政府が発行するデジタル資格証明とプライバシーを取り巻く環境

Heather Flanagan
2023年8月24日

Heather Flanagan（編集）：“Government-Issued Digital Credentials and the Privacy Landscape, v1.1.”）、OpenID Foundation、2023年8月24日。 https://openid.net/Government-issued-Digital-Credentials-and-the-Privacy-Landscape-Final-v1.1.[1]

日付	改訂
2023年8月24日	v1.1の発行
2023年5月4日	最終v 1.0の発行
2023年4月5日	パブリックコメント（草案）の発行
2023年3月14日	プライベートコメント（草案）の発行

[1] 訳注：2026年05月01日時点はリンク切れ

目次

協力：

複数の非営利組織の協力により、本書の取りまとめが可能になった。この場を借りて、深く感謝申し上げる。

加えて本書は、執筆に際して時間を割き知見を共有してくださった複数の方々のご支援なくして完成し得なかった。ここに記して謝意を表する。（敬称略）

- Dr Joseph Atick, ID4Africa
- Daniel Bachenheimer, Accenture
- Vittorio Bertocci, Okta, Inc.
- Debora Comparin, Thales DIS
- Jamie Danker, Venable LLP
- Bill Nelson, Identity Fusion, Inc.
- Gail Hodges, Executive Director, OpenID Foundation
- Mike Kiser, SailPoint Technologies
- Stephanie de Labriolle, Executive Director, Secure Identity Alliance (SIA)
- Giuseppe De Marco, Dipartimento per la trasformazione digitale
- Drummond Reed, Director, Trust Services, Gen Digital
- Rachelle Sellung, Fraunhofer Institute
- Kristel Teyras, Thales DIS
- John Wunderlich, Chair, Kantara Privacy Enhancing Mobile Credential Work Group
- Kristina Yasuda, Microsoft

1 本書について

1.1 対象範囲

本ホワイトペーパーは、政府が発行するデジタル資格情報を取り巻くプライバシー上の論点に焦点を当てる。特に、政府当局が発行し、住民や企業を対象とした効率的で、プライバシー保護に配慮したサービスの実現に役立つ技術となることを目的としたデジタル資格情報に着目する。同様に、法令や規制で個人のプライバシーに対する期待がどう定義され、技術に求められる要件の一部をどのように定められているかを考察している。本書の対象範囲は世界全体であるが、より厳格なプライバシー法を制定し、住民の間でもプライバシーに関する期待が満たされるべきだという意識が高い傾向にある自由民主主義国家の政府が発行するデジタル資格情報に特に重点を置いている。一方で本書は、民間で発行された資格情報、政府発行の資格情報を持たないユーザーにサービスを提供する際に政府が行う必要があること、プライバシーをさほど重視していない中央集権政府のニーズなどについては本書で扱っていない。

1.2 エグゼクティブサマリ

世界各国の政府は今、「デジタルアイデンティティ」という言葉を受け入れつつある。膨大な個人データ（実名や生年月日、国籍（市民権）など）の権威的源泉である政府は、デジタル資格情報を市民や居住者に発行し、かつ企業と政府機関にその資格情報を適切に利用させるための基本原則を定めて、オンラインサービスと対面でのサービスに対する信頼を向上させる立場にある。

政府が発行する資格情報のデジタルアイデンティティを取り巻く環境では、技術面と社会面の両方における信頼が、複数の側面で関わっている。政府は、単独ではプライバシー保護に配慮された、強固なデジタルエコシステムを構築することはできない。政府は、プライバシー上の懸念と技術的可能性に精通した技術者や市民社会と協働しなければならない。さらに当然のこととして、デジタル化が進む世界がプライバシーに及ぼす影響について市民や居住者と協働し、彼らのニーズと期待に確実に応えなければならない。

本書では、政府発行のデジタル資格情報がどこで、どのように利用されているか、それを支えているのはどのような標準や規則か、そしてより安全で効率的な世界を実現するという約束を果たすためにまだ取り組む必要があるのはどこかの例を紹介する。これは政府の政策立案者や市民社会のメンバー、技術者に向けた文書であり、各グループは外部で起きていることの理解を深めることができる。

いくつかの提言を示す。まず、政府発行のデジタル資格情報の発行、保管、検証、利用に関わるシステムのセキュリティおよびプライバシー態勢の改善を推奨する。NISTサイバーセキュリティフレームワークやEUサイバーレジリエンス法案など、政府や各種サービスがデータ管理の基本をより適切に行うための指針となる資料はいくつかあ

る。とはいえ、基本事項を管理するだけでは「必要ではあるが十分ではない」にとどまる。監視をめぐり今も続く懸念や、多様性・公平性・包摂性の課題、適法性のグレーゾーン、そして政権交代の中でも法的保護を持続させられるかといった点についても、認識しておく必要がある。

新たな技術の登場は新たな懸念を招くが、これはデジタルアイデンティティの資格情報にも当てはまる。デジタル資格情報への依存の強まることで、デジタルでの新たな攻撃ベクトルが生み出された。ディープフェイクも、資格情報の遠隔利用を検証する能力を脅かす新たな脅威に加わった。これらはセキュリティ戦争に参入した要素の一例である。

いかなる場合においても、政府と技術者、市民社会のメンバーは、このエコシステムに参加する個人が何を合理的に期待しているか、その実態を常に念頭に置いておかなければならない。個人に選択肢を提供しなければならないが、その選択肢は明確で実際的、かつわかりやすいものであり、また、その人のデータのプライバシー保護を最も簡単な選択肢にする必要がある。

最終的に本書の目標は、政府が発行するデジタルアイデンティティ資格情報に関する今後の道筋を描くために、ソートリーダーのコミュニティを巻き込み、行動を後押しすることである。このコミュニティが一致団結して、政策とプライバシーのギャップを縮め、世界的に受け入れられるプライバシー守る仕組み（解決策）を確実に用意することが重要である。

2 はじめに

世界各国の政府は、市民および登録居住者に対してデジタル資格情報を発行する方向へ移行しつつある。この取り組みは、さまざまなパイロット段階を経てゆっくり進む場合もあれば、十分な資金が投じられる政策的な施策として推進され、すでに地域住民の間で広く普及しつつある場合もある。個人は、自らのモバイルデバイスで、必要なものを全て手に入れることのできるレベルの利便性と制御を期待するようになってきており、また政府は技術が、自身を効率化し、市民や居住者、企業、政府自体のニーズにより迅速に対応可能にしてくれることを実感してきている。民間組織もこうした新たな資格情報の活用法を検討している。これらの資格情報は、求められる本人確認の保証レベルに対し本質的に高い価値を持つ一方で、企業が「Need-to-knowの原則」に対して「過剰に把握してしまい、そのデータについて責任を問われるリスク」とのバランスをどう取るべきかを検討する中で、プライバシー上のリスクも伴う。

デジタル資格情報とは、最も一般的な意味では、個人情報が格納されたデジタルファイルである。本書に記載するさまざまな標準に従い作成すれば、改ざんがあった場合にそれが分かり、資格情報に含まれるデータを要求するサービスに、どのような情報を開示するかを個人が選択することを可能にする設計になる。

政府発行の資格情報が、すべてではないにせよ大半の場合に他の資格情報と異なる点

は、政府発行の資格情報が「法的アイデンティティ」を伝達することにある。加えて、適切に実施されれば、政府が発行する資格情報は、その政府（例えば、国、地域、郡、州など）の住民内で一意性を持ち、正確かつ真正な、言い換えれば権威的源泉となる。

政府発行のデジタル資格情報は初期段階にあり、住民票やワクチン接種記録、運転免許証など既存の物理的資格情報のデジタル化という形を取ることが多い。だが、より多くの機能、より多くのデータ、より多くの実用性などが見込まれており、比較的シンプルなこのデジタルレプリカは、純粋なデジタル資格情報（すなわち、物理的アナログ要素を有さず、電子記録としてのみ存在する）へと進化しつつある。最も有名な政府発行のデジタル資格情報は、国際民間航空機関（ICAO）が1995年に規格を制定した電子パスポートであろう[2]。このデジタル資格情報は暗号学的に検証可能なアイデンティティ情報を含むが、ご存じのように、選択的開示に対応していない。また、生で撮影（taken live）された場合、自動顔認証に必要な生体情報が十分な質を備えている場合と備えていない場合があり、権威的源泉としては疑問符が付く。

世界銀行は、このような進化を次のように評している。「社会のデジタル化が進むにつれ、物理的な資格情報の所持に頼らないデジタルだけのIDシステムに向けた動きがみられるようになってきた。[3][2]」デジタル資格情報は、より動的な情報の集合を提供するし、その時のニーズに合わせて簡単に更新・拡張できる。非常に多くのデータを容易に入手できるようになり、次のステップでそのデータを新しい創造的な方法で利用することになるのは当然と言えるが、同時に個人のプライバシーが受ける影響は増す。

図1 – 基本的なIDシステムが一般的に発行する資格情報と認証器の例[4]

政府のステークホルダーは、デジタル経済全般に関わるプライバシーへの影響、そして最近では、特に政府発行のデジタル資格情報に関わるプライバシーへの影響を感じている。一方、政府自体は公共の安全と消費者保護、データセキュリティの問題を考慮に入れながら、効果的なプライバシー法を制定する方策を探っている。市民社会も同様に、プライバシーに関わる、技術的に強制力のある、さらなる法的保護を求める一方で、その適用範囲を拡大して、この保護が政府とプライベートセクター、両方の

[2] ICAO。Doc Series – Doc 9303. https://www.icao.int/publications/doc-series/doc-9303 （訳注：原稿よりURL更新。。2026年05月01日時点）

[3] 世界銀行。2019年。ID4D 実務者ガイド（Practitioner's Guide）：Version 1.0（2019年10月）。Washington, DC：世界銀行。ライセンス： Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

[4] 同上

行動を確実に網羅することを望んでいる。

政府とプライベートセクター、両方で生じたデータ侵害が広く知られたことで、個人や市民社会のメンバーは、自らの個人情報が流出するリスクに懸念を抱くようになった[5]。同様に、政府が、政府が発行する資格情報がいつ、どこで、どのように利用されたかに関するデータを新たに収集して、保有する個人データとそのデータを組み合わせ、監視手段として利用するとの懸念もある。そのため、プライバシー擁護派と一般の人々は、自分たちの生活において、政府機関や第三者がこれら新たな資格情報を利用できる範囲が拡大される可能性があると知ると、それが寝耳に水の事態である場合、否定的な反応を強く示す[6]。

一方、話題に上らないことが多いポイントであるが、政府を含め、アイデンティティエコシステムに関与するいかなる当事者も、個人データに関しては、完全に信用してはならない。政府が発行する資格情報は、検証済みの個人データが含まれているため、特別なプライバシーの考慮がなされているというのは事実であるが、この分野の文献では、アイデンティティシステムは最も小さいものでも複数当事者による信頼モデルを必要とし、その各当事者は技術的能力という点で同じ成熟度にあるとは限らない、という点がしばしば見落とされている。このマルチパーティ信頼モデルは最低限、プライバシーを強化する安全な方法でアイデンティティ情報を保有者に提供する発行者と、プライバシーを強化する安全な方法でアイデンティティ情報を受け取り、かつ選択的に開示することができる保有者、そしてプライバシーを強化する安全な方法で、要求されたサービスを提供する上で必要な最低限のアイデンティティ情報を要求できる検証者を含む。

見過ごされることが多い要素の1つに、 政府は通例、上記のような対象住民内での一意性の確立を含め、法的あるいは基本的なアイデンシティを確立する責任を負うということがある。これには、一定量の個人データ（典型的なところでは生体情報）を一元的に維持管理して、アイデンティティレゾリューションと呼ばれるプロセスで、同一人物に複数の身元が割り当てられないよう重複を排除することが求められる。法的あるいは基本的なアイデンティティが確立すると、コンテクスチュアル（コンテキストに応じた）アイデンティティあるいは機能的アイデンティティが得られる。法的資格情報の発行者（本書の場合、政府）と機能的資格情報の発行者（有権者登録機関、銀行、学校など）と資格情報消費者（政府機関、民間企業、別の個人など）の間、その資格情報が格納されるデバイスとアプリやウォレットと個人の間にプライバシー要件が存在する。

---

[5] 例えば、2018年のAadhaarの侵害に関するメディアレポート（Sapkale, Yogesh。『Aadhaarのデータ侵害は世界最大規模とWEFのグローバルリスクレポートとAvastが報道（Aadhaar Data Breach Largest in the World, Says WEF's Global Risk Report and Avast）』Moneylife NEWS & VIEWS、2019年2月19日。2023年4月1日にアクセス。https://www.moneylife.in/article/aadhaar-data-breach-largest-in-the-world-says-wefs-global-risk-report-and-avast/56384.html）および米国政府のさまざまなデータ侵害に関するレポート（Lord, Nate。『米国史上最大の政府のデータ侵害トップ10（Top 10 Biggest Government Data Breaches of All Time in the U.S）』（Digital Guardian、2020年10月6日。2023年4月1日にアクセス。https://www.digitalguardian.com/blog/top-10-biggest-us-government-data-breaches-all-time）を参照。

[6] 例えば、Center for Human Rights & Global Justice。『地獄への道を開く？デジタルIDの推進における世界銀行とGlobal Networksの役割に関する入門書（Paving the Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID）』、NYU School of Law。2022年6月。https://chrgj.org/2022-06-paving-digital-road-to-hell/ （訳注：原稿よりURL更新。。2026年05月01日時点）

ガバナンスの考慮に加え、技術的複雑性と多種多様な実装から生じる厄介な問題がある。政府による監視の可能性や、民間エンティティによるデータの悪用の可能性に関して市民社会が提示する懸念を見ると、単独で信頼できる要素が1つもないことを証明している。

国・地域内、またはそれらをまたいで機能するマルチパーティ信頼モデルの必要性以前に、ユーザーエクスペリエンスの問題もある。各ユーザーフローの設計はそれ自体が、ユーザーによる賢明で、プライバシーを保護する選択を助けられるものでなければ、ユーザーをミスリードし、選択を誤ることになる。現在の技術で可能になることの技術的な現実と、法令や規制で求められるプライバシーの保護、検証済みのアイデンティティに関する政府要件との間のギャップは大きく、しかも、デジタルエコシステムの複雑性のなかで、自らのパズルのピースを重視するステークホルダーから忘れられてしまうことも多い。
政府発行のデジタル資格情報の、よりプライバシーを守ることができる未来にたどりつくには何が必要かを理解するためには、まず、現状を理解する必要がある。「ここからたどり着く」にあたり、世界の一部の国・地域におけるプライバシーの現状と政府発行などの資格情報の実態をみていく。また、生体認証とデータ最小化、プライバシー法、ユーザー制御、リライングパーティ（RP）の信頼性と責任に伴う主要な問題についても考察する。デジタルトランスフォーメーションの進行は、個人のプライバシーとデジタル資格情報の有用性の向上をある程度約束しており、どのような約束が、誰に対して行われているかを精査していく。
個人へのデジタル資格情報の提供は、大きな可能性への扉を開くが、その道のりは数多くのギャップとリスクを伴う。「ギャップとリスク」のセクションでは、これらの期待にインターネット規模で果たすには何が必要かをみていく。政策面の考慮からプロトコルの変更まで、関与する全てのステークホルダーのニーズを満たす万能薬はない。だが、政策立案者と市民社会の両方がよりプライバシーを守る未来に向けて進むために講じることができる前向きな対応策はある。

2.1 用語と定義

本書は、定義を完全に表現する単語として、以下の用語を簡略表現として使用する。本書でこの用語が出てきた場合、定義に置き換えて解釈する必要がある。ある特定の用語について、政府や技術者、市民社会のメンバー、研究者、言語学者の見解が必ずしも一致せず、複数の情報源を踏まえて定義を補っている。

用語	定義
プライバシー	個人が自らの個人情報の収集・利用方法を制御する手段を得る権利を含めた、個人がそっとしておいてもらう権利、あるいは干渉や侵害を受けない権利
アイデンティティ	個人に関連する一連の属性のセット
デジタルアイデンティティ	アイデンティティに関する機械可読な構造化されたデジタル表現
資格情報	個人に関する情報が記載された文書
デジタル資格情報	個人に関する情報を格納したデジタルファイル
純粋なデジタル資格情報	物理的なアナログ要素を持たず、電子記録でのみ存在する資格情報。
信頼モデル	ビジネス上・技術的・法的・規制上の要件の組み合わせをベースとしたシステム

3 ポリシーと技術の現状

プライバシーの現状が複雑だと述べるとしたら、それはこの領域における課題の多様性を表現しきれていない。ニュースや裁判所での訴訟で見られる緊張関係は、国・地域により異なるプライバシーと求められる機能性の間の不安定なバランスを反映している。どの地域も、その能力や、またプライバシーを尊重する方法でのデジタル資格情報の発行と利用とはどうあるべきかに関する理解に応じて、それぞれ異なる意思決定を行っている。モバイル運転免許証に代表される大規模なユースケースでは、現在の物理的な資格情報で何が可能かに着目することから議論が始まる。デジタル資格情報にまず最低限期待されるのは、写真と物理的な特徴（生体認証）、偽造防止（発行者の検証可能性）、氏名と住所（個人の識別子）などの提供である。デジタルであるということは、資格情報の利用時に、個人のプライバシーを守るために、もっと多くのことができる方法があることを示唆する。

ただし、その最低限期待されるものですら、対処しなければならない重要な問題をもたらす。デジタル資格情報の提供はしばしば、現在提供されている物理的な資格情報より優れた機能を約束するが、これらの重要な問題はそれがさほど簡単ではないことを示唆する。

多くの組織にとって、政府発行のデジタル資格情報を由来とする個人データに関する保証レベルは、自らのサービスの基盤となる。このオンボーディング（利用開始）プロセスは、リモート環境（ユーザーがデジタルアプリ経由で情報を提出する場合など）ではさらに複雑化する。そこでは、提示者と文書を紐付けるために、政府発行の文書の画像に加え、（正当な）文書保有者の（実在すると推定される）ライブ画像が使用されるからである。 文書をどう認証し、対象者が実在する本人であるとどう特定するかは、リスクベースのアプローチを用いる。組織が、最低年齢や居住地確認など特定の法的要件を順守する必要がある場合、これらの資格情報（資格情報）は最も有益であり、またおそらく唯一の実行可能な選択肢となる。法的要件ではないユースケースであっても、企業にとって、ユーザーに現行の政府発行のアイデンティティ文書の提出を求めることが当たり前になっていることが多い[7]。米国では「運転免許証や身分証明書明書のセキュリティを高める」ためREAL ID法（2005年）が制定された。同法では単にセキュリティ機能を調べるだけでなく、「…発行機関にて、その人が提出する必要がある各文書の発行と有効性、完全性を検証し…」とあり、発行機関に遡って正当性を検証することが義務づけられた[8]。

一方、紙ベースの環境でのこのような特定データの確認は、かなり負担の大きいメカ

[7] 『自分のIDを出会い系サイトやアプリに提供すべきか（Should I Give My ID to a Dating Website/App?）| PrivacyRights.Org』、2020年2月10日。2023年4月1日にアクセス。 https://privacyrights.org/resources/should-i-give-my-id-dating-websiteapp.

