「欧州デジタル ID 枠組み規則」制定の経緯と欧州デジタル ID ウォレットの共通仕様

― EUDIW Architecture framework v1.4からみる技術仕様 ―

中山 靖司｜SBI 金融経済研究所 主任研究員　SBI 大学院大学 客員教授
NPO 法人金融 IT 協会 理事

中山 靖司
SBI 金融経済研究所 主任研究員
SBI 大学院大学 客員教授
NPO 法人金融 IT 協会 理事
1964 年生まれ。東京工業大学（院）経営工学修士。1988 年日本銀行入行。主に情報セキュリティや電子決済関係の実務および調査・研究に従事し、1996 年日銀における CBDC 研究の先駆け「日銀－ NTT 方式」電子通貨を研究・開発。東京大学先端経済工学研究センター（現在先端科学技術研究センターに吸収）助教授、FISC 調査部長等を歴任後、日銀金融高度化センターで「IT（AI）を活用した金融の高度化に関する WS」（全 10 回）を企画し座長を務める。特許「発行機関分離型番号登録式電子現金方法および利用者装置」他。

要約

本稿は、2024 年 5 月に発効された「欧州デジタル ID 枠組み規則」制定の経緯を紹介するとともに、その規則に基づき EU 市民に提供することが義務付けられた欧州デジタル ID ウォレット（EUDIW）のユースケースや技術仕様（設計原則、エコシステム、個人識別データの概要等）について解説したものである。EUDIW は、公共および民間のデジタルサービスを受ける際に本人確認の手段として利用できるアプリであり、ユーザーが自身の ID データや属性情報を安全に保存・管理できる等の特徴がある[1]。一方、日本でも、マイナンバーカードに健康保険証や運転免許証の情報を紐づける取組みや、マイナンバーカード自体をスマートフォンに載せるための法整備等が進んでいるが、EUDIW のような、本人認証にかかる属性情報を管理するデジタル ID ウォレットの発想からデザインされたものではない。そのため、EUDIW を参考に、将来を見据えてグランドデザインを見直すことが必要ではないだろうか。

1．はじめに

「欧州デジタル ID 枠組みの構築に関する規則＜（EU）第 910/2014 号を改正する欧州議会および理事会規則＞」（欧州デジタル ID 枠組み規則）が欧州議会および EU 理事会の双方によって承認され、2024 年 5 月 20 日に発効された[2]。

本規則は、2014 年に制定された「域内市場における電子取引のための電子

1：一般に、「ウォレット」とは主にスマートフォンやタブレットなどのデバイスに搭載される、財布の役割を提供するものであり、支払い機能に加えて、デジタル資産・ID 属性情報などの管理もできるとされる。EUDIW は、ID 属性情報管理機能の面からウォレットを活用するものであり、デジタル資産管理や支払い機能については触れられていない。

2：本規則は、2021 年 6 月に欧州委員会によって提案され、欧州議会、EU 理事会において検討作業が進められていたが、2023 年 6 月、提案の主要な要素についての暫定的な政治的合意に達し、同年 11 月、三者協議で最終合意した。これを受けて、同規制案は 2024 年 2 月に欧州議会で、4 月に EU 理事会で採決が行われ、2024 年 5 月に発効された。これで EU における正式な手続きが一区切りついたことになり、各加盟国は 2026 年までに対応を迫られることになった。

的本人確認およびトラストサービスに関する規則」（eIDAS 規則）[3] を改正するもので、EU 域内で公共サービスを安全に利用し、オンライン上および国境を越えて取引を行うための基礎を築くものである。特に、欧州デジタル ID ウォレット（以下、「EUDIW」と呼ぶ）を通じて、すべての EU 市民、居住者、企業が利用できる欧州デジタル ID の枠組みについて定めているところが注目される。

今後、技術仕様と認証の概要を定めた複数の実施法が採択され、加盟国は 24 カ月以内に、EUDIW を市民に提供する義務を負うことになる。規則承認後 6 ～ 12 カ月で定められた期限[4] までに採択されるこれらの法律は、規則の制定プロセスと並行して検討作業が進められている、技術的な共通仕様や要件を定める「EU デジタル ID ツールボックス」と整合するものとなることが求められており、これによって欧州全体でウォレットが統一的に実装されることが保証されることになった。

図表1　EUDIWに関する規則制定の流れ

2014/7/23	「域内市場における電子取引のための電子的本人確認およびトラストサービスに関する規則」（EU）第 910/2014 号（「eIDAS 規則」）制定
2020/10/1-2	**欧州理事会（European Council）** 欧州委員会に対し、相互運用可能な電子署名を含む、安全な公的電子 ID のための EU 全体の枠組みを提案し、オンライン上の ID やデータを管理できるようにするとともに、公的、私的、国境を越えたデジタルサービスへのアクセスを可能にするよう求めた。
2021/3/9	**欧州委員会（European Commission）** 通達「2030 年デジタル・コンパス:デジタルの 10 年に向けた欧州の道」[5] において、2030 年までに、欧州連合（EU）とその市民が、信頼され、ユーザーが管理できるアイデンティティを広く普及させ、各ユーザーがオンライン上でのやり取りや存在を自分で管理できるようにする、という目標を掲げる。
2021/6/3	**欧州委員会「欧州デジタル ID 枠組みの構築に関する規則**＜（EU）第 910/2014 号を改正する欧州議会および理事会規則＞」（「欧州デジタル ID 枠組み規則：eIDAS 規則改正案」）[6] を提出。
2022/12/14	**欧州議会（European Parliament）および EU 理事会（Council of European Union）**「デジタル 10 年政策プログラム 2030 の策定」[7] で、2030 年までに、信頼され、自発的で、ユーザーが管理するデジタル ID を広く普及させることを目的とした欧州連合の枠組みの目的とデジタル目標を定める。
2023/1/23	**欧州議会、欧州理事会および欧州委員会** 「デジタルの 10 年に向けたデジタルの権利と原則に関する欧州宣言」[8] で、EU に住むすべての人が、データ漏洩や個人情報の盗難や改ざんなどのサイバーセキュリティのリスクやサイバー犯罪から保護された、幅広いオンラインおよびオフラインのサービスへのアクセスを可能にする、安全かつ信頼できるデジタル ID を提供することを宣言した。また、すべての人が使用方法や共有先を自ら管理する等によって、個人データの保護を受ける権利があるとした。

