2010 年度の情報セキュリティ政策の評価等

2011 年７月８日

内閣官房情報セキュリティセンター（NISC）

目次

Ⅰ　はじめに

（１）本文書の位置付け等

本文書は、「国民を守る情報セキュリティ戦略」（以下「戦略」という。）及び 2010 年度の年度計画である「情報セキュリティ 2010」（以下「年度計画」という。）に基づき推進された情報セキュリティ政策の評価等について取りまとめたものである。

評価は、「情報セキュリティ政策の評価等の実施方針」（2011 年７月８日 内閣官房情報セキュリティセンター）に基づき、2010 年度に生じ、又は顕在化した環境の変化を整理した上で、年度計画において示される取組の推進状況を把握しつつ、情報セキュリティ政策が環境の変化に適合しているかどうか、また、種々の脅威に適切に対処することが可能となっているかどうかなどについて検証する形で実施した。

（２）情報セキュリティ政策に係る環境の変化

2010 年度に生じ、又は顕在化した環境の変化として、次のものが挙げられる。

①　大規模なサイバー攻撃事案等の脅威の増大

- DDoS[1]攻撃の脅威の現実化（2010 年９月、政府機関等に対する DDoS 攻撃が発生）
- いわゆる標的型メール攻撃の巧妙化、複数の既存攻撃を組み合わせて特定企業や個人を狙う APT[2]と呼ばれる新たな脅威の出現等脅威の高度化・複雑化
- 個人情報等の漏えい事案の発生

②　社会経済活動の情報通信技術への依存度の増大

- SNS[3]、スマートフォン等の急速な普及

③　新たな技術革新

- クラウドコンピューティング、端末のユビキタス化等の進展

④　グローバル化等

- いわゆるジャスミン革命の発生

⑤　東日本大震災の発生

1　Distributed Denial of Service：サービス不能攻撃。複数のネットワークに分散する大量のコンピュータから、一斉に特定のサーバに通信を行い、通信路を圧迫させてサービスを停止させてしまう攻撃のこと。

2　Advanced Persistent Threats：脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャルエンジニアリングにより特定企業や個人をねらい、対応が難しく執拗な攻撃のこと。

3　Social Networking Service：利用者が互いに幅広いコミュニケーションを取り合うことを目的としたコミュニティ型ウェブサイトのこと。

II　全体の評価等

（1）総評

すべての国民が情報通信技術を安心して利用できる環境の実現に向けて、各政策領域において、所要の取組が推進されているが、クラウドコンピューティング、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や、「Stuxnet」に代表される新たな攻撃や昨年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高度化・複雑化等、情報セキュリティをめぐる環境の変化は著しく、すべての政策領域においてこれらの変化に万全の対応が進められてきているとは言い難い状況にある。

所要の取組について概観すれば、大規模サイバー攻撃事態への対処態勢の整備等や国民生活を守る情報セキュリティ基盤の強化に関する政策領域については、既知の脅威への対応力を高めるための取組は進んでいるが、高度化・複雑化する脅威への対応には課題が残っている。国民・利用者保護の強化に関する政策領域については、各種の普及・啓発活動等を着実に実施してきているものの、未だ有意な成果が上がっていると認められる水準には至っていない。国際連携の強化、技術戦略の推進及び情報セキュリティに関する制度整備等に関する政策領域については、研究開発の推進、情報セキュリティ人材の育成等に関する取組が進められているが、まだ緒に就いたばかりの検討段階の取組も多い。

（2）次年度に向けた課題

本年３月 11 日に発生した東日本大震災は、これまでに経験したことのない規模の大災害であり、情報通信インフラも壊滅的な被害を受け、情報が円滑に流通しないことにより社会の様々な活動が停滞するなどの影響が生じたところであるが、ほとんどの政策領域においては、今回のような大災害の発生を念頭に置いた取組は進められてきていなかった。情報通信技術を安心して利用できる環境を構築するためには、従来の情報セキュリティ政策を推進するとともに、このような大災害の発生を念頭に置き、安全性・信頼性を確保するための情報セキュリティ政策を立案し、推進することが必要不可欠である。

また、詳細は「Ⅲ　各領域における評価等」の記載に譲るが、各政策領域において、新たに対応が必要な事項、改善が必要な事項等が認められるところ、それらの事項について、新たな取組を推進する、既存の取組の推進方法を見直すことなどにより、より効果的な政策を推進する必要がある。

III　各領域における評価等

１　大規模サイバー攻撃事態への対処態勢の整備等

【総評】

2010 年９月の我が国政府機関に対するサイバー攻撃事案の発生に加え、諸外国におけるサイバー攻撃事案の高度化・複雑化等、サイバー攻撃に係る脅威が増大するなか、2011 年３月、新たに、内閣官房及び各府省庁が相互に連携し、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を実施するなど、大規模サイバー攻撃事態への対処態勢の整備は緒に就いたと言える。また、2010 年 12 月に情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議において、平素からの情報収集の強化と情報共有の徹底について申合せを行ったほか、GSOC[4]等を通じたサイバー攻撃等に関する傾向や情勢についての分析及び情報提供を行うなど、対処に資する平素からの情報収集・共有体制の強化が図られた。

【課題】

- 刻々と高度化・複雑化するサイバー攻撃手法等に対処するための、継続的な手法の分析、対処訓練の実施及び諸外国等との連携を含めた対処態勢等の整備の推進

２　新たな環境変化に対応した情報セキュリティ基盤の強化

（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

【総評】

政府機関における対策実施状況報告[5]、重点検査[6]の結果によれば、引き続き一部対策が不十分な部分や課題は残っているものの、各府省庁の情報セキュリティ対策は一定の水準を維持している。また、各府省庁独自の取組も多数報告されるなど、多面的な対策が講じられており、情報セキュリティへの対応力は着実に向上していると評価できる。

一方、種々の環境変化、とりわけ、これまでに経験したことのない大災害である東日本大震災が発生しており、的確な対応が求められている。

詳細については、「政府機関における情報セキュリティに係る年次報告（平成 22 年度）」を参照。

4　Government Security Operation Coordination team：政府横断的な情報収集機能、攻撃等の分析・解析機能等の事案対策促進機能。

5　「政府機関の情報セキュリティ対策のための統一基準（第４版）（平成 21 年度修正）」（以下、「政府機関統一基準」という。）に基づく各府省庁の情報セキュリティ対策の実施状況を把握するための評価。

6　政府機関統一基準に基づく重要なシステム（端末、ウェブサーバ及び電子メールサーバ）について具体的な情報セキュリティ対策状況の把握及び改善促進のための評価。

【課題】

- 業務継続能力の強化、標的型メール攻撃（スピアメール）への対応等上記環境変化を踏まえた対応及び「政府機関における情報セキュリティに係る年次報告（平成 22 年度）」の評価結果等を踏まえた課題への対応

② 重要インフラの基盤強化

【総評】

重要インフラサービスの維持、IT 障害発生時の迅速な復旧等の確保に向け、「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」に基づき諸施策を着実に推進し、2010 年度の目標に沿った一定の成果をあげている。

一方、いわゆる「Stuxnet」と呼ばれる制御システムへの攻撃の顕在化や東日本大震災による大規模な被害の発生といった社会・環境の変化が生じており、これに対しては、これまで整備・強化を図ってきた情報共有体制等に一定の効果がみられたところである。

【課題】

- 上記のような高度化・複雑化するサイバー攻撃や大災害を想定したリスクに対応するための、社会的・技術的な環境変化を踏まえた、重要インフラの一層の基盤強化

③ その他の基盤強化

【総評】

クラウドコンピューティング技術の発達、IPv6 への移行等といった課題について、それらに関する情報セキュリティの確保のための検討が進んでおり、また、それらの技術を活用するに当たって必要となる情報セキュリティ対策に関する企業等の関心は高まっている。一方、コンピュータウイルス等の攻撃手法の巧妙化等により、依然として個人情報が漏えいするといった事案等の発生が続いている。これらの情報セキュリティ上の脅威への対策や、東日本大震災のような大災害が発生した際の対応が求められる状況にある。

【課題】

- 上記事案等に的確に対処するため、クラウドコンピューティングやスマートフォン及び IPv6 などに対応した情報セキュリティ政策の推進、企業等における情報セキュリティ対策の促進等及び大災害を想定した取組の推進

（２）国民・利用者保護の強化

①　普及・啓発活動の充実・強化

【総評】

「情報セキュリティ月間」（2011 年２月）の実施、各種メディア等を通じた普及・啓発活動や、情報セキュリティに関する相談対応力の強化に向けた検討が着実に継続されている一方、各種の脅威が増大する中、「セキュリティ脅威が難解で具体的に理解できない」、「どこまでセキュリティ対策を行えばよいか不明」等をインターネット利用上の不安と感じる者は依然として多く、また、情報セキュリティに関する相談の件数も一定水準にとどまっている。

【課題】

- 上記の状況に対応するため、「情報セキュリティ普及・啓発プログラム」に基づく、取組の着実な推進

②　個人情報保護の推進

【総評】

個人情報漏えいを防止する観点から、暗号化や匿名化等のプライバシー保護技術の適切な利用の促進に資するガイドラインの見直しや、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に、国際的なフレームワークへの対応が進められているが、個人情報が漏えいする事案の発生は依然として続いている。

【課題】

- 上記事案の発生を念頭に置いた取組の継続的な推進

③　サイバー犯罪に対する態勢の強化

【総評】

警察職員に対する教育訓練や資機材の整備等が着実に実施され、サイバー犯罪の検挙件数は増加している。一方、サイバー犯罪の被害防止に向けた広報啓発活動等は着実に推進されているものの、サイバー犯罪に関する相談件数は依然として高い水準にある。

【課題】

- 従前の取組の継続・強化のほか、巧妙化するサイバー空間での犯罪や違法行為に効果的に対応するための取組の検討等

（３）国際連携の強化

【総評】

各国政府機関等を狙ったサイバー攻撃の発生等国境を越えた情報セキュリティ上の課題が顕在化していることから、国際連携・協調を強化すべく、米国、ASEAN[7]等との間で協議を実施するとともに、APEC[8]、ARF[9]、MERIDIAN[10]、OECD[11]、FIRST[12]等国際会合を活用し、情報共有体制等を強化しているが、国際的なコンセンサスを得る状況には至っていない。

【課題】

- 継続的に連携の強化が推進されている米国、ASEAN に加え、ヨーロッパ諸国等との二国間連携や多国間連携の強化

（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

【総評】

情報セキュリティの研究開発に関する個別プロジェクトについては着実に推進されているが、全体の研究開発予算は減少傾向にあり、必ずしも十分な成果があげられているとは言い難い状況にある。

【課題】

- 上記の状況に対応するため、「情報セキュリティ研究開発戦略」について、企業・教育関係者（主に研究者）との相互理解を深めること及び重要テーマのロードマップの詳細化

---

7 Association of South-East Asian Nations：東南アジア諸国連合。
8 Asia-Pacific Economic Cooperation：アジア太平洋経済協力。
9 ASEAN Regional Forum：ASEAN 地域フォーラム。
10 重要情報インフラに関する国際会合。
11 The Organizations for Economic Cooperation and Development：経済協力開発機構。
12 Forum for Incident Response and Security Teams：各国の CSIRT（Computer Security Incident Response Team：コンピュータセキュリティに関する事案が発生した際に対応を行う組織）同士の情報交換、事案対応の協力関係構築等を目的とした国際フォーラム。

② 情報セキュリティ人材の育成

【総評】

先導的 IT スペシャリスト育成プログラムの普及等の取組が着実に進められており、また、情報セキュリティスペシャリスト試験の合格者数や民間資格の取得者数は増加し、専門家のスキル習得へ向けた動きは活発ではあるが、人材育成が十分成功しているとは言い難い状況にある。

【課題】

- 上記の状況に対応するため、「情報セキュリティ人材育成プログラム」に基づく、取組の着実な推進

（5）情報セキュリティに関する制度整備

【総評】

「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」が第 177 回国会で成立したほか、各国の法制等の相違及び連携方策の検討が進められるなど、取組は進められているが、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ための制度や国際連携の在り方についてさらなる検討が必要である。

【課題】

- 上記法律の円滑な施行及び各国において生じた新たな環境変化に対応した検討の継続的な推進

別添１　「情報セキュリティ2010」に盛り込まれた施策の実施状況

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における政府の初動対処態勢の整備

該当項目	施策名	担当省庁	進捗状況
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	・大規模サイバー攻撃事態等が発生した際に、「緊急事態に対する政府の初動対処体制について（平成15年11月21日）」等に基づく迅速かつ適切な初動対処を取るための体制を整備するため、内閣官房及び各府省庁が相互に連携し、初動対処訓練を実施（2011年３月９日）したほか、その結果を踏まえ、対処のあり方に関する検討を行った。
イ）	サイバーテロ対策に係る体制等の強化	警察庁	・サイバーテロ対策に従事する警察職員を対象に、サイバー攻撃に関する知識・技能等の修得を行うための部内外における各種研修を実施。

・官民連携の推進

該当項目	施策名	担当省庁	進捗状況
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	・都道府県警察において、重要インフラ事業者等への個別訪問、サイバーテロ対策セミナー、サイバーテロ対策協議会、重要インフラ事業者等との共同訓練等を通じ、官民の連携を強化。
イ）	サイバー攻撃（インシデント）対応調整支援	経済産業省	・2010年度においては、2,875件のインシデントについて、被害の発生、拡大抑止のための関係者間の調整活動を実施した。そのうち、重要インフラ事業者を主な対象としたインシデントに関する対応支援は、39件であった。

・サイバー攻撃に対する防衛分野での体制の強化

該当項目	施策名	担当省庁	進捗状況
ア）	サイバー企画調整官（仮称）の新設	防衛省	・防衛省統合幕僚監部にサイバー企画調整官を配置するために必要な規則等の整備を行い、2010年度末にサイバー企画調整官を配置した。
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・対処能力向上のために研究試作を行っていたネットワークセキュリティ分析装置の設計・製造が終了し、2010年度中に納入された。また、サイバー攻撃を検知するための基礎的な研究及びマルウェア（ウイルス等の悪意を持ったプログラム）の挙動解析の研究を2009年度に引き続き実施した。
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の調査として、サイバー攻撃の最新技術動向等について調査を実施し、サイバー攻撃対処要員の育成手法の資とする内容を含む報告書を取りまとめた（2011年３月までに完了）。

・サイバー犯罪の取締り

該当項目	施策名	担当省庁	進捗状況
ア）	デジタルフォレンジックに係る取組の推進	警察庁	・サイバー犯罪捜査に従事する警察職員に対し、電磁的記録の解析等に係る研修を実施。 ・デジタルフォレンジック用資機材の増強。 ・2010年12月、関係機関が参加するデジタルフォレンジック連絡会を開催。 ・電子機器等の製造業者を始めとする企業との技術協力を推進。

該当項目	施策名	担当省庁	進捗状況
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	・2010年４月及び10月並びに2011年３月、G8ローマ・リヨン・グループ ハイテク犯罪サブグループ会合に出席。情報通信技術を利用した犯罪に対処するための取組を日本主導により推進。 ・2010年６月、サイバー犯罪条約委員会会合に出席。 ・2010年９月、サイバー犯罪技術情報ネットワークシステム（CTINS）に参加する国・地域のサイバー犯罪の捜査等に当たる技術者等を集めたアジア大洋州地域サイバー犯罪捜査技術会議を開催。 ・2010年11月、ICPOアジア南太平洋IT犯罪作業部会会合に出席。 ・外国が関係するサイバー犯罪捜査に関し、ICPO、刑事共助条約等の国際捜査共助の枠組みを活用し、外国捜査機関等への捜査共助要請等を実施。 ・サイバー犯罪の取締りに関する技術情報を共有し、アジア大洋州地域の治安機関の相互の技術水準の向上を図ることを目的として、CTINSを運用しており、2011年３月現在、14の国・地域が参加。

・サイバー攻撃への対処に係る国際連携の強化

該当項目	施策名	担当省庁	進捗状況
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	・NATOサイバー防衛センター（CCDCOE）主催国際会議（2010年６月エストニア）等における情報交換を通じ、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・分析を実施した。
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	・FIRST年次会合（2010年６月米国）に参加するなど国際連携枠組みを通じて、諸外国との連携強化を図った。
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	・警察庁において、諸外国関係機関との情報交換を行うなど、サイバー攻撃の主体・方法等に関する情報収集・分析を継続的に実施している。 ・公安調査庁において､諸外国関係機関との情報交換を行うなどして、サイバー攻撃の主体・方法等に関する情報収集・分析を継続的に実施している。

1　大規模サイバー攻撃事態への対処態勢の整備等

（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

該当項目	施策名	担当省庁	進捗状況
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	・2010年12月27日の情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議において、平素からの情報収集の強化と情報共有の徹底について申合せを行い、当該申合せに基づいた情報の集約・共有を実施。
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	・内閣官房において、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提供を実施。
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」に基づく情報共有体制、情報共有体制に基づいた、重要インフラ所管省庁、関係機関等との情報連絡、情報提供を着実に推進した。
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	・警察庁において、サイバー攻撃手法に関する知識・技能の修得を目的とした民間委託研修を実施するなど、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の整備を進めた。 ・公安調査庁において、公安調査官を対象に各種研修を実施するなど、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の整備を進めた。
オ）	サイバーテロ対策に係る体制等の強化	警察庁	再掲

・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

該当項目	施策名	担当省庁	進捗状況
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	・日米サイバーセキュリティ会合（2010年11月米国）を開催するなど米国などとの二国間会合を実施して情報交換を行い、連携体制の強化を図った。
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

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

該当項目	施策名	担当省庁	進捗状況
ア）ａ）	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	・内閣官房においては、2010年12月に情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議を開催。 ・各府省庁においては、上記合同会議に参画し、それぞれの最高情報セキュリティ責任者が情報セキュリティ報告書を策定することを再確認。
ア）ｂ）	情報セキュリティガバナンスの高度化に向けた取組		・内閣官房においては、2010年12月開催の情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議において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、2011年１月に第１回会合を開催。 ・各府省庁においては、上記第１回会合に参加。
イ）ａ）	「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	・各府省庁において、平成22年度情報セキュリティ報告書を作成。
イ）ｂ）	「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		・内閣官房においては、2011年４月開催の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、全ての府省庁の情報セキュリティ報告書について、比較・評価等を実施するとともに、優れた取組については、推奨事例候補として選出することにより、各府省庁に対して知見の共有やフィードバックを図った。 ・各府省庁においては、情報セキュリティ対策推進会議の場において報告した。

・政府横断的な情報収集・分析システム（GSOC）の充実・強化

該当項目	施策名	担当省庁	進捗状況
ア）ａ）	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	・内閣官房において、政府機関に対するサイバー攻撃等に関する情報収集の強化のため、引き続き、関係機関との連携強化を進めるとともに、海外政府機関との意見交換を実施。また、分析・解析能力の強化や分析結果等の情報共有を進める取組を実施。
ア）ｂ）	政府横断的な情報収集・分析システム（GSOC）の充実・強化		・内閣官房において、全府省庁の協力を得て、2010年12月に緊急時の連絡体制の確認訓練を実施。

