NISC National Information Security Center

報告書2008（事務局案）の概要について

2009年3月17日

内閣官房情報セキュリティセンター（NISC）

http://www.nisc.go.jp/

資料3

技術戦略専門委員会 報告書2008の構成

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

1．2 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

1．2．1　研究開発・技術開発の方向性の検討
（研究テーマ面）

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
（プロジェクト運営面）

詳細化検討

アプローチ
ニーズ指向

アプローチ
シーズ指向

2. 情報セキュリティ技術の将来に関する検討

2．1　将来の
社会ビジョンに
関する検討
（ニーズ指向）

2．2　技術の
潮流予測
（シーズ指向）

2．3　情報セキュリティ技術のグランド
チャレンジにつながる方向性と進め方

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 公的な競争的研究開発
資金制度に関する論点

3．1．1 研究者側の問題提起

3．1．2 公的な競争的研究開発
資金制度の現状と改善状況

3．2 プロジェクト管理・評価
体制の改善の方向性

4. ま と め

第1章　技術戦略専門委員会
報告書2008の目的と構成

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

1．2 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

1．2．1　研究開発・技術開発の方向性の検討（研究テーマ面）

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（プロジェクト運営面）

技術戦略専門委員会の位置づけと これまでの技術戦略専門委員会報告書の内容

技術戦略専門委員会の位置づけ

- 情報セキュリティに係る研究開発・技術開発、その利用戦略について調査検討を行い、情報セキュリティ政策会議等に対して、「技術戦略専門委員会報告書」としての提言を行う。
- 情報セキュリティの確保において、継続的な技術開発と、その社会展開を円滑に行い、成果をすべ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投資開発の戦略設定が求められているとの認識に基づき、調査研究を行う。

過去の技術戦略専門委員会報告書の概要

○ 報告書2005(2005年11月17日発表)

1 報告書2005の位置づけ～第一次基本計画に向けた報告書

2 報告書2005における技術戦略を考える上での基本的な考え方
- ・我が国における情報セキュリティ上の問題点の全体の俯瞰
- ・情報セキュリティ技術の役割と今後の方向性を検討
- ・情報セキュリティ技術を支える環境整備の必要性

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について

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

5 「グランドチャレンジ型」研究開発・技術開発の推進

○ 報告書2006(2007年6月29日発表)

1 情報セキュリティ技術の現状認識と今後の方向性
- ・情報セキュリティ技術戦略の基本
- ・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
- ・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

2 2007年における実施のポイント
- ・投資領域設定の継続的見直し構造の実現
- ・調達を通して成果を活用するガイドライン策定の検討
- ・「グランドチャレンジ型」テーマ検討の場

