

Verifiable Credentials 周辺動向と 教育機関での活用

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

2022/12/13 @ AXIES 2022





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 ボードメンバー/研究者

Trusted Web推進協議会タスクフォースメンバー

(内閣官房デジタル市場競争会議)

W3C DID WG / VC WG / Credentials CCG メンバー

W3C Keio Team - 2015/11 ~ 2018/3

Recent Papers and Other works

最近の主な研究業績

QulSP: 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 ホワイトペーパー 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 Consortium, 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 Consortium, 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 (Early Access Available)

Security

Quantum Internet

Multistakeholder Governance for the Internet (2020)Shigeya Suzuki, Financial Cryptography and Data Security.
FC 2020, LNCS vol 12063. Springer, Cham.

Multistakeholder Governance

**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ー 2020)**

Identity

Blockchain Privacy

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

[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 Decentralized Fiance

Multistakeholder Governance

Design and Operation Practicies of Service Chaining using NFV (2018)Katsuhiro Horiba, Ryo Nakamura, Shigeya Suzuki, Yuji Sekiya, Jun Murai
IPSJ Transactions on Digital Practice

Network Virtualization

Mitigating Bitcoin Node Storage Size By DHT (2018)

Ryosuke Abe, Shigeya Suzuki, Jun Murai, AINTEC 2018, Bangkok, Thailand

Scalability

Blockchain

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

Traceability

Blockchain



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

W3C Recommendation

Verifiable Credentials Data Model v1.1

W3C Recommendation 03 March 2022

▼ More details about this document

This version:
<https://www.w3.org/TR/2022/REC-vc-data-model-20220303/>

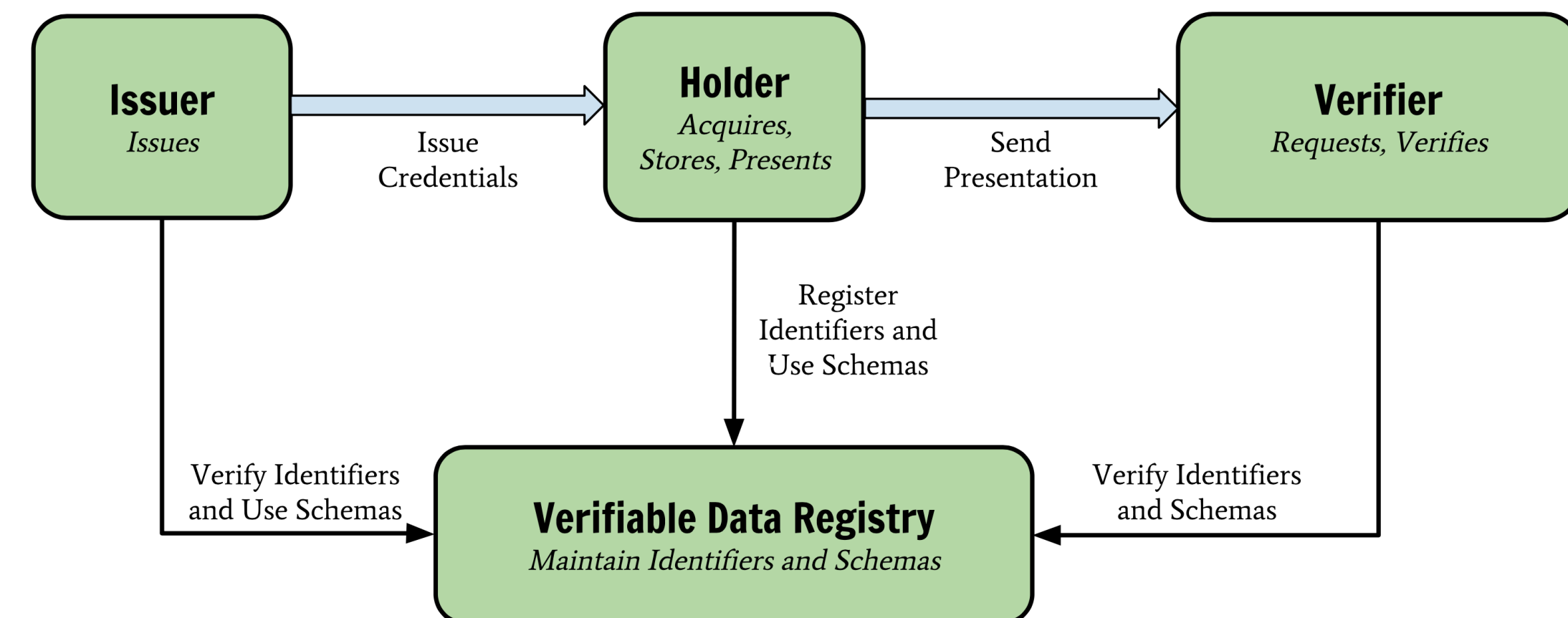
Latest published version:
<https://www.w3.org/TR/vc-data-model/>

