



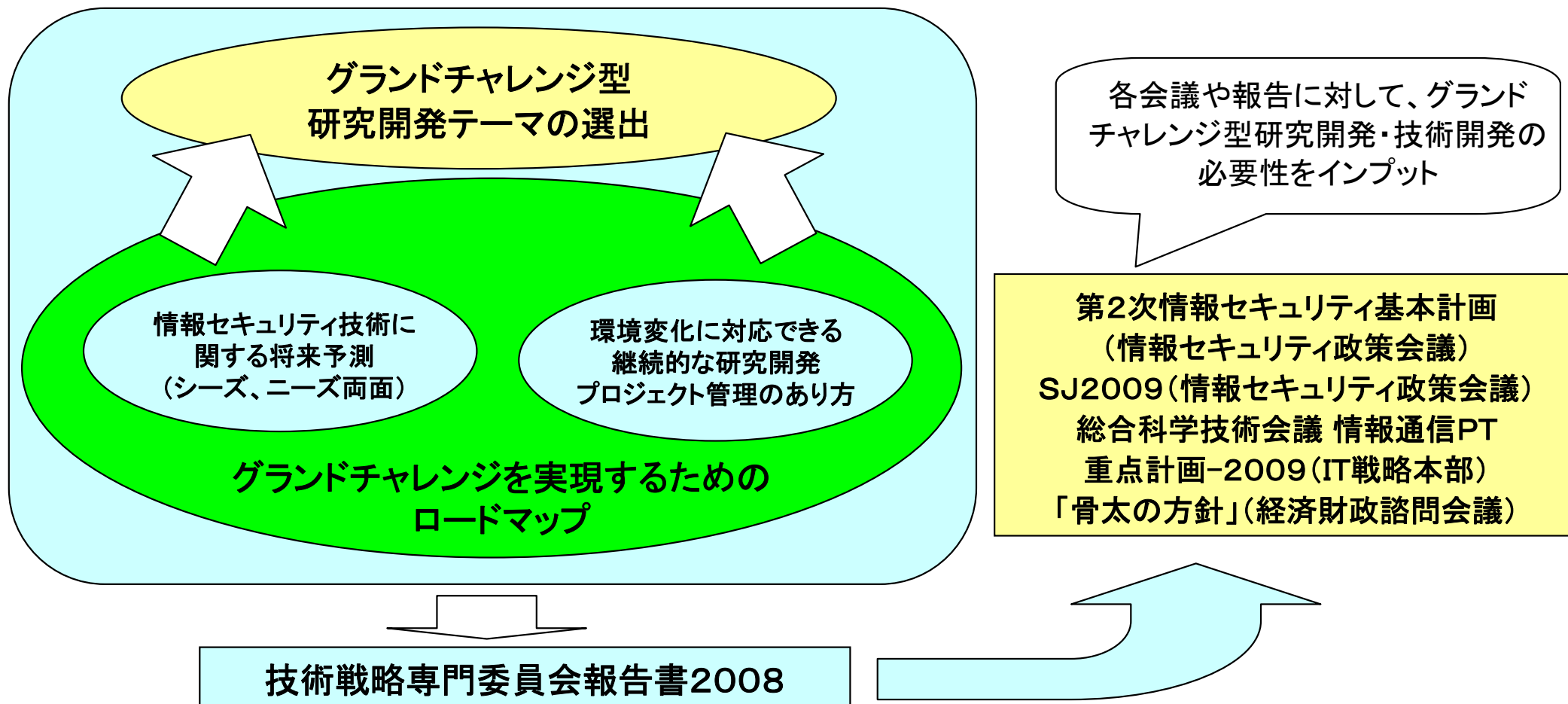
グランドチャレンジ検討WGの議論の方向性について

2008年9月29日

内閣官房情報セキュリティセンター(NISC)