情報セキュリティ技術戦略に係る
検討構造とこれまでの取組み

情報セキュリティ技術戦略

『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

【技術開発分野の方向性形成】

「グランドチャレンジ型」研究開発・技術開発の推進

【具体的な大規模技術開発プロジェクト】

『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』について

【プロジェクト管理等の管理面】

2006年度～2007年度の取組み

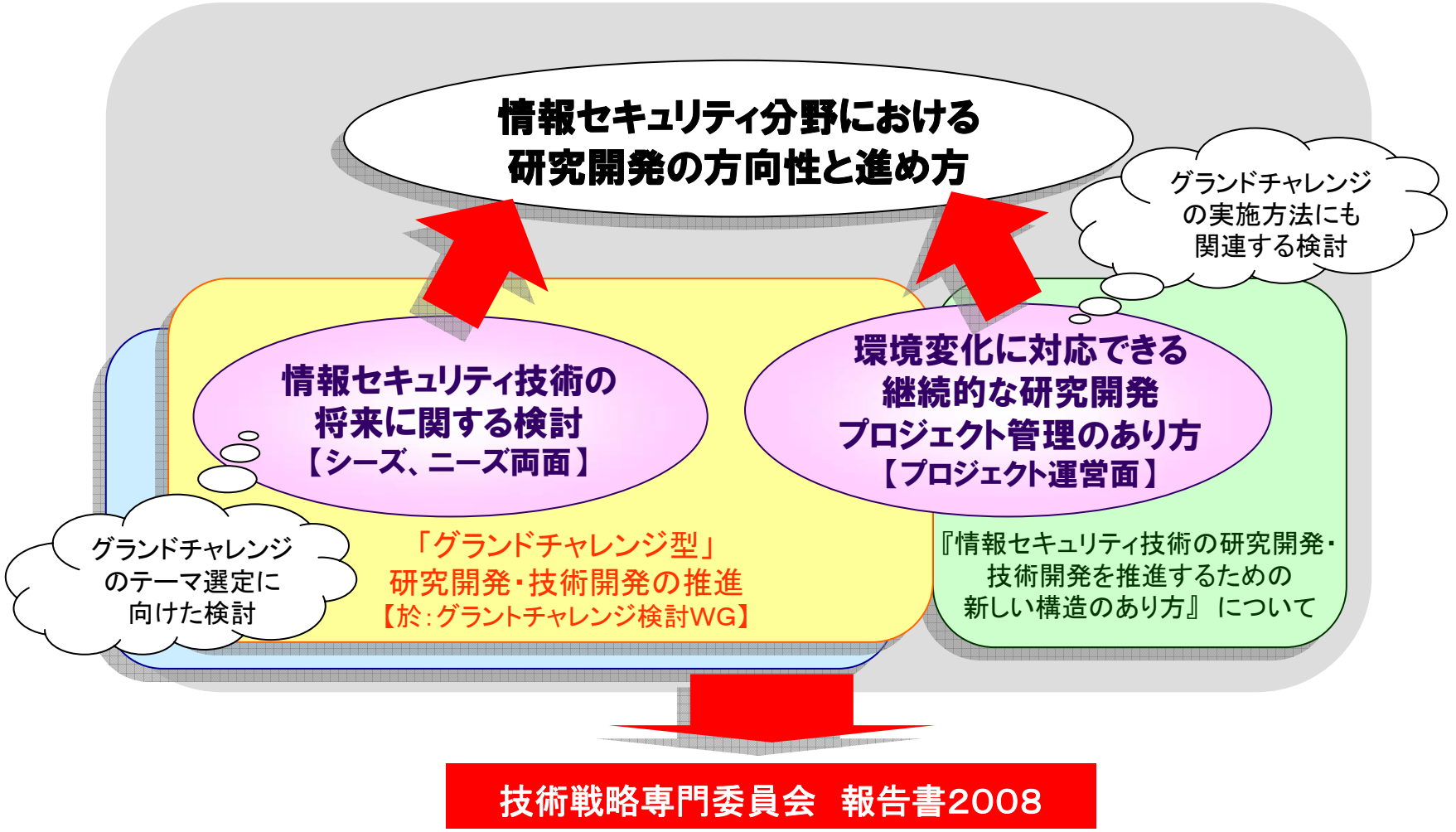
・「グランドチャレンジ型」テーマ検討の場の設置を決定

・投資領域設定の継続的見直し構造の実現

・調達を通して成果を活用するガイドライン策定の検討

本年度の技術戦略専門委員会および グランドチャレンジ検討WGにおける検討内容

2008年度の検討のフレームワーク



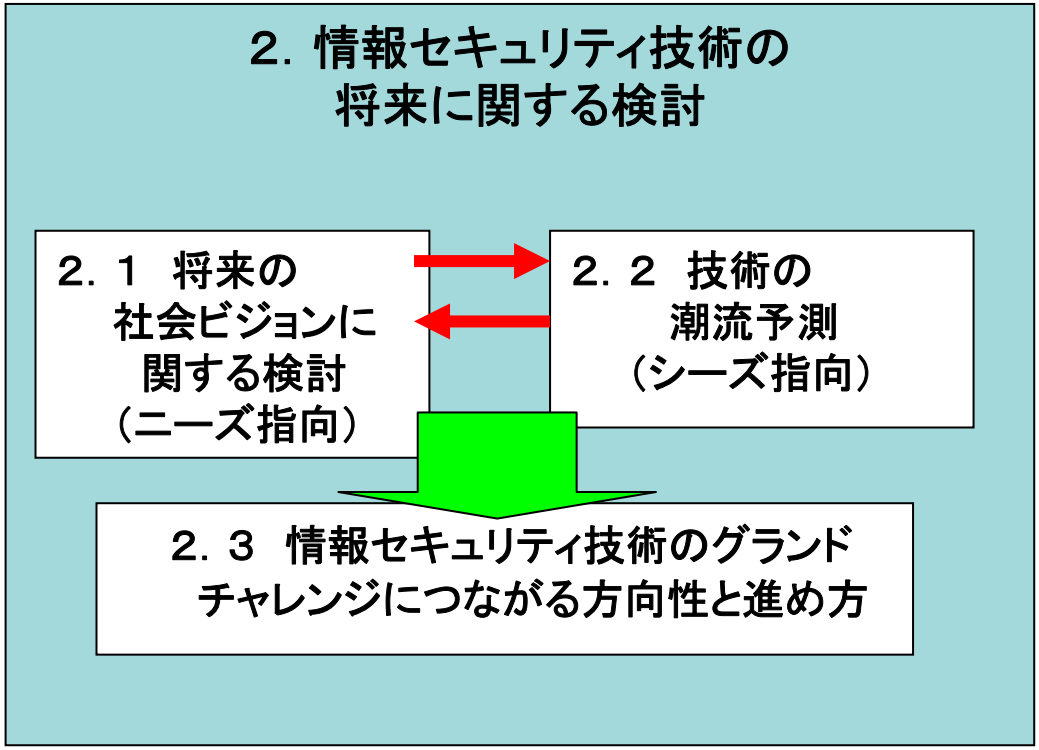
