赤枠内は非公開

資料１

# 重要インフラ統一基準等の検討について

令和８年７月６日
内閣官房国家サイバー統括室

# 今後の主なスケジュール（現時点の想定）



| | |
|---|---|
| 2026年4～5月 | 重要インフラ統一基準案についてのパブリックコメント |
| ７月 | **重要インフラ統一基準の策定**（サイバーセキュリティ戦略本部） |
| ８月頃 | 安全基準等策定ガイドラインについてのパブリックコメント |
| ９月頃 | **安全基準等策定ガイドラインの策定**（国家サイバー統括室） |
| 10月 | 重要インフラ統一基準の**施行** |
| 冬頃 | 重要インフラ統一基準に基づく**成熟度モデルCI-CSA等の実施** |
| 2027年春～夏頃 | 重要インフラ統一基準に基づく実施計画の策定（各政府機関） |

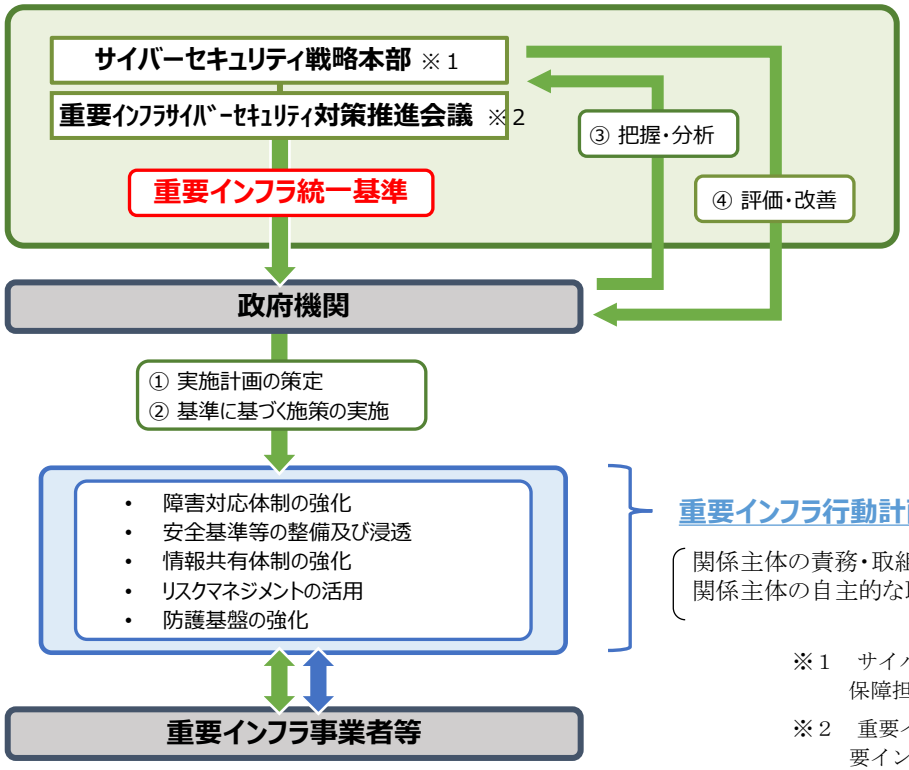
# 重要インフラ統一基準



- 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。




**重要インフラ統一基準**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。

**重要インフラ行動計画**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

※1　サイバーセキュリティ戦略本部：総理を本部長、内閣官房長官・サイバー安全保障担当大臣を副本部長、全ての国務大臣を構成員とする本部。

