資料3

サイバーセキュリティ対策の強化に向けた対応について

2016年10月27日
内閣官房内閣サイバーセキュリティセンター（NISC）

新たな「サイバーセキュリティ戦略」について（全体構成）

2015年9月4日閣議決定

1 サイバー空間に係る認識

- サイバー空間は、「**無限の価値を産むフロンティア**」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがネットワークに連接され、実空間とサイバー空間との融合が高度に深化した「**連接融合情報社会（連融情報社会）**」が到来
  同時に、サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

2 目的

- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「**経済社会の活力の向上及び持続的発展**」、「**国民が安全で安心して暮らせる社会の実現**」、「**国際社会の平和・安定及び我が国の安全保障**」に寄与する。

3 基本原則

① 情報の自由な流通の確保　② 法の支配　③ 開放性　④ 自律性　⑤ 多様な主体の連携

4 目的達成のための施策

①後手から**先手**へ　／　②受動から**主導**へ　／　③サイバー空間から**融合**空間へ

経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

- **安全なIoTシステムの創出**
  安全なIoT活用による新産業創出
- **セキュリティマインドを持った企業経営の推進**
  経営層の意識改革、組織内体制の整備
- **セキュリティに係るビジネス環境の整備**
  ファンドによるセキュリティ産業の振興

国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

- **国民・社会を守るための取組**
  事業者の取組促進、普及啓発、サイバー犯罪対策
- **重要インフラを守るための取組**
  防護対象の継続的見直し、情報共有の活性化
- **政府機関を守るための取組**
  攻撃を前提とした防御力強化、監査を通じた徹底

国際社会の平和・安定及び我が国の安全保障

～ サイバー空間における積極的平和主義 ～

- **我が国の安全の確保**
  警察・自衛隊等のサイバー対処能力強化
- **国際社会の平和・安定**
  国際的な「法の支配」確立、信頼醸成推進
- **世界各国との協力・連携**
  米国・ASEANを始めとする諸国との協力・連携

横断的施策

- **研究開発の推進**
  攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発
- **人材の育成・確保**
  ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

5 推進体制

- 官民及び関係省庁間の連携強化、東京オリンピック・パラリンピック競技大会等に向けた対応

社会で活躍できる人材の育成

人材育成施策について

- 「「日本再興戦略」改訂2015」（平成27年６月閣議決定）、「サイバーセキュリティ戦略」（平成27年９月閣議決定）等を踏まえ、本年3月にサイバーセキュリティ分野の人材育成の具体的な強化方針（サイバーセキュリティ人材育成総合強化方針）を策定。
  - 参考１「日本再興戦略」改訂2015 抜粋
    - ・人材育成に係る施策を総合的に推進するため、本年度中に「サイバーセキュリティ人材育成総合強化方針（仮称）」を策定する。
  - 参考２　サイバーセキュリティ戦略抜粋
    - ・人材育成に係る施策を総合的かつ強力に推進するための方針を策定する。
- 現在、将来の社会・経済やITの利活用の進化を見据えたサイバーセキュリティ人材育成の課題の整理をしつつ、普及啓発・人材育成専門調査会での審議を通じ、人材育成プログラムの策定に向けて検討中。（今年度中に策定予定）

人材育成の基本的考え方

○人材の需要と供給の好循環を形成

人材の需要面（雇用）

適切な認識の下で、雇用・キャリアパスを確保
－経営戦略上の「投資」
－サイバー攻撃への対処の必要性

- 経営層 ○「経営層」のリーダーシップ
- 橋渡し人材層 ○組織内の関係部局間の総合調整や実務者層をまとめリード
- 実務者層 ○情報部門にとどまらず、事業部門、法務部門、工場など**セキュリティの範囲の広がり**

