

2026年5月14日 全12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1部)

デジタルアイデンティティの基本像と、EUDI ウォレットにみる
制度化・実装動向

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をめぐる動向を「取組み」と「実装技術」の両面から体系的に整理することを目的とする。第1部では、デジタルアイデンティティおよびデジタルクレデンシャルの基本概念を整理した上で、EUDIウォレットを例に、制度化の背景、実装プロセス、主要ユースケースを俯瞰する。
- デジタル化の進展により、個人や組織のアイデンティティは、単なる本人確認にとどまらず、資格や権利を含む情報としてデジタル空間で扱われるようになってきている。こうした変化のなかで、証明情報を安全かつ効率的に流通・検証する手段として、デジタルクレデンシャルが社会基盤の一要素として位置づけられつつある。
- デジタルクレデンシャルの実装においては、発行者 (Issuer)・保有者 (Holder)・検証者 (Verifier) の三者モデルを前提に、検証可能な形で情報をやり取りする VC (Verifiable Credentials) の考え方が広く採用されている。各国で制度や提供主体は異なるものの、クレデンシャルをウォレットに保持し、必要な相手に提示・検証するという基本構造には共通性が見られる。
- 一方で、VCの実装方式としては、DID/VC、mdoc など複数の技術標準・データ形式が並立している。これらの違いは表現形式にとどまらず、相互運用性や検証の前提、適合するユースケースにも影響し得るため、取組みの動向とあわせて技術的前提を整理することが重要となる。
- 欧州で進められる EUDI ウォレットは、公的・制度的な信頼基盤を土台に、利用者起点の情報制御と域内での相互運用性を制度要件として組み込んだ象徴的な取組みである。改正 eIDAS 規則の下、共通仕様 (Toolbox) と大規模実証 (Large Scale Pilots : LSPs) を往還させながら、実装の現実性と相互運用性の検証・改善が進められている。

はじめに

世の中の様々な領域でデジタル化が進むなか、個人や組織の「アイデンティティ」も、デジタル環境で取り扱える形へと移行しつつある。なかでも、資格や権利を証明する情報（クレデンシヤル）をデジタル化したデジタルクレデンシヤルは、その中核をなす要素として注目されている。デジタルクレデンシヤルをめぐるのは、制度面・技術面の両面で変化が進み、各国で具体的な取組みが見られる。

欧州では、デジタルクレデンシヤルを保管・管理するウォレット EU Digital Identity Wallet (EUDI ウォレット) の提供が EU 加盟国に義務付けられ、期限の 2026 年末が迫る。日本ではワクチン接種証明書のスマートフォン向け発行やマイナンバーカードのスマートフォン搭載が実現し、米国でもモバイル運転免許証の運用が進むなど、同様の動きが各国で広がっている。

こうした仕組みは、VC (Verifiable Credentials) を核に、発行者 (Issuer)・保有者 (Holder)・検証者 (Verifier) の役割分担を前提とする三者モデルによって実現されている点で共通する。一方で、その実装には DID/VC、mdoc、SD-JWT VC といった複数の標準・データ形式が並立しており、相互運用性や運用設計、適用可能なユースケースにも影響を与え得る。このため、取組みの動向とあわせて、背後にある技術的前提を整理することが重要となる。

本レポートは 3 部構成とし、前半では各国の方針や取組み、その背景を概観し、後半ではそれを支える技術標準・規格を整理する。これにより、デジタルアイデンティティをめぐる動向を「取組み」と「実装技術」の両面から体系的に理解し、今後重要性が高まるデジタルアイデンティティの実装に向けた知識の整理に貢献したいと考えている。

第 1 部 (本レポート) では、デジタルアイデンティティおよびデジタルクレデンシヤルの基本概念を整理した上で、欧州が進める EUDI ウォレットを例に、制度化の背景や実装プロセス、ユースケースを概観する。第 2 部では、EU 加盟各国および日本における取組みを取り上げて、欧州との違いや実装方式の特徴を整理する。第 3 部では、技術的な視点から DID/VC、SD-JWT VC、mdoc といった VC の実装方式について、既存の電子署名付き PDF との違いや要件・仕組み・適用領域を整理・比較していく。

図表 1 本レポートシリーズの構成

第1回	<ul style="list-style-type: none"> デジタルアイデンティティ、デジタルクレデンシヤルの基本概念 欧州におけるEUDIウォレットの取組み
第2回	<ul style="list-style-type: none"> 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回	<ul style="list-style-type: none"> 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

