セキュア・ジャパン2006

－「セキュア・ジャパン」への第1歩－

情報セキュリティ政策会議

2006年6月15日

目次

第1章　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
～2006年度の重点「官民における情報セキュリティ対策の体制の構築」～ 1
第2章　対策実施4領域における情報セキュリティ対策の強化 4
第1節　政府機関・地方公共団体 4
第2節　重要インフラ 14
第3節　企業 19
第4節　個人 23
第3章　横断的な情報セキュリティ基盤の形成 28
第1節　情報セキュリティ技術戦略の推進 28
第2節　情報セキュリティ人材の育成・確保 32
第3節　国際連携・協調の推進 33
第4節　犯罪の取締り及び権利利益の保護・救済 36
第4章　政策の推進体制と持続的改善の構造 39
第1節　政策の推進体制 39
第2節　他の関係機関等との連携 40
第3節　持続的改善構造の構築 41
第5章　2007年度の重点施策の方向性
～2007年度の重点「官民における情報セキュリティ対策の底上げ」～ 43
第1節　模範となる領域の情報セキュリティ対策の底上げ 43
第2節　取組みが遅れがちな主体の対策の底上げ 46
第3節　横断的な情報セキュリティ基盤の底上げ 47

第1章　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

～2006 年度の重点「官民における情報セキュリティ対策の体制の構築」～

IT は我が国の国民生活・社会経済活動を豊かにしてきた。そして、今後も我が国だけでなく世界も一層豊かにするものと期待されている。しかしながら、IT が我が国の国民生活・社会経済活動に深く浸透していくに伴い、IT の利用自体が国民生活・社会経済活動の安全・安心を脅かす事態が発生してきている。このような事態に対する対策を抜本的に強化すべく、官民における統一的・横断的な情報セキュリティ対策を推進するために策定されたのが、我が国の情報セキュリティ対策に係る中長期の戦略である「第1次情報セキュリティ基本計画」（2006年2月2日情報セキュリティ政策会議決定、以下「基本計画」という。）である。

この「セキュア・ジャパン2006」は、基本計画を受け、2006年度における我が国の情報セキュリティ対策の政府の重点施策と2007年度における重点施策の方向性を定めるものである。

2005年に発生した情報セキュリティ問題としては、政府機関の Web サーバへのサイバー攻撃、ファイル共有ソフトの利用やコンピュータウイルス等に起因する情報漏洩、社会的に影響が大きい重要インフラの IT 障害による業務停止、スパイウェアの作成・利用による不正アクセス・預金詐欺等のサイバー犯罪等が挙げられ、これらの問題による IT の利用・活用自体に対する不安が増大してきている。しかしながら、これまでの我が国の情報セキュリティ対策への取組みは政府機関・地方公共団体、重要インフラ、企業、個人といった個々の主体によって、バラバラに行われてきたところであり、全体としても不十分なものであった。

そこで、2006年度は、まず、「セキュア・ジャパン」実現に向けての第一歩として、**「官民における情報セキュリティ対策の体制の構築」**を重点とし、基本計画に掲げられている4つの基本方針について、以下のとおり推進することとする。

（1）官民各主体の共通認識の形成

個々の主体における情報セキュリティを確保するためには、それぞれの主体による、それぞれの行動原理に沿った自律的な取組みが重要である。この自律的な取組みを促進するためには、それぞれが「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を形成することが必要である。

これらのことを踏まえ具体的に官民各主体の共通認識の形成を行うためには、各主体が情報セキュリティ対策への参加意識を持つこと、各主体が情報セキュリティ対策について考え共通認識の形成に参加すること、各主体が積極的に情報セキュリティ対策を行い他の者にも働きかけを行うことが必要である。

よって、政府は、2006年度においては、まず、**「すべての主体に情報セキュリティ対策への参加意識を持たせること」**を重点目標とし、政府一体となって各種施策を推進することとする。

（2）先進的技術の追求

急速に拡大するITの利用・活用に対応し、次から次へと発生する新しい情報セキュリティの脅威に、対症療法的ではなく対応するためには、常に最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策を推進していくことが必要である。

この際、1）単一の技術や単一の基盤に依存することのリスクを認知し、その改善に取り組むこと、2）既存の基盤に対する技術的な解決方法に加え、ビルトイン型の情報セキュリティ機能を持ったそもそもの基盤自体を新たに構築する観点から、IPv6（Internet Protocol version 6）の導入や、さらなる研究開発・技術開発を行うことが重要である。

これらのことを踏まえ具体的に先進的技術の追求を行うためには、情報セキュリティへの脅威を明確にすること、追求すべき先進的技術の領域を特定し資源を計画的に重点投資すること、すでに存在する先進的技術については積極的に導入を図ることが必要である。

よって、政府は、2006年度においては、**「先進的技術の追求に係る取組みを政府全体として一定の方向性を持って行うこと」**を重点目標とし、各種施策を推進することとする。

（3）公的対応能力の強化

我が国が、「情報セキュリティ先進国」としての強みを比較優位にまで高めていくためには、1）公的部門が国内外及び官民における「ベストプラクティス（模範例）」を積極活用した対策を実行する等の率先した対策を行っていくこと、そして同時に、2）多様性を持った社会基盤の構築や、3）ITの利用・活用の拡大によって新たな脅威が発生していることを踏まえた、国防の強化や犯罪やテロへの対抗力、災害対策の強化等、広く物理的脅威も視野に入れながら、安全保障・危機管理的な側面からの取組みを推進する等、公的部門の対応能力を戦略的に強化していくことが必要である。

一方で、公的部門の対応能力を強化していく際には、人権保障や、公的部門の活動の透明性や適法性の確保に、常に留意し続けることが必須である。

これらのことを踏まえ具体的に公的対応能力の強化を行うためには、公的部門の情報セキュリティ対策のレベルを高める仕組みを構築・運用すること、公的部門の事案対処能力を向上させること、官民における必要な連絡体制を構築・訓練することが必要である。

よって、政府は、2006年度においては、まず、**「公的部門の情報セキュリティ対策のレベルを高める仕組み及び官民における必要な連絡体制を構築すること」**を重点目標とし、各種施策を推進することとする。

（4）連携・協調の推進

官民の各主体が連携しながら「新しい官民連携モデル」を構築していくためには、国内における官民の各主体の連携・協調を図り、その英知を結集した取組みを行うことが必要である。

加えて、世界一のブロードバンド大国となった我が国が直面する問題は、他国がこれから直面する問題であり、世界のトップランナーとして、問題解決の責任があることにかんがみ、国際協調・貢献の取組みも不可欠である。この際、情報セキュリティ対策を実施する者が評価される仕組みの導入等を通じ、我が国が生み出した成果を他国が再利用可能な形としてまとめ、情報セキュリティの 「ジャパンモデル」 として提示することも必要である。

また、ITの基盤は、24時間・365日、常時世界と繋がっていることを常に意識した国際的に責任のある取組みを行うことが必要である。

よって、政府は、2006年度においては、すべての主体の取組みが連携・協調の下行われることを確保すべく、**「すべての主体による情報セキュリティ対策に係る情報共有体制を構築すること」**を重点目標とし、各種施策を推進することとする。

第2章　対策実施4領域における情報セキュリティ対策の強化

本セキュア・ジャパン2006においては、基本計画と同様に、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[1]のレベルを世界最高水準のものとし、かつ、2）2009年度初めにはすべての政府機関において政府機関統一基準が求める水準の対策を実施していることを目指し、政府は、2006年度に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

a）政府機関統一基準の見直し（内閣官房）

技術や環境の変化を踏まえ、2006年度に政府機関統一基準の見直しを行う。

イ）PDCA サイクルの確立

[1] 「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。

a）各政府機関での PDCA サイクルの確立（全府省庁）

政府機関統一基準を踏まえた省庁基準に基づき、情報セキュリティ対策の実施のため、具体的な実施手順の整備、情報セキュリティ対策の実施状況の自己点検及び監査等を行い、2006年度に PDCA サイクルを確立する。

また、2006年度に、各府省庁において全職員に対する講習を行い、省庁基準及び実施手順等の遵守を徹底させる。

b）政府全体での PDCA サイクルの確立（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、必要な範囲で検査・評価し、勧告を通じた各府省庁の対策の改善と政府機関統一基準等の改善に結びつけることで、2006年度に政府全体としてのPDCAサイクルを確立する。

c）評価及び結果の公表（内閣官房）

2006年度上半期中に、政府機関統一基準に基づき、重点項目等を対象に行う検査について、試行的評価を実施するとともに、2006年度中に、海外の評価手法等も参考にしつつ、政府全体としての PDCA サイクルを確立するにあたり有効であり、かつ、客観的に比較可能な形での本格的評価の手法の確立を図る。

