資料1

暗号領域の研究について

セキュリティ研究所　特別技術主幹
佐古　和恵
2019.4.26

自己紹介

佐古和恵　博士（工学）

ＮＥＣ　中央研究所　セキュリティ研究所　特別技術主幹

- 理学部（数学）卒業
- 入社以来、電子投票システム、電子抽選システム、匿名認証技術など、セキュリティとプライバシを両立させる暗号プロトコル技術の研究開発に従事。
- 現在はブロックチェーン技術を活用した透明な社会システムの設計研究
- 日本学術会議連携会員
- 日本応用数理学会　第26代目会長
- 電子情報通信学会　H29年度副会長
- Real World Cryptography St.Com
- PKC Steering Committee
- 標準化活動

  ISO/IEC JTC 1 SC 27 WG2,WG5

  ISO TC307

私が関わってきたこと：暗号プロトコル技術を使った設計

投票のデジタライゼーション

- 電子投票

抽選のデジタライゼーション

- 電子抽選

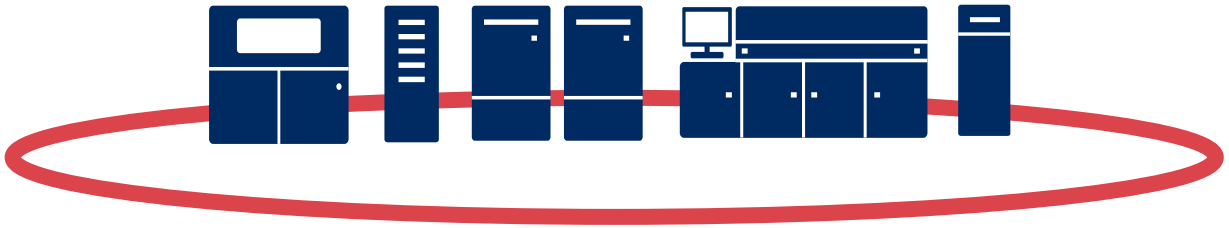
お金のデジタライゼーション

- 暗号通貨、ブロックチェーン

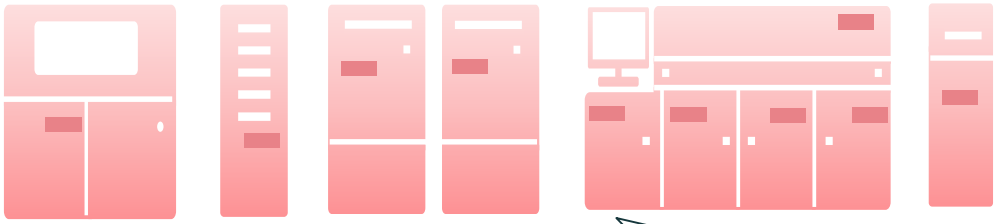
「利用者」のデジタライゼーション

- 匿名認証技術、Self-Sovereign Identity, ID管理

外堀を守るセキュリティとセキュリティバイデザイン



汎用的な
セキュリティ
製品



個別のセキュリ
ティバイデザイ
ン設計

内部不正対策

権限管理
組み込み

「暗号」領域の研究内容

- 暗号:英語ではEncryption (データ暗号化)[E]とCryptography(秘匿技術)[C]
- Encryption: データを暗号化するアルゴリズム
  - 共通鍵暗号（DES, RC4, AES,…）
  - 公開鍵暗号（RSA,　エルガマル暗号、、、）
- デジタル署名：
- ハッシュ関数
- 暗号プロトコル
  - 暗号プリミティブを用いて様々な目的（投票、抽選など）を実現
  - 例：多人数で入力を秘密にしながら、出力を計算（秘密計算：MPC)
- （鍵管理、実装、Crypto Engineering）

プリミティブ E C

活用・応用 C

実装 E C

- foundational theory and mathematics,
- the design, proposal, and analysis of cryptographic primitives,
- secure implementation and optimization in hardware or software,
- applied aspects of cryptography.

暗号領域関連の学会

国際暗号学会（IACR）主催 http://www.iacr.org (1982-)

プリミティブ

- メイン会議　CRYPTO(8月), Eurocrypt(5月), Asiacrrypt(12月)
- 領域会議　公開鍵暗号(PKC), ハードウェア実装（CHES), 高速実装(FSE), 理論(TCC)
- **Real World Cryptography ：産業界で活用されている暗号技術**

国際金融暗号学会(IFCA)

活用・応用

- Financial Cryptography and Data Security　(1994-)

ATMやクレジットカード、電子マネーのセキュリティをはじめとして、金融関係や社会システムに関わる暗号技術、暗号プロトコル技術、実装技術に関わる研究
現在はブロックチェーンがメイン。

