セキュア・ジャパン２００７

－ITを安全・安心に利用できる環境づくりのための情報セキュリティ対策の底上げ－

（案）

情報セキュリティ政策会議

２００７年　月　日

目次

第1章　セキュア･ジャパン2006に基づく取組みと評価について

第1節　セキュア･ジャパン2006に基づく取組みの背景

ITは、その活用を通じて我が国の国民生活･社会経済活動を豊かにしてきた。のみならず、ITは我が国の国民生活･社会経済活動に深く浸透し、社会基盤化してきたことから、あらゆる活動において内在的な存在として欠かせないものとなってきている。

他方で、我々の活動を前向きに支えるITの利用が国民生活･社会経済活動の安全･安心に大きな影響を及ぼす事態も発生してきている。実際、情報セキュリティ面でのリスクは増大しており、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年には政府機関のウェブサーバーへのサイバー攻撃、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えい、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。

このような事態に対する対策を抜本的に強化すべく、官民における統一的･横断的な情報セキュリティ対策を推進するために策定されたのが、我が国の情報セキュリティ対策に係る中長期の戦略である、「第1次情報セキュリティ基本計画」（2006年2月2日情報セキュリティ政策会議決定、以下「基本計画」という。）である。そして、この基本計画を受け、2006年度における我が国の情報セキュリティ対策の政府の重点施策を定める年度計画（セキュア･ジャパン2006（2006年6月15日情報セキュリティ政策会議決定）（以下「SJ2006」という。））に基づき、政府機関を始めとする各対策実施主体が初年度の取組みを行ったところである。

第2節　2006年度の重点目標と取組みの柱立て

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。

そして、「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、各府省庁が2006年度に実施すべき133の具体的な施策が盛り込まれた。

第3節　2006年度の評価

SJ2006に基づく取組み及び取組みを受けた現状に関しては、内閣官房情報セキュリティセンター（National Information Security Center （NISC））（以下、第１章及び第2章の本文において「NISC」という。）が評価等[1]を行った上で、「2006年度の情報セキュリティ政策の評価等」（以下「評価2006」という。）を取りまとめ、情報セキュリティ政策会議に対して報告がなされた。ここでは、評価2006が示唆する方向性などを抽出するとともに、2007年度の年度計画の策定の前提となる現状認識を明確にし、2006年度の評価を行う。この際の主眼は、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すべて網羅的に把握することにあるのではなく、2007年度の政策を検討するにあたって本質的な現状を把握することにある。

本書では、こうした「現状認識」などを踏まえつつ、第2章において2007年度の基本方針について述べ、第3章から第5章において2007年度の実際に取り組む施策をまとめる。また、評価を通じて中期的な課題なども明らかになることから、第6章においては、2008年度の重点施策の方向性について検討を行う。

1．施策の取組み結果に関する評価･分析

SJ2006において2006年度中に推進するとされた133の具体的施策の取組み結果について、評価2006では以下のとおり分類され、評価がなされた。

○ A ：当初の予定どおり施策を推進することができた施策。
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

[1] 本書第1章及び第2章においては、「「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」（2007年2月2日情報セキュリティ政策会議決定）の「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。

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できなかったが、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できる施策

○ 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できなかったが、それが政府機関以外の事情による施策

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、予定どおり推進することができたと評価された。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できたものの、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考えられる。

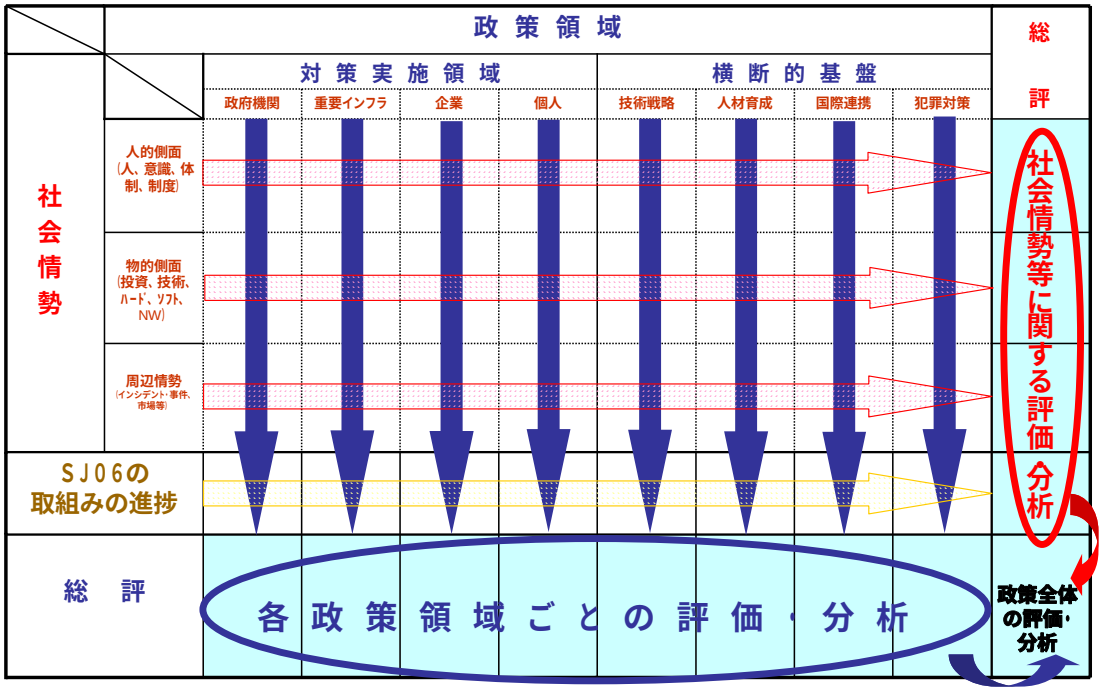
以上を総括すると、SJ2006において、2006年度中に推進するとされた133の具体的施策については、各府省庁において着手がなされ、担当者等の尽力もあって概ね順調に進捗したと言える。しかし、その多くは、今後も引き続き取組みが必要とされる施策、発展的な更なる取組みを必要とする施策であり、来年度以降も取り組みを継続する必要があるが、一部の施策については、今後も引き続き推進して行くための体制や人員等が不十分であると考えられ、これを解決する必要がある。

2． 施策の取組みによる社会的変化に関する評価･分析

ここでは、評価2006における検討の枠組みにのっとって、基本計画に基づく政策領域（対策実施領域、横断的基盤）という、いわば横軸ごとの検討に加え、縦軸として政策領域横断的な社会情勢について、人的側面（人材、意識、体制･制度）、物的側面（投資、技術、ハード、ソフト、ネットワーク）、周辺情勢（インシデント･事件、市場等）の3つの側面から検討を行うことで、縦横の異なった角度から評価･分析を行うこ

ととする。

２００６年度の情報セキュリティ政策の評価･分析に係る検討枠組み



(a) 政策領域

(ア) 政府機関･地方公共団体

２００６年度には、重点検査等に基づく評価によって、対策水準が十分ではない対策事項等が明らかになり、各府省庁は対策の改善の必要性に気づき、改善に向けた努力を行うなど、情報セキュリティ対策のＰＤＣＡサイクルも概ね確立されたと言える。また、必要な予算の獲得に向けた努力も見られた。しかし、情報セキュリティ管理体制の形はできつつあるが、実質的に取組みを推進するための人員が不足している状況にある。今後は、各府省庁のＰＤＣＡの各取組みが確実かつ効果的に進められ、ＰＤＣＡサイクルが適切に機能しているか検証していく必要がある。また、各種業務･システムの最適化を含め、電子政府の取組みが推進されているが、その際、情報セキュリティの観点を考慮することも不可欠となっている。

(イ) 重要インフラ

２００６年度は、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き予定の取組みを行うべく十分な努力が行われた。ただし、この結果、重要インフラ各事業分野に係る情報セキュリティの状況がどのように改善したのかという点については、初年度の取組みが終わった段階でもあり、依然として客観情報により判断

するには至らない。いずれにせよ、今後も、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、継続的に取り組んでいくことが必要である。

⑵ ウ） 企業

ウイルス対策ソフト等の使用率の向上や、情報セキュリティ確保のための体制整備及び事業継続計画の策定など、取組みを着実に強化しつつ実施している状況にあると言える。また、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が出るなど、情報セキュリティ上の問題を起こすことが当該企業にとって大きな経済的損失につながるという認識の高まりもあり、企業総体としては、対策が進展しつつあると考えられる。

しかし、情報流出が依然として続いているのも事実であり、すべての企業において情報セキュリティの意識が徹底されているとは言えず、適切な対策が講じられているとも言えない状況にある。特に、先進的な企業とそうでない企業、大企業と中小企業の間の格差が存在しているものと考えられる。

⑵ エ） 個人

個人を対象とする情報セキュリティ教育や広報啓発活動等が強化されている状況にあり、ウイルス対策ソフトの売れ行きも堅調であるなどの状況も見られることなどを考慮すると、情報セキュリティに対する意識が高まり、また知識が浸透しつつあると思われる。

しかし、依然として対策を講じていないとする個人が無視できない割合で存在し、個人を標的とする新しいリスクも発生している。こうしたことへの対応が今後の課題であると考えられる。

⑵ オ） 情報セキュリティ技術戦略の推進

ＩＴ関連製品の中でセキュリティ製品は増加傾向にあるが、日本発のセキュリティ技術はまだ少なく、研究開発・技術開発に対する公的研究資金の重点的な投入や投資効率の向上などによる底上げ効果が期待される。また、産学官の連携による「高セキュリティ機能を実現する次世代ＯＳ環境の開発」が先導的な役割を果たすことも期待される。

（カ） 情報セキュリティ人材の育成・確保

情報セキュリティ人材の育成に向けた官民における取組みが展開されつつあるが、依然として人材及びそのスキルの不足感は否めず、十分な人材の育成・確保に向けては緒についたばかりという状況であると考えられる。

(キ) 国際連携・協調の推進

国際会合等における我が国の取組みの紹介や、NISCのウェブサイトによる広報活動を通じ、我が国の情報セキュリティ政策に係る認知度の向上は一定の成果が得られた。

しかし、依然として取組みは第一歩目を踏み出したに過ぎず、多国間の枠組みで情報セキュリティに係るリスクの低減・解消を図ることや、我が国の知見の諸外国への提供など取組みの余地は大きい状況である。

(ク) 犯罪の取締り及び権利利益保護・救済

基本計画の初年度である2006年度には、一定の取組みがなされたものと評価できる。しかし、サイバー空間での犯罪や不法行為は多発しており、さらなる対策の強化が喫緊になされなければ、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可能性があると言える。

(b) 社会情勢

(ア) 人的側面 (人材、意識、体制・制度)

人材面では、育成・確保について、政府機関、企業を問わず、いまだ十分なレベルとは言えない。

意識面では、企業のIT統制や事業継続計画 (Business Continuity Plan (BCP)) に対する意識が高まったことや、啓発を目的とする取組みの推進が進められたことなどによって、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。また、これには景気の回復によって企業に余裕が出てきたことや、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、情報セキュリティに関連して問題を生じさせることが経済的損失につながることが認識されたことなども大きく影響を及ぼしていると考えられる。ただし、意識は「発露」の段階であり、対策が「当然のこと」として捉えられるには至っていないと考えられる。

体制・制度面では、内部統制対応の一環として、企業が対応体制を強化するという傾向も見られ、政府機関についても、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・制度が徐々に整いつつある状況である。

(イ) 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について見てみると、政府機関では、政府機関に対する脅威対応のためのシステム等 (GSOC) の構築予算が確保された。企業においては、情報セキュリティで問題を起こすことによる経済的損失との比較の下で投資がなされる傾向にあると考えられる。また、個人分野では情報セキュリティ

対策ソフトの購入が一般的になるなど、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と考えられる。また、研究開発・技術開発投資の効率向上の検討などの動きも見られた。

情報セキュリティ技術面では、具体的な対策の必要性に迫られた製品を中心とした開発が進められる傾向にあった。

(ウ) 周辺情勢(インシデント・事件、市場等)

コンピュータウイルス等による情報流出が依然続き、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。また、政府機関や企業に対しては、特別仕様のウイルス付きメールを送付し、コンピュータに不正なプログラムを潜伏させる攻撃へと変化が見られ、被害が顕在化しにくくなった。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、攻撃手段も進化している状況にある。

また、IT障害については、例えば、社会経済活動の国際化を反映して、IT障害の範囲が一つの国の中にとどまらない事例が発生するなど、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も生じた。

3. 総評

以上を総括すると、2006年度は、情報セキュリティ対策に係る取組みは総じて順調に行われ、「官民における情報セキュリティ対策の体制の構築」が進んだと言える。また、各対策実施領域に属する主体が取組みの必要性に気づいた一年でもあった。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対策を実施してきたところ、NISCの旗振りの下、各々の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も進められた。

つまり、2006年度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)対策実施主体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。

