参考資料２

サイバーセキュリティ2013

平成25年6月27日

情報セキュリティ政策会議

目 次

I　はじめに

情報セキュリティ問題への取組を抜本的に強化することを目的に、2005 年 4 月に内閣官房に情報セキュリティセンター（NISC）が、同年 5 月に高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）に情報セキュリティ政策会議がそれぞれ設置されて以来、8 年が経過した。

この間、情報セキュリティ政策会議は、「第1次情報セキュリティ基本計画」、「第2次情報セキュリティ基本計画」及び「国民を守る情報セキュリティ戦略」を決定し、情報の自由な流通の確保と的確なリスク対応のバランスに配意しつつ、我が国における情報セキュリティ水準の向上を図ってきたところである。

一方、近年、政府機関や企業の機密情報を狙った執拗な標的型攻撃、国民生活や社会経済活動に直結する重要インフラ制御システムの障害をもたらす攻撃、急速に普及したスマートフォン等を介した大規模な個人に関する情報の窃取など高度かつ悪質なサイバー攻撃が国内外で現実のものとなり、海外主要国においてはサイバーセキュリティに関する国家戦略の策定・公表が相次いでいる。

我が国においても、サイバー空間と実空間の融合・一体化とともに、サイバー空間を取り巻くリスクの深刻化が一段と加速しているなか、引き続き国家の安全保障・危機管理、国際的な競争力の維持・強化、国民の安全・安心の確保のためには、これまでとは次元を変えた取組が必要となっている。

以上の認識のもと、平成 25 年 6 月 10 日、情報セキュリティ政策会議において、我が国の情報セキュリティ政策に関する新たな国家戦略となる「サイバーセキュリティ戦略」をとりまとめたところである。本書は同戦略に基づく最初の年次計画であり、世界を率先する強靱で活力あるサイバー空間を構築し、「サイバーセキュリティ立国」の実現に向け、2013 年度及び 2014 年度に実施する具体的な取組の重点について、同戦略記載の体系に沿ってその詳細を示すものである。

Ⅱ　具体的な取組

以下に挙げる具体的施策を着実に実施するものとする。実施時期が特に示されていない施策については、2013 年度中に実施するものである。

なお、複数の項目に関する施策については、同項目において再掲している。

１「強靱な」サイバー空間の構築

サイバー空間の持続性を確保するため、サイバー攻撃への対応を増強するとともに、脆弱性への対処、サイバー攻撃に関するインシデントの認知・解析やインシデント等関連情報の共有等の機能を高めること等により、「強靱な」サイバー空間を構築し、サイバー攻撃等に対する防御力・回復力の強化を目指す。

① 政府機関等における対策

１） 情報及び情報システムに係る情報セキュリティ水準の一層の向上

【 情報の重要度等に応じた政府機関における統一的な仕組みの強化 】

（ア） 業務で扱う情報の機密性の要求度等に応じた対策の重点実施のための枠組みの構築 （内閣官房及び関係府省庁）

a)　内閣官房において、各府省庁のCISO[1]がガバナンス機能を発揮し、機微な取扱いが必要な情報を扱う業務等を特定してリスク評価を行い、限られた人員・予算の中で外部の脅威（標的型攻撃等）から重要な情報資産を守るために必要な情報セキュリティ対策を計画的・重点的に実施するための枠組みを構築する。

b)　内閣官房において、標的型攻撃等の脅威の顕在化や、スマートフォン及びクラウドコンピューティング技術の普及等、新たな技術や環境の変化に対応して、各府省庁が達成目標や実施計画を策定し、PDCA サイクルの適正性やガバナンス機能の有効性を確認するための枠組みの構築等に係る政府機関統一基準群[2]の見直しを行う。

---

[1] Chief Information Security Officer の略。

[2] 「政府機関の情報セキュリティ対策のための統一規範」（2011 年 4 月 21 日情報セキュ

（イ） 政府情報システム管理データベースの利活用 （内閣官房、総務省及び関係府省庁）

a） 内閣官房において、各府省庁の情報システムを管理するために情報資産台帳をデータベース化した「政府情報システム管理データベース」を用いて政府全体を通じたリスク管理、脆弱性の検出等への利活用方法を検討する。

b） 総務省において、同データベースを引き続き維持・管理する。

（ウ） 「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」の推進 （内閣官房及び関係府省庁）

「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」[3]の対象となるオンライン手続を所掌する各府省庁において、同ガイドラインに基づき導出したリスク評価及び保証レベルの総合的な妥当性を確保するため、最高情報セキュリティアドバイザー等連絡会議等の場において、専門的知見を有する者からの助言等を受け、決定するとともに、業務・システム最適化に係るものは、計画への反映状況について、各府省情報化統括責任者（CIO[4]）連絡会議[5]等に報告する。

（エ） 特別管理秘密を取り扱うシステムに係る情報セキュリティ対策 （内閣官房及び関係府省庁）

内閣官房において、関係府省庁と協力し、「カウンターインテリジェンス[6]機能の強化に関する基本方針」に基づく特別管理秘密に係る基準を踏まえた対策の実施状況の重層的なチェックを着実に推進する。

（オ） 特に機密性の高い情報を取り扱う政府機関の情報保全システムの強化に向

リティ政策会議決定、2012 年 4 月 26 日改定）及び「政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針」（2005 年 9 月 15 日同会議決定、2012 年 4 月 26 日改定等）など。

[3] 2010 年 8 月 31 日各府省情報化統括責任者（CIO）連絡会議決定。

[4] Chief Information Officer の略。

[5] 政府全体として情報化推進体制を確立し、行政の情報化等を一層推進することにより国民の利便性の向上を図るとともに、行政運営の簡素化、効率化、信頼性及び透明性の向上に資するため、2002 年 9 月、高度情報通信ネットワーク社会推進戦略本部に設置された会議。

[6] 外国の敵意ある情報活動に対する情報防衛活動。

けた取組の推進（内閣官房及び関係府省庁）

内閣官房において、関係府省庁と協力し、「特に機密性の高い情報を取り扱う政府機関の情報保全システムに関し必要と考えられる措置について」（2011 年7月１日情報保全システムに関する有識者会議[7]）等を踏まえた取組を着実に推進する。

【 多様化する就労形態等への対応の強化 】

（カ） 政府機関におけるスマートフォン等の情報セキュリティ対策の強化（内閣官房）

内閣官房において、政府機関において私物のスマートフォン等を外出先やテレワーク等で業務利用する際の情報セキュリティ対策の手順書を作成するとともに、同手順書を踏まえ、政府機関統一基準群の適切な見直しを行う。

（キ） 重要な情報の提供における SNS の利用への対応 （内閣官房）

内閣官房において、各府省庁に対し、政府機関におけるソーシャルメディアの利用におけるなりすましやアカウント乗っ取りの防止等の情報セキュリティ対策について周知を図る。

（ク） 可搬記憶媒体（USB メモリ等）の情報セキュリティ対策の強化 （内閣官房及び全府省庁）

内閣官房において、関係府省庁と協力し、インターネット等外部との接続を持たないクローズなシステムに対するUSBメモリを介在した攻撃等に対処するため、セキュアUSBの導入を含めた可搬記憶媒体の利用に係る情報セキュリティ対策について検討を行い、全府省庁共通の運用指針を策定する。

（ケ） 複合機等のセキュリティ対策の強化 （内閣官房及び全府省庁）

内閣官房において、関係府省庁と協力し、ネットワーク機能をもつ複合機等に求められる情報セキュリティ対策について検討を行い、各府省庁で保有している複合機の情報セキュリティ機能の検査を実施する。

---

[7] 「政府における情報保全に関する検討委員会」（委員長：内閣官房長官）の下で開催される有識者会議。

【 政府横断的な情報システムの対策強化等 】

(コ) 政府機関におけるクラウドコンピューティングの情報セキュリティ対策の強化（内閣官房及び総務省）

a) 総務省において、クラウドコンピューティング技術を活用した「政府共通プラットフォーム」について、安全性・信頼性を確保するための、設計・構築段階で第三者による情報セキュリティ監査を行った上で、運用を開始した（2013 年3月）。今後、同プラットフォームの円滑な運用を行うとともに、高度化する情報セキュリティ上の脅威に的確な対応を実施する。

b) 内閣官房において、同プラットフォームにおける情報セキュリティ対策について、政府機関統一基準群の改定その他の関連施策により蓄積された専門的知見を提供するなどの支援を実施する。

(サ) 複数の府省庁で共通的に使用する政府情報システム基盤の運用管理に関する体制等の整備（内閣官房、総務省及び関係府省庁）

a) 総務省及び各府省庁において、「政府共通プラットフォーム」及び同プラットフォームへの統合・集約化対象システムについて、各府省庁の責任と役割分担、平常時及び非常時の協力・連携体制、非常時における具体的な対応策等を定めた運用管理基本規程等の規程類に基づき、適切に運用管理を行う。

b) 内閣官房において、同規程類を踏まえ、政府統一基準群の適切な見直しを行う。

(シ) 情報システムの共同利用や統合管理によるセキュリティ対策の強化に向けた取組（内閣官房）

内閣官房において、メールの検疫や安全な添付ファイルの処理等を共同サーバで集中管理（クラウド化）したり、複数の情報システム（サーバ・端末・ネットワーク機器等）のログを総合的に分析する等、情報システムの共同利用や統合管理による情報セキュリティ対策の強化について検討し、結論を得る。

(ス) 政府機関の情報システムの効率的・継続的なセキュリティ向上（内閣官房、総務省及び全府省庁）

a)　各府省庁において、「各政府機関の公開ウェブサーバ及び電子メールサーバの集約化計画の策定について」[8]に基づき、保有する公開ウェブサーバ及びメールサーバの集約化を着実に実施する。

b)　内閣官房において、各府省庁のサーバ集約化計画の実施結果を取りまとめ、情報セキュリティ政策会議等に報告を行う。

（セ）　社会保障・税番号制度に対応した情報セキュリティ対策　（内閣官房及び関係府省庁）

内閣官房及び関係府省庁において、関係機関が管理・運用する情報提供ネットワークシステム等の構築にあたって、適切な個人情報保護及び情報セキュリティの確保を図る。具体的には、①個人情報を一元管理せず分散管理、②情報提供ネットワークシステムを用いた情報連携において個人番号ではなく符号を利用、③アクセス制御によりシステム内の特定個人情報にアクセスできる人を制限、④通信を暗号化、などの対策を講じる。

（ソ）　オープンデータ推進における情報セキュリティの確保　（内閣官房及び関係府省庁）

内閣官房及び関係府省庁において、機械判読に適したデータ形式での公開やデータカタログの整備など電子行政オープンデータに関する具体的な取組を推進するに当たり、十分な情報セキュリティの確保を図る。

【　情報システムにおけるサプライチェーン・リスク等への対応強化　】

（タ）　情報システムに企画・設計段階から情報セキュリティ対策が適切に組み込まれるための方策　（内閣官房、総務省及び全府省庁）

a)　各府省庁において、システム予算全体の中で必要な情報セキュリティ対策を確保できるよう、あらかじめ可能な限りの想定を行い、それぞれの情報システムに係る調達仕様書の作成において、必要なセキュリティ対策を確実に記載するため、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」[9]を活用する。

---

[8] 2010 年 5 月 11 日情報セキュリティ政策会議報告。

[9] 2011 年 3 月 30 日情報セキュリティを企画・設計段階から確保するための方策に係る

b)　内閣官房において、同マニュアルが情報システムに係る政府調達の一環として広く活用されるよう、積極的に本マニュアルの利便性・簡便性の向上、内容の高度化や、各府省庁における普及・利用促進などの取組を行う。また、実際の調達仕様書にどのように活用されるかを確認すると共に、実際の利用にあたっての利用者からの問合せ対応や、作業支援などを実施する。

c)　各府省庁において、同マニュアルの活用又はそれと同等以上の対策を実施し、その結果を検証して内閣官房に報告する。

（チ） 安全性・信頼性の高い IT 製品等の利用推進（経済産業省及び全府省庁）

a)　各府省庁において、安全性・信頼性の高い情報システムを構築するため、IT 製品等を調達する際には、政府機関統一基準群に基づき、「IT セキュリティ評価及び認証制度等に基づく認証取得製品分野リスト」[10]を参照しつつ、「IT セキュリティ評価及び認証制度」[11]（以下「JISEC」[12]という。）により認証された製品等を取り扱う。

b)　経済産業省において、各府省庁が情報セキュリティに配慮した IT システムの調達を実効的かつ効率的に行えるようにするため、独立行政法人情報処理推進機構（以下「IPA」[13]という。）が運営する JISEC 認証製品の活用推進のための検討を行い、本リストの改善を図るなど、政府機関等における活用を促進する。

（ツ） 政府調達における情報セキュリティの確保（内閣官房及び経済産業省）

a)　経済産業省において、政府調達等における情報セキュリティの確保に資するため、IPA を通じ、政府及び地方公共団体の調達担当者等に対して、政府機関統一基準群を遵守するように、調達する機器等のセキュリティ要件及びその要件を満たす認証取得製品等の情報提供や普及啓発を行う。

b)　経済産業省において、IPA を通じ、「IT セキュリティ評価及び認証制度等

検討会。

[10] 2011 年 4 月 21 日経済産業省。

[11] IT 製品・システムについて、そのセキュリティ機能や目標とするセキュリティ保証レベルを、情報セキュリティの国際標準 ISO/IEC 15408 に基づいて第三者が評価し、結果を公的に検証し、原則公開する制度。

[12] Japan Information Technology Security Evaluation and Certification Scheme の略。

[13] Information-technology Promotion Agency の略。

に基づく認証取得製品分野リスト」[14]の適切な製品分野の検討協力及び最新のプロテクション・プロファイル（PP）等の情報提供を行う。

c)　経済産業省において、IPA を通じ、JISEC 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し、統一管理基準への活用の検討を行い、結論を得る。

d)　内閣官房及び経済産業省において、政府における IT 製品利用に係る既知脆弱性への未対応、危殆化された技術の利用、サプライチェーン・リスク、安全保障上のリスク等のリスクに対応した、政府調達に関する協定と整合的なIT 調達について検討を進め、特にCommon Criteria（ISO/IEC15408)など国際規格に基づく適合性評価の活用については、検討の上、結論を得るべく取り組む。

（テ） 政府調達の在り方の検討 （内閣官房）

内閣官房において、新興企業を含む我が国サイバーセキュリティ産業の能力の活用等を通じて、サイバーセキュリティの確保に実質的に有効な製品、システム等の調達を図るべく、応札事業者の技術力評価の在り方など政府による調達の在り方について検討を行い、結論を得る。

（ト） 情報システムの設計等の段階における情報セキュリティの技術基準の整備等（内閣官房及び全府省庁）

内閣官房において、政府機関の情報システムについて、特に標的型攻撃から重要な業務や情報を守る観点で情報システムの設計、構築、運用等の段階について満たすべき情報セキュリティの技術基準を検討、整備し、各府省庁は、情報システムの設計、構築、運用等の段階において、同基準を活用する。

（ナ） 運用・管理を委託している情報システムの情報セキュリティ対策の強化（内閣官房及び全府省庁）

各府省庁において、政府機関統一基準群及び当該個別マニュアル等を踏まえ、クラウドコンピューティングを活用するなどして政府機関外の組織に運用・管理を委託している情報システムについて、情報セキュリティを確保するための取

[14] 2011 年 4 月 21 日経済産業省。

組を推進する。

【 安全な暗号利用の推進 】

（ニ） 政府機関における安全な暗号利用の推進（内閣官房、総務省、経済産業省及び全府省庁）

a) 総務省及び経済産業省において、CRYPTREC[15]暗号リストに掲載された暗号技術の監視、安全性及び信頼性の確保のための調査、研究、基準の作成等を行う。

b) 総務省及び経済産業省において、独立行政法人情報通信研究機構（以下「NICT」[16]という。）及びIPAを通じ、暗号技術の安全性に係る監視及び評価、新世代暗号に係る調査、暗号技術の安全な利用方法に関する調査、暗号の普及促進、セキュリティ産業の競争力強化に係る検討、暗号政策の中長期的視点からの取組の検討を実施するため、暗号技術評価委員会及び暗号技術活用委員会を開催する。

c) 総務省及び経済産業省において、必要に応じて、CRYPTREC 暗号リストに掲載された暗号技術の監視により得られた情報を内閣官房に提供し、内閣官房は、必要な情報を速やかに各府省庁に提供する。また、「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及びRSA1024 に係る移行指針」[17]に従った取組を推進する。

d) 各府省庁において、同移行指針に基づき、それぞれで保有する情報システムについてより安全な暗号アルゴリズムへの対応及び移行を着実に実施する。

e) 内閣官房において、各府省庁における同移行指針への対応状況を把握して、新たな暗号アルゴリズムへの移行開始時期までに、各情報システムが同移行指針の規定する要件に適合させるよう促す。

（ヌ） 安全性・信頼性の高い暗号モジュールの利用推進（内閣官房、経済産業省及び全府省庁）

---

[15] Cryptography Research and Evaluation Committees の略。
[16] National Institute of Information and Communications Technology の略。
[17] 2008 年 4 月 22 日 情報セキュリティ政策会議決定。

a)　内閣官房及び経済産業省において、安全性の高い暗号モジュールを利用するため、IPA の運用する暗号モジュール試験及び認証制度を推進する。

b)　各府省庁において、暗号モジュールを調達する際には、必要に応じて、同制度により認証された製品等を取り扱う。

【 電子メールに係るなりすまし防止等の対応強化 】

（ネ） 政府機関から発信する電子メールに係るなりすましの防止 （内閣官房、総務省及び全府省庁）

a)　内閣官房及び全府省庁において、悪意の第三者が政府機関又は政府機関の職員になりすまし、一般国民や民間企業等に害を及ぼすことが無いよう、送信者側及び受信側における送信ドメイン認証技術の採用を推進するとともに、受信側対策の一層の推進を図る。また、DKIM[18]や S/MIME[19]のように暗号技術を利用した対策の導入を推進する。

b)　総務省において、迷惑メール対策に関わる関係者が幅広く参加し設立された「迷惑メール対策推進協議会」[20]や、国内の主要インターネット接続サービス事業者や携帯電話事業者が中心となって設立された民間団体である「JEAG」[21]等と連携して、送信側及び受信側における送信ドメイン認証技術（SPF[22]、DKIM 等）等の導入を促進する。

