2009 年度の情報セキュリティ政策の評価等

内閣官房情報セキュリティセンター（NISC）

2010 年 7 月 22 日

目次

図表

別添

はじめに

１．本文書の位置づけと基本認識

本文書は、2009 年度から始まった３年間を対象期間とする「第２次情報セキュリティ基本計画」[1]（以下「第２次基本計画」という。）と、それに基づく 2009 年度計画である「セキュア・ジャパン 2009」[2]（以下「SJ2009」という。）によって進められている情報セキュリティ政策について、2009 年度の政策の評価等[3]について報告するものである。

我が国の情報セキュリティ政策の運用は PDCA サイクル[4]の形で行うこととなっており、その詳細は、情報セキュリティ政策の枠組みについて記述した文書である「情報セキュリティの観点から見た我が国社会のあるべき姿及び政策の評価のあり方」(以下「枠組み文書」という。）など[5]により定められている。これらに基づき内閣官房情報セキュリティセンター（以下「NISC」という。）は、評価指標にのっとったデータ等の情報を集め、評価等を行った。

２．本文書の構成

本文書では、第１章においては情報セキュリティ政策全体、第２章においては政府機関、第３章においては重要インフラ、第４章においては企業及び個人、第５章においては横断的な情報セキュリティ基盤[6]について現状の評価等を行う。各章の構成については、他の章との比較を容易にするため、すべての章を通じてほぼ同じ柱立てとしており、各章ともに第１節では「2009 年度の取組み」、第２節では、「2009 年度の評価等に向けた「作業方針」」（以下「作業方針」という。）に基づき、「2009 年度の取組み及び取組みを受けた現状の評価等（2009 年度の評価等)」、第３節では、「2010 年度に向けた課題」について述べる。

---

1 2009 年２月３日　情報セキュリティ政策会議決定。

2 2009 年６月 22 日　情報セキュリティ政策会議決定。

3 本書においては、情報セキュリティ政策会議決定文書（脚注５参照)、「１．評価指標に基づく評価等のための作業方針」における定義に従い、「評価指標に基づく評価、補完調査及び分析等」を「評価等」と記す。

4 計画（Plan)、実施（Do)、点検（Check)、改善処置（Act）の各段階を経て、改めて計画（Plan）に戻る自律的な政策推進サイクル。

5 2007 年２月２日　情報セキュリティ政策会議決定文書（「「セキュア・ジャパン」の実現に向けた取組みの評価等及び合理性を持った持続的改善の推進について」及び 2010 年５月 11 日　情報セキュリティ政策会議了解文書「情報セキュリティの観点から見た我が国社会のあるべき姿及び政策の評価のあり方【第２版】～「セキュア・ジャパン」の実現に向けた情報セキュリティ政策の PDCA サイクルの確立～」

6 「情報セキュリティ技術戦略」、「情報セキュリティ人材の育成・確保」、「国際連携・協調」、「犯罪の取締り及び権利利益保護・救済」の４分野を指す。

第１章　情報セキュリティ政策全体の評価等

第１節　2009 年度の取組み

１．2009 年度の取組みの背景

SJ2009 では、「すべての主体に事故前提の自覚を」が重点とされ、重点目標として、

①新たなテーマに対する官民の共通認識の形成

②電子政府の推進

③情報セキュリティ人材の育成・確保

④国際連携・協調の推進

⑤情報セキュリティ技術戦略の推進

が設定された。

具体的には、「対策実施４領域」[7]、「横断的な情報セキュリティ基盤」、「政策の推進体制と持続的改善の構造（政策の推進体制の強化、他の関係機関等との連携、持続的改善構造の構築）」という柱立てに基づいて施策を実施することとし、NISC を含む各府省庁が計 212 の取組みを行うこととなった。

また、SJ2009 では、「すべての主体の協働による情報セキュリティ対策の強力な推進を」という 2010 年度の重点施策の方向性が設定され、「官民における人的基盤・体制整備に向けた取組み」、「国際連携・協調のための取組み」、「官民による技術の研究開発及び導入の推進」として、計 14 の具体的施策が盛り込まれた。

第２節　2009 年度の取組み及び取組みを受けた現状の評価等（2009 年度の評価等）

１．2009 年度の評価等に関する基本的考え方（評価等の視点）

情報セキュリティ政策全体に係る 2009 年度の評価等は、以下の３つの視点に基づいて行うこととする。

すなわち、

①2009 年度「すべての主体に事故前提の自覚を」の思想を重点とした取組みによる 2012 年度の姿の達成度を測る視点

②情報セキュリティに係る 2009 年度の様々な動向を測る視点

③2010 年度の取組みの具体化等に向けた助けとする視点

である。

２．評価等について（評価指標等）

2009 年度の情報セキュリティ政策全体の評価等は、枠組み文書第２章第２節を踏まえ、各論で行う政策領域ごとの評価等の積み上げによって行う。また、こうした政策領域ごとの評価等に加えて、社会情勢についても評価等を行った上で、これらも合わせて積み上げることで全体としての評価等を行う。

なお、このような評価等の手順については、作業方針第２章において述べた検討の枠組

[7] 「政府機関・地方公共団体」、「重要インフラ」、「企業」、「個人」の４領域を指す。

み及び手順に基づくこととする[8]。

３．評価等の結果と総評

（１）施策の取組み結果に関する評価等

SJ2009 において、2009 年度中に推進するとされた 212 の具体的施策の取組み結果については、2009 年度の評価等では以下のとおり分類され、評価がなされた。

Ａ　：176 施策（83.0%、内Ａ’は２施策）
Ｂ＋： 25 施策（11.8%）
Ｂ　： 11 施策（ 5.2%）
Ｃ　： ０施策（ 0.0%）
－　： ０施策（ 0.0%）

表１　SJ2009 に盛り込まれた施策の実施状況の分類

分類	進捗状況
Ａ	当初の予定どおり推進することが出来た施策。 なお、施策は推進できたが、体制や人員に関して問題が存在するため、今後、継続して推進するためにそれらの解決が必要であるということが、当該施策に関連した作業の進捗や担当へのヒアリング等から明白になった施策については「’」を付した。
Ｂ＋	年度内には完了していないが、着実に取組みを進めており、数ヶ月以内には完了する施策。
Ｂ	予定どおり推進することは出来なかったが、今後も取組みを続けることにより、今後の見通しが立つ施策。
Ｃ	予定どおり推進することはできず、今後の見通しも立たない施策。
－	予定どおり推進することが出来なかったが、その理由が政府機関の事情によるものではない施策。

SJ2009 において、2009 年度中に推進するとされた施策については、各府省庁において着手がなされ、約８割の施策について当初の予定どおり施策を推進した。残り２割（36 施策）の予定どおり推進できなかった施策については、「情報セキュリティ報告書作成のためのガイドラインの策定等」の策定など、数ヶ月以内には完了するＢ＋の 25 施策のほか、刑事共助条約の締結等、施策を推進したものの 2009 年度中に完了できなかったものなど今後も取組みが必要なＢのものが 11 施策であった。

Ａとされた 176 施策は、関係各府省庁の担当者の努力により予定どおり推進することができたものの、Ａ’の２施策については、「各府省庁の情報システムの一元管理」及び「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」となっている。

Ｂ、Ｂ＋、Ａ’と分類・評価された施策のみならず、Ａと分類・評価された施策の中にも今後引き続き取組みを実施することが求められるものも存在している。このような

[8] 横断的な情報セキュリティ基盤については、作業方針第６章において述べたとおり、すべての施策についてその進捗状況を把握するにとどめ、特段評価指標の設定は行わない。

施策については、継続的な取組みや発展的な取組みが求められる。

（２）施策の取組みによる社会的変化に関する評価等

施策の取組みによる社会的変化に関しては、第２節２．の分類にのっとり、政策領域や社会情勢の各領域についてそれぞれ総体として評価等を行う。ただし、個々の政策領域は第２章以降の各論において評価等を行うこととする。

（ア）人的側面（人材、意識、体制・制度）

平成 21 年通信利用動向調査（総務省）によれば、我が国のインターネット利用者数及び人口普及率は、前年よりも増加の傾向にある。その一方でウイルス対策ソフトの導入等、セキュリティ対策を行う利用世帯の割合は横ばいのままであり、また、インターネット利用を通じた著作権の侵害や他者への非難中傷を伴うトラブルの発生等、インターネットリテラシーの面でも課題が依然として存在する。

一方、これらに係る制度面の取組みにおいても、サイバー犯罪条約締結の前提となる関係法令の制定など、法制レベルにおいても、積み残された課題がある。

これらの問題は、根底にいずれも我が国インターネット利用者がどのような利用環境が望ましいと考えるのか、その自覚・意識のあり方に左右されるものである。

したがって、今後、あるべき将来像を定めた上で、各分野における、IT セキュリティ及びリテラシーに係る知識の周知を図るとともに、関係する諸制度を整備し、また IT、法律、教育等関係各分野での人材育成、各専門分野における連携の強化も同時に進めていく必要がある。

（イ）物的側面（投資、技術、ハード、ソフト、ネットワーク）

昨年来の世界的な経済危機の影響から、2009 年度の我が国における IT 関連投資は減少し、これに併せて情報セキュリティ関連の投資も減少している。他方で、複雑で巧妙なウイルスの出現など、ウイルス対策ソフト等の単一の技術のみでは対抗できない脅威が登場している。

この経済危機を背景に、利用者にとって設備投資コストが抑えられるクラウド・コンピューティングの利用が拡大しつつあるが、この新しいネットワークサービスには従来とは異なるリスクが存在する可能性がある一方で、それに係る情報セキュリティ対策は確立していない。

現在、これらの動きに対応して、関連する情報システムの企画・設計段階からセキュリティ対策を作り込むための専門家の連携などの方策の検討が着手されているが、それらの取組みを継続し、高めていく取組みが重要である。

（ウ）周辺情勢（インシデント・事件、市場等）

周辺情勢に関しては、ウイルスベンダーの収集したデータベースによれば、マルウェアの認知件数は３年前の約 10 倍に上る統計数値が公表されている。実際、2009 年末から 2010 年初にかけて企業のホームページを中心に広範なウイルス感染被害が認められている。また、昨年、米国と韓国の政府機関に対する大規模 DDoS 攻撃が行われ

る事件が発生する等、情報セキュリティを巡る状況は依然厳しく、引き続き対策の強化が必要である。

（エ）総評

「事故前提社会への対応力強化」に向けて各政策領域において対応力の強化に着手した。

中でも、政府機関においては能動的な PDCA サイクルを確立するための方策を策定した。また、重要インフラ分野においては、事業セクターごとに情報セキュリティに係る情報の共有を目指す体制（セプター）の運営を開始した。企業においては、内部統制の強化を進める企業が増加していることにみられるように、情報セキュリティガバナンスの確立に向けた取組みが進められたといえる。ただし、中小規模の企業においては、経済危機の影響等から対策実施が停滞している状況である。個人においては、広報啓発・情報発信等により情報セキュリティへの意識を高めることができたが、IT 利活用への不安を取り除くまでには至っていない。

一方、各対策実施領域における情報セキュリティ対策の底上げに関連する横断４分野に目を向けると、技術戦略においては、情報セキュリティ技術開発において、政府が取組むべき技術範囲の洗い出しや政府による支援の在り方に関する検討が進んだが、現実において情報セキュリティに係る研究開発を強力に推進するためのプログラムの策定が必要な状況である。

また、人材育成においては、前年度までの施策の多くが継続して実施される一方、新たな取組みの多くは検討段階にとどまっており、人材の充実という観点から大きな進歩は見られない。今後は、より一層の人材の充実を図るために、新たな取組みを検討する必要がある。

国際連携においては、現在構築しつつある関係国・機関との連携を深めるほか、日・ASEAN 間のプロジェクトを今後どのように個別分野等での具体的な連携に展開できるか次第といえる。

犯罪対策の分野においては、取締り、体制強化、広報啓発等の施策が継続的に推進されているところであるが、それらが目に見える形では国民の IT 利用に係る不安感軽減に結びついていない。取締りや体制強化に引き続き取り組むとともに、国民が能動的に情報セキュリティ対策に取り組むことで不安感を軽減できるよう、情報セキュリティに関する意識の喚起や対策に必要な知識の提供を強化するなど、さらなる内容の充実が必要である。

第３節　2010 年度に向けた課題

毎年、PDCA サイクルにのっとり対策の進捗状況等は確実に把握しているものの、今後の施策の実施に当たっては、PDCA サイクルに基づき年単位での進捗度合いを測ることに加え、我が国の取組みに係る進捗状況を国際的に比較する必要がある。特に、いわゆる IT 先進国と比較した場合の我が国の位置づけについては、今後留意していく必要がある。

技術面での取組みの重要性が低下することはないが、依然として発生するマルウェアの感染流行、DDoS 攻撃等の発生など、IT 関連技術の進歩はセキュリティ対策技術の高度化のみな

らず、マルウェア等のシステムへ脅威を与えうる技術の高度化にも影響を及ぼしており、技術面からの情報セキュリティ対策には一定の限界が認められる。

今後、更なるセキュリティ対策の効果向上を図るためには、法制等の各種枠組みの整備及び運用並びにこれらの枠組みを情勢に応じ的確に構築・運用していく人材の育成・確保が各対策実施領域において求められる。

我が国における各種枠組みの整備等は「情報を預ける主体」と位置づけられる対策実施領域中、「企業」・「個人」の要望を踏まえた内容とするのが望ましいが、多数の主体は漠然とした不安を抱えているものの、社会的セーフティネット構築等の具体的な要望に乏しいのが実情である。

引き続き事故前提社会への対応力強化に向け「自覚」を促す過程で、制度・枠組み面での課題を明らかにしつつ、関係機関との相乗効果を図るための関係主体が協働できる制度・枠組みを検討していく必要がある。

第２章　政府機関における現状の評価等

第１節　2009 年度の取組み

１．2009 年度の取組みの背景

政府機関における情報セキュリティ対策は、各府省庁が政府機関統一基準を踏まえた府省庁基準に基づく PDCA サイクルを持続的に進め、また政府全体としても各府省庁の対策実施状況の評価や政府機関統一基準の適時・適切な見直しも含めた情報セキュリティ対策の PDCA サイクルを推進することが基本となっている。

「2008 年度の情報セキュリティ政策の評価等」[9]では、2007 年度の評価において指摘されたセキュリティ教育に関する実施体制の充実・向上、全職員、全情報システムの対策実施状況の適切な把握、政府統一的な教育プログラムの質の向上及び受講機会の拡大について、2007 年度と比較し一定の成果がみられるものの、依然として対策が不十分な部分や課題が残っており、目標達成に向けた取組みが必要である旨が指摘されている。

２．2009 年度の取組み

SJ2009 において、各府省庁が能動的に情報セキュリティ対策に取り組む体制の確立を目指したマネジメントの強化、電子政府の利便性・セキュリティレベルの向上、政府機関における安全な暗号利用の推進を測る施策等に取り組んだ。

第２節　2009 年度の取組み及び取組みを受けた現状の評価等（2009 年度の評価等）

１．2009 年度の評価等に関する基本的考え方（評価等の視点）

政府機関における情報セキュリティ対策については、各府省庁及び政府全体の２つの PDCA サイクルが着実に定着・浸透しているかという視点に基づいて評価等を実施した。具体的には、2009 年度の対策実施状況報告及び特定の重要項目に係る重点検査の結果も踏まえて、総合的に評価を行った。また、各府省庁が能動的に情報セキュリティ対策に取り組むため、「情報セキュリティに係る年次報告書」（以下「情報セキュリティ報告書」という。）に係る枠組みを構築した点も評価の対象とする。

２．評価等について（評価指標等）

2009 年度対策実施状況報告では、原則としてすべての職員を対象として、政府機関統一基準に規定されている、基本遵守事項（333 項目）について、各府省庁における実施状況を調査した。一方、2009 年度重点検査では、全府省庁を対象として、端末、ウェブサーバ及び電子メールサーバについて、統一基準に準拠した対策が実施されているか否かの調査を実施した。

[9] 2009 年５月８日　情報セキュリティ政策会議報告。

３．評価等の結果と総評

（１）施策の取組み結果に関する評価等

（ア）対策実施状況に関する評価等

① 対策実施状況報告に基づく評価等

政府機関統一基準に基づき、各府省庁における情報セキュリティ対策推進の実施状況の報告を受け、分析及び評価を行った。取りまとめ結果については、結果を報告[10]するとともに、NISC のホームページにおいて公表した（別添２）。

2009 年度は、2008 年度に比べて、より多くの遵守事項において高い水準での実施率となったことから、2008 年度に示した課題への対策の浸透が進んでいることが明らかになった。具体的には、2008 年度の課題となっていた「情報セキュリティ対策の教育」及び「各種規程・手順の整備」に関する遵守事項については、前回（2008 年度）から顕著な改善が認められた。

ａ）情報セキュリティ対策の教育

○2008 年度は職員による教育受講が不十分であり、未受講者への受講指導の徹底も不十分であったが、2009 年度は顕著な改善が認められた。

ｂ）各種規程・手順の整備

○責任者が実施すべき各種情報セキュリティ対策の基礎となるべき規程・手順の整備において、2008 年度は暗号と電子署名、外部委託、府省庁外での情報処理の制限及びドメイン名の使用に係るものが不十分であったが、2009 年度は顕著な改善が認められた。

また、同じく 2008 年度の課題となっていた「情報の格付け・取扱い制限に係る措置」については、一定の改善が認められたものの、一部の項目について今後も改善が求められる。

ｃ）情報の格付け・取扱い制限に係る措置

○情報の保存・移送等の項目については、2008 年度と比較して大幅に実施率が改善された。

○情報の作成と入手時の遵守事項については、2008 年度と同様に 2009 年度においても取組みが不十分であることが認められた。

他方、2009 年度の課題として「業務継続計画との整合的運用の確保」の対策の不十分さが明らかになり、2010 年度の改善に向けた対策が求められる。

ｄ）業務継続計画との整合的運用の確保

○特定の府省庁において業務継続計画と情報セキュリティ対策の整合性の確保について、取組みが不十分であることが判明した。

なお、本件への具体的な対策としては、特定の府省庁にヒアリングを行い、支援を行うことで実施率の向上を図る予定である。

② 重点検査に基づく評価等

政府機関統一基準の基本遵守事項の中でも特に重要な事項として、2008 年度に引

[10] 2010 年５月 11 日　情報セキュリティ政策会議。

き続き、20 府省庁（2009 年度より、消費者庁が対象に追加。）の端末、ウェブサーバ及び電子メールサーバについて検査を行った。取りまとめ結果については、結果を報告[10]するとともに、NISC のホームページにおいて公表した（別添３）。

ａ）分析

2010 年３月末時点で、全府省庁において実施率 100%を達成した。今後も、全府省庁において実施率 100%が維持されるよう指導していくとともに、新たな脅威の動向を常に注視し、必要な対策を各府省庁に促していく。

（イ）SJ2009 施策の取組み結果に関する評価等

① 全ての政府機関において能動的に情報セキュリティ対策に取り組む体制の確立

ａ）情報セキュリティガバナンスの確立に向けた取組み

各府省庁は、情報セキュリティガバナンスの確立を図るため、最高情報セキュリティ責任者の下、最高情報セキュリティアドバイザーの設置等、当該機関の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が可能な体制整備を進めた。

ｂ）PDCA サイクルの定着と浸透

各府省庁は、情報セキュリティ対策の自己点検及び監査の結果等を踏まえて自ら対策の改善を行うなど、PDCA サイクルの定着及び組織全体への浸透を徹底した。

NISC においては、対策実施状況報告や重点検査をもとに各府省庁の情報セキュリティ対策の実施状況の評価等を行うとともに、自己点検の効率化や教育についての支援を行うなど、政府全体としての PDCA サイクルの定着に取り組んだ。

ｃ）情報セキュリティ報告書作成のためのガイドラインの策定等

NISC は、各府省庁における情報セキュリティ報告書作成に向け、2009 年５月以降、情報セキュリティ報告書専門委員会の会合を４回開催して、情報セキュリティ報告書作成のためのガイドライン及び各府省庁が作成した情報セキュリティ報告書の定量的評価等の手法等を検討・報告[10]を行った。

また、総務省及び経済産業省において、2009 年度情報セキュリティ報告書を試行的に作成し、全府省庁における本格的な取組みの実施に向けた情報共有を行った。

ｄ）政府機関統一基準の見直しの実施

政府機関統一基準については、技術や環境の変化を踏まえ、毎年見直しを行うこととしている。

2009 年度においては、2008 年度に第４版へ大幅な改訂を行ったところであり、各府省庁における定着に重点を置く必要があること、最近の脅威についても現行の統一基準で対応可能であることから、適用対象範囲に「消費者庁」を追記するなどの微修正に留めることとし、第４版（平成 21 年度修正）を決定[10]した。

ｅ）情報セキュリティ対策の府省庁共通的課題に対する取組み

NISC は、情報セキュリティ対策の府省庁共通的課題について、府省庁と共同して解決に取り組んだ。

具体的には、政府機関の保有する公開ウェブサーバ及び電子メールサーバの集約化に向けて、各府省庁において、業務・システム最適化計画の枠組みを活用しつつ、集約化計画を策定し、結果を報告[11]するとともに、NISC のホームページにおいて公表した（別添４）。

その結果、2013 年度末までに、2008 年 11 月１日と比較して、公開ウェブサーバについては約 1,000 台から約 550 台、電子メールサーバについては約 1,900 台から約 1,000 台に、概ね半減が達成できる見通しとなった。サーバ集約化により、管理が集約されるとともに、行政コストの削減にも寄与するものである。

ｆ）政府機関における人材の育成・確保及び職員の意識啓発

情報セキュリティ対策を担当する職員の業務遂行及び専門的能力の向上に資するため、NISC 及び総務省において、「情報システム統一研修」の情報セキュリティに係る講義内容を改善するとともに、「新任管理者基本セミナー」において、「管理者に求められる情報セキュリティ対策について」をテーマとする研修を実施するなど、政府統一的な教育プログラムの充実を図った。

② 政府全体を通じて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

情報セキュリティを基本コンセプトとして取り入れた情報システムの企画・設計が行われるための方策について検討するため、NISC において、経験・知見を有する有識者やベンダー等を構成員とする「情報セキュリティを企画・設計段階から確保するための方策に係る検討会」を、2009 年度は３回開催した。ここで、政府機関統一基準に基づきつつ、調達者と調達先ベンダーの協業のあり方、セキュリティを考慮した情報システム開発手法に係る検討を行い、それらを踏まえ、引き続き 2010 年度も検討を行う予定。

③ 電子政府の利便性・セキュリティレベルの向上

「オンライン利用拡大行動計画」[12]に基づき、電子政府の手続に応じたセキュリティ確保策、ユーザビリティ向上方策についての、政府横断的なガイドラインを策定するために設置された「電子政府ガイドライン作成検討会」の下で「セキュリティ分科会」を 2009 年度に５回開催し、認証基盤の普及拡大をはじめ、適切な認証と電子署名を選択するための考え方を整理した。

その結果、2009 年 11 月（第 11 回分科会）に、電子行政手続に関するリスク評価

11　2010 年５月 11 日　情報セキュリティ政策会議。

12　2008 年９月 12 日　IT 戦略本部決定。

手法とこの手法により導出される「リスクの影響度」、影響度に応じた認証方式の「保証レベル」の導出とその対策基準を規定した「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（案）」を策定し、パブリックコメントを実施した。

④ 政府機関における事業継続性確保・緊急対応能力の強化に係る検討

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であり、NISC において、対策実施状況報告に基づき現状調査を行った。

また、各府省庁の保有する重要なシステムや情報のバックアップ体制等について現状把握を行い、政府横断的な方向性の検討を実施するために、IT リスクに係る事業継続計画の在り方についての勉強会を開始した。

⑤ 独立行政法人等の情報セキュリティ対策の推進

各府省庁に対し、所管する独立行政法人等に対してセキュリティ対策の推進に係る要請を行う等の必要な措置を講じるよう事務連絡を発出し、それを踏まえ、情報セキュリティポリシーの整備状況等についての実態調査を行った（概要を別添５に示す。）。

⑥ その他個別の情報セキュリティ対策の推進

ａ）政府機関への成りすましの防止

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ため、各府省庁向け説明会等を開催し、各府省庁における送信ドメイン認証の普及促進を行った。

ｂ）政府機関における安全な暗号利用の推進

電子政府の情報システムに広く使用されているハッシュ関数 SHA-1 及び公開鍵暗号方式 RSA1024 の安全性の低下に対応するため、2008 年度に決定された「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」に基づき、NISC において、各府省庁における急激な安全性の低下に備えた緊急対応計画の策定支援を実施した。

（２）総評

対策実施状況に関しては、政府全体として多くの遵守事項において高い水準での実施率となったが、一部の遵守事項（業務継続計画との整合的運用の確保、情報の作成と入手）について課題が残っている。

また、端末、ウェブサーバ及び電子メールサーバについて重点検査を実施したところ、本年度で対策のすべてを完了とすることができた。昨年度の重点検査で判明した政府機関全体でウェブサーバ約 1,000 台、電子メールサーバ約 1,900 台を設置・運用している現状については、各府省庁において、集約化計画を策定し、2013 年度末までに概ね半減

が達成できる見通しとなった。

さらに、各府省庁が能動的に情報セキュリティ対策に取り組むため、情報セキュリティ報告書の作成、評価等に係る一定の枠組みを構築することができた。

上述の結果を総合すれば、2009 年度は、引き続き一部対策が不十分な部分や課題が残っているものの、多面的な対策を講じることができたと評価できる。

第３節　2010 年度に向けた課題

上記総評を踏まえると、2010 年度の課題としては、まず、すべての政府機関において能動的に情報セキュリティ対策に取り組む体制の確立をさらに促進させる必要がある。そのためには、2010 年度に情報セキュリティ報告書を全府省庁において試行的に作成し、その後の報告といった各府省庁における一連の PDCA を回すことで、PDCA の各プロセスにおけるトップマネジメントの強化を推進するとともに、2009 年に引き続き、政府機関において情報セキュリティを含む IT 分野の専門的知見を有する人材の戦略的な育成・確保、職員の意識啓発の充実等を図ることが不可欠である。

対策実施状況報告で各府省庁での対応が不十分であった事項については、メリハリのある情報セキュリティ教育の実施、トップマネジメントの強化等により、一層の向上を図ることが必要である。

また、政府全体を通じて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は来年度での成果のとりまとめを目指す。

独立行政法人等においては、その業務特性及び対策の実施状況に応じて、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、自らの情報セキュリティ対策に係る PDCA サイクルを構築していくことが課題である。

第３章　重要インフラにおける現状の評価等

第１節　2009 年度の取組み

１．2009 年度の取組みの背景

重要インフラにおける IT 障害が国民生活や社会経済活動に重大な影響を及ぼさないことを目的として重要インフラを防護するとともに、重要インフラ事業者等のサービス・レベルの維持及び重大な IT 障害発生時の迅速な復旧等の確保を図ることを目的として、「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」[13]（以下「第２次行動計画」という。）を定め、関係政府機関及び重要インフラ事業者等が協力して取組みを進めているところである。

２．2009 年度の取組み

第２次行動計画では、重要インフラ関係の５本の施策の柱（①安全基準等の整備及び浸透、②情報共有体制の強化、③共通脅威分析、④分野横断的演習、⑤環境変化への対応）と、各主体における取組み項目を示し、項目ごとにアクションプランとして具体化を図ることにより、重要インフラの情報セキュリティ対策の向上に繋げていくこととしている。

第２節　2009 年度の取組み及び取組みを受けた現状の評価等（2009 年度の評価等）

１．2009 年度の評価等に関する基本的考え方（評価等の視点）

第２次行動計画に基づき、重要インフラ分野における情報セキュリティ対策の評価・検証は、原因と責任を追及することに着目するのではなく、むしろ様々な経験から将来の取組みの改善に活かせる教訓を抽出し、これを関係主体のそれぞれの取組みの改善に役立てるようにすることを主眼とする。

具体的な進捗状況の評価・検証は、個々の情報セキュリティ対策がどのような成果をあげたのかという「成果（アウトプット）を測る視点」と、社会が実際にどの程度理想とする将来像に近づいたのかという「結果（アウトカム）を測る視点」の２つの視点で取り組む。この際、可能な限り客観的な評価指標を用いた検証を行った上で、評価に取り組むこととする。

なお、第２次行動計画においては、「検証」とは各々の取組みについてその進捗状況に関する客観的事実を評価指標として用いて確認することとし、また、「評価」とは目標に照らしてその取組みの妥当性を見直すこととする。

２．評価等について（評価指標等）

2009 年度以降の取組みの進捗状況の評価については、重要インフラ所管官庁及び重要インフラ事業者等の「第２次行動計画」に基づく取組みの進捗状況について、評価・検証を行う。重要インフラ事業者等による対策の成果検証については、重要インフラの分野ごとに検証対象とした重要インフラサービスとし、政府機関等による施策の成果検証について

[13] 2009 年２月３日　情報セキュリティ政策会議決定。

は、第２次行動計画における情報セキュリティ対策の柱ごとの重要インフラ事業者等による寄与を対象とする。

３．評価等の結果と総評

（１）施策の取組み結果に関する評価等

重要インフラにおける情報セキュリティ対策向上の取組みの一環として、情報セキュリティ政策会議の下に我が国全体の重要インフラ防護に資する情報セキュリティにかかる事項について調査・検討を行う専門委員会として「重要インフラ専門委員会」が設置されている。同委員会は、2009 年度において２回（2008 年度は７回）の会合を開催し、それぞれの議題について検討を行った（表２）。

また、2009 年度の施策の実施状況は、別添１に示すとおりである。

表２　重要インフラ専門委員会会合

会合（開催日）	主な議題
第 25 回会合 （2009 年４月６日）	・重要インフラにおける「指針の見直し」について（骨子案の検討） ・情報共有・分析機能の整備について ・2008 年度相互依存性解析について ・2008 年度分野横断的演習について ・「「重要インフラの情報セキュリティ対策に係る第２次第２次行動計画」の情報連絡・情報提供に関する実施細目」の概要について ・重要インフラにおける情報セキュリティ対策に関する 2008 年度の評価等について
第 26 回会合 （2009 年７月７日）	・重要インフラにおける「指針（本編）の見直し」について（パブリックコメント案の検討） ・2009 年度共通脅威分析について ・2009 年度分野横断的演習について

（２）重要インフラ事業者等による対策の成果の検証

対策の成果検証は、第２次行動計画の目標である「IT 障害が国民生活や社会経済活動に重大な影響を及ぼさないようにすること」を踏まえ、重要インフラの分野ごとに検証対象とした重要インフラサービスについて、検証レベルを逸脱した IT 障害等の発生状況を検証することとした。

具体的な評価指標は、検証レベルを逸脱する IT 障害事例のうち NISC が認知したものの 10 分野全体での総数とし、その件数は 185 件となった。

（３）政府機関等による施策の成果の検証

施策の検証で用いる評価指標は、情報セキュリティ対策の５本の柱ごとに、重要インフラ事業者等による情報セキュリティ対策への寄与とした。

（ア）安全基準等の整備及び浸透

指針と安全基準等の項目の充実と、個別事業者等の安全基準等に基づいた取組みの確実な実施に着目し、評価指標の設定・検証を行った。

○指針及び参考資料に採取した対策項目数：19 件

○安全基準等に基づいて定期的な自己検証に取り組んでいる重要インフラ事業者等の数：849 者

○指針の重要インフラ事業者等による評価：次のような意見が寄せられた。

・一般的なセキュリティだけでなく、重要インフラ保護の観点について広く記述されていることから、指針の位置づけを「安全・信頼性確保」または「危機管理」に係る安全基準策定にあたっての指針としてはどうか。

・例示を掲載すると企業の理解が深まるのではないか。

・情報セキュリティ施策に関して、「何を」、「どの程度」するべきかの指針として参考となった。

（イ）情報共有体制の強化

整備された情報共有体制と共有された情報の充実に着目し、評価指標を設定・検証を行った。

○NISC が発信した情報件数：13 件

○セプター等で共有された情報件数：326 件

○共有された情報が情報セキュリティ対策に資すると評価した重要インフラ事業者等の数：評価するとした事業者の割合は、セプターごとの平均を取ると約６割強程度であった。

（ウ）共通脅威分析

毎年度当初に、重要インフラ事業者等の必要性を勘案して策定する共通脅威分析の検討項目に対する年度末時点の達成度に着目し、評価指標を設定・検証を行った。

○重要インフラ事業者等へのアンケート及びヒアリング等により抽出し、分類・調査対象とした脅威の検討項目件数：７件

○上記に基づき分析・調査した結果として共通に起こりうる脅威を５つに類別したことについて、重要インフラ事業者等から適切との評価を得た。

（エ）分野横断的演習

演習参加者の拡大と演習で得られた知見が、重要インフラ事業者等の取組みに貢献したかどうかに着目し、評価指標を設定・検証を行った。

○演習の延べ参加者数：460 人

○演習で得られた知見が所属する組織の情報セキュリティ対策に資すると評価した重要インフラ事業者等の数：参加した 10 セプターのうち６セプター、17 事業者等のうち 14 者

