情報セキュリティ２０１０

2010 年 7 月 22 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対策については、2006 年度から 2008 年度までは、「セキュア・ジャパン」の実現を目指した「第 1 次情報セキュリティ基本計画」（2006 年２月２日）により、2009 年度からは、同計画を「継続・発展」させることとした「第２次情報セキュリティ基本計画」（2009 年２月３日）に基づき、官民の各主体によって取組が推進されてきた。

しかし、2009 年７月の米韓における大規模サイバー攻撃事態等により、情報セキュリティ上の脅威が、安全保障・危機管理上の問題となり得ることが明らかとなる一方、情報セキュリティ上のリスクが多様化・高度化・複雑化し、従来の取組では情報セキュリティの確保が困難な状況が発生していた。

このような環境の変化に的確に対応するため、新たに「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。）を策定した。

同戦略では、

① サイバー攻撃事態の発生を念頭に置いた政策の強化及び対処体制の整備

② 新たな環境変化に対応した情報セキュリティ政策の確立

③ 受動的な情報セキュリティ対策から能動的な情報セキュリティ対策へ

を基本方針として、2020 年までに、世界最先端の「情報セキュリティ先進国」を実現するため、

① IT リスクを克服し、安全・安心な国民生活を実現

② サイバー空間の安全保障・危機管理に係る政策の強化と社会経済活動の基盤としての情報通信技術政策との連携

③ 安全保障・危機管理及び経済の観点に、国民・利用者保護の観点を加えた３軸構造の総合的な政策の確立。特に、国民・利用者の視点を重視した情報セキュリティ政策を推進

④ 経済成長戦略に寄与する情報セキュリティ政策の確立

⑤ 国際連携の強化

に重点的に取組むこととした。

具体的には、今後４年間について、「第２次情報セキュリティ基本計画」に規定された施策に加え、戦略内で明示された具体的な取組を推進していくこととした。

本文書「情報セキュリティ 2010」は、戦略に基づく年度計画である「セキュア・ジャパン 20XX」に該当し、2010 年度及び 2011 年度に実施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。

II　具体的な取組

情報セキュリティ政策の推進にあたっては、情報セキュリティ事案発生時に的確な対応を行い、国民の安全・安心を確保することは言うまでもないが、今後、益々高度化・多様化する情報セキュリティ事案に的確に対応するためには、我が国全体の「基礎対応力」を常に向上させておくことが不可欠である。そのためには、強力なリーダーシップの下、内閣官房が中心となり関係省庁が連携した総合的な政策推進体制を確立することが重要である。特に、国境を越えて様々な事態が発生する可能性が高まることから、国際的な連携を強化する必要がある。

また、情報システムの構築や通信サービスの提供や利用等、情報通信技術基盤の構築・提供・利用が民間分野において行われていることから、情報セキュリティ政策の推進にあたっては、官民それぞれの役割分担を明確にしつつ、官民連携の強化を図っていく必要がある。

さらに、「事故前提社会」であるとの認識を共有するとともに、そのような社会に対する対応力を強化するため、持続的に情報セキュリティ対策の取組を改善していく必要がある。そのためには、政府の取組の成果を可視化し評価した上で、継続的に取組を改善・向上させていく仕組みを確立していくことが重要である。

戦略に記載された以上のような状況を踏まえ、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、2010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

2009 年 7 月に米韓において発生したような大規模なサイバー攻撃事態が、今後我が国においても発生する可能性があること等を踏まえ、国民の生命、身体、財産又は国土に重大な被害が生じ、又は生じるおそれのあるサイバー攻撃事態（大規模サイバー攻撃事態）の発生時における対処態勢の整備、及び「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」等に基づく官民情報共有体制を活用した平素からの情報収集・共有体制の強化を図る。

取組の推進に当たっては、未然防止等の観点から平素からの取組を行う部局と、大規模サイバー攻撃事態発生時の対処を行う部局との十分な連携を図り、総合的な対処に努める。

(1) 対処態勢の整備

・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

「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、大規模サイバー攻撃事態が発生した際に政府及び関係機関が迅速かつ適切な初動対処をとるための態勢を整備する。併せて、大規模サイバー攻撃事態が発生した際の初動対処に係る訓練を実施する。

【具体的施策】

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などにより、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よう努める。

イ）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[1]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。

・官民連携の推進

大規模サイバー攻撃事態における対処においては、重要インフラ事業者等からの協力が不可欠であることにかんがみ、官民が緊密に連携できるよう、重要インフラ事業者等の理解と協力の促進に努める。

【具体的施策】

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

[1]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。

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からの依頼に応じ、国際的な CSIRT[2]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。

・サイバー攻撃に対する防衛分野での体制の強化

諸外国において戦力強化が必要とされる分野としてサイバー空間が取り上げられていること等を踏まえ、防衛分野におけるサイバー攻撃対処能力の強化を図る。

【具体的施策】

ア）サイバー企画調整官(仮称）の新設（防衛省）

2010 年度末に、防衛省統合幕僚監部にサイバー企画調整官（仮称）を配置し、サイバー攻撃に対する態勢を強化する。

イ）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・対処能力をさらに向上させるため、ネットワークセキュリティ分析装置を研究試作するとともに、2009 年度に引き続き、不正アクセス監視・分析技術、サイバー攻撃分析技術及びアクティブ防御技術等について基礎的な研究を実施する。

ウ）情報保証に係る最新技術動向等の調査研究（防衛省）

2009 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に係る最新技術動向を継続的に調査するとともに、一元的な対処態勢等について調査研究を実施する。

[2] Computer Security Incident Response Team の略

・サイバー犯罪の取締り

デジタルフォレンジックの活用や国際的な捜査機関協力の推進を通じ、サイバー犯罪の取締りを推進する。

【具体的施策】

ア）デジタルフォレンジック[3]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、デジタルフォレンジック連絡会の開催等を通じた国内関係機関との連携、技術協力を始めとした官民連携等、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。

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。

・サイバー攻撃への対処に係る国際連携の強化

サイバー攻撃等に係る情報交換、国際会議等への積極的な参加を通じ、国際連携の強化を図る。

【具体的施策】

ア）サイバー攻撃に関する情報交換（内閣官房及び関係府省庁）

諸外国関係機関との２国間情報交換等を通じ、サイバー攻撃の攻撃主体・方法等の対処に資する情報収集・分析を継続的に実施する。

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、2010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

[3] 不正アクセスや機密情報漏洩等、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。

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

・対処に資する情報の収集・分析・共有体制の強化

内閣官房と各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。

【具体的施策】

ア）サイバー攻撃事態への対処に資する情報の集約・共有等（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を、各府省庁が収集して内閣官房に集約し、各府省庁等の必要な範囲に適時・適切に共有される体制を強化する。

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）

2009 年度に引き続き、GSOC[4]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)・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】

[4] Government Security Operation Coordination team

・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

諸外国の関係機関・国際組織と内閣官房及び関係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共有体制の構築・強化を図る。