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

1. 本WGでは、グランドチャレンジを実現するためのロードマップ(情報セキュリティ技術に関する将来予測、環境変化に対応できる継続的な研究開発)と、グランドチャレンジ型研究開発テーマについて検討する。
2. 検討結果を技術戦略専門委員会に報告し、同委員会は報告書として取りまとめる。
3. 取りまとめられた報告書を用いて、総合科学技術会議等の関係機関にグランドチャレンジのインプットを行う。



情報セキュリティ技術に関する 将来予測の進め方について

1. 将来予測を実施する目的

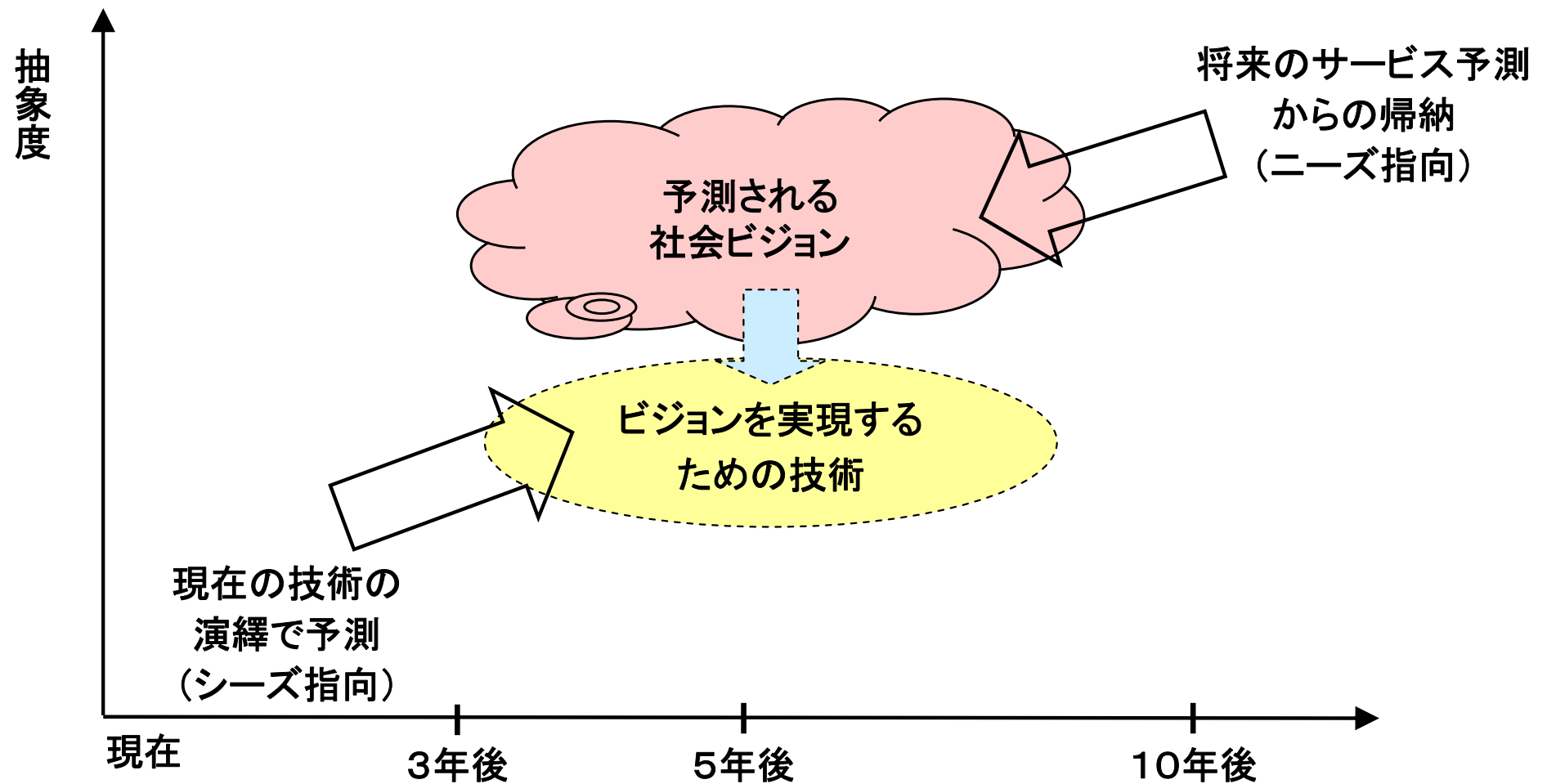
- ・ 政府としての「将来の社会ビジョンと技術像」。
- ・ 政府内で認識を共有するとともに、広く世の中に公表し、情報セキュリティ技術や政策に関する方向性の議論を惹起する。
- ・ 予測された「社会ビジョンと技術像」は、問題提起や提言を行うための前提として用いる。

