セキュア・ジャパン2009（案）

～すべての主体に事故前提の自覚を～

2009年　月　日

情報セキュリティ政策会議

目次

第1章　第１次情報セキュリティ基本計画（2006～2008 年度）に基づく取組みと評価について　- 1 -
第１節　基本計画、過去の年度計画及び評価の経緯と本計画との関係　- 1 -
第2節　第1次基本計画の3年間（2006～2008年度）を通じた施策の取組みと評価　- 3 -
第2章　2009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的方針　- 12 -
第1節 2009年度から2011年度までの3箇年を通じた方向性　- 12 -
第2節 3箇年の取組みの流れ　～　成長の各段階のイメージ　～　- 13 -
第3節 2009年度の課題と情報セキュリティ政策の重点　- 14 -
第3章 2009年度に取り組む重点政策　- 16 -
第1節 対策実施4領域における取組みの推進と政策目的の着実な実現　- 16 -
（1）対策実施4領域　- 16 -
①政府機関・地方公共団体　- 16 -
②重要インフラ　- 32 -
③企業　- 38 -
④個人　- 51 -
（2）横断的な情報セキュリティ基盤の強化と発展　- 56 -
①情報セキュリティ技術戦略の推進　- 56 -
②情報セキュリティ人材の育成・確保　- 62 -
③国際連携・協調の推進　- 67 -
④犯罪の取締り及び権利利益の保護・救済　- 74 -
第4章　政策の推進体制と持続的改善の構造について　- 78 -
第1節 政策の推進体制　－ 78 －
（1）内閣官房情報セキュリティセンター（NISC）の強化と役割　- 78 -
（2）各府省庁の強化と役割　- 79 -
（3）状況の変化の適時適切な把握と新しい課題への対応　- 80 -
第2節 他の関係機関等との関係　- 80 -
第3節 持続的改善構造の構築　- 81 -
（1）「年度計画」の策定とその評価等　- 81 -
（2）年度途中での緊急事態対応に向けた取組みの実施　- 82 -
（3）評価指標の改善　- 82 -
（4）第2次情報セキュリティ基本計画の見直し　- 83 -
第5章　2010年度に喫緊に取り組むべき課題　- 84 -

第1章　第１次情報セキュリティ基本計画（2006～2008 年度）に基づく取組みと評価について

第１節　基本計画、過去の年度計画及び評価の経緯と本計画との関係

「セキュア・ジャパン」の実現（真に「情報セキュリティ先進国」）となることを目指した「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「第 1 次基本計画」という。）は、2008年度末でその計画期間を終え、2009年度から同計画を「継続」・「発展」させることとした「第2次情報セキュリティ基本計画」（2009年2月３日情報セキュリティ政策会議決定。以下「第2次基本計画」という。）に基づく取組みが開始された。

第 1 次基本計画における取組みの概要については第2次基本計画第1章において触れているが、同計画は、おおまかにいえば、我が国における情報セキュリティ政策の立上げとすべての主体にとっての「気付きを与える」ための戦略であった。同計画の目指した「セキュア・ジャパン」の実現に向けて、2006年度から年度計画「セキュア・ジャパン200X」が策定され、「体制構築」→「底上げ」→「集中的取組み」の各段階を経て、情報セキュリティ基盤の整備に向けた具体的な取組みが進められた。

・ 2006年度は、「「セキュア・ジャパン」への第1歩」として、「官民における情報セキュリティ対策の体制の構築」が開始された。133の具体的施策が掲げられ、約87％の施策が予定どおり推進、残りの施策も中長期的にはおおむね推進できるとの評価であった。その結果、
　1)各主体における情報セキュリティ意識の萌芽
　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 1 段階」が進んだ。

・ 2007年度は、「官民における情報セキュリティ対策の底上げ」として、構築が進んだ官民の情報セキュリティ対策推進体制の維持と、対策が不十分な部分の底上げを含めた対策推進の安定化を目指した取組みが進められた。159の具体的施策（及び2008年度の重点施策の方向性として24施策）が掲げられ、約91％の施策が予定どおり推進、残りの施策も中長期的にはおおむね推進できるとの評価であった。その結果、
　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)対策実施領域毎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

という取組みの成果が見られた。

・ 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」に向け、「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」及び「電子政府の情報セキュリティ強化」を中心とした取組みが進められた。157の具体的施策（及び2009年度の重点施策の方向性として21施策）が掲げられ、約89%の施策が予定どおり推進、残りの施策も中長期的にはおおむね推進できるとの評価であった。その結果、第 1 次基本計画に掲げていた4つの基本方針「官民各主体の共通認識の形成」、「先端的技術の追求」、「公的対応能力の強化」及び「連携・協調の推進」において、一定の改善やこれからの継続的な取組み、「場」の形成などの一定の成果が見られた。

第1次基本計画に引き続き、第2次基本計画においても、毎年度、具体的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、その実施状況を社会情勢の変化とともに評価し、結果を公表することとしている。評価の結果は、1年周期の PDCA サイクルの一環として翌年度の年次計画に反映することとなるが、2008年度は第1次基本計画の最終年度でもあり、同計画の計画期間（2006～2008年度）を通じた評価も行うこととしている（「2008年度の情報セキュリティ政策の評価等」（2009年　月　日内閣官房情報セキュリティセンター公表。））。

セキュア・ジャパン2009（以下「SJ2009」という。）においては、同評価等（主として第 1 次基本計画の3年間を通じた評価）も踏まえ施策の方向性を定めることとしている。

第2節　第1次基本計画の3年間（2006～2008 年度）を通じた施策の取組みと評価

第 1 次基本計画の評価は、「情報セキュリティの観点から見た我が国社会のあるべき姿及び政策の評価のあり方について」（2007年2月2日第10回情報セキュリティ政策会議決定）を踏まえ、同文書に描かれている「2009年時の我が国社会の姿」（以下「2009年の姿」という。）の達成度を測ることなどにより実施された。

（1）施策の取組みによる社会的変化に関する評価・分析・課題

① 政府機関・地方公共団体

「2009年の姿」の例とそれらの達成度は、次のとおりである。

- 「政府機関統一基準とそれに基づく評価・勧告によるPDCAサイクルが構築されていること」については、政府機関統一基準の適時見直しにより、政府機関の対策は常に最新かつ適切なものとなっており、また、統一基準に基づく評価・勧告等による政府機関の基本的なPDCAサイクルの構築が進展した結果、端末、サーバ等の基本的項目に係る対策実施状況については大幅に改善された。

- 「中長期的なセキュリティ対策の強化に向けた政府機関共通の取組みが開始されていること」については、次世代の電子政府構築に向けた検討を開始し、政府機関における安全な暗号利用の推進などの取組みが推進されている。

- 「計画的な専門人材の活用・育成が進んでいること」については、各府省庁において、「行政機関におけるIT人材の育成・確保指針」[1]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しているところであり、また、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が図られた。

- 「独立行政法人等において政府機関に概ね準ずる程度まで情報セキュリティ対策が進んでいること」については、政府機関統一基準を参考に、情

1　２００７年４月１３日　各府省情報化統括責任者（ＣＩＯ）連絡会議決定。

報セキュリティポリシーの策定・見直しが進んでいる。

- 政府機関に対するサイバー攻撃等への対応については、GSOC[2]を整備、運用を開始したことにより、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等が図られた。

以上のような状況を総括し、「2009年の姿」として示した当初の目標は、完全とはいえないものの、概ね達成できたものといえる。

② 重要インフラ

「2009年の姿」として次の目標が掲げられている。

- 各分野における情報セキュリティ対策の水準を明示した「安全基準等」が定められており、各重要インフラ事業者等は、自らの情報セキュリティ対策が十分であるか自己検証を行っていること

- 官民の情報連絡・提供体制の整備、セプター、セプターカウンシルなど、重要インフラの情報セキュリティ対策に資する情報を共有する枠組みが官民の各主体間で構築され、IT障害に関しての情報共有、連絡・連携がなされていること

- それぞれの重要インフラ分野に起こりうる脅威が何であるかを把握するとともに、ある重要インフラ分野にIT障害が生じた場合に、他のどの重要インフラ分野に影響が波及するかという相互依存性の解析がなされ、その相互依存関係を踏まえ、重要インフラ分野での対応が適切になされていること

- 想定される具体的な脅威シナリオから毎年度テーマを設定し、各主体の協力を得て行う「重要インフラ分野横断的な演習」等を通じ、情報セキュリティ対策の向上に向けた取組みが継続的に行われていること

この「2009 年の姿」の達成に向けて、官民の緊密な連携の下、重要インフラの情報セキュリティ対策を強化するために取り組むとされた「重要インフラの情報セキュリティ対策に係る行動計画」（2005年12月13日情報セキュリティ政策会議決定）において4本の施策の「柱」が立てられており、第 1 次基本計画下の3年間において38の具体的な施策として取組みが行われてきた

[2] Government Security Operation Coordination teamの略。政府機関情報セキュリティ横断監視・即応調整チーム。

この38の具体的な施策は、2008年度末までにすべて実施済みであり、関係主体間の連携の基礎が整うとともに、各関係主体において情報セキュリティ対策の充実に資する気付きや共通認識の醸成を進める土壌が育ちつつある状況にあるといえる。

一方、これらの取組みを進める間にも、ITの利用の拡大、ITへの依存は益々進む傾向にある。IT障害が国民生活や社会経済活動に重大な影響を及ぼさないようにする観点からは、未然防止だけでなく、IT障害発生時の機能回復に向けた取組みも重要であり、事前及び事後の対策をバランス良く行う必要がある。対策の着実な向上に資するため、今後も、指針及び安全基準等の適切な見直し及び浸透を図ることが引き続き課題になると考えられる。

また、障害発生時の情報や他分野、他事業者の経験から得られた知見の共有の重要性が認識されており、政府内の連絡体制、セプターやセプターカウンシルなどの情報共有の枠組みの有効な活用を含め、それぞれの関係主体に期待される役割をいかに発揮していくかも今後の課題である。

これらの課題への対応に当たっては、関係主体間の円滑な協力が可能となるよう、重要インフラ事業者等の取組みにおける多様性を十分に踏まえ、重要インフラ事業者等間、分野間等の相互理解を深め、共通認識の醸成に努めることが重要である。

③ 企業

「2009年の姿」として**「対策の実施状況が世界トップクラスの水準」**になることを目指して様々な対策が実施された。

企業においては、「重要情報の漏えい」が減少傾向を見せないことから、情報セキュリティ事故による信用失墜の回避や、競争力にかかわる機密情報の保護を目的として自主的に様々な取組みが実施されてきた。さらに、事業継続性についても強く意識されるようになり、企業におけるBCP（事業継続計画）策定の進展が見られる。

このような企業の動きについて、政府は各種認証制度・ガイドライン等の開発・普及を図るといった政策面での支援を行ってきた。

こうした情報セキュリティ面での取組みが進められた結果、ISMS適合性評価制度の認証取得数、情報セキュリティポリシーを策定している企業の割合、技術的対策の導入度合い等の数値は増加傾向にあり、PDCAサイクルの確立に向けた取組みが進んでいるといえる。

他方、情報セキュリティ対策の実施について情報セキュリティ向上以外の効果がないとする企業は依然として4割を超えており、今後、情報セキュリティの底上げを実施するに当たっては、情報セキュリティ対策への取組みが市場で評価され、企業価値や競争力の向上につながる環境を整備することが重要となる。

以上から、第 1 次情報セキュリティ基本計画下においては、PDCAサイクルの構築を中心に、企業における情報セキュリティ対策は進展を見せたが、すべての対策において「対策の状況が世界トップクラスの水準」に到達しているとは言い難い。今後は、引き続き情報セキュリティの底上げを図るとともに、事業規模により情報セキュリティ対策に対する取組み状況に差が見られることから、中小企業等のリソース不足から対策が困難な主体における対策を促進するための方策を実施することを検討する必要もある。

④ 個人

「IT利用に不安を感じる個人が限りなくゼロ」に近づく事を目指して、個人に対して政府・非営利組織等が積極的な広報啓発・普及促進に関する様々な施策を実施した。

そうした取組みに加えて、個人情報の流出を含む様々な情報漏えい事件が報道されたこと等を通じて、個人分野においては、情報セキュリティに対する重要性の認識が高まり、情報セキュリティ対策の実施状況に進展が見られた。

他方、情報漏えいが減少傾向を見せないことや、新たな脅威に対する個人の認識が追いついていないことなどを背景に、依然として4割以上の個人がIT利用について不安を感じており、「ITに不安を感ずるとする個人を限りなくゼロに」するという目標を達成するには、更なる情報セキュリティの底上げが必要である。

個人分野については、新たな脅威を認識させることが難しい、従来から指摘され続けている基本的な対策についても、実施していないとする個人が2割強存在するなど、目標達成に向けては難しい問題も存在する。

また、インターネットの利用が多様化することが見込まれる中で、セキュリティを確保するために、個人の意識についての底上げを図る以外に効果的な取組みが存在するかについても検討の余地が存在する。

今後は、より効果的な広報啓発・普及促進を実施していく必要があるとともに、個人の意識によらずに情報セキュリティ被害を防ぐことができるようなサービス技術開発、多様化するインターネット利用に対応したセキュリティ確保といった取組みについても検討を実施する必要がある。

⑤ 情報セキュリティ技術戦略の推進

第 1 次基本計画期間の3年間を経て、情報セキュリティ技術開発の重点化と環境整備に向けた事例も見られるようになった。具体的には、ボットを使ったサイバー攻撃等の課題を解決するための技術開発などの課題解決型の技術開発が数多く実施され、経路ハイジャックの検知・回復・予防に関する研究開発や仮想機械（バーチャルマシン）技術を用いた安全な環境の開発など、情報セキュリティ技術の高度化に向けた取組みの進展が見られた。

一方、組織・人間系の管理手法の高度化については、取組みが十分でなく、今後の実施が課題となる施策が存在する。また、2007年度に構築した「研究開発・技術開発の効率的な実施体制」、「グランドチャレンジ型」研究開発・技術開発は一層の推進が必要である。

また、3年間のITの利用・活用の拡大などによる情報セキュリティを取り巻く社会情勢の変化に伴い、研究開発・技術開発の面で、新たに取り組むべき次のような課題も浮かび上がってきた。

- 情報機器やデバイスの急速な普及と高機能化、及びネットワーク上のサービス の多様化などに伴って、国民のITへの依存度が高まり、情報セキュリティに係る課題として扱うべき範囲が大幅に拡大する可能性が高いこと

- 高齢化など社会の世代構成の変化に対応して、使い方が簡単で、利用者のミスや誤認が情報セキュリティ上のリスクにつながらないようにするという発想が、サービスや製品の設計・開発に際して、より重要となること

- 新たな脆弱性の発見や攻撃手法の開発のスピードも加速していることから、従来のセキュリティ対策では対応し切れなくなってきたこと

今後は、これらの新たな課題への対応も配慮しつつ、「情報セキュリティ技術開発の重点化と多様性の維持」、「「グランドチャレンジ型」研究開発・技術開発の推進」、「研究開発・技術開発の効率的な実施体制の構築と基盤の整備」の3つの重点施策に取り組んでいく必要がある。

⑥ 情報セキュリティ人材の育成・確保

第1次基本計画下での3年間においては、情報セキュリティ資格・教育の体系化について「人材育成・資格制度体系化専門委員会」報告書によって一定の成果を上げることができ、情報セキュリティにかかわる多種の人材に対する指針を示すことができた。

他方、経営幹部や情報システム部門以外の人材を含む、情報セキュリティを必要とするすべての人材に対して情報セキュリティ知識・スキルが十分に行き渡っている状況まで人材育成・確保を推進することはできていない。加えて、情報セキュリティ人材育成の効果が現れ、社会における情報セキュリティ人材のニーズが満たされるまで、更なる取組みが必要であることが明らかになった。

また、現在情報セキュリティに携わる人材の一部からは、自らのキャリアパスを明確に描くことができないといった不安の声も上がっている。今後は情報セキュリティ人材を必要とする所謂需要側と情報セキュリティ人材を供給する側だけでなく、情報セキュリティ人材そのものからのニーズに着目した施策検討も必要になるものと考えられる。

⑦ 国際連携・協調の推進

第1次基本計画の3年間においては、

- 諸外国との関係において、情報セキュリティ案件等に関するPOC間の情報共有・交換は日常的に行われていること
- 積極的な情報発信を行う結果、我が国の情報セキュリティ関する状況や取組みが諸外国にも十分知られるようになっていること
- 情報セキュリティ問題に対する我が国の様々な取組みがベストプラクティスとして他国の模範となっていること

等を目標として対策を実施してきた。

諸外国との間におけるPOCの明確化については、内閣官房情報セキュリティセンター設置当初は、組織の世界的な知名度も低く、広報活動に困難

を伴う状況であったが、継続的な国際会合への積極的な参加、広報活動を通じて、組織としての知名度及び日常的な情報交換については、大幅に改善されている。

具体的には、情報セキュリティ政策に関する国際会合への参加数は年度を追う毎に大幅に増加し、欧州、アジア太平洋地域を中心に幅広い範囲での活動が実現されている。その結果、当該地域における政府機関とは日常的な情報共有・交換が行われている。

また、このように国際会合や二国間、地域間における取組みを通じて、我が国の情報セキュリティに関する状況や取組みは諸外国にも十分に知られるようになっている。具体的には、欧州地域や米国、アジア地域からの国際会合への参加要請、連携強化の協力要請が寄せられるようになっている。

一方で、我が国の情報セキュリティ政策が、ベストプラクティスとしての他国への模範となり、採用されるためには、継続的な情報発信に加えて、当該国における国内の取組みへの反映という段階に至る仕組み作りが必要となってくる。したがって、内閣官房は、総務省、経済産業省と連携の下、日・ASEAN情報セキュリティ政策会議を開催し、我が国の情報セキュリティに関するベストプラクティスを継続的・効果的に発信することで、日・ASEAN双方がメリットを得ることができる環境の整備を行った。このような取組みはまだ始まったばかりであり、政策の効果を評価するためには、中長期的な視点に立って検討する必要がある。この他、政策等に関する標準化、ベストプラクティス集の作成に向けた取組みは、多国間の国際機関を通じて継続的に実施されていることから、このような機会を効果的に活用した取組みが必要となる。

