資料２－２

２００７年度の情報セキュリティ政策の評価等

－「真の情報セキュリティ先進国」を目指す取組みの２年目の評価－

内閣官房情報セキュリティセンター（ＮＩＳＣ）

２００８年４月２２日

目次

第3章　重要インフラにおける現状の評価等

第4章　企業･個人における現状の評価等

はじめに

1. 本文書の位置づけと基本認識

本文書は、2006年度から始まった3年間を対象期間とする「第１次情報セキュリティ基本計画（以下「基本計画」という。）[1]」と、それに基づく2007年度計画である「セキュア・ジャパン2007（以下「SJ2007」という。）[2]」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、2007年度の政策の評価等[3]を行った結果を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、上述の基本計画及び年度計画に基づく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「情報セキュリティ政策の枠組み文書」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（National Information Security Center）（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。

本文書は、我が国情報セキュリティ政策のＰＤＣＡサイクルの運用において、2007年度施策の点検段階（C）に該当するものであり、情報セキュリティ政策会議は、本文書の報告を受けた後に、我が国の情報セキュリティに関する現状認識を明確にするとともに、翌年度の年度計画である「セキュア・ジャパン2008（以下「SJ2008」という。）」を策定することになる。また、現在、次期基本計画策定に向けて、検討委員会において議論を進めているところであるが、本文書は次期基本計画策定の前提となる現状認識として適宜活用されることともなる。

したがって、本報告書の主眼は、2007年度の情報セキュリティ政策が社会に与えた変化や情報セキュリティに関連のある事象などを全て網羅的に把握することにあるのではなく、上記のようなSJ2008や次期基本計画との関係性を踏まえ、翌年度の政策を検討するための現状認識に有益な情報を、より多く含むものとすることにある。

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、全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「2007年度

---

[1] ２００６年２月２日情報セキュリティ政策会議決定

[2] ２００７年６月１４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（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・了解文書（「「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」［政策会議決定］及び「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～「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サイクル確立へ～」［政策会議了解］）

[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分野が含まれる。

の取組み」、第2節では「2007年度の取組み及び取組みを受けた現状の評価等（2007年度の評価等）」、第3節では、評価等から抽出される「2008年度に向けた課題」について述べる。そして、第2節の2007年度の評価等においては、評価等の視点をはじめとする基本的考え方を述べた上で評価指標などを提示し、さらに、具体的な評価等を「施策の取組み結果」、「施策の取組みによる社会的変化」及び「補完調査の結果」に関して加えた上で、総評を行う。

なお、第1章の情報セキュリティ政策全体の評価等は、上記の情報セキュリティ政策の枠組み文書において述べられているように、「様々な主体ごとの取組み結果の」「積み上げによってわが国総体として」「総合的かつ分析的に」行う。したがって、第1章の政策全体の評価等は、第2章以降の各章における政策領域ごとの評価等の総評を活用しながら行うこととなる。情報セキュリティ政策全体に関する具体的な分析の枠組みと手法については、以下に述べる。

3. 情報セキュリティ政策全体の評価等に係る検討の枠組みと手法

情報セキュリティ政策全体の評価等は、定性的な検討部分と、定量的なデータを適宜組み合わせる形で行う。具体的には、象徴的な事象等がある場合、これに着目してそれらが示唆するものを抽出し、適宜これに即したデータを組み合わせて評価等を行う。

検討の手順は、上述のように各政策領域[7]の評価等からはじめ、これらを積み上げた上で政策全体としての評価等を進める。したがって、まず基本計画及びSJ2007で設定されている政策領域について、各々の領域全体としての評価等を行う。ただし、各々の政策領域の評価等は、第2章以下の各論の中で領域ごとの評価等及び総評においてまとめられることから、これらを活用する。

こうした政策領域をまず念頭に置き、これに組み合わせて各々の政策領域に係る社会の状況などについても検討するために、社会情勢、政府の取組み実績（施策の取組み評価等）を意識する。そして、前者を横軸として捉え、後者を縦軸に捉えて全体を見た上で、縦軸の領域についても個々の領域全体として評価等を行う(図 1)。

社会情勢は、非常に広範な要素を含むことから、検討に当たって、

1）社会環境などに作用を行う主体として「人的要素（人、意識、体制・制度）」
2）社会環境などに作用を行う際の媒介物や、作用を行った結果生み出されるものとして「物的要素（投資、技術、ハード、ソフト、ネットワーク）」
3）実際に作用を受ける社会環境などとして「周辺情勢（インシデント・事件、市場など）」

に分類を行い、また、可能な限り数値やデータを加味し、幅広い視点から各々について評価等を行うこととする。その上で、それらを積み上げる形で情報セキュリティ政策全体について評価等

[7] ここで各々の政策領域とは、「対策実施４領域」である政府機関・地方公共団体、重要インフラ、企業、及び個人、そして「横断的な情報セキュリティ基盤」である情報セキュリティ技術戦略の推進、情報セキュリティ人材の育成・確保、国際連携・協調の推進、犯罪の取締り及び権利利益の保護・救済のことである。

を行うこととする。

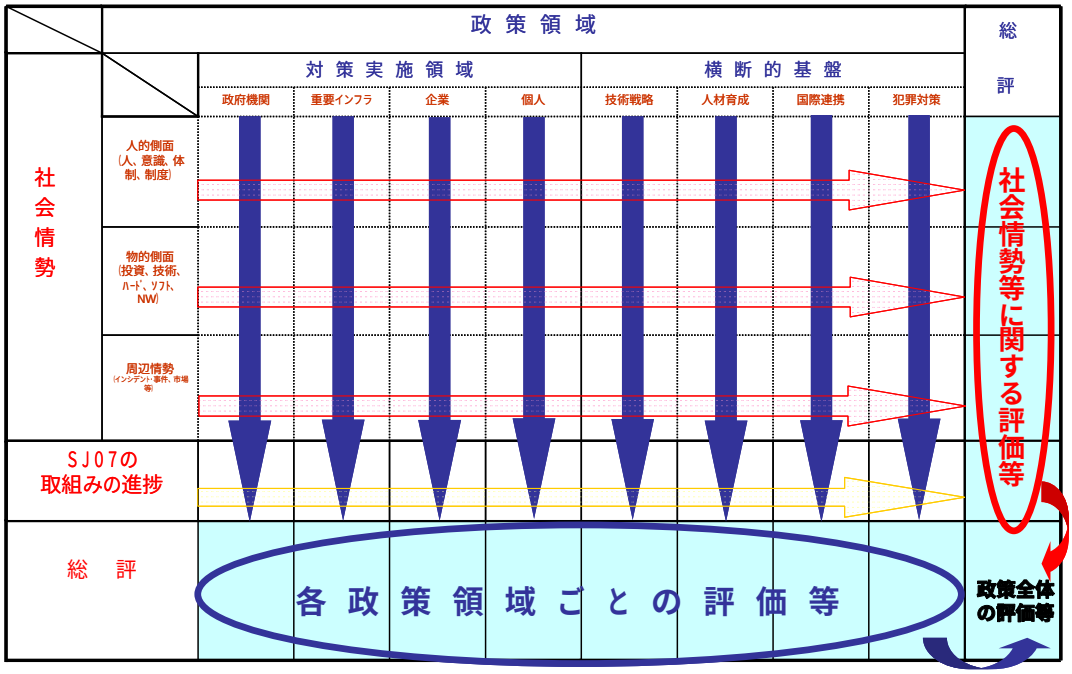


図1：2007年度の情報セキュリティ政策の評価等に係る検討の枠組み

第1章　情報セキュリティ政策全体の評価等

第1節　我が国における情報セキュリティに関する2007年度の取組み

1．2007年度の取組みの背景

我が国の国民生活及び社会経済活動においてITへの依存度が高まる中、ITの利活用における安心・安全を確保するため、情報セキュリティは重要な課題となっている。このような状況を踏まえ、2006年度から2008年度の3年間を対象期間とする基本計画の下、2006年度にはセキュア・ジャパン2006（以下「SJ2006」という。）が策定され、初年度の取組みが行われた。結果、2006年度末には、

1）各主体における情報セキュリティの意識の萌芽
2）対策実施主体ごとの具体的な取組みの着手
3）情報セキュリティ推進体制と持続的改善構造の構築

という「取組みの第一段階」が進んだ状況であった。

これを踏まえ、2007年度当初には、次の段階として、構築が進んだ官民の情報セキュリティ対策を推進する体制の維持と、対策が不十分な部分の底上げを含めて対策推進の安定化を実現することが課題となった。そのため、2007年度は各対策実施主体の意識の維持・向上とともに、PDCAサイクル（「持続的改善構造」）に基づいて実施される施策について、底上げの視点を持ちながら着実に進めることとされた。情報セキュリティに関する2007年度の取組みは、こうした方向性の下でなされたものである。

2．2007年度の取組み

2007年度は、基本計画の下での2年目の取組みとして、2006年度の取組み及び評価を踏まえつつ、年度計画であるSJ2007を6月に策定し、情報セキュリティ対策の政府の重点施策を定めた。

SJ2007では、「官民における情報セキュリティ対策の底上げ」を目標に、（1）官民各主体の共通認識の形成は概ねできたことから、共通認識の維持・向上を図り、（2）情報セキュリティ技術戦略委員会での検討も踏まえつつ、引き続き先進的技術の追求を図り、（3）人権保障や、公的部門の活動の透明性や適法性の確保とバランスを維持しつつ、公的部門の戦略的な対応能力強化を図り、（4）国内における官民の各主体間や、国際的な主体間での連携・協調の推進を図ることが重点として設定され、対策実施主体が施策の取組みを進めた。

具体的には、2006年度に引き続き、「対策実施4領域」、「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）」という基本計画の柱立てに基づいて具体的な施策を実施することとし、内閣官房を含む各府省庁が計159の取組みを行うこととなった。

また、SJ2007では、「情報セキュリティ基盤の強化に向けた集中的な取組み」という2008

年度の重点施策の方向性が設定され、「情報セキュリティ人材の育成・確保に向けた集中的な取組み」、「情報セキュリティ政策の国際展開に向けた集中的な取組み」、「電子政府等の情報セキュリティ強化のための総合的な取組み」として、計24の具体的施策が盛り込まれた。

2007年度は、このようにSJ2007に沿った形で、基本計画の下での2年目の取組みがなされた状況である。

第2節 2007年度の取組み及び取組みを受けた我が国の現状の評価等（2007年度の評価等）

1．2007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2007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、

1）基本計画に基づく政策体系の下での2年目の取組みが実効的に進められ、結果、SJ2007に記載された当初の目標（とりわけ、2007年度の重点である「官民における情報セキュリティ対策の底上げ」）が実現できたか否かを測るという視点
2）2007年度の取組み開始時のリスクが、1年間の取組みによってどう変化したのかなど、情報セキュリティに係る2007年度の様々な動向を測る視点
3）2008年度の重点である「情報セキュリティ基盤の強化に向けた集中的な取組み」の実施において、対応が必要な具体的課題を浮き彫りにするという視点

である。

2．評価等について（評価指標等）

（1）2007年度の評価等について

情報セキュリティ政策全体の評価等は、情報セキュリティ政策の枠組み文書第5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が、特定の評価指標は2007年度では設けていない。

なお、このような評価等の手順については、「はじめに」において述べた検討の枠組み及び手順に基づくこととする。

（2）2008年度以降の評価等について

2008年度以降の評価等において活用する評価指標や評価等の方法は、基本的に2007年度の評価等を踏襲する。しかし、2007年度は情報セキュリティ政策の枠組み文書に盛り込まれた「補完調査」の初年度であったため、2008年度には、例えば前年度からの経年比較も含め、補完調査をより充実させることも考えられる。また、2008年

度の政策を進める過程において、評価指標や評価等のアプローチについて改善を行うことも考えられ、こうした点についても2008年度以降の評価等において反映を行う。

(3) その他

評価等に当たっては、以上に加えて、政府全体の情報セキュリティ予算額なども適宜加味して検討を行うこととする。

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

SJ2007において、2007年度中に推進するとされた159の具体的施策の取組み結果については、2007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 ：１４４施策(９０．６%、内Ａ’は５施策)
B+：　１施策(０．６%)
Ｂ ：　１２施策(７．５%)
Ｃ ：　１施策(０．６%)
－ ：　１施策(０．６%)

＜分類＞

A：当初の予定どおり施策を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、継続して施策を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：予定どおり施策を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、最終的には施策を推進することが出来る施策。

C：予定どおり施策を推進することはできず、今後の見通しも立たない施策。

－：予定どおり施策を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。

SJ2007において、2007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9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1割(15施策)の予定どおり推進できなかった施策については、情報資産台帳の整備や「go.jp」ドメインへの移行など全府省庁が実施しなければならない施策であったものの一部府省庁で実施が完了しなかったものが7施策、刑事共助条約の締結等施策を推進したものの2007年度中に完了できなかったものが6施策、刑法の改正等政府機関の事情以外の理由により推進できなかったものが1施策、他の施策の成果にかんがみ、実施は不要と判断した施策が1施策であった。

Aとされた144の施策は、関係各府省庁の担当者の努力により予定通り推進することができたものの、A'の5施策については、「各政府機関でのPDCAサイクルの定着」、「政府全体でのPDCAサイクルの定着」、「対策実施状況に関する評価等」、「情報セキュリティマネジメントに関する評価等」、「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」と、政府機関の対策実施に係る取組みとなっている。このことから、政府機関の対策推進のための努力は懸命に続けられているものの、体制や人員の不足が課題であることがうかがえる。

また、Aとされる施策においても引き続き取組みが求められるものもあり、このような施策も含め、特にA以外であった施策については、基本計画の最終年度である2008年度において、継続的かつ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.(1)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。

(a) 人的側面(人材、意識、体制・制度)

(ア) 人材面

人材面に関しては、政府においては、2006年度に情報セキュリティ政策会議の下に設置された「人材育成・資格制度体系化専門委員会」の報告を受けて幅広い取組みが行われ、教育拠点や教育ツールの整備が図られるなど、情報セキュリティにかかる人材の育成に資する体制・基盤の整備に着手した。

また、民間の教育事業者団体においても、積極的な情報発信やキャリアパスの構築に向けた検討など、各団体の枠組みを超えた業界横断的な取組みを推進する連携体制が整備された。

これらにかんがみると、2007年度は、官民の積極的な取組みの展開を通じて人材育成のための体制・基盤の整備が図られ、社会全体としての人材の育成に関する意識が浸透し始めたものと考えられる。

しかしながら、こうした人材育成のための体制・基盤が磐石のものとなって、自律的に人材育成が進む状態に至っているとは必ずしも言えない。具体的な人材育成の手法についても手探り状態が続いている。様々な教育機会を活用して、社会のニーズに応えるべく十分な人材育成・確保を図るには、なお時間を要すると考えられ、取組みは発展の途上にあると言える。

(イ) 意識面

2006年度には、情報セキュリティ対策の必要性に関して「意識の発露」がみられたところ、2007年度は、SJ2007に基づく各種の取組みの推進やマスコミ報道(重要情報の漏えいや基盤となるITシステムの障害の報道等)、不正アクセス行為やネットワーク利用犯罪の増加傾向などもあり、各々の対策実施領域において情報セキ

ュリティに関する脅威の認識、対策の必要性に係る意識が向上している状況にある。きっかけは様々であるものの、情報セキュリティに係る意識は徐々に高まっているものと考えられる。

政府機関では、特に担当部局ではセキュリティ対策推進の意識は十分にあるものの、予算との関係など様々な制約の中で、具体的にどのように取り組んでいくことが効率的･効果的であるかが必ずしも明確ではないために、取組みあぐねるという側面もあると考えられる。また、一部では「やらされ感」もあるとみられることから、効率的･効果的な対策の方法や対策実施のメリットについて意識共有していくことも必要である。

重要インフラ分野では、官民が連携して取組みの枠組みや体制を構築しつつあることを通じ、対策の重要性に係る意識も徐々に高まってきていると言える。今後、事業者の自主性を十分に尊重しながら取組みが進むよう、メリットを明らかにしつつ、さらに努力を継続することが必要であると考えられる。

企業分野では、情報漏えいやシステム障害などの発生が、信用の失墜、賠償問題、対策への再投資などを通じて、経済的損失に繋がり得るという点が意識の向上に大きな影響を及ぼしているものと考えられる。また、2007年度は金融商品取引法（日本版ＳＯＸ法）が施行され、企業の内部統制の一環として情報セキュリティを含めたＩＴ統制の重要性に対する意識が更に高まってきたことも要因として挙げられる。

しかしながら、「情報セキュリティ対策への取組みの効果が認識しづらい」とする意識がみられることも指摘されている。また、対策を推進したとしても情報流出等の発生を完璧に防止することは容易でない一方で、最低限これだけは取り組めば良いという事項が見えないことからセキュリティへの過剰投資が生じ、一部では「対策疲れ」の声も聞こえる状況となっている。さらに、対策実施状況に差があることなどから、先進的企業と、規模が小さい企業の間において、意識格差が出てきているのではないかとの懸念もある。継続的に意識の維持･向上を図るため、企業が対策にメリットを感じられるような取組み（情報セキュリティ対策が市場評価に繋がる環境の整備）や費用対効果を意識した情報セキュリティ対策が引き続き求められると言えよう。

個人は、他の対策実施領域に比べ、他の主体による支援が更に重要であることから、ＳＪ2007の下で情報セキュリティに関する普及啓発･情報発信を行うことを重点に各種取組みが積極的に推進された。結果、総体としては情報セキュリティの意識が徐々に向上していることが各指標から見てとれる。

しかしながら、インターネット空間に不安を感じる割合が45．4％（インターネット上の安全確保に関する世論調査（平成19年11月内閣府調査）になるなど、不安感を

持つことが意識の向上を牽引している面もあると考えられるが、一方で、ボット[8]などの新たなリスクに関する認識が希薄な面もあり、今後の継続的な意識の向上には懸念があると言える。

また、対策の必要性の認識、対策実施状況などには、世代、性別といった属性による格差がみられる。

こうしたことから、個人分野では、脅威などの新たな変化を踏まえて対策の実効性を再検討しつつ、普及啓発・情報発信の取組みが引き続き求められる。とりわけ、年代別・男女別の格差の解消は大きな課題である。

(ウ) 体制面

体制面については、具体的な取組み推進のための枠組み構築が徐々に進められた一年であった。

政府機関については、NISCが中心となって総合調整を行いながら政府全体が協力して情報セキュリティ対策を推進する体制が整いつつあると言える。しかし、政府機関の対策実施に係る対応体制については、対策推進のための努力はそれとして懸命に続けられているものの、組織全体を担当する人数が数名程度であったり、専門性が問われる業務であるにもかかわらず、人事異動サイクルが2～3年であるために担当の専門的能力が十分に伸ばしきれなかったり、また、組織によっては情報セキュリティ対策に係る意思決定が当該組織のトップクラスの指示でなされる体制に必ずしもなっていないといった課題が存する。したがって、依然として人材・体制が不十分な状況にあり、政府機関の対策実施に係る体制は、現行体制で対応可能な限界点にまで到達しつつあるとも考えられる。今後は体制強化に向けた更なる取組みが必要である。

重要インフラについては、10分野すべてにおける CEPTOAR の整備が完了し、「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）の創設に向けた検討方針の取りまとめが進められた。また、官民連携による分野横断演習も2006年度に続いて第2回目が実施され、実際の対応により近い「機能演習」という形で行われた。事業継続性の確保を軸に置いて官民の各主体間での情報共有、連絡・連携を進めるための枠組み・体制は徐々に構築されつつあると言える。

企業では、ISMS取得事業者数が継続的に増加するなど、組織的な対応を含む対策、体制の強化への取組みが徐々に進められていると言える。

(ｂ) 物的側面（投資、技術、ハード、ソフト、ネットワーク）

物的側面については、昨年度から大幅な変化はないものの、必要なものについては

[8] コンピュータウィルスの一種で、コンピュータに感染し、そのコンピュータをネットワーク（インターネット）を通じて、外部から操ることを目的として作成されたプログラム

堅実に投資を行い、対策を着実に行おうとしている状況にあると言える。

政府機関においては、政府機関に対するサイバー攻撃等に関する横断的な情報収集・分析・情報共有を行うための体制（ＧＳＯＣ：Government Security Operation Coordination Team）の整備を開始するなど、緊急対処能力の強化に向けた取組みが行われた。また、政府機関の情報セキュリティ対策のための統一基準(以下「政府機関統一基準」という。)遵守にかかわるシステム構築予算も前年度と同規模で確保され、システム対策が着実に進められた状況にある。

企業においては、２００６年度までのウイルス対策ソフトまたは統合セキュリティ対策ソフトの導入状況には著しい変化はみられないことから、情報セキュリティの技術的対策への投資は、経済的損失との比較衡量の下で、各主体の経営判断によってなされる傾向にあると推察される。こうした状況にかんがみると、現行の対策枠組みの下での取組み推進の「均衡点」に到達しつつあるとも考えられる。また、例えばボットへの対策など、技術的にも現行技術水準で守ることのできるセキュリティの「限界点」に到達している可能性もある。

今後、更に取組みを推進するには、対策継続に向けたメリットの明確化や最低限満たすべき水準の明確化、事業継続性の観点からの取組み推進などが有効であると考えられる。

個人分野では、最近の状況をみると、例えばＯＳの定期的なアップデート、ウイルス対策ソフトの導入・活用については、徐々に伸びてきており、全体としての底上げは進みつつあると考えられる。しかしながら、年代別・男女別の格差もみられ、必要な対策ソフトの入手をはじめとして、更なる対策実施状況の向上が望まれる。

研究開発・技術開発では、情報セキュリティ政策会議の下に設置された「技術戦略委員会」の報告等を受けて、政府全体として情報セキュリティ分野への技術・研究開発を推進する枠組み作りも進展しつつある。また、情報セキュリティ対策を進めるためのヴァーチャルマシン開発や、ボットを使ったサイバー攻撃等の課題を解決するための技術開発が進められるなど、情報セキュリティに係る課題の解決を目標とする課題解決型の技術開発も数多く行われている状況にあり、様々な取組みが着実に進められている状況にあると言えよう。こうした取組みの成果によって、セキュリティを確保する技術の限界水準が現在と比べて向上し、対策が大幅に進むことが期待されるところである。

（ｃ）周辺情勢（インシデント・事件、市場等）

周辺情勢に関しては、コンピュータウイルスやファイル共有ソフトに起因する情報の流出が依然として続き、不正アクセスやインターネット利用犯罪も年々増加傾向にある。さらに、ＩＴが国民生活、社会経済に基盤として組み込まれてきている中で、内部要因に起因したシステム障害が大きな混乱を招くような事態も引き続き発生している。

また、リスクの変化という観点からみると、政府機関や企業においては、従来のホームページの改ざんやウェブサーバへのＤｏＳ攻撃[9]といったものに加え、マルウェア[10]を添付したメールを特定の組織、企業へ送付して重要情報を盗み出すものや、攻撃を予告して企業を恐喝するものなども発生している。そして、その目的は愉快犯的なものから経済的利得を狙うものへと変化してきている。さらに個人においては、感染の検出が難しく被害が認識しづらい「ボット」の感染が依然として継続している。

これらを踏まえると、各主体が努力を行っている一方、攻撃の手法・目的が次々と変化し、被害も顕在化しにくくなっており、情報セキュリティに関するリスクは必ずしも軽減していない。

(3) 総評

ここでは、情報システムの社会基盤化が進んできたことを前提に、情報セキュリティが情報システムに対して及ぼす影響などについて網羅性を持って分析・検討するアプローチをとるよりも、むしろ、情報セキュリティ政策を検討していくに当たって有益な情報セキュリティに関する特徴的な事象などを述べ、詳細については各論において言及することとする。

２００７年度においては、ＳＪ２００７に盛り込まれた取組みについて概ね予定通り進められ、1) 官民における情報セキュリティ対策の推進のための体制の維持や、2) 対策推進の安定化に向けて最大限の努力がなされた。

各対策実施領域の取組み状況に関しては、一定の進展があったことが各種指標から明らかであり、対策推進の安定化に際しての重点としてきた「官民における情報セキュリティ対策の底上げ」も進んだものと考えられる。中でも、政府機関対策に関しては、各府省庁の担当者がＰＤＣＡサイクルに基づいた取組みを懸命に進めたことが効果を現し、依然取組みを強化することが必要な水準であるとは考えられるものの、短期間で一定の状況改善を実現できたと言えよう。

また、基本計画に掲げられ、ＳＪ２００７で目標が定められている「4つの基本方針」との関係では、1) 例えば政府機関や重要インフラ等の対策実施主体の意識の向上や、横断的情報セキュリティ基盤の人材育成に係る意識の浸透など、情報セキュリティに係る官民各主体の共通認識が強化されてきている。

また、2) 技術面に関しては、政府全体として情報セキュリティ分野への重点投資を進める環境の整備や課題解決型の技術開発が進められており、先進的技術の追求が続けられている状況にある。今後はこうした取組みによって、技術的な限界水準を向上させていくことが必要である。

---

[9] ネットワーク（インターネット）を通じ、サーバやネットワーク機器へ不正なデータやパケットを大量に送りつけ、サービス停止や機能の低下を発生させる攻撃

[10] コンピュータウィルス、ワーム、トロイの木馬、ボット等のコンピュータに感染し、不正な動作を行うプログラムの総称

3）公的部門の対応能力強化については、政府機関に対するサイバー攻撃、政府機関における情報システムの障害などの発生を防止するとともに、迅速かつ的確に対応するための体制の確立が進められたことが大きいと言えよう。

さらに、4）連携・協調の推進については、国際面については国際協調・貢献に関する基本方針が策定されたことを受けて、本格的な活動が開始された。他方、国内の官民の各主体間での連携・協調については、NISCが結節点となってはいるものの、各主体間で横断的なコミュニケーションが行われるまでには至っておらず、今後の課題であると言える。

以上を踏まえると、2007年度の一年間の取組みを通じて得られた成果は、1）各主体における情報セキュリティの意識の維持・強化、2）対策実施領域ごとの具体的取組みの着実な推進、3）横断的な情報セキュリティ基盤分野における具体的取組みの着実な推進、4）情報セキュリティ推進体制の維持・強化と持続的改善構造に基づく政策運営の推進であったと言える。

他方、政府機関や企業分野においてみられたように、現行の対策推進体制や現行対策枠組みでの限界点に来ているのではないかと考えられる点や、技術面でみられたように現行技術水準の限界点に来ているのではないかと考えられる点が存在する。

また、2006年度の情報セキュリティ政策の評価等（以下「2006度評価等」という。）において述べられたように、人材の育成・確保のように中長期で継続的に取り組むべき方策、国際連携・協調のように本格的な取組みに着手したばかりで加速化が必要な方策、さらに電子政府の情報セキュリティ強化のように時宜に合った喫緊の課題として取組みを迅速かつ集中的に行うことが必要な方策も存在する。

さらに、依然として情報セキュリティ問題は発生し、新たなセキュリティ問題も発生している中、大幅なリスクの軽減がみられていないことから、情報セキュリティ政策の社会的効果（アウトカム）については十分な判断がつかない状況である。このため、社会的効果が現れるように取組みを進めることも必要であると考えられる。

基本計画に基づく3か年の取組みを経て、我が国が真の情報セキュリティ先進国となるよう、最終年度である2008年度における積極的かつ集中的な取組みが期待されるところである。

第3節　2008年度に向けた課題

以上より、2008年度においては、第一に現行の対策推進体制や対策枠組み、技術水準で限界点に到達しているのではないかと考えられる諸点について、ブレークスルーをもたらす方法について検討を行うこと、第二に中長期で取り組むべき人材育成・確保の方策や、国際連携・協調のように加速化が必要な方策、電子政府の情報セキュリティ強化のように取組みを迅速かつ集中的に行うことが必要な方策に関して力強く対応を進めること、第三に情報セキュリティ政策の社会的効果（アウトカム）が現れるように取組みを進めること、が大きな課題である。

第一の課題については、現状把握を更に緻密に行いつつ、2008年度に実施する対策で対応できるものは実施するとともに、長期的な視野に立った抜本的な対策を検討する必要があると考えられる。現在、2009年度以降を視野に入れた次期基本計画策定に向けて検討委員会が様々な議論を深めているところである。このように長期的な視野に立った対策は、次期基本計画の下においても本格的に進められるよう検討を行う必要がある。

第二の課題に係る分野は、主として情報セキュリティ対策を推進するに当たって、強固であることが不可欠な基盤である。対策実施主体による対策の推進と強固な基盤があいまって、我が国が真の情報セキュリティ先進国となると言えよう。2006年度、2007年度は重点目標を主として対策実施領域に設定して取組みを進めてきたことから、2008年度は、これに加えて、情報セキュリティ基盤の強化に向けて集中的に取組みを行うことが必要である。

第三の課題については、そもそも政策の社会的効果（アウトカム）が現れるには、対策の実施からのタイムラグを考慮する必要がある。これまでに述べてきたように、情報セキュリティ政策のアウトプット（取組みの進展）は着実に出ていることから、政策の実現可能性や方向性に問題があるような場合は、これを修正しつつ、引き続き取組みを積極的に継続することが必要である。この観点から、引き続き持続的改善構造にのっとって、対策の底上げを行うべきである。

また、2007年度までの取組みにおいては、例えば、政府機関の横断的監視・即応体制整備や、重要インフラ分野の CEPTOAR－Council 創設に向けた検討、企業分野におけるJ－SOX法対応のためのガイドライン整備、人材分野における官民連携の協議会創設に向けた取組み、国際会議における様々な提案など、ツール・体制といった取組み基盤の整備、すなわち社会的効果（アウトカム）を出すための下地作りが相対的に多かったと言える。今後は、こうした取組み基盤を活用して、その果実たるアウトカムの発現に向けた取組みを進めることも必要であると考えられる。

第2章　政府機関における現状の評価等

第1節　政府機関における情報セキュリティに関する2007年度の取組み

1．2007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サイクルが推進されることが基本となっている。

2006年度の評価等では、2007年度に向けた課題として、2006年度に立ち上がった政府機関のPDCAサイクルが、より自律的かつ継続的なものとして定着することが必要である旨、そのためには、全職員に対する情報セキュリティ教育の徹底等により、セキュリティ意識の向上を図り、省庁基準及び実施手順等の遵守を徹底するとともに、自己点検及び監査について、実施体制の向上を図り、適切な対策実施状況の把握を行うことが不可欠である旨が指摘されている。

2007年度は、これを踏まえ、SJ2007において、政府機関統一基準の見直しの実施、PDCAサイクルの定着、政府機関における安全な暗号利用の促進等を図る施策に取り組んだ。

第2節　2007年度の取組みを受けた政府機関における現状の評価等（2007年度の評価等）

1．2007年度の評価等、及び評価等に関する基本的考え方（評価等の視点）

政府機関対策に関する情報セキュリティ対策の評価等は、各府省庁個別及び政府全体という政府機関の情報セキュリティ対策に係る2つのPDCAサイクルが着実に定着しているか確認を行うという視点に基づいて実施した。具体的には、2007年度の対策実施状況報告、特定の重要項目に係る重点検査及び情報セキュリティマネジメント評価の結果も踏まえて、総合的に評価を行った。

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

[対策実施状況に関する評価等]

（対策実施状況報告に基づく評価等）

政府機関における情報セキュリティ対策の実施状況を把握・分析するため、各府省庁の情報セキュリティ対策の実施状況について、2006年度に実施した評価手法を基本とし、効率化を図りつつ対象を拡大した2007年度の各府省庁の対策実施状況報告を基に、各府省庁の対策実施状況について評価等を行った。とりまとめ結果を別添3に示す。

2007年度は、政府機関統一基準導入の2年目ということもあり、一定の成果がみられるが、なお不十分な点があり、基本計画の最終年度に向けて、取り組むべき課題が依然として残っている。

政府全体として、対策実施が進んでいない遵守事項としては、例えば、

（情報セキュリティ対策の教育）

① 毎年度1回以上実施すべき教育の計画策定や着任・異動後3ヶ月以内に実施すべき教育の計画策定が不十分。計画がなされていても受講状況の把握や未受講者への受講指導の徹底が不十分。

② 職員による教育受講が不十分。

（格付け・取扱い制限に係る措置）

③ 情報の作成と入手時において、情報の格付けの実施や格付けの明示等の実施が不十分。

④ 情報の移送、情報の提供時において、管理者に対して行うべき許可申請、届出が不十分。

（情報システム台帳の整備）

⑤ 情報システムが扱う情報や当該情報の格付けを含む事項を記載した情報システム台帳の整備が不十分。

等があげられ、他方、対策実施が進んだ遵守事項としては、例えば、

（安全区域内における職員識別の徹底）

⑥ 安全区域内における職員識別の徹底については、昨年度は課題とされたが、昨年に比べ、安全区域内の職員識別の徹底について改善がみられる。

等が挙げられ、一定の成果がみられる。

（重点検査に基づく評価等）

政府機関統一基準において必須として実施すべき事項とされている基本遵守事項の中でも特に重要な事項として、前年度に引き続き端末・ウェブサーバについて検査するとともに、外部等と電子メールを送受信するための電子メールサーバについても検査を行った。

端末とウェブサーバに関する情報セキュリティ対策状況（2007年3月末時点）については2007年8月、電子メールサーバに関する情報セキュリティ対策状況（2007年9月末時点）については2007年12月の情報セキュリティ政策会議に結果を報告するとともに、NISCのホームページにおいて公表した。とりまとめ結果を別添4に示す。

＝分析＝

端末及びウェブサーバについて、実施すべき対策が全て実施されている（実施率100%）府省庁はそれぞれ8及び9府省庁となっており、昨年と比較して大きく改善がみられ、各府省庁における対策が着実に向上していると認められたが、まだ半数の省庁では完全な状態ではなく、対策が全て完了するのは2008年度となっている。

電子メールサーバについては、実施率100%の府省庁が10府省庁となっており、端末及びウェブサーバと同水準の対策状況であった。また、政府機関全体で1900台にのぼる電子メールサーバが運用されていた。

[情報セキュリティマネジメントに関する評価等]

各府省庁における情報セキュリティ対策に関するマネジメントが、PDCAサイクルの各段階で確実かつ効果的に行われているかを評価するため、「計画」「周知」「実施」「評価と改善」の各段階にわたる45の評価指標に基づき、政府機関統一基準の導入初年度の政府機関の情報セキュリティマネジメントの状況について調査・分析を行った。結果を別添5に示す。

＝分析＝

政府機関の模範となる優れた取組みを44件選定し、そのうち総務省のｅラーニングの取組みや、防衛省の外部委託における適切な調達仕様・契約の策定の実施等、取組み5件をベストプラクティスとして選定した。しかしながら、政府内外を問わず模範となる先進的な取組みは1件もみられなかった。

また、一般職員の情報セキュリティ教育受講率については、約6割の府省庁は受講率9割以上となっている一方、約4分の1の府省庁では受講率が4割に満たないなど、より組織的な教育の実施に向けた課題があることがわかった。

[SJ2007施策の取組み結果に関する評価等]

(ア) 政府機関統一基準とそれに基づく評価・勧告によるPDCAサイクルの構築

a) 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、毎年見直しを行い、また、その際には政府機関内外で発生したIT障害についても分析を行い、その結果を反映することとしている。

2007年度においては、DNSサーバーや政府ドメイン名に関する事項の追加等を行った政府機関統一基準の第3版を2008年2月の情報セキュリティ政策会議において決定した。

b) PDCAサイクルの定着

各府省庁は、PDCAサイクルを定着させ、組織全体での情報セキュリティ対策の底上げを図るため、特に、2007年度においては、職員に対する教育の拡充等により、セキュリティ意識の向上を図り、省庁対策基準及び実施手順等の遵守を徹底するとともに、自己点検及び監査の充実・向上を進め、対策実施状況の適切な把握を行った。

内閣官房は、各府省庁の対策の実施状況を、政府機関統一基準に基づき検査・評価し、勧告を通じた各府省庁の対策の改善と政府機関統一基準等の改善に結びつけるため、2007年度の各省庁の対策実施状況報告の結果をとりまとめて、情報セキュリティ政策会議に報告した。また、2007年8月に端末及びウェブサーバについて、2007年12月に電子メールサーバについて重点検査を行い、その結果

を情報セキュリティ政策会議に報告した。

c) 本格的な評価の推進及び結果の公表

内閣官房は、情報セキュリティ政策の枠組み文書に基づき、各府省庁における情報セキュリティ対策について、各種評価の実施により改善を促進するとともに、国民への説明責任を果たすためのものとして、情報セキュリティの維持・確保にも配慮しつつ公表を行った。

(イ) 独立行政法人等のセキュリティ対策の改善

政府機関統一基準を踏まえ、独立行政法人等の情報セキュリティ水準の向上を促進するため、内閣官房は各府省庁を通じて、独立行政法人等の情報セキュリティポリシーの整備を2007年7月に要請するとともに、必要な支援等を実施した。

内閣官房においては、独立行政法人等における情報セキュリティ対策の改善に向けた環境を整備した。具体的には、先行的に一部の独立行政法人に対してマニュアル等を提供するなど、情報セキュリティポリシー策定等のための支援を実施するとともに、情報セキュリティポリシーの見直しに取り組む先行的な機関から課題等についての情報を収集した。また、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」を掲載した。

(ウ) 中長期的なセキュリティ対策の強化・検討

a) 次世代の電子政府構築に向けた検討

内閣官房において、電子政府の情報セキュリティを企画・設計段階から確保する(SBD：Security by design)ための、方策の強化について検討を開始し、2008年2月の情報セキュリティ政策会議に検討状況を報告した。

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 等について安全性の低下が報告されていることから、関係する情報システム間における相互運用性を考慮して適切に移行を進めるため、内閣官房において、総務省、経済産業省及び関係府省庁の協力を得て、新たなハッシュ関数への移行に関する指針を策定し、2008年4月の情報セキュリティ政策会議にて指針を決定した。

(エ) サイバー攻撃等に対する政府機関における緊急対応能力の強化

政府機関に対するサイバー攻撃について、従来よくみられた愉快犯的な攻撃と比較して、近年、急速にその手法が巧妙化する中で、個別の府省庁が収集できる情報や整えられる体制ではその対応に限界が見えつつあった。

このような状況を受け、2007年度に、サイバー攻撃等に関する政府横断的な情報収集、攻撃等の分析・解析、各政府機関への助言、各政府機関の相互連携促進及び情報共有を行うための体制（GSOC：Government Security Operation Coordination team）の整備を開始した。

(オ) 政府機関における人材育成

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、2007年度は、内閣官房と総務省行政管理局において7月及び10月実施の「情報システム統一研修」セキュリティIIIの講義内容を改善するとともに、2008年度改訂に向けたセキュリティ関連コースの抜本的な見直しを行い、情報セキュリティ監査の内容を追加するなどの結論を12月に得た。

(2) 補完調査

強化遵守事項の適用状況や迷惑メール対策等情報セキュリティ対策上、重要な事項に関する状況の把握及び社会的に問題となった情報セキュリティ上の突発的事項に関する政府横断的な課題への迅速な対応等のために以下の補完調査を行った。

a) 強化遵守事項等の実施状況の調査(電子メール送信時の主体認証)

ボット対策として有効な対策の1つであることが知られているが、政府機関統一基準上は必須ではなく、各情報システムごとに各府省庁が必要と認めた場合に選択して実施する対策(強化遵守事項)となっている。

補完調査の結果、対策の実施率は94%となっており、政府機関の多くの電子メールシステムで対策の必要性が認められ、実施されていた。

b)迷惑メール対策の実施状況

スパムメールなどの迷惑メールへの対策がどの程度実施されているかについて把握した。

補完調査の結果、ほぼ全ての政府機関で迷惑メール対策の必要性が認められ、実施されていた。

c) 社会的に問題となった情報セキュリティ上の課題に対応するための緊急調査(JRE等を利用する政府機関の公開情報システムに係る緊急調査)

政府機関の電子申請システム等広く国民に向けて公開している情報システムの一部において、これらを利用するに際して、利用者である国民の方々がパソコンなどにインストールすることが必要なJRE(Java Runtime Environment)に脆弱性が存在していることを受け、NISCにおいて緊急調査を実施し、各政府機関の公開情報システムにおけるJREの使用状況などを把握するとともに、脆弱性の問題について利用者に対して情報提供を行っているどうかを確認した。また、その結果について7月20日に報道発表をするとともに、2007年10月の情報セキュリティ政策会議に報告した。

(3) 総評

対策実施状況に関しては、基本計画の目標を達成するためには、政府全体として「情報セキュリティ教育の実施」、「格付け・取扱い制限に係る措置」、「システム台帳の

整備」等の課題が残っている。情報セキュリティ対策の推進に当たって基本となる教育等の重要な課題が前回（2006年度）に続いて不十分な状態にあることは、重大な問題と言わざるを得ない。今後、改善に向けた取組みを加速する必要がある。

また、端末及びウェブサーバについて重点検査を実施したところ、昨年と比較して対策実施状況に大きな改善がみられるとともに、マネジメント評価についても、ベストプラクティスとして外部委託やeラーニングの取組み等5件が選定され、各府省庁における対策が着実に向上していると認められた。しかし、重点検査では、まだ半数の省庁では完全ではなく、対策が全て完了するのは2008年度になるほか、マネジメント評価においては政府内外を問わず模範となる先進的な取組みは1件もみられなかった。引き続き更なる改善に向けた取組みが必要である。

上述の結果を総合すれば、政府機関統一基準に基づく対策実施の2年目ということもあり、2006年度と比較し一定の成果がみられるものの、対策が不十分な部分や課題が残っている結果となり、目標達成に向けた取組みが必要である。

第3節　2008年度に向けた課題

2008年度は基本計画の最終年度であり政府機関のＰＤＣＡサイクルについて、その定着及び組織全体への浸透を徹底することが必要である。そのためには、セキュリティ教育に関する実施体制の充実・向上を図り、全職員、全情報システムの対策実施状況の適切な把握を行うこと、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を図ることが不可欠である。

また、電子政府として構築が進みつつある各種業務・システムに適切に情報セキュリティ要件が取り入れられることは必要不可欠であることから、それを着実に実現するための検討を進めることが求められる。

さらに、2008年度は、これまで実施してきた政府機関対策を通じて得られた知見等に基づき、2009年度から始まる次期基本計画における政府機関対策について政府機関統一基準のあり方や評価のあり方を含めた検討が必要である。

第3章　重要インフラにおける現状の評価等

第1節　重要インフラにおける情報セキュリティに関する2007年度の取組み

1．2007年度の取組みの背景

重要インフラにおいては、そのサービスの安定的供給が最優先課題であるという面から、各事業において発生するIT障害が国民生活・社会経済活動に重大な影響を及ぼさないよう対策を実施することが必要である。このような安全対策は、一義的には各重要インフラ事業者等が担うべきものであるが、社会全体のITへの依存が進む中で、日増しに増大していく各種脅威への対策が個々の取組みだけでは限界に達しつつあるのが現実である。

そこで、中・長期的な取組み課題は山積するものの、先ずは実施可能なものから取組みを開始し、継続的な見直しと改善を通じて、情報セキュリティ対策の向上を図っていくというアプローチが妥当との判断に立ち、「重要インフラの情報セキュリティ対策に係る行動計画」（2005年12月13日情報セキュリティ政策会議決定）（以下「行動計画」という。）を定め、「2009年度初めには、重要インフラにおけるIT障害の発生を限りなくゼロにすること」（基本計画）を目指して取組みを進めているところである。

重要インフラにおける2007年度の取組みは、この行動計画の下で情報セキュリティ対策を推進するため、2006年度の成果を踏まえ、引き続き取り組まれたものである。

2．2007年度の取組み

行動計画においては、重要インフラ関係の4本の施策の柱（①安全基準等の整備　②情報共有体制の強化　③相互依存性解析の実施　④分野横断的な演習の実施）と、各主体における取組み項目を示し、各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つなげていくことにしている。また、行動計画は、3年ごと又は必要に応じ、見直しを行うこととなっている。

これを踏まえ、SJ2007において、具体的取組みを定め、実施したところである（具体的には「第2節2」において後述）。

【参考：　4本の施策の柱】

①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」の整備

2006年2月2日に情報セキュリティ政策会議において決定された「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」（以下、「指針」という。）を踏まえ、それぞれの重要インフラ事業分野ごとに、必要な又は望ましい情報セキュリティ対策の水準について、「安全基準等」に明示することを目標とする。

さらに、指針については1年ごと及び必要に応じて適時見直すこととし、「安全基準等」については、情報セキュリティを取り巻く環境の変化に応じ、随時見直しを行う。

②情報共有体制の強化

IT障害に関する情報について、1）IT障害の未然防止、2）IT障害の拡大防止・迅速な復旧、3）IT障害の要因等の分析・検証による再発防止の3つの側面から、政府等は重要インフラ事業者等に対し適宜・適切に提供する。

また重要インフラ事業者等間並びに相互依存性のある重要インフラ分野間においてはこ

れら情報を共有する体制を強化する。

③相互依存性解析の実施

我が国全体としての重要インフラ対策の向上に向けた、分野横断的な状況の把握のため、それぞれの重要インフラに起こりうる脅威が何であるかを把握するとともに、ある重要インフラにIT障害が生じた場合に、他の重要インフラに、いかなる影響が波及するかという相互依存性の把握を行う。

④分野横断的な演習の実施

想定される具体的な脅威シナリオの類型をもとに、各重要インフラ所管省庁、各重要インフラ事業者等、各重要インフラ分野の CEPTOAR 等の協力の下に、重要インフラ横断的な演習を行う。演習を通じ、安全基準等、情報共有体制、情報共有・分析機能、相互依存性解析等の各施策の実効性・妥当性を定期的に、かつ、段階的に、検証する。

また、この演習やその他の訓練、セミナー等を通じて、重要インフラ所管省庁及び重要インフラ事業者等を中心に、高度なITスキルを有する人材を育成し、確保する。

第2節 2007年度の取組み及び取組みを受けた重要インフラにおける現状の評価等（2007年度の評価等）

1．2007年度の評価等に関する基本的考え方（評価等の視点）

第1節に述べたとおり、重要インフラの情報セキュリティ対策については、行動計画に従って、官民の緊密な連携の下で、情報セキュリティ対策の強化を目指しているところである。行動計画に定める取組みは、IT障害の発生を可能な限り未然に防止するために必要な対策及びIT障害が発生した際の影響を可能な限り極小化するために必要な具体的対策（すなわち、重要インフラにおけるIT障害の発生を限りなくゼロにするための対策）であり、これらの取組みの進捗度合いをみることで、重要インフラにおけるサービスの安定的供給機能の維持とリスクへの適切な対応の実現度合いを把握することができる。このことを踏まえ、2007年度の重要インフラにおける情報セキュリティ対策の評価等は、2006年度同様、対策向上を目的に行動計画で定めた4本の施策の柱それぞれについて、各年度ごとの目標（具体的取組み）に対する実施状況を把握し、その進捗度合いがどの程度の状態であるかということを確認するという視点に立って行うこととする。

2．評価等について（評価指標等）

（1）2007年度の評価等について

2007年度における重要インフラにおける情報セキュリティ対策の評価等を行うに当たり、進捗度合いを把握する対象となる「具体的取組み」（すなわち目標）は、SJ2007に記載されているそれぞれの取組みである（別表1）。そして、これらの取組みの進捗度合いそのものが、2007年度の進捗度合いを把握するための指標である。

（2）2008年度の評価等について

2008年度についても年度計画に盛り込む取組みの進捗度合いが指標となる。目標とする取組みの設定については、重要インフラ専門委員会において、報告された2007年度の実施状況や実際のIT障害の発生状況なども踏まえながら、また2007年12月よ

り開始している行動計画見直しの検討状況も考慮し、重要インフラにおける情報セキュリティ対策の着実な向上を確保することに留意しつつ、行うこととする。

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に関しては、2007年度においては、表-1のとおり、計7回（2006年度・3回）の重要インフラ専門委員会会合を開催し、それぞれ検討を重ねたところである。

また、「「重要インフラ連絡協議会（CEPTOAR－Council）（仮称）」創設に向けた検討の場」を設け、2007年5月から2008年3月まで、8回の会合及び5回のワーキングを開催したほか、「分野横断的演習」及び「相互依存性解析」についても、2007年6月から2008年3月まで、それぞれ5回の検討会と解析7回、演習5回のワーキングを開催し、具体的な検討、取組みを進めたところである。

表-1 重要インフラ専門委員会会合

	主な議題
第9回専門委員会 （2007年4月12日）	・CEPTOAR の整備状況 ・2006年度の進捗状況、及び2007年度の取組目標について
第10回専門委員会 （2007年6月19日）	・2007年度の相互依存性解析及び分野横断的演習の枠組みと進め方
第11回専門委員会 （2007年9月28日）	・2007年度「安全基準等の見直し状況等の把握及び検証」（実施案） ・2007年度「安全基準等の浸透状況等に関する調査」（実施案） ・重要インフラにおける補完調査
第12回専門委員会 （2007年12月3日）	・2007年度「安全基準等の見直し状況等の把握及び検証」（中間報告） ・2007年度「指針」の見直し（実施案） ・「重要インフラ連絡協議会」（仮称）の創設促進に関する報告 ・静的相互依存性解析の総括 ・2007年度における分野横断的演習 ・行動計画見直しの検討スケジュール
第13回専門委員会 （2008年1月31日）	・2007年度「安全基準等の見直し状況等の把握及び検証」（報告） ・2007年度「指針」の見直し（中間報告） ・情報共有・分析機能の整備状況 ・「重要インフラ連絡協議会」（仮称）創設に向けた検討状況 ・2007年度分野横断的演習の実施（具体的シナリオ等） ・行動計画の見直し（論点のたたき台）
第14回専門委員会 （2008年3月4日）	・2007年度「安全基準等の浸透状況等に関する調査」（報告） ・2007年度「指針」の見直し（報告） ・行動計画の見直し（論点整理骨子案）
第15回専門委員会 （2008年3月28日）	・行動計画の見直し（論点整理に関する集中討議）

その結果、行動計画に定める4つの施策の柱それぞれについて、本年度は以下のとおりの取組みの成果が得られた。

(ア) 安全基準等の整備

①「安全基準等」の見直し

2007年6月に行われた指針の改定を踏まえ、重要インフラ10分野すべてにおいて9月末までに「安全基準等」の見直しが実施された。

②「安全基準等」の見直し状況の把握及び検証

第11回重要インフラ専門委員会にて了承された「2007年度重要インフラにおける「安全基準等の見直し状況の把握及び検証」について」に基づき、

ⅰ)「安全基準等」の見直し状況等の把握

ⅱ)「指針」との対応状況の検証

ⅲ)「相互依存性解析」の成果を踏まえ各分野の「安全基準等」において今後反映することが望ましい事項の洗い出し

を行い、第13回重要インフラ専門委員会で報告を行った。

③各重要インフラ分野における安全基準等の浸透状況等に関する調査の実施

第11回重要インフラ専門委員会にて了承された「2007年度重要インフラにおける「安全基準等の浸透状況等に関する調査」について」に基づき、重要インフラ10分野について、2006年度に策定・見直しを行った各重要インフラ分野における安全基準等が事業者等にどの程度浸透しているか、また事業者等が安全基準等に対して準拠しているかを把握するための調査を実施し、第14回重要インフラ専門委員会で報告を行った。

④指針の見直し

第12回重要インフラ専門委員会にて了承された「2007年度「指針」の見直し」に基づき、

ⅰ) 定常的なIT障害の発生状況の分析

ⅱ)「相互依存性解析」の成果

ⅲ) 関連文書の検証

ⅳ) 社会的条件や環境の変化の検証

の4つのアプローチからの分析・検証により、情報セキュリティ対策に関する「問題意識」を抽出して現在の指針と照らし合わせを実施した。その結果を第14回重要インフラ専門委員会に報告し、見直しの要点を重要インフラ10分野に周知する参考資料としてとりまとめた。

(イ) 情報共有体制の強化

①情報共有体制整備と機能強化のための取組み

CEPTOAR特性把握マップのとりまとめ、情報共有訓練及びCEPTOARも参加した官民連携による分野横断的演習を実施した。

②各重要インフラ分野における CEPTOAR 整備の推進

新規追加3分野(水道、医療、及び物流)において、2007年度までに整備が完了した。これにより重要インフラ10分野すべてにおいて整備が完了した。

③CEPTOAR 特性把握マップ

重要インフラ所管省庁等の協力を得て、2007年度末現在の各 CEPTOAR の特性を把握するとともに、整備状況とあわせて CEPTOAR 特性把握マップ(ver2)をとりまとめた。

④CEPTOAR－Council(仮称)設置に向けた検討

CEPTOAR 代表者等から構成される「重要インフラ連絡協議会(CEPTOAR－Council)(仮称)創設に向けた検討の場」を設け、8回の会合を開催した。同「検討の場」において、来年度以降の検討方針を「「重要インフラ連絡協議会(CEPTOAR－Council)」(仮称)の創設についての基本的な考え方」としてとりまとめた。

