資料 1-2

情報セキュリティ２０１２

【案】

2012 年　月　日

情報セキュリティ政策会議

目次

Ⅰ　はじめに

我が国の情報セキュリティ政策については、「国民を守る情報セキュリティ戦略」（2010 年５月 11 日、以下「戦略」という。）や、その年度計画である「情報セキュリティ 2010」（2010 年７月 22 日）及び「情報セキュリティ 2011」（2011 年７月８日）に基づき、国民・利用者の視点を重視した様々な情報セキュリティに関する施策を推進している。

しかしながら、情報セキュリティを取り巻く環境の変化は著しく、2011 年度においても、国や国の安全に関する重要な情報を扱う企業等に対する標的型攻撃が多数顕在化するなど新たな脅威が表面化するとともに、スマートデバイス、クラウドコンピューティング[1]、ソーシャル・ネットワーク・サービス（SNS）が急速に一般に普及するなど、情報通信技術の利用形態において大きな変化が起こった。また、サイバー攻撃に係る脅威の増大は、海外主要国でも現実の問題と受け止められ、米英がサイバーセキュリティ戦略を公表するなど各国が政策面における取組を強化するとともに、国連やサイバー空間に関するロンドン会議等において国際的な議論が活発化し国際的規範作り等の気運も高まっている。

本文書は、このような環境変化を踏まえ、これらに的確に対応するため、2012 年度及び 2013 年度に実施する情報セキュリティに関する具体的な取組の重点について、その詳細を示すものである。

なお、情報セキュリティ対策に係る環境に変化が生じた場合には、その変化の内容に応じ、必要な範囲で、迅速に相応の取組を策定・実施する。また、必要に応じ、戦略等の情報セキュリティ政策の枠組みを規定する文書についても見直しを行うこととする。

[1] データサービスやインターネット技術等がネットワーク上にあるサーバ群（クラウド（雲））にあり、ユーザーは今までのように自分のコンピュータで加工・保存することなく、「どこからでも、必要なときに、必要な機能だけ」を利用することができる新しいコンピュータネットワークの利用形態。

II　情報セキュリティを取り巻く環境の変化

2010 年５月に策定した戦略では、その背景となる環境変化を４つに分類し記述した。具体的には、①大規模なサイバー攻撃事態等の脅威の増大、②社会経済活動の情報通信技術への依存度の増大、③新たな技術革新への対応、④グローバル化等である。また、2011 年７月に策定した「情報セキュリティ 2011」では、⑤東日本大震災の発生を環境変化の１項目として加えている。

本章では、これら５分類をベースに、昨今の情報セキュリティを取り巻く著しい環境変化の特徴をとりまとめる。

①　本格的なサイバー攻撃の発生と深刻化

2011 年には、我が国の政府機関において、かねてから海外で発生事例が報告されていた標的型攻撃[2]の脅威が顕在化した。標的型攻撃は一般に情報窃取等を目的に少数の攻撃対象に密かに潜入して行われるものであり、これまでに多数発生していた DDoS 攻撃（分散サービス不能攻撃）のように攻撃を顕示するものとは性格が異なっている。

メールを用いた標的型攻撃では、攻撃対象にあわせて時事情報等を利用し、文面を巧妙化して開封させやすくするなど、高度なソーシャルエンジニアリングの手法が用いられている。また、メールを介して感染したマルウェアが情報システム内に潜伏し、更にネットワーク利用者を管理するサーバへ侵入を試みるなど技術的に洗練されたものもあるが、更に進化すると見込まれている。

2011 年には複数の府省庁に標的型攻撃メールが届き、そのうち、一部の省庁では職員がメールに添付されたファイルを開封し、マルウェアに感染する結果となった。また、衆議院及び参議院にも標的型攻撃メールが送信され、端末がマルウェアに感染したほか、国の重要な情報を扱う一部の企業においても、標的型攻撃メールを介してマルウェアに感染し、情報が窃取された可能性が生じるなど、その被害は広がりを見せている。

このように、我が国の重要な情報の窃取を意図したと想定される本格的なサイバー攻撃が行われており、そのリスクはさらに深刻化するものと見込まれることから、この状況を改善・克服することが強く求められている。

②　社会経済活動の情報通信技術への依存度の更なる高まりとリスクの表面化

近年、モバイルブロードバンドの拡大、スマートフォン等のスマートデバイ

[2] 複数の攻撃手法を組み合わせ、ソーシャルエンジニアリングにより特定の組織や個人を狙い執拗に行われる攻撃。

スの普及、SNS の急速な利用拡大等により、社会経済活動における情報通信技術に対する依存度は、加速度的な高まりを見せている。

スマートフォンは、携帯電話[3]に比べて高機能で操作性が高く、パソコンのように様々なアプリケーションを利用したり、パソコンと同じウェブサイトを閲覧できるなど、小型で高い利便性を備えているため利用者が急速に拡大している。また、パソコンと同じような使い方が可能なことに加え、GPS 位置情報等を取得し利用するアプリケーションが多数存在することから、携帯電話に比べて利用者の個人情報等が集約される傾向にある一方で、多くの利用者は携帯電話と同レベルで安全であると認識しており、パソコン利用者と比較して情報セキュリティに対する意識が低い傾向にある。さらにスマートフォンは、全世界的に利用者が多いこと、セキュリティ対策ソフトの技術が発展途上であること、マルウェア等の作成が容易なオペレーティングシステム（OS）の利用が進んでいること等により、マルウェア等の開発者にとっては、ローコスト・ハイリターンな攻撃対象となっている。このような背景の下、スマートフォンを対象として、個人情報を利用者に無断で外部に送信する等のマルウェア等が拡大している。今後、収集した個人情報を悪用した金銭詐欺等の事案へと拡大する等の可能性もあり、早急な対策が求められる。

その他にも、個人情報等が掲載される傾向にあるブログ、SNS、動画共有サイト等や、データセンターやクラウドサービス等の導入・利用が本格化しており、これらがサイバー攻撃の対象となるおそれが懸念される。ネットワーク接続機器の更なる増加を可能にする IPv6 では、外部ネットワークとの直接接続の容易性に起因する各種攻撃や、IPv4 との併用によるオペレーションミス等によるセキュリティの脅威等が懸念されている。

また、政府においても、電子政府の推進等が行われており、行政サービスにおいても情報通信技術への依存度が更に高まっている。そのような中、電子申請、電子入札等を行うための政府機関の情報システムにおいて広く使用されている暗号アルゴリズム（SHA-1 及び RSA1024）については、理論的な暗号解読アルゴリズムが公開されていることから、コンピュータの処理能力の向上等により、いずれは解読されるおそれがあり、SHA-256 や RSA2048 等への早急な移行が期待されている。また、政府共通プラットフォームや社会保障・税番号制度及び国民 ID 制度が推進されるなど、今後、行政の電子化は一層進展することとなるため、情報セキュリティの確保が不可欠になっている。

さらに、従来の制御システムについては、情報系システムからは独立しており、また、技術も異なっていたことから、セキュリティが高いと考えられていた。し

[3] 本文中では、スマートフォン以外の従来型の携帯電話のことをいう。

かし、近年、情報系システムと同様の技術が採用され、また、情報系システムと相互接続されるケースが増加し、情報セキュリティ上のリスクが高まっている。制御システム、とりわけ重要インフラの制御システムの情報セキュリティの確保は国民生活の安全に直結するものであり、早急な対応が必要である。

このように社会経済活動における情報通信技術への依存度の更なる高まりに伴い、様々なリスクが表面化しており、安心して情報通信技術を利用できる環境整備に向けた取組を推進する必要がある。

③ 新たな技術革新に伴う新たなリスクの出現

通信機器の小型化とネットワークインフラの発達により、家電や自動車、センサーなど様々なデバイスがネットワークにつながるようになり、それぞれが人を介さずに情報交換を行う M2M[4]の利用が広まりつつある。今後、より進化した位置情報技術、インターフェース技術、センサー技術等により、M2M の利用が更に広まれば、社会の幅広い分野で ICT サービスの介在を特段意識せずその恩恵を享受できる環境が整備されると予想される。

しかしながら、M2M の利用に係る環境整備は緒に就いたばかりであり、情報セキュリティ対策を念頭に置いた整備が行われる状況に必ずしもないことに加え、M2M で用いられる各種デバイスの大多数は、これまでネットワークに接続されていない、若しくは、クローズドネットワークを前提に設計されていた。これらがインターネット等へ接続されることにより、新たな脅威への対応が必要となる。例えば、デバイスのパッチ適用やアンチウイルス対策が行なわれていなかったり、暗号化や認証機能が不十分など、情報セキュリティ対策が適切に行われていない場合、デバイス経由で情報が漏えいしたり、デバイスそのものが不正コントロールされてしまうことなどが懸念される。

そのような M2M における情報セキュリティ対策については、従来の人を介在したネットワークに対する情報セキュリティ対策とは異なることから、政府、産業界をあげて早急に検討する必要がある。

④ 重大な情報システム障害のリスク回避に向けた取組の必要性の高まり

東日本大震災の発生は、電力の喪失や建物の損壊・ネットワークの寸断等、複合的な被害が発生した。これら教訓を受け、災害時に取り組むべき対策やリ

---

[4] M2M （エムツーエム、Machine-to-Machine の略）とは、ネットワークに繋がれた機械同士が人間を介在せずに相互に情報交換し、自動的に最適な制御が行われるシステムを指す。例としては、各種センサー・デバイス（情報家電、自動車、自動販売機、建築物、スマートフォン等）を、ネットワークを通じて協調させ、エネルギー管理、施設管理、経年劣化監視、防災、福祉等の多様な分野のサービスを実現するなど。

スクマネジメントの在り方等の調査が内閣官房情報セキュリティセンター（NISC[5]）において行われた。報告書[6]には、これまでに想定していなかった事項について、優先的に取り組むべき対策と中長期的対策等の課題が示されており、災害時に強靭な情報通信システムの構築に向け、それら課題に着実に取り組む必要がある。

また、2011 年には、携帯電話網におけるデータ通信量の増大、特定口座への振り込み急増等に伴い、携帯電話事業者や銀行の情報通信システムに大規模な障害が発生した。社会経済活動が情報通信技術に依存度を高め、新たな技術・サービスに対する需要が増大する中、情報通信システムには最高レベルの信頼性が求められる。したがって、重大な障害が発生した場合に備え、そのリスク回避に向けた取組を推進する必要がある。

