DID/VC 標準化動向

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研究所データアーキテクチャラボ 副所長（技術統括)
Trusted Web 推進協議会 タスクフォース 構成員
WIDEプロジェクトボードメンバ

2023/10/31

AXIES認証基盤部会 勉強会「続・Verifiable Credentials（VC）を学んで議論に参加してみよう　〜AXIES認証基盤部会編〜」

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 / 博士 (政策・メディア)

Shigeya Suzuki, Ph.D

Project Professor,
Graduate School of Media and Governance, Keio University

shigeya@wide.ad.jp
shigeya@keio.jp

主たる研究領域

ネットワーク化されたセキュアな情報システムの設計 / 開発 / 構築

情報システムアーキテクチャ / コンピューターネットワーク / 分散システム / デジタルアイデンティティ / ネットワークシステムセキュリティ / 量子インターネット

現在の主たる肩書き・活動等

慶應義塾大学SFC研究所 データーアーキテクチャラボ 副所長(技術統括)

慶應義塾大学SFC研究所 トラステッド・インターネット・アーキテクチャ・ラボ 副所長

慶應義塾大学SFC研究所 Auto-ID Labs Japan副所長

WIDEプロジェクト ボードメンバ/研究者

Trusted Web推進協議会タスクフォースメンバ
(内閣官房デジタル市場競争会議)

W3C DID WG / VC WG / Credentials CCG メンバ

Rebooting the Web of Trust, Board Member

Originator Profile技術研究組合 技術開発WG部会長

Recent Papers and Other works 最近の主な研究業績

Mitigation of Seller and Buyer's Dilemma with Transaction History and Escrow *(2023)*
Ryosuke Abe, Seiyo Kurita, Mariko Kobayashi, Shigeya Suzuki
AINTEC'22: The 17th Asian Internet Engineering Conference, Haoni, Vietnam Blockchain

A System for Selective Disclosure of Information about a Patient with Intractable Disease *(2023)*
Erika Sugita, Ryosuke Abe, Shigeya Suzuki, Keisuke Uehara, Osamu Nakamura
ESAS 2023: The 18th IEEE International Workshop on e-Health Systems and Web Technologies, Trino, Italy Verfiable Credentals

Verifiable Issuers & Verifiers *(2022)*
Manu Sporny, Oskar van Deventer, Isaac Henderson Johnson Jeyakumar, Shigeya Suzuki, Konstantn Tsabolov, Line Kofoed, Rieks Joosten
A WHITE PAPER FROM RWOT XI: THE HAGUE, 22 Dec 2022 Verfiable Credentals

QuISP: a Quantum Internet Simulation Package *(2022)* BEST PAPER AWARD Quantum Internet
Ryosuke Satoh, Michal Hajdušek, Naphan Benchasattabuse, Shota Nagayama, Kentaro Teramoto, Takaaki Matsuo, Sara Ayman Metwalli, Poramet Pathumsoot, Takahiko Satoh, Shigeya Suzuki, Rodney Van Meter, 2022 IEEE International Conference on Quantum Computing and Engineering (QCE22), Broomfield, CO, USA

A Quantum Internet Architecture *(2022)* Quantum Internet
Rodney Van Meter, Ryosuke Satoh, Naphan Benchasattabuse, Kentaro Teramoto, Takaaki Matsuo, Michal Hajdusek, Takahiko Satoh, Shota Nagayama, Shigeya Suzuki, 2022 IEEE International Conference on Quantum Computing and Engineering (QCE22), Broomfield, CO, USA

Trusted Web ホワイトペーパ Ver.2.0 *(2022)* Identity Privacy Blockchain Member/Architect
Trusted Web推進協議会 (内閣官房デジタル市場競争会議)

Decentralized Identifiers (DIDs) v1.0 *(2021)* Identity Contributor
Manu Sporny, Amy Guy, Markus Sabadello, Drummond Reed (Editors)
World Wide Web Consoritium, 26 July 2021

DID Core Specification Test Suite and Implementaiton Report *(2021)* Editor Identity
Orie Steele, Shigeya Suzuki, Manu Sporny, Markus Sabadello (Editors)
World Wide Web Consoritium, 26 July 2021

Attacking the Quantum Internet *(2021)* Security Quantum Internet
Takahiko Satoh, Shota Nagayama, Shigeya Suzuki, Takaaki Matsuo, Michal Hajdušek, Rodney Van Meter.
IEEE Transactions on Quantum Engineering

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 (ディスカッションペーパ 2020) Privacy Identity Blockchain
村井 純、鈴木 茂哉、松尾 真一郎、クロサカタツヤ, 慶應義塾大学SFC研究所 ブロックチェーン・ラボ