また、評価の結果については、情報セキュリティの維持・確保にも配慮しつつ公表することとする。

ウ）実施手順の作成支援及び技術的情報の提供と情報の共有（内閣官房）

内閣官房は、各府省庁の情報セキュリティ対策の推進を支援するため、実施手順の作成支援及び技術的な情報の提供を行う。なお、これらの情報については、民間企業、地方公共団体、独立行政法人にとっても、「ベストプラクティス（模範例）」として実効的に活用できるよう、各府省庁の活用実態を反映した改良を加え、2006年度から順次公開及び普及に努める。

エ）コンピュータウイルスなどに起因する情報流出への対応（全府省庁）

ファイル交換ソフトウェア等を介して感染するコンピュータウイルスなどに起因する情報流出を防止するため、2006年度に、政府機関統一基準に基づき、各府省庁において情報の外部持ち出し及び私物パソコンの業務使用に関して厳格な管理を行うなど情報管理を徹底する。

オ）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）

2006年度に、外部委託先の候補者における情報セキュリティ対策の水準を確認するため、必要に応じて、政府調達における選定基準の一要素として情報セキュリティマネジメントシステム適合性評価制度及び情報セキュリティ対策ベンチマークを活用する。

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）

2006年度に、外部委託先の情報セキュリティ対策レベルを適切に評価・確認するため、必要に応じて、国際規格に準拠した管理基準に基づく情報セキュリティ監査制度の活用を図る。

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

経済社会のインフラとなっている情報システムの不具合が、国民に多大な影響を及ぼす事態が発生していることを受け、産業構造審議会（情報経済分科会情報サービス・ソフトウェア小委員会）において、全ての情報システムを対象として、開発運用等のプロセス管理の側面、技術的側面、組織的側面等の総合的観点から、情報システムの信頼性向上の方策を定めた「情報システムの信頼性向上に関するガイドライン」が2006年6月に策定されるところ、2006年度においては、同ガイドラインの政府機関における活用・普及の可能性およびその方策について検討する。

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（内閣官房及び全府省庁）

2006年度に、独立行政法人等の情報セキュリティポリシーの整備状況を調査する。その結果を踏まえ、独立行政法人等については、政府機関統一基準を参考に、情報セキュリティポリシーの策定・見直しを促進する。

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）

2006年度に、独立行政法人等の組織、業務形態等を踏まえ、情報セキュリティ

ポリシーを適用する上での課題等を抽出し、必要となる情報を提供するなど、情報セキュリティ対策の改善に向けた環境を整備する。

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、2006年度に、内閣官房と CIO 補佐官等の連携を強化し、対象システムの開発において効率的な情報セキュリティ機能の実装を推進する。

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）

安全性・信頼性の高い情報システムを構築するため、2006年度に、IT製品等を調達する際には、政府機関統一基準に基づきITセキュリティ評価及び認証制度[2]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

[2] 「ITセキュリティ評価及び認証制度」とは、IT 製品・システムについて、そのセキュリティ機能や目標とするセキュリティ保証レベルを、情報セキュリティの国際標準 ISO/IEC 15408 に基づいて第三者が評価し、結果を公的に検証し、公開する制度を指す。

にするため、原則として2008年度までに、各府省の情報システムの新たな開発（導入）又は更改に合わせて、情報通信機器やソフトウェアのIPv6対応化を図る。

【具体的施策】

ア）次世代の電子政府構築に向けた検討枠組み構築（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・整備に必要な技術的、機能的検討を行うための枠組みを2006年度に構築する。

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

2006年度において、ITの信頼性確保のための喫緊な取組みとして、現在のOSやアプリケーション等の利用環境を維持しつつ、これに依存しない形で情報セキュリティ機能を集約的に提供することのできる仮想機械（VM：Virtual Machine）機能及びこれを稼働させるための最小限のOS機能（これらの機能を併せて「セキュアVM」と呼ぶ。）の開発を、産学官の連携により推進する。

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

2006年度中に、電子政府に係る情報システムを構成するOSについて、そのOSのセキュリティ品質に係る評価尺度の確立に向けた検討を行い、システム調達時に活用可能な評価項目群及び各項目についての評価尺度の確立を図る。また、本格的な電子政府運用開始に向けたOS等システム導入における技術動向調査を2006年度に実施する。

エ）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）総務省は、2006年度前半に、電子政府システムにおけるIPv6ネットワーク整備に向けたガイドラインを策定する。

2）各府省庁は、上記ガイドラインに基づき各電子政府システムにおけるIPv6

対応化による効果を検討し、原則として2006年度末までに、各情報システムにおけるIPv6対応化の具体的な計画を策定する。

3）電子申請等の国民からのアクセスもIPv6で行えるようにするためには、インターネットサービスプロバイダが個人ユーザーに対してIPv6接続サービスを提供することが必要であることから、2006年度より、総務省はインターネットサービスプロバイダにおけるIPv6接続サービス提供状況についてホームページで情報提供する。

オ）電子政府認証ガイドラインの策定（内閣官房、総務省及び経済産業省）

各府省庁の電子行政サービスが独自に手段を決定している電子認証について、リスクに応じた認証強度のレベルを整理、明確化し、行政サービス間の連携を安全性を保ちつつ推進するため「電子政府認証ガイドライン（仮称）」を2006年度に策定する。

（ウ）政府機関への成りすましの防止

悪意の第三者が政府機関に成りすまし、一般国民や民間企業等に害を及ぼすことが無いよう、正統な政府機関であることを容易に確認可能とするため、電子証明書の広範な活用や、政府機関のドメインであることが保証されるドメイン名[3]の利用を推進する。

【具体的施策】

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

政府機関のドメイン名であることが保証されるドメイン名を利用していないサイトについては、原則として2006年9月までに、同ドメイン名の利用を開始する。

また、政府機関のドメイン名であることが保証されるドメイン名を用いることについて、各府省庁は国民に対し広く周知を行う。

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

[3] 「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。

用できる環境の整備、具体的には電子署名を付すための政府内情報システムの共通仕様の検討を2006年度に開始する。

（エ）政府機関における安全な暗号利用の促進

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

【具体的施策】

ア）政府機関で利用する暗号の安全性等確保（総務省及び経済産業省）

電子政府推奨暗号の監視、電子政府推奨暗号の安全性及び信頼性確保のための調査、研究、基準の作成等を2006年度に行う。

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

電子政府推奨暗号について、その危殆化が発生した際の取扱い手順及び実施体制の検討を進めるとともに、電子政府推奨暗号のあり方の見直し等を含めた暗号利用に関する政府内の推進体制について、2006年度に検討を開始する。

ウ）安全性・信頼性の高い暗号モジュールの利用推進（経済産業省）

安全性の高い暗号モジュール[4]の活用を推進するため、独立行政法人情報処理推進機構の運用するITセキュリティ評価及び認証制度を拡充等し、暗号モジュールの認証に係る枠組みを新たに整備するとともに、2006年度に試行運用を開始する。

エ）ファイル（電磁的記録）のセキュリティ対策の推進（防衛庁）

2006年度において、可搬記憶媒体へのファイル書き出し時のセキュリティ確保の観点から、ファイル秘匿化ソフトウェアの製作・導入を推進する。

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

4 「暗号モジュール」とは、各種暗号化機能を実装したハードウェア、ソフトウェア、ファームウェア及びその組み合わせ製品を指す。

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）情報収集、分析・解析機能の強化（内閣官房）

政府機関に対するサイバー攻撃、政府機関における情報漏洩や情報システムの障害等の発生を防止し、発生した場合には迅速かつ的確に対応するための横断的な情報収集機能及び攻撃等の分析・解析機能を強化すべく、2006年度において、各政府機関のWebサーバ等の監視を試行的に開始するとともに、国内外の関係機関と連携した攻撃等の横断的分析・解析機能（「官民連携分析・解析スキーム」（仮称）」を構築する。

その際、様々な機関で研究が進められた最新技術の有効活用を図る。

b）各政府機関への助言機能、相互連携促進機能の強化（内閣官房）

各政府機関におけるIT障害の防止及び対応に資するため、2006年度において、上記 a）の分析・解析結果に基づく各政府機関への助言機能を強化するとともに、各政府機関相互での対策情報の交換等を促進するための総合調整を行う。この際、各政府機関に連絡・対応の結節点としての「リエゾン（連絡要員）」を任命し、定期的に情報交換のためのミーティングを開催する。

c）情報保証に係る最新技術動向等の調査研究（防衛庁）

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

イ）各政府機関における緊急対処能力の強化

a）各政府機関における緊急対応体制の構築（内閣官房）

2006年度中に、各政府機関におけるIT障害の発生時に迅速かつ的確に対応できる各政府機関における初動対処要領を作成するともに、この体制に従事する要員の訓練の仕様のひな形を作成する。

b）サイバーテロ対策に係る体制等の強化・整備（警察庁）

2006年度において、サイバーテロの手段となり得るサイバー攻撃手法の高度化に対応するため、サイバーテロ対策要員の事案対処能力・技術力の維持、向上のための部内外における研修の実施等、警察におけるサイバーテロ対策に係る体制等を強化・整備する。

c）サイバー攻撃等に係る分析・対処及び研究の推進（防衛庁）

2006年度において、昨今の高度化するサイバー攻撃手法に鑑み、防衛庁の保有する情報システムに対するサイバー攻撃等に関する分析・対処能力をさらに向上させる必要性から、不正アクセス監視・分析技術、サイバー攻撃分析技術及びアクティブ防御技術等について基礎的な研究を実施する。

