参 考 資 料 2

技術戦略専門委員会報告書 2006

－　研究開発･技術開発の戦略的推進－

2007年6月29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 ..... **- 4 -**

1. 技術戦略専門委員会報告書(2005年版)策定後の動向 ..... **- 5 -**

1. 1 報告書2005の策定とその後の動き ..... - 5 -
1. 2 総合科学技術会議における動向 ..... - 7 -

2. 情報セキュリティ技術の現状認識と今後の方向性 ..... **- 13 -**

2. 1 情報セキュリティ技術戦略の基本 ..... - 13 -
2. 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 ..... - 15 -
2. 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 ..... - 19 -

3. 2007年における実施のポイント ..... **- 21 -**

3. 1 投資領域設定の継続的見直し構造の実現 ..... - 21 -
3. 2 調達を通して成果を活用するガイドライン策定の検討 ..... - 33 -
3. 3 「グランドチャレンジ型」テーマ検討の場の設置 ..... - 34 -

(参考)技術戦略専門委員会報告書2006までの検討の経緯 ..... **- 39 -**

はじめに

我が国の社会経済活動、国民生活の多くが情報通信基盤に大きく依存すると同時に、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発生など、高度情報通信ネットワーク社会における問題も顕著となっている。

これらの問題解決には、社会全体で効果的な情報セキュリティ対策の実施を促進するだけではなく、情報セキュリティを支える技術や管理手法の持続的な高度化が必要であることは言うまでもない。

しかし、我が国における情報セキュリティに資する研究開発・技術開発をどのように構成し実施していくかについての戦略が2005年当時まで不在であり、その立案が急務であった。2005年7月に情報セキュリティ政策会議の下に編成された技術戦略専門委員会では、我が国の情報セキュリティ技術研究開発の方向性について集中的に審議し、2005年11月に報告書をとりまとめ、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た。

2006年3月に閣議決定された「第3期科学技術基本計画」における情報通信分野に係る分野別推進戦略では、情報セキュリティについて重要な研究開発分野として位置づけ、その推進方策では、2005年に技術戦略専門委員会報告書で提示した様々な方策が取り入れられることとなった。また、内閣官房情報セキュリティセンターや各府省庁においても、情報セキュリティの高度化に資する研究開発の取組みが開始され、それらの取組みが着実に実を結んでいくことを切に願うところである。

しかし、我が国における情報セキュリティに関する技術戦略施策をより効果的に実施するためには、2005年11月に策定した技術戦略専門委員会報告書の内容を最新の動向に合わせたものにするとともに、より具体的な内容の検討を行うなどのフォローアップ作業が必要である。特に、2005年度の議論で問題提起をしたものの、具体的な方向性を提示できなかったものについては、追加的な議論を行い、戦略への組み込みを試みる必要があるのは言うまでもない。以上の観点から、2005年度に技術戦略専門委員会報告書を策定した委員自らがフォローアップ作業を行うことを目標として2006年10月から2007年6月までの間に計4回の委員会を開催し、議論を進めてきたものである。この議論の中では、我が国における情報セキュリティに関連する研究開発・技術開発を俯瞰し、重点化分野の見直し等について多面的な検討が行われ、これらを本報告書としてとりまとめた。

本報告書は、1）技術戦略専門委員会報告書（2005年版）策定後の動向、2）情報セキュリティ技術の現状認識と今後の方向性、3）2007年における実施のポイント、の3部編で構成されている。この中に盛り込まれた重点化分野などの新たな技術戦略については、情報セキュリティ政策会議より総合科学技術会議等に対して提言を行うこと

とされており、これにより情報セキュリティに関連する研究開発・技術開発に対する効率的・効果的な投資の実現、ひいては情報セキュリティ技術の高度化並びにその迅速な社会展開の実現が図られることを期待するものである。

2007年6月29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

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巨大災害研究センター長
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）

注記：篠田陽一委員は、２００７年3月１２日まで在任。

１．技術戦略専門委員会報告書（２００５年版）策定後の動向

我が国における情報セキュリティ政策は、2005年4月に内閣官房に情報セキュリティセンターが、さらに同年5月には内閣官房長官を議長とする「情報セキュリティ政策会議」がIT戦略本部の下に設置され[1]、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の活動を開始し、政府横断的かつ本格的な政策推進体制が整った。

技術戦略専門委員会（以下「本専門委員会」という）は、前述した「情報セキュリティ政策会議」の下に設置され、2005年11月に「技術戦略専門委員会報告書」（以下「報告書2005」という）[2]をとりまとめた。なお、本専門委員会の事務局は内閣官房情報セキュリティセンターに置かれている（以下「委員会事務局」という）。

この報告書2005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た。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たものであった。

本章では、2005年11月に本専門委員会が報告書2005をとりまとめた後の動向をまとめる。これにより、報告書2005によって提言された技術戦略が、現在政府によって遂行されている各種政策にどのように展開されたかを示す。

１．１　報告書2005の策定とその後の動き

⑴　第一次情報セキュリティ基本計画とセキュア・ジャパン2006

2005年11月に報告書2005がとりまとめられたのち、2006年2月に「情報セキュリティ政策会議」（議長；内閣官房長官）の第4回会合が開催され、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」（以下「基本計画」という）[3]について政策会議決定がなされた。これにより基本計画は、政府としての初の情報セキュリティに関わる政策パッケージとなった。

本基本計画は、情報セキュリティを巡る問題が多発し複雑化している中、従来からの個別縦割り的対応、対症療法的対応に問題があり、我が国全体としての戦略的な取組みが必要であるとの指摘を受けてとりまとめられたものであり、1)我が

---

[1] 情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて
http://www.kantei.go.jp/jp/singi/it2/kettei/041207minaosi.pdf

[2] 報告書2005概要（別添1）、報告書2005本文
http://www.nisc.go.jp/conference/seisaku/strategy/common/pdf/tech_rep.pdf

[3] 第1次情報セキュリティ基本計画
http://www.nisc.go.jp/active/kihon/pdf/bpc01_ts.pdf

国が情報セキュリティ問題に取り組む上での基本理念の提示、2)今後3年間に取り組む重点政策の方向性の提示、3)政策の推進体制の提示などが盛り込まれている。

基本計画においては、情報セキュリティ対策の強化が求められる政府機関、重要インフラ、企業、個人という対策実施4領域に加え、これら全分野に跨る課題として、技術戦略の推進、人材の育成・確保、国際連携・協調の推進、犯罪の取締り等、という前述した4領域の横断的な情報セキュリティ基盤の形成が求められている。また、本専門委員会がとりまとめた報告書2005の内容は、基本計画に反映されている。

また、2006年6月には、基本計画の2006年度の実施プログラムである「セキュア・ジャパン2006」が決定された。この「セキュア・ジャパン2006」には、1)基本計画を着実に実行に移すとともに、昨今新たに起こった問題に確実に対応し、情報管理のあり方も含めた総合的な対応策を盛り込んだ「2006年度の実行計画」、2)2006年度の具体的施策を受け継ぎ、基本計画の最終年度である2008年度に向けての確かな道筋を確立するために2007年度に推進する施策の方向性を示した「2007年度の方向性」から構成されており、本専門委員会の報告書2005に掲げられた数多くの施策はこの「セキュア・ジャパン2006」[4]に組み込まれている。

さらに、報告書2005に基づいた施策は内閣官房においても具体的に進められており、人材育成・資格制度体系化専門委員会[5]の開催や、産学官の共同プロジェクトの実施という形であらわれている。

第1次情報セキュリティ基本計画決定から、本専門委員会の活動再開(2006年10月)までの動きを図1にまとめた。

---

[4] セキュア・ジャパン2006
http://www.nisc.go.jp/active/kihon/ pdf/sjf_2006.pdf_

[5] 人材育成・資格制度体系化専門委員会報告書
http://www.nisc.go.jp/conference/seisaku/training/common/pdf/training_report_final.pdf

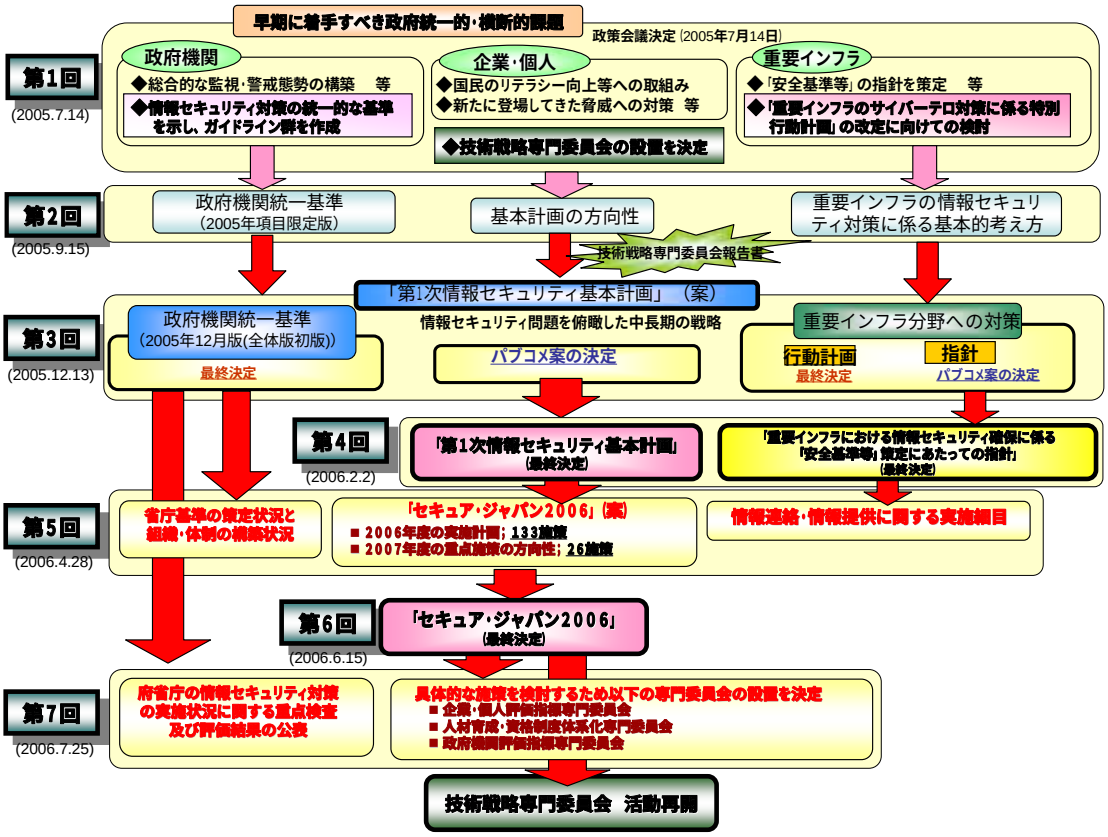


図1　第一次情報セキュリティ基本計画決定等の動き

1．2　総合科学技術会議における動向

本専門委員会がまとめた報告書2005での提言は、主に総合科学技術会議における第3期科学技術基本計画での分野別推進戦略における展開がなされた。ここでは、総合科学技術会議と、第3期科学技術基本計画における「情報通信」分野別戦略について概説する。

(1)　総合科学技術会議の位置付け

総合科学技術会議は内閣総理大臣及び内閣を補佐する「知恵の場」として我が国全体の科学技術を俯瞰し、各省より一段高い立場から、総合的・基本的な科学技術政策の企画立案及び総合調整を行うことを目的とし、2001年1月、内閣府設置法（1999年法律第89号）に基づき、「重要政策に関する会議」の一つとして内閣府に設置された。

総合科学技術会議の任務は以下のとおり。

① 内閣総理大臣等の諮問に応じ、次の事項について調査審議する。

ア．科学技術の総合的かつ計画的な振興を図るための基本的な施策

イ．科学技術に関する予算、人材等の資源配分の方針、その他の科学技術の振興に関する重要事項

② 科学技術に関する大規模な研究開発その他の国家的に重要な研究開発の評価を行う。

③ ①のア．及びイ．に関し、必要な場合には、諮問を待たず内閣総理大臣等に対し意見を述べる。

総合科学技術会議の特徴として①戦略性･適時性（国家的･社会的課題に適時適切に対応するため科学技術に関する総合戦略を立案）、②総合性（人文･社会科学も含み、倫理問題等の社会や人間との関係を重視）、③自発性（内閣総理大臣等の諮問に応じ答申するのみならず、自ら意見具申）が挙げられる。

（2） 第3期科学技術基本計画の概要

1996年7月に閣議決定した第1期科学技術基本計画（1996年度から2000年度）では、社会的･経済的ニーズに対応した研究開発の強力な推進と知的資産を生み出す基礎研究の積極的な振興を基本的方向として示し、講ずべき施策をとりまとめた。続く第2期科学技術基本計画（2001年度から2005年度）[6]においては、新たに科学技術政策の基本的方向として目指すべき国の姿を「知の創造と活用により世界に貢献できる国」、「国際競争力があり持続的発展ができる国」、「安心･安全で質の高い生活のできる国」の「3つの基本理念」として示した。

2005年3月28日に閣議決定した第3期科学技術基本計画[7]では、第2期基本計画の掲げる3つの理念を基本的に継承しながら、科学技術、経済、社会をめぐる国内外の情勢変化と今後の展望等を踏まえて、3つの理念を実現するため、科学技術が何を目指すのかという、より具体化された政策目標を設定した。すなわち、以下のとおり、6つの大目標と、その各々を構成する12の中目標である。

理念1 人類の英知を生む

～知の創造と活用により世界に貢献できる国の実現に向けて～

◆目標1 飛躍知の発見･発明 ― 未来を切り拓く多様な知識の蓄積･創造

---

6 第2期科学技術基本計画
http://www8.cao.go.jp/cstp/kihonkeikaku/kihon.html

7 第3期科学技術基本計画
http://www8.cao.go.jp/cstp/kihonkeikaku/index3.html

(1) 新しい原理・現象の発見・解明
(2) 非連続な技術革新の源泉となる知識の創造
◆目標2 科学技術の限界突破 ― 人類の夢への挑戦と実現
(3) 世界最高水準のプロジェクトによる科学技術の牽引

理念2 国力の源泉を創る

～国際競争力があり持続的発展ができる国の実現に向けて～
◆目標3 環境と経済の両立－環境と経済を両立し持続可能な発展を実現
(4) 地球温暖化・エネルギー問題の克服
(5) 環境と調和する循環型社会の実現
◆目標4 イノベーター日本 ― 革新を続ける強靱な経済・産業を実現
(6) 世界を魅了するユビキタスネット社会の実現
(7) ものづくりナンバーワン国家の実現
(8) 科学技術により世界を勝ち抜く産業競争力の強化

理念3 健康と安全を守る

～安心・安全で質の高い生活のできる国の実現に向けて～
◆目標5 生涯はつらつ生活 ― 子どもから高齢者まで健康な日本を実現
(9) 国民を悩ます病の克服
(10) 誰もが元気に暮らせる社会の実現
◆目標6 安全が誇りとなる国 ― 世界一安全な国・日本を実現
(11) 国土と社会の安全確保
(12) 暮らしの安全確保

第2期基本計画において、国家的・社会的課題に対応した研究開発の中で特に重点を置き、優先的に資源を配分することとされたライフサイエンス、情報通信、環境、ナノテクノロジー・材料の4分野については、次のような観点から、引き続き第3期基本計画においても、特に重点的に研究開発を推進すべき分野（「重点推進4分野」という。）とする。（図2参照）

また、エネルギー、ものづくり技術、社会基盤、フロンティアの4つの分野について、引き続き、国の存立にとって基盤的であり国として取り組むことが不可欠な研究開発課題を重視して研究開発を推進する分野（「推進4分野」という。）と位置付け、適切な資源配分を行う。また、近年世界的に安全と安心を脅かしている国際テロ、大量破壊兵器の拡散、地震・台風等による大規模自然災害・事故、情報セキュリティに対する脅威、ＳＡＲＳ・鳥インフルエンザ等の新興・再興感染症な

どの社会的な重要課題に対して迅速･的確に解決策を提供するものである。その研究開発の実施に当たっては、国が明確な目標の下で、専門化･細分化されてきている知を、人文･社会科学も含めて横断的に統合しつつ進めることが必要であり、総合科学技術会議は、このような社会的な技術について、分野横断的な課題解決のための研究開発への取組みに配慮することを定めている。

(3) 分野別推進戦略の概要

分野別推進戦略は、政策課題対応型研究開発を対象とした、政府研究開発投資の戦略及び研究開発の推進方策をとりまとめたものである。

本戦略策定のため、総合科学技術会議は、2005年12月に、基本政策専門調査会の下に8つの分野別推進戦略プロジェクトチーム（重点推進4分野（ライフサイエンス、情報通信、環境、ナノテクノロジー･材料）及び推進4分野（エネルギー、ものづくり技術、社会基盤、フロンティア））を設け、集中的な調査･検討を進めてきた。

それぞれの分野別推進戦略では、分野毎に「重要な研究開発課題」、「戦略重点科学技術」、「推進方策」を定めている。「重要な研究開発課題」は、今後5年間に政府が取り組むべき重要な課題を、将来波及予測、国際競争、政策目標への貢献、官民の役割分担など総合的な視点から抽出したものである。

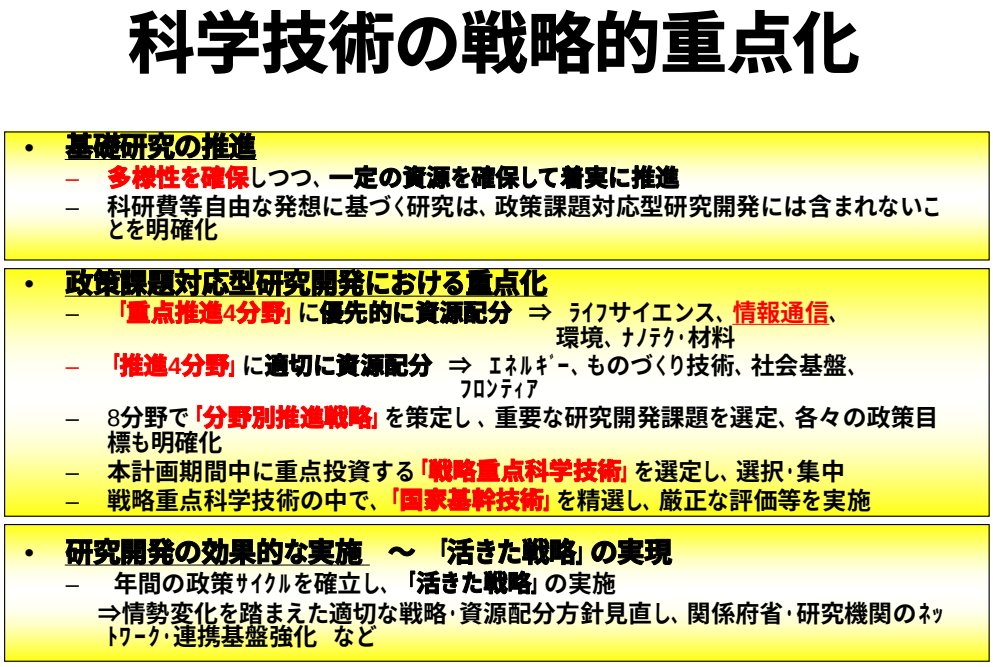


図2 科学技術の戦略重点化

(4) 分野別推進戦略情報通信プロジェクトチームでの検討の概要

情報通信分野における推進戦略を策定するに当たり、以下の7つの研究開発領域に分割して検討することとした。すなわち、基盤的なネットワーク領域、デバイス・ディスプレイ等領域、セキュリティ及びソフトウェア領域、よりアプリケーション側に近いユビキタス(電子タグ等)領域、ロボット領域、ヒューマンインタフェース及びコンテンツ領域、さらに両方に横断的に関わる研究開発基盤(コンピューティング)領域である。これらの領域ごとにワーキンググループ(以下WG)が設置され、短期間に集中的な検討が行われた。

