光輝会特別研究専門委員会

© Advanced IT Corporation 1

個人のネット活動を効果的に促進する環境
ー自己主権型アイデンティティ情報の利活用環境ー

2021年10月26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

1．必要性

© Advanced IT Corporation 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）

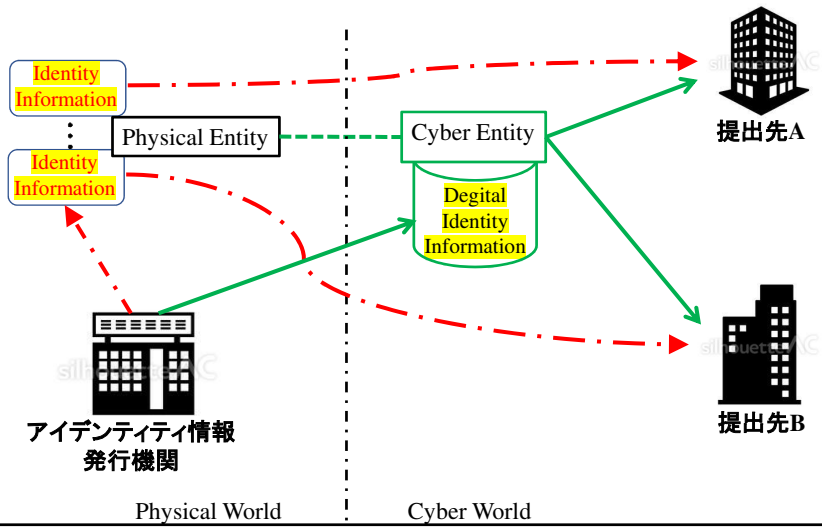
（4）エンティティの各種サービス利用情報等（利用属性）

（5）エンティティの信用、評判等（関係属性）

1．必要性

© Advanced IT Corporation 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

© Advanced IT Corporation 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。

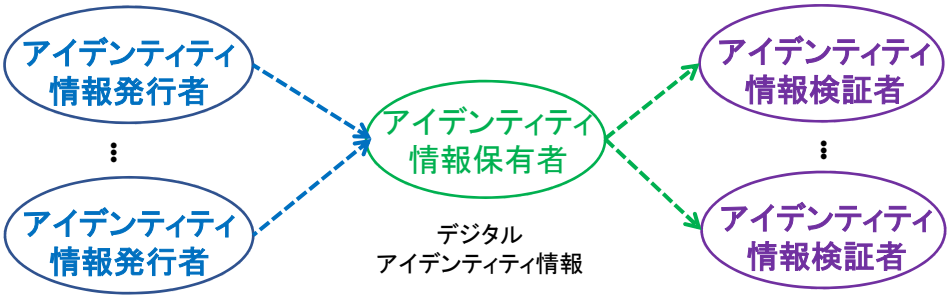
＊Physical Worldで個人の活動で利用されていた様々の書類も
Cyber World内での送受へと移行、様々のアイデンティティ情報も
ネット経由で迅速に効率的に送受信される時代へ移行するのは必至