報告書全体、第1章に関する論点

〇2008年度の技術戦略に関する報告書全体の構成はこれで良いか？

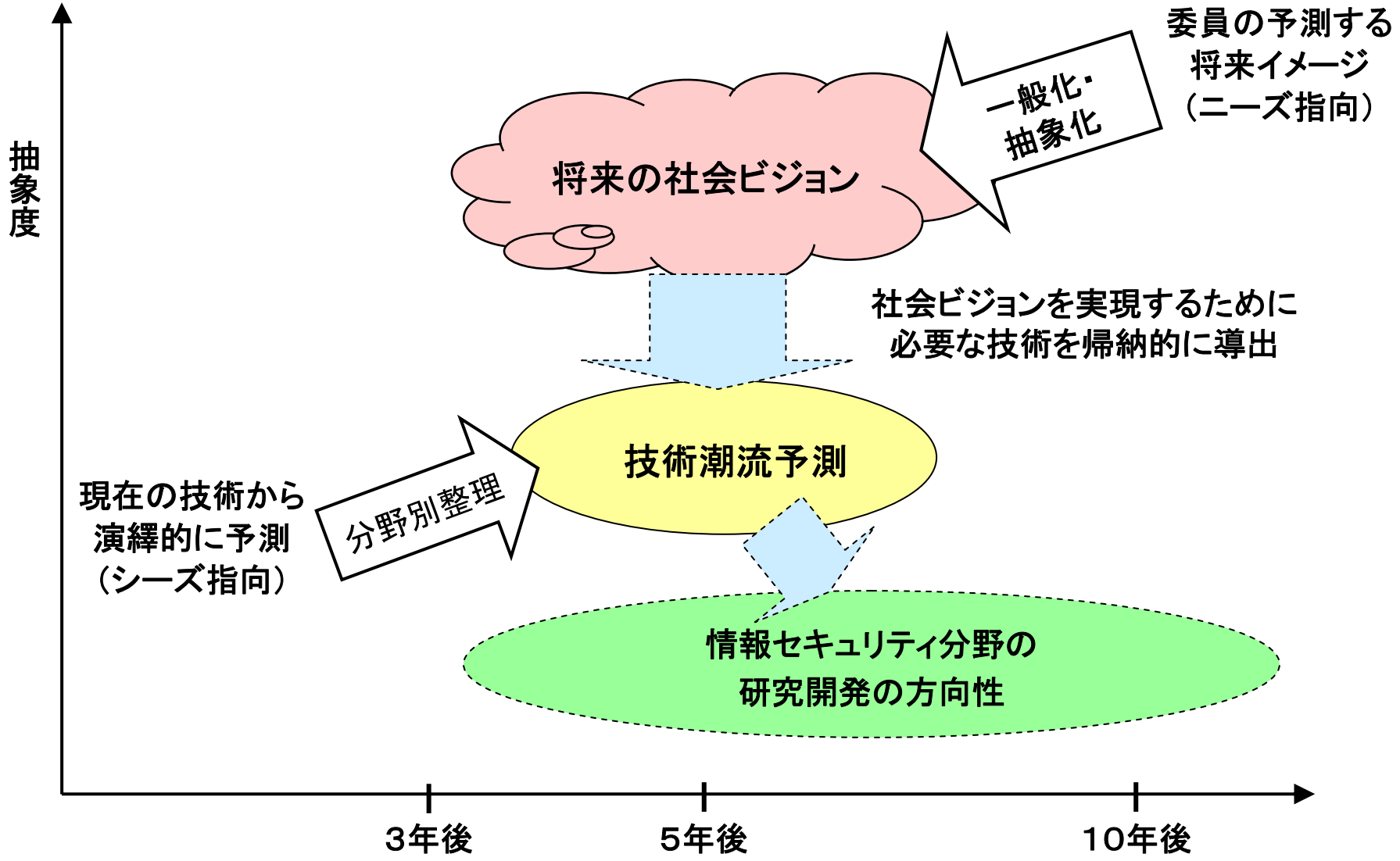
〇今年度は、主としてグランドチャレンジに関連の深い検討を行ってきた（特にテーマ選定面）。しかしながら、具体的なテーマの抽出・決定までに、もう少し検討を深めるべきであり、今後の検討に資するような要素の例示までを今年度のアウトプットとすることで良いか？

