

VCの規格分裂の歴史(W3C VC/mDoc/SD-JWT)

公開: 2025/05/14 | Zenn (idroit-community)

Verifiable Credentials(VC)について調べる上で、W3C VC(JSON-LD), SD-JWT, mDoc/mDLといった主に3種類の規格について聞いたことがある人がいるかもしれません。現在、VCの規格としてこの3つが乱立・分裂しており、これからどの規格が軸となり運用されるのか、もしくは何らかの統合がなされ丸く治まるのか予測できない状況にあります。

今回はそれらの3つの規格が生まれた背景について説明することで、これから先の動向を予測する上で何らかの足掛かりにさせていただけたらと思います。本記事はあくまで私の主観に基づいた解釈です。間違っていることも往々にあるため、その際はご指摘いただければと思います。

各規格の概要

W3C Verifiable Credentials(JSON-LD)

- **主導組織:** Web技術の標準化団体であるW3C(World Wide Web Consortium)や大学などの教育機関
- **誕生の経緯:** インターネット上のアイデンティティ(デジタルアイデンティティ)の問題解決のために、自分でコントロール可能な証明書を提案
- **特徴:** JSON-LD(Linked Data)モデルを用いたWeb中心のアプローチ

ISO/IEC 18013-5 mobile credentials(mdoc / mDL)

- **主導組織:** 主に米国政府やApple, Googleなどの米国企業主導
- **誕生の経緯:** W3CのJSON-LDベースのVCの標準化と同時期に並行して、全く別の標準として議論が進む
- **特徴:** ISO標準なためクローズドな標準。

SD-JWT

- **主導組織:** インターネットの通信規格標準化団体であるIETFや、OIDCなどの認証技術標準化団体であるOpenID Foundationが主導
- **誕生の経緯:** 方向性の違いによりW3CのJSON-LDから分裂する形で規格化
- **特徴:** シンプルで扱いやすいデータフォーマット

技術的な違い

W3C VC (JSON-LD)、ISO mDL/mdoc、SD-JWTの3つの技術的な違いをまとめました。

比較項目	W3C VC (JSON-LD)	ISO mDL/mdoc	SD-JWT
データ形式	JSON-LD (Linked Data)	CBOR (バイナリエンコード)	標準JSON (JWT Claims)
署名方式	Linked Data Proof または JWS	COSE署名 (X.509証明書ベース)	JWS署名 (JWT標準)
選択的開示	BBS+署名など (ゼロ知識証明)	ハッシュ化された属性+エフェメラルキー使用	Salt付きハッシュ

歴史

これらの分裂の経緯には、かなり政治的な狙いや主導する団体の背景が絡んでいるため面白いです。

【図】 VC規格分裂の年表

2015～2018年: 初期の議論開始

ブロックチェーン技術が運用されるにつれて、その応用技術としての検証可能な証明書やトークンのような技術に注目が集まるようになりました。W3Cコミュニティで「Verifiable Claims」を標準化しようという初期議論が始まり、**2017年Verifiable Credentials Working Groupが設立**されました。その一方で、**全く別軸の議論として米国を中心としたISOで運転免許証(mDL)のモバイル化に向けた規格検討がスタート**しました。米国では特に自動運転技術の発展に伴い、mDLのようなデジタルの免許証の議論が加速したと思われます。それぞれの規格は各地で実証実験が行われるようになりました。

2019年: W3C VC Data Model 1.0が正式勧告

W3C Verifiable Credentials Data Model 1.0が正式にW3C標準になりました。W3C VCは**Linked Data (JSON-LD)**を採用し、**@context**により意味論(セマンティクス)を外部参照する仕様を用います。

ウェブページの情報を機械可読可能にするため、**データの意味論(セマンティクス)を重視するセマンティック・ウェブの流れを踏襲**していると考えられます。例えば、VCに **name** という項目に **山田太郎** というデータがあったとして、それが証明書における所有者の名前なのか、はたまた委任者や代表者の名前なのか、解釈が割れてしまいます。

2020年: コロナ禍におけるデジタル証明書需要急増

コロナ禍に入り、ワクチン証明書などのデジタル証明書の需要が急増しました。さらに、この頃から陰謀論やインターネット上の情報の信頼性に関して関心が高まり始めました。

VC利用の急速な拡大に伴い、この頃からシンプルで使いやすさを追求したデータフォーマットが重視され始め、W3Cの中でも意見の分裂が始まります。

2021年: ISO/IEC 18013-5:2021(mDL)が正式発行

モバイル運転免許証の正式国際規格としてISO/IEC 18013-5が発行されました。Apple Wallet や Google Wallet がこの規格を採用してmDL格納を開始します。また、米国TSA(運輸保安庁)が空港でのmDL使用実証をスタートしました。

