

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と。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取る行為。

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#eigen>

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#eigen>

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、産官学を通じ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、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。

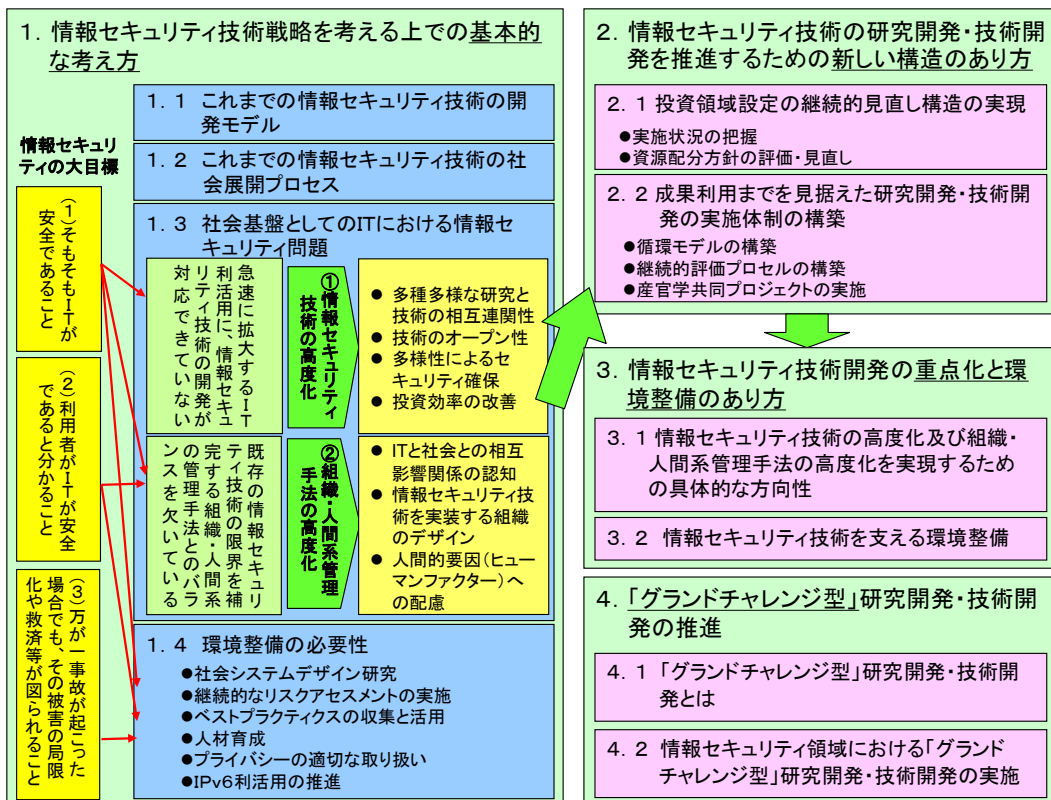


図1 報告書の全体像

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イ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

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。

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、LAN¹¹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/TLS¹⁴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。

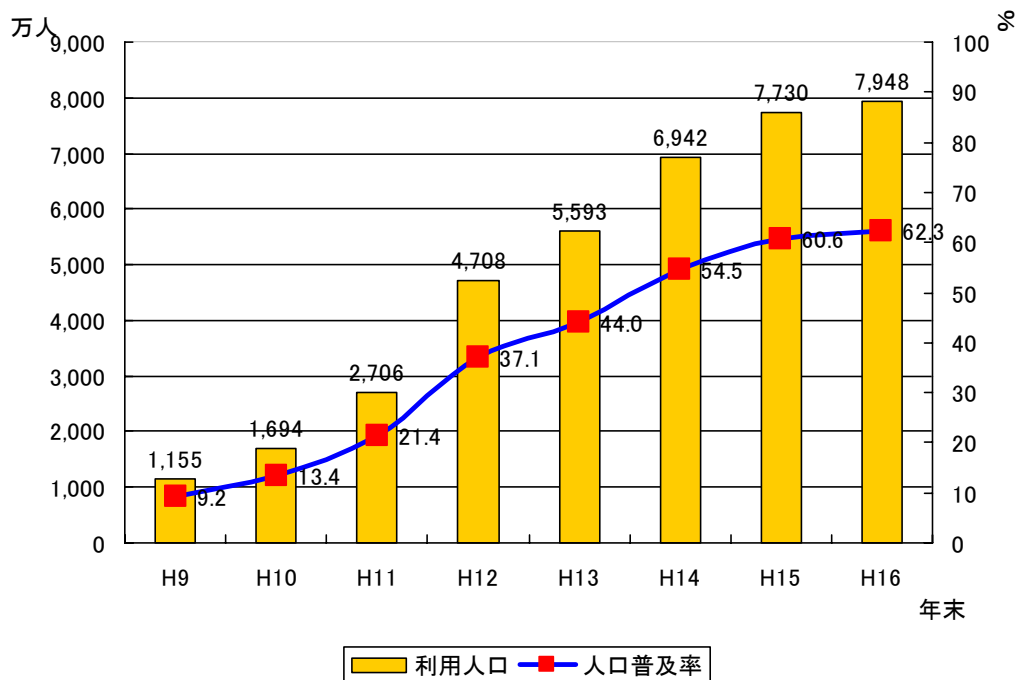


図2 インターネット普及状況

(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的一种で、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。」

(2) 情報セキュリティ技術の役割と今後の方向性

上に述べた3条件を満足する環境を実現するにあたり、情報セキュリティ技術の役割は、まず上記1)の「高度情報通信ネットワーク(IT)が安全である」状態を極限まで高めることである。そして、上記2)の利用者が「高度情報通信ネットワーク(IT)が安全である」ことを分かるようにするという要請に応えるために、技術が活用されることである。

しかしながら、現状を見れば、情報セキュリティ技術が果たす上記の二つの理想的な役割は実現されているとは言い難い。情報システムの不具合や内外から悪意ある攻撃が、原因を引き起こした当事者やトラブルに見舞われた被害者だけの問題ではなく、一国の経済活動全体の停滞や国民全体の生命・財産そのものに関わるリスクをもたらしかねない問題へと拡大する恐れがある。例えば、次のような問題点が発生している。