また、重要な研究開発課題の選定に当たっては、段階的に技術を伸ばしていく領域と、新たに領域を立ち上げ世界的に指導性を保ちながら伸ばしてゆくチャレンジの要素が大きい領域をバランスよく保つ考え方が必要であるとの認識が示された。特に、国主導の研究開発には、リスクも高いが効果が大きい、革新的・不連続的(グランドチャレンジ)技術の研究に対する期待が大きい。この場合には目標を明確化し、研究の段階ごとに十分な評価を行いながら10年程度の長期にわたる研究を進めてゆくことが求められる。さらに、大きな研究開発の段階に至る前の小規模で多様な萌芽的研究を広範囲に実施できるようにする環境の整備が必要となるとの認識を示した。

セキュリティに関わる推進戦略策定においては、分野別推進戦略情報通信プロジェクトチームの下に設置されたWGにおいて実施された。このWGでの議論では、報告書2005にまとめられた戦略の概要が紹介され、WGでの議論に収斂されることになった。この結果WGでのとりまとめでは、技術開発戦略とフォローアップにおいては、情報セキュリティ政策会議と連携しながら実施することが取り入れられた。

(5) 分野別推進戦略の決定

分野別推進戦略情報通信プロジェクトチームでの検討を経て、最終的に情報通信領域の分野別推進戦略は、2006年3月22日に開催された、第53回総合科学技術会議において正式に決定された。

この分野別推進戦略では、情報セキュリティに係る重要な研究開発課題として「【課題5】利用者の要求に応じたデペンダブルなセキュアネットワーク」を設定した。また、他の重要な研究開発課題においてもセキュリティに対する取組みの強化が強く認識され、ソフトウェア領域、ネットワーク領域等においても言及されている。さらに、セキュリティ領域では、ITが我が国社会に広く浸透し、(a) 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、(b) 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意識から、以下の二つの研究開発課題を設定している。

【課題1】 情報セキュリティ技術の高度化

【課題2】 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

セキュリティ領域で述べられている問題意識と、そのための研究開発課題設定は、まさに報告書2005において本専門委員会が提言してきた戦略の方向性と一致しており、本専門委員会の提言が国家レベルの科学技術戦略に取り入れられたと言うことができる。また、具体的な推進プロセスにおいても、報告書2005で述べられていた各種アイディアが盛り込まれたものとなっていることは高く評価できる。

２．情報セキュリティ技術の現状認識と今後の方向性

本専門委員会では、2005年11月に報告書2005をとりまとめ、技術開発に対する政府の取組みについて具体的な方向性を示した。報告書2005の提言は、総合科学技術会議による第3期基本計画分野別推進戦略の情報通信分野にも反映され、また内閣官房情報セキュリティセンターが自ら施策を推進しているものもあり、その着実な実施に取組んできたといえる。一方、報告書2005をとりまとめて以来、さまざまな情報セキュリティに関係する事件・事故などのイベント、新たな技術の社会化などがおき、社会で活用される技術と情報セキュリティの関係も徐々に変化しつつあるといえる。

そこで本章では、報告書2005の段階での情報セキュリティと技術開発における認識を今一度概観し、さらにこの1年間での変化を踏まえたフォローアップとして、いくつかの新たな考え方を示す。これにより、より現状を適確に踏まえた技術戦略の構成と実施を持続的に行うために必要となる、基盤概念の見直しを行うものである。

２．１　情報セキュリティ技術戦略の基本

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。

条件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。
条件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。
条件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。

この3条件を満足する環境を実現するにあたり、報告書2005では、情報セキュリティ技術の役割を次のように定義した。まず情報セキュリティ技術は、条件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に利用される。そして条件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。このためには、1）情報セキュリティ技術の高度化（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）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）からの両面からの取組みが必要であると、報告書2005では提言した。

また、上記3条件のうち、条件③の「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、先に示した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、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との立場を示した。

本報告書においても、この基本的な立場には変化はない。

しかし、ITの活用が社会で急速に広まっている現状を考慮すると、情報セキュリティ技術戦略を考える場合には、条件③を実現するための「情報セキュリティを支える環境整備」については、より踏み込んで高信頼な社会システム[8]の形成をどのように実現するかについて、具体的な方向性とプロセスを考えなければならないだろう。例えば、単純な事故の発生の場合には、各組織が適切な技術を活用して、発生以前に想定していた事業継続プロセスを適切に実行することで対応することができるだろう。しかし、社会基盤を形成する重要なシステムでの大規模トラブルや、大地震といった激甚災害が発生した場合には、そもそも個々の組織が運用する情報システムの運用環境そのものに大きな変化が発生してしまい、単純に一つの組織による技術活用や事業継続性確保の組み合わせだけでは対応することが困難であることはいうまでもない。このような大きな環境変化が発生した場合においても、「高度情報通信ネットワーク（IT）」が適切にサービスを提供し、社会全体としての事業継続性を確保するためには、少なくとも技術とマネージメントの高度化だけでは不十分である。例えば、技術的な観点から見た機能バックアップをどのように提供するのか、他地域が代替機能を提供するといった地域的な機能バックアップをどのように形成するのかということまで含めて、技術的な観点、政策的な観点からの検討が必要である。この検討において生み出されるものが、従来から議論されてきたディペンダブルシステム（依存可能システム）のみではなく、より強固な技術基盤に支えられた依存可能性を持った社会システム、いうなれば「高信頼社会システム」の形成といえよう。政府が行うべき技術開発では、このような領域までをも踏まえた取組みが設計・実施されるべきである。

さらに、技術が社会展開するプロセスについても研究が必要である。例えば、我が国においては認証技術として生体認証（あるいは「生体計測に基づく認証技術」[9]）の研究開発は活発で、多種多様な製品が提供されている。また、最近では一部の金融サービスで本人認証の一つの手段として生体計測が活用されるようになっている。ところが、社会全体としてみた場合、生体計測に基づく本人認証はほとんど普

[8] 高信頼社会システム：trustworthy social system
[9] 生体計測に基づく認証技術：authentication using biometrics technologies

及していない状況のままである。これまでの本人認証の弱点(例えばパスワードや物理的なトークンを使った認証は、常に認証情報の盗難、他者によるなりすましの危険性がある)を補強して余りある生体計測技術は、既に実用の段階に入っており、多くの人たちが広い活用を期待しているにも関わらず、このような状況に留まっている。情報セキュリティにまつわる社会的な問題を解決する技術が存在しているときに、その技術の社会展開、あるいは社会化をどのように促進するかについては、研究対象と認識されていつつも、その取組みは殆ど存在していない。加えて、最近では、コンプライアンスや内部統制に対応した研究課題に対する重要性も増しているといった傾向も見られるところである。これらの領域についても研究活動を活性化させることで、我が国が保有する技術の社会展開、国際展開における競争力強化につながると考えることができる。

2．2 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

報告書2005の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で述べた(1)投資領域設定の継続的見直し構造の実現及び(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について、その具体的な実施方法及び課題を示す。

(1) 投資領域設定の継続的見直し構造の実現

公的資金により横断的な分野に跨る研究開発・技術開発を実施する際、その戦略的な目標設定を誰が実施するのか、また、どのような組織が開発を担当するのかなど、解決に至っていない課題が山積しているのが現状である。

本専門委員会では、これらの課題に対しても明確な方針を提示すべく、総合科学技術会議との密接な連携により、我が国における公的資金を活用した情報セキュリティに関連する研究開発・技術開発を網羅的に把握し、領域全体を俯瞰した評価を実施する。詳細は3．1に示す。

なお、今後、分野横断的な展開の増大が想定される情報セキュリティに関連する研究開発・技術開発では、その実行にあたり、従来からの各府省庁における予算措置だけでは実現できない事例が発生する可能性が高く、特に3．3で述べる「グランドチャレンジ型」プロジェクトの実施にあたり、内閣官房情報セキュリティセンターに設置する「グランドチャレンジ検討WG」において、投資配分方針を詳細に検討する必要が生じる。既存の競争的資金等の有効的活用を図りつつ、新たな資源配分を想定した枠組みの検討にも早急に着手するべきであろう。

(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

報告書2005では、実施される研究開発･技術開発においては、期待される成果の活用までを見越したメカニズムが必要であると提言した。そのために、A) 技術利用の現場からのニーズ掘り起こしから、研究開発現場へのフィードバック、さらには、研究領域の調整という「循環モデル」の構築、B) 研究成果の評価プロセスの高度化、C) 適切な役割分担を考えた産官学共同プロジェクトの実施の3つの構成要素からなる実施体制を構築することが必須であると述べた。

この提言を受け、内閣官房情報セキュリティセンターでは、まずは政府での成果利用を前提とした研究開発実施を試行的に行い、その中で「循環モデル」を構築するための問題点を明らかにするとともに、産官学の役割分担のあり方を明らかにすることに挑戦している。行政機関からの情報漏洩等、情報セキュリティを巡る問題が多発し、情報セキュリティ確保の取組み強化が求められる中、OSから独立した形でのセキュリティ機能の実装を題材として新たな技術開発に取組み、実際に内閣官房において成果を利用しようという目標を明確に打ち出してプロジェクトを運用している。

なお、このプロジェクトの概要については、「高セキュリティ機能を実現する次世代OS環境の開発」として本報告書の別添2に提示する。

(3) 情報セキュリティ技術の循環モデル

報告書2005で記載した「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。」を展開すると、図3のようなモデルが想定できる。」

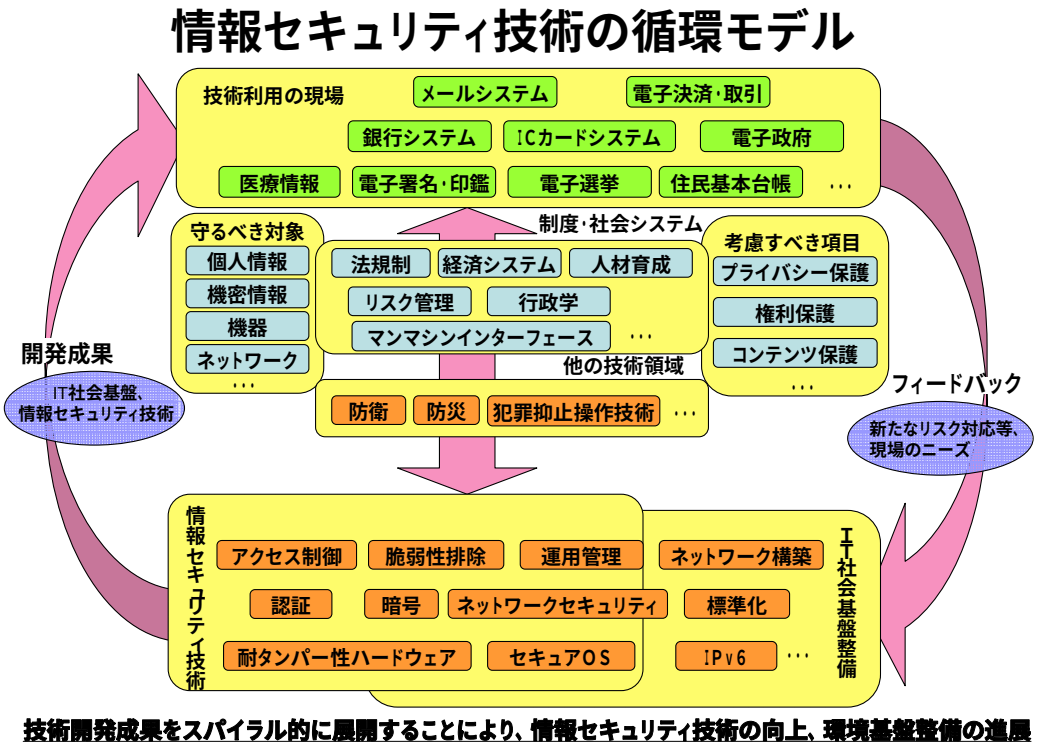


図3　情報セキュリティ技術の循環モデル

ここで最も問題になるのは、技術が社会に展開していくときに影響を与える「社会システム」とは何であるかという認識である。本専門委員会でも、この点については2005年度の開始当初より議論されてきた。直接的には、通貨、法律、契約、商慣行、各種制度などの人々が営む活動の広い意味での基盤を形成する取り決め、さらに、それらの制度の運用を具現化した情報システム（例えば電子政府システムはその代表例）となるであろう。しかし、将来的には、国民の多くの活動が依存する、多種多様な社会性を持った情報システム（例えば医療情報システムや電子決済システム）も、社会システムとして認知されるようになってくるのではないか。このようなことから、報告書2005では「社会システムデザイン研究の実施」を、情報セキュリティ技術を支える環境整備の一つの柱として提示してきた。この循環モデルにおいても、社会システムは広がりを持ったものとして捉えることが重要である。

また、具体的にどのような主体が循環を加速化していくのか、役割をどう分担するのかについては一定の共通理解の基盤は無く、この循環モデルを推進していくためにはドライビングフォースに関する検討が不可欠であり、その主体についての掘り下げが重要な課題となっている。

なお、循環モデルの実現に対して有効に機能する要素としては、以下のものな

どが挙げられる。

① 公的研究成果の積極的還元

公的資金を用いた研究開発･技術開発の成果を最大限に活用するためには、「高セキュリティ機能を実現する次世代ＯＳ環境の開発」のように開発成果を政府自らが利用するようなものでも、その開発成果を可能な限り、最大限社会還元するべきである。これにより、図5で示した情報セキュリティ循環モデルが活発に回り始め、スパイラル的に拡大することにより産業界の活性化、社会基盤の強化及びユーザーニーズに応えるサービスの拡充等が実現可能となり、報告書２００５で掲げた2つの取組み、すなわち①情報セキュリティの高度化、②組織、人間系の管理手法の高度化を実現するための強力なメカニズムとなる。

また、このようなサイクルを加速するためには、同時に社会における評価指標の設定に積極的に取り組むべきである。研究開発･技術開発は、必ずしもすべてが成功するものではなく、他の研究開発プロジェクト、民間企業、各種組織との間で、常に競争関係の中で実施される。このような環境においては、生み出された成果について、合理性を持った評価を行い、同時に技術が社会展開するプロセスの進捗を計ることができる評価指標設定が必要となる。このような評価指標の設定は、まだまだ十分に行われているとは言えず、情報セキュリティ領域だけではなく、政府資金による研究開発実施における大きな課題といえる。

② 新たな研究領域の可能性

これまでの研究開発･技術開発では、課題を設定し、その課題を解決するに資する技術を生み出すことが中心であった。これに対して、実際の問題を解決することで知見を集積し、その中で必要となる技術を同定したり、新たな管理手法を生み出したり、あるいは、評価手順を確立したりするための取組みも、近年科学的な取組みとして認知されるようになってきている。これはいうなれば「実装科学」[10]というべきものであり、問題を解きながら、そのプロセスそのものを科学的に解析し、問題解決を加速するための手法を同定していくものである。

このような実装科学は、我が国において取り組んでいる研究者は少なく、萌芽的な段階にある。しかし、危機管理、災害対策、リスク管理、行政の高度化に資する科学的管理手法などの領域における研究開発において、その重要性が認識されつつあるのも事実である。この「実装科学」の領域に対しての、政府における研究開発投資をどのように加速させるかについては、継続的な議論が必要である。

また、新しい技術の出現により、そのパッケージ要素について速やかな情報セキュリティ上の対応が必要となったり、さらに、既存技術であっても新たな活用方

[10] 実装科学：implementation science

法を採ることにより脆弱性が生じる場合や、関係法令の整備などの社会制度の変化によってリスクがリスクとして初めて認識されるといった事態も起こり得る。したがって、情報セキュリティ対策を考える上では、新しい事態が常に様々な面において出現し得るということについても認識しておく必要がある。

2．3 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

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策としては、基盤としてのITを強化することに直結する中長期的目標に対する投資の重点化と萌芽的研究への投資の強化が必要である。また、情報セキュリティ技術を支える環境整備として、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の必要性が特に指摘されている。

これらの重点化分野、環境整備のあり方については報告書2005においても示されているところであるが、情勢の変化や社会の要請に基づく見直しが不可欠である。さらに、それぞれの重点化分野の相互に、あるいは文科系と理科系を越える、産学官の枠組みを越える、開発と運用の壁を越えるところなどにも情報セキュリティの戦略的研究開発課題が存在する。

それら全体を俯瞰して欠落課題の抽出を行うためにも、従来の情報通信分野の情報セキュリティ領域のみならず、情報セキュリティをとりまく関連技術についても検討が必要である。この検討では、情報通信分野が拡大してきた領域すべてにおいて何らかの課題が存在するという仮定に基づいて検討を実施することが必要である。情報通信技術は、いまや急激に社会化を果たしている技術領域である。情報セキュリティは、情報通信技術とともに成長してきたが、同時にセキュリティの本質から、さまざまな学際領域による問題と関連するようになっている。この意味で、情報通信分野と関連する学際領域の拡大にあわせて、同時に情報セキュリティについて検討することの大切さが分かるであろう。このような観点から、情報セキュリティ領域をとりまく関連技術について試行的にまとめたものを図4に示す。

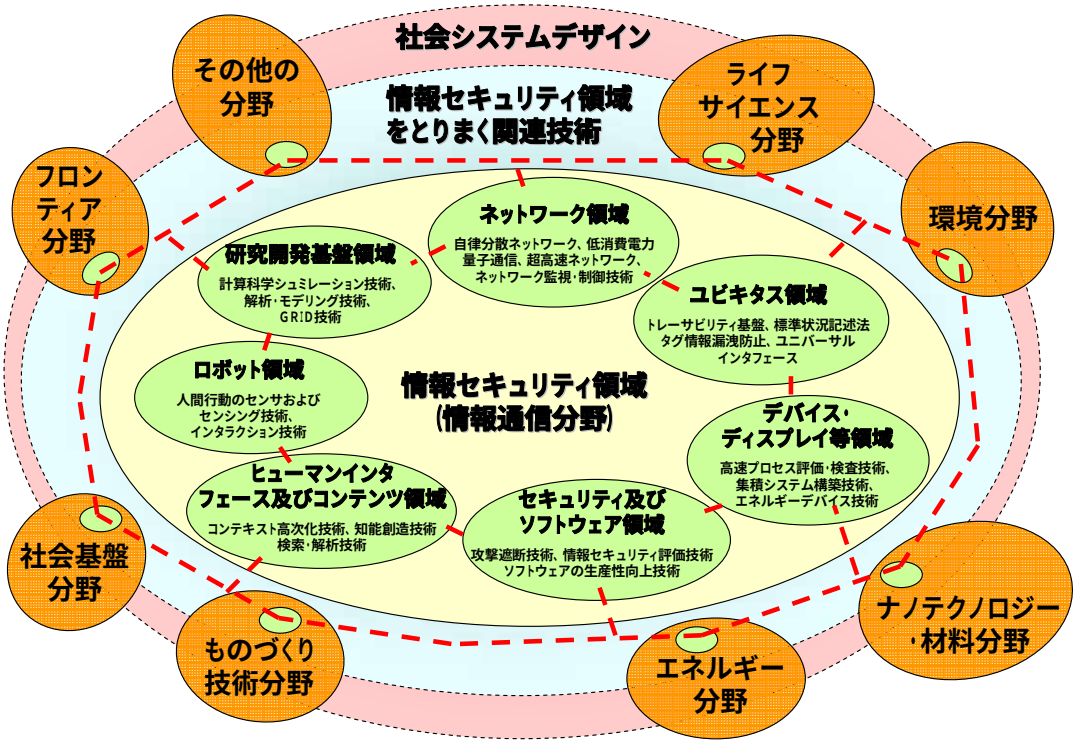


図4　情報セキュリティ領域をとりまく関連技術

効率的・効果的な研究開発・技術開発の実現のためには、以上の観点から新たな情報セキュリティ領域を対象とした研究開発・技術開発の実施状況の把握とその抽出並びに重点化分野の継続的な見直し等が必要である。その具体については、次節「3．1投資領域設定の継続的見直し構造の実現」において提示する。

