

次世代アイデンティティ基盤実証実験 (分散型識別子技術及び資格証明書技術とその応用)

鈴木茂哉

慶應義塾大学大学院政策・メディア研究科 特任教授
慶應義塾大学SFC研究所ブロックチェーン・ラボ 副所長（技術統括）

@ 大学教育における DX オンライン・シンポジウム - 2021/1/13



本日の話題

- 大学におけるデジタルトランスフォーメーションとデジタルアイデンティティ
- 分散型識別子技術 及び 資格証明書技術について
 - Verifiable Credentials (VCs) - (検証可能な)資格証明書技術
 - Decentralized Identifiers (DIDs) - 分散型識別子(アイデンティティ)技術
- KBCLディスカッションペーパーとグローバルデジタルアイデンティティ
- 次世代アイデンティティ基盤実証実験 (DID PoC) について

大学とデジタルトランスフォーメーション



デジタルトランスフォーメーション (定義)

- ・ 初出: エリック・ストルターマンによる定義 (2004) [1]

デジタルトランスフォーメーションの用語の初出は、2004年にスウェーデンのウメオ大学教授のエリック・ストルターマンが提唱した。ストルターマンは「ITの浸透が、人々の生活をあらゆる面でより良い方向に変化させる」と定義し、下記の特徴を提示している。

- ・ デジタルトランスフォーメーションにより、情報技術と現実が徐々に融合して結びついていく変化が起こる。
- ・ デジタルオブジェクトが物理的現実の基本的な素材になる。例えば、設計されたオブジェクトが、人間が自分の環境や行動の変化についてネットワークを介して知らせる能力を持つ。
- ・ 固有の課題として、今日の情報システム研究者が、より本質的な情報技術研究のためのアプローチ、方法、技術を開発する必要がある。なお、ストルターマンの提唱する概念を示した論文は「本論文は、よりよい生活のために技術を批判的に調べることができる研究の出発点として、適切な研究ポジションを確立する試みである」とあることから、研究へのアプローチ・方法論を述べた内容となっている。

- ・ ガートナー (2014)、IDC Japan (2016)の定義の大意は、**【情報技術を用い】
【ビジネスと顧客、ネットとリアル】で【ビジネスを変革・創出】**
- ・ 経済産業省の報告書で用いられているのはIDC Japanの定義 [2]

[1] <https://ja.wikipedia.org/wiki/デジタルトランスフォーメーション>

[2] DXレポート ～ITシステム「2025年の崖」克服とDXの本格的な展開～, 経済産業省, 2018/9/7

https://www.meti.go.jp/shingikai/mono_info_service/digital_transformation/0180907_report.html

ここまでの慶応の【IT化】

- 学内の【IT化】
 - 共通基盤の整備を含め、進行している
 - シングルサインオンによるサービス
- 学外とのやりとりの【IT化】
 - 大学や研究機関の間で緩やかに進行
 - 研究に関する情報基盤の共有
 - 論文の識別子(DOI)、著者の識別子(ORCID等)などといった、対象に対する識別子(ID)の整備や割り振り

これから: デジタルトランスフォーメーション

- これからの大学にとっての【新しいビジネス】は？
→ 外部との、さまざまな形での情報共有

既存の大学における外部への情報提供

- 学生に紐付けられたもの
 - 証明書
 - 学生証
 - 卒業（学位）証明書
 - 成績証明書
- 法人としての運営に関連して
 - 職員証
 - 在籍証明書
 - 給与関係（源泉徴収票, etc.）
 - 決算関係

デジタルトランスフォーメーションにおける課題

- 狭義のデジタルトランスフォーメーション(従来ワークフローのIT化)を礎に、
広義のデジタルトランスフォーメーションへ
- 狭義、広義双方において、組織を跨ぐ情報の信頼性確保が要になる
→ 例: 文書が改竄されていないことの確認に加え、**発行者の確認**が必要
- 組織を跨ぐ情報の信頼性確保には、相互運用可能なデジタルアイデンティティ
基盤が必要

Verifiable Credentials (VC) と Decentralized Identifiers (DID)

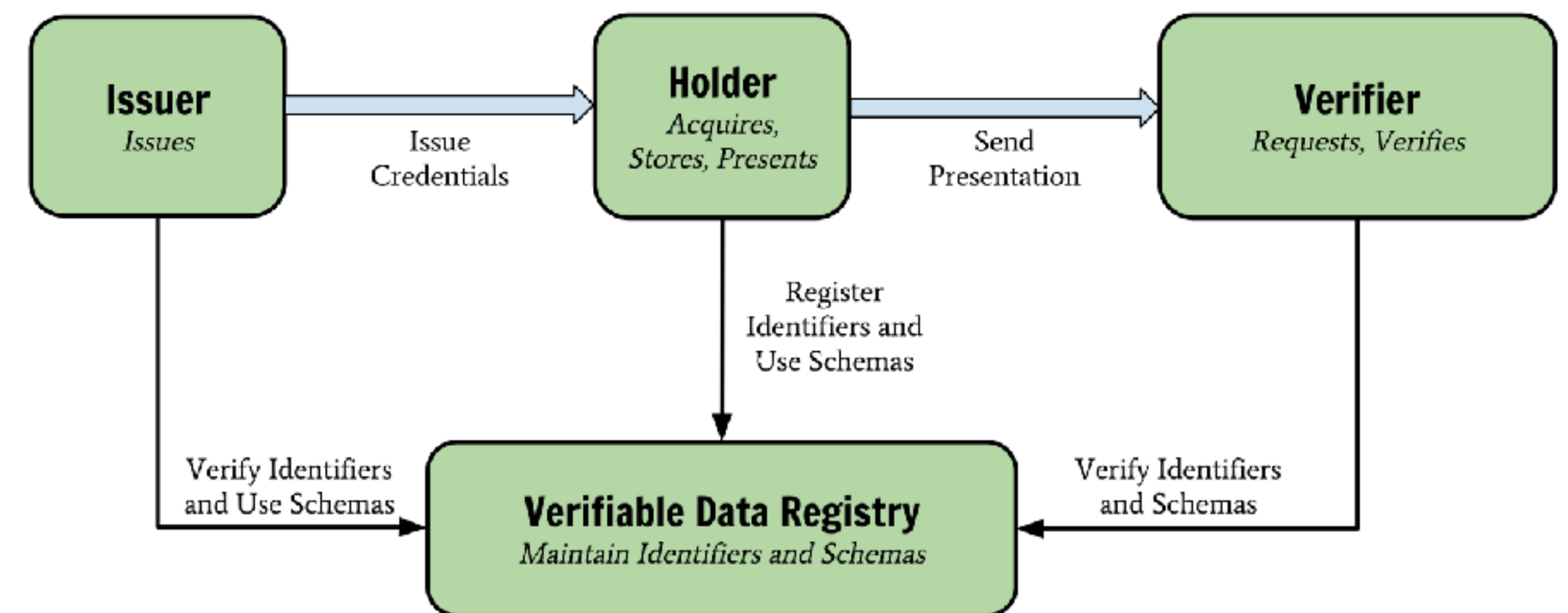


Verifiable Credential - 検証可能な資格証明書

- さまざまな「証明書」のデジタル化手段
- デジタル署名技術を用いた【発行者】(Issuer)により【対象者】(Subject)が特定の条件を満たしている事を【保持者】(Holder) が示すことができる
- W3C で標準化されている [1]