⑤ 諸外国における取組の強化

サイバー攻撃の高度化・多様化に伴うサイバー空間における脅威が高まる中、諸外国において、情報セキュリティに対する戦略的な取組が強化されている。

米国においては 2011 年 5 月にサイバースペースの国際戦略を発表しており、米国及び国際的な安全保障上、経済上の新たな課題を認識すること、基本的自由権、プライバシー権、そして情報の自由な流通という基本原則を維持することなどが基本方針として示されている。また、達成すべき目標として ① 開放性及び共同利用性の確保、② 安全で信頼できること、③ 適切な規範に基づいたサイバースペースの確立を掲げるとともに、将来に向けた取組として、① 各国等との協調を通じた外交、② テロリスト、犯罪者、国家等の脅威に対する諫止及び抑止による防衛、③ 繁栄と安全を両立させたサイバースペースの発展を支えるための施策が重要であるとしている。

他方、英国においても 2011 年 11 月に、新たなサイバーセキュリティ戦略を発表しており、インターネットが社会経済上欠くことのできない革新的な技術であると同時に、考慮しなければならない安全保障上の課題を明らかにした上で、サイバースペースにおける国家安全保障と繁栄を強化するため、適切な法に基づく公平性や透明性を 2015 年までに確保するというビジョンを発表している。このビジョンの下、英国政府が取り組むべき施策として ① サイバー犯罪対策、② サイバー攻撃に対する回復力（レジリエンス）の強化、③ 開放性、

---

[5] National Information Security Center の略。

[6] 「東日本大震災における政府機関等の情報システムに対する被災状況の調査及び分析」（2012 年３月内閣官房情報セキュリティセンター）、「東日本大震災における重要インフラの情報システムに係る対応状況等に関する調査」（2012 年３月内閣官房情報セキュリティセンター）

安定性、そして活力あるサイバースペースの構築、④ 最新の知見の共有と能力向上を掲げている。

また、こうした各国の取組だけではなく、サイバー空間のメリットを享受しつつ国境を越えたサイバー空間における各種脅威に対処するための国際的な規範作りに向けた議論が進んでいる。国連では 2010 年 12 月、国家の ICT 利用に関する規範等について議論すべきことや 2012-13 年に「国際安全保障分野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（国連サイバーGGE[7]）を開催することなどが決議された。これを受け、2011 年 12 月の決議では、同専門家会合において、前記規範等について議論されることが明確化された。また、2011 年 5 月の G8 ドーヴィル・サミットでは首脳宣言においてインターネットがとりあげられた。さらに、同年 12 月に OECD[8]においてインターネット政策原則に関する勧告が採択された。こうした取組に加え、同年 11 月にはサイバー空間に関するロンドン会議が開催されるなど、世界的な国際連携の必要性が認識されたところである。

我が国においても、2011 年度はロンドン会議への参画、二国間・多国間の枠組等を通じ国際連携を進めてきたところであるが、2012 年４月に発出された日英共同声明や同月に実施された日米首脳会談においてサイバー問題に関する二国間の連携を深化させる必要性について一致したこと等も受け、より一層の二国間・多国間連携を強化していくことが重要である。

[7] Group of Governmental Experts の略。

[8] Organisation for Economic Co-operation and Development の略。

III　基本方針

II で示した環境変化に対しては、基本的には「国民を守る情報セキュリティ戦略」に示された「基本的な考え方」を踏まえて対応することが適当である。ただし、以下の点については、昨今の著しい変化を踏まえ、特に重点的対応が必要と考えられる。

① 国や国の安全に関する重要な情報を扱う企業等に対する高度な脅威への対応強化

国や国の安全に関する重要な情報を扱う企業等（以下「国等」という。）に対する標的型攻撃の脅威が現実のものとなっており、対応が急務である。

標的型攻撃は、組織内の情報の窃取等を主目的としたものが多いと考えられ、国等が一たびこの攻撃の被害に遭うと、機密情報や個人情報等が窃取され、国の安全や国民生活に深刻な事態をもたらす可能性がある。

また、標的型攻撃は一般に攻撃対象が絞り込まれ、かつ、ウイルス対策ソフトで検出できない未知のコンピュータウイルス等を用いて行われるため、容易に表面化しない。標的型攻撃への対応強化に際しては、従来の対策で重視されたいわゆる入口対策に止まらず、例えば、重要情報の暗号化、出口対策等多段の対策を講じる必要があるが、確実な対応方法は確立されていない。

このような中、標的型攻撃が発覚しにくいものであるが故、何らかの理由で発覚した攻撃に関する情報は、被攻撃者の個人・企業情報等に配慮しつつ、対策手法等を含め関係者間で共有し、更なる攻撃に備えることが有効であると考える。

このため、国等においては、標的型攻撃に係る官民連携の枠組みを構築し、情報共有・分析検討を進めるとともに、それぞれが CSIRT[9]等の機能を有する体制を構築し、関係機関を跨ぐ情報セキュリティ緊急対応要員の整備・充実が求められる。また、研究開発等を進め、標的型攻撃に対する効果的な対応に向けた取組を推進することが重要である。

② スマートフォンの本格的な普及等新たな情報通信技術の広まりに伴うリスクの表面化に対応した安全・安心な利用環境の整備

情報通信技術の一層の高度化に伴い、大量の情報がスマートフォンやクラウドコンピューティング等に集積され、その情報が大容量の通信回線を介して瞬

[9] Computer Security Incident Response Team の略。

時にやり取りされる。情報セキュリティの確保が不十分な場合、これらの情報は容易に窃取され、悪用されるリスクに晒されることになる。

スマートフォンは、多様な経路によるインターネットへの接続やアプリケーションのダウンロード等が容易であるなど利便性が高い一方、マルウェアも簡単にダウンロードされるなど、携帯電話と比較して情報セキュリティ上の課題が多い。スマートフォンを狙ったマルウェアは急激に増加しており、スマートフォンを巡る脅威は日々変化している。

このような中、多くのスマートフォン利用者は、携帯電話とスマートフォンの情報セキュリティ上の相違を十分に認識していると言えず、最低限取るべき情報セキュリティ対策が必ずしも十分には行われていない状況にある。今後、スマートフォンの更なる高機能化と一層の普及が見込まれることから、スマートフォン利用者に情報セキュリティ上の必要な対策を広く周知するとともに、スマートフォンの高機能化や脅威の動向等に応じた必要な技術的対策の確立に努める必要がある。加えて、青少年保護の観点で携帯電話等に導入されているフィルタリング技術のスマートフォンへの有効な導入方策の検討が求められる。

また、個人情報や企業情報等が大規模に集積されているクラウドコンピューティングやSNS、国民生活の安全に直結する制御システムについても、一層の情報セキュリティの確保に向けた取組が不可欠である。

さらに、近い将来、スマートグリッドをはじめとするM2Mの利用が拡大すると見込まれている。この結果、人が認識しない中で大量の情報がやりとりされ、その情報を基に機械的に最適と判断された状態に移行していくこととなる。これらのネットワークに係る情報セキュリティが侵された場合、システム全体が予期せぬ方向に向かうことも想定され、今後、M2Mに係る情報セキュリティの確保も、重要な課題として取り組むべきである。

③ 国際連携の強化

サイバー攻撃の脅威に対する危機感は世界中で高まっており、今や情報セキュリティの確保は世界各国共通の課題である。

このような中、国連における議論やサイバー空間に関するロンドン会議等を契機に、国際的な枠組み作りへの取組が急速に進展しようとしている。各国の思惑が交錯する中、我が国の情報セキュリティに対するポジションを踏まえた枠組み作りがなされるためには、ハイレベルによる戦略的な情報発信を含め国際的な枠組み作りへの積極的な参画が極めて重要である。

また、国際的な枠組み作り以外に関しても、国際的な連携を構築することが

重要である。日米・日英・日 EU・日 ASEAN[10]等多様な場を通じて構築してきた連携の輪を広げ、確実にする取組を継続する必要がある。

情報セキュリティ政策の国内における展開や国際的な枠組み作りへの参画は、我が国として明確な基本方針の下に行われるべきである。その基本方針とは、「情報セキュリティ 2011」でも示したところであるが、インターネットの「開放性(Openness)」、「相互運用性(Interoperability)」を確保しつつ、安全で信頼できるサイバー空間を確保することである。具体的には、インターネットのもたらす社会的・経済的便益を踏まえつつ、情報セキュリティの確保、通信の秘密の保護、個人情報の保護、知的財産権侵害対策等の課題に配慮し、国境を越えた自由な情報の流通を阻害することのない、バランスのとれたアプローチをとることとする。

[10] Association of South East Asia Nations の略。

IV　具体的な取組

II及びIIIで述べた情報セキュリティを取り巻く環境変化や基本方針を踏まえ、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、2012年度中に実施するものである。

１ 標的型攻撃に対する官民連携の強化等

標的型攻撃を始めとする本格的なサイバー攻撃への対応能力の強化を図るため、官民における情報共有に係る連携強化を図るとともに、各府省庁にCSIRT等の体制を整備しその連携強化を図るなど、政府機関における対処態勢を整備する。

我が国全体としての対応能力を向上させるよう、サイバー攻撃に係る高度解析機能を整備するほか、データベースや分析環境の構築、高度な検知技術等の研究開発等を推進する。

ア 官民の連携強化

(ｱ) 官民の情報共有の更なる推進（内閣官房及び関係府省庁）

NISC 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。

(ｲ) サイバーインテリジェンス対策[11]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。

(ｳ) サイバー情報共有イニシアティブの強化（経済産業省）

サイバー情報共有イニシアティブ（J-CSIP[12]）については、参加団体の増加に向けた取組や諸外国との連携に向けた取組を行う。

(ｴ) テレコムアイザック官民協議会の連携強化（総務省）

テレコムアイザック官民協議会における情報共有体制の強化に向けた取

[11] 「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」をいう。

[12] Initiative for Cyber Security Information sharing Partnership of Japanの略。

組を行う。

(ｵ) 平時からの情報共有体制の構築（内閣官房及び全府省庁）

内閣官房は、民間の CSIRT や SOC[13]事業者の団体等との定期的な会合や日常的な意見交換ができる体制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。

イ 政府機関における対処態勢の整備

(ｱ) CSIRT 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) 各府省庁は、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、CSIRT 等の機能を有する体制を整備し、遺漏なく継続的な対策の実施に努める。

b) 内閣官房は、政府の調整役 CSIRT として、政府機関の CSIRT 等間の連携・調整を図るための取組を行う。

(ｲ) 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) 各府省庁は、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、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) 内閣官房は、国と直接、契約関係にはなっていないが、国の安全に関する重要な情報を扱う企業等に対する取組方策を検討する。

