RCISの活動概要

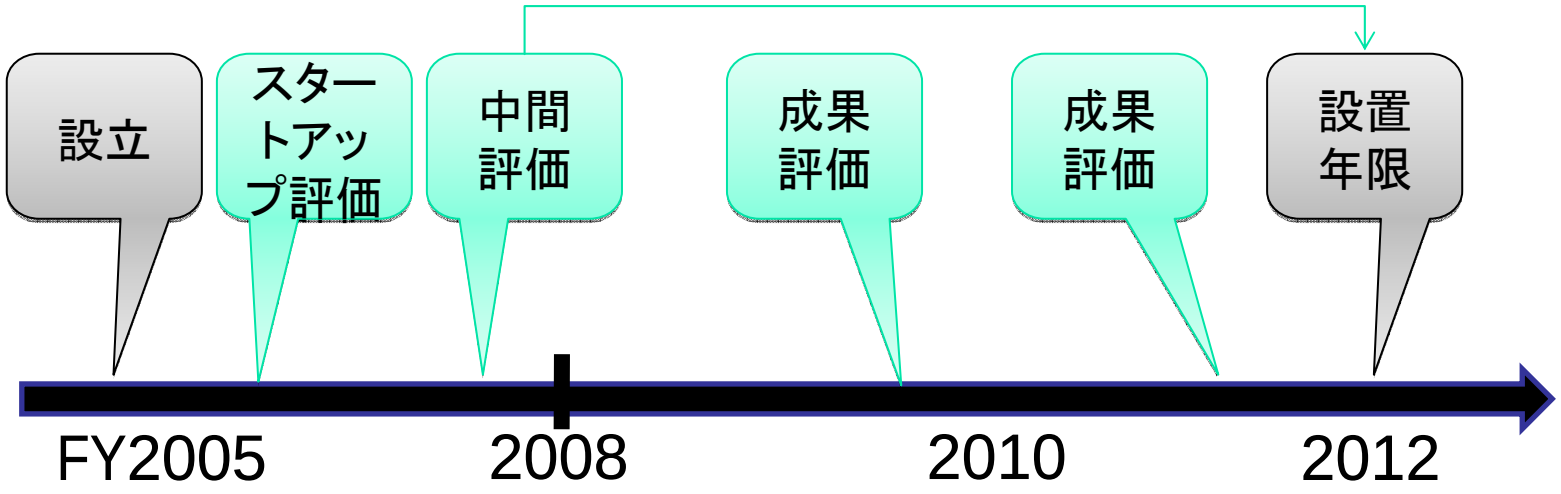
（独）産業技術総合研究所
情報セキュリティ研究センター
主幹研究員　古原　和邦

産総研における研究ユニットの分類

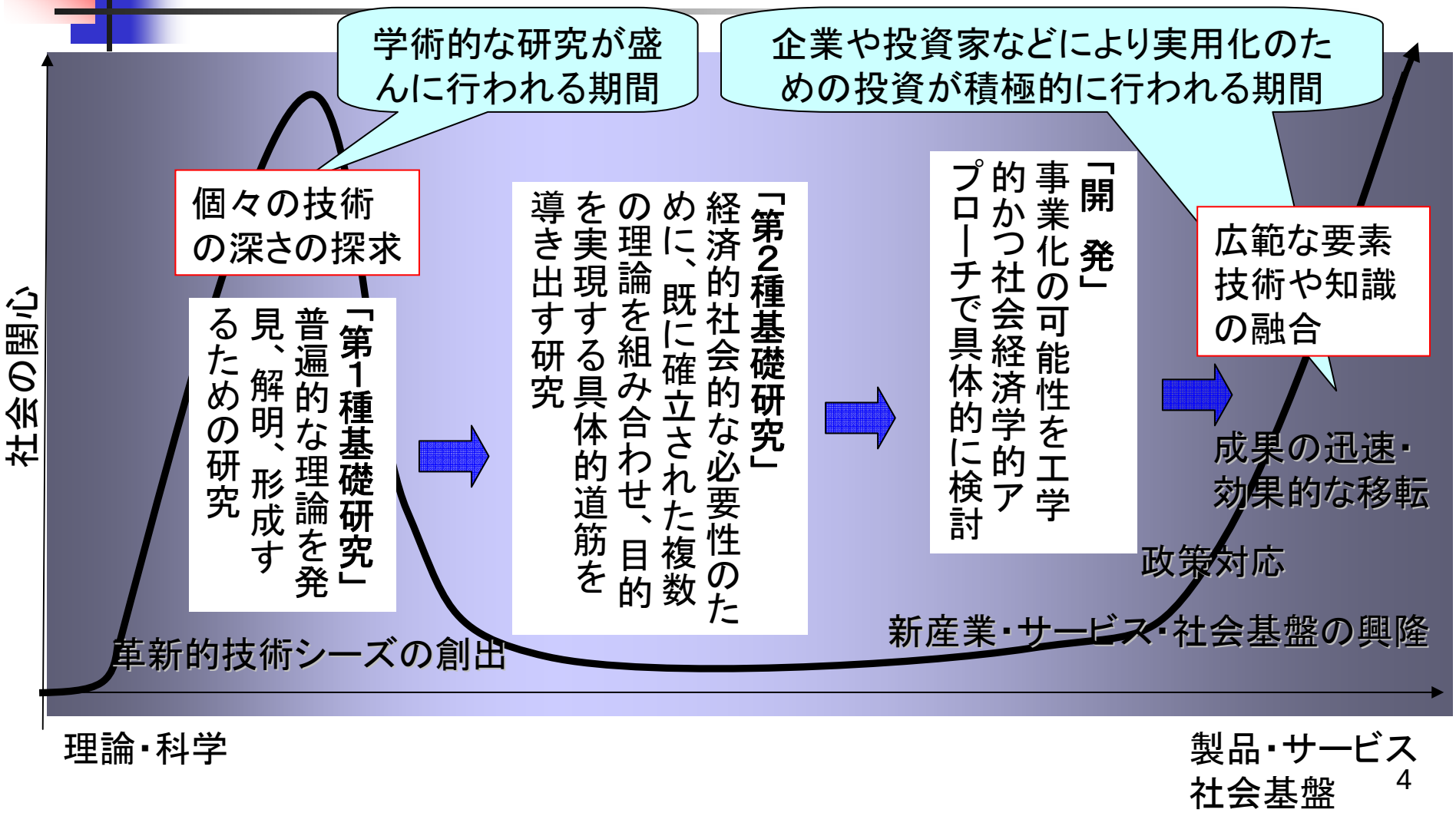
- 研究部門
  - 一定の継続性を持って研究を進める研究ユニット
- 研究センター
  - 研究部門からの派生ないし社会からの要請に応じて、集中的かつ時限的に研究を進める研究ユニット
  - 設置年限は3～7年間
- 研究ラボ
  - 研究部門の新設や研究センター化などの展開を目指して、機動的・時限的に研究を推進する研究ユニット。
  - 設置年限は最長3年。
- 他にも、複数ユニットから構成される領域を組織として定義し代表性を付与した
  - 研究コア・総合センター・連携研究体などがある

