セキュア・ジャパン2008

－情報セキュリティ基盤の強化に向けた集中的な取組み－

（案）

情報セキュリティ政策会議

年　月　　日

目次

第1章　セキュア・ジャパン2007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2007に基づく取組みの背景

我が国の国民生活及び社会経済活動においてITへの依存度が高まる中、ITの利活用における安心・安全を確保するため、情報セキュリティが重要な課題となっている。このような状況を踏まえ、2006年度から2008年度の3年間を対象期間とする第 1 次情報セキュリティ基本計画（以下「基本計画」という。）の下、2006年度にはセキュア・ジャパン2006（以下「SJ2006」という。）が策定され、初年度の取組みが行われた。結果、2006年度末には、

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

という「取組みの第一段階」が進んだ状況であった。

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

第2節　2007年度の重点目標と取組みの柱立て

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

SJ2007では、「官民における情報セキュリティ対策の底上げ」を目標に、(1)官民各主体の共通認識の形成は概ねできたことから、共通認識の維持・向上を図り、(2)情報セキュリティ政策会議技術戦略専門委員会での検討も踏まえつつ、引き続き先進的技術の追求を図り、(3)人権保障や、公的部門の活動の透明性や適法性の確保とバランスを維持しつつ、公的部門の戦略的な対応能力強化を図り、(4)国内におけ

る官民の各主体間や、国際的な主体間での連携・協調の推進を図ることが重点として設定され、対策実施主体が施策の取組みを進めた。

具体的には、2006年度に引き続き、「対策実施4領域」、「横断的な情報セキュリティ基盤」、「政策の推進体制と持続的改善の構造（政策の推進体制の強化、他の関係機関等との連携、持続的改善構造の構築）」という基本計画の柱立てに基づいて具体的な施策を実施することとし、内閣官房を含む各府省庁が計159の取組みを行うこととなった。

また、SJ2007では、「情報セキュリティ基盤の強化に向けた集中的な取組み」という2008年度の重点施策の方向性が設定され、「情報セキュリティ人材の育成・確保に向けた集中的な取組み」、「情報セキュリティ政策の国際展開に向けた集中的な取組み」、「電子政府等の情報セキュリティ強化のための総合的な取組み」として、計24の具体的施策が盛り込まれた。

第3節　2007年度の評価

SJ2007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。以下「NISC」という。）が評価等[1]を行った上で、「2007年度の情報セキュリティ政策の評価等」（以下「評価2007」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2007が示唆する方向性などを抽出するとともに、2008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、2007年度の評価を行う。この際の主眼は、2007年度の情報セキュリティ政策が社会に与えた変化や情報セキュリティに関連のある事象などをすべて網羅的に把握することにあるのではなく、2008年度の政策を検討するに当たって本質的な状況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2008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2008年度に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、2009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

SJ2007において、2007年度中に推進するとされた159の具体的施策の取

[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。

組み結果については、評価2007では以下のとおり分類され、評価がなされた。

Ａ　：　144 施策（90.6％、内Ａ’は５施策）
Ｂ+：　　1 施策（ 0.6％）
Ｂ　：　 12 施策（ 7.5％）
Ｃ　：　　1 施策（ 0.6％）
－　：　　1 施策（ 0.6％）

＜分類＞

Ａ：当初の予定どおり施策を推進することが出来た施策。
なお、施策は推進できたが、体制や人員に関して問題が存在するため、今後、継続して施策を推進するためにそれらの解決が必要であるということが、当該施策に関連した作業の進捗や担当へのヒアリング等から明白になった施策については「’」を付した。

Ｂ＋：年度内には完了していないが、着実に取組みを進めており、数ヶ月以内には完了する施策。

Ｂ：予定どおり施策を推進することは出来なかったが、今後も取組みを続けることにより、最終的には施策を推進することが出来る施策。

Ｃ：予定どおり施策を推進することはできず、今後の見通しも立たない施策。

－：予定どおり施策を推進することが出来なかったが,その理由が政府機関の事情によるものではない施策。

SJ2007において、2007年度中に推進するとされた施策については、各府省庁において着手がなされ、約9割の施策について当初の予定どおり施策を推進した。残り1割（15施策）の予定どおり推進できなかった施策については、情報資産台帳の整備や「go.jp」ドメインへの移行など全府省庁が実施しなければならない施策であったものの一部府省庁で実施が完了しなかったものが7施策、刑事共助条約の締結等施策を推進したものの2007年度中に完了できなかったものが6施策、刑法の改正等政府機関の事情以外の理由により推進できなかったものが1施策、他の施策の結果を踏まえた上で推進する必要があるとの判断により実施を断念した施策が1施策であった。

Aとされた144の施策は、関係各府省庁の担当者の努力により予定通り推進することができたものの、A’の5施策については、「各政府機関でのPDCAサイクルの定着」、「政府全体でのPDCAサイクルの定着」、「対策実施状況に関する評価等」、「情報セキュリティマネジメントに関する評価等」、「情報セキュリティ対策の体制の強化及び府省庁横断的な取組みの実施」と、政府機関の対策実施に係る取組みとなっている。このことから、政府機関の対策推進のための努力は

懸命に続けられているものの、体制や人員の不足が課題であることがうかがえる。

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

2. 施策の取組みによる社会的変化に関する評価・分析

(a) 政策領域

(ア) 政府機関・地方公共団体

2007年度におけるウェブサーバ等に対する重点検査の結果などにかんがみると、政府機関の対策は、十分な水準に到達したとは必ずしも言えないものの、水準の大幅な向上がみられ、短期間で一定の成果が出たと言える。これには、必要な予算獲得や対策実施を含め、担当部門を中心に各府省庁の懸命の努力が続けられたことが大きく作用しているものと考えられる。また、教育拠点や教育ツールの整備が図られるなど、情報セキュリティに係る人材の育成に資する体制・基盤の整備にも着手された状況にある。

しかし、実際の担当の体制を見ると、組織全体を担当する人数が数名程度であったり、専門性を問われる業務であるにもかかわらず、人事異動サイクルが2～3年であるために専門的能力を十分に伸ばしきれなかったり、また、組織によっては情報セキュリティ対策に係る意思決定が当該組織のトップクラスの指示でなされる体制に必ずしもなっていないといった課題が存在する。対策水準の向上は、現行体制では対応可能な限界点にまで到達しつつあるとも考えられ、今後は体制強化に向けた更なる取組みが必要である。

また、電子政府・電子自治体の取組みが推進されているが、その際に情報セキュリティの観点も考慮することが引き続き不可欠の状況にある。

(イ) 重要インフラ

2007年度は、10分野すべてにおけるCEPTOARの整備が完了し、「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）の創設に向けた検討方針の取りまとめが進められた。また、官民連携による分野横断演習も2006年度に続いて第2回が実施され、実際の対応により近い「機能演習」という形で行われた。これらにかんがみると、事業継続性の確保を軸に置いて官民の各主体間での情報共有、連絡・連携を進めるための枠組み・体制は徐々に構築されつつあると言える。また、官民が連携してこれらの取組みを推進していることを通じ、対策の重要性に係る意識も徐々に高まってきていると言える。今後、事業者の自主性を十分に尊重しながら取組みが進むよう、メリットを明らかにしつつ、さらに努力を継続す

