

物理を用いたセキュリティ技術の動向

@平成19年度研究成果発表会 (RCIS Workshop 2008)

2008年5月16日
物理解析研究チーム
チーム長 今福健太郎

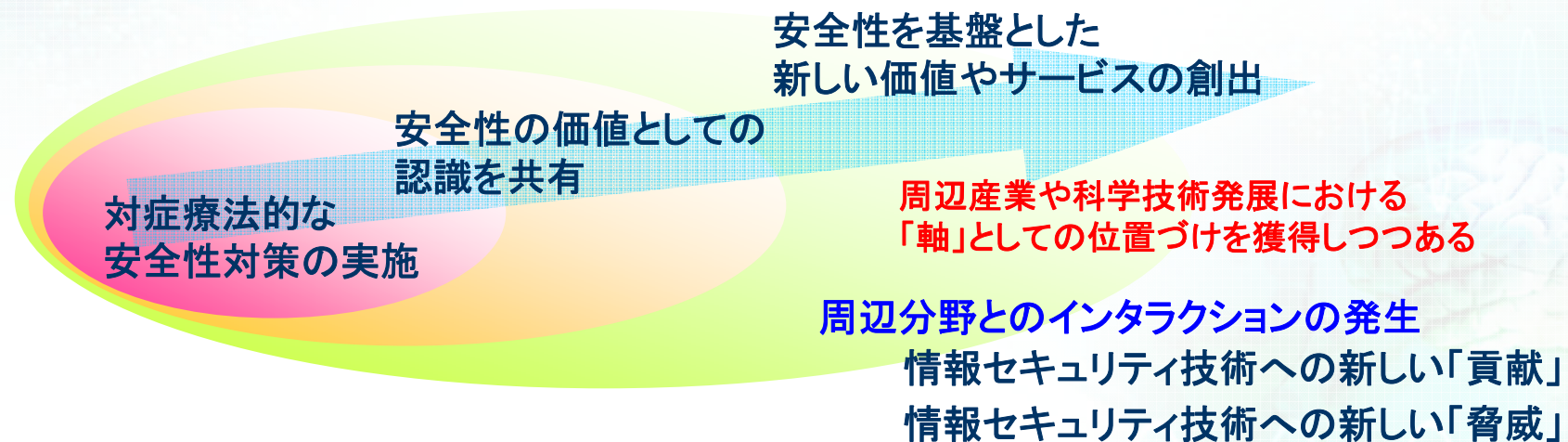


National Institute of
Advanced Industrial Science
and Technology
AIST

RCIS
Research Center for
Information Security

分野の背景、問題の所在など

- 情報セキュリティ技術を取巻く環境の変化
利用される状況の拡大と多様化
- 情報セキュリティ技術に対する価値観の拡大
「付加的な価値」から「新しい価値」へ



■ 周辺分野とのインタラクション

■ 新しいタイプの問題

- 情報セキュリティ技術への新しい貢献
- 情報セキュリティ技術への新しい脅威

■ 問題を複合的かつ複雑化する要因

■ セキュリティ技術への誤解

- セキュリティ技術の考え方や方法論は(セキュリティの研究者が考えるほど)必ずしも広く浸透していない
 - 誤解に基づく新たなセキュリティホールの出現の危険性

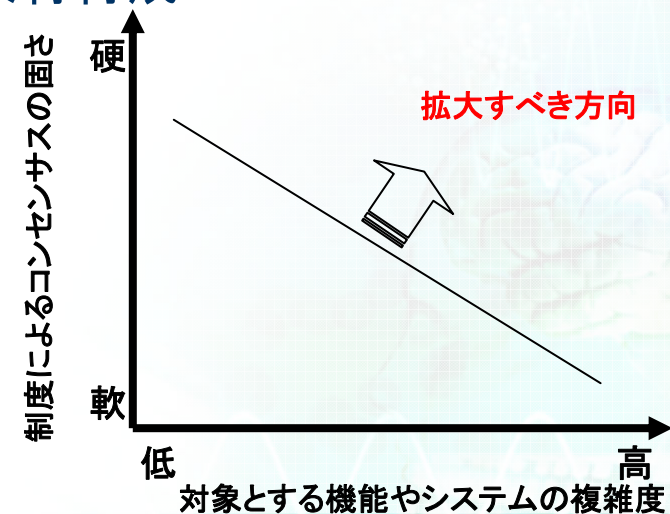
■ 周辺技術の高度化・細分化

- 分野ごとの事情や背景をセキュリティ技術者・研究者が必ずしも的確に把握していない
 - コミュニケーションの不足、発展の阻害

特に、情報セキュリティ技術と「モノ」の技術のインタラクションによる問題が顕在化

- 評価・認証制度などを通じたコンセンサスの形成
万能ではないが有効なアプローチの一つ
 - 制度の利用者が参照可能な情報を提供
 - セキュリティ技術の知見、考え方の反映が可能
JCMVP(ISO/IEC 19790),CC(ISO/IEC15408),・・・など
- 研究コミュニティへの要請
 - 評価技術の確立、研究環境の構築、人材育成
 - 次世代技術への対応
シーズや脅威の発掘
 - 科学としてのセキュリティへの昇華

短期、中期、長期的視点の必要性






National Institute of
Advanced Industrial Science
