資料４

# 重要インフラにおける取組の進捗状況等（年次報告）

## 資料４－１　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」に基づく 2016 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（2016 年度）」の別添４－２に相当。

## 資料４－２　（参考）サイバーセキュリティ政策に係る年次報告（2016年度）（案）（抜粋）

## 資料４－３　（参考）サイバーセキュリティ2016（抜粋）

## 資料４－４　（参考）サイバーセキュリティ2017パブコメ（案）（抜粋）

（注）資料４－１、資料４－２及び資料４－４は非公開。
なお、資料４－２及び資料４－４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4－3

# サイバーセキュリティ２０１６

2016 年８月 31 日

サイバーセキュリティ戦略本部

# 目　次

に関する条約を締結するための「情報処理の高度化等に対処するための刑法等の一部を改正する法律」（サイバー刑法）が施行されたことを踏まえ、その適正な運用を実施する。

(サ)警察庁及び総務省において、安全・安心なサイバー空間を構築するため、通信履歴等に関するログの保存の在り方については、「電気通信事業における個人情報保護に関するガイドライン」の解説を踏まえ、関係事業者における適切な取組を推進するなど必要な対応を行う。

## 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、「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」に従い検討を進め、行動計画の見直しについて2016年度内を目途に結論を得るとともに、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。

(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引き続き実施し、当該調査結果を踏まえ、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、継続的に課題の抽出を行う。

(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、NICTを通じ、重要インフラにおけるサイバー攻撃への対処能力を向上させるための実践的サイバー防御演習（CYDER）を実施する。
- 経済産業省において、重要インフラ等企業におけるサイバー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。
- 金融庁において、金融業界横断的なサイバーセキュリティ演習を実施する。

(カ)経済産業省において、我が国の重要インフラのサイバーセキュリティ対策を抜本的に強化するため、重要インフラのサイバー攻撃に対する防御力を確認し、事業者の意識を喚起するとともに、今後重要インフラ対策の中核を担う人材育成や技術開発を行う体制を強化する。

## (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、「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」に従い、重要インフラに係る防護範囲の見直しについて検討を進め、行動計画の見直しについて2016年度内を目途に結論を得るとともに、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。

## (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、「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」に従い、サイバー攻撃に対する体制強化のため、情報共有の強化について検討を進め、行動計画の見直しについて2016年度内を目途に結論を得るとともに、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。

(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等と協力関係を構築・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や保有するシステムに対するぜい弱性試験を実施する。
- 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。

(キ)経済産業省において、「クレジット取引セキュリティ対策協議会（官民の約40事業者等で構

成)」で策定された「実行計画」を踏まえ、2020年までに、カード情報を保有する事業者における情報漏えい防止対策の徹底やクレジット決済端末のIC対応化100％の実現を含めた不正使用被害の最小化を目指し、割賦販売法の見直しにより、加盟店を含めた関係事業者におけるセキュリティ対策を義務付ける等、クレジットカードを安全に利用できる環境整備を推進する。

### (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)総務省において、関係機関と協力の上、地方公共団体職員がICT-BCP策定の必要性と基本事項を理解・習得することを支援するため、ICT-BCP策定セミナーを実施する。また、情報セキュリティ対策について習得することを支援するため、情報セキュリティ監査セミナー、情報セキュリティマネジメントセミナーを集合研修で、その他情報セキュリティ関連研修をeラーニングで実施する。

(ウ)総務省において、関係機関と協力の上、情報セキュリティ対策の取組事例の収集、情報セキュリティ事故情報の収集・分析の充実を図り、総合行政ネットワーク（LGWAN）内のポータルサイトに、情報セキュリティに関する解説等を提供するなど、その運営を支援し、更なる利用を促進する。

(エ)総務省において、関係機関と協力の上、公開サーバやネットワーク機器等における脆弱性診断、Web感染型マルウェアによる改ざん検知を地方公共団体に対して実施する。また、地方公共団体における緊急時の対応について、訓練ツールを提供する等支援する。

(オ)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強化対策を推進するため、情報システムの強靭性の向上や、自治体情報セキュリティクラウドの構築について、フォローアップを行う等により、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、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拡充するとともに、監視・監督機能を強化する。

(カ)内閣府等の関係省庁において、本人確認の連携による官民のオンラインサービスのシームレスな連携について、2017年１月以降、順次、実施する。データやお知らせ情報をマイナポータルにおいて確認可能とするなど利用者が望むワンストップサービス、マイナンバーカード等の活用によるIDの入力を要しないオンラインサービスの検討などについては、データの重要性に応じた二経路又は二要素認証や、行政機関発行IDと民間発行IDとの連携による認証の導入などにより、重要情報の適正な管理のためのセキュリティ対策を講じつつ、進める。

(キ)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に係る制度を運用する。

(ク)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、それに基づいた実践的な演習を実施する。

(ケ)経済産業省において、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、制御システムのセキュリティに関する評価・認証制度の検討を行う。

(コ)経済産業省において、策定されたスマートメーターシステム及び電力制御システムに係るセキュリティガイドラインを電気事業法の保安規制に位置付ける。

## 2.3. 政府機関を守るための取組

(ア)内閣官房において、統一基準群の改定を行い、その改定による府省庁及び独立行政法人等の情報セキュリティポリシーの見直しについて、進捗状況を把握し、必要な支援を行う。また、新たに直面した脅威・課題への対応について、情報システムにおける対策の迅速・柔軟な見直しを推進する。

### (1) 攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進

(ア)内閣官房において、政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）により、政府機関情報システムのサイバー攻撃等に関する情報を24時間365日収集・分析し、政府機関等に対する新たなサイバー攻撃の傾向や情勢等について、分析結果を各政府機関等に対して適宜提供する。

(イ)内閣官房において、サイバー攻撃への対処に関する政府機関全体としての体制を強化するため、GSOC、CYMAT、各府省庁CSIRT等のインシデント対処に関わる要員による情報共有及び連携の促進に資するコミュニティを形成する。

(ウ)内閣官房において、政府機関におけるセキュリティ・バイ・デザインを推進するため、サプライチェーン・リスクへの対応を含むセキュリティ・バイ・デザインの観点から情報システムの調達仕様書に確実に記載すべき事項について、各府省庁の取組状況を調査する。また、見直しが必要となる事項については、統一基準群等に適切に反映されるよう検討を行う。

(エ)経済産業省において、政府調達等におけるセキュリティの確保に資するため、IPAを通じ、「IT製品の調達におけるセキュリティ要件リスト」の記載内容（製品分野、製品に対する脅威、脅威に対する要件としてのプロテクション・プロファイルなど）の見直しを行うとともに、政府機関の調達担当者等に対し、最新のプロテクション・プロファイル（翻訳版）を含む情報の提供や普及啓発を行う。

(オ)経済産業省において、IPAを通じ、JISEC（ITセキュリティ評価及び認証制度）の利用者の視点に立った評価・認証手続の改善、積極的な広報活動等を実施するとともに、政府調達を推進するため、調達関係者に対する勉強会やヒアリングを実施するとともに必要に応じて手順等の見直しを実施する。