3：「eIDAS 規則」の目的は、公共サービスを利用するための政府電子 ID（「eID」）の国境を越えた承認を可能にし、従来の同等の紙ベースのプロセスと同じ法的地位で国境を越えて承認されるトラストサービスのための連邦市場を確立すること。

4：期限は、欧州デジタル ID 枠組み規則の中で、内容により 2024 年 11 月 21 日ないし 2025 年 5 月 21 日までとされている。

5：COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS 2030 Digital Compass: the European way for the Digital Decade COM/2021/118 final https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

6：EU における立法手続きでは、欧州委員会（European Commission：EU の行政執行機関）が発議権を持ち、EU 理事会（Council of European Union：EU の立法機関）と欧州議会（European Parliament：EU 市民の代表）に法案を提出し、双方で可決されれば、正式に法案成立となり、官報掲載後 20 日後に発効する。同規則に関する具体的な立法手続きの流れについては、以下の URL を参照。
https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=celex:52021PC0281#2023-12-07_APR_AGRPROV_CONSIL_byEP_CMT

7：Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Official Journal of the European Union, L323, 19.12.2022, p.4)

8：European Declaration on Digital Rights and Principles for the Digital Decade (Official Journal of the European Union, C23, 23.1.2023, p.1)

2023/2/10	European Digital Identity Wallet Architecture and Reference Framework（ARF）の初版公開[9]
2023/5 月	ARF を基にした4つの大規模パイロット・プロジェクトの開始
2023/6/29	**欧州委員会**　欧州議会および EU 理事会と、**「欧州デジタル ID 枠組み規則」**の主要な要素について暫定的な政治的合意に達する。
2023/11/8	**三者協議**（欧州委員会、欧州議会、EU 理事会）で最終合意
2024/2/29	**欧州議会**で最終承認
2024/3/26	**EU 理事会**　第 4016 回会合で採択＜ ST 8552 2024 ＞
2024/4/11	**欧州議会議長**および **EU 理事会議長**による**署名**[10]**(EU)第 2024/1183 号**
2024/4/30	**EU 官報に掲載**
2024/5/20	**発効**（EU 官報掲載から 20 日後）　同規則は 2026 年までに完全に施行
2024/5/20	European Digital Identity Wallet Architecture and Reference Framework（ARF）の 1.4 版公開 [11]

出所）　筆者作成

2.「欧州デジタルID枠組み規則」の制定の経緯

2.1 背景

従来の eIDAS 規則では、EU 加盟国は任意で国内の eID（オンラインサービスにおいて利用できるデジタル ID）制度を届け出ることができ、他の加盟国はそれを承認する義務を負っていた（義務化は 2018 年）。しかし、加盟国が eID を整備すること自体は任意であり義務ではなかった。また、様々な eID システムを接続する上部構造を構築することで、相互運用性を確保しようとしていたが、各国間の整合がとれないという技術的な問題が発生しやすく、民間のデジタルサービスへの拡大も妨げられていた。

こうした中、2020 年 10 月、EU 加盟国の首脳らをメンバーとする EU の政治的最高意思決定機関である欧州理事会は、欧州委員会に対し、相互運用可能な電子署名を含む、安全な公的電子 ID のための EU 全体の枠組みを提案し、公的、私的、国境を越えたデジタルサービスへのアクセスを可能にするよう求めた。

これを受け、欧州委員会が実態をまとめたところ、2018 年 9 月に eIDAS 規則の eID 部分が発効して以来、少なくとも 1 つの eID スキームを通知している加盟国は 27 カ国中わずか 14 カ国と約半分に過ぎず（2021 年現在）、その結果、国境を越えて信頼できる安全な eID スキームにアクセスできるのは、EU 居住者の 59% にとどまっていた。また、現在のユーザーニーズに応えられるよう、完全にモバイル対応まで済ませている eID スキームは 7 つしかなかった。

そこで、2030 年までに、少なくとも 80％の市民が、主要な公共サービスを利用する際にデジタル ID ソリューションを使用できるようにするため、現

9：The European Digital Identity Wallet Architecture and Reference Framework v1.0
https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

10：Document 32024R1183, Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1183

11：European Digital Identity Wallet Architecture and Reference Framework v1.4.0
https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/#314-qualified-and-non-qualified-electronic-attestation-of-attributes-schema-providers

行の枠組みを改訂した欧州デジタル ID を新たに提供することを提案した。eIDAS 規則では提供が任意だったことから普及が十分でなかったこともあり、新しい規則では、加盟国に対し、国のデジタル ID を他の個人属性（運転免許証、卒業証明書、銀行口座など）の証明とリンクできるデジタルウォレットを市民や企業に提供することが義務付けられるものとなった。

2.2 EUデジタルIDウォレット（EUDIW）の特徴

EUDIW は、アプリの形をした ID や属性情報を管理する個人用デジタル財布であり、市民がデジタル形式で自分自身を識別し、ID データや公文書を保存・管理することを可能にする。その特徴は、① EU デジタル ID を利用したい EU 市民、居住者、企業は誰でも利用できること[12]、② EU 全域で公共および民間のデジタルサービスへのアクセスをユーザーに提供する際の本人確認手段として使用されること、③利用者が第三者と共有する ID、データ、証明書を選択し、追跡できるようにするとともに、共有する必要のないものは共有されないなど、ユーザー自らが EUDIW を管理できること[13] である。

ユースケースとしては、例えば、運転免許証、医療処方箋、教育資格などが含まれるとされるが、新しい EUDIW により、モバイルデバイスのボタンをクリックするだけで、身元を証明したり、電子文書を共有したりできるようになり、欧州のすべての人々は、欧州全域で利用可能な自国のデジタル ID を使ってオンラインサービスにアクセスできるようになる。その期待されるメリットは以下のとおり。