（ノ） 政府機関のドメイン名であることが保証されるドメイン名の使用の推進 （内閣官房、総務省及び全府省庁）

a)　内閣官房及び総務省において、政府機関が国民に対して情報の発信を行う際に利用するドメイン名については、原則として政府機関であることが保証されるドメイン名（属性型 JP ドメイン名のうち「.GO.JP」ドメイン名）を利用する

---

[18] Domain Keys Identified Mail の略。
[19] Secure / Multipurpose Internet Mail Extensions の略。
[20] 電気通信事業者、送信事業者、広告事業者、配信 ASP 事業者、セキュリティベンダー、各関係団体、消費者、学識経験者、関係省庁など迷惑メール対策に関わる関係者が幅広く集まり、関係者間の緊密な連絡を確保し、最新の情報共有、対応方策の検討、対外的な情報提供などにより、関係者による効果的な迷惑メール対策の推進に資することを目的に 2008 年 11 月 27 日に設立された協議会。
[21] Japan Email Anti-Abuse Group の略。
[22] Sender Policy Framework の略。

よう各府省庁に対して促す。

b)　各府省庁において、政府機関であることが保証されるドメイン名の利用を推進する。

（ハ） 政府認証基盤を活用した電子署名の利用等の推進（内閣官房及び全府省庁）

内閣官房において、関係府省庁と協力し、政府認証基盤（GPKI[23]）を活用した電子署名の利用等により、政府機関において公開しているウェブサイト上の電子ファイルの正当性・安全性を担保するための取組を実施する。

【 国の重要な情報を取り扱う企業等における対策の強化 】

（ヒ） 国の重要な情報を扱う企業等の情報セキュリティ対策の推進（内閣官房及び全府省庁）

a)　各府省庁において、国の安全に関する重要な情報を扱う契約を締結する際には、「調達におけるセキュリティ要件の記載について」[24]を踏まえ、情報セキュリティ要件を定め、これを遵守するよう、契約の相手方に求める。

b)　内閣官房において、各府省庁と協力し、重要インフラ分野等における取組を参考にしつつ、国の安全に関する重要な情報を扱う企業等によるサイバー攻撃に関するインシデント情報の発注元省庁等への報告及び事業者間の情報共有を推進するとともに、政府機関におけるリスク評価手法の運用にも活用できる枠組みを 2014 年度中に構築するため、その在り方について検討し、結論を得る。

【 独立行政法人、地方公共団体等における対策の強化 】

（フ） 独立行政法人等における情報セキュリティ対策の推進（内閣官房、独立行政法人等所管府省庁及び関係府省庁）

a)　関係府省庁において、所管する独立行政法人等に対して、政府機関統一基準群を含む政府機関における一連の対策を踏まえ、情報セキュリティポリ

[23] Government Public Key Infrastructure の略。
[24] 2012 年 1 月内閣官房副長官通知。

シーの策定・見直しを要請するとともに、必要な支援等を行う。

b)　関係府省庁において、独立行政法人等の業務特性及び対策の実施状況に応じて、自らの情報セキュリティ対策に係る PDCA サイクルを構築するための取組を推進するとともに、中期目標に情報セキュリティ対策に係る事項を明記することを推進する。

c)　関係府省庁において、独立行政法人から発信する電子メールについて、悪意の第三者が独立行政法人又は独立行政法人の職員になりすまし、一般国民や民間企業等に害を及ぼすことが無いよう送信側及び受信側における SPF、DKIM 等の送信ドメイン認証技術の採用等を推進する。

d)　内閣官房において、各府省庁と協力し、独立行政法人や特殊法人等の国と密接な関係のある法人によるサイバー攻撃に関するインシデント情報の法人所管府省庁への報告、法人の自主的判断に基づく事案対処省庁への通報及び関係機関との情報共有等を推進するための枠組みを 2014 年度中に構築するため、その方策について検討し、結論を得る。

（へ） 地方公共団体の情報セキュリティ対策水準向上のための普及・啓発 （総務省）

a)　総務省において、地方公共団体職員が業務継続性の重要度を理解し、地方公共団体の ICT 部門における BCP[25]策定の必要性と基本事項を習得することを支援するため、BCP アドバイザーの紹介を行う。また、BCP 策定セミナー、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、入門 ISMS[26]概論コースをｅラーニングで開催し、情報セキュリティ対策について習得する。

b)　総務省において、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。

c)　総務省において、Web サーバ等公開サーバやネットワーク機器等における脆弱性診断を希望する団体に対して実施する。また、脆弱性対策の知識向上を目的に実技形式の講習会等を全国2カ所で開催する。

d)　総務省において、閲覧しただけで感染する Web 感染型マルウェアによる

[25] Business Continuity Plan の略。
[26] Information Security Management System の略。

改ざん検知を希望する地方公共団体に対して実施する。関連のセミナーを全国 5 カ所で開催する。また、標的型攻撃の検知についても希望する団体に対して実施し、防御を支援する。

e) 総務省において、地方公共団体における SPF 等の送信ドメイン認証技術の採用を推進するため、地方公共団体における送信ドメイン認証技術の導入状況を調査するとともに導入の効果・有用性についてセミナーで解説するなど、普及・啓発を推進する。

f) 総務省において、全地方公共団体の職員を対象としたｅラーニングによる情報セキュリティ関連研修を実施する。

g) 総務省において、IPv4とIPv6が共存するネットワーク環境におけるセキュリティ課題の対応方策を確立するための実証実験を実施し、その成果をガイドライン等の形で広く展開する。

2） サイバー攻撃への対処態勢の充実・強化

【 GSOC の抜本的強化 】

（ア） 政府機関情報セキュリティ横断監視・即応調整チーム（GSOC[27]）の運用による緊急対応能力の向上 （内閣官房及び全府省庁）

a) 内閣官房において、全府省庁と協力し、2008 年度に本格運用を開始し、政府機関情報システムの 24 時間監視を行っている GSOC で収集・分析したサイバー攻撃等に関する情報について、速やかに情報共有を進めるとともに、関係機関との連携を通じて、政府全体として緊急対応能力の向上を図る。

b) 内閣官房において、全府省庁と協力し、訓練等を通じて緊急時の連絡体制を確認し、実効性を確保する。

c) 内閣官房において、政府情報システムの集約化の進捗状況を踏まえ、GSOC の監視対象先を拡大するための方策を検討し、着手可能な組織から監視対象の拡大を実施するとともに、監視対象先におけるサイバー攻撃等のインシデント情報の効果的な収集及び高度な解析を行うための技術の採用や人員の配置等について検討し、結論を得る。また、監視対象先からのインシデント情報の収集機能及び高度な解析機能については、2015 年度を目途とする「サイバーセキュリティセンター」（仮称）への改組と合わせて強化するための方策について検討し、結論を得る。

d) 内閣官房において、GSOC で収集したインシデント情報や攻撃手法の分析結果等を監視対象先の政府機関に加え、重要インフラ事業者等に提供するための仕組みについて、2015 年度を目途とする「サイバーセキュリティセンター」（仮称）への改組と合わせて構築するため、情報共有の範囲・方法等の検討を行い、結論を得る。

（イ） サイバー攻撃事態への対処に資する情報の集約・共有の充実 （内閣官房及び全府省庁）

a) 全府省庁において、サイバー攻撃事態への対処に資する情報に関して、内閣官房に集約するとともに、内閣官房において、各府省庁等との間でより適時・適切に情報共有がなされるよう、更なる充実を図る。

---

[27] Government Security Operation Coordination team の略。

b)　内閣官房において、政府機関等に対するサイバー攻撃に関する全般的な傾向や情勢について分析を行い、各政府機関に対して当該分析結果を定期的に提供する。

【 CYMAT と CSIRT 等との連携強化や訓練等による対処態勢の構築・強化 】

（ウ） 政府 CISO による一元的態勢の構築　（内閣官房及び全府省庁）

内閣官房において、関係府省庁と協力し、大規模な情報セキュリティ上の脅威となる事案等に対応するために、政府 CISO を中心に政府が一体となった態勢を構築する。

（エ） 情報セキュリティ緊急支援チーム（CYMAT[28]）要員等への訓練による対処能力の向上　（内閣官房及び全府省庁）

内閣官房において、各府省庁と協力し、大規模サイバー攻撃事態等により発生した支援対象機関等の情報システム障害又はその発生が予想される場合等、政府一体となった対応が必要となる情報セキュリティに係る事象に対応できる人材を養成・維持するため、情報セキュリティ緊急支援チーム（CYMAT）要員等に対し、訓練を実施する。

（オ） CSIRT[29]等の体制の整備及び連携の強化　（内閣官房及び全府省庁）

a)　各府省庁において、情報セキュリティ上の脅威となる事案が発生した際に、機動的に対応するために整備した CSIRT 等の機能を維持・向上させ、他の府省庁の CSIRT 等との連携強化に努める。

b)　内閣官房において、PoC[30]会合の開催や情報連携の枠組みを構築する等、各府省庁の CSIRT 間相互の緊密な連携と機能の維持・向上を図るための取組を行う。

（カ） 公開ウェブサーバに対する脆弱性検査の実施　（内閣官房及び関係府省庁）

内閣官房において、各府省庁との協力の下、希望府省庁の主要な公開ウェブ

[28] CYber incident Mobile Assistant Team の略。
[29] Computer Security Incident Response Team の略。
[30] Point of Contact の略。

サーバに対する脆弱性検査を実施し、その結果を当該府省庁等にフィードバックする。また、得られた知見については、全府省庁等で共有し、その成果を公表するとともに、次年度における重点検査の検査項目に適宜反映することで政府機関全体の対策状況の底上げを図る。

（キ） 標的型攻撃に係る教育訓練の実施及び連絡・報告訓練の訓練方法等の検討（内閣官房及び関係府省庁）

内閣官房において、各府省庁との協力の下、訓練手法を改善しつつ、参加希望府省庁に対して標的型攻撃に対する教育訓練を実施し、その結果を当該府省庁等にフィードバックするとともに、得られた知見については、全府省庁等で共有し、その成果を公表する。

また、標的型攻撃を受けた際、被害を最小限に止めるためには、迅速かつ適切な対応が必要となることから、職員の連絡・報告にかかる訓練を 2014 年度から実施するため、訓練方法等の検討を行う。

（ク） 「新たなサイバー攻撃に対する情報セキュリティ防御モデル」の検討及び演習の実施 （総務省）

総務省において、サイバー攻撃の解析及び防御モデルの検討を行い、官民参加型の実践的な防御演習を行う。

（ケ） 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）

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」[31]、「大規模サイバー攻撃事態等への初動対処について」[32]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 2014 年度以降も継続して実施する。

（コ） 政府機関における業務継続能力の強化（内閣官房及び全府省庁）

a) 内閣官房において、各府省庁と協力し、各府省庁の情報システム運用継続計画の運用及び維持・改善を目的に、計画策定・改善の事例や対処要

[31] 2003 年 11 月 21 日閣議決定。
[32] 2010 年 3 月 19 日内閣危機管理監決裁。

件等の情報提供を行うほか、各府省庁の計画の運用及び維持・改善の状況を把握する。

b) 各府省庁において、業務継続計画を踏まえつつ、内閣官房において策定した「中央省庁における情報システム運用継続計画ガイドライン」[33]を活用して、災害や障害発生時における行政の継続性を確保する観点から、自府省庁の情報システム運用継続計画について、必要に応じて見直しを行う。

（サ） 平時からの情報共有体制の構築 （内閣官房及び全府省庁）

内閣官房において、各府省庁と協力し、民間の CSIRT や SOC[34]事業者の団体等と定期的な会合や日常的な意見交換ができる枠組みを構築するなどにより、官民による情報共有の推進を図る。

（シ） サイバー攻撃に係る脅威・手法分析の推進（内閣官房及び関係府省庁）

内閣官房において、各府省庁と協力し、サイバー攻撃に係る脅威・手法の分析を推進することにより、事態発生時における適切な対処態勢の構築を図る。

（ス） 国際的なセキュリティカンファレンスへの参加等を通じた対処能力の向上（内閣官房）

内閣官房において、国際的なセキュリティカンファレンスへの参加等を通じて、最先端のサイバー攻撃及びこれへの対処に関する情報収集を行い、我が国の対処能力の向上を図る。

【 人材の確保・育成 】

（セ） 採用時における情報セキュリティ関連素養の確認（内閣官房及び関係府省庁）

各府省庁において、国家公務員採用に際して、情報セキュリティに関する素養の確認に努める。

（ソ） 政府職員に対する教育・意識啓発の推進（内閣官房、人事院、総務省及び全府省庁）

---

[33] 2011 年 3 月情報セキュリティセンター。2012 年 5 月改定。
[34] Security Operation Center の略。

a)　内閣官房及び総務省において、政府職員（一般職員、幹部職員及び情報セキュリティ対策担当職員）向けの統一的な教育プログラムの充実を図る。

b)　内閣官房において、各府省庁の CSIRT 要員等について、インシデント対応等に係る教育を実施するなど技術・知見等の向上を図る。

c)　内閣官房及び人事院において、政府職員に対する採用時の合同研修において情報セキュリティに係る内容を盛り込むなど教育機会の付与に努める。

d)　内閣官房において、情報セキュリティ対策上の役割に応じた教育教材のひな形を一層充実させる。また、政府機関職員として最低限実施すべき事項を簡潔にまとめた啓発資料を作成する。これを参考に各府省庁は情報セキュリティ教育を実施する。

e)　各府省庁において、電子政府利用促進週間、情報セキュリティ月間等の機会において、情報セキュリティに係る直近の事故・事例を踏まえた意識啓発を行う。

（タ）　人事ローテーションの工夫（内閣官房及び関係府省庁）

各府省庁において、情報セキュリティ担当部署と内閣官房情報セキュリティセンターで人事交流を行うなど、職員の希望も踏まえつつ、情報セキュリティ担当者が長い間情報セキュリティに係る業務に携われるよう、人事ローテーションの工夫を図る。

（チ）　優秀な外部人材の活用（内閣官房及び関係府省庁）

内閣官房において、優秀な外部人材の活用に関する事例を収集し、情報提供を行うなど、各府省庁と協力し、官民の人事交流等により情報セキュリティに係る外部人材の活用を進める。

【 カウンターインテリジェンス 】

（ツ）　サイバー空間におけるカウンターインテリジェンスに関する情報の集約・共有に係る取組の推進（内閣官房及び関係府省庁）

内閣官房において、各府省庁と協力し、サイバー空間におけるカウンターイン

テリジェンスに関する情報を集約するとともに当該情報について分析し、その結果を各府省庁に提供し、共有を図る。

3)その他

(ア) 情報セキュリティガバナンスの機能強化に向けた取組(内閣官房及び全府省庁)

a) 内閣官房において、各府省庁と協力し、各府省庁の官房長等で構成する情報セキュリティ対策推進会議(最高情報セキュリティ責任者等連絡会議。以下「CISO 等連絡会議」という。)の場を活用して相互の緊密な連携の強化を図るとともに、最高情報セキュリティアドバイザーによる専門的な見地からの助言等も踏まえ、各府省庁の最高情報セキュリティ責任者が、情報セキュリティ対策について責任を持って統括するための体制の充実を図る。

b) 内閣官房において、CISO 等連絡会議の下に設置された最高情報セキュリティアドバイザー等連絡会議を逐次開催し、共通する課題に対する専門的な見地からの助言やベストプラクティスの共有等を通じて、各府省庁の情報セキュリティに関する取組の高度化を図る。

(イ) 「情報セキュリティに係る年次報告書」(情報セキュリティ報告書)に係る取組の推進(内閣官房及び全府省庁)

a) 各府省庁において、最高情報セキュリティ責任者は、自府省庁の情報セキュリティ報告書を作成する。また、作成した情報セキュリティ報告書は、最高情報セキュリティアドバイザー等連絡会議において、比較・評価等を行うとともに、それらを通じて得られた知見の共有やフィードバックを図る。また、最高情報セキュリティ責任者は、作成した情報セキュリティ報告書をCISO 等連絡会議の場において報告する。

b) 内閣官房において、各府省庁における対策の実施状況について、最新版の政府機関統一基準群に基づき、対策実施状況報告及び重点検査をもとに客観的に比較可能な形で評価し、必要な対策の実施を求める。これにより、各府省庁の対策の改善と政府機関統一基準群等の改善に結びつけ、政府全体としての PDCA サイクルの定着と浸透を確実なものとする。そのため、調査項目・方法の改善を図るなど自己点検及び重点検査に係る作業の一層の効率化の方策について検討を行い、各府省庁に提示する。

c) 内閣官房において、政府機関を取り巻く情報セキュリティに関する脅威と

その分析等を行い、「政府機関における情報セキュリティに係る年次報告」として取りまとめる。当該年次報告については、政府全体としての効果的な対策の推進を図るとともに、国民への説明責任を果たすためのものとして、情報セキュリティの維持・確保にも配慮しつつ、CISO 等連絡会議で決定後、情報セキュリティ政策会議に報告し、公表する。

（ウ） 情報セキュリティ対策に関連する独立行政法人等との連携の強化（内閣官房、総務省及び経済産業省）

内閣官房において、NICT、独立行政法人産業技術総合研究所（以下「AIST」[35]という。）及び IPA との間で締結した協力覚書に基づき、情報セキュリティに係る研究者・実務家の知見を蓄積・活用するなど、情報セキュリティ対策に関連する独立行政法人等との連携を強化し、政府機関統一基準群等の施策に反映する。