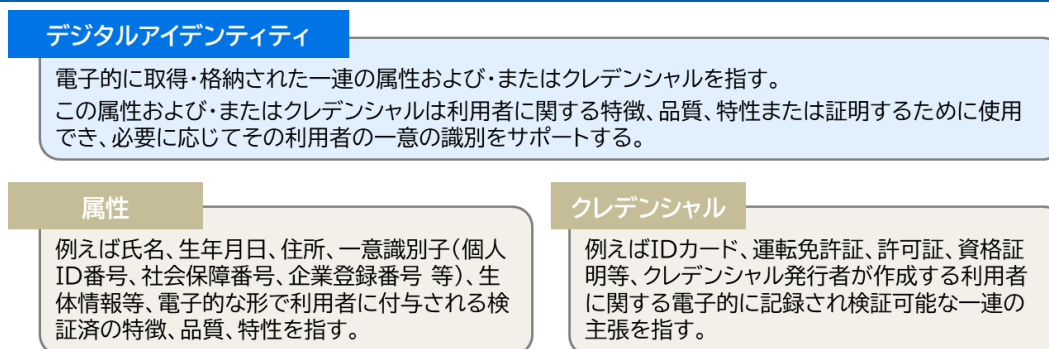
1. デジタルアイデンティティ・デジタルクレデンシャルとは

(1) デジタルアイデンティティの定義と方針¹

まずは、デジタルアイデンティティの定義について整理する。

「デジタルアイデンティティ」とは、ひとことでは、デジタル空間で「その人（または組織）が何者か」を示す情報のまとまりである。定義は一様ではないが、OECD ではこれを、氏名・生年月日などの属性情報と、それらの属性や資格・権利を裏付ける免許・学位などの証明（クレデンシャル）として整理している²。具体例や関係は図表 2 に示す。

図表 2 デジタルアイデンティティの定義



(注) 田邊（2024）（脚注 1）の図表 4 を基に一部修正
（出所）OECD（2023）（脚注 2）より大和総研作成

次に、デジタルアイデンティティを社会実装する際の考え方を整理する。

OECD の勧告は、利用者中心で信頼できるデジタルアイデンティティを整え、国・技術・分野をまたぐ国際的な相互運用を実現するための条件整備を重視している。また G20 でも、人間（利用者）を中心に据えつつ、安全・セキュア・信頼を確保し、プライバシーや個人データ保護に配慮した制度整備を進める姿勢が示されている³。

これらを踏まえると、実務上は「利用者中心」「セキュリティとプライバシーの確保」「相互運用性（越境利用を含む）」「国際協力」といった観点が重要になる（図表 3）。

¹ デジタルアイデンティティに関する定義や方針については、田邊美穂「[デジタル時代の本人確認「デジタルID」](#)」（大和総研レポート、2024年11月28日）も参照ください

² OECD “[Recommendation of the Council on the Governance of Digital Identity](#)”, 2023/6/8

³ デジタル庁 “[G20 MACEIÓ MINISTERIAL DECLARATION ON DIGITAL INCLUSION FOR ALL](#)”（2024年9月13日）、そのうち「デジタルアイデンティティのガバナンスに関する G20 一般原則」に関する記載は、“Annex 2 General Principles on the Governance of Digital Identity”

図表 3 デジタルアイデンティティに関する基本方針

①	利用者中心であること	<ul style="list-style-type: none"> デジタルアイデンティティへのアクセスと使用に対する障壁を最小限に抑える デジタルアイデンティティの利用を望まない/できない人のサービスへのアクセスが制限されないこと
②	セキュリティが優先されること	<ul style="list-style-type: none"> デジタルアイデンティティに対する信頼を確立するために、プライバシー、個人情報を保護し、セキュリティを優先する
③	相互運用性の促進を目指すこと	<ul style="list-style-type: none"> 将来の相互運用性を考慮し、国際的な技術標準や認証の利用を推進する
④	国際協力の必要性	<ul style="list-style-type: none"> 技術標準の理解と整合、国境を越えた相互運用性の実現に関する議論を進めるために国際協力に取り組む

(注) 田邊 (2024) (前掲脚注 1) の図表 5 を基に一部修正

(出所) OECD (2023) (前掲脚注 2)、「デジタルアイデンティティのガバナンスに関する G20 一般原則」(前掲脚注 3) より、大和総研作成

以上の方針を実務で満たすには、デジタル空間における本人確認に加え、免許・学位などのクレデンシャルを安全に提示・検証できることが重要となる。以降では、クレデンシャルのデジタル化と、その実現手段としての VC の考え方を整理する。

