２００６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１年目の評価－

内閣官房情報セキュリティセンター（NISC）

２００７年4月23日

目次（案）

はじめに

第１章　情報セキュリティ政策全体の評価等

第２章　政府機関における現状の評価等

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】

はじめに

1．　本文書の位置づけと基本認識

本文書は、2006年度から始まる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、それに基づく年度計画である「セキュア・ジャパン2006（以下「SJ2006」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、2006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 (NISC)）（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、2006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2007（以下「SJ2007」という。）」を策定することになる。

したがって、本報告書の主眼は、2006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SJ2007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。

---

1 ２００６年２月２日情報セキュリティ政策会議決定

2 ２００６年６月１５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。但し、2006年度は、補完調査は行っていないため、2006年度の「評価等」には実質的には補完調査が含まれない。

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］）

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「2006年度の取組み」、第2節では「2006年度の取組み及び取組みを受けた現状の評価等（2006年度の評価等）」、第3節では、評価等から抽出される「2007年度に向けた課題」について述べる。そして、第2節の2006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」と「施策の取組みによる社会的変化」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SJ2006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。但し、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

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。

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。

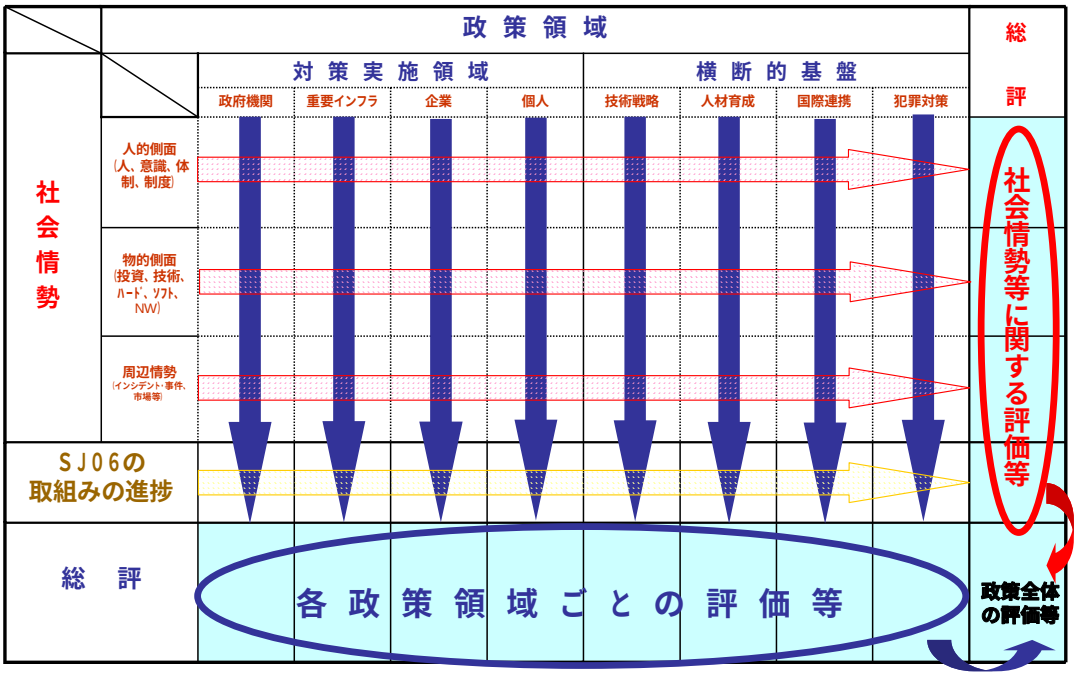
においてまとめられることから、これらを活用する。

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等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（参照：図1）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。社会情勢は、非常に広範な要素を含むことから、検討にあたっては、

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、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を行うこととする。

図1：2006年度の情報セキュリティ政策の評価等に係る検討枠組み



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2006年度の取組み

1．2006年度の取組みの背景

我々の日々の社会経済活動においては、ITが活動の基盤となってきている。そして、これに伴ってIT利用の安心･安全を確保するための情報セキュリティが重要な課題となってきた。実際、情報セキュリティ面でのリスク[8]は増大しており、例えば、チケット販売のオンライン化や電子マネー機能の浸透に見られるような経済活動の電子化･バーチャル化は、処理速度や効率性の大幅な向上とともに利用者に利便性向上をもたらす一方で、IT障害への対応が十分になされていない場合、大きな被害を発生させる可能性がある。また、こうした情報セキュリティ面からの対応を行うに際して、専門的知識やスキルを有した人材が不足しているために、迅速な対応ができない可能性もある。さらに、インシデント･事件の側面から見ても、2005年にはウェブサーバへのサイバー攻撃、ファイル共有ソフトの利用やコンピュータウイルス等に起因する情報漏洩、重要インフラのIT障害による業務停止、不正アクセス等のサイバー犯罪等が発生した。加えて、2006年には、ウイルス付きメールを送付してコンピュータに不正なプログラムを潜伏させるような被害が顕在化しにくい攻撃が見られ、またインターネット上で個人からの情報発信を伴う新たなサービスが急速に普及したことにより、新たなリスクが見られるようになっている。

こうした状況において、官民が一丸となって効果的な対応を行うことで、ITを安心･安全に利用できる環境を構築することを目的として、2006年2月に第１次情報セキュリティ基本計画（以下「基本計画」という。）が策定された。これにより、それまで個別に情報セキュリティ対策に取り組んできた個々の主体が、政府機関･地方公共団体、重要インフラ、企業、個人という対策実施4領域として明確に計画に位置付けられ、全主体の参加の下で対策を実施する新たな政

8 「情報セキュリティ政策の枠組み文書」第１章第２節においては、リスクについて「(i)サイバー攻撃を受ける、情報漏えいが発生する、というようにＩＴ利用の安全性を担保・促進するために解決すべき個々の課題や、(ii)個人の情報セキュリティに関する知識が不足している、情報セキュリティ対応を行う人員が不足している、被害が生じた際に対応が後手にまわる、情報セキュリティを意識しすぎる余り自由な利害が阻害されるなど、取組みを進めることで克服が求められる構造的課題といった、解決し、また克服しなければならない様々な課題」と述べている。

策体系に基づく取組みが開始された。また、技術戦略、人材育成・確保、国際連携・協調、犯罪取締り及び権利利益の保護・救済といった「横断的な情報セキュリティ基盤」の構築についても、総合的に取組みを推進する方針が示された。情報セキュリティに関する2006年度の取組みは、こうした中長期的な方針の下で、初年度の取組みとしてなされたものである。

2．2006年度の取組み

2006年度の取組みでは、まず年度計画であるSJ2006が6月に策定された。SJ2006では、「官民における情報セキュリティ対策の体制の構築」が重点とされ、重点目標として、(1)官民各主体の共通認識の形成のために「すべての主体に情報セキュリティ対策への参加意識を持たせること」、(2)先進的技術の追求のために「先進的技術の追求に係る取組みを政府全体として一定の方向性を持って行うこと」、(3)公的対応能力の強化のために「公的部門の情報セキュリティ対策のレベルを高める仕組み及び官民における必要な連絡体制を構築すること」、(4)連携・協調の推進のために「すべての主体による情報セキュリティ対策に係る情報共有体制を構築すること」が設定された。

また、SJ2006では、「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、内閣官房を含む各府省庁が計133の具体的な施策を実施することが盛り込まれた。

さらに、SJ2006では、「官民における情報セキュリティ対策の底上げ」という2007年度の重点施策の方向性が設定され、「模範となる領域の底上げ」、「取組みが遅れがちな主体の対策の底上げ」、「横断的な情報セキュリティ基盤の底上げ」に向けた計26の具体的施策が盛り込まれた。

2006年度は、このようにSJ2006に沿った形で情報セキュリティに関する取組みがなされた状況である。

第2節　2006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(2006年度の評価等)

1．2006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2006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) 2006年度は基本計画に基づく政策体系の下で取組みを実施する初年度であったことを踏まえ、取組みが実効的に進められ、結果として、SJ2006に記載された当初の目標を実現できたか否かを測るという視点、
2) 2006年度の取組み開始時に存在していたリスクが、1年間の取組みをもってどうなったのか測るという視点、
3) 取組みの結果、2007年度に残った課題、すなわち2007年度に「底上げ」が必要な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) 2006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。特定の評価指標は少なくとも2006年度は設けない。

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) 2007年度以降の評価等について

2007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2006年度の評価等を踏襲することとなる。しかし、2006年度は情報セキュリティ政策の評価等の枠組みの完成（2007年2月2日の情報セキュリティ政策会議で決定・了解）から評価等の実施までの期間が短く、十分な評価等を行うに足りる情勢把握ができていない。したがって、章によっては社会的な変化をはじめとする様々な部分について検討が不十分なものが少なくない。

こうしたことを踏まえ、2007年度は評価等をより充実させる。具体的には、

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」の結果を考慮することが挙げられる。また、2007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となると考えられるが、こうした点についても2007年度以降の評価等において反映を行う。

(3) その他

評価等にあたっては、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

SJ2006において、2006年度中に推進するとされた133の具体的施策の取り組み結果については、別添1の表のとおりである。この結果を当初実現予定の目標と比べ、以下のとおり分類した。すなわち、

- ○ 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ができず、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は出来なかったが、その理由が政府機関の事情によるものではない施策

である。

これによると、133の具体的施策は、

A…110　A′…6　B+…4　B…12　C…0　―…1

と分類することができ、約87.2%(116／133)の施策について、年度内に推進することが出来たと評価された。A の施策は110と大半を占めており、今後も引き続き取組みを継続することや、発展的な更なる取組みを行うことが期待される。A′の施策については、関係各府省庁の担当者等の尽力により予定どおり推進することが出来たものの、政府機関について見ると、「各政府機関でのPDCAサイクルの確立」、「政府全体でのPDCAサイクルの確立」という対策の大部分を占める2つの施策がA′となっていることから、体制や人員等の不足が大きな課題であることがうかがえる。

他方、B+とされた施策は、今後の情報セキュリティ政策会議における決定を経ることにより手続が完了するものなどである。また、Bとされた施策については、慎重に検討を進めた結果として年度内に推進できなかったものなどであり、今後も取組みを続けることによって、最終的には施策を推進することはできると思われる。

以上を総括すると、SJ2006において、2006年度中に推進するとされた133の具体的施策については、各府省庁において着手がなされ、担当者等の尽力もあって概ね順調に進捗したと言える。しかし、その多くは、今後も引き続き取組みが必要とされる施策、発展的な更なる取組みを必要とする施策であり、来年度以降も取組みを継続する必要があるが、一部の施策については、今後も引き続き推進して行くための体制や人員等は不十分であると考えられる

(2) 施策の取組みによる社会的変化に関する評価等

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。但し、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

第一に人材面では、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書でも明らかにされたと

おり、我が国における情報セキュリティに係る人材の育成・確保は、いまだ十分な水準とは言えず、緒についたばかりという状況にある。特に、我が国全体の情報セキュリティの対策を考える上で、最も広範囲に渡ると考えられる政府機関と企業における人材及びその育成方策がいまだ不十分であるほか、先進的な情報セキュリティ技術・製品及び高度な管理手法の研究・開発者や、情報セキュリティに関する製品等を提供する企業等における人材についても、なお一定の課題が見られることが浮き彫りになっている。

(イ) 意識面

第二に意識面では、2006年度の取組みを通じ、各々の対策実施領域において情報セキュリティに係る「意識の発露」が見られたと言える。この背景には、内閣官房を中心に、各府省庁によって基本計画やSJ2006などが策定され、我が国全体として情報セキュリティに関する取組みが進められたことがある。

また、産業界においては、金融商品取引法(日本版 SOX 法)の施行に向け、企業の内部統制の一環としてIT統制の重要性に対する意識が高まったこと、IT障害や災害発生時の事業継続計画(Business Continuity Plan(BCP))に対する意識が高まったことなどが挙げられる。一般的に情報セキュリティ対策はコスト要因と考えられ、取組みが後手にまわりがちであるが、景気の回復によって企業に余裕が出てきたことも意識向上に作用していると考えられる。さらに、様々な情報流出などがマスコミによって大きく取り上げられ、情報セキュリティ問題が、漏えいデータに基づく詐欺や損害賠償、システムに対する再投資といった形で経済的損失につながるということが認識されたことも、大きく影響していると考えられる。

個人については、SJ2006の下で啓発を目的とする各種取組みが積極的に推進されたことも「意識の発露」の背景にあると考えられる[9]。

さらに、例えば個人に関しては「犯罪に遭うかもしれない」との不安をインターネット空間に対して感じる割合が、前年に比して倍増の4割となった[10]ように、「意識の発露」の結果、不安感を持つようになったと思わ

9 取組みの詳細については、別添１「「セキュア・ジャパン２００６」に盛り込まれた施策の実施状況」を参照。

10 内閣府「治安に関する世論調査（２００６年１２月調査)」より

れる調査結果がでたことも象徴的であった。また、情報セキュリティ対策を実施していない個人や[11]、具体的にどう取組めば良いのかわからない事業者や個人も存在していると考えられる。

こうしたことを考慮すると、2006年度の段階では、情報セキュリティに係る意識については「発露」の段階にとどまっており、各主体が情報セキュリティ対策を当然に行うものとして捉えるには至っていない[12]と考えられる。

(ウ) 体制面

第三に体制面については、日本版ＳＯＸ法対応の一環として、企業がＩＴ統制に係る対応体制を強化する傾向も見られる[13]。また、政府機関については、ＳＪ２００６に基づく施策の一つとして、ＮＩＳＣが、官民合わせて約６０名の人材からなる体制に強化された。この結果、内閣官房が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少しずつ整いつつあると言える。しかし、情報セキュリティ担当者は依然不十分な状況にあり、今後引き続き整備が必要である。

(ｂ) 物的側面 (投資、技術、ハード、ソフト、ネットワーク)

情報セキュリティに関する投資面については、例えば、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・情報共有機能（ＧＳＯＣ：Government Security Operation Coordination Team）のためのシステム構築予算が確保された[14]。

また、企業においては、情報セキュリティに関する問題を起こすことによる経済的損失との比較衡量の下で投資がなされる傾向が見

(http://www8.cao.go.jp/survey/h18/h18-chian/、
http://www8.cao.go.jp/survey/h18/h18-chian/images/h04-1.csv)

11 ６５頁及び別添８参照

12 ６４頁及び別添８参照。情報セキュリティ対策は費用がかかるという意識は依然として根強いことが挙げられる。

13 「日本における内部統制の現状に関するアンケート調査」（２００７年２月（株）富士通総研経済研究所）によれば、調査に回答した企業のうち「システム監査の実施」と「ＩＴ全般統制の強化」に取り組んでいると回答している者がそれぞれ約４０％(調査対象：上場企業全社(3,691社)、回収数：814社)。但し、「ＣＯＢＩＴの利用」や「ＩＴＩＬの活用」については、５％前後にとどまった。

14 但し、政府の２００７年度情報セキュリティ予算の金額は、前年度比６％減という状況である。

られる。但し、企業規模などによっても投資に対する積極性は異なるものと考えられる。個人分野では、コンピュータの販売価格に情報セキュリティ対策ソフト代が実質的に含まれていることで、購入者の意識の高低に関係なく対策ソフトを購入しているケースも少なくないと考えられるものの、情報セキュリティ対策ソフトの購入が一般的になりつつある[15]。

これらを総合すると、情報セキュリティ意識の「発露」に伴って、対策のために投資せざるを得ない分の投資は行うという姿勢になりつつあるものと考えられる。また、情報セキュリティ政策会議の下に設置されている技術戦略専門委員会では、単に予算を研究開発に投入するだけではなく、研究開発・技術開発に係る投資効率を向上するための検討が行われるなど、投資の質向上に向けた動きも見られた。

情報セキュリティ技術面については、インシデント・事件の発生などを受け、具体的な対策の必要性に迫られた製品を中心として開発が進められる傾向にあった。今後は、暗号などの既存の高品質の製品に関し、普及を進めることも必要となってくると考えられる。

（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等による情報の流出が依然続いた。但し、従来と異なる点は、インターネット上で個人からの情報発信を伴う新たなサービスなどが複数現れたのに伴い、新しい形の被害が見られるようになったことである。具体的には、流出情報を元に、新しいサービスなどで公表されていた関連情報が収集・突合され、例えば当事者の職業など、各々の情報だけからでは本来判明することのなかった情報が判明する事態が生じている。このように、組織の機密情報のみならず、一個人のプライバシーに関する情報も攻撃の標的とされる事態が生じるようになったことにより、個人レベルでのセキュリティ対策も避けては通れない状況となってきたと言える。

また、政府機関や企業に対しては、従来のホームページの改ざんやウェブサーバへのＤｏＳ攻撃といった被害が顕在化しやすい攻撃

15 ６５頁及び別添８参照

から、特別仕様のウイルス付きメールを送付することによってコンピュータに不正なプログラムを潜伏させようとする攻撃へと変化が見られ、被害が顕在化しにくくなった。これらに加え、ボット[16]に感染することによる被害も新たに発生した。こうした新たなリスクが生じた中、犯罪の絶対数の増加によるものであるのか検挙率の向上によるものであるのかは不明であるが、サイバー犯罪の検挙数が前年比４割増で過去最大となった。中でも、とりわけ不正アクセスに係る件数は顕著で、前年比２．５倍の検挙数となっている[17]。以上をまとめると、ＩＴ利用に係るリスクを抑制する努力が進められる一方で、攻撃手段も次々と進化している状況にあると言える。

ＩＴ障害については、従来はあまり想定されなかったリスクが顕在化する事例が生じたことが特徴的であった。例えば、社会経済活動の国際化を反映して、ＩＴ障害の範囲が一か国内にとどまらない事例が挙げられる。２００６年末の台湾沖での地震によって通信ケーブルが切れた案件では、周辺国に影響が及び、国際的な対応体制が課題になり得ることを示唆している。

(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あ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。

２００６年度においては、情報セキュリティ対策に係る取組みは総じて概ね順調に行われ、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構築が進んだと言える。

また、各対策実施領域が情報セキュリティのための取組みの必要性に気付いた一年であったとも言える。各対策実施領域は、従来、個々の主体の単独の取組みとしてセキュリティ対策を実施してきたとこ

16　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。

17　詳細については、「平成１８年のサイバー犯罪の検挙及び相談状況について」（２００７年2月２２日警察庁広報資料）参照。（http://www.npa.go.jp/cyber/statics/h18/pdf34.pdf）

ろ、ＮＩＳＣの旗振りの下、各々の対策実施領域内における連携が進展した。加えて、ＮＩＳＣが結節点となることで各々の対策実施領域の枠を超え、我が国全体を視野に入れた取組みが進められた。

つまり、２００６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萌芽、２）対策実施領域ごとの具体的取組みの着手、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手、４）情報セキュリティ推進体制と持続的改善構造の構築であった。

他方、政策領域によっては対策のスピード感が欠けていることも事実である。これには、人的資源の不足といった要因も大きく作用しているものと考えられる。ＩＴ利用におけるリスクも大幅に軽減したとは言えず、情勢が変わる中でリスクの変化を捉え大きく増加しないよう様々な努力がなされている状況にある。さらに、ＳＪ２００６に盛り込まれた施策の実施状況としては十分な結果であったが、２００６年度の施策の目標自体がまだ第一歩目に過ぎない施策も存在している。

我が国が真の情報セキュリティ先進国となるよう２００７年度も積極的な取組みが引き続き行われることが期待されるところである。

第3節 2007年度に向けた課題

以上から、２００７年度に向けては、２００６年度に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や、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大きな課題となる。

こうした課題に対応するためには、第一には、対策を実施する主体の意識面として、情報セキュリティに対する意識の維持・向上を図ることが不可欠である。

また、第二には、官民の情報セキュリティ対策を推進するための体制の下、年度単位（１年)、基本計画単位（３年）の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、各対策実施主体が積極姿勢を失わないようにしながらも着実に進めることが重要である。とりわけ、ここでは情報セキュリティ対策の底上げの視点が大きなテーマである。政府機関、重要インフラといった他の模範となるべき領域は、対策の底上げを図ることで取組みのスピードを加速し、取組みが遅れている主体に対

して模範を示す必要がある。また、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や、横断的な情報セキュリティ基盤の底上げも欠かせない。

なお、例えば人材の育成・確保などについては、２００７年度単年度で解決できる課題ではなく、むしろ中長期で継続的に取り組むべき課題と考える必要がある。また、国際連携・協調のように、取組みを着実に進めたことで２００６年度の目標は達成したものの、目標が第一歩目に過ぎず、これから本格的な取組みを行う必要がある課題もある。さらに、急に発生したリスクへの対応を含め、時宜に合った喫緊の課題として取組みを開始し、迅速かつ集中的に対応を行うことが必要な課題も存在する。こうした課題への対応も適時適切に行うことが重要である。

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2006年度の取組み

1．2006年度の取組みの背景

情報セキュリティ対策の実施主体の一つとして先導的な役割を担う政府機関としては、各府省庁ごとの情報セキュリティ対策を確実に実施するとともに、全体として協調して成果の共有化等に取り組む必要がある。しかしながら、政府機関においては、府省庁間に情報セキュリティ水準の格差がある、特に内部からの脅威に対して脆弱である、緊急対応等の観点からの取組みが不足している、年々複雑化する情報セキュリティ問題に対応するための高度な専門知識を有する人材が不足している等の問題を抱えている。

そこで、政府機関の情報セキュリティ対策を強化するため、「政府機関の情報セキュリティ対策の強化に関する基本指針」（2005年9月15日情報セキュリティ政策会議決定）等が定められるとともに、「政府機関の情報セキュリティ対策のための統一基準」（2005年12月13日情報セキュリティ政策会議決定。以下「政府機関統一基準」という。）が策定された。これによって、各府省庁は政府機関統一基準を踏まえた対策を実施し、NISCが各府省庁の対策実施状況を検査・評価する枠組みが整備された。

その後、2006年2月に策定された基本計画においては、1）2008年度までに政府機関統一基準のレベルを世界最高水準のものとし、かつ、2）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こととされており、NISC及び各府省庁は、2006年度は年度計画であるSJ2006の下、当該目標を目指して取組みを進めることとした。

2．2006年度の取組み

2006年度の取組みについては、基本計画の初年度として、重点的に取り組むべき施策がSJ2006にとりまとめられた。

特に、各府省庁は、政府機関統一基準を踏まえた省庁基準に基づき、情報セキュリティ対策の実施のためのPDCAサイクルを確立するものとし、また、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、必要な範囲で検査・評価し、各府省庁の対策の改善と政府機関統一基準等の改

善に結びつけることで、政府全体としてのＰＤＣＡサイクルを確立するものとされた。

その他、独立行政法人等のセキュリティ対策の改善、中長期的なセキュリティ対策の強化･検討、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及び政府機関における人材育成について、具体的な施策が定められた。

第2節　2006年度の取組み及び取組みを受けた政府機関における現状の評価等（2006年度の評価等）

1．2006年度の評価等に関する基本的考え方（評価等の視点）

政府機関における情報セキュリティ対策に係る2006年度の評価等について、以下の2つの視点に基づいて行うこととする。すなわち、2006年度は、政府機関統一基準及び基本計画に基づく政策体系の下で対策を実施する初年度であったことを踏まえ、1）本格的な対策を実施する前の状態を確認し、かつ情報セキュリティの観点から特に重要な部分の状況について検査を行うという視点、2）対策が実効的に進められた結果、当初の目標を実現できたか否かを測るという視点、3）取組みの結果、2007年度に残った課題（「底上げ」が必要な課題）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）2006年度の評価等について

政府機関の情報セキュリティ対策の2006年度の評価等については、本格的な対策を実施する前の現状について、特に重要な部分（端末とウェブサーバ）の対策を把握するための重点検査を実施した上で、政府機関統一基準を踏まえた2006年度の対策実施状況とＰＤＣＡサイクルが確実に回る仕組みとなっているかを把握するための情報セキュリティマネジメントについて評価を行い、さらに、SJ2006の各施策の取組み結果について分析するなど、2007年度以降に取り組むべき課題を明らかにする。

一方、政府機関統一基準に基づく対策以外の施策については、現時点では指標が採り難いことから、進捗状況について把握を行い、2007年度以降取り組むべき課題の整理を行う。

(2) 2007年度以降の評価等について

2007年度以降についても、年度ごとの対策実施報告、特定の重点項目に係る年数回の重点検査等を行うなどにより、各年度の政府機関の対策実施状況と情報セキュリティマネジメントについて評価を行うとともに、各年度の年度計画の各施策の取組み結果について分析するなど、基本計画最終年度である2008年度に向け、取り組むべき課題を明らかにする。また、評価指標について、運用段階で把握された問題点等を踏まえ、逐次見直し、改善を行う。

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

[対策実施状況に関する評価等]

(重点検査に基づく評価等)

2006年7月に、全府省庁の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(2006年3月末時点)について重点検査を行い、その結果の総合評価(AからDまでの4段階評価)を情報セキュリティ政策会議第7回会合において実施した。端末については、不正プログラム対策、情報保護対策及び端末管理の3つの観点から、ウェブサーバについては、不正プログラム対策、不正アクセス対策、情報保護対策及びサーバ管理の4つの観点から、それぞれ評価し、評価結果を、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3に示す。

＝分析＝

端末については、実施率が8割を超えるもの(評価:B以上)は3府省庁にとどまる一方、6割を下回るもの(評価:D)は6府省庁であり、全体として、対策の改善・見直しが必要という結果であった。

ウェブサーバについては、実施率が8割を超えるもの(評価:B以上)は15府省庁である一方、6割を下回るもの(評価:D)はなく、概ね対策は実施されていると言えるが、まだ一部の府省庁では対策の適切な実施が必要という結果であった。

(対策実施状況報告に基づく評価等)

「第1次情報セキュリティ基本計画」において、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こととされており、2006年度における各府省庁の進捗状況について評価を行った。

具体的には、2006年度の各府省庁の対策実施状況報告を基に、各府省庁の進捗度合（全遵守事項中、全対象職員が実施した遵守事項の割合等）について評価等を行った。とりまとめ結果を別添4に示す。

2006年度は、政府機関統一基準の導入初年度ということもあり、全遵守事項について完全に実施されている状況ではないが、到達率の低い遵守事項が明らかになり、各府省庁において、取り組むべき課題が明確化されている。

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、

（行政事務従事者の責務）

○ 情報の格付け・取扱制限に係る措置

（情報セキュリティ責任者等の責務）

○ 情報セキュリティ教育の実施
○ 情報セキュリティ監査の実施
○ 電子署名の付与に必要な機能の導入

等が挙げられ、今後改善が必要となっている。

[情報セキュリティマネジメントに関する評価等]

政府機関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行われているかを評価する指標（マネジメント指標）については、情報セキュリティ政策会議・政府機関評価指標専門委員会（2006年9月～12月）において策定され、「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、情報セキュリティ政策会議了解）にとりまとめられている。

2006年度においては、この指標を基に、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現状に関し把握できるものについて、調査を行った。結果を別添5に示す。

なお、各府省庁における取組みの詳細については、今後、さらに個別ヒ

アリング等で確認を行い、2007年度前半に、各府省庁の情報セキュリティマネジメントの総合的な評価を試行的に実施する。
その際、以下の点について重点的に確認を行う。

○「計画」：担当者等の現状、推進体制（PMO及びCIO補佐官等を含む）の実効性等
○「周知」：ヒヤリハット情報の活用状況、教育に関する取組み状況等
○「実施」：IT活用状況、異常・障害等・例外措置の管理状況等
○「評価と改善」：自己点検・監査の計画及び実施における取組み状況等

［SJ2006施策の取組み結果に関する評価等］

SJ2006施策の取組み結果（概要）については、以下のとおりであり、本格的な対策初年度であったために推進体制が十分に整わないなか、結果として一定の前進が見られたという状況である。

（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、毎年その見直しを行うものとされており、2006年度において、技術・環境の変化や各府省庁における対策実施状況等を踏まえ、内閣官房において見直しを実施した。内閣官房（NISC）は、見直し結果を踏まえ、政府機関統一基準の改訂案を情報セキュリティ政策会議第11回会合に諮った。

b）PDCAサイクルの確立

各府省庁は、政府機関統一基準を踏まえた省庁対策基準に基づき、情報セキュリティ対策の実施のため、具体的な実施手順の整備、情報セキュリティ対策の実施状況の自己点検等を行うなど、PDCAサイクルを実施した。

内閣官房は、2006年7月に、全府省庁の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について重点検査を行い、その結果の総合評価を情報セキュリティ政策会議第7回会合において実施した。また、当該評価結果は、同日、内閣官房（NISC）のホームページにおい

て公表した（評価結果の詳細については、前述のとおり。）。

c）実施手順の作成支援及び技術的情報の提供と情報の共有

内閣官房は、各府省庁の情報セキュリティ対策の推進を支援するため、実施手順の作成支援及び技術的な情報の提供を実施した。また、これらの情報（個別マニュアル群）について、民間企業、地方公共団体、独立行政法人等が活用できるよう31種類を内閣官房（NISC）のホームページにおいて公開した。

d）コンピュータウィルスなどに起因する情報流出への対応

各府省庁の情報管理対策について、政府機関統一基準に基づき、2006年5月に調査を行い、その結果について、情報セキュリティ政策会議第7回会合（2006年7月25日）に報告した。また、府省庁においては、情報管理について、全職員に注意喚起を行い、相談窓口を設置するとともに、現状把握や関係規程の整備等を行った。

e）外部委託先等の情報セキュリティ対策の水準の確保

「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」を策定し、各府省庁に配布した。

（イ） 独立行政法人等のセキュリティ対策の改善

独立行政法人等の情報セキュリティ対策については、基本計画において、政府機関統一基準を踏まえ、その水準の向上を促進することとされており、2006年度は、独立行政法人等の情報セキュリティポリシーの整備状況を調査し、実態の把握を行った（概要を別添6に示す。）。

また、先行的に一部の独立行政法人等に対して、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、課題等について情報を収集した。

