情報技術研究センター（CITECS*）20年のあゆみ

＊ Center for Information Technology Studies

日本銀行 金融研究所 情報技術研究センター長
鈴木　淳人

日本銀行金融研究所

所長

参事役（所内組織運営、
情報技術研究センター長）

参事役（情報技術関係）

経済ファイナンス研究課

総務企画
経済研究
ファイナンス研究

制度基盤研究課

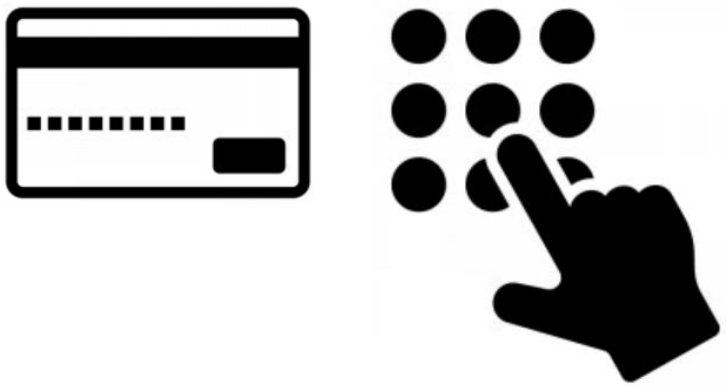
法制度研究
会計研究
情報技術研究センター
- 情報技術研究
- DX研究

歴史研究課

アーカイブ
貨幣博物館
金融史研究

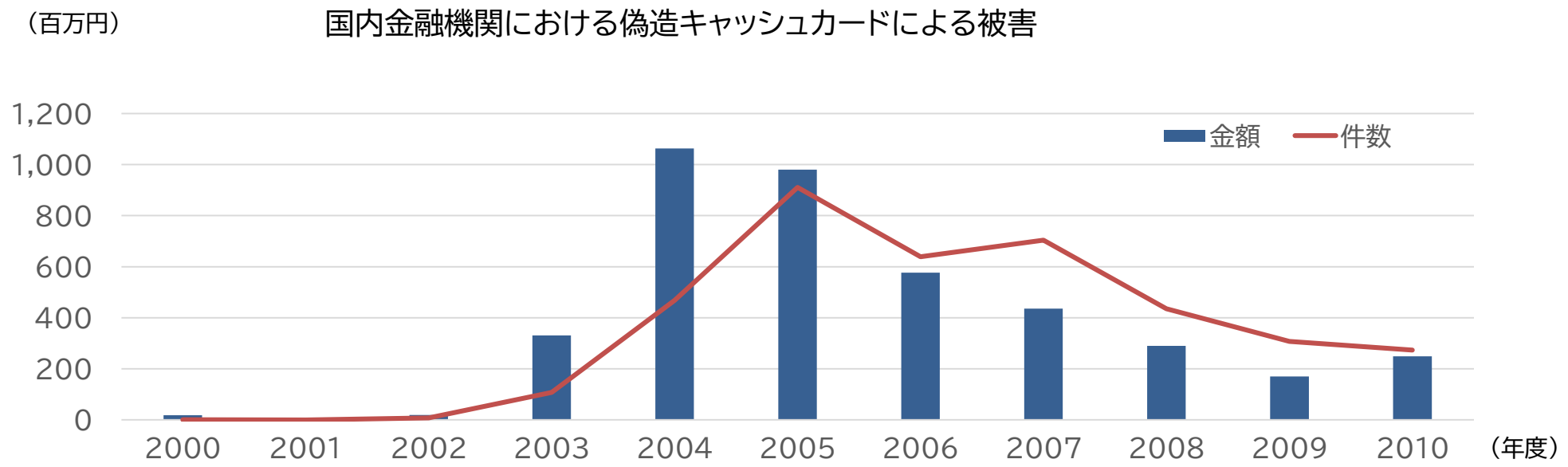
情報技術研究センターの設立経緯

- 日本銀行は、**1980年代から暗号技術・情報セキュリティを研究**
  - ✓ 1988年に稼動した日銀ネットには、共通鍵暗号DESを搭載
- 日本銀行金融研究所は、1990年代から、キャッシュカード取引におけるセキュリティリスクについて警鐘をならしていた
  - 第2回情報セキュリティ・シンポジウム（1999年）では、磁気カードの偽造が容易になっているうえ、暗証番号の盗用や推定が巧妙になっていることを指摘



