第1次情報セキュリティ基本計画

新しい官民連携モデルの構築による
情報セキュリティ先進国への進展

（案）

情報セキュリティ政策会議

年　月　日

目次

はじめに

高度情報通信ネットワーク社会が現実のものとなり、我が国の国民生活・社会経済活動において情報技術（以下、「IT」という。）への依存度が高まってきている今日、ITを安全・安心に活用するための取組み、すなわち情報セキュリティ問題への取組みが不可欠である。高度情報通信ネットワーク社会形成基本法（以下、「IT基本法」という。）第22条（高度情報通信ネットワークの安全性の確保等）にも「高度情報通信ネットワーク社会の形成に関する施策の策定に当たっては、高度情報通信ネットワークの安全性及び信頼性の確保、個人情報の保護その他国民が高度情報通信ネットワークを安心して利用することができるようにするために必要な措置が講じられなければならない。」とうたわれ、IT基本法が制定された2000年以降、様々な取組みが行われてきた。

しかしながら、近年、情報通信基盤の急速なブロードバンド化や電子商取引の浸透に伴い、世界規模でのコンピュータウイルスの蔓延、サイバー犯罪[1]の増加、国民生活・社会経済活動の基盤となる重要インフラにおける情報システムの障害、大量の個人情報の漏洩等が社会問題化し、情報セキュリティ問題への取組みを、抜本的に強化する必要性が認識されるようになってきた。

こうした流れの中で、2005年4月に内閣官房に情報セキュリティセンター（NISC[2]）が、同年5月に高度情報通信ネットワーク社会推進戦略本部（以下、「IT戦略本部」という。）に情報セキュリティ政策会議が設置され、我が国全体としての情報セキュリティ対策強化の中核機関として活動を開始しており、いまや、e－Japan重点計画等の一部となっている「情報セキュリティ」の問題を個別重点的に捉え、戦略的思考に基づいた体系的な計画を構築していく時期に来ていると言える。このような状況を踏まえ、ここに、情報セキュリティ問題を俯瞰した中長期の戦略として、「第1次情報セキュリティ基本計画」を定めることとしたものである。

本基本計画は、IT戦略本部情報セキュリティ専門調査会[3]に設置された情報セキュリティ基本問題委員会[4]の第1次提言[5]及び第2次提言[6]、両提言を受けた政府での取組み、そして、本基本計画の審議に資するために情報セキュリティ政策会議の下に設置されたセキュリティ文化専門委員会及び技術戦略専門委員会の両報告書[7]を踏まえて策定されている。

---

1 「サイバー犯罪」とは、「インターネット等の高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等、情報技術を利用した犯罪」を指す。

2 National Information Security Centerの略。

3 情報セキュリティ専門調査会は、2001年1月22日、IT戦略本部に設置され、2005年5月 30 日、情報セキュリティ政策会議が設置されると同時に廃止された。

4 情報セキュリティ基本問題委員会は、2004年7月22日、IT戦略本部情報セキュリティ専門調査会に設置され、2005年5月 30 日、情報セキュリティ政策会議が設置されると同時に廃止された。

5 情報セキュリティ基本問題委員会第1次提言（2004年11月16日）

6 情報セキュリティ基本問題委員会第2次提言（2005年4月22日）

7 情報セキュリティ政策会議セキュリティ文化専門委員会報告書、技術戦略専門委員会報告書（2005年11月17日）

本基本計画では、第1章において、経済大国日本の持続的発展とITの利用・活用、より良い国民生活の実現とITの利用・活用、新たな観点からの国家の安全保障の確保という国家目標の中での情報セキュリティの位置付けを提示し、その位置付けの下で、我が国が情報セキュリティ問題に取り組む上での基本理念を提示した。第2章では、その基本理念に沿って、あらゆる主体が参加して、情報セキュリティ問題に取り組んでいくための各主体の役割分担を、第3章では、基本理念と役割分担を前提として、政府が今後3年間に取り組むべき重点政策を提示した。最後に、第4章において、これらを実現し、継続させていくための政策の推進体制を示した。

なお、情報セキュリティについては、中長期の視点から見た継続的な取組みが必要である一方、これを取り巻く環境変化が著しいことを踏まえ、本基本計画の計画期間については、今後3年間（2006年度から2008年度まで）を対象とした。さらに、今後、本基本計画に基づき、2006年度から年度毎の推進計画を策定することとする。

第1章　基本理念

本章では、情報セキュリティ問題を考える上で射程に入れるべき我が国の国家目標を提示し、情報セキュリティ問題に取り組む上での基本理念を提示する。

第1節　我が国の国家目標の中での情報セキュリティの位置付けと現在の課題及びその解決

本節では、情報セキュリティ問題を考える上で射程に入れるべき我が国の国家目標と、それを踏まえた情報セキュリティの位置付けと実現すべき基本目標、現在の課題、さらには解決に向けての方向性について提示する。