人材の供給面

人材育成の循環システム
－確かな知識と実践力の下に、
様々な業務経験を経て、人材を育成

- 人材像の提示 ➢産業界で求められる人材像の明確化（平成28年度中）
- 教育の充実 ➢enPiT等の大学教育の充実（平成28年度から大学学部にも拡大）、等
- 演習環境の整備 ➢NICTにおける実践的なサイバー防御演習（CYDER）の拡充（法制度の整備を含む）、等
- 能力の可視化 ➢情報処理安全確保支援士制度（平成32年までに3万人超の有資格者の確保）等

enPiT：「成長分野を支える情報技術人材の育成拠点の形成」事業　Education Network for Practical Information Technologiesの略称（「エンピット」と読む）
NICT：国立研究開発法人情報通信研究機構　National Institute of Information and Communications Technologyの略称
CYDER：実践的なサイバー防御演習　CYber Defense Exercise with Recurrenceの略称

「各府省庁セキュリティ・IT人材確保・育成計画」の作成状況等について
～政府機関におけるセキュリティ・ＩＴ人材の育成～

総合強化方針

◎政府機関におけるセキュリティ・ＩＴ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※）
（平成28年3月　サイバーセキュリティ対策推進会議・各府省情報化統括責任者(CIO)連絡会議）

≪一部抜粋≫
１．各府省庁における司令塔機能の抜本的強化
　サイバーセキュリティ・情報化審議官等の主導の下、組織規模や所管するシステム等の実情を踏まえつつ、人材の着実な確保・育成を図るため、速やかに、**採用、人材育成、将来像等にわたる具体的な取組方策を定めた「セキュリティ・ＩＴ人材確保・育成計画（仮称）」を作成し、各府省庁のサイバーセキュリティ・情報化審議官等で構成する会議において共有の上、フォローアップを実施する。**

（※）サイバーセキュリティ人材育成総合強化方針の第2章として

作成状況

・8月31日までに、対象の全府省庁において作成。
・9月8日　「副CISO等連絡会議/副CIO連絡会議合同会議」において各省計画を共有。

各省計画の内容

①体制の整備
　各府省においては、統括部局のセキュリティ部門を中心に、必要な強化を図るため、一定数の増員要求がなされ、審議官などの機構要求も含め、本省全体で約100人の要求が行われている。

②人材の拡充
　それぞれの府省の業務面の必要性や人材の脆弱性を踏まえた拡充方針を示している。

③有為な人材の確保
　府省の規模やシステム数等に応じ、素養や関心も踏まえ、相応の人材を確保する。

④セキュリティ・IT人材育成支援プログラム
　総務省等の研修に橋渡し人材の規模に応じて相応の人数を参加させる。（29年度府省全体で約2000名が行政管理局が行う情報システム統一研修を受講予定。）
　半数を超える府省では、府省の実情を踏まえた独自の研修も実施する。
　NISC、総務省行政管理局、個人情報保護委員会事務局等へ一定数の人材を出向させる。

⑤人事ルート例（キャリアパスのイメージ）
　具体的な部署・ポスト、出向先、研修内容等を勤務年数に応じて明記したキャリアパスを提示している。

⑥一般職員の情報リテラシー向上
　全職員、新採職員等を対象とした各種の研修を実施する。

今後

・今年度末　「副CISO等連絡会議/副CIO連絡会議合同会議」において、各省計画のフォローアップ、見直し等。

「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」の見直しのポイント

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。

安全なIoTシステムの創出に向けた取組

【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】（2016年8月 NISC）

個別分野の標準のテンプレート（基本原則、共通の要求事項）

【前提となる考え方】　セキュリティ・バイ・デザイン
【明確化すべき要素】
◇定義・範囲　◇安全性・機密性・完全性・可用性
◇確実な動作に必須事項　◇法律等からの要求事項
◇迅速な復旧　◇責任分界点、データの扱い方

さまざまな分野がつながる中、共通言語でサイバーセキュリティ対策を進めていくために不可欠。（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）

代表的なアーキテクチャ・セキュリティの対策事例集
通信系　セキュリティベンダー系　クラウド事業者系　・・・

セキュリティに対する関心の重点が異なる様々な関係者

分野固有の要求事項
自動車分野　電力分野　農業分野　鉄道分野　医療分野　・・・

事業の考え方・内容、文化、用語が異なる中で、個別に発展を遂げてきた各分野

上記体系でサイバーセキュリティ対策を進めるために今後必要な取組例

【国際標準化に向けた取組】

米国等の主要国と連携し、ISOなどの国際標準への提案に向けた取組を検討。今後策定される各分野固有の国際基準等について、標準のテンプレートを踏まえたものにし、我が国の強みを国際標準に反映していく。

