Verifiable Credentials の高度化と社会システムへの適用

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

入学や就職などの申請を電子的に実施する機会が増えている。しかし、例えば海外在住者から卒業証明書のスキャンデータが送付されてきた場合、一見して真正性を確認することは容易ではない。このような個人の資格情報（卒業資格等）を第三者（認定大学等）が電子的に保証する仕組みは Verifiable Credential（検証可能クレデンシャル, VC）と呼ばれ、World Wide Web Consortium（W3C）等で標準化が進められている。また欧州では、EU Digital Identity Wallet（EUDIW）として各国に提供義務が課されるなど、社会実装が急速に進展している。

一方で、現在広く検討されている方式の多くは従来型の暗号技術に依存しており、資格情報を社会横断的に活用する際に、特にプライバシー保護の観点で課題が残されている。そこで本研究では、より高度な暗号プロトコルを用いた検証可能クレデンシャル技術について研究を行った。

具体的には、発行者秘匿（Issuer Hiding）機能の追加、証明対象に応じた効率的なゼロ知識証明技術の開発、量子耐性を有する署名アルゴリズムの検討を進めた。さらに、検証可能クレデンシャルを社会システムへ適用する際の運用面や、利用者に安心感を与える操作性についても検討を行った。

２．主な研究成果

BBS 署名と呼ばれるデジタル署名方式とゼロ知識証明を組み合わせることで、EUDIW において課題とされる名寄せ（異なるサービス間での利用履歴の結び付け）を防止できることが知られている。しかし、BBS 署名は国際標準化が完了しておらず、また対応ハードウェアもほとんど存在しない。

そこで本研究では、FPGA を搭載した USB キー上に BBS 署名機能を実装する構想を提案し、FIDO2 で標準化されているプロトコルを活用した試作実装を行った。その成果を情報処理学会論文誌へ投稿した。(12 月に採録、掲載)

また、Google らが提案した Longfellow-zk と呼ばれる新たなゼロ知識証明技術を応用し、既存の X.509 ベース公開鍵証明書に対してプライバシー保護機能を付与できることを示した。これを踏まえ、マイナンバーカードを活用した新たなデジタルアイデンティティ構想の検討を開始した。

さらに、ISO における Attribute-based Credentials（属性証明書）の標準化活動に参画し、BBS 署名等を含む技術仕様の議論に参加した。また、既存 VC を参照して新たな VC を発行する仕組みについてセコムの IS 研究所とともに検討を行い、安全性上問題となる場合とそうでな

い場合の類型化を行った。B

３． 共同研究者

山本暖、須賀祐治（IIJ)、セコム IS 研究所（国井 裕樹、長谷川 佳祐他）

４． 研究業績

4.1 学術論文

- 渡邉健・山本・佐古和恵「Verifiable Credentials の保有者向け秘密鍵管理デバイスの実装」情報処理学会　論文誌（5/1 投稿、2025 年 12 月号掲載）
- 小林 駿斗・佐古 和恵「こどものデータ保護における法定代理人からの同意確認手法の比較分析」情報処理学会コンピュータセキュリティ研究会 2025 年 7 月発表
- 安部・石橋・髙田・長谷川・国井・島岡・藤井孝輔・水野重弦・渡邉健・佐古和恵「信頼できる VC に基づく Verifiable Credentials の考察」情報処理学会コンピュータセキュリティ研究会 2025 年 7 月発表
- Sako: Building Privacy-Preserving Technologies of Societal Impact “How People would trust a government based on its choice of a digital identity wallet?” Dagstuhl Seminar 2025 年 7 月発表
- 草間　暁・佐古和恵「認証における OAuth 誤用に対する対応ガイドラインの提案」電子情報通信学会 2025 ソサイエティ大会 A-7-09（6/27 投稿、9 月 発表）

4.2 招待講演

- 「暗号技術とデジタルアイデンティティ」神奈川大学情報学シンポジウム 2025.5.30.
- Building Privacy-Preserving Technologies of Societal Impact “How People would trust a government based on its choice of a digital identity wallet?” Dagstuhl Seminar 2025.7.31

4.3 学会および社会的活動

国際暗号学会 Real World Cryptography ステアリングコミッティー委員
RWC 2026 プログラム共同委員長
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
国際暗号学会 Communications in Cryptology (CiC) Editorial Board
日本学術会議　連携会員第三部会員、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
金融庁　金融審議会　委員
金融庁　暗号資産制度に関する研究会　メンバー
文部科学省 情報委員会 専門委員
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
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)
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」
財団法人　国際科学技術財団　2026 Japan Prize 「エレクトロニクス、情報、通信」審査部会委員
一般社団法人 MyDataJapan　副理事長

５． 研究活動の課題と展望

本プロジェクトは 2025 年 4 月から 8 月末までの 5 か月間であったが、その後の研究成果創出につながる基盤研究を推進することができた。実際に、本研究を基盤として、2025 年 10 月のコンピュータセキュリティシンポジウム（CSS）において 3 件、2026 年 1 月の暗号と情報セキュリティシンポジウム（SCIS）において 7 件の研究発表へと発展した。また、各省庁において属性証明を必要とするシステム構成についても提案を行い、実運用を想定したデジタルアイデンティティ基盤に関する議論へ貢献した。

近年は、制度・運用を含めた実践的なデジタルアイデンティティ研究への社会的関心が高まっている。今後も、暗号技術と社会制度設計の両面から、社会で実運用可能なデジタルアイデンティティ技術の研究を深耕していきたい。