【具体的施策】

ア）サイバー攻撃に関する情報共有体制の構築･強化（内閣官房及び関係府省庁）

諸外国関係機関との２国間情報交換等を通じ、サイバー攻撃の攻撃主体・方法等の対処に資する情報収集・分析を継続的に実施するなど関係機関との既存の情報共有体制の強化を推進するとともに、意見交換等を通じた新たな情報共有体制の在り方を検討する。

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)・サイバー攻撃への対処に係る国際連携の強化】

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

・最高情報セキュリティ責任者（CISO）の機能強化

最高情報セキュリティ責任者（CISO）連絡会議の設置や最高情報セキュリティ・アドバイザー連絡会議の設置等を通じて、各省庁の CISO の機能強化を図る。また、各府省庁の CISO が情報セキュリティ報告書を作成し、公表を行うことにより、自ら問題意識を持って情報セキュリティ対策の改善を図る。

【具体的施策】

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最高情報セキュリティ責任者連絡会議（正式名称は「情報セキュリティ対策推進会議」）を速やかに開催し、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) 最高情報セキュリティ責任者連絡会議の下に最高情報セキュリティ・アドバイザー等連絡会議を設置し、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を踏まえ、省内外の知見を活用しつつ、2010 年度から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を確保する観点から、外部監査制度の活用についても、可能な限り推進する。

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、最高情報セキュリティ責任者連絡会議の場において報告した後、準備の整った府省庁においては公表する。

・政府横断的な情報収集・分析システム（GSOC）の充実・強化

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、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。　（注） GSOC: Government Security Operation Coordination team

【具体的施策】

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、関係連携機関との連携強化、海外政府機関等との意見交換を進めること等により、サイバー攻撃等に関する情報収集能力、分析・解析能力を強化するとともに、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) 2010 年中に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。

・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

政府機関のサーバ集約化等を通じて、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。また、各省庁の情報セキュリティ対策の評価を通じて、取組の持続的な改善を図る。

【具体的施策】

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。

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 年中に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。

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）

2010 年度は、新たに設置する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。

エ）業務継続計画の策定の推進（内閣官房及び全府省庁）

a) 各府省庁は、引き続き、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、必要な情報システムについて業務継続計画の策定を推進する。

b) 内閣官房は、各府省庁による 2011 年度末までの業務継続計画の策定を支援するべく、2010 年度末までにガイドラインを作成するなどの取組を行う。

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）

a) 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」を策定するために、必要な取組を行う。

b) 本ガイドラインの対象となるオンライン手続を所掌する各府省は、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、情報セキュリティ対策推進会議等の場において、専門的知見を有する者からの助言等を受け、決定するとともに、業務・システム最適化に係るものは、計画への反映状況について、CIO 連絡会議等に報告する。

カ）政府全体での PDCA サイクルの定着と浸透（内閣官房及び全府省庁）

a) 内閣官房は、各府省庁の対策の実施状況を、政府機関統一基準に基づき、対策実施状況報告をもとに客観的に比較可能な形で評価し、勧告することにより、各府省庁の対策の改善と政府機関統一基準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。そのために、調査項目・方法を改善するなど自己点検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。

b) 評価の結果については、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公表することとする。

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し、各府省庁とともに対応策等について検討・共有する場を新たに設け、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）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。これを参考に各府省庁は、役割に応じた教育教材を整備する。

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。

コ）政府機関から発信する電子メールに係る成りすましの防止（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(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。

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。

サ）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）

2010 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）を利用するよう取り組むとともに、当該取組状況を国民に対して広く周知する。

・政府機関における安全な暗号利用の推進

政府機関で使われている電子政府推奨暗号について、移行指針に従って暗号の着実な移行を進める。また、電子政府推奨暗号の安全性を継続的に監視・調査し、安全性が低下した暗号については速やかに代替となる暗号への移行を進めるための計画を策定するとともに、急激な安全性の低下に備え、あらかじめ緊急避難的な対応（コンティンジェンシープラン）を検討する。

【具体的施策】

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 2010 年度に行う。

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) 内閣官房、総務省及び各府省庁は､「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」[5]に従った取組を推進するとともに、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）についても検討を行う。

d) 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。

[5] 2008 年４月 22 日 情報セキュリティ政策会議決定

・クラウドコンピューティング[6]技術における情報セキュリティの確保等

情報システムの統合・集約化等を可能とするクラウドコンピューティング技術について、電子行政へ効率的に活用するため必要となる情報セキュリティ確保方策を検討する。

また、先進的なセキュリティ対策事例を踏まえ、政府機関においてもテレワークの環境整備を推進する。

【具体的施策】

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た「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含む要求仕様を明確化し、内閣官房は、政府機関統一基準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。

・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

現行の政府機関統一基準の定着を図るとともに、情報通信技術や環境の変化を踏まえ、政府機関統一基準の見直しを適時に行い、新たな情報セキュリティ上の脅威に対応する。

【具体的施策】

ア）政府機関統一基準の見直しの実施（内閣官房）

技術や環境の変化を踏まえ、政府機関統一基準の見直しを行う。特に、2010年度は、クラウドコンピューティング技術等の新たな技術動向等を踏まえた見直しを行い、政府機関統一基準（第５版）に向けた改訂作業を実施する。

イ）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)、独立行政法人情報処理推進機構（IPA）等の独立行政法人や情報セキュリティ関係団体等の研究者・実務家の知見を蓄積・活用し、政府機関統一基準等の施策に反映するため、既存の枠組みを活用しつつ協力体制を構築し、内閣官房と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する。

---

[6] 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。

ウ）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省庁と必要な調整を進める。

エ）安全性・信頼性の高い IT 製品等の利用推進（内閣官房及び全府省庁）

2010 年度も引き続き、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、政府機関統一基準に基づき、「IT セキュリティ評価及び認証制度[7]」により認証された製品等を優先的に取り扱う。

オ）情報セキュリティに配慮したシステム選定・調達の支援（内閣官房及び経済産業省）

a) 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、2010 年に、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、政府機関等における活用を促進する。

b) 諸外国における状況も勘案しつつ、政府機関統一基準に定められている政府情報システム等の調達時における「IT セキュリティ評価及び認証制度」、「暗号モジュール試験及び認証制度」の認証取得の要否に関する要件の一つである「重要なセキュリティ要件」がある場合等について、その明確化を行い、上記統一基準の反映に資する。

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・政府機関における安全な暗号利用の推進】

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・政府機関における安全な暗号利用の推進】

[7]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。

・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

情報システムに係る政府調達について、企画段階から情報セキュリティ対策を適切に組み込む方策を検討し、情報システムに組み込むべき情報セキュリティ要件を定める。
また、情報セキュリティに係る評価・認証取得が必要となる情報セキュリティ要件の明確化を図ること等により、当該評価・認証を受けた製品の活用が促進されるよう取り組む。

【具体的施策】

ア）予算面での取組（全府省庁）

各府省庁は、情報セキュリティ対策について、システム予算全体の中で必要な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、情報システムの調達においては、必要なセキュリティ対策を確実に実施するため、要求仕様に可能な限り要件として記載し、保守契約等においても適時適切な対応が可能となるような契約を交わすなどの取組を進める。

