技術戦略専門委員会報告書

－　力強いIT社会の発展を下支えする情報セキュリティ
研究開発・技術開発の戦略的推進　－

2005年11月17日

情報セキュリティ政策会議

技術戦略専門委員会

目　　次

はじめに ..... **- 2 -**

委員名簿 ..... **- 6 -**

1. 情報セキュリティ技術戦略を考える上での基本的な考え方 ..... **- 7 -**

1. 1. これまでの情報セキュリティ技術の開発モデルー二つの目標設定ー ..... - 8 -
1. 2. これまでの情報セキュリティ技術の社会展開プロセス ..... - 9 -
1. 3. 我が国における情報セキュリティ上の問題点と問題解決に利用される技術の役割とその方向性 ..... - 12 -
1. 4. 情報セキュリティ技術を支える環境整備の必要性 ..... - 16 -
(参考)安心・安全領域の中での情報セキュリティの特殊性 ..... - 20 -

2. 情報セキュリティ技術の研究開発・技術開発を推進するための新しい構造のあり方 ..... **- 22 -**

2. 1. 投資領域設定の継続的見直し構造の実現 ..... - 22 -
2. 2. 成果利用までを見据えた研究開発・技術開発の実施体制の構築 ..... - 22 -

3. 情報セキュリティ技術開発の重点化と環境整備のあり方 ..... **- 26 -**

3. 1. 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を実現するための具体的な方向性 ..... - 26 -
3. 2. 情報セキュリティ技術を支える環境整備 ..... - 30 -

4.「グランドチャレンジ型」研究開発・技術開発の推進 ..... **- 33 -**

4. 1.「グランドチャレンジ型」研究開発・技術開発とは ..... - 33 -
4. 2. 情報セキュリティ領域における「グランドチャレンジ型」研究開発・技術開発の実施 ..... - 33 -

(参考)技術戦略専門委員会報告書までの検討の経緯 ..... **- 35 -**

はじめに

一般に、研究開発・技術開発は、様々な要素を含んだ投資活動である。高度情報通信ネットワーク社会の礎となる科学技術は、近年官民において積極的に研究開発・技術開発に投資され、その成果が短時間に社会展開をする特徴を持つ。また、研究開発・技術開発のプロセス全体が、常に国際競争に晒されている。このため、世界各国がそれぞれより多くの成果を得るために、科学技術開発投資の戦略を策定し、同時に官民それぞれが投資領域の先鋭化を進めている。各国とも、自国が高いプレゼンスを持つ領域の強化を進め、さらに激しい競争状態にあるところでは一歩でも他国に先んずることを目標として、開発投資を行っているのが現状と言える。

（我が国の科学技術政策における「3つの基本理念」）

我が国の科学技術政策は、科学技術創造立国を目指し、科学技術基本計画に基づき科学技術基本計画の下に推進されている。現在は2001年3月に閣議決定された第2期基本計画の最終年である。第2期基本計画では、我が国の科学技術政策における「3つの基本理念」を提示した。

① 知の創造と活用により世界に貢献できる国　ー新しい知の創造ー
② 国際競争力があり持続的発展ができる国　ー知による活力の創出ー
③ 安心・安全で質の高い生活のできる国　ー知による豊かな社会の創生ー

この基本理念に基づき様々な政策が示されたが、さらに情報通信分野、特に情報セキュリティに関連する重点化の考え方では、高度情報通信ネットワーク社会の出現と、そこでの情報通信基盤が安心して安全な国民生活の基盤であることを認知し、「ネットワーク上での安全・安心な活動を担保するための制度等の整備、技術開発のためのテストベッドの提供、標準化等の国際的な取組み、国民が情報通信技術を活用できるようにするための教育及び学習の振興等に取り組む。さらに、コンピュータの誤動作・機能不全による災害、ネットワークを介した不正行為による社会システムの機能停止への対策や、プライバシーなどの情報管理のあり方の検討、情報格差の是正について留意する。」（第2章重要政策、「2. 国家的・社会的課題に対応した研究開発の重点化」（2）情報通信分野）としている。