令和元年度: ブロックチェーン技術等を用いた金融システムのガバナンスに関する研究 Blockchain DeFi Multistakeholder Governance
[慶應義塾大学SFC研究所との合同研究]
金融庁 総合政策局 総合政策課 フィンテック室

Mitigating Bitcoin Node Storage Size By DHT *(2018)* Blockchain Scalability
Ryosuke Abe, Shigeya Suzuki, Jun Murai, AINTEC 2018, Bangkok, Thailand

Blockchain as an Audit-able Communication Channel *(2017)* Blockchain Traceability
Shigeya Suzuki, Jun Murai
STPSA 2017: The 12th IEEE International COMPSAC Workshop on Security, Trust and Privacy for Software Applications, Trino, Italy

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 / 博士 (政策・メディア)

Shigeya Suzuki, Ph.D

Project Professor,
Graduate School of Media and Governance, Keio University

shigeya@wide.ad.jp
shigeya@keio.jp

主たる研究領域

ネットワーク化されたセキュアな情報システムの設計 / 開発 / 構築

情報システムアーキテクチャ / コンピューターネットワーク / 分散システム / デジタルアイデンティティ / ネットワークシステムセキュリティ / 量子インターネット

現在の主たる肩書き・活動等

慶應義塾大学SFC研究所 データーアーキテクチャラボ 副所長(技術統括)

慶應義塾大学SFC研究所 トラステッド・インターネット・アーキテクチャ・ラボ 副所長

慶應義塾大学SFC研究所 Auto-ID Labs Japan副所長

WIDEプロジェクト ボードメンバ/研究者

Trusted Web推進協議会タスクフォースメンバ
(内閣官房デジタル市場競争会議)

W3C DID WG / VC WG / Credentials CCG メンバ

Rebooting the Web of Trust, Board Member

Originator Profile技術研究組合 技術開発WG部会長

Recent Papers and Other works 最近の主な研究業績

Mitigation of Seller and Buyer's Dilemma with Transaction History and Escrow *(2023)*
Ryosuke Abe, Seiyo Kurita, Mariko Kobayashi, Shigeya Suzuki
AINTEC'22: The 17th Asian Internet Engineering Conference, Haoni, Vietnam
Blockchain

A System for Selective Disclosure of Information about a Patient with Intractable Disease *(2023)*
Erika Sugita, Ryosuke Abe, Shigeya Suzuki, Keisuke Uehara, Osamu Nakamura
ESAS 2023: The 18th IEEE International Workshop on e-Health Systems and Web Technologies, Trino, Italy
Verfiable Credentals

Verifiable Issuers & Verifiers *(2022)*
Manu Sporny, Oskar van Deventer, Isaac Henderson Johnson Jeyakumar, Shigeya Suzuki, Konstantn Tsabolov, Line Kofoed, Rieks Joosten
A WHITE PAPER FROM RWOT XI: THE HAGUE, 22 Dec 2022
Verfiable Credentals

QuISP: a Quantum Internet Simulation Package *(2022)*
Ryosuke Satoh, Michal Hajdušek, Naphan Benchasattabuse, Shota Nagayama, Kentaro Teramoto, Takaaki Matsuo, Sara Ayman Metwalli, Poramet Pathumsoot, Takahiko Satoh, Shigeya Suzuki, Rodney Van Meter, 2022 IEEE International Conference on Quantum Computing and Engineering (QCE22), Broomfield, CO, USA
BEST PAPER AWARD
Quantum Internet

A Quantum Internet Architecture *(2022)*
Rodney Van Meter, Ryosuke Satoh, Naphan Benchasattabuse, Kentaro Teramoto, Takaaki Matsuo, Michal Hajdusek, Takahiko Satoh, Shota Nagayama, Shigeya Suzuki, 2022 IEEE International Conference on Quantum Computing and Engineering (QCE22), Broomfield, CO, USA
Quantum Internet

Trusted Web ホワイトペーパ Ver.2.0 *(2022)*
Trusted Web推進協議会 (内閣官房デジタル市場競争会議)
Identity Privacy Blockchain Member/Architect

Decentralized Identifiers (DIDs) v1.0 *(2021)*
Manu Sporny, Amy Guy, Markus Sabadello, Drummond Reed (Editors)
World Wide Web Consoritium, 26 July 2021
Identity Contributor

DID Core Specification Test Suite and Implementaiton Report *(2021)*
Orie Steele, Shigeya Suzuki, Manu Sporny, Markus Sabadello (Editors)
World Wide Web Consoritium, 26 July 2021
Editor Identity

Attacking the Quantum Internet *(2021)*
Takahiko Satoh, Shota Nagayama, Shigeya Suzuki, Takaaki Matsuo, Michal Hajdušek, Rodney Van Meter.
IEEE Transactions on Quantum Engineering
Security Quantum Internet