【日本国内の基準等への適用】

日本国内の様々な関係者が策定する基準やガイドラインについて、標準のテンプレートをベースとしたものとなるよう促し、展開を図ることで我が国のIoTシステムの国際競争力を高めていく。

参　考　資　料

第3次行動計画の見直しのポイント

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

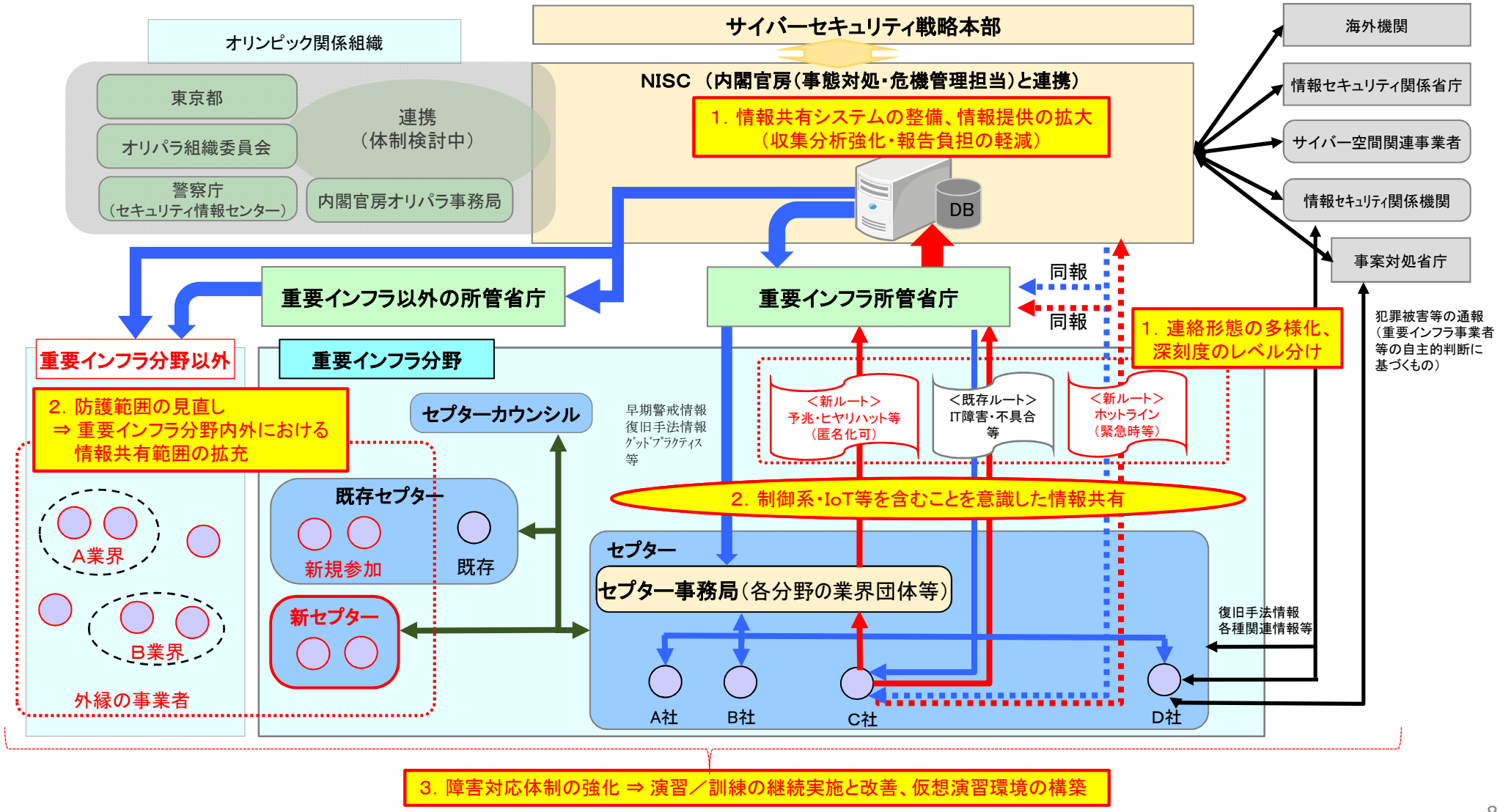
- 先導的取組の実施(例)
  - ◆ISACの設立・加盟
  - ◆侵入テストの実施
  - ◆リスクマネジメントの重点化
  - ◆NISCとのホットライン構築
  - ◆浸透状況調査結果を踏まえた対策の深化