情報セキュリティ研究センター

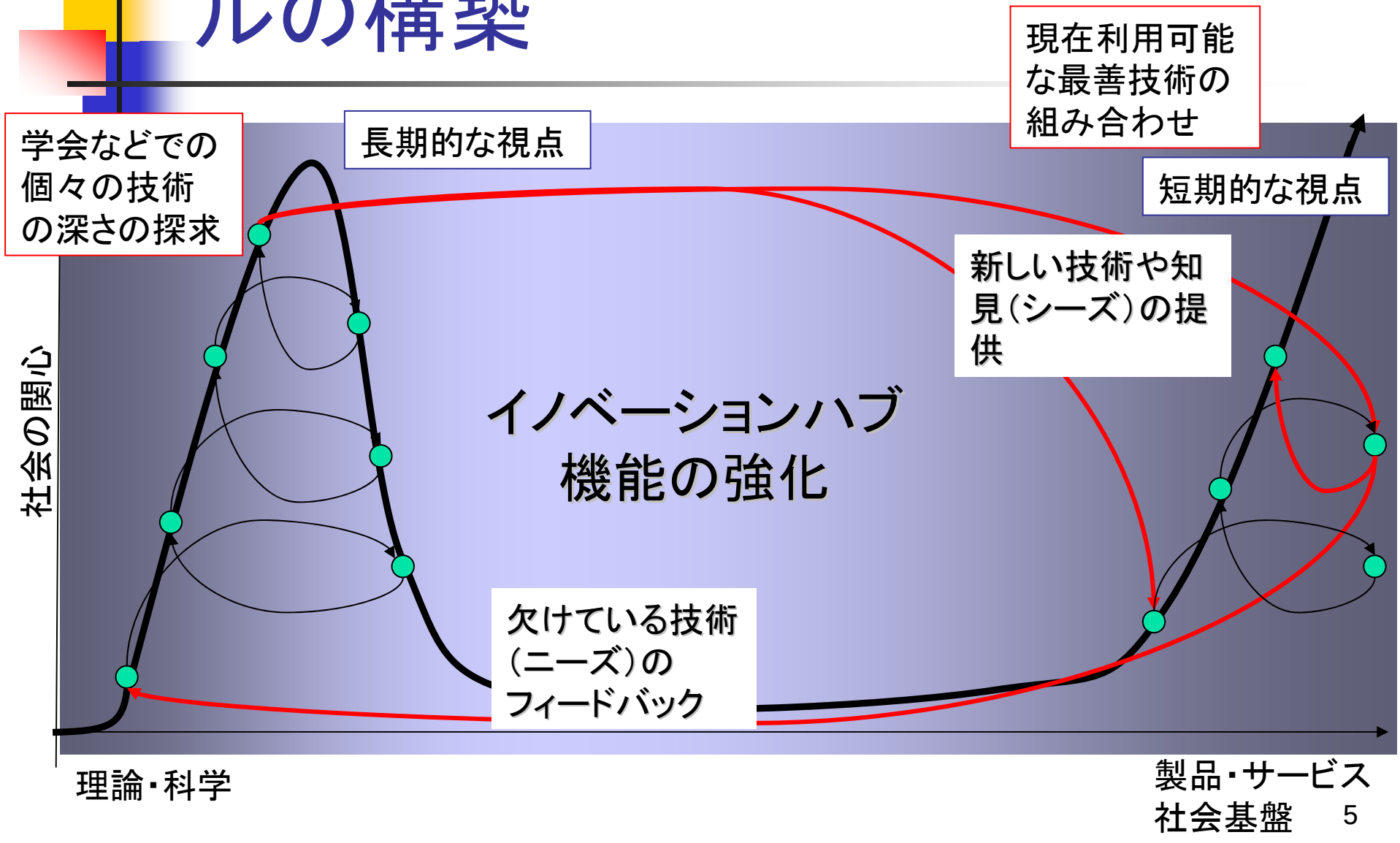
- 社会や政策的要請に応じて設立された研究ユニット
  - ミッション：誰もが安心して利便性を享受できるIT社会の実現