➤ 例1: DDoS 攻撃

現在のインターネットで深刻化しているのが、複数のホストから特定の攻撃目標に対して、同時に大量のパケットを送りつける分散 DoS 攻撃、いわゆる DDoS 攻撃(Distributed Denial of Service 攻撃)である。特に、最近ではボットネットを利用した DDoS 攻撃が問題となっている。この問題を解決するためには、技術的な解決方法、中でも、インターネットそのものの技術的改善方向の提示が必要である。

➤ 例2: 内部の者の行為による企業からの情報漏洩

昨今多発している企業等からの情報漏洩問題においては、強力なユーザ認証に基づいたアクセス制御等のある程度の技術的措置を講じてはいるものの、保護されるべき情報を取り扱う担当者の選別や、適切な情報保護レベルの設定の不備等が原因の一端をなしているとの指摘が多い。

すなわち、より具体的に言えば、1)急速に拡大するIT利活用に、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いているとの問題があると言える。

これを解決するためには、1)そもそもの情報セキュリティ技術の高度化を図ると同時に、2)開発された情報セキュリティ技術が実環境で効果的、効率的に運用されるため組織・人間系の管理手法の高度化の両面からの取組みが必要である。

1)情報セキュリティ技術の高度化

急速に拡大するIT利活用に対応すべく、以下の点に留意しつつ、情報セキュリティ技術高度化の取組みを実施することが必要である。

①多種多様な研究と技術の相互関連性

情報セキュリティ技術は、様々な技術の成果に立脚する、いわゆる複合技術である。情報セキュリティ技術の高度化を達成するためには、情報セキュリティ技術を成立させている様々な基礎技術、関連技術についても、その高度化が必要となる。

例えば、電子メールの暗号化技術を考えてみても、単に暗号技術だけでなく、通信プロトコル技術、復号処理を安全に行うための関連技術が必要である。さらに、それぞれの技術は、例えば暗号であれば応用数学というように、基本的な技術開発や学術成果、基礎研究の成果に依存しているところがある。

このような技術と学術成果の連関構造を理解し、バランスある高度化への取組みが構成されなければならない。

②技術のオープン性

情報システムやネットワークシステムには、その構成要素に、どのような技術から構成されているか、あるいは、機能提供の原理そのものが分からない、いわゆるブラックボックス性を持った構成要素が存在している場合がある。特に、重要インフラなどのトラブル発生時に国民生活・経済活動に多大な影響を与える領域で使用される技術や、安全保障に関わる技術では深刻な問題である。

このためには、技術の特性によりオープン性を確保できないものを除き、知的財産権等に関する問題を整理しつつ、技術のオープン性を様々なレベルで確保し、ブラックボックス性を排除する努力が必要である。具体的には、オープンな実装(オープンソース化¹⁸)によって安全性を検証できる技術を積極的に活用したり、開発する技術をオープンソースによって提供したりするという取組みも考えられる。また、実装はオープンではなくても、仕様をオープンとし検証することが可能とするコモンクライテリア(ISO/IEC15408)に基づく情報セキュリティ評価・認証制度¹⁹を活用することも考えられる。さらには、知的財産権に配慮しつつ代替技術を自主開発することや、構成要素の検査技術を高度化することによりブラックボックス性を持った構成要素の安全性検証の確度を高めることも投資対象として検討することが必要である。

18 ソフトウェアの設計図にあたるソースコードを、インターネットなどを通じて無償で公開し、誰でもそのソフトウェアの改良、再配布が行なえるようにすること。

19 情報セキュリティの観点から、情報システムやそれを構成するハードウェア及びソフトウェアが適切に設計され、その設計が正しく実装されているかどうかを評価するためのセキュリティ基準(コモンクライテリア(ISO/IEC15408))に基づき、評価・認証する制度。

③多様性によるセキュリティ確保

単一の実装に対して依存度を高めることは、技術普及を効率的に行うことができるが、同時にリスクを高めることにもなる。この観点から、同一の機能を提供するも、その実装や設計思想が異なるものを複数用意することで安全性を高めるという解決方法、いわゆる多様性によるセキュリティ確保という手法が存在することにも留意する必要がある。

④投資効率の改善

研究開発・技術開発の投資領域の特定、実施段階での効率的な活動展開、さらに、実用化・普及プロセスにおける効率化などの、研究開発・技術開発のプロセスそのものの効率化も実施されなければならない。

前述した多様性によるセキュリティ確保にも配慮しつつ、投資効率の改善にも持続的に取り組むことが必須である。

2) 組織・人間系の管理手法の高度化

開発された情報セキュリティ技術が実環境で効果的、効率的に運用されるため組織・人間系の管理手法の高度化が必要であり、これを情報セキュリティ技術の一分野として取り入れていくことが必要である。

組織・人間系の管理手法の高度化に関する体系的な研究や実環境での取り組みは十分に進められておらず、情報セキュリティ分野における人的及び社会的側面研究への投資は現在ほとんど体系的に行われていない。この状況を早急に改善し、戦略的な投資を実施することが必要である。

なお、ITと社会の関わりに注目し、組織・人間系の管理手法が作用する対象である高度情報通信ネットワーク社会を①経済・文化も含めた社会全般、②組織、③個人の3層構造から構成されると想定し、以下の点に留意しつつ研究投資を促進し、その成果を広く社会展開することが必要である。

①ITと社会との相互影響関係の認知

科学技術社会論(STS²⁰)の研究などで指摘されているように、科学技術と社会(経済・文化を含む)は相互に強い影響関係にあり、情報セキュリティ技術も例外ではない。情報セキュリティが社会におけるさまざまな主体やその活動とどのような影響関係にあるかを把握することが必要である。従って、たとえばシステムダイナミクスのようなシステム方法論や社会ネットワーク分析などの手法の高度化が必要である。また、そうした相互影響関係や予測され

²⁰ Science, Technology and Society

る脅威、脆弱性情報など情報セキュリティ上重要な事項をいかに社会に向けて伝達・告知するかというリスク・コミュニケーションについての研究が必要である。

②情報セキュリティ技術を実装する組織のデザイン

開発された情報セキュリティを実装するのは、その運用現場を持つ組織である。したがって、組織における情報セキュリティを強化していくための方策を考えることは重要である。現在、産業界でISMS認証²¹やITガバナンス²²が注目され始めているが、今後はさらに組織論的及び経営情報論的な視点からの研究が必要である。このような視点の具体的な例として、複雑な技術システムを取り扱いながら不測の事態に強い高信頼性組織の研究が考えられる。