情報技術研究センターの設立経緯

- 2000年代中盤にかけて、偽造キャッシュカードを用いた預金の不正引き出しが社会問題化



（出典） 金融庁、「偽造キャッシュカード等による被害発生等の状況」（https://www.fsa.go.jp/status/higaijyoukyou/index.html）

情報技術研究センターの設立経緯

- 2005年4月、日本銀行は、情報セキュリティに関する**研究体制の強化**とより**積極的な情報発信**のため、情報技術研究センターを設立
- 金融業界が情報化社会において直面する新たな課題に適切に対処していくことをサポート
- 金融界・学界・IT実務家間の架け橋となり、ひいては金融業界における情報システムの技術革新に貢献していくことを企図

CITECSの活動

調査研究

- 金融分野における新たな情報技術・情報セキュリティに関する調査研究

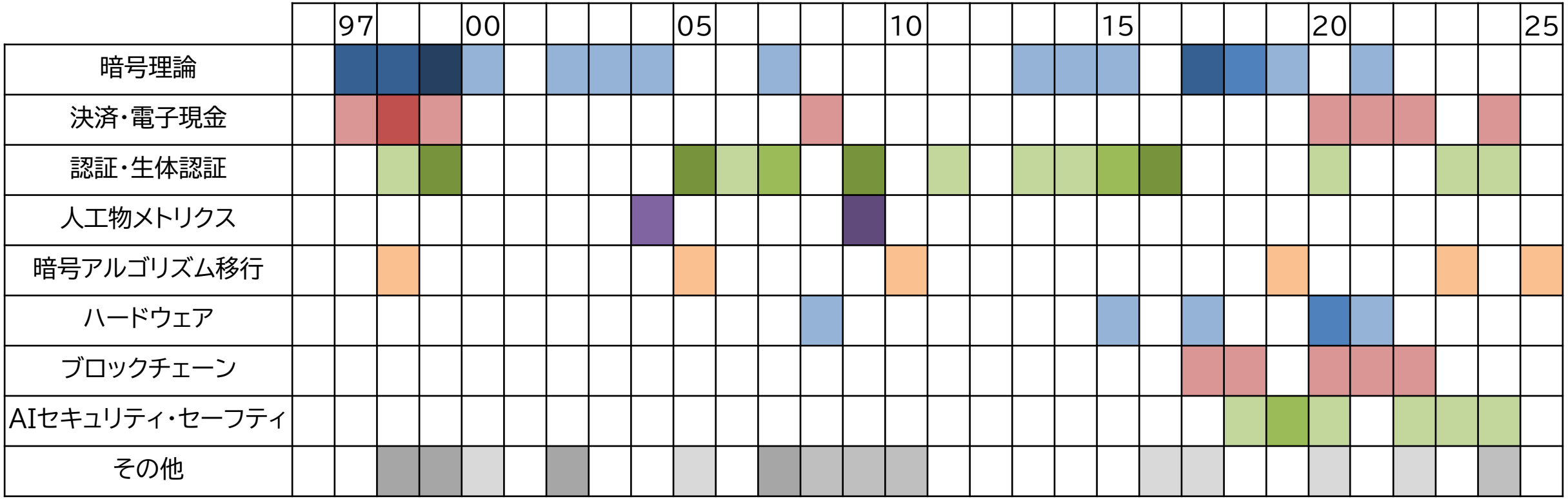
情報発信

- 論文・レポートの公表
- 情報セキュリティ・セミナー、情報セキュリティ・シンポジウムの開催

20年前の10大脅威（IPA情報セキュリティ白書）

第1位	事件化するSQLインジェクション
第2位	Winnyを通じたウイルス感染による情報漏えいの多発
第3位	音楽CDに格納された「ルートキットに類似した機能」の事件化
第4位	悪質化するフィッシング詐欺
第5位	巧妙化するスパイウェア
第6位	流行が続くボットウイルス
第7位	ウェブサイトを狙うCSRFの流行
第8位	情報家電、携帯機器などの組込みソフトウェアにひそむ脆弱性
第9位	セキュリティ製品の持つ脆弱性
第10位	ゼロデイ攻撃