しかし、対策実施領域によっては対策にスピード感が欠けているのも事実であり、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。また、IT利用に係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、リスクが大きく増加しないよう努力がなされている状況にある。さらに、SJ2006に盛り込まれた内容の取組み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かったものも存在している。

我が国が真の情報セキュリティ先進国となるよう、2007年度も引き続き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2章　2007年度に我が国が情報セキュリティ問題に取り組む上での基本方針

第1節　2007年度の課題

セキュア・ジャパン2007（以下「SJ07」という。）は、2006年度の取組みおよびその評価も踏まえつつ、基本計画の下での取組みの2年目である2007年度における情報セキュリティ対策の政府の重点施策を定めるものである。

3か年の基本計画の2年目である2007年度においては、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、ここでは官民における情報セキュリティ対策の底上げ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。

第2節　2007年度の情報セキュリティ政策の重点

そこで、2007年度の我が国情報セキュリティ政策の重点は、2006年度に開始した基本計画の下での情報セキュリティ対策の安定的な推進を図り、それとともに**「官民における情報セキュリティ対策の底上げ」**を実現することとする。基本計画に掲げられている4つの基本方針については、（1）官民各主体の共通認識の形成は概ねできてきたことから、共通認識の維持・向上を図り、（2）情報セキュリティ技術戦略委員会での検討も踏まえつつ、引き続き先進的技術の追求を図り、（3）人権保障や、公的部門の活動の透明性や適法性の確保とのバランスを維持しつつ、公的部門の戦略的な対応能力強化を図り、（4）国内における官民の各主体間や、国際的な主体間での連携・協調の推進を進めるという形で維持・強化していくこととする。

第3節　中期的な視点に基づく取組み及び時宜に合った集中的な取組みの必要性

情報セキュリティ政策は、単年度ごとの PDCA サイクルに基づいて取組みを積み重ねることで基本計画に基づく目標を3年間で実現し、これを踏まえて次の3年間の計画と、その下での単年度ごとの取組みを企画することとしている。しかし、実際の政策運営においては、単年度で成果を完全にあげることが難しく、中期的に時間をかける必要のある取組みや、単年度という枠よりも、むしろその時宜その時宜に合わせて焦点をあてるべき取組みがある。2008年度の重点施策の方向性を含めて2007年度の基本方針を策定するにあたっては、このような課題について十分考慮を行うべきである。この観点からは、以下の3つの視点が重要であると考えられる。

情報セキュリティ政策の人材育成・確保は「ITを安心して利用可能な環境」を実現するために、情報セキュリティを担当する部署の体制強化も含め、2007年度に取組むことが必要な重要課題である。しかし、人材育成・確保は、情報セキュリティ基盤という社会基盤の構築・強化であるため、2007年度単年度での課題というよりも、単年度の枠を超えた継続的・中期的な取組みを必要とする課題と考える必要がある。

また、国際連携・協調は、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障害の影響が一つの国の中にとどまらないこと、我々の社会経済活動が我が国の国内だけ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すると、「世界における日本、日本にとっての世界」という双方向の視点から積極的に取組むべき課題である。当該分野については、取組みを着実に進めたことで2006年度の目標は概ね達成したと言える。しかし、目標が依然第一歩目に過ぎず、これから情報セキュリティ政策の国際展開として本格的な取組みを行う必要がある。こうした課題については、中期的な視点を持って取組みを加速化することが必要な課題と考えるべきである。

さらに、急に発生したリスクへの対応を含め、2008年度の喫緊の課題として、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。現在、電子政府の構築に向けた様々な取組みが進められていることから、情報セキュリティの観点からの検証・強化を始めとする総合的な取組みを、推進するための体制の構築も含め、適時適切に行うことが重要課題となる。

第3章　対策実施4領域における情報セキュリティ対策の強化

本セキュア・ジャパン2007においては、セキュア・ジャパン2006に引き続き、情報セキュリティ対策を実際に適用し実施する主体の領域を、政府機関・地方公共団体、重要インフラ、企業、個人の4領域に分け、それぞれの特性に応じた具体的施策を定めることとする。

第1節　政府機関・地方公共団体

ア　政府機関

政府機関について、1）2008年度までに政府機関統一基準[2]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し、政府は、2006年度に引き続き、以下の施策を重点的に推進する。

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

政府機関の情報セキュリティ対策の水準を世界最高のものとするため、政府機関統一基準について、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する。

また、各政府機関の情報セキュリティ対策の実施状況を、政府機関統一基準に基づき、必要な範囲で検査・評価し、勧告を通じた各政府機関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（Plan・Do・Check・Act サイクル）を確立する。なお、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。

さらに、政府機関の対策の内容・経験及びその他の知識は、民間企業、地方公共団体、独立行政法人等にとっても参照すべき価値のあるものであることが望まれるため、「ベストプラクティス（模範例）」として、これらの知識を分かりやすい形で公開し、その普及に努める。また、外部委託先の情報セキュリティ対策の水準の確保の観点についても十分に留意する必要がある。

【具体的施策】

ア）政府機関統一基準の見直しの実施（内閣官房）

技術や環境の変化を踏まえ、2007年度においても政府機関統一基準の見直しを行う。また、その際には政府機関内外で発生したIT障害についても分析を行

[2] 「政府機関統一基準」とは、「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）を指す。以下同じ。

い、その結果を反映することとする。

ｲ) PDCA サイクルの定着

a) 各政府機関での PDCA サイクルの定着（全府省庁）

各府省庁は、情報セキュリティ対策の実施状況の自己点検及び監査の結果等を踏まえて自ら対策の改善を行うなど、2007年度中に PDCA サイクルの定着を図り、組織全体での底上げを図る。

特に、2007年度において、各府省庁は全職員に対する教育の拡充等により、セキュリティ意識の向上を図り、省庁対策基準及び実施手順等の遵守を徹底するとともに、自己点検及び監査に関する実施体制の充実･向上を図り、対策実施状況の適切な把握を行う。

b) 政府全体での PDCA サイクルの定着（内閣官房及び全府省庁）

内閣官房は、各府省庁の対策の実施状況を、政府機関統一基準に基づき、検査･評価し、勧告を通じた各府省庁の対策の改善と政府機関統一基準等の改善に結びつけるとともに、各府省庁における必要な体制の確保を行うための環境整備に努めることにより、2007年度に政府全体としてのＰＤＣＡサイクルを定着させる。

ｳ) 本格的な評価の推進及び結果の公表

内閣官房は、「『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」（2007年2月2日情報セキュリティ政策会議決定）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」（2007年2月2日情報セキュリティ政策会議了解）に基づき、各府省庁における情報セキュリティ対策について、以下の観点から本格的な評価を行い、改善を促進する。

なお、定常的な評価の実施は、緊急性等を要する場合を除き、原則として、内閣官房が各府省庁に対して事前に示したスケジュールや検査項目に基づいて実施する。

また、評価の結果については、政府全体としての効果的な対策の推進を図るとともに、国民への説明責任を果たすためのものとして、情報セキュリティの維持･確保にも配慮しつつ公表することとする。

a) 対策実施状況に関する評価等（内閣官房）

政府機関統一基準に基づく対策実施状況に関する評価については、2006年度の評価で確立した評価手法に基づき、対策実施状況報告や、特定の重点項目に係る重点検査をもとに、各府省庁の対策の実施状況を客観的に比較可能な形

で本格的に評価する。

b) 情報セキュリティマネジメントに関する評価等（内閣官房）

各府省庁の情報セキュリティマネジメントに関する評価を実施し、情報セキュリティ対策の改善を促進する。

2007年度上半期中に、2006年度の各府省庁の取組みをもとに評価を試行的に実施するとともに、政府全体としての PDCA サイクルを定着させるために有効であり、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。

エ) 政府機関統一基準に基づく取組みへの支援と効率的な運用の促進

a) 情報セキュリティ対策関連情報の提供（内閣官房）

各府省庁における情報セキュリティ対策の推進を支援するため、内閣官房は各府省庁に対して技術情報を含む各種情報セキュリティ対策関連情報や適切なアドバイス等の提供を引き続き行う。

b)情報セキュリティ対策の府省庁共通的課題に対する取組み（内閣官房及び全府省庁）

政府機関統一基準に基づく取組みの円滑化を図るため、内閣官房は、各府省庁の協力の下に、情報セキュリティ対策の運用上の共通的な課題に関して、府省庁が参画して、対応策を検討する場を設け、共同して課題の解決に取り組む。

c)情報セキュリティ対策のベストプラクティスの共有（内閣官房及び全府省庁）

政府機関における情報セキュリティ対策に係る知識の共有を推進するため、内閣官房は、各府省庁における情報セキュリティ対策や上記検討の結果得られた対応策等のうち、ベストプラクティス（模範例）として参照すべき価値があるものについては、取りまとめて、政府機関全体で情報の共有を図る。また、これを可能な限り、民間企業、地方公共団体、独立行政法人等にとっても活用できるよう取りまとめを行い、公表する。

d) 各府省庁における自己点検及び監査の効率化（内閣官房）

政府機関統一基準を踏まえた省庁基準に基づく各府省庁の情報セキュリティ対策の確実な実施のため、内閣官房は教育、自己点検及び監査に係る作業について、IT化等を含めた効率化の方策について検討を行い、2007年度の上半期に各府省庁に提示する。

e) 各府省庁の情報システムの一元的把握（内閣官房及び全府省庁）

各府省庁は、保有している情報システム関する情報セキュリティ対策を組織全体で一元的かつ適切に把握し、実施していくために、それぞれが整備する情報資産台帳等に、各情報システムで取り扱う情報、その情報の格付けを含む情報セキュリティに関する事項を記載することとする。

オ) コンピュータウイルスなどに起因する情報流出への対応（全府省庁）

各府省庁は、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、2007年度も引き続き、政府機関統一基準に基づき、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。

カ) 外部委託先等の情報セキュリティ対策の水準の確保

a) 情報セキュリティマネジメントシステム適合性評価制度等の活用（内閣官房及び全府省庁）

2007年度も引き続き、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。

b) 情報セキュリティ監査制度の活用（内閣官房及び全府省庁）

2007年度も引き続き、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。

c)「情報システムの信頼性向上に関するガイドライン」の活用・普及（内閣官房及び経済産業省）

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」の政府機関における活用・普及を促進する。

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

各政府機関が情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えるようにするため、2007 年度に、独立行政法人情報処理推進機構（以下、「IPA」という。）において、ITセキュリティ要件、ITセキュリティ評価及び認証制度の認証製品の活用可否を確認する際の支援ツールを開発するとともに、政府機関

統一基準の関連マニュアル等に反映することを通じて、政府機関等における当該ツールの活用を促進する。

②独立行政法人等のセキュリティ対策の改善

政府機関統一基準を踏まえ、独立行政法人等の情報セキュリティ水準の向上を促進する。特に、これまで情報セキュリティポリシーを策定していない独立行政法人等については、情報資産及びリスクの状況等、各法人の実情を踏まえつつ、情報セキュリティポリシーの策定を行い、また策定されている独立行政法人等については、ポリシーの見直しを行う等の改善を図る。

【具体的施策】

ア）独立行政法人等における情報セキュリティポリシーの整備（内閣官房及び独立行政法人等所管府省庁）

各府省庁は、所管する独立行政法人等に対して、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・見直しを要請するとともに、必要な支援等を行う。

イ）独立行政法人等の情報セキュリティ対策の改善に向けた環境整備（内閣官房）

独立行政法人等における情報セキュリティポリシーの策定・見直しの促進に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。

③中長期的なセキュリティ対策の強化・検討

情報セキュリティに関する要求仕様の共通化、年度途中での緊急事態対応に向けた取組み等、以下のような、政府機関が全体として協力して行うべき情報セキュリティ対策の実施を図る。

（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

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おいて、新たに開発（導入）するシステムについては、政府機関統一基準等との連携を図りつつ、情報セキュリティ機能の明確化等を通じて、情報セキュリティに関する要求仕様の共通化、信頼性の高い製品等の利用等を推進する。

【具体的施策】

ア）内閣官房及び各府省情報化統括責任者（CIO）補佐官等の連携強化（内閣

官房及び総務省）

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、2007年度も引き続き、内閣官房と CIO 補佐官等が連携し、対象システムの開発の段階から効果的な情報セキュリティ機能の実現を推進する。

イ）安全性・信頼性の高いIT製品等の利用推進（内閣官房及び全府省庁）

2007年度も引き続き、安全性・信頼性の高い情報システムを構築するため、IT製品等を調達する際には、政府機関統一基準に基づきITセキュリティ評価及び認証制度[3]により認証された製品等を優先的に取り扱う。

（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

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・整備について検討等を行うことが重要である。そのプラットフォームについてセキュリティ強化を図るため、IPv6、国家公務員身分証ICカード、暗号、電子署名、生体認証等の新規システム（機能）の導入について総合的な検討等を行い、その実現を推進する。