③人間的要因(ヒューマンファクター)への配慮

情報セキュリティを確かなものとするためには、情報システムやネットワークシステムを運用する人間の生理的・心理的要因の把握やマン・マシン・インタフェースの考慮によって、ミスやエラーを防御することが必要である。したがって、これらを研究の対象としている人間工学や認知科学の研究を推進していかなければならない。

1. 4. 情報セキュリティ技術を支える環境整備の必要性

1. 3. (1)で示した、IT基本法に述べる「高度情報通信ネットワークを安心して利用可能」な環境で求められる前述3条件のうち、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」という点を満足するためには、1. 2. で示した1)情報セキュリティ技術の高度化及び2)組織・人間系の管理手法の高度化だけでは実現することは難しく、こうした情報セキュリティ技術を支える環境整備が同時になされることが必要である。具体的には、1)社会システムデザイン研究の実施、2)継続的なリスクアセスメントの実施、3)ベストプラクティスの収集と活用、4)人材育成、5)プライバシーの適切な取扱い、6)IPv6利活用の推進等が必要である。

²¹ 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

ISMS(Information Security Management System) 企業などの組織が情報を適切に管理し、機密を守るための包括的な枠組み。コンピュータシステムのセキュリティ対策だけでなく、情報を扱う際の基本的な方針(セキュリティポリシー)や、それに基づいた具体的な計画、計画の実施・運用、一定期間ごとの方針・計画の見直しまで含めた、トータルなリスクマネジメント体系。

²² 組織体・共同体が、ITを導入・活用するにあたり、目的と戦略や適切に設定し、その効果やリスクを測定・評価して、理想とするIT活用を実現するメカニズムをその組織の中に確立すること。

(1) 社会システムデザイン研究の実施

既存の社会制度を、情報セキュリティ確保の観点から高度情報通信ネットワーク社会に適合させていくことが必要になる。このプロセスは、情報セキュリティ技術の高度化、新たな法律の制定や既存の法律の改正だけでは不十分であることも、過去の取組みで明らかになっている。この典型例が、我が国へのPKI (Public Key Infrastructure)²³ の導入と普及のプロセスである。PKIを構成する基盤技術は1970年代に開発された。その後、1990年代前半までに技術の実用化と運用技術の蓄積が図られた。しかし、PKIを用いた電子的な経済活動を行うためには、経済活動におけるPKI利用の法的根拠を明確化することが求められていた。例えば2000年に制定された電子署名及び認証業務に関する法律は、このような社会的要請にも応えるものであった。しかしながら、そもそも高度情報通信ネットワーク社会におけるPKIの役割を、長期的、国際的な視点から検討することが不十分であったことや、社会基盤の重要な構成要素としてPKIを捉えるまでの踏み込みが足りなかったために、現在でもPKIが広く普及したとは言えない。またPKIを利用しているサービスでも、PKIの一部の機能を実装していることが大半であり、本来PKIが持っている様々な潜在的可能性を社会として活かし切れていないという状況にある。

この問題を解決するために、技術開発と並行して、新たな技術の普及による高度情報通信ネットワーク社会の変化を捉え、必要となる社会制度の整備や、技術の普及戦略を開発する、いわゆる社会システムデザインに対する研究を実施することが必要である。この研究からは、長期的な視点に立った政策提言や、具体的な法整備の必要性の特定と方向性提示、さらには技術の普及において必要となる補完的な技術開発を特定するといった成果が期待される。

また、社会システムデザイン研究の取組み・成果が広く活用され、さらに従来からの「後付け型」の情報セキュリティ確保の取組みを「ビルトイン型」に転換していくためには、社会システムデザイン研究を継続的に組織的に行うことが必要である。さらに、新たな社会制度の創設や既存の社会制度の改善を行う時に、社会システムデザイン研究を通して得られた問題意識を適時適切に提示し、より主体的に参加することが可能になるためのフレームワークを構築する事も必要である。我が国には、社会システムデザイン研究の成果を促すための組織も存在せず、そのフレームワークや方法論も明確になっていない。社会システムデザイン研究の成果を社会展開するためのメカニズムを生み出すことも、社会システムデザイン研究の一環として取り組む必要がある。

²³ 暗号化と復号に異なる鍵を用いる暗号方式である公開鍵暗号技術を利用する環境を実現するために必要な技術をまとめたもの。

(2) 継続的なリスクアセスメントの実施

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では、そもそも社会を「何から」守るのかという明確な認識が不可欠である。どのようなリスクが存在しているかが分かってなければ、合理性を持った情報セキュリティ確保の取組みを構成することは難しい。このために、様々な観点から社会を捉え、リスクアセスメントを継続的に実施することが必要である。

これには、高度情報通信ネットワーク社会を構成する基盤技術に注目して、その脆弱性を発見する研究も必要となる。また、運用環境に注目してシステムだけではなく、いわゆる組織・人間系までを含めたリスク分析も行わなければならない。さらにITが利活用されたことによる社会変化に伴うリスクの変化についても検討が必要となる。

我が国におけるこのような取組みは、様々な主体によって、多種多様な観点から実施されてきた。しかし、その結果を体系的に収集し、解析することが十分に行われてきたとは言い難い状況にある。我が国のリスクアセスメント能力を強化することは、現在解決すべき問題を特定するだけではなく、新たな研究開発・技術開発の必要性を明らかにし、運用環境整備の方向性の明確化に資する。さらには、前項で述べた社会システムデザインにおける要求条件の明確化も果たすことができる。

また、リスクアセスメント能力の強化は、広い意味での情報セキュリティ確保にも貢献する。例えば、重要インフラにおける情報通信機能の防護、すなわちCIIP²⁴の強化が必要と考えられており、政府においてもその取組みを強化している²⁵。この中で重要インフラの相互依存性解析を積極活用することを一つの柱として掲げている。この相互依存性解析は、我が国の重要インフラを対象としたリスクアセスメントそのものである。このような面までを考慮したリスクアセスメントを行うことにより、リスクが顕在化した際の対応プラン、すなわち、事業継続計画²⁶策定に合理性を与えることが可能となる。

(3) ベストプラクティスの収集と活用

ITの特徴の一つとして、技術開発から実用化、普及までの期間が大きく短縮され、新たな技術が次々と登場し、システムやサービスに投入される状況にある。情報セキュリティ技術においても同じ状況にある。このため、技術を活用するため