（エ） 独立行政法人等との緊急時等の連絡体制の整備（内閣官房及び独立行政法人等所管府省庁）

内閣官房において、各府省庁と協力し、独立行政法人等との間の緊急時を含めた連絡体制について、その実効性を維持するための訓練を行う。

（オ） 行政機関以外の国の機関との連携（内閣官房）

内閣官房において、行政機関及び行政機関以外の国の機関で共通する情報セキュリティ上の課題に適切に対応するため、CISO 等連絡会議や最高情報セキュリティアドバイザー等連絡会議等の場を活用するなどして、行政機関以外の国の機関との情報交換や連携を積極的に行う。

[35] National Institute of Advanced Industrial Science and Technology の略。

② 重要インフラ事業者等における対策

【 新たな「行動計画」の策定 】

（ア） 新たな「行動計画」の策定 （内閣官房及び重要インフラ所管省庁）

内閣官房において、重要インフラ所管省庁と協力し、重要インフラの防護を強化するため、重要インフラ事業者等及び政府機関との間における情報共有の仕組みや重要インフラの範囲及びそれぞれの性格に応じた対応の在り方等について検討を行うほか、「重要インフラの情報セキュリティ対策に係る第２次行動計画」[36]（以下「第２次行動計画」という。）の見直しを実施した上で、新たな「行動計画」を策定する。

【 リスク評価手法に基づく対策の重点化 】

（イ）「安全基準等」策定方針及び重要インフラ分野における「安全基準等」の継続的改善（内閣官房及び重要インフラ所管省庁）

a) 内閣官房において、社会動向の変化等に対応し、新たな知見を適時反映していくために、「重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針（第3版）」[37]及び同指針対策編の分析・検証を行う。

b) 重要インフラ所管省庁において、同指針や各重要インフラ分野の特性を踏まえ、各重要インフラ分野における「安全基準等」の分析・検証を実施する。また、必要に応じて「安全基準等」の改定等の対策を実施する。

（ウ）「安全基準等」の整備浸透状況調査（内閣官房及び重要インフラ所管省庁）

内閣官房において、重要インフラ所管省庁の協力を得つつ、「安全基準等」の整備浸透状況について以下の調査を行う。

〈重要インフラ分野における調査〉

「安全基準等」の分析・検証及び改定等の実施状況、攻撃動向や情報システムに係る環境変化への対応状況の把握及び検証を行い、結果を公表する。

---

[36] 2009 年 2 月 3 日情報セキュリティ政策会議決定。2012 年 4 月 26 日改定。

[37] 2010 年 5 月 11 日情報セキュリティ政策会議決定。2013 年 2 月 22 日改定。

〈重要インフラ事業者等に対する調査〉

「安全基準等」の浸透状況に係る調査を行い、結果を公表する。また次年度の調査のための企画・準備を行う。

（エ） 共通脅威分析の実施（内閣官房）

内閣官房において、重要インフラ分野共通に起こりうる新しい脅威について、システムを取り巻く技術環境の変化に着目しながら、具体的な分析対象を選考し、国内外の研究動向等を踏まえ、詳細な分析を実施する。

新たな「行動計画」期間中に詳細分析の対象とすべき情報セキュリティに関する環境変化やそれに伴い発生する新たな脅威やリスクを抽出するための調査を行う。

なお、調査の実施に当たっては、セプター、重要インフラ事業者等及び重要インフラ所管省庁の協力を得るとともに、その結果を関係者に還元する。

（オ） リスク・コミュニケーションの充実（内閣官房及び重要インフラ所管省庁）

内閣官房において、重要インフラの情報セキュリティを取り巻く環境変化を迅速に把握するとともに、連携して対処すべきリスク対策について共通認識を醸成し、関係主体間の緊密な連携と円滑な対応が可能になるよう、重要インフラ所管省庁の協力を得つつ、重要インフラ事業者等、関係機関及び重要インフラ所管省庁等による相互のリスク・コミュニケーションを推進する。推進に当たっては、官民による互恵的な活動を目指し、セプターカウンシルとの連携を図る。

【 情報共有体制の深化・拡充 】

（カ）「セプターカウンシル」の活動支援（内閣官房）

内閣官房において、重要インフラの各分野により構成され、分野横断的な情報共有の推進等による共助活動の場である「セプターカウンシル」[38]が一層円滑に運用されるよう、その重要インフラサービスの維持・復旧能力の向上やC4TAP[39]等事業者にとって役立つ情報の事業者間での共有の推進等の活動を

[38] 重要インフラの情報セキュリティ対策の向上を図るため、11 のセプターにより、2009 年 2 月 26 日に創設。

[39] Ceptoar Council’s Capability for Cyber Targeted Attack Protection の略。

支援する。

（キ） 共有すべき情報の整理（内閣官房）

内閣官房において、情報共有の枠組みを活用し、情報セキュリティにおける脅威、社会動向の変化を踏まえ、共有すべき情報及び有効な共有方法について整理・充実を行う。

（ク） 第2次行動計画の情報連絡・情報提供に関する実施細目に基づく情報共有の推進（内閣官房）

a) 内閣官房において、重要インフラ事業者等のサービス維持・復旧がより容易になるようにするためには、官民の各主体が協力することが重要であるとの観点から、第2次行動計画に基づく情報共有体制の下、同計画の情報連絡・情報提供に関する実施細目による情報共有を推進する。

b) 内閣官房において、当該情報共有の継続的な改善の観点から、実施細目による情報共有の運用状況や上記（キ）「共有すべき情報の整理」の進捗状況等を踏まえた実施細目の見直しを実施し、必要に応じ改定を行う。

（ケ） 実施細目に基づく情報共有に係るルールの改善等（重要インフラ所管省庁）

a) 重要インフラ所管省庁において、情報提供に係る重要インフラ所管省庁からセプターへの情報共有ルール及び情報連絡に係る重要インフラ事業者等から重要インフラ所管省庁への情報共有のルールそれぞれについて、実施細目との整合性を維持し、必要に応じてこれら情報共有ルールの改善を行う。

b) 重要インフラ所管省庁において、情報提供に係るセプター内の情報共有ルールについて、実施細目との整合性の維持をセプターが行うよう、当該セプターに対して助言等の支援を行うとともに、セプターにおける対応状況を確認する。

（コ） セプターの強化及び訓練（内閣官房及び重要インフラ所管省庁）

a) 内閣官房において、セプターの強化を支援するために、重要インフラ所管省庁の協力を得つつ、各セプターの機能及び活動状況等をとりまとめ、各セプターと共有するとともに、公表する。

b) 内閣官房において、重要インフラ所管省庁の協力を得つつ、各分野にお

けるセプターの情報共有体制の維持及び向上のための情報疎通機能の確認の機会を提供する。

（サ）「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[40]）について、初年度の活動成果をふまえ、より有効な活動に発展させるよう、産業分野と参加メンバを拡大させるとともに、共有情報の充実等を図り、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」[41]等での高度解析に繋げる。

（シ） 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」（Telecom-ISAC Japan）と情報共有を推進する。

【 重要インフラ障害に対する連携対応能力の強化 】

（ス） 分野横断的演習の実施（内閣官房及び重要インフラ所管省庁）

内閣官房において、重要インフラ所管省庁、重要インフラ事業者等、セプター等の協力を得て、具体的な IT 障害発生を想定した演習シナリオの作成とそれに基づく分野横断的な演習を実施し、各事業者等の BCP の改訂等に資する課題を抽出する。

助言方法の改善など演習参加者の気づきを促す効果的な演習の実施方法や情報共有の活性化を検討するとともに、演習成果の浸透を徹底する観点から演習参加者の拡充や演習成果の周知活動の充実等の取組みを推進する。

なお、得られた成果については、関係者間で共有するとともに、可能な範囲で公表する。

（セ） 個別分野におけるサイバー演習（総務省及び経済産業省）

---

[40] Initiative for Cyber Security Information sharing Partnership of Japan の略。
[41] サイバー攻撃の実態を把握し、その結果を関係省庁、重要インフラ事業者等に提供することを目的に、総務省、経済産業省、NICT、IPA、テレコム・アイザック推進会議、JPCERT/CC により 2012 年 7 月に発足した協議会。

a)　総務省において、情報通信分野の事業者による、模擬サイバー攻撃の実施等を内容とするサイバー演習の実施について、支援する。

b)　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、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。

【 評価・認証の導入等によるサプライチェーン・リスクへの対応強化 】

（ソ）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、一般社団法人 JPCERT コーディネーションセンター（以下「JPCERT/CC」[42]という。）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。

（タ）　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システム等の信頼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、IPA 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、既存規格の翻訳等に着手し、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。

（チ）　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、制御システム関連のソフトウェア製品について製品

[42] Japan Computer Emergency Response Team/Coordination Center の略。

の流通後やシステムの稼働後に脆弱性から生じるコストやリスクを最小化するため、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脆弱性ハンドリング体制等の所要の見直しを IPA 及び JPCERT/CC において行う。

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、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。

（ツ） 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[43]）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。

（テ） 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、一般財団法人日本情報経済社会推進協会（JIPDEC[44]）等関係組織に対して支援を行う。

（ト） 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、IPA の推進する制御機器等の国内評価・認証スキームについて、2014 年度の確立に向けて、技術研究組合制御システムセキュリティセンター（以下「CSSC」[45]という。）等関係組織に対して支援を行う。

---

[43] Industrial Control System Security Response Group の略。
[44] Japan Institute for Promotion of Digital Economy and Community の略。
[45] Control System Security Center の略。

（ナ） 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、日本国内で制御関連デバイスのセキュリティ評価について、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。

（ニ） 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制度を確立する。

（ヌ） 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・認証機関において評価・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。

（ネ） 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。

【 訓練等による対処態勢の強化 】

（ノ） 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 2014 年度以降も継続して実施する。

【 人材の育成・普及啓発 】

（ハ） 重要インフラ事業者における人材育成の促進（内閣官房及び重要インフラ所管省庁）

内閣官房において、重要インフラ所管省庁と協力し、重要インフラ事業者における組織内 CSIRT 等の設置や、重要インフラ事業者等を対象としたワークショップ等を開催するなど、情報セキュリティリスクに確実に対応できる職員の採用・育成を通じて、職員の情報セキュリティ意識の啓発と能力の底上げ等の取組を推進する。

（ヒ） 広報公聴活動の充実（内閣官房）

内閣官房において、情報セキュリティの重要性を啓発し、重要インフラ事業者等の情報セキュリティ対策の底上げと、国民の情報リテラシーを高めるため、情報セキュリティ対策に関するウェブサイト等を活用し、広報公聴の充実を図る。また、セミナーや講演等の機会を活用し、行動計画及び同計画に基づく施策の広報活動に積極的に取り組む。

【 国際連携の推進 】

（フ） 重要インフラ分野での国際連携推進（内閣官房、総務省、経済産業省及び重要インフラ所管省庁）

a) 内閣官房において、総務省及び経済産業省と協力し、重要インフラ保護のための国際的な情報共有や連携の促進を目的とする「MERIDIAN」[46]の活動等に積極的に関与するなど、重要インフラ分野での国際連携を促進する。

b) 内閣官房において、重要インフラ所管省庁と協力し、我が国の重要インフラ分野における情報セキュリティ対策の向上に資するため、国際連携や海外の情報収集を通じて得られた IT 障害事例やベストプラクティス等について、国内の関係主体への情報発信を行う。

[46] 重要インフラに関する国際会合。

【 個別分野における取組の強化 】

（ヘ） 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」[47]等を見直す。

（ホ） 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休日夜間の全国一元化を継続して実施するとともに、休日夜間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。

【 その他 】

（マ） 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。

[47] 昭和 62 年郵政省告示第 73 号。

③ 企業・研究機関等における対策

【 中小企業等における対応強化 】

（ア） 中小企業における情報セキュリティ対策の推進（経済産業省）

a) 経済産業省において、中小企業を指導する立場にある者等を対象とした「中小企業情報セキュリティ指導者育成セミナー」を実施するとともに、中小企業団体等との連携により、当該団体等が主催する情報セキュリティ対策セミナーに協力する取組を実施することで、中小企業のセキュリティレベルの向上を図るとともに、IPA 等の作成する啓発資料・ツール等の利用を促進する。

b) 経済産業省において、情報セキュリティ対策の推進が困難と感じている中小企業における情報セキュリティ対策コストの負担の適正化及び対策の推進を目的として、IPA を通じて中小企業の情報セキュリティ対策ガイドラインの普及を促進する。

（イ） 中小企業における情報セキュリティ対策の底上げ（総務省及び経済産業省）

総務省及び経済産業省において、中小企業における情報セキュリティ投資を促進するための関連税制の利用促進等、中小企業の情報セキュリティ対策の底上げを支援する施策を推進する。

（ウ） 中小企業・小規模事業者の IT 活用における情報セキュリティの確保 （経済産業省）

中小企業・小規模事業者の新ビジネス創造促進のための IT 活用に対し、IPA において、情報セキュリティ確保等の観点から必要な支援を行う。

（エ） 個人情報漏えい等防止のための対策（経済産業省）

経済産業省において、標的型攻撃の顕在化を踏まえ、サイバー攻撃等による個人情報漏えい等を防ぐため、必要かつ適切な技術的対策を、個人情報の保護に関する法律[48]（以下「個人情報保護法」という。）のガイドラインに盛り込む。また、これを踏まえつつ、サイバー攻撃等による個人情報漏えい等を防ぐための対策について、個人情報取扱事業者を対象に普及啓発を行う。

---

[48] 2003 年法律第 57 号。

（オ） 技術・営業秘密保護に関する官民フォーラムなどの場の準備 （内閣官房及び経済産業省）

内閣官房及び経済産業省において、日本における技術・営業秘密保護のための取組を促進するために、官民フォーラムの場などで産業界と政府が一体となって営業秘密保護に関する情報共有・検討などを行うための準備を開始する。

【 事業等のリスクの開示 】

（カ） 上場企業における事業等のリスクとしての開示の検討 （金融庁）

金融庁において、上場企業におけるサイバー攻撃によるインシデントの可能性等について、米国の証券取引委員会（SEC[49]）における取組等を参考にしつつ、事業等のリスクとして投資家に開示することの可能性を検討し、結論を得る。その際、関連情報の共有など開示するインセンティブを促すための仕組みの在り方についても併せて検討し、結論を得る。

（キ） セキュリティエコノミクスに関する対応 （経済産業省）

経済産業省において、企業などの組織にとって最適な情報セキュリティ対策への投資や対策のレベルを評価する仕組みについて、IPA を通じ、経済学などの社会科学の知見を導入した検討を実施する。

【 情報セキュリティガバナンスの確立 】

（ク） 情報セキュリティガバナンス確立の促進（経済産業省）

経済産業省において、企業の情報セキュリティに係る負担を軽減し、また海外の動向を勘案しつつ、企業における新たな情報セキュリティガバナンスの確立を図るため、情報セキュリティガバナンスの普及啓発や導入支援を進める「情報セキュリティガバナンス協議会」[50]において、情報リスクの管理に関する参加企業内

---

[49] Securities and Exchange Commission の略。

[50] 企業組織が適切な情報セキュリティガバナンスを確立することを促進するため、経営陣が情報リスクについて正しく理解し、組織として適切なリスク管理と情報セキュリティ対策を実施することをめざし、情報リスクの管理に関する知見の共有や情報セキュ

での知見の共有を図る。

（ケ） 企業における情報セキュリティ対策の支援（経済産業省）

a) 経済産業省において、「2013 年情報処理実態調査」により、企業における情報セキュリティ監査制度の活用・企業における情報セキュリティマネジメントシステム適合性評価制度及び情報セキュリティ対策ベンチマークの活用状況、取引（委託、外注を含む）相手における情報セキュリティ対策実施状況の確認状況、Common Criteria（ISO/IEC15408）認証取得製品の導入状況について調査する。

b) 経済産業省において、国際的な取引等において情報セキュリティ上の信頼性を求められるようになる中、登録者の監査企業台帳に関する規則の遵守徹底を図り監査企業台帳の品質を向上させる等、企業における情報セキュリティ監査制度の更なる普及に向けた各種対応を行う。

c) 経済産業省において、企業における適切な情報管理・情報漏えい防止対策を促進し、情報を預ける国民の権利利益の保護に資するため、情報セキュリティ報告書モデルの普及を図る。

（コ） 「情報システム・モデル取引・契約書」の活用・普及（経済産業省）

経済産業省において、情報システムの信頼性向上の観点から、ユーザー・ベンダ間の取引の可視化・役割分担の明確化を進めるため経済産業省が公表した、「情報システム・モデル取引・契約書（第一版）」[51]、「情報システム・モデル取引・契約書（追補版）」[52]、「e ラーニングで学ぶモデル取引・契約書」[53]及び「情報システム・ソフトウェア取引トラブル事例集」[54]について、ユーザー・ベンダ双方の関係業界団体と連携して普及活動を推進する。

（サ） 企業における電子署名利活用の普及促進（総務省、法務省及び経済産業省）

総務省、法務省及び経済産業省において、2012 年度に開催された「電子署名法の施行状況に係る調査研究会」の検討結果等を踏まえ、利用申込者の本人

リティガバナンスに関する普及啓発等を実施することを目的に 2012 年 5 月 21 日に設立された協議会。

[51] 2007 年経済産業省。

[52] 2008 年経済産業省。

[53] 2009 年経済産業省。

[54] 2010 年経済産業省。

確認の見直しによる本人確認方法の多様化を図るとともに、セミナーの開催等をはじめ、企業における電子署名の利活用の普及促進策を検討・実施する。

（シ） 情報システム調達時等における情報セキュリティの確保の支援 （経済産業省）

a) 経済産業省において、JISEC の運用を推進するとともに、情報システム調達時の同制度の利用拡充を図る。

b) 経済産業省において、「暗号モジュール試験及び認証制度」[55]（以下「JCMVP」[56]という。）及び「暗号アルゴリズム確認制度」の運用を推進する。また、JCMVP について、IPA を通じ、試験等に関する人材の育成を図るとともに、2013 年度中に米国国立標準技術研究所（以下「NIST」[57]という。）と覚書を締結し、共同認証制度を確立する。

c) 経済産業省において、 JISEC における評価・認証対象となる製品のセキュリティ機能について、製品毎のプロテクション・プロファイル（PP）の整備を行う。

（ス） CISO 等の設置促進（経済産業省）

経済産業省において、情報セキュリティを推進する観点から、CISO に求められる役割・能力を整理し、CISO の設置の普及等に努める。

（セ） 組織の緊急対応チームの普及、連携体制の強化（経済産業省）

経済産業省において、CSIRT の構築・運用に関するマテリアルや、インシデント対策・対応に資する脅威情報や攻撃に関する情報、所要の分析を加えた具体的な対策情報等を適切な者の間で共有することにより、CSIRT の普及や JPCERT/CC と国内外の組織内 CSIRT との間における緊急時及び平常時の連携の強化を図るとともに、巧妙かつ執拗に行われる標的型攻撃への対処を念頭においた運用の普及、連携を進める。

