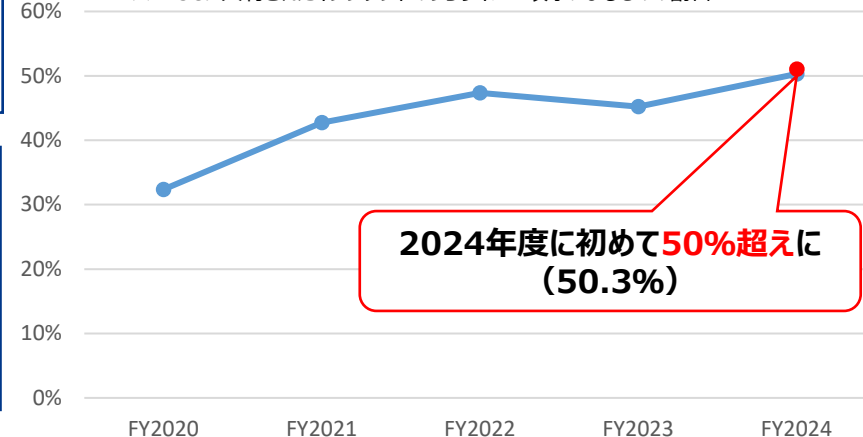
※NISCにおいて政府機関への不審な通信等を検知し、当該政府機関への通報を行った件数



この3年間で約**6倍に**
(41件→238件)

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



2024年度に初めて**50%超えに**
(50.3%)

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、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

□ 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）

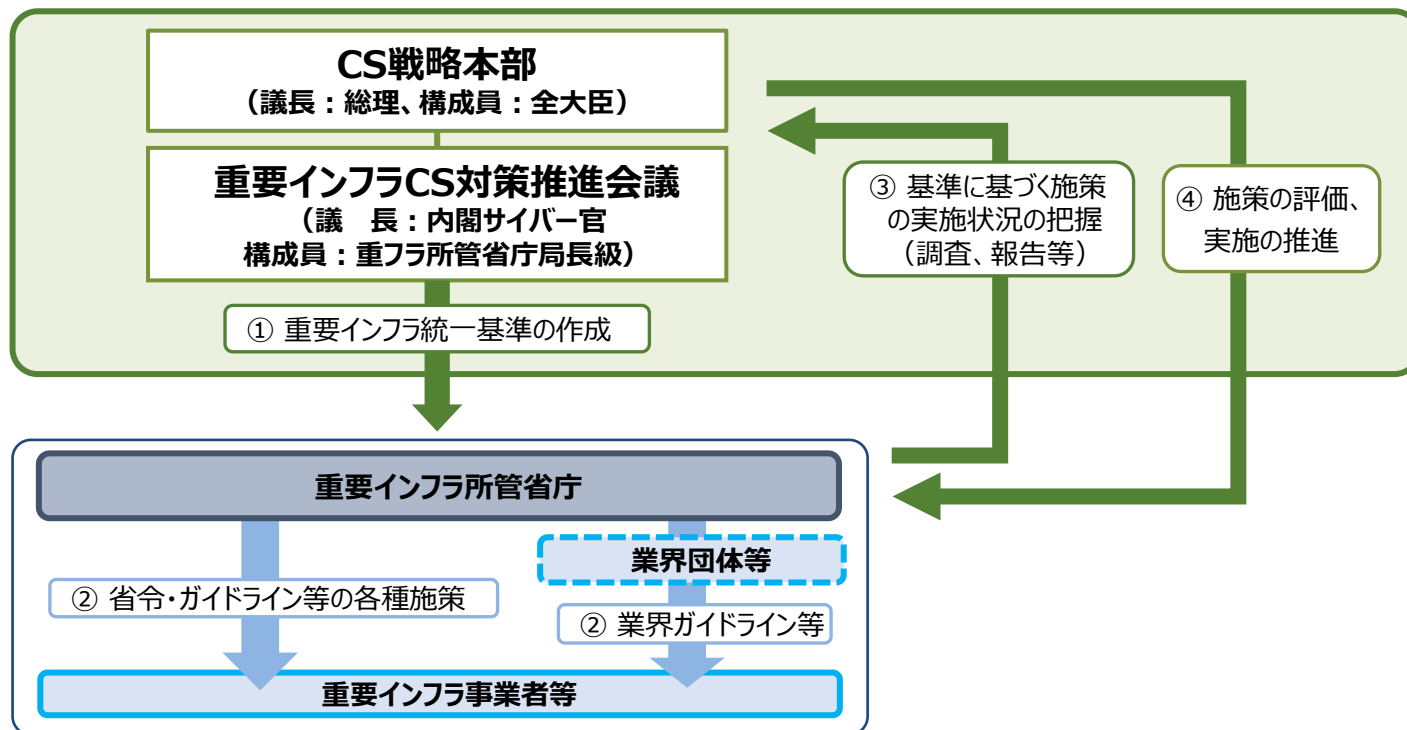
- **重要インフラ事業者等のサイバーセキュリティの確保に関する国の施策の基準の作成**
- **国の行政機関等におけるサイバーセキュリティの確保の状況の評価**

重要インフラ統一基準の作成等

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（重要インフラ統一基準）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。**

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 (重要インフラ統一基準)

- 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（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。

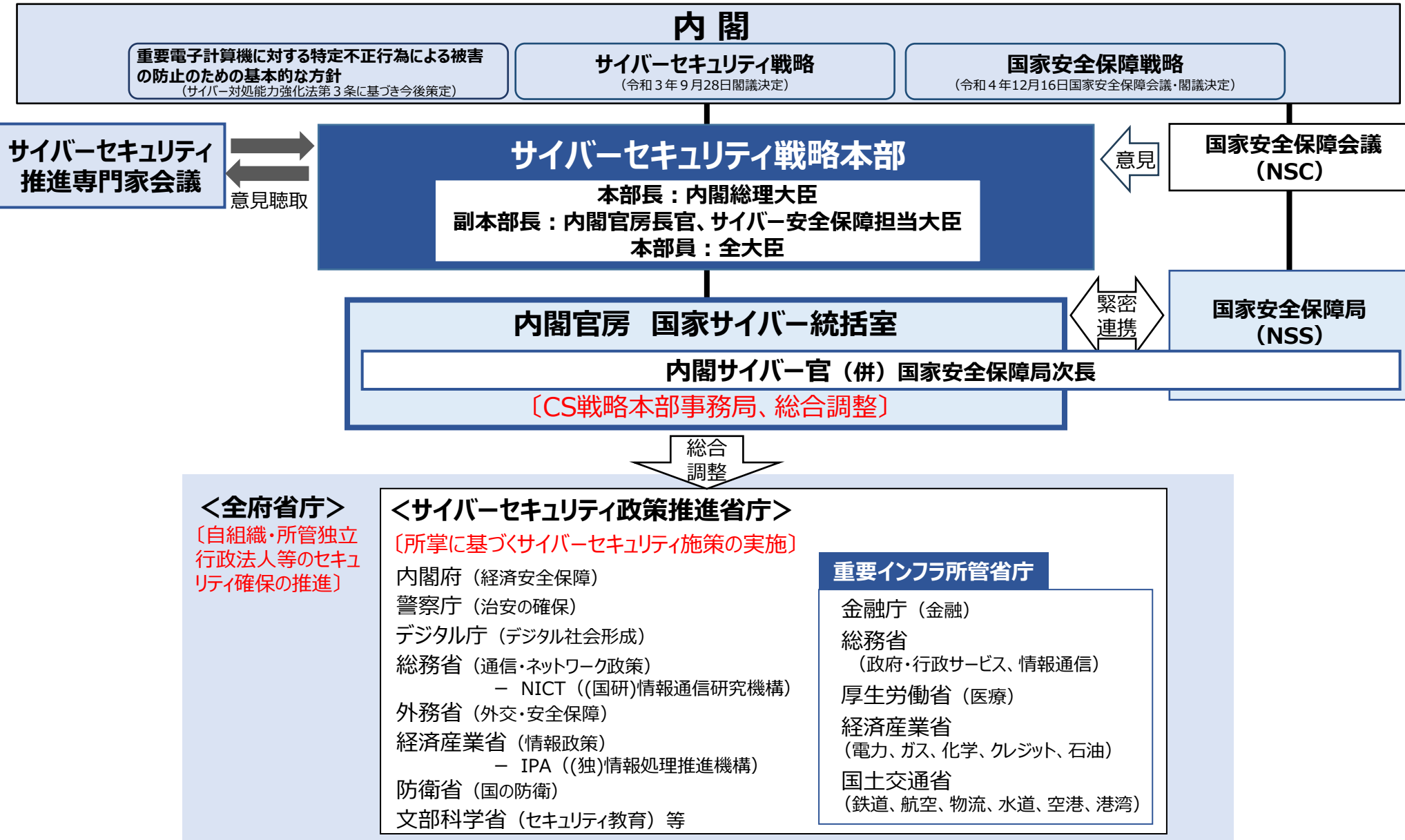
- 武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備することとし、以下の(ア)から(ウ)までを含む必要な措置の実現に向け検討を進める。
 - (ア) 重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化す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