（急激に進展する情報セキュリティ領域）

この計画に基づいて、過去4年間に特に政府主導の研究開発・技術開発投資が行われ、一定の成果を収めてきている。しかし、情報セキュリティ領域では、2001年に想定した社会変化よりも、それ以上の社会変化が起きてしまったというのが率直な状況認識と言えるのではないか。特に、e-Japan戦略による高度情報通信ネットワー

ク構築への官民の取組みが成果を挙げ、社会経済活動、国民生活の多くが情報通信基盤に大きく依存するようになったことは、その代表例と言えよう。同時に、情報漏洩事件の多発、社会経済活動へ多大な影響を及ぼす重要インフラにおけるIT障害[1]の発生、フィッシング[2]等のネットワーク利用犯罪の多発など、高度情報通信ネットワーク社会の影の部分の増大も顕著となっている。このような状況に対応した、新たな研究開発・技術開発に対する投資戦略が必要になることは言うまでもない。

このような状況の中で、本年、総合科学技術会議基本政策専門調査会では、現在第3期基本計画の策定を進めており、2005年6月に「科学技術基本政策策定の基本方針」をとりまとめ、第3期基本計画策定に向けての、いわゆる「中間とりまとめ」を示した。この「科学技術基本政策策定の基本方針」では、【理念3】「健康と安全を守る」・【目標6】「安全が誇りとなる国」の中で、情報セキュリティへの対応が改めて「暮らしの安全確保」という政策目標の中で捉えられており、より社会経済活動・国民生活に密着した問題として認識されている。本報告書を作成している2005年11月現在、具体的な第3期基本計画のとりまとめが進められており、より具体的な投資方針が明らかになることが期待されている。

（情報セキュリティ問題への取組み強化）

一方、我が国における情報セキュリティ問題への取組みも2004年から大きく変化を遂げている。2001年からe-Japan戦略及びe-Japan戦略IIに基づいて進められてきた高度情報通信ネットワーク社会実現の一環として、2004年2月に発表されたe-Japan戦略II加速化パッケージにおいて、情報セキュリティ問題への取組み強化が政府方針として示され、我が国の情報セキュリティへの取組みについての設計と実施を積極的に展開してきた。内閣官房においては、情報セキュリティ問題に関する我が国の全体像を検討するにあたって、これまで、対策に取り組むべき当事者の領域を、概ね、政府機関、重要インフラ（地方公共団体を含む）、企業、個人に分け、それぞれの特性に応じた対策のあり方を検討する手法を採ってきた。2004年7月には、高度情報通信ネットワーク推進戦略本部（以下、「IT戦略本部」という。）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（委員長；金杉明信　日本電気（株）代表取締役執行役員社長）を設置し、情報セキュリティに対する我が国の新たな取組みについての検討を開始した。現在までに、政府機関の対策については2004年11月に第1次提言[3]、重要インフラの対策については2005年4月に第2次提言[4]として公表され、それを受けた政府の取組みも開始されている。具

1 情報技術の機能不全が引き起こす障害。

2 金融機関（銀行やクレジットカード会社）などを装った電子メールを送り、住所、氏名、銀行口座番号、クレジットカード番号等の個人情報を詐取する行為。

3 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） http://www.bits.go.jp/conference/kihon/index.html#teigen

4 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） http://www.bits.go.jp/conference/kihon/index.html#teigen

体的には、2005年4月には、まず、内閣官房に政府における情報セキュリティ確保の取組みについて中心的役割を果たす内閣官房情報セキュリティセンター（NISC）が設置され、2005年5月には、IT戦略本部の下に情報セキュリティ政策会議が設置された。そして、政府の情報システムにおける情報セキュリティ確保についての取組み、重要インフラにおける情報セキュリティ確保のためのフレームワーク作り等が行われている状況にある。

（情報セキュリティにおける技術戦略の必要性）

しかし、これらの検討において、常に情報セキュリティ確保に資する技術をどのように生み出し、社会に展開していくか、いわゆる技術戦略についての議論が十分に果たされていたとはいえない。一方で、先に述べたように、我が国の国民生活・経済活動のあらゆる側面において、情報技術（以下、「IT」という。）の果たす役割が年々増加し、ITへの依存度を急激に高めている中、情報セキュリティ技術の研究開発・技術開発を促進し、その社会展開を積極的に行う戦略が必要になっていることは言うまでもない。このような問題意識から、既に総合科学技術会議において第3期基本計画策定が進められている中で、情報セキュリティに焦点を当てた技術戦略のあり方を検討し、総合科学技術会議と協力しながら、産官学を通した我が国全体としての新しい取組みを行っていくことが必要な時期に来ていると言える。情報セキュリティ政策会議の下に置かれた本専門委員会の役割は、まさにこのあり方を提言することにあるものと言える。