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、こうした投資効率の見直しのみならず、官民とも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。

３．２００７年における実施のポイント

3．1 投資領域設定の継続的見直し構造の実現

限られた投資の中で効率的･効果的な研究開発･技術開発を実現するためには、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及び、投資領域設定の継続的な見直しを実施することが不可欠である。

なお、その実施においては狭義の情報セキュリティ分野に限定せず、情報通信全般、ひいてはITを活用する全ての研究開発･技術開発を対象とし、情報セキュリティの確保に留意することが重要である。

(1) 実施状況把握

本項において、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手法について示す。

実施状況の把握に際しては、「高度情報通信ネットワークを安心して利用可能」な環境を構築すると考えられる3条件（3条件については2．1を参照）を勘案してこれに関連すると思われる研究開発･技術開発を対象とし、本専門委員会としてとりまとめるため委員会事務局が調査する。また、被調査者に対する作業の重複を生じないよう留意する。具体的には、既に総合科学技術会議において「優先順位付け対象プロジェクト」として把握されているものがあり、それらについては総合科学技術会議が集約した情報を用いることとし、併せて総合科学技術会議の把握していないプロジェクトについても調査し、とりまとめに加えるものとする。

なお、研究開発･技術開発の把握は行うものの、個別の研究テーマの評価は行わない。各府省庁等で実施される評価制度を踏まえ、領域全体を俯瞰した評価を行うものとする。また、参考として、各府省庁等の評価制度の例を本報告書の別添3に提示する。

以下、把握手法の具体について提示する。

① 総合科学技術会議の集約した情報を用いるもの

科学技術振興調整費等の競争的資金の個別テーマを除き、国や独立行政法人等が行う研究開発･技術開発のうち、一定規模以上のプロジェクトについては、優先順位付け（ＳＡＢＣ評価）対象のプロジェクトとして総合科学技術会議が把握している。

優先順位付けの対象となるか否かは、以下のカテゴリーごとにその予算規模が異なっている。

ア．　8分野（重点推進4分野及び推進4分野、図2参照）の中の戦略重点科学技術

・・・・・新規全て、継続5億円以上

イ．　8分野の中の戦略重点科学技術以外の施策

・・・・・新規1億円以上、継続10億円以上

ウ．　8分野以外の施策で重点課題

・・・・・新規全て、継続10億円以上

エ．　8分野以外の施策で重点課題以外の施策

・・・・・新規1億円以上、継続10億円以上

「情報セキュリティ技術」そのものは8分野の中の「情報通信分野」に該当するが、ここでは、前述のとおり狭義の情報セキュリティ分野に限定せず、情報通信全般、ひいてはITを活用する全ての研究開発・技術開発を対象として把握することが重要である。なお、以下に、総合科学技術会議において把握されるプロジェクトを図示する。

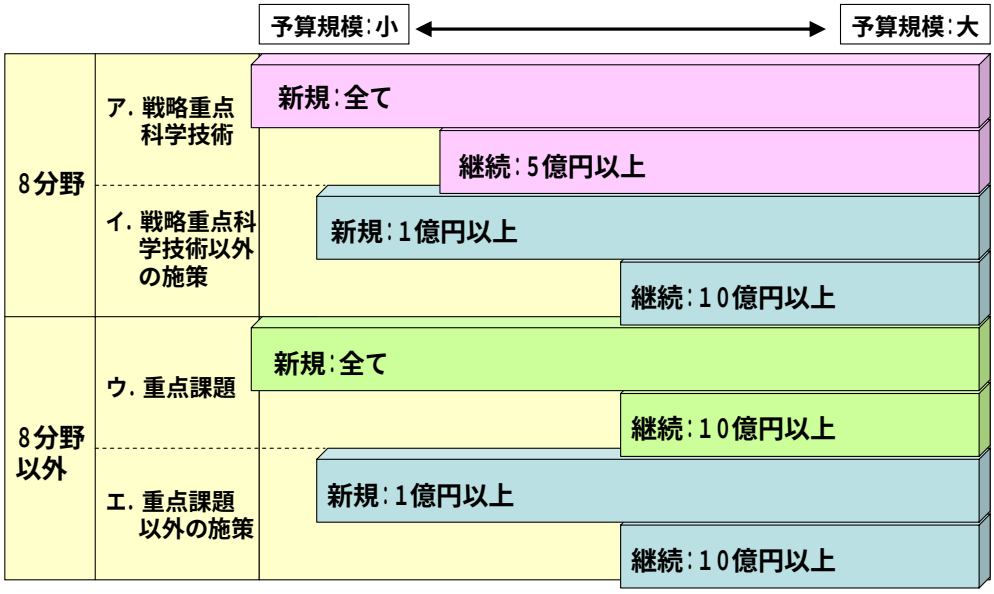


図5　総合科学技術会議において把握されるプロジェクト

② 直接調査を行うもの

競争的資金における個別テーマ並びに国や独立行政法人等が行う一定予算規模以下のプロジェクトについては、先の①において、総合科学技術

会議の把握対象から漏れることとなる。これら及び民間における研究開発・技術開発については、直接調査し、とりまとめる。

この場合においても、狭義の情報セキュリティ分野に限定せず、情報通信全般、ひいてはＩＴを活用する全ての研究開発・技術開発を対象として把握することが重要である。また、①は総合科学技術会議が集約したものを用い、それ以外を②として調査することから調査者、被調査者ともに作業の重複は生じない。

なお、以下に実施状況のとりまとめについて図示する。

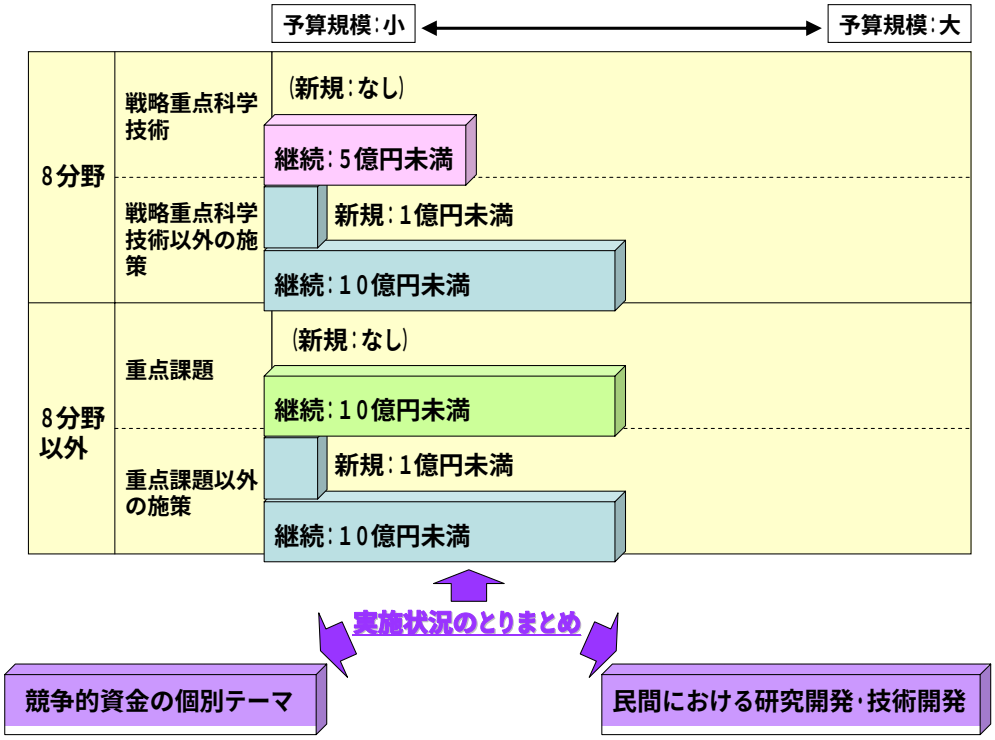


図6　実施状況のとりまとめ

民間における研究開発・技術開発の実施状況の把握に際しては、民間企業においては最先端の開発技術は社外秘であり、その開発テーマについても社外に公表しない可能性や、超初期的な研究開発については研究者個人あるいは研究部門にその情報が閉ざされており、単純な調査では把握できないという難しさを抱えているため、独自に把握することは困難であることが予想される。そこで、その問題を解決する方策として、企業関係者や学識経験者で構成される有識者会議や審議会などにおいて意見具申を行うことや、同様の市場調査、企業動向分析に関する経験やノウハウを有するシンクタンクにその把握を委託することなどが有効な手段であると考えられる。

(2) 情報セキュリティに関連する研究開発・技術開発の抽出及び整理

先の(1)において把握したプロジェクトから情報セキュリティに関連するものを抽出し、分野ごとに整理する。分野ごとの整理においては、複数分野にまたがるターゲットを視野に推進されるプロジェクトもあることを念頭に、整理を行う必要がある。また、整理を行う「分野」については、必要に応じて見直しを行うことが求められる。

今次報告書作成に際しては、本専門委員会における具体的議論の促進を図るため委員会事務局において収集・把握した内容に基づいて抽出及び整理を行った。情報セキュリティに関連する研究開発・技術開発のテーマ件数については306件であった。

なお、ここで分野ごとに整理し、次節以降で領域全体の評価を行うが、個別の研究テーマについては評価を行わない。

以下に、a)既に研究開発・技術開発の終了したもの、b)2006年度に実施中のもの、c)2007年度に概算要求しているもの、の別に分野ごとに整理した俯瞰図を示す。また、俯瞰図作成の元となるテーマの一覧表を「情報セキュリティに関連する研究開発・技術開発テーマ一覧」として本報告書の別添4に提示する。

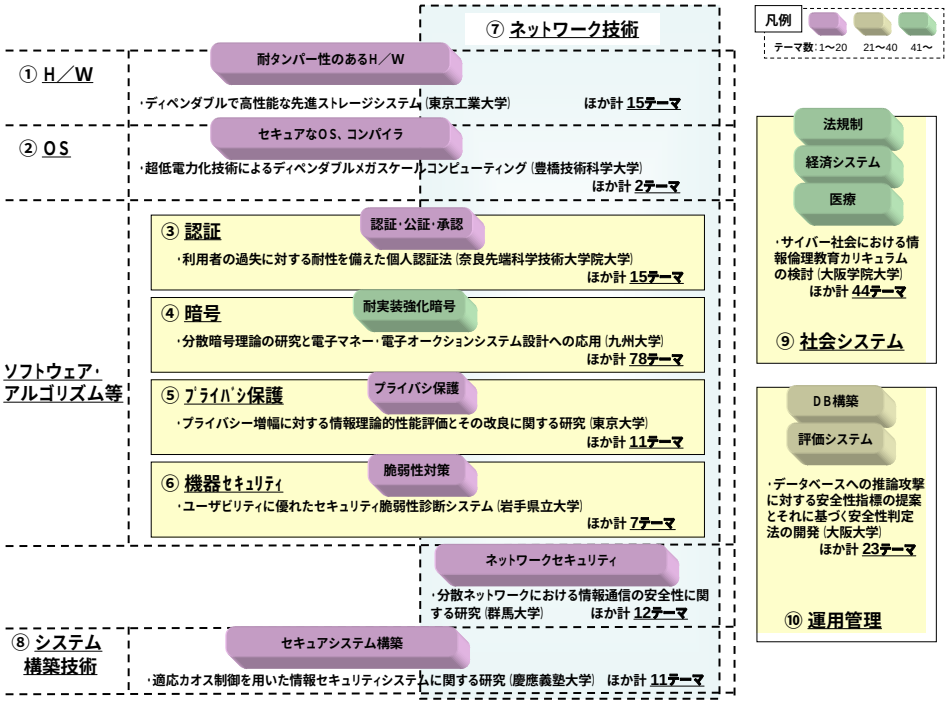


図7　既に実施済みの研究開発・技術開発の俯瞰図

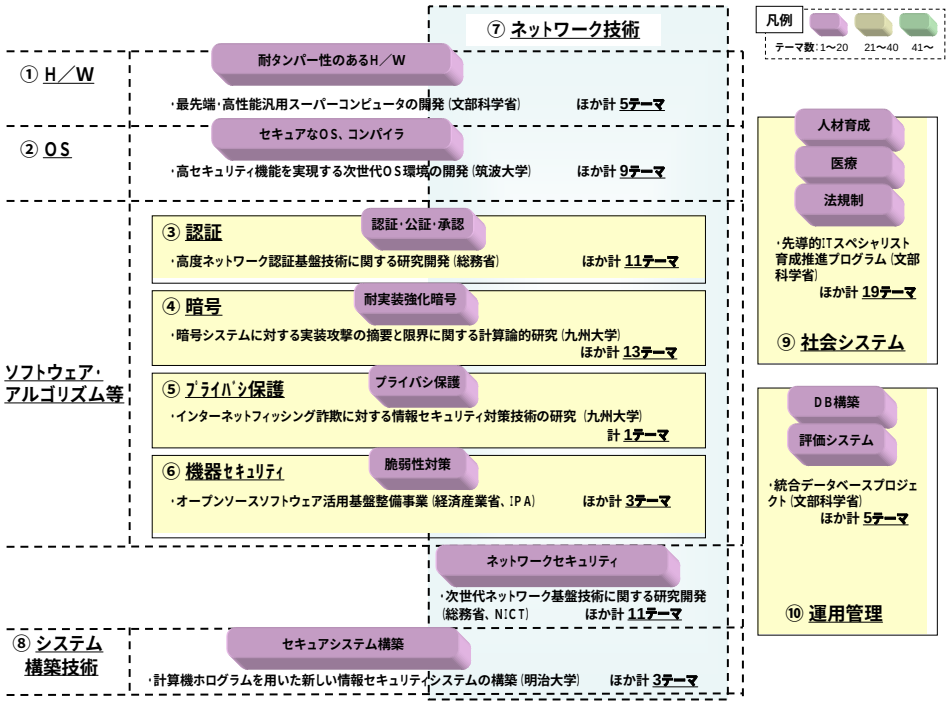


図8　2006年度実施中の研究開発・技術開発の俯瞰図

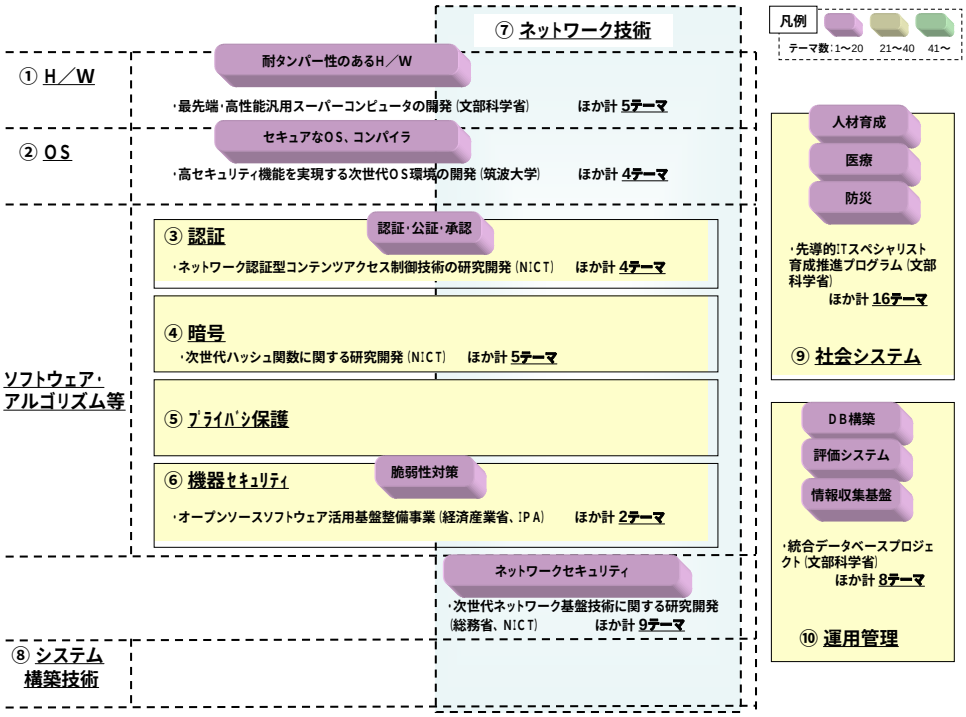


図9　2007年度概算要求の研究開発・技術開発の俯瞰図

(3) 報告書2005にて選定した重点化分野の見直し

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策を実現するためには、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する投資の重点化と、萌芽的研究への投資の強化が必要であり、こうした情報セキュリティ技術については、それらを支える環境整備が同時になされることが必要である。

2005年度の本専門委員会の成果としてこれらを「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」として報告書2005にまとめた。しかしながら、情報システムの利用形態の変化や新たな情報セキュリティ上の問題点の出現等により、求められる情報セキュリティ技術は変化するものであり、重点化分野の内容修正や削除、新たな分野の追加といった適宜のフォローアップ作業が重要である。

本項ではこのような観点から、2005年度に選定した重点化分野について、情勢の変化や社会の要請に基づく見直しを行った。以下に、2005年度に選定した重点化分野について図示する。