⑤政府機関における人材育成

政府として情報セキュリティ対策を一体的に進めていくために、必要な知見や専門性を有する人材を育成・確保することが重要であることにかんがみ、政府機関における情報システム管理部門の担当職員の育成、情報セキュリティに関する専門性の高い人材の活用、教育機関と連携した人材育成の取組み、幹部職員・一般職員の意識の向上方策等を推進する。なお、政府機関の情報システム管理部門において、情報セキュリティ対策業務に携わる専門的職員については、全員が情報セキュリティに関する資格を保有することを目指す。

【具体的施策】

ア）政府職員の人材育成に係る検討（内閣官房及び全府省庁）

政府として情報セキュリティ対策を一体的に進めていくための政府職員の人材育成について検討し、政府全体として戦略的に人材育成を行うための基本方針及び具体策を2006年度に示す。

イ）緊急対応能力に係る人材育成手法の検討（内閣官房）

IT障害への緊急対応に係るノウハウを収集し、各政府機関の人材育成へ反映させる方法について検討し、政府全体として戦略的に人材面での緊急対応能力強化を推進するための基本方針及び具体策を2006年度中に策定する。

ウ）情報セキュリティに関する資格保有率向上に係る検討（内閣官房及び全府省庁）

政府機関の情報システム管理部門における、情報処理技術者試験等の資格保有状況等について調査するとともに方向性について検討し、資格保有率の向上に資する具体策を2006年度に示す。

イ 地方公共団体

地方公共団体について、1）2006年9月を目処に地方公共団体における情報セキュリティ確保に係るガイドラインの見直しを行うとともに、情報セキュリティ監査や研

修等の対策を推進すること、また、2）2006年度末までに地方公共団体間の情報共有体制が整備されることを目指し、政府は、2006年度に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ポリシーの策定・見直しの促進（総務省）

地方公共団体における情報セキュリティ確保に係るガイドラインの見直しを、2006年9月を目処に行うとともに、各地方公共団体における当該ガイドライン等を踏まえた対策の実施を推進する。

イ）情報セキュリティレベル評価ツールの提供（総務省）

2006年度に、各地方公共団体が、自らの情報セキュリティレベルを客観的に評価し、適切な達成目標を定め、計画的、段階的に個人情報保護・情報セキュリティ対策に取り組むことのできる評価ツールを地方公共団体に提供する。

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、2006年度において、情報セキュリティ監査の実施を推進する。

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）「自治体情報共有・分析センター」（仮称）の創設促進及び運営支援（総務省）

地方公共団体におけるIT障害の未然防止、拡大防止及び再発防止並びに IT障害からの迅速な復旧に資するとともに、地方公共団体全体の情報セキュリティレベル向上を図るため、地方公共団体における情報セキュリティに関する情報の収集、分析、共有や政府等から提供される情報等の共有等を行う機能を有する「自治体情報共有・分析センター」（仮称）について、実証実験等を行い、2006年度末までの整備を推進するとともに、運営に必要な支援を行う。

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）地方公共団体における個人情報保護・情報セキュリティ対策技術の開発実証等（総務省）

2006年度に、地方公共団体における個人情報保護・情報セキュリティ対策の強化につながる高度な技術の開発実証を行う。

イ）地方公共団体職員を対象とする情報セキュリティ研修の実施（総務省）

2006年度に、情報セキュリティ対策の中核を担う高度な知識・技術を持つ人材育成のための研修や、様々な自治体業務に携わる幅広い地方公共団体職員を対象に行う研修を実施するなど、地方公共団体職員の研修について支援を行う。

第2節　重要インフラ

2009年度初めには、重要インフラにおけるIT障害の発生を限りなくゼロにすることを目指し、政府は、重要インフラの情報セキュリティ対策について、「重要インフラの情報セキュリティ対策に係る行動計画」（2005年12月13日情報セキュリティ政策会議決定）を別途定めたところであるが、2006年度に以下の施策を重点的に推進する。

①重要インフラにおける情報セキュリティ確保に係る「安全基準等」の整備

「重要インフラにおける情報セキュリティ確保に係る『安全基準等』[5]策定にあたっての指針」[6]（以下、「指針」という。）を踏まえ、それぞれの重要インフラ事業分野ごとに、必要な又は望ましい情報セキュリティ対策の水準について、「安全基準等」に明示することを目標とする。さらに、指針については1年ごと及び必要に応じて適時見直すこととし、「安全基準等」については、情報セキュリティを取り巻く環境の変化に応じ、随時見直しを行う。

【具体的施策】

ア）各重要インフラ分野の安全基準等の策定・見直し

a)安全基準等の策定・見直し（重要インフラ所管省庁[7]）

2006年9月を目処に、指針を踏まえて、各重要インフラ事業分野における安全基準等に必要又は望ましい情報セキュリティ対策の水準を明示するよう努力する。この際、「情報システムの信頼性向上に関するガイドライン」を参考とする。

b)電気通信分野における「安全基準等」の整備（総務省）

電気通信事業者等において設置される「電気通信分野における情報セキュリティ対策協議会（仮称）」を通じて、電気通信事業者等と連携し、「重要インフラの情報セキュリティ対策に係る行動計画」において官民が取り組むべき課題とされている「安全基準等」について、2006年9月を目途に整備すべく検討を行い、電気通信分野における情報セキュリティ対策の強化を図る。

イ）「安全基準等」の策定状況の把握及び評価（内閣官房）

2006年度中に「安全基準等」の策定状況を、各重要インフラ所管省庁の協力を得て把握を行い、相互依存解析の実施状況も踏まえつつ「安全基準等」の評価を実施する。

ウ）指針の見直し（内閣官房）

定常的な IT 障害の発生状況の把握を通じ、各重要インフラ分野に共通する横断的な対策課題の分析・検討を行うとともに、政府機関統一基準、その他関連文書を参照しつつ、各重要インフラ所管省庁の協力を得て、2006年度中を目途に

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

6 「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」（2006年2月2日情報セキュリティ政策会議決定）

7 「重要インフラ所管省庁」とは、重要インフラ事業者等（「重要インフラの情報セキュリティ対策に係る行動計画」（2005年12月13日情報セキュリティ政策会議決定）中「1　目的と範囲」に示す定義による。以下同じ。）と法令に従って直接に接する省庁を指す。以下同じ。

指針の見直しを実施する。

②情報共有体制の強化

IT障害に関する情報について、1）IT障害の未然防止、2）IT障害の拡大防止・迅速な復旧、3）IT障害の要因等の分析・検証による再発防止の3つの側面から、政府等は重要インフラ事業者等に対し適宜・適切に提供し、また重要インフラ事業者等間並びに相互依存性のある重要インフラ分野間においてはこれら情報を共有する体制を強化する。

（ア）官民の情報提供・連絡のための環境整備

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

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

【具体的施策】

ア）情報共有体制整備と機能強化（内閣官房）

2006年度において、各重要インフラ事業者等から連絡された情報及び情報セキュリティ関係省庁[8]、事案対処省庁[9]、関係機関から集約した情報を分析し、適切に各重要インフラ所管省庁及び各重要インフラ事業者等に対し情報提供を実施する。さらに、緊急時においても関係者との間で必要な対処についての調整を行えるようセンター機能[10]の2007年度内運用開始に向けた環境整備に着手する。

イ）情報提供・連絡のための体制強化（重要インフラ所管省庁）

内閣官房にて策定された実施細目[11](仮称)に基づき、重要インフラ事業者等から各重要インフラ所管省庁ごとに選任されたリエゾンを通じて連絡された情報を内閣官房に連絡するための体制を強化する。また、内閣官房から提供された情報を CEPTOAR を通じて、各重要インフラ事業者等に提供するための体制を

8 「情報セキュリティ関係省庁」とは、警察庁、防衛庁、総務省及び経済産業省を指す。
9 「事案対処省庁」とは、警察庁、防衛庁、消防庁、海上保安庁などを指す。
10 「センター機能」とは、IT障害発生時等緊急時における重要インフラ事業者間の調整を行うセンター機能：重要インフラの情報セキュリティ対策に係る行動計画 （7　各主体において取り組むべき事項と横断的施策（1）イ③）参照
11 「実施細目」とは、「重要インフラの情報セキュリティ対策に係る行動計画」の情報連絡・情報提供に関する実施細目（仮称）を指す。

強化する。このため、重要インフラ所管省庁に、内閣官房が構築した情報共有体制を適切な情報管理で行うためのリエゾンを2006年度の可能な限り早期におき、内閣官房に併任する。