本専門委員会での検討では、まず高度情報通信ネットワーク社会において、安全・安心にITを利用することを可能とし、ITが真に依存可能な基盤となるための技術全般が情報セキュリティ技術であるという捉え方をした。これは、単にその基盤を形成するために必要となるソフトウェア、コンピュータハードウェア、ネットワークにおける情報セキュリティ技術だけではなく、それを用いて実現されたアプリケーション、あるいは、社会的な機能を強固なものにするための技術までを考慮に入れた検討が必要である。

また、一口に「真にITが依存可能な基盤となるための技術」といっても、我が国の国民生活・経済活動を構成する主体ごと、すなわち、1）政府機関、2）重要インフラ、3）企業（事業者）、4）個人（国民）それぞれの主体に応じ、必要となる技術要素の性質は異なってくる。例えば、政府機関の情報セキュリティ対策の側面から見ると、企業・国民から負託された情報の管理に責任を有するという観点からの高い情報セキュリティレベルを実現するための技術が必要となるのに対し、個人（国民）の対策の側面から見ると、ユーザの負担を軽減し、個人の知識等に依存せずに情報セキュリティ機能を活用できる製品・サービスの開発・供給が行われるような技術が必要という特性がある。こうした多様性を踏まえた技術戦略の策定が必須である。

（情報セキュリティ技術を高度化させ、迅速な社会展開を果たすための方策）

本報告書では、我が国の情報セキュリティ技術を高度化させ、迅速な社会展開を果たすための方策、また、重点化すべき領域を提示している。これは、直接には政府における研究開発・技術開発への投資のあり方を示しているが、同時に民間における技術開発が促進されることが期待される方向性をも示している。

また、政府が行う研究開発・技術開発への投資では、本報告書が述べる戦略性を持った実施が必要であると考えるが、同時に、数多くの研究機関で研究に従事する研究者達の自由かつ独創的な発想から切り拓かれる研究領域の拡大・活性化にも大きく期待している。この意味で、情報セキュリティ確保のために我が国において実施される研究の多様性維持についても、十分な配慮を行い、広範な萌芽的研究[5]が生み出される環境整備にも、政府は最大限努力することが必須であることは言うまでもない。

2005年11月17日
情報セキュリティ政策会議
技術戦略専門委員会　委員長
佐々木　良一

[5] 「萌芽的研究」は、独創的な発想、特に意外性のある着想に基づく芽生え期の研究のことを指す。科学研究費補助金の研究種目の１つ。

委員名簿

【委員長】

佐々木　良一	東京電機大学教授

【委員】

河田　惠昭	京都大学防災研究所所長
志方　俊之	帝京大学教授
篠田　陽一	北陸先端科学技術大学院大学教授
須藤　修	東京大学大学院教授
田尾　陽一	セコム株式会社顧問
中西　晶	明治大学助教授
西尾　章治郎	大阪大学大学院教授（文部科学省科学官）
宮川　晋	ＮＴＴコミュニケーションズ株式会社先端ＩＰアーキテクチャセンタ・経営企画部（兼務）担当部長
米澤　明憲	東京大学大学院教授

（五十音順、敬称略）

１．情報セキュリティ技術戦略を考える上での基本的な考え方

我が国においてコンピュータが社会進出を果たしたのは1960年代であり、その当時から情報セキュリティ技術が生み出され、活用されてきた。それから半世紀の間、コンピュータとネットワークの普及と利用形態の変遷に応じて、求められる情報セキュリティ技術も大きく変化を遂げてきている。本章では、まず情報セキュリティ技術の開発モデルを整理した上で、我が国における情報セキュリティ上の問題点と、その問題解決に利用される技術の役割を概観する。さらに、そもそも情報セキュリティ技術は何のために求められるのか、そして将来的にどのような目標に向かって研究開発・技術開発が行われるべきなのか、いわば情報セキュリティ技術戦略の基本的な考え方を示す。その際、情報セキュリティ技術領域は他の安心・安全を確保する技術領域（大規模災害、各種犯罪等への対策）とは異なり、技術投資によって特定のリスクが解消してしまうことや、基盤技術の多様性によってリスク低減を図ることができることなどを考慮する。なお、本報告書の全体像を図1に示す。