and Technology
AIST

PCIS
Research Center for
Information Security

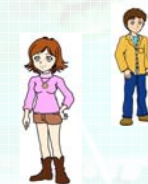
事例と取組みの紹介

事1) ISO/IEC15408関連動向

- ISO/IEC15408（情報技術セキュリティ評価基準）
 - ICチップ、スマートカードなどにも適用
 - 評価方法は実質的に欧州の協議体により決定
 - 評価は欧州が独占状態
 - 国内ベンダーも市場競争上、信用力のある欧州でのセキュリティ評価・認証を利用
 - 欧州主導の評価体制を利用しなければならない不利益
 - 設計技術の流出
 - 市場導入の遅れ
 - 国内評価技術の空洞化
- 
- 国内における評価技術の確立をめざした議論
 - 欧州協議体へ貢献可能な技術蓄積の必要性
 - 評価機関の確立をめざして

事1) 関連プロジェクト

- セキュリティ基盤、ハードウェアセキュリティ研究の両チームとの連携
 - 経産省 SASEBOプロジェクト (H18ーH20)
 - 経産省 新世代情報セキュリティ研究開発 (H17ーH19)
 - 半導体故障解析技術(EBテスト、二次元裏面発光顕微鏡等)の侵襲型解析装置としての性能評価
 - 動作発光データによる設計情報の絞込み
 - 文科省 科学振興調整費 (H18ーH20)
 - 二次元裏面発光顕微鏡を利用した侵襲型解析環境の開発



- 限定された状況であれば既に十分に実用レベルに達しており、製品としての入手も可能
 - ユーザに従来とは質的に異なる安全性を提供することができる
 - 試験的導入事例は既に幾つか存在している
 - 一方、本格運用については未だ見るべき実績はない
 - 本格運用にとって重要な課題は「無条件安全性が達成されること」であるわけではない
- 認証制度あるいは“標準化”の効能
 - 誤解に基づいて設計・開発されたものなど、ユーザや社会にとって不利益となる製品が誤った認識に基づいて広まることを防ぐことができる
 - 適切な認証制度あるいは標準化の導入により、量子情報セキュリティ技術の適切な導入ドメインやアプリケーションを定義することも可能



