資料４

# 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への対応について

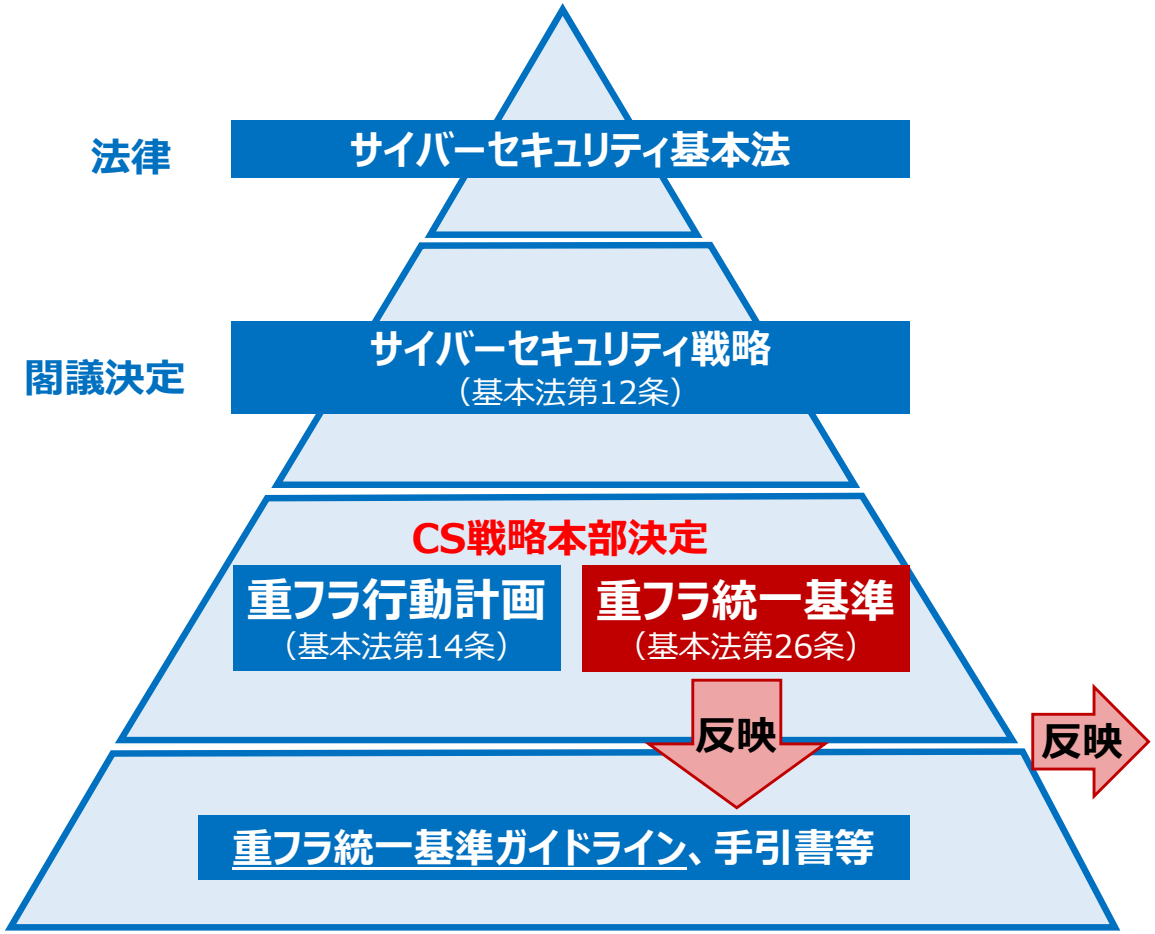
総務省

令和８年６月８日
自治行政局 住民制度課
サイバーセキュリティ対策室

# 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への対応について①

## 論点②

○　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　（以下、「重フラ統一基準」）を踏まえ、重要インフラ所管省庁において、**①各分野で実施する施策に関する計画を作成**するとともに、**②統一基準の内容をガイドライン等に反映**して重要インフラ事業者等に対して示す必要がある。




内閣官房国家サイバー統括室（NCO）作成資料を一部編集

## 関係性

従来は、サイバーセキュリティ基本法第14条に基づき作成されていた**重要インフラ行動計画**において、**重要インフラ事業者等※1における自主的な取組の推進**について示されていた。

新たに、サイバーセキュリティ基本法第26条に基づき、**重フラ統一基準**を策定することで、**重要インフラ分野全体の水準の底上げ**を図る（重フラ統一基準と重要インフラ行動計画は相補的な関係）。

※1 重要インフラのサイバーセキュリティに係る行動計画
(2) 重要インフラ事業者等
行動計画における重要インフラ事業者等は、サイバーセキュリティ基本法第12条第2項第3号に規定する重要社会基盤事業者等であり、具体的には、重要インフラ事業者及びその組織する団体並びに**地方公共団体から構成される。**
重要インフラ事業者は、サイバーセキュリティ基本法第3条第1項に規定する重要社会基盤事業者であり、同法第6条の規定に基づき、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責務を有する。**
**地方公共団体は、サイバーセキュリティ基本法第5条の規定に基づき、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する。**

## 今後の対応

重フラ統一基準や重フラ統一基準ガイドラインの内容を、**「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」に反映**（R8.10月以降）

# 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への対応について②

**論点②**

○ ガイドラインのベースであるISO/IEC27001の考え方は踏襲しつつ、**「組織統治」、「識別」、「防御」、「検知」、「対応及び復旧」の各プロセスの重要性を追加する形**でガイドラインの改定を検討するのはどうか。

## 総務省ガイドライン（現行）

ISO/IEC27001ベース

| 対策基準番号 | 項目 |
|---|---|
| 対策基準１. | 組織体制 |
| 対策基準２. | 情報資産の分類と管理 |
| 対策基準３. | 情報システム全体の強靭性の向上 |
| 対策基準４. | 物理的セキュリティ |
| 対策基準５. | 人的セキュリティ |
| 対策基準６. | 技術的セキュリティ |
| 対策基準７. | 運用 |
| 対策基準８. | 業務委託と外部サービス（クラウドサービス）の利用 |
| 対策基準９. | 評価・見直し |

- **防御中心**に責任者・管理者・担当者等における権限・責任等に関して記載
- CISOにおける**CSIRTの整備やCSIRTの役割**（報告・連絡）に関する記載は、平成30年9月改定において追記

## 総務省ガイドライン（改定イメージ）

ISO/IEC27001ベース＋NIST CSF2.0※

＋

「組織統治」、「識別」、「防御」、「検知」、「対応及び復旧」各プロセスの重要性を追加

＜方向性＞

- **基本方針**に各プロセスを整備することの重要性を示しつつ、**対策基準の項目は変更せず**、境界防御に依拠した対策を中心に記載している「対策基準３『情報システム全体の強靭性の向上』」の箇所を中心に追加・修正等を検討

＜主な検討内容＞

- 組織におけるガバナンスの重要性や**自治体においてガバナンスをどう確立していくか**等を検討
- 境界防御に依拠した対策において万が一境界が突破された場合におけるリスク等を明示した上で、**重要な情報資産におけるサイバー攻撃等に対する耐性とレジリエンスを高めるための考え方**と**責任者・管理者・担当者等における役割**を検討
- 特に、**構成管理・脆弱性管理**、**常時監視によるインシデント予兆等の検知**、**緊急時対応計画や業務継続計画等と連動した対応**等について追記を検討

※重要インフラ統一基準の考え方のベースとなっているThe NIST Cybersecurity Framework (CSF) 2.0