電子情報通信学会ソサイエティ大会

 1

自己主権型アイデンティティ情報管理システム（uPort,Sovrin）に関する考察

2021年9月16日

（株）IT企画　才所敏明

toshiaki.saisho@advanced-it.co.jp

http://www.advanced-it.co.jp

共　著　者

辻井重男
中央大学研究開発機構

櫻井幸一
九州大学　大学院システム情報科学研究院
＆サイバーセキュリティーセンター
（株）国際電気通信基盤技術研究所

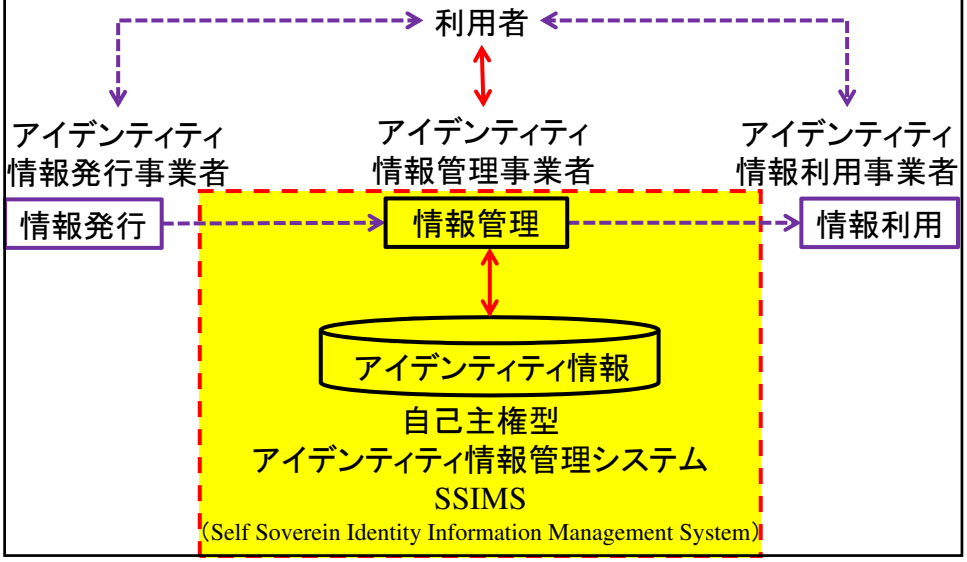
謝辞　本研究の一部は　一般財団法人テレコム先端技術研究支援センターの研究助成、
および　JSPS科研費 基盤(B) JP18H03240　の支援を受けている。

