National Institute of Advanced Industrial Science and Technology
AIST

Research Center for Information Security

ソフトウェアセキュリティ技術の動向

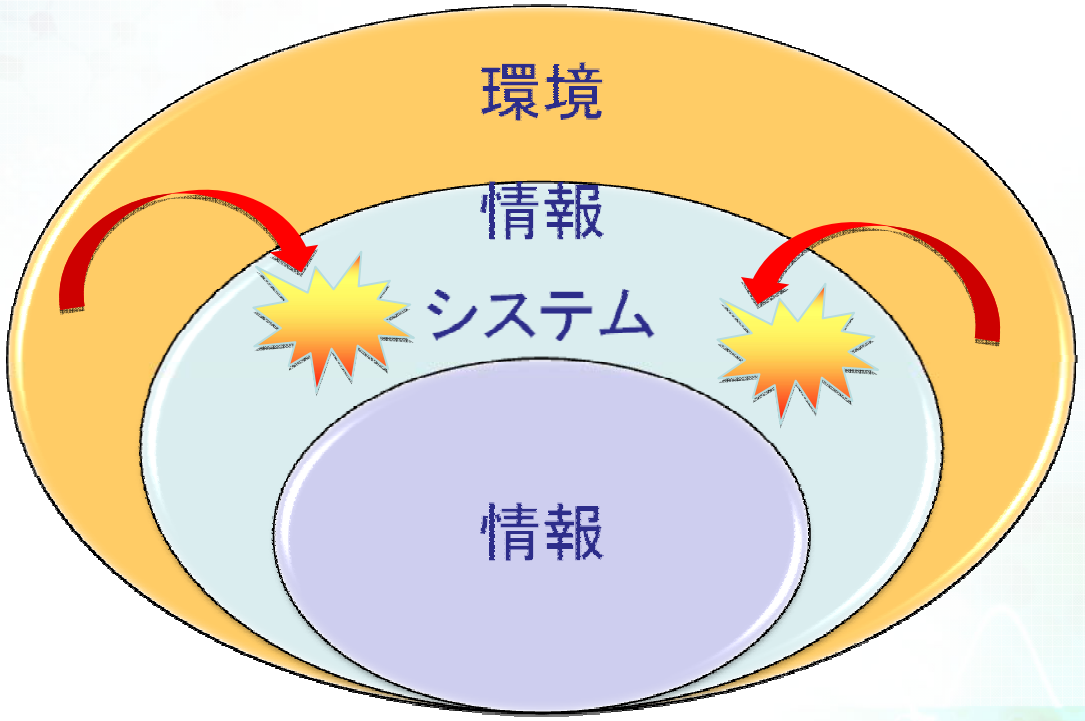
ソフトウェアセキュリティ研究チーム長
柴山悦哉

National Institute of Advanced Industrial Science and Technology
AIST

システムのセキュリティ

Research Center for Information Security

- 情報セキュリティにとって，情報システムのセキュリティは重大な関心事
  - デジタル情報を直接管理するは情報システム

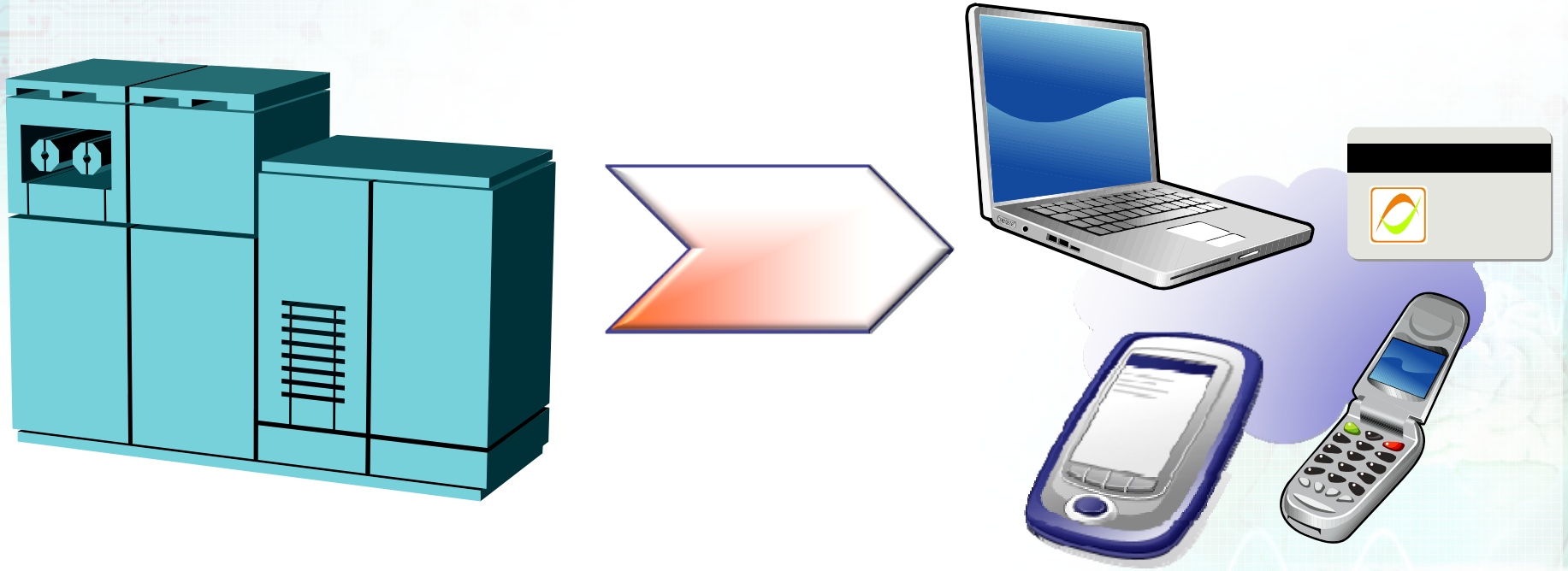


