重要インフラの情報セキュリティ対策に係る第４次行動計画の改定案の概要

1. 第４次行動計画における有効な取組は継続

2. サイバーセキュリティ基本法が公布・施行されたことを踏まえて対応

- ✓ 題名を「重要インフラのサイバーセキュリティに係る行動計画」へ
  - 「情報セキュリティ対策」から「サイバーセキュリティ」へ
- ✓ 行動計画はサイバーセキュリティ基本法に基づき策定することを明示
- ✓ 「サイバーセキュリティ」の定義を明確化
  - サイバーセキュリティ基本法第２条に規定する「サイバーセキュリティ」をいう
    電磁的方式による情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること
- ✓ 関係主体の責務を明確化
  - 「国」、「地方公共団体」、「重要インフラ事業者」、「サイバー関連事業者その他の事業者」

3. 障害対応体制の強化の在り方を抜本的に見直し

- ✓ 現在の「経営層への働きかけ」から、組織統治にサイバーセキュリティを組み入れる方針を具体的に記載

4. 将来の環境変化を先取り

- ✓ サプライチェーン等を含め包括的に対応

改定案における施策群と補強・改善の方向性等

改定案における施策群	第4次行動計画の施策群との対応	第4次行動計画からの主な補強・改善の方向性
1.障害対応体制の強化	「4.リスクマネジメント及び対処態勢の整備」の一部と「5.防護基盤の強化」の一部を統合した上で整理	○ 重要インフラ防護を適切に行うためには、経営層、CISO、戦略マネジメント層、システム担当等組織全体及びサプライチェーン等に関わる事業者の取組の必要性が高まってきていることを踏まえ、組織統治の一部としての障害対応体制の強化を推進 ○ サイバーセキュリティを取り巻く環境が大きく変化することを背景としたサプライチェーン・リスク等の新たな脅威への先取りした対応の推進 ○ 重要インフラ事業者等の自組織のリスクに応じた最適な防護対策の推進 ○ 政府と重要インフラ事業者等の相互連携を密にした官民一体としての対応を検討 ○ 事前対応のリスクマネジメントと障害発生時の危機管理の一体的な対応の推進
2.安全基準等の整備及び浸透	「1.安全基準等の整備及び浸透」を基本的に踏襲	○ 障害対応体制の強化及びリスクマネジメントに資する安全基準等を整備することを明確化 ○ 重要インフラ事業者等の取組の継続的な改善を図ることができる調査手法の検討
3.情報共有体制の強化	「2.情報共有体制の強化」を「3.障害対応体制の強化」の一部と統合した上で整理	○ 重要インフラ事業者等の自主的な取組の活性化を前提とした共助の推進 ○ ISAC連携等による分野間・官民連携の枠組みの整備の検討 ○ ナショナルサートの枠組みの強化の検討との整合性保持
4.リスクマネジメントの活用	「4.リスクマネジメント及び対処態勢の整備」の一部を整理	○ 組織の特性を踏まえた経営層による組織のリスクの明確化 ○ 自組織に適した防護対策の実現を支援するため、既存の手引書の見直しに加え、既存の基準類をどのように自組織に活用するかを含めた新たなガイダンスの整備の方向性の明示 ○ 2020年東京オリンピック・パラリンピック競技大会開催に向けて官民が連携して行ってきた取組の活用を検討
5.防護基盤の強化	「5.防護基盤の強化」の一部を「3.障害対応体制の強化」の一部と統合した上で整理	○ 障害対応体制の有効性検証としての分野横断的演習の推進 ○ 警察による重要インフラ事業者等との協力等の必要な取組の支援 ○ デジタル庁と連携した地方公共団体及び重要インフラに関連する準公共部門におけるサイバーセキュリティの確保に向けた支援等の実施

改定案の要点

1.「重要インフラ防護」の目的

重要インフラにおいて、任務保証の考え方を踏まえ、重要インフラサービスの継続的提供を不確かなものとする自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化等をリスクとして捉え、リスクを許容範囲内に抑制すること、及び重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ることの両面から、強靭性を確保し、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現すること。

2. 関係主体の責務

- 関係主体の責務は、サイバーセキュリティ基本法(平成26年法律第104号)を基本とする。
- 国は、サイバーセキュリティに関する総合的な施策を策定し、及び実施する。
- 地方公共団体は、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。
- 重要インフラ事業者は、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。

（重要インフラ事業者等を構成）

- サイバー関連事業者その他の事業者は、その事業活動に関し、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。

3. 基本的な考え方

- 重要インフラを取り巻く情勢は、システム利用の高度化、複雑化、サイバー空間の脅威の急速な高まりを受け、重要インフラ事業者等においては、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応を一層促進する。特に、経営の重要事項としてサイバーセキュリティを取り込む方向で推進する。
- 自組織の特性を明確化し、経営層からシステム担当者までの各階層の視点を有機的に組み合わせたリスクマネジメントを活用し、自組織に最も適した防護対策を実施する。
- 重要インフラを取り巻く脅威の変化に適確に対応するため、サプライチェーン等を含め、将来の環境変化を先取りした包括的な対応を実施する。

4. 障害対応体制の強化に向けた取組

- リスクマネジメントによる事前対応と危機管理の組合せにより、障害対応体制を強化する。
- 組織におけるサイバーセキュリティに対する経営者と専門組織の関係を経営の重要事項としてサイバーセキュリティを取り込む。
- サイバーセキュリティの確保には、サイバーセキュリティ基本法第2条の定義を踏まえ、外部からの攻撃のみならず、システム調達、設計及び運用に関係する事象を含め対応できるよう障害対応体制を整備・運用する。