資料11

NISC National Information Security Center

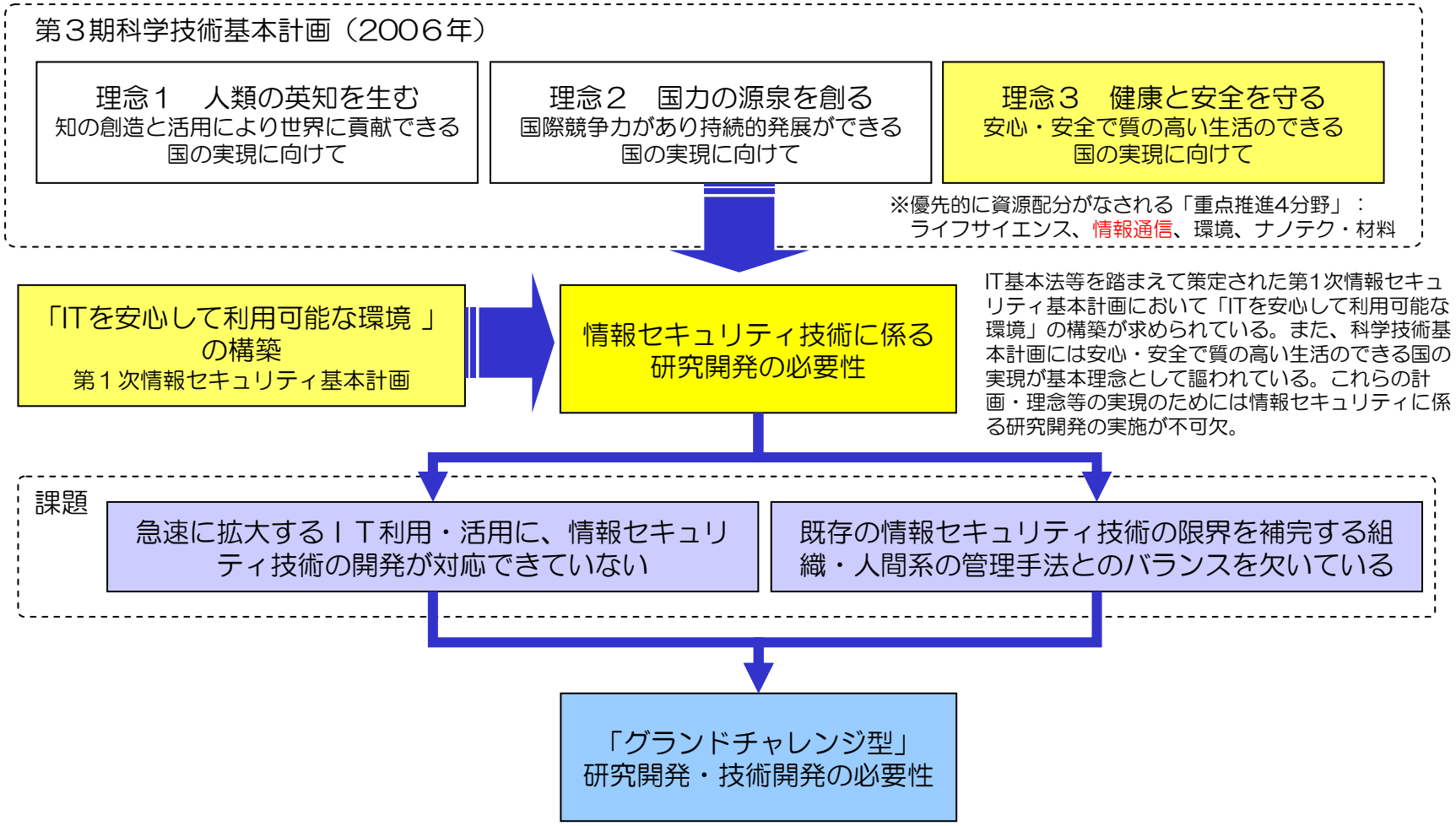
「グランドチャレンジ型」研究開発・技術開発の推進に向けて

2008年4月

内閣官房情報セキュリティセンター（NISC）

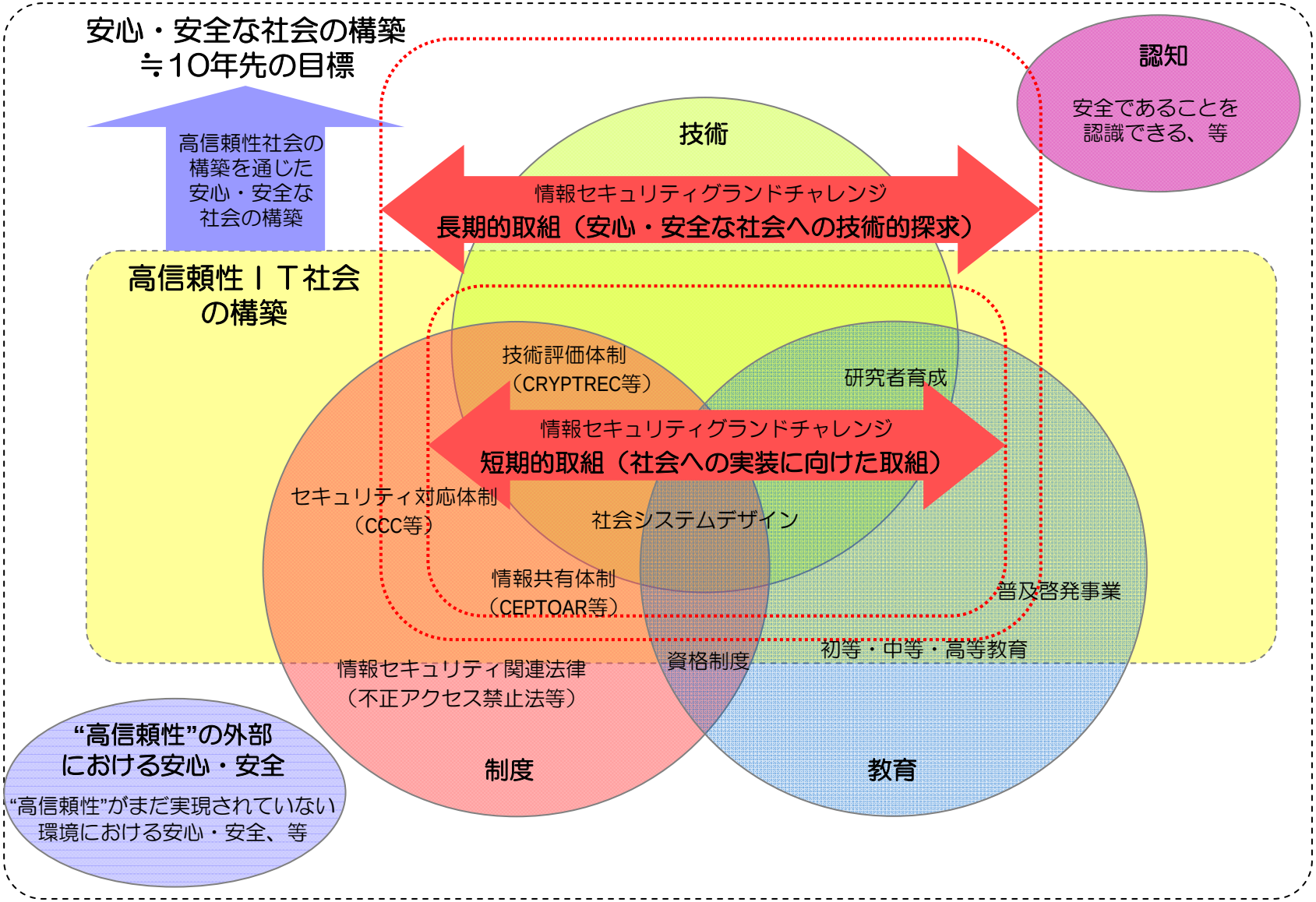
http://www.nisc.go.jp/

情報セキュリティ分野におけるグランドチャレンジ型研究開発・技術開発とは