以上を総括すると、2009年時の姿について、当初の目標は完全に実現しているとはいえない部分も存在するが、概ね達成できたものといえる。

⑧ 犯罪の取締り及び権利利益の保護・救済

第1次基本計画の3年間を通じて、犯罪の取締り及び権利利益の保護・救済のための取組みは継続的に進められており、一定の進展がみられる。一方で、ITそのものの進展やその利活用に関する社会情勢は急速に変化しており、取組みの実態は、現在発生しているサイバー犯罪を着実に取り締まり「一定範囲内に収」めるための基盤整備に注力せざるを得ない状況であり、結果的に単調なものとなっていることが否めない。

なお、法整備に関しては、個人の権利利益との関係から慎重な検討が必要であり、一定の期間を要することはやむを得ないが、現行法の検証や社会

情勢の分析などを通じ、適時、検討を行っていく必要がある。

（２）総評

総体的には、各主体による情報セキュリティ対策の重要性の認識の高まり、組織的な取組みにおいてはPDCAサイクルによる持続的評価改善の構造の確立が進められ、また様々な対策実施状況に着実な進展が見られるなど、IT利用の客観的・主観的信頼性の確保へ向け、一定の成果があったと言える。また、IT安心利用環境の構築の過程として、官民各主体の情報セキュリティに関する連携の枠組み・基盤の整備が実施されるなど、「あるべき姿」として示されている官民連携における具体的なモデルを構築する取組みが行われた。今後、更にIT利用の客観的・主観的信頼性を確保し、IT安心利用環境を構築するためには、情報セキュリティを取り巻く環境の変化を踏まえ、構築された枠組み・基盤を基にして、各主体の自主的な取組みを推進し、その持続的な改善を図っていく必要がある。

引き続き残された課題としては、第一に長期的な視野に立った新たな枠組みからの対策を検討し、具体的に実施すること、第二にすべての対策分野において、リソース不足で対策への取組みが遅れている主体についての支援を実施すること、第三に環境の変化に柔軟に対応した上で、合理的な水準で持続的に対策を実施することが挙げられる。

第一の課題については、新たな枠組みによる取組みが必要な分野についての検討を継続するとともに、検討した対策を具体的な施策として実施する必要がある。

第二の課題については、経済状況が悪化し、情報セキュリティへの潤沢な投資が難しくなる状況が存在することに加えて、すでにリソースの不足により情報セキュリティへの取組みが遅れている主体も観測されている。こうした状況において、情報セキュリティにおいては対策の遅れている組織が全体のセキュリティ水準を決める大きな要因となるため、我が国の情報セキュリティを保つためには、リソースが不足している主体に対しての支援を行うことが必要である。

第三の課題については、対策の社会的な効果（アウトカム）が現れるまでには、継続的な取組みを実施し続けることが必要であるが、取組みを継続するに当たっては、取組みが自己目的化したり、硬直化したりしないように、社会情勢をにらみつつ、情勢に合致した修正・変更を加える必要がある。また、対策を持続するに当たっては、合理的な水準で対策を実施していく必要があることにも留意する

必要がある。

第2章　2009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的方針

第1節　2009年度から2011年度までの3箇年を通じた方向性

第2次基本計画の3箇年においては、2008年度だけでなく、第１次基本計画の計画期間3箇年を通じた取組み及びその評価を踏まえた上で、第 1 次基本計画の取組みを「継続」し、必ずしも十分でなかった取組みについては補強をしつつ、「事故前提社会」への対応力強化等の政策の「発展」に対応した新たな施策展開を行うことが求められている。また、現下の経済情勢への対応など、第 2 次基本計画策定後に発生した情勢変化への対応も考慮する必要がある。それらを踏まえた上で、単に「ITを安心して利用できる環境」を追求するだけでなく、真にITを使いこなすことのできる「力強い「個」と「社会」の確立」を目指し、次のような方向性をもって取組みを進めることとなる。

①「事故前提社会」への対応力強化のための基盤づくり

第 2 次基本計画においては、無謬性の追求を前提とした従来の事前対策中心の取組みから、事故が生じうることを前提とした形での対応力を強めること、すなわち「事故前提社会」への対応力の強化を実現することを政策の柱としている。災害への備えはもちろんのこと、国民生活や社会経済活動に影響を及ぼすようなIT障害も時々発生している状況であることを勘案すると、2009 年度から積極的に取組みを開始すべき事項の一つである。

②「合理性に裏付けられたアプローチの実現」への取組みの開始

第1次基本計画においては、政府機関を中心に、情報セキュリティ対策の基盤整備を最優先とし、集中的に取組みを実施した結果、情報セキュリティ対策を実施するための体制をとにかく整備するに至った反面、何をどこまで実施すれば良いかといった社会的合意が形成されるまでには至っておらず、費用対効果や対策の持続性といった面で課題が残された。その反省から、第2次基本計画の3年間においては、コストと効果のバランスを実現しつつ、情報セキュリティの取組みによって利便性を低下させることなく、むしろ利便性を確固としたものとするような取組みを行うことに力点を置くこととしている。

③ 現下の経済情勢への対応を支える取組みの推進

「百年に一度」、「全治三年」等と形容されている現下の経済情勢を脱するため、「デジタル新時代に向けた新たな戦略　三か年緊急プラン」（2009 年4月９日高

度情報通信ネットワーク社会推進戦略本部決定。以下「緊急プラン」という。）を始め、IT の利活用により経済成長等を図る戦略が打ち出されている。それらにおいて、ITがあらゆる分野の発展を支える「基盤」であり、国民がそれを「安心して利用できる環境」を整備するための情報セキュリティ対策もその不可欠な要素として組み込まれている事実に立脚し、緊急の経済対策等に伴うIT利活用施策の推進においても、情報セキュリティ対策を後回しにすることなく、所要のものを着実に組み込むことが重要である。

第2節　　3箇年の取組みの流れ　～　成長の各段階のイメージ　～

第2次基本計画の目指す「IT時代の力強い「個」と「社会」の確立」のためには、同計画の重要なメッセージである「事故前提社会」への対応力の強化を図ることが第一に求められる。国民の意識を改革し、社会全体での取組みを進め、あらゆる主体が、事前から事後まで一貫した情報セキュリティ対策を進めることができる「成熟した情報セキュリティ先進国」へと我が国を成長させ、その状態を継続させていくことができるようにすることが、この3箇年の取組みの目標である。このため、「個」と「社会」は、おおむね、次のようなプロセスを経て力強く成長することを目指すこととなる。

1年目（2009年度）：「自覚」の時期。すべての主体が、この社会が「事故前提社会」であることを認識し、それを前提とした情報セキュリティ対策を行うよう、改善に着手する。第 1 次基本計画の3箇年に整備された体制やツール等の基盤を活用しつつ、事後対策にも対応できるよう見直しを進める。

2年目（2010年度）：「協働」の時期。すべての主体が、それぞれの取組みの在り方についての検討を進め、関連した取組み間の連携や分担の可能性についての議論を進めるなどにより、社会全体で一貫した取組みが実施可能な状態を創り出すことに向けて、協働を開始する。

3年目（2011年度）：「成熟」の時期。すべての主体が、「事故前提社会」への対応を自主的取組みとして実施しつつ、整備された情報セキュリティ基盤を無理なく効果的に活用できるよう、進捗が遅れている施策等に重点的に取り組み、3箇年の取組みの総仕上げを図る。

第3節　　2009 年度の課題と情報セキュリティ政策の重点

SJ2009 は、第2次基本計画に基づく最初の年次計画であり、我が国の情報セキュリティ政策における 2009 年度の重要施策と 2010 年度の重要施策の方向性を定めるものである。

2009 年度においては、第 2 節に示した成長イメージに即し、「すべての主体に事故前提の自覚を」との思想を中核に据えて各種対策の立案と実施に努めることとする。あわせて、第 1 節に示した方向性を踏まえ、すべての主体が情報セキュリティ対策への取組みに当たり合理性確保を念頭に置くよう再認識を促すこと、緊急性の高いIT投資についても必要な情報セキュリティ対策を確実に盛り込むよう各主体が取り組むことなどについても、基本的な考え方として各種対策の立案と実施に努めることとする。

① 新たなテーマに対する官民の共通認識の形成

新たなテーマとなった「事故前提社会」、「合理性に裏付けられたアプローチの実現」等についての官民各主体の共通認識を形成させ、定着を図ることにより、自主的な取組みを引き出し、それを持続させることのできるよう、所要の環境整備を行うこと。特に、重要インフラに関しては、その機能が停止、低下又は利用不可能な状態に陥った場合に、国民生活や社会経済活動に多大なる影響を及ぼすおそれが生じるものであることから、サービスの維持及びIT障害発生時の迅速な復旧等の確保について各主体の共通認識が早急に醸成されるよう努める。さらに、人材の確保・育成と連動した教育や広報啓発活動の展開、情報セキュリティ対策の評価に関する指標や実施方法等の検討、その他各種実施主体間の情報共有のための体制づくり等の実施に努める。

② 電子政府の推進

緊急プランをはじめ、経済成長に係る各種戦略等において、国民の利便性向上を目的として政府全体で取組みを加速化することとされている電子政府推進に係る施策について、電子政府を便利で安心して利用可能なものとするため、適切な形で情報セキュリティ対策を組み込んでいくこと、具体的には、情報システムの企画・設計段階からの情報セキュリティ対策の組込みについて意識するための方策の検討等を進める。

③ 情報セキュリティ人材の確保・育成

各種施策を着実かつ持続的に推進することができるよう、情報セキュリティに関する知見・技能を有した人材の確保・育成、組織の情報セキュリティ対策実施体

制の整備など、人的基盤の整備を推進すること。具体的には、各種主体に対する情報セキュリティに関する教育プログラムの充実や広報啓発活動の展開、情報セキュリティに関連した資格制度の在り方の検討や活用の推進等の「スキルの見える化」をはじめ、スキルのあまり高くない利用者を身の回りからサポートするなどにより情報セキュリティ対策の底上げを図る者の育成などの取組みに努める。

④ 国際連携・協調の推進

我が国企業の国境を越えた経済活動を支援するため、安全・安心な情報セキュリティ基盤の整備を実施するとともに、IT 化が進む社会の継続性を高めるため、国境を越えて発生するIT障害等に効果的に対処することを目指し、情報セキュリティに関する国際連携・協調を一層加速させること。具体的には、経済面においては、我が国企業の進出が本格化しているアジア地域を中心に、官民及び国際的連携を進めつつ、合意に基づく具体的な取組みが実現するよう所要の取組みの推進を図るほか、社会継続性の面では、重要情報インフラ防護政策や安全保障政策に関する国際会合への我が国の取組みの積極的インプットを通じた連携強化に務める。また、横断分野の取組みとして、国際的なベストプラクティスの国内への還元を積極的に行うことにより、我が国の情報セキュリティ政策が世界最高水準となるための一助となる。

⑤ 情報セキュリティ技術戦略の推進

真に必要とされる情報セキュリティ技術について、「ITを安心して利用可能な環境」の構築に技術面からも取り組むため、「グランドチャレンジ型」研究開発など中長期的な研究開発についても着実に進捗を図るなど、技術戦略を積極的に推進すること。具体的には、技術開発は我が国の得意分野であり「底力」の源であるとの認識の下、これまでに実施されている各種技術開発・研究等の取組みが形式的なものに止まることのないよう、ニーズの積極的発掘と実装に向けた具体的な作業に結びつけるための枠組み作りや検討を強力に推進する。

第3章　2009年度に取り組む重点政策[3]

第2次基本計画においては、第 1 次基本計画の枠組みを踏襲し、情報セキュリティ対策を実際に適用し実施する主体を政府機関・地方公共団体、重要インフラ、企業、個人の4領域としている。SJ2009においても、同様に、この4領域の特性に応じた具体的施策を定めることとする。

また、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 対策実施４領域における取組みの推進と政策目的の着実な実現

（1） 対策実施4領域

①　政府機関・地方公共団体

［政府機関］

第1次基本計画期間中に決定した政府機関統一基準とそれに基づく評価・勧告という枠組みを維持しつつ、国内外の様々な組織にとって模範となるような情報セキュリティ対策を実施し、国民からの信頼に応えることができる安全かつ安心で効率的な行政運営、行政サービスの提供を行うことが可能な情報セキュリティ水準を確保していくことを目標とし、政府は、2009年度には以下の施策を重点的に推進する。

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

3　情報提供主体（個人情報のような自己の情報等を預ける主体）を対象とする取組みについては、便宜的に、第１次基本計画以来の既存の政策構造（対策実施４領域、横断４分野）の中で、関係の深い部分に盛り込む形とする。

1） PDCAサイクルの各プロセスにおけるマネジメントの強化

各政府機関においては、情報セキュリティガバナンスの確立を図るため、最高情報セキュリティ責任者の下で、当該機関の情報セキュリティ対策について責任を持って統括することが可能な体制を、情報システム統括部門（PMO）又はそれと同等の権能を有する部門に整備する。また、最高情報セキュリティ責任者を補佐する専門的知見を有する最高情報セキュリティアドバイザーを設置するとともにそのスタッフとなる人材を必要に応じて確保し、上記の体制の下でこれらの専門家の指示やアドバイスが組織全体に迅速かつ確実に反映できる仕組みを構築する。

各政府機関においては、行政に対する国民の信頼の確保に向けて情報セキュリティ対策に係る説明責任を明らかにする観点から、それぞれの情報システムの現状を把握した上で、情報セキュリティに対する考え方、情報セキュリティ対策に係る目標や計画及びその実績と評価など、それぞれの政府機関においてPDCAサイクルが有効に機能しているかどうかを数値指標などの客観的指標を積極的に活用して記述した「情報セキュリティに係る年次報告書」（情報セキュリティ報告書）を作成する。その際、情報セキュリティ報告書の客観性を確保する観点から、最高情報セキュリティアドバイザーがその作成に参画するほか、外部監査制度の活用についても、導入可能な政府機関においては積極的に推進することとする。また、作成した情報セキュリティ報告書は、最高情報セキュリティ責任者が、情報セキュリティ政策会議の下に設置されている「情報セキュリティ対策推進会議」等の場において報告し、公表する。

各政府機関における情報セキュリティ対策のバランスを確保するとともに、一層の充実・向上を推進する観点から、政府機関の情報セキュリティ報告書作成のためのガイドラインを策定するとともに、各政府機関が作成した情報セキュリティ報告書の定量的評価等を行い、その結果を情報セキュリティ政策会議に報告する。また、各政府機関の最高情報セキュリティアドバイザーが集まる会議体を設置し、情報セキュリティ報告書の比較・評価等を行うとともに、それらを通じて得られた知見の共有やフィードバックを積極的に図ることとする。

技術や環境の変化を踏まえ、政府機関における情報セキュリティ対策を常に最新かつ適切なものとするため、政府機関統一基準については、引き続き毎年その見直しを行う。

政府機関において特別に秘匿すべき情報（特別管理秘密）を取り扱うシステムに係る情報セキュリティ対策については、政府機関統一基準に基づくPDCAサイクルを基本としつつ、「カウンターインテリジェンス機能の強化に関する基本方針」[4]に基づく特別管理秘密に係る基準を踏まえた対策を、各政府機関自らの責任において着実に講じていくこととし、その実施状況を重層的にチェックする仕組みをカウンターインテリジェンスセンターを中心とする内閣官房及び関係政府機関が協力して構築する。

【具体的施策】

ア)情報セキュリティガバナンスの確立に向けた取組（全府省庁）

ⅰ)各府省庁は、情報セキュリティガバナンスの確立を図るため、最高情報セキュリティ責任者の下で、当該機関の情報セキュリティ対策について責任を持って統括することが可能な体制整備の方針を策定する。

ⅱ)各府省庁は、最高情報セキュリティ責任者を補佐する専門的知見を有する最高情報セキュリティアドバイザーの設置を推進するとともにそのスタッフとなる

4 ２００７年８月９日　カウンターインテリジェンス推進会議決定。

人材を必要に応じて確保する。

イ)PDCA サイクルの定着と浸透

a)各政府機関での PDCA サイクルの定着と浸透(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。

b)政府全体での PDCA サイクルの定着と浸透(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、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客観的に比較可能な形で評価し、勧告することにより、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サイクルの定着と浸透を確実なものとする。

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。

ウ)情報セキュリティ報告書作成のためのガイドラインの策定等(内閣官房及び全府省庁)

内閣官房は、各府省庁における情報セキュリティ報告書作成に向け、情報セキュリティ報告書作成のためのガイドラインを策定するとともに、各府省庁が作成した情報セキュリティ報告書の定量的評価等の手法等を検討する。

また、可能な府省庁については、情報セキュリティ報告書を試行的に作成し、情報セキュリティ対策推進会議等の場において報告する。

エ)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、2009年度においても政府機関統一基準の見直しを行う。

オ)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）

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・共有する場を設け、共同して課題の解決に引き続き取り組む。

c)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。

d)各府省庁の情報システムの一元的把握（内閣官房、総務省及び全府省庁）

各府省庁は、保有している情報システムに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取組を引き続き行う。

カ)コンピュータウイルスなどに起因する情報流出への対応（全府省庁）

各府省庁は、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、2009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。

キ)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）

2009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）

2009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）

すべ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、2009年度にはITガバナンス、運用面等を強化した「情報システムの信頼性向上に関するガイドライン第2版」について、政府機関における活用・普及を促進する。

ク)PDCAサイクルの確認等を支援するツールの開発・提供（経済産業省）

2009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、情報システム構成機器等のセキュリティ要件確認を支援するツール開発（2010年度提供開始予定）に着手するなど、政府機関等の情報システムにおける情報セキュリティのPDCAサイクルの確認プロセスの支援等に取り組む。

ケ)特別管理秘密を取り扱うシステムに係る情報セキュリティ対策（内閣官房及び関係省庁）

内閣官房は、関係省庁と協力し、「カウンターインテリジェンス機能の強化に関する基本方針」に基づく特別管理秘密に係る基準を踏まえた対策の実施状況を重層的にチェックする仕組みを検討し、一定の方向性について合意を得る。

2） 政府機関における人材の育成・確保及び職員の意識啓発

政府機関における情報セキュリティ関連業務を調査・検証し、これらの業務に携わる人材に必要とされるスキルをまとめる。

各政府機関においては、まとめられたスキルを踏まえ、情報セキュリティ対策に関わる内部人材の教育や確保・登用等に係る具体的な計画を、「行政機関におけるIT人材の育成・確保指針」に基づき作成した「IT人材育成・確保実行計画」に明記し、それを推進する。

また、各政府機関においては、セキュリティ対策に係る民間専門家の活用を促進するため、最高情報セキュリティアドバイザーやそのサポートスタッフの活用などの戦略的なアウトソーシングを進めるほか、任期付き採用制度などの積極的な活用を図る。