改正後	改正前
<p>第四章 サイバーセキュリティ戦略本部 (所掌事務等)</p> <p>第二十六条 本部は、次に掲げる事務をつかさどる。</p> <p>一・二 (略)</p> <p><u>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</u></p> <p><u>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。</u></p> <p>五・六 (略)</p> <p>2 (略)</p> <p><u>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。</u></p> <p><u>二 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。</u></p> <p><u>三 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。</u></p> <p><u>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。</u></p> <p>4 (略)</p> <p>(サイバーセキュリティ戦略本部長)</p> <p>第二十八条 本部長は、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、<u>内閣総理大臣</u>をもって充てる。</p> <p>2～4 (略)</p> <p>5 (削る)</p> <p>(サイバーセキュリティ戦略本部員)</p> <p>第三十条 (略)</p> <p>2 本部員は、<u>本部長及び副本部長以外の全ての国務大臣</u>をもって充てる。 (削る)</p> <p>(資料の提出その他の協力)</p> <p>第三十三条 (略)</p> <p><u>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。</u></p> <p><u>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。</u></p>	<p>第四章 サイバーセキュリティ戦略本部 (所掌事務等)</p> <p>第二十六条 本部は、次に掲げる事務をつかさどる。</p> <p>一・二 (略)</p> <p>(新設)</p> <p><u>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。</u></p> <p>四・五 (略)</p> <p>2 (略)</p> <p>(新設)</p> <p>3 (略)</p> <p>(サイバーセキュリティ戦略本部長)</p> <p>第二十八条 本部長は、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、<u>内閣官房長官</u>をもって充てる。</p> <p>2～4 (略)</p> <p>5 (略)</p> <p>(サイバーセキュリティ戦略本部員)</p> <p>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。</p> <p>2 本部員は、<u>次に掲げる者（第一号から第六号までに掲げる者にあつては、副本部長に充てられたものを除く。）</u>をもって充てる。</p> <p>一～五 (略)</p> <p>(資料の提出その他の協力)</p> <p>第三十三条 (略)</p> <p>(新設)</p>

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



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

内閣官房 (総合調整)

内閣府 (実施事務)

内閣総理大臣・官房長官

国務大臣

特命担当大臣

官房副長官

危機管理監

国家安全保障局長

独立機関

内閣サイバー官 (併) 国家安全保障局次長

次官

副長官補
内閣情報官
内閣広報官

新たな
司令塔

強力な総合調整、戦略策定を担う組織

兼務

官民連携、
通信情報の利用等、
実施事務を担う組織

強力な総合調整

相互協力

官民連携

通信情報

重要インフラ・
基幹インフラ所管省庁

アクセス・無害化
実施省庁

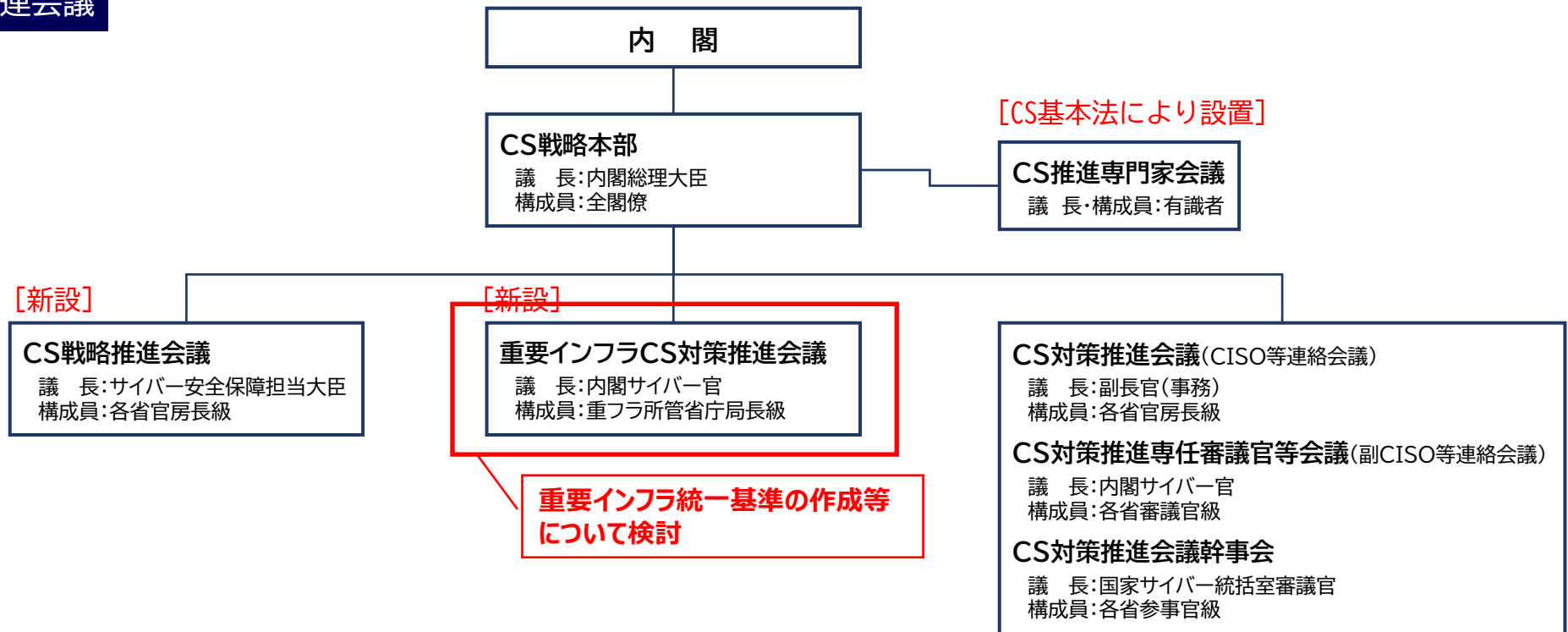
サイバー情報関係省庁

基幹インフラ等

通信事業者

- 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



- 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サイバーセキュリティ対策の推進を図るため、内閣サイバー官を議長とし、関係行政機関の局長級で構成される、重要インフラサイバーセキュリティ対策推進会議を開催。

構成員

議長	飯田 陽一	内閣サイバー官
副議長	木村 公彦	内閣官房内閣審議官（国家サイバー統括室）
構成員	柳瀬 護	金融庁総合政策局総括審議官
	三田 一博	総務省サイバーセキュリティ統括官
	原口 剛	厚生労働省政策統括官（統計・情報システム管理、労使関係担当）
	野原 諭	経済産業省商務情報政策局長
	長井 総和	国土交通省大臣官房政策立案総括審議官