(ｳ) 標的型攻撃に係る教育訓練の実施（内閣官房及び関係府省庁）

内閣官房は、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。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。

(ｴ) 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）

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、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。

---

[13] Security Operation Center の略。

また、GSOC[14]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。

ウ 対応能力の向上に向けた攻撃手法の解析、対策技術の研究開発等

(ｱ) 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）

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を構築する。

(ｲ) サイバー攻撃事案の実態解明に係る情報収集・分析（警察庁）

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。

(ｳ) サイバー攻撃（インシデント）対応調整支援（経済産業省）

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。2012 年度においては、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の整備を図るとともに、巧妙かつ執拗に行われる標的型攻撃に係る対応手法の整備を行う。

(ｴ) 新しい脅威・攻撃の分析・共有（経済産業省）

（独）情報処理推進機構（IPA[15]）の運営する「脅威と対策研究会」において、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。

(ｵ) 情報の収集・共有のためのインフラ構築支援等（経済産業省）

a) 巧妙かつ執拗に行われる標的型攻撃に係る情報を関係者間で共有し、被害の拡大防止につなげるため、所要のデータベースや分析環境の構築に向けた検討を進めるとともに、情報の収集・共有のためのインフラ構築を支援する。

b) 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（平

[14] Government Security Operation Coordination team の略。

[15] Information-technology Promotion Agency の略。

成 15 年法律第 57 号）のガイドラインに盛り込む方向で検討する。また、検討結果を踏まえつつ、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。

c） IPA の「情報セキュリティ安心相談窓口」及び JPCERT/CC[16]のインシデント対応等の既存の取組を通じた標的型攻撃への対応を継続する。

(カ) 標的型攻撃の対策技術に関する研究開発（総務省）

標的型攻撃に対抗するための対策技術の研究開発を実施する。2012 年度は、標的型攻撃によって組織内部に侵入したマルウェアが、組織内外のネットワークとの間で行う異常な通信の検出技術についてプロトタイプ開発を(独)情報通信研究機構（NICT[17]）にて行う。

(キ) 「新たな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）

サイバー攻撃の高度解析によって得られた解析結果や、研究開発の成果などを活用しつつ、多層防御、出口対策、攻撃予知などを含む新たな発想に基づく「新たな情報セキュリティ防御モデル」のプロトタイプの構築に向けた検討を行うとともに、テストベッドを活用した実践的な演習を行う。

エ 国際連携の強化

(ア) 国際会議等への参加を通じた連携の強化（内閣官房及び関係府省庁）

サイバー攻撃への対応能力を向上させるため、2012 年度には、FIRST[18]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。

---

16 Japan Computer Emergency Response Team/Coordination Center の略。

17 National Institute of Information and Communications Technology の略。

18 Forum of Incident Response and Security Teams の略。

２ 大規模サイバー攻撃事態に対する対処態勢の整備等

大規模サイバー攻撃事態の脅威が現実化していることなどを踏まえ、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や情報収集等の取組により、対処態勢の充実を図る。安全保障面からの取組として、「平成23年度以降に係る防衛計画の大綱」に基づき、サイバー空間の安定的利用のため、サイバー攻撃に対する防衛分野での体制の強化を図る。サイバー犯罪の取締り、サイバー攻撃への対処に係る国際連携の強化等を通じて、サイバー攻撃への対処態勢及び対応能力を総合的に強化する。

ア 対処態勢の整備

(ｱ) 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）

「緊急事態に対する政府の初動対処体制について」（平成 15 年 11 月 21 日閣議決定）等に基づき、各府省庁との連携に重点を置いた具体的な訓練を実施し、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の発生時における政府及び関係機関による迅速・適切な初動対処のための態勢を整備する。

また、上記訓練は次年度以降も継続して実施する。

(ｲ) 情報セキュリティ緊急対応要員の訓練による対処能力の向上（内閣官房及び関係府省庁）

大規模サイバー攻撃事態等に対応できる人材を養成・維持するため、内閣官房や他の政府機関の担当者に対し、訓練を実施する。

(ｳ) 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）

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。

(ｴ) 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）

【再掲：１イ(ｴ)】

(ｵ) 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）

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整備し、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・分析を継続的に実施する。

(ｶ) サイバーテロ対策に係る体制等の強化（警察庁）

サイバーテロ[19]の手段となり得るサイバー攻撃手法の高度化等に対応するため、情報収集・分析体制の強化、サイバーテロ対策要員の事案対処能力・技術力の維持・向上のための部内外における研修の実施等、警察におけるサイバーテロ対策に係る体制等の強化を推進する。

(ｷ) 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）

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。

(ｸ) サイバーインテリジェンス対策に係る官民の連携強化（警察庁）

【再掲：１ア(ｲ)】

イ 防衛分野での体制の強化

(ｱ) サイバー攻撃等対処に係る企画機能の強化（防衛省）

サイバー攻撃等の脅威の増大に対応するため、統合幕僚監部のサイバー企画機能を強化する。

(ｲ) 陸自電算機防護システムの整備等（防衛省）

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。

(ｳ) サイバー防護分析装置の機能強化（防衛省）

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。

---

[19] 重要インフラの基幹システムに対する電子的攻撃又は重要インフラの基幹システムにおける重大な障害で電子的攻撃による可能性の高いもの。

(ｴ) サイバー攻撃等に係る分析・対処及び研究の推進（防衛省）

防衛省の保有する情報システムに対するサイバー攻撃等に関する脅威／影響度の分析・対処能力を更に向上させるために研究試作を行ったネットワークセキュリティ分析装置について、性能確認試験を実施する。また、サイバー攻撃を検知するための研究及びマルウェアの挙動解析研究を実施する。

(ｵ) 情報保証に係る最新技術動向等の調査研究（防衛省）

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等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。

(ｶ) 人材育成及び外国との連携強化（防衛省）

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、米国との連携を強化するため各種会議等への参加を行う。

ウ サイバー犯罪の取締り

(ｱ) 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外の研修の積極的な実施、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、全国協働捜査方式の定着化等、サイバー犯罪への対処態勢を強化する。

(ｲ) デジタルフォレンジック[20]に係る取組の推進（警察庁）

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連携等、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。

(ｳ) サイバー犯罪の取締りのための国際連携の推進（警察庁）

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

[20] 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。

果的な情報交換を実施するとともに、G8、ICPO[21]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。

エ　サイバー攻撃への対処に係る国際連携の強化

(ｱ)　諸外国の関係機関等とのサイバー攻撃に係る情報の共有体制の強化と対処能力の向上（内閣官房及び関係府省庁）

諸外国等との間において、情報の共有体制等、協力関係の構築・強化を図る。

(ｲ)　国際会議等への参加を通じた連携の強化（内閣官房及び関係府省庁）

【再掲：１エ(ｱ)】

(ｳ)　サイバーテロ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）

サイバーテロへの対策を強化するため、諸外国関係機関との情報交換等国際的な連携を強化するなどして、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。

[21] International Criminal Police Organization の略。

３ 政府機関等の基盤強化

標的型攻撃等の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、CSIRT 等の機能を有する体制を各府省庁において整備する。また、大規模なインシデント等により政府として迅速かつ的確に対応すべき事態が発生した際には、政府 CISO[22]を中心として政府が一体となって迅速に対処するとともに、他の府省庁の専門的技能を有する要員による機動的な支援を行うため、情報セキュリティ緊急支援チーム（CYMAT[23]）を設置し、即応体制を整える。

政府としての対応力を高めるため、政府機関情報システムの 24 時間監視を行っている政府横断的情報収集・分析システム（GSOC）の充実、強化を図る。

各府省庁の最高情報セキュリティ責任者（CISO）が中心となって作成・公表している「情報セキュリティに係る年次報告書」（以下「情報セキュリティ報告書」という。）に係る取組を本年度も着実に実施し、一連の PDCA サイクルの運用によって、情報セキュリティ対策の継続的な向上を図る。また、標的型メールに係る教育訓練等の取組などにより、職員一人一人の情報セキュリティ水準の更なる向上に努める。

これらに加え、政府機関等を騙るなりすまし防止のための取組については、暗号技術を利用した対策の導入も含め、本年度も一層の推進を図る。また、クラウドコンピューティング技術、スマートフォン等の利用の増加や大規模災害の発生に備えた情報システムの運用継続への対応、新たな暗号アルゴリズムへの適切な移行等、政府機関を取り巻く情報技術の利用環境の変化へ適切かつ迅速に対応するための取組を着実に実施する。

この他、2012 年 4 月に改定した「政府機関の情報セキュリティ対策のための統一基準群」（以下「政府機関統一基準群」という。）を踏まえ、政府機関における情報セキュリティ対策を実施するとともに、同基準群について必要な見直しを行う。

ア CSIRT 等の体制の整備及び連携の強化等

[22] Chief Information Security Officer の略。

[23] Cyber Incident Mobile Assistant Team の略。

(ｱ) CSIRT 等の体制の整備及び連携の強化（内閣官房及び全府省庁）

【再掲：１イ(ｱ)】

(ｲ) 政府 CISO による一元的態勢の構築（内閣官房及び全府省庁）

内閣官房は、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、発生した際、政府 CISO を中心に政府が一体となった態勢を構築する。

(ｳ) 情報セキュリティ緊急支援チーム（CYMAT）の設置（内閣官房及び全府省庁）

内閣官房は、サイバー攻撃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において、政府として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して機動的な支援を行うため、情報セキュリティ緊急支援チーム（CYMAT）を設置し、即応体制を整える。

(ｴ) 平時からの情報共有体制の構築（内閣官房及び全府省庁）

【再掲：１ア(ｵ)】

イ 政府横断的な情報収集・分析システム（GSOC）の充実・強化

(ｱ) 政府横断的な情報収集・分析システム（GSOC）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) 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 については、2012 年度に機器の更改を行い、機能の強化を図ることとする。また、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は、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) 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。

ウ 最高情報セキュリティ責任者（CISO）の機能強化

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

a) 内閣官房は、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。）を定期的に開催して相互の緊密な連携の強化を図るとともに、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) 内閣官房は、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) 各府省庁の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。その際、情報セキュリティ報告書の客観性・専門性を確保するため、外部監査制度の活用等を推進する。

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り、最高情報セキュリティ責任者が、CISO 等連絡会議の場において報告し、公表する。

b) 内閣官房は、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[24]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) 内閣官房は、上記の評価手法等をもとに、各府省庁及び政府機関全体の情報セキュリティ対策の実施状況に係る評価等を行い、「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、速やかに公表し、情報セキュリティ政策会議に報告する。

