資料６

# 「重要インフラの情報セキュリティ対策に係る第３次行動計画」の見直し骨子

資料６－１　第３次行動計画の見直しのポイント

資料６－２　行動計画見直しの骨子について

# 第3次行動計画の見直しのポイント

資料6－1

## 1．行動計画の目的

重要インフラサービスは、安全かつ持続的に提供（機能保証）することが求められることから、自然災害やサイバー攻撃等に起因するＩＴ障害とそれによるサービス障害の発生を可能な限り減らすとともに、発生時の迅速な復旧が可能となるよう、関係主体において経営層の積極的な関与の下、情報セキュリティに関する取組を推進する。また、取組を通じ、オリパラ大会に関係する重要なサービスの安全かつ持続的な提供も図っていく。

## 2．重要インフラを取り巻く現状と課題

◆ 行動計画に基づく施策群により、自主的な取組が浸透しつつあるが、ＰＤＣＡのうちＣＡに課題。一部で先導的な取組も進展。

◆ サービスの安全かつ持続的な提供のため、情報系(ＩＴ)だけではなく、制御系(ＯＴ)を含めた情報共有の質・量の改善等が必要。

◆ 国内外の多様な主体との連携、情報収集・分析に基づく国民への適切な発信の継続・改善が必要。

## 3．行動計画の見直しの３つの重点

次の3つを重点として行動計画に基づく5つの施策群の取組の深化を図る。

### ①　先導的取組の推進(クラス分け)

重要インフラ分野が依存し、短時間のＩＴ障害でも影響が大きくなるおそれがある分野(例：電力、通信、金融)において、一部事業者による先導的な取組を進めるとともに、他の事業者、さらには他の分野にも波及させることにより、重要インフラ全体の機能保証の確保を図る。

### ②　オリパラ大会を見据えた情報共有体制の強化

連絡形態の多様化、事案の深刻度のレベル分け、情報共有システムの整備、情報提供の拡大等により、情報共有を促進するとともに、重要インフラ内外の共有範囲の拡充、制御系を意識した情報共有等を図る。また、演習等の継続・改善等により、障害対応体制の強化を図る。

### ③　リスクマネジメントを踏まえた対処態勢整備の推進

重要インフラサービスの安全・継続的な提供のため、重要インフラ事業者等へのリスクマネジメントの更なる浸透や、CSIRTやコンティンジェンシープランの整備等を含む対処態勢の整備の推進図る。

