CSS2021 1

自己主権型 アイデンティティ情報利活用基盤 に関する考察

2021年10月28日

（株）IT企画　才所敏明
(株)ZenmuTech
中央大学研究開発機構
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．必要性 2

アイデンティティとは

エンティティが保有する属性の集合で示されるエンティティの性質
ISO/IEC24760-1の定義：「実体に関する属性情報の集合」

アイデンティティ情報（属性情報）の例
（1）エンティティの名前、性別、生年月日、住所等（基本属性）

（2）エンティティの現所属・役職、健康状態等（付加属性）

（3）エンティティの学歴、職歴、病歴等（履歴属性）

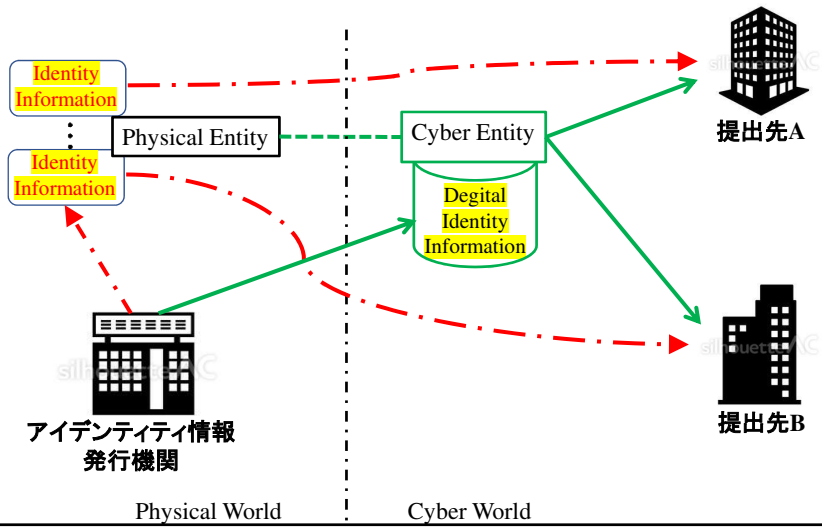
（4）エンティティの各種サービス利用情報等（利用属性）

（5）エンティティの信用、評判等（関係属性）

1．必要性

 3

Cyber Worldでの個人の活動の広がり デジタルアイデンティティ情報の活用へ



1．必要性

 4

個人の活動のDX

デジタル技術の活用によって個人の日々の活動形態を変革し、
新たなデジタル時代に迅速で効率的な活動を可能とすること

＊日本のインターネットの歴史は1984年に始まり、
未だ35年余りだが、産業界の様々の活動はもちろん、
国民の日々の生活に欠かせないものに。

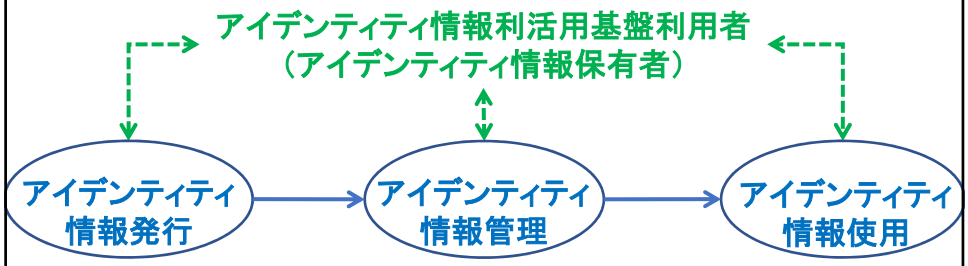
＊ICT技術の発展は留まるところを知らず、
社会はますますインターネット上のサービスへ依存を強め、
Cyber Worldでの個人の活動も大きく進展するのは必至。

＊Physical Worldで個人の活動で利用されていた様々の書類も
Cyber World内での送受へと移行、様々のアイデンティティ情報も
ネット経由で迅速に効率的に送受信される時代へ移行するのは必至

