資料2（2）

第１次提言

情報セキュリティ問題に取り組む政府の機能・役割の見直しに向けて

2004 年 11 月 16 日

高度情報通信ネットワーク社会推進戦略本部
情報セキュリティ専門調査会

情報セキュリティ基本問題委員会

第１次提言の概要

情報セキュリティ問題に取り組む政府の機能･役割の見直しに向けて

2004 年 11 月 16 日

1. 情報セキュリティ問題全般における第1次提言の位置付け

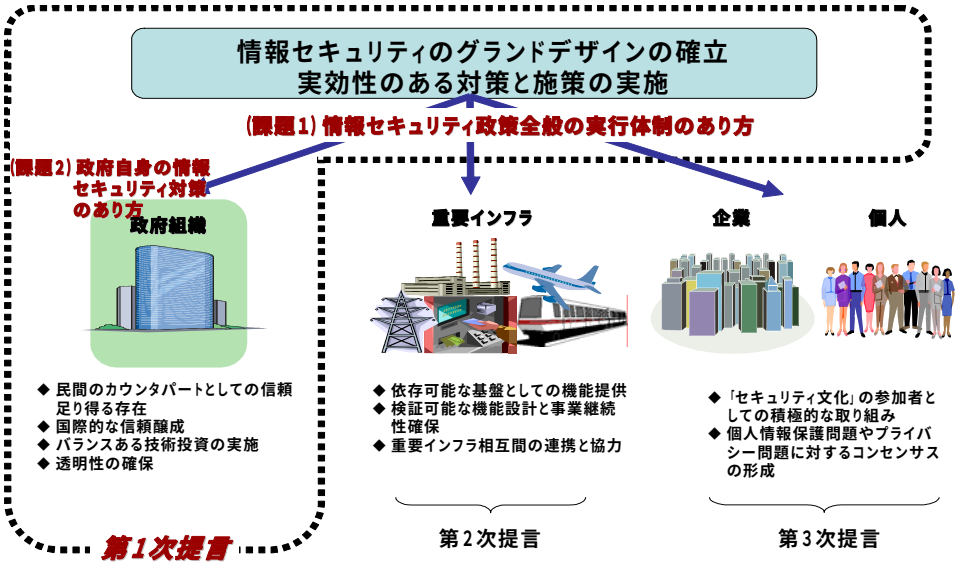
(1)第1次提言の位置付け

○ 情報セキュリティ基本問題委員会は、まず最も喫緊に着手すべき課題として、「政府の情報セキュリティ問題への取組み」に関する 2 つの課題について検討し、「第1次提言」としてとりまとめ。

(課題1) 情報セキュリティ政策全般の実行体制のあり方の検討

(課題2) 政府自身の情報セキュリティ対策のあり方の検討

○ それぞれの課題につき、今後 3 年間 (2007 年中まで) に実現すべきプランとして構成。



「情報セキュリティ基本問題委員会」の検討課題の全体像

(2)基本理念

○ 情報技術 (IT) は、今や社会全体に浸透し、産業･経済活動から国民生活、行政活動に至るまで積極的に利用され、新たな社会基盤として発展。この社会基盤の健全な発展に必要不可欠なのが、情報セキュリティの確保であるとの位置付けの下、政府が情報セキュリティ問題に取り組む場合、次の9つの共通理念を持つことが必要。

①全ての構成要素を守る

②「後付け型」から「ビルトイン型」へ転換する

③合理性と変化への対応を確保する

④フェールセーフの概念を取り入れる
⑤適法性、透明性、人権保障を確保する
⑥持続可能な構造を作り出す
⑦英知を集約し共有する
⑧役割分担の意識を持つ
⑨影響度に応じた優先度設定を行う

○ 加えて、安全保障・危機管理等との関係について、綿密かつ十分な議論が必要。

2．情報セキュリティ問題に取り組む政府の機能と役割の見直し

2．1．情報セキュリティ政策全般の実行体制のあり方（課題1）

(1)基本認識－我が国としての「情報セキュリティに関する基本戦略」の必要性－

○ 各分野における情報セキュリティ問題への取り組みの必要性が高まってきたことに伴い、政策を実施する各府省庁が、それぞれの視点で関連施策の推進を強化。

○ 一方で、これらの総合調整等を行うための内閣官房情報セキュリティ対策推進室や、それが事務局となる情報セキュリティ対策推進会議、情報セキュリティ専門調査会及びその中に本基本問題委員会が設置され活動を実施。しかしながら、担当省庁を超えた我が国としての基本戦略は十分とは言い難い状況。

○ したがって、各担当府省庁における施策の強化が一層必要であるとともに、情報セキュリティに関する我が国としての基本的な戦略を策定していくことが必要。

○ すなわち、現在 e-Japan 重点計画等の一部となっている「情報セキュリティ」（高度情報通信ネットワークの安全性及び信頼性の確保）の部分を個別重点的に捉え、独自の戦略を構築していくべき時期。

(2)望ましい具体的方策

○ 関連府省庁の施策を総合的に把握・調整した上で「情報セキュリティに関する基本戦略」を策定し、それを実行に移す体制を政府内に実装していくことが必要。

①情報セキュリティに関する基本戦略（中長期計画及び年度計画）の策定
②基本戦略策定のための情報収集・分析機能の強化
③基本戦略に基づいた関連施策（予算も含む）の事前評価の実施
④事後評価の実施と結果の公表
⑤広報機能の充実

○ 上記体制の中には、政府が実施する情報セキュリティに関する研究開発投資の有効性評価を行う仕組みを内包することが必要。

2．2．政府自身の情報セキュリティ対策のあり方（課題2）

(1)基本認識－政府の対策のための「統一的・横断的な総合調整機能」強化の必要性－

○ 国民の情報や国家機密を保有する政府の情報セキュリティ対策は、国民の財産・権利を保護し、国際関係上の我が国の信頼感を確保するという責務が表裏一体で求められることから、政府全体として、高い対策レベルを確保することが必要。

○ したがって、各府省庁が各々の対策を講じることに加えて、その対策を促進し、かつ、政

府全体として対策レベルを向上させていくための、「統一的・横断的な総合調整機能」が必要。

○ これまでも「統一的・横断的な総合調整機能」として、内閣官房の情報セキュリティ対策推進室が活動を実施してきたが、その一つの出発点が、外部からの攻撃による政府関係機関のホームページ改ざん事案であったことも要因となり、急激に変化する以下のような視点に対応できていないのが現状。

①内部から行政上重要な情報が漏えいし、改ざんされ、又は破壊される可能性への対応。

②情報システムの設計や設定の誤り等の運用上の過失によって情報システムに障害が発生する可能性への対応。

③政府内の情報管理構造の構築、情報セキュリティに取り組む人材の育成、研究開発の促進、啓発活動までを対象とする必要性への対応。

○ 以上より、各府省庁が各々の対策を強化していくことに加えて、「統一的・横断的な総合調整機能」を強化していくことが必要。

(2)望ましい具体的方策

○ 各府省庁の対策に対する「統一的・横断的な総合調整機能」の強化策として、内閣官房が以下の方策を講じることが必要。

①総合的な対策促進の支援

- 「政府統一的な安全基準」を策定し、それに基づく各府省庁の評価を実施。
- 「政府統一的な安全基準」の定期的に見直すとともに、そのための情報収集・分析を実施。
- 評価結果に基づいた各府省庁への対策促進の勧告を実施するとともに、それに伴う必要な予算を措置。
- 希望する各府省庁の安全な情報システム設計を支援。

②情報セキュリティ関係事案対処に関する対策の支援

- 脆弱性情報や攻撃の予兆等の早期情報収集とその分析機能の強化を実施。
- 同時に、事案発生時に各府省庁にいかなる影響が発生するかという点についての平素からのリスク分析に必要な、各府省庁の業務・情報システム等についての常時の実態調査を実施。
- 各府省庁において情報セキュリティ関係事案が発生した際の、被害情報等の把握と原因分析に関する機能を強化。
- 官民の情報セキュリティ関係事案対応機関（警察庁サイバーフォース、NICT、IPA、

Telecom-ISAC、JPCERT/CC 等）や製品開発者等との間での連携を強化。

- 各府省庁での事案発生時における事案対処ガイドラインを策定するとともに、府省庁における事案対応チーム（IRT: Incident Response Team）の編成を支援。

③政府職員の人材育成・人材確保に関する支援

- 各府省庁における情報セキュリティ対策に従事する専門職の設置を支援。長期的かつ体系的な人材育成が可能となるよう、各府省庁における人事政策への反映を支援。
- 政府内における情報セキュリティに関する専門性の高い人材について、どの府省庁にどのような人材が存在するかを把握し、外部からの人材確保、あるいは政府内での人材育成の必要性を明確化。
- 大学を中心とした教育機関での人材育成の取り組みを体系化するとともに、政府職員になるというキャリアパスを創出。
- 政府職員（エンドユーザー）に対する継続的なOJT等を実施するとともに、幹部職員の意識を向上させるためのプログラムを実施。

3．実現のための行動計画

3．1．新たな体制の整備－「情報セキュリティ政策会議（仮称）」と「国家情報セキュリティセンター（仮称）」の設置

(1)体制整備の方向性

○ 上記 2.1.(2)及び 2.2.(2)に示した「望ましい具体的方策」を実現するため、具体的には、1)政府全体としての「情報セキュリティに関する基本戦略」を策定・実行する機能を実装し、2)政府の対策のための「統一的・横断的な総合調整機能」を強化するため、新たな体制を整備することが適当。

○ 基本戦略の策定、各府省庁の政策の事前評価・事後評価及び政府統一的な安全基準の策定とこれに基づく評価の結果による勧告は、内閣の立場から行うことが適当。したがって、内閣に置かれたIT戦略本部に「情報セキュリティ政策会議（仮称）」を設置してこれを行うことが適当。

○ これ以外のものについては、現在の内閣官房情報セキュリティ対策推進室の機能を強化・発展させ、「国家情報セキュリティセンター（仮称）」を設置して政府全体の総合調整等の一環としてこれを行うことが適当。

○ なお、それぞれの体制整備に際しては、1)国の安全保障に関わる場合もあるため、整備される体制においては十分なセキュリティの管理が求められること、2)各府省庁が有する情報セキュリティに関する機能を最大限に活用しつつ、業務の円滑な遂行に向け、これら府省庁との密接な連携及び十分な調整を図ることに留意が必要。

(2)「情報セキュリティ政策会議（仮称）」の業務

○ 「情報セキュリティ政策会議（仮称）」は以下の業務を実施することが適当。

①情報セキュリティに関する基本戦略（中長期計画及び年度計画）を策定。

②基本戦略に基づいた事前評価（予算を含む）を実施するとともに、年度途中で緊急性のある事業費等に活用する「情報セキュリティ推進調整費（仮称）」を配分。

③政府統一的な安全基準を策定し、これに基づく評価の結果にしたがって、各府省庁の情報セキュリティ対策に対する勧告を実施。

④各府省庁の情報セキュリティ施策及び対策の事後評価を実施するとともに、その結果を公表。

(3)「国家情報セキュリティセンター（仮称）」の業務

○ 「国家情報セキュリティセンター（仮称）」は以下の業務を実施することが適当。

○ なおここで提示する「国家情報セキュリティセンター（仮称）」の業務は、本提言の範囲内

でのものであり、今後検討を行う「重要インフラの情報セキュリティ対策」等について、本センターにて取り扱うことが必要な業務が付加される可能性に留意。

①基本戦略の立案（10 名程度）

- 「情報セキュリティ政策会議（仮称）」の事務局として、各府省庁が行う情報セキュリティに関する政策の総合的把握及び総合調整を行い、我が国全体の情報セキュリティに関する基本戦略（中長期計画及び年度計画）を立案。
- この際、計画の策定に資するため、常時国内の状況、国際的な状況（他国の政策を含む）等について情報収集・分析を実施するとともに、各府省庁の政策実施に資するため、情報収集・分析結果を政策の基盤として各府省庁に提供。
- 政策事項に関する国際的窓口及び戦略的広報を実施。
- 上記の業務を遂行するために、常勤で 10 名程度の人員が必要。

②政府機関の総合対策促進（30 名程度）

- 「情報セキュリティ政策会議（仮称）」が策定する政府統一的な安全基準案の作成とそれに基づく評価作業の実施、評価に基づいた勧告案の策定と必要な対策予算確保の支援を実施。この際、安全基準の定期的な見直しのために必要な情報収集・分析を実施。
- 政府職員の人材育成・人材確保のための支援、希望する各府省庁に対する安全なシステム設計の支援を実施。
- 上記の業務を遂行するため、常勤で 30 名程度の人員が必要。

