

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

2021年3月12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　JSPS科研費 基盤(B) JP18H03240　の支援を受けている。

自己主権型（セルフソブリン）アイデンティティ情報管理システム

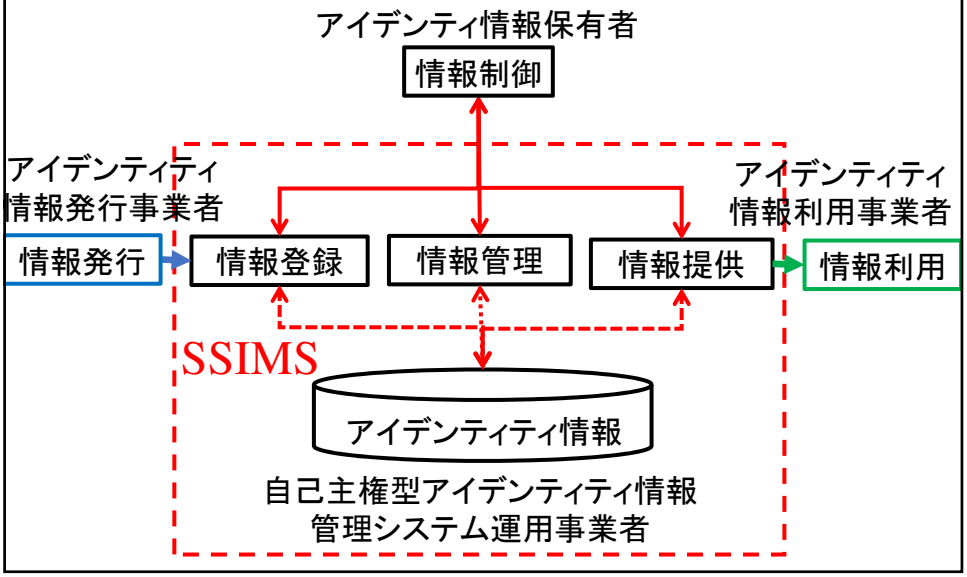
アイデンティティ：
　エンティティが保有する属性の集合で示されるエンティティの性質

アイデンティティ情報管理システム：
　エンティティのアイデンティティを構成する属性情報の管理システム

　ID管理システム（ IDaaS）との違い：
　　ID管理システムは、一般にアクセス制御に使用するIDおよび
　　パスワード等のアクセス時の認証情報の管理を行うシステム

自己主権型（セルフソブリン）アイデンティティ情報管理システム：
　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管理システム

自己主権型アイデンティティ情報利活用環境（SSIUF）の構成



The Laws of Identity by Kim Cameron （2005）

① User Control and Consent	Digital identity systems must only reveal information identifying a user with the user's consent
② Minimal Disclosure for Limited Use	The solution which discloses the least amount of identifying information and best limits its use is the most stable long term soluton
③ Justifiable Parties	Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship
④ Directed Identity	A universal identity system must support both “omni-directional” identifiers for use by public entities and “unidirectional” identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles
⑤ Pluralism of Operators and Technologies	A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers
⑥ Human Integration	The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks
⑦ Consistent Experience Across Contexts	The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies

