情報セキュリティ２０１１

2011 年７月８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）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、クラウドコンピューティング[1]、SNS（ソーシャル・ネットワーク・サービス）、スマートフォン等の急速な普及といった情報通信技術の利用形態の急速な変化、「Stuxnet」に代表される新たな攻撃や 2010 年９月に発生した我が国の政府機関等に対するサイバー攻撃等の脅威の複雑化・高度化、政府機関における情報漏えい等、情報セキュリティを取り巻く環境の変化は著しい。加えて、2011 年３月の東日本大震災の発生に伴い、我が国は国家的な危機に直面し、情報通信システムを含む社会の枠組みそのものの在り方についても、適切な対応が求められている。

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、2011 年度及び 2012 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、必要があれば、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。

[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

戦略では、策定の背景として、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案等の脅威の増大、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。戦略は2010年５月に策定したが、その後も様々な環境変化が生じており、これらを踏まえた情報セキュリティ戦略の推進が求められている。

特に、2011 年３月の東日本大震災は、大規模な地震、津波、原発事故等、これまでに経験したことのない複合的な大災害であり、情報セキュリティの分野においても、この大震災を踏まえた早急な取組が求められている。

そこで、既存の４つの環境変化に「東日本大震災の発生」を新たに追加した、５つの環境変化における特徴的な動きや、今後考慮すべき事象を以下に取りまとめた。

① 大規模なサイバー攻撃事案等の脅威の増大（情報セキュリティの脅威の高度化・多様化）

政府機関、民間企業等に対し、多数の攻撃元から行われるサービス不能攻撃（DDoS 攻撃）をはじめとするサイバー攻撃事案が増加しており、我が国においても、2010 年９月に政府機関等に対するサイバー攻撃事案が発生した。ボットネットの拡大や、フィッシング行為やウイルス感染等を目的とするメールを特定の組織・人物に送付する標的型メール攻撃の巧妙化等、攻撃手法も複雑化・巧妙化している。

近年、世界的規模でコンピュータウイルスがまん延しており、いわゆる「ガンブラー」型攻撃等、その手法は年を追うごとに高度化・複雑化している。また、2009 年から 2010 年にかけて、プラント等の制御システムが「Stuxnet」による攻撃を受けた事例等に見られるように、既存の攻撃手法を巧みに組み合わせ、さらに攻撃目標に合わせて設計した攻撃を敢行し得る、APT（Advanced Persistent Threats[2]）と呼ばれる新たな脅威も出現している。

また、民間企業における大規模な情報システム障害や大規模な個人情報漏えい事案も後を絶たず、益々大規模化している。2010 年度には、行政機関内部の

[2] 情報窃取や組織の重要な局面に関する弱体化又は妨害、あるいは将来においてこれらの目的を実現するための準備行為を目的として、標的とした組織の IT インフラ中に足場を構築し利用し続けることを目的に、複合的な攻撃手法を用いることにより、目的達成の機会を作出することができる、高度な専門的知識と莫大なリソースを有する攻撃主体（NIST SP800-39 “Managing Information Security Risk: Organization, Mission, and Information System View”【Appendix B GLOSSAR Y】）

非公開情報が流出した事例も発生し、社会的に大きな問題となった。

さらに、最近、急速に普及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、SNS 等について、様々な情報セキュリティ上の課題が指摘されている。

このように情報セキュリティ上の脅威は益々高度化・多様化するとともに、大規模なサイバー攻撃事案等の脅威が現実化している状況にあり、このような状況を改善・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増大

社会経済活動や国民生活における「情報」の役割が増大し、我が国の社会経済活動が情報通信技術への依存度を高める中、情報セキュリティは社会基盤のひとつとして重要な役割が期待されている。

我が国のインターネット利用者数は、2009 年末に 9,408 万人[3]に達し、インターネットを通じて商品等の購入や金融取引をしたことのある人の割合も 53.3%にのぼるなど、情報通信技術への依存を深めている。

また、登場してからわずか数年で、国内でも数千万人が利用するようになった SNS や、急速に普及しつつあるスマートフォン等は、人々のコミュニケーションの在り方に急速な変化と革新をもたらしつつある。とりわけ、今般の東日本大震災では、災害時における情報伝達、情報共有等の重要性が改めて認識された。

このように、情報通信システムが社会経済活動の根幹を成す枠組みに不可分に組み込まれていく中、これらのシステムを安全・安心に利活用できる情報セキュリティの確立が強く求められている。

③ 新たな技術革新への対応

近年、コンピュータリソースの仮想化によるクラウドコンピューティングの活用や、端末のユビキタス化、情報家電等における高度な組み込みソフトウェアの利用の拡大等が目覚ましく進展している。今後、家庭やオフィス等に様々なセンサーが設置され、リアルタイム・センシング機能[4]の強化や位置情報やユーザー情報を活用したコンテキスト・アウェアネス（Context Awareness）[5]の動きも加速化する可能性がある。

---

[3] 総務省「平成 22 年　情報通信に関する現状報告」（平成 22 年 7 月）

[4] 様々な状況をセンサー等でリアルタイムに計測・把握する機能。家庭のスマートメーターや個人の心拍センサー等から計測されたデータをリアルタイムに無線ネットワーク等で集約・分析するなどの例が挙げられる。

[5] コンピュータがセンサーやネットワークを介して様々な事柄に関する状況の変化を自動的に認識し、状況の変化に応じて対応する概念。

このように、ユビキタス化やリアルとバーチャルを融合する技術等が急速に発展する可能性があることから、これらの技術を支える情報セキュリティ技術・制度等の適切な対応が求められている。

④ グローバル化等

2010 年末より、北アフリカ諸国で発生した、いわゆるジャスミン革命の動きは、情報通信技術による国境を越えた情報の自由な流通が、社会の枠組みをも揺るがしうることを改めて示した。また、視点は全く異なるが、WikiLeaks の活動は、様々な問題を提起した。

インターネットを経由して情報が国境を越えて流通することは、理念的には従前から主張されてきたが、それが具体的に政治や社会、経済にどのようなインパクトを与えるのか、課題等の検討が求められている。

⑤ 東日本大震災の発生

東日本大震災は、大規模な地震、津波、原発事故等、これまでに経験したことのない複合的な大災害であり、東日本のみならず我が国の社会・経済に甚大な損害をもたらした。既存の情報通信インフラも壊滅的な被害を受け、情報の途絶が救助、救援、復旧を遅らせるとともに、人々の不安も増大させた。

また、社会経済活動の基盤となる情報が円滑に流通しないことにより、様々な活動が停滞を余儀なくされた。一方、SNS 等の新たな情報通信技術の使い方が災害情報の共有等に役立ったとの報告もなされている。

今回の大震災を踏まえ、バックアップシステム、非常用電源の強化、クラウドコンピューティングの活用等、耐災害性の高い情報通信システムの在り方を検討し、再構築を図るとともに、事業継続計画（BCP）の抜本的見直し、「リスク・コミュニケーション[6]」、「リスク・マネジメント[7]」の確立等についても早急な検討が求められている。

---

[6] あるリスクについて、情報通信システムに直接・間接に関係する人たちが意見を交換し、合意を形成する過程。

[7] リスクを明確化し、その影響度や発生頻度等から評価、対策を行い、リスクによる被害を最小限に抑える、PDCA サイクルに従った一連のプロセス。

III　基本方針

本文書の策定に当たっては、「国民を守る情報セキュリティ戦略」に示された基本的考え方に加え、昨今の環境変化を踏まえた、以下の視点を重視して、施策を取りまとめることとする。

①　「サイバー空間[8]」についての基本的考え方

情報通信技術は、社会経済活動の基盤であり、情報通信技術への依存度は益々高まっている。人々が様々な形でインターネットを利用することにより、社会生活の質の向上や経済活動の活性化が図られている。また、オープンでグローバルなネットワークは、経済発展や生活の向上に資するイノベーションを推進するための鍵である。

近年、ブロードバンドネットワークの普及、スマートフォンの普及、クラウドコンピューティング等の新たな技術の進展により、国内外の情報流通が大きく拡大し、我が国の経済成長や世界経済の活性化等の原動力となる一方で、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、知的財産権侵害への対策等、インターネットを巡る課題も顕在化してきている。

いわゆる「サイバー空間」について、各国で安全保障面をはじめとする様々な取組がなされているが、この機会に情報セキュリティの視点から基本的な考え方を確認しておくことは意義深いと考える。

・オープンで相互運用可能で、セキュアで、信頼性の高いサイバー空間の構築

我が国としては、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が重要である。

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、知的財産権侵害への対策等の課題に配慮しつつ、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必要がある。