(1) 我が国の国家目標の中での情報セキュリティの位置付け

①国家目標Ⅰ－経済大国日本の持続的発展とITの利用・活用－

2005年現在、我が国はGDP世界第2位を維持し、その活動を全世界に広げている経済大国である。豊かな天然資源を持たない我が国は、高品質で世界のマーケットニーズに的確に応える製品を供給してきた製造業によって基礎的な経済基盤が築かれてきた。ところが、物質的な豊かさを追求する「工業経済」は、知恵とノウハウの活用の巧みさが問われる「情報経済」へと、その軸足を移しつつある。

この動きに対応するように、我が国の製造業は生産拠点を世界各国に展開することで「工業経済」のグローバル化においても引き続き世界をリードする体制を整備し、同時に製造特許やブランドといった知的財産の保護と活用にも積極的に対応するようになっている。企業活動のグローバル化と分散化に対応して、強固な国際競争力と高い生産性を維持するためには、ITの利用・活用が不可欠であるということは言うまでもない。ITを社会インフラとして他国以上に一層有効に使いこなし、我が国の経済活動の持続的発展を遂げることが重要な国家目標である。

②国家目標Ⅱ－より良い国民生活の実現とITの利用・活用－

経済活動だけではなく、21世紀の我が国が直面する社会問題の解決のためにも、ITの利用・活用が不可欠となり始めている。例えば、少子高齢化の問題に対しても、今後15年以上にわたって就労人口が減少していくと予測される[8]中で、ITを活用してサービスの品質を維持し、同時に少人数で対応できる体制を構築することが必要となっているが、これに対するITの利用・活用による問題解決が進んできている。また、防災や災害対策などの国民生活の安全の確保、医療や福祉、教育など、多面にわたる活動について、生活者の視点に立った、安全・安心で、信頼できるIT社会の実現が求められている。

このように、ITを重要な手段として利用・活用し、我が国が直面する社会問題を解

8　厚生労働省雇用問題研究会,「人口減少下における雇用・労働政策の課題－すべての人が自律的に働くことができ、安心して生活できる社会を目指して－」(2005年7月発表、p.47 等)を参照

決し、安全･安心で、より良い国民生活を実現していくことが重要な国家目標である。

③国家目標III－我が国の安全保障におけるITに起因する新たな脅威への対応－

ITが我が国のあらゆる国民生活･社会経済活動において利用･活用されつつある現在において、ITに対する、あるいはITを用いた犯罪やテロの脅威への対応は、我が国の安全保障の観点から積極的に取り組むべき課題である。

また、食糧、エネルギー、金融、財政等これまで安全保障の枠組みでは捉えられることの少なかった幅広い分野において、我が国の持続的発展や国民生活の安全･安心に対する脅威が意識されるようになってきており、我が国の安全保障を確保するためには、これらの分野におけるITの利用･活用の拡大を踏まえた、ITに起因する脅威を十分考慮に入れる必要がある。

このように、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認識し、これに十分対応していけるよう、関係機関がその体制を強化しつつ連携し、我が国の安全保障を確保していくことが重要な国家目標である。

④上記国家目標の中での情報セキュリティの位置付け

経済大国としての我が国を今後も持続的に発展させ、同時にITを利用･活用したより良い国民生活を実現し、新たな観点からの国家の安全保障を確保しようとする我が国の国家目標の中で、このIT基盤を、真に依存可能で強固なものにすることが、情報セキュリティの役割である。

すなわち、コンピュータウイルスの蔓延等に代表される情報セキュリティ問題の深刻化や近年のサイバー犯罪の多発といった課題に対処するための情報セキュリティ確保の取組み強化はもとより、ITの利用･活用を前提とした取組みを強化していくことが、経済大国たる我が国の持続的発展を可能とし、少子高齢化等に直面する社会の高品質維持に貢献し、同時に国際競争力の強化と我が国の安全保障に直結するという視点を持つべきである。ここに、我が国が情報セキュリティ問題に積極的かつ戦略的に取り組むことの基本的な意義がある。そして、このように、広く、多面的な課題を解決する必要のある情報セキュリティ問題への取組みは、個々の主体が各々で行うだけでなく、我が国全体として一体となって行う必要がある。

