SCIS2022

 1

分散型ID/検証可能属性証明技術を利用した自己主権型アイデンティティ情報利活用基盤

2022年1月19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の支援を受けている。

1．必要性

 2

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。

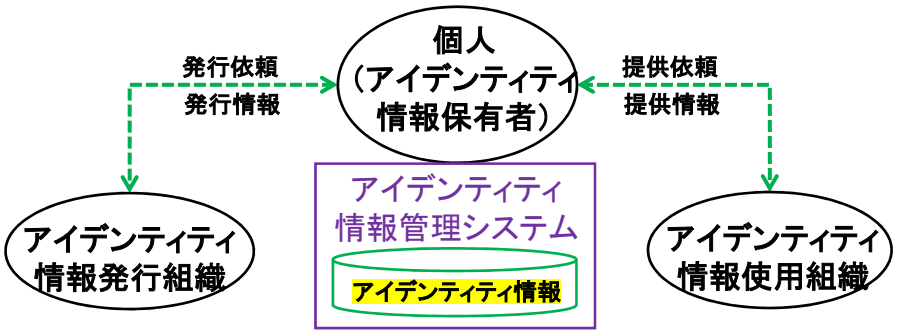
＊ICT技術の発展は留まるところを知らず、
社会はますますインターネット上のサービスへ依存を強め、
Cyber Worldでの個人の活動も大きく進展するのは必至。

＊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、
アイデンティティ情報の安心・安全な利活用を支える環境が重要

