資料７－２

技術戦略専門委員会報告書 2008

2009/4/16

情報セキュリティ政策会議

技術戦略専門委員会

目次

別紙

情報セキュリティ政策会議　技術戦略専門委員会　委員名簿

グランドチャレンジ検討ワーキンググループ委員名簿

はじめに

２００５年７月に情報セキュリティ政策会議（議長：内閣官房長官）の下に設置された技術戦略専門委員会では、我が国における情報セキュリティに係る研究開発及び技術開発並びにそれらの成果利用の戦略に係る事項について調査検討を行っている。

その活動の第一歩として、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、および重点化すべき領域などを検討し、２００５年１１月に「技術戦略専門委員会報告書」をとりまとめた。そこでの検討内容は、２００６年２月の情報セキュリティ政策会議の第４回会合で決定された、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」の、主に技術戦略の推進に関する重点施策に反映されている。加えて、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、報告書で提示した様々な方策が取り入れられるとともに、情報セキュリティが「戦略重点科学技術」の一つとして位置づけられた。

その後、関係府省庁の各主体によって、第１次基本計画に沿った、様々な取組みが進められ、情報セキュリティ技術開発の重点化と環境整備に向けた事例も見られるようになるなど、対策は着実に進展してきた。本委員会でも、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、最新の動向を反映させたフォローアップ作業や、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俯瞰などを行い、その結果を２００７年６月に「技術戦略専門委員会報告書 2006」として取りまとめるなどして、追加的な議論・検討および提言をすすめてきた。

その一方で、経済活動や生活に不可欠な社会基盤となっているＩＴの利用範囲の拡大や、活用方法の進化などによって、情報セキュリティを取り巻く社会情勢はここ数年間で大きく変化している。それに伴って、研究開発・技術開発の面で、新たに取り組むべき課題も浮かび上がってきた。

それは、第一に、情報機器やデバイスの急速な普及と高機能化、およびサービスの多様化などに伴って、国民のＩＴへの依存度が高まり、情報セキュリティに係る課題として扱うべき範囲が大幅に拡大していることが挙げられる。第二は、高齢化など世代構成変化に対応し、サービスや製品の設計・開発に際して、使い方が簡単で利用者のミスがリスクにつながらないという発想が、より重要となりつつあることである。第三は、マルウェアの増加に加え、新たな脆弱性の発見や攻撃手法の開発のスピードが加速していることから、従来のセキュリティ対策では対応し切れないケースが増えてきたということである。

当委員会では、これらの社会情勢の変化や課題の認識のもと、２００８年３月から２００９年４月までの間に計 6 回の委員会を開催し、「技術戦略専門委員会報告書 2006」で示された実施のポイントを受けて、(i)投資領域設定の継続的見直し構造の実現、(ii)調達

を通して成果を活用するガイドライン策定の検討、(iii)「グランドチャレンジ型」テーマ検討の場の設置、の３つの項目の検討に取り組んできた。特に「(iii)「グランドチャレンジ型」テーマ検討の場の設置」に関しては、IT における情報セキュリティ技術の問題、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という状況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・技術開発について、当委員会より提言を行い、さらに委員を選任して検討ＷＧを設立して検討を深め、これらを本報告書にとりまとめた。

本報告書では、１）報告書策定の経緯、２）研究開発・技術開発の方向性検討、３）環境変化に対応する研究開発プロジェクトの管理のあり方、の３項目について検討内容をまとめるとともに、最後に当委員会の２００９年における取り組みの方向性について述べている。

２００９年２月に情報セキュリティ政策会議において決定された、第２次情報セキュリティ基本計画には、当委員会で議論された、情報セキュリティを取り巻く環境の変化、情報セキュリティ技術の研究開発に係る検討課題と今後の方向性などの検討結果が重点施策などに反映されている。これらの施策の進展を期待するとともに、当委員会では、グランドチャレンジ型研究開発・技術開発に関する検討など、第２次基本計画に盛り込まれた論点のさらなる深化を進めていく。

また、研究開発プロジェクトの管理・評価体制の改善の方向性に関する検討結果は、総合科学技術会議等に対して提言を行っているところであり、これにより情報セキュリティに限らず広く IT 分野の研究開発・技術開発に対する効率的・効果的な投資の実現と、その成果の迅速な社会展開が図られることを期待するものである。

２００９年４月１６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

・グランドチャレンジ検討 WG における検討内容を報告するにあたって

「グランドチャレンジ型」研究開発・技術開発を推進する方策の検討に際しては、大きく研究テーマとプロジェクト運営の２つの側面の論点が存在する。グランドチャレンジ検討 WG は、情報セキュリティ研究開発・技術開発の方向性を提案することを目的として設置された。より広範な視点からの検討を深めるため、情報セキュリティのみならず一般のＩＴ関連企業やインフラ事業者、サービスベンダ、消費者団体などの多岐に渡る分野の委員から構成され、「研究開発・技術開発の方向性の検討」と、中長期的な研究開発推進のための「環境変化に対応できる継続的な研究開発プロジェクト管理のあり方」の２つの主題について検討を推進した。

研究テーマ面に関しては、大目標となる研究開発テーマを選定するに先立ち、トップダウン（ビジョナリィ・ゴール型)、およびボトムアップ（テクニカル・コンポーネント型)という二つのアプローチを用いて将来の社会ビジョンや技術潮流の予測を行い、研究開発・技術開発の方向性を検討した。また、プロジェクト運営面に関しては、まず公的な競争的資金制度について、研究者側の問題提起と、制度の現状と改善状況の２つの視点から整理し、その検討結果を受け、プロジェクト管理・評価体制の改善の方向性を提案した。

検討の中で整理された、将来の社会ビジョンに係る主たる要素、および技術潮流予測から導出された大きな潮流予測、そして情報セキュリティ技術のグランドチャレンジ型研究分野の方向性の議論が、関係者の今後の議論を惹起し、検討の参考となれば幸いである。
また、プロジェクト管理・評価体制の改善の方向性の提言が、情報セキュリティに関連する研究開発・技術開発プロジェクトの柔軟な運営や、研究成果のより広範かつ有効な公開につながることを期待する。

２００９年４月１６日
技術戦略専門委員会
グランドチャレンジ検討 WG　主査
後藤　滋樹

１．技術戦略専門委員会報告書 2008 の目的と構成

１．１　技術戦略専門委員会における検討の経緯

（１） 技術戦略専門委員会の設置から報告書 2005 のとりまとめ

① 情報セキュリティ分野における技術戦略の検討と専門委員会の設置

技術戦略専門委員会（以下「本専門委員会」という。）は、我が国における情報セキュリティに資する研究開発・技術開発と、その成果利用をどのように実施していくかの戦略を立案するために、２００５年５月に情報セキュリティ政策会議の下に設置された。本専門委員会は、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。）を、２００７年６月に「技術戦略専門委員会報告書 2006」（以下「報告書 2006」という。）を、これまでにとりまとめてきた。

② 報告書 2005 のポイント

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。具体的には、まず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し、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という「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」を示した上で、以下の３つの課題について検討を行ない、その結果を取りまとめた。

（i）　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
○ 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

（ii）　情報セキュリティ技術開発の環境整備のあり方

○ 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を支える環境整備

（iii）「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
○ 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

これらは、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示したものであった。

③ 報告書 2005 と第１次情報セキュリティ基本計画

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「第１次基本計画」という。） が決定された。

第１次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。この中で、技術戦略の推進に関しては、報告書 2005 における課題の検討結果を反映し、次の３点を重点施策として取り組んでいくこととした。

(i)　研究開発・技術開発の効率的な実施体制の構築

報告書 2005 における「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」での検討に基づき、我が国における情報セキュリティに関連する研究開発・技術開発の実施状況の把握と継続的な見直し、成果利用までを見据えた研究開発・技術開発を実施するための体制の構築などに取り組む。

(ii)　情報セキュリティ技術の重点化と環境整備

報告書 2005 における「情報セキュリティ技術開発の環境整備のあり方」での検討に基づき、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の研究開発・技術開発および萌芽的研究開発の促進などに取り組む。

(iii)　「グランドチャレンジ型」研究開発・技術開発の推進

報告書 2005 における「「グランドチャレンジ型」研究開発・技術開発の推進」での検討に基づき、長期的な視野に立った技術革新等の実現を目指す「グランドチャレンジ型」の研究開発・技術開発に取り組む。

（２） 報告書 2005 を受けた取組みの開始から報告書 2006 のとりまとめ

① 報告書 2005 を受けた取組み

第１次基本計画に加え、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、報告書 2005 で提示した様々な方策が取り入れられるとともに、情報セキュリティが「戦略重点科学技術」の一つとして位置づけられた。具体的には、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や、社会システムデザイン研究の強化などが、推進方策として盛り込まれている。

② 報告書 2006 のポイント

本専門委員会は、２００６年度には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報告書 2005 のフォローアップ作業を行い、報告書 2006 において最新の動向を反映させた。また、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も追加的な議論を行い、報告書 2006 に盛り込んだ。具体的には、報告書 2005 の課題「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」の実現方策のうち「投資領域設定の継続的見直し構造の実現」に関して、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を俯瞰することや、第１次基本計画の「情報セキュリティ技術の重点化と環境整備」[1]に関連して重点化分野を見直すことなどが行われた。

報告書 2006 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。また、２００７年における実施のポイントとして、以下の３項目を盛り込んでいる。

(i)　投資領域設定の継続的見直し構造の実現

(ii)　調達を通して成果を活用するガイドライン策定の検討

(iii)　「グランドチャレンジ型」テーマ検討の場の設置

これらの項目のうち、「(i) 投資領域設定の継続的見直し構造の実現」と「(ii) 調達を通して成果を活用するガイドライン策定の検討」は、報告書 2005 の３つの検討課題の中

[1] この柱は、報告書 2005 における「情報セキュリティ技術開発の環境整備のあり方」での検討を受けて設定されたものである。

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新しい構造のあり方」に関して、実施の方向性を議論した内容となっている。

また、「(iii)「グランドチャレンジ型」テーマ検討の場の設置」は、報告書 2005 の「情報セキュリティ技術開発の環境整備のあり方」と「「グランドチャレンジ型」研究開発・技術開発の推進」（すなわち、第１次基本計画の「情報セキュリティ技術の重点化と環境整備」と「「グランドチャレンジ型」研究開発・技術開発の推進」）の２つの柱の共通的な検討事項として設定されている。そして、報告書 2005 における「「グランドチャレンジ型」研究開発・技術開発の推進」の課題をより深く検討するために、グランドチャレンジ検討ワーキンググループ（以下「検討WG」という。）を設立し、以下の項目などについて検討することを提案した。

（ア）トップダウン（ビジョナリィ・ゴール型)、ボトムアップ（テクニカル・コンポーネント型）という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　【研究テーマ面】

（イ）（グランドチャレンジ型）研究開発・技術開発を推進する体制　【プロジェクト運営面】

【参考】グランドチャレンジ型研究開発・技術開発とは

近年の科学技術研究の問題として、研究領域の細分化や先鋭化が進んだことにより、研究実施の目標設定が短期的なものになったり、他の研究領域との連関性を意識しない研究実施になったりするケースが増加している。このような問題に対しては、総合科学技術会議をはじめとした関係組織において、改善に向けた取り組みがなされているところであるが、解決に向けた方策のひとつとして、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、その大目標の実現に向けて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、まず何を大目標として設定するかが大きな課題となる。このプロセスにおいては、分かりやすく象徴的なターゲットを選定する中で、研究を長期的に行う意味と、細分化・先鋭化しがちな個別研究領域の連関性の再認識、さらには、研究活動と社会との関係などが明確になることが期待できる。また、大目標を複数のサブ目標に分割し時系列に整理するプロセスや、サブ目標の見直し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、グランドチャレンジ型の研究開発を実施する過程において、目標が徐々に実現されていくだけでなく、その途中で生み出される数多くの副産物が社会に展開される効能を期待することができる。加えて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。

（３） 報告書 2006 を受けた取組みと２００８年度の技術戦略専門委員会における検討

① 報告書 2006 を受けた取組み

報告書 2006 で提示された２００７年における実施のポイント（参照：（２）②）を受け、２００７年度は、まず(iii)の検討WGを情報セキュリティ分野の有識者及び内閣官房情報セキュリティセンターの職員から構成される形で設置し、予備的な検討を行なった。検討に際しては、以下の３つの論点を設定した。

第１の論点は、上記（２）②（ア）の研究テーマ面に関するものである。具体的研究開発テーマを選定するに先立ち、グランドチャレンジ型研究開発の対象となるような情報セキュリティ上の脅威は存在するのか、存在する場合、それはどのようなものか。また、プロジェクトを実施する上で達成される・されるべき効果は何か、といった観点から検討を行った。具体的には、グランドチャレンジを実施する意義、具体的な研究開発テーマ、グランドチャレンジを実施することによる被益の対象などについて検討を行った。

第２と第３の論点は、上記（２）②（イ）のプロジェクト運営面に関するものである。
第２の論点では、国としてグランドチャレンジ型研究開発にどう関与し、どのような体制で進めるべきか、説明責任をどのように果たすのかといった観点から検討を行った。具体的には、推進体制、産学官/省庁間の連携体制、予算獲得に向けた方策、などについて検討を行った。

第３の論点では、グランドチャレンジ型研究開発が、有効な成果を出すためのマネジメント上の要件は何か、といった観点から検討を行った。具体的には、プロジェクトマネージャーの役割、成果／進捗評価手法、参加意識の強化などについて検討を行った。

２００７年度のこれらの検討内容は、検討WGから本専門委員会に報告され、本専門委員会では２００８年度の活動方針を議論した。結果、「２００７年における実施のポイント」のうち、「(i) 投資領域設定の継続的見直し構造の実現」と「(ii) 調達を通して成果を活用するガイドライン策定の検討」は継続的な検討事項としつつ、「(iii)「グランドチャレンジ型」テーマ検討の場の設置」に関連しては、さらに深く検討するために、必ずしも情報セキュリティに限定せず、より広範な分野の人材から委員を選任して新たなグランドチャレンジ検討WG（以下「新たな検討WG」という。）を設立し、大きく次の２つの主題について検討することとした。

（ア）研究開発・技術開発の方向性検討
本主題は、第１の論点を深めるため、報告書 2006 で提示された「トップダウン（ビジョナリィ・ゴール型)、ボトムアップ（テクニカル・コンポーネント型）という二つのア

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」の内容を、主に研究テーマの側面から具体的に実施するものである。　【研究テーマ面】

（イ）環境変化に対応できる継続的な研究開発プロジェクトの管理のあり方

本主題は、第３の論点を深めるため、報告書 2006 で提示された「研究開発・技術開発を推進する体制」に関して、主にプロジェクト運営の側面から具体的に検討するものである。　【プロジェクト運営面】

②　２００８年度の技術戦略専門委員会における検討と報告書の構成

２００８年度は、より広範な視点から情報セキュリティ研究開発・技術開発の方向性を提案することを目的とし、情報セキュリティのみならず一般のＩＴ関連企業やインフラ事業者、サービスベンダ、消費者団体などの多岐に渡る分野の委員から構成される新たな検討WGを設置し、「研究開発・技術開発の方向性の検討」と、中長期的な研究開発推進のための「環境変化に対応できる継続的な研究開発プロジェクト管理のあり方」の２つの主題について本専門委員会における検討と連携する形で、それぞれの委員の多様な観点からの知見を活用しつつ検討を推進した。

