参考資料1－4－1

情報通信分野推進戦略（セキュリティ及びソフトウェアWG）報告書（案）
安心して利用可能な環境実現のための情報セキュリティ技術の高度化を軸として

2006年3月2日
セキュリティ及びソフトウェアWG
（セキュリティ技術）

I. 状況認識

情報セキュリティ技術領域の戦略設計の前提として、わが国のさまざまな活動のITへの依存度を考えた場合、2001年当時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。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 の発生、フィッシング 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、総合科学技術会議では、第3期基本計画の「科学技術基本政策策定の基本方針」の【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」という政策目標として捉えられており、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。

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」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。また、情報セキュリティに係わる実用技術が海外ベンダーに依存する状況になれば、それが「安全が誇りとなる国」のアキレス腱となることを十分憂慮すべきである。

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。

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。

特に、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、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。

II. 重要な研究開発課題

前節に述べた状況認識より、広範な研究開発投資が必要であり、その中でも特に以

下の研究開発課題が重要である。

A. 情報セキュリティ技術の高度化

- 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
  - ○ 例えば、脆弱性を作り込んでしまわないための言語及びその処理系の開発、プログラム開発環境などの統合的な開発、ISO15408 などの高信頼システム開発手法の積極活用を達成するための技術
- ユービキタス環境やＧＲＩＤ環境といった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
  - ○ 例えば、資源や処理ノードが大規模分散している環境での安全なデータアクセスとデータ処理の基盤環境作り
- 安全なシステムアーキテクチャとＯＳに係る研究
  - ○ 例えば仮想実行環境を実現する仮想マシン（アダプティブ・セキュア・マシン）技術を使ったセキュリティ管理環境の構築。
- 次世代 Trusted Computing 情報基盤技術及び高信頼情報処理アーキテクチャの研究
- 情報の長期間保存技術に関する研究
- 攻撃遮断技術に関する研究
- 脅威分析、脆弱性情報共有技術に関する研究
- 情報セキュリティ評価技術に関する研究

B. 技術を補完しより強固な基盤を作るための管理手法の研究

- IT に起因するリスクアセスメントに係る研究
- 高信頼性組織デザインについての研究
- 重要な情報を守るための情報管理技術の確立

III. 研究開発の目標

国民生活・社会経済活動の基盤機能を提供する、いわゆる重要インフラにおけるITの利用・活用は、情報通信を基盤とした相互の依存関係の増大などにより拡大が顕著である。IT依存度が急激に高まるなか、各重要インフラでは、サイバー攻撃、シス

テム障害、人為的ミス及び災害等あらゆる脅威から情報通信機能を利用した活動の安全性ならびに安定的供給を確保することが最優先の課題となっている。そのため、各重要インフラにおけるIT障害を限りなくゼロに近づけるため、情報セキュリティ技術を構成している多種多様な基礎技術、関連技術の高度化を含めた研究開発強化は必須となっている。

また、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、利用者が安全であると認識し、安心して各種情報の伝達や、その加工及び共有等を行える社会を実現するためには、世界最高水準の情報通信インフラを構築する必要がある。さらに、重要インフラを含む、超大規模グローバル社会システムの設計・運用管理を可能にする次世代ネットワーク環境を視野に入れた環境を実現するために必要となる各種基盤技術及び、それらの統合化技術に関する研究開発を実施する必要がある。

さらに、モバイル、電子タグ等我が国が国際的に優位に立っている技術を核としたITの利用・活用が進展し普遍化した環境を前提とすると、新たに重要インフラとして機能することが求められているＰＫＩをはじめとした本人認証、機器認証、バイオメトリクス認証等に代表される認証基盤などを国民生活・社会経済活動へスムーズに組み込むための実施戦略の設計として、新たな技術の普及によるIT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研究の強化も併せて実施するべきである。

このため、上記の観点を踏まえつつ平成１８年２月２日に「情報セキュリティ政策会議」（議長：内閣官房長官）により決定した、我が国の情報セキュリティ問題全般についての中長期計画である「第１次情報セキュリティ基本計画」を達成するために必要となる研究開発を実施する。

Ⅳ．戦略重点科学技術と研究開発の推進方策

推進方策では以下の点に留意し、研究実施を行うことが重要。

○　社会システム研究の実施

- 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。

○ 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。

○ 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。

○ 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。

V. 戦略重点科学技術

戦略重点科学技術を選定するにあたり、5年から10年後に、以下に示す大きな問題を解決する（いわゆるグランドチャレンジ）ことを目標とし、それに資する技術を選定すべきである。

- より高信頼・高可用性を提供するシステムの一般化
  （アウトカム例）
  - ○ 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。

○ 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

➢ 利用者に安全・安心を実感させることができる環境の実現

（アウトカム例）

○ 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。

○ 自分自身が利用するサービスの安全性を可視化できる環境構築。