[8] 『REAL ID法 – 第II編（REAL ID Act – Title II）』。2005年。H.R.1268。米国国土安全保障省。 https://www.dhs.gov/xlibrary/assets/real-id-act-text.pdf

ニズムとなっている。これにより、その状況で実際に必要なデータを遥かに超えるものが開示されている実態がわかる。個人がタバコを購入できる法定年齢であることの検証には、具体的な生年月日だけでなく、実名や住所、社会保障番号や運転免許証番号など政府発行の識別子も含まれる。このシステムは、プライバシーは、ほとんど配慮されておらず、また明らかに漏洩を起こしやすい[9]。とはいえ、これら弱点は知られている。一方で、デジタル資格情報がもたらす新たなリスクや課題は、検討すべきトピックとして表面化し始めたばかりである[10]。

デジタル資格情報への移行が進む中、政府および政府データに依存するサービスには、個人にとってより一層プライバシーを強化する環境を支えるための強力な選択肢がある。本書ではまず、政府発行のデジタル資格情報の現状と、これらデジタル資格情報を、関与する全てのステークホルダーにとってより良い選択肢となり得る特長をみていく。次に、現在これらデジタル資格情報を実現している技術と、新たな環境でプライバシーの課題がどのように変化していく可能性が高いかについて考察する。

3.1 影響力の大きい国内・国際規則・標準

デジタル資格情報の発行と維持管理、取り扱いを支える上で必要な技術は、適切な利用について定めた法的要件によって形作られる。多くの国や地域だけでなく、政府間組織さえも、政府がどのようにデジタル資格情報を発行し、使うことができるかに対応するための独自のフレームワークの策定を進めている。そうしたなか、欧州連合（EU）の一般データ保護規則（GDPR）および第2版ネットワーク・情報セキュリティ（NIS2）指令は、人権とプライバシーの保護という点では依然として不十分であるとの批判はあるものの、セキュリティとプライバシーの雛形（テンプレート）として機能しており、他国もこれを参考にしている[11]。同様に、米国ではカリフォルニア州消費者プライバシー法（CCPA）が米国の一部の州が参考とするモデルとなる一方、連邦レベルでみると、基本システムと収集したデータの利用については、1974年プライバシー法が依然として指針となるプライバシーのフレームワークとなっている。こうした国ごとのギャップを埋めるのは、経済協力開発機構（OECD）が策定、採択した「プライバシー原則（Privacy Principles）」である。

[9] LexisNexis Risk Solutions。『FraudTM調査の真のコスト| LexisNexis Risk Solutions』、2022年。2023年4月1日にアクセス。https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study.

[10] Privacy International。『国民デジタルIDシステム：方法と形状、形態（Digital National ID Systems: Ways, Shapes and Forms』、2021年10月26日。2023年4月1日にアクセス。https://privacyinternational.org/long-read/4656/digital-national-id-systems-ways-shapes-and-forms.

[11] Vanberg, Aysem Diker。『GDPR後の情報プライバシー - 道のりの終焉か、それとも長いジャーニーの始まりか（Informational Privacy Post GDPR – End of the Road or the Start of a Long Journey?）』、The International Journal of Human Rights 25, no. 1（2021年1月2日）：52～78。https://doi.org/10.1080/13642987.2020.1789109.

デジタルアイデンティティとそれに伴う資格情報に関連する全ての規則は、その適用範囲が限定されている場合があり、注意深く読む必要がある。例えば、OECDのガイドラインは政府向けのガイダンスとなるのに対して、ISO規格はより一般的な位置づけとなる。一方、国内の法令はプライベートセクターの組織に限定されることが多く、また、プライバシー関連で政府が行うであろう範囲について言及していないか、全く異なる範囲を示しているかのいずれかである。

本セクション（3.1）では、本書の発表時点で最も影響力のある規則を多く精査しているが、全ての規則を網羅することを目指してはおらず、また、環境が急速に変化している点をご了承願いたい。

3.1.1 OECDのプライバシー原則

OECDのプライバシー原則は世界各国のプライバシー法のフレームワークとなる。この原則は「プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD理事会勧告」の一部である[12]。共通の一連の原則を持つことは、個人データに関わる国際取引をはるかに円滑にする。なぜなら、それによって各国の法律が相互運用できる可能性が高まるからである。この原則は政府発行のデジタル資格情報に限定されたものではないが、これを用いることで、プライバシー関連で何がベストプラクティスとなるかの手引きとなる。

プライバシー原則は8項目に分かれる[13]。

1. 収集制限の原則
2. データ内容の原則
3. 目的明確化の原則
4. 利用制限の原則
5. 安全保護の原則
6. 公開の原則
7. 個人参加の原則
8. 責任の原則

この原則は世界各地の重要なプライバシー法令の多くに影響を与えてきた。例えば、この原則はISO/IEC 29001（プライバシーフレームワーク）とアジア太平洋経済協力（APEC）プライバシーフレームに直接的な影響を与えている[14]。

---

[12] OECD。『プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD理事会勧告』。OECD Legal Instruments、2013年10月7日。https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL- 0188.

[13] この原則の具体的な内容については付録Aを参照。

[14] OECDのプライバシーガイドラインの影響について詳しくは、最近機密扱いから外された、以下のレポートを参照されたい。OECD理事会。『プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD理事会勧告の実施に関するレポート：（注釈は事務総長）（Report On The Implementation Of The Recommendation Of The Council Concerning Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data: (Note by the Secretary-General)』、2021年3月17日。https://one.oecd.org/document/C(2021)42/en/pdf。APECプライバシーフレームワークは、https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1 （訳注：原稿よりURL更新。。2026年05月01日時点）で閲覧できる。

3.1.2 ISO/IEC 29100（プライバシーフレームワーク）

ISO/IEC 29001（プライバシーフレームワーク）はISO（国際標準化機構）とIEC（国際電気標準会議）が共同で発行した規格である[15]。この規格は、ISO/IEC 27018（(Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processor（個人を特定する情報（PII）処理事業者として機能するパブリッククラウドにおけるPIIの保護の実施基準））やISO/IEC 27701（プライバシー情報管理に向けて、ISO/IEC 27001とISO/IEC 27002を拡張したもの）など別の一部規格とそれに関係した認証のプライバシーに関するベースラインの役割を果たしている[16]。

ISO/IEC 27701への適合を証明でき、そのためISO/IEC 29001のガイダンスに従っている組織は、世界各地の法的・規制要件をはるかに満たしやすい立場にある。Microsoftが当初、オープンソースコミュニティに無償で公開していたオープンソースのデータ保護マッピングプロジェクトは、これら規格が世界各地のさまざまなデータ保護規則にどのように関連しているかを組織が理解する手助けとなることを目的とする[17]。

ISO/IEC 29100ファミリーでは、このトピックに関連する2つの規格「ISO/IEC 29134:2017（プライバシー影響評価のためのガイドライン）」と「ISO/IEC 29184:2020（オンラインプライバシー通知と同意）」が追加されている[18]。いずれの規格も、PIIを処理するあらゆるエンティティに関係するものである。

政府発行のデジタル資格情報を複数の国・地域にまたいで活用することをめざすサービスプロバイダにとって、この種の標準化されたガイダンスは極めて重要である。

3.1.3 欧州一般データ保護規則（GDPR）

GDPRが世界の舞台に及ぼしてきた影響を軽視することはできない。2018年の発効以来、同規則は欧州連合以外の国・地域でも、デジタルアイデンティティとプライバシーポリシーを牽引し続けている。欧州企業の強力なパートナーとなることで経済的メリットを得る国は、欧州委員会が定める水準の十分なデータ保護規則を備えていなけ

---

[15] ISO/IEC 29100:2011（情報技術 - セキュリティ技術 - プライバシーフレームワーク）。ISO/IEC JTC 1/SC 27。スイス・ジュネーブ：ISO、2011年12月発行、2017年にレビューおよび確認。https://www.iso.org/standard/45123.html.

[16] ISO/IEC 27018:2019（情報技術 — セキュリティ技術 — 個人を特定する情報（PII）処理事業者として機能するパブリッククラウドにおけるPIIの保護の実施基準）。ISO/IEC JTC 1/SC 27。スイス・ジュネーブ：ISO、2019年1月発行。https://www.iso.org/standard/76559.html（訳注：2026年05月01日時点はISO/IEC 27018:2025に更新 https://www.iso.org/standard/27018）およびISO/IEC 27701:2019（セキュリティ技術 — プライバシー情報保護のために、ISO/IEC 27001とISO/IEC 27002を拡張したもの — 要件とガイドライン）。ISO/IEC JTC 1/SC 27。スイス・ジュネーブ：ISO、2019年8月発行。 https://www.iso.org/standard/71670.html. （訳注：2026年05月01日時点はISO/IEC 27701:2025に更新 https://www.iso.org/standard/27701）

17『GitHub – Microsoft／データ保護マッピングプロジェクト：オープンソースデータ保護／プライバシー規則マッピングプロジェクト（GitHub - Microsoft/Data-Protection-Mapping-Project: Open Source Data Protection/Privacy Regulatory Mapping Project）』。GitHub、最終更新日：2022年7月26日。2023年4月1日にアクセス。https://github.com/microsoft/data-protection-mapping-project.

[18] ISO/IEC 29134:2017（情報技術 — セキュリティ技術 — プライバシー影響評価のためのガイドライン）。ISO/IEC JTC 1/SC 27。スイス・ジュネーブ：ISO、2017年6月発行。https://www.iso.org/standard/62289.html（訳注：2026年05月01日時点はISO/IEC 29134:2023に更新 https://www.iso.org/standard/86012.html） and ISO/IEC 29184:2020（情報技術 — オンラインプライバシー通知と同意）。ISO/IEC JTC 1/SC 27。スイス・ジュネーブ：ISO、2020年6月発行。https://www.iso.org/standard/70331.html.

ればならない[19]。そのため、パートナー国の「十分性」要件と、EU加盟国の市民および居住者を含める形での運用を求める、プライベートセクターの幅広い組織に対する順守の義務づけが相まって、GDPRはデータプライバシーのベースラインとみなされている[20]。GDPRは、セキュリティとプライバシーに対するデータ中心型アプローチを提供する。 GDPRは善意によるものではあるが、データ共有に関して多くの障害を生じさせている。こうした障害（厳格さ）は、ビジネスにとってはプラスになるとみなされることが多い一方で、研究や中小企業といった領域にはマイナスの影響を与えている[21]。個人（すなわち「自然人」）の個人データの権利と保護の定義については、GDPRがパラダイムシフトをもたらした。この事実は、政府発行のデジタル資格情報を含めたデジタル資格情報の利用方法に多大な影響を及ぼしてきている。

プライバシー規則がまだ初期段階にあり、デジタル経済がスタート立ち上がったばかりの国では、GDPRの十分性要件が、EUとの強力なパートナーシップへの道を切り開く形で、いかに地域のデジタル経済を前進させるかというロードマップを提示している。こうしたパートナーシップには経済成長をもたらす期待が伴うため、プライバシーとデータ処理、デジタル資格情報の欧州モデルに従う強力なモチベーションとなっている。ある意味、GDPRが示す指示に従うことは、すでに強固な経済を確立し、市民や消費者のプライバシーに独自の見解を持つ国のほうが難しい。

3.1.4 NIS2指令

GDPRがデータ中心のセキュリティに焦点を当てているのに対し、EUのNIS2指令は、システムレベルのセキュリティに焦点を当てている。政府発行のデジタル資格情報システムを含重要なインフラの保護により、個人のプライバシーがさらに強化されることになるが、プライバシーは同指令の複数ある考慮点の1つにすぎない。データの安全確保を義務づける要件は、市民と居住者のデータの具体的な保護策とそのデータへの不適切なアクセスがあった場合の通知を義務化することで、市民と居住者のプライバシーを暗に支えている。同指令は2023年1月16日に発効しており、EU加盟国は2024年10月18日までにNIS2に対応した適切な国内法を策定しなければならない[22]。

---

[19] 欧州委員会。『十分性決定：EUは非EU加盟国が十分なレベルのデータ保護を確保しているかどうかをどのように判断しているのか（Adequacy Decisions: How the EU Determines If a Non-EU Country Has an Adequate Level of Data Protection）』。2023年4月1日にアクセス。 https://commission.europa.eu/law/law-topic/data-protection/international-dimension-dataprotection/adequacy-decisions_en.

[20] Peukert, Christian、Stefan Bechtold、Michail BatikasおよびTobias Kretschmer。『規制の波及効果とデータガバナンス：GDPRが示す根拠（Regulatory Spillovers and Data Governance: Evidence from the GDPR）』。Marketing Science 41, no. 4（2022年7月1日）：318〜40。https://doi.org/10.1287/mksc.2021.1339.

[21] 例えば、「Clarke, Niamh、Gillian L. Vale、Emer P. Reeves、Mary Kirwan、David Smith、Michael Farrell、G. A. HurlおよびNoel G. McElvaney。『GDPR：研究を妨げる障害？（GDPR: An Impediment to Research?）』、Irish Journal of Medical Science 188, no. 4（2019年2月8日）：1129〜35。 https://doi.org/10.1007/s11845-019-01980-2」および「Geradin, Damien、Theano KaranikiotiおよびDimitrios Katsifis。『GDPR短見：善意の規則がどのようにして大規模オンラインプラットフォームを特別扱いするようになったのか - 広告技術の場合（GDPR Myopia: How a Well-Intended Regulation Ended up Favouring Large Online Platforms - the Case of Ad Tech）』。European Competition Journal 17, no. 1（2021年1月2日）：47〜92。https://doi.org/10.1080/17441056.2020.1848059を参照。

[22] 『指令(EU) No 910/2014と指令(EU) 2018/1972を改正し、指令(EU) 2016/1148を撤廃する、欧州連合全体で高共通レベルのサイバーセキュリティを実現するための措置に関する欧州議会および欧州理事会の指令（EU）2022/2555

GDPRと同様、EU法令フレームワークの1部であるとはいえ、同指令は国際的な企業にも多大な影響を及ぼす。サイバーセキュリティに関する主たる意思決定拠点がEU域内にある対象企業は同指令の要件に従わなければならない[23]。

3.1.5 SDGRとワンスオンリー原則

シングルデジタルゲートウェイ規則（Single Digital Gateway Regulation : SDGR）は、第6条にあるように、2023年12月までに21のクロスボーダーサービスをオンラインで提供することをEU諸国に義務づける規則である（欧州議会、2018年）[24]。SDGRには、デジタル公共サービスを国内の市民だけでなく、EUの市民もアクセスできるようにして、クロスボーダー公共サービスの発展を促す必要があると記載されている。シングルデジタルゲートウェイの優先事項の1つは、欧州の行政機関に自らのアプローチでの「ワンスオンリー原則（OOP）」の実践を奨励することである[25]。SDGRが提供するこの法的フレームワークとサービスはEU28カ国に、より構造的かつ協調的な方法でクロスボーダーソリューションを開発する義務を負わせる。2023年末までに、21のオンライン手続きを完全にデジタル化し、ペーパーワークをなくすことが求められる。これら公共サービスは、出生や住居、学習、仕事、転居、退職、事業の経営など、さまざまなライフイベントに関係するものである。

データ最小化全般は、自らのシステムを利用する個人のプライバシーの保護に関心を持つサービスにとって重要な要素となる。これは、行政サービスにも同様に当てはまる。行政サービスは、多くの情報について権威ある情報源になり得る立場なのに、それでもサービス提供のために必要最小限だけを要求する、という難しい線引きをしな

（2022年12月14日）（NIS2指令）（Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive）)』。欧州連合、2020年12月14日。 http://data.europa.eu/eli/dir/2022/2555/oj.