それらの検討結果をまとめたものが、「技術戦略専門委員会報告書 2008」（以下「本報告書」という。）である（参照：図１―１）。本報告書は、（３）①の（ア）、（イ）のそれぞれを受けた、「情報セキュリティ技術の将来に関する検討」と、中長期的な研究開発推進のための「公的資金を用いた中長期的な研究開発の実施方法」の２つの部分から構成されている。

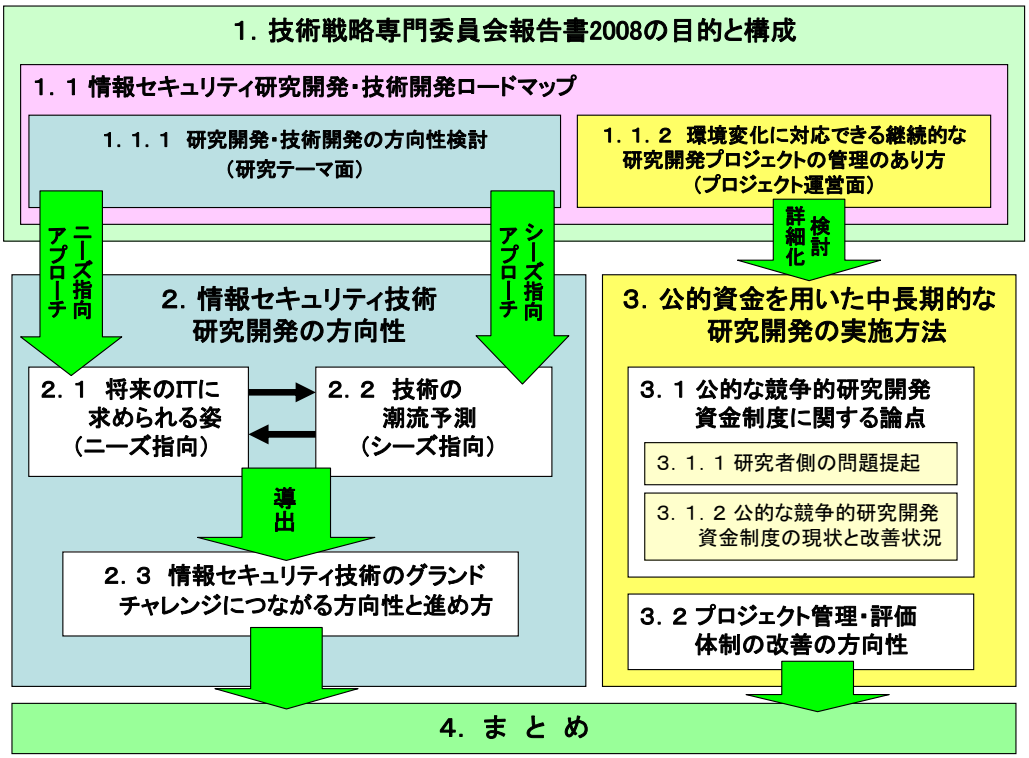

図１―１　本報告書の構成

研究テーマ面の主題である「研究開発・技術開発の方向性の検討」に際しては、ニーズ指向アプローチとシーズ指向アプローチの２種類の取組みを行った。（参照：図１－２）

ニーズ指向アプローチは、将来の社会ビジョンの検討に基づくトップダウンのアプローチである。本専門委員会と検討ＷＧの委員による将来の社会ビジョンの提案から、将来の社会ビジョンに係る主たる要素とグランドチャレンジを通じて実現すべきことを整理した。また、シーズ指向アプローチは、技術潮流予測を用いたボトムアップのアプローチである。情報セキュリティ技術に関する戦略の視点で、社会と情報セキュリティ技術の双方について潮流予測を行い、利用者、ベンダ、制度の３分野における大きな潮流予測をまとめた。

委員会では、これらの２つのアプローチによる検討の結果に基づき、グランドチャレンジにつながる情報セキュリティ分野の研究開発の方向性と今後の進め方についても検討を行った。

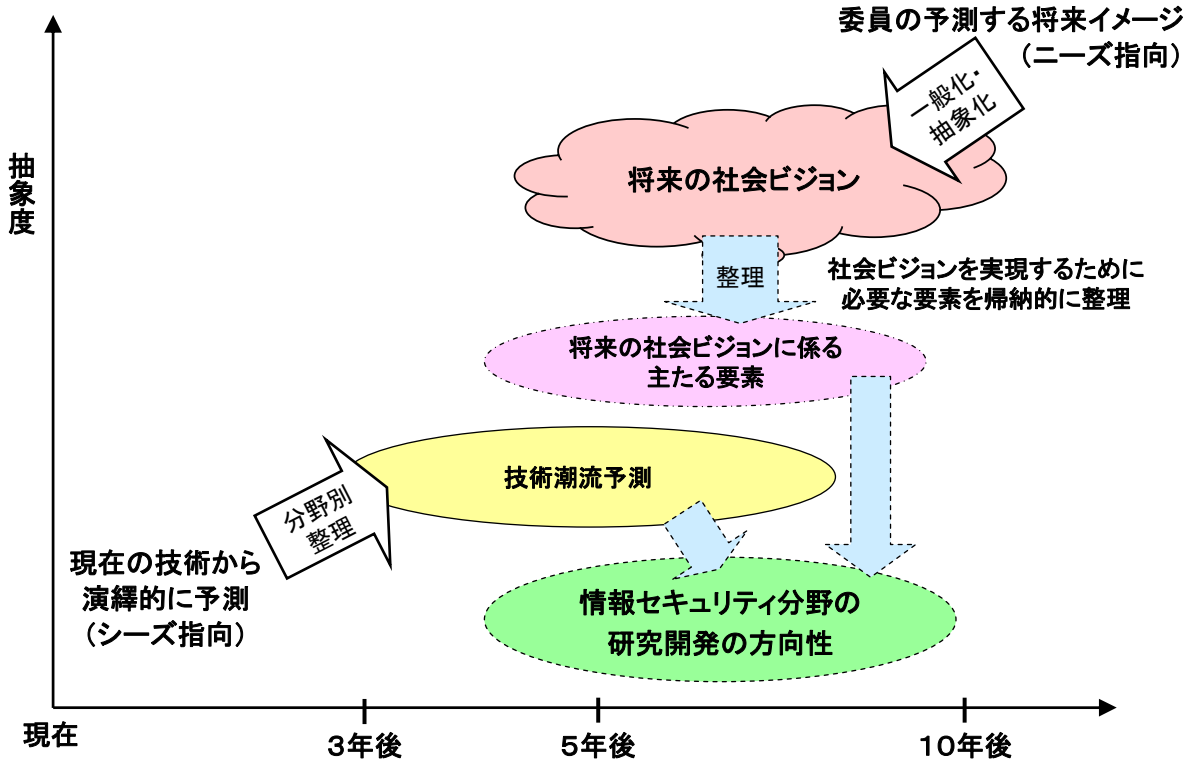

図１－２　情報セキュリティ分野の研究開発の方向性の検討ステップ

また、プロジェクト運営面の主題である「環境変化に対応できる継続的な研究開発プロジェクト管理のあり方」については、まず公的な競争的資金[2]制度に関する論点を、研究者側の問題提起と、制度の現状と改善状況の２つの視点から整理した。そして、その検討結果を受け、プロジェクト管理・評価体制の改善の方向性を提案した。これらは、今後グランドチャレンジ型研究開発の取組みを進める際にも資するものである。すなわち、グランドチャレンジ型研究開発においては、中長期的な大目標のもと、社会や技術の環境変化を評価しつつ、複数の研究テーマを統合的かつ連携して推進する必要がある。そのため、個別の研究開発プロジェクトの途中成果の公開が積極的に行われ、同時に管理体制が柔軟であることが望まれるからである。

③　２００８年度の検討と第２次情報セキュリティ基本計画

第２次情報セキュリティ基本計画（以下「第２次基本計画」という。）は、第１次基本計画の下での取組み状況、情報セキュリティ政策会議の下に設置された基本計画検討委員会の第１次提言、同提言を踏まえた政府での取組み、同じく情報セキュリティ政策会議の

[2] 資金配分主体が、広く研究開発課題等を募り、提案された課題の中から、専門家を含む複数の者による、科学的・技術的な観点を中心とした評価に基づいて実施すべき課題を採択し、研究者等に配分する研究開発資金をいう。（「総合科学技術会議の競争的研究資金制度改革について（意見）」（平成１５年４月２１日））

下に設置された本専門委員会や重要インフラ専門委員会などでの検討などを踏まえて、２００９年２月に情報セキュリティ政策会議において決定された。

第２次基本計画の決定までの過程において、本専門委員会と新しい検討WGは、研究テーマ面、プロジェクト運営面の２つの主題に関する検討を進める中で、第１次基本計画策定時以降の情報セキュリティを取り巻く環境の変化、情報セキュリティ技術の研究開発に係る検討課題と今後の方向性、第２次基本計画に向けた第１次提言において技術戦略の観点からの検討課題と考えられる論点などを併せて議論し、検討結果を基本計画検討委員会に提言した。

その結果、第２次基本計画の「第２章　第２次情報セキュリティ基本計画における基本的考え方と２０１２年の姿」において、

① 利用者による情報セキュリティ対策が不要な端末や情報家電の提供、

② 設計段階から情報セキュリティを作り込む開発手法の普及と定着、

③ リスクの形式的な表記法や、リスクの評価方式の共通化、

という形で、本専門委員会と新しい検討WGが検討を行った将来の社会ビジョンや技術潮流予測の検討内容が適切に反映されている。

また、第２次基本計画の「第３章 今後３年間に取り組む重点政策」における技術戦略部分では報告書 2005 で示された３つの課題、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、「グランドチャレンジ型」研究開発・技術開発の推進、情報セキュリティ技術開発の環境整備のあり方に対応し、

（ア）情報セキュリティ技術開発の重点化と多様性の維持、

（イ）「グランドチャレンジ型」研究開発・技術開発の推進、

（ウ）研究開発・技術開発の効率的な実施体制の構築と基盤の整備

の３つの重点施策が盛り込まれた。また、３つの重点施策の具体的な内容には、２００８年度の本専門委員会での検討結果が盛り込まれている。

１．２　情報セキュリティ研究開発・技術開発に関する２００８年度の検討

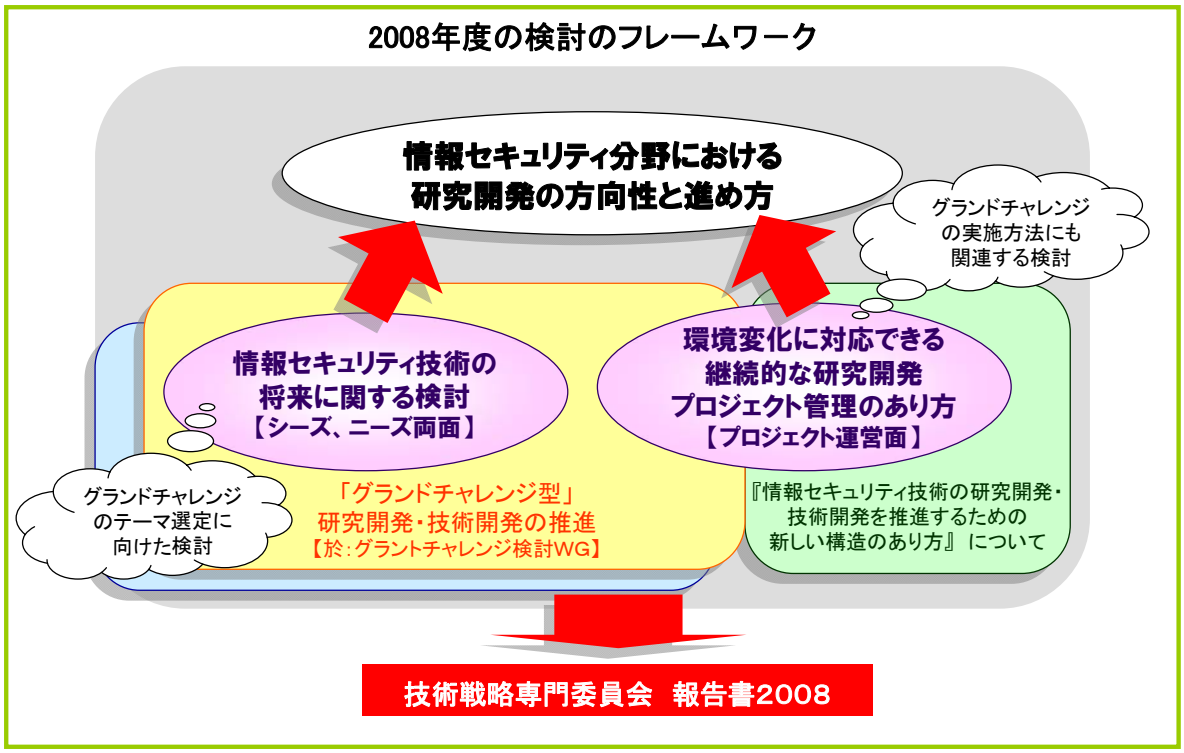

図１－３　技術戦略専門委員会および検討ＷＧにおける検討枠組み

情報セキュリティの研究開発・技術開発に関し、２００８年度は以下のような検討の枠組みを設定して検討を進めた。

１．２．１　研究開発・技術開発の方向性検討

情報セキュリティ技術の将来に関する検討は、グランドチャレンジのテーマ選定に向けた検討の一環である。その目的は、先ず「将来の社会ビジョンと技術の潮流予測」をまとめて公表することで、認識を共有するとともに、情報セキュリティ技術や政策に関する方向性の議論を惹起することである。

また「将来の社会ビジョンと技術の潮流予測」は、問題提起や提言を行うための前提として用いる。即ち、「将来の社会ビジョン」に係る主たる要素を整理することで、グランドチャレンジを通じて実現すべきことが明確となってくる。また「技術の潮流予測」で整理した技術を利活用する結果、新たに登場するであろう情報セキュリティ上の脅威や技術課題が推定できる。その結果、情報セキュリティ分野の研究開発の方向性が浮かび上がることが期待できる。技術の潮流予測の主な対象分野については、検討領域を事前に制限するものではないが、関係者で認識を共有するために、主として、利用者、ベンダ、基盤の３分野にわけて予測を行なった。

１．２．２ 環境変化に対応できる継続的な研究開発プロジェクトの管理のあり方

グランドチャレンジ型研究開発・技術開発が実行段階に移った後のプロジェクト管理にも資するという視点より、中長期的な研究開発プロジェクトにおいて有効な成果を出すためのプロジェクト管理上の要件は何か、といった観点から検討を行った。技術や社会の変化に対応して、グランドチャレンジ型の研究開発を推進するには、大目標の実現のためのマクロ的な視点でのプロジェクト管理と同時に、個々の研究プロジェクトの成果を最大化するためのミクロ的なプロジェクト管理の柔軟性も重要である。当該検討は特に後者の課題を検討することを目的とした。

研究開発の現場の研究者から、現状のプロジェクト管理では、事前に立てた研究計画への強い拘束力が発生し、柔軟で効果的な研究開発が困難な場合があるという意見が出ている。最終目標から要素還元的アプローチによって策定した研究計画に基づき、計画に沿った実施が行われているかについて厳密な検証が行われ、新たな状況変化が認識されても、計画自体への変更は実質的に不可能なケースが少なくない、という主張である。

一方で、各府省庁や独立行政法人などの競争的資金の配分機関による研究開発プロジェクトの管理ルールは年々改善されており、研究者の不満は、研究者自身や所属組織の管理部門あるいは、プロジェクト・マネージャ（ＰＭ）がルールを十分に理解していないことに基づく誤解や、管理ルールの変更の不徹底などに拠るところが大きいという反論もある。

