資料３

重要インフラ統一基準に基づく施策の実施に向けて

令和８年７月６日
内閣官房国家サイバー統括室

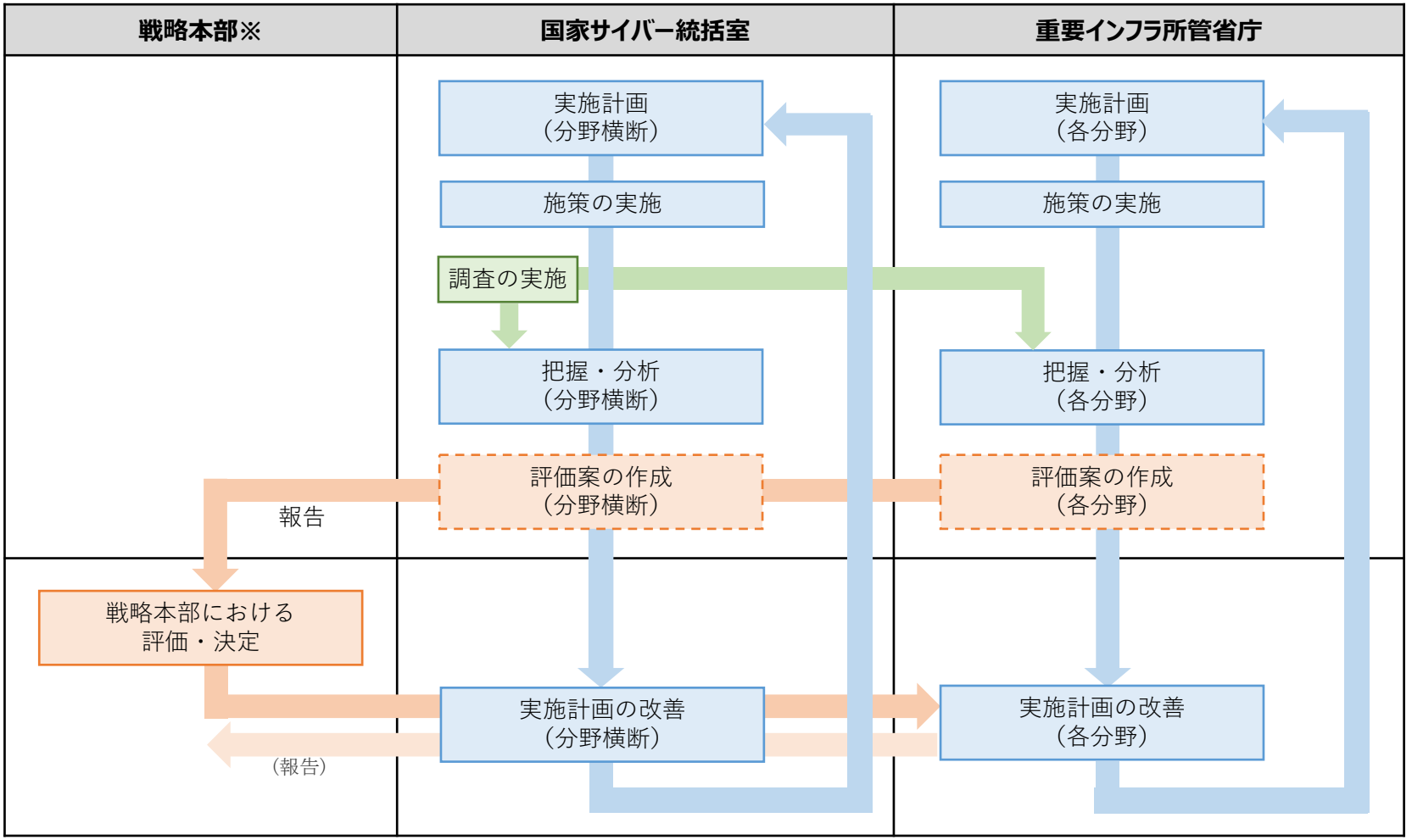
重要インフラ統一基準に基づく施策の実施に向けて

１．PDCAサイクルにおける実施計画等の妥当性確保

２．重要インフラ統一基準に基づく調査

重要インフラ統一基準におけるPDCAサイクル

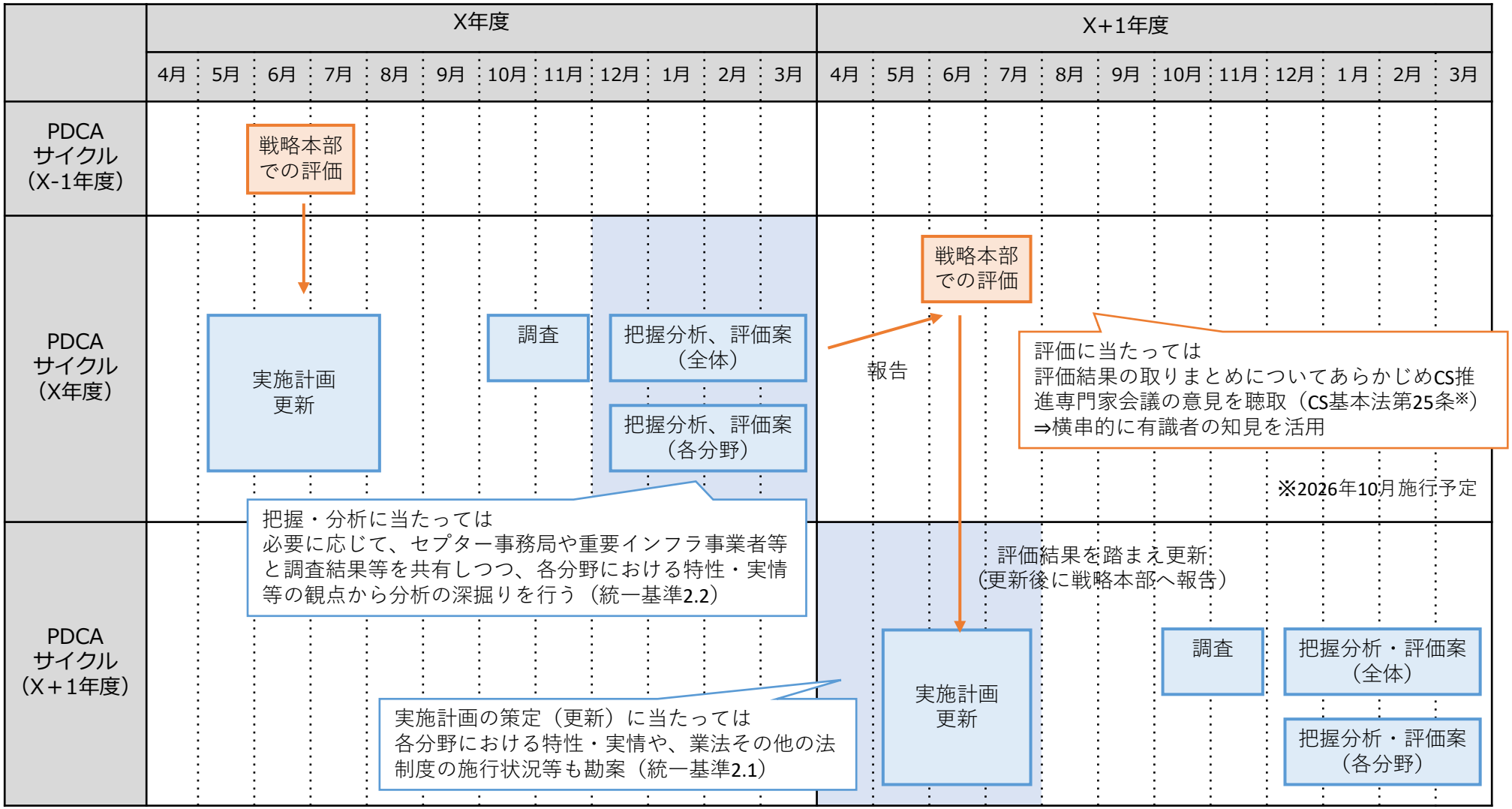
- 本スキームを通じて重要インフラ事業者等の基本的な対策の徹底を図るため、実効性の確保が重要。
- 例えば、各分野や分野横断的な「実施計画」の策定・更新、「評価案」の作成に当たって、内容の妥当性を確保するため、有識者会議などを活用することも考えられる。



※サイバーセキュリティ基本法の規定に基づき、重要インフラ統一基準に基づく施策の評価結果の取りまとめに当たっては、サイバーセキュリティ推進専門家会議の意見を聴くこととされている。

PDCAサイクルにおける実施計画等の妥当性確保に向けた検討

- PDCAサイクルを踏まえると、各年度秋頃に実施の調査の後、冬頃～春頃の把握分析、評価案の作成から実施計画の更新にかけて、有識者会議を活用することが考えられる。



