2026 年 7 月 31 日　全 18 頁

デジタルアイデンティティ・デジタルクレデンシャルをめぐる取組みと実装技術の論点整理（第 3 部／全 3 部）

VC 実装方式の技術整理と日本のデジタル基盤への考察

イノベーション企画部　　シニア IT リサーチャー　大橋 哲行

[要約]

- 本レポートシリーズは、デジタルアイデンティティの導入・実装の判断を支えることを目的に、各国の取組みと実装技術の両面から論点を整理してきた。第 3 部では、第 2 部までに浮かび上がった VC 実装方式（SD-JWT VC、mdoc、VCDM 等）を体系的に整理・比較し、第 2 部で示した日本の論点を技術観点から改めて考察する。

- VC（Verifiable Credentials：検証可能なクレデンシャル）実装に関する技術標準は、大きく「フォーマット」（VC のデータモデルとセキュリティの仕組みを規定）と「プロトコル」（発行・提示手順を規定）に分けられる。フォーマットには、IETF が策定する SD-JWT VC、ISO/IEC が策定する mdoc、W3C が策定する VCDM の 3 系統の代表的な仕様があり、規定範囲や設計思想が異なる。

- SD-JWT VC は Web 技術との親和性を重視する JSON ベースの柔軟な設計、mdoc は対面・近接通信での本人確認を重視した一体的な設計、VCDM はデータモデルのみを規定する柔軟な設計であり、DID と組み合わせて多様な応用に展開されている。

- 各方式は、ユースケースの特徴と適合関係を持ち、各国の技術選択もこの関係を反映している。EUDI ウォレット（EU Digital Identity Wallet）の共通仕様も 3 方式すべてに対応可能として位置づけており、単一方式への統一ではなく、複数方式の並立を前提とした相互運用が国際的な方向性として見られる。

- 日本では mdoc を活用した公的 ID のデジタル基盤の実用化が進んでいる。今後は、この基盤の発展と並行して、資格・卒業証明、社員証等、民間分野での柔軟性の高い他の方式を主とした取組みの蓄積が重要となる。こうした蓄積により、利用者が自ら管理・提示できる VC が多様な分野に広がることで、利用者起点の情報制御が着実に拡張されていく。これは国際的な相互運用の方向性にも親和的であり、技術進化が続く本分野において、変化への対応力を高める基盤となる。

株式会社大和総研 本社　〒135-8460 東京都江東区冬木 15-6

はじめに

本レポートシリーズは、デジタルアイデンティティの導入や実装を検討する際の判断を支えることを目的に、各国の取組みと実装技術の両面から論点を整理するものである。第 1 部ではデジタルアイデンティティの基本概念と VC（Verifiable Credentials）の仕組みを整理し、EUDI ウォレットに見る制度化・実装の動向を俯瞰した[1]。第 2 部では欧州 4 カ国と日本の取組みを比較し、日本にとっての論点を提示した[2]。

第 3 部（本レポート）では、第 2 部を通じて浮かび上がった VC 実装方式の多様性を掘り下げる。VC 実装に関する技術標準の全体構成を整理した上で、SD-JWT VC、mdoc、VCDM を取り上げ、それぞれの出自や特徴を紹介する。その上で、これらを観点ごとに横断的に比較し、第 2 部で提示した日本の論点を技術観点から改めて考察する。「取組み」と「実装技術」を接続した体系的な論点整理を通じて、シリーズの完結を目指す。

図表 1　本レポートシリーズの構成

第1部	• デジタルアイデンティティ、デジタルクレデンシャルの基本概念 • 欧州におけるEUDIウォレットの取組み
第2部	• 欧州各国の取組み • 日本における取組みと各国取組みの特徴整理
第3部	• デジタルアイデンティティを実現する技術標準の概要 • 技術標準の整理･比較

（出所）大和総研作成

1. VC 実装に関する技術標準の構成

第 2 部までに見てきた各国の取組みでは、SD-JWT VC、mdoc、VCDM、DID 等複数の技術的な仕様が登場した。これらは「VC の実装方式」として並列的に語られることが多いが、実際には仕様としての規定範囲や役割が異なる。本章では、具体的な方式の解説に入る前に、これらの全体構成を整理し、各仕様が「何を規定するものか」を確認する。

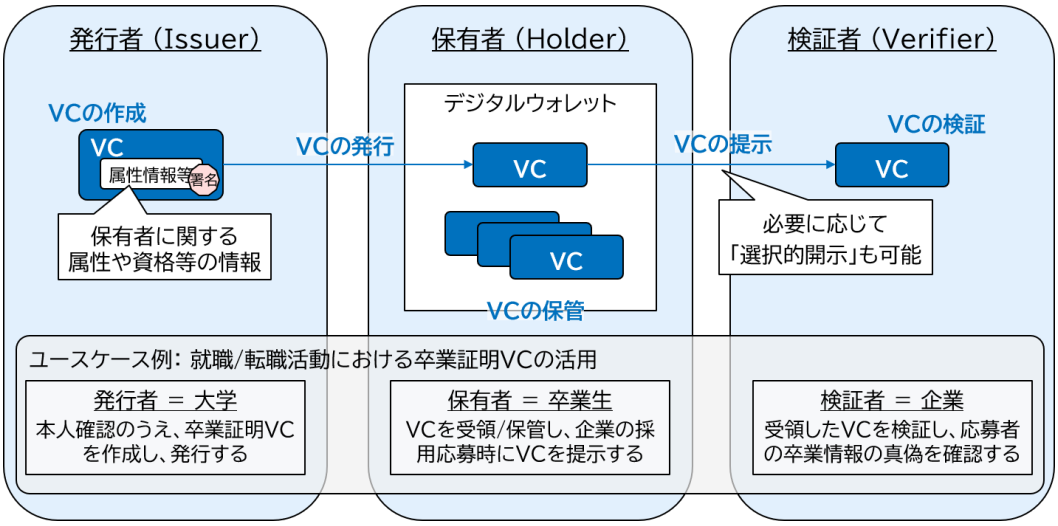
[1] 第 1 部については、大橋哲行「デジタルアイデンティティ・デジタルクレデンシャルをめぐる取組みと実装技術の論点整理（第 1 部／全 3 部）」（大和総研レポート、2026 年 5 月 14 日）を参照

[2] 第 2 部については、大橋哲行「デジタルアイデンティティ・デジタルクレデンシャルをめぐる取組みと実装技術の論点整理（第 2 部／全 3 部）」（大和総研レポート、2026 年 6 月 25 日）を参照

(1) VC 実装の検討ポイント

まず、VC の基本的な仕組みを振り返る。第 1 部で示した通り、VC は発行者（Issuer）・保有者（Holder）・検証者（Verifier）の三者モデルを前提とし、発行者が保有者の属性等を記載した VC を作成・発行し、保有者がデジタルウォレットで保管した上で、必要に応じて検証者に提示する仕組みである（図表 2）。

図表 2　Verifiable Credentials と三者モデル



（注）大橋（2026）（脚注 1）の図表 4 を再掲
（出所）各種資料より大和総研作成

この仕組みを実装するには、VC をどのような形式で表現し、そのセキュリティ（署名・検証の仕組み）をどう担保し、発行・提示をどのような手順で行うか、といった要素をそれぞれ具体化する必要がある。

(2) VC 実装に関する技術標準の全体構成

これらの要素については、複数の標準化団体がそれぞれ仕様を策定しており、各国の取組みで採用されている実装も、これら仕様の組み合わせで構成されている。図表 3 に、VC 実装に関わる主な仕様の構成を整理した。仕様は大きく、VC のデータモデルとセキュリティを規定する「フォーマット」と、発行・提示の手順を規定する「プロトコル」に分けられる。