予測された「社会ビジョンと技術像」から、新たに登場するであろう情報セキュリティ上の脅威や課題、また、いつ頃、どのような情報セキュリティ対策や技術が必要となるか、などが浮かび上がることを期待。

2. 将来予測の主な対象分野

- ・ 政府として関心のある、公共性の高い「社会の基盤となるシステムやサービス」。
(例) 電子政府、重要インフラ、災害対策など

- ・ 中長期(3年後、5年後、10年後の3ポイント)とすることが適当か。



3. ニーズ・シーズ双方から検討

(1) ニーズ指向アプローチ

- ・ 利用側の視点からアプローチする。
- ・ 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、それらを安全に利用するための情報セキュリティ要件を検討。
(例)安全対策として、公共の場所に膨大な数の監視用カメラが設置されて、記録されるようになった場合、プライバシー保護はどうか？

(2) シーズ指向アプローチ

- ・ 提供側の視点からアプローチする。
- ・ 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セキュリティ要件を検討。
(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、ウイルスチェックを行なうのに、従来のパターンマッチング技術で対応可能か？

グランドチャレンジ検討WG第1回会合の発言要旨 (将来予測等について)

■ 10年度のライフスタイルと情報セキュリティ技術

- ・フィッシング等のように、技術だけでなくサービスの使われ方も問題
- ・10年後のライフスタイルと情報セキュリティを併せて考えてゆく必要性

■ 自律して成長する(脅威に対応する)情報セキュリティ技術

- ・パターンファイルによるウィルス対策は限界に来ているとの指摘
- ・攻撃側と防御側の戦争の果ての決着として、免疫機構のような自律発展的で利用者の高度なりテラシーを必要としないセキュリティ・テクノロジーを期待

■ 運用の現場を支える情報セキュリティ自動化技術

- ・日本の情報セキュリティを支える運用の第一線は、さまざまな矛盾を抱えて疲弊
- ・情報セキュリティは未だにドキュメントと人手に頼っている状況、少しでも、自動化、機械化しないと弱いところから綻びてゆくおそれ