（ウ） 中長期的なセキュリティ対策の強化・検討

府省共通的なプラットフォーム（対象システムに必要なセキュリティ機能等を実装するための統一的な技術仕様、当該機能等を実現するためのシステム基盤等）の整備に関し、各府省情報化統括責任者（CIO）補佐官等連絡会議等との連携強化等が図られているが、まだ十分な枠

組み体制であるとまでは言えない。今後、電子政府システムに関しては、その企画・設計段階から、情報セキュリティを確保するための方策の強化が必要である。

(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

政府機関へのサイバー攻撃については、従来は府省庁ホームページの書き換えや、DoS攻撃による一時的なサービス停止といった現象が見られていたところ、2006年度には、特製のウイルス付きメールの送付のような攻撃に気付きにくいものが増えており、この点が重要な傾向であった。こうしたことも受けて、2007年度に、政府機関に対するサイバー攻撃への対応を大幅強化すべく、GSOC (Government Security Operation Coordination Team) の構築を行うこととなった。

(オ) 政府機関における人材育成

2006年8月より人材育成・資格制度体系化専門委員会を開催し、「人材育成・資格制度体系化専門委員会報告書」を策定した。同報告書の中で、政府統一的な教育プログラムの整備等が提言された。2007年度以降、この提言を実施可能なものから順次実施する必要がある。

(2) 施策の取組みによる社会的変化に関する評価等

政府機関の施策の取組みにより、2006年度において、社会的な変化が見られ始めている。特に注目すべき事項としては、政府機関以外の地方公共団体や国立大学法人等においても、政府機関統一基準に準拠した情報セキュリティポリシーのガイドライン等が策定され、それに対応するように政府機関統一基準 (個別マニュアル群を含む) に対応したソリューションを提供する企業も登場し始めている。

(参考)

- ○ 「地方公共団体における情報セキュリティポリシーに関するガイドライン」の公表 (2006年9月29日、総務省)
- ○ 政府機関統一基準に準拠した国立大学法人向け情報セキュリティポリシーの公開 (2007年2月26日、国立情報学研究所・電子情報通信学会)

(3) 総評

対策実施状況に関しては、政府機関統一基準に基づく対策を実施する初年度ということもあり、その評価結果において、まだ到達率の低い遵守事項も見られ、各府省庁において今後改善すべき課題が明らかになった。また、情報セキュリティマネジメントについては、今回の分析により いくつかの課題が浮き彫りになったが、各府省庁のＰＤＣＡサイクルが各段階で確実かつ効果的に行われているかを把握するため、引き続き、各府省庁の取組みについて、詳細な分析等を行い、政府機関全体の底上げにつなげていく必要がある。

上述の結果を総合すれば、2006年度の政府機関の情報セキュリティ対策全体としては、各府省庁が対策の改善の必要性に気付き、必要な予算の獲得に向けた取組みも含め、改善に向けた努力を行った一年間であった。しかし、同基準を踏まえた体系的な取組みは緒についた段階にあり、対策が不十分な部分や、ＰＤＣＡサイクルを回す上での課題も様々見受けられる結果となった。また、情報セキュリティ管理体制は出来つつあるが、実質的に取組みを推進するための人員が不足しているとの指摘も少なくない状況であった。一方、SJ2006に掲げた施策等に関しては、その取組みは総じて順調に行われている。

第3節　2007年度に向けた課題

2007年度に向けては、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。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。こうした取組みを推進するためには、実施体制の強化も前提であり、情報セキュリティ対応人員面での拡充も課題となる。これに向けては、NISC を始め各府省庁の努力によって情報セキュリティ対策のプライオリティの向上等を図る必要がある。

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り、それを着実に実現し、推進する体制の構築が求められる。

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2006年度の取組み

1．2006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」（第1次基本計画）を目指して取組みを進めているところである。

重要インフラ分野における2006年度の取組みは、この行動計画の下で取組みを推進するための初年度の取組みとしてなされたものである。

2．2006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、SJ2006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　2006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（2006年度の評価等）

1．2006年度の評価等に関する基本的考え方（評価等の視点）

冒頭に述べたとおり、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、重要インフラ分野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、重要インフラ分野における情報セキュリティ対策の評価等は、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）2006年度の評価等について

2006年度における重要インフラ分野における情報セキュリティ対策の評価等を行うにあたり、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、SJ2006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、2006年度の進捗度合いを把握するための指標である。

（2）2007年度の評価等について

2007年度以降についても毎年度の年度計画に盛り込む取組みの進捗度合いが指標となる。毎年度の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、報告された前年度の実施状況や実際のIT障害の発生状況等も踏まえながら、行動計画に掲げられている取組みの着実な進捗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

重要インフラ分野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、2006年度においては、下表のとおり、計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、「分野横断的演習」及び「相互依存性解析」については、2006年7月から2007年3月まで、それぞれ10回、計20回の検討会を開催し、具体的な検討、取組みを進めたところである。

	主な議題
第6回専門委員会 （2006年6月12日）	・重要インフラ対策全般の今後の進め方について ・「分野横断的演習」「相互依存性解析」の進め方について
第7回専門委員会 （2006年11月27日）	・重要インフラ分野における情報セキュリティ対策の浸透度合いの評価指標について ・安全基準等の見直し、策定及び情報共有体制の構築の状況について ・「分野横断的演習」「相互依存性解析」の取組みの進捗について
第8回専門委員会 （2007年3月12日）	・「相互依存性解析」「分野横断的演習」の取組みについて ・「安全基準等の策定状況の把握及び評価」について ・「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見直し」について ・「情報共有体制の構築の状況」について

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」の策定・見直し

2006年9月末において、8分野が安全基準等の策定・見直しを実施した。また同年10月には水道分野が安全基準等を策定し、医療分野においても、2007年3月末に見直しを完了した。

②「安全基準等」の策定状況の把握及び評価

各分野における安全基準等の策定状況についてヒアリング等によって状況把握を行い、情報セキュリティ政策会議・重要インフラ専門委員会へ報告を行うとともに、2007年3月には指針との対応状況についての評価を実施した。

③指針の見直し

2007年3月に、定常的なIT障害の発生状況の分析、関連文書の検証、社会的条件や環境の変化の検証といったアプローチから、指針の見直し及び必要な改定のための作業を行い、重要インフラ専門

委員会において改定案をとりまとめた。

⑴ 情報共有体制の強化

①内閣官房と各重要インフラ所管省庁間での体制整備

各重要インフラ所管省庁にリエゾン（内閣官房併任）を置き、内閣官房と各重要インフラ所管省庁との間で情報連絡・情報提供を行うための体制を整備し、運用を開始した。

②各重要インフラ分野における CEPTOAR 整備の推進

7分野の重要インフラ分野において、2006年度末までにCEPTOARの整備を完了した。また、新規追加3分野（医療、水道、物流）において、2007年度中の CEPTOAR の整備に向けた基本的合意が完了した。

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、2006年度末に整備される各ＣＥＰＴＯＡＲ（7分野）の事業特性を把握するとともに、整備状況とあわせてＣＥＰＴＯＡＲ特性把握マップとしてとりまとめた。

④CEPTOAR-Council（仮称）設置に向けた検討

各重要インフラ分野が整備に向け検討中である CEPTOAR の参加を得て、CEPTOAR の代表から構成される CEPTOAR-Council（仮称）設置に向けた検討の場を重要インフラ所管省庁及び重要インフラ事業者等の協力を得て設置し開催した。

⑵ 相互依存性解析の実施、及び、分野横断的な演習の実施

相互依存性解析と分野横断的演習については、2006年度は、行動計画の初年度として、官民での連絡・連携の仕組みづくりを進めた段階であったため、この仕組みづくりと実効性の強化に寄与する知見を提供していくことを目的として、これらの取組みを実施した。

相互依存性解析と分野横断的演習は、官民で連携して行う分野横断的な取組みとしては、いずれも我が国で初めてとなるものであり、行動計画を踏まえ、研究的・試行的レベルから、段階的に進めていくことにしている。

この考え方に沿って、分野横断的演習は、年度上半期で、演習実施の概念、演習課題の設定及び演習方法の理解などを主眼とした研究的演習を2006年7月～10月にかけて実施し、これを踏まえ、2007年2 月に、重要インフラ10分野とこれを所管する5省庁などが参加して、具体的なシナリオの下に課題討議を行う「机上演習」を実施した。また、分野ごと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、知見の共有などの連携を図った。

また、相互依存性解析については、各重要インフラ所管省庁の協力を得て、各重要インフラ分野の特性や状況等に配慮しつつ、依存関係を可視化できる仕組み（静的相互依存性解析）の構築に向けた試行的な相互依存性解析を実施した。

これらの取組みの成果は、以下のように総括される。

①相互依存性解析

IT障害のメカニズムの構造化・可視化との面では、10分野間での定性的な接続関係の全体像の概要の把握の中で、ITシステムの運用に、通信、電力、水が重要なリソースであることが把握できた。

また、「求められる対策」に関する共通認識の醸成との面では、「自助」の取組みは進んでいる中で、「共助」の重要性への認識が高まった。その中でも、特にIT障害時における情報共有に対する期待が大きいことが明らかになった。一方、「依存する分野」と「依存される分野」では、認識に違いがあるものがあり、他分野の状況を把握することにより、他分野からどのように期待されているのか、について認識の共有が図られた。

さらに、演習シナリオに知見提供を行うとともに、ベストプラクティスなど、事例分析からの知見を共有することができた。

②分野横断的演習

2006年度の演習は、セミナー形式から始め、共通認識を形成するステップから検討を重ね、関係者の理解の増進に寄与しつつ実施した。

即ち、2006年度の目的に沿った検証課題を踏まえ、相互依存性解析の結果をインプットし、演習のパターンの検討、机上演習のシナリオへの反映・課題討議というステップを通じ、関係者間での意見交換を実施するというプロセスにより、実証的にアウトプットを導出すると

ともに、次の段階である機能演習の実施等に関する知見を得ることができた。

具体的には、この演習の実施により、①障害発生時等の分野間及び分野内のコミュニケーションと連携のあり方、②官民での情報共有・連携のあり方、③IT障害発生時における迅速な対策等実施のための平時からの対応のあり方、④今後の演習や解析の取組みのあり方などの点につき、現実的対応に当たっての知見や課題等が導出された。

(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、重要インフラ分野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

重要インフラ全10分野において、望ましいと考えられるレベルを満たす情報セキュリティ対策が実施されるための「安全基準等」が整備された。

また、指針の見直しを通じ、情報漏えい問題が引き続き発生していることや、ITの適用範囲の拡大・高度化やIT依存のブラックボックス化が進みつつあること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

政府（内閣官房及び重要省庁所管省庁）内における情報共有体制の整備と、各重要インフラ分野における情報共有体制の整備が進んだことにより、重要インフラ分野における官民の各主体間での情報共有、連絡・連携のための基本的枠組みが構築された。

(ウ) 相互依存性解析及び分野横断的演習

我が国で初めての取組みとして、情報共有の重要性等に関する重要インフラ関係者間での共通認識の醸成に寄与するとともに、前節に

述べたような知見等をとりまとめることができた。

これらの知見等は、その提供により、サプライチェーンの進展などの中での関係者間でのリスクに関するコミュニケーションの向上、「自助」のみならず「共助」の考え方を進めることによる社会のリジリエンシー[18]の向上などを通じ、国民生活や社会経済活動を支える重要インフラ基盤確立に向けたスパイラルアップに寄与するものとなると考えられる。

(3) 総評

以上のことより、2006年度における取組みは、別表2のとおり、当初の目標に沿った成果をあげている。

しかしながら、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、重要インフラ分野における情報セキュリティ対策については、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 2007年度に向けた課題

重要インフラ分野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り、2007年度においては、2006年度における取組みを通じて認識した以下のような課題も踏まえた取り組みを行うことが重要である。

(ア) 安全基準等の整備

①安全基準等の見直し

各重要インフラ分野における安全基準等については、2006年2月に策定された指針の内容を踏まえた対応がなされていること、また、分野の特性に応じた対策項目の具体化などの工夫もなされていることが確認できた。

一方で、指針の見直しを通じ改めて認識された情報セキュリティ対策上の問題意識については、現在の指針の中に既に具体的に盛り込まれているものと、そうでないものがあることも明らかとなった。

そこで、情報セキュリティ対策の向上のためには、これらの問題意識に対

18 リジリエンシーとは、耐障害性と復旧機能を意味する（参照：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）１２頁脚注）。

し、各分野において、対策の状況や今後の方針を確認・検証した上で、必要があれば新たな対策を早急かつ確実に講じる必要がある。

② 各重要インフラ分野における安全基準等の浸透状況等

各重要インフラ分野における「安全基準等」については、各重要インフラ事業者等との関係においては、それが所管省庁により作成した「基準」から業界団体が自主的に作成した「ガイドライン」に至るまで、分野の特性に応じ、形式や位置づけ、拘束力等に様々なケースがあることが改めて認識できた。

一方で、重要インフラ分野における情報セキュリティ対策の向上のためには、各重要インフラ分野において定められた「安全基準等」が、各重要インフラ事業者等が情報セキュリティ対策を行うにあたっての基準又は参考として役割を十分に果たし得るものである必要がある。

③ 指針の見直し

指針の見直しを通じ、定常的なIT障害の発生状況や、国内外の規格文書の動向、リスクマネジメント関連の動きなどを検証した結果、2006年2月の策定時からおよそ1年の間にも、情報セキュリティ対策を取り巻く環境は常に変化を伴うものであることが改めて認識された。また、本年度は見直しに至らなかったものの、今後の相互依存性解析の結果によっては、その成果を踏まえた情報セキュリティ対策の見直しの必要性も考えられる。

各重要インフラ分野における「安全基準等」は、情報セキュリティを取り巻くこれら環境の変化に応じ、随時見直しが行われるべきものであるから、安全基準等の策定・改定を支援することを目的とする指針についても、情報セキュリティに関して可能な限り、最新の問題意識を反映したものである必要がある。

(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年度の取組みにより、重要インフラ分野における官民の各主体間での情報共有、連絡・連携のための基本的枠組みは構築された。しかしながら、IT障害の未然防止、拡大防止・迅速な復旧、再発防止の3つの側面において重要となる情報が適切に共有され、的確な情報セキュリティ対策がなされるためには、状況の変化や実際の運用における課題の認識があった場合に、それに対応した工夫や見直しがなされることが重要である。

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（医療、水道、物流）においては、２００７年度中のCEPTOAR 整備に向けた基本的合意が完了したところであるが、２００６年度末までに整備された7分野の経験を踏まえると、今後実際の整備までの間に、新たに解決すべき課題が発生することも考えられることから、合意に基づいた着実な整備が図られるよう努めることが課題である。

③「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。

２００６年度末までに、7分野の重要インフラ分野において、重要インフラ事業者等との間で２００６年度末の整備を完了したところであるが、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、実際の整備に至るまでの間の様々な課題が明確となった。

その結果、整備初年度から各分野の事業特性に合わせた機能等のすべてが整備されているとは限らず、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。

④ 「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。２００６年度においては、「CEPTOAR－Council」（仮称）創設に向けた検討の場は、各分野でのＣＥＰＴＯＡＲの整備が進み、Councilの構成員の概要がほぼ固まった年度末に開催されたものであり、実質的な検討は今後行われることとなるが、「CEPTOAR－Council」（仮称）の設立に向けては、これらの構成員の間での基本的事項に対する合意が必要不可欠である。

（ウ）相互依存性解析の推進

２００６年度においては、重要インフラ分野間での定性的な接続関係の全体像の概要の把握の中でITシステムの運用に重要なリソースを把握する等

の知見を得たが、2007年度は、脅威の変化・多様化、想定外の脅威の発生などを踏まえ、脅威の類型や脅威と障害の因果関係などについての検討の深化などを行っていくとともに、時間と空間を超えて波及する等のIT障害の特徴などを踏まえつつ、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の実施方法の検討等を行っていくことが重要である。

(エ) 分野横断的演習の推進

2006年度は、行動計画の初年度として、官民での連絡・連携の仕組みづくりを進めた段階であり、机上演習における課題討議などを通じ、この仕組みづくりと実効性の強化に寄与する知見等をとりまとめた。2007年度は、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に寄与していくため、2006年度の取組みから得られた知見などを活用し、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していくことが重要である。

4本の施策の柱	2006 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	安全基準等の策定･見直し	2006年9月を目処に、指針を踏まえて、各重要インフラ事業分野における安全基準等に必要又は望ましい情報セキュリティ対策の水準を明示するよう努力する。この際、「情報システムの信頼性向上に関するガイドライン」を参考とする。
	「安全基準等」の策定状況の把握及び評価	2006年度中に「安全基準等」の策定状況を、各重要インフラ所管省庁の協力を得て把握を行い、相互依存解析の実施状況も踏まえつつ「安全基準等」の評価を実施する。
	指針の見直し	定常的なIT障害の発生状況の把握を通じ、各重要インフラ分野に共通する横断的な対策課題の分析･検討を行うとともに、政府機関統一基準、その他関連文書を参照しつつ、各重要インフラ所管省庁の協力を得て、2006年度中を目途に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	2006年度において、各重要インフラ事業者等から連絡された情報及び情報セキュリティ関係省庁 、事案対処省庁 、関係機関から集約した情報を分析し、適切に各重要インフラ所管省庁及び各重要インフラ事業者等に対し情報提供を実施する。さらに、緊急時においても関係者との間で必要な対処についての調整を行えるようセンター機能 の2007年度内運用開始に向けた環境整備に着手する。
	情報提供･連絡のための体制強化	内閣官房にて策定された実施細目 (仮称)に基づき、重要インフラ事業者等から各重要インフラ所管省庁ごとに選任されたリエゾンを通じて連絡された情報を内閣官房に連絡するための体制を強化する。また、内閣官房から提供された情報を CEPTOAR を通じて、各重要インフラ事業者等に提供するための体制を強化する。このため、重要インフラ所管省庁に、内閣官房が構築した情報共有体制を適切な情報管理で行うためのリエゾンを2006年度の可能な限り早期におき、内閣官房に併任する。
	各重要インフラ分野における CEPTOAR 整備の推進	各重要インフラ所管省庁及び各重要インフラ事業者等間での協議を開始し、2006年度末までに各重要インフラ分野に CEPTOAR が整備されることを目指す。また、新規追加分野（水道、医療及び物流）については、CEPTOAR 整備に関する重要インフラ所管省庁及び重要インフラ事業者等間での基本的合意を2006年度末までに完了することを目指す。
	「CEPTOAR 特性把握マップ」とりまとめ	重要インフラ所管省庁の協力を得て、各重要インフラ分野ごとに設けられる各 CEPTOAR の整備状況を把握するとともに、各分野の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「CEPTOAR 特性把握マップ」を2006年度末を目途に作成する。
	「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）の創設促進	2006年度内に整備される CEPTOAR の代表から構成される検討の場を重要インフラ所管省庁及び重要インフラ事業者等の協力を得て協議会設置に向けた検討の場を設ける。
③相互依存性解析の実施	相互依存性解析の試行的実施	2006年度中に、各重要インフラ所管省庁の協力を得て、2005年度の解析手法に関する調査結果を踏まえ、過去の災害等の調査等を通じて、依存関係を可視化できる仕組み（静的相互依存性解

		析）を構築するとともに、各重要インフラ分野の特性や状況等を配慮しつつ、試行的に相互依存性解析を実施する。
④分野横断的な演習の実施	「研究的演習」の実施	2006年度中に、演習実施の概念、演習課題の設定及び演習手法の理解等を主眼とし、各重要インフラ分野の特性や状況等を配慮しつつ、研究会を併用した演習（「研究的演習」）を実施する。
	「机上演習」 の実施	2006年度中に、類似業態単位又は重要インフラ分野横断的な共通事項単位に議論発掘と具体課題整理のための「机上演習」を実施する。
	各分野サイバー演習との連携	2006年度中に、分野ごとに実施された「情報通信」「電力」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、連携に向けた検討を開始する。

（別表２）

２００６年度における取組みの進捗状況

4本の施策の柱	2006 具体的取組み目標		2006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	安全基準等の策定・見直し	・2006年9月を目処に、**指針を踏まえ**て、各重要インフラ事業分野における**安全基準等に**必要又は望ましい情報セキュリティ対策の**水準を明示**するよう努力。	・2006年9月末において、8分野が**安全基準等の策定・見直し**を実施。 ・同10月水道分野が安全基準等を**策定**。 ・医療分野においては、2007年3月末に**見直し**を完了。
	「安全基準等」の策定状況の把握及び評価	・2006年度中に「安全基準等」の策定状況を、各重要インフラ所管省庁の協力を得て把握を行い、相互依存解析の実施状況も踏まえつつ**「安全基準等」の評価**を実施。	各分野における安全基準等の策定状況についてヒアリング等によって状況把握を行い、情報セキュリティ政策会議・重要インフラ専門委員会へ報告を行うとともに、2007年3月に、**指針との対応状況についての評価**を実施。
	指針の見直し	・2006年度中を目途に**指針の見直しを実施**。	2007年3月に**指針の見直し**及び必要な改定のための作業を行い、重要インフラ専門委員会において**改定案**をとりまとめ。
②情報共有体制の強化	情報共有体制整備と機能強化	・各重要インフラ事業者等から連絡された情報及び情報セキュリティ関係省庁 、事案対処省庁、関係機関から集約した情報を分析し、適切に各重要インフラ所管省庁及び各重要インフラ事業者等に対し情報提供を実施。 ・緊急時においても関係者との間で必要な対処についての調整を行えるよう**センター機能 の**2007年度内運用開始に向けた**環境整備に着手**。	各重要インフラ所管省庁に**リエゾン（内閣官房併任）をおき**、センターと各重要インフラ所管省庁との間で**情報連絡・情報提供を行うための体制を整備**し、運用を開始。
	情報提供・連絡のための体制強化	・内閣官房にて策定された実施細目(仮称)に基づき、重要インフラ事業者等から各重要インフラ所管省庁ごとに選任されたリエゾンを通じて連絡された情報を内閣官房に**連絡するための体制を強化**。 ・重要インフラ所管省庁に、内閣官房が構築した情報共有体制を適切な情報管理で行うための**リエゾンを**2006年度の可能な限り早期におき、**内閣官房に併任**。	・各重要インフラ所管省庁において、情報共有体制を適切な情報管理で行うための**リエゾンを、内閣官房に併任し、情報提供・連絡のための体制強化**を実施。
	各重要インフラ分野におけるCEPTOAR整備の推進	・2006年度末までに**各重要インフラ分野に CEPTOAR を整備** ・新規追加分野（水道、医療及び物流）については、CEPTOAR 整備に関する重要インフラ所管省庁及び重要インフラ事業者等間での**基本的合意**を2006年度末までに完了。	・7分野の重要インフラ分野において、2006年度末までに**整備を完了**。 ・新規追加3分野（医療、水道、物流）において、2007年度中のCEPTOAR整備に向けた**基本的合意**が完了。

	「CEPTOAR 特性把握マップ」とりまとめ	・各 CEPTOAR の**整備状況を把握** ・各分野の特徴把握が容易かつ可視性を工夫した**「CEPTOAR 特性把握マップ」**を2006年度末を目途に作成。	重要インフラ所管省庁等の協力を得て、2006 年度末現在の各 CEPTOAR（7 分野）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**としてとりまとめ。
	「重要インフラ連絡協議会「CEPTOAR-Council」（仮称）の創設促進	協議会設置に向けた**検討の場**の設置。	各重要インフラ分野が整備に向け検討中である CEPTOAR の代表者の参加を得て「CEPTOAR-Council」（仮称）の設置に向けた**検討の場**を重要インフラ所管省庁及び重要インフラ事業者等の協力を得て設置し開催。
③相互依存性解析の実施	相互依存性解析の試行的実施	・依存関係を可視化できる仕組み（**静的相互依存性解析**）を構築 ・**試行的に相互依存性解析**を実施。	各重要インフラ所管省庁の協力を得て、各重要インフラ分野の特性や状況等を配慮しつつ、依存関係を可視化できる仕組み（**静的相互依存性解析）の構築に向けた試行的な相互依存性解析を実施**。
④分野横断的な演習の実施	「研究的演習」の実施	・研究会を併用した演習（「**研究的演習**」）を実施。	演習実施の概念、演習課題の設定及び演習手法の理解等を主眼とし、各重要インフラ分野の特性や状況等を配慮しつつ、2006年7月から10月にかけて「**研究的演習**」を実施。
	「机上演習」 の実施	・議論発掘と具体課題整理のための「**机上演習**」を実施。	「研究的演習」を踏まえ、2007年2月に、重要インフラ分野と重要インフラ所管省庁などが参加して、**具体的なシナリオの下に会議形式で課題討議**を実施。
	各分野サイバー演習との連携	・分野ごとに実施された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、**連携に向けた検討を開始**。	分野ごと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、**知見の共有などの連携**。

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2006年度の取組み

1．2006年度の取組みの背景

(A) 企業

企業においては、我が国経済活動の重要な担い手であると同時に、ITの根幹を担う製品･サービス等を提供する主体でもあるという面からも情報セキュリティ対策を実施する必要がある。

もちろん、企業の対策の実施は、各企業の経営判断に基づいた自主的な取り組みが前提となるが、高度にネットワーク化されたIT社会においては、企業一社の事故によるトラブルが社会全体に波及する可能性があること及び多くの個人に関する情報等の集積度合いが高まっていることを考慮すると、企業は、自身の被害の局限化や法令遵守に留まらず、IT社会を構成する一員としての立場からも情報セキュリティ対策に取り組む責任があり、このことを認識した上で、より積極的に対策に取り組むことが必要である。

企業の取組みは、政府、重要インフラにおける製品･サービスの調達･外部委託等における取組み、その他多様な要因の影響を受ける可能性が高い（個人の取組みについても同様のことが言える）。また、企業の積極的な対策の実施が、個人の情報セキュリティに関する意識にも間接的に影響を及ぼすという循環を作ることも重要である。

かかる認識を背景として、企業領域においては、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にすることを目指しており、その対策初年度に当たる2006年度においては、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的に取り組んだ。

(B) 個人

個人においては、自身が被害者とならない限り、自らが情報セキュリティ対策を行わないことが、実は他人に迷惑を掛けているという認識が薄い状況にある。そのため、悪意がない場合でも社会的に大きな被害を発生させ

る可能性があり、当該個人に被害が発生するだけでなく、ネットワークでつな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ある。

そこで、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があり、一般的な安全に対する認識と同等の認識を情報セキュリティに対しても醸成し、個人の自己責任を明確に認識して行動することが期待されるが、他の対策実施領域に比べ、他の主体による支援が重要である。

かかる認識を背景として、個人領域においては、2009年度初めには、「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ており、その対策初年度に当たる2006年度においては、個人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的に取り組んだ。

2．2006年度の取組み

企業・個人に対しては、自ら自律的・継続的に情報セキュリティ対策を実施するようにすることを念頭に置きつつ、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

社会的責任にも配慮したコーポレートガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用することを推進するため、情報セキュリティ対策ベンチマーク等の普及活動、電気通信事業における情報セキュリティマネジメント指針策定等及び情報セキュリティ関連制度と内部統制制度との整合性確保のための検討を実施した。また、市場評価につながる環境整備の一つとして、政府調達において入札条件等として求めるべき情報セキュリティ対策レベルの評価に関し検討を実施したが、次年度以降の課題として残った。

(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

企業が情報セキュリティ対策を講ずる際、理解のしやすい形で必要な対策を選択出来る環境を整備するため、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関する調査研究及び第三者評価の活用促進のための各種普及活動等を実施した。また、質の高い情報セキュリティ関連製品に対する投資を加速するためのインセンティブとして、各種税制優遇措置の実施及びその普及啓発活動を実施した。

(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育成及び企業関係者の情報セキュリティへの理解を普及させるため、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、情報セキュリティに係る教育のための教材モデルの策定及び講師派遣等方策の検討、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の検討及び情報セキュリティセミナーにおけるコース数の拡充等を実施した。

(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

情報関連事業者等の自主的な協力を得ながら平時からの連絡体制を構築し、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連携対応体制を強化するため、オープンソースソフトウェア（ＯＳＳ）等の脆弱性に係る対応強化のための関連ガイドラインの改定及び有限責任中間法人JPCERTコーディネーションセンターとＯＳＳ開発者等との協力体制の構築及び発注者がウェブアプリケーション構築時に開発者（受注者）に対して示すべきセキュリティ要件に関する実用的なガイドラインの検討を実施した。

(B) 個人

(ア)情報セキュリティ教育の強化・推進

小中学校における情報セキュリティ教育の実施、教材・指導マニュアルの開発及び全国の小中高生を対象とした「情報セキュリティ標語」の募集により、初等中等教育からの情報セキュリティ教育を推進した。また、「インターネット安全教室」の全国的規模での開催とコンテンツの充実及びｅ－ネットキャラバンの全国規模での本格実施により、世代横断的な情報

セキュリティ教育を推進した。

(イ)広報啓発・情報発信の強化・推進

不正アクセス行為の発生状況及び不正アクセス対策等の公表、サイバー犯罪等からの被害防止のための啓発活動、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・情報発信活動を日常的に推進した。

また、「情報セキュリティの日」の創設とこれに伴う広報啓発的行事の開催、情報化月間における情報化促進貢献個人・企業等の表彰における「情報セキュリティ促進部門」の創設等、期間を区切った集中的な広報啓発・情報発信活動を推進した。

さらに、第1次情報セキュリティ基本計画等の英訳版のホームページへの掲載による海外への情報発信も行った。

(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

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、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のための検討の着手等、技術面からの取組みに着手した。また、無線ＬＡＮの利用に関するガイドラインのホームページへの掲載や「インターネット安全教室」において無線ＬＡＮの安全な使い方等を取り上げるなど、普及啓発活動の面からも環境整備を推進した。

第2節　2006年度の取組み及び取組みを受けた企業・個人における現状の評価等（2006年度の評価等）

1．2006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、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) 2006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。

なお、現時点では把握されていないが、政府機関等が中心となって把握していくことが望まれるデータについて、今後の課題として言及してい

るが、今後、このような関連データの把握に向けた努力が期待される。また、情報セキュリティ対策ベンチマークのような、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認識するように促す施策の進捗状況データ等については、サンプル調査ではないことから、現時点で状況把握に活用することは困難であるが、今後、こういったデータの有効活用に向けた検討が進められることも期待される。