特に、今後、すべての政府機関の情報システムがIPv6を早期に利用できるようにするため、原則として2008年度までに、各府省の情報システムの新たな開発（導入）又は更改に合わせて、情報通信機器やソフトウェアのIPv6対応化を図る。

【具体的施策】

ア）次世代の電子政府構築に向けた検討（内閣官房及び総務省）

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・整備に関し、必要な技術的、機能的検討を進め、2007年度末までに結論を得る。

イ）高セキュリティ機能を実現する次世代ＯＳ環境の開発（内閣官房、内閣府、総務省及び経済産業省）

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、2006年度に引き続き、産学官の連携により推進する。

[3] 「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証レベルを、情報セキュリティの国際標準 ISO/IEC 15408 に基づいて第三者が評価し、結果を公的に検証し、公開する制度を指す。

ウ) 情報アクセス権限を統合し集中管理する機構を導入した革新的な仮想化技術の開発（経済産業省）

異なる情報システムを一つのサーバ上に統合するだけではなく、これまで情報システムごとに別々に設定していた情報アクセス権限を統合し集中管理する機構を導入した革新的な仮想化技術（セキュア・プラットフォーム）の開発を2007年度から行う。

エ) 警察における情報セキュリティ対策の強化（警察庁）

2007年度において、外部記録媒体に保存する情報を自動的に暗号化等するソフトの一般業務用端末への導入を開始する。

オ) 電子政府に用いられるOSのセキュリティ品質の評価尺度の確立（内閣官房）

2006年度に、電子政府に係る情報システムを構成する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ったところ、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2007年度に実施する。

カ) 電子政府システムのIPv6対応化（内閣官房、総務省及び全府省庁）

電子政府におけるIPv6の利用が、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) 各府省庁は、2006年度に策定した電子政府システムの IPv6 対応に向けたガイドラインを参考とし、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、2007年度より、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。

2) 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、2007年度も引き続き、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。

キ) 電子政府認証ガイドライン利用の推進（内閣官房、総務省及び経済産業省）

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、2007年度に、政府機関における「電子政府認証ガイドライン（仮称）」の利用を推進する。

ク) 中長期的な視点での電子政府における個人認証の発展方向の検討（内閣官房）

電子政府における個人認証に関して、安心･安全の向上の観点から、中長期的に見た我が国の個人認証のあり方についての検討に資するため、諸外国の政府における個人認証の制度及びシステムの実態等を調査する。

（ウ）政府機関への成りすましの防止

悪意の第三者が政府機関に成りすまし、一般国民や民間企業等に害を及ぼすことが無いよう、正統な政府機関であることを容易に確認可能とするため、電子証明書の広範な活用や、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[4]の利用を推進する。

【具体的施策】

ア) 政府機関のドメイン名であることが保証されるドメイン名の利用の促進（総務省及び全府省庁）

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は促進されつつあるところ、政府機関が国民に対して情報の発信を行う際に利用するドメイン名については、原則として2008年3月までに同ドメイン名を利用するよう、引き続き取り組む。

イ) 政府機関から発信する電子メール及び政府機関のホームページからダウンロードされる電子文書に係る成りすまし及び改ざんの防止（内閣官房、総務省及び全府省庁）

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あり方について検討を行い、2007年度中に結論を得る。

[4] 「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」とは、「属性型jpドメイン名のうち『go.jp』ドメイン名、及び汎用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」を指す。

(エ) 政府機関における安全な暗号利用の促進

電子政府の安全性及び信頼性を確保するため、電子政府で使われている推奨暗号について、その安全性を継続的に監視・調査するとともに、技術動向及び国際的な取り組みを踏まえ、暗号の適切な利用方策について検討を進める。

【具体的施策】

ア) 政府機関で利用する暗号の安全性等確保 (総務省及び経済産業省)

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2007年度に行う。

イ) 政府機関における安全な暗号利用の推進体制等の検討 (内閣官房、総務省及び経済産業省)

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を内閣官房において早急に取りまとめるとともに、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、2007年度中に検討する。

ウ) ハッシュ関数SHA-1の安全性低下への対応 (内閣官房、総務省、経済産業省及び全府省庁)

電子政府の情報システムに広く使用されているハッシュ関数 SHA-1 については、暗号技術検討会から、現時点でただちに利用を停止する状況にはないが、暗号強度の低下が報告されていることから、政府機関における情報システムのライフサイクル等を踏まえ、政府機関においては以下のような対応を行う。

1) 各府省庁は、電子署名やタイムスタンプのようにハッシュ関数を長期間にわたる用途で利用する情報システムを、今後、新規に構築する (更新を含む。) 場合には、以下のいずれかの対応を行うものとする。

① 256 ビット以上のハッシュ関数を選択すること

② SHA-1 を引き続き選択する場合には、現実的な脅威となる攻撃手法が示された時点で、速やかに別のアルゴリズムに変更する等の対応措置が可能な構成とすること

2) ハッシュ関数の移行に関しては、関係する情報システム間における相互運用性を考慮することが必要であることから、内閣官房は、総務省、経済産業省及び関係府省庁の協力を得て、認証基盤システム、電子申請システム等、広範に影響を与える情報システムについて、具体的な課題の抽出等を行い、その結果を踏まえ、2007 年度早期に政府機関における移行に関する指針を策定する。

3) 総務省及び経済産業省は、SHA-1 の安全性について引き続き監視し、内閣官房は、必要な情報を速やかに各府省庁に提供する。

エ) 安全性・信頼性の高い暗号モジュールの利用推進（内閣官房、経済産業省及び全府省庁）

安全性の高い暗号モジュールの活用を推進するため、2007年度に、IPA の運用する暗号モジュール試験及び認証制度を推進するとともに、暗号モジュールを調達する際には、必要に応じて、同制度により認証された製品等を優先的に取り扱う。

オ) ファイル（電磁的記録）のセキュリティ対策の推進（防衛省）

可搬記憶媒体へのファイル書き出し時のセキュリティ確保のため、2006年度に製作したファイル秘匿化ソフトウェアの導入を推進する。

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

サイバー攻撃等への迅速かつ適切な緊急時の対応及び技術や環境の変化への適応を実現するために、政府内において迅速に情報を共有し、統一的に情報を分析し、適切な対策を講ずることができる体制を構築するとともに、対処を行う関係機関の能力を向上させ体制を整備し、過去の緊急時等の対応から得られた知見を政府機関統一基準等の改善や政府における人材育成等に取り入れるなどにより、緊急対応能力を強化する。

【具体的施策】

ア) 政府機関に対するサイバー攻撃等に関する横断的な問題解決機能の強化

a) 政府横断的な対応体制の構築（GSOC の整備）（内閣官房及び全府省庁）

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より確実に防止し、発生した場合にはより迅速かつ的確に対応するため、2008 年度における本格運用に向け、政府横断的な情報収集、攻撃等の分析・解析、各政府機関への助言、各政府機関の相互連携促進及び情報共有を行うための体制（Government Security Operation Coordination team）（略称；GSOC）を整備する。

2007 年度においては、一部府省庁の情報システムに係るリアルタイム監視機能並びに内閣官房情報セキュリティセンターにおける横断的な監視情報の収集機能、攻撃等の分析・解析機能を整備するとともに、当該分析・解析の結果に基づく各政府機関への助言、各政府機関の相互連係促進及び情報共有を行うための体制を強化する。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。

b) 情報保証に係る最新技術動向等の調査研究（防衛省）

2006年度に引き続き、情報システムの情報保証を確保するため、サイバー攻撃及びサイバー攻撃対処に係る最新技術動向等を継続的に調査するとともに、一元的な対処態勢等について調査研究を実施する。

ｲ) 各政府機関における緊急対処能力の強化

a) 各政府機関における緊急対応体制の強化（内閣官房）

各政府機関においてIT障害が発生した場合に対応要領等に基づき迅速かつ的確に対処できるよう、2007年度において、政府機関で発生頻度の高い個別のIT障害への対応方策を策定し、浸透を図る。また、当該IT障害の兆候を早期に発見して対応方策に従った対処が実施できるよう、政府機関の情報システムの監視機能、攻撃の分析機能等に、刻々と変化するIT障害の特徴を迅速に反映することとし、2007年度中にそのための体制を強化する

b) サイバーテロ対策に係る体制等の強化･整備（警察庁）

2007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の強化･整備を推進する。

c) サイバー攻撃等に係る分析･対処及び研究の推進（防衛省）

防衛省の保有する情報システムに対するサイバー攻撃等に関する脅威／影響度の分析･対処能力をさらに向上させるため、サイバー防護用分析器材を整備し運用を開始するとともに、2006年度に引き続き、不正アクセス監視･分析技術、サイバー攻撃分析技術及びアクティブ防御技術等について基礎的な研究を実施する。

d) 統合通信部隊の新設（防衛省）

2007年度に、自衛隊の情報通信について、これまでの静的な機能維持に加えてサイバー攻撃発生時の適時適切な機能回復などの動的な役割を担う常設の統合部隊を新設する。

⑤政府機関における人材育成

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に、必要な知見や専門性を有する人材を育成・確保することが重要であることにかんがみ、政府機関における情報システム管理部門の担当職員の育成、情報セキュリティに関する専門性の高い人材の活用、教育機関と連携した人材育成の取組み、幹部職員・一般職員の意識の向上方策等を推進する。なお、政府機関の情報システム管理部門において、情報セキュリティ対策業務に携わる専門的職員については、全員が情報セキュリティに関する資格を保有することを目指す。

【具体的施策】

ア) 政府職員の人材育成に係る検討

a) 一般職員に対する教育の検討（内閣官房及び全府省庁）

一般職員による安全な情報技術の活用に資するため、2007年度において、一般職員向けに情報セキュリティに関する最低限の知識を啓発するための政府統一的な教育の在り方について検討を行い、可能なものから順次実施する。

b) 幹部職員に対する教育の検討（内閣官房、総務省及び全府省庁）

幹部職員の情報セキュリティに関するリスクの認識・理解に資するため、2007年度において、既存の研修の活用を含め、幹部職員向けの政府統一的な教育の在り方について検討を行い、可能なものから順次実施する。

c) 情報セキュリティ対策を担当する職員に対する教育の検討（内閣官房、総務省、全府省庁）

情報セキュリティ対策を担当する職員の業務遂行及び専門的能力の向上に資するため、2007年度において、総務省が実施している「情報システム統一研修」の活用を含め、担当職員向けの政府統一的な教育の在り方について検討を行い、可能なものから順次実施する。

d) 人材育成・確保実行計画の作成（全府省庁）

情報システムの安全・安心な活用に資する情報セキュリティを含めた知識・能力を有する人材の育成・確保するため、各府省庁は「行政機関におけるIT人材の育成・確保指針」（2007年4月13日各府省情報化統括責任者（CIO）連絡会議決定）に基づき、2007年度末までのできる限り早期に「IT人材育成・確保実行計画」を作成する。

イ 地方公共団体

2006年9月に見直しを行った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を踏まえた情報セキュリティ対策や、情報セキュリティ監査や研修等の対策を推進し、また、2006年度に創設された地方公共団体間の情報共有体制（自治体CEPTOAR）が機能を発揮することを目指し、2006年度に引き続き、以下の施策を重点的に推進する。

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

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等を行うとともに、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。

【具体的施策】

ア）地方公共団体における情報セキュリティ対策の手引きの作成（総務省）

2007年度に、地方公共団体において取組みが不十分な情報セキュリティ対策（情報資産のリスク分析等）について、その運用の現状・課題等を分析し、具体的な導入・運用にあたって参考となる手引きを作成する。

②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、情報セキュリティ監査の実施を推進する。

【具体的施策】

ア）地方公共団体における情報セキュリティ監査実施の推進（総務省）

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、2007年度に地方公共団体情報セキュリティ監査ガイドラインの見直しを行い、当該ガイドラインを踏まえた情報セキュリティ監査の実施を推進する。

③「自治体情報共有・分析センター」（仮称）の創設促進

地方公共団体におけるIT障害の未然防止、拡大防止・迅速な復旧及び再発防止に資するとともに、地方公共団体全体の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）の創設を促進する。

【具体的施策】

ア）「自治体 CEPTOAR」への支援（総務省）

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共有等を行う「自治体 CEPTOAR」が2006年度に創設され、2007年度には、「自治体 CEPTOAR」が効果的に機能するよう、必要な助言等の支援を行う。

④職員の研修等の支援

上記のほか、高度な技術の開発・導入や職員の研修等について支援を行い、地方公共団体のセキュリティ強化を図る。

【具体的施策】

ア）地方公共団体職員を対象とする情報セキュリティ研修の実施（総務省）

2007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。

第2節　重要インフラ

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を目指し、政府は、重要インフラの情報セキュリティ対策について、「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）を別途定めているところであるが、2007年度には以下の施策を重点的に推進する。

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

「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』[5]策定にあたっての指針」[6]（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。