検討内容

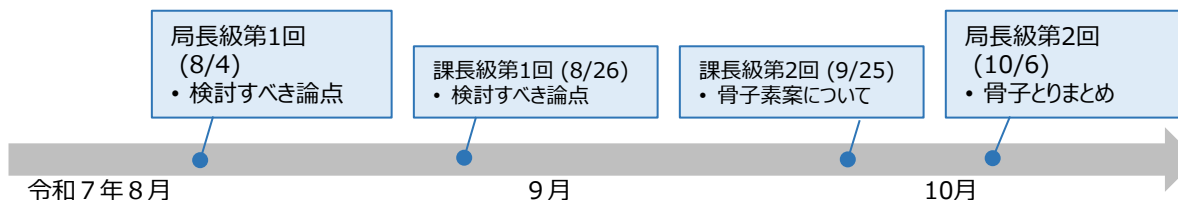
- (1) 重要インフラ防護に資するサイバーセキュリティ対策の基本的枠組みについて
- (2) 重要インフラ防護に資するサイバーセキュリティ対策の推進について
- (3) その他重要インフラ防護に資するサイバーセキュリティ対策に関し必要な事項について

【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

➡ 当面検討すべき論点について、骨子（今後の取組方向性）をとりまとめ

これまでの検討状況



➡ 基準の具体化検討に当たり、各重フ分野における特性や実情、現状課題等を考慮

- 我が国全体の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向けて、重要インフラサイバーセキュリティ対策推進会議における検討に資するため、内閣サイバー官の私的懇談会として、重要インフラサイバーセキュリティ研究会を開催。

開催趣旨

- 重要インフラサイバーセキュリティ対策推進会議における検討に当たり、各重要インフラ分野における特性・実情の把握や現状課題の整理、それらを踏まえた議論等を通じて、民間有識者の知見・示唆を得るため開催。

検討内容

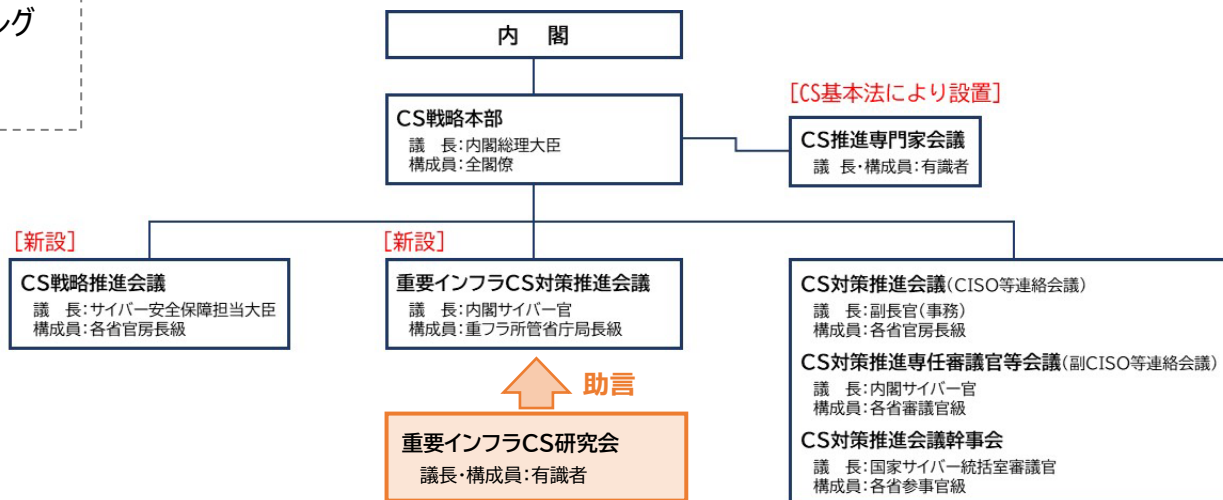
- 各重要インフラ分野における特性・実情の把握及び現状課題の整理
- 重要インフラ統一基準（ガイドライン含む）の検討に資する助言
- 重要インフラのサイバーセキュリティに係る行動計画の検討に資する助言
- その他