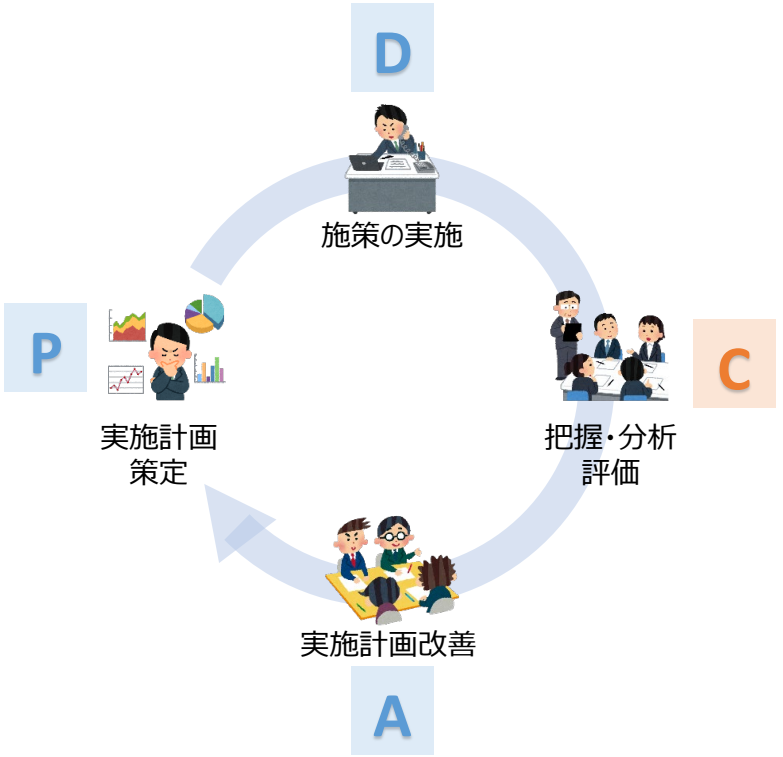
１．PDCAサイクルにおける実施計画等の妥当性確保

２．重要インフラ統一基準に基づく調査

重要インフラ統一基準に基づく調査

- 国家サイバー統括室は、年に１回を目途に、各分野における重要インフラ事業者等による取組の実施状況等を把握するため、重要インフラ所管省庁と連携し、次の調査を行う。（統一基準2.2）
  - 全ての分野・事業者を対象とした質問調査
  - 一部の分野・事業者を対象とした実地調査
  - その他調査（国内外における関連制度との比較等）

政府機関における施策のPDCAサイクル



重要インフラ統一基準に基づく調査

(1) 全ての分野・事業者を対象とした質問調査（成熟度モデル）

- 全分野・事業者を対象とした質問調査の実施により、重要インフラ統一基準（第３部）に定める対策事項に係る重要インフラ事業者等の取組状況を把握・分析し、政府機関における施策の改善に資する情報を提供。
- 本調査では、重要インフラ事業者等が自身の回答を通じて自己評価を行い、自組織のセキュリティ対策の実施状況を客観的に把握、求められるセキュリティ要件との差異を分析、改善すべき対策の優先順位を明確化し、継続的なセキュリティ水準の向上を図ることが期待される（成熟度モデル）。

(2) 一部の分野・事業者を対象とした実地調査

- 一部分野（６分野程度）の事業者を対象として、それら分野におけるサイバーセキュリティ対策上の課題を深掘り抽出し、重要インフラ統一基準の見直しや、政府機関における施策の改善に資する情報を提供。