【具体的施策】

ア）各重要インフラ分野の安全基準等の策定・見直し

a)安全基準等の見直し（重要インフラ所管省庁[7]）

2007年6月を目処に行われる指針の改定を踏まえ、2007年9月を目処に、各重要インフラ分野において、安全基準等の確認・検証を行い、必要に応じ改定等の対策を実施する。

b）「安全基準等」の見直し状況等の把握及び検証（内閣官房）

各重要インフラ分野における「安全基準等」について、各重要インフラ所管省庁の協力を得つつ見直しの状況を2007年中に把握するとともに、相互依存性解析の成果も踏まえた検証を2007年度中に実施する。

イ）各重要インフラ分野における安全基準等の浸透状況等に関する調査の実施（内閣官房及び重要インフラ所管省庁）

2007年度中に、内閣官房は、重要インフラ所管省庁の協力を得つつ、2006

---

5 「安全基準等」とは、重要インフラ事業者等が、様々な判断、行為を行うに当たり、基準又は参考にするものとして策定された文書類を指す。

6 「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」（2006年2月2日情報セキュリティ政策会議決定）

7 「重要インフラ所管省庁」とは、重要インフラ事業者等（「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）中「1　目的と範囲」に示す定義による。以下同じ。）と法令に従って直接に接する省庁を指す。以下同じ。

年度に策定･見直しを行った各重要インフラ分野における安全基準等の浸透状況についての調査を実施する。

ウ) 指針の見直し（内閣官房）

2007年度中に相互依存性解析の成果も踏まえ、各重要インフラ所管省庁の協力を得て、指針の見直しを実施する。

エ) ネットワークのIP化に対応した電気通信システムの安全･信頼性確保（総務省）

ネットワークの IP 化の進展に対応して、ICT サービスの安定的な提供を確保するため、2007年度中に、ネットワークの設備面や運用･管理面について、制度改正など必要な安全･信頼性対策を講じる。

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･適切に提供し、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。

（ア）官民の情報提供･連絡のための環境整備

関係機関と連携し、注意喚起等、各重要インフラ事業者等の対策に資するものとして、重要インフラ事業者等に提供する情報の収集を行い、CEPTOAR（後述）等を通じて、情報を提供する。

また、重要インフラ事業者等が、法令等で報告が義務づけられている事故、障害、業務遅延等のほか、特異重大なものとして重要インフラ事業者等が連絡を要すると判断した情報を政府に連絡するための環境の整備を促進する。

【具体的施策】

ア) 情報共有体制整備と機能強化（内閣官房）

各分野における CEPTOAR の整備及び CEPTOAR-Council（仮称）の整備等の状況変化を踏まえ、2006年度に整備された官民の情報共有体制に対して追加すべき機能･要件等の検討を行う。

（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

IT障害の未然防止、発生時の被害拡大防止･迅速な復旧及び再発防止のた

め、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係重要インフラ事業者等間で共有することにより、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資するため、各重要インフラ分野内に「情報共有・分析機能」（CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response）の整備を促進する。

【具体的施策】

ア）各重要インフラ分野における CEPTOAR 整備の推進（重要インフラ所管省庁）

２００７年度末までに、新規追加分野（水道、医療及び物流）においてCEPTOAR が整備されるよう取組みを進める。

イ）「CEPTOAR 特性把握マップ」のフォローアップ（内閣官房）

2007年度中に、各分野におけるＣＥＰＴＯＡＲの機能・要件の検討状況及び整備状況（新規追加分野については整備状況）の把握を行う。また、2007年度末を目処に、ＣＥＰＴＯＡＲ特性把握マップのフォローアップを行う。

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

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、各ＣＥＰＴＯＡＲ間での横断的な情報共有の場として「重要インフラ連絡協議会（ＣＥＰＴＯＡＲ－Council）」（仮称）の創設を促進する。

【具体的施策】

ア）「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）創設の検討（内閣官房及び重要インフラ所管省庁）

2007年度中に重要インフラ連絡協議会（ＣＥＰＴＯＡＲ－Council）（仮称）の創設についての基本的合意を得るべく、検討の場を開催し課題についての検討を進める。

③相互依存性解析の実施

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。

【具体的施策】

ア) 重要インフラ分野間の相互依存性解析の推進（内閣官房）

重要インフラ分野における IT 化の一層の進展と分野間の関連性の高まりを踏まえ、官民の連絡・連携体制の機能と、事業継続を含むIT障害発生時の対応能力の向上等を図るため、2007 年度は、国内外の脅威の類型や脅威と障害の因果関係、障害と事業継続との関係などについての検討の深化や演習シナリオへの反映を行うとともに、重要インフラにおける障害発生から波及・拡大という連鎖的な伝播プロセスを動的に把握する動的依存性解析を推進する。なお、実施にあたっては、実施方法について十分に検討を行う。

④分野横断的な演習の実施

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。

【具体的施策】

ア) 重要インフラ機能演習[8]の実施（内閣官房及び重要インフラ所管省庁）

官民の連絡・連携体制の機能と、IT 障害発生時の対応能力の向上等を図るため、2007 年度は、重要インフラ所管省庁、各重要インフラ事業者等及び各重要インフラ分野の CEPTOAR 等の協力を得て、相互依存性解析の知見を踏まえつつ、想定される具体的な脅威シナリオの類型をもとにテーマを設定し、分野横断的な機能演習を実施する。

イ) 電気通信事業分野におけるサイバー攻撃への対応強化（総務省）

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 ICT スキルを有する人材の育成を図るため、２００７年度も、２００６年度に引き続き、電気通信事業者を中心に、各重要インフラに跨るインターネット上で発生するサイバー攻撃を想定したサイバー攻撃対応演習を実施する。

ウ) 各分野サイバー演習との連携（内閣官房及び重要インフラ所管省庁）

２００７年度に内閣官房の実施する演習において、「情報通信」等の分野ごとに

8 実際の組織の指示判断系統機能を用いて模擬的に検証するための演習

実施されるサイバー演習の実施形態及びその目的との整合性を考慮しつつ、連携を図る。

⑤「重要インフラの情報セキュリティ対策に係る行動計画」の見直し

【具体的施策】

ア)「重要インフラの情報セキュリティ対策に係る行動計画」の見直し(内閣官房)

2007年中に、各重要インフラ所管省庁の協力を得て、「重要インフラの情報セキュリティ対策に係る行動計画」の見直しに向けて、重要インフラ分野における情報セキュリティ対策向上の状況についての調査・把握に着手する。その際、災害発生時における対応等、他の関連する省庁横断的な取組みとの整合性の確保、連携についても検討を行う。また、官民の連携の在り方についても継続的に検討を行う。

第3節　企業

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、政府は、2007年度に以下の施策を重点的に推進する。

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

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。このため、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・改善を図るとともに、情報システム等の政府調達の競争参加者に対して、必要に応じて、これらの制度や第三者評価の結果等を活用した情報セキュリティ対策レベルの評価を入札条件等の一つとする。また、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。

【具体的施策】

ア）情報セキュリティガバナンス確立の促進

a)企業における情報セキュリティガバナンスの確立促進（経済産業省）

企業における情報セキュリティガバナンスの確立に向け、2007年度に、企業の情報セキュリティ対策に係るベストプラクティス（模範例）を普及させるための方策、及び民間の組織による情報セキュリティ格付けの促進のための方策を検討する。

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、普及活動を継続的に実施する。更に普及促進に資するために、当該ガイドラインの遵守度合いを評価することができる「情報システムの信頼性向上に関する評価指標（仮称）」の確立および評価ツールの提供を2007年度中に実施する。

b)電気通信事業における情報セキュリティマネジメントの強化（総務省）

電気通信事業者の情報セキュリティ体制の構築・運用に資するために、電気通信事業者等や関係団体から構成される「電気通信分野における情報セキュリティ対策協議会（ISeCT：Information Security Conference for Telecommunications）」において2006年度に業界ガイドラインとして策定した、「電気通信事業における情報セキュリティマネジメントガイドライン（ISM－TG）」について、同協議会と連携し、認証をはじめとした普及促進に向けた取組みを行う。

（ＩＳＭ－ＴＧ：Information Security Management Guideline for

Telecommunications)

ｲ) 入札条件等の見直し(内閣官房、総務省、財務省及び全府省庁)

情報システムに係る政府調達において、競争参加者の情報セキュリティ対策レベルの評価等を入札条件や落札条件とする方法について、関係府省庁間で検討を行い、2007年度中に結論を得る。

ｳ) 情報セキュリティ管理を重視した情報サービスマネジメントに関する標準化の推進(経済産業省)

情報サービスの提供者が、情報セキュリティ管理を重視した情報サービスマネジメントを計画し、実行し、点検し、かつ、継続的改善を図っていくことにより、情報サービスの品質の向上、顧客満足度の向上等を実現していく際の標準として、2007年度中に、日本工業規格として、JISQ20000－1(情報技術－サービスマネジメント－第1部:仕様＝ISO／IEC20000－1)及びJISQ20000－2(情報技術－サービスマネジメント－第2部:実践のための規範＝ISO／IEC20000－2)を制定する。

ｴ) 中小企業における情報セキュリティ対策の推進(経済産業省)

中小企業の負担の低減及び対策の推進を目的として、2007 年度中に、中小企業向けの情報セキュリティ対策のパッケージ及び対策実施状況を確認するための標準フォーマットについて検討を開始する。

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

情報セキュリティ対策は、本来業務を達成するために必要な機能とは異なる機能を、リスクに応じて講じていく性質のものであること、また、対策そのものを可視化しにくい特性等を持つことから、企業が情報セキュリティ対策を講ずる際には、理解のしやすい形で必要な対策を選択できる環境が整備される必要がある。このため、企業の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を推進するとともに、ITセキュリティ評価及び認証制度、情報セキュリティマネジメントシステム(ISMS)適合性評価制度、情報セキュリティ監査といった第三者評価の活用を推進することにより、質の高い情報セキュリティ関連製品及びサービスの提供が促進されることを図ることとする。

また、こうした第三者評価の審査等の効率化を図るとともに、質の高い情報セキュリティ関連製品等を活用する企業に対し、その投資を加速するためのインセンティブが与えられる環境の整備を促進する。

【具体的施策】

ア) 情報セキュリティに関するリスク定量化手法についての研究（経済産業省）

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2007年度も引き続き実施する。また、オフショア・アウトソーシングに関連する固有のリスクについても検討を行う。

イ) 第三者評価の活用促進

a)情報セキュリティ監査制度の普及促進（経済産業省）

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、2007年度中に、国際規格との整合性を図りつつ、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。

具体的には、監査人が一定の保証を与える保証型情報セキュリティ監査の普及のため、保証型監査利用ガイドラインの作成等について、検討を行う。

b) 第三者評価の審査の効率化と質の高い情報セキュリティ関連製品等の普及促進（経済産業省）

2007年度に、IPAによるITセキュリティ評価及び認証制度の運用を推進するとともに、同制度の認証製品の活用可否を確認する際の支援ツールの開発等を通じ、情報システム調達時の同制度の利用拡充を図る。また、同機構による暗号モジュール試験及び認証制度の運用を推進する。

ウ) 税制優遇措置

a)情報セキュリティ対策装置の取得時における税制優遇措置（総務省）

2007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。

b)企業の高度な情報セキュリティが確保された情報システム投資に対する税制優遇措置（経済産業省及び総務省）

2007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。

エ) 企業に係る指標の充実等(内閣官房及び経済産業省)

「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)」を踏まえ、「情報処理実

態調査」において、従前より把握している企業における情報セキュリティ監査制度の活用状況に加え、2007 年度に、新たに、企業における情報セキュリティマネジメントシステム適合性評価制度及び情報セキュリティ対策ベンチマークの活用状況、取引(委託、外注を含む)相手における情報セキュリティ対策実施状況の確認状況、ISO/IEC15408 認証取得製品の導入状況について調査する。

また、同了解に掲げられている「政府機関の状況との対比」に基づき、内閣官房は、各省庁の協力を得て、2007 年度に、これら企業の指標と対比して不足するデータの把握方法について検討を行い、可能なものから把握する。

③企業における情報セキュリティ人材の確保・育成

企業においては、経営トップ等の情報セキュリティへの理解や企業内における情報セキュリティ人材が不足している。このため、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を通じて経営トップ等の情報セキュリティへの理解を普及させるとともに、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を推進する。また、各企業において情報セキュリティ対策を行っている担当者のモチベーションの維持のための取組みを促進する。

【具体的施策】

ア) 情報通信人材研修事業支援制度(総務省)

情報通信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、2007年度においても助成を行う。

イ) 組織におけるIT利用者向けのセルフチェックツールの機能強化等(経済産業省)

2007年度中に、組織におけるITの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及びこれを活用したセルフチェックツールの機能強化等を行う。

ウ) 中小企業を対象とした情報セキュリティセミナーの実施(経済産業省)

2007年度に、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、IPAと日本商工会議所が連携して実施している「情報セキュリティセミナー」を全国各地で開催するとともに、IT経営応援隊と連携した普及広報活動の展開や、海外の情報セキュリティ関連動向に関する情報の収集・提供体制に係る検討を行う。