そのため、ここでは研究者サイドと管理・運営サイド（研究開発費を支出し、プロジェクトを管理・運営する側）との双方から現状のルールやその運用、それぞれの認識についてヒアリングを行った。そして、何が研究開発プロジェクトの柔軟性を阻害しているかのファクトを整理し、その課題の改善案を検討した。

２．情報セキュリティ技術の将来に関する検討

以下、「研究開発・技術開発の方向性の検討」に際しては、ニーズ指向とシーズ指向の２種類のアプローチで、情報セキュリティ技術の将来に関する検討を行う。すなわち、将来の社会ビジョンという実現したいニーズを明らかにした上で、ニーズから帰納的に研究開発・技術開発の方向性を検討するアプローチと、現在の技術から技術潮流を予測した上で、シーズから演繹的に研究開発・技術開発の方向性を検討するアプローチの双方から、総合的な検討を行うものである。

２．１ 将来の社会ビジョンに関する検討（ニーズ指向の検討）

本節ではニーズ指向アプローチとして、本専門委員会と検討WGの委員による将来の社会ビジョンの提案から、将来の社会ビジョンに係る主たる要素とグランドチャレンジを通じて実現すべきことを整理する。将来の社会ビジョンを整理することで、本専門委員会として実現することが望ましいと考えられる特徴的な要素、すなわち「主たる要素」を抽出し、こうした要素を満たすような技術を検討することでグランドチャレンジにつながる方向性を明らかにしていく。

（１） 委員会における将来の社会ビジョンの検討

本専門委員会および検討WGの委員が検討の場において提示した、情報セキュリティに軸を置いて考える将来の社会ビジョンとしては、主として以下のようなものがあった。

「（情報セキュリティにも）オートパイロット的（自律的）な概念を導入することで、より快適に生活を営むことが可能となる。」
「高齢者も障害者も初心者も子どもも、生活の中で、現在の読み書き能力と同程度にＩＴ機器を操作して情報を授受し、発信している。そこでは誰でもが使いこなせて、故障しにくく、情報セキュリティに関しても意識が少なくて済む機器が提供されている。」

【このビジョンを実現するための技術の方向性の例】
(a) ＩＴサービスシステムのオートメーション化
- ＩＴシステムの障害自動復旧技術（免疫、治癒能力）の発達
- マシンやデバイス同士による自律的な制御
- システム構成自動最適化技術の進展

(b) 情報格差の顕著化の防止（すべての国民が等しくＩＴの利便性を享受）
- 社会的弱者に配慮した分かり易い情報セキュリティ対策の提供
- 情報セキュリティ対策の複雑性を技術により秘匿し、ユーザーに必要な情報のみを可視化

「家庭においては、個人で使うレベルを超えた能力のＣＰＵを搭載したテレビやパソコン、ゲーム機などが相互接続され、家庭におけるコンピュータ環境がブラックボックス化しており、（社会的弱者に配慮して）その品質や情報セキュリティを含む安全性を向上していく必要がある。」[3]

【このビジョンを実現するための技術の方向性の例】

(a) 脆弱性の少ないコンピューティング環境の実現

- 認証されていないプログラムを利用できないコンピューティング環境

(b) 実用的かつ不便を強いないフィルタリングの発達

- 青少年等の発達段階に配慮したユーザーの利便性が高いインターネット環境を実現するフィルタリング技術
- 文章や画像・映像の内容に基づくフィルタリング技術

(c) 電化製品のネットワーク化の進展

- 情報家電などのパッチの共通化・自動作成によるコスト削減

「ネットワーク接続された多種多様な計算機の上に、高い信頼性・可用性をもつだけでなく、サービスに応じた適切な安全性が確保できるような仮想サーバ環境が実現される。」

【このビジョンを実現するための技術の方向性の例】

(a) システムの統合的な安全性の評価の必要性が増大

- 連関的な情報セキュリティについての評価が必要

(b) リスクや対策の体系的な評価の必要性が増大

- ＩＴシステムの標準化（部品化）
- リスクの数値化、可視化
- リスクのシミュレーション技術の進展

(c) クラウド環境の機密性・完全性・可用性に対する必要性が増大

- 権限があればどこからでも情報やサービスにアクセス可能
- 異なるクラウド・コンピューティング環境へ安全に環境の移行が可能
- 拡大するクラウド・コンピューティング環境においても安定した動作実現
- 情報セキュリティを確保しつつ異なるクラウド・コンピューティング同士が連携可能

[3] 情報家電の安全性を担保するための技術の必要性に係る意見として出されたものである。

「システム運用中に生じた構成の変更や、システムの内部状態、外部環境の変動に応じてシステムの設定や構成などを変更し、適切な情報セキュリティ水準を自律的に維持できる。ただし、業務内容によってシステム構成の自由度や情報セキュリティの強度などは人間が制御できる。」

「クラウドの発達とグローバルな普及によって、利用者はデータの在り処やソフトウェアがどの企業のサーバで実行されているかなどを気にせずにＩＴサービスを利用することが可能になるが、他方で“この情報は国内のデータベースに置いておきたい”とか“この業務はＡ社のサービスで処理させたい”などの要求があった場合には、クラウドはその要求を確実に遵守できる。」

【このビジョンを実現するための技術の方向性の例】

(a) リスクの統制や情報の管理のニーズの増大

- 安全性を確保するため情報の管理権限と制御のためのルール設定は人間が行うが、基本的に自動制御により適切な情報セキュリティ水準を維持
- パーソナルな情報空間とパブリックな情報空間は分離され、どの情報をシェアするか、しないかは、情報の所有権限者によりコントロール

「ネット通販関係は、日本の多くの商店がアジア圏を市場として捉えられるように変貌する。同時に、高品質なアジア圏のネット上の商店も日本へのビジネスが一般化する。一般の企業に関しても、国境を越えたＢ２Ｂ[4]マーケット提供サービスなども立ち上がり、営業・流通が再編成される。」

「ユビキタス社会が進展し、情報通信デバイスが相互に連携しつつ自律的に制御を行い、人間の能力を補完する。これによって、個々の人々がより快適な生活を送ることができる。」

【このビジョンを実現するための技術の方向性の例】

(a) ユビキタスデバイスの普及

- センサー機能を持った情報通信デバイスが日常生活を「アシスト」

(b) 実社会と仮想社会の位置づけが大幅に変化（一部は逆転）

- 企業の格付けを行う評価指標の一つとして情報セキュリティ水準の高さを求められることが一般化
- ネット社会の信頼が実社会に影響（企業の業務範囲拡大や、企業の上場基準などにも、一定以上の「格」が要求される。）

[4] Business to Business の略。

「ＩＴの活用と社会基盤化が一層進展していく中で、情報セキュリティの確保はＩＴを用いた製品・サービスの品質・性能の一部と認識されるとともに、例えば一般企業においては企業統治[5]やいわゆるＣＳＲ[6]の一環、事業継続の手段として適切な情報セキュリティ対策を取ることが不可欠となっている。情報セキュリティ技術の研究開発や情報セキュリティ対策は、問題が発生した際の「受け身」のものではなく、「強み」となるよう戦略的に進められている。」

「クラウドのデータベースにアップロードされた画像は三次元空間にマッピングされ、自由に時間・空間軸でナビゲーションできるようになり、撮影者・利用者によるタウンガイドなどの情報整理の他、ゲーム等へも利用される。」

【このビジョンを実現するための技術の方向性の例】

(a) 情報セキュリティの作り込みによる次世代製品の国際競争力の強化
- セキュアな開発手法の定着（セキュア開発の現場力の確立・向上）
- 形式手法によるソフトウェア開発技術
- 汎用リコンフィギュアブル・プロセッサと形式検証の容易なＯＳ・高級言語

(b) 画像・映像の組織化と地理情報サービスとの連携／メタデータ重畳
- 画像・映像のみならず、その中に映ったオブジェクトも検索可能とするエンジン
- メタデータを重ねた画像を検索／表示するデバイス（電脳眼鏡など）の進化

（２） 将来の社会ビジョンに係る主たる要素

本委員会では、委員から提示された「将来の社会ビジョン」に関連して、これらを構成する主たる要素を、具体的な社会ビジョンよりも一段階抽象的な概念として抽出するべく検討を行った。結果、主に社会に係る要素として①，②，③、主に技術に係る要素として④，⑤，⑥が抽出された。これらは、今後、グランドチャレンジ型研究開発・技術開発のテーマを具体化し、研究開発・技術開発を進める中で、実現していくべき主たる要素として、今後の大きな方向性を示唆するものと言える。

① 安全・安心な生活、社会経済活動の実現

情報セキュリティ技術が実現すべきことは、まずは安全・安心な生活、安全・安心な社

[5] コーポレートガバナンス（Corporate Governance)の訳。企業の目的達成に向けて、適切に内部統制の仕組みを構築し、社会的信用を維持する機能を指す。
[6] CSR: Corporate Social Responsibility)：企業の社会的責任を指す。企業は利潤を追求する組織であるが、それだけでなく、当該組織の活動が社会へ与える影響に責任を持ち、あらゆる利害関係者に対して適切な責任を果たしていくことを求めるものである。

会経済活動の確保である。これらは、例えば高齢者や子供、外国人など、多様なユーザーに対して広く確保されるべきである。

② グローバル・ユビキタス

ＩＴは国境を越えてユーザーがグローバルにつながることを可能としている。このため、例えば日本国内において情報セキュリティをどれほど確保できたとしても、国外での情報セキュリティ確保が不十分な場合、結局は国内におけるユーザーも情報セキュリティ上のリスクにさらされ続けることとなる。この観点から、情報セキュリティ技術は国境を越えてどこででも、いつでも情報セキュリティが確保されるような統合的なリスク制御のための取組みを進めるべきである。

③ 最先端性

ＩＴ先進国である我が国として、情報セキュリティ技術についても先進的であるべきである。我が国が情報セキュリティ確保の観点から世界をリードし、また世界に誇れる技術を開発するべきである。

④ 当然化

ユーザーが脅威・リスクへの対応を意識してＩＴ機器やＩＴサービスを利活用する必要がある場合、現時点では確保される情報セキュリティの水準がユーザーの知識・経験などに左右されることが少なくない。しかし、ＩＴに関する知識や経験が様々な幅広いユーザーの利用に耐え得るという観点からは、製品の機能としてある水準の情報セキュリティが自然に、すなわち当然のこととして担保されていることが必要である。

⑤ 適切性

情報セキュリティは、ＩＴがもたらす利便性や効率を無条件に犠牲にしてでも実現するべきものではない。情報セキュリティさえ確保できれば良いという思考に陥ることなく、製品やサービスの種類や状況等に応じて必要かつ適切な情報セキュリティ水準が柔軟に確保できるよう、技術的対応を進めることが不可欠である。

⑥ マネージャビリティ（可管理性）

ＩＴは利便性を高め、人間の活動の可能性を伸ばし、活動領域を大幅に拡大するツールである。ＩＴに任せられることは任せてそのメリットを追求しつつ、利用者が自身の意思の通りにコントロールしたい点に関しては、確実にＩＴを制御できるようにするべきであ

る。例えば、クラウド・コンピューティングの利用によって、情報資産を自身の手から離れた場所に預けざるを得ないような場合でも、情報資産に関する管理権限を及ぼせるような仕組みが必要となる場合もあり、情報セキュリティ技術の多大な貢献を要する。

（３） グランドチャレンジを通じて実現すべきこと

グランドチャレンジ型研究開発・技術開発の取組みを具体化するにあたっては、少なくとも（２）で挙げた「主たる要素」を満たしていけるようなテーマ選定を早急に進め、我が国全体として大きな方向性を持って研究開発・技術開発を進めるべきである。また、グランドチャレンジの取組みにおいては、技術者のためではなく、あくまでも実際のエンドユーザーのＩＴ利用に大きな影響・利益をもたらすような研究開発・技術開発を行うべきである。このため、テーマ選定に際しては、エンドユーザーの視点に立ち、実現されることが望ましい情報セキュリティ技術が化体した具体物、すなわち「New Secure Product[7]（仮称）」の開発を実現する方向で進めるべきである。

また、国境を越えてネットワークがつながっている状況下において、このような「New Secure Product」によって、我々は情報セキュリティに係る問題を解決するとともに、技術の観点から我が国が世界をリードし、世界に誇れる状況を実現するべきである[8]。

さらに、元来、グランドチャレンジ型研究開発・技術開発が目指す、開発過程での波及効果も確実に実現すべきである。すなわち、様々な関連領域における技術の発展を含めて、社会で実際に大きな効用を有する関連技術の発展を実現すべきである。

２．２　技術の潮流予測（シーズ指向の検討）

本節では、シーズ指向アプローチとして、情報セキュリティ技術に関する戦略の視点で、社会と情報セキュリティ技術の双方について潮流予測を行い、利用者、ベンダ、基盤の３分野に分けて大きな潮流予測をまとめる。グランドチャレンジ型研究開発・技術開発を通じて、現在の技術から考えて大きな革新を生み出すためには、グランドチャレンジの開発テーマから帰納的に開発が必要な個々の技術テーマなどを明らかにすることが基本である。しかし、同時に現在の技術から考えて、今後予測され得る技術開発についても考慮す

[7] 本委員会における検討では、「主たる要素」である「（情報セキュリティの）当然化」が実現された状態を前提に考えると、その時点では既に Secure ということ自体が意識されることはないので、「New Secure Product」の Secure の語は不要ではないか、という旨の指摘もあった。しかし、具体的研究開発・技術開発が未着手である現時点においては、Secure という要素を明確化しておくために、「New Secure Product」として仮称を設定する。

[8] 情報セキュリティにおいては、技術やプロダクトによってのみ確保されるのではなく、運用面が重要であることは言うまでもない。

るべきという現実的な視点も必要と考えられる。シーズ指向アプローチの検討はこの観点から行うものである。

２．２．１　情報セキュリティ技術に関する将来予測の進め方

（１）将来予測の範囲と期間

・ 範囲：社会の基盤となるシステムやサービスとそれらを支えるＩＴ技術
　具体的には、公的なサービスのＩＴインフラ（電子政府など）、重要インフラ関連（情報通信、電力、鉄道など）、一般利用者向けデジタル機器や情報サービス、及びそれらを開発・運営する主体や、実装を支える技術などが、候補として挙げられる。

・予測の期間：中長期（３年～１０年後程度）

（２）将来予測の手法

中期面については、現在の技術とその動向に基づき演繹的に予測を行う。長期面については、単に現在の技術を延長するのみではなく、社会的な視点[9]からも潮流予測の検討を進める。予測された内容は、分野別に整理することで、技術潮流をより明確に描く。

（a）社会的視点のアプローチ

本アプローチの下では、主に利用側の視点から予測を行う。具体的には、将来的に登場するであろう製品、アプリケーション、サービス等を予測し、それらを安全・安心に利用するための情報セキュリティ要件を検討する。

（b）演繹的な技術予測アプローチ

本アプローチの下では、主に提供側の視点から予測を行う。具体的には、現在の技術の延長として、どのような機能、性能のものが登場するかを予測し、その際に必要となる情報セキュリティ要件を検討する。（例：数テラバイトのＨＤＤやメモリが一般家庭に導入された場合、従来のパターンマッチング技術でウィルスチェックを行うことが現実的であるか。困難な場合には、どのような手法や技術が必要になるか。）