行動計画に基づく５つの施策群

安全基準等の整備・浸透

情報共有体制の強化

障害対応体制の強化

リスクマネジメント

防護基盤の強化

## 4．行動計画の見直しに向けた今後のスケジュール

➢　平成28年中に行動計画の見直し（案）を策定・公表、平成29年3月までに結論を得る。

# ① 重要インフラ事業者の先導的取組の推進（相互依存性等を踏まえたクラス分け）

重要インフラ事業者の情報セキュリティ対策における先導的取組を推進するとともに、重要インフラ事業者以外の事業者についても情報セキュリティ対策レベルの向上を図る。

## 重要インフラ事業者

### 先導的取組を行う事業者

**電力分野**
- 一般送配電事業者　等

**情報通信分野**
- 主要電気通信事業者　等

**金融分野**
- 主要都市銀行　等

✓ 他の重要インフラ事業者からの依存が大きい
✓ 比較的短時間のIT障害であってもその影響が大きい

### その他の事業者

**電力分野**
- 左記以外の電気事業者

**情報通信分野**
- 左記以外の情報通信事業者

**金融分野**
- 左記以外の金融機関

- 他の重要インフラ分野の事業者

依存関係

## 重要インフラ事業者以外

- 重要インフラ事業者の主要関係先や外部委託先
- 先端技術等の知的財産や営業秘密を保持する企業、研究機関、大学等
- 安全保障上重要な企業

◆ 行動計画に基づく取組

安全基準等の整備・浸透

情報共有体制の強化

障害対応体制の強化

リスクマネジメント

防護基盤の強化

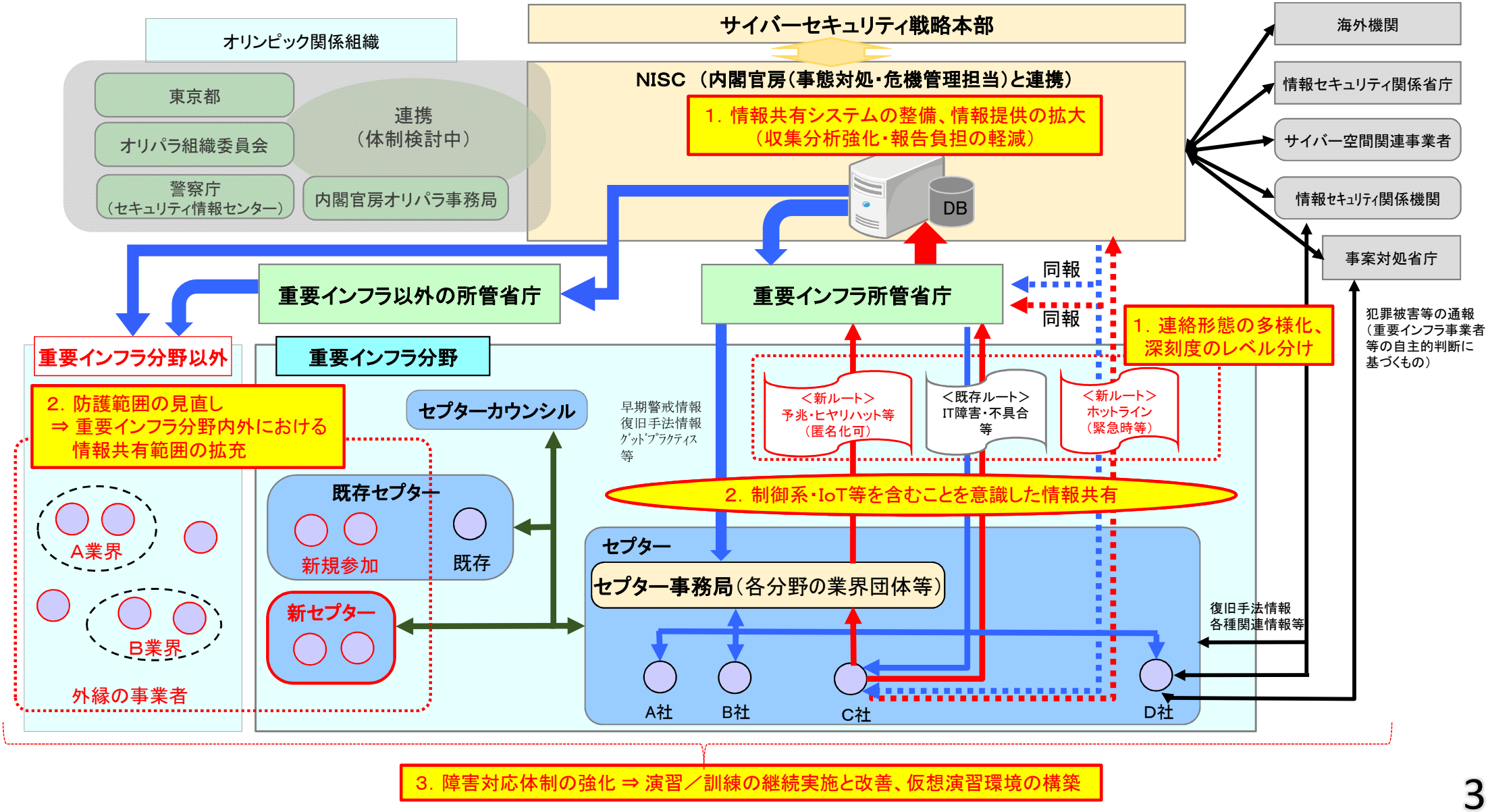
◆ 個々の事業者において情報セキュリティ対策を実施

## 今後の取組

- 先導的取組の実施(例)
  - ◆ISACの設立・加盟
  - ◆侵入テストの実施
  - ◆リスクマネジメントの重点化
  - ◆NISCとのホットライン構築
  - ◆浸透状況調査結果を踏まえた対策の深化
- 先導的取組を実施していくための体制づくり
- NISC又は所管省庁からの情報提供を開始
- NISC又は所管省庁への情報連絡、その他の情報セキュリティに係る取組について、組織内の体制が確実なものとなった後に開始

# ② オリパラ大会を見据えた情報共有体制の強化

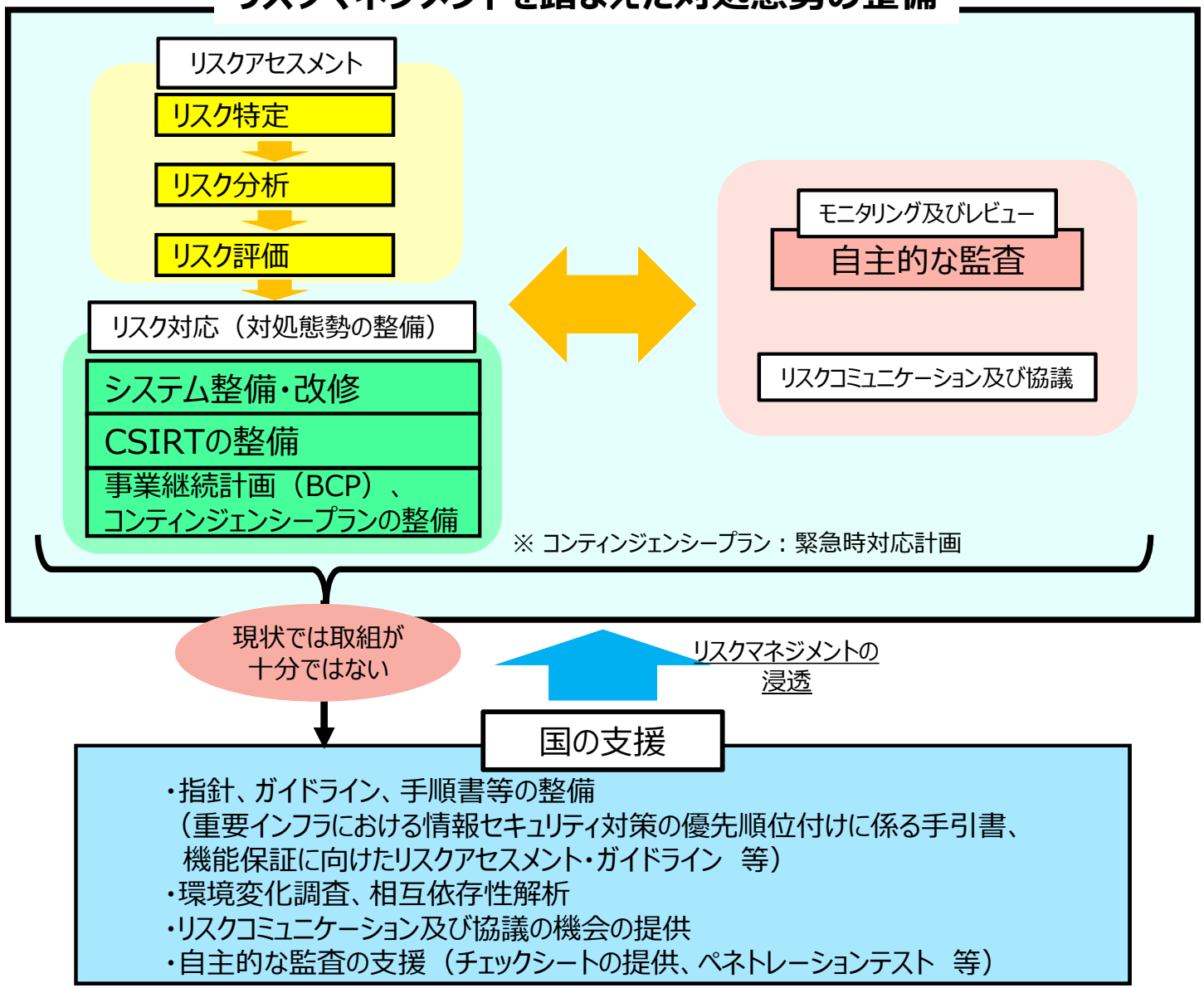
1．情報共有の更なる促進 ⇒ 連絡形態の多様化、事案の深刻度のレベル分け、情報共有システムの整備、情報提供の拡大
2．防護範囲の見直し ⇒ 重要インフラ分野内外における情報共有範囲の拡充、制御系・ＩｏＴ等を含むことを意識した情報共有
3．障害対応体制の強化 ⇒ 演習／訓練の継続実施と改善、仮想演習環境の構築