〇これを受けて、来年度早急に必要な検討を深めるべく、本委員会などを開催するということで良いか？

第2章　情報セキュリティ技術の将来に関する検討
（シーズ、ニーズ両面）



情報セキュリティ技術の将来に関する検討のアプローチ



2．1　将来の社会ビジョン(ニーズ指向)に関する論点

○これまで委員から頂いた御意見に基づく、「将来の社会ビジョン」に係る主たる要素を整理すると、例えば以下のようなものが挙げられる。

・(大前提として)安心な生活、社会経済活動の実現
・製品の機能面においてセキュリティが自然に担保されていること［当然化］
・セキュリティ原理主義ではなく、製品などの種類に応じて柔軟な技術的対応［柔軟性］
・国境を越えてどこででも、いつでもセキュリティが確保［グローバル・ユビキタス］
・IT利用に際してリスクによって人間が支配されるのではなく、人間がリスクをコントロール可能に［コントローラビリティ］
・我が国が世界をリードし、世界に誇れる技術を開発［最先端性］

○今後、グランドチャレンジを通じて、これらのビジョンを実現するための技術開発を行うべきではないか。さらに、ユーザーの視点に立ち、これらの技術が化体した具体物［New Secure Product］を開発するべきではないか？

○そして、国境を越えてネットワークがつながっている状況下で、セキュリティに係る問題を無くし、かつ世界をリードし世界に誇れる具体物を開発するべきではないか？

○開発過程においては、様々な関連領域におけるものを含め、一定の方向性を持って世の中で実際に効用のある関連技術を発展するよう取組みを進めるべきである。

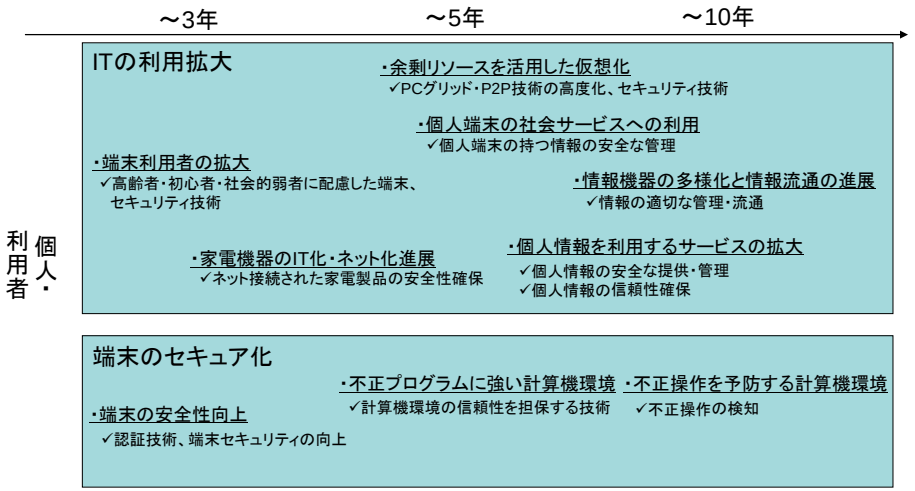
ビジョンを実現するための技術（シーズ指向アプローチ）

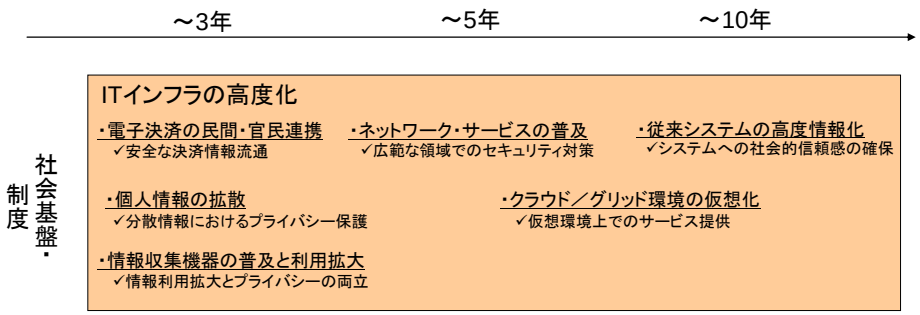
技術潮流予測の進め方

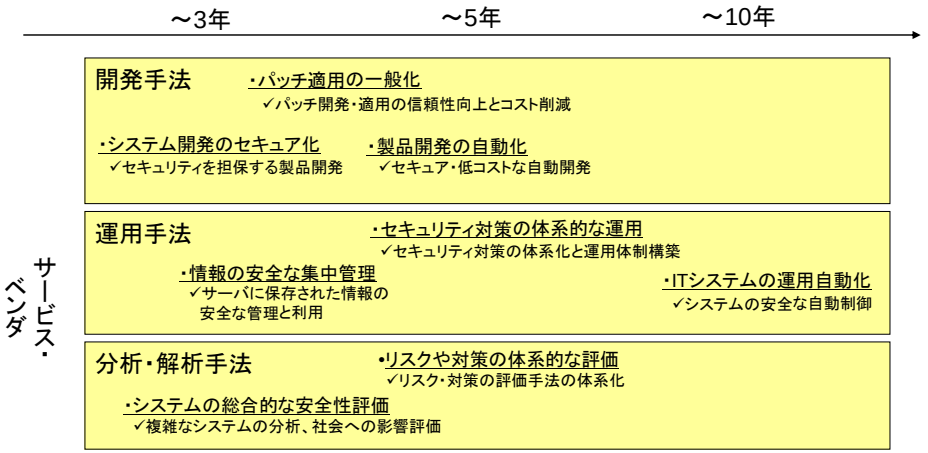
- 委員の意見に基づく、サービスや製品の提供側の視点での演繹的アプローチ
- 現在の技術の延長で、どのような機能、性能のものが登場するかを予測し、その際に必要となるセキュリティ要件を検討

予測の期間・分野

- 現在から3年後、5年後、10年後の予測を行い、その結果を整理
- 「個人・利用者」「サービス・ベンダ」「社会基盤・制度」の3分野で予測







2. 2 技術の潮流予測に関する論点

技術潮流予測の進め方

〇技術潮流は、「個人・利用者」、「サービス・ベンダ」、「社会基盤・制度」の3分野で行なった。他の予測の視点、分野があるか？

社会・技術の大きな潮流予測

〇3分野の大きな潮流を以下のように予測した。これに補足・修正する視点があるか？

「個人・利用者」

・多様な機器がIT化し、生活に密着したITサービスが広く利用
　→　情報の管理やセキュリティ対策に一層の努力が必要となる。
　→　サービスの正当性や不正チェックなど、リアルとデジタルの世界の感覚を共通化により、利用者がITサービスを安全に利用できる技術が必要となる。