National Institute of Advanced Industrial Science and Technology
AIST

情報システムの多様化

Research Center for Information Security

- 機器の小型化と分散化が進んでいる
  - 個々の機器の自律性は低下
  - 個々の機器はもちろん，接続点も攻撃対象になる

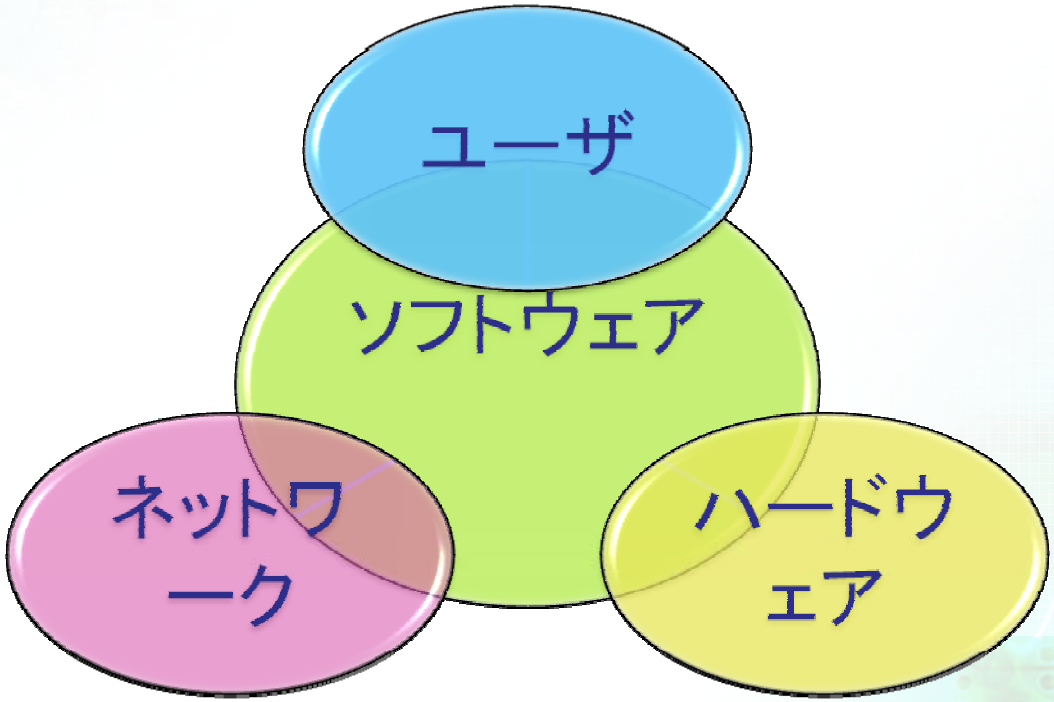


National Institute of Advanced Industrial Science and Technology
AIST

ソフトウェアのセキュリティ

Research Center for Information Security

- ソフトウェアもまた情報の一種
  - （ハードウェアより）改竄されやすい
    - 改竄されると情報システムの制御ロジックが壊れる
  - 取り巻く環境が多様