[9] 当該部分（２．２における）「社会的な視点」からの検討は、２．１における「将来の社会ビジョン」に関する検討とは別のものである。

２．２．２　技術潮流予測

（１） 技術と社会の変化の方向性予測

技術潮流予測を行うにあたり、最初に、各委員による技術の将来予測を行った。そのなかで、委員から挙げられた個々の技術将来予測を、大きく「利用者」「ベンダ」「基盤」の３つの領域に分類して俯瞰することで、今後１０年の技術と社会の変化の方向性まとめることを試みた。

例えば、「高齢者や初心者用に開発された基本的機能のみのパソコン」や「社会的弱者に配慮した情報セキュリティ技術」などの予測からは、およそ３年後には「技術に詳しい専門家や若者達だけに利用される端末のみではなく、広く一般に利用される端末が登場するようになる」という将来像を読み取ることができる。続いて、このようにして導出した将来像を時間軸にマッピングし、技術面の視点から分類するとともに、長期的には社会的な視点も加味して、その技術が対象とする領域ごとに整理することで、今後１０年の方向性をまとめたものが、「図２－１　今後１０年の技術と社会の方向性予測」である。

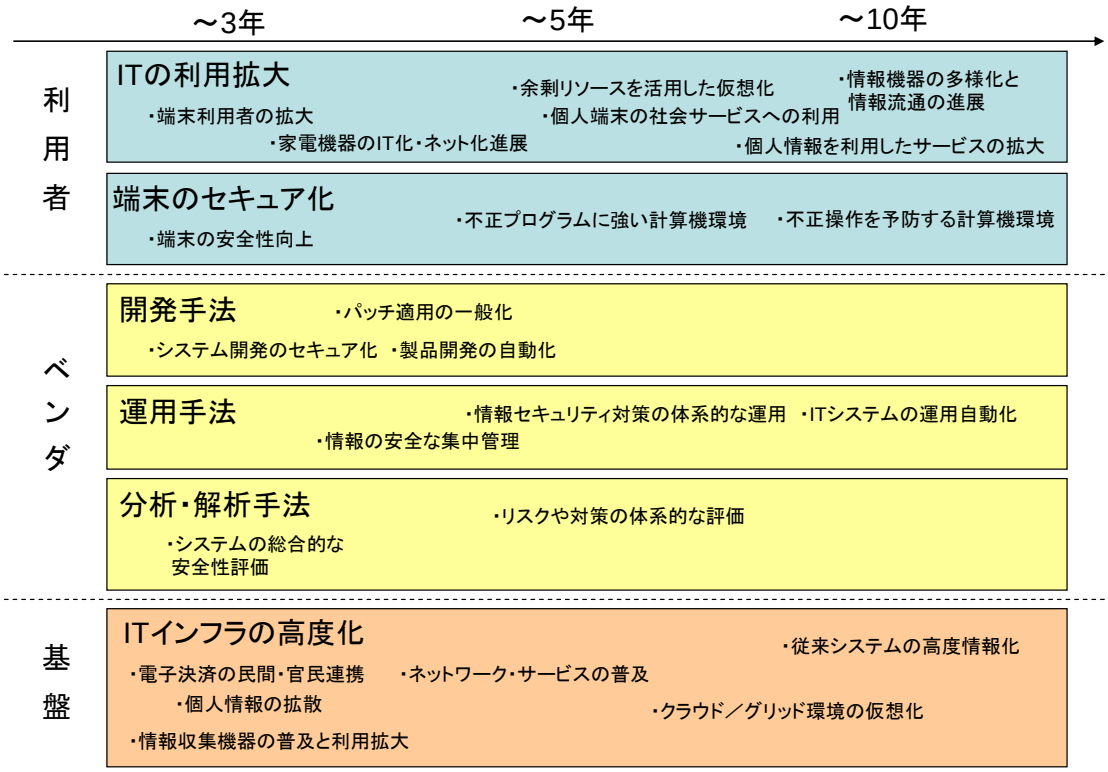

図２－１　今後１０年の技術と社会の方向性予測

「利用者」を対象とした領域では、ＩＴ機器の利用者が拡大し、家電などを含む多種多様な機器のＩＴ化が進展するとともに、それらの機器をつなぐネットワーク上で個人に関する情報を含む多くの情報が広く流通するという「ＩＴの利用拡大」、端末での不正プログラム対策や不正操作の防止が進展する「端末のセキュア化」という２つの方向性として整理した。

「ベンダ」を対象とした領域では、「開発手法」「運用手法」「分析・解析手法」のそれぞれについて、体系化や自動化などが進展していく方向性として整理した。

「基盤」を対象とした領域については、電子決済などのネットワークサービスの普及や仮想化の進展といった、「ＩＴインフラの高度化」という方向性として整理した。

上記のようにして整理した方向性予測における個々の領域の将来像について、その将来像の実現において鍵を握ると思われる技術課題を、委員による将来予測を参考にしつつ抽出し、追記することで技術の潮流予測としたものが図２－２（「利用者」に係る技術潮流予測）、図２－３（「ベンダ」に係る技術潮流予測）、図２－４（「基盤」に係る技術潮流予測）である。

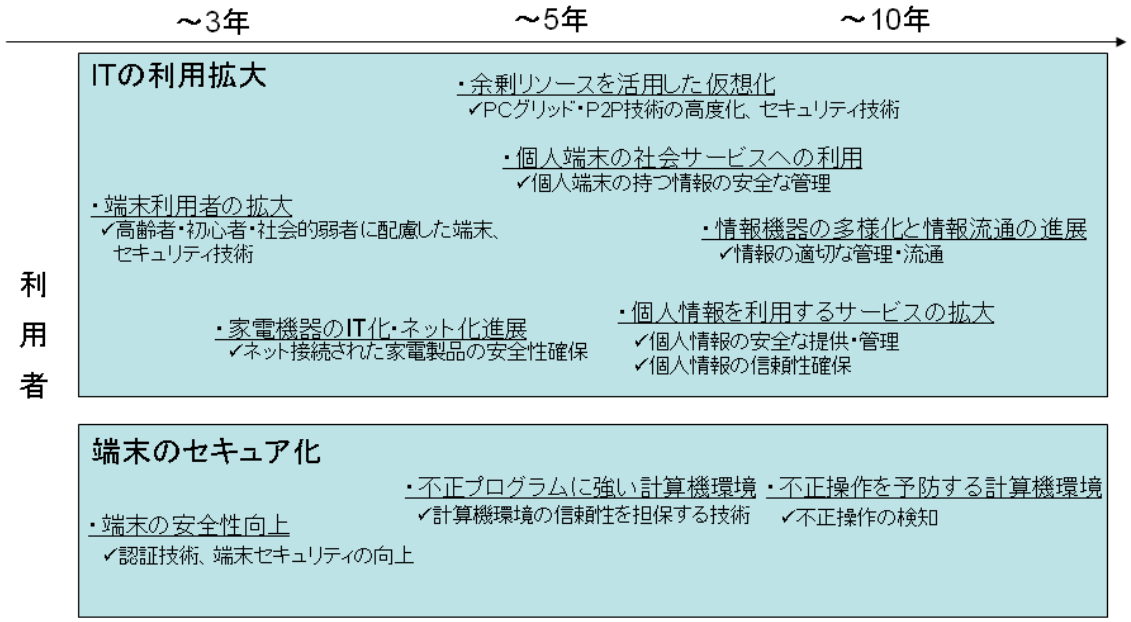

図２－２　「利用者」に係る技術潮流予測

「利用者」の領域における各将来像については、以下のように技術課題を整理した。

- **端末利用者の拡大**

  パソコンや携帯電話などの情報機器の利用者層が拡大するため、高齢者・初心者・社会的弱者などの利用を念頭に置いた端末の開発、特に情報セキュリ

ティ技術の開発が必要となる。
例えば、初心者が誤操作や情報セキュリティリスクの高い操作を行いにくくなるようなヒューマンインタフェイス技術、利用者に特別な操作を強いることなく端末の情報セキュリティ対策の自動更新が行われる技術[10]、幅広い利用者に対して適切に認証を行えるような生体認証技術の向上と、その実現に必要なデバイス・センサー技術の向上、などである。

- **家電機器のＩＴ化・ネット化進展**

テレビ等の家電機器のＩＴ利用が進み、パソコンなみの処理能力を備えたり、ネットワーク接続が可能になるといったＩＴ化・ネット化が進展する。家電製品も従来のパソコンと同様にネットワークからの攻撃にさらされることとなり、その安全性の確保が必要となる。
例えば、いわゆる組み込み機器のソフトウェアにおいては、情報セキュリティ水準の高いソフトウェアの開発（セキュアな組み込みソフトの開発）、家電機器の安全なネットワーク接続を実現するための接続方式の標準化（相互接続の標準化）、家電機器をホームサーバで管理する際に利用者のコンテンツ保護や各機器の情報セキュリティ管理手法の開発（セキュアホームサーバ）などである。

- **余剰リソースを活用した仮想化**

端末の普及やネットへの常時接続のさらなる一般化に伴って、端末の余剰リソースを活用したサービスの仮想化が行われる。ノードの制御や管理機能などの P2P 技術や、クラウド・コンピューティング技術の高度化とともに、仮想環境の情報セキュリティを確保することが必要となる。
例えば、仮想環境にサービスを安全に構築する技術（セキュアな仮想環境の開発技術）、仮想環境の安全性を継続的に維持する技術（ネットワークの監視・制御技術）などである。

- **個人端末の社会サービスへの利用**

広く普及した個人所有の端末を利用して、道路の保全見回りや災害時見回りなどの社会的なサービスを行う。
ただし、個人端末に保管された情報を利用するため、厳重な運用管理を行える必要がある（個人に関する情報の管理運用手法）。

- **個人に関する情報を利用するサービスの拡大**

携帯音楽プレーヤー、携帯電話、PC など、様々な端末が普及し、いろいろな

[10] 特定の OS では情報セキュリティ対策の自動化機能の一部が実現されている。

機器がネットワーク接続され、それらの端末を介して得られる個人に関する情報を使ったサービスや、ネットワーク上に保管された個人に関する情報を参照するサービスが拡大する。個人に関する情報の安全な流通や、流通する個人に関する情報の信頼性の担保が必要となる。

例えば、個人に関する情報のうち、サービス提供に必要な部分のみを開示したり、個人に関する情報を必要以上に紐付けせずに管理する技術（個人に関する情報の安全な部分開示・管理技術）、個人に関する情報の提供や入手の際にその個人に関する情報が正しい情報であることを証明したり確認したりする技術（個人に関する情報の正当性を証明・検証する技術）などである。

- **情報機器の多様化と情報流通の進展**

情報を扱う端末が多様化するとともに、情報の個々の端末への依存度が低くなり、どの端末を使っても同じように情報にアクセスできるようになる。

そのためには、端末間でやりとりされる情報が適切に管理・流通できる必要があり、機器間の相互接続技術、情報が機器を問わず扱えるようにするための標準化や、情報を一意に特定する技術（情報提供フォーマットの標準化、識別技術）、情報に対する所有権などに適切に従った利用・流通を行えるようにする技術（権利に基づく情報流通管理技術）などが重要となる。

- **端末の安全性向上**

端末を個人認証デバイスとして利用する機会が増加するため、端末の利用者を正しく判定し、それを相手に伝える技術の高度化が必要となる（認証技術の高度化）。端末には大量の情報が保管され、それらの情報を利用したサービスも増加するため、情報の安全な管理が必要となる（端末の持つ情報の安全な管理）。端末の利用者が拡大することから、購入後のアップデートに頼らない情報セキュリティ対策（製品組み込み型情報セキュリティ対策）、端末の利用者や利用環境に応じて、リスクの高い操作を防止するような技術（端末利用制限技術の向上）も重要となる。

- **不正プログラムに強い計算機環境**

マルウェア等の不正プログラムに対し、パッチなどの事後対策のみに依存せずに安全性を維持する計算機環境の実現。

例えば、事前登録など何らかの手段で安全性が確認された HW/OS/SW のみの動作を保障する技術（信頼性を担保する HW/OS/SW 技術）、正規のソフトウェアであることを認証したり確認したりする技術（ソフトウェアの正当性保証）が必要となる。また、新たな情報セキュリティ対策が必要となった場合に備え、新たなぜい弱性や攻撃の検出技術、パッチ等の対策を迅速に展開する体制（情報セキュリティ対策の運用管理）も重要となる。

・ **不正操作を予防する計算機環境**

プログラムなどが正当なものであっても、利用者の操作によってはリスクとなる場合がある。不正操作や攻撃などの検知、例えば、利用者の意図と異なる結果をもたらすような操作を排除するため、利用シーンに応じて操作を制限したり、操作の意図を推測したりする技術が必要になる。

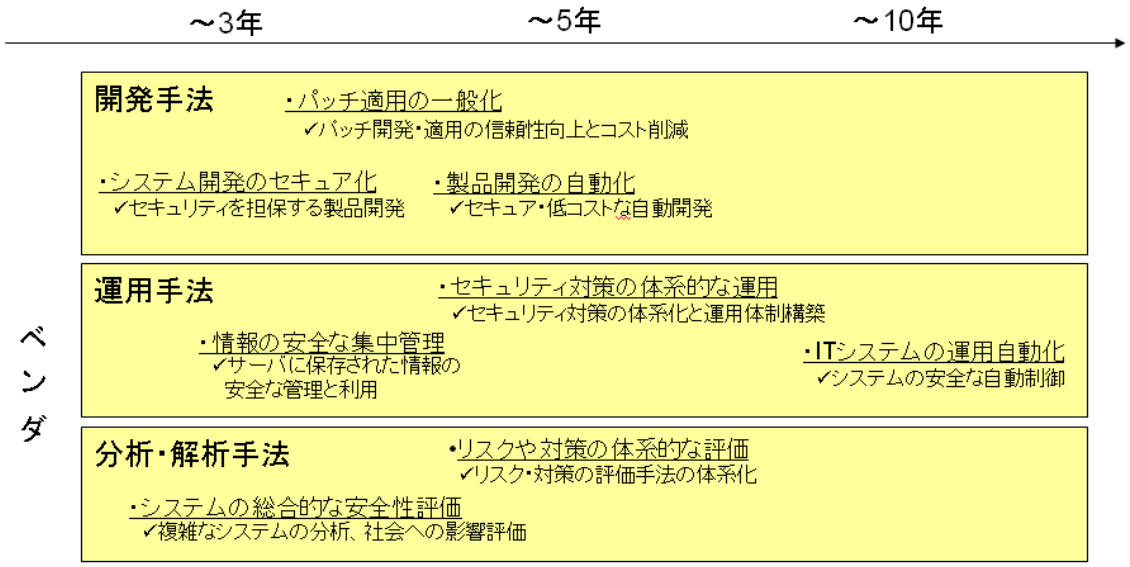

図２－３　「ベンダ」に係る技術潮流予測

「ベンダ」の領域における各将来像については、以下のように技術課題を整理した。

・ **システム開発のセキュア化**

製品開発の段階から情報セキュリティを確保するための手法が採用されるようになる。

例えば、設計・開発段階から情報セキュリティ対策を盛り込んだり（セキュアな開発手法）、過去に開発した製品についてのぜい弱性情報や設計情報をデータベース化して迅速なパッチ開発や新製品の設計に利用したり（開発実績の蓄積）、製品の運用中から廃棄までのライフサイクル全般にわたる情報セキュリティ対策の検討（製品のライフサイクル管理）、などが必要となる。