各政府機関においては、官民人事交流制度の活用による人材育成の促進のほか、階層別研修に情報セキュリティに関する内容を盛り込むなど、幹部職員も含めた全職員の情報セキュリティに関する意識の向上方策を、人事担当部門と情報システム部門の密接な協力の下に推進する。

【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）

内閣官房及び総務省は、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

上等の充実を図る。

イ)情報セキュリティ関連業務の調査等(内閣官房)

内閣官房は、府省庁における情報セキュリティ関連業務を調査・検証し、これらの業務に携わる人材に必要とされるスキルをまとめる。

ウ)人材育成・確保実行計画の実施(内閣官房、総務省及び全府省庁)

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」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。

エ)民間専門家の活用の促進(全府省庁)

各府省庁においては、セキュリティ対策に係る民間専門家の活用を促進するため、最高情報セキュリティアドバイザーやそのサポートスタッフの活用などの戦略的なアウトソーシングを進めるほか、任期付き採用制度などの積極的な活用を図る。

オ)政府職員の人材育成の促進(全府省庁)

各府省庁においては、官民人事交流制度の活用による人材育成の促進のほか、階層別研修に情報セキュリティに関する内容を盛り込むなど、幹部職員も含めた全職員の情報セキュリティに関する意識の向上方策を、人事担当部門と情報システム部門の密接な協力の下に推進する。

3) 情報セキュリティ対策を適時に行うための予算面での取組み

情報セキュリティ対策は適時の対処が必要であるため、各政府機関においては、あらかじめ可能な限りの想定を行うとともに、保守契約等においても適時適切な対応が可能となるような契約を交わすなどの取組みが必要となるが、その際には「成果重視事業[5]」制度の活用も検討するなどの工夫を行うほか、会計部門と情報システム部門が密接に協力し、予算の効率的活用に配慮して対策を進める。

【具体的施策】

ア)予算面での取組(全府省庁)

各府省庁は、情報セキュリティ対策について、あらかじめ可能な限りの想定を行った上で、準備を行うとともに、保守契約等においても適時適切な対応が可能となるような契約を交わすなどの取組みを進める。その際、確実な事業の成

5 限られた財政資金を効率的に活用する観点から、位置付けを明確にして定量的な目標をたて、事後評価を行う事業。予算執行では事業の性格に応じた弾力化を行うなど確実な事業の成果を目指すことになる。

果を目指す「成果重視事業」制度の活用の検討、会計部門と情報システム部門の密接な協力を進め、遅滞無く対処を行うよう努める。

4） 運用・管理を委託している情報システムの情報セキュリティ対策の強化

各政府機関においては、政府機関外の組織に運用・管理を委託している情報システムについて、政府機関統一基準等を踏まえた適切な契約により、委託元の政府機関の情報セキュリティポリシーの遵守を確保するとともに、適切な運用が行われているかを確認するための取組みを進める。

【具体的施策】

ア）運用・管理を委託している情報システムの情報セキュリティ対策の強化（全府省庁）

各府省庁は、政府機関統一基準（第4版では1.2.5.1「外部委託」）等を踏まえ、政府機関外の組織に運用・管理を委託している情報システムについてのセキュリティの確保のための取組みを進める。

5） 技術面の知見を蓄積・活用する仕組みの構築

情報セキュリティ対策の推進に当たって、我が国における情報セキュリティに係る技術的・専門的な知識や経験の利用を図るため、関連する独立行政法人や情報セキュリティ関係団体などの研究者・実務家の知見を集合的に活用するための仕組みの構築を推進する。

【具体的施策】

ア）情報セキュリティ対策に関連する独立行政法人等との連携の強化（内閣官房、総務省及び経済産業省）

内閣官房は、独立行政法人情報通信研究機構（NICT）、独立行政法人産業技術総合研究所（AIST）、IPA 等の独立行政法人や情報セキュリティ関係団体などの研究者・実務家の知見を蓄積・活用するため、定例的な連絡会議を開催するなど連携を強化する。

6） 情報セキュリティに関連する法令との整合性確保

現在検討が進められている文書管理法制等も含め、情報セキュリティと関連が深いと考えられる法制度等と政府機関統一基準との整合性の確保が図られるよう、必要な調整を進める。

【具体的施策】

ア）情報セキュリティに関連する法制度等との整合性確保（内閣官房）

内閣官房は、情報セキュリティと関連が深いと考えられる法制度等と政府機関統一基準との整合性の確保が図られるよう、必要な調整を進める。

（イ） 政府全体を通じて情報システムに情報セキュリティ対策が適切に組み込まれる仕組みの構築

政府機関における各種情報システムの構築を行うに際して、トータルコストの抑制や利便性・柔軟性の実現、情報セキュリティの確保といった様々な方向性をもった要件を止揚する観点から、情報システムの構築や運用段階のみならず、企画・設計段階からの情報セキュリティ対策の組込みについても意識するための方策（Security by Design）を、業務・システムの最適化の取組みと一体的に推進する仕組みの構築を図る。その際、政府全体として情報セキュリティ対策を含めた情報システムのTCO（Total Cost of Ownership：システムの導入、維持・管理などにかかる費用の総額）の低減を推進するための手法について検討を行う。

また、情報システムや物品の調達に際して、必要となる情報セキュリティ対策を設定するために参考となる各種情報を提示し、その活用を図る。

【具体的施策】

ア）企画・設計段階からの情報セキュリティ対策の組込みについても意識するための方策の検討（内閣官房、総務省及び関係府省庁）

情報システムの企画・設計段階からの情報セキュリティ対策の組込みについて意識するための方策（Security by Design）について、2009年度は、政府機関統一基準に基づきつつ、調達者と調達先ベンダの協業のあり方について検討するとともに、セキュリティを考慮した情報システム開発手法及び保証のあり方についての調査等を行う。

イ)内閣官房及び各府省情報化統括責任者（CIO）補佐官等の連携強化（内閣官房及び総務省）

2009年度も引き続き、内閣官房、CIO 補佐官及び最高情報セキュリティアドバイザー等が連携し、政府機関における情報システムのセキュリティ確保のための取組みを推進する。

ウ)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）

2009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[6]により認証された製品等を優先的に取り扱う。

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

---

6 「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。

各府省庁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、2009年度に、IPA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推進のための検討を引き続き行い、政府機関等における活用を促進する。

オ）政府情報システム等の調達時における第三者認証制度の適用範囲の明確化（内閣官房及び経済産業省）

政府情報システム等の調達時における情報セキュリティの向上のため、諸外国における状況も勘案しつつ、政府機関統一基準に定められている政府情報システム等の調達時における「ITセキュリティ評価及び認証制度」、「暗号モジュール試験及び認証制度」の認証取得の要否に関する要件の一つである「重要なセキュリティ要件」がある場合について、その明確化を図るべく必要な検討を行う。また、その検討の結果を踏まえ、政府機関施策への反映を行う。

カ）高セキュリティ機能を実現する次世代OS環境の評価及び性能向上（内閣官房、内閣府、総務省及び経済産業省）

2008年度にプロトタイプ版の開発が完了した「セキュアVM」の内閣官房での試用及び政府機関内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。また、産学官の連携により、セキュアVMの性能向上及び利用環境の拡大を図る。

（ウ） 電子政府の利便性・セキュリティレベルの向上

行政サービスの利便性向上と行政運営の効率化・高度化を推進するとともにセキュリティレベルの向上を図る観点から、電子政府に係るシステムのセキュリティ機能の在り方について検討することとし、特に利用者とのインターフェースに係るものについては、利用者の利便性を向上し、かつ安全を確保できるものとなるよう、費用対効果を勘案した上で、実装方法を含めて検討を行う。

【具体的施策】

ア）電子政府の利便性・セキュリティレベルの向上の検討（内閣官房、総務省及び経済産業省）

行政サービスの利便性向上と行政運営の効率化・高度化を推進するとともにセキュリティレベルの向上を図るため、2009年度は、電子政府ガイドライン作成検討会等の議論も踏まえつつ、実装も含めた方策について検討を行う。

イ）電子認証ガイドラインの策定及び利用の検討（内閣官房及び経済産業省）

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。

（エ） 政府機関における事業継続性確保・緊急対応能力の強化に係る検討

現在、中央防災会議の策定した「首都直下地震対策大綱」（2005年9月）に基づき、各政府機関において首都直下型地震を対象とした業務継続計画の策定は行われているが、その他の災害や障害発生時においても行政の継続性を確保する観点から、各政府機関は保有する情報システムの災害・障害時対応の必要性・優先度について決定するとともに、必要なものについては業務継続計画を策定する。また、政府機関の保有する重要なシステムや情報のバックアップ体制について政府横断的な方向性を検討する。

緊急時における対応力（レスポンス・リカバリー）の強化を図る観点から、2008年度に本格運用を開始したGSOCを核として、各政府機関や国内外の関係機関との連携をより一層深め、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することにより、政府全体としてサイバー攻撃等に対する緊急対応能力を向上させるとともに、我が国の安全保障体制の強化を図る。

【具体的施策】

ア)業務継続計画の策定の推進（全府省庁）

各府省庁は、災害や障害発生時においても行政の継続性を確保する観点から、各政府機関は保有する情報システムの災害・障害時対応の必要性・優先度について検討するとともに、必要なものについては業務継続計画の策定を推進する。

イ)重要なシステムや情報のバックアップ体制についての現状把握等（内閣官房及び総務省）

内閣官房及び総務省は、各府省庁の保有する重要なシステムや情報のバックアップ体制についての現状把握を行い、政府横断的な方向性の検討に着手する。

ウ）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の分析・解析能力の強化（内閣官房及び全府省庁）

2008年度に本格運用を開始したGSOCについて、関係機関との連携強化を進めることにより、政府機関に対するサイバー攻撃等に関する分析・解析能力の向上を図る。

b)情報保証に係る最新技術動向等の調査研究（防衛省）

2008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。

エ）各政府機関における緊急対応能力の強化支援

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年度に引き続き、本格運用を開始した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分析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。

b)サイバー攻撃等に係る分析・対処及び研究の推進（防衛省）

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、2008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。

オ)サイバーテロに関する対策の強化（警察庁及び法務省）

サイバーテロ[7]への対策を強化するため，サイバー空間におけるテロの予兆等の早期把握を可能とする態勢を整備するとともに，諸外国関係機関との情報交換等国際的な連携を強化するなどして，攻撃主体・方法等に関する情報収集・分析を継続的に実施する。

（オ） 独立行政法人等の情報セキュリティ対策の推進

独立行政法人等の情報セキュリティ対策を推進するため、独立行政法人等を所管する政府機関は、中期目標の中に情報セキュリティ対策に係る事項を明記し、独立行政法人等が組織として情報セキュリティ対策に取り組む体制を構築させる。各独立行政法人等は、その業務特性及び対策の実施状況に応じて、政府機関統一基準を含む政府機関における一連の対策を踏まえ、自らの情報セキュリティ対策に係るPDCAサイクルを構築する。また、独立行政法人等及び独立行政法人等を所管する政府機関は、緊急時を含め実効性のある連絡体制を整備する。

【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

7 重要インフラの基幹システムに対する電子的攻撃又は重要インフラの基幹システムにおける重大な障害で電子的攻撃による可能性の高いもの。

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。

ウ)情報セキュリティ対策に係る事項の中期目標への明記（独立行政法人等所管府省庁）

各府省庁は、所管する独立行政法人等の情報セキュリティ対策を推進するため、中期目標に情報セキュリティ対策に係る事項の明記を推進する。

エ)各独立行政法人等におけるPDCAサイクルの構築（独立行政法人等所管府省庁）

各府省庁は、所管する独立行政法人等が、その業務特性及び対策の実施状況に応じて、政府機関統一基準を含む政府機関における一連の対策を踏まえ、自らの情報セキュリティ対策に係るPDCAサイクルを構築するための取組みを推進する。

オ)緊急時等の連絡体制の整備（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と、緊急時を含め実効性のある連絡体制を整備し、実効性の確認を行う。

（カ） その他個別の情報セキュリティ対策の推進

1） 政府機関の情報システムのIPv6対応化

IPv4アドレス枯渇への先導的な対応を実施する観点から、政府機関においては、各情報システムの新たな開発（導入）又は更改に合わせてIPv6対応を計画的に進め、特に電子政府システムをはじめとする外部と直接通信を行う情報システムについては、原則として、2010年までにIPv6対応化を図ることとしているが、その際、IPv4からIPv6への移行期におけるセキュリティ上の課題に適切に対応する。

【具体的施策】

ア)電子政府システムの IPv6 対応化（内閣官房、総務省及び全府省庁）

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・情報漏えい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 アドレス在庫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、2009年度も引き続き、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 対応化を

図る。その際、IPv4 から IPv6 への移行期におけるセキュリティ上の課題に適切に対応する。この円滑な実施のための以下の措置を実施する。

ⅰ）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、2009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」（2008年（平成20年）12月25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。

ⅱ）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、2009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。

2） 政府機関への成りすましの防止

悪意の第三者が政府機関又は政府機関の職員に成りすまし、一般国民や民間企業等に害を及ぼすことが無いよう、正統な政府機関又は政府機関の職員であることを容易に確認可能とするため、電子メールやウェブサーバでドメイン名として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を使用することや、政府機関から発信する電子メールへの電子署名の付与等電子証明書の活用に係る取組みを推進する。

【具体的施策】

ア）政府機関から発信する電子メールに係る成りすましの防止（内閣官房、総務省及び全府省庁）

悪意の第三者が政府機関又は政府機関の職員に成りすまし、一般国民や民間企業等に害を及ぼすことが無いよう、SPF(Sender Policy Framework)等の送信ドメイン認証技術の採用等を推進していく。

イ）政府機関のドメイン名であることが保証されるドメイン名の使用の推進（総務省及び全府省庁）

2009年度も引き続き、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（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」）を利用するよう取り組むとともに、当該取組状況を国民に対して広く周知する。

3） 政府機関における安全な暗号利用の推進

電子政府の安全性及び信頼性を確保するため、政府機関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組みを踏まえ、現行の「電子政府推奨暗号リスト」の2013年度改訂に向けて、関係機関において所要の作業を進める。また、「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA－1及びRSA1024に係る移行指針」[8]の策定時の経験を適切に継承し、安全性が低下した暗号について速やかに安全な暗号への移行を進める。

【具体的施策】

ア)政府機関における安全な暗号利用の推進（内閣官房、総務省、経済産業省及び全府省庁）

ⅰ)総務省及び経済産業省は、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の確保のための調査、研究、基準の作成等を2009年度に行う。

ⅱ)総務省及び経済産業省は、「電子政府推奨暗号リスト」の改訂に向けた取組みを着実に実施する。

ⅲ)内閣官房、総務省及び各府省庁は、「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」に従った取組みを推進する。また、内閣官房は、「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」の策定時の経験を適切に継承し、安全性が低下した暗号について速やかに安全な暗号への移行を進める。

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

安全性の高い暗号モジュールの活用を推進するため、引き続き、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。

［地方公共団体］

各々の地方公共団体において、また幅広い行政分野全体において、望ましい情報セキュリティ対策が実施されることを目標とし、政府は、2009年度には以下の施策を重点的に推進する。

8 ２００８年４月２２日　情報セキュリティ政策会議決定。

（ア） 小規模な地方公共団体も含めた合理的・自主的な情報セキュリティ対策の促進

小規模な地方公共団体も含め、全ての地方公共団体において、望ましい情報セキュリティ対策が実施されることを目指し、対策の促進を行う。具体的には、対策や監査の基となる情報資産のリスク分析の実施を促進するとともに、情報セキュリティポリシーの策定等の検討や監査の実施に向けたガイドラインの見直し、業務継続計画の策定に資するガイドライン[9]の普及などを行う。また、人材面では、取組みを担う職員等の能力向上に向けた共同勉強会や地域セミナーの開催などを進める。

【具体的施策】

ア)地方公共団体の情報セキュリティ対策水準向上のための普及・啓発（総務省）

地方公共団体における情報システム部門の業務継続計画の策定、情報資産台帳の作成及びリスク分析の実施等の促進を図るため、全国数か所において、情報セキュリティに関するセミナーを開催する。

また、情報セキュリティポリシーのガイドラインの見直しを行うほか、取組意欲のある地方公共団体にICT部門における業務継続計画策定アドバイザーの派遣を行う。

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

地方公共団体において情報セキュリティ対策に投資できるリソースの限度を考慮し、複数地方公共団体間で効率的に対策を実施するための連携に向けた取組みを応援する。このため、全国の地方公共団体に対するベスト・プラクティスの紹介やモデルケースができるような応援を行う。また、地方公共団体の長の理解促進のための勉強会や検討会を実施し、組織トップの意識を高めるとともに、例えば、相互監査等の取組みにおけるアドバイザー派遣などを検討する。

【具体的施策】

ア）地方公共団体の情報セキュリティ対策水準向上のための普及・啓発（総務省）

複数団体間での情報セキュリティベストプラクティスやモデルケースの募集を行う。

また、相互監査ができるよう、内部監査アドバイザーの派遣を支援する。

9 総務省「地方公共団体におけるＩＣＴ部門の業務継続計画（ＢＣＰ）策定に関するガイドライン」（平成２０年８月）

（ウ） 地方公共団体の取組みを応援する主体の強化

地方公共団体の対策を進めるには、取組みを応援する主体を強化することが有効である。このため、官・民・NPOによる共同勉強会を開催するなど情報セキュリティに役立つ知見を有するあらゆる主体の協力体制を構築するとともに、LGWAN（総合行政ネットワーク）内のポータルサイトを活用した自治体向け支援体制の強化などを進める。

【具体的施策】

ア）地方公共団体の情報セキュリティ対策水準向上のための普及・啓発（総務省）

LGWAN（総合行政ネットワーク）内のポータルサイトに情報セキュリティに関する解説等を提供するなど、その運営を支援する。

（エ） 地方公共団体が担う幅広い行政分野での対応促進

国家行政組織と地方公共団体の担当組織の間の個別の関係を踏まえた形で、地方公共団体が担う幅広い行政分野における情報セキュリティ対策を促進する。例えば、学校におけるIT基盤の整備に際して、情報セキュリティの視点も十分に加味することや、関係省庁から、都道府県教育委員会に対し、情報セキュリティ対策上有効な方策を伝達することや、ベストプラクティスを紹介し、都道府県教育委員会の意識向上を促進するといったことが考えられる。

