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

本年度は主に以下の成果を得た。

(1)「トラスト」と「検証可能性」の関係性の明確化
(2)「自己主権アイデンティティ」技術の動向調査とゲームアカウント管理への応用
(3) 属性認証における匿名性の定義とチャンネルのモデル化

以下、それぞれについて述べる。

(1)「トラスト」と「検証可能性」の関係性の明確化

トラストという言葉は様々な意味があり、そこを明確にしないまま便利に使われている面がある。ここではトラストを、「確認せずに相手が意図通りにふるまうと信じる度合い」とする。そして、相手が意図通りにふるまうと信じられれば、自分がなにか意思決定を行うと想定する。このとき、なにも情報がなければ、相手を信じて決断するしかない。一方、何か確認できる情報があれば、相手を盲目的に信じる部分が減少する。そこで、IT システムに暗号技術を活用した仕組みを導入し、本人が検証可能な部分を増やすことにより、盲目的相手を信じるというリスクをとらなくても意思決定を支援できることを目標とする(図１)

具体的には、デジタル署名方式はゼロ知識証明方式を活用することにより、データの属性や相手側のデータの処理に関して様々な検証を可能にする。これらをどのように IT システムに組み込めば、無条件にトラストする部分を減らせるか、仕組みを導入しても残るトラストしないといけない部分は何か、を明確にすることがセキュリティバイデザインのプロセスである。例えば、ビットコインに代表されるブロックチェーン技術は多くのプロセ

スを検証可能にしている。しかし、この方式においても、トラストする部分はゼロではない。採用されている署名アルゴリズムに脆弱性がないか、アルゴリズムは安全でも正しく実装されたソフトウェアを使用しているか、など、利用者の目線ではまだ多くの部分をトラストせざるを得ない状況である。

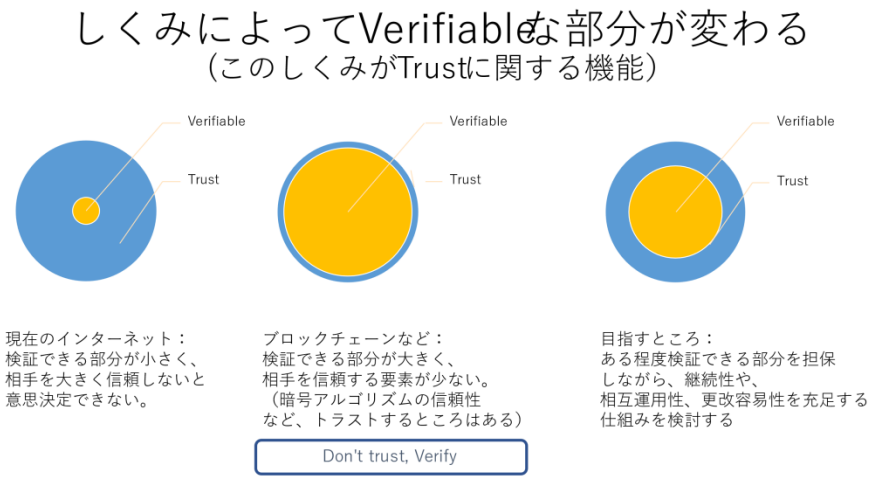

図１　トラストと検証可能性

(2)「自己主権アイデンティティ」技術の動向調査とゲームアカウント管理への応用

検証可能性が重要である一方、検証可能にするために、相手に必要以上の情報提供するのは、プライバシーの観点から望ましくない。自己主権アイデンティティでは、たとえば、本人であることを示すために、本人確認書類のすべてを開示するのではなく、必要な属性だけを提示できる方式が検討されている。このような自己主権アイデンティティのフレームワークが DID(Distributed Identifiers)と VC(Verifiable Credentials)で実現しようと、World Wide Web Consotium や Linux Foundation の Trust over IP で検討がはじまっている。

このような DID/VC のフレームワークが社会基盤として確立したあかつきに考えられる適用例を検討した。具体的には、ゲーム業界において懸念されているゲームアカウントの売買を抑止しつつ、本人のための機種変更には対応できるようなサービスが実現できるのではないかと考えた。他に、主に海外で検討されている DID と VC の適用例としては、ワクチンパスポートがある。ワクチン接種が始まった現在、海外を中心としてワクチンを接種した人は渡航を含む自由な行動が許されつつある状況になっている。ワクチンパスポートとは、自分がワクチンを接種したことを示すデジタル証明書のことで、DID/VC 以外にも、様々な方式が提案されている。今後はこのような題材も社会システムとして検討していきたい。

(3) 属性認証における匿名性の定義とチャンネルのモデル化

自己主権アイデンティティ方式でも採用されている要素技術である属性認証技術の標準化活動にも関わった。2020 年秋の ISO/IEC JTC1 SC 27 WG5 の国際会議で FDIS(Final Draft International Standard)段階にすすんだ ISO/IEC27551 Information technology – Requirements for attribute-based unlinkable entity authentication の策定に参画し

た。具体的にはトランザクションが unlinkable である状態の数学的な定義と、そのチャネルモデルの体系化を議論した。

３． 共同研究者

特になし

４． 研究業績

4.1 学術論文

江口、佐古「TSA を用いた擬似乱数発生アルゴリズムに関する一考察」 (SCIS 2021)

4.2 総説・著書

Blockchain Gaps -From Myth to Real Life- (Springer)

4.3 招待講演

国際赤十字　Follow the Sun イベント　（パネリスト）

金融庁 FINSUM 2021　（パネリスト）

日本数学会 2021 年度年会　企画特別講演「暗号プロトコル技術がもたらす透明性」

日本工学教育協会　事業企画委員会講演「デジタルトランスフォーメーションと暗号技術」

4.4 受賞・表彰

日本応用数理学会フェロー

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 Applied Cryptography and Network Security(ACNS 2021) プログラム共同委員長

ACM Advances in Financial Technologies (AFT 2020) 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

文部科学省 情報委員会 専門委員

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 情報規格調査会　委員(ISO/IEC JTC 1 SC 27 WG 5)

５． 研究活動の課題と展望

初年度は主に動向調査に終始した面があるが、社会の環境変化を踏まえ、社会基盤となる IT システムの重要性を再認識した１年であった。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の難しさはもとより、設計や開発にかけられる時間とコストの制限や、設計者と意思決定者の背景の違いがある。ハンコ出社と揶揄されたり、接触確認アプリ COCOA の開発体制の脆弱性が露呈したり、実社会が IT の恩恵を実感できるまでには多くのチャレンジがある。本研究で目的としている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し、その研究成果を適切に標準化することがこのギャップを埋める一助になるという思いもあらたにした。また、自己主権アイデンティティに関しては、日本政府をはじめ、イギリス、ドイツ、オーストラリアの各国政府も関心を寄せており、

グローバルなあらたな基盤になる可能性が出始めている。その一方で、IT のしくみを導入したことが、却って格差を拡大してしまうという懸念も考慮にいれつつ、導入にあたっては社会への影響も十分に吟味して、研究をすすめていきたい。