（市民と企業）
1. **ユーザーのコントロール**：市民は、自分のアイデンティティやデータのどの側面を第三者と共有するかを選択する権限を持ち、個人情報のプライバシーと管理を保証する。
2. **広範なユーザビリティ**：EU 全域で、公共および民間のデジタルサービスへのアクセスが可能となり、オンラインでのやり取りがよりシームレスで効率的になる。
3. **透明性と安全性**：オープンソースライセンスを採用し、透明性と安全性を確保する。誤用や違法な追跡を防ぐための対策が講じられ、データが安全に取り扱われる。
4. **使いやすさ**：ユーザーフレンドリーなインターフェースを提供し、個人が簡単にデジタル ID を管理し、サービスにアクセスできる。市民であれば誰もが電子署名を無料で使うことができる。
5. **スムーズな移行**：市民は、各国のスキームを使ってウォレットに情報を登録することができ、デジタル ID 管理へのスムーズな移行が保証される。

（政府）
1. **デジタルサービスへのアクセス向上**：ウォレットは本人確認のプロセスを合理化し、市民がオンラインで政府サービスにアクセスしやすくし、利用率を高めることができる。
2. **詐欺防止の強化**：安全で検証可能な ID 手段を提供することにより、政府サービスに関する ID 窃盗や関連詐欺を減らすことができる。
3. **セキュリティの向上**：市民データの全体的なセキュリティが強化され、侵害リスクが軽減される。

（デジタルサービスの提供事業者）
1. **セキュリティとプライバシーの向上**：ウォレットは、従来の認証方法の責任に関連するリスクを軽減することができる。
2. **認証コストの削減**：ウォレットは、本人確認プロセスを簡素化し自動化することで、本人確認プロセスに関連するコストを削減することができる。
3. **競合する大手プラットフォームへの依存回避**：サービス提供事業者は、取得したユーザー・データの利用が不透明な ID サービスへの依存度を下げなければならなくなる。

12：EUDIW の対象ユーザーは加盟国の国内法で定められることになる。なお、欧州デジタル ID 枠組み規則では、加盟国に対し EUDIW を提供する義務を課しているが、一方で、これを保有し使用することを義務付けるものではない。

13：個人データ処理は、一般データ保護規則（GDPR）に完全に準拠して実施されることが求められた。

（社会）
1. **オンライン取引の増加**：認証がより簡単で安全なため、人々はオンライン取引をより行う傾向が強まる可能性がある。
2. **新たなビジネスチャンス**：アイデンティティ・ウォレットの採用はイノベーションを促進し、新しいサービスや製品に繋がる可能性がある。
3. **リソースの再配分**：これまで手作業の検証プロセスに費やしていたリソースを、より生産性の高い用途に振り向けることができる。
4. **経済成長**：オンライン取引の導入拡大、新たなビジネスチャンス、資源配分の改善は、全体として経済の安定と成長に貢献する。

2.3「EUデジタルIDツールボックス」の開発について

多くの加盟国は、属性およびクレデンシャル（認証情報）の統合のために、デジタルウォレットや国家間のトラストフレームワークを含む国家デジタル ID システムを展開または開発している。しかしながら、各国が独自に異なるソリューションを開発することは、規格の相違による分断や障壁を生み、欧州単一市場の恩恵を奪うことになるとして、新たな規則では加盟国に対し、お互いのソリューションを認め合うだけでなく、共通の技術標準に基づいて構築されたスキームの下でデジタルウォレットを発行するよう求めている。そのため、欧州委員会では、本規則を提案するのに合わせ、ウォレットの技術仕様等を定義する「EU デジタル ID ツールボックス」の開発を並行して進めるよう各加盟国に対する勧告を付していた[14]。

EU デジタル ID ツールボックスは、技術アーキテクチャおよび参照フレームワーク、一連の共通の規格および技術仕様、ガイドラインとベストプラクティスからなるもので、加盟国の専門家が、関係官民団体と緊密に連携して開発にあたっている。また、EUDIW を活用する多数の大規模なパイロットテストにおいて、プロトタイプを設計するための基盤として活用することで、改善され精緻化されていくこととなる。

EUDIW の技術アーキテクチャおよび参照フレームワークとしては、Architecture and Reference Framework（以下 EUDIW ARF）の 1.4 版が、欧州デジタル ID 枠組み規則の法文に基づいた最新版（本稿執筆時）として、2024 年 5 月 20 日に公開された[15]。EUDIW ARF1.4 版は説明的な主文書のほか、6 つの付属文書から構成され、付属文書のうち、「付属文書 2：ハイレベル要件」[16] と「付属文書 3：認証ルールブック」[17] の 2 文書については特に技術仕様と規格の参考になるものとされている。

なお、この文書の位置づけは、eIDAS 専門家グループの進行中の作業の現状を示すものであり、その内容等に関して必ずしも正式に合意しているものではないこと、開発作業等を通じ時間の経過とともに補完され、更新されることには留意を要する。以下では、この EUDIW ARF1.4 版の内容をもとに EUDIW の仕様概要について読み解くことにする。

14：Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework (Official Journal of the European Union, L 210, 14.6.2021, p. 51).

15：EUDIW ARF の目的は、eIDAS 規則を実施するために欧州委員会が策定する技術仕様、基準、手順であって、特に新たに改訂された以下のトピックに関連するものを定義することであるとしている。
EUDIW コア機能（第 5a 条）、EUDIW の依拠当事者（第 5b 条）、QEAA の要件（第 45d 条）、真正な情報源に対する属性の検証（第 45e 条）、公的機関（PSB）が発行する／公的機関のために発行される EAA に関する要件（第 45f 条）、国境を越えた ID 照合（第 11a 条）、EUDIW の認証（第 5c 条）、認証 EUDIW リストの公表（第 5d 条）、EUDIW のセキュリティ違反（第 5e 条）、PSB が発行する／ PSB に代わって発行される EAA の要件 - 通知（第 45f 条）

16：EUDIW エコシステムのエンティティに対する要求事項を規定する文章。

17：PID（個人識別データ）、m DL（モバイル運転免許証）の認証に関する具体的な要件を記載している規則集。

3．EUDIW ARF1.4版のポイント

3.1 ユースケース

EUDIW ARF1.4 版では、EUDIW の優先度の高いユースケースの青写真を示すことによって、潜在的な強化領域を浮き彫りにしつつ、サービス設計を助け、ユーザー体験とサービス効率を向上させるツールとして活用してもらうことを狙っている。そのため、ユースケースを知ることで、EUDIW が備えるべき機能や実際の活用イメージを想定することが可能となる。