「サービス・ベンダ」

・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。
・仮想化環境で、システムやサービスの状況を観測できる技術が発達している。
・耐タンパーなフォレンジック技術への必要性が高まる。
・自動的に開発・運用・評価を行ってセキュリティを確保できる技術が必要とされる。

「社会基盤・制度」

・個人・企業に限らず、基盤システムの社会的な信頼感の確保が必要とされる。
・仮想化環境でも重要なデータを安全・安心な場所に保管する方式が必要となる。

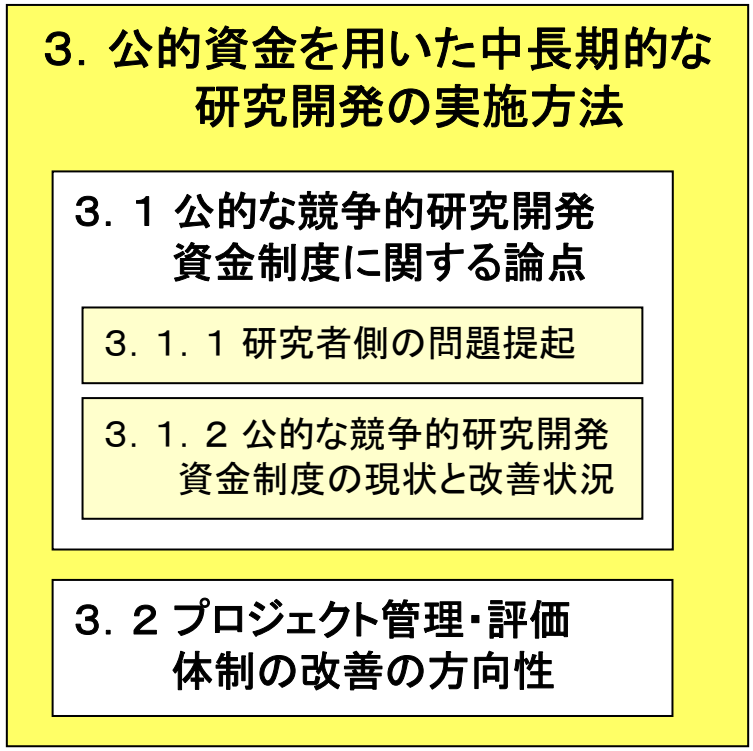
2. 3 情報セキュリティ技術のグランドチャレンジ につながる方向性と進め方 に関する論点

○社会ビジョンや技術の潮流予測を踏まえつつ、今後、グランドチャレンジに関する具体的なテーマを幅広い関係者の参加を得て検討するべきである（その際、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ないか）。

○（本委員会で検討された社会ビジョンを実現するべく）グランドチャレンジに関するテーマ、研究開発対象となる具体物、そしてそれを構成する技術について検討を行う中で、例えば、以下のような要素技術も重要になってくるのではないか？

- 「当然化」を実現するべく、一定のセキュリティ水準が確保されたプロダクトを設計する技術
- 「柔軟性」を実現するべく、利用シーンに応じて動的にセキュリティレベルを最適化するような技術、システム
- 「グローバルユビキタス」や「安心な生活、社会経済活動」を実現するべく、日常の生活、社会経済活動に浸透したIT機器のセキュリティ確保に係る技術
- 「コントローラビリティ」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）

第3章　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（プロジェクト運用面）



研究開発プロジェクト管理・評価体制の問題意識

【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で研究計画を作成する
・中間／事後評価では、計画に沿った実施について非常に厳密に検証される
・新たな状況変化が認識されても、計画自体の変更が非常に困難、ないしは、ほぼ不可能な場合がある
・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*を常時行って、計画に反映させるべき

【２】 途中段階で得た成果利用プロセスの独立

・プロジェクトの途中成果が、十分に公開されていない、あるいは有効に活用されていない場合がある
・当初定めた成果利用計画のみにとらわれることなく、社会ニーズに合致した成果活用プロセスを探求すべき
・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