https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

2. SSIMS/SSIUF

 5

Ten Principles of Self-Sovereign Identity by Christopher Allen （2016）

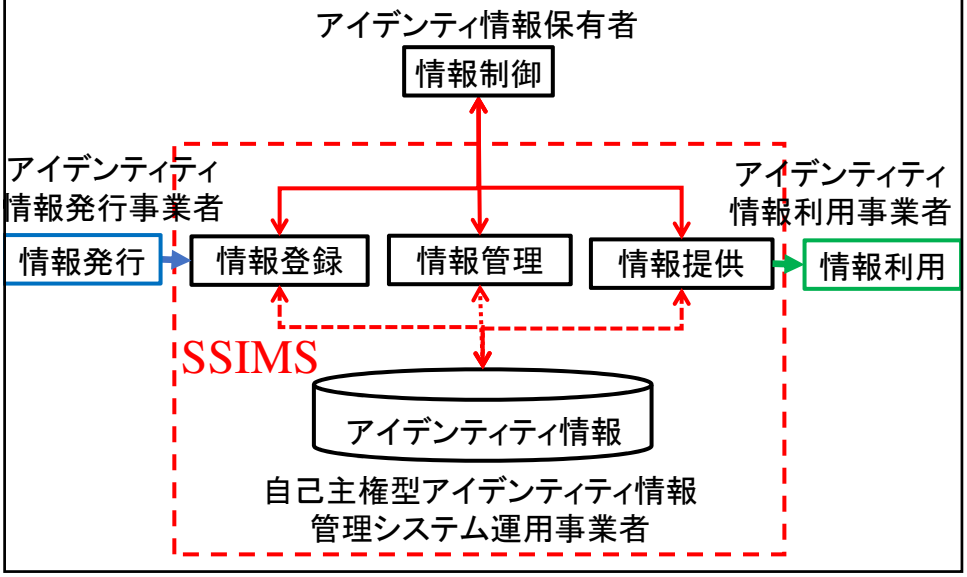
① Existence	Users must have an independent existence
② Control	Users must control their identities
③ Access	Users must have access to their own data
④ Transparency	Systems and algorithms must be transparent
⑤ Persistence	Identities must be long-lived
⑥ Portability	Information and services about identity must be transportable
⑦ Interoperability	Identities should be as widely usable as possible
⑧ Consent	Users must agree to the use of their identity
⑨ Minimalization	Disclosure of claims must be minimized
⑩ Protection	The rights of users must be protected