セキュリティ会議

活用・応用

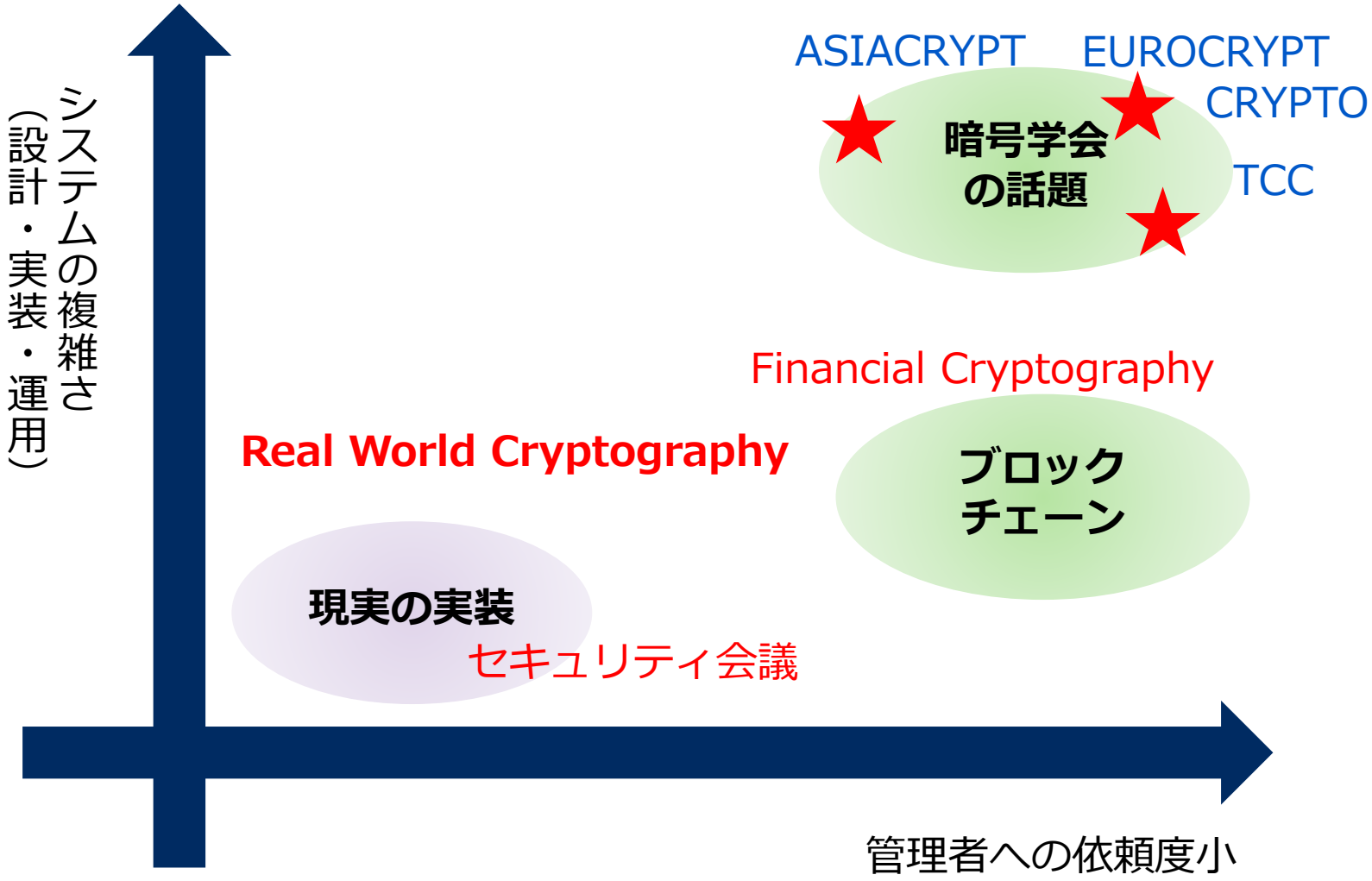
実装

- Usenix Security,
- NDSS,
- ACM CCS,
- IEEE Privacy and Security
- ESORICS（欧州セキュリティ研究）

先週の公開鍵暗号会議（PKC2019)

- 日本で1998年にスタートした国際会議が国際暗号学会の会議に。
- プログラムチェア　中国科学技術院のLin先生と佐古
- 招待講演：NTT 岡本龍明氏（今年の朝日賞受賞）
  「デュアルペアリングベクトル空間の10年」
- セッション
  公開鍵暗号化方式、デジタル署名、暗号プロトコル、ゼロ知識証明、IDベース暗号、関数暗号（秘密鍵によってf(m)のみを伝達)、難読化、格子暗号、耐量子暗号
- 話題：効率化、対象拡大、異なるセキュリティ前提、セキュリティ精度、追加機能など
- 173件中採録42件、うち、日本からの採択6件
- ステアリングコミティ：１１人中3人が日本人。仏３、英２、米２、中１

暗号理論とシステムの複雑さ



懸念事項

- 「花形」の研究だけでは、実際の社会のセキュリティは向上しない。
- 「暗号」技術は必要だが、暗号だけでセキュアになるわけではない。
- 学会の論理で賞賛される技術と、社会で必要とされる技術のかい離

　学会に採録されるのは、「新しい」「間違っていない」手法が多く、その新しさが社会に必要か？はあまり考慮されない。

- 対案はないが、「花形だけが研究」ではない意識を共有したい。
- サイバーセキュリティ戦略(抜粋）の下記の部分に共感

このため、AI、ブロックチェーンなどの先進的な技術を用いたサイバーセキュリティ確保の技術、製品・サービスを構成するシステムの中に**組み込むセキュリティ技術**や、その**組み込みの方法に関する実践的な研究開発**について重点的に取り組む。

これから私自身が取り組んでいきたいこと

- 暗号技術、暗号プロトコル技術やブロックチェーン技術の知見を活かして、世の中のシステム・サービスをより安心・安全・公平・効率的にしていきたい

- ブロックチェーンについては、期待が先行しているので、用語づくり、認識合わせを行っていくとともに、社会に役立つ実例を作っていきたい。

- パスワードをたくさん管理しないといけないという課題を、「インターネットのID管理レイヤー」を実現することによって、構造的に解決していきたい。

sovrin

- 共に、安心・安全・公平・効率的を求めるコミュニティを形成して行きたい。

MyData Japan


Orchestrating a brighter world
NEC