・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

該当項目	施策名	担当省庁	進捗状況
ア）ａ）	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	・各府省庁において、策定したサーバ集約化計画に基づき、情報システムのスリム化や運用効率化を推進しているところ。
ア）ｂ）	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		・内閣官房において、重点検査の実施により各府省庁における公開ウェブサーバ及び電子メールサーバの台数を把握。その結果について「政府機関における情報セキュリティに係る年次報告」に記載し、第26回情報セキュリティ政策会議にて報告。
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	・内閣官房において、検査を希望する府省庁（関係府省庁）の公開ウェブサーバについて、主なものをサンプル抽出し脆弱性検査を実施。検査結果について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、各府省庁で情報を共有。
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	・内閣官房及び総務省において、各府省情報化統括責任者（CIO）補佐官等連絡会議第４ワーキンググループ（情報セキュリティ）等の場において情報セキュリティ施策の意見交換を実施し、その後、当該施策を全府省庁が参加する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報告するなどして連携を強化。

該当項目	施策名	担当省庁	進捗状況
エ）ａ）	業務継続計画の策定の推進	内閣官房及び全府省庁	・各府省庁において、保有する情報システムの災害・障害時対応の必要性・優先度について検討を行い、必要に応じて業務継続計画の策定を進めているところ。
エ）ｂ）	業務継続計画の策定の推進		・内閣官房において、各府省庁における計画策定を支援すべく、「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」を作成・配付済み。
オ）ａ）	オンライン手続におけるリスク評価及び電子署名・認証ガイドラインの推進	内閣官房及び全府省庁	・内閣官房において、2010年８月開催の各府省情報化統括責任者（CIO）連絡会議第41回会合において、「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」を決定。
オ）ｂ）	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		・全府省庁において、「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」に基づく総合的な妥当性の評価等を実施しようとしたが、その評価の場である情報セキュリティ対策推進会議等の開催が時期を逸したために未実施。
カ）ａ）	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	・内閣官房において、対策実施状況報告に係る調査項目の集約、フェーズごとの整理等を実施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し、各府省庁への提示を実施済み。
カ）ｂ）	政府全体でのPDCAサイクルの定着と浸透		・各府省庁においては、対策実施状況報告を着実に実施。 ・内閣官房において、平成22年度の対策実施状況報告の取りまとめを実施し、第26回情報セキュリティ政策会議に報告するとともに、公表。
キ）	政府全体での情報共有の強化	内閣官房及び全府省庁	・内閣官房において、旧型ウェブブラウザから新型ウェブブラウザへの移行等の共通的な課題について各府省庁の状況調査を実施し、その調査結果や技術情報について共有を実施。また、各府省庁が参加する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、各府省庁における対応策等の検討・共有を図った。 ・内閣官房において、政府機関における情報セキュリティ関係職員を対象とする勉強会を新たに立ち上げ、2010年度末までに６回開催。各府省庁が参加し、関係職員の知見の向上を図った。
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	・2010年4月に開催された第７回カウンターインテリジェンス推進会議において、特別管理秘密を取り扱う情報システムに係る情報セキュリティ対策の実施状況を重層的にチェックする仕組みを構築する方向で検討することを決定し、検討を実施しているところ。
ケ）ａ）	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	・内閣官房においては、総務省が開催する情報システム統一研修につき、各コースに関連する情報セキュリティに係る事項を整理。その結果に基づいて既存の教材を見直し情報セキュリティに係る内容を充実。
ケ）ｂ）	政府職員に対する教育・意識啓発の推進		・人事院においては、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追加。 ・内閣官房においては、上記研修向けに、教育教材を提供。
ケ）ｃ）	政府職員に対する教育・意識啓発の推進		・内閣官房において、情報セキュリティ対策上の役割に応じた教育教材の雛型を作成・配付済み。
ケ）ｄ）	政府職員に対する教育・意識啓発の推進		・各府省庁において、電子政府利用促進週間、情報セキュリティ月間等の機会をとらえた意識啓発を実施。
コ）ａ）	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	・内閣官房においては、各府省庁の保有するドメインについてDNSサーバにおけるSPFレコードの付与を呼びかけ、推進。 ・各府省庁においては、本府省庁ドメインについてDNSサーバにおけるSPFレコードの付与を実施済み。
コ）ｂ）	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		・総務省において、迷惑メール対策推進協議会と連携し、「なりすましメール撲滅プログラム」及び「送信ドメイン認証マニュアル」を作成し送信ドメイン認証技術の理解が円滑に進むよう努めた。また、自治体や業界団体等にむけた説明会を８回開催し、送信ドメイン認証技術の一層の普及促進に努めた。

該当項目	施策名	担当省庁	進捗状況
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	・内閣官房においては、各府省庁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が政府ドメイン名ではないことを発見した場合に、当該ドメインを保有する府省庁に対して改善を要求。 ・総務省においては、2009年３月に政府ドメイン名の利用状況調査を実施しており、そのフォローアップの実施を準備。国の政府ドメイン利用の取組についても紹介することについても検討。

・政府機関における安全な暗号利用の推進

該当項目	施策名	担当省庁	進捗状況
ア）ａ）	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	・総務省及び経済産業省において、電子政府推奨暗号の監視、当該暗号の安全性及び信頼性確保のための調査等を実施。平成23年３月に平成22年度の検討結果を取りまとめた。
ア）ｂ）	政府機関における安全な暗号利用の推進		・総務省及び経済産業省において、「電子政府推奨暗号リスト」の改訂に向け、2009年度応募があった暗号アルゴリズムの安全性評価を行った。応募された６つの暗号方式のうち、４方式を、現在の電子政府推奨暗号リストに掲載されている暗号方式とともに、来年度以降詳細に評価することとなった。
ア）ｃ）	政府機関における安全な暗号利用の推進		・内閣官房においては、各府省庁における緊急対応計画の策定の状況把握を行うとともに、暗号技術検討会における議論を踏まえ、緊急避難的な対応について検討を進めているところ。 ・総務省及び各府省庁においては、それぞれが保有する情報システムを対象に、緊急対応計画を策定。
ア）ｄ）	政府機関における安全な暗号利用の推進		・内閣官房において、新たな暗号アルゴリズム切替え開始時期までに、各情報システムを同移行指針の規定する要件に適合させるよう促しているところ。
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	・各府省庁においては、2010年度も引き続き暗号モジュール試験及び認証制度に基づく認証を推進するとともに、必要に応じて認証を取得している製品の活用を実施、又は検討しているところ。

・クラウドコンピューティング技術における情報セキュリティの確保等

該当項目	施策名	担当省庁	進捗状況
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	・総務省において、2011年４月からの意見招請を目指して、「政府共通プラットフォーム」の要件定義書（案）を作成。その際に、内閣官房においては、これまで蓄積した情報セキュリティ確保方策に係る専門的知見をもとに、総務省への情報提供等の必要な調整・支援を行った。

・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

該当項目	施策名	担当省庁	進捗状況
ア）	政府機関統一基準の見直しの実施	内閣官房	・内閣官房において、昨今の情報セキュリティに係る問題意識や技術的・環境的な変化に対応するため、既存の政府機関統一基準の抜本的な見直しを行い、「政府機関の情報セキュリティ対策のための統一規範」を新たに制定するとともに、これまでの政府機関統一基準を「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」（基本的基準）と「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」（技術的基準）に分離し、パブリックコメントを実施。この新たな統一基準群については、第25回情報セキュリティ政策会議にて決定。

該当項目	施策名	担当省庁	進捗状況
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	・情報セキュリティに関する優れた我が国国内の技術的・専門的な知識や経験を活用するため、2010年9月に、総務省の所管する（独）情報通信研究機構（NICT）並びに経済産業省の所管する（独）産業技術総合研究所（AIST）及び（独）情報処理推進機構（IPA）のそれぞれと内閣官房との間で協力覚書を締結。また、2011年２月には、内閣官房において、情報セキュリティ月間キックオフ・シンポジウムを開催、上記独立行政法人によるパネルディスカッションを実施。
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	・内閣官房において、政府機関統一基準の改定に当たり、内閣府、総務省及び関係府省庁と協力の上、情報セキュリティと関連が深いと考えられる法令等との整合性の確保が図られるよう、各制度との整理・調整を実施。
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	・内閣官房においては、統一基準の改定に際して、ITセキュリティ評価及び認証制度の活用を基本遵守事項に変更。 ・各府省庁においては、2010年度も引き続きITセキュリティ評価及び認証制度により認証された製品等の優先的な取り扱いを実施、又は検討しているところ。
オ）ａ）	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	・経済産業省においては、IPAに設置された「情報セキュリティ関連制度等普及委員会」での議論を受け、「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」（案）を取りまとめ、パブリックコメントを実施。第25回情報セキュリティ政策会議の開催と同日付で、経済産業省において策定。
オ）ｂ）	情報セキュリティに配慮したシステム選定・調達の支援		・経済産業省において、「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」（案）「重要なセキュリティ要件」がある場合等の明確化を実施。内閣官房においては、前記リストを踏まえ、統一基準の改定に際して、ITセキュリティ評価及び認証制度の活用を基本遵守事項に変更。
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
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、経済産業省及び全府省庁	再掲

・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

該当項目	施策名	担当省庁	進捗状況
ア）	予算面での取組	全府省庁	・内閣官房においては、必要なセキュリティ対策を確実に実施するに当たり、システムの特性に応じて過不足とならないよう「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」（詳細はウ）を参照）を策定、各府省庁における情報システム調達に際して、必要な情報セキュリティ要件を可能な限り要求仕様書に記載するよう推進。 ・各府省庁においては、当該マニュアルを策定する検討会において問題意識を共有し、情報セキュリティ対策を勘案した適切な契約を交わすなどの取組を進めているところ。
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	・内閣官房においては、統一基準の改定に際して、「外部委託における情報セキュリティ対策実施規程」（政府機関統一基準適用個別マニュアル）の見直しを実施し、第25回情報セキュリティ政策会議の開催と同日付で公表。 ・ 各府省庁においては、政府機関統一基準及びマニュアル等を踏まえ、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ているところ。

該当項目	施策名	担当省庁	進捗状況
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	・内閣官房において、電子政府の情報セキュリティを企画・設計段階から確保するための方策の強化について検討するため、主要ベンダー等を構成員とする検討会を開催、総務省及び各府省庁は適宜参加し、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及び組み込むべき情報セキュリティ要件の取りまとめとして、「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」を策定。
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
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	・ガイドラインの適合度合いを確認するためツールを利用して、重要インフラシステム事業者に対してアンケート調査を実施することにより、活用・普及を行うと共に、ガイドラインの改善案について取りまとめた。
カ） a）	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	・情報システム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した。
カ） b）	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		・政府調達における、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に関して、諸外国の実態も踏まえた検討を行い、その成果を政府統一基準の改訂にあわせて策定した。なお、成果は、政府統一基準の改訂に反映され、具体的な活用促進策が政府統一管理基準に盛り込まれた。
カ） c）	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		・「暗号モジュール試験及び認証制度」の中で、認証実績のある暗号製品を増加させるため、国内における認証実績の無い製品分野であるハードウェアセキュリティモジュール（HSM）製品に関して、ベンダーの負担になる試験費用を無償とした試験の公募を実施した。
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
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

・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

該当項目	施策名	担当省庁	進捗状況
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	・内閣官房において、社会保障・税に関わる番号制度及び国民ID制度の実現のための検討会等を設置し、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を含めて検討を行っているところ。

・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

該当項目	施策名	担当省庁	進捗状況
ア） a）	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	・４団体にICT部門におけるBCP策定支援アドバイザー、16団体に内部監査アドバイザーをそれぞれ派遣した。 ・ICT部門におけるBCP策定支援セミナーを東京で開催した（90名参加）。 ・内部監査の手順等を実践的に学ぶためのセミナーを東京及び大阪で開催した（計82名参加）。 ・「地方公共団体における情報セキュリティポリシーに関するガイドライン」及び「地方公共団体における情報セキュリティ監査に関するガイドライン」の見直し作業を行い、2010年11月に各ガイドラインの改定を行い、地方公共団体に対し周知した。
ア） b）	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		・LGWAN内のポータルサイトにおいて、情報セキュリティベストプラクティスの紹介、情報セキュリティ技術に関する解説等の資料提供を行った。 ・LGWANポータルサイトの利用を促進するため、情報セキュリティ事故事例情報を含め、コンテンツの充実を図った。

該当項目	施策名	担当省庁	進捗状況
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	・eラーニングによる情報セキュリティ研修の受講対象者に教育委員会を含めて実施。
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	・eラーニングによる情報セキュリティ研修を2010年５月から同年12月まで実施し、延べ73,313人が受講。
エ）ａ）	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	・内閣官房において、独立行政法人等における情報セキュリティポリシーの整備状況調査を所管府省庁に依頼し、継続して2010年度末にも実施。第26回情報セキュリティ政策会議にて結果を報告。 ・NISCホームページに「独立行政法人等における情報セキュリティ対策」を掲載しており、独立行政法人等向けのポリシー雛形を、統一基準の改訂に応じて継続的に提供。
エ）ｂ）	独立行政法人等における情報セキュリティ対策の推進		・各府省庁において、所管する独立行政法人等に対して情報セキュリティ対策に係る事項の中期目標明記に向けた取組を実施しているところ。内閣官房は、継続して2010年度末にも調査を実施しており、第26回情報セキュリティ政策会議にて結果を報告。
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	・内閣官房において、各府省庁と所管する独立行政法人等との間で、緊急時を含め実効性のある連絡体制を整備し、実効性の確認を行うよう依頼。継続して2010年度末にも調査を実施しており、第26回情報セキュリティ政策会議にて結果を報告。
カ）	行政機関以外の国の機関との連携	内閣官房	・内閣官房において、情報セキュリティ対策推進会議及び最高情報セキュリティアドバイザー等連絡会議等を開催し、行政機関以外の国の機関をオブザーバーとして登録することで、情報セキュリティ上の共通的な課題について情報交換や連携を実施。

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

② 重要インフラの基盤強化

・情報共有体制の強化

該当項目	施策名	担当省庁	進捗状況
ア）ａ）	共有すべき情報の整理	内閣官房	・情報の提供者、情報共有のタイミング、共有の方法、利用する場面等について、情報の性質、情報提供者の意向等に応じて共有すべき情報についてマトリクスに整理した。
ア）ｂ）	共有すべき情報の整理		・既に構築されている実施細目に基づく情報共有の範囲を超える情報共有について、情報提供元・利用者となる各セプターへのアンケートにより、情報連絡に当たっての制約、有用な情報とは何か等について調査、整理した。
イ）ａ）	「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	・実施細目に基づき、重要インフラ所管省庁を通じ情報連絡を受け、内容に応じて、関係省庁等への情報提供を着実に行った（情報連絡：174件、情報提供49件）。
イ）ｂ）	「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		・実施細目に基づく情報共有、実際に発生したサイバー攻撃事案への対処等における情報共有が適切に機能していることが確認されたこと等を踏まえ、実施細目の検証を行い引き続き現行のもので情報共有を図ることとした。
ウ）ａ）	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	・各分野において、重要インフラ所管省庁から各セプターへの情報共有ルール及び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について情報共有の訓練も活用し、実施細目との整合性の確認等を実施している。
ウ）ｂ）	実施細目に基づく情報共有に係るルールの改善等		・各分野において、セプター内における情報共有のルールについて、実施細目との整合性の確認、状況に応じた助言等を実施。
エ）ａ）	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	・内閣官房において、重要インフラ所管省庁の協力を得て、平成22年度末の各セプターの特性、活動状況を把握するとととともにセプター特性把握マップを公表した。
エ）ｂ）	セプターの強化及び訓練		・内閣官房において、重要インフラ所管省庁の協力を得て2010年７月から10月にかけて10のセプターが参加し情報共有訓練を実施。2010年１月までに結果をとりまとめ、重要インフラ所管省庁及びセプターへ報告した。
オ）	広報公聴活動の充実	内閣官房	・NISC重要インフラニュースレターの発行等の広報活動を実施した。広報公聴に資するウェブサイトを充実させたほか、情報セキュリティ政策に関する講演を６回行った。
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	・内閣官房において、関係機関との意見交換会を四半期ごとに実施した。また、重要インフラ事業者等とリスクコミュニケーションを行なう場として、共通脅威分析及び分野横断的演習検討会やセプターカウンシルとの意見交換会を計８回実施した。
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	・2011年２月に、「2010年度 制御システムの情報セキュリティ動向に関する調査」の成果報告及び、制御システムの有識者の講演（NISCの丹代氏が、日本の重要インフラにおける政府としての取組を解説する等）を行う「重要インフラとスマートグリッドのセキュリティシンポジウム」を開催した。

該当項目	施策名	担当省庁	進捗状況
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	・「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」は、「制御システムセキュリティ情報共有タスクフォース」と名称を改め、啓発対象の範囲を広げ、JPCERT/CCにおいて、隔月発行を基本として号外を含めたニュースレターを2010年度は10回発行している。 ・2011年２月に開催した制御システムセキュリティカンファレンスにおいて、ベンダーやユーザー等国内外の制御システム関係者約250名の参加による、制御システムにおける現実化した脅威と対策課題に関する講演やパネルディスカッション、講演等を行い、様々な立場の参加者に対して問題提起と先進事例の共有を図った。 ・制御システムセキュリティ評価ツールである日本版SSAT（Scada Self Assessment Tool）を2011年２月に関係機関の協力のもとに開発し、公開した。
ケ）ａ）	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は脆弱性情報の調整機関として世界で２番目の米国MITRE社認定のCNA（Candidate Numbering Authority）となり、CVE採番活動を本格化させた。 ・脆弱性に伴う対応コスト等の最小化を目指す活動として長期滞留案件の取扱方針の策定を行った。具体的には、対応する情報セキュリティ早期警戒パートナーシップガイドラインの改訂がなされ、平成23年２月からのパブリックコメントを経て、平成23年３月に情報セキュリティ早期警戒パートナーシップガイドライン改訂版として、IPA及びJPCERT/CCから公表された。また、これに伴い、JPCERT/CC 脆弱性関連情報取扱いガイドラインも改訂を行い、同月に公表した。
ケ）ｂ）	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		・JPCERT/CCにおいて、平成23年３月末日までに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約4,200件収集・分析し、33件の注意喚起、34件の早期警戒情報配信を行った。
ケ）ｃ）	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		・共通脆弱性評価システム（CVSS）の脆弱性評価基準を用いて表現されたソフトウェア等の脆弱性に関する情報を取り扱うMyJVN APIやNIST NVDなどの外部データソースとの連携により、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サービス（VRDAフィードの配信）として、機械処理用途のデータの配信数の増加と安定的な供給を実現し、計5,659件のデータ配信を行った。
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

・「セプターカウンシル」の活動促進

該当項目	施策名	担当省庁	進捗状況
ア）	「セプターカウンシル」の支援	内閣官房	・内閣官房においては、セプターカウンシル事務局として、カウンシルの意思決定を行う総会、総合的な企画調整を行う幹事会及び個別のテーマについての検討・意見交換等を行うWGの運営を通じて、カウンシル活動を支援した。2010年度は、延べ21回の会合を開催し、分野横断的な情報共有の推進を図った。

・「安全基準等」の整備浸透

該当項目	施策名	担当省庁	進捗状況
ア）ａ）	「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	・内閣官房において、重要インフラ所管省庁の協力を得ながら、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」策定に当たっての指針（第３版）」を、第23回情報セキュリティ政策会議にて決定した。