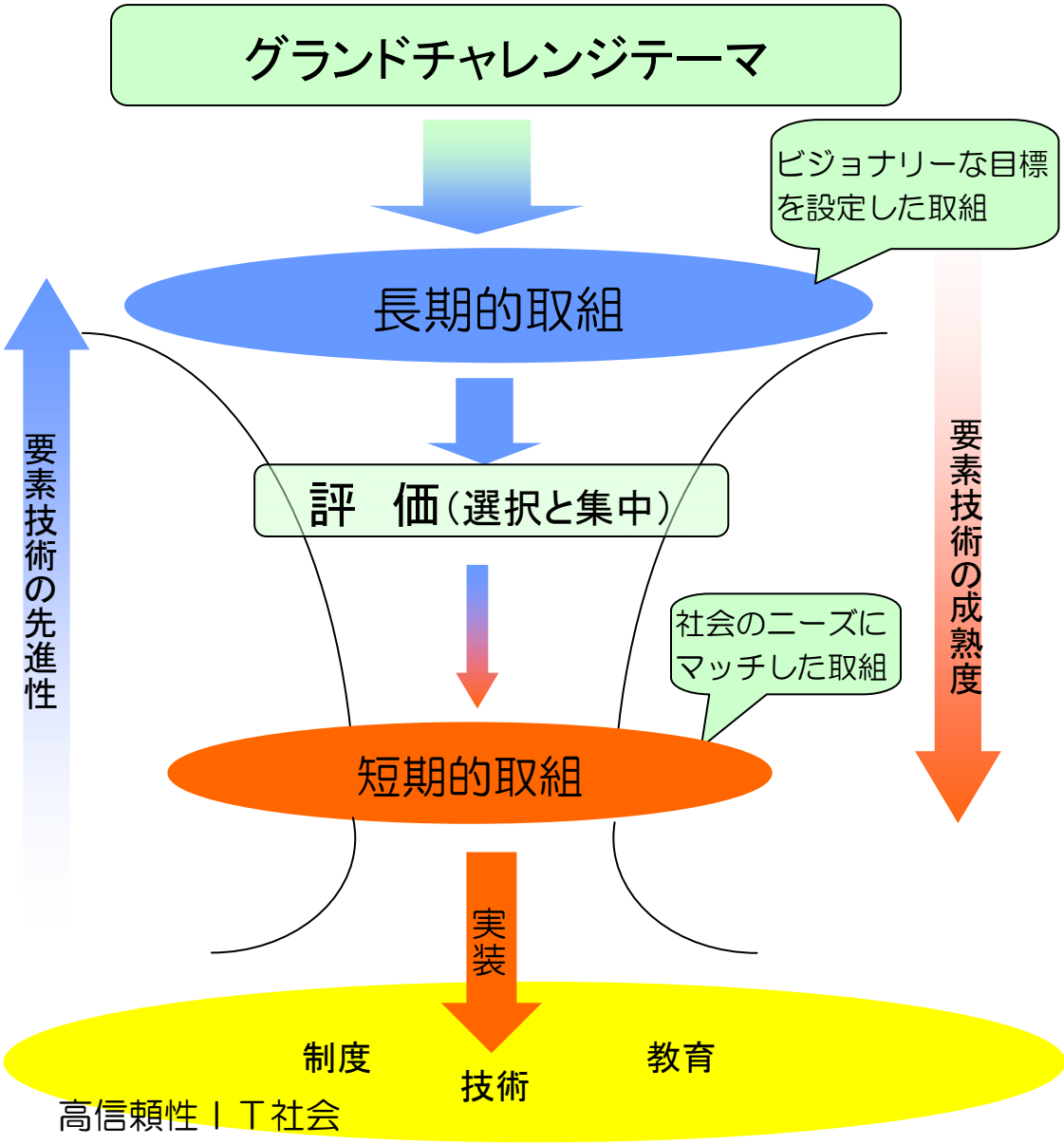


情報セキュリティ対策においては、対症療法的な対応だけでなく、中長期的な視野に立った研究開発等が重要である。したがって、情報セキュリティ技術の研究開発・技術開発においても、短期的な問題解決はもとより、長期的な視野で抜本的な技術革新等の実現を目指す「グランドチャレンジ型」の研究開発・技術開発が必要

グランドチャレンジ型研究開発・技術開発の位置づけ



長期的取組と短期的取組について



・長期的取組

グランドチャレンジテーマの実現に向けた幅広い先進的な技術開発・研究開発

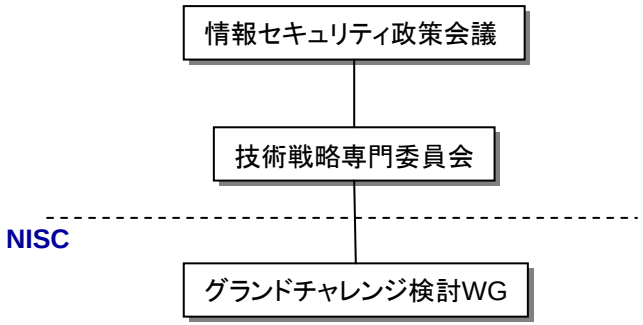
・短期的取組

（社会への実装に向けた取組）

「高信頼性IT社会」のための、充分な成熟度を持った要素技術のインテグレーション

グランドチャレンジ検討WGの目的と体制

■「グランドチャレンジ型」の研究開発・技術開発の具体化に向けたテーマ選定のプロセス及びプロジェクト実施方法等の検討の要請により、内閣官房情報セキュリティセンターはグランドチャレンジ検討WGを平成19年度に設置し、検討を実施した。