# ③ リスクマネジメントを踏まえた対処態勢整備の推進

重要インフラサービスを安全・持続的に提供できるよう、重要インフラ事業者等によるリスクマネジメントを踏まえた対処態勢整備を推進する。

## リスクマネジメントを踏まえた対処態勢の整備




重要インフラサービスの
安全・持続的な提供
（機能保証）

・まずは先導的事業者から
率先して取り組む
・オリパラ関係重要サービス
事業者も対応
⇒オリパラの円滑な実施

# ④ 第３次行動計画の施策群の主な見直し事項

## 第3次行動計画の目標（理想とする将来像）と評価

◆ 重要インフラ事業者等が自主的に見直しの必要性を判断し改善を図るサイクルが浸透しつつあるが、ＰＤＣＡのうちＣＡについてはいまだ十分とは言えない状況。
◆ 官民、民民間の情報共有が着実に進展。演習等により防護能力が向上。脅威の深刻化を踏まえ、情報共有の質・量の改善、ＩＴ障害対応経験等を将来に活かす取組が必要。
◆ 国民への取組内容の発信を実施。しかし、国民の不安感はぬぐい切れていない。引き続き、国内外の多様な主体との連携、情報収集・分析、国民への適切な発信の継続が必要。
◆ 2000年以降、行動計画として策定・公表、定期的な評価・見直しが行われている。これに基づく継続的取組により対策が着実に進展。同計画の基本的枠組みの維持が妥当。
◆ 重要インフラ防護の目的に照らし、機能保証の観点から取組を進めることが重要。また、一部で先導的な取組も進められており、これを適宜展開していく。

| 第３次行動計画の施策群 | 見直しの方向性（案） | 具体化に向け検討すべき事項 |
|---|---|---|
| ①安全基準等の整備及び浸透 | ○経営層に期待される認識・行動、内部統制の強化、ＯＴを視野に入れた人材育成等について追記し、指針を充実<br>○情報セキュリティへの取組を業法における保安規制に位置づける等、制度的な枠組みの検討・整備<br>○安全基準等の浸透状況調査を通じた重要インフラ事業者の情報セキュリティ対策レベルの底上げ | ○経営層に期待される認識・行動を受けた重要インフラ事業者による内規見直しの進め方<br>○現状の制度的枠組みの再確認、課題整理 |
| ②情報共有体制の強化 | ○情報共有の更なる促進<br>・連絡形態の多様化（セプター事務局経由の省庁報告ルート（匿名化））<br>・事案の深刻度のレベル分け<br>・迅速な共有プラットフォーム整備（ホットライン含む）<br>・制御系・ＩｏＴ等を含むことを意識した情報共有<br>・情報提供の拡大　等 | ○その他の情報共有の促進方策 |
| ③障害対応体制の強化 | ○重要インフラ事業者の実用性を重視した分野横断的演習及びセプター訓練の継続実施・改善 | ○重要インフラ事業者等が検証できるような仮想演習環境の構築 |
| ④リスクマネジメント | ○施策のスコープを拡大し、機能保証の観点から、リスクアセスメント結果を踏まえた対処態勢の整備支援に係る取組（オリパラも見据えた取組を含む。）を追加 | ○リスクアセスメント結果を適切に経営意思決定に反映させるための内部統制の強化（自主的な監査の強化等）に対する支援の在り方 |
| ⑤防護基盤の強化 | ○重要インフラ分野内外の情報共有等を行う範囲の見直し<br>○情報セキュリティ対策への経営層の関与の推進<br>○国際会議等で得た情報の関係主体への積極的な提供<br>○人材育成の支援（IT、OT両方に対応できるハイブリッド人材を含む。） | ○拡充を図る重要インフラ分野内外の情報共有先（外縁等） |

資料６－２

# 行動計画見直しの骨子について

平 成 ２ ８ 年 １ ０ 月 １ ２ 日
内閣サイバーセキュリティセンター

## １．基本的考え方

・第3次行動計画の実施状況の評価を踏まえ、行動計画の見直し骨子を作成する
・ロードマップに従い検討を進めた結果を行動計画の見直しに適宜反映させる
・機能保証の考え方に基づくものとする
・2020 東京オリパラ大会に係るサイバーセキュリティ確保のための施策と緊密に連携する