③政府機関の事案対処支援（20 名程度）

- 各府省庁における事案対処に関するガイドラインの策定とその見直しを実施。
- 各府省庁に対して脆弱性情報等早期警戒情報を提供するための起点として機能。その際、各府省庁にいかなる影響が発生するかという点についての、平素からのリスク分析を行うために必要な、各府省庁の業務・情報システム等についての常時の実態調査を実施。
- 各府省庁における被害情報等の把握と原因分析を実施。
- 関係機関（警察庁サイバーフォース、NICT、IPA、Telecom-ISAC、JPCERT/CC 等）との連携を強化。
- 上記の業務を実施するため、常勤で 20 名程度の人員が必要。

(4)実現までのマイルストーン

○ 2 年後（2006 年中）に、上記の業務全体を実現できることを当面の目標とし、来年度

（2005 年度）の可能な限り早期に、法的権能の整理・付与が不要と考えられる以下の業務について、活動を開始。

- 「情報セキュリティ政策会議（仮称）」の業務のうち、1)予算配分の方針を決定する業務、2)各府省庁に対して対策の勧告を行う業務、3) 情報セキュリティ関連研究開発・技術開発についての事前評価を一元的に行う業務以外の業務。
- 「国家情報セキュリティセンター（仮称）」の業務のうち、上記 1)2)3)の事務局業務以外の業務。

3．2．制度等の創設・見直し

○ 「情報セキュリティ政策会議（仮称）」及び「国家情報セキュリティセンター（仮称）」の体制及び機能整備にあわせて以下の関連制度等の検討を行い、2005 年度中の可能な限り早期に結論を得ることが適当。

①情報セキュリティの観点から、現在の公的研究助成等資金の見直しを検討。

②各府省庁が情報セキュリティ担当者のためのキャリアパスを新設すべく支援。同時に、同職に必要な専門性を養成するための研修を実施。

③情報セキュリティ対策モデル事業及び優秀職員に対する表彰制度の創設を検討。

④大学を中心とした教育機関での人材育成の取り組みの体系化を促すべく、「情報セキュリティ奨学金（仮称）」の創設を検討。

情報セキュリティ基本問題委員会委員名簿

【委員長】

金杉　明信	日本電気㈱代表取締役社長

【委員】

伊藤　泰彦	ＫＤＤＩ㈱取締役（執行役員専務）＜委員長代理＞
後藤　滋樹	早稲田大学教授
寺島　実郎	㈱三井物産戦略研究所所長
中村　直司	㈱NTT データ代表取締役副社長
村井　純	慶應義塾大学教授

（五十音順）

情報セキュリティ基本問題委員会第1分科会委員名簿
（政府機能・役割検討分科会）

【座長】

土居　範久	中央大学理工学部教授

【委員】

稲垣　隆一	弁護士
大木栄二郎	IBM ビジネスコンサルティング㈱チーフセキュリティオフィサー
佐々木良一	東京電機大学工学部教授
中尾　康二	KDDI㈱技術開発本部情報セキュリティ技術部長
夏井　高人	弁護士／明治大学法学部教授
松尾　明	中央青山監査法人代表社員
三輪　信雄	㈱ラック代表取締役社長

（五十音順）

第1次提言までの検討の経緯

【情報セキュリティ基本問題委員会】

2004年7月27日　　第1回会合

本委員会の活動方針（テーマ及びスケジュール）について

2004年9月6日　　第2回会合

（1）第1分科会の設置と開催状況について

（2）第1分科会の検討状況報告（中間報告の収受）

2004年10月26日　　第3回会合

「第１次提言（案）」の検討

【情報セキュリティ基本問題委員会第1分科会】

2004年8月6日　　第1回会合

（1）第1分科会の活動方針について

（2）「政府の政策・施策実施体制のあり方」及び「有効性の高い政府自身の情報セキュリティ対策のあり方」についての具体案の検討（その1）

2004年8月23日　　第2回会合

「政府の政策・施策実施体制のあり方」及び「有効性の高い政府自身の情報セキュリティ対策のあり方」についての具体案の検討（その2）

2004年9月1日　　第3回会合

「第1分科会中間報告案」の検討

2004年9月17日　　第4回会合

（1）「中間報告」に対する基本問題委員会からの指摘の反映方法について

（2）「中間報告」の詳細化とマイルストーン設定について

2004年10月8日　　第5回会合

「第1次提言素案」の検討

2004年10月19日　　第6回会合

「第1次提言（案）」の検討

第 1 次提言

情報セキュリティ問題に取り組む政府の機能・役割の見直しに向けて

2004 年 11 月 16 日

高度情報通信ネットワーク社会推進戦略本部
情報セキュリティ専門調査会

情報セキュリティ基本問題委員会

目次

はじめに

2000 年に制定された高度情報通信ネットワーク社会形成基本法、ならびに、2001 年の高度情報通信ネットワーク社会推進戦略本部（以下、本提言において、「IT 戦略本部」という）による「e-Japan 戦略」では、我が国の国民がインターネット等の高度情報通信ネットワークを通じて自由かつ安全に多様な情報または知識を活用することができる環境を構築し、これによりあらゆる分野における創造的かつ活力ある発展を希求した。「e-Japan 戦略」に掲げた目標は、内閣によって強力に推進され、官民を挙げた様々な取り組みの結果、2001 年当時、政府が目標とした「2005 年に世界最先端の IT 国家の実現」が実現されようとしている。この取り組みの基礎には、IT 国家実現のために、方向性について e-Japan 戦略という形で決定を行い、その実行体制として内閣を中心として英知を結集し、各府省庁、民間セクタの協力の中で持続的な発展を遂げる機構を作り出し、着実な発展を達成してきた。さらに、近年は諸外国が経験をしたことがない領域での挑戦が始まっており、その成果をどのように他国に示していくかという点でグローバル社会に対する責任を負うようになってきている。事実、我が国のブロードバンド環境の発展、そしてその環境にまつわる様々な事象と解決方法については、世界中が注目している。このような中で我が国は、より一層の発展を e-Japan の取り組みの中で達成していかなければならない。

情報技術（IT）は、今や社会全体に浸透し、産業・経済活動から国民生活、行政活動に至るまで積極的に利用されている。新たな社会基盤としての情報システムが高まる中、この社会基盤の健全な発展に必要不可欠なのが、情報セキュリティの確保である。高度情報通信ネットワーク社会形成基本法でも、国民がネットワークを安全に利用できることが求められている。さらには、安心して利用できることも必要とされている。特に近年の個人情報保護に対する国民の期待の高まりと、国民の日々の生活での高度情報通信ネットワークへの依存度の急上昇は、高度情報通信ネットワーク社会の持続的な発展を下支えするための情報セキュリティの役割が近年急速に拡大していることを意味する。これは単に、外部の意図的な行為から高度情報通信ネットワークが頑強であることだけでなく、情報システムの不具合が我が国のさまざまな活動に影響を与えるリスクを低減させることも必要である。さらに、情報技術（IT）の利用は既存の重要インフラの中でも拡大しており、情報技術（IT）、あるいは、情報システムを中核に相互依存の構造が生み出されている。この相互依存の構造により、情報システムの不具合が単純な経済的損失を生み出すだけでなく、国民の生命、財産に重大な影響を与えるリスクも生じ始めている。このため、情報セキュリティの確保は、官民問わず喫緊の課題となっている。

一方、現在の情報基盤は、単一の組織、あるいは、地域・国に閉じたものとは限らず、広範囲な相互接続により生み出された国際的、かつ、巨大な情報システムとして捉えることができる。この状況を背景に、国際的にも情報セキュリティの確立は、安心・安全を利用者が体

感できるIT社会の実現に不可欠の課題であり、安全保障・危機管理等の観点からも国全体として早急に取り組みを開始すべき課題である。我が国の情報基盤が真に依存可能な基盤として機能するための取り組みでは、情報基盤に投入される新しい技術が与える影響、さらに、その展開領域の変化を正しく理解しつつ、情報セキュリティ確保の取り組みが継続的に実施されることが必須である。さらに、情報基盤に関わる全ての当事者において、情報セキュリティ確保のための取り組みが努力されなければならない。この取り組みは技術領域に限定されるのではなく、各種社会制度の対応、情報セキュリティに関する理解の促進、さらに、さまざまな手法を使ってのリスク軽減への取り組みまでが含まれる。また、その当事者は、公共セクタだけではなく、民間セクタにおいても、また、個人のレベルにおいても実施されるべきものであり、社会全体が情報セキュリティに対して取り組むことが必要となる。これこそが、2002 年に勧告された OECD の「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」で示されたセキュリティ文化の実装に他ならない。

これまでも、IT戦略本部では、重点政策分野の一つに情報セキュリティ対策を掲げるとともに、民間部門における情報セキュリティ対策及び普及啓発、電子政府に代表される行政機関で構築・運用される情報システムにおける情報セキュリティ対策の推進・徹底、情報セキュリティに係る制度・基盤の整備や研究開発の推進等を行うこととしてきた。しかしながら、我が国の現状を顧みれば、多くの企業や行政機関を含めた各種組織における情報セキュリティ確保への取り組みの不足、相次ぐ重要情報漏洩事件の発生、さらに、重要インフラのシステム障害の発生にみられるように、情報セキュリティに対する国民の意識が低いだけでなく、具体的な対策についても民間セクタや公共セクタにおいて後手に回っているのが現状と言える。この背景には、IT推進政策に比べ、情報セキュリティについては、情報セキュリティの基本政策の不在や、政府・企業・個人の各レベルでの責任の所在と行動方針の提示など、本質的かつ基本的な問題の持続的検討が置き去りにされてきたと言わざるを得ない。また、社会全体での取り組みの調和の取れた調整と実施が不足していたということも言えるであろう。

こうした問題認識の下で、本年7月27日、IT戦略本部情報セキュリティ専門調査会の下に「情報セキュリティ基本問題委員会」が設置され、IT社会の基盤となる情報セキュリティに関する基本的な課題について、専門家の知見を集約して「国家としての戦略」を策定するとともに、実施可能な対策を、優先順位を付けて具体的に提示するための検討を開始した。

本委員会では、社会基盤を形成する主体に注目して、情報セキュリティのあり方を検討する方式を採用した。まず、本委員会では、政府そのものを主体と捉え、①政府の情報セキュリティ政策・施策実施体制のあり方、②有効性の高い政府自身の情報セキュリティ対策のあり方、③情報セキュリティ施策推進の国家的拠点の強化とその方策のあり方について、検討を行った。これは「政府」そのものが社会にとっての基盤サービスを提供する主体としてとら

え、政府活動の継続性確保を情報技術（IT）の視点から見直すことを意味する。

本第 1 次提言の策定にあたっては、本委員会の下に、第 1 分科会（政府機能・役割検討分科会）を組織し、案の作成を付託することになった。第1分科会では、短期間、かつ、集中的な審議を行い、今後 3 年間で実施に移すことを前提に、その具体的な方策を明らかにすることに取り組んだ。

本委員会としては、この第1次提言を受けて、IT戦略本部及び政府が積極的に情報セキュリティ確保のための政策を決定し、世界最高水準の IT 国家に相応の情報セキュリティ確保が実現された社会を作り出していくことを切に願う。

2004 年 11 月

高度情報通信ネットワーク社会推進戦略本部
情報セキュリティ専門調査会
情報セキュリティ基本問題委員会委員長
金 杉 明 信

情報セキュリティ基本問題委員会委員名簿

【委員長】
金杉　明信　　日本電気㈱代表取締役社長

【委員】
伊藤　泰彦　　ＫＤＤＩ㈱取締役（執行役員専務）＜委員長代理＞
後藤　滋樹　　早稲田大学教授
寺島　実郎　　㈱三井物産戦略研究所所長
中村　直司　　㈱NTT データ代表取締役副社長
村井　純　　慶應義塾大学教授