ることが必要であると考えられる。

（ウ）企業

企業では、対策・体制の強化が徐々に進められている。また、対策の重要性に係る意識も向上している。これには、情報漏えいやシステム障害などの発生が、信用の失墜や対策への再投資などを通じて経済的損失につながり得る点が大きな影響を及ぼしているものと考えられる。また、2007年度は金融商品取引法（日本版SOX法）が施行され、IT統制の重要性に対する意識が更に高まってきたことも要因として挙げられる。

他方、例えば2006年度までのウイルス対策ソフトなどの導入状況には著しい変化はみられないことから、情報セキュリティ対策への投資は、経済的損失との比較衡量の下で、各主体の経営判断によってなされる傾向にあると推察される。

また、「情報セキュリティ対策への取組みの効果が認識しづらい」ことも指摘されている。さらに、最低限これだけは取り組めば良いという事項が見えないことからセキュリティへの過剰投資が生じ、一部では「対策疲れ」の声も聞こえる。加えて、先進的企業と、規模が小さい企業の間において、意識格差が生じているのではないかとの懸念もある。

こうした状況にかんがみると、現行の対策枠組みの下で、取組み推進の「均衡点」に到達しつつあるとも考えられる。また、現行技術水準で守ることのできるセキュリティの「限界点」に到達している可能性もある。

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

（エ）個人

個人は、他の対策実施領域に比べ、他の主体による支援が更に重要であることから、SJ2007の下で情報セキュリティに関する普及啓発・情報発信を行うことを重点に各種取組みが積極的に推進された。最近の状況を見ると、例えば、OSの定期的なアップデート、ウイルス対策ソフトの導入・活用については、徐々に伸びてきている状況であり、結果、総体としては情報セキュリティの意識が徐々に向上している。

一方で、ボットなどの新たなリスクに関する認識が希薄な面もあり、今後の継続的な意識の向上には懸念がある。また、対策の必要性の認識、対策実施状況などには、世代、性別といった属性による格差がみられる。

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

（オ） 情報セキュリティ技術戦略の推進

個別技術開発・研究開発では、セキュアVM（VM：Virtual Machine）開発においてβ版が公開され、取組みが着実に進んでいる状況にある。また、政府全体として情報セキュリティ分野への技術・研究開発を推進する枠組み作りも進展しつつある。しかし、こうした枠組みの下、戦略に基づく取組みを本格的に実施するのはこれからであり、効果的な推進が求められる。

（カ） 情報セキュリティ人材の育成・確保

「人材育成・資格制度体系化専門委員会」の報告[2]を受け、人材分野では官民幅広い取組みが実施された。結果、人材育成・確保に向けた体制・基盤の整備が進展し、人材の育成に関わる意識が浸透し始めたと言える。しかしながら、体制・基盤が磐石のものとなり、自律的に人材育成が進む状態にはなっていない。実際に多くの人間が「情報セキュリティ人材」として力を発揮するには時間を要する。社会全体のニーズを満たすに足る人材確保は未だ途上段階であると言える。

（キ） 国際連携・協調の推進

国際会議への参加や国際会議ワークショップの開催提案を通じ、議論過程に積極的に関与した。2007年度は、こうした取組みも含め、情報セキュリティ領域における我が国発の国際貢献へ向けた基本方針[3]を策定し、国際連携・協調の取組みを本格化したところである。しかし、現在は国際連携・協調へ向けて様々な政策提案を行った段階であり、今後、提案内容の実現に向けて継続的な働きかけを行うことが重要である。

（ク） 犯罪の取締り及び権利利益保護・救済

サイバー空間で発生する新たな形態の犯罪や不法行為に対し、捜査能力の向上や体制構築を進め、中長期的なリスク低減へ向け一定の取組みが推進された。安心・安全のための技術開発とその普及によるリスクの低減については、未だ技術開発自体が途上であると言え、取組みの継続、加速化が必要である。

（ｂ）社会情勢

（ア） 人的側面（人材、意識、体制・制度）

---

2 情報セキュリティ政策会議　人材育成・資格制度体系化専門委員会 『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）

3 情報セキュリティ政策会議 『我が国の情報セキュリティ分野における国際協調・貢献へ向けた取組み』（平成19年10月3日）

人材面に関しては、2007年度は、官民の積極的な取組みの展開を通じて人材育成のための体制・基盤の整備が図られ、社会全体として人材の育成に関する意識が浸透し始めたと考えられる。しかし、こうした体制・基盤が磐石のものとなって、自律的に人材育成が進む状態に至っているとは必ずしも言えない。具体的な人材育成の手法についても手探り状態であり、取組みは発展の途上にあると言える。

意識面では、2006年度には、情報セキュリティ対策の必要性に関して「意識の発露」がみられたところ、2007年度は、SJ2007に基づく各種の取組みの推進やマスコミ報道（重要情報の漏えいや基盤となるITシステムの障害の報道等）、不正アクセス行為やネットワーク利用犯罪の増加傾向などもあり、各々の対策実施領域において情報セキュリティに関する脅威の認識、対策の必要性に係る意識が向上している状況にある。きっかけは様々であるものの、情報セキュリティに係る意識は徐々に高まっているものと考えられる。

体制面については、全般的に、具体的な取組み推進のための枠組み構築が徐々に進められた一年であった。しかし、対策推進の努力はそれとして懸命に続けられているものの、政府機関の対策実施に係る対応体制は、現行体制で対応可能な限界点に到達しつつあるとも考えられる。このため、体制強化に向けた更なる取組みが必要である。重要インフラでは事業継続性の確保を軸に置いて官民の各主体間での情報共有、連絡・連携を進めるための枠組み・体制が徐々に構築されつつあると言える。企業では、ISMS取得事業者数が継続的に増加するなど、組織的な対応を含む対策、体制の強化への取組みが徐々に進められていると言える。

（イ）物的側面（投資、技術、ハード、ソフト、ネットワーク）

物的側面については、昨年度から大幅な変化はないものの、必要なものについては堅実に投資を行い、対策を着実に行おうとしている状況にあると言える。政府機関では、政府機関情報セキュリティ横断監視・即応調整チーム（Government Security Operation Coordination team。以下「GSOC」という。）整備の開始、政府機関統一基準遵守にかかわるシステム構築予算の昨年度比同水準の確保など、システム対策が着実に進められた。企業においては、2006年度までのウイルス対策ソフト又は統合セキュリティ対策ソフトの導入状況には著しい変化はみられないことから、情報セキュリティの技術的対策への投資は、経済的損失との比較衡量の下で、各主体の経営判断でなされる傾向にあると推察される。個人分野では、全体としての底上げは進みつつあると考えられるが、年代別・男女別の格差もあり、必要な対策ソフトの入手を始めとして、更なる対策実施