## ２．スケジュール

ロードマップにおいて、行動計画の見直しについて本年度末を目途に結論を得ることとしていることから、これに向け次のスケジュールで作業を進める。

・平成 28 年 9 月 30 日　第3次行動計画の実施状況の評価を踏まえ、行動計画見直し骨子案を作成し、専門調査会において了解
・平成 28 年 12 月　行動計画見直し案を作成し、専門調査会において了解
・平成 29 年 1 月～2 月　パブコメの実施
・平成 29 年 3 月末　行動計画見直しについて結論を得る（戦略本部決定）

# 行動計画見直し骨子

# Ⅰ．行動計画見直し骨子

【行動計画の目的】

重要インフラサービスは、安全かつ持続的に提供（機能保証）することが求められることから、自然災害やサイバー攻撃等に起因するＩＴ障害とそれによるサービス障害の発生を可能な限り減らすとともに、発生時の迅速な復旧が可能となるよう、関係主体において経営層の積極的な関与の下、情報セキュリティに関する取組を推進する。また、取組を通じ、オリパラ大会※に関係する重要なサービスの安全かつ持続的な提供も図っていく。

## 1.　行動計画見直しの重点

見直し後の行動計画においては、オリパラ大会[1]の開催を見据えた重要インフラ防護施策に重点的に取り組む。

また、経営層のあり方について、第３次行動計画を踏まえつつ、「サイバーセキュリティ経営ガイドライン」や「企業経営のためのサイバーセキュリティの考え方」等を反映させて記載し、経営層に訴求する。

加えて、安全で持続的にサービスを提供するという機能保証の考え方について、関係主体が認識を共有して取組を進める。

以上の認識及び第３次行動計画の実施状況の評価を踏まえ、行動計画に基づく5つの施策群の基本的骨格を維持し、制度的枠組みの改善の検討等を進めつつ、次の３つを重点として取組の深化を図る。

### 1.1　重要インフラ事業者等における先導的取組の推進（相互依存性等を踏まえた重要インフラ事業者等のクラス分け）

重要インフラ分野が依存し、比較的短時間の IT 障害であってもその影響が大きくなるおそれがある分野（例：電力、通信、金融）の一部事業者による先導的な取組を進めるとともに、他の事業者、さらには他の分野にも波及させることにより、重要インフラ全体の機能保証の確保を図る。

先導的な取組例として、経営層の指揮の下、機能保証のために必要な関係事業者等のリスクアセスメントやそれを踏まえた対応を含むリスクマネジメントの重点化・侵入テストの結果を踏まえた監査の主体的な実施、より高度で機微な情報の共有体制の構築や短時間で連絡が取れる仕組みの構築、ISAC の設立・加盟による情報共有の強化等があり、これ

[1] 2020 年東京オリンピック・パラリンピック競技大会

らを促進する。

### 1.2　オリパラ大会を見据えた情報共有体制の強化

オリパラ大会を始めとする国際的なビッグイベントにおけるサイバーセキュリティを確実なものとするため、24 時間 365 日、官民間、民民間及び関係省庁間における安全・迅速な情報共有や情報の収集・分析を可能とするシステムの整備、連絡形態の多様化、事案の深刻度のレベル分け、情報提供の拡大等により、情報共有を更に促進する。

また、重要インフラ分野内外における相互依存性を考慮した情報共有範囲の拡充、制御系・IoT等を含むことを意識した情報共有等を図る。

以上の情報共有体制について、分野横断的演習等の継続、改善等を通じ、その有効性を確認するなど、障害対応体制の強化を図るとともに、オリパラ大会終了後においても活用できるレガシーとして引き継ぐ。

### 1.3　リスクマネジメントを踏まえた対処態勢整備の推進

重要インフラ事業者等のほか、オリパラ大会に直接的又は間接的に関わる事業者における機能保証の考え方に立脚したリスクアセスメントの促進のための取組を行う。また、リスクアセスメント結果に基づき CSIRT やコンティンジェンシープランの整備等を含む対処態勢の整備を図る。

## 2.　各論

### 2.1　安全基準等の整備及び浸透

#### 2.1.1 指針の継続的改善

「サイバーセキュリティ経営ガイドライン」や「企業経営のためのサイバーセキュリティの考え方」等を踏まえ、経営層のリーダーシップに関する事項を重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針に盛り込む。

また、重要インフラ事業者等が自主的に行う内部統制の強化や、情報系（IT）のみならず、制御系（OT）も視野に入れたセキュリティ人材の育成や体制整備、情報共有の取組のひとつとして、重要インフラ事業者同士による過去のインシデント対応に係るケーススタディの実施について指針に盛り込む。

### 2.1.2 安全基準等の継続的改善

重要インフラ防護能力の維持・向上に資する取組として、情報セキュリティに関する取組を業法における保安規制に位置づけることを各分野において検討する。

また、安全基準等の体系を確認した上で、更にサイバーセキュリティを高めるための方策について、必要な制度的枠組みを含め検討を行い、継続的な改善を図る。

### 2.1.3 安全基準等の浸透

安全基準等の浸透状況等調査への回答を通じて、重要インフラ事業者等が自らの情報セキュリティへの取組の充足度や課題点、解決策等を認識可能となるように調査票の見直しを行う。

## 2.2 情報共有体制の強化

### 2.2.1 情報共有体制の充実・強化

第3次行動計画期間中に構築された情報共有体制が関係主体の間で定着していることを踏まえ、これを引き続き継承した上で、情報連絡元の秘匿化を可能とする新たな連絡形態（セプター事務局経由）の導入や、オリパラ大会などの国際的イベントを見据えた迅速かつ効果的な情報共有システムの整備（緊急時等におけるホットラインの構築を含む）などの情報共有体制の充実・強化に取り組む。

### 2.2.2 情報共有の更なる促進

事案の深刻度のレベル分けや、予兆脅威情報を含む共有すべき情報の明確化を行うとともに、情報系システムだけでなく制御系システムやIoTシステム等に関する情報共有の活性化を図る。