（オ）環境変化への対応

第２次行動計画の周知機会の充実に着目し、評価指標を設定・検証を行った。

○Web サイトのコンテンツの充実度：NISC の重要インフラグループのホームページのコンテンツを充実させた。

○第２次行動計画を紹介したセミナー等の回数：６回

○セプターカウンシルや分野別横断的演習等の関係主体間のコミュニケーションの機会の回数：７回

（４）補完調査

評価指標を用いた成果検証は実態を捉えるために不可欠なものであるが、それは一側面を捉える物にすぎない。第２次行動計画の期待する結果（アウトカム）の評価をより実態に即すようにするために、評価指標では捉えられない側面を補完的に調査する必要がある。このため、IT 障害等の事例について補完調査を実施し、施策と対策を評価するため材料を得ることとする。また、前年度までの補完調査との継続性を配慮する。

（ア）補完調査～具体的事例の検証～

具体的事例の検証案件は次の２件とした。

① 非意図的要因１（外注先からの情報流出）

ａ）検証結果

○情報処理等業務を外注するにあたっては、外注先に情報流出防止を目的とした適切な情報管理体制を求めるとともに、その実効性確保のため外注先に対する適切な十分な監督、指導を行う必要があることが確認できた。

○外部への情報流出を知り得たのは、第三者からの通報によるものではなく、自身の情報流出に対する積極的な監視活動によるものであり、これらの活動が情報流出の早期発見に寄与することを確認できた。

○問題を認識した後の迅速な対応の重要性が確認できた。

ｂ）課題・留意点

○情報処理等について、自社のみならず外注先の体制も視野に入れて検討、構築していく必要があるのではないか。

○情報の外部流出について､積極的な監視態勢を取る必要があるのではないか。

○このような事例を詳細に分析し、そこから得られた教訓については情報共有をさらに進めていくべきではないか。

② 非意図的要因２（システム障害）

ａ）検証結果

○システムの改修等を行った後にシステム障害が発生する事例が多く、また想定外の要因からシステム障害が発生する場合があることが確認できた。

○また、想定外の要因がシステム障害の原因となる場合、原因の解明に予想以上の時間を要することが確認できた。

○利用者への影響の最小化を図るという観点からも障害が発生した場合に、早期復旧を可能とする方法、体制を整備することの重要性が確認できた。

b）課題・留意点

○システムの改修、増設等を行った後にシステム障害が発生する事例が多いことから、十分な事例検証を行うとともに、障害発生を想定したバックアップ体制の整備等、緊急対応策を準備しておく必要があるのではないか。

○このような事例を詳細に分析し、そこから得た教訓の共有をさらに進めていくべきではないか。

（イ）補完調査のまとめ

IT 障害が国民生活や社会経済活動に重大な影響を及ぼさないようにする観点からは、未然防止だけではなく、障害発生時の影響の最小化のための対応が重要であり、そのための事前の準備が有効である。

個々の重要インフラ事業者等の情報セキュリティ対策については、過去の経験の蓄積や安全基準等の整備、指針の浸透等の効果により、体制や規程の整備等が着実に進展しているものと考えられる一方で、IT 技術の拡大と共に複雑化が進むシステムの管理・運営がいっそう困難になったことや、従来存在しなかった新たな脅威の発生等、依然として課題が残されている。

（5）第２次行動計画に基づく施策の実施についての評価

第２次行動計画に基づく施策の実施に係る結果の評価については、別添１に示すとおりであり、概ね当初の目標に沿った進捗が認められた。

（6）総評

以上の事実により、2009 年度における取組みは当初の目標に沿った成果を上げており、個々の重要インフラ事業者等による情報セキュリティ対策の向上が進んでいるものと理解できる。

また、安全基準等の整備においては、新たに整理した改善状況、浸透状況の調査を通じ、定量的に整備状況を把握できる体制が整い、これにより自己検証の定着化が確認できた。情報共有の面では、実施細目について第２次行動計画で改善した効果があらわれ、情報共有件数が増加し、情報共有が進展するとともにセプターやセプターカウンシルの活動が本格化してきた。一方、共有すべき情報の内容等については、工夫、改善の余地があり、継続的な検討が重要と考える。共通脅威分析での検討の進展と分野横断的演習の参加者の拡大等を背景に今後も情報セキュリティ対策の向上が進むと予想される。

このように第２次行動計画を策定したときに、改善したところについては、その効果が認められつつあるものの、国民生活や社会経済活動における IT の利用は今後とも拡大を続け、関連技術が発展する一方で、IT 障害の要因や脅威は常に変化し続けるものであることから、重要インフラにおける情報セキュリティの向上に向けて継続的に取り組んでいく必要がある。

第３節　2010 年度に向けた課題

2010 年度は、第２次行動計画の２年目にあたり、同計画に基づいて重要インフラサービスの維持や IT 障害発生時の迅速な復旧等の確保に向けて継続的に各種施策に取り組んでいく。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恐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ことが重要である。

情報共有体制の強化については、これまでに整備された官民役割分担に基づき、環境整備を継続的に進めることが重要である。また、活動が本格化している「セプターカウンシル」の活動を通じ、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・強化を促進することも重要である。

「安全基準等」の整備浸透については、2010 年度に改定する「安全基準等」の指針に基づき、重要インフラ分野及び重要インフラ事業者等において作成する「安全基準等」の継続的な改善を図ることが重要である。

重要インフラ防護対策の向上については、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を継続的に実施することが必要である。また、重要インフラ事業者等における事業継続計画に関し、災害対策等と調和する情報セキュリティ対策のあり方について検討することも重要になってくる。

重要インフラ分野に関する情報の共有や活用、国際的な演習への参加といった各種活動を促進することが必要である。

第４章　企業・個人における現状の評価

第１節　2009 年度の取組み

１．2009 年度の取組みの背景

（１）企業

企業については､「企業における情報セキュリティ対策の実施状況を世界トップクラスの水準にすることを目指して引き続き最大限の努力を行う」とし、取組みを進めた。

特に、2009 年度においては、企業における情報セキュリティ対策が真に有効なものとなるよう実効性を強化し、対策を更に推進するとともに、認識不足及びリソース不足などを利用として情報セキュリティ対策を十分に実施することができない主体に対して対策の実施を図った。

（２）個人

個人については､「「IT 利用に不安を感じる」とする個人を限りなくゼロにすることを目指して引き続き最大限の努力を行う」とし、取組みを進めた。

特に、2009 年度においては、個人が様々なサービス等の利用において生じ得るリスクを認識し、そのリスクを被害に変えないための環境を整備するとともに、個人の底上げに向け、広報啓発・情報発信等を関係府省庁と連携し、より効果的に実施できるような取組みを進めた。

２．2009 年度の取組み[14]

企業・個人のうち、取組みが遅れがちな主体の対策の底上げを念頭に置きつつ、自ら自律的・継続的に情報セキュリティ対策を実施していくことを目指し、企業・個人の情報セキュリティ意識を高める施策及び企業・個人自らが自律的・継続的に行う情報セキュリティ対策を支援する環境整備の施策として、それぞれ以下の施策を推進した。

（１）企業

①情報セキュリティガバナンスの「経営の一環としての位置付け」の確立
②企業の情報セキュリティ向上に資する製品やサービスの提供促進と活動の推進
③企業における情報セキュリティ人材の育成・確保
④「事故前提社会」への対応力強化に向けた事業継続性確保・緊急対応体制等の強化
⑤中小企業の情報セキュリティ対策の推進
⑥日系企業のグローバルな事業展開を支える情報セキュリティ政策の推進

（２）個人

①情報セキュリティ教育の強化・推進
②個人の底上げに向けたより効率的な普及・啓発活動の実現

14　各施策の具体的な進捗状況については、別添１を参照。

③対策が困難な個人も含めた情報セキュリティ水準向上に向けた取組み

第２節　2009 年度の取組み及び取組みを受けた現状の評価等（2009 年度の評価等）

１．2009 年度の評価等に関する基本的考え方（評価等の視点）

企業・個人の対策実施領域においては、環境整備等の間接的な働きかけを行うことにより、情報セキュリティに関する問題の重要性と対策の必要性を自らが認識するように導くなど、IT 社会の一員としての社会的責任といった観点も踏まえた形で、各主体が自律的・継続的に取り組んでいくよう対策を促していくことが政府の施策の中心となる。

したがって、昨年度同様、この対策実施領域における評価指標[15]に関しては、すべての主体にわたる詳細な調査を行うよりは、いくつかの既存のデータを収集し、それぞれのデータの特性を考慮しつつ、企業全体・個人全体の傾向を分析する方法により実態を把握することが適当であり、このように対策の浸透の度合いについて評価等を行う。

２．評価等について（評価指標等）

企業・個人に係る評価指標は、行政活動により提供されたモノやサービスの量など、対策の浸透度を測るための評価指標である「アウトプット評価指標」と、行政活動の結果として国民生活や社会生活に及ぼされる効果を測る評価指標である「アウトカム評価指標」により、それぞれのデータの特性を考慮しつつ、企業全体・個人全体の傾向を分析、実態を把握する方法により、評価等を実施する。なお、評価等に際しては、これらの評価指標の測定時点・測定方法によっては、必ずしも対象の状況を適切に把握できない場合があることに留意し、場合によってはこれらの評価指標以外の情報も活用するなど、柔軟に実態の把握に努めることとする。

また、測定時点については 2008 年度以前の資料しか得られないデータも散見されるため、必ずしも十分なデータを収集できない。そこで、基本的には 2008 年度以前の状況について把握することを主眼に置くこととし、2009 年度の状況については、データを収集可能なものについてのみ言及する。

３．評価等の結果と総評

企業及び個人に係る評価等の結果について、以下のとおり述べる。なお、各評価指標におけるデータについては、別添６に示す。

（１）施策の取組み結果に関する評価等

（ア）企業

① 情報セキュリティガバナンスの「経営の一環としての位置付け」の確立[16]

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[17]に基づく認証取得組織

15　各評価指標については、「情報セキュリティの観点から見た我が国社会のあるべき姿及び政策のあり方【第２版】」別添４を参照。

16　別添６－１を参照。

17　「情報セキュリティマネジメントシステム（ISMS）」とは、情報セキュリティの個別の問題ごとの技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用することをいう。

数は、伸び率が落ち着きつつあるとは言え、引き続き高い水準を維持している。また、国／地域ごとでみた場合でも、全世界の取得組織数における半数以上を日本の組織で占めており、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の浸透については、世界トップレベルにあると言える。

② 企業の情報セキュリティ向上に資する製品やサービスの提供促進と活動の推進[16]

2009 年度の IT セキュリティ評価及び認証制度[18]に基づく認証取得製品数は、減少傾向ではあるものの、評価・認証中の製品を含めると高い水準で提供されていると言える。また、認証された製品・サービスを導入する企業も増加傾向にあり、取組みの効果が現れているのではないだろうか。

他方、暗号モジュール試験及び認証制度[19]に基づく認証取得製品数は、認証制度が正式運用されて間もないため、取得製品数も少なく、今後の継続的な取組みが求められる。

③ 企業における情報セキュリティ人材の育成・確保[20]

平成 21 年度春期から創設された、情報セキュリティスペシャリスト試験の受験者数及び合格者数とも、旧試験区分である、テクニカルエンジニア（情報セキュリティ）試験及び情報セキュリティアドミニストレータ試験の受験者数及び合格者数を超える勢いで増加している。また、民間の情報セキュリティ資格においても有資格者数は増加傾向にある。

反面、システム監査技術者試験については、合格者数は増加傾向にあるが、受験者数については減少傾向がみられる。

これらの試験において、受験者数の減少傾向が観測された部分については、情報セキュリティ人材の供給後退が始まらないよう、注意して観測する必要を要する。

④ 「事故前提社会」への対応力強化に向けた事業継続性確保・緊急対応体制等の強化[20]

事業継続計画（BCP）を策定している企業は年々増加傾向にあり、策定していない企業においても必要性の認識が高まりつつある。対応力強化推進のためには、必要性の認識の高まりを実際の取組みにつなげるための方策の検討が必要である。

また、情報関連事業者をはじめとする関係者間の連絡体制の構築、ウイルスや不正アクセス及び脆弱性等に早期に対応するための連携体制は進んでいる。

---

18 「IT セキュリティ評価及び認証制度（JISEC：Japan Information Security Evaluation and Certification Scheme)」とは、IT 関連製品のセキュリティ機能の適切性・確実性を、セキュリティ評価基準の国際標準である ISO/IEC15408 に基づいて第三者（評価機関）が評価し、その評価結果を認証機関が認証する、わが国の制度。

19 「暗号モジュール試験及び認証制度（JCMVP：Japan Cryptographic Module Validation Program）とは、暗号モジュールに暗号アルゴリズムが適切に実装され、その鍵やパスワードといった重要情報が攻撃者から保護されるとともに、許可された物がいつでもその機能を確実に利用できることを、暗号モジュールのユーザが客観的に把握できるように設けられた第三者適合性評価制度。

20 別添６－２を参照。

⑤ 中小企業の情報セキュリティ対策の推進[21]

中小企業のセキュリティ対策推進として期待されるASP･SaaSの利用状況は､年々増加傾向にあり、さらにその効果を多くの企業で認識している。

反面、いまだASP・SaaSについて認識不足の企業も多く存在するため、今後の継続的な普及促進が求められる。

⑥ 日系企業のグローバルな事業展開を支える情報セキュリティ政策の推進[22]

スリランカ、インドネシア、ベトナム、フィリピンなどASEAN諸国において、情報セキュリティに関するセミナーの開催協力や招待講演、企業内CSIRTの構築に資する技術セミナー等の実施により、情報セキュリティの向上に一定の成果を上げているものと考えられる。

引き続き､日系企業がより安心して投資やアウトソーシングを行える環境作りや､安心して通信インフラを利用できる環境の整備に貢献していく必要がある。

（イ）個人

① 情報セキュリティ教育の強化・推進[23]

個人の幅広い世代を対象としたインターネット安全教室は、開催規模及び参加人数の拡大がみられ、今後も継続的な推進、内容の拡充が求められる。

また、公立小中高等学校における情報モラルなどを指導する能力に関しては、約７割の教員が有すると回答しており、また、年々増加傾向にある。

今後も引き続き、児童・生徒や保護者への教育・啓発の推進、学校や地域等における教育の推進等が求められる。

② 個人の底上げに向けたより効率的な普及・啓発活動の実現[24]

個人が情報セキュリティ関連の情報を入手する方法は様々なものが存在し、情報によって入手する経路が千差万別である。

特にウェブサイト及びポータルサイト等のインターネットサービスを利用した情報の入手の割合は高いため、積極的な情報提供が有効であると言える。

他方、政府・自治体からの情報を入手して活用する割合は依然として低いため、個人に対して適切な情報入手の選択肢を提供するという意味においては有益であるが、普及・啓発活動の手法改善を図る必要がある。

③ 対策が困難な個人も含めた情報セキュリティ水準向上に向けた取組み[25]

ボット感染等、被害者が感染した事実を認識し難いことから、取組みにおける正

---

21 別添６－３を参照。
22 別添１－11を参照。
23 別添６－５を参照。
24 別添６－６を参照。
25 別添６－９を参照。

確な効果を測定する事は困難ではあるものの、日本におけるパソコンのボット感染度は世界的に見て低水準であるとのレポートも存在することから、一定の成果を上げているものと考えられる。

（２）施策の取組みによる社会的変化に関する評価等

（ア）企業

① 企業の情報セキュリティ意識に係る指標[26]

情報セキュリティ上のトラブルを重要であると認識している企業は年々増加しており、また、情報セキュリティ対策の阻害要因についても、「手間・コストがかかる」、「対策をどこまでやるべきかがわからない」とする傾向から、「企業のセキュリティ対策方針が明確になっていない」、「専門家（CIO や CISO）がいない」とする企業が増えつつあり、徐々にではあるが関心が高まりつつある。

他方、対策の効果についてはセキュリティ向上以外の効果において、「顧客・取引先からの評価の上昇」がみられるものの、「特に効果はなかった」とする企業が４割存在しており、いまだに情報セキュリティ対策が顧客や市場における評価と強力に結びついているとは言い難い。

② 企業の情報セキュリティ対策状況に係る指標

ａ）情報セキュリティ対策の確立に係る指標[27]

対策実施状況及びセキュリティ向上への寄与への実感は、年々増加傾向がみられる。特に、内部統制の整備強化については大きな改善がみられる。

引き続き、情報セキュリティ対策の実施と定着を進めていくためには、市場評価に繋がるようなメリットを生み出し、企業として取り組むことが「得策である」と認識されるような環境整備が必要である。

ｂ）情報セキュリティ対策の導入及び運用に係る指標[28]

セキュリティ対策ソフトの導入等の技術的対策については、９割程度の企業が実施しているが、セキュリティパッチの適用など運用に係る対策については、４割程度の企業でしか実施されていない。

さらに、従業員に対する情報セキュリティ教育の実施など、人的な対策についても進んでいない状況がみられる。

今後、対策ごとの実施状況を注視し、実施率の低い項目について特に必要性の認識、対策実施状況の向上を図るための取組みが求められる。

ｃ）情報セキュリティ対策の監視及びレビューに係る指標[29]

外部専門家及び内部による定期的な情報セキュリティ監査を実施する企業は増

---

26 別添６－10 を参照。
27 別添６－11 を参照。
28 別添６－14 を参照。
29 別添６－20 を参照。

加傾向にあるものの、大きな伸びは見られない。ただし、効果については８割の企業で認識している状況がある。

今後、定期的なセキュリティ監査の効果が認識されるような環境整備を進めるとともに、情報セキュリティの向上が市場評価に繋がる環境整備を図っていく必要がある。

（イ）個人

① 個人の情報セキュリティ意識に係る指標[30]

情報セキュリティに関する攻撃・脅威の認知は、年々増加している傾向がみられるが、「ボット」、「マルウェア」については、約４割程度の認知にとどまっている。また、インターネットの利用については、いまだ約８割の個人が不安を持っており、特に「ウイルスの感染」、「個人情報の保護」を脅威とする回答が多く見受けられる。

今後、適切な理解を進めるとともに、あわせて不安を払拭するための意識啓発を促進していく必要がある。

② 個人の情報セキュリティ対策状況に係る指標[31]

セキュリティ対策として、「セキュリティ対策ソフト・サービスの利用」などの技術面の対策や「不審な電子メールの添付ファイルを開かない」などの運用面の対策が高い割合で実施されている状況ではあるが、いまだ対策を行っていない個人が多く見受けられる状況がある。さらに、電子メールやUSBメモリなどの可搬媒体の「暗号化」を実施している個人については、約２割にとどまっている。

今後、喫緊に取り組むべき対策内容を適切に普及啓発・情報発信を行うことが必要である。

（ウ）企業・個人共通

① インシデント・犯罪の発生[32]

企業における被害については増加傾向を示しており、「ウイルス等の感染」、「ノートPC盗難」、「内部ネットワーク悪用」などが多くなっている。特に、「ウイルス等の感染」については、いわゆるガンブラー型攻撃の影響が大きかったのではないかと考えられる。これらの状況を踏まえ、引き続き企業における情報セキュリティ対策を推進していくことが求められている。

他方、個人についての被害は減少傾向にあるものの、被害を受けても気付かない場合、セキュリティ対策ソフト等で検出できず認知できない場合もあるため、留意が必要である。

---

30 別添６－21を参照。

31 別添６－22を参照。

32 別添６－24を参照。

②　（参考）IT を活用した経済の発展状況[33]

我が国における電子商取引市場は年々拡大している傾向にある。2009 年度の企業間取引については経済危機の影響などから落ち込みが見られたが、電子商取引化率については、いまだ拡大傾向にある。

他方、個人分野でのインターネットにおける個人情報保護への不安や、電子的決済手段の信頼性への不安については依然として減少していないため、更なる拡大には、情報セキュリティの向上及び個人の不安解消が不可欠であり、今後も各主体のセキュリティ対策の一層の推進、不安の払拭へ向けた取組みが必要不可欠である。

（３）総評

（ア）企業

前年から引き続き情報セキュリティに係る脅威の認識、情報セキュリティに関するトラブルの重大性の認識は着実に高まっている状況である。こうした認識は、システムトラブルや、依然として発生し続ける情報漏えいが報道され続けていることなどから、今後も高まっていくことが予想される。

情報セキュリティ対策については、着実に実施され、その効果についても多くの企業で認識されつつある反面、対策分野によっては約５割の企業で実施されていない状況がある。また、情報セキュリティ向上以外に及ぼす効果についても、「特に効果がなかった」とする企業がいまだ４割存在している。対策を更に推進するにあたっては、情報セキュリティ対策がもたらす企業へのメリットを提示することが重要であることは以前から指摘されていたが、この観点から、市場評価に繋がる環境の整備へ向けた取組みが実施され、一定の成果はみられるものの、いまだ改善の余地が大きく残っているため、引き続き取組みを推進していくことが求められる。

また、ウイルス等の感染、ウェブサイトの改ざん、重大な情報漏えいは減少しておらず、企業が直面する情報セキュリティ上の脅威はいまだに多く存在する。実際に被害に遭わないようにするという意味でも、企業における情報セキュリティ対策は推進されるべきである。

さらに、評価指標からは明らかではないが、「取組みが進む主体」と、コストがかかる、人材が不足するなどの理由で「取組みが遅れがちな主体」との間に差が広がりつつあり、大きな投資を行う企業が増える反面、投資をほとんど実施しない企業も増加しているとの指摘もある。このような「取組みが遅れがちな主体」に対して、費用対効果を見据えた情報セキュリティ対策の検討、市場評価へ繋がる環境の整備など、全体的な底上げへ向けた積極的な取組みが行われてきたが、これらを更に具体的な対策として明確にしていくことが求められる。

なお、情報セキュリティ対策を高水準で推進しても、リスクが現実化する可能性をゼロにはできないため、引き続き、事業継続性の確保及び緊急対応体制の整備を推進していくことが必要である。

---

[33] 別添６－27 を参照。

（イ）個人

2009 年度も引き続き、情報セキュリティ教育、広報啓発・情報発信の取組みを更に強化・充実しつつ実施しており、これらの取組み等も背景として、情報セキュリティに対する意識の向上、対策実施が着実に進んでいることが各評価指標から見てとれる。

しかし、意識の向上や対策実施の着実な伸び等、一定の成果はみられるが、基本的と思われる対策（ウイルス対策ソフトの導入、OS やブラウザのアップデート等）についてさえも、いまだに対策を実施していない層が一定程度存在する。既存の広報啓発・情報発信の取組みは一定の成果を上げているが、既存の取組みが届いていない層についてもセキュリティ向上を図ることのできる効率的・効果的な方策を検討する必要がある。

さらに、情報セキュリティに関する認識については、標的型攻撃・ボット・マルウェア等の新しい脅威に関する認識は依然低いままである。新たな脅威が常に発生しうる環境において個人の情報セキュリティを保つために、新たな脅威に対応しうる形での普及啓発・情報発信等を実施することも求められる。

第３節　2010 年度に向けた課題

１．企業

企業分野においては、リソース不足を主たる原因として情報セキュリティ対策への取組みが困難な主体が観測されるとともに、経済状況の悪化から、情報セキュリティに対する投資が減少することも危惧される。企業分野においては、

○対策が遅れがちな主体・対策が困難な主体に対して情報セキュリティの向上に向けて具体的に支援するための施策

○対策効果が実感でき、市場評価に繋がる環境等の整備のための施策

○情報セキュリティ対策を高水準で推進しても、リスクが現実化する可能性は否定できない中で、事業継続性への目配りなどリスクへの対処の重点の置き方について検討を行うこと

が重要になる。

２．個人

個人分野においては、全体的な底上げに向け特定の属性に属する者の理解度、対策実施状況に改善の余地があり、かつ新たな脅威などに関する認識の不足が懸念される。

2010 年度は、「取組みが遅れがちな主体を含めた対策」とともに、「新たな脅威の発生などの情勢の変化を踏まえた対策」が重要となると考えられ、個人分野においては、

○脅威などの新たな変化を踏まえ、情報セキュリティに関する問題の重大性と対策の必要性を認識させるような施策

○属性に応じた施策、特に既存の対策が行き届いていない個人に対する施策

○多様化する IT 利用に対応して、情報セキュリティを確保するための新たな方策についての検討

の実施が重要になる。

第５章　横断的な情報セキュリティ基盤における現状の評価等

【情報セキュリティ技術戦略】

第１節　2009 年度の取組み

１．2009 年度の取組みの背景

社会全体の IT への依存度が高まり、情報セキュリティの対象範囲と重要性が増すなか、我が国の情報セキュリティ関連技術が、世界で最も効率的・効果的に進められる体制となることを目指して政府は最大限の努力を行うことになっている。

具体的には、

①国民が安心して IT を利用できる環境の実現に向けた研究開発･技術開発を重点的に行う一方で、多様性を維持するための研究に対しては政府が積極的に取り組むこと

②抜本的な技術革新が必要になるなど困難な課題に対応するために「グランドチャレンジ型」の研究開発・技術開発を推進すること

③柔軟なプロジェクト管理の仕組みを導入するなど研究開発・技術開発を効率化するための基盤を整備すること

などを推進する。

２．2009 年度の取組み

①に係る「情報セキュリティ技術開発の重点化と多様性の維持」については、情報セキュリティ技術を網羅的に整理し、技術の進展状況を把握した上で、重点的に研究すべき技術分野の選定を行った。

②に係る「グランドチャレンジ型の研究開発・技術開発」については、研究開発の枠組み検討の一環として、研究開発において技術進展の障壁となる要因を分類し、これらの要因に対する政府関与のあり方を整理し、総合科学技術会議の情報通信 PT に報告した。

③に係る「研究開発・技術開発の効率的な実施体制の構築」の一環として、新設された研究開発プログラムにおいて、研究計画の変更が柔軟に行えるなどの公募要領の見直しを関係者と共に行った。また、情報セキュリティ技術戦略の取組みにおける将来像として示された「設計段階からセキュリティを作り込む開発手法の普及と定着」に向けた取組みとして、専門分野連携事業（ウイルスの分析を行う専門家の知見をシステムインテグレータの設計に活用できるようにする仕組みを整備する事業）を推進した。

第２節　2009 年度の取組み及び取組みを受けた現状の評価等（2009 年度の評価等）

１．2009 年度の評価等に関する基本的考え方（評価等の視点）

2009 年度の評価等の視点としては、前述の３つの重点政策に結びついている SJ2009 の各施策が着実に実施されたかという観点が挙げられる。

２．評価等の結果と総評

（１）施策の取組み結果に関する評価等

SJ2009 に基づく施策の取組み結果については､情報セキュリティ技術戦略に関わる 24 施策のうち、Ａが 22 施策、Ｂ＋が１施策、Ｂが１施策であり、ほぼ予定どおりの推進がなされた。

①に係る施策である「情報セキュリティ技術開発の重点化と多様性の維持」に係る施策については、いずれもほぼ予定どおりの進捗をみた。ただし､「短期的目標設定のなされている研究開発・技術開発の投資バランスの改善検討」については、情報セキュリティに関する研究開発・技術開発の進展状況についての予備的調査を行ったが、ポートフォリオ分析等による検討は今後の課題とした。

②に係る施策である「グランドチャレンジ型の研究開発・技術開発」については、研究開発の枠組み検討の一環として研究開発において技術進展の障壁となる要因を分析し、これらの要因に対して政府が関与すべき取組み内容の検討を行うなど、計画どおりの進捗をみた。

③に係る施策である「研究開発・技術開発の効率的な実施体制の構築」に係わる施策については､「公的な競争的資金制度におけるプロジェクト管理・評価の検討」において新設された研究開発プログラムにおける研究計画の変更が柔軟に行えるようにするなど、公募要領の見直しを関係者と共に行うなど、ほぼ予定どおりの進捗をみた。また､「投資効果に係る継続的評価プロセスの導入」については、概算要求のタイミングを活用して科学技術関係施策の進捗を把握し、改善・見直し事項の指摘及び優先度判定を行なうなど、ほぼ予定どおりの進捗をみた。

（２）施策の取組みによる社会的変化に関する評価等

情報セキュリティの研究開発・技術開発課題は「Moving Target」という特徴を持っており、リスクの変化や攻撃手法の変遷に追従していく側面も必要である。そこで、従来から認識されていたリスクと環境変化に伴う新たなリスクへの対応を分けて評価する。

従来から認識されていたリスクへの対応については、情報セキュリティ対策に資する技術の研究開発及び関連施策の施行によって確実に進んでいる。

一方、誘導型攻撃を要因とするホームページの改ざんなど、利用者のセキュリティ対策だけでは対応が困難な新たなリスクが増大している。これらの新たなリスクに対応するためのサーバ管理者側の対策は、既に開発されている技術が活用できる場面もあることから、実環境で効率的・効果的に運用するための組織・人間系の管理手法の高度化が注目される。また、クラウド・データセンターの拡大による仮想化ビジネス環境のセキュリティ課題、IP アドレスの枯渇問題を契機とした IPv6 対応におけるセキュリティ課題など､情報セキュリティが対象とすべき範囲はますます拡大かつ複雑度を増しており、これらの環境変化と新たなリスクを常に把握し、その課題を解決するための研究開発・技術開発をさらに加速することが期待される。

（３）総評

これら重点項目については、NISC 及び各府省庁において各種の取組みが行われ、情報

セキュリティ技術の高度化に向けたステップが確実に前進した。

①に関しては、情報セキュリティ技術の進展状況の調査方法を検討し、予備的調査を行ったことにより、技術開発の重点化を図る上での基礎データが得られたものと考える。

また、②に関しては、技術の進展の障壁となっている要因を分類し、これらの要因に対する政府関与のあり方を整理したことにより、グランドチャレンジ型の研究開発パッケージを具体化するための方策が得られたものと考える。

さらに、③に関しては、新設された研究開発プログラムにおいて、研究計画の変更が柔軟に行えるなどの公募要領の見直しを関係者とともに行ったことにより、競争的資金による他の研究開発プログラムについても同様の見直しを図っていく足がかりが得られたものと考える。

第３節　2010 年度に向けた課題

①に係る「情報セキュリティ技術開発の重点化と多様性の維持」については、情報セキュリティ技術を網羅的に洗い出した上で、技術の進展状況について予備的調査を行ったが、中長期的に取り組むべき重点課題の選定においては、個別技術の進展状況の詳細な調査に加えて、社会へのインパクトの大きさや政府関与の必要性についても確認する必要がある。また、情報セキュリティ技術開発の多様性を維持する観点において、ポートフォリオ分析による検討を継続して進める必要がある。

②に係る「グランドチャレンジ型の研究開発・技術開発」については、今後、重点課題を選択した上で、政府が関与すべき取組み内容を具体化する必要がある。

③に係る「研究開発・技術開発の効率的な実施体制の構築」については、本年度対象としたもの以外にも競争的資金による研究開発プログラムは多種のものがあり、現状としてはルールも様々であることから、競争的資金の使用ルールの統一化など科学技術政策全体の動きの中で、「研究計画の柔軟な変更等」を実現していくことが望ましい。

【情報セキュリティ人材の育成・確保】

第１節　2009 年度の取組み

１．2009 年度の取組みの背景

2009 年度においては 2008 年度以前から継続されていた専門家人材の育成について、人材育成・確保の特性上、継続的な取組みが求められてきた。

加えて、情報セキュリティ事故が相変わらず発生し続けていることなどから、情報セキュリティを専門としない人材を含む広い層への普及啓発も求められている。

２．2009 年度の取組み

2009 年度においては、情報処理技術者試験の改革や先導的 IT スペシャリスト育成推進プログラムによる情報セキュリティ人材育成拠点の整備、新設された情報セキュリティ月間等による普及啓発の両面から各種施策が着実に実施された。

第２節　2009 年度の取組み及び取組みを受けた現状の評価等（2009 年度の評価等）

１．2009 年度の評価等に関する基本的考え方（評価等の視点）

人材の育成・確保は成果が出るまでに時間のかかる分野であり、取組みのたゆまぬ継続が求められる。2009 年度もそうした特性の例外ではなく、具体的・継続的な取組みが行われているかという視点が挙げられる。

さらに、事故前提社会の自覚という大目標から見ると、専門家だけでなく社会を構成するすべての人を対象とした普及啓発も求められるため、普及啓発が効果を挙げているかどうかと言う視点も加える。

２．評価等の結果と総評

（１）施策の取組み結果に関する評価等

SJ2009 に基づく施策の取組み結果については、別添１のとおりである。全 21 施策のうち、Ａが 21 施策と順調に施策の取組みがなされた。

情報セキュリティ分野における世界最高水準の人材育成については、産学及び大学間の効果的な連携体制が構築されるとともに、実践的な教育カリキュラム、教材、教育方法等が開発され､学生のスキル向上等の教育効果も確認されるなどの成果が認められた。

一方で全国展開を行うための普及展開、補助期間終了後の恒常的な教育実施等に課題が残されている。

（２）施策の取組みによる社会的変化に関する評価等

政府においては各種施策が着実に進められている。また、民間分野においても様々な取組みが実施されると共に､「情報セキュリティ人材育成シンポジウム」の開催や「セキュリティ普及促進委員会」の設立等官民連携による取組みもみられる。

こうした取組みの成果などもあり､民間資格の取得者数は概ね 10%前後のペースで増加している傾向がみられ、専門家のスキル習得へ向けた動きは依然として活発であると

言える。

他方、普及啓発においては、「企業」・「個人」の項目で前述したように情報セキュリティ対策を実施している割合が微増にとどまっている等、更なる取組みの余地が残っている。

（３）総評

2008 年度からの施策が着実に継続されているが、専門家人材の育成・確保については、不況のため民間の投資が減少しているという報告もあり、国に対しては施策の継続のみならず拡充が求められている。

他方、情報セキュリティの普及啓発においては、「情報セキュリティ月間」の新設等、積極的な取組みも行われ、一定の効果がみられた。しかしながら、情報セキュリティに係る課題は解消されておらず、普及啓発効果のさらなる向上を図るためには、新たな枠組みによる画期的な取組みを試みる時期に来ている。