【具体的施策】

ア)地方公共団体の情報セキュリティ対策水準向上のための普及・啓発（内閣官房、総務省及び文部科学省）

教育関係部門での情報セキュリティ事故が比較的多いことから、まずは総務省と関係省庁との連携を行う。これまでの情報セキュリティ対策や取組の実施状況の分析、今後の方策等について具体的なビジョンを組み立てる。また、地方自治体の情報教育担当が集まる会議等において、情報セキュリティの取組みに関する普及・啓発を行う。

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

約1800の地方公共団体の情報セキュリティ対策を促進するには、地方公共団体間でベスト・プラクティスを相互活用することが効率的である。このため、LGWAN（総合行政ネットワーク）内に設置しているポータルサイトを利用し、地方公共団体間での情報共有を促進する。また、ベスト・プラクティスを地方公共団体の長や現場担当者などの様々な階層において共有できるよう検討会や意見交換会等を開催する。

加えて、地方公共団体同様、公的組織である政府機関との間でのベスト・プラクティスの相互活用も有効と考えられることから、これに向けた方策の検討を実施する。

【具体的施策】

ア）地方公共団体の情報セキュリティ対策水準向上のための普及・啓発（総務省）

情報セキュリティベストプラクティスの募集や情報セキュリティ事故情報の充実を図り、LGWAN（総合行政ネットワーク）内に現在設置しているポータルサイトのさらなる利用を促進する。

（カ） 地域の情報セキュリティ対策の担い手の育成支援

地域において情報セキュリティ対策を担えるような人材の育成に際しては、地方公共団体による促進活動が有効であることから、地方公共団体のこのような活動が行いやすくなるような環境整備に取り組む。具体的には、地方公共団体が情報セキュリティをテーマとした住民向け教養講座等を開催しやすいよう、講座で活用できるような参考資料等を作成、紹介する。また、Teaching teachers（教えることのできる人材の教育・育成）の発想に基づき、地方において人材育成が促進されるような取組みを行う。

【具体的施策】

ア）地方公共団体の職員に対する情報セキュリティ関係研修の充実（総務省）

すべての地方公共団体の職員が、時間や場所に制約されずに受講できる e-ラーニングの内容の充実とその実施を促進する。

② 重要インフラ

重要インフラの情報セキュリティ対策に関する関係主体は、「重要インフラの情報セキュリティ対策に係る第2次行動計画」（2009年2月3日情報セキュリティ政策会議決定。以下「第2次行動計画」という。）に基づいて、重要インフラにおける IT 障害が国民生活や社会経済活動に重大な影響を及ぼさないようにすることを目標とし、各々の役割に応じて情報セキュリティ対策に取り組み、重要インフラサービスの維持及びIT障害発生時の迅速な復旧等の確保を図ることとする。2009年度には以下の施策を重点的に推進する。

（ア）「安全基準等」の整備及び浸透

第1次行動計画で策定された指針について、事業継続の観点からの具体的内容の補充を含め、指針の位置づけや記載内容の具体性のレベルの見直しを行う。また、重要インフラ事業者等のPDCAサイクルとの整合性を踏まえた安全基準等の整備の推進などの底上げに資する取組みのみならず、3年毎に個別の先進的な対策を伸ばしその浸透を図る観点からの取組みも推進する。

【具体的施策】

ア）指針の継続的改善（内閣官房）

重要インフラ所管省庁の協力を得つつ、2009年度上半期に指針の分析・検証を行い、2009年10月を目処に「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（第3版）」（仮称）を決定する。加えて、社会動向の変化等に対応し、新たな知見を適時反映していくために、引き続き同指針の分析・検証を行い、必要に応じて2010年度以降における同指針の追補版の公表に向けた準備を行う。

イ）安全基準等の継続的改善

a)安全基準等の継続的改善（重要インフラ所管省庁）

「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（第3版）」（仮称）や各重要インフラ分野の特性を踏まえ、2009年度末を目処に各重要インフラ分野において安全基準等の分析・検証を実施する。また、必要に応じて安全基準等の改定等の対策を実施する。

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において2006年度に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2009年度も引き続き、国際規格化の状況を踏まえつつ、国内標準化機関等と連携し、国内標準化や認証制度の導入等の普及促進に向けた取組みを行う。(ISM-TG : Information Security Management Guideline for Telecommunications)

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

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。

d)安全基準等の継続的改善状況等の把握及び検証（内閣官房）

重要インフラ所管省庁の協力を得つつ、各重要インフラ分野における「安全基準等」について、2009年度中に安全基準等の分析・検証及び改定等の実施状況並びに今後の実施予定等の把握及び検証を実施し、結果を公表する。

ウ)安全基準等の浸透（内閣官房及び重要インフラ所管省庁）

各重要インフラ分野において安全基準等の浸透を実施するとともに、重要インフラ所管省庁の協力を得つつ、2009年度当初に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を実施し、2009年 10 月を目処にそ

の結果を公表する。
また、次年度の調査のための企画・準備を実施する。

（イ） 情報共有体制の強化

第1次行動計画で策定されたセプター[10]、セプターカウンシル[11]を含む関係主体間で共有する情報についての整理を行い、情報提供、情報連絡等に必要な環境整備等を推進するとともに、各セプター、セプターカウンシルの自主的な活動の充実強化を推進する。

【具体的施策】

ア）共有すべき情報の整理（内閣官房）

IT障害に関する情報について、未然防止、拡大防止・迅速な復旧、再発防止の3つの側面を踏まえ、共有対象とする情報とその共有方法等の整理を行う。

イ）情報提供、情報連絡の充実

a)情報共有ルールの見直し（重要インフラ所管省庁）

情報提供に係る重要インフラ所管省庁からセプターへの情報共有ルール及び情報連絡に係る重要インフラ事業者等から重要インフラ所管省庁への情報共有ルールのそれぞれについて、「「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」の情報連絡・情報提供に関する実施細目」との整合性を確認し、必要に応じてこれら情報共有ルールの改定等の改善を行う。

また、情報提供に係るセプター内の情報共有ルールについて、当該細目との整合性の確認をセプターが行えるよう、当該セプターに対して助言等の支援を行い、またセプターにおける対応状況を確認する。

b）第2次行動計画の情報連絡・情報提供に関する実施細目の見直し（内閣官房）

「「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」の情報連絡・情報提供に関する実施細目」の運用状況や、「共有すべき情報の整理」の進捗状況等を踏まえ、実施細目の見直しを実施する。

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

2008年度に引き続き、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、IPA

10 CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response

11 重要インフラ連絡協議会（CEPTOAR-Council）

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、蓄積された情報のセプター等への提供を行う。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。

d)セプター訓練の実施（内閣官房及び重要インフラ所管省庁）

重要インフラ所管省庁の協力を得つつ、各分野におけるセプターの情報共有体制の維持及び向上のための情報疎通機能の確認の機会を提供する。

ウ)セプターの強化（内閣官房及び重要インフラ所管省庁）

重要インフラ所管省庁の協力を得つつ、セプターの強化を支援するために、各セプターの機能及び活動状況等の事例をとりまとめ、各セプターと共有する。また、各セプターの機能及び活動状況をとりまとめ、2009年度末を目処に公表する。

エ)セプターカウンシルの支援（内閣官房）

セプターカウンシルの事務局として、セプターカウンシルの活動を支援する。

（ウ） 共通脅威分析

第1次行動計画で実施してきた、ある重要インフラ分野にIT障害が発生した場合に他のどの重要インフラ分野に影響が波及するか、という相互依存性解析を継続するとともに、重要インフラ分野共通に起こりうる脅威が何であるかを把握するための検討を行う。

【具体的施策】

ア）共通脅威分析の実施（内閣官房）

重要インフラ分野共通に起こりうる脅威の分析と相互依存性解析を合わせた共通脅威分析を、重要インフラ分野のニーズに照らして優先順位が高く、実際に対応可能な分析対象に対して実施する。また、関連する国内外の研究動向、IT 障害事例等の調査を実施する。これらの分析・調査対象については重要インフラ事業者等へのアンケート等で抽出する。

実施にあたっては、重要インフラ所管省庁、セプター及び重要インフラ事業者等の協力を得るとともに、実効性を高めるために研究機関との連携等の実施手法を検討する。

なお、分析・調査結果は報告書として取りまとめ、可能な範囲で公表する。

（エ） 分野横断的演習

第1次行動計画において得られた分野横断的な演習手法に関する知見を踏まえ、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セプター等の協力を得て、IT障害の発生を想定した、重要インフラ分野横断的な演習を実施する。

【具体的施策】

ア）分野横断的演習の実施（内閣官房及び重要インフラ所管省庁）

重要インフラ所管省庁、セプター及び重要インフラ事業者等の協力を得て、具体的な IT 障害発生を想定した演習シナリオの検討とそれに基づく分野横断的な演習を実施し、課題の抽出及び演習実施のための知見の整理を行う。

なお、得られた課題や知見は、関係者間で共有すると共に、可能な範囲で公表する。

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）

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て電気通信事業者を中心に実施するサイバー攻撃対応演習に関して、2009年度も引き続き、電気通信事業者やメーカ等から構成されるテレコムアイザック推進会議と連携して取組を推進する。

ウ）情報セキュリティに関する国際会合の開催（内閣官房及び関係府省庁）

世界的規模で行われるサイバー演習（Cyber Storm III)への参加に向けて、各国の重要インフラ防護政策、緊急対応チーム及び法執行機関等の専門家が参加する国際監視・警戒ネットワーク（IWWN）会合招致に向けた活動を行う。

（オ） 環境変化への対応

社会環境や技術環境等の状況の変化に合わせて情報セキュリティ対策を機敏に対応させていくために、第2次行動計画策定時に想定しなかった環境の変化を察知する能力の向上に努める。また、こうした環境の変化に対して第2次行動計画の枠組みだけでは十分に対応できない場合は、内閣官房は必要な対応が可能となるような体制の検討を行う。

【具体的施策】

ア）広報公聴活動

a）広報公聴活動の充実（内閣官房）

情報セキュリティ対策についての広報公聴に資するWebサイトを構築し、運用する。

セミナーや講演等の機会を活用し、第2次行動計画及び同計画に基づく諸

施策の広報活動に積極的に取り組む。

b）重要インフラ事業者向けの啓発セミナー等の実施（経済産業省）

2009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。）等により開催する。

イ）リスクコミュニケーションの充実

a)リスクコミュニケーションの充実（内閣官房、重要インフラ所管省庁）

重要インフラ所管省庁の協力を得つつ、重要インフラ事業者等、関係機関及び重要インフラ所管省庁等が相互にリスクコミュニケーションを推進できる環境整備に取り組む。

b）ソフトウェアや情報システムの脆弱性の発生を縮減するための対策の推進（経済産業省）

ソフトウェア製品や情報システムについて製品の流通後やシステムの稼働後に脆弱性が発見された場合には、その修正のために製品開発者及びユーザーの双方に対応コストが発生し、対策が適切に行われない場合には、不正アクセス等の攻撃の対象となる等により、さらに深刻な被害が発生する可能性がある。このようなコストやリスクを最小化するため、JPCERT/CC 等において、ソフトウェア製品や情報システムの設計から、プログラミング、出荷前の検査等の各段階において、製品開発者が情報セキュリティ上の観点から配慮すべき事項を、解説資料やセミナーの形で公開し、普及を図る。2009年度においては、流通後の修正が容易でない組込みソフトウェアにおいて多用されている言語について、セキュアコーディングセミナーの実施やコーディングスタンダードの開発現場への浸透を図るための取組み等を行う。

c）重要インフラ事業者に対するソフトウェア等の脆弱性関連情報の優先提供及び情報セキュリティ関連情報マネジメントの支援等（経済産業省）

JPCERT/CC を通じ、一般公開前のソフトウェア等の脆弱性関連情報、その他の重要インフラ事業者において対策が必要となる可能性のある情報セキュリティ上の脅威及びその対策に関する情報を、事前の合意に基づき、早期警戒情報として、セプターまたは重要インフラ事業者に提供する。

また、重要インフラにおける組織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。）の構築・運用に資する情報や、数多く提供される情報セキュリティ関連情報のマネジメントの効率化を図るためのツールを提供するとともに、ソフトウェア等の脆弱性に関する情報をマネジメントツールが自動的に取り

込める形式で配信するサービスの提供を拡大する。

さらに、JPCERT/CC において、重要インフラ事業者の依頼に応じ、攻撃元に対する調整等の情報セキュリティインシデントへの対応支援や、攻撃手法の解析の支援を行う。

d）重要インフラ事業における制御システムの脆弱性に関する情報提供等（経済産業省）

重要インフラ事業における制御システムでの脆弱性リスク削減、及び脅威への対応等について、収集した情報等を当該事業者等へ情報提供を行う。また、制御システムを実運用に近い実証環境で評価することができるテストツールの仕様の調査に着手する。

e）制御システムに関する脆弱性への対応のための連携体制の構築（経済産業省）

制御システム製品に関しては、標準プロトコル（TCP/IP やイーサネット等）や汎用製品の導入が進むことにより、潜在的な脅威が高まることが想定される一方で、対策、ベストプラクティス等は整備段階にあり、開発／構築にたずさわる技術者における情報収集・評価の負担の増加が予想される。このため、2009年度においては、JPCERT/CC を事務局として2008年度に発足した「制御システムベンダーセキュリティ情報共有タスクフォース」の活動を本格化し、制御システムにおけるセキュリティ対策の推進に資する情報の収集、共有を推進することにより、制御システムに関する脆弱性等の脅威への対応の円滑化を図る。

ウ）国際連携の推進（内閣官房）

外国のベストプラクティスを収集するとともに、情報セキュリティ政策に関する国際機関の動向や標準化の動向を把握する。

また、国際的な脅威・脆弱性情報に関する情報収集を行い、関係主体に提供する。

③ 企業

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標とし、政府は、2009年度には以下の施策を重点的に推進する。

（ア） 情報セキュリティガバナンスの「経営の一環としての位置付け」の確立

情報セキュリティガバナンスを経営の一環として位置付けるため、そのための取組みを推進し、経営層に対する啓発活動の推進、合理的な情報セキュリティガバナンス確立プロセスモデルの開発などの取組みを行う。また、経営者における意識向上を図るための体制の強化を目指すとともに、情報セキュリティマネジメントシステム（ISMS）適合性評価や情報セキ

ュリティ監査、ITセキュリティ評価及び認証制度、暗号モジュール試験及び認証制度などの制度、情報セキュリティ報告書モデル、情報セキュリティ対策ベンチマークなどのツールの普及・開発・改善等を更に進め、具体的な取組みが浸透することを目指す。さらに、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。加えて、情報セキュリティガバナンスのための取組みが企業にとって過度の負担とならないよう、投資効率を測る手法を実際に活用可能にするための検討を促進する。また、情報セキュリティガバナンスが「経営の一環としての位置付け」を確保するには、関連法制との関係で整理が必要となる論点もある。このため、関連法制度の分析整理を行い、ガイダンスとして整備するような取組みも推進する。

【具体的施策】

ア）情報セキュリティガバナンス確立の促進（経済産業省）

企業における情報セキュリティガバナンスの更なる確立に向け、「情報セキュリティガバナンス導入ガイダンス（仮称）」、「アウトソーシングセキュリティガイダンス（仮称）」等を策定し、普及促進するとともに、国際的な企業間連携における適用を目指した国際標準化等を進める。

また、2008年度にITガバナンスや運用面を強化して改訂した「情報システムの信頼性向上に関するガイドライン第2版」や「情報システムの信頼性向上に関する評価指標第2版」について、情報システムの構築や運用を各企業が行う際に、当該ガイドライン及び評価指標を活用することを推奨すべく、普及活動を継続的に実施する。

イ）情報セキュリティ監査制度の利用促進（経済産業省）

監査人が被監査主体の情報セキュリティに関する言明に対して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、業界、業種などに注目した管理基準や監査実務指針の策定を支援し、保証型監査の利用促進を行う。

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

2009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、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。

エ）「情報システム・モデル取引・契約書」の活用・普及（経済産業省）

情報システムの信頼性向上の観点から、ユーザー・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、また、特に中小企業の取引の多数を占めるパ

ッケージ・SaaS[12]・ASP[13]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4月に策定、公表した。これらモデル取引・契約の普及について、ユーザー・ベンダ双方の関係業界団体と連携して取り組んでいく。

オ）「情報セキュリティ対策ベンチマークシステム」の提供（経済産業省）

IPA において、「情報セキュリティ対策ベンチマークシステム」を引き続き提供する。

カ）企業に係る指標の充実等（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。

キ）入札条件等の見直し（内閣官房、総務省、財務省、経済産業省及び全府省庁）

情報システムに係る政府調達について、例えば、ISMSや情報セキュリティ監査、情報セキュリティ格付等を含めた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。

ク)企業における電子署名利活用の普及促進（総務省、法務省及び経済産業省）

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、検討を行う。

12 Software as a Service

13 Application Service Provider

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

企業における情報セキュリティ対策が進展するよう、企業が理解しやすい形で必要な情報セキュリティ対策を選択できる環境を整備する。第1次基本計画に続き、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実用化を目指した研究を促進するとともに、ITセキュリティ評価及び認証制度の活用を促進する。

また、情報セキュリティ向上に資する製品やサービスの提供促進と活動の推進のためには、対策支援主体側の取組みの強化も必要である。対策を容易化するSaaSやASPなどの活用促進や、迷惑メール対策の強化、暗号技術や認証技術、NGN／IPv6移行環境のセキュリティ評価システム等の技術開発の促進等の取組みを進める。なお、取組みにあたっては、TCOにも目配りした製品やサービスの提供が促進されるような視点も重要である。

【具体的施策】

ア）ソフトウェア等の脆弱性に係るマネジメントの支援等（経済産業省）

IPA において、2008年度に開始した、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の運用を継続するとともに、機能強化を行う。

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や手法の普及促進及び改善を進めるとともに、ユーザー組織における対応コストの低減のためソフトウェア等の脆弱性に関する情報をマネジメントツールが自動的に取り込める形式で配信するサービスの提供を拡大する。