1．必要性

アイデンティティ情報利活用環境



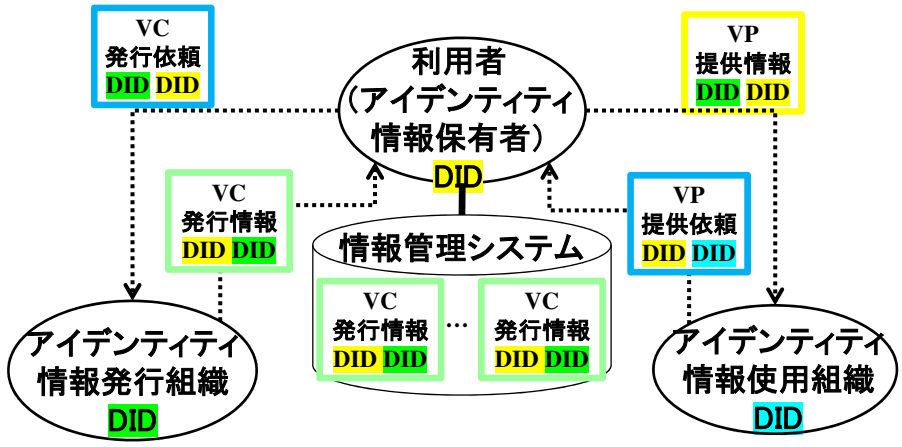
アイデンティティ情報の
情報保有者による確実な利活用制御が可能な環境

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

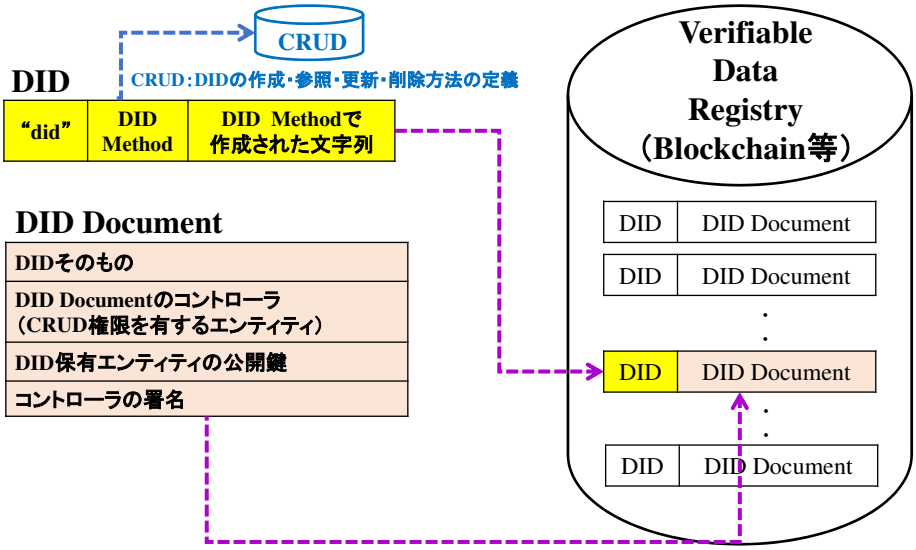
2．DID/VC

自己主権型アイデンティティ情報利活用基盤
DID/VC技術によるSSIUF構成



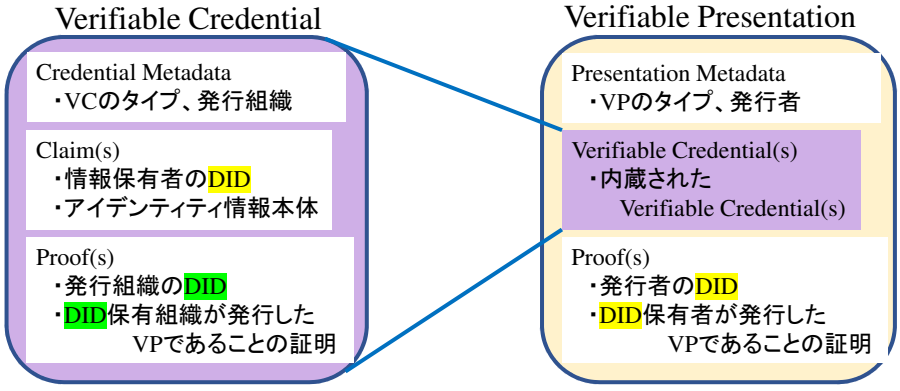
DID：Digital Identifier　VC：Verifiable Credential　VP：Verifiable Presentation

