

①自己主権型 アイデンティティ情報管理システムの評価・課題

2021年6月16日
才所敏明
（株）IT企画・代表取締役社長
中央大学研究開発機構・研究員
（株）ZenmuTech顧問
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp
https://www.facebook.com/toshiaki.saisho

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
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）

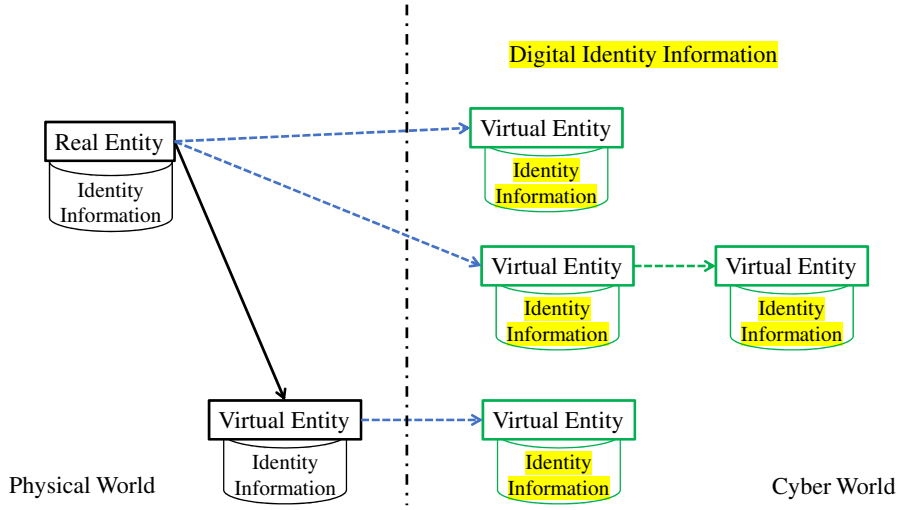
（2）エンティティの現所属・役職、健康状態等（付加属性）

（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）

デジタルアイデンティティ情報



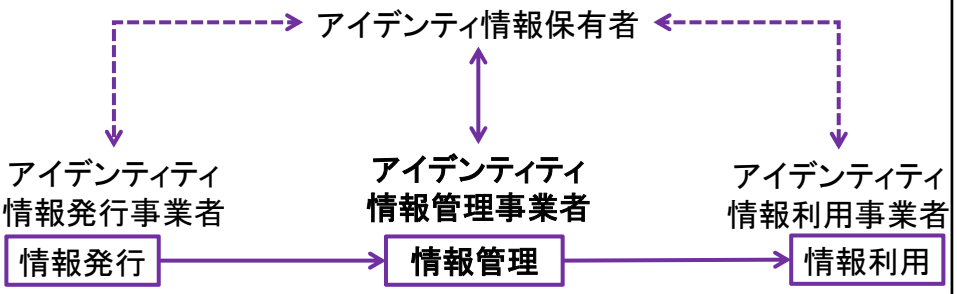
アイデンティティ情報管理システム

エンティティのアイデンティティを構成する
デジタルアイデンティティ情報（属性情報）の管理システム

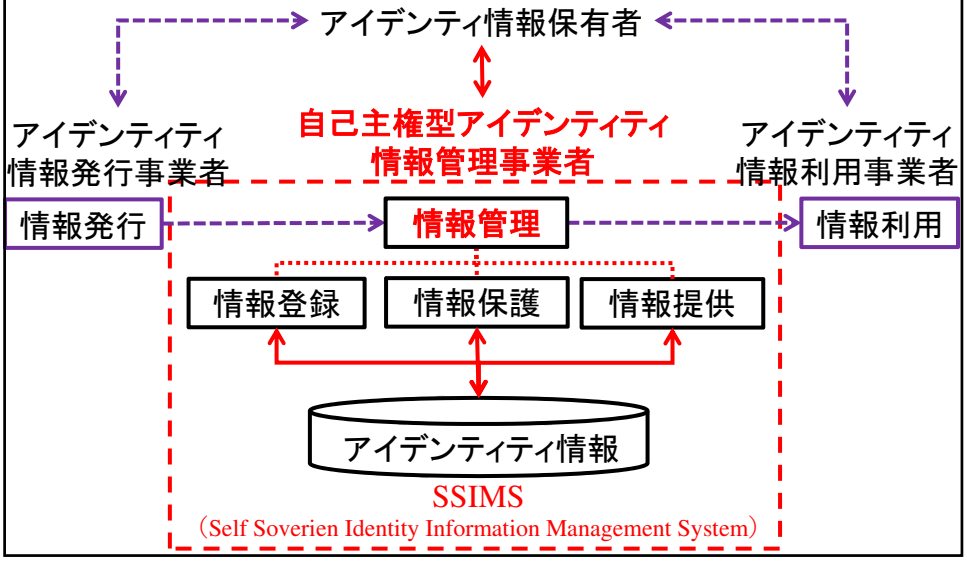
ID管理システム（ IDaaS）との違い：
ID管理システムは、一般にアクセス制御に使用するIDおよび
パスワード等のアクセス時の認証情報の管理を行うシステム

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