すなわち、オープンで相互運用可能で、セキュアで、信頼性の高いサイバー空間を構築する必要がある。これを実現するためには、一国のみの対応では不可能であり、国際的なコンセンサスを得ながら、国際連携を促進することにより実現する必要がある。

米国は、2011年５月に、「サイバー空間の国際戦略」を発表し、これらの問題に対する同国の考え方を世界に提示している。また、2011年５月のG8ドーヴィ

[8] 情報通信技術を用いて情報がやり取りされる、インターネットその他の仮想的な空間。

ル・サミット首脳宣言において、インターネットについての主要な原則が取りまとめられている。

② 情報セキュリティの脅威の高度化・多様化に対応した能動的な対応

II で述べたように、大規模サイバー攻撃事態の発生、APT と呼ばれる新たな脅威、大規模なシステム障害の発生、大規模な個人情報の漏えい等、情報セキュリティに係る脅威は、ますます大規模化・高度化・複雑化してきている。これらに、迅速かつ的確に対応することが極めて重要である。

サイバー空間においては、防御側よりも攻撃側が有利という状況は改善していないどころか、むしろ攻撃側が優位な状況が加速化しており、このような状況の改善・克服が求められている。実空間とサイバー空間の融合化が進展する中、このような非対称性を解消する「ゲーム・チェンジ[9]」のための能動的な取組を強化し、情報システム全体の高い信頼性、いわゆる「ニュー・ディペンダビリティ[10]」を確保することは極めて重要である。

その際、特に留意すべきことは、個別課題への対応はそれぞれ重要であることは言うまでもないが、「つながって、対応すべき課題[11]」の増加に対し、個別課題が全体のフレームの中でどう位置づけられるかを常に認識しながら、官民連携、国際連携を促進することが重要である。

換言すれば、様々なデータやコンテンツ、知識等がクラウドコンピューティング等を通じて、ネットワークの中に集約化される傾向にある。この動きは、非常に加速化しており、その観点からも「つながって、対応すべき課題」が増加していると言える。また、サイバー空間上と実空間上のリソースのリンク化も加速していることから、従前よりも多くの主体で協調して課題を解決する必要がある。

また、脅威が高度化・多様化する中、我が国として情報セキュリティ対策の向上を図るためには、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。

---

[9] 「ゲーム・チェンジ」のゲームは、経済学でいう「ゲーム理論」に近い意味。情報セキュリティ分野においては、攻撃側が防御側よりも優位な状況が続いており、革新的な取組みによって攻撃者の経済的負担を増大させるなどの「チェンジ」が、情報セキュリティ課題の根本解決に繋がるという考え方である。

[10] 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。従来の信頼性に加え、サイバー攻撃を無効化するなど「能動的」な情報セキュリティ要素を追加したもの。詳細は、「情報セキュリティ研究開発戦略」（情報セキュリティ政策会議 2011 年 7 月決定）の基本的考え方を参照。

[11] サイバー空間においては、ネットワークを介して多くの要素が有機的に結び付き、互いに影響を及ぼし得る。情報セキュリティ上の課題のうち、その対応の際に、影響を及ぼし合う要素間の調和を図る必要があるものをいう。

特に、早急に重点化すべき分野を以下に示す。

・政府横断的な情報収集・分析システム（GSOC[12]）の充実・強化

大規模サイバー攻撃事態の脅威の現実化、標的型メールの増加等に対する政府としての対応力を高めるためには、2008 年度から本格運用を開始し、政府機関情報システムの 24 時間監視を行っている GSOC の充実､強化が不可欠である。特に、緊急時における連絡体制や関係連携機関との連携強化等による情報収集能力、攻撃等の分析・解析能力強化等により、政府全体としてサイバー攻撃等に対する緊急対応能力を向上させる必要がある。

・スマートフォンの情報セキュリティ上の課題への早急な対応

スマートフォンを狙ったコンピュータウイルスの登場により、急速に普及しているスマートフォンに係る情報セキュリティ上の課題が顕在化している。スマートフォンの基本的な構成は、パソコンと同じであるとの基本認識を利用者が持つとともに、パソコンと異なる機能制約の下、官民が連携して安心してスマートフォンを利用できる環境整備、基盤整備を早急に進める必要がある。

・Stuxnet 等の制御システムの情報セキュリティ上の課題への対応

従来は、専用回線で分離されていること等から攻撃が困難であると考えられていた重要インフラ分野等の制御システムに対して、「Stuxnet」による攻撃が発生したこと等を踏まえ、重要インフラ分野の SCADA[13]等の制御システムを防御するための早急な取組が求められている。

また、APT による特定の機関、企業等を狙った新たな攻撃も脅威となりつつあり、制御システムが第三者に侵入又は掌握されてしまった場合、物理的な危険に直結する可能性もあることから、その視点からの対応が求められる。

・クラウドコンピューティング、IPv6、SNS 等の情報セキュリティ上の課題への対応

東日本大震災を踏まえ、クラウドコンピューティングの有効性について認識が高まっているほか、IPv4 アドレスの枯渇に伴う IPv6 の本格的利用、SNS の利用拡大等の動きが加速化しているが、一方でこれらに対する情報セキュリティ上の課題も指摘されている。このような状況に対応した情報セキュリティの確保方策を早急に検討する必要がある。

---

[12] Government Security Operation Coordination team の略。

[13] Supervisory Control And Data Acquisition の略。産業部門で利用される制御システムの一種であり、監視制御システム、遠方監視制御装置、通信基盤、ユーザインターフェイスにより構成される。

③ 東日本大震災を踏まえた情報セキュリティ分野における対応

情報セキュリティの各種方策については、「機密性」、「完全性」、「可用性」の確保に重点をおいて推進しているが、大規模な災害発生時においては、特に「可用性」（必要な時に情報やサービスが利用できること）の確保が重要になると考えられる。

このため、耐災害性の高い情報通信システムを検討、再構築するとともに、遠隔地への情報のバックアップや分散化等に対応した事業継続計画（BCP）の見直しが不可欠である。サイバー空間上のセキュリティと物理的なセキュリティ[14]は表裏一体の関係にあるので、複合的な大規模災害が発生することを前提としたBCPの見直しが必要になっている。

・「リスク・マネジメント」、「リスク・コミュニケーション」の確立

大規模な災害の発生時には、状況がダイナミックに変化することで、リスクに対する社会の捉え方が変化する。（例えば、平常時では個人のプライバシーに係る情報を公開することは不適切であるが、災害時には安否確認が優先される）災害時においては、このような状況変化の中で、最適な対応を行うための「ダイナミック・リスク対応」の観点を持つことが必要である。また、一つのリスク対応が従来存在しなかった新たな別のリスクを引き起こすことがあるので、リスクとリスクを比較考量しながら最適な解を模索（「リスク・マネージメント」）する必要がある。

さらに、社会を取り巻くリスクに関する正確な情報を様々な関係者間で共有し、相互に意思疎通を図るとともに、多様な価値観が混在する中で、許容されるリスクを調整する「リスク・コミュニケーション」の仕組みを確立することが重要である。

このように、今回、「リスク・コミュニケーション」、「リスク・マネジメント」の重要性が改めて認識されたところであるが、これらの分野における知見は現時点では必ずしも確立されておらず、早急な対応が求められている。

・情報システム全体の「ニュー・ディペンダビリティ」の確保等

今般の東日本大震災を踏まえ、情報セキュリティの観点から、①耐災害性の高い情報通信インフラの検討・再構築、②災害時の情報通信システムの在り方、③情報通信システムのバックアップ、分散化、④「リスク・コミュニケーション」、「リスク・マネジメント」の確立、⑤情報システム全体の「ニュー・ディペンダビリティ」の確保等の課題に早急に取り組む必要がある。

---

[14] ISO/IEC 27001:2005における「物理的及び環境的セキュリティ」をいう。情報処理施設のある領域における入退室管理や、自然災害や人的災害からの保護等が挙げられる。

これらの課題を克服するにあたり、単なる復旧を図るという視点ではなく、未来志向の創造的な取組に寄与する情報セキュリティ政策を確立するという発想で取り組むことが重要である。

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、2011 年度中に実施するものである。

1 大規模サイバー攻撃事態への対処態勢の整備等

(1) 対処態勢の整備

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各府省庁の連携に重点を置いた具体的な訓練を継続実施するなどの取組により、当該事態への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、サイバー攻撃への対処態勢及び対応能力を総合的に強化する。

