資料１

重要インフラの情報セキュリティ対策に係る
第３次行動計画の進捗状況等

資料１－１　重要インフラにおける取組の進捗状況

※「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 V.3 に基づく 2015 年度の確認・検証に相当。

※「サイバーセキュリティ政策に係る年次報告（2015 年度）」の別添４－２に相当。

資料１－２　（参考）サイバーセキュリティ政策に係る年次報告（2015 年度）（案）（抜粋）

資料１－３　（参考）サイバーセキュリティ 2015（抜粋）

資料１－４　（参考）サイバーセキュリティ 2016（案）（抜粋）

（注）資料１－１、資料１－２及び資料１－４は資料非公開。
なお、資料１－２及び資料１－４の全体についてはサイバーセキュリティ戦略本部決定後に別途公表。

資料１－３

サイバーセキュリティ２０１５

2015 年９月 25 日

サイバーセキュリティ戦略本部

目　次

2.2. 重要インフラを守るための取組

(ア)内閣官房及び重要インフラ所管省庁等において、「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」に基づき、安全基準等の整備及び浸透、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、防護基盤の強化の５つの施策を実施する。また、本年度内を目途に、更なるセキュリティ強化等の具体的内容について取りまとめる。

(イ)内閣官房において、各重要インフラ分野における安全基準等について、強制基準やガイドライン等の体系を明らかにする調査を実施する。その調査結果を踏まえ、安全基準等の体系を明示した調査項目を加えた安全基準等の改善状況調査を実施し、課題の抽出を行う。

(ウ)総務省において、重要インフラにおけるサービスの持続的な提供に向け、重要無線通信妨害事案の発生時の対応強化のため、申告受付の夜間・休日の全国一元化を継続して実施するとともに、妨害原因の排除を迅速に実施する。また、重要無線通信への妨害を未然に防ぐための周知啓発を実施するほか、必要な電波監視施設の整備、電波監視技術に関する調査研究を実施する。

(エ)総務省において、ネットワークIP化の進展に対応して、ICTサービスのより安定的な提供を図るため、電気通信に関する事故の発生状況等の分析・評価等を行い、その結果を公表する。また、事故再発防止のため、「情報通信ネットワーク安全・信頼性基準」等の見直しの必要性について検討する。

(オ)情報共有体制その他の重要インフラ防護体制を実効性のあるものにするため、官民の枠を超えた関係者間での演習・訓練を次のとおり実施する。

- 内閣官房において、重要インフラ事業者等の障害対応能力の向上を図るため、重要インフラ分野や所管省庁等が横断的に参加する演習を実施する。
- 総務省において、重要インフラにおける標的型攻撃への対処能力を向上させ、重要インフラの持続的なサービス提供に向けた実践的な防御演習（CYDER）を実施する。
- 経済産業省において、CSSCを通じて、重要インフラ等企業における標的型攻撃に対する対応能力を向上させるため、模擬システムを活用した実践的なサイバー演習を実施する。

(1) 重要インフラ防護の範囲等の不断の見直し

(ア)内閣官房において、重要インフラ所管省庁等との連携の下、2020年の東京オリンピック・パラリンピック競技大会をテストケースとして、情報システムの障害が当該大会の開催に重大な影響を与えるサービス、それを提供する事業者及びその分野の候補を選定すると共に、所管省庁や事業者が行うリスク評価を支援するための手順を整備する。前記取組により得られた知見も活用し、新たな重要インフラ分野や事業者の候補を選定する。

(イ)内閣官房において、重要インフラ所管省庁の協力の下、第３次行動計画に基づく施策を、中小事業者へ拡大すると共に、取組を拡大する対象として、重要インフラ事業者等が提供するサービスに間接的に関わる外部委託先や主要関係先の洗い出しを行う。

(ウ)内閣官房において、重要インフラ分野以外の民間企業をサイバー攻撃から保護するために、既存の重要インフラ分野いかんに関わらず情報共有等の取組の対象とすべき企業の範囲について検討を行う。

(2) 効果的かつ迅速な情報共有の実現

(ア)内閣官房において、重要インフラ所管省庁の協力の下、サイバー攻撃に対するより効果的な情報を迅速に共有するための在り方を検討すると共に、小規模な障害情報や予兆情報（ヒヤリハット等）の情報共有について政府機関内での連携強化を図る。

(イ)経済産業省において、官民における最新の脅威情報やインシデント情報等の共有のため、IPAが情報ハブとなり実施している「サイバー情報共有イニシアティブ」（J-CSIP）について参加組織の拡大、共有情報の充実を行う。また、重要インフラ事業者等における信頼性・安全性向上の取組を支援するため、IPAを通じ、障害事例や提供情報の分析結果等を重要インフラ事業者等へ提供する。