⑤「セキュリティ立国」の思想に基づく「情報セキュリティ先進国」の実現

我が国は、ＧＤＰ世界第2位の経済大国として高品質･高信頼な工業製品を世界に送り出し、同時に「世界一安全な国」という評価を受け、さらに官民、企業間、地域コミュニティでの協調の中で発展を遂げてきた。このような日本の強み、日本の特長を活かすことは、我が国の様々な政策の中で強く認識されてきており、我が国は、高品質、高信頼性、安全･安心の代名詞としての「ジャパンモデル」を確立する潜在的可能性、すなわち「セキュリティ立国」の思想に基づく国造りが有効であると考えられる。

したがって、情報セキュリティ確保の取組みにおいても、その「セキュリティ立国」の思想に基づく我が国の強みと特長を活かし、世界最高の高度情報通信ネットワーク社会に見合った取組みを実施し、真に「情報セキュリティ先進国」になることが求められている。さらに、我が国の情報セキュリティ確保の取組みが「ジャパンモデル」として世界に展開させる取組みも視野に入れることが肝要である。

(2) 実現すべき基本目標－IT基本法が求める「ITを安心して利用可能な環境」の構築へ－

①「ITを安心して利用可能な環境」の構築

上に述べた位置付けの下で、情報セキュリティ問題に積極的かつ戦略的に取り組んでいくことが必要である。具体的には、IT社会において、以下の3つの条件が満足される環境を構築することが求められている。

1) 事故、災害や攻撃に対して、事前に考えられる対策が十分に施されていること(予防)。

2) その対策を施された環境を、その環境にかかわる者が、その環境を実際に体験し、その構造や技術等を十分に理解した上で使いこなしていること(認識・体感)。

3) その上でも、事故、災害や攻撃にさらされた場合の対処方策があらかじめ検討されており、被害の局限化や救済等がなされ、事業の継続性が確保されること(事業継続)。

これは、IT基本法第22条にうたわれている「ITを安心して利用可能な環境」の構築の具体化にほかならない。すなわち、情報セキュリティ問題への取組みによって実現すべき基本目標は、単に安全であるだけでなく、上記の3条件を満足し、利用者が安心を実感しながらITを利用・活用できる環境を構築することにある。

②利便性とセキュリティの両立

上記の3条件が実現され、利用者が安心を実感しながらITを利用・活用できる環境が構築されれば、ITの利便性と情報セキュリティの両立が図られることとなる。昨今の状況を見ると、例えば、情報漏洩を防止するために、業務で使用するべき外部持ち運び用のコンピュータからの企業内部ネットワークへの接続を一切禁止するといった、情報セキュリティ対策を重視し、利用者の利便性が過度に損なわれる等の情報セキュリティ対策そのものが自己目的化しているような事例が一部には見られるが、利便性とセキュリティを両立させた対策や政策を推進していくことが必要である。

(3) 現在の課題と解決の方向性－「新しい官民連携モデル」の構築へ－

①現在の課題

2000年に制定されたIT基本法において、上記3条件を満足する「ITを安心して利用可能な環境」の構築が求められてきたものの、利用者の視点から見れば、現在

においても、これが実現できているとは言い難く、国際的に見てもその取組みは遅れていると言わざるを得ない。具体的には以下のような問題が近年発生している。これらの問題が我が国で発生している原因としては、1)顕在化した問題のみに対する対症療法的な対応が支配的であること、2)IT社会を構成する各主体が、組織の縦割り構造の中で独自の対応に終始していることが挙げられる。

(例1;予防が不十分な例)

業務遂行に個人保有のコンピュータを利用し、かつ、そのコンピュータにファイル交換等を目的とするソフトウェアがインストールされた状態で、利用者の知らない間に当該ソフトウェアがコンピュータウイルスに感染することにより、深刻な情報漏洩を引き起こす例が後を絶たない。個人保有のコンピュータを安易に業務として使うことはもとより、コンピュータウイルスによる大量の情報漏洩が起きているという事実は以前から認識されていたにもかかわらず、予防の徹底がなされていないために、このような情報漏洩をもたらす結果となっている。

(例2;認識・体感が不十分な例)

無線LAN(Local Area Network)は、ネットワーク構築の際の煩雑なケーブル処理を施す必要なく、インターネット等に接続できるシステムとして、企業から一般家庭における個人に到るまで幅広く普及しつつある。しかしながら、実際使用するにあたり、「無線」という利便性に重きを置くあまり、「電波」という特性が忘れ去られ、かつ適切な暗号化及び電波の範囲設定等の対策への認識が不十分であることから、第三者による盗聴あるいはネットワークへの侵入を許容してしまうケースが散見される。

(例3;事業継続対策が不十分な例)

国際的な証券市場において、想定していなかった情報システムの障害等により、現物の株式取引の停止を余儀なくされた事例や、空港関連施設における停電の発生により航空管制システムが停止し、欠便を発生させた事例等、国民生活・社会経済活動を支える基盤等において、事業継続性確保の取組みが不足している事例が近年頻発している。