イ）ソフトウェアや情報システムの脆弱性の発生を縮減するための対策の推進（経済産業省）【再掲】

ソフトウェア製品や情報システムについて製品の流通後やシステムの稼働後に脆弱性が発見された場合には、その修正のために製品開発者及びユーザーの双方に対応コストが発生し、対策が適切に行われない場合には、不正アクセス等の攻撃の対象となる等により、さらに深刻な被害が発生する可能性がある。このようなコストやリスクを最小化するため、JPCERT/CC 等において、ソフトウェア製品や情報システムの設計から、プログラミング、出荷前の検査等の各段階において、製品開発者が情報セキュリティ上の観点から配慮すべき事項を、解説資料やセミナーの形で公開し、普及を図る。2009 年度においては、流通後の修正が容易でない組込みソフトウェアにおいて多用されている言語について、セキュアコーディングセミナーの実施やコーディングスタンダードの開発現場への浸透を図るための取組み等を行う。

ウ）企業の運営するWebサイトの安全性向上（経済産業省）

ウェブアプリケーションの脆弱性を早期に発見し対処に役立てるため、ログを解析し外部からの攻撃の痕跡を検査する「ウェブサイト脆弱性のログ解析型検査ツール」(iLogScanner)を企業の Web サイト運営者等に引き続き提供するとともに、必要に応じてウェブサイトに対する新たな攻撃パターンに対応する。

エ）組込みソフトウェアの安全性向上のための取組み（経済産業省）

組込み機器や情報家電等の開発者に利用されているプロトコルである TCP/IP 及び SIP の脆弱性検証ツールを開発者に引き続き提供するとともに、新たに発見された脆弱性への対応を行う。

オ）「データセンターの安全・信頼性に係る情報開示指針」の活用・普及（総務省）

近年、企業活動の基盤として高質かつ環境負荷の低いデータセンターへの需要が日々拡大しており、データセンターの比較・評価を行い選択する動きが顕在化してきている状況を踏まえ、データセンターの安全・信頼性に係る情報開示を必須の項目と選択の項目に分け、情報開示項目を共通かつ豊富にするとともに、データセンター利用者によるデータセンターの比較、評価、選択等を容易にすることを目的として、データセンターの建物・設備・セキュリティ等に関し情報開示が求められる項目を示した「データセンターの安全・信頼性に係る情報開示指針(第 1 版)」（2009年2月策定・公表）について、データセンターの事業者及び利用者に広く活用・普及を促進する。

カ）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）【再掲】

2009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、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。

キ）システムLSIのセキュリティ評価体制の整備（経済産業省）

2011年度までに、IC カード等に用いられるシステム LSI について、国内で ISO/IEC15408 に基づくセキュリティ評価が行えるよう必要な体制整備を行う。

ク）信頼性を評価するための共通の評価指標の確立（経済産業省）

システム開発プロジェクトの成功率を高め、情報システムの信頼性を向上するためには、定量データによる品質管理が有効であり、関係業界団体で評価指標を策定し、定量データを蓄積している。こうした定量データによる品質管理をさら

に推進するために、各評価指標や定量データを相互に活用できる共通ルール等を確立し、広く普及活動を推進する。

ク)「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、SaaSの利用者と提供者の双方に広く活用・普及を推進する。

ケ)「ASP・SaaS の安全・信頼性に係る情報開示認定制度」の活用・普及(総務省)

企業が、ASP・SaaS を利用するに当たり、サービスの比較・評価・選択を容易にするため、「ASP・SaaS の安全・信頼性に関する情報開示指針」に基づき民間団体が運営する ASP・SaaS 安全・信頼性に係る情報開示認定制度の普及・活用を図る。

コ)「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」の策定・活用・普及(総務省)

医療情報の重要性から見た高度な安全性の要求を踏まえ、医療情報がASP・SaaS によって適正かつ安全に利用され、医療情報における ASP・SaaS の利用の促進を図ることを目的として、ASP・SaaS 事業者が医療情報を取り扱う際に求められる責任等、ASP・SaaS 事業者への要求事項等、合意形成の考え方等を示した「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」を策定するとともに、医療情報を取り扱う ASP・SaaS の事業者及び利用者に広く活用・普及を促進する。

サ)情報セキュリティ対策を容易化するシステム等の開発(経済産業省)

中小・小規模企業でも安価かつ容易に業務効率化を行える、インターネットを活用したソフトウェア提供サービス(SaaS)の基盤となるシステムや、その上で稼働するセキュリティ管理等のアプリケーションを開発する。

シ)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応するため、2008年の法改正によりオプトイン方式が導入された特定電子メール法及び特定商取引法の着実な執行等所用の措置を講じる。

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、日本に着信するスパムメールの大部分を占める海外から発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塔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。

ス）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。

セ）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）【再掲】

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、検討を行う。

ソ）NGN/IPv6 環境のセキュリティ評価システムの構築（総務省）

NGN/IPv6 への移行に伴う脅威や脆弱性などの具体的なセキュリティ課題を抽出し、その重要度を評価した上で、対応可能性などを追求するため、NGN/IPv6 環境のセキュリティ評価システムを構築する。

タ） 安全性確保のためのソフトウェア等のリバースエンジニアリングの適法性の明確化 （文部科学省）

文化審議会著作権分科会の報告に基づき、情報セキュリティ目的のリバースエンジニアリングの適法性を明確化するための措置を速やかに講ずる。

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

2008年度税制改正により 2 年間延長・拡充された産業競争力のための情報基盤強化税制について、引き続き、その普及・啓発を図ることにより、企業における高度な情報セキュリティが確保された情報システム投資を促進する。

ツ）非機能要求の合意手法の確立（経済産業省）

情報システムの信頼性向上のために、信頼性、性能、あるいはセキュリティ等に関する要求を含む非機能要求項目について、ユーザー・ベンダ間で適切に合意するための手法を策定し、その普及について関係業界等と連携して取り組んでいく。

（ウ） 企業における情報セキュリティ人材の育成・確保

経営層の情報セキュリティ対策への理解増進とともに、企業の情報セキュリティ対策の推進を担う人材の育成・確保が必要不可欠であることから、人材育成に向けたセミナー開催等の広報啓発を推進する。また、対策においては、新たなITの利用・活用など、環境の進化に柔軟に対応できる人材や企業のマネジメント全体を俯瞰した上で判断できるスキルを持った人材などの育成・確保も必要不可欠である。その際には、情報セキュリティ人材の目指すキャリアパスを考慮に入れることも重要である。こうしたことを踏まえ、官民の適切な役割分担のもと、客観的な人材評価メカニズムである各スキル標準の整合化を図った共通キャリア・スキルフレームワークとそれに準拠した情報処理技術者試験の活用、及び民間の人材育成に関するフレームワークや各種資格試験の活用を促進する。また、産学連携による高度情報セキュリティ人材を育成するためのカリキュラム整備や教員強化、インターンシップの充実等に取り組むための体制を整備する。

また、技術者向けの情報セキュリティに係るモデルキャリア開発計画の策定や専門家コミュニティへの支援を進めることで、広く企業の情報セキュリティを担うことのできる人材の育成・確保に取り組む。

さらに、今後の課題となるNGN／IPv6への移行などの新しい環境への移行に対応できる実践的な情報セキュリティ人材や法令遵守、情報資産や事業継続等に関するリスクを特定しつつ、情報セキュリティ対策を実践できる人材の育成を推進する。

【具体的施策】

ア）中小企業情報セキュリティ対策の促進（経済産業省）

中小企業に指導する立場にある者を対象とした「中小企業情報セキュリティ指導者育成セミナー」において、情報セキュリティに関する知識等を習得させ、当該セミナーで習得した知識を基に、中小企業の経営者等に対して情報セキュリティ対策に係る普及啓発を図る。

イ）中小企業を対象とした情報セキュリティセミナー等の実施（経済産業省）

2009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。地域中核団体との連携を強化するとともに、IT 経営応援隊と連携した普及広報活動を行う。

ウ）情報セキュリティ監査知識を有する人材の育成（経済産業省）

情報セキュリティ対策を組織の内部ならびに外部から客観的かつ公正に評価

できる情報セキュリティ監査知識を有する人材の育成を行う。

エ）情報セキュリティ・サポーターの育成（総務省）

情報セキュリティに関する教材作成や講習会・認定試験の開催を支援することにより、利用者の身の回りの詳しい人（情報セキュリティ・サポーター）を育成し、国民全体の情報セキュリティの底上げを行う。

オ）情報処理技術者試験の更なる普及（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種情報分野の人材スキルを測る情報処理技術者試験を共通キャリア・スキルフレームワークに基づく見直しを行い、2009年度から実施する。当該試験合格者が多数輩出されることにより、共通キャリア・スキルフレームワークに基づいた適切な人材評価手法による効果的なキャリアパスが形成されることが期待され、当該試験を活用した人材育成を図る。

カ）民間のセキュリティ資格の周知（内閣官房、総務省及び経済産業省）

民間における情報セキュリティ専門家の充実の観点から、民間の情報セキュリティに関する資格の周知を図る。

キ）産学連携IT人材育成実行事業（経済産業省）

情報セキュリティ人材を含めた高度 IT 人材の育成のため、産業界出身教員等の充実・強化、実践的な教材・カリキュラムの開発・普及、産学マッチングによる実践的なインターンシップなどを推進するための産学連携体制を強化する。

ク） 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、2009年度においても助成を行う。

ケ）IPv6 運用技術習得のためのテストベッドの整備（総務省）

IPv4 アドレス在庫の枯渇に対応するため、我が国においても早急に IPv6 対応化を進める必要があるが、ネットワーク運用者等における IPv6 運用技術やノウハウが十分でないため、IPv6 に対応した人材の育成・確保が大きな課題となっている。

このため、総務省は、2009年度から、民間のネットワーク運用者等の運用技術の向上を図り、IPv6 に対応した人材を育成・確保するため、実ネットワークレベルの複雑さを有した実験用 IPv6 ネットワークを備えた「IPv6 運用訓練センター」を整備する。

コ）モデルキャリア開発計画策定事業（経済産業省）

学生や若い技術者が自らのキャリアパスをイメージできるよう、専門家によるコミュニティを活用した情報セキュリティ人材を含めた高度 IT 人材の育成の職種ごとにモデルキャリア開発計画を策定し、これらを広報・普及する。また、専門家コミュニティの形成を促進し、若手専門家の育成等の支援に取り組む。

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

コンピュータウイルスや脆弱性などの情報セキュリティ上の問題に対する的確かつ実効的な対応を行うため、平時からの情報共有のための連絡体制の構築、主体間の連携強化が図られるための取組みを進める。また、事業継続性確保を強化するために企業における事業継続計画策定の促進を図るとともに、そのための事業継続計画策定ガイドラインの普及、改善の取組みを推進する。さらに、情報セキュリティ上の問題が発生した場合に迅速かつ実効的に対応を行うために必要な緊急時対応体制の強化を推進する。

【具体的施策】

ア）コンピュータセキュリティ早期警戒体制の強化（経済産業省）

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、2009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」を脅威の変化に対応可能な形で強化する。

具体的には、近時のコンピュータウイルス等の攻撃手法の巧妙化に対応するため、インシデント対応の調整支援を行う JPCERT/CC 等の組織において、攻撃手法の分析・解析能力の一層の高度化、専門家間での解析手法等に関する情報共有・連携を推進する。また、脅威の動向を踏まえた、効果的な社内インシデント対応演習の手法等に関する検討・実証、情報共有等を通じて各組織における情報セキュリティ上の問題への対応力の向上を図る。

イ）組織の緊急対応チームの普及、連携体制の強化（経済産業省）

情報セキュリティ上の問題が発生した場合に迅速かつ実効的に対応を行う緊急時対応体制の強化を推進するため、JPCERT/CC を中心として、CSIRT の構築・運用に関するマテリアルや、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、適切な者の間で共有するシステムの利用等により、2009年度において、CSIRT の普及や国内外の組織内 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。

ウ）制御システムに関する脆弱性への対応のための連携体制の構築（経済産

業省）【再掲】

制御システム製品に関しては、標準プロトコル（TCP/IP やイーサネット等）や汎用製品の導入が進むことにより、潜在的な脅威が高まることが想定される一方で、対策、ベストプラクティス等は整備段階にあり、開発／構築にたずさわる技術者における情報収集・評価の負担の増加が予想される。このため、2009年度においては、JPCERT/CCを事務局として2008年度に発足した「制御システムベンダーセキュリティ情報共有タスクフォース」の活動を本格化し、制御システムにおけるセキュリティ対策の推進に資する情報の収集、共有を推進することにより、制御システムに関する脆弱性等の脅威への対応の円滑化を図る。

エ）ソフトウェア等の脆弱性に係るマネジメントの支援等（経済産業省）【再掲】

IPA において、2008年度に開始した、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の運用を継続するとともに、機能強化を行う。

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や手法の普及促進及び改善を進めるとともに、ユーザー組織における対応コストの低減のためソフトウェア等の脆弱性に関する情報をマネジメントツールが自動的に取り込める形式で配信するサービスの提供を拡大する。

オ）標的型攻撃の手法解明と対策情報の提供（経済産業省）

IPA 及び JPCERT/CC において、標的型攻撃の検体の収集・分析を実施し、関係機関と連携しつつ、攻撃手法の解析、対策の策定を行うとともに、必要な情報提供を行う。

（オ） 中小企業の情報セキュリティ対策の推進

人員、予算、ITインフラなど、主にリソース不足から対策が遅れがちである中小企業の情報セキュリティ対策が促進されるよう、様々な対策の中から適切な対策を容易に選択できるような環境を整備する。例えば、適切な情報セキュリティレベルを測るために活用される情報セキュリティベンチマークを引き続き改善し、自社の情報セキュリティレベルを客観的評価として提示するための統一的なチェックリストの開発、普及を図る。

また、中小企業のセキュリティ対策を促進するためには、簡便かつ安価なセキュリティ対策ツールを提供するなどの効果的な取組みが必要であるため、SaaSやASPなどの活用の促進及びこれらサービス提供事業者における情報セキュリティ対策基準の提示・啓発などの取組みを行う。

さらに、中小企業の経営者、情報システム担当者等の情報セキュリティへの理解を深めるため、セミナーの開催など普及・啓発活動を推進し、情報セキュリティ対策の促進を図る。

【具体的施策】

ア）企業における高度な情報セキュリティが確保された情報システム投資に対する税制優遇措置（経済産業省及び総務省）【再掲】

2008年度税制改正により 2 年間延長・拡充された産業競争力のための情報基盤強化税制について、引き続き、その普及・啓発を図ることにより、企業における高度な情報セキュリティが確保された情報システム投資を促進する。

イ）中小企業における情報セキュリティ対策の推進（経済産業省）

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年度に作成した中小企業の情報セキュリティ対策ガイドラインの普及を行うとともに、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。

ウ）「SaaS向けSLAガイドライン」の活用・普及（経済産業省）【再掲】

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、SaaSの利用者と提供者の双方に広く活用・普及を推進する。

エ）情報セキュリティ対策を容易化するシステム等の開発（経済産業省）【再掲】

中小・小規模企業でも安価かつ容易に業務効率化を行える、インターネットを活用したソフトウェア提供サービス（SaaS）の基盤となるシステムや、その上で稼働するセキュリティ管理等のアプリケーションを開発する。

オ）情報セキュリティ監査知識を有する人材の育成（経済産業省）【再掲】

情報セキュリティ対策を組織の内部ならびに外部から客観的かつ公正に評価できる情報セキュリティ監査知識を有する人材の育成を行う。

カ）中小企業情報セキュリティ対策の促進（経済産業省）【再掲】

中小企業に指導する立場にある者を対象とした「中小企業情報セキュリティ指導者育成セミナー」において、情報セキュリティに関する知識等を習得させ、当該セミナーで習得した知識を基に、中小企業の経営者等に対して情報セキュリティ対策に係る普及啓発を図る。

キ）中小企業を対象とした情報セキュリティセミナー等の実施（経済産業省）【再掲】

2009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。地域中核団体との連携を強化するとともに、IT 経営応援隊と連携した普及広報活動を行う。

ク） 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、2009年度においても助成を行う。

（カ） 日系企業のグローバルな事業展開を支える情報セキュリティ政策の推進

我が国企業がグローバルな事業展開を行うにあたり、日本国外のビジネス拠点において情報セキュリティを確保するための取組みを推進する。例えば、アジアなど我が国企業の事業活動に関係の深い国や地域を念頭に、円滑なアウトソーシングを行える環境づくりや、セキュアなネットワーク環境の構築へ向けた国際連携・協力を推進する。

【具体的施策】

ア)アジア域内のセキュアなビジネス環境の構築推進（経済産業省）

2008年度にERIA（東アジア・アセアン経済研究センター）の下で実施したアジア共通の情報セキュリティ対策ベンチマークに関する政策研究を受け、2009年度においても、2008年の日・ASEAN経済大臣会合で我が国より提唱した「アジア知識経済化イニシアチブ」に基づき、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。また、アジア域内数ヶ国において、企業の情報セキュリティ対策に関するセミナー等の普及啓発活動や、人材育成に向けた取組を実施する。

イ)ソフトウェア開発のアウトソーシング先国におけるセキュアコーディングセミナーの実施（経済産業省）

JPCERT/CC を通じ、我が国企業が組込みソフトウェアの開発をアウトソーシングしている先の各国を中心に、脆弱性を作りこまないコーディング手法に関する技術セミナーを実施する。2009年度においては、ASEAN 地域 3 国程度においてセミナーを実施する。

ウ)海外における組織の緊急対応チームの構築・運用支援（経済産業省）

JPCERT/CC を通じ、我が国企業の事業活動に関係の深い国や地域を念頭に、組織内 CSIRTの構築・運用支援を行う。2009年度においては、アジア地

域において、CSIRT 構築セミナー等の普及・啓発、技術支援活動を行う。

④ 個人

「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標とし、政府は、2009年度には以下の施策を重点的に推進する。

（ア） 情報セキュリティ教育の強化・推進

ITの利用・活用には積極的であるものの、リスクの認識や情報セキュリティ対策の重要性の認識が必ずしも十分ではない児童・生徒や保護者への教育・啓発を推進する。こうした観点も踏まえつつ、学校や地域における情報モラル[14]等の教育を推進する。

また、消費者である個人が様々なサービス等の利用において生じ得るリスクを認識し、そのリスクを被害に変えないための環境を整備する。個人に対する啓発活動とともに、サービス提供事業者や対策支援主体によるリスク情報、対策情報の適切な提供、事故発生時の対応等の取組みを促進する。