(ウ) 相互依存性解析の実施

有識者、各重要インフラ分野の分野委員及び重要インフラ所管省庁からなる相互依存性解析検討会を設置し、検討会5回･WG7回を実施し、「相互依存性解析における視点(考え方のポイント)」を整理しつつ、「動的相互依存性解析」を実施した。併せて2006年度と2007年度に実施した解析結果を整理し「相互依存性解析報告書」としてとりまとめた。

(エ)分野横断的演習の実施

有識者、各重要インフラ分野の分野委員及び重要インフラ所管省庁からなる分野横断的演習検討会を設置し、検討会5回･WG5回を通じてシナリオ等についての議論を経て、約120名の参加を得て分野横断的な機能演習を実施した。

(2) 施策の取組みによる社会的変化に関する評価等

以上のような、行動計画に基づく具体的取組みを進めたこと等により、重要インフラにおけるサービスの安定的供給機能を維持しつつリスクに適切に対応する社会の実現に向け、本年度においては、次に掲げるような社会的変化が認められた。

(ア) 安全基準等の整備

重要インフラ10分野で安全基準等の見直しが実施されており、重要インフラにお

ける情報セキュリティ対策が着実に前進していることが確認できた。具体的には、各分野毎の安全基準等のＰＤＣＡサイクルにおいて、各分野毎の独自の観点に加え政府の指針の観点を盛り込んだ見直しが進展するとともに、同一指針に基づく分野横断的な検証によって各分野毎の安全基準等の特徴等が明らかになることで、分野間でのノウハウの共有のための環境整備が進展した。

また、各分野毎の安全基準等に基づき重要インフラ事業者の内規の見直しが進んでおり、事業者毎の内規のＰＤＣＡサイクルにおいても政府指針の観点が反映されつつある事が確認できた。ただし、全事業者への浸透にはなお時間を要することも推定されている。

また、指針の見直しを通じ、安全基準等の適用対象とならないシステムも含めて、我が国の国民生活や社会経済活動に多大なる影響を及ぼすおそれが生じる障害が発生していることや、水道分野と他分野との相互依存性を踏まえた対応の必要性、過去の事例の知見や教訓を受けた対策の重要性などの問題意識が改めて認識された。

(イ) 情報共有体制の強化

重要インフラ10分野すべてにおける CEPTOAR の整備完了や、「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）の創設についての来年度以降の検討方針の取りまとめ、官民連携による分野横断的演習の実施、情報共有訓練などを通じ、重要インフラにおける官民の各主体間での情報共有、連絡・連携のための枠組みの構築が一層進展した。

(ウ) 相互依存性解析及び分野横断的演習

2006年度における静的相互依存性解析に基づき、2007年度においては、相互依存性に関わる「視点の整理（定義化）」を実施し、重要インフラ分野間における相互依存性に対する認識の共有・共通化が図られた。さらに、動的相互依存性解析の実施を通じて重要インフラ事業者間には相互依存関係はあるものの、それぞれに適切な対策が施されていることが判明した。しかしながら、その対策が時間的経過や状況の変化により対策の想定状況を越えた場合には、サービスの停止や機能の低下に至る可能性があることを確認した。

また、分野横断的演習については、NISC、重要インフラ所管省庁、重要インフラ事業者等、さらにはCEPTOARがそれぞれプレイヤーとして参加し、緊急時における情報共有・情報連絡について、具体的事象を想定したシナリオによる演習を実施した。これらの活動を通じて、IT障害発生時における情報共有・情報連絡手法等の確認と検証を実施した。

(3) 補完調査の結果について

(ア) 補完調査の目的及び方法

重要インフラにおける情報セキュリティ対策に関する2007年度の補完調査は、「情報セキュリティ政策2007年度の評価等に向けた「作業方針」」（2007年10月3日）に

基づき、(イ)に示す各項目についてのデータを捕捉するとともに、実際に発生した事例について個別に検証を行うことにより、重要インフラにおける情報セキュリティ対策に関する変化の状況を把握し、上記(2)の評価等を補完するために行う。

(イ) 補完調査①～参考となるデータの捕捉～

i) 安全基準等の整備の状況について

安全基準等の整備状況を示すデータとして、本年度実施した「安全基準等の浸透状況等に関する調査」(※1)で得られたデータをもとに、「安全基準等の認知率」及び「安全基準等の見直し率」の捕捉を行った結果、以下のとおりであった。

なお、算出に当たっては、単純集計では回収数の多い分野の全体集計への影響が大きくなることから、重要インフラ全体の状況把握をより適切に行うため、共通の重みづけ(※2)で集計を実施した。

調査依頼対象	２９５８事業者等
回答数	２８４６事業者等 （回収率９６．２％）
認知率	９７．９　％ 「名称・内容ともに知っている」「名称のみ知っている」を合算
見直し率	５４．８　％ 「定期的に実施している」 「実施したことがある」を合算

※1 「安全基準等の浸透状況等に関する調査」
各重要インフラ分野の事業者等を対象に、各重要インフラ分野のおける安全基準等がどの程度浸透しているか、また事業者等が安全基準等に対して準拠しているかを把握するために行ったアンケート方式による調査。

※2

$$A = \frac{\left(a_1 / \alpha_1\right) + \left(a_2 / \alpha_2\right) + \cdots + \left(a_n / \alpha_n\right)}{n}$$

A:回答Ａに対する全体集計（％）
a_i:分野iにおける回答Ａの数（$1 \leq i \leq n$）
α_i:分野iにおける回収数（$1 \leq i \leq n$）

ii）情報共有体制の強化の状況について

情報共有体制の強化の状況を示すデータとしては、「2007年度における「情報提供」の件数」及び「CEPTOARを構成する事業者等の数」の捕捉を行った。

「情報提供」とは、注意喚起等、各重要インフラ事業者等の対策に資する情報について、内閣官房から重要インフラ所管省庁を通じ各重要インフラ事業者等に対し行うものとして行動計画に規定しているものであるが、2007年度においては、3件（うち情報共有訓練のために実施したもの2件）であった。

また、「CEPTOAR を構成する事業者等の数」については、全10分野、14 CEPTOAR の合計で5,692事業者等であった。各重要インフラ分野ごとの事業者数等については、「CEPTOAR特性把握マップ」のとおりである。

iii）相互依存性解析の実施、分野横断的な演習の実施の状況について

相互依存性解析及び分野横断的演習の実施状況を示すデータとしては、それぞれに要した「年間延べ時間」及び「延べ参加者数」を捕捉した。

先述のとおり、2007年度においては、「相互依存性解析」及び「分野横断的演習」について、2007年6月から2008年3月まで、それぞれ5回の検討会と解析7回、演習5回のワーキングに有識者、各重要インフラの分野委員及び所管省庁といった巾広い参画が得られたところである。その結果、相互依存性解析には年間延べ92．5時間、参加者数延べ395人、計622（人･時間）を費やし、分野横断的演習には年間延べ39時間、参加者数延べ473人、計1178（人･時間）を費やした。

なお、2008年2月6日に実施した本年の分野横断的演習当日参加者は、116名であった。

（ウ）補完調査②～具体的事例の検証～

具体的事例の検証として、2007年度において実際に発生した「IT障害」及びIT障害の要因となり得る「リスク」について、類似事例の発生状況（可能性）や社会的影響の大きさにも着目し、内閣官房において事例を選択し、各重要インフラ分野の協力（情報提供･ヒアリングの実施等）を得ながら、ⅰ）システム障害（非意図的要因）が発生した事例、ii）業務システムがウイルス感染した事例、iii）新潟県中越沖地震発生時の状況　について、それぞれ以下のとおり検証を行った（なお、ⅰ）及びii）において検証の対象とした事例の概要は、別紙のとおり）。

ⅰ）システム障害（非意図的要因）が発生した事例

（検証結果）

○　利用者がサービスの提供を受ける際に使用する情報システムの障害は、利用者への影響が大きく現れやすいことが確認された。

○　障害発生時においては、原因究明よりも応急復旧対応が優先されること、また、復旧のためのシステムの利用制限のタイミングなど、事業継続と障害復旧の両立のための判断が重要でありかつ困難であることが確認された。

○ 同一のシステムを多数の事業者が同時に利用している場合には、当該事業者間での連携が特に重要であり、またシステムを構築・納入する業者（複数であれば尚更）との連携・意思疎通も同様に重要であることが確認された。

○ 障害の発生原因は多様であることや、業務や情報システムの複雑化が進んでいることなどから、未然防止の対策で対応できる範囲には限界があることが改めて確認された。

（課題・留意点）

○ 情報システムを利用したサービス提供の基盤化が進む中、障害の未然防止だけでなく、障害が発生した際の応急対応をより充実したものにすることも効果的。その際は、各事業分野の特性に応じて、以下の事項について留意が必要。

・ 個々の事業者としての応急復旧対応と、他の事業者への情報提供との優先度も踏まえて、情報共有等の事業者間連携について検討すること。

・ システムを構築する事業者だけでなく、システムを利用してサービスを提供する事業者としての役割や責任も踏まえ、適切な対応と連携について検討すること。

・ システム復旧後にも、利用者への影響は残存する場合があることを踏まえた対応を検討すること。

○ 発生した障害の分析を行い、事後の再発防止に活用することは効果的。

ii）業務システムがウイルス感染した事例

（検証結果）

○ ウイルス対策ソフトは導入されていたが、当該ウイルスに対応していなかったため検出できなかったことから、新種のウイルスの場合、未然防止の対策で対応できる範囲には限界があることが改めて認識された。ウイルス等のサイバー攻撃に対しては未然防止の対策も重要であるが、攻撃手法が日々変化していることから事前に準備可能な対策では防ぎきれない場合もある。

○ 障害発生後は、原因究明や利用者等への周知よりも、システム復旧等の応急対応をとることの方が、事業者にとっての優先的関心事であることが確認された。

○ 一度システム内部に侵入したウイルスを完全な駆除を確認するのは困難であり、復旧のための対応に多くの時間やコストがかかる場合があることが確認された。

（課題・留意点）

○ インターネットを経由してのウイルス感染については、特定の分野等に特化したものではなく、何らかの形でインターネットと直接的・間接的に接続関係があるシステムを使用している事業者にとっては、共通的な脅威である。

○ 未知のウイルス等の新たな脅威や事例に関する情報は、幅広く共有することで他の事業者等での未然防止や応急対応に資するのではないか。関係

機関の既存制度を効果的に活用するなど、情報共有体制の充実について考えることが必要。

○ 一方、コスト等の実効性も含めると、未然防止だけでなく、感染時に柔軟かつ適切に対応できるように準備することも必要。

iii) 新潟県中越沖地震発生時の状況

（検証結果）

○ 複数の重要インフラ分野においてサービスが停止したものの、2004 年新潟県中越地震での経験や教訓を活かした対策が立てられていたことから、IT 障害については被害を最小限に抑えることができたものと考えられる。各分野にて整備された安全基準等に基づく対策や、分野間の依存性を考慮した対策が有効であったと考えられる。

○ マシンルームの床全体が免震構造であったためオンラインシステムの通常通り稼動が可能であった例や、本社だけでなく子会社のシステムもデータセンターに収容する等のサプライチェーン全体を見据えた情報システム整備やバックアップの構築が有効であった例などが確認された。

○ 商用電源の停電を原因とする金融分野事業者の一部店舗の休業や、通信回線の輻そうによる原子力発電所の地震計データの一部伝送停止など、重要インフラ分野間での影響の波及が確認された。

○ 災害応急体制のもとでの情報共有、被災状況の把握、各省庁の対応状況等の確認が行われたものの、重要インフラ行動計画に基づく官民の情報連絡は、機能する場面とはならなかった。

（課題・留意点）

○ 首都圏直下地震等では、より大規模な人的被害・物的被害が想定されるとともに、その地理的条件から重要インフラの基幹となるシステムにおいても、大規模なシステム障害の発生のおそれがある。

○ 自然災害発生時の対応について定める既存の法令や防災計画等の枠組み等との整合を図りつつ、情報セキュリティの観点からの官民の情報連絡や総合調整について検討することが必要。

(エ) 補完調査のまとめ

以上のとおり補完調査を行った結果、重要インフラにおける情報セキュリティ対策の状況については、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、向上が進んでいることが確認できた。

一方で、障害リスクの発生時における情報や、他分野、他事業者の「経験」から得られた知見の共有の重要性は改めて確認できたものの、重要インフラ事業者等間及び重要インフラ分野間において、これらの情報共有については、現時点において活発に進んでいるものとは確認できておらず、政府内の連絡体制や CEPTOAR に期待される役割を如何に発揮していけるかが今後の課題であると考えられる。

(4) 総評

以上のことより、2007年度における取組みは、別表2のとおり、2006年度に引き続き、当初の目標に沿った成果をあげており、個々の重要インフラ事象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。

一方で、構築された情報共有体制の活発な運用までには、なお時間を要するものと考えられることや、国民生活、社会経済活動におけるITの利用は引き続き進展や拡大が予想されること、加えてIT障害を発生させる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対策については、引き続き継続的にその向上に取り組んでいくことが必要である。

第3節　2008年度に向けた課題

重要インフラにおける情報セキュリティ対策の向上のためには、行動計画に掲げた取組みの着実な進捗が必要不可欠である。現在の行動計画の最終年度にあたる2008年度においては、これまでの取組みを通じて認識した以下のような課題を踏まえた取組みを行うことが重要である。

(ア) 安全基準等の整備

各重要インフラ分野における安全基準等については、2007年6月に改定された指針の内容を踏まえ全分野で見直しが行われ、指針をトリガーとした分野横断的なＰＤＣＡサイクルが動き出したことが確認できた。今後は、このサイクルがセキュリティレベルの底上げのツールとして有効に機能するよう定着させていくことが必要である。

一方で、安全基準等について「見直し状況等の把握」「浸透状況等調査」「指針の見直し」の各施策を進める中で、その運営サイクルについて、各分野において安全基準等の大規模な改定や検討会等を行う場合に要する期間や、事業者等による内規の見直し期間との重複による混乱の発生などの課題が顕在化しており、実態を踏まえた望ましい形にすることが必要である。

また、「安全基準等の浸透状況等に関する調査」の結果から、2006年9月の安全基準等の策定･見直しから 1 年経過した時点で内規見直しを終えることができた事業者等は半数程度にとどまることが推定されるため、2007年度は、指針改定によって安全基準等の見直しへの新たな視点を喚起するのではなく、内規見直しを終えていない事業者等への安全基準等の着実な浸透を期することを優先したところである。見直しの過程で明らかになった見直しの要点については、現在検討中の行動計画見直しの状況等も踏まえ、来年度以降の指針見直しにて検討する必要がある。

(イ) 情報共有体制の強化

①情報共有体制整備と機能強化

2006年度に構築された、重要インフラにおける官民の各主体間での情報共有、連

絡･連携のための枠組みは、2007年度の取組みによって一層充実進展をした。

しかしながら、重要インフラ事業者等間及び重要インフラ分野間における、障害リスクの発生時の情報や他の分野･事業者の「経験」から得られた知見の共有については、現時点において現実に活発に進んでいるものとは確認できていない。今後は、これらの情報の共有がいかにすればスムーズに進むか、阻害要因の研究とその解決に向けた対策の検討が課題である。

②「CEPTOAR 特性把握マップ」のフォローアップ

「CEPTOAR 特性把握マップ」とは、各重要インフラ分野ごとに設けられる CEPTOAR について、事業特性から反映された機能特色等について業種ごとに把握し、特徴把握が容易かつ可視性を工夫したものであり、今後の CEPTOAR のあり方を考える上で参考となるものである。

2007年度末で重要インフラ10分野すべてにおいて、CEPTOAR の整備が完了したところであるが、整備の過程において、整備目的の共有、既存の連絡体制との整合性、必要となるコストなど、様々な課題の中で整備が進められており、分野によっては、今後具体的な運用等を通じて機能の充実がなされる可能性もある。

③「CEPTOAR－Council」（仮称）創設の検討

「CEPTOAR－Council」（仮称）は、重要インフラ事業者等において、分野横断的な情報共有の推進を図り、多様な知見をサービスの維持･復旧に活かしていくための、各 CEPTOAR 間での横断的な情報共有の場として想定しているものである。

2007年度においては、「CEPTOAR－Council」（仮称）創設に向けた検討の場」を8回及びワーキングを5回開催し、創設に向けての基本的考え方を取りまとめたところであり、今後はこの考え方に基づき創設準備会を設置し、2008年度内の「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）の創設を目指し、より具体的な検討を進める必要がある。

（ウ）相互依存性解析の推進

官民の連絡･連携体制と、IT障害発生時の対応能力の向上を図るため、2006年度及び2007年度における相互依存性解析のとりまとめを踏まえ、「分野間のシステムにおける繋がり」等の課題についてその実施方法も含め検討することにより、相互依存性解析の深化を図る必要がある。

（エ）分野横断的演習の推進

官民の連絡･連携体制と、IT障害発生時の対応能力の向上を図るため、2007年度に引き続き、重要インフラ所管省庁、各重要インフラ事業者等及び各重要インフラ分野の CEPTOAR 等の協力を得て、相互依存性解析の知見を考慮しつつ、想定される具体的な脅威シナリオ等、諸条件を基にテーマを設定し、テーマに応じた最適な演習手法（机上演習、機能演習など）による分野横横断な演習を実施し、その深化を図る必要がある。

（別表1）

4本の施策の柱	2007 具体的取組み目標	
①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」の整備	安全基準等の見直し	2007年6月を目処に行われる指針の改定を踏まえ、2007年9月を目処に、各重要インフラ分野において、安全基準等の確認・検証を行い、必要に応じ改定等の対策を実施する。
	「安全基準等」の見直し状況等の把握及び検証	各重要インフラ分野における「安全基準等」について、各重要インフラ所管省庁の協力を得つつ見直しの状況を2007年中に把握するとともに、相互依存性解析の成果も踏まえた検証を2007年度中に実施する。
	各重要インフラ分野における安全基準等の浸透状況等に関する調査の実施	2007年度中に、内閣官房は、重要インフラ所管省庁の協力を得つつ、2006年度に策定・見直しを行った各重要インフラ分野における安全基準等の浸透状況についての調査を実施する。
	指針の見直し	2007年度中に相互依存性解析の成果も踏まえ、各重要インフラ所管省庁の協力を得て、指針の見直しを実施する。
②情報共有体制の強化	情報共有体制整備と機能強化	各分野における CEPTOAR の整備及び CEPTOAR-Council（仮称）の整備等の状況変化を踏まえ、2006年度に整備された官民の情報共有体制に対して追加すべき機能・要件等の検討を行う。
	各重要インフラ分野におけるCEPTOAR整備の推進	2007年度末までに、新規追加分野（水道、医療及び物流）において CEPTOAR が整備されるよう取組みを進める。
	「CEPTOAR 特性把握マップ」のフォローアップ	2007年度中に、各分野における CEPTOAR の機能・要件の検討状況及び整備状況（新規追加分野については整備状況）の把握を行う。また2007年度末を目処に、CEPTOAR 特性把握マップのフォローアップを行う。
	「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）創設の検討	2007年度中に重要インフラ連絡協議会（CEPTOAR－Council）（仮称）の創設についての基本的合意を得るべく、検討の場を開催し課題についての検討を進める。
③相互依存性解析の実施	重要インフラ分野間の相互依存性解析の推進	重要インフラ分野における IT 化の一層の進展と分野間の関連性の高まりを踏まえ、官民の連絡・連携体制の機能と、事業継続を含む IT 障害発生時の対応能力の向上等を図るため、2007年度は、国内外の脅威の類型や脅威と障害の因果関係、障害と事業継続との関係などについての検討の深化や演習シナリオへの反映を行うとともに、重要インフラにおける障害発生から波及・拡大という連鎖的な伝播プロセスを動的に把握する動的依存性解析を推進する。なお、実施にあたっては、実施方法について十分に検討を行う

④分野横断的な演習の実施	重要インフラ機能演習の実施	官民の連絡･連携体制の機能と、IT 障害発生時の対応能力の向上等を図るため、2007年度は、重要インフラ所管省庁、各重要インフラ事業者等及び各重要インフラ分野のCEPTOAR 等の協力を得て、相互依存性解析の知見を踏まえつつ、想定される具体的な脅威シナリオの類型をもとにテーマを設定し、分野横断的な機能演習を実施する。
	各分野サイバー演習との連携	2007 年度に分野ごとに実施される「情報通信」等のサイバー演習と、内閣官房の実施する演習について、実施形態及びその目的の整合性を考慮しつつ、連携を図る。

(別表2)

2007年度における取組みの進捗状況

4本の施策の柱	2007 具体的取組み目標		2007成果
①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」の整備	安全基準等の見直し	・2007年6月を目処に行われる**指針の改定を踏まえ**、2007年9月を目処に、各重要インフラ分野において、**安全基準等の確認・検証**を行い、必要に応じ改定等の対策を実施。	2007年6月に行われた指針の改定を踏まえ、**重要インフラ10分野について9月末までに実施**。
	「安全基準等」の見直し状況等の把握及び検証	**・各重要インフラ分野における「安全基準等」について**、各重要インフラ所管省庁の協力を得つつ見直しの状況を2007年中に把握 ・相互依存性解析の成果も踏まえた**検証**を2007年度中に実施。	・第11回重要インフラ専門委員会にて提示された「2007年度重要インフラにおける「安全基準等の見直し状況の把握及び検証」について」に基づき**実施**。
	各重要インフラ分野における安全基準等の浸透状況等に関する調査の実施	・2007年度中に、内閣官房は、重要インフラ所管省庁の協力を得つつ、2006年度に策定・見直しを行った**各重要インフラ分野における安全基準等の浸透状況についての調査**を実施。	・第11回重要インフラ専門委員会にて提示された「2007年度重要インフラにおける「安全基準等の浸透状況等に関する調査」について」に基づき**実施**。
	指針の見直し	・2007年度中に相互依存性解析の成果も踏まえ、各重要インフラ所管省庁の協力を得て、**指針の見直しを実施**。	・第12回重要インフラ専門委員会にて提示された「2007年度重要インフラにおける「指針の見直し」について」に基づき検討を**実施**。
②情報共有体制の強化	情報共有体制整備と機能強化	・各分野における CEPTOAR の整備及び CEPTOAR-Council（仮称）の整備等の**状況変化を踏まえ**、2006年度に整備された官民の情報共有体制に対して**追加すべき機能・要件等を検討**。	・**CEPTOAR特性把握マップのとりまとめ**、**情報共有訓練**及び CEPTOARも参加した官民連携による**分野横断的演習**を実施。
	各重要インフラ分野における CEPTOAR 整備の推進	・2007年度末までに、**新規追加分野（水道、医療及び物流）においてCEPTOARが整備**されるよう取組み。	・新規追加3分野（水道、医療、及び物流）において、2007年度までに**整備を完了**。
	「CEPTOAR 特性把握マップ」のフォローアップ	・2007年度中に、**各分野における** CEPTOAR の機能・要件の検討状況及び整備**状況**（新規追加分野については整備状況）**の把握**。 ・2007年度末を目処に、**CEPTOAR特性把握マップをフォローアップ**。	・重要インフラ所管省庁等の協力を得て、2007年度末現在の**各 CEPTOAR の特性を把握**するとともに、整備状況とあわせて**CEPTOAR 特性把握マップ(ver2)をとりまとめ**。
	「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）創設の検討	・2007年度中に重要インフラ連絡協議会（CEPTOAR－Council）（仮称）の創設についての**基本的合意**を得るべく、**検討の場を開催**し課題についての検討を進める。	・CEPTOAR 代表者等から構成される「重要インフラ連絡協議会（CEPTOAR-Council）（仮称）創設に向けた検討の場」を設け、**8回の会合を開催**。 ・「検討の場」において、来年度以降の検討方針を**「「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）の創設についての基本的な考え方」**としてとりまとめ。

③相互依存性解析の実施	重要インフラ分野間の相互依存性解析の推進	・国内外の脅威の類型や脅威と障害の因果関係、障害と事業継続との関係などについての**検討の深化及び演習シナリオへの反映**、 ・重要インフラにおける障害発生から波及・拡大という連鎖的な伝播プロセスを動的に把握する**動的依存性解析を推進**。	・検討会を設置し、**検討会5回・WG7回**を実施。 ・「相互依存性解析における視点（考え方のポイント）」を整理しつつ、「**動的依存性解析**」を実施。 ・2006年度と2007年度に実施した解析結果を整理し「**相互依存性解析報告書**」としてとりまとめた。
④分野横断的な演習の実施	重要インフラ機能演習の実施	官民の連絡・連携体制の機能と、IT障害発生時の対応能力の向上等を図るため、重要インフラ所管省庁、各重要インフラ事業者等及び各重要インフラ分野の CEPTOAR 等の協力を得て、**分野横断的な機能演習を実施**。	・有識者、各重要インフラ分野の分野委員及び重要インフラ所管省庁からなる分野横断的演習検討会を設置し、検討会5回・WG5回を通じてシナリオ等についての議論を経て、約120名の参加を得て分野横断的な**機能演習を実施**した。
	各分野サイバー演習との連携	**分野ごとに実施される**「情報通信」等のサイバー**演習**と、内閣官房の実施する演習について、実施形態及びその目的の整合性を考慮しつつ**連携**。	・**情報通信分野及び航空分野**における机上演習に**NISCが参加**し、演習の実施手法等の知見を受けた。

（別紙）

～検証した具体的事例の概要～

ｉ）システム障害（非意図的要因）が発生した事例

（その1）

① 未明から6時間にわたって、利用者に関する情報を管理するシステムに障害が発生。当初は職員が手作業での処理により対応したが、午前 8 時ごろから対応が追い付かなくなり、サービスの停止や遅延が発生。

② システムを復旧させるため、待機系への切り替え等を行い、午後0時頃にシステム復旧。その間、当該事業者のサービス停止や遅延が発生。システム復旧後も、影響は翌日まで残存。影響を受けた利用者は約7万人。

③ 当該事業者からは後日、所管官庁に原因の報告がなされた。原因は、ハードウェア障害、高負荷状態による通信滞留、プログラムの設定ミスの3種類の障害が、ほぼ同時間帯に発生したことによるものと判明。また、再発防止策として、上記原因に対する技術的対策に加え、監視・運用体制の見直しや利用者への情報提供方法の改善等の管理的側面の対策についても報告。

（その2）

① 早朝、特定分野の16事業者において4378台の業務端末（利用料金清算等に関する端末）が起動しない不具合が発生。不具合の発生は午前4時過ぎに事業者が認知。その後、技術的分析を行いつつ、事態の重大性を判断し、午前5時に対策本部を設置。

② 仮復旧のための方法が確認できたため、当該措置を順次実施し、午前 11 時にはすべての措置を完了。また、一部の事業者においては、利用者の混乱回避のため、当該システム端末を使用せずに利用者へのサービス提供を行う措置を実施。

③ 当日中に原因をほぼ解明。翌日以降、改修ソフトを対象となる全端末にインストールする作業を実施。修正作業が完了するまでの間は、手動による対応を並行して実施。また、HP などにより、事業者から経過や原因など具体的な内容について公表。

④ 3日後に、同様の原因から別の情報処理端末にも不具合が発生。当該端末の製造業者側のチェック漏れにより、不具合発生の可能性についての報告はなかったため、事業者として事前の対応が取れなかったもの。

（その3）

① 特定分野の複数の事業者による特定のサービスにおいて、障害事例が複数回発生。利用者がサービスを利用できないなどの影響が発生。

② それぞれの障害の原因は、サーバ不具合、設備故障、ソフトウェア不具合、保守作業のミス等様々であり、特定の原因によるものではなかった。

③ 障害の発生以降、随時 HP により、復旧状況や原因、再発防止策などに関する情報が公表。

ii）業務システムがウイルス感染した事例

① ホームページの閲覧で職員の端末にコンピュータウイルス（以下、ウイルス）が侵入。侵入したウイルスの感染活動により内部システムの広範にわたり感染が拡大した結果、業務システムに障害が発生し、サービスの継続に一部影響が発生。

② システム障害発覚後、解析により原因がウイルスによるものであることが判明したが、既に多くの端末やシステムへ感染が拡大。

③ ウイルス感染判明後、以下の応急的な措置を実施。翌日には通常体制で業務ができる状態に復旧。

・ネットワークシステムをインターネットから遮断

・業務システムの復旧を最優先し、その後にウイルス駆除を実施

復旧までの間は、未感染端末と手動による運用で対応したが、一部サービスに影響が発生。当該事業者のホームページで情報を掲載し、利用者等への周知等、混乱拡大の防止のための措置を講じた。なお、他の事業者への影響の拡大は確認されていない。

④ ウイルスの特定と駆除方法の特定に数日を要し、対応がほぼ収束するまでには 1 ヶ月以上要した。また、当該事業者においてはウイルス対策ソフトが導入されていたものの、当該ウイルスに対応していなかったため検出できなかったことが判明。

第4章　企業･個人における現状の評価等

第1節　企業･個人分野における情報セキュリティに関する2007年度の取組み

1．2007年度の取組みの背景

(A) 企業

企業は、グローバル社会における経済発展の重要な担い手であり、ITの根幹を担う製品･サービス等を提供する主体でものあるという面からも、各企業の経営判断に基づいた自主的な取組みを前提とした情報セキュリティ対策を実施することが求められる。また、高度にネットワーク化されたIT社会では、局所的な事故･トラブルが社会全体に波及する可能性があること、企業では個人に関する情報等の集積度が高まっていることもあり、社会的責任においても情報セキュリティ対策に積極的に取り組む必要がある。

このような背景の中で、基本計画では2009年度初めには、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とすることを目指し、初年度の取組みである2006年度には企業における情報セキュリティ対策のための体制の構築に特に重点を置いて取組みを行った。その取組みを通じて、情報セキュリティ問題の重大性と対策の必要性を自ら認識し、積極的な情報セキュリティ対策を実施している主体とそうでない主体が存在することについて対応を図ることが、今後の課題となった。このため、基本計画2年目である2007年度は、取組みが遅れがちな主体への対策を中心に置き、情報セキュリティ対策推進の安定化を図るとともに、対策が不十分な部分の底上げを図るための施策の取組みを行った。

(B) 個人

個人においては、現在もインターネット利用者数は増加傾向にある。また、「Web2.0」の概念が広く普及し、ブログ･SNS等の利用者参加型のサービスが普及するなど、その利活用のあり方が多様化し、依存度が増してきている。そのため、個人の情報セキュリティ対策の不備は当該個人だけではなく、社会的に大きな被害を発生させ、ネットワークで繋がっている他の多数の個人等にも被害を及ぼす可能性が増大してきている。個人においても、老若男女を問わず各人がIT社会を構成する一員としての責任を自覚し、一定の自己責任を認識して行動することが期待される。

基本計画では、2009年度初めに「IT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、初年度である2006年度には(1)個人が情報セキュリティ対策を可能な範囲で、自主的に実施することが当たり前のこととして認識できる環境の整備、(2)国民から見てわかりやすい形で多様な広報啓発･情報発信を行うことに特に重点的に取り組んだ。その中で、個人における情報セキュリティ対策の意識の高まりや、知識の浸透がみられ、対策の推進は全般的に進展したと言える。しかしながら、依然として対策を講じていないとする未着手層の存在と、若年層や女性等の特定の属性に属する者の理解度の低さなどが課題であった。2007年度は、これら取組みが遅れがちな主体も含め、全体的な底上げを図るための施策の取組みが行われた。個人においては、属性間での

情報セキュリティに関する理解度の差、ITの仕組みがそもそも理解しがたいという点から、自己責任の限界を補うことが重要であり、情報セキュリティ対策を自律的・継続的に可能な範囲で実施できる環境の整備、国民から見てわかりやすい形で多様な広報啓発・情報発信を引き続き行った。

2．2007年度の取組み

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、以下の施策を推進した。

なお、詳細は別添1参照。

(A) 企業

(ア)企業の情報セキュリティ対策が市場評価につながる環境の整備

企業における情報セキュリティガバナンス確立の促進として、(1) 情報セキュリティ対策に係るベストプラクティス(模範)を普及させるための方策、(2) 情報セキュリティ格付けの促進のための方策、の検討に資する調査研究を実施した。

情報セキュリティガバナンスの確立における各企業の情報システムの信頼性向上のため「情報システムの信頼性向上に関するガイドライン」の遵守度合いを評価する指標(試行版)を公表、これに基づく「情報システムの信頼性向上のための緊急点検」を平成19年6月に実施し、これを受けて信頼性ガイドライン及び評価指標の見直しと評価ツールの構築に着手した。

また、電気通信事業分野においては、電気通信事業者の情報セキュリティマネジメントの強化に向けて、業界ガイドラインである「電気通信事業における情報セキュリティマネジメントガイドライン(ISM－TG)」をITU(国際電気連合)に提案し、平成20年2月に勧告化が決定した。また、同勧告についてISO／IEC(国際標準化機構／国際電気標準会議)においても国際標準規格化すべく最終投票準備が開始された。国内においては、これら国際標準化の進捗動向を踏まえつつ、認証のあり方についての検討を開始した。

情報サービス提供者の情報セキュリティ管理を含む情報サービスマネージメントに関する標準規格として、日本工業規格(JIS)として、JISQ20000-1:2007(情報技術サービスマネジメント-第1部:仕様＝ISO/IEC20000-1)、JISQ20000-2:2007(情報技術サービスマネジメント-第2部:実践のための規範＝ISO/IEC20000-2)、を制定した。

さらに、中小企業の対策推進の観点からは、負担の軽減及び対策推進による水準の底上げを目的とする中小企業向け標準フォーマットの策定に資するための現状調査等を実施した。

(イ)質の高い情報セキュリティ関連製品及びサービスの提供促進

企業の情報セキュリティ対策において、リスクに応じて、理解のしやすい形で必要な対策を選択できる環境整備のため、情報セキュリティ対策によるリスクの変動を定量的に把握する手法に係る調査研究を実施した。また、オフショア・アウトソーシングに関連する固有のリスクについても検討を行うために、オフショア・アウトソーシングの現状等に係る調査研究を実施した。

質の高い情報セキュリティ関連製品及びサービス提供の促進へ向け、ISMS適合性評価、ITセキュリティ評価及び認証制度、情報セキュリティ監査といった第三者評価の活用を促すために、各種セミナーを通した監査制度の普及活動や、今後、監査人が一定の保証を行う保証型情報セキュリティ監査の検討を継続的に実施した。

情報セキュリティ関連製品等の普及促進の取組みとしては、認証製品の活用可否を確認する際の検討支援ツールを独立行政法人情報処理推進機構が開発した。

さらに質の高い情報セキュリティ関連製品を活用する企業に対し、その投資を加速するための、(1)ISO/IEC 15408の評価・認証を受けた一部製品を購入した事業者について、取得価額の一定割合で税額控除等を行う「情報基盤強化税制」、(2)ネットワークセキュリティ維持装置(多機能型ファイアウォール装置等)を購入した場合に、固定資産税の課税標準が圧縮される「ネットワークセキュリティ維持税制(地方税)」、などの優遇措置を実施した。

(ウ)企業における情報セキュリティ人材の確保・育成

情報セキュリティ人材の確保・育成の取組みとして「情報通信人材研修事業支援制度」による情報通信セキュリティ人材育成のための研修事業への助成金の交付を実施した。

また、組織トップの情報セキュリティの理解普及へ向け、IT利用者の情報セキュリティを客観的に測定するためのセルフチェックツールを組織管理者向けに機能を拡張するなど取組みを実施した。

人材育成手法の検討の取組みとして、客観的な人材評価メカニズムの構築へ向け、産業構造審議会情報経済分科会情報サービス・ソフトウェア小委員会人材育成ワーキンググループ報告書(平成19年7月20日)を受け、高度IT人材に求められるスキルについて引き続き検討を行った。また、産学連携人材育成パートナーシップの下、情報処理分科会を設置し、産業界が求める情報セキュリティ分野を含む、高度IT人材像や産業界における実践的な高度IT人材育成方法の検討を実施した。

さらに、情報通信分野セキュリティを含む人材の育成に向け、ICTマネージメント分野の実践的なPBL(Project Based Learning)教材を開発した。

試験制度面では、情報セキュリティ分野を含めた各情報分野の人材スキルを測る情報処理技術者試験制度で、情報処理技術者試験規則等の一部改正し、平成21年度から新試験を実施する。

中小企業の対策推進の観点では、中小企業における経営者、情報システム担当者などによる情報セキュリティへの理解を深めるため独立行政法人情報処理推進機構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について、全国31箇所で開催した。

(エ)コンピュータウィルスや脆弱性等に早期に対応するための体制の強化

コンピュータウィルスや脆弱性等に早期に対応するための情報関連事業者等の連携対応体制、情報共有体制強化として、情報セキュリティ早期警戒パートナーシップガイドライン等の関連ガイドラインを改定・公開（重要インフラへの優先的な情報提供等）を行い、サイトによる早期警戒情報の提供等を開始した。

組織の緊急対応チームの間の連携強化に向け、早期警戒情報の共有ツールの稼働を開始し、重要インフラ10分野中8分野を含む諸団体が利用し、チーム間連携の基礎を構築した。

また、脆弱性情報についての深刻度をより国際的に整合化された基準の下で定量的に比較し、対策の重要性・優先度の判断が行えるよう、独立行政法人情報処理推進機構において、共通脆弱性評価システムをバージョン2へ移行するとともに、JPCERTコーディネーションセンターが、脆弱性の優先度判定のためのシステムを公開した。

更に、Webサイトの安全性の確保へ向け、発注者がWebアプリケーション構築の際に、開発者（受注者）へ示すべきセキュリティ要件に関するガイドラインを独立行政法人情報処理推進機構のホームページで公表した。

(B)個人

(ア)情報セキュリティ教育の強化・推進

小中高等学校における情報セキュリティ教育を推進するための取組みとして、1）情報セキュリティを含む情報モラル等の効果的な指導手法について指導事例等を掲載する教員向けWebサイトの作成、2）各都道府県における市区町村教育委員会指導主事等を対象とした情報モラル指導セミナーの開催などを行った。

情報セキュリティ教育の推進の度合いを測る指標として、教員のICT活用指導力のチェックリストの中に、「児童生徒に対して情報セキュリティを指導する能力」を位置づけ、全国の実態調査を実施した。

また、子どものインターネット、携帯電話等のICTメディアの健全な利用のためのICTメディアリテラシー育成プログラムを公開し、必要な更新を行う等、ICTメディアリテラシー育成を行う団体等に広く普及を図った。

さらに、小中高等学校の児童・生徒の情報セキュリティ意識の普及啓発へ向け、独立行政法人情報処理推進機構が、全国の小学生・中学生・高校生を対象としてに

「情報セキュリティ標語・ポスター」の募集・入選作品の公表を行った。

世代横断的な情報セキュリティ教育の推進への取組みとしては、その内容の充実・強化を図りつつ、「インターネット安全教室」や「e－ネットキャラバン」、「サイバーセキュリティ・カレッジ」の実施を継続して全国各地で開催し情報セキュリティに関する普及・啓発を推進した。

(イ)広報啓発・情報発信の強化・推進

広報啓発・情報発信の強化・推進として、政府機関Webサイト「*@police*」（警察庁）、「国民のための情報セキュリティサイト」（総務省）による情報セキュリティに関する注意喚起等の広報啓発を引き続き実施した。また、一般利用者に情報セキュリティの確保に必要な正しい知識と対策を広めることを目的とした「インターネット美化運動2007」、「CHECK　PC！キャンペーン」を実施し、国民に情報セキュリティ対策の重要性を訴える活動を昨年に続き実施した。

フィッシングや不正アクセス等の具体的脅威に関する普及啓発については、「迷惑メールへの対応の在り方に関する研究会」におけるフィッシングメール対策に関する検討や、不正アクセス行為の発生状況及びアクセス制御機能に関する研究開発の状況の公表を行った。また、独立行政法人情報処理推進機構やJPCERTコーディネーションセンターによる、不正アクセス対策、コンピュータウィルス対策等についての啓発活動を実施した。

さらに、その他、電波利用秩序の維持のための啓発活動等、ホームページやメールマガジン等の各種手段を用いた情報セキュリティに関する広報啓発・情報発信活動を推進した。

「情報セキュリティの日」（毎年2月2日）に伴う広報啓発活動については、各種関連行事の開催（今年度は593件開催）、「情報セキュリティの日」功労者表彰を実施した。さらに、情報化月間における期間集中的な広報啓発・情報発信の取組みとして、「情報化促進貢献表彰（情報セキュリティ促進部門）」を実施した。

我が国の情報セキュリティ戦略の国内外への発信として、基本計画、SJ2006、政府機関統一基準等を英訳し、NISCの英語版ウェブサイトに掲載している。

(ウ)個人が負担感なく情報関連製品・サービスを利用できる環境整備

サイバー攻撃停止に向け、ボットプログラムの感染を防ぐ対策、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についての検討を実施した。

また、IPv6によるユビキタス環境構築に向け、少数かつ特定の利用者が存在する利用環境モデル（小規模オフィス環境等）での実証実験を実施した。

無線LAN利用に関するガイドライン「安心して無線LANを利用するために」を改定し、その普及の推進を図った。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」の冊子を改訂し、無線LANの安全な使い方に関するコンテンツの充実を図った。

第2節　2007年度の取組み及び取組みを受けた企業・個人分野における現状の評価等（2007年度の評価等）

1．2007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大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（以下「指標」という。）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ことが必要である。

なお、評価等に際しては、これらの指標の測定時点・測定方法によっては必ずしも対象の状態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が必要である。

2．評価等について（評価指標等）

(1) 2007年度の評価等について

(A) 総論

① 指標の分類

企業・個人に係る指標は、「アウトプット指標」と「アウトカム指標」に分けて考えることとする。

なお、これらの指標については、政府、重要インフラに係る取組み、その他多様な要因の影響を受ける可能性が高いため、企業・個人に係る取組みだけによって効果を測定するために活用するのではなく、他の主体に係る取組みも含め総合的な視点から活用していくことが望ましい。

② 指標のソースと留意点

企業・個人に係る指標は、巨大な母集団が対象であること、調査の各主体への負担をなるべく軽減すべきであることといった観点から、状況把握に有益な既存のデータ（政府、公的機関等の保有する統計や実態調査結果のうち、内閣官房において、我が国の企業・個人における情報セキュリティの状況把握に有益と判断したデータを指す。）の活用を原則とする。ただし、このデータは固定的なものではなく、今後定期的に、指標自体の見直しと合わせて、見直しを行っていくこととする。

③ 留意事項

今回活用する既存のデータについては、調査目的、調査方法、調査母集団、サンプル抽出手法及び調査時期がそれぞれ異なる、それぞれの統計と調査の質に幅があるなどの留意点がある。また、評価等に際しては、これらの指標の測定時点・測定方法によっては必ずしも対象の状態を適切に把握できない場合がある。評価等に際して

は、こうしたことに留意し、場合によってはこれらの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が必要である。

特に、測定時点については、基本計画の対象期間前である2006年度以前の資料しか得られないデータも散見されるところであり、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2006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、2007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。

④ 政府機関の状況との対比と補完調査について

「情報セキュリティ政策の枠組み文書」においては、政府機関の情報セキュリティ対策は、企業・個人の情報セキュリティ対策の模範となることが期待されている。したがって、政府機関自体の状況について、個人の対策実施領域の指標との対比の観点からも把握することが重要であり、既存の調査結果等から政府機関について必要なデータを得られない場合には、内閣官房は各府省庁の協力を得て必要な調査を行うこととされている[11]。

これを受けて、2007年度は、企業・個人の対策を推進する環境の現況について、政府機関と関わる側面から焦点を当てた補完調査を行う。

具体的には、第一に、電子政府の利用、活用、運用の状況に関して、政府機関と企業等との情報セキュリティに係る現況を比較できるようにすることで企業等における対策推進に貢献させる観点から、電子システムに係るトラブルの発生状況について比較調査を行う。

第二に、調達及び外部委託について調査を行う。当該調査は、SJ2007において示されているように、政府機関が企業・個人から製品・サービスを調達し、また、企業・個人へ外部委託する際の情報セキュリティの観点からの取組みの進展を把握することで、企業・個人分野の対策をさらに進めるために必要な要点を効率的に浮き出させることを狙いとするものである。

(B) アウトプット指標

「アウトプット指標」とは、行政活動により提供されたモノやサービスの量等対策の浸透度を計るものであり、企業・個人を支援する政府の施策の取組み結果を見るものとして活用できる。具体的には、基本計画に記載された政策毎に、別添7の指標をアウトプット指標として活用する。

(C) アウトカム指標

「アウトカム指標」とは、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何らかの効果を計るものであるが、ここでは、企業・個人全体の傾向を分析するという観点から、別添6の指標を活用して企業・個人全体の意識、対策、被害を見ることとし、施策の取組みによりどのような社会的変化が生じたかを見ることとする。

---

[11] 参照「情報セキュリティ政策の枠組み文書」

なお、アウトカム指標については、政策と指標との関係が一対一に定まるものではなく、複数の政策の効果が一つの指標に現れ、あるいは、一つの政策の効果が複数の指標に現れるということが通常であること、被害については、企業と個人との間で指標を明確に分けられないものも存在することに留意する必要がある。

(2) 2008年度以降の評価等について

企業・個人分野においては、原則として2008年度以降においても、2007年度に活用する指標を活用して評価等を行うことになる。ただし、2008年度以降についても前年度までを対象期間とする資料しか得られないデータが散見される事情は同じであるが、少なくとも2008年度については、基本計画策定2年目の状況を示した2007年度のデータが得られることから、当該データから2008年度の状況を推測する方法も併せて用いることで評価等を実施することとする。また、基本計画の最終年度として、2008年度に得られるデータの中から、基本計画に掲げた目標の到達度を測る視点を考慮しつつ評価を行う。

(3) その他

企業・個人分野における現状の評価等に際しては、上記の指標を用いて評価等を実施するほか、SJ2007に盛り込まれた施策の実施状況や各種事例等の内容も加味しつつ、評価等を実施する。

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[12]

(A) 企業

【総評】

各主体の情報セキュリティ意識を高める施策及び各主体が自主的に行う情報セキュリティ対策を支援する環境整備へ向けた当初の施策は、概ね着実に実施された。ただし、情報システムに係る政府調達について、情報セキュリティ対策レベルの評価等を入札条件や落札条件とする方法については、内閣官房において慎重に検討を進めた結果、2007年度においては、内閣官房内での検討の実施にとどまった。今後の方向性について再検討を行う必要があるものと考えられる。

(ア) 企業の情報セキュリティ対策が市場評価に繋がる環境の整備

【指標】

本項目の現状把握に資する既存のデータは存在しない。

【考察】

関係省庁においては、SJ2007に基づき、対策推進が市場評価に繋がるものとして、情報セキュリティガバナンス確立へ向けた施策等を実施してきたところである

[12] なお、各項目の施策の具体的進捗状況については別添1、各指標のデータについては別添7を参照。

が、過去には情報セキュリティ対策がもたらすセキュリティ向上以外の効果に関する認識について、「他に効果がない」と回答した企業の割合が高い傾向もみられている[13]。今後、例えば企業間の取引相手における情報セキュリティ対策の確認状況に関するデータ、事業継続計画の作成状況に関するデータ等の指標の追加を検討し、企業の情報セキュリティ対策と市場評価の関係をより正確に測っていく必要がある。

(イ) 質の高い情報セキュリティ関連製品及びサービスの提供促進

【指標】

○ ISMS[14]認証の取得事業者数(日本情報処理開発協会)

2007年度の1年間の認証取得事業者数は468事業者であった。1年間の認証取得事業者数でみれば、2006年度の528事業者からは若干の減少はあるものの、認証取得事業者数の累計は着実に増加している。

○ IT セキュリティ評価及び認証制度[15]に基づく認証取得製品数(情報処理推進機構)

2007年度の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(新規)は62件であり、2006年度の認証取得製品数(新規)は43件と新規取得製品数は継続して増加傾向にある。

【考察】

指標データの推移の上では、ISMS認証取得事業者数累計及び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は、引き続き増加傾向にある。ISO/IEC 15408 の評価・認証を受けた一部の製品(サーバ用OSやデータベース管理ソフトなど)の購入で税額控除するの優遇措置の実施の取組みをおこなっており、今後もさらに各種普及活動等を積極的に実施し、より質の高い情報セキュリティ関連製品及びサービスの提供が促進されることが求められる。

(ウ) 企業における情報セキュリティ人材の確保・育成

【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)

2007年度の情報セキュリティセミナー開催状況は全国31ヶ所で、96回実

---

[13] 経済産業省 「平成18年情報処理実態調査結果報告書」参照。情報セキュリティ対策全般のセキュリティ向上以外の効果の状況をみると、「他に効果がない」と回答した企業の割合が最も高く、50.1%と約半数であった。また、これについで、「業務効率や生産性の向上」が 21.1%、「顧客・取引先からの評価の向上」が 15.5%であった。

[14] ISMS(情報セキュリティマネジメントシステム)とは、情報セキュリティの個別の問題毎の技術対策の他に、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。

[15] ITセキュリティ評価及び認証制度とは、IT製品・システムについて、そのセキュリティ機能や目標とするセキュリティ保障レベルを、情報セキュリティの国際標準に基づいて第三者が評価し、結果を公的に検証し、公開する制度のこと。なお、「保証継続」とは、既に認証を受けている製品について、バージョンアップ等の軽微な変更の場合に認証の継続を与える制度。

施しており、のべ参加者は8，020名となり、昨年度(6，947名)に比して約15%増となっている。

○ **情報セキュリティアドミニストレータ[16]試験合格者数（情報処理推進機構）**

2005年度の情報セキュリティアドミニストレータ試験の合格者は、3，812人、2006年度は3，337人であった。2007年度について見ると、2，807人である。ここ2年について情報セキュリティアドミニストレータ試験合格者数でみると、受験者数、合格者数ともに減少傾向にあるが、平成18年度春期より、テクニカルエンジニア（情報セキュリティ）試験が創設され、こちらの合格者については、2006年度は1，227人、2007年度については1，788人となっている。

【考察】

情報セキュリティセミナーをはじめとする教育・普及啓発活動は開催数を拡大するなど、着実に人材育成へ向けた積極的な取組みが行われている。

情報セキュリティアドミニストレータ試験合格者数は、ここ2年間で減少傾向にあるが、情報セキュリティに関する資格の多様化とともに、全体としては情報セキュリティに係る人材は増加傾向にある。課題は依然として様々に存するものの、情報セキュリティ人材の確保・育成の重要性の認識促進、人材確保へ向けた各主体の取組みが、少しずつ進んではいると推察される。

（エ） コンピュータ・ウイルスや脆弱性等に早期に対応するための体制の強化

【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）**

JPCERT／CCと連携している国内CSIRTの数は、2005年3月末の時点で8チーム、2006年2月の時点で13チーム、2007年度においては、16となっている。

○ **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）**

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は、2005年3月末の時点で122か所、2006年2月の時点で182である。2007年年度末時点では233となっている。

【考察】

施策の進捗状況及び指標の推移では、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及びコンピュータ・ウイルスや脆弱性等に早期に対応するための体制は徐々に強化されつつあると考えられる。

---

[16] 「情報セキュリティアドミニストレータ」とは、情報セキュリティに関する基本的な知識を持ち、企業をはじめとする各組織において、情報システムのセキュリティポリシの策定及びその実施、分析、見直しを行う者のことである。

(B) 個人

【総評】

各主体の情報セキュリティ意識の向上及び各主体が自主的に行う情報セキュリティ対策を支援する環境整備へ向け、SJ2007に掲げられたた施策が推進された。施策の推進に当たっては、(1)個人が「対策を可能な範囲で自主的に実施すること」を当たり前のこととして認識できる環境の整備、(2)国民から見てわかりやすい形で多様な広報啓発・情報発信を行うことに重点を置いて取組みがなされた。

(ア) 情報セキュリティ教育の強化・推進

【指標】

○ 情報セキュリティに関する指導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)

公立小中高等学校等において、情報セキュリティに関する指導力を有すると回答した教員の割合は、小学校においては6割以上、中学校・高等学校においては5割以上となっている。(詳細は別添7参照)。

○ インターネット安全教室参加者数(概数)(経済産業省)

幅広い世代を受講対象者とするインターネット安全教室の参加者は、参加者は約6,700名であり、2005年度(5,844名)と比較して増加傾向にある。

また、開催箇所が昨年度は98ヶ所であったのに対して、2007年度は全国130ヶ所で開催となり、実施規模の拡大を図るなど積極的な取組みが行われている。

○ e-ネットキャラバン参加者数(概数)(総務省・文部科学省)

児童・生徒を保護・教育する立場にある「保護者」及び「教職員」を対象に、インターネットの安心・安全利用に向けた啓発のためのガイダンスを行うことを目的とし、2005年11月から2006年3月まで、試行実施として計71回の講座(約8,800名が受講)を開催した。2006年度からは全国規模での本格実施を開始し、2006年度は計453件開催(約49,000名が受講)し、2007年度は、計1,089件開催(約120,000名が受講)している。