（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整備の推進

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

各重要インフラ所管省庁及び各重要インフラ事業者等間での協議を開始し、2006年度末までに各重要インフラ分野に CEPTOAR が整備されることを目指す。また、新規追加分野（水道、医療及び物流）については、CEPTOAR 整備に関する重要インフラ所管省庁及び重要インフラ事業者等間での基本的合意を2006年度末までに完了することを目指す。

b） 電気通信分野における情報セキュリティ関連情報共有・分析体制の強化（総務省）

2006年度中に、第2章第2節①に掲げる「電気通信分野における情報セキュリティ対策協議会（仮称）」を通じて、電気通信事業者等と連携し、「重要インフラの情報セキュリティ対策に係る行動計画」において官民が取り組むべき課題とされている CEPTOAR を整備すべく、既存の事業者団体間の連携の在り方について検討を行い、電気通信分野における情報セキュリティ関連情報共有・分析体制の強化を図る。

イ）「CEPTOAR 特性把握マップ」（仮称）とりまとめ（内閣官房）

重要インフラ所管省庁の協力を得て、各重要インフラ分野ごとに設けられる各 CEPTOAR の整備状況を把握するとともに、各分野の事業特性から反映された機能特色等について業種ごとに把握し、特徴把握が容易かつ可視性を工夫した「CEPTOAR 特性把握マップ」（仮称）を2006年度末を目途に作成する。

（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）の設置検討（内閣官房）

2006年度内に整備されるCEPTOARの代表から構成される検討の場を重要インフラ所管省庁及び重要インフラ事業者等の協力を得て設置する。

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）相互依存性解析の試行的実施（内閣官房）

2006年度中に、各重要インフラ所管省庁の協力を得て、2005年度の解析手法に関する調査結果を踏まえ、過去の災害等の調査等を通じて、依存関係を可視化できる仕組み（静的相互依存性解析）を構築するとともに、各重要インフラ分野の特性や状況等を配慮しつつ、試行的に相互依存性解析を実施する。

④分野横断的な演習の実施

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）「研究的演習」の実施（内閣官房及び重要インフラ所管省庁）

2006年度中に、演習実施の概念、演習課題の設定及び演習手法の理解等を主眼とし、各重要インフラ分野の特性や状況等を配慮しつつ、研究会を併用した演習(「研究的演習」)を実施する。

イ)「机上演習」[12]の実施(内閣官房及び重要インフラ所管省庁)

2006年度中に、類似業態単位又は重要インフラ分野横断的な共通事項単位に議論発掘と具体課題整理のための「机上演習」を実施する。

ウ)各重要インフラ分野における対応強化への取組み

a)電気通信事業分野におけるサイバー攻撃への対応強化(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 IT スキルを有する人材の育成を図るべく、2006年度に、電気通信事業者を中心に、各重要インフラ分野に跨る情報通信ネットワーク上で発生するサイバー攻撃を想定したサイバー攻撃への対応演習を実施する。

エ)各分野サイバー演習との連携(内閣官房及び重要インフラ所管省庁)

2006年度中に、分野ごとに実施された「情報通信」「電力」等のサイバー演習と内閣官房の実施する演習について、実施形態及びその目的の整合性を考慮しつつ、連携に向けた検討を開始する。

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、2006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

12 「机上演習」とは、演習参加者が1つのシナリオを元に、会議形式で課題検討を行いながら実施する演習を指す。

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等（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、2006年度中に、情報セキュリティ対策ベンチマーク、情報セキュリティ報告書モデル、事業継続計画策定ガイドラインの普及を図るとともに、必要に応じてこれらのツールの見直し、情報セキュリティガバナンスの確立のための新たな方策の検討を行う。

また、情報システムの構築や運用を各企業が行う際に、「情報システムの信頼性向上に関するガイドライン」を参照することを推奨するべく、2006年度から普及活動に着手する。

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）

2006年度に、電気通信事業者の情報セキュリティ体制の構築・運用に資するため、事業者や事業者団体等と連携して、電気通信事業における情報セキュリティマネジメント指針（ISM－TG）の策定を促進する。

（ＩＳＭ－ＴＧ：Information Security Management Guideline for Telecommunications）

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）

情報システム等の政府調達において、競争参加者に対して入札条件等として求めるべき情報セキュリティ対策レベルの評価について検討を行い、2006年度中に結論を得る。

ウ）情報セキュリティ関連制度と内部統制制度等との整合性確保（内閣官房、金融庁及び経済産業省）

政府が推進する情報セキュリティに関する取組みについて、政府全体としての整合性を確保するため、現在構築が検討されている内部統制制度のIT統制に係る部分において、情報セキュリティに関連する事項については、既存の対策基準等の情報セキュリティ関連制度との関連を考慮しつつ、2006年度に検討を進める。

②質の高い情報セキュリティ関連製品及びサービスの提供促進

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

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

【具体的施策】

ア)情報セキュリティ関連リスクに対する定量的評価手法の研究(経済産業省)

企業における情報セキュリティ対策そのものの可視化を図るため、2006年度中に、情報セキュリティに係るリスク定量化に関する調査研究等を実施する。

イ)第三者評価の活用促進

a) 情報セキュリティマネジメントシステム適合性評価制度の普及促進(経済産業省)

国内外の取引等において、組織の情報セキュリティ水準を適正に評価できる環境を整備するため、2006年度中に情報セキュリティマネジメントシステム適合性評価制度の普及活動を行う。

b)情報セキュリティ監査制度の普及促進(経済産業省)

国内外の取引等の場面において、組織の情報セキュリティ水準を適正に評価できる環境を整備するため、2006年度中に、様々なニーズに応じた質の高い監査サービスを受けられる基準等の検討を行う。

c)情報セキュリティマネジメントに関する標準化の推進(経済産業省)

組織が情報セキュリティマネジメントシステムを効率的に確立、導入、運用、監視、レビュー、維持及び改善する際の標準として、2006年度中に、日本工業規格として、JISQ27001(情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項)(＝ISO／IEC27001)及びJISQ27002(情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範)(＝ISO／IEC17799)を制定する。

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

独立行政法人情報処理推進機構が運用するITセキュリティ評価及び認証制度について、制度の運用改善に資する新たな基準であるコモンクライテリア(CC:Common Criteria)Ver.3 に基づく運用を2006年7月から開始し、IT 製品等の効率的な評価及び認証を推進する。

ウ)税制優遇措置

a)情報セキュリティ対策装置の取得時における税制優遇措置(総務省)

2006年度において、法人又は個人事業者が一定の条件の下でファイアウォール装置等の情報セキュリティ対策装置を取得した場合の税制支援措置を実施する。

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

2006年度において、産業競争力のための情報基盤強化税制の普及・啓蒙を図ることにより、企業の高度な情報セキュリティが確保された情報システム投資を促進する。

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)情報通信セキュリティ人材を育成するための研修事業への支援(総務省)

2006年度において、情報通信ネットワーク・システムに対する攻撃や不正侵入などに対する多面的、双方的知識及び実践的な対処法を習得するための人材育成センターの開設を支援するとともに、セキュリティ人材を含む情報通信分野の専門的な知識や技術を有する人材を育成するための研修事業に対し助成を行う。

イ)情報セキュリティに関する専門家の育成等(経済産業省)

2006年度中に、企業や大学における情報セキュリティ人材育成のあり方を検

討するとともに、組織における IT 利用者を対象とした情報セキュリティ対策レベルを客観的に測定するための指標の検討を開始する。

ウ）中小企業を対象とした情報セキュリティセミナーの実施（経済産業省）

2006年度中に、中小企業の経営者や情報システム担当者等における情報セキュリティへの理解を深めるべく、独立行政法人情報処理推進機構と日本商工会議所が連携して実施している「情報セキュリティセミナー」の規模を拡大するとともに、内容のさらなる充実強化を行う。

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）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、2006年度中に、独立行政法人情報処理推進機構や有限責任中間法人 JPCERT コーディネーションセンター等による「コンピュータセキュリティ早期警戒体制」を強化する。

イ）安全な Web サイトが備えるべき基準の検討（経済産業省）

Web サイトの安全性を確保するため、2006年度中に、発注者がウェブアプリケーション構築時に開発者（受注者）に対して示すべきセキュリティ要件に関する基準の検討を開始する。

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、2006年度に以下の施策を重点的に推進する。

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

①情報セキュリティ教育の強化・推進

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

【具体的施策】

ア）初等中等教育からの情報セキュリティ教育の推進

a）小中学校における情報セキュリティ教育の推進（文部科学省）

児童生徒に対する情報セキュリティを含めた情報教育を推進するため、2006年度に、効果的な指導手法に関する実践事例の収集や、意識啓発のための普及フォーラムの開催などを通じて、教員の指導力の一層の向上を図る。

b）ICTメディアリテラシー[13]育成手法の調査・開発（総務省）

子どものインターネット、携帯電話等のICTメディアの健全な利用の促進を図るため、これらの利用にあたって必要とされる総合的なICTメディアリテラシーに係る指導マニュアルや教材の開発等、新たなICTメディアリテラシー育成手法に関する調査・開発を 2006 年度に行い、2007 年度以降に普及・啓発を図る。

c）「情報セキュリティ対策」標語による普及啓発（経済産業省）

独立行政法人情報処理推進機構において、コンピュータウイルスやコンピュータへの不正な侵入による被害の軽減に資するべく、2006年度中に、全国の小学生・中学生・高校生を対象として、情報セキュリティ対策の意識を高めるための標語募集を行い、入選作品を公表する。

