資料２

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（案）

資料２－１　「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（案）」概要

資料２－２　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（案）

「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（案）」概要

資料2－1

1．行動計画見直しに当たっての基本方針

◆ 重要インフラを標的としたサイバー攻撃の深刻化に伴う重要インフラ防護の必要性が高まっている中、「サイバーセキュリティ戦略」（平成27年9月閣議決定）等に基づき、対策強化に向けた検討課題を整理。その際、「機能保証」の考え方に基づく取組を含める。

◆ 本ロードマップに従い検討を進め、行動計画の見直しについて、平成29年3月末を目途に結論。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。

2．考慮すべき環境変化

(1) **ＩｏＴの浸透に伴う制御技術と情報通信技術の相互依存性の高まり**

- 実空間（モノ・ヒト）とサイバー空間（情報）の物理的制約を越えた連接
- サイバー攻撃の対象となり得る機器が我々の身の周りの隅々まで拡散・浸透

(2) **面的防護に向けた情報共有等の連携体制強化の必要性等**

- ＩｏＴシステムを活用した新たなビジネスの創出や既存ビジネスの高度化・高付加価値化に伴うサプライチェーンリスクの高まり

(3) **諸外国における重要インフラへの取組の加速化**

- 官民間の情報共有の枠組みの強化・推進等の取組が進展

（米国「サイバーセキュリティ法」、EU「ネットワーク及び情報セキュリティ(NIS: Network and Information Security)指令」(案)）

3．強化すべき取組の方向性

1）サイバー攻撃に対する体制強化

➢ **経営層における取組の強化の推進**
- 機能保証の考え方に立脚し自らの経営責任を全うする観点からのセキュリティ経営資源投入の推進（情報開示の在り方）
- 経営層のセキュリティ意識改革を促す環境の整備（インセンティブの在り方）

➢ **情報共有の強化**
- 予兆脅威情報を含む共有すべき情報の範囲の見直しと情報共有の活性化
- 法令に基づく義務的な報告又は補完的な報告の着実な実施、安全基準や報告事項の基準等の見直し

➢ **内部統制の強化の推進**
- 自ら若しくは第三者による監査等の推進（マネジメント監査、侵入試験等）
- リスクマネジメントの推進強化

➢ **マイナンバー制度の運用に係るセキュリティの確保に関する取組**

➢ **2020年東京オリンピック・パラリンピック競技大会等大規模イベントの情報共有・対処体制のモデル化**

2）重要インフラに係る防護範囲の見直し

➢ **情報共有範囲の拡大**
- 相互依存性等を考慮した情報共有体制に組み込むべき主体の拡大

➢ **分野横断的な情報共有の強化**
- スマートシティ、自動車等、従来の業態の枠に収まらない情報共有のための体制の検討（既存の情報共有体制との連携の在り方を含む）

➢ **国の安全等の確保の観点からの取組**
- 重要インフラに属さないものの、我が国の知的財産や営業秘密を保全する観点から情報共有等を推進すべき分野の取組強化（研究機関、大学等を含む）

3）多様な関係者間の連携強化

➢ **国際連携**
- 海外ＩＳＡＣとの連携（共同演習、情報共有を含む）の促進
- 二国間・地域間・多国間の枠組みを活用した国際連携の継続

➢ **人材育成**
- 人材育成強化方針に基づく重要インフラに係るセキュリティ人材の育成支援

4．行動計画の見直しに向けた今後の検討スケジュール

➢ 平成28年夏期に行われる評価を踏まえ、秋頃に行動計画の見直し骨子（案）を策定

➢ 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

➢ 上記検討は、2020年東京オリンピック・パラリンピック競技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

強化すべき取組の方向性(具体的施策)

◆ 本ロードマップでは、**検討時期(結論を得る時期)を可能な限り具体化**。
◆ **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**。

１）サイバー攻撃に対する体制強化

➢ 経営層における取組の強化の推進

○ 制御系（ＯＴ）と情報系（ＩＴ）のシステムの融合を踏まえ、「機能保証（任務保証）」の考え方に立脚し、事業継続を意識して経営層が自らの経営責任を全うする観点からセキュリティに係る経営資源が投入されるよう取り組む（情報開示の在り方について検討を行い、平成28年秋までにその方向性を明確にするとともに、「サイバーセキュリティ経営ガイドライン」の普及推進を継続的に実施。）