（五十音順）

情報セキュリティ基本問題委員会第１分科会委員名簿
（政府機能・役割検討分科会）

【座長】
土居　範久　　中央大学理工学部教授

【委員】
稲垣　隆一　　弁護士
大木栄二郎　　IBM ビジネスコンサルティング㈱チーフセキュリティオフィサー
佐々木良一　　東京電機大学工学部教授
中尾　康二　　KDDI㈱技術開発本部情報セキュリティ技術部長
夏井　高人　　弁護士／明治大学法学部教授
松尾　明　　中央青山監査法人代表社員
三輪　信雄　　㈱ラック代表取締役社長

（五十音順）

第1章　情報セキュリティ問題全般における第1次提言の位置付け

本章では、情報セキュリティ問題全般における第1次提言の位置付け及び基本的な考え方を提示する。

1．1．政府における情報セキュリティ問題への取り組みのあり方

(1) 政府における「情報セキュリティ」に関する二つの立場

政府において情報セキュリティを議論するときには、二つの異なる立場が存在することを明確に意識する必要がある。

一つが、行政権を行使し、我が国の全ての社会領域の活動に影響を与える組織として、情報セキュリティを議論する立場である。この場合、各社会領域における情報セキュリティのあり方を考え、その領域を対象とした行政活動を設計することが、主な論点となる。別の言い方をすれば、情報セキュリティ政策を考える立場である。

もう一つが、行政活動を行う組織として、自組織における情報技術（IT）活用での情報セキュリティの取扱いを議論する立場である。この場合、政府内に存在する情報システムにおける情報セキュリティのあり方を考え、組織としての対応方針と具体的な方策を議論することが主題となる。別の言い方をすれば、政府自身の情報セキュリティ対策を考える立場と言うことができる。

(2) 共通理念

情報セキュリティを議論する場合には、政府においては異なる二つの立場があるものの、政府での情報セキュリティの取り組みでは次の共通理念を持たなければならない。

①全ての構成要素を守る

社会における情報システムの果たす役割が急速に拡大する中、単にハードウェアやOS、アプリケーション実行環境を守るという視点だけでは不十分であるのは明らかである。我が国の官民さまざまな領域で利用されている情報システムにおいて、情報システム及び情報資産を用いて実施される業務とそこから発生する権利や利益を守るという観点から、全ての構成要素、すなわち、(1)情報システムそのもの、(2)情報システム上に蓄積される情報資産、(3)情報システム間でやりとりされるトランザクション、さらに、(4)情報システムの運用の４つの構成要素を対象として、その防護方策を考える。この際、防護方策は、単に技術的手法だけに限定するだけでなく、非技術的手法にも視野を広げ、総合的な対応を実行するとともに、必要に応じて、意図的な行為だけでなく、事故や障害についても対

象とすることが望ましい。

②「後付け型」から「ビルトイン型」へ転換する

2002 年に勧告された OECD の「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」で述べられているように、情報システムやネットワークの構築後に情報セキュリティを勘案することは困難であり、設計段階で情報セキュリティを組み入れることが強く望まれる。加えて、基本となる考え方は技術革新の進展や社会状況の変化に機敏に対応できることが必要である。今後のユビキタスネットワーク社会においては、データと情報処理が分散する傾向が強まることを踏まえ、「後付け型」からの完全脱却と、「ビルトイン型」の考え方を政府内に根付かせなければならない。

③合理性と変化への対応を確保する

情報化社会の姿は、年々急速に変化を遂げてきている。情報基盤の構築で使われる技術そのものは、数多くの技術革新によって短期間に大きく変化しており、同時に情報基盤が利用される領域が年々拡大していることにより、質的にも量的にも大きな変化を引き起こしてきた。刻一刻と変化する情報基盤を対象として情報セキュリティのあり方を考える場合には、「ビルトイン型」の考えに基づいた設計を行うと同時に、情報基盤を継続的に評価し、その評価に基づいた情報セキュリティを設計し合理性を確保する。さらに、変化に対して的確に対応する取り組みを実行する。

④フェールセーフの概念を取り入れる

情報セキュリティの問題を考える場合には、フェールセーフ[1]の考え方を取り入れた設計をすることは必須である。どれだけの情報セキュリティ対策を施したとしても、そこに問題が発生する確率をゼロにすることは不可能である。この意味で、問題発生確率をゼロに近づける努力をするとともに、問題発生時の影響を最小限に食い止めるための方策も同時に設計･実装する。

⑤適法性、透明性、人権保障を確保する

法治国家の我が国においては、政府の活動には全て法的根拠が必要である。また、政府の活動では、透明性を確保し、国民に対する説明責任を果たさなければならない。さらに、政府の活動は、人権保障の確保の観点から、活動を設計することが必須である。

[1] あらかじめ事故が起こることを想定し、被害を最小限にとどめるよう設計しておくという安全思想のこと。

情報セキュリティに係る活動においても、例外なく適法性、透明性、人権保障を確保しなければならない。また OECD ガイドラインで述べられている「民主主義の原則」の確保に留意することが必要である。

⑥持続可能な構造を作り出す

我が国の社会が情報基盤に依存し続ける限り、情報セキュリティ問題への取り組みは、基本的に終わりの無い事業である。情報セキュリティ問題への取り組みは一過性のものとせず、遅滞なく継続的に取り組みを実施できる持続可能な構造を作り出すことが必須である。持続可能な構造を強固なものにするために、継続的な人材育成、予算等の資源の十分な確保と運用を実現する。

さらに、この継続的な取り組みは、情報セキュリティ確保の水準向上を不断に指向する設計でなければならない。

⑦英知を集約し共有する

情報セキュリティ問題に取り組む場合には、技術領域から非技術領域までの広い視点を持ち、周到かつ戦略的な方策を生み出さなければならない。情報システムに対する脅威が人為的なものである場合、脅威を生み出す集団よりも技術的にも運用的にも高いレベルの知見を軸として防護方策を作成しなければ、情報システムを守ることは到底できない。この観点から、情報セキュリティに資する英知を集約する構造を作り、同時に得られた知見を共有する基盤を作り出す。

⑧役割分担の意識を持つ

情報セキュリティが対象とする構成要素は、政府、地方公共団体、重要インフラ、企業、個人といった異なる特性を持った当事者によって運用されている。当事者の特性の違いを理解し、それぞれの当事者の使命と責任を明らかにするとともに、当事者間の協力・連携を円滑にするための基盤整備を行う必要がある。これにより、全ての当事者での情報セキュリティ対策が充実することを強く求めなければならない。

⑨影響度に応じた優先度設定を行う

情報セキュリティ問題に取り組む場合には、構成要素を取り巻く環境の変化及び脅威の変化によって、個々の脅威が顕在化した場合の影響度が大きく変化することに留意しなければならない。影響度の変化を考慮した方策の実施優先度設定と、その継続的な見直しが必須である。

(3) 情報セキュリティと安全保障・危機管理等との関係

政府が取り組む情報セキュリティの問題については、綿密かつ十分な議論が必要な事項が存在する。安全保障・危機管理等と情報セキュリティとの関係である。

①重要インフラにおける情報セキュリティ対策

一つの大きな課題が、サイバーテロ対策である。情報セキュリティ対策推進会議が2000年12月15日付けで取りまとめた「重要インフラのサイバーテロ対策に係る特別行動計画」では、我が国に対するサイバーテロの脅威増大を指摘し、特に重要インフラ分野[2]における情報セキュリティ対策水準の向上、官民の連絡・連携体制の確立・強化、官民連携によるサイバー攻撃の検知と緊急対処、情報セキュリティ基盤の構築、国際連携などについて、具体的な行動計画を策定している。また、この行動計画では、内閣官房を中心に、官民の緊密な協力、計画の実行を求めている。

②安全保障・危機管理の観点からの情報セキュリティの位置付け

我が国の社会構造は情報技術(IT)によって大きく変わりつつあり、大部分の社会経済活動が情報技術(IT)によって支えられる状況になってきた。このような状況は、重要インフラ分野だけではなく、社会全体における情報セキュリティの強化・高度化が必要不可欠であることを意味する。さらに、我が国の社会経済活動は、地理的に我が国の領土内に閉じたものではなく、国際的な広がりと厚みを持つようになっている。このことは、単に国内の情報セキュリティの強化・高度化だけでは不十分であり、国際的な視点に立った効果的な情報セキュリティ政策の立案・実施が必要であることも意味する。

このような状況を踏まえ、安全保障・危機管理の枠組みでの情報セキュリティの位置付けについて考えると、例えば、安全保障の観点からは、情報技術(IT)を活用して我が国が行う社会経済活動に対する脅威に対峙する一連の合理的な取り扱いを、人権保障と適法性を確保しつつ設計することを含むと考えることができる。また、危機管理の観点からは、我が国の社会経済活動基盤に深く組み込まれた情報技術(IT)の基盤の持つ脆弱的な構造やそこから惹起される恐れがある危機の発生を排除し、また、万が一陥っても被害を最小限度に抑えるようあらかじめ適切に準備することであると考えることができる。すなわち、社会経済活動の広範囲なIT化を背景として、幅広い意味での安全保障・危機管理の見地からの情報セキュリティの位置づけについての議論が行われるべきである。

---

[2]平成12年12月15日付けで取りまとめた「重要インフラのサイバーテロ対策に係る特別行動計画」では、対象とする重要インフラ分野を、当面、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス(地方公共団体を含む)としている。

③サイバー犯罪と情報セキュリティ

高度情報通信ネットワーク社会の実現が進む中、情報システムとネットワークを利用した、いわゆるサイバー犯罪の広がりが大きな問題となっている。この状況に対応するために、関係省庁において様々な取り組みを実施してきた。例えば、警察庁では、2004 年に「警察庁情報セキュリティ政策大系−2004」を取りまとめ、活動の充実を図ってきている。前項にも述べたように、情報技術は社会の隅々まで浸透し、同時に社会経済活動を支えるようになってきている。このような状況を考えれば、サイバー犯罪への総合的な取り組みを充実させることが必要であることは言うまでもない。さらに、サイバー犯罪予防・抑止の観点からの多面的な取り組みを、情報セキュリティに関連する各府省庁の協力の中で政府として取り組むことが必要である。

④情報の戦略的活用

また、情報セキュリティの問題は、情報の収集・分析に基づいた情報の戦略的活用といった面とも密接に関係する問題であり、政府においてこれを行うことは、国家運営の根幹に関わる問題として捉える必要がある。

諸外国に目を転じてみても、各国とも異なる形ではあるが、政府において情報セキュリティ問題を統括的に取り扱う中核機関を整備し、または、整備しつつある（表1参照）。そしてその中において、例えば、米国が安全保障問題を統括的に取り扱う国土安全保障省（DHS）に、また仏国が国防総事務局（SGDN）傘下に、そして韓国が国家情報院（NIC）の傘下に情報セキュリティの中核機関を置いているのは、情報セキュリティの問題を、各種情報収集・分析の機能と連携して取り扱うことを選択している証左と言える。

	構成	情報セキュリティ政策 の策定・推進の中核機関	予算
日本	省庁分散型	**内閣官房情報セキュリティ対策推進室**【18人】	内閣官房のみで約3億5千万円
米国	一省庁集中型	**DHS(国土安全保障省)/IA&IP(情報分析及びインフラストラクチャ保護部)** 【800人】 ・米国の情報セキュリティの中核部分をなす組織。	IA&IPのみで8.3億ドル（約1000億円）
英国	省庁横断型	**NISCC(国家インフラストラクチャ安全調査局)**【70人】 ・9省庁が参加する横断的組織	NISCCのみで7億ポンド（約1300億円）
仏国	中央調整型	SGDN（国防総事務局）【20人】 **DCSSI(情報システムセキュリティ中央局)**【100人】	DCSSIで8百万ユーロ（約10億円）
独国	一省庁集中型	**IT-Staβ(IT幹部)**【50人】 ・情報セキュリティに関し基本的に全てを内務省が管理している。	BSIで約4600万ユーロ（約60億円）
韓国	中央調整型	**情報通信部（MIC）** **国家情報院**	−

表1；情報セキュリティ政策策定・推進の中核機関の各国比較（2004 年7月；経済産業省調査を基に内閣官房作成）

1．2．情報セキュリティ問題への取り組みの遅れ

約 3 年半前の「e－Japan戦略」決定以降、官民を挙げた様々な取り組みの結果、当時、政府が目標とした「2005 年に世界最先端のIT国家の実現」は、現実のものになろうとしている。情報技術（IT）の恩恵が産業・経済活動から広く国民生活に浸透するにつれ、新たな社会基盤としての情報システムの重要性が高まる一方で、情報システムの不具合が経済活動はもとより、国民の生命、財産に重大な影響を与えるリスクも急速に増大していることから、情報セキュリティの確保が焦眉の課題となっている。

