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、昨年度に引き続き、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。特に今年度は社会への応用を見据え、類似技術が先行して活用されているオープンバッジの状況と、欧州委員会が 2026 年の導入に向けて動いている欧州デジタルアイデンティティの仕様策定の状況を調査し、その課題を考察した。

オープンバッジは、大学の卒業証書や資格証明書をデジタルで検証可能な形で発行するもので、2011 年から利用されている。最新のバージョンの V3 は W3C の VC の仕様に準拠しているが、一般に使用されているバージョンにはデジタル署名がない場合や、発行者の検証サーバを常時稼働させる必要があることがわかった。また、国内では資格認定団体が、オープンバッジの発行をアウトソースするケースが散見され、トラストの構造が、不明確になっている。今後は運用に関するベストプラクティスをまとめることが急務だと感じた。

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一昨年度から検討している 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、使用できるデジタル署名アルゴリズムが限定されているため、これまで研究してきたプライバシーに配慮した機能を搭載することができない。

特に今後問題になりそうなのは、現在の選択開示機能の仕様である。選択開示機能とは、１つの証明書に記載されている情報の一部を秘匿しても、開示された情報に発行者のお墨付き（デジタル署名）が付与されていることを、受け取り手が確認できる手法である。これを活用したい背景には、１枚の電子証明書を用い、A さんには「名前と住所」の情報のみを、B さんには「年齢」だけを開示したいユースケースを想定するからである。しかし、現状の仕様では A さんと B さんが結託すれば、B さんには年齢だけでなく、名前と住所まで紐づけられてしまうという問題がある。欧州の国が発行したデジタル証明書をさまざまなサイトで活用することが想定されているが、一枚の証明書を使い続けるとスーパークッキーとなる恐れがある。

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、このような紐づけを防止することができるが、BBS 署名はまだ国際標準化されていない。今後、BBS 署名の優位性を明らかにし、IETF や W3C、 ISO などの機関で標準化を推進していく。これによって、昨年までに研究してきた暗号技術が市民のプライバシー保護に貢献できる道が開けると期待する。

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

- Watanabe and Sako: “POSTER: Using Verifiable Credentials for authentication of UAVs in logistics” Applied Cryptography and Network Security (ACNS 2023)
- Zheng and Sako: “Member Removal Mechanism for TreeKEM to Deal with Offline Members” CSEC 7 月
- 森田・渡邉・井上・佐古「指名者による本人特定機能付き Verifiable Presentation」 CSEC 7 月
- 山本・須賀・佐古「 Verifiable Credential における RDF 空白ノードの活用」Computer Security Symposium （CSS 2023 1E4-3 ）
- Zheng and Sako: “ POSTER: Member Removal Mechanism for TreeKEM to Deal with Offline Members” International Workshop on Security (IWSEC 2023)
- 福田・水野・渡邉・佐古・寺田・吉濱 :「 Blockcert OpenBadge 証明書に関する仕組みと考察」CSEC12 月
- 渡邉・森田・山本・佐古「指名者による本人特定機能付き Verifiable Presentation の実装と応用」SCIS2024 1D1-3
- 山本・須賀・佐古 「Anonymous Credentials におけるユーザ秘密鍵の更新」SCIS2024 2D1-1
- 堤・渡邉・佐古 :「連結不可能選択的開示のためのデジタル署名アルゴリズムの比較」SCIS2024 2D1-3
- 井上 ・佐古 ・膳場「集団主義が組織のセキュリティ対策への関心・態度に与える影響に関して」 CSEC 3 月

4.2 総説・著書

佐古「分散型デジタルアイデンティティとは？～概念、仕組み、実現に資する技術と課題～」日本銀行　金融研究所ディスカッションペーパー 2023-J-8

4.3 招待講演

“Digital Identity, Verifiable Credentials and Cryptography” International conference on Big Data Analytics (ICBDA 2024)

“Digital Identity” French-Japanese workshop on blockchain technologies

“Selective Disclosure for Privacy” Joint ITU/WHO Workshop on Future of Verifiable Health Credentials Beyond:

「MPC（Multi-party Computation）の応用／可能性」Fintech 協会第 5 回 Web3 勉強会　パネリスト

“Trusted Personal Data Management Service (TPDMS) Certification Program” Internet Governance Forum(IGF 2023) Panelist

“Mutual Authentication of UAVs using Selective Disclosure” IEEE World Forum on Internet of Things (WFIoT 2023)

「暗号プロトコルとゼロ知識証明」Theory Meets Blockchain Engineers(TMBE)

4.4 受賞・表彰

Watanabe and Sako: “POSTER: Using Verifiable Credentials for authentication of UAVs in logistics” Applied Cryptography and Network Security (ACNS 2023) Best Poster Award

4.5 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、
RWC2023 実行委員長

国際暗号学会 Test of Time Award Committee (2023 Chair)

Financial Cryptography ステアリングコミッティー委員

Casper Brown PET Award 2023 Committee

RSA Conference Cryptographer’s Track Committee

World Wide Web Consortium(W3C) RDF Canonicalization and Hash Working Group (RCH WG) Invited Expert

Usenix Security 2023,4 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 CRYPTO 2023 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

国際産業数理・応用数理会議 ICIAM 2023 Local Scientific Program Committee

International Conference on Selected Areas in Cryptography (SAC 2024) Program Committee

French-Japanese workshop on blockchain technologies Scientific committee
Shonan Seminar 'Biggest Failures in Privacy' Organizer
日本学術会議　連携会員(-2023.9 月)会員（10 月-）
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　国際調査研究「分散金融システムのトラストチェーンにおける技術リスクに関する研究」アドバイザー
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
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
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)
応用数理学会　名誉会員
情報処理学会　理事（-2023 年 6 月）
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」
国際数学オリンピック IMO2023 日本大会実行委員会　委員
男女共同参画学協会連絡会　副委員長（理事）(2023 年 10 月-)
日本銀行　金融研究所　国内客員研究員
一般社団法人 MyDataJapan　副理事長

５．研究活動の課題と展望

日本政府の Trusted Web の取り組みや欧州の EU Digital Identity Wallet の動向、OpenBadge の普及をみると、デジタルトランスフォーメーションを促進するために、Verifiable Credential への期待が高まっていることが実感できる。ただし、この技術は基盤となるため、セキュリティとプライバシがどのように確保されるかは、様々な利用シーンを想定して確認していく必要がある。

また、論文と実際の社会での技術利用の間に大きな壁があることを強く意識させられた一年であった。BBS 署名は 20 年前に論文で提案され、その後安全性解析と性能改善がおこなわれた。しかし、技術者への浸透は進まず、「耐量子性がないからあえて導入する必要はない」という意見もあがった。現代社会では、多様性が増す中中で、マルチステークホルダでの意思決定の重要さが唱えられているが、正しい情報を共有しながら意思決定することのむずかしさが浮き彫りになる。しかし、技術に精通している研究者こそ、リスクとメリットを適切に伝えることができる。それも一つの使命と思い、丁寧に取り組んでいきたい。