第３節　2010 年度に向けた課題

2010 年度からは、経済危機の影響から民間の人材育成投資に戻りが見られない場合も考慮して、専門家人材の育成に向けた施策を引き続き実施していくことが求められる。その中で、官民連携のより一層の充実や産学連携の推進等、組織の垣根を越えた協力によって個別の活動を超える効果を上げるための工夫が求められる。

また、普及啓発については国民意識の向上という観点における停滞を打破するために、新たな枠組みを検討して今までの施策以上に効果的な普及啓発を実施することが求められている。それと併せて、2009 年度に新設された「情報セキュリティ月間」を盛り上げ、国民における認知度を高めることで、普及啓発本来の役割を十分に発揮できるようにすることも必要である。

【国際連携・協調】

第１節　2009 年度の取組み

１．2009 年度の取組みの背景

IT 基盤は、24 時間 365 日、常時世界とつながっていることから、一国のみで情報セキュリティ対策を行うことには限界がある。2009 年には、米国と韓国に対する大規模な DDoS 攻撃が発生するなど、改めて国際レベルにおける協力・連携の必要性が再認識された。

２．2009 年度の取組み

我が国の官民連携を中心とした取組みが世界最先端・最高のベストプラクティスとして世界に貢献することを目標とし、2009 年度には以下の施策を重点的に推進した。

①情報セキュリティ政策に関する POC（海外連絡窓口）機能の強化と情報共有の促進
②世界の脅威動向を把握するための官民連携の確立と、効率的・効果的国際連携活動の推進
③アジアにおける知恵の集結と情報セキュリティ水準の向上
④経済活動のグローバル化に対応した情報セキュリティの確保
⑤標準化を含んだ我が国の戦略的貢献の実現
⑥情報セキュリティ文化の醸成

第２節　2009 年度の取組み及び取組みを受けた現状の評価等（2009 年度の評価等）

１．2009 年度の評価等に関する基本的考え方（評価等の視点）

国際連携・協調分野においては、国外のステークホルダーとの信頼関係の醸成や、特定領域での取組みに関する国際的なコンセンサスが得られるまでの時間が一定期間必要であることから、他の分野に比して、中長期的な視点で考える必要性が高いことに留意するべきである。

他方で、国際会合や多国間の枠組みに単に参加するたけではなく、中長期的な視点を持ちつつも、単年度ごとの成果を積み重ねていく必要がある。

２．評価等の結果と総評

（１）施策の取組み結果に関する評価等

SJ2009 に基づく国際連携・協調に係る施策の取組みについては、別添１のとおりであり、全 22 施策のうち、Ａが 22 施策と順調に主要６施策への取組みがなされた。

①の施策については、多国間の枠組みや、二国間の会合の場を活用し、我が国の情報セキュリティ戦略・体制に係るプレゼンスの明確化、広報活動の推進の観点から積極的な貢献を行ったことで、NISC が POC として国際的な認知を得つつある。特に、重要情報インフラ防護に関する多国間会合である MERIDIAN においてプログラムの内容を検討するプログラム委員会への参加や、制御システムセキュリティに関するワーキンググループを我が国に招致するなどの貢献を行った。

②の施策については、国内の関係機関との連携を図りながら、IWWN（国際監視・警戒ネットワーク）などの国際会議において、情報共有ルール構築の議論に参加した。また、海外の CSIRT 構築や運用支援などを通じて、海外の関係機関との連携強化を推進した。さらに、ネットワークオペレータ間の連携を開始するため、我が国及び ASEAN 各国の POC 情報を収集した。

③の施策については、2009 年 10 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」を我が国で開催し、ASEAN 諸国との間における政府のセキュリティレベル向上に関する協力関係の構築を検討。また 2010 年３月にタイで開催された「第２回日・ASEAN 情報セキュリティ政策会議」（以下「日・ASEAN 政策会議」という。）では、地域で共通する情報セキュリティ上の課題について議論を深めた。

CSIRT 間連携においては、データの観測・分析の研究などに関する連携枠組みである APCERT（Asia Pacific Computer Emergency Response Team）のインターネット定点観測情報共有システムワーキンググループにおける活動を推進した。

④の施策については、第２回日・ASEAN 政策会議において、我が国が共同議長を務めるなど積極的に参加したほか、今後の日・ASEAN における情報セキュリティに関する協力事項を定めた「連携枠組み」を採択した。また、2009 年２月に我が国で開催された第１回日・ASEAN 政策会議で決定された取組みを着実に実施した。

⑤の施策については、2009 年度も関連する国際会合などへの出席を通して、情報の収集を行うとともに、積極的な提案や議論への参加など我が国からの情報発信・貢献に努めた。

⑥の施策については、第２回日・ASEAN 政策会議において、人材育成、意識啓発を各国が協力して推進することが合意されたほか、各種国際会合において、我が国のベストプラクティスを発表することで国際的な意識啓発の向上に努めた。

（２）施策の取組みによる社会的変化に関する評価等

日・ASEAN 政策会議の開催や、合意された連携枠組みの実施により、ASEAN 地域における情報セキュリティ対策の推進に貢献。結果として、情報セキュリティの面から、日本企業がより安心して投資やアウトソーシングを行える環境作りや、安心して通信インフラを利用できる環境の整備に貢献した。

（３）総評

主要６施策の実現に向けた基盤の構築は概ね達成できた。

①については、国際連携・協調のための基盤となる POC 機能の充実化においては、国際的な認知が獲得できつつあるほか、国際会合などにおいて我が国からベストプラクティスなどについて情報の発信を行っている。他方で、国際会合や枠組みが増加していることを踏まえ、我が国に最も有益な会合を選択・集中することにより、協力関係を強化すべき会合や、国の優先順位を見極めた上で、個別分野における具体的な協力関係の構築を図る必要がある。

③及び④については、日・ASEAN 政策会議にみられるようなリージョナルな関係の構築に力をいれながら、具体的な施策の実現に向け取組んでいるところである。今後は、

リージョナルな活動の成果をグローバルな活動とリンクさせる取組みも重要となる。

②、⑤及び⑥については、グローバルな視点が必要な分野であるが、サイバー攻撃の手法は日々進化しており、議論百出の状況である標準化については流動的要素が強いほか、情報セキュリティ文化醸成には各国と連携した活動が重要となることから、今後も社会情勢の変動などを視野におきつつ柔軟な取組みが必須となる。

第３節　2010 年度に向けた課題

2009 年の米韓への大規模サイバー攻撃のように IT 障害の影響が一国内にとどまらないこと、我々の社会経済活動が国内のみで行われるものではないこと、さらには国家の国際的相互依存関係が深化しつつあることを考慮し、引き続き中長期的な視野に立って国際的な安全・安心の基盤づくり・環境の整備への貢献につき、多国間の枠組みを基本として取組む必要がある。

そのため、2010 年度は、社会情勢の変動を踏まえつつ、主要６施策におけるリージョナルな施策とグローバルな施策を有機的に結び付けていくことが肝要となる。これら施策の実施に際しては、中長期的な視点を持ちつつも、一年ごとの着実な成果につなげる必要がある。なかでも、近年諸外国においても情報セキュリティに関する意識啓発に積極的に取組んでいることから、多国間、二国間の枠組みを通じて、意識啓発の分野のベストプラクティスの交換、共同イベントの開催等に取組むことは検討に値すると思われる。

【犯罪の取締り及び権利利益保護・救済】

第１節　2009 年度の取組み

１．2009 年度の取組みの背景

インターネットを始めとする情報通信技術の利活用に伴い、国民生活や経済活動への情報通信技術への依存度は高まっている。一方で、2008 年中に都道府県警察の相談窓口で受理したサイバー犯罪等に関する相談件数は 81,994 件で前年より 12.0%の増加であるなど、サイバー空間における不法行為等による国民の不安感は増大する傾向にあった。また、情報通信技術を利用した新たなサービスが出現していることから、これらを利用したサイバー犯罪の発生に警戒しつつ、犯罪の取締り、権利利益の保護・救済を一層推進することが必要となってきていた。

２．2009 年度の取組み

2009 年度においては、警察による取締り態勢の強化、取締り、国際連携の強化、広報啓発を進めてきた。併せて官民連携に向けた取組みを推進しており、ファイル共有ソフトを利用した著作権法違反事件の一斉取締りが行われるなど、権利利益の保護・救済についても取組みが推進された。また、インターネット・オークションにおける盗品の流通防止対策について、有識者、関係事業者等で構成する総合セキュリティ対策会議で検討して報告書をまとめた。さらに、民間団体等で構成される「児童ポルノ流通防止協議会」の発足に協力した。

第２節　2009 年度の取組み及び取組みを受けた現状の評価等（2009 年度の評価等）

１．2009 年度の評価等に関する基本的考え方（評価等の視点）

犯罪の取締り及び権利利益保護・救済に係る取組みに関する評価等については、施策の実施から実際の効果（アウトプット）が現れるまでに時間を要するため、中長期的な視点で把握する必要がある一方で、短期的には施策の実施がどれだけ着実に行われているかに着目すべきである。

その上で、2009 年度の評価等の視点としては、サイバー空間における犯罪の動向の変化等を踏まえて、捜査能力や態勢の構築、法制度の整備等により、リスクを減少させることができたのかという視点が必要である。

２．評価等の結果と総評

（１）施策の取組み結果に関する評価等

SJ2009 に基づく犯罪の取締り及び権利利益保護・救済に係る施策の取組みについては、別添１のとおりであり、全 15 施策のうち、Aが 13 施策、B＋が１施策、Bが１施策と、概ね順調に取組みがなされたものの、一部の施策に滞りがあった。

サイバー犯罪の取締り及び権利利益の保護救済のための基盤整備については、全国の警察職員に対する各種研修の実施や取締りの強化、捜査・解析用資機材の充実・強化、情報技術の解析に係る国際会議の開催により知見の集約・体系化・相互活用を図るなど

諸外国の関係機関との連携等が推進された。一方、サイバー犯罪条約を締結するための法整備等は所要の法案が国会において廃案となったため、今後条約締結等のためにどのような法整備が必要か等の観点から検討していく必要がある。

（２）施策の取組みによる社会的変化に関する評価等

取締り態勢の強化によって、警察におけるサイバー犯罪の検挙は着実に進められており、2009 年度のサイバー犯罪の検挙件数は 6,690 件（前年より 369 件（5.8%）増加）であった。また、官民の連携による違法情報対策にも進展が見られ、児童ポルノ流通防止協議会はインターネット上での児童ポルノの流通の防止対策を推進するため平成 21 年３月、「児童ポルノ掲載アドレスリスト作成管理団体運用ガイドライン」を作成した。

しかし、2009 年中に都道府県警察の相談窓口で受理したサイバー犯罪等に関する相談件数は 83,739 件であり、前年に比べ 2.1%増加している。2009 年においては、不正アクセス禁止法違反の認知件数が 2,795 件と前年と比べ 506 件増加するなど、サイバー犯罪の増加傾向は続いている。また、企業の Web サイトが不正アクセスによりウイルスを埋め込まれ、当該サイトの閲覧者がウイルスに感染する事案が相次いで発生するなど、国民が安全に安心して情報通信技術を利用できる状況には至っていない。

（３）総評

サイバー犯罪の取締り及び権利利益の保護・救済については、継続的な取組みが進められており一定の進展がみられるものの、サイバー空間での犯罪や不法行為はなお多発、巧妙化している状況にあり、第４章で述べたとおり、情報通信技術の利用にあたっての国民の不安も軽減されていない。

第３節　2010 年度に向けた課題

一定の施策の取組みがなされているものの、サイバー空間での犯罪や不法行為はなお多発、巧妙化している状況にある。サイバー犯罪の取締りのための態勢の強化など施策の着実な実施を行うほか、サイバー犯罪に適切に対処すべく、サイバー犯罪条約締結の早期締結に向けた法整備等の方策を引き続き検討するとともに、犯罪対策閣僚会議において決定される「児童ポルノ排除総合対策」に基づく、既存の議論の枠組みにおける児童ポルノ流通の防止対策を始めとした違法情報対策を推進する必要もある。

別添

別添１

「セキュア・ジャパン2009」に盛り込まれた施策の実施状況

＜進捗状況分類＞

分類	内容
A	当初の予定どおり推進することが出来た施策。 なお、施策は推進できたが、体制や人員に関して問題が存在するため、今後、継続して推進するためにそれらの解決が必要であるということが、当該施策に関連した作業の進捗や担当へのヒアリング等から明白になった施策については「'」を付した。
B＋	年度内には完了していないが、着実に取組みを進めており、数ヶ月以内には完了する施策。
B	予定どおり推進することは出来なかったが、今後も取組みを続けることにより、今後の見通しが立つ施策。
C	予定どおり推進することはできず、今後の見通しも立たない施策。
－	予定どおり推進することが出来なかったが、その理由が政府機関の事情によるものではない施策。

第3章　2009年度に取り組む重点政策

第1節　対策実施4領域における取組みの推進と政策目的の着実な実現

(1) 対策実施4領域

①政府機関・地方公共団体

[政府機関]

(ア) 全ての政府機関において能動的に情報セキュリティ対策に取り組む体制の確立

1) PDCAサイクルの各プロセスにおけるマネジメントの強化

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	情報セキュリティガバナンスの確立に向けた取組み	全府省庁	・各府省庁において、最高情報セキュリティ責任者及び最高情報セキュリティアドバイザーを設置、又は設置を検討しており、情報セキュリティガバナンスの確立に向けて取り組んでいるところ。	A
イ) a)	各政府機関でのPDCAサイクルの定着と浸透	全府省庁	・各府省庁において、政府機関統一基準を踏まえた省庁対策基準に基づき、PDCAサイクルの定着及び組織全体への浸透に取り組むとともに、情報セキュリティ対策についての対策実施状況報告を全職員・全システムを対象として実施。	A
イ) b)	政府全体でのPDCAサイクルの定着と浸透	内閣官房 全府省庁	・内閣官房において、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、政府全体としてのPDCAサイクルの定着に取り組んでいるところ。	A
ウ)	情報セキュリティ報告書作成のためのガイドラインの策定等	内閣官房 全府省庁	・平成21年5月以降、情報セキュリティ報告書専門委員会を4回開催し、情報セキュリティ報告書作成のためのガイドラインの策定等について報告書をとりまとめ、第23回情報セキュリティ政策会議にて報告。	B＋
エ)	政府機関統一基準の見直しの実施	内閣官房	・これまでの政府機関対策を通じて得られた知見等に基づき、政府機関統一基準の見直しについて検討を行い、平成21年度修正版を第23回情報セキュリティ政策会議にて決定。	B＋
オ) a)	情報セキュリティ対策関連情報の提供	内閣官房	・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、内閣官房において、政府機関統一基準に係るアドバイス等の情報提供を随時実施。	A
オ) b)	情報セキュリティ対策の府省庁共通的課題に対する取組み	内閣官房 全府省庁	・政府機関の保有する公開ウェブサーバ及び電子メールサーバの集約化に向け、各府省庁において、業務・システム最適化計画の枠組みを活用しつつ、集約化計画を策定し、第23回情報セキュリティ政策会議にて報告。	A
オ) c)	各府省庁における自己点検及び監査の効率化	内閣官房	・内閣官房において、各府省庁が対策実施状況報告を行う際の集計ツール、第4版読替えツール等の支援ツールを提供済み。	A
オ) d)	各府省庁の情報システムの一元的把握	内閣官房 総務省 全府省庁	・各府省庁において、各々が整備する情報資産台帳等へのセキュリティに関する事項を記載する取組みを進めているところ。	A'
カ)	コンピュータウイルスなどに起因する情報流出への対応	全府省庁	・各府省庁において、政府機関統一基準を踏まえた省庁対策基準に基づき、情報管理を徹底。	A
キ) a)	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等の活用	内閣官房 全府省庁	・各府省庁において、平成21年度も引き続き必要に応じて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を実施、又は検討しているところ。	B
キ) b)	情報セキュリティ監査制度の活用	内閣官房 全府省庁	・各府省庁において、平成21年度も引き続き必要に応じて国際規格に準拠した管理基準に基づく情報セキュリティ監査制度の活用を実施、又は検討しており、活用に向けた取り組みは着実に進んでいる。	B
キ) c)	「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	内閣官房 経済産業省	・経済産業省において、平成21年3月、「情報システムの信頼性向上に関するガイドライン」を改訂・公表し、普及を図った。	A
ク)	PDCAサイクルの確認等を支援するツールの開発・提供	経済産業省	「情報システムの構成機器等のセキュリティ要件確認を支援するツール」開発に伴うセキュリティ要件などを検討するため、有識者による検討委員会を設置（4回開催）。ツール開発に着手。（開発完了は平成22年度を予定）	A

（続く）

（続き）

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ケ）	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 関係省庁	・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の実施状況を重層的にチェックする仕組みを検討し、一定の方向性について合意を得た。	B＋

2）政府機関における人材の育成・確保及び職員の意識啓発

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア）	政府職員向け教育プログラムの充実	内閣官房 総務省	・内閣官房において政府統一的な教育プログラムについて、政府機関統一基準（第4版）に対応した教材のひな形を作成し各府省庁に提供済み。	A
イ）	情報セキュリティ関連業務の調査等	内閣官房	・各府省庁における情報セキュリティ関連業務に携わる人材に求められるスキルについて、各府省庁の最高情報セキュリティアドバイザーの協力を得て取りまとめた。	A
ウ）	人材育成・確保実行計画の実施	内閣官房 総務省 全府省庁	・各府省庁において、「行政機関におけるIT人材の育成・確保指針」に基づいて策定した「行政機関におけるIT人材育成・確保実行計画」に基づき、人材の育成・確保に取り組んでいるところ。	A
エ）	民間専門家の活用の促進	全府省庁	・各府省庁において、最高情報セキュリティアドバイザーの設置等、情報セキュリティ対策に係る民間専門家の積極的な活用を図っているところ。	A
オ）	政府職員の人材育成の促進	全府省庁	・各府省庁において、階層別研修等を活用して、全職員の情報セキュリティに関する意識の向上を推進しているところ。	A

3）情報セキュリティ対策を適時に行うための予算面での取組み

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア）	予算面での取組み	全府省庁	・各府省庁において、「成果重視事業」制度の活用等を通じて、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みを進めているが、不十分である。	B

4）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

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア）	運用・管理を委託している情報システムの情報セキュリティ対策の強化	全府省庁	・各府省庁において、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みを進めているところ。	A'

5）技術面の知見を蓄積・活用する仕組みの構築

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア）	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 経済産業省	・内閣官房では、情報セキュリティ関係の独立行政法人や団体などを訪問し、所属する研究者・実務家と意見交換することでその知見を蓄積・活用するとともに、連携強化の方策について検討しているところ。	B＋

6）情報セキュリティに関連する法令との整合性確保

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア）	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	内閣官房において、情報セキュリティと関連が深いと考えられ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、各制度との整理を行っているところ。	B＋

（イ）政府全体を通じて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	進捗状況分類
ア）	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 関係府省庁	・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本年度3回実施。	A
イ）	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	・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）等の場において意見交換を実施。	A
ウ）	安全性・信頼性の高いIT製品等の利用推進	内閣官房 全府省庁	・各府省庁において、平成21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。	B
エ）	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 経済産業省	・独立行政法人情報処理推進機構（以下、「IPA」という。）において平成19年度に開発した、ITセキュリティ要件、ITセキュリティ評価制度及び認証制度の認証可否を確認する際の支援ツール「調達におけるセキュリティ要件検討支援ツール（SRAS）」に公開されている認証製品の内容を詳細に提供する機能を追加し、利用者限定で運用開始（平成21年5月）。	A
オ）	政府情報システム等の調達時における第三者認証制度の適用範囲の明確化	内閣官房 経済産業省	・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」がある場合について、その明確化を図るべく必要な検討を行っているところ。	A
カ）	高セキュリティ機能を実現する次世代OS環境の評価及び性能向上	内閣官房 内閣府 総務省 経済産業省	・セキュアVMの1つである「BitVisor」を用い、政府機関内の利用を想定したセキュアな環境を構築し、導入・運用面の評価を実施した。また、政府機関が「セキュアVM」を導入するための調達面及び機能面の要件を整理し、当該要件をXenやVMware等の汎用的な仮想化製品がどの程度満たしているかの比較評価を行なって、これらの評価結果を報告書として取り纏めた。	A

(ウ) 電子政府の利便性・セキュリティレベルの向上

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	電子政府の利便性・セキュリティレベルの向上の検討	内閣官房 総務省 経済産業省	・電子政府ガイドライン作成検討会において、行政運営の効率化・高度化を勘案した上で行政サービスの利便性を向上させつつ、適切なセキュリティレベルを確保するためのガイドラインを策定。現在、パブリックコメント対応を実施しているところ。	B＋
イ)	電子認証ガイドラインの策定及び利用の検討	内閣官房 経済産業省	・電子政府ガイドライン作成検討会　セキュリティ分科会において、政府機関における電子認証の在り方についてガイドラインを策定。現在、パブリックコメント対応を実施しているところ。	B＋

(エ) 政府機関における事業継続性確保・緊急対応能力の強化に係る検討

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	業務継続計画の策定の推進	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ICT部門における業務継続計画の策定を進めているところ。	B
イ)	重要なシステムや情報のバックアップ体制についての現状把握等	内閣官房 総務省	・内閣官房において、各府省庁の保有する重要なシステムや情報のバックアップ体制等について現状把握を行い、政府横断的な方向性の検討に着手。	A
ウ) a)	GSOCの分析・解析能力の強化	内閣官房 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、分析・解析能力の強化に向けた取組みを実施。	A
ウ) b)	情報保証に係る最新技術動向等の調査研究	防衛省	・平成20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調査及び防衛省における一元的な対処体制等検討に関する調査研究を平成21年10月から開始した。インターネット上に潜在する脅威動向から各種サイバー攻撃手法を調査し、各種特性から特徴があるサイバー攻撃について調査分析を実施（平成22年3月までに完了）。それを踏まえ、防衛省としてサイバー攻撃に対する情報保証上必要な機能・対処方法・体制について検討した。	A
エ) a)	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。	A
エ) b)	サイバー攻撃等に係る分析・対処及び研究の推進	防衛省	・サイバー攻撃に関する分析・対処能力をさらに向上させるためのアクティブ防御を実現するネットワークセキュリティ分析装置の研究試作の基本設計を完了し、詳細設計、製造作業を引き続き実施中（平成22年度まで）。また、定点観測サイトを用い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平成20年度に引き続き実施。	A
オ)	サイバーテロに関する対策の強化	警察庁 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を整備している。また、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、公安調査官を対象に、外部有識者による技術的な内容の講義を含めた各種研修を実施し、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。また、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。	A

(オ) 独立行政法人等の情報セキュリティ対策の推進

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	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	内閣官房 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、第21回情報セキュリティ政策会議で調査結果を報告・公表。平成21年度末にも再度進捗状況を調査しており、第24回情報セキュリティ政策会議にて結果を報告し、その後公表予定。	A
イ)	独立行政法人等の情報セキュリティ対策の改善に向けた環境整備	内閣官房	・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している。	A
ウ)	情報セキュリティ対策に係る事項の中期目標への明記	独立行政法人等 所管府省庁	・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。平成21年度末に進捗状況を調査しており、その後の情報セキュリティ政策会議にて結果を報告・公表予定。	A
エ)	各独立行政法人等におけるPDCAサイクルの構築	独立行政法人等 所管府省庁	・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PDCAサイクル構築に向けた取組を実施しているところ。平成21年度末に進捗状況を調査しており、第24回情報セキュリティ政策会議にて結果を報告し、その後公表予定。	B＋
オ)	緊急時等の連絡体制の整備	内閣官房 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。平成21年度末に進捗状況を調査しており、第24回情報セキュリティ政策会議にて結果を報告し、その後公表予定。	A

(カ) その他個別の情報セキュリティ対策の推進

1) 政府機関の情報システムのIPv6対応化

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	電子政府システムのIPv6 対応化	内閣官房、総務省及び全府省庁	・総務省において、平成19年8月より開催した「インターネットの円滑なIPv6移行に関する調査研究会」において、IPv6対応化を実現するためのアクションプランをとりまとめ、平成20年6月に公表。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平成21年3月に公表したところであり、引き続き調査の上、平成22年3月に調査結果を更新・公表した。	A

2) 政府機関への成りすましの防止

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	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 全府省庁	・内閣官房において、政府機関における基盤となる情報システムの整備状況、電子メールの成りすまし等に効果的な送信ドメイン認証の普及状況等について調査・課題の抽出等を実施。平成21年度は各府省庁における送信ドメイン認証の普及促進を実施しているところ。	B＋
イ)	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	総務省 全府省庁	・総務省において、平成21年3月に政府ドメイン名の利用状況調査を実施済。国の政府ドメイン利用の取り組みについても紹介することについて検討中。	B

3) 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	進捗状況分類
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 全府省庁	・第2次情報セキュリティ基本計画において整理された、新たに安全性が低下した暗号からの移行については、各府省庁における緊急対応計画の策定を支援。 ・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22年3月に平成21年度の検討結果を取りまとめた。 ・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」の改訂に向けた、暗号技術の公募を平成21年10月1日から平成22年2月4日まで行い、6件の応募があった。平成21年度は、応募された暗号技術に関する評価基準の検討を行った	A
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 全府省庁	・各府省においては、平成21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。 ・IPAにおいて、暗号モジュール試験及び認証制度に基づく認証を新たに2件実施したほか、暗号アルゴリズム試験により実装が確認された製品のべ14件を新たに暗号アルゴリズム確認登録簿に登録した。	B＋

[地方公共団体]

(ア) 小規模な地方公共団体も含めた合理的・自主的な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	進捗状況分類
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	・平成21年4月から5団体にBCP策定支援アドバイザーを派遣。 ・平成21年11月から「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」の見直し中。 ・平成21年10月にBCP普及セミナーを山梨県で開催。他のセミナーにおいても、BCP普及のための講演を行った（16回）。	B＋

(イ) 複数地方公共団体間での情報セキュリティ対策の連携に向けた取組みの応援

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
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	・平成21年6月から19団体に内部監査アドバイザーを派遣。 ・複数団体間での情報セキュリティベストプラクティスをLGWAN内のポータルサイトにおいて紹介。	A

(ウ) 地方公共団体の取組みを応援する主体の強化

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
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	・LGWAN内のポータルサイトにおいて情報セキュリティに関する解説等の提供を行った。	A

(エ) 地方公共団体が担う幅広い行政分野での対応促進

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
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	内閣官房 総務省 文部科学省	・e-ラーニングによる情報セキュリティ研修を教育委員会まで拡大。 ・教育指導主事会議で情報セキュリティに関する情報提供を実施。	A

(オ) 地方公共団体間、地方公共団体と政府機関間でのベスト・プラクティスの相互活用の促進

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
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	・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情報を含め、コンテンツの充実を図った。	A

(カ) 地域の情報セキュリティ対策の担い手の育成支援

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	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平成21年7月から9月まで実施し、約43,500人が受講。	A

第3章　2009年度に取り組む重点政策

第1節　対策実施4領域における取組みの推進と政策目的の着実な実現

(1) 対策実施4領域

②重要インフラ

(ア)「安全基準等」の整備及び浸透

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	指針の継続的改善	内閣官房	・改定案は、第26回重要インフラ専門委員会（平成21年7月7日開催）において承認を受け、パブリックコメントを実施した（7/22から8/24）。パブリックコメント結果を反映した最終案は、第23回情報セキュリティ政策会議で審議・決定され、指針第3版として公表される予定。	B＋
イ)　a)	安全基準等の継続的改善	重要インフラ所管省庁	・各重要インフラ分野において安全基準等の分析・検証は実施済。指針改定を受けた安全基準等の分析・検証及び改定については、指針第3版の決定がなされていないことから、現在検討中。	B＋
イ)　b)	電気通信事業における情報セキュリティマネジメントの強化	総務省	・電気通信事業における情報セキュリティマネジメントに関する認証制度の導入等の普及促進に向けて、民間における検討の場として、安心・安全インターネット推進協議会にISM-TG検討SWGを設置した（平成21年6月）。また、情報セキュリティマネジメントガイドラインの国内規格化については、国内標準化機関と調整を進めているところ。	B
イ)　c)	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	・平成21年7月28日に情報通信審議会情報通信技術分科会一部答申（ネットワークのIP化に対応した電気通信設備に係る技術的条件のうち電気通信事故等に関する事項）で、総務省の他、各事業者、関係団体、専門家等が参画・連携し事故を詳細に分析・評価等を行うため、本審議会に「電気通信安全・信頼性委員会（仮称）」の体制整備が必要である旨の答申があり設置に向けた検討を実施中。	A
イ)　d)	安全基準等の継続的改善状況等の把握及び検証	内閣官房	・重要インフラ所管省庁の協力を得て調査を実施済。平成22年4月中に、内閣官房にて調査結果を取りまとめた。重要インフラ専門委員会終了後、公表予定。	B＋
ウ)	安全基準等の浸透	内閣官房 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て、平成21年度の調査を実施。重要インフラ専門委員会で調査結果を報告後、公表する予定。 ・重要インフラ所管省庁の協力を得て、平成22年1月から3月に企画・調査の準備を実施。平成22年10月を目処に調査結果を取りまとめた後、公表する予定。	B＋

(イ) 情報共有体制の強化

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	共有すべき情報の整理	内閣官房	・IT障害に関する情報について、未然防止、拡大防止・迅速な復旧、再発防止の3つの側面を踏まえた共有対象とする情報についての整理・検討作業を実施。共有方法等の基本的な整理のマトリクス案のとりまとめを行った。	A
イ)　a)	情報共有ルールの見直し	重要インフラ所管省庁	・重要インフラ所管省庁と各セプター間の情報共有ルールについて、「「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」の情報連絡・情報提供に関する実施細目」との整合性の確認等を実施。また、セプターに対し、セプター内ルールと実施細目と整合性確保に関する助言を行うとともにセプターにおける情報共有ルールの確認を行った。	A
イ)　b)	第2次行動計画の情報連絡・情報提供に関する実施細目の見直し	内閣官房	・「「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」の情報連絡・情報提供に関する実施細目」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、実施細目のレヴューを実施した。	A
イ)　c)	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	・平成21年9月にシステムの信頼性に関する取組状況を把握する「信頼性自己診断ツール」を公表し、今後、企業から提供のあった情報をマクロ的に定量分析・解析する環境を整備した。	A
イ)　d)	セプター訓練の実施	内閣官房 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て平成21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。その結果をとりまとめ重要インフラ所管省庁およびセプターへ報告済。	A
ウ)	セプターの強化	内閣官房 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て、平成21年度末の各セプターの特性、活動状況を把握するとともにセプター特性把握マップを取りまとめた。重要インフラ専門委員会に報告後、公表する予定。	B＋
エ)	セプターカウンシルの支援	内閣官房	・セプターカウンシルの事務局として、総合的な企画調整・運営を行う幹事会と具体的な活動を行うWG等の運営を通じ、カウンシルの活動を支援している。	A

(ウ) 共通脅威分析

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	共通脅威分析の実施	内閣官房	・有識者・各重要インフラ分野委員・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」（平成21年7月設置）における議論を踏まえ、重要インフラ事業者等と個別打ち合わせを行いながら、脅威分析を実施。平成22年3月中に分析結果を取りまとめた。重要インフラ専門委員会に報告後、公表する予定。	B＋

(エ) 分野横断的演習

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	分野横断的演習の実施	内閣官房 重要インフラ所管省庁	・有識者・各重要インフラ分野委員・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」（平成21年7月設置）におけるシナリオ等についての議論を踏まえ、平成21年11月27日に116名の参加を得て分野横断的な演習を実施し、平成22年3月に結果を取りまとめた。重要インフラ専門委員会に報告後、公表する予定。	B＋
イ)	電気通信事業分野におけるサイバー攻撃への対応強化	総務省	・電気通信事業者やメーカ等から構成されるテレコムアイザック推進会議に平成21年5月に設置された、サイバー攻撃対応演習WGにおいて、平成18年度から平成20年度までに総務省が実施したサイバー攻撃対応演習の成果を踏まえ、平成21年度のサイバー攻撃対応演習が実施された。	A
ウ)	情報セキュリティに関する国際会合の開催	内閣官房 関係府省庁	・平成21年6月にハンガリーで開催された国際監視・警戒ネットワーク（IWWN）会合において、日本での開催を提案。	A