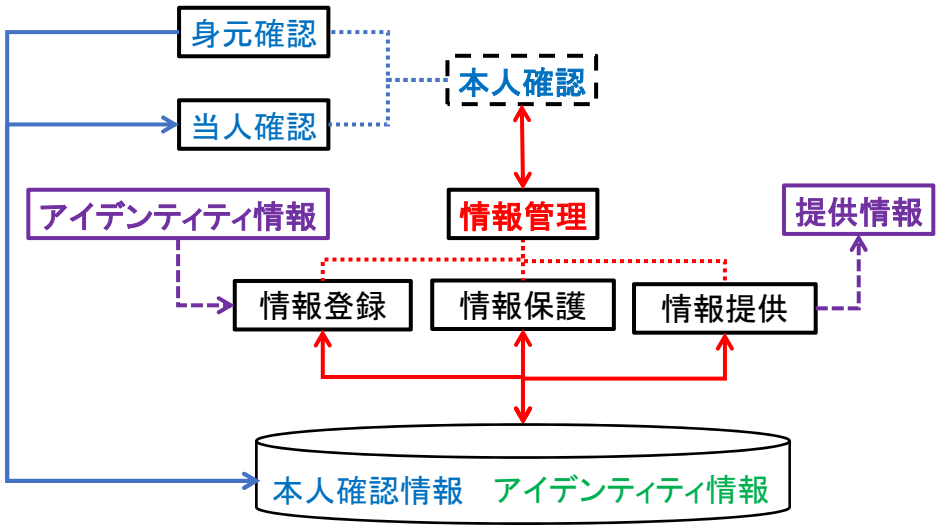
SSIUF
アイデンティティ情報利活用環境
（Self Sovereign Identity Information Utilization Framework）



自己主権型アイデンティティ情報管理システム
Self Sovereign Identity Information Management System



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



利用者の本人確認

確実な本人確認は、自己主権を主張する大前提

本人確認は、身元確認と当人確認より構成 ➔ 説明図

（1）利用登録時の身元確認

登録情報に責任を有する情報登録者の特定・追跡性の確認

（2）利用時の当人確認

自己主権を主張する利用者が情報登録者であることの確認

本人確認の確実さ＝身元確認の確実さ×当人確認の確実さ

身元確認の確実さ：NIST SP 800-63A　IAL1～IAL3

当人確認の確実さ：NIST SP 800-63B　AAL1～AAL3

本人確認の実施方法：

SSIMSにおいて実施

本人確認基盤（NAF）の本人確認結果を利用 ➔ 説明図

管理対象情報およびその格納方式

管理対象アイデンティティ情報
- 情報内容
  - 個人情報・プライバシー情報？　不正確な情報？
  - 他人の情報？　悪意のある情報？
- 情報表現形式
  - JOSE（JSON Object Signed and Encryption）等
- 情報発行元
  - TTP発行、自己発行