フォーマットには、Internet Engineering Task Force（IETF）が策定する SD-JWT VC[3]、ISO/IEC が 18013-5 として策定する mdoc[4]、World Wide Web Consortium（W3C）が策定する

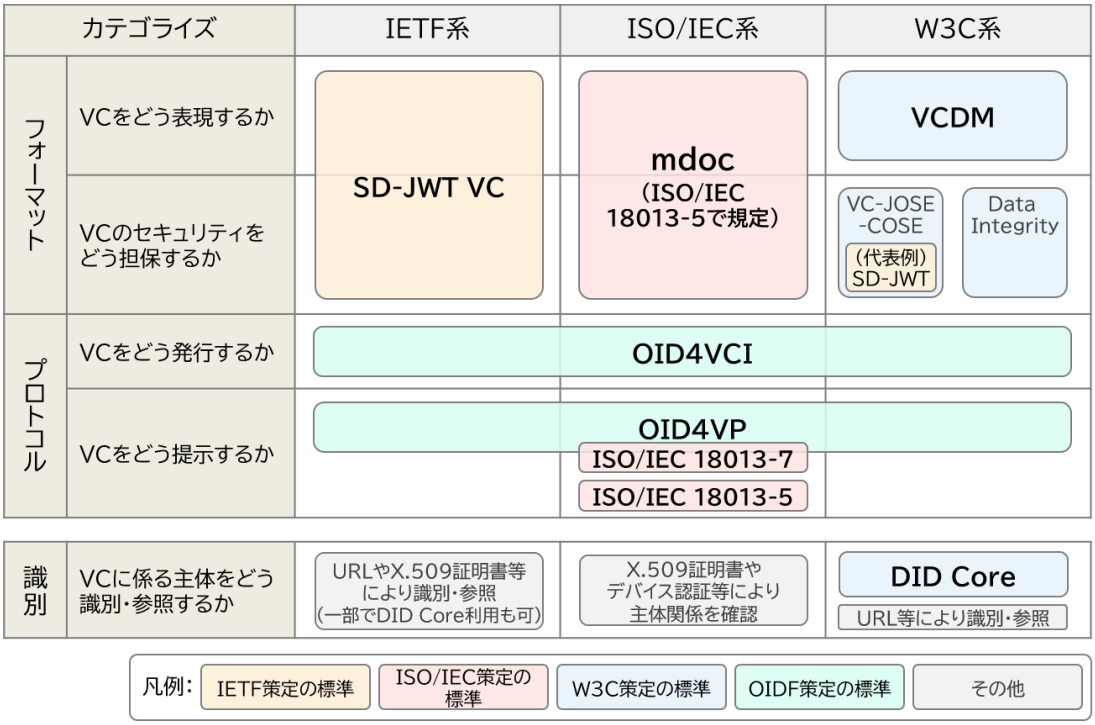
[3] IETF “draft-ietf-oauth-sd-jwt-vc-17 - SD-JWT-based Verifiable Digital Credentials (SD-JWT VC)”（2026 年 7 月 6 日更新）

[4] 本レポートにおける ISO/IEC の mdoc に関する記述については、ISO 公式ページで公開されている規格名、Abstract、ステータス情報に加え、関連する公的資料・公開仕様に基づいて整理した。主な参考資料として、AAMVA “AAMVA mDL Implementation Guidelines”（2025 年 5 月）や EU “European Digital Identity Wallet - Architecture and Reference Framework”（2026 年 5 月 21 日）等がある

Verifiable Credentials Data Model（VCDM）[5]という 3 系統の代表的な仕様が存在する。これらは「VC をどう表現するか」と「VC のセキュリティをどう担保するか」のそれぞれを、どこまで規定するかで構造が異なる。

SD-JWT VC と mdoc はデータモデルとセキュリティを一体的に規定するのに対し、VCDM はデータモデルのみを規定し、セキュリティは関連仕様に委ねる構造を採る。関連仕様には、VC 全体を署名情報で包む「包み込み式」の VC-JOSE-COSE[6]と、VC 内部に署名を直接埋め込む「包含式」の Data Integrity[7]の 2 系統がある。VC-JOSE-COSE では、IETF で策定された SD-JWT も署名技術として活用される。

図表 3　VC 実装に関する技術標準の構成



（注）「識別」カテゴリは、DID Core の位置づけを示すための補助的な観点として整理したものであり、各仕様の詳細には踏み込まず、汎化した記載としている
（出所）各種資料より大和総研作成

プロトコルには、フォーマット非依存の仕様として、OpenID Foundation（OIDF）が策定する OID4VCI[8]（発行手順）と OID4VP[9]（提示手順）がある。これらは SD-JWT VC、mdoc、VCDM のいずれのフォーマットも扱える。

[5] W3C “Verifiable Credentials Data Model v2.0”（2025 年 5 月 15 日）
[6] W3C “Securing Verifiable Credentials using JOSE and COSE”（2025 年 5 月 15 日）
[7] W3C “Verifiable Credential Data Integrity 1.0”（2025 年 5 月 15 日）
[8] OIDF “OpenID for Verifiable Credential Issuance 1.0”（2025 年 9 月 16 日）
[9] OIDF “OpenID for Verifiable Presentations 1.0”（2025 年 7 月 9 日）

加えて mdoc については、mdoc フォーマットを規定する ISO/IEC 18013-5 自身が対面・近接通信による提示手順を併せて規定している。また、オンライン提示については、同シリーズの ISO/IEC 18013-7 で対応しており、OID4VP をプロファイルする（用途に合わせて調整する）形で利用している。これらにより、mdoc は利用形態に合わせて最適化された実装が可能となっている。

なお、フォーマットとプロトコルに加えて、W3C は関係主体を識別する分散型の識別子である DID（Decentralized Identifier）に関する仕様（業界通称「DID Core」）を策定している[10]。DID は VCDM と組み合わせて用いられることが多く、両者を併せて「DID/VC」と呼ばれることも多い。ただし、DID は特定のフォーマットに紐付くものではなく、他のフォーマットと組み合わせて利用することも可能である。

以上の全体構成のうち、ユースケースに応じた技術選択の中心となるのは、複数の標準が並立しているフォーマットである。そこで以降では、フォーマットに焦点を絞って解説を進める。

(3) VC フォーマットの仕組み

フォーマットは、「VC をどう表現するか」と「VC のセキュリティをどう担保するか（署名・検証の仕組み）」の 2 つを規定する。本節では、各フォーマットの個別解説に入る前に、この 2 点について、フォーマットに共通するイメージを確認する。