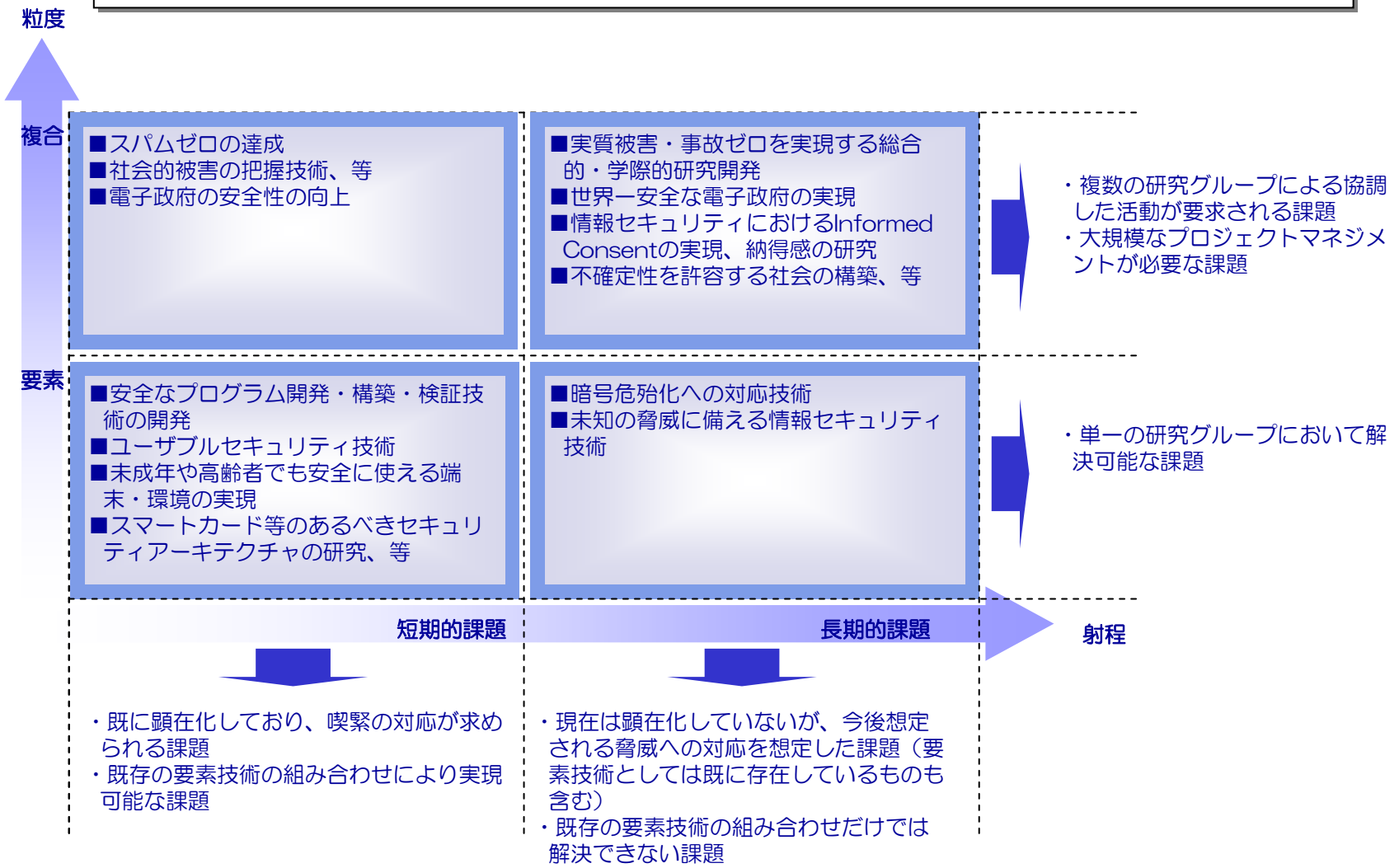
（座長）
武田 圭史　カーネギーメロン大学日本校 教授
（構成員）
新井 悠　株式会社ラック サイバースペース総合研究所 先端技術開発部長
大岩 寛　産業技術総合研究所 情報セキュリティ研究センター 研究員
門林 雄基　奈良先端科学技術大学院大学 情報科学研究科 准教授
鎌田 敬介　JPCERT/Coordination Center 早期警戒グループマネージャー
小池 英樹　電気通信大学 大学院情報システム学研究科 教授
寺田 真敏　株式会社日立製作所 Hitachi Incident Response Team (HIRT)
野川 裕記　株式会社セキュアウェア 取締役
福本 佳成　楽天株式会社 システムセキュリティ部 部長
星澤 裕二　株式会社セキュアブレイン 執行役員
吉岡 克成　横浜国立大学 学際プロジェクト研究センター 助教