情報の管理（格納）場所
- on-Ledgerかoff-Ledgerか？
- パブリックスペースかプライベートスペースか？

情報管理への利用者の自己主権性

情報管理における自己主権性
＝情報登録・保護・提供機能に対する利用者の自己制御性

（1）情報登録
情報の登録・更新・削除に対する利用者の制御能力

（2）情報保護
管理情報の秘匿・開示に対する利用者の制御能力

（3）情報提供
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

（1）情報登録の自己主権性評価の視点

①情報登録・更新・削除の指示における自己制御性
　利用者による指示のみか（完全自己制御）
　SSIMSによる指示、あるいはSSIMSの関与があるかどうか

②登録・更新・削除の指示内容（情報内容等）における自己制御性
　利用者の指示内容に従った対応（完全自己制御）
　内容・形式・発行元に応じたSSIMSの判断に左右されるか

（2）情報保護の自己主権性評価の視点

①保護対象情報・公開範囲の指定に対する自己制御性
　利用者による指示のみか（完全自己制御）
　何らかの形でのSSIMSの関与があるか

②情報保護方法における自己制御性
　提供されている情報保護（秘匿）方法の多様性と
　　利用者による自由な選択
　＊アクセス制御
　＊暗号化
　＊秘密分散　等

（3）情報提供の自己主権性評価の視点

①提供先・提供情報指定における自己制御性
　利用者による指示のみか（完全自己制御）
　何らかの形でのSSIMSの関与があるか

②提供情報の最小化機能およびその自己制御性
　最小化のために提供されている加工/処理機能の多様性と利用者による自由な選択
　＊選択された登録情報を提供
　＊登録情報から必要情報のみ抽出/
　　マスク等により、必要な情報のみを提供
　＊質問への回答のみを提供　等

SSIMSの自己主権性評価の視点（まとめ）

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

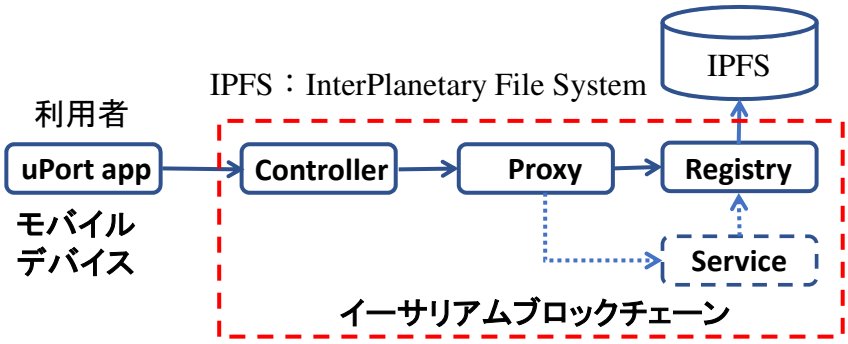


図3　uPortシステム構成

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）

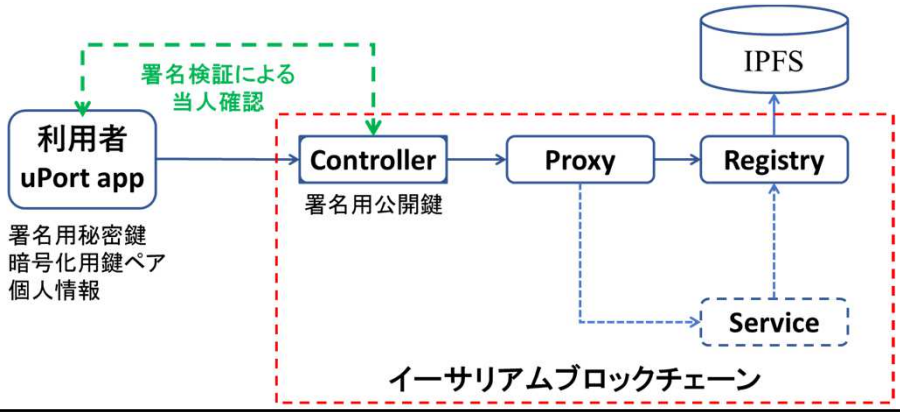
https://developer.uport.me/
uPort：2015年発足の米国企業（注：最近sertoへ名称変更）