状況の向上が望まれる。

研究開発・技術開発では、様々な取組みが着実に進められている状況にあると言えよう。取組みの成果によって、セキュリティを確保する技術の限界水準が現在と比べて向上し、対策が大幅に進むことが期待される。

（ウ） 周辺情勢（インシデント・事件、市場等）

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

また、リスクの変化という観点から見ると、政府機関や企業においては、従来のホームページの改ざんやウェブサーバへのDoS攻撃[4]といったものに加え、マルウェア[5]を添付したメールを特定の組織、企業へ送付して重要情報を盗み出すものや、攻撃を予告して企業を恐喝するものなども発生している。そして、その目的は愉快犯的なものから経済的利得を狙うものへと変化してきている。個人においては、感染の検出が難しく被害が認識しづらい「ボット[6]」の感染が依然として継続し、被害が顕在化しにくいものになってきていると考えられる。

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

3. 総評

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

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

---

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

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

6 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

期間で一定の状況改善を実現できたと言えよう。

また、基本計画に掲げられ、SJ2007で目標が定められている「4つの基本方針」との関係では、

1）例えば政府機関や重要インフラ等の対策実施主体の意識の向上や、横断的情報セキュリティ基盤の人材育成に係る意識の向上など、情報セキュリティに係る官民各主体の共通認識が強化されてきている。

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

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

さらに、

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

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

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

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

さらに、依然として情報セキュリティ問題は発生し、新たなセキュリティ問題も発生

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

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

第2章　2008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　2008年度の課題

セキュア・ジャパン2008（以下「SJ2008」という。）は、2007年度の取組み及びその評価も踏まえつつ、基本計画の下での取組みの最終年度である2008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3年目である2008年度においては、第一に現行の対策推進体制や対策枠組み、技術水準で限界点に到達しているのではないかと考えられる諸点について、ブレークスルーをもたらす方法について検討を行うこと、第二に中長期で取り組むべき人材育成・確保の方策や、国際連携・協調のように加速化が必要な方策、電子政府の情報セキュリティ強化のように取組みを迅速かつ集中的に行うことが必要な方策に関して力強く対応を進めること、第三に情報セキュリティ政策の社会的効果（アウトカム）が現れるように取組みを進めること、が大きな課題である。

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

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

第三の課題については、そもそも政策の社会的効果（アウトカム）が現れるには、対策の実施からのタイムラグを考慮する必要がある。これまでに述べてきたように、情報セキュリティ政策のアウトプット（取組みの進展）は着実に出ていることから、政策の実現可能性や方向性に問題があるような場合は、これを修正しつつ、引き続き取組

みを積極的に継続することが必要である。この観点から、引き続きPDCAサイクルにのっとって、対策の底上げを行うべきである。

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

第2節　2008年度の情報セキュリティ政策の重点

そこで、2008年度の我が国情報セキュリティ政策の重点は、現行の対策推進体制や対策枠組み、技術水準の限界点への対処を長期的な視点に立って検討しつつ、それとともに**「情報セキュリティ基盤の強化に向けた集中的な取組み」**を図り、大きな社会的効果（アウトカム）が発現するよう努力を続けることとする。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維持・向上を引き続き図り、（2）先進的技術の追求を通じて現行技術水準の限界点を少しでも超えられるように努力し、（3）GSOCに関する取組みなど、公的部門の対応能力の強化を引き続き図り、（4）国内外の様々な主体の連携・協調の強化によるアウトプットの強化を図るという形で取り組むこととする。

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SJ2008においては、SJ2007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[7]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、2007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）

技術や環境の変化等を踏まえ、2008年度においても政府機関統一基準の見直しを行う。

---

7 「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。

また、これまでの政府機関対策を通じて得られた知見等に基づき、基本計画以降における政府機関統一基準のあり方について検討し、その結果を踏まえ、改訂を行う。

イ）PDCA サイクルの定着と浸透

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、PDCA サイクルの定着及び組織全体への浸透を徹底する。

特に、2008年度において、各府省庁はセキュリティ監査に関する実施体制の充実・向上を図り、全職員、全情報システムの対策実施状況の適切な把握を行うとともに、職員のセキュリティ対策の意識向上を図る。

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、政府全体としてのPDCAサイクルの定着を確実なものとする。

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、改善を促進するとともに、これまでの政府機関対策を通じて得られた知見等に基づき、基本計画以降における政府機関の評価のあり方について検討する。

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、各府省庁の作業負担を考慮して、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、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については、2007年度に試行的に実施した評価手法やその結果について検証し、情報セキュリティ対策の改善の促進に有効な評価手法の確立を図る。

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引き続き取り組む。

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、引き続き取りまとめて、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の効率化の方策について引き続き検討を行い、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。

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、2008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）

2008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）

2008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」について、2008年度中にIT ガバナンス、運用面等を強化した改訂版を策定し、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、2008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Webを通じて提供を開始するとともに、引き続き公開されている認証製品の内容を詳細に提供する機能を追加する。

また、当該ツールの政府機関等における活用を促進する。

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、

2008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）

2008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[8]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）電子政府の情報セキュリティを企画・設計段階から確保する（SBD）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について検討を進め、得られた成果を政府機関政策に反映する。

イ）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SBDの一環として進める。

ウ）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）

8 「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、原則公開する制度を指す。

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。2008年度はセキュアVMの性能向上及び利用環境の拡大を図るとともに、政府機関での利用を想定した実証実験を実施し、実運用に向けた課題の整理を実施する。

エ）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年度から行っており、その成果を踏まえ、2008年度も引き続き行っていく。

オ）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）

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）各府省庁は、「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」（2007年(平成19年)3月30日総務省）を参考として、2008年度も引き続き、情報システムにおけるIPv6対応化を「電子政府推進計画」（2007年(平成19年)8月24日一部改定各府省情報化統括責任者（CIO）連絡会議決定）に従って進める。

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、2008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。

カ）電子政府認証ガイドラインの策定及び利用の検討（内閣官房及び経済産業省）

政府機関における今後の電子認証システムの要件規定のあり方を示すため、

電子政府認証ガイドライン（仮称）の素案について引き続き検討し、策定する。また、その成果を踏まえ、利用のあり方についてSBDの一環として、検討する。

キ）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引続き検討を行う。

（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[9]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）

2007年度までに、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、原則として政府機関であることが保証されるドメイン名を利用するよう取り組んできたところ、2008年度中に、当該取組を国民に対して広く周知する。

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について、具体的な課題の抽出等を行う。

（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

[9] 「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。

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2008年度に行う。

イ）ハッシュ関数 SHA-1 及び公開鍵暗号方式 RSA1024 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）

1）内閣官房、総務省及び各府省庁は、「政府機関において使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」に従った取組みを推進する。

2）総務省及び経済産業省は、現在使用されている SHA-1 及び RSA1024 並びに新たに使用する SHA-256 及び RSA2048 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。