国際的に見ても、情報セキュリティの確立はIT社会の実現に不可欠の課題であり、安全保障・危機管理等の観点からも国全体として早急に取り組みを開始すべき課題である。一方、我が国の場合、近年の相次ぐ重要情報漏洩事件や重要インフラのシステム障害の事案にみられるように、情報セキュリティに対する国民の関心が高い一方で、対策については政府も含め後手に回っている[3]のが現状と言える。この背景には、IT推進政策に比べ、情報セキュリティについては、基本政策の視座や政府、企業、個人の各レベルでの責任の所在と何をすべきかなど、本質的かつ基本的な問題の検討が置き去りにされてきたという実態がある。

1．3．情報セキュリティ基本問題委員会の役割と第1次提言の射程

(1) 情報セキュリティ基本問題委員会の役割

こうした中、2004 年 7 月 27 日、IT戦略本部の下に「情報セキュリティ基本問題委員会」が設置され、情報セキュリティに関する基本的な課題について、専門家の知見を集約して「国家としてのグランドデザイン」を策定するとともに、実施可能な対策を優先順位を付けて具体的に提示するための検討を開始した。

情報セキュリティの問題は、政府や重要インフラの対策といった「公的側面」の強い部分への投資と民間部門の投資が全体として効果的に配分され、我が国全体として、「安心・安全」で信頼性の高い基盤が構築されることが必要である。したがって、本委員会が民間専門家の意見を結集し、内閣総理大臣を本部長とし関係閣僚も参加する IT 戦略本部に提言を行うという構造で設計されていることには意義がある。

---

[3] 政府機関の情報セキュリティ対策については、内閣官房が 2003 年に実施した「各省庁情報システムに対する脆弱性検査」の結果（http://www.bits.go.jp/kaigi/suisinkaigi/dai8/pdfs/8siryou2.pdf）においても、水準の高い省庁と低い省庁の格差が大きいことが明らかとなった。また、企業の対策についても、例えば、コンピュータ・ウイルス対策に関する体制整備の国際比較（2003 年；情報処理振興事業協会調査（http://www.ipa.go.jp/security/fy15/reports/virus-survey/documents/2003_virus_oversea.pdf））によれば、対策を行う体制整備を行っている企業の比率は、米国；91.7%、オーストラリア；89.3%、ドイツ；75.4%、台湾；77.8%、韓国；69.6%、日本；66.1%となっており、日本の対策の遅れが指摘される。

(2) 第1次提言の位置付け

本委員会は、情報セキュリティに関する基本的な課題について包括的にグランドデザインを提示することをその役割としているが、テーマを段階的かつ機動的に設定して結論を提示しながら、短期間で実現のプロセスに載せていくとの検討方法をとっている。

そして、まず最も喫緊に着手すべき課題として、以下の 2 つの課題についての検討を行い、「第1次提言」としてとりまとめることとした。

(課題1) 情報セキュリティに関する我が国としてのグランドデザインを確立し、実効性のある対策と施策を実施していくための機能として、政府の体制が、本委員会も含めた現在のもので十分かどうかを検証、すなわち、「情報セキュリティ政策全般の実行体制のあり方」の検討。

(課題2) 情報セキュリティ対策を行うべき一つの主体としての「政府組織」について、その対策のあり方が十分かどうかを検証、すなわち、「政府自身の情報セキュリティ対策のあり方」を検討。

つまり、「情報セキュリティ問題における政府の機能と役割」について包括的に検討を行ったものが、この第 1 次提言となる。今後は、第 2 次提言として、重要インフラにおける情報セキュリティ対策の強化のあり方、第 3 次提言として、個人情報等の情報管理･流通のあり方を含む国民の権利･財産の法的保護等のあり方について検討を行う予定である(図1参照)。

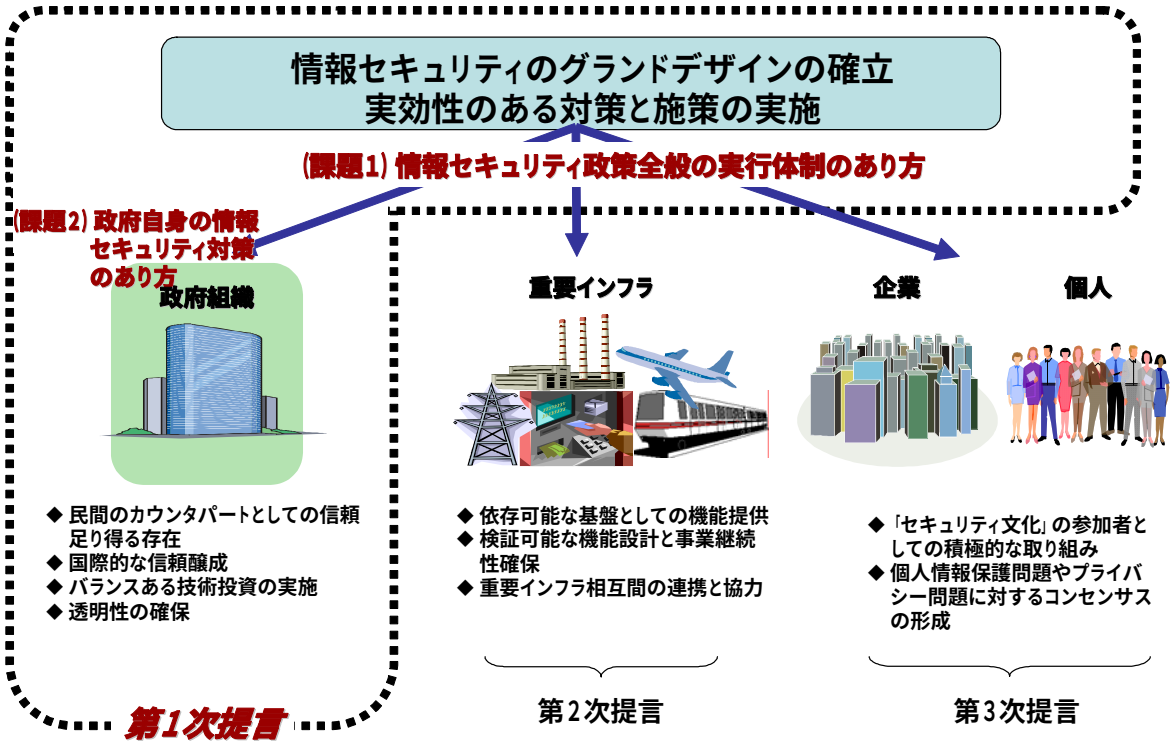


図1;「情報セキュリティ基本問題委員会」の検討課題の全体像

(3) 本提言の目標年限

本提言が描く「情報セキュリティ問題における政府の機能と役割」のあり方は、現在から3年後、すなわち2007年中までに実現すべきプランとして構成することを目指した。

加えて、この提言を真に実現可能とするために、現時点の状態から本提言が描くあるべき状態への移行プロセスを併せて設計する。具体的には、3 年後のゴールに向けてのマイルストーン設定と、プライオリティ設定を行う。また、当然ながら、この提言を実行するためには、財政的な裏付け、各府省庁との調整が発生する。この意味から、各府省庁が持つ役割と機能を最大限活用し、できる限り短期間にあるべき状態に移行するための、具体的な移行プロセス設計を行う。

本提言は次のような構造を持つ。

① 「情報セキュリティ政策全般の実行体制のあり方」(課題 1) 及び「政府自身の情報セキュリティ対策のあり方」(課題 2) について、基本認識と、これを解決するための望ましい具体的方策を提示した上で (**第 2 章**)、

② その実現にあたっての行動計画を示す (**第 3 章**)。

第2章　各課題の解決方策
－情報セキュリティ問題に取り組む政府の機能と役割の見直し－

本章では、前章で示した基本理念に従い、「情報セキュリティ問題における政府の機能と役割」における課題、すなわち「情報セキュリティ政策全般の実行体制のあり方」（課題 1）及び「政府自身の情報セキュリティ対策のあり方」（課題 2）について、現状及び課題についての基本認識と、それを解決するための望ましい具体的方策を提示する。

2．1．情報セキュリティ政策全般の実行体制のあり方

本節では、前章で示した基本理念に基づいて、情報セキュリティに関する我が国としてのグランドデザインを確立し、実効性のある施策と対策を実施していくための機能として、政府の体制が本委員会も含めた現在のもので十分かどうかを検証する。

2．1．1．基本認識

(1) 我が国の情報セキュリティ政策全般の実行体制の現状

各分野における情報セキュリティ問題への取り組みの必要性が高まってきたことに伴い、政策を実施する各府省庁が、それぞれの視点で関連施策の推進を強化している。例えば、ソフトウェア等の脆弱性やコンピュータ・ウイルスの分析、インターネット定点観測や関連技術開発など、それぞれの分野で進めている施策による成果は充実してきていると言える（関連資料参照）。

また、警察庁の「警察庁情報セキュリティ政策大系－2004」[4]、総務省の「情報通信ソフト懇談会セキュリティワーキンググループ最終報告書」[5]、経済産業省の「情報セキュリティ総合戦略」[6]など、それぞれの担当省庁の視点から見た情報セキュリティ問題に関するグランドデザインも作られてきた。

一方で、これらの総合調整等を行うための内閣官房情報セキュリティ対策推進室[7]や、それが事務局となる情報セキュリティ対策推進会議[8]、情報セキュリティ専門調査会[9]及び

---

4 2004 年 8 月 19 日（http://www.npa.go.jp/cyber/sec_taikei/2004.pdf 参照）

5 2003 年 12 月 25 日発表（http://www.soumu.go.jp/s-news/2003/pdf/031225_8_3.pdf 参照）

6 2003 年 10 月 10 日策定（http://www.meti.go.jp/policy/netsecurity/downloadfiles/Strategy_body.pdf 参照）

7 内閣官房情報セキュリティ対策推進室は、「官民における情報セキュリティ対策の推進に係る企画及び立案並びに総合調整を行う」ことを任務として設置（情報セキュリティ対策推進室の設置に関する規則；2000 年 2 月 29 日内閣総理大臣決定）。

8 「関係行政機関相互の緊密な連携の下、官民における情報セキュリティ対策の推進を図る」ために、2000 年 2 月 29 日にIT戦略本部の下に設置。（http://www.bits.go.jp/kaigi/suisinkaigi/0229suisinkaigi.html）

9 IT 戦略本部の専門調査会として 2001 年 1 月 22 日に設置され、「官民における情報セキュリティ対策の推

その中に本基本問題委員会が設置され活動を行っている。しかしながら、担当省庁を超えた我が国としての基本戦略は十分とは言い難い状況にある。

(2) 情報セキュリティに関する国家としての基本戦略の必要性とその視点

こうした中、各担当府省庁において施策の充実が進んでいるソフトウェア等の脆弱性に関する情報の流通、複数の府省庁が協力した関連技術開発や関連法整備などについても、限られた資源を我が国全体として最大活用することの必要性が高まっている。

したがって、各担当府省庁における施策の強化が一層必要であるとともに、情報セキュリティに関する我が国の状況や、関連府省庁の施策を総合的に把握・調整し、かつ、全般的視点から見た際に整備が不足している法制上、制度上の基盤等を補いながら、我が国としての基本的な戦略を策定していくことが求められている。この際、この基本戦略は、安心・安全を利用者が体感できるIT社会の実現に寄与するとともに、安全保障・危機管理等の観点も視野に入れた戦略であることが必要である。

これは、現在 e-Japan 重点計画等の一部となっている「情報セキュリティ」(高度情報通信ネットワークの安全性及び信頼性の確保) の部分を個別重点的に捉え、独自の戦略を構築していくべき時期にきていることを意味する。

なお、基本戦略を立案するにあたって、情報セキュリティ問題に関する国内全般における状況、他国政府の政策を含めた国際状況に関する戦略的な情報収集・分析の機能が、より強化されることが必要であることは言うまでもない。広報戦略の見直しも含めて、強化策の検討を行う必要がある。

(3) 基本戦略の実効性を確保するための機能の必要性

また、策定した基本戦略は、単なる「ビジョン」として提示するものではなく、実効性が確保されなければならない。さらに、基本戦略は一度策定されれば済むものではなく、時代と環境変化に応じた見直しがなされなければならない。