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、等の留意点がある。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、2006年度については、基本計画の対象期間前である2005年度以前の資料しか得られない統計が散見されるところであり、十分な統計資料を収集できない。そこで、今回は次年度以降の評価等の基となる2005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、2006年度の状況については、統計資料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

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、内閣官房は各省庁の協力を得て必要な調査を行うこととする。ただし、2006年度評価等においては、必要な調査を実施する十分な時間的余裕がないため、データが得られた部分についてのみ、政府機関の状況との対比を実施することとする。

(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り組み結果を見るものとして活用できる。具体的には、第1次情報セキュリティ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7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。

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) 2007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2007年度以降においても、2006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、2007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統計が散見される事情は同じであるが、少なくとも2007年度については、第1次基本計画策定後の状況を示した2006年度の統計が得られることから、当該統計から2007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。

(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、SJ2006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[19]

(A) 企業

【総評】

SJ2006に盛り込まれた施策の実施状況調査の結果を見る限り、2006年度は、概ね当初の予定どおり、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の施策を推進することができた。但し、環境整備の有効な手段の一つである「入札条件等の見直し」については、内閣官房において慎重に検討を進めた結果、2006年度においては内閣官房内での検討の実施にとどまっており、次年度以降の課題として残った。

(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】

情報セキュリティ対策が市場評価につながった場合、市場メカニズムに基づき企業の情報セキュリティ対策が進展すると考えられる。

本項目に関する現状把握のデータは存在しないものの、関係省庁においては、SJ2006に基づく施策を実施してきたところであり、このうち、情報セキュリティ対策ベンチマークの普及については、2007年2月25日現在で利用件数が8,687件[20]であるなど、施策が浸透していることによると思われる結果が出ているものもある。

しかし、情報セキュリティ対策を実施した結果として、取引先・顧客からの評価や競争力強化につながったとの認識はほぼ皆無であったとの報告もあることに留意する必要がある[21]。

(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

---

19 なお、各項目毎の施策の具体的進捗状況については別添1、各指標の統計データについては別添8を参照。

20 「情報セキュリティ白書 2007年版」(情報セキュリティ検討会) 80頁参照

21 「グローバル情報セキュリティ戦略」(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(案)) 参照。

【指標】

○ ISMS[22]認証の取得事業者数（日本情報処理開発協会）

2005年度の1年間のISMS認証の取得事業者数は、720事業者であり、前年から急増している。

他方、2006年度のISMS認証の取得事業者数は、528事業者であり、この数値は前年度と比較すると減少しているが、2004年度（418事業者）及び2003年度（276事業者）と比較した場合、依然として高い水準にある。

○ ITセキュリティ評価及び認証制度[23]に基づく認証取得製品数（情報処理推進機構）

2005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は23件であった。同制度は2002年度から開始され、2004年度に認証取得製品数が急増したが、2005年度も前年と同水準で推移した。

他方、2006年4月から2007年2月までの認証取得製品数（新規）は36件であり、前年から更に増加する傾向にある。

【考察】

指標の推移を見る限り、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を促進する施策については、2005年度以前においても積極的に実施していたと考えられる。

2006年度においても、ISMS認証取得事業者数及び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。また、本施策の推進のため、各種普及活動を積極的に実施したほか、2006年10月にコモンクライテリア（CC）Ver. 3に基づくITセキュリティ評価及び認証制度を運用開始するなど質的側面からの取組みの強化、さらには税制優遇措置の実施が行われている。

これらのことを考えると、質の高い情報セキュリティ関連製品及びサ

---

22 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。

23 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。

ービスの提供を促進する施策は順調に進んでいると考えられる。

(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)

2005年度は、全国16ヶ所で情報セキュリティセミナーを実施した。これは、2004年度と同じであるが、過去の反響等を踏まえ、開催総数を約1.5倍とし、コースの種類も細分化している。

さらに、2006年度においては、情報セキュリティセミナーを全国30ヶ所において計84回実施しているが、これは2005年度のほぼ倍にあたる。また、開催コースについても、情報セキュリティ対策技術に関するコースを受講者のレベルに応じて細分化することにより、更なる内容の充実強化を図っている。

○ 情報セキュリティアドミニストレータ[24]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。ここ2年についてみると、受験者数、合格者数とも減少傾向にある。

【考察】

情報セキュリティセミナーを始めとする、情報セキュリティ人材の確保・育成のための研修事業については、これを積極的に推進しており、とりわけ情報セキュリティセミナーについては、2005年度以前においても前年までの開催結果を踏まえて開催回数の増加やコースの見直し等を行っていたところ、2006年度に入っても引き続き積極的な施策展開を行っていると言える。このことからも、企業の情報システム担当者等に対する全国規模での広報啓発のための施策は、順調に進められていると考えられる。

他方、情報セキュリティアドミニストレータ試験合格者数については、当該試験区分が創設された2001年以降増加傾向にあったが、2004年以降、減少に転じており、業種別では情報処理・提供サービス業の

[24] 「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。

減少が顕著である[25]。これは、情報セキュリティに関する資格が多様化していることが影響しているとも考えられるが、今後も引き続き、その動向を注視して行く必要がある。

(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チームである。

○ 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。

【考察】

施策の進捗状況及び指標の推移を見る限り、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ィルスや脆弱性等に早期に対応するための連携対応体制の構築が進んでいると考えられる。

(B) 個人

【総評】

SJ2006に盛り込まれた施策の実施状況調査の結果を見る限り、2006年度は、概ね当初の予定どおり、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の施策を推進することができた。

(ア) 情報セキュリティ教育の強化・推進

25 1,107名(2005年、受験者は8,717名)→563名(2006年、受験者は4,605名)

【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（学校における情報化の実態等に関する調査：文部科学省）

初等中等教育において、情報セキュリティ教育を含む情報教育の担い手である教員に対する研修を2005年度中に受講した教職員数は、458，763人であり、教員総数（876，715人）の52.3％を占める。研修形態としては、校内研修形式の研修を受講した者が多い（409，393人。なお、上記注参照。）。

○ 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について、2005年度の参加者は5，844名（来賓等を除いた参加者は5，073名）で、前年度（3，581名）と比較して2，263名増加した。

また、2006年度は、コンテンツを充実させるとともに、全国98か所で開催した。

○ 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 e-ネットキャラバンは、まず、2005年11月から2006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。

そして、試行実施の結果を受け、2006年4月から全国規模での本格実施を開始、2007年3月31日までに計453件の講座を開催し、約49，000名が受講した。

【考察】

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の実施については、毎年ほぼ半数の教員が受講しており、単純に計算すると2年に1度は研修を受講していることになる。その多くは校内研修による受講であることを考えると、校内研修の充実が初等中等教育における情報セキュリティ教育強化・推進の鍵になるものと考えられる。

なお、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、教員向け研修の充実方策とも考えることが出来る。2006年から本格実施をしているが、まずは順調な滑り出しで捉えることが可能であると思料されるところ、今後の動向に注目したい。

他方、幅広い世代を対象とする情報セキュリティ教育として、インターネット安全教室が挙げられる。2005年以前においても着実な推進が見られたところであるが、2006年度も引き続き、質量共に充実が図られた。

(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）

2006年度若しくは2006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519,184人（2006年）、警察庁の「サイバー犯罪対策」のページが275,245人（2006年度）、「@police」が1,994,054人（2006年）、総務省の「国民のための情報セキュリティサイト」が359,258件（2006年度）、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150,032人（2006年度）、「CHECKPC！キャンペーンホームページ」が798,155件（2007年1月～3月）、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18,969,754件（2006年度）であった[26]。

○ 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）

※ 今年度の報告書案を作成する時点では、担当省において調査結果を精査中。

○ 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、ソフトメーカーやパソコンメーカーのウェブサイトからが、それぞれ4割台を数えている。以下、家族や知

26 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。

人、ポータルサイトのニュース等、IT関連のウェブサイト等及びテレビ・新聞等が、それぞれ2割前後で推移している。

なお、世代別に見ると10代、職業別に見ると主婦・アルバイト・学生層において、情報を入手していないと回答している割合が高い。

2006年についても、ほぼこの傾向で推移しており、情報の入手経路として、「ウェブページ（解説やニュース）」が約7割、CMやニュース等が約3割前後で続いている。また、今後希望する情報提供方法についても、ウェブを活用するものが約4割強、メールマガジンが約3割、CM等テレビによるものが約2割5分前後である。

○ 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）

今後希望する情報提供方法は、ウェブ活用が約5割、メールマガジンが約3割5分前後、CM等テレビによるものが約2割5分前後である。

【考察】

広報啓発・情報発信は、個人を対象とする施策の中心に位置づけられるものであり、SJ2006に基づいて多くの施策が積極的に進められた。その方法はウェブを中心とし、テレビも積極的に活用したが、「情報の入手経路」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かったという調査結果を考慮すると、これらの活動は一定の効果があったと思われる。

また、希望する情報提供方法についても、情報の入手経路同様、やはりウェブ系が中心になっているが、テレビを希望する者が一定の数を占める。特に、情報を入手していないと回答している割合が高かった世代及び職業層において、テレビを経由した情報入手を希望する割合が比較的高い。

以上の結果を踏まえると、今後も引き続きウェブ及びテレビを中心とした広報啓発・情報発信が有用であると思料されるが、特に情報を入手していないと回答している割合が高かった世代において、テレビを経由して情報入手している割合が比較的高い。全体的な底上げの観点からは、これらの世代への対策が重要であること、テレビというのはウェブに比べ無意識的に情報収集出来るという特性があることを考慮すると、テレビを活用することの重要性は、依然として高い。

(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

【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）

※ 今年度の報告書案を作成する時点では、担当省において調査結果を精査中。

【考察】

進捗状況調査等の結果を見る限り、情報関連事業者が情報関連製品・サービスを開発・供給する環境の整備は着実に進められている。このうち、無線ＬＡＮのセキュリティに関する問題については、セキュリティ対策の必要性が周知されているというデータも存在する。他方、ボット対策の実施状況等に係る指標は、現時点で存在しないため、引き続き、指標追加の可能性を検討する必要がある。

なお、個人における取組みを促進する観点からは、負担感なく利用できる製品やサービスを開発・供給する環境の整備を促進することも重要である。不断の努力と進歩が見られるところではあるが、長期的な課題として留意しておくことが必要である。

(2) 施策の取組みによる社会的変化に関する評価等[27]

(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）

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）の重要性の認識について、非常に重要と考える企業の割合は、２００５年調査で７１．

[27] 各指標の統計データについては別添8を参照。

0%となっている。これは、2004年度の68．4%から微増となっている。

【考察】

この数値は、2004年度に調査した結果であるが、調査結果を見る限り、全体の意識レベルは、比較的高い状況にあると考えられる。しかし、調査対象範囲[28]を考慮すると、零細企業については実態がわからない。

また、最新の報告[29]によれば、企業全体の情報セキュリティ対策レベルは向上しつつあるものの、コストがかかることや外部から評価されないことなどから、その取組みには差があり、先進的な企業とそうでない企業、大企業と中小企業の間での格差が広がりつつあるとのことである。

社会全体の底上げの観点からは、情報セキュリティ対策への取組みが遅れている企業に注目することが不可欠であり、これを対象とする施策を実施する必要があると考えられる。

(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、30．6%の企業が既にリスク分析を実施し（2004年度は20．4%）、43．9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（2004年度は29．7%）、47．1%の企業が、既にセキュリティ管理者を配置している（2004年度は35．2%）。

他方、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8．7%（2004年度は11．

---

[28] 本調査の調査対象範囲は、日本標準産業分類に基づく全27業種、資本金3，000万円以上及び総従業者50人以上の民間事業者9，500事業者である。つまり、資本金及び総従業者がそれに満たない事業者は含まれていない。

[29] 「グローバル情報セキュリティ戦略」（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（案））参照。

1%)、情報セキュリティポリシーの策定が6．6%（2004年度は8．9%)、セキュリティ管理者の配置が5．7%（2004年度は7．3%)であった。

[考察]

2004年度までの調査結果であるが、SJ2006の策定前の時点においても、セキュリティ対策が徐々に進んでいることがわかる。

しかし、その効果について調査したところ、いずれの項目についても、実施している又は実施を検討している企業の1割前後が「あまり効果がない」と回答し、2割前後が「よくわからない」と回答している。情報セキュリティ対策の更なる導入と定着を進めて行くためには、導入者においてその効果が認識されるような環境整備を推進していくことが必要であると考える。

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、57．5パーセントの企業が既に重要なシステムへの内部でのアクセス管理を実施し（2004年度は50．7%)、27．6%の企業が既にデータの暗号化（PKIを含む）を実施し（2004年度は調査未実施)、72．4%の企業が、既に外部接続へのファイアーウォールを配置し（2004年度は66．7%)、47．0%の企業が既にセキュリティ監視ソフトを導入している（2004年度は40．6%)。

他方、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6．9%（2004年度は8．2%)、データの暗号化（PKIを含む）の実施が2005年度の時点で15．2%（2004年度は調査未実施)、外部接続へのファイアーウォールの配置が2005年度の時点で6．4%（2004年度は7．7%)、セキュリティ監視ソフトの導入が2005年度の時点で7．6%である（2004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）**

2005年度の時点で、80．5%の企業が「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し、64．3%の企業がサーバにウィルスチェックプログラムを導入し、44．6パーセントの企業がID・パスワードによるアクセス制御を実施し、46．8%の企業がファイアウォールを設置している。データやネットワークの暗号化を実施している企業は、10．7%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）**

2005年度の時点で、45．9%の企業等が、情報セキュリティ教育を実施している（2004年度は35．5%）。

他方、必要性を感じていない企業等の割合は、2005年度の時点で1．2パーセントである（2004年度は2．2%）[30]。

○ **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、40．1%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27．2%）。

他方、必要性を感じていない企業の割合は、2005年度の時点で4．6%である（2004年度は5．6%）。

○ **パッチ[31]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）**

2005年度の時点で、32%の企業が常に最新状態にしており（2004年度は31．2%）、32．2%の企業がパッチの適用を定期的に実施している（同25．2%）。

他方、時々しか実施していない企業は20%（同18．2%）、稀に又は全く実施していない企業は12．2%（同9．5%）、把握し

30 なお、本調査の対象は、全国の企業（東証一部、二部上場企業、店頭公開企業を対象）、情報通信関連（電気通信事業者を対象）、医療関連（病床数100床以上の病院を対象）、教育関連（国立・私立大学（短大を含む）を対象）、行政サービス機関（都道府県、特別区、政令指定都市、市町村を対象）から偏りのないよう2,500件を無作為に抽出したものである。

31 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）」

ていない企業が2．4％（同13．3％）であった。

○　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）

2005年度の時点で、所有するパソコンの9割以上にウィルス対策ソフトを導入している企業は86．4％であった（2004年度は73．8％）。

他方、半数以上と回答した企業は4．9％（同7．2％）、半数未満が5．5％（同10．9％）、導入していない企業は2．4％（同7．1％）であった。

【考察】

いずれも2005年度以前の調査結果であるが、SJ2006の策定前の時点においても、セキュリティ対策が徐々に進んでいることがわかる。

しかし、その効果について調査結果を見ると、情報セキュリティ対策について、調査を実施したいずれの項目についても、その対策を実施している又は実施を検討している企業の1割から2割がその効果について「よくわからない」と回答している。また、企業における情報セキュリティ教育については、1割強が「あまり効果がない」と回答し、2割弱が「よくわからない」と回答している。情報セキュリティ対策の更なる導入と定着を進めて行くためには、導入者においてその効果が認識されるような環境整備を推進していくことが必要であると考える。

また、パッチの適用については、3割が最新、3割が定期的更新、2割が時々、1割がほとんど実施せず、という傾向で推移しているが、パッチを適用しない場合、ＯＳの脆弱性を利用した攻撃を許してしまうという問題があるため、セキュリティの観点からは、常に最新の状態であることが望ましい。その観点からは、定期的に更新する場合でも、可及的速やかに最新のパッチがあてられているような状況にする必要があるが、まずは「時々」以下の割合の増減について、注視することが必要である。

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）

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

【考察】

以上に示した数値は、2004年度までの調査結果であり、今後の数値の推移に注視する必要がある。

なお、本項目についても、その効果について調査したところ、2割弱が「よくわからない」と回答している。情報セキュリティ対策の更なる導入と定着を進めて行くためには、導入者においてその効果が認識されるような環境整備を推進していくことが必要であると考える。

（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）

2005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、「個人情報の保護に不安がある」が44．2％、「ウィルスの感染が心配である」が34．6％、「電子的決裁の信頼性に不安がある」が26．2％、「違法・有害情報が氾濫している」が20．8％である。また、これらは前年と比較し、ほぼ横ばいの数値である。

他方、「特に不満は感じていない」と回答したのは、11．5％である。

○ 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）

※ 今年度の報告書案を作成する時点では、担当省において調査結果を精査中。

○ 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）

2005年度の時点で、「ウィルス感染」という言葉を聞いたことある者は調査対象の98．7％、スパムメールが82．3％、スパイウェアが78．9％である。他方、ボットは12．8％、ファーミングは10．4％であった（2005年度から調査を実施）。また、2006年度の調査では、2005年度の調査と集計方法等で違いが存在するため単純に比較することは出来ないが、統計の数値を見る限り、2005年度と同じ傾向が見て取れた。

○ 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対して負担に感じること及び対策を実施しない理由として、2005年度においては、「費用がかかる」が59．2％と最も高く、「手間がかかる」が40．2％で続いた。また、男女別に見ると、「対策方法がわからない」という意見が、女性や利用歴の浅い者で目立った。また、2006年度の調査では、2005年度の調査と集計方法等で違いが存在するため単純に比較することは出来ないが、統計の数値を見る限り、2005年度と同じ傾向が見て取れた。

（2005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を見る指標について、効果があったと言うためには、認知度が全体的に向上し、不満や不安等のネガティブな意識が低下すればよいと考える。

この考え方に基づいて分析を実施すると、インターネットに対する不満や不安について、2005年度は前年と比較し、全体としては横ばいに近い状況である。また、情報セキュリティに関する言葉の認知度については、既に報道で多く取り上げられている言葉の認知度は高く、最近問題になり出したものは低い。なお、男女別・世代別に見ると、一般的には男性のほうが認知度が高い。他方、情報セキュリティ対策に関する意識については、費用や手間がかかるという意識が根強い一方で、女性やインターネット経験が浅い者を中心に、対策方法等がわからない、わかりにくいという意見も目立つ。

以上の結果に着目すると、属性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。

⑷ 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）

何らかのウィ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57．0％である（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）

※ 今年度の報告書案を作成する時点では、担当省において調査結果を精査中。

○ 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）

2004年度の調査によれば、パッチをあてている者が77．3％（うち、本人で実施は67．4％）、セキュリティ対策ソフトの導入が79．7％（うち、本人で実施は57．8％）、怪しい電子メール・添付ファイルの削除が88．6％（うち、本人で実施は76．1％）と高率である。他方、パスワードの定期的な変更は、実施している者（42．6％）と実施していない者（42．3％）が拮抗している状況である。

【考察】

個人の情報セキュリティ対策の状況を見る指標は、調査対象者中で情報セキュリティ対策を実施している者の割合を調査したものであり、この率が高いほど対策を実施していると評価することが可能である。

総務省・通信利用動向調査によれば、インターネットのウィルスや不正アクセスに対し何らかの対応を行っている者の割合は、2005年末において57．0％であり、前年までと比較して横ばいの状況である。

他方、男女別・職種別に結果を公表している情報処理推進機構の調査結果では、全般的な傾向として、女性は男性と比べ、家族や友人にセキュリティ対策の実施を任せる割合が高く、また、10代の利用者は対策について「わからない」と回答する割合が、他の世代より高かったが、このことは、意識面同様、属性に応じた各種普及啓発の重要性を示しているものと考えられる。

今後、SJ2006に基づく施策の効果が統計上現れてくることになるが、情報処理推進機構の調査結果は、意識面同様、属性に応じた各種普及啓発の重要性を示している。

(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)

2004年度において、84.4%の企業がコンピュータウィルス関係のトラブルを経験した (2003年度は90.1%)。また、39.7%の企業がシステムトラブル関係のトラブルを経験した (2003年度は40.4%)

○ 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)

2005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40.2%であった (2004年は56.9%)。

○ 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)

2005年において、32.8%の企業等がウィルス等の感染を経験した (2004年は45.5%)。また、8.3%の企業等がノートPCの盗難を (同12.3%)、同じく8.3%の企業等がスパイウェアの感染を (2004年度まで調査項目なし) 経験した[32]。

○ 不正アクセス行為の発生状況 (警察庁)

2005年中の不正アクセス行為の認知件数は592件であり、前年と比べ、236件増加した (2004年は356件)。

---

32 なお、本調査の対象は、全国の企業 (東証一部、二部上場企業、店頭公開企業を対象)、情報通信関連 (電気通信事業者を対象)、医療関連 (病床数100床以上の病院を対象)、教育関連 (国立・私立大学 (短大を含む) を対象)、行政サービス機関 (都道府県、特別区、政令指定都市、市町村を対象) から偏りのないよう2,500件を無作為に抽出したものである。

○ 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）

2005年の届出件数は、コンピュータウィルスが54，174件（2004年は52，151件）、不正アクセスが515件（2004年は594件）、脆弱性に関する情報が401件（2004年は172件、但し、同年7月から制度開始）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）

2005年中において、パソコンでインターネットを利用した際にセキュリティ関連の被害に遭遇したことがあると回答した者は37．2％であった。なお、性別では男性の方が41％でやや多く、世代別では、大きな差は見られない。

○ コンピュータウィルス遭遇率（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）

2005年において、69．8％の企業がコンピュータウィルスに遭遇（感染又は発見）した（2004年は69．1％）。

○ 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）

2005年において、31．4％の企業がスパイウェアに遭遇（実行又は発見）した（2005年から調査を開始したため、2004年以前の数値は存在しない。）。

[考察]

インシデント又は犯罪の被害については、各省庁及び関連団体から様々な調査結果が出ているが、共通する問題点として、被害を受けても気付かない者は被害を申告しないため、全体の正確な割合がわからないということがある。そのため、各調査結果を見るに際しては、このことに留意する必要がある。

企業分野における被害については、減少傾向を示す調査回答が見られる。このことは、施策実施前の時点において、企業では既に情報セキュリティ対策の重要性を認識し、所要の対策を行ってきた結果であるとも考えられる。但し、企業を対象とした調査の中には、調査回答率が低いものも存在するが、このことは、相当数の暗数の存在を推

知させる。

個人分野における被害については、総務省の調査によると、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、減少する傾向にある。また、情報処理推進機構では、男女別及び年代別の調査を実施しているが、これによると、女性より男性の方が被害に遭った割合が高かったものの、世代間の差は大きく見られない。

(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)

我が国の企業間における電子商取引について見ると、インターネットによる商取引の市場規模は140兆円 (米国は92兆円)、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224兆円である (米国は189兆円)。これを電子商取引化率で見ると、前者が12.9% (米国は5.7%)、後者が20.6% (米国は11.9%) 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3.5兆円であり (米国は15.9兆円)、電子商取引化率は1.2% (米国は2.4%) である。

【考察】

我が国における電子商取引市場規模を米国と比較してみると、企業間については米国に先行しているものの、消費者向けについては米国の後塵を拝している状況にあることが明らかになった。個人分野では、依然として新たなリスクが発生しているなどの事情が情報セキュリティ上の不安を招いており、そのことが電子商取引の浸透を阻害しているのではないかと考えられる。

このような状況を踏まえると、IT やセキュリティに関する意識の向上や、不安の払拭が喫緊の課題となっている。

(3) 総評

今回は、基本計画（2006年2月）及びSJ2006（2006年6月）以降の取組みの成果を表す統計が取れなかった項目も散見され、取組み以前の現状の分析にのみ指標を活用したという項目も存在した。
全般的な傾向としては、以下のとおりである。

(A) 企業

企業については、2005年以前から情報セキュリティに対する取組みを着実に行っており、2006年についても、その取組みを強化しつつ実施していたことが、施策の進捗状況調査及び指標から見てとれる。また、指標から直接明らかではないが、ウィルス対策ソフト等を使用している割合の向上は、情報セキュリティに対する投資額が増大していることを推知させる。これは、各省庁による普及啓発活動の効果のほか、個人情報保護法の施行（2005年4月）や金融商品取引法の成立（2006年6月）などを背景として、情報セキュリティ確保のための体制整備や事業継続計画の策定などの必要性を企業が認識したことで、企業の情報セキュリティに対する意識が向上したと言えることも影響していると推察される。個人情報を流出させた企業に対する損害賠償責任を認める判決[33]も出ており、これらがもたらす効果として、「企業」総体としては、企業の情報セキュリティ意識は引き続き維持され、対策が進展することが期待される。

しかし、企業の情報セキュリティ対策については、総体的には進展しつつあるものの、依然として情報流出が続いているのも事実である。また、

○ ウィルス対策ソフトやファイアウォールの導入等の技術面での基本的対策は進んだ反面、情報セキュリティ監査や外部からの常時監視といった高度な対策については、必ずしも十分と言えるほどの対策が取られている状況にはない。

○ すべての企業において適切な対策が講じられているとは言いがたい状況にある。特に、先進的な企業とそうでない企業の間に格差が存在し、さらに、大企業と比較して中小企業においては取組みの遅れが存在し、それが拡大する傾向にある。

[33] 東京地判平成19年（2007年）2月8日

と考察する報告もある[34]。

(B) 個人

個人についても、2005年以前から情報セキュリティに対する取り組みを着実に行っており、2006年についても、その取組みを強化しつつ実施していたことが、施策の進捗状況調査及び指標から見てとれる。ウィルス対策ソフトの売れ行きも堅調であるなどの事情も考慮すると、情報セキュリティに関する意識及び知識も浸透しつつあると思われる。

しかし、全般的には着実に進展しつつあるものの、依然として対策を講じていないとする個人が一定数存在し（以下「未着手層」とする。）、また、年代別・男女別・職業別に調査結果を見ると、特定の属性について、情報セキュリティに対する理解度等が低い。全般的な対策もさることながら、属性に応じた情報セキュリティ対策を検討することが必要になると思われる。

また、個人を標的とする情報セキュリティに関するリスクは、個人が対策を強化することに対抗するかの如く、フィッシングやボットといった新しいリスクを発生させており、また、携帯電話によるネット利用やSNS[35]の普及に伴う新たなリスク発生の可能性も考えられる。

第3節 2007年度に向けた課題

(A) 企業

企業分野においては、既に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。

2007年度は、「取組みが遅れがちな主体への対策」が重要になるが、企業分野においては、

○ 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

---

34 「グローバル情報セキュリティ戦略」（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（案））参照。

35 SNS（Social Networking Service）とは、インターネット上で友人を紹介しあって、個人間の交流を支援するサービス（サイト）。誰でも参加できるものと、友人からの紹介がないと参加できないものがある。（総務省「2006年 情報通信に関する現状報告」）

の実施が重要になる。

(B) 個人

個人分野においては、未着手層の存在と特定の属性に属する者の理解度等の低さが、全体的な底上げに際しての阻害要因となっている。

2007年度は、「取組みが遅れがちな主体への対策」が重要になるが、個人分野においては、

○ 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分野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　2006年度の取組み

1．2006年度の取組みの背景

「ITを安心して利用可能な環境」を実現するためには、情報セキュリティ技術の高度化と、その技術を理解した上での利用・活用が不可欠である。しかし、

1）急速に拡大するIT利用・活用に、情報セキュリティ技術の開発が対応できていない
2）既存の情報セキュリティ技術の限界を補完する組織・人間系の管理手法とのバランスを欠いている

という問題が存在していた。これを解決するためには、

1）そもそもの情報セキュリティ技術の高度化
2）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の組織・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った。

2．2006年度の取組み

研究開発・技術開発の実施状況を把握するための検討並びにその研究開発・技術開発の投資効果の評価についての検討を実施するとともに、政府調達における成果利用の方策について検討を行なった。

また、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検討並びに萌芽的研究開発への投資強化に向けた検討を行うとともに、各種の研究開発・技術開発等を推進した。

加えて、長期的な視野で抜本的な技術革新等の実現を目指す「グランドチャレンジ型」の研究開発・技術開発への取組みとして、その「グランドチャレンジ型」に相応しいテーマ検討の場の設置について検討を進めた。

第2節 2006年度の取組み及び取組みを受けた現状の評価等（2006年度の評価等）

1．2006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。

2006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初年度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) 2006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」[36]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) 2007年度以降の評価等について評価等

2007年度以降についても、基本的には2006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

36 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。

(1) 施策の取組み結果に関する評価等

SJ2006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、20の施策のうち、Cの施策はなかったものの、Aの施策が15、Bの施策が5と、一部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問題となる施策が存在していることも事実である。

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、2006年10月より再開した技術戦略専門委員会において、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、「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)が開始されるなど、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、具体的な検討の開始には至らなかったものの、技術戦略専門委員会の中で、継続的にグランドチャレンジに相応しいテーマを検討する場の設置について審議が進められた。

(2) 施策の取組みによる社会的変化に関する評価等

情報セキュリティ確保の抜本的対策が求められる中、セキュアOSやセキュリティを意識した言語処理系の実現など、中長期課題への取組みが実施されている。例えば、ITの信頼性確保のための喫緊な取組みとして「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)が推進されたが、我が国におけるOS開発能力を有する人材育成をも視野にした本取組みの推進には、産業界、学界の関心も高く、本取組みをバックアップする産学連携コンソーシアムが設立されるなど、産学官を挙げて情報セキュリティ技術の高度化を図る機運が醸成された。

また、コンピュータウィ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。

2007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

SJ2006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、セキュアOS等への取組みによりIT基盤技術の強化を目指すコンソーシアムが新たに設立されるなど、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や、「「グランドチャレンジ型」研究開発・技術開発の推進」など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。

第1次情報セキュリティ基本計画に基づく取組みの2年目に当たる2007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 2007年度に向けた課題

