National Institute of
Advanced Industrial Science
and Technology
AIST

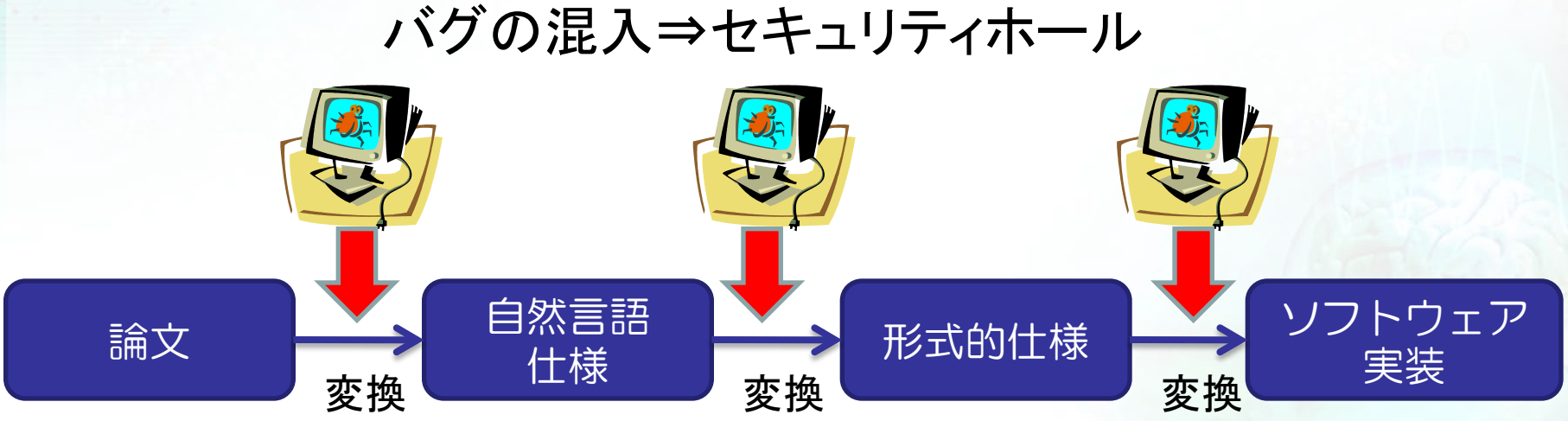
Research Center for
Information Security

研究成果と今後の展開

産業技術総合研究所
情報セキュリティ研究センター（RCIS）
2011年2月1日

セキュリティ事故の防止に向けて

- 主な原因：ソフトウェア実装のミス
  - 数学的に安全性が証明された暗号技術
  - 実装のミス⇒安全性が崩壊
    - 例：乱数の実装ミス



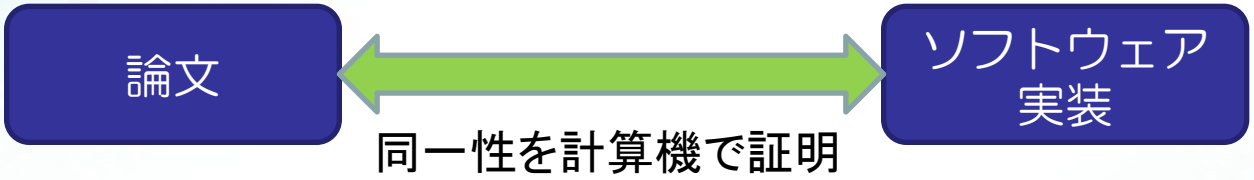
National Institute of Advanced Industrial Science and Technology
AIST

最近の研究成果

Research Center for Information Security

- 暗号処理プログラム（機械語レベル）の
  - 暴走せずに動作
  - 常に正しい計算結果を出力
  - 暗号として満たすべき数学的な性質を充足

  全ての性質を直接的に計算機で証明する手法を開発



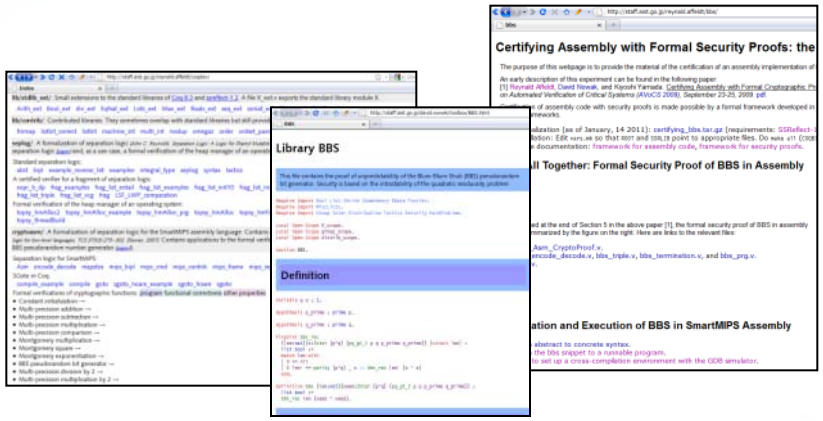
- 必要となった技術
  - 数学的性質を計算機上で表現する際のギャップを埋める定理の証明
    - 例：連続値を0,1で計算機上で表現した場合のギャップ
  - 数学的性質の計算機ライブラリとしての整備

National Institute of Advanced Industrial Science and Technology
AIST

今後の展開

Research Center for Information Security

- 厳密であるが手間が必要
  - コア部分への適用による証明の付与
  - 汎用ライブラリの公開
- 長期的には…
  - ソフトウェア製品の安全性認証制度へ展開
    - 現状（欧州ロケット制御ソフトが使用）より高い安全性レベルの設定にも活用



安全性証明の実装例