（事例①）オンラインサービスにアクセスするための本人確認と認証

EUDIW は主に、公共および民間の様々なオンラインサービスにおいて、依拠当事者（Relying Party）がサービスを提供する利用者の身元を確実に確認できるよう、高い保証レベル（Levels of Assurance）での安全なユーザー識別と認証を容易にするよう設計されている。複数の本人確認方法を使用でき、ユーザーは、オンラインで個人識別データ（PID）を共有する際に懸念しうるプライバシーとセキュリティに特に留意している。このシナリオは、有効なウォレットインスタンスの取得から、オンラインサービスのための識別と認証のプロセスまでが含まれるなど、ユーザーの視点から EUDIW のライフサイクル全体をカバーしている。

（事例②）適格な電子署名

EUDIW では、ユーザーが適格な電子署名または印鑑を作成できなければならない。この目標は、ローカル QSCD、または QTSP によって管理されるリモート QSCD の一部として、EUDIW の認証と署名 / 印鑑機能を使用することで実現できる。

（事例③）携帯運転免許証

運転免許証は、EUDIW にとって重要なユースケースである。ユーザーはモバイル運転免許証（mDL）を取得、保存、表示しておき、必要の都度、例えば交通警察等に提示することができる。なお、EUDIW を使って mDL 属性の交換と開示を行うには、近接技術（例えば、NFC、Bluetooth）が用いられるが、人間またはその支配下にあるデバイス等に mDL 属性を提示する監視フローのシナリオと、無人の機械に対し mDL 属性を提示する非監視フローのシナリオが想定される。

（事例④）仮名（ペンネーム）によるアクセス

基本的な仮名のユースケースは、実名の提示を受けなくても、サービス提供者があらかじめ把握しているユーザーや、以前にやり取りしたことのあるユーザーであること等を認識できるようにするためのものである。ただし、この仮名は、必ずしもすべてのユースケースに適合するように設計されているわけではない。

（事例⑤）e ヘルス

健康関連データへ簡単にアクセスできることは、国内外の両方において極めて重要である。患者サマリー、e 処方箋などへのアクセスを可能にすることも推奨されている。

（事例⑥）学歴・専門資格の証明

EUDIW は、学歴や専門資格等の教育関係の属性電子証明書（教育デジタル・クレデンシャル）のリポジトリであり、関連するサービス提供者との間でそれらを交換するための手段となりうる。例えば、デジタル卒業証明書は、検証可能な信頼できる利用可能なフォーマットで、他の教育機関や訓練機関または将来の雇用主等に対し、国境を越えて提示される可能性がある。

（事例⑦）デジタル金融

EUDIW は、デジタルファイナンスや決済等の金融サービスにおける厳格な顧客認証要件へ準拠する強力なユーザー認証機能を提供することができる。

（事例⑧）デジタル・トラベル・クレデンシャル

ICAO（国際民間航空機関）が、パスポート情報をスマートフォンなどのデジタルデバイスに保持するために DTC（Digital Travel Credential）の規格化を進めているが、EUDIW に対しても DTC プロバイダーが対応するフォーマットで DTC を発行することができる。

3.2 設計原則

EUDIW の設計においては、４つの設計原則（ユーザー中心主義、プライバシー、セキュリティ、国境を越えた相互運用性を重視した要件への準拠が保証される。）が掲げられている。

ユーザー中心主義：EUDIW は、ユーザー中心主義を設計の基本方針としている。これは、ユーザーのニーズと経験をすべての設計決定に優先することを意味しており、ウォレットは直感的で使い易く、既存のユースケースにシームレスに統合されるべきとしている。ユーザーは、どのデータが誰と共有されているかについての透明性のある情報とともに、自分のデータとプライバシーを明確にコントロールできる。また、ウォレットは様々な技術的背景や能力を持つユーザーにも対応できるよう、アクセシブルになっている。

相互運用性：EUDIW は、EU 域内の国境を越えてシームレスに機能することを保証している。相互運用性は、標準化されたプロトコルを通じた安全なデータ交換を促進し、信頼できるエンティティがクレデンシャルを簡単に検証できるようにするため、ユーザーは自由に移動しながら、電子政府プラットフォームからプライベートなオンライン交流に至るまで、様々なサービスにウォレットを利用することができる。

デザインによるプライバシー：EUDIW アーキテクチャは、デザインによるプライバシーの原則を体現している。必要なものだけが収集されることを保証（データ最小化の原則）し、どのデータが誰と共有されるかをきめ細かくコントロールできる権限をユーザーに与え、データがどのように使用され、保護されるかがわかるようにシステムに組み込まれている（透明性の確保）。

