Verifiable Credentials 及び Decentralized Identifiers の概要

鈴木茂哉

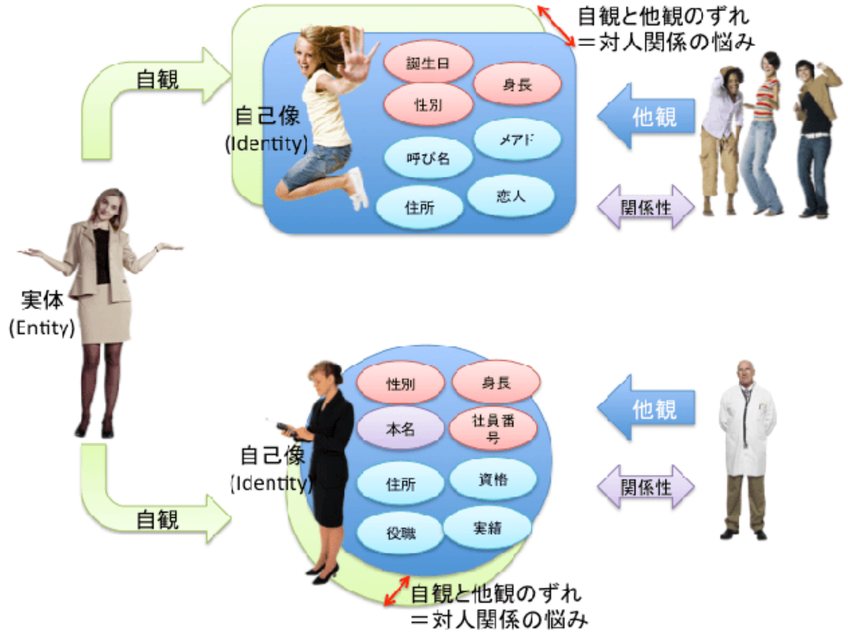
慶應義塾大学大学院政策・メディア研究科 特任教授
慶応義塾大学SFC研究所ブロックチェーン・ラボ 副所長（技術統括)
WIDEプロジェクトボードメンバ
2022/3/15

デジタルアイデンティティ

- ものすごく「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)



[1] 非技術者のためのデジタル・アイデンティティ入門, @_Nat Zone, 2011/6/21
https://www.sakimura.org/2011/06/1124/

自己主権型で実装可能な分散型ID (Decentralized Identifier) とデジタル証明書 (Verifiable Credential)

- 自己主権型デジタルアイデンティティ
  - 誰にも依存せずに自身で制御可能なデジタルアイデンティティ

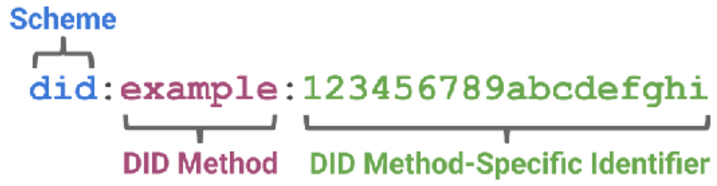
- Decentralized Identifier (DID) / W3C Candidate Recommendation
  - 属性情報と紐付けられていない「限り無く無色の」アイデンティティ
  - 分散システム指向であり、自己主権型で実装可能
  - ブロックチェーンに依存**<u>していない</u>**

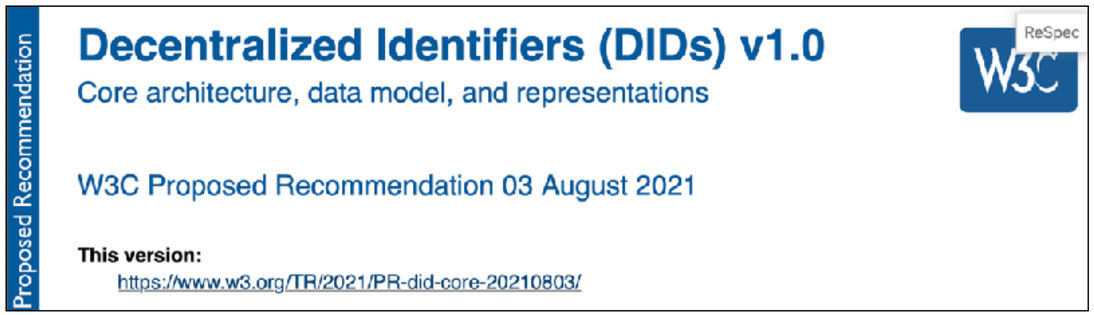
- Verifiable Credential / W3C Recommendation
  - 属性情報を第三者に証明してもらうための【デジタル証明書】仕様
  - DIDで示されたアイデンティティに対し、属性情報を紐付ける役割
  - ゼロ知識証明などの技術の組み合わせにより個人情報の「選択的最小開示」を実現できる