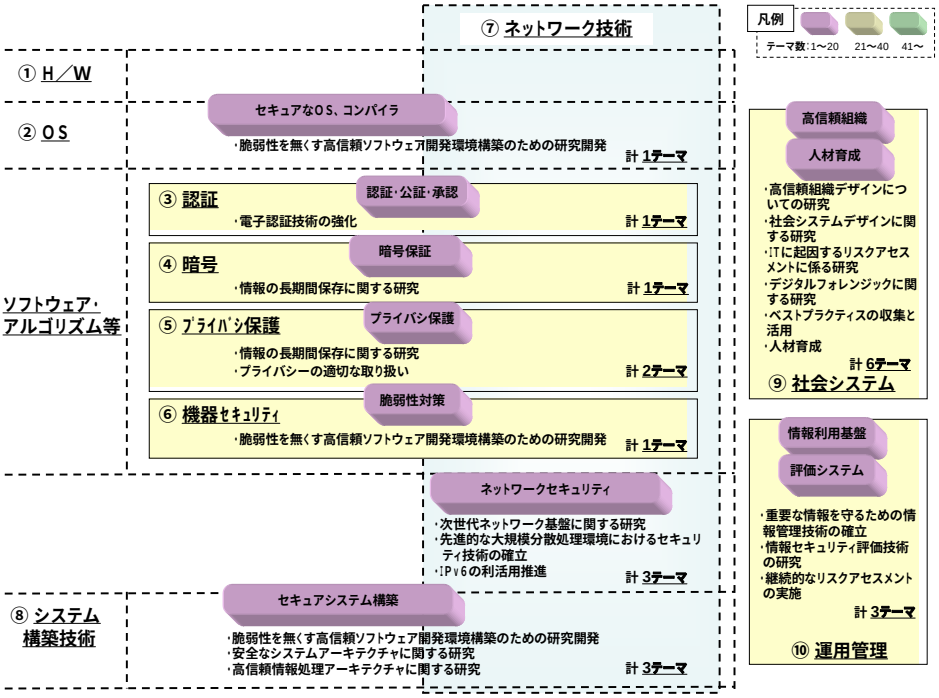


図10　報告書2005における重点化分野の俯瞰図

2005年度に選定した重点化分野のうち、認証技術については単に技術開発だけではなく、その社会展開までを含めた研究が必要である。このため、報告書2005の「電子認証技術の強化」を次の項目に置き換える。

○ **認証基盤のガバナンスの確立と高度化**

ＰＫＩに代表される高度な認証技術は１９９０年代から開発され、その社会展開が１９９０年代後半から行われている。この社会展開プロセスでは、関係する法整備、ＧＰＫＩや公的認証基盤等のシステム開発が行われた。しかし、依然として認証基盤の利用は広がっていない。また、近年認証基盤の構造と運用に関して、様々な研究成果が生まれてきているが、既存の認証基盤への組込みは進展していない。このようなことから、今一度認証基盤のあり方と必要な技術開発、運用環境の見直し、国内制度と国際的な動向のすり合わせ、法律を含む制度の点検が必要になってきている。このような複合的な要素（技術開発、制度点検と整備、運用体制の整備とサービス提供）についての取組みを総合すれば、認証基盤のガバナンスの確立と高度化を達成できると考える。このような取組みを早期に開始し、その成果を持続的に電子政府や、政府が行うＩＴ政策に展開する積極的な実施が必須である。

また、生体計測に基づく認証技術においても、迅速な社会展開を促進するための多面的な方策の立案と実施を行うことが必要となっている。生体計測に基づく認証技術は、我が国が国際的にも優位性をもった技術であり、その社会展開方策立案・実施は、今後の国際的な技術展開においても有用なものとなると期待される。また、生体計測に基づく認証方式は、従来のパスワードやトークンを活用した認証方式よりも、より高い安全性を提供するものであり、その積極的な活用を実現することは、安全・安心な高度情報通信ネットワーク社会を作り出す上でも大きく寄与することはいうまでもない。

また、新たな重点化分野として次の一点を追加する。これは従来から指摘されていた問題であり、報告書２００５においても「投資対象として検討することが必要」とされていたものであるが、昨今、その懸念が顕在化してきていることから重点化分野として加えることとしたものである。

○ **情報通信構成要素の検査技術の高度化**

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、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が重要で

ある。

さらに、報告書2005で示した「情報セキュリティ技術を支える環境整備」については、次の一点を追加する必要があると考える。

○ 情報通信基盤に対する依存性についての広範な検討

我が国の経済活動等の諸活動は、明らかに国内外の情報通信基盤に依存して展開していることはいうまでもない。しかし、どのような依存関係にあり、環境変化（事故、事件、災害等）が発生した場合の対応はどのようにあるべきかを検討することが必要である。これは、別の言い方をすれば、我が国の各種基盤が、規模の大小に関わらず環境変化が発生してもサービス提供を持続可能にするためには、どうあるべきかを明らかにする研究活動である。このためには、技術の役割、政策のあり方、社会投資の考え方なども検討対象として、多種多様な視点からの検討が必要となる。この研究は、情報セキュリティのみと関係するものではなく、広く重要インフラ防護、防災、危機管理に関係する。このために、領域横断的な研究活動の構成と加速が必要である。

報告書2005に対し、以上の更新を加えたものを、「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2007」として本報告書の別添5に提示する。

(4) 技術戦略策定

先の1）実施状況把握、2）抽出及び整理、3）重点化分野の見直し、を踏まえて情報セキュリティ関連の施策全体について総合的な評価を行い、あらたな技術戦略を策定する。

① 全体俯瞰の把握

今次報告書作成に際しては、委員会事務局において収集･把握した内容に基づき領域全体の俯瞰を行った（「(2) 情報セキュリティに関連する研究開発･技術開発の抽出及び整理」）。この作業結果は実施状況把握が十分に行われたものではないが、重点化分野とのマッピングによっていくつかの特徴があらわれている。

まず、重点化分野に挙げられている「電子認証技術の強化」については、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、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とともに、施策推進のネックとして公的個人認証が挙げられている事例もあり、当該技術を短期間に社会に

普及させるための方策と併せてその進展が期待されるところである。この観点から、重点化分野「電子認証技術の強化」については、前節に示したように、その方向性をより明確化し、総合的な取組みを構成する施策設計と実施が必要である。

また、プライバシーの保護については実施施策が少ないという傾向がある。認証強化と合理的な匿名性（anonymity）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できる。こうした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。

「ＩＴに起因するリスクアセスメントに係る研究」については、情報セキュリティ政策会議の下に設置された重要インフラ専門委員会における相互依存性解析の取組みや、民間団体である日本ネットワークセキュリティ協会（ＪＮＳＡ）における個人情報漏洩の経済的損失の試算[11]等の取組みがある。しかし、より体系的な取組みが構成されているとは言えず、特定のリスク、特定の環境における検討が開始されたばかりといった状況にあるといえよう。この意味で、より対象範囲を広げるための取組強化が必要であることは言うまでもない。さらに、リスクアセスそのものの方法論、さらにはリスクアセスメントを支援する技術の高度化についても、取組強化が必要である。

報告書２００５では「萌芽的研究への投資強化」において取り上げた「デジタルフォレンジックに係る研究」については、近年の法改正等によって発生している内部統制強化の一環としてのＩＴ統制の取組みの中で、成果利用が期待されているところである。しかしながら、研究そのものに従事する研究者が少ない状態で推移したことも原因となって、研究が活性化されていない。このため、引き続き公的研究資金の投入による、研究の絶対量増加を誘導することが重要であると考えられる。

なお、人材育成が重要であり、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・技術者の育成のみならず、広くＩＴ利用者のリテラシー向上の必要性も指摘されているが、この分野については、人材育成・資格制度体系化専門委員会において議論が行われ、２００７年1月２３日に報告書をとりまとめたところである（脚注 5）。

また、成果利用については問題山積の状態にある。現在の成果評価の方法は単純かつ未熟であり、成果の社会展開を促進させる観点からの評価が不在などの問題から、学術的成果（具体的には論文）の生産には研究者は積極的になるが、実際に有効性の高い研究成果を提供し、さらに社会展開

[11] ＪＮＳＡ「2004 年度情報セキュリティインシデントに関する調査報告書」
http://www.jnsa.org/houkoku2004/incident_survey.pdf

までも取り組む研究活動が少ない状況にある。また、成果利用を実施する側でも、創意工夫を施して新しい技術を活用することに挑戦するよりも、既存のシステムの単純な拡張を行って安定的にシステム構築を行う方向に留まる傾向が強い。このため、新しい技術の社会展開がなかなか進まない状況が続いている。この問題を解決する単純な方法は無く、様々な複合的な取組みを実施することが必要であることは明らかであるが、具体的に何をなすべきかは答えが出ていない白紙状態であるといえよう。このため、広く議論を喚起し、この問題に着手する体制から整備する必要があるといえよう。

② 公的資金の重点的投入方法の検討

情報セキュリティ技術の高度化の推進のためには、政府機関が行う研究開発・技術開発への投資においては戦略性を持った実施が必要であるが、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される。その観点から、研究者の研究費の選択の幅と自由度を拡大し、競争的な研究開発環境の形成に貢献する競争的資金の積極的な運用が期待される。具体的には、科学技術振興調整費等の既存の施策を積極的に活用するほか、必要に応じて新たな施策を推進することも重要である。

③ 民間との役割分担の検討

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なされるよう働きかける。

また、研究開発・技術開発は我が国のみで行われるものではなく、他国の研究機関、企業との競争環境の中で実施される。この意味で、我が国の競争力を強化し、成果の国際展開を加速することができるような体制も官民で整備すべきである。具体的には、広く国際的な観点からの研究開発テーマの絞込みと、国際展開のための標準化活動や国際実証実験の遂行などについても積極的に行うべきである。

個別には、産学官それぞれにおいて、次のような役割分担を行うことが期待される。

【産】

- 産学が協働した人材育成
- 民間企業による研究開発の促進

・ 技術的優位分野における主導性の発揮（日本発の国際標準の獲得）

【学】

・ 人材育成機能の強化

・ 競争力の強化（世界の科学技術をリードする大学の形成等）

【官】

・ 府省を越えた研究費制度の改革

・ 本格的な産学官連携への深化

・ 知的財産戦略、標準化戦略の策定

④ 新たな学際領域への挑戦

高い投資効率が見込まれるものの、民間での研究開発・技術開発の取組みが期待できない研究については、政府が主体的に取り組む必要がある。また、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り、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幅広にその実施を行う必要がある。

一方、近年問題となっているのが、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。例えば、医療機関における様々な電子化は典型的な問題である。従来、医療行為そのものは医師によって患者を対象にして行われるＩＴとは比較的無縁なものであった。しかし、近年、特に大規模医療機関では、カルテの電子化、コンピュータシステムを利用した投薬管理、患者の治療履歴管理、検査データの電子的な交換などが行われ、医療の現場にもＩＴが浸透し始めている。このため、事業継続性確保や、患者情報の保全、医療行為に直結した情報処理機器の保全など、医療が実施される環境に即した情報セキュリティに関する問題解決が必要となっている。

さらに、「ヒューマンリレーテッドＩＴリスク」[12]への対応も課題となっている。例えば、万が一事故が起こった場合でも、その被害の局限化を図るためには、関係主体間において正確な情報の共有とともに相互の意思疎通の確保が重要である。一方、人間の行動的側面・心理的側面を巧みに悪用する攻

[12] ヒューマンリレーテッド IT リスク（human related IT risk）：人為的、人間的な要素が関係した IT リスク。様々なシステムを構築し、利用するのは人間であり、情報セキュリティ対策上、人間がどのように考え、行動するのかという視点で方法論を研究することが求められる。

撃や内部犯行者による不正行為、あるいは人為的なミスやエラーなどへの対処には、攻撃者やシステム利用者、管理者における心理学的な分析と対応策が不可欠である。このような観点から、リスクコミュニケーションやセキュリティ心理学についての組織的な研究が必要となっている。

また、2003年7月にとりまとめられたe－Japan戦略Ⅱや2006年1月に示された「IT新改革戦略」においても、「安心・安全なIT社会の実現」という目標の下、産学官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。

このような新たな領域への取組みについて、広範な調査を行い、どのような成果が生み出されているかを把握することが、内閣官房情報セキュリティセンターや各省庁において積極的に行われ、同時にその情報の集積と評価を実施すべきである。また、他領域で生み出されたベストプラクティスの利用可能性検討等の取組みの拡大も検討すべきである。

(5) 提言

前述の手順を踏まえ、(4)に示した技術戦略策定結果を総合科学技術会議等に提言する。提言の観点として、例えば検討の結果導き出された重点化分野に関して、1)重点化分野を戦略重点科学技術分野とする、2)各種機関で実施する競争的資金のテーマとする等が想定される。なお、以下に提言の仕組みについて図示する。

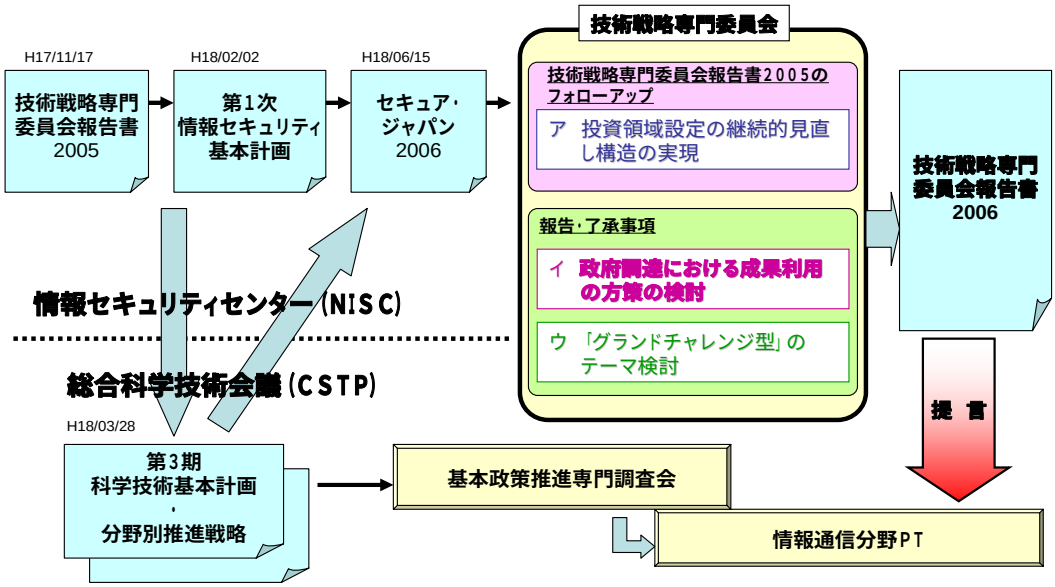


図11 提言の仕組み

この手順を毎年継続的に実施することにより、情報セキュリティにおける投資領域設定の継続的見直し構造を実現する。

3．2　調達を通して成果を活用するガイドライン策定の検討

急激に進展したIT社会において、企業1社のトラブルが社会全体に波及する可能性もあり、企業は社会全体への影響も考えた情報セキュリティ対策が必要となっている。しかし既存の情報セキュリティに関連する対策では企業価値に必ずしも直結しないこと、また、IT関連トラブル発生時のリスクが明確でないことなどから企業の取組みが思うように進展していないのも事実である。こうした状況は企業に限らず、政府や、個人の生活でも同様である。

このような状況を改善するためには、ITに関連したトラブルについて自身の被害の局限化という観点に止まらず、社会秩序を乱す行動や社会から非難される行動をしないように努め、IT社会の一員としての社会的責任を果たすという観点から、情報セキュリティを適正なレベルで確保する構造、いわゆる情報セキュリティガバナンスと、そのデザインが重要である。しかしながら、本概念を実践するためには必要となる技術の開発、導入するシステムの調達及び利用する組織、人間系の管理手法など様々な要件を分析し、総合的な視点から検討を積み重ねていかなくてはならず、この情報セキュリティガバナンスのデザイン自体が情報セキュリティ技術における研究分野である。

ITが社会全体に大きな影響を与えるようになった現在、このような考え方は、社会システムのデザインそのものである。例えば、1）公的個人認証や民間認証、政府の認証の信頼感をどう作っていくかといった、グローバルトラストネットワークの設計を日本から世界に提案し、グローバルスタンダード化を目指す。2）政府による研究開発・技術開発の成果を政府自ら調達し、その成果をどのように社会に還元し、国際的なマーケッティングを含め、広く普及させていく。3）IT社会や電子政府の全体を俯瞰し、現実の脅威その他を分析しながら、どのように脅威が出て来るのか、どのような対処方法があるのかを考え、実証し、その機能を政府が調達基準として示すことにより技術開発に携わる開発者の意識をリードしていく、などの研究課題が考えられる。

以上の観点から政府自らが関与する情報セキュリティ技術戦略の一環として調達を通して成果を活用するガイドライン策定を本専門委員会として検討する。本ガイドラインでは政府で活用することを前提にした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、直接政府が活用し、人間組織の管理手法について、その方法をどのようにするかに関しても併せて提言する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。

具体的には文部科学省科学技術振興調整費の重要課題解決型研究により2006年度から筑波大学を中心とした産学官の共同研究開発プロジェクトとして開始した「高セキュリティ機能を実現する次世代OS環境の開発」を通して、開発、調達及びその利用という政府における一貫した成果利用までを見据えた研究開発・技術開発を実施し、その過程において発生する様々なノウハウをガイドラインとしてとりまとめる。(プロジェクト概要は別添2を参照)

なお、本専門委員会において議論された意見をもとに、調達を通して成果を活用するガイドライン策定に関しての試案を「調達に向けたガイドラインの検討及び留意点」として本報告書の別添6に提示する。

3．3 「グランドチャレンジ型」テーマ検討の場の設置

報告書2005で示した社会基盤としてのITにおける情報セキュリティ問題、すなわち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。に対する有効な解決策の一つである「グランドチャレンジ型」の研究開発・技術開発を実際に具体化するためには、テーマ選定のプロセス及びプロジェクト実施方法等を詳細に検討する必要がある。

(1) 基本的な考え方

重要な研究開発課題の選定に当たっては、段階的に技術を伸ばしていく領域と、新たに領域を立ち上げ世界的に指導性を保ちながら伸ばしていくチャレンジの要素が大きい領域とをバランスよく保つ考え方が必要である。特に、国主導の研究開発には、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」の研究開発に対する期待が大きい。この場合には目標を明確化し、研究の段階ごとに十分な評価を行いながら、10年程度の長期にわたる研究を進めていくことが求められる。さらに、大きな研究開発の段階に至る前の小規模で多様な萌芽的研究を広範囲に実施できるようにする環境の整備が必要となる。

(2) グランドチャレンジ検討WGの設置

委員会事務局である内閣官房情報セキュリティセンターが検討体制(以下「グランドチャレンジ検討WG」という)を整備する。

(3) グランドチャレンジ検討WGでの検討事項

「グランドチャレンジ型」の研究開発・技術開発テーマを設定するプロセスとし

て、例えばアポロ計画における「月に人を立たせる」というような大目標をまず決め、その大目標の下でトップダウン的に関連の深いテーマをいくつかのサブ課題として決め、統合的に推進する方法（ビジョナリィ・ゴール型）と、大目標を先決めせず、情報セキュリティの技術要素として非常に重要なものをボトムアップ的に精査し、その中で世界のリーダーシップを取って推進していくべき技術を決め、それについては我が国の総力を結集して大がかりに取り組んでいく（テクニカル・コンポーネント型）という二つのアプローチが考えられる。

グランドチャレンジ検討WGではこの二つのアプローチについて、検討を深めるとともに具体的なテーマ選定のプロセスについて検討する。「ビジョナリィ・ゴール型」の場合、分かりやすく象徴的なターゲットを選定する段階で、長期的な研究を実施する意義、サブ課題間の関連性及び研究開発と社会の関係等の観点を明確化する。「テクニカル・コンポーネント型」に関しては本専門委員会で実施する「投資領域設定の継続的見直し構造の実現」の検討内容に基づいて、情報セキュリティの技術要素の選定を実施する。