ウ）政府機関における安全な暗号利用のための取組み（内閣官房、総務省及び経済産業省）

内閣官房は、SHA-1 及び RSA1024 以外の電子政府推奨暗号について、安全性が著しく低下することによって近い将来に危殆化が発生すると予測される場合に必要な指針を取りまとめられるよう、SHA-1 及び RSA1024 と同様に安全な技術方式への移行のための指針を取りまとめることとする。また、総務省及び経済産業省は、電子政府推奨暗号の改訂に向けた取組みを進める。

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、2008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。

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) GSOC の本格運用と分析・解析能力の強化（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2007年度に整備を開始した GSOC について、本格運用を開始する。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。

b）情報保証に係る最新技術動向等の調査研究（防衛省）

2007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支援

a）各政府機関における緊急対応体制の強化支援（内閣官房）

2008年度に本格運用を開始する GSOC 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。

b）サイバーテロ対策に係る体制等の強化・整備（警察庁）

2008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、北海道洞爺湖サミット等の開催に伴う脅威の増大に対応するため、情報収集・分析体制の強化、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、ネットワークセキュリティ分析装置を研究試作するとともに、2007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。

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機会の拡大を図る。

イ）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、引き続き、一般職員向けに情報セキュリティに関する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、引き続き、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、引き続き、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・確保実行計画の実施（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）に基づき策定した「IT人材育成・確保実行計画」に基づく施策を推進する。

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）がさらに機能を発揮することを目指し、2007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）

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、ICT部門のBCP、外部委託に係る個人情報の管理等）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年度に見直しを行った地方公共団体情報セキュリティ監査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。具体的には、取組みの遅れている地方公共団体に対して内部監査アドバイザーを派遣する。

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）

2006年度に創設された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」が効果的に機能するよう、引き続き、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見直し（総務省）

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、組織体制ごとの権限・責任に応じたコース設定とするなどの研修の見直しを行い、引き続き、幅広い地方公共団体職員を対象に研修を実施する。

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。以下「行動計画」という。）を別途定めているところであるが、2008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』[10]策定にあたっての指針」[11]（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[12]）

2007年度の指針見直しを踏まえ、2008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・検証を実施する。また、必要に応じて安全基準等の改定等を進める。

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、2008年度中に安全基準等の確認・検証及び改定等の実施状況の把握及び検証を行う。

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）

---

10 「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。

11 「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）

12 「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。

内閣官房は、2007年度の調査の結果を踏まえ、重要インフラ所管省庁の協力を得つつ、各重要インフラ分野における安全基準等の浸透状況に関する調査を2009年度当初に実施するための企画・準備を実施する。

ウ）指針の見直し（内閣官房）

行動計画の見直し状況や、相互依存性解析の成果等を踏まえ、各重要インフラ所管省庁の協力を得て、情報セキュリティ対策に関する問題意識の抽出に向けた分析・検証を実施し、必要に応じて指針の改定等の対策の検討を進める。

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、2009年度までに、ネットワークの設備面や運用・管理面について、高度な事故分析手法の確立など、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

a）情報共有体制に対して追加すべき機能・要件等の検討（内閣官房）

行動計画の見直し状況、各分野における CEPTOAR の整備状況及び「「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）創設準備会」（後述）の検討状況を踏まえ、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。

b）関係機関等との連携の強化（内閣官房）

情報セキュリティ関係省庁、事案対処省庁、関係機関との連携を強化し、各重要インフラ事業者等の対策に資する情報を、重要インフラ事業者等に対し適宜・適切に提供する。

c）行動計画の情報連絡・情報提供に関する実施細目の見直しの検討（内閣官房）

行動計画の見直し状況、「「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）創設準備会」及び分野横断的な演習の検討状況を踏まえ、各重要インフラ所管省庁の協力を得て、行動計画の情報連絡・情報提供に関する実施細目の見直しについて検討する。

イ）CEPTOAR訓練の実施（内閣官房及び重要インフラ所管省庁）

各分野におけるCEPTOARの整備状況を踏まえ、CEPTOARの情報共有機能の維持及び改善に資する訓練の機会を提供する。

（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）「CEPTOAR 特性把握マップ」のフォローアップ（内閣官房）

2008年度の各CEPTOAR活動状況及び機能・要件の検討状況を踏まえ、2008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。

イ）重要インフラで利用される情報システムの信頼性向上のための支援体制の整備（経済産業省）

重要インフラ事業者による情報システムの信頼性向上のための自発的な取組みを支援するため、専門的・技術的な観点から、独立行政法人情報処理推進機構ソフトウェア・エンジニアリング・センターがデータベースの整備や、自発的に提供のあった情報のマクロ的な定量分析・解析、蓄積された情報のCEPTOAR等への提供を行う。また、重要インフラ事業者等の求めに応じ、情報システム開発・運用等に関する支援を行う。

（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）

「「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）創設に向けた検討の場」における協力のもと2007年度にとりまとめた「「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）の創設についての基本的な考え方」に基づき、各重要インフラ分野の CEPTOAR の協力を得て、 2008年6月を目処に「「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）創設準備会」を設置する。同準備会において2008年度中に「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）の創設を目指す。

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）

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

なお、その実施に当たっては、その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[13]の実施（内閣官房及び重要インフラ所管省庁）

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

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、2008年度も、2007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）重要インフラ事業者向けの啓発セミナー等の実施（経済産業省）

2008年度において、国内外の先進的なIT障害対応方策等に関する、重要インフラ事業者に対する情報提供を目的として、「重要インフラ情報セキュリティフォーラム」をIPAやJPCERT／CC等により開催する。

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）行動計画の見直し（内閣官房）

重要インフラ専門委員会における議論等を踏まえ、各重要インフラ所管省庁の協力を得つつ、2008年中に行動計画の見直し案（パブリックコメント案）を取りまとめる。そのため、2008年9月を目処に素案の取りまとめに向けた検討を進める。

13 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

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、2008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、企業における情報セキュリティ対策が効率よく進められるよう、2008年度に情報セキュリティに関係する既存の法制度に配慮した企業が行うべき情報の管理及び情報システムの管理に関するガイダンス等を作成する。

また、2006年度に策定した「情報システムの信頼性向上に関するガイドライン」について、企業の情報システム信頼性向上施策の現状についての調査を踏まえた上で、IT ガバナンスや運用面を中心とした当該ガイドライン及び「情報システムの信頼性向上に関する評価指標」の見直しを実施する。さらに、情報システムの構築や運用を各企業が行う際に、当該ガイドラインを参照することを推奨すべく、普及活動を継続的に実施する。

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、国際規格化の状況

を踏まえつつ、同協議会と連携し、国内標準化や認証などの普及促進に向けた取組を行う。
（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・落札に際して適切に考慮する方法について、検討を関係府省庁間で進める。

ウ）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）
　中小企業における情報セキュリティ対策コストの負担の適正化及び対策の推進を目的として、2008年度に対策実施状況を確認するための標準フォーマット等を策定するとともに、中小企業向け情報セキュリティ対策パッケージについて引き続き検討する。