²⁴ Critical Information Infrastructure Protection

²⁵ 情報セキュリティ政策会議では、重要インフラ専門委員会を2005年9月に設置し、この中で具体的な防護方策検討を行い、2005年末を目途に「重要インフラの情報セキュリティ対策に係る行動計画(仮称)」の策定を進めている。また、中央防災会議の下に置かれた首都直下地震対策専門調査会においても、首都における情報通信機能の災害時対策について、その方策を精力的に検討している。

²⁶ Business Continuity Plan

のノウハウの蓄積が単一の組織、個人では十分に行えないという問題が発生している。この問題を解決するには、様々なノウハウを収集し、その中で有効性の高いもの、いわゆるベストプラクティスを発見することが大きな意味を持つ。そして、ベストプラクティスを、社会知として活用していく取組みも強化する必要がある。

(4) 人材育成

技術立国の我が国が、今後も持続的に発展していくためには、研究者、技術者が安定的に育成され供給されることが必要である。ITあるいは情報セキュリティの領域では、少なくともITを使いこなし、高い使命感を持った技術者が安定供給されることが期待されている。しかし近年、高校生や大学生の「理系離れ」の問題が指摘されており、さらに「IT離れ」も具体的な現象として現れてきている。IT技術を持続的に発展させるためには、長期的には「理系離れ」、「IT離れ」問題を解決する取組みが必須である。また、ITや情報セキュリティ技術に関わる研究者、技術者のサクセスストーリーも生み出し、夢あるキャリアパスであることを示していくことも必要であることは言うまでもない。

我が国で情報セキュリティ技術の研究開発・技術開発に携わる研究者、技術者は、その絶対数が不足している。このため、情報セキュリティ技術の研究開発・技術開発に従事する人材育成を強化することは急務であり、具体的な方策が求められている。

また、広くITの研究開発・技術開発に携わる人達が、情報セキュリティについて理解し、既存成果を具体的に活用する能力を持つことも、今後のITの基盤化とセキュリティ機能の実装を求めていく上では必要となる。このため、現在IT戦略本部等で検討が進められている高度IT人材育成において、情報セキュリティに関わる能力開発を目的とした取組みが含められることも求めていかなければならない。

さらに、各組織においてITを運用するオペレータにおいても、情報セキュリティ技術についての理解と活用方法を体得することが必要となる。この意味で、オペレータ教育においても、情報セキュリティ要素を加味し、同時に資格制度においても情報セキュリティ活用能力を求める取組みにも着手することが必要であろう。

(5) プライバシーの適切な取扱い

ネットワークサービスの不正利用を防ぎ、各利用者の利用環境と権利を守るために、近年、認証機能強化の取組みが広く行われている。認証機能の強化は、各利用者にとってプライバシーを保ったサービス利用環境を構築することに大きく貢献する。一方、合理的な匿名性 (anonymity) を保証する基盤を成立させることもプライバシー保護を強化することにつながる。この認証強化と合理的な匿名

性機能提供をバランス良く行うことにより、真にプライバシー保全に貢献することができ、ひいては健全な高度情報通信ネットワーク社会の発展に寄与することが可能になる。このような視点からの、認証機能強化、匿名性保証基盤確立についても取組みが不可欠である。

(6) IPv6利活用の推進

現在の高度情報通信ネットワーク社会の中核機能の一つであるインターネットは、1980年代に基礎的な技術が開発され、ネットワーク構築と運用を通じて多くの改良が施されてきた。しかし1990年代中盤になり、インターネットの急速な拡大、ネットワーク利用形態の変化、セキュリティに対する要件変化などを受けて、従来の改良による対応ではなく、それまでに判明していた技術要件を満足する新しい基盤を構成することになった。この結果誕生したのがIPv6である。

その後の積極的な取組みによって、日本が中心となりIPv6の基礎を固め、2000年代に入り実際の運用が広がりはじめている。IPv6は個々のノードにインターネット全体で一意的アドレス(グローバルアドレス)を付与でき、またグローバルアドレスの利用に対して制限がほぼ存在しないことから、インターネットの通信モデルであるエンド間通信に忠実なサービス構成が可能であり、現在のインターネットでの構造的限界を克服することができる。

また、耐故障性の向上、エンドノードの良好な追跡性の確保、移動ノードに対する対応といったネットワーク管理、セキュリティ管理の観点からも利点が多く、運用コストの削減も可能とする。さらに、近年開発されているネットワーク技術、さらには今後開発が進められる次世代ネットワーク技術もIPv6を基盤とするようになっており、研究開発・技術開発成果の積極的活用の観点からもIPv6の利活用を推進することが重要である。

(参考) 安心・安全領域の中での情報セキュリティの特殊性

現在、総合科学技術会議において行われている、「安心・安全な社会の形成」に資する科学技術政策検討では、発生しうる脅威を特定し、脅威が顕在化することによって発生が予想される被害を低減させるための技術(被害発生予防)と、脅威の顕在時の対応体制の整備と稼働(初動対応)に資する技術を中心に据えている。広く安全・安心を考えた場合、予防と初動対応はリスク管理と危機管理の基本であり、当然ながら情報セキュリティの問題を考える場合に、その強化方策を考えることは看過してはならない。

しかし、情報セキュリティ技術을考えた場合、防災等の通常の安心・安全領域に含まれる技術とは、異なる特性を持つことに留意することが必須である。

情報セキュリティ技術は社会基盤化している IT を適用対象としている。情報セキ

セキュリティ技術の高度化は、IT そのものの改善・改良を果たすことになる。さらには、新たなアーキテクチャを持った革新的な技術の適用により、社会基盤化しているITそのものに対する脅威を減らすことや、脅威の顕在化のシナリオ、発生しうる被害を変えることが可能である。つまり、自然災害などとは異なり、リスクそのものが技術によって変化することを勘案した戦略策定が必要である。特に、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は、投資戦略を検討する上で強く意識する必要がある。この点が、人工的に産み出された技術集積体としての社会基盤である IT を対象とする情報セキュリティ技術の特殊性といえることができ、この特殊性を考慮した戦略策定が必須である。

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

本章では、前章で述べた基本的考え方を実現する方策の大前提として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構造のあり方、すなわち、前章の基本的考え方のうち、情報セキュリティ技術の高度化のために必要な投資効率の改善(1. 3. (2) 1)④))を実現する方策を具体的に提示する。