[23] Vladimirova-Kryukova, Anna。『NIS2指令のEU内外への影響（The Influence of the NIS2 Directive In and Outside of the EU）』。ISACA NOW BLOG、2021年11月10日。https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/the-influence-of-the-nis2-directive-in-and-outside-of-the-eu.

[24] 欧州委員会。『規則(EU) No 1024/2012（シングルデジタルゲートウェイを確立して、情報、手続きおよび支援・問題解決サービスへのアクセスを提供し、かつ規則(EU) No 1024/2012を改正する欧州議会および欧州理事会の規則(EU) 2018/1724（2018年10月2日）（EEAにスイスとトルコを加えた国を対象）（Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 Establishing a Single Digital Gateway to Provide Access to Information, to Procedures and to Assistance and Problem-Solving Services and Amending Regulation (EU) No 1024/2012 (Text with EEA Relevance)）』。欧州委員会、2018年11月21日。https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.295.01.0001.01.ENG.

[25] 欧州委員会。『国境を超えた証拠の自動交換用の技術システムの運用仕様および欧州議会および欧州理事会の規則(EU) 2018/1724に従った「ワンスオンリー」原則の適用を定めた欧州委員会実施規則(EU) 2022/1463（2022年8月5日）（EEAにスイスとトルコを加えた国を対象）（Commission Implementing Regulation (EU) 2022/1463 of 5 August 2022 Setting out Technical and Operational Specifications of the Technical System for the Cross-Border Automated Exchange of Evidence and Application of the 'Once-Only' Principle in Accordance with Regulation (EU) 2018/1724 of the European Parliament and of the Council (Text with EEA Relevance)）』、2022年8月5日。https://eur-lex.europa.eu/eli/reg_impl/2022/1463/oj.

ければならない。

SDGR第42条には、同規則とOOPを全てのデータ保護ルールに適合させるにはどうすればいいかについて記載されている。同条で具体的に挙げられている原則は、データ最小化、正確性、保存の制限、完全性、機密性、必要性、比例性、目的の制限である。また、規則の実施は「セキュリティバイデザインとプライバシーバイデザインの原則に完全に従ったものであるべきであり、また、公平性と透明性に関係するものを含め、個人の基本的権利も尊重するものであるべきである」と強調している。

EU域内でのOOPの理解には、ばらつきがある。OOPを他データベースに複製物がなくオリジナルデータしか存在しないことと法律で理解している国もあれば、市民や企業が一度しかデータを提供しないことと理解している国もある。EUのフレームワークでは、OOPとは、すでに一度政府機関に自分の基本データを提供していれば、その市民は何度もそれを提供する必要がないことを意味する。OOPには、市民は自分のデータを共有することを行政に許可することで、デジタル化された公共サービスの利用前に自らの標準情報を何度も提供する必要がなくなると記載されている。加えて、交換するデータの量を最小限に減らし、要求されているデータだけにするにはどうすればいいかについて光を当てた条項もある。

3.2 政府発行のデジタル資格情報システム

政府にデジタル資格情報の発行を促すユースケースはさまざまある。デジタル保険証からモバイル運転免許証まで、世界各国はデータをより最新かつ便利で、不正行為を受けにくくする方法を模索している。先に紹介したように、政府が発行する資格情報は、住民の中で真正性（veracity）と一意性を確認する本人確認（identity resolution）の結果として、法的アイデンティティを示し得る。政府がデジタル資格情報に移行するにつれ、関連する法的（基礎的）アイデンティティ情報（生体認証データを含む）を不正から守るため、暗号技術によりデータの真正性と完全性を担保するデジタル署名が用いられている。すなわち、検証者が、提出された情報が信頼できるソースからのものであるかどうか、また改ざんされていないかどうかを判断できる。暗号もプライバシーの向上に利用される場合がある。政府がどのようにデジタル資格情報をプロビジョニングするのか、また政府がこのデータをどのように共有するつもりかは、プライバシーの成果に重要な影響を与える。例えば、現在の電子パスポートは安全な施設でプロビジョニングされ、暗号化されたチャネルでデータを共有するよう設計されている。一方、現行の物理的パスポートは、選択的開示やゼロ知識証明によるデータ最小化に対応していない。これはICAOのデジタルトラベル資格情報にも当てはまる。データフィールドレベルで暗号化するのではなく、全てのデータを同じデータバンドルに暗号化する、物理パスポートと同様の暗号化モデルを踏襲しているため、データ最小化を支える仕組みがない。これとは対照的に、最新のISO mDL仕様（下記セクション3.3.1.6に詳述）はデータフィールドレベルでの暗号化が可能で、選択的開示に対応している。ただし、これらmDL資格情報の発行（プロビジョニング）については、発

行（プロビジョニング）や遠隔での共有の方法を十分に扱う標準が、まだ最終確定していない。

多くの国がプライバシー原則を規則やサービスに反映させているとはいえ、プライバシーはこれら新システムの数多くの考慮事項の1つにすぎない。デジタル資格情報を政府が発行する、より直接の動機は以下などである。

- 住民がより簡単にオンラインで、また対面で、自分のアイデンティティをアサートする手助け（例えば、銀行口座の開設、年齢制限のある商品の購入、政府の給付金にアクセスする権利のアサート、より手軽な旅行など）、
- 不正行為（例えば、給付金の不正受給や偽の資格情報を提出しての金融口座開設など）の防止 、
- 住民が年齢制限のある商品を購入したり、その他のサービスにアクセスしたりする権利をアサートする手助け、および
- 旅行をしやすくすること

政府が同時に資格情報の発行者であり、利用者であり、規制当局であることは、興味深い課題である。政府はその国・地域全体で用いるための資格情報を発行し、デジタル資格情報を用いて給付へのアクセス権を確認し、同時に自らの利用のあり方も規制する。いずれの役割もほぼ同時に成熟させる必要があり、また今後、部署、地方、国、さらには地域レベルで横断することが多くなるという事実が、これらの視点を複雑にしている。この点、シンガポールのSingpassのような都市国家モデルは単一の管轄であり、統治構造が集中している。

eIDAS 2.0は、政府が市民に発行するデジタル資格情報をどのように開発するかの潜在的モデルであるとEU域外の政府からみなされるようになり始めた。だが、この領域では、他地域も主導権を発揮している。インドのAadhaarシステム[26]や、シンガポールのSingpass[27]、イタリアのパブリックデジタルIDシステム、米国のさまざまな州のモバイル運転免許証は、かなりの住民が日常的に利用する政府発行デジタル資格情報プログラムのごく一部にすぎない。また無論、各プログラムは、その運用を司る法律と、それで利用する技術を通じてプライバシーに影響を及ぼす。

eIDAS 2.0に基づく欧州デジタルアイデンティティ・ウォレットは重要なモデルである。法律上必要な場合以外に個人識別データ（PID）を共有しておらず、これが、依然として政府（加盟国）の活動であり、検証プロセスである発行プロセスにおいて、PIDを他の適格・非適格なアイデンティティデータから分離しているのである。AadhaarやSingpassなど政府が一元管理するアイデンティティモデルとは異なり、 発行者は検証プロセスに関与しないため、トランザクションのリンク可能性が低下する。詳しくは、次のセクションで説明する。

[26] インド政府、『myAadhaar』、インド固有識別番号庁、website, https://uidai.gov.in/en/.
[27] Singpass、https://www.singpass.gov.sg/main/

現在稼働しているシステムはほかにもあるが、ある国で機能するシステムが、法的フレームワークや住民のデジタルリテラシーのレベル、文化的期待の違いにより、別の国では機能しない場合もある。本書で取り上げるシステムは、現時点で利用されている導入形態の多様性を示すために選んだ[28]。

3.2.1 eIDAS 2.0（電子識別と認証、信頼サービス）

eIDAS規則は元々、EU規則910/2014として2014年7月23日に制定されたが、一般にeIDAS 2.0と呼ばれる最近の改正により、新たに注目を集めている。eIDAS 2.0は、EU域内全体で相互運用可能なデジタルアイデンティティ・ウォレット（EUDIウォレット）をEUの全ての市民と居住者、企業が利用できるようにすることを全てのEU加盟国に義務づけている。つまり、eIDAS 2.0は、資格情報ではなく、ウォレット全般に焦点を当てた法的枠組みであるが、これらウォレットに政府発行のデジタル資格情報を含めることに重点を置いているため、資格情報に関する本セクションで取り上げた。
EUは、デジタル資格情報を物理的な資格情報の単なる代替ではなく、これに改善を加えたものとするべく、取り組みを強力に推し進めている。アーキテクチャを明確に定め、大規模な試験的実装を奨励することで、加盟国はイノベーションがすぐに、かつ大規模に起きることを期待している[29][28]。GDPRが個人データのプライバシー保護の中核的な法的フレームワークを提供し、また（プライバシーに特化してはいないが）サイバーセキュリティ要件を定めるNIS2により今後、プライバシー問題に取り組むEUの姿勢が向上するはずであり、この新たなデジタルエコシステムではプライバシー保護が強く考慮されている。
eIDAS 2.0は、デジタル資格情報利用時のプライバシー保護を高めるいくつかの特性を備えることを求めているが、そのなかで最も重要なのは「人々が自らのアイデンティティとデータ、証明書のどの部分を第三者と共有するかを選択し、また、その共有の動向を常に把握することを」可能にすることである[30]。各加盟国はeIDASの要件に合致した技術を自由に開発できる。ただし、その技術は国境を超えて相互運用可能なものでなければならない。その詳細については、開発者に委ねられている。

とはいえ、一部のプライバシー擁護派や市民社会からは、一意で永続的な識別子（個人の追跡とプロファイリングを可能にする）に関する問題からデータの一元管理（監

[28] デジタルアイデンティティリファレンスデプロイメントについて詳しくは、Secure Identity Allianceの白書『世界中のデジタルアイデンティティに発言の場を与える（Giving Voice to Digital Identities Worldwide）』に記載されている。『世界中のデジタルアイデンティティに発言の場を与える - 共通の課題を克服するための主なインサイトと経験（Giving Voice to Digital Identities Worldwide - Key Insights and Experiences to Overcome Shared Challenges）』、2022年3月16日。https://secureidentityalliance.org/utilities/news-en/entry/giving-voice-to-digital-identities-worldwide-1-1.（訳注：2026年05月01日時点はリンク切れ）

[29] 欧州委員会。『欧州デジタルアイデンティティウォレットのアーキテクチャとリファレンスフレームワーク（European Digital Identity Wallet Architecture and Reference Framework）』。Shaping Europe's Digital Future、2023年2月10日。https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture- and-reference-frameworkと欧州委員会。『資金調達&入札：シングルエレクトロニックデータインターチェンジエリア（SEDIA）（Funding & Tenders: Single Electronic Data Interchange Area (SEDIA)』、2022年12月16日。https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022- deploy-02-electronic-id.

[30] 欧州委員会。『欧州委員会が、全ての欧州人が信頼、安心できるデジタルアイデンティティを提案（Commission Proposes a Trusted and Secure Digital Identity for All Europeans）』。Press Corner、2021年6月3日。https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663.

視国家になるという不安を抱かせる）まで、eIDAS 2.0に関する大きな懸念の声も聞かれる[31]。さらに、国境をまたぐ利用において、システムの犯罪利用や不正利用を特定し、対処するための法的メカニズムが欠けている点は、警戒すべき論点である[32]。個人にコントロールを与えることはプライバシー確保に必要だが、それだけでは十分ではない。というのも、サービス提供者が厳密には不要な情報まで求め得るからである（何が「必要」かについて見解が分かれる可能性はある）。同様に、eIDAS 2.0には、個人は国境をまたいで利用するために一意かつ永続的な識別子の発行を要求できるとする条項があるが、これは、主たる目的が最終結果にたどり着くことである場合、トランザクション中に全ての選択肢が自分に開かれていることを個人が理解することを期待したものであり、理想的とは言えない[33]。

eIDAS 2.0は、政府が内部で保存できる資格情報の形式の定義ではなく、ウォレット自体に焦点を当てている。形式やプライバシー保護、政府発行のデジタル資格情報の一般的用途に関するガイダンスは、eIDAS 2.0の実施法に盛り込まれることが予想される[34]。本書の執筆時点で、欧州委員会はアーキテクチャリファレンスフレームワーク[35]と、自ら選定したISO/IEC 18013-5（モバイル運転免許証）やOpenID for Verifiable Credential Issuance、OpenID for Verifiable Presentation、OpenID for Self-Issued OpenID Provider v2に加え、Selective Disclosure for JSON Web Tokenを実際にどのように機能させるかを詰めているところである。加えて、欧州委員会はリファレンスアプリケーション開発と、欧州人に関係のある一連のユースケースに対応するよう設計された大規模パイロットプロジェクトにも資金を提供してきた。これらユースケースやプロジェクトが開発や展開の段階を進んでいくにつれ、標準とポリシーのギャップが特定、修正され、地域的な相互運用性に対応できるようになることが予想される。

---

[31] Hoepman, Jaap-Henk。『欧州デジタルアイデンティティフレームワークのアーキテクチャを分析する（Analysing the Architecture of the European Digital Identity Framework）』、2023年2月14日。https://blog.xot.nl/2023/02/14/analysing-the-architecture-of-the-european-digital-identity-framework/index.htmlに加え、欧州議会およびVestager上級副委員長、Breton委員に宛てたデジタル権に関する書簡（epicenter.worksが取りまとめ）、2023年6月20日、https://epicenter.works/sites/default/files/cso-eidas-open_letter_2023.pdf.を参照。

[32] epicenter.works。『EIDAS 2.0 – プライバシーにとって過去に例を見ないリスク（EIDAS 2.0 – Unprecedented Risk for Privacy）』、2022年12月1日。https://epicenter.works/en/content/european-electronic-id-without-privacy-safeguards （訳注：原稿よりURL更新。。2026年05月01日時点）

[33] eIDAS 2.0改正版第11.a (2)条：「第１項に記載するサービスにアクセスするための要請に応じて、自然人を識別するために、加盟国は第12.4.(d)条に記載する最小限の個人識別データを提供するものとする。少なくとも１つの一意の識別子を有する加盟国は、ユーザーから要請があれば、国境を超えた利用のために一意で永続的な識別子を発行するものとする。当該の識別子はユーザーを域内全域で一意に識別するかぎりにおいて、セクター固有であっても、relying party固有であっても構わない（In order to identify natural persons upon their request for accessing services as described in paragraph 1, Member States shall provide a minimum set of person identification data referred to in Article 12.4.(d). Member States that have at least one unique identifier shall, at the request of the user, issue unique and persistent identifiers for cross-border use. Those identifiers may be sector or relying party-specific as long as they uniquely identify the user across the Union）」を参照。

[34] 実施法がどのように策定されているかについて詳しくは、https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vha0t8afc0yaを参照。

[35] 欧州委員会。『欧州デジタルアイデンティティウォレットのアーキテクチャおよびリファレンスフレームワーク（The European Digital Identity Wallet Architecture and Reference Framework）』。Shaping Europe’s Digital Future、2023年2月10日。https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture- and-reference-framework

3.2.2 インドのAadhaarシステム

登録参加者数と月間トランザクション数で世界最大の政府発行のアイデンティティプログラムはインドのAadhaarシステムである[36]。元々は2010年に開始され、Aadhaarの法的有効性を支持する判決をインドの最高裁判所が2018年に下したことで、幅広い普及へと進んだAadhaarシステムは、大規模導入を検討するにあたって興味深いモデルである[37]。

この生体認証をベースとする一元管理型識別システムはインド固有識別番号庁（Unique Identification Authority of India：UIDAI）が運用し、以下の主たるアイデンティティ機能を提供している。

1. **登録** – 顔や指、虹彩の生体認証データとともに、基本的な人口統計学的情報を登録する。
2. **重複排除** – 指紋と虹彩、および複数の生体認証サービスプロバイダを利用して一意性を確立する。
3. **審査（裁定）** – 重複などの異常が合法的なものか、不正行為であるかを手作業で判定する。
4. **付番（発行）** – 一意性の確立後にAadhaar番号を生成し、登録者に通知する。
5. **認証** – リクエストで提示された生体情報（プローブ）を、当該Aadhaar番号に紐づく登録済み情報と照合し、結果を返す。

Aadhaarシステムに関する調査・報告機関は、Aadhaarシステムが概ねインドの憲法に従っているとする、2018年の最高裁判所の判決を掲載した[38]。この判決は、Aadhaarが幅広い普及へと移行する道を開いたという点で大きな意義を持っていた。同判決は、このシステムのプライバシーの考慮に関し、いくつかの一般的なテーマを含むが、改変後のシステムがインドの憲法に沿っていると判断した。インドの最高裁判所を別にして、学術研究者など市民社会のメンバーは、Aadhaarシステムを市民や登録した居住者の政府による監視の懸念すべき事例とみなしている[39]。それに反論する形で、政府はAadhaarシステムにより国が過去9年間に2兆ルピー（240億米ドル）を超える節約をし

---

[36] インド固有識別番号庁| インド政府。『ホーム - インド固有識別番号庁（Unique Identification Authority of India）| インド政府（Home - Unique Identification Authority of India | Government of India）』。2023年4月1日にアクセス。https://uidai.gov.in/en/.

[37] 『K.S. Puttaswamy判事（退官）、他1名対Union Of Indiaなど（Justice K.S. Puttaswamy (Retd.) And Another Versus Union Of India And Others）』。インド最高裁判所、Civil Original Jurisdiction、2018年9月26日。https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf.

[38] Supreme Court Observer。『Aadhaar法の合憲性 - Supreme Court Observer（Constitutionality of Aadhaar Act - Supreme Court Observer）』、2021年12月24日。https://www.scobserver.in/cases/puttaswamy-v-union-of-india-constitutionality-of-aadhaar-act-case-background/.