イ）世代横断的な情報セキュリティ教育の推進

a）全国的な普及啓発活動の実施（経済産業省及び警察庁）

2006年度において、新たな脅威の動向を教材に反映する等、「インターネット安全教室」の内容の充実・強化を図りつつ、全国各地で継続的に開催することを通じ、一般利用者における情報セキュリティに関する基礎的な知識の普及を図る。

b） e－ネットキャラバンの実施（総務省及び文部科学省）

2006年度において、主に保護者及び教職員を対象にインターネットの安心・安全利用に向けた啓発のための講座のキャラバンを、通信関係団体等と連携し

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

ながら全国規模で実施する。

②広報啓発・情報発信の強化・推進

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

【具体的施策】

ア）全国的規模での広報啓発・情報発信の継続的実施

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

国民の情報セキュリティ意識の向上を図るため、急速に高度化・複雑化している情報セキュリティの脅威に関する情勢等を踏まえ、2006年度に、「*@police*」、「国民のための情報セキュリティサイト」、「フィッシング対策協議会」、「フィッシング対策推進連絡会」等の取組みを通じた国民一人一人に対する適切な情報提供や、メディア等を活用した広報啓発活動を積極的に実施する。

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

2006年度において、不正アクセス行為の禁止等に関する法律に基づき、不正アクセス行為の発生状況及びアクセス制御機能に関する研究開発の状況を公表するなどの取組みを通じ、不正アクセス行為に対する防御に関する啓発及び知識の普及を図る。

c）ネットワークの不適正な利用からの被害防止対策の推進（警察庁）

2006年度において、サイバー犯罪等の被害を防止するために、ネットワーク相談対応システム等を効果的に活用してサイバー犯罪等に係る情報提供を広く受け付けるとともに、広報啓発を効果的に実施する。

d）電波利用秩序の維持のための周知啓発活動の強化（総務省）

ユビキタスネット社会を迎え、無線によるブロードバンドサービスの利用が不可欠となる中で、安心・安全に電波を利用できる環境を保護する必要性が急速に高まっている。

このため、混信・妨害の未然防止をはじめ電波利用秩序の維持を図る上で、適正な無線機器の購入・使用を促すことが益々重要となっている。そこで、一般国民が安心して無線機器の購入・使用できる環境づくりに向けて、2006年度に、

全国のマスメディア媒体、ポスター、インターネットなどを利用して、無線機器に添付される「技術基準適合マーク」の確認を促すための周知啓発活動を実施する。

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」の創設（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、2006年度に「情報セキュリティの日」を創設し、これに伴う広報啓発的行事を全国的規模で開催するとともに、これにあわせて、個人、企業、地方公共団体、教育機関及び研究機関等を表彰するための制度の創設を検討する。

ウ）日常からの世論喚起・情報提供の仕組みの構築

a）日常からの世論喚起・情報提供の実施（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、メールマガジンの発行及び政府全体としての情報セキュリティポータルサイトの構築を実施する。

メールマガジンについては、2006年度の可能な限り早期に発行を開始し、月に1度以上の頻度で配信を行う。また、情報セキュリティポータルサイトについては2006年度中に開設する。

b）情報セキュリティ貢献表彰(仮称)の創設（総務省及び経済産業省）

情報セキュリティの確保に多大な貢献を果たした個人、企業等を表彰するべく、情報化月間に新たに「情報セキュリティ貢献表彰（仮称）」を2006年度中に創設する。なお、その際、「『情報セキュリティの日』の創設」（第2章第4節②イ）a））との連携に配意する。

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、2006年度中に内閣官房情報セキュリティセンターの英文ホームページを開設し、「第1次情報セキュリティ基本計画」の英語版等を示すこととする。

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、2006年度中に技術面及び対策面を含めた検討を開始し、2010年度までに総合的な枠組みを構築する。

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[14]を2009年度までに構築することを目指して、2006年度中に利用環境をモデル化した実証実験を開始し、IPv6によるユビキタス環境構築に向けたセキュリティ確保上の課題解決を進める。

ウ)無線LANのセキュリティ対策(総務省及び経済産業省)

2006年度において、無線 LAN のセキュリティに関するガイドライン「安心して無線 LAN を利用するために」の更なる普及の推進を図るとともに、「インターネット安全教室」の冊子等においても、無線LANの安全な使い方に関するコンテンツの充実を図る。

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

第3章　横断的な情報セキュリティ基盤の形成

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

第1節　情報セキュリティ技術戦略の推進

民間部門における取組みとの役割分担を明確にしつつ、情報セキュリティに関する技術戦略として、政府は、2006年度に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を把握するための検討を2006年度中に開始する。

イ）投資効果に係る継続的評価プロセスの導入（内閣官房及び内閣府）

情報セキュリティ政策会議は総合科学技術会議との連携の下に、情報セキュリティ技術に関する研究開発・技術開発の投資効果について、1）事前、2）中間、3）事後の各段階における評価を2006年度中に開始し、その結果については速やかに公表する。

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の検討を2006年度中に開始する。

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、防衛庁、総務省、文部科学省及び経済産業省）

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検討を行い、その基本方針及び具体策を2006年中に示す。

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[15]全体の安定運用等を実現する技術を確立することを目標として、2006年度において、次世代バックボーンに関する研究開発を推進する。

c）経路ハイジャック[16]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、2006年度から経路ハイジャックの検知・回復・予防に関する研究開発に着手する。

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）

情報セキュリティの一層の向上を図るべく、2006年度より、ネットワーク自身及びネットワーク上を流通する情報の安全性・信頼性を確保するためのセキュリティ

15 「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。

16 「経路ハイジャック」とは、各インターネットサービスプロバイダ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。

技術と、大規模災害時にも切れずに防災・減災情報を瞬時に、かつ的確に利用できる技術と併せて、総合的な情報のセキュリティを確保するための技術に関する研究開発を実施する。

e）新世代のアクセス制御技術の研究開発（経済産業省）

高信頼性社会の実現に不可欠な基盤技術として、既存の情報システムを前提とした従来の技術にとらわれない新世代のアクセス制御技術、認証技術、ソフトウェア技術等の研究開発を2006年度に実施する。

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

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

g）フェイルセーフな情報セキュリティ技術の研究開発（経済産業省）

「事故は起こりうるもの」との前提に立ち、情報やシステムを保護するだけではなく、実際にシステム障害が発生した場合、あるいは情報の一部が漏洩したような場合でも、一定程度の安全性を確保できるような技術やフェイルセーフの概念に基づいたソフトウェアの設計・開発手法の研究開発等を2006年度に実施する。

h）情報セキュリティに関するリスク定量化手法についての研究開発（経済産業省）

組織・人間系の管理手法の高度化のため、組織における情報セキュリティのリスクの定量化、情報セキュリティ対策に関する費用対効果の測定等の研究開発を2006年度に実施する。

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、防衛庁、総務省、文部科学省及び経済産業省）

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の調整をきめ細かく行うための検討を行い、その具体策を2006年度中に示す。

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】

2006年度において、ITの信頼性確保のための喫緊な取組みとして、現在のOSやアプリケーション等の利用環境を維持しつつ、これに依存しない形で情報セキュリティ機能を集約的に提供することのできる仮想機械（VM：Virtual Machine）機能及びこれを稼働させるための最小限のOS機能（これらの機能を併せて「セキュアVM」と呼ぶ。）の開発を、産学官の連携により推進する。

c）電子政府に用いられるOSのセキュリティ品質の評価尺度の確立（内閣官房及び総務省）【再掲】

2006年度中に、電子政府に係る情報システムを構成するOSについて、そのOSのセキュリティ品質に係る評価尺度の確立に向けた検討を行い、システム調達時に活用可能な評価項目群及び各項目についての評価尺度の確立を図る。また、本格的な電子政府運用開始に向けたOS等システム導入における技術動向調査を2006年度に実施する。

d）デジタルフォレンジック[17]分野の確立に向けた産官学の連携強化（警察庁）

2006年度中に、警察におけるデジタルフォレンジック分野に係る調査研究を推進するとともに、民間企業との技術協力、デジタルフォレンジックに係る研究会への参加等を通じ、情報共有を推進する。

e)高い保証レベルを有する情報システムの開発及び評価（防衛庁）

2006年度において、情報セキュリティ基準ISO／IEC15408で規定される評価保証レベルEAL6の保証要件を満足する情報システムを試作し、評価試験を行うことにより評価手法の確立を推進する。

f)ネットワークのオールIP化に対応した重要通信の運用技術の確立（総務省）

ネットワークがオールIP化された場合においても災害時等に重要な通信が確保できるよう、2008年までにIPネットワーク等に対応した重要通信の運用技術を確立することを目標として、2006年度に実験システムの開発に着手する。