ア　大規模サイバー攻撃事態における政府の初動対処態勢の整備

(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)　情報分析態勢の整備等（内閣官房）

大規模サイバー攻撃事態等の発生時における情報の分析態勢を整備・充実させる。

(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) サイバーテロ対策に係る体制等の強化（警察庁）

サイバーテロ[15]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。

イ　官民連携の推進

(ｱ) 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の業務の特性を踏まえつつ、必要に応じ、サイバーテロ対策の意識の向上につながる啓発活動を行うとともに、重要インフラ事業者等の意向を尊重しつつ、共同訓練の実施、各種演習等への参画を通じ、サイバーテロ発生時の緊急対処活動に資する取組を行う。

(ｲ) サイバーインテリジェンス対策[16]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[17]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。

(ｴ) 新しい脅威・攻撃の分析（経済産業省）

情報セキュリティに関する新しい脅威・攻撃を分析する「脅威と対策研究会」を（独）情報処理推進機構（IPA）に設置し、分析結果等、利用者に必要な情報を迅速に提供する。

---

[15] 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。

[16] 「サイバー空間における諜報活動（サイバーインテリジェンス）への対策」をいう。

[17] Computer Security Incident Response Team の略。

ウ　サイバー攻撃に対する防衛分野での体制の強化

(ｱ)　サイバー防護専門部隊の新編に向けた準備体制の整備（防衛省）

防衛省・自衛隊に対するサイバー攻撃等への統合的な対処の中核となる、サイバー防護専門部隊の新編に向けた準備要員を確保する。

(ｲ)　サイバー防護分析装置の運用開始（防衛省）

新たなサイバー防護分析装置の運用を開始し、自衛隊セキュリティ要員に対するサイバー攻撃等対処訓練の支援やサイバー攻撃対処の研究等を実施する。

(ｳ)　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。

(ｴ)　情報保証に係る最新技術動向等の調査研究（防衛省）

2010 年度に引き続き、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。

(ｵ)　サイバー攻撃等対処に向けた人材育成の取組（防衛省）

防衛大学校におけるネットワークセキュリティ分野の教育・研究体制を整備する。

エ　サイバー犯罪の取締り

(ｱ)　デジタルフォレンジック[18]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。

---

[18] 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。

(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）

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との効果的な情報交換を実施するとともに、G8、ICPO 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。

オ　サイバー攻撃への対処に係る国際連携の強化

(ｱ)　サイバー攻撃等に関する諸外国等との情報共有体制の構築・強化（内閣官房及び関係府省庁）

サイバー攻撃等への対処に関し、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）

サイバー攻撃への対応能力を向上させるため、2011 年度には、FIRST（Forum of Incident Response and Security Teams）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。

(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。

(2) 平素からの情報収集・共有体制の構築強化

内閣官房と各府省庁との間において、サイバー攻撃事態への対処に資する情報の収集・分析・共有体制を強化するほか、諸外国の関係機関との間において、サイバー攻撃事態への対処に資する情報の共有体制の構築・強化を図る。

ア　対処に資する情報の収集・分析・共有体制の強化

(ｱ)　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。

(ｲ)　各政府機関における緊急対応体制の強化支援（内閣官房）

2010 年度に引き続き、GSOC において、政府機関に対するサイバー攻撃等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とともに、個々の対策に必要となる攻撃手法の分析結果等の情報を適時・適切に提供する。

(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」に基づく情報共有体制による情報収集、情報共有の実施（内閣官房）

重要インフラ事業者等に対するサイバー攻撃に係る情報について、「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。）に基づく情報共有体制による情報収集、情報共有の充実を図る。

(ｴ)　サイバーテロ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）

サイバーテロへの対策を強化するため、サイバー空間におけるテロの予兆等の早期把握を可能とする態勢を整備し、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。

(ｵ)　サイバーテロ対策に係る体制等の強化（警察庁）

【再掲：１(1)ア】

イ　サイバー攻撃等に関する諸外国等との情報共有体制の構築・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を通じた対処能力の向上（内閣官房及び関係府省庁）

諸外国の関係機関等との意見交換等を通じ、サイバー攻撃の攻撃主体・方法等の対処に資する情報の共有を進め、我が国の対処能力の向上を図る。

(ｲ)　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）

【再掲：１(1)オ】

２ 新たな環境変化に対応した情報セキュリティ政策の強化

(1) 国民生活を守る情報セキュリティ基盤の強化

① 政府機関等の基盤強化

政府機関における情報セキュリティ対策については、

大規模サイバー攻撃事態の脅威の現実化、標的型メールの増加などに対する政府としての対応力を高めるため、2008 年度から本格運用を開始し、政府機関情報システムの 24 時間監視を行っている政府横断的な情報収集・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)が中心となって能動的に改善を図っていく枠組みとして、「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。）の作成を本年度より本格的に実施する。こうした情報セキュリティ報告書を中心とした一連の PDCA サイクルにおいて、自己点検及び重点検査に係る作業の一層の効率化などを通じ、情報セキュリティ対策の向上を図るとともに、「政府機関の情報セキュリティ対策のための統一基準群」[19]（以下「政府機関統一基準群」という。）の周知徹底や標的型メールに係る教育訓練といった教育の改善等を実施することにより、職員一人ひとりの情報セキュリティ水準の更なる向上に努める。

また、政府機関を取り巻く環境の変化に迅速に対応するため、東日本大震災による情報システムへの影響を分析・評価し、「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）の改善等を行うほか、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の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）に係る発動要件の決定を行う等の取組を着実に実施する。

[19] 「政府機関の情報セキュリティ対策のための統一基準群」とは、「政府機関の情報セキュリティ対策のための統一規範」、「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」、「政府機関の情報セキュリティ対策のための統一管理基準」及び「政府機関の情報セキュリティ対策のための統一技術基準」を指す。

ア　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）の充実・強化（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、関係機関との連携強化等により、サイバー攻撃等に関する情報収集能力、分析・解析能力の更なる強化を図るとともに、分析結果等の情報共有を進め、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。

イ　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から成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、各府省庁が自律的に、最高情報セキュリティ責任者の下で、情報セキュリティ対策について責任を持って統括することを可能とする体制の充実を図る。

b) 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、情報セキュリティに係る専門的知見を各府省庁の取組の高度化に反映させる。

(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、情報セキュリティ報告書作成のためのガイドライン及び 2010 年度の情報セキュリティ報告書の作成における経験を踏まえ、府省庁内外の知見を活用しつつ、2011 年度以降、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。

b) 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。

c) 内閣官房は、政府機関における評価手法として、各府省庁の対策の実施状況を、

政府機関統一基準群[20]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、勧告する。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・方法を改善す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。

d) 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、情報セキュリティ政策会議情報セキュリティ報告書専門委員会報告（2009年９月11日）においてその取扱いが規定されているが、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2011年度以降は、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こととする。

(ｳ) 内閣官房及び各府省情報化統括責任者（CIO）補佐官等の連携強化（内閣官房、総務省及び全府省庁）

2011年度は、最高情報セキュリティアドバイザー等連絡会議とCIO補佐官等連絡会議が連携し、政府機関における情報システムのセキュリティ確保のための取組を強化する。

ウ　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。

[20] 2011年４月21日情報セキュリティ政策会議決定

(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、2010 年に引き続き 2011 年においても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行う。

(ｳ) 標的型メール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、2011 年中に希望府省庁に対して標的型メール攻撃に係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とともに、情報セキュリティに係る教育の改善及び対策実施状況報告との比較・評価を行う。

(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) 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 年度末までに必要な情報システムについて運用を継続するために必要な計画を策定する。

b) 内閣官房は、各府省庁の情報システム運用継続計画の策定・改善に資するため、東日本大震災による情報システムへの影響を分析・評価し、適宜、各府省庁に対する情報提供や上記ガイドラインの改善等を行う。

c) 内閣官房は、各府省庁において策定される情報システム運用継続計画につき、対策レベルの維持・継続的改善に向けた適切なマネジメントに資するよう、当該計画の評価手法について検討する。

(ｵ) 政府機関における適切な物理的セキュリティ対策の検討（内閣官房）

内閣官房は、東日本大震災といった物理的セキュリティに甚大な影響を及ぼす可能性のある環境変化に対応するため、民間事業者等における先進的事例等を調査し、各府省庁における適切な物理的セキュリティ対策の在り方を検討する。その上で、政府機関における実態等を踏まえ、指針等として取りまとめる。

(ｶ) 「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）

a) 「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）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。

b) 内閣官房は、「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」において配慮事項として記載した「証跡管理」について、実際の判例などを参考にしつつ、その有効性についての整理及び政府機関における適切な管理の在り方を検討する。