※2　重要インフラサイバーセキュリティ対策推進会議：内閣サイバー官を議長、重要インフラ所管省庁局長級を構成員とする会議。

# （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）　※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。

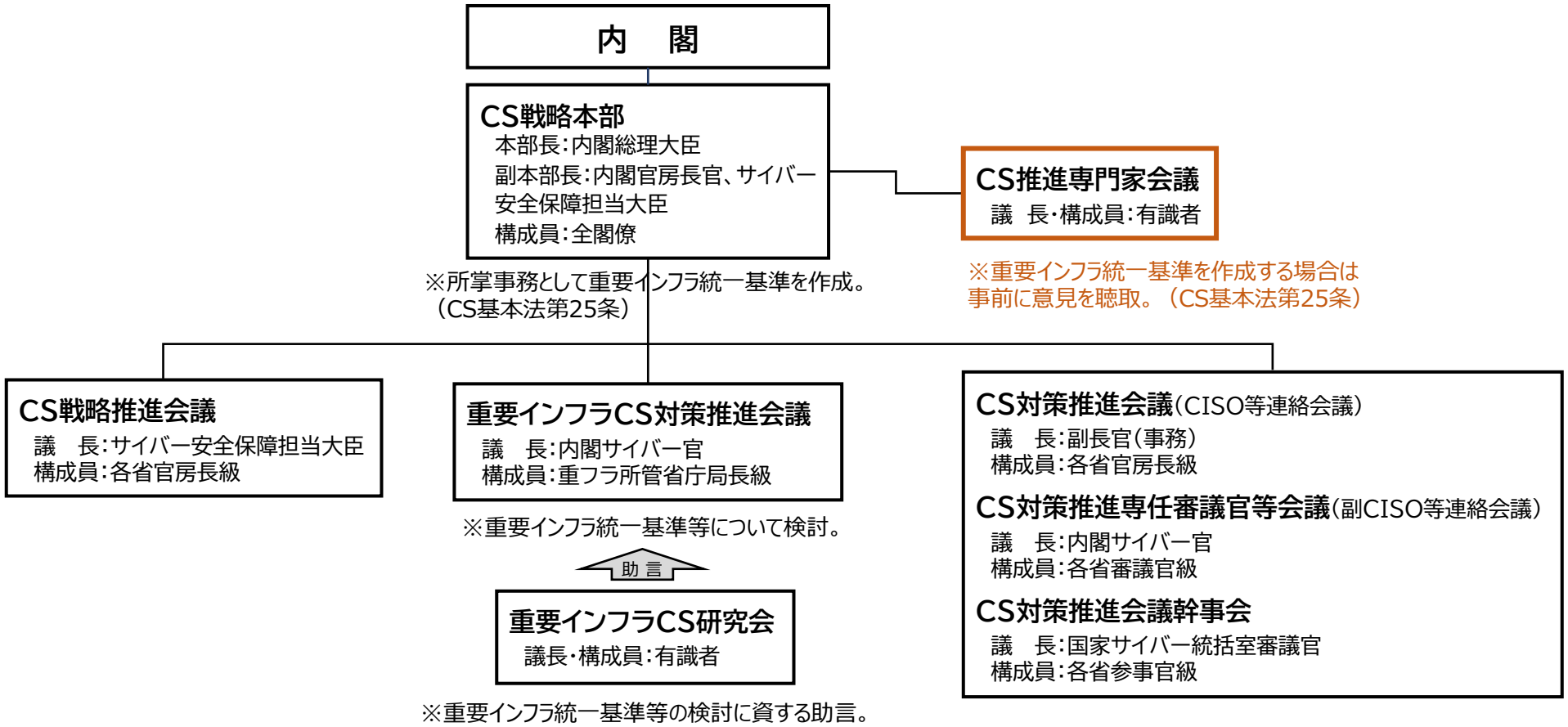
（資料の提出その他の協力）
第三十三条　本部は、その所掌事務を遂行するため必要があると認めるときは、地方公共団体及び独立行政法人の長（略）に対して、サイバーセキュリティに対する脅威による被害の拡大を防止し、及び当該被害からの迅速な復旧を図るために国と連携して行う措置その他のサイバーセキュリティに関する対策に関し必要な資料の提出、意見の開陳、説明その他の協力を求めることができる。この場合において、当該求めを受けた者は、正当な理由がある場合を除き、その求めに応じなければならない。
２　本部は、その所掌事務を遂行するため必要があると認めるときは、重要社会基盤事業者及びその組織する団体の代表者に対して、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