(2) Verifiable Credentials (検証可能なクレデンシャル) について

クレデンシャルのデジタル化は、紙やカードを「データとして扱えるようにする」だけで完結する話ではない。手続きのデジタル化が進むほど、クレデンシャルはデータとして流通し自動処理される。よって、改ざん・偽造への耐性と、個人情報を安全に扱うための要件が重要になる。現状は運転免許証などを撮影して画像や PDF の形式で提出する方法もあるが、改ざん検出による真正性確認が難しく、送信・保存時の保護が不十分な場合は漏洩リスクもある⁴。

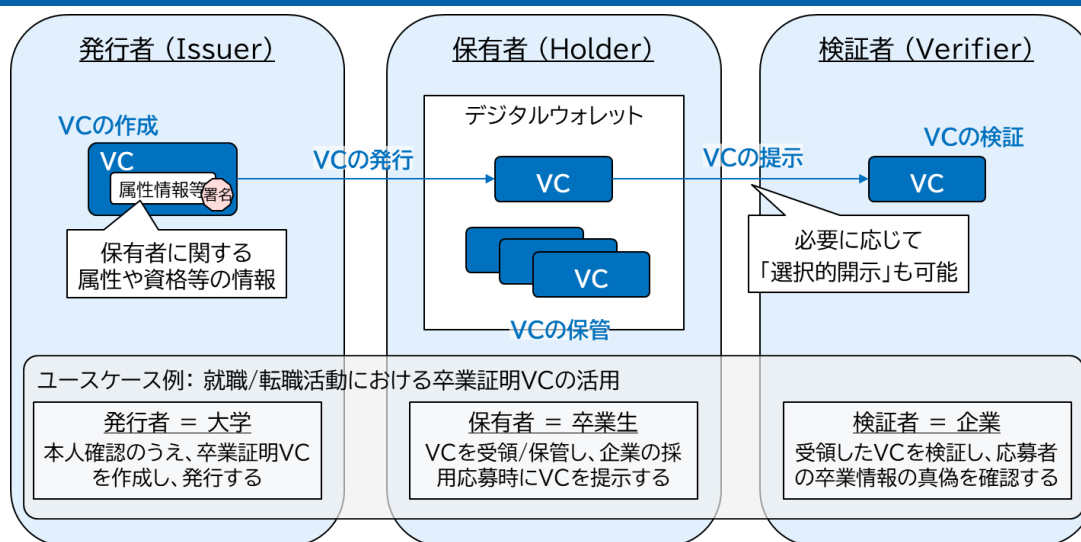
こうした課題を前提に、検証可能な形でセキュアにクレデンシャルを扱う方法として注目されているのが、VC (Verifiable Credentials: 検証可能なクレデンシャル) である。VC は、発行者が内容に電子署名を付した、改ざんを検知できるデータとしてクレデンシャルを表現する仕組みになっており、そのやり取りは図表 4 に示す三者モデル (Issuer/Holder/Verifier) によって成り立つ。

まず、発行者 (Issuer) が属性や資格などの情報に電子署名を付した VC を発行し、保有者 (Holder) はそれを保管する。保有者は必要に応じて VC を提示し、それを受け取った検証者 (Verifier) は署名を検証することで、「誰が (どの発行者が) 発行したものか」「内容が改ざんされていないか」を機械的に確認できる。さらに、保有者が提示する際に必要な情報だけを選んで示す (選択的開示) といった設計も取り込める。

⁴ クレデンシャルのデジタル化については、田邊美穂「[急速に広がる資格情報等のデジタル化](#)」(大和総研レポート、2025年4月28日)も参照ください

この VC を保有者がスマートフォンなどのデバイスに格納し、必要な相手に提示する際には「デジタルウォレット」が用いられることが多い。デジタルウォレットは、VC を安全に保管し、提示時には（方式によっては）必要な情報だけを選んで渡せるようにするスマートフォンアプリなどであり、提示・同意といった保有者によるやり取りの“窓口”になる。

図表 4 Verifiable Credentials と三者モデル⁵



(出所) World Wide Web Consortium (2025)⁶等、各種資料より大和総研作成

このデジタルウォレットを軸に、デジタルアイデンティティとデジタルクレデンシャルの仕組みを制度と技術の両面から整えようとしている代表例が欧州の「EUDI ウォレット」である。