・ **パッチ適用の一般化**

ぜい弱性などが発見された際に、迅速にパッチを開発し、広く普及した端末に確実にパッチを適用するとともに、開発や適用にかかるコストを削減して

くことが課題となる。
そのため、例えば、パッチをある程度自動的に作成したり（パッチの自動作成）、パッチ適用などのソフトウェア更新を確実かつ低コストで実施する手法（高信頼・低コストな更新手法）の確立が必要となる。

・ **製品開発の自動化**

製品開発時のバグの作りこみや開発の手戻りなどを減らすため、セキュアかつ低コストな自動開発を行うことが課題となる。
そのため、例えば、形式手法を用いて自動的に実行コードの開発を行ったり（形式手法による開発技術）、仕様や製品の情報セキュリティを自動的に検証したりする技術（情報セキュリティの自動検証技術）が必要となる。

・ **情報の安全な集中管理**

端末の高度化により保管される情報が増加するが、同時に端末からサーバに蓄積される情報は今後も増大する。**サーバ側では、パーソナライズドサービス等のために個人ごとに特化した情報が**含まれることから、サーバに保存された情報の安全な管理と利用が課題となる。
例えば、クライアントからサーバに提供される情報の扱いなどのポリシーについて、クライアントとサーバとで適切なネゴシエーションを行ったり監視したりする技術（サーバ・クライアント協調）が必要となる。

・ **情報セキュリティ対策の体系的な運用**

情報セキュリティ対策を効果的に実施するため、情報セキュリティに関する基準やぜい弱性情報など、対策に関する情報の体系化、運用体制の構築が課題となる。
例えば、各種の情報セキュリティ基準など対策を統一的に扱うフレームワークを作成したり、標準化を行ったりすること（情報セキュリティ対策の体系化・標準化）が必要となる。

・ **ＩＴシステムの運用自動化**

ＩＴへの依存度の高まりと、システムの複雑化に対応するため、人的要因による情報セキュリティ侵害の発生や、人手に頼った情報セキュリティ対策からの脱却のための、ＩＴシステムの自動運用が重要となる。ＩＴシステムを安全に自動制御することと、サービスを止めないためにその可用性を確保することが必要であり、例えば、ＩＴシステムを管理しやすい単位に部品化し、相互接続の仕様などを標準化（システムの部品化・標準化）し、ＩＴシステムに障害が発生した場合にそれを自動的に検知し、ある程度自動的に復旧する技術（障害自動復旧技術）が必要となる。また、そのような運用自動化が

なされたＩＴシステムについて、システム全体の運用終了までを考慮したシステム設計（ライフサイクル設計技術）が必要となる。

・ **システムの総合的な安全性評価**

複数のシステムが相互に連携することが多くなり、複雑さを増す。個別システムの情報セキュリティ上の問題が他のシステムやシステム全体に与える影響、場合によっては社会への影響も分析評価することが重要になる。

例えば、システム同士が相互に与える影響を評価すること（システムの相互影響評価）、個々のシステムやシステム全体が内包するリスクの分析（システムのリスク分析技術）、システムの不具合等が社会へ与える影響の分析や評価（社会への影響の分析評価）などが課題となる。

・ **リスクや対策の体系的な評価**

優先して対策するべきリスクの明確化や、効果的・効率的な対策の選択を行えるようにするため、リスクや対策の評価手法の体系化が課題となる。

例えば、リスクを把握しやすく分類・整理したり、潜在的なリスクを明確化する技術（リスクの整理・抽出技術）、リスクや対策を重要度や効果、コストなどの指標によって評価しやすくするための可視化技術、対策の有効性を明確にするための評価技術（情報セキュリティ対策の定量評価）などが必要となる。

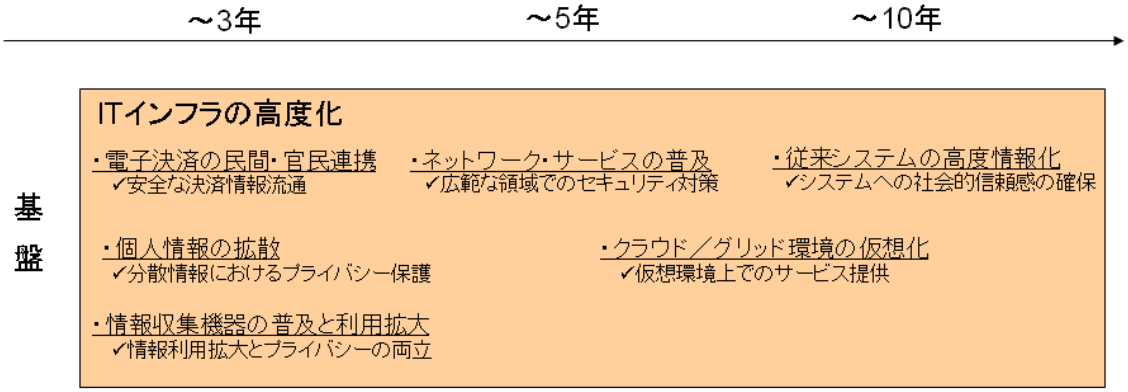

図２－４　「基盤」に係る技術潮流予測

「基盤」の領域における各将来像については、以下のように技術課題を整理した。

・ **電子決済の民間・官民連携**

民間の電子決済システム同士で連携したり、公的なシステムで民間の電子決済システムを利用するようになることも考えられる。その場合、システム同

士で決済情報を安全に流通させることが必要となる。
例えば、システム同士で異なる運用ポリシーを持つときに情報をどのように流通させるか（複数ポリシーの連携技術）、また、情報をポリシーに従って保護する手段（プライバシー情報保護[11]技術）などが重要となる。

- **個人に関する情報の拡散**

多種多様な機器がＩＴ化し、それを利用する利用者の個人に関する情報はあちこちの機器に記録されることになる。さらにネットワーク化が進み、ネットワークを介して収集した情報によるサービスが行われるようになるなど、個人に関する情報が広く拡散するようになる。このような分散的な環境における個人に関する情報の保護が課題となる。
例えば、個別の情報を匿名化してもサービス提供が可能なようにしたり（データマイニング技術）、利用者自身が自分の個人に関する情報の流通を制御できるようにしたり（利用者による個人に関する情報の制御）、分散環境のシステム間で情報のやりとりが必要な場合に個人に関する情報を保護する（分散環境での個人に関する情報保護技術）ことが重要になる。

- **情報収集機器の普及と利用拡大**

多種多様な機器のＩＴ化とともに、機器のセンサー機能も向上・普及し、そうして集められた情報の利用とプライバシー情報保護との両立が課題となる。
例えば、センサーで収集した情報をサービスに結びつける技術（センシング情報の利活用技術）と同時に、センサーで取得した情報をプライバシー情報を保護しつつ提供する技術が重要となる。

- **ネットワークサービスの普及**

ネットショッピングをはじめ、多くのサービスがネットワーク上で提供されるようになる。サービスごとに情報セキュリティ要件も多様であることが想定され、幅広いサービス領域で情報セキュリティ対策の実施が必要となる。
例えば、各サービス分野における情報セキュリティ要件や対策について適切な判断を行えるような人材の育成や、サービスがネットワーク化した際にどういった脅威が想定されるか分析を行う技術（脅威分析・検出）などが重要となる。

- **クラウドやグリッド環境の仮想化**

仮想環境が高度化し、サービス自体がネットワーク上に仮想的環境上に構築されるようになる。その一方で仮想化は、攻撃や障害の状況や原因を見えづ

11 プライバシーの概念は、自己の情報をコントロールすることができる権利を含んでおり、個人を特定できる情報（個人情報）の保護よりもマネージャビリティの要素が強いと考えて個人情報保護と区別している。

らくする要因となる。そのような環境下で安全にサービスを提供することが必要となり、例えば、構築された仮想環境でのサービスやシステムの状態管理、デバッグや情報管理等、仮想環境における情報セキュリティを維持する技術（仮想環境の情報セキュリティ確保）が課題となる。

・ **従来システムの高度情報化**

鉄道の自動改札やＩＴＳに代表されるように、既存のシステムの情報化が進展する。システムに対する社会的な信頼感を確保することが課題であり、例えば、システムで利用されている技術や運用制度に対する社会的な合意形成、技術的なシステムの安全性・信頼性向上といったことや、問題発生時に原因等の究明が可能であることが重要となる。

（２）情報セキュリティ技術の発展方向予測

導出された技術潮流予測において、例えば、ある将来像の実現が別の将来像の実現を促進する、といった将来像の間での関連を示すことで、技術発展の方向性について予測を行った。

図２－５（「利用者」に係る技術発展の方向予測）は、前述の技術潮流予測で各将来像について抽出した技術課題につき、その課題解決に必要と思われる要素技術を追記し、将来像の間の関連を矢印などで示したものである。

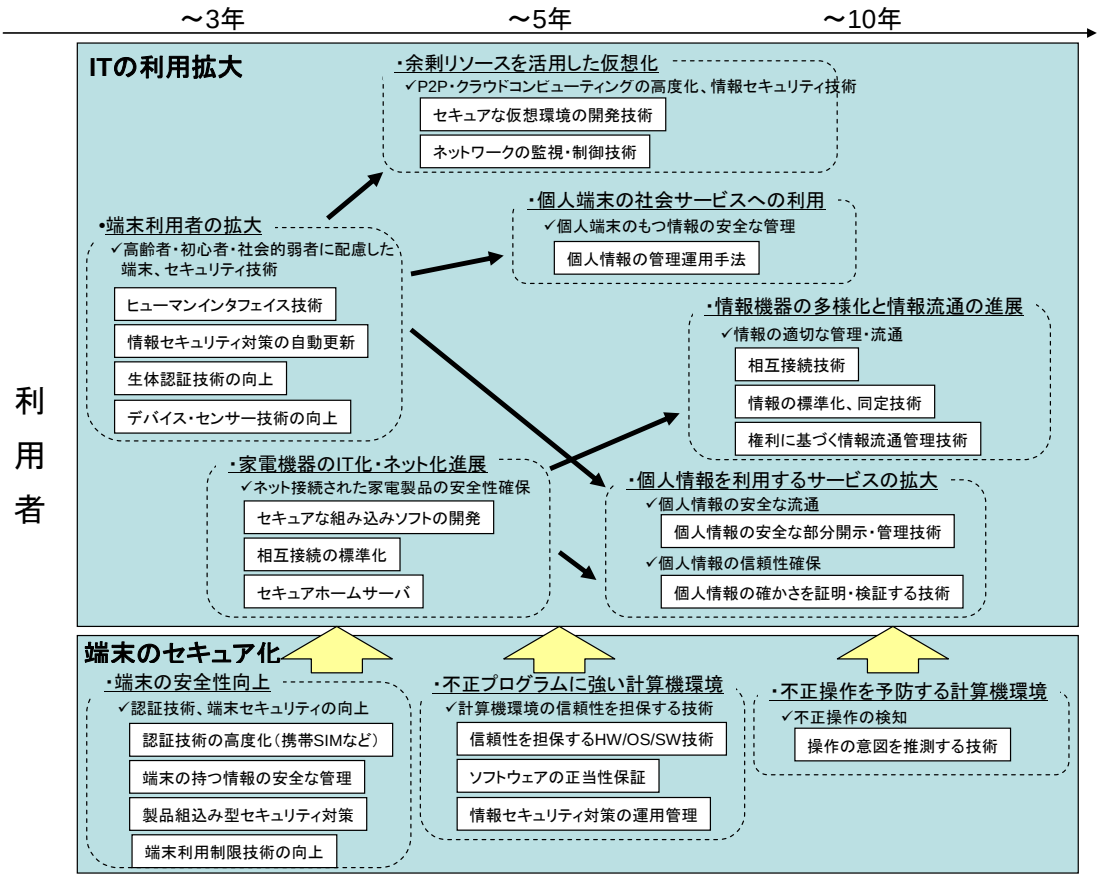

図２－５　「利用者」に係る技術発展の方向予測

「利用者」の領域については、全体として、「端末のセキュア化」の潮流が「ＩＴの利用拡大」の潮流を全般的に支えると考えられる。「ＩＴの利用拡大」の中では「端末利用者の拡大」により端末が普及し、「余剰リソースを活用した仮想化」「個人端末の社会サービスへの利用」「個人に関する情報を利用するサービスの拡大」といった将来像の実現を促進すると考えられる。また、「家電機器のＩＴ化・ネット化進展」によって生活の隅々までＩＴ機器が浸透することで、「個人に関する情報を利用するサービスの拡大」や「情報機器の多様化と情報流通の進展」につながると考えられる。

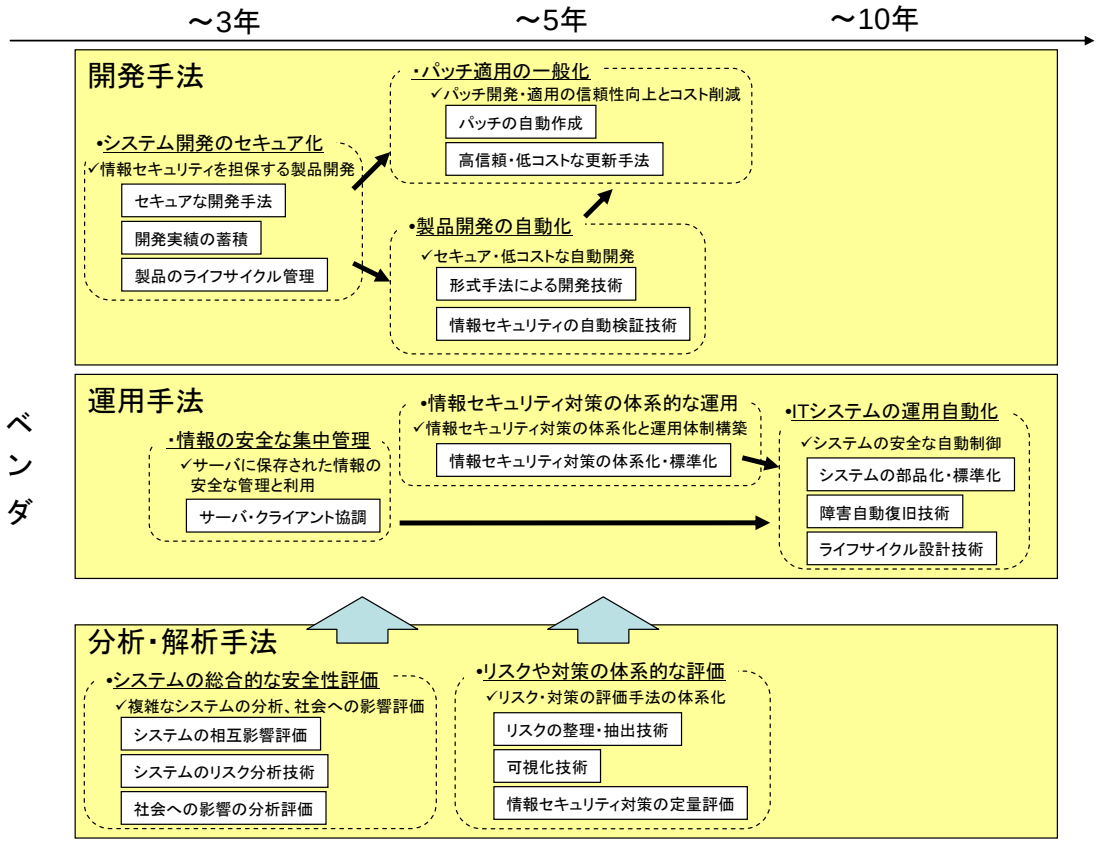

図２－６　「ベンダ」に係る技術発展の方向予測

「ベンダ」の領域については、「分析・解析手法」が「開発手法」「運用手法」を全体的に下支えすると考えられる。「開発手法」の中では、「システム開発のセキュア化」が「パッチ適用の一般化」「製品開発の自動化」について、ある程度の前提となり、「製品開発の自動化」の進展は「パッチ適用の一般化」を促進すると考えられる。
また、「運用手法」については、「情報の安全な集中管理」と「情報セキュリティ対策の体系的な運用」が実現されることが「ＩＴシステムの運用自動化」の実現に重要な前提となると考えられる。