開催頻度

- 今年度は3回程度。

今後のスケジュール案

- 第1回（11/5）：キックオフ、分野別ヒアリング
- 第2回（12月頃）：分野別ヒアリング
- 第3回（2月頃）：基準案への助言

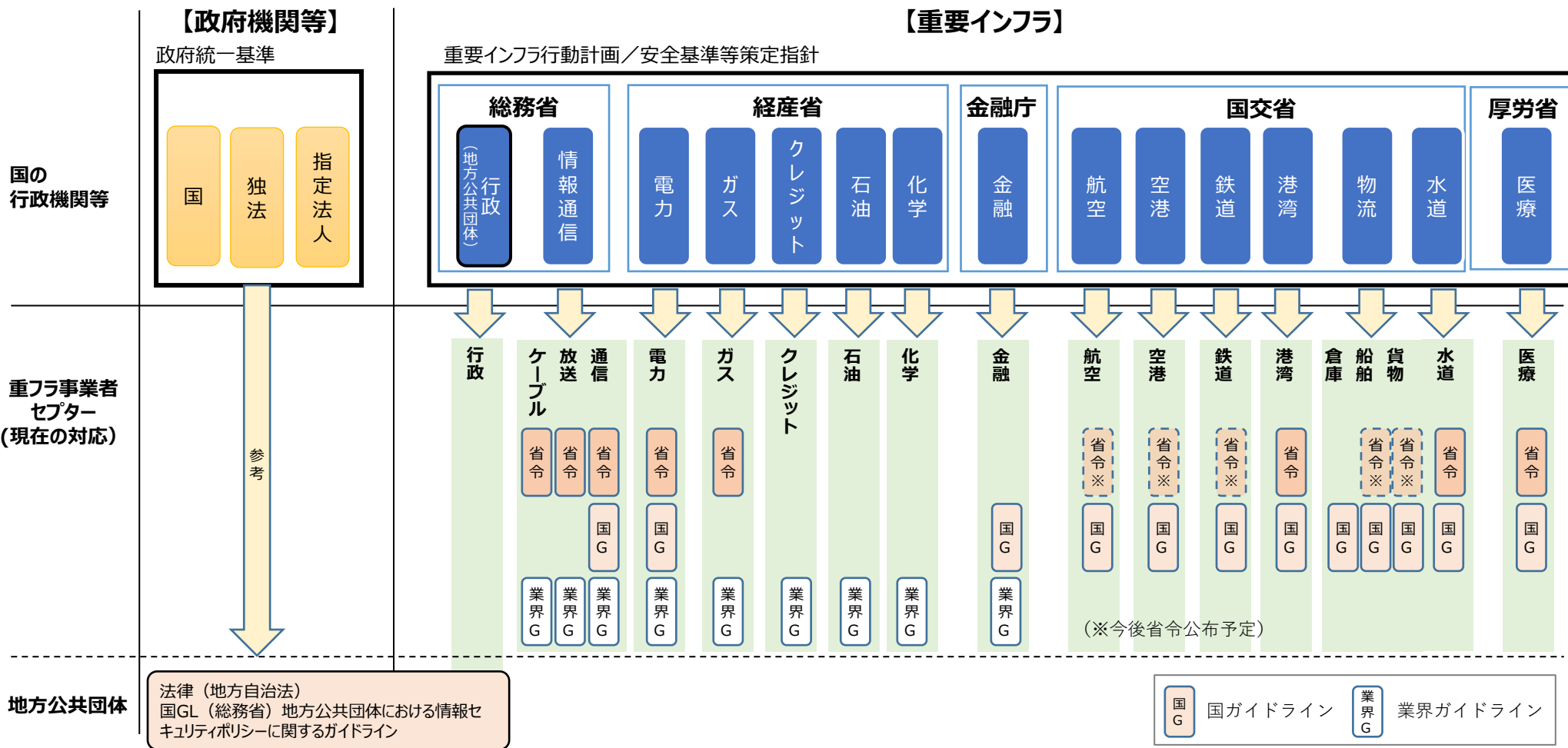


重要インフラサイバーセキュリティ対策推進会議
骨子－今後の取組方向性－

骨子2. 重要インフラ統一基準の作成

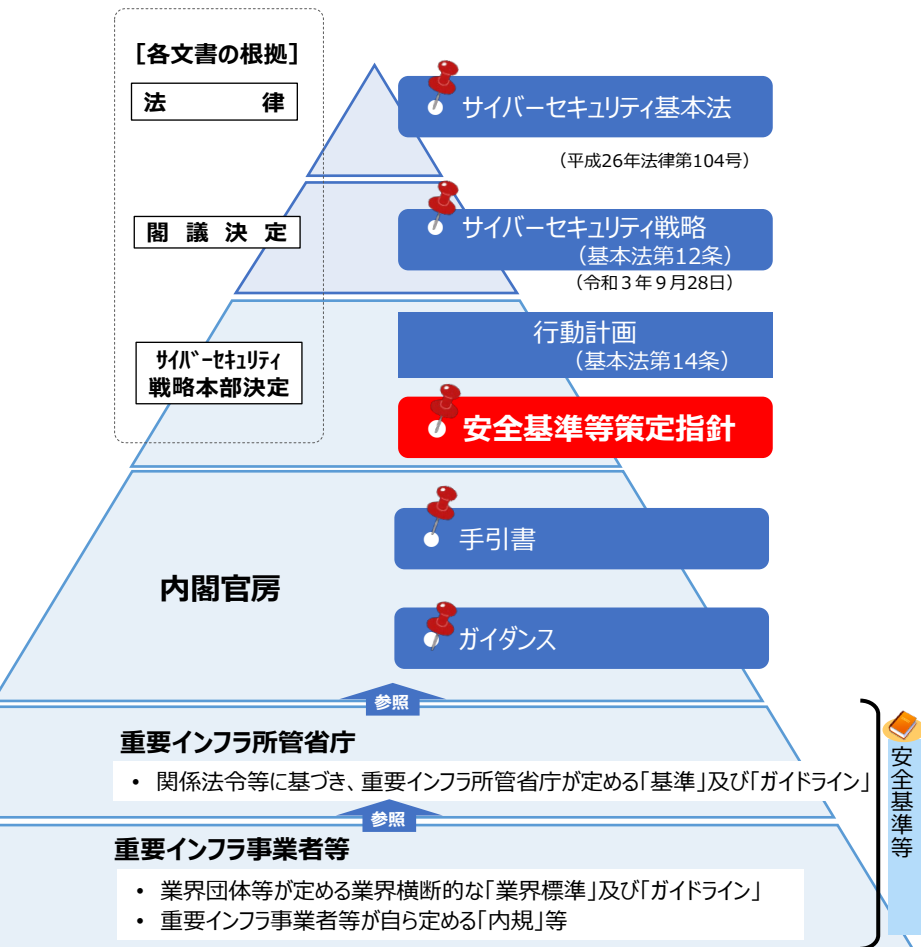
現状課題：分野・事業者によるサイバーセキュリティ確保のばらつき

- 各重要インフラ分野においては、現在、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。
- 他方で、各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、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。

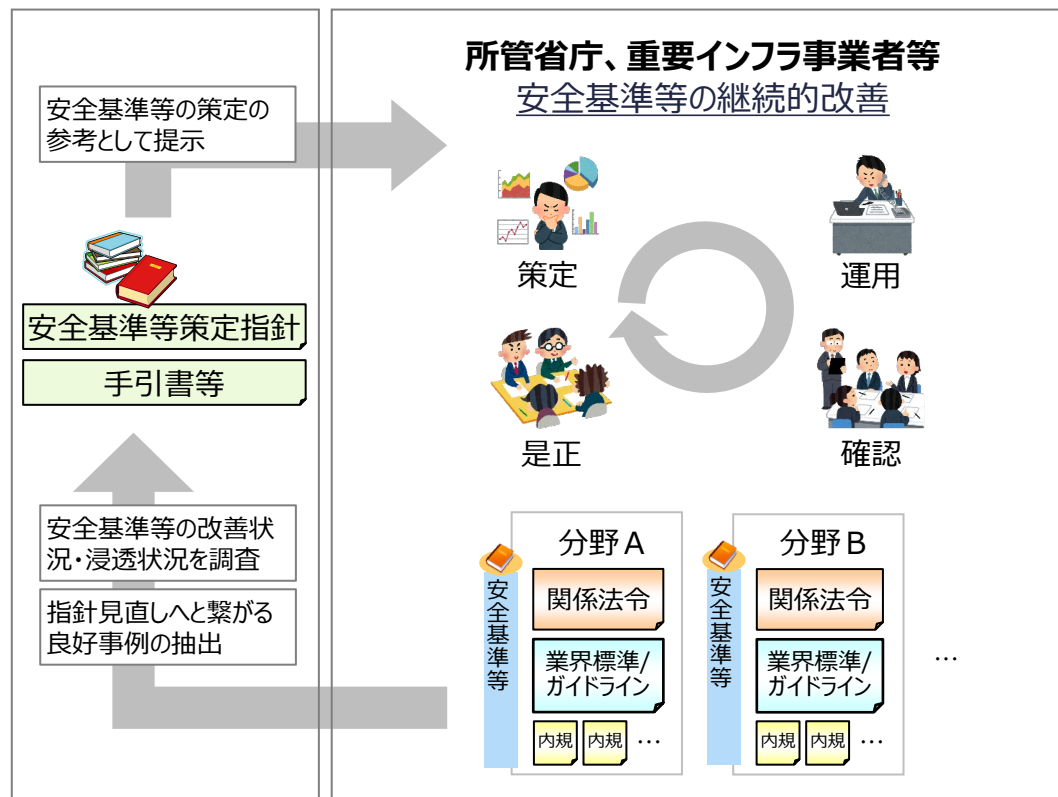


安全基準等策定指針※とは、重要インフラサービスの安全かつ持続的な提供を図る観点から、**安全基準等において規定が望まれる項目を整理・記載**し、重要インフラ事業者や重要インフラ所管省庁の「安全基準等」の策定・改定を支援することを目的とするもの。

