National Institute of Advanced Industrial Science and Technology
AIST

Research Center for Information Security

セキュリティ基盤技術の動向

セキュリティ基盤技術研究チーム
研究チーム長　大塚　玲

National Institute of Advanced Industrial Science and Technology
AIST

目標

Research Center for Information Security

- 大目標：安全かつ安心な社会の実現に貢献する
- 確固とした安全性基礎理論の構築
  - 確固とした理論に基づいて実際的な情報セキュリティ問題に挑戦する。
  - さまざまな情報セキュリティ領域において、安全性概念や攻撃モデルの形式化を行い、強度関係を明確にする。
- 既存の情報セキュリティ基盤に不足している機能の追加および問題点の克服
  - 主要情報セキュリティ領域
    - プライバシー保護
    - 著作権保護
    - 情報漏えい対策
    - 代替方式
    - ヒューマンクリプト

National Institute of Advanced Industrial Science and Technology
AIST

セキュリティ基盤技術 研究課題

Research Center for Information Security

プライバシー	著作権保護	耐漏洩機能	代替方式	ヒューマンクリプト
プライバシー保護技術に関する研究	著作権保護技術に関する研究	漏えいに強い機能に関する研究	仮定が崩れた場合の対処方法や代替方式	ヒューマンエラーに強く、わかりやすいセキュリティ技術
軽量匿名認証技術 ブラインド署名技術 匿名パスワード鍵交換	結託耐性符号 電子透かし技術 放送暗号	漏洩耐性を持つ鍵交換技術 鍵漏洩に対して堅牢な公開鍵暗号(Key-Insulated Encryption)	情報量的安全性 符号に基づく公開鍵暗号	バイオメトリクスセキュリティ 漏洩耐性を持つパスワード鍵交換

