セキュリティバイデザインによる社会システムの設計

研究代表者　佐古　和恵
（基幹理工学部 情報理工学科　教授）

１．研究課題

電子投票システムや ID 管理基盤、マイクロペイメントといった社会の基盤となる IT システムでは、多様な利用者の便益を考えつつ、セキュリティやプライバシーや公平性を考慮して設計することが重要である。そのためには、これらの要件が充足できるように設計時からシステムの機能として織り込んでいくセキュリティバイデザインのプロセスが肝要になる。本研究では、インターネットに欠如しているといわれる「アイデンティティのレイヤー」を実現するデジタルアイデンティティや本人が自分のデータを管理する MyData の理念を実現する様々な社会システムを題材にし、セキュリティバイデザインのベストプラクティスを確立する。そして、健全なエコシステムが構成され、社会に広く使われる基盤になることを目指し、適切な標準的 API（アプリケーションインターフェイス）の設計手法を研究し、安心・安全で公平な IT 社会の実現に寄与する。

２．主な研究成果

デジタルアイデンティティの基盤を設計するにあたって、過年度に引き続き、W3C(World Wide Web Consortium)で標準化されている VC(Verifiable Credential)の活用と発展を検討した。欧州委員会が 2026 年の導入に向けて欧州デジタルアイデンティティの仕様策定ををその先に必要となる機能についての検討をすすめた。

欧州委員会では、全 27 か国の欧州の居住者や企業のデジタルアイデンティティ基盤を整備することを目指し、2023 年 2 月に欧州デジタルアイデンティティウォレットのアーキテクチャと参照フレームワーク(European Digital Identity Wallet Architecture and Reference Framework, EU DIW ARF)を公表した。これは本研究プロジェクトで検討している VC(Verifiable Credential)をベースにしたもので、選択開示機能があることをアピールしている。しかしながら、プライバシーに配慮可能な先進的な機能が備わっておらず、2023 年秋には暗号研究者中心に意見書が提出された。

特に大きな問題とされたのは、選択開示機能をしたときに、名寄せができてしまう問題である。BBS 署名と呼ばれるデジタル署名アルゴリズムとゼロ知識証明を用いれば、このような名寄せを防止することができるが、BBS 署名の国際標準化が完了しておらず、またこの仕様を搭載したハードウェアもほとんどない。そこで、本プロジェクトでは FPGA を搭載した USB キーに BBS 署名を搭載するという実装をすすめた。また、将来を見据え、証明書発行者を秘匿できる方法や、量子耐性のある方式についての調査を開始した。一方、Google らが、名寄せを防ぐ選択的開示機能を、既存の ECDSA 署名とゼロ知識証明技術を組み合わせて実現する方法

を提案したので、その実用性検討も開始した。IETF や W3C、 ISO などの機関で標準化を推進していくとともに、提案されている様々な方式の比較研究をすすめ、技術が市民のプライバシー保護に貢献できる手法を模索していく。

３． 共同研究者

山本暖、須賀祐治（IIJ）

４． 研究業績

4.1 学術論文

- Tsutsumi and Sako“Benchmarking zkVMs: Efficiency, Bottlenecks, and Best Practices” 国際ワークショップ　ZKProof 7
- 山本・須賀・佐古「NymCreds: 仮名クレデンシャルシステムの安全性と構成」暗号と情報セキュリティシンポジウム SCIS 2025
- 水野・渡邉・山本・佐古「Issuer-Hiding Verifiable Credentials の実装と考察」暗号と情報セキュリティシンポジウム SCIS 2025
- 渡邉・山本・佐古「Verifiable Credentials の保有者向け秘密鍵管理デバイスにおける BBS 署名のゼロ知識証明生成の効率化と実装」暗号と情報セキュリティシンポジウム SCIS 2025
- 森下・大塚・佐古「「格子に基づく実用的な匿名認証フレームワーク」の実態」暗号と情報セキュリティシンポジウム SCIS 2025
- Otsuka, Mizuno, Watanabe, Tsutsumi and Sako “Revisiting the Comparison of Digital Signature Algorithms for Unlinkable Selective Disclosure” 暗号と情報セキュリティシンポジウム SCIS 2025
- 堤・佐古「zkVM の効率化に向けた課題と展望」暗号と情報セキュリティシンポジウム SCIS 2025
- 福田（優）・佐古「日本における携帯回線契約時の本人確認制度の考察」暗号と情報セキュリティシンポジウム SCIS 2025
- 田中・佐古「新しい装置による数独用物理ゼロ知識証明プロトコルの提案」暗号と情報セキュリティシンポジウム SCIS 2025
- 渡邉・佐古「VC の保有者向け秘密鍵管理デバイスの実装」コンピュータセキュリティシンポジウム CSS 2024
- 福田（岐）・佐古「Verifiable Credentials における Issuer の運用方式についての考察」情報処理学会 CSEC 研究会 2024 7 月
- Wu, Tsutsumi, Shioya, Watanabe and Sako “Exploring the Possibility of Defi Lending Protocols to offer Unsecured Personal Loans” 報処理学会 CSEC 研究会 2024 7 月