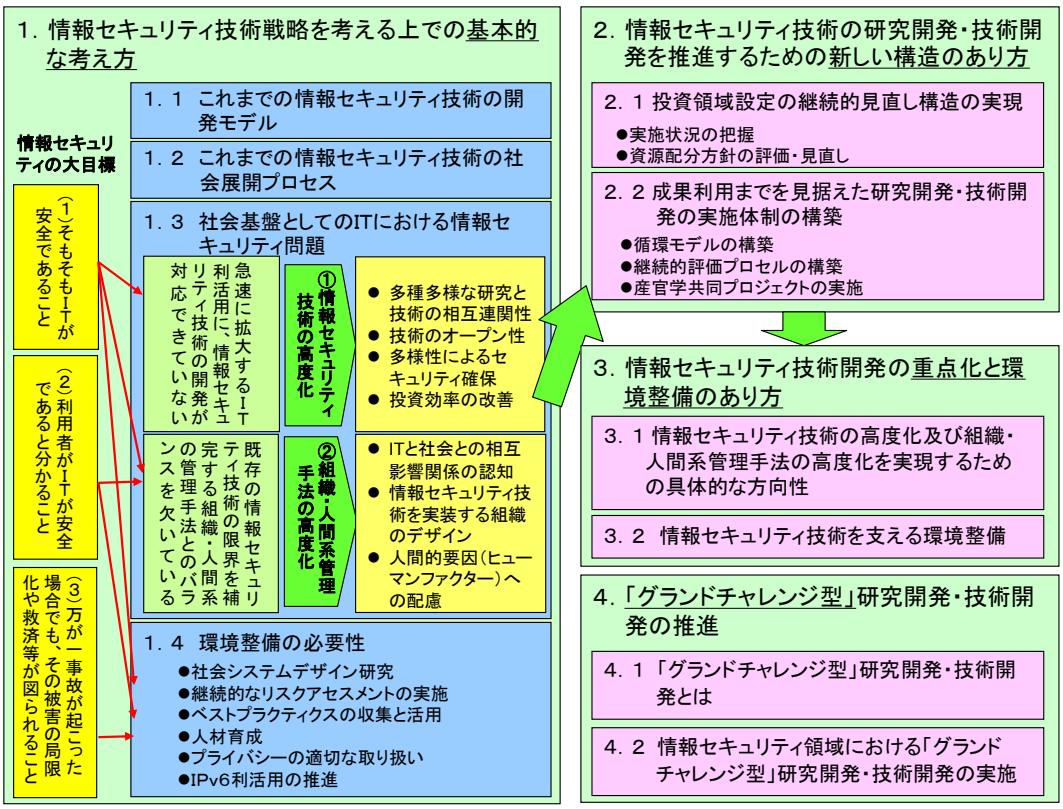

図1　報告書の全体像

1．1．これまでの情報セキュリティ技術の開発モデルー二つの目標設定ー

これまで、計算機科学などの研究領域で「情報セキュリティ技術」は、ネットワーク化された情報処理システム群における、1）蓄積されたデータ、2）情報処理そのもの、3）システム間で交換されるトランザクションのデータ、4）システムとネットワークそのものの防護のために資する技術として考えられてきた。例えば、情報セキュリティ技術として代表的な暗号技術は、情報セキュリティの様々な基礎を形成している。しかし、暗号技術だけで情報セキュリティ技術は成立するのではなく、プログラミング言語とライブラリ[6]を含めた処理系におけるセキュリティ確保の取組み、オペレーティングシステム（以下、「OS」という。）やシステムソフトウェア[7]におけるセキュリティ機能の強化、ネットワークプロトコル[8]における暗号化や認証機能の追加など、様々な角度から情報セキュリティ技術が生み出されてきている。