（4） 具体的なテーマ選定方法

具体的なテーマ選定にあたって、特に「ビジョナリィ・ゴール型」の場合、集中した議論が不可欠である。テーマ選定者は、情報セキュリティの知識だけでなく、情報通信の技術知識はもとより、組織・人間系の管理手法や社会システムデザイン等の知識も必要となる。また、予算配分等での客観的な選定者（現実主義者）だけではグランドチャレンジ型のテーマ選定は出来ない。夢を見られる人（ドリーマー）が必要であるのは、アポロ計画当時の技術水準で「月に人を立たせる」等のキャッチフレーズを考えれば明白である。

テーマ選定は、上記の観点で選定した専門家による集中的な議論を合宿方式により実施することが有意義と考えられる。仮にテーマ選定が不調に終わったとしても、その過程で議論した様々な観点は個々の研究開発に有効であろう。また、継続的にテーマ選定を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。

また、上記の選定方法以外にも、公募やワークショップ等の開催により、自薦、他薦を含めた様々なアイディアを広く発掘することも考えられる。

（5） 研究開発・技術開発を推進する体制

選定されたテーマによる研究開発・技術開発を推進するにあたり、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構築が最重要事項となる。具体的には、以下の点に留意する必要がある。

- プログラムマネージャー制等の検討
- イノベーション25との密接な連携
- プロジェクト評価手法及び体制の確立
- 開発予算の確保
  - 競争的資金等の既存の制度の有効活用
  - 長期間にわたるプロジェクト実施が可能な新たな制度の検討

(6)「グランドチャレンジ型」プロジェクトの実現行程

「グランドチャレンジ型」のプロジェクトを実現するためには2007年度中にグランドチャレンジ検討WGを開催し、実施方法の詳細な検討を行い、その検討結果をふまえた具体的なテーマを選定する。

選定されたグランドチャレンジテーマに関連する各種の個別テーマは、当面の間、関係各府省庁施策の競争的研究資金等により実施する。本専門委員会はその個別テーマの進捗に関して、グランドチャレンジテーマにおける個別要素の観点として着目し、総合的な領域俯瞰評価を実施する。

また、グランドチャレンジテーマ検討及び関連する個別テーマの実施と並行して、(5)に示した研究開発・技術開発を推進する体制(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新たな枠組み)をグランドチャレンジWGが設計し、その結果を本専門委員会が総合科学技術会議に対して提言し、2009年度以降の本格的な「グランドチャレンジ型」研究開発・技術開発環境の実現を目指す。

先行して実施している各種個別テーマは、必要に応じて順次新たな枠組みとして実施するグランドチャレンジプロジェクトに移行する。

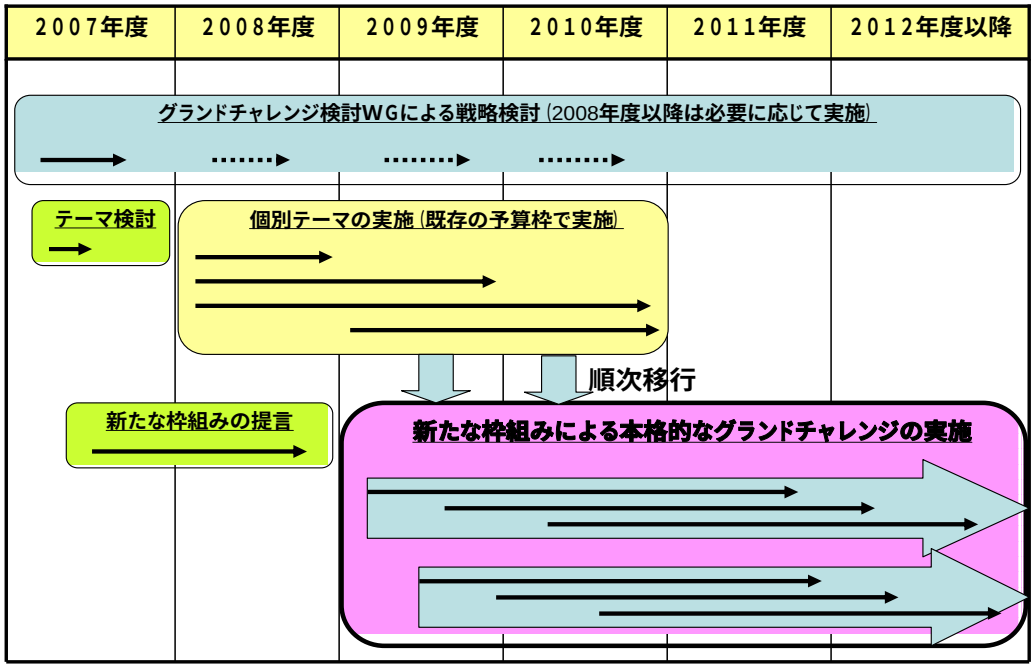


図13　グランドチャレンジプロジェクト行程（イメージ）

（7）「グランドチャレンジ型」研究開発・技術開発の留意点

分野横断的戦略目標を設定した場合、その目標を実施する組織も人もいないというような状況が発生する恐れがある。我が国において、科学と技術の関係は曖昧で、社会科学、自然科学と技術の関係についても構造的にあまり理解されていない。このような状況でこれらの領域を横断する戦略テーマを設定しようとすると、様々な問題を包含する恐れがある。

また、先鋭的な個別分野の研究成果にとらわれ過ぎず、既存技術の有効活用を考え、それら全体を統合して、どのようにセキュリティを利便性のあるものにするか、コストを下げるのかという側面も十分に検討するべきである。

なお、グランドチャレンジ型プロジェクトは10年程度の長期的視野での研究開発・技術開発を想定しているため、周辺分野での状況変化に特に注意するべきである。プロジェクトの評価を厳密に実施し、周囲の状況にそぐわないような状況であると確認された場合には、プロジェクトの中止を含め、大幅な目標設定変更等が生じる可能性も考慮しなければならない。

＜参考＞

報告書2005で「グランドチャレンジ型」領域の例として取り上げたテーマ

○ **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。

（参考）技術戦略専門委員会報告書２００６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

【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

問題点の抽出と論点の整理

２００５年　９月２１日　第２回会合

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

「報告書2005」骨子案についての検討

２００５年１１月　４日　第４回会合

「報告書2005」案についての検討

２００６年１０月３１日　第５回会合（２００６年度第１回会合）

課題整理及び検討

２００６年１１月２８日　第６回会合

「報告書2006」骨子案についての検討

２００７年　１月１０日　第７回会合

「報告書2006」案についての検討

２００７年　６月　６日　第８回会合

「報告書2006」案についての検討

＜別添一覧＞

別添1：技術戦略専門委員会報告書（2005年版）概要
別添2：高セキュリティ機能を実現する次世代ＯＳ環境の開発
別添3：各府省庁等の評価制度の例
別添4：情報セキュリティに関連する研究開発・技術開発テーマ一覧
別添5：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2007
別添6：調達に向けたガイドラインの検討及び留意点

別添1

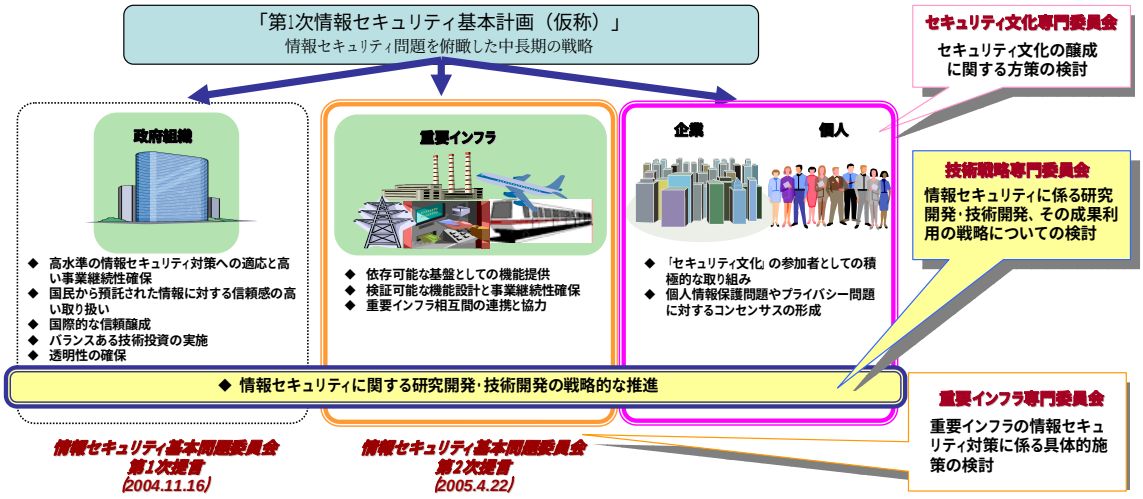
技術戦略専門委員会の概要

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

1 技術戦略専門委員会報告書の位置づけ

○ 「第1次情報セキュリティ基本計画（仮称）」に関する当面の審議の充実に資するため、情報セキュリティに係る研究開発・技術開発、その成果利用の戦略について検討し、「技術戦略専門委員会報告書」としてとりまとめ。

○ 情報セキュリティの確保においては、継続的な技術開発と、その社会展開を円滑に行い、成果を全ての主体が享受できる環境作りが必要であり、喫緊の課題を解決するための技術開発と、中長期的な視点に立った研究開発投資の戦略設定が強く求められているとの認識に基づいて議論。



「第1次情報セキュリティ基本計画（仮称）」に向けた検討の全体像

2 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

○ 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。

○ 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。

○ 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か、情報セキュリティ技術戦略の基本的な考え方を提示。

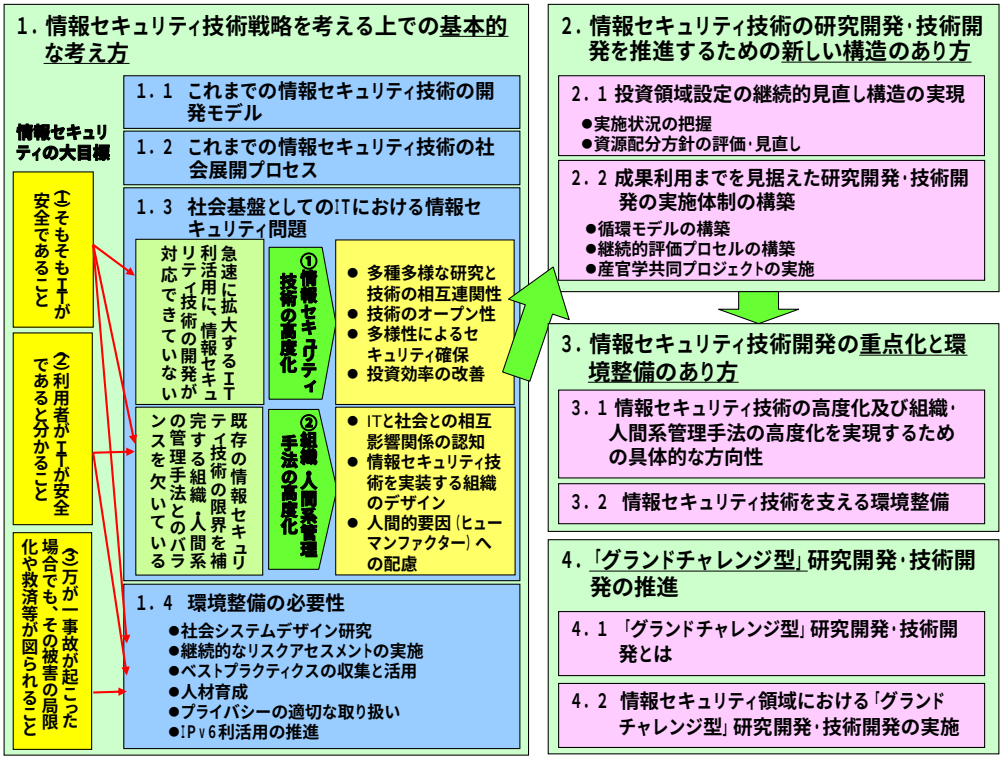


図1　報告書の全体像

(1) 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

(ア) 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

○ 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」[1]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。

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。

○ 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

[1] 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。」

難い。

(イ) 情報セキュリティ技術の役割と今後の方向性

○ 情報セキュリティ技術の問題点

- 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。
- 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。

○ 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。

①多種多様な研究と技術の相互連関性

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。

②技術のオープン性

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。

③多様性によるセキュリティ確保

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。

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投資効率の改善にも持続的に取り組むことが必須。

○ 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、以下の点に留意しつつ、組織・人間系の管理手法の高度化が必要。

①ITと社会との相互影響関係の認知

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。相互影響関係や予測される脅威、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。

②情報セキュリティ技術を実装する組織のデザイン

組織論的及び経営情報論的な視点からの研究が必要。

③人間的要因（ヒューマンファクター）への配慮

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。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。

（ウ）情報セキュリティ技術を支える環境整備の必要性

○ 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、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。具体的には、以下の通り。

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。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。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。

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。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。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。

③ ベストプラクティスの収集と活用

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し、社会知として活用していく取組みを強化。

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。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。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。

⑤プライバシーの適切な取扱い

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。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。

⑥IPv6利活用の推進

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はIPv6が基盤となり、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。

3 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

○ 投資領域設定の継続的見直し構造の実現

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、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。

＜具体的な方策＞

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。

○ 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。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。

(ア) 循環モデルの構築

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。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。

(イ) 継続的評価プロセスの構築

成果利用の可能性を評価する枠組みも必要。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。

(ウ) 産官学の共同プロジェクトの実施

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。

＜具体的な方策＞

①循環モデルの構築

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。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。

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。

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。

4 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

○ 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及び組織・人間系の管理手法の高度化の具体的な方策を実現するためには、以下の投資強化が必要。

(ア) IT強化直結型研究への重点化

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。

①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
②次世代ネットワーク基盤に関する研究
③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
④安全なシステムアーキテクチャに係る研究
⑤電子認証技術の強化
⑥IT に起因するリスクアセスメントに係る研究
⑦高信頼性組織デザインについての研究
⑧重要な情報を守るための情報管理技術の確立
⑨情報セキュリティ評価技術の研究

(イ) 萌芽的研究への投資強化

民間の取組みが乏しい萌芽的研究として考えられる例は以下のとおり。

①デジタルフォレンジック[2]に係る研究
②情報の長期間保存技術に関する研究
③高信頼情報処理アーキテクチャに関する研究

(ウ) 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。

○ 情報セキュリティ技術を支える環境整備

情報セキュリティ技術を支える環境整備として、以下の取組みが必要。

(ア) 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。

(イ) 継続的なリスクアセスメントの実施

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。

2 (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。

(ウ) ベストプラクティスの収集と活用

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。

(エ) 人材育成

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。

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の体得。

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。

(オ) プライバシーの適切な取扱い

プライバシー保護の強化に向けて、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。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。

(カ) IPv6の利活用推進

政府は、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。

5 「グランドチャレンジ型」研究開発・技術開発の推進

○ 「グランドチャレンジ型」研究開発・技術開発とは

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連関性の再認識、さらには、研究と社会の関係を明確化されることが期待。

○ 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

「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。

①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。

②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。

③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。

④認証等の基礎となるトラストポイント[3]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。

⑤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。

3 (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。

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）

（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

別添2

高セキュリティ機能を実現する次世代ＯＳ環境の開発

本紙では、文部科学省科学技術振興調整費の重要課題解決型研究により２００６年度から筑波大学を中心とした産学官の共同研究開発プロジェクトとして開始した「高セキュリティ機能を実現する次世代ＯＳ環境の開発」について、その概要を提示する。

行政機関からの情報漏洩等、情報セキュリティを巡る問題が多発し、情報セキュリティ確保の取組み強化が求められる中、内閣官房情報セキュリティセンターでは、ＯＳから独立した形でのセキュリティ機能の実装を題材として新たな技術開発に取組み、実際に内閣官房において成果を利用しようという目標を明確に打ち出して本プロジェクトを運用している。

具体的には、本プロジェクトにおいて、その研究開発方針を議論し、方針を決定する研究開発運営委員会の委員として、内閣官房をはじめ、内閣府、総務省、経済産業省、独立行政法人情報通信研究機構及び独立行政法人情報処理推進機構が参加し、本プロジェクトの運営を積極的に支援する。また、開発、調達及びその利用という政府における一貫した成果利用までを見据えた研究開発･技術開発を実施することにより、その過程において発生する様々なノウハウをガイドラインとしてとりまとめることとしている。

なお、本プロジェクトにおける実施内容及び開発のポイントについては以下のとおり。

①「高セキュリティ機能を実現する次世代 OS 環境の開発」の実施

情報セキュリティ確保の取組み強化が求められる中、以下の方針を定め、研究開発を実施する。

A) Windows等の既存ＯＳ環境で提供されるセキュリティ機能に加え、ＯＳから独立した形でセキュリティ機能を実装し、同時にＯＳ及びアプリケーション等からなる現在の利用者環境を活用可能な、次世代のＯＳ基盤環境の確立を目指す。
B) 政府機関（内閣官房情報セキュリティセンター等）における実運用を前提とする。
C) 優秀な若手研究者による集中的研究開発方式を通し、ＯＳ開発能力を有する人材を育成することを目指す。

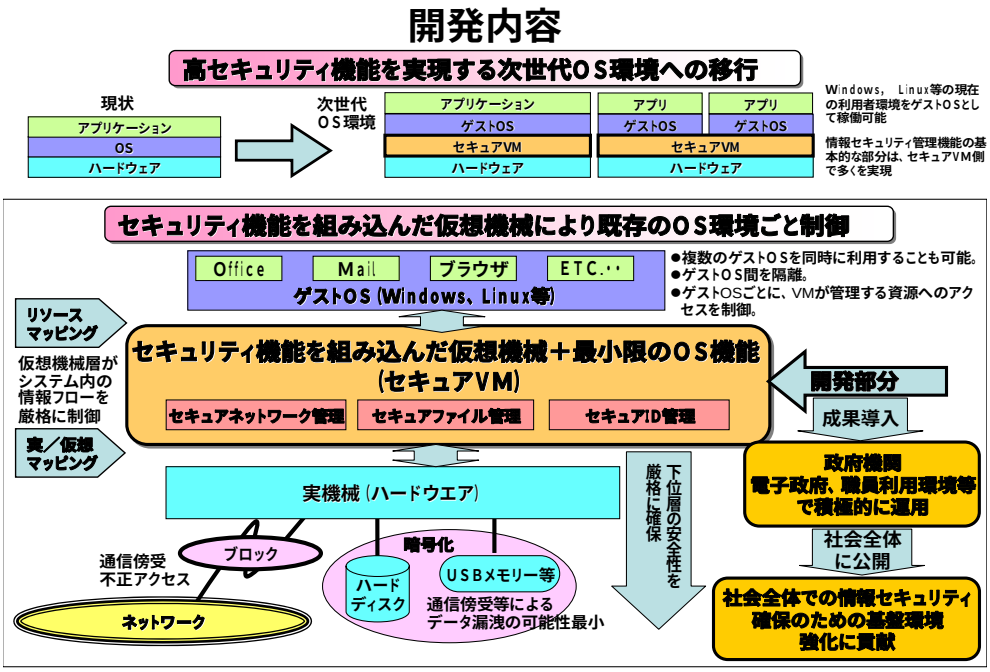


図　「高セキュリティ機能を実現する次世代ＯＳ環境の開発」開発内容

②研究開発のポイント

A) Windows、Linux等の現在の利用者環境をゲストＯＳとして稼働可能とし、同時に情報セキュリティ機能を、利用者環境に依存しない形で集約的に提供する仮想機械（VM：Virtual　Machine）機能と、これを稼働させるための最小限のＯＳ機能（以下、併せてこれら機能を「セキュアVM」と呼ぶ）を開発する。