※ 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）

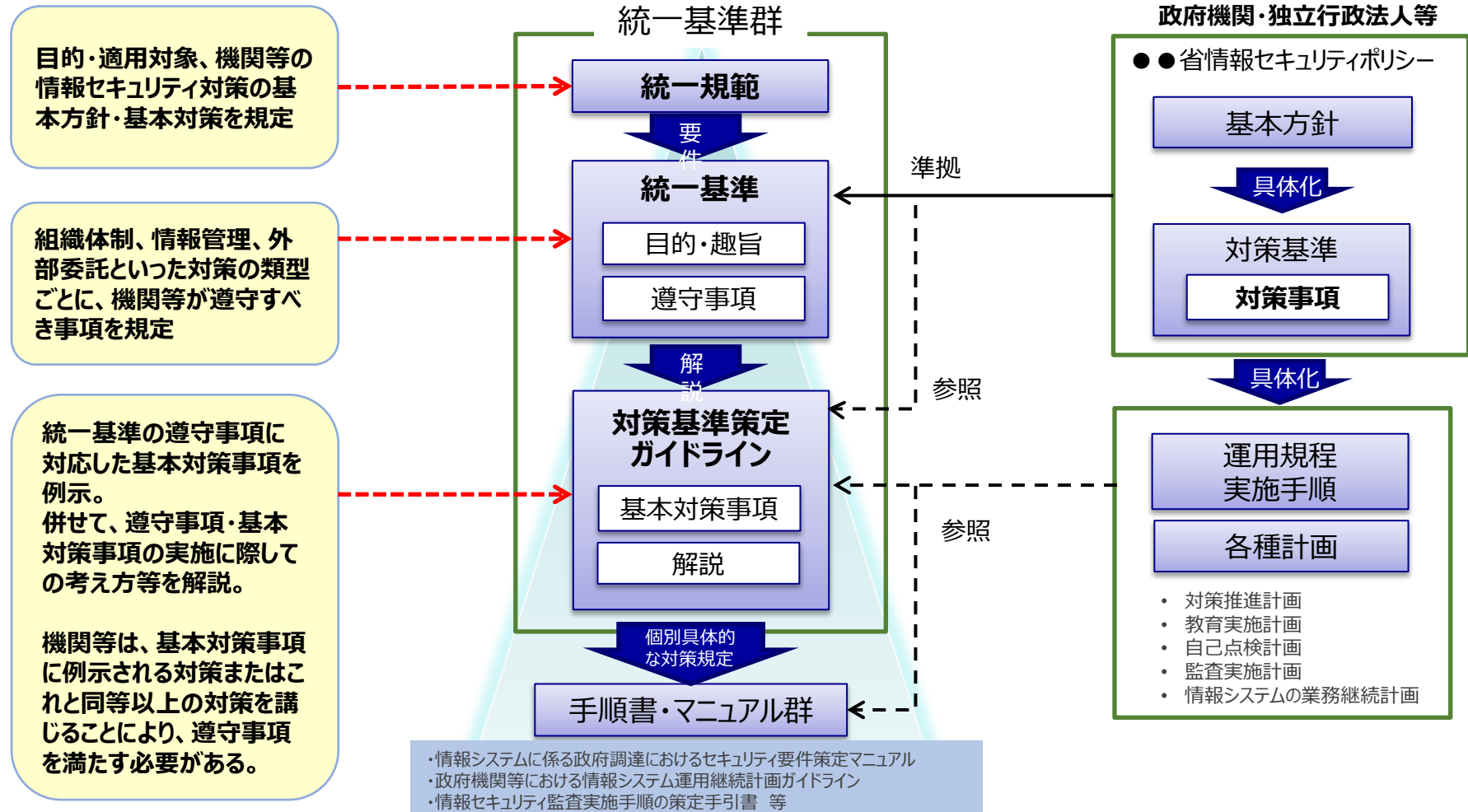


【安全基準等策定指針の活用方法】



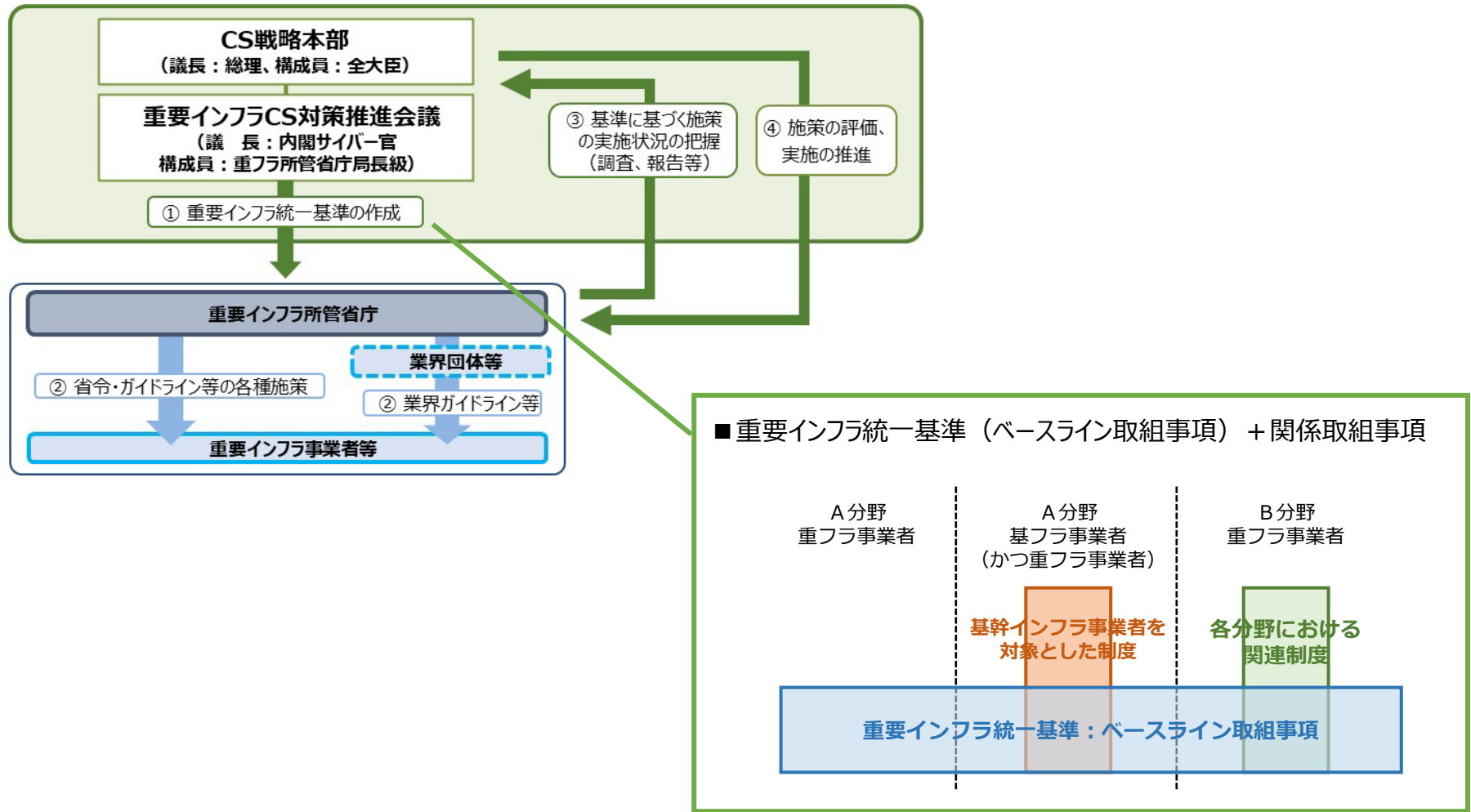
✓ 政府機関及び独立行政法人等は、**政府統一基準**※に準拠しつつ、組織及び取り扱う情報の特性等を踏まえ**各組織の情報セキュリティポリシー**を策定。

※ 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）



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）

- 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に関する国の行政機関の施策について、新たに重要インフラ統一基準を定め、各分野における国や業界団体等による基準・ガイドライン等への反映、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、それら関係省庁における施策や重要インフラ事業者等における取組の評価及び改善を図ることにより、重要インフラにおけるサイバーセキュリティ強化の実効性を確保する。



骨子2. 重要インフラ統一基準の作成

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、次について考慮する。
 - 現行制度等：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
 - 関係制度：経済安全保障推進法やサイバー対処能力強化法に基づく基幹インフラ事業者を対象とした制度
 - 国際標準等：国際標準規格や諸外国における取組、技術・脅威の動向等

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

- 基幹インフラ事業者を対象とした制度
 - ✓ 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）
 - ✓ 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



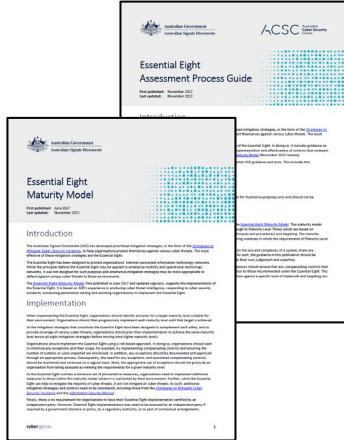
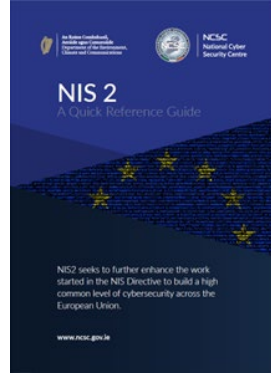
重要インフラ事業者等において分野・事業者横断的に講ずべきサイバーセキュリティ対策（ベースライン）を徹底し重要インフラ分野全体におけるサイバーセキュリティ水準を引上げ