【考察】

情報セキュリティに関する指導力に関しては、公立小中高等学校等において、ほぼ半数以上の教員が有すると回答しているが、今後も教員のICT活用指導力の向上が児童生徒の情報セキュリティに対する意識向上の鍵となるため、引き続き、その指導力の向上へ向けた取組みが求められる。具体的には、平成19年度に作成した教員向けWebサイトの全国的な普及や教員のICT活用指導力の実態に関する調査・公表、教員のICT活用指導力の向上に関する実践的な調査研究等の継続的な取組みが期待される。併せて、児童・生徒の保護者及び教職員を対象とする e-ネットキャラバンは、教職員の指導力の向上に資するだけでなく、保護者に対する情報モラルの啓発にも資するものであるため、学校・家庭の両面でイ

ンターネットのトラブルから子どもを守るための取組みとして2008年度も引き続き着実な普及を図ることが求められる。

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2007年度も引き続き着実な推進、開催規模の拡大がみられ、今後も継続的な推進、内容の拡充が求められる。

（イ） 広報啓発・情報発信の強化・推進

【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（内閣官房、警察庁、総務省、経済産業省）

2007年度若しくは2007年における、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は、内閣官房情報セキュリティセンターのホームページが421,570人（2007年）、警察庁の「サイバー犯罪対策」のページが206,399人（2007年度）、「@police」が1,469,025人（2007年）、総務省の「国民のための情報セキュリティサイト」が266,904件（2007年）、経済産業省の「情報セキュリティに関する政策・緊急情報」が129,709人（2007年度）、「CHECKPC！キャンペーンホームページ」が1,174,617件（2007年1月16日～3月31日）、情報処理推進機構（IPA）のIPAセキュリティセンターホームページが26,924,532件（2007年度）であった[17]。

○ 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）

2007年度の調査結果によると、情報セキュリティ脅威に関する情報の入手では、定期的に実施しているが17.6%（2006年度調査37.7%）、不定期に入手が48.3%(2006年度調査42.3%)となっており、定期・不定期を合わせると6割以上が情報の入手を行っている。

また、情報の入手先としては、Web（ニュース配信サイト等）が73.7%（2006年度調査70.8%）と最も高く、次いでセキュリティ対策ソフトの会社からが51.0%(2006年度調査57.7%)となっている。その他、テレビ・ラジオが30.5%(2006年度調査25.4%)、ISPからのお知らせが22.9%（2006年度調査39.1%）、新聞が20.6%(2006年度調査20.8%)、雑誌・広告が15.7%(2006年度調査17.5%)、会社の担当部署や知人からが11.1%(2006年度調査11.2%)、Web（政府、地方公共団体）が6.5%(2006年度調査6.6%)と続いている。

情報セキュリティ対策に関する情報の入手では、定期的に入手しているが19.9%(2006年度調査38.7%)、不定期に入手が49.5%(2006年度調査44.2%)となっており、定期・不定期を合わせると7割近くが情報の入手を行っている。

[17] なお、アクセス状況の集計方法は、各省庁によって異なるため、一概に比較することはできない。

また、情報の入手先としては、Web（ニュース配信サイト等）が67．4%(2006年度調査66．3%)と最も高く、次いでセキュリティ対策ソフトの会社からが54．1%（2006年度調査57．5%）となっている。その他、ISPからのお知らせ（Web・メール）が23．7%（2006年度調査39．4%）、テレビ・ラジオが21．4%（2006年度調査19．9%）、職場、学校、知人からが15．6%(2006年度調査12．5%)、新聞が14．5%(2006年度調査16．2%)、雑誌・広告が13．6%(2006年度調査16．8%)、Web（政府、地方公共団体）が6．0%(2006年度調査6．8%)と続いている。

○ 情報の入手経路（情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構）

情報の入手経路として、セキュリティ対策ソフトメーカのウェブサイトやメールマガジン等、パソコンメーカやプロバイダ等のウェブサイト・メールマガジン等、テレビＣＭ、雑誌や専門書、新聞、家族・友人・知人の話が多く、それぞれ３割台を数えている。情報について、「見聞きしたことはない」と回答する割合は６．７％であり、なんらかの方法で情報を入手して割合は高いと言える。

なお、世代別に見ると、１０代（１５～１９歳）では「見聞きしたことはない」と回答している割合が１５．７％と他の年代と比べて相対的に高くなっている。

○ 希望する情報提供方法（情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構）

希望する情報提供方法は、「ポータルサイトの目立つ場所」が52．7%、「ウェブ上のニュース」が44．6%と割合が高い。つまり、ウェブの活用、分かり易い場所、ある程度速報性をもったものを希望する割合が高いと言えよう。その他は、テレビのニュース・情報番組での解説コーナー、テレビCM等が2割後半で続く。

また、「特に情報を得たいとは思わない」とする割合は、5．4%となっており、多くが何らかの形での情報入手を希望している。世代別で見ると、10代（15～19歳）では「特に情報を得たいとは思わない」とする割合が11．5%と、他の世代の4．4～5．6%と比して高い状況にある。

【考察】

広報啓発・情報発信は、個人が情報セキュリティ対策を可能な範囲で自主的に実施することを当たり前のこととして認識するためにも、重要施策として位置づけられるものであり、SJ2007の下でも、引き続き、ウェブを中心とした広報啓発・情報発信を行い、加えてテレビ等のメディアの活用を行った。今後も「希望する情報提供方法」として、ウェブ及びテレビを経由した情報の入手の割合が高いこともあり、更に提供のあり方・内容の改善を図りつつ、ウェブやテレビ等による積極的な情報提供が今後も有効であると言える。

他方、「特に情報を入手していない」、「特に情報を得たいとは思わない」と回答し

た割合が高い世代もあり、全体的な底上げの観点からは、これらの世代への広報啓発・情報発信のあり方に留意した取組みが重要となってくると考えられる。

(オ) 個人が負担感なく情報関連製品・サービスを利用できる環境整備

【指標】

○ 無線LAN機器のセキュリティ対策の必要性に関する周知状況(インターネットの利用実態に関する調査:総務省)

2007年度の調査結果によると、無線LANセキュリティ対策の重要性の認知度では、「重要性を知らない」とする割合が42.5%(2006年度調査33.7%)であった。また、重要性について、どこで知り得たかについては、「製品パッケージ、取扱説明書等の記載を見て」が20.1%(2006年度調査24.9%)、「知人等から知らされた」が17.7%(2006年度調査13.0%)、「専門誌等を見て」が17.3%(2006年度調査26.9%)と高い割合になっている。その他、「製品購入時に定員から説明をうけた」3.9%(2006年度調査4.0%)、「ISP等から説明を受けた」3.7%(2006年度調査6.3%)、「ISP等のHPを見て」7.3%(2006年度調査13.1%)となっている。

【考察】

無線LAN利用では、発生し得る脅威を認識し、適切な対策を利用環境に応じて行うことが重要である。重要性の周知の状況については、4割以上が「重要性を知らない」としており、脅威の認識を含めた適切な対策方法について普及啓発を行うことが重要である。また、重要性を知り得た先としては、専門誌や製品パッケージ、取扱説明書との割合が高いことから、対策の重要性を認識しているのはある程度IT利用について知識を有する個人が中心であると推測される。無線LANは、利便性や低価格化等により、今後も利用が進むと考えられ、幅広い層の一般利用者に向けた普及啓発が一層求められる。

(2) 施策の取組みによる社会的変化に関する評価等[18]

(A) 企業

(ア) 企業の情報セキュリティ意識に係る指標

【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、コンピュータウイルス、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)

情報セキュリティ上のトラブルの中では、重要情報の漏えいについて「非常に重要である」と答える割合が最も高く(82.5%)、依然として重要情報漏えいが発生することから、認識が高いということが見てとれる。重要情報漏えいについては、「ウイルス、ファイル共有ソフトに起因する情報漏えいの重要性の認識」が

[18] 各指標のデータについては別添7を参照。

最も高く、同レベルで「内部者による情報漏えい」が続いている。また、18年調査では、「システムトラブルを非常に重要である」とする割合は70．2%と、17年調査の56．4%と比して高くなっており、「わからない」とする割合が17．8%から3．8%へ減少するなど、システムトラブルについての重要性の認識の高まりがみられる。

コンピュータウイルスに関する重要性の認識も68．2%と依然として高く、17年調査の59．6%から増加している。ウイルスやワームの感染、スパムメール中継利用等は減少傾向にあるも、トロイの木馬の重要性の認識が高まっている。不正アクセスへの認識も、66．0%と同レベルで高い。不正アクセスとしては、内部者の不正アクセスの重要性が最も高く、73．5%で17年調査58．5%から大きく増加している。続いて、IP・メールアドレスの詐称62．7%、リソースの不正使用61．8%となっている。

【考察】

これらの数値は、2005年度の調査結果であるが、全体の意識レベルは、徐々に高くなる傾向がみられる。

情報セキュリティ対策全般のセキュリティ向上に関する効果の認識[19]は、組織的対策の実施については77．2%、技術的対策　86．5%、監視体制　82．8%、評価の実施　81．2%となっているが、セキュリティ向上以外の効果[20]については、特に効果がなかったとする企業が50．1%で約半数、これについで、業務効率や生産性の向上」が21．1%、顧客・取引先からの評価の向上が15.5%である。

対策の効果については、組織的対策の実施について3割近くが「効果がない」又は「良くわからない」としており、対策効果の認識を含めた情報セキュリティ対策の意識の向上を継続的に図るための施策が必要となってくる。

(イ) 企業の情報セキュリティ対策状況に係る指標

① 情報セキュリティ対策の確立状況

【指標】

○ リスク分析の実施状況・情報セキュリティポリシーの策定状況・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）

2005年度の時点で、29．7%の企業が既にリスク分析を実施し（2004年度は30．6%、2003年度は20．4%）、43．5パーセントの企業が、既に情報セキュリティポリシーを策定している（2004年度は43．9%、2003年度は29．7%）。既に全社的なセキュリティ管理者を配置している企業の割合は、44．1%（2004年度は47．1%、2003年度は35．2%）、部門ごとのセキュリティ管理者の配置は、32．1%（2004年度は34．1%、2003年度は24．

[19] 経済産業省 「平成18年情報処理実態調査結果報告書」 情報セキュリティ対策について効果があった企業の割合の推移より

[20] 経済産業省 「平成18年情報処理実態調査結果報告書」 情報セキュリティ対策全般のセキュリティ向上以外の効果の状況（平成17年度）より

4%)となっている。

また、それぞれについて必要性を感じていない企業の割合は、2005年度の時点でリスク分析が12．5%(2004年度は8．7%、2003年度は11．1%)、情報セキュリティポリシーの策定が9．6%(2004年度は6．6%、2003年度は8．9%)であった。全社的なセキュリティ管理者の配置は9．5%(2004年度は5．7%、2003年度は7．3%)、部門ごとのセキュリティ管理者の配置は、16．1%(2004年度は11．8%、2003年度は13．0%)であった。

【考察】

2005年度時点の調査ではあるが、効果について調査したところ、リスク分析については「効果がない」1．7%、「よくわからない」31．8%であった。セキュリティポリシーの策定は「効果がない」3．1%、「よくわからない」29．6%である。全社的なセキュリティ管理者の配置については「効果がない」2．4%、「よくわからない」23．4%、部門ごとのセキュリティ管理者の配置については「効果がない」3．3%、「よくわからない」26．3%となっている。「既に実施」又は「実施を検討している」企業で、その2割から3割がその効果について、「効果がない」又は「わからない」としている。

対策実施状況は若干の減少傾向がみられるものの、同等のレベルで推移しており、今後、情報セキュリティ対策の更なる実施と定着を進めて行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、対策実施者において取組むことが「得である」と認識されるような環境を整備していくことが必要であると考えられる。

② 情報セキュリティ対策の導入及び運用状況

【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・データの暗号化実施状況・外部接続へのファイアウォールの配置状況・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)

2005年度の時点で、「既に重要なシステムへの内部でのアクセス管理を実施」が59．0%(2004年度は57．9%、2003年度は50．7%)、「既にデータの暗号化(PKIを含む)を実施している」は29．2%(2004年度は27．9%、2003年度は調査未実施)となっている。また、「既に外部接続へのファイアウォールを配置している」が71．3%(2004年度は73．4%、2003年度は66．7%)、「既にセキュリティ監視ソフトを導入している」は54．4%(2004年度は49．1%、2003年度は40．6%)となっている。

これらについて「必要性を感じていない」企業の割合は、重要なシステムへの内部でのアクセス管理が2005年度の時点で8．1%(2004年度は6．9%、2003年度は8．2%)、データの暗号化(PKIを含む)の実施が18．2%(2004年度は15．2%、2003年度は調査未実施)、外部接続へのファイアウォールの配置が8．9%(2004年度は6．4%、2003年度は7．7%)、セキ

ュリティ監視ソフトの導入が9．8％である（2004年度は7．6％、2003年度は8．8％）。

○　重要なシステムへの内部でのアクセス管理の実施状況・データの暗号化実施状況・外部接続へのファイアウォールの配置状況・セキュリティ監視ソフトの導入状況（通信利用動向調査：総務省）

2006年末の時点で、80．9％の企業が「パソコンなどの端末（OS、ソフト等）にウイルスチェックプログラムを導入し、66．1％の企業がサーバにウイルスチェックプログラムを導入」し、51．3％の企業が「ファイアウォールを設置」、51．0％の企業が「ID・パスワードによるアクセス制御を実施」している。「データやネットワークの暗号化を実施」している企業は、13．9％である。

○　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）

2007年調査では、28．4％の企業等が、「情報セキュリティ教育を実施している」（2006年は54．5％、2005年は45．9％）。

他方、「必要性を感じていない」企業等の割合は、2007年調査では18．4％である（2006年は1．5％、2005年度は1．2％）

○　従業員に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）

2005年度の時点で、43．1％の企業が、従業員に対する情報セキュリティ教育を実施している（2004年度は41．1％、2003年度　27．2％）。

他方、「必要性を感じていない」企業の割合は6．6％であった（2004年度は4．6％、2003年度は5．6％）。

○　パッチ[21]適用実施率（コンピュータウイルスに関する被害状況調査：情報処理推進機構）

2006年度の時点でクライアントPCに対して、36．6％の企業が「常に最新状態」にしており（2005年度は32．2％）、29．6％の企業が「定期的に実施している」（2005年度は27．6％）。

他方、「気づいたときに適用」は16．7％（2005年度23．1％）、「ほとんど適用していない」企業は12．9％（2005年度12．4％）、「把握していない」企業が3．5％（2005年度3．0％）であった。

○　ウイルス対策ソフト導入率（コンピュータウイルスに関する被害状況調査：情報処理推進機構）

2006年度の時点で、「所有するパソコンの9割以上にウイルス対策ソフトまたは統合セキュリティ対策ソフトのいずれかを導入している」企業は87．6％であった（ウイルス対策ソフトについて2005年度は82．3％、2004年度は63．9％）。

他方、「半数以上」と回答した企業は3．4％（ウイルス対策ソフトについて2005年度は6．4％、2004年度は9．6％）、「半数未満」が6．1％（ウイルス

[21] セキュリティの脆弱性を除去するプログラムのこと。（IPA「情報セキュリティ読本（改訂版）」

対策ソフトについて2005年度は7．2%、2004年度は15．0%)、「いずれも導入していない」企業は2．4%(ウイルス対策ソフトについて2005年度は3．2%、2004年度は10．4%)であった。

【考察】

ウイルス対策ソフトの導入等の技術的な対策については、徐々に向上しているものの、大きな改善はみられない状況にあると言える。特にクライアントへのパッチ適用率は依然として3割程度にとどまっており、ウイルス対策ソフト導入率の9割に対して、非常に低くなっている。パッチ適用しない場合、OSやアプリケーションの脆弱性を利用した攻撃を許してしまうため、常に最新のパッチを適用することが望ましい。

今後も、各対策毎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。

③ 情報セキュリティ対策の監視及びレビューの状況

【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)

2005年度において、「外部専門家による監査を受けた」企業は11．0%(2004年度は10．6%、2003年度は8．1%)、「内部による監査を受けた」企業は20．3%(2004年度は18．8%、2003年度は12．6%)であった。

【考察】

以上に示した数値は、2005年度までの推移では、外部専門家及び内部による情報セキュリティ監査共に実施する企業は、大きな伸びはみられない状況である。効果の認識については、2割弱が「よくわからない」と回答している。

対策実施者においてその効果が認識されるような環境整備、監査実施等による対策推進やそれによる情報セキュリティ向上が市場評価に繋がる環境の整備が今後も求められる。

(B)個人

(ア) 個人の情報セキュリティ意識に係る指標

【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)

2006年度における、インターネットを利用して感じる不安や不満、利用しない理由の主なものは、「ウイルスの感染が心配である」が最も高く、66．8%、同レベルで「個人情報の保護に不安がある」が66．6%となっている。続いて、「どこまでセキュリティ対策を行えばよいか不明」が57．3%、「電子的決裁の信頼性に不安がある」が39．5%、「セキュリティ脅威が難解で具体的に理解できな

い」が30．8％、「違法・有害情報が氾濫している」が28．2％、「認証技術の信頼性に不安がある」が15．4％、「送信した電子メールが届くかどうかわからない」が7．4％、「知的財産の保護に不安がある」が7．0％となっている。これらは前年と比較し、いずれも増加している。

○ 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）

2007年度調査の結果では、情報セキュリティの脅威について知っているかの問いに、「コンピュータウイルス感染」が95．5％(2006年度調査97．7％)、「スパイウェア」が77．3％(2006年度調査84．8％)、「ボット（ボットネット）」が23．5（2006年度調査26．2％）、「個人情報漏えい」が83．9％（2006年度調査87．6％）、「フィッシング詐欺」が81．4％（2006年度調査83．9％）、「不正アクセス」が73．2％(2006年度調査79．5％)の割合で知っているとしている。「どれも知らない」は2．0％（2006年調査1．3％）となっている。

○ 情報セキュリティに関する言葉の認知度（情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構）

2007年度の調査で、「コンピュータ・ウイルス」（という言葉を聞いたことがある者）は調査対象の97．8％、「セキュリティホール（脆弱性）」が79．4％、「スパムメール」が86．5％、「フィッシング」が87．9％、「スパイウェア」が88．7％である。他方、「ボット」は35．5％、「ワンクリック不正請求」が89．3％、「セキュリティ対策ソフトの押し売り行為」が50．5％であった。年々、情報セキュリティに関する認知度は高くなっている。「ボット」35．5％については、他の項目に対して相対的に低くなっているが、2006年度の15．0％から認知度は高くなっている。

○ 情報セキュリティ対策に関する意識（情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構）

情報セキュリティ対策に関する意識について、必ず必要とする割合は各項目で、「Microsoft Update等によるセキュリティパッチの更新」が58．3％、「セキュリティ対策ソフトの導入・活用」63．9％、「パスワードの定期的な変更」が26．8％、「パスワードを誕生日など推測されやすいものを避けて設定」が60．4％、「怪しいメール・添付ファイルの削除」が76．5％、「電子メールの暗号化ソフト等の利用」が28．7％、「怪しいと思われるウェブサイトにはアクセスしない」が65．6％、「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」が67．9％、「パソコンの重要なデータのアックアップ」が63．1％、「不要になった自宅パソコンの廃棄・リサイクル前のデータ消去」が69．8％となっている。世代別でみると、各項目において必ず必要と回答する割合は10代（15～19歳）が相対的に低い傾向がみられる。

他方、「情報セキュリティに関する被害というと、具体的にどのようなことがおこるかイメージがわかない」に対して、「そう思う」又は「ややそう思う」人が38．9％と高い割合で存在する。また、情報セキュリティに関する情報収集への不満として、「知らない用語が多い」46．6％、「情報が複雑すぎる」42．3％、「内容が

難しい」40．0%となっている（2007年度から調査を実施）。

【考察】

個人の情報セキュリティに関する意識の状況は、言葉の認知度から見ると徐々に高くなっているが、新たな脅威などの用語については、他よりも低くなる傾向がみられる。

セキュリティ対策に関する意識については、セキュリティパッチの更新、セキュリティ対策ソフトの導入・活用等、基本的と思われる対策への意識は改善すべき余地があると考えられる。

世代別に見た対策意識については、若い年代の層で他の年代に比して低い傾向がみられる。また、情報セキュリティ被害について具体的なイメージがわかないとする割合も高いことにも留意する必要がある。

以上の傾向をみると、脅威などの新たな変化を踏まえ、属性（特に若年層）に応じた普及啓発活動を推進することが、全体の底上げの観点からは重要である。また、様々な脅威やその被害のイメージ、対策等について各層がわかり易い形で普及啓発を行っていくことが必要と考えられる。

（イ） 個人の情報セキュリティ対策状況に係る指標

【指標】

○ インターネットのウイルスや不正アクセスへの対応（通信利用動向調査：総務省）

2006年では「何らかのウイルス対策あるいは不正アクセス対策を行っている者」は、インターネット利用者の68．3%である（2005年は57．0%、2004年は59．6%）。

○ 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）

2007年度調査の結果では、「MACアドレスフィルタリングをしている」が14．5%(2006年度調査13．7%)、「SSID隠蔽機能の使用」が11．2%(2006年度調査10．3%)、「暗号化（WEP）」が23．1%(2006年度調査18．5%、「暗号化（WPA／PSK）」が7．5%(2006年度調査6．0%)、「暗号化（WPA2（IEEE802．11i））」が5．9%(2006年度調査4．5%)、「方法はわからないが対策している（初期設定等）」19．1%(2007年度調査から)となっている。他方、「対策をしていない」が19．2%（2006年度調査41．5%）、「わからない」が25．8%(2006年度調査27．5%)となっている。

○ 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新たな脅威に対する意識調査：情報処理推進機構）

2007年度の情報セキュリティ対策の実施状況について、実施しているとする割合は、「Microsoft Update等によるセキュリティパッチの更新」が69．5%、「セキュリティ対策ソフトの導入・活用」75．6%、「パスワードの定期的な変更」が25．1%、「パスワードを誕生日など推測されやすいものを避けて設定」が72．8%、

「怪しい電子メール・添付ファイルの削除」が83．6%、「電子メールの暗号化ソフト等の利用」が29．4%、「怪しいと思われるウェブサイトにはアクセスしない」が75．7%、「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」が78．4%、「パソコンの重要なデータのアックアップ」が48．6%、「不要になった自宅パソコンの廃棄・リサイクル前のデータ消去」が41．7%となっている。世代別でみると、各項目とも10代（15～19歳）の実施割合が相対的に低い。また、性別でみると基本的な対策と考えられる「Microsoft Update等によるセキュリティパッチの更新」は男性80．1%に対して、女性が57．5%、「セキュリティ対策ソフトの導入・活用」では男性が81．2%に対して女性が69．4%と差がみられる。

【考察】

個人の情報セキュリティ対策の実施状況では、「Microsoft Update等によるセキュリティパッチの更新」、「セキュリティ対策ソフトの導入・活用」等の基本的と思われる対策についても未実施とする割合が高く、さらに改善の余地があると考えられる。対策の実施状況では、特に技術的な対策（パッチの更新、セキュリティ対策ソフトの導入・活用）において男女間に実施状況の差が見らる。また、総じて若い世代での対策実施率が低い傾向にあるため、属性（特に若年層、男女間）に応じた普及啓発活動が、全体の底上げの観点からは重要であると考えられる。

無線ＬＡＮ利用における対策は、2割近くが対策を実施しておらず、また、「わからない」を含めると4割以上に上る。無線ＬＡＮ利用において、幅広い一般個人が生じ得る脅威の内容を正しく認識し、対策の内容や方法を理解できる分かりやすい形で普及啓発・情報発信を行うことが求められるものと考えられる。

（C）企業・個人共通

（ウ） インシデント・犯罪の発生面

【指標】

○ 情報セキュリティ上のトラブルの経験（企業）（情報処理実態調査：経済産業省）

2005年度において、企業の経験したトラブルで「コンピュータウイルス」関係のトラブルは63．1%（2004年度は84．4%、2003年度は90．1%）、「不正アクセス」については8．6%（2004年度は14．2%、2003年度は15．3%）となっており、（調査項目の構成が異なるため必ずしも単純に比較はできないが）減少傾向にある。他方、「システムトラブル」は58．7%（2004年度は39．7%、2003年度は40．4%）、「重要情報の漏洩」が26．8%（2004年度は20．4%、2003年度は1．9%）で、いずれも増加傾向にある。

○ インターネットを利用して受けた被害（通信利用動向調査：総務省）

2006年中に、「パソコン又は携帯電話からインターネットを利用した際に何らかの被害を受けた者」の割合は56．9%であった。2004年は40．2%、2003年は56．9%と再び増加に転じている。

○ 過去1年間の情報セキュリティに関する被害状況（不正アクセス行為対策等の実態調査：警察庁）

2007年の調査では、企業等が経験する被害では、最も割合が高いもので「ウィルス等の感染」が9．3%となっている（2006年は24．1%、2005年は32．8%）。次いで、「スパイウェアの感染」が2．3%（2006年は6．8%、2005年は8．3%）、「ファイル共有ソフト利用に伴う情報漏洩」が1．7%(2006年は2．1%（2006年より調査））、内部者のネットワーク悪用」が1．3%（2006年は3．5%、2005年は2．3%）となっている。

○ 不正アクセス行為の発生状況（警察庁）

2007年中の不正アクセス行為の認知件数は1，818件であり、前年と比べ、872件増加した（2006年は946件、2005年は592件）。

○ コンピュータウイルス、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）

2007年の届出件数は、コンピュータウイルスが34，334件（2006年は44，840件、2005年は54，174件）、不正アクセスが218件（2006年は331件、2005年は515件）、脆弱性に関する情報が572件（2006年は593件、2005年は401件）であった。

○ 情報セキュリティ被害経験（個人）（情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構）

2007年中において、「全く知らない差出人から大量にメールが送られてきた」が24．5%と最も高く、次いで「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）ことがある」と回答した者は17．3%となっている。

○ コンピュータウイルス遭遇率（企業）（コンピュータウイルスに関する被害状況調査：情報処理推進機構）

2006年において、61．0%の企業が「コンピュータウイルスに遭遇（感染又は発見）」した（2005年は65．5%、2004年は58．8%）。

○ スパイウェア遭遇率（企業）（コンピュータウイルスに関する被害状況調査：情報処理推進機構）

2006年において、27．0%の企業が「スパイウェア」を発見、「情報流出」などを確認した割合は0．3%となっている（2005年調査の「スパイウェアの侵入を受けた、スパイウェアが実行された」又は「スパイウェアを発見したが、侵入や実行には至らなかった」の割合は31．8%）。

【考察】

企業分野での被害については、ウイルスやワーム感染の被害等、減少傾向を示しており、ウイルス対策等の浸透がうかがえる。システムトラブルについては高い割合の企業が経験している結果であった。重要情報の漏えいについては、ノートパソコン及び携帯記憶媒体等の盗難・紛失が22．9%と高い割合で経験している。ついで、コンピュータウイルス、ファイル共有ソフトに起因する情報漏えいが3．3%と

なっている。

個人分野における被害については、調査対象母数に違いがあるが、2006年は、2005年から増加に転じている。

被害については、被害を受けても気付かない場合、ウイルス対策ソフト等で検出できず認知できない場合もあるので留意が必要である。特に現在はボット感染等、被害を受けていることを認知しづらい脅威もあり、今後はこのような脅威などの新たな変化を踏まえつつ、意識向上、対策推進のための取組みを行い、被害状況の推移を注視していく必要がある。

(エ) (参考) IT を活用した経済の発展状況

【指標】

○ 企業間 (BtoB) 電子商取引の現場 (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)

2006年度調査での我が国の企業間における電子商取引 (2006年1月から12月) について見ると、インターネットによる商取引の市場規模は148兆円 (米国は95兆円)、インターネット以外の専用線などによるコンピュータ・ネットワークシステムを介した商取引も含む市場規模は231兆円である (米国は196兆円)。これを電子商取引化率で見ると、前者が12.6% (米国は4.4%)、後者が19.8% (米国は9.3%) である。

○ 消費者向け (BtoC) 電子商取引の現場 (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)

我が国における消費者向け電子商取引市場規模は4.4兆円であり (米国は19.3兆円)、電子商取引化率は2.03% (米国は4.37%) である。

【考察】

我が国における電子商取引市場は企業間、消費者向けともに拡大している。米国と比較すると、企業間取引については米国より先行しているものの、消費者向け取引は米国の規模に大きく及ばない状況にある。

我が国の状況は、IT利用者の立場から見ると、個人分野では、個人情報の保護についての不安や、電子的決済手段の信頼性への不安等、インターネット利用への不安は依然として減少していない。情報セキュリティの向上は今後の電子商取引市場規模の拡大に不可欠であり、今後も各主体のセキュリティに関する意識の向上や、不安の払拭へ向けた取組みが重要であると言える。

(3) 補完調査の結果について

(ア) 補完調査項目及び調査方法

2007年度の企業・個人対策の補完調査は、企業・個人の対策を推進する環境に係る現況について、政府機関と関わる側面から焦点を当てた調査を実施することとし、以下の3点について調査を行った。

(i)　電子政府の利用、活用、運用の状況に関する情報セキュリティの観点からの調査
(ii)　政府機関が企業・個人から調達する製品・サービスに対する要求水準や選定プロセスの妥当性の確認調査
(iii) 政府機関が企業に外部委託する際の委託先管理の適切性の確認

(i) 電子政府の利用、活用、運用の状況に関する情報セキュリティの観点からの調査については、政府機関と企業等との情報セキュリティの現状を比較できるようにすることで企業等における対策推進に貢献させる観点から、利用者である国民が電子政府のサービスを利用する際のトラブル発生状況について調べた。

(ii) 政府機関が企業・個人から調達する製品・サービスに対する要求水準や選定プロセスの妥当性の確認調査及び(iii)政府機関が企業に外部委託する際の委託先管理の適切性の確認では、政府機関が企業・個人から製品・サービスを調達し、また企業・個人へ外部委託する際の、情報セキュリティの観点からの取組みの進展を把握することで、企業・個人分野の対策をさらに進めるために必要な要点を効率的に浮き出させるための調査を実施した。

情報セキュリティに係るトラブルの経験についての調査

① 調査内容

企業に関しては、「情報処理実態調査」において情報システムに関するトラブルの発生状況が、以下の細目ごとに調査されている（調査結果は、「平成18年情報処理実態調査結果報告書」（平成19年11月13日）として公表）。このため、政府機関の状況との対比を行うことで企業における対策をさらに推進するべく、情報処理実態調査に相当する項目について政府機関の状況を調査した。

（調査項目）

- システムトラブル
  内部要因によるシステムの停止／外部要因（地震、火災等の問題）によるシステムの停止／DoS 攻撃／スパムメールの中継利用等／ホームページやファイル、データの改ざん
- 不正アクセス
  IP・メールアドレス詐称／リソースの不正使用／内部者の不正アクセス
- コンピュータウイルス
  ウイルスなどの感染／トロイの木馬
- 重要情報の漏えい
  コンピュータウイルス、ファイル共有ソフトに起因する情報漏えい／不正アクセスによる情報漏えい／内部者による情報漏えい／委託先による情報漏えい／ノートパソコン及び携帯記憶媒体等の盗難・紛失
- その他
  ホームページ上での誹謗中傷等／その他

今回の補完調査では、これらと同じトラブル分類に従い、2007年度内の経験の「有」、「無」又は「わからない」（有無を把握していない場合）の別を調査した。

② 調査範囲

- 本府省庁かつ情報システム担当部門が把握している範囲
- 対象期間は、平成 19 年 4 月 1 日から平成 20 年 2 月 21 日まで

③ 調査対象

インターネットに接続している情報システム及び電子申請システム等国民に直接にサービスを提供している情報システム

ITセキュリティ評価及び認証制度の活用状況の調査

① 調査内容

情報システムを構成する製品のセキュリティ機能が適切に設計・実装されていることを認証する制度として ISO/IEC 15408 に基づく「ITセキュリティ評価及び認証制度」について、府省庁における本認証制度の活用状況及び活用における課題を調査した。

i 認証取得製品[22]を調達仕様において優先的に扱うこととした案件がある場合、優先的な扱いの具体的内容（「サーバのオペレーティングシステム、プリンタ複合機（情報システムの構成要素として調達するもの）等について認証取得製品を使用する場合に総合評価落札方式の加点要素としている」等）

ii 本制度による認証取得を委託先選定における評価の要素に加えることに関する意見等

② 調査範囲

- 本府省庁かつ情報システム担当部門が把握している範囲
- 対象期間は、平成 19 年 4 月 1 日から平成 20 年 2 月 21 日まで

③ 調査対象

情報システムの構築（新規及び更改）の調達で、予定価格が 10 万 SDR（1,600 万円）以上であって総合評価落札方式によるもの

[22] 本認証については国際的な相互認証制度（CCRA; Common Criteria Recognition Arrangement）が存在すること、及び、認証取得製品に修正を加えた製品は必ずしも認証を取得していると認められないことに留意する必要がある。本留意事項にかんがみ、外部委託における認証取得製品の考慮においては、認証取得として扱う範囲を下記①に限ることなく、②、③及び④も含めることが妥当であると考えられる。
① 「IT セキュリティ評価及び認証制度」に基づく認証を得ている製品
② 日本の制度である「IT セキュリティ評価及び認証制度」と相互認証関係にある外国の制度により認証されている製品
③ 上記①又は②の認証を取得している製品の更新版（修正の適用、バージョン等の更新を含む）
④ 上記①、②又は③の日本語版

ISMS適合性評価制度及び情報セキュリティ対策ベンチマークの活用状況の調査

① 調査内容

企業における情報セキュリティマネジメントシステム（ISMS）の評価に係る制度の導入状況について分析及び評価を行うために、府省庁から企業への外部委託における当該制度の活用状況と、当該活用における課題を把握することを目的とし、「委託先候補におけるISMS適合性評価制度に基づく認証取得」又は「情報セキュリティ対策ベンチマークの結果の活用状況及び活用における課題」を調査した。

i　ISMS適合性評価制度について

- ISMS適合性評価制度に基づく認証取得を委託先選定における評価の要素に含めた案件がある場合、選定における扱いの具体的内容
  - a. 必須の条件としている場合がある
  - b. 総合評価落札方式の加点要素としている場合がある
  - c. その他

    上記 a.及び b.の場合、要求した認証の内容
- 本認証制度を委託先選定における評価の要素に加えることに関する意見等

ii　情報セキュリティ対策ベンチマークについて

- 情報セキュリティ対策ベンチマークを活用した案件がある場合、当該活用の具体的内容
  - a. 応札において結果の提出を求めた場合がある（当該結果の活用方法）
  - b. 提出を受けた結果を委託先の選定に活用した場合がある（その具体的内容）
  - c.その他
- 情報セキュリティ対策ベンチマークを活用することに関する意見等（自由記述）

② 調査範囲

- 本府省庁かつ情報システム担当部門が把握している範囲
- 対象期間は、平成 19 年 4 月 1 日から平成 20 年 2 月 21 日まで

③ 調査対象

情報システムの構築（新規及び更改）の調達で、予定価格が 10 万 SDR（1,600 万円）以上であって総合評価落札方式によるもの

（イ） 補完調査の結果

情報セキュリティに係るトラブルの経験についての調査

調査対象とした19府省庁全てから回答が得られ、調査の結果は、図2のとおりである。また、図2における企業の割合については、「平成18年情報処理実態調査結果報告書」（平成19年11月13日公表）をもとに再編集した。

結果の分析は以下のとおりである。

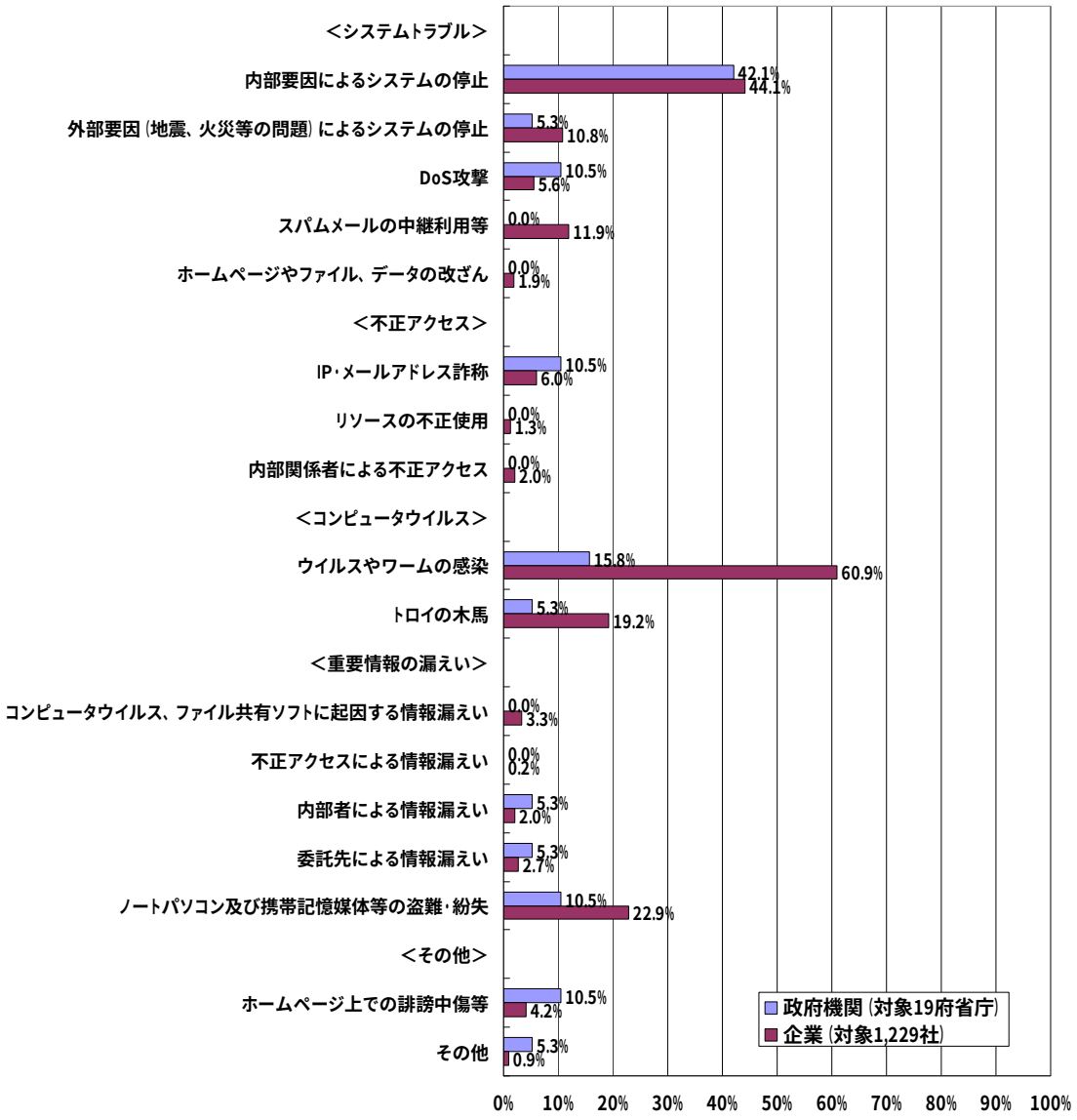


図 2：情報セキュリティに係るトラブルの経験（経験有の割合）

【トラブルの傾向】

企業が経験するトラブルで最も多いのは、ウイルスやワームの感染（60．9%）であり、次いで内部要因によるシステムの停止（44．1%）となっている。政府機関（19府省庁）では、内部要因によるシステムの停止が最も多く（42．1%）、次いで、ウイルスやワームの感染（15．8%）となっている。

【内部要因によるシステムトラブル】

企業・政府機関のいずれにおいても内部要因によるシステムトラブルを多く経験している。今回の調査（企業・政府機関）では、トラブル発生時にシステム冗長化等によりサービスの停止・業務への直接的な影響までは至らなかったケースが含まれる可能性もあるが、企業、政府機関を問わず設計・開発段階におけるシステム品質の確保、或いはシステムトラブルに備えた冗長化等、可用性を高めるための方策が重要となっていると考えられる。

また、各主体が対策を講じる上では、企業及び政府機関の双方がトラブルに関して多くの経験・知見を有しているものと考えられることから、その要因や効果的な事後・事前の対応策について、各主体間で情報共有を図ることを検討することも有効であると考えられる。

【ウイルスやワームの感染】

（調査対象母数に違いがあるため、単純な比較は必ずしも行えないが）企業ではウイルスやワームの感染を多く経験しており政府機関に比して高い割合となっている。先端的企業レベルに達しているかは必ずしも分からないが、政府機関でのウイルス対策ソフトウェアの導入・活用、パッチの定期的更新の徹底などの取組みは一定の効果をあげているものと考えられる。

企業の調査対象には、あらゆる業種・規模の企業が含まれ、その対策レベルには企業間で差があるものと推測されるが、企業全体のレベルを少なくとも政府機関レベルまで底上げするには、依然、対策を推進する余地があると考えられる。

【外部からの脅威などによるトラブル】

企業では、政府機関に比して、ＤｏＳ攻撃やホームページ上での誹謗中傷、ＩＰ・メールアドレス詐称等の外部からの脅威などによるトラブルの経験が低い傾向にある。これは、裏を返すと、政府機関は国家を代表する機関として、攻撃の対象、攻撃ツールとして目をつけられやすいということを表しているものと言える。この観点からは、外部からの脅威などへの対応の必要性は政府機関に比べて低いと考えられるが、近年、経済的利得を目的とした脅威などが増加していることもあり、必要な対策は行う必要がある。

また、ＩＰ・メールアドレスの詐称では、政府機関の名を騙ったメールが第三者から送信されるような事象も含まれている。企業・個人としては、政府機関の対策や注意喚起が行われるものとしても、こうした事象の可能性への留意・対策も必要である。

【重要情報の漏えい】

重要情報の漏えいについては、政府機関・企業の双方において依然として発生しており、今後も継続的な対策が求められるところである。重要情報漏えいの要因としては、ノートパソコン及び携帯記憶媒体等の盗難・紛失が企業・政府機関ともに最も高く、内部者あるいは委託先による重要情報の漏えいもその要因となっている。企業においては、盗難・紛失に続きコンピュータウイルス、ファイル共

有ソフトに起因する情報漏えいが高い割合となっている。

こうしたことから、重要情報漏えいでは人的要因が大きいものと考えられ、情報格付けやそれに基づく情報の適正な取扱いの徹底、組織要員に対する教育・啓発等による情報セキュリティ意識の向上を図ることが重要であると考えられる。

ITセキュリティ評価及び認証制度の活用状況の調査

【現状　－限定的な活用】

ISO/IEC 15408 に基づく「ITセキュリティ評価及び認証制度」について、平成19年度の時点での本認証制度の活用状況は、「必須の条件とする場合がある」、又は「総合評価落札方式において加点要素としている」府省庁は19府省庁中6府省庁であった。

本制度の実際の活用について見ると、全体的には総合評価落札方式における加点要素として考慮するにとどまっていると言える。しかし、個々のシステムで情報セキュリティ対策の要と判断される製品（ファイアウォール、サーバのオペレーティングシステム、暗号化ソフトウェア等）のように、一部では必須の条件とされた例もある。

【活用が限定的となる理由】

「必須条件とする場合、現状では認証製品や対応ベンダーがかなり限られてしまう」といった意見もみられるように、本制度の全面的活用によって対応できる製品が、依然として市場には十分に存在しないという状況にある。また、「手続きが煩雑であること」、「認証取得において、かかる時間とコストが大きい」などとする企業側からの意見も存する。

すなわち、(1)本制度の急激かつ全面的な導入は、調達への参入障壁となるために、調達を行う側、応札する側双方にとって大きなデメリットを生じさせる可能性があり、また、(2)本制度の導入に対応して各製品が認証取得に動くと、取得に係るコストの発生によって製品自体の競争力が削がれる可能性もあると言えよう。このため、本制度の活用が限定的にならざるを得ないと考えられる。

【本制度活用推進の利点と今後のあり方】

他方、本制度による認証取得を委託先選定における評価の要素に加えることに関しては、「厳密な運用がなされる第三者評価による認証制度であり、セキュリティ水準の向上への有効性は高い」とする意見も存在する。また、「今後の活用においては、こうした認証制度等による情報セキュリティ要件の明確化の枠組みのニーズは極めて強い」との意見等もみられ、情報セキュリティ対策の推進及びセキュリティ水準の高い高品質製品の市場への提供という観点からは、利点を生み出す潜在性を有する制度であると言えよう。

したがって、今後は、情報セキュリティ対策の推進にとどまらず、コストや利便性、競争力強化といった様々な観点のバランスをとりながら本制度をより幅広い製品へ適用拡大するべく取組みを推進することが有効であると考えられる。具体的に

は、例えば製品提供企業への普及啓発、認証取得に向けた作業工程の円滑化（評価内容や必要な要件定義を分かりやすい形でブレークダウンするなど）、評価用資料を作成／申請する開発担当者の育成、調達機器の種類などに応じた段階的な制度活用（例：より高水準のセキュリティを求められる製品の調達は速やかに制度活用を推進するなど）を検討することも考えられるのではないか。

ＩＳＭＳ適合性評価制度及び情報セキュリティ対策ベンチマークの活用状況の調査

① ＩＳＭＳ適合性評価制度の活用状況

【本制度活用の現状】

ＩＳＭＳ適合性評価制度の活用状況については、１９府省庁中、

a. 必須の条件としている場合がある
・・・８府省庁

b. 総合評価落札方式の加点要素とする場合がある
・・・２府省庁

c. その他
・・・６府省庁

（重複回答有）

であった。ＩＳＭＳ適合性評価制度については、ISO/IEC 15408 と比較し、多くの省庁が活用をしている。

なお、その他には、「（今回の調査対象ではないものの）ISO/IEC 27001:2005 又は財団法人日本情報処理開発協会のプライバシーマークのいずれかを取得を条件とし、両方を取得している場合、総合評価落札方式の加点要素とするもの」や、「外部にＯＡ教育を委託する場合にＩＳＭＳ認証を取得していることを必須条件としたもの」、「ＩＳＭＳ（ISO/IEC 27001 又は BS7799）の適合認証を取得しているか審査中であること、加えてプライバシーマークを取得しているか審査手続き中であることを条件とするもの」が含まれる。

【本制度活用の利点と課題】

本認証制度を活用し、「認証取得した業者に委託することにより、運用まで含めた信頼性の担保、情報システム内に限らない情報セキュリティの確保が一層図られるなど、情報セキュリティ水準の向上に資する観点で有効である」という意見がみられる。

他方で、「当該認証を取得していることを条件とすることで、応札できる業者の範囲が限定され、契約金額への影響が懸念される」とする意見もみられた。また、「委託する案件（ソフトウェア開発なのかコンサルティング業務なのかなど）により求める要件が異なることも考えられ、一律に必須とすること」への疑問もみられる。さらに、本認証取得の実効性について、「制度に基づき認証さ

れた組織が、各案件や要員ごとに適正に運用され、十分機能することが求められる」ことも指摘されている。

【本制度活用に係る今後のあり方】

今後の本制度の活用においては、「単に資格取得の有無を条件とするだけではなく、委託元から案件ごとの特性を考慮した明確な遵守事項を委託先へ明示することが必要である」との意見も出されている。また、「契約における入札資格のように、政府全体として対象企業のセキュリティ水準を確認し、レベル付けを行うなどの措置を講じることで調達の適正性もより確保でき、企業側の認証取得意欲の向上にも繋がる」との意見もみられた。認証取得企業の拡大に従い、その活用が促進されていくことも期待されるが、これら意見にみられるような制度活用のあり方を検討することも重要と考えられる。

② 情報セキュリティ対策ベンチマークの活用状況

【本制度活用の現状】

情報セキュリティ対策ベンチマークの活用状況については、調査対象の期間において、当該ベンチマークの結果の提示を求めた場合があるとする府省庁は19省庁中1省庁であった。当該府省庁では、「必須の条件として提示を求める場合がある」としている。

【本制度活用の利点と課題】

本ツール自体は、「情報セキュリティ対策の実状について容易に診断すること」を可能とする「効果的な診断ツールであり、情報セキュリティ対策レベルの目安とするには有効である」。一方で、評価は「自己評価的な側面があり、その客観性、信憑性に乏しいという面がある」のも事実である。評価には客観性、第三者性を求め、この点を満たさない手法に対する信頼性が落ちると捉えられるのはもっともなことであり、こうしたことが積極的な活用に至らない背景であると考えられる。

【本制度活用に係る今後のあり方】

当該ベンチマークは、企業内部での対策向上のための簡易分析ツール、或いはISMS等の認証取得へ向けた情報セキュリティポリシー策定の助け、維持改善へ向けた現況把握の指標として活用することが有効であると考えられる。調達によって当該調達案件のセキュリティ向上を直接的に期待するよりも、むしろ簡易で効果的な診断ツールの普及啓発であるとの認識の共有を進めることも有効である。

(4) 総評

今回は、基本計画若しくはSJ2007策定以降の取組みの成果を表すデータが得られなかった項目も散見され、取組み以前の現状の分析しか行えなかったという項目も存在することに留意が必要である。

全般的な傾向としては、以下のとおりである。

(A) 企業

企業においては、2005年までの傾向では、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徐々に高まっている状況であった。こうした認識は、2007年の不正アクセス禁止法違反での検挙数の増加や、相次ぐシステムトラブルに関する報道、依然として発生し続ける情報漏えいから、今後も高まっていくこととなると推測される。

対策実施状況では、取組みは継続的に進展しこのような認識の高まりが、今後の対策意識の向上、自主的な対策の更なる伸びに繋がることも期待される。他方、情報セキュリティ対策が着実に実施される中で、その効果については、「あまり効果がない」、「よくわからない」とする割合も高い。また、対策が情報セキュリティ向上以外に及ぼす効果については、「特に効果がない」とする割合が約半数となっている指標もある。今後も対策を更に推進するには、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不可欠であると考えられる。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着実に実施されることが求められる。そして、今後、これら取組みの評価は、2006年以降の効果に関する認識等の指標の推移を見据えて行い、必要に応じて取組みの強化・促進が図られるべきである。

また、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」との格差が存在するとの指摘もある[23]。特に大企業と中小企業の間での格差が広がる傾向があるとの指摘がある。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は否定できない。この意味で、企業側から見ると、対策は守るべきセキュリティと投資可能なコストの均衡点に到達している可能性は否定できない。また、技術的にも現行技術水準で守ることのできるセキュリティの限界点に到達している可能性もある。今後は例えば事業継続性的な視点に目配りを行うなど、対策枠組みの重点の置き方についての検討が必要となるかもしれない点にも留意が必要である。

(B) 個人

個人においては、2007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、情報セキュリティ対する意識の向上、対策実施が着実に進んでいることが各指標から見てとれる。

---

[23] 経済産業省　産業構造審議会情報セキュリティ基本問題委員会報告書「グローバル情報セキュリティ戦略」(平成19年5月公表)

しかし、全体として着実に進展しつつあるとはいえ、基本的と思われる対策（パッチの適用やセキュリティ対策ソフトの導入・活用等）についても、必要性の認識、対策実施状況はまだ改善の余地がある。年代別・男女別の調査結果を見ると、特定の属性について取組みを進める必要性が高いものと考えられる。

また、情報セキュリティに関する被害の認識では、4割近くの個人が「具体的な被害のイメージがわかない」（どのようなリスクがあるのかがわからない）との回答があった。ボット等の新しい脅威が発生し、また見えにくい脅威が発生している状況の中で、新たな変化を踏まえつつ、各属性に応じてわかりやすい形での普及啓発・情報発信を行っていくことが求められる。

第3節　2008年度に向けた課題

(A) 企業

企業分野においては、全体として情報セキュリティ対策の意識の向上、着実な対策の実施はみられるが、積極的な情報セキュリティ対策を実施している主体とそうでない主体が依然として存在する。また、対策実施に対しての効果の認識が低い指標もみられる。企業分野においては、

○ 対策が遅れがちな主体に対して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
○ 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。

(B) 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。

2008年度は、「取組みが遅れがちな主体への対策」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

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　2007年度の取組み

1．2007年度の取組みの背景

情報セキュリティ技術戦略の基本として以下の３つの条件が満足される環境として構築されるべきと考えられている。

○　そもそも「高度情報通信ネットワーク（ＩＴ）が安全であること。
○　利用者が「高度情報通信ネットワーク（ＩＴ）が安全である」と分かる（認識・体感できる）こと。
○　万が一事故が起こった場合でも、その被害の局限化や救済が図られるとともに業務の継続性が保たれること。

この３条件を満足する環境を実現するに当たり、

情報セキュリティ技術の高度化（そもそもの情報セキュリティ技術の高度化）、組織・人間系の管理手法の高度化（開発された情報セキュリティ技術が実環境で効果的、効率的に運用されるため組織・人間系の管理手法の高度化）の両面からの取組みが必要であるとの認識に基づき、昨年度に引き続き各種施策を実施した。

2．2007年度の取組み

研究開発・技術開発の効率的な実施体制を構築するための取組みをはじめ情報セキュリティ技術開発の重点化と環境整備及び「グランドチャレンジ型」研究開発・技術開発の推進を実施した。

第2節　2007年度の取組み及び取組みを受けた現状の評価等（2007年度の評価等）

1．2007年度の評価等に関する基本的考え方（評価等の視点）

2006年度に引き続き、情報セキュリティにおける技術開発・研究開発を評価する上で、ＩＴを安心して利用できる環境を強化することに直結する研究開発・技術開発が着実に実施されたかという点に留意し、研究開発・技術開発の実施状況の的確な把握がなされるべきである。