(ｷ) 政府全体での情報共有の強化（内閣官房及び全府省庁）

内閣官房は、各府省庁における情報セキュリティ対策の推進を支援するため、情報セキュリティ対策の運用上の共通的な課題に関して、技術情報を含む各種情報セキュリティ対策関連情報を提供する。また、各府省庁とともに対応策等について検討・共有する場を定期的に設け、共同して課題の解決に取り組む。

(ｸ) 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を重層的にチェックする仕組みの構築に向けた取組を着実に実施する

(ｹ) 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）

2010 年 12 月、内閣官房長官を委員長とする「政府における情報保全に関する検討委員会」を設置し、秘密保全法制に関する法制の在り方及び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ついて必要と考えられる措置に関する検討を開始したところ、その結論を得て、必要な取組を推進する。

(ｺ) 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。

c) 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。
d) 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。

(ｻ) 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、SPF[21]等の送信ドメイン認証技術の採用等を推進していく。また、政府機関又は政府機関の職員になりすました電子メールが、政府機関あてに送信されることもあることから、受信側においても送信ドメイン認証技術の採用を推進する。
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り設立された民間団体である「JEAG(Japan Email Anti-Abuse Group)」等と連携して、送信ドメイン認証技術等の導入を促進する。

(ｼ) 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、2011 年度も引き続き、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。

エ 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

[21] Sender Policy Framework の略。電子メールにおける送信元ドメイン認証のひとつであり、メール送信者のメールアドレスの送信元ドメインのなりすましの検出が可能となる。

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 2011 年度も引き続き行う。

b) 総務省及び経済産業省は、「電子政府推奨暗号リスト」の改訂に向けた取組を着実に実施する。

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」[22]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、2011 年度も引き続き、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切替え開始時期までに、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の活用を推進するため、引き続き、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優先的に取り扱う。

オ　クラウドコンピューティングにおける情報セキュリティの確保等

(ｱ) 新たな技術に対する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・構築を開始し、内閣官房は、政府機関統一基準群の改訂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。

[22] 2008 年４月 22 日 情報セキュリティ政策会議決定

カ　政府機関の情報セキュリティ対策のための統一基準の見直し

(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）

各府省庁においては、東日本大震災といった情報システムに多大なる影響を及ぼす可能性のある環境変化の際にも、適切なセキュリティ対策を実施することが求められる。そのため、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とともに、各府省庁で保有する情報資産の範囲及びその取扱方法の明確化を図ることを目的に、政府機関におけるリスク・マネジメント手法の在り方を検討し、指針等として取りまとめる。また、その成果を各府省庁に対して共有することで、各府省庁相互におけるリスク・コミュニケーションの醸成を図る。

(ｲ)　政府機関統一基準群の見直しの実施（内閣官房）

技術や環境の変化を踏まえ、政府機関統一基準群の見直しを行う。特に、2011年度は、東日本大震災によって顕在化した新たな情報システム上の脅威及びIPv6 等の技術動向等を踏まえ、業務継続計画や物理的セキュリティ対策、IPv6等に係る遵守事項等の見直しを行い、改訂版に向けた作業を実施する。

(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）及び独立行政法人情報処理推進機構（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)　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[23]」により認証された製品等を取り扱う。

[23] 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。

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引き続き行い、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。

(ｵ) 情報セキュリティに関連する法制度等との整合性確保（内閣官房、内閣府、総務省及び関係府省庁）

内閣官房は、情報セキュリティに関連する法制度等と政府機関統一基準群との整合性の確保が図られるよう、内閣官房内の関係部局をはじめ法制度等を所管する関係府省庁と意見交換の場を設け、相互の緊密化を図る。

(ｶ) 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）

【再掲：２(1)①エ】

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

【再掲：２(1)①エ】

キ 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、情報セキュリティの確保のための取組を進める。

(ｲ) 企画・設計段階からの情報セキュリティ対策の組込みについても意識す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。

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普及・利用促進を行う。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。

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

【再掲：２(1)①エ】

(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）

すべ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。

(ｶ) 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）

【再掲：２(1)①カ】

ク　社会保障・税の共通番号制に対応した情報セキュリティ対策の検討

(ｱ)　社会保障・税に関わる番号制度及び国民 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）

政府横断的に検討が行われている社会保障・税に関わる番号制度及び国民 ID 制度については、国民の安心と利便性を確保するため、2011 年度も引き続き、適切な個人情報保護及び情報セキュリティに配慮した制度の具体化に向けた検討を進める。

ケ　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 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、LGWAN（総合行政ネットワーク）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、Web ページを閲覧しただけで感染するタイプのマルウェアの有無について確認し、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成りすまし、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への情報セキュリティに関する普及・啓発の推進（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、情報セキュリティの取組に関する普及・啓発のための支援を行う。

(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) 2010 年度に引き続き、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、SPF 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）

2010 年度に引き続き、独立行政法人等と、緊急時を含めた連絡体制を整備し、2011 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。

② 重要インフラの基盤強化

重要インフラの情報セキュリティ対策については、

第２次行動計画に基づき、分野横断的な官民連携体制の充実を引き続き図る。具体的には、重要インフラ分野における横断的な情報セキュリティに関する情報共有、分析体制を強化するため、「セプターカウンシル[24]」の活動の一層の促進を図るとともに、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。

特に、制御システムに関する新たな攻撃に対応するため、障害事例の精査とシステムの堅牢化等についての検討、情報の共有、安全基準策定のための指針の検討等を行う。

今般の大震災への対応、大規模なシステム障害の発生等を踏まえ、官民の役割分担を明確にした上で、情報セキュリティの観点から事業継続計画（BCP）の在り方等について検討する。

また、重要インフラ分野における国際連携を推進する。

ア　情報共有体制の強化

(ｱ)　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、引き続き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。

(ｲ)　「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、年度末に、実施細目による情報共

[24] 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。

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、必要に応じ改訂を行う。

(ｳ) 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。

(ｴ) 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、2011 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。

(ｵ) 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、2010 年度に引き続き、情報セキュリティ対策に関する Web 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。

(ｶ) 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ための方策を検討する。その際、大震災等を踏まえた観点（大規模災害時の情報共有、ダイナミック・リスク対応等）も考慮する。また、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。

(ｷ) 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。

(ｸ) 「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：２(1)①キ】

イ 「セプターカウンシル」の活動促進

(ｱ) 「セプターカウンシル」の支援（内閣官房）

重要インフラの各分野により構成される共助活動の場として 2009 年 2 月に発足した「セプターカウンシル」が一層円滑に運用されるよう、分野横断的な情報共有の推進等のサービスの維持・復旧能力の向上に資することを目的とした「セプターカウンシル」の活動を支援する。

ウ 「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、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、引き続き「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）」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。

b) 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、2011 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〉

2011 年度中に「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〉

2011 年度当初に「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）

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。

エ 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。

2011 年度においては、昨今注目を集めている標的型サイバー攻撃について、制御システムを含む国内外の障害事例を精査し、重要インフラ分野における各種重要システムが同様のサイバー攻撃により IT 障害を引き起こすリスクを分析するとともに、その対応策としてのシステムの堅ろう化等について検討する。

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。

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

a) 2010 年度に引き続き、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) 重要インフラ等の制御システムの脆弱性低減のための情報セキュリティ対

策を普及・啓発するための資料作成に向け、製造事業、プラント事業の制御システム及び次世代伝送網（スマートグリッド）等のセキュリティへの対応について国内外の状況を調査する。

(ｴ) 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(1)イ】

(ｵ) 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、2011 年度に同施設のセンサーを更改する。

c) 電波の広帯域利用に対応した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。

オ　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) 制御システムの課題を踏まえた対策の検討と対応（内閣官房）

重要インフラにおける SCADA 等の制御システム等について「Stuxnet」による海外事例を始めとする障害事例の精査及び我が国の特徴を踏まえたシステムの堅牢化等について検討を行う。これらの調査・検討等を踏まえ、有益な情報や早急に実施すべき対策等については、重要インフラ所管省庁等を通じ重要インフラ事業者等へ共有を図る。更に必要に応じ、「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」等への反映を検討する。

なお、制御システムの障害が発生した場合には、内容に応じた迅速な対応状況等の共有などにより、被害の拡大防止、収束を図る。

(ｲ) 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）

制御システムの情報セキュティの向上を図るため､タスクフォースを設置する。当該タスクフォースにおいて、制御システムの情報セキュリティ基準の策定、国際標準化を検討するとともに、評価・認証制度の構築に向けた検討を行う。