B) 利用者はゲストＯＳであるWindows等が提供する環境で業務を実施するが、システム運用上の要となる情報セキュリティ管理機能の基本的な部分は、セキュアVM側で多くを実現し、ゲストＯＳに依存しない管理環境を構築する。

C) 統一のIDを利用してのPC起動管理、そのIDを利用してのハードディスクやＵＳＢメモリ等の暗号化、さらにはＶＰＮを利用した通信経路の暗号化などを、セキュアＶＭで実現し、情報漏洩等のリスクを低減する。将来は政府職員に２００６年度から導入が予定されている国家公務員ICカード等との連動も図る。

D) IPv6やそのほかの新しい技術を導入するための基盤環境としても、このセキュアVMを活用する。

別添3

各府省庁等の評価制度の例

情報セキュリティに関連する研究開発･技術開発の評価方法について

総務省

施策名	事前評価	中間評価	事後評価
プロジェクト型研究開発	1．評価項目 達成目標、研究開発概要、政策効果の把握の手段、政策評価　等 2．評価基準 各評価項目ごとに必要性、有効性、効率性などの政策評価の観点から、定性的な評価を実施 3．評価者 外部有識者 4．手続 評価案について「情報通信技術の研究開発の評価に関する会合」に諮るなどして決定	1．評価項目 研究開発の目標達成（見込み）状況、研究資金使用状況、研究開発実施計画、研究開発実施体制　総合評価　等 2．評価基準 各評価項目ごとに5段階（SABCD）評価を実施 S：非常に優れている A：優れている B：普通 C：やや劣っている D：劣っている 3．評価者 外部有識者 4．手続 受託者からヒアリングを行い評価案を作成し、「情報通信技術の研究開発の評価に関する会合」に諮るなどして決定	1．評価項目 事業の目的および政策的な位置付け、研究開発目標、研究開発マネジメント、研究成果の達成状況、研究成果の展開および波及効果　総合評価　　等 2．評価基準 各評価項目ごとに5段階（SABCD）評価を実施 S：非常に優れている A：優れている B：普通 C：やや劣っている D：劣っている 3．評価者 外部有識者 4．手続 受託者からヒアリングを行い評価案を作成し、「情報通信技術の研究開発の評価に関する会合」に諮るなどして決定

情報セキュリティに関連する研究開発･技術開発の評価方法について

文部科学省

施策名	事前評価	中間評価	事後評価
科学技術振興調整費	科学技術振興調整費審査部会が設置するワーキンググループ（以下「WG」）において、採択課題を選定する。その後、審査部会において、採択候補課題の中から採択課題を決定する。審査の実施に当たっては、科学技術振興調整費のプログラムディレクター及びプログラムオフィサーの協力を得ることとする。 審査部会は、WGにおける審査の開始に先立ち、公募要領に示された評価項目及び審査基準をもとにした「書面審査の視点」及び、プログラムの趣旨等を勘案した「採択課題選定の留意事項」を定める。WGにおいては、書面審査及びヒアリング審査の二段階審査を経て採択候補課題を選定する。	中間評価は実施過大のプログラムにおいてあらかじめ定められた時期に実施する。また、中間評価においては、当該実施課題に関し、計画の進捗度、中間的な成果の価値等についての見当を行うとともに、これらを踏まえ、次年度以降の継続の可否、研究内容の見直しの要否等についての検討を行う。 具体的な課題評価に当たっては、評価方法（評価手法、評価の観点、評価項目･基準、評価過程、評価手段等）を明確かつ具体的に設定し、被評価者に対してあらかじめ周知する。また、実施課題に係る分野又は領域に関する豊富な知見を有する外部専門家や、科学技術システム改革、研究開発マネジメント等に関する豊富な経験･知見を有する外部有識者による評価を原則とする。このため、専門家及び有識者からなる委員で構成されるワーキンググループを部会のしたに設置する、ワーキンググループは、科学技術振興調整費のプログラムオフィサーの協力（課題評価の実施に当たって必要となる情報提供等）を得て、プログラムの趣旨、目的等を踏まえ、科学的･技術的な視点や社会的･経済的な視点からの調査･検討を行い、その結果を部会に報告する。部会は、ワーキンググループの報告を踏まえ、総合的な視点で検討を行い、評価結果を取りまとめる。	事後評価は、原則として実施課題の終了年度の翌年度に実施する。ただし、プログラムごとに事後評価時期を別途定めている場合はその時期に実施する。 具体的な課題評価に当たっては、評価方法（評価手法、評価の観点、評価項目･基準、評価過程、評価手段等）を明確かつ具体的に設定し、被評価者に対してあらかじめ周知する。また、実施課題に係る分野又は領域に関する豊富な知見を有する外部専門家や、科学技術システム改革、研究開発マネジメント等に関する豊富な経験･知見を有する外部有識者による評価を原則とする。このため、専門家及び有識者からなる委員で構成されるワーキンググループを部会のしたに設置する、ワーキンググループは、科学技術振興調整費のプログラムオフィサーの協力（課題評価の実施に当たって必要となる情報提供等）を得て、プログラムの趣旨、目的等を踏まえ、科学的･技術的な視点や社会的･経済的な視点からの調査･検討を行い、その結果を部会に報告する。部会は、ワーキンググループの報告を踏まえ、総合的な視点で検討を行い、評価結果を取りまとめる。

情報セキュリティに関連する研究開発･技術開発の評価方法について

文部科学省

施策名	事前評価	中間評価	事後評価
社会技術研究開発事業(計画型)	**評価項目及び評価基準：** (研究課題について)社会問題の解決を目指す技術、自然科学と人文･社会科学との融合による技術及び市場メカニズムが作用しにくい技術に関する研究であるとともに、卓越した指導的研究者を中心に流動的な研究体制を組織してミッション達成を目指す研究であること。 (研究統括について) 当該ミッションの指揮を委ねるに相応しい優れた研究者であること。 **評価者：** システム統括がシステム運営会議の協力を得て行う。 **手続：** システム運営会議が決定する方法により、評価を行う。 (平成15年6月9日(発足時)実施)	**目的：** 研究開発の進捗状況や研究開発成果を把握し、これを基に適切な資源配分、研究開発計画の見直しを行う等により、研究開発運営の改善及び社会技術研究開発センターの支援体制の改善に資することを目的とする。 **評価項目及び評価の基準：** 研究開発の進捗状況と今後の見込、及び、研究開発成果の現状と今後の見込。なお、具体的基準については、研究開発のねらいの実現という視点から、評価者が社会技術研究開発センターと調整の上決定する。 **評価者：** 外部の有識者による常設の評価委員会が行う。 **手続：** 領域統括が指定する外部専門家により、研究開発課題又は研究開発テーマ毎に研究活動を日常的に評価し、その結果を蓄積する。評価者は、蓄積された評価結果とともに、被評価者による報告及び被評価者との意見交換等により評価を行う。 また、評価実施後、被評価者が説明を受け、意見を述べる機会を確保する。 (平成17年5月の改組後の方針に基き、平成17年11月から平成18年3月に実施)	**目的：** 研究開発の実施状況、研究開発成果、波及効果等を明らかにし、今後の研究開発成果の展開及び事業運営の改善に資することを目的とする。 **評価項目及び評価の基準：** 社会技術研究開発の目的の達成状況、及び、研究開発マネジメントの状況。 なお、具体的基準については、研究開発のねらいの実現という視点から、評価者が社会技術研究開発センターと調整の上決定する **評価者：** 外部の有識者による常設の評価委員会が行う。 **手続：** 評価委員会により、研究開発活動を日常的に評価し、その結果を蓄積する。評価者は、蓄積された評価結果とともに、被評価者による報告及び被評価者との意見交換等により評価を行う。 また、評価実施後、被評価者が説明を受け、意見を述べる機会を確保する。

情報セキュリティに関連する研究開発・技術開発の評価方法について

経済産業省

評価名	評価の概要	事前評価	中間評価	事後評価
施策評価	当省における施策は、政策－施策－事業の政策体系の一部をなすものであり、政策評価法上必要な評価単位として経済産業省政策評価基本計画にて定められるものである。	・評価者は施策の主管課（評価の責任者は、事前評価を行った主管の政策調整官（主管課が部に属する場合にあっては、主管の部長）） ・評価手続・評価方法については、可能な限り有識者等の知見を活用しつつ評価を行う。	・評価者は施策の主管課（評価の責任者は、事前評価を行った主管の政策調整官（主管課が部に属する場合にあっては、主管の部長））又は外部評価者 ・評価手続・評価方法については、主管課が評価者となる場合には、可能な限り有識者等の知見を活用しつつ評価を行う。推進課及び主管課事前評価段階で予め決定していた方法により、指標を計測する。なお、政策着手後に置いても、必要があれば指標を追加する。	・評価者は施策の主管課（評価の責任者は、事前評価を行った主管の政策調整官（主管課が部に属する場合にあっては、主管の部長））又は外部評価者 ・評価手続・評価方法については、主管課が評価者となる場合には、可能な限り有識者等の知見を活用しつつ評価を行う。推進課及び主管課事前評価段階で予め決定していた方法により、指標を計測する。なお、政策着手後に置いても、必要があれば指標を追加する。

機関評価	研究開発機関として国の資金が投入されている特殊法人、特別認可法人、公益法人、技術研究組合などの機関に対する評価を行う。なお、機関が独立行政法人の場合には経済産業省技術評価指針に基づく機関評価を行わず、独立行政法人通則法の規定に基づく評価体系の下で実施される独立行政法人評価委員会による評価に委ねることとする。なお、国費の支出を受けて研究開発を実施する民間機関については、プロジェクト評価の際等に、当該プロジェクトの研究開発体制に係る運営面に関し、国費の効果的・効率的執行を確保する観点から、必要な範囲で評価を行う。	・評価項目・評価基準は技術評価調査課が定める標準的な評価項目・評価基準又は評価者が定めるものとする。 ・評価者は外部評価者 ・評価手続・評価方法については、研究開発機関ごとの例えば、中長期計画の期間にあわせて5年程度ごとに研究開発機関の役割、位置付け等を含めて評価内容全般にわたって総合的に外部評価を行う。研究開発の実施・運営に関しては、研究開発機関によっては多様な範囲にわたる事業が存在する。これらを一律に評価を行うことは適切ではないため事業の性格に応じて、例えば、事業のまとまりごとに、短期的に（例えば毎年）評価を行うことにより研究開発機関全体の評価に資することができる。なお、必要に応じて研究開発の実施・運営面以外の点に関する評価（例えば、組織運営、会計等に関する評価）についても短期的に評価を行う。

プロジェクト評価	プロジェクトの創設及び改善、見直しを行うために実施する評価。	・技術評価調査課が定める標準的な評価項目・評価基準又は評価者が定めるものとする。全てのプロジェクトについてプロジェクト実施予定期間及び中間・事後評価の時期の妥当性に関して評価する。 ・評価者は推進課 ・評価手続・評価方法については、可能な限り有識者等の知見を活用しつつ評価を行う。	・技術評価調査課が定める標準的な評価項目・評価基準又は評価者が定めるものとする。 ・評価者は外部評価者 ・評価手続・評価方法については、事業原簿、成果報告、運営状況報告等を基に外部評価を行う。また、評点法の活用による評価の定量化を行うこととする。	・技術評価調査課が定める標準的な評価項目・評価基準又は評価者が定めるものとする。 ・評価者は外部評価者 ・評価手続・評価方法については、事業原簿、成果報告、運営状況報告等を基に外部評価を行う。また、評点法の活用による評価の定量化を行うこととする。
研究開発以外の技術に関する事業評価	経済産業省における研究開発以外の技術に関する事業（人材育成、普及促進等のための事業）についての評価を行う。原則、施策評価の中で実施する。	・評価項目・評価基準は、評価者が定めるものとする。全ての事業について事業実施予定期間及び中間・事後評価の時期の妥当性に関して評価する。 ・評価者は推進課 ・評価手続・評価方法については、可能な限り有識者等の知見を活用しつつ評価を行う。	・技術評価調査課が定める標準的な評価項目・評価基準又は評価者が定めるものとする。 ・評価者は推進課、技術評価調査課又は外部評価者 ・評価手続・評価方法については、推進課、技術評価調査課が評価者となる場合には、可能な限り有識者等の知見を活用しつつ評価を行う。	・技術評価調査課が定める標準的な評価項目・評価基準又は評価者が定めるものとする。 ・評価者は推進課、技術評価調査課又は外部評価者 ・評価手続・評価方法については、推進課、技術評価調査課が評価者となる場合には、可能な限り有識者等の知見を活用しつつ評価を行う。

競争的資金による研究課題に関する評価	内閣府（総合科学技術会議）が認めた競争的研究資金制度についての研究開発課題に関する評価を実施する。	・評価項目・評価基準は技術評価調査課が定める標準的な評価項目・評価基準又は評価者が定めるものとする。全ての事業について実施予定期間及び中間・事後評価の時期の妥当性に関して評価する。 ・評価者は有識者等。採択の際、被評価者と同じ研究開発機関に所属する等の専門家は排除する必要があるため、例えば評価事務局はあらかじめ全評価者名を公表し、被評価者に対して申請時に利害関係者の存在を併せて書面にて宣誓することを求める等の措置を講ずる。また、評価者には秘密保持を義務付ける。 ・採択に当たっては、研究目標及びエフォート（一研究員の全研究活動時間のうち当該競争的資金による研究活動に充てる時間の割合をいう。）の明記を原則求める。ただし、エフォートについては、企業等法人を対象にする場合を除く。また、被評価者 と利害関係のない有識者等によるパネルレビュー又はメールレビューによる評価を行う。採択に当たっては、他の競争的資金による研究課題等との重複が生じないようにする。評価事務局は研究課題の提案者へ不採択の結果を通知する場合には、原則とし て評価項目別に詳細な評価内容を提示するとともに、不採択となった提案者からの問い合わせに応じるための環境を整備する。	・評価項目・評価基準は技術評価調査課が定める標準的な評価項目・評価基準又は評価者が定めるものとする。 ・評価者は有識者等 ・評価手続・評価方法については、競争的資金による継続的な研究の必要性及びプロジェクトへの発展の可能性（主として技術シーズの創造を目的とする研究の場合に限る。）の有無が判断できる手法により評価を行う。	・評価項目・評価基準は技術評価調査課が定める標準的な評価項目・評価基準又は評価者が定めるものとする。 ・評価者は有識者等 ・評価手続・評価方法については、競争的資金による継続的な研究の必要性及びプロジェクトへの発展の可能性（主として技術シーズの創造を目的とする研究の場合に限る。）の有無が判断できる手法により評価を行う。

分野別評価	対象となる複数の事業を分野ごとにまとめて俯瞰的視点から事業分布の妥当性を評価するとともに、これらの事業に係る中間・事後評価結果等を踏まえ、これら事業の相対的位置付けや分野全体の今後の方向性等に関する評価を行う。	・評価項目・評価基準は技術評価調査課が定める標準的な評価項目・評価基準又は評価者が定めるものとする。 ・技術評価調査課と各分野の関係課との合同又は外部評価者 ・評価手続・評価方法については、技術評価調査課と各分野の関係課とが合同の評価者となる場合には、有識者等の知見を活用し、評価を行う。複数の事業をまとめて分野別に俯瞰的観点から整理・分析するとともに、評点法を適宜活用しつつ相対的評価を行い、各事業ごとの今後の方向性や、分野別の今後の方向性等について提言する。
追跡評価	終了して数年経った事業を対象に、その研究開発活動や研究開発成果が産業、社会に及ぼした効果について調査し、その調査結果を基に現在の視点から総合的に評価を行う。	・評価項目・評価基準は技術評価調査課が定める標準的な評価項目・評価基準又は評価者が定めるものとする。 ・評価者は外部評価者 ・評価手続・評価方法については、過去の事業原簿等の文献データ、関連部署・機関及びその他関係者等からの聞き取り調査等による情報を基にパネルレビュー又は第3者機関への委託による外部評価を行う。また、可能な限り定量的な評価に努める。

事業評価	各事業担当課が個別に実施	・事業担当課が定める	・事業担当課が定める	・事業担当課が定める

※「行政機関が行う政策の評価に関する法律」に基づき、全府省庁で行われている政策評価については、記載していない。
※総合科学技術会議によって実施されている、いわゆるＳＡＢＣ評価に関しては、記載していない。

別添4

情報セキュリティに関連する研究開発･技術開発テーマ一覧

※ 本資料については、委員会事務局にて調査･把握した内容である。
※ 把握に際しては、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、を勘案し、これらに関連すると思われる研究開発･技術開発を把握対象としている。
※ 「平成１９年度概算要求における科学技術関係施策（ＳＡＢＣ評価）」については、コンピュータシステム、ネットワーク、データベース等を含む研究開発･技術開発テーマを抽出したものである。

①ＨＷ

	テーマ	所管又は研究機関	実施時期			備考
			済み	H18	H19	
1	最先端･高性能汎用スーパーコンピュータの開発	文部科学省		○	○	平成１９年度概算要求における科学技術関係施策（ＳＡＢＣ評価）
2	将来のスーパーコンピューティングのための要素技術の研究開発プロジェクト（次世代IT基盤構築のための技術開発プロジェクト）［競争的資金］	文部科学省		○	○	
3	高機能･超低消費電力コンピューティングのためのデバイス･システム基盤技術の研究開発	文部科学省			○	
4	次世代ネットワーク基盤技術に関する研究開発	総務省 独立行政法人情報通信研究機構		○	○	
5	組込みシステム向け情報セキュリティ技術	独立行政法人産業技術総合研究所		○	○	科学技術振興調整費における研究テーマ
6	ユビキタス環境での公開鍵電子認証実現のための拡大体演算の世界最高速マイコン実装	岡山大学	○			科学研究費補助金における研究テーマ
7	テラバイトセキュリティホログラフィック光メモリディスク	神戸大学	○			
8	社会基盤を構築するためのＬＳＩ設計手法の研究	九州大学		○		
9	可視空間を制御する視覚復号型暗号を用いたセキュアな情報ディスプレイ	徳島大学	○			
10	2重ランダム偏光変調暗号化法とそのセキュリティー光メモリへの応用	神戸大学	○			
11	超高速インターネットルータに適用するスケーラブルIPルーティング制御	国立情報学研究所	○			
12	ソフトウェア無線の概念に基づくアダプティブアレーアンテナに関する研究	横浜国立大学	○			
13	冗長表現を用いた高速演算回路の自動合成に関する研究	京都大学	○			
14	スプレッドスペクトラム高度情報ワイヤレス通信モデムの研究	東北大学	○			
15	情報社会を支える新しい高性能情報処理技術	情報セキュリティ大学院大学	○			戦略的創造研究推進事業（ＣＲＥＳＴ）における研究テーマ
16	ヒューマノイドのための実時間分散情報処理	独立行政法人産業技術総合研究所	○			
17	ディペンダブルで高性能な先進ストレージシステム	東京工業大学	○			
18	全シリコン量子コンピュータの実現	慶應義塾大学	○			
19	超高速ペタバイト情報ストレージ	豊橋技術科学大学	○			
20	超低電力化技術によるディペンダブルメガスケールコンピューティング	豊橋技術科学大学	○			
21	多相的分子インタラクションに基づく大容量メモリの構築	東京大学	○			
			15	5	5	