- 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

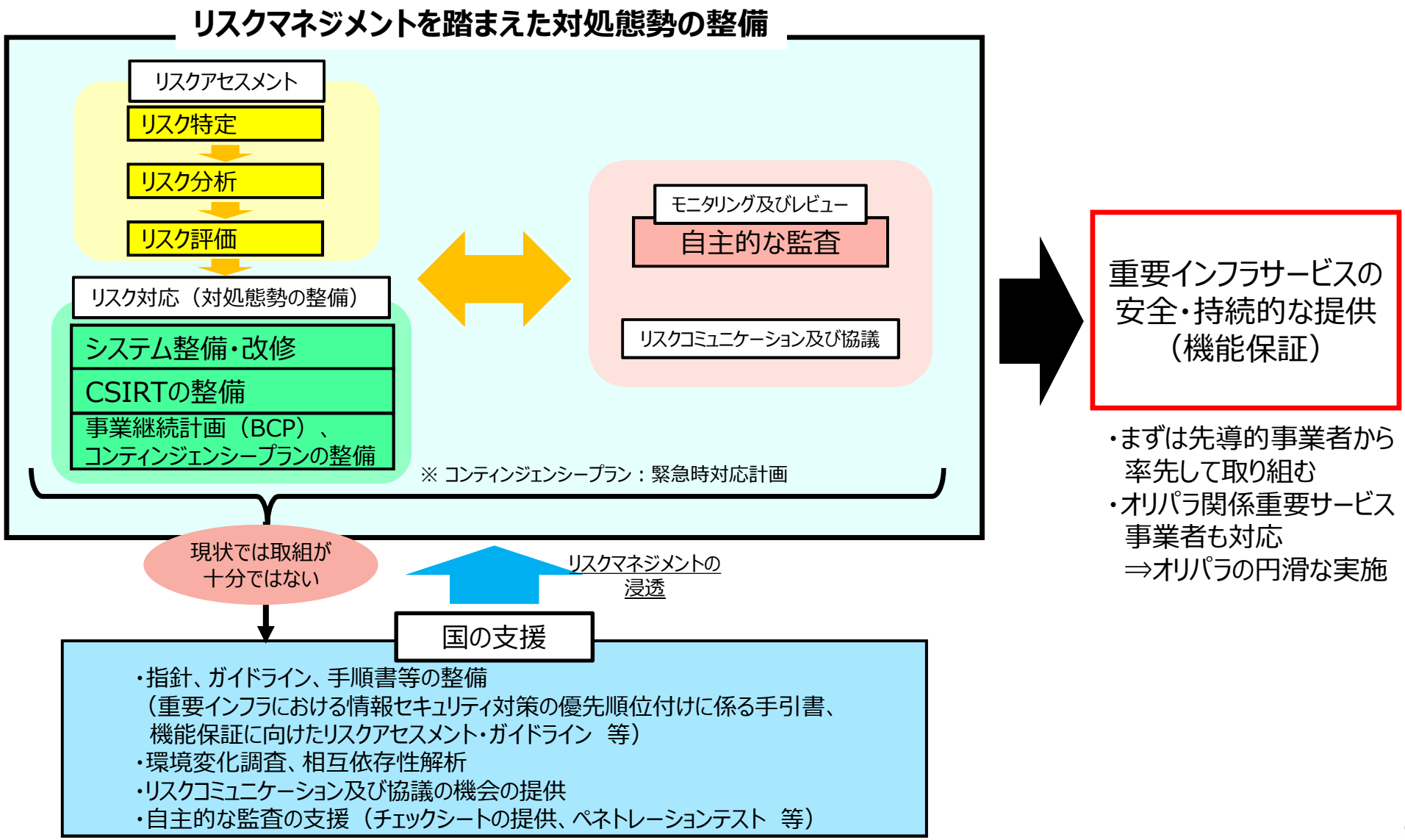
第3次行動計画の見直しのポイント
② オリパラ大会を見据えた情報共有体制の強化

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



第3次行動計画の見直しのポイント
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。



第3次行動計画の見直しのポイント
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 ○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 ○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 ○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 ・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）） ・事案の深刻度のレベル分け ・迅速な共有プラットフォーム整備（ホットライン含む） ・制御系・ＩｏＴ等を含むことを意識した情報共有 ・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 ○情報セキュリティ対策への経営層の関与の推進 ○国際会議等で得た情報の関係主体への積極的な提供 ○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）

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について（概要）

目的

- IoT(Internet of Things)システムは、従来の情報セキュリティの確保に加え、新たに**安全確保が重要**
- **セキュリティ・バイ・デザイン**の思想で設計・構築・運用されることが不可欠
- 安全なIoTシステムが具備すべき**一般要求事項としてのセキュリティ要件の基本的要素**を明らかにしたもの

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み（個別分野の標準の**"テンプレート"**）

個別分野固有の要求事項

自動車分野 | **電力分野** | **農業分野** | **鉄道分野** | **医療分野** | **・・・**