基礎理論・未開拓領域

暗号理論

IDベース暗号　CMA安全な電子署名

高機能暗号　CCA安全な公開鍵暗号

暗号強度評価

情報セキュリティ管理

情報セキュリティROI

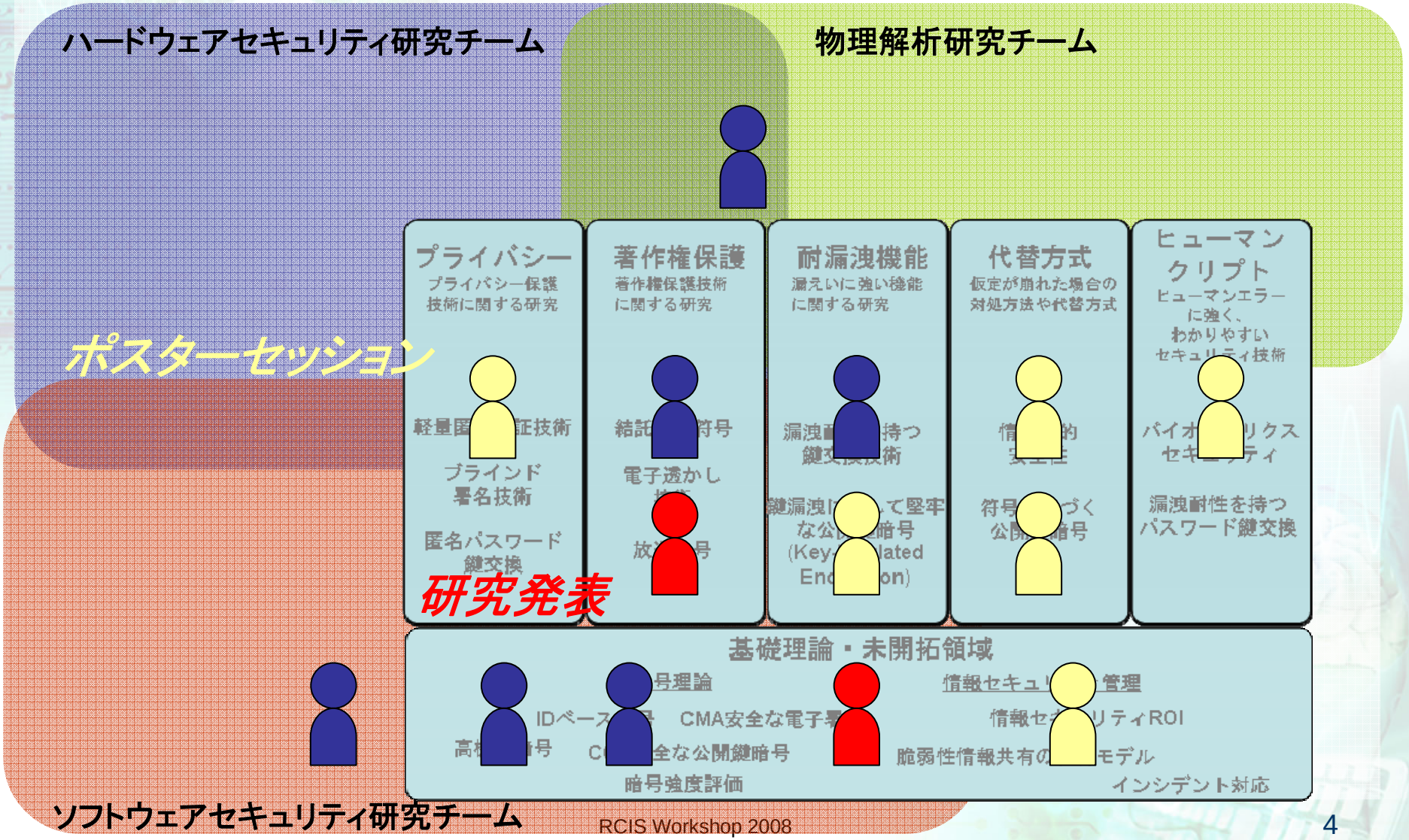
脆弱性情報共有の経済モデル

インシデント対応

National Institute of Advanced Industrial Science and Technology
AIST

本日の研究発表

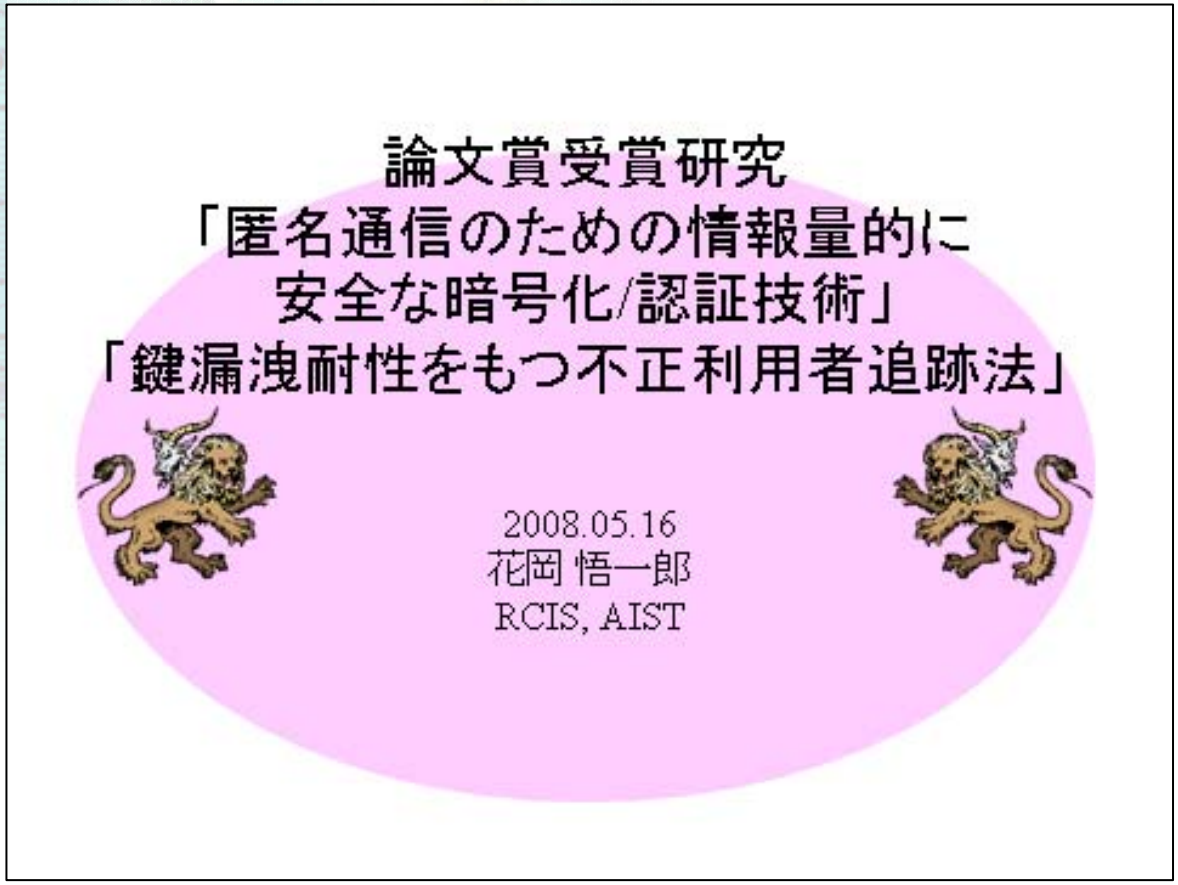
Research Center for Information Security