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 (ディスカッションペーパ 2020)
村井 純、鈴木 茂哉、松尾 真一郎、クロサカタツヤ, 慶應義塾大学SFC研究所 ブロックチェーン・ラボ
Privacy Identity Blockchain

令和元年度: ブロックチェーン技術等を用いた金融システムのガバナンスに関する研究
[慶應義塾大学SFC研究所との合同研究]
金融庁 総合政策局 総合政策課 フィンテック室
Blockchain DeFi Multistakeholder Governance

Mitigating Bitcoin Node Storage Size By DHT *(2018)*
Ryosuke Abe, Shigeya Suzuki, Jun Murai, AINTEC 2018, Bangkok, Thailand
Blockchain Scalability

Blockchain as an Audit-able Communication Channel *(2017)*
Shigeya Suzuki, Jun Murai
STPSA 2017: The 12th IEEE International COMPSAC Workshop on Security, Trust and Privacy for Software Applications, Trino, Italy
Blockchain Traceability

本日のお題

- DID Core 1.0 / VC 1.1
- VC 2.0 Charter
- 関係するコミュニティ
- 現況
- デプロイメントに向けて

VC 1.1 / DID 1.0

プライバシー状の考慮が可能なデジタル証明書 (Verifiable Credentials)と自己主権型で実装可能な分散型ID (Decentralized Identifiers)

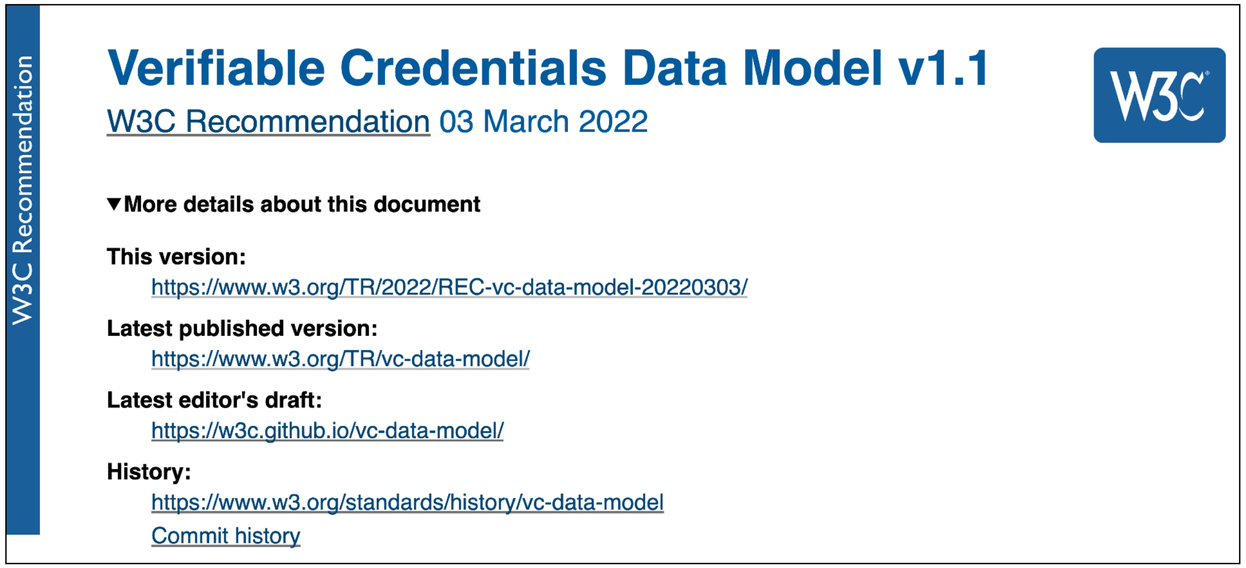
- **Verifiable Credentials / W3C Recommendation (v1.1 - v2.0作業中)**
  - 属性情報を第三者に証明してもらうための【デジタル証明書】仕様
  - ゼロ知識証明などの技術の組み合わせにより個人情報の「選択的最小開示」を実現できる