(3) その他調査（国内外における関連制度との比較等）

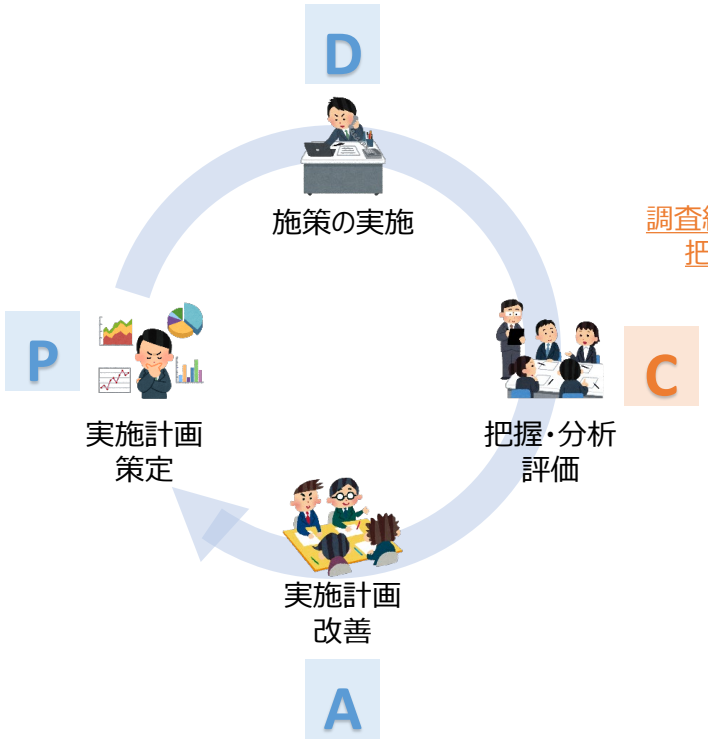
- 重要インフラ統一基準と国内外における関連制度とで、対策事項の構成や対策水準等の比較を行い、妥当性を分析、重要インフラ統一基準の見直しに資する情報を提供。

成熟度モデル「CI-CSA」（重要インフラ・サイバーセキュリティ・自己評価）

- 政府機関は、重要インフラ統一基準に基づき、重要インフラ事業者等を対象とした質問調査等を実施。その結果を踏まえ、把握・分析を行い、各分野の施策を推進するための実施計画を策定・改善。
- 同質問調査における成熟度モデル「CI－CSA」※は、重要インフラ事業者等が自身の回答を通じて自己評価を行い、自組織のセキュリティ対策の実施状況を客観的に把握、求められるセキュリティ要件との差異を分析、改善すべき対策の優先順位を明確化し、継続的なセキュリティ水準の向上のために活用されることが期待される。

※CI-CSA：Critical Infrastructure Cybersecurity Self-Assessment（重要インフラ・サイバーセキュリティ・自己評価）

政府機関における施策のPDCAサイクル

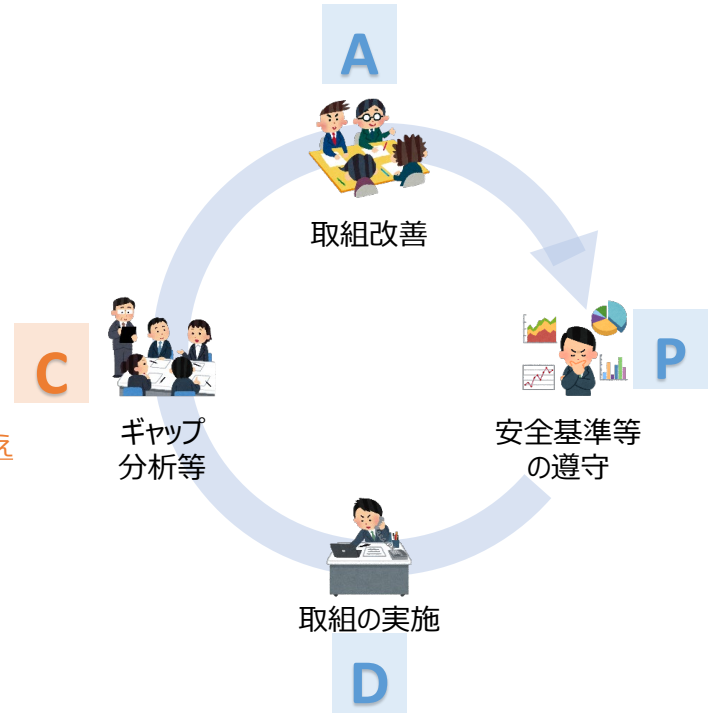


調査結果を踏まえ
把握・分析

CI-CSA
（成熟度モデル）

自己評価結果を踏まえ
ギャップ分析

重要インフラ事業者等における取組のPDCAサイクル



CI-CSAの概要

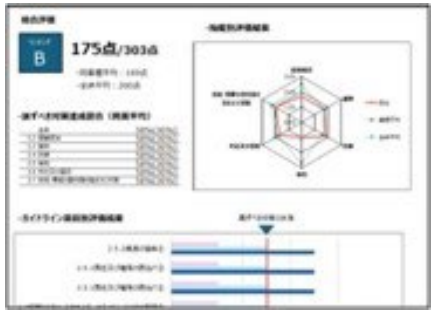
- CI-CSAでは、重要インフラ統一基準（第３部）に定める対策事項を基に設問及び回答を設定。
- これにより、重要インフラ統一基準に基づく対策事項の取組状況を可視化するとともに、重要インフラ事業者等に対して、継続的なセキュリティ水準の向上に資する分析データや助言等のフィードバックを提供。

