デジタルアイデンティティを巡る世界の潮流

柴田 健久｜PwC コンサルティング合同会社ディレクター
崎村 夏彦｜OpenID Foundation 理事長、PwC Japan グループ Digital Identity 顧問

柴田 健久

PwC コンサルティング合同会社
ディレクター
地政学リスクや経済安全保障、各国の政策や規制、サイバー脅威を扱う Trust & Risk Consulting 部門に所属。
デジタルアイデンティティ技術を駆使した KYC、認証認可などが専門。
大手シンクタンクを経て PwC コンサルティング合同会社に入社。
デジタルアイデンティティ技術をコアとする事業企画などを担当。

崎村 夏彦

PwC Japan グループ
Digital Identity 顧問、OpenID Foundation Chairman
デジタルアイデンティティおよびプライバシー関連技術の国際標準化を専門としており、現在世界で 30 億人以上に使われている JWT、JWS、OAuth PKCE、OpenID Connect、FAPI、ISO/IEC 29100、ISO/IEC 29184 などの国際規格の著者・編者。

要約

デジタル社会は急速に進化し、金融業界においても、セキュリティの確保、プライバシーの保護、規制の遵守、そしてオープンバンキングの導入と企業間のデータ共有などが進んできた。このような中で、シームレスなユーザ体験を提供し、個々のユーザが自身の情報を管理できるようなデジタルアイデンティティの整備がますます重要となっている。

この論文では、オープンバンキングの動向に触れた上でデジタルアイデンティティが今後担う役割を説明したのち、金融業界に関係が深いと考えられる新たな技術であるデジタルアイデンティティウォレットを紹介する。そして最後に、デジタルアイデンティティ整備にあたり今後求められる相互運用性、政府を含む市場に求められる対応について考察する。

1．はじめに

現代社会は、デジタル技術の急速な発展により、かつてないスピードで変化している。API の普及で様々なサービスを組み合わせたサービスが生まれ、さらに時間の経過とともに生成された膨大なデータによって、新しいサービスが日々生まれている。ユーザも、様々な業種で自分のニーズや好みに合ったサービスが利用可能となり、ユーザ中心主義の視点で設計されたサービスを使用するデジタルライフを送ることができるようになってきた。

金融業界もこの例外ではなく、デジタル化・オープン化の波に直面している。オープンバンキングやオープンファイナンスの概念が広まり、金融機関は顧客データの共有と連携を通じて、より革新的で顧客中心の金融サービスを提供することが求められている。

この変革の中で、デジタルアイデンティティは、次世代のデジタル金融サービスを支える重要な役割を果たす。

本稿は、このデジタルアイデンティティに関する世界の動きについて紹介する。

2．デジタル社会とデジタルアイデンティティ管理の重要性

デジタル社会の進展に伴い、個人のアイデンティティ管理はより複雑かつ重要になっている。オンラインサービスの普及で便利となった一方、デジタル犯罪も多く発生しており、個人情報の保護とセキュリティの確保が喫緊の課題となっている。

デジタルアイデンティティは、個人に関するデジタル情報の集合体である。これには、氏名、住所、生年月日などの基本的な情報に加え、生体情報や行動データなど、あらゆる情報が含まれる。裏を返せば、デジタルアイデンティティを適切に管理することで、オンラインサービスへのアクセス制御、不正防止、個人情報の保護などを実現することができる。

金融業界においては、デジタルアイデンティティの管理は特に重要である。

オンラインバンキングはほぼすべての金融機関で導入されており、すでにデータの安全性と顧客のプライバシー保護が最優先事項となっているが、昨今はオープンバンキング、オープンファイナンスを導入する動きが各国で活発化しており、顧客データの共有と連携が進む中、さらに重要性が増してきている。

3．各国のオープン化に向けた取り組み状況

オープンバンキングについて、日本では 2017 年に改正銀行法が成立して API の提供が努力義務となった。その後も金融情報システムセンター（FISC）による API 接続チェックリスト[1]が策定されるなどで徐々にその活用が広がっているが、世界各国では、オープンバンキングの導入に向けた取り組みが進められている。