VC のデータ構造

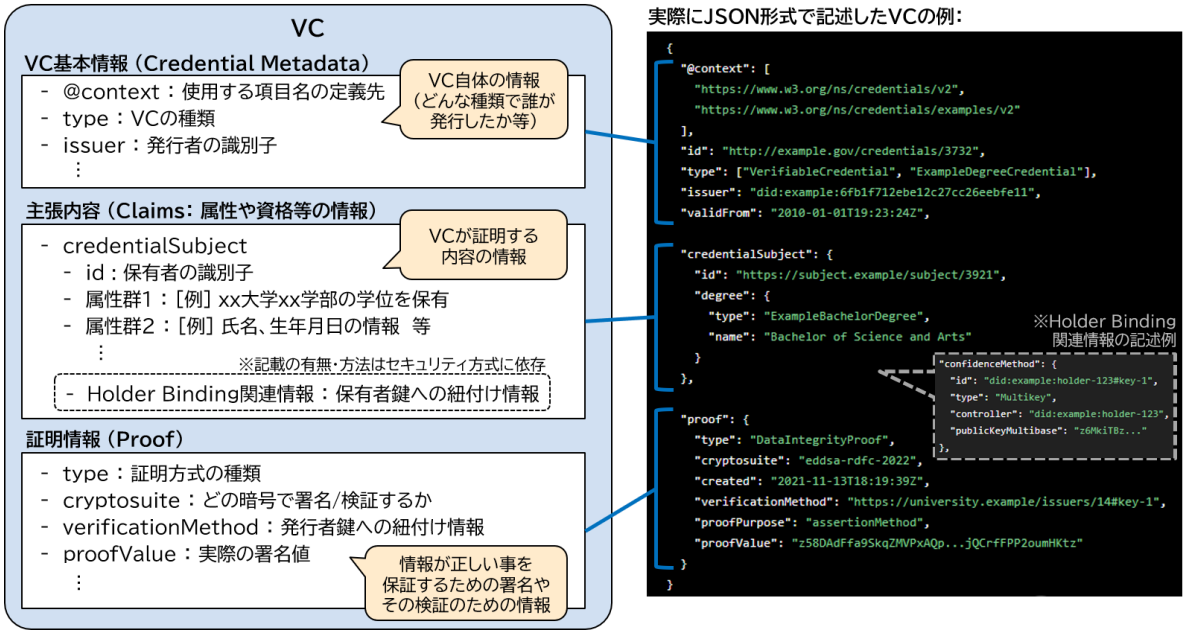
ここでは、VC フォーマットの中で最初に策定された VCDM を例として取り上げる。VCDM は JSON 形式で記述され、他のフォーマット（SD-JWT VC、mdoc）にも通底する基本的な構成要素を備えている。図表 4 に、VCDM を例として、VC がどのような要素で構成され、実際に JSON 形式でどのように記述されるかを示した。

VCDM の規定する VC は、大きくは 3 つの構成要素で表現される。VC 基本情報（Credential Metadata）で、VC の種類や発行者等の基本情報を示し、主張内容（Claims）で、保有者に関する属性や資格等の情報を、証明情報（Proof）で、VC の真正性を担保する署名情報を示す。それぞれの構成要素には”@context”, ”type”といった複数の項目が含まれ、図表 4 には代表的な項目を例として示している。なお、保有者との紐付け（Holder Binding）に用いる情報が、実装によっては主張内容に含まれる場合がある。

ここで示した 3 つの構成要素に相当する概念は、他のフォーマット（SD-JWT VC、mdoc）にも存在するが、それらの構造や表現形式はフォーマットによって異なる。

[10] W3C ”Decentralized Identifiers (DIDs) v1.1”（2026 年 3 月 5 日）

図表 4　VC のデータ構造（VCDM の例）

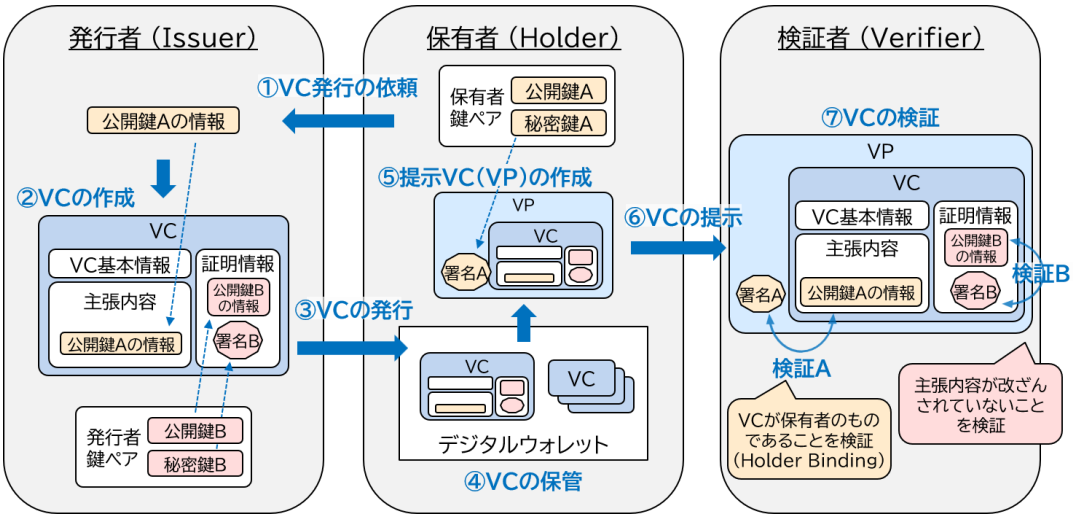


（注）図の証明情報（Proof）部分は Data Integrity による例（VC 内部に署名を直接埋め込む包含式）。JSON 形式の記述例は W3C VCDM v2.0（脚注 3）Example 15 を参考に、説明用に一部簡略化
（出所）各種資料より大和総研作成

VC のセキュリティ

続いて、VC のセキュリティの仕組みを説明する。VC のセキュリティは、主に公開鍵と署名を用いた仕組みによって担保されている[11]。ここでは、その仕組みの大枠を掴んでいただくため、図表 5 に示す基本的な流れをもとに、VC の発行から検証までの過程を解説する。

図表 5　VC の発行から検証までの流れ（公開鍵と署名の観点）



（注）図は基本的な VC 利用の流れを示したもので、方式や実装により細部は異なる。例えば、保有者の証明には署名以外の方法が用いられる場合もあり、利用形態によっては省略されることもある
（出所）各種資料より大和総研作成

[11] 本レポートでは、公開鍵暗号による署名と検証の仕組みは既知のものとして扱い、詳細には立ち入らない

この仕組みでポイントとなるのは、発行者と保有者がそれぞれ持つ鍵ペアである。まず、保有者は自身の鍵ペア（公開鍵 A と秘密鍵 A）を生成し、VC の発行を依頼する際、公開鍵 A の情報（公開鍵そのもの、またはその参照情報等）を発行者に伝える。発行者は VC を作成する際、この公開鍵 A の情報を VC 内に含めることで、保有者との紐付け（Holder Binding）を実現する。併せて、発行者は自身の秘密鍵 B を用いて VC に署名 B を付し、その検証に使う公開鍵 B の情報（公開鍵そのもの、または参照情報等）と併せて証明情報に含める。

VC の提示に向けては、保有者の秘密鍵 A で署名 A を付し、VC を含めた提示用のデータ構造（VP：Verifiable Presentation）を作成する[12]。この時、元の VC に含まれる属性等の情報のうち一部のみを開示する「選択的開示」に対応した VP を作成することもできる。

検証者は、VP を受け取ると、2 種類の検証を行う。1 つ目は、署名 B と発行者の公開鍵 B による検証で、VC が正当な発行者によって発行されたものであり、内容が改ざんされていないことを確認する。2 つ目は、VP の署名 A と VC 内の公開鍵 A による検証で、VC を提示している者が、VC の正当な保有者であることを確認する（Holder Binding 検証）。

以上が、公開鍵と署名によって VC のセキュリティを担保する基本的な仕組みである。セキュリティに関連する観点は、各フォーマットの特徴を左右する重要な要素となる。

次章以降では、各フォーマットの特徴を解説する上で、Holder Binding、選択的開示、信頼の起点、非リンク性という 4 つの観点を軸とする。前二者は本節の説明でも触れたが、残る信頼の起点と非リンク性については、ここで補足しておく。