次章では、欧州の EUDI ウォレットを例に、制度化の背景から実装の進め方、ユースケースまでを俯瞰し、本章で整理した概念を、制度と実装の具体例に当てはめて確認していく。

⁵ VC の内容や処理の流れについては、分かりやすさを重視し、一部簡略化して記載している。より詳細な仕組みについてはレポートの第 3 部にて解説を予定している

⁶ World Wide Web Consortium "Verifiable Credentials Data Model v2.0", 2025/5/15

2. 欧州における EUDI ウォレットの取組み

欧州では、デジタルアイデンティティの実装基盤として、EU Digital Identity Wallet (EU デジタルアイデンティティウォレット：EUDI ウォレット) を中心に据えた制度整備が本格的に進められている。EUDI ウォレットは、スマートフォン上で本人確認を行い、運転免許証や資格証明などのデジタルクレデンシャルを保管・提示するための仕組みである。

本章では、EUDIウォレットの要点と制度化の経緯を整理した上で、共通仕様 (Toolbox) と Large Scale Pilots (LSPs) を軸に、仕様策定と実証がどのように推進されているかを確認する。あわせて、設計思想が形成された背景要因を整理する。

(1) EUDI ウォレットの要点と制度化の経緯

本レポートでは、欧州委員会の公式ウェブサイト⁷が示す「安全・信頼・プライバシー保護」と「データの自己コントロール」「域内での越境利用」を踏まえ、EUDI ウォレットの要点を「公的・制度的信頼基盤」「利用者起点」「相互運用性と利用可能性」の3つに整理する。これらは、前章で示したデジタルアイデンティティの基本方針 (利用者中心・セキュリティ・相互運用性) を制度要件として具体化しつつ、越境利用を支える公的な信頼を土台に据えた枠組みと整理できる。

この枠組みが制度要件としてどのように位置づけられたかを理解するため、制度化の経緯を確認する。

図表 5 EUDI ウォレットの要点

① 公的・制度的信頼基盤(セキュリティ・認証を含む)

加盟国が提供する公的なデジタルアイデンティティ基盤を土台に、法制度、監督・認証の枠組みの下で、発行・提示・検証を信頼できる形で成立させる

② 利用者起点の情報制御(選択的開示)

利用者は、自分の情報から必要な情報だけを選んで提示できる「選択的開示」などにより、本人が共有する情報を自らコントロールできる

③ EU域内での相互運用性と利用可能性(共通仕様に基づく)

共通仕様に基づき、国境を越えて公的・民間サービスで一貫して利用できることを前提とする

(出所) 欧州委員会の公式ウェブサイト (脚注 7) 等、各種資料より大和総研作成

EUDI ウォレットの制度的な根拠は、EU 域内の電子取引の信頼基盤を定めた EU 法令「eIDAS 規則」の改正に求められる。

⁷ European Commission “[EU Digital Identity Wallet Home - EU Digital Identity Wallet](#) –” (最終閲覧日 2026/4/22)

2014年に制定された eIDAS 規則は、加盟国の電子 ID (eID) を相互に認め合う枠組みと、電子署名などのトラストサービスに関する共通ルールを整備し、越境的な電子取引を支えることを目指した⁸。

しかし、当枠組みでは、市民・企業が日常的に利用できる電子 ID スキームの提供が加盟国に義務付けられておらず、加盟国間で整備状況にばらつきが残った⁹。

こうした課題を受け、EU は 2024 年に eIDAS 規則を改正して EUDI ウォレットを制度の中心に位置付け、加盟国に 2026 年末までの提供を求めている¹⁰ (図表 6)。

図表 6 eIDAS 規則 改正の流れ

eIDAS規則 (2014年発行)

目的: EU域内の電子取引に対し、電子IDとトラストサービスの共通的な信頼基盤を整備
特徴: 各国が通知した電子IDの相互承認の枠組みを整備
電子署名・電子シール等のトラストサービスに共通ルールを整備



課題点

- 加盟国による電子IDスキームの整備は義務ではなく、整備状況にばらつきがあった
- EU域内で共通に使える(ウォレット型の)デジタルアイデンティティ手段は制度としては未整備で、利用者が日常的に使える共通基盤が弱かった

改正eIDAS規則 (2024年発行)

目的: eIDAS規則の枠組みを拡張し、利用者が実際に使える欧州共通のデジタルアイデンティティ基盤を構築
特徴: ウォレットを制度の中心に据え、公的信頼に基づく本人起点の利用を強化
本人確認に加え、属性証明や電子文書の保管・提示まで対象を拡大
共通仕様に基づき、EU域内での相互運用を前提とする