---

[55] 電子政府推奨暗号リスト等に記載されている暗号化機能、ハッシュ機能、署名機能等の承認されたセキュリティ機能を実装したハードウェア、ソフトウェア等から構成される暗号モジュールが、その内部に格納するセキュリティ機能並びに暗号鍵及びパスワード等の重要情報を適切に保護していることを、第三者による試験及び認証を組織的に実施することにより、暗号モジュールの利用者が、暗号モジュールのセキュリティ機能等に関する正確で詳細な情報を把握できるようにすることを目的とした制度。

[56] Japan Cryptographic Module Validation Program の略。

[57] National Institute of Standards and Technology の略。

（ソ） 企業の運営するウェブサイトの安全性向上（経済産業省）

経済産業省において、IPA を通じ、ウェブアプリケーションの脆弱性を早期に発見し、対処に役立てるため、ログを解析し外部からの攻撃の痕跡を検査する「ウェブサイト攻撃の検出ツール」(iLogScanner)を企業の ウェブサイト運営者等に提供する。

（タ） 内部者の不正行為によるセキュリティインシデント防止の検討（経済産業省）

経済産業省において、内部者の不正による情報セキュリティインシデントを防止するための方策に関するガイドラインの普及浸透を図る。

（チ） 経営層向けセミナーの開催等（内閣官房、総務省及び経済産業省）

内閣官房、総務省及び経済産業省において、企業等の経営層、人事担当、採用担当等を対象としたセミナー等の開催や啓発資料の作成を推進するとともに、経済団体等が主催する会議も活用するなど、あらゆる機会を捉えて普及啓発を行う。 また、「情報セキュリティガバナンス協議会」の活動を支援する。

（ツ） 情報セキュリティ対策に資する各種ツール・分析等の提供（経済産業省）

経済産業省において、IPA を通じ、情報セキュリティ対策ベンチマークを提供する。

【教育機関における取組の強化】

（テ） 地方公共団体の教育関係部門における情報セキュリティに関する取組の推進（文部科学省）

文部科学省において、教育関係部門での情報セキュリティを確保するため、情報セキュリティの取組に関する普及・啓発を推進するとともに、情報セキュリティを含む情報通信技術の活用指導力の向上を目的とした取組が地方公共団体等において進められるよう、各地域で情報教育を推進する中核的な役割を担う指導主事等を対象とした研修を行う。

（ト） 大学に対する情報セキュリティに関する最新情報の提供（内閣官房、総務省、文部科学省及び経済産業省）

内閣官房、総務省、文部科学省及び経済産業省において、大学における情報セキュリティに関する教育の実施に資するような情報セキュリティに関する最新情報を提供する。その一環として、大学の自主的な判断に基づく情報セキュリティに係る資格試験合格による単位認定の導入、資格に関する学習プログラムの導入、経営学修士課程等における情報セキュリティ関連講義の実施等の検討に資する情報を提供する。

【その他】

（ナ） 個人情報保護法の見直し（消費者庁及び関係府省庁）

消費者庁及び関係府省庁において、個人情報保護法について、2015 年 3 月迄の消費者委員会における法改正も視野に入れた問題点についての審議に資するよう必要な協力を行い、その審議の結果を踏まえ検討に着手する。

④ サイバー空間の衛生

【普及啓発】

（ア） 新たな情報セキュリティ普及啓発プログラムの策定（内閣官房及び関係府省庁）

内閣官房において、各府省庁と協力し、「情報セキュリティ普及・啓発プログラム」[58]の見直しを行い、2014 年度以降の具体的な取組について「新たな情報セキュリティ普及・啓発プログラム」（仮称）を策定し、公表する。

（イ） 各府省庁と連携した普及啓発活動の推進（内閣官房、内閣府、警察庁、消費者庁、総務省、外務省、経済産業省、文部科学省、防衛省及び関係省庁）

内閣官房において、内閣府、警察庁、消費者庁、総務省、外務省、経済産業省、文部科学省、防衛省及び関係省庁と協力し、相互の連携強化を図るため、関係府省庁との連絡会等を定期的に開催する。

（ウ）「サイバー衛生の日（サイバー・クリーン・デー）」（仮称）の新設 （内閣官房、内閣府、警察庁、消費者庁、総務省、外務省、経済産業省、文部科学省、防衛省及び関係省庁）

内閣官房、内閣府、警察庁、消費者庁、総務省、外務省、経済産業省、文部科学省、防衛省及び関係省庁において、一般利用者等の認識の更なる醸成を図るため、「サイバー衛生の日（サイバー・クリーン・デー）」（仮称）を定める。

（エ） ソフトウェア教育との連携 （内閣官房及び文部科学省）

内閣官房において、文部科学省と協力し、放送大学における「情報コース」[59]等の情報セキュリティの基礎となるソフトウェア教育と連携した普及啓発を進める。

（オ） 表彰等の充実（総務省及び経済産業省）

a) 総務省及び経済産業省において、情報セキュリティ確保の観点から、多大な貢献を果たした個人・企業等を表彰する。

---

[58] 2011 年 7 月情報セキュリティ政策会議決定。

[59] ソフトウェア、情報数理、マルチメディア、ヒューマン、情報基盤という 5 つの領域により、情報処理の技術を学ぶのみならず、情報という視点から様々な問題を解決する術を身につけることを目指したコースとして、2013 年 4 月、放送大学教養学部に開設。

b)　経済産業省において、「未踏 IT 人材発掘・育成事業」[60]を実施する。

（カ）「情報セキュリティ月間」の充実（内閣官房及び関係府省庁）

内閣官房において、各府省庁と協力し、これまでの「情報セキュリティ月間」の実施結果等を踏まえ、国民に対する効果的な情報発信の方法や官民連携の強化等について検討を行い、「情報セキュリティ月間」における取組の充実と更なる周知を図る。

（キ） 国際連携を活用した普及・啓発活動の実施（内閣官房及び関係府省庁）

内閣官房及び関係府省庁において、国際連携を一層推進するため 2012 年 10 月に開始した「情報セキュリティ国際キャンペーン」について、その実施結果等を踏まえ、諸外国と連携しながら国内における普及・啓発を強化する。

（ク）「情報セキュリティ国際キャンペーン」の実施（内閣官房及び関係府省庁）

内閣官房及び関係府省庁において、ASEAN、欧米を始めとする諸国と国際連携を活用した行事や情報セキュリティ対策に関する情報提供等を行い、国際連携の推進と国内における情報セキュリティ対策の一層の普及・啓発を図る。

（ケ）「情報セキュリティ普及・啓発プログラム」の推進（内閣官房及び関係府省庁）

a)　内閣官房において、各府省庁と協力し、「情報セキュリティ普及・啓発プログラム」に基づき、同プログラムに掲げられた施策を着実に推進する。

b)　内閣官房において、各府省庁と協力し、国民一人ひとりの情報セキュリティについての関心を高めるため、自ら実施している対策がどのフェーズにあるのかを客観的に認識するためのツールである自己診断チェックリストの活用を進める。

c)　内閣官房において、各府省庁と協力し、高齢者層に対していたずらに不安感を煽ることのないように配慮しつつ、平易な言葉で情報セキュリティ対策を分かりやすく伝えるため高齢者向け資料の活用を進める。

d)　内閣官房において、各府省庁と協力し、企業の経営層が情報セキュリティに関する認識を高め、情報セキュリティに関するリスク判断を適切に行えるよ

[60] 2000 年度から「未踏ソフトウェア創造事業」として開始し、2008 年度により若い人材の発掘・育成に重点化すべく「未踏 IT 人材発掘・育成事業」に再編。

うにするための情報提供を行う。

（コ） 各種メディア等を通じた普及・啓発の推進（内閣官房、警察庁、総務省、経済産業省及び文部科学省）

a) 内閣官房において、各府省庁と協力し、国民の情報セキュリティ意識の向上を図るため、急速に高度化・複雑化している情報セキュリティ上の脅威に関する情勢等を踏まえ、「国民を守る情報セキュリティサイト」、「@police」、「国民のための情報セキュリティサイト」、「インターネット安全教室」、「フィッシング対策協議会」[61]、「フィッシング対策推進連絡会」[62]、「情報セキュリティ安心相談窓口」、「ここからセキュリティ！」等を通じ、国民一人一人に対する適切な情報提供を実施する。これらの取組においては、IT 初心者の層だけでなく、情報セキュリティ無関心層に対する働き掛けも重視することとする。

b) 警察庁において、情報セキュリティに関する意識・知識の向上を図るため、教育機関関係者、地方公共団体職員、インターネットの一般利用者等を対象として、サイバー犯罪の現状や検挙事例、スマートフォン等の情報端末やSNS 等の最新の情報通信技術を悪用した犯罪等の身近な脅威等を交えた講演等を全国各地で実施する。

c) 総務省及び文部科学省において、各府省庁と協力し、保護者、教職員及び児童生徒を対象に、子どもたちのインターネットの安心・安全な利用に向けた啓発のための講座（「e-ネットキャラバン」）を、通信関係団体等と連携しながら全国規模で実施する。

d) 総務省において、各府省庁と協力し、スマートフォン等が急速に普及していることを踏まえ、利用者に対して、スマートフォン等の情報セキュリティ対策について総合的な普及・啓発を推進する。

e) 経済産業省において、各府省庁と協力し、情報モラル/セキュリティの大切さを児童・生徒が自身で考えるきっかけとなるように、IPA 主催の標語・ポスター・4コマ漫画の募集及び入選作品公表を行い、国内の若年層における情報モラル/セキュリティ意識の情勢と向上を図る。

f) 経済産業省において、各府省庁と協力し、家庭や学校からインターネッ

[61] フィッシングに関する情報収集・提供、注意喚起等の活動を中心とした対策を促進することを目的として、平成 17 年 4 月 28 日に設立された協議会。
[62] フィッシングに関する情報の共有を図るとともに、その効果的な対策について検討することを目的として、平成 17 年 1 月に設置された連絡会。

トを利用する一般の利用者を対象として情報セキュリティに関する啓発を行う安全教室について、全国各地の関係団体と連携し引き続き開催していく。

g) 経済産業省において、IPA を通じ、広く企業及び国民一般に情報セキュリティ対策を普及するため、地域で開催されるセミナーや各種イベントへの出展、普及啓発資料の配布、情報セキュリティに関するコンクール、セキュリティプレゼンター制度の運用などにより情報の周知を行い、セキュリティ啓発サイトや各種ツール類を用いて、対策情報の提供を行う。

h) 経済産業省において、IPA、JPCERT/CC における統合的な脆弱性対策情報の提供環境を整備し、開発者、運用者及びエンドユーザに対して、脆弱性対策の普及啓発を推進する。

i) 経済産業省において、急速に変化しつつある脅威を的確に把握し、ウイルスや不正アクセス等の情報を積極的に収集・分析し、IPA を通じ広く国民一般に対し、傾向や対策等情報提供を行うとともに、「情報セキュリティ安心相談窓口」の運用により得た情報を踏まえ、コンピュータ利用者への注意喚起等の対策に反映する。

（サ） 情報セキュリティに関する事故事例等に関する普及啓発の推進 （内閣官房、経済産業省及び関係府省庁）

内閣官房及び経済産業省において、各府省庁と協力し、IPA 等に集約される情報セキュリティに関する事故事例等について、プライバシー保護など情報提供者等に配慮した上で収集し、主に一般国民を対象に普及啓発を進める。

（シ） 無線 LAN の情報セキュリティ確保の推進（総務省）

総務省において、一般及び企業による利用が拡大する一方、情報窃取等の情報セキュリティ上の課題が指摘されている無線LANについて、手引書「一般利用者が安心して無線LANを利用するために」[63]及び「企業等が安心して無線LANを導入・運用するために」[64]を活用し、適切な無線LANの情報セキュリティ対策の普及・啓発に努める。

（ス） 電波利用秩序維持のための周知啓発活動の強化（総務省）

総務省において、毎年6月の電波利用環境保護周知啓発強化期間において、

[63] 2012 年 11 月 2 日総務省。
[64] 2013 年 1 月 30 日総務省。

関係府省庁の協力を受け、各種メディアにより周知啓発を実施する。

（セ） 情報漏えい対策への取組（経済産業省）

a） 経済産業省において、個人情報も含む情報漏えい対策に取り組むため、IPA を通じ、ファイル共有ソフトによる情報漏えいを防止する等の機能を有する「情報漏えい対策ツール」を一般国民に提供する。

b） 経済産業省において、情報漏えいの新たな手法や手口の情報収集に努め、一般国民に対し、対策情報等、必要な情報提供を行う。

【インシデントの認知・解析機能の向上】

（ソ） サイバー攻撃高度解析機能の整備（総務省及び経済産業省）

総務省及び経済産業省並びにNICT、IPA、テレコム・アイザック推進会議及びJPCERT/CC の4団体が参加する「サイバー攻撃解析協議会」において、攻撃手法がますます複合化・複雑化するサイバー攻撃に対応するため、各団体が自らの活動やプロジェクト等により得られたサイバー攻撃関連情報を結集し、高度な解析を行う。その解析結果については、各機関の活動や外部への情報提供を通じて、サイバー攻撃への対処に活用する。また、攻撃手法がますます複合化・複雑化するサイバー攻撃に対応するため、官民関係者がそれぞれ把握できる情報を結集し、それらに対して高度解析を加える仕組みの運用を進める。

（タ） サイバー攻撃（インシデント）対応調整支援 （経済産業省） ※再掲

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。

（チ） サイバー攻撃の予兆の早期把握と情報収集・分析の強化 （警察庁及び法務省）

警察庁及び法務省において、サイバー攻撃への対策を強化するため、サイバー空間における攻撃の予兆等の早期把握を可能とする態勢を拡充し、オープンソースの情報を幅広く収集するなど、攻撃主体・方法等に関する情報収集・分析を強化する。

（ツ） サイバー攻撃事案の実態解明に係る情報収集・分析等（警察庁）

a) 警察庁において、違法行為に対する捜査等を推進するため、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。

b) サイバー攻撃事案の実態解明に資するよう、インターネット観測技術に関する調査研究を行う。

（テ） 新しい脅威・攻撃の分析・共有（経済産業省）

経済産業省において、IPA の運営する「脅威と対策研究会」を通じ、情報セキュリティに関する新しい脅威・攻撃を分析するとともに、分析結果等の利用者に必要な情報を迅速に提供する。

（ト） コンピュータセキュリティ早期警戒体制の強化 （経済産業省）

a) 経済産業省において、関係者間においてコンピュータウイルス、不正アクセス、脆弱性等に関する迅速な情報共有、円滑な対応を確保するため、IPA や JPCERT/CC 等による「コンピュータセキュリティ早期警戒体制」を、脅威の変化に対応可能な形で強化する。具体的には、近時のコンピュータウイルス等の攻撃手法の巧妙化に対応するため、インシデント対応の調整支援を行う JPCERT/CC 等の組織において、攻撃手法の分析・解析能力の一層の高度化、専門家間での解析手法やインシデント事例等に関する情報共有・連携を推進する。

b) 経済産業省において、JPCERT/CC がインシデント対応支援活動等において解析したマルウェア検体及びその解析結果について、同様の情報を有する国内外の関係機関との適切な相互共有やインターネット定点観測情報共有システム（TSUBAME）の運用との連動等の有効活用やその高度化を進める。

c) 経済産業省において、2012 年度に整備した制御システムに係るインシデントに特化した対応調整支援体制や、巧妙かつ執拗に行われる標的型攻撃に係る対応手法について、JPCERT/CC における効果的な運用を進めつつ、報告受付制度や対処手法の普及を図る。

d) 経済産業省において、フィッシング対策協議会及び JPCERT/CC を通じたフィッシングに関するサイト閉鎖依頼その他の対策実施に向けた取組につ

いて、改正不正アクセス禁止法[65]も踏まえた所要の見直し等を行う。

（ナ） 注意喚起等による情報セキュリティリスクの低減 （経済産業省）

経済産業省において、IPA を通じ、最新の脆弱性情報やインシデント情報を収集、分析し、注意喚起による危険回避や対策の徹底を図り、情報セキュリティリスクの低減を促進する。

（ニ） サイバー攻撃事前防止・早期対策に向けた取組の推進 （総務省）

a) 総務省において、近年、被害が拡大しているサイバー攻撃（DDoS 攻撃等、マルウェアの感染活動）に対処し、我が国におけるサイバー攻撃のリスクを軽減するため、国内外のインターネットサービスプロバイダ（ISP）、大学等との協力によりサイバー攻撃、マルウェア等に関する情報を収集するネットワークを国際的に構築し、諸外国と連携してサイバー攻撃の発生を予知し即応を可能とする技術について、その研究開発及び実証実験を実施する。

b) 総務省において、米国とは、インターネットエコノミーに関する日米政策協力対話にて、サイバー攻撃に関するデータを共有し、研究開発の分野での協力関係を加速化していくべきであるということで一致したことを踏まえ、サイバー攻撃の発生を予知し即応を可能とする技術の研究開発等を効果的に実施するため、データの共有を開始しているところであり、引き続き、米国との情報共有を強化する。

c) 総務省において、欧州連合（EU）とは、引き続き、ネットワーク上の攻撃の軽減のための共同研究の実施等の課題について議論を進める。

d) 総務省において、ASEAN 諸国とは、既に着手済みであるインドネシア、タイ、マレーシアとのサイバー攻撃の観測データの共有を足がかりに、他の ASEAN 諸国との連携を推進する。