信頼の起点は、検証者が発行者を信頼するために依拠する根拠を指す。信頼性の高い認証局（Certificate Authority：CA）を頂点とする階層的な信頼チェーンを介するモデル（従来の電子署名基盤と同じ考え方）と、発行者自身を直接信頼するモデルの 2 つがあり、フォーマットによって、どちらのモデルを採用するかが異なる。前者は基盤構築の手間はかかるが、広範な信頼を一括で確保できる。後者は構築が容易な一方、発行者ごとに信頼確認が必要となる。

非リンク性は、同一の保有者による複数の提示が同一人物のものと結び付けられない性質を指し、保有者の行動追跡を防ぐ観点で重要となる。

これら 4 つの観点は、フォーマット（SD-JWT VC、mdoc、VCDM）や関連仕様によって対応の有無や仕組みが異なる。次章では、この違いを念頭に、各方式の出自や特徴について解説していく。

[12] VP（Verifiable Presentation）は VCDM 由来の用語であり、他フォーマットでは異なる呼称・構造（mdoc の DeviceResponse 等）が用いられる。ここでは代表として「VP」を用いる

2. 代表的な方式の解説（SD-JWT VC、mdoc、VCDM・DID/VC）

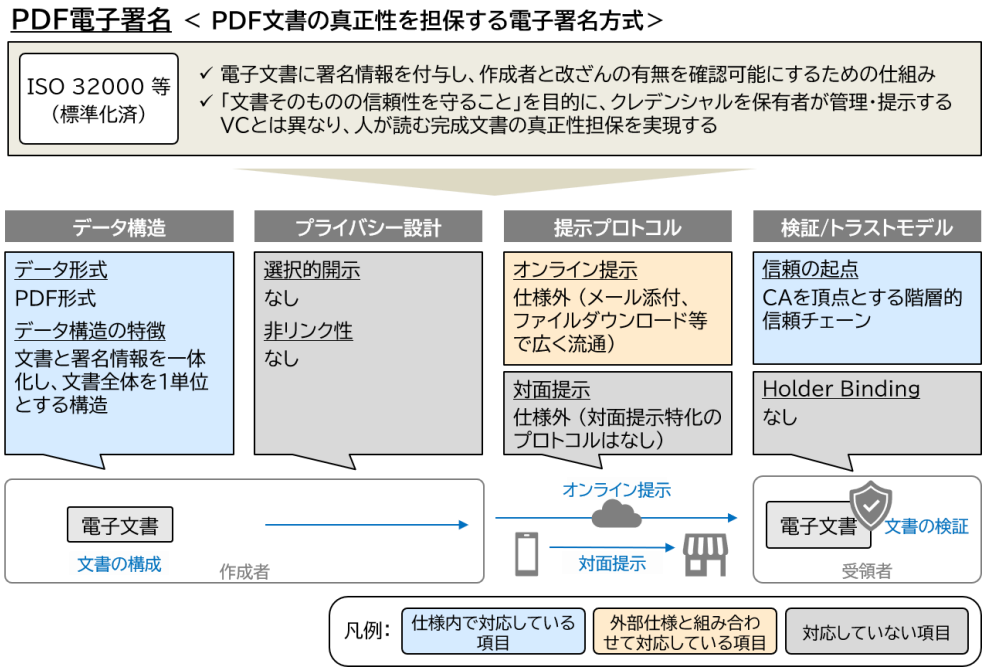
本章では、代表的な 3 つの VC フォーマット（SD-JWT VC、mdoc、VCDM）を取り上げ、それぞれの出自と特徴を解説する。併せて、これらの参照点として、従来から実用化されている PDF 電子署名[13]も取り上げる。

PDF 電子署名は電子文書への電子署名の仕組みであり、契約書等のデジタル化を含め幅広く利用されている。一方、これら 3 方式は、PDF 電子署名では対応が想定されていない、属性の選択的な提示や保有者との紐付け（Holder Binding）等を実現するために検討された、比較的新しい仕様である。両者を対比することで、VC が何を新たに実現しようとしているのか、その設計思想の違いを明確にしたい。

(1) PDF 電子署名

PDF 電子署名は 1990 年代から実用化され、契約書や各種証明書のデジタル化を支える基盤として広く社会に定着している。その設計は、電子文書の作成者と改ざんの有無を検証可能とすることに主眼を置き、従来の紙文書における「印鑑」や「サイン」のデジタル代替として位置づけられるもので、VC が目指す「保有者が主体的に情報を管理する」という発想は含まれていない。図表 6 に、以降で扱う 3 方式と同じフレームで、PDF 電子署名の全体像を示す。

図表 6　PDF 電子署名の出自と特徴



（出所）各種資料より大和総研作成

[13] 技術仕様としては、PDF フォーマット自体を規定する ISO 32000 シリーズに電子署名の基本仕様が含まれ、高度電子署名の拡張仕様として、ETSI により PAdES（ETSI EN 319 142）が策定されている。本レポートでは、これら仕様の総称として、分かりやすさを重視し「PDF 電子署名」と呼称する

代表的な特徴として、文書全体を単位として電子署名を付与する構造を持つ。この構造ゆえに、選択的開示や Holder Binding は設計上想定されていない。提示プロトコルは規定されず、メール添付やファイルダウンロード等の一般的な手段で流通する。信頼の起点は認証局（CA）による階層的信頼チェーンであり、既存の電子署名基盤をそのまま活用する形式となっている。

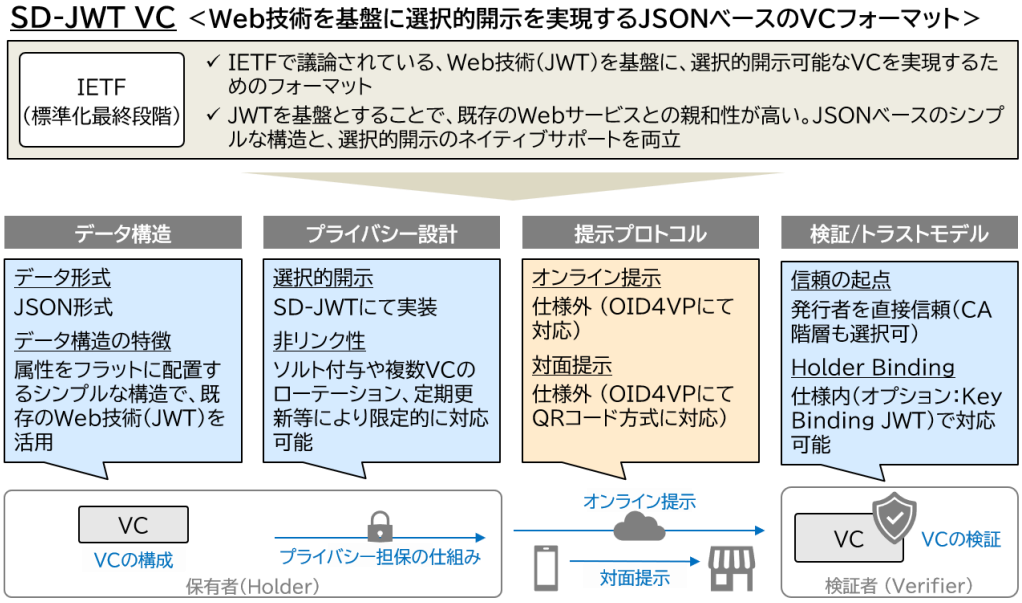
PDF 電子署名は「文書」を単位として真正性を担保する仕組みであるのに対し、SD-JWT VC、mdoc、VCDM の 3 方式は「クレデンシャル（属性や資格等の情報のまとまり）」を単位とする点で、根本的に設計思想が異なる。