3. uPort

 16

uPort
利用者の本人確認

①利用登録時の身元確認　➔　身元確認機能は提供されていない
②利用時の当人確認　➔　公開鍵ペアによる署名検証により実施



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

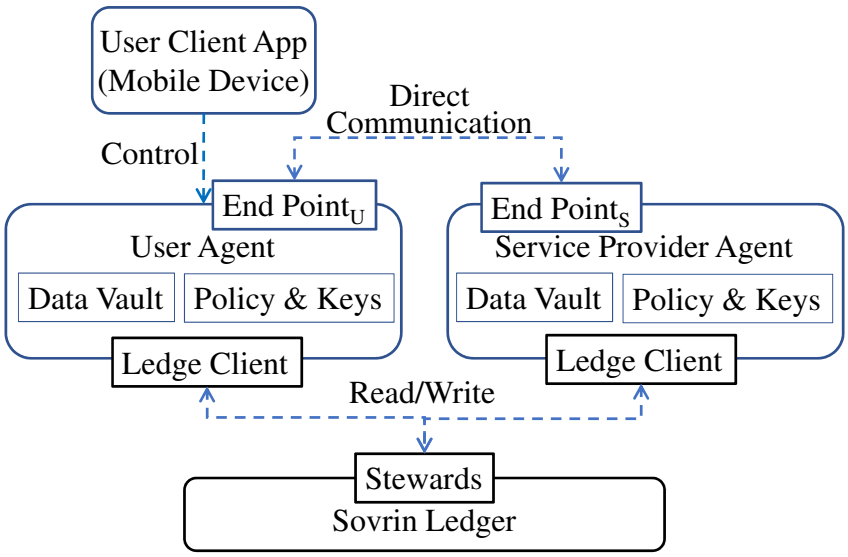


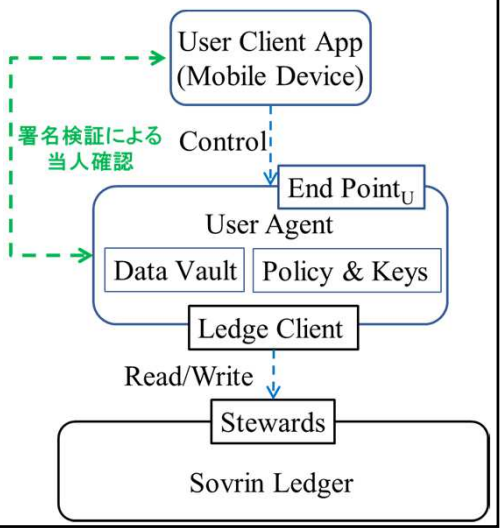
図4　Sovrinシステム構成

4. Sovrin

 20

Sovrin
利用者の本人確認

（1）利用登録時の身元確認
➔身元確認機能は
提供されていない
（2）利用時の当人確認
➔公開鍵ペアによる
署名検証により実施



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

SSIMSに期待される自己主権性の観点からの考察

		uPort	Sovrin
本人確認	身元確認	共通：身元確認機能無し	
	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

①uPort、Sovrin共に、身元確認機能無し

➔SSIMSとしては確実な本人確認は不可欠

（信頼できる外部サービス（NAF/GAF等）との連携

あるいは独自実装による対応が必要）

5. 考察

SSIMSに期待される自己主権性の観点からの考察

		uPort	Sovrin
管理情報	内容	自由	個人情報・プライバシー情報は、原則Ledgerへ登録しない
	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	提供情報の検証のための情報をLedgerへ登録