②解決の方向性－「新しい官民連携モデル」の構築と「情報セキュリティ先進国」の実現－

今後は、「ITを安心して利用可能な環境」の構築を目指し、対症療法的対応から脱却することが必要である。また、IT社会を構成するあらゆる主体が、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、情報セキュリティにおける「新しい官民連携モデル」を構築し、我が国全体として国家的視野に立って情報セキュリティ問題へ取り組んでいくことが必要である。「新しい官民連携モデ

ル」の下で、我が国全体としての資源の重点的･戦略的投入の強化が図られ、国際的に見ても、我が国が常に世界をリードする「情報セキュリティ先進国」になることを求め続けることが重要である。

第2節　我が国が情報セキュリティ問題に取り組む上での4つの基本方針

前節で述べたように、「ITを安心して利用可能な環境」を構築するとの基本目標を実現するためには、IT社会を構成するあらゆる主体が適切な役割分担の下で参加した「新しい官民連携モデル」を構築し、我が国全体として国家的視野に立った情報セキュリティ問題への取組みが必要である。

このために各主体が果たすべき役割については、次章で提示するが、その前提として、ここでは、我が国全体としての資源の重点的･戦略的投入の強化に向けた4つの基本方針を提示することとする。すなわち、「官民各主体の共通認識の形成」、「先進的技術の追求」、「公的対応能力の強化」、「連携･協調の推進」の4つの基本方針を、すべての主体が共有し、問題に取り組んでいくことが必要である。

(1) 官民各主体の共通認識の形成

まず大前提として、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。

(2) 先進的技術の追求

前節で示したように、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。

(3) 公的対応能力の強化

前節で示したように、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

害対策の強化等の安全保障・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。

(4) 連携・協調の推進

前節で示したように、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。

第2章 「新しい官民連携モデル」の構築における各主体の役割と連携

前章で述べたように、情報セキュリティ問題への取組みにあたっては、IT社会を構成するあらゆる主体が、それぞれが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、「ITを安心して利用可能な環境」の構築に参加し、「新しい官民連携モデル」を実現していくことが必要である。あらゆる主体が参加するための取組みを推進していくためには、各主体が自らの行動が「ITを安心して利用可能な環境」を構築することに対してどのような影響を与えており、どのような行動を行うことが期待されているかということについて、具体的に認識することが重要である。

IT社会を構成する主体としては、まず、1）対策を実際に適用し、実施する主体が存在する。本基本計画においては、対策を実際に適用し実施する主体の領域を、①政府機関・地方公共団体、②重要インフラ[9]、③企業、④個人の4領域に分け、それぞれの特性に応じた対策のあり方を検討することが有効であるとの立場に立っている。

また、2）この4領域の主体が実際に対策を適用し、実施するにあたり、その対策の手法や環境整備を側面的に支援し、問題の理解・解決を促進する主体が存在する。本基本計画では、①政策を立案・実施する主体としての政府・地方公共団体、②初等中等教育機関、高等教育機関及び研究開発・技術開発実施機関（以下、「教育機関・研究機関」という。）、③情報システムの構築や通信サービスの提供等IT基盤を構築・提供している事業者（以下、「情報関連事業者」という。）や非営利組織（以下、「情報関連非営利組織」という。）、そして、④メディア[10]の4主体を、問題の理解・解決を促進する主体のうち重要な役割を有するものとして取り上げるものとする。

したがって、ここでは、1）対策を実際に適用し、実施する4領域の各主体と、2）問題の理解・解決を促進するための4主体のそれぞれについて期待される役割と連携のあり方を提示する。

第1節 対策実施主体の役割と連携

（1）政府機関・地方公共団体

政府機関・地方公共団体が取り扱う情報には、高い機密性を有する情報をはじめ、法令に基づき収集した個人や企業に関する情報等、その漏洩、改ざん又は破壊等が発生した場合には極めて重大な結果を招くおそれがあるものが多数含まれている。また、電子政府・電子自治体の進展により、個人や企業との関係での行政サービスのオンライン化が進む中、その停止があってはならない情報システムも存在する。

すなわち、政府機関・地方公共団体における情報セキュリティの確保は、個人の権利・財産の保護から、国民生活・社会経済活動、行政機能の維持、さらには我が国の

---

9 「重要インフラ」とは、「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活・社会経済活動の基盤であり、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、我が国の国民生活・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」を指す。以下同じ。