2007年度の評価等の視点としては、現在の施策体系の下での対策の中間年であったことを踏まえ、研究開発・技術開発の効率的な実施体制が構築されているか、セキュリティ技術開発の高度化とともに、組織・人間系の高度化が図られているか、「グランドチャレンジ型」研究開発・技術開発が着実に推進されたかなどが挙げられる。

2. 評価等について（評価指標等）

(1) 2007年度の評価等について

情報セキュリティ政策の枠組み文書で述べられているように、「対策実施4領域以外の分野については、」「必要に応じて政府機関を始めとする各主体による調査を実施し、これをもって点検段階（C）の仕組みとして活用」[24]していくこととしている。この点は、技術戦略の分野についても例外ではなく、指標を設定することは難しいと考える。したがって、数値を可能であれば適宜加えつつ、評価等を行うことをもって点検段階の検討とする。

(2) 2008年度以降の評価等について評価等

2008年度以降についても、基本的には2007年度と同様の方法に基づいて評価等を行うこととなる。また、必要に応じ、総合科学技術会議をはじめとする他の関係機関等における評価結果の活用を図る。

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

SJ2007に基づく施策の取組み結果については、別添1の表のとおりであり、それぞれの施策におけるA、B、Cの分類で見ると、25の施策のうち、Aの施策が24、Cの施策が1となっている。Cの施策については、他の施策の成果にかんがみ、実施は不要と判断した。

具体的に実施された主な施策としては、「①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、技術戦略専門委員会報告書2006において、整理した情報セキュリティに関連する研究開発・技術開発テーマ一覧を更新し、その情報に基づく効率的な実施体制を検討した。情報セキュリティに関連する研究開発・技術開発の実施状況の把握に向けた検討が開始されるなど、限られた投資の中で効率的・効果的に研究開発・技術開発を実施するための体制が構築された。

また、「②情報セキュリティ技術開発の重点化と環境整備」については、2006年度から実施している「高セキュリティ機能を実現する次世代OS環境の開発」（内閣官房、内閣府、総務省、経済産業省）や「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）が着実に推進されるなど、情報セキュリティ技術の高度化に向けた施策が推進された。

さらに、「③「グランドチャレンジ型」研究開発・技術開発の推進」については、グランドチャレンジWGを立ち上げ、研究開発・技術開発を推進する体制、グランドチャレンジ型プロジェクトの実行行程及び具体的なテーマ選定の議論が進められた。

(2) 施策の取組みによる社会的変化に関する評価等

ネット接続ゲーム機の普及や仮想化、サーバ統合の進展などを背景に、情報セキュリティ確保の抜本的対策が求められる中、各種攻撃ツールによるアプリケーションソフトウ

[24] 情報セキュリティ政策の枠組み文書「第5章第3節1.（2）対策実施四領域以外の分野」を参照。

ェアの脆弱性をつくゼロデイアタックやＷＥＢサイトの脆弱性を突く攻撃の発生度合いが高まる中、情報漏えい対策の研究開発が2007年度より着手されたのをはじめ、ITの信頼性確保のための喫緊な取組みとして2006年度から実施している「高セキュリティ機能を実現する次世代ＯＳ環境の開発」（内閣官房、内閣府、総務省及び経済産業省）では、中間成果がβ版としてオープンソース化されるなど研究開発が着実に進展している。

また、コンピュータウイルスの蔓延や情報システム障害の発生など、現在のIT基盤において認められる情報セキュリティ課題を解決することを目標とした課題解決型の技術開発も数多く行われており、近年問題が深刻化しているボットを使ったサイバー攻撃等の課題を解決するための技術開発等が積極的に行われている。

2008年度においても、これらの技術開発の一層の加速化が期待される状況である。

（3）総評

SJ2007に基づく施策は、技術戦略専門委員会により、研究開発・技術開発の投資領域の検討がなされたのを始め、内閣官房及び各府省庁において各種の取組みがなされ、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。しかしながら、情報セキュリティ技術の高度化と共に推進するべき組織・人間系の管理手法の高度化に対する取組みにおいては十分に実施されたとは言えず、情報セキュリティ政策推進において課題となる施策が存在していることも事実である。

基本計画に基づく取組みの最終年に当たる2008年度には、このような事態が生じないよう、一層の積極的な取組みが求められる状況にある。

第3節　2008年度に向けた課題

2008年度に向けては、2007年度に構築した「研究開発・技術開発の効率的な実施体制」の一層の推進を図るとともに、研究開発・技術開発の継続的な実施が必要である。また、「グランドチャレンジ型」研究開発・技術開発については、ＷＧで議論した内容を技術戦略専門委員会に図り、一層の審議を経た上で、総合科学技術会議に研究開発・技術開発を推進する体制、グランドチャレンジ型プロジェクトの実行行程及び具体的なテーマを提言し、その実現に向けた一層の推進を図る。

【情報セキュリティ人材の育成・確保】

第1節　2007年度の取組み

1．2007年度の取組みの背景

情報セキュリティに係る人材の不足が叫ばれる中、情報セキュリティ政策会議の下に設置された「人材育成・資格制度体系化専門委員会」（以下、「人材委員会」という。）の報告書の中で、情報セキュリティに係る人材の育成・確保に関する数々の課題や取り組むべき施策が明らかになったところであった。

このため、これら取り組むべきとされた施策について着実に実施するとともに、社会全体としての取り組みの拡大を促していくことが必要であった。

2．2007年度の取組み

2007年度においては、人材委員会の報告を受け、具体的に取り組むべき施策としてSJ2007に盛り込まれた各種施策が着実に実施された。

具体的には、産学連携により高度情報セキュリティ人材育成プログラムを開発・実施する教育拠点として2件の教育プロジェクトが支援対象として選定されたほか、情報処理技術者試験制度の改革や組織におけるIT利用者のためのセルフチェックツールの機能拡張など、企業における情報セキュリティ人材の育成・確保に向けた様々な取組みが実施された。

政府内においても、各府省庁において情報セキュリティ能力も含めた「行政機関におけるIT人材の育成・確保指針」の策定が進むとともに、各府省庁の幹部職員向け研修として総務省が主催する「新任管理者合同セミナー」において情報セキュリティに関する研修を実施したほか、情報セキュリティ担当職員や一般職員向けの研修ツールとして総務省が実施した「情報システム統一研修」の改訂作業の中で、情報セキュリティ関連コースの抜本的見直しを行うなど、各種の人材育成プログラムの整備が進んだところである。

第2節　2007年度の取組み及び取組みを受けた現状の評価等（2007年度の評価等）

1．2007年度の評価等に関する基本的考え方（評価等の視点）

2007年度は、人材委員会の報告書を受けた「人材育成元年」ともいうべき年度として、具体的に取り組むべきとされた各種施策について着実にスタートすることが求められた年度であった。こうした前提の下、2007年度の評価等の視点としては、これら各種取組みが着実に進められたかという視点、さらにはこれら政府の取組みに加えて、社会全体として人材の育成に関する意識の浸透や取組みの広まりがみられたのかという視点が挙げられる。

2．評価等について（評価指標等）

(1) 2007年度の評価等について

情報セキュリティ人材の育成・確保に関して、2007年度は、人材委員会の報告を受け各種取り組みの展開が開始された年であり、まずはこれらの取組みが具体的にあげた効果について評価を行うことが必要であり、可能な限り定量的な評価が行われることが望ましい。また、民間の教育事業者連絡会が発足したことにより、業界全体とした見た資格取得者数などのデータも把握可能となっているので、こうしたデータも社会全体にお

ける兆候を測る指標として活用していくことが適当である。

(2) 2008年度以降の評価等について

2008年度以降の評価に当たっては、2007年度に把握されたデータ項目を継続的に活用・収集し、その変化による人材育成の動向等を評価することが求められる。加えて、様々な政策や社会環境の状況を踏まえ、必要と考えられる評価指標を適宜把握・活用していくことも必要と考えられる。

3. 評価等結果と総評

(1) 施策の取組み結果に関する評価等

SJ2007に基づく施策の取組み結果については、別添1の表のとおりである。SJ2006と比較して施策数は8施策と拡大し(2006年度は4施策)、このうち6施策がA、1施策がBとなっており、予定していた取組みは概ね着実に実施された。

具体的には、文部科学省の「先導的ITスペシャリスト育成推進プログラム」による高度情報セキュリティ人材の教育拠点の整備や経済産業省における情報処理技術試験制度の改革や組織におけるIT利用者向けのセルフチェックツールの機能拡張など、情報セキュリティに係る人材の育成に資する教育拠点やツールなどの基盤の整備が進んだところである。

また、政府内においても、各府省庁におけるIT人材の育成・確保指針の整備、幹部職員・一般職員・セキュリティ担当職員向けの研修機会の拡大やコンテンツの充実など、情報セキュリティに係る人材の育成のために必要となる様々な体制・基盤が整いつつある。

この中では例えば、幹部職員向け研修として活用された「新任管理者合同セミナー」において、新たに本府省庁の課室長等に就任した者367名に対して「管理者に求められる情報セキュリティ政策について」との内容で講義を行ったところ、「大変良かった」と回答した幹部職員が41.2%、「良かった」と回答したのが47.3%、「普通」と回答したのが8.5%と、ほとんどの新任管理者がその内容について研修効果を認めているところであり、今年度の取組みとして一定の成果を上げたものと評価できる。

(2) 施策の取組みによる社会的変化に関する評価等

政府において各種施策が進められる一方、民間分野においても、特筆すべき動きがみられた。具体的には、情報セキュリティ教育を実施する多数の団体が「情報セキュリティ教育事業者連絡会」を発足し、情報セキュリティ人材の育成の必要性について訴えるためのセミナーの開催や、人材育成の指標となるキャリアパスの検討など各団体の枠組みを越えた業界横断的な取組みを推進するための連携体制が整備された。この動きは、人材育成委員会の報告書が訴えた情報セキュリティ人材の育成拡大に向けて、民間団体が主導的に連携の枠組みを構築したものとして高く評価される。

こうした官民の様々な取組みを受け、情報セキュリティに関する研修を受講したり、主

要な資格を取得する者の数も着実に増加しつつある。具体的に同連絡会に所属する、ある資格団体においては、この一年間で資格取得者数が3割近く増加しており、情報セキュリティのスキルを身に付けようとする動きが拡大していることが見てとれるところであり、歓迎すべき動きである。

(3) 総評

2007年度においては、人材委員会の報告書を受けて、政府において幅広く取り組みが行われ、教育拠点や教育ツールの整備が図られるなど、情報セキュリティにかかる人材の育成に資する体制・基盤が整いつつある。民間の教育事業者団体においても、各団体の枠組みを越えた積極的な情報発信やキャリアパスの構築に向けた検討が進められ、官民における積極的な取組みの展開を通じて、人材の育成も広まりつつあるところである。

このように、2007年度においては、人材育成のための体制・基盤の整備が図られ、その具体的な効果がみられつつあるという意味では大きな成果が上がった一年と考えられる。他方、実際により多くの方がこうした教育機会を活用して、一定のスキルをもった「情報セキュリティ人材」として組織内など様々な立場で技能を発揮することが可能となるには、なお時間を要すると考えられる。そういった意味で、人材育成に関してはなお発展途上の途中と言うことができると考えられる。

第3節 2008年度に向けた課題

2008年度からは、2007年度までに整備が進んだ様々な体制・基盤について、実際にその有効活用が図られ、社会のあらゆる場面において必要な場所・部署に必要な人材が配置されるよう育成が進むことが必要となる。そのためには、人材を育てようとする組織などいわば需要側において、人材育成の必要性と具体的に必要となる人材像を正しく理解・認識し、具体的な人材育成計画を立てて実行に移すことが求められる。このためには、これら需要側と人材育成のいわば供給側に相当する各種基盤・体制側との間で、十分な情報流通がなされることが必要であり、こうした動きを加速・促進するための官民双方での取組みが期待される。

【国際連携・協調】

第1節　2007年度の取組み

1．2007年度の取組みの背景

我が国の国民生活・社会経済活動においてITへの依存度が高まる一方で、ITの基盤は、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り、「ITを安心して利用可能な環境」を実現するための情報セキュリティ政策には、国際的な連携・協調が必要であると認識されていた。

また、世界一のブロードバンド大国となった我が国は、情報セキュリティ問題についても他国に先んじて直面することが予測されるため、世界のトップランナーとして問題解決の責任があることを自覚し、情報セキュリティ領域における我が国発の国際貢献に取り組む必要があると考えられた。

2．2007年度の取組み

2006年度に引き続き、国際連携・協調が必要であるという認識の下、まずは諸外国との連携の窓口の明確化を図るため、主に多国間の枠組みであるAPEC、OECD、ARF、Meridian等の国際会合に参加し、我が国の新しい情報セキュリティ戦略・体制に係るプレゼンスの明確化、広報活動の推進を行った。

また、情報セキュリティ領域での我が国発の国際貢献に向けた第一歩として、政府全体として戦略的に国際協調・貢献に取り組むための基本方針となる「我が国の情報セキュリティ分野の協調・貢献に向けた取組み」を策定した。

第2節　2007年度の取組み及び取組みを受けた現状の評価等（2007年度の評価等）

1．2007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・協調に係る取組みに関する評価等については、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つき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が多いことに留意するべきである。

その上で、2007年度の評価等の視点としては、現在の施策体系の下での取り組みの初年度であったことを踏まえ、我が国の情報セキュリティ政策に係る体制と戦略の認知度が向上したか否かという視点、多国間の国際連携・協調の枠組みを使い、情報セキュリティに係るリスクを減少若しくは解消させることができたのかという視点、情報セキュリティ領域での我が国発の国際貢献を実際に行えたのかという視点が挙げられる。

2．評価等について（評価指標等）

（1）2007年度の評価等について

情報セキュリティ政策の枠組み文書で述べられているように、「対策実施4領域以外の分野については、」「必要に応じて政府機関をはじめとする各主体による調査を実施

し、これをもって点検段階（C）の仕組みとして活用」[25]していくこととしている。このことも踏まえ、2007年度は特段指標の設定は行わない。

（2）2008年度以降の評価等について

横断的な基盤分野については、定量的な評価等よりもむしろ定性的な評価等が求められる分野であるため、指標を定めることは困難であるとされている。

その上で、定量的な指標としては、例えば我が国の情報セキュリティ政策に係る体制と戦略の認知度について、NISCが2006年度に作成した英文ウェブサイトのアクセス数をカウントできるようにし、我が国政府の取組みに関心を持つ人々の推移を把握することは可能である。

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

SJ2007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11施策のうち、Aが11施策と、概ね順調に取組みがなされた。我が国の情報セキュリティ政策に係る認知度向上については、様々な国際会合等で、情報セキュリティ政策会議やNISCの設立、基本計画の策定等、我が国の情報セキュリティ政策に係る体制と戦略を説明し、あわせてNISCの英語版ウェブサイトを充実させるなどの広報活動を行ってきたことから、一定の成果を得たと考えられる。そのため、諸外国の情報セキュリティ機関等から、窓口（POC）機能の不明確さを理由に情報が入手できないといったリスクは、ある程度軽減されていると考えられる。

また、情報セキュリティ領域での我が国発の国際貢献についても、我が国発の国際貢献に向けた基本方針が策定されたことから、当該基本方針に基づき、「ベストプラクティス」の発信のほか、グローバルなIT安心利用環境の実現に向けた取組みが試み始められており、国際社会におけるセキュリティ文化の実現にも貢献していると考えられる。

（2）施策の取組みによる社会的変化に関する評価等

サイバー空間においては、国家という枠組みを超えて情報セキュリティ問題が起こり得ることから、国内における情報セキュリティ問題が、国際的にも起こる可能性は高い。したがって、国際連携・協調について、様々な国際会合等で国内と同様の問題意識に基づいた議論が行われ、社会・経済活動がITへの依存性を高めている一方で、情報セキュリティリスクが必ずしも万人に理解されていないという危機感を共有し、各国の関係者間でPOCを明確化すること、ベストプラクティスの共有・交換をすることについては一定のコンセンサスが生まれつつある。

このような中で、我が国は国際連携・協調を通じたグローバルなIT安心利用環境の実現のため、我が国の情報セキュリティ分野の国際協調・貢献に向けた基本方針を策定した。

これを踏まえて、我が国の国際連携・協調に関する取組みが行われており、情報セキ

[25] 情報セキュリティ政策の枠組み文書「第5章第3節1.（2）対策実施四領域以外の分野」を参照。

ュリティリスクに対応した体制を整える初期段階は達成したものといえるが、次の段階へのステップとして、基本方針を実行に移すため、引き続き関係者との信頼関係の醸成や、我が国の取組みの具体化・充実化に取り組む必要がある。

(3) 総評

国際連携・協調については、国際会合等における我が国政府の取組みの紹介や、ウェブサイトを通じた広報活動により、我が国の情報セキュリティ政策に係る認知度の向上については一定の成果を得たと考えられる。また、諸外国の情報セキュリティ機関にPOCを認識されることにより、必要な情報が入手できないといったリスクは、ある程度軽減されていると考えられる。

一方、国際社会におけるセキュリティ文化の実現のための取組みや、情報セキュリティ領域での我が国発の国際貢献については、我が国の情報セキュリティ分野における国際協調・貢献のための基本方針が策定された。基本方針を実行に移すため、今後、取組みの具体化を図る必要がある。

第3節 2008年度に向けた課題

国際連携・協調の推進については、サイバー空間が国家という枠組みを超えたものであることやIT障害の影響が一か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り組む必要がある。

連携・協調に当たっては、国外のステークホルダーとの信頼関係の醸成が必要であることから、継続的に活動を定着させ、十分な成果を上げるための人的資源を確保するとともに、政策体系の理解や窓口の相互確認等、信頼関係の構築に向けた初期段階にとどまっている現状から、一歩進んだ取組みを行う必要がある。

また、国際社会におけるセキュリティ文化の実現のための活動の一環として、情報セキュリティ領域での「ジャパンモデル」を明確化し、対外的に発信することで、国際貢献に資する必要がある。

そのため、我が国の情報セキュリティ分野における国際協調・連携のための基本方針に従い、セキュリティ文化の醸成を通じた利用者のモラル・認識の形成・向上、情報セキュリティ関連制度・ルール構築、サイバー攻撃等のITに起因する脅威への対応等の取組みを具体化していく必要がある。

【犯罪の取締り及び権利利益保護・救済】

第1節　2007年度の取組み

1．2007年度の取組みの背景

「ITを安心して利用可能な環境」に構築するためには、サイバー空間における犯罪の取締りや権利利益の保護・救済の確保が必要である。しかし、インターネットをはじめとするITの普及に伴い、サイバー空間における犯罪や権利利益の侵害は急激に増加する傾向にあり、例えば、2006年中のサイバー犯罪（情報技術を利用する犯罪）の検挙件数が、前年に比べ40．0％増加し、2001年から過去5年間で約3．3倍となっているなど、サイバー空間における犯罪の取締りや権利利益の侵害に対処するため、一層の情報セキュリティ対策の体制強化等を図ることが必要であった。

2．2007年度の取組み

サイバー犯罪の取締り基盤の更なる強化のため、サイバー犯罪捜査に従事する警察職員に対する研修等による捜査技能水準の向上、多様化・巧妙化するサイバー犯罪を的確に取り締まるための捜査体制の強化・整備、捜査・解析用資機材の充実・強化等のほか、諸外国の関係機関との国際連携の推進、デジタルフォレンジックに係る知見の集約・体系化等の推進等を行った。

また、サイバー空間における権利利益の保護・救済に資するため、その基盤に係る実態の調査研究及びプロバイダ責任制限法等の周知の促進を行った。

さらに、サイバー空間の安全性・信頼性を向上させる技術の開発・普及のため、サイバーテロ対策に係る共同研究を行った。

第2節　2007年度の取組み及び取組みを受けた現状の評価等（2007年度の評価等）

1．2007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の保護・救済に係る取組みの評価等については、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差があり、中長期的な視点で把握する必要がある一方、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、2007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、捜査能力や体制の構築、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、技術開発とその普及が進み、リスクを減少又は解消させることができたのかという視点が挙げられる。

2．評価等について（評価指標等）

（1）2007年度の評価等について

情報セキュリティ政策の枠組み文書で述べられているように、「対策実施4領域以外の分野については、…必要に応じて政府機関をはじめとする各主体による調査を実施し、これをもって点検段階（C）の仕組みとして活用」していくこととしている。これを踏まえて、2007年度は特段指標の設定は行わない。

(2) 2008年度以降の評価等について

2008年度以降についても、基本的には2007年度と同様の方法に基づいて評価等を行うこととなる。

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

SJ2007に基づく施策の取組み結果については、別添1の表のとおりである。全12施策のうち、Aが10施策、Bが1施策、政府機関の事情以外の理由により予定どおり推進することができなかった施策が1施策となっており、課題を残しつつも概ね順調に推移している。

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体制の強化、捜査・解析用資機材の充実・強化、諸外国の関係機関との連携、デジタルフォレンジックに係る知見の集約・体系化等の推進、プロバイダ責任制限法等の周知の促進等が推進されたほか、権利利益の保護・救済のための基盤に係る調査研究が行われた。一方、国会で審議中という理由により、サイバー犯罪に適切に対処するための法整備等が滞っているものもあった。

また、サイバー空間の安全性・信頼性を向上させる技術の開発・普及については、サイバーテロ対策に係る共同研究が行われた。

(2) 施策の取組みによる社会的変化に関する評価等

施策の取組みによって、サイバー犯罪の取締りのための基盤の整備が図られたほか、権利利益の保護・救済のための基盤に係る現状が把握された。また、技術開発については、直ちに有用な技術が開発されてはいないものの、そのような技術の開発と社会への普及に向けた取組みが行われたと言える。

これらの結果から、短期的には大幅な社会的変化としてはとらえにくいものの、中長期的にみれば、ITを安心して利用可能な環境の構築に向けて進んでいるものと言える。

(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、サイバー空間において次々に発生する新たな形態の犯罪や不法行為に対して、その捜査能力や体制の構築を進め、中長期的なリスクを減少させることについて、一定の取組みができたと言える。一方、安心のための技術の開発とその普及により、リスクを減少させることについては、未だ技術開発自体が途上であるため、取組みをさらに継続し、加速化させる必要がある。

第3節 2008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多発している状況にあり、現状のままでは、インターネット上の犯罪等への不安はさらに増加し、施策の取組み以上にリスクが増加する可能性もある。例えば、2007年においては、不正アクセス

禁止法違反の認知件数が1，818件と前年の約2倍に増加するなど、サイバー犯罪の増加傾向は続いている。また、権利利益の保護・救済についても、著作権侵害やインターネット上の掲示板における名誉毀損の横行等未だ対応が十分とは言えない状況もある。

なお、内閣府が2007年11月に行った調査によれば、インターネットの利用に不安を感じる人が45．4％に上っており、犯罪の取締りと権利利益の保護・救済については、引き続き対策の一層の強化が必要である。

＜資料一覧＞

「セキュア・ジャパン2007」に盛り込まれた施策の実施状況　別添1

＜分類＞
Ａ：当初の予定どおり施策を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、継続して施策を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：予定どおり施策を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、最終的には施策を推進することが出来る施策。
Ｃ：予定どおり施策を推進することはできず、今後の見通しも立たない施策。
－：予定どおり施策を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　対策実施4領域における情報セキュリティ対策の強化

第1節　政府機関・地方公共団体

ア　政府機関

①政府機関統一基準とそれに基づく評価・勧告によるＰＤＣＡサイクルの構築

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	政府機関統一基準の見直しの実施	内閣官房	・情報セキュリティ政策会議第16回会合（平成20年2月4日）において、ＤＮＳサーバーに関する事項の追加等を行った政府機関統一基準の第3版を決定。	A
イ)　a)	各政府機関でのＰＤＣＡサイクルの定着	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、具体的な実施手順の整備及び職員への教育についての取組みを進めるとともに、情報セキュリティ対策の実施状況の自己点検を実施。	A’
イ)　b)	政府全体でのＰＤＣＡサイクルの定着	内閣官房 全府省庁	・内閣官房において、平成18年度における各府省庁の情報セキュリティ対策状況を対策実施状況報告として取りまとめ、その概要を情報セキュリティ政策会議第11回会合（平成19年4月23日）に報告。 ・内閣官房において、各府省庁の端末・ウェブサーバ、メールサーバについて重点検査を行い、それぞれの評価結果を各省に通知するとともに総合評価結果を情報セキュリティ政策会議第13回及び15回会合（平成19年8月3日、平成19年12月12日）に報告。	A’
ウ)　a)	対策実施状況に関する評価等	内閣官房	・内閣官房において、上記の通り各府省庁の端末・ウェブサーバ、メールサーバについて重点検査を実施し、各府省庁の対策の実施状況を客観的に比較可能な形で評価した結果を情報セキュリティ政策会議に報告。 ・評価の結果について、情報セキュリティ政策会議終了後直ちに、内閣官房（NISC）のホームページにおいて公表。	A’
ウ)　b)	情報セキュリティマネジメントに関する評価等	内閣官房	・内閣官房において、平成18年度における各府省庁の情報セキュリティマネジメントの評価を行い、政府機関の模範となる優れた取組み（44件）の選定及びその内からベストプラクティス（5件）の選定を、情報セキュリティ政策会議第13回会合（平成19年8月3日）において実施。	A’
エ)　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、内閣官房においては、自己点検の効率化の情報提供（「情報システム対策に関する自己点検の随時実施について」（平成19年8月1日））、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
エ)　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	・内閣官房において、情報セキュリティ対策の運用上の共通的な課題である情報セキュリティ監査の実施に係る勉強会を平成19年10月11日に開催。	A
エ)　c)	情報セキュリティ対策のベストプラクティスの共有	内閣官房 全府省庁	・内閣官房において、平成18年度における各府省庁の情報セキュリティマネジメントの評価を行い、政府機関の模範となる優れた取組み（44件）の選定及びそのうちからベストプラクティス（5件）の選定を、情報セキュリティ政策会議第13回会合（平成19年8月3日）において実施。政府機関の模範となる優れた取組みについては、政府機関全体で情報を共有。また、評価の結果については、同日、内閣官房（NISC)のホームページにおいて公表。	A
エ)　d)	各府省庁における自己点検及び監査の効率化	内閣官房	・総務省人事恩給局が主催した「新任管理者合同セミナー」（平成19年8月30日）にて、「管理者に求められる情報セキュリティ対策について」をテーマとして研修を実施。	A
エ)　e)	各府省庁の情報システムの一元的把握	内閣官房 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記載について検討又は実施した。	B
オ)	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
カ)　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19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検討又は実施した。 ・内閣官房から、利用を促進するための参考資料として、「外部委託における情報セキュリティ対策に関する評価手法の利用の手引」の改訂版を平成19年11月に各府省庁に配布。	B
カ)　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19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検討又は実施した。 ・内閣官房から、利用を促進するための参考資料として、「外部委託における情報セキュリティ対策に関する評価手法の利用の手引」の改訂版を平成19年11月中に各府省庁に配布。	B
カ)　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19年6月に、当ガイドラインを基にした情報システムの信頼性の向上のための緊急点検を実施。本点検結果を受けて、平成20年度内を目途に信頼性ガイドラインの改訂作業を実施予定。	B
キ)	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	・各政府機関がITシステムの調達を情報セキュリティに配慮しつつ、実効的かつ効率的に行えるようにするため、平成19年度に、独立行政法人情報処理振興機構において、ITセキュリティ要件、ITセキュリティ評価及び認証制度の認証製品の活用可否を確認する際の支援ツールを開発。	A

②独立行政法人等のセキュリティ対策の改善

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	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、各府省庁を通じて、独立行政法人等の情報セキュリティポリシーの整備を平成19年7月に依頼した。また、独立行政法人等における整備状況について、総務省が行う電子政府基本調査の結果から把握する。	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	・内閣官房において、先行的に一部の独立行政法人に対して、マニュアル等を提供するなど、情報セキュリティポリシー策定等のための支援を実施するとともに、情報セキュリティポリシーの見直しに取り組む先行的な機関から課題等についての情報を収集。 ・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、霞ヶ関WANインフォメーションボードに「独法向け：統一基準第2版改定内容説明」を、それぞれ掲載。	A

③中長期的なセキュリティ対策の強化・検討

（ア）最適化対象の府省共通業務・システム及び一部関係府省業務・システムの開発との連携

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	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	業務システムの最適化に関して、対象システムの開発の段階から効果的な情報セキュリティ機能を実現するため、 ・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。また、同WGが主催した平成19年10月のCIO補佐官対象のセミナーにおいて、NISCから講演を実施。 ・さらに、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(SBD：Security by design)ための方策の強化について議論を行い、その結果をSBDの検討にフィードバックすることとした。	A
イ)	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、例えば調達の際には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を確認するなど、平成19年度も引き続き同制度により認証された製品等の優先的な取り扱いを検討又は実施した。 ・内閣官房から、利用を促進するための参考資料として、「情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書」及び「情報システムの構築等におけるST評価・ST確認の実施に関する解説書」の改訂版を平成19年11月に各府省庁に配布。	B

（イ）セキュリティ強化に資する新規システム（機能）の導入検討とその実現

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	次世代の電子政府構築に向けた検討	内閣官房 総務省	・次世代の電子政府構築に向けて、共通的なプラットフォームの構築・整備に関する技術的・機能的検討の結果、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(SBD：Security by design)ための方策の強化について議論を行い、その結果をSBDの検討にフィードバックすることとした。	A
イ)	高セキュリティ機能を実現する次世代OS環境の開発	内閣官房 内閣府 総務省 経済産業省	・現在のOSやアプリケーション等の利用環境を維持しつつ、情報セキュリティ機能を集約的に提供することのできる仮想機械（VM:Virtual Machine）機能及びこれを稼働させるための最小限のOS機能（これらの機能を併せて「セキュアVM」と呼ぶ。）の開発を、産官学の連携により平成18年7月から着手。平成19年3月には機能検証用のα版を開発完了、β版は、計画通り平成20年3月に完成。	A
ウ)	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	・本技術開発である「平成19年度セキュア・プラットフォームプロジェクト」について、平成19年6月末に公募、採択し、8月末より研究開発に着手、セキュア・プラットフォームの基盤技術の研究開発調査を実施。	A
エ)	警察における情報セキュリティ対策の強化	警察庁	・外部記録媒体に保存する情報を自動的に暗号化等するソフトの一般業務用端末への導入が平成20年3月に完了。	A
オ)	電子政府に用いられるOSのセキュリティ品質の評価尺度の確立	内閣官房	・本格的な電子政府開始に向けたOS等システム導入における技術動向調査実施に向けて準備を進めていたところであるが、既存OS環境でのセキュリティレベルの向上や現在開発中の高セキュリティ機能を実現する次世代OS環境の開発（セキュアVM）の成果をかんがみると、施策実施は不要と判断した。	C
カ)	電子政府システムのIPv6対応化	内閣官房 総務省 全府省庁	・総務省において、インターネットサービスプロバイダにおけるIPv6接続サービス提供状況調査を平成19年3月に公表したところであり、引き続き調査の上、平成20年3月に調査結果を更新・公表した。 ・各府省庁において、情報システムにおけるIPv6化の具体的な計画の策定について実施又は検討した。	A
キ)	電子政府認証ガイドライン利用の推進	内閣官房 総務省 経済産業省	・平成18年度に策定された電子政府認証ガイドラインの素案について第三者レビューを行った結果、政府機関における今後の電子認証のあり方についてSBD（Security by design）の一貫として引き続き検討することとした。	B
ク)	中長期的な視点での電子政府における個人認証の発展方向の検討	内閣官房	・諸外国の電子政府における、公的個人認証システムの動向、普及状況に関する調査を実施。今後の個人認証発展方向の検討に資する情報として活用。	A

(ウ) 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)	政府機関のドメイン名であることが保証されるドメイン名の利用の促進	総務省 全府省庁	・総務省において、平成19年6月から8月にかけて各政府機関の利用するドメイン名について調査を実施。 ・総務省において、平成19年9月に、各政府機関のドメイン名利用状況及び「go.jp」以外のドメイン名から「go.jp」への移行状況について各政府機関に周知するとともに、本施策の必要性、今後の進め方、主要質問事項への回答等に関する説明資料を配付し、今年度中の移行を改めて促した。 ・内閣官房において、政府機関統一基準（第3版）において、政府機関がドメイン名を使用する際の対策について示した。 ・総務省において、「go.jp」の登録組織、利用状況について調査を行い、各政府機関で認識されていない「go.jp」の登録実態の把握を促した。 ・総務省において、平成20年1月から3月にかけて各政府機関の利用するドメイン名について調査を実施。	B
イ)	政府機関から発信する電子メール及び政府機関のホームページからダウンロードされる電子文書に係る成りすまし及び改ざんの防止	内閣官房 総務省 全府省庁	・政府機関統一基準（第2版）において、電子署名を付すための政府内情報システムの在り方について示した。	A

(エ) 政府機関における安全な暗号利用の促進

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	政府機関で利用する暗号の安全性等確保	総務省 経済産業省	・暗号技術検討会等を開催し、電子政府推奨暗号の監視並びに電子政府推奨暗号の安全性及び信頼性確保のための調査等を実施。	A
イ)	政府機関における安全な暗号利用の推進体制等の検討	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において、電子政府推奨暗号の危殆化が発生した際の取扱い手順及び実施体制について、SHA-1における対応を基に検討を進めているところ（SHA-1における対応については、ウ）を参照）。 ・暗号技術検討会において、電子政府推奨暗号リスト改訂に係る基本方針について決定。	B
ウ)	ハッシュ関数SHA-1の安全性低下への対応	内閣官房 総務省 経済産業省 全府省庁	・内閣官房において、総務省、経済産業省及び関係府省庁の協力を得て、新たなハッシュ関数への移行に関する指針の策定のための具体的な課題の抽出等に係る連絡会を平成19年9月から実施し、平成20年2月の政策会議に指針案を諮った。	A
エ)	安全性・信頼性の高い暗号モジュールの利用推進	内閣官房 経済産業省 全府省庁	・内閣官房において、暗号モジュール試験及び認証制度の利用を促進するため、政府機関統一基準（第2版）解説書において、当該制度を紹介。	A
オ)	ファイル（電磁的記録）のセキュリティ対策の推進	防衛省	・可搬記憶媒体に出力するデータを強制的に暗号化するソフトの導入を完了。	A

④サイバー攻撃等に対する政府機関における緊急対応能力の強化

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア) a)	政府横断的な対応体制の構築（GSOCの整備）	内閣官房 全府省庁	・政府横断的な情報収集、攻撃等の分析・解析、各政府機関への助言、各政府機関の相互連携促進及び情報共有を行うための体制（GSOC）を整備。平成20年4月より運用開始予定。	A
ア) b)	情報保証に係る最新技術動向等の調査研究	防衛省	・情報システムの情報保証を確保するためサイバー攻撃及びサイバー攻撃対処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実施。	A
イ) a)	各政府機関における緊急対応体制の強化	内閣官房	・各省庁実務担当者によるIT障害の対処に関する会議を平成19年12月に開催。 ・発生が多発しているIT障害に対処できるよう、必要な情報を迅速に各省庁に提供していくことにより当該IT障害への対処体制の強化を推進。	A
イ) b)	サイバーテロ対策に係る体制等の強化・整備	警察庁	・事案対処能力・技術力の維持、向上のため、部内外におけるOSやネットワーク機器等に係る緊急対処等に必要な各種研修を推進。 ・各都道府県警察のサイバーテロ対策要員である警察官を対象に、サイバー攻撃に関する知識・技能の修得のための民間委託研修を平成19年10月及び平成20年1月に実施。	A
イ) c)	サイバー攻撃等に係る分析・対処及び研究の推進	防衛省	・防衛省の保有する情報システムに対するサイバー攻撃等に関する脅威／影響度の分析・対処能力をさらに向上させるため、サイバー防護用分析器材を導入、平成20年3月から運用開始。また、不正アクセス監視・分析技術、サイバー攻撃分析技術及びアクティブ防御技術等について基礎的な研究を実施し、その結果を取りまとめた。	A
イ) d)	統合通信部隊の新設	防衛省	・自衛隊の情報通信について、これまでの静的な機能維持に加えてサイバー攻撃発生時の適時適切な機能回復などの動的な役割を担う自衛隊指揮通信システム隊を平成20年3月に新設。	A

⑤政府機関における人材育成

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア） a)	一般職員に対する教育の検討	内閣官房 全府省庁	・内閣官房と総務省行政管理局において「情報システム統一研修」の平成20年度改訂に向けたセキュリティ関連コースの抜本的見直しを行い、平成19年12月に結果を得た。	A
ア） b)	幹部職員に対する教育の検討	内閣官房 総務省 全府省庁	・総務省人事恩給局が主催した「新任管理者合同セミナー」（平成19年8月30日）にて、「管理者に求められる情報セキュリティ対策について」をテーマとして研修を実施。	A
ア） c)	情報セキュリティ対策を担当する職員に対する教育の検討	内閣官房 総務省 全府省庁	・内閣官房と総務省行政管理局において平成19年7月及び10月実施の「情報システム統一研修」セキュリティIIIの講義内容を改善したとともに、平成20年度改訂に向けたセキュリティ関連コースの抜本的見直しを行い、平成19年12月に結果を得た。	A
ア） d)	人材育成・確保実行計画の作成	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」（平成19年4月13日各府省情報化統括責任者(CIO)連絡会議決定）に基づき、「IT人材育成・確保実行計画」の作成を検討又は実施した。	B+

イ 地方公共団体

①情報セキュリティ確保に係るガイドラインの見直し等

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア）	地方公共団体における情報セキュリティ対策の手引きの作成	総務省	・地方公共団体における情報セキュリティ対策の実効性確保のため、事業継続計画（BCP）、リスク分析及び外部委託管理の手引き作成の調査研究を引き続き実施中。調査結果を取りまとめた上、報告書として平成20年中に公表予定。	B

②情報セキュリティ監査実施の推進

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア）	地方公共団体における情報セキュリティ監査実施の推進	総務省	・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を、平成19年7月に実施。 ・内部監査の実施方法を学ぶ情報セキュリティ内部監査研修を全国主要都市で実施。 ・情報セキュリティ監査の実施に要する経費に対して、地方財政措置を実施。	A

③「自治体情報・分析センター」（仮称）の創設促進

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア）	「自治体CEPTOAR」への支援	総務省	・自治体CEPTOAR事務局（(財)地方自治情報センター）と今後の自治体CEPTOARの効果的な運用のあり方について意見交換を実施。	A

④職員の研修等の支援

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア）	地方公共団体職員を対象とする情報セキュリティ研修の実施	総務省	・情報セキュリティ対策の中核を担う高度な知識・技術を持つ人材育成のための研修を全国主要都市で実施。 ・インターネットを用いたe-ラーニングによる情報セキュリティ研修を実施。	A

第3章 対策実施4領域における情報セキュリティ対策の強化

第2節 重要インフラ

①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」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) a)	安全基準等の見直し	重要インフラ所管省庁	・平成19年6月に行われた指針の改定を踏まえ、重要インフラ10分野について平成19年9月末までに実施。	A
ア) b)	「安全基準等」の見直し状況等の把握及び検証	内閣官房	・第11回重要インフラ専門委員会（平成19年9月28日開催）にて提示された「2007年度重要インフラにおける「安全基準等の見直し状況の把握及び検証」について」に基づき実施。第16回情報セキュリティ政策会議（平成20年2月4日開催）において検証結果を報告。	A
イ)	各重要インフラ分野における安全基準等の浸透状況等に関する調査の実施	内閣官房 重要インフラ所管省庁	・第11回重要インフラ専門委員会（平成19年9月28日開催）にて提示された「2007年度重要インフラにおける「安全基準等の浸透状況等に関する調査」について」に基づき実施。第14回重要インフラ専門委員会（平成20年3月4日開催）において調査結果を報告。	A
ウ)	指針の見直し	内閣官房	・第12回重要インフラ専門委員会（平成19年12月3日開催）にて提示された「2007年度重要インフラにおける「指針の見直し」について」に基づき検討を実施。第14回重要インフラ専門委員会（平成20年3月4日開催）において検討結果を報告。	A
エ)	ネットワークのIP化に対応した電気通信システムの安全・信頼性確保	総務省	・ネットワークのIP化に対応した技術基準、管理基準等を盛り込むため、電気通信設備規則、電気通信事業法施行規則等の制度を改正（平成19年11月）。安全・信頼性関係基準等の関係告示について、パブリックコメントを実施（平成20年2月）。	A

②情報共有体制の強化

（ア）官民の情報提供・連絡のための環境整備

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	情報共有体制整備と機能強化	内閣官房	・CEPTOAR特性把握マップのとりまとめ、情報共有訓練及びCEPTOARも参加した官民連携による分野横断的演習を実施。	A

（イ）各重要インフラ分野における情報共有・分析機能（CEPTOAR）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)	各重要インフラ分野におけるCEPTOAR整備の推進	重要インフラ所管省庁	・新規追加3分野（水道、医療及び物流）において、平成19年度までに整備を完了。	A
イ)	「CEPTOAR特性把握マップ」のフォローアップ	内閣官房	・重要インフラ所管省庁等の協力を得て、平成19年度末現在の各CEPTOARの特性を把握するとともに、整備状況とあわせてCEPTOAR特性把握マップ(ver2)をとりまとめた。	A

（ウ）「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）の創設促進

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）創設の検討	内閣官房 重要インフラ所管省庁	・CEPTOAR代表者等から構成される「重要インフラ連絡協議会（CEPTOAR-Council）（仮称）創設に向けた検討の場」を設け、8回の会合を開催。同「検討の場」において、平成20年度以降の検討方針を「「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）の創設についての基本的な考え方」としてとりまとめた。	A

③相互依存性解析の実施

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	重要インフラ分野間の相互依存性解析の推進	内閣官房	・有識者、各重要インフラ分野の分野委員及び重要インフラ所管省庁からなる相互依存性解析検討会を設置し、検討会5回・WG7回を実施し、「相互依存性解析における視点（考え方のポイント）」を整理しつつ、「動的依存性解析」を実施した。併せて平成18年度と平成19年度に実施した解析結果を整理し「相互依存性解析報告書」としてとりまとめた。	A

④分野横断的な演習の実施

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	重要インフラ機能演習の実施	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の分野委員及び重要インフラ所管省庁からなる分野横断的演習検討会を設置し、検討会5回・WG5回を通じてシナリオ等についての議論を経て、約120名の参加を得て分野横断的な機能演習を実施。	A
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	・平成18年度に引き続き「電気通信事業分野におけるサイバー攻撃対応演習」において、平成19年11月から平成20年1月にかけて、複合的なサイバー攻撃の発生を想定した机上演習と、個別のサイバー攻撃を想定した4シナリオの演習（DDoS攻撃対応演習、DNS攻撃対応演習、IPスパム攻撃対応演習、フィッシング攻撃対応演習）を実施。	A
ウ)	各分野サイバー演習との連携	内閣官房 重要インフラ所管省庁	・情報通信分野及び航空分野における机上演習に、NISCが参加し、演習の実施手法等の知見を受けた。	A

⑤「重要インフラの情報セキュリティ対策に係る行動計画」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)	「重要インフラの情報セキュリティ対策に係る行動計画」の見直し	内閣官房	・第12回重要インフラ専門委員会（平成19年12月3日開催）より、「重要インフラの情報セキュリティ対策に係る行動計画」の見直しに向けた検討作業に着手。重要インフラ分野における情報セキュリティ対策向上の状況を把握するとともに、見直しに向けた論点整理を実施。	A

第3章　対策実施4領域における情報セキュリティ対策の強化

第3節　企業

①企業の情報セキュリティ対策が市場評価に繋がる環境の整備

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア）　a）	企業における情報セキュリティガバナンスの確立促進	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確立を促進するため、企業が参考にできるような情報セキュリティ対策に関する先進事例、情報セキュリティガバナンス構築・確立事例（ベストプラクティス）等について、調査研究を実施し、事例集のとりまとめを行う。また、民間組織による情報セキュリティ格付けの促進を後押しするため、格付け機関が満たすべき要件・基準等について調査研究を実施し、中間とりまとめを実施。 ・平成19年4月に企業が信頼性向上の取組状況を把握するためのツールとして、「情報システムの信頼性向上に関する評価指標（試行版）」を公表。また、企業における信頼性向上のための取組状況の把握と普及促進のために、信頼性ガイドラインを基にした「情報システムの信頼性向上のための緊急点検」を平成19年6月に実施。 ・現在、緊急点検結果を受けて、信頼性ガイドラインと評価指標の見直しと、評価ツールの構築に着手。平成20年度内を目途に改訂版と評価ツールを公開予定。	A
ア）　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	・ＩＳＭ－ＴＧ（Information Security Management Guideline for Telecommunications）の国際標準化の進捗動向を踏まえつつ、認証のあり方について検討を開始。	A
イ）	入札条件等の見直し	内閣官房 総務省 財務省 全府省庁	・平成19年度に実施した、内閣官房における研究の内容を踏まえ、内閣官房において今後の具体的な進め方について検討しているところ。	B
ウ）	情報セキュリティ管理を重視した情報サービスマネジメントに関する標準化の推進	経済産業省	・情報セキュリティ管理を重視した情報サービスマネジメントに関する標準化を推進するため、平成19年4月20日付けで、以下のJIS（日本工業規格）を制定。 ★JIS Q 20000-1:2007　情報技術-サービスマネジメント　第1部：仕様 ★JIS Q 20000-2:2007　情報技術-サービスマネジメント　第2部：実践のための規範	A
エ）	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	・独立行政法人情報処理推進機構において、中小企業向けの標準フォーマット策定の検討を行うべく「中小企業の情報セキュリティ対策に関する研究会」を設置し、現状調査等を実施。	A

②質の高い情報セキュリティ関連製品及びサービスの提供促進

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するリスク定量化手法についての研究	経済産業省	・情報セキュリティ対策による情報セキュリティ関連リスクの変動を定量的に把握する手法に係る調査研究を実施。	A
イ）　a）	情報セキュリティ監査制度の普及促進	経済産業省	・各種セミナー等の場を活用して、情報セキュリティ監査制度の普及活動を行うとともに、保証型監査の枠組みについて検討を実施。	A
イ）　b）	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	・独立行政法人情報処理推進機構において、「調達におけるセキュリティ要件研究会」を設置。また、そこでの意見を踏まえ、セキュリティ要件検討支援ツールを開発。 ・ＩＳＯ／ＩＥＣ１５４０８の評価・認証を受けた一部の製品（サーバ用ＯＳやデータベース管理ソフトなど）を購入した事業者について、情報基盤強化税制による取得価額の一定割合で税額控除等の優遇措置を実施。	A
ウ）　a）	情報セキュリティ対策装置の取得時における税制優遇措置	総務省	・「ネットワークセキュリティ維持税制（地方税）」により、ネットワークセキュリティ維持装置（多機能型ファイアウォール装置等）を購入した場合に、固定資産税の課税標準が圧縮される税制優遇措置実施。	A
ウ）　b）	企業の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	経済産業省 総務省	・経済産業省及び総務省において、産業競争力のための情報基盤強化税制のパンフレットをホームページ上で公開している。また、当該印刷物について、関係機関・利用者に配布している。	A
エ）	企業に係る指標の充実等	内閣官房 経済産業省	・平成19年度「情報処理実態調査」の実施に向けて、準備を開始。また、企業の指標と対比して不足する政府機関の状況に係るデータの把握のための補完調査を平成20年2月から実施。	A

③企業における情報セキュリティ人材の確保・育成

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	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)	組織におけるIT利用者向けのセルフチェックツールの機能強化等	経済産業省	・組織におけるIT利用者の情報セキュリティ対策レベルを客観的に測定するためのセルフチェックツールについて、組織管理者向けに機能を拡張し、平成20年1月に改訂。	A
ウ)	中小企業を対象とした情報セキュリティセミナーの実施	経済産業省	・独立行政法人情報処理推進機構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について、平成19年度末までに全国31箇所で開催。	A
エ)	客観的な高度IT人材評価メカニズムの構築	経済産業省	・産業構造審議会情報経済分科会情報サービス・ソフトウェア小委員会人材育成ワーキンググループ報告書（平成19年7月20日）を受け、有識者によりセキュリティ人材も含めた高度IT人材に求められるスキルについて引き続き検討する。	B
オ)	産学官協議会の設置	経済産業省	・文部科学省と連携し、産学連携人材育成パートナーシップの下、情報処理分科会を設置。これまでに2回の審議を実施。（第1回：平成19年11月15日、第2回：平成20年1月24日）	A
カ)	ファカルティ・ディベロップメントの支援	文部科学省 経済産業省	・大学における教育内容等の改善のための組織的な研修等（FD）については、大学設置基準第25条の2の他、各設置基準において規定されており、各大学においてFDの取組みが進められている。 　また、産学協同実践的IT教育促進事業から得られたノウハウを蓄積し、これを有効活用すべく、その成果のディレクトリ化を進めている。さらに、平成20年度以降、他省庁等の成果等も反映させる取組を進めていく。	A
キ)	情報処理技術者試験制度の改革	経済産業省	・情報処理技術者試験制度については、平成19年12月28日付で情報処理技術者試験規則等の一部改正を行った（平成19年経済産業省令第79号）。平成21年度から新試験を実施。	A
ク)	高度情報通信人材育成体系の開発	総務省	・企業等の情報化戦略や新たなビジネス創出を担う人材を育成するため、情報通信セキュリティ分野を含むICTマネージメント分野の実践的なPBL（Project Based Learning）教材を開発。	A

④コンピュータウイルスや脆弱性等に早期に対応するための体制の強化

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	組織の緊急対応チーム間の連携体制の強化	経済産業省	・平成19年8月に、早期警戒情報の共有ツールの稼働を開始。現時点までに、重要インフラ10分野中8分野を含む諸団体が利用し、チーム間連携の基礎を構築。	A
イ)	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	・脆弱性に係る対応を強化すべく、平成19年6月に関連ガイドラインの改定・公開を行い、平成19年8月にサイトによる早期警戒情報の提供等を開始。	A
ウ)	安全なWebサイト構築のためのガイドライン検討	経済産業省	・ウェブアプリケーション構築時に発注者が受注者（開発者）に対して示すべきセキュリティ要件に係るガイドラインとして「セキュアプログラミング講座（ウエブアプリケーション編）」を独立行政法人情報処理推進機構のHPで公表。	A
エ)	ソフトウェア等の脆弱性の重要度・優先度等に係る判断基準の整備等	経済産業省	・ソフトウェア等の脆弱性の重要度・優先度、適切な対策情報等に係る判断基準の整備等を実施するため、平成19年8月に独立行政法人情報処理推進機構において共通脆弱性評価システムをバージョン2へ移行。更に平成19年12月、JPCERTコーディネーションセンターが、脆弱性の優先度判定のためのシステムを公開。	A

第3章　対策実施4領域における情報セキュリティ対策の強化

第4節　個人

①情報セキュリティ教育の強化・推進

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア）　a)	小中高等学校における情報セキュリティ教育の推進	文部科学省	・教員向けWebサイトの作成に向け、情報モラル指導実践事例を収集するとともに、本Webサイトを通じて普及を図る予定。 ・各都道府県において、市区町村教育委員会指導主事等を対象とした情報モラル指導セミナーを平成20年3月末までに47件開催。	A
ア）　b)	ICTメディアリテラシー 育成手法の調査・開発	総務省	・開発したICTメディアリテラシー育成プログラムを公開（平成19年7月）。プログラムの普及を図り、必要な更新を実施。	A
ア）　c)	「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	・独立行政法人情報処理推進機構において、全国の小学生・中学生・高校生を対象に「情報セキュリティ標語・ポスター」の募集を行い、平成19年6月に合計38作品の大賞及び入選を発表。さらに、平成19年10月に合計44作品の大賞及び入選を発表。	A
ア）　d)	教員の情報セキュリティに関する指導力の向上	文部科学省	・「学校における教育の情報化の実態等に関する調査」（平成19年3月現在）において、情報セキュリティに関する指導を含む「教員のICT活用指導力の基準」を活用した教員のICT活用指導力の実態調査を実施。当該調査結果について平成19年7月に公表。	A
イ）　a)	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	・警察庁及び都道府県警察の協力の下、経済産業省がNPO日本ネットワークセキュリティ協会やNPO等と連携して実施している「インターネット安全教室」につき、コンテンツを充実させるとともに、本年度も引き続き全国各地で開催しており、平成19年度末までに130件開催し、のべ約6，700人が参加した。	A
イ）　b)	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件実施。 ・平成19年度は1，089件の講座を実施し、約120，000人が受講。	A
イ）　c)	サイバーセキュリティ・カレッジの実施	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・カレッジ」について、広報啓発強化月間として5月に2，511件実施するなど、重点的に実施。	A