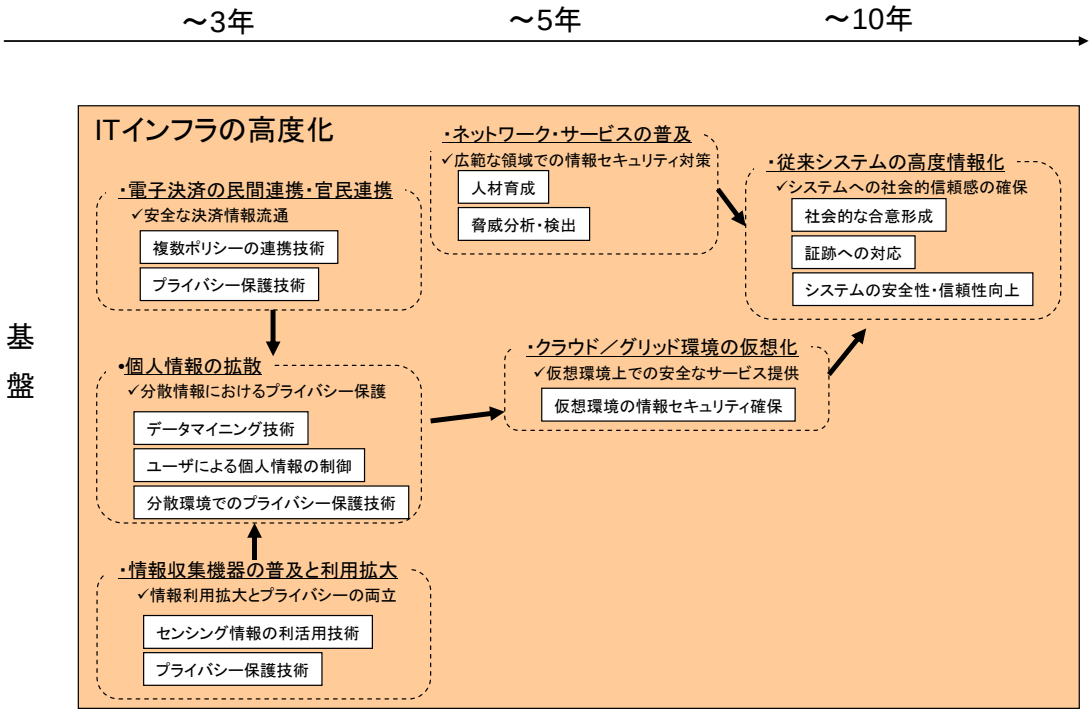

図２－７　「基盤」に係る技術発展の方向予測

「基盤」の領域については、「情報収集機器の普及と利用拡大」「電子決済民間連携・官民連携」の進展が「個人に関する情報の拡散」の進展を促進し、「個人に関する情報の拡散」により分散した情報を前提として「クラウド／グリッド環境の仮想化」が進むと想定される。また、「ネットワークサービスの普及」「クラウド／グリッド環境の仮想化」は「従来システムの高度情報化」を支える基盤となると考えられる。

（３）技術の大きな潮流予測

ここまでの技術発展の方向予測を再び俯瞰することで、「利用者」「ベンダ」「基盤」それぞれの領域について、以下のような大きな潮流があると考えられる。

「利用者」

家電などを含む多様な機器がＩＴ化し、利用者が広く一般に拡大するとともに、生活に密着したＩＴサービスが広く利用されるようになっていく。その一方でＩＴサービスのネットワーク化・仮想化が進展し、情報の管理や情報セキュリティ対策に一層の努力が必要となる。

このような状況で、機器やサービス自体の情報セキュリティの水準を向上させることに加えて、サービスの正当性や不正のチェックなど、リアルとデジタルの世界の感覚を共通化することで、一般の利用者がＩＴサービスを安全・安心に利用できるようにするための技術が必要とされる。

「ベンダ」

従来のパッチ適用に代表される事後的な対策だけでなく、設計開発段階でのリスク分析や形式手法による開発などの事前対策の強化が進む。仮想化の浸透している環境では、既存の手法では障害の原因の特定や対策が困難になるため、システムやサービスの状況の観測技術が発達している。また、外部のみならず内部犯行に対しても事後検証が可能な、耐タンパーなフォレンジック技術への必要性が高まる。その結果、システムの開発・運用・評価の各段階で手法の体系化が進み、最終的には、ある程度、自動的に開発・運用・評価を行い情報セキュリティを確保できるような技術が必要とされる。

「基盤」

生活に密着した IT サービスが広く利用されるようになる中で、IT サービスにおいて扱われる個人に関する情報・企業情報が飛躍的に増加する。さらに、ネットワーク化・仮想化の進んだ IT 基盤の上で多くの社会サービスが提供されるようになり、個人に関する情報・企業情報の適切な管理に限らず、システムの安定性・安全性に対する社会的な信頼感を確保することが必要とされる。具体的には、通信やサービスの基盤には現代よりはるかに高い信頼性が求められると同時に、ボットやルートキットなどの見えない脅威など、これまでの方式では解けない問題への対策が重要となっている。また、仮想化によって、データの実際の存在位置が不明確になることに対して、安全な場所に保管するための方式の確立も必要となる。

２．３　情報セキュリティ技術のグランドチャレンジ型研究分野の方向性

今後は、２．１で検討した「社会の将来ビジョン」と２．２で検討した「技術潮流予測」に基づきつつ、グランドチャレンジに関する具体的なテーマ、研究開発対象となる具体物、そしてそれらを構成する情報セキュリティ技術について早急に検討・確定するべきである［開発面］。その際には、グランドチャレンジプロジェクト全体の管理や進め方、とりまとめ方についても併せて検討を行うことが不可欠である［管理面］。

なお、２００８年度のグランドチャレンジに関する新しい検討WGにおける議論も踏まえると、開発面に関する検討を行う中で、例えば、今年度の検討によって得られた以下のような方向性も重要となってくると考えられる。なお、いずれの要素技術においても、世界をリードできるような**「最先端性」**を満たす技術であることが重要であるのは言うまでもない。

・「安全・安心な生活、社会経済活動」や「グローバル・ユビキタス」を実現するべく、日常の生活、社会経済活動に浸透したＩＴ機器の情報セキュリティ確保に係る技術

今後、家電や携帯端末、ゲーム機器などの生活に密着したＩＴ機器を用いた、個人ごとに特化したサービスの提供が増加すること、さらにそれらのサービスは時間や場所の制約が従来よりも遥かに少なくなり、まさにシームレスになることが予想される。こうしたサービスは、個人的な情報を扱うために社会的な信頼感が特に求められると考えられることから、プライバシー情報保護や個人に関する情報の流通制御のための技術や、システム全体で情報セキュリティの水準を維持するための高水準のリスク評価技術や運用管理技術などの実現が重要となる。

・「当然化」を実現するべく、一定の情報セキュリティ水準が確保されたプロダクトを設計開発する手法および技術

一般の利用者がＩＴ機器やＩＴを活用したサービスを安全・安心に利用できるようにするため、設計開発段階から情報セキュリティを作りこみ、煩雑な操作やカスタマイズなどを行わなくとも、常に一定の情報セキュリティ水準が確保されたプロダクトを設計する手法や技術の開発が重要である。[12]

---

[12] 現在の情報セキュリティ対策では、ソフトウェアのパッチ適用に代表されるように、プロダクト（ソフトウェアだけでなく、ハードウェアやサービスシステムなども含む）の販売後に事後対策として行われる対策が多く見受けられる。しかし、今後、様々な機器がＩＴ化・ネットワーク化し、対策の対象となる機器や利用者の数も拡大するにつれて、対策の展開速度やコスト等の面で、事後対策だけでは不十分となってくることが予想される。また、攻撃にさらされていることに気付きにくい高度なインシデントへの対策・対応という面からも事後ではない対策が求められる。
そのため、一定の情報セキュリティ水準が担保されたプロダクトが確実に提供され、事後対策への依存を減らすことが必要になると考えられる。プロダクトの設計段階から運用、廃棄までのライフサイクルを通して、一定の安全性が確保されるような開発・運用体制を構築することが必要になる。

・「適切性」を実現するべく、利用シーンに応じて動的に情報セキュリティ水準を最適化するような技術・システム

現在の多くのＩＴシステムは、高い安全性が必要な状況でも、そうではないときも似たような操作感・システム環境である場合が多い。このため、誤認・誤操作による事故が発生したり、逆に利用者が必要以上に警戒することなどにより、結果的に利用者の混乱や生産性の低下、システムへの信頼感の低下を招いている面がある。この状況を解消するため、製品やサービスの種類あるいは利用環境等に応じて必要な情報セキュリティ水準を柔軟に確保するための技術的対応が必要である。例えば、利用シーンに応じて動的に情報セキュリティの強度や操作感などを変化させ、危険度のレベルを利用者に直感的に認識させるなどによって、リアルとデジタルの世界の感覚を共通化し、情報セキュリティ水準を適切に維持する技術やシステム環境が例の一つとして挙げられる。[13]

・「マネージャビリティ（可管理性）」を実現するべく、人間がリスクをコントロールできることで安心して情報を管理できるような技術（例えば、高度に仮想化が進展したネットワークに関する技術等）

人間の生活や業務のＩＴへの依存度がさらに高まることによって、自身に関係する情報やサービスの管理も必然的にＩＴから切り離せなくなってくる。これらの情報やサービスの管理や監視を全てＩＴ任せにするのではなく、自身の意思と判断に基づいて主体的に行いたい部分に関してはその意図を反映させ、ＩＴの客観的な安全性を向上させるべくリスクをコントロールできる技術が重要となる。

[13] 現在は、単純なウェブ閲覧を行っているときも、ネットショッピングや在宅業務を行っているときもほぼ同様の環境で作業が行われることが多い。そのため、利用者の誤認・誤操作や単純なウェブ閲覧中のウイルス感染等を原因として、パスワードのような重要な情報の流出が発生し、また必要以上に情報セキュリティ水準が高く効率的でない環境で作業を行うような事態が生じている。こうした状況が、ＩＴシステムに対する信頼感の低下の一因ともなっていると考えられる。このため、「常識的に」利用していれば安全に利用できる技術・システムが重要となっていると言える。

３．公的資金を用いた中長期的な研究開発の実施方法

３．１　公的な競争的資金制度に関する論点

研究者が研究開発を進めるための研究費には複数の形態が存在するが、本報告書においては、研究者からの申請書の内容と実施能力に関する評価に基づいて採択が決定される、競争的資金に関して主に検討を行なった。

情報通信分野では、技術の進歩や環境の変化が特に激しいため、プロジェクトの実施期間中に研究を取り巻く状況が研究者の予期してなかった方向に変化することがある。その結果、競争的資金を活用した研究開発においては、研究者自身が作成した研究計画を見直さざるを得ない場合が少なくない。本報告書において、特に競争的資金を用いた研究開発に着目し、検討したのはこの特性による。

３．１．１　研究者側の問題提起

研究開発にかかわる研究者から、プロジェクト管理・運用体制に対して、以下のような問題提起が報告されている。

（１）問題提起

【問題提起１】　計画変更の柔軟化とリファクタリングの必要性

一般的には、最終的な目標から要素還元的アプローチによって策定した研究計画を作成する。中間評価／事後評価では、計画に沿った実施が行われているかについて、非常に厳密な検証が行われる。さらに、新たな状況変化が認識されても、計画自体への変更が非常に困難、ないしはほぼ不可能な場合がある、という問題提起である。

このような管理体制では強い拘束力が発生し、硬直的な計画実施となる。ただし、短期的な研究開発、あるいは目標が非常に明確な開発ならば有効だが、研究開発の分野やテーマによっては、３年間は短期とは言えない場合も多い。

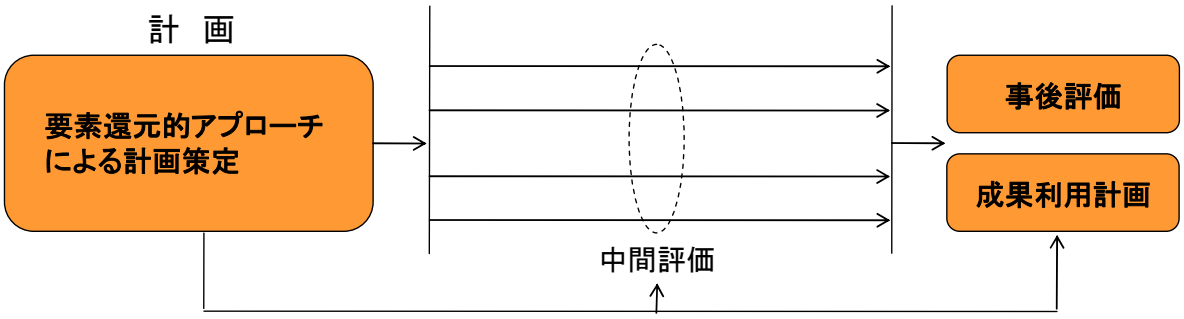

図３－１　現在の研究開発プロジェクト管理体制

中長期的な研究開発プロジェクトでは、リファクタリング（大きな目標を実現するために、状況の変化を評価しつつ途中の目標を動的に見直すこと）[14]を常時行い、計画に反映させるべきとの意見が多かった。

（提案）

・社会情勢変化、技術革新の影響を、同じ研究プロジェクト内で評価し、動的な計画変更を実施し、研究開発投資の効果の最大化を図る。

・大目標は維持しつつ、社会要請に的確に応える体制作りが必要。

【問題提起２】　途中段階で得た成果利用プロセスの独立

当初の研究計画で定めた成果利用計画のみにとらわれることのない、社会ニーズに合致した成果活用プロセスを探求すべきである、という問題提起である。得られた成果を積極的に活用するための独立した手順設計を行い、様々な視点から検討すべきであるという意見が多かった。