➔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

1．必要性

© Advanced IT Corporation

デジタルアイデンティティ情報の利活用を支える基盤の構成要素



基本要件

①個人情報・プライバシー情報の保護

②アイデンティティ情報保有者の自己制御性（自己主権性）

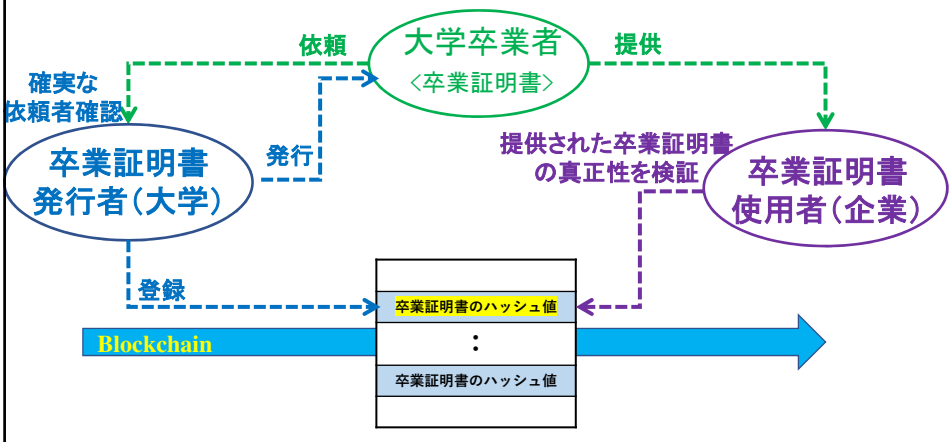
③効率的なアイデンティティ情報発行・管理・検証の仕組み

2．先行事例

© Advanced IT Corporation

デジタルアイデンティティ情報活用への動き

Blockcertsによるデジタル卒業証明書活用の仕組み（2016年～）



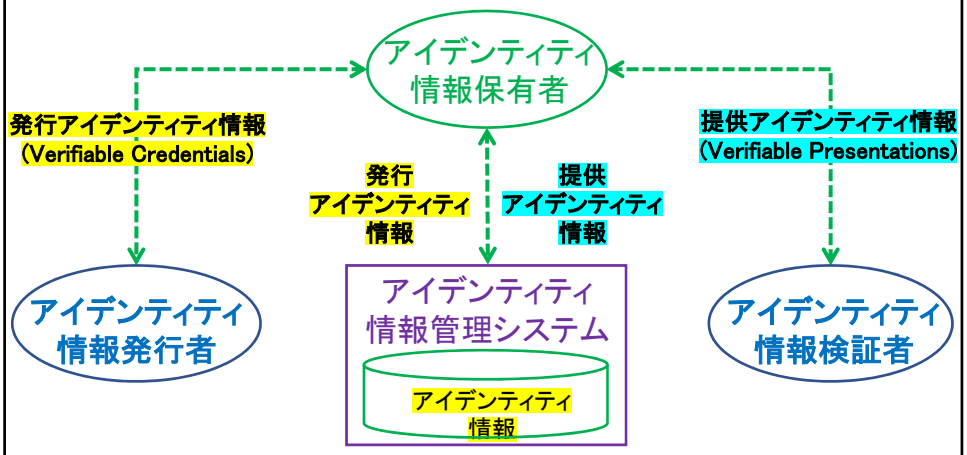
Blockcerts：MIT Media Lab を中心に Learning Machine 社と開発された
ブロックチェーン基盤の卒業証明書を管理するプラットフォーム