1．SSIUF

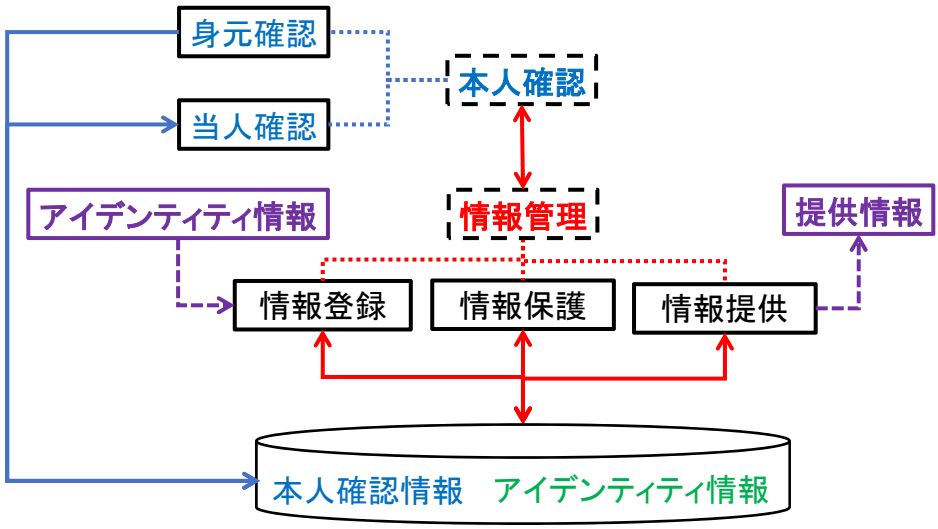
 2

アイデンティティ情報利活用環境

Identity Information Utilization Environment



自己主権型アイデンティティ情報管理システム（SSIMS）を構成する機能・情報



SSIMSにおける自己主権性評価の視点

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

3. uPort

uPort基本構成要素関連図

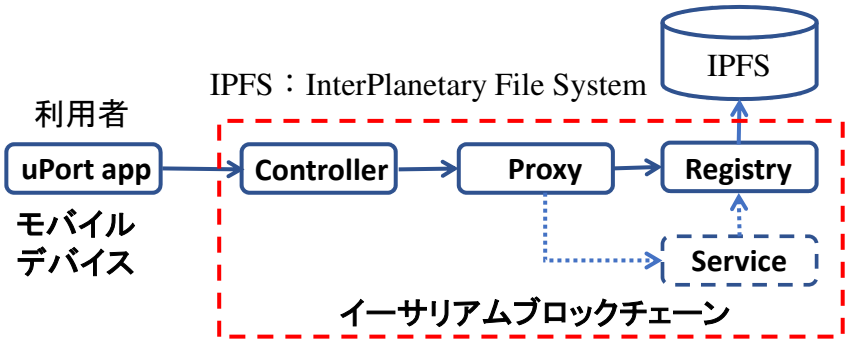


図3　uPortシステム構成

幅広い応用分野のSSIMS開発に利用可能な基本モジュール
（基本機能のみの実装、対象分野ごとの追加開発を想定）

https://developer.uport.me/
uPort：2015年発足の米国企業（注：最近sertoへ名称変更）

3. uPort

uPortにおける自己主権性（1）

		自己主権性の観点からの評価
本人確認	身元確認	身元確認機能は提供されていない
	当人確認	公開鍵ペアによる署名検証により当人確認
管理情報	内容	自由（応用分野によって規定）
	発行	TTP発行、自己発行
	形式	JOSE（JSON Object Signed and Encryption）
	格納	情報はLedgerではなくIPFSに登録 （モバイルデバイス側での格納も可）

3. uPort

uPortにおける自己主権性（2）

		自己主権性の観点からの評価
情報管理	情報登録	①uPort app経由の利用者の指示でのみ登録・更新・削除が可能 ②TTP発行、自己発行の任意の情報の登録が可能
	情報保護	①uPort app経由の利用者の指示でのみ情報保護・公開範囲の指定が可能 ②暗号化による情報保護が可能（JSON Web Algorithms (JWA)）
	情報提供	①uPort app経由の利用者のみが提供先・提供情報の承認可能 ②モバイルデバイスにて、提供先に応じた開示情報の最小化機能の実装は可能

4. Sovrin

Sovrin基本構成要素関連図

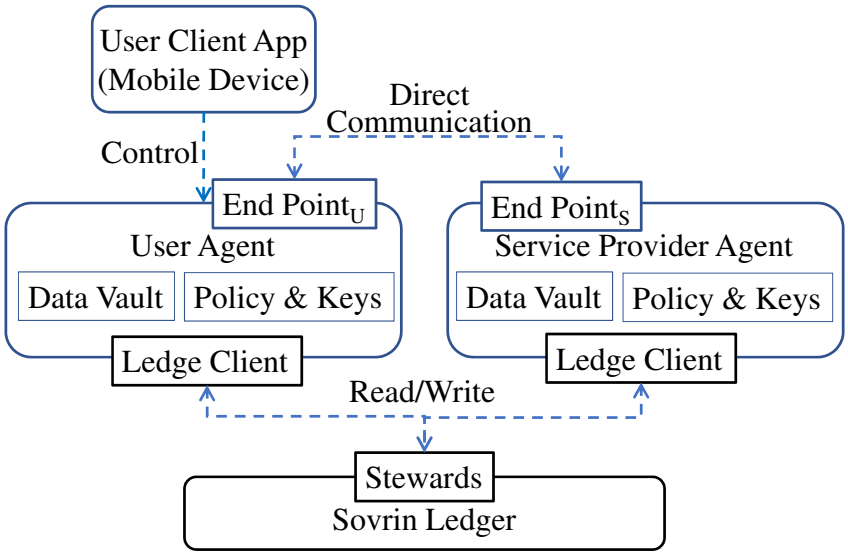


図4　Sovrinシステム構成

Sovrinにおける自己主権性（1）

本人確認	身元確認	身元確認機能は提供されていない
	当人確認	公開鍵ペアによる署名検証により当人確認
管理情報	内容	個人情報・プライバシー情報は、原則Ledgerへ登録しない（User Agent/モバイルデバイス上で管理）
	発行	TTP発行、自己発行
	形式	JOSE（JSON Object Signed and Encryption）
	格納	提供情報の情報提供先による検証のための情報をLedgerへ登録 （個人情報・プライバシー情報はUser Agent/モバイルデバイス上で管理）

Sovrinにおける自己主権性（2）

情報管理	情報登録	①User Client App経由の利用者の指示でのみ登録・更新・削除が可能 ②TTP発行、自己発行の任意の情報の登録が可能 但し、情報登録者は以下の条項を含むTransaction Author Agreementに署名が求められる ＊法律に違反したり他人の権利を侵害するトランザクションは書き込まないこと ＊パーソナルデータを含むトランザクションは書き込まないこと （必要な場合は、Sovrin Foundationの許可を得ること） ＊Ledger上のデータは恒久的に公開され、消去の保証はないこと ＊Ledger上のデータの信頼性や正確性は保証しないこと
	情報保護・情報提供は次スライド	