2007年度に向けては、2006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、2006年度に着手、実施した研究開発・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、具体的なテーマ検討のプロセスを開始するなど、その取組みを着実に進めることが重要な課題となっている。

【情報セキュリティ人材の育成・確保】

第1節　2006年度の取組み

1．2006年度の取組みの背景

「ITを安心して利用可能な環境」を実現するためには、対策実施主体における情報セキュリティ対策の運用や、情報セキュリティに関する高度な研究開発・技術開発を支える人材の育成・確保が不可欠であるにもかかわらず、情報セキュリティに係る人材の育成が十分に行われているとは言い難い状況であった。また、情報セキュリティに係る人材のキャリアパスを検討する上で、最高情報セキュリティ責任者（CISO）、各組織の情報システムの運用担当者等のそれぞれに応じた適切なスキルや、これらのスキルに相当する各種の資格制度との関係が必ずしも明らかではなかった。

このため、関係省庁において、情報セキュリティ人材の育成のために早期に実施できる施策について着実に実施するとともに、情報セキュリティに関する資格制度の体系化も含めた情報セキュリティ人材の育成方策について総合的に整理することが必要であった。

2．2006年度の取組み

情報セキュリティ人材の育成のために早期に実施できる施策として、産学連携による高度IT人材育成プログラムを開発・実施する教育拠点として6大学が選定され、プログラムの開発等が進められたほか、2つの地方拠点（大垣、神戸）において「情報通信セキュリティ人材育成センター」が開設されるなどセキュリティ人材の育成拠点の展開が進むとともに、大学等において情報セキュリティ教育を行う際の教材モデルや組織における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も策定された。

また、情報セキュリティ政策会議の下に「人材育成・資格制度体系化専門委員会」が設置され、資格制度も含めた多様な情報セキュリティに関する各種教育プログラムの体系図が整理されたほか、我が国の情報セキュリティ人材の育成に関する総合的な検討が行われた。

第2節　2006年度の取組み及び取組みを受けた現状の評価等（2006年度の評価等）

1．2006年度の評価等に関する基本的考え方（評価等の視点）

2006年度においては、情報セキュリティに係る人材に求められる適切なスキル等についても明らかにされていない状況の中で、関係省庁が早期に実施できる施策や人材育成方策に関する総合的な整理が主たる取組みとならざるを得なかった。こうした前提の下、2006年度の評価等の視点としては、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整備が図られたかという視点、さらには、情報セキュリティ人材のスキルが明らかにされたか、こうしたスキルの習得に資する資格制度の体系化が行われたか、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) 2006年度の評価等について

情報セキュリティ人材の育成・確保に関しては、人材育成・資格制度体系化専門委員会において、我が国全体の情報セキュリティ対策を考える上で関係する様々なカテゴリの人材の現状と課題について外部の有識者委員により定性的な分析がなされたほか、特に情報セキュリティ対策を実施する機関である政府機関、企業についても、政府機関に対する実態調査及び日本経団連を通じたアンケート調査が実施され、一定の定量的な分析も実施されたところである。このため、情報セキュリティ人材の育成・確保に関する2006年度における評価等においては、これらの定性的・定量的な分析の結果を活用することが適当である。

(2) 2007年度以降の評価等について

情報セキュリティ人材の育成・確保に関する2006年度における評価等においては、人材育成・資格制度体系化専門委員会における一定の定性的・定量的分析の結果の活用が図られるところである。しかしながら、これらの分析結果についても、人材の不足感などが推測されるにとどまり、実際に不足している人材の具体的な数字までは現れていない。

このため、2007年度以降の評価等においては、人材の育成に関して実施すべき施策を検討するために必要となる人材の質や量について具体的に明らかにするため、例えば政府機関における人材や資格制度等の各種

教育プログラムの受講者数といった一定の指標を設定し、把握することも視野に入れていくべきと考えられる。

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

SJ2006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。掲げられた4施策全てがAとなっており、予定していた取組みは全て着実に実施された。

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」や総務省の「情報通信セキュリティ人材育成センター開設事業」に基づき、各種教育拠点の整備が図られるとともに経済産業省において教育用の教材モデルや組織におけるIT利用者向けのセルフチェックツールも策定され、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整備に一定の成果が見られるところである。

また、情報セキュリティ政策会議の下に「人材育成・資格制度体系化専門委員会」が設置され、2007年1月に報告書がとりまとめられた。本報告書は、我が国の情報セキュリティに係る人材について包括的に分析を行っており、関係者が現状についての共通認識を共有するとともに、2007年度以降、早期に取り組むべき事項について提言を行ったという意味で、意義のある報告書であったと評価される。

(2) 施策の取組みによる社会的変化に関する評価等

人材育成・資格制度体系化専門委員会が開催され、情報セキュリティ人材の育成の必要性についての認識が高まる中、文部科学省が2006年度まではソフトウェア技術者等を中心としたIT人材育成に力点を置いていた「先導的ITスペシャリスト育成推進プログラム」について、2007年度からは情報セキュリティ人材にも拡充されるなど政策面での手当てがなされた。また、情報セキュリティ資格を運営する各種団体においても、それぞれが個別に自らが運営する資格のPRに務めるだけでなく、複数の団体が連携・協同して、一般的な情報セキュリティスキルの確保の必要性について理解を深めるためのセミナーを開催するなどの動きが見られ、官民双方に、情報セキュリティ人材の育成拡大に向けた動きが見られるところである。

また、大手ベンダー各社において情報システム障害に対応するための若手プログラマの社内研修の充実が図られている、人材派遣業界においてIT人材の派遣単価が上昇しているといった動向も報じられており、製品等の供給サイドにおいても情報セキュリティを確保するための人材を積極的に育成・確保しようという動きが市場動向として見られるところである。

(3) 総評

情報セキュリティ人材の育成・確保については、当初予定していた施策が着実に実施され、人材の育成に資する教育拠点やツールなどの整備が図られるとともに、今後の情報セキュリティ人材の育成方策を検討する上でベースとなるべき人材のスキルやこれに相応する各種教育プログラムの体系図も整理され、一定の成果を上げたことができると考えられる。また、上記(2)のとおり、こうした取組みと機を一にするように、情報セキュリティ人材の育成に向けた官民における積極的な取組みの展開が図られつつあるところである。

このように、2006年度における評価等の視点に立った場合にはそれなりの成果が認められるものの、人材育成・資格制度体系化専門委員会の報告書によれば、どの領域においても人材及びそのスキルの不足感は否めず、我が国全体の情報セキュリティ対策の向上という観点から必要十分な人材の育成・確保という視点で見た場合には、到底十分とは言えないと考えられる。

第3節 2007年度に向けた課題

我が国における情報セキュリティに係る人材の育成・確保については、到底十分とは言えないと考えられる中、2007年度においては、人材育成・資格制度体系化専門委員会の報告書における各種提言に基づく施策を着実に実施していくことが必要となる。

とりわけ、基本計画において他の模範となるべきとされている政府機関においては人材の質・量ともに不足していると考えられ、早急な対応が求められる。また、先進的な技術の研究・開発を行う者や、セキュリティ対策を実施する企業や製品等を供給する民間部門における人材についても、民間の取組みを支援するような各種取組みが必要となる。

【国際連携・協調】

第1節　2006年度の取組み

1．2006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。

2．2006年度の取組み

国際連携・協調が必要であるという認識の一方で、我が国がここ数年急速に整備してきた情報セキュリティ政策に係る戦略や体制は、未だ諸外国に広く認識されているとは言い難い現状があった。そのため、主に多国間の枠組みにおける国際連携を念頭に、G8やOECD、FIRST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、ベストプラクティスの国際的な発信・普及に努めるとともに、国際的な標準開発への貢献に資する取組みが行われた。

第2節　2006年度の取組み及び取組みを受けた現状の評価等（2006年度の評価等）

1．2006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、2006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) 2006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」[37]していくこととしている。このことも踏まえ、2006年度は特段指標の設定は行わない。

(2) 2007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。

また、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については、例えば我が国の情報セキュリティ政策に係る体制や戦略を引用している海外の媒体記事を数える方法が考えられる。

3．評価等の結果と総評

37 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。

(1) 施策の取組み結果に関する評価等

SJ2006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の通りであり、全9施策のうち、Aが6施策、A'が3施策と、概ね順調に推移している。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、「情報セキュリティ基本計画」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、「ベストプラクティス」の発信が試み始められているなど、国際社会におけるセキュリティ文化の実現にもある程度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。国内では、政府機関や民間企業、一般国民を含めて情報漏えい問題が報道される機会が多く、これに伴い各主体の情報セキュリティに関する適切な役割分担や連携・協調、意識向上の必要性について認識が高まった。

国際連携・協調についても、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、引き続き関係者との信頼関係の醸成や、我が国からの情報発信内容の具体化・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、ウェブサイトを通した広報活動により、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、一部の取組みが始められたものの、我が国の経験・知見から世界に貢献できる具体的な内容が明確でないなど、未だ不十分な部分があると考えられる。

第3節　２００７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留まらないこと、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・協調にあたっては、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、十分な成果をあ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歩段階に留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、情報セキュリティ基本計画では基本理念が述べられていたものの、具体化の遅れていた企業活動の国際化に伴う情報セキュリティ対策や、国際的に連携すべき具体的な事項や相手、我が国の経験・知見から世界に貢献できる要素の具体化・明確化等を含み、「世界における日本、日本にとっての世界」という双方向の観点を持った、我が国の情報セキュリティ政策に関して基礎となる国際戦略を策定する必要がある。

【犯罪の取締り及び権利利益保護・救済】

第1節　2006年度の取組み

1．2006年度の取組みの背景

「ITを安心して利用可能な環境」を実現するためには、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。しかしながら、インターネットを始めとするITの普及と比例して、サイバー空間における犯罪の件数は急激に増加する傾向にあり、たとえば、2005年のサイバー犯罪等に関する相談受理件数は前年に比べて約20％増加し、サイバー空間の中での行為が外での行為に比べて捕捉しにくく、まだ犯罪取締りや権利利益の保護や救済が実態に十分に追いついていないという状況にあった。

このため、犯罪や権利利益の侵害に対処するための官民における情報セキュリティ対策の体制の構築を図ることが必要であった。

2．2006年度の取組み

サイバー犯罪の取締りの基盤の構築のため、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、捜査体制の強化・整備、捜索現場での活用や検証のための装備資機材の強化・整備、犯罪取締りに係る法制度の整備の推進、外国機関との国際連携の推進等を行った。

また、サイバー空間における権利利益の保護・救済のため、その基盤に係る実態の調査を行った。

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、基礎技術の開発や対策の共同研究を行った。

第2節　2006年度の取組み及び取組みを受けた現状の評価等（2006年度の評価等）

1．2006年度の評価等に関する基本的考え方（評価等の視点）

犯罪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野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、2006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初年度であったことを踏まえ、サイバー空間において次々に発生する様々な犯罪や不法行為に対して、能力や体制の構築や法制度の整備ができ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) 2006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」[38]していくこととしている。このことも踏まえ、2006年度は特段指標の設定は行わない。

(2) 2007年度以降について

2007年度以降についても、基本的には2006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

SJ2006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10施策のうち、Aが8施策、Bが2施策と、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、都道府県警察が行うサイバー犯罪捜査に関する指導・調整能力の向上を図るための警察庁の体制強化、警察職員に対する各種研修の実施、装備資機材の整備、外国関係機関との連携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が行われた。一方、国会

38 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。

での審議が進まないという理由によって、サイバー犯罪に適切に対処するための法整備等、進捗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、安全なネットワーク利用やサービス提供を実現するための基礎技術の開発等が実施された。

(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、サイバー犯罪捜査に精通した警察職員が増加し、全国で行われているサイバー犯罪捜査への指導・調整や外国捜査機関との国際連携が強化され、都道府県への現場用の装備資機材の整備が進んだほか、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たわけではないものの、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実現に向けて進んでいる、と言える。

(3) 総評

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様々な犯罪や不法行為に対して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が進みリスクを減少又は解消させることについては、未だ技術開発自体が途中であるため、努力を継続し、加速化していく余地がある。

第3節 2007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おり、このままでは、インターネット上の犯罪等への不安はさらに増加していく、つまり、施策の取組み以上にリスクが増加する可能性もある。たとえば、2006年においては、サイバー犯罪の主な類型である、不正アクセス行為の認知件数は946件と前年の1.6倍と増加するなど、犯罪の増加傾向は続いており、権利利益の保護・救済についても、インターネット上の掲示板における名誉

毀損問題など、いまだ対応が十分とは言えない状況にある。内閣府が2006年12月に行った調査によれば、インターネット上の犯罪が不安という人は10人中4人とのことである。

したがって、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＞

別添１　「セキュア・ジャパン２００６」に盛り込まれた施策の実施状況
別添２　平成１９年度情報セキュリティ関連予算について
別添３　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　各府省庁からの対策実施状況報告（２００６年度）
別添５　政府機関の情報セキュリティマネジメントの現状把握（２００６年度）
別添６　独立行政法人等の情報セキュリティ対策の現状について
別添７　企業・個人における情報セキュリティの評価指標
別添８　企業・個人における現状の評価（統計資料）

別添1

「セキュア・ジャパン2006」に盛り込まれた施策の実施状況

＜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ができず、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は出来なかったが、その理由が政府機関の事情によるものではない施策

第2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） a)	(政府機関統一基準の見直しの実施) 技術や環境の変化を踏まえ、2006年度に政府機関統一基準の見直しを行う。	内閣官房	・技術・環境の変化や各府省庁における対策実施状況等を踏まえ、内閣官房において見直しを実施。改訂案を情報セキュリティ政策会議第11回会合（平成19年4月開催）に諮る予定。	B+
イ） a)	(各政府機関でのＰＤＣＡサイクルの確立) 政府機関統一基準を踏まえた省庁基準に基づき、情報セキュリティ対策の実施のため、具体的な実施手順の整備、情報セキュリティ対策の実施状況の自己点検及び監査等を行い、2006年度にPDCAサイクルを確立する。 また、2006年度に、各府省庁において全職員に対する講習を行い、省庁基準及び実施手順等の遵守を徹底させる。	全府省庁	・各府省庁は、政府機関統一基準を踏まえた省庁基準及び具体的な実施手順に基づき、情報セキュリティ対策教育を実施するなど情報セキュリティ対策を推進。また、これらに基づいて情報セキュリティ対策の実施状況の自己点検等を行い、その結果を対策実施状況報告として取りまとめ、内閣官房に提出。	A′
イ） b)	(政府全体でのＰＤＣＡサイクルの確立) 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、必要な範囲で検査・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ことで、2006年度に政府全体としてのＰＤＣＡサイクルを確立する。	内閣官房 全府省庁	・内閣官房において、平成18年度上半期に、全府省庁の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について重点検査を行い、その結果の総合評価を情報セキュリティ政策会議第7回会合（平成18年7月25日）において実施。 ・各府省庁から提出された対策実施状況報告を内閣官房において取りまとめ、分析を行うとともに、内閣官房は情報セキュリティマネジメント評価に係る調査を実施。	A′
イ） c)	(評価及び結果の公表) 2006年度上半期中に、政府機関統一基準に基づき、重点項目等を対象に行う検査について、試行的評価を実施するとともに、2006年度中に、海外の評価手法等も参考にしつつ、政府全体としてのPDCAサイクルを確立するにあたり有効であり、かつ、客観的に比較可能な形での本格的評価の手法の確立を図る。 また、評価の結果については、情報セキュリティの維持・確保にも配慮しつつ公表することとする。	内閣官房	・内閣官房において、平成18年度上半期に、全府省庁の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について重点検査を行い、その結果の総合評価を情報セキュリティ政策会議第7回会合（平成18年7月25日）において実施。 ・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。 ・平成18年9、10月に政府機関評価指標専門委員会を開催し、その検討結果を踏まえて評価指標及び評価の枠組みを策定。	A
ウ）	(実施手順の作成支援及び技術的情報の提供と情報の共有) 内閣官房は、各府省庁の情報セキュリティ対策の推進を支援するため、実施手順の作成支援及び技術的な情報の提供を行う。なお、これらの情報については、民間企業、地方公共団体、独立行政法人にとっても、「ベストプラクティス（模範例）」として実効的に活用できるよう、各府省庁の活用実態を反映した改良を加え、2006年度から順次公開及び普及に努める。	内閣官房	・政府機関統一基準適用個別マニュアル群について、31種類を内閣官房（NISC）ホームページにおいて公開。	A
エ）	(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) ファイル交換ソフトウェア等を介して感染するコンピュータウイルスなどに起因する情報流出を防止するため、2006年度に、政府機関統一基準に基づき、各府省庁において情報の外部持ち出し及び私物パソコンの業務使用に関して厳格な管理を行うなど情報管理を徹底する。	全府省庁	・内閣官房において、各府省庁における情報管理対策について、政府機関統一基準に基づき、平成18年5月に「各府省庁の情報管理対策に関する状況調査」を実施。その結果について、情報セキュリティ政策会議第7回会合（平成18年7月25日）にて報告。 ・各府省庁は、情報管理について全職員に注意喚起し、相談窓口を設置するとともに、半数以上の府省庁で現状把握や関係規程の整備等を実施。	A
オ） 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) 2006年度に、外部委託先の候補者における情報セキュリティ対策の水準を確認するため、必要に応じて、政府調達における選定基準の一要素とし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を活用する。	内閣官房 全府省庁	・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」を各府省庁に配付。	A
オ） b)	(情報セキュリティ監査制度の活用) 2006年度に、外部委託先の情報セキュリティ対策レベルを適切に評価・確認するため、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図る。	内閣官房 全府省庁	・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」を各府省庁に配付。	A

オ） 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） 経済社会のインフラとなっている情報システムの不具合が、国民に多大な影響を及ぼす事態が発生していることを受け、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）において、全ての情報システムを対象として、開発運用等のプロセス管理の側面、技術的側面、組織的側面等の総合的観点から、情報システムの信頼性向上の方策を定めた「情報システムの信頼性向上に関するガイドライン」が2006年6月に策定されるところ、2006年度においては、同ガイドラインの政府機関における活用・普及の可能性およびその方策について検討する。	内閣官房	・経済産業省において、ガイドラインの政府調達における活用方策を検討していることに加え、政府調達も視野に入れたモデル契約の策定を進めている。	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） 2006年度に、独立行政法人等の情報セキュリティポリシーの整備状況を調査する。その結果を踏まえ、独立行政法人等については、政府機関統一基準を参考に、情報セキュリティポリシーの策定・見直しを促進する。	内閣官房 全府省庁	・情報セキュリティポリシーの整備状況について調査を実施。	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） 2006年度に、独立行政法人等の組織、業務形態等を踏まえ、情報セキュリティポリシーを適用する上での課題等を抽出し、必要となる情報を提供するなど、情報セキュリティ対策の改善に向けた環境を整備する。	内閣官房	・先行的に一部の独立行政法人等に対して、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。 ・情報セキュリティポリシーの見直しに取り組んでいる先行的な機関から課題等について情報収集。	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） 府省共通業務・システム及び一部関係府省業務・システムの最適化に関して、2006年度に、内閣官房とCIO補佐官等の連携を強化し、対象システムの開発において効率的な情報セキュリティ機能の実装を推進する。	内閣官房 総務省	・府省共通的なプラットフォーム（対象システムに必要なセキュリティ機能等を実装するための統一的な技術仕様、当該機能等を実現するためのシステム基盤等）の整備に関し、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）等と意見交換を実施。	A
イ）	（安全性・信頼性の高いIT製品等の利用推進） 安全性・信頼性の高い情報システムを構築するため、2006年度に、IT製品等を調達する際には、政府機関統一基準に基づきITセキュリティ評価及び認証制度 により認証された製品等を優先的に取り扱う。	内閣官房 全府省庁	・内閣官房は、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」を各府省庁に配付。	A

（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枠組み構築） 次世代の電子政府構築に向けて、政府全体の業務・システムの基盤となる共通的なプラットフォームの構築・整備に必要な技術的、機能的検討を行うための枠組みを2006年度に構築する。	内閣官房 総務省	・内閣官房において、府省共通的なプラットフォーム（対象システムに必要なセキュリティ機能等を実装するための統一的な技術仕様、当該機能等を実現するためのシステム基盤等）の整備に関し、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）等と意見交換を実施。 ・内閣官房において、府省共通業務・システム等の最適化の担当府省庁に対し、個別に、最適化の進捗状況、情報セキュリティ対策の措置状況を確認するとともに、府省共通的なプラットフォームの整備に係る意見交換を実施。	B
イ）	（高セキュリティ機能を実現する次世代OS環境の開発） 2006年度において、ITの信頼性確保のための喫緊な取組みとして、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、これに依存しない形で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、産学官の連携により推進する。	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、これに依存しない形で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。）の開発に、産官学の連携の下、平成18年7月から着手、3月には初年度の成果としてα版を開発。	A
ウ）	（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） 2006年度中に、電子政府に係る情報システムを構成するOSについて、そのOSのセキュリティ品質に係る評価尺度の確立に向けた検討を行い、システム調達時に活用可能な評価項目群及び各項目についての評価尺度の確立を図る。また、本格的な電子政府運用開始に向けたOS等システム導入における技術動向調査を2006年度に実施する。	内閣官房 総務省	・内閣官房において、本格的な電子政府運用開始に向けたOS等システム導入における技術動向調査を実施。 ・総務省において、電子政府に用いられるOSのセキュリティ品質に係る評価尺度の確立に向け、評価項目の抽出及び検証を実施し、評価基準案を策定。	A

エ)	(電子政府システムのIPv6対応化) IPv6の電子政府における利用が、電子政府サービスにおける不正使用・情報漏洩防止等のセキュリティ強化、インタラクティブ化、府省庁をまたがる共同利用システム構築等に有益であることを考慮し、また、早ければ2010年頃にIPv4アドレスが枯渇するとの予測があることへの先導的な対応を実施する観点から、各府省庁は、原則として2008年度までに、各情報システムの新たな開発(導入)又は更改に合わせて、情報通信機器及びソフトウェアのIPv6対応を図る。この円滑な実施のための以下の措置を実施する。 1)総務省は、2006年度前半に、電子政府システムにおけるIPv6ネットワーク整備に向けたガイドラインを策定する。 2)各府省庁は、上記ガイドラインに基づき各電子政府システムにおけるIPv6対応化による効果を検討し、原則として2006年度末までに、各情報システムにおけるIPv6対応化の具体的な計画を策定する。 3)電子申請等の国民からのアクセスもIPv6で行えるようにするためには、インターネットサービスプロバイダが個人ユーザーに対してIPv6接続サービスを提供することが必要であることから、2006年度より、総務省はインターネットサービスプロバイダにおけるIPv6接続サービス提供状況についてホームページで情報提供する。	内閣官房 総務省 全府省庁	・総務省は、各府省庁が電子政府システムにおけるIPv6対応化の具体的な計画を策定する際の参考とするため、電子政府システムのIPv6対応に向けたガイドラインを策定し、各府省庁に配布した。 ・総務省は、インターネットサービスプロバイダにおけるIPv6接続サービス提供状況について調査を実施した。これにより得られた結果は総務省のホームページにて周知した。	B
オ)	(電子政府認証ガイドラインの策定) 各府省庁の電子行政サービスが独自に手段を決定している電子認証について、リスクに応じた認証強度のレベルを整理、明確化し、行政サービス間の連携を安全性を保ちつつ推進するため「電子政府認証ガイドライン(仮称)」を2006年度に策定する。	内閣官房 総務省 経済産業省	・内閣官房及び経済産業省において、米国の「連邦政府機関向け電子認証ガイダンス(OMBガイダンス)」及び「電子認証ガイドライン(NISTガイドライン)」を参考として、我が国における電子政府認証マニュアルを作成。	B+

(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) 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を利用していないサイトについては、原則として2006年9月までに、同ドメイン名の利用を開始する。 また、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を用いることについて、各府省庁は国民に対し広く周知を行う。	総務省 全府省庁	・総務省において、平成18年2月、各府省の情報システム担当者に対してドメイン名に関する説明を行い、政府機関のドメインであることが保証されるドメイン名利用の早期実施について働きかけを行った。 ・また、汎用jpドメイン名における日本語ドメイン名の中で行政等に関するものとして予約されたドメイン名のリスト全体について、組織改称・改編等に対応した現行化を行い、「政府機関のドメインであることが保証されるドメイン名」の整備を実施した。	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) 政府機関に係る電子文書の成りすまし及び改ざん防止のため、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電子署名を付すことにより、一般国民や民間企業等の利用者が安心して利用できる環境の整備、具体的には電子署名を付すための政府内情報システムの共通仕様の検討を2006年度に開始する。	内閣官房 総務省 全府省庁	・政府機関に係る電子文書の成りすまし及び改ざん防止に向けた方策について検討を開始。	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) 電子政府推奨暗号の監視、電子政府推奨暗号の安全性及び信頼性確保のための調査、研究、基準の作成等を2006年度に行う。	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、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) 電子政府推奨暗号について、その危殆化が発生した際の取扱い手順及び実施体制の検討を進めるとともに、電子政府推奨暗号のあり方の見直し等を含めた暗号利用に関する政府内の推進体制について、2006年度に検討を開始する。	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検討を開始。	A
ウ)	(安全性・信頼性の高い暗号モジュールの利用推進) 安全性の高い暗号モジュール の活用を推進するため、独立行政法人情報処理推進機構の運用するITセキュリティ評価及び認証制度を拡充等し、暗号モジュールの認証に係る枠組みを新たに整備するとともに、2006年度に試行運用を開始する。	経済産業省	・独立行政法人情報処理推進機構において、平成18年6月より「暗号モジュール試験及び認証制度」の試行運用を開始。	A
エ)	(ファイル(電磁的記録)のセキュリティ対策の推進) 2006年度において、可搬記憶媒体へのファイル書き出し時のセキュリティ確保の観点から、ファイル秘匿化ソフトウェアの製作・導入を推進する。	防衛庁 (防衛省)	・可搬記憶媒体へのファイル書き出し時のセキュリティ確保のため、ファイル秘匿化ソフトウェアを製作し、同ソフトウェアの基礎的試験を完了するとともに適用システム毎の試験を開始。	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）	（情報収集、分析・解析機能の強化） 政府機関に対するサイバー攻撃、政府機関における情報漏洩や情報システムの障害等の発生を防止し、発生した場合には迅速かつ的確に対応するための横断的な情報収集機能及び攻撃等の分析・解析機能を強化すべく、２００６年度において、各政府機関のＷｅｂサーバ等の監視を試行的に開始するとともに、国内外の関係機関と連携した攻撃等の横断的分析・解析機能（「官民連携分析・解析スキーム」（仮称）」を構築する。 その際、様々な機関で研究が進められた最新技術の有効活用を図る。	内閣官房	・各省庁のホームページのトップページにつき閲覧が可能かどうかを常時監視。 ・発生が多発しているIT障害への対策を協議するための会議を開催。 ・平成19年度予算で政府機関の情報収集、分析・解析機能を強化するための体制整備を要求。	B
ア） b）	（各政府機関への助言機能、相互連携促進機能の強化） 各政府機関におけるIT障害の防止及び対応に資するため、２００６年度において、上記a）の分析・解析結果に基づく各政府機関への助言機能を強化するとともに、各政府機関相互での対策情報の交換等を促進するための総合調整を行う。この際、各政府機関に連絡・対応の結節点としての「リエゾン（連絡要員）」を任命し、定期的に情報交換のためのミーティングを開催する。	内閣官房	・発生が多発しているIT障害につき、全省庁の担当者を集め、対策会議を開催。IT障害の特徴及び対策を紹介した資料を全省庁に配布。	A
ア） c）	（情報保証に係る最新技術動向等の調査研究） ２００６年度において、情報システムの情報保証を確保するため、サイバー攻撃及びサイバー攻撃対処に係る最新技術動向等を調査するとともに、一元的な対処態勢等について調査研究を実施する。	防衛庁（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。研究結果は2007年度以降継続的に実施するサイバー攻撃統合対処体制の検討に資する予定。	A
イ） a）	（各政府機関における緊急対応体制の構築） ２００６年度中に、各政府機関におけるIT障害の発生時に迅速かつ的確に対応できる各政府機関における初動対処要領を作成するとともに、この体制に従事する要員の訓練の仕様のひな形を作成する。	内閣官房	・政府機関におけるIT障害発生時の対処手順の策定手引書及びひな形を作成。 ・訓練の仕様のひな形の作成に代えて、発生が多発しているIT障害につき、発生時の対応方策を策定。	A
イ） b）	（サイバーテロ対策に係る体制等の強化・整備） ２００６年度において、サイバーテロの手段となり得るサイバー攻撃手法の高度化に対応するため、サイバーテロ対策要員の事案対処能力・技術力の維持、向上のための部内外における研修の実施等、警察におけるサイバーテロ対策に係る体制等を強化・整備する。	警察庁	・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18年11月及び平成19年２月に実施。また、サイバーテロ対策の推進を指導する者に対し、部内研修を平成18年10月に実施。 ・事案対処に必要な技術力等の維持・向上のため、OSやネットワーク機器等に係る緊急対処等に関する部内研修や民間委託研修を実施。	A
イ） c）	（サイバー攻撃等に係る分析・対処及び研究の推進） ２００６年度において、昨今の高度化するサイバー攻撃手法に鑑み、防衛庁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分析・対処能力をさらに向上させる必要性から、不正アクセス監視・分析技術、サイバー攻撃分析技術及びアクティブ防御技術等について基礎的な研究を実施する。	防衛庁（防衛省）	・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の基礎的な研究を実施。	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）	（政府職員の人材育成に係る検討） 政府として情報セキュリティ対策を一体的に進めていくための政府職員の人材育成について検討し、政府全体として戦略的に人材育成を行うための基本方針及び具体策を２００６年度に示す。	内閣官房 全府省庁	・平成18年７月25日に、情報セキュリティ政策会議の下に「人材育成・資格制度体系化専門委員会」を設置して検討を行い、資格制度も含めた情報セキュリティに関する各種教育プログラムの体系図や我が国の情報セキュリティ人材の育成に関する様々な提言を「人材育成・資格制度体系化専門委員会報告書」（平成19年１月23日決定）に取りまとめた。	A
イ）	（緊急対応能力に係る人材育成手法の検討） IT障害への緊急対応に係るノウハウを収集し、各政府機関の人材育成へ反映させる方法について検討し、政府全体として戦略的に人材面での緊急対応能力強化を推進するための基本方針及び具体策を２００６年度中に策定する。	内閣官房	・平成18年７月25日に、情報セキュリティ政策会議の下に「人材育成・資格制度体系化専門委員会」を設置して検討を行い、資格制度も含めた情報セキュリティに関する各種教育プログラムの体系図や我が国の情報セキュリティ人材の育成に関する様々な提言を「人材育成・資格制度体系化専門委員会報告書」（平成19年１月23日決定）に取りまとめた。 ・発生が多発しているIT障害を中心に緊急時対応に関する資料を作成。	A
ウ）	（情報セキュリティに関する資格保有率向上に係る検討） 政府機関の情報システム管理部門における、情報処理技術者試験等の資格保有状況等について調査するとともに方向性について検討し、資格保有率の向上に資する具体策を２００６年度に示す。	内閣官房 全府省庁	・平成18年７月25日に、情報セキュリティ政策会議の下に「人材育成・資格制度体系化専門委員会」を設置して検討を行い、資格制度も含めた情報セキュリティに関する各種教育プログラムの体系図や我が国の情報セキュリティ人材の育成に関する様々な提言を「人材育成・資格制度体系化専門委員会報告書」（平成19年１月23日決定）に取りまとめた。	A