エ) 客観的な高度IT人材評価メカニズムの構築(経済産業省)

客観的な人材評価メカニズムの構築に向けて、2007 年度中に、情報セキュリティ人材を含めた高度IT人材に求められるスキルを体系的に整理した共通キャリア・スキルフレームワークを構築する。

オ) 産学官協議会の設置（経済産業省）

2007 年度に、産業界が求める高度IT人材像や産業界及び教育界における実践的な高度IT人材育成手法について検討する産学官協議会を設置する。

カ) ファカルティ・ディベロップメントの支援（文部科学省及び経済産業省）

情報セキュリティ分野を含めた各情報分野における実践的な教育を促進するため、教員の能力向上のための各大学等のファカルティ・ディベロップメント（FD）の取組みを支援する。

キ) 情報処理技術者試験制度の改革（経済産業省）

情報セキュリティ人材を含めた高度IT人材の育成強化のため、情報セキュリティ分野を含めた各情報分野の人材スキルを測る情報処理技術者試験を抜本的に見直し、共通キャリア・スキルフレームワークとの整合性を確保した上で、2008 年度を目途に新たな試験を実施する。

ク) 高度情報通信人材育成体系の開発（総務省）

2007年度に、企業等の情報化戦略や新たなビジネス創出を担う人材を育成するため、情報通信セキュリティ分野を含むICT マネージメント分野の実践的なPBL（Project Based Learning）教材を開発する。

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

企業における情報セキュリティ問題に的確に対応するためには、情報関連事業者をはじめとする関係者間において、迅速な情報共有、対策の策定及び対策の普及を円滑に図る必要がある。このため、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、コンピュータウイ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。

【具体的施策】

ア) 組織の緊急対応チーム間の連携体制の強化（経済産業省）

攻撃の対象になり得る組織に対して、直接、脅威情報や対策情報を提供するため、有限責任中間法人 JPCERT コーディネーションセンター（以下「JPCERT/CC」という。）を中心として、2007 年度において、諸外国のコンピュータセキュリティ緊急対応チーム（以下、「CSIRT」という。）や国内の CSIRT から得られた関連情報を分

析する能力の高度化、組織の CSIRT 間の連携体制の強化について、検討を行う。

イ) コンピュータセキュリティ早期警戒体制の強化（経済産業省）

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、2007年度中に、IPA や JPCERT/CC 等による「コンピュータセキュリティ早期警戒体制」を強化する。

具体的には、情報セキュリティ問題に係る情報収集の強化、収集した情報を効果的・効率的に発信する仕組み、国際連携の強化等について検討を行う。

ウ) 安全な Web サイト構築のためのガイドライン検討（経済産業省）

Web サイトの安全性を確保するため、2007年度中に、発注者が Web 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ガイドラインを策定する。

エ) ソフトウェア等の脆弱性の重要度・優先度等に係る判断基準の整備等（経済産業省）

2007 年度に、IPA 及び JPCERT/CC において、ベンダやユーザーが脆弱性の深刻度を国際的に整合化された基準の下で定量的に比較し、対策の重要性・優先度の判断に資するような情報提供の仕組み及び各利用者の環境に応じた対策の優先度に関する意思決定を支援するツールを作成等し、その運用を開始する。

第4節　個人

2009年度初めには、「IT利用に不安を感じる」とする個人を限りなくゼロにすることを目指し、政府は、2007年度に以下の施策を重点的に推進する。

なお、①及び②の具体的施策の推進にあたっては、個人が情報セキュリティ対策を可能な範囲内で自主的に実施することが当たり前のこととして認識できる環境の整備や、国民から見てわかりやすい形での多様な広報啓発・情報発信を行うことが重要であり、内閣官房及び関係府省庁が整合性をとりつつ緊密に連携することとする。

①情報セキュリティ教育の強化・推進

初等中等教育からの情報セキュリティ教育や世代横断的な情報セキュリティ教育を推進する。

【具体的施策】

ア）初等中等教育からの情報セキュリティ教育の推進

a）小中高等学校における情報セキュリティ教育の推進（文部科学省）

情報セキュリティを含む情報モラル等の効果的な指導手法等について検討を行い、それらの指導事例をとりまとめ、Web サイトを作成し広く紹介することにより教員への普及等を行う。また、指導主事や教員を対象に、情報セキュリティを含めた情報モラル等の指導の普及を図るためのフォーラムを実施し、情報セキュリティ教育の一層の推進を図る。

b）ICTメディアリテラシー[9]育成手法の調査・開発（総務省）

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の育成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年度に行った。開発されたプログラムについては、2007年度以降、公開するとともに、ICTメディアリテラシーの育成を行う団体等に広く普及を図る。

c）「情報セキュリティ対策」標語・ポスターによる普及啓発（経済産業省）

IPA 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、2007 年度に、全国の小学生・中学生・高校生を対象として、

9 「ICTメディアリテラシー」とは、単にICTメディアにアクセスし、それを活用する能力のみならず、ICTメディアのそれぞれの特質を理解し、発信される情報について能動的に選択する能力、ICTメディアを通じてコミュニケーションを創造する能力まで含む概念。

情報セキュリティ対策の意識を高めるための標語・ポスターの募集を行い、入選作品を公表する。

d) 教員の情報セキュリティに関する指導力の向上（文部科学省）

2006年度に策定した教員のICT活用指導力のチェックリストの中に、「児童生徒に対して情報セキュリティを指導する能力」を位置付けたことを踏まえ、2007 年中に全国の実態調査を行うとともに、全ての教員が情報セキュリティ教育の指導ができるよう、教員のICT活用指導力の向上を図る。

イ) 世代横断的な情報セキュリティ教育の推進

a) 全国的な情報セキュリティ教育の推進（経済産業省及び警察庁）

2007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。

b) e－ネットキャラバンの実施等（総務省及び文部科学省）

2006年度に引き続き、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を、通信関係団体等と連携しながら全国規模で実施する。また、国際的な協力イベント等の検討を行う。

c) サイバーセキュリティ・カレッジの実施（警察庁）

2007年度において、情報セキュリティに関する意識・知識の向上を図るため、教育機関関係者、地方公共団体職員、インターネットの一般利用者等を対象として、サイバー犯罪の現状や検挙事例を交えた講演等を全国各地で実施する。

②広報啓発・情報発信の強化・推進

全国的規模での広報啓発・情報発信の継続的実施、ランドマーク的イベントの実施（「情報セキュリティの日」の創設等）、日常からの世論喚起・情報提供の仕組み（「情報セキュリティ天気予報」（仮称）の実施検討）の構築、我が国の情報セキュリティの基本戦略の国内外への発信を行う。

【具体的施策】

ア) 全国的規模での広報啓発・情報発信の継続的実施

a) 情報セキュリティに関する周知・啓発活動の推進（内閣官房、警察庁、総務省及び経済産業省）

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、2007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、「CHECK PC！キャンペーン」など、メディア等を活用した広報啓発活動を関連する企業や機関等における活動との連携も視野に入れつつ積極的に実施する。

なお、これらの取組みにおいては、IT初心者の層だけでなく、積極的なIT利用者であるものの情報セキュリティへの関心が低い層に対する働きかけも重視することとする。

b) 不正アクセス行為からの防御に関する啓発及び知識の普及（警察庁、総務省及び経済産業省）

2006年度に引き続き、不正アクセス行為の禁止等に関する法律に基づき、不正アクセス行為の発生状況及びアクセス制御機能に関する研究開発の状況を公表するなどの取組みを通じ、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。

c) ネットワークの不適正な利用からの被害防止対策の推進（警察庁）

2006年度に引き続き、サイバー犯罪等の被害を防止するため、インターネット安全・安心相談システムを活用し、インターネット利用者の困りごとに応じた基本的な対応策を教示するとともに、サイバー犯罪等に係る情報提供を受け付けるなど、広報啓発・情報収集を効果的に実施する。

d) 電波利用秩序の維持のための周知啓発活動の強化（総務省）

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・使用ができる環境づくりに向けて、2006年度に引き続き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。

イ) ランドマーク的イベントの実施

a)「情報セキュリティの日」の実施（内閣官房、警察庁、総務省、文部科学省及び経済産業省）

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、毎年2月2日の「情

報セキュリティの日」の趣旨を踏まえ、これに伴う広報啓発的行事を全国的規模で開催する。

また、これにあわせて、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表彰する。

ウ) 日常からの世論喚起・情報提供の仕組みの構築

a) 内閣官房情報セキュリティセンター（NISC）メールマガジンの継続的発行（内閣官房）

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、2007年度においても継続的にメールマガジンを月に1回程度発行する。

b) 情報化促進貢献表彰における情報セキュリティ促進部門表彰の実施（総務省及び経済産業省）

2007年度の情報化月間において、情報セキュリティの確保の観点から多大な貢献を果たした個人・企業等を表彰するため、「情報化促進貢献表彰（情報セキュリティ促進部門）」を実施する。

エ) 我が国の情報セキュリティ基本戦略の国内外への発信

a) 我が国の情報セキュリティ戦略の国内外への発信（内閣官房）

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、2007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に、「セキュア・ジャパン2007」の英語版等を示すこととする。

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

情報関連事業者が、個人が高度な情報セキュリティ機能を享受しながら負担感なく利用できる製品やサービス（「情報セキュリティ・ユニバーサルデザイン」）を開発・供給する環境の整備を促進する。

【具体的施策】

ア) サイバー攻撃停止に向けた枠組みの構築（総務省及び経済産業省）

悪意のある第三者からの遠隔操作によりサイバー攻撃等を行うコンピュータウイルス（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、2010年度までに総合的な枠組みを構築することを目標に、技術面及び対策面を含めた試行、検討を実施する。

また、我が国の取組みについて、海外関係機関との間で必要な情報交換等を実施する。

イ）IPv6によるユビキタス環境構築に向けたセキュリティの確保（総務省）

IPv6対応ユビキタスセキュリティサポートシステム[10]を2009年度までに構築することを目指して、2007年度も引き続き、利用環境をモデル化した実証実験を実施し、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。

ウ）無線LANのセキュリティ対策（総務省及び経済産業省）

2007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」の更なる普及を図るとともに、一般利用者向けの普及啓発施策である「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。

10 「IP対応ユビキタスセキュリティサポートシステム」とは、膨大な数のユビキタス機器の複雑なセキュリティ対策をユーザだけでなく、IPv6インターネット網側からサポートするシステムを指す。

第4章　横断的な情報セキュリティ基盤の形成

各主体がそれぞれ「何のために、どの程度のリスクに対応して情報セキュリティ対策を行うのか」という点についての共通認識の形成を促進し、官民による持続的かつ強固な情報セキュリティ対策を継続させるためには、各対策実施領域における取組みのほか、その土台となる社会全体の基盤を形成することが必要である。このため、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・救済という視点から、中長期的戦略を明確にしながら、以下の具体的施策に総合的に取り組んでいくことが必要である。

第1節　情報セキュリティ技術戦略の推進

民間部門における取組みとの役割分担を明確にしつつ、情報セキュリティに関する技術戦略として、政府は、2006年度に引き続き以下の施策を重点的に推進する。

①研究開発・技術開発の効率的な実施体制の構築

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に、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の把握と継続的な見直しを行う。また、投資効率の改善のため、成果利用までを見据えた研究開発・技術開発を実施するための体制を構築し、その成果を政府が活用することを前提とした新たな研究開発・技術開発に取り組むこととする。

【具体的施策】

ア）実施状況の把握及び継続的な見直しの実施（内閣官房及び内閣府）

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の把握を2007年度中に開始する。

イ）投資効果に係る継続的評価プロセスの導入（内閣官房及び内閣府）

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2007年度中に本格的に実施し、その結果については速やかに公表する。

ウ）政府調達における成果利用の方策の検討（内閣官房及び全府省庁）

情報セキュリティ研究開発・技術開発における成果を、調達を通じ、最大限、直接政府が活用するための方策について、その検討を2007年度も引き続き行う。

②情報セキュリティ技術開発の重点化と環境整備

情報セキュリティ技術の高度化及び組織・人間系の管理手法の高度化のため、基盤としてのITを強化することに直結する中長期的な目標に対する研究開発・技術開発を促進する。一方、短期的な目標設定がなされている研究開発・技術開発については、その投資効率を把握し、バランスの良い投資を行う。なお、高い投資効率が見込まれるものの民間の取組みが期待できない萌芽的研究開発に対しては政府が主体的に取り組むこととする。