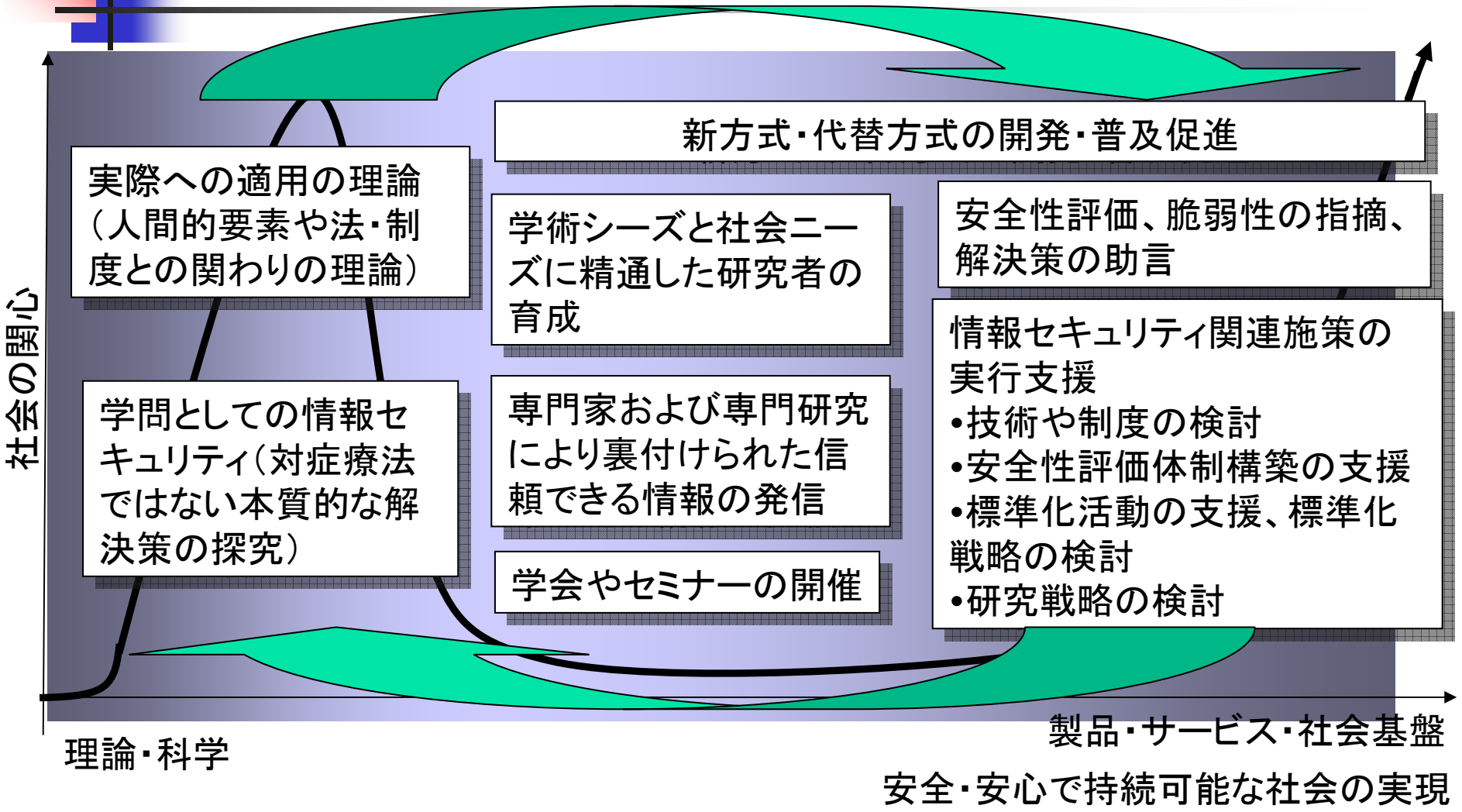
本格研究

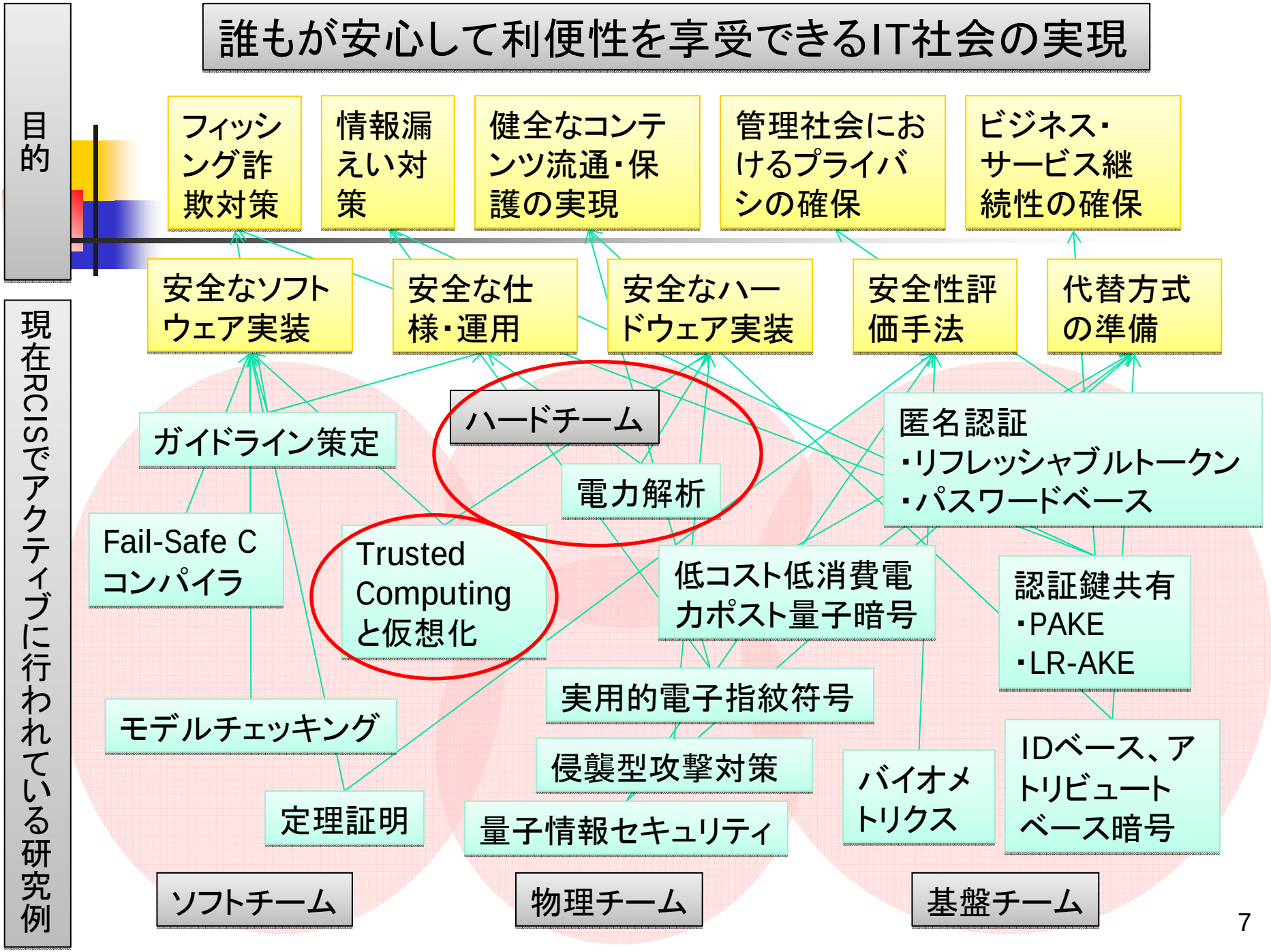

学術的な研究が盛んに行われる期間
企業や投資家などにより実用化のための投資が積極的に行われる期間
個々の技術の深さの探求
「第1種基礎研究」普遍的な理論を発見、解明、形成するための研究
「第2種基礎研究」経済的社会的な必要性のために、既に確立された複数の理論を組み合わせ、目的を実現する具体的道筋を導き出す研究
「開発」事業化の可能性を工学的かつ社会経済学的アプローチで具体的に検討
広範な要素技術や知識の融合
成果の迅速・効果的な移転
政策対応
革新的技術シーズの創出
新産業・サービス・社会基盤の興隆
社会の関心
理論・科学
製品・サービス
社会基盤

より強力なグローバルスパイラルの構築



情報セキュリティ研究センターの活動内容の分類




誰もが安心して利便性を享受できるIT社会の実現
目的
フィッシング詐欺対策
情報漏えい対策
健全なコンテンツ流通・保護の実現
管理社会におけるプライバシの確保
ビジネス・サービス継続性の確保
安全なソフトウェア実装
安全な仕様・運用
安全なハードウェア実装
安全性評価手法
代替方式の準備
現在RCISでアクティブに行われている研究例
ガイドライン策定