(出所) eIDAS 規則条文、改正 eIDAS 規則条文、欧州委員会公式 FAQ (脚注 8~10) 等、各種資料より大和総研作成

⁸ EU "[Regulation - 910/2014 - EN - e-IDAS - EUR-Lex](#)", 2014/10/18

⁹ European Commission "[Q&A Digital Identity | Shaping Europe's digital future](#)" (2024/4/4 更新)

¹⁰ EU "[Regulation - EU - 2024/1183 - EN - EUR-Lex](#)", 2024/4/30

(2) 共通仕様 (Toolbox) と Large Scale Pilots (LSPs) による実装の推進

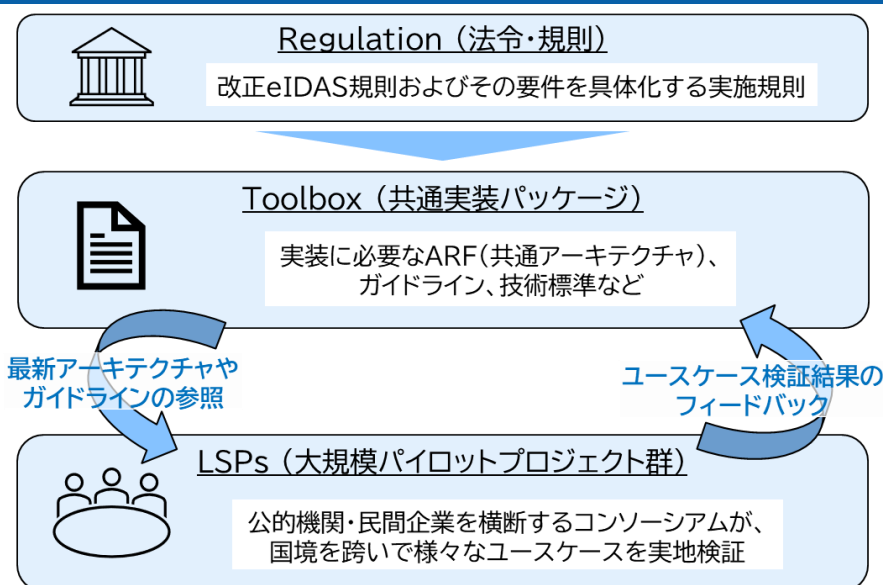
では、制度化された方針は、どのように具体化されているのか。ポイントとなる「共通仕様 (Toolbox)」および「Large Scale Pilots (大規模実証プロジェクト：LSPs)」を中心に見ていく。

EUDI ウォレットの実装に必要な共通仕様は、改正 eIDAS 規則をはじめとする要件を具体化する形で整理されており、その中核が Toolbox である。Toolbox は、EUDI ウォレットの共通アーキテクチャである Architecture and Reference Framework (共通アーキテクチャ：ARF) を中核に、関連する技術標準やガイドラインなどを体系化したもので、加盟国や関係主体が実装を検討する際の共通の参照点となる¹¹。

一方、仕様が実運用で機能するかは机上だけでは検証しきれないため、LSPs が設けられている。LSPs は Toolbox を前提に、実環境に近い条件でユースケースを検証する大規模な実証プロジェクト群である¹²。相互運用性や運用上の実現可能性を検証し、得られた知見や課題を ARF や関連仕様の改善点として Toolbox にフィードバックする。

このように、法令を起点に整備された Toolbox と、現実のユースケースを通じて検証を行う LSPs とが往還することで、仕様が実証を通じて磨き込まれ、実装が前進している。

図表 7 Toolbox と LSPs による仕様と実証の往還



(出所) 欧州委員会の公式ウェブサイト (脚注 11, 12) 等、各種資料より大和総研作成

¹¹ European Commission “[EU Digital Identity Wallet Toolbox process | Shaping Europe’s digital future](#)” (2025/7/23 更新)

¹² European Commission “[What are the Large Scale Pilot Projects - EU Digital Identity Wallet](#) -” (最終閲覧日 2026/4/22)

(3) LSPs が検証を進めるユースケース

次に LSPs の具体的な取組みについて見ていく。

LSPs は複数の国から様々な主体が参加し、行政、教育、モビリティ、金融などの分野横断ユースケースを、国境を越えた利用や制度差を前提に検証する枠組みである。2023年に第1ラウンドとして4件が始動し、2025年には第2ラウンドとして2件が追加された。現在は、第2ラウンドの2件を中心に検証が続いている。図表8に各プロジェクトの概要を整理した。