そのために、現在は、IT 戦略本部に対して調査結果を報告し、提言を行うのみである情報セキュリティ専門調査会及び本基本問題委員会の機能や位置付けも含めて、基本戦略の策定とその実行にあたっての体制・権能を見直すべきである。

(4) 情報セキュリティに関する研究開発・技術開発における問題点

なお、情報セキュリティに関する基本戦略の策定・実行にあたっては、その基礎的基盤として重要な、関連研究開発及び技術開発に対する戦略的な取り組みを行う構造とする

進に係る事項の調査」を行っている (http://www.bits.go.jp/kaigi/tyousakai/tyousakaisetti.html)。

ことが必要である。その際、以下の問題点を認識する必要がある。

①政府による成果利用の欠如

情報セキュリティ関連の技術開発に対する投資結果を、最大限、直接政府が使うことが必要である。実用化まで含めた技術開発投資により、その投資が実を結ぶが、実用化までを視野に入れた場合、具体的な研究成果の購入者が必要である。しかしながら、政府は、研究成果の購入者に成り得るにもかかわらず、これまで最終成果物を政府自らが利用することを期待した研究開発投資を行うとの視点が不足していたといえる。

②技術開発・研究開発の対象の偏り

情報セキュリティ関連研究は、高い先端性と網羅性の確保が重要であるにもかかわらず、情報セキュリティ関連の政府研究資金が、学術研究からの視点を中心に配分されている。さらに、基礎領域に対する投資についても、研究と教育との相互作用に注目した投資設計がなければ、持続的な基礎領域の発展が望めない（特に応用数学、システム解析、暗号理論等）。

そもそも、情報セキュリティに関する研究開発・技術開発は行われているが、基礎理論や社会学等との統合的領域への投資が不足している。例えば、緊急対応時における組織行動解析とその最適化への取り組みといった領域に対する研究投資が、我が国では十分に行われているとは言い難い。

また、犯罪捜査や軍事関連と見られる研究に対して、十分に投資することが難しい。大学や多くの研究機関は、犯罪捜査、軍事関連技術開発に対する研究資金受け入れをしていないか、あるいは、受け入れられない状態となっている。

さらに、個別技術に偏っており、統合技術に対する投資ができていない。例えば、暗号技術などへの投資は行われても、暗号等のさまざまな技術を統合したセキュアな情報システム・アーキテクチャ開発等への投資は不十分と言わざるを得ない。

2．1．2．望ましい具体的方策

以上の基本認識を踏まえると、政府の情報セキュリティ政策推進において、以下の機能を政府内に実装していくことが必要である。

(1) 情報セキュリティに関する基本戦略の策定及び実行を行うための機能の実装

各担当府省庁における情報セキュリティ関連施策の強化が一層必要であるとともに、情報セキュリティに関する我が国の状況や、関連府省庁の施策を総合的に把握・調整し、か

つ、全般的視点から見た際に整備が不足している法制上、制度上の基盤等を補いながら、我が国としての基本的な戦略を策定し、これを実行に移すための機能を実装する。

①情報セキュリティに関する基本戦略（中長期計画及び年度計画）の策定

情報セキュリティに関する我が国全体としての基本戦略を策定する。基本戦略としては、まず、中長期的な計画を策定する。さらに、情報セキュリティ問題を巡る急激な環境変化に追従するために、1)中長期計画の継続的な見直しと改善を行う母体を恒常的に政府内に有し、硬直的な執行とならない体制を確保する。この母体は情報セキュリティの専門家だけではなく、行政活動に対して高い知見を持つ専門家も含める。加えて、2)中長期計画に基づいた年度計画を毎年度定めるとともに、年度途中でも「基本方針」の変更を行うことのできる枠組みを構築する。

②基本戦略策定のための情報収集・分析機能の強化

基本戦略を立案するため、情報セキュリティ問題に関する国内全般における状況、他国政府の政策を含めた国際状況等について、常時、戦略的に情報収集・分析する機能を強化する。国際状況の情報収集・分析に関しては、内閣官房が国際的な統一的窓口として広く認知され、同時に実を伴った活動を行うことに加え、各府省庁との連動、連携に積極的に取り組む。

また、各府省庁の政策実施に資するため、情報収集・分析結果を政策の基盤として各府省庁に提供する。

③基本戦略に基づいた関連施策の事前評価の実施

基本戦略（中長期計画及び年度計画）に基づき、情報セキュリティ関連施策（予算も含む）の事前評価を実施する。その際、以下の観点を確保することが重要である。

1) 技術的専門性と組織運営（セキュリティマネジメント等）などの関連領域の専門性が複合し構成される情報セキュリティの専門性が全体として確保される形での評価を行うこと。
2) 評価結果を公表すること。
3) 施策の実施とともに事前評価の反映に対する各府省庁の責任の明確化を行うこと。
4) 関連施策の中で情報セキュリティの観点から評価が必要なものの抽出と評価意見の付与を行うこと。すなわち、関連事業において、情報セキュリティの要素が適切に考慮されているか否かについて評価を行うこと。
5) 不必要な重複排除を行うとともに、年度途中での緊急の予算確保が行われることを

担保すること。

6) 冗長性確保の機能を実装することが適切な領域においては、逆に重複の許容も必要であること。このため、情報セキュリティ面から検討された合理性の高い判断尺度を同時に確立し、社会に公開していくこと。

④事後評価の実施と結果の公表

実施された施策についての事後評価を行い、その結果を公表するとともに、基本戦略（中長期計画及び年度計画）の改定に反映する。その際、以下の観点を確保することが重要である。

1) 相対比較可能な客観的評価指標を設定すること。
2) 長期の事後評価と短期の事後評価の両者を行うこと。
3) 評価結果の対処の責任が各府省庁にあることを明確化すること。

⑤広報機能の充実

国内外に我が国政府の情報セキュリティに対する取り組みを広く理解してもらうための戦略的な広報機能の充実を図る。一つには、政府の取り組みを理解してもらう啓発活動の意味があり、国内外での円滑な相互理解の助けになることは言うまでもない。また同時に広報活動の充実は、我が国政府全体としての取り組みが現状でどのようになっているかを政府自身が点検する機会を与えることになる。

(2)情報セキュリティ関連の研究開発・技術開発の方向付けを行う構造のあり方

政府が実施する情報セキュリティに関する研究開発投資に対して、投資の有効性について検証を行うとともに、その成果について政府をはじめとする利用者がいるかどうかを評価する母体を確立することが必要である。そして、この母体は、以下の視点を確保しながら、活動を行うことが必要である。

1) 情報セキュリティ関連技術の開発の方向性を継続的に策定するとともに、達成状態の評価も同時に実施すること。
2) 政府・大学だけでなく、民間企業における技術開発能力を活用すること。また、国際的な共同研究を推進すること。
3) 「ボトムアップ型」での研究開発投資先選定だけでなく、上記母体が政府内外の専門家を集約し、研究開発プログラムを設定する「トップダウン型」の投資先選定も並立させること。
4) 情報セキュリティ技術の質の向上に必要な学問領域を抽出し、その領域（促進領域）での研究を促進するとともに、活動する研究者が存在しない場合でも戦略的に重

要な領域（戦略領域）での研究立ち上げを支援すること。

5) 各府省庁が所管する重要インフラを防護するための技術開発経費において、情報セキュリティ関連の投資を一定割合確保するべくルールを確立すること。

6) 国内産業の育成と、我が国の情報セキュリティ面での防御力向上のために、国産技術開発に対する投資のあり方を検討する。

2．2．政府自身の情報セキュリティ対策のあり方

本節では、情報セキュリティ対策を行うべき一つの主体としての「政府組織」自身について、その対策のあり方が十分かどうかを検証する。

2．2．1．基本認識

(1) 各府省庁の責任による対応と統一的・横断的な取り組み

政府自身の情報セキュリティ対策を考えるとき、一次的には各府省庁の情報セキュリティ確保の責任は各府省庁が負い、それぞれの業務や情報システムの形態に適合した対策を講じていくことが原則となる。

しかしながら、それぞれの業務や情報システムは異なるといっても同じ我が国の政府組織であり、共同で利用している情報システム等も存在するほか、そもそも他の組織と比べれば、共通の部分が多いのも事実である。また、国民の情報や国家機密を保有する政府の情報セキュリティ対策は、国民の財産・権利を保護し、国際関係上の我が国の信頼感を確保するという責務が表裏一体で求められることから、政府全体として、高い対策レベルを確保することが強く要請されている。

したがって、政府自身の情報セキュリティ対策にあたっては、各府省庁が各々の対策を講じることに加えて、その対策を促進し、かつ、政府全体として対策レベルを向上させていくための、統一的・横断的な総合調整機能を設計することが必要となる。

(2) これまでの統一的・横断的な取り組み

2000 年 1 月に、政府関係機関のホームページ改ざん事案が発生したことを一つの契機として、同年 2 月に、内閣官房に情報セキュリティ対策推進室が設置され、政府自身の情報セキュリティ対策における統一的・横断的な総合調整機能を担う組織として活動を開始した[10]。その代表的な活動として、1)「情報セキュリティポリシーに関するガイドライン」(2000 年 7 月 18 日情報セキュリティ対策推進会議決定)[11]の策定や、2)NIRT (緊急対応支援チーム) の設置[12]とその運用等が挙げられる。

---

10 内閣官房情報セキュリティ対策推進室は、「官民における情報セキュリティ対策の推進に係る企画及び立案並びに総合調整を行う」ことを任務としており (情報セキュリティ対策推進室の設置に関する規則；2000 年 2 月 29 日内閣総理大臣決定)、政府自身のほか、重要インフラの対策等についてもその活動の対象である。

11 http://www.bits.go.jp/sisaku/2002_1128/ISP_Guideline_20021128.html 参照。

12 「電子政府や民間重要インフラ事業者等の情報システムへのサイバーテロ等の国民生活に重大な影響を与えるおそれのある情報セキュリティに係る事案に対し、各省庁等における情報セキュリティ対策の立案に必要な調査・助言等を行うための体制」として、2002 年 4 月に内閣官房情報セキュリティ対策推進室内に設置。NIRT は National Incident Response Team の略。

(3) 環境の変化と統一的・横断的取り組み強化の必要性

2000 年から行われているこれらの統一的・横断的な取り組みは、その一つの出発点が、外部からの攻撃による政府関係機関のホームページ改ざん事案であったことも要因となり、急激に変化し、多様化する以下のような視点に十分に対応できていない状況となっていると言える。

1) 最近民間企業等において多発している個人情報漏えいの事案の多くに見られるように、政府に対する情報セキュリティの脅威は、外部からの攻撃や不正な侵入に限られるわけではなく、府省庁の内部から行政上重要な情報が漏えいし、改ざんされ、又は破壊される可能性を軽視すべきではない。
2) 単に情報システムに対する意図的な行為によって引き起こされる障害に対応する活動のみ限定するのではなく、行政サービスの提供継続性確保の視点から、情報システムの設計や設定の誤り等の運用上の過失によって情報システムに障害が発生し、又は情報システムが損壊するという可能性を軽視すべきではない。
3) 政府保有の情報システムにおける対策だけではなく、政府内の情報管理構造の構築、情報セキュリティに取り組む人材の育成、情報セキュリティに資する研究開発の促進、政府職員における情報取扱いまでを含めた啓発活動までを対象とする必要がある。

したがって、こうした環境変化に対応し、各府省庁が各々の対策を強化していくことに加えて、その対策を促進し、かつ、政府全体として対策レベルを向上させていくための、統一的・横断的な総合調整機能を強化していくことが必要な時期にきていると言える。

(4) 統一的・横断的取り組み強化の3分野

統一的・横断的な取り組みの強化にあたっては、上記に示した環境変化に対応する観点から、以下の 3 分野から多面的に機能を設計していくことが適当である。

1) 各府省庁が情報セキュリティ対策を行う上での、技術的側面のみではなく、人的側面や物理的側面も含めた総合的な対策の支援（2.2.2.）
2) 各府省庁が情報セキュリティ対策を行う上での、情報セキュリティ関係事案[13]対処（事前予防も含む）に関する対策の支援（2.2.3.）
3) 各府省庁の情報セキュリティ対策に資する、各府省庁の職員の人材育成・人材確