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ポリシーの策定・見直しの促進） 地方公共団体における情報セキュリティ確保に係るガイドラインの見直しを、２００６年９月を目処に行うとともに、各地方公共団体における当該ガイドライン等を踏まえた対策の実施を推進する。	総務省	・地方公共団体における情報セキュリティ確保に係るガイドラインについて、「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」を踏まえるとともに、セキュリティ対策水準を強化し、かつ分かりやすい表現となるような見直しを、平成18年９月に行った。	A

イ)	(情報セキュリティレベル評価ツールの提供) 2006年度に、各地方公共団体が、自らの情報セキュリティレベルを客観的に評価し、適切な達成目標を定め、計画的、段階的に個人情報保護・情報セキュリティ対策に取り組むことのできる評価ツールを地方公共団体に提供する。	総務省	・自らの情報セキュリティレベルを客観的に評価し、その結果に基づき具体的な改善計画を策定することができる評価ツールを、平成18年6月、地方公共団体に提供した。	A

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) 各地方公共団体が講じる情報セキュリティ対策について、その実効性の評価、見直しによる継続的な対策レベルの向上に資するため、2006年度において、情報セキュリティ監査の実施を推進する。	総務省	・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9カ所で実施。 ・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)	(「自治体情報共有・分析センター」(仮称)の創設促進及び運営支援) 地方公共団体におけるIT障害の未然防止、拡大防止及び再発防止並びにIT障害からの迅速な復旧に資するとともに、地方公共団体全体の情報セキュリティレベル向上を図るため、地方公共団体における情報セキュリティに関する情報の収集、分析、共有や政府等から提供される情報等の共有等を行う機能を有する「自治体情報共有・分析センター」(仮称)について、実証実験等を行い、2006年度末までの整備を推進するとともに、運営に必要な支援を行う。	総務省	・「自治体情報共有・分析センター」(仮称)の整備に向けて、情報共有プロセスの試行等の実証実験を実施。 ・なお、実証実験の結果等を踏まえ、地方公共団体が参加する行政専用ネットワーク(LGWAN)を活用し、地方公共団体の情報セキュリティ対策の実施に必要な情報やツール等を地方公共団体で共有することで、適切な予防及び復旧に役立てる機能「自治体CEPTOAR」が創設された。	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)	(地方公共団体における個人情報保護・情報セキュリティ対策技術の開発実証等) 2006年度に、地方公共団体における個人情報保護・情報セキュリティ対策の強化につながる高度な技術の開発実証を行う。	総務省	・地方公共団体における個人情報保護・情報セキュリティを強化する技術を実装したシステムの開発実証事業を実施。	A
イ)	(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) 2006年度に、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や、様々な自治体業務に携わる幅広い地方公共団体職員を対象に行う研修を実施するなど、地方公共団体職員の研修について支援を行う。	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9カ所で実施。 ・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2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）	（安全基準等の策定・見直し） 2006年9月を目処に、指針を踏まえて、各重要インフラ事業分野における安全基準等に必要又は望ましい情報セキュリティ対策の水準を明示するよう努力する。この際、「情報システムの信頼性向上に関するガイドライン」を参考とする。	重要インフラ所管省庁	平成18年9月末において、8分野が安全基準等の策定・見直しを実施。同年10月水道分野が安全基準等を策定。医療分野においては、平成19年3月末に見直しを完了。	A
ア）　b）	（電気通信分野における「安全基準等」の整備） 電気通信事業者等において設置される「電気通信分野における情報セキュリティ対策協議会（仮称）」を通じて、電気通信事業者等と連携し、「重要インフラの情報セキュリティ対策に係る行動計画」において官民が取り組むべき課題とされている「安全基準等」について、2006年9月を目途に整備すべく検討を行い、電気通信分野における情報セキュリティ対策の強化を図る。	総務省	・電気通信分野における情報セキュリティ対策協議会において、安全基準等WGを設置し、平成18年9月に「電気通信分野における情報セキュリティ確保に係る安全基準（第1版）」をとりまとめた。	A
イ）	（「安全基準等」の策定状況の把握及び評価） 2006年度中に「安全基準等」の策定状況を、各重要インフラ所管省庁の協力を得て把握を行い、相互依存解析の実施状況も踏まえつつ「安全基準等」の評価を実施する。	内閣官房	各分野における安全基準等の策定状況についてヒアリング等によって状況把握を行い、情報セキュリティ政策会議・重要インフラ専門委員会へ報告を行うとともに、平成19年3月に、指針との対応状況についての評価を実施した。	A
ウ）	（指針の見直し） 定常的なIT障害の発生状況の把握を通じ、各重要インフラ分野に共通する横断的な対策課題の分析・検討を行うとともに、政府機関統一基準、その他関連文書を参照しつつ、各重要インフラ所管省庁の協力を得て、2006年度中を目途に指針の見直しを実施する。	内閣官房	平成19年3月に指針の見直し及び、必要な改定のための作業を行い、重要インフラ専門委員会において改定案をとりまとめた。	B＋

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） 2006年度において、各重要インフラ事業者等から連絡された情報及び情報セキュリティ関係省庁、事案対処省庁、関係機関から集約した情報を分析し、適切に各重要インフラ所管省庁及び各重要インフラ事業者等に対し情報提供を実施する。さらに、緊急時においても関係者との間で必要な対処についての調整を行えるようセンター機能 の2007年度内運用開始に向けた環境整備に着手する。	内閣官房	・各重要インフラ所管省庁にリエゾン（内閣官房併任）をおき、センターと各重要インフラ所管省庁との間で情報連絡・情報提供を行うための体制を整備し、運用を開始した。 ・重要インフラ所管省庁及び重要インフラ事業者等に情報提供を実施するための環境整備を実施した。	A
イ）	（情報提供・連絡のための体制強化） 内閣官房にて策定された実施細目（仮称）に基づき、重要インフラ事業者等から各重要インフラ所管省庁ごとに選任されたリエゾンを通じて連絡された情報を内閣官房に連絡するための体制を強化する。また、内閣官房から提供された情報をCEPTOARを通じて、各重要インフラ事業者等に提供するための体制を強化する。このため、重要インフラ所管省庁に、内閣官房が構築した情報共有体制を適切な情報管理で行うためのリエゾンを2006年度の可能な限り早期におき、内閣官房に併任する。	重要インフラ所管省庁	・各重要インフラ所管省庁において、情報共有体制を適切な情報管理で行うためのリエゾンを内閣官房に併任し、情報提供・連絡のための体制強化を実施した。	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）　a）	（各重要インフラ分野におけるCEPTOAR整備の推進） 各重要インフラ所管省庁及び各重要インフラ事業者等間での協議を開始し、2006年度末までに各重要インフラ分野にCEPTOARが整備されることを目指す。また、新規追加分野（水道、医療及び物流）については、CEPTOAR整備に関する重要インフラ所管省庁及び重要インフラ事業者等間での基本的合意を2006年度末までに完了することを目指す。	重要インフラ所管省庁	・7分野の重要インフラ分野において、平成18年度末までに整備を完了した。また、新規追加3分野（医療、水道、物流）において、平成19年度中のCEPTOAR整備に向けた基本的合意が完了した。	A
ア）　b）	（電気通信分野における情報セキュリティ関連情報共有・分析体制の強化） 2006年度中に、第2章第2節①に掲げる「電気通信分野における情報セキュリティ対策協議会（仮称）」を通じて、電気通信事業者等と連携し、「重要インフラの情報セキュリティ対策に係る行動計画」において官民が取り組むべき課題とされているCEPTOARを整備すべく、既存の事業者団体間の連携の在り方について検討を行い、電気通信分野における情報セキュリティ関連情報共有・分析体制の強化を図る。	総務省	・「電気通信分野における情報セキュリティ対策協議会」において、CEPTOAR検討WGを設置し、平成19年1月に「T-CEPTOAR設置要綱」をとりまとめた。	A
イ）	（「CEPTOAR特性把握マップ」（仮称）とりまとめ） 重要インフラ所管省庁の協力を得て、各重要インフラ分野ごとに設けられる各CEPTOARの整備状況を把握するとともに、各分野の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「CEPTOAR特性把握マップ」（仮称）を2006年度末を目途に作成する。	内閣官房	・重要インフラ所管省庁等の協力を得て、平成18年度末現在の各CEPTOAR（7分野）の特性を把握するとともに、整備状況とあわせてCEPTOAR特性把握マップとしてとりまとめた。	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)の設置検討) 2006年度内に整備されるCEPTOARの代表から構成される検討の場を重要インフラ所管省庁及び重要インフラ事業者等の協力を得て設置する。	内閣官房	・各重要インフラ分野が整備に向け検討中であるCEPTOARの代表者の参加を得て、CEPTOAR-Council(仮称)の設置に向けた検討の場を重要インフラ所管省庁及び重要インフラ事業者等の協力を得て設置し開催した。	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)	(相互依存性解析の試行的実施) 2006年度中に、各重要インフラ所管省庁の協力を得て、2005年度の解析手法に関する調査結果を踏まえ、過去の災害等の調査等を通じて、依存関係を可視化できる仕組み(静的相互依存性解析)を構築するとともに、各重要インフラ分野の特性や状況等を配慮しつつ、試行的に相互依存性解析を実施する。	内閣官房	・各重要インフラ所管省庁の協力を得て、各重要インフラ分野の特性や状況等を配慮しつつ、依存関係を可視化できる仕組み(静的相互依存性解析)の構築に向けた試行的な相互依存性解析を実施した。	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)	(「研究的演習」の実施) 2006年度中に、演習実施の概念、演習課題の設定及び演習手法の理解等を主眼とし、各重要インフラ分野の特性や状況等を配慮しつつ、研究会を併用した演習(「研究的演習」)を実施する。	内閣官房 重要インフラ所管省庁	・演習実施の概念、演習課題の設定及び演習手法の理解等を主眼とし、各重要インフラ分野の特性や状況等を配慮しつつ、平成18年7月から10月にかけて「研究的演習」を実施した。	A
イ)	(「机上演習」の実施) 2006年度中に、類似業態単位又は重要インフラ分野横断的な共通事項単位に議論発掘と具体課題整理のための「机上演習」を実施する。	内閣官房 重要インフラ所管省庁	・「研究的演習」を踏まえ、平成19年2月に、重要インフラ分野と重要インフラ所管省庁などが参加して、具体的なシナリオの下に会議形式で課題討議を実施した。	A
ウ) a)	(電気通信事業分野におけるサイバー攻撃への対応強化) 2008年度までに、緊急時における、関係事業者間及び事業者・政府間の連携体制の強化や調整力を発揮できる高度なITスキルを有する人材の育成を図るべく、2006年度に、電気通信事業者を中心に、各重要インフラ分野に跨る情報通信ネットワーク上で発生するサイバー攻撃を想定したサイバー攻撃への対応演習を実施する。	総務省	・平成18年度の「電気通信事業分野におけるサイバー攻撃対応演習」の請負先が決定し、平成18年12月から平成19年1月にかけて3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)を実施。 ・平成19年の情報セキュリティの日(2月2日)の情報セキュリティ政策会議において本演習を再演するとともに、今後、実施結果をもとにサイバー攻撃への対応手順等をまとめたマニュアル等を作成し、公表する予定。	A
エ)	(各分野サイバー演習との連携) 2006年度中に、分野ごとに実施された「情報通信」「電力」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、連携に向けた検討を開始する。	内閣官房 重要インフラ所管省庁	・分野ごと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、知見の共有など、連携を図った。	A

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等) 企業における情報セキュリティガバナンスの確立に向け、2006年度中に、情報セキュリティ対策ベンチマーク、情報セキュリティ報告書モデル、事業継続計画策定ガイドラインの普及を図るとともに、必要に応じてこれらのツールの見直し、情報セキュリティガバナンスの確立のための新たな方策の検討を行う。 また、情報システムの構築や運用を各企業が行う際に、「情報システムの信頼性向上に関するガイドライン」を参照することを推奨するべく、2006年度から普及活動に着手する。	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に向け、各種セミナー等の場を活用し、情報セキュリティ対策ベンチマーク、情報セキュリティ報告書モデル及び事業継続計画策定ガイドラインの普及活動を実施中。また、「情報システム信頼性向上ガイドライン」の普及活動及び同ガイドラインの実効性を高めるためのベンチマークツール等の整備を実施。	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) 2006年度に、電気通信事業者の情報セキュリティ体制の構築・運用に資するため、事業者や事業者団体等と連携して、電気通信事業における情報セキュリティマネジメント指針（ISM－TG）の策定を促進する。 (ISM－TG：Information Security Management Guideline for Telecommunications)	総務省	・平成18年6月、「電気通信分野における情報セキュリティ対策協議会」において、「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」を業界ガイドラインとして策定・公表。 ・FAQや認証方法の検討など、普及促進に向けた各種取り組みを推進中。	A
イ）	(入札条件等の見直し) 情報システム等の政府調達において、競争参加者に対して入札条件等として求めるべき情報セキュリティ対策レベルの評価について検討を行い、2006年度中に結論を得る。	内閣官房 総務省 財務省 全府省庁	・政府と企業の情報セキュリティ対策レベルを向上させる政府調達制度のあり方について、内閣官房において研究を行った。	B
ウ）	(情報セキュリティ関連制度と内部統制制度等との整合性確保) 政府が推進する情報セキュリティに関する取組みについて、政府全体としての整合性を確保するため、現在構築が検討されている内部統制制度のIT統制に係る部分において、情報セキュリティに関連する事項については、既存の対策基準等の情報セキュリティ関連制度との関連を考慮しつつ、2006年度に検討を進める。	内閣官房 金融庁 経済産業省	・財務報告に係る内部統制報告制度の導入を盛り込んだ金融商品取引法が平成18年6月7日成立、6月14日公布。同制度を実務に適用するにあたっての基準等を金融庁企業会計審議会において平成19年2月15日公表。同制度は、財務諸表に重要な虚偽記載が発生しないために必要な内部統制を整備することを目的としており、ITへの対応についても、専らその目的の範囲に限定されるものであるが、情報セキュリティに関する事項については、既存の対策基準等の情報セキュリティ関連制度との関係を考慮しつつ金融庁において整備。 ・経済産業省において、情報セキュリティ関連制度と内部統制制度等との整合性確保の観点から、既存の基準であるシステム管理基準等の追補版（システム管理基準追補版）を作成中。	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）	(情報セキュリティ関連リスクに対する定量的評価手法の研究) 企業における情報セキュリティ対策そのものの可視化を図るため、2006年度中に、情報セキュリティに係るリスク定量化に関する調査研究等を実施する。	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ついて、調査研究を実施中。	A
イ）　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の普及促進) 国内外の取引等において、組織の情報セキュリティ水準を適正に評価できる環境を整備するため、2006年度中に情報セキュリティマネジメントシステム適合性評価制度の普及活動を行う。	経済産業省	・各種セミナー等の場を活用して、情報セキュリティマネジメントシステム適合性評価制度の普及活動を行うとともに、各種ガイドラインの改訂を実施。	A
イ）　b)	(情報セキュリティ監査制度の普及促進) 国内外の取引等の場面において、組織の情報セキュリティ水準を適正に評価できる環境を整備するため、2006年度中に、様々なニーズに応じた質の高い監査サービスを受けられる基準等の検討を行う。	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中。	A
イ）　c)	(情報セキュリティマネジメントに関する標準化の推進) 組織が情報セキュリティマネジメントシステムを効率的に確立、導入、運用、監視、レビュー、維持及び改善する際の標準として、2006年度中に、日本工業規格として、JISQ27001（情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項）（＝ISO／IEC27001）及びJISQ27002（情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範）（＝ISO／IEC17799）を制定する。	経済産業省	・情報セキュリティマネジメントに関する標準化を推進するため、平成18年5月20日付けで、以下のJIS（日本工業規格）を制定。 ・JIS Q 27001 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項（＝ISO/IEC 27001：2005） ・JIS Q 27002 情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範（＝ISO/IEC 17799 ： 2005）	A
イ）　d)	(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) 独立行政法人情報処理推進機構が運用するITセキュリティ評価及び認証制度について、制度の運用改善に資する新たな基準であるコモンクライテリア(CC：Common Criteria)Ver.3に基づく運用を2006年7月から開始し、IT製品等の効率的な評価及び認証を推進する。	経済産業省	・平成18年9月に発効したコモンクライテリア（CC）Ver.3に基づくITセキュリティ評価及び認証制度を平成18年10月に運用開始した。	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） ２００６年度において、法人又は個人事業者が一定の条件の下でファイアウォール装置等の情報セキュリティ対策装置を取得した場合の税制支援措置を実施する。	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（ファイアウォール／VPNアプライアンス等）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を実施。	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） ２００６年度において、産業競争力のための情報基盤強化税制の普及・啓蒙を図ることにより、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を促進する。	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中。また、当該印刷物について、関係機関・利用者に配布中。	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）	（情報通信セキュリティ人材を育成するための研修事業への支援） ２００６年度において、情報通信ネットワーク・システムに対する攻撃や不正侵入などに対する多面的、双方的知識及び実践的な対処法を習得するための人材育成センターの開設を支援するとともに、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助成を行う。	総務省	・平成17年度情報通信セキュリティ人材育成センター開設事業の補助金交付を受けた（財）ソフトピアジャパンおよび（財）ひょうご情報教育機構の「情報通信セキュリティ人材育成センター」が開設され、18年度も支援を実施中。また、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も助成中。	A
イ）	（情報セキュリティに関する専門家の育成等） ２００６年度中に、企業や大学における情報セキュリティ人材育成のあり方を検討するとともに、組織におけるIT利用者を対象とした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指標の検討を開始する。	経済産業省	・情報セキュリティに係る教育を行う際の教材モデルを策定するとともに、産業界等と連携した講師派遣等の方策につき、その効果や問題点等を検討中。また、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を策定・公表。	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） ２００６年度中に、中小企業の経営者や情報システム担当者等における情報セキュリティへの理解を深めるべく、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」の規模を拡大するとともに、内容のさらなる充実強化を行う。	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き、本年度から受講者のレベルに応じたコース数の拡充を行うとともに、全国約31ヶ所（昨年度16ヶ所）で開催。	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）	（コンピュータセキュリティ早期警戒体制の強化） コンピュータウイルス、不正アクセス、脆弱性等日々進化する情報セキュリティ問題に関して、関係者間における迅速な情報共有、円滑な対応を確保するため、２００６年度中に、独立行政法人情報処理推進機構や有限責任中間法人JPCERTコーディネーションセンター等による「コンピュータセキュリティ早期警戒体制」を強化する。	経済産業省	・OSS等の脆弱性に係る対応を強化すべく、関連ガイドラインを改定するとともに、OSS開発者等との協力体制を構築。	A
イ）	（安全なWebサイトが備えるべき基準の検討） Webサイトの安全性を確保するため、２００６年度中に、発注者がウェブアプリケーション構築時に開発者（受注者）に対して示すべきセキュリティ要件に関する基準の検討を開始する。	経済産業省	・実用的なガイドライン策定を目標に、発注者がウェブアプリケーション構築時に開発者（受注者）に対して示すべきセキュリティ要件について検討中。	A

第2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）	(小中学校における情報セキュリティ教育の推進) 児童生徒に対する情報セキュリティを含めた情報教育を推進するため、2006年度に、効果的な指導手法に関する実践事例の収集や、意識啓発のための普及フォーラムの開催などを通じて、教員の指導力の一層の向上を図る。	文部科学省	・児童生徒に対する情報セキュリティを含めた情報教育の充実に向けて、「情報モラル等指導サポート事業」を実施中。教員の指導力の一層の向上を図ることを目的として、効果的な指導手法に関する調査研究を実施するとともに、教員の意識啓発のための普及フォーラムを全国9地域において開催した。	A
ア）　b）	(ICTメディアリテラシー 育成手法の調査・開発) 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促進を図るため、これらの利用にあたって必要とされる総合的なICTメディアリテラシーに係る指導マニュアルや教材の開発等、新たなICTメディアリテラシー育成手法に関する調査・開発を2006年度に行い、2007年度以降に普及・啓発を図る。	総務省	・子どもたちがインターネットを安心して利用できるようにするため、ICTメディアリテラシーを育成する手法を調査、開発し、その普及を図る。平成18年度は、教材・指導マニュアル及びインターネット補助教材を開発した。	A
ア）　c）	(「情報セキュリティ対策」標語による普及啓発) 独立行政法人情報処理推進機構において、コンピュータウイルスやコンピュータへの不正な侵入による被害の軽減に資するべく、2006年度中に、全国の小学生・中学生・高校生を対象として、情報セキュリティ対策の意識を高めるための標語募集を行い、入選作品を公表する。	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」の募集を行い、平成18年5月に合計10作品の大賞及び入選を発表。	A
イ）　a）	(全国的な普及啓発活動の実施) 2006年度において、新たな脅威の動向を教材に反映する等、「インターネット安全教室」の内容の充実・強化を図りつつ、全国各地で継続的に開催することを通じ、一般利用者における情報セキュリティに関する基礎的な知識の普及を図る。	経済産業省 警察庁	・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をはじめとするNPO等と連携し、全国各地98か所で「インターネット安全教室」を開催。	A
イ）　b）	(e－ネットキャラバンの実施) 2006年度において、主に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講座のキャラバンを、通信関係団体等と連携しながら全国規模で実施する。	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た。 ・平成18年度は、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。	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) 国民の情報セキュリティ意識の向上を図るため、急速に高度化・複雑化している情報セキュリティの脅威に関する情勢等を踏まえ、2006年度に、「@police」、「国民のための情報セキュリティサイト」、「フィッシング対策協議会」、「フィッシング対策推進連絡会」等の取組みを通じた国民一人一人に対する適切な情報提供や、メディア等を活用した広報啓発活動を積極的に実施する。	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、政策会議等の開催状況をはじめとした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、6月には、NISCメールマガジンの配信及び英文ホームページの開設について、報道発表を実施。 ・都道府県警察において、「サイバーセキュリティ・カレッジ」等を通じて、教育機関関係者、地方公共団体職員、一般国民等に対し、サイバー犯罪の予防のための助言・指導を行うなど、情報セキュリティ対策を促すための情報提供を実施。 ・行政機関、教育機関及び産業界が、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、4～5月、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。 ・警察庁セキュリティポータルサイト(@police)において、アプリケーション等の脆弱性や新種のコンピュータウイルスの発生に係る注意喚起等の広報啓発を実施。 ・総務省「国民のための情報セキュリティサイト」について、情報通信の利用動向及び情報セキュリティの状況を踏まえつつ、同サイトのコンテンツ更新を実施中。 ・総務省において、6月に、ISP等の協力を得て、情報セキュリティ対策の必要性を周知する「情報セキュリティ対策の集中啓発」を実施。 ・総務省において、4月に、「職場外のパソコンで仕事をする際のセキュリティガイドライン」を公表。 ・総務省において、電気通信事業者とともに「フィッシング対策推進連絡会」を定期的に開催し、同連絡会において取りまとめた「フィッシングの現状及びISPによるフィッシング対策の方向性」に基づき、情報の共有を図るとともに、関係法令との整合性を確保しつつ、技術的な対策の導入促進等に関する検討など、フィッシング対策の更なる検討を実施中。 ・経済産業省において、フィッシング情報を継続して収集・分析するとともに、フィッシング対策協議会サイトにおいて、最新のフィッシングメール情報の提供や手口の紹介、注意喚起等を継続して実施している。 ・経済産業省において、テレビCM、新聞広告、専用ホームページ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） ２００６年度において、不正アクセス行為の禁止等に関する法律に基づき、不正アクセス行為の発生状況及びアクセス制御機能に関する研究開発の状況を公表するなどの取組みを通じ、不正アクセス行為に対する防御に関する啓発及び知識の普及を図る。	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18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技術の研究開発の状況を平成19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、民間委託による調査を実施。 ・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、コンピュータウイルス対策等についての啓発活動を実施中。 ・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98か所で「インターネット安全教室」を開催。	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） ２００６年度において、サイバー犯罪等の被害を防止するために、ネットワーク相談対応システム等を効果的に活用してサイバー犯罪等に係る情報提供を広く受け付けるとともに、広報啓発を効果的に実施する。	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、国民にその内容をより分かりやすくするため、平成18年８月、掲載内容を改善。 ・インターネット利用者からインターネット上の違法・有害情報に関する通報を受け付け、当該情報について警察への通報やプロバイダ等への削除依頼等を行うインターネット・ホットラインセンターの運営を平成18年６月に開始。 ・平成18年７月、警察庁ホームページにおいて、スパイウェアの被害に遭わないよう注意喚起。 ・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付するとともに、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 ユビキタスネット社会を迎え、無線によるブロードバンドサービスの利用が不可欠となる中で、安心・安全に電波を利用できる環境を保護する必要性が急速に高まっている。 このため、混信・妨害の未然防止をはじめ電波利用秩序の維持を図る上で、適正な無線機器の購入・使用を促すことが益々重要となっている。そこで、一般国民が安心して無線機器の購入・使用できる環境づくりに向けて、２００６年度に、全国のマスメディア媒体、ポスター、インターネットなどを利用して、無線機器に添付される「技術基準適合マーク」の確認を促すための周知啓発活動を実施する。	総務省	・平成18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18年６月～７月及び11月に総合通信局所在地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、７月、11月及び３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へバナー広告を実施。 ・無線利用機器に係る登録証明機関、無線機器製造業者、無線利用機器を販売している店舗の全国本社・関係事業者団体等へ周知啓発の協力依頼を実施。 ・８月の政府広報として、ラジオスポット、CSTV広告を実施するとともに、12月に政府広報番組(NTV系列31局ネット)を放映。	A
イ） a）	（「情報セキュリティの日」の創設） 情報セキュリティに関する国民の意識の醸成を促進すべく、２００６年度に「情報セキュリティの日」を創設し、これに伴う広報啓発的行事を全国的規模で開催するとともに、これにあわせて、個人、企業、地方公共団体、教育機関及び研究機関等を表彰するための制度の創設を検討する。	内閣官房 警察庁 総務省 文部科学省 経済産業省	・第８回情報セキュリティ政策会議（平成18年10月25日開催）において、「第1次情報セキュリティ基本計画」を定めた日でもある毎年２月２日を「情報セキュリティの日」と定めた。 ・また、同会議において、情報セキュリティへの取組みに関し、特に顕著な功績又は功労のあった個人又は団体を顕彰し、優れた取組みを広く普及することを目的として、「情報セキュリティの日」功労者表彰要綱を定め、平成19年２月２日に開催した第１０回政策会議にあわせて、第１回表彰式を執り行うとともに、「情報セキュリティの広報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、１月26日から３月２日までの間、全国各地で300件以上の関連行事を開催した。	A
ウ） a）	（日常からの世論喚起・情報提供の実施） 情報セキュリティについて国民に対して日常から世論喚起・情報提供を行うために、メールマガジンの発行及び政府全体としての情報セキュリティポータルサイトの構築を実施する。 メールマガジンについては、２００６年度の可能な限り早期に発行を開始し、月に１度以上の頻度で配信を行う。また、情報セキュリティポータルサイトについては２００６年度中に開設する。	内閣官房	・NISCメールマガジンを毎月１回を目途に発行し、本年３月23日に第９号を発行。 ・情報セキュリティ教育コンテンツなどを掲載した情報セキュリティポータルサイトを構築した。	A
ウ） b）	（情報セキュリティ貢献表彰(仮称)の創設） 情報セキュリティの確保に多大な貢献を果たした個人、企業等を表彰するべく、情報化月間に新たに「情報セキュリティ貢献表彰（仮称）」を２００６年度中に創設する。なお、その際、「『情報セキュリティの日』の創設」（第２章第４節②イ）a））との連携に配意する。	総務省 経済産業省	・毎年10月に行われる情報化月間の情報化促進貢献個人・企業等の表彰において、新たに平成18年度から「情報セキュリティ促進部門」を創設。当該部門においては、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） ウェブサイト、広報資料等の広報啓発媒体を活用し、我が国における情報セキュリティ戦略を国内外に対して積極的に発信していく。 具体的には、２００６年度中に内閣官房情報セキュリティセンターの英文ホームページを開設し、「第１次情報セキュリティ基本計画」の英語版等を示すこととする。	内閣官房	・NISC英文ホームページを本年７月に運用開始し、「第１次情報セキュリティ基本計画」、「セキュア・ジャパン2006」等の英訳を掲示。 ・政府インターネットテレビ英語版に我が国の情報セキュリティ政策の取組みやベスト・プラクティスの発信を内容とした英語版映像を公表。	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) 悪意のある第三者からの遠隔操作によりサイバー攻撃等を行うコンピュータウイルス（ボットプログラム）の感染を防ぐ対策、ボットプログラムに感染したコンピュータからのスパムメール送信やサイバー攻撃等を迅速かつ効果的に停止させるための対策等について、個人が負担感なく対応できるよう、2006年度中に技術面及び対策面を含めた検討を開始し、2010年度までに総合的な枠組みを構築する。	総務省 経済産業省	・総務省及び経済産業省の連携の下、財団法人日本データ通信協会テレコム・アイザック推進会議、電気通信事業者、独立行政法人情報処理推進機構、JPCERTコーディネーションセンター等が協力して、ボットプログラムの感染を防ぐ対策、ボットプログラムに感染したコンピュータからの攻撃等を停止させるための対策等を実施中。	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) IPv6対応ユビキタスセキュリティサポートシステム を2009年度までに構築することを目指して、2006年度中に利用環境をモデル化した実証実験を開始し、IPv6によるユビキタス環境構築に向けたセキュリティ確保上の課題解決を進める。	総務省	2006～2009年度の4か年計画の初年度として、IPv6によるユビキタス環境構築に向けたセキュリティ確保に関する実証実験を実施中。	A
ウ)	(無線LANのセキュリティ対策) 2006年度において、無線LANのセキュリティ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」の更なる普及の推進を図るとともに、「インターネット安全教室」の冊子等においても、無線LANの安全な使い方に関するコンテンツの充実を図る。	総務省 経済産業省	・総務省ホームページにおいて、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。また、当該ガイドラインの改訂の必要性等について検討を実施中。 ・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98か所で「インターネット安全教室」を開催。	A