➔個人の活動のDX推進には、
デジタルアイデンティティ情報の利活用を支える基盤が重要

自己主権型アイデンティティ情報利活用基盤

SSIUF：Self-Sovereign Identity-information Utilization Framework



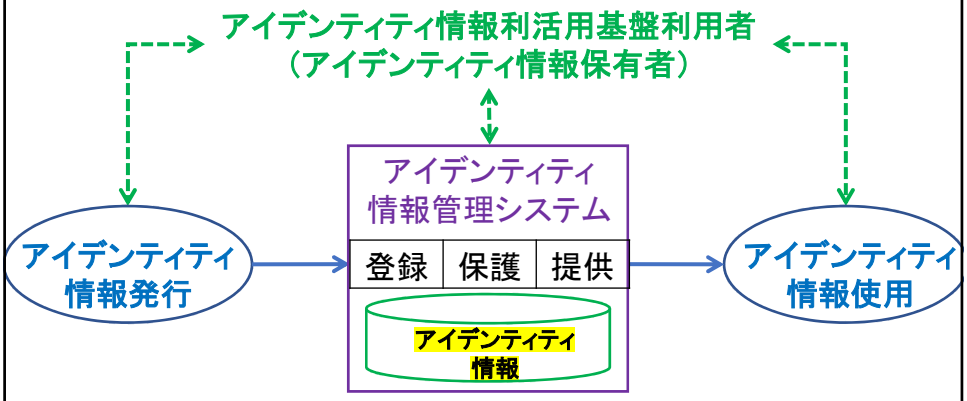
自己主権型（セルフソブリン）アイデンティティ情報利活用基盤：
エンティティ（属性保有者）によるアイデンティティ情報の
確実な利活用制御が可能なシステム

SSIUF社会実装のための検討課題

フェーズ		主要な検討課題
情報発行		①情報保有者の意思に基づくアイデンティティ情報発行制御 ②アイデンティティ情報の一定の標準化（形式、表現方法等） ③アイデンティティ情報発行主体の信頼性確認可能性
情報管理	（情報登録）	①情報保有者の意思に基づくアイデンティティ情報登録 ②不正な情報の登録への対応 ③登録情報の整合性
	（情報保護）	①情報保有者の意思に基づくアイデンティティ情報保護 ②登録情報の多様な保護ニーズへの対応 ③登録情報へのアクセス検証・監査可能性
	（情報提供）	①情報保有者の意思に基づくアイデンティティ情報提供 ②提供先・提供依頼情報の妥当性 ③提供情報の最小化機能 ④提供情報の標準化（形式、表現方法等） ⑤提供先への安全な情報提供 ⑥提供先・提供情報の検証・監査可能性
情報使用		①情報保有者の意思に基づく提供情報の使用制御 ②提供情報の利用記録の検証・監査可能性 ③提供情報の抹消/抹消確認

自己主権型アイデンティティ情報管理システム

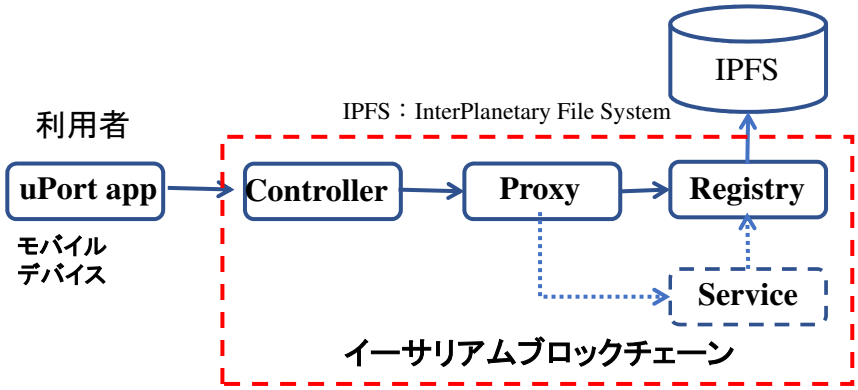
SSIMS：Self-Sovereign Identity-information Management System



SSIMSに期待される機能

機能分類		期待される機能および検討が必要な課題
本人確認	（身元確認）	①利用登録時の情報保有者の確実な身元確認
	（当人確認）	①利用時の情報保有者の確実な当人確認
情報管理	（情報登録）	①情報保有者以外の情報登録の排除 ②不正な情報の登録回避/登録情報の不正確認後の対応 ③既登録情報との整合性確認
	（情報保護）	①情報保有者以外の情報保護制御の排除 ②登録情報の多様な保護方式 ③登録情報へのアクセスの記録
	（情報提供）	①情報保有者以外の情報提供制御の排除 ②提供情報の多様な最小化対応 ③提供先・提供情報の記録