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、防衛庁、総務省、文部科学省及び経済産業省）

17 「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。

民間での技術開発が行われている領域については民間の自主性に任せ、民間の取組みが乏しい萌芽的な研究については公的研究資金を投入する等のポートフォリオ調整の実施に向けた検討を行い、その基本方針と具体策を2006年中に示す。

b)高信頼性端末の電子認証基盤の研究開発（経済産業省）

暗号処理機能、暗号鍵の保護機能、プラットフォームの正当性検証機能等のセキュリティ機能を持つTPM（Trusted Platform Module）を搭載したPCの活用による安全なコンピューティング環境の実現に向けた研究開発を2006年度に実施する。

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）

継続的にグランドチャレンジ型に相応しいテーマを検討するための場を、総合科学技術会議、情報セキュリティ政策会議が連携して2006年度中に設置する。また、その際、設定されたテーマを基に研究開発・技術開発を推進する体制として、例えば、プログラムマネジャー制等、大目標の下での多岐にわたる各種要素技術の総合管理と最適な資源配分を促進するための枠組みの構築を検討する。

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、2006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）情報セキュリティ関連の高等教育機関における多面的・総合的能力を有する人材の育成（文部科学省）

2006年度に、大学・大学院において産学連携による高度IT人材育成プログラムを開発・実施する拠点形成を支援する。

イ）情報セキュリティに関する専門家の育成等（経済産業省）【再掲】

2006年度中に、企業や大学における情報セキュリティ人材育成のあり方を検討するとともに、組織における IT 利用者を対象とした情報セキュリティ対策レベルを客観的に測定するための指標の検討を開始する。

ウ）情報通信セキュリティ人材を育成するための研修事業への支援（総務省）【再掲】

2006年度において、情報通信ネットワーク・システムに対する攻撃や不正侵入などに対する実践的な対処法を習得するための人材育成センターの開設を支援するとともに、セキュリティ人材を含む情報通信分野の専門的な知識や技術を有する人材を育成するための研修事業に対し助成を行う。

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。

【具体的施策】

ア）情報セキュリティに関する資格制度の体系化等のための検討（内閣官房、総務省、文部科学省及び経済産業省）

高い能力を有する情報セキュリティ技術者、各組織における最高情報セキュリティ責任者（CISO）、情報システム運用受託者、各組織の情報システムの運用担当者、情報システム利用者等それぞれに応じた適切なスキルについて関係府省庁間で連携を図りつつ検討を行い、情報セキュリティに関わる技術者等にとってキャリアパスとなるための情報処理技術者試験をはじめとする情報セキュリティに関する資格制度の体系化について、その基本方針及び具体策を2006年中に示す。

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、2006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）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、2006年度においては、G8及び OECD などの多国間の枠組みにおける協力を積極的に実施するとともに、FIRST（Forum of Incident Response and Security Teams）等へ積極的に参加することなどにより、諸外国の関係機関との連携を強化する。さらに、諸外国の情報セキュリティ対策の動向を把握したうえで、諸外国の関係機関との間で、情報交換・知見の共有・信頼関係の構築などを通じ、グローバルに希求される「安全・安心」の基盤づくり・環境の整備に貢献する。

イ）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、または、諸外国からみてコンタクト・ポイントが明確でない情報セキュリティ案件については、内閣官房情報セキュリティセンター（NISC）が我が国としての POC 機能を有することを明確化し、2006年度は、その国際的な周知を実施し、諸外国との間でより効果的で円滑な連携を図るインターフェースとなる。

ウ）情報セキュリティ政策に関する国際的な広報活動の推進（内閣官房）

情報セキュリティ先進国としての我が国の情報セキュリティ政策の基本理念や戦略、政府全体の政策、その中核を担う内閣官房情報セキュリティセンター（NISC）の位置づけと機能などについて、国際的な広報活動を2006年度に実施する。

エ）OECDにおける重要情報インフラ保護のための各国施策の分析及び情報共有に関する取組みへの参加（総務省及び経済産業省）

OECDにおける重要情報インフラ保護のための各国施策の分析及び加盟国間の情報共有に関する取組みに参加し、2006年中に取りまとめられる予定の報告

書の作成に貢献する。

オ）国際的なセキュリティ文化実現のための取組み（内閣官房）

2002年に OECD が策定した「情報システム及びネットワークのセキュリティのためのガイドライン」で定義された「セキュリティ文化」を実現するため、2006年度に、国内のみならず、国際的にも認識を共有しうるよう、環境整備に貢献する。

カ）APT研修・セミナー等の開催（総務省）

アジア太平洋地域のセキュリティに関する環境整備に資するために、APT[18]の人材育成スキーム等を活用し、2006年度にセキュリティに関する国際的な研修・セミナー等を開催する。

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、2006年度においては、IT障害への対処、防災や災害などへの対応、各国が共通に抱える社会的課題への対応など、様々な課題への多面的な知見・成果を、国際標準等に戦略的に反映させることも含めて、世界に先駆けて国際的に提供していく。

イ）海外のコンピュータセキュリティ緊急対応チーム（CSIRT）の体制強化の支援（経済産業省）

有限責任中間法人JPCERTコーディションセンター（JPCERT/CC）を通じ、アジア太平洋地域における海外CSIRTの構築を支援する。具体的には、2006年度に、同地域におけるCSIRTの集合であるAPCERTとも連携をとりながら、JPCERT/CCにおけるインシデント運用技術や蓄積された経験を同地域の関係諸機関と共有し、これらの機関の能力向上を図る。

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

18 「APT（アジア・太平洋電気通信共同体）」は、アジア太平洋地域の電気通信専門の国際機関であり、33ヶ国・4地域が加盟しており、電気通信の均衡した発展を目的として、研修やセミナーを通じた人材育成、標準化や無線通信などの地域的政策調整及び地域的な電気通信問題の解決等を行っている。

電気通信分野の情報セキュリティマネジメントガイドラインの国際規格化を目指し、２００６年度は、国際電気通信連合（ITU：International Telecommunications Union）に対して、第2章第3節①に掲載の電気通信事業における情報セキュリティマネジメント指針（ISM-TG）について提案を行い、国際標準として採択されるよう努め、もって国際的な情報セキュリティマネジメントのレベルの向上に貢献する。

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、2006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、2006年度に積極的に実施する。

b)サイバー犯罪の取締りのための体制の強化・整備（警察庁）

地理的制約をほとんど持たないという特性を持つサイバー犯罪に適切に対処するため、県境・国境を越えて敢行されるサイバー犯罪を的確に取り締まるための捜査体制を2006年度に強化・整備する。

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批准に伴う新たな法制度の施行に対応するため、2006年度に、捜索現場での活動やコンピュータウイルス等の動作検証を行うための資機材の整備・増強を実施する。

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、サイバー犯罪に適切に対処すべく、サイバー犯罪条約を締結するための法整備等を2006年度に推進する。

（2005年10月４日に、「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」を第163回国会に提出したところ、現在継続審議中。）

e）サイバー犯罪の取締りのための国際連携の推進（警察庁）

2006年度中に、サイバー犯罪対策に係る海外の法執行機関との連携について、2国間における取組みを進めるとともに、G8ハイテク犯罪サブグループ会合、ICPO等のサイバー犯罪対策に係る国際的な枠組みへの参画の継続的推進、アジア地域サイバー犯罪捜査技術会議の参加国拡大等を通じた多国間における協力関係の構築を推進する。

f）中央当局制度[19]を活用した国際捜査共助の迅速化（法務省）

捜査・司法当局を中央当局として指定し、外交ルートを経由せずに共助の授受を行うことで共助の迅速化を図るとともに、原則として共助を義務的とする日米・日韓の二国間における捜査共助条約が2006年度に発効する見込みであるところ、国際的なサイバー犯罪に適切に対処すべく、2006年度においては、同種の二国間条約を締結する作業を進める。また、サイバー犯罪条約上の「中央当局」の指定について、関係省庁と協議の上、検討する。

g）重要無線通信妨害対策の強化（総務省）

航空無線や消防無線などの重要無線通信インフラに対し、混信・妨害が発生し、システムの機能低下や停止が起こり、人命・財産等の脅威に派生するなどの事態が発生しており、あるいは重要無線通信インフラを意図的に操作し、システムの誤動作を引き起こす等の懸念もあり、その迅速な排除に向けての対策強化が益々重要となる。

このため、重要無線通信に係る混信・妨害の申告・相談に対する的確な対応、並びに混信・妨害の迅速な排除に向けて、「電波監視充実3カ年計画」に基づき電波監視の充実・強化を図るとともに、2006年度末までに電波監視施設の更改、大都市圏での電波監視職員の増員などにより電波監視の強化を図る。