National Institute of Advanced Industrial Science and Technology
AIST

チームの主な研究活動

Research Center for Information Security

- ソフトウェアの保護
  - メモリ安全なプログラミング言語 Fail-Safe C
- ハードウェアと連携した信頼(trust)の確立
  - TPMを使った Trusted Boot
- ネットワーク型プログラムのセキュアな構築支援
  - ソースコードレベルのモデル検査
  - 暗号プロトコルの検証
  - Webアプリケーションのガイドライン

National Institute of Advanced Industrial Science and Technology
AIST

Fail-Safe C (1/3)

Research Center for Information Security

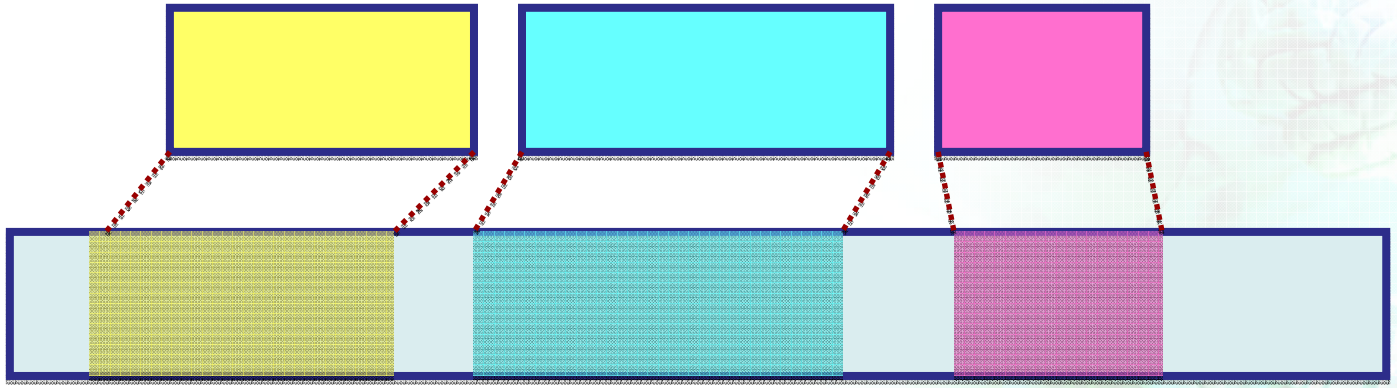
- C言語の問題点
  - 安全性より実行性能と記述力を重視
    - 時代背景が現在とは異なる
  - C言語特有のセキュリティホールが蔓延
    - e.g. バッファオーバーフローバグ
    - メモリ関係の脆弱性が多い
  - 多くのアプリケーション（サーバ等）が C言語で記述されている

National Institute of Advanced Industrial Science and Technology
AIST

Fail-Safe C (2/3)

Research Center for Information Security

- 結局，何が問題か？
  - 低級言語(e.g. 機械語)のメモリモデルはフラット
    - セキュリティドメインを構成できない
  - 高級言語のメモリモデルは構造的
    - セキュリティドメインを構成できる
  - C言語のメモリモデルは，高級言語の皮をかぶった機械語のもの