[39] 例えば、Henne, Kathryn。『ガバナンスという名の下での監視：インドの漏洩システムの解決策としてのAadhaar（Surveillance in the Name of Governance: Aadhaar as a Fix for Leaking Systems in India）』。Information, Technology and Control in a Changing World、2019年6月22日、223〜45。https://doi.org/10.1007/978-3-030-14540- 8_11およびBhandari, VrindaおよびKaran Lahiri.『インドにおける監視状況とプライバシー、犯罪捜査：Puttaswamy後の世界で考えられる未来（The surveillance state, privacy and criminal investigation in India: Possible futures in a post-Puttaswamy world）』。U. Oxford Hum. Rts. Hub J. (2020)： 15、Tyagi, Amit Kumar、Gillala RekhaおよびN. Sreenath。『Aadhaarであなたのプライバシーは安全か：オープンディスカッション（Is Your Privacy Safe with Aadhaar? : An Open Discussion）』。Grid Computing、2018年12月1日。https://doi.org/10.1109/pdgc.2018.8745836を参照。

て、重複と偽のアイデンティティをなくすことができたと報告している[40][39]。平時であってもプライバシーに金銭的価値を付すのは難しく、これは明らかに同等のもの同士の比較ではない。だが、これにより、全国的なアイデンティティシステムへの移行と、強力な個人のプライバシー保護策を設けることの間で生じる緊張を説明することはできる。

Aadhaar番号保有者が利用できるサービスとサービスプロバイダには、以下などがある[41]。

- **Aadhaar番号の検証：**これによりサービスプロバイダとAadhaar番号保有者はAadhaar番号が有効であり、無効化されていないかどうかを検証できる。
- **電子メール／モバイル番号の検証：**Aadhaar番号保有者の登録モバイル番号はAadhaarオンラインサービスと、Aadhaarを活用した給付金制度へのアクセスに不可欠となる。居住者はすでに登録した電子メールアドレスとモバイル番号を検証できる。
- **生体認証のロック／ロック解除：**Aadhaar番号保有者は生体認証をロックすることで自分の生体認証の安全を確保できる。いったんロックした生体認証を認証に用いることはできない。居住者は生体認証のロックを解除すれば、生体認証トランザクションが再びできるようになる。
- **Aadhaarと銀行口座の 紐づけ状況のチェック：**Aadhaar番号保有者は Aadhaar番号が自分の銀行口座に紐づけられているかどうかチェックできる。Aadhaarの紐づけ状況はNPCIサーバから取得する。いかなる状況においても、UIDAIは表示された状況に責任または義務を負わないものとする。さらに、UIDAIはNPCIサーバから取得したいかなる情報も保存していない。
- **Aadhaarの認証履歴：**Aadhaar番号保有者は自分が行ったAadhaarの認証アクションの詳細をみることができる。
- **オフラインでのAadhaarデータ検証：**これは、Aadhaar番号保有者がIDのオフライン検証に用いることができる、安全な共有可能な文書。
- **バーチャルID生成器：**Aadhaar番号保有者は16桁のバーチャルID（VID）を生成できる。

このシステムは基本的に個人の生体認証情報に依存して登録時の重複を防ぐ。これについては、セクション4.2.2「生体認証技術」で詳しく述べる。Aadhaarシステムへの登録を親が選択した児童は5歳から、重複排除の目的で、自分の生体認証データを提出しなければならない。Silvia MasieroおよびS. Shaktiは次のように指摘しており、このシステムは新たなタイプの監視も可能にする。

[40] News。『政府の福祉スキームの「基盤」Aadhaarで2兆ルピーを節約：NITI Aayog（Aadhaar “‘bedrock’” for Govt Welfare Schemes, Saved over Rs 2 Lakh Crore: NITI Aayog』。Microsoft Start、2022年6月1日。https://www.aninews.in/news/national/general-news/aadhaar-a-bedrock-for-govt-welfare-schemes-saved-over-rs-2-lakh-crore-niti-aayog20220602045413/ （訳注：原稿よりURL更新。。2026年05月01日時点）

[41] インド固有識別番号庁。『myAadhaar　全てのオンラインサービスを扱う1つのポータル（myAadhaar One portal for all online services）』、ウェブサイト、 https://www.uidai.gov.in/en/16-english-uk/aapka-aadhaar/1035-view-all-services.html.

「これが監視の構造を、一元型から分散型へと変えている。そのため、このようなデータにアクセスできるエンティティは、公的組織（社会保障スキームのプロバイダなど– Nayak、『この特別な問題（this Special Issue）』を参照）– であれ、民間組織であれ、監視権限を有することができる。さらに、Shakthi（『この特別な問題（this Special Issue）』）が強調するように、プラットフォーム所有者、ひいては監視ツールは、それ自体が私的領域へと分散されるようになった。これが、重要なデータへのアクセスとその所有権、両方に基づく新たなタイプの監視という概念を生んでいる」 - Frank Hersey, Biometric Update[42][1]

いかなるプライバシー関連の懸念にもかかわらず、Aadhaarは多くの国から手本となる導入モデルとみなされ、これが「手軽なAadhaar」であるモジュール型オープンソース識別プラットフォーム（Modular Open-Source Identification Platform：MOSIP）を開発する取り組みへとつながった[43]。MOSIPは無料のオープンソースシステムで、アフリカで採用が広がりつつある。各国が政府発行のデジタル資格情報とアイデンティティサービスのモデルとしてこれを選択していることから、プライバシーの考慮に関わるものを含め、Aadhaarシステムの長所と短所の両方が広まる可能性が高い。

3.2.3 イタリアのパブリックデジタルアイデンティティシステム

イタリアでは、政府が10年近くにわたり、政府発行のデジタル資格情報に取り組んできた。この取り組みは、同国のデジタルトランスフォーメーションに向けた大規模な取り組みの一環である。市民と行政を中心に設計された最初の公的システムがSistema Pubblico di Identità Digitale（SPID）、英語にするとパブリックデジタルアイデンティティシステムである。このシステムは2014年10月に構築され、2016年に運用が開始された[44]。同時期に、電子身分証明書（CIE）も、SPIDで用いるのと同じ技術を利用して、そのデジタルアイデンティティシステムの運用を開始した。SPIDもCIE も、eIDAS規則（規則(EU) No. 910/2014）に従った、欧州でも受け入れられるデジタルアイデンティティツールである。Security Assertion Markup Language version 2 （SAML2）をベースとし、SPIDもCIEも、公共サービスと民間サービス、両方に政府の検証を受けたアイデンティティを市民が利用することを可能にする。新たなプロトコルが新たな機能を提供するなど、このシステムは進化を続けており、OpenID Connect （OIDC）をベースとした2代目のシステムが試験段階にあり、2023年中旬にはフル稼働に移行する見通しであ

[42] Masiero, SilviaおよびS. Shakthi。『Aadhaarに対処する：生体認証および社会的アイデンティティ、インドの現状（Grappling with Aadhaar: Biometrics, Social Identity and the Indian State）』。South Asia Multidisciplinary Academic Journal, no. 23（2020年9月15日）。https://doi.org/10.4000/samaj.6279.

[43] Hersey, Frank。『成熟中のMOSIPが、パートナーシップとベンダ群の拡大に伴い高まるID4Africaへの注目を享受（Maturing MOSIP Enjoys ID4Africa Limelight as It Expands Its Partnerships and Vendors Flock）』。Biometric Update、2023年3月23日。2023年4月1日にアクセス。https://www.biometricupdate.com/202206/maturing-mosip-enjoys-id4africa-limelight-as-it-expands-its-partnerships-and-vendors-flock.

[44] Agenzia per L’Italia Digitale。『SPID – パブリックデジタルアイデンティティシステム|Agenzia per l’Italia Digitale（SPID - Public Digital Identity System|Agenzia per l’Italia Digitale）』。2023年4月1日にアクセス。https://www.agid.gov.it/en/platforms/spid.

る。この新たなシステムは、関連するEU規則全てに確実に準拠するよう定期的に点検されている。

プライバシーの観点から、これらサービスを管理する組織（SPID はデジタルイタリア庁（Agency for Digital Italy：AGID)、CIEは内務省）は、このシステムでの資格情報の利用を求める全てのサービスを点検するとともに、行政・技術的な使用開始手続きで、行政・技術・セキュリティ要件を評価している。サービスはプライバシー関連法令を遵守しなければならない。受け取れるのは、要求された属性に関する証明情報に限られ、資格情報そのものは受け取らない。これらは本人の明示的同意がある場合に限り提供される。

EU域内の手本となるシステムであるが、これらデジタル資格情報の1つを有しているのは、成人住民の半数強にすぎない[45]。

3.2.4 ナイジェリアのeID

ナイジェリアの政府発行資格情報プログラムはアフリカ最大規模を誇る。当初はスマートカードに焦点を合わせていた同国のモバイルIDプログラムは現在、トライアル段階にある。国家ID管理委員会（National Identity Management Commission：NIMC）が取りまとめるこのプロジェクトの最大の目的は「安全で統合された中央アイデンティティデータベースにデータを取り込むことである[46]」ナイジェリアには法的なID記録がほとんどなく、権威あるソースの確立は必要な第一歩となる。とはいえ、ナイジェリア連邦政府は安全なバーチャル資格情報を発行する意向であり、この資格情報は期限付きで、また特定の加盟店や検証者のためにアイデンティティ保有者が発行することになる。

これと並行して、ナイジェリアはナイジェリアデータ保護法案でもかなり前進をしており、同法案はナイジェリア連邦行政評議会（Nigeria Federal Executive Council：FEC）で可決され、2023年2月に国民議会（National Assembly）に送られた[47]。このデータ保護法案は、2019年に成立した現行のナイジェリアデータ保護規則より、強固なデータ保護の法的フレームワークを提供すると予想される[48]。

ナイジェリアは、世界銀行に触発され、ナイジェリア人があらゆるrelying party（RP）

---

[45] Mascellino, Alessandro。『イタリアの国民デジタルIDスキームのユーザーが3,000万人の大台に（Italian National Digital ID Scheme Reaches 30 Million Users Milestone）』。Biometric Update、2022年5月9日。https://www.biometricupdate.com/202205/italian-national-digital-id-scheme-reaches-30-million-users-milestone.

[46] Secure Identity Alliance.『世界中のデジタルアイデンティティに発言の場を与える（Giving Voice to Digital Identities Worldwide）』。2021年2月18日、https://secureidentityalliance.org/utilities/news-en/entry/giving-voice-to-digital-identities-worldwide-1-1の72ページを参照。

[47] ナイジェリアデータ保護局。『FECがNASSへの転送に関するナイジェリアデータ保護法案を可決（FEC approves Nigeria data protection bill for transmission to NASS）』。2023年2月25日。https://ndpb.gov.ng/Home/NewsDetails/20 （訳注：2026年05月01日時点はリンク切れ）。

[48] Aliu, PatienceおよびNkechi Udeze。『ナイジェリア：ナイジェリアデータ保護法案（2022年）の主な変更点の概要（Nigeria: An Overview of Key Changes in the Nigeria Data Protection Bill 2022）』。Mondaq。2023年2月22日。https://www.mondaq.com/nigeria/privacy-protection/1283496/an-overview-of-key-changes-in-the-nigeria-data-protection-bill-2022.

にユーザー同意トークンを発行してから、ID保有者のPIIを要求できるようにすることを目的に、本格的なユーザー同意管理システムも2021年に実装した。そのため、このイニシアチブは、ID保有者が自分の実際の国民識別番号（NIN）を共有する必要がなくなり、その代わりに、「一度限りの」同意をRPに行い、NIMCからRPに付与されるアクセス権で制限されるPIIの要求をできるようになることを意味する[49]。

eIDプログラムの資金の調達先はさまざまであるが、その多くはナイジェリア国外である。欧州投資銀行（EUの融資部門）に加え、世界銀行も同国のデジタルアイデンティティ（eID）インフラの整備とナイジェリアの全市民への 生体認証アイデンティティの付与を支援してきた[50]。

3.2.5 シンガポールのSingpass

シンガポールのデジタルアイデンティティシステムはSingpassと呼ばれる[51]。このシステムには約700の組織が参加し、450万人の登録ユーザーに対して2,000を超えるサービスを提供している[52]。Singpassはモバイルアプリへの依存度が高く、全手続の85%が同アプリ経由で行われている。Singpassが提供するサービスは、以下などである。

- 「Myinfo」：オンライン手続のデジタル申請フォームの自動入力（事前入力）をサポートし、その他のあらゆるSingpassサービスの権威あるソースの役割を担う。
- 生体認証ベースのアイデンティティ検証のための「Verify」：QRコードをスキャンすることで、居住者が安全な対面でのアイデンティティ検証とデータ共有をすることを可能にする。
- 「Face Verification」：顔の生体認証データと、政府保有のデータを比較する基本的な認証サービス。および「Sign」：文書にデジタル署名をする。

世界銀行とシンガポールの政府技術庁（Government Technology Agency）が実施したケーススタディの結果から、対象となる住民の97%がSingpassを利用してオンラインサービスにアクセスしていることがわかった[53]。SingpassのMyinfoサービスを利用する組織

---

[49] NIMC Data Privacy Knowledgebase： https://kb.nimc.gov.ng （訳注：2026年05月01日時点はリンク切れ）

[50] Privacy International。『EUおよび移動抑制の外面化、IDシステム：ここから「今何が起きていて、何を変える必要があるのか」がみえてくる（The EU, the Externalisation of Migration Control, and ID Systems: Here's What's Happening and What Needs to Change）』。2021年10月15日。https://privacyinternational.org/long-read/4651/eu-externalisation-migration-control-and-id-systems-heres-whats-happening-and-what.

[51] シンガポール政府。『Singpass – あなたのデジタルIDの向上（Singpass - Your Improved Digital ID）』。2023年4月1日にアクセス。https://www.singpass.gov.sg/main/.

[52] シンガポール政府スマートネーションデジタル政府オフィス（SNDGO）。『Singpass　シンガポールの国民デジタルアイデンティティ（ファクトシート）Singpass Singapore's National Digital Identity (Factsheet)』。2023年4月1日にアクセス。https://www.smartnation.gov.sg/media-hub/press-releases/singpass-factsheet-02032022.　（訳注：2026年05月01日時点はリンク切れ）

[53] 世界銀行、国際復興開発銀行。『シンガポールの国民デジタルアイデンティティおよび政府データ共有：SingpassとAPEXのケーススタディ（National Digital Identity and Government Data Sharing in Singapore: A Case Study of Singpass and APEX）』、

は、「ユーザーの申請時間が平均で80%短縮された」と報告し、企業も「データ品質の向上と、顧客獲得プロセスにおける大幅なコスト削減により、支持率が15%も上昇した」と報告している[54]。サービスは、そのユーザーが本人であることを確信することができ、ユーザーはサービスへのタイムリーなアクセスの便利さを享受している。

Singpassは、ソースコードを公開し、かつ、オープン開発のOpenID Connectプロトコルを使用することで、このシステムにある程度の透明性を持たせている[55]。

Singpassエコシステムの侵害に関する報告はほとんどない。政府はVerifiable Credentialベースのアイデンティティウォレットという形での分散型サービスの開発を検討しているが、トランザクションごとに検証するシステムの多くは依然として、中央集約型データベースへの照会（問い合わせ）に依存している[56]。しかも、プライバシー擁護派は相変わらず生体認証データなど重要な個人データが悪用される可能性があることを懸念する。政府機関が当初の目的範囲を超えて生体認証データにアクセスし得るという懸念は、このような行動をシンガポールの公共セクター（ガバナンス）法で認めているため、確かな根拠に基づいたものである（詳しくは後で説明）。

監視と同意を得ないでの個人データの政府機関間利用に関する懸念は、全ての政府発行のデジタル資格情報に共通するテーマである。分散型モデルの出現に伴い、シンガポールなどの国が、プライバシーの懸念への対処や、政府システムのトランザクション負荷軽減、シンガポールの市民や居住者、企業による国境を超えた利用の増加を目指して、このモデルに移行するか否かを見守ることは興味深いであろう。

3.2.6 米国の州の実装状況

米国連邦政府は現時点で、汎用のデジタル資格情報を発行しておらず、また連邦レベルの一般的なプライバシー法もない[57]。米国連邦政府は国境をまたいだ旅行向けの電子パスポートを発給してはいるが、先に述べたように、このデジタル資格情報には暗号学的に検証可能なアイデンティティ情報が含まれているものの、選別的情報開示に対

2022年。pp. xiv. https://www.developer.tech.gov.sg/assets/files/GovTech%20World%20Bank%20NDI%20APEX%20report.pdf.

[54] 世界銀行、国際復興開発銀行。『シンガポールの国民デジタルアイデンティティおよび政府データ共有：SingpassとAPEXのケーススタディ（National Digital Identity and Government Data Sharing in Singapore: A Case Study of Singpass and APEX）』、2022年。46ページ。https://www.developer.tech.gov.sg/assets/files/GovTech%20World%20Bank%20NDI%20APEX%20report.pdf.