これまでの情報セキュリティ技術の研究開発・技術開発では、大きく二つの目標設定が行われている。

一つが、現在運用されている情報システムにおけるリスクを把握し、そのリスクを低減し、かつ、ゼロに限りなく近づけるための技術開発である。これは、既存の情報システムを構成するシーズ技術を発展させ、さらに、既存技術を積極的に改良することにより情報セキュリティ機能を強化する、いわば短期的な目標設定である。例えば、現在のOSの情報セキュリティの観点からの問題点を指摘し、具体的にその問題を解決するような技術開発や、運用技術の開発は、短期的な目標設定によって実現されている。また、システムやネットワークに発生する障害を回避し、仮に障害が発生してもシステム全体が機能を提供し続けるためのフォールトトレラントデザイン[9]も、近年注目されている情報セキュリティ技術の一つといえる。

一方、脅威をモデル化し、情報処理システムとネットワークにおけるリスクをゼロにするための新たなアーキテクチャを実現する、中長期的な目標設定を行った研究開発も実施されている。例えば、最近では、既知のセキュリティホール[10]を徹底してモデル化し、同様のセキュリティホールがプログラマの手によって組み込まれることのないプログラミング言語処理系の開発、情報セキュリティ機能を徹底的に強化し、かつ、検証可能な形で構成した高信頼OS（あるいはセキュアOSとも呼ぶ）の開発、現在多くの利用者を苦しめているコンピュータウィルスなどが発生しない情報処理基盤環境構築など、根本的に情報セキュリティの問題を解決する新たなアーキテクチ

---

6 ある目的や規則に沿ってまとめられたソフトウェア部品の集合体のこと。

7 カーネルやOSに機能を追加するツールやドライバなど、OSを動作させるために必要となるソフトウェア。

8 ネットワークを介してコンピュータ同士が通信を行なう上で、相互に決められた約束事の集合。通信手順、通信規約などと呼ばれることもある。

9 システムの一部に何らかの障害が発生した場合でも、システムを停止せずに継続処理できるようにすること。

10 ソフトウェアの設計ミスなどによって生じた、システムのセキュリティ上の弱点。

ャ研究が代表例と言える。

1．2．これまでの情報セキュリティ技術の社会展開プロセス

この二つの目標設定によって生み出されてきた種々の情報セキュリティ技術は、ネットワーク化された情報処理システム群が1990年代までに急速に社会基盤化し、さらに現在の高度情報通信ネットワーク社会を形成する過程で大きな役割を果たした。

（1）基礎的な情報セキュリティ技術の普及

まず、1980年代中盤からの企業、研究機関におけるコンピュータの大量導入、LAN[11]に代表されるコンピュータネットワークの導入、さらには大企業におけるエンタープライズネットワーク[12]構築が引き金となり、多くの情報セキュリティ技術が実用化された。現在多くのシステムで利用されている基礎的な情報セキュリティ技術が提供され、データの暗号化、ユーザ認証技術、通信路での暗号化、可用性管理と運用技術向上の基礎が形成された。この当時は、様々なアーキテクチャが提供され、革新的な技術導入による大幅な機能拡張と信頼性確保を達成している。

（2）インターネットによる分散処理への適合

1990年代になると、世界規模のオープンなコンピュータネットワークであるインターネットが社会基盤化を果たす。それまでのコンピュータの利用は集中型情報処理が中心であったが、インターネットの社会基盤化によって、オープンネットワークにおける分散型情報処理にモデルが大きくシフトすることになった。これは、従来の情報セキュリティ技術に大きな変革を求めることになり、オープンなネットワーク環境を前提とした情報セキュリティ技術への必要性が明確に意識された。この結果、ユーザ認証ではPKI (Public Key Infrastructure)[13]が実現され、SSL/TLS[14]等の暗号化通信機能が広く使われるようになった。また、電子メールの暗号化など、ノード間で交換されるデータの暗号化も広く実現されてきている。これらの機能が充実したことにより、実アプリケーションの広範な実現の基礎が作り上げられたと言えよう。このような情報セキュリティ機能の一般化によって、インターネットは経済活動で本格的に利用される段階へと突入していく（図2）。