19 「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。

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

サイバー空間における権利利益の保護・救済のための基盤の整備の必要性について、関係府省庁と連携しながら、2006年度に現状把握等の調査を行う。

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）高度なネットワーク認証基盤実現のための技術開発（総務省）

インターネット上のやりとりを安心・安全に行うことができるよう、厳格な本人確認機能を有するネットワーク基盤構築のための技術開発に取り組み、2006年度中に基礎技術を開発する。

イ）サイバーテロ対策に係る官民の共同研究の推進（警察庁）

2006年度において、民間企業や大学等と連携して、ファイアウォール等のログ等の分析によるサイバー攻撃の予兆把握等に関する共同研究を実施する。

第4章　政策の推進体制と持続的改善の構造

政府は、2006年度に、前章に示した重点政策に、以下に示す体制と持続的構造の下で総合的に取り組むこととする。

第1節　政策の推進体制

（1）内閣官房情報セキュリティセンター（NISC）の強化

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

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

【具体的施策】

ア）内閣官房情報セキュリティセンター（NISC）の強化（内閣官房）

政府全体の情報セキュリティ対策の推進体制の中核となるべく、内閣官房情報セキュリティセンター（NISC）の人員体制を引き続き強化し、体制面として2006年度の早期に60名体制を確保するとともに、最高の英知を結集するため、官民を問わず優れた人材を積極的に活用する。

こうした体制の下、政府機関統一基準とそれに基づくPDCAサイクルを確立し、また、政府全体としての緊急対応能力を強化するため、第2章第1節に示した施策を実施するとともに、重要インフラの情報セキュリティ対策に係る行動計画等に従って、第2章第2節に示した施策を実施する。

また、府省庁横断的な情報セキュリティ案件についての我が国の国際的なPOCとしての内閣官房情報セキュリティセンター（NISC）の機能を充実させるとともに、国際的なコミュニケーションや情報共有を通じ、諸外国から信頼される国際的なインターフェースとしての役割を果たすべく、POC としての認知度向上、諸外国との信頼関係の構築を推進し、また、情報収集の充実、関係機関等との情報の共有・分析機能の強化を図り、横断的な情報セキュリティ政策推進の中核としての機能

を確保する。

さらに、内閣官房情報セキュリティセンター（NISC）の活動状況及び情報セキュリティに係る動向等を広く国民に知ってもらうとの観点から、2006年度より定期的に内閣官房情報セキュリティセンター（NISC）のメールマガジンを発行する。

（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）

2006年度において、各府省庁は、自らの情報セキュリティ対策の体制の強化を行うとともに、政府機関全体で協調し、官民における情報セキュリティ対策の実施手順及び成果等の共有化や対策の統一化等の府省庁横断的な取組みを実施する。

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）

2006年度において、情報セキュリティ政策会議は、IT戦略本部はもとより、経済財政諮問会議、総合科学技術会議等、他の関係する本部・会議等との意見交換を密にし、これらとの役割分担をより明確化していくとともに、様々な方策の提案や実施

において緊密に協力し、政府全体として情報セキュリティ政策を一体的に推進する。

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[20]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、2006年度以降、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とともに、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）評価の実施及び公表（内閣官房）

2006年度において、セキュア・ジャパン2006を適切に評価するための手法について検討を行いつつ、そこに記載されている具体的施策の取組状況について評価を実施し、その結果を半年ごとに公表する。その際、IT戦略本部評価専門調査会の検討との連携を図る。

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）

2006年度において、基本計画の実現に向けて、政府以外の関係機関における対応をあらかじめ促す等の観点から、政府機関自らの情報セキュリティ向上に係る施策について、2008年度までのマイルストーンを検討する。

[20] 「第3期科学技術基本計画」（2006年3月28日閣議決定）

ウ)「重要インフラの情報セキュリティ対策に係る行動計画」に基づく取組み(内閣官房)

「重要インフラの情報セキュリティ対策に係る行動計画」に基づく2006年度における取組状況を、重要インフラ専門委員会の場を活用して把握する。

(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、本セキュア・ジャパン2006の実施途中であっても、迅速に相応の取組みを策定の上実施する。

(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)

基本計画(セキュア・ジャパンの実現)の実現に向けた道筋を可視化する視点に立ち、各対策実施領域(政府機関、地方公共団体、重要インフラ、企業、個人等)における情報セキュリティ対策の浸透の度合いを評価することができる指標を検討するための体制を2006年度のできる限り早期に設置し、2006年度中に的確な評価指標を確立した上で、これらの指標の政府内及び国際機関等における活用を推進する。

なお、当該評価指標の確立に資するため、独立行政法人情報処理推進機構による「国家情報セキュリティ水準評価指標(仮称)」の策定を促進するほか、「情報通信インフラのセキュリティ水準評価指標(仮称)」の策定について検討する。

第5章　2007年度の重点施策の方向性

～2007年度の重点「官民における情報セキュリティ対策の底上げ」～

第2章から第4章では、3か年計画である基本計画の第一歩として**「官民における情報セキュリティ対策の体制の構築」**を重点とし、2006年度に実施すべき具体的施策を挙げてきた。

我が国全体としての情報セキュリティ対策は、あらゆる主体が、情報セキュリティ問題への取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が必要である。しかし、「体制の構築」によってはカバーできない部分として、重要性の認識が不足している者や自らの実施が現状では困難な者の存在があり、これら取組みが遅れている主体のレベルを「底上げ」することが、全体のレベルを上げる目的に照らして、極めて重要である。

これら取組みが遅れている主体のレベルを「底上げ」するための施策の柱としては、①取組みが遅れている主体その他の主体に対して模範例を示すことが期待される領域の取組み、②取組みが遅れがちな主体への対策、③取組みが遅れている主体が発生しないように横断的に情報セキュリティ基盤を強化・安定させる取組み、がある。

そこで、2007年度は、2006年度の施策を受け継ぐとともに、3か年計画の実施最終年である2008年度に向けての確かな道筋を確立すべく、**「官民における情報セキュリティ対策の底上げ」**を重点として、特に、以下の施策を推進することとする。

第1節　模範となる領域の情報セキュリティ対策の底上げ

政府機関の領域及び重要インフラの領域は、基本計画において、それぞれ、「2009年度初めまでに、すべての政府機関において世界最高水準の対策の実施を目指すこと」、「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すこと」とされているところであり、他の主体に対して模範となることが期待される領域である。また、地方公共団体は政府機関の取組みも踏まえながら情報セキュリティ対策の強化を図ることが必要とされている。そこで、この3つの領域においては、2007年度は、2006年度の体制の構築に続き、以下の施策に取り組み、取組みが遅れている者その他の主体に対して模範を示すこととする。

【具体的施策】

ア）政府機関における情報セキュリティ対策の底上げ

a)PDCA サイクルの定着と本格的評価の推進(内閣官房及び全府省庁)

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等の結果を

踏まえて自ら対策の改善を行い、PDCA サイクルの定着により組織全体での底上げを図る。また、内閣官房は、2006年度中に確立した評価手法に基づき、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して、それを公表し、政府全体として効果的な対策の促進を図る。

b)情報セキュリティ対策の先導的実証モデルの提示(内閣官房)

技術的には確立されているものの、先導的なセキュリティ対策及び政府機関において導入が遅れている対策について、導入すべき現場の実態に応じた移行手法や設定方法等のノウハウ不足により、普及が進まない現状を踏まえ、内閣官房が実証モデルとしてこれらの情報セキュリティ対策を導入することで実施手順等を作成し、政府機関及び他の主体が導入するための参考となる技術情報等を提供することにより、対策の導入を促進する。

c)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(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防止し、発生した場合には迅速かつ的確に対応するため、内閣官房情報セキュリティセンターにおける横断的な情報収集機能、攻撃等の分析・解析機能、各政府機関への助言機能及び各政府機関の相互連携促進機能の強化を図る(「事案対策促進機能(Government Security Operation Coordination Team)(略称;GSOC)(仮称)」の本格稼働)。この際、内閣官房情報セキュリティセンターを中心に、政府機関において各情報システムのリアルタイム監視と即時対応機能の強化を図る。

d)サイバーテロに関する情報の収集及び事案対処能力の強化(警察庁)

サイバーテロ発生時の対処を適切かつ的確に行うために、新たなインターネット観測機能、現場活動用資機材、サイバーテロ発生時における現場の状況を適切に把握し、迅速な指揮・命令を行うための資機材等、装備資機材の整備・高度化を図るほか、警察におけるサイバーテロ対策に係る国際連携の強化を推進する。

e)サイバー攻撃時の対処に必要な教育訓練、攻撃手法の分析及び防御体制の評価(防衛庁)