重要インフラ統一基準

第3部　安全基準等において規定されるべき事項

- 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

<重要インフラ事業者等へのフィードバック イメージ>



重要インフラ統一基準の対策事項に対応した設問

設問内容	回答1（レベル１）	回答2（レベル２）	・・・	・・・	・・・
（例）事業継続計画等 事業継続計画等にサイバーセキュリティを組み入れているか。	実施していない。	事業継続計画等を策定している。	・・・	・・・	・・・
・・・					
・・・					

CI-CSAの構成イメージ

- 設問は、重要インフラ統一基準第３部で定める対策事項を基に設定（60問程度）。
- 回答は、安全基準等策定ガイドラインで定める対策事項を基に論理的・段階的に配置して設定。
- 設問に沿って対策をより多く実施することにより、理解が深まるとともに、成熟度が高まることが期待される。

＜構成イメージ＞

設問内容	回答1（レベル１） 【実施していない】	回答2（レベル２） 【一部の取組を実施】	回答3（レベル3） 【設問に沿って対策をより多く（深く）実施】	回答４（レベル４）	回答５（レベル５） 【網羅的に実施】
（例）事業継続計画等 事業継続計画等にサイバーセキュリティを組み入れているか。	実施していない。	事業継続計画等を策定している。	回答２の取組に加え、事業継続計画等にサイバーセキュリティを組み入れている。	回答３の取組に加え、サイバー攻撃等の予兆を認識した場合に、現在のセキュリティ対策で対処可能かを確認し、必要に応じて、対策の見直しや新たな対策の導入等を速やかに実施している。	回答４の取組に加え、インシデントへの対応を通じて得た知識を、将来のインシデントへの備えとして活用するための仕組みを確立している。
・・・					
・・・					

設問：重要インフラ統一基準第３部で定める対策事項を基に設定（60問程度）

（例）3.6.1　事業継続計画等
① サイバーインシデントが事業継続に及ぼす影響を踏まえ、事業継続に関する悪影響を許容範囲に抑制するための初動から完全復旧までの対応方針にサイバーセキュリティを組み入れる。

回答：安全基準等策定ガイドラインで定める対策事項を基に、論理的・段階的に配置

（例）6.1　事業継続計画等
6.1 ①-1　サイバーインシデントが事業継続に及ぼす影響を踏まえ、事業継続計画等にサイバーセキュリティを組み入れる。
6.3 ①-1　サイバー攻撃等の予兆を認識した場合、現在のセキュリティ対策で対処可能かを確認し、必要に応じて、対策の見直しや新たな対策の導入等を速やかに実施する。
6.2.1⑤-1　インシデントへの対応を通じて得た知識を、将来のインシデントへの備えとして活用するための仕組みを確立する。

（参考）日本成長戦略会議におけるKPIの検討

日本成長戦略会議／分野横断的課題「サイバーセキュリティ」におけるKPI：

「必要な防護策※1を実施できている重要インフラ事業者等※2の割合を2031年度末までに100%とする※3。」

※1　今夏策定される、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「重要インフラ統一基準」という。）に基づく、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の中でも、セキュリティ対策水準の底上げの観点から確実に実施すべきもの。具体的には、重要インフラ統一基準の詳細事項を記載した、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（今後策定）の内容を踏まえて、重要インフラ統一基準に基づく実施計画において確定（サイバーセキュリティ技術の進展に即しその後も適時に見直し。）。

※2　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として、重要インフラ統一基準に基づき重要インフラ所管省庁において特定する者。

※3　重要インフラ統一基準に基づく調査においてフォローアップを実施。初回の調査は、重要インフラ統一基準の施行後（2026年秋～冬頃）の実施を想定。

KPIの考え方と対象範囲

重要インフラ統一基準に基づく対策事項	基幹インフラ事業者	重要インフラ事業者等 ※今後、重要インフラ統一基準に基づく実施計画において事業者等を特定
講ずべき対策事項	確実に実施すべき	実施すべき （政府として優先度の高い部分） **KPIで想定する対象範囲**
講ずることが望ましい対策事項	事業者による自助努力を優先	今後の中長期的課題