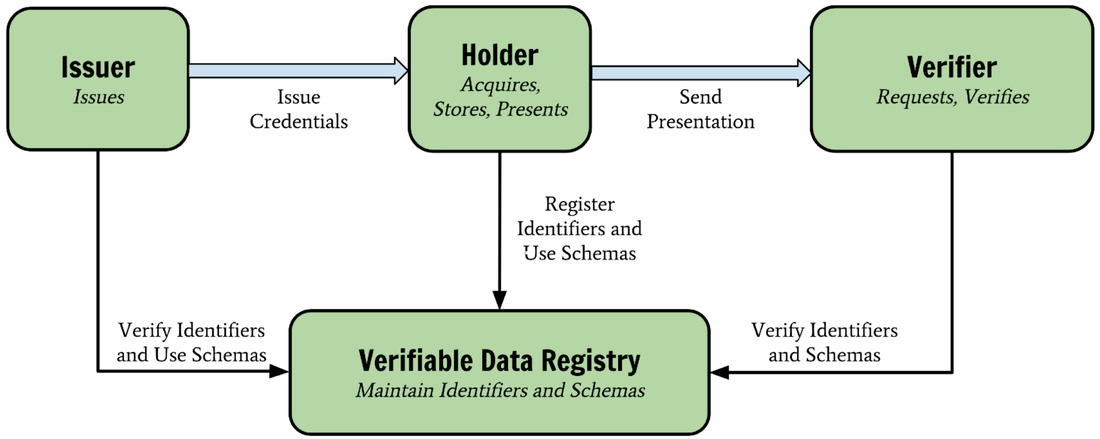
- **Decentralized Identifiers (DID) / W3C Candidate Recommendation (v1.0)**
  - 属性情報と紐付けられていない「限り無く無色の」アイデンティティ
  - 分散システム指向であり、自己主権型で実装可能
  - **自己主権型デジタルアイデンティティ**
    - 一つの定義: 誰にも依存せずに自身で制御可能なデジタルアイデンティティ

- **よくある勘違い:** VCはDIDと共に用いることでプラバシーリークを抑えることができるが、必ずしも組み合わせて使う必要はない。またDIDはブロックチェーンだけのものではない

Verifiable Credentials Data Model v1.1 (W3C Recommendation)

- 検証可能なデジタル証明書の**データモデル標準**
- 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



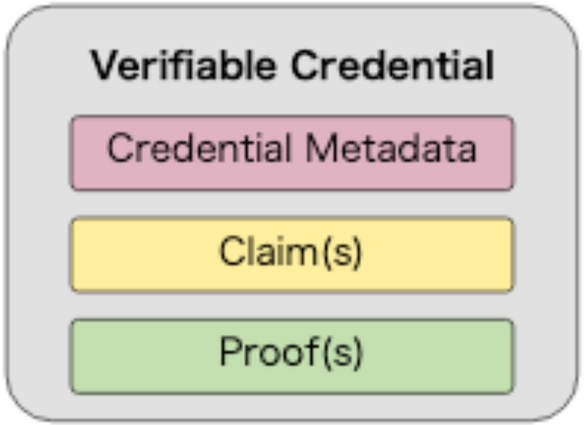


Latest Version:
Verifiable Credentials Data Model v1.1, W3C Recommendation 03 March 2022
https://www.w3.org/TR/2022/REC-vc-data-model-20220303/

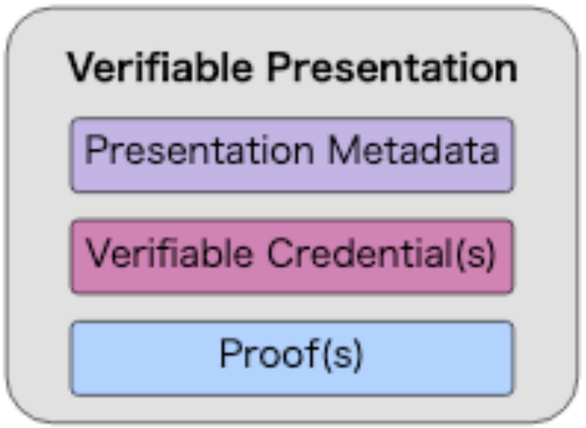
First Major Version:
Verifiable Credentials Data Model v1.0, W3C Recommendation 19 Nov 2019
https://www.w3.org/TR/2019/REC-vc-data-model-20191119/

Verifiable Credentialと Verifiable Presentation

- **Verifiable Credential**: 単一の証明書
  - Credential Metadata: 発行者や発行日時などを示すメタデータ
  - Claim(s): 証明書が示す証明内容
  - Proof(s): 発行者によるデジタル署名など
- **Verifiable Presentation**: （複数の）証明書を検証者へ提示するためのデータ形式
  - Presentation Metadata: 提示者や発行日時などを示すメタデータ
  - Verifiable Credential(s): 提示する証明書
  - Proof(s): 作成者が保有者であることを示すデジタル署名など