また、この制度を担う人材及び制御システムに関するインシデントへ対応するための人材の育成について検討する。

さらに、制御システムユーザーに対し、情報セキュリティに関する普及啓発を実施する。

(ｳ) 制御システムに関する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脆弱性等の脅威への対応の円滑化を図る。

(ｴ) 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。

カ 事業継続計画（BCP）の充実

(ｱ) 事業継続計画（BCP）の充実（内閣官房）

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。

2011 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を実態調査し、情報システムの安定運用の視点で重要インフラの BCP に盛り込むべき課題を抽出した上で、2012 年度中に、対策の在り方について取りまとめる。

キ 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）

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 IWWN

（国際監視･警戒ネットワーク）やMERIDIANの活動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。また、インフラ輸出等の我が国の対外活動とリンクすることも想定し、国内の関係主体から関係諸国への情報発信を支援する。

③ 情報セキュリティ産業の振興

新たな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、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グローバル展開に貢献する。

(ｱ) 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、スマートフォン、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」の下にワーキンググループを設け検討する。

(ｲ) IPv6 環境のセキュリティ評価システムの構築（総務省）

NICT において、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、その重要度を評価した上で対応策を検討する。

2011 年度は、産業界との連携の下、中規模な IPv6 セキュリティ検証環境を構築し、その中で複数の攻撃シナリオを実行して、各種のセキュリティ評価試験を実施する。

(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) 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）

【再掲：２(1)①カ】

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

【再掲：２(1)①エ】

(ｶ) 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：２(1)①キ】

(ｷ) クラウドコンピューティングのセキュリティ（経済産業省）
【再掲：２(1)④イ】

④ その他の基盤強化

新たな技術革新に対応し、社会経済活動としての情報通信技術基盤の安全・安心を確保するため、

急速に普及しているスマートフォンに係る情報セキュリティ上の課題への対応を図る。

利用拡大の動きが顕在化している一方、情報セキュリティ上の課題も指摘されている、クラウドコンピューティング、IPv6 及び SNS 等に対応した情報セキュリティ確保策を検討、推進する。

マルウェア対策の充実・強化を図るため、サイバー攻撃防御、標的型サイバー攻撃対応等に効果的な枠組みについて検討・構築する。

ア　スマートフォンに関する情報セキュリティ確保方策

(ｱ)　スマートフォンのセキュリティ確保推進（内閣官房、総務省及び経済産業省）

急速に普及しているいわゆるスマートフォンについては、利用者層の拡大に伴いコンピュータウイルスが増加する傾向にある。安全・安心な環境を整え、世界的な市場拡大に貢献するよう、従来の携帯電話端末、PC 等との特性の違いを踏まえ、スマートフォン普及に伴って発生する問題点について利用者周知を行うとともに、必要に応じ、技術的な課題等について検討を行う。

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、標準化

(ｱ)　クラウドコンピューティングのセキュリティ（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 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。

(ｲ)　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。

(ｳ) 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。

2011 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。また、クラウドコンピューティング・セキュリティに関する監査の枠組み及び基準案を策定し、報告書にまとめる。

(ｴ) 最先端のグリーンクラウド基盤構築に向けた研究開発（総務省）

2012 年度までに、平常時においては全体の２～３割もの省電力化を図りつつ高信頼・高品質なクラウドサービスを提供するとともに、広域災害時には重要なデータの消失を防ぐため、複数のクラウド間を瞬時に連携させる技術の確立を目指し、引き続き要素技術の開発、機能検証等を実施する。

(ｵ) クラウド対応型セキュリティ技術の研究開発（総務省）

情報漏えい等の情報セキュリティ上の課題を残したまま発展しつつある、クラウド等を利用した社会経済基盤を安心・安全な状態に保つため、新たな情報セキュリティ対策技術を開発する。

(ｶ) 新たな技術に対する情報セキュリティ対策の強化（内閣官房及び総務省）

【再掲：２(1)①オ】

ウ　IPv6 対応、SNS に関する情報セキュリティ確保方策

(ｱ) IPv4/v6 併用環境におけるセキュリティ対策（総務省）

IPv4/v6 併用環境において適切なセキュリティが確保されるよう、官民共同で情報セキュリティ上の技術的課題の整理を行う。

また、インターネットサービスプロバイダが個人ユーザーに対して IPv6 接続サービスを提供することが必要であることから、インターネットサービスプロバイダにおける IPv6 接続サービス提供状況についてホームページで情報提供する。

(ｲ)　IPv6 環境のセキュリティ評価システムの構築（総務省）

【再掲：２(1)③】

(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）

【再掲：２(1)③】

(ｴ)　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）

a) 近年のソーシャルメディアサービスの利用拡大に伴い、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、内閣官房においてソーシャルメディアサービスの利用に係る情報セキュリティの確保や周知するための方策について検討を行う。

b) 東日本大震災の発生以降、国、地方公共団体等の公共機関におけるソーシャルメディアの利用が増加していることから、内閣官房、総務省及び経済産業省が共同し、なりすましの防止等当面留意すべき事項について周知するとともに、必要に応じて見直し等を行う。

エ　マルウェア対策等の充実・強化等

I) 情報セキュリティインシデントへの対応

(ｱ)　サイバー攻撃停止に向けた枠組みの構築（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検討、試行する。

また、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・早期対策及び危害サイト回避に向けた取組の推進（総務省）

a) サイバー攻撃(マルウェアの感染活動、分散型業務妨害攻撃等)に関する情報収集ネットワークを国際的に構築し、ISP、大学等と協力して、サイバー攻撃に対抗するための研究開発を実施し、日本におけるサイバー攻撃等のリスクを軽減する。

b) 電気通信事業者等と連携して、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回避する仕組みの実証実験を行う。

(ｳ) 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。

(ｴ) 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。

II) 検体解析

(ｱ) 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。

(ｲ) マルウェアに関する情報収集・提供（経済産業省）

従来の脆弱性に関する届出の受付等、受け身の情報セキュリティ対策のみならず、自ら能動的にサイバー攻撃や脆弱性の検出を行うための取組に着手する。

(ｳ) 標的型サイバー攻撃への対応（経済産業省）

a) セキュリティ監視企業やアンチウイルスベンダ等の情報セキュリティ企業コミュニティ及び公的機関において、標的型サイバー攻撃に関する情報を共有し、被害の拡大防止につながる枠組みの構築に向けた取組を支援する。この

一環として、情報の収集・共有に関するパイロットプロジェクトを実施する。

b) 標的型サイバー攻撃の各段階において攻撃成功リスクを低減するためには、多重の防護対策が必要である。できる限り早期に技術基準として対策項目を整理し、最低限必要な技術的対策については、個人情報の保護に関する法律（平成 15 年法律第 57 号）の運用において活用する方向で検討する。また、検討結果を踏まえつつ、標的型サイバー攻撃の防止に向けたユーザー企業による取組に関する普及啓発を行う。

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

d) 企業や社会に与える影響が極めて高い、組織の内部の者による攻撃への対策確立に資するため、内部からの脅威、攻撃を分析する。

III) ソフトウェアの脆弱性対策

(ｱ) 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) ベンダやユーザーが国際的に整合化された基準の下で脆弱性の深刻度を定量的に比較し、対策の重要性・優先度を判断することに資する情報の提供を継続するとともに、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、既存のツール等の機能強化等を行う。

①「JVN iPedia」（脆弱性対策情報データベース）の脆弱性分類情報の検索・統計機能の追加及び管理機能強化を行い、一般にリリースする。

② 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、「MyJVN」（情報システム利用者の脆弱性対策支援ツール）のサポート対象をサーバ OS やサーバ製品に拡張する。また、IPA の注意喚起と連動し、特定のインシデントに対応できるように、チェック項目のカスタマイズを行える機能を設ける。

(ｲ) 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) 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。

b) 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。

c) 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引き続き提供する。

d) Web 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。

e) 今後、車載システムの高機能化や、外部接続機器等を通したネットワークへの接続が考えられる自動車において、発生しうる情報セキュリティ上の課題とその対策について検討する。

f) インターネット接続の増加が見込まれるデジタルテレビ等の組込みシステムの脆弱性を早期に検出し、対策を促すため、脆弱性検出業務を立ち上げ、試行運用を開始し、組込み製品の脆弱性対策を促進する。

(ｳ) 企業の運営する Web 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「ウェブサイト脆弱性のログ解析型検査ツール」(iLogScanner)を企業の Web サイト運営者等に引き続き提供する。

(ｴ) 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：２(1)②オ】

(ｵ) 制御システムに関する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：２(1)②オ】

IV) 他の関連取組

(ｱ) 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」を一般国民に引き続き提供する。

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。

(ｲ) 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。2011 年度は、ソフトウェアの品質を可視化するための指標を整備し、国際標準化機関への提案を行う。