(2) SD-JWT VC

SD-JWT VC は、IETF で議論されている VC フォーマットで、標準化に向けた最終段階にある。Web で広く使われるトークン形式である JWT（JSON Web Token）を基盤に選択的開示（Selective Disclosure）を実現する、SD-JWT[14]の仕組みを組み込んだ、JSON ベースのフォーマットである。

設計上の特徴は、Web 技術との親和性の高さにある。JWT は Web アプリケーションで広く使われており、既存の技術基盤やライブラリを活用しやすい。Web サービスのログインや権限管理で標準的に用いられる技術（OAuth2.0 等）と親和性が高く、Web サービスの延長線上で VC を扱える点に強みがある。

図表 7　SD-JWT VC の出自と特徴



（出所）各種資料より大和総研作成

仕様上の特徴として、選択的開示を直接規定している点が挙げられる。非リンク性については、属性ごとにランダムな値（ソルト）を加えてハッシュ化する仕組みにより、個々の属性の

[14] IETF “RFC 9901 - Selective Disclosure for JSON Web Tokens”（2025 年 11 月）

結び付きを防ぐ。加えて、複数 VC のローテーションや定期更新等による実装も可能である。ただし、同じ VC を繰り返し提示すると、複数の検証者の間でその提示が同一の保有者によるものと特定され得る限界がある。

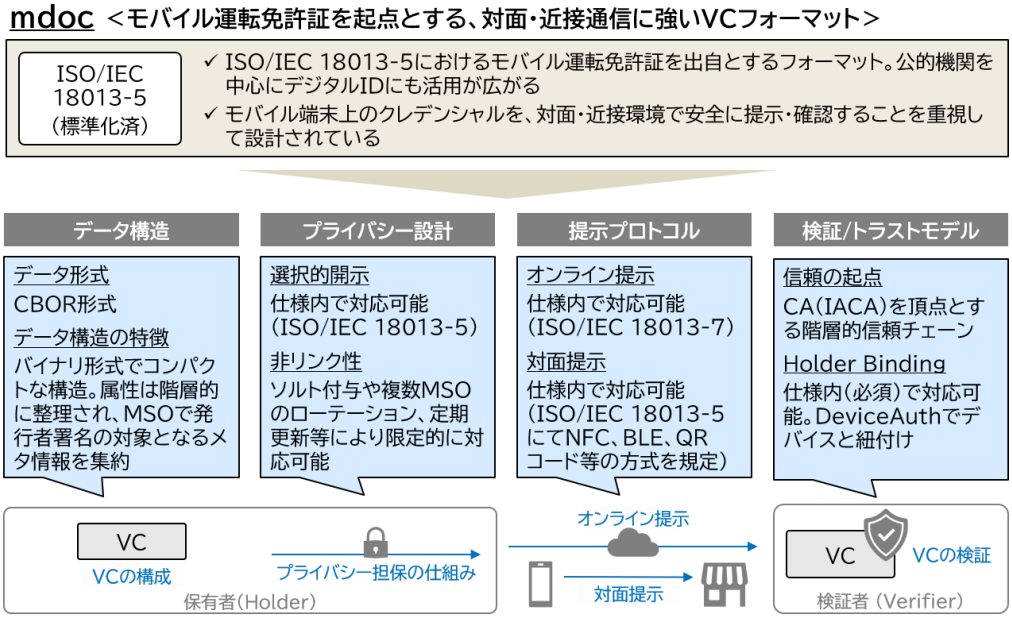
Holder Binding は、前章の図表 5 で示した保有者による署名（署名 A）の仕組み（Key Binding JWT と呼ばれる）が任意で仕様に含まれている。信頼の起点は発行者を直接信頼する形式が基本だが、CA 階層を採用することも可能で、両方の信頼モデルに対応可能である。提示プロトコルは仕様の範囲外で、OID4VP 等の外部仕様と組み合わせて利用される。関連仕様として、失効管理のための Token Status List、発行者検証のための JWT VC Issuer Metadata 等が策定されており、実装に必要な周辺機能の整備が進んでいる。

(3) mdoc（ISO/IEC 18013-5）

mdoc は、ISO/IEC が策定する VC フォーマットで、モバイル運転免許証（mDL）の国際規格である ISO/IEC 18013-5 として 2021 年に標準化された。mDL を出自とするフォーマットだが、その汎用性から、公的機関を中心に、本人識別情報等の各種デジタル ID への活用も広がっている。

設計上の特徴は、対面・近接環境での確実な本人確認を重視する点にある。データモデル、セキュリティ、提示プロトコルを一体的に規定する設計を採っており、対面・近接通信のプロトコル（NFC、BLE、QR コード等）を ISO/IEC 18013-5 で直接規定する。また、通信環境が限定的な場面での本人確認を想定し、信頼アンカーの事前配布によりオフラインでの検証にも対応する。加えて、オンライン提示についても ISO/IEC 18013-7 で規定されており、対面（オフライン環境を含む）とオンラインの双方を仕様内でカバーする点に強みがある。

図表 8　mdoc の出自と特徴



（出所）各種資料より大和総研作成

仕様上の特徴として、CBOR というバイナリ形式のエンコーディングにより、コンパクトなデータ構造を持つ。属性情報はグループごとに階層的に整理され、MSO（Mobile Security Object）と呼ばれるオブジェクトに、各情報項目（氏名や生年月日等の属性）のハッシュ値、保有者の鍵情報、有効期間等のメタ情報がまとめられ、発行者の署名で保護される。選択的開示は仕様内で対応する。非リンク性については、SD-JWT VC と同様に、属性ごとのソルト付きハッシュや複数 MSO のローテーション、定期更新等により対応する。信頼の起点は CA（IACA：Issuing Authority Certificate Authority）を頂点とする階層的な信頼チェーンである。Holder Binding は、前章の図表 5 で示した保有者による署名（署名 A）の仕組み（DeviceAuth と呼ばれる）が必須で仕様に含まれている。署名 A に用いる鍵はデバイス上での管理が想定されており、実装ではハードウェアによる強固な保護が採用される。関連規格として、mdoc を他のデジタル ID にも体系的に適用するための枠組みを規定する ISO/IEC 23220 シリーズが策定されており、mdoc の適用範囲を広げる動きが進んでいる。

(4) VCDM・DID/VC

VCDM は、W3C が策定する VC のデータモデルの仕様である。VC フォーマットの中で最も早く、初版が 2019 年に W3C 勧告として策定され、現行の VCDM 2.0 が 2025 年 5 月に勧告として策定された。早期からの標準化と柔軟な設計を背景に、教育・資格証明やサプライチェーン等、幅広い領域で応用が進んでいる[15]。

設計上の特徴は、データモデルのみを規定し、セキュリティや提示プロトコル等は関連仕様に委ねる柔軟性の高い設計を採る点にある。この設計により、多様な発行者・応用領域への適用が可能となる。

仕様上の特徴として、データ形式に JSON-LD を用いる。前章の図表 4 にも示した@context と呼ばれる項目に複数の項目定義（URL）を列挙することで、VCDM 基本項目に加え、他の共通項目や独自項目を組み合わせて記述できる。これにより、用途ごとの独自要件も標準の枠組みで表現でき、VCDM の拡張性を支えている。

選択的開示や非リンク性は仕様として規定せず、関連仕様（VC-JOSE-COSE、Data Integrity）を組み合わせて実現する。特に、Data Integrity にはゼロ知識証明（ZKP）方式[16]を用いる暗号スイートも規定されており、より高度な非リンク性を実現し得る。