National Institute of Advanced Industrial Science and Technology
AIST

セキュリティ基盤技術研究チームからの発表①

Research Center for Information Security



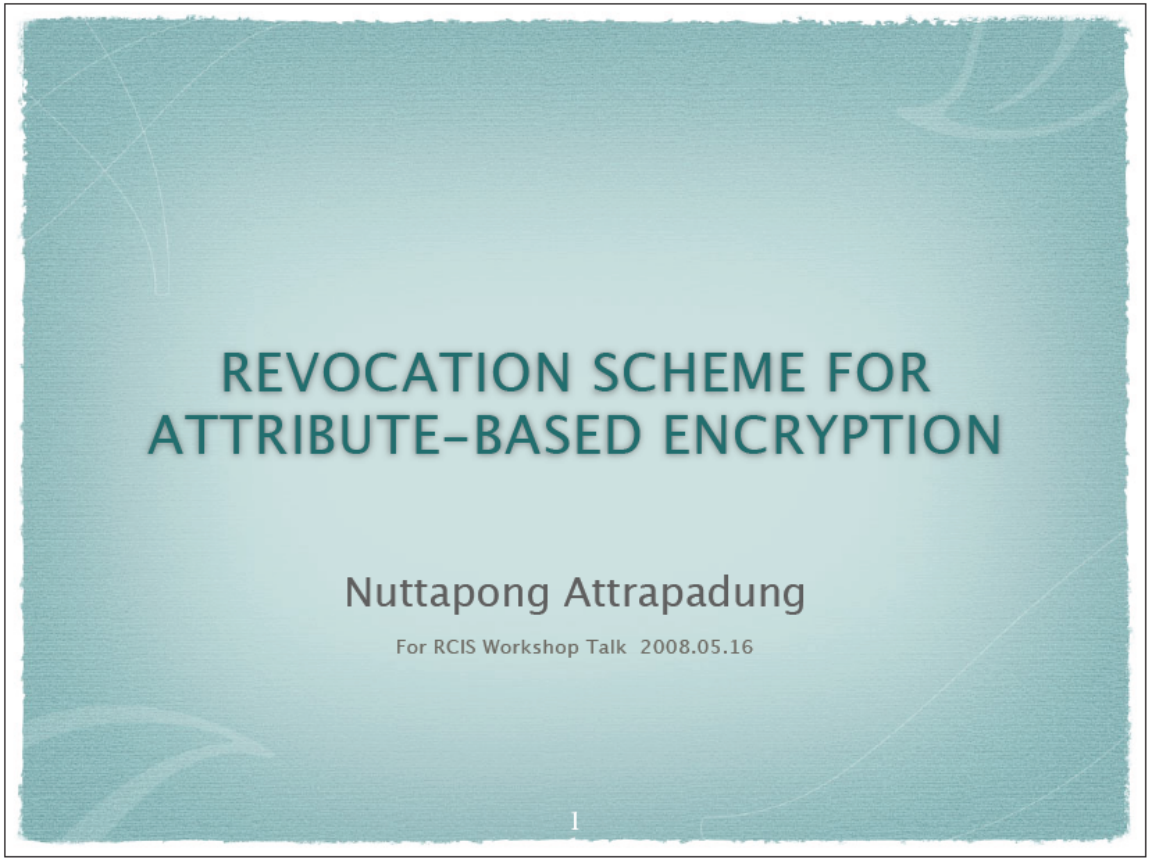
花岡 悟一郎
（研究員）

British Comp. Society「The Wilkes Award」
電子情報通信学会「Best Paper Award」
受賞研究に関する内容

National Institute of Advanced Industrial Science and Technology
AIST

セキュリティ基盤技術研究チームからの発表②

Research Center for Information Security



ナッタポン アットラパドゥン

Attrapadung Nuttapong

（研究員）

National Institute of Advanced Industrial Science and Technology
AIST

セキュリティ基盤技術研究チームからの発表③

Research Center for Information Security

辛 星漢
SeongHan Shin
（研究員）

National Institute of Advanced Industrial Science and Technology
AIST

セキュリティ基盤技術研究チームからの発表(ポスター)

Research Center for Information Security

- 崔 洋 (Yang Cui)（JSPS特別研究員）
  - Code-Based Public-Key Cryptosystem and Its Application
- Frederique Oggier（特別研究員）
  - Information Theoretic Security for Multiple Antenna Communication
- 井沼 学（招聘研究員）
  - バイオメトリクスセキュリティの評価
- 繁富 利恵：研究員
  - 匿名認証を用いたセキュアなプローブシステムの検討
- 田沼 均（研究員）
  - 情報セキュリティと社会
- 辛 星漢 (SeongHan Shin)（研究員）
  - A Leakage-Resilient Authentication and Data Management System