エ 政府機関情報システムの効率的・継続的な情報セキュリティ対策の向上

(ｱ) 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」(2010 年５月 11 日情報セキュリティ政策会議報告)に基づき、各府省庁は、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 2013 年

[24] 2012 年４月 26 日情報セキュリティ政策会議において平成 24 年度版を改定。

度末までに着実に実施することにより、情報システムのスリム化や運用効率化を一層推進し、情報セキュリティ対策の向上・効率化を図る。

b) 内閣官房は、サーバ集約化の着実な推進に向けて継続的に状況を把握し、情報セキュリティ政策会議等に報告を行う。

(ｲ) 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）

内閣官房は、各府省庁との協力の下、希望府省庁の主要な公開ウェブ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。

(ｳ) 標的型攻撃に係る教育訓練の実施（内閣官房及び関係府省庁）

【再掲：１イ(ｳ)】

(ｴ) 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) 内閣官房は、各府省庁の情報システム運用継続計画の運用及び維持・改善に資するため、「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」（平成 23 年３月策定）について、東日本大震災の経験を踏まえ、バックアップシステム等の強靱な情報システムの構築等を含めた改善を行う。また、大規模災害時の情報システムの運用継続に向けた対処要件等の検討及び必要な情報の提供等の支援を行う。

b) 各府省庁は、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」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、2011 年度に策定した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。

(ｵ) 「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（内閣官房及び全府省庁）

「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」（2010 年８月 31 日各府省情報化統括責任者（CIO[25]）連絡会議決定）の対象となるオンライン手続を所掌する各府省庁は、本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及び CISO 等連絡会議の場において、専門的知

[25] Chief Information Officer の略。

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、CIO 連絡会議等に報告する。

(カ) 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）

内閣官房は、関係府省庁と協力し、「カウンターインテリジェンス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実施する。

(キ) 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けた取組の推進（内閣官房及び関係府省庁）

「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[26]）等を踏まえた取組を着実に推進する。

(ク) 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）

a) 内閣官房及び総務省は、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) 内閣官房は、他の府省庁の CSIRT 等の要員による支援が可能となるような要員の育成プログラムを検討する。

c) 内閣官房及び人事院は、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) 内閣官房は、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) 各府省庁は、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。

(ケ) 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は、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

[26] 「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。

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、国民に向けて広く周知し、受信側対策の一層の推進を諮る。また、DKIM[27]やS/MIME[28]のように暗号技術を利用した対策の導入を積極的に検討する。

b) 総務省は、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」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[29]」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[30]、DKIM等）等の導入を促進する。

(ｺ) 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は、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）を利用するよう各府省庁に対して促すとともに、当該取組状況を国民に対して広く周知する。

b) 各府省庁は、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。

(ｻ) 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）

内閣官房は、政府認証基盤（GPKI[31]）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推進する。

(ｼ) 災害関連行政情報の公開と二次利用に係る情報セキュリティ対策の検討（内閣官房及び関係府省庁）

災害発生時において、災害・避難・生活等に関連する行政情報を国民等に広く公開し、二次利用も可能となるような取組を推進するに当たり、情報セキュリティの確保について検討を行う。

オ 政府機関における安全な暗号利用の推進

(ｱ) 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

---

[27] Domain Keys Identified Mail の略。

[28] Secure / Multipurpose Internet Mail Extensions の略。

[29] Japan Email Anti-Abuse Group の略。

[30] Sender Policy Framework の略。

[31] Government Public Key Infrastracture の略。

及び全府省庁）

a） 総務省及び経済産業省は、電子政府推奨暗号の監視、電子政府推奨暗号の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は、暗号技術に関する最新の知見に基づき、「電子政府推奨暗号リスト」の改訂を行う。

c） 総務省及び経済産業省は、必要に応じて、電子政府推奨暗号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など、「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」[32]に従った取組を推進する。

d） 内閣官房及び各府省庁は、暗号技術検討会における議論等を参考に、急激な安全性の低下に備え、緊急避難的な対応（コンティンジェンシープラン）に係る発動要件について検討を行い、CISO等連絡会議において当該要件の決定を行う。

e） 各府省庁は、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。

f） 内閣官房は、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。

(ｲ) 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）

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とともに、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。

カ 情報通信技術の利用環境変化に伴う情報セキュリティの確保等

(ｱ) 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）

クラウドコンピューティング技術を活用し、IPv6にも対応する「政府共通プラットフォーム」について、総務省は、情報セキュリティ確保方策を勘案した設計・構築及び運用を開始し、内閣官房は、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。

[32] 2008年4月22日 情報セキュリティ政策会議決定。

(ｲ) 複数の府省庁で共通的に使用する基盤となる情報システムの運用管理に関する体制等の整備（内閣官房及び総務省）

内閣官房及び総務省は、複数の府省庁で共通に使用する基盤となる情報システムの一つである「政府共通プラットフォーム」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、適切な運用管理を行うために必要な事項について整理・検討を行う。

(ｳ) 政府情報システム管理データベースの整備（内閣官房及び総務省）

各府省庁の情報システムを把握するため、情報資産台帳をデータベース化し、政府全体を通じたリスク評価、脆弱性の検出等に利用可能な「政府情報システム管理データベース」を整備・管理する。

(ｴ) 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）

内閣官房は、政府機関においてスマートフォン等を業務利用する際の情報セキュリティを確保するための方策について検討する。

キ 政府機関の情報セキュリティ対策のための統一基準群の見直し

(ｱ) 政府機関統一基準群の適切かつ円滑な運用等に係る方策の検討（内閣官房）

内閣官房において、新たな政府機関統一基準群の枠組みの適切かつ円滑な運用を確保するため、最新の脅威等を踏まえた情報セキュリティマネジメント手法の在り方を検討する。

(ｲ) 政府機関統一基準群の見直しの実施（内閣官房）

内閣官房は、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を踏まえ、政府機関統一基準群の適切な見直しを行う。

(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）

内閣官房は、独立行政法人情報通信研究機構（NICT）、独立行政法人産業技術総合研究所（AIST[33]）及び独立行政法人情報処理推進機構（IPA）との間で

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

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

a) 各府省庁は、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」（平成 23 年４月 21 日経済産業省）を参照しつつ、「IT セキュリティ評価及び認証制度[34]」により認証された製品等を取り扱う。

b) 経済産業省は、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、IPA が運営する IT セキュリティ評価及び認証制度の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。

ク 政府機関情報システムに情報セキュリティ対策が適切に組み込まれる仕組みの構築

(ｱ) 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（全府省庁）

各府省庁は、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組を推進する。

(ｲ) 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）

【再掲：１イ(ｲ)】

(ｳ) 政府機関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の検討（内閣官房、総務省及び全府省庁）

a) 各府省庁は、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

[34] 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、原則公開する制度を指す。

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」を活用するとともに、そのための各府省庁内への普及・啓発を行う。

b) 内閣官房は、「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」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) 各府省庁は、「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」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。

(ｴ) 「情報システムの信頼性向上に関するガイドライン」の活用・普及（経済産業省）

全ての情報システムを対象として、開発運用等のプロセス管理の側面、技術的側面、組織的側面等の総合的観点から、情報システムの信頼性を向上させるために、「情報システムの信頼性向上に関するガイドライン第２版」及びガイドラインへの適合状況を可視化する「情報システムの信頼性向上に関する評価指標（第１版）」を、これをツール化した「信頼性自己診断ツール」も含めて、民間企業や政府機関における活用・普及を促進する。

(ｵ) 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) 「IT セキュリティ評価及び認証制度」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) 「暗号モジュール試験及び認証制度」及び「暗号アルゴリズム確認制度」の運用を推進する。

c) 「IT セキュリティ評価及び認証制度」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・プロファイルの整備を検討する。

ケ 社会保障・税番号制度に対応した情報セキュリティ対策の検討

(ｱ) 社会保障・税番号制度及び国民 ID 制度に対応した情報セキュリティ対策の検討

（内閣官房及び関係府省庁）

社会保障・税番号制度及び国民 ID 制度については、国民の安心と利便性を確保するため、適切な個人情報保護及び情報セキュリティに配慮したセキュリティ対策の具体化に向けた検討を進める。

コ 地方公共団体、独立行政法人等における情報セキュリティ対策の促進

(ｱ) 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) 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[35]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 策定セミナーの開催やアドバイザーの紹介を行う。また、情報セキュリティ監査を促進するため、情報セキュリティ監査セミナーを開催する。

b) 情報セキュリティ取組事例の収集、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) 希望する地方公共団体に対して、Web サーバ等公開サーバの OS、ミドルウェアアプリケーション及び Web アプリケーションの脆弱性のほか、ファイアウォールやルータ等のネットワーク機器の脆弱性の有無を診断し、その対処方法を知らせることでセキュリティ対策強化を支援する。

d) 希望する地方公共団体に対し、いわゆるガンブラー等、ウェブサイトを閲覧しただけで感染するタイプのマルウェアや標的型攻撃の有無について検知し、マルウェアを検出した場合には、その対処方法等を知らせることで、早期復旧を支援する。

e) 地方公共団体から発信する電子メールについて、悪意の第三者が地方公共団体又は地方公共団体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、SPF 等の送信ドメイン認証技術の採用等を推進する。

(ｲ) 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）

教育関係部門での情報セキュリティを確保するため、以下の取組を行う。

a) 情報セキュリティの取組に関する普及・啓発を推進する。

b) 情報セキュリティを含む ICT 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

[35] Business Continuity Plan の略。

割を担う指導主事等を対象とした研修を行う。

(ｳ) 地方公共団体の職員に対する情報セキュリティ関係研修の充実（総務省）

地方公共団体の職員が時間や場所に制約されずに研修を受講でき、情報セキュリティに関する知識を習得することを支援する。

(ｴ) 独立行政法人等における情報セキュリティ対策の推進（独立行政法人等所管府省庁）

a) 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) 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) 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。

(ｵ) 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）

独立行政法人等と、緊急時を含めた連絡体制を整備し、2012 年度内にその実効性の確認を行う。

(ｶ) 行政機関以外の国の機関との連携（内閣官房）

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、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。

サ 内閣官房情報セキュリティセンターの機能強化

(ｱ) 体制の強化（内閣官房）

政府全体の情報セキュリティ対策の推進体制の中核となるべく、官民を問わず優れた人材を積極的に活用する。

こうした体制の下、情報収集の充実、関係機関等との情報の共有・分析機

能の強化を図り、横断的な情報セキュリティ政策の推進において必要となる基礎情報や様々な動向等について調査・検討を行う機能を拡充する。

(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、緊急時における技術的な助言等、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、同センターの専門家による情報セキュリティ・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）