Latest editor's draft:
<https://w3c.github.io/vc-data-model/>

History:
<https://www.w3.org/standards/history/vc-data-model>
[Commit history](#)

Implementation report:
<https://w3c.github.io/vc-test-suite/implementations/>





Verifiable Credentials Data Model v1.1, W3C Recommendation 03 March 2022

<https://www.w3.org/TR/2022/REC-vc-data-model-20220303/>

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 (鈴木から提案[2])**
-
- ・ 承認されてから2年間の作業

[1] Verifiable Credentials' WG new charter

<https://w3c.github.io/vc-wg-charter/>

[2] Standardization of Multilingual Support

<https://github.com/w3c/vc-wg-charter/issues/19>



Verifiable Credentials周りのホットトピック・課題

- Integrity Protection: JWT か LDP か？
- Credential Walletのデザイン
- トランスポート
- 選択的開示 (SD-JWTの登場)
- Holder Binding
- 既存のトラストフレームワークとの関係

- **ドメイン知識とスキーマ → Open Badges 3.0?**
 - **W3C CCG VC-EDU Plus Fest**
- **多言語化 → Verifiable Credentials 2.0 で議論予定**

採択されたプロジェクト（令和4年度Trusted Webユースケース実証事業）

Trusted Workplace Solution by TTEC and CG	ワークプレイスの信頼できる電子化文書の流通システム	文書(IoT)
電通・ISID パブリックDXコンソーシアム	中小法人・個人事業者を対象とする補助金・給付金の電子申請における「本人確認・実在証明」の新しい仕組み	行政
工業会証明書デジタル化コンソーシアム	法人税制と工業会証明書	行政
人材育成のためのTrustedな学修情報流通システム開発コンソーシアム	人材育成のためのTrustedな学修情報流通システム	個人（人材スキル）
SSI/FIDOコンソーシアム	学修歴等の本人管理による人材流動の促進	個人（人材スキル）
メタバース×自己主権型IDコンソーシアム	仮想現実空間におけるサービス利用資格と提供データのTrust検証	個人（メタバース）
株式会社DataSign	オンラインマーケティングにおけるパーソナルデータの流通	個人
大日本印刷株式会社	共助アプリにおけるプラットフォームを超えたユーザートラストの共有	個人
株式会社ORPHE	下肢運動器疾患患者と医師、研究者間の信用できる歩行データ流通システム	ヘルスケア
ヘルスケア情報流通システム開発コンソーシアム	臨床試験及び医療現場における信頼性及び応用可能性の高い情報流通システム	ヘルスケア
DataGateway PTE LTD	分散型IDを活用した炭素排出量トレースシステム	サプライチェーン(CO2)
ヤンマーホールディングス株式会社	機械製品サプライチェーンにおけるトレーサビリティ管理	サプライチェーン
アラクサラネットワークス株式会社	Trusted Networkによる社会ITインフラの信頼性・強靱性向上の実現	サプライチェーン



Open Badges [1]

- 学習歴を示すための仕掛け
 - もともとWebサイトに貼れる【バッジ】としてデザインされていた
 - 昨今話題の「リスキリング」等に向けての重要な要素と言われる
- 国際的に広く用いられている

「オープンバッジ・ネットワーク」サイトの説明から[1]