[13] サイバー攻撃等による情報システムに係る障害の発生又はそのおそれがある事案のことを指す。

保のための支援（2.2.4.）

以下、3 分野について、より詳細な現状及び課題の整理と、統一的･横断的取り組みを強化するための具体的方策について提示する。

なお、それぞれの機能の強化に際しては、1)国の安全保障に関わる場合もあるため、十分なセキュリティの管理が求められること、2)各府省庁が有する情報セキュリティに関する機能を最大限に活用しつつ、業務の円滑な遂行に向け、これら府省庁との密接な連携及び十分な調整を図ることに留意が必要である。

2．2．2．具体的方策①－総合的な対策促進の支援－

(1) 現状及び課題

①内閣官房による従来からの対策促進枠組みの問題点

2003 年に内閣官房が実施した各府省庁に対する脆弱性検査の結果[14]からも、1)セキュリティ水準の高い府省庁と低い府省庁の格差が大きい、2)内部からの侵入等に対して脆弱といった問題点が明確となったように、「情報セキュリティポリシーに関するガイドライン」に基づいて行ってきた内閣官房による対策促進支援の枠組みは、以下のような限界が指摘される状態となっている。

1) 「情報セキュリティポリシーに関するガイドライン」は、「具体的な対策レベル」については各府省庁任せになっている。
2) 最近の官民における情報漏洩事案等は、技術的な側面に起因するものだけでなく、データ保存メディアの紛失など運用面にも起因するものであるが、その対応が遅れている。
3) 府省庁ごとに「自己点検」や「外部委託監査」が行われているだけであり、統一的な基準に基づく客観的評価がなされていない。
4) そもそもセキュリティポリシー、対策基準が作成されていても、その運用が伴っていない組織が存在する。また、セキュリティポリシーや対策基準、実施手順書などの見直しは着実に行われているものの、合理性が確保されているかどうかは各府省庁任せで、政府全体として把握できていない。
5) 情報システムや保有するデータの特性に踏み込んだ行政サービスの提供継続性に注目した対策が実施されてこなかった。例えば、行政機能の東京一極集中は、社会的脆弱性を内包しており、行政機関における情報システムにおいても同様のリスク

[14] 各府省庁の情報システムに対する脆弱性検査は、2003年7月10日から12月24日までの間に実施。情報セキュリティ対策推進会議第8回会合（2004年3月3日）に結果を報告（http://www.bits.go.jp/kaigi/suisinkaigi/dai8/pdfs/8siryou2.pdf）。

が存在する。

②対策予算についての問題点

また、各府省庁が対策を講じようとしても、適切な予算措置の手当が不足しており、かつ、情報セキュリティ対策は危機管理の側面も持ち機動的に講じることが不可欠である中で、年度途中での予算確保等が困難な状況にある。

さらに、情報セキュリティ対策のための投資は、情報システム投資に関するものであるものが多く、裏返せば情報システム調達の一部となるが、その調達を高水準の技術開発・研究開発や国内産業の育成に活用するとの視点が不足しがちである。

(2) 望ましい具体的方策

以上の問題点及び課題を踏まえ、内閣官房において以下の方策を講じることが必要である。また同時に、以下の方策を講じるために、現在の内閣官房情報セキュリティ対策推進室では不足している人員を確保し、体制を強化することが必要である。

①政府統一的な安全基準の策定とそれに基づく評価の実施

内閣官房は、第1章で述べた「持続可能な構造」[15]の一つとして、政府として統一的な安全基準を策定するとともに、策定した安全基準に基づき、政府統一的な情報セキュリティ監査及び評価[16]を実施する。

「政府として統一的な安全基準」は、1)情報分類等に応じた複数の「具体的な対策レベル」を示した基準であること、2)政府内で統一的に実施すべき対策の基準であること、3)各府省庁が最低限実施すべき対策の基準であること、4)既存の標準・ガイドライン等を適切に活用した基準であること、5)技術的セキュリティに関する事項だけでなく、調達、運用（事案対処等）、人的資源及び物理的セキュリティに関する事項を含んだ基準であること、6)監査結果及び評価結果による基準の内容の定期的な見直しの実施が行われることが必要である。

また、政府統一的な情報セキュリティ監査及び評価においては、1)秘密保持及び責任の所在の明確化を図りつつ外部の知見の活用について考慮する一方、監査及び評価を行う専門的な人材を政府内部でも育成すること、2)評価結果について、各府省庁の情報

---

15 1.1.(2)⑥参照。

16 ここでいう情報セキュリティ監査と評価の違いは、前者が、基準に対する準拠性を確認するものであるのに対し、後者が、その時点での優先的テーマ等を定めたり、他の要素（予算要素等）を勘案したりして行うものを想定している。両者とも、その確認のための手段として、情報システムに対する脆弱性検査を用いることもあり得る。

セキュリティ水準が客観的に明示できる方法で提示すること、3)各府省庁において自己点検及び監査を行うことを怠らないこと、4)適法性を確保することが必要である。

なお、この点については、「各府省庁の情報システム及びその運用に関する安全基準の策定に係る基本方針について」（2004 年 7 月 26 日情報セキュリティ対策推進会議幹事会決定）[17]によって、政府内において検討が開始されており、まずはこの取り組みを完結させることが必要である。

②安全基準の定期的見直しのための情報収集・分析の強化

各府省庁における情報セキュリティの環境は常時変化する。したがって、内閣官房は、監査結果及び評価結果を踏まえて安全基準を定期的に見直すことが必要であるが、加えて、各府省庁において常時変化する情報セキュリティ環境を的確に把握するための情報収集・分析をより一層強化して行うことが必要である。

具体的には、1）情報システムに発見される各種脆弱性情報の収集、2)各脆弱性についての影響評価、3)政府自身が持つリスクの分析（政府組織内に遍在する情報システムとそこでの業務把握、各システムにおける運用体制と現状の把握も含む）、さらには、4)現在利用可能な各種技術情報の収集・分析などをより一層強化して行う。ここには、実際に政府の取り組みがどのようなレベルにあるかを判断するために、他国における情報セキュリティ対策や、民間組織におけるベストプラクティスの現状把握なども含まれる。

③各府省庁への対策促進の勧告と必要な予算措置

内閣官房が行った上記の統一的な安全基準に基づく監査の結果及び評価の結果に基づいた各府省庁への対策促進の勧告を行うとともに、必要な予算措置を講ずる。その際、以下の観点を確保することに留意する。

1) 内閣官房に、技術的専門性と組織運営（セキュリティマネジメント等）などの関連領域の専門性が複合し構成される情報セキュリティの専門性が全体として確保されるべく、人材を配置すること。
2) 政府が実施する研究開発投資に対して、有効性検証を行うとともに、その成果が政府として利用可能かどうかを評価する母体を確立し（2.1.2.(2)参照）、積極的に、当該成果を調達に活用すること。
3) IT 投資評価の手法（例えば、複数年度にわたる予算執行評価、初期コスト償却、TCO[18]、ライフサイクルコスト等）を導入すること。

---

[17] http://www.bits.go.jp/kaigi/kanjikai/dai1/1siryou1.html 及び http://www.bits.go.jp/kaigi/kanjikai/dai1/1siryou4.html 参照。

[18] 情報システムの導入、維持・管理などにかかる費用の総額（Total Cost of Ownership）のこと。従来は情報システムのコストは製品価格(導入費用)で評価されることが多かったが、導入後の維持管理費用(ランニングコ

4) 情報セキュリティ対策に使われる費用を十分なものとするには、情報セキュリティ対策を目的とした予算だけに頼るのではなく、情報システム等の構築を目的とする予算の中で、上記の安全基準で定められた情報セキュリティ対策の要件を満たす費用を確保すること。

④各府省庁の安全な情報システム設計の支援

内閣官房は、希望する各府省庁の情報システムに対して、その安全な情報システム設計の支援を行う。

2．2．3．具体的方策②－情報セキュリティ関係事案対処に関する対策の支援－

⑴ 現状及び課題

内閣官房情報セキュリティ対策推進室は、各府省庁における事案対処に係る取り組みを支援するため、2002 年 4 月に NIRT（緊急対応支援チーム）を設置し活動を行うなど、ソフトウェア等の脆弱性情報や攻撃の予兆の情報を各府省庁に提供するとともに、実際に事案が発生した場合の被害拡大防止のための情報提供を行うための取り組みを行っている。また、そのための平素からの攻撃の予兆や被害に関する情報収集・分析を行っている。

しかしながら、情報セキュリティ関係事案の多様化等が進む中で、現在の取り組みにおいては、主に以下の問題点及び課題があると言える。

1) 脆弱性情報や脅威情報等について、より早い段階で各府省庁に対して優先的に情報を提供する枠組みが十分でない。
2) NIRT（緊急対応支援チーム）については、ほとんど常駐していないことから、集中的かつ恒常的に情報の集約及び分析を実施することは難しい状況にある。また、同チームの人員構成は、インターネット関連技術の専門家が中心であり、多様化しつつある情報セキュリティ関係事案の全てに対処することは必ずしも容易でない現状にある。
3) 情報セキュリティ関係事案に対する対処のための情報収集・分析は、現状として内閣官房だけではなく、警察庁・防衛庁等でも実施している。このため、内閣官房と警察庁・防衛庁等とのより緊密な連携を行うべきである。しかし、この面での議論が十分に行われていない。
4) 情報セキュリティ関係事案が発生した場合等の緊急事態における政府全体としての意志決定の仕組みが十分ではない。

スト)が相対的に増加したため、全体の総額で評価する手法が導入されている。

(2) 望ましい具体的方策

以上の問題点及び課題を踏まえると、各府省庁における情報セキュリティ関係事案の対処の支援を行うため、内閣官房において、以下の方策を講じることが必要である。また同時に、以下の方策を講じるために、現在の内閣官房情報セキュリティ対策推進室（NIRT も含む）では不足している人員を確保し、体制を強化することが必要である。

① 各府省庁に対する早期の情報提供の実施と情報収集・分析機能の強化

各府省庁が情報セキュリティ関係事案への対処を適切に行うことを支援するため、内閣官房は、より早い段階で各府省庁に対してソフトウェア等の脆弱性情報や攻撃の予兆等に関する情報を提供する起点として機能することが必要である。そのため、以下の方策を講じることが適当である。

1) 早期の情報提供のための情報収集・分析機能の強化

内閣官房は、脆弱性情報や攻撃の予兆等の早期情報収集とその分析機能の強化を行う。この際同時に、事案発生時に各府省庁にいかなる影響が発生するかという点についての平素からのリスク分析が必要であり、そのために必要な、各府省庁の業務・情報システム等についての常時の実態調査を実施することが必要である。

2) 被害情報等の把握と原因分析に関する機能の強化

内閣官房は、各府省庁において情報セキュリティ関係事案が発生した際の、被害情報等の把握と原因分析に関する機能を強化し、被害の拡大防止と再発防止のための情報を各府省庁に提供する。

3) 関係機関との連携の強化

内閣官房は、官民の情報セキュリティ関係事案対応機関（警察庁サイバーフォース、NICT[19]、IPA[20]、Telecom-ISAC[21]、JPCERT/CC[22]等）や、製品開発者等との間での連携を強化する。連携の強化においては、特に、1)脆弱性情報の集約・配布（当該対

[19] 独立行政法人情報通信研究機構
[20] 独立行政法人情報処理推進機構
[21] インシデント情報共有・分析センター（Telecom-ISAC Japan）
[22] 有限責任中間法人 JPCERT コーディネーションセンター

応機関からの内閣官房への優先提供を含む）、2)定点観測等に基づく予兆検知情報が対象となる。この際、適法性の確保に留意しながら、アドホックな連携ではない事案情報等の交換の内容を予め取り決めておくことが必要である。また、サイバー犯罪やサイバーテロ等の事案が発生した場合の警察庁・防衛庁等との緊密な連携について、検討する必要がある。

なお、この点については、「攻撃の予兆や被害に関する情報収集・分析に係る基本方針について」（2004年7月26日情報セキュリティ対策推進会議幹事会決定）[23]によって、政府内において検討が開始されており、まずはこの取り組みを完結させることが必要である。

② 各府省庁における事案対処に関するガイドラインの策定とIRT編成支援

内閣官房は、各府省庁での事案発生時に、各府省庁の情報システム運用担当者において迅速な対応を可能にするための、事案対処ガイドラインを策定し、定期的にその見直しを行う。また、同時に、各府省庁において、いわゆる事案対応チーム（IRT: Incident Response Team）が編成されるための支援を行う。