# （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～）。
- 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。



# 重要インフラ統一基準のポイント



- 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

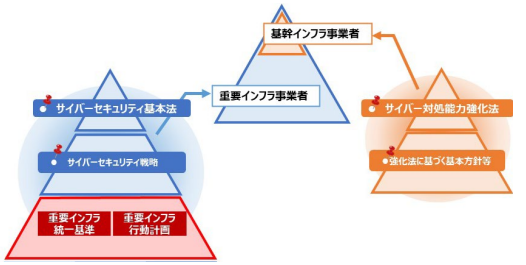
第３部　安全基準等において規定されるべき事項 ※１

- 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

## 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、閉域網という理由でサイバー攻撃が想定されていなかった基盤・制御システムにおいても、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。まずは認識のアップデートが重要。

**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**

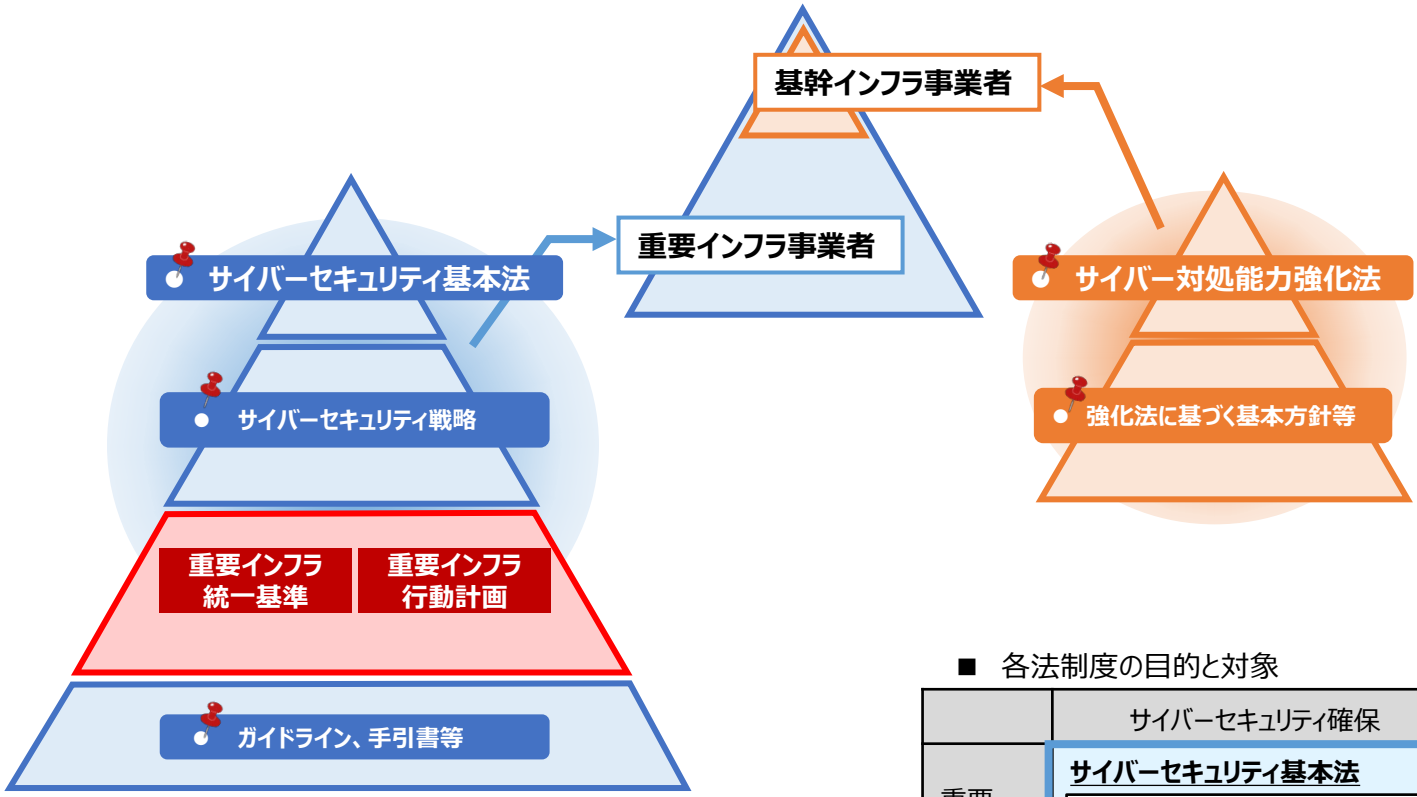
国家を背景とした攻撃キャンペーン等、深刻化するサイバー脅威に対しては、官のみ、民のみの防御では限界がある。サイバー攻撃による被害拡大防止に向けた官民双方向でのコミュニケーションの強化が重要。