第3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) 情報セキュリティ政策会議は総合科学技術会議との連携の下に、産官学を通じた我が国における情報セキュリティに関連する研究開発・技術開発の実施状況を把握するための検討を2006年度中に開始する。	内閣官房 内閣府	・平成18年10月より技術戦略専門委員会を再開し、同委員会の中で情報セキュリティに関連する研究開発・技術開発の実施状況を把握するための検討を実施。	A
イ)	(投資効果に係る継続的評価プロセスの導入) 情報セキュリティ政策会議は総合科学技術会議との連携の下に、情報セキュリティ技術に関する研究開発・技術開発の投資効果について、1) 事前、2) 中間、3) 事後の各段階における評価を2006年度中に開始し、その結果については速やかに公表する。	内閣官房 内閣府	・平成18年10月より技術戦略専門委員会を再開し、同委員会の中で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について評価を行うための検討を実施。	B
ウ)	(政府調達における成果利用の方策の検討) 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、最大限、直接政府が活用するための方策の検討を2006年度中に開始する。	内閣官房 全府省庁	・平成18年10月より技術戦略専門委員会を再開し、同委員会の中で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の検討を実施。	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) 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検討を行い、その基本方針及び具体策を2006年中に示す。	内閣官房 内閣府 警察庁 防衛庁 (防衛省) 総務省 文部科学省 経済産業省	・平成18年10月より技術戦略専門委員会を再開し、同委員会の中で、基盤としてのITを強化することに直結する中長期目標に対して公的研究資金を重点的に投入するための検討を実施。	B
ア)　b)	(次世代バックボーンに関する研究開発) 2009年度までに、通常のネットワーク運用では見られない異常なトラヒックを検出・制御しIPバックボーン 全体の安定運用等を実現する技術を確立することを目標として、2006年度において、次世代バックボーンに関する研究開発を推進する。	総務省	・平成21年度中に技術を確立することを目指し、基本設計・試作を行うとともに、機能の検証等を実施中。	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) 2009年度までに、経路ハイジャックの検知・回復を数分以内で可能とする技術を確立するとともに、経路ハイジャックの発生を予防可能とする技術を確立することを目標として、2006年度から経路ハイジャックの検知・回復・予防に関する研究開発に着手する。	総務省	2006～2009年度の4か年計画の初年度として、経路ハイジャックの検知・回復・予防に関する技術を開発中。	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) 情報セキュリティの一層の向上を図るべく、2006年度より、ネットワーク自身及びネットワーク上を流通する情報の安全性・信頼性を確保するためのセキュリティ技術と、大規模災害時にも切れずに防災・減災情報を瞬時に、かつ的確に利用できる技術と併せて、総合的な情報のセキュリティを確保するための技術に関する研究開発を実施する。	総務省	情報セキュリティの一層の向上を図るべく、「ネットワークセキュリティ技術の研究開発」、「暗号・認証技術及びコンテンツ真正性保証技術の研究開発」、「防災・減災のための情報通信技術の研究開発」を実施中。	A
ア)　e)	(新世代のアクセス制御技術の研究開発) 高信頼性社会の実現に不可欠な基盤技術として、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の研究開発を2006年度に実施する。	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、研究開発を実施中。	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) 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の研究開発を2006年度に実施する。	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、研究開発を実施中。	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) 「事故は起こりうるもの」との前提に立ち、情報やシステムを保護するだけではなく、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・開発手法の研究開発等を2006年度に実施する。	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、研究開発を実施中。	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開発) 組織・人間系の管理手法の高度化のため、組織における情報セキュリティのリスクの定量化、情報セキュリティ対策に関する費用対効果の測定等の研究開発を2006年度に実施する。	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ついて、調査研究を実施中。	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) 既存技術の改良や運用技術の開発等、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、官民での取組みの状況を把握し、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の調整をきめ細かく行うための検討を行い、その具体策を2006年度中に示す。	内閣官房 内閣府 警察庁 防衛庁 (防衛省) 総務省 文部科学省 経済産業省	・平成18年10月より技術戦略専門委員会を再開し、同委員会の中で、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、過小投資、過大投資が発生しないための投資ポートフォリオ調整を実施する検討を実施。	B
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】) 2006年度において、ITの信頼性確保のための喫緊な取組みとして、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、これに依存しない形で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、産学官の連携により推進する。	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、これに依存しない形で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。)の開発に、産官学の連携の下、平成18年7月から着手、3月末には初年度の成果としてα版を開発。	A
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】) 2006年度中に、電子政府に係る情報システムを構成するOSについて、そのOSのセキュリティ品質に係る評価尺度の確立に向けた検討を行い、システム調達時に活用可能な評価項目群及び各項目についての評価尺度の確立を図る。また、本格的な電子政府運用開始に向けたOS等システム導入における技術動向調査を2006年度に実施する。	内閣官房 総務省	・内閣官房において、本格的な電子政府運用開始に向けたOS等システム導入における技術動向調査を実施。 ・総務省において、電子政府に用いられるOSのセキュリティ品質に係る評価尺度の確立に向け、評価項目の抽出及び検証を実施し、評価基準案を策定。	A
イ) d)	(デジタルフォレンジック分野の確立に向けた産官学の連携強化) 2006年度中に、警察におけるデジタルフォレンジック分野に係る調査研究を推進するとともに、民間企業との技術協力、デジタルフォレンジックに係る研究会への参加等を通じ、情報共有を推進する。	警察庁	・電磁的記録の解析に係る知見の集約と体系化を行うため、各種電磁的記録媒体や携帯電話等の解析方法の調査研究を実施。 ・民間企業と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、情報共有を推進。 ・平成18年12月、産官学で構成される「デジタル・フォレンジック・コミュニティ2006inTOKYO」に参加し、情報共有を推進。	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) 2006年度において、情報セキュリティ基準ISO/IEC15408で規定される評価保証レベルEAL6の保証要件を満足する情報システムを試作し、評価試験を行うことにより評価手法の確立を推進する。	防衛庁 (防衛省)	・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および評価方法論(Evaluation Methodology)の研究を実施し研究試作を終了。	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) ネットワークがオールIP化された場合においても災害時等に重要な通信が確保できるよう、2008年までにIPネットワーク等に対応した重要通信の運用技術を確立することを目標として、2006年度に実験システムの開発に着手する。	総務省	・学識経験者、主要電気通信事業者、メーカー等からなる検討会の設立に向け準備中。 ・ネットワークがオールIP化された場合においても災害時等に重要な通信を確保するために必要となる運用技術を確立するため、関連の技術の動向等について調査を実施中。	A
ウ) a)	(萌芽的研究開発に係る基本方針等の策定) 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調整の実施に向けた検討を行い、その基本方針と具体策を2006年中に示す。	内閣官房 内閣府 警察庁 防衛庁 (防衛省) 総務省 文部科学省 経済産業省	・平成18年10月より技術戦略専門委員会を再開し、同委員会の中で、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調整の実施に向けた検討を実施。	B
ウ) b)	(高信頼性端末の電子認証基盤の研究開発) 暗号処理機能、暗号鍵の保護機能、プラットフォームの正当性検証機能等のセキュリティ機能を持つTPM(Trusted Platform Module)を搭載したPCの活用による安全なコンピューティング環境の実現に向けた研究開発を2006年度に実施する。	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、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) 継続的にグランドチャレンジ型に相応しいテーマを検討するための場を、総合科学技術会議、情報セキュリティ政策会議が連携して2006年度中に設置する。また、その際、設定されたテーマを基に研究開発・技術開発を推進する体制として、例えば、プログラムマネジャー制等、大目標の下での多岐にわたる各種要素技術の総合管理と最適な資源配分を促進するための枠組みの構築を検討する。	内閣官房 内閣府	・平成18年10月より技術戦略専門委員会を再開し、同委員会の中で、継続的にグランドチャレンジ型に相応しいテーマを検討する場の設置について審議を進めた。	B

第3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)	(情報セキュリティ関連の高等教育機関における多面的・総合的能力を有する人材の育成) 2006年度に、大学・大学院において産学連携による高度IT人材育成プログラムを開発・実施する拠点形成を支援する。	文部科学省	・本年度より、「先導的ITスペシャリスト育成推進プログラム」を実施し、産学連携による高度IT人材育成プログラムを開発・実施する教育拠点として、6大学を選定した。	A
イ)	(情報セキュリティに関する専門家の育成等【再掲】) 2006年度中に、企業や大学における情報セキュリティ人材育成のあり方を検討するとともに、組織におけるIT利用者を対象とした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指標の検討を開始する。	経済産業省	・情報セキュリティに係る教育を行う際の教材モデルを策定するとともに、産業界等と連携した講師派遣等の方策につき、その効果や問題点等を検討中。また、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を策定・公表。	A
ウ)	(情報通信セキュリティ人材を育成するための研修事業への支援【再掲】) 2006年度において、情報通信ネットワーク・システムに対する攻撃や不正侵入などに対する実践的な対処法を習得するための人材育成センターの開設を支援するとともに、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助成を行う。	総務省	・平成17年度情報通信セキュリティ人材育成センター開設事業の補助金交付を受けた(財)ソフトピアジャパンおよび(財)ひょうご情報教育機構の「情報通信セキュリティ人材育成センター」が開設され、18年度も支援を実施中。また、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も助成中。	A

②情報セキュリティに関する資格制度の体系化

該当項目	施策名	担当省庁	進捗状況	進捗状況分類
ア)	(情報セキュリティに関する資格制度の体系化等のための検討) 高い能力を有する情報セキュリティ技術者、各組織における最高情報セキュリティ責任者(CISO)、情報システム運用受託者、各組織の情報システムの運用担当者、情報システム利用者等それぞれに応じた適切なスキルについて関係府省庁間で連携を図りつつ検討を行い、情報セキュリティに関わる技術者等にとってキャリアパスとなるための情報処理技術者試験をはじめとする情報セキュリティに関する資格制度の体系化について、その基本方針及び具体策を2006年中に示す。	内閣官房 総務省 文部科学省 経済産業省	・平成18年7月25日に、情報セキュリティ政策会議の下に「人材育成・資格制度体系化専門委員会」を設置して検討を行い、資格制度も含めた情報セキュリティに関する各種教育プログラムの体系図や我が国の情報セキュリティ人材の育成に関する様々な提言を「人材育成・資格制度体系化専門委員会報告書」(平成19年1月23日決定)に取りまとめた。	A

第3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・強調の推進

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)	(多国間の枠組み等における国際連携・協力の推進) 情報セキュリティの脅威のボーダーレス化、増加・多様化の進展等を踏まえ、2006年度においては、G8及びOECDなどの多国間の枠組みにおける協力を積極的に実施するとともに、FIRST (Forum of Incident Response and Security Teams) 等へ積極的に参加することなどにより、諸外国の関係機関との連携を強化する。さらに、諸外国の情報セキュリティ対策の動向を把握したうえで、諸外国の関係機関との間で、情報交換・知見の共有・信頼関係の構築などを通じ、グローバルに希求される「安全・安心」の基盤づくり・環境の整備に貢献する。	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中。 ・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。	A´
イ)	(国際的なPOC機能としてのプレゼンスの明確化) 府省庁横断的な情報セキュリティ案件、または、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ついては、内閣官房情報セキュリティセンター (NISC) が我が国としてのPOC機能を有することを明確化し、2006年度は、その国際的な周知を実施し、諸外国との間でより効果的で円滑な連携を図るインターフェースとなる。	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を国際会合等で解説し、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中。	A
ウ)	(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) 情報セキュリティ先進国としての我が国の情報セキュリティ政策の基本理念や戦略、政府全体の政策、その中核を担う内閣官房情報セキュリティセンター (NISC) の位置づけと機能などについて、国際的な広報活動を2006年度に実施する。	内閣官房	・NISCの英語版ウェブサイトを構築し、政府全体の情報セキュリティ政策や、その中核を担うNISCの位置づけと機能等を解説。 ・平成18年5月に韓国・ソウルで開催されたOECD/ICCP/ISP (情報セキュリティ・プライバシー作業部会) において、情報セキュリティ政策会議及びNISCの創設、第1次情報セキュリティ基本計画の策定等の取り組みについて発表。 ・OECD等のウェブサイトに、「第1次情報セキュリティ基本計画」、「セキュア・ジャパン2006」、「重要インフラの情報セキュリティ対策に係る行動計画」等の英訳資料を掲載。	A
エ)	(OECDにおける重要情報インフラ保護のための各国施策の分析及び情報共有に関する取組みへの参加) OECDにおける重要情報インフラ保護のための各国施策の分析及び加盟国間の情報共有に関する取組みに参加し、2006年中に取りまとめられる予定の報告書の作成に貢献する。	総務省 経済産業省	・OECDのISP (情報セキュリティ・プライバシー作業部会) において、重要情報インフラ保護に係る各国のケーススタディが行われている。日本も、10月2日及び4日に開催されたISP会合において、ケーススタディを行うボランティアグループへの参加を表明した。 ・ボランティアグループにおける貢献の一環として、事務局からの質問票に回答する形で我が方から情報提供を実施 (1/29に提出済)。	A
オ)	(国際的なセキュリティ文化実現のための取組み) 2002年にOECDが策定した「情報システム及びネットワークのセキュリティのためのガイドライン」で定義された「セキュリティ文化」を実現するため、2006年度に、国内のみならず、国際的にも認識を共有しうるよう、環境整備に貢献する。	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することで、「セキュリティ文化」の国際的な醸成に向けて取組み中。	A´
カ)	(APT研修・セミナー等の開催) アジア太平洋地域のセキュリティに関する環境整備に資するために、APT の人材育成スキーム等を活用し、2006年度にセキュリティに関する国際的な研修・セミナー等を開催する。	総務省	・本年度、「ブロードバンドネットワーク技術とセキュリティ」に関するAPT研修を実施。	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) 世界最先端のIT国家として貢献するため、2006年度においては、IT障害への対処、防災や災害などへの対応、各国が共通に抱える社会的課題への対応など、様々な課題への多面的な知見・成果を、国際標準等に戦略的に反映させることも含めて、世界に先駆けて国際的に提供していく。	内閣官房 全府省庁	・政府インターネットテレビに、海外向けコンテンツとして「情報セキュリティ政策に関する日本政府の取組み」を掲載し、政府内の情報セキュリティ関連組織の整備や国家戦略等を、ベストプラクティスとして国際的に発信。	A´
イ)	(海外のコンピュータセキュリティ緊急対応チーム (CSIRT) の体制強化の支援) 有限責任中間法人JPCERTコーディネーションセンター (JPCERT/CC) を通じ、アジア太平洋地域における海外CSIRTの構築を支援する。具体的には、2006年度に、同地域におけるCSIRTの集合であるAPCERTとも連携をとりながら、JPCERT/CCにおけるインシデント運用技術や蓄積された経験を同地域の関係諸機関と共有し、これらの機関の能力向上を図る。	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 構築支援に向けて、各国関連組織との連携体制を強化。 ASEAN CERT の窓口である シンガポールのSingCERTとも連携し、ASEAN 諸国の関係諸機関の能力向上や CSIRT 構築に向けたセミナーの開催を検討中。	A

ウ)	(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) 電気通信分野の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を目指し、2006年度は、国際電気通信連合(ITU:International Telecommunications Union)に対して、第2章第3節①に掲載の電気通信事業における情報セキュリティマネジメント指針(ISM-TG)について提案を行い、国際標準として採択されるよう努め、もって国際的な情報セキュリティマネジメントのレベルの向上に貢献する。	総務省	・総務省の電気通信分野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標準化を目指し、平成18年4月に国際電気通信連合(ITU)においてX.1051の改正案を提案。同年12月に行われるITU会合において修正案の審議を行った。	A

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) 多様化・複雑化するサイバー犯罪に適切に対処するため、サイバー犯罪捜査に従事する全国の警察職員に対する部内外の研修を、2006年度に積極的に実施する。	警察庁	・平成18年7月、警察大学校において、都道府県警察のサイバー犯罪捜査指揮を担当する警部及び警部補対象の「サイバー犯罪取締り・対策専科」を実施。 ・平成18年9月、関東管区警察学校において、都道府県警察の情報セキュリティアドバイザーのレベルアップを目的とした「情報セキュリティアドバイザー専科」を部外に委託して実施。 ・平成18年11月及び平成19年1月、関東管区警察学校において、都道府県警察のサイバー犯罪特別捜査官のレベルアップを目的とした「サイバー犯罪捜査技術専科」を部外に委託して実施。 ・都道府県警察学校において、第一線の警察官のサイバー犯罪捜査能力向上を目的とした「サイバー犯罪対策専科」を実施。 ・都道府県警察において、サイバー犯罪捜査等に従事する職員に対する民間委託研修を実施。 ・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、ネットワーク及び電磁的記録の解析等に係る各種研修を実施。	A
ア) b)	(サイバー犯罪の取締りのための体制の強化・整備) 地理的制約をほとんど持たないという特性を持つサイバー犯罪に適切に対処するため、県境・国境を越えて敢行されるサイバー犯罪を的確に取り締まるための捜査体制を2006年度に強化・整備する。	警察庁	・平成18年4月、警察庁生活安全局情報技術犯罪対策課に「情報技術犯罪捜査指導官」を新設し、サイバー犯罪の捜査に関する都道府県警察に対する指導・調整及び当該犯罪に係る国際捜査共助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) 多様化・複雑化する不正アクセス等の犯罪手口やサイバー犯罪条約の批准に伴う新たな法制度の施行に対応するため、2006年度に、捜索現場での活動やコンピュータウイルス等の動作検証を行うための資機材の整備・増強を実施する。	警察庁	・都道府県警察におけるサイバーパトロール用携帯電話の整備に向け、補助金を交付。 ・捜索現場での活動やコンピュータウイルス等の動作検証を行うため、ハードディスクコピー装置や現場臨場用のパーソナルコンピュータ等の資機材を整備。	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) 近年における情報処理の高度化の状況等にかんがみ、サイバー犯罪に適切に対処すべく、サイバー犯罪条約を締結するための法整備等を2006年度に推進する。 (2005年10月4日に、「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」を第163回国会に提出したところ、現在継続審議中。)	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回国会に提出したところ,現在継続審議中。)。	―
ア) e)	(サイバー犯罪の取締りのための国際連携の推進) 2006年度中に、サイバー犯罪対策に係る海外の法執行機関との連携について、2国間における取組みを進めるとともに、G8ハイテク犯罪サブグループ会合、ICPO等のサイバー犯罪対策に係る国際的な枠組みへの参画の継続的推進、アジア地域サイバー犯罪捜査技術会議の参加国拡大等を通じた多国間における協力関係の構築を推進する。	警察庁	・平成18年4月、児童ポルノ事犯等児童を被害者とするサイバー犯罪の国際的な動向について理解を共有するとともに、その捜査手法や捜査技術について習熟を図ることを目的として、アジア等の6か国からサイバー犯罪捜査担当者を招き、インターネット利用児童ポルノ事犯捜査セミナーをICPO及び児童失踪・児童虐待国際センター(ICMEC)と共催。 ・平成18年10月、G8・24時間コンタクトポイント訓練会合において、英国及び米国と共同でトレーナーを担当。 ・平成18年5月、英国の重大組織犯罪対策庁(SOCA)電子犯罪部との間で、情報技術解析に関する協力を含むサイバー犯罪の防止及び取締りのための協力を推進することを内容とする意図表明文書に署名。 ・アジア大洋州地域サイバー犯罪捜査技術会議(平成18年9月開催)への各国・地域の参加を積極的に促し、参加国・地域を拡大(3か国1地域が新規参加)。また、サイバー犯罪技術情報ネットワークシステム(CTINS)により、参加国・地域との情報共有・連携を推進。	A
ア) f)	(中央当局制度を活用した国際捜査共助の迅速化) 捜査・司法当局を中央当局として指定し、外交ルートを経由せずに共助の授受を行うことで共助の迅速化を図るとともに、原則として共助を義務的とする日米・日韓の二国間における捜査共助条約が2006年度に発効する見込みであるところ、国際的なサイバー犯罪に適切に対処すべく、2006年度においては、同種の二国間条約を締結する作業を進める。また、サイバー犯罪条約上の「中央当局」の指定について、関係省庁と協議の上、検討する。	法務省	・日米刑事共助条約は平成18年7月21日に、また、日韓刑事共助条約は平成19年1月26日に発効した。 ・現在、香港、中華人民共和国及びロシア連邦と刑事共助条約の締結に向けて、警察庁及び外務省などの関係省庁と共に交渉中。	B
ア) g)	(重要無線通信妨害対策の強化) 航空無線や消防無線などの重要無線通信インフラに対し、混信・妨害が発生し、システムの機能低下や停止が起こり、人命・財産等の脅威に派生するなどの事態が発生しており、あるいは重要無線通信インフラを意図的に操作し、システムの誤動作を引き起こす等の懸念もあり、その迅速な排除に向けての対策強化が益々重要となる。 このため、重要無線通信に係る混信・妨害の申告・相談に対する的確な対応、並びに混信・妨害の迅速な排除に向けて、「電波監視充実3カ年計画」に基づき電波監視の充実・強化を図るとともに、2006年度末までに電波監視施設の更改、大都市圏での電波監視職員の増員などにより電波監視の強化を図る。	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(一部デジタル復調機能の実現)並びに混信が恒常的に発生している地域への計画的な整備を実施。 ・電波利用の多様化、高度化、周波数逼迫等への対応として、ディジタル復調のためのスクランブル推定技術の検討及び発射源可視化システムの開発を実施中。 ・監視機能強化・不法無線対策強化のため関東・近畿総合通信局に各2名(合計4名)を増員。	A

イ)	(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) サイバー空間における権利利益の保護・救済のための基盤の整備の必要性について、関係府省庁と連携しながら、2006年度に現状把握等の調査を行う。	内閣官房	・有識者からヒアリングによる調査を実施し、その結果をとりまとめた。	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)	(高度なネットワーク認証基盤実現のための技術開発) インターネット上のやりとりを安心・安全に行うことができるよう、厳格な本人確認機能を有するネットワーク基盤構築のための技術開発に取り組み、2006年度中に基礎技術を開発する。	総務省	・認証技術を活用した高度なセキュリティ機能を有するネットワーク実現のため、安心なネットワーク利用やサービス提供を実現するための基礎技術の開発を実施。	A
イ)	(サイバーテロ対策に係る官民の共同研究の推進) 2006年度において、民間企業や大学等と連携して、ファイアウォール等のログ等の分析によるサイバー攻撃の予兆把握等に関する共同研究を実施する。	警察庁	・ファイアウォールから集約されたログ等の分析によるサイバー攻撃の予兆把握、早期検知等に関して、民間や大学と共同で調査研究を実施。	A

第4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) 政府全体の情報セキュリティ対策の推進体制の中核となるべく、内閣官房情報セキュリティセンター（NISC）の人員体制を引き続き強化し、体制面として2006年度の早期に60名体制を確保するとともに、最高の英知を結集するため、官民を問わず優れた人材を積極的に活用する。 こうした体制の下、政府機関統一基準とそれに基づくPDCAサイクルを確立し、また、政府全体としての緊急対応能力を強化するため、第2章第1節に示した施策を実施するとともに、重要インフラの情報セキュリティ対策に係る行動計画等に従って、第2章第2節に示した施策を実施する。 また、府省庁横断的な情報セキュリティ案件についての我が国の国際的なPOCとしての内閣官房情報セキュリティセンター（NISC）の機能を充実させるとともに、国際的なコミュニケーションや情報共有を通じ、諸外国から信頼される国際的なインターフェースとしての役割を果たすべく、POCとしての認知度向上、諸外国との信頼関係の構築を推進し、また、情報収集の充実、関係機関等との情報の共有・分析機能の強化を図り、横断的な情報セキュリティ政策推進の中核としての機能を確保する。 さらに、内閣官房情報セキュリティセンター（NISC）の活動状況及び情報セキュリティに係る動向等を広く国民に知ってもらうとの観点から、2006年度より定期的に内閣官房情報セキュリティセンター（NISC）のメールマガジンを発行する。	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進め、平成18年度上半期末までに約60名の体制を確保した。 ・政府機関統一基準に基づき、平成18年7月に、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を公表し、これらを踏まえ同基準の見直しを実施したこと、また、重要インフラの情報セキュリティ対策に係る行動計画等に従い、平成19年2月に重要インフラ分野における分野横断的な机上演習を実施したことなど、第2章に示した施策を推進した。 ・府省庁横断的な情報セキュリティ政策を推進するため、我が国の国際的なPOCとしてのNISCの認知度を向上させるとともに、諸外国との信頼関係の構築を推進した。 ・NISCメールマガジンを毎月1回を目途に発行し、平成19年3月23日に第9号を発行。	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) 2006年度において、各府省庁は、自らの情報セキュリティ対策の体制の強化を行うとともに、政府機関全体で協調し、官民における情報セキュリティ対策の実施手順及び成果等の共有化や対策の統一化等の府省庁横断的な取組みを実施する。	全府省庁	・各府省庁は、自らの情報セキュリティの体制の強化に向け、体制の整備及び見直しを実施。 ・内閣官房は、各府省庁等担当者による「政府機関統一基準の実施のための勉強会」を実施するとともに、政府機関統一基準適用個別マニュアル群の提供等により官民における情報セキュリティ対策に関する情報を共有。	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) ２００６年度において、情報セキュリティ政策会議は、ＩＴ戦略本部はもとより、経済財政諮問会議、総合科学技術会議等、他の関係する本部・会議等との意見交換を密にし、これらとの役割分担をより明確化していくとともに、様々な方策の提案や実施において緊密に協力し、政府全体として情報セキュリティ政策を一体的に推進する。	内閣官房 内閣府	・ＩＴ戦略本部との連携を図り、「IT重点計画-2006」(平成18年７月26日IT戦略本部決定)に「セキュア・ジャパン2006」の内容を盛り込んだ。 ・経済財政諮問会議との連携を図り、「経済財政運営と構造改革に関する基本方針2006」(平成18年７月７日閣議決定)に「セキュア・ジャパン2006」の内容を盛り込んだ。 ・総合科学技術会議との連携を図り、高セキュリティ機能を実現する次世代ＯＳ環境の開発プロジェクトに7月から着手、3月に初年度の成果としてα版を開発した。	A

第4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)	(評価の実施及び公表) 2006年度において、セキュア・ジャパン2006を適切に評価するための手法について検討を行いつつ、そこに記載されている具体的施策の取組状況について評価を実施し、その結果を半年ごとに公表する。その際、IT戦略本部評価専門調査会の検討との連携を図る。	内閣官房	・平成18年7月25日に、情報セキュリティ政策会議の下に「企業・個人評価指標専門委員会」及び「政府機関評価指標専門委員会」を設置、これに「重要インフラ専門委員会」を加えた各専門委員会において、各対策実施領域における評価指標の検討を実施し、その成果を「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」(平成19年2月2日政策会議了解)に取りまとめた。 ・「セキュア・ジャパン2006」の進捗状況について、調査を実施し、その結果も踏まえ評価を実施した。 ・IT戦略本部評価専門調査会が実施するIT政策の評価に際し、本評価の結果を活用する方針で作業中。	B+
イ)	(政府機関の情報セキュリティ対策強化に向けたマイルストーンの検討等) 2006年度において、基本計画の実現に向けて、政府以外の関係機関における対応をあらかじめ促す等の観点から、政府機関自らの情報セキュリティ向上に係る施策について、2008年度までのマイルストーンを検討する。	内閣官房	・マイルストーンを検討する前提として、2009年時の我が国社会の姿及び情報セキュリティ政策の評価の枠組みについて検討を実施、その結果を「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」(平成19年2月2日情報セキュリティ政策会議了解)にとりまとめた	B
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」に基づく取組み) 「重要インフラの情報セキュリティ対策に係る行動計画」に基づく2006年度における取組状況を、重要インフラ専門委員会の場を活用して把握する。	内閣官房	・平成18年度は3回の重要インフラ専門委員会を開催し、行動計画に基づく取組みの状況を継続的に把握した。また、行動計画で定めた4本の施策の柱それぞれについて、各年度ごとの目標に対する進捗度合いを指標として、重要インフラ分野における情報セキュリティ対策の評価を行うことを確認した。	A

(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	新分類(案)
ア)	(計画の見直しについての検討) 情報セキュリティに関する大規模な災害や攻撃の発生等の緊急事態や急激な情勢の変化が起こった際に、本セキュア・ジャパン2006の実施途中であっても、迅速に相応の取組みを策定の上実施する。	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発生していない。	A