イ）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、政府機関統一基準等を踏まえ、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のセキュリティの確保のための取組を進める。

ウ）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）

情報システムの企画・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意識するための方策（Security by Design）について、2010 年度は、情報システムに係る政府調達に関して、当該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について検討をおこない、情報システムに組み込むべき情報セキュリティ要件の取りまとめを行う。

エ）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・政府機関における安全な暗号利用の推進、２(1)①・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】

オ）「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）」について、民間企業や政府機関における活用・普及を促進する。

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）

a) 情報システムの調達者の業務を支援するため、情報システムの主要な構成要素の技術的セキュリティ要件に関する情報を提供するツールを開発する。

b) 「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。

c) 「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。

キ）安全性・信頼性の高い IT 製品等の利用推進（内閣官房及び全府省庁）【再掲：２(1)①・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】

ク）情報セキュリティに配慮したシステム選定・調達の支援（内閣官房及び経済産業省）【再掲：２(1)①・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】

・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

社会保障・税の共通番号制の検討に際し、プライバシーポリシーの下で適切な情報セキュリティ対策が講じられるよう、課題の抽出及び解決方策の検討を行う。

【具体的施策】

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、適切なプライバシー保護対策及び情報セキュリティ対策がとられるよう、検討を行う。

・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

政府機関統一基準等の見直し等を行うとともに、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一層の推進を図る。

【具体的施策】

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) 地方公共団体における ICT 部門の業務継続計画の策定、情報セキュリティ監査の実施、情報資産台帳の作成及びリスク分析の実施等の促進を図るため、業務継続計画に関するセミナー等の開催や内部監査アドバイザーの派遣を実施する。また、情報セキュリティポリシーガイドラインの見直しを行う。

b) 情報セキュリティベストプラクティスやモデルケースの募集、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。

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（総務省及び文部科学省）

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）

すべての地方公共団体の職員が、時間や場所に制約されずに受講できる情報セキュリティに関する e ラーニングの内容の充実とその実施を促進する。

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) 2009 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。

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）

2009 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、2010 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、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

重要インフラの関係主体は、「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」に基づいて、重要インフラサービスの維持に努め、また、ＩＴ障害発生時の迅速な復旧等を確保することに努めることとする。これに加え、最近の環境変化を踏まえ、国民生活に重大な影響を及ぼすおそれのある重要インフラに対する情報セキュリティ上の脅威に的確に対応する。

（「分野横断的な官民連携体制」の強化）

各重要インフラサービスの情報通信技術に対する依存性が高まり、重要インフラサービスにおける情報セキュリティ上の脅威も高度化、多様化していること等を踏まえ、官民の役割分担を明確にした上で、官民の緊密な連携の下、重要インフラ分野の情報セキュリティ対策を強化するため、以下の事項に重点的に取り組む。

・情報共有体制の強化

重要インフラにおける情報セキュリティ対策に資する情報共有体制を強化するため、これまでに整備された官民の役割分担に基づき、情報提供、情報連絡等に必要な環境整備等を実施する。

【具体的施策】

ア）共有すべき情報の整理（内閣官房）

a) 重要インフラ事業者等のサービスの維持・復旧の容易化に資するため、下記イ）に掲げる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、社会動向の変化等を踏まえ、共有すべき情報についての整理を行い、共有すべき情報について引き続き整理・充実を行う。

b) 2009 年度の検討による共有が望まれる情報のまとめを基に、2010 年度は、関係主体の保有する情報の確認、提供に際しての制約等の整理を行うとともに、関係主体の保有する情報ごとに、重要インフラ事業者等にとって有用な情報の共有の方法等（即応性の観点等を含めたタイミング、様式、方法等）の検討を行う。また、2011 年度末を目処に整理結果の全体取りまとめを行い、公表を行う。

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の維持・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」（以下「実施細目」という。）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 2010～2011 年度の各年度末に、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、必要により改訂を行う。

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[8]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ルールのそれぞれについて、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、2010 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、2009 年度に拡充した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

[8] CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response

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。検討に当たっては、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。

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）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）

JPCERT/CC を事務局として 2008 年度に発足した「制御システムベンダーセキュリティ情報共有タスクフォース」の活動をベースに、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。また、制御システムのセキュリティ水準を評価できるツール類の有効性検証を行う。

ケ）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) ソフトウェア製品や制御システム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、迅速な対応及び利用者の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。

コ）「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・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】

・「セプターカウンシル」の活動促進

各重要インフラ事業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、分析体制の充実・強化に向けて、「セプターカウンシル」の活動を促進する。

【具体的施策】

ア）「セプターカウンシル」の支援（内閣官房）

2009 年２月に発足した重要インフラの各分野により構成され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、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分野横断的な情報共有の推進等の「セプターカウンシル」の活動を支援する。

・「安全基準等」の整備浸透

社会経済動向の変化等に対応し、また新たな知見を適時反映していくとともに、重要インフラ分野及び重要インフラ事業者等の「安全基準等」整備浸透を推進するため、「安全基準等」策定指針の分析・検証を行い、継続的な改善を図る。

【具体的施策】

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、重要インフラ所管省庁の協力を得つつ、指針の分析・検証を行い、「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)」を決定する。

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、引き続き同指針の分析・検証を行い、必要に応じて、2011 年以降における同指針の追補版の公表に向けた準備を行う。

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、2010 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〉

2010 年度中に「安全基準等」の分析・検証及び改定等の実施状況なら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〉

2010 年度当初に「安全基準等」の浸透状況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）ネットワークの IP 化に対応した電気通信システムの安全・信頼性確保（総務省）

ネットワークの 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・評価等を行う体制整備の在り方について 2010 年度中を目処に引き続き検討を行う。

・重要インフラ防護対策の向上

重要インフラ各分野における脅威の分析や分野横断的演習の継続的な実施を通じて、重要インフラ事業者等の情報セキュリティ対策を向上させ、重大な IT 障害等が発生した場合においても、その被害が局所化・最小化されるよう促す。

また、被害があった場合でもサービス提供が維持できるよう、制御システムを含め、システムの堅ろう化等について検討する。

【具体的施策】

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脅威として、2009 年度の分析で５つに類別した共通脅威について、2010 年度は共通性を踏まえ、脅威の具体的検討及び分析を行う。特に、システムを取り巻く技術環境の変化に伴う脅威に着目して実施する。また、これらに関する国内外の研究動向等の調査を行う。

実施に当たっては、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るとともに、分析結果をこれらの関係者に還元する。

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作成とそれに基づく分野横断的な演習を実施し、課題の抽出及び演習実施のための知見の整理を行う。なお、得られた課題や知見については、関係者間で共有するとともに、可能な範囲で公表する。