② ＯＳ

	テーマ	所管又は研究機関	実施時期			備考
			済み	H18	H19	
1	最先端･高性能汎用スーパーコンピュータの開発利用	文部科学省		○	○	平成１９年度概算要求における科学技術関係施策（ＳＡＢＣ評価）
2	セキュア･プラットフォームプロジェクト	経済産業省			○	
3	組込みシステム向け情報セキュリティ技術	独立行政法人産業技術総合研究所		○	○	科学技術振興調整費における研究テーマ
4	高セキュリティ機能を実現する次世代ＯＳ環境の開発	筑波大学		○	○	
5	複数のＯＳの連携と上位層機能の取り込みによるＯＳのセキュリティ基盤強化方式	情報セキュリティ大学院大学		○		科学研究費補助金における研究テーマ
6	実用化を目指した組込みシステム用ディペンダブル･オペレーティングシステム	ソニー株式会社		○		戦略的創造研究推進事業（ＣＲＥＳＴ）における研究テーマ
7	高信頼組込シングルシステムイメージＯＳ	東京大学		○		
8	マイクロユビキタスノード用高信頼ＯＳ	慶應義塾大学		○		
9	超高機能情報家電のためのオペレーティングシステム	早稲田大学		○		
10	高信頼システムソフトウェア構築技術に関する研究	東京大学		○		
11	超低電力化技術によるディペンダブルメガスケールコンピューティング	豊橋技術科学大学	○			
12	日常生活を拡張する着用型情報パートナーの開発	奈良先端科学技術大学院大学	○			
			2	9	4	

③ 認証

	テーマ	所管又は研究機関	実施時期			備考
			済み	H18	H19	
1	ＰＫＩの安全性向上化技術の研究	筑波大学	○			科学研究費補助金における研究テーマ
2	移動通信システムを対象としたバイオメトリック認証方式に関する研究	北九州市立大学	○			
3	ユーザがパスワードを覚える必要のない行動履歴ベース個人認証システムの実装	静岡大学	○			
4	ＰＫＩの安全性と柔軟性に関する研究	筑波大学	○			
5	Ｉｎｔｅｒ　ＰＫＩの研究	東邦大学	○			
6	利用者の過失に対する耐性を備えた個人認証法	奈良先端科学技術大学院大学	○			
7	人と物品を含む大規模システムにおける簡便で安全な認証方式の研究	東京大学	○			
8	高度ネットワーク認証基盤技術に関する研究開発	総務省		○		その他
9	モバイルセキュリティ基盤技術の研究開発	独立行政法人情報通信研究機構		○		
10	モバイル端末におけるセキュリティ保護技術に関する研究開発	独立行政法人情報通信研究機構		○		
11	ネットワーク認証型コンテンツアクセス制御技術の研究開発	独立行政法人情報通信研究機構		○	○	
12	ＩＣカード等における認証のための高度な暗号技術に関する研究開発	独立行政法人情報通信研究機構	○	○		
13	大容量データの安全な流通･保存技術に関する研究開発	独立行政法人情報通信研究機構	○	○	○	
14	異なるCA間の認証ローミング技術に関する研究開発	独立行政法人情報通信研究機構	○	○		
15	次世代型電子認証基盤の整備	経済産業省	○	○		
16	アクセスグラフに基づくボットネット検出技術の研究開発	経済産業省	○	○		
17	情報えいに堅牢な認証･データ管理方式とそのソフトウェアによる安全な実装･検証手法に関する研究開発	経済産業省	○	○	○	
18	ユビキタスネットワーク向けセキュアアセットコントロール技術の研究開発	経済産業省	○	○	○	
19	強制的アクセス制御に基づくWebサーバーに関する調査･設計	独立行政法人情報処理推進機構	○			
			15	11	4	

④ 暗号

	テーマ	所管又は研究機関	実施時期			備考
			済み	H18	H19	
1	情報セキュリティのための離散数学研究	お茶の水女子大学		○		科学研究費補助金における研究テーマ
2	分散ＤＮＡ鍵による情報セキュリティ方式の開発	北海道大学		○		
3	不正行為に強い耐性を持つ電子透かし情報符号化法に関する研究	独立行政法人産業技術総合研究所		○		
4	安全性と効率性を両立した木構造鍵管理方式に関する研究	奈良先端科学技術大学院大学	○			
5	暗号技術に基づく関数を用いたプログラムに対する情報フロー解析法の開発	大阪大学	○			
6	実用的かつ証明可能安全なブロック暗号利用モードに関する研究	茨城大学	○			
7	最小ベクトル問題と格子アルゴリズムの公開鍵暗号への応用に関する研究	電気通信大学		○		
8	暗号鍵紛失対策システムの研究	筑波大学		○		
9	暗号システムに対する実装攻撃の摘要と限界に関する計算論的研究	九州大学		○		
10	暗号解析手法の計算量理論による改良とそれに基づく暗号方式	東京工業大学		○		
11	暗号認証システムにおける双対性原理の確立と応用	九州大学	○			
12	量子アルゴリズムに対する公開鍵暗号及び秘密鍵暗号の安全性評価	電気通信大学	○			
13	量子鍵配送方式の安全性および鍵共有に関する通信路容量の解析	国立情報学研究所	○			
14	著作権保護のための計算機ホログラフィにおける電子透かしの新しい研究	明治大学	○			
15	最適性をもつ視覚復号型秘密分散法の代数的な構成法に関する研究	筑波大学	○			
16	電子透かしの安全性評価基準に関する研究	東北大学	○			
17	デコンボリューション技法による電子透かしシステムの改良	九州産業大学	○			
18	アニメーション画像に適した電子透かしの開発	京都工芸繊維大学	○			
19	暗号アルゴリズムの実装攻撃に対する耐性評価に関する体系的研究	九州大学	○			
20	公開鍵暗号と電子署名の証明可能安全性における双対性原理･変換不変量の解析と応用	九州大学	○			
21	代数曲線のセコビ多様体に関するアルゴリズムとその公開鍵暗号への応用についての研究	電気通信大学	○			
22	一方向ハッシュ関数の構成と応用に関する研究	京都大学	○			
23	代数的暗号解読アルゴリズムに対して証明可能な安全性を実現する暗号設計法	独立行政法人情報通信研究機構	○			
24	世界最高速かつ最も安全な楕円曲線暗号システムの構築	岡山大学	○			
25	電子透かしにおける検出誤り確率推定法の開発	大阪大学	○			
26	自然画像の視覚的暗号化手法	東京大学	○			
27	3次元モデルの形状を対象とする類似検索と電子透かしの技術	山梨大学	○			
28	高階差分･補間攻撃等の解析的攻撃に対する共通鍵暗号の強度評価ツールの開発	東京理科大学	○			
29	秘密鍵系列の一致のための誤り訂正法に関する研究	玉川大学	○			
30	超大規模暗号通信ネットワーク用新鍵管理システムに関する研究	神戸大学	○			
31	組合せ的デザイン理論を用いた光直交符号の構成に関する研究	筑波大学	○			
32	現実的な装置を用いた場合の量子暗号プロトコルの安全性評価と量子情報理論の定式化	東京大学	○			

④ 暗号

	テーマ	所管又は研究機関	実施時期			備考
			済み	H18	H19	
33	量子アルゴリズムに対する共通鍵暗号の安全性評価	電気通信大学	○			科学研究費補助金における研究テーマ
34	無証拠性を満たす暗号プロトコルの設計とインターネット投票システムへの応用	九州大学	○			
35	素因数分解および離散対数問題の難しさに頼らない公開鍵暗号方式に関する研究	東京大学	○			
36	2重ランダム偏光変調暗号化法とそのセキュリティー光メモリへの応用	神戸大学	○			
37	デジタルカオス同期に関する研究	明治大学	○			
38	電子透かし技術の評価とその支援システムの開発	九州産業大学	○			
39	情報理論的立場からの情報セキュリティおよび乱数生成の研究	九州大学	○			
40	代数曲線における離散対数問題と情報セキュリティ	大阪大学	○			
41	公開鍵暗号と電子署名の証明可能安全性における双対性原理の確立と応用	九州大学	○			
42	秘密関数分散法に対する情報理論的性能評価と応用に関する研究	東京大学	○			
43	暗号理論。特に代数曲線暗号における安全性の考察	大阪大学	○			
44	書換えモデルを用いた暗号プロトコルの形成的設計法	和歌山大学	○			
45	h誤り線形複雑度の計算方法とその応用に関する研究	八代工業高等専門学校	○			
46	3次元モデルを対象とした電子透かし･検索･圧縮技術に関する研究	山梨大学	○			
47	標本化格子の位相変調に基づく電子透かし手法の開発と静上画像への応用に関する研究	広島国際学院大学	○			
48	整数論の難かしい問題に安全性の根拠を置く公開鍵暗号の開発とその強度評価	山形大学	○			
49	偏微分法程式とトモグラフィの函数解析的及び数値的研究	お茶の水女子大学	○			
50	電子透かし技術を応用した画像情報管理システムの開発	九州大学	○			
51	分散暗号理論の研究と電子マネー･電子オークションシステム設計への応用	九州大学	○			
52	電子透かしアルゴリズムの安全性評価手法とバイオメトリクスへの応用に関する研究	早稲田大学	○			
53	情報量的に安全なIDベース暗号インフラストラクチュアの構築および運営に関する研究	東京大学	○			
54	検証者限定署名の楕円曲線暗号による実現と高速化に関する研究	北九州市立大学	○			
55	追跡可能な放送型暗号系に関する研究	東京工業大学	○			
56	動画像及び文書への電子透かしに関する研究	九州大学	○			
57	電子透かし技術を用いた3次元形状モデルの著作権保護に関する研究	北海道大学	○			
58	超楕円曲線を用いた公開鍵暗号システムの開発研究	九州大学	○			
59	マルチメディア情報における電子透かし技術に関する基礎的研究	京都工芸繊維大学	○			
60	視覚特性を利用した画像情報の暗号化技術に関する研究	神戸大学	○			
61	多元情報通信システムの符号化に関する理論的検討とその応用	九州大学	○			
62	移動通信に適した秘密鍵暗号方式と認証付鍵共有に関する研究	京都大学	○			

④ 暗号

	テーマ	所管又は研究機関	実施時期			備考
			済み	H18	H19	
63	正標数の数論の暗号理論への応用	埼玉大学	○			科学研究費補助金における研究テーマ
64	Reed－Solomon符号の構造解析と高速復号法の開発に関する研究	徳島大学	○			
65	画像やオーディオデータを利用したSteganographyの研究	九州工業大学	○			
66	マルコフノイズ系の解に対する特異摂動法を用いた漸近解析とその応用	神奈川大学	○			
67	計算困難な問題を利用した公開鍵暗号アルゴリズムの設計とその解析	九州大学	○			
68	多値画像に対するデジタル透かし技法の開発	奈良先端科学技術大学院大学	○			
69	多値画像に対するデジタル透かし技法の開発	奈良先端科学技術大学院大学	○			
70	カラー画像を用いた深層暗号方式の提案と評価	神戸大学	○			
71	マルチメディア信号に対するディジタル･ウォ･ターマークの研究	九州大学	○			
72	楕円曲線に基づく安全性の高い暗号システムに関する研究	中央大学	○			
73	カオス2値系列に基づくストリーム暗号システム	九州大学	○			
74	暗号系とその評価に関する研究	北陸先端科学技術大学	○			
75	知識の対話型証明に関する研究と暗号認証システム効率改善への応用	九州大学	○			
76	正標数数論的空間における調和解析の研究	埼玉大学	○			
77	ゼータ関数の極の研究とその応用	埼玉大学	○			
78	暗号を用いたプロトコルの安全性検証法に関する研究	奈良先端科学技術大学院大学	○			
79	離散対数問題に基づく暗号系の帰着関係の研究	東北大学	○			
80	ＤＣＴ符号化に適した画像暗号化に関する研究	東京工業大学	○			
81	複数の情報源出力を伴うシャノン暗号システムに対する符号化定理に関する研究	東京大学	○			
82	ID情報に基づく暗号システムの研究	神戸大学	○			
83	Key Predistribution Systemの実現と応用に関する基礎研究	横浜国立大学	○			
84	計算機代数の諸算法	京都大学	○			
85	Obscure表現に基づく高速暗号化及びディジタル署名方式の理論的･数値的研究	横浜国立大学	○			
86	誰でも使用、改良、評価できる安全な電子透かし技術の研究開発	独立行政法人情報通信研究機構		○		その他
87	第3世代暗号技術の研究開発	独立行政法人情報通信研究機構		○		
88	暗号の技術的評価に関する研究開発	独立行政法人情報通信研究機構		○		
89	ユビキタス暗号技術に関する研究開発	独立行政法人情報通信研究機構		○	○	
90	ユビキタスネットワークにおける環境に応じた暗号プロトコルの自動生成･カスタマイズ技術に関する研究開発	独立行政法人情報通信研究機構		○	○	
91	ICカード等における認証のための高度な暗号技術に関する研究開発	独立行政法人情報通信研究機構		○		
92	次世代ハッシュ関数に関する研究開発	独立行政法人情報通信研究機構			○	
93	適切な暗号等を選択可能とするための新しい暗号等技術の評価手法に関する研究開発	独立行政法人情報通信研究機構			○	
94	安全な暗号技術を利用し続けるための暗号利用フレームワークに関する研究開発	独立行政法人情報通信研究機構			○	
			78	13	5	

⑤ ﾌﾟﾗｲﾊﾞｼｰ保護

	テーマ	所管又は研究機関	実施時期			備考
			済み	H18	H19	
1	インターネットフィッシング詐欺に対する情報セキュリティ対策技術の研究	九州大学		○		科学研究費補助金における研究テーマ
2	内部告発を支援する情報セキュリティ技術に関する研究	神戸大学	○			
3	プライバシー増幅に対する情報理論的性能評価とその改良に関する研究	東京大学	○			
4	ＪＰＧ２０００－ＢＰＣＳステガノグラフィを用いた大容量秘匿通信	九州工業大学	○			
5	零知識証明を用いた分散認証システムの研究開発	東京工業大学	○			
6	利用者のプライバシーを考慮したネットワーク･アクセス制御方式の開発研究	東京工科大学	○			
7	量子計算と古典通信路を用いた電子署名方式	東京工業大学	○			
8	ステガノグラフィ技術を利用した匿名秘匿Ｅ－メールシステムの研究	九州工業大学	○			
9	レーザカオスを用いた高秘匿光通信方式の開発	拓殖大学	○			
10	パーソナルセキュリティモジュールの研究	筑波大学	○			
11	デジタル署名を委任する方法についての研究	北陸先端科学技術大学院大学	○			
12	Ｏｂｓｃｕｒｅ表現に基づく高速暗号化及びディジタル署名方式の理論的･数値的研究	横浜国立大学	○			
			11	1	0	

⑥ 機器セキュリティ

	テーマ	所管又は研究機関	実施時期			備考
			済み	H18	H19	
1	オープンソースソフトウェア活用基盤整備事業	経済産業省 独立行政法人情報処理推進機構		○	○	平成19年度概算要求における科学技術関係施策（SABC評価）
2	コンピュータセキュリティ早期警戒態勢の整備事業	経済産業省 独立行政法人情報処理推進機構		○	○	
3	セキュリティ情報の分析と共有システムの開発	慶應義塾大学		○		科学技術振興調整費における研究テーマ
4	ユーザビリティに優れたセキュリティ脆弱性診断システム	岩手県立大学	○			科学研究費補助金における研究テーマ
5	生物指向型アプローチによるコンピュータウイルスの伝播防止システムに関する研究	神奈川工科大学	○			
6	多重パーティ計算の安全性、故障耐性、効率に関する研究	群馬大学	○			
7	エンタープライズセキュリティのためのシステム基盤ソフトウェアの研究	東京理科大学	○			
8	真に解きたい問題を隠しつつ計算機の力を利用する実用的な依頼計算方式の研究	東京大学	○			
9	情報セキュリティに関する基本プロトコル･アルゴリズムの理論的研究	横浜国立大学	○			
10	フルーエンシ情報理論にもとづくマルチメディアコンテンツ記述形式	筑波大学	○			戦略的創造研究推進事業（CREST）における研究テーマ
			7	3	2	

⑦ ネットワーク技術

	テーマ	所管又は研究機関	実施時期			備考
			済み	H18	H19	
1	次世代ネットワーク基盤技術に関する研究開発	総務省 独立行政法人情報通信研究機構		○	○	平成19年度概算要求における科学技術関係施策（SABC評価）
2	ダイナミックネットワーク技術の研究開発	総務省 独立行政法人情報通信研究機構			○	
3	ユビキタスネットワーク（何でもどこでもネットワーク）技術の研究開発	総務省		○	○	
4	電子タグの高度利活用技術に関する研究開発	総務省		○	○	
5	情報家電の高度利活用技術の研究開発	総務省		○	○	
6	スパムメールやフィッシング等サイバー攻撃の停止に向けた試行	総務省		○	○	
7	情報漏えい対策技術の研究開発	総務省			○	
8	電気通信サービスに関する情報信憑性検証技術等に関する研究開発	総務省 独立行政法人情報通信研究機構			○	
9	セキュリティ情報の分析と共有システムの開発	慶應義塾大学		○		科学技術振興調整費における研究テーマ
10	多端子情報理論的立場からの情報通信網の効率、信頼性および安全性解析	九州大学		○		科学研究費補助金における研究テーマ
11	量子情報のセキュアな伝送のための量子誤り訂正符号の構成法	愛知県立大学	○			
12	ネットワーク上における戸口通信に関する研究	岩手県立大学	○			
13	キャンパスネットワークの情報コンテンツ保護と著作権制御に関する研究	神奈川大学	○			
14	ソフトウェア無線の情報通信ネットワークへの拡張に関する研究	横浜国立大学	○			
15	マルチメディア移動通信に適した符号分割多元接続方式に関する研究	京都大学	○			
16	分散ネットワークにおける情報通信の安全性に関する研究	群馬大学	○			
17	マルチメディア通信における通信品質設計法の研究	富山県立大学	○			
18	スペクトル拡散通信方式による耐干渉性と秘話性の高いディジタル放送の研究	横浜国立大学	○			
19	多次元ディジタル信号処理に基づく音声と画像の周波数スクランブルに関する研究	東北大学	○			
20	情報化社会に対応する情報通信網の高度化・高信頼化に関する総合研究	早稲田大学	○			
21	量子情報処理ネットワーク要素技術	北海道大学	○			戦略的創造研究推進事業（CREST）における研究テーマ
22	超低電力化技術によるディペンダブルメガスケールコンピューティング	豊橋技術科学大学	○			