【具体的施策】

ア）中長期的な研究開発・技術開発の施策

a）中長期的目標に対する研究開発・技術開発の促進（内閣官房、内閣府、警察庁、総務省、文部科学省、経済産業省及び防衛省）

基盤としてのITを強化することに直結する中長期的目標に対して、公的研究資金を重点的に投入するための方策に関する検討を2007年度中に開始する。

b）次世代バックボーンに関する研究開発（総務省）

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[11]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、2007年度においても引き続き、次世代バックボーンに関する研究開発を推進する。

c）経路ハイジャック[12]の検知・回復・予防に関する研究開発（総務省）

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、2007年度も引き続き、経路ハイジャックの検知・回復・予防に関する研究開発を推進する。

d）情報通信分野における情報セキュリティ技術に関する研究開発（総務省）

2006年度からの5か年計画により、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を併せた、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。

---

11 「IPバックボーン」とは、一般的に、電気通信事業者の中継設備を相互に接続したインターネットプロトコルの基幹通信回線のことを指す。

12 「経路ハイジャック」とは、各 ISP のルータは通信経路を確立するために経路情報を保持・交換しているが、誤った経路情報がネットワーク上に広報されることにより、通信の障害が発生すること。

e) 新世代のアクセス制御技術の研究開発（経済産業省）

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年度に引き続き実施する。

f) 柔軟かつ確実な情報管理を達成するための情報処理・管理技術の開発（経済産業省）

情報の所有者・管理者が情報の開示の是非とその範囲を自ら決定し、それを確実に達成できるようにすること等を目的とした情報セキュリティ技術の研究開発を2006年度に引き続き実施する。

g) フェイルセーフな情報セキュリティ技術の研究開発（経済産業省）

「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年度に引き続き実施する。

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（経済産業省）【再掲】

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年度に引き続き実施する。また、オフショア・アウトソーシングに関連する固有のリスクについても検討を行う。

i) 情報漏えい対策技術の研究開発（総務省）

2009年度末までに、利用者の自助努力のみでは対処が困難となっているファイル共有ソフトの利用などによる情報漏えいの被害を最小限に抑える技術を確立することを目標として、ネットワークを通じた情報漏出の検知及び漏出情報の自動流通停止のための研究開発、情報の来歴管理等の高度化・容易化に関する研究開発に2007年度から着手する。

j) 情報通信構成要素の安全性検証技術の高度化に関する研究開発（総務省）

情報通信ネットワークを構成する機能・機器等の安全性検証の確度を高めることを目的に、2007年度より当該技術に関する研究開発に向けた検討に着手する。

k) ダイナミックネットワーク技術の研究開発（総務省）

2010年度までに、多種多様なネットワークや端末から構成される次世代ネットワークにおいて、ネットワーク障害が発生しても自動的に復旧することにより、最適な通信環境が安定的に提供され、誰もがネットワーク上に蓄積された情報に自由にアクセスできる環境を実現するために必要となる基盤技術を確立することとし、

2007年度においては、ダイナミックネットワーク技術の要素技術について、基本設計・試作を行う。

l) IP化の進展に対応した通信端末のセキュリティ機能の確保の推進（総務省）

IP化の進展に伴い、通信端末とネットワークが連携してセキュリティ機能を実現することが期待されるため、これらのIPネットワークを利用する際に必要不可欠な通信端末の基本機能の在り方及び所要の機能の確保に必要な推進方策について、2007年度中に方向性を得る。

イ) 短期的な研究開発・技術開発の施策

a) 短期的目標設定のなされている研究開発・技術開発の投資バランスの改善検討（内閣官房、内閣府、警察庁、総務省、文部科学省、経済産業省及び防衛省）

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に関する分析を2007年度中に開始する。

b) 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）【再掲】

2007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。

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（内閣官房）【再掲】

2006年度に、電子政府に係る情報システムを構成する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ったところ、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2007年度に実

施する。

d) デジタルフォレンジック[13]の確立に向けた技術開発等の推進（警察庁）

２００７年度において、デジタルフォレンジックの確立に向け民間企業等との技術協力を推進するとともに、情報技術の解析に係る技術開発を推進する。

e)高い保証レベルを有する情報システムの開発及び評価（防衛省及び経済産業省）

防衛省は、２００６年度に引き続き、情報技術セキュリティ評価基準ＩＳＯ／ＩＥＣ１５４０８で規定される評価保証レベルＥＡＬ６相当を満足する情報システム及び評価方法論(Evaluation Methodology)の研究を実施する。２００７年度は、これまでに製作した試作品を使用した評価試験を継続する。また、防衛省とIPAとの間で、防衛省が取得したセキュリティ評価技術の新たな国際的な評価基準への適用に関する事項について研究協力を行う。

f)ネットワークのオールIP化に対応した重要通信の運用技術の確立（総務省）

ネットワークがオール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、国内外の運用手法の調査を 2007 年度に実施する。

g) 情報セキュリティ関連製品・サービスの新しい傾向に関する調査（内閣官房、総務省及び経済産業省）

２００７年度に、優れた情報セキュリティ対策技術等を有する製品・サービスを調査するための方策等とともに、当該調査結果及び関連情報を、政府機関、地方公共団体、重要インフラ事業者に周知するための方策等を検討する。

ウ) 萌芽的研究開発への投資強化への検討

a)萌芽的研究開発に係る基本方針等の策定（内閣官房、内閣府、警察庁、総務省、文部科学省、経済産業省及び防衛省）

民間での技術開発が行われている領域については民間の自主性に任せ、民間の取組みが乏しい萌芽的な研究については公的資金を投入する等のポートフォリオに関する分析を２００７年度中に開始する。

b)高信頼性端末の電子認証基盤の研究開発（経済産業省）

13 「デジタルフォレンジック」とは、不正アクセスや機密情報漏洩などコンピュータに関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。Digital Forensics。

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2007年度に実施する。

③ 「グランドチャレンジ型」研究開発・技術開発の推進

情報セキュリティ対策においては、対症療法的な対応だけでなく、中長期的な視野に立ったビルトイン型の研究開発等が重要である。したがって、情報セキュリティ技術の研究開発・技術開発においても、短期的な問題解決のための技術開発だけでなく、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・技術開発に取り組むこととする。

【具体的施策】

ア）「グランドチャレンジ型」のテーマ検討（内閣官房及び内閣府）

総合科学技術会議と情報セキュリティ政策会議の連携の下、グランドチャレンジ型に相応しいテーマについて、具体的な検討を開始する。

第2節 情報セキュリティ人材の育成・確保

政府は、政府機関の対策のための人材育成、重要インフラの対策のための人材育成、企業の対策のための人材育成に取り組むと同時に、2007年度に以下の施策を重点的に推進する。

①多面的・総合的能力を有する実務家・専門家の育成

情報セキュリティ関連の高等教育機関（大学院等を中心）において、他分野の学生や社会人を受け入れる等、多面的・総合的能力を有する人材の育成・確保やリカレント教育 への主体的な取組みを促進する。

【具体的施策】

ア）先導的ITスペシャリスト育成推進プログラム（文部科学省）

2007年度に、大学院において産学連携により、国民が安全・安心にITを活用できる環境を構築するための高度セキュリティ人材育成プログラムを開発・実施する拠点形成を支援する。

イ）組織におけるIT利用者向けのセルフチェックツールの機能強化等（経済産業省）【再掲】

2007年度中に、組織におけるITの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及びこれを活用したセルフチェックツールの機能強化等を行う。

ウ) 客観的な高度IT人材評価メカニズムの構築（経済産業省）【再掲】

客観的な人材評価メカニズムの構築に向けて、2007 年度中に、情報セキュリティ人材を含めた高度IT人材に求められるスキルを体系的に整理した共通キャリア・スキルフレームワークを構築する。

エ) 産学官協議会の設置（経済産業省）【再掲】

2007 年度に、産業界が求める高度IT人材像や産業界及び教育界における実践的な高度IT人材育成手法について検討する産学官協議会を設置する。

オ) ファカルティ・ディベロップメントの支援（文部科学省及び経済産業省）【再掲】

情報セキュリティ分野を含めた各情報分野における実践的な教育を促進するため、教員の能力向上のための各大学等のファカルティ・ディベロップメント（FD）の取組みを支援する。

カ) 情報処理技術者試験制度の改革（経済産業省）【再掲】

情報セキュリティ人材を含めた高度IT人材の育成強化のため、情報セキュリティ分野を含めた各情報分野の人材スキルを測る情報処理技術者試験を抜本的に見直し、共通キャリア・スキルフレームワークとの整合性を確保した上で、2008 年度を目途に新たな試験を実施する。

キ) 情報通信人材研修事業支援制度（総務省）【再掲】

情報通信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、2007年度においても助成を行う。

ク) 高度情報通信人材育成体系の開発（総務省）【再掲】

2007年度に、企業等の情報化戦略や新たなビジネス創出を担う人材を育成するため、情報通信セキュリティ分野を含むICTマネージメント分野の実践的なPBL（Project Based Learning）教材を開発する。

②情報セキュリティに関する資格制度の体系化

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）、各組織の情報システムの運用担当者等それぞれに応じた適切なスキルを確定し、情報セキュリティに関する資格制度の体系化を推進する。

第3節　国際連携･協調の推進

情報セキュリティ分野に関する国際連携･協調の推進に関し、政府は、2007年度に以下の施策を重点的に推進する。

①国際的な安全･安心の基盤づくり･環境の整備への貢献

ＯＥＣＤやG8等の多国間の枠組みにおける協力を推進するとともに、重要インフラ防護のための早期警戒･監視･警報ネットワーク等へ積極的に参加すること等により、諸外国の関係機関との情報交換等の連携を強化する。この際、横断的な情報セキュリティ問題に関する我が国としてのＰＯＣ(Point of Contact)の機能を明確化し、より効果的で円滑な連携の促進を図る。

さらに、国際的なレベルでの文化醸成、リテラシー向上に努め、国際面でも、環境整備に貢献していく。

【具体的施策】

ア) 国際協調･貢献に係る検討(内閣官房及び全府省庁)

「情報セキュリティ先進国」の実現を目指す上で、国際的に連携すべき具体的な事項や連携先等を明確化し、また、国内外に向けて積極的に情報発信するための「ジャパンモデル」を明確化するため、政府全体として戦略的に国際協調･貢献に取り組むための基本方針及び具体策を2007年度に検討する。

イ) 多国間の枠組み等における国際連携･協力の推進(内閣官房及び全府省庁)

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、2007年度においては、G8、ＯＥＣＤ、ＡＰＥＣ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。また、諸外国の情報セキュリティ対策の動向を把握した上で、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。さらに、必要に応じ2国間の横断的政策対話の場において、情報セキュリティについても議論を行うこと等を通じて、海外の関係政府機関との政策対話を強化する。

ウ) 国際的なPOC機能としてのプレゼンスの明確化(内閣官房)

府省庁横断的な情報セキュリティ案件又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、2007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。

エ）情報セキュリティ政策に関する国際的な広報活動の推進（内閣官房）

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2007年度に実施する。

オ）国際的なセキュリティ文化実現のための取組み（内閣官房）

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、OECDにおける当ガイドラインの改訂作業の進捗を踏まえつつ、2007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。

カ）国際的な意識・リテラシー向上のための取組み(内閣官房、総務省及び経済産業省)

2007年度に、情報セキュリティに係る国際的な意識・リテラシー向上のための方策について検討し、必要に応じて、政策対話等の場を通じて諸外国との間での議論を深める。

②情報セキュリティ領域での我が国発の国際貢献

我が国発の付加価値の高いイノベーションの創出、先見性をもった技術開発の国際的活用、「ベストプラクティス（模範例）」の普及・啓発、国際的な標準開発への貢献等を通じ、我が国の強みを発揮しつつ、我が国の役割を積極的に果たしていく。

【具体的施策】

ア）ベストプラクティスの国際的な発信・普及（内閣官房及び全府省庁）

世界最先端のIT国家として貢献するため、2007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。

イ）海外の CSIRT の体制強化の支援（経済産業省）

JPCERT/CC を通じ、アジア太平洋地域等における海外CSIRTの構築を支援する。具体的には、2007年度に、同地域におけるCSIRTの集まりであるAPCERTとも連携しつつ、JPCERT/CCにおけるインシデント対応業務の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するとともに、アジア太平洋地域等に

おける海外CSIRTと国内関係機関との連携によるインシデント対応演習の実施を推進することにより、これらの機関の能力向上を図る。

ウ) アジア太平洋地域等でのインターネット定点観測情報の共有促進（経済産業省）

2007年度に、JPCERT/CC において、アジア太平洋地域等の関係機関等と連携しつつ、同地域を対象としたインターネット定点観測情報共有システムの構築について検討を開始する。

エ) 攻撃手法の分析能力の強化及び分析結果情報の共有の促進（経済産業省）

攻撃に対して効果的な防御策を策定するため、攻撃に利用される技術や手法及びその傾向等を分析し、世界各国のセキュリティ関連組織の間で分析結果を共有する仕組みについて、検討を行う。

具体的には、2007 年度に、IPA 及び JPCERT/CC において、攻撃手法の分析能力の高度化、分析結果を安全かつグローバルに共有するためのベストプラティクス等について、検討を行う。

