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、ブロックチェーン技術を活用した「自己主権アイデンティティ(Self-Sovereign Identity)」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

本年度は主に、自己主権アイデンティティの基盤を設計するにあたって、欧州でも導入が検討されている W3C(World Wide Web Consortium)で標準化されている Verifiable Credential の活用を見据え、さまざまな機能追加を検討した。

Verifiable Credential はあるサブジェクト（人間や物体など）がもつ属性に関して、Issuer とよばれる権限者が与えるお墨付きのことである。サブジェクト名とそのサブジェクトの属性データに対して、Issuer のデジタル署名が発行されることでそのサブジェクトにその属性があることを Issuer が保証していることを誰でも検証できる。

しかし、通常のデジタル署名は、署名対象のメッセージが正しいかどうかの保証しか与えない。たとえば、署名対象のメッセージに複数の属性が記述されていた場合は、その中で開示したい属性が一つであっても、他のすべての属性を含むメッセージを開示して、メッセージと署名が正しいことを検証してもらう必要がある。これでは自己主権として重要視される Selective Disclosure（本人が選んだ属性のみを開示すること）を達成できない。

そこで、複数の属性に署名していても、その部分集合だけを相手に開示し、その正当性が検証できる方式を、BBS+署名アルゴリズム（2004 年に Boneh, Boyen, Shacham によって提案されたグループ署名アルゴリズムに基づいて、署名対象のメッセージの選択開示を可能にする署名アルゴリズム）を使って構築することを考える。特に、そのときに、複数の属性がそれぞれ何を意味しているかを記述できる、JSON-LD 式の Verifiable Credentials をベースに、どのように Selective Disclosure を安全に実施できるかを議論した。その結果、安全性評価には、何も漏らさない強秘匿の概念と、メッセージ内の属性の個数とその相対位置のみを漏らす弱

秘匿の概念を定義できることを示し、具体的に弱秘匿性を実現する方式を設計した。その成果を記した論文「Formalising Linked-Data based Verifiable Credentials for Selective Disclosure」が Security Standardisation Research Conference 2022 に採録された。また、秘匿した属性に関して、その属性がどのような範囲に存在しているかを示す範囲証明を実現するゼロ知識証明プロトコルも、効率のよい Bulletproofs をベースに構築することができた。今後は、強秘匿性を実現する方式を考案するとともに、具体的な社会システムの設計に活用していき、さらには提案の安全な方式が標準化されるよう、関係者に働きかけていく所存である。

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

山本・須賀・佐古「Linked Data 型 Verifiable Credentials の構成と安全性」 (SCIS2022)

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）

4.2 総説・著書

オーム社　情報セキュリティ（改訂 2 版）

4.3 招待講演

国際暗号学会 ASIACRYPT 2021「Cryptography for Secure, Privacy-enhancing and Fair Society」

The Forum Math for Industry 2021@Vietnam 「Cryptography and Transparency」

ミュンヘン工科大学 Maths in Society 「Cryptography for Transparent Society」

ASOCIO Digital Summit 2021@Bangladesh パネリスト

大阪大学 数理・データ科学教育研究センター　AI・データ利活用研究会「データとトラストと暗号技術」

日本 ITU 協会　情報通信研究会「NFT ってなんだろう」

JEITA デバイス・ハードウェアセキュリティ研究分科会「ブロックチェーン技術と最近の話題」

JST CRDS トラスト研究俯瞰セミナー「暗号プロトコルとトラスト」

JST CRDS 数学領域俯瞰セミナー　パネリスト

4.4 受賞・表彰

一般財団法人　テレコム先端技術研究支援センター　SCAT 会長賞

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

国際会議 ACM Asia Conference on Computer and Communication Security (AsiaCCS 2022)

プログラム共同委員長
Casper Brown PET Award 2021 Committee
国際暗号学会 Test of Time Award Committee
RSA Conference Cryptographer's Track Committee
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「ブロックチェーン技術等を用いたデジタルアイデンティティの活用に関する研究」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

今年度は、「セキュリティバイデザインによる社会システムの設計」を実施するために、そもそも社会システムに必要な「トラスト」について深く掘り下げる機会があった。JST の 15 回に及ぶ俯瞰セミナーシリーズでは、医療から社会科学までの様々な分野におけるトラストの研究の紹介を受けた。また、内閣官房の TrustedWeb 推進協議会でも何を目指すべきかの議論が行われ、デジタル庁のトラストを確保した DX 推進委員会でもトラストサービスの在り方を協議した。翻って見ると、人類が社会的な生活をおくるなかで、危害を加えられるかもしれない相手と、どうおりあって協力関係を結んでいくかが、人類の歩みだといってもよいかもしれない。そのために、ルールや制度が作られ、進化してきた。現在は、デジタル化によって社会の環境が変わりつつある中、従来のルールや制度をどう見直したらよいのかという問いがつきつけられている。紙という物理的な媒体を前提に構築されてきたルールの本質をとらえ、その本質を情報化技術や暗号技術でマッピングした社会システムを、今後も設計していきたい。