本WGにおける主な検討項目

a）長期的な研究開発の実施方法について
・ プログラムマネージャー制等の検討
・ プロジェクト評価手法及び体制の確立
・ 開発予算（競争的資金等の活用を含む）の確保手法
・ 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
b）研究開発の推進体制について
・ 多岐にわたる各種要素技術の統合管理手法
・ 最適な資金配分を促進するための枠組み構築方法
c）具体的なテーマについて
・ 長期的な研究を実施する意義及び課題間の関連性の明確化
・ 情報セキュリティの技術要素の選定

グランドチャレンジ型研究開発・技術開発のテーマについて

■グランドチャレンジ型研究開発テーマについて、研究開発の射程（短期・長期）、粒度（複合・要素）の２軸、計４象限で整理
■検討されたテーマについて、それぞれの特性を踏まえ４象限に分類



高信頼性社会の構築に向け、情報セキュリティ技術において早急に対応が必要な技術開発・研究開発テーマ

情報セキュリティリスクの評価・分析技術

（1） 背景と目的：
- 情報セキュリティ対策の基本はリスク分析であるにもかかわらず、リスク分析が正しく行われていることは少ない。
- 複合的なコンポーネントから構成される情報システムのリスク分析技術は確立されていない。
- また、定量的リスク分析に必要なデータの蓄積がない。

（2）期待される効果：
- 人間系も含めた情報システムの信頼性向上。

（3）概要：
- 小規模なシステム（組込システム等）から大規模システム情報システム（重要インフラの業務システム等）に対応できる、リスク分析技術。
- 情報システムを運用する人間系を含めたリスク分析技術。
- システム間、あるいは外部環境とシステムの相互依存性を加味したリスク分析技術。
- リスク分析に必要な基礎的データの収集と蓄積。
- 脆弱性の存在がシステムに与えるリスク量の算出技術。

情報セキュリティ実装工学

（1） 背景と目的：
- 情報セキュリティ関係の個々の要素については、これまで様々な研究が行われてきているところ。
- しかしながら、それら技術をシステムとして実装したり、社会に普及していく際に検討すべきことについては、十分に研究がなされていない。

（2）期待される効果：
- ソフトウエア脆弱性や暗号危殆化時における社会的コストの最小化。

（3）概要：
- 情報システムのライフサイクルを通じたセキュリティ確保・技術の体系的研究。
- 暗号危殆化時において、社会的影響を最小化するようなシステム構成技術。また、ユーザーへのデプロイ手法の研究。
- 稼動を停止できないシステム（原子力発電所の制御システム）等における脆弱性発生時の対処技術。

新たな情報システムアーキテクチャに対応した新しいセキュリティモデルの提示

（1） 背景と目的：
- 従来の情報システム構築技術は、信頼できるドメイン内に閉じたシステムを対象に研究されてきた。
- 今後普及が見込まれる、P2P、SaaS、グリッドなどの新しいシステムアーキテクチャに対応したセキュアなシステム構築技術について十分な研究がなされていない。

（2）期待される効果：
- 安全なインターネットサービスの提供。

（3）概要：
- 新しいシステムアーキテクチャに対応した脆弱性のモデル化、体系化の研究。
- 分散化、匿名化された情報の保護技術。
- 問題が発生したときの責任分界のあり方に関する研究。
- 事業継続性・可用性の確保技術。