参考資料：https://decentralized-id.com/web-standards/blockcerts/

© Advanced IT Corporation

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



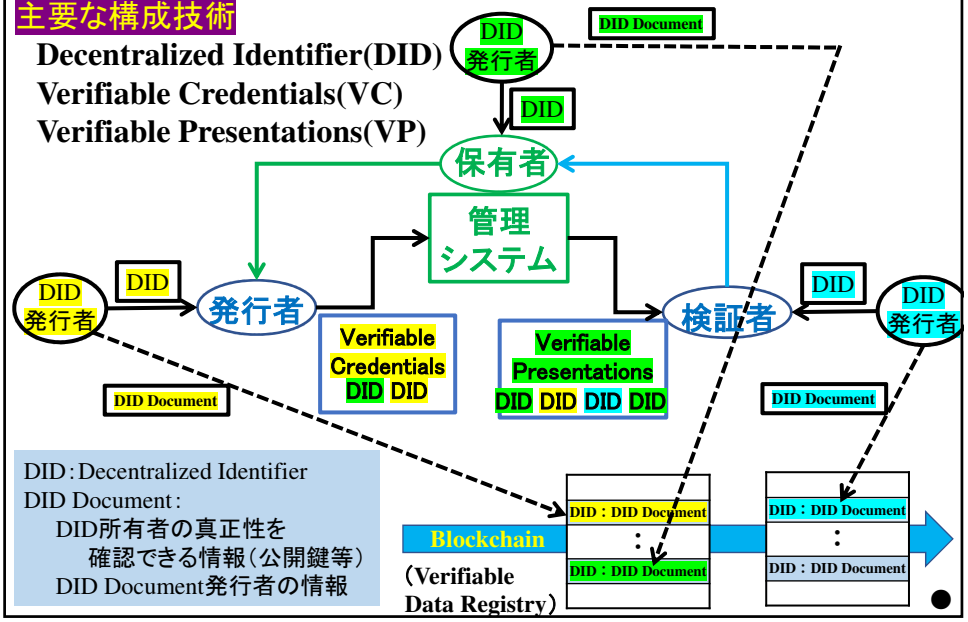
自己主権（セルフソブリン）型とは、情報保有者による
アイデンティティ情報の確実な利活用制御が可能なこと

© Advanced IT Corporation

SSIUFの構成・仕組み例

主要な構成技術

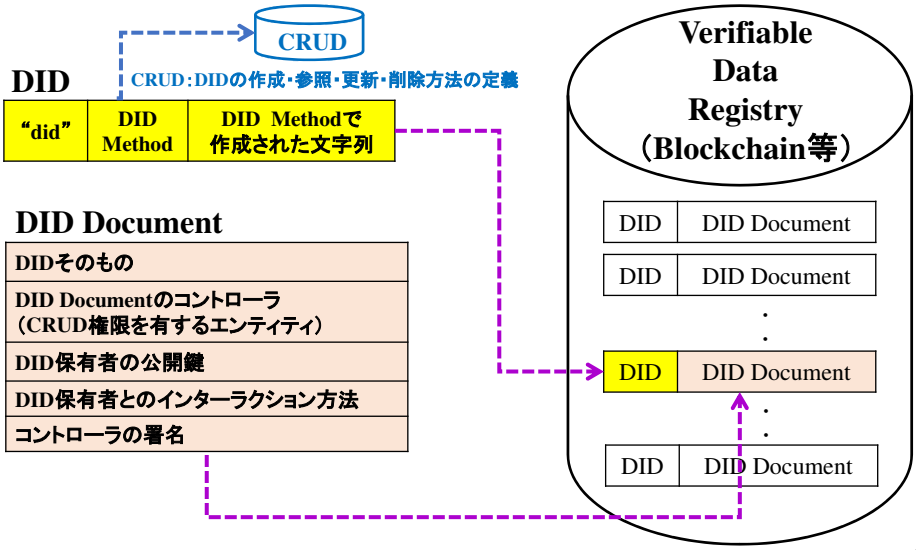
Decentralized Identifier(DID)
Verifiable Credentials(VC)
Verifiable Presentations(VP)



DID：Decentralized Identifier
DID Document：
DID所有者の真正性を
確認できる情報（公開鍵等）
DID Document発行者の情報