(ウ)経済産業省において、JPCERT/CCを通じ、重要インフラ事業者等からの依頼に応じ、国際的なCSIRT間連携の枠組みも利用しながら、攻撃元の国に対する調整等の情報セキュリティインシデントへの対応支援や、攻撃手法の解析の支援を行う。また、重要インフラ事業者等において対策が必要となる可能性のある脅威情報及びその対策に関する情報を、事前の合意に基づき、早期警戒情報として、JPCERT/CCから重要インフラ事業者等へ提供する。

(エ)内閣官房において、情報セキュリティ関係機関と協力関係を構築・強化していくと共に、得られた情報を適切に重要インフラ事業者等に情報提供する。

(オ)総務省において、標的型攻撃に関する情報の収集・分析能力の向上に向け、官公庁・大企業のLAN環境を模擬した実証環境を用いて標的型攻撃の解析を実施する。また、サイバー攻撃に関する情報を収集・分析・共有するための基盤となるプラットフォームの整備・構築に向けた検討を行う。

(カ)警察庁において、サイバー攻撃を受けたコンピュータや不正プログラムの分析、関係省庁との情報共有等を通じて、サイバー攻撃事案の攻撃者や手口の実態解明に係る情報収集・分析を継続的に実施する。また、都道府県警察において、サイバー攻撃特別捜査隊を中心として、サイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査を推進するとともに、重要インフラ事業者等の意向を尊重し、以下の取組を実施することにより、緊急対処能力の向上を図る。

- 重要インフラ事業者等への個別訪問を行い、各事業者等の特性に応じた情報提供を行う。
- 事案発生を想定した共同対処訓練を実施する。
- サイバーテロ対策協議会を通じて、参加事業者間の情報共有を実施する。

(3) 各分野の個別事情への支援

(ア)内閣官房において、サイバーセキュリティ基本法等に基づいて、地方公共団体に対して情報の提供など、地方公共団体におけるサイバーセキュリティの確保のために必要とされる協力を行う。

(イ)内閣官房及び総務省において、総合行政ネットワーク（LGWAN）について集中的にセキュリティ監視を行う機能を設けるなどして、GSOCとの情報連携を通じた、国・地方全体を俯瞰した監視・検知体制を整備するとともに、地方公共団体のセキュリティ対策に関する支援の強化を図ること等により、マイナンバー制度を含めたセキュリティ確保を徹底する。また、情報提供ネットワークシステム等のマイナンバー関係システムについて、インターネットから独立する等の高いセキュリティ対策が講じられたものとなるよう、管理・監督・支援等を行

う。加えて、特定個人情報保護委員会において、関係省庁等と連携しつつ、特定個人情報の適正な取扱いに関するガイドラインの遵守、特定個人情報に係るセキュリティの確保を図るため、専門的・技術的知見を有する体制を立ち上げるとともに、監視・監督方針を速やかに策定するなど、本年度中を目途に、監視・監督体制を整備する。

(ウ)内閣官房において、マイナンバー制度の下で認証連携を行うに当たって、利便性の向上とセキュリティの確保がバランスの取れたものとなるよう、政府内及び官民での認証連携について、多要素認証等の認証方式や連携条件についての検討を行い、本年中を目途に取組方針を策定する。

(エ)内閣官房において、我が国で使用される制御系機器・システムに関する脆弱性情報やサイバー攻撃情報などの有益な情報について、非制御系の情報共有体制と整合性のとれた情報共有体制により、収集・分析・展開していく。また、経済産業省において、経済産業省告示に基づき、IPAとJPCERT/CCにより運用され、制御システムの脆弱性情報の届出も受け付ける「脆弱性関連情報届出受付制度」を運用する。

(オ)経済産業省において、重要インフラの制御系の情報セキュリティ対策のため、CSSCを通じて、セキュリティ対策に関する知見を収集し、それに基づいたセミナー及びより実践的な演習を実施する。

(カ)経済産業省において、CSSCが実施する制御機器のセキュリティ評価・認証の利用促進を図るとともに、制御システム全体のセキュリティに関する評価・認証制度の構築を行う。また、制御システムのセキュリティマネジメントシステム適合性評価スキームの普及について、JIPDEC等関係機関に対して支援を行う。さらに、CSSCの制御システムセキュリティテストベッド施設を利用した研究開発成果の展開を図り、その成果を用いて制御システムセキュリティに係る国際標準化の推進を図るとともに、それに基づいた国際的な相互承認制度の拡大を推進する。