骨子3. 重要インフラ防護範囲の在り方 重要インフラ事業者等と基幹インフラ事業者

- 重要インフラ事業者等と基幹インフラ事業者は、それぞれ法律の趣旨の下に対象分野・事業者が定められており、それらの間には差異が見られる。
- 基幹インフラ事業者は、サイバー対処能力強化法に基づきインシデント報告等が求められるなど、サイバーセキュリティ確保の重要性が増大していることに鑑み、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、それぞれの特性を踏まえつつ、新たに重要インフラ防護の対象として位置付ける等、重要インフラ防護範囲の在り方の見直しを検討する。

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）	放送（地上基幹放送）
	郵便（郵便事業）
—	金融（銀行業、系統中央機関が行うもの、資金移動業 等）
金融（銀行等、生命保険、損害保険 等）	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）
クレジット（クレジットサービス）	—
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）	—

- 諸外国では、**レジリエンスの強化**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、**対策強化の優先順位等の判断の困難性**や、それによる**成熟度のばらつき**に課題があるとの認識
- そのため、近年、各国では、**特に重要な事項として**、優先順位をつけて分野横断的な対策の**ベースラインを明示**

米 (CISA)	英 (NCSC)	豪 (ACSC)	EU
<p>Cross-Sector Cybersecurity Performance Goals (CPGs) (2022策定、2023更新)</p> 	<p>Cyber Assessment Framework (CAF) (2019策定、2024最終更新)</p> 	<p>Essential Eight Maturity Model (2017策定、2023最終更新)</p> 	<p>NIS2指令 (Network and Information Systems Directive 2) (2022発表)</p> 
<ul style="list-style-type: none"> ・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。 <p>※CSF: Cyber Security Framework</p>	<ul style="list-style-type: none"> ・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。 <p>※IGPs: Indicators of Good Practice</p>	<ul style="list-style-type: none"> ・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)。 	<ul style="list-style-type: none"> ・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。

- 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。

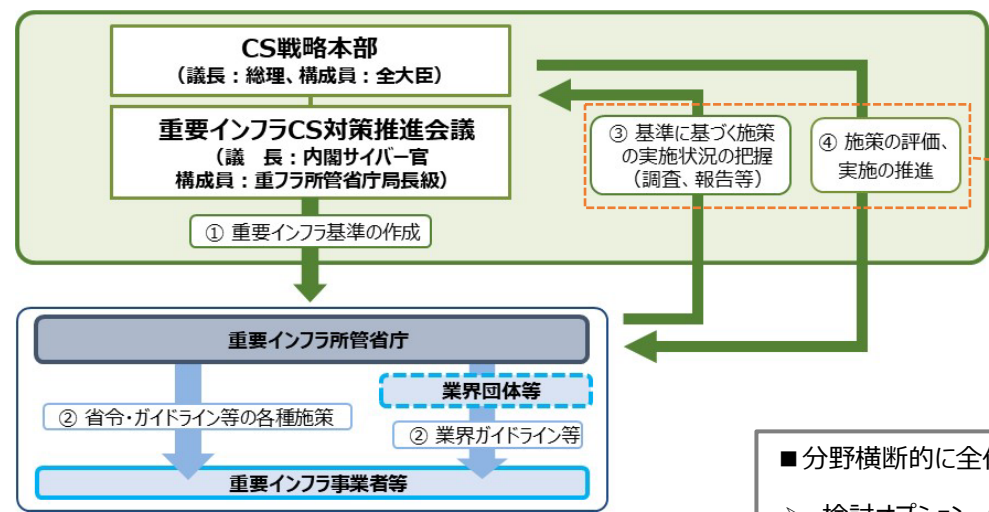
	米 (CISA)	英 (NCSC)	豪 (ACSC)	EU
基準名	Cross-Sector Cybersecurity Performance Goals (CPGs)	Cyber Assessment Framework (CAF)	Essential Eight Maturity Model	NIS2指令 (うちリスク管理措置)
適用対象	重要インフラ全体	国家重要インフラを含む民間事業者	重要インフラを含む様々な組織	基幹事業者及び重要事業者
主な内容	1. 識別 資産インベントリ、ITとOTのサイバーセキュリティ関係の改善、既知の脆弱性の緩和、サプライチェーンでのインシデントの報告等 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 (脆弱性対策等) ・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

骨子4. 施策の評価及び改善の方法

サイバーセキュリティ確保の着実なレベルアップが図られる仕組み

- 各分野の重要インフラ事業者等における取組や、それらに関する所管省庁の施策の実施状況について、調査及び評価を実施。それらの結果を踏まえ、取組や施策の改善につなげることで、重要インフラ分野全体におけるサイバーセキュリティ水準の引上げを図る。
- 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を記載した「対策基準策定ガイドライン」は、重要インフラ統一基準から各分野の基準・ガイドライン等への反映を通じて、官民の間で共通理解を形成し、サイバーセキュリティ強化に努めることができるような、実効性のあるものとする。
- 現状、分野・事業者によって、サイバーセキュリティ確保の取組やその水準についてばらつきが見られることを踏まえ、各分野におけるサイバーセキュリティ確保の取組水準の着実なレベルアップが図られる仕組みにする。



- 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。

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

【基準作成に当たっての考慮事項等】

- 基準作成にあたり、①国際基準等との整合性、②重要インフラ事業者と委託先との間での共通理解の形成や実効性確保が可能な枠組み、③啓発活動など重要インフラ事業者の理解促進のためのフォローアップの3点の検討をお願いしたい。
- サードパーティに対してもサイバーセキュリティ対策が求められるという理解を醸成する内容となるよう期待。
- 重要インフラ事業者が前向きに取り組むことができるよう、取組の意義やメリット、取組を行わない場合のリスクを示すことも必要。
- 重要インフラ事業者における自主的な取組が進む一方で、高度な攻撃への備えが必要。地方公共団体における対策の状況は様々であり、多様性を踏まえた支援と全体の底上げが重要。基準は、重要インフラ事業者等に過度な負担をかけず、実効性があり、現場の対策に役立つものとするのが重要。
- 重要インフラ事業者の数が多く、規模や取組も様々であること等から、官民で実行可能な枠組みとなるよう、前広な情報提供と丁寧な合意形成をお願いしたい。
- 医療分野はセキュリティ対策への投資余力が無い等の課題がある。基準の具体化検討に当たっては、現場の実情に合わせた対策レベルとする等の考慮が必要。
- 事業者によって規模や取組が様々ある中で、全体としてレベルが上がっていくような仕組みを検討。
- 基準の検討に当たっては、業界団体等によるガイドライン等を含め、既存の制度との整理も考慮することが必要。また、JC-STAR制度等の評価制度の活用促進について基準に反映いただきたい。

【基準とあわせて行うべき取組】

- 経営資源が限られた中小規模の重要インフラ事業者においては、重要インフラ統一基準を満たすことが難しい場合も考えられる。これらの事業者が取り残されないよう、支援の枠組みを検討することも必要。
- 医療分野においては、今後、重要インフラ統一基準を具体化するに際し、業界に対する支援についても分かりやすく示すことが、業界の理解の促進につながる。

【基準の作成に伴う行動計画の見直し】

- 行動計画の見直しに当たっては、強化法施行後のセキュリティ対策の全体像と必要性が、経営層を含む関係者に広く理解されるものとすることが重要。
- 今後、検討を進めるにあたっては、重要インフラ事業者にとって基準や行動計画それぞれの位置付けが分かりやすいものとなるよう、全体の体系を整理いただきたい。

