

# 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

## Consideration on Self-Sovereign Identity Information Management System

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  
Kouchi Sakurai

\*3 九州大学大学院システム情報科学研究所  
(株) 国際電気通信基盤技術研究所

### 1. はじめに

個人の活動がインターネット上で展開されるサイバー社会へ移行する中、利用者の本人確認はもちろん、さまざまなアイデンティティ情報のインターネット上での確認を可能とするアイデンティティ情報の安全な利活用の仕組みが期待されている。本稿では、ブロックチェーンベースのセルフソブリンアイデンティティ情報管理システム (SSIMS) の自己主権性の観点からの評価の視点を整理・提案し、当該視点での uPORT の評価結果を報告する。

### 2. SSIMS 概要

アイデンティティ情報の利活用環境は、情報保有者、情報管理事業者、情報発行业者、情報使用事業者から構成される。SSIMS はアイデンティティ情報の利活用環境の中核に位置し、アイデンティティ情報保有者による情報登録・管理・提供を支援するシステムである (図 1)。

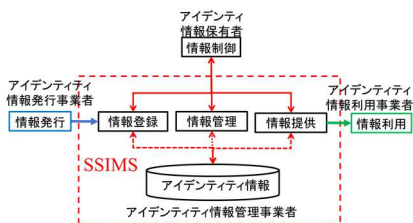


図1 アイデンティティ情報利活用環境の構成

SSIMS の管理対象情報は、登録実エンティティに対応する登録仮想エンティティの識別情報、実エンティティの身元確認情報、登録仮想エンティティとの同一性確認に使用される本人確認情報、登録仮想エンティティに対し登録されたアイデンティティ情報群の 4 種から構成される。また、SSIMS で実装される機能は一般に、利用者本人確認、アイデンティティ情報登録、アイデンティティ情報管理、アイデンティティ情報提供の 4 つに分類できる (図 2)。

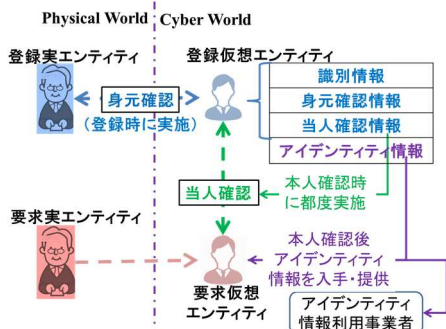


図2 SSIMS管理情報と本人確認

### 3. SSIMS の自己主権性評価の視点

SSIMS の自己主権性の評価にあたっては、“自己”確認の確実さ、情報登録の“自己”制御性、情報管理の“自己”制御性、情報提供の“自己”制御性、の 4 つの視点で評価する方式を提案する。“自己”確認の確実さは、“自己”

確認 (本人確認) を構成する身元確認および本人確認の確実さで評価する。情報登録の“自己”制御性は、情報の登録・更新・削除に対する利用者の制御能力、情報管理の“自己”制御性は、管理情報の秘匿・開示に対する利用者の制御能力で評価する。情報提供の“自己”制御性は、提供先・提供情報の選択・最小化に対する利用者の制御能力で評価する。

### 4. uPORT 評価

イーサリアムのスマートコントラクトを利用し実装された SSIMS である uPORT を対象に、提案した自己主権性の 3 つの視点での評価を実施した。

#### <uPORT 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、アイデンティティ情報の追加・更新・削除・参照の場合は Registry を直接起動する。他のアプリケーション経由の情報参照も可能である。アイデンティティ情報は、イーサリアムブロックチェーン上のトランザクションあるいは Registry から参照されるファイル (IPFS) に格納される (図 3)。

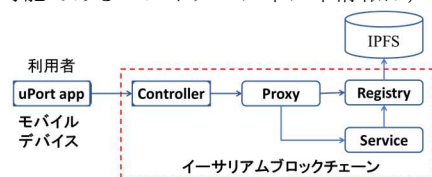


図3 uPORT基本構成要素関連図

#### <自己主権性評価>

“自己”確認：本人確認は、uPort app および Controller 間での公開鍵暗号を利用した署名検証で実施。身元確認機能は用意されていない。(外部サービスの利用またはスマートコントラクトによる別途の実装が想定されている)  
情報登録制御：情報登録・更新・削除は、利用者のみが可能。確実な自己主権性を実現 (SSIMS は制御不可)  
情報管理制御：管理情報の秘匿は利用者の判断で実施。暗号化・復号には利用者が管理する鍵を使用。確実な自己主権性を実現 (SSIMS は制御不可)。  
情報提供制御：情報提供先・提供情報は利用者の uPort app での承認が必要。確実な自己主権性を実現 (SSIMS は制御不可)。  
総括：“自己”確認以外、確実な自己主権性を実現。

### 5. おわりに

SSIMS の自己主権性の評価の視点を提案し、uPORT への適用を試みた。引き続き SSIMS の調査を進め、提案した評価の視点の妥当性の検証と具体的評価項目を検討したい。

**謝辞** 本研究の一部は、JSPS 科研費 基盤(B) JP18H03240 の支援を受けている。