（ヌ） 高度化・巧妙化するマルウェアを検知・除去し、感染を防止するためのフレームワークの構築 （総務省）

総務省において、高度化・巧妙化するマルウェアの被害を防止するため、ネットワーク型のボットウイルスに感染したユーザーを検知し、マルウェアの除去を当該ユーザーに促すほか、マルウェアを配布する等の悪性サイト情報を蓄積する

[65] 平成 24 年法律第 12 号。

データベースを構築し、悪性サイトにアクセスしようとする一般利用者に対する注意喚起等を、ISP 等により実施し、マルウェア感染を防止するための仕組みを構築する。

また、得られたサイバー攻撃関連情報については、必要に応じて、サイバー解析協議会や学会等に対して提供し、連携を図る。

（ネ） 革新的な情報セキュリティ技術の研究開発基盤の構築 （総務省）

総務省において、NICT を通じ、潜在型マルウェアの挙動・検知など、サイバー攻撃の検知機能の向上に向けた革新的な情報セキュリティ技術の研究開発・実証実験を実施するため、サイバー攻撃の観測・解析のための研究基盤を構築する。

（ノ） 情報セキュリティ目的の通信解析の可能性等関連制度の柔軟な運用の在り方の検討 （総務省）

総務省において、情報セキュリティを目的とした通信解析の可能性等、通信の秘密等に配慮した、関連制度の柔軟な運用の在り方について、可能な範囲で速やかに一定の結論を得るよう、サイバー攻撃等の実態、これに対する現行の取組状況等の実態把握に努めるとともに、情報セキュリティを目的とした通信解析における課題の洗い出し等を行う。

【ソフトウェアの脆弱性への対応】

（ハ） 脆弱性に関する情報収集・提供 （経済産業省）

経済産業省において、従来の届出の受付等に基づく脆弱性関連情報の調整・提供のみならず、自ら能動的にサイバー攻撃や脆弱性の検出を行い、調整・提供につなげるための取組を行う。

（ヒ） 脆弱性関連情報届出受付制度の運営及び脆弱性関連情報の提供 （経済産業省）

経済産業省において、IPA と JPCERT/CC により運用されている「脆弱性関連情報届出受付制度」を着実に実施するとともに、関係者との連携を図りつつ、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」の運用などにより、脆弱性関連情報をより確実に利用者に提供する。また、未調整案件への対応等、

これまでの運用において明らかとなった問題に対応できるよう、経済産業省の告示改正を進める。さらに制御システムの脆弱性に関する扱いについても引き続き検討し、方針を定める。

（フ） ソフトウェア等の脆弱性に係る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、ソフトウェア等の脆弱性に関する情報を、マネジメントツールが自動的に取り込める形式で配信する等、ユーザー組織における、ソフトウェア等の脆弱性マネジメントの重要性の啓発活動及び脆弱性マネジメント支援に関する JPCERT/CC の活動を強化する。

b) 経済産業省において、IPA を通じ、ソフトウェア等の脆弱性に関する情報をタイムリーに発信するサイバーセキュリティ注意喚起サービス「icat」を提供する。

（ヘ） ソフトウェアや情報システムの安全な利用の推進及び脆弱性の発生を縮減するための対策の推進（経済産業省）

a) 経済産業省において、経済産業省告示[66]に基づき、脆弱性関連情報の届出受付を行い、定期的に受付状況を公表するとともに、関係者との連携を図りつつ、脆弱性関連情報をウェブサイト運営者、ソフトウェア製品開発者に提供し、脆弱性対策を促進する。

b) 経済産業省において、ソフトウェア製品や情報システムについて製品の流通後やシステムの稼働後に発見される脆弱性に伴う対応コストや被害発生リスクを最小化するため、ソフトウェア製品等の脆弱性に対する迅速な対応を可能とする体制（脆弱性ハンドリング体制）等について既存の枠組みを見直す。また、ソフトウェア製品や情報システムの開発段階において、製品開発者が情報セキュリティ上の観点から配慮すべき事項を、解説資料やセミナーの形で公開し、普及を図る JPCERT/CC 等の取組を継続する。

c) 経済産業省において、流通後の修正が容易でないとされる組込みソフトウェア及びスマートフォン等のアプリケーションにおいて多用される言語に関し、IPA において整備したコーディングスタンダードについて、更なる開発の高信頼化を図るための取組等を行う。

d) 経済産業省において、組込み機器や情報家電等の開発者に利用されて

[66] 「ソフトウェア等脆弱性関連情報取扱基準」）（2004 年 7 月 7 日経済産業省告示第 235 号）

いるプロトコルである TCP/IP 及び SIP の脆弱性検証ツールを IPA を通じて開発者に提供する。

e) 経済産業省において、ウェブサイト運営者や製品開発者が脆弱性対策の必要性及び対策手法等を自ら学習することを支援するため、「安全なウェブサイトの作り方」と体験的かつ実践的に学ぶツール「AppGoat」をセットにして IPA を通じて普及啓発を図る。

f) 経済産業省において、自動車に含まれるソフトウェアを活用したサービスの増加や、スマートフォン等の普及による自動車と外部ネットワークの連携強化を受け、IPA を通じて自動車の情報セキュリティ対策の普及を図る。

g) 経済産業省において、IPA を通じ、情報システムの脆弱性に対して、プロアクティブに脆弱性を検出する技術の普及・啓発活動を行う。

（ホ） ソフトウェアの脆弱性への対応に関する制度の在り方 （経済産業省）

経済産業省において、社会インフラの重要構成要素を制御するソフトウェアについて、一般的な情報システムにおけるソフトウェアと比べ、すぐに修正プログラムを適用することが困難である点や、修正プログラム適用のための緊急な運転停止が困難な点、製品のライフサイクルが長い点等の特徴があることも踏まえ、脆弱性への対応に関する既存の枠組みの特則の検討など脆弱性への対応に関する制度の在り方を検討し、結論を得る。

（マ） 脆弱性ハンドリングの国際調整 （経済産業省）

経済産業省において、全世界で公開される全ての脆弱性情報を言語を問わず集約し、識別できるようにする仕組みの実現可能性を探る国際組織（FIRST[67]）の活動に、JPCERT/CC を通じて参加し、協力する。また、国際的な標準化が進む製品開発者の脆弱性情報ハンドリングプロセスに関し、国内の「脆弱性関連情報届出受付制度」が齟齬なく対応できるよう JPCERT/CC における調整機能の高度化を図る。

（ミ） 組込み機器の脆弱性対策の推進 （経済産業省）

経済産業省において、IPA を通じ、我が国の競争力の源泉となる組込み機器の脆弱性に関する対策の提示等を行う。

---

[67] Forum of Incident Response and Security Teams の略。

（ム） 制御システムに係る脆弱性ハンドリング体制の改善 （経済産業省）

経済産業省において、制御システム関連のソフトウェア製品について製品の流通後やシステムの稼働後に脆弱性から生じるコストやリスクを最小化するため、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脆弱性ハンドリング体制等の所要の見直しを IPA 及び JPCERT/CC において行う。

（メ） 情報システム等の安全性・信頼性等に関する利用者への品質説明力の強化（経済産業省）

経済産業省において、情報システム等におけるソフトウェアの不具合が社会に与える混乱や被害を防止する観点から、更なる開発・検証技術の高度化を図りつつ、ソフトウェアによって中核機能が実現される製品、システム及びサービスについて第三者がその安全性・信頼性等を利用者に対し十分に説明できるよう、利用者への品質説明力を強化する。

【その他】

（モ） SOC 事業者間等における情報共有の促進 （内閣官房、総務省及び経済産業省）

内閣官房、総務省及び経済産業省において、SOC 事業者間及び諸機関との脅威に関する情報の共有を促進する。

（ヤ） スパムメール対策の強化 （内閣官房、総務省及び消費者庁）

a) 総務省及び消費者庁において、巧妙化・悪質化が進展し全体として増加が続くスパムメールに対応するため、特定電子メール法及び特定商取引法の着実な執行等所要の措置を講じる。

b) 総務省において、国内の主要なインターネット接続サービス事業者や携帯電話事業者が中心となり設立された民間団体である「JEAG」等の業界団体と連携して、スパムメール送信の防止に効果のある技術である 25 番ポートブロックや送信ドメイン認証技術（SPF、DKIM 等）等の導入を促進する。

c) 総務省において、我が国に着信するスパムメールの大部分を占める海外から発信されるスパムメールに対応するため、スパムメール対策を行う外国執

行当局との連携を強化するとともに、民間における国際的なスパムメール対策の連携を推進する。

d) 総務省において、その他、違法なスパムメールに関する情報を当該スパムメールの送信等に利用されたインターネット接続サービス事業者に通知し利用停止等の措置を促進する「迷惑メール追放支援プロジェクト」[68]を実施する。

（ユ） 暗号・認証技術等を用いた通信プロトコルの利用による安全な通信環境の実現（総務省）

総務省において、NICT を通じ、安全な通信環境の実現に向け、暗号・認証技術等を利用した通信プロトコルの安全性に関する評価を実施するとともに、評価結果の情報を集約してプロトコルの脆弱性情報の提供を行う。

（ヨ） IPv4 アドレスの枯渇に伴う諸課題への対応推進（総務省）

総務省において、IPv4 アドレスを共同利用する環境における通信の安全性・信頼性の確保のため、情報セキュリティ等に係る技術的諸課題を解決するための実証実験を実施し、その成果をガイドライン等の形で広く展開する。

（ラ） IPv6 ネットワークのための情報セキュリティ検証環境の構築（総務省）

総務省において、NICT を通じ、IPv6 ネットワークの情報セキュリティの確保に向け、IPv6 への移行に伴う脅威や脆弱性等の具体的なセキュリティ課題を抽出し、これまで構築してきた検証環境を用いてそれらの重要度を評価した上で、必要な情報セキュリティ対策の研究開発を行う。

（リ） IPv6 環境における脆弱性検証ツールの貸出し（経済産業省）

経済産業省において、IPv6 環境において脆弱性検証が可能な TCP/IP に係る既知の脆弱性検証ツールの利用促進を図るため、普及・啓発活動を継続して実施する。

（ル） インターネット利用環境の変化に伴う情報セキュリティ対応推進 （総務省）※再掲

---

[68] 民間事業者による自主的な迷惑メール対策を促すことを目的として、2005 年 2 月から開始。

総務省において、IPv4とIPv6が共存するネットワーク環境におけるセキュリティ課題の対応方策を確立するための実証実験を実施し、その成果をガイドライン等の形で広く展開する。

⑤ サイバー空間の犯罪対策

【サイバー攻撃対策等の強化】

（ア） サイバー攻撃対策に係る体制等の強化（警察庁）

サイバー攻撃手法の高度化等に対応するため、以下に掲げる施策を実施して、警察におけるサイバー攻撃対策に係る体制等の強化を推進する。

a) 都道府県警察に「サイバー攻撃特別捜査隊」を設置し、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ための体制を強化する。

b) 警察庁に「サイバー攻撃対策官」及び「サイバー攻撃分析センター」を設置し、情報の収集・分析や広域捜査・国際捜査を推進するための体制を強化する。

c) サイバー空間に関する観測機能の強化を図るとともに、サイバーフォースセンター[69]の技術力向上等を通じて、サイバー攻撃対策に係る体制等を強化する。

d) サイバー攻撃対策要員の事案対処能力・技術力の維持・向上のため、民間の知見を活用した研修を実施する。

（イ） 悪質・巧妙化するサイバー犯罪の取締りのための態勢の強化（警察庁）

新たな手口の不正アクセスや不正プログラム（スマートフォン等を狙ったものを含む。）等急速に巧妙化するサイバー犯罪の取締りを推進するため、サイバー犯罪捜査に従事する全国の警察職員に対する部内研修及び民間企業への講義委託の積極的な実施、サイバー犯罪の取締りを行うための資機材の整備の推進、全国協働捜査方式による取締りの推進等、サイバー犯罪への対処態勢を強化する。

（ウ） サイバー空間の安全と秩序を維持するための民間との連携強化（警察庁）

サイバー空間の安全と秩序を維持するため、各都道府県警察と関係事業者等

[69] サイバー攻撃対策の技術的基盤として、警察庁情報通信局に設置。サイバー攻撃の予兆・実態把握、標的型メールに添付された不正プログラム等の分析を実施するほか、サイバー攻撃発生時には技術的な緊急対処の拠点として機能。

から成る各種協議会等を通じ、官民連携した取組を推進する。

（エ） 犯罪に強いIT社会構築のための官民連携に向けた取組の推進（警察庁）

有識者、関連事業者等で構成する総合セキュリティ対策会議を開催し、日本版 NCFTA[70]の創設に向け、サイバー空間の脅威に対処するための産学官連携の在り方について検討し、結論を得る。

（オ） サイバー犯罪の被害防止対策の推進（警察庁）

インターネット利用者の各種トラブルに応じた基本的な対応策やサイバー犯罪の手口やその対応策を警察庁ウェブサイトに掲載するなどの広報啓発を実施する。

（カ） 不正アクセス禁止法の適正な運用を始めとした不正アクセス防止対策の推進（警察庁、総務省及び経済産業省）

不正アクセス行為の禁止等に関する法律に基づき、不正アクセス行為、フィッシング行為、他人の識別符号を不正に取得・保管する行為等の取締りを強化するとともに、情報セキュリティ関連事業者団体に対する不正アクセス行為の具体的手口に関する最新の情報の提供や、不正アクセス行為の発生状況及びアクセス制御機能に関する研究開発の状況の公表等を通じ、不正アクセス行為からの防御に関する啓発及び知識の普及を図るなど、官民連携した不正アクセス防止対策を更に推進する。

（キ） フィッシング対策協議会（経済産業省）

フィッシング詐欺被害の抑制のため、フィッシング対策協議会を通じて、海外、特に米国を中心として大きな被害を生んでいるフィッシング詐欺に関する事例情報、技術情報の収集及び提供を行う。

（ク） 重要インフラに対するサイバーテロ対策に係る官民の連携強化（警察庁）

警察庁において、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ことにより、昨今の我が国政府機関等に対するサイ

[70] National Cyber-Forensics and Training Alliance の略。FBI、民間企業、学術機関を構成員として米国に設立された非営利団体。サイバー犯罪に係る情報の集約・分析、海外を含めた捜査機関等の職員に対するトレーニング等を実施。

バー攻撃事案の発生等を踏まえた、サイバーテロに対する危機意識の醸成を図るとともに、事案発生を想定した共同訓練の実施やサイバーテロ対策協議会を通じた事業者間の情報共有により、重要インフラ事業者等の意向を尊重し、サイバーテロ発生時における緊急対処能力の向上に資する取組を行う。

（ケ） サイバーインテリジェンス対策[71]に係る官民の連携強化（警察庁）

サイバー攻撃の標的となるおそれのある事業者等との情報共有体制を強化し、サイバーインテリジェンス対策に資する取組を行う。

（コ） 諸外国におけるサイバー攻撃等の調査研究（警察庁）

諸外国におけるサイバー攻撃事案及びサイバーディフェンス施策並びにサイバー犯罪捜査手法に関して調査を行い、効果的・先進的な取組については我が国の施策に反映させることを検討するなどして、我が国のサイバー攻撃・サイバー犯罪対策の強化を図る。

【事後追跡可能性の確保】

（サ） ログの保存の在り方の検討（警察庁及び総務省）

警察庁及び総務省において、相互に連携しつつ、サイバー犯罪に対する事後追跡可能性を確保するため、可能な範囲で速やかに一定の結論を得るよう、関係事業者における通信履歴等に関するログの保存の在り方やデジタルフォレンジックに関する取組を促進するための方策について検討する。

特に、通信履歴の保存については、通信の秘密との関係、セキュリティ上有効な通信履歴の種類、保存する通信事業者等における負担、海外でのログ保存期間、一般利用者としての国民の多様な意見等を勘案した上で、サイバー犯罪における捜査への利用の在り方についての検討を行う。

（シ） デジタルフォレンジック[72]に係る取組の推進（警察庁）

a) 多様化・複雑化するサイバー犯罪に適切に対処するため、サイバー犯罪

---

[71] 情報通信技術を用いた諜報活動（サイバーインテリジェンス）に対する対策。

[72] 不正アクセスや機密情報漏えい等、コンピュータに関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。Digital Forensics。

捜査に従事する警察職員に対する研修の実施、資機材の増強のほか、関係会合への参加や技術協力を通じた関係機関及び民間との協力等、デジタルフォレンジックに係る体制等の強化を推進する。

b) 不正プログラム解析センターを中心として、不正プログラムの解析のための体制等を強化する。

c) デジタルフォレンジックを取り巻く課題とその対応方策に関する調査研究を行う。

【人材育成等による体制強化】

（ス） サイバー犯罪対策のための人材育成の強化 （法務省）

検察官及び検察事務官が、複雑・巧妙化するサイバー犯罪に適切に対処するため、捜査上必要とされる知識と技能を習得できる研修を全国規模で実施し、捜査能力の充実を図る。

（セ） サイバー防犯ボランティア育成の推進（警察庁）

サイバー空間におけるボランティア活動の促進を図るため、サイバー防犯ボランティアの結成及び育成や活動の支援を強化することにより、安全で安心なインターネット空間の醸成に向けた取組を推進する。

【その他】

（ソ） スマートフォンの安全利用のための環境整備 （警察庁）

スマートフォン利用者等を狙ったサイバー犯罪等の減少に向け、アプリのチェックの仕組みの充実、関係省庁との連携によるスマートフォンに関する青少年に対する有害環境対策の徹底等、スマートフォンの安全利用のための環境整備に向けた取組を実施する。