Sovrinにおける自己主権性（3）

情報管理	情報登録は前スライド	
	情報保護	①User Client App経由の利用者のみが情報保護・公開範囲の指定が可能 ②暗号化による情報保護が可能（JSON Web Algorithms (JWA)）
	情報提供	①User Client App経由の利用者でのみ提供先・提供情報の指定・承認が可能 ②User Agent内に、提供先に応じた提供情報の最小化のためのZKPを利用した次の機能が用意されている ＊指定された属性の値が、 指定された属性値に一致しているかどうか ＊指定された属性の値が、 指定された範囲に入っているかどうか ＊指定された属性の値が、 指定された集合の要素に含まれているかどうか

uPort、Sovrinの評価結果とSSIMSに期待される自己主権性に関する考察（1）

		uPort	Sovrin
本人確認	身元確認	共通：身元確認機能無し（別途実装を想定）	
	当人確認	共通：公開鍵ペアによる署名検証により当人確認	

考察　SSIMSとしては確実な本人確認は不可欠

uPort、Sovrin共に、身元確認機能無し

➔実用展開時には別途実装要

（信頼できる外部サービス（NAF/GAF等）との連携も選択肢）

5. 考察

uPort、Sovrinの評価結果と SSIMSに期待される自己主権性に関する考察（2）

		uPort	Sovrin
管理情報	内容	共通：制限なし	
	発行	共通：TTP発行、自己発行	
	形式	共通：JOSE（JSON Object Signed and Encryption）	
	格納	情報は原則IPFSに登録（公開を制限する情報は暗号化）	提供情報の検証のための情報をLedgerへ登録（個人情報・プライバシー情報は、原則Agentへ登録）

考察　個人情報・プライバシー情報の異なる格納場所の評価？

➔uPort：すべてIPFSで管理、公開限定情報は暗号化により保護

➔Sovrin：提供情報検証のために必要な情報をLedgerへ登録
個人情報等は、原則User Agentへ登録

5. 考察

uPort、Sovrinの評価結果と SSIMSに期待される自己主権性に関する考察（3）

		uPort	Sovrin
情報管理	情報登録	共通：①登録・更新・削除指示は利用者のみ	
		②任意の情報の登録が可能	②任意の情報の登録が可能だが、他人の権利を侵害しない、個人情報・プライバシー情報が含まれていないこと等を表明するTransaction Author Agreementへの署名が求められる

考察　共に、不適切な情報登録の検査機能無し！

➔登録情報の不適切さによる問題発生の抑止・防止策が必要
（万一の発生時の責任の所在を明確にしておく必要がある）

5. 考察

uPort、Sovrinの評価結果と SSIMSに期待される自己主権性に関する考察（4）

		uPort	Sovrin
情報管理	情報保護	共通：①情報保護・公開範囲の指定は利用者のみ 共通：②暗号化による情報保護	
	情報提供	共通：①提供先・提供情報の指定・承認は利用者のみ	
		②具体的提供機能無し（開示情報の最小化機能はモバイルデバイスにて実装可能）	②User Agent内に、ZKPを利用した最小化のための機能（一致、大小関係、集合要素）が用意されている

考察　情報本体の提供方式の違い？提供情報の最小化機能の有無！

➔uPortはIPFS経由、SovrinではP2Pで情報本体を提供

➔Sovrinでは、ZKPを利用した提供情報の最小化機能を提供

（応用分野に応じ、多様な最小化機能が必要となるか）

共に、提供先・提供情報の記録機能は無い➔必要ではないか

6. おわりに

 16

まとめ

（1）SSIMSの自己主権性評価の視点を整理・提案

本人確認、管理対象情報、情報管理（登録・保護・提供）

（2）タイプの異なるuPort, Sovrinの自己主権性評価結果を報告

①幅広い応用分野のSSIMS開発に利用可能な基本モジュール

②幅広い応用分野を対象にサービス提供を目指したSSIMS

（3）SSIMSの自己主権性に関する課題を報告

期待されるSSIMSにおける検討テーマの把握

本人確認機能、個人情報・プライバシー情報の保護方式、
不適切な情報の登録への対応、監査機能、
提供情報の最小化方式

（4）今後の検討課題

提案したSSIMSの自己主権性評価の視点の見直し、
期待される安心・安全なSSIMSとしての要件整理

 17

終

（ご清聴、ありがとうございました）