○ 経営層のセキュリティ意識改革を促す環境整備を図る（平成28年度中に具体策について一定の結論を得る。）

➢ 情報共有の強化

○ 予兆脅威情報を含む共有すべき情報の範囲の見直しと情報共有の活性化（平成28年度末までに一定の結論を得て、その後も継続的に見直しを行う。報告事例集の作成は、平成28年度上期に実施。）

○ 法令に基づく義務的又は補完的な報告の着実な実施、安全基準や報告事項の基準等の見直し（平成28年度末までに具体的な方針について結論を得る。）

➢ 内部統制の強化の推進

○ 自ら又は第三者による監査等の推進（マネジメント監査、侵入試験（情報システムに対する擬似的攻撃による評価（監査））等）（平成28年度末までに推進策についての結論を得る。）

○ 演習の取組強化（平成28年度中に仮想演習環境の構築に向けての検討を開始し、平成２９年度末までに結論を得る。）

○ リスクマネジメントの推進強化（平成28年度中に推進強化策についての結論を得て、平成２９年度以後に推進を行う。（手順書については、平成２７年度の取組成果を平成28年度半ばに提供する。その他前倒し可能な取組は、結論を得た後に速やかに取り組む。））

➢ マイナンバー制度の運用に係るセキュリティの確保に関する取組

○ マイナンバーの利用に係るサイバーセキュリティの確保に関する取組を継続的に実施する。

➢ 2020年東京オリンピック・パラリンピック競技大会等大規模イベントの情報共有・対処体制のモデル化

○ 2020年東京オリンピック・パラリンピック競技大会に向けた情報共有・対処体制の整備についてのノウハウ等のモデル化（各年度の取組成果について、翌年度を目途に公表）

➢ 安全基準の不断の見直し等

○ 業法によってサービスの維持及び安全確保に係る水準が求められている分野の安全基準の見直し等（継続実施）

２）重要インフラに係る防護範囲の見直し

➢ 情報共有範囲の拡大

○ 相互依存性等を考慮した情報共有体制に組み込むべき主体の拡大（平成28年度末までに一定の結論を得て、その後も継続的に見直しを行う。）

➢ 分野横断的な情報共有の強化

○ スマートシティ、自動車等、従来の業態の枠に収まらない情報共有のための体制の検討（既存の情報共有体制との連携の在り方を含む。）（平成28年度中を目途にＩｏＴシステムに関する分野横断的な情報共有の在り方についての検討を行う。）

➢ 国の安全等の確保の観点からの取組

○ 重要インフラに属さないものの、我が国の知的財産や営業秘密を保全する観点から情報共有等を推進すべき分野の取組強化（研究機関、大学等を含む）（平成28年度末までに一定の結論を得て、その後も継続的に見直しを行う。）

３）多様な関係者間の連携強化

➢ 国際連携

○ 海外ＩＳＡＣとの連携（共同演習、情報共有を含む。）に向けた取組の促進（継続実施）

○ 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し、我が国の取組を積極的に公表（平成28年度以降、継続的に実施。）

➢ 人材育成

○ 人材育成強化方針に基づく重要インフラに係るセキュリティ人材の育成支援、官民人材交流、資格取得促進（平成28年度以後継続実施）

資料２－２

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（案）

１．行動計画見直しに当たっての基本方針

重要インフラを標的とするサイバー攻撃が深刻化し、重要インフラ防護の必要性が急速に高まっている。こうした中、平成２９年度は、「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」（平成２６年５月情報セキュリティ政策会議決定）[1]（以下「行動計画」という。）の見直しの時期とされているところであり、「サイバーセキュリティ基本法」（平成２６年法律第１０４号）及び「サイバーセキュリティ戦略」（平成２７年９月閣議決定）を踏まえ、その見直しに向けた具体的な検討を行う。

見直しに当たっては、重要インフラを標的とするサイバー攻撃の状況や、その背景としての環境変化を踏まえる。また、情報通信技術が社会経済システムに広く実装されてきていることや、２０２０年東京オリンピック・パラリンピック競技大会の運営を支障なく遂行させることを考慮し、「機能保証（任務保証）」の考え方[2]に基づく取組を含めるものとする。

なお、行動計画の見直しについては、本ロードマップに従い検討を進め、平成２９年３月末を目途に結論を得る。ただし、検討の中途においても、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速やかに対処することとする。