エ）「情報システム・モデル取引・契約書（第一版）」及び「情報システム・モデル取引・契約書（追補版）」の活用・普及（経済産業省）
　情報システムの信頼性向上の観点から、ユーザ・ベンダ間の取引の可視化・役割分担の明確化を進めるため、2007年4月に「情報システム・モデル取引・契約書（第一版）」を公表したところ。本契約書で課題とされた事項を踏まえ、特に中小企業の取引の多数を占めるパッケージ・SaaS[14]・ASP[15]活用型の取引に関し、「重要事項説明書」を活用した簡易・透明な取引モデルである「情報システム・モデル取引・契約書（追補版）」を2008年度早々に策定、公表予定。当該追補版を活用し、資格制度の創設も含めたモデル取引・契約の普及について、関係業界団体と連携して取り組んでいく。

オ）「SaaS 向け SLA ガイドライン」の活用・普及（経済産業省）
　企業が SaaS を利用するに当たり適切な取引関係を確保し、より効果的に利用することを目的に、情報セキュリティ確保の観点に重点を置き、利用者とサービス提供者が合意すべきサービスレベルに関する指針を示した「SaaS 向け SLA ガイドライン」（2008年1月策定・公表）について、2008年度に、SaaS の利用者と提供者の双方に広く活用・普及を推進する。

14 Software as a Service
15 Application Service Provider

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）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）

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に作成した保証型監査利用ガイドラインの作成等につき、利用の促進及びその更なる活用方法の検討を行う。

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）

2008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利用を推進し、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。

イ）税制優遇措置

a)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）

2008年度に、産業競争力のための情報基盤強化税制を2年間延長・拡充するとともに、本税制の普及・啓発を図ることにより、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。

ウ）企業に係る指標の充実等(内閣官房及び経済産業省)

「情報処理実態調査」において、企業における情報セキュリティ監査制度の活用状況・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。

エ)企業における電子署名利活用の普及促進(総務省、法務省及び経済産業省)

2007年度に開催された「電子署名及び認証業務に関する法律の施行状況に係る検討会」における検討結果等を踏まえ、企業における電子署名の利活用の普及促進策について、取りまとめる。

オ)ASP・SaaS における情報セキュリティ対策の推進(総務省)

企業等における生産性向上の基盤となり得る ICT サービスとして普及が進むASP・SaaS の情報セキュリティ対策の推進に資するため、「ASP・SaaS の情報セキュリティ対策に関する研究会」において策定した「ASP・SaaS における情報セキュリティ対策ガイドライン」(2008年1月30日)について、業界における普及促進活動及び継続的な見直し・改善に向けた取組みを支援する。

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、2008年度においても助成を行う。

イ)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)

2008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」を全国各地で開催し、更なる展開を図るため地域主体の開催の試行を進めるとともに、IT経営応援隊と連携した普及広報活動を行う。

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）

産業構造審議会情報サービス・ソフトウェア小委員会人材育成 WG の報告書を踏まえ、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2008年度中に構築し、ITスキル標準、組込みスキル標準、情報システムユーザースキル標準及び情報処理技術者試験の整合化を図る。

エ）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。

オ）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たところ。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つつ、2009年度から新たな試験を実施する。

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）

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、インシデント対策・対応に資する攻撃情報や、所要の分析を加えた具体的な脅威・対策情報を必要とする者の間で共有するシステム（2007年度までに開発済み）の利用等により、2008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。）や国内の組織内 CSIRT との間における、緊急時及び平常時の連携の一層の効率化を図る。

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、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。

ウ）ソフトウェア等の脆弱性に係るマネジメントの支援等（経済産業省）

2008年度に、IPA 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の運用を開始するとともに、機能強化を検討する。

また、JPCERT/CC において、ユーザー組織における、ソフトウェア等の脆弱性マネジメントの重要性の啓発活動及び支援活動を強化する。具体的には、重要インフラを含む組織の脆弱性マネジメントに資する各種ツール（2007年度に一部開発済み）や手法の普及促進及び改善を進める。

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、2008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当たっては、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）

子どもたちに情報セキュリティを含む情報モラルの大切さを理解させるためのフォーラムを2008年度中に開催するなど、情報モラル教育を通じた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[16]育成プログラムの調査・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プログラムについての調査・開発を2006年度に行った。開発したプログラムは2007年7月に公開し、ICTメディアリテラシーの育成を行う団体等に普及を図っている。2008年度も引き続きプログラムの普及を図るとともに、必要な更新を行う。

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、2008年度に、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・ポスターの募集を行い、入選作品を公表する。

16 「ICTメディアリテラシー」とは、単なるICTの活用・操作能力のみならず、メディアの特性を理解する能力、メディアにおける送り手の意図を読み解く能力、メディアを通じたコミュニケーション能力まで含む概念。

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）

児童生徒が情報セキュリティの基本的な知識を身につけるよう指導する能力を含む「教員のICT活用指導力の基準（チェックリスト）」を活用し、2008年度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年度に引き続き、「インターネット安全教室」を全国各地で開催し、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とともに、当該安全教室を開催している民間団体等同士による情報の共有・連携を図るため、「インターネット安全教室全国連絡会議」を開催する。

b） e－ネットキャラバンの実施等（総務省及び文部科学省）

2007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。

c）サイバーセキュリティ・カレッジの実施（警察庁）

2007年度に引き続き、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。

ウ）若年層からの高度セキュリティ人材の育成（経済産業省）

2008年度に、若年層に対し、セキュリティ意識の向上と優れたセキュリティ人材の発掘と育成を図るため、産業界の第一線で活躍する技術者を講師とした実践的な講義等を合宿形式で実施する。また、講義の成果・内容を普及させるために全国各地で講習会を行う。

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、2008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）

2007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）

2008年度において、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・安心相談システムにより、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、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作成し、各都道府県警察において配布するとともに、警察庁ウェブサイトにも掲載するなど、広報啓発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）

2008年度から、各総合通信局所において、電波利用環境に関する国民相談窓口として電波利用環境相談巡回車の運行を予定している。

また、2008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、各種広報誌への掲載等）により周知啓発を実施予定。

さらに、2008年5月～7月及び9月～11月に、総合通信局所において、電波利用機器販売店への周知・啓発を実施するとともに、6月に「技術基準適合マー

ク」の確認についてニュースサイトにバナー広告を実施予定。

e)「情報通信の安心安全な利用のための標語」による啓発活動(総務省)

情報通信における安心安全推進協議会において、情報通信を安心・安全に利用するためのルールやマナー、情報セキュリティ等に関して、標語を募集し、受賞作のポスター掲示等による啓発活動を行うことにより、初心者を含む情報通信利用者の意識向上を図る。

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、これに合わせて、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)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、2008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)

2008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、2008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、SJ2008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[17]を2009年度までに構築することを目指して、2008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)

2008年度は、引き続き、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」を通じ、及び「インターネット安全教室」を通じ、無線LANのセキュリティ対策について、一般利用者に対する周知啓発を図る。

エ)プロアクティブな取組みによる悪意あるサイト等の情報収集・提供(経済産業省)