(3) 評価指標の確立

該当項目	施策名	担当省庁	進捗状況	新分類(案)
ア)	(情報セキュリティ対策に関する評価指標の確立) 基本計画(セキュア・ジャパンの実現)の実現に向けた道筋を可視化する視点に立ち、各対策実施領域(政府機関、地方公共団体、重要インフラ、企業、個人等)における情報セキュリティ対策の浸透の度合いを評価することができる指標を検討するための体制を2006年度のできる限り早期に設置し、2006年度中に的確な評価指標を確立した上で、これらの指標の政府内及び国際機関等における活用を推進する。 なお、当該評価指標の確立に資するため、独立行政法人情報処理推進機構による「国家情報セキュリティ水準評価指標(仮称)」の策定を促進するほか、「情報通信インフラのセキュリティ水準評価指標(仮称)」の策定について検討する。	内閣官房 総務省 経済産業省	・平成18年7月25日に、情報セキュリティ政策会議の下に「企業・個人評価指標専門委員会」及び「政府機関評価指標専門委員会」を設置、これに「重要インフラ専門委員会」を加えた各専門委員会において、各対策実施領域における評価指標の検討を実施し、その成果を「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」(平成19年2月2日政策会議了解)に取りまとめた。 ・上記政策会議了解に基づき、情報セキュリティ対策の評価を実施した。 ・独立行政法人情報処理推進機構において、「情報セキュリティ水準評価指標研究会」を設置し、「情報セキュリティ水準評価指標」の検討を実施、具体的な指標の選定を行った。 ・総務省において、「電気通信事業分野におけるサイバー攻撃対応演習」の一環として、「サイバー攻撃の発生時における電気通信事業者の対応状況に関する評価指標」について検討を行った。	A

別添２

平成19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１９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　予算額

○ 平成１９年度予算額　　３０，００１百万円

○ 予算額推移

	平成１６年度	平成１７年度	平成１８年度	平成１９年度
当初予算	２６７億円	２８８億円	３１９億円	３００億円
補正予算	―	―	―	―
合　　計	２６７億円	２８８億円	３１９億円	３００億円
		⇒	⇒	⇒
		7.9%増	10.8%増	6.0%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１９年度のＩＴ関係予算額は１２，４８４億円であり、情報セキュリティ関連予算はその２．４％を占めることになる。（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）
１　政府機関（政府機関統一基準を満たすためのもの）	２０，７１５	１８，１１３
２　政府機関（１以外）		８１８
３　地方公共団体		７６
４　重要インフラ	１，７２５	４８６
５　企業	３，５５３	１，４８２
６　個人	４１	２，０２５
７　横断的な基盤の形成	５，８８４	７，００１

対策実施領域の分類について、平成１８年度から平成１９年度にかけて変更があったものについて、平成１８年度の金額を平成１９年度の分類に合わせた金額は以下のとおり。

分類	平成１８年度 （単位：百万円）
１　政府機関（政府機関統一基準を満たすためのもの）	２０，０６９
２　政府機関（１以外）	
３　地方公共団体	
４　重要インフラ	７２３
５　企業	１，７８１
６　個人	１，１０３
７　横断的な基盤の形成	８，２４２

また、平成１９年度の分類１（１８，１１３（百万円））について、さらに詳細な分類を行った結果は以下のとおり。

分類	平成１８年度 （単位：百万円）
Ａ　システム構築関連予算	１５，８０８
Ｂ　体制整備のための予算	９２９
Ｃ　その他	１，３７６

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：百万円）	平成１９年度予算額 （単位：百万円）
内閣官房	３５３	８６８
内閣法制局	７	８
人事院	２１	２９
内閣府	１６７	１５６
宮内庁	４１	２５
公正取引委員会	３１	３７
警察庁	１，２４４	１，３３５
金融庁	１５３	１３９
総務省	７，２４３	５，９４１
法務省	１４９	５３９
外務省	２，７０３	２，９５９
財務省	９１８	７３６
文部科学省	６８３	６５５
厚生労働省	５５４	６５
農林水産省	２７４	５１７
経済産業省	３，８６２	４，４４２
国土交通省	５９７	４６６
環境省	１２４	１７４
防衛省	１２，７９６	１０，９０９

合計	３１，９１８	３０，００１

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

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 ・アンチウィルスソフトの運用状況
情報保護対策	・モバイルPCの暗号化機能の運用状況
端末管理	・端末の物理的対策状況

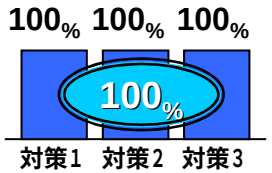
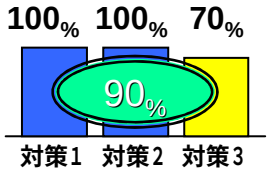
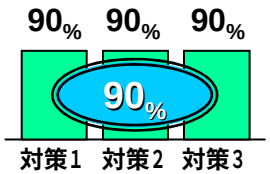
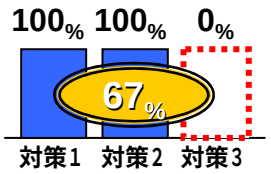
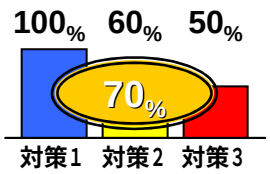
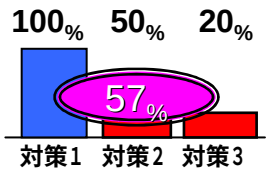
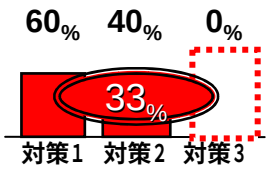
ウェブサーバに関する重点検査項目	
不正プログラム対策	・OSのパッチ等の適用状況 ・ウェブサーバAPのパッチ等の適用状況等
不正アクセス対策	・不正アクセス対策状況
情報保護対策	・利用者に対する権限管理等の実施状況
サーバ管理	・管理者に対する権限管理等の実施状況 ・データ復旧対策状況

・府省庁の調査に基づく結果
・平成18年3月末時点

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

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%

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。	 

各府省庁からの対策実施状況報告（2006年度）の概要

別添4

【報告の目的】 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

各府省庁の責任で情報セキュリティ対策を実施することが大前提 ⇨ **運用状況の把握が必要**

【報告の概要】 報告内容 ：政府機関統一基準の基本遵守事項について、**責務が発生した場合の対策の措置状況**等

報告対象 ：・ 情報セキュリティ責任者等、**情報セキュリティに係る役割を担う者**
・ **本府省庁課長相当職以上**の行政事務従事者（地方支分部局を含む。）
・ **電子申請ｼｽﾃﾑ、文書管理ｼｽﾃﾑ、府省庁LAN**及び**最適化対象ｼｽﾃﾑ**（個別府省業務・ｼｽﾃﾑ）

統一基準の構成	記載内容（抜粋）
第2部　組織と体制	管理体制の確立、ｾｷｭﾘﾃｨ教育、自己点検、監査
第3部　情報の取扱い	情報の格付け、情報の作成・利用等取扱いに係る対策
第4部　情報ｾｷｭﾘﾃｨ機能等	ﾕｰｻﾞ認証機能、ﾛｸﾞ管理機能、暗号・電子署名、不正ﾌﾟﾛｸﾞﾗﾑ対策
第5部　情報ｼｽﾃﾑの構成要素	安全区域、端末・ｻｰﾊﾞ、ｱﾌﾟﾘｹｰｼｮﾝ（ﾒｰﾙ・ｳｪﾌﾞ）に係る対策
第6部　個別事項	機器等購入、外部委託、庁舎外情報処理、私物ﾊﾟｿｺﾝ利用に係る対策

①実施率・②到達率による分析

【把握した主な課題】

今後、改善が求められる事項

行政事務従事者

第3部　情報の取扱い
- ○ 情報の格付け・取扱制限に係る措置

第5部　情報ｼｽﾃﾑの構成要素
- ○ 安全区域内における職員識別の徹底

情報セキュリティ責任者等

第2部　組織と体制
- ○ 情報セキュリティ教育及び情報セキュリティ監査の実施

第4部　情報セキュリティ機能等
- ○ 電子署名の付与に必要な機能の導入

第6部　個別事項
- ○ 外部委託先のアクセス範囲等に係る基準の整備

統一基準の導入初年度であり、十分な実施状況ではないが、課題は明確にされた。

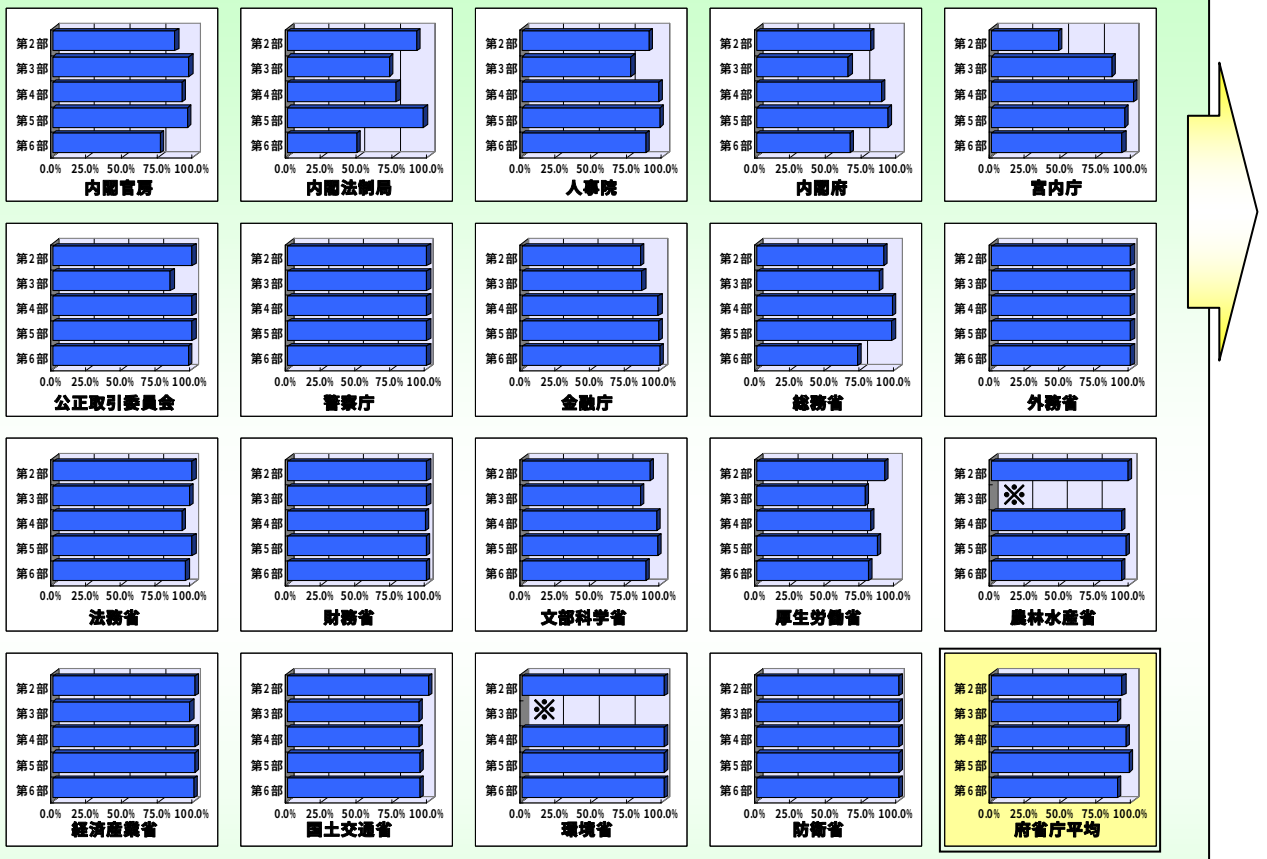
各府省庁の対策実施状況報告（2006年度）の集計結果①

各府省庁からNISCへの報告

機関名	把握率
内閣官房	99.2 %
内閣法制局	95.9 %
人事院	99.9 %
内閣府	73.5 %
宮内庁	100.0 %
公正取引委員会	99.2 %
警察庁	100.0 %
金融庁	63.3 %
総務省	97.6 %
外務省	100.0 %
法務省	100.0 %
財務省	100.0 %
文部科学省	100.0 %
厚生労働省	95.7 %
農林水産省 （独自の調査を含める場合）	31.2 % （98.2 %）
経済産業省	100.0 %
国土交通省	100.0 %
環境省 （独自の調査を含める場合）	40.7 % （94.2 %）
防衛省	94.1 %

※　2006年度においては報告対象を限定

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の平均）



※：2006年度においては、独自の把握状況調査を実施（分析の対象から除外）

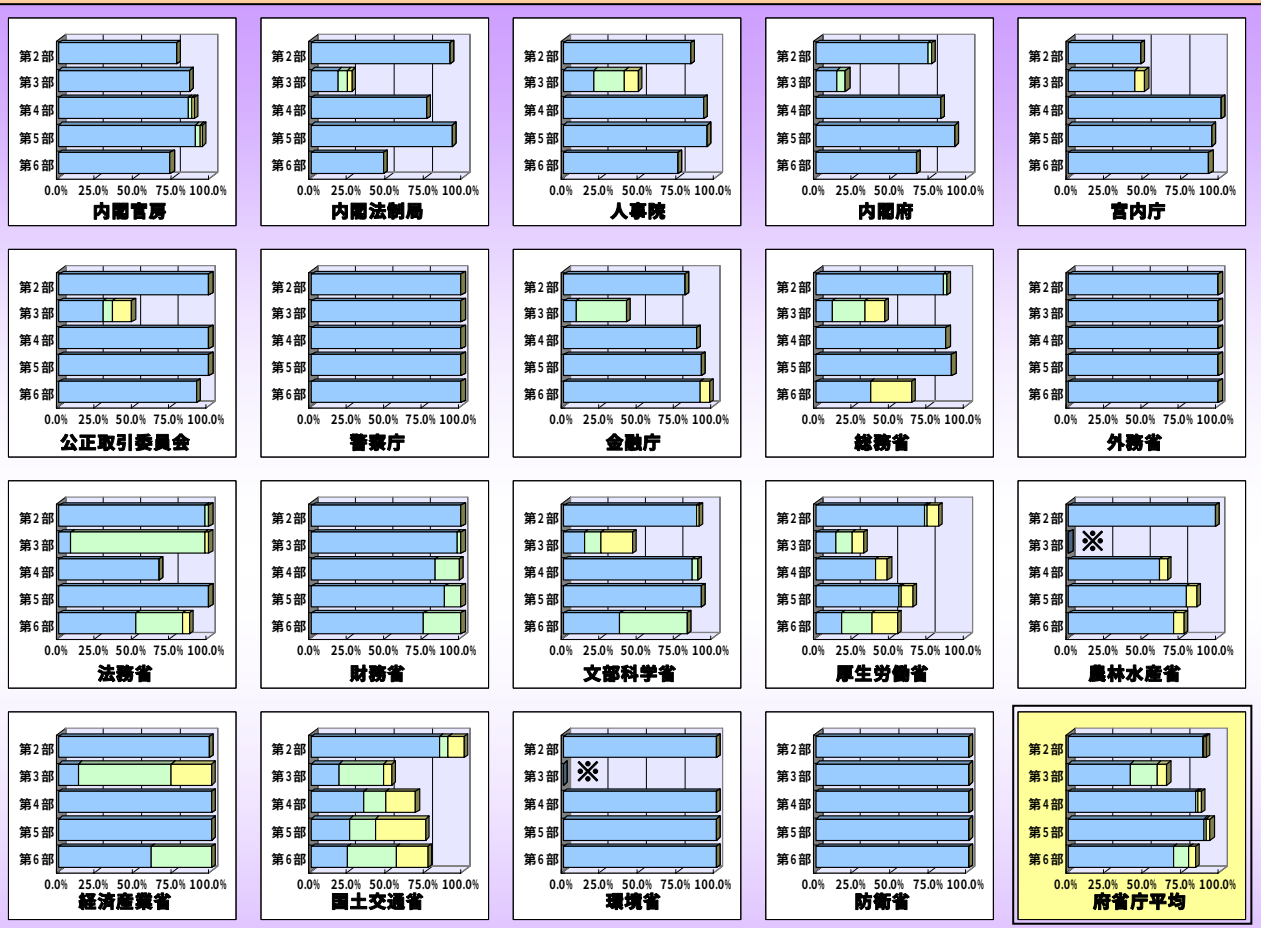
第2部　組織と体制
第3部　情報の取扱い
第4部　情報セキュリティ機能等
第5部　情報システムの構成要素
第6部　個別事項（外部委託等）

第○部の集計（実施率の算出例）

	実施状況	割合	実施率
遵守事項（a）	2人中1人実施	50%	割合の単純平均 75%
遵守事項（b）	100人中75人実施	75%	
遵守事項（c）	10人中10人実施	100%	

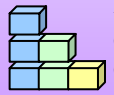
各府省庁の対策実施状況報告（2006年度）の集計結果②

到達率（把握した者のうち、責務が生じた全員が対策を実施した遵守事項の割合）



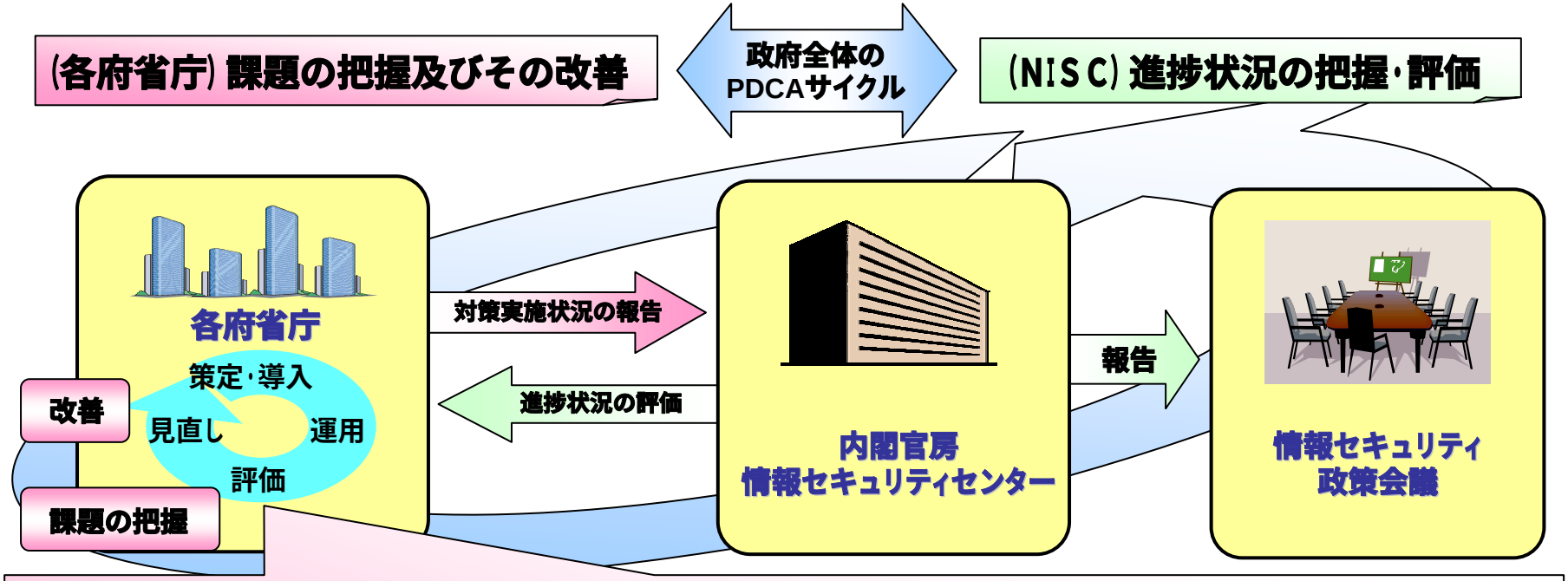
※：2006年度においては、独自の把握状況調査を実施（分析の対象から除外）

第2部　組織と体制
第3部　情報の取扱い
第4部　情報セキュリティ機能等
第5部　情報システムの構成要素
第6部　個別事項（外部委託等）



全員が対策を実施した遵守事項の割合
95%以上の者が対策を実施した遵守事項の割合
90%以上の者が対策を実施した遵守事項の割合

対策実施状況の傾向とその対応



【2006年度対策実施状況報告で把握した課題】

今後、改善が求められる事項

行政事務従事者

第3部　情報の取扱い

○ 情報の格付け・取扱制限に係る措置

第5部　情報システムの構成要素

○ 安全区域内における職員識別の徹底

情報セキュリティ責任者等

第2部　組織と体制

○ 情報セキュリティ教育の実施
○ 年度情報セキュリティ監査計画の策定

第4部　情報セキュリティ機能等

○ 電子署名の付与に必要な機能の導入
○ セキュリティ設計仕様書のST評価・ST確認

第6部　個別事項

○ 機器等の購入に係る選定基準等の整備
○ 外部委託先のアクセス範囲等に係る基準の整備

統一基準の導入初年度であり、十分な実施状況ではないが、課題は明確にされた。

集計方法と結果の見方

1．報告内容の集計 ：

把握率 ＝ Σ（各遵守事項について対策実施状況が把握できた者の数） / Σ（各遵守事項における報告対象者数）

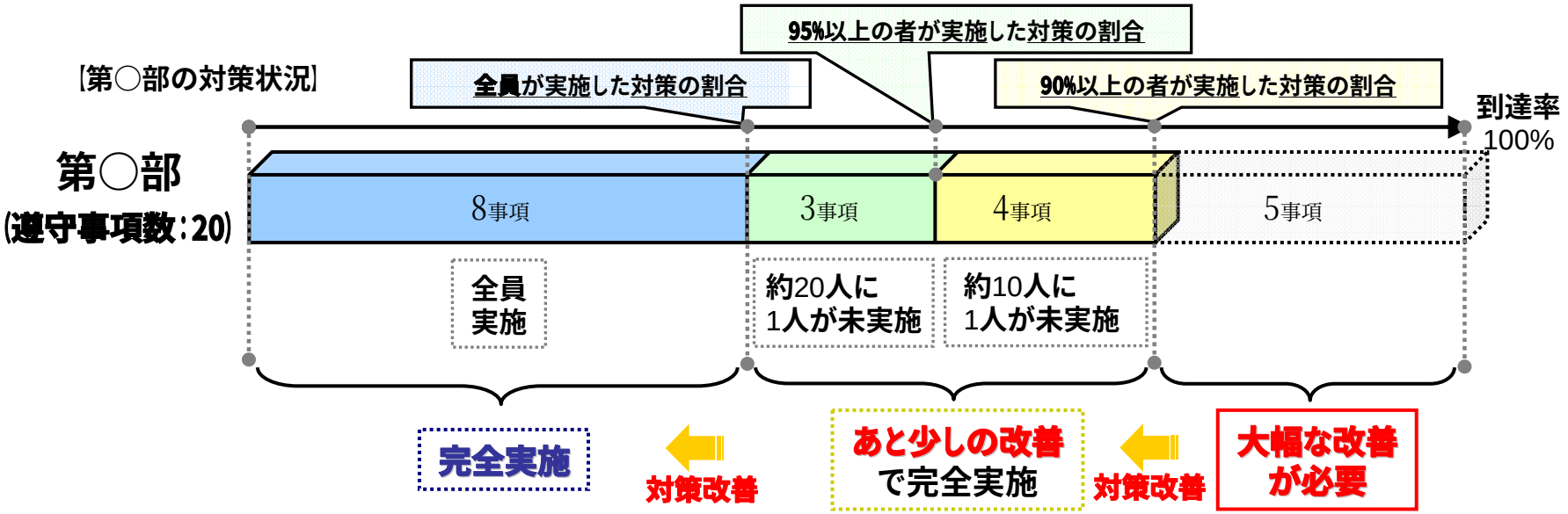
実施率 ＝ Σ（各遵守事項について責務が生じた者に占める実施した者の割合） / 責務が生じた遵守事項の数

実施率（政府平均） ＝ Σ（各府省庁の実施率） / 府省庁の数

到達率 ＝ 責務が生じた全員が必要な対策を実施した遵守事項の数 / 責務が生じた遵守事項の数

到達率（政府平均） ＝ Σ（各府省庁の到達率） / 府省庁の数

2．集計結果②の見方 ：



政府機関の情報セキュリティマネジメントの現状把握（２００６年度）

別添５

(1/2)

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 ・10府省庁で2%超　5府省庁で0.5%以下 ○ 8府省庁で、常任と同数以上の一時的な担当者が従事。特に、上記割合が低い府省庁において顕著に見られる。 ○ 情報セキュリティ担当者の平均経験年数： ・府省庁ごとの平均の分布は1年～2年、2年～3年が中心。 ⇒ 情報セキュリティ担当者の業務について今後ヒアリングを行い、その具体的内容と課題を把握する。
	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、推進体制は存在。 ・PMO、CIO補佐官、最高情報セキュリティアドバイザー等 ⇒ 推進体制の稼動状況について今後ヒアリングを行い、実効性、課題等を把握する。
	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。
		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、規程の見直しを行う必要性の有無を適時検討。 ○ 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現状把握（２００６年度）

(2/2)

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	○ 規程を理解やすいものとし、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
		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、ヒヤリハット情報を含む障害等の事例を収集する仕組みがある。 ○ 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。 ⇒ヒヤリハット情報活用の状況についてヒアリングを行い、実施範囲及び活用度合い等を把握する。
	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、受講状況管理不足 ○ eラーニングの活用は、現状では一部に限られている。 ・eラーニング教材のない府省庁が約半数 ⇒ 情報セキュリティ教育への取組み、改善についてヒアリングを行う。
実施	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。 ○ 調達仕様等についてPMO又はCIO補佐官による確認や助言を重視する府省庁もある。調達案件の多様性への対応。 ⇒ 調達・外部委託についてヒアリングを行い、課題等を把握する。

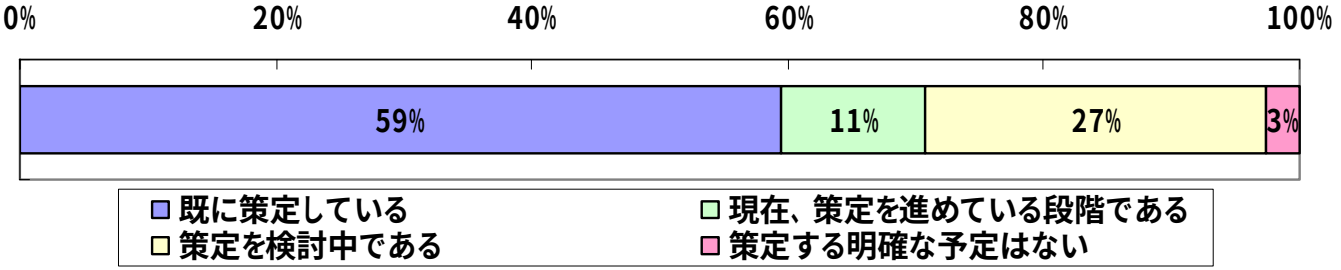
上記分類の他、大分類「実施」の業務改善、異常・障害等への対応、例外措置及び大分類「評価と改善」については、引き続いて調査。

独立行政法人等の情報セキュリティ対策の現状について

別添6

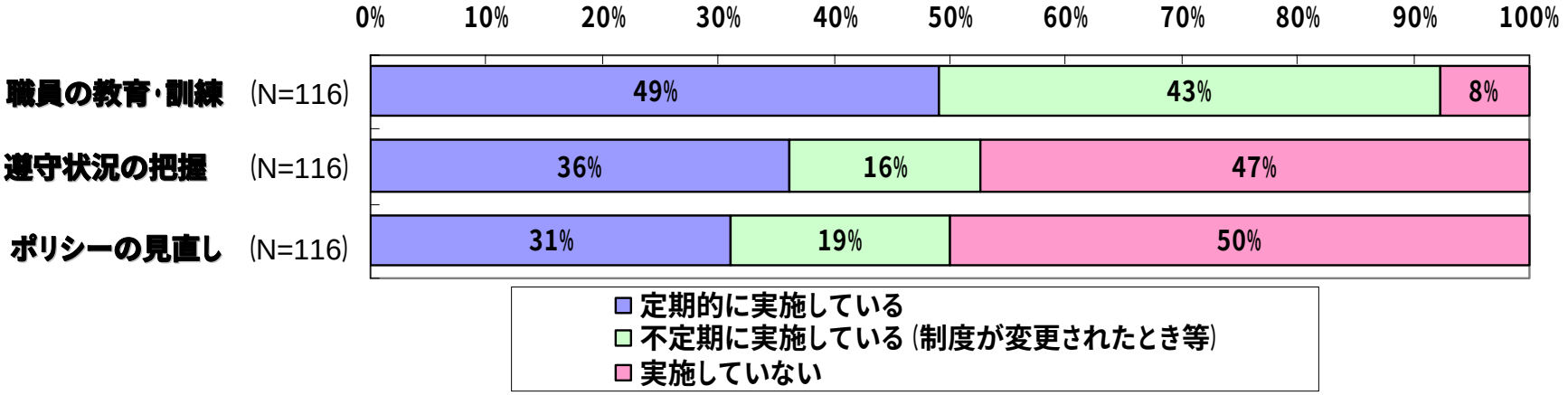
対象機関： 独立行政法人、国立大学法人及び大学共同利用機関法人 （195法人）
調査時点： 平成19年2月末時点

情報セキュリティポリシーの策定状況 (N=195)