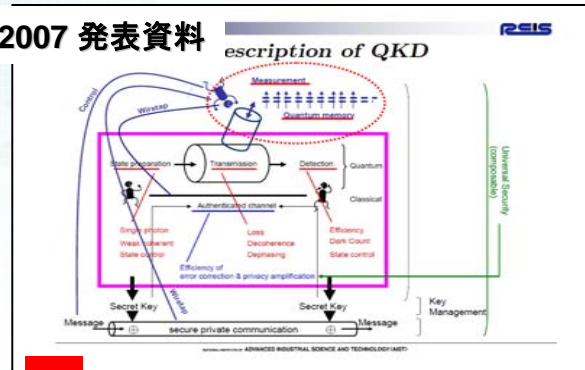
- 海外における評価・認証制度の確立をめざした議論
 - 米) NIST/Cambridge MIT Institute Initiative
 - 欧) SECOQC (ETSI) Initiative
 - 米) Telcordia Initiative
 - セキュリティ技術(セキュリティ機能)としてのコンセンサス
 - 通信技術としてのインターオペラビリティ
 - 将来的な認証制度や品質保証に必要な技術開発課題の展望

■ 国際会議UQC2007の開催

- NICT, IPA, AISTの三機関主催 10/1—10/3 @秋葉原
- 国内外から産官学関係者の出席



UQC2007 発表資料



攻撃者の特徴づけ

Examples/Images, Cont.

Attacker issues:

- Practical Parameters
 - A) Unbounded quantum memory
 - B) Bounded quantum memory, 100 qubit/s
 - C) No quantum memory
 - D) Photon counter with efficiency WW %
 - E) Etc...
- Attack strategies
 - a) Coherent attack with the unbounded quantum memory & known message attack
 - b) Individual attack only to quantum channel
 - c) Etc...

Level	Practical Parameters	Strategy of Attacks	Security Definition
Level 1	C) D)	c)	II)
Level 2	B) D) E)	b) c) I)	I)
Level 3	A) D) E)	a)	I)

攻撃者の特徴付けと安全性の定義により「レベル」を導入

Examples/Images

Legitimate Users issues:

- Protocols
 - BB84 with single photon state (and specific error correction & privacy amplification schemes)
 - Decoying BB84 with WCS (and specific...)
 - Plug and Play BB84 with WCS (and specific...)
 - Etc...
- Practical Parameters
 - X) Transmission loss (optic fiber + Sys.) XX dB/km, YY dB Z) Etc.
 - Y) Efficiency of detector, ZZ %
- Security Definition
 - I) Universal Security
 - II) Security based on Estimation of Eve's Accessible Information
 - III) Etc.

正規ユーザーの特徴づけ

プロトコル

Examples/Images, Cont.

	Level 1	Level 2	Level 3
BB84 with single photon state (and specific...)	must be used within X km with X1,Y1,Z1	must be used within Y km with X1,Y1,Z1	must be used within R km with X1,Y1,Z1
Decoying BB84 with WCS (and specific...)	must be used within P km with X1,Y1,Z1	must be used within Q km with X1,Y1,Z1	must be used within C km with X1,Y1,Z1
Plug and Play BB84 with WCS (and specific...)	must be used within A km with X1,Y1,Z1	must be used within B km with X1,Y1,Z1	must be used within C km with X1,Y1,Z1
Protocol Z (and specific...)	N.A with X1,Y1,Z1	N.A with X1,Y1,Z1	N.A with X1,Y1,Z1