(ｳ) DNSSEC[25]導入の促進（総務省）

DNSSEC の円滑な導入に向けた周知等を 2010 年度に引き続き実施する。

(ｴ) 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：２(1)①ウ】

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等の導入を促進する。

c) 日本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～）を引き続き実施する。

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、SPF(Sender Policy Framework)等の送信ドメイン認証技術の採用等を推進していく。また、政府機関又は政府機関の職員になりすました電子メールが、政府機関あてに送信されることもあることから、受信側においても送信ドメイン認証技術の採用を推進する。

---

[25] Domain Name System Secure Extensions の略。DNS における応答の正当性を保証するための拡張仕様。

オ　情報家電、モバイル端末、電子タグ、センサーネットワーク等の情報セキュリティ確保方策

(ｱ)　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）

【再掲：２(1)④エ】

(ｲ)　システムLSIのセキュリティ評価・認証体制の整備（経済産業省）

2011 年度までに、IC カード等に用いられるシステム LSI について、国内で ISO/IEC15408 に基づくセキュリティ評価・認証が行えるよう必要な体制整備を行うため、脆弱性評価用標準スマートカードの整備、人材育成、調査等を着実に実施する。

(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）

【再掲：２(1)②オ】

(ｴ)　制御システムに関する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：２(1)②オ】

(ｵ)　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：２(1)②オ】

(ｶ)　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：２(1)①キ】

カ　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) IPA が、中小企業に指導する立場にある者等による情報セキュリティに係る相談対応等を支援するツール等の提供に向けて、開発に着手する。

キ 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。

ク 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）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かける。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）の活用を促進する。

(ｲ) ACTA（模倣した物品の取引の防止に関する協定（仮称））の参加促進（外務省、経済産業省、文部科学省、総務省、法務省、財務省）

ブランドの価値を国際的に守るため、アジアをはじめとする諸外国に対し、ACTAへの参加拡大を促す。

⑤ 内閣官房情報セキュリティセンターの機能強化

NISC において、情報セキュリティに関する高度な情報収集や分析機能の強化を実施し、専門性の向上を図るとともに、官民連携を強化する。

ア　NISC の総合調整機能の強化

(ｱ)　NISC 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関連の対応、緊急時対応等、各府省庁の情報セキュリティ対策推進に向けた様々なニーズへの対応のため、引き続き、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、新成長戦略実現会議、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。

(2) 国民・利用者保護の強化

国民・利用者がITリスクを認識し、自ら情報セキュリティ対策を実施することができる社会を構築するため、「情報セキュリティ普及・啓発プログラム」に基づき、普及・啓発活動の充実・強化を図る。「普及・啓発、人材育成専門委員会」等を設置し、普及・啓発に係る司令塔機能を明確化する。また、国際社会での役割と責任を果たす観点から、普及・啓発活動に関する国際連携を積極的に推進する。

また、情報セキュリティに係る相談窓口の充実、個人情報保護の推進、サイバー犯罪に対する態勢の強化について、取組の継続的な推進を図る。

① 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の着実な推進を行う。

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として、国民・利用者を対象とした自己診断チェックリスト作成に向けた検討を行う。

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、平易な言葉で分かりやすく伝えるため、高齢者向けの情報セキュリティ対策に関する資料作成に向けた検討を行う。

d) 企業におけるセキュリティ管理として、情報システム部門の現場におけるセキュリティ管理だけでなく、経営層による情報セキュリティ統制としてリスク管理を行う必要があることを企業のトップが認識を共有するための普及・啓発の在り方について検討を行う。

(ｲ) 「普及・啓発、人材育成専門委員会」等の設置（内閣官房及び関係府省庁）

情報セキュリティの普及・啓発を専任とする司令塔機能を明確化するため、「情報セキュリティ政策会議」の下に、新たに「普及・啓発、人材育成専門委員会」（仮称）を設置し、情報セキュリティに関する普及・啓発、人材育成施策について、助言、評価等を行う。

また、官民連携による普及・啓発施策を推進するため、「普及・啓発、人材育成専門委員会」（仮称）の下に、「官民連携ワーキンググループ」（仮称）を設置

し、官民連携プロジェクトの企画立案、推進を図る。

(ｳ) 「情報セキュリティ月間」の充実（内閣官房及び関係府省庁）

国民一人ひとりが情報セキュリティについての関心を高め、理解を深めるため、「情報セキュリティ月間」の更なる周知と、期間中に開催される関連行事等の充実を図る。

(ｴ) 「情報セキュリティ月間」10 月開催の検討（内閣官房及び関係府省庁）

今後、国際連携を一層推進する観点から、我が国の「情報セキュリティ月間」について、従来の２月開催から 10 月開催に変更する、あるいは、２月開催は維持しつつも 10 月中に新たな「国際連携情報セキュリティ意識啓発週間」（仮称）等を開催することを検討する。

(ｵ) 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) 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」等の取組を通じ、国民一人ひとり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かけも重視することとする。

b) 2011 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) 2010 年度に引き続き、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）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。

(ｶ) 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周知啓発を実施する。

さらに、総合通信局所において、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。

(ｷ) 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システムを引き続き提供する。

b) 情報セキュリティ対策を推進するための人間の行動等について調査及び社会科学的分析を行う。

c) 2010 年度の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 2011」にとりまとめて、公表する。

(ｸ) 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：２(1)①キ】

(ｹ) 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。

(ｺ) 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。

② 情報セキュリティ安心窓口（仮称）の検討

㈠ 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。

㈡ 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）

従来からある相談窓口を、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としてリニューアルした「情報セキュリティ安心相談窓口」を引き続き運用し、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。

㈢ 情報セキュリティ・サポーターの育成・活用（総務省）

各地域において、情報セキュリティに関する知見を持った身近な相談相手（情報セキュリティ・サポーター）を育成・活用し、国民全体の情報セキュリティの底上げを行う。

③ 個人情報保護の推進

ア　個人情報保護法の見直し

(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、2011 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　国際的なフレームワークへの対応

(ｱ)　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）

2011 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 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。

(ｲ)　データプライバシー保護に関する対応策の研究協力に向けた検討（内閣官房）

OECD や APEC 等の既存の国際的な議論の動向を踏まえつつ、日・ASEAN 情報セキュリティ政策会議等国際会議を通じて、環境の急速な変化に伴う、データプライバシー保護に関する対応策の研究協力に向けた検討を行う。

④ サイバー犯罪に対する態勢の強化

ア　犯罪取締りのための基盤整備の推進

(ｱ)　サイバー犯罪の取締りのための態勢の強化（警察庁）

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を積極的に実施するとともに、サイバー犯罪の取締りを行うための資機材の整備を推進するなど、サイバー犯罪に適切に対処するための態勢を強化する。

(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：１(1)エ】

(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）

サイバー犯罪に適切に対処するための官民の連携を強化するため、各都道府県警察におけるインターネットカフェ連絡協議会の設立等の取組を推進する。

(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するなどし、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：１(1)エ】

(ｶ)　中央当局制度[26]を活用した国際捜査共助の迅速化（法務省及び警察庁）

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。

[26] 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。

イ　犯罪抑止のための広報啓発の推進

(ｱ)　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（警察庁、総務省及び経済産業省）

2010 年度に引き続き、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を公表するなどの取組みを通じ、不正アクセス行為に対する防御に関する啓発及び知識の普及を図る。

(ｲ)　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を交えた講演等を全国各地で実施する。

(ｳ)　サイバー犯罪の被害防止対策の推進（警察庁）

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、サイバーボランティアの育成を支援し、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。

(3) 国際連携の強化

二国間関係の強化については、従来の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及び英国をはじめとする関係国との連携を推進する。

ASEAN 地域との連携については、連携枠組みに基づく施策を着実に実施するとともに、第４回日 ASEAN 情報セキュリティ政策会議において、これまでの取組みの評価及び今後の協力の在り方の検討を行う。

国際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。

① 米国、ASEAN、欧州等との連携強化（二国間、ASEAN との関係強化）

(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）

情報セキュリティ政策における地域間の緊密な連携を構築するため、2011 年度中に、米国と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二国間会合を開催して、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、引き続き戦略的二国間連携の強化を図る。また、英国をはじめとする欧州諸国等と情報セキュリティ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。