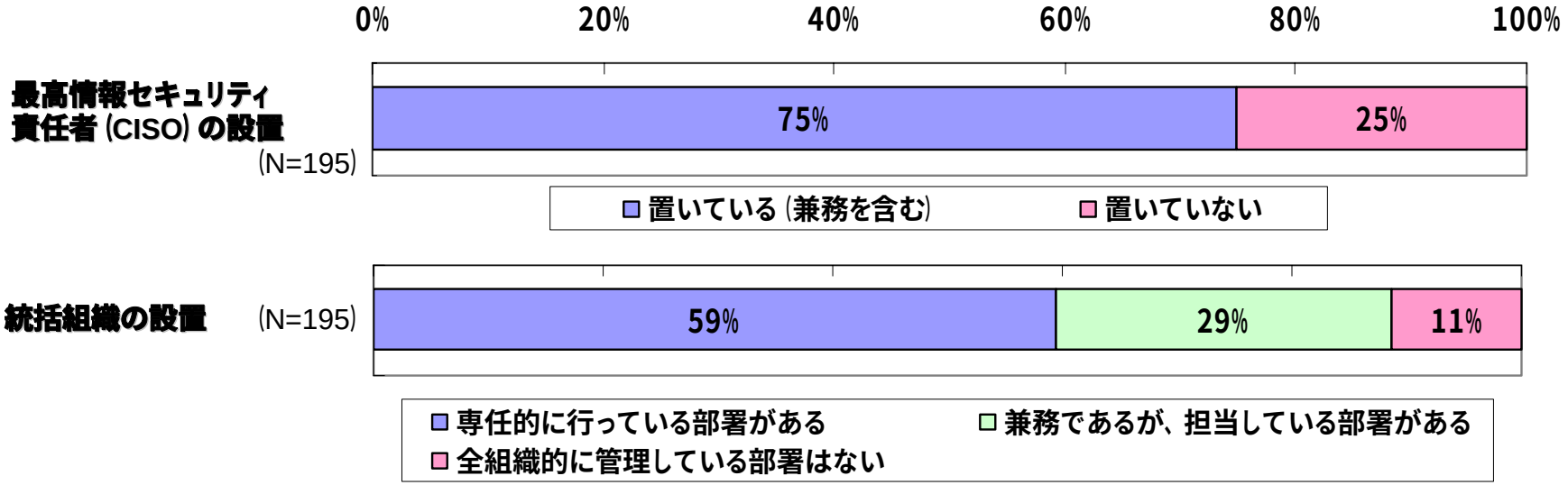
独立行政法人等において、全体の約6割で情報セキュリティポリシーが策定済みである。
まだ策定されていない残りの法人に対しても、引き続き、政府機関統一基準等を参考に、情報セキュリティポリシーの策定を促進していくことが必要である。

＜情報セキュリティポリシー策定済み法人の対策実施状況＞

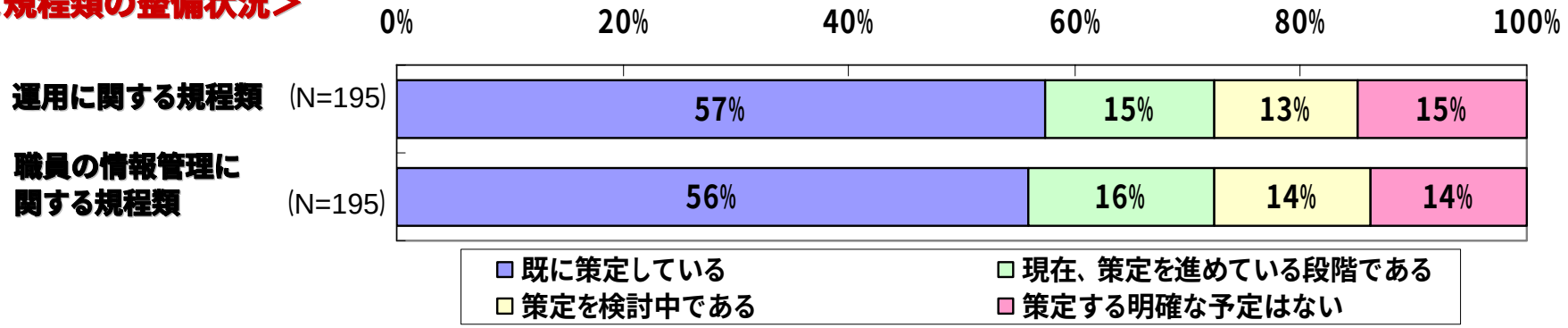


情報セキュリティポリシー策定済みの法人においても、ポリシーに基づく対策の実施（Do）、評価（Check）、見直し（Act）の徹底は不十分な状況であり、更にポリシーに基づく対策の実施が重要である。

＜管理体制の整備状況＞



＜規程類の整備状況＞



独立行政法人等においては、情報セキュリティポリシーの策定、組織・体制、規程類の整備等の計画策定（Plan）段階について半数以上の法人で取組みが進みつつある。一方、規程類の整備について、情報セキュリティポリシー策定状況に比べ、策定の予定がないと回答した法人が多くみられ、現場における実効性が懸念される。

別添７

企業・個人における情報セキュリティの評価指標

(1) 指標に関する基本的な考え方

ア 指標のあり方

企業・個人の対策実施領域においては、政府の役割は、政策により、各主体の情報セキュリティ意識を高めること、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など環境を整備すること、である。言いかえると、この対策実施領域が政府機関・重要インフラといった他の対策実施領域に比べて巨大な母数を抱え、かつ、多種多様な主体の集合体であるために一律の対策を設定することが困難であること等を踏まえ、企業・個人に対しては、環境整備等の間接的な働きかけを行い、各主体に「気付き」を起こさせる等、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、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を評価することが必要である。

イ 指標の分類

企業・個人に係る指標は、企業全体・個人全体の傾向を分析するという観点から、企業全体・個人全体の意識、対策、被害を見る「アウトカム指標」、企業・個人を支援する政府の姿を見る「アウトプット指標」とに分けて考えることとする。

ウ 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、の観点から、状況把握に有益な既存のデータ[1]の活用を原則とし、項目ごとに記載するが、このデータ一覧は、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。

また、現時点では把握されていないが、政府機関等が中心となって把握していくことが望まれるデータについても今後の課題として挙げており、今後、このような関連データの把握に向けた努力が期待される。情報セキュリティ対策ベンチマークのような各主体の「気付き」を促す施策の進捗状況データ等については、サンプル調査ではないことから、現時点で状況把握に活用することは困難であるが、今後、こういったデータの有効活用に向けた検討が進

1 「状況把握に有益な既存のデータ」とは、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。

められることも期待される。

なお、これらのデータの活用にあたっては、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こと、それぞれの統計と調査の質に幅があること、に留意することが必要である。

エ 政府機関の状況との対比

政府機関の情報セキュリティ対策は、企業・個人といったその他の情報セキュリティ対策の模範となることが期待される。したがって、政府機関自体の状況について、企業・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って、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、内閣官房は各省庁の協力を得て必要な調査を行うこととする。

(2) 企業･個人に係るアウトカム指標

「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。

ここでは、我が国政府の情報セキュリティ政策の結果として、各主体の対策や政府の取組みに比べると間接的であるが､何らかの効果が期待され､現象として把握できるものとして、「各主体の意識」､「各主体の対策」及び「インシデント・犯罪の発生」を企業個人に係る主なアウトカム指標として挙げる。ただし、これらの指標については、政府や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。

なお、評価に際しては、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。

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）

(3) 企業・個人に係るアウトプット指標

「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る。ここでは、我が国政府の情報セキュリティ政策の浸透度に関連するものとして、「企業を支援する政府の施策」「個人を支援する政府の施策」を企業・個人に係る主なアウトプット指標として挙げる。ただし、これらの指標については、政府や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。

なお、評価に際しては、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。

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。

(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８

企業・個人における現状の評価（統計資料）

○　ＩＳＭＳ認証の取得事業者数（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
ISMS認証 取得事業者数	276	418	720	528

○　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	合計
認証取得製品数 （新規認証）	2	5	17	21	42	87
認証取得製品数 （保証継続）	―	―	3	10	9	22

○　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
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
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）

○　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
受験者数	27,913	33,581	27,744	22,563
合格者数	3,149	4,174	3,812	3,337

○　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
CSIRTの数	7	8	13

※　ここにあげているのは、ＪＰＣＥＲＴ／ＣＣと連携している国内のＣＳＩＲＴの数である。

○　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）

単位：か所

	16年3月末	17年3月末	18年2月
担当窓口数	64	122	182

○　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）

（研修を受けた教員総数）

単位：特に記載がない場合、人

	15年度	16年度	17年度
教員総数	881,873	880,343	876,715
各年度中に研修を受けた教員数	524,853	504,935	458,763
割合（%）	59.5%	57.4%	52.3%

（研修内訳）

単位：特に記載がない場合、人

	15年度	16年度	17年度
各年度中に研修を受けた教員数	524,853	504,935	458,763
国及び教育委員会が行う研修を受講	130,430	128,008	110,144
校内研修を受講	470,429	455,153	409,393
大学等の公開講座等の研修を受講	5,030	6,906	5,565
各種研究団体の主催する研修を受講	31,470	29,753	25,402
民間企業が主催する研修を受講	17,969	15,137	13,689
その他	35,322	37,585	100,441

※　複数回答を含むため、各研修受講者の和と各年度中に研修を受けた教員数は

一致しない。

○　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
開催数（か所）	11	28	71	98
参加者総数（人）	2,069	3,581	5,844	−
うち、一般参加者	1,955	3,170	5,073	−

○　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。

○　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 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。

○　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）

（※　今年度の報告書案を作成する時点では、担当省において調査結果を精査中。）

○　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

※　何れも、複数回答による。

※　平成17年と平成18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＞

（全体）

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

※　何れも、複数回答による。

※　平成17年と平成18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）

（※　今年度の報告書案を作成する時点では、担当省において調査結果を精査中。）

○　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）

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 (%)		
		17年調査	16年調査	増減	17年調査	16年調査	増減	17年調査	16年調査	増減	17年調査	16年調査	増減
システムトラブル	システム・トラブル計	56.4	-	-	22.8	-	-	3.1	-	-	17.8	-	-
	システム破壊・サーバ停止	79.0	75.8	3.2	5.2	6.2	△ 1.0	0.5	0.5	0.0	15.4	17.4	△ 2.0
	Dos攻撃	52.7	49.8	2.9	20.7	20.5	0.2	3.2	3.3	△ 0.1	23.4	26.5	△ 3.1
	ホームページやファイル、データの改ざん	59.2	56.3	2.9	16.7	17.1	△ 0.4	1.7	2.0	△ 0.3	22.3	24.6	△ 2.3
	自然災害による障害（地震、火災等の問題）	61.9	57.8	4.1	16.6	18.6	△ 2.0	0.9	1.5	△ 0.6	20.5	22.2	△ 1.7
不正アクセス	不正アクセス計	51.8	-	-	25.2	-	-	3.2	-	-	19.9	-	-
	IP・メールアドレス詐称	53.1	51.1	2.0	23.6	23.4	0.2	2.2	2.4	△ 0.2	21.0	23.1	△ 2.1
	リソースの不正使用	51.3	49.0	2.3	22.7	22.2	0.5	2.2	2.3	△ 0.1	23.7	26.6	△ 2.9
	内部者の不正アクセス	58.5	55.8	2.7	17.8	18.1	△ 0.3	1.5	1.8	△ 0.3	22.2	24.2	△ 2.0
コンピュータウィルス	コンピュータウィルス計	59.6	-	-	20.5	-	-	2.5	-	-	17.4	-	-
	ウィルスやワーム	77.1	75.4	1.7	15.5	17.1	△ 1.6	1.6	1.5	0.1	5.8	6.0	△ 0.2
	スパムメールの中継利用等	57.2	53.4	3.8	20.0	21.1	△ 1.1	1.9	1.6	0.3	20.9	23.8	△ 2.9
	トロイの木馬	60.7	55.8	4.9	18.2	20.1	△ 1.9	1.5	1.4	0.1	19.6	22.7	△ 3.1
重要情報の漏洩	重要情報の漏洩計	61.8	-	-	17.0	-	-	2.0	-	-	19.3	-	-
	パスワードの盗用	64.9	63.0	1.9	12.5	12.4	0.1	0.9	1.0	△ 0.1	21.6	23.6	△ 2.0
	内部者による情報漏洩	69.4	66.7	2.7	8.6	9.2	△ 0.6	0.7	0.8	△ 0.1	21.3	23.3	△ 2.0
	委託先による情報漏洩	65.4		-	10.7		-	1.4		-	22.5		-
	ノートパソコン及び携帯記憶媒体等の盗難・紛失	65.8		-	13.9		-	1.1		-	19.2		-
その他	その他計	23.9	-		18.5	-		3.3	-		54.3	-	
	ホームページ上での誹謗中傷等	39.8	40.0	△ 0.2	30.6	27.8	2.8	5.3	5.3	0.0	24.3	26.9	△ 2.6
	その他	6.1	7.3	△ 1.2	2.3	3.2	△ 0.9	1.1	1.0	0.1	90.4	88.6	1.8

※　回答企業数　　17年調査：4,241社　　16年調査：3,838社
※　調査対象期間　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。

○　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			
	17年	16年	17年	16年	17年	16年	17年	16年	17年	16年
リスク分析	30.6 (0.9)	20.4	14.5	16.6	47.1	51.9	8.7	11.1	4,138	3,944
セキュリティポリシーの策定	43.9 (0.7)	29.7	15.5	21.4	34.8	40.1	6.6	8.9	4,224	3,944
全社的なセキュリティ管理者の配置	47.1 (0.5)	35.2	12.2	16.7	35.5	40.9	5.7	7.3	4,233	3,944
部門ごとのセキュリティ管理者の配置	34.1 (0.4)	24.4	12.2	16.5	42.3	46.2	11.8	13.0	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			
	17年	16年	17年	16年	17年	16年	17年	16年
リスク分析	65.3	66.0	8.5	6.2	26.2	27.7	1,297	739
セキュリティポリシーの策定	63.3	64.1	11.4	8.6	25.3	27.4	1,814	1,085
全社的なセキュリティ管理者の配置	70.4	69.8	10.3	7.3	19.3	22.9	1,841	1,129
部門ごとのセキュリティ管理者の配置	65.2	65.1	13.3	10.7	21.5	24.2	1,384	848

※　調査対象期間　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。

○　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			
	17年	16年	17年	16年	17年	16年	17年	16年	17年	16年
重要なシステムへの内部でのアクセス管理	57.9 (0.4)	50.7	10.5	13.5	25.1	27.7	6.9	8.2	4,247	3,944
データの暗号化(PKIを含む)	27.9 (0.3)		16.0		41.2		15.2		4,167	3,944
外部接続へのファイアウォールの配置	73.4 (1.0)	66.7	5.8	6.9	15.4	18.7	6.4	7.7	4,249	3,944
セキュリティ監視ソフトの導入	49.1 (2.1)	40.6	14.6	16.8	30.8	33.8	7.6	8.8	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			
	17年	16年	17年	16年	17年	16年	17年	16年
重要なシステムへの内部でのアクセス管理	80.7	83.0	4.7	3.8	14.6	13.2	2,171	1,441
データの暗号化(PKIを含む)	72.6		4.8		22.7		1,217	
外部接続へのファイアウォールの配置	87.1	87.9	1.8	1.9	11.1	10.2	2,583	1,738
セキュリティ監視ソフトの導入	81.2	80.3	3.6	3.3	15.2	16.4	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
※　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。
※　「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)
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
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
ファイアウォールの設置	52.2	46.4	46.8
ID、パスワードによるアクセス制御	54.2	37.6	44.6
データやネットワークの暗号化	11.0	6.1	10.7

○　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
実施している	24.9%	35.5%	45.9%
実施を予定している	9.8%	12.4%	9.9%
実施はしていないが必要性を感じる	60.5%	49.2%	41.6%
実施の必要性を感じない	3.7%	2.2%	1.2%
無回答	1.1%	0.6%	1.5%
（参考）発送数	2,000	2,000	2,500
（参考）回収数	732	628	606
（参考）回収率	36.6%	31.4%	24.2%

○　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）

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			
	17年	16年	17年	16年	17年	16年	17年	16年	17年	16年
従業員に対する情報セキュリティ教育	41.1 (1.0)	27.2	15.6	21.6	39.7	45.6	4.6	5.6	4,241	3,944

（効果）

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			
	17年	16年	17年	16年	17年	16年	17年	16年	17年	16年
従業員に対する情報セキュリティ教育	41.1 (1.0)	27.2	15.6	21.6	39.7	45.6	4.6	5.6	4,241	3,944

※　調査対象期間　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。

○　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）

クライアント			15年	16年	17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%
		企業	28.6%	27.7%	32.2%
		自治体	33.6%	38.1%	31.5%
定期的に適用している	全体		23.5%	25.2%	32.2%
		企業	21.2%	21.0%	27.6%
		自治体	26.7%	33.5%	43.2%
気がついたときに適用している	全体		19.5%	18.2%	20.0%
		企業	17.2%	19.6%	23.1%
		自治体	22.6%	15.5%	12.3%
ほとんど適用していない	全体		13.8%	9.5%	12.2%
		企業	14.6%	10.4%	12.4%
		自治体	12.7%	7.7%	11.5%
分からない	全体		10.2%	13.3%	2.4%
		企業	15.1%	18.1%	3.0%
		自治体	3.4%	3.9%	0.8%
無回答	全体		2.3%	2.6%	1.4%
		企業	3.4%	3.3%	1.7%
		自治体	0.9%	1.3%	0.6%
(参考) 回答総数	全体		1,115	1,150	1,701
		企業	651	762	1,206
		自治体	464	388	495

ネットワークサーバ			15年	16年	17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%
		企業	24.9%	22.6%	29.6%
		自治体	43.5%	42.3%	33.1%
定期的に適用している	全体		20.8%	19.9%	33.4%
		企業	12.4%	12.1%	27.7%
		自治体	32.5%	35.3%	47.3%
気がついたときに適用している	全体		10.0%	6.3%	8.2%
		企業	9.8%	5.8%	8.3%
		自治体	10.3%	7.5%	8.1%
ほとんど適用していない	全体		16.4%	12.6%	7.3%
		企業	23.0%	16.0%	8.3%
		自治体	7.1%	5.9%	4.8%
分からない	全体		13.0%	21.6%	9.5%
		企業	20.6%	30.4%	12.4%
		自治体	2.4%	4.1%	2.4%
無回答	全体		7.1%	10.3%	10.9%
		企業	9.2%	13.1%	13.7%
		自治体	4.1%	4.9%	4.2%
(参考) 回答総数	全体		1,115	1,150	1,701
		企業	651	762	1,206
		自治体	464	388	495

ローカルサーバ			15年	16年	17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%
		企業	21.8%	20.7%	24.5%
		自治体	29.7%	31.4%	24.6%
定期的に適用している	全体		22.8%	22.7%	35.7%
		企業	16.9%	15.9%	30.6%
		自治体	31.0%	36.1%	48.1%
気がついたときに適用している	全体		14.7%	13.3%	14.5%
		企業	14.1%	12.2%	16.0%
		自治体	15.5%	15.5%	10.7%
ほとんど適用していない	全体		17.8%	15.5%	16.2%
		企業	20.4%	18.5%	17.7%
		自治体	14.2%	9.5%	12.5%
分からない	全体		13.2%	17.7%	5.4%
		企業	18.9%	24.3%	6.5%
		自治体	5.2%	4.9%	2.8%
無回答	全体		6.4%	6.4%	3.7%
		企業	7.8%	8.4%	4.7%
		自治体	4.3%	2.6%	1.2%
(参考) 回答総数	全体		1,115	1,150	1,701
		企業	651	762	1,206
		自治体	464	388	495

			15年	16年	17年
(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)
		企業	16.6% (663/4,000)	19.3% (770/4,000)	21.9% (1,206/5,500)
		自治体	46.5% (465/1,000)	39.0% (390/1,000)	46.7% (495/1,061)

※　この表で言う「ネットワークサーバ」とは、メールサーバ、ウェブサーバなどを指し、「ローカルサーバ」とは、ファイルサーバ、プリントサーバなどを指す。

○　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
9割以上のパソコンに導入済	全体		70.4%	73.8%	86.4%
		企業	56.8%	63.9%	82.3%
		自治体	89.4%	93.3%	96.6%
半数以上のパソコンに導入済	全体		7.5%	7.2%	4.9%
		企業	10.1%	9.6%	6.4%
		自治体	3.9%	2.6%	1.4%
半数未満のパソコンに導入済	全体		10.3%	10.9%	5.5%
		企業	14.0%	15.0%	7.2%
		自治体	5.2%	2.8%	1.4%
導入していない	全体		8.0%	7.1%	2.4%
		企業	12.6%	10.4%	3.2%
		自治体	1.5%	0.8%	0.2%
無回答	全体		3.8%	1.0%	0.8%
		企業	6.5%	1.2%	0.9%
		自治体	-	0.5%	0.4%
(参考) 回答総数	全体		1,115	1,150	1,701
		企業	651	762	1,206
		自治体	464	388	495

ネットワークサーバ		15年	16年	17年
9割以上のパソコンに導入済	全体	65.8%	58.0%	70.8%
	企業	53.1%	47.6%	65.5%
	自治体	83.6%	78.4%	83.8%
半数以上のパソコンに導入済	全体	3.5%	4.4%	4.3%
	企業	3.4%	4.2%	4.1%
	自治体	3.7%	4.9%	4.8%
半数未満のパソコンに導入済	全体	5.2%	3.0%	3.1%
	企業	6.9%	2.9%	3.3%
	自治体	2.8%	3.1%	2.6%
導入していない	全体	21.4%	27.4%	14.9%
	企業	31.6%	35.8%	18.5%
	自治体	7.1%	10.8%	6.3%
無回答	全体	4.0%	7.2%	6.8%
	企業	4.9%	9.4%	8.6%
	自治体	2.8%	2.8%	2.4%
(参考) 回答総数	全体	1,115	1,150	1,701
	企業	651	762	1,206
	自治体	464	388	495

ローカルサーバ		15年	16年	17年
9割以上のパソコンに導入済	全体	55.5%	60.6%	74.1%
	企業	44.5%	49.9%	69.7%
	自治体	70.9%	81.7%	84.8%
半数以上のパソコンに導入済	全体	5.6%	5.5%	7.1%
	企業	4.8%	5.8%	7.2%
	自治体	6.7%	4.9%	6.9%
半数未満のパソコンに導入済	全体	4.9%	5.1%	4.7%
	企業	5.7%	5.2%	4.8%
	自治体	3.9%	4.9%	4.4%
導入していない	全体	29.0%	25.0%	11.8%
	企業	39.3%	34.3%	15.6%
	自治体	14.4%	7.0%	2.4%
無回答	全体	5.0%	3.7%	2.4%
	企業	5.7%	4.9%	2.7%
	自治体	4.1%	1.5%	1.4%
(参考) 回答総数	全体	1,115	1,150	1,701
	企業	651	762	1,206
	自治体	464	388	495

		15年	16年	17年
(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)
	企業	16.6% (663/4,000)	19.3% (770/4,000)	21.9% (1,206/5,500)
	自治体	46.5% (465/1,000)	39.0% (390/1,000)	46.7% (495/1,061)

※　この表で言う「ネットワークサーバ」とは、メールサーバ、ウェブサーバなどを指し、「ローカルサーバ」とは、ファイルサーバ、プリントサーバなどを指す。

○　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）

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			
	17年	16年	17年	16年	17年	16年	17年	16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	10.6　(0.1)	8.1	7.2	7.5	50.8	52.0	31.5	32.4	4,165	3,944
内部による定期的な情報セキュリティ監査	18.8　(0.3)	12.6	12.0	13.5	51.9	54.2	17.6	19.8	4,181	3,944

（効果）

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			
	17年	16年	17年	16年	17年	16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	76.1	73.9	4.2	5.1	19.7	21.0	457	257
内部による定期的な情報セキュリティ監査	77.1	73.7	5.7	4.0	17.2	22.2	825	445

※　調査対象期間　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）

利用しない理由		15年	16年	17年	順位変化（15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%	①→①→①
	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%	②→②→②
	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%	④→③→③
	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%	⑥→④→④
	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%	⑦→⑦→⑥
	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%	⑧→⑧→⑦
	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%	⑨→⑤→⑧
	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%	⑤→⑨→⑨
	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%	⑪→⑪→⑪
	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%	⑩→⑩→⑫
	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%	⑭→⑬→⑬
	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%	⑫→⑭→⑭
	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からない		2.6%	3.4%	3.1%	
（内訳）	利用経験有	3.6%	4.6%	3.9%	⑯→⑮→⑮
	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%	⑰→⑯→⑯
	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%	⑮→⑯→⑰
	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%	⑫→⑫→⑩
	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%	③→⑥→⑤
	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	

○　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）

（※　今年度の報告書案を作成する時点では、担当省において調査結果を精査中。）

○　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者）	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（その他）	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・無職	98.7%	72.0%	66.8%	66.3%	31.4%	4.9%	6.1%	0.7%	1,017
パート・アルバイト	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	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%	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%	0.4%
会社員等（情報システム関係の技術者）	98.5%	91.3%	93.4%	95.7%	42.6%	23.4%	89.5%	50.4%	26.8%	1.0%
会社員・公務員・派遣社員（その他）	98.2%	70.9%	81.1%	88.3%	16.0%	11.4%	79.7%	25.4%	8.4%	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%	1.1%
専業主婦／家事手伝い・無職	97.8%	51.0%	68.9%	75.0%	7.0%	5.2%	66.3%	20.0%	2.6%	1.7%
パート・アルバイト	97.0%	53.0%	66.9%	73.8%	9.2%	7.4%	67.2%	22.5%	4.1%	2.0%
学生	96.7%	64.0%	70.3%	79.1%	21.7%	14.0%	80.9%	35.9%	13.2%	2.4%
その他	97.5%	58.5%	75.3%	86.3%	10.5%	6.9%	78.7%	26.0%	5.2%	0.5%

※　平成17年と平成18年では調査方法が異なる。

○　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）

＜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

○　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
ウィルスチェックソフトの導入	32.0%	35.9%	36.7%
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%
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%
OS、ブラウザのアップデート	17.8%	19.4%	17.1%
ファイアウォールの使用	8.9%	12.3%	14.4%
ファイル等のバックアップ	13.4%	8.1%	8.3%
スパイウェア対策ソフトの導入			8.0%
メールソフトのアップデートや変更	3.8%	5.6%	6.1%
パスワードの定期的な変更		2.1%	2.7%
アカウント毎にパスワードを複数使い分け		1.7%	2.3%
その他	2.4%	1.6%	1.4%
何も行っていない	26.5%	14.6%	22.1%
無回答	22.4%	25.8%	20.9%
(参考) 回答数	6,936	8,776	9,174

※　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）

（※　今年度の報告書案を作成する時点では、担当省において調査結果を精査中。）

○　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）

全体 (回答:5142)	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%

（職種別）

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。

○　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）

情報セキュリティ上のトラブル経験（回答企業数：4,370社）		17年 回答数	17年 比率
	有	2,418	55.3%
	無	1,952	44.7%

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）	
		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%
	システム破壊･サーバ停止	730	28.1%	679	28.2%
	Dos攻撃	259	10.0%	215	8.9%
	ホームページやファイル、データの改ざん	62	2.4%	57	2.4%
	自然災害による障害（地震、火災等の問題）	247	9.5%	209	8.7%
不正アクセス	不正アクセス計	398	15.3%	343	14.2%
	IP･メールアドレス詐称	355	13.7%	280	11.6%
	リソースの不正使用	40	1.5%	37	1.5%
	内部者の不正アクセス	62	2.4%	57	2.4%
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%
	ウィルスやワーム	2,276	87.7%	1,957	81.2%
	スパムメールの中継利用等	400	15.4%	332	13.8%
	トロイの木馬	507	19.5%	423	17.6%
重要情報の漏洩	重要情報の漏洩計	48	1.9%	491	20.4%
	パスワードの盗用	21	0.8%	15	0.6%
	内部者による情報漏洩	34	1.3%	39	1.6%
	委託先による情報漏洩			29	1.2%
	ノートパソコン及び携帯記憶媒体等の盗難･紛失			458	19.0%
その他	その他計	137	5.3%	139	5.8%
	ホームページ上での誹謗中傷等	128	4.9%	129	5.4%
	その他	10	0.4%	10	0.4%

※　調査対象期間　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。

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

○　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)
ウイルス等の感染	56.1%	45.5%	32.8%
ノートPC盗難	12.6%	12.3%	8.3%
スパイウェアの感染			8.3%
内部者のネットワーク悪用	6.0%	4.0%	2.3%
DoS攻撃	4.4%	4.3%	2.3%
メールの不正中継	3.7%	2.1%	1.7%
Webや掲示板上での誹謗中傷	3.8%	3.2%	1.5%
踏み台	4.5%	1.1%	1.3%
ホームページの改竄	1.9%	0.3%	1.3%
なりすまし	3.8%	4.5%	1.0%
盗聴	0.1%	0.2%	0.7%
その他情報機器盗難	1.0%	1.0%	0.5%
情報漏洩	0.4%	1.4%	0.5%
システム破壊･データ改竄	0.8%	0.3%	0.5%
インターネット上の著作権侵害	0.3%	0.5%	0.2%
フィッシング		0.0%	0.0%
ネットワークを利用した詐欺		0.0%	0.0%
その他	0.7%	1.0%	1.0%
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%	

○　不正アクセス行為の発生状況（警察庁）

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

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

※　平成16年７月から制度開始。

○　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）

	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%

（職種別）

	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%

○　コンピュータウィルス遭遇率（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）

	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15年	平成16年	平成17年	平成15年	平成16年	平成17年	平成15年	平成16年	平成17年	平成15年	平成16年	平成17年
総数	1,115	1,150	1,701	22.2%	20.9%	15.3%	47.4%	48.0%	53.7%	29.8%	31.1%	29.9%	0.6%	-	1.1%
企業	651	762	1,206	21.4%	21.3%	17.6%	35.5%	37.5%	47.9%	42.4%	41.2%	33.2%	0.8%	-	1.3%
地方自治体	464	388	495	23.3%	20.1%	9.7%	64.2%	68.6%	67.9%	12.1%	11.3%	21.8%	0.4%	-	0.6%

○　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。

○　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）

17年		市場規模		電子商取引化率	
		日本	米国	日本	米国
企業間電子商取引	狭義EC	140兆円	92兆円	12.9%	5.7%
	広義EC	224兆円	189兆円	20.6%	11.9%

			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）

17年	市場規模		電子商取引化率	
	日本	米国	日本	米国
消費者向け電子商取引	3.5兆円	15.9兆円	1.2%	2.4%

		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。