また、機能保証の考え方を踏まえ、重要インフラ分野内外における相互依存性を考慮した情報共有範囲を拡充し、サプライチェーン全体に情報セキュリティ関連情報の浸透を図るなど「面としての防護」の実現に向けて取り組む。

### 2.2.3 重要インフラ事業者等の活動の更なる活性化

セプターカウンシルをはじめ、民間事業者主体の自主的な体制が構築されていることを踏まえ、各セプターにおける取組・連携が一層活性化していくよう、セプター側からの要望

等に応じて国として必要な支援を継続する。

## 2.3 障害対応体制の強化

### 2.3.1 分野横断的演習の改善

これまで蓄積してきた運営手法や成果を踏まえ、最新の攻撃手法を考慮した演習シナリオの検討に取り組み、重要インフラ事業者等におけるインシデントハンドリングや組織内規程等の実態に即した演習となるよう改善を図りつつ、継続的に実施する。また、演習参加に対する旺盛なニーズに応えるべく、関係省庁・民間機関との連携や演習参加モデルの提示、仮想演習環境の構築等に取り組む。

### 2.3.2 セプター訓練の改善

より実態に即した訓練となるよう、重要インフラ全分野において日程を定めない訓練（抜き打ち訓練）の実施や分野特性に応じた模擬情報のカスタマイズ化、緊急時における情報連絡体制・手段等の検証に取り組む。

## 2.4 リスクマネジメント及び対処態勢の整備

### 2.4.1 リスクアセスメントの支援

「機能保証に向けたリスクアセスメント・ガイドライン」のオリパラ大会に係るリスクアセスメントでの活用等を通じて、重要インフラ事業者等における機能保証の考え方に立脚したリスクアセスメントの浸透を推進する。

重要インフラにおける環境変化調査及び相互依存性解析等を継続的に実施し、その調査・分析結果の活用を図る。

また、重要インフラ防護についてのリスクコミュニケーション及び協議の支援のために、セプターカウンシル及び分野横断的演習を利活用し、分野横断的な意見交換の機会の提供等を行う。

### 2.4.2 対処態勢整備の支援

重要インフラ事業者等において、リスクアセスメント結果を踏まえ、「サイバーセキュリティ経営ガイドライン」等を参考として、CSIRT の構築、事業継続計画・コンティンジェンシープラ

ンの整備、監査の実施等が主体的に行われるよう、政府機関において必要な支援を行う。

### 2.4.3 本施策と他施策による結果の相互反映プロセスの確立

本施策における調査・分析結果の他施策への活用及び他施策において顕在化した分野横断的な対策を要する新たなリスク源・リスクについての必要な調査・分析を継続して行う。

## 2.5 防護基盤の強化

### 2.5.1 重要インフラに係る防護範囲の見直し

国民の安全や知的財産の保護等、防護対象として情報共有等を推進すべき分野についての取組強化を行う。

また、新たな重要インフラとして位置付けるべきサービスを適切に防護するための重要インフラ分野の見直し等の継続的な取組を行う。

### 2.5.2 広報広聴活動の推進

国民に安心感を与え、関係主体による冷静な対応に資するため、行動計画の枠組みや取組について国民への積極的な発信を行う。

また、機能保証の考え方の浸透や、面的防護の実現に向けて、経営層や重要インフラ分野に関連する他の事業者等の理解・協力が得られるよう、広報広聴活動を継続・強化する。

### 2.5.3 国際連携の推進

二国間・地域間・多国間の枠組みを活用した国際連携を継続・強化し、我が国の取組を積極的に発信していくとともに、国際会議等で得られた事例、ベストプラクティス等について、共有可能な範囲を確認した上で、関係主体に積極的に提供するまた、重要インフラ事業者等においても、海外の情報の把握など、国際連携に取り組むことが期待される。

### 2.5.4 規格・標準及び参照すべき規程類の整備

リスクアセスメント・ガイドラインの作成等、オリパラ大会等に備えた規格・標準及び参照すべき規程類の整備について推進する。

### 2.5.5 人材育成等の推進

「サイバーセキュリティ人材育成総合強化方針」（平成 28 年3月　サイバーセキュリティ戦略本部決定）及び次期人材育成プログラム（新・情報セキュリティ人材育成プログラム（平成 26 年 5 月）を今年度中に改訂予定）に基づき、サイバーセキュリティに係る演習や教育等により、重要インフラ事業者等におけるサイバーセキュリティ人材の育成支援、官民人材交流、資格取得等を推進する。また、重要インフラ事業者等が自主的に行う内部統制の強化や、情報系（IT）に限らず、制御系（OT）を含め、様々な役割や能力を持った複数の人材が一体となり、連携して業務を遂行する体制の中で情報セキュリティ人材の育成に取り組む。

### 2.5.6 マイナンバーに関するセキュリティ確保

政府機関は、地方公共団体等、マイナンバーを利用する重要インフラ事業者等のセキュリティを確保するため、必要な支援の実施や対策の検討を行い、マイナンバーを利用する重要インフラ事業者等は、セキュリティを確保するために必要な取組を行う。

## Ⅱ　第３次行動計画に基づく施策の評価

### 1. 第３次行動計画期間の目標（理想とする将来像）と評価

第3次行動計画に掲げられた当該計画期間の目標（理想とする将来像）と、それに照らした第3次行動計画の施策群全体の総合的、分析的な評価は、以下のとおりである。

＜将来像＞

**〇各関係主体の自覚に基づく自主的な取組はそれぞれの行動規範として浸透しており、その行動様式が情報セキュリティ文化を形成するようになっている。**

第3次行動計画においては、基本的な考え方として「情報セキュリティ対策は、重要インフラ事業者等が自らの責任において実施するものである」ことを明示し、本将来像のコンセプトについて訴求した。