2. 1. 投資領域設定の継続的見直し構造の実現

情報セキュリティ技術の高度化のために必要な投資効率の改善を実現するためには、具体的な研究開発・技術開発のどの領域について推進するかを判断する場合に、現在の研究開発領域の意味、技術構成要素の特性、研究期間の考え方が、投資主体と研究開発・技術開発の実施主体によって大きく変化することを踏まえた投資を推進する必要がある。

しかしながら、公的研究資金提供母体においても、民間企業における技術開発投資においても、この構造に対する理解不足があり、結果として、投資のアンバランスを産み出している。このアンバランスを是正しつつ、状況に適応した継続的な見直しが可能となる仕組みが必要である。

<具体的な方策>

具体的には、以下の方策を講じることが適当である。

① 実施状況の把握

総合科学技術会議の協力を得て、情報セキュリティ政策会議は、産官学を通じた我が国における情報セキュリティに関連する研究開発・技術開発の実施状況の把握を実施する。

② 資源配分方針の評価・見直し

総合科学技術会議に対して、情報セキュリティ政策会議は、情報セキュリティ領域に対する資源配分方針について継続的に評価・見直しの提言を行う枠組みを構築する。

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

情報セキュリティ技術の高度化のために必要な投資効率の改善を実現するためには、成果利用までを見据えた研究開発・技術開発の実施体制を構築することが必要である。そのためには、以下の3点からなる新たな体制を構築することが適当で

ある。

(1) 循環モデルの構築

まず、技術利用の現場からのニーズの掘り起こしと研究開発現場へのフィードバック、研究領域の調整という循環モデルを構築することが必要である。その際に、政府は、情報セキュリティ技術への政府自身のニーズが大きいという特性に鑑み、その成果を政府自身が積極利用するよう検討していくこと、客観的に評価された技術を活用するという視点を盛り込むことが必要である。なお、「客観的に評価された技術の活用」に当たっては、1) 情報セキュリティの技術領域は、技術の安全性についての客観的測定が困難な領域であり、技術を評価する能力が我が国において不足している、2) 情報セキュリティ技術を「評価する技術」の開発が、一般的に研究開発・技術開発として認知されていないのが現状であり、「評価技術」の開発及び利用が未発達であるとの問題があることに鑑み、情報セキュリティ技術に係る最先端の評価技術の開発を推進する必要がある。

(2) 継続的評価プロセスの構築

そもそも、成果利用の可能性を評価する枠組みも必要である。その際、成果の国際展開を視野に入れた評価、特に標準化、リファレンスモデル化などの取組みによる国際性を持った成果利用を積極的に推進することが不可欠である。また、評価に当たっては、情報セキュリティの技術領域は、技術の安全性についての客観的測定が困難な領域であるにもかかわらず、技術を評価する能力を有する者が不足し、技術を評価するための技術が未発達であることに留意し、当面は評価結果を絶対視しない必要があるとともに、保全上の観点から部外評価(実施状況の把握を含む。)を行うことが適当でない研究開発・技術開発については、部内評価等により、投資効果の評価を実施することも必要である。

(3) 産官学の共同プロジェクトの実施

さらに、情報セキュリティ技術の研究開発・技術開発、そしてその成果の活用を行う、産官学の関係者が適切な役割分担の下で、共同してプロジェクトを行うことにより、成果の社会展開の加速化を実現することが必要である。なお、産官学それぞれには、一般的には以下のような役割分担が存在するものと考えられこの特性を反映したプロジェクトが実施されることが適当である。

1) 産業界の主な役割

ビジネスに直結する技術開発、研究開発に積極的に投資するとともに国家プロジェクト等によって創出された技術を利活用することにより、技術の広範な普及及びコスト削減に努める。

2) 政府の主な役割

「公共上の見地から国として実施すべき領域に関する投資(基盤技術、ハイリスク研究開発、安全保障等)」を政策立案し、必要な資源を確保する。また、国内企業の振興、育成に寄与するとの視点も視野に入れる。

3) 独立行政法人(旧国立研究所等)の主な役割

独立行政法人通則法等に基づき、独立行政法人として実施すべきプロジェクトに関して、その実施方針、内容、体制等を詳細にプランニングすると共にプロジェクトを指揮する。また、大学や企業と同じように研究開発を行うのではなく、研究プロジェクトの運営、新たなテーマ設定のための領域動向調査、政府の政策決定プロセスへの積極的な関与など、政府の行政活動へのコミットメントを増大させていく方向で活動を展開する。

4) 大学の主な役割

産業界及び政府主導によるプロジェクトに積極的に人材及び蓄積された技術を投入し、プロジェクトの高度化を図る。また、情報セキュリティ分野に限定されない領域との学際的な接点を提供する。さらに、人材育成を通じた1)研究者の育成、2)萌芽的領域における知見の体系化といった、研究実施機関であり、同時に教育機関でもある特性を活かした活動も展開する。

<具体的な方策>

具体的には、以下の方策を講じることが適当である。

① 循環モデルの構築－政府調達における成果利用と新たな研究開発・技術開発の主導－

情報セキュリティ研究開発・技術開発における成果を、調達を通し、最大限、直接政府が活用するためのガイドラインを策定する。また、政府において活用することを前提とし、情報セキュリティ政策会議と内閣官房が主導した、新たな研究開発・技術開発を推進する。

② 継続的評価プロセスの導入

総合科学技術会議の協力を得て、情報セキュリティ政策会議が、情報セキュリティ技術に関する研究開発・技術開発全般について、1)事前評価、2)中間評価、3)事後評価の各段階における投資効果の評価を実施する。

③ 産官学の共同プロジェクトの実施

総合科学技術会議の協力を得て、情報セキュリティ政策会議が、産官学共同による研究プロジェクトを主導する。

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

本章では、第1章で述べた基本的考え方を実現する方策として、前章で示した新しい推進構造を前提とした具体的な研究開発・技術開発の方向性を提示する。すなわち、第1章で述べた、1) 情報セキュリティ技術の高度化(1. 3. (2) 1))及び組織・人間系の管理手法の高度化(1. 3. (2) 2))を実現するための公的研究資金投入の具体的な方向性、そして、2) 情報セキュリティ技術を支える環境整備のための具体的な方策を提示する。

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

情報セキュリティ技術の高度化(1. 3. (2)①)及び組織・人間系の管理手法の高度化(1. 3. (2)②)を実現するための具体的な方策を実現するためには、1) 基盤としてのITを強化することに直結する中長期目標に対する投資の重点化と、2) 萌芽的研究への投資の強化が必要である。