検討の視点

- 一つのIoTシステムリスクが他のIoTシステムに波及する可能性→**System of Systems**としての捉え方
- **機密性、完全性、可用性に加え、安全性**の要件確保

基本原則

- 関係者間の相互理解及び相互信頼の下、ネットワーク側とモノ側が、一体となり**システム全体としてセキュリティ確保**を図ることが必要。
- **セキュリティ・バイ・デザイン**を基本原則とし、**システム稼働前に確認・検証できる仕組**が必要。
- その際、基本方針の設定、リスク評価、システム設計、システム構築、運用・保守の**各段階の要件定義**が必要であり、以下の項目の明確化が必要。
  - ✓ 定義・範囲
  - ✓ 安全性・機密性・完全性・可用性
  - ✓ 確実な動作に必須事項、障害発生時の回復に必要な要件
  - ✓ 法律等からの要求事項
  - ✓ サイバー攻撃時の機能確保と迅速な復旧
  - ✓ 責任分界点、データの扱い方

取組方針

- **法令等の要求事項の明確化**
- IoTシステムの構成を**適切にモデル化**し、モデルを参照しながらセキュリティ要件を議論
- リスクアセスメントを活用した**セキュリティ対策や実装方法等の明確化**。ただし、リスクに応じた**柔軟な対応が必要**。
- 普遍的な**性能要求**とその時点での有効な手段の具体的方法を示す**仕様要求**の適切な適用
- 技術革新を前提とした**段階的・継続的アプローチ**
- IoTシステムに関連する者の**役割分担**（連携・協調によるセキュリティ確保の在り方や責任分界点の明確化を含む）
- データの利活用と個人情報保護の仕組み、機器認証の在り方などの**運用ルールの明確化**

米国商務省 国家通信情報管理局「IoT の利益・課題・政府の役割について」パブリックコメントに対し、提出されたコメント例

（実施期間：2016 年4 月6 日～6 月2 日）

Consumer Technology Association (全米民生技術協会)

現在、IoT に関する最大の課題は、連邦政府がバラバラに推進していることである。連邦政府が別々に対策を進めることは、IoT の発展に大きなダメージを与える。例えば、FDA の規則であるHIPPA は、医療健康器具ベンダが提供するウェアラブル端末に適用されるが、それらの器具は小売店で販売されることからFTC の規則で異なった要求をされることもある。消費者向けIoT はケースバイケースの法制度を適用される。従って、特定のIoT 機器またはアプリケーションに適用される具体的な法律、規則及び規制はいつも明らかなわけではないかもしれず、重複するか、矛盾しさえするかもしれない。