【具体的施策】

ア）児童・生徒や保護者への教育・啓発の推進

a）メディアリテラシー向上のための調査・開発、啓発活動の展開（総務省）

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に必要なICTメディアリテラシー[15]の向上を図るため、メディアの特性に応じたリテラシーに関する教材の開発等について検討する。また、2008年度までに開発済みの教材（小学5，6年生を主な対象）についても引き続き公開し普及を図る。

b）「情報セキュリティ対策」標語・ポスターによる普及啓発（経済産業省）

IPA において、2009年度に、韓国情報保護振興院(KISA)との共同事業として、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。

c）e－ネットキャラバンの実施等（総務省及び文部科学省）

2008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。

イ）学校や地域等における情報モラル等の教育の推進

14 情報モラルとは、「情報社会で適正な活動を行うための基になる考え方と態度」（高等学校学習指導要領解説情報編）のこと。

15 「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。

a）若年層からの高度セキュリティ人材の育成（経済産業省）

2009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（1日）を行う。

b）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）

2008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。

c）サイバーセキュリティに関する講習の実施(警察庁)

2008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）リスク情報、対策情報の適切な提供、事故発生時の対応等の取組みの促進

a）Web脆弱性に関する学習・検証ツールの提供（経済産業省）

Web サイト運営者や製品開発者が脆弱性対策の必要性及び対策手法等を自ら学習することを支援するため、体験型の脆弱性学習・検証ツールの開発に着手する。

b）情報セキュリティに関する情報収集を支援するツール提供（経済産業省）

情報セキュリティに関する主要な Web ニュースサイト等の発信する RSS を収集・蓄積する「最新セキュリティ情報 Navi(セキュリティ情報 RSS ポータル)」を引き続き提供し、Web 等を通じた情報セキュリティ対策に関する情報収集を支援する。

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

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

また、ゼロデイ攻撃への対策として、Exploit コード 等の解析により脅威を分析し、ゼロデイ攻撃の自動検出を行うためのツール開発に着手する。

（イ） 個人の底上げに向けたより効果的な普及・啓発活動の実現

個人の底上げに向け、周知・啓発活動を、関係府省庁が更に連携し、より効果的に実施できるような取組みを進めていく。また、ITに関して必ずしも詳しくない個人を含めた一般利用者のセキュリティレベルを効果的に上げるために、質問への適切なアドバイスや訪問対応を行えるサポータの育成、地域団体ネットワークの実現を促進する。

【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、２００９年度に、「@police」、「国民のための情報セキュリティサイト」、「インターネット安全教室」「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）

２００８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）サイバー犯罪の被害防止対策の推進（警察庁）

２００９年度において、サイバー犯罪被害防止のためのパンフレット等や出会い系サイトに関連した犯罪の被害防止のための中学生・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、これらのパンフレット等のほか、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やサイバー犯罪の手口やその対応策を警察庁ウェブサイトに掲載するなどの広報啓発を実施する。

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）

２００９年6月の電波利用環境保護周知啓発強化期間において、関係省庁の協力を受け、「電波のルールを守りましょう」をキャッチフレーズに「技術基

準適合マーク」の確認を促すなどの電波利用ルールの重要性について各種メディア（全国紙・地方紙・業界専門誌、TVCM、電車・バス車内吊り広告、地方公共団体・関係機関等へのポスター配布・掲示、リーフレットの配布、各種広報紙への掲載等）により周知啓発を実施予定。

さらに、２００９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」の確認についてインターネット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）

昨年に引き続き、「情報通信における安心安全推進協議会」において、「情報通信の安心安全な利用のための標語」の募集を行い、最優秀作（総務大臣賞）を含む作品の選定・表彰を実施予定。

f)無線LANのセキュリティ対策（総務省及び経済産業省）

２００９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。

g)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）【再掲】

２００８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。

h)ｅーネットキャラバンの実施等（総務省及び文部科学省）【再掲】

２００８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。

i)情報セキュリティ・サポーターの育成（総務省）【再掲】

情報セキュリティに関する教材作成や講習会・認定試験の開催を支援することにより、利用者の身の回りの詳しい人（情報セキュリティ・サポーター）を育成し、国民全体の情報セキュリティの底上げを行う。

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、２００９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の表彰（総務省及び経済産業省）

２００９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、２００９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、SJ２００９の英語版等を示すこととする。

（ウ） 対策が困難な個人も含めた情報セキュリティ水準向上に向けた取組み

対策の必要性を認識していても対策を実施しない個人など、対策が困難な個人を含めた情報セキュリティ水準の向上のためには、対策支援主体による取組みが必要不可欠である。このため、迷惑メール対策の強化や電気通信事業者が予防的措置として実施する情報セキュリティ対策の利用促進などの取組みを促進する。

【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）マルウェア配布等危害サイト回避システムの実証実験（総務省）
　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、電気通信事業者等と連携して、ユーザーがマルウェア等配布する悪性サイトへアクセスするのを回避する仕組みの実証実験を行う。

ウ）e－ネットキャラバンの実施等（総務省及び文部科学省）【再掲】
　2008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。

エ）スパムメール対策の強化（総務省及び経済産業省）【再掲】
　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応するため、2008年の法改正によりオプトイン方式が導入された特定電子メール法及び特定商取引法の着実な執行等所用の措置を講じる。
　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、日本に着信するスパムメールの大部分を占める海外から発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塔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。

（2） 横断的な情報セキュリティ基盤の強化と発展

① 情報セキュリティ技術戦略の推進

　我が国の情報セキュリティ関連技術の研究開発が、世界で最も効果的・効率的に進められる体制となることを目標とし、政府は、2009年度には以下の施策に重点的に推進する。

（ア） 情報セキュリティ技術開発の重点化と多様性の維持

基盤としてのITの強化、および国民が安心してITを利用できるような環境の実現を目標とした、研究開発・技術開発を重点的に促進する。経済環境が厳しさを増す中で、ITを利用して生産性向上を図ることと、その分野における将来にわたる主導的かつ優位な地位を確保するという視点を持って、研究開発・技術開発を推進することが、従来以上に求められる。具体的には、利用者に対策への過度の負担を強いない、事前に情報セキュリティ対策が埋め込まれた、安全・安心な機器の実現や利用者環境の提供を、重点的に取り組むべき課題として取組みを推進する。

一方で、研究開発・技術開発の多様性を確保するため、市場として成立していないために企業が取り組まない分野や将来的なリスクに対抗するための先行的な開発、開発コストが巨大な分野、および基礎研究など、我が国として戦略的に維持すべき分野に対しては、政府が積極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2008年度に引き続き実施する。

b)セキュアクラウドネットワーキング技術の研究開発（総務省）

2013年度までに、安全性・信頼性の高いクラウドサービスを誰でも利用可能とするための先導的技術を確立することを目標として、NGN の積極活用や異なるクラウド間の連携等を実現するセキュアクラウドネットワーキング技術の研究開発を実施する。

c)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[16]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、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。

d)経路ハイジャックの検知・回復・予防に関する研究開発（総務省）

2009年度末までに、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、2009年度も引き続き、経路ハイジャックの検知・回復・予

16 「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。

防に関する研究開発を推進する。

e)情報通信分野における情報セキュリティ技術に関する研究開発（総務省）

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。

f)新世代の情報セキュリティ技術の研究開発（経済産業省）

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生活の生命・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として、ゼロデイ脆弱性対策技術開発、開発段階で脆弱性検出することを目指したフォーマルメソッド適用可能性研究、組込システムの脆弱性検出技術開発等を2009年度に実施する。

g)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2008年度に引き続き実施する。

h)情報処理基盤の安全性等の確保（マルウェア検体の活用方法の検討）（経済産業省）

IPA の保有するマルウェア検体及び検体分析結果等の活用方法を検討する。

i)情報通信構成要素の安全性検証技術の高度化に関する研究開発（総務省）

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、2008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。

j)システムLSIのセキュリティ評価体制の整備（経済産業省）【再掲】

2011年度までに、IC カード等に用いられるシステム LSI について、国内で ISO/IEC15408 に基づくセキュリティ評価が行えるよう必要な体制整備を行う。

k)新世代ネットワーク基盤技術に関する研究開発（総務省）

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。2009年は、2008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。

l)セキュアでグリーンなクラウドコンピューティング環境の整備（経済産業省）

経営・事業戦略に柔軟に対応できる伸縮自在で高効率・高信頼な情報システムを、 企業や官公庁といったビジネスシーンでユーザーが安心・安全に利用できるよう、 クラウドコンピューティングに係る省エネ、セキュリティ及び安定した稼働を確保する信頼性向上に関する技術等についての研究開発を行う。

m）ソフトウェア構築状況の可視化技術の開発普及（文部科学省）

「事故前提社会」への対応力強化として、ソフトウェアに対するトレーサビリティの概念を普及させ、世界最高水準の安心・安全なIT社会を実現するため、オフショアを含むマルチベンダによるソフトウェア開発に関する実証的データ(エンピリカルデータ)を収集し、ソフトウェア開発が適正な手順で行われたかどうかをソフトウェア発注者によって把握・検証可能とする「ソフトウェアタグ」をソフトウェア製品に添付して提供する技術を2012年3月までに開発する。

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さらに適切な分析の方法を検討する。

b)高セキュリティ機能を実現する次世代OS環境の評価及び性能向上（内閣官房、内閣府、総務省及び経済産業省）【再掲】

2008年度にプロトタイプ版の開発が完了した「セキュアVM」の内閣官房での試用及び政府機関内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。また、産学官の連携により、セキュアVMの性能向上及び利用環境の拡大を図る。

c）IP 化されたネットワークにおける重要通信の高度化の推進（総務省）

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、重要通信の高度化の在り方に関する研究会の報告（2008年5月）等を踏まえ、関係事業者と重要通信の取扱いを実現するために不可欠な情報の共有や共通課題の検討を行い、必要な施策を実施する。

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

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、これまでの成果を踏まえ、最終年度である2009年度も引き続き行っていく。

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が必要である。2009年度においては、特に技術開発領域に対する投資対効果の精度を高めるための手法の見直しについて検討する。

（イ）「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、喫緊の対応が必要でありながら対策が十分でない課題や、中長期的な視野で抜本的な技術革新等の実現が求められる課題が存在する。これらの対策が困難な課題に対応するため、「グランドチャレンジ型」の研究開発・技術開発を推進する。

喫緊の課題の解決に向けては、要素技術の統合化・実装化で迅速な対応を図る。また、既に開発済みであっても、制度や教育が追いついてないなどの理由から技術成果が利用されていない場合があり、組織・人間系の管理手法の高度化や利用者の啓発と並行して、統合的な対策を推進することが有効となる。

中長期的な研究開発の推進のためには、将来の社会像を予測し、そこで必要となる情報セキュリティ技術を検討することで、研究開発・技術開発テーマの開拓を行なう。具体的には、設計段階から製品にセキュリティを作り込むための手法の確立や、開発ノウハウの蓄積は短期的に実現できるものではなく、また多くの知見を集約する必要があるため、中長期的なビジョンと実施体制、および支援環境をもって当たることが望ましい。

【具体的施策】

ア)「グランドチャレンジ型」のテーマ及び推進の枠組み検討（内閣官房、内閣

府、警察庁、総務省、文部科学省、経済産業省及び防衛省）

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、2009年度では、プロジェクトのより詳細なテーマ及びグランドチャレンジ型研究を推進するための枠組みについて、検討を実施する。

（ウ） 研究開発・技術開発の効率的な実施体制の構築と基盤の整備

国が支援するプロジェクトにおいては、その投資効果を最大化するために、研究開発・技術開発の計画策定時にプロジェクトの途中で得られた成果を活用する手順（プロセス）を組み込むとともに、プロジェクトの内容および実施状況の公開を促進する。また、情報セキュリティを取りまく環境の移り変わりが激しい中で、社会情勢変化や技術革新の影響を評価し、必要性が高い場合には計画変更が可能な、柔軟なプロジェクト管理の仕組みを導入し、新たな脅威への迅速な対応を可能とする。

さらに、直接的な研究開発・技術開発の取組みに加え、情報セキュリティ分野の特殊性にかんがみ、研究開発支援の環境整備を官民の連携によって積極的に推進する。具体的には、リスクの表記法や評価方式の共通化、情報セキュリティに関するデータベースの整備と共有、及び隔離ワークベンチ[17]の構築などによって、研究開発の支援と加速を図る。

【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2008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2008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）公的な競争的資金制度におけるプロジェクト管理・評価の検討（内閣官房、内閣府及び関係省庁）

研究開発プロジェクトについて、開発期間中の新たな状況変化に応じた柔軟な計画変更を可能とするとともに、研究開発の中間成果の利用を促進するための制度の改善を検討する。

エ）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）

17 マルウェアなどを実際に動作させて研究を行うための、ネット環境を模した実験設備。現実のインターネットからは隔離されており、マルウェアは物理的に封じ込められている。

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2009年度も引き続き行う。

オ)小規模攻撃再現テストベッド・マルウェア隔離解析テストベッド等の構築（総務省）

サイバー攻撃の解明と対策技術の検証を行うためのテストベッドを構築し、高度化・巧妙化が進むサイバー攻撃・マルウェアの解析能力・対策技術の高度化を推進する。

② 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重要性が社会で十分に認識され、その業務が魅力的なものとして、優秀な人材が官民問わず情報セキュリティ分野にすすんで集まることを目標とし、政府は、2009年度には以下の施策を重点的に推進する。

（ア） 政府機関における人材の育成・確保及び職員の意識啓発（再掲）

政府機関における情報セキュリティ関連業務を調査・検証し、これらの業務に携わる人材に必要とされるスキルをまとめる。

各政府機関においては、まとめられたスキルを踏まえ、情報セキュリティ対策に関わる内部人材の教育や確保・登用等に係る具体的な計画を、「行政機関におけるIT人材の育成・確保指針」[18]に基づき作成した「IT人材育成・確保実行計画」に明記し、それを推進する。

また、各政府機関においては、セキュリティ対策に係る民間専門家の活用を促進するため、最高情報セキュリティアドバイザーやそのサポートスタッフの活用などの戦略的なアウトソーシングを進めるほか、任期付き採用制度などの積極的な活用を図る。

各政府機関においては、官民人事交流制度の活用による人材育成の促進のほか、階層別研修に情報セキュリティに関する内容を盛り込むなど、幹部職員も含めた全職員の情報セキュリティに関する意識の向上方策を、人事担当部門と情報システム部門の密接な協力の下に推進する。

【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）【再掲】

内閣官房及び総務省は、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、その質の向上等の充実を図る。

イ)情報セキュリティ関連業務の調査等（内閣官房）【再掲】

18 ２００７年４月１３日　各府省情報化統括責任者（ＣＩＯ）連絡会議決定。

内閣官房は、府省庁における情報セキュリティ関連業務を調査・検証し、これらの業務に携わる人材に必要とされるスキルをまとめる。

ウ)人材育成・確保実行計画の実施(全府省庁)【再掲】

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。

エ)民間専門家の活用の促進(全府省庁)【再掲】

各府省庁においては、セキュリティ対策に係る民間専門家の活用を促進するため、最高情報セキュリティアドバイザーやそのサポートスタッフの活用などの戦略的なアウトソーシングを進めるほか、任期付き採用制度などの積極的な活用を図る。

オ)政府職員の人材育成の促進(全府省庁)【再掲】

各府省庁においては、官民人事交流制度の活用による人材育成の促進のほか、階層別研修に情報セキュリティに関する内容を盛り込むなど、幹部職員も含めた全職員の情報セキュリティに関する意識の向上方策を、人事担当部門と情報システム部門の密接な協力の下に推進する。

カ)情報システム及び暗号モジュールの評価技術の向上(経済産業省)

IPA において、セキュリティ LSI 等を用いたシステムの安全性評価体制の構築及び、次世代の暗号モジュール試験関連規格に対応するため、セキュリティ LSI に対するサイドチャネル攻撃を含む耐タンパー性評価を行うための人材の育成を行う。

（イ） 企業における情報セキュリティ人材の育成・確保(再掲)

経営層の情報セキュリティ対策への理解増進とともに、企業の情報セキュリティ対策の推進を担う人材の育成・確保が必要不可欠であることから、人材育成に向けたセミナー開催等の広報啓発を推進する。また、対策においては、新たなITの利用・活用など、環境の進化に柔軟に対応できる人材や企業のマネジメント全体を俯瞰した上で判断できるスキルを持った人材などの育成・確保も必要不可欠である。その際には、情報セキュリティ人材の目指すキャリアパスを考慮に入れることも重要である。こうしたことを踏まえ、官民の適切な役割分担のもと、客観的な人材評価メカニズムである各スキル標準の整合化を図った共通キャリア・スキルフレームワークとそれに準拠した情報処理技術者試験の活用、及び民間の人材育成に関するフレームワークや各種資格試験の活用を促進する。また、産学連携による高度情報セキュリティ人材を育成するためのカリキュラム整備や教員強化、インターンシップの充実等に取り組むための体制を整備する。

また、技術者向けの情報セキュリティに係るモデルキャリア開発計画の策定や専門家コミュニティへの支援を進めることで、広く企業の情報セキュリティを担うことのできる人材の育成・確保に取り組む。

さらに、今後の課題となるNGN／IPv6への移行などの新しい環境への移行に対応できる実践的な情報セキュリティ人材や法令遵守、情報資産や事業継続等に関するリスクを特定しつつ、情報セキュリティ対策を実践できる人材の育成を推進する。

【具体的施策】

ア)情報通信人材研修事業支援制度（総務省）【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、2009年度においても助成を行う。

イ）情報セキュリティ・サポーターの育成（総務省）【再掲】

情報セキュリティに関する教材作成や講習会・認定試験の開催を支援することにより、利用者の身の回りの詳しい人（情報セキュリティ・サポーター）を育成し、国民全体の情報セキュリティの底上げを行う。

ウ）先導的ITスペシャリスト育成推進プログラム（文部科学省）

2009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。

エ）情報セキュリティ監査知識を有する人材の育成（経済産業省）【再掲】

情報セキュリティ対策を組織の内部ならびに外部から客観的かつ公正に評価できる情報セキュリティ監査知識を有する人材の育成を行う。

オ）情報処理技術者試験の更なる普及（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種情報分野の人材スキルを測る情報処理技術者試験を共通キャリア・スキルフレームワークに基づく見直しを行い、2009年度から実施する。当該試験合格者が多数輩出されることにより、共通キャリア・スキルフレームワークに基づいた適切な人材評価手法による効果的なキャリアパスが形成されることが期待され、当該試験を活用した人材育成を図る。

カ）モデルキャリア開発計画策定事業（経済産業省）【再掲】

学生や若い技術者が自らのキャリアパスをイメージできるよう、専門家によるコミュニティを活用した情報セキュリティ人材を含めた高度 IT 人材の育成の職種ごとにモデルキャリア開発計画を策定し、これらを広報・普及する。また、専門家コミュニティの形成を促進し、若手専門家の育成等の支援に取り組む。