IT 戦略本部はもとより、国家戦略会議、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。

４ 重要インフラの基盤強化

東日本大震災において重要インフラ分野に生じた複合的な障害における教訓を踏まえ、事業継続計画（BCP）において情報セキュリティ上のリスクを十分想定し得るよう「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）」（以下「指針」という。）の内容を充実させる。また、安全基準等の分析・評価にあたり、標的型攻撃、制御システムへの攻撃など最近の環境変化に対応しているか否かの分析・検証を行う。

さらに、重要インフラ分野における横断的な情報共有、分析体制を強化するため、「セプターカウンシル[36]」活動の一層の促進を図り、特に事業者間においても相互に役立つ情報の共有を進める。また、重要インフラ分野共通に起こる脅威の分析、分野横断的演習の実施を通じて、重要インフラ防護対策の向上を図るとともに、重要インフラ分野における国際連携を推進する。

この他、2012 年 4 月に改定した「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」（以下「第２次行動計画」という。）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等の施策を推進する。

ア 「安全基準等」の整備浸透

(ｱ) 「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) 内閣官房は、重要インフラ事業者等の事業継続計画の実効性を確保するための情報セキュリティ対策の在り方について、関係機関等と連携し検討する。その際、関係機関等で検討されている災害対策や事業継続計画のガイドライン等と整合性を図る。

2012 年度は、震災が重要インフラの情報システムの安定運用に及ぼした影響及び重要インフラサービスへの波及状況の実態調査で、情報システムの安定運用の視点で抽出した重要インフラの BCP に盛り込むべき課題をもとに、対策の在り方について取りまとめる。

b) 内閣官房は、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」

[36] 2009年2月に発足した、重要インフラ各分野のセプター(CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response の略。重要インフラ分野における情報共有・分析機能を行う体制。）により構成される共助活動・情報共有の場。

策定にあたっての指針（第３版)」及び同指針対策編の分析・検証を行い、必要に応じて同指針の追補版の検討を行う。

c)　重要インフラ所管省庁は、同指針や各重要インフラ分野の特性を踏まえ、2012 年度末を目処に、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。

(ｲ)　「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）

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〉

2012 年度に「安全基準等」の分析・検証及び改定等の実施状況、震災を踏まえた改善、攻撃の動向、情報システムへの変化等環境変化への対応状況等並びに今後の実施予定等の把握及び検証を実施し、結果を公表する。

〈重要インフラ事業者等に対する調査〉

2012 年度に「安全基準等」の浸透状況、震災を踏まえた改善等に関する調査を実施し、結果を公表する。また次年度の調査のための企画・準備を実施する。

(ｳ)　電気通信システムの安全・信頼性確保（総務省）

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、事故発生状況や事故発生時に電気通信事業者から報告された内容等について、分析・評価等を行い、その結果を定期的に公表する。

また、大規模災害や携帯電話網におけるデータ通信量の増大等を踏まえて、「情報通信ネットワーク安全・信頼性基準」の見直しを行う。

イ　情報共有体制の強化

(ｱ)　「セプターカウンシル」の活動支援（内閣官房）

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」が一層円滑に運用されるよう、重要インフラサービスの維持・復旧能力の向上や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に資する「セプターカウンシル」の活動を支援する。

(ｲ)　共有すべき情報の整理（内閣官房）

a)　情報共有の枠組みを基盤にしつつ、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、共有すべき情報についての整理・充実を行う。

b) 震災対応における課題も踏まえ、重要インフラ事業者にとって有用な情報共有の方法等の検討を加え、2012 年度中に整理結果の取りまとめを行う。

(ｳ) 「重要インフラの情報セキュリティに係る第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) 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、「第２次行動計画」の情報連絡・情報提供に関する実施細目」による情報共有を推進する。

b) 当該情報共有の継続的な改善の観点から、2012 年度末に、実施細目による情報共有の運用状況や「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。

(ｴ) 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) 上記イ）に掲げる情報共有において、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) 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。

(ｵ) 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) 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、2012 年度末を目処に公表する。

b) 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。

(ｶ) 広報公聴活動の充実（内閣官房）

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。

(ｷ) 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）

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。

(ｸ) 重要インフラ事業者向けの啓発セミナー等の実施（経済産業省）

重要インフラシステム等の情報セキュリティに関するフォーラムを IPA や関係団体等の協力により開催する。

(ｹ) 「情報システムの信頼性向上に関するガイドライン」の活用・普及（経済産業省）

【再掲：３ク(ｴ)】

ウ 重要インフラ防護対策の向上

(ｱ) 共通脅威分析の実施（内閣官房）

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。

2012 年度においては、東日本大震災発生時に見られたような同時多発型重要インフラ障害に対しての情報セキュリティ対策として、技術環境や社会環境の変化を加味した相互依存性の見直し、高度化について検討する。

なお、分析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。

(ｲ) 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）

セプター及び重要インフラ事業者等の協力を得て、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。

2012 年度においては、より効果的なシナリオ策定や演習実施における助言方法の在り方の検討等による効果的な演習を実施するとともに、演習後の意見交換会の活性化等による更なる情報共有の活性化及び演習成果の普及促進と演習参加者の拡充の取組について推進する。

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。

(ｳ) 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) 重要インフラ分野（通信、電力、ガス等）を対象に模擬サイバー攻撃の実施等を内容とするサイバー演習を行う。

b) サイバー演習を通じ、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するとともに、我が国の制御システムのセキュリティ対策への示唆を得る。

(ｴ) 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) 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、障害事例データベースの整備・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) 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う。

(ｵ) 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：１ウ(ｳ)】

(ｶ) 重要無線通信妨害対策の強化（総務省）

a) 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) 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、2012 年度に同施設のセンサーを更改する。

c) 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。

エ 制御システムに関する情報セキュリティ上の課題への対応

(ｱ) 制御システムの情報セキュリティ基準の策定及び評価・認証制度構築

（経済産業省）

平成 24 年度中に、主たる実施場所を東北地域とし、制御システムのサイバーセキュリティ検証施設を米国の協力を得つつ構築する。

また、当該検証施設において、評価・認証手法に関する研究を行い、競争力強化に資する国際標準化を推進する。合わせて、評価・認証機関同士の国際相互承認の実現に向けた取組を促進する。

(ｲ) 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）

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。

(ｳ) 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) 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行う。

b) 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等に提供する。

c) 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。

オ 重要インフラ分野における国際連携の推進

(ｱ) 重要インフラ分野での国際連携推進（内閣官房、総務省及び経済産業省）

a) 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[37]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) 我が国の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。

[37] 重要インフラに関する国際会合。

５ 情報通信技術の高度化・多様化への対応

① 急速に普及が拡大している新たなサービスに係るセキュリティの確保

急速に普及が拡大しているスマートフォン、クラウドコンピューティング、IPv6 及び SNS 等の新たなサービスについて、これらに依存する社会経済活動への影響に配意しつつ、標準化や調査研究等、様々な取組による情報セキュリティ確保策を講じる。

ア スマートフォン等に関する情報セキュリティ確保方策

(ｱ) 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) 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) 具体的な脅威や課題を国際的に連携して把握するとともに、対策を検討するため、国際会議や二国間会合の場を捉え、引き続き、積極的な情報交換を実施する。

c) 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。

(ｲ) 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）

【再掲：３カ(ｴ)】

(ｳ) 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）

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。

(ｴ) 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）

スマートフォン等におけるフィルタリングの在り方を検討する。

(ｵ) スマートフォン等の情報セキュリティ対策に係る普及・啓発の推進（内閣官房、総務省及び経済産業省）

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。

(カ) 情報セキュリティに関する講習の実施（警察庁）

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。

(キ) 新しい脅威・攻撃の分析（総務省及び経済産業省）

スマートフォン等を狙ったコンピュータウイルス等を入手し解析を行い、研究開発や、対策の検討、情報発信等に活用する。

(ク) 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。

イ クラウドコンピューティング化に対応した情報セキュリティ確保方策

(ア) 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（総務省及び経済産業省）

社会基盤として使用されはじめたクラウドコンピューティングについて、セキュリティ上の課題を調査し、必要な対策を講じる。

(イ) 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）

【再掲：３カ(ア)】

(ウ) 複数の府省庁で共通的に使用する基盤となる情報システムの運用管理に関する体制等の整備（内閣官房及び総務省）

【再掲：３カ(イ)】

(エ) 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）

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。

(オ) 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。また、監査の枠組みに関する環境の整備の検討を行う。

2012 年度は、クラウドコンピューティングに関する信頼性、互換性、エネルギー効率等を向上させる技術の開発事業を実施する。

(カ) 広域災害対応型クラウド基盤構築に向けた研究開発（総務省）

広域災害時において、被災地のクラウドから遠隔地の安全なクラウドに重要データを迅速に退避させ、業務処理を継続する高信頼かつ大幅に省電力なクラウド間連携基盤の構築に向けた研究開発を推進する。

(キ) 災害に備えたクラウド移行促進セキュリティ技術の研究開発（総務省）

クラウドは、災害時における業務継続性等の確保に有用である一方、情報漏えい等情報セキュリティ上の課題やデータの保管場所・処理方法が不明確であることなどが指摘されていることから、その普及を促進するため情報漏えいを防止する技術等の研究開発を実施する。

(ク) 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）

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。

ウ IPv6 対応、SNS 等に関する情報セキュリティ確保方策

(ｱ) IPv4 アドレスの枯渇に伴う諸課題への対応推進（総務省）

IPv4 アドレスの枯渇により導入が見込まれる IPv4 アドレスの共有環境等において、通信の十分な安全性・信頼性が確保できるよう、情報セキュリティに係る技術的課題を調査し、必要な対策を推進する。

(ｲ) 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）

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を検討する。

2012 年度は、昨年度に実施した検証環境での評価試験の結果を踏まえ、IPv6 ネットワークのための情報セキュリティ対策を体系的に検討し、検証環境を用いた有効性評価を NICT で実施する。

(ｳ) IPv6 環境における脆弱性検証ツールの貸出し（経済産業省）

IPv6 環境において 14 種類の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。

(ｴ) SNS 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）

近年の SNS 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、内閣官房、総務省及び経済産業省は、SNS 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。