連邦政府は、IoT が広まっていく際に唯一国全体を把握できる立場であることを認識し、透明性を持って情報を共有し、産業界がIoT 全体の広がりを理解できるようにすることがIoT の発展に寄与できる。

Booz-Allen-Hamilton

連邦政府がIoT へ取り組むには、まずIoT の定義を考慮すべきである。適切なIoT の定義は、エコシステム全体を考慮したものになるべきである。わが社としては、IoT はデジタル世界と物理世界を融合するデバイス、センサその他の機器が相互接続されたエコシステムと定義する。
IoT では新たなセキュリティモデルを作らなければならない。連邦政府が行う標準化は重要である。

国際社会の平和・安定及び我が国の安全保障に係るサイバーセキュリティ戦略

■ サイバーセキュリティ戦略（2015年9月4日 閣議決定）

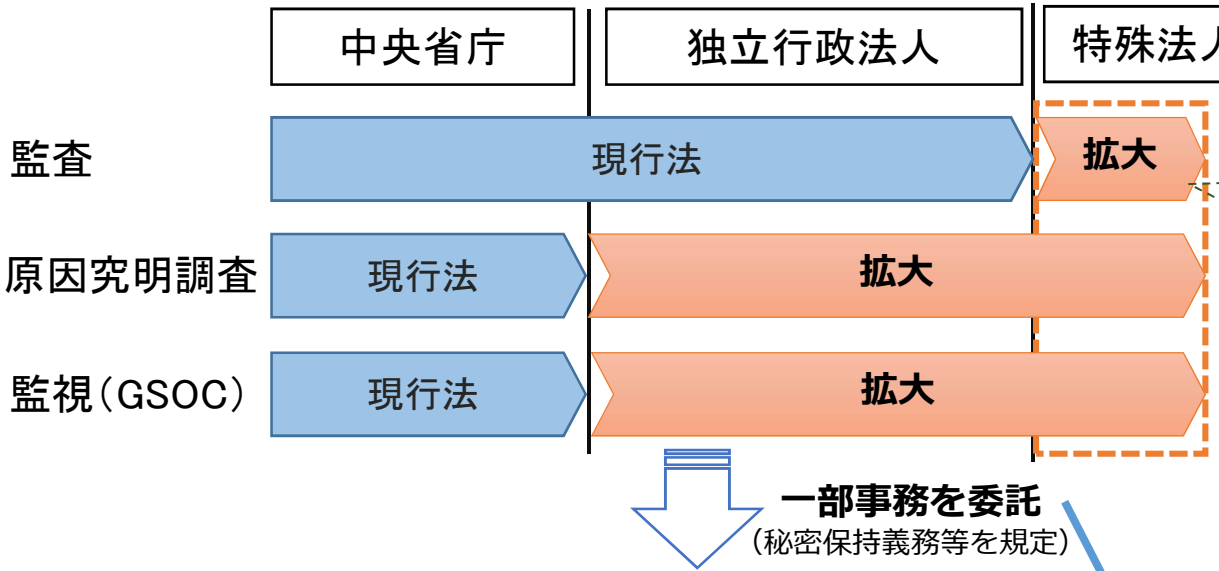
- 政策目的：自由、公正かつ安全なサイバー空間を創出・発展させ、もって①経済社会の活力の向上及び持続的発展、②国民が安全で安心して暮らせる社会の実現、③国際社会の平和・安定及び我が国の安全保障に寄与すること
- 国際社会の平和・安定及び我が国の安全保障を達成するための施策：①我が国の安全の確保、②国際社会の平和・安定、③各国との協力・連携によって、達成していくことを宣言