■情報セキュリティ上の脅威や実態を可視化し動的に把握する技術

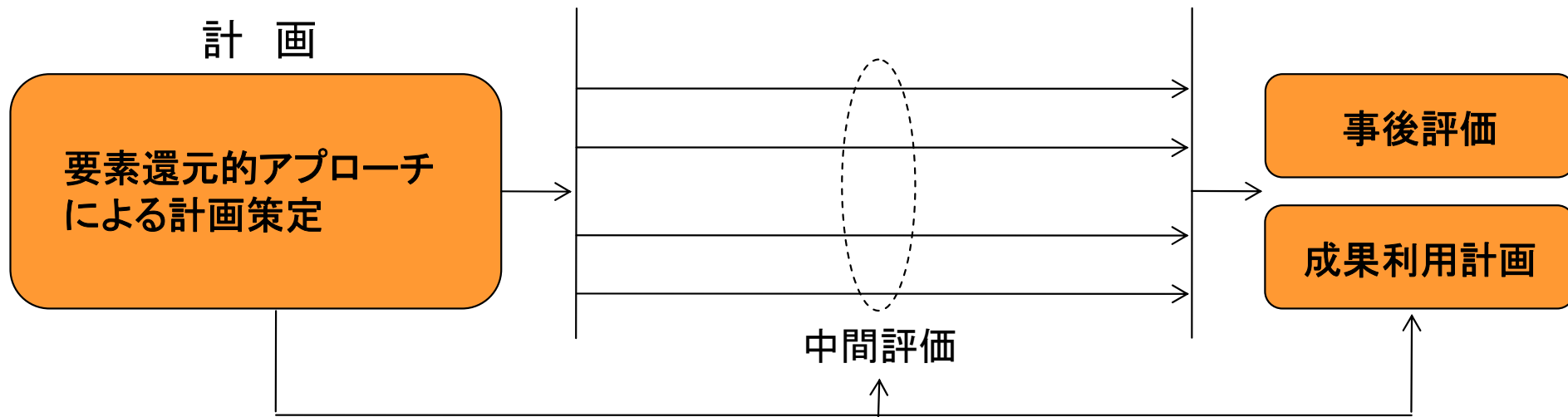
- ・情報セキュリティ技術の議論は、各論の積み上げになっており全体像が不明（言わば分子は見えるが分母が見えない状態）
- ・対策疲れも指摘される情報セキュリティ対策において、脅威に応じた適切な相場感を掴むためには、全体像の議論が不可欠
- ・現在のセキュリティについては、成長するモデルは考えられていないが、健全にセキュアシステムを成長させる環境やそれをモニタするシステムは重要
- ・広範にわたる全体像の正確な把握は難しいが、クラウドコンピューティングのように 上位層において、膨大なデータを集約して活用する新技術が生まれる可能性に期待

■情報家電に関する情報セキュリティ技術

- ・家電機器のセキュリティは、被害が認識されておらず、また、その価値について一般ユーザーに理解されにくいいため、価格に上乘せすることは出来ず、対策に多くのコストを掛けることは困難
- ・家電等のプロダクトセキュリティに対しては売り切りモデルのため、販売後のコストについては、非常にセンシティブ、システムセキュリティとは分けて考える必要性
- ・一方、セキュリティレビュー等を実施し、出荷前にセキュリティ対策を済ませることは、出荷後に脆弱性が明らかとなってから対策を打つのに比べるとより経済的であり、対策実施のインセンティブがある
- ・よって、コストなどの兼ね合いで、出来る範囲で出来るだけのことをやってゆく、費用対効果に優れたライトウェイトアプローチが実施されており、さらに模索されている