サイバー攻撃対応要員の教育訓練、攻撃手法の分析及び防御体制の評価を行うため、サイバー攻撃等の様相を模擬するシステムの整備を促進する。また、不正アクセス監視・防御技術、サイバー攻撃分析技術、アクティブ防御技術等サイバー攻撃等の対処を迅速かつ効果的に行うための施策を進める。さらに、上記の取組みを推進するための環境の整備及び研究体制の充実強化を図る。

イ）重要インフラにおける情報セキュリティ対策の底上げ

a）重要インフラ分野横断的な対策の推進に向けた状況把握能力の強化（内閣官房）

内閣官房は、継続的な脅威分析と重要インフラ分野ごとに把握した取組状況とを組み合わせて、総合的なリスク分析等を行い、最新の脅威情勢を把握するとともに、各重要インフラ所管省庁の協力の下、機密性の保持を要する各重要インフラ事業者等の安全対策の状況を把握する。

b）官民連携対処の円滑化に向けた情報共有基盤の強化（内閣官房）

重要インフラの各事業において発生する IT 障害から重要インフラを防護するためには、内閣官房の情報共有体制を活かし、官民の連携対処活動をより効果的かつ効率的に展開していくため、人的資源に加え、IT 障害に適正かつ迅速に対応できる機密性や完全性の確保なども取り込んだ情報共有環境の基盤の構築を図る。

c）重要インフラ分野間の動的依存性解析の推進（内閣官房及び重要インフラ所管省庁）

重要インフラ事業者の IT システムは国民へのサービスの維持に不可欠であるだけでなく、他分野の重要インフラ事業者に対しても密接に関連している。今後一層の IT 化の進展と分野間の関連性の更なる高まりが予想されるところ、重要インフラ防護は分野毎の個別対策だけでは、全体システムに対する俯瞰的分析および対策が不十分であることから、IT 障害発生から被害の波及、拡大の影響を、相互依存性の影響伝搬構造を把握した上で予測できる動的シミュレーションを推進する。

d）重要インフラ機能演習の推進（内閣官房及び重要インフラ所管省庁）

情報提供・共有体制や種々の情報セキュリティ対策が、現実の IT 障害発生時に有効に機能するかを検証するために、IT 障害波及シナリオ（想定される具体的な脅威シナリオの類型をもとにテーマを設定）を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 等との協力を得て、重要インフラ分野機能演習を行い、官民の連携体制の機能確認と円滑な対処活動を展開する上で機能演習実施計画[21]の立案等を行う。

e）インターネットの安定的な運用の確保（総務省）

サイバー攻撃、コンピュータウイルス、情報漏洩といった通信サービスの提供の

[21]「機能演習実施計画」とは、機能演習実施計画には演習シナリオを統裁（コントロール）するための計画や、CEPTOAR／重要インフラ事業者等の参加形態等が規定されることを指す。

妨げとなっている事案に際し、今や国民生活や社会経済活動の基盤である、インターネットの安定的な運用が確保されるよう、適切な環境整備を行う。

f）電力分野における情報セキュリティ対策の強化（経済産業省）

制御システムの要となる電力用制御通信システムについて、汎用技術を用いたモデルシステムを構築し、最新技術に基づくセキュリティ評価及び対策の検討を行うとともに、これらの汎用技術を用いた脅威等に関する情報の取扱いに係る調査等を推進する。

g）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）

重要インフラ事業者等の業務の特性等を踏まえつつ、必要に応じ、重要インフラ事業者等の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。また、民間企業や大学等へサイバーテロの脅威やその対策に関する調査研究の委託及びサイバーテロ発生の早期検知等に関する共同研究を検討する。

ウ）地方公共団体における情報セキュリティ対策の底上げ

a）情報セキュリティ確保に関する運用手順等の整備の推進（総務省）

地方公共団体における情報セキュリティ対策の実効性を確保するため、情報セキュリティ確保に関する運用手順等の整備を推進する。

第2節　取組みが遅れがちな主体の対策の底上げ

企業及び個人等は、情報セキュリティ対策の領域の中でも、情報セキュリティ事件・事故の被害を受けやすいにもかかわらず、市場原理の影響やそもそもの関心の低さにより、対策が遅れがちな主体が存在する領域である。そこで、2007年度においては、2006年度の施策（第2章第3節及び第4節を参照）を加速させることに加えて、以下の施策に取り組み、企業、個人のうち、取組みが遅れがちな主体の情報セキュリティ対策の底上げを推進することとする。

【具体的施策】

ア）政府機関の情報に係るポータルサイトの充実・整備（内閣官房及び全府省庁）

政府機関の情報を一覧できるポータルサイトを充実・整備する。また、政府の各分野における情報セキュリティ対策に係る資料を可能な限り公表し、このポータルサイトとリンクする。

イ）一般利用者向け普及・啓発活動の強化（総務省）

情報通信サービスの一般利用者が安心・安全にサービスを利用できるよう、情報

セキュリティに関する普及・啓発活動の強化を図る。

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

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

エ）サイバー犯罪の情勢を適切に反映した被害防止対策の推進（警察庁）

サイバー犯罪による被害を的確に防止するため、把握したサイバー犯罪等の情勢の分析を強化し、最新の手口を踏まえた普及啓発活動を行う。

第3節　横断的な情報セキュリティ基盤の底上げ

我が国の社会全体の情報セキュリティ対策を、長い目で見て、強化し安定させていく上で不足しているものとして、社会全体の情報セキュリティ基盤の弱さを挙げることができる。具体的には、情報セキュリティの状況を評価し公表する仕組み、情報セキュリティ教育者、専門家等に係る人材育成・訓練策、誰でもITを安心して使えるための研究開発・技術開発及び基準の策定、捜査機関の能力の底上げ等が挙げられる。そこで、2007年度は、以下の施策を推進することとする。

なお、これらの情報セキュリティ基盤の底上げ方策は、短期にできるものだけでなく、中長期の取組みを必要とするものが多いことに留意することが必要である。

【具体的施策】

ア）「情報セキュリティ対策白書（仮称）」の作成・発行（内閣官房）

我が国の社会全体の情報セキュリティの状況の可視化を図るべく、「情報セキュリティ対策白書（仮称）」の作成・公表を図る。

イ）情報セキュリティ教育者、専門家等に係る人材育成・訓練（内閣官房、総務省、文部科学省及び経済産業省）

情報セキュリティ教育者、専門家等に係る人材育成・訓練の機会を増加させるとともに、これらの者の重要性を社会全体が認識し、職業上の地位と評価が確保されるようなキャリアパスの構築に向けた戦略を検討する。

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

2006年度に実施する「高セキュリティ機能を実現する次世代OS環境の開発」における部分的成果の実証利用を2007年度から積極的に図るとともに、基盤機能拡大に向けた暗号化通信、ID管理及び資源管理等の開発を産学官の連携により推進する。また、その実証結果を踏まえ、電子政府での利用を前提とした本格的な高セキュリティ機能を実現するOS環境の開発を射程に、OS等システム導入における政府調達仕様の策定も併せて推進する。

エ）開発者向け啓発資料の普及（経済産業省）

情報関連事業者が、情報セキュリティ機能をビルトインしながら製品開発・供給を行うことができるような環境を整備するため、独立行政法人情報処理推進機構において組込みソフトウェアに係るセキュリティ対策のポイント集等をとりまとめ、普及等を図る。

オ）安全なWebサイトが備えるべき基準の構築（経済産業省）

Webサイトを構築する際の統一的なセキュリティ要件をとりまとめ、安全なWebサイトが備えるべき基準の策定を目指す。

カ）暗号モジュール試験及び認証制度の本格運用の推進（経済産業省）

安全性の高い暗号モジュールの活用を推進するため、独立行政法人情報処理推進機構の運用するIT セキュリティ評価及び認証制度を拡充等した暗号モジュールの認証に係る枠組みについて、本格運用の開始を図る。

キ）サイバー犯罪に対する捜査能力の総合的底上げ（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、不正指令電磁的記録の作成等に適切に対処するためのシステムや、電磁的記録解析用資機材等の整備・高度化を進める。また、デジタルフォレンジックに係る体制の強化・整備、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の実施、国際連携の推進その他のサイバー犯罪の取締りのための取組みを効果的かつ効率的に実施するとともに、捜査能力の底上げのための整備を推進する。

ク）情報処理基盤の安全性等の確保（経済産業省）

日々進化する脅威、新たに発見される脆弱性に対して、情報システム及びソフトウェアの安全性等を確保するため、迅速な情報共有、脆弱性対応策の速やかな提供、時代に即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。

また、急速に変化しつつある企業の組織体制、新たな法制度等の動きを踏まえ、

適切な組織的管理策・ガイドラインの提供等を通じ、我が国企業の情報セキュリティの向上を図る。

ケ）情報通信分野に対する新たな情報セキュリティ脅威への対処（総務省）

情報通信ネットワークの安定運用を継続的に確保するため、新たな情報セキュリティ脅威に対し、即時かつ的確な対応を図るための状況調査を実施するとともに、必要な研究開発・技術開発等を推進する。