[55] Singpassの技術アーキテクチャとOIDCの利用に関して詳しくは、シンガポール政府。ログイン：より高度な保証での既存Singpassユーザーの認証とオンボーディング（Login: Authenticate and onboard existing Singpass users with higher assurance）。Singpass API Overview。最終更新日：2023年4月26日を参照。https://api.singpass.gov.sg/library/login/developers/overview-at-a-glance を参照。

[56] Hersey, Frank。『Singpassはデジタル身分証明書を搭載して、オンボーディング当たり36ドルを節約し、分散化を検討（Singpass Incorporates Digital Identity Card, Saves $36 per Onboarding, Considers Decentralization）』。Biometric Update |、2022年9月9日。2023年4月1日にアクセス。 https://www.biometricupdate.com/202207/singpass-incorporates-digital-identity-card-saves-36-per-onboarding-considers-decentralization。

[57] 米国政府によるデジタル資格情報発行が進んでいる点に留意されたい。米国内務省安全保障科学技術局（Security Science and Technology Directorate）局。『ニュースリリース：DHSがデジタル資格情報の検証に181,000ドルを拠出 | 国土安全保障（News Release: DHS Awards $181K to Verify Digital Credentials | Homeland Security）』、2019年11月14日。https://www.dhs.gov/science-and-technology/news/2019/11/14/news-release-dhs-awards-181k-verify-digital-credentialsを参照。

応していない。また、改ざん（写真のモーフィングなど）されやすい写真（生体認証データ）を含み、自動顔認識に必要な質を備えていないことが多い。一方、米国の州はモバイル運転免許証（mDL）という形で、政府発行のデジタル資格情報の発行を開始した。米国では国民身分証明書（すなわち国民ID）がないことから、他国では国民IDの用途となっているものの多くで、運転免許証が利用されている。電子パスポート規格と同様、モバイル運転免許証規格（SO/IEC 18013-Xシリーズ）も国際標準化機構が開発した。同シリーズについては、後で詳しく説明する。

州レベルでのmDLの実装状況には、「実装していない」から「現在稼働中」までとばらつきがあり、これが米国の実情の考察を特に複雑にしている。本書では、実情の多様性の一部を反映した3つの事例（Appleウォレットでの取り組みを試験的に実施し、その後、対象を拡大してGoogleも含めたメリーランド州と、そのmDLが米国運輸保安局（Transportation Security Administration：TSA）から州として初めて承認されたアリゾナ州、自州向けに開発された規格に準拠したアプリを使って稼働させたユタ州）に着目する。本書で精査する全ての州で、mDLのユースケースは、物理的免許証が使えるあらゆる場面で利用するためのものである。これら資格情報をオンライン取引で利用できるようにしている組織があるとしても、これらの州はその情報を公表してこなかった。

米国とカナダで政府発行のデジタル資格情報の実装を先導しているのは、米国自動車管理者協会（American Association of Motor Vehicle Administrators：AAMVA）と呼ばれる組織である[58]。AAMVAのmDL合同小委員会（Joint mDL Subcommittee）（AAMVAのカード設計規格小委員会と電子アイデンティティ小委員会で構成）の作業を通じて、AAMVAはこの地域のmDLの相互運用性の実現に不可欠な実装ガイドラインを策定した[59]。

mDLを法的（基本的）アイデンティティの代わりに利用して、その他のアイデンティティが取得されることもあることから、自動車管理者が必要不可欠なアイデンティティレゾリューションを実施して（一意性の確立）、自動認識に必要な十分な質を備えた生体認証データを含む、必要不可欠な、暗号学的に検証可能なアイデンティティ情報 を提供することが欠かせない。自撮りをし、その写真を政府発行の文書（物理的またはデジタル）と比較する能力は、リファレンスデータの正確性と真正性 - 権威あるソースに依存する。

残念ながら、しかし驚くべきことではないが、犯罪者はすでにこれらの新しい資格情報を悪用した不正の手口を見つけつつある[60]。

[58] AAMVA。『ホーム -米国自動車管理者協会 – AAMVA 』、2023年4月1日にアクセス。https://www.aamva.org/.

[59] 米国自動車管理者協会 – AAMVA。『運転免許証』。2023年4月1日にアクセス。https://www.aamva.org/topics/mobile-driver-license#?wst=4a3b89462cc2cff2cbe0c7accde57421

[60] McConvey, Joel R。『生体認証データ不正利用と偽モバイル運転免許証が銀行を直撃（Banks Hit with Biometric Fraud, Fake Mobile Driver’s Licenses）』。Biometric Update、2023年3月20日。 https://www.biometricupdate.com/202303/banks-hit-with-biometric-fraud-fake-mobile-drivers-licenses.

3.2.6.1 メリーランド州

メリーランド州は2022年にスマートフォンユーザーへのmDLの提供を開始した[6160]。この資格情報は、自分の物理的な運転免許証の表面と裏面の写真と、自分のショート動画を撮影して作成してから、発行当局に送り検証をしてもらう。情報の検証が終わると、本人はGoogleやAppleのウォレットにそれを追加し、承認された場合、利用が認められている場所では物理的な資格情報の代わりに利用できる。このパターンは、他州と共通する。

メリーランド州は、プライバシーに焦点を当てた法律（個人情報保護法（PIPA））がある州の1つでもある[62]。ただ、同法は消費者のユースケースに焦点を当てており、mDLの利用に明確に対応しているわけではない。その代わりに、メリーランド州運輸省自動車管理局（MDOT MVA ）には、mDL保有者向けの 利用規約合意書（Terms and Conditions agreement）がある。これには、デジタルウォレットプロバイダとMDOT MVAの間でいつ、どのように情報が共有されるかが記載されている。その一方で、「MDOT MVAは、デジタルウォレットプロバイダが保有する可能性のあるあなたの情報のプライバシーとセキュリティを管理せず、その管理はデジタルウォレットプロバイダから通知されるプライバシーポリシーに準拠する」という免責条項も盛り込まれている[63]。

3.2.6.2 アリゾナ州

アリゾナ州は2022年初旬に初のAppleウォレットへの mDL実装を行い、稼働を開始した。これらmDLの保有者は、物理的な運転免許証が利用できる場面であれば、どこでもこの新しい資格情報を利用できた。加えて、これら資格情報はフェニックス・スカイハーバー国際空港のTSA指定の保安検査場でも利用でき、連邦の仕組みとの重要な接点となっている[64]。

アリゾナ州はデジタルプライバシー法を備えた米国州の1つではない。その代わりに、ウェブサイトに掲載した一般的なプライバシーポリシーステートメントに依拠している[65]。mDLの新たなリリースでは、プライバシーの考慮を概ねAppleの手に委ね、同社が広報、展開、端末サポートを引き続き管理している。 これが、プライバシー擁護派の懸念を招いているが、現時点でこれら懸念は新たな法律に反映されていない[66]。

---

[61] Pascale, Jordan。『メリーランドがIPhoneで運転免許証のデジタル版をスタート（Maryland Launches Digital Version Of Driver's License On IPhone）』。DCist。2022年5月26日。 https://dcist.com/story/22/05/26/maryland-digital-drivers-license/.

[62] メリーランド州議会。『個人情報保護法（PIPA）、Md. Code Ann. Comm. Law 14-3504（The Personal Information Protection Act (PIPA), Md. Code Ann. Comm. Law 14-3504）』、2019年4月30日。 http://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gcl§ion=14- 3504&enactments=False&archived=False.

[63] メリーランド州運輸省自動車管理局。『モバイル運転免許証（MDL）規約（Mobile Driver's License (MDL) Terms and Conditions）』、2022年4月12日。https://mva.maryland.gov/Documents/mDL-Terms-and-Conditions.pdf.

[64] アリゾナ州運輸省。『アリゾナ州民が国内で初めてAppleウォレットに運転免許証を追加| ADOT（Arizonans Are First in the Nation to Add Driver Licenses to Apple Wallet | ADOT）』。2022年3月23日。https://azdot.gov/adot-news/arizonans-are-first-nation-add-driver-licenses-apple-wallet.

[65] アリゾナ州。『プライバシーポリシー（Privacy Policy）』。2023年4月1日にアクセス。https://az.gov/policy/privacy.

[66] MacDonald-Evoy, Jerod。『アリゾナのApple運転免許証がプライバシーに対する懸念を引き起こす（Digital Driver's License in Arizona Raise Privacy Concerns』。AZ Mirror、2022年3月25日。 https://www.azmirror.com/2022/03/25/apple-digital-drivers-license-in-arizona-raise-privacy-concerns/.

3.2.6.3 ユタ州

ユタ州が米国で初めてmDLを発行した州であることはほぼ間違いない。その実装では、GoogleやAppleと提携するのではなく、第三者であるGET Group North AmericaとモバイルデジタルIDベンダのScytálesと連携することを選んだ[66][67]。ただ、デュープロセス面の課題がいくつかあり、実装の道のりは決して平たんなものではなかった。同州のモバイル運転免許証について定める当初の法案の修正（S.B. 88）に関する2021年の審議が、この技術と、それが自分の生活に及ぼす影響に懸念を持つ人々の反発や不安の的となった[68]。（修正案を撤回した）その議論の結果、以下のような文言を含め、提案されていた追加のプライバシー保護の一部は実現せず、事実上失われた。

> *(4) 同部（division）は、電子ライセンス証明書または電子身分証明書に利用されるシステムおよび技術が確実に、*
>
> > *(i) ライセンス証明書または身分証明書を有する個人と同じように、当該個人のデータセキュリティとプライバシーを維持し、*
> >
> > *(ii) デジタルトラッキング、ジオトラッキング、それ以外の方法でのデバイスやエンドユーザーからの情報収集ができないようにするものとする[69][68]*

新たな法律が導入されるかどうあるかは不透明である。ユタ州に加え、米国のそれ以外の州の状況は急速に変化している。

3.2.6.4 その他の州および米国のプロジェクト

ミズーリやテネシー、ミシシッピなどその他の州は異なるアプローチをとっている[70]。さらに、mDLを支えるだけでなく、AAMVAはアメリカン航空が発行するものなど、派生デジタル資格情報の代替形態も間接的に支える[71]。アメリカン航空のデジタル資格

---

[67] Nash, Jim。『ユタとアリゾナではモバイル運転免許証を信用組合のトランザクションに利用（Mobile Driving Licenses Live in Utah, Arizona for Credit Union Transaction）』。Biometric Update、2022年8月11日。https://www.biometricupdate.com/202208/mobile-driving-licenses-live-in-utah-arizona-for-credit-union-transactions.

[68] Beal-Cvetko, Bridger。『コロナと国際連合に関するデマは、ユタ州議会議事堂のトレンドか？（Is Misinformation about COVID, United Nations a Trend at Utah Capitol?）』。Deseret News、2022年3月11日。https://www.deseret.com/utah/2022/2/8/22923842/misinformation-conspiracy-theories-utah-legislature-united-nations-salt-lake-city-digital-ids.

[69] ユタ州法。『S.B. 88デジタル運転免許証修正（S.B. 88 Digital Driver License Amendments）』、2022年3月4日。https://le.utah.gov/~2022/bills/static/SB0088.html.

[70] その他の州の活動については、Thales Group。『デジタル運転免許証 - スマートフォンの中のあなたのID（Digital Driver's License - Your ID in Your Smartphone）』、2021年4月7日。2023年8月24日にアクセス。（訳注：2026年05月01日時点はリンク切れ） https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/driving-licence/digital-driver-licenseを参照。

[71] 『アメリカン航空がTSA PreCheck®でモバイルIDの提供を開始（American Airlines Launches Mobile ID with TSA PreCheck®）』、日付不明。https://news.aa.com/news/news-details/2022/American-Airlines-Launches-Mobile-ID-With-TSA-PreCheck-OPS-OTH-06/default.aspx.

情報はAAMVAのDVLAサービスを発行プロセスの一部として活用しており、この航空会社のサービスは、空港の保安検査を通過する用途についてTSAにより利用が認められている。

3.2.7 サマリ

IDシステム	アイデンティティ数	対応サービス	第三者が利用可能	セキュリティ侵害の影響を受けたアイデンティティの報告	プライバシーの考慮
EU eIDAS 2.0	（未定）	開発中。eIDASの参考となるユースケースは以下など：一般的なオンラインサービス、モビリティ・デジタル運転免許証、医療・教育用資格情報・職業資格、デジタルファイナンス・デジタルトラベル用資格情報[72]	はい	該当なし	
インドのAadhaar	13億5,900万（総人口の最大88%）	給付金の支給・ソーシャルサービス、キャッシュレス決済（ユニバーサル決済インターフェースを参照）	はい	さまざまな侵害で10億超の記録が流出する恐れがある[73]	インド最高裁判所が、以下を指摘[74][73] ・固有識別番号庁（UIDAI）は取引の目的や場所、詳細を収集していない。 ・収集される情報は、プライバシー権と、食料・住まい・雇用などの基本的なサービスを受ける権利との間で、合理的な均衡が図られている。 ・銀行口座の開設にAadhaar識別番号の提示を義務づけることはできない（ただし、一部の政府サービスでは義務づけることができる）
イタリアの	3,300万	2022年11月	はい	該当なし	このサービスは全ての該当する

[72] 『欧州デジタルアイデンティティウォレットのアーキテクチャとリファレンスフレームワーク（European Digital Identity Wallet Architecture and Reference Framework）』。https://digital- strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework.

[73] 世界経済フォーラム。『グローバルリスクレポート2019（The Global Risks Report 2019）』、2019年1月15日。https://www.weforum.org/publications/the-global-risks-report-2019/（訳注：原稿よりURL更新。。2026年05月01日時点）

[74] Doshi, Menaka。『Aadhaar：最高裁判所の過半数の命令の簡単な概要（Aadhaar: A Quick Summary Of The Supreme Court Majority Order）』。BQ Prime、2018年9月27日。https://www.bqprime.com/aadhaar/aadhaar-a-quick-summary-of-the-supreme-court-majority-order.

IDシステム	アイデンティティ数	対応サービス	第三者が利用可能	セキュリティ侵害の影響を受けたアイデンティティの報告	プライバシーの考慮
SPID	（成人人口の63%）	2022年10月時点で12,000超の行政機関が1以上のオンラインサービスをSPIDで提供。2022年10月時点で民間企業141社がSPIDに加入[75]。			EU・国内法令（GDPR、NIS2、eIDAS2.0など）に準拠。
ナイジェリアのeID	5,400万（対象居住者の最大40%）	銀行・金融サービス、投票、年金、医療給付、運転免許証、税金など向け	はい	データが限定的。 政府システムのデータ侵害は報告されているが、それがeIDサービスに関係しているかは不明	これらの資格情報を利用するサービスは、現行のナイジェリア・データ保護規則、および（成立した場合）将来のナイジェリア・データ保護法案に準拠することが求められる。
シンガポールのSingpass	420万（対象居住者の97%）	700を超える政府機関と企業の2,000のサービス	はい	1,500	Singpassの顔検証技術は特定目的に必要なデータしか集めない。 顔認識に必要な写真は政府のサーバに30日間保持される。 顔画像を政府の生体認証データベースに照らして検証した時には合致率のみを第三者（すなわちプライベートセクター）と共有。
米国の州	不明	モバイル運転免許証	はい	該当なし	プライバシーへのアプローチは州により異なり、現時点で米国には一貫したパターンがない。

[75] Tosques, Lara。『イタリアにおけるデジタルアイデンティティの実装状況　2022年（State of Play on Adoption of Digital Identity in Italy 2022）』。Namirial.Com、2022年12月1日。https://www.namirial.com/en/news/digital-identity-state-of-play-italy-end-of-2022/.

3.3 技術的な多様性と能力

政府などのエンティティがどのようにデジタル資格情報を発行し、その後、当該データをどのように利用できるかに対する保護の1つのレベルが規則で定められるなか、個人のプライバシーと政府が発行・管理するデータのセキュリティを支える技術は、それ自体が固有の脅威と機会ももたらし得る。技術に関わる最大の課題の1つは、技術自体はニュートラルであり、「良い」か「悪い」かは、その利用法で決まるという考えである。例えば、生体認証はシステムとサービスへの安全で簡単なアクセスを可能にするかもしれないが、同時に非倫理的なトラッキングも可能にし得る。取引の基本的な記録（ログ）は、システムの安全性と説明責任を支える一方で、利用者のウェブ上の行動を関連付けて推測する目的にも使われ得る。さらに重要なのは、同意を要件にすることで本人が自分で判断できるようになる点である。もっとも、目先の利便性を優先して同意が十分に読まれないことも多い[76]。ある状況で合理的で適切なことが、別の状況では有害で不必要かもしれない。技術はその判断をすることができない。同意バナーでそのギャップを埋めようとしても、結果として利用者が表示を無視しやすい利用体験を生みがちである。

それでも、規制による統制への信頼と、可能な限り下位層にプライバシー保護を組み込むことの間には隔たりがあり、技術で補える余地は残っているかもしれない。政府は技術に依存してデジタルトランスフォーメーションの約束を支えると同時に、住民を守っている。そのため、何が可能で、より多くの取り組みが必要なのはどこかを完全に把握する上では、何ができ、何ができないかを考えることが不可欠である。

[76] Solove, Daniel。『不正な同意取得：同意のでっち上げに対するプライバシー法のアプローチ（Murky Consent: An Approach to the Fictions of Consent in Privacy Law）』。TeachPrivacy、2023年1月23日。https://teachprivacy.com/murky-consent-an-approach-to-the-fictions-of-consent-in-privacy-law/.