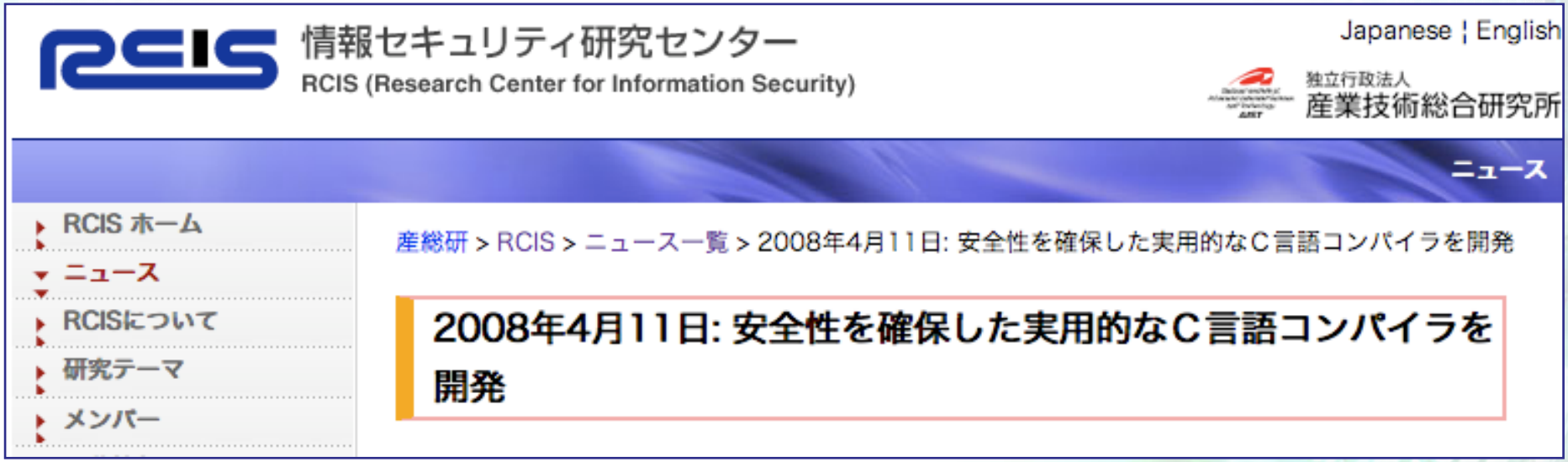


National Institute of Advanced Industrial Science and Technology
AIST

Fail-Safe C (3/3)

Research Center for Information Security

- メモリ安全な C 言語処理系
  - メモリブロック間に壁を設けることができる
- ANSI/ISO/JIS 規格準拠
  - 既存ソフトと高い親和性
- Release 1 を 2008年4月11日に公開

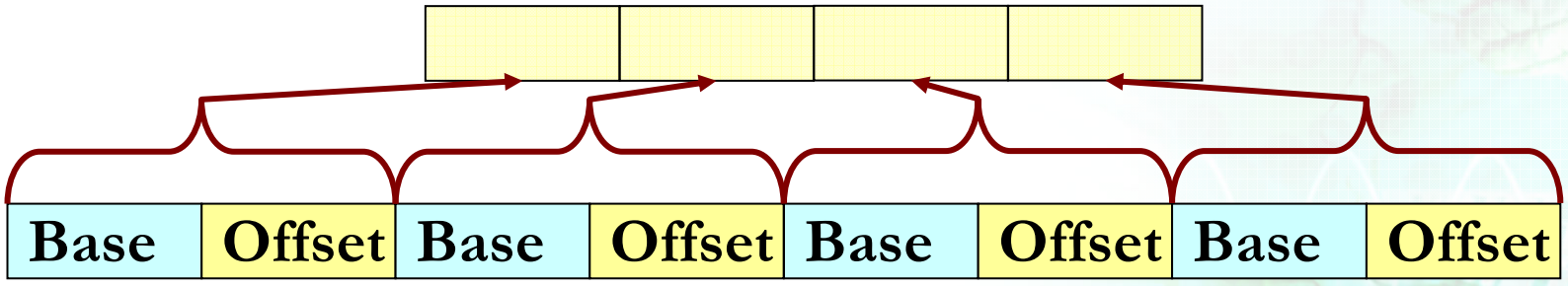


National Institute of Advanced Industrial Science and Technology
AIST

Fail-Safe C の実現技術

Research Center for Information Security

- Fail-Safe C の基本的なアイデア
  - ポインタと整数をBaseと offset の組に拡張
    - ポインタ演算はoffset への操作
  - メモリをブロック単位で管理
    - 境界とデータ型の情報を各ブロックが保持
    - Offsetが範囲外，型が異なる等なら，アクセス不許可
  - Virtual offset
    - ポインタや整数を，仮想的には1ワードと見なす