CITECSにおける調査研究



色の濃さは論文の数を示す。
その他は、オープンAPI、量子通信、プライバシー保護技術、国際標準化など

CITECSにおける調査研究：暗号アルゴリズム移行

		97			00					05					10					15					20					25
暗号アルゴリズム移行																													

DESの
安全性低下

① DES→AES

計算機能力の
向上

②暗号の2010年問題

- 1,024ビットRSA→2,048ビットRSA
- SHA-1→SHA-2
- 2-keyトリプルDES→AES／3-keyトリプルDES

量子コンピュータの
実現可能性の高まり

③量子コンピュータによるリスク対応

- 現代暗号→耐量子計算機暗号

CITECSにおける調査研究：AIセキュリティ

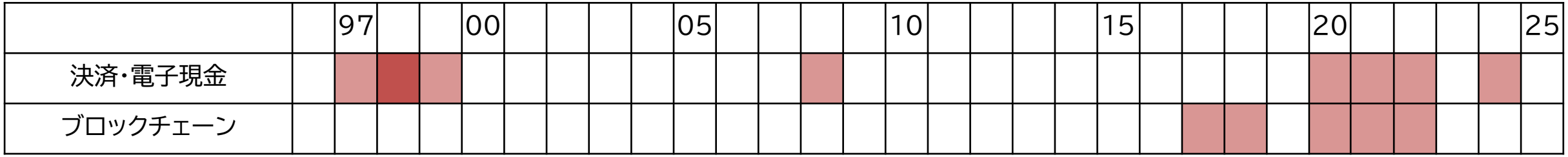
		97			00					05					10					15					20					25
AIセキュリティ・セーフティ																													

AI技術の急速な発展

【公表論文】

- 機械学習システムのセキュリティに関する研究動向と課題
- 金融分野で活用される機械学習システムのセキュリティ分析
- 機械学習システムにおけるソフトウェアの品質評価の現状と課題
- 機械学習システムの脆弱性とセキュリティ・リスク：「障害モード」による分類と今後へのインプリケーション
- 機械学習による予測・推論の公平性：金融サービスにおいて求められる配慮とは
- 深層学習による自然言語処理の急進化と事業サービス応用における課題
- スマートフォンによる顔認証のセキュリティ：ディープフェイクによる脅威と対策

CITECSにおける調査研究：決済・電子現金



「電子現金」に関する研究

フィンテックの勃興
ブロックチェーンの登場

キャッシュレス決済の普及
ブロックチェーンの進展

CITECSの情報発信（シンポジウム）

1998 金融分野における情報セキュリティ技術の現状と課題	2012 多様化するリテール取引の安全性
1999 金融業務と認証技術	2013 多様化するリテール取引の安全性Ⅱ
2000 情報セキュリティ技術の評価と信頼性	2014 金融サービスにおける技術進歩と課題
2001 インターネットを利用した金融サービスの情報セキュリティ対策	2015 金融取引を安心安全に実現するための認証技術
2002 デジタル署名の長期的な利用とその安全性	2016 新たな金融サービスを支える高機能暗号
2003 金融分野における人工物メトリクス	2017 量子コンピュータが金融サービスのセキュリティに与える影響
2004 金融業界における情報システムの脆弱性検知と情報共有	2018 金融分野における機械学習システムの適切な活用に向けて
2005 金融機関の情報セキュリティ対策のあり方	2019 暗号資産のセキュリティ
2006 リテールバンキングのセキュリティ	2021 スマートフォンの利用にかかるセキュリティ
2007 金融業務と情報セキュリティ技術	2022 OSSのセキュリティ
2008 偽造防止技術の新潮流	2023 データ活用とプライバシー保護の両立
2009 環境変化に耐える情報セキュリティ・システムとは	2024 金融分野におけるセキュリティの潮流
2011 金融分野における情報セキュリティ技術の最新動向と今後の方向性	

＊西暦は年度

本日のプログラム

- 金融高度化センターの活動
  金融機構局金融高度化センター長・須藤
- **量子耐性**を有するシステムの実現に向けた金融分野での取組み
  金融研究所・宇根
- **AI**がもたらすリスクに対するセキュリティ
  金融研究所CITECS・菅×情報セキュリティ大学院大学・大塚教授
- さまざまな**決済スキーム**とそのセキュリティ
  金融研究所CITECS・田村×筑波大学システム情報系・面教授
- 金融分野における今後のセキュリティ対策～シンポジウム総括を兼ねて～
  京都大学公共政策大学院・岩下教授