考察

①個人情報・プライバシー情報の異なる管理方式

➔どう評価するか

5. 考察

SSIMSに期待される自己主権性の観点からの考察

		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

①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）

➔各国の法制度等の違いが障害となるか

5. 考察

SSIMSに期待される自己主権性の観点からの考察

		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

①uPortはIPFS経由、SovrinではP2Pで情報提供

➔異なる情報提供方式をどう評価するか

②Sovrinでは、提供情報の最小化機能が用意されている

➔応用分野に応じ、多様な最小化機能が必要となるか

③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

まとめ

（1）SSIMSの自己主権性評価の視点を整理・提案

本人確認機能：身元確認、当人確認

管理対象情報：情報内容、情報表現形式、情報発行元

情報の管理（格納）場所

パブリックスペースかプライベートスペースか？

情報管理機能：情報登録、情報保護、情報提供

（2）タイプの異なるuPort, Sovrinの自己主権性評価結果を報告

uPort：幅広い応用分野の

SSIMS開発に利用可能な基本モジュール

Sovrin：幅広い応用分野を対象とした

サービスの提供に利用可能なSSIMS

6. おわりに

期待されるSSIMSに向けて

（1）確実な身元確認の実現方式

インターネット上のアプリケーションサービスに共通の課題

NAF（National Authentication Framework）

/GAF（Global Authentication Framework）

（2）個人情報・プライバシー情報の保護方式

“非公開”による保護vs“暗号化”による保護

（3）不適切な情報登録・提供への対応方式

登録・提供時点での検査機能 （vs情報保護の自己主権性）

問題発生時に登録・提供者の特定・追跡機能

（vs登録・提供者の匿名性）

（4）提供情報の最小化方式

ゼロ知識証明のさらなる活用

登録情報の正規化、最小単位化の可能性

関連発表一覧

自己主権型アイデンティティ情報管理

＊才所敏明，辻井重男，櫻井幸一，”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電子情報通信学会・総合大会，2021年3月2日．

本人確認基盤

＊才所敏明，辻井重男，「インターネット上のサービスにおける利用者の匿名性と特定・追跡性の両立」，2021年暗号と情報セキュリティシンポジューム（SCIS2021），2021年1月20日．

＊才所敏明，辻井重男，「インターネット時代の本人確認基盤に関する考察－NAFからGAFへ －」，コンピュータセキュリティシンポジューム2020（CSS2020），2020年10月26日．

＊才所敏明，「NAFJPにおける本人確認方法に関する考察 － National Authentication Framework in Japan －」，コンピュータセキュリティシンポジューム2019（CSS2019），2019年10月21日．

＊才所敏明，辻井重男，「日本における本人確認基盤（NAFJA）の考察 － National Authentication Framework in Japan －」，情報処理学会・第85回コンピュータセキュリティ研究発表会，2019年5月24日．