ウ）重要インフラに影響を及ぼす可能性の高い環境変化への対応（内閣官房）

情報セキュリティ対策に大きな影響を及ぼす可能性が高い環境変化を見いだすため、技術動向等を調査するとともに、被害があった場合でもサービス提供

が維持できるよう、制御システムを含め、システムの堅ろう化等について検討する。

2010 年度においては、IPv6 の導入や制御システムのオープン化等の環境変化が重要システムの堅ろう性に与える影響について基礎的な調査を実施する。

エ）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) 2009 年度に引き続き、重要インフラ事業者による情報システム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。

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(1)・官民連携の推進】

カ）重要無線通信妨害対策の強化（総務省）

a) 電波監視体制充実・強化３カ年計画に基づき、重要無線通信妨害事案の発生時の対応強化のため、2010 年 10 月から重要無線通信妨害申告受付について休日夜間の全国一元化を実施する。

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、2010 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・高機能化のため、広帯域監視技術等の調査研究を実施する。

・事業継続計画（BCP）の充実

重要インフラ事業者等において作成されつつある事業継続計画に関し、想定される情報セキュリティ上の脅威（大規模なサイバー攻撃、地震、疾病等）を踏まえ、災害対策等と調和する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。

【具体的施策】

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。

2010 年度中に課題抽出を行い、2011 年度中に対策の在り方について取りまとめる。

・重要インフラ分野における国際連携の推進

MERIDIAN（重要情報インフラに関する国際会合）等の国際会合を利用して、各国のベストプラクティスに関する情報の共有や活用、国際的な演習への参加等を通じた、重要インフラ分野における国際連携を促進する。

【具体的施策】

ア）重要インフラ分野での国際連携推進（内閣官房）

a) 重要情報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) 2010 年秋に世界的規模で行われるサイバー演習（Cyber Storm Ⅲ）に IWWNの一員として参加する。また、2011 年に我が国で IWWN 会合を開催することを目指して準備を行う。

c) 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。

③ その他の基盤強化

・マルウェア対策等の充実・強化等

マルウェアへの感染対策等を強化するため、情報セキュリティインシデントへの対応能力の維持・向上や利用者への普及・啓発といったコンピュータ等の情報セキュリティ対策を強化するとともに、情報セキュリティ脅威の収集解析システム等の充実や、利用者・ISP[9]等への情報提供を通じたネットワーク等の情報セキュリティ対策を強化する。加えて、国際的な連携を推進する。

また、マルウェア対策としての検体解析等を行う際のリバースエンジニアリングやダウンロードの適法性を明確化するための措置を速やかに講じる。さらに、脆弱性関連情報の速やかな流通により、不正アクセス等の未然防止に引き続き取り組む。

【具体的施策】

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、個人が負担感なく対応できるよう、2010年度までに総合的な枠組みを構築することを目標に、技術面及び対策面を含めた試行、検討を実施する。

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) ISP と協力してサイバー攻撃に関わる情報収集ネットワークを構築し、サイバー攻撃の事前防止・早期対策に向けた枠組みの構築を検討する。

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

[9] Internet Service Provider の略

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）マルウェアの難読化に対応したウイルス検出・対応技術の検討（内閣官房）

マルウェアの難読化やモジュール化によって、最新のウイルス対策ソフトでも検出困難なタイプが出現している状況に対し、高度化・多様化する攻撃等に対応できる技術の開発を推進する。2010 年度は、マルウェアの検体解析・対策の研究開発における課題について調査する。

イ）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）マルウェアに関する情報収集・提供（経済産業省）

a) インターネット上の Web サイトへ自動的にアクセスし、マルウェア等の収集･解析及び解析結果の蓄積を行うシステム(TIPS)を引き続き運用し、それらの情報を一般利用者へ提供する。また、ウェブサイトや可搬型媒体（USB メモリ等）による新たなウイルス感染手口等に呼応した的確な情報の収集・分析及び提供を行うため、ゼロデイ攻撃への対策を含む、TIPS 等の対策ツールの

機能強化を行う。

b) 情報セキュリティ対策普及の観点から、IPA が保有する又は他の事業より入手したマルウェア検体及び検体分析結果等を活用してウイルス対策ベンダと連携を行う。

エ）標的型攻撃の手法解明と対策情報の提供（経済産業省）

IPA の「不審メール 110 番」及び JPCERT/CC のインシデント対応により、それぞれが標的型攻撃の検体の収集・分析を実施し、関係機関と連携しつつ、攻撃手法の解析、対策の策定を行うとともに、必要な情報提供を行う。

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機能追加及び管理機能強化に着手する。

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 OS 等のサポート対象を拡張するとともに、ソフトウェア等のバージョンとセキュリティ設定を同時確認する等の機能を設ける。

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、セキュアコーディングセミナーの実施や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とともに、新たに発見された脆弱性への対応を行う。

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、体験的かつ実践的に学ぶツール「開発者向け脆弱性実習ツール」を開発し、公開する。

e) インターネット上でのやり取りされる脅威情報を自動的に収集・監視し、必要に応じて警報等する技術について検討する。

f) ソフトウェア製品等の脆弱性に対する迅速な対応を図ることを可能とする脆弱性ハンドリング体制等の検討を行う。

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。2010 年度は、特に iLogScanner については最新の攻撃パターンへの対応、検出対象のアクセスログフォーマットの追加、Web Application Firewall(WAF)のログ解析機能（対象は ModSecurity）の追加を行い、年度中に公開する。

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・情報共有体制の強化】

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・情報共有体制の強化】

IV) 他の関連取組

ア) サービス妨害攻撃対策に係る調査・情報発信（経済産業省）

Web 等を活用した企業活動の妨げになり得る DDoS(Distributed Denial of Services)攻撃等のサービス妨害攻撃の事例及び対策方法について検討し、DDoS 攻撃等への対処に役立てるため、検討結果を企業等の対策担当者に提供する。

イ）情報漏えい対策への取組（経済産業省）

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ウイルス感染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。

ウ）DNSSEC 導入の促進（総務省）

2010 年度においては、DNSSEC（DNS における応答の正当性を保証するための拡張仕様）の円滑な導入に向けた周知等を実施する。

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。2010 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。

オ）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・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】

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、2008 年の法改正によりオプトイン方式が導入された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) 内閣官房は、悪意の第三者が政府機関又は政府機関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（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。

・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

クラウドコンピューティングを利用したサービスを構築・運用・利用するための情報セキュリティ要件に関するガイドライン、クラウドコンピューティング技術の適用が見込まれる分野ごとの情報の取扱い等に関するガイドライン等を検討、策定する。

【具体的施策】

ア）クラウド化に対応した情報セキュリティ確保方策の検討（内閣官房、総務省及び経済産業省）

クラウドサービスを構築・運用・利用するための情報セキュリティ要件に関するガイドライン、クラウド技術の進展に関するデータセンターの利用指針、データセンターの安全・信頼性に係る情報開示認定制度等を検討する。2010 年度はガイドラインの策定を推進するための体制整備を行う。

イ）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）

今後の利用拡大が予想されるクラウドコンピューティングについて、中小企業等が活用する際にセキュリティ上考慮すべき事項について検討する。また、情報セキュリティ監査に反映する。さらに、国際標準化に向けた取組を行う。