(オ) 環境変化への対応

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア) a)	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Webサイトを充実させたほか、情報セキュリティ対策に関する講演を5回行った。	A
ア) b)	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	・国内外の先進的なIT障害対応方策等に関する、重要インフラ事業者に対する情報提供を目的として、「重要インフラ情報セキュリティフォーラム」をIPAとJPCERT/CCが共同で平成22年1月25日に開催。(会場:秋葉原コンベンションホール、参加者262名)。	A
イ) a)	リスクコミュニケーションの充実	内閣官房 重要インフラ所管省庁	・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7回開催した。	A
イ) b)	ソフトウェアや情報システムの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において、米国CERT/CCと共同で、ソフトウエア設計工程における脆弱性低減策の一つとして、一連の「セキュアデザインパターン」を定義し、平成21年6月に公開後、平成21年11月に新たに6つのパターンを追加。 ・JPCERT/CCにおいて、東京および大阪でそれぞれ3回ずつセキュアコーディングセミナーを実施(参加者は約400名)。その他、国内各種イベントでの講演などにより、個人開発者も含めて幅広く開発現場に対する安全な開発技術の浸透を図った。	A
イ) c)	重要インフラ事業者に対するソフトウェア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	・JPCERT/CCにおいて、平成22年2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6,500件収集・分析し、27件の注意喚起、25件の早期警戒情報配信を行った。また、重要インフラ事業者からの依頼や情報提供に基づき、情報セキュリティインシデントによる被害の発生、拡大抑止のための関係者間の調整活動を、22件実施。	A
イ) d)	重要インフラ事業における制御システムの脆弱性に関する情報提供等	経済産業省	・IPAにおいて、監視制御システムにおける脆弱性を含めたセキュリティ課題の解決に向けたオランダのガイドである、「上水道分野のSCADA(監視制御システム) セキュリティ グッド・プラクティス」を21年11月に翻訳・公開。 ・IPAにおいて、海外で利用されているテストベッドやツールの利用状況等を踏まえた、重要インフラにおける制御システムの脆弱性低減と普及施策についての課題整理と検討等に関する調査に着手。平成22年2月中に結果をとりまとめた。	A
イ) e)	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において、「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」のメーリングリストを用意し、平成22年7月から隔月のニュースレター発行を開始。 ・JPCERT/CCのウェブ・ページの一部を再構成し、制御システム・セキュリティに関連した情報を整理して提供を開始。 ・平成22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、開発者や利用者等国内外の制御システム関係者による、それぞれの立場からの先進的な活動に関する講演やパネルディスカッション等を行い、様々な立場の参加者間で、問題意識や先進事例の共有を図った。	A
ウ)	国際連携の推進	内閣官房	・平成21年6月にIWWNに参加し、わが国の政策を説明。また10月に開催されるメリディアンに参加し、欧米やアジア各国の重要インフラ防護担当者と情報セキュリティ政策の国際的な動向についての意見交換や情報収集を行った。 ・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、重要インフラ関連の委員会等で各国の情報共有組織や演習等について情報提供を行った。	A

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	情報セキュリティガバナンス確立の促進	経済産業省	・企業における情報セキュリティガバナンスの更なる確立に向け、産業構造審議会情報セキュリティ基本問題委員会において「情報セキュリティガバナンス導入ガイダンス」等のガイダンス類を策定し、平成21年6月に公開した。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。 ・「情報システムの信頼性向上に関するガイドライン」を改訂し、平成21年3月に第2版として公表。また、当ガイドラインの適合度合いを可視化する信頼性評価指標第1版及び自動的に点数化するソフトウェアを平成21年9月に公開。	A
イ)	情報セキュリティ監査制度の利用促進	経済産業省	・日本セキュリティ監査協会において、平成21年度のサプライチェーンにおける情報セキュリティ監査に関する検討結果等を活用し、業界団体等と連携しつつ個別分野ごとの管理基準、監査手続及び実務指針などに関する検討を行い、平成22年3月までに実務指針などを完成した。 ・平成21年度全国縦断情報セキュリティ監査セミナーを3月末までに9回開催（参加者は延べ1,171名）。情報セキュリティ実践セミナーは毎回対象者・テーマを絞り、3月末までに東京9回、大阪2回開催（参加者は延べ543名）。	A
ウ)	第三者評価の審査の効率化と質の高い情報セキュリティ関連製品等の普及促進	経済産業省	・IPAにおいて、平成21年度に新たに31件（2009年末時点）の認証を追加。 ・IPAにおいて、CCタスクフォースを開催（年度中3回開催）してITセキュリティ評価・認証制度の普及促進のための検討と対応を認証機関、評価機関、関連する申請者（ベンダー）で実施。 ・昨年度に引き続き、ISO15408の認証を取得した製品を購入した事業者について、一定割合で税額控除等の優遇措置を実施。	A
エ)	「情報システム・モデル取引・契約書」の活用・普及	経済産業省	・平成21年度にモデル契約書普及のための「情報システム・ソフトウェア取引高度化コンソーシアム」を組成し、不適切な契約に起因するトラブル事例の調査、取りまとめを行うとともに、調査事例を用いて契約に対する意識向上のためのセミナーを開催した。	A
オ)	「情報セキュリティ対策ベンチマークシステム」の提供	経済産業省	・「情報セキュリティ対策ベンチマークシステム」については、診断の基礎データを最新のデータに入れ替え、バージョン3.2として平成21年5月からサービスを更新。 ・平成21年5月に、蓄積した統計情報の企業規模別・業種別の分析結果をウェブで公開。 ・平成21年度のアクセス件数は約11万件（平成22年2月25日時点）	A
カ)	企業に係る指標の充実等	経済産業省	・「平成21年情報処理実態調査」を平成21年11月から実施。	A
キ)	入札条件等の見直し	内閣官房 総務省 財務省 経済産業省 全府省庁	・平成19年度及び平成20年度に実施した内閣官房における研究の結果を踏まえ、内閣官房において今後の具体的な進め方について引き続き検討しているところ。	B
ク)	企業における電子署名利活用の普及促進	総務省 法務省 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6都市で開催）等を通じて、電子署名の一層の普及を図る予定。	A

(イ) 企業の情報セキュリティ向上に資する製品やサービスの提供促進と活動の推進

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
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	・JPCERT/CCにおいては、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）により、平成21年4月から平成22年2月の間、271件の脆弱性情報を機械処理可能な形式で配信した。今後IPAが提供するMyJVN APIを活用し、データの配信量を増加させる予定。また、脆弱性対応意思決定支援システムに関し、その利用の普及を図るため、平成20年度に引き続き、国内の利用者の協力を得る形で有効性の検証を継続しつつ、米国CERT/CCと協力して実施した有効性検証の結果に関する報告書を平成21年8月に公開。 ・IPAにおいて、脆弱性対策情報データベースJVNIPediaを運用・提供し、ベンダやユーザに情報提供を引き続き実施。平成21年6月に、共通脆弱性タイプ一覧CWE（Common Weakness Enumeration）の詳細説明等の機能強化をしたVer3.1を公開。 ・IPAにおいて、ユーザの利便性と脆弱性情報の取りこぼし防止のために、情報システム利用者の脆弱性対策支援ツールMyJVNを引き続き提供。更に、MyJVNに各種アプリケーションソフトの脆弱性対策漏れを確認するためのバージョンチェッカ機能を追加開発。平成21年11月から提供開始。累計100万件を超えるアクセス数（平成22年1月時点）	A
イ)	【再掲】 ソフトウェアや情報システムの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において、米国CERT/CCと共同で、ソフトウエア設計工程における脆弱性低減策の一つとして、一連の「セキュアデザインパターン」を定義し、平成21年6月に公開後、平成21年11月に新たに6つのパターンを追加。 ・JPCERT/CCにおいて、東京および大阪でそれぞれ3回ずつセキュアコーディングセミナーを実施（参加者は約400名）。その他、国内各種イベントでの講演などにより、個人開発者も含めて幅広く開発現場に対する安全な開発技術の浸透を図った。	A
ウ)	企業の運営するWebサイトの安全性向上	経済産業省	・IPAにおいて、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。平成21年度に19,334件のアクセス（平成22年2月時点） ・ウェブサイトに対する新たな攻撃パターンに対応するため、平成22年1月にWAF（Web APplication Firewall） のログ検査機能追加開発に着手した。（平成22年度開発完了・提供開始予定）	A
エ)	組込みソフトウェアの安全性向上のための取組み	経済産業省	・IPAにおいて、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。TCP/ Pツールは累計103社、SIPツールは累計21社に貸出。 ・さらに、新たに発見された脆弱性へ対応するため、平成22年1月に上記ツールの機能強化開発に着手した。（平成22年度開発完了・提供開始予定）	A
オ)	「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	・NPO法人ASP・SaaSインダストリ・コンソーシアム内に設置された「ASP・SaaSデータセンター促進協議会」において、本指針を活用した情報開示認定制度の検討を実施し、平成22年3月に方向性を取りまとめた。	A
カ)	【再掲】 第三者評価の審査の効率化と質の高い情報セキュリティ関連製品等の普及促進	経済産業省	・IPAにおいて、平成21年度に新たに31件（2009年末時点）の認証を追加。 ・IPAにおいて、CCタスクフォースを開催（年度中3回開催）してITセキュリティ評価・認証制度の普及促進のための検討と対応を認証機関、評価機関、関連する申請者（ベンダー）で実施。 ・昨年度に引き続き、ISO15408の認証を取得した製品を購入した事業者について、一定割合で税額控除等の優遇措置を実施。	A
キ)	システムLSIのセキュリティ評価体制の整備	経済産業省	・国内にシステムLSIのセキュリティ評価・認証体制の整備を進めるべく、平成21年度から平成23年度までの3年計画で、整備を進める予定。	A
ク)	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	・「情報システムの信頼性向上に関するガイドライン」を改訂し、平成21年3月に第2版として公開。また、当ガイドラインの適合度合いを可視化する信頼性評価指標第1版及び自動的に点数化するソフトウェアを平成21年9月に公開。	A
ケ)	「SaaS向けSLAガイドライン」の活用・普及	経済産業省	・インターネットを活用したソフトウェア提供サービス（J-SaaS）におけるサービスレベルを当該ガイドラインをベースに策定し、サービス自体も平成21年3月から開始。	A
コ)	「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	・財団法人マルチメディア振興センターにおいて、平成20年4月に本制度を創設以来、94件を認定（平成22年3月現在）。	A
サ)	「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」の策定・活用・普及	総務省	・総務省において、平成21年7月に本ガイドラインを策定し、公表。	A
シ)	情報セキュリティ対策を容易化するシステム等の開発	経済産業省	・インターネットを活用したソフトウェア提供サービス（J-SaaS）の運用を平成21年3月より開始。 ・セキュリティ管理を支援するサービスの提供も平成21年7月から開始。	A
ス)	スパムメール対策の強化	総務省 経済産業省	・平成20年の法改正によるオプトイン規制の導入などを受けて、着実な法執行等、迷惑メール対策の強化を図っている。また、迷惑メール対策推進協議会において、業界団体と協力して迷惑メール対策技術の導入等を推進している。さらに「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ところ。	A
セ)	組込みシステム等のディペンダビリティ確保のための体制整備等	経済産業省	・平成20年度からのIPAを始めとしたわが国認証関連機関等の働きかけが結実し、欧州のセキュリティLSIに関する評価手法を定める作業部会JHASに、リエゾンとしてIPA及び日本のCC評価認証部会（国内の評価機関、スマートカードベンダー等から構成）が参加することが認められた。（平成21年7月10日） ・引き続き、JIWG 、JHAS 等との信頼関係を維持しつつ、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に向け、評価能力向上に努める。	A
ソ)	【再掲】 企業における電子署名利活用の普及促進	総務省 法務省 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6都市で開催）等を通じて、電子署名の一層の普及を図る予定。	A
タ)	NGN/IPv6環境のセキュリティ評価システムの構築	総務省	・平成21年4月より、ネットワーク上でのセキュリティ脅威や脆弱性を把握・確認するための評価用プロトタイプシステムの研究開発に着手。平成22年4月から実証評価試験を開始予定。	A

（続く）

（続き）

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
チ）	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、検討を進めている。なお、現在、文化審議会著作権分科会において、「権利制限の一般規定」について検討が行われており、この課題は権利制限規定の在り方を含む著作権法体系全体に関わるものであることから、当該課題の議論の動向も踏まえつつ、取組を進める予定。	B
ツ）	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に対する税制優遇措置	総務省 経済産業省	・平成20年4月より平成22年3月まで、情報基盤強化税制により特別償却制度、税額控除制度を措置。	A
テ）	非機能要求の合意手法の確立	経済産業省	・非機能要求の合意手法を実証する委員会を設置し、実際の稼働システムを対象として、合意手法の有効性を検証した。平成22年2月18日に評価報告書を公開。	A

（ウ）企業における情報セキュリティ人材の育成・確保

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア）	中小企業情報セキュリティ対策の促進	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21カ所で開催。	A
イ）	中小企業を対象とした情報セキュリティセミナー等の実施	経済産業省	・経済産業省、IPAと日本商工会議所が連携して実施している情報セキュリティセミナーを、平成21年度については全国34箇所で開催し、のべ8,512名が参加。	A
ウ）	情報セキュリティ監査知識を有する人材の育成	経済産業省	・日本セキュリティ監査協会において、平成21年度全国縦断情報セキュリティ監査セミナーのプログラムの一つとして、情報セキュリティ監査知識を有する人材の育成方法を紹介。3月末までに9回開催（参加者は延べ1,171名）。	A
エ）	情報セキュリティ・サポーターの育成	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、情報セキュリティ・サポーターに求められる資質やスキル、適切な育成方法等について検討を行った。 ・情報セキュリティ人材の実態に関する調査を実施し、情報セキュリティ・サポーター体制の現状等を把握した。また、情報セキュリティ・サポーターの育成・確保に向けて、「情報セキュリティ人材育成シンポジウム」を開催した。	A
オ）	情報処理技術者試験の更なる普及	経済産業省	・共通キャリア・スキルフレームワークに基づく、新たな情報処理技術者試験を平成21年4月より実施。 ・平成21年度の試験応募者は、7年振りに対前年度比で増加。 ・産業界及び教育界の団体の長等を発起人とする「ITパスポート試験普及協議会」を発足	A
カ）	民間のセキュリティ資格の周知	内閣官房 総務省 経済産業省	・情報セキュリティ人材の充実に関するシンポジウムやセミナーにおいて、民間のセキュリティ資格についての周知を実施。 ・総務省において、情報セキュリティ資格保有者等の育成・確保に向けて、「情報セキュリティ人材育成シンポジウム」を開催した。	A
キ）	産学連携IT人材育成実行事業	経済産業省	・産業界出身の教員の充実・強化、実践的な教材・カリキュラムの開発・普及、産学マッチングによる実践的なインターンシップなどを推進するための事業を実施した。平成22年4月中に事業報告書を公表する予定。	A
ク）	情報通信人材研修事業支援制度	総務省	・セキュリティ人材を含む情報通信分野の専門的な知識や技術を有する人材を育成するための研修事業に対して、助成金を交付。	A
ケ）	IPv6運用技術習得のためのテストベッドの整備	総務省	・平成21から平成22年度の2か年計画の1年目として、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）を整備した。	A
コ）	モデルキャリア開発計画策定事業	経済産業省	・専門家コミュニティを活用し、IT職種ごとのモデルキャリア開発計画を策定するための事業を実施した。平成22年4月中に事業報告書を公表する予定。	A

(エ)「事故前提社会」への対応力強化に向けた事業継続性確保・緊急対応体制等の強化

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	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強化するためのフローを構築し、また、制御システムの脆弱性の問題に対応すべく、「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」の活動として、制御システム・セキュリティに関連した情報の提供を開始。 ・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開催した（約22回）。 ・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し、平成20年度2,600人に対して実施した成果をもとにより効果的な演習の実施方法に関する考察を報告書に取りまとめ、平成21年6月に公開。平成21年度については、ITセキュリティ予防接種の効果の経年変化検証、実施手法の改善による合理化などを目的として約3000人に対して調査を実施し現在調査結果の分析を行った。	A
イ)	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、平成21年6月、ローカルホストとして、21st Annual FIRST Forum for Incident Response and Security Teams）の京都開催に協力し、52の国と地域から参加した約400名の各国のCSIRTメンバー等との間で、インシデント対応等に関する協力、連携関係の強化を図った。 ・JPCERT/CCにおいて、平成21年7月には、ASEANを中心とする14のチームが参加した「ASEANサイバーセキュリティ演習」に、また、平成22年1月には、アジア太平洋地域のCSIRT間連携の枠組みであるAPCERT（Asia Pacific Computer Emergency Response Team） メンバによる演習に参加 し、マルウエアインシデントへの対応に関する国際連携の強化、効率化を図った。 ・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た。	A
ウ)	[再掲] 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において、「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」のメーリングリストを用意し、平成22年7月から隔月のニュースレター発行を開始。 ・JPCERT/CCのウェブ・ページの一部を再構成し、制御システム・セキュリティに関連した情報を整理して提供を開始。 ・平成22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、開発者や利用者等国内外の制御システム関係者による、それぞれの立場からの先進的な活動に関する講演やパネルディスカッション等を行い、様々な立場の参加者間で、問題意識や先進事例の共有を図った。	A
エ)	ソフトウェア等の脆弱性に係るマネジメントの支援等 [再掲]	経済産業省	・JPCERT/CCにおいては、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）により、平成21年4月から平成22年2月の間、271件の脆弱性情報を機械処理可能な形式で配信した。今後IPAが提供するMyJVN APIを活用し、データの配信量を増加させる予定。また、脆弱性対応意思決定支援システムに関し、その利用の普及を図るため、平成20年度に引き続き、国内の利用者の協力を得る形で有効性の検証を継続しつつ、米国CERT/CCと協力して実施した有効性検証の結果に関する報告書を平成21年8月に公開。 ・IPAにおいて、脆弱性対策情報データベースJVNIPediaを運用・提供し、ベンダやユーザに情報提供を引き続き実施。平成21年6月に、共通脆弱性タイプ一覧CWE（Common Weakness Enumeration）の詳細説明等の機能強化をしたVer3.1を公開。 ・IPAにおいて、ユーザの利便性と脆弱性情報の取りこぼし防止のために、情報システム利用者の脆弱性対策支援ツールMyJVNを引き続き提供。更に、MyJVNに各種アプリケーションソフトの脆弱性対策漏れを確認するためのバージョンチェッカ機能を追加開発。平成21年11月から提供開始。累計100万件を超えるアクセス数（平成22年1月時点）	A
オ)	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、約100件の情報提供を行った。 ・IPAにおいて、標的型攻撃の調査・分析結果として、ツールを利用した標的型攻撃の広がりについてまとめた「脆弱性を利用した新たなる脅威の監視・分析による調査」報告書を平成21年7月に公表した。	A

(オ) 中小企業の情報セキュリティ対策の推進

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	[再掲] 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に対する税制優遇措置	総務省 経済産業省	・平成20年4月より平成22年3月まで、情報基盤強化税制により特別償却制度、税額控除制度を措置。	A
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	・平成20年度に引き続き、独立行政法人情報処理推進機構（IPA）において「中小企業の情報セキュリティ対策に関する研究会」を開催し、平成20年度に策定した「中小企業の情報セキュリティ対策ガイドライン」等の普及促進を図るべく検討を実施した。具体的には、平成20年度に作成した普及パンフレット「5分でできる自社診断」の改善を実施した。また、地域機関との連携を強化した（2機関→5機関） ・「5分でできる自社診断」パンフレットを、1万7千部配布（平成22年2月時点）。 ・中小企業向けの情報セキュリティ学習ツールとして「5分でできる情報セキュリティポイント学習」を開発し、平成21年10月から提供を開始した。以降、16,801件のダウンロードがあった（平成22年2月時点）。	A
ウ)	[再掲] 「SaaS向けSLAガイドライン」の活用・普及	経済産業省	・インターネットを活用したソフトウェア提供サービス（J-SaaS）におけるサービスレベルを当該ガイドラインをベースに策定し、サービス自体も平成21年3月から開始。	A
エ)	[再掲] 情報セキュリティ対策を容易化するシステム等の開発	経済産業省	・インターネットを活用したソフトウェア提供サービス（J-SaaS）の運用を平成21年3月より開始。 ・セキュリティ管理を支援するサービスの提供も平成21年7月から開始。	A
オ)	[再掲] 情報セキュリティ監査知識を有する人材の育成	経済産業省	・日本セキュリティ監査協会において、平成21年度全国縦断情報セキュリティ監査セミナーのプログラムの一つとして、情報セキュリティ監査知識を有する人材の育成方法を紹介。3月末までに9回開催（参加者は延べ1,171名）。	A
カ)	[再掲] 中小企業情報セキュリティ対策の促進	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21カ所で開催。	A
キ)	[再掲] 中小企業を対象とした情報セキュリティセミナー等の実施	経済産業省	・経済産業省、IPAと日本商工会議所が連携して実施している情報セキュリティセミナーを、平成21年度については全国34箇所で開催し、のべ8,512名が参加。	A
ク)	[再掲] 情報通信人材研修事業支援制度	総務省	・セキュリティ人材を含む情報通信分野の専門的な知識や技術を有する人材を育成するための研修事業に対して、助成金を交付。	A

(カ) 日系企業のグローバルな事業展開を支える情報セキュリティ政策の推進

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	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	・JPCERT/CCにおいて、スリランカ、インドネシア、ベトナム、フィリピン等9カ国において、企業等の情報セキュリティに関するセミナーの開催協力や招待講演等を実施した。 ・経済産業省において、情報セキュリティの強化を通じたASEAN諸国におけるビジネス環境の更なる強化、活性化を目的とし、タイ及びインドネシアにおいて企業の情報セキュリティに関するセミナーを開催した。	A
イ)	ソフトウェア開発のアウトソーシング先国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、平成21年9月タイにおいて、開発者約100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、アンケートを用いて、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。平成21年10月末にインドネシア（約45名）、平成22年1月にベトナム（約40名）において、それぞれ同様にセキュアコーディングに関するセミナーを現地日本法人からの参加者を含む開発者に実施した。	A
ウ)	海外における組織の緊急対応チームの構築・運用支援	経済産業省	・JPCERT/CCにおいて、スリランカ、フィリピン、ベトナム、マレーシア等において、企業内CSIRTの構築に資するための技術セミナーを実施した。 ・経済産業省において、平成22年1月、タイ、インドネシア、ベトナム、フィリピン、カンボジアのCSIRT関係者をに対し、CSIRT間の連携に関する指導方法についての研修を東京で行った。	A

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア）　a）	メディアリテラシー向上のための調査・開発、啓発活動の展開	総務省	・平成20年度までに開発したプログラムについて引き続き普及を図るとともに、新たなプログラムの開発に着手し、平成22年3月に完成。	A
ア）　b）	「情報セキュリティ対策」標語・ポスターによる普及啓発	経済産業省	・IPAにおいて、全国の小中高生を対象に「情報セキュリティ標語・ポスター」の募集を実施（募集期間：平成21年7月1日から同年9月10日）。計7,297件（標語6,772件、ポスター525件）の応募作品の中から優秀な作品を選考し、平成21年10月29日に表彰式を開催した。	A
ア）　c）	e-ネットキャラバンの実施等	総務省 文部科学省	・平成18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、平成19年度は1,089件、平成20年度は1,208件の講座を実施した。 ・平成21年度は、624件の講座を実施した（3月末現在）。	A
イ）　a）	若年層からの高度セキュリティ人材の育成	経済産業省	・平成16年度より「早期IT人材育成支援事業」として若年層を対象にセキュリティキャンプを実施。平成20年度からはプログラミングコースも加わり、セキュリティ＆プログラミングキャンプとして実施。 ・全国各地での講習会と併せ、これまでにのべ約2,000人が参加。 ・平成21年度は、セキュリティ＆プログラミングキャンプの応募者の大幅な増加を踏まえ、定員を大幅に拡大して実施。	A
イ）　b）	全国的な情報セキュリティ教育の推進	経済産業省 警察庁	・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、平成21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。平成21年度末までに154件開催。	A
イ）　c）	サイバー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サイバーセキュリティに関する講習を、平成22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。	A
ウ）　a）	Web脆弱性に関する学習・検証ツールの提供	経済産業省	・平成22年1月に体験型の脆弱性学習・検証ツールの開発に着手した。（平成22年度中に開発完了・公開予定）	A
ウ）　b）	情報セキュリティに関する情報収集を支援するツール提供	経済産業省	・「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。平成21年度下期に、さらに多くの情報の提供を行うために、ニュースサイトの追加登録を働きかけ、新たに3社を登録。 ・月平均約3万6千アクセス。	A
ウ）　c）	プロアクティブな取組みによる悪意あるサイト等の情報収集・提供	経済産業省	・IPAにおいて、平成21年3月に運用を開始した、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、問い合わせのあった一般利用者に対して提供。（80件） ・ゼロデイ攻撃への対策として、Exploit コード 等の解析により脅威を分析し、ゼロデイ攻撃の自動検出を行うためのツール開発をについて、ウェブサイトを改ざんするような新たな攻撃（ガンブラー等）に対応するため開発内容等の仕様を検討。	A

(イ) 個人の底上げに向けたより効果的な普及・啓発活動の実現

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア) a)	情報セキュリティに関する周知・啓発活動の推進	内閣官房 警察庁 総務省 経済産業省	・内閣官房において、NISCホームページ等を活用し、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。 ・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、ソフトウェア等の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、平成21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。平成21年度末までに154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の紹介を行った。	A
ア) b)	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 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21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平成22年3月公表。 ・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、委託調査を実施する予定。 ・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、平成21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。平成21年度末までに154件開催。	A
ア) c)	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平成21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。 ・最近のサイバー犯罪の検挙状況、相談状況を分析し、「インターネット安全・安心相談」の回答項目に反映。	A
ア) d)	電波利用秩序の維持のための周知啓発活動の強化	総務省	・平成21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、「電波のルールを守りましょう」をキャッチフレーズに「技術基準適合マーク」の確認を促すなどの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・業界専門誌、TVCM、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、各種広報紙への掲載等）により周知啓発を実施。 ・平成21年6月から8月、10月から11月に総合通信局所において、主要都市の電波利用機器販売店への周知・啓発を実施。 ・平成21年6月に「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。	A
ア) e)	「情報通信の安心安全な利用のための標語」による啓発活動	総務省	・「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、平成21年6月、最優秀作（総務大臣賞）を含む計10作品の選定・表彰を実施。	A
ア) f)	無線ＬＡＮのセキュリティ対策	総務省 経済産業省	・平成19年12月に改訂したガイドライン「安心して無線LANを利用するために」の総務省ホームページへの掲載を通じて、引き続き、その普及の推進を図っているところ。 ・経済産業省において、一般利用者等を対象とした普及啓発事業である「インターネット安全教室」において、無線LANの安全な使い方についての啓発活動を実施。	A
ア) g)	【再掲】 全国的な情報セキュリティ教育の推進	経済産業省 警察庁	・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、平成21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。平成21年度末までに154件開催。	A
ア) h)	【再掲】 e-ネットキャラバンの実施等	総務省 文部科学省	・平成18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、平成19年度は1,089件、平成20年度は1,208件の講座を実施した。 ・平成21年度は、624件の講座を実施した（3月末現在）。	A
ア) i)	【再掲】 情報セキュリティ・サポーターの育成	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、情報セキュリティ・サポーターに求められる資質やスキル、適切な育成方法等について検討を行った。 ・情報セキュリティ人材の実態に関する調査を実施し、情報セキュリティ・サポーター体制の現状等を把握した。また、情報セキュリティ・サポーターの育成・確保に向けて、「情報セキュリティ人材育成シンポジウム」を開催した。	A
イ) a)	「情報セキュリティの日」の実施	内閣官房 警察庁 総務省 文部科学省 経済産業省	・普及啓発の強化のため、平成22年より新たに2月を情報セキュリティ月間に設定し、官房長官からのメッセージの発信、セミナー等関連行事の開催などを行った。	A
ウ) a)	NISCメールマガジンの継続的発行	内閣官房	・平成21年度においては、編集方針等の見直しを図り、平均月1回程度の頻度で発行している。	A
ウ) b)	情報化促進貢献表彰における情報セキュリティ促進部門の表彰	総務省 経済産業省	・平成21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。	A
エ) a)	我が国の情報セキュリティ戦略の国内外への発信	内閣官房	・NISCの英語版ウェブサイト上でNISCの我が国政府における位置づけ、機能、政策等を掲載。 ・政策の進捗状況を報告するため、「セキュア・ジャパン2009」の英語版等を新たに掲載した。	A

〔ウ〕 対策が困難な個人も含めた情報セキュリティ水準向上に向けた取組み

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア〕	サイバー攻撃停止に向けた枠組みの構築	総務省 経済産業省	・平成18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中。平成23年度からの民間による自主的な取組みに向けて検討中。	A
イ〕	マルウェア配布等危害サイト回避システムの実証実験	総務省	・平成21から23年度の3か年計画の1年目として、マルウェア配布等危害サイト回避システムの開発及び、危害サイトリストの有効性検証を実施。	A
ウ〕	〔再掲〕 e-ネットキャラバンの実施等	総務省 文部科学省	・平成18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、平成19年度は1,089件、平成20年度は1,208件の講座を実施した。 ・平成21年度は、624件の講座を実施した〔3月末現在〕。	A
エ〕	〔再掲〕 スパムメール対策の強化	総務省 経済産業省	・平成20年の法改正によるオプトイン規制の導入などを受けて、着実な法執行等、迷惑メール対策の強化を図っている。また、迷惑メール対策推進協議会において、業界団体と協力して迷惑メール対策技術の導入等を推進している。さらに「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ところ。	A

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア) a)	中長期的目標に対する研究開発・技術開発の促進	内閣官房 内閣府 警察庁 総務省 文部科学省 経済産業省 防衛省	・公的研究資金の投入を含む政府の施策を検討するために、政策系の有識者を含む検討会を開催し、情報セキュリティの研究開発・技術開発において政府の果たす役割について整理した。また、当該検討結果を報告書に纏めると共に、情報通信PTに報告した。	A
ア) b)	セキュアクラウドネットワーキング技術の研究開発	総務省	・平成21年7月から安全性・信頼性の高い次世代のクラウドサービスを誰でも利用可能とするためのネットワーク基盤技術に必要な研究開発を実施し、基本技術について平成22年3月までに確立。	A
ア) c)	次世代バックボーンに関する研究開発	総務省	・平成17年度から、通常のネットワーク運用では見られない異常なトラヒックを検出・制御し、IPバックボーン全体の安定運用等を実現する技術を確立するための研究開発を実施した。平成21年度は実用化技術の研究開発や総合検証評価を実施し、平成22年3月に完成。	A
ア) d)	経路ハイジャックの検知・回復・予防に関する研究開発	総務省	・平成18年度から平成21年度の4か年計画の4年目として、経路ハイジャックの検知・回復・予防に関する技術について、基礎研究や基本機能の開発・実験・実証・評価を実施した。平成22年3月までに実装可能な技術を確立した。並行して、日本国内への実装を図るとともに、国際的な導入に向け経路管理に係る国際機関への働きかけを実施した。	A
ア) e)	情報通信分野における情報セキュリティ技術に関する研究開発	総務省	・送出機器のアドレスを詐称している通信であっても、本当の送出機器を探知しうるトレースバック技術に関する研究開発に平成17年度に着手。以降、調査・方式検討・設計・実装を経て、平成20から21年度にかけて実証実験と評価を実施。 ・多数の拠点に分散するインシデント情報を統合し、より広域的かつ階層的な解析を実現するためのインシデント分析の広域化・高速化技術に関する研究開発（平成20年度から22年度）を実施中。 ・高度化・巧妙化するマルウェアに柔軟に対応可能な総合的なセキュリティユーザサポートシステムを構築するための、効率的なマルウェア検出、自動駆除技術の研究開発（平成21年度から平成23年度）を実施中。	A
ア) f)	新世代の情報セキュリティ技術の研究開発	経済産業省	・ゼロデイ攻撃のリスク対策技術、フォーマルメソッドの開発工程全般への適用等、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。	A
ア) g)	情報漏えい対策技術の研究開発	総務省	・平成19年度から平成21年度の3か年計画の3年目として、自動情報流出アプリケーションのトラフィック集中化技術及び流出情報検知技術に関する基礎研究や基本機能開発・詳細設計・評価、並びに情報の来歴管理等の高度化・容易化に関する研究開発を実施し実装可能な技術を確立した。	A
ア) h)	情報処理基盤の安全性等の確保（マルウェア検体の活用方法の検討）	経済産業省	・IPAの保有するコンピュータウイルス検体等を市販のウイルス対策ソフトのパターンファイルに反映させること等により、利用者の安全性を高めることを目的として、ウイルス対策ベンダに対する検体提供のために必要な規程を制定。運用開始（平成21年5月）。 ・ウイルス対策ベンダ各社に働きかけ、平成21年度中に計2社と検体提供の契約を締結。	A
ア) i)	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	・ブラックボックス化されている情報通信ソフトウエアの安全・信頼性の検証・評価について、体制を整備し、初期的な検討等を実施。	A
ア) j)	[再掲] システムLSIのセキュリティ評価体制の整備	経済産業省	・国内にシステムLSIのセキュリティ評価・認証体制の整備を進めるべく、平成21年度から平成23年度までの3年計画で、整備を進める予定。	A
ア) k)	新世代ネットワーク基盤技術に関する研究開発	総務省	・新世代ネットワークアーキテクチャの概念設計及びダイナミックネットワーク技術に関する研究開発を平成19年度に開始し、平成20年度から、仮想化技術に関する研究開発に着手。平成21年度はこれらの研究開発を引き続き着実に実施。平成22年度末までに、新世代ネットワークアーキテクチャの概念設計等を完了する予定。	A
ア) l)	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セキュリティに関する課題、及び必要なセキュリティ技術について検討するとともに、セキュリティ上重要となる暗号技術に関するドライバプログラムの開発、クラウド環境中におけるアカウント情報に基づいたデータ管理手法に関する調査研究、業務シナリオに基づく実証実験を実施。	A
ア) m)	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	・ソフトウエアの構築状況を可視化し、ソフトウエアの構築手順が適正であることを把握可能にするソフトウェアタグ規格を開発し、平成20年10月に公開。平成22年度までソフトウェアタグ利用シナリオ構築に向けた実証実験を実施。 ・ソフトウェアタグ利用に関する法的問題点の整理を行い、ソフトウェアタグ利用の有用性を平成22年度中にまとめる。 ・平成20年10月エンピリカルソフトウェア工学研究会（東京、参加者110名）、平成20年12月国際ワークショップＡＴＧＳＥ2008（中国北京、参加者20名）、平成21年10月エンピリカルソフトウェア工学研究会（東京、参加者100名）を主催。	A
イ) a)	短期的目標設定のなされている研究開発・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 防衛省	・情報セキュリティ技術を網羅的に洗い出し、さまざまな領域において過小投資、課題投資が発生しないようなポートフォリオとするために、それぞれの研究開発の進展状況について調査を行い、技術系の有識者を含む検討会において評価を行った。当該調査について報告書に取り纏めたが、投資ポートフォリオ等による分析方法の検討は今後の検討課題とした。	B
イ) b)	[再掲] 高セキュリティ機能を実現する次世代ＯＳ環境の評価及び性能向上	内閣官房 内閣府 総務省 経済産業省	・セキュアVMの1つである「BitVisor」を用い、政府機関内の利用を想定したセキュアな環境を構築し、導入・運用面の評価を実施した。また、政府機関が「セキュアVM」を導入するための調達面及び機能面の要件を整理し、当該要件をXenやVMware等の汎用的な仮想化製品がどの程度満たしているかの比較評価を行なって、これらの評価結果を報告書として取り纏めた。	A