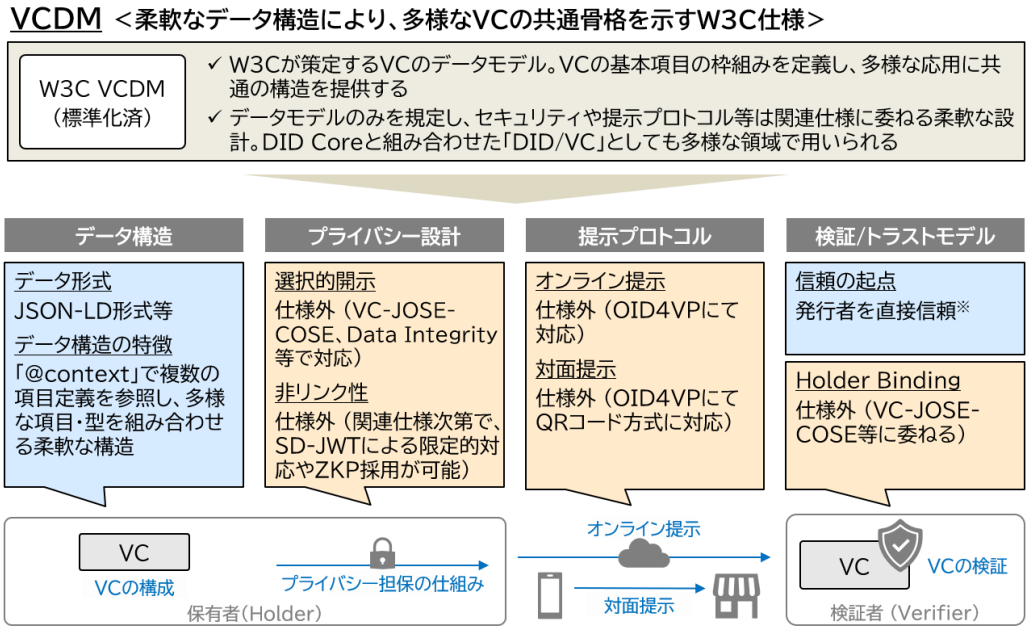
信頼の起点は発行者を直接信頼する形式が基本で、Holder Binding も関連仕様に委ねる。提示プロトコルも仕様の範囲外で、OID4VP 等の外部仕様と組み合わせて利用される。関連仕様

[15] 教育・資格証明分野の代表例として、1EdTech Consortium が策定する Open Badges 3.0（学習成果やスキルを証明するデジタルバッジの仕様）が VCDM 2.0 をベースに構築されている

[16] ゼロ知識証明（Zero-Knowledge Proof）：ある事実を、その事実以外の情報を明かさずに証明できる暗号技術。VC への応用では、生年月日などの属性値を開示せずに条件（成人であること）を証明する、同じ VC から提示毎に異なる証明を生成することで非リンク性を高める、といった使い方が可能

として、Recognized Entities[17]等の周辺仕様の策定も進んでおり、広い仕様群が VCDM を取り巻いている。

図表 9　VCDM の出自と特徴



（※）直接信頼の補完として、W3C では発行者や検証者等、エンティティの信頼性を第三者の VC で検証可能にする Recognized Entities の仕様が議論されている

（出所）各種資料より大和総研作成

VCDM は、同じく W3C が策定する DID Core と組み合わせて用いられることが多く、この組み合わせは「DID/VC」と呼ばれる。DID は、特定のプラットフォームや中央の管理者に依存しない分散型の識別子であり、識別子から公開鍵等の情報を取り出す仕組み（DID メソッド）が多様に用意されている。シンプルに公開鍵から生成する方式から、ブロックチェーンを活用した分散的な方式まで、様々な選択肢の中から用途に応じて選択できる。DID/VC は、こうした DID の柔軟性を活かして、発行者や保有者の識別子設計を用途に応じて最適化できる。VCDM の柔軟性を、識別子の観点からさらに補強する組み合わせといえる。

このように、各方式はそれぞれの背景と設計思想を持つ。特に、PDF 電子署名は「文書」を単位とする真正性の担保に主眼を置く仕組みであり、「クレデンシャル」を単位とする 3 方式とは根本的に異なる。続く第 3 章では、PDF 電子署名を除き、3 方式に焦点を絞って体系的に比較していく。

[17] W3C “Recognized Entities v1.0”（2026 年 5 月 12 日）

3. 方式間の体系的比較と考察

第 2 章では、SD-JWT VC、mdoc、VCDM の 3 方式を、参照点としての PDF 電子署名と合わせて解説した。本章では、これらを踏まえて 3 方式を横断的に比較し、各方式の特徴と用途との適合関係を整理した上で、第 2 部で提示した日本の論点に対する技術観点からの考察を行う。

(1) 機能・特徴の比較

本節では、SD-JWT VC、mdoc、VCDM の 3 方式を、「規定範囲と利用形態」「プライバシーとトラストモデル」「標準化と実装」の 3 つの観点から比較する。

規定範囲と利用形態

図表 10　規定範囲と利用形態の比較

項目		SD-JWT VC	mdoc（ISO/IEC 18013-5）	VCDM
規定範囲	データモデル	規定あり （JSON形式）	規定あり （CBOR形式）	規定あり （JSON-LD形式等）
	セキュリティ	規定あり （SD-JWTによる署名）	規定あり （COSEによる署名）	規定なし （VC-JOSE-COSE等の関連仕様に委ねる）
	提示プロトコル	規定なし （OID4VP等を利用）	規定あり （ISO/IEC 18013シリーズ）	規定なし （OID4VP等を利用）
利用形態	オンライン提示	仕様外 （OID4VPにて対応可能）	仕様内で対応可能 （ISO/IEC 18013-7）	仕様外 （OID4VPにて対応可能）
	対面/近接提示	仕様外 （OID4VPのQRコード方式で対応可能）	仕様内で対応可能 （ISO/IEC 18013-5のNFC、QRコード等の方式を規定）	仕様外 （OID4VPのQRコード方式で対応可能）
	オフライン検証	仕様外 （外部仕様でも対応は困難）	仕様内で対応可能 （ISO/IEC 18013-5）	仕様外 （外部仕様でも対応は困難）

凡例　青：仕様内対応 ― 各技術標準の仕様内で対応される項目
オレンジ：外部仕様対応 ― 各技術標準の外部仕様と組み合わせて対応される項目

（出所）各種資料より大和総研作成

規定範囲の観点では、3 方式で明確な設計思想の差が見られる。mdoc はデータモデル、セキュリティ、提示プロトコルのすべてを規定する一体的な設計、SD-JWT VC と VCDM は提示プロトコルを外部仕様に委ね、特に VCDM はセキュリティを含めた広い範囲を関連仕様に委ねる設計を採っている。この規定範囲の広さは、規格としての柔軟性と、一貫性のトレードオフを反映している。

利用形態の適性は、この規定範囲の差に直結する。mdoc は、対面・近接通信のプロトコル（NFC、BLE、QR コード等）を仕様内で規定し、オンライン提示・オフライン検証にも対応する。一方、SD-JWT VC と VCDM は、OID4VP 等の外部仕様と組み合わせることでオンライン提示に広く対応する。対面提示についても OID4VP がサポートする QR コード方式で対応可能だが、NFC や BLE による近接通信は仕様の対応外である。

プライバシーとトラストモデル

図表 11　プライバシーとトラストモデルの比較

項目		SD-JWT VC	mdoc（ISO/IEC 18013-5）	VCDM
プライバシー	選択的開示	仕様内で対応可能（SD-JWT）	仕様内で対応可能（属性単位のハッシュ）	仕様外（関連仕様に委ねる）
	非リンク性	仕様内で限定的に対応可能（ソルト付きハッシュ、複数VCのローテーション等）	仕様内で限定的に対応可能（ソルト付きハッシュ、複数MSOのローテーション等）	仕様外（関連仕様に委ねる。ZKPの採用も可能）
トラストモデル	信頼の起点	発行者を直接信頼（CA階層も選択可）	CA（IACA）を頂点とする階層的信頼チェーン	発行者を直接信頼
	Holder Binding	仕様内（オプション）で対応可能（Key Binding JWT）	仕様内（必須）で対応可能（DeviceAuth）	仕様外（関連仕様に委ねる）