- Subject / Issuer / Holder を示すための手段が必要

→ デジタルアイデンティティが必須

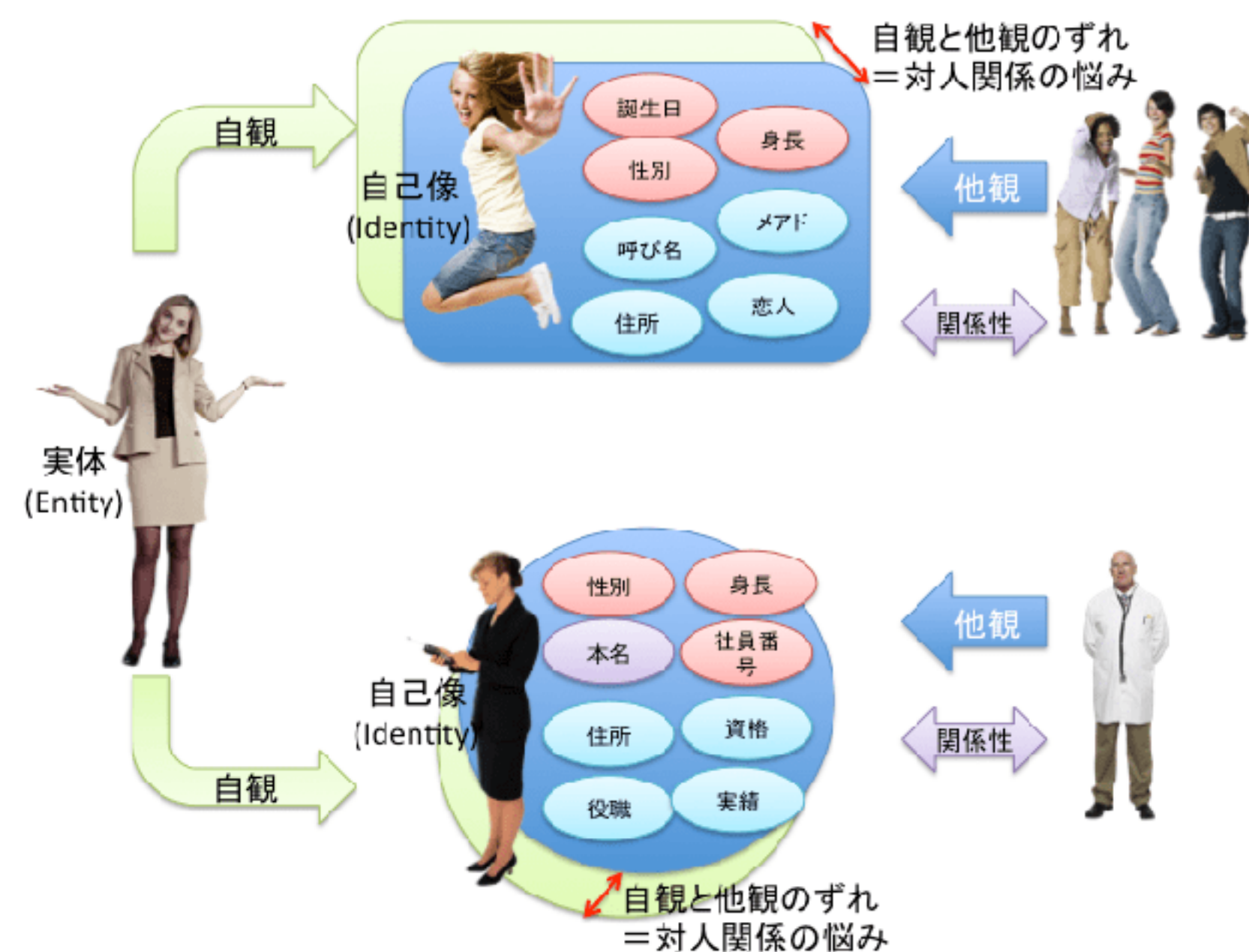


デジタルアイデンティティ

- 今回のプレゼンテーションに見合う形で、丸めて表現すると:
「ある人(= 実体: 一つ)に対応するサイバー空間中で識別可能な自己像(複数可)」

- 実体と自己像、自己像に対する自観、他人からみた他観や関係性など、厳密に説明するのは難しい。
[1]参照のこと (右図も同文書から)

- ISOの定義では
「実体を構成する属性の集合」
(ISO/IEC 24760-1)



グローバルデジタルアイデンティティ

- ・ 「組織間で相互運用性のある、デジタルアイデンティティ基盤が必要」
 - ➡ インターネット上で単一の識別子(identifier)を表現し、かつ、紐付いたアイデンティティを統一的に利用・管理する手段が必要である
 - ➡ 「グローバルデジタルアイデンティティ」
- ・ **グローバル**とは、インターネットと同様に、インターネット上のどこでも用いる事ができること
 - ・ 特定のサービス、組織、国などでサイロ化されていない
- ・ グローバルデジタルアイデンティティの一つの実現形態が「自己主権型アイデンティティ (Self-Sovereign Identity)」である

自己主権型アイデンティティ (Self-Sovereign Identity)



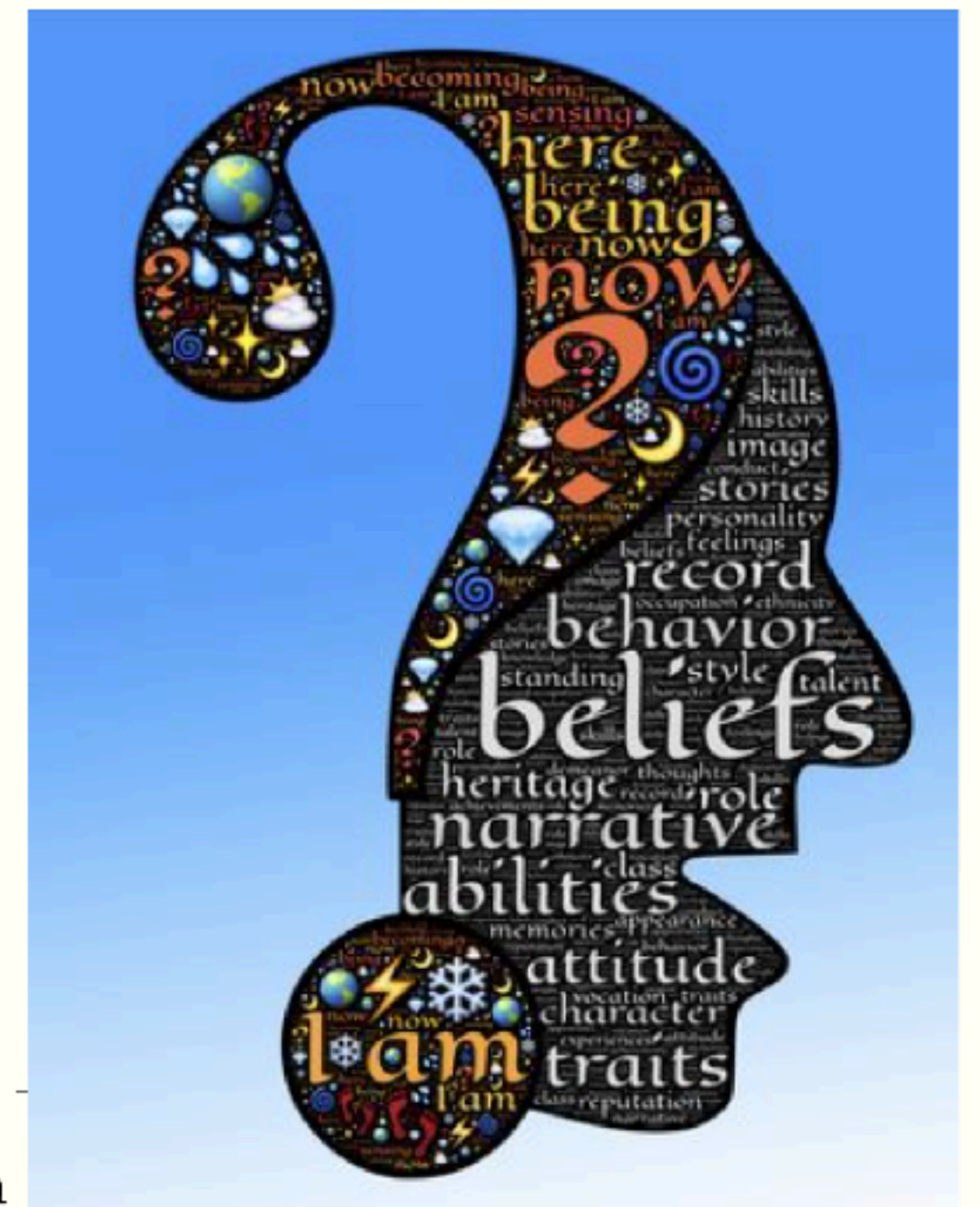
The Path to Self-Sovereign Identity

- ・ 「自己主権型アイデンティティへ至る道筋」
- ・ 自己主権型アイデンティティ
(Self-Sovereign Identity - SSI)の
生みの親の一人とも言える
Christopher Allenによる、SSIに至る
までの過程とSSIの定義、SSIの10個の
基本原則についての議論

The Path to Self-Sovereign Identity

April 25 2016 - 4200 Words
by Christopher Allen

Today I head out to a month-long series of events associated with identity: I'm starting with the 22st (!) Internet Identity Workshop next week; then I'm speaking at the blockchain conference Consensus about identity; next I am part of the team putting together the first ID2020 Summit on Digital Identity at the United Nations; and finally I'm hosting the second #RebootingWebOfTrust design workshop on decentralized identity.