1:「API 接続チェックリスト〈2018 年 10 月版〉」一部改訂のお知らせ〈API 接続チェックリスト〉（2024-05-05 取得）

図1　各国のオープンバンキング状況

出所）筆者作成

ヨーロッパは早くからオープンバンキングに取り組んでおり、英国では2014年以降競争・市場庁（CMA）が主導して、オープンバンキングの標準APIの開発と導入、制度化が進められている。欧州連合（EU）でも2015年に制定された改正決済サービス指令（Payment Services Directive：PSD）2により、オープンバンキングの法的枠組みが整備された。

また、米国では包括的なオープンバンキング規制はないものの、市場主導型のオープン化が進んでいる。大手銀行やフィンテック企業が自主的にAPIを公開し、サードパーティーとの連携を進めている。2023年10月 に米消費者金融保護局（CFPB）が金融機関のAPIアクセスの無償化等の制度化を提案[2]。カナダでは、2024年中にオープンバンキングのフレームワーク（Consumer-Driven Banking Framework）を導入予定[3]と発表された。

アジアでも多くの国でオープン化が進んでいる。シンガポールでは、2015年に金融管理局（MAS）がフィンテック環境の整備を目的とした「FinTech & Innovation Group」を設立[4]し、オープンバンキングの推進に取り組んでいる。また、オーストラリアでは、2020年7月から段階的に実施されている[5]。

南米では、ブラジルがオープンバンキングの導入をリードしている。ブラジル中央銀行は2021年にオープンバンキング規制を施行し、金融セクターの競争力強化と金融包摂の促進を図っている。現在、5億口座以上が月間50億トランザクションをさばいているなど急速な成長を示している[6]。また、これに続く形でコロンビア、チリなどがオープンバンキングを推進している。

中東地域では、アラブ首長国連邦（UAE）、サウジアラビア、バーレーンなどが導入しており、金融セクターの革新と顧客サービスの向上を目指している。UAEでは特にドバイとアブダビの金融センターがオープンバンキングを推進[7]しており、サウジアラビアではOpen Banking Frameworkがすでに導入されている。

アフリカでは、ナイジェリアやケニアなどで進展が見られる。ナイジェリア中央銀行は2021年にオープンバンキング規制の枠組みを発表[8]し、金融包摂の促進を目指している。ケニアでは、モバイルマネーサービスが広く普及しており、オープンバンキングへの基盤が整っている。

2：CFPB Proposes Rule to Jumpstart Competition and Accelerate Shift to Open Banking< https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-jumpstart-competition-and-accelerate-shift-to-open-banking/>（2024-05-05取得）

3：Budget 2024: Canada's Consumer-Driven Banking Framework<https://www.canada.ca/en/department-finance/programs/financial-sector-policy/open-banking-implementation/budget-2024-canadas-framework-for-consumer-driven-banking.html>（2024-05-05取得）

4：MAS sets up new FinTech & Innovation Group<https://www.mas.gov.sg/news/media-releases/2015/mas-sets-up-new-fintech-and-innovation-group>（2024-05-05取得）

5：Australian Banking Association「Open Banking」<https://www.ausbanking.org.au/priorities/open-banking/#:~:text=Open%20banking%20gives%20you%20the,products%20or%20banks%20more%20easily.>（2024-05-05取得）

6：Banco Central do Brasil（2024），Pix Statistics < https://www.bcb.gov.br/en/financialstability/pixstatistics>（2024-05-15取得）

7：Arab Regional Fintech Working Group「Open Banking Regulatory Principles」（2021/3）<https://www.amf.org.ae/sites/default/files/publications/2021-12/open-banking-regulatory-principles.pdf>

8：REGULATORY FRAMEWORK FOR OPEN BANKING IN NIGERIA <https://www.cbn.gov.ng/out/2021/psmd/circular%20on%20the%20regulatory%20framework%20on%20open%20banking%20in%20nigeria.pdf>（2024-05-05取得）