（出所）各種資料より大和総研作成

プライバシーに関しては、選択的開示については SD-JWT VC と mdoc が仕様内で対応するのに対し、VCDM は関連仕様に委ねる。非リンク性については、いずれの方式も完全な実現には追加の工夫が必要となる。特に VCDM は、関連仕様の選択次第でゼロ知識証明（ZKP）方式の採用も可能であり、より高度な非リンク性を実現し得る。

トラストモデルに関しては、信頼の起点に 2 つの設計思想が見られる。mdoc は CA（IACA）を起点とする階層的な信頼チェーンを採る一方、SD-JWT VC と VCDM は発行者を直接信頼する設計を基本とする。前者は公的 ID のような階層的な信頼が成立する領域に、後者は多様な発行者が並立する文脈に適合しやすい設計思想である。

Holder Binding についても、各方式の設計思想が反映される。mdoc が特定デバイスとの強固な紐付けを必須として規定するのに対し、SD-JWT VC は任意、VCDM は関連仕様に委ねる。これは、対面提示で物理的な保有者を確認することを重視する mdoc と、オンラインで保有者の証明手段を柔軟に選択する SD-JWT VC、VCDM の設計思想の違いを反映している。

標準化と実装

図表 12　標準化と実装の比較

項目		SD-JWT VC	mdoc（ISO/IEC 18013-5）	VCDM
実装	標準化ステータス	ドラフト（IETF標準化最終段階）	標準化済（ISO/IEC 発行済）	標準化済（W3C 勧告）
	実装柔軟性	クレーム表現は柔軟 Web技術との親和性が高く実装しやすいが、セキュリティ方式はJOSE系に限定	一体的規定により選択肢は限定的（ハードウェア依存によるプラットフォーム制約も一部あり）	クレーム表現の柔軟性に加え、セキュリティ方式等、多くの要素で複数選択可
	事例蓄積	進展中（現状は限定的）	公的ID関連を中心に多数	教育/資格証明、サプライチェーンなど広い領域で多数

（出所）各種資料より大和総研作成

標準化の観点では、mdoc は ISO/IEC 18013-5 として発行済み、VCDM は W3C 勧告として確立、SD-JWT VC は IETF での標準化が最終段階にある。

実装柔軟性は、規定範囲の広さと表裏の関係にある。VCDM はデータモデル以外の要素（セキュリティ方式等）を関連仕様の選択に委ねる設計であり、多くの要素で複数の選択肢から選べる柔軟性を持つ。加えて、DID との組み合わせ（DID/VC）により、多様な DID メソッドを活かした柔軟な識別子設計も可能である。SD-JWT VC は Web 技術との親和性の高さから実装のハードルが低い一方、セキュリティ方式は JOSE 系に限定される。mdoc はデータモデルからプロトコルまでを一体的に規定するため、実装時に選べる選択肢は少ない。加えて対面・近接通信を実現するハードウェア機能への依存により、iOS 上の独自ウォレット実装等でプラットフォーム側の制約を受ける場面もある[18]。

事例の蓄積状況にも、各方式の設計思想が反映される。mdoc は、仕様内で一定のセキュリティ水準を担保できる設計を背景に、公的 ID 関連を中心に多数積み上がっている。VCDM は教育・資格証明やサプライチェーン等、幅広い領域に広がっている。SD-JWT VC は、標準化のタイミングを反映し、蓄積が進展中である。

(2) 各方式の特徴と用途への適合

前節までで整理した各方式の特徴は、実際のユースケースへの適合関係にどう反映されるだろうか。図表 13 に、対面/非対面とセキュリティ要件の観点から、代表的なユースケースと適合する方式をマッピングした。

図表からは、各方式の特徴が用途への適合に素直に反映されていることが読み取れる。

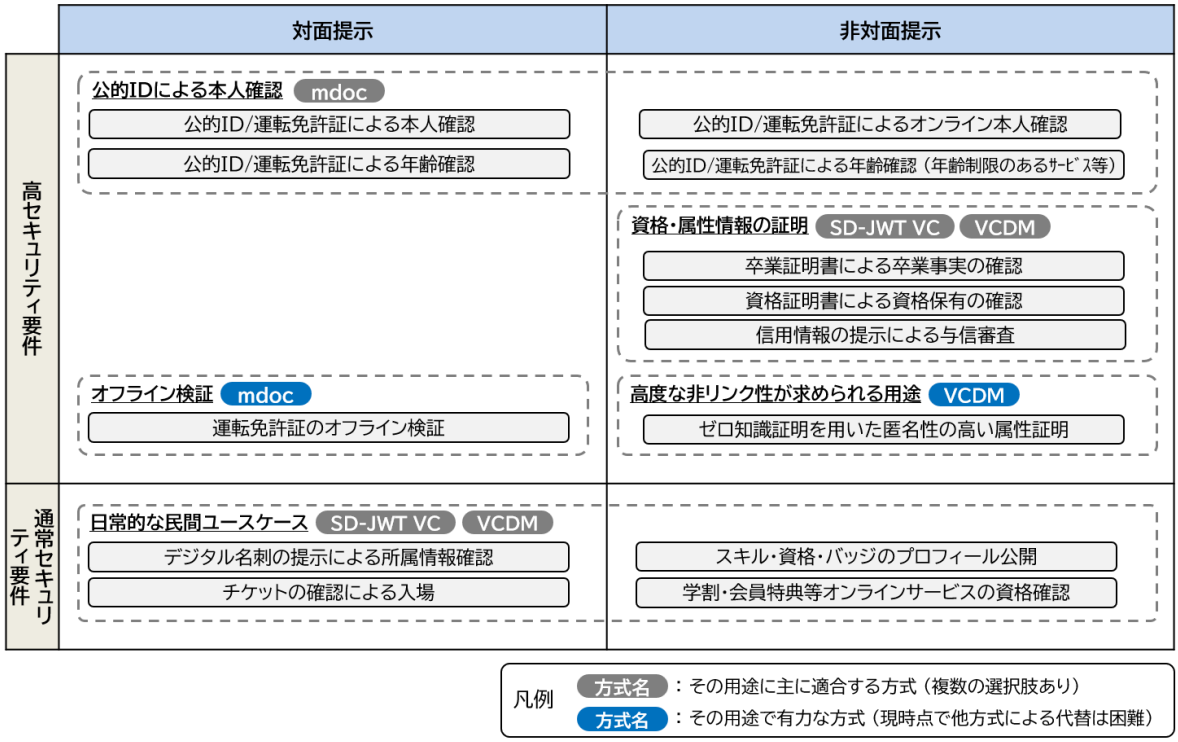
mdoc は、高いセキュリティ要件が求められる公的 ID による本人確認や年齢確認に主に適合する。加えて、対面・近接通信での対応の広さと、オフライン検証を仕様として規定する点で、運転免許証の路上検証のように通信環境が限定される場面を含めた対面の利用形態では他方式では代替しにくい有力な方式となる。

一方、SD-JWT VC と VCDM は、柔軟な設計により、卒業・資格証明書の提示や信用情報を用いた与信審査といった資格・属性情報の証明から、デジタル名刺やチケット提示等の日常的な民間ユースケースまで、多様な発行者・利用場面に広く適合する。