（続く）

（続き）

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
イ） c）	IP 化されたネットワークにおける重要通信の高度化の推進	総務省	・重要通信の取扱いを実現するために不可欠な情報の関係事業者との共有や共通課題の検討を実施し、平成22年2月に情報通信行政・郵政行政審議会へ重要通信の義務化に関する制度改正について諮問を行い、パブリックコメントを実施した。	A
イ） d）	情報アクセス権限を統合し、集中管理する機構を導入した革新的な仮想化技術の開発	経済産業省	・平成19年度から平成21年度の3か年計画で「セキュア・プラットフォームプロジェクト」を実施。本事業の目標である、次世代情報システムのプラットフォームに求められる安定性・安全性の確保と導入・運用コストの削減を実現し、省電力にも寄与するサーバ統合技術を確立した。	A
ウ） a）	萌芽的研究開発に係る基本方針等の策定	内閣官房 内閣府 警察庁 総務省 文部科学省 経済産業省 防衛省	・情報セキュリティに係わる技術のうち、民間での取組みが乏しい萌芽的な研究領域について、公的研究資金の投資対効果の精度を高めるために、政府の取り組むべき支援施策について有識者を含む検討会にて検討し、当該内容を報告書に取り纏めた。	A

（イ）「グランドチャレンジ型」研究開発・技術開発の推進

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア）	「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 防衛省	・研究開発の枠組み検討の一環として、研究開発において技術進展の障壁となる要因を分析し、これらの要因に対して政府が関与すべき取組み内容の検討を行った。具体的には、情報セキュリティに係わる技術を目的別に分類するとともに、政府として取り組むべき技術開発分野を選択するための基準（クライテリア）を検討し、このクライテリア及びグランドチャレンジ型テーマの目的に照らして、テーマ選定及び推進の枠組みについて検討した。	A

（ウ）研究開発・技術開発の効率的な実施体制の構築と基盤の整備

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア）	実施状況の把握及び継続的な見直しの実施	内閣官房 内閣府	・情報セキュリティに関する研究開発・技術開発の実施状況を把握するため、関連技術を網羅的に洗い出し、各技術の進展状況についての調査を行った。当該調査結果については、技術系の有識者に意見を伺った後、報告書に取り纏めた。 ・セキュリティ領域の重要な研究開発課題に関し、各府省庁の施策の進捗状況と今後の取組みを中間フォローアップとして取り纏めた。	A
イ）	投資効果に係る継続的評価プロセスの導入	内閣官房 内閣府	・情報セキュリティに係る研究開発・技術開発の投資効果を把握する手法について有識者の委員会において検討した。 ・平成22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、および、優先度判定を行った。	A
ウ）	公的な競争的資金制度におけるプロジェクト管理・評価の検討	内閣官房 内閣府 関係省庁	・公的な競争的資金制度における各制度の規定や実施手順の整備状況を調査し、変更ルールや実施手順に「曖昧さ」が残る部分について明確化するための方策について検討した。 ・研究計画の変更が柔軟にできるようにするため、内閣府等の関係機関への働きかけを行い、一部の研究プログラムについては公募要領に反映した。	B＋
エ）	政府調達における成果利用の方策の検討	内閣官房 全府省庁	・情報セキュリティ研究開発・技術開発の成果を調達を通じて政府が活用できるようにするため、諸外国の研究開発戦略について調査したうえで、研究開発・技術開発に係わる政策の1つとして政府調達を有効に活用する方策を検討し、調査報告書に取り纏めた。	A
オ）	小規模攻撃再現テストベッド・マルウェア隔離解析テストベッド等の構築	総務省	・定常的かつ迅速に小規模攻撃・マルウェア等の再現実験・解析を行うための専用のマルウェア隔離解析テストベッドの構築に着手。平成21年12月にはプロトタイプを試験構築し、再現データセットの試験提供とテストベッドの試験運用を開始した。平成22年12月に完成予定。	A

第3章　2009年度に取り組む重点政策

第1節　対策実施4領域における取組みの推進と政策目的の着実な実現

(2) 横断的な情報セキュリティ基盤の強化と発展

②情報セキュリティ人材の育成・確保

(ア) 政府機関における人材の育成・確保及び職員の意識啓発

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	[再掲] 政府職員向け教育プログラムの充実	内閣官房 総務省	・内閣官房において政府統一的な教育プログラムについて、政府機関統一基準（第4版）に対応した教材のひな形を作成し各府省庁に提供済み。	A
イ)	[再掲] 情報セキュリティ関連業務の調査等	内閣官房	・各府省庁における情報セキュリティ関連業務に携わる人材に求められるスキルについて、各府省庁の最高情報セキュリティアドバイザーの協力を得て取りまとめた。	A
ウ)	[再掲] 人材育成・確保実行計画の実施	全府省庁	・各府省庁において、「行政機関におけるIT人材の育成・確保指針」に基づいて策定した「行政機関におけるIT人材育成・確保実行計画」に基づき、人材の育成・確保に取り組んでいるところ。	A
エ)	[再掲] 民間専門家の活用の促進	全府省庁	・各府省庁において、最高情報セキュリティアドバイザーの設置等、情報セキュリティ対策に係る民間専門家の積極的な活用を図っているところ。	A
オ)	[再掲] 政府職員の人材育成の促進	全府省庁	・各府省庁において、階層別研修等を活用して、全職員の情報セキュリティに関する意識の向上を推進しているところ。	A
カ)	情報システム及び暗号モジュールの評価技術の向上	経済産業省	・IPAにおいて、平成21年6月から9月の間にIPAの認証要員を欧州4か国のセキュリティ評価機関に派遣し、セキュリティLSI等を用いたシステムの安全性評価及び次世代の暗号モジュール試験に対応可能な技術知識及び技能を習得させた。 ・経済産業省において、平成22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。	A

(イ) 企業における情報セキュリティ人材の育成・確保

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	[再掲] 情報通信人材研修事業支援制度	総務省	・セキュリティ人材を含む情報通信分野の専門的な知識や技術を有する人材を育成するための研修事業に対して、助成金を交付。	A
イ)	[再掲] 情報セキュリティ・サポーターの育成	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、情報セキュリティ・サポーターに求められる資質やスキル、適切な育成方法等について検討を行った。 ・情報セキュリティ人材の実態に関する調査を実施し、情報セキュリティ・サポーター体制の現状等を把握した。また、情報セキュリティ・サポーターの育成・確保に向けて、「情報セキュリティ人材育成シンポジウム」を開催した。	A
ウ)	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	・平成19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（申請：10件）。 ・平成20年度は、それぞれの拠点において実際に学生の受入が開始され、先進的な教育プログラムの開発・実施が進められるとともに、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の「拠点間教材等洗練事業」を実施。 ・平成21年度には、2拠点における教育プロジェクトの中間評価を実施。	A
エ)	[再掲] 情報セキュリティ監査知識を有する人材の育成	経済産業省	・日本セキュリティ監査協会において、平成21年度全国縦断情報セキュリティ監査セミナーのプログラムの一つとして、情報セキュリティ監査知識を有する人材の育成方法を紹介。3月末までに9回開催（参加者は延べ1,171名）。	A
オ)	[再掲] 情報処理技術者試験の更なる普及	経済産業省	・共通キャリア・スキルフレームワークに基づく、新たな情報処理技術者試験を平成21年4月より実施。 ・平成21年度の試験応募者は、7年振りに対前年度比で増加。 ・産業界及び教育界の団体の長等を発起人とする「ITパスポート試験普及協議会」を発足	A
カ)	[再掲] モデルキャリア開発計画策定事業	経済産業省	・専門家コミュニティを活用し、IT職種ごとのモデルキャリア開発計画を策定するための事業を実施した。平成22年4月中に事業報告書を公表する予定。	A
キ)	[再掲] 産学連携IT人材育成実行事業	経済産業省	・産業界出身の教員の充実・強化、実践的な教材・カリキュラムの開発・普及、産学マッチングによる実践的なインターンシップなどを推進するための事業を実施した。平成22年4月中に事業報告書を公表する予定。	A
ク)	[再掲] 中小企業情報セキュリティ対策の促進	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21カ所で開催。	A
ケ)	[再掲] 中小企業を対象とした情報セキュリティセミナー等の実施	経済産業省	・経済産業省、IPAと日本商工会議所が連携して実施している情報セキュリティセミナーを、平成21年度については全国34箇所で開催し、のべ8,512名が参加。	A
コ)	[再掲] 民間のセキュリティ資格の周知	内閣官房 総務省 経済産業省	・情報セキュリティ人材の充実に関するシンポジウムやセミナーにおいて、民間のセキュリティ資格についての周知を実施。 ・総務省において、情報セキュリティ資格保有者等の育成・確保に向けて、「情報セキュリティ人材育成シンポジウム」を開催した。	A

(ウ) 情報セキュリティ人材が保有するスキルの見える化の推進

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	共通キャリア・スキルフレームワークの普及	経済産業省	・平成21年度より、共通キャリア・スキルフレームワークに基づく、新たな情報処理技術者試験を実施すると共に、新たなバージョンの各種スキル標準を公開して普及。 ・平成21年度の情報処理技術者試験の応募者は、7年振りに対前年度比で増加。	A
イ)	[再掲] 情報処理技術者試験の更なる普及	経済産業省	・共通キャリア・スキルフレームワークに基づく、新たな情報処理技術者試験を平成21年4月より実施。 ・平成21年度の試験応募者は、7年振りに対前年度比で増加。 ・産業界及び教育界の団体の長等を発起人とする「ITパスポート試験普及協議会」を発足	A
ウ)	[再掲] モデルキャリア開発計画策定事業	経済産業省	・専門家コミュニティを活用し、IT職種ごとのモデルキャリア開発計画を策定するための事業を実施した。平成22年4月中に事業報告書を公表する予定。	A
エ)	[再掲] 産学連携IT人材育成実行事業	経済産業省	・産業界出身の教員の充実・強化、実践的な教材・カリキュラムの開発・普及、産学マッチングによる実践的なインターンシップなどを推進するための事業を実施した。平成22年4月中に事業報告書を公表する予定。	A
オ)	[再掲] 民間のセキュリティ資格の周知	内閣官房 総務省 経済産業省	・情報セキュリティ人材の充実に関するシンポジウムやセミナーにおいて、民間のセキュリティ資格についての周知を実施。 ・総務省において、情報セキュリティ資格保有者等の育成・確保に向けて、「情報セキュリティ人材育成シンポジウム」を開催した。	A

(ア) 情報セキュリティ政策に関するPOC機能の強化と情報共有の促進

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
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 関係府省庁	・内閣官房及び関係府省庁は、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、国際監視・警報ネットワーク（IWWN）の机上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。 ・内閣官房及び関係府省庁は、情報セキュリティに係る問題を議論するASEAN、OECD、MERIDIAN等の国際会合のほか、諸外国の政府機関・民間企業等との連携強化を年度内に推進。	A
イ)	[再掲] 情報セキュリティに関する国際会合の開催	内閣官房 関係府省庁	・平成21年6月にハンガリーで開催された国際監視・警戒ネットワーク（IWWN）会合において、日本での開催を提案。	A
ウ)	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 関係府省庁	・内閣官房及び関係府省庁は、日米サイバーセキュリティ二国間会合を実施するなど二国間連携を強化。	A

(イ) 世界の脅威動向を把握するための官民連携の確立と、効率的・効果的な国際連携活動の推進

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	国内関係機関との連携強化	内閣官房	・内閣官房は、関係府省庁と連絡を密にするとともに、IWWNでの決定事項について関連委員会で報告するなど継続的に国内関連機関に情報を提供。	A
イ)	国際的な情報共有ルール整備に向けた検討	内閣官房 関係府省庁	・内閣官房及び関係府省庁は、IWWNにおける標準手順の策定に参加するなど国際会議や二国間の対話において各国との情報共有を推進。	A
ウ)	海外のCSIRT の体制強化の支援	経済産業省	・JPCERT/CCにおいて、アジア太平洋地域における海外CSIRTの構築支援に関しては、平成20年度から継続してJICAの枠組みによるカンボジア国家ICT開発庁への支援プロジェクトを通じ、CamCERT（カンボジア）に対して専門家を派遣し、CamCERTの体制強化の支援を行ったほか、モンゴル、ラオス、フィジー（Pacific-CERT）においてCSIRT向けのトレーニングを実施した。 ・JPCERT/CCにおいて、IWWN（InterNational Watch and Warning Network）主催によるインシデント対応演習への参加（平成21年6月12日から13日）、FIRSTの「21st Annual FIRST Conference」の京都開催（平成21年6月28日から7月3日）に関するローカルホストとしての協力、ASEANサイバーセキュリティ演習への参加（平成21年7月）、欧州におけるCERTシンポジウムへの参加（平成21年10月）、APCERTサイバー演習（平成22年1月）、APCERT年次会合（平成22年3月）への参加、中国、韓国および米国等のNational-CSIRTとの個別会合等により、各国CSIRTとの間の連携の強化を図った。 ・JPCERT/CCにおいて、FIRSTの京都開催の機会を利用したミーティング等により、湾岸地域等のイスラム圏や中南米のチーム等との間においても連携関係の構築・強化を図った。	A
エ)	日中韓におけるネットワーク情報セキュリティに関する情報共有体制等の強化	総務省	・平成21年7月に開催した日韓テレコム・アイザック会合における、両国のTelecom-ISACを中心とする官民連携体制の構築や情報の共有等、情報セキュリティ分野における2国間協力の方向性に関する協議に基づき、ボット対策に関する情報交換体制の整備を開始。	A
オ)	日・ASEAN におけるネットワークオペレータ間の情報共有の促進	総務省	・日・ASEAN間におけるネットワークオペレータ間の情報共有を促進するため、ASEAN各国のネットワークオペレータの窓口（POC）情報を収集した。 ・平成22年3月に開催された第2回日・ASEAN情報セキュリティ政策会議において、ネットワークセキュリティに関する地域内共通の脅威・課題を共有し、具体的な連携方策について協議を行った。	A

(ウ) アジアにおける知恵の結集と情報セキュリティ水準の向上（One-Asiaの実現）

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	日・ASEAN におけるネットワークセキュリティ分野の研究協力の推進	総務省	・平成21年8月より、NICTを中心とした、日・ASEAN間でのネットワークセキュリティ分野における研究協力の実現に向けた具体的な取り組み方法について検討中。 ・平成22年3月に開催された第2回日・ASEAN情報セキュリティ政策会議において、ネットワークセキュリティに関する地域内共通の脅威・課題を共有し、協力の可能性がある研究分野について協議を行った。	A
イ)	アジア太平洋地域等での早期警戒情報の共有促進	経済産業省	・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14の国・経済地域で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実施した。	A
ウ)	アジア地域における攻撃手法の分析能力の強化及び分析結果情報の共有の促進	経済産業省	・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、マルウエアやソフトウエアの脆弱性、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（平成22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実施した。また、平成21年7月に実施したASEANを中心とする14のチームが参加した「ASEANサイバーセキュリティ演習」、及び、平成22年1月に実施したAPCERT（Asia Pacific Computer Emergency Response Team）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。	A
エ)	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み	経済産業省	・平成21年5月に、AISEC Forum第1回会合を東京で開催した（参加国：韓国・マレーシア・台湾・インド）。	A

(エ) 経済活動のグローバル化に対応した情報セキュリティの確保

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	日・ASEAN 情報セキュリティ政策会議合意内容の着実な実施	内閣官房 総務省 経済産業省	・内閣官房、総務省及び経済産業省は、平成22年3月に開催された第2回日・ASEAN情報セキュリティ政策会議に参加。日・ASEAN間の情報セキュリティ分野における中長期的な戦略として位置づけられる「情報セキュリティ分野における日・ASEAN連携枠組み」を最終合意。 ・内閣官房は、第1回日ASEAN政策会議の合意内容を実行に移すため、10月にASEAN諸国関係者を招へいし、政府ネットワークセキュリティに関するワークショップを実施。 ・総務省は、平成21年10月に開催された日・ASEAN情報通信大臣会合において、平成21年2月に東京で開催した第1回日・ASEAN情報セキュリティ政策会議の結果を報告。 ・総務省は、日・ASEANにおける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や、ネットワークセキュリティ分野における研究協力等の実施に向け準備中。 ・経済産業省は、ASEANにおいて現地企業の情報セキュリティ水準の向上に向けたセミナーの開催や情報セキュリティ管理ベンチマークに関するERIAの研究等を実施。 ・経済産業省は、平成21年7月に開催された日・ASEAN経済担当高級実務者会合において、平成21年2月に開催した第一回日・ASEAN情報セキュリティ政策会議の結果を報告し、同会合にテイクノートされた。	A
イ)	[再掲] 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	・JPCERT/CCにおいて、スリランカ、インドネシア、ベトナム、フィリピン等9カ国において、企業等の情報セキュリティに関するセミナーの開催協力や招待講演等を実施した。 ・経済産業省において、情報セキュリティの強化を通じたASEAN諸国におけるビジネス環境の更なる強化、活性化を目的とし、タイ及びインドネシアにおいて企業の情報セキュリティに関するセミナーを開催した。	A
ウ)	[再掲] ソフトウェア開発のアウトソーシング先国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、平成21年9月タイにおいて、開発者約100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、アンケートを用いて、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。平成21年10月末にインドネシア（約45名）、平成22年1月にベトナム（約40名）において、それぞれ同様にセキュアコーディングに関するセミナーを現地日本法人からの参加者を含む開発者に実施した。	A
エ)	情報処理技術者試験及びIT スキル標準の国際展開	経済産業省	・平成21年4月にITPECにおいてアジア統一試験を実施。同年10月に秋期試験を実施予定。 ・平成21年度に我が国で新設されたITパスポート試験を平成22年度以降、ITPEC各国においても実施可能とするため、平成22年3月までに教材の開発等を実施。 ・平成22年3月までに、ITPEC各国に対し専門家の派遣や研修の実施などの支援を実施。	A

(オ) 標準化を含んだ我が国の戦略的貢献の実現

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	電気通信事業における情報セキュリティマネジメントの強化	総務省	・電気通信事業における情報セキュリティマネジメントに関する要求事項の国際規格化等に向けて、民間における検討の場として、安心・安全インターネット推進協議会にISM-TG検討SWGを設置した（平成21年6月）。	A
イ)	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	・JASAにおいて、平成21年11月に米国で行われた国際会合（ISO/IEC JTC1/SC27/WG1会合）での審議結果を踏まえ、平成22年3月に情報セキュリティ監査手続ガイドラインの一部をもとに、セキュリティ管理策の評価ガイドラインの提案書を作成。 ・IPA及びJPCERT/CCにおいて、平成21年5月に北京で開催されたISO/IEC JTC1 SC27会合へ、研究員が参加し、国際標準化活動に協力。 ・IPAにおいて、平成21年5月に北京で開催されたISO/IEC JTC1 SC27春期会合およびへ、研究員が参加し、国際標準化活動に協力。 ・IPAにおいて、平成21年10月に米国で開催されたる同SC27秋期会合に参加し、我が国のIT環境・基準・ガイドライン等を踏まえて、暗号技術、CC、JCMVP、脆弱性情報やネットワークセキュリティ等に関する国際標準化活動に規格への反映が行われるよう積極的に参画した。	A

(カ) 情報セキュリティ文化の醸成

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	我が国の情報セキュリティ戦略に関する国際的な広報活動の推進	内閣官房	・内閣官房は、各種国際会議において我が国の施策について積極的に報告しているほか、NISCホームページにおいて、基本理念や戦略、SJ2009等を英語で公表している。	A
イ)	多国間会合を通じた情報セキュリティ政策に関する途上国の底上げ支援	内閣官房 関係府省庁	・内閣官房及び関係府省庁は、FIRST参加者との協議やASEAN諸国との連携を深める中で、発展途上国における国際的な意識向上を図っているところ。	A
ウ)	ITU-Dを活用した国際協力の推進	内閣官房 総務省	・電気通信開発セクターのSG（研究委員会）会合を年1回ベースで開催。平成21年9月に開催されたSG1会合において、我が国から「安心・安全なインターネット環境整備に関する戦略対話」の結果（平成21年6月開催）に関し、概要及び成果を報告。	A
エ)	APT研修・セミナー等の開催	総務省	・アジア・太平洋電気通信共同体（APT=Asia-Pacific Telecommunity）への我が国からの特別拠出により平成21年11月4日から13日の間「ブロードバンド通信のための情報セキュリティ」研修を実施した。	A
オ)	国際的なセキュリティ文化実現及び意識・リテラシー向上のための取組み	内閣官房	・内閣官房は、FIRST参加者との協議やASEAN諸国との連携などのほか、国際会議の場でセキュリティ文化実現及び意識・リテラシー向上に資する発表・意見交換を継続的に実施しているところ。	A

第3章　2009年度に取り組む重点政策

第1節　対策実施4領域における取組みの推進と政策目的の着実な実現

〔2〕横断的な情報セキュリティ基盤の強化と発展

④犯罪の取締り及び権利利益の保護・救済

〔ア〕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	進捗状況分類
ア)	サイバー犯罪の取締りのための態勢の強化	警察庁	・平成21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。 ・広域にわたるサイバー犯罪捜査に対応する取締対策車両を整備・増強。	A
イ)	デジタルフォレンジックに係る取組みの推進	警察庁	・デジタルフォレンジック用資機材を増強。 ・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各種研修を実施。 ・平成21年10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。	A
ウ)	サイバー犯罪の取締りのための国際連携の推進	警察庁	・平成21年4月及び11月並びに平成22年2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。 ・平成21年2月の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おいて決定した、日本主導による情報通信技術を利用した犯罪に対処するための取組みを推進。 ・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法執行機関の相互の技術水準の向上を図ることを目的として、サイバー犯罪技術情報ネットワークシステム（CTINS）を運用しており、平成22年3月末現在、14の国・地域が参加。 ・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平成21年9月に開催。 ・デジタルフォレンジックに関する協力を推進することを目的として、平成21年5月、オランダ司法省法科学研究所との間で意図表明文書に署名。 ・平成21年12月、情報技術の解析に係る知見の集約・体系化・相互活用を図るため、IOCE（国際電子計算機証拠機構）・ICPO・警察庁共催で情報技術の解析に係る国際会議を開催。	A
エ)	中央当局制度を活用した国際捜査共助の迅速化	法務省	・刑事共助条約の締結作業について，予定どおりに施策を推進。 ・平成20年5月、刑事に関する共助に関する日本国と中華人民共和国との間の条約につき国会承認。11月、発効。 ・平成21年7月、刑事に関する共助に関する日本国と中華人民共和国香港特別行政区との間の協定につき国会承認。9月、発効。 ・平成21年5月、ロシア連邦との間で刑事共助条約の署名。平成22年2月、国会の承認を得るため国会に提出。第174回国会において審議。 ・平成21年12月、EU（欧州連合）との間で刑事共助協定の署名。平成22年2月、国会の承認を得るため国会に提出。第174回国会において審議。	A
オ)	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	・近年における情報処理の高度化の状況等にかんがみ，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等の観点から検討していく予定。）。	B
カ)	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か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。 ・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協議会」の発足（平成21年6月発足）に協力し、同協議会に出席するなど、違法情報対策に関して民間との連携強化を推進した。	A
キ)	犯罪に強いIT 社会構築のための官民連携に向けた取組みの推進	警察庁	・インターネット・オークションにおける盗品の流通防止対策について、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で検討し、報告書にとりまとめた。	A
ク)	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・技能等の修得のための部内外における各種研修を実施。 ・緊急対処を行うための資機材を整備。	A
ケ)	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、官民の連携強化を図っている。	A
コ)	重要無線通信妨害対策の強化	総務省	・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、平成21年10月から重要無線通信妨害申告受付体制の一部強化を実施。引き続き電波監視体制の充実を実施予定。 ・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センサを整備するため、平成21年9月末に契約手続きを実施。平成21年度末までに16式を整備した。 ・アップリンク干渉源特定機能の実用化に向け宇宙電波監視施設の機能・性能向上及び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平成21年度末までに実施した。	A

(イ) 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	進捗状況分類
ア)	[再掲] 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平成21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。 ・最近のサイバー犯罪の検挙状況、相談状況を分析し、「インターネット安全・安心相談」の回答項目に反映。	A
イ)	犯罪抑止のための広報啓発の推進	警察庁	・警察庁セキュリティポータルサイト「@police」において、ソフトウェア等の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。	A
ウ)	[再掲] 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 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21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平成22年3月公表。 ・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、委託調査を実施する予定。 ・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、平成21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。平成21年度末までに154件開催。	A

(ウ) 権利利益の保護・救済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	進捗状況分類
ア)	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	・平成21年8月に「違法・有害情報相談センター」を開設し、プロバイダー等向けに相談業務を実施するなど、同法及び関係ガイドラインの周知を実施。	A
イ)	情報セキュリティ報告書の策定・公表の推進	経済産業省	・重要インフラ事業者を対象とした「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対策編（案）」に情報セキュリティ報告書の策定・公表を推奨事項として盛り込むことを通じて、情報セキュリティ報告書の普及を推進しようとしているところ。 なお、「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」については、第23回情報セキュリティ政策会議で承認され、公表。	B＋

第4章　政策の推進体制と持続的改善の構造について

第1節　政策の推進体制

(1) 内閣官房情報セキュリティセンター (NISC) の強化と役割

(ア) 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	進捗状況分類
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、第3章に掲載した施策を推進。 ・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の机上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。	A
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	・内閣官房では、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継続的に図っている。	A

(2) 各府省庁の強化と役割

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	情報セキュリティ対策の体制の強化及び府省庁横断的な取組みの実施	全府省庁	・各府省庁では引き続き、自らの情報セキュリティ体制の強化を推進。 ・内閣官房では、政府機関統一基準及びその適用個別マニュアル群の提供、普及啓発活動における政府機関における情報セキュリティ対策の説明等を通じ、官民において情報セキュリティ対策に関する情報の共有を推進。	A
イ)	情報セキュリティの分析・提言	経済産業省	・平成20度調査において、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・投資などについて調査及び社会科学的分析を行い、情報セキュリティ対策の対策実施意思と行動の間のギャップの存在が明らかとなった。 ・国内における情報セキュリティと行動科学の研究活動の推進拠点として、類似活動を行っている情報処理学会、電子通信学会との共催で、情報セキュリティの学際的なワークショップを平成21年10月7日に開催した。	A

(3) 状況の変化の適時適切な把握と新しい課題への対応

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	各専門分野情報共有スキームの連携性及び情報交換モデルに関する検討	内閣官房 総務省 経済産業省	・平成21年12月から平成22年3月まで内閣官房において検討を行い、「リスク要件リファレンスモデル」「組織リスク動的判断モデルチャート」「専門分野連携マップ」を作成した。	A

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	関係機関等との連携強化	内閣官房 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。	A

第4章　政策の推進体制と持続的改善の構造について

第3節　持続的改善構造の構築

⑴「年度計画」の策定とその評価等

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	評価等の実施及び公表	内閣官房	・内閣官房において、平成21年度の評価等の実施及び報告・公表に向けて、評価のスケジュールや評価項目を「情報セキュリティ政策2009年度の評価等に向けた「作業方針」」として策定し、第23回情報セキュリティ政策会議において報告。	B＋
イ)	政府機関の情報セキュリティ対策強化に向けたマイルストーンの検討等	内閣官房	・内閣官房において、定常的な評価のスケジュールや評価項目、評価項目選定の趣旨などについて、「情報セキュリティ政策2009年度の評価等に向けた「作業方針」」として策定し、第23回情報セキュリティ政策会議において報告。	B＋
ウ)	重要インフラ領域の情報セキュリティ対策の年度毎の成果検証の実施	内閣官房 重要インフラ所管省庁	・第2次行動計画に基づき重要インフラ事業者等が行う対策と政府が行う施策について、重要インフラ所管省庁の協力を得て、年度内に成果検証、補完調査を実施。重要インフラ専門委員会に報告後、公表する予定。	B＋

⑵ 年度途中での緊急事態対応に向けた取組みの実施

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	計画の見直しについての検討	内閣官房	・年度計画については、平成21年度中、計画の見直しが必要となるような情勢の変化は起こっていない。	A

⑶ 評価指標の改善

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	情報セキュリティ対策に関する評価指標の改善	内閣官房 総務省 経済産業省	・第2次情報セキュリティ基本計画における今後3か年の評価等の基本方針、評価指標等を「情報セキュリティ観点から見た我が国社会のあるべき姿及び政策の評価のあり方【第2版】」として策定し、第23回情報セキュリティ政策会議において了解。	B＋

⑷ 第2次情報セキュリティ基本計画の見直し

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	第2次情報セキュリティ基本計画の見直し	内閣官房	・「第2次情報セキュリティ基本計画」に基づく従来の施策の継続や新たな重点的取組みを推進するとともに安全保障・危機管理も観点から速やかに実施すべき施策を強力に推進するため、「国民を守る情報セキュリティ戦略」を策定し、第23回情報セキュリティ政策会議において決定。	B＋

別添２

政府機関の対策実施状況報告の概要

政府機関の対策実施状況報告（２００９年度）の概要

NISC

1　対策実施状況報告の実施目的

政府機関統一基準（1.1.1 2(6)）において、政府機関全体としての情報セキュリティ対策推進の観点から、各府省庁が対策の実施状況をNISCに報告することとしており、また、NISCは、政府機関統一基準に関する評価指標に基づき、各府省庁の情報セキュリティ関係規程の整備状況及び対策実施状況について検査し、評価することとしている。これらを踏まえ、**各府省庁の対策の実施状況をNISCにおいて把握し、課題及びその改善に向けた今後の取組みについて報告**することを目的とする。

2　2009年度の報告の範囲

2009年度は、2008年度と同様、原則として**すべての職員を対象として報告することを求めた。**
（休職等により、情報を取り扱わないものを除き、政府機関のすべての職員が報告対象。）

3　報告の概要及び2010年度に向けた取組み

報告の概要

・ 政府機関全体で約55万人分の対策実施状況について報告があった。これを分析した結果、把握率、実施率及び到達率については昨年度より高い水準を達成していることが確認できた。分析結果の概要は以下のとおり。（数値は全府省庁の平均値）
　－ 状況が把握できた者の割合を示す**把握率**は、約99%（2008年度：約97%）
　－ 責務が生じた者に占める対策を実施した者の割合を示す**実施率**は、約98%（2008年度：約97%）
　－ 一定の割合以上の実施率を有する遵守事項の割合を示す**到達率**のうち、実施率が１００%の遵守事項の割合は、約83%（2008年度：約76%）
・ 政府全体として、「業務継続計画との整合的運用の確保」及び「情報の作成と入手」に関する遵守事項について課題が認められた。他方、昨年度の課題となっていた、「情報セキュリティ対策の教育」及び「各種規程・手順の整備」に関する遵守事項については、前回（2008年度）から改善が認められた。

2010年度に向けた取組み

【情報セキュリテイ教育】
・ 対策実施状況報告で明らかになった課題を分析し、メリハリのある情報セキュリティ教育等を実施することで、情報セキュリティ対策の徹底を図る。

【トップマネジメントの強化】
・ 最高情報セキュリティ責任者が責任をもって、情報セキュリティ対策を推進するための政府全体の枠組みを構築する。

【対策実施状況報告の改善・効率化】
・ 各府省庁の負担を軽減するとともに、現状の維持・向上の観点から、対策実施状況報告の調査項目・手法の改善・効率化を図る。

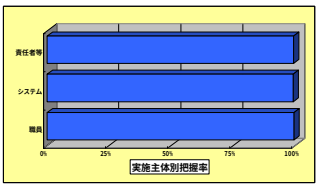
政府機関の対策実施状況報告（２００９年度）の評価結果【実施主体ベース】

NISC

1　把握率

全府省庁の平均把握率

９９．３%



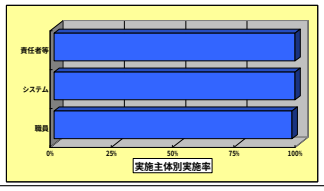
① 昨年度と同様、政府機関のすべての職員を対象としており、対象数は約55万人となっている。
　平均把握率は約99%と昨年より向上しており、多くの省庁で対策実施状況が把握できている結果であった。

② ただし、対策実施状況の把握は、情報セキュリティ水準の維持・向上に不可欠であることから、政府機関全体で把握率100%を達成すべく、今後、更なる向上が望まれる。特に、把握率の低い府省庁にあっては、把握率の改善手段を早急に検討する必要がある。