(ｵ) 無線 LAN の情報セキュリティ確保の推進（総務省）

a) スマートフォン等の急速な普及による無線 LAN の利用者数の増大、利用者層の拡大、利用形態の変化等を踏まえ、無線 LAN の利用者向けガイドラインである「安心して無線 LAN を利用するために」（平成 19 年 12 月総務省）を改訂し、利用者に適切な無線 LAN の情報セキュリティ対策を提供するとともに、その普及・啓発に努める。

b) 企業等の組織においても無線 LAN の導入が進められていることから、無線 LAN の導入及び運用に当たって考慮すべき事項（運用管理、調達、技術）を示す企業等の組織における無線 LAN の導入・運用に関するガイドラインを策定する。

(ｶ) マルチファンクションプリンタの情報セキュリティ確保方策の検討（経済産業省）

マルチファンクションプリンタの普及が進んでいるところ、情報セキュリティ上の課題や対応策について、早急に検討を行う。

② M2M における情報セキュリティの在り方

スマートグリッドをはじめ、今後本格的な普及が予想される M2M について、適切な情報セキュリティ確保策を検討し、研究開発を推進する。

(ｱ) M2M における情報セキュリティの在り方の検討及び研究開発の推進（内閣官房、総務省及び経済産業省）

M2M においては、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、M2M における情報セキュリティの在り方の検討を行い、情報セキュリティ確保の観点も踏まえた研究開発を推進する。

(ｲ) スマートグリッドにおける情報セキュリティの在り方の検討（総務省及び経済産業省）

スマートグリッドについて、情報セキュリティが確保されるようセミナー等のあらゆる場を通じた検討を行う。

(ｳ) スマートグリッドの情報セキュリティ確保に向けた研究開発(経済産業省)

スマートグリッドについて、情報セキュリティの確保の観点も踏まえた研究開発を実施する。

(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）

スマートメータやセンサなどでデータの収集を行う際、当該データの情報セキュリティの確保やプライバシーの保護は重要な課題である。このような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などの研究開発を行う。

③ 脅威の高度化・多様化に対するその他の対応

脅威の高度化・多様化に的確に対応するため、情報セキュリティインシデントへの対応能力の維持・向上、ソフトウェアの脆弱性対策等に取り組むほか、安全な電子商取引の推進、中小企業に対する情報セキュリティ対策の取組を推進するための環境の整備等に向けた取組を推進する。

ア 情報セキュリティインシデントへの対応の強化

(ｱ) サイバー攻撃停止に向けた取組の推進（総務省及び経済産業省）

悪意のある第三者からの遠隔操作によりサイバー攻撃等を行うコンピュータプログラム（ボットプログラム）の感染を防ぐ対策、ボットプログラムに感染したコンピュータからのスパムメール送信やサイバー攻撃等を迅速かつ効果的に停止させるための対策等について、2010 年度までに構築して来た枠組みを基礎として、継続的な取組を関係組織で実施する。また、インターネットサービスプロバイダ（ISP）がこのような利用者の情報セキュリティ確保に向けた取組に参画できるよう、その方策について検討を行う。

さらに、我が国の取組について、海外関係機関との間で必要な情報交換等を実施する。

(ｲ) 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) 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) 米国とは、2011 年度に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、2012 年度は米国と具体的な議論を進める。

c) 欧州連合(EU)とは、2012 年度に日 EU インターネット・セキュリティフォーラムを開催し、ネットワーク上の攻撃の軽減のための共同研究の努力の実施等の課題について議論を進める。

d) ASEAN 諸国とは、既に着手済みであるインドネ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。

(ｳ) 危害サイト回避に向けた取組の推進（総務省）

ユーザーがマルウェア等を配布する危害サイトへアクセスすることを電気通信事業者等との連携により回避する仕組みについて、2011 年度まで実施した実証実験の成果の活用を図る。

(ｴ) 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) 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) 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手法について、検討を進める。

c) 2012 年度においては、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の整備を図るとともに、巧妙かつ執拗に行われる標的型攻撃に係る対応手法の整備を行う。

d) 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も踏まえた所要の見直し等の検討を行う。

(ｵ) 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）

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。

(ｶ) SOC 事業者における標準的な契約、ひな形約款の策定に向けた検討（内閣官房、総務省及び経済産業省）

SOC 事業者における脅威に関する情報を、SOC 事業者と諸機関が共有できるような標準的な契約、ひな形約款の策定に向けた取組を行う。

(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）

情報通信ネットワークを誰もが安心・安全に利用でき、かつそれを支えるセキュリティ技術の存在を利用者に意識させない世の中の実現を目指し、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、理論と実践を高度に融合させたネットワークセキュリティ技術の研究開発を実施する。

2012 年度は、ドライブ・バイ・ダウンロード攻撃に対抗するため新たなセキュリティフレームワークの構築を目指し、当該攻撃の観測・分析技術の基礎開発を NICT にて行う。

(ｸ) 情報漏えい対策への取組（経済産業省）

a) 個人情報も含む情報漏えい対策に取り組むため、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) 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。

(ｹ) 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）

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を検討する。

イ ソフトウェアの脆弱性対策等

(ｱ) 脆弱性に関する情報収集・提供（経済産業省）

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。

(ｲ) 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) 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) 情報システムの利用者及び開発者等による脆弱性対策のより確実な実施を

促進するため、機構がこれまでに整備したデータベース（JVN iPedia）、及び脆弱性関連情報を利用者やサーバ管理者等に確実に展開するための「MyJVN」（脆弱性対策支援ツール）の機能拡張を行う。

c) 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。

(ｳ) 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) 経済産業省告示[38]に基づき、脆弱性関連情報の届出受付を行い、定期的に受け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) 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とともに、ソフトウェア製品や情報システムの設計、プログラミング、出荷前検査等の各段階において、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) 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、コーディングスタンダードの開発現場への浸透を図るための取組等を行う。

d) 組込み機器や情報家電等の開発者に利用されて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開発者に提供する。

e) 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」をセットにして普及啓発に努める。

f) 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、自動車の情報セキュリティ対策の普及に向けて、自動車に関する最新セキュリティ関連活動及び電気自動車に関する情報セキュリティの課題について調査する。

g) 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ことにより、脆弱性検出技術の普及・啓発活動を行う。

---

[38] 「ソフトウェア等脆弱性関連情報取扱基準」）（平成 16 年 7 月 7 日経済産業省告示第 235 号）

(ｴ) 信頼性を評価するための共通の評価指標の確立（経済産業省）

システム開発プロジェクトにおける定量データによる品質管理を更に推進するために、関係業界団体で策定した各評価指標や定量データを相互に活用できる共通ルール等を確立し、広く普及活動を推進する。

(ｵ) システムLSIのセキュリティ評価・認証体制の強化（経済産業省）

2012 年度は、IC カード等に用いられるシステム LSI について、国内の ISO/IEC15408 に基づくセキュリティ評価・認証の技術向上のため研究開発等を着実に実施する。

(ｶ) 企業の運営するウェブサイトの安全性向上（経済産業省）

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。

(ｷ) 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）

【再掲：４エ(ｲ)】

(ｸ) 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)

【再掲：４エ(ｳ)】

(ｹ) 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。

ウ 安全な電子商取引の推進

(ｱ) 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）

2007 年度に開催された「電子署名及び認証業務に関する法律の施行状況に係る検討会」における検討結果等を踏まえ、企業における電子署名の利活用の普及促進策について、検討を行う。

エ 中小企業に対する情報セキュリティ対策支援

(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) 中小企業に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。

b) 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、2008 年度に作成した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) 中小企業等を対象とした情報セキュリティに係る相談窓口の対応と適切かつ的確な情報提供（経済産業省）

a) 「中小企業情報セキュリティ指導者育成セミナー」を受けた中小企業に指導する立場にある者等が、講習会等の場を活用して情報セキュリティに係る相談を受け付けるとともに、IPA 等の作成する啓発資料・指導用ツール等の紹介及び提供を行う。

b) 中小企業に対し、情報セキュリティに関する情報提供を支援するツール等を提供する。

(ｳ) 中小企業の情報セキュリティ投資を促進する税制の維持（経済産業省）

中小企業における情報セキュリティ対策の促進を図るため、中小企業の情報セキュリティ投資を促進する税制を維持する。

オ スパムメール対策の強化

(ｱ) スパムメール対策の強化（内閣官房、総務省及び消費者庁）

【 e)のみ再掲：３エ(ｹ)】

a) 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用の措置を講じる。

b) 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) 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)　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」(2005 年２月～）を実施する。

e)　内閣官房及び全府省庁は、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、国民に向けて広く周知し、受信側対策の一層の推進を諮る。また、DKIM や S/MIME のように暗号技術を利用した対策の導入を積極的に検討する。

カ　知的財産保護の推進

(ｱ)　インターネット上の著作権侵害の抑止（総務省、文部科学省及び経済産業省）

a)　インターネット上でグローバルに流通する著作権侵害コンテンツを抑止する観点から、正当な権利者に関する情報を共有する仕組みを構築するため、国際的枠組での検討を進める。

b)　二国間政府協議や知的財産保護官民合同代表団（政府と国際知的財産保護フォーラム（IIPPF[39]）により構成）の派遣を通じ、侵害発生国に対して著作権侵害コンテンツ対策の強化を働き掛ける。また、海外のプロバイダに対し、著作権侵害コンテンツを削除させるため、民間企業による一般社団法人コンテンツ海外流通促進機構（CODA[40]）の活用を促進する。

[39] International Intellectual Property Protection Forum の略。

[40] Content Overseas Distribution Association の略。

６ 研究開発、産業振興の推進

「情報セキュリティ研究開発戦略」及びそのロードマップに基づき、新たな防御モデルの確立、安全な通信環境の実現等、能動的で信頼性の高い（ディペンダブルな）情報セキュリティに関する技術の研究開発を推進する。

新たな情報通信技術に対応した情報セキュリティ技術の活用方法の確立、世界を先導する情報セキュリティに関する研究開発の促進などを通じて、我が国の情報セキュリティ産業の活性化や国際競争力の強化に貢献する。

ア 研究開発の推進

(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）

「情報セキュリティ研究開発戦略」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[41]、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う。また、進捗状況の把握の際に、情報セキュリティ研究の活性化の基盤として、科学的な評価フレームワークの確立に向けた検討を行う。

(ｲ) M2M における情報セキュリティの在り方の検討及び研究開発の推進（内閣官房、総務省及び経済産業省）

【再掲：５②(ｱ)】

(ｳ) スマートグリッドの情報セキュリティ確保に向けた研究開発（経済産業省）

【再掲：５②(ｳ)】

(ｴ) 標的型攻撃の対策技術に関する研究開発（総務省）

【再掲：１ウ(ｶ)】

(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）

[41] 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。

2020 年頃の実現を視野に、IP ネットワークの限界を克服し、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。2012 年度は、前年度成果である新世代ネットワークに関わるグランドデザインに基づいたシステムの詳細設計等に取り組む。