２．考慮すべき環境の変化

昨今、国民の個人情報の漏えいや財産の侵害等をはじめ、実生活に悪影響を及ぼすサイバー攻撃の事例が頻繁に報告されており、被害が深刻化している。また、２０２０年東京オリンピック・パラリンピック競技大会を始めとする国際的なビッグイベントに向けて、我が国は、国際的に大きな注目を集める一方で、悪意ある者の関心の対象ともなり、サイバー攻撃等のリスクが高まりつつあると考えられる。

こうした深刻化するサイバー攻撃等の脅威から重要インフラを防護するためには、以下に示すような重要インフラを取り巻く技術環境や社会環境の変化を考慮した上で、その取組の方針を定めることが必要である。

(1) ＩｏＴ[3]の浸透に伴う制御技術と情報通信技術の相互依存性の高まり

近年、センサーデバイス等のハードウェアの進化、低廉かつ高速なインターネットの普及、ビッグデータ解析技術の進歩等を背景に、パソコンのみならず、家電、自動

[1] 本行動計画は、平成２７年５月、サイバーセキュリティ戦略本部において改訂された。

[2] 各重要インフラ事業者等が、重要インフラの機能の発揮やサービスの提供を全うするという観点でのリスクアセスメントを行い、経営層による総合的な判断を踏まえたリスク対応を進めていくことにより、当該重要インフラを防護し、事業継続を確保していくという考え方

[3] **I**nternet **o**f **T**hings

車、ロボット、スマートメーター等のあらゆるモノがインターネット等のネットワークに接続され始めており、そこから得られるビッグデータの利活用等により新たなサービスの実現が可能となるシステム（以下「ＩｏＴシステム」という。）が普及しつつある。こうした状況が進展し、実空間のモノやヒトがサイバー空間上の情報の自由な流通とデータの正確な通信により物理的制約を越えて多層的につながる(連接する)ことで、実空間とサイバー空間の融合が高度に深化した社会、すなわち「連接融合情報社会」が到来しつつある。サイバー攻撃の対象となり得るＩｏＴシステムが我々の身の周りの隅々まで行き渡り、仮に重大な脆弱性を抱えた製品が広く流通し更新(アップデート）されないまま使用され続けられれば、サイバー攻撃による悪意ある操作や意図しない動作に起因して国民の生命や財産に深刻な影響をもたらしうることとなる。

また、我が国の重要インフラにおいても、電力分野のスマートメーターや化学・石油分野の工場生産系システムに代表されるような、制御技術（ＯＴ[4]）に情報通信技術（ＩＴ[5]）を融合させた新たな制御システムの基盤が導入されつつある（制御系と情報系のシステムの一体化)。こうした制御システムは、汎用製品の使用や標準プロトコルの導入といった技術のオープン化、ネットワークのオープン化等が進むにつれて従来機器の置換なども含め広く利用されるようになると考えられる。

一方で、制御系と情報系のシステムの一体化や技術のオープン化・標準化等は、従来に比してＩＴの不具合やサイバー攻撃による影響を受けやすく、意図しない動作をするよう遠隔操作される可能性が高まることから、安全を確保し、持続的なサービスを提供していくためにはこれまで以上に十分な対策が求められる。

(2) 面的防護に向けた情報共有等の連携体制強化の必要性等

今後、企業は、これまでの事業領域にとどまらず、ＩｏＴシステムを活用した新たなビジネスの創出や既存ビジネスの高度化・高付加価値化を図る方向に向かうと見込まれる。オープンイノベーションの進展は、異業種のテクノロジーの利用を促進し、既存の産業との垣根が低くなることで、新たな事業領域への参入が容易になるといった大きなビジネスチャンスをもたらす。そして、企業がこうしたビジネスチャンスを確実に捉えることは、我が国の経済社会の活力の向上及び持続的発展にとって極めて重要である。

一方、連接融合情報社会においては、前述のとおり、社会経済システム全体へのリスクの拡散や被害の深刻化が懸念される。このため、企業経営に当たっては、経営層が自らの経営責任を全うする観点から、これまで以上にセキュリティリスクの把握や経営資源に係る投資判断を適切に行い、製品・サービスへのセキュリティ機能の実装

[4] Operation Technology
[5] Information Technology

の推進、セキュリティ人材の育成、組織能力の向上等を図ることが必要となってくる。また、国境を越えてその経営資源を調達することも考えられるため、サプライチェーン全体のセキュリティを向上するための方策を講じることが重要となる。