Verifiable Credentials



Verifiable Presentation

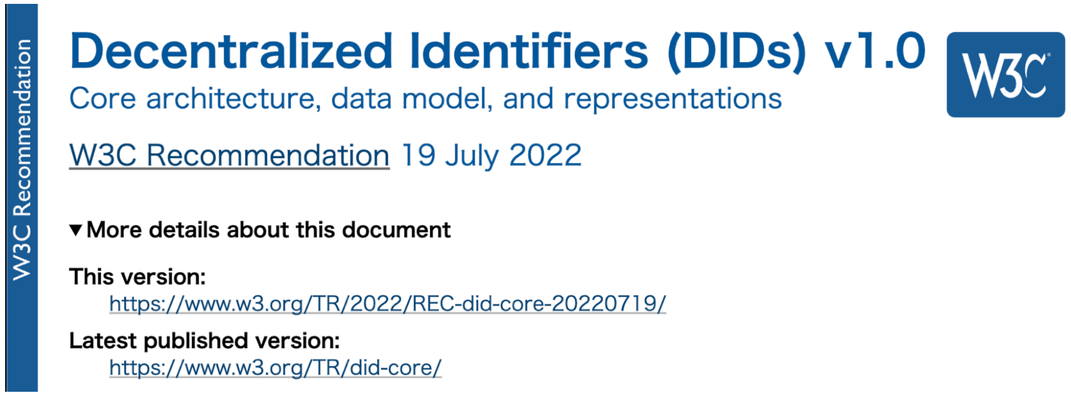
Verifiable Credentials 標準に関するタイムライン

- 2014年8月: Credentials Community Group のローンチ [1]
- Web Payments Interest Groupの議論[1]から、同グループの Task Force として2015年11月にVerifiable Claims Task Force がローンチされる[3]
- 2017年5月にVerifiable Claims Working Groupがローンチされる[4]
  その後期限延長され、2019年9月まで継続
- 2019年3月: Verifiable Credentials Data Model v1.0 勧告案[5]
- 2019年11月: Verifiable Credentials Data Model v1.0 勧告[6]
- 2022年3月: Verifiable Credentials Data Model v1.1 勧告[7]
- 2022年6月: Verifiable Credentials Working Group v2.0に向けての新チャータで作業開始

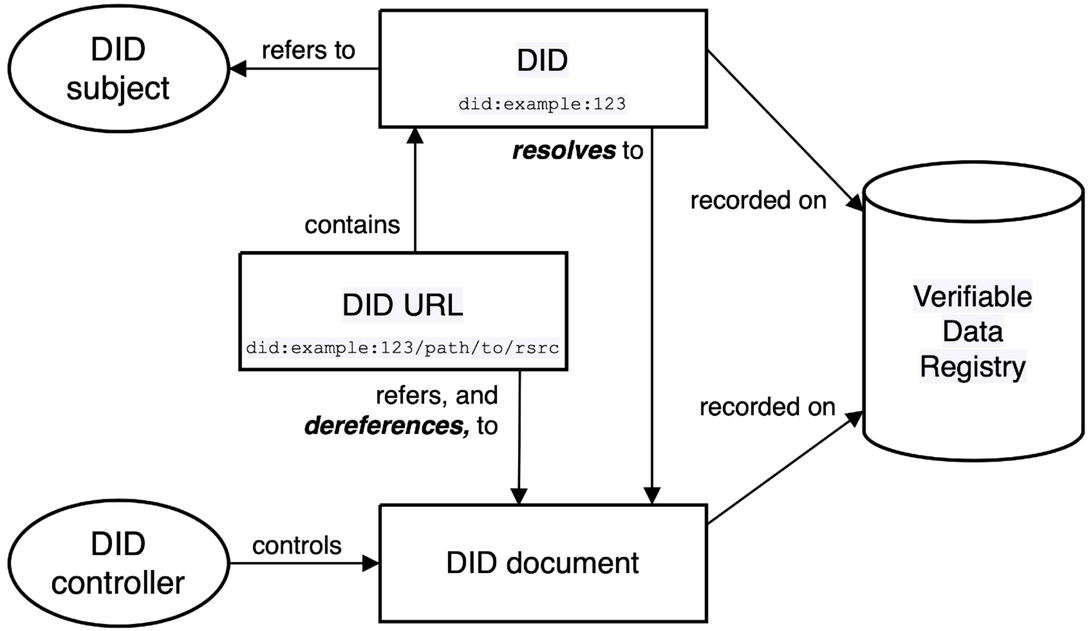
[1] Call for Participation in Credentials Community Group https://www.w3.org/community/credentials/2014/08/06/call-for-participation-in-credentials-community-group/
[2] Web Payments Road Map https://web-payments.org/specs/source/roadmap/
[3] The Verifiable Claims Task Force http://w3c.github.io/vctf/
[4] Verifiable Claims Working Group Charter https://www.w3.org/2017/vc/WG/charter.html
[5] Verifiable Credentials Data Model 1.0 Candidate Recommendation (28 March 2019) https://www.w3.org/TR/2019/CR-verifiable-claims-data-model-20190328/
[6] Verifiable Credentials Data Model 1.0 W3C Recommendation (19 November 2019) https://www.w3.org/TR/2019/REC-vc-data-model-20191119/
[7] Verifiable Credentials Data Model 1.1 W3C Recommendation (03 March 2022) https://www.w3.org/TR/2022/REC-vc-data-model-20220303/
[8] Verifiable Credentials Working Group Charter https://www.w3.org/2022/06/verifiable-credentials-wg-charter.html

