自己主権型アイデンティティ情報管理システム（uPort,Sovrin）考察

Considerations on self-sovereign identity information management system (uPort, Sovrin)

才所　敏明[*1]
Toshiaki Saisho
[*1] (株)IT 企画
Advanced IT Corporation

辻井　重男[*2]
Shigeo Tsujii
[*2] 中央大学研究開発機構
R&D Initiative, Chuo University

櫻井　幸一[*3]
Kouichi Sakurai
[*3] 九州大学大学院システム情報科学研究院
（株）国際電気通信基盤技術研究所

1. はじめに

本稿は、自己主権型アイデンティティ管理システム（SSIMS）に関する研究の第 2 報である。本稿では、アイデンティティ情報管理システム（IMS）に期待される機能を定義し、代表的 SSIMS である uPort および Sovrin について、自己主権性の観点からの調査・分析結果を報告する。

2. SSIMS における自己主権性

SSIMS として必要な機能は、本人確認機能および情報管理機能である。本人確認機能は身元確認および当人確認から構成され、情報管理機能は情報登録、情報保護、情報提供から構成されている。また、SSIMS を構成する主たる情報は、本人確認情報およびアイデンティティ情報である（図 1）。

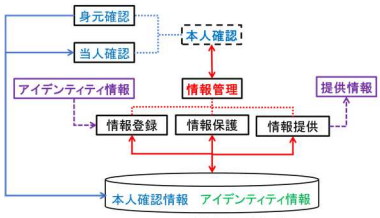

図1 SSIMSを構成する機能・情報

SSIMS の自己主権性の評価においては、SSIMS に期待される機能の提供内容、およびその機能に対する自己制御性と定義し、評価の視点をまとめた（図 2）。

本人確認	身元確認	確実な身元確認機能の有無
	当人確認	信頼できる当人確認機能の有無
管理情報	内容	情報内容に対する自己制御性（選択の自由・範囲）
	発行	情報発行主体に対する自己制御性（選択の自由・範囲）
	形式	管理情報形式に対する自己制御性（選択の自由・範囲）
	格納	情報格納方法に対する自己制御性（選択の自由・範囲）
情報管理	情報登録	①情報登録・更新・削除の指示における自己制御性 ②登録・更新・削除対象情報の内容における自己制御性
	情報保護	①保護対象情報・公開範囲の指定における自己制御性 ②情報保護方法における自己制御性
	情報提供	①提供先・提供情報指定における自己制御性 ②提供情報の最小化機能およびその自己制御性

図2 SSIMSの自己主権性評価の視点

3. SSIMS（uPort、Sovrin）の自己主権性評価

3.1 uPort システム概要

利用者は，uPort app からイーサリアムブロックチェーン上の Controller を起動する．Controller は更に Proxy を起動し，Registry 経由で IPFS へアイデンティティ情報を登録する．アイデンティティ情報の提供は，第三者からのイーサリアムブロックチェーン経由、あるいは別チャネルで依頼を受け、uPort app からの利用者の指示の元、提供情報そのものあるいは IPFS 上の情報へのアクセス情報が提供される（図 3）．

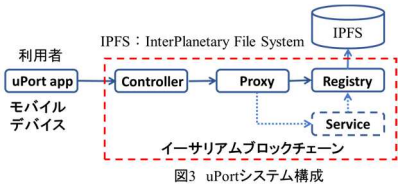

図3 uPortシステム構成

3.2 Sovrin システム概要

利用者は、User Client App 経由、User Agent をアクセスし、User Agent 経由、アイデンティティ情報の Sovrin Ledger への登録を申請する。個人情報を含むアイデンティティ情報は Sovrin Ledger には登録せず、User Agent で管理する。アイデンティティ情報の提供には User Agent 間の Direct Communication チャネルを使用し、Sovrin Ledger に登録されたアイデンティティ情報は、提供された情報の検証に使用される（図 4）。

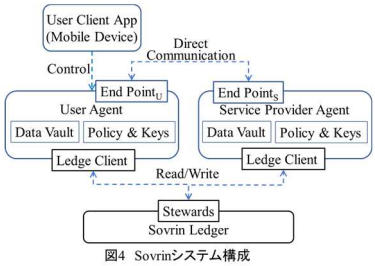

図4 Sovrinシステム構成

3.3 uPort、Sovrin の自己主権性の観点からの考察

(1)本人確認機能

uPort、Sovrin 共に、身元確認機能は外部サービスに依存している。SSIMS システム構築・採用時には身元確認を含む確実な本人確認機能の実装・連携の確認が必要である。

(2)管理情報

uPort ではアイデンティティ情報は IPFS に格納され、公開を制限すべき情報は暗号化により保護する方式、Sovrin では個人情報等は User Agent に格納し、公開できる情報を Sovrin Ledger で管理する方式。Sovrin の方が利用者へ多くの選択肢を提供している。

(3)情報管理

情報登録は、uPort、Sovrin 共に、登録情報の検査は行わず、利用者の判断で登録可能だが、不適切な情報が登録されるリスクが存在する。Sovrin の場合は登録情報に不適切な情報が含まれていないことを利用者が表明する必要があり、一定の抑止力が期待できる。

情報保護は、uPort、Sovrin 共に暗号技術による保護であり、共に暗号化・復号の指示は利用者のみ可能である。情報格納場所による保護については(2)に記載の通り。

情報提供は、uPort、Sovrin 共に利用者の指示のみ可能である。最小化機能については、uPort は暗号技術を利用した基本的機能のみだが、Sovrin ではゼロ知識証明を利用した最小化機能が提供されている。

4. おわりに

今回の調査・分析から確認できた、社会基盤として期待される SSIMS のために検討すべき事項は、以下の通り。

① 登録情報未検査の弊害の評価および回避策
② 登録情報の管理方式の評価（格納場所、使い分け）
③ 提供情報の多様な最小化機能（ゼロ知識証明の活用）
④ SSIMS の監査対応と必要なログの記録・管理方式

参考文献

”自己主権型アイデンティティ情報管理システムに関する一考察”，才所敏明，辻井重男，櫻井幸一、2021 電子情報通信学会・総合大会.

謝辞

本研究の一部は，一般財団法人テレコム先端技術研究支援センターの研究助成、および JSPS 科研費 基盤(B) JP18H03240 の支援を受けている．