該当項目	施策名	担当省庁	進捗状況
ア）ｂ）	「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	・内閣官房において、IT障害事例、社会動向の変化、分野横断的演習等の動向を踏まえ、指針の分析・検証を実施した。現行の指針で特段支障ないものの2010年度以降も引き続き分析・検証を行う。
ア）ｃ）	「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		・重要インフラ所管省庁においては、指針や各重要インフラ分野の特性を踏まえ各重要インフラ分野における「安全基準等」の分析・検証、必要に応じて「安全基準等」の改定等を実施している。
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	＜重要インフラ分野における調査＞ ・内閣官房において、2010年度に、「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た。 ＜重要インフラ事業者等に対する調査＞ ・内閣官房において、重要インフラ所管省庁の協力を得て、2010年度の調査を実施し、とりまとめた調査結果を公表した。 ・内閣官房において、重要インフラ所管省庁の協力を得て、2011年度の企画・調査の準備を実施している。
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	・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・評価を行い、その結果を2010年12月に公表。当該分析・評価の内容を踏まえ、安全・信頼性確保のあり方を検討中。

・重要インフラ防護対策の向上

該当項目	施策名	担当省庁	進捗状況
ア）	共通脅威分析の実施	内閣官房	・有識者、重要インフラ事業者及び重要インフラ所管省庁からなる「共通脅威分析及び分野横断的演習検討会」を設置し、「クラウドコンピューティング」を本年度の分析テーマに掲げ、重要インフラ事業者等との個別打ち合わせや検討会での意見交換を行いながら脅威分析を実施し、報告書を取りまとめ、結果を公表した。
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	・内閣官房において、有識者、重要インフラ事業者及び重要インフラ所管省庁からなる「共通脅威分析及び分野横断的演習検討会」を設置し、「大規模通信障害」をテーマに、検証課題やシナリオ等についての議論を進め、平成22年12月13日に延べ人数141人（試行的に行った自職場からの演習参加者17人を含む）が参加する分野横断的演習（CIIREX2010）を実施し、報告書を取りまとめ、結果を公表した。
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	・システムの堅ろう化について、堅ろう化の概念や海外のサイバー攻撃事例の調査をした。また、制御システムのオープン化、情報システムのサプライチェーンの広がり、スマートグリッドの導入といった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調査を実施した。
エ）ａ）	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	・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った。
エ）ｂ）	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		・「2010年度 制御システムの情報セキュリティ動向に関する調査」を実施し、2009年度調査の欧州、米国に引き続きアジアにおける制御システム動向と、スマートグリッド（スマートメータ等）のセキュリティ動向について調査を行なった。また、アジアにおいて、「ガイド・ツール」、「評価・検証」、「データベース」、「認証」の４つの視点から制御システム動向について調査を行い、調査報告書にまとめた（本調査報告書は2011年５月に公開済み）。
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
カ）ａ）	重要無線通信妨害対策の強化	総務省	・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した。

該当項目	施策名	担当省庁	進捗状況
カ）ｂ）	重要無線通信妨害対策の強化	総務省	・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更新及び性能向上並びに混信が発生している地域へDEURASセンサーを整備するため、2010年度末までに32式を更改した。
カ）ｃ）	重要無線通信妨害対策の強化		・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2010年度末までに実施し、所期の目的を達成した。

・事業継続計画（BCP）の充実

該当項目	施策名	担当省庁	進捗状況
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あり方について、国内海外の災害対策や事業継続計画等の事例を2010年度に調査し、検討課題を洗い出した。

・重要インフラ分野での国際連携推進

該当項目	施策名	担当省庁	進捗状況
ア）ａ）	重要インフラ分野での国際連携推進	内閣官房	・2010年６月及び９月にIWWNに参加し、IWWNとしてのサイバーストームⅢへの参加準備に貢献した。また10月に台湾で開催されたメリディアンに参加し、情報共有に関するワークショップをとりまとめるとともに、欧米やアジア各国の重要インフラ防護担当者との意見交換を通じ、情報セキュリティ政策の国際的な動向に関する情報収集を行った。
ア）ｂ）	重要インフラ分野での国際連携推進		・2010年９月に開催された世界的規模のサイバー演習であるサイバーストームⅢにIWWNの一員として参加した。また、2011年に我が国でIWWN会合を開催することを視野に入れて準備を行った。
ア）ｃ）	重要インフラ分野での国際連携推進		・重要インフラニュースレター等において海外の関連動向を紹介したほか、セプターカウンシル等において各国の動向や演習等について情報提供を行った。

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

③ その他の基盤強化

・マルウェア対策等の充実・強化等

該当項目	施策名	担当省庁	進捗状況
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	・2006年度より、総務省及び経済産業省の連携の下、関連団体と協力し、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攻撃等を停止させるための対策等を実施してきた。平成23年度からの民間による自主的な取組へ移行。
イ）ａ）	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	・「国際連携によるサイバー攻撃予知・即応技術の研究開発」を2011年度施策として実施予定。
イ）ｂ）	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		・「マルウェア配布等危害サイト回避システムの実証実験」（2009～2011年度）の２年目として、１年目に構築したマルウェア配布等危害サイト回避システムの問題点を抽出・改良を行った。
ウ）ａ）	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	・JPCERT/CCにおいて、インシデント報告の受付、攻撃手法の解析及び被害の発生・拡大の抑止のためのインシデント発生源等への連絡調整、脅威情報の収集・分析、注意喚起等の情報発信、脆弱性関連情報に関する製品開発者間の調整、製品開発者への情報提供から対策情報公開に至るまでの調整を迅速に行うための製品開発者連絡網の拡充等の活動を継続して行うとともに、国内ブランドのフィッシングサイトの増加や震災関係事案に対応すべく「フィッシング対策協議会」との間の情報連携を一層強化した。制御システムの脆弱性の問題に対応すべく「セキュリティ情報共有タスクフォース」の活動として、制御システム・セキュリティに関連した情報を提供した。 ・2010年度は、特に、Exploit Kit等の攻撃に使われるツール類の解析に力をいれ、攻撃手法の変化に関する分析を試みたほか、国内外の専門家等との間で、分析結果に関する情報交換を行った。 ・JPCERT/CCにおいて、攻撃手法や脅威動向に関する情報共有・連携を目的とする、情報セキュリティに関する専門家や事業者、関係機関間での会合を年間で約20回以上開催した。 ・JPCERT/CCにおいて、標的型メール攻撃への対応に関する組織内演習のプログラムであるITセキュリティ予防接種に関する調査レポートを日本語及び英語にてウェブ上で公開した。
ウ）ｂ）	コンピュータセキュリティ早期警戒体制の強化		・JPCERT/CCにおいて、APCERT（Asia Pacific computer emergency Response Team）のメーリングリストやAPCERTに設置されたTSUBAMEワーキンググループにおける活動等を通じ、マルウェアやソフトウェアの脆弱性、その他の攻撃手法、DDoS等に関する状況や分析結果等に関する情報共有を進めている。また、2010年９月に実施したASEANを中心とする15のチームが参加した「ASEANサイバーセキュリティ演習」、及び、2011年２月に実施したAPCERTメンバによる演習も、各国チームがマルウェアや攻撃手法の解析を行い、結果を共有するシナリオで実施された。 ・また、海外の関係機関と共有している攻撃手法の分析レポートについては、2010年度は、新たにタイ、インドネシア、ベトナム、マレーシアとの共有を開始した。 ・国内においては、JPCERT/CCにおいて、攻撃手法や脅威動向に関する情報共有・連携を目的とする、情報セキュリティに関する専門家や事業者、関係機関間での年間で20回以上の会合を開催した。

該当項目	施策名	担当省庁	進捗状況
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	・JPCERT/CCにおいて、国内においては、日本シーサート協議会に対する貢献活動を通じて、国内のCSIRTとの共同活動を通じた相互理解と信頼関係の醸成を図っている。 ・海外における組織内CSIRT構築・運用支援活動として、JPCERT/CCは、2010年７月にインドネシアAcademy CERT Meetingにおいて、大学のCSIRT向けにプレゼンテーション及びトレーニングを実施しインドネシア国内の14大学から約100名の参加者があった。 ・また、2010年５月にはルワンダにおいて、11月には南アフリカ共和国において、AAF（Africa Asia Forum on Network Research and Engineering）主催の、アフリカ地域のCSIRT要員向けCERT Trainingで、講師を務めた。
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	・情報セキュリティ研究開発戦略の策定の一環として、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し、検討結果を報告書に取りまとめた。
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を踏まえ、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具体的制度設計等について、関係者との意見交換及び調整を行いつつ、検討を進めたところであり、今後とも当該検討等を踏まえ、引き続き著作権分科会報告書に基づいた措置を講ずるべく、作業を進めることとする。
ウ）ａ）	マルウェアに関する情報収集・提供	経済産業省	・TIPSを引き続き運用するとともに、ウェブサイトにおける新たなウイルス感染手口（新型のGumblar型攻撃など）を調査、検知するための機能として、パターンに依存しない脅威検出技術である「高対話型ウェブクローラ」について調査を行い、その機能要件の整理、及びゼロデイ攻撃の判定機能を包含した形で、「TIPS第一次機能強化」として手続きを進めた。 なお、可搬型媒体（USBメモリ等）の機能を悪用するウイルスについては、民間企業による対策（※）が行われたため、IPAとしての特別な対策は不要となった。 ※ マイクロソフト社が、USBメモリ等の自動実行（オートラン）機能を無効化する修正プログラムを、一般利用者向けにWindows Updateで配信した。
ウ）ｂ）	マルウェアに関する情報収集・提供		・標的型攻撃の検体を収集し、関係機関と連携しつつ、攻撃手口の解析、対策の策定を行なった。この結果については、ウェブによる情報提供（2010年11月）、経済産業省主催の研究会での報告（「サイバーセキュリティと経済研究会」（2010年12月））を行うとともに、必要に応じてウイルス対策ソフトベンダーに検体提供を行なった。
エ）	標的型攻撃の手法解明と対策情報の提供	経済産業省	・JPCERT/CCにおいて、標的型攻撃に用いられた検体について解析を行い、対策の検討を行うとともに、その内容に応じ、注意喚起、早期警戒情報による情報発信を行ったほか、関係機関への通知等、150件以上の情報提供を行った。
Ⅲ　ソフトウェアの脆弱性対策			
ア）ａ）	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	・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サービス（VRDAフィードの配信）については、JPCERT/CCにおいて、データ配信数の増加などの利便性を向上させるため、2010年６月よりIPAが運用するMyJVN API及びNIST（National Institute of Standards and Technology）のNVD（National Vulnerability Database）を外部データソースとして利用する方式への切替えを実施した。これによる配信件数は5,659件である。

該当項目	施策名	担当省庁	進捗状況
ア）ｂ）①	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	・一般利用者が使用するソフトウェアが脆弱性対策が施された最新バージョンであるか、簡易的な操作で確認できる「MyJVNバージョンチェッカ」を2009年度に続き、公開した。月平均で100万件を超えるダウンロードが行われ、企業の脆弱性対策等で活用された。また、次期バージョンについても、2011年度に公開すべく、開発に着手した。
ア）ｂ）②			
イ）ａ）	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	・JPCERT/CCは脆弱性情報の調整機関として世界で２番目の米国MITRE社認定のCNA（Candidate Numbering Authority）となり、CVE採番活動を本格化させた。 ・2008年５月から開始した英語による脆弱性関連情報の発信については2010年度は、発信案件の約80%を日英同時公開し、海外のセキュリティ対策機関への情報公開の迅速化を図った。 ・脆弱性に伴う対応コスト等の最小化を目指す活動として長期滞留案件の取扱方針の策定を行った。具体的には、対応する情報セキュリティ早期警戒パートナーシップガイドラインの改訂がなされ、平成23年２月からのパブリックコメントを経て、平成23年３月に情報セキュリティ早期警戒パートナーシップガイドライン改訂版として、IPA及びJPCERT/CCから公表された。また、これに伴い、JPCERT/CC 脆弱性関連情報取扱いガイドラインも改訂を行い、同月に公表した。 ・危険なコーディング作法や未定義の動作を削減するセキュアコーディングスタンダードについてセミナー実施及び資料公開（CERT C Secure coding Standard 日本語版）を行った。
イ）ｂ）	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		・JPCERT/CCにおいて、東京、名古屋、大阪等合計16回のセキュアコーディングセミナー・講演を実施した（参加者は約600名）。セミナー・講演の実施と併行して解説資料の開発も行い、コース内容の一層の充実を図った。 ・また、2010年10月にインド、11月にベトナム、12月にフィリピンにおいて、各国の開発者合計約230名に対し、C/C++セキュアコーディングセミナーを実施するとともに、今後、より効果的な海外向け啓発活動を実施するため、各国における開発現場の課題、開発手法、プロジェクトの傾向など情報収集を行った。
イ）ｃ）	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		・2010年11月に「TCP/IP 既知の脆弱性検証ツール V5」として、新バージョンでの貸出を開始した。新バージョンでは、既に19件の貸出依頼があり、旧バージョンからの通算では139件の貸出を行っている。 また、併せて「SIP既知の脆弱性検証ツール V2」についても、新バージョンでの貸出を開始した。新バージョンでは、検証項目の拡充を含めて、検証でカバーできる脆弱性の数を増やした。
イ）ｄ）	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		・2011年1月に「開発者向け脆弱性体験学習ツール AppGoat」を公開し、企業の研修等でも本ツールが活用された。
イ）ｅ）	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		・TIPSを引き続き運用するとともに、ウェブサイトにおける新たなウイルス感染手口（新型のGumblar型攻撃など）を調査、検知するための機能として、パターンに依存しない脅威検出技術である「高対話型ウェブクローラ」について調査を行い、その機能要件の整理、及びゼロデイ攻撃の判定機能を包含した形で、「TIPS第一次機能強化」として手続きを進めた。

該当項目	施策名	担当省庁	進捗状況
イ）ｆ）	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	・脆弱性に伴う対応コスト等の最小化を目指す活動として長期滞留案件の取扱方針の策定を行った。具体的には、対応する情報セキュリティ早期警戒パートナーシップガイドラインの改訂がなされ、2011年２月からのパブリックコメントを経て、2011年３月に情報セキュリティ早期警戒パートナーシップガイドライン改訂版として、IPA及びJPCERT/CCから公表された。また、これに伴い、JPCERT/CC 脆弱性関連情報取扱いガイドラインも改訂を行い、同月に公表した。
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、対処に役立てる為、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ツール」（iLogScanner）を企業のウェブサイトに提供中。2010年８月には、新規の攻撃に対応できるように新たな攻撃パターンの検知や検出対象のログフォーマットの拡張を行い、一般にリリースした。新バージョンでは、１ヶ月当たり約2,300件利用されており、ウェブサイト運営者に有効に活用されている。
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
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
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	・学識経験者、弁護士、IT技術者等で構成される「サービス妨害攻撃対策検討会」を設置して、サービス妨害攻撃の構造や攻撃に対する対策を検討するとともに、有識者へのインタビュー調査等を実施し、企業や団体のサービス妨害攻撃に対する留意点を取りまとめ、公開した。
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」の一般国民への提供を2011年３月より開始した。
ウ）	DNSSEC導入の促進	総務省	・電気通信事業者及び企業のネットワーク管理者がDNSSECを導入するためのポイントや注意事項等を盛り込むと共に、一般及び子供向けにもDNSSECの利点を解説し、DNSSEC対応のプロバイダの利用で安全性が高まる旨の解説を加えたコンテンツを作成した。現在「国民のための情報セキュリティサイト」に掲載準備中。
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	・信頼性を評価するための評価指標（メトリクス）の標準化案について取りまとめ、国際標準化組織であるISO/IECに提案した。
オ）ａ）	スパムメール対策の強化	内閣官房、総務省及び消費者庁	・総務省及び消費者庁において、2010年度は特定電子メール法及び特定商取引法に基づき、計10件の行政処分を実施した。
オ）ｂ）	スパムメール対策の強化		・総務省において、迷惑メール対策推進協議会と協力し、各種業界団体に対して送信ドメイン認証技術等迷惑メール対策技術の導入を推進するための説明会を８回開催した。
オ）ｃ）	スパムメール対策の強化		・総務省において、2010年５月にブラジルと第１回ジャパン－ブラジル アンチスパムワークショップを開催し、迷惑メール対策について意見交換を実施した。2010年９月に、ベトナムとICT分野における協力関係に関するMOUが締結され、同文書中において迷惑メール対策における連携について確認した。2011年２月に、インドと日印経済連携協定が締結され、電気通信サービス付随書において、迷惑メール対策に関するベストプラクティス等の情報交換を行うことを確認した。また、迷惑メールの送信元IPアドレスの交換を、中国、ブラジル等と実施している。
オ）ｄ）	スパムメール対策の強化		・総務省及び消費者庁において、「迷惑メール追放支援プロジェクト」としてインターネット接続サービス事業者への違法スパムメールに関する情報提供を引き続き実施している。
オ）ｅ）	スパムメール対策の強化		再掲

・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

該当項目	施策名	担当省庁	進捗状況
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	・内閣官房において、統一基準の改定に際してクラウド化への対応を図るとともに、「外部委託における情報セキュリティ対策実施規程」（政府機関統一基準適用個別マニュアル）についてもクラウド化への対応に係る見直しを実施し、第25回情報セキュリティ政策会議の開催と同日付で公表。
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し、JIS Q 27001ベースの「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」を策定した。また、本ガイドラインを情報セキュリティ監査に反映させるために調整した。さらに、ISO/IEC27001における国際標準化に向けた取組を開始した。
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	・「クラウドと日本の競争力に関する研究会」の中で、クラウドサービスレベルチェックリストを策定し、研究会報告書と共に、2010年８月16日に公表。
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	・2010年度は高信頼クラウドサービス制御基盤技術及び環境対応型ネットワーク構成シグナリング技術に関し、クラウドシステム間におけるリソース再構成などの基本機能のプロトタイプ開発等を進めるとともに、クラウド連携のための高信頼・省電力なネットワーク自律最適制御技術等に係るアーキテクチャ設計などを行った。

・IPv6対応に関する情報セキュリティ確保方策

該当項目	施策名	担当省庁	進捗状況
ア）	IPv6運用技術習得のためのテストベッドの整備	総務省	・2009～2010年度の２か年計画の２年目として、引き続きIPv6ネットワークの運用技術を習得可能な実験用ネットワーク（テストベッド）を広く提供した。
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、IPv6普及・高度化推進協議会においてIPv6対応セキュリティガイドラインの策定に向け検討を開始した。 また、インターネットサービスプロバイダにおけるIPv6接続サービスの提供状況調査を実施し、現在調査結果の公表に向け準備中。

・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

該当項目	施策名	担当省庁	進捗状況
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	・内閣官房において、2010年度に情報セキュリティや個人情報保護の専門家を集め、従来の情報セキュリティ政策にとらわれず幅広い観点から検討（サイバー空間の安全性・信頼性向上のための課題等に関する検討会）を行い、海外動向等も踏まえながら、主に制度的な観点から今後我が国で対応が求められる課題について論点整理を行い、平成23年３月25日に報告書を取りまとめた。
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
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	・システムLSIのセキュリティ評価を実施する評価者の能力判定を行なうためのスマートカード形状のテストビークル（評価対象）を開発すると共に、既に購入済みのセキュリティ評価ツールを用いた認証要員の訓練を実施した。
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
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