インターネットプロトコルでのプライバシーの考慮 （RFC 6973）

数多のインターネットの標準やベストプラクティスを定めてきたIETF（Internet Engineering Task Force）は2013年に、ユーザーのプライバシーが影響を受ける可能性があるRFCにおけるプライバシー考慮事項セクションをいつ、どのように作成するかに関するガイダンスを策定した。このRFCは最終的に「インターネットプロトコルの設計者と実装者、ユーザーにプライバシーに関係する設計の選択肢を認識させることを目指す。」

その発行以来、明確なプライバシー考慮事項セクションが盛り込まれたRFCは（RFC 6973以降に発行された2500近くのうち）101になる。加えて、7つのRFC（1つはそのうちの別のRFCの最新版）が特定プロトコルのプライバシー考慮のみに関するものである（『DNSのプライバシーの考慮事項（DNS Privacy Considerations）』（RFCs 7626および9076）および『IPv6アドレス生成メカニズムのセキュリティとプライバシーの考慮事項（Security and Privacy Considerations for IPv6 Address Generation Mechanisms）』（RFC 7721）、『DHCPのプライバシーの考慮事項（Privacy Considerations for DHCP）』（RFC 7819）、『DHCPv6のプライバシーの考慮事項（Privacy Considerations for DHCPv6）』（RFC 7824）、『IPv6適応層メカニズムのプライバシーの考慮事項（Privacy Considerations for IPv6 Adaptation-Layer Mechanisms）』（RFC 8065）、『IPブロードキャストまたはマルチキャストに依存するプロトコルのプライバシーの考慮事項（Privacy Considerations for Protocols Relying on IP Broadcast or Multicast）』（RFC 8386）を参照。

この種の標準化されたガイダンスは、仕様書作成者に自らが定義している技術についてもっと広い視野で考えることを促すのに有益な要素である。このガイダンスは、OpenID FoundationやOASISなど、他の標準化団体も利用してきた。だが、これは必須とされたり、一貫して使われたりしてきたわけではなく、また、仕様書作成者が常に、自らの仕様がプライバシーに及ぼす影響を最もよく理解し、文書化する個人であるとはかぎらない。

3.3.1 デジタル資格情報を支える技術

政府発行のデジタル資格情報の発行と利用の一環として、個人のプライバシーを確保し、高めるには、法律と技術を組み合わせて活用する必要がある。このセクションでは、現在のこれら資格情報向けで、現在利用されている、または検討されている代表的な技術を概観する。

3.3.1.1 デジタルウォレット

最もシンプルな形のデジタルウォレットは、デジタル資格情報を格納する、デバイスのアプリケーションである。スマートフォンを持つ個人にはおなじみの存在となってきており、人は交通カードや航空券、ポイントカードなどを格納する。一方、アイデンティティウォレットの要件は、他のユースケースより強固である。アイデンティティウォレットは、個人がどのような個人データを、要求するサービスに提供したいと思うかを選択する手助けをすることを目的としたものであり、この選択には、そのサービスとウォレットの両方が共に対応するプロトコルを用いた取引への同意も含まれる。ウォレットは、さまざまな資格情報をホスティングすることを目的としており、複数のユースケースに対処しているため、複数の形式の資格情報に対応する必要性が、インターネット接続の有無に関係なく、ユーザーが属性を提出する必要性とともに高まっている。プライバシーの観点から言うと、デジタル資格情報の格納方法はさておき、デジタルウォレットは、いかにプライバシーを強化する安全な方法でデジタルウォレットにデジタル資格情報を入れ、それから出すかで重要な役割を担う。

OpenID for Verifiable Credential仕様は、あらゆる形式（IETF SD-JWT、ISO/IEC 18013-5など）のデジタル資格情報の発行と提示、およびエンドユーザーから検証者への仮名による認証を含むプロトコルを定義する[77]。ISOコミュニティは発行と信頼、プロビジョニングに関するいくつかの基本的事項を定義することを目的としたISO/IEC 23220（個人識別のカードとセキュリティデバイス - モバイルデバイスを通じたアイデンティティ管理の構成要素）シリーズに取り組んでいる[78]。ISO/IEC 23220シリーズの一部草案文書は、OpenID for Verifiable Credential仕様のプロファイルを定義する[79]。共通のパターン（発行、提示など）に対応する必要があることから、ウォレットの標準化の必要性が示唆される。さらに、ウォレットのバックアップと復元をどのような仕組みにするか、ウォレットのユーザーエクスペリエンスに加え、ユーザーとrelying partyが取引の決済に利用することを望むのはどのウォレットと資格情報かをどのようにすれば

[77] OpenID Foundation。『OpenID for Verifiable Credentials - 仕様』。2023年7月25日。https://openid.net/sg/openid4vc/specifications/。このウェブサイトには全てのOpenID for Verifiable Credentials仕様の実装者の草案とエディターの草案、ワーキンググループの草案が掲載されている。

[78] ISO/IEC 23220-1:2023。個人識別のカードとセキュリティデバイス - モバイルデバイスを通じたアイデンティティ管理の構成要素（Cards and security devices for personal identification — Building blocks for identity management via mobile devices）— 第1部：モバイルeID システムの一般的システムアーキテクチャ（Part 1: Generic system architectures of mobile eID systems）。ISO/IEC JTC 1/SC 17。スイス・ジュネーブ： ISO、2023年2月発行。 https://www.iso.org/standard/74910.html.

[79] OpenID Foundation。『デジタル資格情報プロトコル（DCP）ワーキンググループ』。2023年8月18日。https://openid.net/wg/digital-credentials-protocols/。このウェブサイトにはISO/IEC TS 23220-4およびISO/IEC TS 18013-7、ISO/IEC TS 23220-3におけるOpenID for Verifiable Credential仕様への参照が掲載されているが、いずれも最終的なISO仕様ではない。

ブラウザやデジタルアプリは知ることができるかなど、その周辺の考慮事項にも対象範囲が拡大されるかもしれない。
ウォレットの開発は、公共セクターでも、民間セクターでも行われている。先に述べたように、eIDAS 2.0は欧州デジタルアイデンティティウォレットの全加盟国への普及を試みており、2023/2024年度には最初の試験的実装が実施される。全てのニーズに応えるため、EUの規制当局は複数の形式の資格情報に対応するEUデジタルIDウォレットの設計を進めている。この設計は、さまざまな標準をベースとし、幅広いユースケースに対応したものになる。
Linux Foundationが2022年9月に発表し、2023年2月にスタートしたOpen Wallet Foundationは、「発行者とウォレットプロバイダ、relying partyが利用して自力で実装することができる、標準ベースのOSSコンポーネントでの連携を通じた、ユーザーの選択肢とセキュリティ、プライバシーを守るデジタルウォレット技術のベストプラクティス」に焦点を当てている[80]。

3.3.1.2 SAML2

当初OASISが2001年に発行し、2005年に大規模な改正（SAML2）を発行したAssertion Markup Language（SAML）標準は、アイデンティティプロバイダ（IdP）とサービスプロバイダ（SP）間の認証データと認可データの転送に関する標準である[81]。このプロトコルはブラウザでのクロスドメイン・シングルサインオン（SSO）を実現するために設計された。SAML2は今でも、教育や政府などいくつかのセクターで広く利用されている。だが、積極的な開発は2012年前後に終了した。

SAML 2.0仕様から：

> *4.5 SAMLにおけるプライバシー*
>
> *情報技術の文脈では、プライバシーとは一般的に、自分のアイデンティティデータがどのように共有・利用されるかを制御するユーザーの能力と、複数のサービスプロバイダでのユーザーのアクションが不適切に相互関連づけされることを防ぐメカニズムの両方を意味する。*
>
> *SAMLは、このようなプライバシー要件に責任を負わなければならないというシナリオで採用されることが多い（また、その他の手段や階層を通じて適切な保護が実現されているという前提で、このようなプライバシーに明確に対処する必要がないというシナリオで採用されることも多い）。*
>
> *SAMLにはプライバシーに配慮した導入を支援する仕組みを支えるメカニズムが数多くある。*
>
> - *SAMLは、IdPとSPの間で仮名を設定する仕組みに対応してい*

[80] 『OpenWallet Foundation – Linux Foundation プロジェクト（OpenWallet Foundation – Linux Foundation Project）』。2023年4月1日にアクセス。https://openwallet.foundation/.
[81] OASIS Security Services (SAML) Technical Committee。『SAML V2.0標準（SAML V2.0 Standard）』。FrontPage - SAML Wiki、2020年6月26日。https://wiki.oasis-open.org/security/FrontPage.

る。このような仮名自体が、（IdPがユーザーについて同一の識別子（いわゆるグローバル識別子）をあらゆるSPに提示／送信した場合には可能になると思われる）サービスプロバイダ間の不適切な関連づけを可能にすることはない。

- *SAMLはワンタイムまたは一時的な識別子に対応している - このような識別子は、特定のユーザーがアイデンティティプロバイダから一回のサインオン操作で、あるサービスプロバイダにアクセスする都度、そのサービスプロバイダが、前回訪れた同じ個人であると認識できないようにする（その識別子のみに基づき、SAML以外のハンドルを通じれば関連づけが可能かもしれない）。*
- *SAMLの認証コンテキスト（Authentication Context）メカニズムは、十分な（だが、必要以上ではない）保証レベルで、ユーザーがあるサービスプロバイダでアクセスしようとしているリソースに適した人物であると、そのユーザーを認証することを可能にする。*
- *SAMLは、特定の操作（連携する行為など）にユーザーが同意したという主張を、プロバイダ間で伝達することを可能にする。その同意をいつ、どこで、どのように取得したかはSAMLの適用範囲に入っていない。*

今でも世界各地で利用されているSAML2にはかなりの制限がある。例えば、SAMLはeXtensible Markup Language（XML）で表現されているため、XMLで表現されるため、モバイル環境ではXMLパーサ等の都合で対応が難しい場合が多いXMLで表現されるため、モバイル環境ではXMLパーサ等の都合で対応が難しい場合が多い。また、ユーザーの同意を、完全にプロトコル外で処理しなければならないことを考えると、SAMLはモバイル用途に必ずしも適した方式ではない。SAMLでの国境を超えた検証も、属性や形式、基盤となるポリシー要件に関わる標準化の欠如を踏まえると難しい。SAML2は、その複雑性を完全に理解した上で、十分に注意を払い、別のメカニズムと併用すれば、プライバシーを守るオンライン環境で利用できるが、簡単ではない。

3.3.1.3 OAuth2

IETF（Internet Engineering Task Force）はネットワークをまたいだビットのトランスポートから、アプリケーションレベルの相互運用性まで、ネットワークスタックのあらゆる階層のインターネット技術標準を策定している。認証・認可領域では、その標準が、アプリケーション層にとどまらない方向性を示す。とはいえ、デジタル資格情報領域では、OAuthの文書群のそれがアプリケーションレベルの認証と認可の最も影響力のある標準群となっている。

OAuth仕様の関係のマッピングは本書の対象範囲外であるが、それが政府発行のデジタル資格情報にどのような影響を及ぼすかと、プライバシーに及ぼす影響全体を理解す

ることは本書の対象範囲内である。

OAuth 2.0仕様は、モバイルデバイスのアプリケーションなどのクライアントが、サービスプロバイダ（政府機関のサービスポータルなど）のユーザーリソースへのアクセスをどのように確保するかを定義する。OAuth 2.0はアイデンティティを直接扱っていないが、デジタルアイデンティティのアクションの実施に必要な強力な基盤となる。OAuth仕様の中核を成す委任認可フレームワークとAPI はモバイルデバイスでの認証と認可への対応に不可欠である。

> *「モバイル環境でSAMLは申し分のない標準とは言えない。モバイルプラットフォームにXMLパーサーが組み込まれておらず、暗号要件も厳格であった。その結果、アクセス管理のパラダイムとなったのが、連携プロトコルと層を成すことができる（layer with）『委任認可フレームワーク』のOAuth 1.0である。OAuthはユーザーを（本人確認として）提示しない形でアクセストークンを用い、ユーザーに代わって限定された範囲のデータやサービスへアクセスする、という形を扱う」– Pamela Dingle、『アイデンティティ入門 - 第2部：アクセス管理（Introduction to Identity - Part 2: Access Managemen）』*[82]

OAuth 2.0仕様群はよく練られたものであるが、固定化されていない。個々人が、IETFのOAuthワーキンググループを通じて、新たな機能の提案と標準化や、既存の仕様の改良を続けている[83]。

OAuth2を実装する個人にとって最大の課題はおそらく、異なる仕様全てをどのようにお互いに関連させるか、そして、ある特定の状況でどの仕様を用いるべきかを把握することであろう。開発者は仕様の一部だけを実装して、セキュリティのためのトークン署名や、ユーザー情報の要求の効率化を目的としたJSON Web Tokens（JWT）の正しい利用などの要素を抜かしてしまうかもしれない。OAuth2準拠の認定（適合性評価・認証制度）の仕組みはない。ウェブ上にガイダンスがあるが、どのようなルールに従うべきかを知ることは常に難しい。

OAuth2は技術的には認証プロトコルではなく認可プロトコルである。しかし認証と密接に結びついて使われることが多いため、OAuth2の適用範囲に認証まで含まれると誤解する開発者も多い[84]。実際の認証プロトコルについては、一連のOpenID Connect（OIDC）仕様に目を向けるべきである。

3.3.1.4 Verifiable Credential

Verifiable Credentialという概念は広く浸透しており、最も基本的には「何らかの方法で検証可能なデジタル資格情報」である。政府や組織がW3C Verifiable Credentials（VC）

[82] Dingle, Pamela。『アイデンティティ入門 - 第2部：アクセス管理（Introduction to Identity - Part 2: Access Management）』。IDPro Body of Knowledge 1, no. 2。2020年6月18日。https://doi.org/10.55621/idpro.45.
[83] IETF。『ウェブ認可プロトコル（Oauth）（Web Authorization Protocol (Oauth)）』。2023年4月1日にアクセス。https://datatracker.ietf.org/wg/oauth/documents/.
[84] Richer, Justin。『OAuth 2.0でのエンドユーザー認証（End User Authentication with OAuth 2.0）』。2023年4月1日にアクセス。 https://oauth.net/articles/authentication/.

を指しているのか、あるいは別の（独自仕様の可能性もある）検証可能な資格情報を指しているのかは、実装ごとに調査する必要がある。

World Wide Webコンソーシアム（W3C）で標準化されたVCに着目すると、VCは、政府がデジタル資格情報を発行することを、主要な動機となるユースケースの1つとして設計された[85]。仕様の用語集に従うと、「Verifiable Credentialとは、誰が発行したかを暗号的に証明する、一連の改ざん検知策を施したクレームとメタデータ」を意味する。

中核的なVC仕様のプライバシー考慮事項セクションは広範に及ぶ[86]。そこでは、プライバシーは二値的な概念ではないこと、また政府発行の識別子は相関付けされやすいことが指摘されている。

3.3.1.5 ブロックチェーンに限定されてはいないが、ブロックチェーン技術を検討する

国々の中には、サービス提供にVCを活用している例がある。欧州委員会と欧州ブロックチェーンパートナーシップのイニシアチブであるEBSI（European Blockchain Services Infrastructure）W3CおよびEBSIの標準に従ってVerifiable Credentialsがどのように機能するかを理解するため、Verifiable Credentialsのライフサイクルへの対応を求めた[87]。

3.3.1.6 ISO/IEC 18013-5:2021 個人識別 — ISO準拠の運転免許証 — 第5部： モバイル運転免許証（mDL）アプリケーション

国際的に、最もローカルな管轄に至るまで運転免許証が受け入れられていることにより、運転免許証は世界各地で有力な身分証明手段となっている。
このようなレベルの相互運用性の原動力となっているのは標準化である。カード型の運転免許証はすでに国際規格に従っている前提とされているため、モバイル運転免許証（mDLs）にも、同様の相互運用性が求められる。それを受けて、運転免許証のISO/IEC 18013規格群の適用範囲が拡大され、「ISO/IEC 18013-5 -2021 – 個人識別 - ISO準拠の運転免許証 - 第5部：モバイル運転免許証（mDL）アプリケーション」にモバイル運転免許証資格情報が盛り込まれた[88]。

この規格の要旨に従うと：

> *本書はモバイルデバイスに関連した運転免許証の実装に関するインターフェース仕様を定める。本書はmDLとmDLリーダの間のインターフェース、およびmDLリーダと発行当局のインフラの間のインターフェースについて規定する。本書はまた、発行当局以外の当事者（他の発行当局や、他国のmDL 検証者など）が、以下を行うことを可能にする。*
> *— 機械を利用してmDLデータを取得すること*

[85] Sporny, Manu、Dave LongleyおよびDavid Chadwick。『Verifiable Credentialデータモデルv1.1』、W3C Recommendation。2022年3月3日。https://www.w3.org/TR/2022/REC-vc-data-model-20220303/.
[86] Sporny, Manu、Dave LongleyおよびDavid Chadwick。『Verifiable Credentialデータモデルv1.1』、2022年3月3日。https://www.w3.org/TR/vc-data-model. セクション7「プライバシーの考慮（Privacy Considerations）」を参照。
[87] 欧州委員会EBSI（European Blockchain Services Infrastructure）。『サクセスストーリー』。2023年4月1日にアクセス。https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Verifiable+Credentials+Success+Stories.
[88]

— *mDLをmDL保有者に紐づけること*
— *mDLデータの出自（発行元）の真正性を確認すること*
— *mDLデータの完全性を検証すること*

以下の項目は本書の対象範囲外となる。

— *mDL保有者の情報共有への同意をどのように取得するか*
— *mDLデータとmDLプライベートキーの保存要件*

ISO/IEC 18013-5は、中核的なISO/IECプライバシー原則を念頭に設計された（ISO/IEC 29100:2011を参照）[89]。この原則は、同意と選択、目的の特定と保持、データ最小化、収集の制限、正確性と品質、開放性、透明性、個人参加、説明責任とプライバシー順守、情報セキュリティが含まれる[9089]。

そのため、mDLに向けた動きは世界各地で政府発行のデジタル資格情報の範囲と利用、プライバシーに対する期待に影響を及ぼす可能性が高い。

資格情報の対面での提示に対応した、発行済みのISO/IEC 18013-5を補完するため、18013-7が間もなく後に続き、資格情報のオンライン提示をカバーする。今後は、18013-4でプロビジョニング規格、18013-6で認定規格も仕様群も検討対象とされている。全体的に見て、ISO mDL規格は幅広い機能（接続モードと非接続モード、両方での対面での検証、オンライン認証など）をカバーすることになり、エンドユーザーによる自分のデータの制御を維持しながら、新たなユースケースの扉を開けることができる。

ISO/IEC 18013-5の適用範囲はmDLに限定されているが、通信プロトコルとデータエンコーディング、セキュリティメカニズム、データプライバシー・最小化要件についての詳細度は、マルチプル資格情報ウォレットアプローチで、アイデンティティや医療資格情報など別の種類のデジタル資格情報に適用でき、また利益をもたらすことができる。

[89] ISO/IEC 29100:201。https://www.iso.org/standard/45123.html.　（訳注：2026年05月01日時点はISO/IEC 29100:2024に更新 https://www.iso.org/standard/85938.html）

[90] Kelts, David。『モバイルID普及の成否は市民のプライバシー保護に大きく左右される（Successful Adoption of Mobile ID Hinges Largely on Protection of Citizen Privacy）』。International Association of Privacy Professionals、2022年3月1日。https://iapp.org/news/a/successful-adoption-of-mobile-id-hinges-largely-on-protection-of-citizen-privacy/.