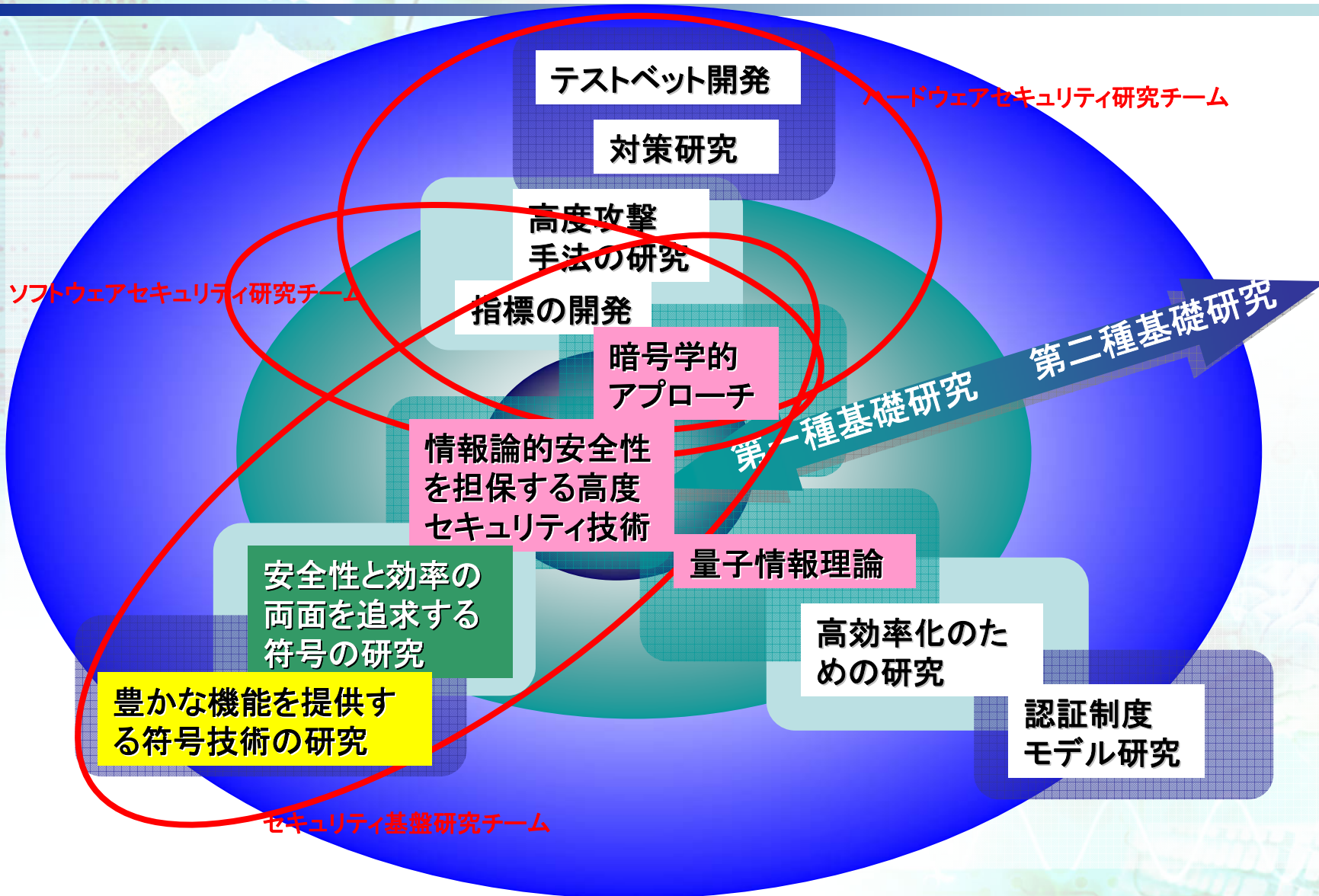
どのような条件で実装・運用されるべきか



National Institute of
Advanced Industrial Science
and Technology
AIST

RCIS
Research Center for
Information Security

メンバーの紹介



■ 講演

■ 縫田 光司 (ぬいだ こうじ)

- 電子指紋技術に用いる符号の設計と安全性評価

■ ポスター

■ 張 銳 (ちょう えい)

- Public key encryption with keyword search on encrypted data

■ Kirill MOROZOV (きりる もろぞふ)

- Information-theoretically secure commitment based on noisy channel

■ 萩原 学 (はぎわら まなぶ)

- セキュリティ技術をもっと身近に ~印刷された二次元コードを守れるか~

■ 宮寺 隆之 (みやでら たかゆき)

- Uncertainly relations and quantum information security

■ 木村 元 (きむら げん)

- How to detect correlation from information of subsystem?