VCDM については、関連仕様の選択次第でゼロ知識証明（ZKP）の採用も可能であり、匿名性の高い属性証明のように高度な非リンク性が求められる用途において、現時点では他方式による代替が困難な方式となる。

[18] 例えば、iOS 上で NFC／Secure Element を使った独自アプリ実装を行う場合、Apple との契約、エンタイトルメント取得等の条件がある（Apple “NFC & SE Platform for Secure Contactless Transactions - サポート - Apple Developer”（最終閲覧日 2026 年 7 月 8 日））

図表 13　各方式の特徴とユースケースの適合関係



（注）各クラスタは、各方式が主に適合するユースケースの領域を示す目安である。ユースケースは主な利用場面に配置しており、他の場面で使われる場合もある。本図は方式選択の参考として整理したものであり、実際の方式選択はユースケースの具体的要件やエコシステムの状況等を踏まえた総合的な判断となる
（出所）各種資料より大和総研作成

こうした適合関係は、第 2 部で見た各国の取組みにも反映されている。

公的 ID 関連での実用化を進めるフランス（デジタル運転免許証）や日本（マイナンバーカード由来の本人確認情報）は mdoc、卒業証明等の非対面での属性提示を想定するオランダは SD-JWT VC、スペインは成人確認における非リンク性の実現に DID/VC の活用が見られる。各国の技術選択は、単なる方式の重点の違いではなく、各方式の特徴と用途の適合関係を反映したものと捉えられる。

(3) 方式の並立と現状認識

SD-JWT VC、mdoc、VCDM の 3 方式は、それぞれ異なる特徴と適合領域を持って並立している。加えて、各方式では本体仕様の策定・改訂や周辺仕様の追加が継続しており、標準化の枠組みはなお発展途上にあると考えられる。

具体的には、mdoc は本体（ISO/IEC 18013-5）の改訂や mdoc の適用範囲を広げる ISO/IEC 23220 シリーズの策定が、SD-JWT VC は本体仕様の策定が最終段階に、VCDM は本体の改訂（v2.1 の検討）や周辺仕様（Recognized Entities 等）の策定が進んでいる。各方式が固定されたものではなく、技術的な広がりが継続している状況にある。

この複数方式並立の状況を前提とした相互運用の動きも進んでいる。EUDI ウォレットの共通仕様は、SD-JWT VC、mdoc、VCDM のいずれも対応可能として位置づけており（SD-JWT VC と mdoc が必須、VCDM が任意）、単一方式への統一ではなく、相互運用が国際的な方向性として広がっている。

こうした相互運用を技術的に支えるのが、フォーマット非依存のプロトコルである OID4VCI/VP で、3 方式のいずれのフォーマットも扱えるよう設計されており、プロトコル層で複数方式の相互運用を支える共通のレイヤーとして機能する。加えて、特に高いセキュリティ・プライバシー要件が求められる領域向けには、OID4VCI/VP や SD-JWT VC の技術要件を絞り込んだ HAIP（High Assurance Interoperability Profile）[19]等の相互運用プロファイルの整備も進められている。

前節で見たユースケースの特徴に応じて方式が選択されるという構図は、こうした複数方式並立の国際的方向性とも整合する。

最後に、これらの技術整理を踏まえ、日本の論点への技術観点からの方向性を考察する。

（4）考察：日本の論点と技術観点からの方向性

第 2 部では、日本にとっての論点として利用者起点の情報制御と相互運用性の 2 点を提示した。本章での技術整理を踏まえ、これらの論点を発展させる方向性を考察したい。

日本では mdoc を活用した公的 ID のデジタル基盤の実用化が進んでいる。一方で、EU のように公的ウォレットを整備して複数のフォーマットに対応した公的・民間の VC を一体的に管理する取組みは 1 つの理想形と考えられるが、日本では現時点でそのような公的ウォレット整備の方針は確認されていない。こうした状況を踏まえると、mdoc による公的 ID のデジタル基盤の発展と、柔軟性の高い他の方式を主とした民間による取組みの蓄積を、並行して進めていくことが重要になるだろう。

各方式の特徴に目を向けると、前節で確認した通り、mdoc は対面・近接通信に強みを持つ規格である。日本の現状の活用はオンラインが中心であり、mdoc の強みである対面・近接通信での活用はまだ限定的であるが、利用に必要な検証者側のインフラ整備等が進むことで、対面・近接通信での活用も広がっていくと見られる。こうした幅広い活用の広がりが、公的 ID のデジタル基盤をより盤石なものへと発展させていく。

一方、柔軟性が高く様々な領域での活用が見られる VCDM や DID/VC、標準が固まりつつあり様々な検証が進む SD-JWT VC は、特定の発行体や検証者に限定されず、様々な領域での応用に適合する特徴を持つ。実際、資格・卒業証明、社員証、学生証、イベントの参加証等、民間分野での取組みが現れ始めている。こうした実装の蓄積により、利用者が自ら管理・提示できる VC の種類や活用領域が広がっていき、利用者起点の情報制御が着実に拡張されていく。

[19] OIDF “OpenID4VC High Assurance Interoperability Profile 1.0”（2025 年 12 月 24 日）

実装を担う企業や大学等においては、各方式の特徴を踏まえ、ユースケースに合った方式を選択していくことが重要になる。

これらの取組みは、EU の複数方式に対応する統一ウォレットの整備とは異なる道筋だが、官民がそれぞれ各方式の基盤を整備することで、結果として利用者が多様な VC を扱える環境が整い、複数方式の並立を前提とする国際的な相互運用の方向性とも親和的である。

技術的にも進化が続く本分野において、政府による公的 ID のデジタル基盤の発展と、民間による多彩な実装の蓄積が並行して進むことで、日本のデジタルアイデンティティのエコシステムは、利用者にとって使いやすく信頼できる社会基盤へと成熟し、環境変化への適応力を備えていくと考えられる。

おわりに

本レポートシリーズでは、デジタルアイデンティティ・デジタルクレデンシャルをめぐる動向を「取組み」と「実装技術」の両面から整理してきた。第 1 部で基本概念と EUDI ウォレットの動向、第2部で欧州4カ国と日本の取組み比較、第3部で実装技術の整理と考察を通じて、この分野の全体像を体系的に示すことを目指した。

本レポートで扱ってきた技術標準は、今もなお議論が続き、アップデートが重ねられている。加えて、法人を対象とした検証可能なクレデンシャルの枠組みである vLEI（verifiable Legal Entity Identifier）[20]や、AI エージェントに委任された取引権限を検証可能な形で表現・管理するための VC 活用（Google の「Agent Payments Protocol（AP2）[21]」）等、新たな標準や応用も登場している。デジタルアイデンティティに関連する技術は、標準と応用の両面で現在進行形で拡大しつつある領域である。

本レポートで示したレイヤー構造や各方式の特性整理は、こうした今後の動向を追う上での見取り図としても機能すると考えている。新たな仕様が登場した際に、それがどのレイヤーで何を規定し、既存方式とどう関係するかを位置づけることで、継続的な情報の吸収と検討に役立てていただければ幸いである。

デジタルアイデンティティは、今後さらに社会基盤としての重要性を増していく分野である。本シリーズが、その動向を読み解き、実装に向けた判断を支える 1 つの手がかりとして機能することを期待したい。

以上

[20] GLEIF “The verifiable LEI (vLEI) - LEI & vLEI - Organizational Identity – GLEIF”（最終閲覧日 2026 年 7 月 29 日）

[21] Google Cloud “Announcing Agent Payments Protocol (AP2) | Google Cloud Blog”（2025 年 9 月 17 日）