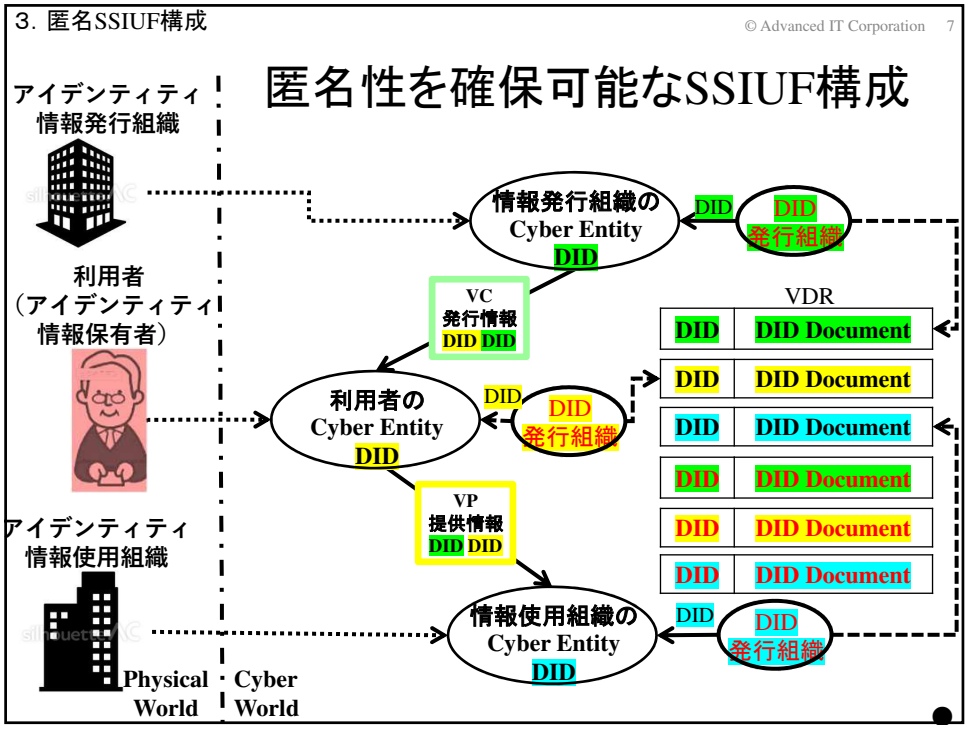
分散型ID（DID：Decentralized Identifier）

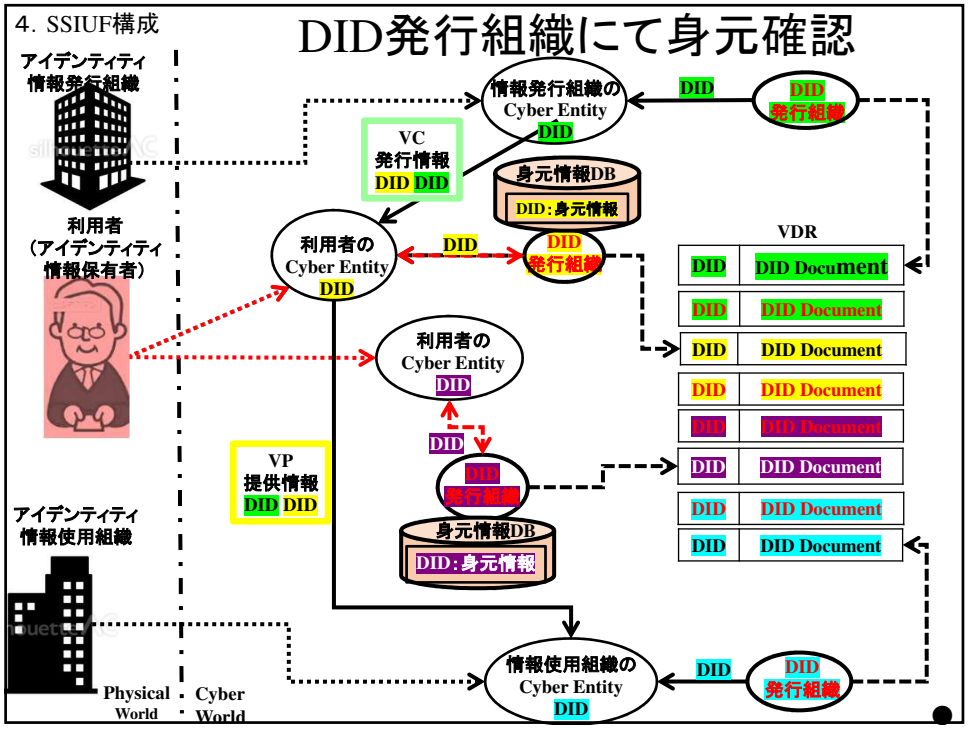


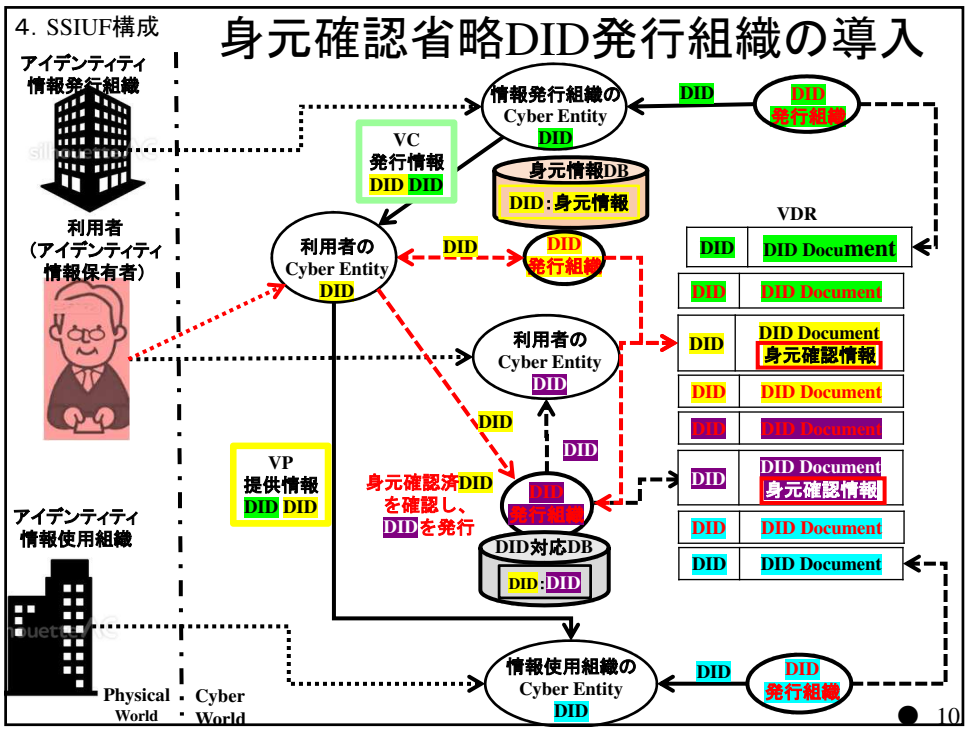
https://www.w3.org/TR/did-core/

VC/VPの構成・内容概要




3. 匿名SSIUF構成
© Advanced IT Corporation 7
匿名性を確保可能なSSIUF構成
アイデンティティ
情報発行組織
利用者
（アイデンティティ
情報保有者）
アイデンティティ
情報使用組織
情報発行組織の
Cyber Entity
DID
DID
DID
発行組織
VC
発行情報
DID DID
利用者の
Cyber Entity
DID
DID
DID
発行組織
VP
提供情報
DID DID
情報使用組織の
Cyber Entity
DID
DID
DID
発行組織
VDR
DID
DID Document
Physical
World
Cyber
World


4. SSIUF構成
DID発行組織にて身元確認
アイデンティティ
情報発行組織
利用者
（アイデンティティ
情報保有者）
アイデンティティ
情報使用組織
情報発行組織の
Cyber Entity
DID
DID
DID
発行組織
VC
発行情報
DID DID
身元情報DB
DID:身元情報
利用者の
Cyber Entity
DID
DID
DID
発行組織
利用者の
Cyber Entity
DID
VP
提供情報
DID DID
DID
DID
発行組織
身元情報DB
DID:身元情報
情報使用組織の
Cyber Entity
DID
DID
DID
発行組織
VDR
DID
DID Document
Physical
World
Cyber
World