オ) 電気通信事業における情報セキュリティマネジメントガイドラインの国際規格化（総務省）

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）」について提案を行なったところであるが、2007年度には、本提案が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。

第4節　犯罪の取締り及び権利利益の保護・救済

サイバー空間が安心して安全かつ快適に利用できるものとすることが必要であるという観点を踏まえ、政府は、2007年度に以下の施策を重点的に推進する。

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

法執行機関のサイバー犯罪捜査の技能水準の向上や体制の強化を図るとともに、サイバー犯罪条約の締結に伴う法制度の改正や国際協力の強化により、サイバー犯罪の取締りを強化する。あわせて、他の権利利益である通信の秘密をはじめとする基本的人権に十分配慮しつつ、サイバー空間における権利利益の保護・救済

のための基盤のさらなる整備に努める。

【具体的施策】

ア) サイバー犯罪の取締りの強化

a) サイバー犯罪の取締りのための技能水準の向上（警察庁）

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、2007年度において積極的に推進する。

b)サイバー犯罪の取締りのための体制の強化・整備（警察庁）

地理的制約を受けず県境を越えて敢行され、かつ、多様化・複雑化するサイバー犯罪を的確に取り締まるための捜査体制を2007年度に強化・整備する。

c) サイバー犯罪の取締りのための捜査・解析用資機材の充実・強化（警察庁）

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締結に伴う新たな法制度の施行に対応するため、2007年度において、アクセス記録の解析、コンピュータウイルス等の動作検証、電磁的記録の復元等を行うための資機材の整備・増強を推進する。

d) サイバー犯罪に適切に対処するための法整備等の推進（法務省）

近年における情報処理の高度化の状況等にかんがみ、ハイテク犯罪に適切に対処すべく、サイバー犯罪条約を締結するための法整備等を推進する（「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」を第163回国会に提出したところ，現在継続審議中。）。

e) 重要インフラに対するサイバーテロ対策に係る官民の連携強化（警察庁）

2007年度において、重要インフラ事業者等の業務の特性を踏まえつつ、必要に応じ、サイバーテロ対策の意識の向上につながる啓発活動を行う。

f) サイバー犯罪の取締りのための国際連携の推進（警察庁）

2007年度において、我が国のサイバー犯罪情勢に関係の深い国々の法執行機関との効果的な情報交換を実施するとともに、G8 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積極的な参加、アジア大洋州地域サイバー犯罪捜査技術会議の主催等を通じた多国間における協力関係の構築を推進する。

g) 中央当局制度[14]を活用した国際捜査共助の迅速化（法務省）

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直接中央当局間で共助実施のための連絡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刑事共助条約が既に発効しているところ、2007年度においては、香港、中華人民共和国及びロシア連邦との間でも同種の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。

h) 重要無線通信妨害対策の強化（総務省）

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、2006年度に引き続き「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、2007年4月より混信その他の妨害に係る原因究明を強化するための体制整備を行うなど、電波監視の強化を図る。

i) デジタルフォレンジックに係る知見の集約・体系化等の推進（警察庁）

2007年度において、犯罪の立証のための情報技術の解析に係る知見の集約・体系化を推進するとともに、デジタルフォレンジック連絡会の開催等を通じて国内関係機関との連携強化を推進するなど、デジタルフォレンジックの確立に向けた取組みを推進する。

イ）サイバー空間における権利利益の保護・救済のための基盤の整備

a)サイバー空間における権利利益の保護・救済のための基盤に係る調査研究（内閣官房）

サイバー空間における権利利益の保護・救済のための基盤の整備に資するため、サイバー空間における権利利益の侵害が起こった際の対応のあり方、情報の流出・不正取得に対する法的措置も含めた対策及び本人認証を容易に行うことが可能な環境の整備の必要性について、海外の状況も踏まえつつ、2007 年度に調査研究を実施する。調査研究の結果については公表するとともに、これを踏まえ

14 「中央当局制度」とは、特定の当局を中央当局として指定し、外交ルートを経由せずに中央当局間で共助の授受を行なう制度を指す。

て関係省庁に必要な働きかけを行う。

b)プロバイダ責任制限法及び関係ガイドラインの周知の促進（総務省）

サイバー空間において利用者が権利利益の侵害を受けた際の救済のため、2007 年度に、特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（プロバイダ責任制限法）の周知を促進する。具体的には、広報啓発等を通じて利用者に対する当該法の周知を図るとともに、業界団体等による関係ガイドラインの周知を支援する。

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

通信相手が誰なのかをすべての通信当事者の承認の下に確認可能とするための認証技術その他のサイバー空間の安全性及び信頼性を向上させるための技術の開発・普及を推進する。

【具体的施策】

ア）サイバーテロ対策に係る大学との共同研究の推進（警察庁）

2007 年度において、大学と連携して、ファイアー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推進する。

第5章　政策の推進体制と持続的改善の構造

政府は、2007年度に、前章に示した重点政策に、以下に示す体制と持続的構造の下で総合的に取り組むこととする。

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

内閣官房情報セキュリティセンター(NISC)は、政府全体の情報セキュリティ政策に関する基本戦略の立案、成果を政府が活用することを前提とした新たな研究開発・技術開発の主導等による情報セキュリティに関する技術戦略の立案、政府機関の情報セキュリティ対策の検査・評価、重要インフラの情報セキュリティ対策のための相互依存性の解析、「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」の策定・見直し、分野横断的演習の推進や、横断的な情報セキュリティ問題に関する国際POC(Point of Contact)としての機能を果たすなど、国際的にも国内的にも、最高の英知を結集していくための体制として、政府全体の推進体制を有効に機能させるための中核として強化することを目指す。

さらに、内閣官房情報セキュリティセンター(NISC)は、情報セキュリティにかかわる多くの知見が民間に蓄積されていることから、民間の人材を積極的に活用することに努め、同時に、政府職員の人材育成の中核拠点として機能することを目指す。

【具体的施策】

ア) 内閣官房情報セキュリティセンター(NISC)の強化(内閣官房)

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)の人員体制を継続的に確保し、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、政府機関対策としては、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3章第1節に示した施策を実施する。また、政府機関統一基準関連の対応及び緊急時対応以外にも、電子政府の情報セキュリティ強化のための対応など各府省庁の情報セキュリティ対策推進に向けた様々なニーズに対応するべく、取組みを行う。重要インフラに関する対策としては、情報セキュリティ対策に係る行動計画等に従って、第3章第2節に示した施策を実施する。

さらに、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)の体制・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、加えて、情報収集の充実、関係機関等との情報の共有・分析機能の強化を図り、横断的な情報セキュリティ政策推進の中核としての機能を確保する。また、情報セキュリティ政策の推進において必要となる基礎情報や様々な動向などについて調査・検討を行う機能を拡充する。

イ）各府省庁の情報セキュリティ対策推進のための情報セキュリティ・コンサルティング機能の充実（内閣官房）

各府省庁の情報セキュリティ対策の推進を支援するため、内閣官房情報セキュリティセンター（NISC）は、政府機関統一基準関連の対応、緊急時対応、及び電子政府の情報セキュリティ強化のための対応など、各府省庁の情報セキュリティ対策推進に向けた様々なニーズへの対応のため、同センターの専門家による情報セキュリティ・コンサルティング機能の充実を図る。

ウ）潜在的に大きなリスク等への政府としての対処方法のあり方の検討（内閣官房）

潜在的に大きなリスク（例えば、2000年問題（Y2K問題）のようなもので、将来発生しうるものを想定）や現行の政府の体制では解決が難航しうる課題（例えば、府省庁間で所掌の所在がはっきりしないもの等を想定）を取り上げ、対処するための、政府としての方法のあり方を検討し、2007年度中に結論を得る。

（2）各府省庁の強化

各府省庁は、今後、情報セキュリティ政策会議、内閣官房情報セキュリティセンター（NISC）を中核とした、政府全体の情報セキュリティ対策を積極的に推進すべく、自府省庁の情報セキュリティ体制の充実・強化を図るとともに、従来の縦割りになりがちな推進体制を改め、官民における統一的・横断的な情報セキュリティ対策の推進が行われるよう、各種政策の実施に努めることとする。

【具体的施策】

ア）情報セキュリティ対策の体制の強化及び府省庁横断的な取組みの実施（全府省庁）

2007年度において、各府省庁は、引き続き、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。

イ）情報セキュリティ分析部門（仮称）の創設に向けた検討（経済産業省）

国内外の関連データや研究結果を幅広く収集、分析等するため、2007 年度に、

国内の関係機関に情報セキュリティ分析部門（仮称）を創設することについて検討を行う。

第2節　他の関係機関等との連携

第2節　他の関係機関等との連携

基本計画は、我が国の情報セキュリティ問題を俯瞰した中長期の戦略を定めるものであるが、情報セキュリティ政策は、国民生活・社会経済活動に広く関係するものであり、その実施に当たっては、様々な関係機関との連携を行っていく必要がある。

様々な関係機関の中でも、IT戦略本部との関係においては、情報セキュリティ政策がIT政策の主要な部分の一つとして位置付けられるものであり、かつ、基本計画が「IT新改革戦略」の情報セキュリティ関連部分を実質的に担うものであることに留意する必要がある。また、総合科学技術会議との関係においては、情報セキュリティ政策のうち研究開発・技術開発関連部分と全体の科学技術政策とが整合して推進されることを確保する必要がある。したがって、情報セキュリティ政策会議及び内閣官房情報セキュリティセンター（NISC）は、両者の十分な協力を得つつ、情報セキュリティ政策を推進することとする。

【具体的施策】

ア）関係機関等との連携強化（内閣官房及び内閣府）

2007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・会議との連携を密にし、これらとの役割分担を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。

特に、総合科学技術会議との関係において、第3期科学技術基本計画期間中における分野別推進戦略（情報通信分野）に基づき、内閣官房情報セキュリティセンターとの連携を保ちつつ、2007年度以降も引き続き、セキュリティ領域における研究開発・技術開発を推進する。また、防災・減災における情報セキュリティ対策のあり方については、中央防災会議等、他の関連する会議等との意見交換を密にすることにより緊密に協力し、重要インフラの情報セキュリティ政策を一体的に推進する。

第3節　持続的改善構造の構築

情報セキュリティを巡る問題は、新たなリスク要因が次々と発生し、また想定し得なかった事故、災害や攻撃が発生する等、その状況変化が早いことから、政策の効果を常に評価し、改善を行うことが必要である。このため、政府は、以下のような持続的改善のための構造を構築することが必要である。

(1)「年度計画」の策定とその評価等

政府は、基本計画の実現を図るため、毎年度、より具体的な施策の実施プログラムを「年度計画」として策定するとともに、その実施状況を評価し、その結果を可能な限り公表する。

なお、政府以外の関係機関における対応が不可欠である等、施策を円滑に進捗させる観点から、中長期的な計画を定めることが必要なものについては、単年度にこだわらず、複数年度のマイルストーン設定も検討する。

【具体的施策】

ア) 評価等[15]の実施及び公表(内閣官房)

セキュア・ジャパン2007に記載されている具体的施策の取組状況について、半年ごとに進捗状況を公表するとともに、年度末にはその評価等を実施する。

イ) 政府機関の情報セキュリティ対策強化に向けたマイルストーンの検討等(内閣官房)

2007年度第一四半期において、基本計画の実現に向けた2008年度までのマイルストーンとして、政府機関自らの情報セキュリティ向上のための対策に係る定常的な評価のスケジュールや評価項目、評価項目選定の趣旨などについて策定する。

ウ)「重要インフラの情報セキュリティ対策に係る行動計画」の見直し(内閣官房)【再掲】

2007年中に、各重要インフラ所管省庁の協力を得て、「重要インフラの情報セキュリティ対策に係る行動計画」の見直しに向けて、重要インフラ分野における情報セキュリティ対策向上の状況についての調査・把握に着手する。その際、災害発生時における対応等、他の関連する省庁横断的な取組みとの整合性の確保、連携についても検討を行う。また、官民の連携の在り方についても継続的に検討を行う。

(2) 年度途中での緊急事態対応に向けた取組みの実施

政府は、「年度計画」の実施途中であっても、新たなリスク要因や想定し得なかった事故、災害や攻撃の発生等の緊急事態に対応するための取組みを実施する。

---

15 本施策においては、「「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」(2007年2月2日情報セキュリティ政策会議決定)の「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。

【具体的施策】

ア）計画の見直しについての検討（内閣官房）

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2007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。

（3）評価指標の確立

各対策実施領域等における、情報セキュリティに関する評価の指標は、これまで確固としたものが策定されてこなかったところであるが、このような指標は、各対策実施領域等における、情報セキュリティ対策の浸透の度合いを評価するために不可欠なものであることから、政府は、これを早急に検討し、基本計画の実施状況を評価するものとして活用することを目指す。