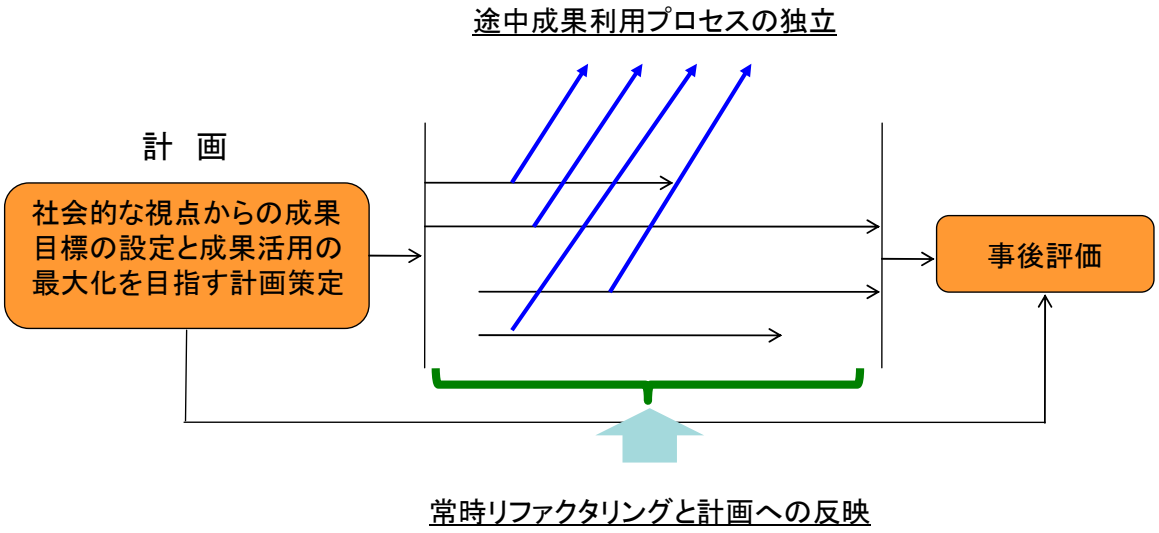

図３－２　プロジェクト管理・評価体制改善のイメージ

[14] 科学技術振興機構の平成 19 年度業務実績報告書（平成 20 年 6 月）によると、同機構の競争的資金である戦略的創造研究推進事業では、「研究計画、研究体制の見直し等」が 10 件、「研究費の増額および研究計画、研究体制の見直し等」が 6 件あるとされている。

（２）情報セキュリティ分野でこの問題を論じる必要性

このような問題意識は、特定の研究分野に限ったものではないが、ＩＴ分野、特に情報セキュリティの研究者からの意見が多い。その原因として以下のようなものが考えられる。

・情報セキュリティ課題解決は、“moving target”型課題解決である
- リスクが変容することによって、目標は動的に変化していく
- 新たな技術の登場によって、リスクの変容が発生する
- 攻撃側と防御側の非対称性が存在する
- 上記の原因が複合的に働くことで、課題を取り巻く環境の変化が激しい（例：2 年前のリスクが、現在はリスクではないようなケースが多発している。）

・究極の目標は、実は大きな変化は少ないことが多い
究極の目標の例：- 情報資産と情報処理の保護
- 事業継続性の円滑な確保

・社会要請によって研究開発内容は変化するが、しかし、同時に短期間では解決できない課題が多い
（例）プライバシー情報保護に資する技術、サービスの正当性を保証するための技術など

このように情報セキュリティは特殊性の高い研究分野であるが、ＩＴに係る研究開発には情報セキュリティ技術の課題が不可分に組み込まれている場合が多い。また、情報セキュリティ技術のみに特化した競争的資金制度が存在しないことから、以降の議論では競争的資金制度一般に関しての現状を踏まえつつ、情報セキュリティ技術を含む IT 技術分野全般に関する研究開発を行うにあたっての改善の方向性について検討している。

３．１．２　公的な競争的資金制度の現状と改善状況

研究開発プロジェクトの管理・運用・評価を行う側においても、管理ルールとその運用について、継続的に問題点の把握と改善の努力がなされているところである。こうした改善のうち、ここ１～２年になされたものは、現場の研究者まで浸透していないケースがあると言われている。

他方、政府資金の適正な使用の要請や競争における公正性などから生じる制約は残す必要があるとされている。

（１） 公的な競争的資金に係る制度・ルールの階層構造

公的研究費の使用に関する制度・ルールは、一般的に次のような階層構造[15]となっている。

① 法令レベルによる規制

財政法、会計法、補助金等適正化法、独立行政法人通則法などの法令による規制がある。国（府省）が直接助成する場合においては、こうした法令の規制が直接及ぶことになるため、柔軟性を欠くとの批判もある。

② 各研究費制度レベルの問題

(a) 各研究費の個別制度による規制

各研究費は個々の制度ごとに予算を所管する府省・資金配分機関が定める使用・管理・報告等に関するルール・手続きが存在している。競争的資金等の不正使用防止のために、各制度間で機関内の責任体系やルールの明確化を統一的に推進することの必要性が指摘[16, 17]されているが、このような取組みは不正使用防止の目的のみでなく、広く資金制度の改善に資すると考えられる。この階層における諸問題は後述するように多くの点で改善が進んでいるが、計画変更の手続き、承認権限などの点で不明確な部分が残されている。

(b) 資金配分機関のプロジェクト管理・評価関係者の裁量・判断（プロジェクト管理・評価体制）

前述の問題提起にある柔軟な計画変更については、プロジェクトマネージャーや計画の進捗状況を管理する委員会レベルの判断が硬直的ではないかとの指摘があった。この問題については後で検討を行う。

③ 各研究機関レベルの問題

(a) 研究機関の独自ルールによる規制

大学などの研究機関が定める独自のルールについては、研究機関間での情報交換等により、それぞれが改善の努力をしていくべきものである。

---

[15] 文部科学省　「研究費の使用ルールの階層構造」（研究機関における公的研究費の管理・監査に関する検討会　第 8 回配布資料）
[16] 文部科学省　「研究費の不正対策検討会報告書」（平成 18 年 12 月 26 日）
[17] 総合科学技術会議　基本政策推進専門調査会　「競争的資金の拡充と制度改革の推進について」（平成 19 年 6 月 14 日）

(b) 研究機関の担当者等の裁量・判断

資金配分機関の担当者においても同様のケースがあり得るが、補助条件等を保守的に判断し、結果として計画変更等の柔軟性を失っている場合があると言われている。その原因として、特にルールがわかりにくい、十分な周知がなされていない、相談窓口がないことなどが背景となっているとの意見がある。

（２） 会計制度の制約と資金使用の柔軟化への努力

計画変更の柔軟化そのものではないが、年度内使用制限の緩和など、資金の使用に当たっての柔軟化により、結果的に、実施時期等の計画変更が可能となるとされている。

特に研究費の不正使用の発生を背景として、その防止策とともに不正使用を誘発する要因となった競争的資金等の制度・運用上の問題解決[18]という観点からの努力がなされている。

① 単年度会計主義[19]に関する改善

年度単位[20]で予算の執行を行う必要がある単年度会計主義は、研究の進展に応じて臨機応変の対応が求められる研究活動の性格に必ずしも適合していないとの指摘があり、他方、米国の公的研究資金には、研究機関内であれば会計年度を越えて研究費を使用できるものがあることから、わが国での改善が求められていた。

現在では、繰越明許費制度[21]の活用が推進されており、例えば、文部科学省・日本学術振興会の科学研究費補助金においては、平成 15 年度から繰越明許費として登録され、さらに平成 18 年 4 月の繰越事由の明確化及び繰越し事由の具体例の充実[22]により、大幅に利

---

[18] 同省　「研究費の不正対策検討会報告書」（平成 18 年 12 月 26 日）

[19] 予算の単年度主義
日本国憲法第８６条 内閣は、毎会計年度の予算を作成し、国会に提出して、その審議を受け議決を経なければならない。

[20] 会計年度独立の原則
財政法第１２条 各会計年度における経費は、その年度の歳入を以て、これを支弁しなければならない。
財政法第４２条 繰越明許費の金額を除く外、毎会計年度の歳出予算の経費の金額は、これを翌年度において使用することができない。但し、（中略）年度内に支出負担行為をなし避け難い事故のため年度内に支出を終わらなかったもの（中略）は、これを翌年度に繰り越して使用することができる。

[21] 財政法第１４条の３　歳出予算の経費のうち、その性質又は予算成立後の事由に基づき年度内にその支出を終わらない見込のあるものについては、予め国会の議決を経て、翌年度に繰り越して使用することができる。
② 前項の規定により翌年度に繰り越して使用することができる経費は、これを繰越明許費という。

[22] 例示としては、
・研究を実施していくなかにおいて、○○の事象が生じたことで当初予定していた成果が得られないことが判明したため、当初の研究計画を変更する必要が生じた、
・研究の進展に伴い、当初予想し得なかった新たな知見が得られたことから、その知見を使用し十分な研究成果を得るために、当初の研究計画を変更する必要が生じた、 など

用が増加[23]している。

なお、年度を超えた研究期間の確保や複数年度にまたがる研究費の使用について、中長期的課題として提起されているところであるが、既に制度として可能となっている戦略的創造研究推進事業[24]もあり、中長期的な研究においては、このような改善の普及が望まれる。

② その他の資金使用面での改善

総合科学技術会議の基本政策推進専門調査会「競争的資金の拡充と制度改革の推進について」（平成 19 年 6 月 14 日）においては、競争的資金の改善の方向性として、資金制度間の連携の強化、ルールの共通化、研究期間を実質的に延長できる「更新制」の拡大、研究資金の交付時期の早期化、間接経費 30%化の早期実現、研究費の複数年契約の拡大などが謳われており、この提言に基づいて改善が進行しているところである。例えば科学研究費補助金や戦略的創造研究推進事業など幾つかの制度では、これに先立って多くの改善[25], [26]がこれまでもなされている。

（３） 採択後の研究計画変更に係る制約（公正競争等の問題）

---

[23] 文部科学省科学研究費補助金における繰越明許費の利用状況
平成 15 年７月 研究振興局長・会計課長通知
平成 15 年度 ２４件　　平成 16 年度 １０件　　平成 17 年度 ５５件
平成 18 年４月 研究振興局長・会計課長通知
平成 18 年度 ６４１件　　平成 19 年度 １２９７件

[24] 「戦略的創造研究推進事業（ＣＲＥＳＴ・さきがけ・発展）大学等向け・複数年度契約用委託研究契約書」

[25] 文部科学省「科研費の『経費執行の弾力化』に関するこれまでの制度改革」

[26] 以下は、文部科学省・独立行政法人日本学術振興会「科学研究費補助金制度について」（平成 20 年 9 月）より引用。

・研究分担者への間接経費の配分
　研究代表者と異なる研究機関に所属する研究分担者に、当該研究分担者が使用する直接経費の３０％相当額の間接経費を配分することとした。
・合算使用の制限の緩和
　一つの契約で１個の消耗品等を購入する場合に、科研費の研究に使用する数量と他の用途に使用する数量を分割して、科研費の研究に使用する数量分について直接経費を使用することができることとした。
　直接経費に、委託事業費、私立大学等経常費補助金、他の科研費及び間接経費など、当該経費の使途に制限のある経費以外の経費を加えて、補助事業に使用することができることとした。
・直接経費の使用内訳の変更
　直接経費の各費目において、自由に変更できる直接経費の割合を「３０％」から「５０％」に引き上げた。
・自己評価報告書の作成・提出
　研究期間が４年以上の研究課題（一部研究種目等を除く）について、研究期間の３年目にあたる研究課題の研究代表者は、自己点検による中間評価を実施し、翌年度の実績報告時に、自己評価報告書を提出することとした。
・新たな様式による研究成果報告書の作成・提出
　平成２０年度が研究期間の最終年度に当たる研究課題（一部研究種目等を除く）から、研究成果報告書を従来の冊子体から、数枚の様式に変更した。また、新たな様式により作成・提出された研究成果報告書については、国立情報学研究所においてデータベース化し、インターネットで公表することとした。

現在の競争的資金等による研究の多くは、事前に申請した研究計画・資金計画通りに進めることが前提であり、変更に制約があることが多い。原則的には、公募により事前に提出された計画を審査して、優れたものに資金が与えられるものであり、採択後に研究計画等を変更することは、資金獲得競争の審査過程において勝敗を決めた根拠を覆す面があるためである。資金配分側の立場からは、競争の公平性を保つために変更については慎重でなくてはならないと主張されている。

また、研究者側も、自己のテーマが採択されやすいように、申請内容を具体的に書き込む傾向があり、これも柔軟性を損なわせる原因の一つとされている。

しかし、研究の進展によっては、当初予定しなかった方向に変更する必要が生じることがある。例えば、当初目指したものよりも良い方向が発見されたり、環境の変化により当初目指したものの価値がなくなったりすることがあり得る。

こうした場合には、研究の進展に応じた計画の変更を柔軟に認めることが資金の有効活用の観点から必要である。公正競争とのバランスからは、変更を認める時点や研究終了後の審査・評価や、研究費の使途のチェックが重要となってくる。なお、科学技術振興機構の競争的資金である戦略的創造研究推進事業[27]では、中間評価時に「新たな方向性や方針変更等、当初計画では想定されていなかった新たな展開が生じたか。」を評価項目に導入するなど、柔軟な計画変更を是とした取り組み[28]を先駆的に行っている。

研究計画等の変更が真に必要かつ適切なものであるか、あるいは研究者の怠慢・努力不足に由来するものであるか、見極めなければならないと考える。公正競争の問題のみならず、原資が税金である以上、国民の信頼に応えるために適正な使用が求められるからである。計画変更時・研究終了時の評価等については、プロジェクト管理そのものの問題であり、次で検討を行うこととする。

３．２　プロジェクト管理・評価体制の改善の方向性

今回、問題提起された、①柔軟な研究計画・資金計画変更、②途中で得た成果利用プロセスの独立の２点を可能とするプロジェクト管理・評価体制のあり方について、ここで検討する。

（１） プロジェクト管理・評価体制の現状

総合科学技術会議「競争的資金制度改革について（意見)」（平成 15 年 4 月 21 日）において、資金配分機関におけるプロジェクト管理について、プログラムオフィサー（ＰＯ)、

[27]科学研究費補助金に次ぐ予算規模の戦略的創造研究推進事業では、本文中に記載した先駆的取り組みの他、配分機関に返金することなく年度をまたがった予算繰越を可能としており、また、直接経費の各費目において、自由に変更できる直接経費の割合を科学研究費補助金と同様に「３０％」から「５０％」に引き上げるなど、不断の改善が行われている。

[28] 独立行政法人科学技術振興機構「平成 19 年度業務実績報告書」の「Ⅰ.1.新技術の創出に資する研究」において、中間評価結果を受けて研究体制や資源配分の見直しを行った例が記載されている。

プログラムディレクター（ＰＤ）[29]による一元的な管理・評価体制の整備が必要であり、米国はじめ諸外国の配分機関のように、外部専門家に加えて、研究経歴のある多数のＰＯやＰＤを擁し、プログラムの計画から、最後の評価の段階まで一貫してマネジメントする体制を徹底すべきであるとされた。

現在多くの資源配分機関にＰＯ、ＰＤが置かれているが、問題点として、上記の総合科学技術会議の意見において、

- 人数の面でも、また、雇用形態(非常勤、大学等からの併任等)等制度の位置付けの面からも、必ずしも十分とはいえない状況
- ＰＯ・ＰＤ の具体像が明確でないため、制度間でＰＯやＰＤの役割に関する理解にばらつき
- ＰＯやＰＤという職務が、研究者のキャリアパスとして確立されていないため、質および量の面での確保の困難

という指摘がなされており、これらは現在でも引き続き課題として認識されている。

このような現状から、本専門委員会・グランドチャレンジ検討ＷＧでの報告書をまとめる議論において、適切な進捗状況や予算執行の把握、研究計画の変更に係る提言が実現できていない、変更を認める権限が必ずしも明確でないという指摘がなされている。

また、上記総合科学技術会議の意見では、公正な評価の確立の観点から、厳正な利害関係の排除が求めているが、本専門委員会・グランドチャレンジ検討ＷＧでは、当該研究プロジェクトの本来の意味での専門家が不在となり、適正な評価が不可能になるのではないかという指摘もなされている。