モバイル資格情報のプライバシーを強化するモデルを開発する

Kantara Initiative（カンターライニシアチブ）のPEMC WG（Privacy Enhancing Mobile Credentials Work Group）は、各ステークホルダーがその準拠を証明できるような、発行者と検証者、プロバイダ向けの一連のプライバシー要件の策定に取り組んでいる。このPEMC WGのプロセスの中心に据えられているのは、資格情報を保有する個人のプライバシーに対する合理的な期待を確実に満たすという目標である。下の「信頼のトライアングル」はエコシステムの主要ステークホルダーを表す。各交点で、ステークホルダーは個人である場合も、組織である場合もあり、またさまざまな標準を適用できるが、この非中央集権型モデルでも、求められるプライバシー要件は概ね共通である。

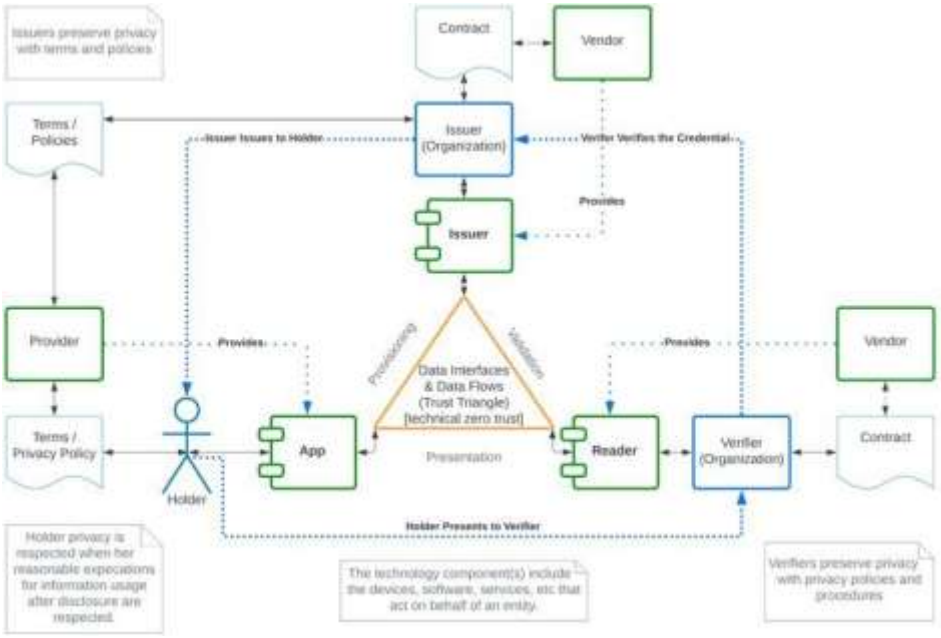

図2：PEMCの「信頼のトライアングル」モデル

現在「早期実装者のガイダンス（Early Implementor's Guidance）」レポートの取りまとめが進められており、関係者はPEMC WGに加わることが推奨される。PEMCワーキンググループは今後も引き続き詳細な要件、ひいては準拠プロセスの定義を進める。この作業により、主要な第一歩となる、市場参加者が共通のプライバシーガイドラインの順守状況を自己認証する合理的な基盤を築くことができる。

だが、これは長い取り組みの始まりにすぎない。現在はこれらガイドラインの順守を義務づけるポリシーや、順守を大規模に自動化するメカニズム（監査人による実施状況の手作業によるチェック対プロトコルで可能な自動テストスイートなど）がないため、期待される影響には限界がある。

3.3.1.7 OpenID for Verifiable Credentials

OpenID for Verifiable Credentials（OpenID4VC）仕様群は、認証およびVerifiable Credentialの発行・提示を可能にする標準仕様群である[91]。OpenID4VCは、EU Digital Identity WalletのArchitecture and Reference Frameworkにおいて認知され、採用が進みつつある。また、米国NIST（NCCoE）によるmdocsおよびmDLの参照実装においても、採用が進められている。OpenID4VCは、さまざまな導入モデルとセキュリティ水準に対応できるよう設計されている。

OpenID4VCは、個人が自分のデータに対する主体性を持ち、「いつ」「どの情報」を共有するかという重要な決定について、より強いコントロールを維持できるべきだという原則に基づいて設計されている。

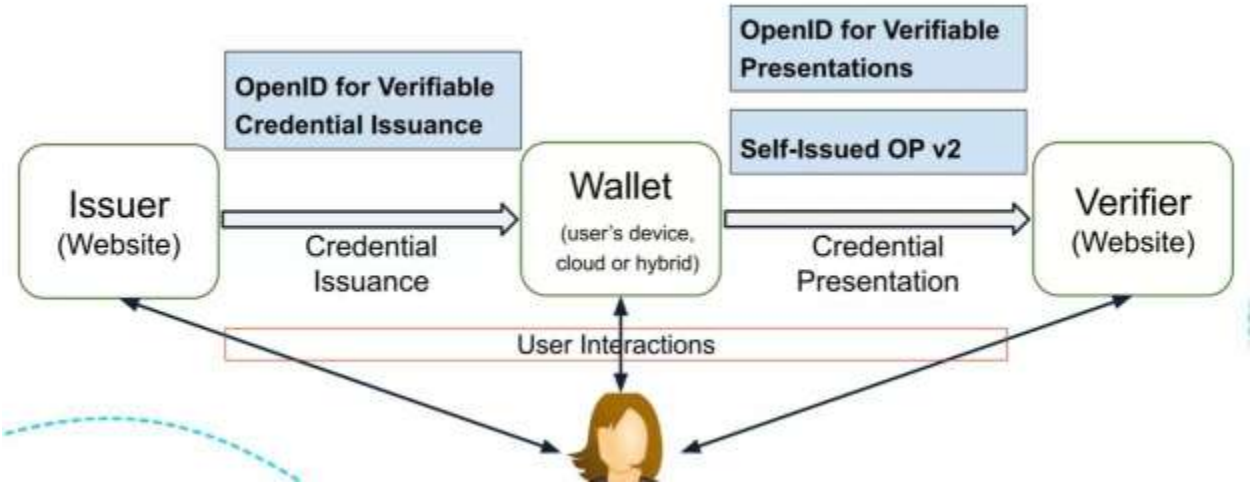

図3：分散型アイデンティティ認証パターンをOpenID4VCに合わせる[92] [91]

OpenID Foundationにおける中核仕様は次の3つである。

- OpenID for Verifiable Credential Issuance – Verifiable Credential発行のAPIと、対応するOAuthベースの認可メカニズムを定義。
- OpenID for Verifiable Presentations – OAuth 2.0の上に築かれた仕組みにより、プロトコルフローの一部として、Verifiable Credentialの形でクレームを提示する。
- Self-Issued OpenID Provider v2 – エンドユーザーが自ら制御するOpenID Provider（OP）を利用できるようにする。

ISO/IECでは、OpenID for Verifiable Credential IssuanceとOpenID for Verifiable

[91] OpenID Foundation。『OpenID for Verifiable Credentials - OpenID Foundation』。 OpenID Foundation。2023年5月5日。https://openid.net/sg/openid4vc/.

[92] Yasuda, Kristina（Microsoft）およびTorsten Lodderstedt。日付不明。『OpenID for Verifiable Credentialsで相互運用可能な分散型アイデンティティシステムを構築するには（How to Build Interoperable Decentralized Identity Systems with OpenID for Verifiable Credentials）』。スライドショー。https://www.slideshare.net/slideshow/how-to-build-interoperable-decentralized-identity-systems-with-openid-for-verifiable-credentials-258329870/258329870.（訳注：原稿よりURL更新。。2026年05月01日時点）

Presentationsの具体的なプロファイルを策定する作業が進行中である[93]。

ワーキンググループが以下などの追加の仕様を策定しており、この仕様群は拡大している。

- OpenID for Verifiable Presentations over BLE – BLE（Bluetooth Low Energy）を用いてVerifiable Credentialの提示を要求できる。OID4VPで定義されたリクエスト／レスポンスの構文を用いる。
- OpenID Connect UserInfo Verifiable Credentials - OpenID Connect UserInfo Endpointからその時点で提供されているユーザー属性をVerifiable Credentialとして発行することを可能にする。

セクション3.3.1.1「デジタルウォレット」で述べるOpenID for Verifiable Credentials の策定作業は、OpenID FoundationのDigital Credential Protocols Working Groupで進められており、実装者の草案とエディターの草案、ワーキンググループの全てのドラフトのリストが公開されている[94]。

3.3.2 生体認証を支える標準

本書に記載するデジタル資格情報は全て、生体認証を何らかの形で利用しており、交換やプライバシー、プロファイルなどに対処する関係標準は多い。ここでは政府発行のデジタル資格情報に焦点を当てる。政府発行の資格情報は、状況に応じた／機能的なアイデンティティを確立するための、法的または基盤的なアイデンティティとして用いられることが多い。そのため、生体情報の真正性と品質を担保することが不可欠である。

- **生体認証の真正性**は発行プロセスに応じて、リスクや保証のレベルが異なり、対面での処理（キャプチャ）が最も低いリスク（最も高い保証度）を生み、遠隔処理が最も高いリスク（最も低い保証度）を生む。
- **生体情報の品質**は、生体照合（マッチング）の性能を予測する指標になり

[93] 以下を参照されたい。ISO/IEC WD TS 23220-4 — 個人識別のカードとセキュリティデバイス - モバイルデバイスを通じたアイデンティティ管理の構成要素（Cards and security devices for personal identification — Building blocks for identity management via mobile devices）— 第4部：運用段階のプロトコルとサービス（Part 4: Protocols and services for operational phase）。ISO/IEC JTC 1/SC 17。スイス・ジュネーブ：ISO、日付不明。2023年8月24日にアクセス。 https://www.iso.org/standard/79126.html（訳注：2026年05月01日時点はISO/IEC TS 23220-4:2026に更新　https://www.iso.org/standard/86785.html）、OID4VPのプロファイルによるmdocsの提示向け、およびISO/IEC CD TS 18013-7 — 個人識別 — ISO準拠の運転免許証 — 第7部：モバイル運転免許証（mDL）のアドオン機能。策定中。ISO/IEC JTC 1/SC 17。スイス・ジュネーブ：ISO、日付不明。2023年8月24日にアクセス。https://www.iso.org/standard/82772.html（訳注：2026年05月01日時点はISO/IEC TS 18013-7:2025に更新 https://www.iso.org/standard/91154.html）、 OID4VPのプロファイルによるmdocsの提示向け、ISO/IEC WD TS 23220-3 — 個人識別のカードとセキュリティデバイス - モバイルデバイスを通じたアイデンティティ管理の構成要素（Cards and security devices for personal identification — Building blocks for identity management via mobile devices） — 第3部：発行段階のプロトコルとサービス。ISO/IEC JTC 1/SC 17。スイス・ジュネーブ：ISO、日付不明。2023年8月24日にアクセス。https://www.iso.org/standard/79125.html mdocsを発行するための OID4VPのプロファイル向け、本レポートの発行時点で、これら仕様は最終的なものではなく、また公開されてもいないことに留意されたい。（訳注：2026年05月01日時点はISO/IEC TS 23220-3に更新　https://www.iso.org/standard/86783.html）

[94] Digital Identity Credentials Protocols Working Group、 https://openid.net/wg/digital-credentials-protocols/およびOpenID for Verifiable Credentials – 仕様、https://openid.net/sg/openid4vc/specifications/.

得ることが示されている。そのため、政府発行のリファレンス生体情報の品質は極めて重要であり、ISO/IEC 19794-Xや39794-X、間もなく発行される29794-Xシリーズなど関係規格は多い。

政府発行のデジタル資格情報に関わる、生体認証の主な用途には、アイデンティティ証明プロセスの一環としての一意性の確立もある。おそらくこの最も良い例は、インドの居住者13億人以上の超について、生体情報に基づく重複排除（デデュプリケーション）を行い、一意のAadhaar番号を割り振ってきたインド固有識別番号庁のAadhaarプログラムである。

プライバシーに配慮した形でデジタル資格情報を利用する方法を示す標準の例として、NIST SP 800-63-3（国家レベルの標準の一例）がある[95]。他にも利用中・策定中の標準は多数あるが、ここでは一部のみを示す。

3.3.2.1 ISO/IEC 27533

現在2 2部構成のこの規格は、モバイルデバイスにおける生体認証の高レベルの要求事項をまとめたものである。第1部は、この規格が「ローカルモード」と呼ぶ、生体認証データと派生認証データがデバイスから出ないモードに焦点を当てている。つまり本規格は、端末外のリモートサービスへのアクセス制御ではなく、デバイスにある生体情報データの保護に焦点を当てている。この規格は2022年11月に承認、発行された[96]。

第2部は策定中であるが、は第1部の続きとして、リモートモード（生体情報または派生生体情報が端末とリモートサービス間で送受信される形態）に焦点を当てている[97]。

ISOには生体認証攻撃と生体認証アルゴリズムのテストにより大きな焦点を当てた規格がほかにもある（生体認証データ提示攻撃の検知に関するISO/IEC 30107シリーズと生体認証性能のテストに関するISO/IEC 19795-1:2021を参照）[98]。これら規格の基準の精査は、政府と企業による生体認証データの安全で公平な利用に大いに役立つかもしれない。

3.3.2.2 NIST SP 800-63-3デジタルアイデンティティガイドライン

---

[95] この領域の興味深い標準のリスクは長くなっており、これがほんの一例であることに留意されたい。

[96] ISO/IEC 27553-1:2022（情報セキュリティおよびサイバーセキュリティ、プライバシー保護 — モバイルデバイスの生体認証データを利用した認証のセキュリティ要件およびプライバシー要件） — 第1部：ローカルモード。ISO/IEC JTC 1/SC 27。スイス・ジュネーブ：ISO、2022年11月発行。https://www.iso.org/standard/71671.html.

[97] ISO/IEC WD 27553-2 I（情報セキュリティおよびサイバーセキュリティ、プライバシー保護 — モバイルデバイスの生体認証データを利用した認証のセキュリティ要件およびプライバシー要件） — 第2部：遠隔モード。ISO/IEC JTC 1/SC 27。策定中。https://www.iso.org/standard/71670.html.

[98] ISO/IEC 30107-1:2016（情報技術 — 生体認証データ提示攻撃検知） — 第1部：フレームワーク。ISO/IEC JTC 1/SC 37。スイス・ジュネーブ：ISO、2016年1月。https://www.iso.org/standard/53227.html（訳注：2026年05月01日時点はISO/IEC 30107-1:2023に更新　https://www.iso.org/standard/83828.html）およびISO/IEC 19795-1:2021（情報技術 — 生体認証性能のテストおよび報告） — 第1部：原則とフレームワーク。ISO/IEC JTC 1/SC 37。スイス・ジュネーブ：ISO、2021年5月。https://www.iso.org/standard/73515.html.