---

11 電気通信事業者の回線を経由しない構内情報通信網のこと。

12 大企業や中央官庁等の組織内のネットワークのこと。

13 公開鍵暗号技術と電子署名を使って、インターネットで安全な通信ができるようにするための環境のこと。「公開鍵基盤」と訳される。

14 公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせ、データの盗聴や改ざん、なりすましを防ぐ機能。

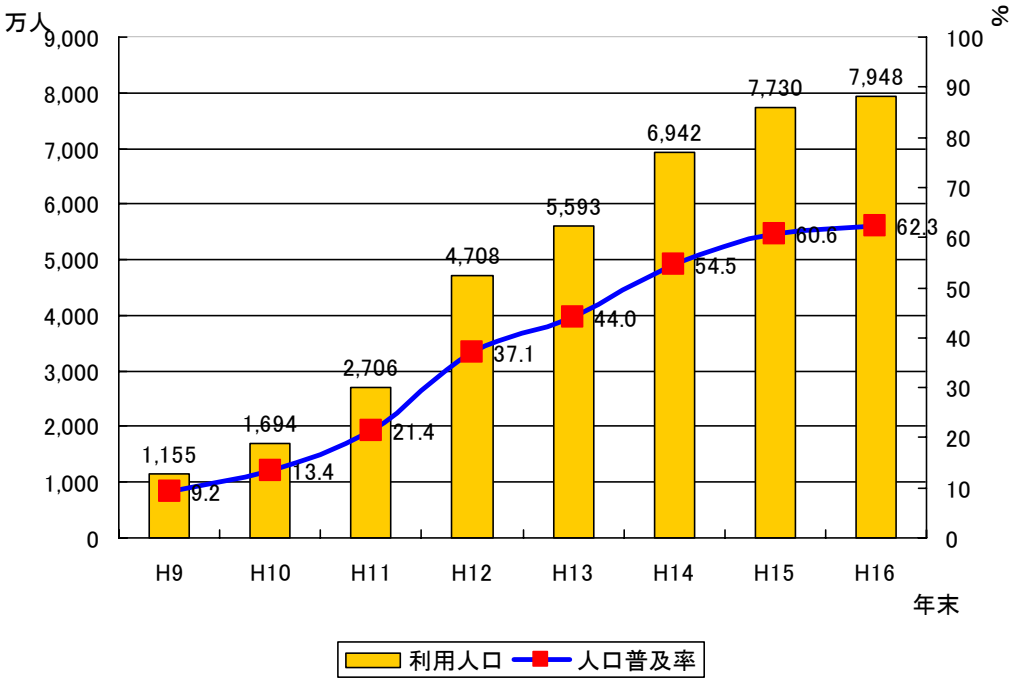

図2　インターネット普及状況

（出典：平成 16 年「通信利用状況調査」）

（3）依存可能な社会基盤に向けて

2000年代になると、我が国はインターネットを中核とする高度情報通信ネットワーク社会構築に本格的に着手する。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（以下、「IT基本法」という。）及び2001年に策定されたe-Japan 戦略では、社会基盤としてのインターネットを、我が国の国民生活・経済活動で広く利用し、「インターネットその他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世界的規模で入手し、共有し、あるいは発信することにより、あらゆる分野における創造的かつ活力ある発展が可能となる社会」を目標とした。官民協力しての取組みの結果、インフラ整備は順調に推移し、現在では世界最高水準のブロードバンドインターネットが利用可能な社会となっている。また、図2に示したようにインターネットの普及も急速に進み、国民の大多数がインターネットを活用するようになっている。ブロードバンドインターネット上では多種多様なサービスが提供され、今やインターネットは我が国の経済活動・国民生活において無くてはならないものとなり、依存度を高めていると言える。

一方、同時にIT基本法第22条では、「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。」とし、情報セキュリティ技術の広範な社会展開と、同時にそれを支える社会制度の創設が求められている。

（4）現在の取組み

現在、政府では e-Japan 戦略 II の下に、高度情報通信ネットワーク社会構築に積極的に取り組んでいる。情報セキュリティ確保の目標は、我が国の国民生活・経済活動で広く利用されるネットワーク化された情報処理システム群とそれらが提供する機能、いわゆるITが、依存可能な社会基盤として持続的に成立することである。