⑦ ネットワーク技術

	テーマ	所管又は研究機関	実施時期			備考
			済み	H18	H19	
23	広域モニタシステムに関する基盤技術の研究開発	独立行政法人情報通信研究機構		○		その他
24	ネットワーク環境の脆弱性レベルをリアルタイムで定量評価し、情報流通をセキュアに運用するための意思決定支援システムの研究開発	独立行政法人情報通信研究機構		○		
25	インターネット中枢機能のセキュリティ強化に関する研究開発	独立行政法人情報通信研究機構		○		
26	IPパケットトレースバック技術に関する研究開発	独立行政法人情報通信研究機構		○	○	
			12	11	9	

⑧ システム構築技術

	テーマ	所管又は研究機関	実施時期			備考
			済み	H18	H19	
1	量子情報セキュリティ技術を取り入れた情報基盤設計のための基礎研究	独立行政法人産業技術総合研究所		○		科学研究費補助金における研究テーマ
2	計算機ホログラムを用いた新しい情報セキュリティシステムの構築	明治大学		○		
3	「社会基盤としてのセキュアコンピューティングの実意現方式の研究」の推進と評価	東京大学	○			
4	ディジタルコンテンツの知的財産権保護を可能にするセキュアファイルシステムの構築	静岡大学	○			
5	分散システムにおける通信の耐故障性と機密性に関する研究	群馬大学	○			
6	領域予測のための機械発見システムの研究	九州大学	○			
7	適応カオス制御を用いた情報セキュリティシステムに関する研究	慶應義塾大学	○			
8	情報システムにおける情報自己保護機能の研究	北陸先端科学技術大学	○			
9	高次コミュニケーションの高信頼化設計に関する研究	東京工業大学	○			
10	省電力高信頼組込み並列プラットフォーム	筑波大学		○		戦略的創造研究推進事業（ＣＲＥＳＴ）における研究テーマ
11	情報社会を支える新しい高性能情報処理技術	情報セキュリティ大学院大学	○			
12	自律連合型基盤システムの構築	筑波大学	○			
13	ディペンダブル情報処理基盤	東京大学	○			
14	超低電力化技術によるディペンダブルメガスケールコンピューティング	豊橋技術科学大学	○			
			11	3	0	

⑨ 社会システム

	テーマ	所管又は研究機関	実施時期			備考
			済み	H18	H19	
1	先導的ITスペシャリスト育成推進プログラム	文部科学省		○	○	平成19年度概算要求における科学技術関係施策（SABC評価）
2	情報家電センサー・ヒューマンインターフェース活用技術の開発	経済産業省		○	○	
3	自律移動支援プロジェクトの推進経費	国土交通省		○	○	
4	戦略的情報通信研究開発推進制度	総務省		○	○	
5	民間基盤技術研究促進制度［競争的資金］	総務省 独立行政法人情報通信研究機構		○	○	
6	バイオインフォマテックス推進センター	文部科学省 独立行政法人科学技術振興機構		○	○	
7	農林水産生物ゲノム情報統合データベースの構築	農林水産省		○	○	
8	創薬基盤推進研究（疾患関連たんぱく質解析研究）	厚生労働省		○	○	
9	医療安全・医療技術評価総合研究［競争的資金］	厚生労働省		○	○	
10	健康危機管理・テロリズム対策システム研究	厚生労働省		○	○	
11	データ統合・解析システム	文部科学省		○	○	
12	一塩基多型（SNPs）分析による生体資料からの異同識別検査法の開発	警察庁			○	
13	高度な交通事故分析技術の開発	警察庁			○	
14	首都直下地震防災・減災特別プロジェクトのうち、高感度地震計を用いた地殻活動の現状把握、既存地震計の共有・活用システム及び多機能リアルタイム強震計の開発を除いた部分	文部科学省			○	
15	地震・津波観測監視システム（海底ネットワークシステムの開発）	文部科学省		○		
16	全天候・高密度運航技術	文部科学省 独立行政法人宇宙航空研究開発機構		○	○	
17	電子情報発信・流通促進	文部科学省 独立行政法人科学技術振興機構		○		
18	首都直下地震防災・減災特別プロジェクト	文部科学省			○	その他
19	業務プロセス品質向上（業務プロセス効率と情報セキュリティレベル向上）に関する研究	専修大学		○		科学研究費補助金における研究テーマ
20	サステナブル電子社会を支える情報セキュリティ基盤とソーシャルクリプトに関する研究	東京大学		○		
21	研究デザインデータベース構築及び個人情報セキュリティシステムの開発・臨床応用	東京大学		○		
22	情報セキュリティ教育に関する実践的研究：情報リテラシー教育の新たな視点	山口大学		○		
23	個人情報保護の個別法の研究	東京大学		○		
24	電子商取引の制度的プラットフォーム構築に関する研究	国立情報学研究所	○			
25	情報セキュリティ基盤に起因するリスクを管理するための情報経済工学的研究	東京大学	○			
26	大学看護学教育における情報リテラシー教育方法の開発と評価	静岡県立大学	○			
27	サイバー攻撃の国際的規制に関する研究	稚内北星学園大学	○			
28	サイバー社会における情報倫理教育カリキュラムの検討	大阪学院大学	○			
29	地域学術コンソーシアムにおけるe－Learning地域ハブに関する研究	名古屋大学	○			
30	NPO諸組織を連携する知識型情報システムの構築とナレッジマネジメントに関する研究	石巻専修大学	○			

⑨ 社会システム

	テーマ	所管又は研究機関	実施時期			備考
			済み	H18	H19	
31	将来にわたる確実な安全性を保証可能な電子決済方式の実現方法に関する研究	東京大学	○			科学研究費補助金における研究テーマ
32	ボーダレス化時代における法システムの再構築	東京大学	○			
33	HTML形式による画像診断ティーチングファイルの改良	徳島大学	○			
34	京都府におけるネットワーキング型の地域振興政策に関する実証的研究	立命館大学	○			
35	利用者の意志を確実に伝える情報セキュリティ基盤技術の研究	横浜国立大学	○			
36	グローバルな規模で進展する情報経済と新たな社会制度デザインに関する研究	東京大学	○			
37	ITの深化の基盤を拓く情報学研究	慶應義塾大学	○			
38	広域分散環境における電子カルテの安全性に関する研究	神戸大学	○			
39	情報倫理教育のためのWebベース教材の開発と活用	関西学院大学	○			
40	汚染データ配信方式によるディジタルコンテンツの知的財産権保護	静岡大学	○			
41	インターネットの教育利用における発信者側でのアクセス制御に関する研究	東京工業大学	○			
42	養護教諭の連携と自己理解リフレッシュをはかるネットワークシステムの開発研究	東京理科大学	○			
43	薬学情報教育体系化と医療・薬学情報処理システム開発	金沢大学	○			
44	マルチメディア情報の著作権制御に関する研究	神奈川大学	○			
45	情報の概念の知識論および行為論における役割の理論的、応用的考察	千葉大学	○			
46	インターネットで共有する画像診断情報システムの構築	九州大学	○			
47	不均一誤り保護と依頼計算を応用したディジタル著作権管理に関する研究	東京大学	○			
48	数式処理システムを利用した創造的理工系数学教育の研究	高知工業高等専門学校	○			
49	ユーザレベルでの保護モデルを持つ広域ネットワーク利用の保健室用システムの開発研究	芦屋大学	○			
50	マルチメディアの進展に対応した著作権法制の研究	専修大学	○			
51	情報セキュリティと電子貨幣	東京電機大学	○			
52	箱庭の操作過程をデータベースとして持つマルチメディア相談室用システムの開発研究	芦屋大学	○			
53	個人情報の保護が重視される学校相談事例データベースシステムの開発研究	芦屋大学	○			
54	金融ネットワークにおける情報セキュリティに関する研究	東京工業大学	○			
55	2次元メルケスプトラムを用いる雑音下の単語音声認識	名古屋工業大学	○			
56	高度メディア社会の生活情報技術	独立行政法人情報通信研究機構	○			戦略的創造研究推進事業（CREST）における研究テーマ
57	セマンティック・タイポロジーによる言語の等価変換と生成技術	鳥取大学	○			
58	デジタルヒューマン基盤技術	独立行政法人産業技術総合研究所	○			
59	連想に基づく情報空間との対話技術	国立情報学研究所	○			
60	テレイグジスタンスを用いる相互コミュニケーションシステム	東京大学	○			
61	情報のモビリティを高めるための基盤技術	東京大学	○			

⑨ 社会システム

	テーマ	所管又は研究機関	実施時期			備考
			済み	H18	H19	
62	人間中心の知的情報アクセス技術	独立行政法人産業技術総合研究所	○			戦略的創造研究推進事業（CREST）における研究テーマ
63	文化遺産の高度メディアコンテンツ化のための自動化手法	東京大学	○			
64	デジタルシティのユニバーサルデザイン	京都大学	○			
65	表現豊かな発話音声のコンピュータ処理システム（EXPRESSIVE SPEECH PROCESSING）	株式会社国際電気通信基礎技術研究所	○			
66	高度メディア社会のための協調的学習支援システム	中京大学	○			
67	心が通う身体的コミュニケーションシステム Ｅ－COSMIC	岡山県立大学	○			
			44	19	16	

⑩ 運用管理

	テーマ	所管又は研究機関	実施時期			備考
			済み	H18	H19	
1	革新的シュミレーションソフトウェアの研究開発プロジェクト[競争的資金]	文部科学省		○	○	平成19年度概算要求における科学技術関係施策（SABC評価）
2	産学連携ソフトウェア工学の実践の整備のうち ①産学連携ソフトウェア工学の実践事業	経済産業省		○	○	
3	産学連携ソフトウェア工学の実践の整備のうち ②産学連携ソフトウェア工学の実践拠点	経済産業省		○	○	
4	ソフトウェア構築状況の可視化技術の開発普及	文部科学省			○	
5	企業・個人の情報セキュリティ対策事業	経済産業省 独立行政法人情報処理推進機構		○	○	
6	情報大航海プロジェクト	経済産業省			○	
7	革新的実行原理に基づく超高性能データベース基盤ソフトウェアの開発	文部科学省			○	
8	統合データベースプロジェクト	文部科学省		○	○	
9	動的配布モジュールによるコンテンツアクセス制御に関する研究	近畿大学	○			科学研究費補助金における研究テーマ
10	RFID情報システムの基盤となるデータ管理技術の研究	九州大学	○			
11	項書換え系を対象としたモデル検査手法に関する研究	奈良先端科学技術大学院大学	○			
12	ソフトウェア難読化技術の安全性に関する理論的解析と統一的性能指標の確立	九州大学	○			
13	自治体の電子化レベルに関する評価尺度の構築とその適用	摂南大学	○			
14	コンテンツ配信管理における複雑度と安全性のトレードオフ及び安全性保証に関する研究	大阪大学	○			
15	コンテンツ配信管理システムに関する統合的セキュリティ技術の研究	大阪大学	○			
16	データベースへの推論攻撃に対する安全性指標の提案とそれに基づく安全性判定法の開発	大阪大学	○			
17	アクセス行列モデルにおける安全問題の研究	北陸先端科学技術大学院大学	○			
18	解析情報に基づくソフトウェアシステムのモデル表示に関する研究	大阪大学	○			
19	オブジェクト指向データベースにおける問い合わせの推論攻撃に対する安全性判定法の開発	奈良先端科学技術大学院大学	○			
20	タブレットの時系列情報を利用した実時間筆者照合システム	東京理科大学	○			
21	暗号を用いたプロトコルにおけるデータの偽造不可能性検証システムの開発	大阪大学	○			
22	発見的探索アルゴリズムの理論と実働化	九州大学	○			
23	個票データの階層的秘匿を可能とするデータベースシステムの開発	信州大学	○			
24	プログラム論証システムの信頼性と安全性に関する研究	九州大学	○			
25	推論を利用した暗号プロトコルの自動検証に関する研究	東京工業大学	○			
26	データベースへのアクセス制御の設計法に関する体系的研究	中央大学	○			
27	自律協調型データベース処理のシステム構成法とアクセスのセキュリティに関する研究	早稲田大学	○			
28	情報ネットワークのセキュリティ強度評価法の研究	北陸先端科学技術大学院大学	○			
29	公共データベースセンタにおける機密文書の管理とそのアクセス方式に関する研究	早稲田大学	○			

⑩ 運用管理

テーマ		所管又は研究機関	実施時期			備考
			済み	H18	H19	
30	検証における記述量爆発問題の構造変換による解決	独立行政法人産業技術総合研究所	○			戦略的創造研究推進事業（ＣＲＥＳＴ）における研究テーマ
31	日常生活を拡張する着用型情報パートナーの開発	奈良先端科学技術大学院大学	○			
			23	5	8	

別添5

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２００７

本紙では、報告書2005においてとりまとめられた「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」について、見直しを行い、項目の追加及び更新を加えて「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2007」としたものである。

以下に、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。

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[1]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、

[1] 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[2]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[3]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。

○認証基盤のガバナンスの確立と高度化

PKIに代表される高度な認証技術は1990年代から開発され、その社会展開が1990年代後半から行われている。この社会展開プロセスでは、関係する法整備、GPKIや公的認証基盤等のシステム開発が行われた。しかし、依然として認証基盤の利用は広がっていない。また、近年認証基盤の構造と運用に関して、様々な研究成果が生まれてきているが、既存の認証基盤への組込み

2 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享受できるようにするための次世代インフラ。

3 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。

は進展していない。このようなことから、今一度認証基盤のあり方と必要な技術開発、運用環境の見直し、国内制度と国際的な動向のすり合わせ、法律を含む制度の点検が必要になってきている。このような複合的な要素（技術開発、制度点検と整備、運用体制の整備とサービス提供）についての取組みを総合すれば、認証基盤のガバナンスの確立と高度化を達成できると考える。このような取組みを早期に開始し、その成果を持続的に電子政府や、政府が行うIT政策に展開する積極的な実施が必須である。

また、生体計測に基づく認証技術においても、迅速な社会展開を促進するための多面的な方策の立案と実施を行うことが必要となっている。生体計測に基づく認証技術は、我が国が国際的にも優位性をもった技術であり、その社会展開方策立案・実施は、今後の国際的な技術展開においても有用なものとなると期待される。また、生体計測に基づく認証方式は、従来のパスワードやトークンを活用した認証方式よりも、より高い安全性を提供するものであり、その積極的な活用を実現することは、安全・安心な高度情報通信ネットワーク社会を作り出す上でも大きく寄与することはいうまでもない。

○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、研究領域の相互連関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[4]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[5]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。

○　情報通信構成要素の検査技術の高度化

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、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が重要である。

(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

---

4 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。

5 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。

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[6]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。

○情報の長期間保存技術に関する研究

ディ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

6 〔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。

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。

2. 情報セキュリティ技術を支える環境整備

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。

(7)情報通信基盤に対する依存性についての広範な検討

我が国の経済活動等の諸活動は、明らかに国内外の情報通信基盤に依存して展開していることはいうまでもない。しかし、どのような依存関係にあり、環境変化(事故、事件、災害等)が発生した場合の対応はどのようにあるべきかを検討することが必要である。これは、別の言い方をすれば、我が国の各種基盤が、規模の大小に関わらず環境変化が発生してもサービス提供を持続可能にするためには、どうあるべきかを明らかにする研究活動である。このためには、技術の役割、政策のあり方、社会投資の考え方なども検討対象として、多種多様な始点からの検討が必要となる。この研究は、情報セキュリティのみと関係するものではなく、広く重要インフラ防護、防災、危機管理に関係する。このために、領域横断的な研究活動の構成と加速が必要である。

別添6

調達に向けたガイドラインの検討及び留意点

本紙では、技術戦略専門委員会において議論された意見をもとに、調達を通して成果を活用するガイドライン策定に関しての試案を「調達に向けたガイドラインの検討及び留意点」として提示するものである。

(1) 調達に向けたガイドラインの検討

「高セキュリティ機能を実現する次世代 OS 環境の開発」は、政府機関（内閣官房情報セキュリティセンター等）における実運用を前提としており、実際に政府機関での利用に至るまでのプロセスを以下に示す。

A) 開発したセキュアVMは順次内閣官房情報セキュリティセンターにより実証実験を実施し、政府組織内での運用性改善に向け、その内容を開発側にフィードバックする。

B) 振興調整費による研究開発成果は知財権等を考慮しつつ、基本的にオープンソースソフトウェアとして公開し、産業界による製品化開発に提供する。

C) 政府組織内の連携による検討では、内閣官房情報セキュリティセンターを中心とした関連組織により、政府組織内への本格的な導入に向けた具体的な方針を検討し、ガイドラインを策定する。

D) ガイドラインに基づいた政府調達仕様を策定後、速やかに公開し、産業界による製品化開発を促進する。

E) 製品化開発では実利用に対応可能な周辺部分の整備を行うとともに、各種動作テストを実施する。また、実利用で必須となるマニュアル類を含めたドキュメント類を作成する。

F) 政府組織内への本格導入は産業界による製品化開発の動向を見極めながら2009年度以降に予定される各府省での調達時に実施する。

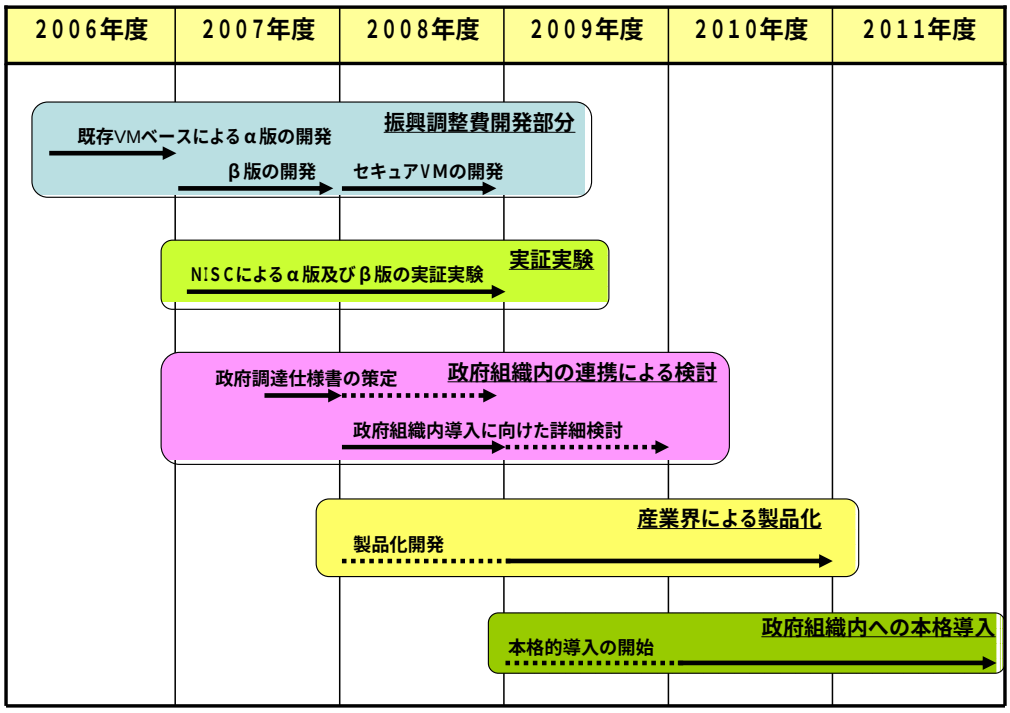


図14　セキュアVM開発と政府組織内への運用の行程（イメージ）

（2） 留意点

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。

A) 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。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。

B) 成果利用の可能性を評価する枠組みも必要。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。

C) 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。