National Institute of Advanced Industrial Science and Technology
AIST

Fail-Safe の意味

Research Center for Information Security

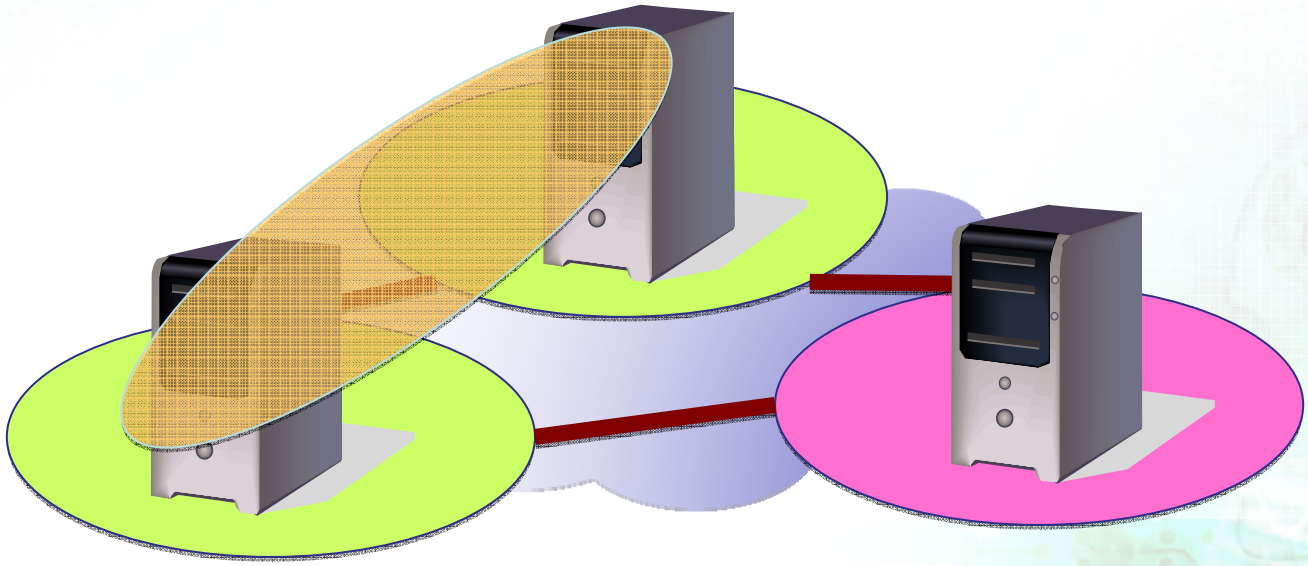
- クラッシュするかもしれないが乗っ取られない
  - メモリ安全性を保証する代わりに，バグのあるプログラムの実行は保証しない

National Institute of Advanced Industrial Science and Technology
AIST

暗号プロトコルの検証 (1/4)

Research Center for Information Security

- 分散ソフトウェアのセキュリティは，単体ソフトウェアのセキュリティの単純な組み合わせではない
  - メモリだけではなくメッセージも守る必要がある
- 機器の境界を超えたセキュリティドメインが必要
  - チャネルの保護とメモリの保護はかなり異なる



National Institute of Advanced Industrial Science and Technology
AIST

暗号プロトコルの検証 (2/4)

Research Center for Information Security

- 世間一般の考え方
  - 厳密性が必要なら，数学的に証明しよう
- ソフトウェアの専門家の考え方
  - 厳密性が必要なら，人間が書いたものを簡単には信じるべきでない
  - 人間が書いた機械可読な証明を機械的にチェックしたら，まあ信じてやるか

Manually Provable Security → Mechanically Provable Security

National Institute of Advanced Industrial Science and Technology
AIST

暗号プロトコルの検証 (3/4)

Research Center for Information Security

- ソフトウェア検証の枠組みを暗号プロトコルの検証に利用
  - 攻撃者の手順と暗号プロトコルを確率的ゲームと捉え，これを確率的プログラミング言語でモデル化
  - 確率的な操作的意味を定理証明支援系 Coq で定義
  - 意味を確率的に保存するプログラム変換により，既知の困難な問題に還元
  - この過程の正当性を Coq を用いて証明

National Institute of Advanced Industrial Science and Technology
AIST

暗号プロトコルの検証 (4/4)