さらに、内閣官房と各府省庁との連携を強化するため、各府省庁の担当職員の一部がリエゾンとして活動するための体制を整備する。

2．2．4．具体的解決策③－政府職員の人材育成・人材確保に関する支援－

(1) 現状及び課題

政府機関における情報システムの開発・運用両面で、外部業者に依存している分野もある中で、政府としての情報セキュリティ対策を一体的に進めていこうとしても、必要な知見や専門性を有する人材は政府内に不足しており、育成の体系も整備されていないのが現状である。

また、例えば、情報通信システムの管理システムやモニタリングシステムに関する技術を典型例として挙げられるように、情報セキュリティに関連する技術領域のいくつかは、年々先端化、先鋭化し、同時に激しく変化している。このような領域での高い専門性をもった人材を政府内で育成することは非常に難しいため、必要に応じて民間に存在する人材を、政府として適宜確保し、情報セキュリティ関連の活動の中で利用することが必要である。しかしながら、民間に存在する人材を、政府内で有効に利用する制度が十分に機能していない。

---

[23] http://www.bits.go.jp/kaigi/kanjikai/dai1/1siryou1.html 参照。

さらに、既存の人材を育成･確保するだけではなく、大学を中心とした教育機関から政府に対して、継続的に人材が供給される枠組みが構築されていない。

(2) 望ましい具体的方策

以上の問題点及び課題を踏まえ、以下のような対策を講じることが必要である。また同時に、以下の対策を講じるために、現在の内閣官房情報セキュリティ対策推進室では不足している人員を確保し、体制を強化することが必要である。

①各府省庁における情報システム管理部門の担当職員の育成

内閣官房は、各府省庁情報システム管理部門の担当職員を対象として、以下のような長期的かつ体系的な人材育成が可能となるよう、各府省庁における人事政策への反映を支援する。

1) 各府省庁に、各々の情報セキュリティ対策に従事する専門職を設置。
2) 専門職については、体系的な知識･経験の吸収と府省庁間連携体制の確立の観点から、ジョブローテーションを長期化。また、セキュリティ管理、システム運用に従事することは、責任とともに大きなストレスが付与されることに留意し、ジョブローテーションの長期化に伴うインセンティブ付与を実施。
3) 国家危機管理における実務経験と安全保障に関する視野の醸成を目的として、一定期間、内閣官房に出向。
4) 必要に応じて、民間に存在する専門性の高い人材を、政府として適宜確保し、情報セキュリティ関連の活動の中で利用。

②専門性の高い人材の活用

内閣官房は、政府内における情報セキュリティに関する専門性の高い人材について、どの府省庁にどのような人材が存在するかを把握し、外部からの人材確保、あるいは政府内での人材育成の必要性を明らかにする。

③教育機関からの人材育成の取り組み

大学を中心とした教育機関での人材育成の取り組みを体系化するとともに、政府職員になるというキャリアパスを創出する。

④幹部職員・一般職員の意識の向上

限られた予算等の中で政府内部の対策を徹底するためには、情報セキュリティ実践者としての政府職員（エンドユーザー）に対し、継続的なOJTの実施、職員全員に対する教育を行うなどの環境整備が必要である。また、幹部職員の意識を向上させるためのプログラムを実施することも必要である。

第3章　実現のための行動計画

本章では、前章で示した「望ましい具体的方策」を実現していくために政府が今後実行すべき具体的な行動計画を提示する。

3．1．新たな体制の整備

3．1．1．体制整備の目的･方向性

体制整備の目的は、我が国における行政機関、民間企業、個人などにおける情報基盤の構成要素の安定的･継続的な稼働の維持を図るために実施される各府省庁の政策を総合調整し、政府全体としてのこれらに関する基本戦略を策定するための機能を強化することである。つまり、我が国全体としての情報セキュリティの水準のより一層の向上を図ることであり、このための計画等の策定、各府省庁の政策の事前評価･事後評価、政府統一的な安全基準の策定とこれに基づく評価の結果による勧告、広報、人材育成、安全なシステム設計支援、事案発生時における迅速かつ円滑な各府省庁間の協力･連携や対策の策定、そのための情報収集･分析などを行うための体制を整備･強化するということである。この体制整備に当たっては、以下の点に配慮する必要がある。

① 国の安全保障に関わる場合もあるため、整備される体制においては十分なセキュリティの管理が必要である。

② 各府省庁が有する情報セキュリティに関する機能を最大限に活用しつつ、業務の円滑な遂行に向け、これら府省庁との密接な連携及び十分な調整を図ることが必要である。

戦略の策定、各府省庁の政策の事前評価･事後評価及び政府統一的な安全基準の策定とこれに基づく評価の結果による勧告は、内閣の立場から行うことが適当と考えられるので、内閣に置かれたIT戦略本部に「情報セキュリティ政策会議（仮称）」を設置してこれを行うこととし、これ以外のものについては、内閣官房に「国家情報セキュリティセンター（仮称）」を設置して政府全体の総合調整等の一環としてこれを行うことが適当と考えられる。

3．1．2．具体的行動計画①～「情報セキュリティ政策会議（仮称）」の設置

「情報セキュリティ政策会議（仮称）」は、基本戦略の決定、基本戦略に基づいた各府省庁の政策の事前評価、政府統一的な安全基準の策定、これに基づく評価の結果による各府省庁の情報セキュリティ対策に対する勧告、各府省庁の施策の事後評価を内閣の立場から行う。

(1) 機能

「情報セキュリティ政策会議（仮称）」は以下の機能を有するものとする。

① 情報セキュリティに関する基本戦略（中長期計画及び年度計画）の策定

情報セキュリティ分野における我が国内外の政策、民間におけるサービス、各種の発生事案、研究開発などの現状、動向等を調査検討し、我が国の政府全体としての情報セキュリティに関する我が国の基本戦略（中長期的な計画及び年度計画）を策定する（2.1.2.(1)①参照）。

②基本戦略に基づいた事前評価

情報セキュリティ分野における限られた資源を有効活用し、政府全体としての重点政策を明確にするため、基本戦略（中長期計画及び年度計画）に基づいて、各府省庁の情報セキュリティに関する政策の事前評価を実施する（2.1.2.(1)②参照）。この際、情報セキュリティ関連予算の配分の方針を決定する（2.1.2.(1)②参照）とともに、年度途中での緊急性のある事業費（施策・対策ともに対象）等に活用する「情報セキュリティ推進調整費（仮称）」を新設し、それを配分する。

③各府省庁の情報セキュリティ対策に対する勧告

政府統一的な安全基準を策定し、これに基づく評価の結果に従って、各府省庁の情報セキュリティ対策に対する勧告を行う（2.2.2.(2)③参照）。

④各府省庁の情報セキュリティ施策及び対策の事後評価と公表

各府省庁において実施された施策及び対策についての事後評価を行い、その結果を公表する（2.1.2.(1)③参照）。

(2) 実現にあたって必要な資源と権能

本会議が、基本戦略等について自律的に決定を行うためには、新たな法制上の権限付与も検討する必要がある。

また、1)予算配分の方針を決定する権限（上記②参照）、2)各府省庁に対して対策の勧告を行う権限（上記③参照）を付与するためには、新たな法制上の措置も検討する必要がある。

さらに、情報セキュリティ関連研究開発・技術開発についての事前評価を一元的に行う（上記②参照）ためには、総合科学技術会議との法制的な権限整理も検討する必要がある。

(3) 実現までのマイルストーン

2 年後（2006 年中）に、法的権能も付与・整理した上で、上記を実現することを当面の目標とする。

それを踏まえ、来年度（2005 年度）は、法制上の措置が不要な部分について段階的に活動を開始する。

3．1．3．具体的行動計画②～「国家情報セキュリティセンター（仮称）」の設置

内閣官房情報セキュリティ対策推進室の機能を強化・発展させ、内閣官房に「国家情報セキュリティセンター（仮称）」を置く。

(1) 機能

「国家情報セキュリティセンター（仮称）」は以下の機能を有するものとする。

①基本戦略立案機能

各府省庁が行う情報セキュリティに関する政策の総合的把握及び総合調整を行い、我が国全体の情報セキュリティに関する基本戦略（中長期計画及び年度計画）を立案する。

具体的には、「情報セキュリティ政策会議（仮称）」の事務局として、会議にて策定する中長期計画及び年度計画素案の作成、各省庁の施策の事前・事後評価結果素案の策定を行う（3.1.2.(1)①②④参照）。この際、計画の策定に資するため、常時国内の状況、国際的な状況（他国の政策を含む）等について情報収集・分析を実施するとともに、各府省庁の政策実施に資するため、情報収集・分析結果を政策の基盤として各府省庁に提供する（2.1.2.(1)④参照）。

また、政策事項に関する国際的窓口（2.1.2.(1)④参照）及び戦略的広報を行う（2.1.2.(1)⑤参照）。

②政府機関総合対策促進機能

各府省庁が行うべき、技術的側面のみではなく、人的側面や物理的側面も含めた

総合的な情報セキュリティ対策についての政府統一的な安全基準を策定し、それに基づいて各府省庁の対策を評価するとともに、対策レベルの向上についての支援を行う。

具体的には、「情報セキュリティ政策会議（仮称）」が策定する政府統一的な安全基準案の作成とそれに基づく評価作業の実施、評価に基づいた勧告案の策定と必要な対策予算確保の支援を行う（3.1.2.(1)③及び 2.2.2.(2)③参照）。この際、安全基準の定期的な見直しのために必要な情報収集・分析を行う（2.2.2.(2)②参照）。

また、政府職員の人材育成・人材確保のための支援（2.2.4.参照）、希望する各府省庁に対する安全なシステム設計の支援（2.2.2.(2)④参照）を行う。

③政府機関事案対処支援機能

各府省庁が情報セキュリティ対策を行う上での、情報セキュリティ関係事案対処（事前予防も含む）に関し、ソフトウェア等の脆弱性情報や攻撃の予兆の情報を早期に各府省庁に提供するとともに、実際に事案が発生した場合の被害拡大防止のための情報提供を行う。そして、そのための平素からの情報収集・分析を行う。

具体的には、各府省庁における事案対処に関するガイドラインの策定とその見直し（2.2.3.(2)②参照）、各府省庁に対して脆弱性情報等早期警戒情報を提供するための起点として機能し、関係機関（警察庁サイバーフォース、NICT、IPA、Telecom-ISAC、JPCERT/CC 等）からの情報提供枠組みの構築・運用を行う（2.2.3.(2)①参照）。その際、各府省庁にいかなる影響が発生するかという点についての、平素からのリスク分析を行うために必要な、各府省庁の業務・情報システム等についての常時の実態調査を実施する（2.2.3.(2)①参照）。

また、各府省庁における被害情報等の把握と原因分析を実施する（2.2.3.(2)①参照）。

なお、上記で提示した「国家情報セキュリティセンター（仮称）」の業務は、本提言の範囲内でのものであり、今後検討を行う「重要インフラの情報セキュリティ対策」等について、本センターにて取り扱うことが必要な業務が付加される可能性がある。

⑵ 実現にあたって必要な資源と権能

①法的権能

上記の機能は、現在の内閣官房の所掌事務内（内閣法に規定）で活動可能であると考えられる。

②人員

「戦略企画機能」で 10 名程度、「政府機関総合対策促進機能」で 30 名程度、「政府機関事案対処支援機能」で 20 名程度の常勤職員が必要である。

常勤職員には、プロパーの職員の育成に努力するとともに、各府省庁からの出向者や民間に存在する優秀な人材の採用も検討し、国家の安全保障に関わる場合もあることから、職員に対して一般公務員に比べても高い機密性の保持等が要求されることを規定化する。

また、各府省庁の情報セキュリティ担当職員の一部をセンターの職員として内閣官房に併任する（3.2.参照）。

⑶ 実現までのマイルストーン

人員及び予算を 2005 年度中の可能な限り早い段階で確保し、活動を開始。

3．1．4．両者の関係

「国家情報セキュリティセンター（仮称）」（以下、「センター」とする。）は、我が国政府の情報セキュリティに関する実質上の中核機関として機能するが、その機能は、①「情報セキュリティ政策会議（仮称）」（以下、「会議」とする。）の事務局となるものと、②それ以外の独自業務に分かれる。なお、後者の業務についても、会議が策定・決定する基本戦略の内枠となるため、センターの業務は、会議の評価を受ける形になる（表2参照）。