4．次世代デジタル金融とデジタルアイデンティティの関係

デジタル化とオープンバンキングの進展により、次世代のデジタル金融サービスが登場しつつある。

オープン API を通じたデータの共有と連携は、革新的な金融サービスの開発を加速させている。

欧州委員会は PSD3 の提案に際して公開したデータで、EU における電子決済は、2017 年の 184.2 兆ユーロから、2021 年には 240 兆ユーロに増加したとしている[9]。

9：https://ec.europa.eu/commission/presscorner/detail/en/fs_23_3558

これらの次世代デジタル金融サービスを支えるのが、デジタルアイデンティティである。デジタルアイデンティティは、ユーザを一意に識別し、認証し、プライバシーデータを管理し、利活用するために必要な機能を持つ。これにより、ユーザは個人情報を安心して預けられるし、事業者はユーザの同意を得られた範囲でデータを分析し、ユーザのニーズに合ったサービスを提供することができる。

さらに、デジタルアイデンティティは、金融包摂の実現にも大きな役割を果たす。

デジタル化されたセキュアな本人確認・認証により、これまで金融サービスへのアクセスが限られていた層に対して、新たな金融サービスを提供することが可能になる。また、モバイルマネーサービスなどのデジタル金融サービスを安全かつ効率的に展開することができる。

次世代のデジタル金融サービスにおいては、セキュリティとコンプライアンスの確保が非常に重要である。特に、デジタルオンボーディングプロセスでは、金融サービス機関は身元確認を厳密に行うことが必要である。これにより、新規アカウント詐欺、アプリケーション詐欺、カード情報盗難、アカウントの乗っ取りなどから自身と顧客を守ることができる。また、銀行支店で発生する特定の種類の詐欺を防ぐためにも、デジタル身元証明の利用が有効である。

また、オープン API を通じたデータの共有と連携をする場合、プライバシー保護、セキュリティ確保とリスク管理をエコシステム全体で構築する必要がある。そのためには、金融機関、フィンテック企業、規制当局が協力し、データの適切な取り扱いとセキュリティ対策を確保することが不可欠である。そして、オープンバンキングにおけるデータ保護とセキュリティに関する明確なガイドラインを策定し、関係者がこれらのルールを遵守していることを監督する仕組みをつくることが必要だろう。

次世代のデジタル金融サービスにおいては、デジタルアイデンティティの管理が重要な役割を果たす。金融機関、規制当局、テクノロジー企業が協力し、デジタルアイデンティティの管理体制を強化しながら、革新的で包摂的なデジタル金融の未来を築いていくことが求められている。

5．次世代デジタル金融におけるデジタルアイデンティティの役割

これまで述べたように、次世代デジタル金融において、デジタルアイデンティティには大きな貢献が期待されている。まず、デジタル身元確認と呼ばれる技術を活用することで、オンラインでの本人確認が容易になり、金融サービスへのアクセスが大幅に向上する。これにより、これまで金融サービスを利用できなかった人々も、容易にサービスを利用できるようになる。また、複数のフィンテックサービスで同様の手続きをしなくてもよくなることで、ユーザはサービスごとに異なるアカウントを管理する必要がなくなり、利便性が飛躍的に向上する。これにより、金融サービスの実利用率が向上し、金融包摂の進展に寄与することが期待される。

しかし、これらの期待に応えるためには同時に、デジタルアイデンティティがいくつかの重要な役割を果たす必要がある。具体的には、個人のプライバシー保護と信頼性の向上、金融犯罪の防止とコンプライアンスの強化、そして分散型アーキテクチャによる相互運用性の実現である。以下では、これらの役割について詳しく説明する。

5.1 個人のプライバシー保護と信頼性の向上

デジタルアイデンティティが果たすべき最も重要な役割の一つは、個人のプライバシー保護と信頼性の向上である。プライバシーについては、日本の個人情報保護法の他、EU の EU 一般データ保護規則（General Data Protection Regulation) 等、各国・地域で法整備が進んでいる。米国でも現在、米国プライバシー権法（American Privacy Rights Act）が審議中である。これらの法制度は、消費者のプライバシーを守るために、事業者に対して消費者データの収集、使用、販売に関する高い透明性と、データプライバシーとセキュリティの管理監督を義務付けている。