Research Center for Information Security

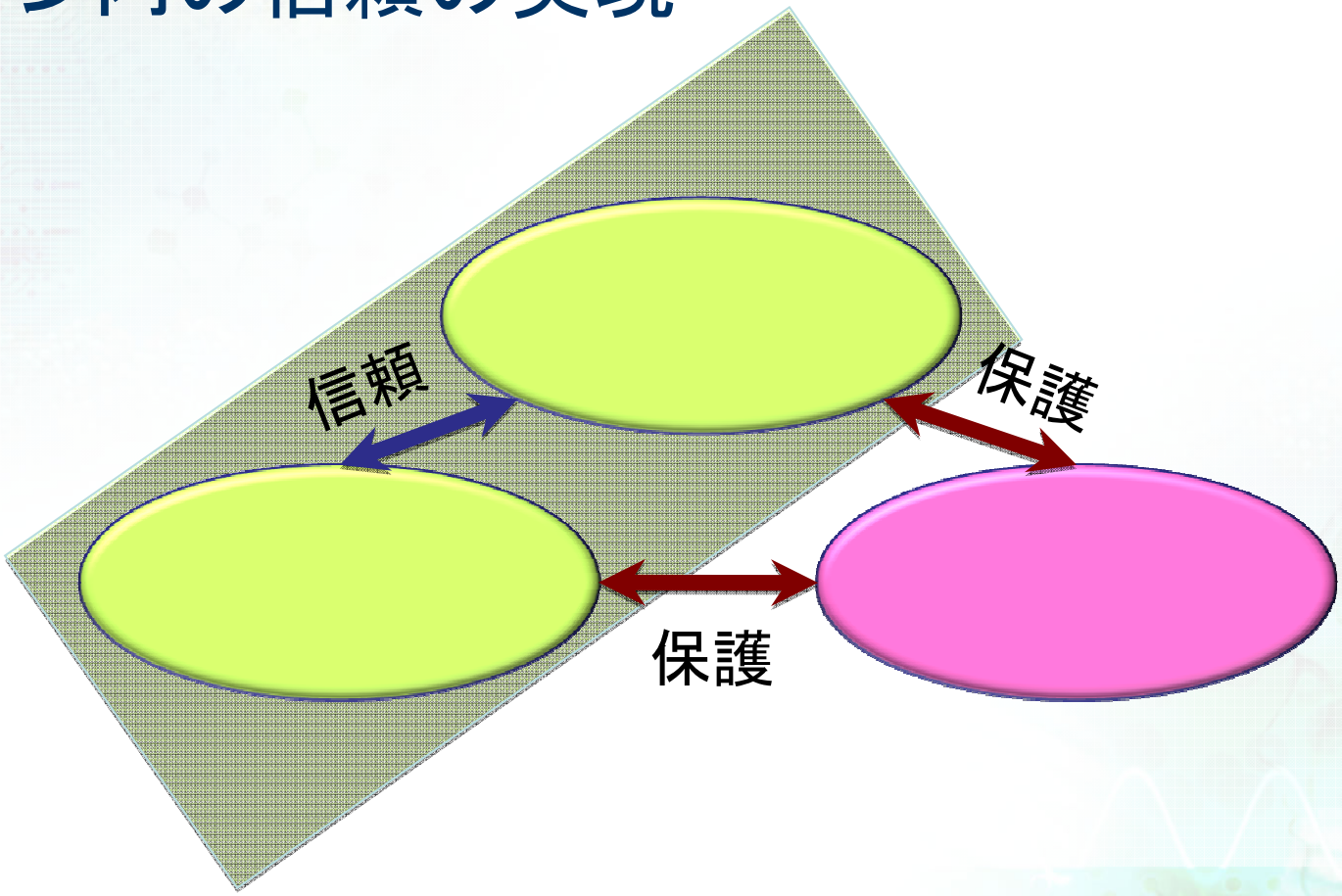
- 人間にも機械にも可読な証明を記述する方法の大枠が見えてきた段階
  - ElGamalなどの例題には適用済み
- 計算の複雑さとプログラムの意味論の境界領域を開拓中
  - 同じ理論計算機科学でも，量の科学と質の科学は別世界
- 目指すべきは，プロトコルの正しさとソフトウェアの正しさの同時証明

National Institute of Advanced Industrial Science and Technology
AIST

信頼と保護

Research Center for Information Security

- セキュリティドメイン間の保護とセキュリティドメイン内の信頼の実現



National Institute of Advanced Industrial Science and Technology
AIST

主な成果

Research Center for Information Security

- Fail-Safe C
  - メモリブロックの間に壁を作る
- 暗号プロトコルの検証
  - チャネルの保護の正しさを厳密に証明
- Trusted Boot
  - TPMをベースに信頼関係の連鎖を構成
- ネットワークアプリケーションのモデル検査
  - 並行動作にともなう干渉の検査
- Webアプリケーションのガイドライン
  - セッションの保護，クロスドメインの干渉の防止，証明書の使い方等をガイド

National Institute of Advanced Industrial Science and Technology
AIST

今後の方向性

Research Center for Information Security

- 従来の常識
  - ソフトウェア研究者にとって，暗号やハードウェアは他人任せの分野
    - e.g. Perfect encryption の仮定
    - e.g. ハードウェアは完全であるか，あるいは比較的単純な故障モデルに従って壊れる
- 実際のところは
  - 計算量的暗号が破れる確率は，低いかもしれないがゼロではない
  - サイドチャネル攻撃等も存在しうる
- この種のギャップの存在が弱点となる可能性も想定する必要がある