(参考) 諸外国における取組

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) 、プロフィール (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))
プロフィール (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。

	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。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 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



組織プロフィールを作成、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

(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

- 米国では、重要インフラ事業者、特に中小組織への体制整備等の支援を念頭に、最低限のベースラインとしてCross-Sector Cybersecurity Performance Goals (CPGs)を策定。
- 対策は、NIST CSF ver.1.1の分類に沿って提示され、当該文書のクイックスタートガイドとしても機能するよう設計されている。

取組の概要

項目名	概要
策定目的	<ul style="list-style-type: none">■ 重要インフラ業務と米国民の両方に対するリスクを有意義に低減すること。■ CPGsは、包括的なサイバーセキュリティプログラムを反映したものではなく、組織が実装することが望ましい最低限のプラクティスであり、重要インフラ事業者、特に中小組織への体制整備等の支援を目的としている。
策定年月	■ 2023年3月
策定組織	■ サイバーセキュリティ・インフラセキュリティ庁 (CISA)
適用対象	■ すべての重要インフラ組織 ※ サイバーセキュリティの経験、リソースが不足している組織、体制が整っていない組織を含む
対策向上の仕組み	■ CPGsのプラクティスは最低限のベースラインを示すものであり、「成熟度」のカテゴリに階層化されていない。 ※ 階層化された枠組みについては、別途NIST CSFにおける「CSFティア」を参照すること等が考えられる。

規定の概要

識別 (Identify)

資産インベントリ、組織的なサイバーセキュリティのリーダーシップ、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 計9項目

防御 (Protect)

デフォルトパスワードの変更、最小のパスワード強度、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、不正な機器の接続禁止、公衆インターネットへのOT接続の制限 等 計25項目

検知 (Detect)

関連する脅威及びTPPの検知 計1項目

対応 (Respond)

インシデント報告、脆弱性報告、SECURITY.TXT ファイルの配置 計3項目

復旧 (Recover)

インシデント計画及び準備 計1項目

- CSETは米CISAが提供する質問ベースの自己診断ツールであり、利用者はツールのガイドに沿って自社の体制・対策状況に関する質問に回答する。質問は事前に選択したセキュリティ規格やフレームワークに基づいて自動生成される。
- CSETが対応可能な基準（15程度）にはCPGsも含まれる。

■ 概要

- ✓ CSETは組織のセキュリティ体制を自己評価するのに必要な以下のような包括的な機能を備える。
- ✓ 評価実施者にて基準を選択したうえで、当該基準に応じた質問に回答する。
- ✓ CSETが対応可能な基準（15程度）にはCPGsも含まれる。

機能	説明
ICS/OT・IT統合評価	ICSやSCADA等の制御システムと、企業ITネットワークを一括評価。
質問ベースのセルフアセスメント	対策状況を問う質問にYes/No回答し、段階的に詳細深掘り。
ギャップ分析と改善提案	回答結果から未実施・不十分な対策を抽出し、推奨改善策を提示。
標準フレームワーク対応	NISTやISO等の主要基準を内蔵し、選択した基準に沿って評価実施。
レポート生成と可視化	スコアチャートや優先度付き対策リスト等の報告書を自動作成。
ネットワーク図編集・資産インベントリ	資産リストやネットワーク構成図をツール上で作成・管理。
SSP計画書カスタマイズ出力	組織のセキュリティ計画書(System Security Plan)を自動生成。
モジュール追加・カスタム評価	組織独自の質問セットを作成可能。ランサム対策等の新モジュール提供。

■ ツールの概要

- ✓ CSETは質問ベースの自己診断ツールであり、利用者はツールのガイドに沿って自社の体制・対策状況に関する一連の質問に回答する。質問は事前に選択したセキュリティ規格やフレームワークに基づいて自動生成される。

Access Control - Standard Questions

Access Agreements

Do you have any access agreements (formal or informal) for third party access to your system? Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, operational or service level agreements and conflict-of-interest agreements.

1 Are appropriate agreements finalized before access is granted, including for third parties and contractors?

Reviewed

2 Are access agreements periodically reviewed and updated?

Reviewed

Evaluation

- Facility Cybersecurity framework (FCF) は、米国エネルギー省等が提供する NIST CSFに準拠したサイバーセキュリティリスク管理の推進を補助する自己診断ツールであり、NIST CSFの定義する成果に対する対応状況に関する評価(FI：完全に実施/LI：概ね実施/PI：部分的に実施/MI：未実施)を行わせることが可能。

■ ツールの概要

- ✓ FCFは、米DoE等が提供するNIST CSFに準拠した自己評価ツールであり、成熟度モデルに近い形で評価を行わせるものである。
- ✓ 回答者はNIST CSFのフレームワークコアに対応した100件超の設問に対して、対応状況を以下のように、FI/LI/PI/NIの4つから選択して回答する。

FCFの回答画面

	FI Fully Implemented	LI Largely Implemented	PI Partially Implemented	NI Not Implemented
<p>1. Networks and network services are monitored to find potentially adverse events The federal facility monitors networks and network services to detect potentially adverse events. Continuous monitoring helps identify and respond to threats promptly, maintaining the security and integrity of the network infrastructure.</p> <p>Implementation Notes ></p>	✓	✓	✓	✗

対応状況の考え方

分類	定義
完全に実施(FI)	<ul style="list-style-type: none"> ■ ポリシーが整備されており、設定されたポリシーに従って対応が実施されている。 ■ 担当者が割り当てられ、責任を負っている。
概ね実施(LI)	<ul style="list-style-type: none"> ■ 規定が整備されており、定められた方針に従って実施されている。 ■ この件について責任を負う担当者がいない。
部分的に実施(PI)	<ul style="list-style-type: none"> ■ 場当たりに実施されている。 ■ 方針が存在しない。 ■ 責任者として割り当てられた者がいない。
未実施(MI)	<ul style="list-style-type: none"> ■ 実際には行われていない。 ■ 関連する方針が存在しない。 ■ 本件を担当する責任者が割り当てられていない。

[出典] Facility Cybersecurity

<https://facilitycyber.labworks.org/>

User Guide to the Facility Cybersecurity Framework (FCF) Core Assessment

<https://facilitycyber.labworks.org/media/User%20Guide%20to%20the%20FCF%20Core%20Assessment.pdf>

- Cyber Assessment Framework (CAF)は、主に政府、重要インフラ等を対象にした枠組であり、サイバーセキュリティリスク管理で達成すべき4つの目的に対応する14の原則を提示し、原則毎に具体的に実施すべき項目(IGP)を明示。
- IGPの達成状況により、原則の実施状況は、「達成」、「部分的達成」、「未達成」のいずれかに分類される。

取組の概要

項目名	概要
策定目的	<ul style="list-style-type: none"> ■ 組織が自社のサイバーセキュリティとレジリエンスを評価・改善し、サイバーリスクを管理し、重要サービスをサイバー脅威から保護すること
策定年月	<ul style="list-style-type: none"> ■ 2025年8月 ※最新版(v4.0)の公開
策定組織	<ul style="list-style-type: none"> ■ 国家サイバーセキュリティセンター(NCSC)
適用対象	<ul style="list-style-type: none"> ■ 主に、エネルギー、医療、運輸、デジタルインフラ、政府等の分野で重要サービスを運営する組織
対策向上の仕組み	<ul style="list-style-type: none"> ■ 達成すべき成果は優れた実践の指標(IGP)に紐づいており、IGPの実施状況により成果の達成状況は以下3種類に分類される。 <ul style="list-style-type: none"> ✓ 未達成：成果未達成の組織の典型的な特徴に該当 ✓ 部分的達成：「部分的達成」のために定義された指標を全て達成 ✓ 達成：「達成」のために定義された指標を全て達成