そして、その実現には個人、その個人から個人データを収集する主体、個人データを処理する主体の役割と責任を明確にし、適切に運用することが必要である。これらが実現できれば、信頼性が大幅に向上する。

他に個人情報の開示についても、個人が状況に応じて選択的に開示することができるような技術の標準化が進められているが、このような技術が普及すれば、個人は自分の情報を自分の意思で管理できるようになり、プライバシーと利便性の両立に寄与し得る。

5.2 金融犯罪の防止とコンプライアンスの強化

デジタルアイデンティティのもう一つの重要な役割は、金融犯罪の防止とコンプライアンスの強化である。

そのためにはまず、信頼できる証拠に基づく厳格な本人確認プロセスの実施と、その実施記録の保存をすることが重要である。このことにより、なりすましや不正アカウントの作成の抑止、不正行為の調査や監査が可能となる。

さらに、マネーロンダリングや不正送金などのリスクの高い取引にデジタルアイデンティティをキーとする行動分析技術を適用すれば、利便性とのバラ

ンスを保ちながら不正リスクの低減や規制当局からの要件遵守に寄与するだろう。

日本ではすでに、金融機関は eKYC やマネーロンダリング対策（AML）をより効果的に行うことができるようになり、効率化が進められてきた。2018年の「犯罪による収益の移転防止に関する法律施行規則」の改正でオンラインでの本人確認が認められ、PC やスマートフォンで撮影した本人確認書類の送付や公的個人認証サービス（JPKI）の署名用電子証明書（マイナンバーカードに搭載されている署名用電子証明書）の利用が可能となっている。

ただし現在、各国ではさらにこの見直しが進もうとしている。

例えばデジタル庁が公表する「DS500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（DS500）のベースの一つとなった米国 NIST の「SP 800-63 Revision 3 Digital Identity Guidelines」は、Revision 4 として更改される動きがある。ここには、リモートで厳密な身元確認を実施する場合、訓練されたオペレータによる監視下であること[10]などが記載されているが、現在日本はこれを必須としていない。

他にも、英国でも 2024 年 1 月に身元確認の基準となるガイド「How to prove and verify someone's identity Good Practice Guide 」[11]が更新された。また、AML にあたってデジタルアイデンティティの技術をどのように活用できるか、具体的なガイダンス作成が検討されている。

今後、国境を越えたデータのやり取りを行うことを視野に入れた場合、これらのグローバル規制との乖離はできるだけ発生しないようにすべきである。2023 年 6 月には犯罪対策閣僚会議より「国民を詐欺から守るための総合対策」[12]がとりまとめられ、オンラインの本人確認手法はマイナンバーカードの公的個人認証に原則として一本化し、運転免許証や顔写真のない本人確認書類等は廃止する方針が示された。また、上記の DS500 も現在、グローバルとの乖離があった場合、どう向き合うのかデジタル庁にて見直しの議論が進められている。当然、民間サービスへの波及も考えられることから注目が必要である。

5.3 シームレスなデジタルライフを実現する仕組みと相互運用性の実現

次世代デジタル金融においては、様々な金融サービスが相互に連携し、シームレスなユーザ体験を提供することが求められる。しかし現状では、多くの金融機関が独自のデジタルアイデンティティシステムを構築しているためサイロ化が進んでおり、サービス間の連携が困難になっている。

この問題を解決するためには、接続が容易なデジタルアイデンティティアーキテクチャを採用し、相互運用性を実現することが不可欠である。これができれば、様々なシーンで検証可能なアイデンティティの発行や管理を行うことができる。これにより、異なる金融サービス間でもアイデンティティの相互運用性を確保することができるであろう。

現在、分散型アイデンティティの標準技術として、Verifiable Credential や OpenID Connect の拡張仕様の検討が活発となっている。これらの標準技術を採用することで、金融サービス間でのアイデンティティの相互運用性を実