(1) IT強化直結型研究への重点化

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には、基盤としてのITを強化することに直結する中長期目標に対して、公的研究資金を重点的に投入して研究開発・技術開発を促進することが望ましい。公的研究資金の重点的な投入によって、多くの成果創出が期待される領域を例示すると以下のとおりである。

○脆弱性を無くす高信頼ソフトウェア開発環境構築のための研究開発

情報システムの安全性を確保するためには、アプリケーションプログラム²⁷における脆弱性を無くすためのプログラミング環境が必要である。また、アプリケーションを実行した場合の脆弱性を排除するためには、コンピュータシステムの中核となるOSの信頼性を高め、同時にセキュリティ機能強化が必要である。これらを統合した、高信頼ソフトウェア開発環境を構築し、広くソフトウェア開発で利用するように社会展開することで、広く情報セキュリティ確保を達成することが期待できる。

○次世代ネットワーク基盤に関する研究

高度情報通信ネットワーク社会の中核機能の一つであるインターネットは、

²⁷ 応用ソフトウェア。ワープロソフトや表計算ソフトなど、必要に応じて作られたソフト。

IPv6 の開発と展開によって、パケット通信網として従来のインターネットが持っていた課題の多くを解決した。しかし、現在のインターネットは、多種多様な実アプリケーションによって使われており、実時間性能制御、優先通信機能、複数のセキュリティ機能実装、エンドノード追跡、性能保証、通信経路の信頼性確保等といった、新たに多くの技術的要件が提示されてきている。このような技術的要件を満足し、さまざまな実アプリケーションに対応することが可能な、いわゆる次世代ネットワーク基盤に関する研究を強化することが必要である。

○先進的な大規模分散処理環境におけるセキュリティ技術の確立

2000年頃から研究開発が進められているグリッド²⁸技術は、広域ネットワーク上の計算、データ、実験装置、センサー、人間などの資源を仮想化・統合し、必要に応じて仮想計算機（Virtual Computer）や仮想組織（Virtual Organization）を動的に形成するためのインフラを形成しつつあり、次世代情報処理環境として、その社会展開が大きく期待されている。これまで学術研究ネットワークに実装されていた先進的な大規模分散処理環境も実用段階を迎え、さらにグリッド技術をビジネス環境に適用しようとする動きが活発化してきている中、大規模分散処理環境でのセキュリティ機能の実装が必須であると考えられはじめている。このような環境を実用に供し、さらに産業界における利用を可能にするためにも、大規模分散処理環境におけるセキュリティ技術を確立し、セキュリティの確保された安全な情報サービスを享受できるようにすることが必要である。

○安全なシステムアーキテクチャに係る研究

ビルトイン型の技術を導入したシステムアーキテクチャや、フェイルセーフ²⁹の概念によるセキュリティ技術の研究開発は、対症療法的な対策を超えた、問題を根治するための技術として推進すべきものの一つである。

○電子認証技術の強化

PKIをはじめとした本人認証、機器認証³⁰、バイオメトリクス認証、時刻認証、構成管理など、様々な認証手法を統合的に研究し、全体として安全性の高い認証基盤を構築していくことが重要である。

この研究分野は、「認証」行為が想定される様々な領域における研究が必要

28 電気を伝える高圧送電線網（パワーグリッド）に由来。情報コンセントに接続するだけで、ネットワークを通して、安全に・安定して・安易に様々な情報サービスを楽しむことができるようになるための次世代インフラ。

29 障害が発生してもシステムが安全な方向に動作するようにするための仕組みや考え方。

30 利用機器固有の値を用いて、その機器が「なりすまし等」のない正しい機器であるかどうかを確認すること。

であるとともに、当該技術を短期間に社会に普及させるための方策としては、その技術が実装される環境として提供し、他の技術も併せて提供される必要がある。

○IT に起因するリスクアセスメントに係る研究

組織の情報セキュリティに係るリスクを分析し、例えば、被害額の算定モデルを適用するなどして定量的に評価することにより、どの程度の情報セキュリティ対策を行うことが投資対効果の観点から正当化され得るのかを明らかにする研究は重要である。この研究においては、研究領域の相互関連構造への理解を踏まえ、観点から、情報セキュリティ対策技術、数学、社会科学、組織論も対象としてこれらの領域における共同研究や知見の共有化を行うことが考えられる。

○高信頼性組織デザインについての研究

情報システム、の高い信頼性・安全性を確保するために、それらを運用する組織のあり方についての研究を推進することが重要である。複雑・高度な技術を取り扱い、不測の事態が起こりうることを前提としながら高い信頼性・安全性を維持する高信頼性組織のデザインの研究は、情報システムが持つ技術的側面と人間的側面の相互理解を深め、組織的に情報セキュリティを確保していくために重要である。

○重要な情報を守るための情報管理技術の確立

現在においては、情報の動的なコントロールが困難であり、いったん漏洩した場合に情報の拡散を自らの意思で食い止めることが難しい。このため、技術による情報管理と運用(人による情報管理)を連携させ、運用のミスを最小限にする技術や、問題が発生した際にも適切に情報を管理し、重要な情報を守る技術を適用していく情報管理技術の確立が重要である。

例えば、セキュアアセットコントロール技術³¹については、これに、運用と技術の連携の観点や、組織・人間系の管理手法の高度化の概念との関係からも重要である。

○情報セキュリティ評価技術の研究

そもそも情報セキュリティ技術を導入したときの効果は可視化しにくく、また安全性を測定することが極めて困難な分野であるため、情報システムの安全性を評価することそのものが、研究の対象として重要である。例えば、情報システ

³¹ 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、それを確実に達成したり、自分の管理下を離れた情報についても検出・無効化することが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。

ム全体の安全性を客観的に評価するための技術の開発、暗号モジュール³²について、様々な脅威に対応するための客観的な安全性の測定尺度の研究等、ITを適用した領域での、IT要因によるリスク増加についての研究、脅威研究、リスクアセスメント方法論研究等を体系化し、評価技術として確立していくものである。また、評価結果を分かりやすく提示するための処理や、総体比較を可能にするための評価尺度設計についても広く実用化を試み、利用者にとって「安全であることが分かる」環境作りに取り組む。

(2) 萌芽的研究への投資強化

一方、既存技術の改良や運用技術の開発等、短期的な目標設定がされているものについては、官民での取組みの現状を把握し、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に投資ポートフォリオの調整をきめ細かく行うことで、バランスの良い投資を行うことが必要である。例えば、民間での技術開発が活発に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というようなポートフォリオ調整が実施されることが望ましい。