- 詳細については本日この後のセッションで紹介する
  「経済産業省委託事業【Trusted Webの国際標準化に向けた調査】報告書」参照

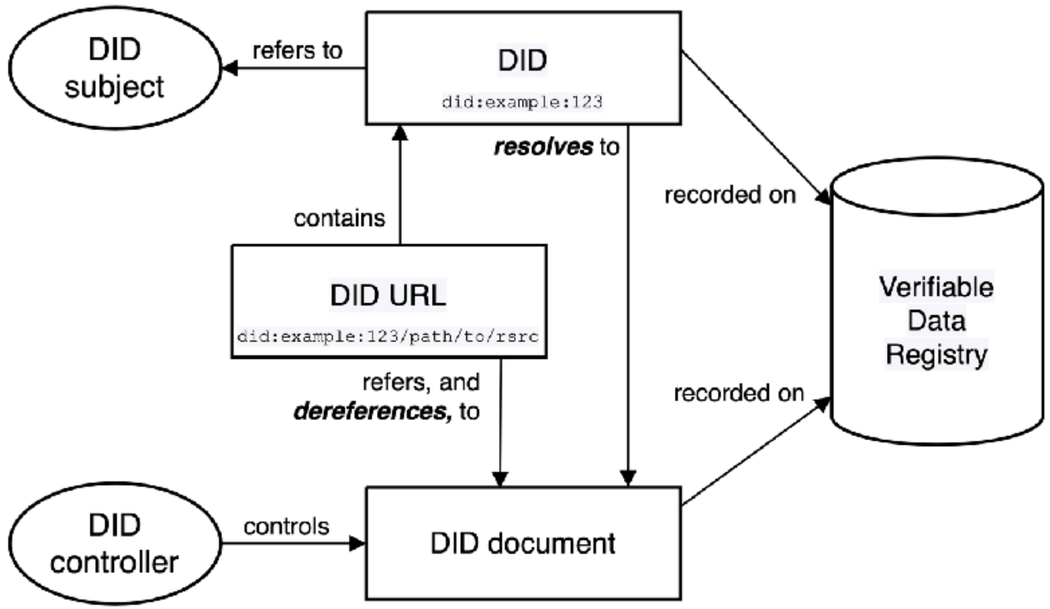
Decentralized Identifier (DIDs) v1.0 (Proposed Recommendation)

- 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
  - 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、しないものもある





Decentralized Identifier (DIDs) v1.0 (Proposed Recommendation)
https://www.w3.org/TR/2021/PR-did-core-20210803/



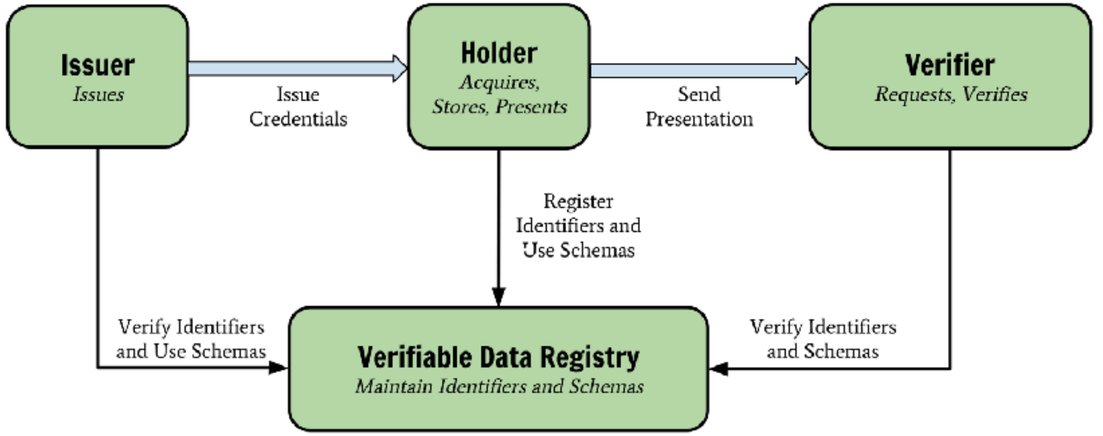
2021/9/28：3つのメンバ組織から Formal Objectionがあり議論がなされている / WG Charterは3ヶ月延長

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

→ **<u>デジタルアイデンティティ技術が必須</u>**



[1] Verifiable Credentials Data Model v1.1, W3C Recommendation 03 March 2022 https://www.w3.org/TR/vc-data-model/

Trusted Webと公開鍵暗号技術

- 対象となるデータの完全性とデータの出所と共に確かめられるようにするには、公開鍵暗号技術を用いたデジタル署名が活用できる

- 確認されたデータを組み合わせ、データの確認を出来る限り広範囲に適用することで「検証可能な領域を広げることでTrustを高める」Trusted Webの効果を得る

公開鍵暗号技術とVC

- 対象となるデータの完全性（確認された時点から変化がないこと）とデータの出所をともに確かめることが可能である。ただし、公開鍵暗号アルゴリズムと公開鍵基盤(PKI)だけでは実現できず、以下の要素が必要

    1. 対象となるデータへの参照(同梱)方法、または、パッケージングの方法
       （シリアライゼーション、場合によっては正規化を含む）
    2. 対象となるデータへの公開鍵暗号によるデジタル署名におけるアルゴリズム選択
       （暗号アルゴリズムとハッシュアルゴリズム等の組み合わせ）
    3. デジタル署名に用いられた公開鍵暗号鍵の出所を示す情報。一般には公開鍵証明書
    4. 上記1.〜3.を、ひとかたまりにパッケージングする方式

- e-Taxは 1と2。PKI (GPKI) の役割は3。4はトランスポート依存。
- VC関連技術では、上記が整っており、さらに既存のPKIとの連係もできる