Self-Sovereign Identity - Ideology & Architecture

- Christopher Allenによる、SSIの意義についてのプレゼンテーション
 - SSIの意義と背景について理解するために大いに参考になる

注: 本プレゼンテーションの一部は、このスライドからお借りしています



Self-Sovereign Identity Ideology & Architecture



Christopher Allen — Decentralized Identity & Blockchain Architect,
Co-Chair W3C Credentials Community Group



CC BY-SA 4.0



自己主権型IDへ至る道筋

- ・ **フェーズ 1：中央集権型アイデンティティ**

(単一の、あるいは、階層化された管理権限域によるコントロール)

- ・ ドメイン名システム(DNS)、公開鍵認証局(CA)

- ・ **フェーズ 2：フェデレーションされたアイデンティティ**

(複数の管理権限域間の連合によるコントロール)

- ・ Liberty Alliance, Microsoft Passport

- ・ **フェーズ 3：ユーザ中心のアイデンティティ**

(複数の権限域にまたがる個人または管理者によるコントロール)

- ・ Internet Identity Workshop コミュニティなどを起点とした、様々な標準: OpenID (2005), OpenID 2.0 (2006), Open ID Connect (2014), OAuth (2010), FIDO (2013)

- ・ **フェーズ 4：自己主権型アイデンティティ**

(複数の権限域にまたって個人がコントロール)

- ・ Decentralized Identifiers (DIDs)



自己主権型アイデンティティの基本原則10

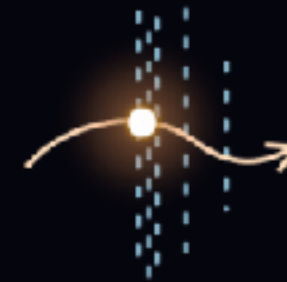
10 PRINCIPLES OF SELF-SOVEREIGN IDENTITY



existence



control



access



transparency



persistence



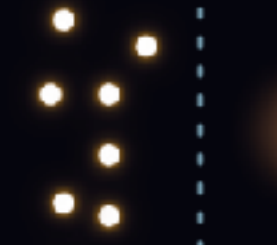
portability



interoperability



consent



minimization



protection

10 principles of SSI by Christopher Allen • Visual design by Jolocom



<https://jolocom.io/blog/a-universal-identity-layer-we-can-only-build-together/>

自己主権型アイデンティティの基本原則10[1] (鈴木による仮訳)



- **実在:** ユーザは独立した存在である。決してデジタルだけでは存在しえない
- **コントロール:** ユーザーは、自分のアイデンティティ、秘匿性あるいは顕名性を望みに応じてコントロールできなければならない
- **アクセス:** ユーザは自身のデータへのアクセスができなければならない — 門番は存在せず、隠されるものが一切ない
- **透明性:** システムとアルゴリズムはオープンかつ透明性が確保されなければならない
- **永続性:** アイデンティティはユーザーが望の望みに応じ長期にわたり用いることができなければならない
- **可搬性:** アイデンティティに関する情報とサービスはユーザによって移動可能でなければならない
- **相互接続性:** アイデンティティは、越境を許す等、可能な限り広く利用できるようにすべきである
- **同意の自由:** ユーザーは、自分の個人情報がどのように使用されるかの同意について自由であるべきである
- **最小化:** アイデンティティについての主張の開示は最小にとどめるべきである
- **保護:** 個々のユーザの権利は、強権を持つ者から保護されなければならない

[1] <https://ssimeetup.org/self-sovereign-identity-why-we-here-christopher-allen-webinar-51/>

自己主権IDの基本原則 (Sovrin Foundationによる)

- 1. 代理証明:** 自己主権IDのエコシステムは実在する存在に対し人間的、法的、自然的、物理的、もしくはデジタルによって 実現するデジタル上での識別子の数で証明できる環境を提供します。
- 2. 相互互換性:** 自己主権IDのエコシステムは実在する存在に対してデジタルIDデータを証明、交換、安全、保護、そしてデータ互換性の確認を前提としてオープンで公共な手数料が無い環境を提供します。
- 3. 分散性:** 自己主権IDのエコシステムは中央集権型のシステムに依存する事なく、管理、もしくは実在する存在の確認を デジタルIDに記録されたデータを下に行う事ができる環境を提供します。
- 4. 管理とエージェント:** 自己主権IDのエコシステムは自然、人間、もしくは法的なアイデンティティと関連がある（アイデンティティ 所有者） 実在する存在がデジタルIDデータと選択によって個人や組織、デバイスやソフトウェアなどのエージェントの採用、データ保護管理を実施できる環境を提供します。
- 5. 参加:** 自己主権IDのエコシステムはアイデンティティ所有者の参加を必要としない環境を提供します。
- 6. 公正と包括:** 自己主権IDのエコシステムはガバナンス設計に置いてアイデンティティ所有者によって差別、排除を行わない環境を提供します。
- 7. 利便性、アクセス性、一貫性:** 自己主権IDのエコシステムは利便性とエージェントのアクセス性を最大化し、他アイデンティティ所有者の自己主権IDとの一貫した利用者体験を実現できる環境を提供します。
- 8. 可搬性:** 自己主権IDのエコシステムはアイデンティティ所有者によるアイデンティティの携帯、もしくはエージェント、システムにより選択されたアイデンティティデータのコピーの移行を制限する事はありません。
- 9. 安全性:** 自己主権IDのエコシステムはアイデンティティ所有者が自身のデジタルIDデータを暗号鍵や取引のエンドツーエンド暗号化を通じて安全に管理できる環境を提供します。
- 10. 確認と認証:** 自己主権IDのエコシステムはアイデンティティ所有者がデジタルIDデータを下に、認証に必要な確認証明を発行できる環境を提供します。
- 11. プライバシーと公開の最小化:** 自己主権IDのエコシステムはアイデンティティ所有者がデジタルIDのプライバシーと取引に必要なデジタルIDデータの最小化を実現できる環境を提供します。
- 12. 透明性:** 自己主権IDのエコシステムはアイデンティティ所有者と全てのステークホルダーが簡易にアクセス、情報の確認ができ、インセンティブやルール、ポリシー、アルゴリズムなどエコシステム内で機能する内容を知る事ができる環境を提供します。

Decentralized Identifier (DIDs) v1.0 (WD)

- DID = Decentralized Identifier @ World Wide Web Consortium (W3C)
[注: Decentralized Identity Foundation (DIF) という関連団体がある]
- 自己主権型の識別子にまつわるデータモデル標準
 - 周辺技術との組み合わせで自己主権型のアイデンティティを実現できる
- 現在 Working Draft(WD)
- 近々 Candidate Recommendation (CR) にすべく、精力的に作業が行われている

W3C Working Draft

Decentralized Identifiers (DIDs) v1.0

Core architecture, data model, and representations

W3C Working Draft 10 January 2021

This version:
<https://www.w3.org/TR/2021/WD-did-core-20210110/>

Latest published version:
<https://www.w3.org/TR/did-core/>

Latest editor's draft:
<https://w3c.github.io/did-core/>

Previous version:
<https://www.w3.org/TR/2020/WD-did-core-20201108/>

ReSpec

W3C

<https://w3c.github.io/did-core/>

DID

- DID グローバルにユニークかつ永続性のある識別子で、暗号技術を用いて生成または登録されることにより、中央に登録機関を必要としない。
- DIDは、複数の方式(メソッド)で実装され、メソッドにより、ブロックチェーン技術を下支えにするものもある（必ず、そのように実装されているとは限らない）
- DID document は DIDで示される主体

EXAMPLE 1: A simple example of a decentralized identifier (DID)