こうした状況において、サイバー空間に関わる多種多様な主体が、それぞれの役割を発揮しつつ、相互に連携しながら共助することにより、社会経済システム全体の柔軟な対応力を強化していくことが重要であり、また、「面としての防護」の確保に向け、既存分野領域を越えたグローバルな連携体制の強化が必要となる。

(3) 諸外国における重要インフラへの取組の加速化

諸外国においても、技術環境や社会環境の変化を踏まえ、情報共有の強化を始めとする重要インフラへの取組を加速化している状況にある。例えば、米国においては、２０１５年１２月にサイバーセキュリティ法（Cybersecurity Act of 2015）が成立し、サイバー脅威の指標（インディケーター）の官民間の自主的な情報共有について必要な手続を策定することを関係省庁に義務付けている。また、欧州連合（ＥＵ）においては、「ネットワーク及び情報セキュリティ（ＮＩＳ:Network and Information Security）指令」（案）に、ＥＵ域内の越境商取引やサービスの提供を阻害するセキュリティ・インシデントの報告を企業に義務付ける規定を盛り込むなど、法整備を伴う官民間の情報共有の枠組みの強化・推進等の取組が進められている。

こうした諸外国の動向を見据えつつ、我が国においても、多様な関係者（ステークホルダー）が連携し、重要インフラに係る官民間の情報共有の強化を始めとするサイバーセキュリティ確保のための取組を推進していくことが必要である。

３．強化すべき取組の方向性

前述の環境の変化を考慮し、短期的に取り組むべき事項及び行動計画を見直した上で取り組むべき事項とその方向性を以下に示す。

なお、各取組に共通する観点として、重要インフラの機能やサービスは、それ自体が国民生活・経済社会活動を支える基盤となっており、その提供に支障が生じると国民の安全・安心に直接的かつ深刻な負の影響が生じる可能性があり、対策に万全を期す必要があることを踏まえ、前記「機能保証（任務保証）」の考え方の浸透を図る。

(1) サイバー攻撃に対する体制強化

重要インフラ事業者等がサイバー攻撃を受けたとしても国民生活・経済社会活動に重大な影響が出ないように、重要インフラサービスの安全かつ安定的な提供に資する体制・制度の強化を図る。

ア　経営層における取組の強化の推進

・制御系（ＯＴ）と情報系（ＩＴ）のシステムの融合を踏まえ、「機能保証（任務保証）」の考え方に立脚し、事業継続を意識して経営層が自らの経営責任を全うする観点からセキュリティに係る経営資源が投入されるよう取り組む（情報開示の在り方について検討を行い、平成２８年秋までにその方向性を明確にするとともに、「サイバーセキュリティ経営ガイドライン」の普及推進を継続的に実施。）
・経営層のセキュリティ意識改革を促す環境整備を図る（平成２８年度中に具体策について一定の結論を得る。）

重要インフラ事業者等の経営層が十分なリーダーシップを発揮し、セキュリティリスクの評価や経営資源に係る投資判断を適切に行うために、事業継続を意識し、経営層が自らの経営責任を全うする観点からサイバーセキュリティの確保に取り組むよう、経営層に対する取組の強化を推進する（セキュリティ意識を持った企業経営の推進）。

また、重要インフラ事業者等が積極的な投資を行う環境を整備することにより、サイバーセキュリティ関連産業を振興し、対策の強化につなげる。

(a) サイバーセキュリティへの取組状況に係る情報開示の推進（経営リスクマネジメントに積極的な取組を行っていることを明らかにするため、サイバーセキュリティ対策の状況について、サイバーセキュリティへの取組を踏まえたリスクの性質・度合いに応じて、情報セキュリティ報告書、ＣＳＲ報告書、サステナビリティレポートや有価証券報告書等への記載を通じた情報開示の在り方を検討し、平成２８年秋までに方向性を明確化）
(b) 「サイバーセキュリティ経営ガイドライン」[6]の継続的な見直し及び普及推進（平成２８年度以後、継続実施）
(c) 各取組を推進する上での企業へのインセンティブ付与（公的支援、政府調達におけるサービス品質保証（ＳＬＡ[7]）への反映（総合評価落札方式で行う場合における加点）等）の在り方等、経営層のセキュリティ意識改革を促す環境整備（平成２８年度中に具体策について一定の結論を得る。）
(d) 重要インフラ事業者等に対する高度なサイバー攻撃からの防護の観点から、高度な技術や人材育成等サイバーセキュリティ対策の高度化について、ベンダーのみならず、重要インフラ事業者等の積極的な取組を促す（平成２８年度中に具体策について一定の結論を得る。）