②広報啓発・情報発信の強化・推進

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している。 ・総務省において、「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を踏まえつつ、同サイトのコンテンツ更新を図るための検討及び作成を実施。 ・総務省において、一般利用者に情報セキュリティの確保に必要な正しい知識と対策を広めることを目的とした「インターネット美化運動2007」を平成19年6月に実施。 ・総務省において、「迷惑メールへの対応の在り方に関する研究会」において、フィッシングメールへの対応を含めた迷惑メール対策についての検討を実施。 ・行政機関、教育機関、産業界が、新たな体制で情報セキュリティ対策を講じる時期に合わせ、平成19年5月に全国警察を挙げてサイバー犯罪防止のための広報啓発を重点的に実施。また、「情報セキュリティの日」に係る政府全体の取組みにあわせ、平成20年2月にもサイバー犯罪防止のための広報啓発を重点的に実施。 ・警察庁セキュリティポータルサイト（@police）にて、アプリケーション等の脆弱性や新種コンピュータウィルス発生に係る注意喚起等の広報啓発を実施。 ・警察庁及び都道府県警察の協力の下、経済産業省がNPO日本ネットワークセキュリティ協会やNPO等と連携して実施している「インターネット安全教室」につき、コンテンツを充実させるとともに、本年度も引き続き全国各地で開催しており、平成19年度末までに130件開催し、のべ約6，700人が参加した。 ・経済産業省において、WEBバナー、専用ホームページ、交通広告等を通じて、国民に情報セキュリティ対策の重要性を訴える「CHECK　PC！キャンペーン」を平成20年1月16日～3月31日まで実施。	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19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20年2月に公表。 ・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、調査委託を実施。 ・経済産業省において、独立行政法人情報処理推進機構やJPCERTコーディネーションセンターを通じて、情報システムの管理者等を対象とした不正アクセス対策、コンピュータウィルス対策等についての啓発活動を実施。 ・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として、警察庁及び都道府県警察の協力の下、NPO日本ネットワークセキュリティ協会やNPO等と連携し、全国各地で「インターネット安全教室」を開催しており、平成19年度末までに130件開催し、のべ約6，700人が参加した。	A
ア）　c)	ネットワークの不適正な利用からの被害防止対策の推進	警察庁	・ネットワーク相談対応システムにより情報提供を行っているインターネットトラブルに対する基本的な対応策について、アクセスが増加している相談の注意喚起といった、国民にその内容をより分かりやすく（する改善を実施。 ・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7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にも掲載。	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19年6月の電波利用保護旬間において、「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について各種メディア（全国紙・地方紙・業界専門紙、TVCM、ラジオスポット、電車・バス車内中吊り広告、街頭ビジョン・劇場広告、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19年5月～7月及び9月～11月に総合通信局所において電波利用機器販売店への周知啓発・指導を実施するとともに、6月、10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オークションサイト並びに12月、3月にヤフーのニュースサイトへバナー広告を実施。	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	・平成20年2月の「情報セキュリティの日」に伴う「情報セキュリティの日」功労者表彰について、平成20年2月4日に開催した第16回情報セキュリティ政策会議にあわせて表彰式を実施。 ・情報セキュリティ対策への気運を全国的に波及・浸透させ、広く官民における意識と理解を深めるための啓発活動として、平成20年1月26日から3月2日までの間、全国47の全ての都道府県において593件の関連行事を開催。	A
ウ） a）	内閣官房情報セキュリティセンター（NISC）メールマガジンの継続的発行	内閣官房	・概ね月に1回の頻度でメールマガジンを発行。	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表彰の実施	総務省 経済産業省	・平成19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、総務省情報通信政策局長表彰及び経済産業省商務情報政策局長表彰を実施。	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	・日本の情報セキュリティ政策文書である「第1次情報セキュリティ基本計画」、「セキュア・ジャパン2006」、「政府機関の情報セキュリティ対策のための統一基準」等を英訳し、NISCの英語版ウェブサイトに掲載している。政策の進捗状況を報告するため、「セキュア・ジャパン2007」、「政府機関の情報セキュリティ対策のための統一基準」及び「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」の改正部分等を新たに掲載。	A

③個人が負担感なく情報関連製品・サービスを利用できる環境整備

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開始。平成23年度からは民間の自主的な取組みとして実施予定。	A
イ）	IPv6によるユビキタス環境構築に向けたセキュリティの確保	総務省	・平成18～平成21年度の4か年計画の2年目として、少数かつ特定の利用者が存在する利用環境モデル（小規模オフィス環境等）での実証実験を実施。平成20年度に「公共機関」を想定した実証実験を行った上で平成22年3月までに総合的なセキュリティ支援サービスのためのガイドラインを作成予定。	A
ウ）	無線LANのセキュリティ対策	総務省 経済産業省	・総務省のHPにおいて、引き続き、ガイドライン「安心して無線LANを利用するために」を掲載し、その普及の推進を図っているところ。平成19年12月に当該ガイドラインの改定を行い、総務省ホームページに公開。 ・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」の冊子を改訂する際に、無線LANの安全な使い方に関するコンテンツを、国民にその内容をより分かりやすくするための見直しを実施。	A

第4章 横断的な情報セキュリティ基盤の形成

第1節 情報セキュリティ技術戦略の推進

①研究開発・技術開発の効率的な実施体制の構築

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	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連する研究開発・技術開発の実施状況の把握を開始。	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関連する研究開発・技術開発の投資効果の把握をするための評価を実施。また、その結果については今後速やかに公表する予定。	A
ウ)	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・技術開発における成果を、調達を通じ政府が活用するための方策について、平成18年度から引き続き検討を実施。	A

②情報セキュリティ技術開発の重点化と環境整備

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	・基盤としてのITを強化することに直結する中長期的目標に対して、公的研究資金を重点的に投入するための方策に関する検討を開始するため事前準備を行っており、平成19年度内に検討を開始。	A
ア) b)	次世代バックボーンに関する研究開発	総務省	・平成21年度中に技術を確立することを目指し、要素技術の検証や要素間連携の検討等を推進。	A
ア) c)	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～平成21年度の4か年計画の2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・実験を実施。平成22年3月までに実装可能な技術を確立する予定。	A
ア) d)	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（平成17～21年度）等を実施しているところ。	A
ア) e)	新世代のアクセス制御技術の研究開発	経済産業省	・既存の情報システムを前提とした従来の技術にとらわれない新世代のアクセス制御技術、認証技術、ソフトウェア技術等をテーマとした事業を選定し、平成18年度に引き続き研究開発を実施。	A
ア) f)	柔軟かつ確実な情報管理を達成するための情報処理・管理技術の開発	経済産業省	・情報の所有者・管理者が情報の開示の是非とその範囲を自ら決定し、それを確実に達成できるようにすること等を目的とした情報セキュリティ技術をテーマとした事業を選定し、平成18年度に引き続き研究開発を実施。	A
ア) g)	フェイルセーフな情報セキュリティ技術の研究開発	経済産業省	・実際にシステム障害が発生した場合、あるいは情報の一部が漏洩したような場合でも、一定程度の安全性を確保できるような技術やフェイルセーフの概念に基づいたソフトウェアの設計・開発手法をテーマとした事業を選定し、平成18年度に引き続き研究開発を実施。	A
ア) h)	情報セキュリティに関するリスク定量化手法についての研究［再掲］	経済産業省	再掲	
ア) i)	情報漏えい対策技術の研究開発	総務省	・平成19～平成21年度の3か年計画の初年度として、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、情報の来歴管理等の高度化・容易化に関する研究開発に着手。平成22年3月までに実装可能な技術を確立する予定。	A
ア) j)	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、平成19年度から体制を整備し、初期的な検討等を開始。	A
ア) k)	ダイナミックネットワーク技術の研究開発	総務省	・平成32年までに新世代ネットワークの実現を目指して、情報の伝達効率の飛躍的向上や故障時の自動復旧を可能とするダイナミックネットワークの基礎技術を確立するため、基本設計・試作を実施。	A
ア) l)	IP化の進展に対応した通信端末のセキュリティ機能の確保の推進	総務省	・8月に「IP化時代の通信端末に関する研究会」報告書を取りまとめ、IP化時代の通信端末にはセキュリティ機能等の安全・信頼性の確保が必要と提言。 ・同報告書を受け、9月より通信端末の技術的要件の検討を開始し、平成20年3月26日に、情報通信審議会において答申。	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	・短期的目標設定のなされている研究開発・技術開発について、官民での取組状況を把握し、さまざまな領域において過小投資、過大投資が発生しないよう投資ポートフォリオに関する分析を開始。	A
イ) b)	高セキュリティ機能を実現する次世代ＯＳ環境の開発［再掲］	内閣官房 内閣府 総務省 経済産業省	再掲	

イ） c)	電子政府に用いられるＯＳのセキュリティ品質の評価尺度の確立［再掲］	内閣官房	再掲	
イ） d)	デジタルフォレンジック の確立に向けた技術開発等の推進	警察庁	・プログラム上の脆弱性等の各種技術情報の提供を受けるなど、民間企業等との技術協力を推進。 ・警察における情報技術の解析に係るツール等の開発を推進し、平成２０年３月、開発の成果を部内において報告。	A
イ） e)	高い保証レベルを有する情報システムの開発及び評価	防衛省 経済産業省	・防衛省は、平成１８年度に引き続き、情報技術セキュリティ評価基準ＩＳＯ／ＩＥＣ１５４０８で規定される評価保証レベルＥＡＬ６相当を満足する情報システム及び評価方法論(Evaluation Methodology)の研究を平成２０年度まで実施。また、防衛省と独立行政法人情報処理推進機構との間で、防衛省が取得したセキュリティ評価技術の新たな国際的な評価基準への適用に関する事項について研究協力を実施。	A
イ） f)	ネットワークのオールIP化に対応した重要通信の運用技術の確立	総務省	・ネットワークのIP化等に対応した重要通信の運用技術について、国内外の運用手法の調査を実施。また、平成１９年１１月より重要通信の高度化の在り方に関する研究会を開催。平成２０年5月目途に電気通信事業においてIP化されたネットワーク等における重要通信の高度化の在り方についてとりまとめる予定。	A
イ） g)	情報セキュリティ関連製品・サービスの新しい傾向に関する調査	内閣官房 総務省 経済産業省	・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・設計に関する調査及びその調査結果の周知の方法ついて検討を実施。	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	・民間での技術開発が行われている領域については、民間の自主性に任せ、民間での取組みが乏しい萌芽的な研究については、公的研究資金を投入する等のポートフォリオ分析の実施に向けて事前準備をおこなっており、平成１９年度内に分析を開始。	A
ウ） b)	高信頼性端末の電子認証基盤の研究開発	経済産業省	・ＴＰＭ（Trusted Platform Module）を搭載したＰＣ間で、各ＰＣの信頼性を確認しつつ、各ＰＣ間の途中経路が保護されていない状態でも安全に情報交換する手法について研究開発を実施。	A

③「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」のテーマ検討	内閣官房 内閣府	・総合科学技術会議と情報セキュリティ政策会議の連携の下、グランドチャレンジ型に相応しいテーマについて具体的な検討を開始。	A

第4章　横断的な情報セキュリティ基盤の形成

第2節　情報セキュリティ人材の育成・確保

①多面的・総合的能力を有する実務家・専門家の育成

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	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年度の高度セキュリティ人材育成プログラムを開発・実施する拠点形成の支援について、平成19年5月に国公私立大学長宛に公募を行った結果、10件（国立6件、公立1件、私立3件）の申請があり、「先導的情報セキュリティ人材育成推進委員会」（委員長：筧捷彦　早稲田大学理工学部教授）の審査を経て、平成19年9月に2件の教育プロジェクトが選定された。	A
イ)	組織におけるIT利用者向けのセルフチェックツールの機能強化等【再掲】	経済産業省	再掲	
ウ)	客観的な高度IT人材評価メカニズムの構築【再掲】	経済産業省	再掲	
エ)	産学官協議会の設置【再掲】	経済産業省	再掲	
オ)	ファカルティ・ディベロップメントの支援【再掲】	文部科学省 経済産業省	再掲	
カ)	情報処理技術者試験制度の改革【再掲】	経済産業省	再掲	
キ)	情報通信人材研修事業支援制度【再掲】	総務省	再掲	
ク)	高度情報通信人材育成体系の開発【再掲】	総務省	再掲	

第4章　横断的な情報セキュリティ基盤の形成

第3節　国際連携・協調の推進

①国際的な安全・安心の基盤づくり・環境の整備への貢献

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	国際協調・貢献に係る検討	内閣官房 全府省庁	・内閣官房（NISC）において「情報セキュリティの国際協調・貢献に向けた取組み（平成19年10月3日情報セキュリティ政策会議決定）」策定。今後、速やかな遂行を図る。	A
イ)	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 全府省庁	・内閣官房（NISC）や各府省庁から、情報セキュリティに係る問題を議論するG8、OECD、APECの作業部会、早期警戒・監視・警報ネットワーク、FIRST等の国際会合に参加し、諸外国の政府機関・民間企業等との連携強化を推進。 ・諸外国の情報セキュリティ対策の動向を精査するため、NISCにおいて調査研究を実施。 ・サイバーセキュリティ日米会合を平成19年8月に開催し、情報セキュリティ政策についての情報交換、知見の共有、議論を行うとともに、より高い頻度で定期的な会合を行うことに同意するなど、日米の政策対話を強化。	A
ウ)	国際的なPOC機能としてのプレゼンスの明確化	内閣官房	・NISCの英語版ウェブサイトを構築し、NISCの我が国政府における位置づけ、機能、政策等を掲載。 ・NISCが内閣官房に設置された意義について、国際会合やサイバーセキュリティ日米会合等の二国間の政策対話を通じて引き続き解説し、NISCが府省庁横断的な情報セキュリティ案件や諸外国からみてコンタクト・ポイントが明確でない情報セキュリティ案件に係るPOC機能を日本政府内で有することを周知。	A
エ)	情報セキュリティ政策に関する国際的な広報活動の推進	内閣官房	・NISCの英語版ウェブサイトにおいて、政府全体の情報セキュリティ政策のアップデートや、その中核を担うNISCの位置づけと機能等を解説。 ・現在、国際機関等のウェブサイトに、「セキュア・ジャパン2007」の他、「重要インフラの情報セキュリティ対策に係る行動計画」及び「政府の統一基準」の改正部分について英訳資料を掲載するための取組みを実施。 ・平成19年10月にプサン（韓国）で開催されたARF（ASEAN Regional Forum)サイバーテロセミナーに出席し、NISCの取組みを発表。今後開催が予定されているバーチャルWGに参加する予定。 ・平成19年10月に開催された重要情報インフラ防護に関する国際会合であるMeridian Conferenceにおいて、重要インフラに関する我が国の取組を発表。	A
オ)	国際的なセキュリティ文化実現のための取組み	内閣官房	・日本の情報セキュリティ政策文書である「第1次情報セキュリティ基本計画」、「セキュア・ジャパン2006」、「政府機関の情報セキュリティ対策のための統一基準」等を英訳し、NISCの英語版ウェブサイトに掲載している。政策の進捗状況を報告するため、「セキュア・ジャパン2007」、「政府機関の情報セキュリティ対策のための統一基準」及び「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」の改正部分等を新たに掲載。	A
カ)	国際的な意識・リテラシー向上のための取組み	内閣官房 総務省 経済産業省	・現在、内閣官房（NISC）において情報セキュリティの国際協調・貢献に向けた基本方針を策定中であり、基本方針策定後、国際的な意識・リテラシー向上のための取組みににについても具体化を図る。 ・サイバーセキュリティ日米会合を平成19年8月に開催し、多国間等の枠組みを利用した国際的な意識の向上に向けた取組みについて意見交換を実施。 ・平成19年4月のAPEC TEL（電気通信・情報作業部会）に際して開催されたAPEC TEL/OECD合同マルウェア・ワークショップにて、経済産業省及び総務省の出席者から、ボットネット対策を中心に我が国における情報セキュリティ政策を紹介。 ・総務省において、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金により、平成19年12月に「ブロードバンドネットワーク技術と情報セキュリティ」研修を実施。 ・総務省において、財団法人海外通信・放送コンサルティング協力（JTEC：Japan Telecommunications Engineering and Consulting Service）への補助金による事業の一環として、平成20年1月に、情報セキュリティ技術研修を実施。 ・平成19年10月に開催されたAPEC TEL（電気通信・情報作業部会）において、NISC及び総務省による情報セキュリティに関するワークショップの開催を提案し、了承された。平成20年3月に東京で開催されたAPEC TELにおいてワークショップを開催し、我が国における情報セキュリティ政策を紹介。 ・総務省において、平成20年3月に東京で開催されたAPEC TELに際して開催されたAPEC TELボットネット・ワークショップで、ボットネット対策に関する我が国における情報セキュリティ政策を紹介。	A

②情報セキュリティ領域での我が国発の国際貢献

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	ベストプラクティスの国際的な発信・普及	内閣官房 全府省庁	・内閣官房（NISC）において「情報セキュリティの国際協調・貢献に向けた取組み（平成19年10月3日情報セキュリティ政策会議決定）」を策定。今後、速やかな遂行を図る。 ・OECDの重要情報インフラ保護に関するベストプラクティスをまとめることを目的とするケーススタディに参加し、日本の取組みを含めた7カ国のボランティア国の政策を取りまとめた報告書の作成に貢献。当該報告書及びこれを参照して作成される予定のガイドラインはOECD加盟国のみならず非加盟国に対しても公表される。 ・平成19年10月に開催されたARF（ASEAN Regional Forum)サイバーテロセミナーに出席し、NISCの取組みを発表。 ・平成19年10月に開催された重要情報インフラ防護に関する国際会合であるMeridian Conferenceにおいて、重要インフラに関する我が国の取組を発表。	A
イ)	海外のCSIRTの体制強化の支援	経済産業省	・JPCERTコーディネーションセンターを通じて、アジア太平洋地域におけるCSIRT構築支援に向け、各国関連組織との連携体制を強化するため、平成19年9月末までにASEAN諸国の関係諸機関の能力向上やCSIRT構築に向けた情報収集等7カ国を訪問。平成20年3月に、6か国計30名の技術者に対する研修を実施。	A
ウ)	アジア太平洋地域等でのインターネット定点観測情報の共有促進	経済産業省	・JPCERTコーディネーションセンターを通じて、アジア太平洋地域におけるインターネット定点観測情報の共有促進に向けて、各国関連組織との連携体制の強化に着手。平成20年3月のAPCERT年次総会にて、アジア太平洋広域ネットワーク観測データ可視化システムのコンセプトや今度の展開につき発表。	A
エ)	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	・攻撃手法の分析能力の強化及び分析結果情報の共有を促進すべく、平成19年10月にワークショップを開催。	A
オ)	電気通信事業における情報セキュリティマネジメントガイドラインの国際規格化	総務省	・ISM－TG（Information Security Management Guideline for Telecommunications）について平成20年2月にITU-T（International Telecommunication Union Telecommunication Standardization Sector））において勧告化が決定。また、同勧告について、ISO（International Organization for Standardization）／IEC（International Electrotechnical Commission）においても国際標準規格化すべく、最終投票準備中。	A

第4章 横断的な情報セキュリティ基盤の形成

第4節 犯罪の取締り及び権利利益の保護・救済

①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

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア) a)	サイバー犯罪の取締りのための技能水準の向上	警察庁	・平成19年7月、警察大学校において、「サイバー犯罪取締・対策専科」を実施。 ・平成19年9月、関東管区警察学校において、「情報セキュリティ・アドバイザー専科」を実施。 ・平成19年11月及び平成20年1月、関東管区警察学校において、「サイバー犯罪捜査技術専科」を実施。 ・サイバー犯罪に適切に対処するため、部内外（海外研修を含む）におけるOS及びネットワークに関する技術並びに電子機器及びコンピュータウィルス等の解析に係る各種研修を推進。	A
ア) b)	サイバー犯罪の取締りのための体制の強化・整備	警察庁	・都道府県警察においては、サイバー犯罪対策に従事する体制を強化する等サイバー犯罪の取締りのための体制を強化。	A
ア) c)	サイバー犯罪の取締りのための捜査・解析用資機材の充実・強化	警察庁	・平成20年2月、アクセス記録の解析、コンピュータウィルス等の動作検証、電磁的記録の復元等を行うための資機材の整備を完了。	A
ア) d)	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，ハイテク犯罪に適切に対処すべく，サイバー犯罪条約を締結するための法整備等を推進する（「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」を第163回国会に提出（現在，国会において審議中）。）。	―
ア) e)	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	・都道府県警察等において、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、サイバーテロ対策の意識の向上につながる啓発活動を実施。	A
ア) f)	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19年4月、同年11月及び平成20年2月、G8ハイテク犯罪サブグループ会合に出席。 ・平成19年9月、ICPOサイバー犯罪国際会議に出席。 ・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20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19年10月に開催。 ・平成19年10月、警察庁・FBIサイバー犯罪ワーキング・グループにおいて、サイバー犯罪に関する最近の情勢、捜査手法や証拠解析の方法等について、意見交換を実施。	A
ア) g)	中央当局制度 を活用した国際捜査共助の迅速化	法務省	・平成19年12月1日，我が国と中華人民共和国との間で刑事共助条約の署名が行われ，現在，国会の承認を得るなどの所要の手続を進めているところ。その他，香港及びロシア連邦との間で締結に向けて，警察庁及び外務省などの関係省庁と共に交渉中。	B
ア) h)	重要無線通信妨害対策の強化	総務省	・電波利用秩序維持のため遠隔操作による電波監視施設等の更新及び性能向上並びに混信が恒常的に発生している地域へ、平成19年度、DEURASセンサ19式等の整備を実施。 ・電波利用の多様化、高度化、周波数逼迫等への対応として、デジタル復調のためのスクランブル推定技術の検討及び電波発射源可視化装置の開発を実施し、電波発射源可視化装置については、平成19年度末に関東総合通信局に実用機を配備。また、デジタル復調のためのスクランブル推定技術についても、技術開発が終了し、一部について導入済み。また、混信その他の妨害に係る原因究明を強化するため、平成19年4月、関東総合通信局に電波障害分析課を設置。	A
ア) i)	デジタルフォレンジックに係る知見の集約・体系化等の推進	警察庁	・情報技術解析に係る全国の知見の集約・体系化の作業を進め、平成20年3月、マニュアルを作成。 ・国内関係機関とのデジタルフォレンジックに関する情報共有・情報交換を目的としたデジタルフォレンジック連絡会第3回及び第4回会合を開催。	A
イ) a)	サイバー空間における権利利益の保護・救済のための基盤に係る調査研究	内閣官房	・サイバー空間における権利利益の保護・救済のための基盤に係る調査研究を実施し、内閣官房（NISC）のホームページにおいて公表。	A
イ) b)	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	・総務省として、業界団体によるWebサイト等を通じた同法及び関係ガイドラインの周知を支援しており、業界団体と共同でプロバイダ向け説明会を実施。	A

②サイバー空間の安全性・信頼性を向上させる技術の開発・普及

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	サイバーテロ対策に係る大学との共同研究の推進	警察庁	・ファイヤーウォールから集約されたログ等の分析等サイバー攻撃の予兆把握、発生の早期検知等に関して、大学と共同研究を推進。研究成果は、ログ等の分析プログラムの改良に随時反映。	A

第5章 政策の推進体制と持続的改善の構造

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

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	内閣官房情報セキュリティセンター(NISC)の強化	内閣官房	・内閣官房情報セキュリティセンター(NISC)において、官民からの人材活用を継続的に進め、平成19年度末に68名の体制となった。 ・政府機関統一基準に基づくPDCAサイクルの確立のため、平成19年6月14日及び平成20年2月4日に政府機関統一基準を改訂したほか、平成19年8月3日及び12月12日に、府省庁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等を公表した。また、電子政府の情報セキュリティ強化のための対応として、平成19年7月20日にはJRE等を利用する政府機関の公開情報システムに係る緊急調査の結果を公表するなど、第2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、平成19年10月3日に「我が国の情報セキュリティ分野における国際協調・貢献に向けた取組み」を情報セキュリティ政策会議決定とした。	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、情報セキュリティセンター(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
ウ)	潜在的に大きなリスク等への政府としての対処方法のあり方の検討	内閣官房	・西暦2000年問題(Y2K問題)において実施された官民の対応及びその経験から将来に向けて学ぶべき事項について調査を実施。 ・当面、従来の政府の体制では解決が難航されると想定される地上デジタル放送への対応に関して、全政府横断的な問題として取り組むための関係省庁連絡会議を平成19年9月に設置。	A

(2) 各府省庁の強化

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、これまでの情報セキュリティ対策とその成果を踏まえ、各府省庁の協力のもと、「政府機関統一基準」の改訂を実施(平成19年6月、平成20年2月)。また、各府省庁等担当者による政府機関統一基準に係る勉強会を引き続き実施するとともに、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)	情報セキュリティ分析部門(仮称)の創設に向けた検討	経済産業省	・平成19年7月に独立行政法人情報処理推進機構において、「情報セキュリティ分析ラボラトリー準備室」を設置し、情報セキュリティ分析部門(仮称)の創設に向けた検討を行った結果、平成20年4月から「情報セキュリティ分析ラボラトリー」として正式に設立。	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、「IT重点計画－2007」（平成19年7月26日IT戦略本部決定）に「セキュア・ジャパン2007」の内容を盛り込んだ。 ・経済財政諮問会議との連携を図り、「経済財政改革の基本方針2007」（平成19年6月19日）に「セキュア・ジャパン2007」の内容を盛り込んだ。 ・総合科学技術会議情報通信PTにおいて、「セキュア・ジャパン2007」等との整合性も踏まえつつ、関係省庁の研究開発のフォローアップを実施。	A

第5章 政策の推進体制と持続的改善の構造

第3節 持続的改善構造の構築

(1)「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	・「セキュア・ジャパン2007」の進捗状況について、半期毎に調査を実施。上半期の進捗状況については、第14回情報セキュリティ政策会議に報告・公表した。年間の進捗状況については、平成20年4月の公表に向けて、作業を実施。 ・第14回情報セキュリティ政策会議において、平成19年度末に実施する評価等の基本方針について報告・公表。当該方針を踏まえ、かつ、上記進捗状況調査の内容等を踏まえ、評価作業を実施。その結果について、平成20年4月に公表予定。	A
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	・基本計画の実現に向け、内閣官房において、具体的目標の設定を平成19年8月の情報セキュリティ政策会議において実施すると共に、作業方針を平成19年10月の情報セキュリティ政策会議において策定。	A
ウ)	「重要インフラの情報セキュリティ対策に係る行動計画」の見直し〔再掲〕	内閣官房	再掲	

(2) 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	・現時点において、新たなリスク要因や想定し得なかった事故といった、計画の見直しが必要になるような情勢の変化は無かった。	A

(3) 評価指標の確立

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確立	内閣官房 総務省 経済産業省	・内閣官房及び各府省庁では、第13回情報セキュリティ政策会議（平成19年4月23日）に報告した「2006年度の情報セキュリティ政策の評価等」の内容もふまえつつ、情報セキュリティ政策を推進。 ・第14回情報セキュリティ政策会議において、平成19年度末に実施する評価等の基本方針について報告・公表。当該方針を踏まえ、評価作業を実施。その結果について、平成20年4月に公表予定。 ・平成18年度に実施した「電気通信事業分野におけるサイバー攻撃対応演習」において検討した評価指標について、平成19年度の同施策において活用し、改善等の検討を実施。	A

別添2

平成20年度情報セキュリティ関連予算について

内閣官房情報セキュリティセンター

平成２０年度予算のうち、情報セキュリティ関連のものは次のとおり。

１　要求額

○ 平成２０年度予算額　　２９，９４０百万円

○ 予算額推移（平成２０年度は概算要求額）

	平成１６年度	平成１７年度	平成１８年度	平成１９年度	平成２０年度
当初予算	２６７億円	２８８億円	３１９億円	３００億円	２９９億円
補正予算	―	―	―	―	―
合　　計	２６７億円	２８８億円	３１９億円	３００億円	２９９億円
		⇒	⇒	⇒	⇒
		7.9%増	10.8%増	6.0%減	0.2%減

（注）通常のシステム管理一般の中でセキュリティ対策を行っているなど、情報セキュリティ関連予算のみを取り出すことが困難なものは除く。

なお、平成２０年度のＩＴ関係予算額は１２，１６６億円であり、情報セキュリティ関連予算はその２．５％を占めることになる。
（平成１９年度は２．４％、平成１８年度は２．４％、平成１７年度は２．２％、平成１６年度は２．０％）

２　施策の内訳

各施策を第１次情報セキュリティ基本計画に掲げる対策実施領域別に分類した結果は以下のとおり。

分類	平成１８年度（単位：百万円）	平成１９年度（単位：百万円）	平成２０年度（単位：百万円）
１-１政府機関（政府機関統一基準遵守に係るシステム構築関係）	２０，７１５	１８，１１３	１７，１６４
１-２政府機関（政府機関統一基準遵守に係る体制整備関係）			５１７
１-３政府機関（政府機関統一基準遵守に係るその他）			３４３
２　政府機関（１以外）		８４８	２，７１０
３　地方公共団体		７６	１０５
４　重要インフラ	１，７２５	４６０	４３３
５　企業	３，５５３	１，４８２	１，５８１
６　個人	４１	１，５２１	２，５２４
７　横断的な基盤の形成	５，８８４	７，５０２	４，５６３

３　府省庁別予算額

各府省庁別の予算額は以下のとおり。

府省庁名	平成１８年度予算額（単位：千円）	平成１９年度予算額（単位：千円）	平成２０年度予算額（単位：千円）
内閣官房	３５３，４１６	８６７，６０６	１，３１２，５３７
内閣法制局	６，８３２	７，７４３	７，７４３
人事院	２１，１０５	２８，９４４	２３，４１２
内閣府	１６６，７０２	１５６，０８３	１５４，８０３
宮内庁	４０，７９９	２４，９２３	１８，３７１
公正取引委員会	３０，６１９	３６，５４９	３３，６４９
警察庁	１，２４４，３３３	１，３３４，８８４	１，４３６，６５７
防衛省	１２，７９６，４４６	１０，９０９，４５１	１０，０６１，１１５
金融庁	１５２，５８０	１３９，２４５	９９，０５０
総務省	７，２４３，３２５	５，９４１，０７０	４，８８２，１３１
法務省	１４８，７７６	５３９，３７５	６０９，９８３
外務省	２，７０２，６９４	２，９５９，２８６	３，３５５，０４９
財務省	９１７，６４０	７３６，０９３	１，０３８，９７４
文部科学省	６８２，６２６	６５４，８８０	１，５３１，９０７
厚生労働省	５５３，７１９	６５，４２６	７６，６８９
農林水産省	２７３，５６１	５１６，８４６	２７６，０３５
経済産業省	３，８６２，４０３	４，４４１，７５８	４，５６０，４４６
国土交通省	５９７，１４２	４６６，４７３	３６６，０９１
環境省	１２３，５９８	１７４，２６２	９５，８２７

合計	３１，９１８，３１６	３０，０００，８９７	２９，９４０，４６９

政府機関の対策実施状況報告（２００７年度）の概要

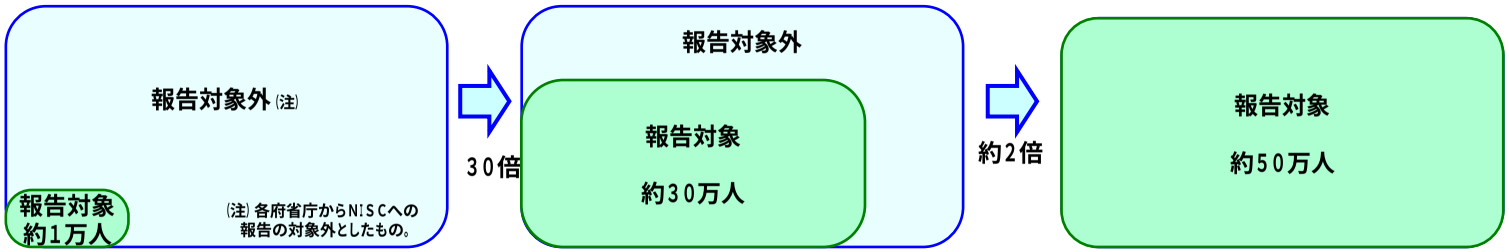
別添3

1　対策実施状況報告の実施目的

政府機関の情報セキュリティ対策は、「２００９年度初めには、すべての政府機関において政府機関統一基準が求める水準の対策を実施していることを目指す」（第１次情報セキュリティ基本計画）ことが目標とされている。
この**目標を達成するため、政府機関全体としての情報セキュリティ対策を推進する観点から、各府省庁の対策の実施状況をＮＩＳＣにおいて把握**。

2　２００７年度の報告の範囲

２００７年度は、目標達成のための中間地点と位置づけ、**２００８年度に全ての対象を報告することを明確化**するとともに、２００７年度は**できるかぎり多くの対象に係る対策実施状況の報告を求めた（前年度比約３０倍）。**
（２００７年度の報告対象については組織の規模や繁忙期等に配慮し、各府省庁から事前に提示された対象範囲とした。）



3　報告の概要及び２００８年度に向けた課題

報告の概要

- 政府機関全体で約３０万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、各府省庁が報告対象とした者のうち状況が把握できた者の割合を示す**把握率は全府省庁平均で約９３％、実施率は全府省庁平均で約９３％**、到達率については、**１００％の職員が実施した遵守事項の割合では約６４％、９０％の職員が実施した遵守事項の割合では約８２％**であった。
- 一定の成果が見られるが、なお不十分な点があり、第一次基本計画の最終年度に向けて、取り組むべき課題が依然として残っている

２００８年度に向けた課題

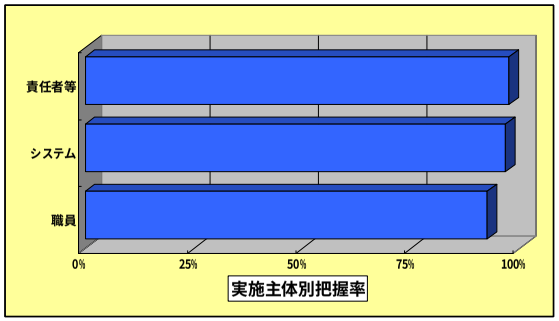
- 第１次基本計画の目標を達成するためには、政府全体として「**情報セキュリティ対策の教育**」、「**格付け・取扱い制限に係る措置**」、「**情報システムの台帳整備**」等の課題が残っている。これらのほとんどについては、前回（２００６年度）からの課題でもあり、改善に向けた取組みを加速する必要がある。
- 一方、前回（２００６年度）に課題とされた「**安全区域内における職員識別の徹底**」等については、各府省庁とも改善がみられている。
- 今後、教育の実施など十分進んでいない遵守事項について各省庁はその改善に努めるとともに、ＮＩＳＣにおいてはその実施状況をフォローし、必要な協力を行う必要がある。

政府機関の対策実施状況報告（２００７年度）の評価結果【実施主体ベース】

１　把握率

全府省庁の平均把握率

９３．４％



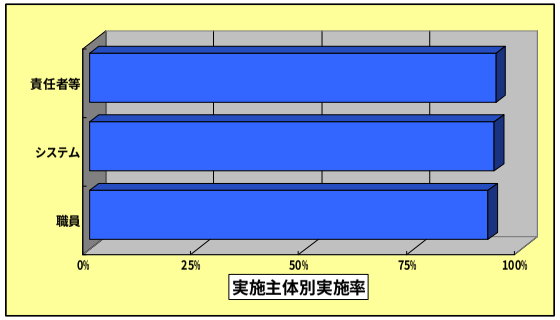
① 昨年度比で３０倍と大幅に報告対象が増えた中、平均把握率は約９３％となっており、多くの省庁では対策実施状況が把握できている結果であった。

② 来年度は全対象であること、今年度は対象を各省庁が事前に設定した範囲内であったこと、特に職員の把握率が低いことから、来年度に向け、把握率の改善手段をあらかじめ検討する必要がある。

２　実施率

全府省庁の平均実施率

９３．４％



③ 平均実施率は約９３％となっており、責任者等が高く、システム担当、職員の順に低い結果であった。

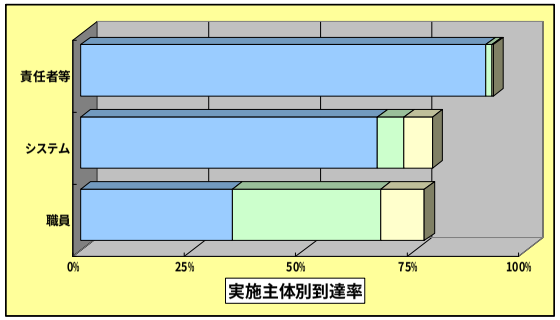
④ 情報セキュリティ対策について組織的な責務を果たすべき責任者等の実施率が１００％に満たないことは問題であり、職員についても実施率が低い状態の改善が必要である。

３　到達率

全府省庁の平均到達率

１００％実施した割合	６４．１％
９５％以上実施した割合	７５．８％
９０％以上実施した割合	８１．７％

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



⑤ 到達率でみると、責任者等に比べシステム担当や職員が低くなる傾向が顕著に現れた。

⑥ これは職員については、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、責任者等やシステム担当と比して１００％達成に困難な面があるためだが、万一の事故防止のためには日々の取り組みが重要であり、到達率向上の努力が必要である。
一方、責任者等やシステム担当については、日常的なものは少なく、早急に１００％を達成する必要がある。

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、許可権減車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（２００７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　情報セキュリティ対策の教育

[統一基準2．2．1]

全府省庁の平均実施率

84．2%

遵守事項	実施率
(1)教育の実施	84．1%
(2)教育の受講	84．8%

遵守事項別実施率

①毎年度1回以上実施すべき教育の計画策定や着任・異動後3ヶ月以内に実施すべき教育の計画策定が不十分。
　計画がなされていても受講状況の把握や未受講者への受講指導の徹底が不十分。

②職員による教育受講が不十分である。

2　格付け・取扱い制限に係る措置

[統一基準3．2．1～3．2．6]

全府省庁の平均実施率

89．7%

遵守事項	実施率
(1)情報の作成と入手	87．3%
(2)情報の利用	96．6%
(3)情報の保存	87．7%
(4)情報の移送	86．3%
(5)情報の提供	90．6%
(6)情報の消去	96．5%

遵守事項別実施率

③情報の作成と入手時において、情報の格付けの実施や格付けの明示等の実施が不十分である。

④　情報の移送、情報の提供時において、管理者に対して行うべき許可申請、届出が不十分である。

3　情報システムの台帳整備

[統一基準4．3．1（5）]

全府省庁の平均実施

77．9%

⑤　情報システムが扱う情報や当該情報の格付けを含む事項を記載した情報システムの台帳整備が不十分。

4　安全区域内における職員識別の徹底

[統一基準5．1．1（4）]

全府省庁の平均実施率

93．2%

⑥　安全区域内における職員識別の徹底については、昨年度は課題とされたが、昨年に比べ、安全区域内の職員識別の徹底について改善がみられる。

○　今後、教育の実施など十分進んでいない遵守事項について各省庁はその改善に努めるとともに、NISCにおいてはその実施状況をフォローし、必要な協力を行う必要がある。

(参考1) 報告対象範囲

2007年度は、2008年度に全対象を報告対象とするためのロードマップとして位置づけ、組織の規模や事務繁忙期等に配慮し、各府省庁から事前に提示された範囲を報告対象とした。

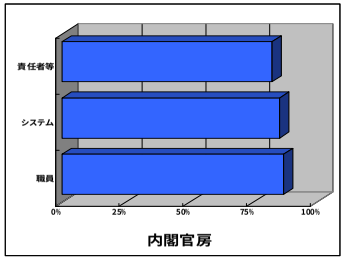
	2007年度の把握率	2007年度に報告対象とした範囲		2008年度の報告対象範囲
		職員	情報システム	
内閣官房	78.2%	すべて対象	すべて対象	すべての職員・すべての情報システムが報告対象
内閣法制局	100%	すべて対象	すべて対象	
人事院	100%	すべて対象	すべて対象	
内閣府	91.4%	本府（地方支分部局を除く）：すべて対象	すべて対象	
宮内庁	100%	係長相当職以上で単独でパソコンを使用する職員	前回対象4情報システム類型（※）	
公正取引委員会	96.7%	本局：課室長級以上及び各課室総括担当職員 地方機関：課室長級以上及び総務課職員	前回対象4情報システム類型＋主要情報システム	
警察庁	100%	本庁内部部局：すべて対象 附属機関及び地方機関：課長相当職以上	前回対象4情報システム類型＋インターネットに接続された情報システム	
金融庁	100%	課長補佐相当職以上	前回対象4情報システム類型＋主要情報システム	
総務省	93.6%	すべて対象	すべて対象	
法務省	100%	本省（外局含む）：すべて対象 所管各庁：本省課室長相当職以上	本省において所管しているすべての情報システム	
外務省	100%	すべて対象（ただし、在外公館の現地職員は除く）	前回対象4情報システム類型＋主要情報システム＋その他要保護情報を扱う情報システム	
財務省	100%	本省（外局含む）：すべて対象 地方機関（税関、国税局、財務局）：すべて対象 地方機関（税務署）：各署統括官（課室長相当職）以上	前回対象4情報システム類型＋主要情報システム	
文部科学省	56.4%	係長相当職以上	前回対象4情報システム類型＋主要情報システム	
厚生労働省	80.4%	本省（外局含む）：すべて対象 地方機関等：政令職以上	すべて対象	
農林水産省	100%	本省：すべて対象 地方出先機関：一部対象外	すべて対象	
経済産業省	95.9%	行政職俸給表（一）における6級以上（指定職含む）	すべて対象	
国土交通省	100%	本省（外局含む）：課室長以上 地方機関：本省課室長相当職以上	前回対象4システム類型＋主要情報システム	
環境省	83.8%	すべて対象	すべて対象	
防衛省	98.8%	すべて対象	すべて対象	

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

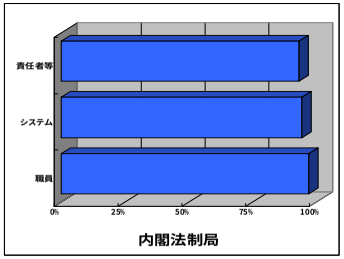
（※前回対象4情報システム類型：電子申請システム、文書管理システム、府省庁LANシステム、最適化対象システム）

(参考2) 各府省庁の対策実施状況報告 (2007年度) の集計結果

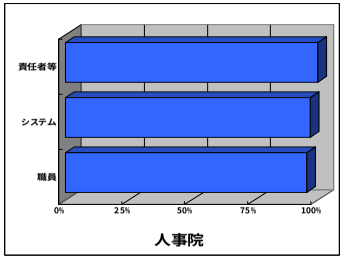
○ 実施率



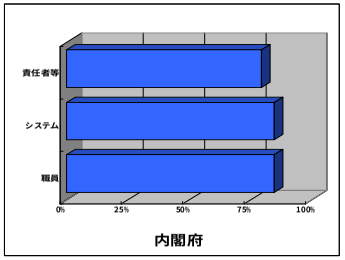
内閣官房



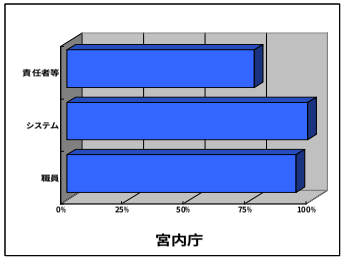
内閣法制局



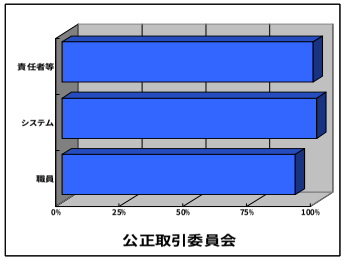
人事院



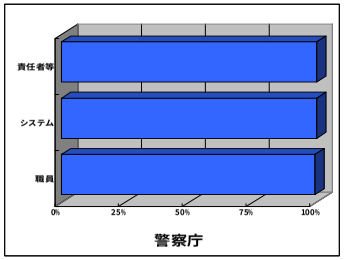
内閣府



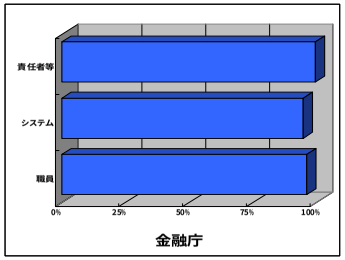
宮内庁



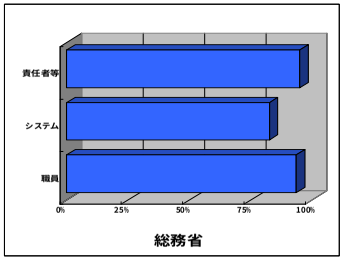
公正取引委員会



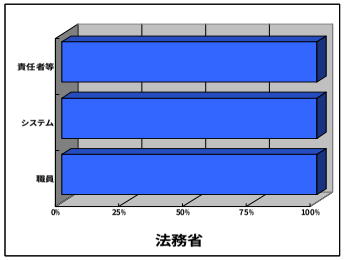
警察庁



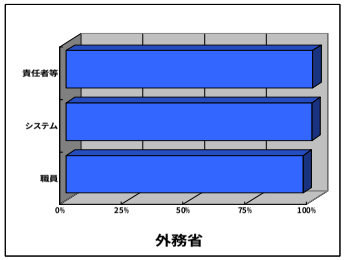
金融庁



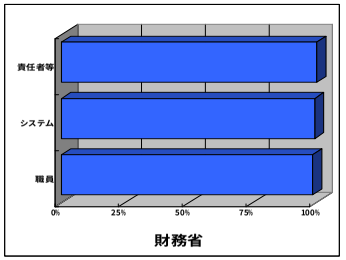
総務省



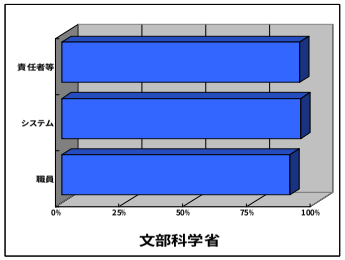
法務省



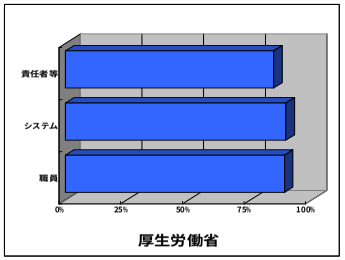
外務省



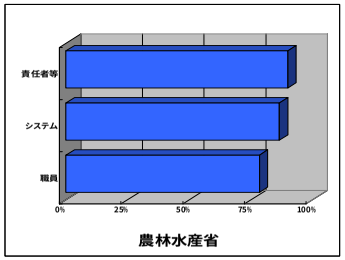
財務省



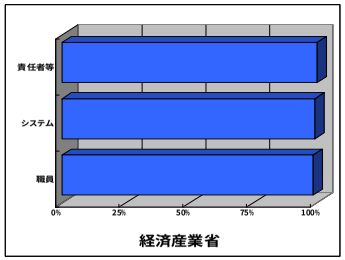
文部科学省



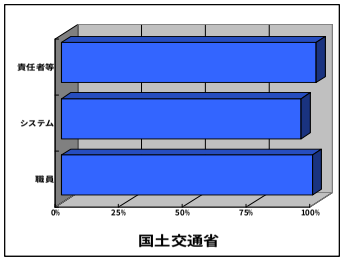
厚生労働省



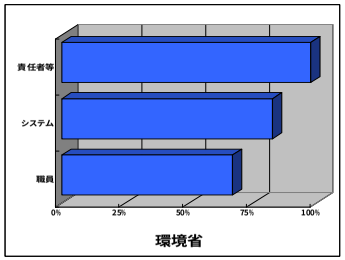
農林水産省



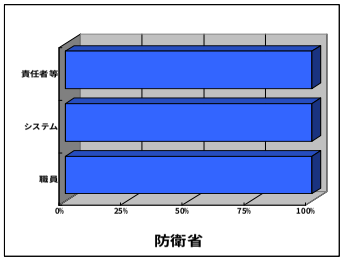
経済産業省



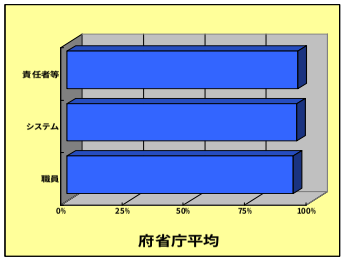
国土交通省



環境省



防衛省

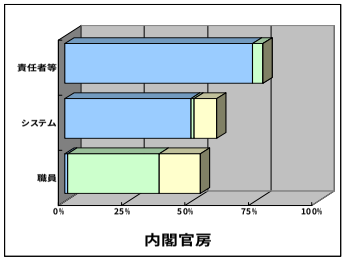


府省庁平均

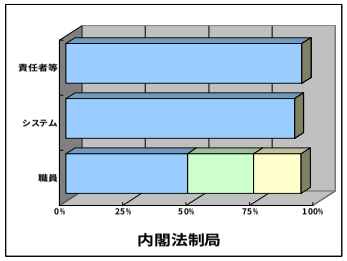
実施率：把握した者のうち、責務が生じた者に占める対策を実施した者の割合

(参考2) 各府省庁の対策実施状況報告 (2007年度) の集計結果

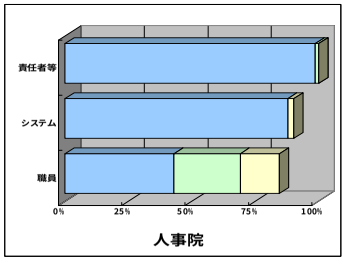
○ 到達率



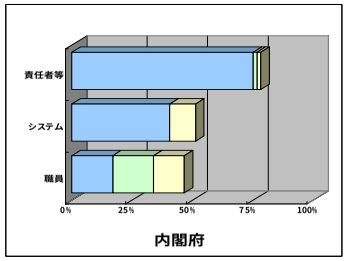
内閣官房



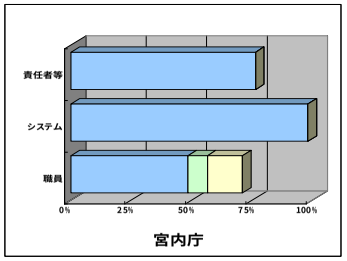
内閣法制局



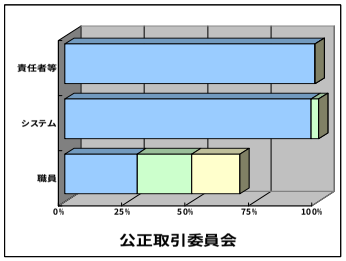
人事院



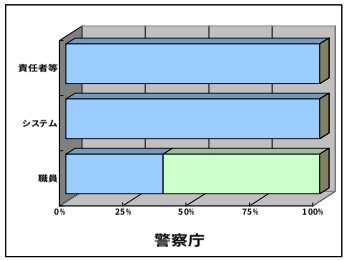
内閣府



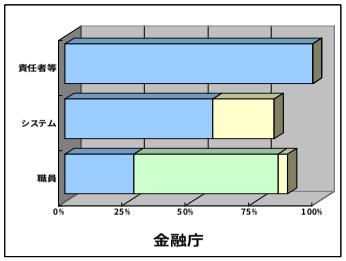
宮内庁



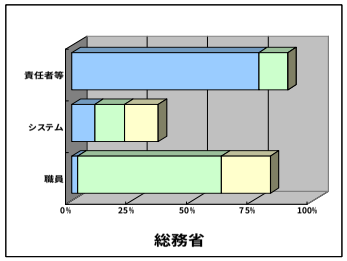
公正取引委員会



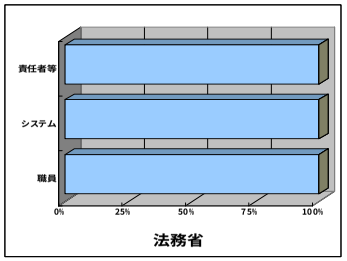
警察庁



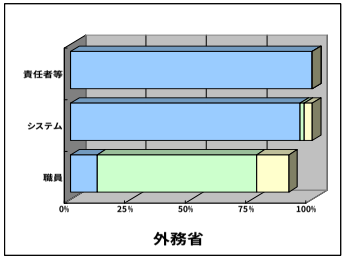
金融庁



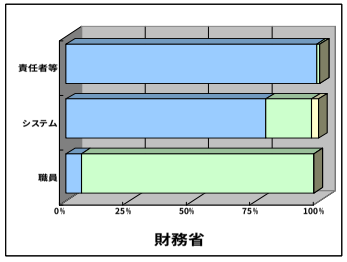
総務省



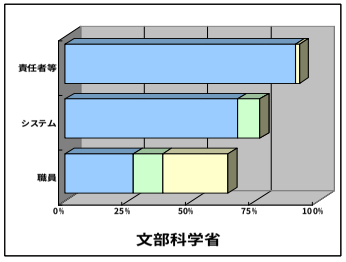
法務省



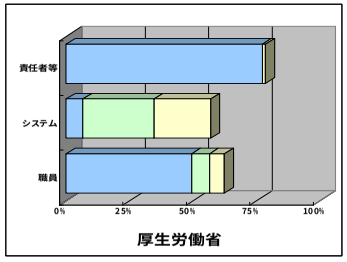
外務省



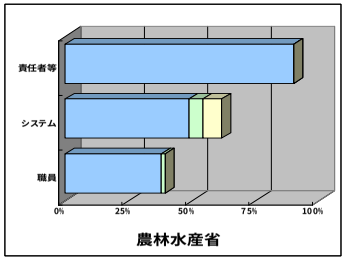
財務省



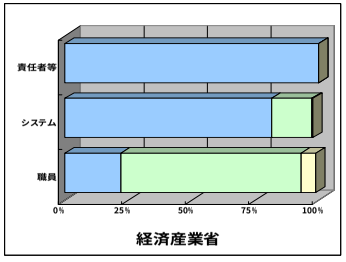
文部科学省



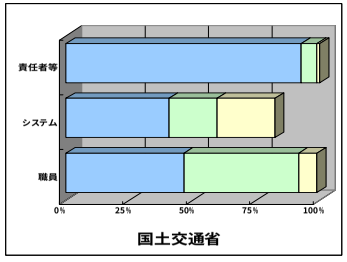
厚生労働省



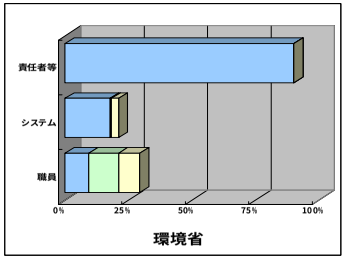
農林水産省



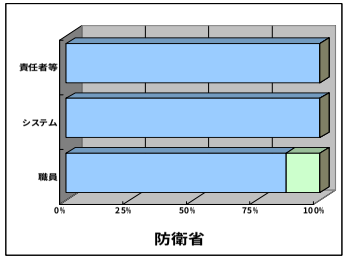
経済産業省



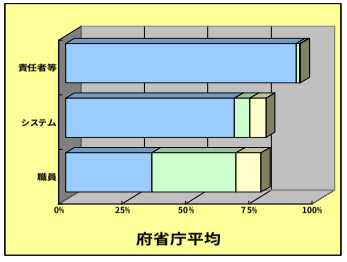
国土交通省



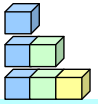
環境省



防衛省



府省庁平均



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

端末及びウェブサーバに関する情報セキュリティ対策の総合評価

別添4

重点検査の項目

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 ・アンチウイルス対策ソフトの運用状況
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