© Advanced IT Corporation

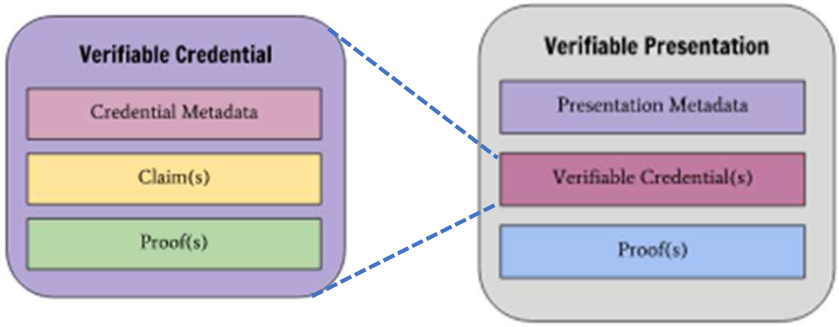
DID（Decentralized Identifier）



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

© Advanced IT Corporation

Verifiable Credentials（VC）/Verifiable Presentations（VP）



Credential Metadata:
このCredentialの情報

Claim(s):
アイデンティティ情報本体
アイデンティティ情報の保有者を示すDIDを含む

Proof(s):
発行者および真正性を示す情報
発行者のDIDに対応する
秘密鍵による署名

Presentation Metadata:
このPresentation情報

Verifiable Credential(s):
発行者が発行した情報
前頁の内容をそのまま

Proof(s):
提供者および真正性を示す情報
提供者のDIDに対応する
秘密鍵による署名
提供先の情報

参考資料：https://www.w3.org/TR/vc-data-model/

© Advanced IT Corporation

VPによる提供情報の最小化のために
Selective Disclosure/Predicate Proofs

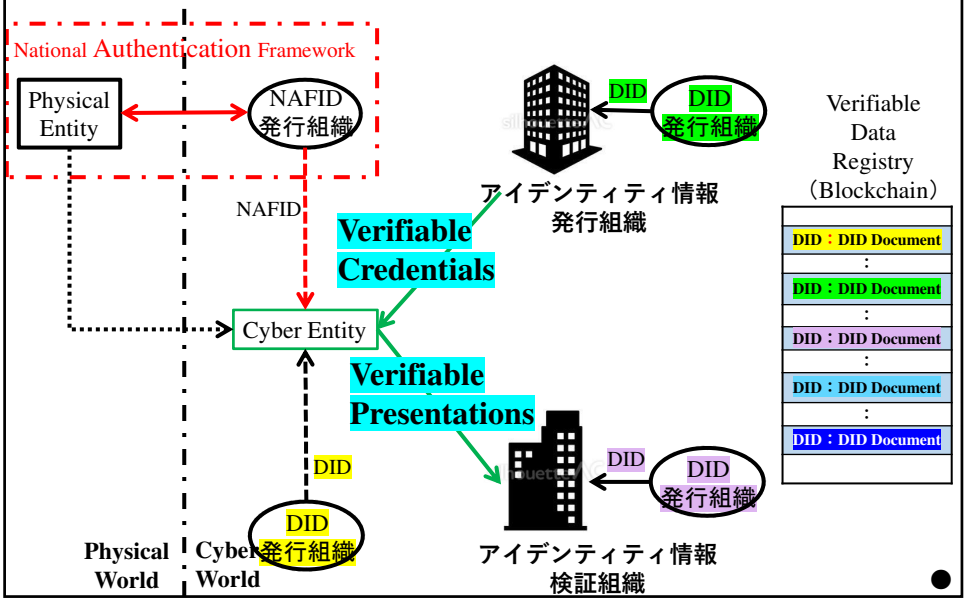
Selective Disclosure
VPによる、VCの一部の属性のみの提供（開示）、の難しさ
VC:[{名前、住所、性別、生年月日}，発行者の署名]
＊名前、住所のみを提供したい場合（他の属性は秘匿）
＊VCの信頼性・検証可能性の維持

Predicate Proofs
VPによる、属性そのものの提供ではない、述語証明の難しさ
VC:[{名前、住所、性別、生年月日}，発行者の署名]
＊年齢のみを提供したい場合（生年月日も含め秘匿）
＊VCの信頼性・検証可能性の維持

活用が検討されている技術
Camenisch Lysyanskaya signatures/Zero Knowledge Proof
BBS+ signatures/Zero Knowledge Proof
＜Zero Knowledge Proofを利用した
Selective DisclosureおよびPredicate Proofsに対応可能な技術＞