■ 取組実績（2016年10月現在）

- サイバーセキュリティ戦略及び日米防衛協力のための指針を踏まえ、日米サイバー協力を強化
- G7サミット等、首脳・閣僚のハイレベル国際協議や国連政府専門家会合、法執行機関間の連携強化により、サイバー空間における法の支配の確立に積極的に寄与
- サイバーセキュリティ国際キャンペーン（毎年10月）を開催し、ASEAN及び米と連携した意識啓発を推進
- 国際サイバー演習の主催や積極的な参加を通じ、重大な情報セキュリティ事案発生時における国外関係機関との連絡体制の整備を推進
- 二国間協議（2016年10月現在12か国・地域との間でサイバー協議等を実施）や多国間会議を通じ、我が国のサイバーセキュリティ関係施策や考え方等の積極的な発信、連携の具体化や信頼醸成を推進
- 関係省庁間で、サイバーセキュリティ分野における能力構築支援に関する基本方針を策定。引き続きオールジャパンでASEANを中心とした支援の取組みを強化

サイバーセキュリティ基本法の改正法の施行（2016年4月15日成立、4月22日公布、10月21日施行）

■ 国が行う不正な通信の監視、監査、原因究明調査等の対象範囲を拡大
■ サイバーセキュリティ戦略本部の一部事務を独立行政法人情報処理推進機構（IPA）に委託



監視、監査、原因究明調査等の対象となる法人の指定（本部決定）

- ✓ 日本年金機構等の公的年金関係法人（※）及び地方公共団体情報システム機構（J-LIS）を指定。（9法人）

※ 日本年金機構、国家公務員共済組合連合会（KKR）、地方公務員共済組合連合会、地方職員共済組合、都職員共済組合、全国市町村職員共済組合連合会、日本私立学校振興・共済事業団、公立学校共済組合

- ✓ IPAへの委託は「サイバーセキュリティ対策を強化するための監査に係る基本方針」「サイバーセキュリティ戦略本部重大事象施策評価規則」を踏まえて実施

情報処理安全確保支援士制度の開始に伴う規定の整備（情報処理の促進に関する法律の一部改正に伴う政省令の整備）

その他法改正に伴い整備する規則等（本部決定）

- ✓ 政府機関等の情報セキュリティ対策のための統一基準群（※前回戦略本部で改定済）
- ✓ サイバーセキュリティ対策を強化するための監査に係る基本方針
- ✓ サイバーセキュリティ戦略本部重大事象施策評価規則
- ✓ サイバーセキュリティ戦略本部資料提供等規則