・府省庁の調査に基づく結果
・平成19年3月末時点

総合評価	端末			ウェブサーバ		
	H18		H19	H18		H19
内閣官房	B	▷▷	B	B	▷	B
内閣法制局	C	▷▷	B	B	－	B
人事院	C	▷▷▷	A	B	▷▷	B
内閣府	C	▷▷▷	B	C	▷▷	B
宮内庁	D	▷▷▷▷	A	C	▷▷▷	A
公正取引委員会	C	▷▷▷	A	A	－	A
警察庁	D	▷▷▷▷	A	B	▷▷	A
金融庁	B	▷▷	B	B	▷	A
総務省	C	▷▷▷	B	B	▷	B
法務省	D	▷▷▷▷	B	C	▷▷▷	B
外務省	D	▷▷▷▷	A	B	▷▷	B
財務省	C	▷▷	B	B	▷▷	B
文部科学省	C	▷▷▷	A	B	▷▷	A
厚生労働省	D	▷▷▷	B	B	▷	B
農林水産省	C	▷▷▷	A	B	▷	A
経済産業省	C	▷▷▷	A	B	▷	A
国土交通省	D	▷▷▷	B	C	▷▷	B
環境省	B	▷	B	B	▷▷	A
防衛省	C	▷▷▷▷	B	B	▷▷	A

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		上昇率		上昇率		上昇率	
▷▷▷▷	x＞ 40%	▷▷▷	x＞ 30%	▷▷▷	x＞ 20%	▷▷	x＞ 10%	▷	x＞ 0%	－	x＝ 0%

評価結果を受けての対応予定

	端　末	ウェブサーバ
内閣官房	平成２０年度	平成２０年度
内閣法制局	今年度	今年度
人事院	実施済み	実施済み
内閣府	平成２０年度	平成２０年度
宮内庁	実施済み	実施済み
公正取引委員会	実施済み	実施済み
警察庁	実施済み	実施済み
金融庁	今年度	実施済み
総務省	平成２０年度	平成２０年度
法務省	平成２０年度	平成２０年度
外務省	実施済み	今年度
財務省	平成２０年度	平成２０年度
文部科学省	実施済み	実施済み
厚生労働省	平成２０年度	平成２０年度
農林水産省	実施済み	実施済み
経済産業省	実施済み	実施済み
国土交通省	平成２０年度	平成２０年度
環境省	今年度	実施済み
防衛省	今年度	実施済み

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

重点検査の項目

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
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
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

・府省庁の調査に基づく結果
・平成19年9月末時点

総合評価	電子メールサーバ	（参考）端末	（参考）ウェブサーバ
	平成19年9月末	平成19年3月末	平成19年3月末
内閣官房	B	B	B
内閣法制局	B	B	B
人事院	A	A	B
内閣府	B	B	B
宮内庁	B	A	A
公正取引委員会	B	A	A
警察庁	A	A	A
金融庁	A	B	A
総務省	B	B	B
法務省	B	B	B
外務省	B	A	B
財務省	A	B	B
文部科学省	A	A	A
厚生労働省	A	B	B
農林水産省	A	A	A
経済産業省	A	A	A
国土交通省	B	B	B
環境省	A	B	A
防衛省	A	B	A

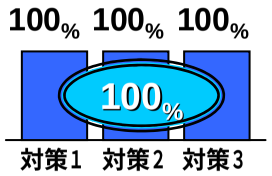
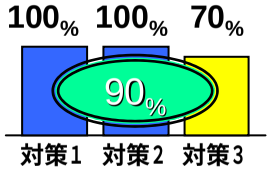
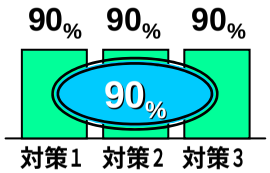
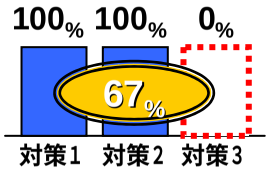
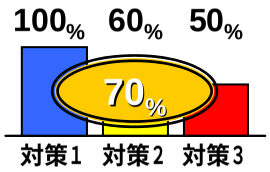
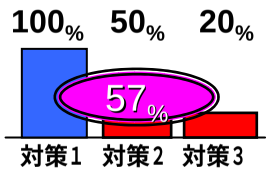
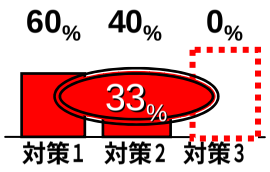
評価	実施率	評価	実施率	評価	実施率	評価	実施率
A	x＝100%	B	80%≦x＜100%	C	60%≦x ＜80%	D	x＜ 60%

電子メールサーバの評価結果を受けての対応完了予定

府省庁名	総合評価	平成１９年度	平成２０年度
内閣官房	B	→	
内閣法制局	B	→	
人事院	A	実施済み	
内閣府	B	→	
宮内庁	B	→	→
公正取引委員会	B	→	
警察庁	A	実施済み	
金融庁	A	実施済み	
総務省	B	→	→
法務省	B	→	→
外務省	B	→	→
財務省	A	実施済み	
文部科学省	A	実施済み	
厚生労働省	A	実施済み	
農林水産省	A	実施済み	
経済産業省	A	実施済み	
国土交通省	B	→	→
環境省	A	実施済み	
防衛省	A	実施済み	

※　平成19年度中に対応完了予定 →
※　平成20年度中に対応完了予定 →

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

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。	
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。	 
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。	 
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。	 

政府機関の情報セキュリティマネジメントの総合的な評価

別添5

「マネジメント評価」

- 府省庁における情報セキュリティマネジメントがPDCAサイクルの各段階で確実かつ効果的におこなわれているかを評価
- 「計画」「周知」「実施」及び「評価と改善」の各段階にわたる45の評価指標に基づき府省庁におけるプラクティスを抽出し、評価

★★★ 政府内外を問わず模範となる先進的な取り組みを実践している
★★ 政府機関の模範となる工夫が見られる
★ おおむね適切に行われている

政府機関評価指標専門委員会
（2006年9月～10月）
『政府機関評価指標マネジメント指標』を策定

評価指標

情報セキュリティ政策会議
第9回会合（2006年12月13日）
第10回会合（2007年2月2日）

『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』（2007年2月2日）

意見募集（パブリックコメント）

2006年度 マネジメント評価

評価指標に基づく調査・評価を実施 （2007年2月～）

中間報告
情報セキュリティ政策会議
第11回会合 （2007年4月23日）

今回報告
情報セキュリティ政策会議
第13回会合 （今回）

政府機関の情報セキュリティマネジメントの総合的評価　～2006年度～

- 2006年度 情報セキュリティ・ベストプラクティス

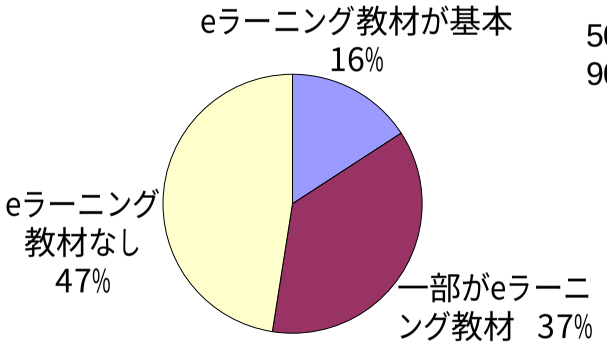
★★ 省内ネットワークを活用した職員の支援
・eラーニングシステム　・実施手順等の運用　総務省　経済産業省

★★ 幹部職員の下で全庁一体となった対策の推進　警察庁

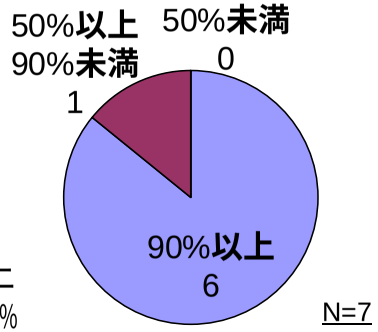
★★ 外部委託における情報セキュリティの確保　外務省　防衛省

  - 政府機関の模範となるプラクティス（★★）は「計画」及び「周知」を中心に44件。
  - 政府内外を問わず模範となる先進的な取り組み（★★★）は見られなかった。

- 各府省庁の体制等の調査結果
  - 情報セキュリティ担当者（常任）の職員に占める割合：
    2%超＝4府省庁、0．5%以下＝7府省庁
  - 情報セキュリティ担当者（常任）の平均経験年数：
    1年～3年が中心
  - eラーニング導入は府省庁全体では部分的：
    「eラーニング教材が（一部でも）ある」＝10府省庁



eラーニング教材の整備状況　N=19



N=7

eラーニング教材が利用可能な職員の割合

※eラーニング：コンピュータネットワークなどを活用して教育を行うこと

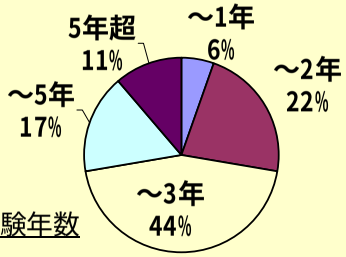
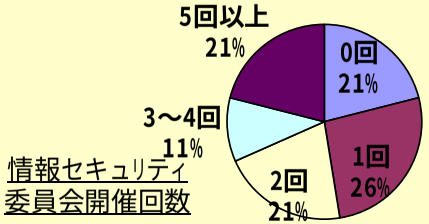
政府機関の情報セキュリティマネジメントに関する評価結果

評価指標			評価		
			★（I）	★★（II）	★★★（III）
			おおむね適切に行われている。	適切に行われているだけでなく、対策を確実に行うための政府機関の模範となる工夫が見られる。	適切に行われているだけでなく、対策を確実に行うための政府内外を問わず模範となる先進的な取組みを実践している。
				○ 対策を確実に行うための工夫 ○ 政府機関の模範となる水準	○ 対策を確実に行うための先進的な工夫 ○ 政府内外を問わず模範となる水準
計画	資源	【担当者の情報セキュリティに係る知識向上】 ①情報セキュリティ対策管理部門の担当者の情報セキュリティ知識向上のための対策を講じているか	官房、人事、官内、公取、金融、総務、法務、財務、文科、厚労、農水、経産、国交、環境	警察、外務、防衛 ・ 研修の実施等について、組織として明確な目標を定めている。 ・ 長期的な人材運用の観点から研修を実施している。	
	組織	【総合調整を行う部署の有無】 ①府省庁全体の業務について、その把握や総合調整を行う権限を有する部署があるか	全府省庁		
		【業務・システム最適化における取組みの管理】 ②各府省庁のPMOにおいて、業務・システム最適化の中で、情報システムの安全性・信頼性を確保するための取り組みを管理しているか（例えば業務・システム最適化の企画段階での情報システムセキュリティ対策要領の作成、情報システムの構築の要求仕様策定段階での情報セキュリティ要件定義の作成等の管理）	法制、人事、官内、公取、警察、金融、総務、法務、外務、財務、文科、農水、経産、国交、環境	厚労、防衛 ・ 情報セキュリティを担当するCIO補佐官を定めており、情報セキュリティ要件定義等の作成等においてその意見を反映している。 ・ 情報システムの整備において、安全性・信頼性を確保するために国際規格の評価基準を広く適用している。	
		【情報資産台帳の整備】 ③各府省庁のPMOにおいて、情報資産台帳を整備しているか	法制、内府、官内、公取、総務、法務、文科、環境	警察、外務、経産、防衛 ・ 情報の格付けを記載事項に含む情報資産台帳を整備しており、適切に更新している。	
		【最高情報セキュリティアドバイザーの設置】 ④最高情報セキュリティアドバイザーを置いているか（最高情報セキュリティ責任者に助言を行う専門家の有無） （関連：政府機関統一基準2.1.1(1)(c)）	官房、法制、内府、公取、警察、財務、文科、厚労、農水、経産、国交	金融、総務、法務、外務、環境 ・ 情報セキュリティに係る業務に専ら従事する者を情報セキュリティアドバイザーとして任命しており、当該情報セキュリティアドバイザーを有効に活用している。	
		【幹部職員に対する報告】 ⑤省議等、府省庁幹部職員が出席する会議で当該府省庁の情報セキュリティ状況について報告を行っているか	官房、人事、内府、官内、公取、金融、総務、法務、外務、財務、文科、厚労、農水、経産、国交、環境	警察、防衛 ・ 大臣等が出席する会議において、情報セキュリティを議題として扱い、その実施に係る決定・指示が行われている。	
		【横断的な連絡会議等の有無】 ⑥情報セキュリティ責任者、情報システムに係る責任者等を集めた府省庁内横断的な連絡会議等を行っているか	官房、人事、内府、官内、公取、金融、総務、法務、外務、財務、厚労、農水、国交、環境	警察、経産、防衛 ・ 一方的な伝達・説明の場としてではなく、情報セキュリティ対策の実施等に直接携わる職員による議論や意見交換がなされるなど、実務に則した情報セキュリティ対策を検討するための場として機能している会議等を開催している。	
		【支分部局ごとの担当者の設置】 ⑦地方支分部局等を持つ場合に、情報セキュリティに係る責任者及び担当者をそれぞれの支分部局ごとに置いているか	人事、内府、官内、公取、法務、外務、財務、厚労、農水、国交、環境、防衛	警察、総務、経産 ・ 地方支分部局等に情報セキュリティに係る責任者・担当者が配置され、地方機関と効果的な情報共有を図るための措置を講じている。	
	規程	【責任者による実施手順書等の内容確認】 ①情報システムに係る実施手順等の策定に当たり、当該情報システムの情報システムセキュリティ責任者がかかわり、内容を確認しているか （政府機関統一基準5.2.1(1)(a), 5.3.1(1)(a)）	法制、人事、公取、警察、金融、総務、法務、外務、財務、文科、厚労、農水、経産、国交、環境、防衛		
		【情報セキュリティ関係規程の見直し】 ②情報セキュリティ関係規程の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にその見直しをしているか （政府機関統一基準2.4.1(1)(a)）	官房、法制、人事、内府、官内、公取、警察、金融、総務、法務、外務、財務、厚労、農水、経産、国交、環境、防衛		
周知	啓発	【一般職員向け実施手順等の平易化】 ①一般職員向けの実施手順等は、その策定にあたり、遵守事項を漏れなく含めるだけでなく、理解しやすいものとすることに努めたか	官房、人事、内府、官内、公取、警察、金融、総務、法務、外務、財務、文科、厚労、農水、経産、国交、環境、防衛		
		【一般職員向け実施手順等の参照の容易化】 ②一般職員向けの実施手順等は、府省庁内ウェブサイト等の分かりやすい場所に置いて日常的に参照可能としているか	法制、人事、内府、官内、公取、総務、法務、外務、財務、文科、厚労、農水、国交、環境	警察、金融、経産、防衛 ・ ウェブサイトによる実施手順の周知において、目的等から関連する実施手順書等を検索できるFAQの充実や、実施手順書の遵守事項から帳票や手続画面へのリンクの設定等、一般職員にとり利便性の高いものとするための措置がとられている。	
		【ひやり事案を含む障害等の事例の活用】 ③組織内外のひやり事案を含む障害等の事例を活用しているか ・事例収集　・モデル化　・訓練・教育への活用	人事、内府、官内、公取、警察、金融、総務、法務、外務、文科、厚労、農水、経産、国交、環境、防衛		
	教育	【教育計画の策定】 ③教育に関する計画が定められているか （政府機関統一基準2.2.1(1)）	警察、金融、総務、法務、外務、文科、厚労、経産、環境		
		【責任者、管理者の役割に応じた教育の企画】 ④教育に関する計画では、情報セキュリティに係る責任者及び管理者の役割に応じた教育を企画しているか （関連：政府機関統一基準2.2.1(1)）	人事、官内、公取、警察、金融、総務、法務、外務、財務、厚労、環境、防衛		
		【教育計画策定時における人事部門等との調整】 ⑤教育の年次計画を定める際には、人事部門、情報システム部門等、関係者と調整をしているか（府省庁教育メニューへの組み込み、情報システム部門の支援等、教育の準備及び実施のための条件整備）	警察、法務	公取、金融、総務、外務、厚労、経産、防衛 ・ 府省庁全体の研修計画に府省対策基準や実施手順に係る教育が含まれており、異動、昇進等の際に実施される教育に当該教育も統合されている。	
		【対象者の役割に応じた教育教材の整備】 ①すべての対象者（一般職員、各責任者・管理者）に対して、教育教材が整備されているか （政府機関統一基準2.2.1(1)）	人事、警察、金融、法務、外務、厚労、経産、国交、防衛		
		【システムの更新、事故等の教育教材への反映】 ②教育教材は、情報システムの更新、セキュリティ事故の状況等を反映して更新されているか	警察、金融、総務、法務、財務、文科、厚労、農水、経産、環境、防衛		
		【教育受講状況の管理】 ⑦教育の受講状況を管理する仕組みはできているか （政府機関統一基準2.2.1(1)(e)）	法制、人事、官内、公取、警察、金融、法務、財務、厚労、農水、経産、国交、環境、防衛	総務、外務 ・ 情報セキュリティ教育の受講状況管理がシステム化されており、当該システムを有効に活用した受講率向上のための取組みを実施している。	

		[教育の理解度の確認] ⑧教育の実施時等に、試験等により職員の理解度を確認しているか	**警察、法務、外務、厚労、防衛**	**総務** ・ 情報セキュリティ教育に係る職員の理解度調査がシステム化されており、当該システムを有効に活用した理解度向上のための取組みが実施されている。	
		[人事異動等に伴う教育の実施] ⑥行政事務従事者の転入や情報セキュリティに係る責任者及び管理者の指名にあわせて、役割に応じた教育を行っているか	**公取、警察、金融、総務、法務、外務、厚労、農水、経産、防衛**		
実施	業務改善	**[IT活用等による対策実施の自動化、強制化]** ①対策を確実に実施するために、IT活用等により対策実施の自動化や強制をしているか 例：外部記録媒体に格納する情報の暗号化の強制	**官房、法制、人事、内府、宮内、公取、警察、金融、総務、法務、外務、財務、文科、厚労、農水、経産、国交、防衛**		
	異常	**[一般職員向けの注意喚起]** ①一般職員向けの注意喚起（ウイルスについての警告、ソフトウェアの更新指示等）を、府省庁内ウェブサイトへの掲載、電子メールでの通知又は文書での通達等により適時に広く周知しているか	**全府省庁**		
		[障害対応に係る対応手順の整備等] ②障害等が発生した際の対応手順があるか、また、発生時に容易に参照できるようになっているか 例：ウイルス感染時の対応手順 　　情報システムの停止時の代替業務手順	**法制、人事、内府、宮内、公取、警察、金融、総務、法務、外務、財務、文科、厚労、農水、経産、国交、環境**	**防衛** ・ 障害等の発生に係る対応手順について、その参照を容易とするための措置に加え、当該対応手順の内容の妥当性を演習等により検証し、内容の改善に努めている。	
		[再発防止のための措置の実施] ③障害等が発生した場合に、その原因を調査して再発防止策を策定し、必要な措置を講じているか。 ［政府機関統一基準2.2.2(3)(a), (b)］	**官房、法制、人事、内府、宮内、警察、金融、総務、法務、外務、財務、文科、厚労、農水、経産、国交、環境、防衛**		
	例外措置	**[例外措置に係る適用期間等の検討]** ④採用した例外措置について、継続することの妥当性を適時に判断しているか、また、例外措置を終了するための検討や準備を行っているか（予算措置、基準への反映の要求等）	**人事、宮内、公取、警察、金融、総務、法務、外務、財務、国交、環境**		
	調達・外部委託	**[調達仕様への記載事項の標準化等]** ①調達仕様に記載する情報セキュリティ関連事項について標準を定め、手順書や雛形に含めて示しているか ［関連：政府機関統一基準4.3.1(1)(b), (c), 6.1.1(1)(a), (b), (2)(c), 6.1.2(1)(b), (2)(a), (b), (c), 6.1.3(1)(a), (b)］	**官房、法制、人事、内府、宮内、公取、警察、金融、法務、外務、厚労、農水、経産、国交、環境**	**防衛** ・ 機器等及び外部委託に関する調達仕様に記載する事項を定めた標準があり、政府機関統一基準で定められた事項が当該基準に網羅的に含まれている。	
		[契約書への記載事項の標準化等] ②契約に記載する情報セキュリティ関連事項について標準を定め、手順書や雛形に含めて示しているか ［関連：政府機関統一基準6.1.2(4)(a)］	**官房、法制、人事、内府、宮内、公取、警察、法務、外務、厚労、農水、国交、環境**	**金融、経産、防衛** ・ 契約に記載する事項を定めた標準があり、政府機関統一基準で定められた事項が当該標準に網羅的に含まれている。 ・ 会計担当課が策定している府省庁内標準の契約雛形に情報セキュリティ関連項目を設けており、政府機関統一基準で定められた事項が当該雛形に網羅的に含まれている。	
		[カストマイズを想定した調達の雛形等の策定] ③調達・契約の手順書や雛形は、留意点を記述する等により、案件ごとにカストマイズして運用できるようになっているか	**官房、法制、人事、内府、宮内、公取、警察、金融、法務、厚労、農水、経産、国交、防衛**	**外務、環境** ・ 調達・契約の雛形が具体的に整備されており、また、雛形が適用できない箇所等については、情報セキュリティに係る専門的な知見を有する者が個別に内容を確認・決裁する手続となっている。	
評価と改善	評価	**[自己点検計画の策定]** ①当該年度の自己点検計画が定められているか ［政府機関統一基準2.3.1(1)(a)］	**官房、法制、人事、宮内、公取、警察、金融、総務、法務、外務、財務、文科、厚労、農水、経産、国交、環境、防衛**		
		[自己点検結果に基づく改善指示等の有無] ②自己点検結果に基づき、その評価及び必要な場合に改善指示がなされているか ［政府機関統一基準2.3.1(5)］	**全府省庁**		
		[情報セキュリティ監査計画の策定] ③当該年度の情報セキュリティ監査計画が定められているか ［政府機関統一基準2.3.2(1)(a)］	**全府省庁**		
		[過去の監査結果を考慮した監査計画の策定] ④以前実施した監査結果で明らかになった課題及び問題点の改善状況についての監査が当該年度の情報セキュリティ監査計画に盛り込まれているか ［関連：政府機関統一基準2.3.2(1)(a)］	**公取、警察、金融、総務、法務、外務、農水、経産、国交、環境、防衛**		
		[監査報告の実施] ⑤当該年度の監査報告が行われているか ［政府機関統一基準2.3.2(5)］	**官房、法制、人事、内府、宮内、公取、警察、金融、総務、法務、外務、文科、厚労、農水、経産、国交、防衛**		
		[最高情報セキュリティ責任者への監査報告書の説明] ⑥監査報告書の内容を最高情報セキュリティ責任者に（単に提出するだけでなく）説明しているか	**官房、法制、内府、宮内、公取、警察、金融、総務、法務、外務、厚労、農水、経産、国交、環境**		
		[監査報告書に基づく対応の実施] ⑦監査報告書の内容を踏まえ、改善のための以下の措置をとっているか a. 指摘事案に対する対応実施の指示（最高情報セキュリティ責任者） b. 同種の課題及び問題点の有無についての確認の指示（最高情報セキュリティ責任者） c.改善を指示された事案についての対応計画（達成可能な対応目標の設定を含む。）の作成と報告（情報セキュリティ責任者） d. 情報セキュリティ関係規程の妥当性評価と必要に応じ見直しの指示（情報セキュリティ責任者） ［政府機関統一基準2.3.2(6)(a), (b), (c), (d)］	**官房、法制、人事、内府、宮内、公取、警察、金融、法務、外務、財務、文科、農水、経産、国交、防衛**	**総務** ・ 監査における指摘事項に基づく改善において、チェックシートを用いた処理手続の整備等、対応をより確実なものとするための措置を講じている。	

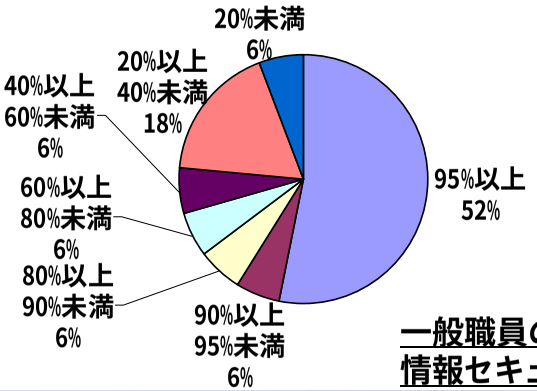
官房：内閣官房　法制：内閣法制局　人事：人事院　内府：内閣府　宮内：宮内庁　公取：公正取引委員会　警察：警察庁　金融：金融庁　総務：総務省　法務：法務省
外務：外務省　財務：財務省　文科：文部科学省　厚労：厚生労働省　農水：農林水産省　経産：経済産業省　国交：国土交通省　環境：環境省　防衛：防衛省

政府機関の情報セキュリティマネジメントの状況　～2006年度～

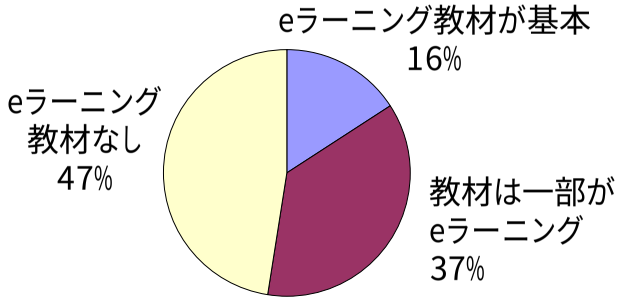
大分類	小分類	観点	調査結果
計画	資源	情報セキュリティ対策管理部門に適切な人的資源が割り当てられているか  	○ 情報セキュリティ担当者(注)（常任）の人数と職員に占める割合： (注)　情報セキュリティを含む情報システムに係る業務を主たる担当業務とする者 ・4府省庁で2%超　　7府省庁で0.5%以下 ・6府省庁で4名以下 府省庁内共通システム担当等が情報セキュリティ推進も兼務 ・7府省庁で100名超 各情報システムの担当が情報セキュリティ対策も実施 ○ 8府省庁で、常任と同数以上の一時的な担当者が従事している。 ○ 情報セキュリティ担当者の平均経験年数： ・府省庁内平均の分布は1年～3年が中心。
	組織	基準で定める責任者等が指名されているだけでなく、実態において組織として機能し得るものであるか  	○ 各府省庁において、責任者等の指名に加えて、推進体制が存在。 ・PMO、CIO補佐官、最高情報セキュリティアドバイザー等 ・6府省庁において情報セキュリティの専門家を登用し、対策推進における助言、技術仕様の整備等で実績 ○ 情報セキュリティ組織の活動に加え、府省庁の幹部が指示・決定を行っている例は一部にとどまる。 ○ 情報セキュリティ委員会の運営は、一部の府省庁で不足している。 ・4府省庁で開催なし、5府省庁で開催1回
	規程	情報システムに適用する規程は、それぞれの情報システムの特性や取り扱う情報等を考慮して策定されているか	○ 各府省庁において、情報システムに適用する規程を、情報システムセキュリティ責任者の確認を受けて概ね整備している。
		現場への適合性を適時に評価し、必要に応じて見直しをしているか	○ 各府省庁において、規程の見直しの必要性有無を適時検討している。 ○ 判断を行う仕組みとしてPMOや情報セキュリティ委員会を活用する例もある。

政府機関の情報セキュリティマネジメントの状況　～2006年度～

大分類	小分類	観点	調査結果
周知	啓発	規程が定められているだけでなく、職員一人一人まで理解しうるものであるか	○ 規程を理解しやすいものとし、また参照・利用の利便を図る施策が採られている。 ・策定時に利用予定者が査読 ・府省庁内のウェブサイトに掲載 ・FAQ、ガイドブックの整備、質問対応体制　等
		規程がその利用者にとって容易に参照・利用できるようになっているか	
		組織内外のヒヤリハット情報を事例として活用しているか	○ 多くの府省庁で障害等の事例を収集する仕組みがあるが、ヒヤリ・ハット情報収集を意図した組織的な活動まではしていない。 ○ 収集した事例を対策、規程、教育等の改善に活用している例がある。
	教育	情報セキュリティ教育を適切に実施し、また試験等により職員の理解度を確認しているか	○ 教育については、より組織的な実施に向けて課題がある。 ・計画の不備、受講不徹底、受講状況管理・理解度確認不足 ・6府省庁で一般職員の教育受講率が80%未満 ○ eラーニングの活用は、現状では一部に限られている。 ・3府省庁で教材を概ねeラーニングにより整備し、7府省庁で一部の教材をeラーニングで整備している ・6府省庁でeラーニング教材が地方支分部局等でも広く利用可能

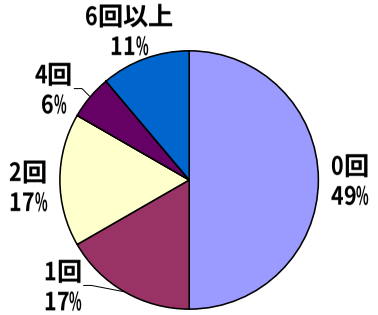
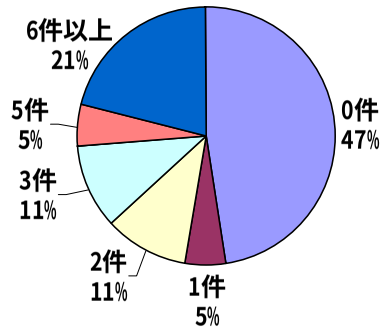


一般職員の情報セキュリティ教育受講率
N=19



eラーニング教材の整備状況 N=19

政府機関の情報セキュリティマネジメントの状況　～2006年度～

大分類	小分類	観点	調査結果
実施	業務改善	先端的技術の活用（対策のシステム化等）等により、情報セキュリティ対策が業務プロセスにシームレスに組み込まれているか	○ 各府省庁において、情報セキュリティ対策の確実な実施等を目的としてITを活用している。
	異常・障害等への対応	府省庁外からの脅威情報を周知しているか	○ 各府省庁において、脅威情報（ウイルスに関する警告等）を府省庁内の職員に適時に周知している。
		障害等（インシデント及び故障を含む）への対応が適切に行われるか	○ 各府省庁において、障害等の対応手順が整備されている。 ○ 9府省庁において、情報システムの障害等に備えた対応訓練を実施している。 対応訓練実施回数 
		障害等の事後策を実施しているか	○ 各府省庁において、障害等の再発防止策を策定している。
	例外措置	基準への例外事項をあまねく把握し、例外措置を適用できているか	○ 規程等への例外措置は10府省庁で適用実績がある。このうち8府省庁では代替措置も検討し適用している。 例外措置件数 

政府機関の情報セキュリティマネジメントの状況　～2006年度～

大分類	小分類	観点	調査結果
実施 (続き)	調達・外部委託	調達及び外部委託における情報セキュリティ確保のために十分な対策が採られているか	○ 調達仕様書及び契約に関して、情報セキュリティ関連事項の標準を示した手順等や雛形が概ね用意されている。ただし、会計課等の雛形で省庁基準等の要件に対応している府省庁は一部にとどまる。 ○ 多様な調達案件に対応するため、調達仕様等についてCIO補佐官による確認や助言を組織的に採り入れている例もある。
評価と改善	評価と改善	自己点検が有効に行われ、必要な改善が図られているか	○ 各府省庁において、自己点検結果に基づく改善指示が行われている。
		情報セキュリティ監査が有効に行われ、必要な改善が図られているか	○ 各府省庁において、情報セキュリティ監査の計画策定、実施、報告及び改善指示が概ね行われている。

別添6

企業・個人における情報セキュリティの評価指標

⑴ 企業･個人に係るアウトプット指標

ア 企業を支援する政府の施策

① 企業の情報セキュリティ対策が市場評価に繋がる環境の整備に係る指標

今のところ該当する既存のデータはないが、企業間の取引相手における情報セキュリティ対策の確認状況に関するデータ、事業継続計画（ＢＣＰ）の作成状況に関するデータ等の指標の追加については、今後、見直しの際に検討する。

② 質の高い情報セキュリティ関連製品及びサービスの提供促進に係る指標

企業による第三者評価制度等の利用状況を指標とする。

（既存のデータ）

・「ＩＳＭＳ認証の取得事業者数」（日本情報処理開発協会）

・「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）

③ 企業における情報セキュリティ人材の確保･育成に係る指標

a 企業に対する情報セキュリティ教育等に係る指標

政府等による企業に対する情報セキュリティ教育や政府等の情報セキュリティに係る資格の取得者等の状況を指標とする。

（既存のデータ）

・「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）

・「情報セキュリティアドミニストレータ試験合格者数」（情報処理推進機構）

b 今後の検討課題

さらなる指標の追加の可否については、今後、見直しの際に検討する。

④ コンピュータウィルスや脆弱性等に早期に対応するための体制の強化に係る指標

コンピュータウィルスや脆弱性等への対応のための体制の整備状況等を指標とする。

（既存のデータ）

・「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）

・「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）

イ 個人を支援する政府の施策

① 情報セキュリティ教育の強化･推進に係る指標

a 実施体制･実施状況

学校等における個人向けの教育の機会の状況を指標とする。

（既存のデータ）

・「情報セキュリティを含む情報教育に関する教員向け研修を受けたことがある教員の状況」（学校における情報化の実態等に関する調査：文部科学省）
・「インターネット安全教室参加者数（概数）」（経済産業省）
・「e-ネットキャラバン参加者数（概数）」（総務省・文部科学省）

b 今後の検討課題

小学校における情報セキュリティを含む情報モラル教育を実施できる教員の存在率等の指標の追加の可否については、今後、見直しの際に検討する。

② 広報啓発･情報発信の強化･推進に係る指標

政府等による情報発信へのアクセスの状況を指標とする。

（既存のデータ）

・「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」（内閣官房、警察庁、総務省、経済産業省）
・「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）
・「情報の入手経路」（情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構）
・「希望する情報提供方法」（情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構）

③ 個人が負担感なく情報関連製品･サービスを利用できる環境整備に係る指標

a 利用環境整備に係る指標

（既存のデータ）

・「無線ＬＡＮ機器のセキュリティ対策の必要性に関する周知状況」（インターネットの利用実態に関する調査：総務省）

b 今後の検討課題

その他ボット対策の実施状況等に係る指標の追加については、今後、見直しの際に検討する。

⑵ 企業･個人に係るアウトカム指標

ア 各主体の意識

① 企業の情報セキュリティ意識に係る指標

a 企業の情報セキュリティ意識に係る指標

企業全体の情報セキュリティの意識の状況を指標とする。

（既存のデータ）

・「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）

b 今後の課題

情報セキュリティ対策を行ったことによる顧客･市場等からの評価に関するデータ等の指標の追加について、今後の見直しの際に検討する。

② 個人の情報セキュリティ意識に係る指標

個人全体の情報セキュリティの意識の状況を指標とする。

（既存のデータ）

- 「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）
- 「情報セキュリティに関する言葉の認知度」（情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構）
- 「情報セキュリティ対策に関する意識」（情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構）

イ 各主体の対策

① 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

企業全体の情報セキュリティに取り組む組織的な体制等の確立に関連するものを指標とする。

（既存のデータ）

- 「リスク分析実施状況」（情報処理実態調査：経済産業省）
- 「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）
- 「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）

b 情報セキュリティ対策の導入及び運用に係る指標

企業全体の情報システムを構築･運用する場合の情報セキュリティ対策の導入及び運用の状況（教育の状況も含む）を指標とする。

（既存のデータ）

- 「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）
- 「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）
- 「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）
- 「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）
- 「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）
- 「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）

・「パッチ適用実施率」（国内におけるコンピュータウィルス被害状況調査：情報処理推進機構）

・「ウィルス対策ソフト導入率」（国内におけるコンピュータウィルス被害状況調査：情報処理推進機構）

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

企業全体の情報セキュリティ対策の監視及びレビューの状況を指標とする。

（既存のデータ）

・「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）

d 今後の課題

情報セキュリティ対策の維持及び改善に係る指標については、現時点で適当な指標が見あたらないことから、今後他の対策実施領域での取組みを参考にしつつ検討していくものとする。

② 個人の情報セキュリティ対策状況に係る指標

個人全体の情報セキュリティ対策の状況を指標とする。

（既存のデータ）

・「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）

・「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）

・「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新たな脅威に対する意識調査：情報処理推進機構）

ウ インシデント･犯罪の発生

① インシデント又は犯罪の被害に係る指標

インシデント又は犯罪の被害は、認知した者は申告するとしても被害を受けても気が付かない者は申告せず、全体の正確な割合が分からない、という限界はある。しかし、ここでは、企業・個人全体へのリスクの傾向を計測する観点から、企業・個人全体がインシデント又は犯罪の被害を経験した割合等を指標とする。

（既存のデータ）

・「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）

・「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）

・「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）

・「不正アクセス行為の発生状況」（警察庁）
・「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）
・「情報セキュリティ被害経験」（個人）（情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構）
・「コンピュータウィルス遭遇率」（企業）（国内におけるコンピュータウィルス被害状況調査：情報処理推進機構）
・「スパイウェア遭遇率」（企業）（国内におけるコンピュータウィルス被害状況調査：情報処理推進機構）

エ （参考指標）ITを活用した経済の発展状況

ＩＴを活用した経済の発展状況は、情報セキュリティと直接関係するわけではないが、この情報セキュリティの裏付けが伴って発展がなされると思料されることから、参考指標として扱うものとする。

・「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）
・「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）

（備考）既存のデータとして引用した主な調査

○ 「情報処理実態調査」（経済産業省）：有効回答数 4641 件、回収率 48.9%（H17）
http://www.meti.go.jp/policy/it_policy/statistics/jyojitsu.htm
○ 「通信利用動向調査」（世帯編）（総務省）：有効回答数 3982 件、回収率 62.2%(H17)
http://www.johotsusintokei.soumu.go.jp/statistics/statistics05b1.html
○ 「不正アクセス行為対策等の実態調査」（警察庁）：有効回答数 606 件、回収率 24.2%(H17)
http://www.npa.go.jp/cyber/research/index.html
○ 「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）
http://211.120.54.153/b_menu/houdou/18/07/06072407.htm
○ 「情報セキュリティに関する新たな脅威に対する意識調査」（独立行政法人情報処理推進機構）：有効回答数 5142 件、回収率 51.4%（H17）
http://www.ipa.go.jp/security/products/products.html
○ 「国内におけるコンピュータウィルス被害状況調査」（独立行政法人情報処理推進機構）：有効回答数 1,701 件、回収率 25.9%（H17）
http://www.ipa.go.jp/security/products/products.html

別添7

企業・個人における現状の評価

○ ＩＳＭＳ認証の取得事業者（日本情報処理開発協会）

単位：事業者

	15年度	16年度	17年度	18年度	19年度
ISMS認証取得事業者数	276	418	720	528	468

○ 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）

単位：件

	14年度	15年度	16年度	17年度	18年度	19年度	計
認証取得製品数（新規認証）	2	5	17	23	43	62	**152**
認証取得製品数（保証継続）	－	－	3	10	9	12	**34**

○ 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）

	15年度	16年度	17年度	18年度	19年度
開催回数	全国８ヶ所 計８回	全国16ヶ所 計27回	全国16ヶ所 計40回	全国30ヶ所 計84回	全国31ヶ所 計96回
開催コース	（種類分けなし）	２種類 ・概要 ・詳細 ※他、 特別行事１回	３種類 ・基礎 ・マネジメント ・対策技術 ※他、 特別行事１回	４種類 ・基礎 ・マネジメント ・技術（標準編） ・技術（専門編）	種類 ・基礎 ・マネジメント ・技術（標準編） ・技術（専門編）

○ 情報セキュリティアドミニストレータ試験合格者数（情報処理推進機構）

単位：人

	15年度	16年度	17年度	18年度	19年度
受験者数	27,913	33,581	27,744	22,563	20,709
合格者数	3,149	4,174	3,812	3,337	2,807

テクニカルエンジニア（情報セキュリティ）※試験合格者数（情報処理推進機構）

単位：人

	18年度	19年度
受験者数	18,128	14,649
合格者数	1,227	1,788

※平成18年春期より開始

○ 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）

単位：チーム

	16年３月末	17年３月末	18年２月	19年３月末
CSIRTの数	7	8	13	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）

単位：か所

	16年３月末	17年３月末	18年２月	19年３月末
担当窓口数	64	122	182	233

○ 情報セキュリティに関する指導力を有すると回答した教員の割合※

※情報セキュリティ政策　２００７年度の評価等にむけた「作業方針」（平成 19 年 10 月 3 日策定）での指標「情報セキュリティを含む情報教育に関する教員向け研修を受けたことがある教員の状況」から、より適切なものとして本指標を使用する。

わりとできる／ややできる　と回答した割合

		H18年度
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。	高等学校	63.4%
	中学校	62.3%
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。	小学校	66.6%
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に対して適切に判断し行動できるように指導する。	高等学校	64.0%
	中学校	63.1%
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。	小学校	68.5%
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。	高等学校	63.1%
	中学校	63.5%
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、健康面に気をつけて活用できるように指導する。	小学校	69.9%
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。	高等学校	54.5%
	中学校	52.9%
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。	小学校	60.3%

○ インターネット安全教室参加者数（概数）（経済産業省）

	15年度	16年度	17年度	18年度	19年度
開催数（か所）	11	28	71	98	130
参加者総数（人）	2,069	3,581	5,844	－	6,700

○ **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１７年度（試行実施）＞

平成１７年１１月から平成１８年３月まで、関東及び東海で試行実施し、計７１回の講座を開催し、約８，８００名が受講した。

＜平成１８年度＞

平成１８年４月から全国規模での本格実施を開始、平成１９年３月３１日までに４５３件の講座を開催し、約４９，０００名が受講した。

＜平成１９年度＞

平成１９年４月から、平成２０年３月３１までに　１，０８９件の講座を実施し、約１２０，０００名が受講した。

○ **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（内閣官房、警察庁、総務省、経済産業省）**

省　庁　等	名　　称	アクセス状況	備　　考
内閣官房	情報セキュリティセンターホームページ	519,184人	18年
警　察　庁	サイバー犯罪対策	275,245人	18年度
	@police	1,994,054人	18年
総　務　省	国民のための情報セキュリティサイト	359,258件	18年度
経済産業省	情報セキュリティに関する政策・緊急情報	150,032人	18年度
	CHECKPC！ホームページ	798,155件	19年1/22～3/31
	JP Vender Status Notes(JVN)	1,482,484人	18年度
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	18,969,754件	18年度
有限責任中間法人ＪＰＣＥＲＴコーディネーションセンター	ＪＰＣＥＲＴ／ＣＣホームページ	607,607人	18年度

※アクセス状況の集計方法については、各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。

省　庁　等	名　　称	アクセス状況	備　　考
内閣官房	情報セキュリティセンターホームページ	421,570人	19年
警　察　庁	サイバー犯罪対策	206,399人	19年度
	@police	1,469,025人	19年
総　務　省	国民のための情報セキュリティサイト	266,904人	19年度
経済産業省	情報セキュリティに関する政策・緊急情報	129,709件	19年度
	CHECKPC！ホームページ	1,174,617件	20年1/16～3/31
	Japna Vulnerability Notes(JVN) （※）	1,894,139件	19年度
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	26,924,532件	19年度
有限責任中間法人ＪＰＣＥＲＴコーディネーションセンター	ＪＰＣＥＲＴ／ＣＣホームページ	1,070,338件	19年度

（※）　「JP Vender Status Notes(JVN)」は、平成19年4月に「Japan Vulnerability Notes(JVN)」に名称を変更

※アクセス状況の集計方法については、各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。

○ 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

	１８年	１９年
定期的に入手	37.7%	17.6%
不定期に入手	42.3%	48.3%
入手していない	19.9%	34.2%
全回答者数	2,979	3,027

※各年度で調査方法(設問の構成・内容)や調査手法が異なるため、単純な経年比較はできない。

「セキュリティ脅威」に関する情報の入手先

	１８年	１９年
テレビ・ラジオ	25.4%	30.5%
新聞	20.8%	20.6%
雑誌・広告	17.5%	15.7%
Ｗｅｂ（ニュース配信サイトなど）	70.8%	73.7%
Ｗｅｂ（政府、地方公共団体）	6.6%	6.5%
ＩＳＰからのお知らせ	39.1%	22.9%
セキュリティ対策ソフトの会社	57.7%	51.0%
会社の担当部署や知人から	11.2%	11.1%
その他	2.1%	3.8%
全回答者数	2,385	1,993

※各年度で調査方法(設問の構成・内容)や調査手法が異なるため、単純な経年比較はできない。

「セキュリティ対策」に関する情報の入手の有無

	１８年	１9年
定期的に入手	38.7%	19.9%
不定期に入手	44.2%	49.5%
入手していない	17.2%	30.5%
全回答者数	2,979	3,090

※各年度で調査方法(設問の構成・内容)や調査手法が異なるため、単純な経年比較はできない。

「セキュリティ対策」に関する情報の入手先

	１８年	１9年
テレビ・ラジオ	19.9%	21.4%
新聞	16.2%	14.5%
雑誌・広告	16.8%	13.6%
Ｗｅｂ（ニュース配信サイト等）	66.3%	67.4%
Ｗｅｂ（政府、地方公共団体）	6.8%	6.0%
ＩＳＰからのお知らせ(Ｗｅｂ・メール）	39.4%	23.7%
ウィルスを含むセキュリティ対策ソフトの会社	57.5%	54.1%
職場、学校、知人	12.5%	15.6%
その他	1.3%	2.2%
全回答者数	2,468	2,147

※各年度で調査方法(設問の構成・内容)や調査手法が異なるため、単純な経年比較はできない。

○　情報の入手経路（情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構）

＜平成 17 年＞

（男女別）

単位：%

	ソフトメーカーのウェブサイト等	パソコンメーカー等のウェブサイト等	家族や知人	ポータルサイトのトピックス・ニュース等	IT関連のウェブサイト等	テレビ・新聞等	雑誌や専門書	セキュリティ関連の組織のウェブサイト等	セミナーや研究会	その他	入手していない
全体	46.6	44.8	23.4	20.1	19.5	17.6	10.1	7.0	0.6	0.9	14.9
男性	55.6	48.3	13.1	26.1	27.6	16.9	14.0	9.4	0.9	1.0	11.9
女性	38.1	41.5	33.1	14.5	12.0	18.3	6.4	4.8	0.3	0.8	17.7

（年代別）

単位：%

	ソフトメーカーのウェブサイト等	パソコンメーカー等のウェブサイト等	家族や知人	ポータルサイトのトピックス・ニュース等	IT関連のウェブサイト等	テレビ・新聞等	雑誌や専門書	セキュリティ関連の組織のウェブサイト等	セミナーや研究会	その他	入手していない
全体	46.6	44.8	23.4	20.1	19.5	17.6	10.1	7.0	0.6	0.9	14.9
10代	31.5	27.2	28.0	19.8	16.4	15.1	9.5	6.0	0.4	0.9	28.0
20代	39.1	37.3	25.6	22.0	22.1	16.1	11.4	6.2	0.5	0.8	17.1
30代	48.5	45.3	24.7	21.0	19.6	16.7	9.3	6.9	0.7	0.8	14.1
40代	55.7	53.4	18.1	18.7	19.0	19.5	10.0	8.6	0.5	0.8	11.2
50代以上	45.6	51.6	21.8	14.8	15.4	22.2	10.4	6.8	0.6	1.2	14.0

（職業別）

単位：%

	ソフトメーカーのウェブサイト等	パソコンメーカー等のウェブサイト等	家族や知人	ポータルサイトのトピックス・ニュース等	IT関連のウェブサイト等	テレビ・新聞等	雑誌や専門書	セキュリティ関連の組織のウェブサイト等	セミナーや研究会	その他	入手していない
全体	46.6	44.8	23.4	20.1	19.5	17.6	10.1	7.0	0.6	0.9	14.9
経営者・役員	52.9	55.8	10.6	16.3	25.0	13.5	8.7	11.5	1.0	0.0	8.7
会社員等（情報システム関係の技術者）	55.2	43.4	13.8	31.7	41.5	17.7	16.8	14.7	2.3	2.1	9.3
会社員・公務員・派遣社員（その他）	51.6	48.8	18.1	22.2	20.1	16.7	11.0	7.2	0.5	1.1	14.0
自営業・自由業	58.5	55.4	18.3	24.1	21.0	20.8	10.3	5.8	1.1	0.4	8.7
専業主婦／家事手伝い・無職	37.5	39.7	34.7	11.8	9.0	19.4	5.9	4.9	0.1	0.6	17.4
パート・アルバイト	39.5	43.3	30.8	14.0	15.2	17.5	7.8	4.8	0.0	0.3	16.4
学生	35.1	30.9	28.3	23.7	22.7	15.9	12.2	7.2	0.6	0.6	22.0

＜平成 18 年＞

（男女別）

単位:**%**

	テレビCM	テレビの特集番組	テレビニュース・情報番組での解説コーナー	ポスター	ウェブページ（解説やニュース）	ウェブページ（クイズ、ゲーム、アニメ等）	チラシ・冊子	新聞広告	街頭キャンペーン	その他
全体	31.2	23.6	28.7	9.8	72.2	10.6	16.0	15.4	7.0	3.6
男性	32.3	24.4	27.6	11.9	76.9	12.7	19.2	17.3	8.5	3.7
女性	30.0	22.8	30.0	7.4	67.2	8.4	12.5	13.4	5.3	3.4

（年代別）

単位:**%**

	テレビCM	テレビの特集番組	テレビニュース・情報番組での解説コーナー	ポスター	ウェブページ（解説やニュース）	ウェブページ（クイズ、ゲーム、アニメ等）	チラシ・冊子	新聞広告	街頭キャンペーン	その他
全体	31.2	23.6	28.7	9.8	72.2	10.6	16.0	15.4	7.0	3.6
10代	35.1	22.1	21.7	13.7	67.8	12.0	17.7	12.6	6.9	3.5
20代	34.3	21.3	25.6	12.7	72.4	12.8	17.5	11.6	8.0	2.3
30代	29.8	26.4	27.7	9.6	75.4	10.0	15.3	11.8	7.7	3.0
40代	31.4	23.4	31.4	9.2	76.4	9.9	17.4	18.1	7.8	3.0
50代	28.3	22.4	30.8	5.4	71.3	11.1	13.0	19.8	5.4	5.8
60代	27.5	26.7	36.9	7.6	64.4	7.1	14.1	21.6	4.3	4.8

＜平成 19 年＞

（男女別）

	セキュリティ対策ソフトメーカのウェブサイト、メールマガジン等	テレビのニュース、情報番組での解説コーナー	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	テレビCM	雑誌や専門書	新聞	家族・友人・知人の話	テレビの特集番組	ポータルサイトのトピックス、ニュース等	IT関連のウェブサイト、メールマガジン等
全体	38.7%	38.4%	37.6%	36.5%	35.2%	34.5%	32.6%	29.0%	24.6%	16.6%
男性	45.3%	36.9%	41.4%	37.7%	44.6%	37.6%	24.5%	30.2%	30.6%	22.8%
女性	31.3%	40.0%	33.3%	35.2%	24.6%	31.1%	41.7%	27.8%	17.8%	9.6%