`did:example:123456789abcdefghi`

メソッド名 メソッド固有の情報

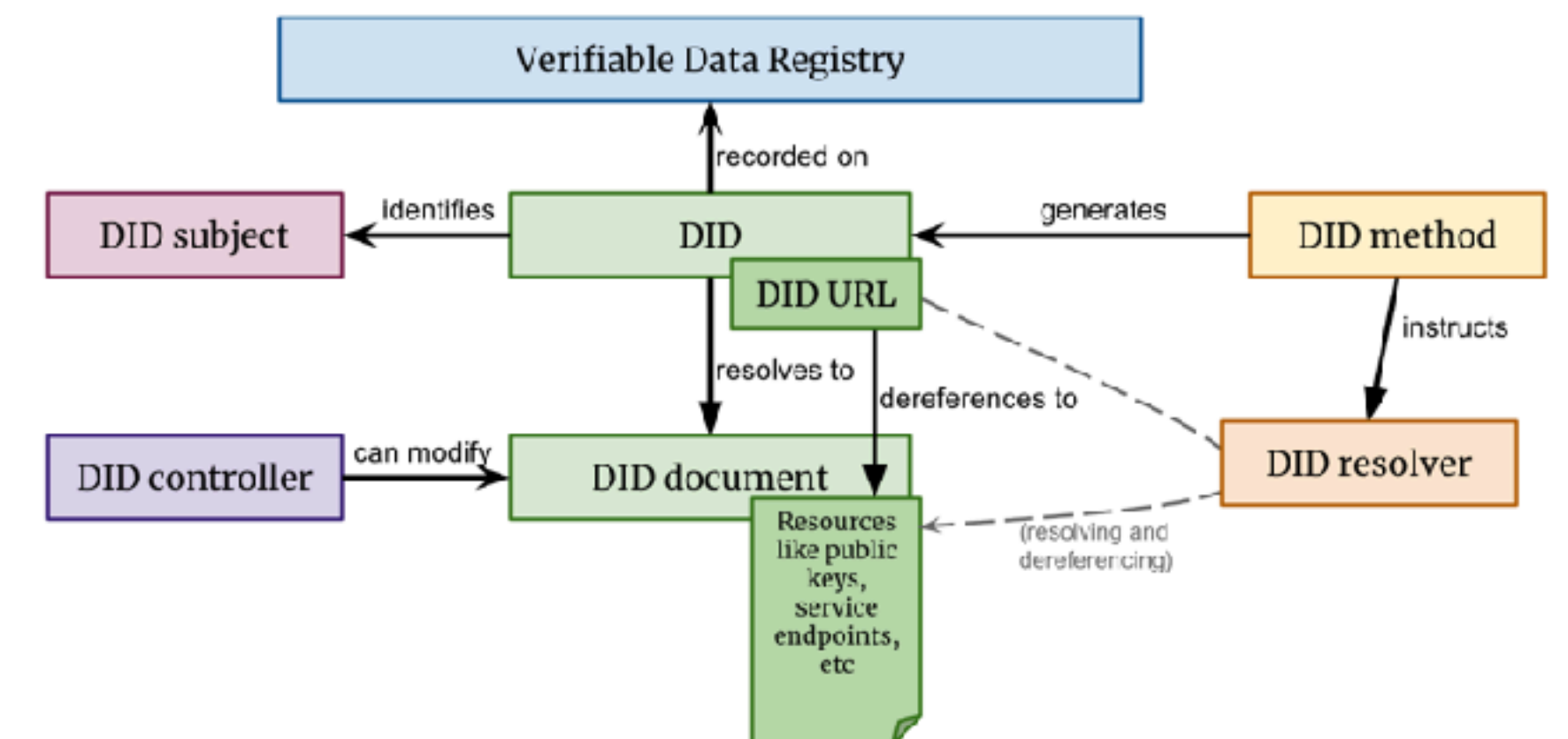


Figure 1 The basic components of DID architecture.

DID document

- DID document は DIDで示される主体を表現するのに必要なデータ（やメカニズムが記載されたデータの集まりである
- データとしては、公開鍵、特定のブロックチェーン中の位置を示す情報などが例としてあげられる

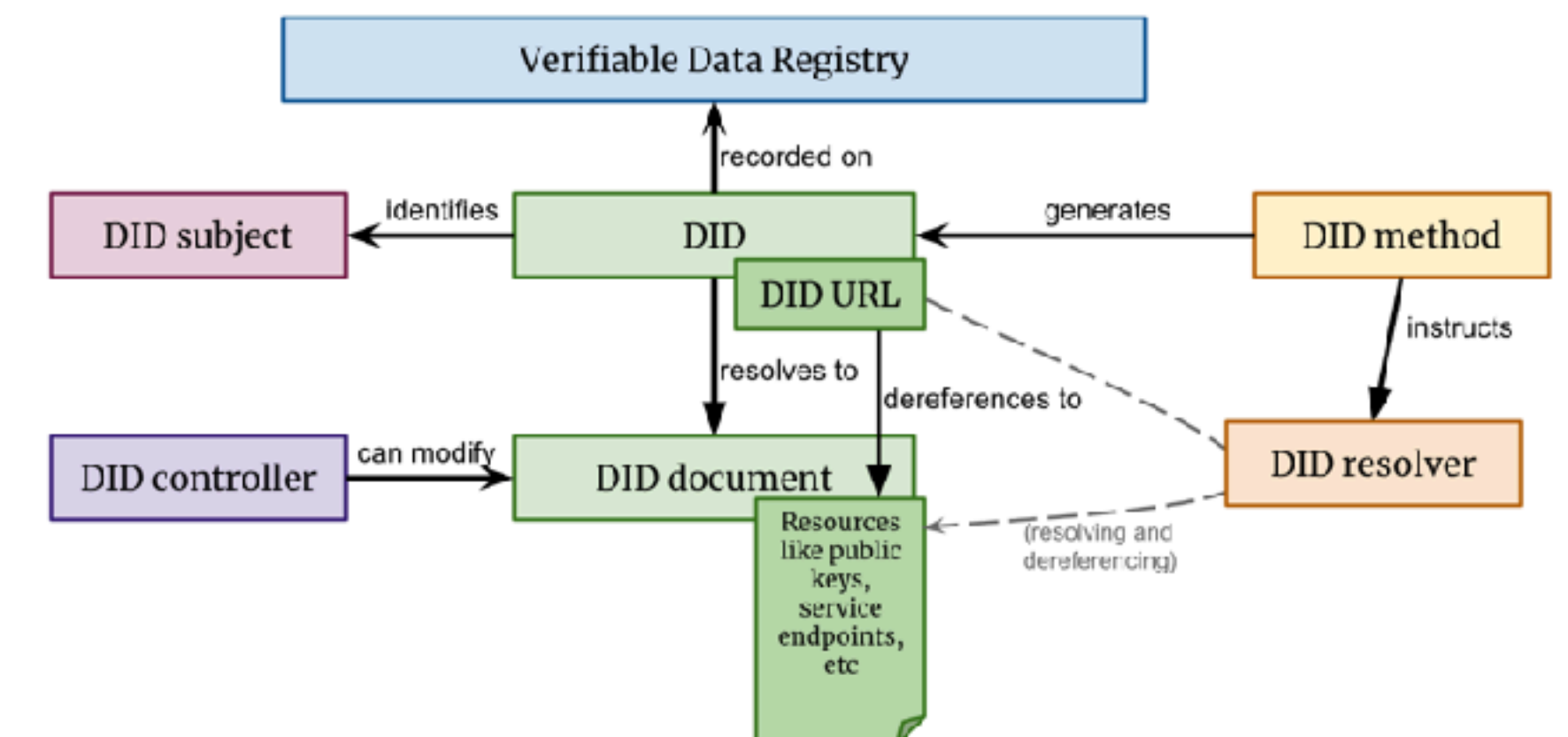


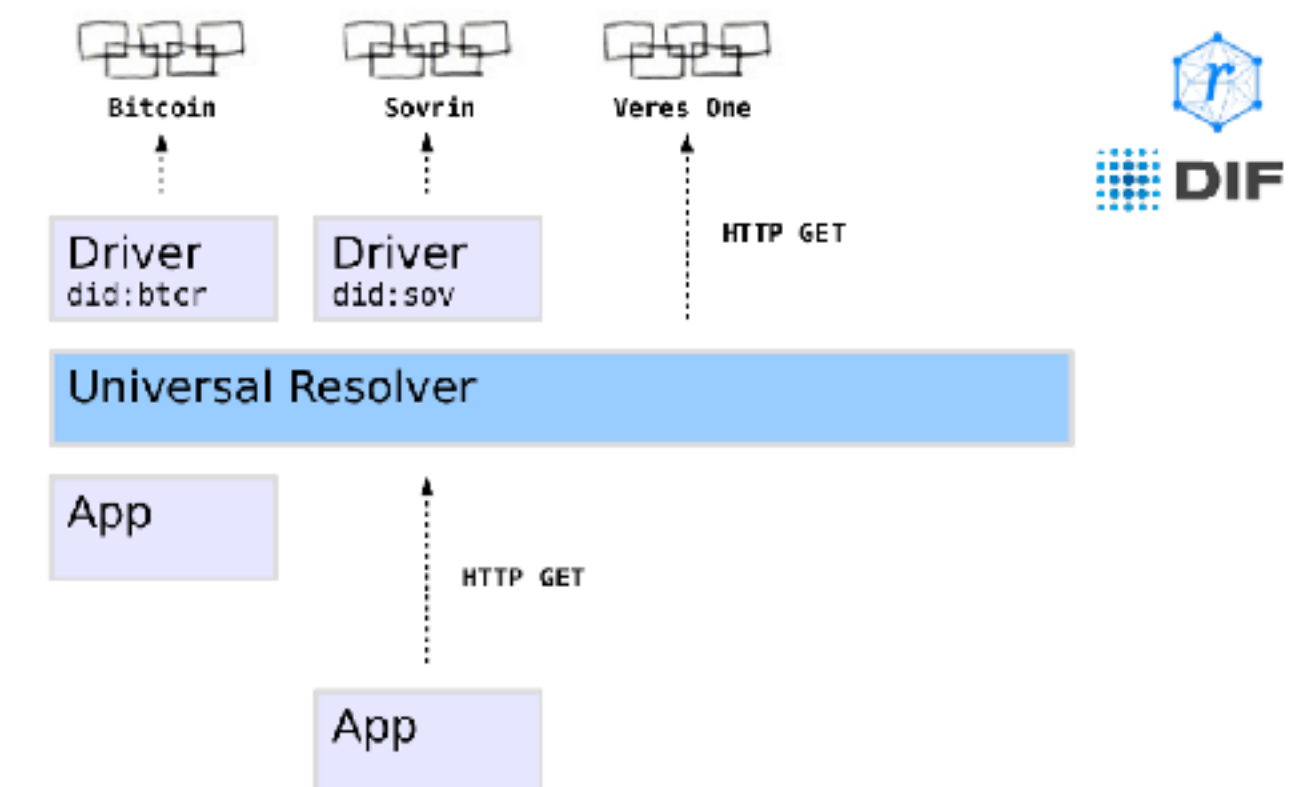
Figure 1 The basic components of DID architecture.