ハードチーム
匿名認証
・リフレッシャブルトークン
・パスワードベース
電力解析
Fail-Safe C コンパイラ
Trusted Computing と仮想化
低コスト低消費電力ポスト量子暗号
認証鍵共有
・PAKE
・LR-AKE
実用的電子指紋符号
モデルチェッキング
侵襲型攻撃対策
IDベース、アトリビュートベース暗号
バイオメトリクス
定理証明
量子情報セキュリティ
ソフトチーム
物理チーム
基盤チーム

センターの構成（2008年5月）

研究センター長：今井　秀樹（中央大）

副研究センター長：渡辺　創
米澤　明憲（東大）

研究顧問：　松本　勉　（横国大）

主幹研究員：古原　和邦

セキュリティ基盤技術研究チーム（17（7）名）
研究チーム長：　大塚　玲

物理解析研究チーム（9（6）名）
研究チーム長：　今福　健太郎

ソフトウェアセキュリティ研究チーム（13(7)名）
研究チーム長：　柴山　悦哉（東大）

ハードウェアセキュリティ研究チーム（3(3)名）
研究チーム長：　佐藤　証

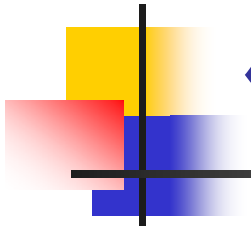
研究系47名（常勤研究職員25，招聘研究員5，PD6，テクニカルスタッフ6，インターン1，非常勤研究職員4，内常駐39）
客員研究員5名，外来研究員3名
事務系5名
合計60名