	セキュリティ関連のブログ	セキュリティ専門のウェブサイト、メーリングリスト等	ウェブページ（クイズ、ゲーム、アニメ等）	政府・自治体、その他セキュリティ関連の組織団体のウェブサイト、メー	セミナー・研究会	eラーニング	その他	見聞きしたことはない	（参考）回答者数人
全体	16.5%	14.3%	6.2%	5.9%	4.1%	4.0%	0.9%	6.7%	5,160
男性	19.7%	18.4%	6.8%	8.9%	5.9%	5.3%	0.7%	5.4%	2,734
女性	12.8%	9.7%	5.5%	2.6%	2.1%	2.6%	1.2%	8.1%	2,427

（年代別）

	セキュリティ対策ソフトメーカのウェブサイト、メールマガジン等	テレビのニュース、情報番組での解説コーナー	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	テレビCM	雑誌や専門書	新聞	家族・友人・知人の話	テレビの特集番組	ポータルサイトのトピックス、ニュース等	IT関連のウェブサイト、メールマガジン等
全体	38.7%	38.4%	37.6%	36.5%	35.2%	34.5%	32.6%	29.0%	24.6%	16.6%
15～19歳	20.0%	32.2%	20.6%	39.1%	24.7%	23.1%	30.9%	29.2%	18.6%	12.6%
20～29歳	28.0%	38.5%	25.1%	42.0%	33.1%	30.3%	33.9%	30.7%	26.3%	17.1%
30～39歳	39.4%	36.7%	35.0%	35.2%	37.9%	29.8%	34.5%	29.7%	27.4%	17.7%
40～49歳	47.7%	38.5%	44.7%	35.2%	42.3%	32.4%	31.8%	27.7%	24.7%	17.2%
50～59歳	43.4%	41.2%	46.2%	36.5%	36.9%	43.5%	29.8%	28.9%	24.4%	16.9%
60歳以上	47.2%	41.4%	51.2%	30.9%	28.6%	47.6%	32.7%	27.3%	20.7%	15.2%

	セキュリティ関連のブログ	セキュリティ専門のウェブサイト、メーリングリスト等	ウェブページ（クイズ、ゲーム、アニメ等）	政府・自治体、その他セキュリティ関連の組織団体のウェブサイト、メールマガジン等	セミナー・研究会	eラーニング	その他	見聞きしたことはない	（参考）回答者数
全体	16.5%	14.3%	6.2%	5.9%	4.1%	4.0%	0.9%	6.7%	5,160
15～19歳	11.2%	10.5%	12.0%	3.3%	2.1%	2.6%	2.6%	15.7%	425
20～29歳	14.7%	13.1%	8.3%	4.5%	5.4%	5.7%	1.5%	8.7%	1,031
30～39歳	16.7%	14.1%	5.6%	3.5%	3.2%	4.3%	0.6%	4.8%	1,224
40～49歳	17.9%	15.1%	4.4%	6.8%	4.6%	4.7%	0.9%	5.3%	915
50～59歳	16.9%	14.5%	5.2%	6.5%	4.5%	3.3%	0.5%	4.9%	885
60歳以上	19.5%	17.6%	4.3%	12.1%	4.1%	1.5%	0.2%	5.5%	682

※何れも、複数回答による。
※平成 17 年、平成 18 年、平成 19 年では調査方法が異なる。

○ **希望する情報提供方法（情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構）**

＜平成 17 年＞

（男女別）

単位：**%**

	ポータルサイトの目立つ場所	最新情報が自動的にデスクトップ表示	メールマガジン	テレビのCM	ニュース内	新聞内	無料配布冊子	RSS配信	行政や業者による無料セミナー	その他
全体	48.8	40.9	36.4	26.4	23.6	19.1	15.6	7.6	5.2	1.3
男性	54.3	37.5	40.5	21.0	20.4	17.6	13.7	10.7	5.1	1.6
女性	43.5	44.1	32.5	31.4	26.7	20.4	17.4	4.6	5.2	1.0

（年代別）

単位：**%**

	ポータルサイトの目立つ場所	最新情報が自動的にデスクトップ表示	メールマガジン	テレビのCM	ニュース内	新聞内	無料配布冊子	RSS配信	行政や業者による無料セミナー	その他
全体	48.8	40.9	36.4	26.4	23.6	19.1	15.6	7.6	5.2	1.3
10代	48.3	25.0	20.7	40.1	32.3	19.0	19.0	6.5	2.2	1.7
20代	51.8	37.5	28.3	35.7	27.5	18.6	19.4	9.6	4.9	0.7
30代	50.2	41.7	35.0	25.5	24.5	19.6	14.6	7.6	4.8	1.2
40代	47.0	43.9	46.1	17.2	17.7	17.5	11.6	6.4	5.0	1.8
50代以上	39.2	47.6	49.2	19.0	19.0	21.6	17.0	5.2	9.0	1.6

（職業別）

単位：%

	ポータルサイトの目立つ場所	最新情報が自動的にデスクトップ表示	メールマガジン	テレビのCM	ニュース内	新聞内	無料配布冊子	RSS配信	行政や業者による無料セミナー	その他
全体	48.8	40.9	36.4	26.4	23.6	19.1	15.6	7.6	5.2	1.3
経営者・役員	50.0	29.8	43.3	17.3	15.4	15.4	8.7	5.8	1.9	1.9
会社員等（情報システム関係の技術者）	57.1	31.7	38.7	19.3	20.3	17.7	10.0	15.2	6.1	1.4
会社員・公務員・派遣社員（その他）	51.1	40.7	37.7	23.3	20.7	17.2	14.5	7.7	5.0	1.5
自営業・自由業	52.2	45.8	50.0	18.1	19.0	15.8	14.1	9.2	5.4	1.1
専業主婦／家事手伝い・無職	40.3	47.9	32.9	30.6	27.2	23.2	18.0	4.4	5.8	0.8
パート・アルバイト	45.3	42.8	36.3	30.5	27.1	21.3	17.4	5.5	5.6	1.4
学生	50.5	31.6	24.0	38.8	32.0	20.1	19.8	8.5	3.5	0.9

＜平成 18 年＞

（男女別）

単位：%

	ポータルサイトの目立つ場所	ウェブ上のニュース	e-ラーニング	RSS配信	メールマガジン・メーリングリスト	最新情報が自動的にデスクトップに表示	テレビのCM	テレビニュース・情報番組の解説コーナー	新聞	行政や業者による無料セミナー	無料配布冊子	その他	特に希望するものはない
全体	44.0	45.7	2.6	5.4	30.8	25.2	24.5	24.1	21.2	7.1	19.7	0.6	10.8
男性	47.5	48.7	3.3	7.2	34.9	24.4	20.4	20.1	20.5	6.5	17.6	0.7	10.1
女性	40.2	42.5	1.9	3.3	26.3	26.2	29.1	28.4	22.0	7.8	22.1	0.6	11.6

（年代別）

単位：%

	ポータルサイトの目立つ場所	ウェブ上のニュース	e-ラーニング	RSS配信	メールマガジン・メーリングリスト	最新情報が自動的にデスクトップに表示	テレビのCM	テレビニュース・情報番組の解説コーナー	新聞	行政や業者による無料セミナー	無料配布冊子	その他	特に希望するものはない
全体	44.0	45.7	2.6	5.4	30.8	25.2	24.5	24.1	21.2	7.1	19.7	0.6	10.8
10代	41.2	37.7	2.7	6.0	16.3	17.0	34.4	22.2	17.1	5.2	23.0	0.6	18.5
20代	49.3	46.6	3.5	5.9	21.5	19.7	30.3	26.9	17.7	6.4	23.0	0.5	11.7
30代	51.3	49.1	2.0	5.7	29.3	22.7	26.4	23.8	19.8	6.9	19.6	0.5	9.1
40代	44.4	46.9	2.7	5.7	38.1	25.9	21.3	23.1	21.0	6.7	16.1	0.7	10.2
50代	35.8	45.4	2.4	4.5	40.6	33.4	15.8	21.3	24.0	8.3	18.9	1.0	8.2
60代	34.3	45.0	2.5	3.7	39.8	36.6	17.8	27.7	31.3	10.4	18.1	0.9	8.6

（職業別）

単位：%

	ポータルサイトの目立つ場所	ウェブ上のニュース	e-ラーニング	RSS配信	メールマガジン・メーリングリスト	最新情報が自動的にデスクトップに表示	テレビのCM	テレビニュース・情報番組の解説コーナー	新聞	行政や業者による無料セミナー	無料配布冊子	その他	特に希望するものはない
全体	44.0	45.7	2.6	5.4	30.8	25.2	24.5	24.1	21.2	7.1	19.7	0.6	10.8
経営者・役員	50.4	47.2	2.4	4.9	45.4	24.3	12.1	21.4	23.7	9.1	17.4	1.0	5.7
会社員等（情報システム関係の技術者）	60.4	53.3	8.4	14.2	33.6	19.6	18.9	21.2	16.8	8.5	15.9	1.2	7.2
会社員・公務員・派遣社員（その他）	47.1	49.1	3.1	5.5	33.1	24.9	20.9	19.9	18.0	7.7	17.5	0.6	9.4
自営業・自由業	44.7	51.2	2.7	7.4	40.4	28.1	19.6	22.0	21.5	6.1	17.0	0.7	8.5
専業主婦／家事手伝い・無職	38.7	43.0	1.3	3.3	29.6	31.0	25.7	30.3	27.3	8.1	20.6	0.6	10.5
パート・アルバイト	36.6	41.2	1.0	2.4	29.9	22.6	27.8	27.3	21.6	7.3	22.6	0.6	13.4
学生	45.5	39.7	3.7	6.5	17.8	18.2	35.3	24.2	19.4	5.0	24.5	0.8	16.2
その他	39.2	46.4	0.7	5.2	35.8	29.4	23.6	25.4	22.0	4.7	19.0	0.5	8.8

＜平成 19 年＞

（男女別）

単位：%

	ポータルサイトの目立つ場所	ウェブ上のニュース	テレビのニュース、情報番組での解説コーナー	テレビCM	新聞	無料配布冊子	メールマガジン、メーリングリスト	最新情報が自動的にデスクトップに表示	Q&Aサイト	パソコン売場など量販店の店頭ポスター・チラシ	ブログ・掲示板等	mixiなどのSNS内コミュニティ	行政や業者による無料セミナー
全体	52.7	44.6	29.2	26.5	26.2	22.0	21.1	20.0	17.7	15.6	12.7	10.5	7.5
男性	57.1	45.5	24.9	21.6	24.8	20.1	23.8	18.4	18.4	14.0	13.6	9.4	7.5
女性	47.7	43.6	34.0	32.0	27.8	24.3	18.0	21.9	16.9	17.3	11.8	11.8	7.5

	ウェブページ（クイズ、ゲーム、アニメ等）	その他	現在入手している情報で十分	特に情報を得たいとは思わない
全体	7.5	0.5	3.4	5.4
男性	8.4	0.7	4.3	5.7
女性	6.5	0.3	2.4	5.1

（年代別）

単位：%

	ポータルサイトの目立つ場所	ウェブ上のニュース	テレビのニュース、情報番組での解説コーナー	テレビCM	新聞	無料配布冊子	メールマガジン、メーリングリスト	最新情報が自動的にデスクトップに表示	Q&Aサイト	パソコン売場など量販店の店頭ポスター・チラシ	ブログ・掲示板等	mixiなどのSNS内コミュニティ	行政や業者による無料セミナー
全体	52.7	44.6	29.2	26.5	26.2	22.0	21.1	20.0	17.7	15.6	12.7	10.5	7.5
15～19歳	54.4	46.4	32.8	38.1	21.9	24.1	11.1	11.7	17.2	16.4	18.6	18.5	4.2
20～29歳	62.7	47.5	31.8	35.6	23.1	26.6	12.7	18.6	18.0	19.2	15.7	22.0	7.3
30～39歳	56.4	47.5	29.5	26.5	24.2	22.7	16.6	19.4	20.5	15.9	14.2	9.7	6.3
40～49歳	52.0	43.7	27.6	21.4	24.5	21.5	24.5	20.3	18.2	13.7	9.9	6.2	8.0
50～59歳	44.9	41.4	24.1	19.8	28.5	18.9	29.2	25.8	15.3	14.2	10.8	5.1	7.9
60歳以上	40.7	39.4	31.0	21.0	36.5	17.5	32.7	28.3	14.9	13.3	8.2	2.6	10.9

	ウェブページ（クイズ、ゲーム、アニメ等）	その他	現在入手している情報で十分	特に情報を得たいとは思わない
全体	7.5	0.5	3.4	5.4
15～19歳	13.5	0.3	1.9	11.5
20～29歳	8.6	0.7	1.5	5.4
30～39歳	7.7	0.5	2.2	4.3
40～49歳	5.9	0.6	4.3	4.3
50～59歳	6.2	0.3	4.4	5.6
60歳以上	5.4	0.5	6.8	4.9

※何れも、複数回答による。

※平成 17 年,平成 18 年,平成 19 年では調査方法が異なる。

○ **無線ＬＡＮ機器のセキュリティ対策の必要性に関する周知状況（インターネットの利用実態に関する調査：総務省）**

	１８年	１９年
製品パッケージ、取扱説明書を見て	24.9%	20.1%
製品購入時に店員から説明を受けた	4.0%	3.9%
ＩＳＰ等から(直接又はメール等により）説明を受けた	6.3%	3.7%
ＩＳＰ等のＨＰを見て	13.1%	7.3%
専門誌等を見て	26.9%	17.3%
知人等から知らされた	13.0%	17.7%
その他	7.7%	5.5%
セキュリティ対策の重要性を知らない	33.7%	42.5%
回答者数	2,979	3,090

※各年度で調査方法(設問の構成・内容)や調査手法が異なるため、単純な経年比較はできない。

○ 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、重要情報の漏洩等）の重要性の認識（情報処理実態調査：経済産業省）

（下段（）内数値は前年度からの増減）　　単位%

トラブルの種類		トラブルの認識											
		非常に重要である（%）			どちらかといえば重要である（%）			重要でない（%）			わからない（%）		
		18年調査	17年調査	16年調査	18年調査	17年調査	16年調査	18年調査	17年調査	16年調査	18年調査	17年調査	16年調査
システムトラブル	システム・トラブル計（*1）	70.2 (13.8)	56.4	-	22.3 (0.0)	22.3	-	3.7 (0.6)	3.1	-	3.8 (△14.0)	17.8	-
	内部要因によるシステムの停止	82.5 (-)	-	-	13.4 (-)	-	-	1.9 (-)	-	-	2.2 (-)	-	-
	システム破壊・サーバ停止	-	79.0 (3.2)	75.8	-	5.2 (△1.0)	6.2	-	0.5 (0.0)	0.5	-	15.4 (△2.0)	17.4
	外部要因（地震、火災等の問題）によるシステムの停止	72.3 (-)	-	-	23.1 (-)	-	-	1.9 (-)	-	-	2.7 (-)	-	-
	自然災害による障害（地震、火災等の問題）	-	61.9 (4.1)	57.8	-	16.6 (△2.0)	18.6	-	0.9 (△0.6)	1.5	-	20.5 (△1.7)	22.2
	Dos攻撃	57.0 (4.3)	52.7 (2.9)	49.8	29.9 (9.2)	20.7 (0.2)	20.5	6.7 (3.5)	3.2 (△0.1)	3.3	6.5 (△16.9)	23.4 (△3.1)	26.5
	ホームページやファイル、データの改ざん	68.3 (9.1)	59.2 (2.9)	56.3	23.6 (6.9)	16.7 (△0.4)	17.1	4.3 (2.6)	1.7 (△0.3)	2.0	3.8 (△18.5)	22.3 (△2.3)	24.6
不正アクセス	不正アクセス計	66.0 (14.2)	51.8	-	25.8 (0.6)	25.2	-	3.9 (0.7)	3.2	-	4.4 (△15.5)	19.9	-
	IP・メールアドレス詐称	62.7 (9.6)	53.1 (2.0)	51.1	28.5 (4.9)	23.6 (0.2)	23.4	4.5 (2.3)	2.2 (△0.2)	2.4	4.3 (△16.7)	21.0 (△2.1)	23.1
	リソースの不正使用	61.8 (10.5)	51.3 (2.3)	49.0	28.2 (5.5)	22.7 (0.5)	22.2	4.6 (2.4)	2.2 (△0.1)	2.3	5.5 (△18.2)	23.7 (△2.9)	26.6
	内部者の不正アクセス	73.5 (15.0)	58.5 (2.7)	55.8	20.6 (2.8)	17.8 (△0.3)	18.1	2.6 (1.1)	1.5 (△0.3)	1.8	3.3 (△18.9)	22.2 (△2.0)	24.2
コンピュータウィルス	コンピュータウィルス計	68.2 (8.6)	59.6	-	24.6 (4.1)	20.5	-	3.3 (0.8)	2.5	-	4.0 (△13.4)	17.4	-
	ウィルスやワーム	75.0 (△2.1)	77.1 (1.7)	75.4	20.4 (4.9)	15.5 (△1.6)	17.1	2.1 (0.5)	1.6 (0.1)	1.5	2.5 (△3.3)	5.8 (△0.2)	6.0
	スパムメールの中継利用等(*2)	56.1 (△1.1)	57.2 (3.8)	53.4	31.6 (11.6)	20.0 (△1.1)	21.1	6.1 (4.2)	1.9 (0.3)	1.6	6.2 (△14.7)	20.9 (△2.9)	23.8
	トロイの木馬	72.8 (12.1)	60.7 (4.9)	55.8	22.2 (4.0)	18.2 (△1.9)	20.1	1.7 (0.2)	1.5 (0.1)	1.4	3.3 (△16.3)	19.6 (△3.1)	22.7
重要情報の漏洩	重要情報の漏洩計（*1）	82.5 (20.7)	61.8	-	12.9 (△4.1)	17.0	-	1.9 (△0.1)	2.0	-	2.6 (△16.7)	19.3	-
	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洩	85.1 (-)			11.2 (-)			1.3 (-)			2.5 (-)		
	不正アクセスによる情報漏洩	83.7 (-)			12.0 (-)			1.8 (-)			2.5 (-)		
	パスワードの盗用	-	64.9 (1.9)	63.0	-	12.5 (0.1)	12.4	-	0.9 (△0.1)	1.0	-	21.6 (△2.0)	23.6
	内部者による情報漏洩	85.0 (15.6)	69.4 (2.7)	66.7	11.0 (2.4)	8.6 (△0.6)	9.2	1.6 (0.9)	0.7 (△0.1)	0.8	2.3 (△19.0)	21.3 (△2.0)	23.3
	委託先による情報漏洩	80.2 (14.8)	65.4 (65.4)		13.5 (2.8)	10.7 (10.7)		2.8 (1.4)	1.4 (1.4)		3.6 (△18.9)	22.5 (22.5)	
	ノートパソコン及び携帯記憶媒体等の盗難・紛失	78.5 (12.7)	65.8 (65.8)		17.0 (3.1)	13.9 (13.9)		2.3 (1.2)	1.1 (1.1)		2.2 (△17.0)	19.2 (19.2)	
その他	その他計	44.3 (20.4)	23.9	-	35.3 (16.8)	18.5	-	8.7 (5.4)	3.3	-	11.7 (△42.6)	54.3	-
	ホームページ上での誹謗中傷等	46.9 (7.1)	39.8 (△0.2)	40.0	38.7 (8.1)	30.6 (2.8)	27.8	8.6 (3.3)	5.3 (0.0)	5.3	5.8 (△18.5)	24.3 (△2.6)	26.9
	その他	31.9 (25.8)	6.1 (△1.2)	7.3	18.8 (16.5)	2.3 (△0.9)	3.2	9.5 (8.4)	1.1 (0.1)	1.0	39.8 (△50.6)	90.4 (1.8)	88.6

(*1) 含まれる項目が異なるため単純比較はできない。
(*2) 18 年調査ではスパムメールの中継利用等は不正アクセスの項。前年との比較のため本項に含める。
※　回答企業数　　18 年調査：3,647 社　17 年調査：4,241 社　16 年調査：3,838 社
※　調査対象期間　18 年調査：平成 17 年度　17 年調査：平成 16 年度　16 年調査：平成 15 年度
※　19 年調査については、現在実施中

○ リスク分析の実施状況・情報セキュリティポリシーの策定状況・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）

単位:特段記載がない場合、%

対策の種類	対策の実施状況												（参考）回答企業数（社）		
	既に実施している			実施を検討している			必要性を感じるが、未実施			必要性を感じず、未実施					
	18年	17年	16年	18年	17年	16年	18年	17年	16年	18年	17年	16年	18年	17年	16年
リスク分析	29.7 (△0.9)	30.6 (10.2)	20.4	12.7 (△1.8)	14.5 (△2.1)	16.6	45.6 (△1.5)	47.1 (△4.8)	51.9	12.5 (3.8)	8.7 (△2.4)	11.1	3,340	4,138	3,944
セキュリティポリシーの策定	43.5 (△0.4)	43.9 (14.2)	29.7	13.4 (△2.1)	15.5 (△5.9)	21.4	33.7 (△1.1)	34.8 (△5.3)	40.1	9.6 (3.0)	6.6 (△2.3)	8.9	3,374	4,224	3,944
全社的なセキュリティ管理者の配置	44.1 (△3.0)	47.1 (11.9)	35.2	10.6 (△1.6)	12.2 (△4.5)	16.7	36.5 (1.0)	35.5 (△5.4)	40.9	9.5 (3.8)	5.7 (△1.6)	7.3	3,366	4,233	3,944
部門ごとのセキュリティ管理者の配置	32.1 (△2.0)	34.1 (9.7)	24.4	11.2 (△1.0)	12.2 (△4.3)	16.5	41.2 (△1.1)	42.3 (△3.9)	46.2	16.1 (4.3)	11.8 (△1.2)	13.0	3,347	4,200	3,944

（効果）

単位:特段記載がない場合、%

対策の種類	効　　果									（参考）回答企業数（社）		
	効果があった			あまり効果がない			よくわからない					
	18年	17年	16年	18年	17年	16年	18年	17年	16年	18年	17年	16年
リスク分析	66.5	65.3	66.0	1.7	8.5	6.2	31.8	26.2	27.7	1,027	1,297	739
セキュリティポリシーの策定	67.2	63.3	64.1	3.1	11.4	8.6	29.6	25.3	27.4	1,434	1,814	1,085
全社的なセキュリティ管理者の配置	74.2	70.4	69.8	2.4	10.3	7.3	23.4	19.3	22.9	1,352	1,841	1,129
部門ごとのセキュリティ管理者の配置	70.5	65.2	65.1	3.3	13.3	10.7	26.3	21.5	24.2	1,040	1,384	848

※　調査対象期間　18 年調査：平成 17 年度　17 年調査：平成 16 年度　16 年調査：平成 15 年度

※　19 年調査については、現在実施中。

※　実施状況中、「既に実施している」には、「トラブルがあったので対策を講じた」を含む（全体に占める割合は括弧内、平成 16 年は未調査。）。

※　効果については、「既に実施している」及び「実施を検討している」と回答した者についてのみ、調査。

○ 重要なシステムへの内部でのアクセス管理の実施状況・データの暗号化実施状況・外部接続へのファイアウォールの配置状況・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）

単位：特段記載がない場合、%

対策の種類	対策の実施状況												(参考) 回答企業数（社）		
	既に実施している			実施を検討している			必要性を感じるが、未実施			必要性を感じず、未実施					
	18年	17年	16年	18年	17年	16年	18年	17年	16年	18年	17年	16年	18年	17年	16年
重要なシステムへの内部でのアクセス管理	59.0 (1.1)	57.9 (7.2)	50.7	10.2 (△0.3)	10.5 (△3.0)	13.5	23.2 (△1.9)	25.1 (△2.6)	27.7	8.1 (1.2)	6.9 (△1.3)	8.2	3,366	4,247	3,944
データの暗号化（PKIを含む）	29.2 (1.3)	27.9 (27.9)		13.1 (△2.9)	16.0 (16.0)		39.7 (△1.5)	41.2 (41.2)		18.2 (3.0)	15.2 (15.2)		3,336	4,167	3,944
外部接続へのファイアウォールの配置	71.3 (△2.1)	73.4 (6.7)	66.7	5.0 (△0.8)	5.8 (△1.1)	6.9	15.6 (0.2)	15.4 (△3.3)	18.7	8.9 (2.5)	6.4 (△1.3)	7.7	3,380	4,249	3,944
セキュリティ監視ソフトの導入	54.4 (5.3)	49.1 (8.5)	40.6	10.6 (△4.0)	14.6 (△2.2)	16.8	26.8 (△4.0)	30.8 (△3.0)	33.8	9.8 (2.2)	7.6 (△1.2)	8.8	3,401	4,251	3,944

（効果）

単位：特段記載がない場合、%

対策の種類	効　果									(参考) 回答企業数（社）		
	効果があった			あまり効果がない			よくわからない					
	18年	17年	16年	18年	17年	16年	18年	17年	16年	18年	17年	16年
重要なシステムへの内部でのアクセス管理	81.2	80.7	83.0	1.4	4.7	3.8	17.4	14.6	13.2	1,738	2,171	1,441
データの暗号化（PKIを含む）	73.5	72.6		1.3	4.8		25.2	22.7		968	1,217	
外部接続へのファイアウォールの配置	85.7	87.1	87.9	0.7	1.8	1.9	13.6	11.1	10.2	1,973	2,583	1,738
セキュリティ監視ソフトの導入	82.7	81.2	80.3	1.0	3.6	3.3	16.4	15.2	16.4	1,553	1,828	1,181

※　調査対象期間　17 年調査：平成 16 年度　16 年調査：平成 15 年度

※　19 年調査については、現在実施中。

※　実施状況中、「既に実施している」には、「トラブルがあったので対策を講じた」を含む（全体に占める割合は括弧内、平成 16 年は未調査。）。

※　効果については、「既に実施している」及び「実施を検討している」と回答した者についてのみ、調査。

※　「データの暗号化」については、平成 17 年から調査を開始。

○ **重要なシステムへの内部でのアクセス管理の実施状況・データの暗号化実施状況・外部接続へのファイアウォールの配置状況・セキュリティ監視ソフトの導入状況（通信利用動向調査：総務省）**

単位：%

	15年末 (n=2,251)	16年末 (n=1,855)	17年末 (n=1,391)	18年末 (n=1,823)
パソコンなどの端末（OS、ソフト等）にウィルスチェックプログラムを導入	72.7	81.0	80.5	80.9
サーバにウィルスチェックプログラムを導入	56.5	59.0	64.3	66.1
ファイアウォールの設置	52.2	46.4	46.8	51.3
ID、パスワードによるアクセス制御	54.2	37.6	44.6	51.0
データやネットワークの暗号化	11.0	6.1	10.7	13.9

○ **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）**

	15年	16年	17年	18年	19年
実施している	24.9%	35.5%	45.9%	54.5%	28.4%
実施を予定している	9.8%	12.4%	9.9%	8.9%	6.4%
実施はしていないが必要性を感じる	60.5%	49.2%	41.6%	34.6%	44.7%
実施の必要性を感じない	3.7%	2.2%	1.2%	1.5%	18.4%
無回答	1.1%	0.6%	1.5%	0.6%	2.1%
（参考）発送数	2,000	2,000	2,500	2,500	2,500
（参考）回収数	732	628	606	1024	613
（参考）回収率	36.6%	31.4%	24.2%	41.0%	24.5%

○ **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）**

単位：%

対策の種類	対策の実施状況												（参考）回答企業数（社）		
	既に実施している			実施を検討している			必要性を感じるが、未実施			必要性を感じず、未実施					
	18年	17年	16年	18年	17年	16年	18年	17年	16年	18年	17年	16年	18年	17年	16年
従業員に対する情報セキュリティ教育	43.1 (2.0)	41.1 (13.9)	27.2	13.7 (△1.9)	15.6 (△6.0)	21.6	37.6 (△2.1)	39.7 (△5.9)	45.6	6.6 (2.0)	4.6 (△1.0)	5.6	3,376	4,241	3,944

（効果）

単位：%

対策の種類	効果									（参考）回答企業数（社）		
	効果があった			あまり効果がない			よくわからない					
	18年	17年	16年	18年	17年	16年	18年	17年	16年	18年	17年	16年
従業員に対する情報セキュリティ教育	74.4 (5.7)	68.7 (4.0)	64.7	2.3 (△9.5)	11.8 (△0.1)	11.9	23.3 (3.8)	19.5 (△3.9)	23.4	1,384	1,685	1,014

※　調査対象期間　18 年調査：平成 17 年度　17 年調査：平成 16 年度　16 年調査：平成 15 年度
※　19 年調査については、現在実施中。
※　実施状況中、「既に実施している」には、「トラブルがあったので対策を講じた」を含む（全体に占める割合は括弧内、平成 16 年は未調査。）。
※　効果については、「既に実施している」及び「実施を検討している」と回答した者についてのみ、調査。

○ パッチ適用実施率（コンピュータウィルスに関する被害状況調査：情報処理推進機構、2006 年　国内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）

クライアント			15年	16年	17年	18年
常に最新のセキュリティパッチを適用している	全体		30.7%	31.2%	32.0%	35.4%
		企業	28.6%	27.7%	32.2%	36.6%
		自治体	33.6%	38.1%	31.5%	32.9%
定期的に適用している	全体		23.5%	25.2%	32.2%	32.9%
		企業	21.2%	21.0%	27.6%	29.6%
		自治体	26.7%	33.5%	43.2%	40.0%
気がついたときに適用している	全体		19.5%	18.2%	20.0%	15.6%
		企業	17.2%	19.6%	23.1%	16.7%
		自治体	22.6%	15.5%	12.3%	13.3%
ほとんど適用していない	全体		13.8%	9.5%	12.2%	12.6%
		企業	14.6%	10.4%	12.4%	12.9%
		自治体	12.7%	7.7%	11.5%	11.7%
分からない	全体		10.2%	13.3%	2.4%	2.7%
		企業	15.1%	18.1%	3.0%	3.5%
		自治体	3.4%	3.9%	0.8%	1.1%
無回答	全体		2.3%	2.6%	1.4%	0.8%
		企業	3.4%	3.3%	1.7%	0.7%
		自治体	0.9%	1.3%	0.6%	0.9%
（参考）回答総数	全体		1,115	1,150	1,701	1,775
		企業	651	762	1,206	1,213
		自治体	464	388	495	562

ネットワークサーバ		15年	16年	17年	18年
常に最新のセキュリティパッチを適用している	全体	32.6%	29.2%	30.6%	30.5%
	企業	24.9%	22.6%	29.6%	28.1%
	自治体	43.5%	42.3%	33.1%	35.6%
定期的に適用している	全体	20.8%	19.9%	33.4%	33.7%
	企業	12.4%	12.1%	27.7%	29.2%
	自治体	32.5%	35.3%	47.3%	43.4%
気がついたときに適用している	全体	10.0%	6.3%	8.2%	7.0%
	企業	9.8%	5.8%	8.3%	7.7%
	自治体	10.3%	7.5%	8.1%	5.5%
ほとんど適用していない	全体	16.4%	12.6%	7.3%	9.0%
	企業	23.0%	16.0%	8.3%	10.1%
	自治体	7.1%	5.9%	4.8%	6.4%
分からない	全体	13.0%	21.6%	9.5%	8.5%
	企業	20.6%	30.4%	12.4%	11.0%
	自治体	2.4%	4.1%	2.4%	3.0%
無回答	全体	7.1%	10.3%	10.9%	11.4%
	企業	9.2%	13.1%	13.7%	13.8%
	自治体	4.1%	4.9%	4.2%	6.0%
（参考）回答総数	全体	1,115	1,150	1,701	1,775
	企業	651	762	1,206	1,213
	自治体	464	388	495	562

ローカルサーバ		15年	16年	17年	18年
常に最新のセキュリティパッチを適用している	全体	25.1%	24.3%	24.6%	24.4%
	企業	21.8%	20.7%	24.5%	23.9%
	自治体	29.7%	31.4%	24.6%	25.4%
定期的に適用している	全体	22.8%	22.7%	35.7%	38.3%
	企業	16.9%	15.9%	30.6%	34.7%
	自治体	31.0%	36.1%	48.1%	45.9%
気がついたときに適用している	全体	14.7%	13.3%	14.5%	12.5%
	企業	14.1%	12.2%	16.0%	14.3%
	自治体	15.5%	15.5%	10.7%	8.7%
ほとんど適用していない	全体	17.8%	15.5%	16.2%	16.4%
	企業	20.4%	18.5%	17.7%	17.3%
	自治体	14.2%	9.5%	12.5%	14.4%
分からない	全体	13.2%	17.7%	5.4%	5.4%
	企業	18.9%	24.3%	6.5%	6.3%
	自治体	5.2%	4.9%	2.8%	3.4%
無回答	全体	6.4%	6.4%	3.7%	3.0%
	企業	7.8%	8.4%	4.7%	3.5%
	自治体	4.3%	2.6%	1.2%	2.1%
（参考）回答総数	全体	1,115	1,150	1,701	1,775
	企業	651	762	1,206	1,213
	自治体	464	388	495	562

（参考）回収率					
	全体	**22.6%（1,128/5,000）**	**23.2%（1,160/5,000）**	**25.9%（1,701/6,561）**	**21.6%（1,775/8200）**
	企業	**16.6%（663/4,000）**	**19.3%（770/4,000）**	**21.9%（1,206/5,500）**	**17.3%（1,213/7,000）**
	自治体	**46.5%（465/1,000）**	**39.0%（390/1,000）**	**46.7%（495/1,061）**	**46.8%（562/1,200）**

○ ウィルス対策ソフト導入率（コンピュータウィルスに関する被害状況調査：情報処理推進機構）

クライアント		15年	16年	17年	18年
９割以上のパソコンに導入済	全体	70.4%	73.8%	86.4%	90.3%
	企業	56.8%	63.9%	82.3%	87.6%
	自治体	89.4%	93.3%	96.6%	96.1%
半数以上のパソコンに導入済	全体	7.5%	7.2%	4.9%	2.9%
	企業	10.1%	9.6%	6.4%	3.4%
	自治体	3.9%	2.6%	1.4%	2.0%
半数未満のパソコンに導入済	全体	10.3%	10.9%	5.5%	4.6%
	企業	14.0%	15.0%	7.2%	6.1%
	自治体	5.2%	2.8%	1.4%	1.2%
導入していない	全体	8.0%	7.1%	2.4%	1.7%
	企業	12.6%	10.4%	3.2%	2.4%
	自治体	1.5%	0.8%	0.2%	0.2%
無回答	全体	3.8%	1.0%	0.8%	0.5%
	企業	6.5%	1.2%	0.9%	0.5%
	自治体	-	0.5%	0.4%	0.5%
（参考）回答総数	全体	1,115	1,150	1,701	1,775
	企業	651	762	1,206	1,213
	自治体	464	388	495	562

※　平成１８年度については、ウィルス対策ソフト及び統合セキュリティ対策ソフトの導入状況について調査

ネットワークサーバ		15年	16年	17年	18年
９割以上に導入済	全体	65.8%	58.0%	70.8%	74.4%
	企業	53.1%	47.6%	65.5%	69.2%
	自治体	83.6%	78.4%	83.8%	85.8%
半数以上に導入済	全体	3.5%	4.4%	4.3%	1.6%
	企業	3.4%	4.2%	4.1%	1.6%
	自治体	3.7%	4.9%	4.8%	1.6%
半数未満に導入済	全体	5.2%	3.0%	3.1%	1.9%
	企業	6.9%	2.9%	3.3%	2.3%
	自治体	2.8%	3.1%	2.6%	0.9%
導入していない	全体	21.4%	27.4%	14.9%	10.1%
	企業	31.6%	35.8%	18.5%	12.2%
	自治体	7.1%	10.8%	6.3%	5.5%
無回答	全体	4.0%	7.2%	6.8%	12.1%
	企業	4.9%	9.4%	8.6%	14.8%
	自治体	2.8%	2.8%	2.4%	6.2%
（参考）回答総数	全体	1,115	1,150	1,701	1,775
	企業	651	762	1,206	1,213
	自治体	464	388	495	562

ローカルサーバ		15年	16年	17年	18年
９割以上に導入済	全体	55.5%	60.6%	74.1%	78.2%
	企業	44.5%	49.9%	69.7%	75.6%
	自治体	70.9%	81.7%	84.8%	83.8%
半数以上に導入済	全体	5.6%	5.5%	7.1%	4.2%
	企業	4.8%	5.8%	7.2%	4.0%
	自治体	6.7%	4.9%	6.9%	4.6%
半数未満に導入済	全体	4.9%	5.1%	4.7%	3.2%
	企業	5.7%	5.2%	4.8%	3.5%
	自治体	3.9%	4.9%	4.4%	2.5%
導入していない	全体	29.0%	25.0%	11.8%	10.5%
	企業	39.3%	34.3%	15.6%	12.4%
	自治体	14.4%	7.0%	2.4%	6.2%
無回答	全体	5.0%	3.7%	2.4%	3.9%
	企業	5.7%	4.9%	2.7%	4.4%
	自治体	4.1%	1.5%	1.4%	2.8%
（参考）回答総数	全体	1,115	1,150	1,701	1,775
	企業	651	762	1,206	1,213
	自治体	464	388	495	562

(参考) 回収率	全体	22.6% (1,128/5,000)	23.2% (1,160/5,000)	25.9% (1,701/6,561)	21.6% (1,775/8200)
	企業	16.6% (663/4,000)	19.3% (770/4,000)	21.9% (1,206/5,500)	17.3% (1,213/7,000)
	自治体	46.5% (465/1,000)	39.0% (390/1,000)	46.7% (495/1,061)	46.8% (562/1,200)

○ 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）

単位：%

対策の種類	対策の実施状況												（参考）回答企業数（社）		
	既に実施している			実施を検討している			必要性を感じるが、未実施			必要性を感じず、未実施					
	18年	17年	16年	18年	17年	16年	18年	17年	16年	18年	17年	16年	18年	17年	16年
外部専門家による定期的な情報セキュリティ監査	11.0 (0.4)	10.6 (2.5)	8.1	4.9 (△2.3)	7.2 (△0.3)	7.5	47.1 (△3.7)	50.8 (△1.2)	52.0	37.2 (5.7)	31.5 (△0.9)	32.4	3,304	4,165	3,944
内部による定期的な情報セキュリティ監査	20.3 (1.5)	18.8 (6.2)	12.6	9.8 (△2.2)	12.0 (△1.5)	13.5	48.9 (△3.0)	51.9 (△2.3)	54.2	21.2 (3.6)	17.6 (△2.2)	19.8	3,322	4,181	3,944

（効果）

単位：%

対策の種類	効果									（参考）回答企業数（社）		
	効果があった			あまり効果がない			よくわからない					
	18年	17年	16年	18年	17年	16年	18年	17年	16年	18年	17年	16年
外部専門家による定期的な情報セキュリティ監査	80.1	76.1	73.9	0.3	4.2	5.1	19.7	19.7	21.0	346	457	257
内部による定期的な情報セキュリティ監査	78.5	77.1	73.7	1.4	5.7	4.0	20.1	17.2	22.2	646	825	445

※　調査対象期間　18 年調査：平成 17 年度　17 年調査：平成 16 年度　16 年調査：平成 15 年度

※　18 年調査については、現在実施中。

※　実施状況中、「既に実施している」には、「トラブルがあったので対策を講じた」を含む（全体に占める割合は括弧内、平成 16 年は未調査。）。
※　効果については、「既に実施している」及び「実施を検討している」と回答した者についてのみ、調査。

○ 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）

＜平成 16 年～17 年＞

利用しない理由		15年	16年	17年
個人情報の保護に不安がある		38.6%	47.4%	44.2%
（内訳）	利用経験有	55.4%	63.3%	56.9%
	利用経験無	13.0%	19.0%	15.1%
ウィルスの感染が心配である		28.6%	34.8%	34.6%
（内訳）	利用経験有	43.1%	49.6%	46.9%
	利用経験無	5.8%	7.7%	6.2%
電子的決済手段の信頼性に不安がある		19.4%	25.5%	26.2%
（内訳）	利用経験有	28.4%	35.3%	34.6%
	利用経験無	5.8%	7.7%	6.9%
違法・有害情報が氾濫している		16.0%	20.8%	20.8%
（内訳）	利用経験有	22.5%	27.7%	26.5%
	利用経験無	6.0%	8.5%	7.7%
通信料金が高い		15.0%	16.9%	17.2%
（内訳）	利用経験有	20.0%	22.3%	21.2%
	利用経験無	7.5%	7.4%	7.9%
パソコンなどの機器の操作が難しい		13.8%	16.6%	16.3%
（内訳）	利用経験有	10.3%	12.4%	14.8%
	利用経験無	21.8%	26.7%	20.8%
パソコンなどの機器が高すぎる		13.7%	18.8%	15.9%
（内訳）	利用経験有	17.0%	22.4%	19.2%
	利用経験無	9.5%	12.7%	8.3%
利用する必要がない		16.1%	15.9%	14.7%
（内訳）	利用経験有	6.4%	3.9%	4.7%
	利用経験無	36.1%	43.7%	41.6%
認証技術の信頼性に不安がある		7.4%	9.6%	10.1%
（内訳）	利用経験有	11.2%	13.6%	13.5%
	利用経験無	1.3%	2.3%	2.3%
接続速度が遅い		9.1%	9.7%	9.8%
（内訳）	利用経験有	14.2%	14.4%	13.6%
	利用経験無	0.8%	1.1%	1.1%
知的財産の保護に不安がある		6.0%	8.9%	8.4%
（内訳）	利用経験有	8.3%	11.5%	10.5%
	利用経験無	2.7%	4.0%	3.7%
情報検索に手間がかかる		7.3%	7.1%	6.8%
（内訳）	利用経験有	10.5%	9.7%	8.8%
	利用経験無	2.2%	2.3%	2.5%
送信した電子メールが届くかどうかわ		2.6%	3.4%	3.1%
（内訳）	利用経験有	3.6%	4.6%	3.9%
	利用経験無	0.6%	1.1%	1.0%
必要な情報がない		2.1%	2.6%	2.8%
（内訳）	利用経験有	1.5%	2.2%	2.3%
	利用経験無	3.7%	4.0%	3.9%
その他		2.7%	2.6%	2.3%
（内訳）	利用経験有	2.1%	1.7%	1.4%
	利用経験無	4.1%	5.0%	4.7%
特に不満は感じていない		7.3%	9.2%	11.5%
（内訳）	利用経験有	7.8%	8.5%	11.6%
	利用経験無	6.7%	11.8%	11.9%
無回答		26.5%	17.8%	18.5%
（内訳）	利用経験有	12.8%	8.6%	9.9%
	利用経験無	42.0%	28.3%	33.6%
（参考）回答数		10,019	11,003	11,394
	利用経験有	6,936	7,704	8,188
	利用経験無	2,304	2,758	2,394

＜平成 18 年＞

インターネット利用で感じる不安の内容

利用しない理由	18年
ウィルスの感染が心配である	66.8%
個人情報の保護に不安がある	66.6%
どこまでセキュリティ対策を行えばよいか不明	57.3%
電子的決済手段の信頼性に不安がある	39.5%
セキュリティ脅威が難解で具体的に理解できない	30.8%
違法・有害情報が氾濫している	28.2%
認証技術の信頼性に不安がある	15.4%
送信した電子メールが届くかどうかわからない	7.4%
知的財産の保護に不安がある	7.0%
その他	1.4%
無回答	0.4%
（参考）回答数	1,651

インターネットを利用して感じる不満、利用しない理由

利用しない理由		18年
特に不満はない		25.0%
（内訳）	利用経験有	25.0%
	利用経験無	29.5%
通信料金が高い		20.4%
（内訳）	利用経験有	22.5%
	利用経験無	15.1%
パソコンなどの機器が高価すぎる		17.8%
（内訳）	利用経験有	18.8%
	利用経験無	15.8%
利用する必要がない		14.0%
（内訳）	利用経験有	6.9%
	利用経験無	49.6%
接続速度が遅い		13.5%
（内訳）	利用経験有	16.8%
	利用経験無	0.9%
パソコンなどの機器の操作が難しい		13.3%
（内訳）	利用経験有	10.8%
	利用経験無	27.8%
インターネットについてよく知らない		11.7%
（内訳）	利用経験有	6.3%
	利用経験無	37.8%
情報検索に手間がかかる		7.0%
（内訳）	利用経験有	8.4%
	利用経験無	1.7%
必要な情報がない		2.6%
（内訳）	利用経験有	2.3%
	利用経験無	4.5%
その他		5.3%
（内訳）	利用経験有	4.9%
	利用経験無	7.7%
無回答		24.9%
（内訳）	利用経験有	25.3%
	利用経験無	12.3%
（参考）回答数		4,999
	利用経験有	3,931
	利用経験無	486

○ 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）

	１８年	１９年
コンピュータウィルス感染	97.7%	95.5%
スパイウェア	84.8%	77.3%
ボット（ボットネット）	26.2%	23.5%
個人情報漏えい	87.6%	83.9%
フィッシング詐欺	83.9%	81.4%
不正アクセス	79.5%	73.2%
どれも知らない	1.3%	2.0%
全回答者数	2,979	3,090

※各年度で調査方法(設問の構成・内容)や調査手法が異なるため、単純な経年比較はできない。

○ 情報セキュリティに関する言葉の認知度（情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構）

＜平成 17 年＞

（男女別）

	ウィルス感染	スパムメール	スパイウェア	フィッシング	セキュリティホール（脆弱性）	ボット	ファーミング	聞いたことがあるものはない	（参考）回答者数
全体	98.7%	82.3%	78.9%	74.6%	50.6%	12.8%	10.4%	0.6%	5,142
男性	98.4%	88.7%	90.1%	82.7%	66.4%	20.2%	14.0%	0.7%	2,496
女性	99.0%	76.2%	68.3%	67.0%	35.7%	5.9%	7.0%	0.5%	2,646

（年代別）

	ソフトメーカーのウェブサイト等	パソコンメーカー等のウェブサイト等	家族や知人	ポータルサイトのトピックス・ニュース等	IT関連のウェブサイト等	テレビ・新聞等	雑誌や専門書	セキュリティ関連の組織のウェブサイト等	セミナーや研究会	その他	入手していない
全体	46.6	44.8	23.4	20.1	19.5	17.6	10.1	7.0	0.6	0.9	14.9
10代	31.5	27.2	28.0	19.8	16.4	15.1	9.5	6.0	0.4	0.9	28.0
20代	39.1	37.3	25.6	22.0	22.1	16.1	11.4	6.2	0.5	0.8	17.1
30代	48.5	45.3	24.7	21.0	19.6	16.7	9.3	6.9	0.7	0.8	14.1
40代	55.7	53.4	18.1	18.7	19.0	19.5	10.0	8.6	0.5	0.8	11.2
50代以上	45.6	51.6	21.8	14.8	15.4	22.2	10.4	6.8	0.6	1.2	14.0

（職業別）

	ウィルス感染	スパムメール	スパイウェア	フィッシング	セキュリティホール（脆弱性）	ボット	ファーミング	聞いたことがあるものはない	（参考）回答者数
全体	98.7%	82.3%	78.9%	74.6%	50.6%	12.8%	10.4%	0.6%	5,142
経営者・役員	97.1%	83.7%	89.4%	77.9%	53.8%	15.4%	15.4%	0.0%	104
会社員等（情報システム関係の技術	98.4%	91.4%	89.3%	84.8%	77.6%	31.0%	21.2%	0.9%	429
会社員・公務員・派遣社員（その	98.8%	86.1%	85.3%	79.9%	58.2%	12.2%	10.3%	0.6%	1,989
自営業・自由業	98.7%	85.9%	86.4%	78.8%	54.2%	13.2%	10.5%	0.4%	448
専業主婦／家事手伝い・無	98.7%	72.0%	66.8%	66.3%	31.4%	4.9%	6.1%	0.7%	1,017
パート・アルバイ	99.3%	76.8%	69.0%	69.3%	37.1%	7.5%	7.5%	0.3%	587
学生	98.0%	83.7%	72.6%	64.9%	49.4%	21.3%	12.0%	0.9%	541

＜平成 18 年＞

（男女別）

	コンピュータ・ウィルス	セキュリティホール	フィッシング	スパイウェア	ボット	ファーミング	ワンクリック不正請求	セキュリティ対策ソフトの押し売り行為	ルートキット	脆弱性	どれも知らない	（参考）回答者数
全体	97.8%	63.6%	75.5%	82.7%	15.0%	10.3%	76.1%	27.2%	7.9%	49.8%	1.4%	5,316
男性	98.3%	74.0%	84.5%	91.0%	21.7%	12.2%	83.8%	33.6%	11.7%	67.5%	0.8%	2,770
女性	97.1%	52.4%	65.7%	73.6%	7.6%	8.1%	67.6%	20.3%	3.7%	30.5%	2.0%	2,546

（年代別）

	コンピュータ・ウィルス	セキュリティホール	フィッシング	スパイウェア	ボット	ファーミング	ワンクリック不正請求	セキュリティ対策ソフトの押し売り行為	ルートキット	脆弱性	どれも知らない	（参考）回答者数
全体	97.8%	63.6%	75.5%	82.7%	15.0%	10.3%	76.1%	27.2%	7.9%	49.8%	1.4%	5,316
10代	96.1%	63.0%	67.8%	76.9%	19.8%	14.5%	80.0%	37.2%	12.1%	43.3%	2.8%	656
20代	97.8%	66.2%	75.2%	83.6%	21.2%	12.1%	78.4%	29.7%	12.1%	52.8%	1.2%	1,062
30代	98.0%	67.2%	79.8%	86.5%	16.4%	9.4%	79.9%	27.1%	8.3%	54.3%	1.0%	1,123
40代	99.1%	68.0%	79.0%	86.2%	14.2%	10.9%	77.3%	26.2%	7.3%	53.7%	0.6%	1,067
50代	97.6%	59.0%	75.0%	80.9%	8.8%	8.2%	70.6%	21.3%	3.3%	46.6%	1.5%	834
60代	96.9%	51.4%	70.9%	75.9%	5.8%	5.4%	65.3%	22.1%	2.1%	40.2%	2.1%	574

（職業別）

	コンピュータ・ウィルス	セキュリティホール	フィッシング	スパイウェア	ボット	ファーミング	ワンクリック不正請求	セキュリティ対策ソフトの押し売り行為	ルートキット	脆弱性	どれも知らない
全体	97.8%	63.6%	75.5%	82.7%	15.0%	10.3%	76.1%	27.2%	7.9%	49.8%	1.4%
経営者・役員	98.9%	69.6%	85.5%	91.7%	16.3%	13.0%	83.6%	37.1%	6.7%	63.3%	0.4%
会社員等（情報システム関係の技術	98.5%	91.3%	93.4%	95.7%	42.6%	23.4%	89.5%	50.4%	26.8%	87.9%	1.0%
会社員・公務員・派遣社員（その	98.2%	70.9%	81.1%	88.3%	16.0%	11.4%	79.7%	25.4%	8.4%	60.8%	0.8%
専門職・自営業・自由業	98.4%	67.6%	79.4%	87.2%	15.3%	10.1%	79.2%	29.9%	6.9%	56.9%	1.1%
専業主婦／家事手伝い・無	97.8%	51.0%	68.9%	75.0%	7.0%	5.2%	66.3%	20.0%	2.6%	32.1%	1.7%
パート・アルバイ	97.0%	53.0%	66.9%	73.8%	9.2%	7.4%	67.2%	22.5%	4.1%	29.8%	2.0%
学生	96.7%	64.0%	70.3%	79.1%	21.7%	14.0%	80.9%	35.9%	13.2%	48.6%	2.4%
その他	97.5%	58.5%	75.3%	86.3%	10.5%	6.9%	78.7%	26.0%	5.2%	49.9%	0.5%

＜平成 19 年＞

（男女別）

	コンピュータ・ウィルス	セキュリティホール	スパムメール	フィッシング	スパイウェア	ボット	ファーミング	ワンクリック不正請求	セキュリティ対策ソフトの押し売り行為	脆弱性	（参考）回答者数
全体	97.8%	79.4%	86.5%	87.9%	88.7%	35.5%	30.8%	89.3%	50.5%	65.1%	5,316
男性	97.9%	87.1%	91.2%	93.1%	94.4%	45.1%	36.0%	93.6%	57.4%	80.4%	2,770
女性	97.7%	70.9%	81.3%	82.2%	82.4%	25.1%	25.2%	84.6%	43.0%	48.4%	2,546