この目標達成のために、2000年以来、情報セキュリティ技術への積極的投資が公的研究資金においても、また、民間における技術開発でも積極的に行われてきた。また、政府においては、高度情報通信ネットワーク社会における情報セキュリティ確保のために必要な種々の施策を実施してきた。

研究開発・技術開発においては、現在のIT基盤において認められる情報セキュリティ課題（例えばコンピュータウィルスの蔓延や情報システム障害の発生など）を解決することを目標とした、短期集中型の技術開発が数多く行われている。現在では、迷惑メール[15]及びフィッシング、さらには近年問題が深刻化しているボットネット[16]等の課題を解決するための技術開発が積極的に行われている。一方で、セキュアOSやセキュリティを意識した言語処理系の実現など、中長期課題への取組みも実施されている。

一方、近年問題となっているのが、例えば食品流通、医療等の、ITの適用が比較的遅れていた領域における情報セキュリティ確保の問題である。こうした領域において、IT が適用されたことから産み出されたリスクが顕在化しつつある。そのリスクを解明し、新たな技術要件を特定し、それを満足するための研究開発・技術開発の実施も必要であることが、近年強く認知されている。e-Japan 戦略 II においても、「安心・安全な IT 社会の実現」という目標の下、産官学での広範な取組みによる情報セキュリティ技術の研究開発・技術開発と、多種多様な国民生活・経済活動領域への適用を行い、社会システムそのものの信頼性向上を希求することが必須であるとしている。

さらに、政府は、産み出される情報セキュリティ技術の普及を加速させるため、情報セキュリティ政策会議や内閣官房情報セキュリティセンターの設置を行い、我が国の戦略策定を行う体制を整備した。同時に、総合科学技術会議や中央防災会議等、関連する政策決定母体との連携を促進し、成果の迅速な利活用の広

---

15 公開されている Web サイトなどから手に入れた e-mail アドレスに向けて、営利目的のメールを無差別に大量配信すること。インターネットを利用したダイレクトメール。

16 コンピュータウィルスの一種で、コンピュータに感染し、そのコンピュータを、ネットワーク (インターネット)を通じて外部から操ることを目的として作成されたプログラム。

範囲な実施を実現する体制整備を開始している。

1．3．我が国における情報セキュリティ上の問題点と問題解決に利用される技術の役割とその方向性

上に示した形で、現在まで、情報セキュリティ技術に関する取組みを進めてきたところであるが、我が国の社会基盤としてのITにおける情報セキュリティ問題は、年々複雑化しており、技術、社会制度、運用環境等、多面的かつ総合的に問題解決に取り組まなければならない。

以下、現在の我が国における情報セキュリティ上の問題点全体を俯瞰した上で、その問題解決における技術の役割と今後の方向性を提示する。また、次節では、この技術の役割を支える環境整備の必要性とその方向性を提示する。

（1） 我が国における情報セキュリティ上の問題点の全体俯瞰

我が国の国民生活・経済活動のあらゆる場面においてITが深く利用されるようになった現在、我が国の社会経済活動の持続的発展と国際競争力の維持という観点から、情報セキュリティ確保のための取組みが不可欠である。すなわち、IT基本法にいう「高度情報通信ネットワークを安心して利用可能」[17]な環境とすることが求められている。ここでいう、「安心して利用可能」な環境とは、大きく、以下の3つの条件が満足される環境として構築されるべきものと考えられる。

1) そもそも「高度情報通信ネットワーク（IT）が安全である」こと。
2) 利用者が、「高度情報通信ネットワーク（IT）が安全である」と分かる（認識・体感できる）こと。
3) 万が一事故が起こった場合でも、その被害の局限化や救済等が図られるとともに業務の継続性が保たれること。

我が国では IT 基本法により、上記3条件を満足する「安心して利用可能」な環境の実現が求められているものの、これまでは顕在化した問題のみに対処する対症療法的な対応が先行してきたため、利用者の視点からみれば、この3条件を満足した環境として実現できているとは言い難い。

17 高度情報通信ネットワーク社会形成基本法第22条（高度情報通信ネットワークの安全性の確保等）には以下のように記されている。「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。」