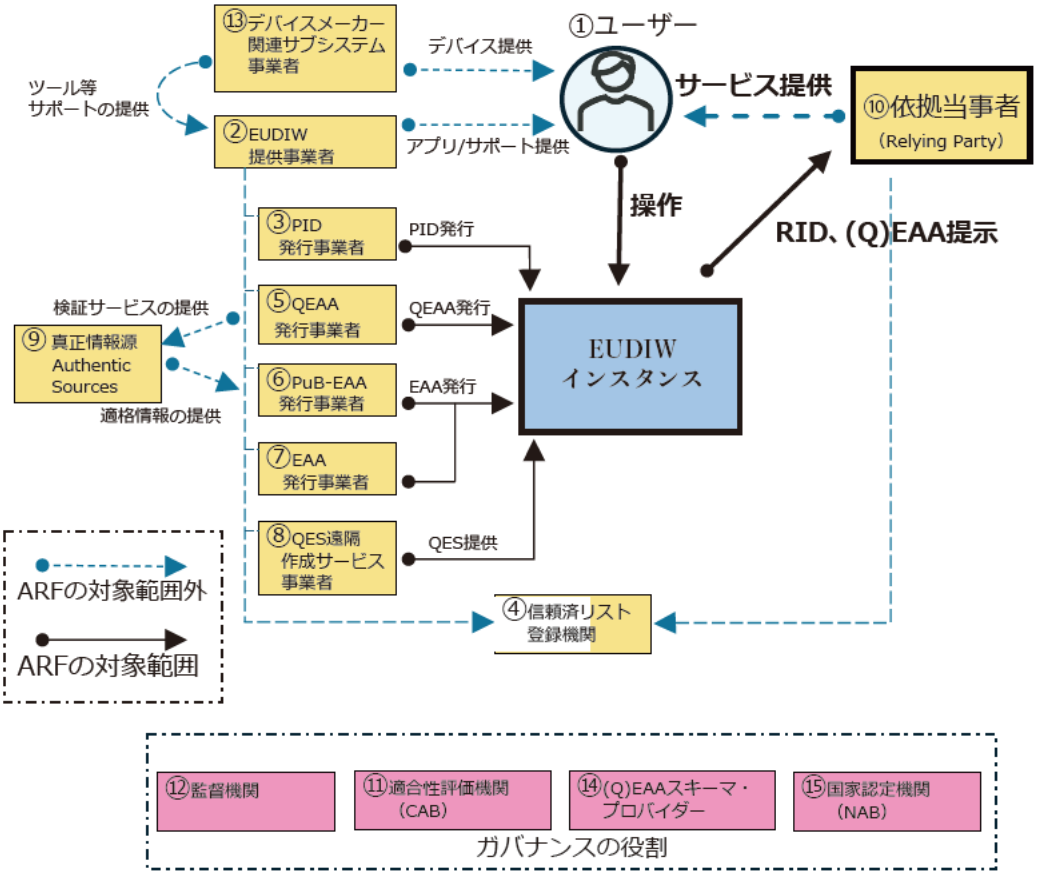
デザインによるセキュリティ：セキュリティへの配慮がウォレットの設計そのものに織り込まれている。設計プロセスを通して、潜在的な脆弱性への対応が行われているほか、セキュア・コーディングが義務付けられ、アーキテクチャ自体が機密データとアクセス制御を区分することで攻撃面を最小化している。

3.3 EUDIWのエコシステム

EUDIW ARF では、欧州デジタル ID 枠組み規則で想定されている EUDIW のエコシステムについて説明している。基本的な流れとしては、まず、ユーザーはデバイスメーカーやソフトウェア開発業者から EUDIW を入手し、その EUDIW のアプリ等を操作することで、個人識別データ（PID）や Attestation と呼ばれる用途に応じた様々な属性を認証できる電子形式の認証書（電子属性証明）をそれぞれの事業者から EUDIW に対して発行してもらっておく。そして、サービスを提供する依拠当事者（Relying Party）に対

して、EUDIW の中の必要な PID や電子属性証明のみを選択的に提示することで、必要なサービスを受けることになる。なお、こうしたエコシステムに存在するエンティティは、信頼済リスト登録機関に登録されていることが求められる。EUDIW のエコシステムにおける様々なエンティティとその役割の概要は図表 2 のとおりである。

図表2　EUDIWの役割の概要



出所）　筆者作成

① EUDIW のユーザー

EUDIW のユーザーは、EUDIW インスタンス[18] を使用して、PID や様々な電子属性証明を受信、保存、提示する。ユーザーはまた、EUDIW インスタンスにより適格電子署名 / 印鑑（QES）を作成し、ウォレット間のやり取りで利用することもできる。

② EUDIW 提供事業者（EUDI Wallet Provider）

EUDIW 提供事業者とは、EUDIW をエンドユーザーに提供する組織。その EUDIW ソリューションのインスタンスを通じてトラストサービス等を提供することで、利用者はその EUDIW 内の PID と電子属性証明、およびその他の個人情報の使用を完全に制御できるようになる（技術的には、関連する暗号秘密鍵等に対する制御権をユーザーが保有）。また、EUDIW 提供事業者は EUDIW が要件に準拠していることを保証する責任を持っている。

18：あらかじめ定義されたコンピュータプログラムやデータ構造などを、メインメモリ上に展開して処理・実行できる状態にしたもの。この文脈では「アプリ」が比較的近い意味。

③ PID 発行事業者（Person Identity Data Providers）

PID（個人識別データ）発行事業者は、以下の責任を負う信頼できるエンティティである。

・高い保証レベルの要求事項に従って EUDIW ユーザーのアイデンティティを確認する。
・EUDIW に統一された共通フォーマットで PID を発行する。
・依拠当事者（Relying Party）が PID の有効性を検証するための情報を提供する。

なお、PID 発行事業者は、例えば、公的身分証明書、電子身分証明書等を発行する組織や EUDIW 発行事業者と同じこともありうる。

④信頼済リスト登録機関（Trusted Lists Registrar）

信頼済リスト登録機関は、信頼済リストの維持、管理、公開に責任を持つ。EUDIW エコシステム内では、様々なエンティティに信頼済リストが存在する。信頼済リストには、主に関連するエンティティのトラストアンカー（ルート証明書）が含まれ、エンティティが作成した署名等の検証に用いられる。

⑤ QEAA 発行事業者（Qualified Electronic Attestation of Attributes Providers）

QEAA（適格電子属性証明）は、QTSP（Qualified Trust Service Providers：適格トラストサービス提供事業者）によって提供される。QEAA 発行事業者は、QEAA を要求・提供するために、EUDIW との相互認証インターフェースのほか、属性を検証するための真正情報源（Authentic Sources）とのインターフェースを保持する。なお、QEAA 発行事業者は、QEAA の有効性を照会するために必要な情報を提供するが、証明書の使用に関する情報は受け取らない。

⑥ PuB-EAA 発行事業者（Public Body Authentic Source Electronic Attestation of Attributes Providers）

PuB-EAA（公的電子属性証明）は、真正情報源に責任を負う公的機関等によって発行される電子属性証明である。 PuB-EAA の発行と運用に関する要件は、法的レベルで QEAA として認識できるようにするためのものである。