※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「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」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。

# （参考）統一基準の適用範囲（重要インフラ防護範囲の見直し）



- 基幹インフラの対象範囲を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。




分野・事業者横断的に講ずべき基本的な対策を徹底

■ 各法制度の目的と対象

| | 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**<br>✓ 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**<br>✓ 資産届出（義務）<br>✓ インシデント報告（義務） 等 | **経済安全保障推進法**<br>✓ 特定重要設備の届出（リスク管理措置） 等 |

**【関連】 重要インフラ統一基準**
第１部　1.2　統一基準の適用範囲
第２部　2.1.1　施策の実施体制　（対象となる重要インフラ事業者等の特定）

# （参考）取り組むべき主な対策①～④



## ① 「閉域網だから安全」との考え方の刷新

- 従来、閉域網だから、専用OSだから、独自技術仕様だからという理由でサイバー攻撃が想定されていなかった基盤・制御システムにおいても、自動化やIoT化に伴いネットワーク接続機会が増加。
- 「閉域網」と思っていても、保守のために用いるリモートデスクトップやVPN、USBメモリを狙ったマルウェア感染リスク、さらには内部不正による感染リスクもあり。
- 「閉域網だから安全」といった過信が、サイバーリスクを高める。
- 資産やアカウントの管理、アクセス制御といった対策が必要。

**【関連】 重要インフラ統一基準　第３部**
- 3.1　基本的な考え方／(3)　対象範囲
- 3.3.1　資産の管理
- 3.4.1　アカウント管理・認証・アクセス制御
- 3.4.6　インフラストラクチャ（ネットワーク等）の対策　等

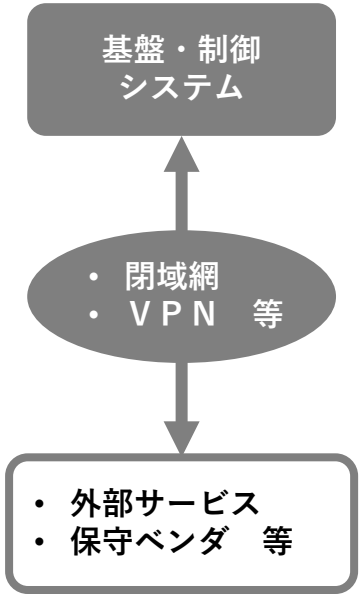
## ② サプライチェーン・リスクへの対応

- サイバー攻撃は、脆弱な部分が狙われる。
- 重要インフラサービスの提供に必要なサプライチェーンに関わる取引先や外部サービス等に潜む脆弱な部分を起点として、自組織が狙われるといった事案が頻繁に発生。
- 取引先のセキュリティ対策状況の把握、製品・サービスの調達に当たっての要求事項の整理、責任範囲の明確化といった対策の実施とともに、組織の壁を越えたサプライチェーン全体としての対策が求められる。