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

情報セキュリティ分野でこの問題を論じる必要性

前述の問題意識は、特定分野に限らないが、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

・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)プライバシー保護、サービスの正当性の保証に資するための技術など

＊情報セキュリティ技術は特殊性の高い分野であるが、ITの研究課題には情報セキュリティが不可分な場合が多いため、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の運営の改善の方向性について検討を行なった

公的な競争的資金制度の現状と改善事例

本年度、当委員会で、特に「競争的資金」を用いた研究開発に着目し、検討した理由

・情報セキュリティ分野では、技術の進歩や環境の変化が特に激しく、プロジェクトを取り巻く状況が研究の実施期間中に研究者が予期してなかった方向に変化することがある。
・その結果、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。

（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、法令／各研究費制度／各研究機関レベルの3階層構造になっている
・階層間での手続きや承認権限などに不明確な部分が残されていたり、保守的な判断や誤解、周知不十分などによって、改善されたルールが有効に活用されていない可能性がある

（２）会計制度の制約と資金使用の柔軟化

科学研究費補助金や戦略的創造研究推進事業などの取組み例
・繰越明許費制度 の活用を推進中
・優れた研究を長期安定的に推進するための「更新制」の拡大
・研究費の複数年契約の拡大など

（３）採択後の研究計画変更

科学技術振興機構の戦略的創造研究推進事業の取組み例
・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

3. 1 公的な競争的研究開発資金制度に関する論点

研究開発プロジェクト管理・評価体制の問題意識

○大きく「計画変更の柔軟化とリファクタリングの必要性」と「途中段階で得た成果利用プロセスの独立」の2つの課題を指摘した。他に、検討すべき課題はあるか？

公的な競争的研究開発資金制度の現状と改善状況

○研究開発プロジェクトの柔軟性を阻む原因として、他に考えうるものはあるか？
○優れた改善状況の例が他にあるか？

情報セキュリティ分野でこの問題を論じる必要性

○情報セキュリティ分野の特殊性として挙げた内容に追記修正すべき点はあるか？

計画変更の柔軟化とリファクタリングの必要性に関する論点

○ 年次計画の精度を維持するには、研究者及び資金配分機関で、当初計画の見直しを行うことが、必要ではないか。

○ 或いは、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が有効ではないか。

○ 上記の仕組みを効果的に動かすには、資金配分機関において、できるだけ対象研究領域に知見を有し、評価、資金の使用状況の審査を適切に行える人材（例：プログラム・オフィサー（PO）を確保することが望ましいと考えるが、そのために、処遇等の改善などが必要ではないか。

○ 一方で、判断をPOなどの担当者にのみ任せるべきではない、という意見もある。そのため、計画変更などの重要な要望があった際は、それを判定するための場（例：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ことが必要ではないか。

途中段階で得た成果利用プロセスの独立に関する論点

○中間成果の扱い（公表や活用など）について、研究者と資金配分機関との間で、判断に迷って遠慮している可能性があるため、事前に研究開発計画等で明記するようルール化することが必要ではないか。

○既に幾つかの競争的資金や資金配分機関などで取り組まれているように、Webサイトや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が有効ではないか。

○特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が必要ではないか。

○メーカーなどの成果を活用する側との連携、実用化／製品化にむけての成果の実装へのつなぎ部分についても（大学などの研究者があまり得意ではないため）、支援の強化の方策を検討することが有効ではないか。

第4章　まとめ

4．ま と め

4 まとめに関する論点

〇以上の議論を踏まえて、来年度は技術戦略に関して少なくとも以下の取組みを行うべきではないか？　また、他に来年度、是非とも取組むべき重要課題はあるか？

・グランドチャレンジに関する検討の継続（テーマ選定、グランドチャレンジプロジェクト全体の進め方の検討の両面を検討。その上で、可能であれば「09年版グランドチャレンジ・ロードマップ」を策定。検討の場や参加者については、別途検討・調整が必要）
・本年度検討を行った「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の検討
・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、など

【参考】公的資金による研究開発プロジェクト管理・運営体制の一例