2　実施率

全府省庁の平均実施率

９８．１%



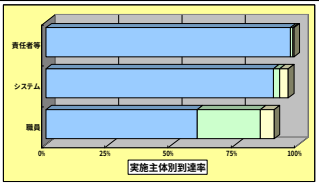
③ 平均実施率は約98%となっており、システム担当が高く、責任者等、職員の順に低い結果であった。

④ 情報セキュリティ対策について組織的な責務を果たすべき責任者等の実施率が未だに１００%に満たないことは問題であり、早急に改善が必要である。

3　到達率

全府省庁の平均到達率

１００%実施した割合　：**８３．０%**
９５%以上実施した割合：**９１．６%**
９０%以上実施した割合：**９４．９%**



⑤ 到達率でみると、責任者等に比べ、特に職員が低くなる傾向が顕著に現れた。

⑥ 職員は責任者等やシステム担当と比して、対象数が多いことや、日々の業務において日常的に実施しなければならない遵守事項が多いことから、すべての職員が遵守事項を実施することは難しく、到達率１００%達成には困難な面があるが、万一の事故防止のためには日々の取組みが重要であり、対策がすみずみまで浸透するような努力が必要である。

把握率：各府省庁が報告対象とした者のうち、対策実施状況が把握できた者の割合
実施率：把握した者のうち、責務が生じた者に占める対策を実施した者の割合
到達率：把握した者のうち、責務が生じた一定の割合（１００%、９５%、９０%）以上の者が対策を実施した遵守事項の割合

責任者等：最高情報セキュリティ責任者、情報セキュリティ委員会、情報セキュリティ監査責任者、情報セキュリティ監査実施者、統括情報セキュリティ責任者、情報セキュリティ責任者、課室情報セキュリティ責任者、許可権限者及び情報セキュリティ関係規程を整備した者
システム：情報システムセキュリティ責任者 情報システムセキュリティ責任者を含む複数の者が主体となっているものを含む）、情報システムセキュリティ管理者及び権限管理を行う者

政府機関の対策実施状況報告（2009年度）の評価結果【遵守事項ベース】

政府機関全体の実施状況について特筆すべき遵守事項は次のとおり。

1 今年度の課題

(1) 業務継続計画との整合的運用の確保

[政府機関統一基準（第4版）1.2 5 2]

全府省庁の平均実施率

90.6 %

① 特定の省庁において業務継続計画と情報セキュリティ対策の整合性の確保と業務継続計画と情報セキュリティ関係規程の不整合の報告について、取組みが不十分である。

→ **特定の府省庁にヒアリングを行い、NISCが支援を行うことで実施率の向上を図る。**

(2) 情報についての対策

[政府機関統一基準（第4版）1.3.1]

全府省庁の平均実施率

遵守事項	実施率	
	2008年度	2009年度
(1)情報の作成と入手	86.6%	91.6%
(2)情報の利用	95.8%	96.4%
(3)情報の保存	88.8%	95.1%
(4)情報の移送	89.7%	96.1%
(5)情報の提供	94.0%	97.2%
(6)情報の消去	96.9%	98.1%

② 昨年度より課題となっていた情報についての対策において、情報の保存・移送等の項目については大幅に実施率が改善したが、情報の作成と入手時の遵守事項については、取組みが不十分である。

→ **[行政事務従事者向けの対策]**
毎年、課題としてあげられる項目のため、ポイントを絞った重点的な教育を行うことで実施率の向上を図る。

→ **[責任者等向けの対策]**
責任のある立場のものが、自ら実施し指導を行うことで、組織的な情報セキュリティの向上を行うことができるような体制を構築する。

2 今年度改善した昨年度の課題

(1) 情報セキュリティ対策の教育

[政府機関統一基準（第4版）1.2 2.1]

全府省庁の平均実施率

教育の実施	教育の受講
99.7 %	**96.0 %**

③ 2008年度は、職員による教育受講が不十分であり、未受講者への受講指導の徹底も不十分であったが、2009年度は改善が認められる。

〔参考〕昨年度の実施率

教育の実施	教育の受講
98.6 %	**87.6 %**

(2) 各種規程・手順の整備

[統一基準（第4版）1 2.5.1(1),1.4.1.1(1),1 5.2.4(1),1 5.2 6(1)]

全府省庁の平均実施率

94.5 %

④ 2008年度は、各種規程・手順の整備について、取組みが不十分であったが、2009年度は改善が認められる。

〔参考〕昨年度の実施率

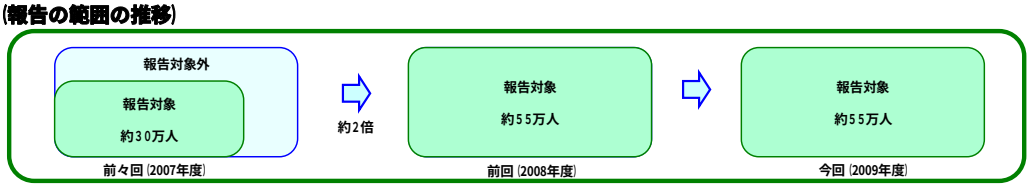
86.9 %

（参考1）対策実施状況報告（2007～2009年度）の推移

2008年度に引き続いて、2009年度も、平均把握率、平均実施率及び平均到達率は、総じて向上しており、政府機関全体に、対策が着実に浸透してきていることが認識できる。

2007年度	2008年度	2009年度
全府省庁の平均把握率	全府省庁の平均把握率	全府省庁の平均把握率
93.4%	**97.3%**	**99.3%**
全府省庁の平均実施率	全府省庁の平均実施率	全府省庁の平均実施率
93.4%	**96.9%**	**98.1%**
全府省庁の平均到達率	全府省庁の平均到達率	全府省庁の平均到達率
100%実施した割合　：**64.1%** 95%以上実施した割合：**75.8%** 90%以上実施した割合：**81.7%**	100%実施した割合　：**76.1%** 95%以上実施した割合：**86.5%** 90%以上実施した割合：**91.2%**	100%実施した割合　：**83.0%** 95%以上実施した割合：**91.6%** 90%以上実施した割合：**94.9%**

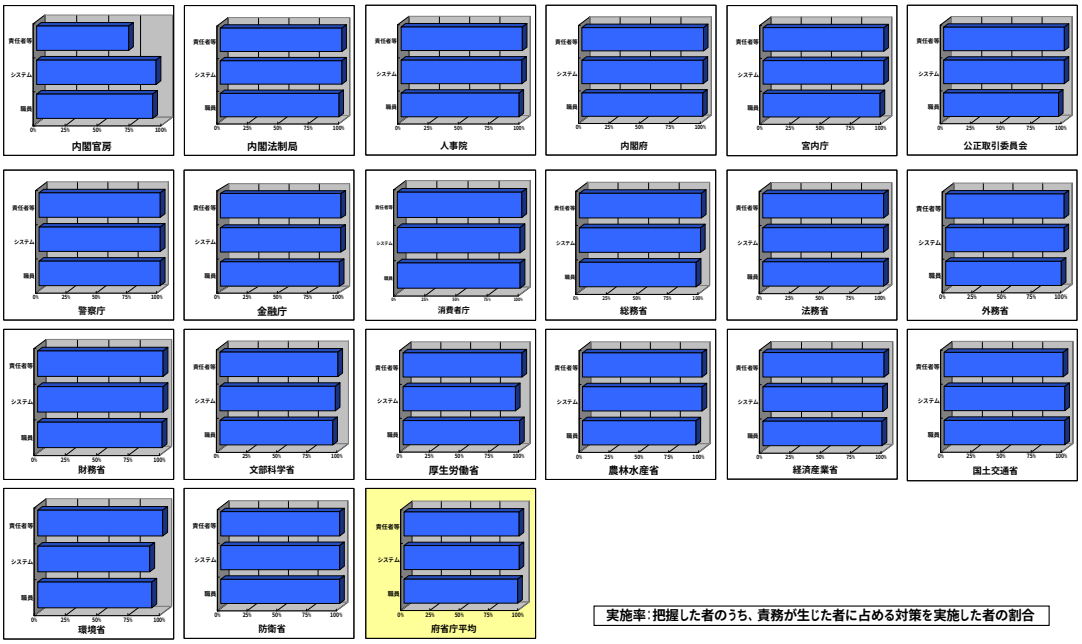
（報告の範囲の推移）



(参考2) 各府省庁の対策実施状況報告 (2009年度) の集計結果

NISC

○ 実施率

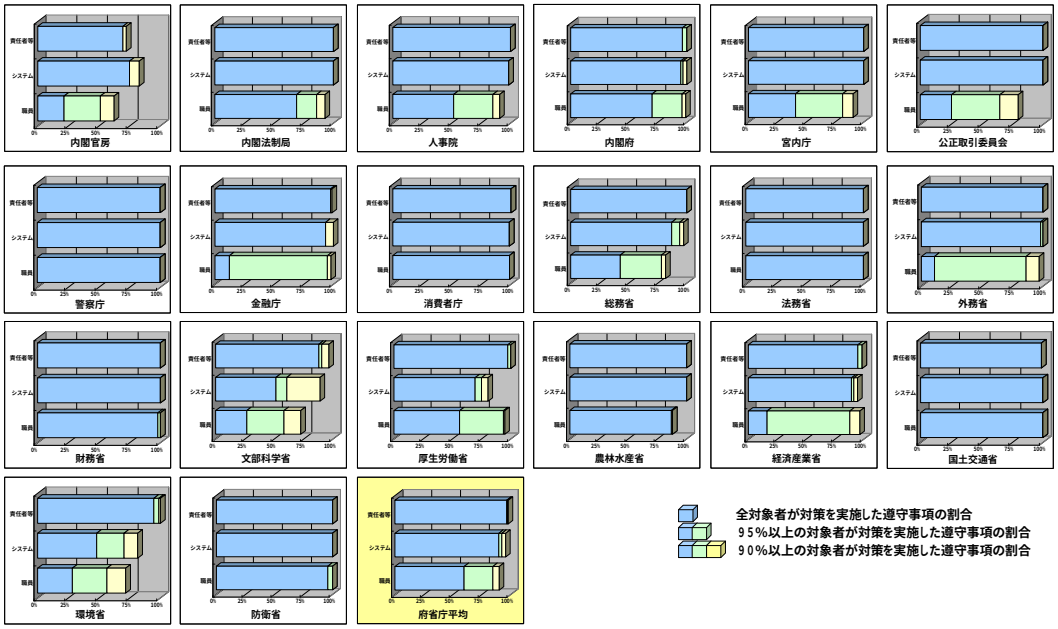


実施率:把握した者のうち、責務が生じた者に占める対策を実施した者の割合

(参考2) 各府省庁の対策実施状況報告 (2009年度) の集計結果

NISC

○ 到達率



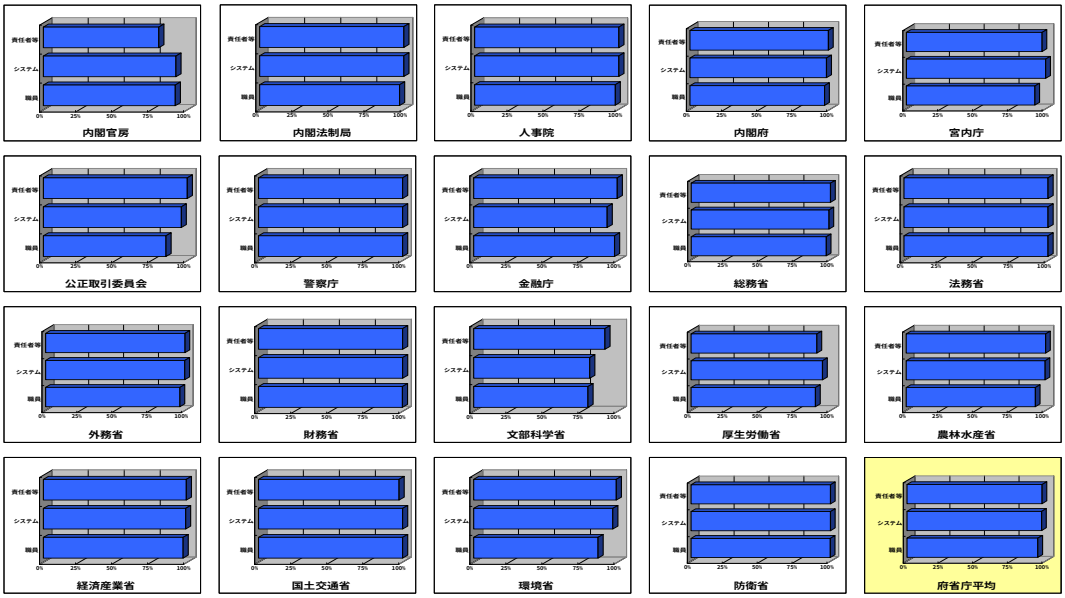
全対象者が対策を実施した遵守事項の割合
95%以上の対象者が対策を実施した遵守事項の割合
90%以上の対象者が対策を実施した遵守事項の割合

到達率:把握した者のうち、責務が生じた一定の割合 (100%、95%、90%) 以上の者が対策を実施した遵守事項の割合

(参考3) 各府省庁の対策実施状況報告 (2008年度) の集計結果

NISC

○ 実施率

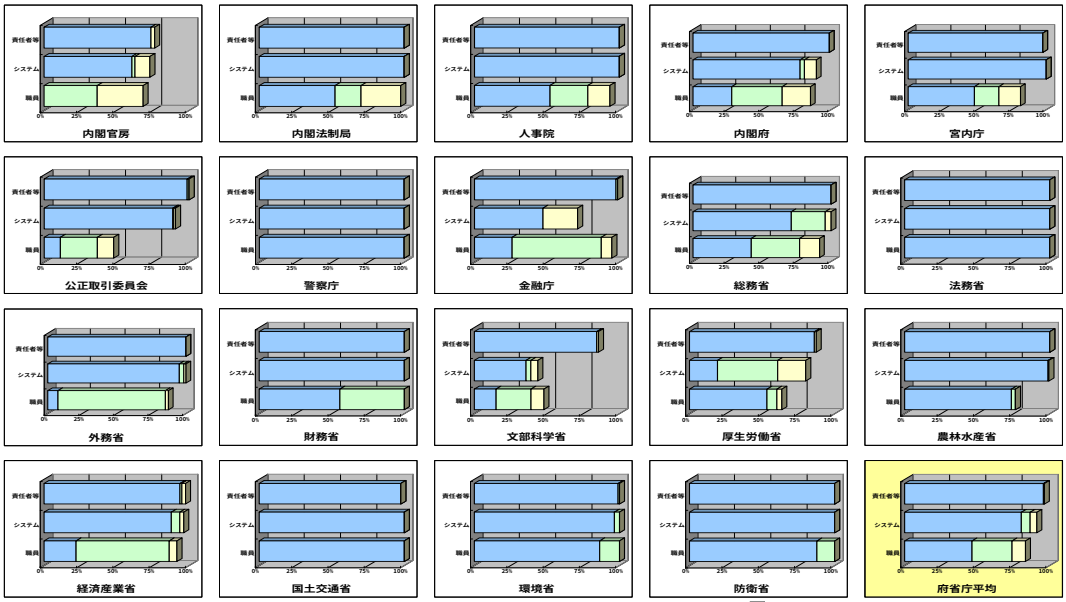


実施率:把握した者のうち、責務が生じた者に占める対策を実施した者の割合

(参考3) 各府省庁の対策実施状況報告 (2008年度) の集計結果

NISC

○ 到達率



到達率:把握した者のうち、責務が生じた一定の割合 (100%、95%、90%) 以上の者が対策を実施した遵守事項の割合

全対象者が対策を実施した遵守事項の割合
95%以上の対象者が対策を実施した遵守事項の割合
90%以上の対象者が対策を実施した遵守事項の割合

(参考4) 対策実施状況報告の調査対象

NISC

政府機関統一基準の項目

第1.2部　組織と体制の整備
- 1.2.1　導入
- 1.2.2　運用
- 1.2.3　評価
- 1.2.4　見直し
- 1.2.5　その他

第1.3部　情報についての対策
- 1.3.1　情報の取扱い

第1.4部　情報処理についての対策
- 1.4.1　情報処理の制限

第1.5部　情報システムについての基本的な対策
- 1.5.1　情報システムのセキュリティ要件
- 1.5.2　情報システムに係る規定の整備と遵守

第2.1部　情報セキュリティ要件の明確化に基づく対策
- 2.1.1　情報セキュリティについての機能
- 2.1.2　情報セキュリティについての脅威

第2.2部　情報システムの構成要素についての対策
- 2.2.1　施設と環境
- 2.2.2　電子計算機
- 2.2.3　アプリケーションソフトウェア
- 2.2.4　通信回線

第2.3部　個別事項についての対策
- 2.3.1　その他

政府機関統一基準に規定されている、基本遵守事項
(333項目) について、各府省庁における実施状況を調査

別添３

政府機関の情報セキュリティ対策の実施状況に関する重点検査及び評価結果について

重点検査の概要（端末、ウェブサーバ、電子メールサーバ）

NISC

1．検査対象機関・システム等 ： 全20府省庁（本省及び地方支分部局）の情報システム

内閣官房、内閣法制局、人事院、内閣府、宮内庁、公正取引委員会、国家公安委員会（警察庁）、金融庁、消費者庁（※）、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省、防衛省

（※）平成21年度から新規追加

2．検査期間 ： 平成21年7月（調査票配布）から同年12月（平成21年11月1日時点の実施状況を検査）

3．検査方法 ： NISCが配布した調査票に基づき、各府省庁が端末、ウェブサーバ及び電子メールサーバについて内部調査を行い回答。両者間で回答内容の確認作業等を行い、NISCから評価結果を各府省庁に通知。

① **端末**（据置型PC、モバイルPC）について、3つのカテゴリーに関して検査 **《対象数：約55万台》**	② **ウェブサーバ**（公開ウェブサーバ）について、4つのカテゴリーに関して検査 **《対象数：約800台》**	③**電子メールサーバ**について、４つのカテゴリーに関して検査 **《対象台数約1,300台》**

端末に関する重点検査項目	
不正プログラム対策	・OSのパッチ等の適用状況 ・主要APのパッチ等の適用状況 ・アンチウィルスソフトの運用状況
情報保護対策	・モバイルPCの暗号化機能の運用状況
端末管理	・端末の物理的対策状況

ウェブサーバに関する重点検査項目	
不正プログラム対策	・OSのパッチ等の適用状況 ・ウェブサーバAPのパッチ等の適用状況等
不正アクセス対策	・不正アクセス対策状況
情報保護対策	・利用者に対する権限管理等の実施状況
サーバ管理	・管理者に対する権限管理等の実施状況 ・データ復旧対策状況

電子メールサーバに関する重点検査項目	
不正プログラム対策	・OSのセキュリティパッチ適用状況（アップデートの状況） ・電子メールサービス提供ソフトウェアのセキュリティパッチ適用状況（アップデートの状況） ・電子メールコンテンツに対する不正プログラム対策の状況
不正アクセス対策	・不正中継対策の状況
情報保護対策	・電子メールの受信に係わる利用者に対する認証等の実施状況
サーバ管理	・電子メールサーバの管理者に対する認証等の実施状況 ・電子メールサーバの障害等の発生時における復旧対策の状況 ・時刻同期機能の動作

端末、ウェブサーバ、電子メールサーバに関する情報セキュリティ対策の総合評価

NISC

府省庁名	端末					ウェブサーバ					電子メールサーバ					府省庁名
	前回 H20.11	上昇率	H21.11	上昇率	H22.3	前回 H20.11	上昇率	H21.11	上昇率	H22.3	前回 H20.11	上昇率	H21.11	上昇率	H22.3	
内閣官房	A	－	A	－	A	※A	－	※A	－	※A	B	▷	A	－	A	内閣官房
内閣法制局	A	－	A	－	A	◆対象なし	－	◆対象なし	－	◆対象なし	A	－	A	－	A	内閣法制局
人事院	A	－	A	－	A	◆対象なし	－	◆対象なし	－	◆対象なし	A	－	A	－	A	人事院
内閣府	A	－	A	－	A	B	▷	A	－	A	B	▷	A	－	A	内閣府
宮内庁	A	－	A	－	A	A	－	A	－	A	B	▷	A	－	A	宮内庁
公正取引委員会	A	－	A	－	A	A	－	A	－	A	A	－	A	－	A	公正取引委員会
国家公安委員会（警察庁）	A	－	A	－	A	A	－	A	－	A	A	－	A	－	A	国家公安委員会（警察庁）
金融庁	A	－	A	－	A	B	－	B	▷	A	A	－	A	－	A	金融庁
消費者庁	-	－	A	－	A	-	－	A	－	A	-	－	A	－	A	消費者庁
総務省	B	－	B	▷	A	A	－	A	－	A	A	－	A	－	A	総務省
法務省	B	▷	A	－	A	A	－	A	－	A	B	▷	A	－	A	法務省
外務省	A	－	A	－	A	A	－	A	－	A	A	－	A	－	A	外務省
財務省	A	－	A	－	A	B	▷	A	－	A	A	－	A	－	A	財務省
文部科学省	B	－	B	▷	A	B	▷	A	－	A	A	－	A	－	A	文部科学省
厚生労働省	B	▷	A	－	A	B	▷	A	－	A	A	－	A	－	A	厚生労働省
農林水産省	A	－	A	－	A	A	－	A	－	A	A	－	A	－	A	農林水産省
経済産業省	A	－	A	－	A	A	－	A	－	A	A	－	A	－	A	経済産業省
国土交通省	A	－	A	－	A	A	－	A	－	A	A	－	A	－	A	国土交通省
環境省	A	－	A	－	A	A	－	A	－	A	A	－	A	－	A	環境省
防衛省	A	－	A	－	A	A	－	A	－	A	A	－	A	－	A	防衛省

評価	実施率	評価	実施率	評価	実施率	評価	実施率
A	x＝100%	B	80%≦x＜100%	C	60%≦x ＜80%	D	x＜ 60%

上昇率		上昇率		上昇率	
▷▷	x＞ 10%	▷	x＞ 0%	－	x≦0%

※内閣官房のウェブサーバについては、内閣府との共有システムを除く
◆内閣法制局、人事院のウェブサーバについては、ホスティング、e-gov移行済みのため対象なし

第2次情報セキュリティ基本計画における重点検査の総評

NISC

１．重点検査結果について

○　政府機関全体における検査対象の保有台数及び情報セキュリティ対策の実施率・評価

- 端末：約55万台（前回：約55万台）　99.2%・評価Ｂ（前回：98.6%・評価Ｂ）
- ウェブサーバ：約800台（前回：約1,000台）　99.5%・評価Ｂ（前回：99.2%・評価Ｂ）
- 電子メールサーバ約1,300台（前回：約1,900台）　100%・評価Ａ（前回：99.5%・評価Ｂ）

政府機関統一基準に準拠した適切な対策が概ね実施されているものの、一部に対策が不十分な項目がみられた。

２．所見

① 端末、ウェブサーバ及び電子メールサーバは、対策が不十分な場合、情報の漏えい、改ざん及び破壊等の要因となり、府省庁業務や利用する国民・職員に影響を及ぼすリスクが高く、また、検査対象の項目は、政府機関統一基準の基本遵守事項であることから、本来100%実施することが期待されるものである。平成21年11月1日時点では、大部分の府省庁で実施されているが、一部の府省庁でわずかに未実施の項目があった。このため、**当該府省庁に改善を促し平成21年度末までに全府省庁で全項目100%実施を完了した。引き続き、100%実施されている状態が維持されるよう促していく必要がある。**

② 重点検査は、各府省庁が、すべての項目で統一基準に準拠した対策が実施されているA評価の部分を維持するとともに、不十分な項目がみられるB評価等の部分を認識し、改善していくための指標として有意義であった。今後は、情報セキュリティ報告書の作成・評価の枠組みの中で、検査内容のさらなる充実を図る必要がある。

政府機関の情報セキュリティ対策の総合評価の見方について

NISC

評価	実施率	対策状況	個別対策項目についての評価パターン例
A	100%	適切に実施すべき対策について、**すべての項目で**統一基準に準拠した**対策が実施**されている。	100% 100% 100%（100%）対策1 対策2 対策3
B	80%≦x<100%	適切に実施すべき対策について、**概ねすべての項目で**統一基準に準拠した**対策が実施**されているが、**一部の項目で不十分なもの**が含まれている。	100% 100% 70%（90%）／90% 90% 90%（90%）対策1 対策2 対策3
C	60%≦x<80%	適切に実施すべき対策について、**不備の項目が一部に見られる**など、対策が遅れている。	100% 100% 0%（67%）／100% 60% 50%（70%）対策1 対策2 対策3
D	60%未満	適切に実施すべき対策について、**不備の項目が相当数、見られるなど**、対策が著しく遅れている。	100% 50% 20%（57%）／60% 40% 0%（33%）対策1 対策2 対策3

◆ **評価方法** ：

各カテゴリーの平均実施率（項目毎に算出した対策実施率（※）の総平均値）の平均値を総合評価の実施率とした。

政府機関統一基準で求める情報セキュリティ対策がすべて実施されていれば、総合評価の実施率は100%、すなわち“A評価”となる。

（※）対策実施率 ＝ 実際に情報セキュリティ**対策を実施している対象数**（端末・サーバ台数） ／ 情報セキュリティ**対策を実施すべき対象数**（端末・サーバ台数） ×100 （%）

別添４

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

サーバ集約化計画策定の取組の概要等

1．計画策定機関 ： **全20府省庁（本省及び地方支分部局）**
内閣官房、内閣法制局、人事院、内閣府、宮内庁、公正取引委員会、国家公安委員会（警察庁）、金融庁、消費者庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省、防衛省

2．対象システム ： **公開ウェブサーバ及び電子メールサーバ**

3．計画策定前の現状 ： **公開ウェブサーバ約1,000台、電子メールサーバ約1,900台** （2008年11月1日時点）

4．問題認識 ： **統制なく多数のサーバを設置・運用すると、コストが増大し、緊急時に迅速かつ的確な対応が困難となるなどセキュリティリスクが高まる。**

5．取組の概要 ： **各府省庁において、最適化計画の枠組みも活用し、省全体の2010年度から2013年度末までの公開ウェブサーバ及び電子メールサーバに係る集約化計画を定め、NISCが政府機関全体の状況を取りまとめ、情報セキュリティ政策会議に報告する。**

6．目標 ： **2013年度末までに政府機関全体として公開ウェブサーバ及び電子メールサーバを半減する。**

政府機関全体におけるサーバ集約化計画の総評

１．集約台数について

	2008年11月1日時点		2013年度末見込み
○ 公開ウェブサーバ：	約1,000台	→	約550台（約45%を削減）
○ 電子メールサーバ：	約1,900台	→	約1,000台（約47%を削減）

【集約の主な方法】
- 基盤となる情報システムのサーバに統合
- 地方の出先機関ごとに設置されていたサーバを本省庁等に集約

【集約を行わない主な理由】
- 業務との密接な連携や独自分野に特化した運用が必要なため他のサーバへの集約が困難
- 災害発生時等の可用性を確保する観点から負荷分散・冗長構成が不可欠

２．所見

① 地方の出先機関ごとに設置・運用されていた情報システムの構成を横断的に見直し、階層的に集約する等により、情報システムを集中管理する体制が強化され、情報セキュリティが向上する見通しとなった。
② 半減との目標は概ね達成できる見通しであるが、各府省庁においては、引き続き、最適化計画の枠組みも活用し、集約化計画の実現に向け努力するとともに、情報システムの更改等の際には、サーバの管理・運用体制を一層強化していくことを推奨する。
③ 集約による効果として、情報セキュリティの向上のほか、情報システムの運用に係るコスト削減にもつながる。

別添５

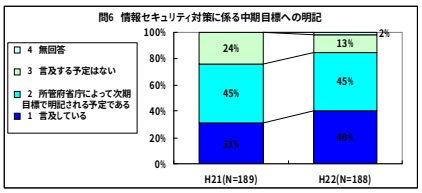
独立行政法人等の情報セキュリティ対策の現状について

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　（188法人）
調査時点：　平成22年2月末時点
※前回調査は、平成21年2月末時点に189法人に実施。

「第2次情報セキュリティ基本計画」（平成21年2月3日情報セキュリティ政策会議決定）
第3章　第1節　（1）　①　（オ）　独立行政法人等の情報セキュリティ対策の推進
独立行政法人等の情報セキュリティ対策を推進するため、独立行政法人等を所管する政府機関は、中期目標の中に情報セキュリティ対策に係る事項を明記し、独立行政法人等が組織として情報セキュリティ対策に取り組む体制を構築させる。各独立行政法人等は、その業務特性及び対策の実施状況に応じて、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、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。また、独立行政法人等及び独立行政法人等を所管する政府機関は、緊急時を含め実効性のある連絡体制を整備する。

情報セキュリティ対策に係る中期目標への明記



前回結果と比べ、明記済の法人は増加。
一方で、言及する予定なしの法人が13%存在。

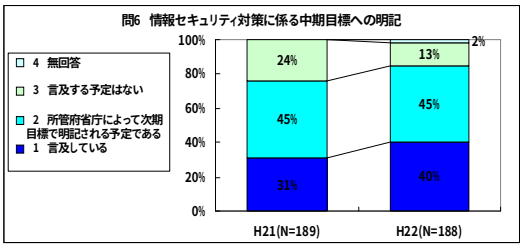
情報セキュリティ対策に係るＰＤＣＡサイクルの構築

項番	対策内容	H21（率）	H22（率）	進捗
1	情報セキュリティポリシーの策定	77%	85%	UP
2	情報セキュリティポリシーの見直し	68%	75%	UP
3	情報セキュリティポリシーの職員教育・訓練	72%	83%	UP
4	情報セキュリティポリシーの遵守状況の把握	69%	74%	UP
5	情報セキュリティ対策の中期目標への明記	76%	85%	UP
6	CISOの設置	73%	83%	UP
7	CISO補佐官の設置	37%	37%	EVEN
8	統括組織の設置	94%	95%	UP
9	注意喚起等に関する連絡体制の整備	99%	100%	UP
10	職員への教育・訓練の実施	89%	90%	UP

前回結果と比べ、情報セキュリティ対策に係るＰＤＣＡサイクルの構築は一定の進展あり。一方で、CISO補佐官の設置など、体制の強化への後押しが必要。

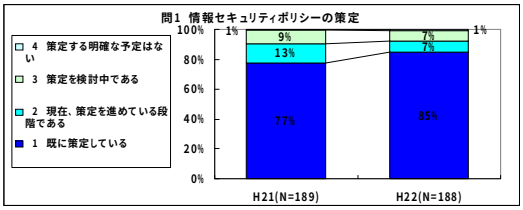
前回の調査結果と比べ、情報セキュリティ対策に係る中期目標への明記・ＰＤＣＡサイクルの構築ともに一定の進捗が見られた。
しかし、第2次基本計画決定にも関わらず、依然として、1割以上の独立行政法人等において中期目標への明記予定がない、2割近い独立行政法人等においてCISOが設置されてない、また、多くの独立行政法人等において最高情報セキュリティアドバイザーの設置に進捗が見られないなど、組織全体での情報セキュリティへの取組に欠けるとともに、組織マネジメント上の問題が残されていると言わざるを得えない。今後このような点を重点的に後押しする必要がある。

＜情報セキュリティ対策に係る中期目標への明記＞



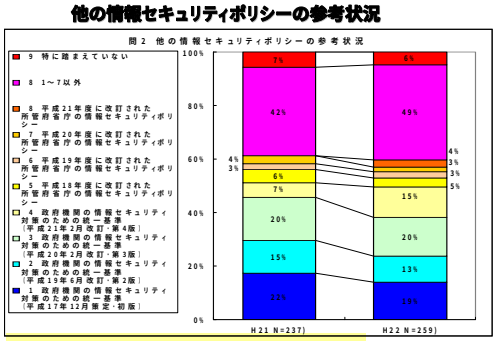
前回の調査結果と比べ、既に中期目標に明記されている法人の割合が増加し、一定の進捗が見られている。一方で、第2次基本計画で明記が決定されているにも関わらず、言及する予定がないとする法人が未だ13%存在しており、所管府省庁へのより一層の働きかけが必要。

＜情報セキュリティポリシーの策定状況＞



前回の調査結果と比べ一定の進捗が見られ、全体の8割弱で情報セキュリティポリシーが策定済みとなった。
しかし、情報セキュリティポリシー策定の際に、数年前の基準を基にしているものも多く、最新の脅威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。