図表8 EUDI ウォレットの Large Scale Pilots

プロジェクト名	参加国/団体	重点領域	主なユースケース
POTENTIAL	フランスやドイツを中心に20か国から140超の政府機関と銀行・通信・医療分野などの民間事業者が参加	デジタルIDを安全に相互運用可能にすることを狙い、分野横断で広く検証	行政サービスの利用、銀行口座開設、携帯回線の契約、デジタル運転免許証、電子署名、電子処方箋
EWC	スウェーデンを中心にオランダ、ギリシャ、イタリア、スペイン等24か国から80の政府機関と民間事業者が参加(旅行・決済・ID関連事業者が中心)	Digital Travel Credentials を軸に、決済や組織ウォレットまで含めて検証	旅行・搭乗・宿泊の手続、支払い、組織や会社の身元確認
DC4EU	スペインを中心に、ギリシャ、オーストリア、北欧系等、22か国から教育・資格・社会保障の公的機関を中心に99機関が参加	教育と社会保障に特化し、越境で使えるデジタルクレデンシャルの実装を検証	社会保障の証明、健康保険資格の確認、学歴証明、専門資格の確認
NOBID	ノルウェーを中心に、北欧、バルト三国やイタリア、ドイツから政府デジタル機関と銀行・決済事業者を中心に34機関が参加	越境決済を中心課題とし、北欧・バルトを中心に、署名・本人確認も含めた決済エコシステムを検証	店頭やネットでの支払い、電子署名、国をまたぐ本人確認
APTITUDE	フランスを中心に、ポーランド、ギリシャ、ドイツなど12か国から117の公的機関、民間企業、研究機関が参加	相互運用性・使いやすさ・スケールビリティを重視し、生活者向けユースケースを広く検証	デジタル旅券、予約・乗車/搭乗手続、車の登録証明、本人確認を強化した支払い
WE BUILD	オランダを中心とした26か国から民間事業者(企業登記、税務、金融、ウォレット、技術、研究機関など)を中心に180の団体が参加	ビジネス向けのウォレットや決済に軸足を置き、B2B・B2G・B2Cの実運用に近いユースケースを検証	越境での会社登録・登記、税務申告、会社を代表しての署名(代理権限)、取引先・取引関係の確認、物流の関係者確認、銀行手続・企業決済

※「POTENTIAL」「EWC」「DC4EU」「NOBID」は初期案件として2023年～2025年に活動

※「APTITUDE」「WE BUILD」は第2ラウンドとして2025年～2027年にかけて活動予定

(出所) 欧州委員会の公式ウェブサイト(前掲脚注12)等、各種資料より大和総研作成

2023年に始動した POTENTIAL、EWC、DC4EU、NOBID の4プロジェクトは、いずれも2025年に活動を終え、実証結果や得られた知見を成果物として公表している。これらのプロジェクトで進められてきた主なユースケースには以下のようなものがある。

POTENTIAL では、モバイル運転免許証が代表的なユースケースの1つとして扱われた。これは、運転免許証をウォレット内のデジタルクレデンシャルとして保持し、レンタカー利用や警察による確認などの場面で、対面・オンラインの双方で提示・検証できるようにするものである。最終成果物では、越境利用を前提とした提示・検証を試行し、相互運用性の技術的成立可能性が示された。一方で、オフライン検証やUX上の論点(オンボーディングの複雑さや加盟国間でのUI不統一)に加え、失効などの状態管理やモバイル運転免許証をIDとして認める法的整理など、「公的・制度的な信頼基盤」を実運用として成立させるための課題も整理された。

共通標準が一貫して適用されれば、モバイル運転免許証は EUDI ウォレットの代表的ユースケースになり得ると総括されている¹³。

教育分野では、DC4EU が卒業証明書を含む教育資格情報を主要テーマの 1 つとして取り上げた。ここでは、学位情報をデジタルクレデンシャルとしてウォレットに保持し、留学先大学への登録などの場面で、真正性・有効性の確認や、所持者との紐付けを行えるようにすることが目指されている。公表されたレポートでは、留学先大学への登録を含む越境的な学修手続を想定し、パイロットで得られた知見も踏まえながら、資格情報の発行・失効/停止・検証を成立させる運用ルール、利用者のデータ最小化/自己主権といった原則、ならびに相互運用要件・データモデルを「あるべき前提」として取りまとめている¹⁴。