DID URL

- DIDを起点としたリソースロケータ
- DIDを含み、URLのようにパス、クエリ、フラグメント等の要素をもち、DIDで示される対象（リソース）に含まれるであろう要素を示す
- DID documentの中では、フラグメントを用い、DID document中の公開鍵を相対的に指定するために使われる（#key-1）

Universal Resolver (1/3)

- 複数のメソッド用のドライバが組み込まれ、ドライバを使い分けることで、DID から DID document および関係メタデータを取得できるサーバ実装 [1]
- DIFで開発され、二つのサーバインスタンスが運用中[2] **(実運用向けでは無い)**



[1] A Universal Resolver for self-sovereign identifiers



<https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c>

[2] The Universal Resolver Infrastructure

<https://medium.com/decentralized-identity/the-universal-resolver-infrastructure-395281d2b540>

Universal Resolver (2/3)

- ブラウザで確認可能



[See configuration](#)

SUPPORTED METHODS:

did:btcr	did:web	did:github	did:kilt	did:sirius	did:bid	did:vaa
did:sov	did:jolo	did:stack	did:evan	did:mpg	did:schema	+ Add your driver?
did:v1	did:erc725	did:hcr	did:echo	did:io	did:ion	
did:key	did:ipid	did:ccp	did:factom	did:trust	did:gatc	
did:ethr	did:elem	did:work	did:dock	did:bba	did:ace	
did:nac	did:neoid	did:ont	did:abt	did:cy	did:icon	

did-url

did:sov:WRfXPg8dantKVubE3HX8pw

Resolve

Clear

Examples

RESULT

DID DOCUMENT

RESOLUTION METADATA

DOCUMENT METADATA

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:sov:WRfXPg8dantKVubE3HX8pw",
  "verificationMethod": {
    "type": "Ed25519VerificationKey2018",
    "id": "did:sov:WRfXPg8dantKVubE3HX8pw#key-1",
    "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXnqPV"
  },
  "authentication": {
    "type": "Ed25519SignatureAuthentication2018",
    "verificationMethod": "did:sov:WRfXPg8dantKVubE3HX8pw#key-1"
  },
  "service": [
    {
      "type": "agent",
      "serviceEndpoint": "https://agents.danubecLOUDS.com/agent/WRfXPg8dantKVubE3HX8pw"
    },
    {
      "type": "xdi",
      "serviceEndpoint": "https://xdi03-at.danubecLOUDS.com/cl/+:did:sov:WRfXPg8dantKVubE3HX8pw"
    }
  ]
}
```

Universal Resolver (1 / 3)

```
% curl -sX GET https://resolver.identity.foundation/1.0/identifiers/did:sov:WRfXPg8dantKVubE3HX8pw | jsonpp
```