また、重要インフラ事業者等の自主的な取組を促すことを目的として、安全基準等の策定指針をいわゆるPDCAサイクルに沿う形に改定した。これを受けた形で、各重要インフラ分野におけるガイドライン等の見直し、そして重要インフラ事業者等の内規等の見直しが進められている。

このことから、重要インフラ事業者等が、自主的に見直しの必要性を判断し改善できるサイクルが行動規範として浸透しつつあると認められる。しかしながら、PDCAサイクルのうち″CA″の取組については、いまだ十分とは言えない状況である。

今後、上記の行動規範に基づく行動様式が各関係主体に根付き、PDCAサイクルに沿った取組が継続されることによって、各関係主体及び関係主体間における情報セキュリティ文化が形成されることが期待される。

＜将来像＞

**〇各関係主体間において、IT障害の予防的対策を強化するためのコミュニケーションが日常的に行われるとともに、IT障害が発生した場合にはその経験を確実に将来の対策に活かすための継続的な改善がなされている。**

官民の情報共有については、重要インフラ事業者等から所管省庁・内閣官房への情報連絡の件数が着実に増加しており、より積極的な情報共有が行われつつある。

また、民間における情報共有についてはセプターカウンシルの事務局を民間主体とし、セプター間の情報共有等の活動に関する主体性、積極性の向上が図られた。また、各セプターにおけるセプター構成員の拡大もあり、幅広い情報交換による情報セキュリティ知識の向上と情報セキュリティ担当者間の人的つながりの形成が進んでおり、関係主体間のコミュニケーションの環

境整備に着実な進展がみられた。加えて、いくつかの分野においては、ISACを組織するなど情報共有の活性化、サイバー攻撃対策の高度化も進んでいる。

障害対応体制については、分野横断的演習やセプター訓練を継続的に実施しており、演習参加者の大幅な増加やシナリオの高度化が見られるところであり、これらの取組が、重要インフラ事業者等のニーズに応え、防護能力の向上に寄与していると認められる。

一方、脅威がより深刻化する中、IT障害の予防的対策を強化するためには、その目的に照らしてコミュニケーション手法を分類、具体化し、質・量ともに改善し続ける必要がある。また、障害発生時の対応については、演習、訓練を通じてその向上が図られている一方、IT障害への対応経験等を分野を越えて将来の対策に生かす取組は十分とは言えない。重要インフラの面的防護を図るためには、障害対応事例等の分析、共有による継続的改善が重要であり、今後もその取組を継続していく必要がある。

＜将来像＞

**〇関係主体が連携して重要インフラ防護に取り組んでいることが広く国民に知られ、国民に安心感を与えるようになっている。また、多様な主体間でのコミュニケーションが充実し、IT障害の発生時に冷静に対処できるようになっている。**

関係主体間のコミュニケーションは、前述のとおり、着実に進展しており、また、関係主体以外の一般国民への取組内容の発信として、行動計画及びその取組結果を公表しているほか、分野横断的演習に関する動画の配信を行うなど、認知度を高めるための取組を行っている。

一方で、標的型メール攻撃による情報漏えい等の報道を目にする機会が増加し、国民の不安感が拭い切れていないことも事実である。

IT障害発生時の対応については、前述のとおり演習や訓練を通じてインシデント対応の確認を行うとともに改善のための取組を行っている。また、海外の関係機関等とも各種枠組みを通じ情報共有を行うなど連携を推進している。

国民に安心感を与え、IT障害発生時の冷静な対処を可能とするためには、国内外の多様な主体と連携し、新たなリスクやインシデントについて情報を収集・分析し、関係主体間で共有するとともに、機能保証の観点も踏まえ、積極的に国民に向けて発信するなど、取組の継続、強化が必要である。

＜将来像＞

**〇こうした取組が行動計画として公表され、定期的に評価されるとともに必要に応じて適切に見直されている。**

重要インフラの情報セキュリティ対策については、2000年以降、行動計画として策定・公表さ

れ、当該行動計画に基づく取組に関し毎年度評価が行われている。また、見直しの必要性を踏まえ、3年ないし5年の間隔で行動計画の見直しが行われてきている。

こうした取組により、我が国の重要インフラ防護は、特別行動計画から見て16年間、現行の形態となった行動計画で11年間の実績を有しており、5つの施策に基づく対策が着実に進展したものと評価できる。今後も同行動計画の基本的枠組みの下、取組を継続する必要があると認められる。

＜将来像＞

**〇これら各関係主体の取組が社会の持続的な発展を支えるものとして確実に定着している。**

以上のとおり、行動計画に基づく取組が着実に進展していると認められる。今後は、関係主体に定着している第3次行動計画の5つの施策の基本的骨格を維持しつつ、重要インフラ防護の目的に照らし、機能保証の観点も含め、各施策において取組を深化することが求められる。この際、一部事業者による先導的な取組をさらに推進するとともに、他の事業者等へも展開し、重要インフラ全体の防護を図ることが必要である。

## 2. 施策群ごとの評価

### 2.1安全基準等の整備及び浸透

#### 2.1.1 指針の継続的改善

「重要インフラ分野における情報セキュリティ確保に係る安全基準等策定指針」の本編及び対策編の改訂を行った。同指針では、第3次行動計画の記載内容に照らして、重要インフラ事業者等の PDCA サイクルに沿って情報セキュリティの対策項目を再整理するとともに、本行動計画の他施策から得た知見等を活かし、497 項目の対策項目を採録した。さらに、重要インフラ事業者等による情報セキュリティ対策の段階的な実現に資するべく、対応の優先順位付け、対応策決定の考え方等を例示した「重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書」を新たに策定した。

本行動計画においては、情報セキュリティ対策への取組における経営層の在り方の重要性を訴求しているが、企業経営からの観点を入れる等、経営層がより積極的に関与出来るよう指針の見直しの検討が必要である。