Decentralized Identifier (DIDs) v1.0 (W3C Recommendation)

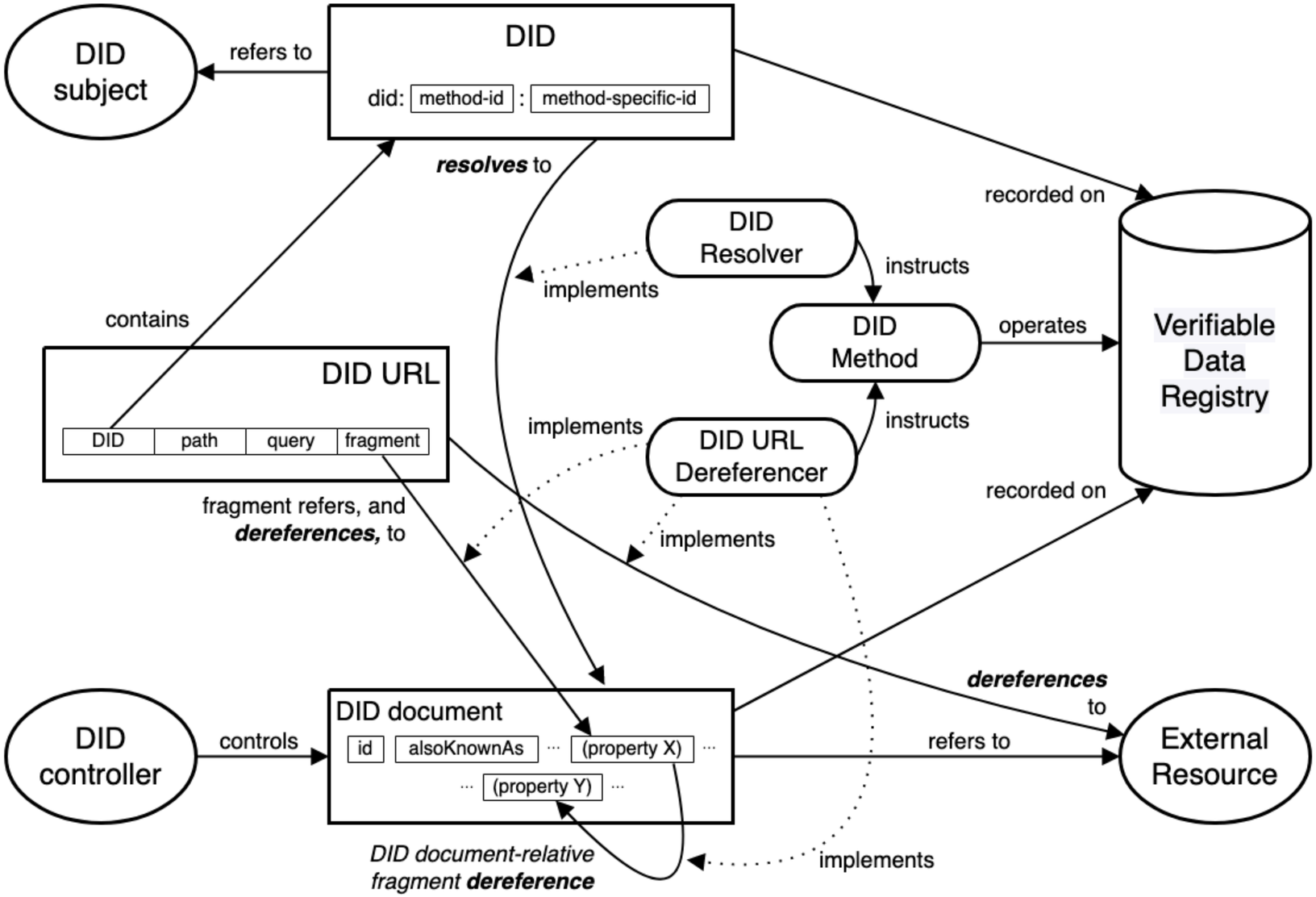
- 自己主権型の識別子にまつわる**データモデル標準**
  - 周辺技術との組み合わせで自己主権型のアイデンティティを実現できる
  - 複数の方式(メソッド)で実装され、メソッドにより、ブロックチェーン技術を下支えにするものも、しないものもある



Decentralized Identifier (DIDs) v1.0 (W3C Recommendation)
https://www.w3.org/TR/2022/REC-did-core-20220719/



Decentralized Identifier (DIDs) v1.0 (W3C Recommendation)