ウ）クラウド・サービス・レベルのチェックリストの策定（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整備する。

エ）クラウドサービスを支える高信頼・省電力ネットワーク制御技術の研究開発（総務省）

2012 年度までに、ネットワーク全体の省電力化を図りつつ、高信頼で高品質なクラウドサービスを誰でも利用可能とするための先導的技術を確立することを目標として、クラウド間の連携等を実現する高信頼・省電力ネットワーク制御技術の研究開発を実施する。

・IPv6 対応に関する情報セキュリティ確保方策

IPv6 対応における情報セキュリティ上の課題に適切に対応するため、検証環境の活用等により、具体的な情報セキュリティ課題の抽出や人材育成等を実施し、円滑な移行を図る。

【具体的施策】

ア）IPv6 運用技術習得のためのテストベッドの整備（総務省）

2010 年度も引き続き、民間のネットワーク運用者等の運用技術の向上を図り、IPv6 に対応した人材を育成・確保するため、実ネットワークレベルの複雑さを有した実験用 IPv6 ネットワーク（テストベッド）を整備する。

イ）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。

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

情報家電、モバイル端末、電子タグ、センサー等あらゆるものがネットワークに繋がった場合の情報セキュリティの確保方策として、開発者に対する検証ツールや安全性評価体制の整備等の環境整備・技術課題の解決を図るとともに新たな利用指針等を検討する。

【具体的施策】

ア）情報家電、モバイル端末、電子タグ、センサーネットワークのセキュリティ確保方策の検討（内閣官房）

あらゆるものがネットワークに繋がった場合の情報セキュリティの確保方策として、開発者に対する検証ツールや安全性評価体制の整備を進める。2010 年度は、ユビキタス環境における情報セキュリティ上の技術課題を整理する。

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）【再掲：２(1) ③・マルウェア対策等の充実・強化等】

ウ）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、2010 年度には、昨年度に引き続き、セキュリティ評価・認証のための共同利用設備の整備、人財育成、技術開発、調査等を着実に実施する。

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・情報共有体制の強化、２(1)③・マルウェア対策等の充実・強化等】

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・情報共有体制の強化】

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・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】

・医療、教育分野等における情報セキュリティ確保方策

医療、教育分野等において、医療・教育機関、国民等が安全・安心に情報通信技術を活用するためのガイドラインの充実等情報セキュリティ対策の推進方策について検討する。

【具体的施策】

ア）医療分野・教育分野における ASP・SaaS の普及に向けた取組（総務省）

ASP[10]・SaaS[11]サービスを提供する事業者及び利用者等に活用される以下の資料を作成し、普及に努める

a）「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」に基づいて、ASP・SaaS 事業者が医療機関等に対してサービス提供を行う際に求められる合意事項等を整理した SLA[12]の参考例

b）ASP・SaaS 事業者が教育分野（校務分野）のサービスを展開する際に、遵守又は留意すべき事項について整理したガイドライン等

[10] Application Service Provider
[11] Software as a Service
[12] Service Level Agreement

・中小企業に対する情報セキュリティ対策支援

中小企業に対し、高度な情報セキュリティが確保された戦略的な情報通信技術投資を促進するための環境整備や、独立行政法人や関係機関等を活用し、情報セキュリティに係る情報提供、相談窓口の提供等の支援を行う。

【具体的施策】

ア）中小企業における高度な情報セキュリティが確保された情報システムの普及（総務省及び経済産業省）

a) 中小企業等基盤強化税制の普及・啓発を図ることにより、中小企業における高度な情報セキュリティが確保された情報システム投資を促進する。

b) 中小・小規模企業でも安価かつ容易に業務効率化及び経営改善を行える、インターネットを活用したソフトウェア提供サービス（SaaS）の基盤となるシステムや、その上で稼働するセキュリティ管理等のアプリケーションを普及する。

イ）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」や地域の中小企業等向けの「情報セキュリティセミナー」を開催し、当該セミナーにおいて情報セキュリティに関する知識等を習得させ、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。

ウ）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、開発の検討を行う。
2010 年度中に、IPA が中小企業を指導する立場にある者等、地域 NPO 等による相談対応等への支援、各主体間の連携方策、各主体に対する情報提供等に関する検討を行う。

・安全な電子商取引の推進

クレジットカード情報等の保護のため、国際標準を踏まえた情報セキュリティ対策を推進し、電子商取引を行うウェブサイトについて、情報セキュリティ基準の策定やその準拠を推進するとともに、新たな情報漏えい防止対策等を検討する。

【具体的施策】

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。

・知的財産保護の推進

企業等の知的財産を適切に保護するため、「知的財産推進計画 2010」（2010 年 5 月策定）に基づき、インターネット上の著作権侵害コンテンツ対策の推進、模倣品・海賊版拡散防止条約（ACTA）交渉の妥結を通じ、世界に知的財産保護の輪を広げる。

【具体的施策】

ア）アクセスコントロール回避規制の強化（文部科学省、経済産業省及び財務省）

製品開発や研究開発の萎縮を招かないよう適切な除外規定を整備しつつ、著作物を保護するアクセスコントロールの一定の回避行為に関する規制を導入するとともに、アクセスコントロール回避機器について、対象行為の拡大（製造及び回避サービスの提供）、対象機器の拡大（「のみ」要件の緩和）、刑事罰化及びこれらを踏まえた水際規制の導入によって規制を強化する。

このため、法技術的観点を踏まえた具体的な制度改革案を 2010 年度中にまとめる。

イ）プロバイダによる侵害対策措置の促進（総務省）

プロバイダと権利者が協働し、インターネット上の侵害コンテンツに対する新たな対策措置（例えば、警告メールの転送や技術的手段を用いた検知）を図る実効的な仕組みを、2010 年度中に構築する。あわせて、現行のプロバイダ責任制限法の検証を図った上で、実効性を担保するための制度改正の必要性について検討し、2010 年度中に結論を得る。さらに、それらの取組の進捗状況を踏まえて、必要な措置を講じる。

ウ）ACTA 交渉の妥結及び妥結後の加盟国拡大（外務省、総務省、法務省、財務省、文部科学省及び経済産業省）

2010年中に模倣品・海賊版拡散防止条約（ACTA）の交渉を妥結するとともに、締結後、主要国・地域への加盟国拡大や二国間協定を通じ、世界大に保護の輪を広げる。

④ 内閣官房情報セキュリティセンターの機能強化

・NISC の総合調整機能の強化

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。

【具体的施策】

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推進の中核としての機能を確保する。また、PDCA サイクルに基づく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、成長戦略策定会議、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

① 普及・啓発活動の充実・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を促すため、普及・啓発活動を強力に推進する。2010 年 2 月から、新たに２月を「情報セキュリティ月間」として定め、普及・啓発を強化したところであるが、更なる充実強化を図るため、「包括的な普及・啓発プログラム」を策定する。