10 ここでいう「メディア」とは、新聞、テレビ、ラジオ等の報道機関を指す。

安全保障の確保に至る様々な分野に関係する重要課題であり、政府機関においては、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し、常に最高水準の情報セキュリティ対策レベルを維持していくことが必要である。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である。

その際、政府機関においては、それぞれの業務や情報システムは異なるとしても、行政機能を司る、同じ我が国の政府機関であり、共同で利用している情報システム等も存在するほか、共通の部分も多いことから、政府機関全体で協調し、成果の共有化や対策の統一化等の横断的取組みを実施していくことが重要である。また、地方公共団体においても同様のことが言え、横断的取組みを実施していくことが重要である。

なお、地域と密着した行政サービスを実施し、個人情報を取り扱う業務が多く、規模も様々である地方公共団体と、国家レベルでの基盤の構築を担当し、全体的に規模の大きい政府機関とはその特性に違いがあることにも留意が必要である。

（2）重要インフラ

重要インフラは、文字通り国民生活・社会経済活動の基盤であり、あらゆる脅威からその安定的供給を確保することが最優先の課題である。特に、近年発生した大地震を含めた事例からも分かるとおり、各重要インフラ分野におけるＩＴ化の進展や相互の依存関係の増大に伴い、各重要インフラ事業者等[11]が個別に対策を講じるだけでは、国全体としての重要インフラの安全性が確保できない状況が生じつつある。このため、重要インフラのＩＴ障害[12]に対して、分野を越えた横断的情報セキュリティ対策を一層強化していくことが喫緊の課題となっている。

ＩＴ障害については、これまでサイバー攻撃等意図的要因に起因する障害に対する取組みを中心として、官民の連絡・連携体制が構築されてきたが、実社会で経験するＩＴ障害の多くは、システム障害や人為的なミス、あるいは災害等多種多様な脅威に起因するものであり、今後はかかる脅威も想定して対策を講じていく必要がある。

また、重要インフラの大部分は、民間事業者が各事業分野ごとに各重要インフラ所管省庁の許認可の下で運営を担っていることから、情報セキュリティ対策も各分野ごとに重要インフラ所管省庁を中心に進められてきた。このため、重要インフラ全体を見渡すと、各分野ごとにその事業環境や業界構造の多様性も相まって、情報セキュリティへの取組みの歴史も対策水準もかなり異なっているのが実態である。今後、各重要インフラ間の相互依存性がますます増大していくことを考えれば、重要インフラの情報セキュリティ水準の向上とＩＴ障害への対応能力の強化（未然防止、被害拡大防止・迅速な復旧、再発防止）の両面で、各事業分野や重要インフラ事業者等の特質を踏まえながら、

---

11 「重要インフラ事業者等」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」（　年　月　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。

12 重要インフラの各事業において発生する障害(サービスの停止や機能の低下等)のうちＩＴの機能不全が引き起こすものを「ＩＴ障害」という。以下同じ。

従来の縦割り型の施策実施体制だけでなく、分野横断的な取組みを含めた新たな官民の連携体制を再構築していく必要がある。

(3) 企業

企業においては、グローバル社会における経済発展の担い手であると同時に、ITの根幹を担う製品・サービス等を提供する主体でもあるという面から、情報セキュリティ対策を実施することが必要である。その対策の実施は、各企業の経営判断に基づいた自主的な取組みが前提とはなるが、高度にネットワーク化されたIT社会においては、企業一社の事故によるトラブルが社会全体に波及する可能性があること、多くの個人に関する情報等の集積度合いが高まっていることから、企業は、自身の被害の局限化や法令遵守に留まらず、IT社会を構成する一員としての立場からも情報セキュリティ対策に取り組む責任があることを認識した上で、より積極的に対策に取り組むことが期待される。

また、企業の積極的な対策の実施が、個人の情報セキュリティに関する意識にも間接的に影響を及ぼすという循環を作ることも重要である。

(4) 個人

個人においては、自身が被害者とならない限り、自らが情報セキュリティ対策を行わないことが、実は他人に迷惑をかけているという認識が薄い状況にある。個人においても、老若男女を問わず各人がIT社会を構成する一員としての責任があり、「知らない人に付いていかない」といった極めて一般的な安全に対する認識と同等の認識を情報セキュリティに対しても、醸成していくことが必要である。自分の身は自分で守るという原点を明確に認識して行動することが期待される。

しかしながら、我が国の8000万人のインターネット利用者の情報セキュリティに対する理解が世代間で違うという点や、そもそも一般個人にとってはITの仕組みは理解しがたいという点から、個人の自己責任の限界を補うことが必須であり、他の対策実施領域に比べ、他の主体による支援が重要である。