Decentralized Identifier (DIDs) v1.0 (W3C Recommendation). https://www.w3.org/TR/2022/REC-did-core-20220719/

この図は鈴木が作成

DID標準化に関するタイムライン[1]

- 2014 - W3C WebPayment Groupでの議論が発端 [2]
- 2015 - XDI.org での議論継続 [3],
  - 第一回 Rebooting Web Of Trust (RWOT1) [4] でのホワイトペーパ "Decentralized Public Key Infrastructure" [5]
- 2016 - RWOT2でのホワイトペーパ: "Requirements for DIDs" [6]
- 2017 - RWOT3でのホワイトペーパ: "DID (Decentralized Identifier) Data Model and Generic Syntax 1.0 Implementer's Draft 01" [7]
  - W3C Credentials Community Group [8] の作業に統合
- 2019 - W3C Decentralized Identifiers Working Group による標準化開始 [9]
- 2021 - Decentralized Identifiers (DIDs) v1.0 が Proposed recommendation に [10]

[1] Decentralized Identifiers (DIDs) v1.0, Appendix D. Acknowledgements (Editor's Working Draft), https://w3c.github.io/did-core/#acknowledgements
[2] Web Payments Community Group Telecon Minutes 2014-05-07, https://web-payments.org/minutes/2014-05-07/#topic-1
[3] XDI.org Registry Working Group Charter, https://docs.google.com/document/d/1EP-KhH60y-nl4xkEzoeSf3DjmjLomfboF4p2umF51FA/edit
[4] Rebooting Web of Trust, https://www.weboftrust.info
[5] Decentralized Public Key Infrastructure, https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/dpki.pdf
[6] Requirements for DIDs, https://github.com/WebOfTrustInfo/rwot2-id2020/blob/master/final-documents/requirements-for-dids.pdf
[7] DID (Decentralized Identifier) Data Model and Generic Syntax 1.0 Implementer's Draft 01, https://github.com/WebOfTrustInfo/rwot3-sf/blob/master/final-documents/did-implementer-draft-10.pdf
[8] W3C Credentials Community Group, https://www.w3.org/community/credentials/
[9] W3C Decentralized Identifiers Working Group, https://www.w3.org/2019/did-wg/
[10] Decentralized Identifiers (DIDs) v1.0, W3C Proposed Recommendation 03 August 2021, https://www.w3.org/TR/2021/PR-did-core-20210803/

Verifiable Credentials 2.0 (Work in Progress)

Verifiable Credentials 2.0 に向けての作業[1]

- 検証可能な証明書データモデルの旧バージョンで見つかった誤りに対処
- クレデンシャル、プレゼンテーション、および証明のデータモデル
- データモデルのレジストリ
- 既存の暗号プリミティブを利用した証明の表現と検証のためのアルゴリズム
- 多言語化

- 作業期間: 2022/6/15 ～ 2024/6/30

[1] Verifiable Credentials' WG new charter
https://w3c.github.io/vc-wg-charter/

Trust にかかわる Community と対象領域の差異による影響

Trust にかかわる Community と対象領域の差異による影響 (1)

- Decentralized Identifiers / Verifiable Credentials周辺の議論参加者を眺めていると、複数のグループを観測できる

  - 既存のアイデンティティ技術に関わっているグループ
  - 自己主権型アイデンティティを推進するグループ
  - Semantic Webの実現に資する技術を考えるグループ
  - 上記によらずにデジタル証明書の発行に興味があるグループ

Trust にかかわる Community と対象領域の差異による影響 (2)

- これらのグループの目的に伴い、意見の相違や衝突が明瞭
  - 要求仕様が違う。たとえば、
    - online/offline
    - セキュリティに関連したパラメータ
    - 時間に関連するパラメータ: 有効とすべき期間、キャッシュの仕方、etc.
    - トラストマネジメント (《トラストアンカー》の共有を含む)
  - 差異
    - ステークホルダー
      - 理念
      - 原則
    - ルールやポリシー
    - データモデル（スキーマ）
    - ボキャブラリ

現況

証明書に関するさまざまな標準

- 証明書自身
- 証明書発行や提示における通信プロトコル
- 証明書の有効性確認についてのプロトコル
- Issuer等のエンティティの用いる鍵の情報の取得方法

- 基盤となる標準
  - シリアライゼーション（レプリゼンテーション）
  - エンベロープ
  - 署名アルゴリズムの組み合わせ
  - 署名アルゴリズム
  - 鍵の表現方式
  - …