```
{
  "didDocument": {
    "@context": "https://www.w3.org/ns/did/v1",
    "id": "did:sov:WRfXPg8dantKVubE3HX8pw",
    "verificationMethod": {
      "type": "Ed25519VerificationKey2018",
      "id": "did:sov:WRfXPg8dantKVubE3HX8pw#key-1",
      "publicKeyBase58": "H3C2AVvLMv6gmMnam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
    },
    "authentication": {
      "type": "Ed25519SignatureAuthentication2018",
      "verificationMethod": "did:sov:WRfXPg8dantKVubE3HX8pw#key-1"
    },
    "service": [
      {
        "type": "agent",
        "serviceEndpoint": "https://agents.danubeclouds.com/agent/WRfXPg8dantKVubE3HX8pw"
      },
      {
        "type": "xdi",
        "serviceEndpoint": "https://xdi03-at.danubeclouds.com/cl/+!:did:sov:WRfXPg8dantKVubE3HX8pw"
      }
    ]
  },
  "authentication": {
    "type": "Ed25519SignatureAuthentication2018",
    "verificationMethod": "did:sov:WRfXPg8dantKVubE3HX8pw#key-1"
  },
  "service": [
    {
      "type": "agent",
      "serviceEndpoint": "https://agents.danubeclouds.com/agent/WRfXPg8dantKVubE3HX8pw"
    },
    {
      "type": "xdi",
      "serviceEndpoint": "https://xdi03-at.danubeclouds.com/cl/+!:did:sov:WRfXPg8dantKVubE3HX8pw"
    }
  ]
}
```

— 以下略 —

プライバシー重視の仕様策定

- DID は単一のユーザが多数用い、自由に使い分けができるようになっている
 - DID は、DID を伝える対象、組み合わせるVC等に応じて、対象ごとに都度作成 (pair-wise) で使われることが前提となっている
- DID および DID document に含まれる情報に、個人識別情報(PII)を含めるだけでなく、個人識別に繋がる可能性のある情報が含まれないように、注意深く検討、仕様化（必要に応じた注意書き）などが行われている

| Verifiable Credentials

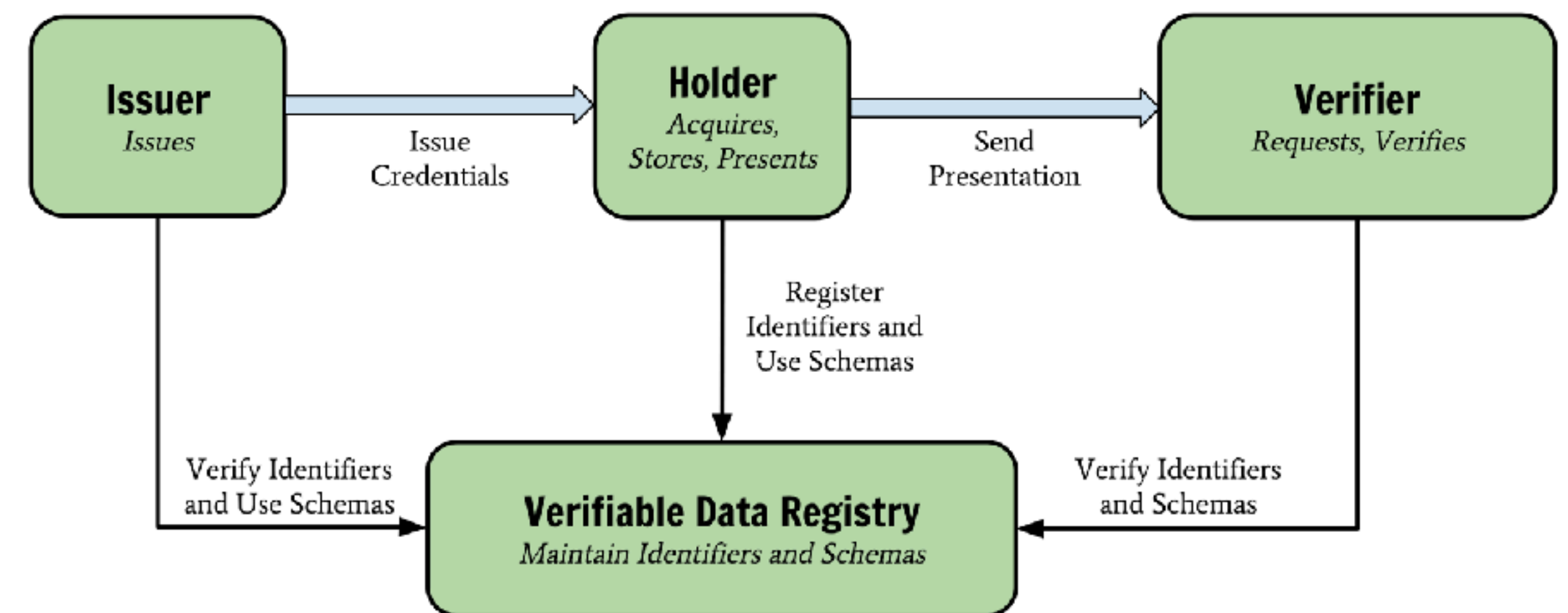


Verifiable Credentials - 検証可能な資格証明書

- さまざまな「証明書」のデジタル化手段
- デジタル署名技術を用いた【発行者】(Issuer)により【対象者】(Subject)が特定の条件を満たしている事を【保持者】(Holder) が示すことができる
- W3C で標準化されている [1]

- Subject / Issuer / Holder を示すための手段が必要

→ デジタルアイデンティティが必須



Presentation Exchange

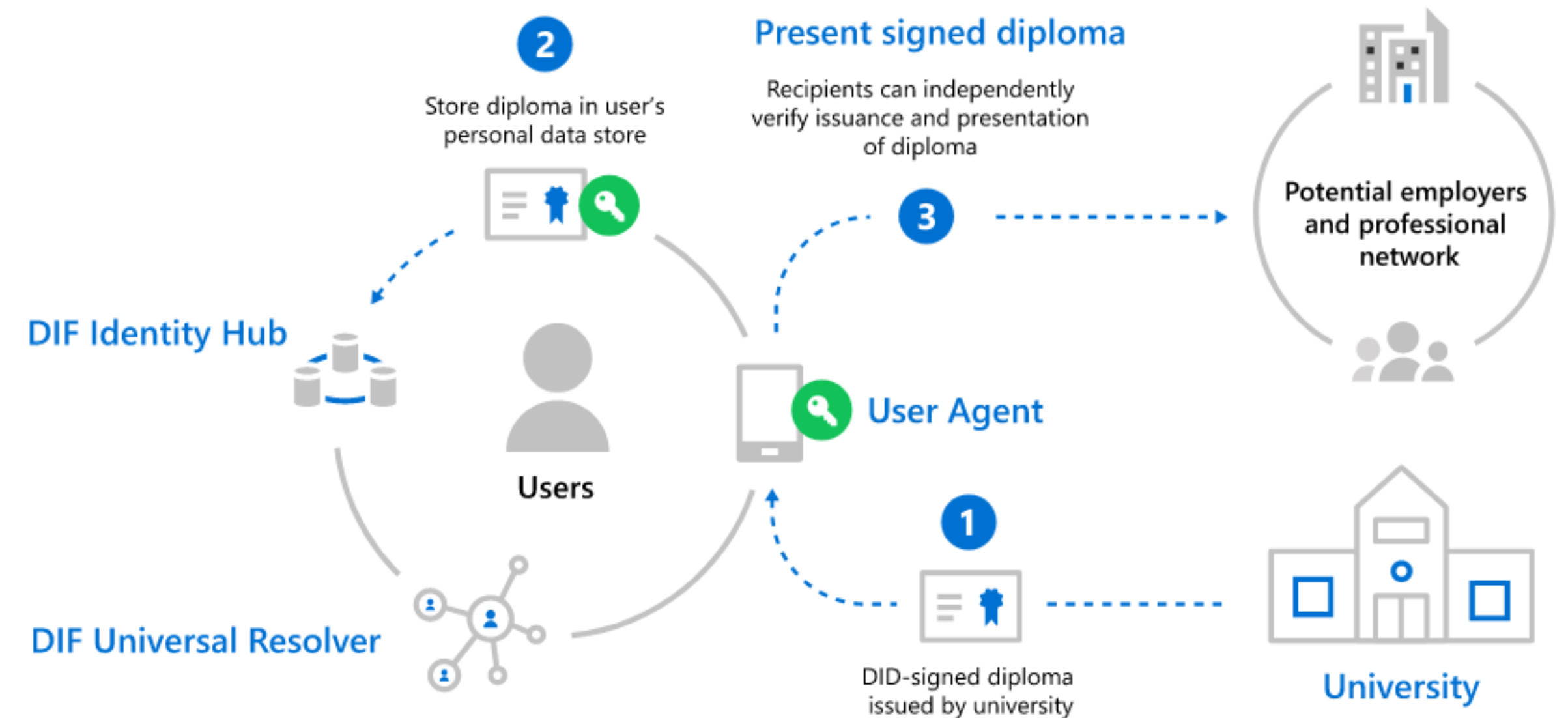
- 【データ開示の最小化】の視点では、資格証明書を持っている者(Holder)が、証明書を丸ごと引き渡すのではなく、選択的に内容を提示できることが望ましい
- このために、検証者(Verifier)が、必要な情報を提示し、資格証明書を持っている者(Holder)との間で調整(ネゴシエーション)するためのプロトコルが、Presentation Exchange [1] である
- Decentralized Identity Foundation (DIF)で議論が行われている