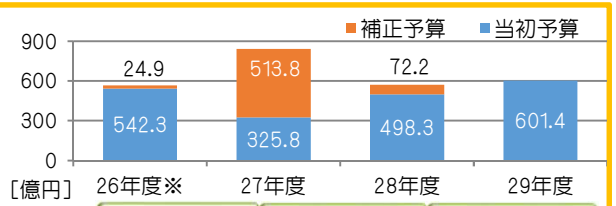
政府のサイバーセキュリティに関する予算

平成29年度予算概算要求額

601.4億円

（平成28年度当初予算額　498.3億円）

サイバーセキュリティに関する予算として切り分けられない場合には計上していない。



主な施策例及び予算額

		平成29年度概算要求	平成28年度第2次補正	平成28年度当初予算
【内閣官房】	内閣サイバーセキュリティセンター予算	28.7億円	4.2億円	17.3億円
【警察庁】	サイバーテロ対策用資機材の増強等	4.1億円	—	4.0億円
【警察庁】	サイバーセキュリティ対策に係る人材育成基盤の整備	8.7億円	—	—
【総務省】	ナショナルサイバートレーニングセンター（仮称）の構築	35.1億円	—	7.2億円
【総務省】	ICT環境の変化に応じた情報セキュリティ対応方策の推進事業	4.0億円	—	4.0億円
【総務省】	IoT時代におけるサイバーセキュリティ総合対策実証事業	—	5.0億円	—
【総務省】	自治体の情報セキュリティ対策の強化	5.0億円	—	—
【外務省】	情報セキュリティ対策の強化	6.3億円	—	4.1億円
【外務省】	サイバー空間に関する外交及び国際連携	0.2億円	—	0.1億円
【経済産業省】	産業系サイバーセキュリティ推進事業	8.0億円	25.0億円	—
【経済産業省】	（独）情報処理推進機構（IPA）交付金	45.5億円	4.0億円	42.5億円
【経済産業省】	サイバーセキュリティ経済基盤構築事業	23.5億円	—	21.6億円
【防衛省】	作戦システムセキュリティ監視装置の整備	7.0億円	—	—
【防衛省】	サイバー攻撃等への対処能力を強化するサイバーレジリエンス技術の研究	7.0億円	—	—
【個人情報保護委】	特定個人情報（マイナンバーをその内容に含む個人情報）に係るセキュリティの確保を図るための委員会における監視・監督体制の拡充	14.3億円	—	2.6億円
【厚生労働省】	本省及び日本年金機構等の関係機関における情報セキュリティ対策の強化	47.1億円	1.8億円	39.6億円
【文部科学省】	大学や高専におけるセキュリティ人材の育成	4.5億円	—	3.8億円
【金融庁】	金融業界横断的なサイバーセキュリティ演習の実施	0.6億円	—	0.3億円
【国土交通省】	重要インフラ事業者等に対する情報セキュリティ強化策	2.2億円	—	0.3億円

平成28年度第2次補正予算

72.2億円

サイバーセキュリティに関する予算として切り分けられない場合には計上していない。

※　平成26年度の数値は、社会保障と税に関する番号制度の導入に伴うシステム開発（内閣官房）等も含む。

「日本再興戦略2016」（サイバーセキュリティ関連部分抜粋）

第２　具体的施策

Ⅰ　新たな有望成長市場の創出、ローカル・アベノミクスの深化等

１．第４次産業革命の実現

（２）新たに講ずべき具体的施策

ⅱ）第４次産業革命を支える環境整備

⑥ サイバーセキュリティの確保とIT利活用の徹底等

ア）サイバーセキュリティの確保

IoTにより全てのモノがインターネットにつながる時代において、サイバーセキュリティ対策は、「コスト」ではなく、国民生活や企業の円滑な経済活動を支える「未来への投資」である。こうした観点から、サイバーセキュリティの成長産業化等を進めつつ、昨年閣議決定したサイバーセキュリティ戦略（平成27年９月４日閣議決定）や今年成立した改正サイバーセキュリティ基本法に基づく官民を挙げた取組を進め、人材育成、政府機関及び重要インフラの対策や、IoTシステム対策、研究開発、国際ルール等の形成等を強力に推進する。

・人材育成に関しては、「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31日サイバーセキュリティ戦略本部決定）に沿って検討を進める。その際、企業のセキュリティ対策の推進に必要な橋渡し人材層の育成と経営層の意識改革によって、人材需要の喚起を進める。また、今後必要となる人材像のビジョンを明確化し、2020年までに情報処理安全確保支援士の登録者数３万人超を目指すことをはじめとして、産学官連携による教育・演習実施・資格整備等を通じた人材供給を進める。こうした人材の需要と供給の好循環を形成するための各施策をつなぐ取組について検討を進め、本年度中に策定・公表する次期人材育成プログラムに盛り込む。さらに、各府省庁における司令塔機能の抜本的強化、橋渡しセキュリティ・IT人材（部内育成の専門人材）の確保・育成や対処機関における人的基盤の強化等に取り組む。

・重要インフラ防護に関しては、「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」（平成28年３月31日サイバーセキュリティ戦略本部決定）に従い、経営層における取組や情報共有、内部統制の強化やマイナンバー制度の運用に係るセキュリティ確保等の「サイバー攻撃に対する体制強化」、情報共有範囲の見直し等の「重要インフラに係る防護範囲の見直し」、国際連携や産学官連携による人材育成等の「多様な関係者間の連携強化」等に係る検討を進め、本年度末までに行動計画の見直しについて結論を得る。なお、早急に対処すべき事項については行動計画の見直しを待たずに対処することとする。特に、産学官連携による重要インフラ・産業におけるセキュリティ人材育成・技術開発のための体制については、2020年東京オリンピック・パラリンピック競技大会に向け、来年度中に整備する。