該当項目	施策名	担当省庁	進捗状況
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

・医療、教育分野等における情報セキュリティ確保方策

該当項目	施策名	担当省庁	進捗状況
ア）ａ）	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・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」等を踏まえ、ASP・SaaS事業者が医療機関と契約する際に合意すべき事項（サービスレベルや責任分界等）を整理し、SLAの参考例としてまとめ、平成22年12月24日に「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くSLA参考例」として公表した。
ア）ｂ）	医療分野・教育分野におけるASP・SaaSの普及に向けた取組		・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留意すべき事項をガイドラインとして整理し、2010年10月15日に「校務分野におけるASP・SaaS事業者向けガイドライン」として公表した。

・中小企業に対する情報セキュリティ対策支援

該当項目	施策名	担当省庁	進捗状況
ア）ａ）	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	・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。
ア）ｂ）	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		・民間の取組の中で、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が普及促進した。
イ）ａ）	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	・中小企業の情報セキュリティ対策実施を促進するため、全国各地の商工会議所・商工会関係者・ITコーディネータ等に対して、中小企業情報セキュリティ対策指導者育成セミナーを、全国25カ所で開催。 また、地域の中小企業などに対して情報セキュリティ対策を推進するための「IPA中小企業情報セキュリティセミナー」にて、マネジメントコース入門編Ⅰ、マネジメントコース入門編Ⅱ、技術コース標準編Ⅰ、技術コース標準編Ⅱの４コースを開設し、商工会議所及びNPOなどの協力を得て、全国27都道府県34か所で開催した。４コース合計では、106回開催、計6,391名が出席し、情報セキュリティ対策のマネジメント及び技術の両面から、情報セキュリティに関する知識等を取得させ、中小企業のセキュリティレベルの向上を図った。
イ）ｂ）	中小企業における情報セキュリティ対策の推進		・「IPA中小企業情報セキュリティセミナー」にて、情報セキュリティ対策のコストをなるべくかけずに実施できる中小企業の情報セキュリティ対策ガイドラインの「５分でできる自社診断シート」の内容を詳細に説明し、普及を促進した。また、経済産業省の「中小企業情報セキュリティ対策促進事業」の中小企業向け指導者育成セミナーにおいてチェックシート等の紹介を行うなどの普及啓発を実施した。このチェックシートは2010年度累計で約５万部を発行し、中小企業が自ら情報セキュリティ対策をチェックし、更なる対策を進められるよう普及に努めた。さらに、このチェックシートのeラーニングツールである「５分でできる！情報セキュリティポイント学習」を紹介するコースを、「IPA中小企業情報セキュリティセミナー」において設置、開催するとともに「５分でできる！情報セキュリティポイント学習」等の収録された普及啓発用CD-ROMを約6,400枚配布した。

該当項目	施策名	担当省庁	進捗状況
ウ）ａ）	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	・中小企業情報セキュリティ指導者育成セミナーの受講者が、中小企業者に対して講習会を全国各地で９５回開催し、地域の中小企業者の相談窓口対応と情報提供等を行った。
ウ）ｂ）	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		・マルウェア及び不正アクセス全般の相談に一元的に対応する、「情報セキュリティ安心相談窓口」を2010年10月に開設した。 また、地域の情報セキュリティの中核となる団体と調整を進め、（株）石川県IT総合人材育成センター（石川）、NPO法人 みちのく情報セキュリティ推進機構（宮城）、（株）いばらきIT人材開発センター（茨城）、NPO法人 鹿児島インファーメーション（鹿児島）、NPO法人 情報セキュリティ研究所（和歌山）、NPO法人 情報セキュリティフォーラム（神奈川）、（財）ソフトピアジャパン（岐阜）との連携を深め、地域での身近な情報セキュリティ人材を育成するための協力体制を構築した。これらの協力団体にて育成された人材は即戦力として、山形県山形市、栃木県宇都宮市、東京都三鷹市、神奈川県横浜市、神奈川県厚木市、千葉県市川市、新潟県新潟市、石川県金沢市、静岡県浜松市、愛知県名古屋市、京都府京都市、兵庫県尼崎市、兵庫県たつの市、和歌山県海南市、岡山県岡山市、熊本県熊本市及び鹿児島県鹿児島市の「IPA中小企業情報セキュリティセミナー」に講師として派遣した。さらに、（株）いばらきIT人材開発センターが主催するセミナーにて、IPAのセミナーテキストを基にしたセキュリティコースを設けるなど、相互協力関係を強化した。

・安全な電子商取引の推進

該当項目	施策名	担当省庁	進捗状況
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	・企業における電子署名の利活用の普及促進策について引き続き検討を行うとともに、電子署名の活用事例等について紹介するセミナー（全国５都市で開催）等を通じて、電子署名の一層の普及を図った。

・知的財産保護の推進

該当項目	施策名	担当省庁	進捗状況
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	・2011年１月に開催された文化審議会著作権分科会において、著作権法における技術的保護手段及びその回避規制に関する制度改革案に係る報告書が取りまとめられた。文化審議会著作権分科会報告書を踏まえ、速やかに法制化に向けて取り組む。 ・不正競争防止法のアクセスコントロール等の技術的制限手段に係る規律のあり方に関する制度改革案を年度内に取りまとめるべく、産業構造審議会知的財産政策部会技術的制限手段に係る規制のあり方に関する小委員会を立ち上げ、2011年２月に、報告書を取りまとめた。当該小委員会の結論を踏まえ、第177回通常国会に「不正競争防止法の一部を改正する法律案」が提出される予定。（なお、2011年４月１日に国会に提出された。） ・2010年11月、関税・外国為替等審議会において「アクセスコントロール等回避機器について、国内規制が整備される場合には、関税法上の輸出入禁止品に追加する」旨を盛り込んだ「平成23年度関税改正に関する論点整理」が取りまとめられ、また、同年12月、同様の内容を盛り込んだ「平成23年度税制改正大綱」が閣議決定された。不正競争防止法においてアクセスコントロール等回避機器の国内規制が整備される予定であることから、上記閣議決定等を踏まえ、アクセスコントロール等回避機器を関税法上の輸出入禁止品に追加することを盛り込んだ「関税定率法等の一部を改正する法律案」を2011年１月、国会に提出した。法案が成立した場合に向け、改正法の内容の周知等に係る準備を実施する。
イ）	プロバイダによる侵害対策措置の促進	総務省	・プロバイダ責任制限法ガイドライン等検討協議会等、民間におけるプロバイダと権利者による協働の仕組みを促進するとともに、2010年３月に「コンテンツ不正流通対策連絡会」を設置、2010年９月にコンテンツ不正流通対策の共同検知システムの実証実験の請負事業者を決定し、実証実験を実施することにより、コンテンツの不正流通を効率的に検知・排除するために必要な不正流通対策の仕組み、コンテンツの不正流通をネットワーク上で効率的に検知・排除を行うシステムや体制等のあり方について検討を実施した。 ・2010年９月７日、総務省の「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」において、「プロバイダ責任制限法検証WG」（主査：東京大学長谷部恭男教授）が設置され、同WGにおいてプロバイダ責任制限法の検証が実施された。
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、経済産業省	・関係国間での交渉の結果、2010年10月、東京で開催された関係国会合で大筋合意に至り、2010年中に交渉を終了した。

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

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

該当項目	施策名	担当省庁	進捗状況
ア）	NISCの強化	内閣官房	・政府機関統一基準に基づくPDCAサイクルの確立のため、各府省庁に対し政府機関統一基準に基づく調査・評価を行うとともに、自己点検の効率化や教育についての支援を行うなどの施策を推進。 ・我が国の国際的なPOC機能としての役割を果たすべく、情報セキュリティに係る問題を議論する国際会合であるFIRST、APECの作業部会等に参加したほか、IWWNのメンバー国として国際的なサイバー演習に参加するなど諸外国の政府機関・民間企業等との連携強化を推進。
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	・内閣官房において、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、NISCで蓄積した専門的知見をもとに情報セキュリティ・コンサルティング機能の充実を継続的に図っている。
ウ）	関係機関等との連携強化	内閣官房及び内閣府	・IT戦略本部との連携を図り、「新たな情報通信技術戦略」（平成22年５月11日）に「国民を守る情報セキュリティ戦略」についての内容を盛り込んだ。

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

（2）国民・利用者保護の強化

① 普及・啓発活動の充実・強化

該当項目	施策名	担当省庁	進捗状況
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	・2011年２月の「情報セキュリティ月間」において、キャッチフレーズ及び「情報セキュリティ３か条」の制定、特設ページ「国民を守る情報セキュリティサイト」の新設、キックオフ・シンポジウムをはじめ、官民による3,000を超える関連行事を開催。 ・内閣官房において、「情報セキュリティ月間」の周知及び情報セキュリティに関する普及・啓発を促進するため、ポスター・ステッカー・ウェブバナーを作成、配布。 ・内閣官房において、「政府インターネットテレビ」を通じ、日本語及び英語による「情報セキュリティ月間」の周知を実施した。
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関する普及・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、包括的な普及・啓発プログラムとして「情報セキュリティ普及・啓発プログラム（案）」を取りまとめた。（2011年４月にパブリックコメントの募集を開始。）
ウ）ａ）	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	・韓国の韓国インターネット振興院との共同事業の一環として、コンピュータウイルスの感染やコンピュータへの不正な侵入、ワンクリック詐欺などの被害に遭わないよう、特に若年層の「情報セキュリティ対策」の意識を高めるために、2006年からIPA主催事業として実施し、2010年７月１日から９月10日まで、全国の小学生・中学生・高校生を対象に募集を行い、302校、8,676件（標語8,118件、ポスター558件）の応募があった。なお、応募作品について、９月に「第６回 IPA情報セキュリティ標語・ポスター」コンクールの審査委員会を開催し、入選候補作品合計50作品を決定し、10月に開催した「IPA Forum 2010」において、入選者の授賞式を行った。
ウ）ｂ）	各種メディア等を通じた普及・啓発の推進		・2010年10月に行われた情報化月間の「情報化促進貢献表彰（情報セキュリティ促進部門）」において、総務大臣表彰、経済産業大臣表彰、総務省情報通信国際戦略局長表彰及び経済産業省商務情報政策局長表彰を行った。
ウ）ｃ）	各種メディア等を通じた普及・啓発の推進		・「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、2010年６月、最優秀作（総務大臣賞）を含む計11作品の選定・表彰を実施するとともに、受賞作品を用いた啓発活動を2010年度中に実施した。

該当項目	施策名	担当省庁	進捗状況
ウ）ｄ）	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	・内閣官房において、NISCのウェブページ等を活用し、情報セキュリティ政策会議の開催状況を始めとしたNISCの活動につき適時適切な広報啓発を実施している。また、NISCメールマガジンを定期的に発行。なお、2010年度には、普及・啓発活動のポータルサイトである「国民を守る情報セキュリティサイト」を新設し、広報啓発を実施。 ・内閣官房において、企業、一般国民等に対し、情報セキュリティ政策、情報セキュリティ対策等に関する講演を実施。 ・都道府県警察において、学校等教育機関、行政機関、企業、一般国民に対し、情報セキュリティに関する意識・知識の向上を図るため、サイバー犯罪の手口や被害防止対策等について、講演の実施やパンフレット配布等の広報啓発を実施。 ・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や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適宜、提供。 ・経済産業省において、警察庁及び都道府県警察の協力の下、全国のNPO法人等と連携し、2010年度も引き続き全国各地で「インターネット安全教室」を開催。2010年度末までに150件開催。 ・総務省「国民のための情報セキュリティサイト」について、情報通信の利用動向及び情報セキュリティの状況等を踏まえたコンテンツを作成。 ・内閣官房が発行するNISCメールマガジンにおいて、情報セキュリティガバナンス導入ガイダンス等を紹介。
ウ）ｅ）	各種メディア等を通じた普及・啓発の推進		・2006年４月から、e-ネットキャラバンの全国規模での本格実施を開始し、同年度は453件、2007年度は1,089件、2008年度は1,208件、2009年度は624件の講座を実施した。 ・2010年度は、557件の講座を実施した。
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	･2010年10月に沖縄で開催されたAPEC電気通信・情報産業大臣会合の開催と併せて、APEC-TEL-WGにおいて各国の普及啓発に関するポスター展示会を我が国の主催で実施したほか、日・ASEAN情報セキュリティ政策会議等において意識啓発に関する情報の共有及び共同イベント開催に向けた議論を進展させた。
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	・情報の削除要請等を受けた中小プロバイダからの問い合わせ等に対応する相談窓口「違法・有害情報センター」を設置する等の取組や、業界団体によるウェブ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の支援を実施した。
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	・2010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、「守ろう！電波のルール」をキャッチフレーズに、電波利用ルールの重要性について各種メディア（全国紙、地方紙、業界専門紙、テレビCM、電車・バス車内吊り広告、地方公共団体・関係機関等へのポスター配布・掲示、リーフレットの配布、各種広報誌への掲載等）により周知啓発を実施した。 ・さらに、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した。

該当項目	施策名	担当省庁	進捗状況
キ）ａ）	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	・2010年度のアクセス件数は92,579件（2010年４月１日～2011年３月31日の１年間）であり、アクセストータル件数は、2005年８月４日～2011年３月31日の間で548,950件となった。2010年６月29日には、情報セキュリティ対策ベンチマークシステムVer.3.3として改訂し、情報セキュリティを巡る環境変化や対策レベルの変化を勘案し、診断の基礎データを最新２年分のデータに入替えた。さらに、新しく診断に用いる1,540件の診断基礎データの統計情報及び、2006年から2009年までの４年間の企業規模別の情報セキュリティ対策状況の経年比較データの分析結果を2010年６月29日に公開した。
キ）ｂ）	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		・情報セキュリティに関する主要なウェブ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、ウェブ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した。
キ）ｃ）	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		・情報セキュリティ対策に資する各種ツール・分析等の提供情報セキュリティ対策を実施する人間の行動について、分析し、その結果を第２回情報セキュリティと行動科学ワークショップ、暗号と情報セキュリティシンポジウム2011で発表した。
キ）ｄ）	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		・情報セキュリティ対策を実施する人間の行動原理について国際的な研究分析状況と、IPAでの活動を紹介することを目的に10月に、電子情報通信学会と共催で、「情報セキュリティと行動科学ワークショップ」を開催した。
キ）ｅ）	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		・2009年度の情報セキュリティ事象について、動向、今後の展望をまとめ、2010年９月に「情報セキュリティ白書2010」を出版した。
ク）	情報システム調達地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
ケ）	非機能要求の合意手法の活用・普及	経済産業省	・非機能要求グレードについて英語版を作成し、海外展開を行うと共に、非機能要求を合意することの重要性について理解を深めるため、国内の経営層向けの小冊子を作成した。

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

（2）国民・利用者保護の強化

② 情報セキュリティ安心窓口（仮称）の検討

該当項目	施策名	担当省庁	進捗状況
ア）	「情報セキュリティ安心窓口（仮称）」の検討	内閣官房	・「情報セキュリティ安心窓口（仮称）」のあり方を検討し、各府省庁が既に設置している情報セキュリティに関する相談窓口について連携を強化するなど相談体制を充実させること、及び消費者に対する窓口相談対応力の強化を検討することを「情報セキュリティ普及・啓発プログラム（案）」に盛り込んだ。
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	・従来からある相談窓口を、マルウェア及び不正アクセス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」を開設し、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した。 IPAウェブサイトに「よくある相談と回答（FAQ）」ページを掲載することで、相談対応業務の効率化を図った。電話・メール・FAX・自動応答システムなどで相談を受付け、2010年度は合計で22,389件の相談を処理した。相談対応で得た情報を基に、毎月、ウイルス・不正アクセス届出状況公表の際に「今月の呼びかけ」や相談事例として紹介。また、長期休暇前やその他特異なインシデントが発生したタイミングで、広く国民に対する注意喚起を計８回実施した。
ウ）	情報セキュリティ・サポーターの育成・活用	総務省	・利用者の身の回りの詳しい人（情報セキュリティ・サポーター）の育成に向けて、効果的な育成カリキュラムのあり方や、サポーター制度普及に向けたあり方について検討を行った。 ・情報セキュリティサポーターがユーザーサポート部門で利用できるコンテンツを作成するため、調査・検討を行った。

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

（2）個人・利用者保護の推進

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

該当項目	施策名	担当省庁	進捗状況
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	・内閣官房において、2010年度に情報セキュリティや個人情報保護の専門家を集め、従来の情報セキュリティ政策にとらわれず幅広い観点から検討（サイバー空間の安全性・信頼性向上のための課題等に関する検討会）を行い、海外動向等も踏まえながら、主に制度的な観点から今後我が国で対応が求められる課題について論点整理を行い、2011年３月25日に報告書を取りまとめた。
イ）	情報漏えい対策への取組	経済産業省	再掲

・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

該当項目	施策名	担当省庁	進捗状況
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	・内閣官房において、2010年度に情報セキュリティや個人情報保護の専門家を集め、従来の情報セキュリティ政策にとらわれず幅広い観点から検討（サイバー空間の安全性・信頼性向上のための課題等に関する検討会）を行い、海外動向等も踏まえながら、消費者庁と連携しつつ、主に制度的な観点から今後我が国で対応が求められる課題について論点整理を行い、2011年３月25日に報告書を取りまとめた。
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	・2010年７月にガイドラインを改正し、ノートブック型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、本人に対して二次被害が生じないよう適切な技術的保護措置が講じられていた場合には、電気通信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を明記した。

・国際的なフレームワークへの対応

該当項目	施策名	担当省庁	進捗状況
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	・APECデータ・プライバシー・パスファインダー・プロジェクト等の国際的な取組を把握・分析し、各省庁と連携しつつ、我が国として必要な対応・措置を検討した。 ・国際的な会合への出席等を通じ、我が国の個人情報保護法制についての説明等を行うことにより、国際的な理解を求めた。
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	・「情報セキュリティ分野における日・ASEANの連携枠組み」等を踏まえ、データプライバシー保護に関する対応策について調査を進め、その成果をNISCのウェブページに公開している。

・個人情報保護法の見直し

該当項目	施策名	担当省庁	進捗状況
ア）	個人情報保護法の見直し	消費者庁及び関係府省庁	・消費者委員会個人情報保護専門調査会における検討の過程で、必要な資料の提出や説明など、必要な協力を行った。

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

（2）国民・利用者保護の強化

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

該当項目	施策名	担当省庁	進捗状況
ア）	サイバー犯罪の取締りのための態勢の強化	警察庁	・2010年７月、都道府県警察のサイバー犯罪捜査指揮を担当する警察職員対象の専科教養を実施。 ・2011年２月、都道府県警察のサイバー犯罪捜査用資機材の更新・増強を実施。
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
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	・都道府県警察において、インターネットカフェ連絡協議会等を設置し、匿名性排除のための会員制導入の働き掛けや防犯情報の提供等の情報共有を行うなど、事業者との連携強化を図っている。東京都では2010年７月にインターネット端末利用営業の規制に関する条例が施行。 ・インターネットにおける児童ポルノの流通防止に向け、民間団体等で構成される「児童ポルノ流通防止対策専門委員会」の発足（2010年12月）に協力、事業者による４月のブロッキング開始に向け、その環境整備を実施。
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、関係事業者、PTAの代表者等で構成する総合セキュリティ対策会議において、「不正アクセス対策」、「違法有害情報対策」及び「サイバーボランティア育成」の３つのテーマについて議論。
オ）	サイバー犯罪の取締りのための態勢の強化のための国際連携の推進	警察庁	再掲
カ）	中央当局制度を活用した国際捜査共助の迅速化	法務省	・2011年１月、日・EU刑事共助協定につき発効。 ・2011年２月、日・露刑事共助条約につき発効。 ・更なる刑事共助条約の締結につき検討中。