⑦（非認証）EAA 発行事業者（Non-Qualified EAA Providers）

EAA（非認証電子属性証明）は、どのような TSP（トラストサービスプロバイダー）からも提供される可能性がある。EAA は eIDAS 規則 のもとで監督されるが、EAA の提供、使用、承認に関する規則は、主に eIDAS 以外の他の法的または契約的枠組みによって規定されていることがほとんどであると考えられる（学歴証明書やデジタル決済など）。EAA を使用するためには、TSP はユーザーに対し、EAA を要求し取得する方法を提供しなければならず、必然的に EUDIW インターフェース仕様に準拠する必要がある。また、用途によっては、EAA 発行事業者は、EAA の有効性を照会するために必要な情報を提供することもできるが、ユーザー側の証明書の使用に関する情報は受け取らない仕組みとなっている。

⑧ QES 遠隔作成サービス事業者（Qualified Electronic Signatures Remote Creation Service Providers）

EUDIW を使用することで、ユーザーはあらゆるデータに対し無料で QES（適格電子署名）を作成することができる。これは、署名目的で EUDIW の普及が促されることに繋がる。

EUDIW を利用した電子署名の方法としては、「適格署名 / 印鑑作成デバイス」（QSCD: qualified signature/seal creation device）として認証されている EUDIW 自体で作成する方法のほか、QTSP（適格トラストサービス事業者）によって管理されるリモート QSCD 等の一部として、EUDIW に実装されている「セキュア認証と電子署名 / 印鑑の呼び出し機能」を用いる方法がある。図表 2 は、QES 遠隔作成サービス事業者がリモート QSCD になっている例である。

適格電子署名 / 印鑑の機能には共通のインターフェース／プロトコルが採用され、技術的相互運用性が確保されているため、リモート署名サービスを提供する QTSP の統一欧州市場が形成される。

⑨真正情報源（Authentic Sources）

真正情報源とは、法律で規定されている公的または私的なリポジトリないしシステムのことである。例えば、住所、年齢、性別、市民的地位、家族構成、国籍、教育・訓練の資格タイトルおよびライセンス、専門資格タイトルおよびライセンス、公的許可およびライセンス、財務および企業データ、などの情報源である。真正情報源は、QEAA プロバイダーに対し、上記属性の真正性を確認するためのインターフェースを、指定仲介機関を通じて提供することが求められるが、eIDAS 規則の要件を満たせば、自ら PuB-EEA を発行することもできる。

⑩依拠当事者（Relying Parties）

依拠当事者は、電子身分証明書またはトラストサービスに依拠することでユーザーを確認し、ユーザーに対して何らかのサービスを提供する自然人または法人である。 EUDIW の文脈では、依拠当事者は、ウォレット所有者であるユーザーの承認を条件として、適用される法律および規則の範囲内で、PID、QEAA、Pub-EAA、および EAA に含まれる必要な属性を要求する。EUDIW を活用したサービスの提供は、法的要件、契約上の合意、または依拠当事者自身の判断に基づくが、予め加盟国に対し設立場所とその利用意図を通知しておく必要がある。また、依拠当事者は相互認証で電子属性証明書等を要求するために EUDIW とのインターフェースを維持する必要がある。

⑪適合性評価機関（CAB：Conformity Assessment Bodies）

適合性評価機関（CAB）は、加盟国によって指定された国家認定機関によって認定された公的または民間の機関であり、EUDIW を発行する前、またはトラストサービスプロバイダーに認定ステータスを提供する前に必要な評価を実施する責任を負っている。例えば、EUDIW は CAB によって認証される必要があるほか、QTSP は CAB によって定期的に監査されることになっている。

⑫監督機関（Supervisory Bodies）

監督機関はウォレット提供事業者およびその他の関連団体の適切な機能を審査し、適切に機能していることを確認するために重要である。監督機関は加盟国に設置され、任命される。

⑬デバイスメーカーおよび関連サブシステム事業者

デバイスメーカーや関連サブシステム事業者などの商業主体は、EUDIW を安全かつ円滑に動作させるのに必要な、ハードウェア、オペレーティングシステム、セキュアな暗号機器、ライブラリ、アプリストア等のコンポーネントを提供する重要な役割を果たしている。

⑭（Q）EAA スキーマ・プロバイダー（Qualified and Non-Qualified Electronic Attestation of Attributes Schema Providers）

（Q）EAA の構造とセマンティクスを記述するスキーマと語彙を公開する主体が（Q）EAA スキーマ・プロバイダーである。これにより、依拠当事者など他のエンティティが（Q）EAA を検出して検証できるようになる。欧州委員会は、この目的のために最低限の技術仕様、標準、および手順を定めているが、セクター固有組織によるものも含む共通のスキーマは、（Q）EAA を広く普及させるために不可欠である。

⑮国家認定機関（NAB：National Accreditation Bodies）

国家認定機関は、加盟国由来の権限で認定を実行する加盟国の機関である。国家認定機関は、要件を規定する規範文書（法律、仕様、保護プロファイルなど）に照らして、製品 / サービス / プロセスを認証する責任を負う独立した監督下の専門認証機関として、適合性評価機関（CAB）を認定するとともに、これらを監視する。

EUDIW から依拠当事者に提示される情報には PID（個人識別情報）のほか、３つの電子属性証明書（Attestations）があるが、それらは以下のとおり区分され、法的に定義されている。

（EUDIWから提示されるAttestation等の種類）

―個人識別データ― PID（Person Identification Data）	欧州連合法または国内法に従って発行され、自然人もしくは法人、あるいは別の自然人もしくは法人を代表する自然人の身元を確認することができる一連のデータ。
―公的電子属性証明書― PuB-EAA（Electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source）	真正な情報源に責任を負う公的機関、または加盟国によって指定された代理の公的機関が発行する電子的な属性証明（Attestation）。
―適格電子属性証明― QEAA（Qualified Electronic Attestation of Attributes）	適格なトラストサービスプロバイダーによって発行され、規定される要件を満たす電子的な属性証明（Attestation）。
―非認定電子属性証明書― Non-Qualified EAA	QEAA でも PuB-EAA でもない EAA。

これらの認証の種類の違いは、純粋に法的なものであり、例えば、「卒業証明」は、適格なトラストサービスプロバイダー（QTSP）により発行されるか、非認定のトラストサービスプロバイダーにより発行されるかによって、QEAA となる場合もあれば、非認定 EAA となる場合もある。

