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次行動計画の進捗状況等

資料２－１　重要インフラにおける取組の進捗状況
（年次報告(案) 第３章部分）

資料２－２　重要インフラにおける取組等
（年次報告(案) 別添４部分）

資料２－３　年次計画評価
（年次報告(案) 別添２部分の一部抜粋）

資料２－４　（参考）サイバーセキュリティ 2014(抄)

(注)資料２－１、資料２－２及び資料２－３は資料非公開。
なお、年次報告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２－４

サイバーセキュリティ２０１４

（抄）

２０１４年7月１０日

情報セキュリティ政策会議

目　次

② 重要インフラ事業者等における対策

【 安全基準等の整備及び浸透 】

(ア)「安全基準等の整備及び浸透」に関する内閣官房の施策 （内閣官房）

a) 2014 年度に指針の改定に係る検討を、他施策との連携を強化した上で実施し、これらの結果を公表する。

b) 必要に応じて社会動向の変化及び新たに得た知見に係る検討を、他施策との連携を強化した上で実施し、これらの結果を公表する。

c) 上記 a)・b)を通じて、各重要インフラ分野の安全基準等の継続的改善を支援する。

d) 重要インフラ所管省庁の協力を得つつ、各重要インフラ分野における安全基準等の継続的改善状況を把握するための調査を実施し、結果を公表する。

e) 重要インフラ所管省庁の協力を得つつ、安全基準等の浸透状況等の調査を実施し、結果を公表する。

(イ)「安全基準等の整備及び浸透」に関する重要インフラ所管省庁の施策 （重要インフラ所管省庁）

a) 指針として新たに位置付けることが可能な安全基準等に関する情報等を内閣官房に提供する。

b) 自らが安全基準等の策定主体である場合は、定期的に、安全基準等の分析・検証を実施することに加えて、必要に応じて、安全基準等の改定を実施する。

c) 重要インフラ分野ごとの安全基準等の分析・検証を支援する。

d) 重要インフラ事業者等に対して、対策を実装するための環境整備を含む安全基準等の浸透を実施する。

e) 内閣官房が実施する安全基準等の継続的改善状況の把握に協力する。

f) 内閣官房が実施する安全基準等の浸透状況等の調査に協力する。

【 情報共有体制の強化 】

(ウ)「情報共有体制の強化」に関する内閣官房の施策 （内閣官房）

a) 平時及び大規模 IT 障害対応時の情報共有体制の運営を通じた更なる促進及び必要に応じた見直しをする。

b) 重要インフラ事業者等に提供すべき情報の集約及び適時適切な情報提供をする。

c) 重要インフラ所管省庁の協力を得つつ、各セプターの機能、活動状況等を把握するための定期的な調査・ヒアリング等を実施する。

d) 先進的なセプターの機能や活動の紹介をする。

e) セプターカウンシルに参加するセプターと連携しつつ、セプターカウンシルの運営及び活動に対する支援を実施する。

f) セプターカウンシルの活動の強化及びノウハウの蓄積や共有のために必要な環境を整備する。

g) 必要に応じてサイバー空間関連事業者との連携を個別に構築し、IT 障害発生時に適時適切な情報提供を実施する。

(エ)「情報共有体制の強化」に関する重要インフラ所管省庁の施策 (重要インフラ所管省庁)

a) 内閣官房と連携しつつ、情報共有体制を運用する。

b) 重要インフラ事業者等との緊密な情報共有体制を維持する。

c) 重要インフラ事業者等からの IT 障害に係る報告の内閣官房への情報連絡をする。

d) 内閣官房が実施する各セプターの機能や活動状況を把握するための調査・ヒアリング等への協力をする。

e) セプターの機能充実への支援をする。

f) セプターカウンシルへの支援をする。

g) セプターカウンシル等からの要望があった場合、意見交換等を実施する。

(オ)「情報共有体制の強化」に関する情報セキュリティ関係省庁の施策 (情報セキュリティ関係省庁)

a) 内閣官房と連携しつつ、情報共有体制を運用する。

b) 攻撃手法及び復旧手法に関する情報等の収集及び内閣官房への情報連絡をする。

c) セプターカウンシル等からの要望があった場合、意見交換等を実施する。

(カ)「情報共有体制の強化」に関する事案対処省庁の施策 (事案対処省庁)