[6] 平成２７年１２月、経済産業省において策定・公表
[7] **S**ervice **L**evel **A**greement

イ　情報共有の強化

・予兆脅威情報を含む共有すべき情報の範囲の見直しと情報共有の活性化（平成２８年度末までに一定の結論を得て、その後も継続的に見直しを行う。報告事例集の作成は、平成２８年度上期に実施。）
・法令に基づく義務的又は補完的な報告の着実な実施、安全基準や報告事項の基準等の見直し（平成２８年度末までに具体的な方針について結論を得る。）

サイバー攻撃に係るより効果的な情報共有を実現するため、情報共有を妨げる障壁を排除する仕組み、共有情報の拡充・共有体制の強化、共有の迅速化及び提供情報の活用の推進の観点から情報共有の活性化を図る。

①　情報共有の障壁の排除（情報共有をしやすくする環境整備）

(a) サイバー攻撃に係る情報を連絡することが営業上の利益の毀損（経済的な利益喪失）や社会的評価の低下につながるのではないかといった懸念を払拭するための情報共有の仕組みの構築（情報連絡元を秘匿化した情報共有システムの構築等）（平成２８年度中を目途に情報共有スキームの設計を実施。）

(b) 報告すべきセキュリティ事象（インシデント）の判別等に係る各報告主体の共通認識の醸成（報告基準の明確化、報告事例の例示等）（平成２８年度上期において、報告事例集を作成し、周知を図る。）

②　共有情報の拡充・共有体制の強化

(a) 業法等に基づく所管省庁への報告体制の強化（各所管省庁と連携しつつ、平成２８年度末までに法令に基づく義務的又は補完的な報告が着実に行われるよう事業者等に再確認するとともに、法令の体系に基づく安全基準やそれを補完するガイドライン、報告事項の基準等の見直し方針についての結論を得る。）

(b) 共有すべき情報の範囲の見直し（予兆脅威情報の共有等）（平成２８年度末までに一定の結論を得て、その後も継続的に見直しを行う。）

(c) 制御系システムについての情報共有の活性化（制御技術と情報通信技術の融合により、業法等において従来想定していなかったサイバー攻撃によるサービス停止等が発生した際の企業における関係法令等を考慮した情報連絡体制の見直し等）（平成２８年度末までに方針についての結論を得る。）

(d) セプター[8]内・セプター間における情報共有の活性化（セプターに対する各種支援の強化等）（継続実施）

[8]「セプター（CEPTOAR）」とは、各重要インフラ分野で整備されている情報共有体制のこと。
CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response

③　共有の迅速化

(a) 共通化・自動化を実現するための仕組みの検討（標準化された脅威情報の様式、戦略的イノベーション創造プログラム（ＳＩＰ[9]）で検討中の情報共有プラットフォーム等を活用した自動化された交換手順等）（上記①(a)の取組とともに検討を進め、平成２９年度末を目途に情報共有基盤（プラットフォーム）の活用等の方針について結論を得る。）

(b) 緊急性の高い脅威情報について、内閣サイバーセキュリティセンター（ＮＩＳＣ）が重要インフラ事業者等から直接的に情報連絡を受ける仕組みの検討（ホットラインの構築等）（各所管省庁と連携しつつ、上記①(a)の取組とともに検討を進め、平成２８年夏までに方針について結論を得る。）

(c) 「我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針」（平成２８年１月サイバーセキュリティ戦略本部決定）において、「サイバーセキュリティ戦略本部長は、本部が行う関係行政機関における重要インフラ事業者等に関する施策に対する評価に基づき、又は本部が関係行政機関の長を通じて入手した重要インフラ事業者等に係る資料又は情報等に基づき、必要があると認めるときは、関係行政機関の長への勧告を行う」こととしており、基本的な運用方針を策定する（平成２８年度上期に実施）

④　提供情報の重要インフラ事業者等による活用の推進

(a) 脅威情報の活用に係るグッドプラクティス事例等の共有（平成２８年度上期にセプターから事例を収集・共有し、その後、定期的に実施する。）

(b) 分野横断的な提供情報の高度化の検討（各種データを分野横断的に分析し、それにより得られる攻撃傾向を重要インフラ事業者等に展開する取組を強化する方針について検討を行い、平成２８年度上期に基本的枠組について一定の結論を得るとともに、以後、継続的に具体化に向けた検討を進める。）