10：National Institute of Standards and Technology:NIST (2023), NIST SP 800-63 Digital Identity Guidelines SP 800-63A 5.5.3 In-person Proofing Requirements <https://pages.nist.gov/800-63-4/sp800-63a.html#vip> (2024-05-05 取得)

11：イギリス政府 (2023), Guidance How to prove and verify someone's identity <https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual> (2024-05-05 取得)

12：犯罪対策閣僚会議「国民を詐欺から守るための総合対策」（総務省 < https://www.soumu.go.jp/main_content/000953287.pdf>）(2026-07-04 取得)

現し、ユーザの利便性を大幅に向上させることが可能となるだろう。

本節では、次世代デジタル金融におけるデジタルアイデンティティの役割について紹介した。デジタルアイデンティティは、個人のプライバシーを保護しつつ、金融サービスのアクセシビリティと利便性を向上させるために不可欠である。また、金融犯罪を防止し、コンプライアンスを強化するためにも、デジタルアイデンティティのセキュリティ要件が重要である。

さらに、異なる金融サービス間でのアイデンティティの相互運用性を確保するためには、標準化が不可欠である。

次節では、これらの点についての最新動向を紹介する。

6．デジタルアイデンティティの技術動向

6.1 Verifiable Credentialの必要性

サービス登録に必要なアイデンティティ情報は多岐にわたる。具体的に3つの事例を取り上げて確認してみよう。

法人口座開設の例

- 履歴事項全部証明書（商業登記簿謄本）：法人の基本情報が記載されている公的な書類。法務局で取得可能。
- 法人の印鑑証明書：法人が登録している印鑑の証明書。法務局で取得可能。
- 代表者の本人確認書類：代表者の身分を証明するための書類（運転免許証、パスポートなど）。
- 法人番号が確認できる書類：法人番号を記載した書類。法人番号通知書などが該当。
- 事業実態を証明する資料：会社案内、ホームページのプリントアウト、契約書のコピーなど、事業が実際に存在していることを示す資料。
- 委任状：代表者以外の人が口座開設の手続きを行う場合に必要な書類。

携帯電話契約の例

- 運転免許証
- マイナンバーカード（個人番号カード）
- パスポート
- 在留カード
- 身体障害者手帳、精神障害者保健福祉手帳、療育手帳
- 預金通帳＋お届け印（クレジットカードやキャッシュカードがない場合）

大学院入学の例

- 卒業証明書ないし卒業見込み証明書
- 成績証明書
- 推薦書

- 健康診断書

これらは従来、紙やプラスチック板の目視やコピー、またはそれに準ずる手段で確認されることが多かった。
しかし、偽造技術の進展とともにこの検証が非常に困難になってきており、一人数百万円オーダーの被害が相次ぐようになってきている。

これをデジタル化して容易に検証が可能にしようというのが検証可能クレデンシャル（Verifiable Credential：VC）の取り組みである。これらがデジタルで自動検証できるようになることで、事故が減るだけでなく、経済効率性も大幅に向上し、GDP の増加にも寄与すると考えられる。そのためには、こうした証明書類がすべからず検証可能資格証明書として提供されるようになることが肝要である。

VC は証明対象となるデータに、証明書発行者の電子署名ないしは電子シールがついたものだ。現在主流のフォーマットには CBOR ベースの mdoc（ISO/IEC 18013-5 で定義）と、SD-JWT VC（IETF で定義）があるが、それ以外にも多種多様なものが存在する。日本政府がマイナンバーカード関連で利用している X.509 も広い意味ではこの中に含まれる。Open Wallet Foundation は 2024 年 5 月 8 日時点で 16 種類をリストしている[13]。