第2節　問題の理解・解決を促進する主体の役割と連携

(1) 政府・地方公共団体－政策実施主体として－

政策立案・実施主体としての政府は、我が国全体の情報セキュリティの基盤を強化するため、制度整備、広報啓発や注意喚起、新技術の導入、教育環境の整備等に係る政策の立案・実施に、今まで以上に積極的に取り組む必要がある。

その際、政府のそれぞれの機関が、その役割に応じて政策の立案・実施に取り組むことが必要であるが、それに際しては、我が国全体として統一性がとれ、資源の重点的かつ戦略的な配分が図られた政策とすることが必要であり、縦割り的対応による戦略性のない取組みを排除していくことが必須である。

なお、政府が情報セキュリティ問題に関する政策を立案し、実施するにあたっては、

小さくて効率的な政府を実現するという点、そして、1）企業等各主体の競争的活動・自主的取組みを促進する部分と、2）市場原理等が働きにくい等の理由により、政府が主体的に関与を行う必要がある部分とに分けた取組みが必要であり、やみくもに政府の関与を強めていくことは有効ではないという点に留意する必要がある。

また、地方公共団体においても、地域における情報セキュリティの基盤を強化するため、地域における広報啓発や注意喚起、官民の連携・協力等に積極的に貢献することが望ましい。

（2）教育機関・研究機関

本章第1節（4）で示したように、我が国全般の情報セキュリティの基盤を強化するにあたり、個人が、老若男女を問わず情報セキュリティに関するリテラシーを向上させていくことが必要であり、そのためには初等中等教育から、そして世代横断的な情報セキュリティ教育を推進していくことが必要である。このため、初等中等教育や社会教育を行う教育機関、またはそれらを教える人材を教育する機関は、一般的な安全に対する認識と同等の認識を、情報セキュリティに関して醸成していくための取組みを、今まで以上に積極的に実施することが期待される。

また、大学をはじめとする高等教育機関及び独立行政法人等の研究機関は、情報セキュリティに関する高度の研究開発と人材育成の中核である。国家戦略的な方針に沿った研究開発・技術開発課題の受け皿としての取組みと、多面的・総合的能力を有する人材や情報セキュリティに関する教育者を育成する取組みを、今まで以上に積極的に実施することが期待される。

さらに、すべての教育機関・研究機関は、その環境において教育・研究が行われる場であること、また、教員等の基本的素養が醸成される場であることにかんがみ、当該機関自身の情報セキュリティ対策について、他の模範となる取組みを行うよう積極的に取り組んでいく必要がある。

（3）情報関連事業者・情報関連非営利組織

情報関連事業者は、政府機関・地方公共団体、重要インフラ、企業、個人のそれぞれが対策を実施するにあたり、直接的なサービスを実際に提供する主体であり、我が国の情報セキュリティの基盤強化を支える役割を担う。したがって、それぞれが提供する製品・サービスにおける脆弱性を極力排除する責任を負うという点を改めて認識し、より安全・安心な製品・サービスを提供するよう努める必要がある。なお、その際には、安全・安心なサービスの提供が、最終的には、その情報関連事業者の国際的競争力の向上にも繋がるというプラスの視点を持つことも重要である。

また、情報関連非営利組織が、全国的に、または地域ごとに設立され、活動を行っていることは、適切なITの利用・活用推進、トラブル発生時における利用者の対応能力向上、民間における連携対応体制の強化等の観点から極めて望ましいことであり、今後も、こうした非営利組織の積極的な活動が行われることが期待される。こうした非営利

組織には、情報セキュリティに関する啓発活動、警戒・脅威情報や脆弱性情報等の提供、そして我が国に求められる実践的人材の育成にも寄与することが期待される。

(4) メディア

メディアは、企業・個人をはじめとした対策を実施する各主体に対し、直接情報発信するという機能を持っており、「何のために情報セキュリティ対策を行うのか」といった点について、各主体における共通認識を形成することや、IT社会全体の堅牢性強化の必要性について国民全体が理解・共有することに大きな影響を与える存在である。このため、情報セキュリティに係る事件・事故のみならず、情報セキュリティ対策の好事例やIT社会全体の堅牢性強化の必要性等の情報セキュリティに関する幅広い情報が、メディアによって取り上げられるような環境の整備が必要である。

第3章　今後3年間に取り組む重点政策－「新しい官民連携モデル」の構築－

IT社会を構成するあらゆる主体が、前章に示した適切な役割分担の下で、「ITを安心して利用可能な環境」を構築するため、政府は、今後3年間、以下の重点政策に総合的に取組み、「新しい官民連携モデル」を構築する。