**【関連】 重要インフラ統一基準**
**第２部**
- 2.1.2　取り組むべき施策／（１）障害対応体制の強化

**第３部**
- 3.2.9　サプライチェーン・リスクマネジメント
- 3.4.7　クラウドサービス利用時の対策　等

＜基盤・制御システムのネットワーク構成例＞




## 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

- ネットワーク接続機会の増加等に加え、日々、サイバー攻撃の巧妙化・高度化が進む中、それら脅威からの完全な防御は困難。
- 重要インフラにおいて求められるのは、サイバーインシデントによる壊滅的被害を回避し、早期復旧によって、サービスの安全かつ継続的な提供を維持すること。
- そのためには、サイバー攻撃の防御・抑止のみならず、障害等が発生した際の影響を許容範囲内に抑制するレジリエンスの確保が必要。

**【関連】 重要インフラ統一基準　第３部**
- 3.1　基本的な考え方／（２）記載の観点及び構成（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）
- 3.4.2　意識向上とトレーニング　（人材育成、演習等）
- 3.4.3　データのセキュリティ対策　（バックアップ等）
- 3.4.6　インフラストラクチャの対策　（セグメント分割等）
- 3.6　対応及び復旧　（事業継続計画等）　等

## 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。

**【関連】 重要インフラ統一基準　第３部**
- 3.7　技術・脅威の動向等を踏まえた対策

① リスクベースの観点から、技術・脅威の動向等を踏まえ、対策を講ずる。

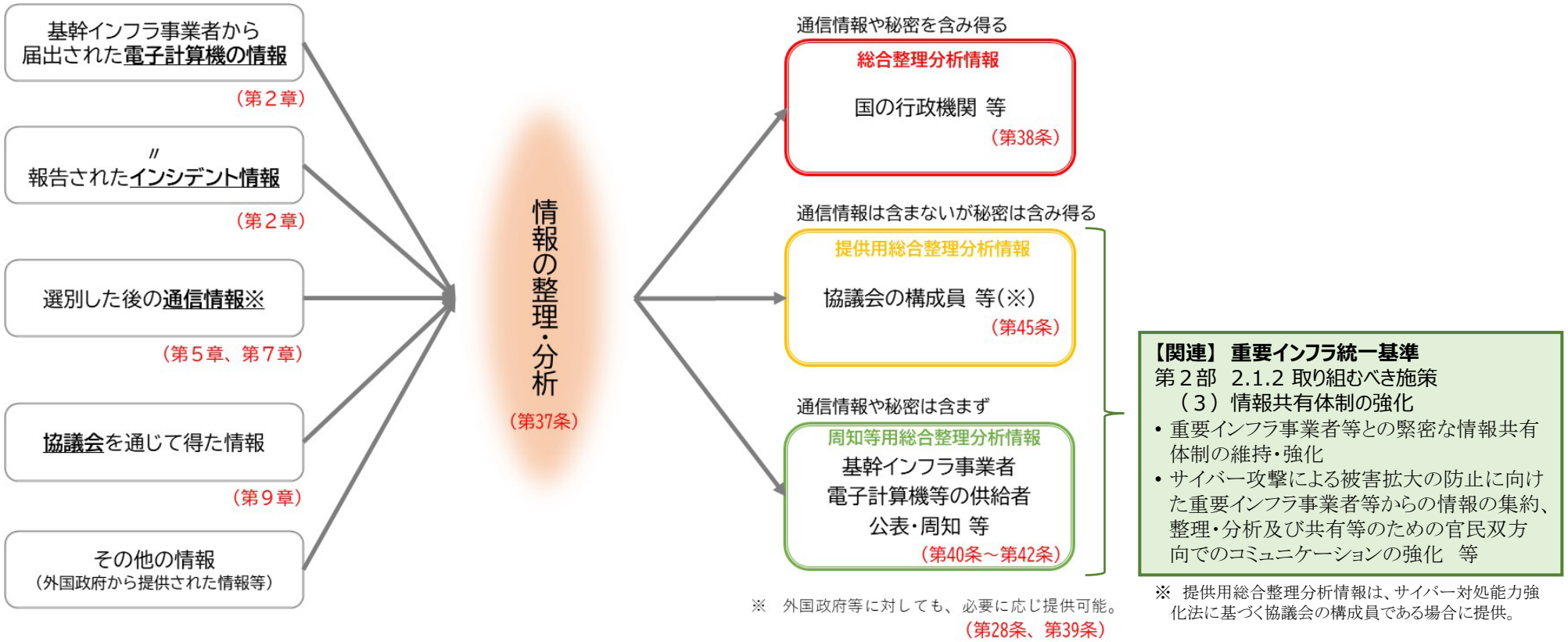
※　具体的な内容については、第３部の詳細を記載する「重要インフラのサイバーセキュリティに係る安全基準等策定ガイドライン」において今後検討していく。