(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引き続き ASEAN 諸国との連携を強化する。

a) 第 3 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(2011 年度)

b) 日・ASEAN 情報セキュリティ政策会議をマレーシア（第４回、2011 年度)、 5

回日・ASEAN 情報セキュリティ政策会議を開催（第５回、2012 年度）
c) 第３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我が国で開催
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（2011 年度）
e) ASEAN 諸国との普及啓発共同事業の実施（2011 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（2011 年度）
g) 具体的な研究協力の実現に資するため、我が国と ASEAN 加盟国においてネットワークセキュリティ分野の研究活動に取り組んでいる研究者及び研究機関を特定（2011 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）

我が国と APEC 域内各国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等の連携を推進する。

(ｴ) 途上国向け研修・セミナー等の開催（総務省）

途上国の政府関係者及び電気通信事業者等を対象とした情報セキュリティ研修を実施する。

(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）

2011 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）

2008 年の日・ASEAN 経済大臣会合で我が国より提唱した「アジア知識経済化イニシアティブ」に基づき、アジア域内におけるセキュアな投資・ビジネス環境の構築を推進するための政策や取組についての検討を進めるとともに、関係者との対話を実施する。

また、情報セキュリティ製品の評価・認証制度に関し、関係国に対し、国際慣行に沿った対応を促していく。

さらに、アジア版情報セキュリティ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に着手する。

(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。2011 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。201１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 (Forum of Incident Response and Security Teams)、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、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。

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) 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：２(1)④エ】

② APEC、ARF、ITU、MERIDIAN、IWWN 等国際会合を活用した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(Asia -Pacific Economic Cooperation) 、OECD(The Organizations for Economic Cooperation and Development)、ASEAN(Association of South - East Asian Nations)、EU (European Union)、G8 (Group of Eight)等のグローバルな経済活動に係る分野、FIRST(Forum for Incident Response and Security Teams)等のインシデント対応に係る分野、ARF (ASEAN Regional Forum)等の国家安全保障に係る分野、ITU(International Telecommunications Union)や ACF (APT Cybersecurity Forum)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。

(ｲ) 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：２(3)①】

(ｳ) 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 IPA が主体となって設立した AISEC(Asian IT Security Evaluation and Certification) Forum の第３回会合（2011 年 11 月に開催予定）において、アジア地域の国々の評価・認証制度確立のための支援及びセキュリティ評価・認証の技術や動向について情報交換を行う。

(ｴ) 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/SC27、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。

(ｵ) クラウドコンピューティングのセキュリティ（経済産業省）

【再掲：２(1)④イ】

③ 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（Point of Contact）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。たとえば、2011 年度中に戦略及び本文書の英語版を NISC の Web ページに公開するなど、ホームページ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。

(4) 技術戦略の推進等

「情報セキュリティ研究開発戦略」に基づき、社会を支える基盤として、より安全・安心で、新しい価値を創造できる情報通信システムを実現するために、世界を先導し、「ゲーム・チェンジ」を実現する、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。

「情報セキュリティ人材育成プログラム」に基づき、情報セキュリティ人材の育成に積極的に取り組む。

① 情報セキュリティ関連の研究開発の戦略的推進等

(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[27]、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) クラウド対応型セキュリティ技術の研究開発（総務省）

【再掲：２(1)④イ】

(ｳ) 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、研究開発を 2010 年度に引き続き実施する。

(ｴ) 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）

NICT において、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

[27] 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。

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。

2011 年度は、昨年度までに構築したマルウェア対策ユーザーサポートシステムの実験環境を用いて、一般ユーザーを募った実証実験を実施し、システムの有効性検証を行う。

(オ) 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）

NICT において、2012 年度中に、情報通信ネットワークの安全性を保障する上で、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を目指し、2011 年度は、2010 年度の成果を活用して、評価手法に関して詳細設計や拡張、及び評価システムの検証基盤の構築を行う。

(カ) サイバーセキュリティ研究テストベッドの構築（総務省）

NICT において、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。

2011 年度は、セキュリティデータセットの安全な外部利用のための、フィルタリング機能やサニタイジング機能に関する基礎検討を行い、プロトタイプ開発を行う。

(キ) IPv6 環境のセキュリティ評価システムの構築（総務省）

【再掲：２(1)③】

(ク) 新世代ネットワーク基盤技術に関する研究開発（総務省）

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。2011 年度は、各要素技術の有機的な融合等によるシステム構成技術や多様なネットワークサービスを収容するプラットフォーム構成技術等に取り組む。

(ケ) ソフトウェア構築状況の可視化技術の開発普及（文部科学省）

「事故前提社会」への対応力強化として、ソフトウェアに対するトレーサビリティの概念を普及させ、世界最高水準の安心・安全な情報通信社会を実現す

るため、オフショアを含むマルチベンダによるソフトウェア開発に関する実証的データ(エンピリカルデータ)を収集し、ソフトウェア開発が適正な手順で行われたかどうかをソフトウェア発注者によって把握・検証可能とする「ソフトウェアタグ」をソフトウェア製品に添付して提供する技術を 2011 年度末までに開発する。2011 年度は、本研究課題の最終年度として、ソフトウェアタグ普及の基盤を構築するため以下を実施する。

① ソフトウェアタグの適用実験の分析にもとづきタグ運用基盤の仕様を決定し、リファレンス実装とともに公開する。
② ソフトウェアタグ生成基盤ツールの評価と機能拡張、可視化・評価ツール群との連携を進め、実用化サービス基盤の要件をまとめる。
③ ソフトウェアタグが国際規格として採用されるよう活動を実施する。
④ 法的な観点からソフトウェアタグの適用について検討を行うとともに、ユーザー・ベンダ間の紛争解決基準のとりまとめを試みる。

(ｺ) 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 2011 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。

(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）

【再掲：２(1)④イ】

② 情報セキュリティ人材の育成

(ｱ) 「情報セキュリティ人材育成プログラム」の推進（内閣官房及び関係府省庁）

中長期的な視点による情報セキュリティ人材の育成・確保方策の在り方について取りまとめた「情報セキュリティ人材育成プログラム」に基づき、「普及・啓発人材育成委員会」等の設置、先端的な情報セキュリティ研究者・技術者等の育成、政府機関、企業及び教育機関における人材育成、官民連携、国際連携等の施策の着実な推進を行う。

(ｲ) 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）

a) 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。

b) IPA において、セキュリティ LSI 等を用いたシステムの安全性評価体制の構築及び次世代の暗号モジュール試験関連規格に対応するため、セキュリティ LSI に対するサイドチャネル攻撃を含む耐タンパー性評価を行うための人材の育成を行う。

(ｳ) 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（IT Professionals Examination Council)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行く。

(ｴ) 情報セキュリティ資格の周知（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の周知を図る。

(ｵ) 途上国向け研修・セミナー等の開催（総務省）

【再掲：２(3)①】

(ｶ) 情報セキュリティ・サポーターの育成・活用（総務省）

【再掲：２(2)②】

(ｷ) サイバー攻撃等対処に向けた人材育成の取組（防衛省）

【再掲：１(1)ウ】

③ 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) 2011 年度は、企業における新たな情報セキュリティガバナンスの導入に際して、情報セキュリティが明確に位置付けられるための方策について検討し、報告書をまとめる。

c) 2008 年度に IT ガバナンスや運用面を強化して改訂した「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。

d) 2010 年度において、評価指標に基づいて評価された実プロジェクトのデータの収集・解析を実施した。この解析結果を共有することを可能にするツールを、2011 年度を目処に公開する。

(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 23 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。2011 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。2011 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。

(5) 情報セキュリティに関する制度整備

サイバー犯罪に適切に対処するための法整備を推進するとともに、サイバー空間の安全性・信頼性を向上させる制度について積極的な検討を行う。

① 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、新設されたいわゆるウイルス作成罪等についての内容の周知の徹底に努めるとともに、手続法規定について円滑な施行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協力（外務省）

平成 23 年６月にサイバー犯罪条約の国内担保法が成立した（未施行）ことを受け、早期に同条約を締結できるよう、関係府省庁と協力して準備を進めていく。

(ｳ) サイバー空間の安全性・信頼性を向上させる制度の検討（内閣官房）

「サイバー空間の安全性・信頼性向上のための課題等について」（2011 年３月）を踏まえ、昨今の情報セキュリティをめぐる環境変化に対応したサイバー空間の安全性・信頼性を向上させる制度に係る課題について引き続き検討を行う。