### 2.1.2 安全基準等の継続的改善

安全基準等の改善状況等の調査を行い、重要インフラ所管省庁及び重要インフラ事業者等が、本行動計画期間の指針改定やサイバー攻撃の動向、所管事業者の対策状況調査結果等を受けて、安全基準等の継続的な改善に取り組んでいることを把握した。

一方、社会動向の変化の下、新たな安全基準等の策定が進められていることを踏まえ、改めて安全基準等の体系を確認し、新たな安全基準等を含めた継続的な改善状況の把握を今後の課題とする。

### 2.1.3 安全基準等の浸透

重要インフラ事業者等における安全基準等の浸透状況を把握するため、情報セキュリティ対策の状況について調査を実施した。重要インフラ事業者の自主時な取組の状況としては、安全基準等に基づく自己検証への取組が7割強、定期的な自己検証への取組が5割弱、定期的な自己検証に基づく課題抽出・改善への取組が3割強の実施率であった。

アンケート方式の調査では、新たな調査項目の追加によって、より具体的な対策状況の確認や、対策状況の退化の検知が可能となった。また、調査項目を PDCA サイクルに沿って再整理することによって、重要インフラ事業者等がアンケート回答を通じ、対策状況のセルフチェックを行えるよう改善を行った。

さらに、2014 年度からの3年間で 11 セプター34 事業者に対して往訪調査を実施し、情報セキュリティに係る社内体制や規程類の整備、障害対応体制等について意見交換を行い、経営層への訴求の必要性や情報セキュリティ人材の不足等の課題及び良好事例の収集を行った。

今後は、本調査結果を重要インフラ事業者等が有効活用できるよう、調査項目の見直しも含め調査結果のフィードバック方法等を検討していく必要がある。

## 2.2 情報共有体制の強化

### 2.2.1 情報共有の更なる促進

官民間の情報共有においては、情報連絡手順の整備や情報連絡様式の改良等、円滑な情報共有のための環境整備に取り組んだ。また、各種会合の場を通じて小規模事象も含む情報共有の必要性の周知徹底を実施した。その結果、重要インフラ事業者等からの情報連絡件数は 3 年間で大幅に増え、積極的な情報共有が行われたと評価できる。

ただし、報告を行う分野に偏りもみられるため、引き続き情報共有の必要性を訴求するとともに情報提供しやすい環境の構築について検討していく必要がある。

### 2.2.2 重要インフラ事業者等の活動の更なる活性化

セプターの取組として、一部の分野については ISAC が設立または拡大され、自主的な分野内情報共有体制を確立した。またセプターカウンシルにおける組織体制の改良や運用方法の改善が行われ、自主的で円滑な情報共有体制の強化が図られた。

更に、IT 障害発生時に当該セプター内の情報集約を行い、IT 障害の拡大防止に努めたセプターがあったこと等、重要インフラ事業者の活動の更なる活性化が図られている。

ただし、セプターによっては情報共有の必要性について理解度が異なるため、情報共有の必要性を継続的に周知する必要がある。

## 2.3 障害対応体制の強化

### 2.3.1 分野横断的演習の改善

第3次行動計画行動計画の開始年度（2014 年度）から、東京会場のほかに地方会場を新設し、重要インフラ事業者等の演習への参加機会の拡大を図るとともに、自社環境に即したインシデントハンドリング実現のための各社毎のサブコントローラ選出、演習の周知を目的とする見学会の新設など、演習環境・内容の改善に取り組んだ。その結果、演習参加者は大幅増となり、事業者の自社内における課題点の抽出に寄与している。今後は、分野横断的演習の運営を通じて得られた知見等を活用するなど、さらなる改善を図る必要がある。

### 2.3.2 セプター訓練

第3次行動計画期間では、重要インフラ事業者等に情報が届いているかを確認（受信確認）する「往復」訓練や、訓練日時を予め通知しない抜き打ち方式、メール等通常の情報共有手段が利用できない場合を想定した共有手段の検証、各分野の特性に応じた模擬情報の具体化など、より実態に即した訓練を実施した。その結果、多くのセプターで情報共有の体制や手段等で改善すべき点の明確化が図られ、本訓練の有用性があらためて確認された。今後も、緊急時の体制検証に資するべく実践的な訓練に引き続き取り組んでいく必要がある。

## 2.4 リスクマネジメント

### 2.4.1 リスクマネジメントの標準的な考え方

オリパラ大会をテストケースと定め、関連事業者等が実施するリスクアセスメントの手法を手

順書（「機能保証に向けたリスクアセスメント・ガイドライン」）として整備した。また、当該手順書を用いて、関連事業者等によるリスクアセスメントのトライアルを実施した。

こうした取組により、重要インフラ事業者等が実施しているリスクマネジメントの更なる最適化及び情報セキュリティ対策の水準の向上に資することが期待されるが、第3次行動計画期間の最終年度の取組であることから、その効果測定については、引き続きフォローアップしていく必要がある。

なお、重要インフラ事業者等が自主的に行うリスクアセスメントを促進することが今後の課題であり、引き続きガイドラインに基づくリスクアセスメントの浸透を推進するとともに、その実施に当たっての必要な支援を実施することを検討する。また、リスクアセスメントを実効性のあるものにするために、重要インフラ事業者等がリスクアセスメントの結果を適切に意思決定に反映させることが課題であり、重要インフラ事業者等における内部統制の強化に資する取組を支援することも検討する。

### 2.4.2　リスクマネジメントの支援

#### 2.4.2.1 リスクアセスメント

第3次行動計画期間において新たに追加した3分野である化学分野、クレジット分野及び石油分野を対象に、相互依存性解析と密接に関連するITへの依存度に関する調査1件を行った。調査結果については、当該3分野に個別に提供するとともに、それ以外の重要インフラ事業者等に対しても2015年3月にその概要を公表・共有した。また、相互依存解析の関連調査として、重要インフラ事業者等の外部サービスへの依存性に関する調査1件を行い、その調査結果を公表した。