	機能	情報セキュリティ政策会議（仮称）	国家情報セキュリティセンター（仮称） （内閣官房情報セキュリティ対策推進室を強化・発展）	
センターが会議の事務局となる機能	基本戦略（中長期計画及び年度計画）の策定	関係各所からの知見を集約し、策定・決定	会議での審議を踏まえ、案を策定	
	各府省庁の施策・対策の事前評価	評価結果を決定（予算の配分方針含む）	会議での審議を踏まえ、案を策定	
	各府省庁の対策に対する勧告の実施	安全基準の策定と、これに基づく評価に従い勧告	会議での審議を踏まえ、安全基準案を策定 会議での審議を踏まえ、勧告案を策定	
	各府省庁の施策・対策の事後評価と結果の公表	評価結果を決定／その結果を公表	会議での審議を踏まえ、案を策定	
上記以外の機能		基本戦略の一部に含まれる	基本戦略立案	センター全体の企画立案
				政策事項に関する国際的窓口
				戦略的広報
			政府機関総合対策促進	政府統一的な安全基準に基づく評価
				政府職員の人材育成・人材確保
				安全なシステム設計支援
			政府機関事案対処支援	各府省庁における事案対処に関するガイドラインの策定とその見直し
				各府省庁に対して脆弱性情報等早期警戒情報を提供するための起点として機能
				各府省庁における被害情報等の把握と原因分析
				関係機関からの情報提供枠組みの構築・運用

表2；「情報セキュリティ政策会議（仮称）」と「国家情報セキュリティセンター（仮称）」の関係

3．2．制度等の創設・見直し

「情報セキュリティ政策会議（仮称）」及び「国家情報セキュリティセンター（仮称）」の体制及び機能整備にあわせて以下の検討を行い、2005 年度中の可能な限り早期に結論を得る。

（1）公的研究助成資金の見直し（2.1.2.(2)参照）

情報セキュリティの観点から、現在の公的研究助成等資金の見直しを検討する。

（2）情報セキュリティ関係事案への対応の強化（2.2.3.(2)参照）

内閣官房（センター）は、事案対処に関するガイドラインを策定するとともに、各府省庁でのＩＲＴの設立支援を行う。

（3）政府職員の人材育成・確保のための措置（2.2.4.(2)参照）

①情報セキュリティ対策に従事する専門職の設置

内閣官房（センター）は、各府省庁が情報セキュリティ担当者のためのキャリアパスを新設すべく、支援する。同時に、同職に必要な専門性を養成するための研修を実施する。

また、各府省庁の情報セキュリティ担当者のうち、内閣官房に併任された者については、国内外のＩＲＴ研修プログラムに参加させるとともに、情報セキュリティ事案対応策に関する特別調査研究予算の支給及び手当の支給について検討する。

②情報セキュリティ対策モデル事業の実施

内閣官房（センター）は、情報セキュリティ対策モデル事業及び優秀職員に対する表彰制度の創設を検討する。

③「情報セキュリティ奨学金（仮称）」の創設

内閣官房（センター）は、大学を中心とした教育機関での人材育成の取り組みの体系化を促すべく、「情報セキュリティ奨学金（仮称）」の創設を検討する。

(参考) 第1次提言までの検討の経緯

【情報セキュリティ基本問題委員会】

2004 年 7 月 27 日　　第1回会合

本委員会の活動方針（テーマ及びスケジュール）について

2004 年 9 月 6 日　　第2回会合

（1）第1分科会の設置と開催状況について

（2）第1分科会の検討状況報告（中間報告の収受）

2004 年 10 月 26 日　　第3回会合

「第１次提言（案）」の検討

【情報セキュリティ基本問題委員会第1分科会】

2004 年 8 月 6 日　　第1回会合

（1）第1分科会の活動方針について

（2）「政府の政策・施策実施体制のあり方」及び「有効性の高い政府自身の情報セキュリティ対策のあり方」についての具体案の検討（その1）

2004 年 8 月 23 日　　第2回会合

「政府の政策・施策実施体制のあり方」及び「有効性の高い政府自身の情報セキュリティ対策のあり方」についての具体案の検討（その2）

2004 年 9 月 1 日　　第3回会合

「第1分科会中間報告案」の検討

2004 年 9 月 17 日　　第4回会合

（1）「中間報告」に対する基本問題委員会からの指摘の反映方法について

（2）「中間報告」の詳細化とマイルストーン設定について

2004 年 10 月 8 日　　第5回会合

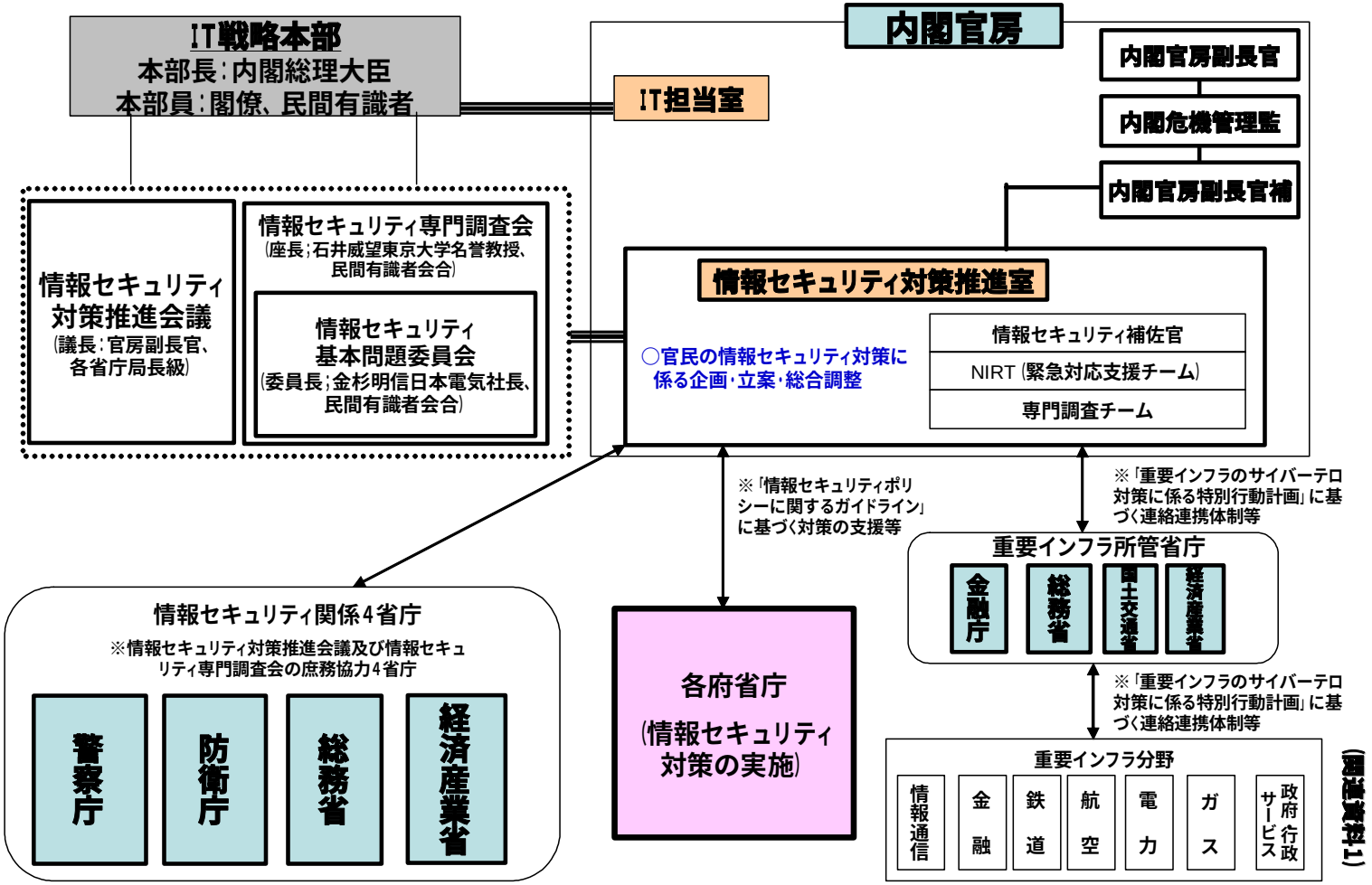
「第1次提言素案」の検討

2004 年 10 月 19 日　　第6回会合

「第1次提言（案）」の検討

関 連 資 料

政府の情報セキュリティ政策実施体制

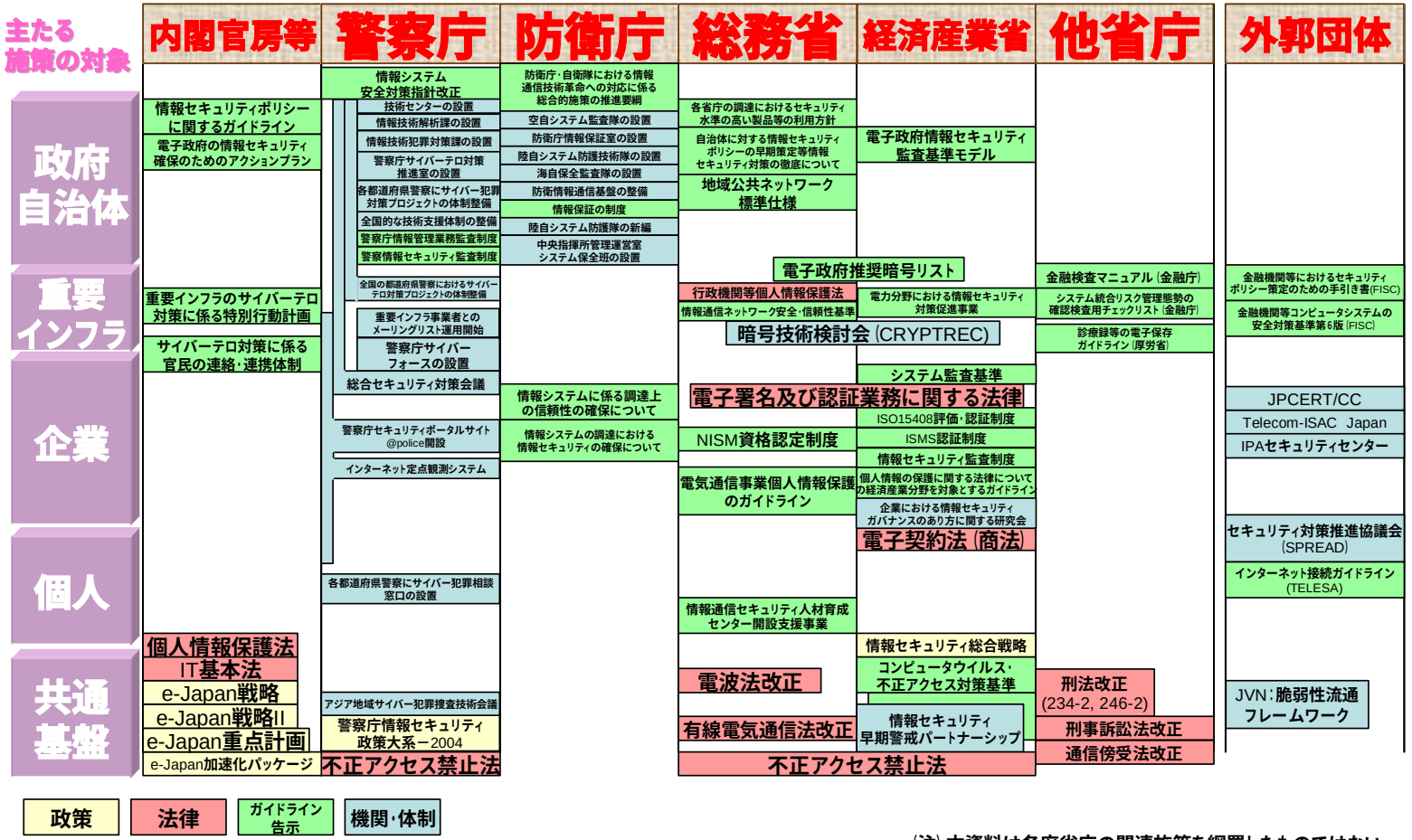


政府の情報セキュリティ関連施策の実施状況（経緯）

（注）本資料は各府省庁の関連施策を網羅したものではない。

（関連資料2）

政府の情報セキュリティ関連施策の実施状況（現況）



（注）本資料は各府省庁の関連施策を網羅したものではない。

（関連資料3）