リスキリングの時代といわれるようになりました。人生は100年と長期化する一方、時代の変化は加速するという中で、20歳前後の一時期にどの教育機関で学んだということだけでは、一生対応していくことに限界があるということが背景にあります。

そのニーズにこたえるための学びの手段も、インターネットの普及によって実にさまざまな形で提供されるようになりました。また、その学びの単位も学位のような体系化されたものから、仕事をしながら学べるマイクロラーニングのようなもので多種多様になっています。それらを学習者自身で**いろいろ組み合わせ、知識やスキルを身につける**ことができるようになってきているのです。

しかし、多種多様で個性的に組み合わせたスキルには一律的な名称がありません。そこで、それらの**学習歴**をわかりやすく明示する、つまり、**可視化**する必要性が生まれてきているのです。

オープンバッジは、人の目にもコンピュータにも**可視化**された「**学習歴**」として、重要な役割をになうと私たちは考えています。

[1] 一般社団法人 オープンバッジネットワーク <https://www.openbadge.or.jp/about-ob>

Open Badges の問題

- そもそも、Webページに貼る【バッジ】としてデザインされており、何らかの改竄防止のメカニズムは無かった
- 後日、改竄防止のメカニズムが追加されたが、ほぼ、使われなかった
- プライバシー視点や、検証可能性の点で問題があった

Open Badges 3.0 [1]

- Verifiable Credentials ベースでの検証メカニズムを取り入れた形で発展した
- Verifiable Credentials ベースの教育や職歴領域におけるデータモデル標準として、データモデルと発行者API等、必要な機能が網羅されている

VC-Edu PlugFest 2

- 2022年11月14日に、W3C CCG の VC-EDU と JFF の主催で、VCについての、2回目のInteroperability PlugFest が行われた[1]
- サンフランシスコベイエリア(Mountain View)にあるコンピュータ歴史博物館で実施
- 150名の参加者
- プロトコル
 - Verifiable Credential API (VC-API) [2]
 - Credential Handler API (CHAPI) [3]
 - OpenID Connect [4]
 - DIDComm v2 [5]
 - Open Badges 3.0 [6]

vc-ed

Verifiable Credentials for Education Task Force

[View the Project on GitHub](#)
w3c-ccg/vc-ed

JFF & VC-EDU

Interoperability Plugfest 2

August-November 2022

Demo Event: November 14, 2022 (9 am Pacific Time) - Computer History Museum, Mountain View, CA, USA

The purpose of this event is to issue W3C Verifiable Credentials in the Open Badges v3 format and Decentralized Identifiers to wallets using protocols that are popular in the education and workforce ecosystem.

Kick-Off Meeting September 14, 2022

- [Slides](#)
- [Zoom Recording](#) passcode: 6U+e#p%M

- [Requirements](#)
- [Participation Overview](#)
- [Frequently Asked Questions](#)
- [Example Badges](#)
- [Resources](#)

[1] JFF & VC-EDU Interoperability Plugfest 2 <https://w3c-ccg.github.io/vc-ed/plugfest-2-2022/>

[2] Verifiable Credentials API <https://w3c-ccg.github.io/vc-api/>

[3] Credential Handler API 1.0 <https://w3c-ccg.github.io/credential-handler-api/>

[4] Welcome to OpenID Connect <https://openid.net/connect/>

[5] DIDComm Messaging v2.x Editor's Draft <https://identity.foundation/didcomm-messaging/spec/>

[6] Open Badges Specification - Candidate Final Spec Version 3.0 https://1edtech.github.io/openbadges-specification/ob_v3p0.html



Plug Fest の結果

ドラフト報告書をプレゼンしました
最終報告書でないので配布資料から割愛させていただきます

国内での課題

- ・ 海外はどんどん進んでいる状況
- ・ VCを使う場合のスキーマの国内での合意 -> 海外との整合性
- ・ マルチリンガル
- ・ VC 1.1 vs VC 2.0
 - ・ 今やりたいとすると VC1.1 になるが、将来的にはマイグレーション必要
 - ・ インターオペラビリティが無い。
 - ・ OpenBadges は VC 2.0 に合わせて行くはず
 - ・ Evidence の表現方法への議論がある