(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：２(1)④エ】

(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：２(1)④キ】

② 各国の情報セキュリティ制度の比較検討

㈠ 各国のセキュリティ法制度の調査（内閣官房）

引き続き主要国等の法制度の調査・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。

Ⅴ　東日本大震災を踏まえた情報セキュリティ政策

東日本大震災からの復旧・復興、そして新たな成長に寄与するため、情報セキュリティの視点から、災害時に強靭な情報通信システムの構築や「リスク・マネジメント」、「リスク・コミュニケーション」の確立、情報システム全体の「ニュー・ディペンダビリティ」の確保等に努め、被害状況や経験を踏まえた大規模災害時における安全性・信頼性の向上を図る。

(1) 災害時に強靭な情報通信システムの構築

(ｱ) 政府機関における適切な物理的セキュリティ対策の検討（内閣官房）

内閣官房は、東日本大震災といった物理的セキュリティに甚大な影響を及ぼす可能性のある環境変化に対応するため、民間事業者等における先進的事例等を調査し、各府省庁における適切な物理的セキュリティ対策の在り方を検討する。その上で、政府機関における実態等を踏まえ、指針等として取りまとめる。

(ｲ) 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）

各府省庁においては、東日本大震災といった情報システムに多大なる影響を及ぼす可能性のある環境変化の際にも、適切なセキュリティ対策を実施することが求められる。そのため、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とともに、各府省庁で保有する情報資産の範囲及びその取扱方法の明確化を図ることを目的に、政府機関におけるリスク・マネジメント手法の在り方を検討し、指針等として取りまとめる。また、その成果を各府省庁に対して共有することで、各府省庁相互におけるリスク・コミュニケーションの醸成を図る。

(ｳ) 業務継続能力の強化（内閣官房及び全府省庁）

a) 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 年度末までに必要な情報システムについて運用を継続するために必要な計画を策定する。

b) 内閣官房は、各府省庁において策定される情報システム運用継続計画につき、対策レベルの維持・継続的改善に向けた適切なマネジメントに資するよう、

当該計画の評価手法について検討する。

(エ) 重要インフラ分野における IT システムの再検証（内閣官房）

重要インフラ分野において、大震災で情報システムが受けた被害とその重要インフラサービスへの影響、当該事業者が行った応急・復旧対応とその効果を調査・分析する。特に今回の大震災では、被害の連鎖が大きく影響したことを踏まえ、既往調査で設定した重要インフラ分野間の相互依存性についても検証する。

また、これらに基づき、サプライチェーンをどのように確保するかという視点を加えながら、大規模災害時において最低限維持すべき IT システムの機能、その機能を維持するためのシステムの堅ろう化、データの完全な消失の防止等の対応策の検討を順次進め、今後の安全基準の指針の見直しや情報システムの視点からの BCP の検討に必要に応じて反映するとともに、分野横断的演習等の機会を活用して検証を行う。

(オ) 重要インフラで利用される情報システムの信頼性向上のための支援体制の整備（経済産業省）

a) 2010 年度に引き続き、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) 重要インフラ等の制御システムの脆弱性低減のための情報セキュリティ対策を普及・啓発するための資料作成に向け、製造事業、プラント事業の制御システム及び次世代伝送網（スマートグリッド）等のセキュリティへの対応について国内外の状況を調査する。

(カ) 大災害発生直後の情報通信システムの在り方の検討（内閣官房及び総務省）

大災害発生直後は、想像を絶する混乱状態にあり、それ故、一秒でも早くその状況を把握出来る情報通信システムの確立は、焦眉の急である。

今回の大震災において、現地の一人ひとりの創意工夫により、SNS などインターネットを活用した安否情報の確認など、災害時に我が国が今まで経験したことのない情報伝達、情報共有の方法が報告されている。

大震災発生直後の情報伝達等の状況を調査、分析することにより、情報セキュリティの観点から、「リスク・コミュニケーション」の視点も包含し、災害発生直後における情報伝達における産・学・官及び個人の役割を再定義した上で、非常時における情報システム、情報伝達の在り方を検討する。この検討は、年

度計画に記述している他の項目と併せて行う。

(ｷ) 情報セキュリティ技術の耐災害性の向上（内閣官房）

内閣官房は、災害発生時における情報連絡や情報共有が確実かつ正確に行えるようにするため、今回の大震災を踏まえ、災害時における認証方式や暗号化方式など情報セキュリティ技術に係る課題について検証し、情報セキュリティ技術の耐災害性の向上を図る。

(2)「リスク・マネジメント」、「リスク・コミュニケーション」の確立

(ｱ) 東日本大震災による情報システムへの影響分析及び評価（内閣官房）

内閣官房は、各府省庁の情報システム運用継続計画の策定・改善等に資するため、東日本大震災による情報システムへの影響を分析・評価し、適宜、各府省庁に対する情報提供を行うとともに、業務継続能力の強化に向けた検討等に反映する。

(ｲ) 東日本大震災を踏まえたリスク・マネジメント手法の検討（内閣官房）

災害時においては、潜在的リスク等について、関係者に正確な情報を迅速かつ十分に伝え、関係者間で合意形成を図っておく必要がある。このため、東日本大震災を踏まえ、リスク・コミュニケーション及びそれを活用したリスク・マネジメント手法の有効性を検討する。

(ｳ) 個人情報等の柔軟管理方法等の検討（内閣官房及び関係府省庁）

電子化された個人情報等を柔軟に管理することを可能とするため、その技術的手段及びマネジメント手法の検討に係る取組を推進する。

(ｴ) 重要インフラ事業者間の相互連携の拡充（内閣官房）

大震災に関する調査を基に、想定を超える被害が発生した状況で事業継続計画等に基づく対策をどのように変更したか、応急・復旧対応における事業者間、分野間の連携がどのように行われたか等について分析を加え、状況のダイナミックな変化に応じてリスクレベルも合せて変動させていくようなダイナミック・リスク対応の在り方を検討するとともに、大規模な災害・障害時の事業者間、分野間の協力促進に有効な共有情報を抽出する。

(ｵ) 重要インフラ分野間のリスク・コミュニケーションの促進（内閣官房及び重要インフラ所管省庁）

大震災において複数の重要インフラ分野が広範囲かつ横断的に被災したことを踏まえ、大規模災害対応の経験・教訓を重要インフラ分野間で共有する等のリスク・コミュニケーションを促進する。この取組みを通じ、ダイナミック・リスク対応に関する認識を深める。実施に当たっては、重要インフラ所管省庁や関係機関、セプターカウンシル等との連携を図る。

(ｶ) 「安全基準等」策定指針への震災関連の知見の反映（内閣官房及び重要インフラ所管省庁）

重要インフラにおける大震災への対応から得られた知見を有効に活用していくために、重要インフラ分野間のリスク・コミュニケーション等で得られた教訓等を踏まえ、「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）」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への反映等について検討を行う。

(ｷ) 重要インフラ分野におけるリスク・マネジメントの在り方の検討（内閣官房）

重要インフラ分野における大震災に関する調査・分析から、システムの堅ろう化やデータ保全等の視点を取り入れてリスク・マネジメントの在り方を検討する。得られた知見は、分野横断的演習等においてその実効性を検証するとともに、情報システムの安定運用のための BCP に盛り込むべき視点等として活用する。

(3) 情報システム全体の「ニュー・ディペンダビリティ」の確保

(ｱ) 「情報セキュリティ研究開発戦略」の推進（内閣官房及び関係府省庁）

情報システムのニュー・ディペンダビリティを確保するため、「情報セキュリティ研究開発戦略」に掲げられた耐災害性の高い情報通信システムの実現のため、リアルとバーチャルが融合した次世代ネットワークにおける情報セキュリティ基盤技術、障害に対する自動リカバリー可能なネットワーク・アーキテクチャの構築技術に係る研究開発を促進する。

(ｲ) システムのセキュリティ設定を上位から下位まで自動保証する技術の研究開発の推進（総務省）

NICT において、情報セキュリティ確保における重要な要素である、正しいセキュリティ設定を自動的に実現・検証する技術を確立するため、適材適所にセキュリティ技術を自動選択し、セキュアなネットワークを最適に構成するためのセキュリティアーキテクチャの研究開発を推進する。

(ｳ) 最先端のグリーンクラウド基盤構築に向けた研究開発（総務省）

2012 年度までに、平常時においては全体の２～３割もの省電力化を図りつつ高信頼・高品質なクラウドサービスを提供するとともに、広域災害時には重要なデータの消失を防ぐため、複数のクラウド間を瞬時に連携させる技術の確立を目指し、引き続き要素技術の開発、機能検証等を実施する。

(ｴ) 新世代ネットワーク基盤技術に関する研究開発（総務省）

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。2011 年度は、各要素技術の有機的な融合等によるシステム構成技術や多様なネットワークサービスを収容するプラットフォーム構成技術等に取り組む。