【具体的施策】

ア）情報セキュリティ対策に関する評価指標の確立（内閣官房、総務省及び経済産業省）

2006年度中に確立した評価指標に基づき、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から、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）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指標の政府内及び国際機関における活用を推進するとともに、評価の結果等を受けて当該評価指標の改善を検討する。また、評価等[16]にあたっては補完調査も適宜実施することから、調査担当機能を内閣官房が強化しつつ評価等のプロセス全体の円滑な推進を図る。

なお、2006年度に、上記評価指標の確立に資するものとして、総務省において、SJ2006第2章第2節④に掲げる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が、2007年度には、より多くの電気通信事業者において当該評価指標の活用を促進し、評価結果等を受けた当該評価指標の改善等を検討する。

16 本施策においては、「「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」（2007年2月2日情報セキュリティ政策会議決定）の「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。

第6章　2008年度の重点施策の方向性

～2008年度の重点「情報セキュリティ基盤の強化に向けた集中的取組み－情報セキュリティ人材の育成・確保、情報セキュリティ政策の国際展開、電子政府等の情報セキュリティ強化を中心に－」～

第3章から第5章までは、3か年計画である基本計画の2年目として、2007年度に実施すべき具体的施策を挙げてきた。これらは、初年度であった2006年度の取組みを受け継ぎ、**「官民における情報セキュリティ対策の底上げ」**を重点とするものである。この2年間の取組みの結果、情報セキュリティ対策の水準は、基本計画の目標実現に向けて各対策実施主体において一定程度まで向上するものと見込まれる。

しかしながら、第2章第3節で述べたように、情報セキュリティ対策においては、1）取組みの開始から実際に効果が現れるまでに時間をかける必要がある分野も少なくはない。また、2）対策の取組みを開始したもののその取組みはまだ入り口の段階に過ぎず、今後取組みを加速化するべき分野、3）時宜に合った喫緊の課題として迅速な対応が必要となる分野も存在すると考えられる。

こうした観点から見ると、第1章及び第2章の中で示されているように、情報セキュリティ人材の育成・確保という情報セキュリティ基盤の構築・強化は、様々な側面で急がれる課題であり、2007年度の単年度を超えて継続的・集中的に取組みを行う必要がある。また、国際連携・協調の推進を中心とする情報セキュリティ政策の国際展開は、第1章で述べたように、依然として第一歩目を踏み出したに過ぎず、2007年度に続いて、取組みの一層の加速化が必要である。さらに、電子政府基盤の情報セキュリティ強化のための取組みは、電子政府を構成する様々なシステムの構築スケジュールも考慮しつつ、適時適切に行われるべきである。

これらを踏まえて、基本計画の最終取組み年度である2008年度は、**「情報セキュリティ基盤の強化に向けた集中的な取組み」**を重点として、それまで取り組んできた方向性に則した施策に引き続き注力するとともに、特に、以下の方向性で施策の推進を図ることとする。

第1節　情報セキュリティ人材の育成・確保に向けた集中的な取組み

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、2007年度においては、人材育成・資格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が、2007年度の一年間という短期間で十分に解決

がなされるとは考えられない。このため、基本計画の最終取組み年度である２００８年度においては、当該分野について継続的かつ集中的に取組みを図ることとする。

【具体的施策】

ア）業界横断的な人材育成支援体制の整備と総合的な人材育成・確保支援（内閣官房、総務省及び経済産業省）

我が国全体における情報セキュリティ人材の質の向上と量の拡大を効果的に推進するため、資格制度を含めた各種教育プログラムを運営する団体による業界横断的なセキュリティ人材の育成支援体制を整え、総合的な人材育成・確保の支援を図る。

イ）先導的ＩＴスペシャリスト育成推進プログラム（文部科学省）

高度なセキュリティ人材の育成を目的とするプログラムを開発・実施する拠点形成の支援を行うとともに、プログラムの開発・実施を通じて得られた教育用教材等の成果の他大学等への普及・展開の実施を推進する。

ウ）政府機関における情報セキュリティ人材の重点確保（全府省庁）

政府機関における情報セキュリティ対策に係る人材の慢性的な不足状況を踏まえ、各府省庁における情報セキュリティ対策の要となる者の確保を図る。

エ）政府職員向け教育プログラムの充実（内閣官房及び総務省）

２００７年度における検討状況を踏まえつつ、政府職員（一般職員、幹部職員及び情報セキュリティ対策担当職員）向けの政府統一的な教育プログラムについて、その質の向上及び受講回数等の拡大を図る。

オ）ネットワーク利用者の情報セキュリティに関する意識・能力向上の一層の促進（総務省）

ネットワーク利用経験の浅い初心者層等に対する情報セキュリティ意識の一層の向上を図るための取組みを推進するとともに、利用者自らが直面したセキュリティ脅威に適切に対応できるよう、ＷＥＢサイトの活用等により、利用者自身のセキュリティ脅威への対応能力の向上に向けた取組みの強化を図る。

カ）わかりやすく実用的な情報セキュリティ対策を学べる教育コンテンツの作成・配布（総務省及び経済産業省）

小中学校及び高等学校の教師、児童生徒が、インターネットを安全に活用するための考え方、リテラシー能力やノウハウを学べる環境を整備するため、情報セキュリティに関する最新の動向も踏まえつつ、小中学校及び高等学校での授業等において、教育コンテンツの活用の促進を図る。

キ) 中小企業における情報セキュリティ対策の推進（経済産業省）

中小企業の負担の低減及び情報セキュリティ対策の推進を目的として、中小企業における情報セキュリティ対策を担当する人材の業務の効率化を図るため、中小企業向けの情報セキュリティ対策のパッケージ及び、対策の実施状況を確認するための標準フォーマットの策定等を推進する。

ク) 保証型情報セキュリティ監査の普及（経済産業省）

監査人が一定の保証を与える保証型情報セキュリティ監査の普及のため、保証型監査ガイドラインを作成等するとともに、その普及方策について検討を行う。

ケ) サイバーテロ対策に係る体制等の強化（警察庁）

サイバーテロの手法の高度化、2008年サミットの開催等によるサイバーテロの脅威の増大に対応するため、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の強化を推進するほか、重要インフラ事業者等に対して、それぞれの業務の特性を踏まえつつ、必要に応じ、サイバーテロ対策の意識の向上につながる啓発活動を行う。

コ) サイバー犯罪の取締りのための体制の強化・整備及び技能水準の向上（警察庁）

多様化・複雑化するサイバー犯罪に対して、デジタルフォレンジックを的確に活用した取締りを推進するため、捜査体制の強化・整備に努めるほか、サイバー犯罪捜査に従事する全国の警察職員に対してデジタルフォレンジック等に係る部内外の研修を推進する。

第2節　情報セキュリティ政策の国際展開に向けた集中的な取組み

国際連携・協調を中心とする情報セキュリティ政策の国際展開については、2007年度に政府全体として戦略的に国際協調・貢献に取組むための基本方針及び具体策を検討することとしている。2008年度においては、これに基づく取組みを本格化・加速化を図ることとする。

【具体的施策】

ア) 内閣官房情報セキュリティセンター（NISC）による窓口機能の強化　（内閣官房）

IT の基盤が、24時間・365日、常時世界とつながっていることから、内閣官房情報セキュリティセンター（NISC）に、国内外からの政府機関の情報セキュリティ問題に係

る情報連絡に迅速･適切に対応できる体制を、2008年度中に構築を図る。

イ）2007年度に策定する国際戦略の推進　（内閣官房及び全府省庁）

国内外に向けて積極的に情報発信を行うため、また、政府全体として戦略的に国際協調･貢献に取り組むために、2007年度に策定する基本方針及び具体策に基づき、2008年度に情報セキュリティに関する国際関係の活動の戦略的な推進を図る。

ウ）情報セキュリティ政策に係る国際会合の開催（内閣官房及び関係府省庁）

情報セキュリティに関わる政策担当者や専門家が官民より幅広く参加して、お互いの知識や経験など交換しあえるような国際会合の2008年度における開催を図る。

エ）組織管理策･関連ガイドライン等の充実及び国際展開等（経済産業省）

情報セキュリティ面も含めた情報システムの管理策など、組織管理策･関連ガイドライン等について充実を図るとともに、国内のみならず海外への情報発信に努める。

また、アジア太平洋地域の国々における企業等の情報セキュリティ対策の底上げに貢献すべく、これら国々に対して、情報セキュリティ対策ベンチマークの内容等を紹介する。

オ）CSIRT 及び関連組織の国際的な対応体制の強化、情報連携の高度化（経済産業省）

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、2008 年度中に、IPA や JPCERT/CC 等による「コンピュータセキュリティ早期警戒体制」を強化する。具体的には、情報セキュリティ問題に係る情報収集の強化、収集した情報を効果的･効率的に発信する仕組み、国際連携の強化等について検討を行う。

特に、アジア太平洋地域等のコンピュータセキュリティ緊急対応チーム（CSIRT）の体制強化を行うとともに、これら CSIRT との定点観測データの共有、可視化システムの構築、マルウエア解析･分析情報の共有等、連携範囲の拡大やレベルの高度化を図る。

カ）情報セキュリティ分析部門（仮称）の創設（経済産業省）

諸外国の機関とも連携等しつつ、国内外の関連データや研究結果を幅広く収集、分析等するため、国内の関係機関に情報セキュリティ分析部門（仮称）の創設を図る。

キ）情報セキュリティに関する情報収集及び分析機能の充実（総務省）

国内外の関係機関との連携を視野に、独立行政法人 情報通信研究機構(NICT)

情報通信セキュリティ研究センターにおける、情報セキュリティに関する情報収集・管理、分析・対策に係る研究等を推進するとともに、Telecom ISAC (Information Sharing and Analysis Center：インシデント情報共有・分析センター) Japan において、関係機関との情報分析・共有等を推進する。

ク) G8司法内務閣僚会合を通じた国際連携・協力の推進（警察庁）

2008年に我が国で開催されるG8司法内務閣僚会合において、関係各国とサイバー犯罪の現状等についての共通認識を深めるなど、サイバー犯罪対策の加速化を図る。

ケ) デジタルフォレンジックに係るアジア大洋州地域における国際連携・協力の強化（警察庁）

デジタルフォレンジックに係るアジア大洋州地域における国際連携・協力を強化するため、アジア大洋州地域サイバー犯罪捜査技術会議の参加国拡大等によるデジタルフォレンジックに係る情報共有機能の強化を図る。

第3節　電子政府等の情報セキュリティ強化のための総合的な取組み

現在、電子政府に関しては、「重点計画－2006」（2006年7月26日IT戦略本部決定）及び「電子政府推進計画」（2006年8月31日各府省情報化統括責任者（CIO）連絡会議決定）等に基づき、担当府省庁において様々な施策が進められている。府省共通の業務については、集中型のシステムによる全府省庁統一的な運用が進められることとなっており、また、全体最適化に向けた取組みにあたって、府省共通システムの集中化・共同利用化の検討等が進められることとなっている。2008年度においては、これらにあたっての情報セキュリティの観点からの検証をはじめ、電子政府の情報セキュリティ強化のための総合的な取組みを図ることとする。

また、電子自治体に関しては、政府機関の取組みも踏まえながら、情報セキュリティ強化のための方策を講じる必要がある。

【具体的施策】

ア) 電子政府の情報セキュリティを企画・設計段階から確保する（Security by design）ための方策の強化（内閣官房、総務省及び関係府省庁）

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、情報セキュリティを基本コンセプトとして取り入れた情報システムの企画・設計が行われるための方策を強化する。

イ) 電子政府に係る情報セキュリティリスクの検証の推進とその手法の統一化の推進（内閣官房及び関係府省庁）

電子政府の情報セキュリティ強化のため、擬似的な攻撃による脆弱性の検証や政府機関内外で発生したIT障害に係る分析等を通じて、情報セキュリティリスクの検証を行うことなどにより、政府機関において導入すべき情報セキュリティ対策の現場の実態に応じた検証手法や実施方法等を検討し、その統一的な運用を推進する。

ウ) 情報セキュリティの維持・向上に向けた暗号政策の検討（内閣官房、総務省及び経済産業省）

情報システムにおける安全性及び信頼性を確保するため、2007年度の政府機関における検討結果等を踏まえ、安全な暗号利用方策について、そのあるべき姿の検討と体系的な推進を図る。

エ) GSOCの着実な運用と分析・解析機能の強化（内閣官房）

2007年度に整備するGSOCについて、その着実な運用を図る。また、その運用状況を踏まえて政府機関に対するサイバー攻撃等に関する全般的な傾向や情勢について分析を行い、各政府機関に対してその結果を定期的に提供するとともに、個々の対策に必要となる攻撃手法の分析結果等の情報を適宜提供するための体制の強化を図る。また、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））の構築を図る。

オ) 地方公共団体における暗号利用の促進方策等の検討（総務省）

政府機関における取組みを踏まえ、暗号利用など地方公共団体ではこれまで十分でなかった情報セキュリティ対策について、効果的な利用促進策を検討する。また、地域における情報セキュリティ向上等のため、地域レベルでの官民連携や住民に対する周知・啓発等の進め方を検討する。