また、ここで示した政策の方向性に従い、政府は、毎年度、より具体的な施策の実施プログラムを「年度計画」として策定し、本基本計画の実現を図る。

第1節　対策実施4領域における情報セキュリティ対策の強化

第2章第1節で示したように、本基本計画においては、我が国全般の情報セキュリティ基盤の強化策を総合的に講じていくにあたり、対策を実際に適用し実施する主体の領域を、①政府機関・地方公共団体、②重要インフラ、③企業、④個人の4領域に分け、その対策のあり方を検討することが有効であるとの立場に立っている。政府は、この対策実施4領域について、前章第1節で示したそれぞれの役割に応じた対策を促進するための政策に、総合的に取り組んでいくことが必要である。

(1) 政府機関・地方公共団体

政府機関においては、第2章第1節で示したように、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し、常に最高水準の情報セキュリティ対策レベルを維持していくことが必要であり、また、地方公共団体においては、政府機関の取組みも踏まえながら情報セキュリティ対策の強化を図ることが必要である。

しかしながら、現在の状況を見ると、政府機関においては、情報セキュリティ水準に格差がある、特に内部からの脅威に対して脆弱である、緊急対応及び事業継続の観点からの取組みが不足している、年々複雑化する情報セキュリティ問題に対応するための高度な専門知識を有する人材が不足しているという問題を抱えている。また、地方公共団体においては、IT障害や情報漏洩などへの対策が徹底されておらず、また、地方公共団体間の情報共有体制が十分に構築されていないという問題を抱えている。

したがって、政府は、1）2008年度までに政府機関統一基準[13]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、地方公共団体については、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、今後3年間に、主に以下の政策に重点的に取り組んでいくこととする。

---

13 「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」（　　年　月　日情報セキュリティ政策会議決定）を指す。以下同じ。

ア 政府機関

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。

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。

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。

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。

（イ）セキュリティ強化に資する新規システム（機能）の導入検討とその実現

次世代の電子政府構築に向けて、政府全体の業務・システムの基盤となる共通的なプラットフォームの構築・整備について検討等を行うことが重要である。そのプラットフォームについてセキュリティ強化を図るため、IPv6、国家公務員身分証ICカード、暗号、電子署名、生体認証等の新規システム（機能）の導入について総合

的な検討等を行い、その実現を推進する。

特に、今後、すべての政府機関の情報システムがIPv6を早期に利用できるようにするため、原則として、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。

（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[14]の利用を推進する。

④サイバー攻撃等に対する政府機関における緊急対応能力の強化

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

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。

イ　地方公共団体

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。

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

[14]「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。

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。

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。

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。

（2）重要インフラ

重要インフラにおいては、第2章第1節で示したようにそのサービスの安定的供給が最優先課題であるという面から、各事業において発生するIT障害が国民生活・社会経済活動に重大な影響を及ぼさないよう対策を実施することが必要である。しかしながら、現在の状況を見ると、サイバー攻撃等意図的要因に起因する障害以外のIT障害への対策についての検討が不足しており、官民の情報共有体制が十分に構築されていない等の問題を抱えている。したがって、政府は、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、今後3年間に、主に以下の政策に重点的に取り組んでいくこととする。なお、重要インフラの情報セキュリティ対策については、「重要インフラの情報セキュリティ対策に係る行動計画」（　　年　月　日情報セキュリティ政策会議決定）が別途定められており、本行動計画に従って、より具体的な対策に取り組んでいくこととする。

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』[15]策定にあたっての指針」[16]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。

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

15 「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。

16 「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」（　　年　月　日情報セキュリティ政策会議決定）

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。

(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。

(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。

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。

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。

(3) 企業

企業においては、第2章第1節で示したように、グローバル社会における経済発展の担い手であると同時に、ITの根幹を担う製品・サービス等を提供する主体でもあるという面から、対策を実施することが必要である。しかしながら、現在の状況を見ると、企業におけるセキュリティ対策が市場評価に十分に繋がっていない、企業における情報セキュリティ人材の確保・育成が十分でないという問題を抱えている。したがって、政府は、2009年度初めには、すべての公開企業が、リスクに応じた適切な対策を実施していることを目指し、今後3年間に、主に以下の政策に重点的に取り組んでいくこととする。

①企業の情報セキュリティ対策が市場評価に繋がる環境の整備

社会的責任にも配慮したコーポレートガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用することを推進する。このため、情報セキュリティ対策ベンチマーク、情報セキュリティ報告書モデル及び事業継続計画策定ガイドラインの普及・改善を図るとともに、情報システム等の政府調達の競争参加者に対して、必要に応じて、これらの制度や第三者評価の結果等を活用した情報セキュリティ対策レベルの評価を入札条件等の一つとする。また、政府が推進する情報セキュリティに関する取組みについて、政府全体としての整合性を確保する。