© Advanced IT Corporation

SSIUFにおけるDID/VC・VP活用イメージ
匿名性と特定・追跡性の両立

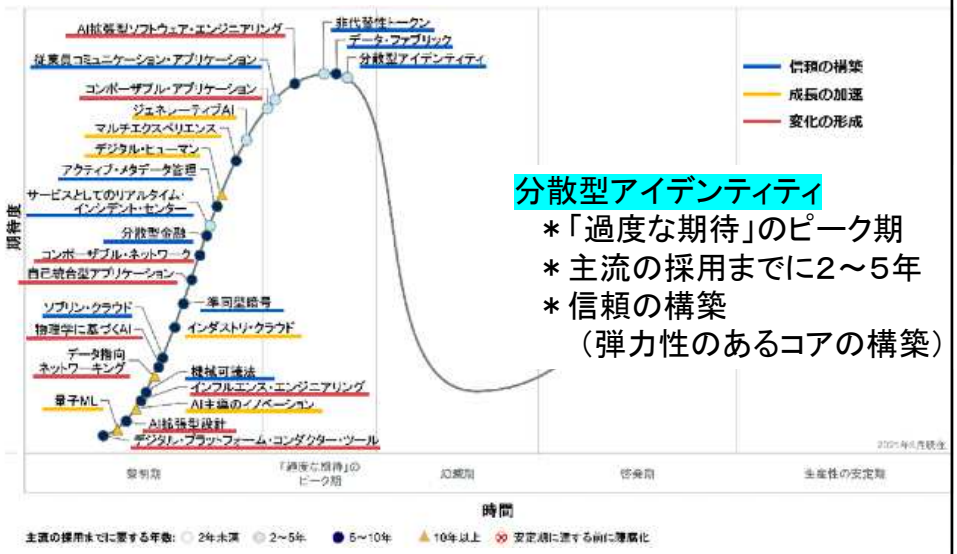


4. おわりに

© Advanced IT Corporation 13

「先進技術におけるハイプ・サイクル2021年版」

（12 August 2021　Gartner）



分散型アイデンティティ

＊「過度な期待」のピーク期

＊主流の採用までに2～5年

＊信頼の構築

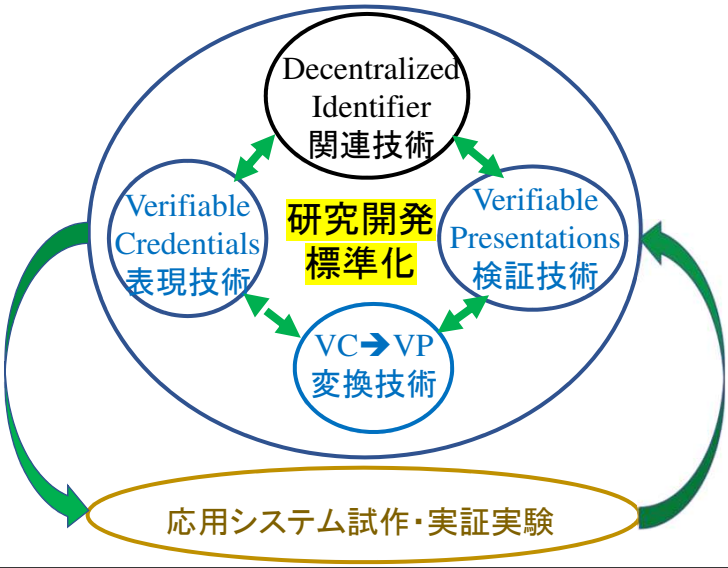
（弾力性のあるコアの構築）

参考資料：https://aty800.com/highest-goal/it-impact/hype-cycle-2021.html

4. おわりに

© Advanced IT Corporation 14

自己主権型アイデンティティ情報利活用基盤社会実装に向けた今後の動向



終

（ご清聴、ありがとうございました。）

個人のネット活動を効果的に促進する環境
ー自己主権型アイデンティティ情報の利活用環境ー