3.4 EUDIWで扱うPID（個人識別データ）の概要

EUDIW ARF 文書では、PID、仮名、mDL、卒業証明書、電子処方箋などの各 attestation タイプについて、その証明の属性スキーマ、データ形式、証明メカニズム[19]、および認証と承認の信頼メカニズムを規定する認証ルールブックを定義することが要求されている。特に、組織間および / または国境を越えて使用されることを意図した認証ルールブックは、可能な限りすべての利害関係者が代表される組織によって定義されることになっており、これによって、同じタイプの認証（例えば、卒業証書）に対して複数の認証ルールブックが定義されることがなくなるとしている。

既に、PID ルールブック[20]、mDL ルールブック等に関するものは定義されているが、このルールブックによると、EUDIW で管理され依拠当事者へ提示できる個人識別データは次のとおりである。

19：属性スキーマは、認証された属性の構造、論理構成、タイプ、名前空間、および認証、発行者、検証メカニズム、基礎となる身元保証、プロパティが関連するトラストフレームワーク、正当なユーザーによる所有の証明などの追加情報である。データ形式は、文字セット、エンコード、シリアル化など、証明書のデータの形式を指す。証明メカニズムは、選択的開示も含め、完全性と真正性の証明に使用される方法を意味する。

20：ANNEX 3.1 - PID Rulebook https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/annexes/annex-3/annex-3.01-pid-rulebook.md

図表3　PIDの概要

Attribute identifier（属性識別子）	定義	
family_name（姓名）	現在の姓または名	必須
given_name（名前）	ミドルネームを含む現在のファーストネーム	必須
birth_date（生年月日）	生まれた日、月、年	必須
age_over_18（18歳以上）	現在成人（true）か未成年（false）	必須
age_over_NN（年齢）	NN 歳以上か?	任意
age_in_years（年齢）	現在の年齢	任意
age_birth_year（年齢_誕生年）	生まれた年	任意
family_name_birth（姓名_出生）	出生時の姓または名	任意
given_name_birth（出生）	出生時の姓名（ミドルネームを含む）	任意
birth_place（出生地）	生まれた国、州、都市	任意
birth_country（出生国）	生まれた国。ISO 3166-1 alpha-2国コード	任意
birth_state（出生地）	生まれた州、県、地区、または地域	任意
birth_city（出生地）	生まれた市町村	任意
resident_address（居住者住所）	現在居住している、または連絡が取れる場所の完全な住所（通り名、家屋番号、市町村など）	任意
resident_country（居住国）	現在居住している国。ISO 3166-1 alpha-2国コード	任意
resident_state（居住州）	現在居住している州、県、地区、または地域	任意
resident_city（居住都市）	現在居住している市町村	任意
resident_postal_code（居住者郵便番号）	現在居住している場所の郵便番号	任意
resident_street（居住ストリート）	現在居住している通りの名前	任意
resident_house_number（住居番号）	現在居住している家の番号	任意
Gender（性別）	性別。ISO/IEC 5218の定義値	任意
Nationality（国籍）	国籍、ISO 3166-1 alpha-2国コード	任意
issuance_date（発行日）	PIDが発行された日付	必須
expiry_date（有効期限）	PIDの有効期限が切れる日付	必須
issuing_authority（発行機関）	このPIDインスタンスを発行した行政当局の名前等	必須
document_number（ドキュメント番号）	PIDプロバイダーによって割り当てられたPIDの番号	任意
administrative_number（管理番号）	監査管理などの目的でPIDプロバイダーが割り当てる番号	任意
issuing_country（発行国）	PIDプロバイダーの国または地域。ISO 3166-1 alpha-2国コード	必須
issuing_jurisdiction（発行管轄）	PIDを発行した法域の国細分コード。ISO 3166-2:2020の第8節で定義	任意

出所）　筆者作成

これを見ると、生年月日に関連するものだけでも、以下の属性が定義されている。

必須	birth_date（生年月日） age_over_18（18 歳以上か?）
任意	age_birth_year（誕生年） age_in_years（年齢） age_over_NN（NN 歳以上か?）

生年月日について 1 つの属性だけでなく粒度の異なる複数の属性を持つことで、ニーズに応じてリクエストやレスポンスで使い分けることができ、PID プロバイダーと依拠当事者は保有データを必要最小限に抑えることができるとしている。例えば、いくつかのユースケースにおいて、依拠当事者は PID ユーザーが未成年者でないことを証明するだけでよく、その場合、age_over_18 を要求すれば十分である。PID ユーザーの年齢や誕生年など、より具体的な情報を公開することは、ユーザーのプライバシーを不必要に侵害することになる。

本文書では age_over_18 を必須属性とし、その他の age_over_NN 属性（NN は年齢）を任意属性としているが、PID プロバイダーは複数の age_over_NN 属性を自由に追加することができる。

このほか、出生地関連属性としても、「国、州、都市」、「ISO 3166-1 alpha-2 国コード」、「州、県、地区、または地域」、「市町村」と異なる粒度のものが存在するほか、アドレス（住所）関連属性についても完全な住所を含む 7 種類の属性が定義されるなど、複数の属性を持つようになっている。

なお、PID は相互運用性を高める観点から標準フォーマットが決められており、ISO/IEC 18013-5:2021[ISO18013-5] で規定されている形式と、[SD-JWT VC] で規定されている形式の両方で発行されなければならないと規定されている。前者の場合、属性は CBOR でエンコードされなければならないほか、後者の場合、属性は JSON でエンコードする必要がある。

4．おわりに

わが国のマイナンバーカードは、対面で公的な身分証明書として使う以外に、IC チップ部分に保存された電子証明書を用いて、オンラインでの本人認証にも使うことが可能である。マイナンバーカードでの健康保険証利用も始まり 2024 年 12 月から一体化が決まっている。自動車運転免許証についても、2022 年 4 月に公布された改正道路交通法でマイナンバーカードに免許関連の情報を電磁的に記録する規定が整備され、2024 年中にはマイナンバーカードの運転免許証としての利用がスタートするといわれている。