（タ） スマートフォン利用者等を狙ったサイバー犯罪への対処（警察庁）

スマートフォン利用者等を狙ったサイバー犯罪に関し、情報セキュリティ関連事業者等との連携強化による情報集約等に努め、取締りの強化を図る。また、取締りにより判明した実態等を踏まえ、一般利用者等の情報セキュリティ対策の向上

に資する情報発信等を推進する。

⑥ サイバー空間の防衛

【自衛隊等の態勢の強化】

（ア） サイバー防衛隊（仮称）の新編 （防衛省）

防衛省において、日々高度化・複雑化するサイバー攻撃の脅威に適切に対処するため、サイバー防衛隊（仮称）を新編する。

（イ） サイバー攻撃等対処に係る企画機能の強化 （防衛省）

防衛省において、サイバー攻撃等の脅威の増大に対応するため、運用企画局及び統合幕僚監部のサイバー企画機能を強化する。

（ウ） ネットワーク監視態勢の強化 （防衛省）

防衛省において、防衛情報通信基盤（DII[73]）について、サイバー攻撃等に関する状況把握能力を向上させるとともに、サイバー攻撃等発生時における被害局限化、早期復旧等の対処能力を強化するため、ネットワーク監視器材を整備する。

（エ） サイバー演習環境構築技術に関する研究 （防衛省）

防衛省において、指揮系システムについて、サイバー攻撃時においても部隊運用を継続するとともに、被害の拡大を防止するなどの事後対処能力の練度向上を目的としたサイバー演習環境の構築技術に関する研究を実施する。

（オ） 陸自電算機防護システムの整備等 （防衛省）

防衛省において、陸上自衛隊の情報システムを対象とした陸自電算機防護システム等、各自衛隊の情報システムを監視、防護するための機材を整備する。

（カ） サイバー防護分析装置の機能強化 （防衛省）

防衛省において、サイバー攻撃等に関する技術は日々進歩していることを踏まえ、サイバー防護分析装置の情報収集機能や分析機能、演習機能の強化等、技術の進化に対応した機能向上等を行う。

---

[73] Defense Information Infrastructure の略。

（キ） 国外におけるサイバー攻撃関連情報に関する情報収集・分析機能強化（防衛省）

防衛省において、2014 年度以降、情報本部等による国外におけるサイバー攻撃関連情報の収集・分析体制を強化・向上させる。

（ク） 情報保証に係る最新技術動向等の調査研究（防衛省）

防衛省において、情報システムの情報保証を確保するため、サイバー攻撃及びサイバー攻撃対処に係る最新技術動向等を調査するとともに、有効な対処態勢等について調査研究を実施する。

（ケ） 人材育成及び外国との連携強化（防衛省）

防衛省において、サイバー攻撃等対処に向けた人材育成の取組として、国内外の大学院等への留学等を行う。また、米国等との連携を強化するため各種会議等への参加を行う。

【国家レベルのサイバー攻撃への対応の強化】

（コ） 国家レベルのサイバー攻撃への対応の強化（内閣官房、警察庁、総務省、外務省、経済産業省、防衛省及び関係府省庁）

内閣官房において、警察庁、総務省、外務省、経済産業省及び防衛省等の関係府省庁と協力し、外国政府等の関与が疑われる国家レベルのサイバー攻撃への対応体制の整備等を行うため、サイバー攻撃に関するインシデントの認知、インシデント情報等の収集・共有や高度な解析及びわが国に甚大な被害が生じるサイバー攻撃が発生した場合の対処の在り方等について、個別具体的な国際法の適用も整理しつつ、平時及び非常時における警察、防衛省・自衛隊等の政府機関やサイバー空間関連事業者など関係機関の役割の整理・明確化を行う。

２「活力ある」サイバー空間の構築

サイバー空間の発展性を確保するため、サイバー攻撃への対応の担い手となる産業の活性化、高度な技術の開発、人材やリテラシーの育成・涵養等により、「活力ある」サイバー空間を構築し、サイバー空間を取り巻くリスクに自立的に対応できる創造力・知識力の強化を目指す。

① 産業活性化

（ア） M2M における情報セキュリティの確保に関する検討及び研究開発の推進（総務省及び経済産業省）

総務省及び経済産業省において、M2M について、情報の機密性や完全性等が失われた場合、社会的混乱を招くばかりでなく、情報通信技術基盤に対する信頼が損なわれる可能性があることを踏まえつつ、「情報セキュリティ研究開発ロードマップ」[74]に記載のセンサーネットワーク技術等を考慮し、M2M における情情報セキュリティ確保に関する検討及び研究開発を実施する。

（イ） スマートコミュニティ普及等に資する高セキュアな半導体デバイスの研究開発等の推進（経済産業省）

経済産業省において、M2M 等を基盤としたスマートコミュニティ・スマートグリッド等の普及、パーソナルデータ等を利活用した新サービスの開発・育成、ハードウェアに内在するセキュリティ上の脅威への対応等を促進するための高セキュアな半導体デバイス等に関する研究開発を強化する。また、BEMS[75]等の先進的なエネルギー設備導入にあたってのサイバーセキュリティ確保の研究開発を行う。

（ウ） 新たな情報流通形態に対応した情報秘匿・認証・改ざん防止技術の研究開発（総務省）

総務省において、NICT を通じ、クラウド等の新たな情報流通形態に対応するため、情報の円滑な利用を妨げず、必要な情報秘匿及び認証を両立するための研究開発を行う。

---

[74] 2012 年 6 月 22 日情報セキュリティ政策会議技術戦略専門委員会決定。
[75] Building Energy Management System の略。

（エ） 省リソースデバイスにおける情報セキュリティ技術の研究開発（総務省）

総務省において、NICT を通じ、スマートメータセンサ等の省リソースデバイスに実装可能な軽量暗号技術や大規模ノードにおける認証・プライバシー保護技術等の研究開発を行う。

（オ） 社会基盤としてのクラウドコンピューティングの情報セキュリティ確保の推進（総務省）

総務省において、安心・安全なクラウド利用環境を実現するため、クラウドサービスを提供する事業者が実施すべき情報セキュリティ対策について、国際標準等の動向を踏まえ、ガイドラインとして取りまとめる。

（カ） クラウドサービスレベルのチェックリスト等の普及・促進（経済産業省）

経済産業省において、クラウドコンピューティング利用時におけるデータ保護及びサービス品質に関する責任主体を明確化するために、サービス提供側に過度の負担とならないよう、クラウド事業者とクラウド利用者の間で、サービス内容・範囲・品質等（例：サービス稼働率、信頼性レベル、データ管理方法、セキュリティレベル等）に関する保証基準の共通認識の形成を促す、クラウドサービスレベルのチェックリスト等を普及・促進する。

（キ） クラウドコンピューティングの国際標準化に向けた取組（総務省及び経済産業省）

a) 総務省及び経済産業省において、情報セキュリティ分野の国際標準化活動である ISO/IEC JTC 1/SC27 、ITU-T SG17 等が主催する国際会合等に参加し、我が国の研究開発成果や IT 環境・基準・ガイドライン等を踏まえて国際規格への反映が行われるよう積極的に参画する。

b) 経済産業省において、2011 年に策定した「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」[76]の改訂を行うとともに、クラウドセキュリティガイドライン活用ガイドブックとともに公開する。また、ISO/IEC 27000 シリーズに標準として組み入れるべく日本案を ISO/IEC JCT1 SC27 WG1 に提案をしているが、この標準化を推進する。

（ク） 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

[76] 2011 年 4 月 1 日経済産業省。

省） ※再掲

経済産業省において、日本国内で制御関連デバイスのセキュリティ評価について、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。

（ケ） 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） ※再掲

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制度を確立する。

（コ） 国際的なルールに基づくセキュリティ製品の貿易の推進 （経済産業省）

経済産業省において、日本が強みを持つ複合機や制御システム等の日本製品が貿易において不利な扱いを受けることがないよう、IPA を通じ、セキュリティの国際標準化や評価・認証の国際的な相互承認枠組みに積極的に参画、働きかけを進める。

（サ） 自動車に係る情報セキュリティの確保 （経済産業省）

経済産業省において、携帯端末等の機器との相互接続が拡大する自動車の制御システムに関するセキュリティ上の諸問題について調査し対策等の検討を行い、結論を得る。

（シ） 政府調達の在り方の検討（内閣官房） ※再掲

内閣官房において、新興企業を含む我が国サイバーセキュリティ産業の能力の活用等を通じて、サイバーセキュリティの確保に実質的に有効な製品、システム等の調達を図るべく、応札事業者の技術力評価の在り方など政府による調達の在り方について検討を行い、結論を得る。

（ス） 安全性確保のためのソフトウェア等のリバースエンジニアリングの適法性の明確化（文部科学省）

文部科学省において、文化審議会著作権分科会の報告に基づき、情報セキュリティ目的のリバースエンジニアリングの適法性を明確化するための措置を速やかに講ずる。

② 研究開発

（ア）「情報セキュリティ研究開発戦略」の研究開発の推進（内閣官房及び関係府省庁）

内閣官房において、各府省庁と協力し、「情報セキュリティ研究開発戦略」[77]に基づき、情報通信システム全体のニュー・ディペンダビリティの確保、攻撃者の行動分析に基づくゼロデイ・ディフェンス[78]、個人情報等の柔軟管理の実現、研究開発の促進基盤の確立とセキュリティ理論の体系化に係る研究開発を推進するとともに、その進捗状況の把握を行いつつ、次期の研究開発戦略のための見直し方針を策定する。

（イ） スマートコミュニティ普及等に資する高セキュアな半導体デバイスの研究開発等の推進（経済産業省） ※再掲

経済産業省において、M2M 等を基盤としたスマートコミュニティ・スマートグリッド等の普及、パーソナルデータ等を利活用した新サービスの開発・育成、ハードウェアに内在するセキュリティ上の脅威への対応等を促進するための高セキュアな半導体デバイス等に関する研究開発を強化する。また、BEMS 等の先進的なエネルギー設備導入にあたってのサイバーセキュリティ確保の研究開発を行う。

（ウ） 標的型攻撃の対策技術に関する研究開発（総務省）

総務省において、NICT を通じ、標的型攻撃の対策技術として、マルウェアに感染したコンピュータからの情報流出に対処する技術の研究開発を行う。

（エ） 情報セキュリティ強化を含むビッグデータ利活用のための研究開発（文部科学省）

文部科学省において、ビッグデータ利活用のための研究開発として、データ連携技術等（データの収集、蓄積・構造化、データ処理・分析、処理結果の可視化・検証等の各段階における技術等）の研究開発を実施する中で、情報セキュリティ強化のための取組を実施する。

---

[77] 2011 年 7 月 8 日情報セキュリティ政策会議決定。

[78] ゼロデイ攻撃（OS やアプリケーションの脆弱性を修正するパッチが提供されるより前に、その脆弱性を突いた攻撃が行われる状態）に対応するディフェンス（防御）技術を指す造語。具体的には、攻撃者のプロファイリングや行動モデルの分析により、サイバー攻撃対策の最適化を「先読み」して行うなど能動的な防御技術を指す。

（オ） 新世代ネットワーク基盤技術に関する研究開発（総務省）

総務省において、2020 年頃の実現を視野に、現在のインターネットの限界を克服し、ユーザーからの要求に応じた最適な品質やセキュリティ・耐災害性等に優れた新世代ネットワークの基盤技術の研究開発を推進する。

（カ） 量子情報通信ネットワーク技術の研究開発（総務省）

総務省において、NICT を通じ、情報理論的安全性（暗号が情報理論的な意味で無条件に安全である性質）を具備した量子暗号からなる量子情報通信ネットワーク技術の確立に向け、研究開発を実施する。

（キ） ネットワーク等の安全性・信頼性確保に資する情報セキュリティ技術に関する研究開発（総務省）

総務省において、NICT を通じ、世界最先端のサイバー攻撃観測・分析・対策・予防技術、セキュアネットワークの設計・評価と最適構成技術、次世代暗号基盤技術等、ネットワークセキュリティ技術の研究開発を実施する。

（ク） 情報通信構成要素の安全性検証技術の高度化に関する研究開発（総務省）

総務省において、NICT を通じ、情報通信ネットワークの安全性を保証する上で、ルータ等のネットワーク機器に実装されている通信プロトコル等が安全性の高いものであるかを検証するための評価手法の確立に向けた研究開発を実施する。

（ケ） サイバーセキュリティ研究基盤の構築（総務省）

総務省において、NICT を通じ、サイバーセキュリティの研究開発を促進するため、攻撃トラフィック、マルウェア検体等のデータセットについて、大学等の外部の研究機関の安全な利用を可能にする研究基盤（NONSTOP[79]）を運用する。

（コ） システムにおける適切な情報セキュリティ設定を自動的に導出する技術の研究開発の推進（総務省）

総務省において、NICT を通じ、ネットワークの各構成要素（ノード）における最

[79] Nicter Open Network SecurityTest-Out Platform の略。

適な情報セキュリティ設定を自動的に導出することを目指し、利用者環境のプライバシーを保護しつつネットワーク全体におけるリスク評価・検証技術の研究開発を実施する。

（サ） セキュアでグリーンなクラウドコンピューティング環境の整備（経済産業省）

経済産業省において、経営・事業戦略に柔軟に対応できる伸縮自在で高効率・高信頼な情報システムを、企業や官公庁といったビジネスシーンでユーザーが安心・安全に利用できるよう、クラウドコンピューティングに係る省エネ、セキュリティ及び安定した稼働を確保する信頼性向上に関する技術等についての研究開発を行う。

（シ） スマートフォンにおけるリスクの可視化（総務省）

総務省において、NICT を通じ、スマートフォンの多様な利用形態に応じたリスク評価結果の可視化を行う技術の研究開発を行う。

（ス） イノベーション創出を支える情報基盤強化のための新技術開発（文部科学省）

文部科学省において、科学技術基盤としてイノベーションを支える情報基盤に係る耐災害性強化（分散システム導入や自己修復機能の付加等）等、課題達成に貢献する機能の強化等をより一層推進するため、研究開発を実施する。

（セ） M2M における情報セキュリティの確保に関する検討及び研究開発の推進（総務省及び経済産業省） ※再掲

総務省及び経済産業省において、M2M について、情報の機密性や完全性等が失われた場合、社会的混乱を招くばかりでなく、情報通信技術基盤に対する信頼が損なわれる可能性があることを踏まえつつ、「情報セキュリティ研究開発ロードマップ」に記載のセンサーネットワーク技術等を考慮し、M2M における情報セキュリティ確保に関する検討及び研究開発を実施する。

（ソ） 省リソースデバイスにおける情報セキュリティ技術の研究開発（総務省）※再掲

総務省において、NICT を通じ、スマートメータセンサ等の省リソースデバイスに実装可能な軽量暗号技術や大規模ノードにおける認証・プライバシー保護技術等の研究開発を行う。

（タ） 新たな情報流通形態に対応した情報秘匿・認証・改ざん防止技術の研究開発（総務省） ※再掲

総務省において、NICT を通じ、クラウド等の新たな情報流通形態に対応するため、情報の円滑な利用を妨げず、必要な情報秘匿及び認証を両立するための研究開発を行う。

（チ） サイバー攻撃の解析・検知に関する研究開発 （総務省）

総務省において、利用者の行動特性等を利用した、標的型攻撃等の新たなサイバー攻撃への対策技術に関する研究開発を実施する。

（ツ） 革新的な情報セキュリティ技術の研究開発基盤の構築 （総務省） ※再掲

総務省において、NICT を通じ、潜在型マルウェアの挙動・検知など、サイバー攻撃の検知機能の向上に向けた革新的な情報セキュリティ技術の研究開発・実証実験を実施するため、サイバー攻撃の観測・解析のための研究基盤を構築する。

（テ） サイバーセキュリティ研究開発拠点の構築 （総務省）

総務省において、NICT を通じ、「サイバー攻撃対策総合研究センター（CYREC）」を構築し、サイバー攻撃のモニタリング（観測）・解析の高度化に向け、官民の英知を集めたオールジャパン体制での研究開発・実証実験を実施する。また、同センターにおいては、産業界との連携を強化するとともに、NICTにおける高度情報セキュリティ人材の育成を促進する。

（ト） 制御システムセキュリティに関する研究開発 （経済産業省）

経済産業省において、CSSC が宮城県多賀城市に構築したテストベッド施設を中核として、制御システムのセキュリティ検証方法及び第三者による評価・認証方法に関する研究開発に取り組み、日本発の技術的基盤を確立する。

（ナ） 産業技術総合研究所における研究開発の促進（経済産業省）

経済産業省において、AIST を通じ、拡散するリスクに対して、国民の情報や権利、社会システム等を保護するための情報セキュリティ技術の確立などに向けた先端技術の開発に取り組む。

③ 人材育成

（ア） 情報セキュリティ人材育成プログラムの改訂（内閣官房）

内閣官房において、情報セキュリティをとりまく最新の状況を踏まえ、「情報セキュリティ人材育成プログラム」[80]の改訂を行う。

（イ） リカレント教育の促進（文部科学省）

文部科学省において、高等教育機関等における社会人学生受入れを支援する。

（ウ） 情報セキュリティに関する教育における産学連携の促進（文部科学省及び経済産業省）

a) 文部科学省において、産学連携により実践的教育を推進する体制の構築や、インターンシップや PBL[81]（課題解決型学習）の実施を支援する。

b) 経済産業省において、実践的インターンシップモデルに基づき、企業等と大学・学生のマッチングの支援を行う。

c) 文部科学省及び経済産業省において、産業界と教育界が協力して作成された授業や教材のデータベースを拡充するとともに、その利用促進を図る。

（エ） 大学等における情報セキュリティに関する教育（内閣官房、総務省、文部科学省及び経済産業省）

a) 文部科学省において、複数大学や産学連携による高度で実践的な教育活動の支援を行う。

b) 内閣官房、総務省、文部科学省及び経済産業省において、情報セキュリティに関する研究科等の設置に資するよう、情報セキュリティに関する最新の情報を大学等に対し積極的に提供する。