なお、現状で情報セキュリティ技術に対する社会全体での投資は、過小投資状況にあると一般的に考えられており、官民共に情報セキュリティ技術の研究開発・技術開発に対する投資拡大を行うべきであることは言うまでもない。

具体的に、民間の取組みが乏しい萌芽的研究として考えられる例として以下のものが考えられる。

○デジタルフォレンジック³³に係る研究

情報通信技術の発展や利用者の増加に伴い、情報セキュリティに係る事案は増加し、その被害は拡大する傾向にある。事案の取扱いでは、司法機関による刑事的な処理だけではなく、損害賠償等で民事的に解決することも必要となる。これらの処理では、発生した事案に対し、その事実を調査・解明し、証拠としての取扱いを可能とする技術が必要である。また、民事訴訟などを受ける可能性のある企業が正しく行動している証拠を残し、安全・公正に証拠を開示する技術も大切となる。この技術を生み出すのがデジタルフォレンジックである。デジタルフォレンジックに係る研究は、社会的に必要とされているものの、民間での研究投資はほとんど行われておらず、公的研究資金の投入による研究遂行が適切である萌芽的研究として取り扱うことが適切である。

³² 暗号機能を有するソフトウェア、ファームウェア、ハードウェア、もしくはその組合せ。

³³ (Digital Forensics) 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。

○情報の長期間保存技術に関する研究

デジタル化された情報を安全に長期間保存するための技術が必要となっている。これは暗号の特性として、経年に応じて暗号強度が劣化することを考慮し、電子署名などが数十年のオーダーで有効に検証でき、かつ、安全に暗号化されていることを保証するための技術であり、現時点では研究着手されたばかりである。電子政府だけではなく、民間企業における様々なドキュメントが電子化された状態で保存されるようになることを考慮すると、長期間保存技術は必須の技術であり、重点的な投資が必要となる。

○高信頼情報処理アーキテクチャに関する研究

ソフトウェアは常に改竄や偽造の恐れがあり、さらに誤操作による情報漏洩の危険性も存在する。このように、コンピュータ内部から自ずと生ずる脆弱性を克服するために、プラットフォームの安全性や完全性を保証する仕組みの上にコンピュータシステムを構築するという考え方、いわゆる信頼できるプラットフォーム(trusted platform)を構築する技術が不可欠である。現状でも TCG (Trusted Computing Group)による TPM (Trusted Platform Module)などの実現例があるが、鍵の喪失を主とする運用に関する課題、互換性に関する問題、及びプライバシー保護の問題など、広く実用化されるには数多くの課題を解決しなければならない。

(3) 基礎研究領域に対する投資の充実・強化

情報セキュリティに関連する技術の基盤となる基礎研究領域、特に応用数学、離散数学、コンピュータ言語、情報理論、符号理論、シミュレーション技術及びソフトウェア・ハードウェアの安全性検証などに対して積極的な投資を行い、技術基盤の拡充を図る。

また、事前に特定の仮説を用意しない探索的研究を促進することにより、広い視野での知見の醸成や新たな仮説の発見に努めるとともに、情報セキュリティ技術の次期研究シーズの育成を図ることも重要である。

3. 2. 情報セキュリティ技術を支える環境整備

1. 4. で述べたように、情報セキュリティ技術を支える環境整備として、1) 社会システムデザインに関する研究促進、2) 継続的なリスクアセスメントの実施、3) ベストプラクティスの収集と活用への取組み強化、4) 人材育成、5) プライバシーの適切な取扱い、6) IPv6利活用等が必要である。

(1) 社会システムデザインに関する研究促進

社会システムデザインに関する研究は、新たな技術の普及による高度情報通信ネットワーク社会の変化を捉え、必要となる社会制度の整備や、技術の普及戦略を開発することが主目的となる。さらに、このような社会システムデザインが必要とされる領域として何が存在するかも、研究活動の一環として取り扱われなければならない。

情報セキュリティ技術に関連して、社会システムデザインが必要と考えられている領域として、例えば迷惑メール対策やコンテンツ流通におけるコンテンツ保護方策の開発が挙げられる。どちらの領域も技術だけでは解決が難しく、法整備を含む社会制度による対応も必要であり、さらに技術普及の実施戦略も必要となる。

具体的には、内閣官房は、社会システムデザインに関する研究が必要となる領域が何であるかを継続的に検討し、特定された領域について、長期的な視点にたった政策提言、具体的な法整備の必要性の特定と方向性提示、技術普及で必要となる補完的な技術開発の特定を行う。

さらに、情報セキュリティ確保がなされたITを社会でどのように活用していくのかという問題について研究を実施する体制を検討し、その政策や経営、産業界への成果展開方法についても検討を行う。

(2) 継続的なリスクアセスメントの実施

継続的なリスクアセスメントの実施は、情報セキュリティ技術の研究開発・技術開発、社会システムデザイン関連の研究を行う前提となる現状認識を与える重要な活動である。これまでもリスクアセスメントそのものは、官民の様々な主体によって実施されているが、その結果を集積し総合的に解析することが必要となっている。

具体的には、内閣官房で着手している重要インフラの相互依存性解析を広範に実施することや、官民連携しての現在のインターネットで観測される情報セキュリティ攻撃事象の収集と解析に着手する。

(3) ベストプラクティスの収集と活用

いわゆるベストプラクティスは、主に民間セクタにおいて蓄積が進んでいる。このベストプラクティスを政府が選別し、電子政府の開発、運用において積極的に活用する。

具体的には、内閣官房がベストプラクティスの収集に努め、別に定める政府統一的基準に含まれるガイドラインに、個々のベストプラクティスの活用方法を含めることで、各府省庁でのベストプラクティスの活用を促進する。

(4) 人材育成

第1章で示したように、人材育成では、①情報セキュリティ技術の研究開発・技術開発に従事する人材育成の強化、②広くITの研究開発・技術開発に携わる人達を対象に情報セキュリティについて理解し、既存成果を具体的に活用する能力を持たせること、③ITを運用するオペレータが、情報セキュリティの理解と活用法を体得することを目標とする。

具体的には、①、②については、大学、大学院などの高度IT人材育成機関による教育カリキュラムの開発と実施、③については官民が実施しているIT人材資格制度において情報セキュリティ活用能力を求めるよう制度を変更することを、内閣官房が関係省庁や関係諸団体に対して働きかける。