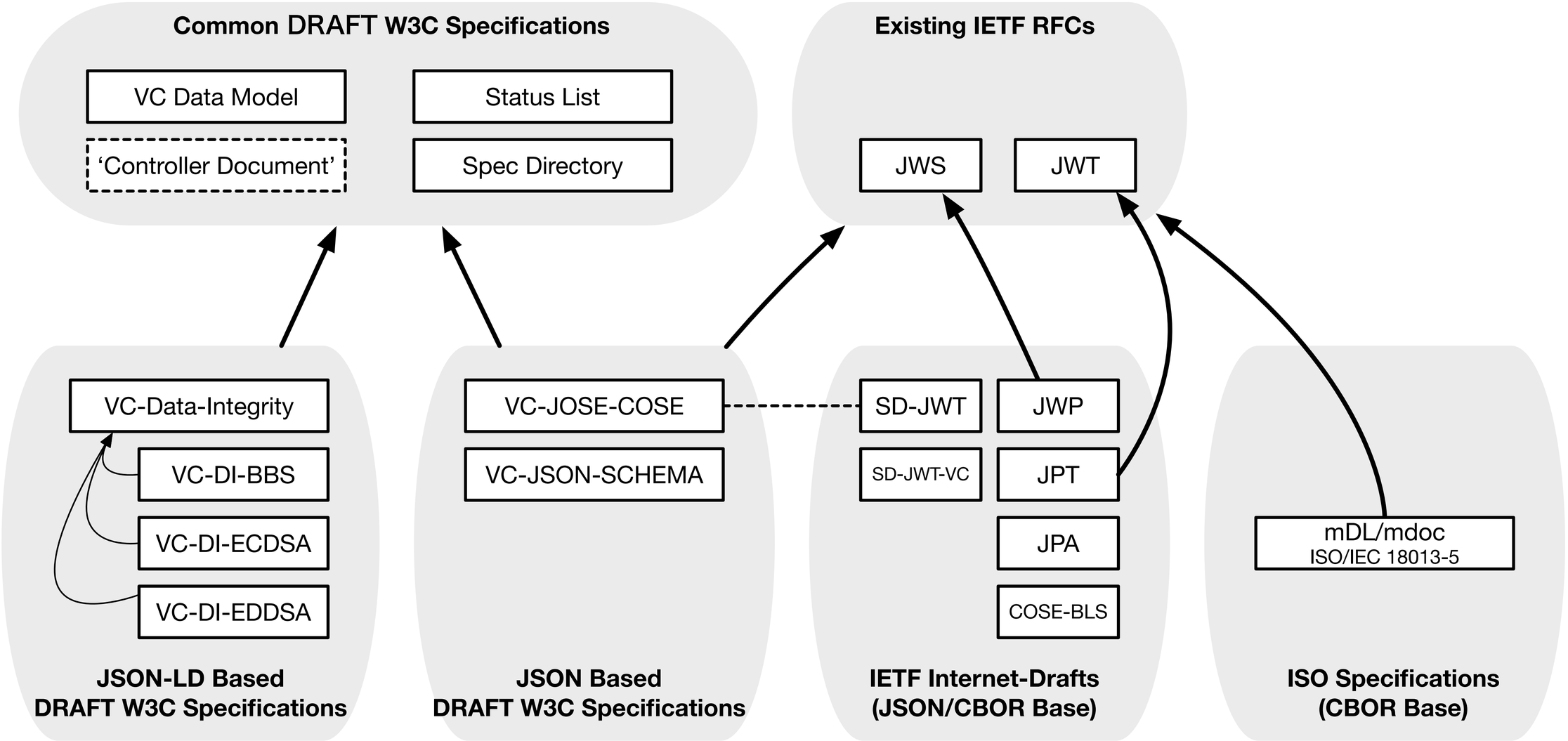
証明書発行や提示におけるプロトコル

- Authlete の川崎さんの資料参照[1]
  - VCの説明を含め現状を概ね取り込んで議論している

- 主な議論の場:
  - OpenID Foundation, IETF

[1] https://www.authlete.com/ja/developers/oid4vci/

証明書データ関連標準 (ご参考)



実装に向けて

証明書エコシステムを成立させるための要素

- Issuer
  - 証明書発行
    - 証明書の対象となる者を識別する手段
    - 証明書に書き込むべき情報の管理
- Holder
  - 証明書の入手
    - 証明書発行に関わる情報入手と手続き
    - 発行された証明書の保存
  - 証明書の検証
  - Verifierへの提示
    （Verifier自身の検証を含む）
    - 必要に応じた証明書の組み合わせと選択的開示
- Verifier
  - 証明書の受け取り・ネゴシエーション
  - IssuerとHolderを検証する手段
  - 証明書の検証
- すべてにおいて
  - 証明すべきデータのモデル
  - 開示範囲のコントロール
  - インターオペラビリティ

ラップアップ

- DID Core 1.0 / VC 1.1
- VC 2.0 Charter
- 関係するコミュニティ
- 現況
- デプロイメントに向けて