【具体的施策】

ア）「情報セキュリティ月間」の実施（内閣官房及び関係府省庁）

国民一人一人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、毎年２月を「情報セキュリティ月間」とし、情報セキュリティに関する普及啓発活動を強化する。

イ）情報セキュリティに係る普及・啓発手法の検討（内閣官房）

情報セキュリティに対する国民の不安を解消するため、情報セキュリティに関する国際的な取組も踏まえつつ、官民が連携して、普及・啓発活動を推進するための基本方針及び具体策を検討し、2011 年３月までに「包括的な普及・啓発プログラム」を策定し、公表する。

ウ）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) 韓国インターネット振興院(KISA)との共同事業として、情報セキュリティ対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。

b) 2010 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、「情報化促進貢献表彰（情報セキュリティ促進部門)」を実施する。

c) 「情報通信における安心安全推進協議会」において、「情報通信の安心安全な利用のための標語」の募集を行い、最優秀作（総務大臣賞）を含む作品の選定・表彰を実施する。

d) 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、2010 年度に、「@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」等の取組を

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、積極的なIT利用者であるものの情報セキュリティへの関心が低い層に対する働きかけも重視することとする。

e) 2009年度に引き続き、主に保護者及び教職員を対象に、子どもたちのインターネットの安全・安心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。

エ）多国間会合を通じた情報セキュリティ政策に関する普及啓発等の推進（内閣官房及び関係府省庁）

APEC-TEL-WG、MERIDIAN（重要インフラに関する国際会合）、日・ASEAN情報セキュリティ政策会議等の多国間会合の場を通じ、各国の情報セキュリティに対する意識の底上げや人材開発における協調を図るため、各国と協力した国際的な意識向上に向けた取組を積極的に実施していく。

オ）プロバイダ責任制限法及び関係ガイドラインの周知の促進（総務省）

2010年度は、引き続き、業界団体によるWebサイト等を通じたプロバイダ責任制限法及び関係ガイドラインの周知を支援する。

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、2010年６月～８月及び10月～11月に総合通信局所において、電波利用機器販売店への周知・啓発を実施するとともに、「技術基準適合マーク」の確認についてインターネットバナー広告を実施する。

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) 情報セキュリティに関する主要なWebニュースサイト等の発信するRSSを収集・蓄積する「最新セキュリティ情報Navi(セキュリティ情報RSSポータル)」を引き続き提供し、Web等を通じた情報セキュリティ対策に関する情報収集を支援する。

c) 情報セキュリティ対策を推進するためのリスクや、リスクに対する人間の行動・投資等について調査及び社会科学的分析を行う。

d) 国内関連機関等との共催によるワークショップの開催等を通じ、コストや対策の成果、社会システムにおける対策行動の位置づけ等を明らかにする。

e) 2009 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 2010」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・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、２(1)③・情報家電、モバイル端末、電子タグ、センサーネットワークの情報セキュリティ確保方策】

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[13]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。

[13] レスポンスタイム、バッチ処理の制限時間、あるいはユーザビリティといった情報システム・ソフトウェアの性能や品質に関する要求事項を非機能要求という。

② 情報セキュリティ安心窓口（仮称）の検討

国民・利用者の情報セキュリティ水準を向上させるための活動を行う地域 NPO 法人等の支援を行うとともに、国民・利用者からの情報セキュリティに関する相談を受け付けるため、既存の枠組みも活用しつつ、「情報セキュリティ安心窓口（仮称）」の設置を検討する。

【具体的施策】

ア）「情報セキュリティ安心窓口（仮称）」の検討（内閣官房及び関係府省庁）

国民・利用者からの情報セキュリティに関する相談を受け付けるため、2010 年度中を目途に、既存の枠組みを活用しつつ、内閣官房において「情報セキュリティ安心窓口（仮称）」の在り方を検討する。

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）

IPA が開設しているコンピュータウイルス等に関連する相談窓口に偽ウイルス対策ソフト等のマルウェア全般の相談対応を追加し、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）

情報セキュリティに関する教材作成や講習会・認定試験の開催等を支援することにより、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

・プライバシー保護技術の適切な利用促進

大規模な個人情報漏えいを防止する観点から、アクセス権の設定、認証情報の管理、暗号化、匿名化等のプライバシー保護技術の適切な利用を促進する。

【具体的施策】

ア）プライバシー保護技術の適切な利用方法の検討（内閣官房）

大規模な個人情報漏えいを防止する観点から、アクセス権の設定、認証情報の管理、暗号化、匿名化等のプライバシー保護技術の適切な利用方法について検討する。

イ）情報漏えい対策への取組（経済産業省）【再掲：２(1)③・マルウェア対策等の充実・強化等】

・各事業分野ごとの個人情報保護に関するガイドラインの見直し

企業から個人情報等の情報の漏えいを防止する観点から、情報の適切な暗号化等を促進するため、漏えいした個人情報に適切な技術的安全管理措置が施されていた場合の手続の簡略化等、各事業分野の特性を踏まえつつ、事業者に暗号化等を行うインセンティブを付与するための見直しを行う。

【具体的施策】

ア）各事業分野における個人情報保護に関するガイドラインの見直しの検討（内閣官房及び関係府省庁）

2011 年６月を目途に、企業から個人情報等の情報の漏えいを防止する観点から、情報の適切な暗号化等を促進するため、漏えいした個人情報に適切な技術的安全管理措置が施されていた場合の手続の簡略化等、各事業分野の特性を踏まえつつ、事業者に対する暗号化等を行うインセンティブの在り方を検討する。

イ）安全管理措置に係る「電気通信事業における個人情報保護に関するガイドライン」の見直し（総務省）

モバイル PC 等の紛失等に際して、漏えい等が発生した個人情報に対し適切な技術的保護措置が講じられていた場合には、事業者に求められる手続（本人への通知、事実の公表、監督官庁への報告）の一部を緩和すること等をガイドラインに明記する。

・国際的なフレームワークへの対応

個人情報の国際的な流通が適切かつ安全な形で行われることを促進するため、OECD（The Organizations for Economic Cooperation and Development）をはじめとして、APEC（Asia-Pacific Economic Cooperation）、EU（European Union）等様々な場で進められている国際的な取組を踏まえ、プライバシー保護に関する越境執行協力等、国際的な協調を図っていくとともに、我が国の法制度についても国際的な理解を求め、データプライバシー保護に係る諸外国の制度と我が国の法制度との整合性に留意しつつ、我が国として必要な対応を検討する。

【具体的施策】

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）

2010 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。

・個人情報保護法の見直し

個人情報保護法について、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。

【具体的施策】

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、2010 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。

④ サイバー犯罪に対する態勢の強化

・ 犯罪取締りのための基盤整備の推進

サイバー犯罪の取締り体制の強化を図るとともに、デジタルフォレンジックを活用したサイバー犯罪の取締り、国際協調の推進等の基盤強化を推進する。

さらに、原因特定や犯行過程解明に不可欠な情報提供がなされ、被疑者の検挙や被害の拡大防止につなげられるよう、法執行機関と被害者等との間の良好な協力関係の構築を一層推進するなど、犯罪に強い社会構築のための官民連携に向けた取組を推進する。