(カ) 災害に備えたクラウド移行促進セキュリティ技術の研究開発（総務省）

【再掲：５①イ(ｷ)】

(キ) 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）

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手法を確立するための調査、実証実験等に着手する。

(ク) 量子情報通信ネットワーク技術の研究開発（総務省）

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、NICT にて研究開発を実施する。

(ケ) 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）

【再掲：５③ア(ｷ)】

(コ) 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）

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。

2012 年度は、NICT にて、同機関の 2011 年度の成果を活用し、評価手法に関しての拡張、及びシステムを用いた通信プロトコル評価手法の実用性評価を行う。

(サ) サイバーセキュリティ研究テストベッドの構築（総務省）

サイバーセキュリティの研究開発を促進するため、攻撃トラフィックやマルウェア検体等のセキュリティデータセットの安全な外部利用を可能にするテストベッドを構築する。

2012 年度は、NICT にて当該テストベッドに仮想化技術を応用してマルウェ

ア解析機能を付加するなどの高度化を行うとともに、外部組織との連携の下、テストベッドを運用する。

(シ) 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）
【再掲：５①ウ(イ)】

(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）

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ついて、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）等について、2012 年度より新たに研究開発を開始し、情報基盤の耐災害性強化等、課題達成に貢献する機能の強化等をより一層推進する。

(セ) 新世代の情報セキュリティ技術等の研究開発（経済産業省）

情報技術の社会基盤化に伴い、情報システムに起因する事故が、経済活動全体の停滞や国民生活の生命・財産そのものにかかわるリスクをもたらしかねない状況が生まれつつあることを踏まえ、新世代情報セキュリティ技術の研究開発を2012年度に継続し、対症療法的でなく根本的な問題解決を目指す。

(ソ) 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）

ネットワークにおいて適切な情報セキュリティを確保するに当たっては、その始点から終点までを考慮した総合的な情報セキュリティの管理が重要となることから、ネットワークの各構成要素（ノード）における最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、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 NICT にて行う。

2012 年度は、最適構成の導出に必要な情報セキュリティ知識ベースの構築を行う。

(タ) 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）
【再掲：５①イ(オ)】

イ 情報セキュリティ産業の振興

㈠ 情報セキュリティ産業の振興（内閣官房、総務省及び経済産業省）

我が国の情報セキュリティの水準を高めるためには、それを支える情報セキュリティ産業の活性化が不可欠である。

クラウドコンピューティング、IPv6、スマートデバイス、SNS 等新たな情報通信技術に対応した情報セキュリティ技術やその活用方法の確立、世界を先導する能動的で信頼性の高い（ニュー・ディペンダブル）情報セキュリティに関する研究開発の促進、情報セキュリティに係る高度人材育成などを通じて、我が国の情報セキュリティ産業の活性化や国際競争力の強化に貢献する。

我が国の情報セキュリティ産業を活性化する方策について、「技術戦略専門委員会」の下に設置したワーキンググループにて検討する。

㈡ 制御システムの情報セキュリティ基準の策定及び評価・認証制度構築（経済産業省）

【再掲：４エ㈠】

7 情報セキュリティ人材の育成

情報セキュリティ人材の育成については、「情報セキュリティ人材育成プログラムを踏まえた2012年度以降の当面の課題等について」において提言された、企業等の情報セキュリティ担当者、情報セキュリティ産業人材、先端的な研究者・技術者、政府機関等の情報セキュリティ担当者の四分類の人材の育成等において必要となる施策を着実に推進する。

ア　企業等の情報セキュリティ担当者、情報セキュリティ産業人材、先端的な研究者・技術者

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

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。

(ｲ) スキル、資格、教育プログラム等の整理（総務省及び経済産業省）

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て公表する。

(ｳ) CISO等の設置促進（経済産業省）

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。

(ｴ) リカレント教育の促進（文部科学省）

高等教育機関等における社会人学生受入れを支援する。

(ｵ) 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）

内閣官房情報セキュリティセンター、（独）情報通信研究機構、（独）産業技術総合研究所、（独）情報処理推進機構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。

(ｶ) 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）

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。

(ｷ) 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) 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) 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。

(ｸ) 「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）

【再掲：６ア(ｱ)】

(ｹ) 経営層向けセミナーの開催等（内閣官房、総務省、文部科学省及び経済産業省）

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を開催するとともに、経済団体等が主催する会議も活用するなど、あらゆる機会をとら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。

(ｺ) 情報セキュリティに係る競技会等の実施（総務省及び経済産業省）

a) セキュリティキャンプについて、更なる充実を図る。

b) 情報セキュリティ人材が実践的技能を競えるような競技会等の開催について検討する。

c) 競技会等において優秀な成績を残した者の雇用促進につながる普及啓発について検討する。

(ｻ) 表彰等の充実（総務省及び経済産業省）

a) 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。

b) 「未踏 IT 人材発掘・育成事業」を実施する。

(ｼ) 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）

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。

イ 政府機関等の情報セキュリティ担当者

㈠ CSIRT 等の体制の整備及び連携の強化（内閣官房及び全府省庁）

【再掲：１イ㈠】

㈡ 人事ローテーションの工夫（内閣官房及び関係府省庁）

各府省庁等の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検討する。

㈢ 優秀な外部人材の活用（内閣官房及び関係府省庁）

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を活用する人事の在り方を検討する。

㈣ 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）

【再掲：３エ㈦】

㈤ 公務員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）

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よう、関係府省庁に対し要請する。

㈥ 人材育成及び外国との連携強化（防衛省）

【再掲：２イ㈥】

㈦ 重要インフラ事業者における人材育成の促進（内閣官房及び関係府省庁）

重要インフラ事業者において、組織内 CSIRT 等の設置、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、職員の情報セキュリティ意識の啓発と能力の底上げ等、政府に準じた取組を推進する。

また、各セプター内で横断的に実施する研究プログラムを検討する。

ウ 人材類型を跨ぐ横断的課題等

(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) 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) 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 ICT 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検討する。

(ｲ) 大学入試センター試験における情報科の出題に係る検討（文部科学省）

高等学校の教育の実態や大学及び高等学校関係者の意見を踏まえながら、大学入試センター試験において情報科を出題教科とすることについて検討するよう大学入試センターに要請する。

(ｳ) 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）

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。

(ｴ) 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) 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[42]（課題解決型学習）の実施を支援する。

b) 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) 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。

(ｵ) 情報セキュリティに関する事故事例等の共有化の検討（内閣官房、経済産業省及び関係府省庁）

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、情報

[42] Project Based Learning の略。

提供者等に配慮し、学習教材として提供する手法について検討する。

(カ) 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）

外部人材を活用するなどして、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ついて検討を進める。

(キ) 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) 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) 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。

(ク) 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）

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。

(ケ) 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) 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) 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) 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) 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[43]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。

---

[43] IT Professionals Examination Council の略。

８ 情報セキュリティリテラシーの向上等

国民・利用者がITリスクを認識し、自発的に情報セキュリティ対策を実施することができるようにするため、「情報セキュリティ普及・啓発プログラム」に基づき、「情報セキュリティ月間」の充実等、普及・啓発活動を充実・強化する。特に、スマートフォン等の本格的な普及を踏まえた普及・啓発等、環境の変化を踏まえた普及・啓発活動を実施する。

また、情報セキュリティに係る相談窓口や個人情報保護について取組を継続するとともに、サイバー犯罪取締りのための基盤整備及び犯罪抑止のための広報啓発の推進、情報セキュリティガバナンスの確立に向けた取組を行う。

ア 普及・啓発活動の充実・強化

(ｱ) 「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) 「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) 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) 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) 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うにするための情報提供を行う。

(ｲ) 「情報セキュリティ月間」の充実（内閣官房及び関係府省庁）

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、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。

(ｳ) 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）

国際連携を一層推進するため、10 月に国際連携を活用した普及・啓発活動を実施し、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。

(ｴ) 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）【f】のみ再掲：５①ア(オ)】

a) 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」、「フィッシング対策推進連絡会」、「情報セキュリティ安心相談窓口」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) 2012 年度の情報化月間において、情報セキュリティの確保の観点から多大な貢献を果たした個人・企業等を表彰するため、「情報化促進貢献個人等表彰」を実施する。

c) 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) 韓国インターネット振興院(KISA[44])との連携事業として、情報セキュリティ政策の意識を高めるための標語・ポスター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セキュリティ意識の醸成と向上を図る。

e) 更なる情報セキュリティの普及啓発促進を図るため、官民合わせた情報セキュリティ対策の普及啓発資料をまとめたポータルサイトを構築し、広く国民一般に公開する。

f) 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普及啓発を行う。

(オ) 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）

【再掲：７ウ(ア)】

(カ) 大学入試センター試験における情報科の出題に係る検討（文部科学省）

【再掲：７ウ(イ)】

(キ) 電波利用秩序維持のための周知啓発活動の強化（総務省）

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、関係府省庁の協力を受け、各種メディアにより、不法無線局対策の強化等について周知啓発を実施する。

---

[44] Korea Internet & Security Agency の略。

さらに、総合通信局等において、電波の利用機器販売店や製造業者への周知啓発を実施する。

(ｸ) 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）

a) 情報セキュリティ対策ベンチマークを提供する。

b) 情報セキュリティに関する現状と展望等を「情報セキュリティ白書」にとりまとめて、公表する。

(ｹ) 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）

【再掲：３ク(ｵ)】

(ｺ) 非機能要求の合意手法の活用・普及（経済産業省）

情報システムの信頼性向上のために、信頼性、性能、あるいはセキュリティ等に関する要求を含む非機能要求項目について、ユーザー・ベンダ間で適切に合意するための手法の活用・普及について、関係業界等と連携して取り組んでいく。

(ｻ) 情報セキュリティに関する事故等の事例の収集・共有化（内閣官房）

情報セキュリティ事故の未然の防止や、事故が発生した場合に適切に対応するためには、過去に発生した情報セキュリティに関する事故等を検証し、反省、教訓等の共有化を図ることが重要である。既存の公開されている事例を収集するとともに、企業秘密、プライバシー保護等の観点から収集が困難な事例については、匿名化等収集の方法について検討する。収集した情報セキュリティ事故に関する事例等については、多くの人々に利活用してもらえるよう普及に努める。