最近のコンピュータ・ウイルス等の不正プログラム(マルウェア)は、メールで大量にばら撒かれる従来のタイプから、ユーザ自らが Web サイトからダウンロードしてしまうものや、ブラウザ等の脆弱性を突いて気付かぬうちに侵入し、陰に潜むタイプのものへと推移しつつある。これらの不正プログラムの対応に当たっては、一般利用者と同様のアクセスを行うこと等による能動的な検体及び情報収集が必要となってきている。

17 「IPv6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。

このため、インターネット上の Web サイトへ自動的にアクセスし、マルウェア等の収集・解析及び解析結果の蓄積を行うシステムを運用し、それらの情報を即時に広く一般利用者へ提供する。

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、2007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年度に引き続き実施する。

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年度に引き続き実施し、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2008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年度に引き続き実施する。

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[19]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、2008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[21]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、2008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）

---

19 「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。

21 「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。

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。

e）新世代の情報セキュリティ技術の研究開発（経済産業省）

情報技術の社会基盤化に伴い、情報システムに起因する事故が、経済活動全体の停滞や国民全体の生命・財産そのものにかかわるリスクをもたらしかねない状況が生まれつつあるため、対症療法的ではなく根本的な問題解決を目指した新世代情報セキュリティ技術の研究開発を2008年度に実施する。

f）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を2007年度に引き続き実施する。

g）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年度に引き続き当該技術に関する研究開発に向けた検討を実施する。

h）新世代ネットワーク基盤技術に関する研究開発（総務省）

2020年頃の実現を視野に入れ、IPネットワークの限界を克服し、ユーザーからの多種多様な要求に応え、自由自在に最適な品質やセキュリティ等を確保することができる、新世代ネットワークの基盤技術の研究開発を推進する。2008年は、2007年に引き続き、ダイナミックネットワークの要素技術を開発するとともに、新世代ネットワークアーキテクチャの概念設計等を実施する。

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年度に引き続き実施する。

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】

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。2008年度はセキュアVMの性能向上及び利用環境の拡大を図るとともに、政府機関での利用を想定した実証実験を実施し、実運用に向けた課題の整理を実施する。

c）デジタルフォレンジック[22]に係る技術開発等の推進（警察庁）

2008年度において、デジタルフォレンジックに係る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。

d)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、2007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。2008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。

e)IP化されたネットワークにおける重要通信の高度化の推進（総務省）

IP化されたネットワーク等において、災害時等に重要な通信が確保されるように、2007年に引き続き、調査等を実施し、2008年までに、重要通信の高度化の在り方を検討し、とりまとめた上で、必要な施策・技術開発・支援等を実施する。

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

22 「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。

オに関する分析を2007年度に引き続き実施する。

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、2008年度では、プロジェクトの実施期間、実施規模、推進体制、予算及び関連法令等を考慮したより詳細なテーマについて、具体的な検討を実施する。

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、2008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)

2008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。

また、各拠点で多様な教育プログラムの開発・実施を通じて得られた成果について、より効果的・効率的な普及・展開及び教材等を更に洗練するための事業を支援する。

イ)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】

産業構造審議会情報サービス・ソフトウェア小委員会人材育成 WG の報告書を

踏まえ、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2008年度中に構築し、IT スキル標準、組込みスキル標準、情報システムユーザースキル標準及び情報処理技術者試験の整合化を図る。

ウ）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。

エ）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たところ。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つつ、2009年度から新たな試験を実施する。

オ）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、2008年度においても助成を行う。

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、2008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、2008年度においては、2007年度に策定した国際協調・貢献に取り組むための基本方針の具体化に着手する。

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、2008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）アジア地域における情報セキュリティ政策会合の創設（内閣官房、総務省及び経済産業省）

我が国との経済関係の深化が進むアジア地域におけるセキュアなビジネス環境の構築、安定したネットワーク環境確保に向けた地域的対応等に資するため、日 ASEAN 間で情報セキュリティに関する政策会合を新たに設置し、高級事務レベルでの政策対話、国際研究機関等を活用した政策研究・普及啓発の実施及びそれらの成果を活用した日 ASEAN の協力強化等について議論を深める。

エ）日中韓におけるネットワーク情報セキュリティに関する情報共有体制等の強化（総務省）

2004年に設置された日中韓ネットワーク情報セキュリティワーキンググループを通じて、各国の基本政策、インシデントレポート及びセキュリティトレンド等に関する情報共有を強化するとともに、ネットワークオペレータ組織を含む関係機関の協力を推進する。

オ）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、NISCが我が国としてのPOC機能を有することを明確化し、2008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。

カ）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NISCの位置づけと機能などについて、国際的な広報活動を2008年度に実施する。

キ）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、2008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。

ク）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)

2008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。

ケ）APT 研修・セミナー等の開催(総務省)

アジア・太平洋電気通信共同体（APT=Asia-Pacific Telecommunity）への我が国からの特別拠出金により、2008年度に「ブロードバンド通信のための情報セキュリティ構築」研修を実施予定。

コ）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の構築支援を行う。2008年度においては、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の共有などの支援を行う。

また、アジア地域においてオリンピックやサミット等の世界の注目を集めるイベントが開催されることから、アジア太平洋地域におけるインシデント対応演習等の活動を通じ、各国 CSIRT との連携を一層強化することにより、迅速かつ効果的なインシデント対応を行うことができるよう各国内における調整能力の向上に協力する。

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、2008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）アジア太平洋地域等での早期警戒情報の共有促進（経済産業省）

2008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、2007年度に開発したシステムを各国に設置し、試験的な運用を開始する。

また、2007年度から日次ベースでアジア太平洋地域の各 CSIRT 向けに配信している、情報セキュリティに関する脅威情報やソフトウェア等の脆弱性に関する分析情報について、配信対象地域の拡大および双方向化を進める。

ウ）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）

サイバー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、国内外のセキュリティ関連組織の間で分析結果の共有方法について、検討を行う。

具体的には、2008年度に、IPA及びJPCERT／CCにおいて、分析にかかわる情報をグローバルに共有し、分析対象の脅威度判断に役立てる手法の検討等を行う。

エ）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年度から2007年度にかけて、国際電気通信連合（ITU：International Telecommunications Union）に対して、第3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ガイドライン（ISM-TG）について提案を行い、国際規格化した。2008年度には、国際標準化機構（ISO）における同案の国際規格化の採択に努め、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。

オ)アジア域内のセキュアなビジネス環境の構築推進(経済産業省)

アジア域内におけるセキュアなビジネス環境の構築を推進するための手法等について、我が国の知見を活用しつつ、アジア諸国の研究者との共同研究等を実施する。

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、2008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、2008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)

サイバーパトロール業務を民間に委託するなど、多様化・複雑化するサイバー犯罪に適切に対処するための体制を2008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、2008年度において、不正プログラムやファイル共有ソフトによる犯罪や不正行為等に係る情報の収集・分析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)

2008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とともに、重要インフラ事業者等の意向を尊重しつつ、共同訓練の実施、各種演習等への参画を通じ、サイバーテロ発生時の緊急対処活動に資する取組みを行う。

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)

2008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、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[24]を活用した国際捜査共助の迅速化(法務省)