・犯罪抑止のための広報啓発の推進

該当項目	施策名	担当省庁	進捗状況
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	・国家公安委員会（警察庁）、総務省及び経済産業省において、平成22年中の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。 ・警察庁において、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について、委託調査を実施。
イ）	情報セキュリティに関する講習の実施	警察庁	・都道府県警察において、学校等教育機関、行政機関、企業、一般国民に対し、情報セキュリティに関する意識・知識の向上を図る目的で行っている情報セキュリティに関する講習を、2011年２月のサイバー犯罪防止のための広報月間において重点的に実施。
ウ）ａ）	サイバー犯罪の被害防止対策の推進	警察庁	・出会い系サイトに関連した犯罪の被害防止を図るため、中学生・高校生向けのリーフレットを2010年６月に作成し、各都道府県警察において配布するとともに警察庁ホームページへ掲載。 ・携帯電話からのホームページの閲覧の増加を踏まえ、サイバー犯罪被害防止のための携帯電話専用ページを作成。
ウ）ｂ）	サイバー犯罪の被害防止対策の推進		・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や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適宜、提供。
エ）	サイバーボランティア育成の推進	警察庁	・有識者、関係事業者、PTAの代表者等で構成する総合セキュリティ対策会議において、実際にサイバー空間でボランティア活動に従事している団体を紹介し、サイバーボランティアの活動要領、サイバーボランティアの育成のあり方について検討を実施。

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

（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）

該当項目	施策名	担当省庁	進捗状況
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	内閣官房及び関係省庁	・日米サイバーセキュリティ会合（2010年11月米国）、インターネットエコノミーに関する日米政策協力対話（2010年７月課長級（TV会議）、11月局長級（東京））、日・シンガポール二国間会合（2010年７月、2011年３月）を開催するなど米国、ASEAN諸国及びEU諸国と二国間会合を実施して情報交換を行い、連携体制の強化を図った。
イ）ａ）	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	・第２回日・ASEAN情報セキュリティ政策会議でまとめられた「情報セキュリティ分野における日・ASEANの連携枠組み」は、2011年１月の日・ASEAN情報通信大臣会合及び日・ASEAN経済大臣会合プロセスにおいて承認又は報告された。 ・第３回日・ASEAN情報セキュリティ政策会議を開催したほか、情報セキュリティ分野における日・ASEANの連携枠組みを踏まえ、施策等（イ）ａ）～ｇ））を実施するとともに2011年度の実施予定の施策に着実に着手している。事業の進捗状況については、第３回日・ASEAN情報セキュリティ政策会議の場において、報告がなされたところである。
イ）ｂ）	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		・2011年３月に第３回日・ASEAN情報セキュリティ政策会議をASEAN諸国の局長級ら30名が来日して開催した。同会議では、情報セキュリティ分野における意識啓発に関する日・ASEAN間の共同取組等を進めるなどASEAN諸国との連携・取組を強化するための意見交換を実施した。
イ）ｃ）	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		・2010年12月に日・ASEAN政府ネットワークセキュリティワークショップをNISC及びベトナム情報通信省の共催で同国においてASEAN諸国の政府関係者ら約50名を集めて開催し、政府ネットワークの防護などに関する協力の強化を確認したほか、2011年に我が国で同ワークショップを開催することを決定した。
イ）ｄ）	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		・2010年８月に日・ASEAN情報セキュリティ研修をASEAN諸国から30名の参加を得て、日本で開催した。研修参加者の研修満足度アンケートでは、５点満点の中で平均4.76点をつけるなど、ASEAN政府職員のレベル向上に貢献した。
イ）ｅ）	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		・第２回政府ネットワークセキュリティワークショップ及び第３回日・ASEAN情報セキュリティ政策会議において、各国の取組に関する情報共有を目的とするポータルサイトを立ち上げたほか普及啓発に関する共同イベントなどの実施を決定した。
イ）ｆ）	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		・日本及びASEANのネットワークオペレータ間の情報共有を促進するためのワークショップについて、Telecom-ISAC Japanが主催（総務省後援）し、2011年１月13日及び14日に東京で開催。
イ）ｇ）	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		・日・ASEANの連携枠組みにおける研究者連携を進めるに当たり、ASEAN各国の研究者も参加しているアジア地域の研究者連携会合であるRAISE会合の場を活用して、研究者研究結果の共有等を行い研究者間の連携を強めていく予定。
ウ）	APECにおける情報セキュリティ分野の連携推進	総務省	・2010年10月30～31日、第８回APEC電気通信・情報産業大臣会合が沖縄で開催され、安全・安心なICT環境の推進を含む、情報通信分野に関してAPECとして目指すべき共通目標を定めた「沖縄宣言」が採択された。 ・同大臣会合において「APECサイバーセキュリティ意識啓発ポスター展示イベント」を韓国と共催した。 ・2011年３月９日には、アジア太平洋地域の成長に向けたICTシンポジウムを開催し、情報セキュリティ意識啓発の取組に関して議論を行った。 ・APEC電気通信・情報作業部会（2010年５月、８月、2011年３月）において、日本の取組を紹介し、各国との意見交換を実施した。

該当項目	施策名	担当省庁	進捗状況
エ）	途上国向け研修・セミナー等の開催	総務省	・APT研修「ブロードバンド通信のための情報セキュリティ構築」（2011年１月）にて、APT（アジア・太平洋電気通信共同体）加盟国を対象とした情報セキュリティ研修を実施することにより、情報共有を進めるとともに連携を強化。
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	・JPCERT/CCにおいて、2010年10月にインド、11月にベトナム、12月にフィリピンにおいて、各国の開発者合計約230名に対し、C/C++セキュアコーディングセミナーを実施するとともに、今後、より効果的な海外向け啓発活動を実施するため、各国における開発現場の課題、開発手法、プロジェクトの傾向など情報収集を行った。
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	・2011年１月に、ベトナム、マレーシア及びフィリピンにおいて、我が国政府・産業界及び現地国政府の参加を得て、現地企業を対象とした「ビジネスのための情報セキュリティ」に関するセミナーを開催した。また、この機会を得て、現地国の政府を始めとする関係者に対し、企業の情報セキュリティの強化について要請・意見交換を行った。 ・情報セキュリティ製品の評価・認証に関し、現在の国際慣行に沿った対応をうながすべく、アジアの関係国と意見交換を行い、現在の国際的な制度に関しての理解の向上を図った。加えて、情報セキュリティ製品の利用に関する制度に関する意見交換を行い、国際慣行に沿った対応を求めた。
キ）	海外の組織内CSIRTの構築・運用支援	経済産業省	・2010年７月にインドネシアAcademy CERT Meetingにおいて大学内CSIRT向けにプレゼンテーション及びトレーニングを実施しインドネシア国内の14大学から約100名の参加者があった。 ・また、2010年５月にはルワンダにおいて、11月には南アフリカ共和国において、AAF（Africa Asia Forum on Network Reseach and Engineering）主催の、アフリカ地域のCSIRT要員向けCERT Trainingで、講師を務めた。
ク） a）	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	・2010年７月にインドネシア及びベトナムにおいてMalware Lab構築に関する分析トレーニングを実施するとともに、ベトナムのNational CSIRTのマルウェア分析ラボの構築に協力し、同チームのアナリストに対するおよそ３ヶ月にわたる研修（研修生受入）を実施した。
ク） b）	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		・JPCERT/CCは、2010年６月、FIRSTの第22回年次会合に参加し、情報収集を行うだけでなく、各国からの参加者と今後の活動について意見交換を実施した。また、欧米をはじめとする 15ヶ国の政府機関、法執行機関、CSIRT組織で構成されるIWWN（International Watch and Warning Network）に参加し、国際的なサイバー攻撃や脆弱性対応について情報共有を行った。 ・また、2010年９月には、ASEAN（東南アジア諸国連合）を中心とする15のチームが参加したASEANサイバーセキュリティ演習 ACID（ASEAN CERT Incident Drill）に、2011年２月には、15の国及び経済地域から20のAPCERT加盟チームが参加して実施した演習に、それぞれ参加して、実際のインシデント対応時の国際間連携の手続きを確認した。 ・さらに、JPCERT/CCは、シンガポールにおけるRegional Collaboration in Cyber Security（2010年７月）、オランダにおけるGOVCERT.NLカンファレンス（11月）等、多数の情報セキュリティ又はインシデント対応に関するカンファレンスに参加して、講演を行う等により、関係機関との連携強化に努めた。 ・さらに、2010年９月末に米国国家安全省が主催した大規模なサイバー演習「Cyber Storm Ⅲ」については、JPCERT/CCは、準備段階から参画し、演習当日においても、警察庁、NISCとともに、IWWN参加組織として参加。

該当項目	施策名	担当省庁	進捗状況
ケ）ａ）	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	・JPCERT/CCが運営するアジア太平洋地域を主な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）は、現在19の国・経済地域、22の海外CSIRTにおいてセンサーが稼働しており、同システムにより収集され、参加各チーム間で共有しているデータの観測・分析手法の研究等に関する連携の枠組みとして、APCERT（Asia Pacific Computer Emergency Response Team）にTSUBAMEワーキンググループが設置されている。 ・JPCERT/CCから日次で各国に配信している情報セキュリティに関する脅威情報やソフトウェア等の脆弱性に関する分析情報の配信先の拡大及び双方向化については、情報連携に関する覚書締結先国の拡大等と合わせて進めている。
ケ）ｂ）	アジア太平洋地域での早期警戒情報の共有促進		・JPCERT/CCにおいて、APCERT（Asia Pacific Computer Emergency Response Team）のメーリングリストを通じ、マルウェアやソフトウェアの脆弱性、その他の攻撃手法、DDoS等に関する状況や分析結果等に関する情報共有を行ったほか、各国からの問い合わせに応じてインシデント対応の実施の方法等に関する情報共有等の活動を実施した。アジア地域における分析情報の共有に関しては、APCERTの年次会合（2011年３月開催）その他の会合や、APCERTに設置されたTSUBAMEワーキンググループにおける活動等を通じて進めている。また、2010年９月に実施したASEANを中心とする15のチームが参加した「ASEANサイバーセキュリティ演習」、及び2011年２月に実施したAPCERTメンバによる演習も、各国チームがマルウェアや攻撃手法の解析を行い、結果を共有するシナリオで実施された。 ・また、海外の関係機関と共有している攻撃手法の分析レポートについては、2010年度は、新たにタイ、インドネシア、ベトナム、マレーシアとの共有を開始した。
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 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

（3）国際連携の強化

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

該当項目	施策名	担当省庁	進捗状況
ア）	多国間の枠組み等における子国際連携・協力の推進	内閣官房及び関係府省庁	・APEC、ITU、MERIDIAN、OECD、ASEAN、FIRST、ARFなど各分野の多国間枠組みにおいて、会議に参加して議題の設定への貢献や発表の実施など積極的な情報共有を行った。
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
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	・2010年10月独ベルリンで開催された国際会合に参加し、セキュリティ技術に関する標準を検討する委員会であるISO/IEC SC27において国際標準化の推進を提案し、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を行うというプロジェクト化が承認された。2011年４月開催予定のシンガポール会合に向けて国内委員会で議論を行っている。

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

（3）国際連携の強化

③ NISCの窓口機能の強化

該当項目	施策名	担当省庁	進捗状況
ア）ａ）	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	・国民を守る情報セキュリティ戦略、情報セキュリティ2010の英語版をNISCのウェブページに公開するなど国際的な広報、情報発信に努めた。
ア）ｂ）	国際的な窓口機能の強化を通じて各国との連携		・各種会議等を通じて国際的な最先端の動向について国内の関係機関などとの情報の共有、還元に努めた。

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

（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

該当項目	施策名	担当省庁	進捗状況
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	・情報セキュリティ研究開発戦略を策定するため、情報セキュリティの有識者による検討会を開催し、今後重要となる研究テーマの整理を行った。また、検討会の成果及び震災を踏まえた新たな観点を技術戦略専門委員会で議論した。これらの議論を整理し、2011年６月を目処に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	・情報セキュリティ研究開発戦略の検討の一環として、有識者による検討会を開催し、今後重要となる研究テーマの整理を行った。また、この検討会の成果を踏まえ、技術戦略専門委員会の中で、トップダウンの発想（震災を踏まえて政府として優先的に取り組むべきテーマなどの観点）による検討も行った。検討結果は、情報セキュリティ研究開発戦略に盛り込む予定。
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	・2010年度概算要求における科学技術関係施策（セキュリティ領域を含む）についてヒアリングを行い、改善・見直し事項の指摘及び優先度判定を行った。
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	・内閣官房においては、内閣府と連携し、研究計画の柔軟な変更について内閣府の「競争的資金の使用ルール等の統一化」の中で継続して検討を進めた。
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	・それぞれの課題について個別に要素技術の研究開発（基本・詳細設計）を行うとともに、各要素技術間のインタフェースの検討、総合実験モデルの検討、要素技術の一部実装と単体評価を実施した。
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	・2010年度は、インシデント分析の広域化・高度化技術に関して協力団体へシステム展開を行って実験環境を構築し、実証実験を実施した。また、マルウェア対策ユーザーサポートシステムの実験環境の構築を行った。
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	・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として、隠蔽通信路評価プラットフォームに関する構築手法及びPCルータ実装への実現性の検証、並びに評価ルールに関する標準フォーマットの開発に向け検証ツールの試作やフレームワーク等の設計を行った。また、形式的手法によるプロトコル実装の検証技術として、形式検証基盤の構築及び実証、並びにプロトコルの網羅的なテスト検証が可能となるように仕様の検討を行った。
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	・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版を用いた動作記録データセットを2つの学術会議に提供した。また、より柔軟に再現環境を構築できるβ版プロトタイプを開発した。
ケ）	IPv6環境のセキュリティ評価システムの構築	総務省	・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、IPv6ネットワーク上のセキュリティ脅威等を把握するための実証評価試験を実施した。
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	・2010年度は、ダイナミックネットワーク技術に関する研究開発について、最終年度としてその要素技術の確立を図った。また、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についてテストベッド上での技術検証を実施した。

該当項目	施策名	担当省庁	進捗状況
サ）	量子情報通信ネットワーク技術の研究開発	総務省	・独立行政法人情報通信研究機構（NICT）において、将来のどのような技術でも解読不可能な安全性（無条件安全性）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、産学官連携のもとで研究開発を推進中。 ・2010年度は、量子波長多重技術及び光子検出技術等の研究開発を実施し、各要素技術を確立。また、これらの成果のシステム化も進め、NICTの研究開発試験ネットワーク「JGN2plus」上に量子暗号ネットワーク「Tokyo QKD Network」を構築し、試験運用を開始（2010年10月14日）。50km圏において、盗聴者の計算能力に依存しない完全秘匿テレビ会議システムを世界で初めて実現。
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	・これまでに開発したツール群の評価・改善・機能拡張を行うとともに、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とタグデータ生成基盤ツールとの連携を進めた。開発したツールの一部をウェブサイト等を通じて公開した。 ・ソフトウェアタグ利用シナリオの構築法を整備し、シナリオの開発とシナリオ例の蓄積を行った。また、ソフトウェアタグの適用実験として、シナリオに沿って実際にソフトウェアを発注してタグデータの収集・分析を行い、ケーススタディとしてまとめた。 ・これまでに開発・公開したソフトウェアタグ規格Ver.1.0に定めるタグ項目が国際規格として採用されるよう、JTC1/SC07/WG10及び情報規格調査会に参画して活動を行った。 ・法的な観点からユーザーとベンダーにアンケートを行い、システム開発現場での要求に関する調査結果をとりまとめた。具体的には、紛争解決の５つの判断基準について、それらの実証、事例収集、その他の基準の有無などについて調査を行った。 ・以下の研究会、国際ワークショップ、講演会などを開催した。 ○エンピリカルソフトウェア工学研究会（2010年12月、東京、参加者116名） ○International Workshop on Empirical Software Engineering in Practice（IWESEP2010）（2010年12月、奈良、参加者61名） ○Mining Software Repository School in Asia（2010年12月、奈良、参加者61名）
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	・クラウドコンピューティングに関するセキュリティ対策技術、情報家電・スマートグリッド等における情報セキュリティ対策技術及びアクセス制御技術に関して、対症療法的ではなく抜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実施しているところ。
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	・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」、「信頼性」等を向上させる計９件の技術開発について、実施しているところ。2010年度の成果については、報告書に取りまとめ公表済み。 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、報告書にまとめた。

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

（4）技術戦略の推進等

② 情報セキュリティ人材の育成

該当項目	施策名	担当省庁	進捗状況
ア）ａ）	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	・各府省庁における監査計画の作成に先立ち各府省庁担当者を対象とする説明会を実施し、監査の目的、監査人に求められる資質、監査技法等について周知しているところ。 ・各府省庁に対し、監査責任者向け教育教材の雛型を作成・配付済み。
ア）ｂ）	情報セキュリティ専門家等の育成の促進		・経済産業省において、2010年2月に欧州の評価機関の評価要員を招聘し、チップハードウェアセキュリティ評価手法関連の講習会を行なった。
イ）ａ）	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	・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の強化を推進。
イ）ｂ）	情報セキュリティ人材育成に係る枠組みの検討		・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の広報・普及を推進。
イ）ｃ）	情報セキュリティ人材育成に係る枠組みの検討		・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。
イ）ｄ）	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	・アジアでの更なるセキュリティ人材の育成を含めた高度IT人材育成を図るため、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取組を拡大するとともに、我が国のITスキル標準を普及。
ウ）ａ）	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	・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促進。
ウ）ｂ）	情報セキュリティ資格の周知		・情報セキュリティ人材の育成に関するシンポジウム等において、民間のセキュリティ資格についての周知を実施。
エ）ａ）	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	・2007年度に、世界一安心できるIT社会の実現を担う、情報セキュリティ分野における世界最高水準の人材を育成するための教育拠点として２拠点を選定。 ・2008年度より、それぞれの拠点において実際に学生の受入れが開始され、先進的な教育プログラムの開発・実施が進められた。2008年度には２拠点で計70名がプログラムを修了した。
エ）ｂ）	先導的ITスペシャリスト育成プログラム		・先導的ITスペシャリスト育成プログラムにおける各拠点において得られた教材等の成果を効果的・効率的に普及展開していくため、2008年度より「拠点間教材等洗練事業」を開始。 ・2009年度には映像教材ポータルサイト「edubase Portal」を構築し、2010年３月から一般公開を実施。 ・2010年度には先導的ITスペシャリスト育成プログラムで実施されているPBL（プロジェクト・ベースト・ラーニング）に関するノウハウの普及を目的としたワークショップや、先導的ITスペシャリスト育成プログラムの成果の普及等を目的としたシンポジウムを開催。
オ）	途上国向け研修・セミナー等の開催	総務省	再掲
カ）	情報セキュリティ・サポーターの育成・活用	総務省	再掲
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を実施。 2011年６月を目途に工程表を取りまとめ、公表する予定。