（オ） 情報セキュリティに係る競技会・演習等の実施（総務省及び経済産業省）

a) 経済産業省において、若年層のセキュリティ意識向上と突出した人材の発

[80] 2011 年 7 月 8 日 情報セキュリティ政策会議決定。
[81] Project Based Learning の略。

掘・育成を目的としてIPAと「セキュリティ・キャンプ実施協議会」[82]にて共催してきたセキュリティ・キャンプについて、さらなる充実を図るとともに、キャンプ卒業生の社会における採用・活用を促進するなどさらなる深化を図る。

b) 経済産業省において、情報セキュリティをテーマとした様々な競技を通して、攻撃・防御両者の視点を含むセキュリティの総合力を試すハッキングコンテスト「CTF[83]」について、2012 年度に初めて各地域にて開催した。今後、成果を踏まえてNPO 法人日本ネットワークセキュリティ協会及び企業が共同で開催地域拡大や競技内容の向上を図り、さらなる人材候補者を増やすべく、大学等との連携や多用なコンテストの在り方を検討するとともに、同協会で実施するコンテスト(「SECCON CTF 2013」)について経済産業省において普及・広報の支援を行う。

c) 総務省及び経済産業省において、情報セキュリティ人材が、最新の防御モデルに基づくサイバー攻撃への対処方策を体験できるような演習を実施する。

(カ) 横断的キャリアパス・モデルの普及、人材育成計画の策定促進 (経済産業省及び関係府省庁)

経済産業省において、関係府省庁と協力し、IPA が策定した情報セキュリティ人材のキャリアパス・モデルの普及に努めるとともに、企業等における人材育成計画の策定を促進する。

(キ) スキル、資格、教育プログラム等の整理 (経済産業省)

経済産業省において、情報セキュリティ関連業務で求められるスキルと関連する資格、教育プログラムを整理した結果の普及浸透を図るとともに、当該結果を共通キャリア・スキルフレームワークに反映し、普及浸透を図る。

(ク) 情報セキュリティ資格の周知及び普及 (内閣官房、総務省及び経済産業省)

a) 内閣官房及び経済産業省において、情報セキュリティ人材を含めた高度IT 人材の育成強化のため、情報セキュリティ分野を含めた各種情報分野の

---

[82] 次代を担う日本発で世界に通用する若年層のセキュリティ人材を発掘・育成するため、産業界、教育界を結集した講師による「セキュリティ・キャンプ」(22 歳以下を対象) を実施し、それを全国的に普及、拡大していくことを目的とした協議会。

[83] Capture The Flag の略。

人材スキルを測る情報処理技術者試験について一層の周知及び普及を図る。

b)　内閣官房、総務省及び経済産業省において、民間における情報セキュリティ専門家の充実の観点から、民間の情報セキュリティに関する資格及び教育プログラムについて一層の周知及び普及を図る。

（ケ） 情報セキュリティに関する国家試験の改善 （経済産業省）

経済産業省において、企業等における情報セキュリティ人材の必要性が高まっていることを受け、情報セキュリティを含む IT 能力を評価する情報処理技術者試験について、「情報セキュリティスペシャリスト試験」等の普及を図るとともに、社会ニーズに対応した更なる試験内容改善の検討を行い、結論を得る。

（コ） IT スキル標準の活用（公共機関での活用を含む）（経済産業省）

経済産業省において、IPA において整備・普及をすすめている IT スキル標準を活用し、実践的な教育プログラム等に関する大学等専門教育課程の充実化、産学連携の強化などセキュリティレベルに対応した多様な資格・能力評価制度の在り方などを検討し、結論を得る。

（サ） 先端的な研究者等の国際会議への参加支援等（内閣官房及び関係府省庁）

内閣官房において、各府省庁と協力し、国際会議への参加支援や我が国で国際会議を開催するなどにより、グローバルに活躍できる人材の育成を行う。

（シ） 大学に対する情報セキュリティに関する最新情報の提供 （内閣官房、総務省、文部科学省及び経済産業省） ※再掲

内閣官房、総務省、文部科学省及び経済産業省において、大学における情報セキュリティに関する教育の実施に資するような情報セキュリティに関する最新情報を提供する。その一環として、大学の自主的な判断に基づく情報セキュリティに係る資格試験合格による単位認定の導入、資格に関する学習プログラムの導入、経営学修士課程等における情報セキュリティ関連講義の実施等の検討に資する情報を提供する。

（ス） 情報セキュリティに詳しい法律家の育成（内閣官房及び関係府省庁）

内閣官房において、情報セキュリティに詳しい法律家の活用に関する事例を

収集し、情報提供を行うなど、関係府省庁と協力し、情報セキュリティ分野をリードし得る司法関係者の育成に資するよう、外部人材の活用等を進める。

（セ） 情報セキュリティ専門家等の育成の促進（内閣官房及び経済産業省）

内閣官房及び経済産業省において、情報セキュリティ対策を組織の内部及び外部から客観的かつ公正に評価できる情報セキュリティ監査知識を有する人材の育成を行う。

（ソ） 情報セキュリティ人材育成に係る枠組みの検討 （経済産業省）

a) 経済産業省において、情報セキュリティ人材を含めた高度 IT 人材の育成のため、産学が自立的かつ継続的に実施するためのプラットフォーム構築の実証を行うなど、産学連携体制を強化する。

b) 経済産業省において、情報セキュリティ人材を含めた高度 IT 人材育成のため、IT サービス産業において求められる次世代の高度 IT 人材像を発信するとともに、学生や若手技術者が将来のキャリアパスをイメージできるように、新たな IT サービスビジネスの創造事例をとりまとめ、広報・普及する。

c) 経済産業省において、共通キャリア・スキルフレームワークに基づき、情報セキュリティ人材を含めた高度 IT 技術者のスキル標準を一層高度化、共通化する。

d) 経済産業省において、アジアでの更なるセキュリティ人材の育成を図るため、アジア 11 ヶ国・地域と相互・認証を行っている「情報処理技術者試験」について、我が国の情報処理技術者試験制度を移入して試験制度を創設した国（フィリピン、ベトナム、タイ、ミャンマー、マレーシア、モンゴル）が協力して試験を実施するための協議会である ITPEC[84]がアジア統一試験を実施しているところ、ITPEC の取組を拡大するとともに、我が国の IT スキル標準を普及させていく。

（タ） 制御システムセキュリティに係る人材育成 （経済産業省）

経済産業省において、CSSC のテストベッド施設を活用し、制御システムセキュリティに係る人材育成のための研修等を実施する。

---

[84] IT Professionals Examination Council の略。

（チ） 内閣官房情報セキュリティセンターや独立行政法人等を活用した人材育成（内閣官房、総務省及び経済産業省）

内閣官房、総務省及び経済産業省において、内閣官房情報セキュリティセンター、NICT、AIST、IPA が優秀な人材を輩出する中心的機能を果たすことを目標として、関係機関との連携を強化するための連絡会を開催する。

（ツ） 政府機関等による民間セキュリティ人材の一時的受入れ（内閣官房及び関係府省庁）

内閣官房において、各府省庁と協力し、政府機関や独立行政法人等がハブとなり産学官のセキュリティ関連業務を交互に経験できる機会を設けることなどにより、幅広いネットワークの形成を図り、情報セキュリティ人材を育成する。

（テ） 優秀な外部人材の活用（内閣官房及び関係府省庁） ※再掲

内閣官房において、優秀な外部人材の活用に関する事例を収集し、情報提供を行うなど、各府省庁と協力し、官民の人事交流等により情報セキュリティに係る外部人材の活用を進める。

④ リテラシー向上

【 初等中等教育段階における取組 】

（ア） 初等中等教育段階における情報に関する教育（文部科学省）

a) 文部科学省において、学習指導要領の改訂等を踏まえ、発達段階に応じ、情報セキュリティを含む情報モラルに関する教育を積極的に推進する。

b) 文部科学省において、初等中等教育に携わる全ての教員並びに教育委員会及び学校の全ての管理職等の情報セキュリティに関する基本的な知識を含む情報通信技術の活用指導力の向上を目指した取組が地方公共団体等において進められるよう、各地域で情報教育を推進する中核的な役割を担う指導主事、リーダー的教員等を対象とした研修や指導方法等に関する情報交換の機会の提供等を行う。

【 高齢者層などリテラシーの強化が必要とされる層における対策 】

（イ） 情報セキュリティ・サポーターの育成・活用（総務省）

総務省において、利用者の身近なところで利用者を支援する情報セキュリティに詳しい人（情報セキュリティ・サポーター）を育成・活用する活動を支援し、国民全体の情報セキュリティの底上げを行う。

（ウ） 情報セキュリティ相談窓口の充実（内閣官房及び関係府省庁）

内閣官房において、各府省庁と協力し、各府省庁が既に設置している情報セキュリティに関する相談窓口について、国民・利用者の視点に立ち、連携を強化するなど、相談体制を充実させる。また、消費者保護全般を担当する消費者庁と内閣官房及び関係府省庁が連携して、消費者に対する窓口相談対応力を強化する。

【スマートデバイスへの対応】

（エ） スマートフォン等による安心・安全な無線 LAN の利用の推進（総務省）

総務省において、スマートフォン等の普及により急増するモバイルトラヒックに

対処するため、利用者が適切な情報セキュリティを確保しながら、無線 LAN にオフロードする方策を検討し、電波の能率的な利用を促進する。

（オ） 官民連携・国際連携によるスマートフォン等の情報セキュリティ確保の推進（総務省及び経済産業省）

a) 総務省及び経済産業省において、スマートフォン等の普及に伴って情報セキュリティ上発生する問題点について、官民連携しつつ技術的な課題等について検討を行い、必要な対策を講じる。

b) 総務省及び経済産業省において、政府や事業者等における技術的対策、サービス運用面での対策、利用者への普及啓発の取組等を定期的に取りまとめ、情報を発信する。

（カ） スマートフォン等におけるフィルタリングの在り方の検討（総務省及び経済産業省）

総務省及び経済産業省において、スマートフォン等に対応したフィルタリングの改善に向け、関係事業者との調整に取り組む。

（キ） スマートフォン時代における利用者情報保護に関する取り組みの推進（総務省）

総務省において、「スマートフォン プライバシー イニシアティブ」[85]に示された「スマートフォン利用者情報取扱指針」に基づき、 業界ガイドライン及びアプリケーションのプライバシー・ポリシーの作成促進及び利用者に対する情報提供・周知啓発等、総合的な利用者保護に関する取組みを推進するとともに、スマートフォンのアプリについて、一般利用者がリスクを認知し、利用などの判断を自ら行うことが可能な仕組みを構築する。

（ク） ソーシャルメディアの利用に係る情報セキュリティ確保方策（内閣官房、総務省及び経済産業省）

内閣官房、総務省及び経済産業省において、近年のソーシャルメディアの利用拡大に伴い、それを狙う攻撃者も増えてきている背景もあることから、ソーシャルメディアの利用に係る情報セキュリティの確保について検討を行うとともに、必要に応じて留意すべき事項等について周知を図る。

---

[85] 2012 年 8 月 7 日「利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会」提言。

３「世界を率先する」サイバー空間の構築

グローバルなサイバー空間に対応するため、閣僚レベルによる発信の強化、国際的なルールづくりへの積極的な参画、海外市場への積極的な展開、能力構築支援や信頼醸成措置等により、「世界を率先する」サイバー空間を構築し、グローバルな戦略空間における貢献力・展開力の強化を目指す。

① 外交

【 基本的な価値観を共有する国等との多角的なパートナーシップの構築・強化 】

（ア） ハイレベルによる戦略的な取組の強化 （内閣官房、外務省及び関係府省庁）

内閣官房、外務省及び関係府省庁において、サイバー空間に関する国際的な議論において、我が国の基本的な価値観が国際的な規範作りに最大限に反映されるよう、ハイレベルによる働き掛け・取組の強化を行う。

【 国際法の適用に関する検討の深化 】

（イ） サイバー空間に関する国際規範作りへの参画等 （内閣官房、総務省、外務省、経済産業省及び関係府省庁）

内閣官房、総務省、外務省、経済産業省及び関係府省庁において、活発化するサイバー空間に関する国際的な議論に対して、二国間の協議・意見交換、国際会議などのマルチの場など、様々な場を活用し、サイバー空間を利用した行為に対する国際法の適用に関する議論や国際的な規範作りに積極的に関与する。

（ウ）「国際安全保障の文脈における情報及び電気通信分野の進歩」に関する政府専門家会合への政府専門家の派遣等による安全保障分野での国際議論への参画（内閣官房、外務省及び関係府省庁）

内閣官房、外務省及び関係府省庁において、国連からの要請に基づき、国連総会決議「国際安全保障の文脈における情報及び電気通信分野の進歩」に基づき設置される政府専門家会合に対し、我が国から政府専門家を派遣する等、安全保障面での議題やサイバーセキュリティ分野における行動規範作りなどに

ついて積極的に寄与する。

【 二国間・多国間の協議・対話等の継続・拡大 】

（エ） サイバーセキュリティ政策に関する二国間対話の強化 （内閣官房、外務省、総務省、経済産業省及び関係府省庁）

内閣官房、外務省、総務省、経済産業省及び関係府省庁において、2013 年度及び 2014 年度、日米サイバー対話、インターネットエコノミーに関する日米政策協力対話等の二国間会合等を開催し、政府一体となった関与を一層強めるような枠組みの構築を通じてサイバーセキュリティに関する個別分野における連携について協議するなどして、米国との連携強化を図る。

また、英国と日英サイバー協議を開催するほか、日 EU インターネット・セキュリティフォーラムを開催するなど、欧州諸国ともサイバーセキュリティ分野に関する協力体制の構築に向けた議論を行うほか、日 EU ICT 政策対話等の場を活用して、サイバー空間に関する議論を実施する。

加えて、インドと日印サイバー協議を開催するほか、アジア諸国とのサイバーセキュリティ分野に関する情報交換、協議等も積極的に行う。

（オ） 海外情報セキュリティ機関との情報交換 （経済産業省）

経済産業省において、NIST、韓国インターネット振興院（KISA[86]）等の各国の情報セキュリティ機関との連携を通じて、情報セキュリティに関する最新情報の交換や技術共有等に取組む。

（カ） 多国間の枠組み等における国際連携・協力の推進 （内閣官房、外務省及び関係府省庁）

内閣官房及び関係府省庁において、MERIDIAN 等の重要情報インフラ防護に係る分野、APEC[87]、OECD 等のグローバルな経済活動に係る分野、IWWN[88]等の国際的な情報共有等に関する分野、FIRST 等のインシデント対応に係る分野、国連や ARF[89]等の国家安全保障に係る分野、ITU[90]や ACF[91]等の ICT 利活用に

[86] Korea Internet & Security Agency の略。
[87] Asia -Pacific Economic Cooperation の略。
[88] International Watch and Warning Network の略。
[89] ASEAN Regional Forum の略。
[90] International Telecommunications Union の略。

係る分野、国際犯罪防止刑事司法委員会や G8 ローマ・リヨン・グループ等のサイバー犯罪対策に係る分野等の様々な分野の国際会合に積極的に参加し、重要インフラ防護、標準化を含むグローバルな取組、インシデント対応、サイバー攻撃への対応等に関して積極的な情報共有を行う。

また、2013 年に開催予定のサイバー空間に関するソウル会議に参加し、セキュリティ分野を含めたサイバー空間における各分野の課題等に対する国際協調・協力に積極的に寄与する。

【 日米安保体制を基軸とした米国との協力の深化 】

(キ) サイバー空間における米国との協力の深化 (内閣官房、警察庁、総務省、外務省、経済産業省、防衛省及び関係府省庁)

2013年5月に開催された日米サイバー対話において、両国におけるサイバー空間に関する幅広い能力を深化させ、日米同盟を強化させるため、サイバー空間に関する脅威情報の交換、国際的なサイバー政策についての連携、それぞれのサイバー戦略の比較、重要インフラに対する共通の脅威に対抗するための取組や計画における協力、及び防衛・安全保障政策におけるサイバーセキュリティ分野の協力について議論が行われたことを踏まえ、第2回日米サイバー対話の開催を含め、サイバー空間における更なる日米協力の深化を図る。

---

[91] APT Cybersecurity Forum の略。

② 国際展開

【 ASEAN 地域等と共に成長できる関係の構築 】

（ア） 日・ASEAN 情報セキュリティ政策会議の推進による日・ASEAN 関係の連携強化（内閣官房、総務省、外務省及び経済産業省）

内閣官房、総務省、外務省及び経済産業省において、我が国との経済関係の深化が進むアジア地域におけるセキュアなビジネス環境の構築、経済活動・技術革新を支える情報通信インフラの信頼性の確保、政府による横断的な情報セキュリティ政策の立案に向けた取組を加速化するため、日・ASEAN 情報セキュリティ政策会議を通じ ASEAN 諸国との連携を強化する。

a) 内閣官房、総務省及び経済産業省において、第 5 回日・ASEAN 情報セキュリティ政策会議の決定事項の着実な推進。

b) 内閣官房、総務省及び経済産業省において、日・ASEAN 友好協力 40 周年記念事業の一環として、ASEAN 諸国におけるセキュリティ水準の向上とサイバーセキュリティ分野における日 ASEAN 間の協力関係強化を図るため、「日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議」を開催。

c) 内閣官房、総務省及び経済産業省において、第 6 回日・ASEAN 情報セキュリティ政策会議をフィリピンで開催。

d) 内閣官房において、第 5 回日・ASEAN 政府ネットワークセキュリティワークショップを東京で開催。

e) 内閣官房、総務省及び経済産業省において、ASEAN 諸国との情報セキュリティ意識啓発共同事業及びサイバー演習等の実施。

f) 内閣官房、総務省、外務省及び経済産業省において、他の ASEAN 諸国への効果波及にも留意しつつインドネシアに対する情報セキュリティ能力向上のための技術協力プロジェクトを実施。

g) 内閣官房及び総務省において、ワークショップの開催等を通じて、我が国と ASEAN 加盟国のネットワークオペレータによって培われた知見や経験の相互共有を促進。

h) 内閣官房、総務省及び経済産業省において、研究や技術面での連携に資するため、我が国と ASEAN 加盟国におけるネットワークセキュリティ分野の専門家の交流を促進。

