IPA暗号フォーラム2006・パネルディスカッション
平成18年10月5日

金融分野におけるハッシュ関数の利用について

宇根　正志

独立行政法人　産業技術総合研究所(AIST)
情報セキュリティ研究センター(RCIS)

Research Center for Information Security (RCIS)
National Institute of Advanced Industrial Science and Technology (AIST)

自己紹介

- ✓ もともと大学では「経済学」。
- ✓ 平成6年、日本銀行入行。
- ✓ 平成8年より、日本銀行金融研究所にて、金融分野と関連が深い情報セキュリティ技術の調査・研究に従事。
- ✓ 平成18年より、AIST/RCISにて、情報セキュリティ技術の基礎研究に従事。
  - ✓ ただし、現在でも、日本銀行金融研究所には在籍。

本パネルでの役割

- ✓ 金融界（ハッシュ関数のユーザ）の一員という立場から、
- ✓ 金融分野でのハッシュ関数の利用の現状について、情報提供、あるいは、コメントさせていただく。

どんなハッシュ関数が採用されているか？

- ✓ SHA-1が主流。

国際標準・業界仕様	概要	規定／記述されているハッシュ関数
ISO TR 17944	セキュリティ管理の枠組み	ISO/IEC 10118準拠 (SHA-1, SHA-2シリーズ, RIPEMDシリーズ, Whirlpool ….)
ISO 11568-4	鍵管理（公開鍵暗号）	
全銀協ICキャッシュカード標準仕様	主としてキャッシュカード取引での用途を想定したICカードの国内仕様	SHA-1
EMV version 4.1	主としてクレジットカード取引を想定したICカードの国際仕様	SHA-1
FINREAD	ICカード・リーダ／ライタの欧州仕様	SHA-1, MD5, RIPEMD-160

金融業界へのインパクト と対応は？

- ✓ インパクト：　大きい。

- ✓ 対応：
  - ✓ 私の認識「議論がはじまりつつある」という段階。
  - ✓ ISO/TC68において、国際標準の側から、暗号アルゴリズムの2010年問題ともからめて、対応の検討を開始したという状況。