[1] Presentation Exchange - DIF

<https://identity.foundation/presentation-exchange/>

VCでのゼロ知識証明(ZKP)の利用

- アイデンティティワレット(図中のUser Agent)に保存した資格証明書(複数も可能)から、必要な情報だけを抜き出して、提示することができる
- 資格証明書の一部(求められたもののみ)を、署名が確認できる状態を確保しつつ開示可能



■ DID/VCについての周辺事情



関連コミュニティ

- World Wide Web Consortium (W3C)
 - Decentralized Identifier Working Group [1]
 - DID の中心となる(core)仕様と、そのメンテナンス
 - W3Cメンバーのみ参加可能
 - Credentials Community Group [2]
 - 資格証明書(credentials)の相互運用性に関連した標準策定
 - W3Cメンバーでなくても参加可能
- Decentralized Identity Foundation (DIF) [3]
 - 中立的な分散アイデンティティについてのコラボレーションの場
 - W3C外で標準についての議論が行われている

[1] <https://www.w3.org/2019/09/did-wg-charter.html>

[2] <https://www.w3.org/community/credentials/charter/>

[3] <https://identity.foundation/>



LESS アイデンティティ と トラストレスアイデンティティ

LESS アイデンティティ

"合法的な自己主権型" アイデンティティ
(“Legally-Enabled Self-Sovereign” Identity[1])

主な特性:

- 最小限の情報開示
- 完全なコントロール
- 必要な証明が出来る
- 合法

トラストレスアイデンティティ

あるいは「トラストを最小化した」アイデンティティ

主な特性:

- 匿名性
- ウェブ状の信頼関係 (Web of Trust)
- 検閲に対する耐性
- 権力者に対する人権保護
(民族国家、多国籍企業、マフィア、等)

[1] Tim Boumaによる (@trbouma)
<https://medium.com/@trbouma/less-identity-65f65d87f56b>

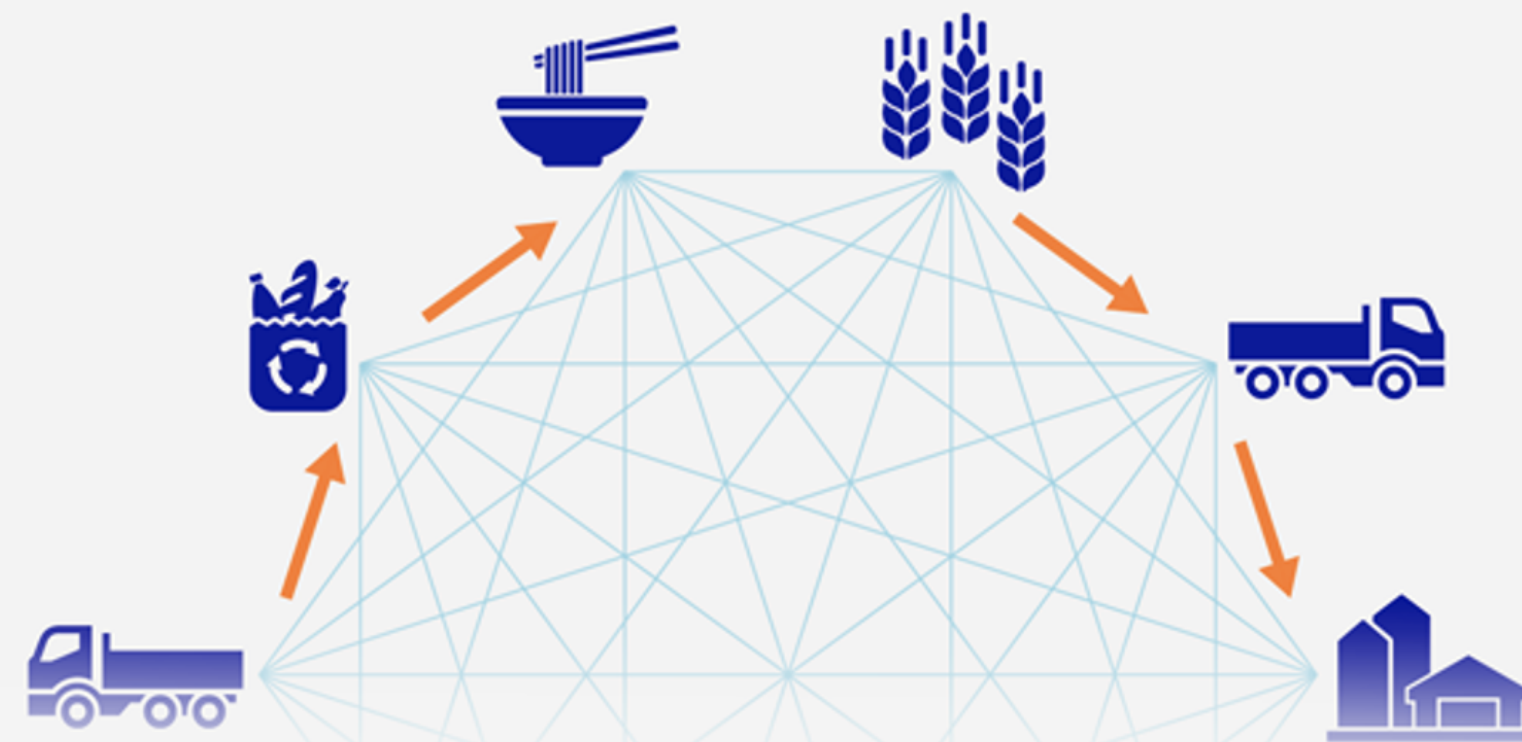
<https://ssimeetup.org/self-sovereign-identity-why-we-here-christopher-allen-webinar-51/>

各国政府の支援の拡大 (1)



Increasing Government Support

- Cross borders
- Improve Supply Chain Management
- Combat Counterfeit Goods



[CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/)

To that end, DHS S&T is pursuing two broad courses of action to encourage a more open and inclusive future for blockchain technology:

1. Support development of globally available specifications (precursor to standards) that are open, royalty free, and free to implement to ensure interoperability across systems while ensuring there is no vendor lock-in.
 - a. Decentralized Identifiers (DIDs) via World Wide Web Consortium (W3C) Standardization Process
 - b. Verifiable Claims Data Model via W3C Standardization Process
 - c. Decentralized Key Management System via TBD (Potentially OASIS)