（イ） 国際連携を活用した普及・啓発活動の実施（内閣官房及び関係府省庁）
※再掲

内閣官房及び関係府省庁において、国際連携を一層推進するため 2012 年 10 月に開始した「情報セキュリティ国際キャンペーン」について、その実施結果等を踏まえ、諸外国と連携しながら国内における普及・啓発を強化する。

（ウ）「情報セキュリティ国際キャンペーン」の実施 （内閣官房及び関係府省庁）
※再掲

内閣官房及び関係府省庁において、ASEAN、欧米を始めとする諸国と国際連携を活用した行事や情報セキュリティ対策に関する情報提供等を行い、国際連携の推進と国内における情報セキュリティ対策の一層の普及・啓発を図る。

（エ） APEC における情報セキュリティ分野の連携推進（総務省及び経済産業省）

a) 総務省及び経済産業省において、APEC 電気通信・情報産業大臣会合で定められた、情報通信分野に関して APEC として目指すべき共通目標において、安全・信頼性のある ICT 環境の推進が含まれていることを踏まえて、我が国と APEC 域内各国・地域との間でネットワークセキュリティ分野における研究開発や意識啓発等の連携を推進する。

b) 経済産業省において、JPCERT/CC を通じ我が国の CSIRT 構築支援活動の経験の蓄積を活かし、APCERT 等の国際枠組みを通じて、APEC 域内各国・地域に対し、対外・対内調整を担う CSIRT の構築及び運用、連携の支援を行う。

（オ） 海外の組織内 CSIRT の構築・運用支援（経済産業省）

経済産業省において、アジア太平洋地域等我が国企業の事業活動に関係の深い国や地域を念頭に、CSIRT 構築セミナー等の普及・啓発、サイバー演習の実施等の活動等を行う。

（カ） 各国における対外・対内調整を担う CSIRT の体制強化の支援及び連携の強化（経済産業省）

a) 経済産業省において、JPCERT/CC を通じ、アジア太平洋地域、アフリカ等において、各国における対外・対内調整を担う CSIRT の構築及び運用、連

携の支援を行う。JPCERT/CC における CSIRT 構築支援活動の経験の蓄積をもとに、インシデント対応業務の運用技術やCSIRT間連携／運用に関する経験の共有やサイバー演習の実施のためのツールの提供等の支援を行う。

b) 経済産業省において、FIRST、IWWN や APCERT における活動、及びアジア太平洋地域におけるインシデント対応演習等の活動等を通じ、JPCERT/CC を通じ、各国 CSIRT と JPCERT/CC とのインシデント対応に関する連携を一層強化する。

（キ） ASEAN のビジネス環境整備（ISMS 等）（経済産業省）

経済産業省において、今後、ますますの経済連携が求められる ASEAN 各国において、日本企業が安全に活動でき、また、日本の持つノウハウを ASEAN 諸国と共有できるよう、セキュリティマネジメント導入のためのノウハウ支援や、IPAにおいて整備・推進している情報セキュリティ対策ベンチマーク等のツールの技術提供と導入の支援を実施する。

（ク） サイバー攻撃事前防止・早期対策に向けた取組の推進 （総務省） ※再掲

a) 総務省において、近年、被害が拡大しているサイバー攻撃（DDoS 攻撃等、マルウェアの感染活動）に対処し、我が国におけるサイバー攻撃のリスクを軽減するため、国内外のインターネットサービスプロバイダ（ISP）、大学等との協力によりサイバー攻撃、マルウェア等に関する情報を収集するネットワークを国際的に構築し、諸外国と連携してサイバー攻撃の発生を予知し即応を可能とする技術について、その研究開発及び実証実験を実施する。

b) 総務省において、米国とは、インターネットエコノミーに関する日米政策協力対話にて、サイバー攻撃に関するデータを共有し、研究開発の分野での協力関係を加速化していくべきであるということで一致したことを踏まえ、サイバー攻撃の発生を予知し即応を可能とする技術の研究開発等を効果的に実施するため、データの共有を開始しているところであり、引き続き、米国との情報共有を強化する。

c) 総務省において、欧州連合（EU）とは、引き続き、ネットワーク上の攻撃の軽減のための共同研究の実施等の課題について議論を進める。

d) 総務省において、ASEAN 諸国とは、既に着手済みであるインドネシア、タイ、マレーシアとのサイバー攻撃の観測データの共有を足がかりに、他の

ASEAN 諸国との連携を推進する。

（ケ） アジア太平洋地域等での早期警戒情報の共有促進（経済産業省）

a) 経済産業省において、アジア太平洋地域等を対象としたインターネット定点観測情報共有システム（TSUBAME）に関し、運用主体の JPCERT/CC と各参加国関係機関等との間での共同解析やマルウェア解析連携との連動等の取組を進める。また、アジア太平洋地域以外への観測点の拡大について調整を進める。

b) 経済産業省において、アジア地域の CSIRT を中心とするメンバ間で共同又は連携して、サイバー攻撃に対して効果的な対策の検討、策定を行うため、JPCERT/CC において、攻撃に利用される技術や手法及びその傾向、地域特性等を分析し、分析手法や分析結果の共有方法について検討を進める。

（コ） 途上国向け研修・セミナー等の開催（総務省）

総務省において、ネットワークセキュリティ分野における APT[92]加盟国等との国際連携を考慮し、当該国の政府関係者及び電気通信事業者等を対象として、情報セキュリティの動向、技術、政策等に関する研修やセミナー等を実施する。

（サ） 途上国に対する技術援助の推進（サイバー犯罪対策のための刑事司法制度整備）（警察庁、法務省及び外務省）

警察庁、法務省及び外務省において、国境を越えるサイバー犯罪の脅威に対抗するため、特にアジア太平洋地域諸国におけるサイバー犯罪対策に関する刑事司法制度の整備が進むよう、二国間又は多国間の枠組みを活用した技術援助活動を積極的に推進する。

（シ） ソフトウェア開発のアウトソーシング先国等におけるセキュアコーディングセミナーの実施（経済産業省）

経済産業省において、ASEAN 地域等、我が国企業が組込みソフトウェアの開発をアウトソーシングしている先の各国を中心に、脆弱性を作りこまないコーディング手法に関する JPCERT/CC 開催の技術セミナーを実施する。

---

[92] Asia-Pacific Telecommunity の略。

【 日本企業の国際展開の促進 】

（ス） 情報セキュリティ分野での国際標準化への参画 （総務省及び経済産業省）

a) 総務省において、NICT とともに、情報セキュリティ分野の国際標準化活動である ITU-T SG17、ISO/IEC JTC 1/SC27 等が主催する国際会合等に参加し、我が国の研究開発成果や IT 環境・基準・ガイドライン等を踏まえて、国際規格への反映が行われるよう積極的に参画する。

b) 経済産業省において、IPA を通じ情報セキュリティ分野と関連の深い国際標準化活動である ISO/IEC JTC 1/SC27 が主催する国際会合等へ機構職員を派遣し、暗号技術、暗号・セキュリティ製品やモジュールの認証等の国際標準化において、国内の意見が反映されるよう活動する。

（セ） 脆弱性対策に関する国際標準化活動等への参画（経済産業省）

経済産業省において、情報システム等がグローバルに利用される実態に鑑み、IPA 等を通じ脆弱性対策に関するSCAP[93] 、CVSS[94]等の国際的な標準化活動等に参画し、情報システム等の国際的な安全性確保に寄与する。

（ソ） Common Criteria (ISO/IEC15408)における国際協調 （経済産業省）

経済産業省において、IPA による CCRA[95]などの海外連携を通じ、セキュリティ評価に係る国際基準の作成に貢献するとともに、政府調達のための国際共通プロテクション・プロファイル（PP）の開発、情報収集を実施する。

（タ） ハードウェア CC[96]評価・認証制度における欧州との協調関係の構築 （経済産業省）

経済産業省において、IPA を通じ、技術的評価能力の向上に資する最新技術動向の情報収集等を行うため、JIWG[97]及びその傘下の JHAS[98]、JTEMS[99] と定期

---

[93] Security Content Automation Protocol の略。
[94] Common Vulnerability Scoring System の略。
[95] Common Criteria Recognition Arrangement の略。
[96] Common Criteria の略。
[97] Joint Interpretation library WG の略。
[98] Joint Interpretation Library (JIL) Hardware-related Attacks SWG の略。
[99] JIL Terminal Evaluation Methodology Subgroupの略。

的に協議を行う。

（チ） 制御システムセキュリティに関する国際支援 （経済産業省）

経済産業省において、CSSC を中心として、日本産業が強みを持つ分野について、制御システムセキュリティに係る評価・認証の標準化をリードし、各国にも受け入れられるよう働きかけ、協力関係構築を強化する。

（ツ） 制御システムのセキュリティに係る米国との連携推進 （経済産業省）

経済産業省において、米国等との間で制御システムセキュリティに関する評価・認証の相互承認の推進や CSSC のテストベッド施設の運用及び訓練の実施を含む人材育成のための情報共有など、制御システムセキュリティに係る連携を推進する。

（テ） 国際的なルールに基づくセキュリティ製品の貿易の推進 （経済産業省） ※再掲

経済産業省において、日本が強みを持つ複合機や制御システム等の日本製品が貿易において不利な扱いを受けることがないよう、IPA を通じ、セキュリティの国際標準化や評価・認証の国際的な相互承認枠組みに積極的に参画、働きかけを進める。

（ト） 個人情報の保護に関する国際的な取組への対応（消費者庁）

消費者庁において、OECD 情報コンピュータ通信政策委員会情報セキュリティプライバシーワーキンググループ会合、APEC 電子商取引運営委員会データプライバシーサブグループ会合等に出席し、OECD におけるプライバシー法執行の越境的な課題の検討や APEC データ・プライバシー・パスファインダー・プロジェクト等の取組を把握し、国際的な協調の観点から我が国として必要な対応・措置を検討するとともに、我が国の個人情報保護関連法制等について国際的な理解を求める。

③ 国際連携

【 サイバー犯罪対策における連携強化 】

（ア）サイバー攻撃に関する諸外国関係機関との連携の強化 （警察庁及び法務省）

警察庁及び法務省において、サイバー攻撃対策を推進するため、諸外国関係機関との情報交換等国際的な連携を通じて、攻撃主体・方法等に関する情報収集・分析を継続的に実施する。

（イ）サイバー犯罪の取締りのための国際連携の推進（警察庁）

警察庁において、我が国のサイバー犯罪情勢に関係の深い国々の法執行機関それぞれとの効果的な情報交換を実施するとともに、G8、ICPO[100]等のサイバー犯罪対策に係る国際的な枠組みへの積極的な参加、アジア大洋州地域サイバー犯罪捜査技術会議の主催等を通じた多国間における協力関係の構築を推進する。

また、外国捜査機関等とのサイバー犯罪に関する情報交換を継続的に行うとともに、サイバー犯罪に関する最新の捜査手法を修得し、外国捜査機関との連携を強化するため、職員の派遣に向けた検討を進める。

さらに、証拠の収集等のため外国捜査機関からの協力を得る必要がある場合について、外国の捜査機関に対して積極的に捜査共助を要請し、的確に国際捜査を推進する。

（ウ）中央当局制度[101]を活用した国際捜査共助の迅速化（警察庁及び法務省）

警察庁及び法務省において、原則として共助を義務的なものとする日・米、日・韓、日・中、日・香港、日・EU 及び日・露間の刑事共助条約・協定の発効を受け、これらの条約・協定の下で、中央当局を設置し、外交ルートを経由せずに直接中央当局間で共助実施のための連絡を行うことで共助の迅速化を図る。

今後は、更なる刑事共助条約の締結について検討していく。

（エ）サイバー犯罪条約普及への参画 （外務省）

外務省において、我が国が 2012 年7月にサイバー犯罪条約を締結し，同年 11

---

[100] International Criminal Police Organization の略。

[101] 特定の当局を中央当局として指定し、外交ルートを経由せずに中央当局間で共助の授受を行う制度を示す。

月から我が国について同条約の効力が生じたことを受け、2013 年から同条約ビューローや議定書策定作業部会メンバとなり、同条約の普及等に積極的に参画する。

【 情報共有・信頼醸成措置の推進 】

（オ）国際会議等への参加を通じた連携の強化（内閣官房、警察庁、総務省、経済産業省及び関係府省庁）

内閣官房、警察庁、総務省、経済産業省及び関係府省庁において、サイバー攻撃への対応能力を向上させるため、IWWN や FIRST 等の国際連携枠組みへの参加を通じて、諸外国との連携強化を推進する。

インシデント対応調整や脅威情報の共有等、サイバー攻撃への対応能力を向上させるため、JPCERT/CC を通じ、FIRST 等の国際連携枠組みへの参加により、諸外国との連携強化を推進する。

（カ）諸外国との CSIRT 間連携の強化（経済産業省）

インシデント対応調整や脅威情報の共有に係る CSIRT 間連携の窓口としての JPCERT/CC の機能強化を図るとともに、各国の窓口チームとの間の MOU/NDA[102] に基づく継続的な連携関係の維持を図り、迅速かつ効果的なインシデントへの対処を継続する。

（キ）国際的な窓口機能の強化を通じた各国との連携（内閣官房）

a) 内閣官房において、国際的な POC として、情報セキュリティ先進国である我が国の情報セキュリティ政策の基本理念や戦略、官民等のベストプラクティスに関する国際的な広報、情報発信に努める。

b) 内閣官房において、会議等で把握した情報セキュリティ政策に関する国際機関や標準化の動向、海外のベストプラクティス、脅威・脆弱性に関する情報等を国内の関係機関等と共有、還元する。

（ク）重要インフラ分野での国際連携推進（内閣官房、総務省、経済産業省及び重要インフラ所管省庁） ※再掲

[102] Memorandum Of Understanding/Non-Disclosure Agreement の略。

a)　内閣官房において、総務省及び経済産業省と協力し、重要インフラ保護のための国際的な情報共有や連携の促進を目的とする「MERIDIAN」の活動等に積極的に関与するなど、重要インフラ分野での国際連携を促進する。

b)　内閣官房において、重要インフラ所管省庁と協力し、我が国の重要インフラ分野における情報セキュリティ対策の向上に資するため、国際連携や海外の情報収集を通じて得られた IT 障害事例やベストプラクティス等について、国内の関係主体への情報発信を行う。

（ケ）インターネット国際接続の冗長化の推進 （総務省）

総務省において、海外ケーブルの複数ルート化等、日本のインターネットの国際接続の冗長化を推進する。

4 推進体制等

（ア）NISC の機能強化 （内閣官房）

a) 内閣官房において、関係府省庁と協力し、2015 年度を目途とする「サイバーセキュリティセンター」（仮称）への改組に向けて、GSOC の抜本的な強化、サイバー攻撃に関するインシデントに関する情報等の集約、サイバーセキュリティに関する国内外の動向等の実態及び政府の関連施策の現状に関する分析・周知の在り方、国際的なインシデント対応における我が国の窓口 CSIRT 機能の在り方について検討し、結論を得る。

b) 内閣官房において、2015 年度を目途に「サイバーセキュリティセンター」（仮称）へ改組するため、必要となる人材や権限等の組織体制の在り方について検討し、結論を得る。

（イ）各府省庁の情報セキュリティ対策推進のための情報セキュリティ・コンサルティング機能の充実 （内閣官房）

各府省庁の情報セキュリティ対策の推進を支援するため、NISC は、政府機関統一基準群に関連した相談の受付、脆弱性に関する対応策の提案や技術的な助言等、各府省庁の情報セキュリティ対策の推進に向けた様々なニーズへの対応を図るため、情報セキュリティ・コンサルティング機能の充実を図る。

（ウ）関係機関等との連携強化（内閣官房及び内閣府）

内閣官房及び内閣府において、IT 総合戦略本部はもとより、総合科学技術会議、中央防災会議、知的財産戦略本部等、関係する本部・会議との連携を密にし、様々な方策の提案や実施において緊密に協力し、政府全体として情報セキュリティ政策を一体的に推進する。

（エ）情報セキュリティ対策に資する各種ツール・分析等の提供（経済産業省）

経済産業省において、情報セキュリティ対策・プライバシーに関する状況の調査・分析を行うとともに、「情報セキュリティ白書 2013」の編集、作成、出版等を IPA を通じて実施する。

（オ）官民の情報共有の更なる推進 （内閣官房及び関係府省庁）

内閣官房は各府省庁が運用する官民の情報共有ネットワークと政府機関の情報共有ネットワークの結節点の役割を果たすことにより、サイバー攻撃に関する官民の情報共有の更なる推進を図る。

（カ）サイバー攻撃に関するインシデント情報等の政府機関や重要インフラ事業者等の関係機関間における共有の促進 （内閣官房）

内閣官房において、関係府省庁と協力し、サイバー攻撃に関するインシデント情報等の政府機関や重要インフラ事業者等の関係機関間における共有を促進するための秘密の保持の枠組みについて、2015 年度を目途とする「サイバーセキュリティセンター」（仮称）への改組と合わせて整備するため、既存の仕組みの活用の在り方、共有する目的、共有される情報等の内容や共有する者の範囲等の検討を行い、結論を得る。

（キ）サイバーセキュリティに関する国際戦略の策定（内閣官房）

内閣官房において、関係府省庁と協力し、二国間や多国間等による協議・対話の拡大を通じた多角的パートナーシップの強化、我が国が強みを持つセキュリティ技術の国際展開等を政府一体となって加速させるため、サイバーセキュリティに関する国際戦略を新たに策定する。