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。

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。

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。

(4) 個人

個人においては、第2章第1節で示したように、8000万人のインターネット利用者の情報セキュリティに対する理解が均一ではないという現状を認識し、老若男女を問わず各人がその状況に応じて情報セキュリティに関するリテラシーを向上させることを支援すべく、関係する各主体が様々な対策を実施することが必要である。しかしながら、現在の状況を見ると、個人が情報セキュリティを当たり前のこととして認識できる環境、また、一般個人にとってITの仕組みは理解しがたいにも関わらず、個人の自己責任の限界を補う環境が不足している、という問題を抱えている。したがって、政府は、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、今後3年間に、主に以下の政策に重点的に取り組んでいくこととする。

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。

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。

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。

第2節　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、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の政策に総合的に取り組んでいくことが必要である。

(1) 情報セキュリティ技術戦略の推進

第1章に述べた「ITを安心して利用可能な環境」を実現するためには、情報セキュリティ技術の高度化と、その技術を理解した上での利用・活用が不可欠である。しかし、現状は、1) 急速に拡大するIT利用・活用に、情報セキュリティ技術の開発が対応できていない、2) 既存の情報セキュリティ技術の限界を補完する組織・人間系の管理手法とのバランスを欠くという問題が存在している。

したがって、政府は、民間部門における取組みとの役割分担を明確にしつつ、今後3年間に、情報セキュリティに関する技術戦略として、主に以下の政策に重点的に取り組んでいくこととする。

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。

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。

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。

(2) 情報セキュリティ人材の育成・確保

第1章に述べた「ITを安心して利用可能な環境」を実現するためには、対策実施主体における情報セキュリティ対策の運用や、情報セキュリティに関する高度な研究開発・技術開発を支える人材の育成・確保が不可欠である。

この際、高い能力を有する情報セキュリティ技術者の育成に努めることは重要であるが、これに加えて、広い知識と鋭い洞察力を持つ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やIT分野に関する法律家等、多面的・総合的能力を有する実務家・専門家の育成が必要なこと、人材の育成には時間を要すること、に留意が必要である。

したがって、政府は、今後3年間に、政府機関の対策のための人材育成（第3章第1節（1）ア⑤）、重要インフラの対策のための人材育成（第3章第1節（2）④）、企業の対策のための人材育成（第3章第1節（3）③）に取り組むと同時に、主に以下の政策に重点的に取り組んでいくこととする。

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[17]への主体的な取組みを促進する。

②情報セキュリティに関する資格制度の体系化

高い能力を有する情報セキュリティ技術者、各組織における最高情報セキュリティ責任者（CISO）、各組織の情報システムの運用担当者等それぞれに応じた適切なスキルを確定し、情報セキュリティに関する資格制度の体系化を推進する。

(3) 国際連携・協調の推進

ITの利用・活用と経済活動のグローバル化が進展する中、国際的にも、情報セキュリティの基盤を整備し、その便益を享受できるようにすることが重要である。その際、1）情報セキュリティの脅威がボーダーレス化し、増加・多様化していることから、国際的に協調しつつ、取り組んでいくことが重要であるとともに、2）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、情報セキュリティの「ジャパンモデル」を国際的に提示していくことも不可欠である。

以上の観点を踏まえ、政府は、今後3年間に、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、主に以下の政策に重点的に取り組んでいくこととする。

---

17 「リカレント教育」とは、「職業人を中心とした社会人に対し、学校における教育を終えて社会に出た後に行われる各種教育」を指す。

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。

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。

（4）犯罪の取締り及び権利利益の保護・救済

「ＩＴを安心して利用可能な環境」を構築するためには、サイバー犯罪が未然に防がれること、サイバー犯罪を行った者が検挙されること、サイバー空間で権利や利益を侵害された者が保護・救済されること等、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。

以上の観点を踏まえ、政府は、今後3年間に、主に以下の政策に重点的に取り組んでいくこととする。

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。

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。

第4章　政策の推進体制と持続的改善の構造

政府は、今後3年間、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

「新しい官民連携モデルの構築」による「情報セキュリティ先進国」の進展を目指し、「ITを安心して利用可能な環境」の構築を行うためには、あらゆる主体の参加が必要である。その中で、政府は、第1章の基本理念に示すように公的対応能力を強化する一方で、第2章第2節に示した政府の役割を調整しながら、第3章に示した重点政策を中心に、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べく、全体としての適正な資源配分を行っていく必要がある。

(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。

(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。

第2節　他の関係機関等との連携

本基本計画は、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、本基本計画が「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。

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、本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。

(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。

(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、本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。

(4) 本基本計画の見直し

政府は、本基本計画について、3年毎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。