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

（4）技術戦略の推進等

③ 情報セキュリティガバナンスの確立

該当項目	施策名	担当省庁	進捗状況
ア）ａ）	情報セキュリティガバナンス確立の促進	経済産業省	・国際連携や海外展開の方向を検討するため、米国、欧州、韓国、豪州における情報セキュリティガバナンスの動向を調査した。また、2009年度に策定した「情報セキュリティガバナンス導入ガイダンス」に新たな課題に対応した検討結果を盛り込んだ補足資料を作成した。現在、普及促進を図るとともに、国際標準化へ向けた対策を実施しているところ。
ア）ｂ）	情報セキュリティガバナンス確立の促進		・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、報告書をまとめた。
ア）ｃ）	情報セキュリティガバナンス確立の促進		・ホームページを通じ、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。
ア）ｄ）	情報セキュリティガバナンス確立の促進		・IPAを通じセキュリティプログラミングキャンプ等、セキュリティ人材を含めた人材育成を促
イ）ａ）	企業における情報セキュリティ対策の支援	経済産業省	・民間企業の情報処理の実態を把握するため、「平成22年情報処理実態調査」を2010年11月から実施した。
イ）ｂ）	企業における情報セキュリティ対策の支援		・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した。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、報告書をまとめた。また、東京（10月６日）、愛知（11月18日、１月13日）、韓国（１月20日）において、情報セキュリティ監査制度の普及・啓発、及びクラウドセキュリティ監査の活用をテーマにしたセミナー、シンポジウムを開催した。
イ）ｃ）	企業における情報セキュリティ対策の支援		・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、個別企業への紹介等を通じ、情報セキュリティ報告書の普及に努めた。
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	・ホームページを通じ情報システムの信頼性向上の観点から、ユーザー・ベンダー間の取引の可視化・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・ベンダー双方の関係業界団体と連携して普及活動を推進。

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

（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

該当項目	施策名	担当省庁	進捗状況
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るとともに、サイバー犯罪条約を締結するため、「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案」の立案を進め、2011年３月11日、同法律案の国会提出について閣議決定に至った（同年４月１日提出済み）。
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	・内閣官房において、2010年度に情報セキュリティや個人情報保護の専門家を集め、従来の情報セキュリティ政策にとらわれず幅広い観点から検討（サイバー空間の安全性・信頼性向上のための課題等に関する検討会）を行い、海外動向等も踏まえながら、主に制度的な観点から今後我が国で対応が求められる課題について論点整理を行い、2011年３月25日に報告書を取りまとめた。
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	・民間団体において、「データセンターの安全・信頼性に係る情報開示指針」を踏まえ、クラウド技術の進展も勘案しつつ、クラウド時代に適した情報開示認定制度の創設に向けた検討を実施。
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」について、2011年３月現在、127件を認定。
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
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 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

（5）情報セキュリティに関する制度整備

② 各国の情報セキュリティ制度の比較検討

該当項目	施策名	担当省庁	進捗状況
ア）	各国のセキュリティ法制度の調査	内閣官房	・アジア諸国をはじめとする各国の法制度に関する整理を行った。マルウェア作成に関する主要国の法律概要については、その成果をNISCのウェブページに公開した。

別添２　各情報セキュリティ政策領域における評価に当たり考慮すべき現状

２（１）② 重要インフラの基盤強化

- **重要インフラ事業者等の取組の検証**

	2010 年度	2009 年度
検証レベルを逸脱した IT 障害の件数	167	37

- **安全基準等の整備及び浸透状況**

	2010 年度	2009 年度
事業者における基準・内規の制定率	95%	91%

- **情報共有体制の強化**

	2010 年度	2009 年度
NISC が発信した情報件数	49	13
重要インフラ所管省庁を通じて連絡のあった重要インフラの IT 障害件数	174	128

- **共通脅威分析**

	2010 年度	2009 年度
分析内容が情報セキュリティ対策に役立ったと回答した事業者等	65%	―

- **分野横断的演習**

	2010 年度	2009 年度
参加規模	38 組織 141 人	34 組織 116 人
有意義と回答した事業者等	80%	82%

- **環境変化への対応**

	2010年度	2009年度
重要インフラにおける情報セキュリティ政策を紹介したセミナー等の回数	6	6
セプターカウンシルや分野横断的演習等の関係主体間のコミュニケーション機会の回数	8	7

２（１）③ その他の基盤強化

● インシデント報告関連件数

（JPCERT/CC インシデント報告対応レポート：JPCERT/CC）

	2010 年度	2009 年度
報告件数	9,865	10,751
インシデント件数	10,467	9,944
調整件数	2,875	2,820

● 安全なサーバ数[1]

（ICT 基盤に関する国際比較調査：総務省）

	平成 22 年	平成 21 年
日本	48.4	48.0
韓国	57.1	51.1
中国	37.4	35.3
シンガポール	―	46.7
台湾	46.3	44.8
イタリア	39.7	37.6
カナダ	58.3	61.1
オーストリア	49.1	48.0
オランダ	67.5	60.1
フィンランド	54.4	52.6
スイス	61.1	61.1
オーストラリア	63.1	61.0
フランス	41.8	39.8
米国	63.6	69.0
ニュージーランド	59.9	61.6
ポルトガル	40.3	38.1
イギリス	56.6	59.3
香港	―	43.0
ドイツ	51.0	49.9
スペイン	41.4	39.8
ベルギー	44.0	41.4
デンマーク	62.2	60.9
スウェーデン	55.6	54.4
インド	37.4	35.3
ブラジル	37.9	―
ロシア	37.6	―
南アフリカ	38.2	―

[1] 偏差値。100 万人当たりの暗号化通信をブラウザとの間で行えるサーバの数。

● コンピュータウイルス届出状況

（情報処理推進機構）

	2010 年度	2009 年度
届出（件）	12,903	15,469

● コンピュータ不正アクセス届出状況

（情報処理推進機構）

		2010 年度	2009 年度
届出（件）		159	176
	被害あり	98	112
	被害なし	61	64
相談（件）		536	490
	被害あり	196	193
	被害なし	340	297
合計（件）		695	666
	被害あり	294	305
	被害なし	401	361

● 脆弱性関連情報の届出状況

（情報処理推進機構）

		2010 年度	2009 年度
合計（件）		423	921
	ソフトウェア製品	115	138
	ウェブサイト	308	783

● SaaS 利用に伴う外部への支払い費用（年間事業収入規模別）

（情報処理実態調査：経済産業省）

	平成 21 年度[2]			平成 20 年度[3]		
	回答社数	発生した	発生しなかった	回答社数	発生した	発生しなかった
合計（社）	4,815	405	4,410	4,480	320	4,160
～１億円以下	22	1	21	12	1	11
１億円超～５億円以下	82	5	77	67	3	64
５億円超～10 億円以下	218	8	210	204	10	194
10 億円超～20 億円以下	538	20	518	458	23	435
20 億円超～100 億円以下	1,782	144	1,638	1,559	93	1,466
100 億円超～1,000 億円以下	1,447	124	1,323	1,506	104	1,402
1,000 億円超～	421	70	351	530	69	461
不明	305	33	272	144	17	127

● SaaS 導入・利用時の SLA 締結状況（年間事業収入規模別）

（情報処理実態調査：経済産業省）

	平成 21 年度[2]			平成 20 年度[3]		
	回答社数	締結した	締結していない	回答社数	締結した	締結していない
合計（社）	383	165	218	299	131	168
～１億円以下	1	―	1	―	―	―
１億円超～５億円以下	4	2	2	3	―	3
５億円超～10 億円以下	8	5	3	10	4	6
10 億円超～20 億円以下	14	4	10	21	11	10
20 億円超～100 億円以下	141	49	92	92	41	51
100 億円超～1,000 億円以下	121	55	66	95	42	53
1,000 億円超～	65	40	25	63	28	35
不明	29	10	19	15	5	10

[2] 平成 20 年度実施調査（平成 21 年度公表）。
[3] 平成 19 年度実施調査（平成 20 年度公表）。

● クラウドサービスの利用状況

（通信利用動向調査：総務省）

クラウドサービスの利用状況

	平成 22 年末
集計企業数	2,119
利用している	13.7%
全社的に利用している	4.1%
一部の事業所又は部門で利用している	9.7%
利用していない	58.4%
利用していないが、今後利用する予定がある	21.3%
利用していないし、今後も利用する予定もない	37.0%
クラウドサービスについてよく分からない	25.3%
無回答	2.6%

クラウドサービスの利用効果の有無

	平成 22 年末
集計企業数	300
非常に効果があった	18.1%
ある程度効果があった	61.8%
あまり効果がなかった	5.6%
マイナスの効果であった	―
効果はよく分からない	14.5%
無回答	―

● クラウドサービスを利用しない理由

（通信利用動向調査：総務省）

	平成 22 年末
集計企業数	790
クラウドの導入に伴う既存システムの改修コストが大きい	36.4%
クラウドの導入によって自社コンプライアンスに支障をきたす	8.3%
通信費用がかさむ	10.5%
ニーズに応じたアプリケーションのカスタマイズができない	26.2%
ネットワークの安定性に対する不安がある	19.7%
セキュリティに不安がある	37.9%
その他	29.2%
無回答	2.2%

● **ASP・SaaS の利用状況**

（通信利用動向調査：総務省）

	平成 21 年末
回答数	1,834
利用しており、非常に効果があった	4.2%
利用しており、ある程度効果があった	11.5%
利用しているが、あまり効果がなかった	0.7%
利用しているが、効果はよく分からない	3.6%
利用していないが、今後利用する予定	18.6%
利用していないし、今後も利用する予定はない	28.4%
ASP、SaaS についてよく分からない	30.6%
無回答	2.4%

● **IPA 中小企業情報セキュリティセミナー**

（情報処理推進機構）

	2010 年度	2009 年度
開催地数	36	35
開催回数	106	113
開催内容	４種類 ・マネジメントコース入門編Ⅰ ・マネジメントコース入門編Ⅱ ・技術コース標準編Ⅰ ・技術コース標準編Ⅱ	４種類 ・マネジメント（入門編） ・マネジメント（実践編） ・技術（標準編） ・技術（専門編）

● **BtoB EC（企業間電子商取引）市場規模について**

（我が国情報経済社会における基盤整備：経済産業省）

	2009 年	2008 年
広義市場規模[4]（兆）	205	250
狭義市場規模[5]（兆）	131	159
EC 化率[6]	13.7%	13.5%

[4] 「コンピュータ・ネットワーク・システムを介して商取引が行われ、かつその成約金額が捕捉されるもの」。ここで商取引行為とは、「経済主体間での財の商業的移転に関わる、受発注者間の物品、サービス、情報、金銭の交換」をさす。狭義の EC に加え、VAN・専用線等、TCP/IP プロトコルを利用していない従来型 EDI（例．全銀手順、EIAJ 手順などを用いたもの）が含まれる。

[5] 「インターネット技術を用いたコンピュータ・ネットワーク・システムを介して商取引が行われ、かつその成約金額が捕捉されるもの」。ここで商取引行為とは、「経済主体間での財の商業的移転に関わる、受発注者間の物品、サービス、情報、金銭の交換」をさす。「インターネット技術」とは、TCP/IP プロトコルを利用した技術を指しており、公衆回線上のインターネットの他、エクストラネット、インターネット VPN、IP-VPN 等が含まれる。

[6] 全ての商取引における、電子商取引（EC）による取引の割合。

● **BtoC EC（消費者向け電子商取引）市場規模について**

（我が国情報経済社会における基盤整備：経済産業省）

	2009 年	2008 年
市場規模（兆）	6.7	6.1
EC 化率[6]	2.1%	1.8%

● **ISMS 認証取得組織数**

（日本情報経済社会推進協会）

	平成 22 年度	平成 21 年度
組織数	3,787	3,553

● **ITSMS 認証取得組織数**

（日本情報経済社会推進協会）

	平成 22 年度	平成 21 年度
組織数	149	130

● **Number of Certificates Per Country**

（ISMS International User Group）

	2011 年４月		2010 年３月	
	順位	取得数	順位	取得数
日本	1	3,790	1	3,480
インド	2	516	2	495
中国	3	495	5	347
イギリス	4	460	3	444
台湾	5	410	4	385
ドイツ	6	154	6	136
韓国	7	106	7	106
チェコ	8	101	9	85
米国	9	99	8	95
ハンガリー	10	72	10	70

● 情報セキュリティの対策状況（事業継続計画（BCP）の作成）

（情報処理実態調査：経済産業省）

対策実施状況

	平成 21 年度[7]		平成 20 年度[8]	
	回答数	割合	回答数	割合
回答企業数	4,404	―	4,134	―
既に実施している	806	18.3%	648	15.7%
トラブルがあったので対策を講じた	7	0.2%	11	0.3%
実施を検討している	612	13.9%	615	14.9%
必要性を感じるが、未実施	2,167	49.2%	2,105	50.9%
必要性を感じず、未実施	819	18.6%	766	18.5%

セキュリティ向上への寄与

	平成 21 年度[7]		平成 20 年度[8]	
	回答数	割合	回答数	割合
回答企業数	1,053	―	949	―
寄与した	626	59.4%	569	60.0%
寄与しなかった	44	4.2%	26	2.7%
わからない	383	36.4%	354	37.3%

● 情報セキュリティ対策のセキュリティ向上以外の効果

（情報処理実態調査：経済産業省）

	平成 21 年度[7]		平成 20 年度[8]	
	回答数	割合	回答数	割合
回答企業数	3,453	―	3,090	―
顧客・取引先からの評価の上昇	803	23.3%	791	25.6%
市場や投資家からの評価の上昇	97	2.8%	111	3.6%
製品やサービスの質の向上	290	8.4%	303	9.8%
業務効率や生産性の向上	492	14.2%	408	13.2%
特に効果はなかった	1,465	42.4%	1,218	39.4%
その他	771	22.3%	721	23.3%

[7] 平成 20 年度実施調査（平成 21 年度公表）。

[8] 平成 19 年度実施調査（平成 20 年度公表）。

● 情報セキュリティ対策の阻害要因

（情報処理実態調査：経済産業省）

	平成 21 年度[7]		平成 20 年度[8]	
	回答数	割合	回答数	割合
回答企業数	4,755	―	4,404	―
実施する知識・ノウハウがない	1,194	25.1%	987	22.4%
手間・コストがかかる	3,067	64.5%	2,935	66.6%
予算がとれない	1,266	26.6%	1,098	24.9%
必要性や効果がわからない	496	10.4%	380	8.6%
対策をどこまでやるべきかがわからない	1,938	40.8%	1,816	41.2%
情報セキュリティガバナンスが確立されていない	739	15.5%	632	14.4%
トップの理解・協力が得られない	355	7.5%	294	6.7%
従業員の理解・協力が得られない	538	11.3%	496	11.3%
企業のセキュリティ対策方針が明確になっていない	835	17.6%	746	16.9%
専門家（CIO や CISO）がいない	810	17.0%	668	15.2%
その他	120	2.5%	135	3.1%
問題はない	512	10.8%	386	8.8%

● 情報セキュリティの対策状況（リスク分析）

（情報処理実態調査：経済産業省）

対策実施状況

	平成 21 年度[7]		平成 20 年度[8]	
	回答数	割合	回答数	割合
回答企業数	4,448	―	4,201	―
既に実施している	1,503	33.8%	1,413	33.6%
トラブルがあったので対策を講じた	37	0.8%	44	1.0%
実施を検討している	371	8.3%	412	9.8%
必要性を感じるが、未実施	2,040	45.9%	1,906	45.4%
必要性を感じず、未実施	534	12.0%	470	11.2%

セキュリティ向上への寄与

	平成 21 年度[7]		平成 20 年度[8]	
	回答数	割合	回答数	割合
回答企業数	1,490	―	1,482	―
寄与した	1,140	76.5%	1,102	74.4%
寄与しなかった	27	1.8%	33	2.2%
わからない	323	21.7%	347	23.4%

● 情報セキュリティの対策状況（セキュリティポリシーの策定）

（情報処理実態調査：経済産業省）

対策実施状況

	平成 21 年度[9]		平成 20 年度[10]	
	回答数	割合	回答数	割合
回答企業数	4,509	―	4,246	―
既に実施している	2,222	49.3%	2,078	48.9%
トラブルがあったので対策を講じた	52	1.2%	44	1.0%
実施を検討している	428	9.5%	453	10.7%
必要性を感じるが、未実施	1,463	32.4%	1,368	32.2%
必要性を感じず、未実施	396	8.8%	347	8.2%

セキュリティ向上への寄与

	平成 21 年度[9]		平成 20 年度[10]	
	回答数	割合	回答数	割合
回答企業数	2,140	―	2,102	―
寄与した	1,618	75.6%	1,552	73.8%
寄与しなかった	45	2.1%	49	2.3%
わからない	477	22.3%	501	23.8%

● 情報セキュリティの対策状況（情報セキュリティ報告書の作成）

（情報処理実態調査：経済産業省）

対策実施状況

	平成 21 年度[9]		平成 20 年度[10]	
	回答数	割合	回答数	割合
回答企業数	4,457	―	4,181	―
既に実施している	709	15.9%	631	15.1%
トラブルがあったので対策を講じた	18	0.4%	14	0.3%
実施を検討している	367	8.2%	425	10.2%
必要性を感じるが、未実施	2,336	52.4%	2,220	53.1%
必要性を感じず、未実施	1,045	23.4%	905	21.6%

セキュリティ向上への寄与

	平成 21 年度[9]		平成 20 年度[10]	
	回答数	割合	回答数	割合
回答企業数	807	―	823	―
寄与した	519	64.3%	506	61.5%
寄与しなかった	28	3.5%	28	3.4%
わからない	260	32.2%	289	35.1%

9 平成 20 年度実施調査（平成 21 年度公表）。

10 平成 19 年度実施調査（平成 20 年度公表）。

● 情報セキュリティの対策状況（全体的なセキュリティ管理者の配置）

（情報処理実態調査：経済産業省）

対策実施状況

	平成 21 年度[9]		平成 20 年度[10]	
	回答数	割合	回答数	割合
回答企業数	4,524	―	4,247	―
既に実施している	2,167	47.9%	2,029	47.8%
トラブルがあったので対策を講じた	53	1.2%	45	1.1%
実施を検討している	327	7.2%	373	8.8%
必要性を感じるが、未実施	1,630	36.0%	1,487	35.0%
必要性を感じず、未実施	400	8.8%	358	8.4%

セキュリティ向上への寄与

	平成 21 年度[9]		平成 20 年度[10]	
	回答数	割合	回答数	割合
回答企業数	2,008	―	1,970	―
寄与した	1,559	77.6%	1,525	77.4%
寄与しなかった	46	2.3%	41	2.1%
わからない	403	20.1%	404	20.5%

● 情報セキュリティの対策状況（部門ごとのセキュリティ管理者の配置）

（情報処理実態調査：経済産業省）

対策実施状況

	平成 21 年度[9]		平成 20 年度[10]	
	回答数	割合	回答数	割合
回答企業数	4,492	―	4,230	―
既に実施している	1,555	34.6%	1,452	34.3%
トラブルがあったので対策を講じた	40	0.9%	29	0.7%
実施を検討している	347	7.7%	397	9.4%
必要性を感じるが、未実施	1,836	40.9%	1,732	40.9%
必要性を感じず、未実施	754	16.8%	649	15.3%

セキュリティ向上への寄与

	平成 21 年度[9]		平成 20 年度[10]	
	回答数	割合	回答数	割合
回答企業数	1,533	―	1,519	―
寄与した	1,152	75.1%	1,152	75.8%
寄与しなかった	50	3.3%	43	2.8%
わからない	331	21.6%	324	21.3%