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

山口英 情報セキュリティ補佐官



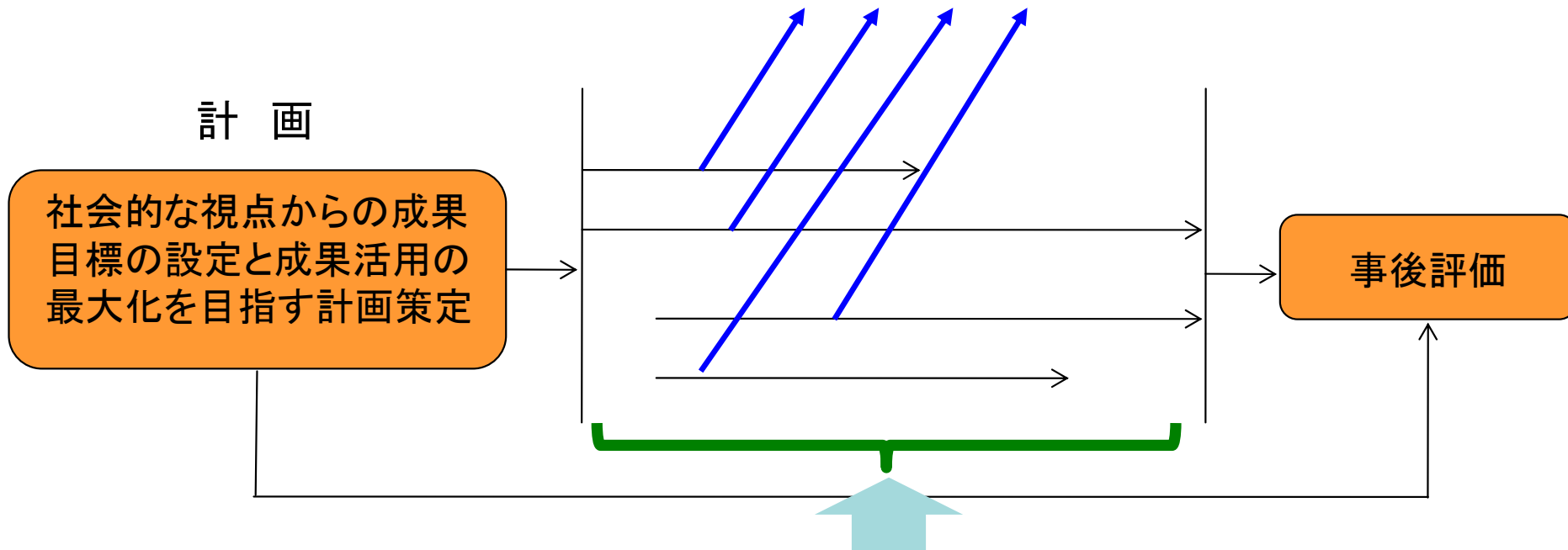
強い拘束力が発生

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、計画自体への変更はほぼ不可能

- 硬直的な計画実施
- 短期的な研究開発ならば適用可能
(3年は短期か?)

成果利用プロセスの独立

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。
社会ニーズに合致した成果活用プロセスの探求



常時リファクタリングを実施し計画に反映

- ・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。
動的な計画変更を実施し、研究開発投資の効果を最大化
- ・社会要請に的確に応える体制作り

- ・情報セキュリティ課題解決は、“moving target” 型課題解決である
 - リスク変容によって、目標は動的に変化
 - 新たな技術の登場によって、リスク変容が発生する
 - 攻撃側と防御側の非対称性
 - 2年前のリスクが、現在のリスクではないことが多発

- ・究極の目標は、実は大きな変化は少ないことが多い
 - 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問題が多い
 - 例) プライバシー保護に資する技術開発とは何か

グランドチャレンジ検討WG第1回会合の発言要旨 (プロジェクト管理のあり方について)

■日本のプロジェクト管理の硬直性

- ・日本のプロジェクトは、計画性が強すぎるとの指摘
- ・日本では、ウォーターフォールモデルにしがみつきがちとの問題点
- ・アジアの国の中でも、プロジェクトの流れを変えることが出来る国がある
- ・韓国では、80%は予定のとおり、残り20%はフレキシブルにやって良いと言われていた

■民間におけるプロジェクト管理の具体例

- ・民間において、大きな環境変化があった際の対応例
 - ① 地道な継続的改善
 - ② 学術コミュニティの中での評価
 - ③ 企業買収
- ・民間と言えども、大きな変更をPMOが出来ず、官同様に硬直化した運用をおこなってしまうこともある

■民間におけるプロジェクト管理の具体例

- ・あまりにも、成果目標の組み替えばかりでも迷走するため、メインストリームのプロジェクトとは、別の例えば“潜水艦”と呼ばれる小さな別計画を作っておいて、適当なタイミングでメインストリームに引き上げるという手もある。
- ・グランドチャレンジにおいては、“巨大潜水艦”を作るといった感覚ではないか。

■グランドチャレンジを支える情報共有の仕組み

- ・グランドチャレンジが、各サブテーマに書き下された後に、それらを繋ぐ組織的な情報共有の仕組みが必要