学問としての情報セキュリティ・実際への適用の理論

- バイオメトリクス評価手法
- 暗号・安全性評価基礎理論
- IDベース・アトリビュートベース暗号
- 量子情報セキュリティ
- 形式手法（モデルチェッキング）
- プライバシ保護技術（匿名パスワード認証）
- 認証鍵共有
- 電子指紋技術・結託耐性符号

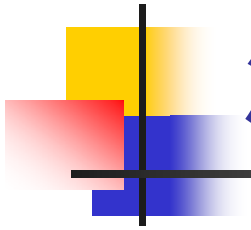
- 左記を中心に学術的な知見が多数得られる
  - 紙上発表：132件
  - 口頭発表：145件
- 受賞
  - Wilkes Award (British Computer Society 最優秀論文賞) [花岡ほか]
  - 電子情報通信学会論文賞 [花岡ほか]
  - IACR Fellow [今井センター長]
  - IACR Asiacrypt 2007論文賞 [Peyrin]
  - 2007年度YRP奨励賞 [張]
  - 情報セキュリティ文化賞[高木、今井センター長]

新方式・代替方式の開発・普及促進



- Fail-Safe C Compiler
- フィッシング防止のためのパスワードHTTPパスワード相互認証プロトコル
- 情報漏えいに堅牢な認証とデータ管理システム
- 匿名認証方式
- Trusted Computingと仮想化

安全性評価、脆弱性の指摘、解決策の助言



- ソフトウェア脆弱性の発見と報告
  - 累積8件
  - GNUTLS, Mozilla の証明書検証の脆弱性 (不正な Parameter フィールドの埋め込みに基づくもの)
    - GNUTLS-SA-2006-4
  - tDiary の任意コード実行脆弱性 (2006-12-10)
- ガイドラインの策定
  - 安全なWebアプリケーション開発のための発注仕様作成ガイドラインの策定
  - 安全なWebサイト利用の鉄則