(5) プライバシーの適切な取扱い

プライバシーの保護については、例えば電子投票における匿名性確保といったように、これまでも様々な取組みが行われてきた。第1章で示したように、今後、プライバシー保護の強化に向けては、①認証機能の評価、②合理的な匿名性保証基盤の確立に向けた取組みが不可欠である。このため、これらの研究状況を把握するとともに、必要となる技術的要素を特定する。

(6) IPv6の利活用推進

第1章で示したように、IPv6は今後のインターネットを利用した新しい技術の基盤となる。インターネットに関わる研究開発・技術開発の成果の利活用の観点からもIPv6環境を構築することが肝要である。この観点から、政府は2010年度末までに、各府省庁のネットワーク基盤である霞が関WAN、各府省庁内ネットワーク及び電子政府システムをIPv6に対応させる。同時に、民間におけるIPv6利活用をより一層推進し、我が国の世界最高のブロードバンド基盤を、技術レベルの面からも最先端とする取組みを強力に推し進める。

4. 「グランドチャレンジ型」研究開発・技術開発の推進

本章では、第1章で述べた基本的考え方を実現する方策として、前章に示した取組みに加えて、より長期的な視野で、根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・技術開発を情報セキュリティ領域において実施することが効果的であることを提示する。

4. 1. 「グランドチャレンジ型」研究開発・技術開発とは

最近の科学技術研究の問題として、研究領域の細分化、先鋭化が進み、研究実施の目標設定が短期的なものが中心になったり、他の研究領域との関連性を意識しない研究実施が行われたり、さらに最悪の場合には研究者が研究実施の目的を見失ったりすることが発生している。このような問題を解決する一つの方策として、10年程度の長期間にわたる持続的な研究開発を念頭に置き、特定の大目標を設定し、各種要素技術全体の統合的開発を行う、「グランドチャレンジ型」の研究開発を設定することが注目されている。

グランドチャレンジ型の研究開発を設定するプロセスでは、まず大目標として何を設定するかが大きな課題となる。この検討プロセスでは、分かりやすく象徴的なターゲットを選定する段階で、長期的な研究を行う意味と、先鋭化した個別研究領域の関連性の再認識、さらには、研究と社会の関係を明確化されることが期待できる。また、目標設定の検討プロセスを継続的に実施することにより、情報セキュリティ技術領域の問題点や新たな研究の方向性等が、より明確になることも期待できる。

さらに、実際にグランドチャレンジ型の研究開発を実施することで、目標が実現されるだけでなく、目標実現の過程で生み出される数多くの副産物が社会展開される効能を期待することができる。さらに、極度に細分化された研究領域を融合し、新たな意味づけを行うことも期待される。

また現在、ITは、我が国の国民生活・経済活動のあらゆる場面において深く利用されるようになったが、IT社会を支える情報セキュリティ技術そのものは、必ずしも国民生活・経済活動にとって身近な技術とはなっていない。そこでこうしたグランドチャレンジ型の研究開発を推進することにより、国民の関心を高め、ひいては情報セキュリティ技術への投資に対して、幅広い支持を得られることが期待できる。

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

より長期的な視野で、根本的な技術革新等の実現を目指すため、今後、総合科学技術会議の協力を得て、情報セキュリティ政策会議が、「グランドチャレンジ型」の研究開発・技術開発を情報セキュリティ領域において推進することが効果的である。

具体的には、まず、継続的にグランドチャレンジに相応しいテーマを検討するための場を、情報セキュリティ政策会議の傘下に設置し、総合科学技術会議の協力を得て、「グランドチャレンジ型」のテーマを設定する取組みを開始することが必要である。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、プログラママネージャー制等、大目標の下での多岐にわたる各種要素技術の統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も検討することが必要である。

なお、「グランドチャレンジ型」領域としては、現時点において、例えば次のようなテーマが考えられる。

- コンピュータウィルスなどの悪意を持ったプログラムによる脅威を根絶できるような情報処理環境の構築。
- 情報システムを運用する回避不可能な人為的ミス等から発生するトラブルやエラーを根絶する、「情報セキュリティ・ユニバーサルデザイン」の確立。
- 情報サービス、ネットワークサービスにおいて、利用者側が情報セキュリティサービスの品質グレードを指定し、利用できる環境の構築。例えば、電気通信事業者やプロバイダーが指定するのではなく、利用者がグレードをコントロールし、かつユーザブルに利用可能な「迷惑電話・迷惑メール防止サービス」の提供など。
- 認証等の基礎となるトラストポイント³⁴の国際化とネットワーク化。例えば日本が先導してトラストポイントに求められる要件と検証を行い、各国が持つトラストポイントについて相互互換性を保証する「グローバルトラストネットワーク」を形成する取組み。
- 通信障害等を自律的に検知し、回復することのできる高信頼性のあるインターネット環境の構築。

³⁴ (Trust point)電子商取引などでユーザはCA (Certificate Authority) (電子的な身分証明書を発行する機関)が発行する証明書をアプリケーションで利用する。その際、ユーザはルートCA、もしくはいずれかのCAを信頼し、そのCAが発行する証明書は正しいという前提に立って証明書を検証する。ユーザが信頼するCAはそのユーザにとっての「トラストポイント」と呼ばれる。

(参考) 技術戦略専門委員会報告書までの検討の経緯

【情報セキュリティ政策会議】

2005年 7月14日 第1回会合

セキュリティ分解専門委員会及び技術戦略専門委員会の設置について

2005年 9月15日 第2回会合

「第1次情報セキュリティ基本計画（仮称）」の骨子と方向性について

【情報セキュリティ政策会議技術戦略専門委員会】

2005年 8月22日 第1回会合

- (1) 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設置について
- (2) 会議の公開等について
- (3) 情報セキュリティ政策会議の概要について
- (4) 我が国における情報セキュリティに係る技術戦略の推進についての問題意識について
- (5) 政府による情報セキュリティ関連研究開発・技術開発の現状について
- (6) 技術戦略に関する問題点の抽出と論点の整理についての検討

2005年 9月21日 第2回会合

情報セキュリティ技術戦略の骨子と方向性についての検討

2005年10月12日 第3回会合

技術戦略専門委員会報告書骨子（案）についての検討

2005年11月 4日 第4回会合

技術戦略専門委員会報告書(案)についての検討