2. Actively work with and support our DHS Component customers, such as CBP, to understand their potential use cases for blockchain and help them achieve their outcomes with the needed R&D expertise and technologies.

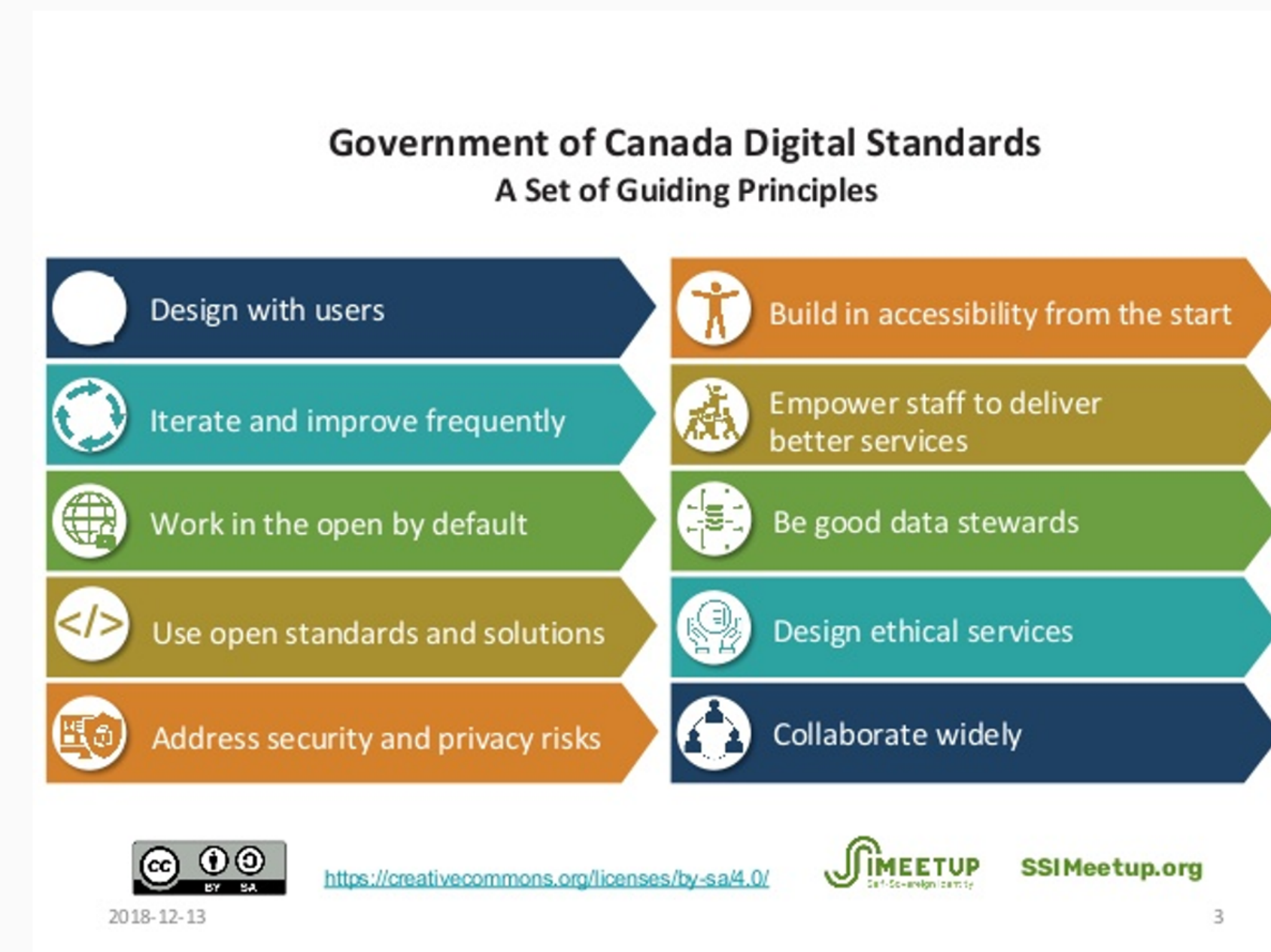
Source: DHS Science and Technology Directorate's Testimony before the US House of Representatives, May 8, 2018



各国政府の支援の拡大 (2)



Increasing Government Support



[CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/)



<https://ssimeetup.org/self-sovereign-identity-why-we-here-christopher-allen-webinar-51/>

KBCLディスカッションペーパーと グローバルデジタルアイデンティティの課題



ニューノーマル時代における人間の社会活動を支える情報基盤の在り方とデジタルアイデンティティの位置づけ

Version 0.1 (2020/8/3)

慶應義塾大学SFC研究所 ブロックチェーン・ラボ

村井 純

慶應義塾大学 教授

鈴木 茂哉

慶應義塾大学大学院政策・メディア研究科 特任教授

松尾 真一郎

慶應義塾大学大学院政策・メディア研究科 特任教授(非常勤)

ジョージタウン大学研究教授

クロサカタツヤ

慶應義塾大学大学院政策・メディア研究科 特任准教授(非常勤)

ニューノーマルと新たなインターネット文明の調和

新型コロナウイルス感染症（COVID-19）の感染拡大は、人間社会に新しい生活様式を要求しはじめている。我が国をはじめ、世界中の多くで、人間との接触（フィジカル・コンタクト）への制限が求められる中、デジタル・テクノロジーの活用は、従来のような付加価値向上という水準を超えて、すでに生命や健康の安全にとって重要な手段として位置づけられはじめている。こうした現状を、マイクロソフトのサテニア・ナデラCEOは、同社の決算発表において「この2ヶ月間で2年分に匹敵するほどのデジ



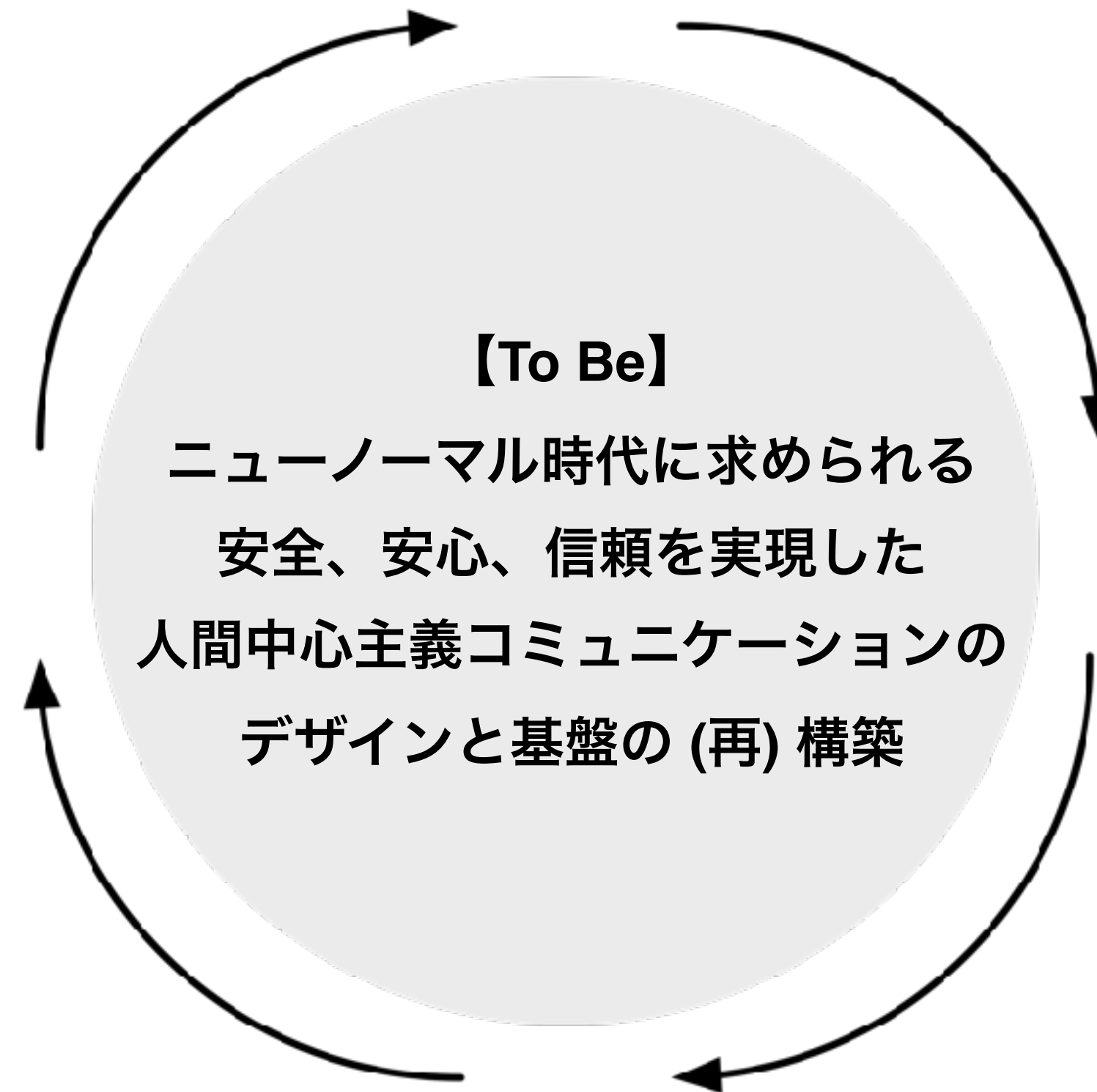
ニューノーマルと新たなインターネット文明の調和

人間と社会軸の重視

- 身体や物理的な生活空間の希少性と価値の向上 (priceless化)
- 日常的な活動の多くがデジタル化 (できることはデジタルで)
- 感情のデジタル表現等により、人間やその活動の「トラスト」が形成される
⇒人間の行動がデジタルの価値観と協調しながら変容する
「ニューノーマル社会」の出現

デジタルファーストの完全化

- 人間とその活動がフィジカル起点からデジタル起点にシフトし、必要なサービスがデジタル前提でデザインされる
- 価値交換メカニズムのデジタル化
⇒デジタル技術とネットワークが人間とその活動（法人等を含む）の必須条件となる
「フルコネクテッド社会」の出現



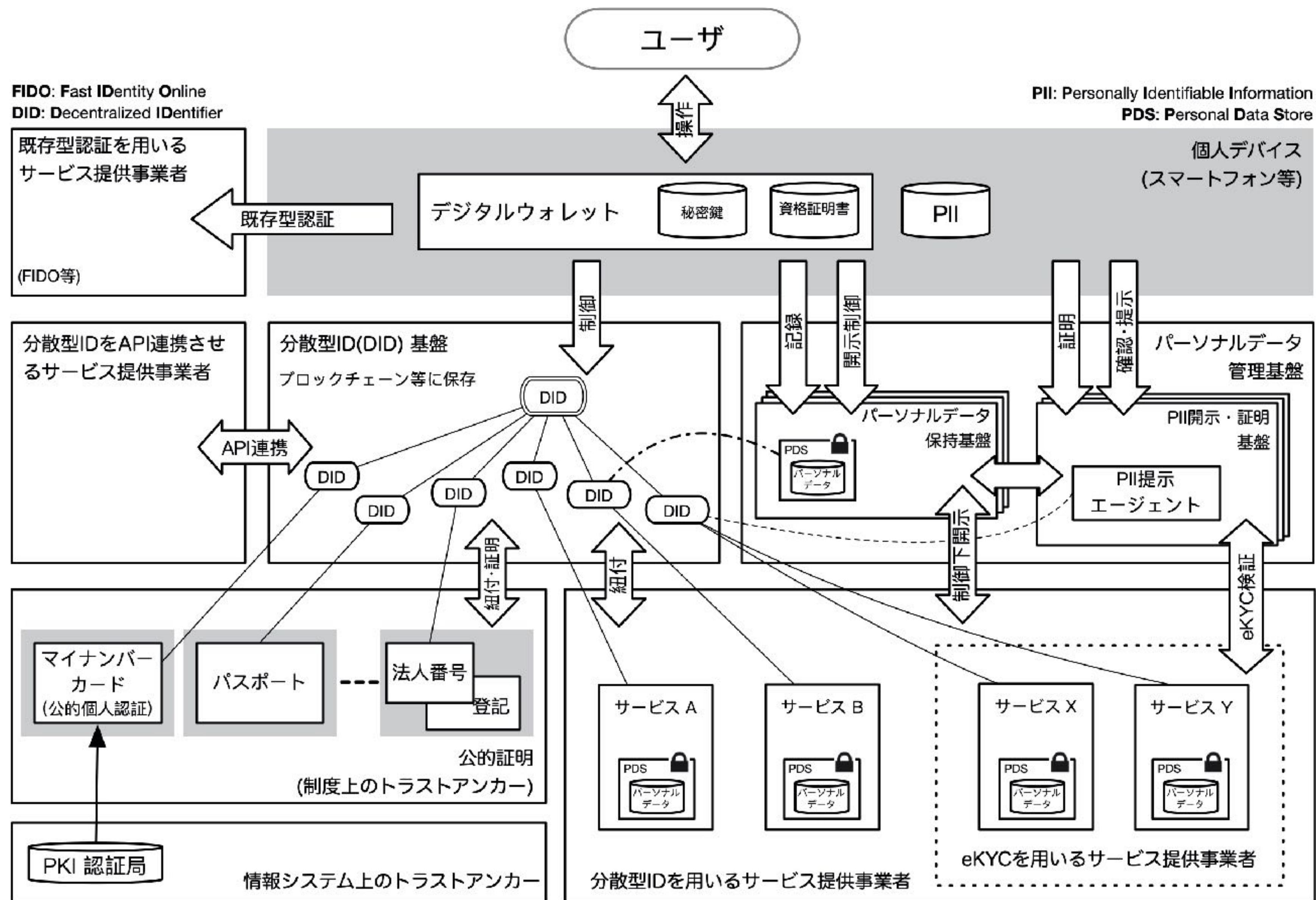
技術のコモディティ化

- 高精細デバイスのネットワーク化
- イノベーションコストがゼロに
cf.5G, AI, IoT, 8Kの普及
⇒人間のあらゆる振るまいが記録可能な
「エビデンスベース社会」への期待

経済戦略とビジョンの再構成

- 予測技術と誘導（ナッジ）の普及
- 短期的な行動変容促進の台頭と、それによる私権や倫理との衝突
⇒行動変容を促進する技術の受容に向けた、
人間とその活動にとっての価値と展望
（ビジョン）を明確にする必要性が顕在化

グローバルデジタルアイデンティティ基盤構築



次世代アイデンティティ基盤実証実験 (DID PoC) について



課題



大学DXにおけるDID/VC利用の課題

- DIDの運用上の問題
 - 全てのresolverで全てのmethodが利用できる保証がない → 運用で解決できるか？
 - methodを超えた移転 → 運用で解決するしかない
 - 鍵のロールオーバー → 議論はある。現時点は運用で解決可能
- 学歴VCの標準化
 - 学歴に関するデジタル署名を用いた実績あるフォーマットが無い → 議論中
 - 学歴のデジタル化プロジェクトは星の数ほどあるが、国際的にも無い
 - 諸外国と日本でのデータモデル違い → 教育実績の捉え方の違い
 - 職歴との関係 → 海外のユースケースでは、一連の情報として捉えられている