これを対象者 (subject) が操る（通常はスマホ上で稼働する）ウォレットと呼ばれるソフトウェアに発行、格納する。発行に使われるプロトコルとして、例えば、EU が制定中のウォレット関連の規格である EU Digital Identity Architecture and Reference Framework 1.4（ARF 1.4）[14] では OpenID for Verifiable Credential Issuance（OpenID4VCI）が指定されている。
こうして保管された VC は、対象者のウォレット操作によって「提示（presentation）」と呼ばれるプロセスを通じてその利用者（RP、検証者）に検証可能提示（Verifiable Presentation：VP）として提供される。VP には対象者がウォレット上で生成した鍵による署名がついている。ARF 1.4 では、この提示のプロトコルとしては、近接提示は ISO/IEC 18013-5 が、遠隔提示には、OpenID for Verifiable Presentation が指定されている。

検証者はこれを受け取り、VC にかかっている署名を確認し、署名者の正当性を確認することによって、証明書記載事項が正しいことを確認できる。
また、提出者と証明書に記載されている人が等しいことは（ここでは提出者同一性とよぶ）、証明書に含まれる
A）提出者の生体情報
B）提出者の鍵情報（ウォレットソフトウェアが生成したもの）
などによって確認可能である。

生体情報は主に提示を受けるのが「人」であるケースを想定している。VC

13：OWF(2024) credential-format-comparison-sig/data/Credential-Format/ https://github.com/openwallet-foundation/credential-format-comparison-sig/tree/main/data/Credential-Format

14：European Commission (2024), EU Digital Identity Architecture Reference Framework 1.4 < https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md> (2024-07-04 取得)

に入っている顔写真と提示者を目視確認するような場合だ。専用ハードウェアが利用できる場合、この目視はカメラ画像による確認で代替できるかもしれない。

鍵情報の場合は、VC を VP として提示する時に、その鍵による署名が付されることによって示される。

提出者の鍵情報を VC に含めることによって提出者同一性を確保する場合には、VC に含む鍵が本当に想定する個人や法人のものであるか、発行先となるウォレットが正しいものであるかを確かめる必要がある。この確認の厳密さによって、欧州では 2 段階のものが設定されている。

6.2 従来のモデル（アイデンティティ・フェデレーション）との違い

こうした属性連携のデジタルな仕組みで現在主流であるのは、OpenID Connect などのアイデンティティ連携（Identity Federation）の方式である。OpenID Connect でも、VC における発行者にあたる Claims Provider (CP) というものが存在する。ここが署名付きの属性証明を出し、これを OpenID Provider (OP) と呼ばれる上記のウォレットにあたるソフトウェア（ただし、通常これはクラウド上のシェアードサービスとして実装される）を通じて提供される形だ。トポロジー的にはほぼ同じものになるが、実態上はいくつかの大きな差がある。

① OpenID Connect の場合、検証者が受け取るデータには OP の署名（対象者の署名とは異なる）がついている。したがって、個人の署名の代替としては使えない。一方で、EU Digital Identity Wallet（EUDIW）では署名サービスを提供することになっている。

② ウォレットは殆どの場合ユーザは一人であるのに対して、OP は大量の人でシェアする。これは、受け取り手による個人の識別性を下げる（k- 匿名性の確保）という意味では望ましいが、多量のユーザをプロバイダが観測して広告に使うなどという観点からはプライバシー的に望ましくないとされる（ただし、EUDIW がそうしているように、法規制すれば良い問題ではある。逆に、これができないようにすることによって EUDIW にはビジネスモデルがなくなり、民間レベルでの運用が難しいということも指摘されている。）。

③ OP はネットワーク上で常にオンラインであることが期待され、検証者は随時最新の情報を得ることができるが、ウォレットはオフラインであることが期待され、ユーザが行動を起こした時にしか情報が提供されない。

④ CP からの情報を OP が中継する方式は標準で定義されているものの、実際にはほぼ使われておらず、各 CP が OP として振る舞って直接属性提供する場合が殆ど。一方、EUDIW では直接提供のパスは用意されておらず、必ずウォレット経由での提供となるため、中継機能が必ず活用されるようになることが期待される。また、これによってユーザからすると一括管理がしやすくなるというメリットがある。

⑤ OP は CP から事前に発行を受けた属性証明はその一部を選択的に提供す

ることはできない。選択的に提供しようとすると、都度 CP から必要なものだけを取得することになり、これは CP も 24 時間 365 日運用が必要であるということになり、運用負荷が重い。