こうした取組の結果を踏まえ、内閣官房は、重要インフラの面的防護の重要性を認識し、「重要インフラの情報セキュリティ対策に係る第3次行動計画の見直しに向けたロードマップ」に反映し、今後の重要インフラ防護に係る施策の検討において勘案した。

技術環境や社会環境は日々変容していることから、継続的に自らの置かれた状況を再確認することが課題であり、環境変化調査及び相互依存性解析又はその関連調査の継続的な取組を検討する。また、それらの結果を踏まえ、必要があれば、行動方針や行動計画を適宜見直すことも検討する。

#### 2.4.2.2 リスクコミュニケーション及び協議

重要インフラ事業者等その他関係主体間のリスクコミュニケーション及び協議の機会の提供に取り組み、セプターカウンシルの活動を支援したほか、分野横断的演習についても各重要イ

ンフラ分野が検討に参加する検討会（4回）及び拡大作業部会（3回）をそれぞれ開催した。また、重要インフラ専門調査会についても8回開催し、重要インフラ防護施策に関する意見交換を行った。

こうした取組を通じ、新たに鉄道分野及び航空分野においてセプター事務局を民間に移行するとともに、セプターカウンシルにおいても内閣官房が担っていた事務局業務や機能を構成員に移行するなど、関係主体間のリスクコミュニケーション及び協議に係る環境の整備に着実な進展が見られた。

一方、各関係主体間が情報や意見の交換を実施する機会は提供されているが、その機会の活用（IT障害の予防的対策に結びつく日常的なコミュニケーションなど）については、質・量ともに改善の余地があるといえる。

このため、セプターカウンシルや分野横断的演習等の情報や意見の交換の機会の提供を継続するとともに、環境変化調査や相互依存性解析等の結果を利活用した情報提供を行うなど、より一層のコミュニケーションの活性化を検討する。

### 2.4.3　本施策と他施策による結果の相互反映プロセスの確立

前述のとおり、重要インフラ事業者等の外部サービスへの依存性に関する調査の結果を踏まえ、内閣官房は、「重要インフラの情報セキュリティ対策に係る第3次行動計画の見直しに向けたロードマップ」に反映し、今後の重要インフラ防護に係る施策の検討において勘案した。

こうした取組については、継続的かつ計画的に取り組むことが重要であるが、実行上、必ずしも計画的な対応となっていなかったことに鑑み、行動計画期間中の相互反映プロセスとして明示的に予定を立て、計画的に取り組むことを検討する。

## 2.5防護基盤の強化

### 2.5.1 広報広聴活動

NISC の Web サイト等において、分野横断的演習やセプターカウンシルの開催等、第3次行動計画に基づく取組や進捗状況について、国民への周知や重要インフラ事業者等への広範な協力・支援を得るための広報公聴活動を実施した。また、2014 年、2015 年ともに、重要インフラ事業者等に対して、NISC 重要インフラニュースレターを 22 回発行し、重要インフラ防護に関する講演を 23 回実施した。

このような取組により、行動計画の枠組みについて国民の関心を高めることができ、国民のサイバーセキュリティに関するインシデント対応への理解に資することができた。

今後も、国民に安心感を与えるとともに、関係主体による冷静な対応に資することを目的に、行動計画の枠組みについて国民の認識・理解を深めていき、本行動計画への協力者を関係主体以外へも拡大していくことや、情報セキュリティ対策に経営層を関与させていくことが課題であり、引き続き、広報公聴活動を行っていく。

### 2.5.2 国際連携

重要インフラ所管省庁及び情報セキュリティ関係機関と連携し、多国間会合（Meridian 会合、日・ASEAN 情報セキュリティ政策会議等）や二国間協議（米国、EU 等）等を通じて、重要インフラ防護等に関するベストプラクティスの共有等を行うなど、国際的な情報セキュリティ対策の水準向上のためのキャパシティビルディング（能力向上）と各国の重要インフラ防護担当者との緊密な関係性の構築に向けた取組を実施した。

このような取組により、国際連携を強化することができ、我が国だけではなく国際的な情報セキュリティ対策の水準の向上に資することができた。

ただし、情報セキュリティ対策の水準は各国間で差があることから、国際的な情報セキュリティ対策の水準向上のため、今後も引き続き、二国間・地域間・多国間の枠組みの積極的な活用を通じて、各国との情報交換や支援・啓発を行っていく必要がある。また、このような取組によって得られた情報を有効活用していくことが課題であり、関係主体への積極的な提供を検討していく。

### 2.5.3 規格・標準及び参照すべき規程類の整備

内閣官房及び重要インフラ所管省庁等を対象として、重要インフラ防護に関する規程集の作成・配布を実施した。具体的には、国際基準等を重要インフラ防護に適用する場合の手引書として、リスクマネジメントに関する手引書を作成することとし、国内外で策定される重要インフラ防護に活用できるリスクマネジメント関係規格について整理し、手引書の作成に活用した。また、重要インフラ分野でも今後の利用が拡大していくと想定される IoT システムについて、同システムが具備すべき一般要求事項としての情報セキュリティ要件の基本的要素を明確化した「安全な IoT システムのためのセキュリティに関する一般的枠組」を作成した。今後、国際標準化に向けた取組を進めていくほか、分野別における安全な IoT システムに向けたセキュリティの取組の検討を促していく。

このような取組により、関係主体による重要インフラの情報セキュリティ対策の有効性の確保に資することができた。

今後、関連規程が追加・更新され、アップデートする必要が生じると考えられるため、今後も必要に応じて、関連規程の追加・更新を行っていく必要がある。