イ 情報セキュリティ安心窓口（仮称）の検討

(ｱ) 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）

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の強化を検討する。

(ｲ) 情報セキュリティに係る相談窓口の対応と適切かつ的確な情報発信（経済産業省）

マルウェア及び不正アクセス等に関する総合的な相談窓口「情報セキュリティ安心相談窓口」を運用し、コンピュータ利用者が直面する情報セキュリティに係る相談対応を拡充するとともに、その窓口を国民に広く PR する。

さらに、相談を受けた情報等を踏まえ、コンピュータ利用者に対する注意喚起等の対策に反映する。

(ｳ) 情報セキュリティ・サポーターの育成・活用（総務省）

利用者の身の回りの詳しい人（情報セキュリティ・サポーター）を育成・活用を支援し、国民全体の情報セキュリティの底上げを行う。

ウ 個人情報保護の推進

(ｱ) 個人情報保護法の見直し（消費者庁及び関係府省庁）

個人情報保護法について、2012 年度以降、法改正も視野に入れた問題点についての審議を踏まえ検討を行う。

(ｲ) 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）

2012 年度においては、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[45]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。

エ サイバー犯罪取締りのための基盤整備の推進

(ｱ) 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）

【再掲：２ウ(ｱ)】

(ｲ) デジタルフォレンジックに係る取組の推進（警察庁）

【再掲：２ウ(ｲ)】

(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）

[45] Asia -Pacific Economic Cooperation の略。

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、PTA の代表者等で構成する総合セキュリティ対策会議を開催し、情報セキュリティに関する産業界と政府の連携の在り方について検討する。

(ｵ) サイバー犯罪の取締りのための国際連携の推進（警察庁）

【再掲：２ウ(ｳ)】

(ｶ) 中央当局制度[46]を活用した国際捜査共助の迅速化（警察庁及び法務省）

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。

オ 犯罪抑止のための広報啓発の推進

(ｱ) 改正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）

平成 24 年３月に改正された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。

(ｲ) 情報セキュリティに関する講習の実施（警察庁）

【再掲：５①ア(ｶ)】

(ｳ) サイバー犯罪の被害防止対策の推進（警察庁）

[46] 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。

a)　出会い系サイトに関連した犯罪の被害防止のための中学生・高校生向けのリーフレットを作成し、各都道府県警察において配布するとともに、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。
b)　警察庁セキュリティポータルサイト「@police」において、各種ソフトウェアに係るぜい弱性情報、インターネット定点観測情報等の情報セキュリティ関連情報を情勢の変化に応じて適切に提供するなど、犯罪抑止のための広報啓発活動を推進する。

(ｴ)　サイバー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育成・支援の在り方に関する調査研究を実施し、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。

カ　情報セキュリティガバナンスの確立

(ｱ)　情報セキュリティガバナンス確立の促進（経済産業省）

a)　企業の情報セキュリティに係る企業の負担を軽減し、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。
b)　2012 年度は、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において、情報リスクの管理に関する参加企業内での知見の共有を図る。

(ｲ)　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)　「平成 24 年情報処理実態調査」において、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、ISO/IEC15408 認証取得製品の導入状況について調査する。
b)　登録者の負担軽減、及び、利用者の利便性向上のため、監査企業台帳の電子申告等の対応を検討する。また、保証型監査の利用促進を図る。2012 年度は、登録者の負担軽減及び利用者の利便性向上のために監査企業台帳はいかにあるべきかなどについて、監査企業台帳の利便性向上に関する検討会を実施し、報告書をまとめる。また、セミナー等の実施により、保証型監査に関する理解を深め、利用促進を図る。
c)　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。2012 年度は、個別企業への照会等を通じ、情報セキュリティ報告書の普及に努める。

(ｳ) 「情報システム・モデル取引・契約書」の活用・普及（経済産業省）

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）」（2007 年公表）、「情報システム・モデル取引・契約書（追補版）」（2008 年公表）、「e ラーニングで学ぶモデル取引・契約書」（2009 年公表）及び「情報システム・ソフトウェア取引トラブル事例集」（2010 年公表）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。

キ 情報システム障害等による社会混乱の防止

(ｱ) 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）

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・信頼性等を総合的に評価・認証する枠組みを、2013 年度を目途に構築し、利用者への品質説明力を強化する。

９ 制度整備

サイバー犯罪条約の早期締結に向けた準備、サイバー刑法、改正不正アクセス禁止法の円滑な施行を行う等、サイバー空間の安全性・信頼性を向上させる取組を実施する。

ア サイバー空間の安全性・信頼性を向上させる制度の検討等

(ｱ) サイバー刑法の円滑な施行（法務省）

サイバー犯罪に適切に対処するとともにサイバー犯罪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）が公布されたことを踏まえ、手続法規定について円滑な施行[47]に向けた準備を進める。

(ｲ) サイバー犯罪条約の締結に向けた準備（外務省）

早期にサイバー犯罪条約を締結するため、関係府省庁と協力して準備を進めていく。

(ｳ) 改正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）

【再掲：８オ(ｱ)】

(ｴ) 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）

【再掲：５③イ(ｹ)】

(ｵ) 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）

【再掲：５③ウ(ｱ)】

イ 各国の情報セキュリティ制度の比較検討

(ｱ) 各国のセキュリティ法制度等の調査（内閣官房）

主要国等の法制度等の調査・分析を進めることで、各国を取り巻く課題及び連携方策について検討する。

---

[47] 施行日：平成 24 年６月 22 日

１０ 国際連携の強化

二国間関係の強化については、日米間で日米サイバーセキュリティ会合や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における議論を深めつつ、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目指すほか、日英サイバー協議等二国間会合などの枠組みを通じて、具体的な協力事項の検討や推進を行う。また、欧州との関係では、欧州委員会等の機関を始めとする関係国との連携を推進する。

ASEAN 地域については、情報セキュリティ共同意識啓発活動の推進、人材育成、技術支援、研究協力、第５回日・ASEAN 情報セキュリティ政策会議の東京での開催等を通じ、更なる連携の強化を図る。

多国間連携の分野としては、サイバーインシデント等への対応に関する協力、重要インフラ防護のための官民連携及び国際連携、情報セキュリティ分野の意識啓発における協力、人材育成における協力などを促進するとともに、サイバー空間における国際的な行動規範作りに対し積極的に寄与する。

ア ハイレベルによる戦略的な取組

(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）

サイバー空間に関する国際的な議論において、我が国のポジション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。

イ 米国、欧州諸国、アジア諸国、ASEAN 等との連携強化

(ｱ) 情報セキュリティ政策に関する二国間政策対話の強化（内閣官房及び関係府省庁）

2012 年度中に、日米サイバーセキュリティ会合、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を開催しつつ、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等を通じて情報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、米国との戦略的二国間連携の強化を図る。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、欧州諸国とも情報セキュリティを含めたサイバー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、情報セキュリティに関する議論を実施する。加えて、アジア諸国とのサイバー分野に関する情報交換、協議等も積極的に行う。

(ｲ) 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、総務省及び経済産業省）

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て ASEAN 諸国との連携を強化する。

a) 第 4 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 (2012 年度)
b) 日・ASEAN 情報セキュリティ政策会議を東京で開催（第 5 回、2012 年度）
c) 第 4 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ブルネイで開催
d) 国家戦略策定及び政府ネットワークセキュリティに関する ASEAN 諸国の政府職員向け研修を我が国で開催（2012 年度）
e) ASEAN 諸国との情報セキュリティ意識啓発共同事業の実施（2012 年度）
f) 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（2012 年度）
g) 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（2012 年度）

(ｳ) 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) 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である「沖縄宣言」において、安全・安心な 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) 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。

(ｴ) 途上国向け研修・セミナー等の開催（総務省）

ネットワークセキュリティ分野における APT[48]加盟国等との国際連携を考

[48] Asia-Pacific Telecommunity の略。

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。

(ｵ) 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）

2012 年度においては、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。

(ｶ) アジア域内のセキュアなビジネス環境の構築推進（経済産業省）

アジア版情報セキュリティ対策ベンチマークへの機能変更及びアジア諸国への普及・情報交換を行うための事業を実施する。

(ｷ) 海外の組織内 CSIRT の構築・運用支援（経済産業省）

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 の構築及び運用、連携の支援を行う。2012 年度においては、CSIRT 構築セミナー等の普及・啓発、技術支援活動等を行う。

(ｸ) 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) アジア太平洋地域等において、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。2012 年度においては、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等の支援を行う。

b) FIRST、IWWN [49]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、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。

(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) 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) 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

[49] International Watch and Warning Network の略。

攻撃に対して効果的な対策の検討、策定を行うため、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) サイバー犯罪の取締りのための国際連携の推進（警察庁）

【再掲：２ウ(ｳ)】

(ｻ) 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：５③ア(ｲ)】

(ｼ) 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）

【再掲：５①ア(ｱ)】

(ｽ) スパムメール対策の強化（内閣官房、総務省及び消費者庁）

【再掲：５③オ(ｱ)】

ウ 各種国際会合を活用した国際連携・協力の推進、情報共有体制等の強化

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

MERIDIAN 等の重要情報インフラ防護に係る分野、APEC 、OECD、ASEAN 等のグローバルな経済活動に係る分野、IWWN 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[50] 等の国家安全保障に係る分野、ITU[51]や ACF[52]等の ICT 利活用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、2012 年に開催予定のサイバー空間に関するブダペスト会議に参加し、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。

(ｲ) 「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）

---

[50] ASEAN Regional Forum の略。

[51] International Telecommunications Union の略。

[52] APT Cybersecurity Forum の略。

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。

(ｳ) 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、外務省及び関係府省庁）

昨年以降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、サイバー空間におけ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。

(ｴ) 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）

【再掲：10 イ(ｸ)】

(ｵ) アジア地域における情報セキュリティ評価・認証技術向上のための取組（経済産業省）

情報セキュリティ評価・認証の国際的な相互承認協定のアジア地域における推進を目的に、セキュリティ評価・認証の技術や動向について情報交換を行う。

(ｶ) 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）

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/SC 27、ITU-T SG17 等が主催する国際会合等に参加し、我が国の 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。

(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（経済産業省）

【再掲：５①イ(ｸ)】

(ｸ) APEC における情報セキュリティ分野の連携推進（総務省）

【再掲：10 イ(ｳ)】

エ NISCの窓口機能の強化

(ｱ) 国際的な窓口機能の強化を通じて各国との連携（内閣官房）

a) 国際的なPOC[53]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。例えば、2012年度中に本文書の英語版をNISCのウェブサイト[54]に公開するなど、ウェブサイト等を通じた積極的な広報活動を展開する。

b) 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。

[53] Point of Contactの略。

[54] http://www.nisc.go.jp/eng/index.html