● 情報セキュリティの対策状況（内部統制の整備強化）

（情報処理実態調査：経済産業省）

対策実施状況

	平成 21 年度[11]		平成 20 年度[12]	
	回答数	割合	回答数	割合
回答企業数	4,503	―	4,222	―
既に実施している	1,739	38.6%	1,566	37.1%
トラブルがあったので対策を講じた	31	0.7%	31	0.7%
実施を検討している	614	13.6%	741	17.6%
必要性を感じるが、未実施	1,733	38.5%	1,553	36.8%
必要性を感じず、未実施	417	9.3%	362	8.6%

セキュリティ向上への寄与

	平成 21 年度 [11]		平成 20 年度 [12]	
	回答数	割合	回答数	割合
回答企業数	1,836	―	1,814	―
寄与した	1,311	71.4%	1,264	69.7%
寄与しなかった	37	2.0%	47	2.6%
わからない	488	26.6%	503	27.7%

● 情報セキュリティの対策状況（ISO/IEC15408 認証取得製品の導入）

（情報処理実態調査：経済産業省）

対策実施状況

	平成 21 年度 [11]		平成 20 年度 [12]	
	回答数	割合	回答数	割合
回答企業数	4,359	―	4,076	―
既に実施している	354	8.1%	362	8.9%
トラブルがあったので対策を講じた	1	―	2	―
実施を検討している	187	4.3%	198	4.9%
必要性を感じるが、未実施	1,617	37.1%	1,573	38.6%
必要性を感じず、未実施	2,201	50.5%	1,943	47.7%

セキュリティ向上への寄与

	平成 21 年度 [11]		平成 20 年度 [12]	
	回答数	割合	回答数	割合
回答企業数	396	―	439	―
寄与した	248	62.6%	254	57.9%
寄与しなかった	10	2.5%	16	3.6%
わからない	138	34.8%	169	38.5%

[11] 平成 20 年度実施調査（平成 21 年度公表）。
[12] 平成 19 年度実施調査（平成 20 年度公表）。

● セキュリティ対策ソフト導入状況

（国内における情報セキュリティ事象被害状況調査：情報処理推進機構）

ネットワークサーバ

	平成 21 年	平成 20 年
回答数	1,658	1,907
９割以上に導入済	84.1%	84.6%
半数に導入済	2.9%	2.5%
半数未満に導入済	2.8%	2.3%
導入していない	5.4%	7.9%
無回答	4.7%	2.7%

ローカルサーバ

	平成 21 年	平成 20 年
回答数	1,658	1,907
９割以上に導入済	76.1%	76.5%
半数に導入済	4.8%	4.9%
半数未満に導入済	3.7%	3.7%
導入していない	9.7%	12.2%
無回答	5.6%	2.8%

各自クライアント（パソコン）

	平成 21 年	平成 20 年
回答数	1,658	1,907
９割以上に導入済	87.4%	89.0%
半数に導入済	4.6%	4.1%
半数未満に導入済	3.6%	3.6%
導入していない	1.9%	2.2%
無回答	2.5%	1.0%

● ISO/IEC15408 に関する意識・実態

（情報セキュリティ製品の調達等に関する意識調査：情報処理推進機構）

ISO/IEC15408（CC：コモンクライテリア）の認知度

	2010 年度
回答数	545
内容を含めよく知っている	2.6%
イメージはだいたい知っている	11.0%
名前だけ知っている	16.0%
知らない	70.5%

ISO/IEC15408（CC：コモンクライテリア）認証製品の利用実績

	2010 年度
回答数	161
利用（調達）したことがある	5.0%
実績はないが、関心がある	58.4%
実績がなく、関心もない	26.1%
わからない	10.6%

● CC に係る税制についての意識

（情報セキュリティ製品の調達等に関する意識調査：情報処理推進機構）

情報基盤強化税制または中小企業等基盤強化税制の認知度

	2010 年度
回答数	545
活用したことがある	1.7%
活用したことはないが、内容は知っている	10.3%
名前だけ知っている	20.0%
知らない	68.1%

中小企業等基盤強化税制の対象製品の今後の利用意向

	2010 年度
回答数	545
利用したいと思う	79.6%
利用したいと思わない	20.4%

● 情報セキュリティの対策状況（外部専門家による定期的な情報セキュリティ監査）

（情報処理実態調査：経済産業省）

対策実施状況

	平成 21 年度[13]		平成 20 年度[14]	
	回答数	割合	回答数	割合
回答企業数	4,456	―	4,166	―
既に実施している	634	14.2%	581	13.9%
トラブルがあったので対策を講じた	4	0.1%	7	0.2%
実施を検討している	155	3.5%	165	4.0%
必要性を感じるが、未実施	1,782	40.0%	1,807	43.4%
必要性を感じず、未実施	1,885	42.3%	1,613	38.7%

セキュリティ向上への寄与

	平成 21 年度 [13]		平成 20 年度 [14]	
	回答数	割合	回答数	割合
回答企業数	600	―	591	―
寄与した	512	85.3%	486	82.2%
寄与しなかった	11	1.8%	8	1.4%
わからない	77	12.8%	97	16.4%

[13] 平成 20 年度実施調査（平成 21 年度公表）。
[14] 平成 19 年度実施調査（平成 20 年度公表）。

● 情報セキュリティの対策状況（内部による定期的な情報セキュリティ監査）

（情報処理実態調査：経済産業省）

対策実施状況

	平成 21 年度[13]		平成 20 年度[14]	
	回答数	割合	回答数	割合
回答企業数	4,476	―	4,197	―
既に実施している	1,197	26.7%	1,107	26.4%
トラブルがあったので対策を講じた	10	0.2%	8	0.2%
実施を検討している	331	7.4%	401	9.6%
必要性を感じるが、未実施	1,991	44.5%	1,863	44.4%
必要性を感じず、未実施	957	21.4%	823	19.6%

セキュリティ向上への寄与

	平成 21 年度[13]		平成 20 年度[14]	
	回答数	割合	回答数	割合
回答企業数	1,173	―	1,197	―
寄与した	975	83.1%	954	79.7%
寄与しなかった	20	1.7%	26	2.2%
わからない	178	15.2%	217	18.1%

2（2）① 普及・啓発活動の充実・強化

● インターネット利用上の不安の有無

（通信利用動向調査：総務省）

	平成 22 年末	平成 21 年末
回答数	20,283	4,230
特に不安は感じない	17.9%	20.2%
対策を行っているのでそれほど不安を感じない	26.0%	31.5%
対策を行っているが少し不安を感じる	23.7%	28.7%
不安を感じる	13.8%	14.0%
無回答	18.7%	5.6%

● インターネット利用上で感じる不安の内容

（通信利用動向調査：総務省）

	平成 22 年末	平成 21 年末
回答数	6,986	1,795
ウィルスの感染が心配である	69.6%	70.6%
個人情報の保護に不安がある	71.6%	69.9%
どこまでセキュリティ対策を行えばよいか不明	61.9%	58.6%
電子的決済手段の信頼性に不安がある	42.4%	40.4%
セキュリティ脅威が難解で具体的に理解できない	38.4%	33.3%
違法・有害情報が氾濫している	29.3%	32.5%
認証技術の信頼性に不安がある	17.3%	15.4%
知的財産の保護に不安がある	8.0%	7.8%
送信した電子メールが届くかどうかわからない	6.9%	6.9%
その他	2.0%	2.1%
無回答	0.2%	0.2%

● インターネットを利用しない理由

（通信利用動向調査：総務省）

	平成 22 年末	平成 21 年末
回答数	22,271	4,547
通信料金が高い	34.1%	35.6%
特に不満はない	20.3%	27.4%
パソコンなどの機器が高価すぎる	19.9%	24.8%
接続速度が遅い	18.8%	23.2%
パソコンなどの機器の操作が難しい	17.4%	18.8%
情報検索に手間がかかる	7.8%	10.5%
インターネットについてよく知らない	10.6%	8.4%
利用する必要がない	12.0%	7.4%
必要な情報がない	2.4%	2.3%
その他	3.3%	3.8%
無回答	12.0%	10.4%

● 情報セキュリティトラブルの重要性に対する認識

（情報処理実態調査：経済産業省）

	平成 21 年度[15]				平成 20 年度[16]			
	非常に重要である	どちらかといえば重要である	重要ではない	わからない	非常に重要である	どちらかといえば重要である	重要ではない	わからない
システムの停止								
内部要因によるシステムの停止	86.2%	11.9%	0.8%	1.1%	87.2%	10.9%	0.7%	1.2%
外部要因（地震、火災等の問題）によるシステムの停止	75.9%	21.3%	1.3%	1.5%	77.7%	19.6%	1.2%	1.5%
その他システムトラブル								
DoS 攻撃	53.1%	34.6%	5.4%	6.9%	53.6%	33.2%	5.3%	7.9%
スパムメールの中継利用等	53.9%	35.0%	5.1%	6.0%	53.7%	34.4%	5.1%	6.8%
ホームページやファイル、データの改ざん	65.3%	27.5%	3.6%	3.5%	66.6%	26.6%	3.2%	3.5%
不正アクセス								
IP・メールアドレス詐称	61.8%	30.8%	3.8%	3.6%	63.4%	29.0%	4.0%	3.6%
リソースの不正使用	59.5%	31.6%	3.9%	5.0%	60.5%	30.7%	3.7%	5.1%
内部関係者による不正アクセス	72.1%	22.7%	2.3%	2.9%	72.8%	22.1%	2.2%	2.8%
コンピュータウイルス								
ウィルスなどの感染	76.9%	21.1%	0.9%	1.1%	78.2%	19.8%	0.8%	1.2%
トロイの木馬	72.0%	24.1%	1.3%	2.5%	72.6%	23.3%	1.3%	2.8%
重要情報の漏えい								
コンピュータウィルス、ファイル共有ソフトに起因する情報漏えい	85.9%	11.9%	0.9%	1.3%	87.6%	10.2%	0.8%	1.3%
不正アクセスによる情報漏えい	83.7%	13.5%	1.5%	1.3%	85.1%	12.2%	1.2%	1.5%
内部者による情報漏えい	86.1%	11.6%	1.2%	1.1%	87.2%	10.7%	0.8%	1.4%
委託先による情報漏えい	79.8%	15.3%	2.6%	2.3%	80.8%	14.6%	2.1%	2.6%
ノートパソコン及び携帯記憶媒体等の盗難・紛失	78.1%	18.9%	1.8%	1.3%	79.1%	17.6%	1.8%	1.5%
その他								
ホームページ上での誹謗中傷等	44.1%	41.6%	9.3%	4.9%	43.4%	42.5%	9.3%	4.7%
その他	27.1%	29.0%	8.4%	35.5%	26.6%	29.7%	9.4%	34.3%

15 平成 20 年度実施調査（平成 21 年度公表）。

16 平成 19 年度実施調査（平成 20 年度公表）。

● 情報セキュリティに関する攻撃・脅威の認知

（情報セキュリティの脅威に対する意識調査：情報処理推進機構）

	2010 年度	2009 年度
回答数	5,019	5,019
フィッシング詐欺	91.8%	93.7%
ワンクリック不正請求	92.9%	94.4%
スパイウェア	84.5%	88.3%
セキュリティホール（脆弱性）	72.9%	76.9%
標的型攻撃	41.2%	43.7%
ボット	38.9%	39.0%
マルウェア	36.9%	36.6%
偽セキュリティ対策ソフト	49.9%	49.1%

● セキュリティに関する現在の情報源と望ましい情報源

（情報セキュリティの脅威に対する意識調査：情報処理推進機構）

	2010 年度			2009 年度		
	利用あり	利用なし・意向あり	利用なし・意向なし	利用あり	利用なし・意向あり	利用なし・意向なし
ポータルサイト（検索サイトやプロバイダのサイトなど）	52.5%	8.1%	39.4%	39.0%	7.7%	53.3%
ウェブ上のニュース	50.1%	7.1%	42.9%	50.8%	8.3%	40.9%
専門機関のウェブサイト	18.8%	10.4%	70.8%	19.5%	10.9%	69.5%
ブログ、掲示板等	17.4%	3.4%	79.2%	18.8%	3.6%	77.6%
Q&A サイト	16.5%	3.9%	79.7%	18.1%	4.5%	77.3%
mixi などの SNS 内コミュニティ	8.8%	3.8%	87.3%	8.3%	3.7%	88.0%
マイクロブログ（Twitter 等）	5.1%	3.5%	91.4%	—	—	—
メールマガジン、メーリングリスト	18.1%	4.2%	77.7%	20.5%	4.3%	75.2%
最新情報が自動的にデスクトップに表示（ウィジェット、RSS など）	6.3%	7.6%	86.1%	7.1%	7.7%	85.2%
テレビ CM	17.1%	7.3%	75.6%	14.4%	7.5%	78.1%
新聞	20.9%	7.4%	71.7%	18.8%	7.2%	73.9%
パソコン売場など量販店の店頭ポスター・チラシ	10.2%	7.1%	82.6%	11.4%	6.8%	81.8%
無料配布冊子	6.8%	7.7%	85.5%	7.0%	8.1%	84.9%
行政や業者による無料セミナー	3.9%	7.2%	88.9%	3.9%	7.7%	88.4%
その他	1.1%	1.0%	97.9%	1.3%	1.0%	97.7%

● 情報セキュリティ対策の必要性

（不正アクセス行為対策等の実態調査：警察庁）

	平成 22 年度	平成 21 年度
回答数	841	930
非常に感じている	72.8%	77.5%
ある程度感じている	23.8%	18.9%
あまり感じていない	1.3%	1.8%
感じていない	0.0%	0.0%
無回答	2.1%	1.7%

● 情報セキュリティに係る政府系ウェブサイトへのアクセス状況[17]

（内閣官房、警察庁、総務省、経済産業省）

府省庁等	サイト名	2010 年度評価	2009 年度評価
内閣官房	情報セキュリティセンター ホームページ	817,991 人[18]	566,834 人[18]
	国民を守る情報セキュリティサイト	140,776 人[19]	―
警察庁	サイバー犯罪対策	1,697,351 件[18]	509,902 件[18]
	@police	1,349,142 件[18]	2,242,578 件[18]
総務省	国民のための情報セキュリティサイト	138,869 件[20]	150,961 件[20]
経済産業省	情報セキュリティに関する政策・緊急情報	1,336,114 件[20]	293,856 件[20]
	CHECK PC! ホームページ	4,779,915 件[20]	6,784,919 件[21]
	Japan Vulnerability Notes (JVN)	5,248,580 件[20]	5,697,482 件[20]
情報処理推進機構	IPA セキュリティセンター ホームページ	21,429,665 件[20]	27,960,232 件[20]
JPCERT/CC	JPCERT/CC ホームページ	11,275,459 件[20]	7,783,354 件[20]

● 情報セキュリティサポータをとりまとめる地域団体の数

（セキュリティ対策推進協議会：総務省）

	平成 22 年３月末
地域団体数	26

[17] 各ウェブサイトへのアクセス概数。集計方法については、各府省庁及び各ウェブサイトによって異なるため、一概に単純比較することはできない。

[18] 年による集計。

[19] 平成 23 年２月１日から３月 31 日までの集計。

[20] 年度による集計。

[21] 平成 21 年５月 29 日から３月 31 日までの集計。

● 情報セキュリティ安心相談窓口における相談対応状況

（情報処理推進機構）

	2010 年度	2009 年度
合計（件）	22,389	22,581
自動応答システム	12,834	12,717
電話	8,633	9,107
電子メール	877	715
その他	45	42

● 被害・トラブル時に対処をしなかった理由

（情報セキュリティの脅威に対する意識調査：情報処理推進機構）

	2010 年度	2009 年度
回答数	379	464
対処の必要性を感じなかった	51.2%	54.5%
何をしてよいかわからなかった	36.4%	36.2%
面倒だった	18.2%	15.5%
その他	5.3%	4.7%

● 知りたいセキュリティ情報

（情報セキュリティの脅威に対する意識調査：情報処理推進機構）

	2010 年度	2009 年度
回答数	5,019	5,019
被害を防ぐための予防策や被害が生じた場合の対応策などの具体的事例に関する情報	38.8%	36.5%
最新のセキュリティ事象やセキュリティに関する被害の情報	34.7%	31.2%
被害が起きたときの相談や届出に関する情報	27.4%	27.3%
市販されているセキュリティサービス・製品に関する情報	22.4%	22.3%
ユーザの被害や対策実施等に関する体験談やレポートの情報	16.9%	17.5%
その他	0.2%	0.5%
特にない	37.7%	39.6%

２（２）② 個人情報保護の推進

● 「個人情報の保護に関する 27 分野 40 のガイドライン」について見直しされた件数[22]

（消費者庁）

	所管省庁	ガイドラインの名称	該当箇所
1	総務省	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（告示）	（漏えい等が発生した場合の対応） 第２２条 電気通信事業者は、個人情報の漏えいが発生した場合は、速やかに、当該漏えいに係る事実関係を本人に通知するものとする。ただし、当該個人情報の漏えいがノートブック型パーソナルコンピュータ等の紛失又は盗難により発生したものであって、かつ、本人に対して二次被害が生じないよう適切な技術的保護措置が講じられているときは、この限りでない。
2	経済産業省	個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（告示）	Ｐ．28（エ）影響を受ける可能性のある本人への連絡 事故又は違反について本人へ謝罪し、二次被害を防止するために、可能な限り本人へ連絡することが望ましい。 ただし、例えば、以下のように、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には、本人への連絡を省略しても構わないものと考えられる。 ・高度な暗号化等の秘匿化が施されている場合（ただし、（オ）に定める報告の際、高度な暗号化等の秘匿化として施していた措置内容を具体的に報告すること。） Ｐ．29（カ）事実関係、再発防止策等の公表 二次被害の防止、類似事案の発生回避等の観点から、個人データの漏えい等の事案が発生した場合は、可能な限り事実関係、再発防止策等を公表することが重要である。 ただし、例えば、以下のように、二次被害の防止の観点から公表の必要性がない場合には、事実関係等の公表を省略しても構わないものと考えられる。 ・高度な暗号化等の秘匿化が施されている場合（ただし、（オ）に定める報告の際、高度な暗号化等の秘匿化として施していた措置内容を具体的に報告すること。）

２（２）③ サイバー犯罪に対する態勢の強化

● 不正アクセス行為の認知件数

（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技術の研究開発の状況：警察庁）

	平成 22 年	平成 21 年
認知件数	1,885	2,795
海外からのアクセス	57	40
国内からのアクセス	1,755	2,673
アクセス元不明	73	82

[22] 「個人情報の保護に関する 27 分野 40 のガイドライン」の中で、適切な技術的措置が講じられているときは、求められる手続きの一部が緩和されることが明記されたものの件数。

● **サイバー犯罪の検挙状況**

（サイバー犯罪の検挙状況等について：警察庁）

	平成 22 年度	平成 21 年度
検挙件数	6,933	6,690
不正アクセス禁止法違反	1,601	2,534
コンピュータ・電磁的記録対象犯罪	133	195
ネットワーク利用犯罪	5,199	3,961

● **サイバー犯罪等に関する相談状況**

（サイバー犯罪の検挙状況等について：警察庁）

	平成 22 年度	平成 21 年度
相談件数	75,810	83,739
詐欺・悪徳商法	31,333	40,315
オークション	6,905	7,859
名誉棄損・誹謗中傷	10,212	11,557
不正アクセス・ウィルス	3,668	4,183
迷惑メール	9,836	6,538
違法、有害情報	3,847	3,785
その他	10,009	9,502