キ）産学連携IT人材育成実行事業（経済産業省）【再掲】

情報セキュリティ人材を含めた高度 IT 人材の育成のため、産業界出身教員等の充実・強化、実践的な教材・カリキュラムの開発・普及、産学マッチングによる実践的なインターンシップなどを推進するための産学連携体制を強化する。

ク）中小企業情報セキュリティ対策の促進（経済産業省）【再掲】

中小企業に指導する立場にある者を対象とした「中小企業情報セキュリティ指導者育成セミナー」において、情報セキュリティに関する知識等を習得させ、当該セミナーで習得した知識を基に、中小企業の経営者等に対して情報セキュリティ対策に係る普及啓発を図る。

ケ）中小企業を対象とした情報セキュリティセミナー等の実施（経済産業省）【再掲】

2009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。地域中核団体との連携を強化するとともに、IT 経営応援隊と連携した普及広報活動を行う。

コ）民間のセキュリティ資格の周知（内閣官房、総務省及び経済産業省）【再掲】

民間における情報セキュリティ専門家の充実の観点から、民間の情報セキュリティに関する資格の周知を行う。

（ウ） 情報セキュリティ人材が保有するスキルの見える化の推進

情報セキュリティ分野に人材を集め、高い能力を有する人材に支えられた情報セキュリティを構築するためには、長期的な視点から、情報セキュリティ人材が自らの能力を高めることが業務に結びつくようにし、人材の側からキャリアパスを描くことができるようにすることが有効である。

このため、実際の業務において求められるスキルを明確にするとともに、人材が保有するスキルが外部からわかりやすくするための政策を実施する。例としては、情報セキュリティ資格制度・教育制度と業務において求められるスキルや情報セキュリティ人材の目指すキャリアパスの関係を見えやすくするための取組みや、共通キャリア・スキルフレームワーク：ITSS[19]や民間の人材育成における各種有効なフレームワークの活用により、保有するスキルを外部に

19 ＩＴスキル標準（Information Technology Skill Standards）の略。

明示できる仕組みを構築する取組みが挙げられる。

【具体的施策】

ア）共通キャリア・スキルフレームワークの普及（経済産業省）

産業構造審議会情報経済分科会情報サービス・ソフトウェア小委員会人材育成ワーキンググループ報告書(平成19年7月20日）において、客観的な高度 IT 人材評価メカニズムの構築が提言され、平成20年10月に IT 技術者の体系的な評価手法である IT スキル標準、組み込みスキル標準、ユーザースキル標準の整合化を図り、情報処理技術者試験と準拠した「共通キャリア・スキルフレームワーク」を構築したところ。今後、当該フレームワークの更なる普及を促進することによって、高度セキュリティ人材の育成を図る。

イ）情報処理技術者試験の更なる普及（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種情報分野の人材スキルを測る情報処理技術者試験を共通キャリア・スキルフレームワークに基づく見直しを行い、2009年度から実施する。当該試験合格者が多数輩出されることにより、共通キャリア・スキルフレームワークに基づいた適切な人材評価手法による効果的なキャリアパスが形成されることが期待され、当該試験を活用した人材育成を図る。

ウ)モデルキャリア開発計画策定事業（経済産業省）【再掲】

学生や若い技術者が自らのキャリアパスをイメージできるよう、専門家によるコミュニティを活用した情報セキュリティ人材を含めた高度 IT 人材の育成の職種ごとにモデルキャリア開発計画を策定し、これらを広報・普及する。また、専門家コミュニティの形成を促進し、若手専門家の育成等の支援に取り組む。

エ)産学連携IT人材育成実行事業（経済産業省）【再掲】

情報セキュリティ人材を含めた高度 IT 人材の育成のため、産業界出身教員等の充実・強化、実践的な教材・カリキュラムの開発・普及、産学マッチングによる実践的なインターンシップなどを推進するための産学連携体制を強化する。

オ)民間のセキュリティ資格の周知（内閣官房、総務省及び経済産業省）【再掲】

民間における情報セキュリティ専門家の充実の観点から、民間の情報セキュリティに関する資格の周知を行う。

③ 国際連携・協調の推進

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

（ア） 情報セキュリティ政策に関するPOC機能の強化と情報共有の促進

第1次基本計画に引き続き、NISCは様々な国際機関やフォーラムにおいて、情報セキュリティ政策を横断的に取り扱うPOCとしての役割を明確化する努力を継続し、その機能を強化することを目指す。

具体的には、三つの観点からの取組みを行う。第一に、国家安全保障、重要情報インフラ防護、グローバルな経済活動の継続性確保、サイバー犯罪防止等の様々な観点から議論が行われる情報セキュリティ関連の国際会合等の機会に、最新の動向の把握・収集をより強力に進める。そのためには、信頼（Trust）の醸成及び顔の見える貢献が必要であることから、これらの国際会合等を機会横断的に把握・収集する機能を強化する。第二に、高い信頼関係を通じて把握・収集した動向については、国内の必要な関係機関・関係者に適切に共有されることで、初めて意味あるものとなる。このことを十分に踏まえ、NISCはPOCとして、国内の政府関係機関に対して、適切なルールに基づいた共有を進め、政府関係機関の政策立案・実施への意味ある貢献を目指す。第三に、グローバルにITを安全・安心に利用できる環境を構築する観点から、我が国の動向について、必要かつ適切なものについては、POCを通じて公式に発信することで、世界に貢献することを目指す。

【具体的施策】

ア）多国間の枠組み等における国際連携・協力の推進（内閣官房及び関係府省庁）

2009年度も引き続き、内閣官房は、ARF (ASEAN Regional Forum)等の国家安全保障に係る分野、MERIDIAN 等の重要情報インフラ防護に係る分野、FIRST(Forum for Incident Response and Security Teams)等のインシデント対応に係る分野、APEC (Asia Pacific Economy Cooperation) 、OECD (The Organizations for Economic Cooperation and Development) 、ASEAN (Association of South Easit Asia)等のグローバルな経済活動に係る分野等の様々な分野の国際会合に積極的に参加し、POC 機能として情報発信を行うとともに、会合で得られた成果について、関係省庁・諸機関との積極的な情報共有を行う。

イ）情報セキュリティに関する国際会合の開催（内閣官房及び関係府省庁）【再掲】

世界的規模で行われるサイバー演習（Cyber Storm III)への参加に向けて、各国の重要インフラ防護政策、緊急対応チーム及び法執行機関等の専門家が参加する国際監視・警戒ネットワーク（IWWN）会合招致に向けた活動を行う。

ウ）情報セキュリティ政策に関する二国間政策対話の強化（内閣官房及び関係府省庁）

情報セキュリティ政策における地域間の緊密な連携を構築するため、日米のサイバーセキュリティ二国間会合の2009年度における実施のほか、戦略的二国間連携を強化するため、新たな情報交換の場の創設に向けた検討を行う。

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

サイバー空間の安全・安心の確保に向けて、政府にとどまらず、国家レベルのCSIRT[20]、ISP[21]や様々な企業内のCSIRT、研究機関等の主体も、従来から緊密な国際連携を進めてきている。このような状況を踏まえ、政府は、特に強みを発揮できる分野に注力する。また、世界の脅威動向の把握やインシデントへの対応をはじめとする情報セキュリティ関連の国際的な活動に関して、我が国全体として、効率的・効果的に進めるための官民連携体制を構築する。これによって、既に活動を行っている国内の関係機関と、国際連携活動における補完・共助の関係を築くことを目指す。

具体的には三つの観点から取組みを行う。第一に、日本政府が持つ官民連携体制について海外に積極的に発信し、国際連携に関する官民の役割分担を明確化する。第二に、官民連携を通じて、我が国から発信が可能な情報を明確化するための国内の連携強化を行う。第三に、諸外国の政府内外機関との信頼関係を向上し、情報共有を加速するため、国際的な情報共有に係る考え方を整理する。

なお、上述の政府が特に強みを発揮できる分野としては、従来から諸外国政府機関等との間で進めてきた最新の政策動向に関する意見交換に加え、例えば、政府機関、重要インフラに関係の深い脅威や脆弱性等のリスク情報の共有、政府機関、重要インフラ分野におけるインシデント対応の国際的な連携体制構築が考えられる。その際には、関係機関等による既存の国際的な活動を活用しつつ進めることとする。

【具体的施策】

ア）国内関係機関との連携強化(内閣官房)

国際的な情報セキュリティ政策動向を国内に情報提供し、共有するため、国内関係機関との連携を強化する。

イ）国際的な情報共有ルール整備に向けた検討（内閣官房及び関係府省庁）

グローバルな脅威動向を把握するための国際的な枠組みへの積極的参加や二国間の対話を通じて、情報共有に関するルール作りに向けた検討を開始する。

ウ）海外の CSIRT の体制強化の支援（経済産業省）

20 Computer Security Incident Response Team の略。

21 Internet Service Provider の略。

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。2009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、FIRST（Forum of Incident Response and Security Teams）、IWWN や APCERT における活動、及び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等を通じ、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。

特に2009年度においては、6月にFIRST会合が京都で開催されることから、この機会を利用して、来日する海外メンバチームとの間の一層の連携の強化を図る。

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）

2009年度も継続的に、日中韓における情報通信ネットワークのセキュリティ確保に関する取組みを通じて、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）日・ASEAN におけるネットワークオペレータ間の情報共有の促進（総務省）

2009年度においては、我が国のネットワークオペレータ間連携によって培われた知見や経験について、ASEAN 加盟国のネットワークオペレータとの間で共有を図り、日・ASEAN 間におけるネットワークオペレータ間の情報共有を促進する。

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

不正アクセス、フィッシング、スパム、標的型攻撃、ウェブサイトからのマルウェアの感染等の脅威は、国境を越えて生じると同時に、地理的、文化的、政治的に関係の深い地域においてある程度共通の特徴が存在する。したがって、既に欧州地域内や、米国を中心とする地域において象徴的に見られるように、地域内における連携が行われるようになってきている。このような状況を踏まえ、我が国は、アジアにおける脅威に対応し、情報セキュリティ対策の強化のための連携を推進するべく、以下の取組みを実現することを目指す。

取組みは、三つの観点から行う。第一に、人のつながりの必要性を認識し、アジアにおける脅威動向の把握・分析を我が国とともに行う専門家・研究者を積極的に養成する。第二に、現在、国際機関や国際フォーラム等で議論されているアジアにおける共同の脅威動向の把握機能創設のための取組みに対し、我が国にとっても大きなメリットのある形で支援を行う。第三に、我が国は第1次基本計画期間中に構築した米国、欧州との連携を更に強化し、ベストプラクティスの共有や共同の取組みを通じて得られた教訓、情報をアジア地域に積極的に還元していく。

なお、取組みの推進に際しては、効率性を重視し、既存の枠組みを最大限活用するとともに、関係機関と連携することとする。

【具体的施策】

ア）日・ASEAN におけるネットワークセキュリティ分野の研究協力の推進（総務省）

2009年度においては、我が国と ASEAN 加盟国との間でのネットワークセキュリティ分野における研究協力に関する検討を開始する。

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）

2009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、本格運用への移行及び各参加国間での共同解析に着手する。

また、2008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、2009年度は、配信対象地域の拡大及び双方向化を進める。

ウ）アジア地域における攻撃手法の分析能力の強化及び分析結果情報の共有の促進（経済産業省）

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、地域特性等を分析し、分析手法や分析結果の共有方法について検討を進める。

具体的には、2009年度において、アジア地域の CSIRT を中心とするメンバ間で、 共同で、又は連携して、検討を進める。

エ)アジア地域における情報セキュリティ評価・認証技術向上のための取組み（経済産業省）

IPA が主体となって、アジアにおける評価・認証技術の向上、各種情報の共有化等を図るため、日本、韓国、シンガポール、マレーシア等による AISEC(Asian IT Security Evaluation and Certification) Forum を設立し、第 1 回会合を日本で開催する（平成21年5月予定）

（エ） 経済活動のグローバル化に対応した情報セキュリティの確保

政府は、日系企業のグローバルな経済活動の安全・安心を確保するためのビジネス環境構築に向けた取組みを行う。すなわち、海外のビジネス拠点において重要な情報資産が確実に守られ、高い事業継続性が確保されることを目指す。

具体的には、第一に、日系企業の事業活動に係る海外拠点において、高い水準の情報

セキュリティ対策が実現されるような体制の構築を目指す。第二に、可用性の確保された、信頼性の高いネットワーク環境の構築を目指す。第三に、IT製品・サービスについて、グローバル化を阻害しない形で、製造過程のサプライチェーン全体を通じて一貫したセキュリティ、信頼性を確保するための取組みの国内外における推進を目指す。このような取組みは、情報セキュリティの面でも品質の高い我が国の製品・サービスの国際競争力の向上に資することとなる。

政府は、特に関係の深い地域との間で直接議論を行う場を活用するとともに、後発の国・地域に対して積極的に支援を行う国際機関への積極的な関与等を通じ、取組みを進める。

【具体的施策】

ア）日・ASEAN 情報セキュリティ政策会議合意内容の着実な実施（内閣官房、総務省、経済産業省）

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、経済活動・技術革新を支える情報通信インフラの信頼性の確保、政府による横断的な情報セキュリティ政策の立案に向けた取組みを加速化するため、第１回日・ASEAN 情報セキュリティ政策会議の合意内容の着実な実施に向けた取組みを実施する。

イ）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）【再掲】

2008年度にERIA（東アジア・アセアン経済研究センター）の下で実施したアジア共通の情報セキュリティ対策ベンチマークに関する政策研究を受け、2009年度においても、2008年の日・ASEAN経済大臣会合で我が国より提唱した「アジア知識経済化イニシアチブ」に基づき、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。また、アジア域内数ヶ国において、企業の情報セキュリティ対策に関するセミナー等の普及啓発活動や、人材育成に向けた取組みを実施する。

ウ）ソフトウェア開発のアウトソーシング先国におけるセキュアコーディングセミナーの実施（経済産業省）【再掲】

JPCERT/CC を通じ、我が国企業が組込みソフトウェアの開発をアウトソーシングしている先の各国を中心に、脆弱性を作りこまないコーディング手法に関する技術セミナーを実施する。2009年度においては、ASEAN 地域 3 国においてセミナーを実施する。

エ）情報処理技術者試験及び IT スキル標準の国際展開（経済産業省）

情報処理技術者試験については、アジア11ヶ国・地域と相互認証を行っている。特に、我が国の情報処理技術者試験制度を移入し、試験制度を創設した

国（フィリピン、ベトナム、タイ、ミャンマー、マレーシア、モンゴル）が協力して試験を実施するための協議会であるITPEC（IT Professional Examination Council）では、同日、同一時刻においてアジア統一試験を実施している。今後、ITPEC各国における試験合格者の適正な能力評価手法を構築させるため、我が国のITスキル標準を普及させることによって、アジアでの更なるセキュリティ人材の育成を図る。

（オ） 標準化を含んだ我が国の戦略的貢献の実現

情報セキュリティ対策に係る統一的な基準作りや標準化は、従来から様々な国際機関で行われている。近年、標準化の取組みは、従来のような技術的な領域のみならず、政策的な領域についても行われている。議論は多岐にわたり、情報セキュリティの分野に限定しても、幅広い活動の中から政府が全ての活動に関与することは非常に困難な状況となっている。一方で、我が国からは、標準化には数多くの企業を含めた関係機関が継続的な参加・貢献を通じて個別に行っている。

国際機関を通じた国際貢献には、海外の関係者との継続的な関係の構築が不可欠であるため、政府は、標準化の取組みに参画し関係を構築している国内の関係機関、企業等と連携しながら、国際機関におけるガイドラインの策定や標準化の動向を把握し、我が国が戦略的に貢献できる体制を整備することを目指す。

【具体的施策】

ア）電気通信事業における情報セキュリティマネジメントの強化（総務省）

電気通信分野の情報セキュリティマネジメントについて、2006年度から2008年度にかけて、国際電気通信連合(ITU : International Telecommunications Union)及び国際標準化機構（ISO : International Organization for Standardization）に対して第 3 章第1節②に掲載のガイドライン（ISM-TG）について提案を行い、国際規格化に主導的な役割を果たした。2009年度は、ITU及びISOにおける議論の動向を踏まえ、要求事項の国際規格化につとめ、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。

イ）情報セキュリティ分野での国際標準化への参画（経済産業省）

情報セキュリティ分野の国際標準化活動であるISO/IEC JTC 1/SC27 等が主催する国際会合等に参加し、我が国のIT環境・基準・ガイドライン等を踏まえて国際規格への反映が行われるよう積極的に参画する。

（カ） 情報セキュリティ文化の醸成

情報セキュリティ文化の醸成は、第1次基本計画においても、目的の一つとして掲げられている。近年、情報システム、インターネットの分野と関係の深い国際機関における議論を通じ、意識も国際的に高まってきている状況である。

真の情報セキュリティ文化の醸成のためには、企業における経営者の意識向上が必要であることと同様、世界の政府ハイレベルの認識の共有を通じた取組みが必要であることを認識し、政府は、諸外国の政府機関と協力しながら、G8、APEC等のハイレベルの場を活用した取組みを目指す。

このような共通認識の醸成を通じ、インシデント発生時のオペレーションによる連携のみならず、ハイレベルからのメッセージを発出することができる環境の構築を目指す。

以下に、国際連携・協調の推進に向けた取組みの各種施策の俯瞰図を示す。

分野	リージョナル	グローバル
政策	（ウ）アジアにおける知恵の結集と情報セキュリティ水準の向上（One-Asia の実現） （エ）経済活動のグローバル化に対応した情報セキュリティの確保	（エ）経済活動のグローバル化に対応した情報セキュリティの確保 （カ） 情報セキュリティ文化の醸成
オペレーション	（ウ）アジアにおける知恵の結集と情報セキュリティ水準の向上（One-Asia の実現）	（イ）世界の脅威動向を把握するための官民連携の確立と、効率的・効果的な国際連携活動の推進
標準化	（オ） 標準化を含んだ我が国の戦略的貢献の実現	

（注）（ア）の施策については、全ての政策実施の前提となるため、ここに掲載されていない。

【具体的施策】

ア）我が国の情報セキュリティ戦略に関する国際的な広報活動の推進（内閣官房）

情報セキュリティ先進国として、我が国における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行う。SJ2009 は英語版を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掲載する。