4. SSIUF構成

利用者の匿名性と特定・追跡性の両立が可能なSSIUF構成の特徴

匿名性のみを確保可能なSSIUF構成へ次の機能を追加

①身元確認実施DID発行組織における
- a:身元の確認
- b:身元情報DBの管理
- c:DID Documentへ身元確認済情報の付加

②身元確認省略DID発行組織における
- a:身元確認済DIDの確認
- b:DID対応DBの管理
- c:DID Documentへ身元確認済情報の付加

4．SSIUF構成

SSIUFの構成方式に関する考察

①DID発行組織にて確実な身元確認を実施する方式

SSIUF利用者の確実な身元確認は必須の要件

インターネット上の共通の本人確認基盤（NAF）の利用が望ましい

NAF整備が進むまではSSIUF独自に身元確認機能も内蔵が必須

②身元確認を実施するDID発行組織を限定する方式

身元確認情報の維持・管理はDID発行組織のリスク

多くのDID発行組織へ身元情報の開示は利用者のリスク

DID発行組織および利用者のリスク軽減のための限定方式

③DID発行組織にて利用者の特定・追跡のための情報の管理方式

身元情報DBおよびDID対応DBは、利用者の特定・追跡には不可欠の情報

身元情報DBおよびDID対応DBは、DID発行には不要な情報のため

それぞれのDID発行組織の負担を減らす管理方式の可能性？

④DID Documentへ身元確認済情報を付加する方式

新たなDID発行依頼時に提示されたDIDが身元確認済かどうかの判断に必要

身元確認済情報からDID間の連結が推測されないような情報であることが必要

（NIST定義の身元確認方式の信頼性レベル等を想定）

4．SSIUF構成

利用者の確実な匿名性確保の観点からの考察

DID発行組織	追加機能	考察結果（実装・運用上の要件）
①身元確認実施	a：身元の確認	＊DID発行組織の身元確認プロセスでの、個人情報・プライバシー情報の確実な保護が必要
	b：身元情報DBの管理	＊DID発行組織では、個人情報である身元情報が漏洩しないよう、身元情報DBの安全な管理が必要
	c：DID Documentへ身元確認済情報の付加	＊DID Documentへ付加する身元確認済情報には利用者を推測できるような情報を含めないことが必要
②身元確認省略	a：身元確認済DIDの確認	＊DID Document内の身元確認済情報の確認のみでよい（特に留意すべき事項は無い）
	b：DID対応DBの管理	＊身元確認済DIDと新たに発行するDIDの対応情報の漏洩は、DIDに対応する利用者の特定不能性の大きなリスクとなるため、DID対応DBの安全な管理が必要
	c：DID Documentへ身元確認済情報の付加	＊DID Documentへ付加する身元確認済情報には、DID間の連結を推測できるような情報を含めないことが必要

➔上記のような要件に配慮したSSIUFの実装・運用により、
利用者の匿名性の確保が可能

4. SSIUF構成

利用者の確実な特定・追跡性確保の観点からの考察

DID発行組織	追加機能	考察結果（実装・運用上の要件）
①身元確認実施	a：身元の確認	＊DID発行組織が実施する身元確認および入手する身元情報の高い信頼性が必要
	b：身元情報DBの管理	＊DID発行組織では、身元情報DBの確実な維持が必要
	c：DID Documentへ身元確認済情報の付加	＊身元確認済であることが確認できる情報の付加であれば良い（特に留意すべき事項は無い）
②身元確認省略	a：身元確認済DIDの確認	＊身元確認済情報が付加されていることの確認（身元確認済情報の高い信頼性が必要）
	b：DID対応DBの管理	＊身元確認済DIDと新たに発行するDIDの対応情報の消失は、利用者の特定・追跡を不可能とするため、DID対応DBの確実な維持が必要
	c：DID Documentへ身元確認済情報の付加	＊身元確認済であることが確認できれば良い（特に留意すべき事項は無い）

➔上記のような要件に配慮したSSIUFの実装・運用により、
利用者の特定・追跡性の確保が可能

14

5. おわりに

まとめ

(1)個人の活動もインターネット上へ大きく移行し個人の活動のDXの進展が期待

ネット上での安心・安全なアイデンティティ情報の利活用基盤が重要

(2)DID/VC技術をベースにした、利用者の匿名性と特定・追跡性を両立可能な自己主権型アイデンティティ情報利活用基盤（SSIUF）を提案

(3)SSIUFの詳細仕様、NAFとの連携方式、グローバル化については、今後の検討予定

参考：EUでは27か国での利用を想定しているESSIFの構築を推進中
ESSIF：European self-sovereign identity framework

終

（ご清聴、ありがとうございました）