# （参考）取り組むべき主な対策⑤



**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。
- 政府は、サイバー対処能力強化法に基づく分析情報・脆弱性情報の提供等も通じて、重要インフラのサイバーセキュリティを確保。




**【関連】 重要インフラ統一基準**
第２部 2.1.2 取り組むべき施策
（３）情報共有体制の強化
- 重要インフラ事業者等との緊密な情報共有体制の維持・強化
- サイバー攻撃による被害拡大の防止に向けた重要インフラ事業者等からの情報の集約、整理・分析及び共有等のための官民双方向でのコミュニケーションの強化 等

※ 提供用総合整理分析情報は、サイバー対処能力強化法に基づく協議会の構成員である場合に提供。

**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）
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。

# 重要インフラ統一基準群



## 統一基準群

### 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

第２部　政府機関における施策の基準

第３部　安全基準等において規定されるべき事項

第３部を解説

### 安全基準等策定ガイドライン
（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）

1　基本的な考え方
2　組織統治
3　識別
4　防御
5　検知
6　対応及び復旧
7　技術・脅威の動向等を踏まえた対策

反 映

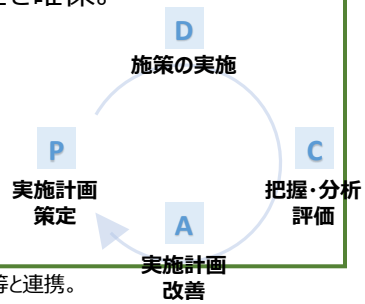
### 各分野における安全基準等

情報通信、金融、航空、空港、鉄道、電力、ガス、行政サービス、医療、水道、物流、化学、クレジット、石油、港湾、郵便（16分野）

### 政府機関の施策のPDCAサイクル

政府機関の施策のPDCAサイクル（実施計画の策定等）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。

＜政府機関において取り組むべき施策＞
- 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




※業界団体等が安全基準等の策定主体である場合は業界団体等と連携。

### 各分野における安全基準等の整備及び浸透

重要インフラ所管省庁や各分野の業界団体等（以下「所管省庁等」）が策定する安全基準等を通じて、重要インフラ事業者等が分野・事業者横断的に講ずべきサイバーセキュリティ対策の実施を促進。

＜安全基準等策定ガイドライン＞
- 本ガイドラインは、統一基準第３部について解説。所管省庁等が安全基準等を策定するに当たって参照。
- 統一基準第３部に定める対策事項ごとに、より具体的な対策事項を記載。
  - 講ずべき対策事項：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事項
  - 講ずることが望ましい対策事項：分野・事業者によっては直ちに実施することが困難である場合が想定されるが、可能な範囲で講ずることが望ましい対策事項
- 統一基準第３部に定める各対策をどのような形で安全基準等に盛り込むかについては、関係法令の規定及び安全基準等の構成等を踏まえ、重要インフラ分野ごとに検討されることを想定。

# 安全基準等策定ガイドライン案の検討



（非公開）

# 安全基準等策定ガイドライン案の検討



（非公開）

# 安全基準等策定ガイドライン案の検討



（非公開）