イ）多国間会合を通じた情報セキュリティ政策に関する途上国の底上げ支援（内閣官房及び関係府省庁）

多国間会合の場を通じ、途上国における情報セキュリティ政策の底上げを図るため、サイバーセキュリティの国家戦略や重要情報インフラ防護に関する基本計画の策定支援、国際的な意識向上に向けた取組を2009年度以降も積極的に実施していく。

ウ)ITU－Dを活用した国際協力の推進（総務省、内閣官房）

2009年度においては、ITU-D（国際電気通信連合 電気通信開発部門）を通じて途上国における情報通信ネットワークの安全に関する政策の策定支援を

実施する。

エ)APT 研修・セミナー等の開催（総務省）

アジア・太平洋電気通信共同体（APT=Asia-Pacific Telecommunity）への我が国からの特別拠出金により、2009年度に、APT 加盟国の政府関係者及び電気通信事業者等を対象とした情報セキュリティ研修を実施予定。

オ)国際的なセキュリティ文化実現及び意識・リテラシー向上のための取組み（内閣官房）

OECD における「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」で定義されている「セキュリティ文化」をめぐる国際的議論の動向などを踏まえつつ、国内外の場で、セキュリティ文化醸成に貢献する。同時に政策対話等の場を通じて、諸外国との間で情報セキュリティ意識・リテラシー向上のための方策について議論を深める。

④ 犯罪の取締り及び権利利益の保護・救済

サイバー空間が安全にかつ安心して利用できるものとすることを目標とし、政府は、2009年度には以下の施策を重点的に推進する。

（ア） 犯罪取締りのための基盤整備の推進

法執行機関における取締り体制の強化、技能の向上、国際協調の推進等の基盤強化を一層推進する。

さらに、原因特定や犯行過程解明に不可欠な情報提供がなされ、被疑者の検挙や被害の拡大防止につなげられるよう、法執行機関と被害者等との間の良好な協力関係の構築を一層推進するなど、犯罪に強いIT社会構築のための官民連携に向けた取組みを推進する。

また、サイバーテロに対しても、その特性を考慮した上記の取組みにより備えを強化する。

【具体的施策】

ア）サイバー犯罪の取締りのための態勢の強化（警察庁）

2009年度において、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積極的に実施するとともに、サイバー犯罪の取締りを行うための車両の整備を推進するなど、サイバー犯罪に適切に対処するための態勢を強化する。

イ）デジタルフォレンジック[22]に係る取組みの推進（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、2009 年度において、サイバー犯罪捜査に従事する警察職員に対する研修の実施、資機材の増強、デジタルフォレンジック連絡会の開催等を通じた国内関係機関との連携、技術協力を始めとした官民連携等、デジタルフォレンジックに係る体制等の強化を推進する。

ウ）サイバー犯罪の取締りのための国際連携の推進（警察庁）

2009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。

エ)中央当局制度[23]を活用した国際捜査共助の迅速化（法務省）

中央当局を設置し，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，日韓及び日中間の二国間における刑事共助条約が既に発効しており，日・香港間においても，平成20年5月23日，刑事共助協定の署名が行われた。2009年度においては，同協定及び日露間の刑事共助条約（平成20年5月に実質合意済み）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，EU（欧州連合），ブラジル及びアジア諸国との間における刑事共助条約の早期締結に向けた作業を進める。

オ)サイバー犯罪に適切に対処するための法整備等の推進（法務省）

近年における情報処理の高度化の状況等にかんがみ，サイバー犯罪に適切に対処すべく，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）。）。

カ)サイバー空間の安全と秩序を維持するための民間との連携強化（警察庁）

サイバー犯罪に適切に対処するための官民の連携を強化するため、各都道府県警察におけるインターネットカフェ連絡協議会の設立等の取組みを推進す

---

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。

23 「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う制度を指す。

る。

キ)犯罪に強い IT 社会構築のための官民連携に向けた取組みの推進(警察庁)

有識者、関連事業者、PTA の代表者等で構成する総合セキュリティ対策会議を開催し、情報セキュリティに関する産業界と政府の連携の在り方について検討する。

ク)サイバーテロ対策に係る体制等の強化(警察庁)

2009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等に対応するため、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、緊急対処を行うための資機材の強化等、警察におけるサイバーテロ対策に係る体制等の強化を推進する。

ケ)重要インフラに対するサイバーテロ対策に係る官民の連携強化(警察庁)

2009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。

コ)重要無線通信妨害対策の強化(総務省)

・電波監視体制充実・強化3カ年計画に基づき、重要無線通信妨害事案の発生時の対応強化のため、重要無線通信妨害申告受付体制の強化を含む電波監視体制の充実を実施する。
・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21年度 DERUAS センサ16式等の整備を実施予定。
・アップリンク干渉源特定機能の実用化に向け宇宙電波監視施設の機能・性能向上及び電波監視施設の高度化・高機能化のため、広帯域監視技術等の調査研究を実施予定。

(イ) 犯罪抑止のための広報啓発の推進

国民がサイバー犯罪の被害者とならないよう、犯罪の被害状況や手口、具体的な対策の方法等に関する広報啓発を一層推進する。

【具体的施策】

ア)サイバー犯罪の被害防止対策の推進(警察庁)【再掲】

2009年度において、サイバー犯罪被害防止のためのパンフレット等や出会い系サイトに関連した犯罪の被害防止のための中学生・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、これらのパンフレット等のほか、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やサイバー犯罪の手口やその対応策を警察庁ウェブサイトに掲載するなどの広報啓発を実施する。

イ)犯罪抑止のための広報啓発の推進(警察庁)

2009年度において、警察庁セキュリティポータルサイト「@police」において、各種ソフトウェアに係る脆弱性情報、インターネット定点観測情報等の情報セキュリティ関連情報を情勢の変化に応じて適切に提供するなど、犯罪抑止のための広報啓発活動を推進する。

ウ)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)【再掲】

2008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。

(ウ) 権利利益の保護・救済のための基盤整備の推進

国民の基本的人権に十分配慮しつつ、サイバー空間の権利利益の保護・救済のための基盤の更なる整備に努める。具体的には、情報を預ける側の権利利益を情報を預かる側が保護・救済する取組みに係る情報開示の促進、サイバー空間の安全性・信頼性を向上させる技術の開発・普及などに取り組む。

【具体的施策】

ア)プロバイダ責任制限法及び関係ガイドラインの周知の促進(総務省)

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。

イ) 情報セキュリティ報告書の策定・公表の推進 (経済産業省)

広く国民から預託された情報を取り扱う企業における情報管理や法令遵守等の取組みに関する情報が国民にわかりやすく比較可能な形で開示されることにより、企業における適切な情報管理・情報漏えい防止対策を促進し、情報を預ける国民の権利利益の保護に資するため、情報セキュリティ報告書モデルの普及を図る。

第4章　政策の推進体制と持続的改善の構造について

政府は、2009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）の強化と役割

NISCは、第1次基本計画の下での取組みと同様、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引き続き目指す。また、横断的な情報セキュリティ問題に関する国際POCとしての役割を十分に果たせるよう引き続き強化を図る。

さらに、NISCは、情報セキュリティに関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るとともに、柔軟に、政府内の人材を最大限活用し、その能力の維持・強化を図る。また、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も引き続き目指す。

本基本計画の内容からも明らかなように、情報セキュリティ政策の政策領域は多岐にわたる。このため、NISCは関連領域を担当する様々な機関との結節点となるとともに、課題ごとに解決に向けた関係機関の連携体制の最適化を柔軟に進め、情報セキュリティに関連する課題に対する我が国全体としての解決能力の最大化を実現するために、率先して活動に取り組む。

【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、第3章第1節（1）①[政府機関]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。重要インフラ領域に関する対策としては、第2次行動計画等に従って、第3章第1節（1）②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、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） 各府省庁の強化と役割

各府省庁は、引き続き、情報セキュリティ政策会議、NISCを中核とした、情報セキュリティ政策を推進する枠組みの下、自府省庁の情報セキュリティ政策及び関連領域に係る体制の充実・強化を図る。体制の充実・強化にあたっては、必要に応じて民間の人材の積極的な活用を含め、有効な方策を柔軟にかつ最大限活用する。そして、推進体制が縦割りにならないよう十分に留意しながら、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、各種政策の実施に引き続き努める。

【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）

2009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）

2009年度に、IPA において、情報セキュリティ対策を推進するためのリスクや、リスクに対する人間の行動・投資などについて調査及び社会科学的分析を行う。また、国内関連機関等との共催によるワークショップの開催等を通じ、コストや対策の成果、社会システムにおける対策行動の位置づけなどを明らかにする。

（3） 状況の変化の適時適切な把握と新しい課題への対応

情報セキュリティ分野は、脅威や技術など、様々な側面において変化が早い。このため、刻々と変化する状況を適時適切に把握するとともに、新たに生起する課題に対して迅速かつ的確な対応を行うことが重要となる。また、新たにトレンドとなる政策手法についても適切な検討を進めることが不可欠である。さらに、情報提供主体を対象とした新たな取組みを進めることも必要である。

このため、NISCをはじめとする様々な関係機関・関係者が連携し、また情報セキュリティ政策会議の下に適宜設置される専門委員会も活用し、法律、技術、啓発など政策に係る幅広い視点全般から、検討を動的にかつ柔軟に進める体制を強化する。

【具体的施策】

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

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処が必要である。

このため、2010年3月末までに「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。

第2節　　他の関係機関等との関係

第2次基本計画は、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、第1次基本計画同様、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、第2次基本計画が「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、総務省行政管理局とは行政情報システムに関連する取組みを中心に連携を更に強化することが不可欠である。

中央防災会議との関係においては、情報セキュリティ政策のうち重要インフラ関連部分について必要な連携を行うことが必要である。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。さらに、国民生活審議会との関係においては、個人情報保護等の観点から、情報を提供する側の主体に係る取組みを進めるにあたって十分な連携を確保する必要がある。

情報セキュリティ政策会議及びNISCは、これらの会議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）

2009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、2009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、その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、第1次基本計画の下での取組みに続き、以下のような持続的改善のための構造を活用する。

（1）「年度計画」の策定とその評価等

政府は、第2次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（セキュア・ジャパン20XX）」として策定するとともに、その実施状況を社会情勢の変化とともに評価し、結果を公表する。また、補完調査を必要に応じて実施し、この結果も併せて、「20XX年度の情報セキュリティ政策の評価等」として公表する。この取組みに当たっては、詳細を情報セキュリティ政策の評価等の枠組み文書によって定められた枠組みにのっとることとする。

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行う。

【具体的施策】

ア）評価等[24]の実施及び公表（内閣官房）

24　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

SJ2009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)重要インフラ領域の情報セキュリティ対策の年度毎の成果検証等の実施(内閣官房及び重要インフラ所管省庁)

重要インフラ領域の情報セキュリティ対策の評価については、第2次行動計画に基づき、重要インフラ所管省庁の協力を得て、対策の成果検証、施策の成果検証、補完調査をそれぞれ実施する。また、同計画に指標が示されたものについて、これをとりまとめて公表する。

(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 SJ2009 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) 評価指標の改善

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、情報セキュリティ政策の枠組み文書によって設定されているところ、政府は、同枠組み文書に定めた方法により、今後も引き続き評価指標の改善を図る[25]。

【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改善(内閣官房、総務省及び経済産業省)

2009年度中に確立する評価指標に基づき、各対策実施領域(政府機関、地

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。

25 なお、重要インフラの領域については第２次行動計画において先行的に評価指標の改善を行っているため、同枠組み文書における評価指標の改善に際しては、第２次行動計画における評価指標を基本として検討することとする。

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。

（4） 第2次情報セキュリティ基本計画の見直し

政府は、第2次基本計画について、3年後に見直しを行うとともに、環境変化が生じた場合には、期間中であっても見直しを行うこととする。

【具体的施策】

ア）第2次情報セキュリティ基本計画の見直し（内閣官房）

政府は、第2次基本計画について、環境変化が生じた場合には、期間中であっても見直しを行うこととする。

第5章　2010年度に喫緊に取り組むべき課題

～2010年度の重点「すべての主体の協働による情報セキュリティ対策の強力な推進を」～

第3章及び第4章では、3箇年計画である第2次基本計画の初年度として、**「すべての主体に事故前提の自覚を」**との思想を重点とし、2009年度に実施すべき具体的施策を掲げてきた。この取組みは、あらゆる主体が情報セキュリティ問題への取り組みの重要性についての共通の認識の下、自らの責任を自覚しながら、それぞれの立場に応じた適切な役割分担の下で対策を実施することを目指した「新しい官民連携モデル」の実現に向けた取組みを、「事故前提社会」や「合理性に裏付けられたアプローチ」等の新しい要素を加えたものに進化させることを意図したものである。

第2章第2節に示したように、我が国が「成熟した情報セキュリティ先進国」へと成長するためには、「自覚」→「協働」→「成熟」といった「個」と「社会」の成長プロセスが必要となる。2009年度は新しいステージの第 1 歩に過ぎず、今後、取組みを強力に推進していくことが求められる。そのためには、「新しい官民連携モデル」の考え方が示すように、それぞれの主体が情報セキュリティ対策の重要性を自覚し、自発的に取組みを行うことに加え、それぞれの立場に応じ、適切な役割分担の下で対策を実施することが必要である。

このような各主体の「連携」や「協働」により取組みを進めることによって、2009年度に着手した取組みが効果を発揮し始めるとともに、第1次基本計画から継続的に実施している取組みの効果も高めることが可能となる。このようなことから、第2次基本計画における2年目となる2010年度は、第2章第1節に示した今後3年間の取組みの方向性を基本としつつ、**「すべての主体の協働による情報セキュリティ対策の強力な推進を」**との思想を重点として、特に、以下の方向性で施策の推進を図ることとする。

［官民における人的基盤・体制整備に向けた取組み］

便利で安心して利用できる電子政府の推進、サイバー攻撃やサイバー犯罪への的確な対応、企業等における情報セキュリティガバナンス確立の促進、民間における情報セキュリティ向上など、第2次基本計画において取り組むべき課題は多岐にわたる。

各対策実施主体が具体的な取組みを推進する上で、情報セキュリティに関する知見を有した人材

の育成・確保や情報セキュリティ対策推進のための体制整備は不可欠である。

政府では、すべての情報セキュリティ対策推進の基礎となる人的基盤や推進体制の整備に関し検討を進めるとともに、以下の施策を重点として官民における取組みを推進する。

【具体的施策】

ア)情報セキュリティガバナンスの確立に向けた取組(全府省庁)

各府省庁は、2009年度に策定した情報セキュリティガバナンスの確立を図るための体制の整備方針に基づく取組を推進する。特に、最高情報セキュリティ責任者を補佐する専門的知見を有する最高情報セキュリティアドバイザーを設置するとともにそのスタッフとなる人材の確保に取り組む。

イ)情報セキュリティ報告書(試行版)の作成等(内閣官房及び全府省庁)

各府省庁は、2009年度に策定された情報セキュリティ報告書作成のためのガイドラインを踏まえ、情報セキュリティ報告書(試行版)を作成する。その際、情報セキュリティ報告書の客観性を確保する観点から、最高情報セキュリティアドバイザーがその作成に参画するほか、外部監査制度の活用についても、導入可能な府省庁においては積極的に推進する。また、作成した情報セキュリティ報告書は、最高情報セキュリティアドバイザー連絡会議(仮称)において、比較・評価等を行うとともに、それらを通じて得られた知見の共有やフィードバックを図り、最高情報セキュリティ責任者が、情報セキュリティ政策会議の下に設置されている「情報セキュリティ対策推進会議」等の場において報告する。

ウ) 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)

内閣官房及び総務省は、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、その質の向上等の充実を図る。

エ)サイバー攻撃等に対する政府機関における緊急対応能力の強化(内閣官房)

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、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一層の向上、効果的な取組みを図るための方策について検討を行う。

オ)情報セキュリティガバナンスの確立の促進（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を推進するため、ガイドライン等の普及を引き続き継続する。特に中小企業について、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強化を図る。

カ)情報セキュリティ・サポーターの活用(総務省)

民間における情報セキュリティ向上のための活動を支援し、利用者の身の回りの詳しい人（情報セキュリティ・サポーター）を活用することにより、国民全体の情報セキュリティの底上げを図る。

キ）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。

ク）サイバー犯罪取締りのためのデジタルフォレンジックに係る取組みの推進（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、サイバー犯罪捜査に従事する警察職員に対する研修を始めとした体制等の強化を推進する。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。

[国際連携・協調のための取組み]

国際連携・協調に関しては、2009年 2 月に、内閣官房、総務省及び経済産業省の連携により、日・ASEAN 情報セキュリティ政策会議を開催し、アジア域内のセキュアなビジネス環境の構築等を始め、アジアにおける情報セキュリティ政策に関する連携強化に向けた取組みを本格化させたところである。

このような取組みは中長期にわたり積み重ねることで効果を発揮するものであることから、2010年

度においても、引き続き、以下の施策を重点として官民における取組みを推進する。

【具体的施策】

ア）情報セキュリティ政策に係る国際会合の開催（内閣官房、総務省、経済産業省）

2009年2月に開催された日・ASEAN 情報セキュリティ政策会議での合意を踏まえ、情報セキュリティ政策について、各国の成功事例を共有し、連携強化に向けた施策を議論するための会議を2011年中に日本で開催するための準備を進める。

イ）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）

「アジア知識経済化イニシアティブ」に基づき、アジア諸国におけるセキュアな投資・ビジネス環境を構築するための更なる具体的な推進策について検討する。

[官民による技術の研究開発及び導入の推進]

各対策実施主体による情報セキュリティ対策をより効果的に、かつ、より容易に行えるようにする上で、技術の研究開発や導入の推進は不可欠である。

研究開発には中長期の取組みと、各種知見の結集が必要であることから、以下の施策を重点として官民における取組みを推進する。

【具体的施策】

ア）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。

イ）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。

ウ）組込システム等のセキュリティ及び信頼性確保のための体制整備等（経済産業省）

情報システムやIT製品などの組込システム等のセキュリティ及び信頼性の取組強化に向けた技術開発や環境の整備を行う。

エ)産学官連携による新たな情報環境におけるセキュリティ対策の検討(総務省)

クラウドコンピューティングのような新技術が普及していく中で、情報漏えい等の情報セキュリティ脅威の拡がりにより新技術の普及が阻害されることがないよう、技術開発や人材育成等のセキュリティ対策を検討する。