（参考）

図３－３に「研究開発プロジェクト管理・運営体制のモデル」の一例を示す。本

[29] 同意見におけるＰＯとＰＤの基本的役割は次のとおり

ＰＯの基本的役割

- プログラムの方針(案)(目的、目標、重点テーマ、新規テーマ設定)の作成
- 評価者の選任。
- 外部評価（ピアレビュー）に基づき、採択課題候補(案)の作成(優先順位付け、研究費の査定、研究分担者の必要性、重複の排除)
- 評価内容や不採択理由の開示。それに対する申請者からの質問、不服申立への対応。
- 採択課題について、研究計画の改善点の指摘。不採択の申請者にも助言
- 進捗状況や予算執行の状況を把握。必要に応じて、現地調査
- 研究計画の変更(中止・縮小・拡大を含む)の提言
- プログラム全体の運営見直し等の提案

ＰＤの基本的役割

- 競争的研究資金制度におけるマネジメントシステムの向上
- プログラムの方針決定。新規プログラムや新規領域設定を決定
- 各制度内の領域間・分野間・プログラム間等の資金の配分額や配分方式(個人研究とグループ研究等)を決定
- プログラムオフィサー間の調整
- 採択課題の決定
- プログラムオフィサーの評価

モデルにおいては、研究開発プロジェクトは、次のように管理・運用されている。

プロジェクトの採択時に、審査委員会が提案書（実施計画案）の内容を評価し、提案の内容が公募の目的に適ったものかどうかを判断する。

プロジェクト管理業務を委託された資金配分機関が、採択された提案を実施する実施チーム（実施機関と協働機関を含む）と契約締結など経理的な処理を行なう。

実施チームは、推進委員会を組織して状況の管理、調整を行う。プロジェクト終了時には、評価委員会が実施計画と照らして成果の評価を行う。

資金配分機関におけるプロジェクト管理は、個々のプログラムを担当するＰＯ、研究領域毎にプロジェクトを担当する専門性の高い非常勤ＰＯ、契約や会計などを管理するＰＯ補佐によって遂行される。推進委員会には、プロジェクトの関係者の委員から成る運営委員会と、外部有識者から構成される諮問委員会の２種類があり、運営委員会はプロジェクトの潤滑な推進を図ることを、諮問委員会は計画の実現状況を評価することをそれぞれ目的とする。

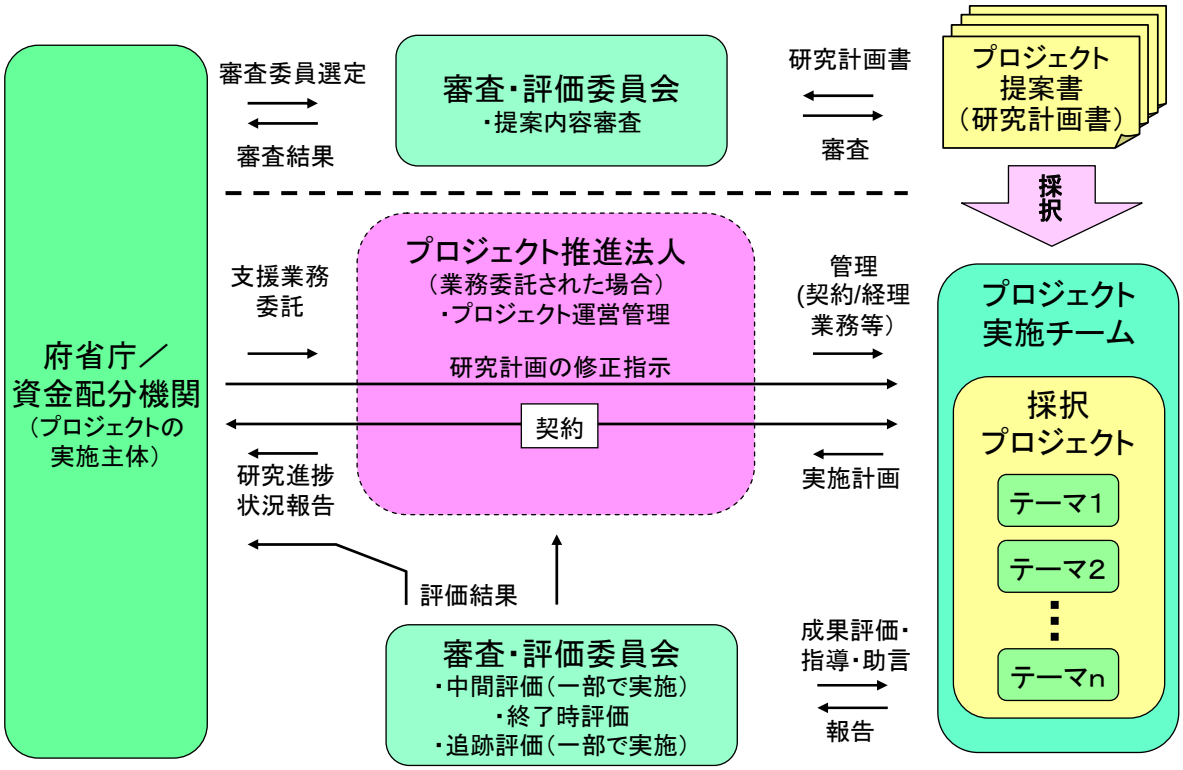

図３－３　研究開発プロジェクト管理・運営体制のモデルの一例

（２）　プロジェクトの管理・評価に関して生じる問題と解決の方向性

本専門委員会としては、プロジェクト管理・評価の問題と理由を以下のように推定し、これらの問題を本質的に解決するためには、ＰＯを含む資金配分機関側の評価体制を拡充し、計画変更を判断する時点や研究終了後の審査・評価や、研究費の使途のチェックを適切に行うことが重要であると考えている。

（ａ）年次計画の精度

問題：予算や契約は単年度なのに、プロジェクト開始時の計画に要求される粒度が１年目も３年目もほぼ同じ。
→ 長期的な部分の計画の精度は非常に悪くなる。

理由：プロジェクト採択時の審査は、最終的な成果予定まで含めて行なわれるので、最終年度まで詳細な計画が求められる。

改善の方向性：研究者及び資金配分機関側において、研究途中での当初計画の見直しを行い、常に精度の高いものとしておく。見直しする際に、研究の方向性や資金計画変更の必要性についてもよく検討する。あるいは、戦略的創造研究推進事業で取り組まれているように、中間評価時に「新たな方向性や方針変更等、当初計画では想定されていなかった新たな展開が生じたか。」を評価項目に導入するなど、柔軟な計画変更を行える先駆的な取り組みを検討する。

（ｂ）計画実施の硬直性

問題：プロジェクト開始時の計画に沿った実施が基本で、厳密な検証が行なわれる。
→　新たな状況変化が認識されても、計画の変更や中断はほぼ不可能。

理由：・省庁・資金配分機関側の規則や要領には明示的な記載がないものがあり[30]、資金配分機関の運用が硬直的
となっている。また、計画変更を判断する委員等の選定の制約がある。
→　プロジェクト実施チームと利害関係のないＰＯや委員等を選ぼうとすると、その分野の第一線の研究者・技術者を排除する可能性が高くなる。
・変更を認める場合の公正競争上の問題と権限の所在

[30] 当初の実施計画書に記載された内容の変更手続きが公募要領に記されておらず、変更できるか否かは不明確であるが、プロジェクトの置かれた環境の変化によって計画を変更する必要性が高まった場合には、運用上は諮問委員会に諮り承認を得ることで計画の修正が可能な例もある。

→　計画変更を認めるということは、プロジェクトを採択した審査委員会の決定を覆すことになり、公正競争上の問題、計画変更の権限の問題が生じる可能性がある。

改善の方向性：資金配分機関において、処遇等の改善を通じて、できるだけ対象研究領域に知見を有し、変更を認める時点での評価、研究終了後の事後評価、資金の使用状況の審査を適切に行える人材を確保[31]する。

また、ＰＯ等の担当者に対し、計画変更の要望があった際は、それを判定するための場（例えば有識者による委員会）を組織するなど、研究の進展等に応じて柔軟に計画変更するための仕組みを、資金配分機関内に設け、必要な場合においても計画変更を承認しない場合の不服申立て制度について検討する。

（ｃ）途中段階での成果活用の障害

問題：プロジェクトの中間成果やノウハウを、外部から知り、入手する手段がない。

→　プロジェクト完了時にまとめて成果が公表されるので、プロジェクト初期の成果は時代遅れになり、結果的に活用も困難となる。

理由：・ 中間成果を公開する仕組みや体制がない。

・ 資金配分機関も実施チームも、競争者に対して研究の秘密を守る等の観点から、中間進捗をあまり公表したくない。

・ 他のプロジェクトの成果を活用する際の権利や制約等に関する規約が無い。

改善の方向性：

・中間成果の扱いについて、研究開発計画等で定めるようにルール化を検討する。

・研究者が望む場合には、研究開発データベースなどを活用し、中間成果を公表できる体制を整備する。

・知的財産権上の扱い等、中間成果を活用する際の開発者と利用者の権利についてのルールの明確化[32]を検討する。

・成果を活用する側と研究実施者でニーズとシーズをすり合わせる機会を検討する。

・研究開発成果の実装へのつなぎ部分に係る支援策を検討する。

---

[31] 「国の研究開発評価に関する大綱的指針」（平成 20 年 10 月 31 日　内閣総理大臣決定）は、評価人材を養成・確保するよう努めることとしている。

[32] 戦略的創造研究推進事業では、中間評価結果の扱いについて、ルール化しており、知的財産権の取扱に配慮しながら、既に全課題の中間評価結果がインターネットで公開されている。

４．まとめ

４．１　情報セキュリティ分野のグランドチャレンジにつながる研究開発の方向性

グランドチャレンジ型研究開発・技術開発の取組みの具体化に向けて、本年度は技術戦略専門委員会の下にグランドチャレンジＷＧを設置し、本委員会と双方で集中的な検討を行った。その過程では、ニーズ指向アプローチ（実現すべきことから考える、帰納的な「将来の社会ビジョンに関する検討」）、シーズ指向アプローチ（今後の流れを予測しながら考える、演繹的な「技術の潮流予測」）の双方の観点からの検討を経て、今後、グランドチャレンジに係るテーマ、研究開発対象となる具体物、そしてそれらを構成する情報セキュリティ技術についての検討を進める際に、重要となると考えられる方向性の例の検討も行った。

今後、少なくとも２．１（２）で挙げた「主たる要素」を満たしていけるようなテーマ選定を早急に進め、我が国全体として大きな方向性を持って研究開発・技術開発を進めるべきである。また、グランドチャレンジの取組みにおいては、エンドユーザーの視点に立ち、実現されると望ましい情報セキュリティ技術が化体した具体物、すなわち「New Secure Product[33]（仮称）」の開発を実現する方向で進めるべきである。そして、この取組みを通じて、情報セキュリティに係る問題の解決が進むとともに、技術の観点から我が国が世界をリードし、世界に誇れる状況を実現するべきである。また、開発過程における関連分野への波及効果も確実に実現すべきである。

４．２ 研究開発プロジェクト管理・評価体制に関する提言

今回、取上げた（１）研究状況に応じた研究計画・資金計画の柔軟な変更、（２）途中段階で得た成果利用プロセスの独立の２つの問題提起に対し、プロジェクト管理・評価体制の改善の方向性は次のとおりと考えている。

（１） 研究状況に応じた研究計画・資金計画の柔軟な変更

第一に、年次計画の精度について、研究者及び資金配分機関側において、研究途中での当初計画の見直しを行い、常に精度の高いものとしておくこと。あるいは、複数年の研究計画は粗い粒度で立て、詳細計画は毎年設定できる形態とすること。

第二に、資金配分機関において、処遇等の改善を通じて、できるだけ対象研究領域に知見を有し、変更を認める時点での評価、研究終了後の事後評価、資金の使用状況の審査を適切に行える人材を確保すること。

[33] 脚注６を参照。

第三に、ＰＯ等の担当者に対し、計画変更の要望があった際は、それを判定するための場（例えば有識者による委員会）を組織するなど、研究の進展等に応じて柔軟に計画変更するための仕組みを、資金配分機関内に設けるとともに、必要な場合においても計画変更を承認しない場合の不服申立て制度について検討すること

（２） 途中段階で得た成果利用プロセスの独立

第一に、中間成果の扱いについて、研究開発計画等で定めるようにルール化を検討すること

第二に、研究者が望む場合には、研究開発データベースなどを活用し、中間成果を公表できる体制を整備すること

第三に、知的財産権上の扱い等、中間成果を活用する際の開発者と利用者の権利についてのルールの明確化を検討すること

第四に、成果を活用する側との連携、成果の実装へのつなぎ部分についても、支援の強化の方策を検討すること

４．３　今後の方向性

技術戦略に関し、技術戦略専門委員会として、来年度は少なくとも以下の取組みを行うべきであると考えられる。

（１） グランドチャレンジ型研究開発・技術開発に関する検討の加速化

２００８年度の検討を踏まえ、グランドチャレンジ型研究開発・技術開発に係る検討の加速化を図る。具体的には、検討の場や参加者について早急に検討・調整を行った後に、テーマ選定等の開発面、グランドチャレンジプロジェクト全体の進め方の検討等の管理面の双方の検討を進める。その上で、可能であれば今後の取組みスケジュールや進め方などを具体的にまとめた「２００９年版グランドチャレンジ・ロードマップ」を策定する。

（２） 「環境変化に対応できる継続的な研究開発プロジェクト管理」に関連した具体的取組み

２００８年度の検討を踏まえ、研究開発プロジェクト管理・評価体制に関する提言の内容をいくつかの研究開発事業で関係者とともに試行する。

（３） その他、第２次情報セキュリティ基本計画の技術戦略に盛り込まれた論点に関する検討、過去の報告書のうち、継続的・追加的な検討が必要な事項の検討

例えば、「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」に関して、報告書 2005 に盛り込まれた「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、研究領域の調整を行う循環モデルの構築」に資するものとして、政府機関におけるＩＴのユーザー環境の情報セキュリティ向上を技術的に担保するための方策を検討することなどが挙げられる。

別紙

情報セキュリティ政策会議　技術戦略専門委員会　委員名簿

【委員長】

佐々木　良一	東京電機大学教授

【委員】

小柳　和子	情報セキュリティ大学院大学　教授
河田　惠昭	京都大学防災研究所巨大災害研究センター長
後藤　滋樹	早稲田大学　理工学術院　教授
志方　俊之	帝京大学教授
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：米澤明憲委員は、2008年6月まで在任。

グランドチャレンジ検討ワーキンググループ　委員名簿

【主　査】

後藤　滋樹　　早稲田大学　理工学術院　教授

【主査代理】

安達　淳　　国立情報学研究所　コンテンツ科学研究系教授　学術基盤推進部長

【委　員】

磯村　浩子　　社団法人日本消費生活アドバイザー･コンサルタント協会
消費生活研究所　所長

伊藤　光恭　　NTT情報流通プラットフォーム研究所
セキュアコミュニケーション基盤プロジェクト　グループリーダ

加藤　雅彦　　株式会社 アイアイジェイ テクノロジー IBPS 本部
システム技術部　部長代理

楠　正憲　　マイクロソフト株式会社　CTO補佐

西本　逸郎　　株式会社ラック　サイバーリスク総合研究所　所長

二木　真明　　住商情報システム株式会社　情報セキュリティ･IT統括部　担当部長

松並　勝　　ソニーデジタルネットワークアプリケーションズ株式会社
セキュリティテクノロジマネージャ

三河尻　浩泰　　株式会社富士通大分ソフトウェアラボラトリ　セキュリティセンター長

森山　浩幹　　株式会社エヌ･ティ･ティ･ドコモ　法人事業部
ソリューションビジネス部　担当部長

山田　安秀　　情報処理推進機構　セキュリティセンター長

（五十音順、敬称略）