⑥ 複数の CP からの情報を連携しようとするとそれだけ取得時間がかかることになり、あらかじめ取得しておいてまとめて提示できるウォレットモデルに対して使用体験が悪くなる。

また、一般の方がウォレットを初めて知ったときに受ける印象として、

① ウォレットはユーザデバイス上で稼働するのでユーザのコントロール下にあり、プライバシー的に有利

② 個人の情報がサーバに蓄積されないので、抜かれることがなくなり安全

といった点も指摘されるが、実はこれらは必ずしも正しくない。例えば、対象者に関する情報をウォレットがバックエンドのサーバに送って利用するということは十分に考えられる。また、属性情報をオンラインで集積している問題は、元となる情報はもとより VC の発行者に溜まっているのであり、そこを攻撃すれば OP を攻撃するのと同様かそれ以上の効果がある。また、ある個人を攻撃するという観点で言えば、ウォレットに溜まった情報を詐欺サイトなどを通じて一気に抜く方が効率が良い。そのため、上記のメリットを享受しようとすると、追加で条件が必要になる。EU のデジタルアイデンティティフレームワークでは以下のような条件が課されている。

① ウォレットのアプリ部分はオープンソースで提供されなければならない（EU DIF 5a-3）。

② ウォレットの提供者に、プライバシー保護技術と不可観測性を実装し、提供者がユーザの行った取引の詳細を見ることができないようにしなければならない。また、その提供者は審査機関によって審査・認定を受けなければならない。

③ VC を利用する RP/ 検証者はその正当性を示すために、ウォレットに対して運用者情報を含めてクライアント認証を実施できなければならない。

④ PID の発行を受けるウォレットは認定されたものでなければならず、Wallet Instance Attestation というものを使ってそのインスタンスのクライアント認証が可能である必要がある（なお、こうしたウォレットは特定の認可されたスマートフォンの上でしか稼働しない模様。2024 年 4 月時点 4 種類のみとされる[15]。）。

ウォレットのオープンソース化ということに関しては、すでに EU ではオープンソースのリファレンス実装が公開されており、各国はこれを元に実装を行っていく方針となっている。また、このソースコードは Open Wallet Foundation にとりこまれ、そこでメンテナンスが行われていく見込みである。ただし、これにかかる費用を誰がどのように負担していくのかというのはまだ検討課題として積み残されている。

また、そのウォレットの提供者の運用に関しては、上記のとおり厳しく規制

15：Bradley, (2024) Split Key ECDSA and ARKG for Wallet Proof of Possession, IIW38 Notes https://docs.google.com/document/d/1DjOS1MOjJtt0BporEHXrcfHnfbfJmif9uXhHEhGIC1s/edit（2024-05-15 取得）

がなされる。

加えて、RP の正当性およびその要求する属性が必要最低限のものになっているかの確認が第三者によって行われ、それが明示されることが望ましいと思われる。

この他、EUDIW には以下のような機能が期待されている。

- EUDIW は、EU 市民と居住者が自分の個人データとアイデンティティ関連情報を安全、ユーザフレンドリー、かつ透明性の高い方法で管理、保存、共有できるように設計されたツールである。
- このウォレットにより、ユーザは自分の個人データと属性の電子的証明を安全に要求、取得、選択、組み合わせ、保存、削除、共有、提示することができ、データを信頼当事者に選択的に開示することができる。
- ウォレットを通じて実行されたすべての取引を追跡し、信頼当事者に個人データの即時消去を要求し、個人データの疑わしい要求を管轄の国内データ保護機関に報告することもできる。
- ゼロ知識証明などのプライバシー保護技術を統合し、基礎となるデータを明らかにすることなく、ユーザの識別データに基づいて記述を検証することができる（ただし、ARF 1.4 にはゼロ知識証明は入っておらず、選択的属性開示だけが入っている。）。
- ユーザには、EUDIW の設計に組み込まれた共通のダッシュボード機能が提供され、自分の個人データに対する透明性、プライバシー、コントロールを持つことができる。
- データの取り扱いに関する目的の制限、収集するデータの最小化、設計段階からデータ保護の観点を含め、利活用と保護の設定を可能とする場合は保護をデフォルト設定する。