ウ　内部統制の強化の推進

- 自ら又は第三者による監査等の推進（マネジメント監査、侵入試験（情報システムに対する擬似的攻撃による評価（監査））等）（平成２８年度末までに推進策についての結論を得る。）
- 演習の取組強化（平成２８年度中に仮想演習環境の構築に向けての検討を開始し、平成２９年度末までに結論を得る。）
- リスクマネジメントの推進強化（平成２８年度中に推進強化策についての結論

[9] Cross-ministerial **S**trategic **I**nnovation Promotion **P**rogram

を得て、平成２９年度以後に推進を行う。（手順書については、平成２７年度の取組成果を平成２８年度半ばに提供する。その他前倒し可能な取組は、結論を得た後に速やかに取り組む。））

セキュリティ意識を持った企業経営の推進のため、前記「経営層における取組の強化」と併せて、技術環境や社会環境の変化等を踏まえた継続的なリスク評価が行われること、経営層に対しリスク評価に基づく適切な助言がなされること、経営層による意思決定や意思決定に至るプロセスに対する妥当性等の評価がなされることなどの内部統制の取組を強化する。

(a) 重要インフラ事業者等が自律的に行う情報セキュリティ管理に係る内部監査・外部監査の推進（情報セキュリティ監査制度に準拠した監査の推進等）（推進策について、平成２８年度末までに結論を得る。）

(b) 重要インフラ事業者等が責任を持って自律的に行う脆弱性検査等の推進（平成２８年度前半までに侵入試験（ペネトレーションテスト）等の実施計画を策定するほか、継続的な推進策について、平成２８年度末までに結論を得る。）

(c) 重要インフラ事業者等の障害対応能力の検証体制の強化（分野横断的演習やセプター訓練等の取組継続に加え、重要インフラ事業者等が独力で検証できるような仮想演習環境の構築等）（仮想演習環境の構築に向けては、平成２８年度中に検討を開始し、平成２９年度末までに結論を得る。）

(d) 重要インフラ事業者等が自律的に行うリスクマネジメントの推進強化（リスクマネジメントを支援する資料（手順書、脅威リスト等）の提供や講習会の実施等）（推進強化策について、平成２８年度中に結論を得て、平成２９年度以後に推進する。（手順書については、平成２７年度の取組成果を平成２８年度半ばに提供する。その他前倒し可能な取組については、結論を得た後に速やかに取り組む。））

エ　マイナンバー制度の運用に係るサイバーセキュリティの確保に関する取組

・マイナンバーの利用に係るサイバーセキュリティの確保に関する取組を継続的に実施する。

平成２８年１月から社会保障・税・災害対策の行政手続においてマイナンバーの利用が始まっており、利用範囲拡大に関する検討も進められている。

こうした状況において、政府としてもサイバーセキュリティが確保されたものとなるよう、既に以下の取組を進めているところであり、引き続きこの取組を推進する。

(a) 地方公共団体の情報システムについて、マイナンバー制度の運用に係るセキュリティを強化する観点から、個人情報保護委員会等の政府機関及び地方

公共団体情報システム機構等の関係主体とが連携し、必要な支援を継続する（継続実施）

(b) マイナンバー利用事務系では、住民情報流出を防止し、マイナンバーによる情報連携に活用される LGWAN 環境のセキュリティを確保するため、LGWAN 接続系とインターネット接続系を分割するとともに、都道府県と市区町村が協力して、自治体情報セキュリティクラウドを構築するなどの所要の対策を講じる（継続実施）。

(c) マイナンバー法における個人番号利用事務に関するシステムについて、関係機関が連携し専門的・技術的知見を有する監視・監督体制を整備する。また、連携・接続する国・地方の関連システム全体を俯瞰した監視・検知体制の整備に向けて、政府機関情報セキュリティ横断監視・即応調整チーム（ＧＳＯＣ）との情報連携も踏まえたインシデントの監視・検知を迅速に行える体制を整備する（継続実施）。

オ　２０２０年東京オリンピック・パラリンピック競技大会等大規模イベントの情報共有・対処体制のモデル化

・２０２０年東京オリンピック・パラリンピック競技大会に向けた情報共有・対処体制の整備についてのノウハウ等のモデル化（各年度の取組成果について、翌年度を目途に公表）

２０２０年東京オリンピック・パラリンピック競技大会やサミット等の大規模イベントは、国際的にも注目され、サイバー攻撃の激化が予想されることから、情報共有体制や対処体制の強化を進める。また、こうした大規模イベントにおける取組の経験を踏まえた対処体制のモデル化を行い、継続的に改善・活用していく。