一方、マイナンバーのスマートフォン対応については、Android スマホでは 2023 年 5 月から、マイナンバーカードの「電子証明書」の機能を内蔵する「スマホ用電子証明書搭載サービス」が開始されている。さらに、「マイナンバーカードのすべての機能をスマートフォンに搭載できるようにする」マイナンバー法の改正案が 2024 年 5 月 29 日、国会で成立した。一部の認証サービス提供企業では、「スマホ用電子証明書搭載サービス」を自社サービスとして既に提供し始めている。iPhone では対応が遅れていたが、これにより「スマホ用電子証明書搭載サービス」のみならずマイナンバーカードの「券面記載事項」（氏名、生年月日、住所、性別、マイナンバー、顔写真等）の搭載も可能となり、来年春には iPhone の Apple ウォレットにマイナンバーカードを追加することでアップル社と合意している。機能的には、本人が所有する国家資

格証明書などもスマホ画面上で提示できるようになるとの見方もある。

これらの動きを見ると、結果的に、わが国でも EUDIW と同様の取組みが行われているようにも見えるが、マイナンバーカードの機能拡張の文脈で検討されているものであり、必ずしもデジタル ID ウォレットのあるべき姿をデザインして導かれた姿ではない。そのため、

- 十分考えられたエコシステムが存在しない中で官民、特に民間での活用に制限がある、
- 技術仕様や共通ルールの透明性が不十分であり、相互運用性に懸念がある（欧州のような国境を跨る運用も想定されていない）、
- 現在搭載されている電子証明書は「署名用電子証明書」と「利用者照明用電子証明書」の 2 種類のみであり、プライバシーに配慮して制御可能な細かい属性認証（例えば「18 歳以上」等）への対応の検討が遅れている、

といった課題がある。

こうした課題を含めマイナンバーカードの抱える問題に対しては、これまでのマイナンバーカードにはグランドデザイン（全体設計）が欠如していたことが問題であったと指摘する専門家[21]も散見される。これに対しては、先行して進んでいる EUDIW の取組みをもとに、日本版デジタル ID ウォレットのグランドデザインを検討することが解決に繋がる可能性があると思われる[22]。そして、マイナンバーカードがデジタル ID ウォレットとして進化を遂げ、官民で使えるオンラインサービスが拡充されるなど高い利便性が伴ってくれば、わが国特有のマイナンバーに対する誤解や不信も薄まるのではないだろうか。

なお、EUDIW ARF では、EUDIW エコシステムのコアとなるコンポーネントを概説した「リファレンス・アーキテクチャ」や、それらのコンポーネント間で安全なやり取りを可能とするために、当事者間でどのような信頼関係が確立されるかを記述した「トラストモデル」についても、多くのページが割かれているが、大部である他かなり技術的な内容になるため本稿では割愛した。これについては、機会があれば改めて解説したい。

21：一般社団法人 情報システム学会 マイナンバー制度研究会が公表した「「マイナンバー制度の問題点と解決策」に関する提言の補足」（2024/7/3）の付属文書「やさしい解説：マイナンバー制度のあるべき姿とは」でも、「問題の根本は、目的に到達するためのグランドデザインすなわち全体像を描いた制度設計がないまま、マイナンバーカードの普及に力点を置いてデジタル化を推進してきた点にあります。政府はマイナンバーカードを「デジタル社会のパスポート」と呼んで、次から次へと機能を追加しています。一方、デジタル先進国で日本のような多機能 IC カードを発行している国は見当たりません。むしろ IC カードを使わないでデジタル化を推進し成果を上げた国の方が多いくらいです。」としている。

また、国際政治学者の舛添要一氏も、「マイナンバーカードですべての用事が済むようにするためには、カードを構想する段階から、グランドデザインが必要である。例えば、納税データとの連結などがそうである。しかし、このようなデザイン設計を最も苦手とするのが役人である。官庁の縦割り、縄張り根性も邪魔になる。最初から民間の優秀な専門家に任せていれば、こうはならなかったであろう。」と主張している。

22：デジタル庁が公表した「次期個人番号カードタスクフォース最終とりまとめ」（2024/3/18）によると、2026 年を視野に導入の検討が進められている次期マイナンバーカードでは、諸外国 eID カードの事例を参考に一部の機能を見直そうとしていることが読み取れるが、エコシステムを含むグランドデザインの検討に関する記述はみられない。

参考文献

European Commission（2021), COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS 2030 Digital Compass: the European way for the Digital Decade COM/2021/118 final, 2021/3/9, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

――――――――― (2021), Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework, Official Journal of the European Union, L 210, 2021/6/14, p. 51

――――――――― (2023), The European Digital Identity Wallet Architecture and Reference Framework v1.0, 2023/2/10, https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

――――――――― (2024), European Digital Identity Wallet Architecture and Reference Framework v1.4.0, 2024/5/23, https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/#314-qualified-and-non-qualified-electronic-attestation-of-attributes-schema-providers

――――――――― (2024), European Digital Identity Wallet Architecture and Reference Framework v1.4.0 ANNEX 3.1 - PID Rulebook, 2024/5/23, https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/annexes/annex-3/annex-3.01-pid-rulebook.md

European Parliament, Council of European Union (2022), Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, Official Journal of the European Union, L323, 2022/12/19, p. 4

――――――――――――――――――――――――――― ,European Commission (2023), European Declaration on Digital Rights and Principles for the Digital Decade, Official Journal of the European Union, C23, 2023/1/23, p. 1

――――――――――――――――――――――――――― (2024), Document 32024R1183, Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, 2024/4/11, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1183

一般社団法人情報システム学会マイナンバー制度研究会（2024）「『マイナンバー制度の問題点と解決策』に関する提言の補足―やさしい解説：マイナンバー制度のあるべき姿とは」、2024 年 7 月 3 日、https://www.issj.net/teigen/2024_myno_kaisetu.pdf, p. 1

デジタル庁（2024）「次期個人番号カードタスクフォース最終とりまとめ」、2024 年 3 月 18 日、https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/58b82d5b-338d-4f5b-be7e-7b771135e2c3/0d7a6b39/20240318_meeting_mynumber-card-renewal_outline_06.pdf

舛添要一（2023）「混迷するマイナカード、『グランドデザイン』描けない役人に最大の責任がある」Shirabee ニュース、2023 年 6 月 18 日、https://sirabee.com/2023/06/18/20163098937/#