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。2021 年 12 月にデジタル庁がリリースしたワクチン接種証明アプリはこの VC のフォーマットを採用することによって、国際的にデータ共有・検証を可能にしている。単なる一方向の証明書の発行、提示、検証にとどまらず、様々な応用を見据え、ドローンの相互認証のユースケースを土台として、今後有効に使われると思う機能追加を検討した。

具体的には、異なる２社の異なる運送業者に属するドローンそれぞれが、共通の依頼主の契約に基づき、荷物を配送するシナリオを検討した。依頼主との契約の VC と、運送業者からドローンへの指令を示す VC などの複数の VC を組み合わせて、相互に不必要な情報を開示せずに、同じ契約に基づく業務で荷物の受け渡しをしているということが確認できる相互認証プロトコルを設計した。これには JSON-LD で表現され、BBS+署名方式で署名された VC を発行し、選択開示プロトコルを活用した。

さらに、運送業者は、相互認証プロトコルのログより自身のどのドローンがその相互認証プロトコルに参加していたかを特定したいニーズがある。そのため、このプロトコルにドローンの ID を暗号化して埋め込み、後日運送業者の鍵で復号できる機能も追加した。

また、このシナリオでは荷物を受け渡しがあり、渡した方は受け取った側に領収書を発行してもらいたいニーズがある。選択開示機能で、受け取ったドローンを特定する識別子も秘匿されている中で、確かに「同じ契約に基づく業務についているドローンが発行した」領収書であることを確認する必要がある。そのために、相互認証時に領収書検証用の一時公開鍵の

生成プロセスを正当性証明付きで組み込むことにより、この要件を充足するプロトコルを考案した。

今年度の研究成果により、VC のモデルには柔軟にさまざまな機能が追加できることがわかり、今後拡充すべきアイデンティティレイヤーの在り方がみえてきた。

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

Yamamoto, Suga and Sako 「Formalising Linked-Data based Verifiable Credentials for Selective Disclosure」Security Standardisation Research Conference 2022（国際会議 EuroS&P 併設）

山本・須賀・佐古「zk-SPARQL: SPARQL クエリに対して検証とプライバシ保護が可能な結果を返すパーソナル RDF データストア」SCIS2023 2B1-2

渡邉・佐古・山本「BBS+署名を用いた Holder-Binding 機能付き Verifiable Credential の認証方法」SCIS2023 2B1-4

丸山・江口・近藤・上野・渡邉・佐古「超多数・多種移動体による物流に向けた Verifiable Credential を用いた移動体認証プロトコル設計」SCIS2023 3A4-2

江口・佐古・柴田・佐藤（俊）・佐藤（拓）「BLS 署名による LPWA ネットワーク上の分散台帳決済システムの通信データ長改善の評価」SCIS2023 1D2-3

4.2 総説・著書

佐古「数論を用いた問題解決~安心なネット社会であるために」サイエンス社「数理科学」2022 年 9 月号

4.3 招待講演

Computers, Privacy and Data Protection (CPDP 2022) “ DATA PROTECTION FRIENDSHIP: THE EU AND JAPAN”パネリスト

電子情報通信学会 DPF 研究会「DX とトラストと検証可能性」

テレコム技術情報セミナー「暗号プロトコル技術の理論基盤の研究開発」

FIT 2022 「IoT が拓く未来：〜IoT 技術が起こす近未来の社会変革とは〜」パネリスト

東京大学 卓越大学院プログラム FoPM セミナー “ Digital Identity -- How do we want to be authenticated using cryptography?”

スウェーデン・リンネ大学 ゲスト講演 “Cryptography for transparent society”

4.4 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)

Casper Brown PET Award 2022 Committee

RSA Conference Cryptographer's Track Committee
World Wide Web Consortium(W3C) RDF Canonicalization and Hash Working Group (RCH WG) Invited Expert
Internet Identity Workshop(IIW) Digital Identity Across Asia Co-Host
Usenix Security 2023 プログラム委員
国際暗号学会 CRYPTO 2023 プログラム委員
日本学術会議　連携会員
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
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　トラストを確保した DX 推進サブワーキンググループ　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)
情報処理学会　理事
情報処理学会 情報規格調査会　委員(ISO/IEC JTC 1 SC 27 WG 5)
国際数学オリンピック IMO2023 日本大会実行委員会　委員

５．研究活動の課題と展望

今年度の研究成果により、VC のモデルには柔軟にさまざまな機能が追加できることがわかった。今後、VC をベースにした認証プラットフォームを拡充していくことで、望ましい「アイデンティティのレイヤー」の姿が見えてくると思う。W3C のワーキンググループ、コミュニティグループのメンバーと議論しながら、また日本政府の Trusted Web の活動や欧州の EU Digital Identity Wallet の動向を注視しながら、安全で便利な方式の普及に尽力したい。

また、2023 年 3 月にアジアで初めて開催された国際暗号学会の Real World Cryptography において、「Boring Cryptography」というキーワードがあがっていた。これは耐量子暗号や完全準同形暗号などの華やかな最先端の暗号研究と対比して、暗号アルゴリズムや手法そのものはよく知られたものであっても、実社会の複雑な環境や制限に呼応するように適切に組み合わせ、周辺の鍵管理技術や丁寧なパラメータ調整などを経て、社会におけるどのような人でも安全に効率よく暗号技術が活用できるようになるための研究の重要さを主張しているキーワードである。暗号技術が社会に広く使われる基盤になることを目指し、地道に研究していきたいと思っている。