全体として、このウォレットは、民主主義社会、基本的権利、法的保護措置を守ることを目的として、透明性が高く、ユーザが管理でき、相互運用性のあるように設計されることが期待されている。

また、プライバシー面に関しては、電子識別と認証に最高レベルのデータ保護とセキュリティを課している点を強調しており、ユーザが EUDIW の使用とデータを完全にコントロールできること、そして、そのようなウォレットの使用は任意であり、それを使用しない人に対して公的または私的サービスへのアクセスを制限しないことを保証するものになっている。

7．今後の展望と課題

以上、次世代デジタル金融におけるデジタルアイデンティティの重要性と、その実現に向けた技術動向について述べてきた。

ユーザが自身のアイデンティティをコントロールできる分散型のアーキテクチャとして、DID（分散型識別子）や VC などの具体的な実現手段が成熟し、関連するフレームワークや規制が進歩することは、異なるサービス間でのアイデンティティの相互運用性の実現を後押しし、デジタルアイデンティティがパーソナライズされた金融サービスの提供や、異なる金融サービス間でデータを連携させ、より最適化された金融サービスの提供が可能になる。

最後に、特に注目すべき 2 つの動きとその課題について紹介する。

7.1 ウォレットの普及と官民の役割分担

前述のように eIDAS2.0 が承認され、EU では EUDIW の普及と社会実装が進められることが予想される。

また、日本では 2023 年来、スマートフォンでマイナンバーカードが提示できるようになってきている。同じく 2023 年には「マイナンバーカード機能等のスマートフォンへの搭載に係る実証事業（技術検証・要件検討）」の調達公募などもあり、政府によるウォレットの提供に向けた検討が進められていると考えられている。

そして、このウォレットに関する議論が国内外で活発に行われている。

ウォレットを使用することで、ユーザは自身の個人データを安全に管理し、必要な場面で適切に提示することができるようになることが期待されている。また、政府発行のアイデンティティ情報でユーザオンボーディングしたり、民間事業者の提供する個人データを政府の提供するウォレットに格納したりすることで、利便性が高まる可能性がある。

民間事業者にとっても、本人確認のコストを下げるなどのメリットを享受できる可能性もある。

ただし、政府が提供するアプリケーションに個人データを格納し、様々なシーンで利用できるようになることは、政府が国民がいつどんなオンラインサービスを使っているのかなど、プライバシー情報へアクセスできる可能性があることを意味する。

この点について、日本で議論になっている他、同じように EU でも多くの意見が寄せられたとされており、今後、管理・監督方法や透明性確保の方法などの議論が必要な状況となっている。

7.2 国際的な相互運用性の確保

オープンバンキング、ウォレットなどの普及には大きな期待がかかる反面、参加者の間で信頼性の高い異業種・国際間の連携をシームレスに実現するには、相互運用性の確保はますます重要な課題となるだろう。

こうした中 2024 年 5 月、デジタル庁が EU とデジタルアイデンティティに関する協力覚書を交わしたとの発表があった[16]。将来的なアイデンティティマネジメント体系の相互承認に向けた課題についても検討を始めるとされている。

デジタルアイデンティティ技術の発展は、次世代デジタル金融におけるビジ

16：デジタル庁（2024）, 河野デジタル大臣はブルトン欧州委員と会談を行い、EU とデジタル・アイデンティティに関する協力覚書を交わしました <https://www.digital.go.jp/news/eea22370-19d8-4a1a-ae92-89e28476f9a1>（2024-05-05 取得）

ネスの加速とセキュリティの向上に大きく貢献することが期待される。そのために技術や相互運用性の確保のための議論は開始されており、政府側の動きが活発である。

金融機関が、デジタルアイデンティティを核とした新たなビジネスモデルの創出に積極的に取り組むのであれば、これらの動向は注視すべきであり、必要に応じて参加していくべきであろう。