[出典] Cyber Assessment Framework 4.0
<https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf>
<https://www.ncsc.gov.uk/collection/cyber-assessment-framework>

規定の概要

- ✓ 4つの目的に対応する14の原則を提示し、原則毎にIGPを規定。

目的A：セキュリティリスク管理

ガバナンス、リスク管理、資産管理、サプライチェーン 計4原則

目的B：サイバー攻撃に対する保護

サービス保護ポリシー・プロセス・手順、アイデンティティ・アクセス制御、データセキュリティ、システムセキュリティ、ネットワークとシステムのレジリエンス、従業員の意識向上と訓練 計6原則

目的C：サイバーセキュリティ事象の検知

セキュリティ監視、脅威ハンティング 計2原則

目的D：サイバーセキュリティインシデントの影響最小化

対応・復旧の計画、教訓の学習 計2原則

- ✓ 原則毎のIGPは、未達成、部分的達成、達成という3分類にて提示。

未達成	部分的達成	達成
以下の1つ以上が該当	「部分的達成」に必要な以下すべてを実施	「達成」に必要な以下すべてを実施
<ul style="list-style-type: none"> ■ リスク評価が明確な脅威の想定に基づいていない ■ … 	<ul style="list-style-type: none"> ■ 社内プロセスによりリスクが特定、分析、優先順位づけ、管理されている。 ■ … 	<ul style="list-style-type: none"> ■ 社内プロセスによりリスクが特定、分析、優先順位づけ、管理されている。 ■ …

- Cyber Essentialsは、一般的なサイバー攻撃からの防御を念頭に置いた最低限の要求事項を課し、遵守が認められる企業等を認証する枠組みで、自己宣言をベースとしたものと、第三者機関による技術的監査を行うもの(Cyber Essentials Plus)を設けている。
- 要求事項としては、セキュア構成、利用者アクセス制御、マルウェア保護、セキュリティアップデート管理、ファイアウォールの5つを規定。

■ 取組の概要

項目名	概要
制度の目的	<ul style="list-style-type: none"> ■ 一般的なサイバー攻撃から組織や顧客のデータを守ることを支援する最低限の要求事項の実装を促進すること。
開始年月	<ul style="list-style-type: none"> ■ 2014年6月 ※要求事項等は都度改定
関係組織	<ul style="list-style-type: none"> ■ 制度所管：科学イノベーション技術省(DSIT) ■ 技術支援：国家サイバーセキュリティセンター(NCSC)
適用対象	<ul style="list-style-type: none"> ■ あらゆる規模及び分野の組織
対策向上の仕組み	<ul style="list-style-type: none"> ■ 要求事項はあくまでベースラインを示すものであり階層化されていないが、上位の認証区分(Cyber Essentials Plus)では要求事項遵守をより高い確度で確認するため、取得にあたり技術的監査を受ける必要がある。

■ 規定の概要

セキュア構成

- ✓ 不要なアカウントを削除し、デフォルト又は推測容易なパスワードを変更すること
- ✓ 端末ログイン連続失敗時の端末ロックの仕組みを導入すること 等

利用者アクセス制御

- ✓ クラウドサービス利用時に多要素認証を適用すること
- ✓ パスワード認証において安全なもの(例：8桁以上で危険なものを自動ブロック)を利用すること 等

マルウェア保護

- ✓ 適用範囲内の全ての機器へマルウェア対策を講じること

セキュリティアップデート管理

- ✓ 適用範囲内の機器上のソフトウェアから不要機能を削除すること
- ✓ 重大な脆弱性をリリース後14日以内に修正すること 等

ファイアウォール

- ✓ 適用範囲内の全ての機器をファイアウォール等により保護すること
- ✓ ファイアウォール等を適切に設定すること 等

[出典] Cyber Essentials

<https://www.ncsc.gov.uk/cyberessentials/overview>

Cyber Essentials: Requirements for IT Infrastructure v3.2

<https://www.ncsc.gov.uk/files/cyber-essentials-requirements-for-it-infrastructure-v3-2.pdf>

- Essential Eight Maturity Modelは、サイバー脅威から組織を保護するための最も効率的な戦略として、パッチ適用、パッチ運用システム、多要素認証等の8つの優先的な対策領域を特定。
- 8つの領域それぞれについて、3段階からなる成熟度レベルごとに必要な対策を提示。

取組の概要

項目名	概要
策定目的	■ 様々なサイバー脅威から組織を保護するための最も効率的な戦略を提示すること
策定年月	■ 2023年11月 ※最新版の公開
策定組織	■ 豪州サイバーセキュリティセンター (ACSC)
適用対象	■ あらゆる規模及び分野の組織
対策向上の仕組み	<ul style="list-style-type: none"> ■ 以下のように4段階の成熟度を定義 ✓ 成熟度レベル0：組織全体のサイバーセキュリティ態勢に脆弱性がある状態 ✓ 成熟度レベル1：広く入手可能な汎用的な手法を活用する悪意ある攻撃者への対処 ✓ 成熟度レベル2：レベル1と比較して標的に多くの時間を費やし、ツールの有効性にも注力する攻撃者への対処 ✓ 成熟度レベル3：適応性が高く、公開ツールや手法への依存度が低い悪意のある攻撃者への対処

規定の概要

- ✓ 8つの対策カテゴリについて、3つの成熟度レベルごとに対策を提示。

パッチ適用

※一部の共通の対策を含む。

成熟度1：日次でのオンラインサービスの脆弱性スキャン 等 (計9件)

成熟度2：サポート切れオンラインサービスの削除 等 (計11件)

成熟度3：サポート切れの各種アプリケーションの削除 等 (計13件)

パッチ運用システム

多要素認証

管理特権の制限

アプリケーション管理策

マクロの制限

アプリケーションの堅牢化

定期的なバックアップ

- NIS2は、主要事業体及び重要事業体を対象に、インシデント報告義務等を定めることに加え、第21条でリスク管理措置の実施を求めている。
- リスク管理措置には、システムセキュリティに関する方針、インシデント対応、サプライチェーンのセキュリティ等の10項目が含まれる。

■ 取組の概要

項目名	概要
策定目的	<ul style="list-style-type: none"> ■ 社会的・経済的に重要な役割を担うインフラや企業におけるサイバーリスクの軽減と対応能力の向上 ■ 欧州全体で統一されたセキュリティ基準の確立
策定年月	■ 2024年10月 ※NIS2指令施行
策定組織	■ EU ※欧州委員会にて起草
適用対象	<ul style="list-style-type: none"> ■ 主要事業体 (エネルギー、運輸、銀行、金融市場インフラ、ヘルスケア、飲料水、下水、デジタルインフラ、公的サービス、宇宙等) ■ 重要事業体 (郵便・宅配、廃棄物管理、化学品、食品、製造業(医療機器、自動車等)、デジタルプロバイダー、研究)
対策向上の仕組み	■ 特になし

[出典] NIS2 Directive: securing network and information systems
<https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
 NIS2 Directive Final Text
https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html
 NIS2: Commission implementing regulation on critical entities and networks
<https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks>

■ 規定の概要

- ✓ 第21条にて以下10項目からなるリスク管理措置の実施を求める。
- ✓ 同管理措置は、実施法にて項目ごとに詳細化されている。

リスク分析および情報システムセキュリティに関する方針

リスク分析および情報システムセキュリティに関する方針

役割・責任・権限

インシデント対応

バックアップ管理、災害復旧、危機管理などの事業継続

サプライチェーンのセキュリティ

システムの取得、開発、保守におけるセキュリティ

リスク管理策の有効性を評価するための方針および手順

基本的なサイバー衛生の実践とサイバーセキュリティ研修

暗号の使用に関する方針と手順

人材のセキュリティ、アクセス制御ポリシー、資産管理

多要素認証または継続的認証ソリューション