● **インターネット安全教室開催数**

（インターネット安全教室 実施報告書：日本ネットワークセキュリティ協会：経済産業省）

	2010 年度	2009 年度
開催数	167	154
参加人数	11,818	9,600

２（３）国際連携の強化

● **日・ASEAN 政府ネットワークセキュリティワークショップの開催状況**

	2010 年度	2009 年度
参加者人数	30	―
研修における自身の達成度[23]	4.59	―
業務遂行に必要な知識向上[23]	4.45	―

２（４）② 情報セキュリティ人材の育成

● **情報セキュリティサポータの人数**

（情報セキュリティ対策推進協議会：総務省）

	平成 22 年３月末
人数	561

[23] ５段階評価の平均値。

● e-ネットキャラバン開催状況

（総務省・文部科学省）

	平成 22 年度	平成 21 年度
申込件数	557	624
実施件数	557	624

● 情報セキュリティスペシャリスト試験合格者数

（情報処理推進機構）

	平成 22 年度	平成 21 年度
応募数	59,285	52,043
受験者数	39,342	34,074
合格者数	5,804	5,906
合格率	14.8%	17.3%

● システム監査技術者試験合格者数

（情報処理推進機構）

	平成 22 年度	平成 21 年度
応募数	5,415	5,313
受験者数	3,534	3,271
合格者数	506	455
合格率	14.3%	13.9%

● 教員の ICT 活用指導力の状況

（学校における教育の情報化の実態等に関する調査：文部科学省）

	平成 21 年度		平成 20 年度	
	回答	割合	回答	割合
児童が発信する情報や情報社会での行動に責任を持ち、相手のことを考えた情報のやりとりができるように指導する。	608,565	69.7%	581,327	67.7%
児童が情報社会の一員としてルールやマナーを守って、情報を集めたり発信したりできるように指導する。	618,542	70.8%	592,575	69.0%
児童がインターネットなどを利用する際に、情報の正しさや安全性などを理解し、健康面に気を付けて活用できるように指導する。	618,924	70.9%	595,004	69.3%
児童がパスワードや自他の情報の大切さなど、情報セキュリティの基本的な知識を身に着けることができるように指導する。	551,215	63.1%	526,583	61.3%

● 情報セキュリティ教育の実施状況

（不正アクセス行為対策等の実態調査：警察庁）

	平成 22 年	平成 21 年
回答数	814	930
実施している	63.9%	56.3%
実施を予定している	5.1%	6.2%
実施はしていないが必要性を感じる	28.5%	34.1%
実施の必要性を感じない（実施していない）	1.7%	2.5%
無回答	0.8%	0.9%

● 情報セキュリティの対策状況（従業員に対する情報セキュリティ教育）

（情報処理実態調査：経済産業省）

対策実施状況

	平成 21 年度[24]		平成 20 年度[25]	
	回答数	割合	回答数	割合
回答企業数	4,544	―	4,269	―
既に実施している	1,977	43.5%	1,879	44.0%
トラブルがあったので対策を講じた	109	2.4%	119	2.8%
実施を検討している	455	10.0%	507	11.9%
必要性を感じるが、未実施	1,830	40.3%	1,638	38.4%
必要性を感じず、未実施	282	6.2%	245	5.7%

セキュリティ向上への寄与

	平成 21 年度 [24]		平成 20 年度 [25]	
	回答数	割合	回答数	割合
回答企業数	1,946	―	1,939	―
寄与した	1,550	79.7%	1,527	78.8%
寄与しなかった	35	1.8%	32	1.7%
わからない	361	18.6%	380	19.6%

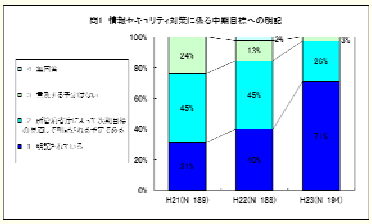
[24] 平成 20 年度実施調査（平成 21 年度公表）。
[25] 平成 19 年度実施調査（平成 20 年度公表）。

別添３　独立行政法人等の情報セキュリティ対策の現状について

対象機関：　独立行政法人、国立大学法人及び大学共同利用機関法人　（194法人）
調査時点：　平成23年3月末時点　　※前回調査は、平成22年2月末時点に188法人に実施。

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決定）
Ⅱ 具体的な取組
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
・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
【具体的施策】
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。

情報セキュリティ対策に係る中期目標への明記



中期目標への明記（明記予定）は増加。
一方で、明記の予定がない法人が3%存在。

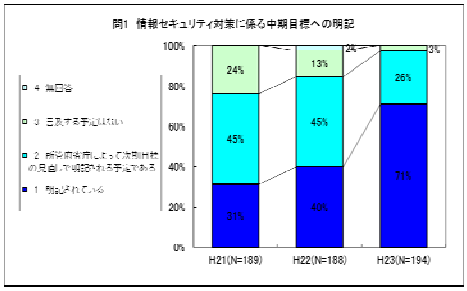
情報セキュリティ対策に係るPDCAサイクルの構築

項番	対策内容	状況	H22(率)	H23(率)	進捗
1	情報セキュリティポリシーの策定	策定している。	85%	90%	UP
2	情報セキュリティポリシーの見直し	実施している。	75%	81%	UP
3	情報セキュリティポリシーの遵守状況の把握	実施している。	74%	79%	UP
4	情報セキュリティ対策の中期目標への明記	実施している。	85%	90%	UP
5	CISOの設置	置いている。	83%	88%	UP
6	CISO補佐官の設置	置いている。	37%	46%	UP
7	統括組織の設置	置いている。	95%	97%	UP
8	注意喚起等に関する連絡体制の整備	整備している。	100%	100%	－
9	職員の情報管理対策	実施している。	90%	92%	UP

情報セキュリティ対策に係るPDCAサイクルの構築は着実に増加。CISO補佐官の設置など、体制の強化は引き続き推進の必要。

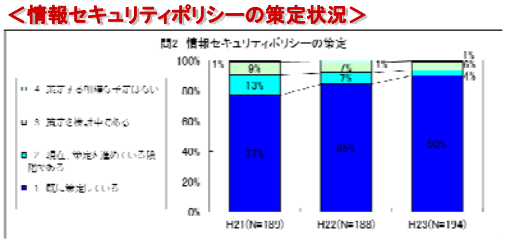
情報セキュリティ対策に係る中期目標への明記・PDCAサイクルの構築ともに進捗が見られた。
しかしながら、情報セキュリティ2010で推進するとした、中期目標への明記の予定のない独立行政法人等が3%存在し、また、CISOが設置されていない（12%）など、情報セキュリティ対策の推進体制構築に今後も取組みが必要。

＜情報セキュリティ対策に係る中期目標への明記＞



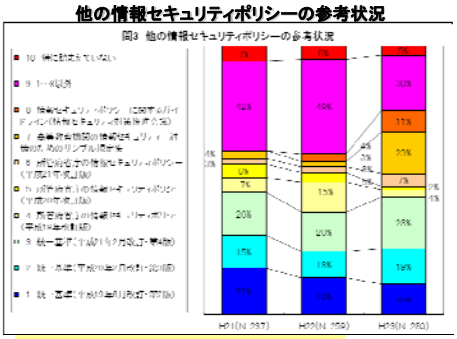
情報セキュリティ対策に係る中期目標への明記を行っている法人は大きく増加（40%→71%）また、明記を予定している法人をあわせると、90%以上となっており、進捗が見られる。
しかしながら、情報セキュリティ2010で推進するとしているにもかかわらず、言及する予定のない法人が3%存在しており、対策の推進体制構築に一層の取組みが必要。

＜情報セキュリティポリシーの策定状況＞



情報セキュリティポリシーの策定は、着実な進捗が見られ、策定済みあるいは予定を含めてほぼ100%となった。
（予定がない法人は、早々に廃止予定となっているものみ。）
しかしながら、情報セキュリティポリシー策定が数年前に行われ、見直しがされていないものもあり、最新の脅威等に対応した情報セキュリティポリシーとなっているか懸念が残る。引き続き取り組みが必要。

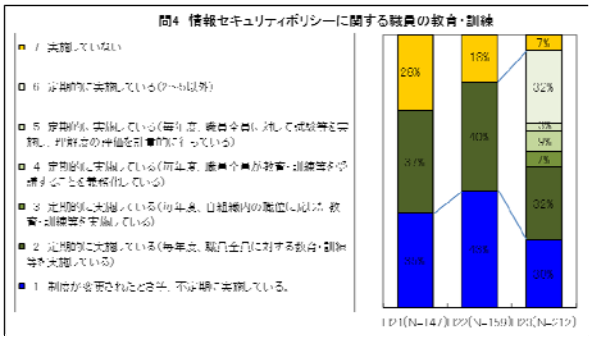
他の情報セキュリティポリシーの参考状況



『上記以外』の主なもの：
・高等教育機関の情報セキュリティ対策のためのサンプル規程集（27）
・情報セキュリティポリシーに関するガイドライン（15）
・ISO27001、17799系（6）

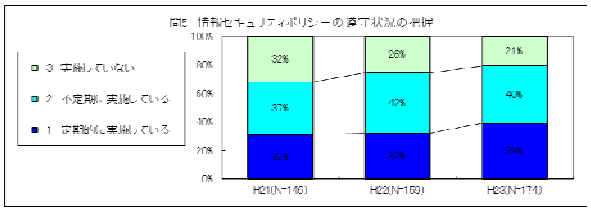
＜情報セキュリティポリシー策定済み法人の対策実施状況　その1＞

職員の教育・訓練



定期・不定期で、
全体の83%と実施が増加。

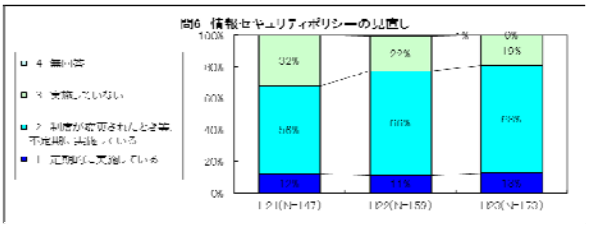
遵守状況の把握



定期・不定期で、
全体の79%と実施が増加。

＜情報セキュリティポリシー策定済み法人の対策実施状況　その2＞

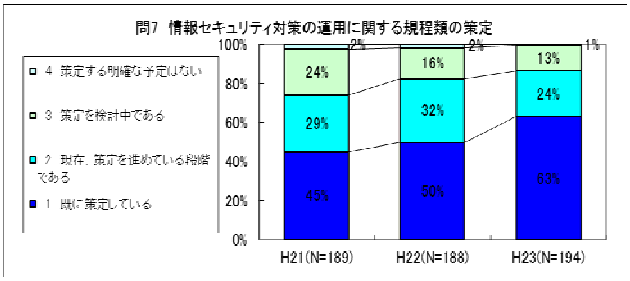
ポリシーの見直し



定期・不定期で、
全体の81%と実施が増加。

情報セキュリティポリシー策定済みの法人では、ポリシーの見直し、職員の教育・訓練、遵守状況の把握の全てにおいて前回より一定の進捗が見られ、ポリシー（Policy）に基づく対策の実施（Do）、評価（Check）、見直し（Act）の徹底は着実に進んでいる。

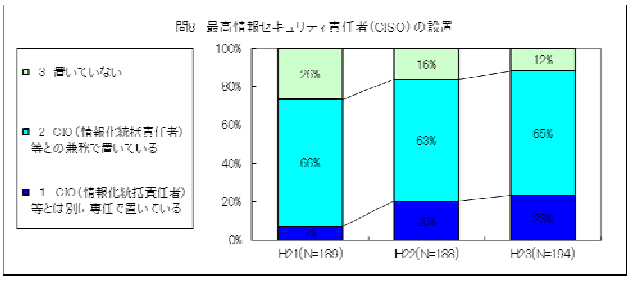
＜情報セキュリティポリシー対策の運用に関する規程類の策定状況＞



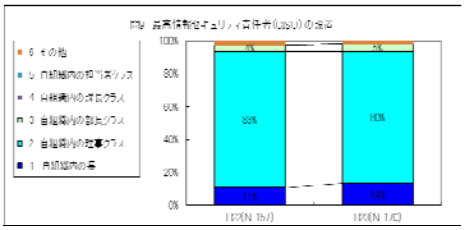
情報セキュリティポリシー対策の運用に関する規程類の策定状況においても、着実に進捗している。

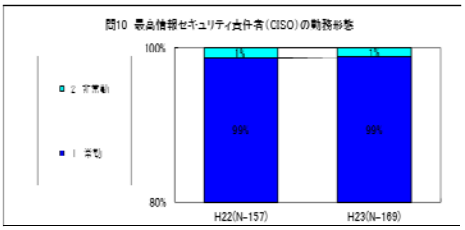
＜情報セキュリティ対策推進体制の整備状況　その1＞

最高情報セキュリティ責任者（CISO）の設置



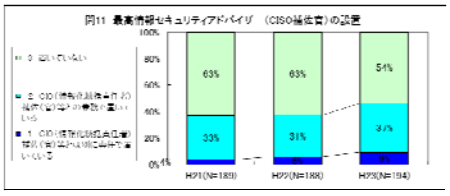
最高情報セキュリティ責任者（CISO）の設置は、進捗。しかしながら、推進体制の構築のためには、確実な設置が望まれる。
職位・勤務形態については、理事クラス・常勤が大半である。

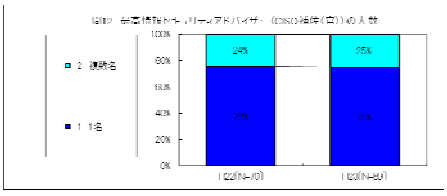


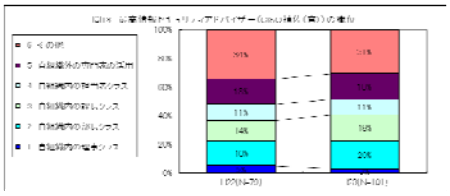


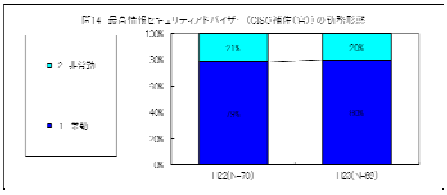
＜情報セキュリティ対策推進体制の整備状況　その2＞

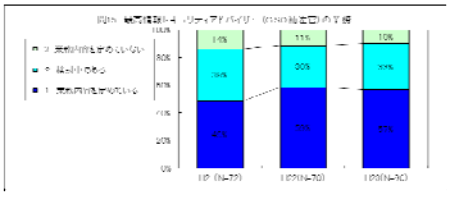
最高情報セキュリティアドバイザー（CISO補佐官）の設置

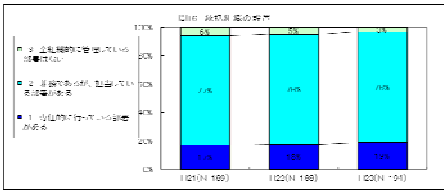








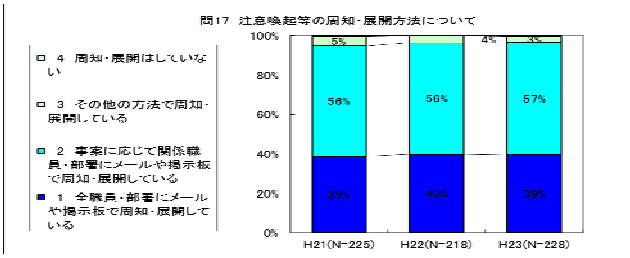




最高情報セキュリティアドバイザー（CISO補佐官）の設置は、10%増加して全体の46%。
職位・勤務形態については、補佐官の人数・勤務形態は、1名・常勤が大半であったが、職位については法人によって異なっている。

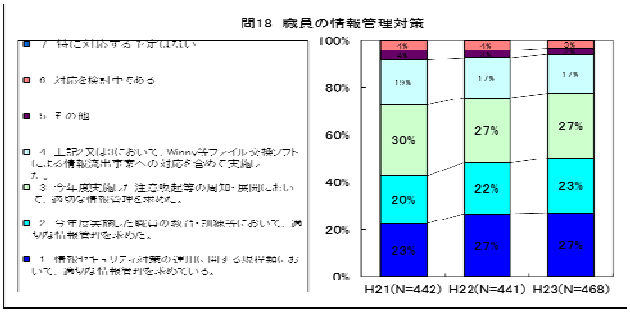
＜平常時の体制の整備＞

注意喚起等の周知・展開方法



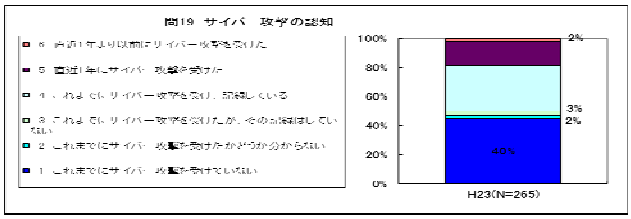
全職員・部署もしくは関係職員・部署への周知・展開は、97%。

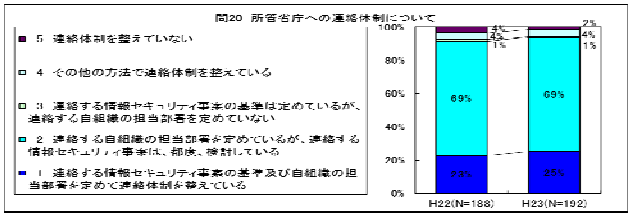
職員の情報管理対策

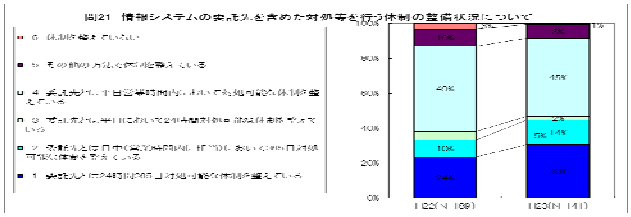


注意喚起による情報管理対策の徹底に加え、規程類の整備や教育・訓練等の体制を構築して恒常的な徹底へ進捗。

＜情報セキュリティ事案が発生した際の体制の整備＞





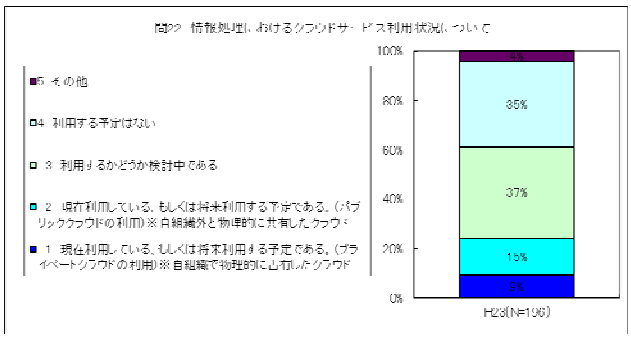


緊急時を含め実効性のある連絡体制の整備 として、注意喚起等の周知・展開方法及び職員の情報管理対策については、進捗が見られる。

所管府省庁への連絡体制及び情報システムの委託先を含めた対処等の体制整備は、共に9割超となっている。

事案の発生に適切に対処できるよう、体制整備の確実な構築が必要であり、今後とも継続的な確認が必要。

＜その他＞



利用している、利用予定は、24%。利用するかどうか検討中を含めると61%となっており、利用の拡大が確認された。