捜査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おり、日中間においても、平成19年12月1日，刑事共助条約の署名が行われたところ、2008年度においては、日中間の刑事共助条約につき国会の早期承認を得るなどの所要の手続を進めるとともに、香港及びロシア連邦との間でも交渉中の刑事共助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)

・北海道洞爺湖サミットに向けて訓練実施を含む電波監視強化体制を確保し、期間中は、総務省に重要無線通信妨害対策本部を設置し、重要無線通信妨害事案の発生時の対応に万全を期す。
・電波利用秩序維持のため、遠隔操作による電波監視施設等の更新及び性能向上並びに混信が恒常的に発生している地域へ、平成20年度DEURASセンサ27式等の整備を実施予定。

---

24 「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。

・アップリンク干渉源位置特定システムの試行運用における機能・性能向上及び電波発射源可視化装置（短バースト波対応機）の配備を検討。併せて、広帯域監視技術の調査研究を実施予定。

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）

2008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に係る取組みを推進する。

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)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）

これまでと同様、総務省として、業界団体によるWebサイト等を通じた同法及び関係ガイドラインの周知を支援していく。

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）

2008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、2008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）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、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、GSOCの本格運用に向けた体制整備をはじめ、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、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、引き続き、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。

（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）

2008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）情報セキュリティの分析・提言（経済産業省）

2008年度に、IPAの情報セキュリティ分析部門として情報セキュリティ分析ラボラトリーを設置する。同ラボラトリーにおいては、情報セキュリティ分野における脅威、攻撃、リスク、対策等を社会経済的・技術的観点から分析し、提言をするための検討を行う。

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）

2008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、2008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[26]の実施及び公表（内閣官房）

SJ2008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）

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）行動計画の見直し（内閣官房）【再掲】

重要インフラ専門委員会における議論等を踏まえ、各重要インフラ所管省庁の協力を得つつ、2008年中に行動計画の見直し案（パブリックコメント案）を取りまとめる。そのため、2008年9月を目処に素案の取りまとめに向けた検討を進める。

（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。

【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SJ2008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。

[26]本章においては、「「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。

（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[1]に当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。

また、2006年度から2007年度にかけて、SJ2006第2章第2節④及びSJ2007第3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において検討した、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手法について、2008年度も引き続き、同演習において当該評価指標の活用を促進し、改善等を検討する。

第６章　２００９年度に喫緊に取り組むべき課題

～２００９年度の重点「持続的な情報セキュリティ対策の推進体制の構築に向けた基盤整備」～

第3章から第5章までは、3か年計画である基本計画の3年目（最終年度）として、2008年度に実施すべき具体的施策を挙げてきた。これらは、2006年度、2007年度にわたる2年間の取組みを受け継ぎ、**「情報セキュリティ基盤の強化に向けた集中的な取組み」**を重点とするものである。

この3年間の取組み、すなわち、2006年度の「官民における情報セキュリティ対策の体制の構築」、2007年度の「官民における情報セキュリティ対策の底上げ」、そして最終年度である2008年度の「情報セキュリティ基盤の強化に向けた集中的な取組み」を重点とした各種施策の展開により、基本計画が目標とした「新しい官民連携モデルの構築」については相当の成果が上がりつつある。具体的に、対策実施主体（政府機関・地方公共団体、重要インフラ、企業、個人）ごとに情報セキュリティ対策の必要性が認識され、そのための体制の整備が図られたほか、問題の理解・解決を促進する主体としての政府・地方公共団体、教育機関・研究機関、情報関連事業者・情報関連非営利組織、メディアなどにおいても、対策実施主体による対策を促進するための各種取組みが進められ、対策の向上に貢献したものと考えられる。

こうした3年間の取組みの結果を踏まえ、現在、情報セキュリティ政策会議においては「基本計画検討委員会」を設置し、次期（第二次）情報セキュリティ基本計画の検討に着手している。これにより、2009年度以降の中期的な計画がまとめられることになるが、これまで3年間の取組みの結果・評価を踏まえて、喫緊に取り組むべき課題も明らかになってきている。

具体的には、これまでの3年間は「現在の状況・体制の中で、（取りあえず）対策を実施するための体制・基盤」が整ったに過ぎないという点である。言い換えれば、5年間やそれ以上の期間を見据えた中で、的確な情報セキュリティ対策を継続的に実施しつつ、IT を巡る技術革新や社会制度の変化等を踏まえ柔軟に対策の修正・向上を図っていくための持続的な枠組みまでが十分に整ったとは言い難い。

例えば、政府機関においては、PDCA サイクルに基づく対策実施について、政府機関統一基準をツールとして3年という短期間で一定の成果を出しているが、多くの各府省庁においては、数名の担当者が組織全体に対策の徹底を図ろうと努力している状況であり、組織全体への定着や職員への浸透、対策の効率化、負担軽減の面で改善の余地があるほか、組織全体としてのマネジメントシステムが整えられていない府省庁も見受けられる。また、その担当者も2～3年ごとの人事異動によって入

れ替わるため、対策実施のためのノウハウや技術に関する知識の継承が十分になされず、効果的・効率的な対策が持続しにくいという問題がある。

重要インフラ分野において、各事業者が、これまで情報セキュリティ対策に取り組んできたところである。今後、更に取組みを進めるために、こうした努力に対して社会全体の認知を高めていくことが重要である。

このような状況を踏まえ、2009年度においては、次期基本計画の方向性を念頭に置きつつ喫緊に取り組むべき課題として、**「持続的な情報セキュリティ対策の推進体制の構築に向けた基盤整備」**を重点として施策の推進を図ることとする。

第１節　政府機関における持続的な情報セキュリティ対策の推進体制の構築に向けた基盤整備

【具体的施策】

ア)組織横断的な情報セキュリティ対策のためのマネジメントシステムの導入に向けた検討（内閣官房）

情報セキュリティ対策が組織全体で継続して取り組まれるためには情報セキュリティ担当部局が中心となって組織全体の理解と対策実施が徹底されることが必要であり、この実現に必要な枠組みや効果的なマネジメントシステムの導入に関する検討を行う。

イ)客観性を確保したチェック機能の在り方についての検討（内閣官房）

政府機関のPDCAサイクルを主体的かつ持続的なものとするためには、客観性が確保されたチェック機能（特に監査的な機能と指導的な機能）が求められる。このため、客観性の確保や実施能力の確保などチェック機能のあり方に関する検討を行う。

ウ)電子政府の情報セキュリティを企画・設計段階から組み込むための方策（SBD）の推進（内閣官房及び各府省庁）

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ることから、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（SBD）について、電子政府構築における最適化計画の次期サイクルの機会も捉え、その推進を図る。

エ)中小規模府省庁の情報セキュリティ対策の底上げ支援（内閣官房及び関係府省庁）

情報セキュリティ対策の推進に当たって人材面、資金面といったリソースが必ずしも十分ではない中小規模府省庁の対策を底上げするべく、効率的な形で専門知識やノウハウを提供する取組みを推進する。

オ)電子政府認証ガイドライン利用の推進(内閣官房)