(a) ２０２０年東京オリンピック・パラリンピック競技大会に備えた対処体制等の構築に係るノウハウ等をモデル化し、閉会後に活用できるレガシーとして引き継ぐ（リスクアセスメント手順や、ＣＳＩＲＴ[10]等の官民情報共有体制のノウハウ等の文書化等）（各年度の取組成果について、翌年度を目途に公表する。）

カ　安全基準の不断の見直し等

・業法によってサービスの維持及び安全確保に係る水準が求められている分野の安全基準の見直し等（継続実施）

[10] **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam

業法によってサービスの維持及び安全確保に係る水準が求められている分野については、昨今のサイバー空間を取り巻く環境変化を踏まえ、安全基準について不断の見直しを行う。

電力分野においては、スマートメーターシステム、制御系システムの安全基準を策定し、電気事業法における保安規制に位置づける（本年夏を目途）。２０２０年の東京オリンピック・パラリンピックに向けて、対策を確実なものとするため、他の業種においても、サイバーセキュリティ対策を、業法における保安規制に位置づけることを検討する。制御系機器・システム等の調達及び運用に関して、可能なものについては国際標準に準拠した第三者認証制度を活用する（継続実施）。

(2) 重要インフラに係る防護範囲の見直し

重要インフラの防護に向けては、前述のとおり、サプライチェーン全体のセキュリティを向上するための方策を講ずることが重要となる。その方策を講ずるに当たり、「面としての防護」の確保に向けた防護範囲の拡充について、以下の観点から検討を行う。

ア　情報共有範囲の拡大

・相互依存性等を考慮した情報共有体制に組み込むべき主体の拡大（平成２８年度末までに一定の結論を得て、その後も継続的に見直しを行う。）

「面としての防護」を確保するため、「機能保証（任務保証）」の考え方を踏まえ、重要インフラ間の相互依存や重要インフラの外部サービス（既存の重要インフラ事業者等でない外部委託先等の周辺事業者等が提供するサービス）への依存等の実態を踏まえ、サプライチェーン全体にセキュリティ関連の情報共有等の取組を拡充していく。また、重要インフラ間の相互依存を考慮し、中小規模の事業者を含む重要インフラ事業者間の情報共有を充実させる。

(a) 重要インフラ事業者等を支える外部委託先等の周辺事業者への情報共有範囲の拡大（平成２８年度末までに一定の結論を得て、その後も継続的に見直しを行う。）

(b) 既存の重要インフラ分野における情報共有の活性化（セプターを通じた情報共有がなされていない中小事業者その他の重要インフラ事業者等をセプターに組み入れる。）（まずは平成２８年度中を目途にセプターを通じた情報共有がなされていない重要インフラ事業者等を把握し、参加を促す。）

(c) 電力・ガス分野における市場改革、金融分野におけるフィンテック（FinTech）の進展等の環境の変化に対応した情報共有体制の検討（関係省庁と連携しつつ、継続して検討）

イ　分野横断的な情報共有の強化

・スマートシティ、自動車等、従来の業態の枠に収まらない情報共有のための体制の検討（既存の情報共有体制との連携の在り方を含む。）（平成２８年度中を目途にＩｏＴシステムに関する分野横断的な情報共有の在り方についての検討を行う。）

前記既存分野領域を越えた連携体制強化の必要の高まりを踏まえ、自動車の自動運転技術、スマート家電、スマートシティ等の既存分野の枠に収まらないＩｏＴシステムのサイバーセキュリティの確保のために、分野横断的な情報共有の取組を強化する。

(a)　「自動車」、「スマート家電」、「スマートシティ」等のＩｏＴシステムに関する分野横断的な情報共有体制（分野横断的セプター）の在り方（既存のセプターや関係省庁との連携）（平成２８年度中を目途にＩｏＴシステムに関する分野横断的な情報共有の在り方についての検討を行う。）

(b)　各セプターやセプターカウンシル[11]と連携した分野横断的な情報共有の推進強化（継続実施）

ウ　国の安全等の確保の観点からの取組

・重要インフラに属さないものの、我が国の知的財産や営業秘密を保全する観点から情報共有等を推進すべき分野の取組強化（研究機関、大学等を含む）（平成２８年度末までに一定の結論を得て、その後も継続的に見直しを行う。）