【具体的施策】

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)・サイバー犯罪の取締り】

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)・サイバー犯罪の取締り】

カ）中央当局制度[14]を活用した国際捜査共助の迅速化（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・中及び日・香港間の刑事共助条約・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

[14] 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。

うことで共助の迅速化を図る。また、日・露及び日・EU 間においても、平成 21 年５月、同年 12 月にそれぞれ刑事共助条約・協定の署名が行われ、平成 22 年４月にそれぞれ我が国の国会の承認を得た。今後は、同条約・協定の発効を目指すとともに、更なる刑事共助条約の締結について検討していく。

・犯罪抑止のための広報啓発の推進

サイバー犯罪抑止を図るため、国民一人一人が自らサイバー犯罪から身を守るという意識を高めるための、情報セキュリティに関する講習等の啓発活動を強力に推進する。

【具体的施策】

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）

2009 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) サイバー犯罪被害防止のためのパンフレット等や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、これらのパンフレット等のほか、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脆弱性情報、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と育成方策を確立してサイバーボラ

ンティアの育成促進を図り、安全で安心なインターネット空間の醸成に向けた取組を推進する。

(3) 国際連携の強化

① 米国、ASEAN、欧州等との連携強化（二国間、ASEANとの関係強化）

日米サイバーセキュリティ会合や日・ASEAN情報セキュリティ政策会議等の開催を通じ、政策面における海外との連携を戦略的に強化するとともに、情報セキュリティ対策セミナーの開催等の海外CSIRT(コンピュータセキュリティ緊急対応チーム)の構築支援等、実務面におけるネットワークの構築を図る。

また、従来の取組に加え、インターネットが急速に普及している国々の状況も踏まえつつ、新たな二国間関係の構築等に努める。

【具体的施策】

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、2010年度中に、米国、ASEAN諸国等と二国間会合を開催して、個別分野における連携について協議するなど戦略的二国間連携の強化を図る。また、欧州諸国等との協力関係構築に向けた検討を開始する。

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ASEAN諸国との連携を強化する。

a) 第2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（2010、11年度）

b) 第3回日・ASEAN情報セキュリティ政策会議を我が国で開催（2010年度）

c) 日・ASEAN 政府ネットワークセキュリティワークショップをベトナム（第2回、2010年度）及び我が国で開催（第3回、2011年度）

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（2010年度）

e) ASEAN諸国との普及啓発イベントの共同開催（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（2010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（2010 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）

2010 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。

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。2010 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。2010 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。2010 年度においては、IWWN コミュニティとして、Cyber Storm III への参加が予定されており、この機会を利用して、海外 CSIRT メンバチームとの間の一層の連携の強化を図る。

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防御策を策定するため、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)③・マルウェア対策等の充実・強化等】

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

APEC、ARF、ITU、MERIDIAN、IWWN、FIRST(Forum for Incident Response and Security Teams)、APCERT(Asia Pacific Computer Emergency Response Teams)等、様々な分野の国際会議に積極的に参加し、外国機関等との情報共有体制を強化する。

【具体的施策】

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)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２回会合（2010 年 7 月にクアラルンプールで開催予定）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（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。

③ NISC の窓口機能の強化

NISC は、横断的な情報セキュリティ問題に関する国際ＰＯＣ(Point of Contact)として、各国の情報セキュリティに関するベストプラクティスの共有、各国の重要インフラの情報セキュリティ対策等を含む情報セキュリティ政策全般について、諸外国等の関係機関との連携を強化する。

【具体的施策】

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、2010 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

① 情報セキュリティ関連の研究開発の戦略的推進等

米国等の動向も踏まえ、情報セキュリティに係る研究開発を戦略的に推進するため、新たな情報セキュリティ研究開発戦略を策定する。

インターネットを始めとする情報通信技術を利用者が活用するにあたっての脆弱性の克服や、IPv6 や、クラウドコンピューティング、情報家電、携帯端末、センサーネットワーク等の情報通信技術の環境の変化に対応した情報セキュリティ技術の開発、高度化・多様化する攻撃等に対応できる情報セキュリティ技術（「グランドチャレンジ型」研究開発・技術開発）の実現・普及の実現を目指す。また、情報セキュリティ脅威の実態を踏まえた、システム設計管理対策の強化・普及を図る。

【具体的施策】

ア）新たな情報セキュリティ研究開発戦略の策定（内閣官房）

米国のサイバーセキュリティ強化法案等の動向を踏まえ、情報セキュリティに係る研究開発を戦略的に推進するため､2011 年 6 月を目処に新たな情報セキュリティ研究開発戦略を策定する。

イ）「グランドチャレンジ型」のテーマ及び推進の枠組み検討（内閣官房、内閣府、警察庁、総務省、文部科学省、経済産業省及び防衛省）

2009 年度に実施した「情報セキュリティ技術の研究開発における政府関与のあり方」の検討結果を踏まえ、総合科学技術会議と情報セキュリティ政策会議の連携の下、2010 年度は「グランドチャレンジ型」研究開発・技術開発を推進するための枠組み全体の設計、これを実現する上での技術的課題、制度的課題等の検討を行なう。また、これらの課題を解決するためにとり得る具体的な施策（技術的な手法を示すだけでなく、分析等に必要な情報を入手するための枠組み作りを含む。）の検討を行なう。

ウ）研究開発・技術開発の投資バランスの改善検討（内閣官房、内閣府、警察庁、総務省、文部科学省、経済産業省及び防衛省）

情報セキュリティの研究開発・技術開発について、それぞれの領域において過小投資、過大投資が発生しないようにするため、総合科学技術会議との連携の下、産官学を通じた我が国における情報セキュリティに関連する研究開発・技術開発の実施状況を調査し、2011 年２月を目処に官民での取組状況や技術の進展状況を整理する。

エ）研究開発プロジェクトの管理・評価における改善施策の検討（内閣官房、内閣府及び文部科学省）

情報セキュリティの研究開発の特徴である「Moving Target」に起因する非効率面を克服するため、研究段階で生じた新たな状況変化に応じて研究計画の変更を柔軟に行えるように制度の見直し作業を継続するとともに、総合科学技術会議との連携の下、イノベーション研究開発を活性化し、研究開発の成果の利活用を促進する目的において有効な施策について検討する。

オ）大規模仮想化サーバ環境における情報セキュリティ対策技術の研究開発（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、大規模仮想化サーバ環境を利用した社会経済基盤を安心・安全な状態に保つため、2012 年度迄にプライバシー保護型処理技術、セキュリティレベル可視化技術等新たな情報セキュリティ対策技術を開発する。初年度である 2010 年度は、各要素技術の基本設計と単体評価を行なうとともに、各要素技術間のインタフェースや総合実験モデルの検討を行なう。

カ）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、ネットワーク自身及びネットワーク上を流通する情報の安全性・信頼性を確保するための総合的な情報セキュリティを確保するための技術に関する研究開発を実施する。