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、2008年度における検討の結果を踏まえ、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。

カ)「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」に基づく取組み(内閣官房、総務省及び各府省庁)

政府機関の情報システムの安全性及び信頼性を確保するため、安全性低下が指摘されている暗号アルゴリズムSHA-1及びRSA1024について、情報システムのライフサイクル等を踏まえつつ、適時に、より安全なものに移行するための取組みを進める。

キ)情報セキュリティ人材の重点確保(内閣官房及び各府省庁)

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、最高情報セキュリティアドバイザー(CISO補佐官)の配置など各府省庁における情報セキュリティ対策の要となる専門家及び情報セキュリティ対策部門の実務担当者の確保を図る。

ク)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)

2008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。

ケ)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(内閣官房)

2008年度に本格運用を開始するGSOCの運用状況や各政府機関における緊急対応体制の整備状況等を踏まえつつ、政府機関や官民関係機関との連携を深め、緊急時における連絡体制や攻撃等の分析・解析及び対策立案機能を強化し、政府全体としてのサイバー攻撃等に対する緊急対応能力の向上を図る。

第２節　各対策実施領域における持続的な情報セキュリティ対策の推進体制の構築に向けた基盤整備

ア)重要インフラ全体としての取組みに関する広報公聴活動(内閣官房)

重要インフラ事業者の情報セキュリティ対策への取組みの広報を強化することで、事業者の情報セキュリティ対策に対する国民の理解を促進し、事業者における情報セキュリティ活動を側面から支援する。

イ)電気通信事業者等による情報セキュリティ対策の実施に係る検討の促進(総務省)

インターネットを利用する個人等が、ボット等に感染することにより、自らが被害者となるだけでなく、本人が気付かないうちに他人に被害を及ぼす加害者となる場合があることにかんがみ、電気通信事業者等が予防的措置等として実施する情報セキュリティ対策について検討する。

ウ)地方公共団体における情報セキュリティ対策の水準向上に向けた取組みの促進(総務省)

2008年度に検討する情報資産のリスク分析や情報システムの外部委託等に伴う個人情報の漏えい防止の具体的方策等について、小規模な地方公共団体を含め着実な浸透を図るとともに、PDCAサイクルを実効性あるものとするために情報セキュリティ監査を促進し、さらに災害の発生等による業務の中断の未然防止、業務の早期復旧等を目的とするICT部門の業務継続計画(BCP)の策定に向けた地方公共団体の取組みを支援する。

エ)ICTサービス利用者に対する情報セキュリティ対策の重要性に関する普及啓発活動の継続的実施の推進(総務省)

インターネット等を通じたマルウェアの感染手法が常に高度化・巧妙化している状況に対して、利用者として実施することが望ましい情報セキュリティ対策について、その普及啓発活動の継続的実施を推進する。

オ)産学官連携によるマルウェア感染手法等の高度化・巧妙化に対応した先進的な研究開発の推進(総務省)

インターネット等を通じたマルウェアの感染手法の悪質化、被害の局所化等に対し、迅速に状況を把握し、障害に対する適切な対策手法を確立するための先進的な研究開発の強化を図る。

カ)スパムメール対策の強化(総務省及び経済産業省)

巧妙化・悪質化が進展し全体として増加が続くスパムメールに対して対策の実効性を高めるため、必要な体制の整備や、スパムメール対策業務の高度化等所要の措置を講じる。

また、国内の主要インターネット接続サービス事業者や携帯電話事業者が中心となり設立された民間団体である「JEAG」等の業界団体と連携して、スパムメール送信の防止に効果のある技術である 25 番ポートブロックや送信ドメイン認証技術等の導入を促進する。

さらに、急増する海外のコンピューターから送信されるスパムメールに対応するため、スパムメール対策を行う外国執行当局との連携を強化するとともに、民間における国際的なスパムメール対策の連携を推進する。

その他、違法なスパムメールに関する情報を当該スパムメールの送信等に利用されたインターネット接続サービス事業者に通知し利用停止等の措置を促進する「迷惑メール追放支援プロジェクト」(2005 年 2 月～)を引き続き実施する。

キ)情報セキュリティガバナンス確立の促進(経済産業省)

企業における情報セキュリティガバナンスの確立に向けた取組みを推進するため、2008年度に策定するガイドライン等の普及を図る。特に、中小企業については、IPA等の関係機関とも協力し、情報セキュリティ対策推進のためのサポート体制の整備を図る。

ク)組込みシステム等のディペンダビリティ確保のための体制整備等(経済産業省)

組込みシステム等のディペンダビリティを確保するため、開発者等が留意すべき事項等について検討する。また、組込みシステムの核となるLSIチップやICカード等の安全性について、関係機関において耐タンパー技術等の解析及び安全性評価を行うための能力向上・体制整備を図る。

ケ)アジア域内のセキュアなビジネス環境の構築推進(経済産業省)

2008年度に実施した研究等の成果を踏まえ、アジア域内におけるセキュアなビジネス環境を構築するための更なる推進策について検討する。

コ)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に対応するため、情報収集・分析体制の強化、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・整備を推進する。また、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とともに、重要インフラ事業者等の意向を尊重しつつ、共同訓練の実施、各種演習等への参画を通じ、サイバーテロ発生時の緊急対処活動に資する取組みを行う。

サ)サイバー犯罪対策に係る体制等の強化(警察庁)

サイバー犯罪の複雑・巧妙化に対し適切に対処するため、体制の強化・整備やデジタルフォレンジックに係る取組みの強化に努めるほか、サイバー犯罪の取締り、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、被害防止のための広報啓発活動、官民連携のあり方の検討等を推進する。また、アジア大洋州地域サイバー犯罪捜査技術会議の主催等により、国際連携・協力の強化を図る。

シ)各専門分野情報共有スキームの連携性及び情報交換モデルに関する検討(内閣官房、総務省及び経済産業省)

昨今の高度化されたサイバー攻撃及びIT障害対処等に関する適切な対処立案には、多様な専門性を有する情報収集・相関分析と各々の情報共有スキームの目的・機能に応じた連携対策が必要である。

このため、「システム設計分野・ウイルス解析分野・CSIRT 分野・ISP 分野」等の各専門分野の情報共有スキームの役割と連携性を整理し、それぞれの目的・機能に応じた情報連携と情報交換モデル(連携構図設計)の検討を行う。

ス)情報処理基盤の安全性等の確保(経済産業省)

サイバー攻撃の局所化、攻撃手法の洗練化・隠蔽化、攻撃の対象となるシステム(制御システム等)の拡大に対応するため、攻撃に利用される技術、手法等に関する分析能力の強化を推進するとともに、国内外の産官学の関係組織間におけるマルウェア検体、検知情報、脆弱性関連情報、分析技術・ツール等の共有体制の整備を図る。

また、インシデント対応支援や IT 製品・システムの開発者に対するセキュアな製品開発手法や検証手法に関する情報提供、イントラ管理者、IT利用者等に対する普及啓発活動や時代に即応した技術的対応策の開発等を通じて、適切な情報処理環境の整備を図る。