a) 内閣官房と連携しつつ、大規模 IT 障害対応時における情報共有体制を運用する。

b) 被災情報、テロ関連情報等の収集をする。

c) 内閣官房に対して、必要に応じ情報連絡を実施する。

d) セプターカウンシル等からの要望があった場合、意見交換等を実施する。

【 障害対応体制の強化 】

(キ)「障害対応体制の強化」に関する内閣官房の施策 (内閣官房)

a) 他省庁の IT 障害対応の演習・訓練の情報を把握し、連携の在り方を検討する。

b) 重要インフラ所管省庁の協力を得つつ、定期的及びセプターの求めに応じて、セプター

の情報疎通機能の確認（セプター訓練）等の機会を提供する。

c) 分野横断的演習のシナリオ、実施方法、検証課題等を企画し、分野横断的演習を実施する。

d) 分野横断的演習の改善策を検討する。

e) 分野横断的演習の機会を活用して、リスク分析の成果の検証並びに重要インフラ事業者等が任意に行う IT 障害発生時の早期復旧手順及び IT-BCP 等の検討の状況把握等を実施し、その成果を演習参加者等に提供する。

f) 分野横断的演習の実施方法等に関する知見の集約・蓄積・提供をする。

g) 分野横断的演習で得られた重要インフラ防護に関する知見の普及・展開をする。

(ク)「障害対応体制の強化」に関する重要インフラ所管省庁の施策 （重要インフラ所管省庁）

a) 内閣官房が情報疎通機能の確認（セプター訓練）等の機会を提供する場合の協力をする。

b) 分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力をする。

c) 分野横断的演習へ参加する。

d) セプター及び重要インフラ事業者等の分野横断的演習への参加を支援する。

e) 分野横断的演習の改善策検討への協力をする。

f) 必要に応じて、分野横断的演習成果を重要インフラ所管省庁の施策へ活用する。

g) 分野横断的演習と重要インフラ所管省庁が実施する重要インフラ防護に資する演習・訓練との相互の連携への協力をする。

(ケ)「障害対応体制の強化」に関する事案対処省庁の施策 （事案対処省庁）

重要インフラ事業者等からの要望があった場合、IT 障害対応能力を高めるための支援策を実施する。

【 リスクマネジメント 】

(コ)「リスクマネジメント」に関する内閣官房の施策 （内閣官房）

a) リスクマネジメントの標準的な考え方や定義等の利活用や国際標準等を読み替えた手引書等の提示による関係主体間の共通認識を醸成する。

b) 本施策における調査・分析による重要インフラ事業者等におけるリスクマネジメントを支援する。

c) 本施策における調査・分析の結果を安全基準等に反映する基礎資料として提供する。

d) セプターカウンシル及び分野横断的演習等を通じて重要インフラ事業者等のリスクコミュニケーション及び協議を支援する。

(サ)「リスクマネジメント」に関する重要インフラ所管省庁の施策 （重要インフラ所管省庁）

a) リスクマネジメントに関する調査・分析を必要とする対象に関する情報、あるいは、当該調査・分析に必要な情報を内閣官房に提供する。

b) リスクマネジメントに関する調査・分析を重要インフラ所管省庁の施策へ活用する。

c) 重要インフラ事業者等のリスクコミュニケーション及び協議を支援する。

【 防護基盤の強化 】

(シ)「防護基盤の強化」に関する内閣官房の施策 （内閣官房）

a) Web サイトやニュースレターを通じた広報を実施する。

b) 講演等を通じた公聴活動を実施する。

c) 二国間・地域間・多国間の枠組みの積極的な活用を通じた国際連携を強化する。

d) 国際連携で得た事例、ベストプラクティス等を国内の関係主体に積極的に提供する。

e) 重要インフラ防護に係る関係主体におけるナレッジベースの平準化を目的に、関係主体が共通に参照する関連文書を合本し、規程集を発行する。

f) 関連規格を整理、可視化する。