2010 年度は、インシデント分析の広域化・高速化技術に関して協力団体へシステム展開し、実験環境を構築し、実証実験を実施する。また、総合的なセキュリティユーザサポートシステムの実験環境の構築を行う。

キ）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、2010 年度は評価手法の基礎検討及び評価システムの基本設計を行なう。

ク）小規模攻撃再現テストベッド及びマルウェア隔離解析テストベッド等の構築（総務省）

NICT において、サイバー攻撃の解明と対策技術の検証、データセットの生成を行うためのテストベッドを構築し、高度化・巧妙化が進むサイバー攻撃・マル

ウェアの解析能力・対策技術の高度化を推進するための基盤を構築する。

2010 年度は、昨年度に構築した小規模攻撃再現テストベッドのα版プロトタイプの試験を行なった上で、評価結果を踏まえてβ版プロトタイプの構築を行う。また、α版を用いた動作記録データセットを学術会議に提供する。

ケ）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うえで、対応策を検討する。

2010 年度は、昨年度までに開発した IPv6 検証環境(テストベッド)を用いて、ネットワーク上のセキュリティ脅威等を把握するために実証評価試験を実施する。

コ）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、ユーザからの要求に応じた最適な品質やセキュリティ等を確保できる新世代ネットワークの基盤技術の研究開発を推進する。2010 年度は、ダイナミックネットワークの要素技術の研究開発を進め、その成果についての最終評価を実施・公表する。さらに、複数方式のネットワークを同一インフラ上で提供可能とする仮想化ノードのプロトタイプの技術評価をテストベッド上で行う。

サ）量子情報通信ネットワーク技術の研究開発（総務省）

安心・安全で利便性の高い情報通信サービスの実現を目指し、極めて高い安全性が保証された量子暗号や、将来のどのような技術でも解読できない安全性（無条件安全性）を備えた量子情報通信ネットワークの実現に向けた研究開発を実施する。2010 年度は、量子鍵配送に必要な量子波長多重技術及び光子検出技術、量子雑音秘匿暗号の多値化技術等の研究開発を実施する。

シ）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。

2010 年度は、これまでの研究成果を踏まえ、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 ソフトウェアタグデータの加工・実装、可視化等のためのツール群の試作・改善・機能拡張及びツールの公開を行う。
② ソフトウェアタグの適用実験を実施する。
③ ソフトウェアタグ規格の改定や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。

ス）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ため、対症療法的ではなく根本的な問題解決を目指した新世代情報セキュリティ技術の研究開発を 2010 年度に、公募・実施する。

セ）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。

2010 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。

② 情報セキュリティ人材の育成

一般利用者の情報セキュリティ水準を底上げするため、利用者の身近で情報セキュリティ対策をサポートできる人材を育成する。

また、共通的な人材評価・育成ツールを活用して、産学連携による実践的な人材育成手法等に基づく高度な情報セキュリティ人材を育成するとともに、このような人材を育成するためのモデル的なキャリアパスを策定、可視化し、普及等を図る。

また、情報セキュリティ人材の中長期的な確保メカニズムの確立も視野に入れつつ、幅広い分野における情報セキュリティ人材育成に係る工程表を策定する。

【具体的施策】

ア）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。

イ）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、産業界出身教員等を対象とした教育プログラムの実証、産学マッチングによる実践的なインターンシップの実証等を推進するための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、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職種ごとのモデルキャリア開発計画を広報・普及する。また、新たにユーザー企業における情報システム部門人材のモデルキャリアパス開発計画を策定することによって、ユーザー企業におけるセキュリティ人材のキャリアパス形成を支援すると共に CIO 人材等へ向けて広報・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 の取り組み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。

ウ）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。

エ）先導的 IT スペシャリスト育成推進プログラム（文部科学省）

a) 大学院において、産学連携により、国民が安全・安心に IT を活用できる環境を構築するための高度セキュリティ人材育成プログラムを開発・実施する拠点形成を支援する。

b) 各拠点における多様な教育プログラムの開発・実施を通じて得られた成果について、より効果的・効率的な普及・展開を図るとともに教材等を更に洗練するための事業を支援する。

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）情報セキュリティ人材育成に係る工程表の策定の推進（内閣官房）

情報セキュリティ人材の育成・確保方策のあり方について、中長期的な視点から検討し、2011 年６月を目途に工程表として取りまとめを行う。

③ 情報セキュリティガバナンスの確立

事業継続計画（BCP）の策定、情報セキュリティ監査の実施や財務システム等の業務システムの入れ替え時における情報セキュリティ確保を図るため、普及・啓発活動を通じ、情報セキュリティガバナンスが経営課題として位置付けられ、経営者の意識改革が行われることを促すとともに、新たなリスクマネジメント等に関する手法の導入において情報セキュリティが明確に位置づけられるような方策を推進する。

【具体的施策】

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) 2010 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）」について、民間企業や政府機関における活用・普及を促進する。

d) 2010 年度は、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を収集・解析し、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 22 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。2010 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。2010 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

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

サイバー犯罪条約の早期締結に向けて必要な検討を進め、また、コンピュータウイルス関連の法改正等の法整備を推進するとともに、機微な情報へのアクセス権限を明確化するための方策や情報漏えい等を防止するための方策の検討等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。

【具体的施策】

ア）サイバー犯罪に適切に対処するための法整備等の推進（法務省）

サイバー犯罪に適切に対処すべく、サイバー犯罪条約を締結するための法整備等を推進する（「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」を第 163 回国会に提出し、継続審議となっていたが，平成 21 年 7 月の衆議院解散に伴って廃案となったことから，条約締結等のためにどのような法整備が必要かなどの観点から検討を進める。）。

イ）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）

機微な情報へのアクセス権限を明確化するための方策や情報漏えい等を防止するための方策等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検討を行う。

ウ）「データセンターの安全・信頼性に係る情報開示指針」の活用・普及（総務省）

「データセンターの安全・信頼性に係る情報開示指針(第１版)」(2009 年２月策定・公表）を踏まえ、情報開示認定制度の創設に向けた検討を行い、その普及・活用を図る。

エ）「ASP・SaaS の安全・信頼性に係る情報開示認定制度」の活用・普及（総務省）

ASP・SaaS を利用するに当たり、サービスの比較・評価・選択を容易にするため、「ASP・SaaS の安全・信頼性に関する情報開示指針」に基づき民間団体が運営する、ASP・SaaS 安全・信頼性に係る情報開示認定制度の普及・活用を図る。

オ）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)③・マルウェア対策等の充実・強化等】

カ）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)③・安全な電子商取引の推進】

② 各国の情報セキュリティ制度の比較検討

情報セキュリティに関する国際連携・協調を推進するため、各国間の法制度等の相違について分析し、課題の抽出と連携方策の検討を行う。

【具体的施策】

ア）各国のセキュリティ法制度の調査（内閣官房）

2010 年度中に、アジア諸国の法制度の調査に着手し、2011 年度中は、主要国の法制度の調査・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。