2022年頃: IETFのSD-JWTドラフト登場

W3C VCから分裂する形でIETF OAuthワーキンググループにて**Selective Disclosure for JWT (SD-JWT)** の策定が本格化していきます。SD-JWTではJSON Web Token (JWT) に選択的開示機能を追加することで、VCを簡単に発行・検証できる形式を取ります。既存のJWTライブラリやOAuth 2.0/OIDCインフラとの親和性が高く、開発者にとって扱いやすいのが特徴です。また、W3C VCのような@context も不要です。IETFのようなインターネットのプロトコルを支えてきた組織にとって、難解で学習コストの高い技術が廃れてきた歴史から、よりシンプルで扱いやすい仕様を好むのは腑に落ちます。

また、この頃同時にOpenID FoundationでOpenID4VCI（発行）、OpenID4VP（提示）プロトコルもドラフト化されました。

一方で、EUがeIDAS 2.0案を発表しました。eIDAS 2.0においてデジタル署名やタイムスタンプを元にしたEU全域でのデジタルIDとトラストサービスの枠組みを広め、EU Digital Identity Wallet(EUDIW)の導入を義務付けました。EUDIWではW3C VCとISO mDL、SD-JWTに対応する方針を打ち出しています。eIDAS 2.0とEUDIWに関しては今度記事にする予定です。

2023年～現在: 米国(Apple, Google) vs EU

このようにW3CからスタートしたVC規格が広まる一方で、米国政府は頑なにmDoc/mDL形式のみを推奨しています。米政府は「ベンダー独自仕様で国家IDがコントロール不能になること」を本気で嫌っており、国家レベルでの「ID標準の支配権を守りたい」という広い安全保障的な背景がみて取れます。

米国政府の狙い

あくまで身分証明書を発行するのは国です。AppleやGoogleが身分証明書を発行する権限を勝手に取り、独自路線に走るなどは米政府にとっては許し難いことでしょう。また、安全保障の面からも、身分証のコントロールをしたいという思惑が読み取れます。

なので、米国行政手続きにおけるガイドラインでもあるNISTや、米運輸保安庁(TSA)・アメリカ合衆国国土安全保障省(DHS)などの運送や交通に関する機関を中心とした政府がmDoc/mDLを推奨しています。米政府は、Appleに対して「ISO 18013-5準拠」で実装するよう強く促しています。そのため、**Apple Walletに格納されるmDL（モバイル運転免許証）は、州政府発行であること、州政府管理のPKI署名、ISO 18013-5互換データ構造であることが絶対条件**になっています。

EU方面からの圧力

一方でEUが推進するeIDAS 2.0のEUDI Walletにおいて、**SD-JWTとmDocのサポートを必須**としています。そのため、**AppleもGoogleもeIDAS 2.0／EUDI Wallet要件に適合しないとヨーロッパ市場でのID連携ができなくなるため、危機感を持って動いている**ようです。

- **Google**
 - 2024年後半に「Google WalletがW3C VC形式のVerifiable Credentialsを保存・提示可能にする」計画があると表明。
 - OpenWallet Foundation（OWF）にも参加し、W3C準拠VC仕様への対応を進める。
- **Apple**
 - Appleは公式発表ではないが、EUDI Wallet要件対応のためにVCベースの証明書管理機能を検討している。

相互運用性確保への動き

技術的・政治的な分裂はありましたが、現在は「競争」から「相互運用性重視の協調」への動きがあります。

- **デュアルフォーマット（複数形式）対応**
 - 発行者（例: 政府）がW3C VC版とISO mDL版の両方の証明書を同時に発行。
- **プロトコルの共通化（OpenID Connectベース）**
 - 証明書の形式は異なっても、検証者とウォレットの間の通信プロトコルは共通化。
- **W3C VC 2.0の「エコシステム互換性」ガイドライン**
 - 外部フォーマット（ISO mDL, SD-JWTなど）をW3C VC形式にマッピング（変換）できる手引きを用意。

出典: <https://zenn.dev/idroit/articles/baef7e459d9805>