g) 国際基準等を重要インフラ防護に係る迅速かつ柔軟な対応の実現に際して適用可能とするため、必要に応じて、手引書等を整備する。

h) 制御系機器・システムの第三者認証制度の拡充を支援する。

(ス)「防護基盤の強化」に関する重要インフラ所管省庁の施策 （重要インフラ所管省庁）

a) 内閣官房と連携して、二国間・地域間・多国間の枠組みの積極的な活用を通じた国際連携を強化する。

b) 内閣官房と連携して、国際連携にて得た事例、ベストプラクティス等を国内の関係主体に積極的に提供する。

c) 内閣官房と協力し、関連規格を整理、可視化する。

d) 国際基準等を重要インフラ防護に係る迅速かつ柔軟な対応の実現に際して適用可能とするため、内閣官房と協力し、必要に応じて、手引書等を整備する。

e) 内閣官房と協力し、制御系機器・システムの第三者認証制度の拡充を支援する。

【 その他の施策 】

(セ)大規模サイバー攻撃事態等発生時の初動対処に係る訓練の実施等 （内閣官房及び関係府省庁）※再掲

内閣官房において、関係府省庁と協力し、大規模サイバー攻撃事態等の発生を想定した関係者による対処訓練を実施し、当該結果を踏まえた検討を行うこと等により、大規模サイバー攻撃事態等が発生した際に、「緊急事態に対する政府の初動対処体制について」、「大規模サイバー攻撃事態等への初動対処について」等に基づき官民が連携して的確な対応を行うことができる態勢を整備する。また、上記訓練は 2015 年度以降も継続して実施する。

(ソ) 情報通信分野における事業者との官民連携の推進　(総務省)

総務省において、情報セキュリティ上の事案について、ISP 事業者団体の「テレコム・アイザック推進会議」をはじめとした関係団体等と情報共有を推進する。

(タ) 個別分野におけるサイバー演習　(総務省及び経済産業省)

a) 総務省において、巧妙化・複雑化するサイバー攻撃に対応するため、情報通信分野の事業者によるサイバー攻撃対応演習の実施を支援し、事業者間連携等を促進する。

b) 経済産業省において、CSSC を通じて、重要インフラの制御系の情報セキュリティ対策のため、今後、実際にサイバー攻撃が発生することを前提としたサイバー演習又はセミナーを実施し、制御システムのセキュリティ評価及びセキュリティ対策に関する知見を蓄積し、我が国の制御システムのセキュリティ対策に繋げる。

(チ) 電気通信システムの安全・信頼性確保　(総務省)

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、適宜「情報通信ネットワーク安全・信頼性基準[11]」等を見直す。

(ツ) 重要無線通信妨害対策の強化　(総務省)

a) 総務省において、重要無線通信妨害事案の発生時の対応強化のため、重要無線通信妨害申告受付の夜間・休日の全国一元化を継続して実施するとともに、夜間・休日における迅速な出動体制を強化する。

b) 総務省において、電波利用秩序維持のため、遠隔操作による電波監視施設等の性能向上を図りつつ、同施設のセンサーを更改する。

c) 総務省において、電波監視施設の高度化・高機能化等、昨今の電波利用環境の変化を踏まえ、電波監視技術に関する調査研究を実施する。

(テ) 「サイバー情報共有イニシアティブ」の強化　(経済産業省)

経済産業省において、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、２年間の活動成果を踏まえ、より有効な活動に発展させるよう、産

[11] 昭和 62 年郵政省告示第 73 号。

業分野と参加メンバーを拡大させるとともに、共有情報の充実等を図るとともに、引き続きセプターとの情報共有等を推進する。

また、同じく IPA で実施している「標的型サイバー攻撃の特別相談窓口」により得られた標的型攻撃の解析情報等と合わせて、「サイバー攻撃解析協議会」等での高度解析に繋げる。