下記URLより、論文・プレゼン資料ダウンロード可

http://advanced-it.co.jp/2016_wp/president/

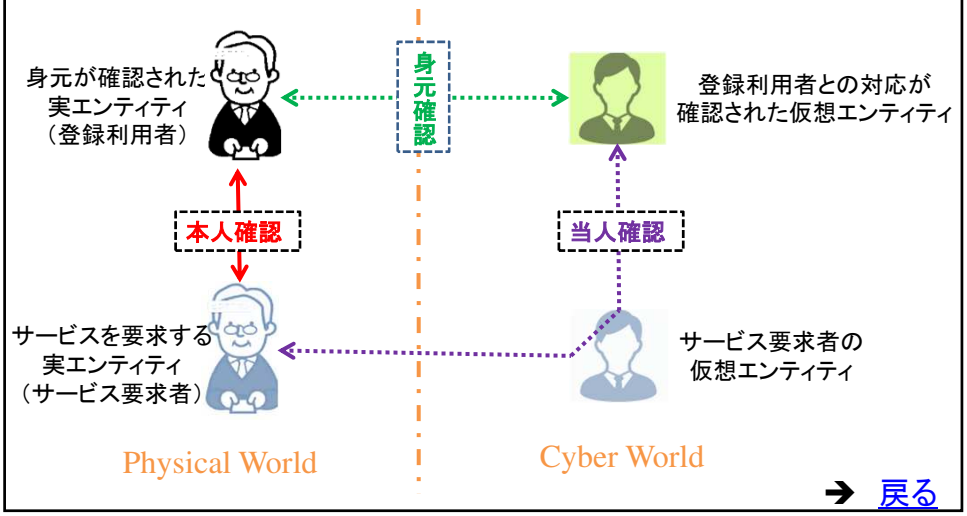
 31

終

 32

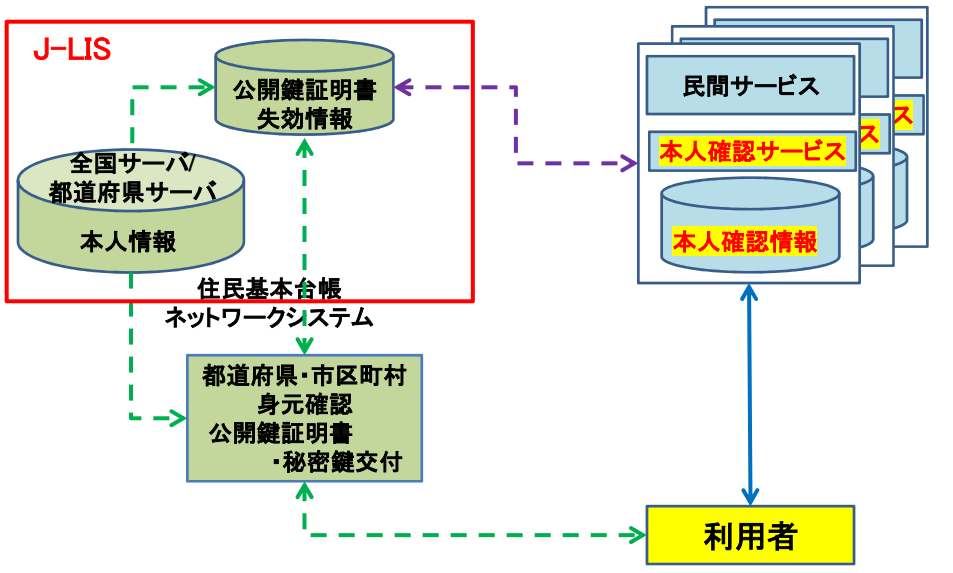
補足説明資料

本人確認＝身元確認＋当人確認

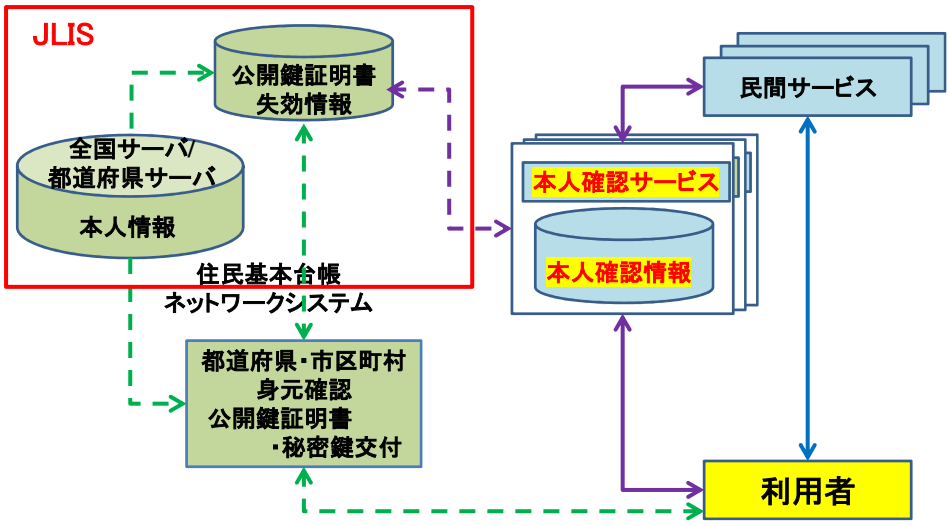


➔ 戻る

日本の民間サービスにおける本人確認の現状



日本の民間サービス向け本人確認基盤NAFJP



➔ 戻る