http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

3. 自己主権性評価の視点

 6

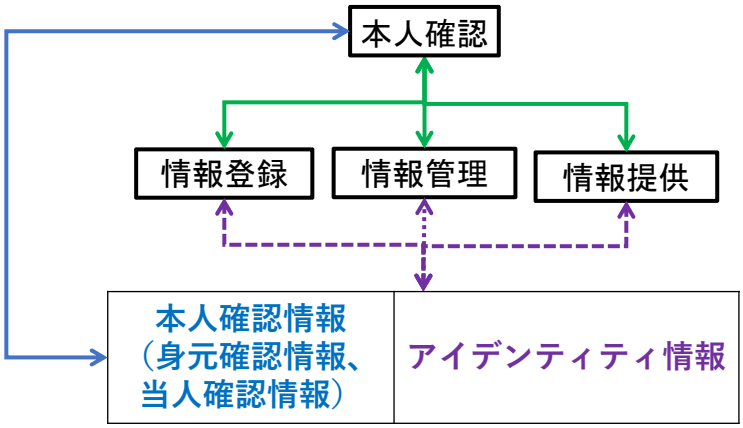
自己主権型アイデンティティ情報利活用環境（SSIUF）の構成



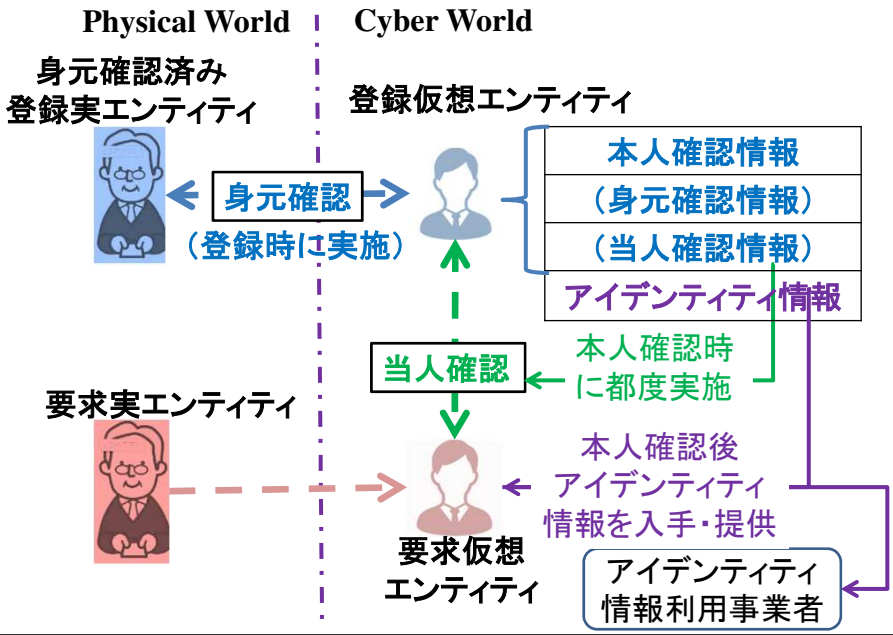
SSIMS

（Self-Sovereign Identity Information Management System）

4つの機能と2つの情報から構成



SSIMSにおける本人確認手順



SSIMSの自己主権性評価の視点

自己主権性＝SSIMSの各機能に対する“自己”制御性

（1）“自己”確認（本人確認）の確実さ
　　本人確認を構成する身元確認・当人確認の確実さ

（2）情報登録の“自己”制御性
　　情報の登録・更新・削除に対する利用者の制御能力

（3）情報管理の“自己”制御性
　　管理情報の秘匿・開示に対する利用者の制御能力

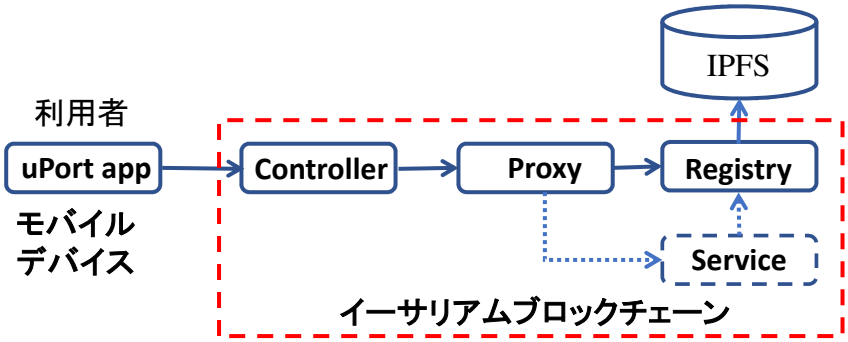
（4）情報提供の“自己”制御性
　　提供先・提供情報の選択・最小化に対する利用者の制御能力

Ten Principles of SSIと 自己主権性評価の視点との対応

Ten Principles of SSI by Christopher Allen	SSIMSの自己主権性評価の視点			
	“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
① Existence	○	－	－	－
② Control	○	○	○	○
③ Access	○	○	○	○
④ Transparency	－	－	－	－
⑤ Persistence	－	－	－	－
⑥ Portability	－	－	－	－
⑦ Interoperability	－	－	－	－
⑧ Consent	○	○	○	○
⑨ Minimalization	－	－	○	○
⑩ Protection	○	○	○	○

4. uPORT

uPORT基本構成要素関連図



IPFS：InterPlanetary File System

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

4. uPORT

 12

“自己”確認を除き、確実な自己主権性を実現

（1）“自己”確認（本人確認）の確実さ
当人確認は，uPort appおよびController間での署名検証
身元確認機能は無し（別途の実装を想定）

（2）情報登録の“自己”制御性
情報登録・更新・削除は、uPort app経由で利用者のみ可
確実な自己主権性を実現（SSIMSは制御不可）

（3）情報管理の“自己”制御性
情報秘匿制御のための暗号化・復号はuPort appで利用者のみ可
確実な自己主権性を実現（SSIMSは制御不可）

（4）情報提供の“自己”制御性
情報提供先・提供情報は、uPort appでの利用者の承認が不可欠
確実な自己主権性を実現（SSIMSは制御不可）

5. 評価の視点の評価

 13

SSIMSの分類・評価に関する今後の検討項目

（1）取り扱うアイデンティティ情報
　　信頼できる第三者機関発行の情報vs自己発行の情報

（2）登録アイデンティティ情報の妥当性・整合性検証
　　管理下のアイデンティティ情報へのSSIMS運用事業者の責任

（3）アイデンティティ情報の提供時の提供情報の最小化
　　アイデンティティ情報の登録時の分割（単位情報化）
　　提供依頼に対する必要十分な情報の抽出・合成（加工機能）

（4）アイデンティティ情報利活用環境SSIUFの持続性
　　SSIUFを構成するSSIMS間連携/アイデンティティ情報の移行

（5）SSIUF/SSIMSのグローバルな運用性・連携性

6. おわりに

 14

まとめ

（1）SSIMSの自己主権性評価の視点を提案
　　“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

（2）uPORTの自己主権性評価に適用
　　uPORTは、“自己”確認を除き、確実な自己主権性を実現
　　＜uPORTはシンプルな機能であることが要因か＞

（3）今後の検討課題
　　①自己主権性評価の視点の見直し/妥当性検証
　　②SSIUF/SSIMSの分類・評価のための課題の検討
　　③SSIUF/SSIMSのあるべき姿の検討/具体的提案

終

（ご清聴、ありがとうございました）