（年代別）

	コンピュータ・ウィルス	セキュリティホール	スパムメール	フィッシング	スパイウェア	ボット	ファーミング	ワンクリック不正請求	セキュリティ対策ソフトの押し売り行為	脆弱性	（参考）回答者数
全体	97.8%	79.4%	86.5%	87.9%	88.7%	35.5%	30.8%	89.3%	50.5%	65.1%	5,316
10代	95.9%	77.2%	86.8%	83.0%	85.7%	38.8%	32.0%	90.0%	56.1%	56.2%	656
20代	98.0%	79.8%	91.5%	87.7%	89.2%	39.7%	32.9%	91.7%	50.9%	68.0%	1,062
30代	97.7%	80.5%	89.8%	89.1%	88.6%	36.6%	33.3%	90.2%	50.7%	67.5%	1,123
40代	98.4%	82.1%	88.9%	91.5%	93.2%	36.0%	30.3%	90.3%	47.9%	69.5%	1,067
50代	98.4%	77.3%	81.3%	88.7%	87.9%	29.1%	28.2%	87.3%	49.2%	64.2%	834
60代	97.8%	76.9%	73.5%	83.9%	83.9%	30.2%	25.7%	82.8%	49.5%	58.5%	574

（職業別）

	コンピュータ・ウィルス	セキュリティホール	スパムメール	フィッシング	スパイウェア	ボット	ファーミング	ワンクリック不正請求	セキュリティ対策ソフトの押し売り行為	脆弱性	（参考）回答者数
全体	97.8%	63.6%	86.5%	75.5%	82.7%	15.0%	10.3%	76.1%	27.2%	49.8%	5316
経営者・役員	98.4%	82.5%	88.7%	92.1%	93.3%	44.2%	39.1%	92.4%	53.1%	75.9%	154
会社員・公務員・教員（管	98.0%	89.6%	90.7%	94.3%	95.5%	40.2%	34.7%	89.1%	70.3%	81.3%	392
会社員・公務員・教員（情報システムおよび通信関係の技術	97.6%	96.7%	96.2%	96.2%	97.6%	68.6%	56.2%	95.5%	53.1%	92.3%	230
会社員・公務員・教員（情報システムおよび通信関係の技術	97.8%	86.1%	91.6%	91.9%	92.4%	39.5%	33.7%	93.9%	63.5%	78.6%	1089
医者・弁護士、専	98.7%	81.5%	89.2%	81.3%	83.4%	42.3%	40.5%	84.9%	54.8%	72.5%	96
契約社員／派遣社	97.8%	76.7%	87.6%	87.9%	88.3%	34.7%	35.8%	89.3%	54.8%	67.9%	227
自営業・自由業	98.5%	82.6%	88.2%	91.3%	94.1%	35.7%	31.1%	92.5%	36.8%	72.7%	436
専業主婦	98.7%	65.0%	77.2%	82.1%	80.2%	20.1%	19.9%	83.2%	44.5%	38.9%	942
家事手伝い・無職	97.1%	78.4%	80.8%	84.3%	88.1%	37.2%	27.7%	87.0%	44.3%	64.6%	222
パート・アルバイ	97.3%	74.5%	82.5%	85.1%	85.1%	30.1%	26.4%	85.0%	54.3%	55.1%	560
高校生	95.0%	75.7%	84.1%	83.1%	86.4%	37.0%	30.6%	88.2%	56.1%	52.5%	342
大学生・大学院生	97.9%	80.0%	92.8%	85.6%	87.8%	38.5%	31.9%	92.0%	51.1%	66.1%	443
その他	98.0%	83.2%	81.9%	89.2%	88.1%	33.0%	26.1%	88.6%	51.0%	69.3%	183

○ 情報セキュリティ対策に関する意識（情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構）

＜平成 17 年＞

（男女別）

	費用がかかる	手間がかかる	対策を講じるとパソコンの利便性が損なわれる	対策方法がわからない	関連情報の収集・勉強が面倒	何が危険なのかわからない	対策の必要性を感じない	その他	特にない	（参考）回答者数
全体	59.2%	40.8%	24.3%	17.3%	15.6%	6.2%	2.5%	2.5%	14.4%	5,142
男性	63.7%	42.3%	28.6%	8.1%	12.7%	4.2%	2.6%	2.6%	14.0%	2,496
女性	54.8%	39.4%	20.2%	26.1%	18.3%	8.2%	2.5%	2.3%	14.8%	2,646

（年代別）

	費用がかかる	手間がかかる	対策を講じるとパソコンの利便性が損なわれる	対策方法がわからない	関連情報の収集・勉強が面倒	何が危険なのかわからない	対策の必要性を感じない	その他	特にない	（参考）回答者数
全体	59.2%	40.8%	24.3%	17.3%	15.6%	6.2%	2.5%	2.5%	14.4%	5,142
10代	48.7%	44.4%	20.3%	17.2%	12.5%	4.7%	4.3%	2.6%	24.6%	232
20代	61.7%	46.6%	23.2%	23.3%	19.1%	7.3%	2.7%	1.7%	10.6%	1,315
30代	61.4%	40.3%	25.1%	17.4%	16.5%	5.2%	1.6%	2.7%	13.7%	2,005
40代	58.8%	37.4%	25.1%	11.5%	12.4%	5.8%	2.8%	2.8%	15.3%	1,090
50代以上	49.2%	33.4%	23.6%	14.4%	10.8%	9.2%	4.2%	2.8%	20.6%	500

（職業別）

	費用がかかる	手間がかかる	対策を講じるとパソコンの利便性が損なわれる	対策方法がわからない	関連情報の収集・勉強が面倒	何が危険なのかわからない	対策の必要性を感じない	その他	特にない	（参考）回答者数
全体	59.2%	40.8%	24.3%	17.3%	15.6%	6.2%	2.5%	2.5%	14.4%	5,142
経営者・役員	58.7%	26.0%	26.0%	10.6%	12.5%	5.8%	7.7%	0.0%	22.1%	104
会社員等（情報システム関係の技術者）	64.6%	47.6%	29.6%	6.1%	13.8%	3.0%	1.4%	3.5%	12.8%	429
会社員・公務員・派遣社員（その他）	62.6%	41.6%	25.8%	14.6%	15.3%	4.3%	2.4%	2.6%	13.0%	1,989
自営業・自由業	60.5%	40.0%	29.9%	11.2%	11.6%	8.3%	2.7%	3.1%	15.0%	448
専業主婦／家事手伝い・無職	53.0%	35.2%	19.0%	25.5%	17.4%	8.8%	2.3%	2.1%	16.1%	1,017
パート・アルバイト	56.9%	40.0%	21.8%	23.9%	16.7%	8.3%	2.4%	2.0%	14.7%	587
学生	56.0%	48.8%	22.7%	20.0%	16.5%	7.2%	3.7%	2.6%	15.7%	541

＜平成 18 年＞

（男女別）

	費用がかかる	手間がかかる	対策方法がわからない	説明や用語などがわかりにくい	対策を講じるとパソコンの利便性が損なわれる	関連情報の収集や勉強が面倒	対策の必要性を感じない	何が危険なのかわからない	その他	特にない	（参考）回答者数
全体	62.0%	39.9%	17.8%	33.1%	25.2%	17.4%	1.8%	5.2%	3.6%	12.6%	5,287
男性	67.1%	40.2%	10.6%	23.8%	29.1%	14.6%	1.9%	3.4%	3.9%	13.0%	2,758
女性	56.4%	39.5%	25.8%	43.1%	20.9%	20.6%	1.8%	7.2%	3.4%	12.3%	2,529

（年代別）

	費用がかかる	手間がかかる	対策方法がわからない	説明や用語などがわかりにくい	対策を講じるとパソコンの利便性が損なわれる	関連情報の収集や勉強が面倒	対策の必要性を感じない	何が危険なのかわからない	その他	特にない	（参考）回答者数
全体	62.0%	39.9%	17.8%	33.1%	25.2%	17.4%	1.8%	5.2%	3.6%	12.6%	5,287
10代	55.0%	44.9%	22.7%	34.0%	18.3%	18.9%	3.4%	5.6%	3.4%	17.8%	650
20代	64.2%	45.3%	21.3%	37.2%	25.4%	20.1%	2.3%	5.9%	3.7%	8.6%	1,057
30代	66.6%	41.7%	17.7%	36.7%	27.7%	19.7%	1.5%	4.5%	3.8%	8.4%	1,120
40代	63.4%	38.2%	16.1%	29.5%	28.2%	15.2%	0.7%	4.2%	4.3%	13.1%	1,058
50代	59.7%	32.6%	13.6%	27.5%	24.5%	12.8%	2.1%	5.0%	3.6%	16.0%	832
60代	57.5%	34.4%	15.6%	31.9%	23.0%	17.4%	1.9%	7.3%	2.2%	17.1%	570

＜平成 19 年＞

（全体）

	情報セキュリティに関する被害というと、具体的にどのようなことが起こるかイメージがわかない				自分が被害を受ける確率は低いと思っている				たとえ被害を受けても、特に困るようなことにはならないと思う				自分が被害を受けてもほかの人に迷惑が及ぶことはないと思う				（参考）回答者数
	そう思う	ややそう思う	あまりそう思わない	そう思わない	そう思う	ややそう思う	あまりそう思わない	そう思わない	そう思う	ややそう思う	あまりそう思わない	そう思わない	そう思う	ややそう思う	あまりそう思わない	そう思わない	
全体	7.7%	31.2%	32.3%	28.8%	6.3%	33.0%	36.6%	24.1%	2.9%	15.0%	36.5%	45.6%	3.2%	15.8%	34.6%	46.5%	5,160

（年代別）情報セキュリティに関する被害というと、具体的にどのようなことが起こるかイメージがわかない

	情報セキュリティに関する被害というと、具体的にどのようなことが起こるかイメージがわかない				（参考）回答者数
	そう思う	ややそう思う	あまりそう思わない	そう思わない	
全体	7.7%	31.2%	32.3%	28.8%	5,160
15～19歳	10.8%	35.9%	31.6%	21.7%	425
20～29歳	10.2%	32.6%	32.6%	24.6%	1,031
30～39歳	4.9%	30.9%	35.7%	28.5%	1,224
40～49歳	4.3%	27.8%	35.8%	32.1%	915
50～59歳	8.3%	28.8%	30.5%	32.4%	885
60歳以上	10.9%	34.4%	24.0%	30.7%	682

（男女別）情報収集に関する不満

	知らない用語が多い	情報が複雑すぎる	内容が難しい	情報が多すぎる	自分から情報収集や勉強するのが面倒	情報の更新が早すぎて追いつけない	セキュリティ対策ソフトを利用していれば十分である	情報の在り処が分からない	その他	特に問題は感じていない	（参考）回答者数
全体	46.6%	42.3%	40.0%	34.2%	29.3%	26.9%	16.7%	16.3%	0.7%	13.7%	5,160
男性	36.2%	38.2%	32.2%	32.2%	24.3%	24.6%	19.1%	12.8%	1.0%	18.1%	2,734
女性	58.3%	46.9%	48.8%	36.5%	34.9%	29.4%	14.0%	20.3%	0.4%	8.7%	2,427

（年代別）情報収集に関する不満

	知らない用語が多い	情報が複雑すぎる	内容が難しい	情報が多すぎる	自分から情報収集や勉強するのが面倒	情報の更新が早すぎて追いつけない	セキュリティ対策ソフトを利用していれば十分	情報の在り処が分からない	その他	特に問題は感じていない	（参考）回答者数
全体	46.6%	42.3%	40.0%	34.2%	29.3%	26.9%	16.7%	16.3%	0.7%	13.7%	5,160
15～19歳	42.0%	38.7%	40.8%	34.4%	25.6%	19.4%	14.2%	18.7%	0.7%	20.0%	425
20～29歳	48.2%	44.9%	44.4%	40.6%	34.1%	29.1%	12.9%	20.4%	0.6%	11.1%	1,031
30～39歳	49.2%	43.0%	41.2%	36.2%	32.3%	29.5%	15.3%	15.5%	0.7%	12.4%	1,224
40～49歳	44.6%	42.3%	36.7%	33.0%	28.2%	27.7%	14.4%	13.2%	0.4%	14.4%	915
50～59歳	43.7%	39.7%	35.4%	27.9%	25.8%	24.4%	19.3%	15.2%	1.0%	17.0%	885
60歳以上	48.5%	42.9%	41.2%	30.6%	25.0%	25.2%	26.3%	15.8%	1.0%	10.9%	682

（男女別）情報セキュリティ対策に対する意識

	Microsoft Update等によるセキュリティﾊﾟｯﾁの更新				セキュリティ対策ソフトの導入・活用				パスワードの定期的な変更				パスワードを誕生日など推測されやすいものを避けて設定				（参考）回答者数
	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	
全体	58.3%	28.5%	1.7%	11.4%	63.9%	28.2%	1.8%	6.1%	26.8%	56.1%	8.8%	8.4%	60.4%	31.5%	3.4%	4.7%	5,160
男性	68.4%	24.4%	2.2%	5.0%	68.5%	26.7%	2.0%	2.8%	26.8%	57.7%	9.7%	5.8%	60.0%	32.7%	4.2%	3.0%	2,773
女性	47.0%	33.1%	1.2%	18.6%	58.8%	29.8%	1.5%	9.9%	26.8%	54.2%	7.7%	11.3%	60.8%	30.0%	2.5%	6.6%	2,427

	怪しいメール・添付ファイルの削除				電子メールの暗号化ソフト等の利用				怪しいと思われるウェブサイトにはアクセスしない				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				（参考）回答者数
	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	
全体	76.5%	18.3%	1.7%	3.5%	28.7%	49.1%	9.5%	12.7%	65.6%	28.7%	2.1%	3.5%	67.9%	26.2%	1.9%	3.9%	5,160
男性	75.7%	20.1%	2.3%	1.9%	28.0%	53.2%	11.7%	7.1%	56.1%	37.9%	3.4%	2.6%	62.7%	32.1%	2.7%	2.5%	2,773
女性	77.4%	16.2%	1.1%	5.2%	29.5%	44.4%	7.0%	19.1%	76.4%	18.4%	0.6%	4.6%	73.8%	19.6%	1.0%	5.6%	2,427

	パソコンの重要なデータのアックアップ				不要になった自宅パソコンの廃棄・リサイクル前のデータ消去				（参考）回答者数
	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	
全体	63.1%	28.9%	2.7%	5.4%	69.8%	21.7%	3.2%	5.4%	5,160
男性	64.5%	29.3%	3.4%	2.8%	68.2%	23.6%	4.1%	4.0%	2,773
女性	61.5%	28.4%	1.9%	8.2%	71.6%	19.5%	2.1%	6.9%	2,427

（年代別）情報セキュリティ対策に対する意識

	Microsoft Update等によるセキュリティパッチの更新				セキュリティ対策ソフトの導入・活用				パスワードの定期的な変更				パスワードを誕生日など推測されやすいものを避けて設定				（参考）回答者数
	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	
全体	58.3%	28.5%	1.7%	11.4%	63.9%	28.2%	1.8%	6.1%	26.8%	56.1%	8.8%	8.4%	60.4%	31.5%	3.4%	4.7%	5,160
15～19歳	45.6%	34.6%	4.4%	15.3%	54.8%	33.4%	2.2%	9.6%	18.6%	47.1%	23.3%	11.0%	51.7%	32.9%	8.6%	6.7%	424
20～29歳	55.0%	30.2%	1.8%	13.0%	60.4%	31.3%	1.7%	6.6%	25.2%	52.9%	12.2%	9.7%	57.8%	32.4%	4.3%	5.6%	1,031
30～39歳	60.6%	28.3%	1.6%	9.4%	66.9%	27.5%	1.5%	4.1%	28.2%	59.1%	6.9%	5.8%	61.0%	32.3%	3.3%	3.5%	1,224
40～49歳	63.2%	27.6%	1.2%	8.0%	69.8%	24.6%	1.5%	4.1%	27.1%	60.6%	5.9%	6.4%	60.9%	34.3%	1.7%	3.1%	914
50～59歳	59.3%	26.8%	1.6%	12.3%	62.9%	28.5%	2.0%	6.5%	29.0%	56.5%	5.4%	9.1%	63.4%	28.7%	2.4%	5.5%	885
60歳以上	59.5%	25.9%	1.1%	13.5%	63.0%	25.8%	2.1%	9.1%	28.6%	54.3%	6.2%	10.9%	64.1%	27.5%	2.8%	5.6%	682

	怪しいメール・添付ファイルの削除				電子メールの暗号化ソフト等の利用				怪しいと思われるウェブサイトにはアクセスしない				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				（参考）回答者数
	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	
全体	76.5%	18.3%	1.7%	3.5%	28.7%	49.1%	9.5%	12.7%	65.6%	28.7%	2.1%	3.5%	67.9%	26.2%	1.9%	3.9%	5,160
15～19歳	62.5%	26.1%	4.8%	6.6%	21.2%	45.5%	19.1%	14.3%	48.6%	40.0%	5.5%	5.9%	47.3%	39.6%	5.4%	7.8%	424
20～29歳	69.4%	23.3%	2.7%	4.6%	24.9%	49.6%	11.4%	14.2%	56.0%	36.1%	2.9%	4.9%	57.9%	33.9%	2.5%	5.8%	1,031
30～39歳	77.8%	18.7%	1.4%	2.1%	28.7%	51.3%	9.1%	10.8%	66.9%	28.3%	2.2%	2.5%	67.2%	28.1%	1.8%	2.9%	1,224
40～49歳	81.6%	15.7%	0.7%	2.0%	31.5%	52.4%	7.5%	8.6%	68.0%	28.6%	1.2%	2.2%	74.3%	22.8%	1.0%	1.8%	914
50～59歳	80.2%	14.7%	1.6%	3.4%	31.9%	46.8%	7.2%	14.1%	71.8%	23.6%	1.0%	3.6%	74.9%	20.1%	1.5%	3.4%	885
60歳以上	82.1%	13.2%	0.4%	4.3%	31.5%	44.7%	7.0%	16.8%	77.5%	18.1%	0.9%	3.6%	79.3%	15.6%	1.0%	4.1%	682

	パソコンの重要なデータのアックアップ				不要になった自宅パソコンの廃棄・リサイクル前のデータ消去				（参考）回答者数
	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	必ず必要	インターネットの使い方によっては必要	やらなくても良い／不要	どの程度必要かわからない	
全体	63.1%	28.9%	2.7%	5.4%	69.8%	21.7%	3.2%	5.4%	5,160
15～19歳	44.3%	38.6%	6.4%	10.7%	51.0%	29.5%	7.0%	12.4%	424
20～29歳	57.0%	33.5%	3.3%	6.2%	61.2%	27.4%	4.2%	7.2%	1,031
30～39歳	65.7%	27.4%	2.9%	3.9%	70.9%	21.8%	3.0%	4.3%	1,224
40～49歳	68.1%	27.5%	1.6%	2.8%	74.9%	20.5%	1.9%	2.8%	914
50～59歳	66.9%	26.0%	1.5%	5.6%	74.9%	18.6%	2.5%	4.0%	885
60歳以上	67.8%	23.7%	2.0%	6.4%	79.2%	13.5%	2.1%	5.3%	682

○ 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）

	15年	16年	17年	18年
ウィルスチェックソフトの導入	32.0%	35.9%	36.7%	46.4%
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		34.3%	30.2%	35.6%
プロバイダ等が提供するウィルスチェックサービスの利用	18.4%	19.8%	17.3%	21.2%
OS、ブラウザのアップデート	17.8%	19.4%	17.1%	21.0%
ファイアウォールの使用	8.9%	12.3%	14.4%	21.6%
ファイル等のバックアップ	13.4%	8.1%	8.3%	11.6%
スパイウェア対策ソフトの導入			8.0%	14.8%
メールソフトのアップデートや変更	3.8%	5.6%	6.1%	6.4%
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				4.5%
パスワードの定期的な変更		2.1%	2.7%	3.5%
アカウント毎にパスワードを複数使い分け		1.7%	2.3%	4.0%
その他	2.4%	1.6%	1.4%	1.2%
何も行っていない	26.5%	14.6%	22.1%	10.6%
無回答	22.4%	25.8%	20.9%	21.0%
（参考）回答数	6,936	8,776	9,174	3,931

※　15 年末の調査は 15 歳以上を対象、各年で選択肢に若干の相違がある。

○ 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）

	１８年	１９年
MACアドレスフィルタリングをしている	13.7%	14.5%
ＳＳＩＤ隠蔽機能(ステルスモード）の使用	10.3%	11.2%
暗号化（ＷＥＰ）	18.5%	23.1%
暗号化（ＷＰＡ／ＰＳＫ）	6.0%	7.5%
暗号化（ＷＰＡ２（ＩＥＥＥ８０２．１１ｉ）	4.5%	5.9%
その他	1.1%	1.2%
方法はわからないが対策している（初期設定等）	-	19.1%
対策をしていない	41.5%	19.2%
わからない	27.5%	25.8%
全回答者数	2,661	1,459

※各年度で調査方法(設問の構成・内容)や調査手法が異なるため、単純な経年比較はできない。

○ 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新たな脅威に対する意識調査：情報処理推進機構）

＜平成 17 年＞

（全体）

全体（回答：5,142）	パッチの適用	セキュリティ対策ソフトの導入	パスワードの定期的な変更	怪しい電子メール・添付ファイルの削除	セキュリティ関連情報の収集
実施	77.3%	79.7%	42.6%	88.6%	69.5%
今後実施予定	1.1%	2.8%	8.9%	1.0%	3.8%
未実施	10.8%	11.5%	42.3%	5.0%	19.4%
わからない	10.8%	6.0%	6.2%	5.3%	7.3%

（年代別）

年代別（回答数）		10代（232）	20代（1,315）	30代（2,005）	40代（1,090）	50代以上（500）
パッチの適用	実施	63.4%	75.6%	79.3%	80.5%	72.2%
	今後実施予定	1.3%	1.1%	1.1%	1.0%	1.4%
	未実施	11.6%	10.4%	9.7%	11.4%	15.8%
	わからない	23.7%	12.8%	9.9%	7.1%	10.6%
セキュリティ対策ソフトの導入	実施	68.1%	77.1%	81.5%	82.0%	80.0%
	今後実施予定	1.7%	3.2%	2.9%	2.8%	1.6%
	未実施	11.6%	12.6%	10.3%	11.7%	12.8%
	わからない	18.5%	7.1%	5.4%	3.5%	5.6%
パスワードの定期的な変更	実施	30.2%	40.7%	44.7%	45.6%	38.4%
	今後実施予定	5.6%	8.8%	9.2%	9.4%	8.0%
	未実施	43.5%	44.1%	40.1%	41.5%	47.8%
	わからない	20.7%	6.3%	5.9%	3.6%	5.8%
怪しい電子メール・添付ファイルの削除	実施	78.5%	87.4%	90.2%	91.6%	84.4%
	今後実施予定	0.0%	1.3%	0.5%	1.0%	2.2%
	未実施	4.3%	5.8%	4.2%	4.8%	7.2%
	わからない	17.2%	5.6%	5.1%	2.6%	6.2%
セキュリティ関連情報の収集	実施	54.3%	64.7%	71.6%	75.3%	68.2%
	今後実施予定	3.9%	4.6%	3.2%	3.5%	4.6%
	未実施	20.7%	22.1%	18.9%	16.7%	19.8%
	わからない	21.1%	8.6%	6.3%	4.5%	7.4%

※　いずれの表についても、「実施」には自分自身で実施したもの、家族や知人が実施したもの、プロバイダ提供のセキュリティサービスを利用したものが全て含まれる。

（職業別）

職業別（回答数）		経営者・役員（104）	会社員など（情報システム関係の技術者）（429）	会社員・公務員・派遣社員（その他）（1,989）	自営業・自由業（448）	専業主婦/家事手伝い・無職（1,017）	パート・アルバイト（587）	学生（541）
パッチの適用	実施	77.3%	88.6%	81.9%	82.8%	68.4%	68.8%	71.5%
	今後実施予定	1.1%	0.7%	0.8%	0.9%	1.4%	1.9%	1.8%
	未実施	10.8%	7.5%	11.4%	10.3%	11.2%	12.9%	9.6%
	わからない	10.8%	3.3%	5.9%	6.0%	19.1%	16.4%	17.0%
セキュリティ対策ソフトの導入	実施	89.5%	88.2%	82.4%	84.2%	74.7%	73.2%	73.9%
	今後実施予定	1.0%	1.9%	2.7%	2.2%	3.2%	2.9%	3.5%
	未実施	6.7%	8.6%	11.7%	10.5%	11.9%	15.3%	10.4%
	わからない	2.9%	1.4%	3.2%	3.1%	10.1%	8.7%	12.2%
パスワードの定期的な変更	実施	58.6%	56.9%	45.1%	46.9%	37.7%	36.0%	33.1%
	今後実施予定	5.8%	4.4%	9.2%	10.0%	9.6%	9.4%	8.9%
	未実施	30.8%	36.6%	42.5%	39.7%	41.6%	47.5%	45.7%
	わからない	4.8%	2.1%	3.2%	3.3%	11.1%	7.2%	12.4%
怪しい電子メール・添付ファイルの削除	実施	94.2%	95.4%	91.4%	93.3%	83.4%	83.9%	83.5%
	今後実施予定	1.9%	0.7%	0.6%	0.2%	1.3%	1.3%	0.9%
	未実施	0.0%	2.3%	5.5%	3.1%	5.9%	7.0%	4.6%
	わからない	3.8%	1.6%	2.5%	3.3%	9.3%	7.0%	10.9%
セキュリティ関連情報の収集	実施	85.6%	82.5%	72.5%	78.1%	61.4%	64.7%	60.1%
	今後実施予定	1.9%	2.3%	3.6%	3.6%	4.3%	5.1%	4.1%
	未実施	9.6%	12.8%	20.1%	13.6%	20.9%	24.0%	20.7%
	わからない	2.9%	2.3%	3.8%	3.8%	13.4%	8.2%	15.2%

※　いずれの表についても、「実施」には自分自身で実施したもの、家族や知人が実施したもの、プロバイダ提供のセキュリティサービスを利用したものが全て含まれる。

＜平成 18 年＞

（全体）

全体（回答：5,287）	Windows Update等によるセキュリティパッチの	セキュリティ対策ソフトの導入	パスワードの定期的な変更	怪しい電子メール・添付ファイルの削除※	電子メールの暗号化・電子署名の利用	パソコンの重要データのバックアップ	不要になったパソコンの廃棄リサイクル	セキュリティ関連情報の収集
実施	76.9%	83.7%	38.6%	93.2%	30.7%	59.0%	39.4%	
今後実施予定	1.2%	1.8%	8.5%	1.0%				5.8%
未実施	8.7%	11.7%	45.7%	6.0%	46.7%	25.4%	41.2%	25.1%
わからない	15.4%	6.5%	8.0%	5.5%	18.8%	9.0%	11.0%	9.5%

※『プロバイダ提供のセキュリティサービスを利用』を含む

（男女別）

年代別（回答数）		男性（2,758）	女性（2,529）
パッチの適用	実施	84.1%	69.0%
	今後実施予定	1.0%	1.5%
	未実施	7.2%	10.4%
	わからない	9.3%	22.2%
セキュリティ対策ソフトの導入	実施	87.9%	79.2%
	今後実施予定	1.6%	2.0%
	未実施	10.5%	13.0%
	わからない	2.9%	10.4%
パスワードの定期的な変更	実施	42.6%	34.2%
	今後実施予定	9.0%	8.0%
	未実施	43.9%	47.7%
	わからない	5.2%	11.1%
怪しい電子メール・添付ファイルの削除	実施	93.8%	92.6%
	今後実施予定	0.9%	1.0%
	未実施	6.2%	5.8%
	わからない	3.2%	8.0%
電子メールの暗号化・電子署名の利用	実施	33.9%	27.2%
	今後実施予定		
	未実施	47.5%	45.9%
	わからない	13.2%	24.9%
パソコンの重要データのバックアップ	実施	65.2%	52.3%
	今後実施予定		
	未実施	22.3%	28.8%
	わからない	5.2%	13.1%
不要になった自宅パソコンの廃棄・リサイクル	実施	45.1%	33.2%
	今後実施予定		
	未実施	38.7%	43.8%
	わからない	7.2%	15.2%
セキュリティ関連情報の収集	実施		
	今後実施予定	5.6%	6.1%
	未実施	21.9%	28.7%
	わからない	5.5%	14.0%

（年代別）

年代別（回答数）		10代（650）	20代（1,057）	30代（1,120）	40代（1,058）	50代（832）	60代（570）
Windows Update等によるセキュリティパッチの更新	実施	65.6%	76.7%	81.2%	83.3%	73.8%	74.0%
	今後実施予定	1.8%	1.4%	1.0%	0.8%	1.2%	1.6%
	未実施	8.1%	9.1%	8.6%	7.2%	11.1%	8.3%
	わからない	28.3%	15.2%	11.7%	10.9%	15.2%	17.1%
セキュリティ対策ソフトの導入	実施	77.2%	80.9%	86.4%	89.5%	83.0%	81.7%
	今後実施予定	2.4%	2.2%	1.9%	1.2%	1.5%	1.4%
	未実施	9.4%	13.4%	10.4%	9.6%	13.9%	14.6%
	わからない	16.4%	6.3%	4.8%	4.2%	5.1%	4.9%
パスワードの定期的な変更	実施	33.6%	35.0%	41.4%	41.8%	37.8%	40.3%
	今後実施予定	5.1%	6.7%	8.6%	9.6%	10.2%	11.2%
	未実施	46.2%	50.9%	44.0%	43.0%	46.6%	42.6%
	わからない	16.4%	7.8%	7.1%	6.6%	6.0%	6.3%
怪しい電子メール・添付ファイルの削除	実施	85.5%	90.4%	98.6%	96.0%	93.2%	91.4%
	今後実施予定	1.5%	0.5%	1.1%	1.2%	0.7%	0.9%
	未実施	9.6%	9.2%	3.7%	4.2%	6.0%	4.1%
	わからない	12.0%	4.8%	4.3%	4.1%	4.4%	6.0%
電子メールの暗号化・電子署名の利用	実施	29.6%	31.3%	34.7%	32.1%	25.5%	28.0%
	今後実施予定	2.8%	3.8%	4.7%	4.5%	6.2%	6.8%
	未実施	40.6%	46.4%	43.9%	48.3%	53.8%	46.8%
	わからない	28.8%	19.0%	18.1%	16.4%	14.8%	18.8%
パソコンの重要データのバックアップ	実施	49.6%	56.7%	63.5%	61.1%	59.8%	60.2%
	今後実施予定	7.9%	8.0%	7.1%	9.8%	9.5%	8.3%
	未実施	25.6%	28.3%	24.7%	24.3%	25.3%	23.9%
	わからない	19.9%	9.2%	7.0%	6.1%	6.7%	8.8%
パソコンの重要データのバックアップ	実施	27.5%	34.2%	42.0%	43.1%	43.6%	44.5%
	今後実施予定	6.3%	7.9%	8.3%	10.2%	9.8%	11.6%
	未実施	42.0%	46.0%	42.1%	40.2%	39.1%	34.2%
	わからない	24.6%	12.5%	8.3%	6.9%	8.3%	10.0%
セキュリティ関連情報の収集	実施	51.8%	58.0%	68.0%	67.3%	64.6%	62.0%
	今後実施予定	4.9%	6.1%	4.4%	5.9%	7.4%	6.8%
	未実施	26.6%	27.5%	24.4%	24.2%	23.7%	24.2%
	わからない	20.7%	10.3%	7.9%	6.2%	7.0%	8.7%

＜平成 19 年＞

（全体）

全体（回答：5,160）	Windows Update等によるセキュリティパッチの更新	セキュリティ対策ソフトの導入・活用	パスワードの定期的な変更	パスワードを誕生日など推測されやすいものを避けて設定	怪しい電子メール・添付ファイルの削除	電子メール暗号化ソフト等の利用	怪しいと思われるウェブサイトにはアクセスしない	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	パソコンの重要データのバックアップ	不要になった自宅パソコンの廃棄・リサイクル前のデータ消去
実施	69.5%	75.6%	25.1%	72.8%	83.6%	29.4%	75.7%	78.4%	48.6%	41.7%
今後実施予定	7.6%	7.4%	26.4%	10.4%	5.9%	17.1%	9.3%	8.6%	25.9%	31.3%
未実施	11.8%	10.8%	44.4%	13.1%	6.5%	41.8%	10.6%	9.0%	19.6%	19.2%
わからない	11.1%	6.2%	4.1%	3.7%	4.0%	11.7%	4.4%	4.0%	5.8%	7.9%

（男女別）

性別（回答数）		男性（2,733）	女性（2,427）
Windows Update等によるセキュリティパッチの更新	実施	80.1%	57.5%
	今後実施予定	6.1%	9.3%
	未実施	9.6%	14.3%
	わからない	4.2%	18.9%
セキュリティ対策ソフトの導入・活用	実施	81.2%	69.4%
	今後実施予定	6.7%	8.1%
	未実施	9.6%	12.1%
	わからない	2.6%	10.4%
パスワードの定期的な変更	実施	28.0%	21.9%
	今後実施予定	27.6%	25.1%
	未実施	42.5%	46.5%
	わからない	1.9%	6.5%
パスワードを誕生日など推測されやすいものを避けて設定	実施	74.4%	71.0%
	今後実施予定	11.3%	9.4%
	未実施	12.5%	13.8%
	わからない	1.8%	5.8%
怪しい電子メール・添付ファイルの削除	実施	84.7%	82.3%
	今後実施予定	6.5%	5.1%
	未実施	6.8%	6.3%
	わからない	2.0%	6.3%
電子メールの暗号化ソフトの利用	実施	31.8%	26.6%
	今後実施予定	18.4%	15.8%
	未実施	44.3%	39.1%
	わからない	5.6%	18.5%
怪しいウェブサイトにアクセスしない	実施	69.2%	82.9%
	今後実施予定	12.4%	5.9%
	未実施	15.3%	5.3%
	わからない	3.1%	5.8%
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	実施	75.4%	81.8%
	今後実施予定	10.7%	6.3%
	未実施	11.4%	6.2%
	わからない	2.6%	5.7%
パソコンの重要データのバックアップ	実施	53.8%	42.9%
	今後実施予定	25.6%	26.3%
	未実施	18.4%	21.1%
	わからない	2.3%	9.8%
不要になった自宅パソコンの廃棄・リサイクル前のデータ消去	実施	44.9%	38.1%
	今後実施予定	31.5%	31.0%
	未実施	19.8%	18.5%
	わからない	3.8%	12.4%

（年代別）

性別（回答数）		15～19歳（424）	20～29歳（1,031）	30～39歳（1,224）	40～49歳（914）	50～59歳（885）	60歳以上（682）
Windows Update等によるセキュリティパッチの更新	実施	56.1%	66.3%	71.3%	75.6%	70.7%	69.6%
	今後実施予定	9.9%	8.0%	9.2%	7.3%	4.7%	6.6%
	未実施	12.4%	12.9%	11.7%	9.2%	12.7%	12.3%
	わからない	21.6%	12.8%	7.8%	7.9%	11.9%	11.5%
セキュリティ対策ソフトの導入・活用	実施	65.4%	73.8%	78.1%	80.4%	75.9%	73.6%
	今後実施予定	8.8%	8.6%	7.1%	7.2%	6.0%	7.1%
	未実施	10.7%	10.3%	10.0%	9.0%	12.7%	12.7%
	わからない	15.1%	7.3%	4.8%	3.4%	5.4%	6.6%
パスワードの定期的な変更	実施	16.0%	22.6%	28.6%	25.6%	26.4%	26.2%
	今後実施予定	16.4%	21.4%	26.7%	29.4%	27.5%	34.2%
	未実施	57.1%	51.0%	41.6%	42.7%	42.9%	35.7%
	わからない	10.4%	5.0%	3.1%	2.4%	3.2%	3.9%
パスワードを誕生日など推測されやすいものを避けて設定	実施	63.7%	69.1%	75.3%	74.9%	75.1%	73.8%
	今後実施予定	7.4%	11.1%	10.1%	10.8%	10.1%	11.9%
	未実施	19.3%	14.8%	12.1%	12.0%	12.1%	11.1%
	わからない	9.5%	5.0%	2.4%	2.3%	2.8%	3.3%
怪しい電子メール・添付ファイルの削除	実施	71.2%	77.0%	86.2%	88.4%	87.1%	85.6%
	今後実施予定	6.5%	7.8%	5.6%	4.6%	5.3%	5.3%
	未実施	12.1%	10.1%	5.7%	4.0%	4.3%	5.3%
	わからない	10.2%	5.1%	2.4%	2.9%	3.3%	3.8%
電子メールの暗号化ソフトの利用	実施	21.9%	28.2%	29.9%	33.9%	30.2%	27.8%
	今後実施予定	10.1%	14.5%	17.7%	16.9%	19.5%	21.8%
	未実施	45.7%	43.9%	43.4%	39.0%	40.4%	39.0%
	わからない	22.3%	13.4%	9.1%	10.2%	9.9%	11.4%
怪しいウェブサイトにアクセスしない	実施	57.3%	68.1%	77.0%	80.1%	81.0%	83.3%
	今後実施予定	9.5%	11.6%	8.7%	8.9%	9.0%	8.1%
	未実施	22.6%	14.7%	11.0%	8.6%	6.2%	4.6%
	わからない	10.6%	5.7%	3.3%	2.4%	3.8%	4.0%
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	実施	57.2%	70.2%	80.1%	83.5%	85.6%	84.6%
	今後実施予定	10.1%	10.9%	8.4%	8.0%	7.2%	7.6%
	未実施	21.9%	13.6%	9.1%	5.8%	4.1%	4.3%
	わからない	10.8%	5.3%	2.4%	2.7%	3.2%	3.6%
パソコンの重要データのバックアップ	実施	34.0%	40.9%	49.2%	54.8%	53.2%	54.5%
	今後実施予定	21.5%	28.0%	29.2%	23.7%	24.3%	24.7%
	未実施	28.5%	24.4%	17.9%	18.4%	18.0%	13.9%
	わからない	16.0%	6.7%	3.8%	3.1%	4.6%	7.0%
不要になった自宅パソコンの廃棄・リサイクル前のデータ消去	実施	23.1%	33.9%	43.5%	45.9%	45.5%	51.3%
	今後実施予定	27.7%	32.1%	32.7%	32.2%	32.0%	27.6%
	未実施	29.0%	23.7%	18.8%	17.0%	16.5%	13.1%
	わからない	20.2%	10.2%	5.1%	4.8%	6.0%	8.0%

○ 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新たな脅威に対する意識調査：情報処理推進機構）

情報セキュリティ上のトラブル経験		17年		18年	
		回答数	比率	回答数	比率
	有	2,418	55.3%	1,232	35.9%
	無	1,952	44.7%	2,197	64.1%

当該トラブルを経験した企業（なお、複数回答）		16年（総回答数2,594社）		17年（総回答数2,409社）		18年（総回答数1,229	
		回答数	比率	回答数	比率	回答数	比率
システムトラブル	システム・トラブル計	1,047	40.4%	957	39.7%	721	58.7%
	システム破壊・サーバ停止	730	28.1%	679	28.2%		
	内部要因によるシステムの停止					542	44.1%
	Dos攻撃	259	10.0%	215	8.9%	69	5.6%
	スパムメールの中継利用等(＊1)					146	11.9%
	ホームページやファイル、データの改ざん	62	2.4%	57	2.4%	23	1.9%
	自然災害による障害（地震、火災等の問	247	9.5%	209	8.7%		
	外部要因（地震、火災等の問題）によるシステムの停止					133	10.8%
不正アクセス	不正アクセス計	398	15.3%	343	14.2%	106	8.6%
	IP・メールアドレス詐称	355	13.7%	280	11.6%	74	6.0%
	リソースの不正使用	40	1.5%	37	1.5%	16	1.3%
	内部者の不正アクセス	62	2.4%	57	2.4%	24	2.0%
コンピュータウイルス	コンピュータウィルス計	2,336	90.1%	2,034	84.4%	775	63.1%
	ウィルスやワーム	2,276	87.7%	1,957	81.2%	748	60.9%
	スパムメールの中継利用等（※1）	400	15.4%	332	13.8%		
	トロイの木馬	507	19.5%	423	17.6%	236	19.2%
重要情報の漏洩	重要情報の漏洩計	48	1.9%	491	20.4%	329	26.8%
	パスワードの盗用	21	0.8%	15	0.6%		
	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洩					41	3.3%
	不正アクセスによる情報漏洩					3	0.2%
	内部者による情報漏洩	34	1.3%	39	1.6%	24	2.0%
	委託先による情報漏洩			29	1.2%	33	2.7%
	ノートパソコン及び携帯記憶媒体等の盗難・紛失			458	19.0%	282	22.9%
その他	その他計	137	5.3%	139	5.8%	63	5.1%
	ホームページ上での誹謗中傷等	128	4.9%	129	5.4%	52	4.2%
	その他	10	0.4%	10	0.4%	11	0.9%

（＊1）　１８年調査よりシステムトラブルへ分類
※　調査対象期間　18 年調査: 平成 17 年度　17 年調査：平成 16 年度　16 年調査：平成 15 年度
※　トラブル経験の有無については、平成 17 年から調査を実施。

○ インターネットを利用して受けた被害（通信利用動向調査：総務省）

	15年（総数：6,482）	16年（総数：8,649）	17年（総数：8,985）	18年（総数：3,633）
何らかの被害を受けた	62.2%	56.9%	40.2%	56.9%
ウィルスを発見又は感染	18.8%	24.5%	18.6%	31.7%
ウィルス発見したが感染なし		15.3%	12.7%	20.4%
ウィルスに１度以上感染		10.1%	6.0%	14.1%
迷惑メールを受信	57.0%	48.8%	31.9%	46.7%
迷惑メールを受信（架空請求を除く）		47.6%	31.1%	45.6%
迷惑メールを受信（架空請求）		7.3%	4.6%	7.8%
不正アクセス	3.4%	1.8%	1.2%	2.5%
スパイウェアなどによる個人情報の漏洩		1.5%	1.1%	2.0%
ウェブ上（電子掲示板等）での誹謗中傷等	0.6%	0.3%	0.2%	0.7%
フィッシング		0.2%	0.3%	0.6%
その他（著作権の侵害等）	2.3%	0.1%	0.1%	0.2%
特に被害はない	24.2%	35.3%	43.1%	25.0%
無回答	13.6%	26.4%	16.7%	18.1%

※パソコン又は携帯電話利用して受けた被害を記載

○ 過去1年間の情報セキュリティに関する被害状況（不正アクセス行為対策等の実態調査：警察庁）

事案内容	15年 （総数：732）	16年 （総数：628）	17年 （総数：606）	１８年 （総数：1024）	１９年 （総数：613 ）
ウイルス等の感染	56.1%	45.5%	32.8%	24.1%	9.3%
ノートPC盗難	12.6%	12.3%	8.3%	8.1%	0.8%
スパイウェアの感染			8.3%	6.8%	2.3%
内部者のネットワーク悪用 （H18年、H19年調査項目は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））	6.0%	4.0%	2.3%	3.5%	1.3%
DoS攻撃	4.4%	4.3%	2.3%	1.7%	1.0%
メールの不正中継	3.7%	2.1%	1.7%	1.0%	0.3%
Webや掲示板上での誹謗中傷 （H18年、H19年調査項目はWebや掲示板上での貴社・団体に対する誹謗中傷）	3.8%	3.2%	1.5%	2.6%	0.7%
踏み台 （H18年、H19年調査項目は踏み台（バックドア設置等））	4.5%	1.1%	1.3%	1.5%	0.7%
ホームページの改竄	1.9%	0.3%	1.3%	1.2%	0.2%
なりすまし	3.8%	4.5%	1.0%	1.3%	0.5%
盗聴 （H18年、H19年調査項目は盗聴（キーロガー含む））	0.1%	0.2%	0.7%	0.3%	0.0%
その他情報機器盗難 （H18年、H19年調査項目はその他情報機器盗難（外部記憶装置等））	1.0%	1.0%	0.5%	1.6%	0.7%
情報漏洩 （H18年、H19年調査項目はファイル共有ソフトによるものを除く）	0.4%	1.4%	0.5%	0.9%	0.3%
ファイル共有ソフトの利用に伴う情報漏洩				2.1%	1.7%
システム破壊・データ改竄	0.8%	0.3%	0.5%	0.2%	0.0%
インターネット上の著作権侵害 （H18年、H19年調査項目は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））	0.3%	0.5%	0.2%	0.2%	0.0%
フィッシング		0.0%	0.0%	0.5%	0.0%
ネットワークを利用した詐欺		0.0%	0.0%	0.2%	0.0%
その他	0.7%	1.0%	1.0%	0.3%	0.7%
参考事項	上記につき被害無し：37.4% 無回答：1.2%	上記につき被害無し：36.9% 無回答：9.6%	- -	上記につき被害無し：56.1% -	上記につき被害無し：67.2% -

○ 不正アクセス行為の発生状況（警察庁）

	15年	16年	17年	18年	19年
認知件数（件）	212	356	592	946	1,818
海外からのアクセス	35	37	53	37	79
国内からのアクセス	158	303	487	855	1,684
アクセス元不明	19	16	52	54	55

○ **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）**

	15年	16年	17年	18年	19年
コンピュータウィルス	17,425	52,151	54,174	44,840	34,334
不正アクセス	407	594	515	331	218
ソフトウェア製品・ウェブサイトの脆弱性情報		（※）172	401	593	572

○ **情報セキュリティ被害経験（個人）（情報セキュリティに関する新たな脅威に対する意識調査：情報処理推進機構）**

＜平成 18 年＞

（全体）

	被害者の回答者全体に占める割合	被害内容別、被害者全体に占める割合（複数回答）							
		ウィルス感染	起動異常・システム不調	大量メール送信	不正アクセス	個人情報の流出	ワンクリック詐欺	データの消失・改竄	その他
全体（回答数：5,142）	37.2%(1,915)	77.1%	34.6%	13.0%	11.6%	10.0%	8.3%	2.9%	2.9%
男性（2,496）	41.6%(1,038)	77.7%	36.0%	11.5%	13.0%	8.4%	11.8%	3.5%	2.7%
女性（2,646）	33.1%（877）	76.4%	32.8%	14.7%	9.9%	12.0%	4.0%	2.3%	3.2%

（年代別）

	被害者の回答者全体に占める割合	被害内容別、被害者全体に占める割合（複数回答）							
		ウィルス感染	起動異常・システム不調	大量メール送信	不正アクセス	個人情報の流出	ワンクリック詐欺	データの消失・改竄	その他
全体（回答数：5,142）	37.2%(1,915)	77.1%	34.6%	13.0%	11.6%	10.0%	8.3%	2.9%	2.9%
10代（232）	39.2%(91)	91.2%	40.7%	7.7%	11.0%	6.6%	8.8%	4.4%	0.0%
20代(1,315)	36.3%(477)	79.9%	34.2%	11.3%	11.3%	8.0%	8.2%	2.9%	2.7%
30代(2,005)	36.5%(732)	77.2%	33.1%	14.8%	10.0%	10.5%	7.5%	2.5%	3.3%
40代(1,090)	39.8%(434)	71.4%	36.9%	13.6%	11.1%	11.8%	9.4%	2.8%	2.8%
50代以上(500)	36.2%(181)	76.2%	33.1%	11.0%	20.4%	11.0%	8.3%	4.4%	3.9%

（職業別）

	被害者の回答者全体に占める割合	被害内容別、被害者全体に占める割合（複数回答）							
		ウィルス感染	起動異常・システム不調	大量メール送信	不正アクセス	個人情報の流出	ワンクリック詐欺	データの消失・改竄	その他
全体（回答数：5,142）	37.2%(1,915)	77.1%	34.6%	13.0%	11.6%	10.0%	8.3%	2.9%	2.9%
経営者・役員(104)	49%(51)	76.5%	27.5%	15.7%	15.7%	7.8%	9.8%	5.9%	2.0%
会社員など（情報システム関係の技術者）(429)	42.7%(183)	80.9%	30.6%	7.7%	13.1%	7.1%	7.1%	1.1%	1.1%
会社員・公務員・派遣社員（その他）(1,989)	36.2%(720)	76.4%	34.3%	13.1%	10.4%	11.0%	10.0%	3.3%	2.2%
自営業・自由業(448)	47.5%(213)	73.7%	38.5%	16.9%	13.1%	6.6%	11.3%	3.3%	2.8%
専業主婦/家事手伝い・無職（1,017）	31.4%(319)	73.0%	33.2%	15.0%	9.4%	10.0%	2.5%	1.9%	6.3%
パート・アルバイト(587)	34.9%(205)	76.6%	34.6%	13.2%	12.2%	12.7%	7.3%	2.0%	3.9%
学生(541)	39.7%(215)	87.0%	38.1%	9.3%	13.5%	9.3%	9.3%	4.7%	0.9%

＜平成 19 年＞

（全体）

	被害内容別、被害者全体に占める割合（複数回答）											
	コンピュータウィルスに感染した（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）	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	全く知らない差出人から大量にメールが送られてきた	メールに記載されたURLをクリックしたら、個人情報の求めるウェブページが表示された。	HP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	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	知らない間に銀行口座からお金が引き出された	知らない間に自分のパソコンから他者へメールを送信していた	個人情報流出の被害にあったことがある。	個人情報を流出させてしまったことがある。	左記以外の被害	被害にあったことはない／分からない
全体（回答数：5,160）	17.3%	1.9%	24.5%	5.6%	8.7%	6.3%	0.4%	1.2%	4.5%	0.5%	0.7%	57.8%

○ コンピュータウイルス遭遇率（企業）（コンピュータウイルスに関する被害状況調査：情報処理推進機構）

	回答総数				感染した				ウィルスを発見したが感染には至らなかった				感染も発見もしなかった				無回答			
	平成15年	平成16年	平成17年	平成18年	平成15年	平成16年	平成17年	平成18年	平成15年	平成16年	平成17年	平成18年	平成15年	平成16年	平成17年	平成18年	平成15年	平成16年	平成17年	平成18年
総数	1,115	1,150	1,701	1,775	22.2%	20.9%	15.3%	12.0%	47.4%	48.0%	53.7%	51.3%	29.8%	31.1%	29.9%	36.1%	0.6%	-	1.1%	0.6%
企業	651	762	1,206	1,213	21.4%	21.3%	17.6%	14.7%	35.5%	37.5%	47.9%	46.3%	42.4%	41.2%	33.2%	38.3%	0.8%	-	1.3%	0.7%
地方自治体	464	388	495	562	23.3%	20.1%	9.7%	6.2%	64.2%	68.6%	67.9%	61.9%	12.1%	11.3%	21.8%	31.5%	0.4%	-	0.6%	0.4%

○ スパイウェア遭遇率（企業）（コンピュータウィルスに関する被害状況調査：情報処理推進機構）

平成17年	回答総数	スパイウェアの侵入を受けた、スパイウェアが実行された。	スパイウェアを発見したが、侵入や実行には至らなかった。	侵入や実行は無く、発見もしなかった。	無回答
総数	1,701	7.5%	23.9%	66.6%	1.9%
企業	1,206	8.3%	23.5%	66.4%	1.8%
地方自治体	495	5.7%	25.1%	67.1%	2.2%

※　平成 17 年から調査開始。

平成18年	回答総数	スパイウェアの発見のみ	情報流出などを確認した	なし	無回答
総数	1,775	26.9%	0.2%	72.1%	0.8%
企業	1,213	27.0%	0.3%	72.0%	0.7%
地方自治体	562	26.5%	0.0%	72.4%	1.1%

○ 企業間（BtoB）電子商取引の現場（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）

		市場規模				電子商取引化率			
		日本		米国		日本		米国	
		17年	18年	17年	18年	17年	18年	17年	18年
企業間電子商取引	狭義EC	140兆円	148兆円	92兆円	95兆円	12.9%	12.6%	5.7%	4.4%
	広義EC	224兆円	231兆円	189兆円	196兆円	20.6%	19.8%	11.9%	9.3%

			13年	14年	15年	16年
企業間電子商取引	狭義EC	市場規模	34兆円	46.3兆円	77.4兆円	102.7兆円
		電子商取引化率	5.0%	7.1%	11.2%	14.7%
	参考・広義EC市場規模				157兆円	191兆円

※　「狭義ＥＣ」とは、インターネットによる商取引を計上したものであり、「広義ＥＣ」とは、インターネットによる商取引に加えて、インターネット以外のＶＡＮや専用線によるコンピュータ・ネットワークシステムを介した商取引も計上したものである。
※　平成１７年の数値から調査方法を変更しているため、平成１６年以前の数値との単純比較は出来ない。
※　平成１５年及び１６年の広義ＥＣ市場規模については、調査により確認できた情報のみで規模を算出しており、実際の市場規模はこれを上回るものと考える。

○ 消費者向け（BtoC）電子商取引の現場（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）

	市場規模				電子商取引化率			
	日本		米国		日本		米国	
	17年	18年	17年	18年	17年	18年	17年	18年
消費者向け電子商取引	3.5兆円	4.4兆円	15.9兆円	19.3兆円	1.2%	2.03%	2.4%	4.37%

		13年	14年	15年	16年
消費者向け電子商取引	市場規模	1.5兆円	2.7兆円	4.4兆円	5.6兆円
	電子商取引化率	0.6%	1.0%	1.6%	2.1%

※　平成１７年の数値から調査方法を変更しているため、平成１６年以前の数値との単純比較は出来ない