(ト)サイバー攻撃（インシデント）対応調整支援　（経済産業省）

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。

(ナ)重要インフラで利用される情報システムのセキュリティ・信頼性向上のための支援体制の整備　（経済産業省）

a) 経済産業省において、重要インフラ事業者の情報処理システム等の信頼性・安全性向上のための自発的な取組を支援するため、IPA を通じ、障害事例集の整備・共有や、自発的に提供のあった情報のマクロ的な定量分析・解析、蓄積された情報のセプター等への提供を行う。

b) 経済産業省において、CSSC を通じ、必要に応じ現在策定中の制御システムのセキュリティに係る国際標準について、我が国としての要求事項等について寄書を行う。また、制御システムのセキュリティに係る評価・認証に関して国際的な連携の実施や、既存企画の翻訳等に着手し、国内製品の認証取得を容易化するための検討を行い、結論を得る。

(ニ)重要インフラ事業者に対するソフトウェアや制御システム等の脆弱性関連情報の優先提供及び情報セキュリティ関連情報マネジメントの支援等　（経済産業省）

a) 経済産業省において、IPA 及び JPCERT/CC を通じ、制御システム関係者による計画的な対応及び安全な対策の実施を可能とするよう前年度に行った脆弱性ハンドリング体制の見直し結果を踏まえて、当該体制を運用する。

b) 経済産業省において、重要インフラ事業者において対策が必要となる可能性のある情報セキュリティ上の脅威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 からセプター又は重要インフラ事業者その他の国民の社会活動に大きな影響を与えるインフラ、サービス及びプロダクトなどを提供している組織等に提供する。

c) 経済産業省において、IPA、JPCERT/CC を通じ、ソフトウェア等の脆弱性に関する情報の利活用し易い形式での発信を進める。

(ヌ)制御システムに関するインシデントや脆弱性への対応のための連携体制の構築　（経済産業省）

経済産業省において、2012 年 7 月に起ち上げた JPCERT/CC の制御システムセキュリティ対策グループ（ICSR）を通じ、制御システム関連団体とともに、制御システムにおけるセキュリティ対策の推進に資する情報の収集、共有、発信を推進することにより、制御システムに関するインシデントや脆弱性等の脅威への対応の円滑化を図る。

(ネ)制御システムにおける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確立支援 （経済産業省）

経済産業省において、IPA の推進する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について、2014 年度の確立に向けて、JIPDEC 等関係組織に対して支援を行う。

(ノ)制御機器等の評価・認証スキームの確立支援 （経済産業省）

経済産業省において、CSSC の推進する制御機器等の評価・認証について、2015 年度の評価・認証機関の確立に向けて、CSSC の取組を支援する。

(ハ)制御システムセキュリティの国際標準に基づく評価・認証機関設立 （経済産業省）

経済産業省において、日本国内で制御システム等のセキュリティ評価・認証が行えるよう、パイロット認証等の実施を経て体制を確立し、CSSC を中心とした制御システムのセキュリティに関する評価・認証機関の設立を目指す。

(ヒ)制御システムセキュリティ評価・認証の国際相互承認 （経済産業省）

経済産業省において、CSSC の制御セキュリティ検証施設を利用して研究開発成果の展開を図り、制御システムセキュリティに係る国際標準化の推進とそれをベースにした国際的な相互承認の対象制度の拡大を推進する。

(フ)制御システムセキュリティ評価・認証の利活用に向けた検討 （経済産業省）

経済産業省において、CSSC による制御システムのセキュリティに関する評価・認証を受けたシステムの導入を推進するための制度整備を進める。

(ヘ)ソフトウェア、情報システムの信頼性向上 （経済産業省）

経済産業省において、重要インフラ分野の情報システムに係るソフトウェア障害情報の収集・分析及び対策や利用者視点でのソフトウェア信頼性の見える化の促進を図る。

(ホ)社会的に重要な情報システムについての情報セキュリティ強化 （経済産業省）

経済産業省において、重要インフラ分野や制御システム等の社会的に重要な情報システムについて、関係省庁等の求めに応じて、IPA を通じ、情報セキュリティ強化のための調査、協力を行う。

(マ)我が国の重大なセキュリティ事案に対する対応支援 （経済産業省）

経済産業省において、IPA を通じ、我が国経済社会に被害をもたらすおそれが強く、一組織

で対処が困難なサイバー攻撃を受けた組織等を支援するため、被害状況を把握し、再発防止に係る対処方針の策定支援を行う。