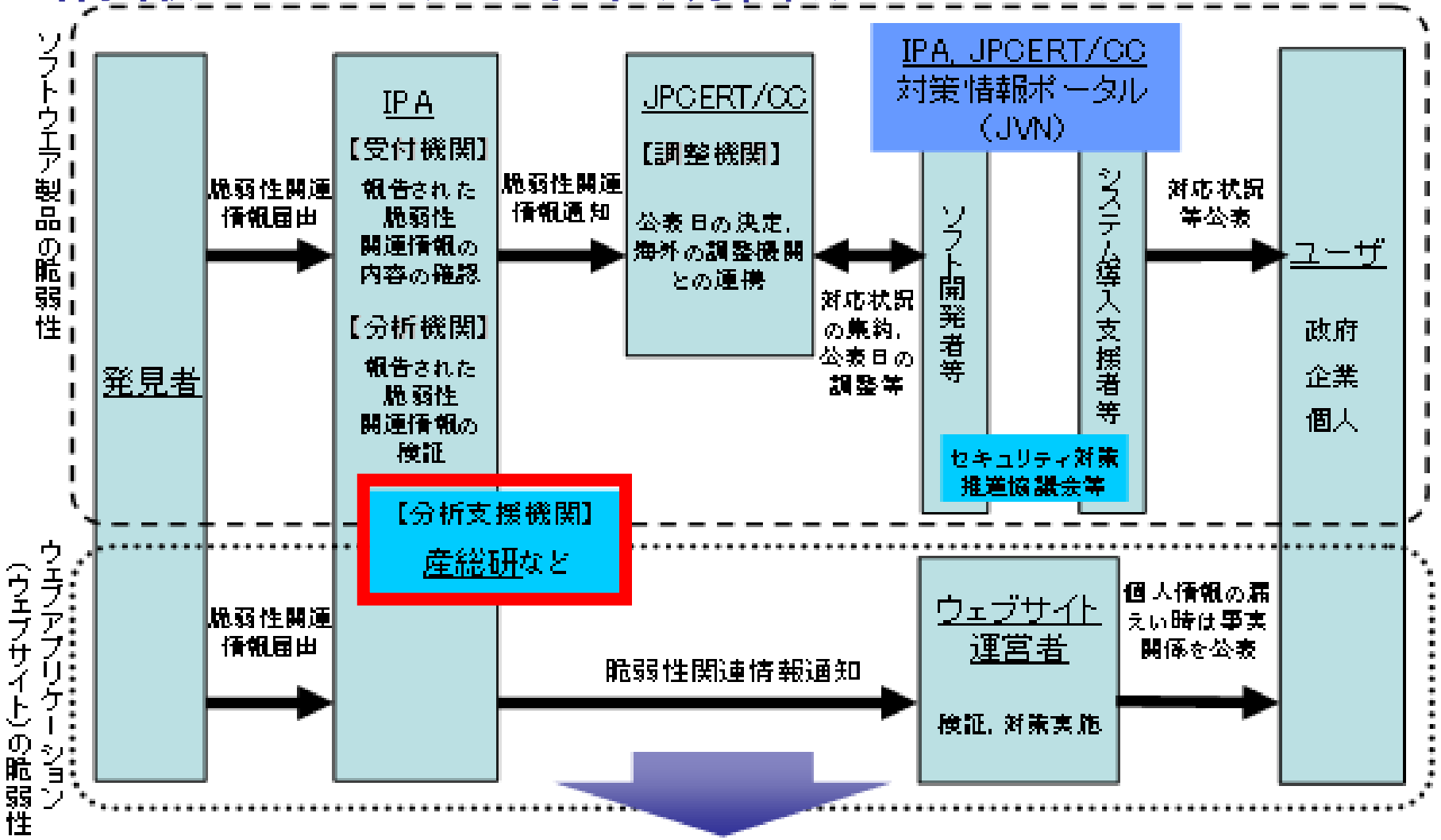
学会やセミナー等の開催

- 2007.8: Trusted Computing に関するサマースクールを大学、企業などと開催（中国珠海）
- 2007.10: 国際量子暗号会議 (UQC 2007) をIPA, NICT と開催
- 2007.10: サイエンスカフェ@アキバ～研究者が思うこと、企業ができること～を開催
  - 研究者と企業の方々との間の気軽なコミュニケーション
- 2008.3: ACM Symposium on Information, Computer and Communications Security (ASIACCS‘08) を開催
- 2008.12頃:国際量子暗号会議 (UQC 2008)

情報セキュリティ関連施策の実行支援(1/3)

- 情報処理推進機構 (IPA)、JPCERT/CC
  - 情報セキュリティ早期警戒パートナーシップの分析機関として協力
- 内閣官房情報セキュリティセンター(NISC)
  - メンバーを派遣し
  - 暗号行政の推進などに貢献
- 米 NIST(National Institute of Standards and Technology)
  - 定期的に情報交換
  - 開発したボード SASEBO の提供
  - 研究者を派遣中（5月より1年間）

情報セキュリティ早期警戒パートナーシップ



【期待効果】

①製品開発者及びウェブサイト運営者による脆弱性対策を促進
②不用意な脆弱性関連情報の公表や脆弱性の放置を抑制
③個人情報等重要情報の流出や重要システムの停止を予防

※IPA：独立行政法人 情報処理推進機構、JPCERT/CC：有限責任中間法人 JPCERT コーディネーションセンター、産総研：独立行政法人 産業技術総合研究所

情報セキュリティ関連施策の実行支援(2/3)

- CRYPTREC（暗号技術検討会、暗号技術監視委員会、暗号モジュール委員会）
  - 座長、構成員、委員長および委員を派遣
- 情報処理推進機構(IPA)「JCMVP」
  - 委員長、副委員長兼座長を派遣
- 科学技術振興機構 研究開発戦略センター(JST/CRDS)
  - 国際技術力比較と注目研究開発動向報告書作成

情報セキュリティ関連施策の実行支援(3/3)

- ISO/IEC JTC1 SC27
  - Project Editor ２名を派遣
- 日本規格協会
  - 「アイデンティティ管理技術標準化調査研究委員会」
  - 「耐タンパー性標準化調査研究委員会 」
  - 委員長、主査、委員を派遣
- 日本自動認識システム協会
  - 「バイオメトリクスアプリケーションインターフェース標準規格へのアプリケーションの適合性試験に関する標準化委員会」
  - 座長および委員を派遣

ご清聴ありがとうございます

- 企業・大学との共同・受託研究も複数行っております。
- まずは、お気軽にご相談ください。