昨今のサイバー攻撃の深刻化に伴い、国民生活・経済社会活動の防護等に関し、安全保障上の観点を踏まえる必要性が高まっている。また、連接融合情報社会においては、企業がこれまでの事業領域にとどまらず、新たなビジネスの創出や既存ビジネスの高度化･高付加価値化を図ることになる。こうした社会環境の変化に伴い、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や、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。

(a)　核物質防護等の措置が要求される安全保障上重要な企業への情報共有体制の整備（平成２８年度末までに原子力規制庁等との調整を行い一定の結論を得て可能なものから実施するとともに、その後も継続的に見直しを行う。）

(b)　我が国の国際競争力強化にとっても重要な先端技術等の知的財産や営業秘密

11 各重要インフラ分野で整備されたセプターの代表で構成される協議会。

を保持する企業、研究機関、大学等への情報共有体制の整備（平成２８年度末までに一定の結論を得て、その後も継続的に見直しを行う。）

(c) 社会環境の変化等により新たに重要インフラと位置付けるべきものについての継続的な検討（必要に応じて重要インフラ分野の見直しを行うものとし、この際、新規の分野に対しては、必ずしも既存分野と同水準の対応を求めることが妥当でないこと等を考慮し、まずは情報提供体制の整備から始めることなど、当該分野の状況に合わせた取組を行うことを明確にする。）（平成２８年度末までに一定の結論を得て、その後も継続的に見直しを行う。）

(3) 多様な関係者（ステークホルダー）間の連携強化

刻々と変化する重要インフラを取り巻く技術環境や社会環境の変化に適切に対応するため、多様な関係者間の連携を強化する。

ア　国際連携

・海外ＩＳＡＣとの連携（共同演習、情報共有を含む。）に向けた取組の促進（継続実施）
・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し、我が国の取組を積極的に公表（平成２８年度以降、継続的に実施。）

ＩｏＴシステムの普及に伴い、国境を越えたサプライチェーン全体の情報セキュリティ向上の必要性が高まっている。また、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のため、キャパシティビルディング（能力向上）への積極的な寄与についても重要性を増している。こうした状況を踏まえ、社会経済システム全体の国際的な「面としての防護」の確保に向けて、国際連携を強化する。

(a) 各セプターやＩＳＡＣが自主的に行う内外連携（海外ＩＳＡＣ等との情報共有等）の強化に対する支援（継続実施）

(b) 分野横断的演習における内外連携の推進（継続実施）

(c) 欧米・ＡＳＥＡＮやＭｅｒｉｄｉａｎ[12]等の二国間・地域間・多国間の枠組みを活用した国際連携を継続し、我が国の取組を積極的に公表していくとともに、平成２８年度以後の国際会議等で得た事例、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（平成２８年度以降、継続的に実施。）

[12] 重要インフラ防護に係る情報共有を目的とした各国政府機関による国際会議

イ　人材育成

・人材育成強化方針に基づく重要インフラに係るセキュリティ人材の育成支援、官民人材交流、資格取得促進（平成２８年度以後継続実施）

重要インフラ事業者等がセキュリティ意識を持った企業経営を行うに当たっては、経営層に対してサイバーセキュリティに係る取組を経営戦略の一環として積極的に取り組むよう意識改革を促すとともに、経営層の示す経営方針を理解した上でサイバーセキュリティに係るビジョンの提示や実務者層との間のコミュニケーションの支援を行うことができる橋渡し人材層を育成し、経営層がセキュリティリスクの評価や経営資源に係る投資判断を適切に行うことができる体制を整備することが必要である。また、実務者層におけるサイバーセキュリティの知識の底上げを図っていくことも重要である。

こうした背景を踏まえ、産学官が連携した上で、人材育成の取組を推進する。

(a) 「サイバーセキュリティ人材育成総合強化方針」(平成２８年　月サイバーセキュリティ戦略本部決定）に基づく重要インフラ事業者等におけるセキュリティ人材の育成支援、官民人材交流、資格取得等の推進（平成２８年度以後継続実施）

４．行動計画の見直しに向けた今後の検討スケジュール

行動計画の見直しに向けては、平成２８年夏に行われる評価を踏まえ、秋頃に行動計画の見直し骨子（案）を策定する。次に本年中に行動計画の見直し（案）を策定・公表（パブリックコメント手続きの実施）し、平成２９年３月までに行動計画の見直しについての結論を得ることとする。

なお、行動計画の見直しに係る検討は、２０２０年東京オリンピック・パラリンピック競技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を取りつつ進めていくものとする。