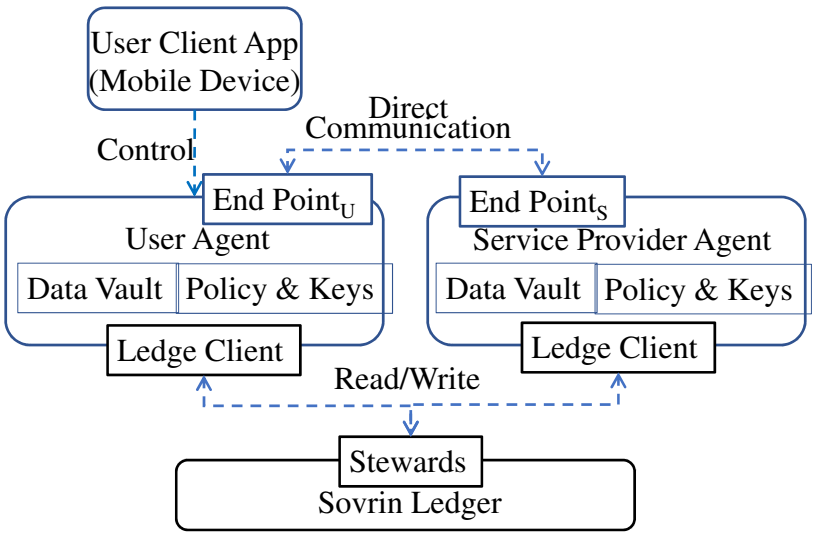
uPort基本構成要素関連図



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）

Sovrin基本構成要素関連図



幅広い応用分野での利用を想定し運用を目指したSSIMS

uPort-Sovrin比較

機能分類		機能・課題番号	uPort	Sovrin
本人確認	（身元確認）	①	身元確認機能無し	
	（当人確認）	①	公開鍵暗号による署名検証当人確認方式 （NISTガイドラインによる当人確認保証レベルはAAL2）	
情報管理	（情報登録）	①	情報保有者のみIPFS登録可能	情報保有者のみLedger登録可能
		②	登録回避機能無し Registryコントラクト内の データへのリンク削除可能 （IPFS上には登録情報が残存）	登録回避機能無し （不正な情報を登録をしないことの 誓約書へ署名を要求） Leger上のデータ削除は困難 （無効化あるいは 改定版の情報登録は可能）
		③	既登録情報との整合性チェック機能無し	
	（情報保護）	①	保護情報・保護方式の指示は情報保有者のみ可能	
		②	IPFS上の情報は 暗号化により保護が可能	Ledger上の情報は 暗号化により保護が可能 非公開領域であるUser Agentへの 登録による保護も可能
		③	参照の記録機能無し	
	（情報提供）	①	提供先・情報情報の指示は情報保有者のみ可能	
		②	登録情報は そのままの提供が原則 （登録情報の加工による 提供には別途実装が必要）	Ledger登録情報は 参照による提供が原則 User Agent登録情報は、ZKPを利用した 提供情報の最小化が機能有り （属性値の一致、指定された範囲内、 指定された集合の要素、かどうか）
		③	提供の記録機能無し	

uPort-Sovrin調査・比較結果に基づく SSIMSに期待される機能に関する考察（1）

（1）本人確認について＜自己主権性は、確実な本人確認が大前提＞

①身元確認は必須だが、その実現方法？

＊個別のSSIMSで身元確認、身元情報管理する方法？

＊信頼できる組織が身元確認後に発行するDID、
各国NAFが身元確認後に発行するNAF-ID等の利用？

（2）情報管理について

①SSIMS運用者による不正・不法・不適切な情報登録の回避？
登録情報は暗号化等で秘匿され検査はそもそも困難
個人情報・プライバシー情報の閲覧・検査の是非

＊信頼できるアイデンティティ情報発行者の署名検証で代替？

＊事後の確実な対応で代替？

uPort-Sovrin調査・比較結果に基づく SSIMSに期待される機能に関する考察（2）

②アイデンティティ情報の保護方法？
- ＊非公開領域で保護？（Sovrin方式）
- ＊公開領域で、暗号化による保護？（uPort方式）

③提供後のアイデンティティ情報への自己制御性？
以下の機能が望ましいが・・・実現方式の検討要
- ＊提供情報の使用の確認？
- ＊使用目的外使用の禁止？
- ＊使用終了後の抹消？

おわりに

（1）自己主権型アイデンティティ情報利活用基盤（SSIUF）
- SSIUFの必要性提案
- SSIUF社会実装のための主要な検討課題提案

（2）自己主権型アイデンティティ情報管理システム（SSIMS）
- SSIMSに期待される機能提案
- uPort-Sovrin比較・評価とSSIMSの機能に関する考察

（3）今後の活動予定
- SSIUF、SSIMSの要件や機能の分析・評価を継続
- W3Cで議論されているDIDおよびVC関連技術を活用した SSIUF/SSIMS構想の具体化検討

終

（ご清聴、ありがとうございました）