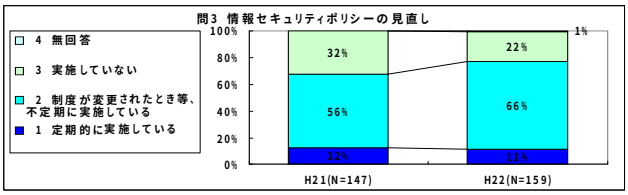
他の情報セキュリティポリシーの参考状況



『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）

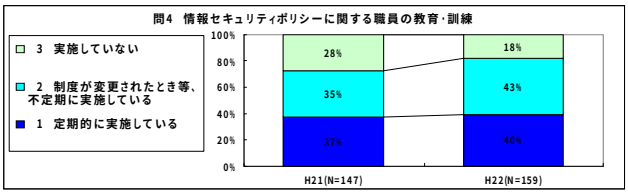
＜情報セキュリティポリシー策定済み法人の対策実施状況＞

ポリシーの見直し



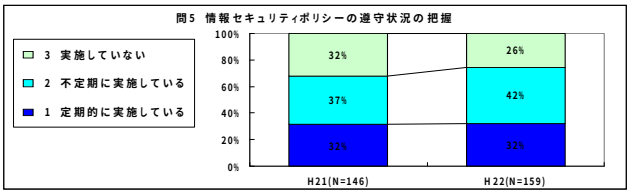
定期・不定期で、全体の88%が実施。

職員の教育・訓練



定期・不定期で、全体の83%が実施。

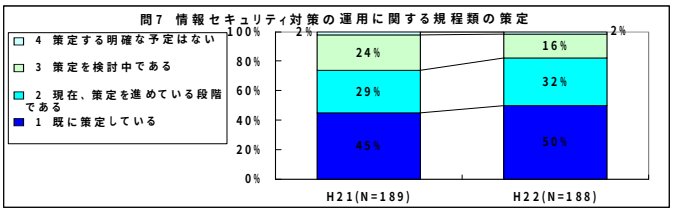
遵守状況の把握



定期・不定期で、全体の75%が実施。

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、ポリシーに基づく対策の実施（Do）、評価（Check）、見直し（Act）の徹底は前回調査よりも進んでいるが、遵守状況の把握などにける未実施の改善が今後も必要。

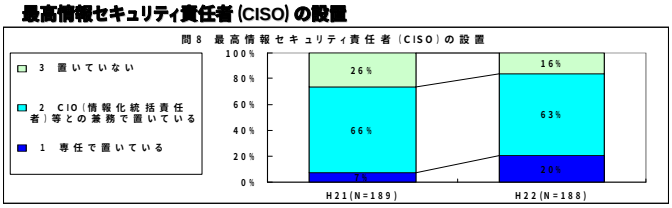
＜情報セキュリティポリシー対策の運用に関する規程類の策定状況＞



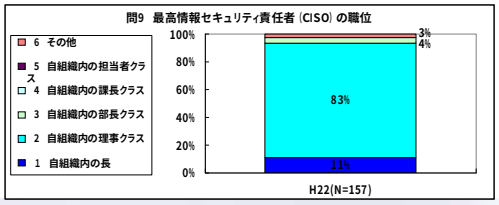
情報セキュリティポリシー対策の運用に関する規程類の策定状況においても、前回調査よりも着実に進捗しているが、2割近くが未策定。

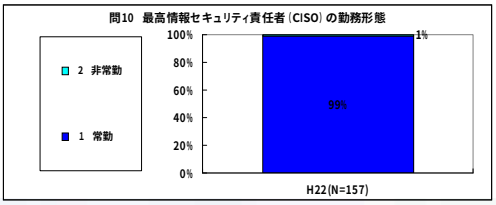
＜情報セキュリティ対策推進体制の整備状況　その1＞

最高情報セキュリティ責任者（CISO）の設置



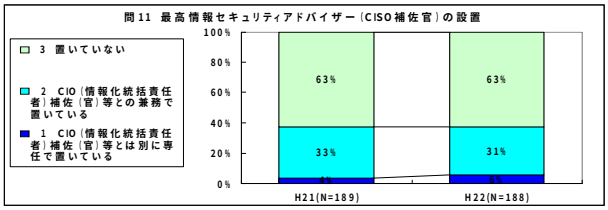
最高情報セキュリティ責任者（CISO）の設置は、前回調査より進捗したが、2割近くが未設置。
職位・勤務形態については、理事クラス・常勤が大半であることが判明した。



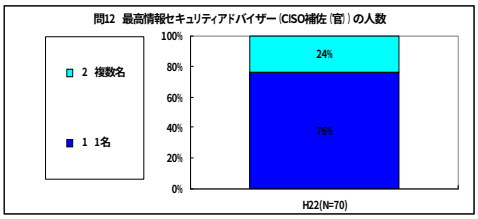


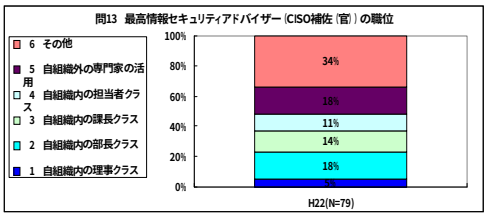
＜情報セキュリティ対策推進体制の整備状況　その2＞

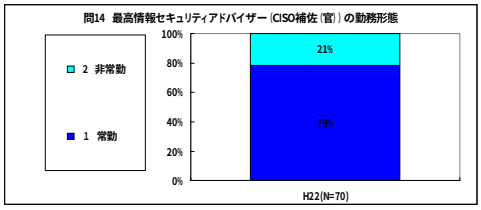
最高情報セキュリティアドバイザー（CISO補佐官）の設置

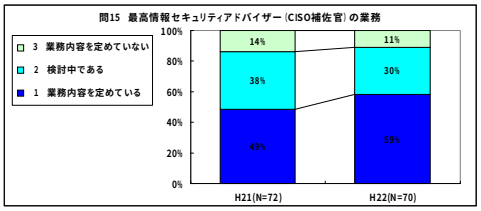


最高情報セキュリティアドバイザー（CISO補佐官）の設置は、前回調査より進捗なく、多くの法人において未設定。職位・勤務形態については、補佐官の人数・勤務形態については、1名・常勤が大半であったが、職位については法人によって異なっていることが判明した。



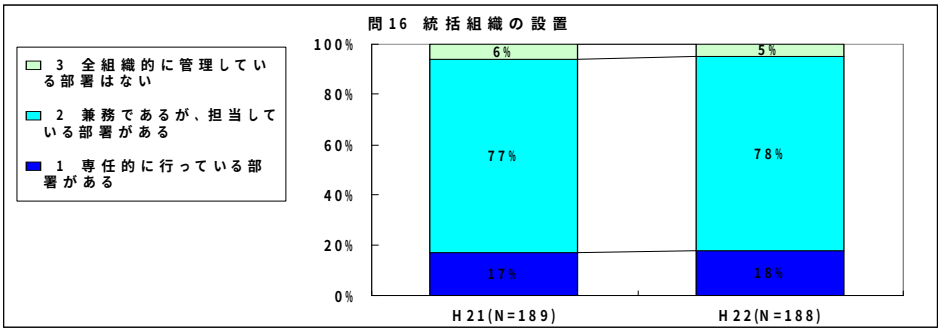






＜情報セキュリティ対策推進体制の整備状況　その3＞

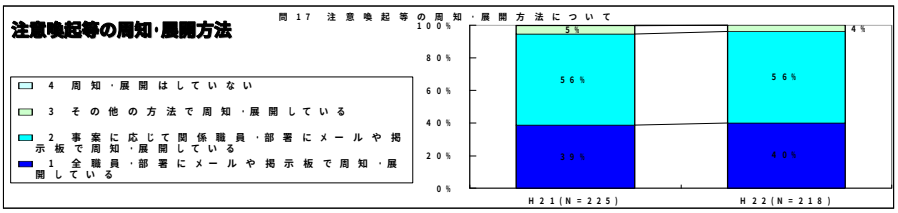
統括組織の設置



情報セキュリティ対策の統括組織の設置状況については、専任部署と兼務部署の比率は前回調査とほぼ変化していない。

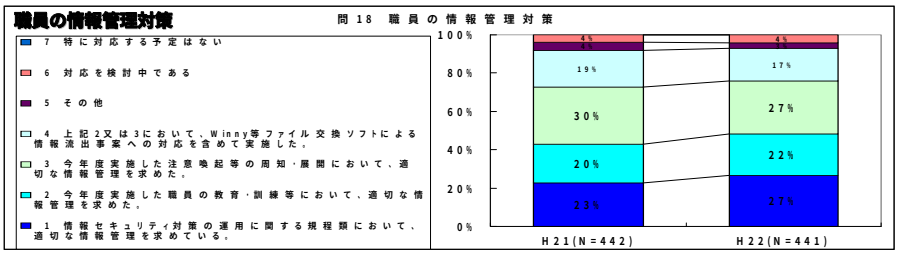
＜緊急時を含め実効性のある連絡体制の整備 その1＞

注意喚起等の周知・展開方法



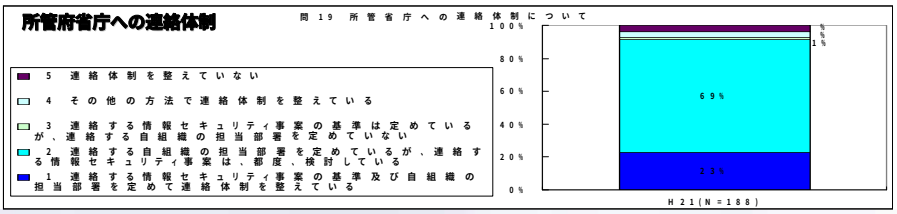
全職員・部署もしくは関係職員・部署への周知・展開の割合は、前回調査より進捗。

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から、規程類や教育・訓練等の体制を構築しての恒常的な徹底へと変化。

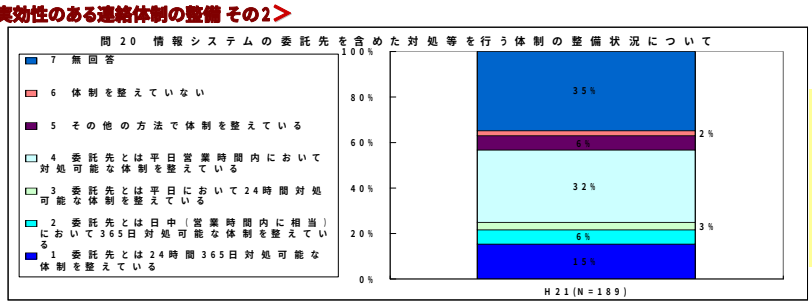
所管府省庁への連絡体制



連絡する担当部署を定めている場合がほとんどであることが判明した。一方、連絡する事案は都度検討が大半であった。

＜緊急時を含め実効性のある連絡体制の整備 その2＞

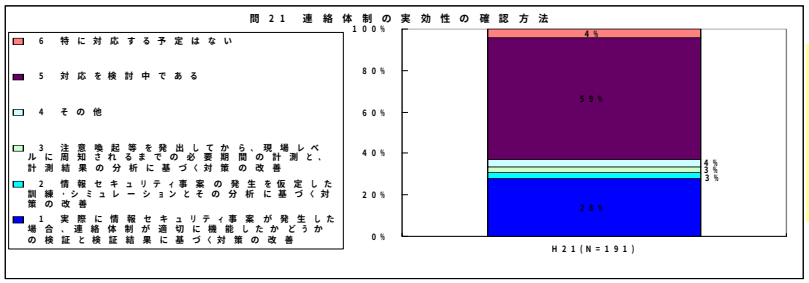
委託先を含めた体制整備



委託先とは、平日営業時間内もしくは24時間365日での対処可能な体制を整えていることが判明。

一方、無回答の割合が多く、把握が不十分な法人が多いものと推察されることに懸念。

連絡体制の実効性の確認方法



連絡体制の実効性確認については、その方法を検討している法人が多くを占めた。

一方、実際に検証を実施し、それによる改善を行っている法人も3割弱あり、今後の増加に期待。

緊急時を含め実効性のある連絡体制の整備 として、前回より調査している注意喚起等の周知・展開方法及び職員の情報管理対策については、それぞれ進捗が見られている。
一方、所管府省庁への連絡体制、委託先を含めた体制整備、連絡体制の実効性の確認方法については、昨年6月発出の事務連絡を受けて進捗しているものと考えられるが、今後とも調査を行うことで継続的な確認が必要。

別添６

企業・個人における現状の評価

（１）施策の取組み結果に関する評価等

（ア）企業

① 情報セキュリティガバナンスの「経営の一環としての位置付け」の確立に係る指標

・「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に基づく認証取得組織数」

（日本情報処理開発協会）

	平成 21 年度	平成 20 年度
組織数	3,474	3,171

・「Number of Certificates Per Country」

（ISMS International User Group）

平成 22 年3月			平成 20 年 11 月		
国／地域	組織数	割合	国／地域	組織数	割合
―	6,385	―	―	4,987	―
日本	3,480	54.5%	日本	2,863	57.4%
ｲﾝﾄﾞ	495	7.8%	ｲﾝﾄﾞ	433	8.7%
英国	444	7.0%	英国	368	7.4%
台湾	385	6.0%	台湾	202	4.1%
中国	347	5.4%	中国	174	3.5%
ﾄﾞｲﾂ	136	2.1%	ﾄﾞｲﾂ	108	2.2%
韓国	106	1.7%	韓国	71	1.4%
米国	95	1.5%	米国	82	1.6%
チェコ	85	1.3%	チェコ	66	1.3%
ハンガリー	70	1.1%	ハンガリー	74	1.5%

② 企業の情報セキュリティ向上に資する製品やサービスの提供促進と活動の推進に係る指標

・「IT セキュリティ評価及び認証制度に基づく認証取得製品数」

（情報処理推進機構）

	平成 21 年度	平成 20 年度
新規認証	38	60
保証継続	9	12

・「暗号モジュール試験及び認証制度に基づく認証取得製品数」

（情報処理推進機構）

平成 21 年度	平成 20 年度
2	5

③ 企業における情報セキュリティ人材の育成・確保に係る指標

・「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 21 年度[1]	平成 20 年度[2]
応募者数	52,043	46,582
受験者数	34,074	29,300
合格者数	5,906	4,507
合格率	17.3%	15.4%

・「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 21 年度	平成 20 年度
応募者数	5,313	7,347
受験者数	3,271	4,145
合格者数	455	422
合格率	13.9%	10.2%

④ 「事故前提社会」への対応力強化に向けた事業継続性確保・緊急対応体制の強化に係る指標

・「JPCERT/CC と連携しているコンピュータセキュリティ緊急対応チーム（CSIRT）の数」

（JPCERT/CC）

平成 22 年3月末	平成 21 年3月末
19	16

・「JPCERT/CC に登録している国内の製品開発ベンダー等の担当窓口の数」

（JPCERT/CC）

平成 22 年3月末	平成 21 年3月末
329	283

[1] 情報セキュリティスペシャリスト試験

[2] テクニカルエンジニア（情報セキュリティ）試験及び情報セキュリティアドミニストレータ試験

・「事業継続計画策定状況」

（情報処理実態調査：経済産業省）

対策実施状況

	平成 20 年度[3]		平成 19 年度[4]	
	回答数	割合	回答数	割合
回答企業数	4,134	—	3,826	—
既に実施している	648	15.7%	516	13.5%
トラブルがあったので対策を講じた	11	0.3%	9	0.2%
実施を検討している	615	14.9%	642	16.8%
必要性を感じるが、未実施	2,105	50.9%	1,958	51.2%
必要性を感じず、未実施	766	18.5%	710	18.6%

セキュリティ向上への寄与

	平成 20 年度 [3]		平成 19 年度 [4]	
	回答数	割合	回答数	割合
回答企業数	949	—	916	—
寄与した	569	60.0%	537	58.6%
寄与しなかった	26	2.7%	29	3.2%
わからない	354	37.3%	350	38.2%

⑤ 中小企業の情報セキュリティ対策の推進に係る指標

・「情報セキュリティセミナーの実施状況」

（情報処理推進機構）

	平成 21 年度	平成 20 年度
開催地数（全国）	35	34
開催回数	113	110
開催内容	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）	4種類 ・基礎 ・マネジメント ・技術（標準編） ・技術（専門編）

[3] 平成 19 年度実施調査（平成 20 年度公表）

[4] 平成 18 年度実施調査（平成 19 年度公表）

・「SaaS 利用に伴う外部への支払い費用・SLA の締結状況」（企業規模別）

（情報処理実態調査：経済産業省）

SaaS にかかる外部支払いの発生状況（年間事業収入規模別）

	平成 20 年度[5]			平成 19 年度[6]		
	回答数	発生した	発生しなかった	回答数	発生した	発生しなかった
～1億円以下	12	1	11	14	―	14
1億円超～5億円以下	67	3	64	94	4	90
5億円超～10 億円以下	204	10	194	211	11	200
10 億円超～20 億円以下	458	23	435	425	19	406
20 億円超～100 億円以下	1,559	93	1,466	1,377	90	1,287
100 億円超～1,000 億円以下	1,506	104	1,402	1,350	85	1,265
1,000 億円超～	530	69	461	474	48	426
不明	144	17	127	146	11	135
全体	4,480	320	4,160	4,091	268	3,823

SaaS 導入・利用時の SLA 締結状況（年間事業収入規模別）

	平成 20 年度[5]			平成 19 年度[6]		
	回答数	発生した	発生しなかった	回答数	発生した	発生しなかった
～1億円以下	―	―	―	―	―	―
1億円超～5億円以下	3	―	3	4	1	3
5億円超～10 億円以下	10	4	6	11	4	7
10 億円超～20 億円以下	21	11	10	19	7	12
20 億円超～100 億円以下	92	41	51	87	35	52
100 億円超～1,000 億円以下	95	42	53	84	35	49
1,000 億円超～	63	28	35	48	29	19
不明	15	5	10	9	4	5
全体	299	131	168	262	115	147

・「ASP・SaaS の利用状況」

（通信利用動向調査：総務省）

	平成 21 年末	平成 20 年末
回答数	1,834	2,012
利用しており、非常に効果があった	4.2%	2.5%
利用しており、ある程度効果があった	11.5%	8.9%
利用しているが、あまり効果がなかった	0.7%	0.5%
利用しているが、マイナスの効果であった	―	0.0%
利用しているが効果はよく分からない	3.6%	3.5%
利用していないが、今後利用する予定	18.6%	13.7%
利用していないし、今後も利用する予定はない	28.4%	36.1%
ASP・SaaS についてよく分からない	30.6%	32.5%
無回答	2.4%	2.2%

[5] 平成 19 年度実施調査（平成 20 年度公表）

[6] 平成 18 年度実施調査（平成 19 年度公表）

（イ）個人

① 情報セキュリティ教育の強化・推進に係る指標

・「情報モラルなどを指導する能力を有すると回答した教員の割合」

（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）

小学校

	平成 20 年度		平成 19 年度	
	回答	割合	回答	割合
全体	―	69.8%	―	68.0%
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。	277,530	70.0%	273,469	68.2%
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。	284,823	71.9%	281,411	70.2%
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。	288,225	72.9%	285,258	71.1%
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つけることができるように指導する。	254,861	64.4%	250,646	62.5%

中学校

	平成 20 年度		平成 19 年度	
	回答	割合	回答	割合
全体	―	64.7%	―	63.2%
生徒が情報社会への参画にあたって責任ある態度と義務を果たし、情報に関する自分や他者の権利を理解し尊重できるように指導する。	147,260	65.8%	146,880	64.8%
生徒が情報の保護や取り扱いに関する基本的なルールや法律の内容を理解し、反社会的な行為や違法な行為などに対して適切に判断し行動できるように指導する。	149,507	67.0%	148,865	65.7%
生徒がインターネットなどを利用する際に、情報の信頼性やネット犯罪の危険性などを理解し、情報を正しく安全に活用できるように指導する。	149,926	67.2%	148,968	65.7%
生徒が情報セキュリティに関する基本的な知識を身に付け、コンピュータやインターネットを安全に使えるように指導する。	131,032	58.6%	128,837	56.8%

高等学校

	平成 20 年度		平成 19 年度	
	回答	割合	回答	割合
全体	―	66.4%	―	64.4%
生徒が情報社会への参画にあたって責任ある態度と義務を果たし、情報に関する自分や他者の権利を理解し尊重できるように指導する。	120,944	68.0%	120,834	66.3%
生徒が情報の保護や取り扱いに関する基本的なルールや法律の内容を理解し、反社会的な行為や違法な行為などに対して適切に判断し行動できるように指導する。	122,087	68.7%	121,853	66.8%
生徒がインターネットなどを利用する際に、情報の信頼性やネット犯罪の危険性などを理解し、情報を正しく安全に活用できるように指導する。	120,652	67.9%	120,605	66.1%
生徒が情報セキュリティに関する基本的な知識を身に付け、コンピュータやインターネットを安全に使えるように指導する。	107,979	60.9%	106,812	58.6%

・「インターネット安全教室参加者数（概数）」

（経済産業省）

	平成 21 年度	平成 20 年度
開催数	154	125
参加人数	9,600	7,451

・「e-ネットキャラバン参加者数（概数）」

（総務省・文部科学省）

	平成 21 年度	平成 20 年度
講座数	624	1,208
受講人数	65,000	130,000

② 個人の底上げに向けたより効果的な普及・啓発活動の実現に係る指標

・「情報セキュリティに係る政府系 web サイトへのアクセス状況」[7]

（内閣官房、警察庁、総務省、経済産業省）

省庁等	名称	今回評価	前回評価
内閣官房	情報セキュリティセンターホームページ	566,834 人[8]	423,540 人[9]
警察庁	サイバー犯罪対策	509,902 件[8]	181,474 人[11]
	@police	2,242,578 件[8]	1,225,538 人[9]
総務省	国民のための情報セキュリティサイト	150,961 件[10]	163,742 件[9]
経済産業省	情報セキュリティに関する政策･緊急情報	138,770 件[10]	159,890 件[11]
	CHECK PC! ホームページ	6,784,919 件[12]	1,460,305 件[13]
	Japan Vulnerability Notes (JVN)	2,552,007 件[10]	2,321,257 件[11]
情報処理推進機構（IPA）	IPA セキュリティセンターホームページ	27,960,232 件[10]	27,588,987 件[11]
JPCERT コーディネーションセンター	JPCERT/CC ホームページ	1,692,190 件[10]	1,511,674 件[11]

[7] 集計方法については各府省庁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。

[8] 平成 21 年

[9] 平成 20 年

[10] 平成 21 年度

[11] 平成 20 年度

[12] 平成 21 年５月 29 日から３月 31 日まで

[13] 平成 21 年１月 30 日から２月 28 日まで

・「インターネットにおける情報セキュリティ脅威に関する情報・対策情報の入手方法」

（インターネットの利用実態に関する調査：総務省）

「セキュリティ脅威」に関する情報の入手の有無

	平成 20 年	平成 19 年
回答者数	2,979	3,027
定期的に入手	14.9%	17.6%
不定期に入手	43.2%	48.3%
入手していない	41.9%	34.2%

「セキュリティ脅威」に関する情報の入手先

	平成 20 年	平成 19 年
回答者数	2,385	1,993
テレビ・ラジオ	18.3%	30.5%
新聞	18.5%	20.6%
雑誌・広告	13.3%	15.7%
Web（ニュース配信サイトなど）	68.0%	73.7%
Web（政府、地方公共団体）	5.4%	6.5%
ISP からのお知らせ	19.0%	22.9%
セキュリティ対策ソフトの会社	64.8%	51.0%
会社の担当部署や知人から	8.8%	11.1%
その他	3.2%	3.8%

「セキュリティ対策」に関する情報の入手の有無

	平成 20 年	平成 19 年
全回答者数	2,979	3,090
定期的に入手	21.1%	19.9%
不定期に入手	46.0%	49.5%
入手していない	32.9%	30.5%

「セキュリティ対策」に関する情報の入手先

	平成 20 年	平成 19 年
回答者数	2,468	2,147
テレビ・ラジオ	11.6%	21.4%
新聞	11.9%	14.5%
雑誌・広告	10.6%	13.6%
Web（ニュース配信サイト等）	59.1%	67.4%
Web（政府、地方公共団体）	4.4%	6.0%
ISP からのお知らせ(Web・メール)	18.3%	23.7%
ウィルスを含むセキュリティ対策ソフトの会社	67.2%	54.1%
職場、学校、知人	7.9%	15.6%
その他	2.5%	2.2%

・「セキュリティ情報の入手方法」

（情報セキュリティに関する脅威に対する意識調査：情報処理推進機構）

平成 21 年度

回答数：5,019	現在入手している情報源	今後望ましい情報源
ウェブ上のニュース	50.8%	35.4%
ポータルサイト	39.0%	28.0%
メールマガジン、メーリングリスト	20.5%	12.1%
テレビのニュース、情報番組での解説コーナー	19.7%	18.2%
専門機関のウェブサイト	19.5%	22.7%
ブログ、掲示板等	18.8%	8.5%
新聞	18.8%	16.6%
Q&A サイト	18.1%	10.1%
テレビ CM	14.4%	12.7%
パソコン売場など量販店の店頭ポスター・チラシ	11.4%	10.6%
mixi などの SNS 内コミュニティ	8.3%	5.7%
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）	7.1%	10.8%
無料配布冊子	7.0%	10.2%
行政や業者による無料セミナー	3.9%	9.4%
その他	1.3%	1.8%
特にない	25.3%	24.7%

平成 20 年度[14]

回答数：5,000	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	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	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	被害が起きたときの相談や届出に関する情報	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
テレビ、新聞、雑誌、専門書	26.8%	19.6%	14.7%	13.5%	13.1%
家族、友人、知人の話	11.4%	10.3%	9.5%	7.9%	6.9%
セキュリティ対策ソフトベンダーのウェブサイト、メールマガジン等	20.2%	20.5%	22.1%	13.5%	11.8%
セキュリティベンダー以外のベンダー（パソコンメーカー、プロバイダ等）のウェブサイト、メールマガジン等	11.5%	10.5%	9.2%	7.0%	6.6%
政府、自治体、その他セキュリティ関連団体のウェブサイト、メールマガジン等	3.5%	3.1%	1.5%	5.1%	2.2%
インターネットのニュース、掲示板	29.9%	24.6%	22.2%	19.6%	23.0%
その他	0.4%	0.3%	0.5%	0.3%	0.2%

[14] 平成 20 年度 第 2 回調査

③ 対策が困難な個人も含めた情報セキュリティ水準向上に向けた取組みに係る指標

・「サイバークリーンセンター活動実績」

（サイバークリーンセンター：総務省、経済産業省）

	平成 22 年3月末	平成 21 年3月末
ウィルス対策ソフトへの反映状況（各ベンダ平均値）	99.3%	99.6%
収集検体に対する CCC クリーナーの対応状況	99.5%	99.4%
ユーザに対する注意喚起数	113,815	140,720
駆除ツールのダウンロード数	451,202	379,904

・「パソコンのボット感染度」[15]

（日本の ICT インフラに関する国際比較評価レポート：総務省）

	平成 21 年	平成 20 年
日本	78.1	77.6
韓国	50.5	50.2
中国	42.3	42.1
シンガポール	43.2	43.0
台湾	42.2	42.0
イタリア	46.1	45.8
カナダ	46.6	46.3
オーストリア	53.5	53.1
オランダ	58.5	58.0
フィンランド	78.1	77.6
スイス	47.8	47.5
オーストラリア	45.7	45.4
フランス	42.7	42.5
米国	46.6	46.3
ニュージーランド	49.5	49.1
ポルトガル	41.9	41.6
イギリス	44.6	44.3
香港	53.5	53.1
ドイツ	43.2	43.0
スペイン	41.2	40.9
ベルギー	50.5	50.2
デンマーク	55.6	55.2
スウェーデン	55.6	55.2
インド	42.5	―

15 「（偏差値）＝（（各国・地域の値）－（平均値））÷標準偏差×10＋50」にて算出。各国・地域の値、平均値はブロードバンド加入者 100 人当たりのボット感染 PC 台数の逆数。

（２）施策の取組みによる社会的変化に関する評価等

（ア）企業

① 企業の情報セキュリティ意識に係る指標

・「情報セキュリティ上のトラブル（システムトラブル、不正アクセス、コンピュータウィルス、重要情報の漏えい等）の重要性の認識」

（情報処理実態調査：経済産業省）

		平成 20 年度[16]				平成 19 年度[17]			
		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	87.2%	10.9%	0.7%	1.2%	84.4%	12.7%	1.4%	1.5%
	外部要因（地震、火災等の問題）によるシステムの停止	77.7%	19.6%	1.2%	1.5%	73.1%	23.8%	1.4%	1.7%
その他のシステムトラブル	DoS 攻撃	53.6%	33.2%	5.3%	7.9%	51.5%	33.7%	6.9%	7.9%
	スパムメールの中継利用等	53.7%	34.4%	5.1%	6.8%	50.2%	36.2%	6.1%	7.5%
	ホームページやファイル、データの改ざん	66.6%	26.6%	3.2%	3.5%	66.0%	26.1%	4.3%	3.6%
不正アクセス	IP・メールアドレス詐称	63.4%	29.0%	4.0%	3.6%	62.8%	28.7%	4.6%	4.0%
	リソースの不正使用	60.5%	30.7%	3.7%	5.1%	58.4%	31.4%	4.4%	5.8%
	内部関係者による不正アクセス	72.8%	22.1%	2.2%	2.8%	73.1%	21.2%	2.6%	3.0%
コンピュータウイルス	ウィルスなどの感染	78.2%	19.8%	0.8%	1.2%	78.2%	19.3%	1.0%	1.5%
	トロイの木馬	72.6%	23.3%	1.3%	2.8%	71.9%	23.1%	1.7%	3.4%
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	87.6%	10.2%	0.8%	1.3%	86.2%	11.0%	1.3%	1.6%
	不正アクセスによる情報漏えい	85.1%	12.2%	1.2%	1.5%	84.2%	12.3%	1.7%	1.8%
	内部者による情報漏えい	87.2%	10.7%	0.8%	1.4%	86.3%	11.1%	1.1%	1.6%
	委託先による情報漏えい	80.8%	14.6%	2.1%	2.6%	79.3%	15.3%	2.7%	2.6%
	ノートパソコン及び携帯記憶媒体等の盗難・紛失	79.1%	17.6%	1.8%	1.5%	78.1%	18.3%	2.0%	1.6%
その他	ホームページ上での誹謗中傷等	43.4%	42.5%	9.3%	4.7%	44.3%	41.8%	8.8%	5.2%
	その他	26.6%	29.7%	9.4%	34.3%	27.1%	28.0%	8.5%	36.4%

16 平成 19 年度実施調査（平成 20 年度公表）

17 平成 18 年度実施調査（平成 19 年度公表）

・「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 20 年度 [16]		平成 19 年度 [17]	
	回答数	割合	回答数	割合
回答企業数	3,090	—	3,033	—
顧客･取引先からの評価の上昇	791	25.6%	762	25.1%
市場や投資家からの評価の上昇	111	3.6%	123	4.1%
製品やサービスの質の向上	303	9.8%	267	8.8%
業務効率や生産性の向上	408	13.2%	448	14.8%
特に効果はなかった	1,218	39.4%	1,268	41.8%
その他	721	23.3%	560	18.5%

・「情報セキュリティ対策の阻害要因（トップの理解、予算等）」

（情報処理実態調査：経済産業省）

	平成 20 年度 [16]		平成 19 年度 [17]	
	回答数	割合	回答数	割合
回答企業数	4,404	—	4,000	—
実施する知識･ノウハウがない	987	22.4%	1,053	26.3%
手間･コストがかかる	2,935	66.6%	2,852	71.3%
予算がとれない	1,098	24.9%	954	23.9%
必要性や効果がわからない	380	8.6%	—	—
対策をどこまでやるべきかがわからない	1,816	41.2%	1,920	48.0%
情報セキュリティガバナンスが確立されていない	632	14.4%	—	—
トップの理解･協力が得られない	294	6.7%	302	7.6%
従業員の理解･協力が得られない	496	11.3%	553	13.8%
企業のセキュリティ対策方針が明確になっていない	746	16.9%	241	6.0%
専門家（CIO や CISO）がいない	668	15.2%	—	—
その他	135	3.1%	262	6.6%
問題はない	386	8.8%	—	—

② 企業の情報セキュリティ対策状況に係る指標

a）情報セキュリティ対策の確立に係る指標

・「リスク分析実施状況」

（情報処理実態調査：経済産業省）

対策実施状況

	平成 20 年度 [16]		平成 19 年度 [17]	
	回答数	割合	回答数	割合
回答企業数	4,201	—	3,881	—
既に実施している	1,413	33.6%	1,193	30.7%
トラブルがあったので対策を講じた	44	1.0%	31	0.8%
実施を検討している	412	9.8%	477	12.3%
必要性を感じるが、未実施	1,906	45.4%	1,832	47.2%
必要性を感じず、未実施	470	11.2%	379	9.8%

セキュリティ向上への寄与

	平成 20 年度 [16]		平成 19 年度 [17]	
	回答数	割合	回答数	割合
回答企業数	1,482	—	1,406	—
寄与した	1,102	74.4%	1,034	73.5%
寄与しなかった	33	2.2%	30	2.1%
わからない	347	23.4%	342	24.3%

・「情報セキュリティポリシーの策定状況」

（情報処理実態調査：経済産業省）

対策実施状況

	平成 20 年度[18]		平成 19 年度[19]	
	回答数	割合	回答数	割合
回答企業数	4,246	—	3,938	—
既に実施している	2,078	48.9%	1,821	46.2%
ﾄﾗﾌﾞﾙがあったので対策を講じた	44	1.0%	50	1.3%
実施を検討している	453	10.7%	537	13.6%
必要性を感じるが、未実施	1,368	32.2%	1,309	33.2%
必要性を感じず、未実施	347	8.2%	271	6.9%

セキュリティ向上への寄与

	平成 20 年度 [18]		平成 19 年度 [19]	
	回答数	割合	回答数	割合
回答企業数	2,102	—	2,030	—
寄与した	1,552	73.8%	1,466	72.2%
寄与しなかった	49	2.3%	52	2.6%
わからない	501	23.8%	512	25.2%