移動・旅行の領域では、EWC がデジタル渡航資格 (Digital Travel Credential : DTC) を扱った。これは、旅券などの渡航文書情報を DTC としてウォレットに保持し、渡航前に必要情報を国境当局へ共有して事前審査を可能にし、国境手続の効率化を図る想定である。関連ページでは、渡航前共有を成立させる構成要素や、旅券・ID カードの信頼リストとウォレット側の信頼ルールを組み合わせた真正性確認の考え方が論点として整理され、あわせて技術規格により標準化されたデータ形式を前提に、越境利用を見据えた検討事項が示されている¹⁵。

金融分野では、NOBID が決済を中心的なユースケースとして検証した。これは、EUDI ウォレットを強固な顧客認証を伴う取引承認の基盤として活用し、対面・オンライン双方の支払いを支えることを目指すものである。関連ページでは設計・試験・影響評価の成果物が整理されており、技術的成立性が確認される一方、決済スキーム/ウォレット間の相互運用性や金融事業者の役割・責任の明確化などが課題として示されている¹⁶。

以上のとおり、EUDI ウォレットは本人確認にとどまらず、免許・学位・渡航・決済といったクレデンシャルの提示・検証まで射程を広げつつある。

各 LSP の検証は、本レポートで 3 つの要点として整理した公的・制度面の担保、利用者起点の運用、国境を越えた相互運用といった観点で、成立条件や課題を具体化し、共通仕様の改善に向けた材料を提供してきた。

次節では視点を変え、このような要件が EUDI ウォレットにおいて重視されるに至った背景を整理する。

¹³ POTENTIAL “[Potential takeaways and lessons learned.pdf](#)”, September 2025

¹⁴ DC4EU “[DC4EU_WP5_D5.1_Business_BluePrint.pdf](#)”, 2025/10/1

¹⁵ European Commission “[Travel Credentials - EU Digital Identity Wallet](#) -” (最終閲覧日 2026/4/22)

¹⁶ European Commission “[LSP-NOBID - EU Digital Identity Wallet](#) -” (最終閲覧日 2026/4/22)

(4) EUDI ウォレットの設計思想を支える背景要因

EUDI ウォレットが重視する「利用者起点の情報制御」は、サービス側に個人データが偏在しやすい従来モデルとは異なる設計思想に基づく。利用者がクレデンシャルを携行し、必要最小限を都度提示する運用を成立させるには、技術・運用・エコシステムの各面で実装上の負荷が大きい。その一方で、EU は当該方針を制度化し、実装を推進している。

この背景を、政策・文化・技術の蓄積として整理し、三者が合流して改正 eIDAS 規則に至る流れを示す。

文化面では、欧州では 20 世紀の権威主義体制下における個人監視や情報統制の経験も背景の 1 つとして、国家による個人情報の集中管理への警戒感が強いとされる。こうした問題意識は、「個人の尊厳」や「私生活の保護」を重視する価値観として定着し、欧州人権条約や EU 基本憲章などの法的枠組みに結実している。