4.2 総説・著書

佐古「検証可能クレデンシャルにおける本人紐づけを巡る論点：適用事例にみる対応方法と金融分野への含意」 日本銀行　金融研究所ディスカッションペーパー 2024-J-22

4.3 招待講演

- Keynote ”Cryptography to Support Our Digital Society” K. Sako, ProveSec 2024.9.25-27.
- Keynote ”Digital Identity and Cryptography” K. Sako, Cryptology and Information Security Conference (台湾 CISC)　2024.8.29-30.
- 招待講演「SSI/DID より VC でしょ」コンピュータセキュリティシンポジウム(CSS) ブロックチェーンワークショップ 2024
- 　パネリスト「 PWS とプライバシー 10 年の歩み ～法と技術の観点から～」コンピュータセキュリティシンポジウム(CSS) プライバシーワークショップ 2024

4.4 受賞・表彰

- 渡邉・佐古「VC の保有者向け秘密鍵管理デバイスの実装」コンピュータセキュリティシンポジウム CSS 2024 (学生優秀論文賞受賞)

4.5 学会および社会的活動

東大五月祭 2024　「社会と数学、共鳴する」登壇
国際暗号学会 Real World Cryptography ステアリングコミッティー委員
RWC 2025 Contributed Talk Program Committee
Financial Cryptography ステアリングコミッティー委員
FC2025 実行共同委員長
RSA Conference Cryptographer’s Track Committee
World Wide Web Consortium(W3C) RDF Canonicalization and Hash Working Group (RCH WG) Invited Expert
Usenix Security 2024 プログラム委員
ACM Computer Security Symposium 2024 プログラム委員
国際暗号学会 Communications in Cryptology (CiC) Editorial Board
国際暗号学会 Public Key Cryptography 2024 Area Chair for Applied Cryptography, SNARKs, Verifiable Computation
International Conference on Selected Areas in Cryptography (SAC 2024) Program Committee
Shonan Seminar ‘Biggest Failures in Privacy’ Organizer
日本学術会議　連携会員第三部会員（10 月-）情報学委員会幹事、サイバーセキュリティ分科会　副委員長
内閣官房 革新的事業活動評価委員会 委員
内閣官房 Trusted Web 推進協議会 タスクフォース 委員、ユースケース委員
金融庁　金融審議会　委員
金融庁　デジタル・分散型金融への対応のあり方等に関する研究会 メンバー
金融庁　暗号資産に関連する制度のあり方等の検証 勉強会メンバー
文部科学省 情報委員会 専門委員
デジタル庁　DIW（Digital Identity Wallet）アドバイザリーボード　構成員
デジタル庁 Verifiable Credential (VC/VDC) の活用におけるガバナンスに関する有識者会議委員

厚労省　保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議 構成員
最高裁判所　裁判の迅速化に係る検証に関する検討会　委員
総務省 情報通信審議会 情報通信技術分科会 ITU 部会 専門委員
経産省 「令和 5 年度 Web3.0・ブロックチェーンを活用したデジタル公共財等構築実証事業」スペシャルアドバイザー
JST 経済安全保障重要技術育成プログラム「セキュアなデータ流通を支える暗号関連技術(高機能暗号)」 分科会委員(アドバイザー)
JST さきがけ領域アドバイザー(数理構造活用 領域)
JST さきがけ領域アドバイザー(IoT 領域)
情報処理学会 情報規格調査会　委員(ISO/IEC JTC 1 SC 27 WG 5)「ID 管理とバイトメトリックスとプライバシ」
情報処理学会 情報規格調査会　エキスパート(ISO/IEC JTC 1 SC 27 WG 2)「暗号メカニズム」
一般社団法人 男女共同参画学協会連絡会　理事（副委員長）
一般社団法人 MyDataJapan　副理事長

５． 研究活動の課題と展望

日本のデジタル庁による取り組みや、EU における「EU Digital Identity Wallet」の動向を見ても明らかなように、デジタルトランスフォーメーションの推進においては、Verifiable Credential（VC）への期待がますます高まっている。この技術においてセキュリティとプライバシをいかに確保するかは、まさに設計段階からの検討が不可欠であり、セキュリティ・バイ・デザイン、プライバシー・バイ・デザインの理念が実践される領域である。

実際、暗号研究者をはじめとする技術者や有識者の働きかけにより、いったんは決定されたかに見えた EU の仕様が再検討されるに至った。また、ハードウェア実装が少ない BBS 署名アルゴリズムに依存せずに要件を満たそうとする Google らによる新たなアプローチも提案されている。汎用的なゼロ知識証明がここまで実用に資する技術として活用されるようになったことは、大きな進展と言える。

今後も、特定の技術や方式に固執することなく、常に中立的な視点から技術を吟味し、その時点で最も適切と思われる技術を社会に提案していきたい。