・「情報セキュリティ報告書の作成状況」

（情報処理実態調査：経済産業省）

対策実施状況

	平成 20 年度 [18]		平成 19 年度 [19]	
	回答数	割合	回答数	割合
回答企業数	4,181	—	3,871	—
既に実施している	631	15.1%	525	13.6%
ﾄﾗﾌﾞﾙがあったので対策を講じた	14	0.3%	11	0.3%
実施を検討している	425	10.2%	467	12.1%
必要性を感じるが、未実施	2,220	53.1%	2,131	55.1%
必要性を感じず、未実施	905	21.6%	748	19.3%

セキュリティ向上への寄与

	平成 20 年度 [18]		平成 19 年度 [19]	
	回答数	割合	回答数	割合
回答企業数	823	—	790	—
寄与した	506	61.5%	475	60.1%
寄与しなかった	28	3.4%	25	3.2%
わからない	289	35.1%	290	36.7%

[18] 平成 19 年度実施調査（平成 20 年度公表）

[19] 平成 18 年度実施調査（平成 19 年度公表）

・「セキュリティ管理者の配置状況」

（情報処理実態調査：経済産業省）

全社的なセキュリティ管理者の配置

対策実施状況

	平成 20 年度 [18]		平成 19 年度 [19]	
	回答数	割合	回答数	割合
回答企業数	4,247	—	3,941	—
既に実施している	2,029	47.8%	1,763	44.7%
トラブルがあったので対策を講じた	45	1.1%	51	1.3%
実施を検討している	373	8.8%	449	11.4%
必要性を感じるが、未実施	1,487	35.0%	1,445	36.7%
必要性を感じず、未実施	358	8.4%	284	7.2%

セキュリティ向上への寄与

	平成 20 年度 [18]		平成 19 年度 [19]	
	回答数	割合	回答数	割合
回答企業数	1,970	—	1,901	—
寄与した	1,525	77.4%	1,454	76.5%
寄与しなかった	41	2.1%	42	2.2%
わからない	404	20.5%	405	21.3%

部門ごとのセキュリティ管理者の配置

対策実施状況

	平成 20 年度 [18]		平成 19 年度 [19]	
	回答数	割合	回答数	割合
回答企業数	4,230	—	3,929	—
既に実施している	1,452	34.3%	1,282	32.6%
トラブルがあったので対策を講じた	29	0.7%	36	0.9%
実施を検討している	397	9.4%	435	11.1%
必要性を感じるが、未実施	1,732	40.9%	1,680	42.8%
必要性を感じず、未実施	649	15.3%	532	13.5%

セキュリティ向上への寄与

	平成 20 年度 [18]		平成 19 年度 [19]	
	回答数	割合	回答数	割合
回答企業数	1,519	—	1,472	—
寄与した	1,152	75.8%	1,076	73.1%
寄与しなかった	43	2.8%	44	3.0%
わからない	324	21.3%	352	23.9%

・「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 20 年度[20]		平成 19 年度[21]	
	回答数	割合	回答数	割合
回答企業数	4,222	—	3,909	—
既に実施している	1,566	37.1%	1,026	26.2%
ﾄﾗﾌﾞﾙがあったので対策を講じた	31	0.7%	19	0.5%
実施を検討している	741	17.6%	1,011	25.9%
必要性を感じるが、未実施	1,553	36.8%	1,599	40.9%
必要性を感じず、未実施	362	8.6%	273	7.0%

セキュリティ向上への寄与

	平成 20 年度 [20]		平成 19 年度 [21]	
	回答数	割合	回答数	割合
回答企業数	1,814	—	1,627	—
寄与した	1,264	69.7%	1,063	65.3%
寄与しなかった	47	2.6%	39	2.4%
わからない	503	27.7%	525	32.3%

b）情報セキュリティ対策の導入及び運用に係る指標

・「重要なシステムへの内部でのアクセス管理の実施状況」

（情報処理実態調査：経済産業省・通信利用動向調査：総務省）

対策実施状況

	平成 20 年度 [20]		平成 19 年度 [21]	
	回答数	割合	回答数	割合
回答企業数	4,250	—	3,902	—
既に実施している	2,700	63.5%	2,369	60.7%
ﾄﾗﾌﾞﾙがあったので対策を講じた	42	1.0%	47	1.2%
実施を検討している	308	7.2%	367	9.4%
必要性を感じるが、未実施	918	21.6%	918	23.5%
必要性を感じず、未実施	324	7.6%	248	6.4%

セキュリティ向上への寄与

	平成 20 年度 [20]		平成 19 年度 [21]	
	回答数	割合	回答数	割合
回答企業数	2,434	—	2,271	—
寄与した	2,052	84.3%	1,906	83.9%
寄与しなかった	23	0.9%	30	1.3%
わからない	359	14.7%	335	14.8%

	平成 21 年末	平成 20 年末
回答数	1,830	1,996
対応している	96.1%	96.4%
ID、パスワードによるアクセス制御	62.0%	63.3%
アクセスログの記録	39.7%	39.2%
認証技術の導入による利用者確認	20.5%	20.5%
特に対応していない	2.1%	2.2%
無回答	1.8%	1.4%

[20] 平成 19 年度実施調査（平成 20 年度公表）

[21] 平成 18 年度実施調査（平成 19 年度公表）

・「データの暗号化実施状況」

（情報処理実態調査：経済産業省・通信利用動向調査：総務省）

対策実施状況

	平成 20 年度 [20]		平成 19 年度 [21]	
	回答数	割合	回答数	割合
回答企業数	4,187	—	3,860	—
既に実施している	1,398	33.4%	1,199	31.1%
ﾄﾗﾌﾞﾙがあったので対策を講じた	37	0.9%	23	0.6%
実施を検討している	415	9.9%	468	12.1%
必要性を感じるが、未実施	1,628	38.9%	1,538	39.8%
必要性を感じず、未実施	746	17.8%	655	17.0%

セキュリティ向上への寄与

	平成 20 年度 [20]		平成 19 年度 [21]	
	回答数	割合	回答数	割合
回答企業数	1,470	—	1,347	—
寄与した	1,181	80.3%	1,054	78.2%
寄与しなかった	17	1.2%	19	1.4%
わからない	272	18.5%	274	20.3%

	平成 21 年末	平成 20 年末
回答数	1,830	1,996
対応している	96.1%	96.4%
データやﾈｯﾄﾜｰｸの暗号化	23.7%	22.9%
特に対応していない	2.1%	2.2%
無回答	1.8%	1.4%

・「外部接続へのファイアーウォールの配置状況」

（情報処理実態調査：経済産業省・通信利用動向調査：総務省）

対策実施状況

	平成 20 年度 [20]		平成 19 年度 [21]	
	回答数	割合	回答数	割合
回答企業数	4,233	—	3,881	—
既に実施している	3,113	73.5%	2,797	72.1%
ﾄﾗﾌﾞﾙがあったので対策を講じた	69	1.6%	78	2.0%
実施を検討している	137	3.2%	168	4.3%
必要性を感じるが、未実施	655	15.5%	612	15.8%
必要性を感じず、未実施	328	7.7%	304	7.8%

セキュリティ向上への寄与

	平成 20 年度 [20]		平成 19 年度 [21]	
	回答数	割合	回答数	割合
回答企業数	2,657	—	2,489	—
寄与した	2,327	87.6%	2,165	87.0%
寄与しなかった	18	0.7%	20	0.8%
わからない	312	11.7%	304	12.2%

	平成 21 年末	平成 20 年末
回答数	1,830	1,996
対応している	96.1%	96.4%
外部接続の際にｳｨﾙｽｳｫｰﾙを構築	29.0%	29.1%
特に対応していない	2.1%	2.2%
無回答	1.8%	1.4%

・「セキュリティ監視ソフトの導入状況」

（情報処理実態調査：経済産業省・通信利用動向調査：総務省）

対策実施状況

	平成 20 年度[22]		平成 19 年度[23]	
	回答数	割合	回答数	割合
回答企業数	4,222	—	3,893	—
既に実施している	2,285	54.1%	1,973	50.7%
トラブルがあったので対策を講じた	118	2.8%	89	2.3%
実施を検討している	328	7.8%	374	9.6%
必要性を感じるが、未実施	1,188	28.1%	1,168	30.0%
必要性を感じず、未実施	421	10.0%	378	9.7%

セキュリティ向上への寄与

	平成 20 年度 [22]		平成 19 年度 [23]	
	回答数	割合	回答数	割合
回答企業数	2,046	—	1,882	—
寄与した	1,743	85.2%	1,544	82.0%
寄与しなかった	19	0.9%	20	1.1%
わからない	284	13.9%	318	16.9%

	平成 21 年末	平成 20 年末
回答数	1,830	1,996
対応している	96.1%	96.4%
不正侵入検知システム(IDS)の導入	13.4%	12.4%
特に対応していない	2.1%	2.2%
無回答	1.8%	1.4%

・「情報セキュリティ教育の実施状況等」

（不正アクセス行為対策等の実態調査：警察庁）

	平成 21 年	平成 20 年
回答数	930	775
実施している	56.3%	44.1%
実施を予定している	6.2%	5.0%
実施はしていないが必要性を感じる	34.1%	45.5%
実施の必要性を感じない（実施していない）	2.5%	4.1%
無回答	0.9%	1.2%

[22] 平成 19 年度実施調査（平成 20 年度公表）

[23] 平成 18 年度実施調査（平成 19 年度公表）

・「従業員に対する情報セキュリティ教育の実施状況」

（情報処理実態調査：経済産業省）

対策実施状況

	平成 20 年度 [22]		平成 19 年度 [23]	
	回答数	割合	回答数	割合
回答企業数	4,269	—	3,953	—
既に実施している	1,879	44.0%	1,675	42.4%
トラブルがあったので対策を講じた	119	2.8%	110	2.8%
実施を検討している	507	11.9%	534	13.5%
必要性を感じるが、未実施	1,638	38.4%	1,552	39.3%
必要性を感じず、未実施	245	5.7%	192	4.9%

セキュリティ向上への寄与

	平成 20 年度 [22]		平成 19 年度 [23]	
	回答数	割合	回答数	割合
回答企業数	1,939	—	1,901	—
寄与した	1,527	78.8%	1,485	78.1%
寄与しなかった	32	1.7%	29	1.5%
わからない	380	19.6%	387	20.4%

・「セキュリティパッチ適用」

（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）

外部公開ネットワークサーバ

	平成 20 年			平成 19 年		
	全体	企業	自治体	全体	企業	自治体
回答数	2,317	1,907	410	2,280	1,859	421
ほぼ全サーバに計画的に適用している（常に適用し、適用状況も把握している）	44.9%	42.9%	54.1%	44.2%	39.6%	64.1%
一部のサーバには計画的に適用、他は気がついたら適用（常に適用する方針・設定だが、実際の適用状況は不明）	12.4%	11.9%	14.9%	13.3%	12.7%	15.9%
気がついたときに適用（各ユーザーに適用を任せている）	9.1%	8.9%	10.2%	6.7%	7.0%	5.2%
ほとんど適用していない	14.2%	14.9%	10.7%	11.6%	12.7%	6.9%
分からない	11.7%	12.6%	7.6%	14.6%	16.9%	4.5%
無回答	7.6%	8.8%	2.4%	9.6%	11.0%	3.3%

内部利用ローカルサーバ

	平成 20 年			平成 19 年		
	全体	企業	自治体	全体	企業	自治体
回答数	2,317	1,907	410	2,280	1,859	421
ほぼ全サーバに計画的に適用している（常に適用し、適用状況も把握している）	38.0%	36.8%	43.4%	38.2%	35.8%	48.7%
一部のサーバには計画的に適用、他は気がついたら適用（常に適用する方針・設定だが、実際の適用状況は不明）	17.3%	17.0%	18.3%	19.4%	19.0%	21.1%
気がついたときに適用（各ユーザーに適用を任せている）	14.0%	14.7%	10.7%	10.8%	11.6%	7.1%
ほとんど適用していない	21.7%	22.1%	19.5%	21.4%	22.5%	16.2%
分からない	6.8%	6.7%	7.3%	6.7%	7.3%	3.8%
無回答	2.2%	2.6%	0.7%	3.6%	3.7%	3.1%

クライアント

	平成 20 年			平成 19 年		
	全体	企業	自治体	全体	企業	自治体
回答数	2,317	1,907	410	2,280	1,859	421
常に適用し、適用状況も把握している	32.8%	29.8%	46.8%	33.8%	30.6%	48.2%
常に適用する方針・設定だが、実際の適用状況は不明	27.6%	27.7%	26.8%	29.3%	29.7%	27.8%
各ユーザーに適用を任せている	19.5%	21.9%	8.0%	20.0%	22.2%	10.2%
ほとんど適用していない	14.7%	14.7%	14.6%	13.3%	13.5%	12.6%
分からない	3.5%	3.8%	2.0%	2.1%	2.5%	0.0%
無回答	1.9%	2.0%	1.7%	1.5%	1.6%	1.2%

・「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 20 年[24]			平成 19 年[25]		
	全体	企業	自治体	全体	企業	自治体
回答数	2,317	1,907	410	2,280	1,859	421
9割以上に導入済	86.3%	84.6%	94.1%	80.9%	78.5%	91.2%
半数に導入済	2.3%	2.5%	1.2%	2.3%	2.4%	1.9%
半数未満に導入済	2.0%	2.3%	1.0%	2.2%	2.5%	1.0%
導入していない	6.8%	7.9%	1.7%	9.7%	11.0%	4.0%
無回答	2.6%	2.7%	2.0%	5.0%	5.6%	1.9%

ローカルサーバ

	平成 20 年 [24]			平成 19 年 [25]		
	全体	企業	自治体	全体	企業	自治体
回答数	2,317	1,907	410	2,280	1,859	421
9割以上に導入済	78.1%	76.5%	85.9%	72.1%	70.0%	81.7%
半数に導入済	4.5%	4.9%	2.7%	2.3%	2.5%	1.4%
半数未満に導入済	3.5%	3.7%	2.9%	2.4%	2.4%	2.1%
導入していない	1.0%	12.2%	5.9%	18.2%	19.7%	11.6%
無回答	2.8%	2.8%	2.7%	5.0%	5.4%	3.1%

各自クライアント（パソコン）

	平成 20 年 [24]			平成 19 年 [25]		
	全体	企業	自治体	全体	企業	自治体
回答数	2,317	1,907	410	2,280	1,859	421
9割以上に導入済	90.2%	89.0%	95.6%	90.7%	89.3%	96.7%
半数に導入済	3.7%	4.1%	1.7%	3.2%	3.6%	1.2%
半数未満に導入済	3.2%	3.6%	1.0%	3.7%	4.4%	0.5%
導入していない	1.9%	2.2%	0.5%	1.8%	2.0%	1.0%
無回答	1.0%	1.0%	1.2%	0.7%	0.6%	0.7%

・「IT セキュリティ評価及び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 20 年度[26]		平成 19 年度[27]	
	回答数	割合	回答数	割合
回答企業数	4,076	—	3,747	—
既に実施している	362	8.9%	296	7.9%
トラブルがあったので対策を講じた	2	—	1	—
実施を検討している	198	4.9%	225	6.0%
必要性を感じるが、未実施	1,573	38.6%	1,526	40.7%
必要性を感じず、未実施	1,943	47.7%	1,700	45.4%

セキュリティ向上への寄与

	平成 20 年度 [26]		平成 19 年度 [27]	
	回答数	割合	回答数	割合
回答企業数	439	—	379	—
寄与した	254	57.9%	238	62.8%
寄与しなかった	16	3.6%	8	2.1%
わからない	169	38.5%	133	35.1%

[24] セキュリティ対策ソフト

[25] ウイルス対策ソフト

[26] 平成 19 年度実施調査（平成 20 年度公表）

[27] 平成 18 年度実施調査（平成 19 年度公表）

c）情報セキュリティ対策の監視及びレビューに係る指標

・「定期的な情報セキュリティ監査の実施状況」

（情報処理実態調査：経済産業省）

外部専門家による定期的な情報セキュリティ監査

対策実施状況

	平成 20 年度[28]		平成 19 年度[29]	
	回答数	割合	回答数	割合
回答企業数	4,166	—	3,840	—
既に実施している	581	13.9%	490	12.8%
トラブルがあったので対策を講じた	7	0.2%	7	0.2%
実施を検討している	165	4.0%	183	4.8%
必要性を感じるが、未実施	1,807	43.4%	1,788	46.6%
必要性を感じず、未実施	1,613	38.7%	1,379	35.9%

セキュリティ向上への寄与

	平成 20 年度 [28]		平成 19 年度 [29]	
	回答数	割合	回答数	割合
回答企業数	591	—	513	—
寄与した	486	82.2%	419	81.7%
寄与しなかった	8	1.4%	8	1.6%
わからない	97	16.4%	86	16.8%

内部による定期的な情報セキュリティ監査

対策実施状況

	平成 20 年度 [28]		平成 19 年度 [29]	
	回答数	割合	回答数	割合
回答企業数	4,194	—	3,857	—
既に実施している	1,107	26.4%	866	22.5%
トラブルがあったので対策を講じた	8	0.2%	13	0.3%
実施を検討している	401	9.6%	415	10.8%
必要性を感じるが、未実施	1,863	44.4%	1,828	47.4%
必要性を感じず、未実施	823	19.6%	748	19.4%

セキュリティ向上への寄与

	平成 20 年度 [28]		平成 19 年度 [29]	
	回答数	割合	回答数	割合
回答企業数	1,197	—	1,021	—
寄与した	954	79.7%	827	81.0%
寄与しなかった	26	2.2%	13	1.3%
わからない	217	18.1%	181	17.7%

[28] 平成 19 年度実施調査（平成 20 年度公表）

[29] 平成 18 年度実施調査（平成 19 年度公表）

（イ）個人

① 個人の情報セキュリティ意識に係る指標

・「インターネットを利用して感じる不安や不満、利用しない理由」

（通信利用動向調査：総務省）

インターネット利用上の不安の有無

	平成 21 年末	平成 20 年末
回答数	4,230	4,070
特に不安は感じない	20.2%	19.5%
対策を行っているのでそれほど不安を感じない	31.5%	28.3%
対策を行っているが少し不安を感じる	28.7%	30.0%
不安を感じる	14.0%	17.5%
無回答	5.6%	4.8%

インターネット利用上で感じる不安の内容

	平成 21 年末	平成 20 年末
回答数	1,795	1,908
ウィルスの感染が心配である	70.6%	67.2%
個人情報の保護に不安がある	69.9%	71.2%
どこまでセキュリティ対策を行えばよいか不明	58.6%	61.7%
電子的決済手段の信頼性に不安がある	40.4%	40.4%
セキュリティ脅威が難解で具体的に理解できない	33.3%	33.7%
違法・有害情報が氾濫している	32.5%	35.5%
認証技術の信頼性に不安がある	15.4%	15.6%
知的財産の保護に不安がある	7.8%	7.9%
送信した電子メールが届くかどうかわからない	6.9%	9.2%
その他	2.1%	1.5%
無回答	0.2%	0.1%

インターネットを利用しない理由

	平成 21 年末			平成 20 年末		
	全世帯	利用世帯	非利用世帯	全世帯	利用世帯	非利用世帯
回答数	4,547	4,230	271	4,515	4,070	389
通信料金が高い	35.6%	37.0%	18.7%	34.5%	36.5%	16.7%
特に不満はない	27.4%	27.4%	29.2%	23.7%	25.8%	3.3%
パソコンなどの機器が高価すぎる	24.8%	25.5%	14.8%	24.5%	25.7%	13.2%
接続速度が遅い	23.2%	25.0%	0.3%	20.3%	22.3%	0.5%
パソコンなどの機器の操作が難しい	18.8%	18.2%	27.1%	18.1%	17.4%	28.0%
情報検索に手間がかかる	10.5%	11.2%	2.9%	10.5%	11.4%	1.6%
インターネットについてよく知らない	8.4%	6.3%	37.5%	8.3%	6.4%	29.7%
利用する必要がない	7.4%	4.1%	52.4%	8.3%	4.4%	50.7%
必要な情報がない	2.3%	2.1%	5.1%	1.9%	1.8%	3.0%
その他	3.8%	3.6%	5.4%	3.6%	3.7%	3.2%
無回答	10.4%	9.9%	11.3%	10.1%	9.2%	13.7%

・「インターネットにおける情報セキュリティの認知度」

（インターネットの利用実態に関する調査：総務省）

	平成 20 年	平成 19 年
回答者数	2,979	3,090
コンピュータウィルス感染	95.2%	95.5%
スパイウェア	73.0%	77.3%
ボット（ボットネット）	18.9%	23.5%
個人情報漏えい	81.4%	83.9%
フィッシング詐欺	77.8%	81.4%
不正アクセス	69.2%	73.2%
どれも知らない	2.2%	2.0%

・「情報セキュリティに関する攻撃・脅威に対する認知状況」

（情報セキュリティに関する脅威に対する意識調査：情報処理推進機構）

	平成 21 年度	平成 20 年度[30]
回答数	5,019	5,000
フィッシング詐欺	93.7%	92.7%
ワンクリック不正請求	94.4%	92.1%
スパムメール	―	88.0%
スパイウェア	88.3%	87.8%
セキュリティホール（脆弱性）	76.9%	76.5%
標的型攻撃	43.7%	42.9%
ボット	39.0%	35.3%
コンピュータ・ウイルス	―	―
マルウェア	36.6%	31.8%
セキュリティ対策ソフトの押し売り行為	―	―
偽セキュリティ対策ソフト	49.1%	―

② 個人の情報セキュリティ対策状況に係る指標

・「インターネットのウィルスや不正アクセスへの対応」

（通信利用動向調査：総務省）

	平成 21 年末	平成 20 年末
回答数	4,230	4,070
何らかの対策を実施	82.9%	80.2%
ウィルス対策ソフトの導入	52.2%	53.4%
知らない人からのメールや添付ファイル、HTML ファイルを不用意に開かない	36.5%	37.6%
プロバイダ等が提供するウィルス対策サービスの利用	25.4%	26.1%
ファイアウォールの使用	24.7%	26.1%
OS、ブラウザのアップデート	22.4%	23.7%
スパイウェア対策ソフトの導入	15.4%	16.0%
ファイル等のバックアップ	11.9%	13.8%
メールソフトのアップデートや変更	6.5%	8.3%
プロバイダ等が提供するファイアウォールサービスの利用	5.7%	6.4%
アカウントごとにパスワードを複数使い分け	4.5%	4.9%
パスワードの定期的な変更	4.1%	4.1
その他	6.1%	1.8%
何も行っていない	10.4%	13.7%
無回答	6.7%	6.1%

・「インターネットにおける無線 LAN 等のセキュリティ対策状況」

（インターネットの利用実態に関する調査：総務省）

	平成 20 年	平成 19 年
回答者数	1,224	1,459
MAC アドレスフィルタリングをしている	15.5%	14.5%
SSID（ステルスモード）隠蔽機能の使用	11.2%	11.2%
暗号化（WEP）	27.0%	23.1%
暗号化（WPA/PSK）	7.5%	7.5%
暗号化（WPA2（IEEE802.11i））	6.6%	5.9%
その他	0.9%	1.2%
方法はわからないが対策している（初期設定等）	19.0%	19.1%
対策をしていない	15.4%	19.2%
わからない	23.9%	25.8%

[30] 平成 20 年度 第 1 回調査

・「情報セキュリティ対策の実施状況」

（情報セキュリティに関する脅威に対する意識調査：情報処理推進機構）

	平成 21 年度	平成 20 年度 [30]
回答数	5,019	5,000
セキュリティ対策ソフト・サービスの利用	79.3%	76.3%
不審な電子メールの添付ファイルは開かない	77.7%	—
怪しいメール・添付ファイルの削除	—	—
怪しいと思われるウェブサイトにはアクセスしない	72.8%	—
Windows Update 等によるセキュリティパッチの更新	72.3%	76.7%
よく知らないウェブサイトではファイル（ソフトウェア）をダウンロードしない	69.5%	—
パソコンの重要なデータのバックアップ	47.3%	50.1%
不要になった自宅パソコンの破棄・リサイクル前のデータ消去	35.4%	37.8%
ルータの利用	31.8%	40.2%
必要時以外はネットにつながない	28.3%	—
有害なウェブサイトへのアクセスを防止するソフトまたはサービスの導入・活用	27.6%	41.4%
暗号化された USB メモリの利用や、重要なファイルの暗号化	18.7%	32.3%
電子メールの暗号化ソフト等の利用	—	—
ウェブサイトの安全性評価ツールの利用	17.7%	33.1%
パソコンのログインパスワードの設定	—	57.0%
パスワードの定期的な変更	—	—
特にない	4.9%	—

（ウ）企業・個人共通

① インシデント・犯罪の発生

・「情報セキュリティ上のトラブル（システムトラブル、不正アクセス、コンピュータウィルス、重要情報の漏えい等）の経験」（企業）

（情報処理実態調査：経済産業省）

情報セキュリティ上のトラブルの発生

	平成 20 年度[31]		平成 19 年度[32]	
	回答数	割合	回答数	割合
回答企業数	4,577	—	4,215	—
トラブルが発生した企業数	1,313	28.7%	1,044	24.8%
トラブルが発生しなかった企業数	3,264	71.3%	3,171	75.2%

発生したトラブル

	平成 20 年度[31]		平成 19 年度[32]	
	回答数	割合	回答数	割合
回答企業数	1,288	—	1,037	—
システムトラブル[33]	787	61.1%	563	54.3%
システムの停止[33]	707	54.9%	—	—
内部要因によるシステムの停止	632	49.1%	421	40.6%
外部要因（地震、火災等の問題）によるシステムの停止	162	12.6%	87	8.4%
その他のシステムトラブル[33]	150	11.6%	—	—
DoS 攻撃	45	3.5%	48	4.6%
スパムメールの中継利用等	108	8.4%	108	10.4%
ホームページやファイル、データの改ざん	8	0.6%	12	1.2%
不正アクセス[33]	84	6.5%	65	6.3%
IP・メールアドレス詐称	64	5.0%	47	4.5%
リソースの不正使用	6	0.5%	11	1.1%
内部関係者による不正アクセス	16	1.2%	13	1.3%
コンピュータウイルス[33]	719	55.8%	617	59.5%
ウィルスなどの感染	698	54.2%	593	57.2%
トロイの木馬	171	13.3%	122	11.8%
重要情報の漏えい[33]	359	27.9%	318	30.7%
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	31	2.4%	48	4.6%
不正アクセスによる情報漏えい	2	0.2%	4	0.4%
内部者による情報漏えい	24	1.9%	22	2.1%
委託先による情報漏えい	43	3.3%	36	3.5%
ノートパソコン及び携帯記憶媒体等の盗難・紛失	323	25.1%	263	25.4%
その他[33]	70	5.4%	60	5.8%
ホームページ上での誹謗中傷等	41	3.2%	40	3.9%
その他	30	2.3%	20	1.9%

[31] 平成 19 年度実施調査（平成 20 年度公表）

[32] 平成 18 年度実施調査（平成 19 年度公表）

[33] 「発生したトラブル」の各カテゴリーの計は、「発生したトラブル」について、各カテゴリーに属するいずれかのトラブルの種類を回答した企業数。ただし、「システムトラブル計」は、「発生したトラブル」について、「システムの停止」または「その他のシステムトラブル」に属するいずれかのトラブルの種類を回答した企業数。

・「インターネットを利用して受けた被害（ウィルス感染、スパムメールの中継利用・踏み台、不正アクセス、DoS 攻撃等）」（ウィルス感染、不正アクセス以外は企業のみ）

（通信利用動向調査：総務省）

	平成 21 年末	平成 20 年末
回答数	4,064	3,923
何らかの被害を受けた	61.7%	57.6%
ウィルスを発見又は感染	32.8%	31.1%
ウィルス発見したが感染なし	21.6%	22.7%
ウィルスに1度以上感染	11.4%	8.6%
迷惑メールを受信	50.8%	50.7%
迷惑メールを受信（架空請求を除く）	47.8%	48.3%
迷惑メールを受信（架空請求）	14.8%	15.7%
不正アクセス	1.4%	0.8%
スパイウェアなどによる個人情報の漏洩	1.4%	1.1%
ウェブ上（電子掲示板等）での誹謗中傷等	0.7%	1.2%
フィッシング	1.4%	1.5%
その他（著作権の侵害等）	0.3%	0.1%
特に被害はない	36.5%	39.4%
無回答	1.8%	3.1%

・「過去１年間の情報セキュリティに関する被害状況」（企業）

（不正アクセス行為対策等の実態調査：警察庁）

	平成 21 年	平成 20 年
回答数	930	775
ウイルス等の感染	31.9%	22.3%
ノート PC 盗難	6.2%	5.8%
スパイウェアの感染	4.3%	4.5%
内部者のネットワーク悪用（私用メール、ポルノ画像閲覧等）	3.0%	1.8%
その他情報機器盗難（外部記憶装置等）	1.4%	1.2%
ホームページの改ざん	1.4%	1.0%
情報漏洩（ファイル共有ソフトによるものを除く）	0.4%	0.9%
ファイル共有ソフトの利用に伴う情報漏洩	0.8%	0.9%
Web や掲示板上での貴社・団体に対する誹謗中傷	3.0%	0.9%
なりすまし	1.3%	0.8%
DoS 攻撃	2.4%	0.6%
メールの不正中継	0.9%	0.4%
踏み台（バックドア設置等）	1.0%	0.3%
システム破壊／データ改ざん	0.2%	0.1%
盗聴（キーロガー含む）	0.2%	0.1%
ネットワークを利用した詐欺	0.0%	0.1%
フィッシング	0.3%	0.1%
インターネット上の著作権侵害（記事、写真、ロゴ等の無断使用等）	0.6%	0.0%
その他	1.0%	0.3%
上記項目について被害はなかった	54.6%	71.1%

・「不正アクセス行為の発生状況」

（国家公安委員会、総務省、経済産業省）

	平成 21 年	平成 20 年
認知件数	2,795	2,289
海外からのアクセス	40	214
国内からのアクセス	2,673	1,993
アクセス元不明	82	82

・「コンピュータウィルス、不正アクセス、ソフトウェア製品・ウェブサイトの脆弱性に関する情報の届出状況」

（情報処理推進機構）

	平成 21 年	平成 20 年
コンピュータウイルス	16,392	21,591
不正アクセス	149	155
被害あり	96	120
被害なし	53	35
脆弱性関連情報	1,626	2,628
ソフトウェア製品	157	237
ウェブサイト	1,469	2,391

・「情報セキュリティに関する被害やトラブルの遭遇状況」（個人）

（情報セキュリティに関する脅威に対する意識調査：情報処理推進機構）

	平成 21 年度	平成 20 年度[34]
回答数	5,019	5,000
全く知らない差出人から大量のメールが送られてきた	24.2%	32.0%
コンピュータウイルスに感染した（感染後にセキュリティ対策ソフトが検出したケースを含む）	14.9%	20.1%
身に覚えのない料金の支払いを要求するメールが送られてきた	6.2%	9.1%
ホームページ閲覧中に、契約した覚えのない料金の支払いを要求するメッセージが表示された	5.1%	10.1%
他者による個人情報流出の被害にあったことがある	3.6%	3.8%
メールに記載された URL をクリックしたら、個人情報の入力を求めるウェブページが表示された	2.9%	5.6%
自分のパソコンのシステムやファイルが書き換えられたり、削除された	1.5%	1.9%
知らない間に、クレジットカードが利用されていた	0.9%	―
ネットオークションにおいて、勝手に本人になりすまされ、架空の商品を出品されたり、お金を振り込んだのに商品が届かなかったことがある	0.7%	0.9%
知らない間に、自分のパソコンから他者へのメールを送信していた	0.6%	1.4%
オンラインゲームにおいて、ゲーム通貨を不正に搾取されたり、アイテムを騙し取られたことがある	0.5%	0.7%
偽のセキュリティ対策ソフトをインストールしてしまったことがある	0.5%	―
自分のパソコンから個人情報を流出させてしまったことがある	0.4%	0.8%
知らない間に、銀行口座からお金が引き出された	0.4%	0.6%
その他	0.4%	1.0%
被害にあったことはない	44.2%	32.7%
被害にあったかどうかわからない	16.3%	16.3%

・「コンピュータウィルス遭遇経験」（企業）

（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）

	平成 20 年			平成 19 年		
	総数	企業	自治体	総数	企業	自治体
回答数	2,317	1,907	410	2,280	1,859	421
ウイルスには感染も発見もしなかった	38.8%	40.8%	29.5%	41.6%	43.9%	31.1%
ウイルスを発見したが、感染には至らなかった	44.6%	42.2%	56.1%	45.4%	42.7%	57.5%
ウイルスに感染した	15.8%	16.3%	13.9%	12.4%	12.7%	10.9%
無回答	0.7%	0.8%	0.5%	0.6%	0.6%	0.5%

[34] 平成 20 年度 第 1 回調査

② （参考指標）IT 投資状況及び IT を活用した経済の発展状況

・「企業間（BtoB）電子商取引の現状（国内市場規模、電子商取引化率）」

（電子商取引に関する市場調査：経済産業省）

	平成 20 年		平成 19 年	
	EC 市場規模（億円）	EC 化率	EC 市場規模（億円）	EC 化率
広義 EC[35]	2,495,890	21.2%	2,533,970	20.8%
狭義 EC[36]	1,588,600	13.5%	1,616,510	13.3%

・「消費者向け（BtoC）電子商取引の現状（国内市場規模、電子商取引化率）」

（電子商取引に関する市場調査：経済産業省）

平成 20 年		平成 19 年	
EC 市場規模（億円）	EC 化率	EC 市場規模（億円）	EC 化率
60,890	1.8%	53,440	1.5%

35 「コンピューター・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。

36 「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。