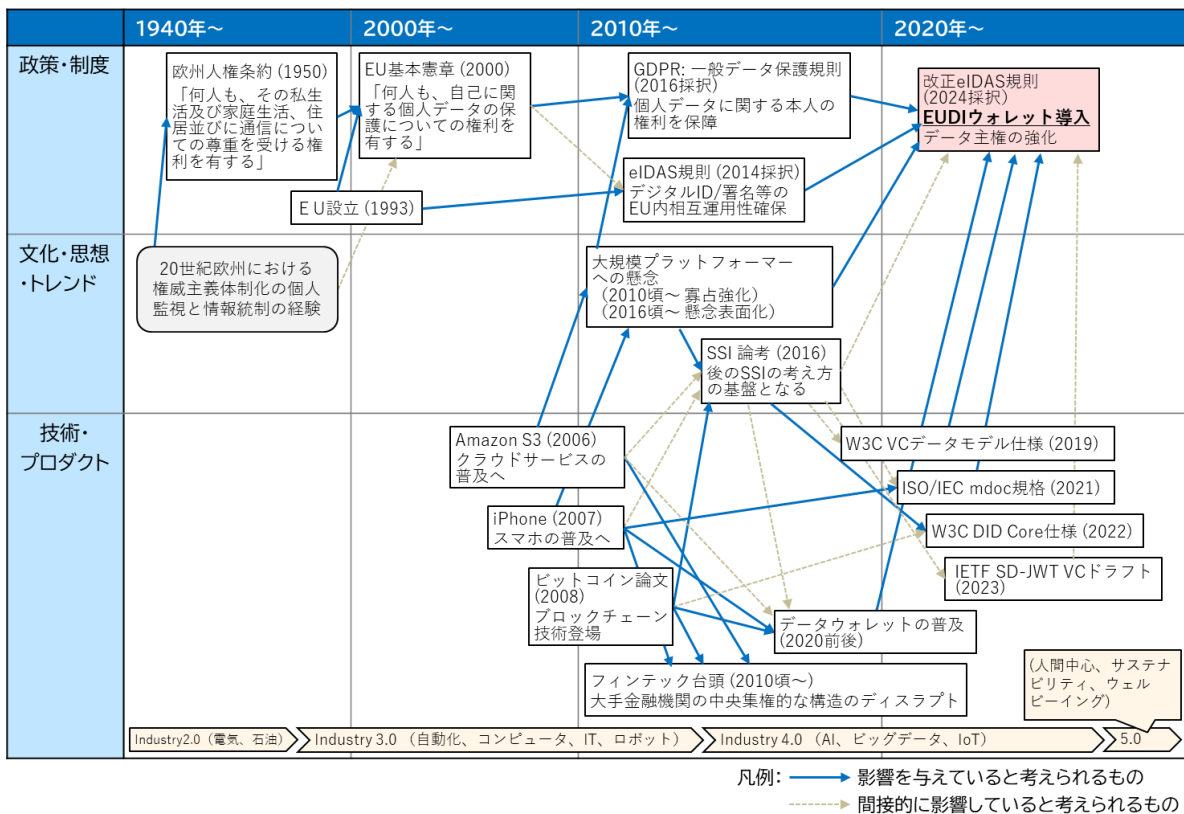
政策・制度面では、EU 統合の進展により人やサービスが国境を越えて移動するなかで、個人データの越境利用に関する共通ルールの必要性が高まった。2000 年代以降、個人データ保護を基本的人権と位置づける考え方が明確化され、2010 年代には GDPR として制度化された。GDPR が掲げる「データ主体の権利」や「データ最小化」の原則は、個人が自身の情報の扱いに主導権を持つべきだという考え方を制度として具体化したものと整理できる。

技術面でも変化が積み重なってきた。スマートフォンの普及やブロックチェーン技術の登場などにより、中央集権的な基盤に依存しない情報管理が現実的な選択肢となった。加えて、デジタル化社会において影響力を強める米国発の大規模プラットフォームへの懸念も相まって、分散型技術や暗号技術を活用した新たな信頼モデルが模索されるなかで、SSI (Self-Sovereign Identity: 自己主権型アイデンティティ) といった概念も注目を集めるようになった。

こうした文化的背景、制度的蓄積、技術環境の変化が相互に補強し合うことで、利用者が証明情報を保持・提示する EUDI ウォレットが制度の中核に据えられ、改正 eIDAS 規則へと収斂したと考えられる。

様々な背景の基に制度化され、共通仕様について大規模な実地検証による検証・改善を進めてきた EUDI ウォレットは、いよいよ本年末 (2026 年末) に、EU 加盟国による提供の期限を迎えようとしている。

図表 9 改正 eIDAS 規則に至る政策・文化・技術の流れ¹⁷



(出所) 各種資料より大和総研作成

本レポートでは3部作の導入として、デジタルアイデンティティの基本概念と、VC/三者モデルに代表されるデジタルクレデンシャルの共通構造を整理した。また、EUDI ウォレットを例に、制度化の背景（法制度・文化・技術）と実装推進の枠組み、検討される主要ユースケースを概観し、デジタルアイデンティティの導入が実社会でどのように進められているかの具体例を示した。

続く第2部では、EUDI ウォレットの提供期限（2026年末）が迫るなかで、EU加盟各国が進める取組みを中心に俯瞰する。あわせて、日本における取組みも取り上げ、実装の特徴などを比較することで、具体例を体系立てて示す。そして、第3部にて DID/VC、mdoc などの実装方式を技術面から整理・比較することで、「取組み」と「実装技術」を接続した体系的な整理を目指す。

デジタルアイデンティティの実装が加速するなか、各国の取組みを踏まえた方針策定や実装技術の選択は、すでに実務の要件定義・設計の判断として迫っている。その判断を支える論点整理を、本シリーズを通じて提示したい。

以上

¹⁷ 年数については、公表や提供開始年などを記載。明確な公表日などが確認できない事象については、各種資料を参照し、概ねの時期として年号を付している