NIST SP 800-63は2004年6月の最初の発行以来、極めて有力な標準であり続けている。その後、このガイドラインは2回の改正を経て、今、3版目（NIST SP 800-63-4）の取りまとめが進められている。このガイドラインの目的は、「資格情報サービスプロバイダ（CSP）にデジタル認証の実装に関する技術ガイドラインを提供する」ことである[99]。政府発行のデジタル資格情報は一般的に、特定のサービスを対象に発行されており、国家レベルのアイデンティティスキームの一部ではない。

このガイドラインは米国政府機関に義務づけられる方向性を示すものであるが、世界各国の政府はその内容が自国デジタル資格情報の発行に有用であると感じている。NIST SP 800-63-3は保証に新たなアプローチをとり、保証レベルを1つに統一するという考え方から脱却し、認証プロセスに伴うリスクのさまざまな要素を考慮に入れた。

> *「このガイドラインは、アイデンティティ保証の個々の要素を別々の構成部分に分けることで生じる認証エラーの悪影響を軽減する対応を示す。非フェデレーテッドシステムの場合、政府機関は2つの構成要素身元保証レベル（Identity Assurance Level（IAL））と「認証保証レベル（Authenticator Assurance Leve（AAL））を選ぶ。フェデレーテッドシステムの場合、政府機関は3番目の構成要素「フェデレーション保証レベル（Federation Assurance Level（FAL））を選ぶ。*

> *このガイドラインは、実装別の要件を推進する、保証レベル（level of assurance（LOA））を1つに統一するという考え方から脱却する。その代わりに、適切なビジネス・プライバシーリスク管理をミッションのニーズと組み合わせることで、政府機関は、はっきりと異なる選択肢としてIALおよびAAL、FALを選択する。多くのシステムはIALおよびAAL、FAL、各々が同じ数値レベルになるだろうが、これは要件ではない。政府機関は、どのシステムでも同じレベルになると思い込んではならない。」 – Paul Grassi、Michael GarciaおよびJames Fenton、NIST SP 800-63-3[100]*

NISTには、顔認識プログラムの正確性評価の一助となる顔認識のアルゴリズムとテストを提供するNIST顔認識ベンダテスト（Facial Recognition Vendor Test：FRVT）プロジェクトもある点に留意されたい[101]。FRVTは標準ではないが、顔認識による生体認証に

[99] Grassi, Paul、Justin Richer、Sarah Squire、James Fenton、Ellen Nadeau、Naomi Lefkovitz、Jamie Danker、Yee-Yin Choong、Kristen GreeneおよびMary Theofanos。『デジタルアイデンティティガイドラインの連携とアサート：連携とアサート（Digital Identity Guidelines Federation and Assertions: Federation and Assertions）』。米国商務省国立標準技術研究所、2017年6月。https://doi.org/10.6028/NIST.SP.800-63c。セクション1「目的」を参照。

[100] Grassi, Paul、Michael GarciaおよびJames Fenton。『デジタルアイデンティティガイドライン』。米国商務省国立標準技術研究所、2017年6月。https://doi.org/10.6028/NIST.SP.800-63-3。エグゼクティブサマリを参照。

[101] 『顔認識ベンダテスト（FRVT）| NIST（Face Recognition Vendor Test (FRVT) | NIST』。米国商務省国立標準技術研究所、2020年11月30日。https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt.

取り組む組織にとって有益なツールとなる。

3.3.3 アイデンティティ保証

政府発行のデジタル資格情報の、おそらくは最も有益な特長は、ある人が主張するアイデンティティが、政府が判断した真のアイデンティティである（その人が本人である）という、当該資格情報がもたらす信用の度合いである。だが、全てのユースケースが同じ保証を必要としているわけではない。そのため、ユースケースを分類し、身元保証の各レベルに到達する方法について指針を示す必要が高まっている。

このセクションでは、政府と組織が、個人のデジタルアイデンティティに関わり必要となる保証の構築の仕方に取り組む一助となる、現在利用されている標準を少し紹介する。これは複雑で、急速に変化する領域であり、（カナダのDIACCやタイのETDA、英国のDIATFなど）これから取り上げる以外の国・地域でも作業が進められている。本書に類似するペーパー『人間中心のデジタルアイデンティティ：官僚向けの入門書（Human Centric Digital Identity: A Primer for Government Officials）』（現在、パブリックコメントを募集中）はより幅広い政府のデジタルアイデンティティ環境に加え、信頼フレームワークと標準の両方をまたいだグローバルな相互運用性の実現に向けた道への対処、そして各国・地域が政府の一元管理モデルやプライベートセクターを活用したモデルをどの程度追求しているかの考察を試みる[102]。

3.3.3.1 NIST SP 800-63A

NIST SP 800-63-3全般について述べてきたが、アイデンティティ保証に関わる特定のNIST標準「NIST SP 800-63A」は光を当てるに値する[103]。NIST刊行物に示されたガイダンスは明確に米国連邦政府機関を対象としている。この標準は、組織と政府の要件や有用性、プライバシーのバランスを取る必要性を認めている。ただし、米国政府規模の組織が直面し得る多様なユースケースに対応しようとした結果、身元保証レベル（IAL）が複数あることに加え、さまざまな認証者保証レベル（NIST SP 800-63B）と、アイデンティティ連携プロセスに伴うリスクを定量化する連携保証レベル（NIST SP 800-63C）（FAL）も併存している。これらの複雑さが、順守を難しくしている。

3.3.3.2 Kantara Initiative（カンターライニシアチブ）のアイデンティティ保証フレームワーク

Kantara Initiativeの目的は技術と標準の技術的架け橋となり、評価プログラムを「電子アイデンティティ証明と資格情報管理サービスの管理と運用、プロビジョニングに適用される厳格度に関心を持ち、かつ、それに依存する幅広い当事者に」提供することである。

その評価プログラムの中核を成すアイデンティティ保証フレームワークは商品とサー

[102] Garber, E.およびHaine, M. (eds)『草案：人間中心のデジタルアイデンティティ：官僚向けの入門書（DRAFT: Human-Centric Digital Identity: a Primer for Government Officials）』 OpenID Foundation、2023年7月7日。2023年8月22日にアクセス。https://openid.net/wp-content/uploads/2023/07/OIDF-Whitepaper_Human-Centric-Digital-Identity_Draft.pdf.

[103] Grassi, Paul、James Fenton、Naomi Lefkovitz、Jamie Danker、Yee-Yin Choong、Kristen GreeneおよびMary Theofanos。『デジタルアイデンティティガイドライン：登録とアイデンティティ証明要件（Digital Identity Guidelines: Enrollment and Identity Proofing Requirements）』。米国商務省国立標準技術研究所、2017年6月。 https://doi.org/10.6028/NIST.SP.800-63a.

ビス向けのISO/IEC 17065適合性評価に強く整合している[104]。米国政府機関もこのプログラムを利用して、NIST SP 800-63-3準拠が認定された企業やプロバイダからの購買判断に役立てている。

3.3.3.3 OpenID Connect for Identity Assurance 1.0

よりコード駆動型の仕様をめざし、OpenID FoundationはOpenID Connect for Identity Assurance標準を2022年に発行した[105]。この仕様はOIDCの拡張版となり、アイデンティティ情報に加え、その情報の検証状況（どの枠組みで検証されたか、検証時にどの証拠を用いたか等）を明示したうえで、身元情報をサービスに提供できるようにする。この仕様は、eIDAS 2.0の一環として開発されている、複数の国民デジタルアイデンティティプログラムで利用されている[106]。

3.3.4 Open Standard Identity APIs（OSIA）

実用的で保守可能なシステムとして機能させるためには、必要な形で技術同士が相互に連携できなければならない。そのためには、技術全体を一貫して扱える枠組みが必要である。そこで登場したのがOSIAである[107]。

2019年に複数の組織が、包摂的で信頼でき、責任ある国民識別システムの開発に取り組み、一連の共通「優れた識別の原則（Principles for Good Identification）」の策定を支えた[108]。

その構想は、各国政府が利用できる指針となる枠組みを作り、包摂的で信頼できるデジタル身元確認と住民登録の仕組みを整備することにより、人々の生活を改善し、社会的・経済的機会へのアクセスを後押しすることである。

原則5「オープンな標準を利用し、ベンダと技術の中立性を確保すること」は、オープンな標準を利用して、効率性・機能性の向上と、IDシステムの進化と経時的な変化への対応を可能にすることの両方を実現させる重要性を明記している。OSIAは、技術やソリューション、アーキテクチャ、ベンダに関係なく、ID管理システムの構成要素間のシームレスな接続性を実現させるオープンな標準インターフェース（API）を提供する。ITU-Tはこの規格の認可を受けているため、ITU-T規格でこれを規範として参照

---

[104] Kantara Initiative Leadership Council。『アイデンティティ保証フレームワーク』。2023年4月1日にアクセス。https://kantara.atlassian.net/wiki/spaces/LC/pages/1737392/Identity+Assurance+Framework.

[105] Lodderstedt, Torsten、D. Fett、M. Haine、K. Lehmann、A. PulidoおよびK. Koiwai。『OpenID Connect for Identity Assurance 1.0』、2022年8月19日。https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html.

[106] Sharif, Amir、Matteo Ranzi、Roberto Carbone、Giada Sciarretta、Francesco Antonio MarinoおよびSilvio Ranise。『EIDAS規則：欧州電子アイデンティティスキームの技術的傾向調査（The EIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes）』。Applied Sciences 12, no. 24（2022年12月10日）： 12679. https://doi.org/10.3390/app122412679.

[107] Secure Identity Alliance。『OSIA』。2023年4月4日にアクセス。https://secureidentityalliance.org/osia.（訳注：2026年05月01日時点はサーバー停止中）

[108] 世界銀行、ID4D。『1. 原則 | 開発用の識別（1. PRINCIPLES | Identification for Development）』。2023年4月4日にアクセス。https://id4d.worldbank.org/guide/1-principles.

できる[109]。

政府発行のデジタル資格情報は、運転免許証であれ、身分証明書であれ、パスポートであれ、市民のウォレットに資格情報を安全に発行する上で必要な、一連の複雑な構成要素の氷山の一角にすぎない。

これら構成要素は全て、市民の個人データ（履歴データや生体認証データ）の収集と、身元の一意性を確保するためのその取扱い、場合によってはその保存を担う。OSIA規格の標準的な国民識別システム構成要素を整理した図を下に示した[110]。

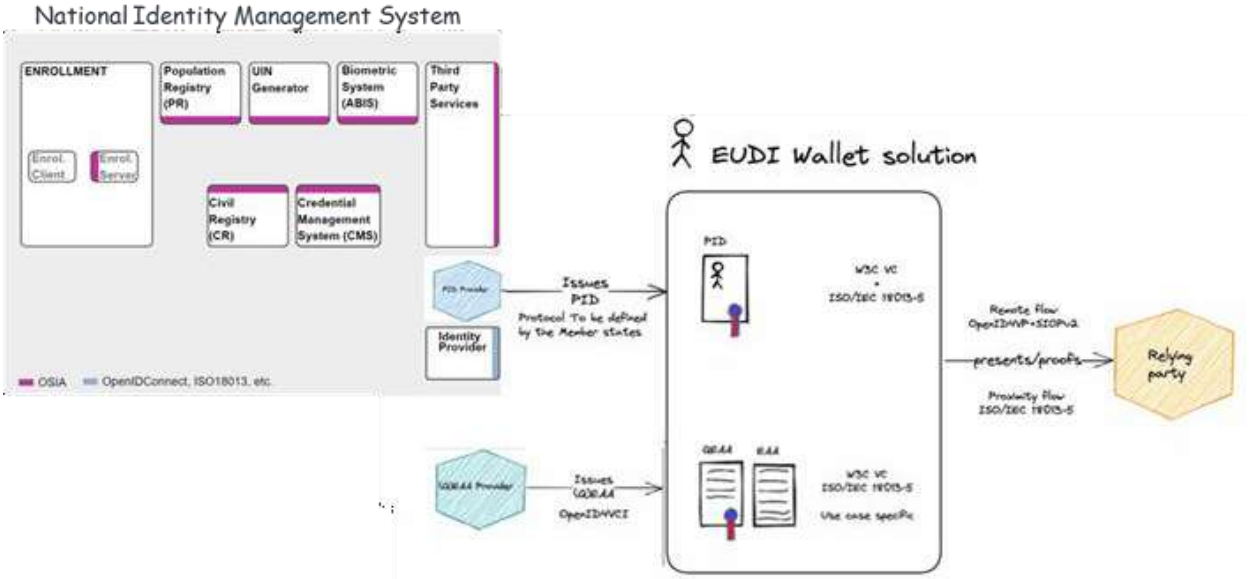

図4 – 国民IDシステムのOSIA構成要素

eIDAS 2.0によれば、国民識別システムはPIDを導出し、デジタルIDウォレットに発行できる信頼の起点（root of trust）となる。現在はPID発行プロトコル用に選定された標準はないが、OSIA規格は、PIDプロバイダが関係するデータベースとシステムと連携して、PIDを収集し、発行手続きを進めるのを支援し得る。

すでに複数の国で実装されているOSIAの適用範囲は以下のとおりである。

1. 国民アイデンティティ管理システムを構成する要素の機能的範囲についての共通理解を形成する

OSIAの最初のステップは、アイデンティティ管理システムを構成する各要素の定義と範囲、主な機能を形式化することである。

[109] Secure Identity Alliance。『Secure Identity Allianceが正規のITU-Tリファレンス組織ステータスを取得 – 重要な資格を得たことでITU-TがOSIA仕様を規範として参照することが可能に（Secure Identity Alliance Awarded Qualified ITU-T Reference Organization Status - Landmark Qualification Enables the ITU-T to Normatively Reference OSIA Specifications）』、2022年11月11日。https://secureidentityalliance.org/news-events/news/secure-identity-alliance-awarded-qualified-itu-t-reference-organization-status.

[110] Secure Identity Alliance。『2.機能図 - OSIA 6.2.0-草案文書（2. Functional View — OSIA 6.2.0-DRAFT Documentation）』。2023年4月4日にアクセス。https://osia.readthedocs.io/en/latest/02%20-%20functional.html.

2. 一連の標準化されたインターフェースを構築する
この中核的な作業でOSIAが焦点を当てているのは、アイデンティティシステムを構成する複数の要素をつなぎ、定義済みのサービスからのシームレスなインタラクションを確保するのに必要な一連のインターフェースの開発である。

4 ギャップとリスク

肯定的な意図からの取り組みであったとしても、デジタルアイデンティティと実世界のアイデンティティの統合から生じるプライバシーリスクの管理に規則と技術は苦労している。規則の場合、相反する運用要件と人間性、技術的限界のバランスを見いだす試みで課題が生じている。技術標準コミュニティでは、いずれかの文化に大きく偏ることなく、本質的には道徳的・倫理的な選択である事柄を技術仕様として定義するのはほぼ不可能である。問題を複雑にしているのは、使うことが求められる（想定される）のかに関する、個人の期待である。

規制と技術の双方に改善の余地はあるが、互いの強みを活かして各自の所掌範囲に内在する限界を補うには、双方がその点を理解している必要がある。

このセクションでは、相反するモチベーションと、政府発行のデジタル資格情報の利用時に、プライバシーを支えるために技術と規則に現実的にできることの限界がもたらすギャップの一部を精査する。

4.1 モチベーションを大きな規模で認識する

政府発行のデジタル資格情報を世界規模で考えるときには、デジタルトランスフォーメーションを望む気持ちは同じである一方で、その気持ちを高める要因は極めて異なることを認識しなければならない。サービスの確立前に考慮に入れられる各要素に置く重きが異なるのは、そのためである。

発展途上国はデジタルアイデンティティと高度なアイデンティティ保証を、住民が経済的機会に参加することを可能にする上で必要な手段（イネーブラー）とみなすことが多い。一方、経済がより強固な国では、デジタルアイデンティティがどちらかというと便利な手段と位置づけられることが多い。その背景には、市民を支えるインフラが非常に奥深く、かつ幅広いため、大規模な技術的強化をせずに（取り組みを進めるには当然のことながら、何らかの強化が必要であったが）、自立してきたことがある。デジタルアイデンティティを「経済的機会のための手段にすぎない」あるいは「現代社会の利便性のためのものにすぎない」とみなす見方は、変化しつつある。その変化をもたらしている要因は、モバイルデバイスの普及とアイデンティティ関連のサイバー犯罪や不正行為の増加により、社会で「オンライン」と「オフライン」の境界線があいまいになってきたことである。

システムのリスクとギャップに対処する取り組みも、その取り組みの原動力に応じて異なってくるため、モチベーションにばらつきがあるという事実は重要な意味を持つ。例えば、主たる原動力が金銭的なものであれば、プライバシーリスクへの対処を経済的便益として掲げなければならず、主たる原動力が利便性であれば、個々のユーザーの期待が体験と需要を呼び起こす。また、いかなる場合においても、規則の要件と技術の能力で何が可能であるかが決まる。

4.1.1 きわめて局所的な期待

政府を動かすモチベーションは、国全体や地域全体ベースで考えられることが多い。とはいえ、これら資格情報を用いる当事者とそれを利用する個人を動かすモチベーションもある。企業と組織だけでなく、個人も、高い価値を持つ、政府が妥当性確認した情報のメリットを、この情報が予想外で、意図せぬ、しかも場合によっては不適切な方法で利用されるリスクと比較して検討しなければならない。

「機微な個人データのキャプチャと保存、利用には、プライバシー侵害とデータの窃取や悪用、アイデンティティの不正利用、差別に伴うリスクが内在する。」 – 世界銀行「開発プログラム用の識別（Identification For Development Program）」[111]

政府発行のデジタル資格情報を利用するトランザクションに関与するあらゆるエンティティが個人のプライバシーに責任を負う場合、そのエンティティはいずれも自らの期待と要件をユーザーエクスペリエンスに反映させる。その結果、個人が表明するプライバシー選好と、個人の実際の情報開示行動との間に矛盾が生じる、いわゆる「プライバシーパラドックス」が起きがちである[112]。

4.2 技術の限界

政府発行のデジタル資格情報はさまざまな技術標準やツールに依存しているが、その採用の領域は、複数のプロトコルが実装されるなど広いと同時に、そのツールを利用できるモバイルプラットフォームが少ないという点で狭い。多くの場合、技術標準は実装の幅が広く、その結果、相互運用性の向上よりも、むしろ混乱を招くおそれがある[113]。全体的に、ツールは複雑で、プライバシーの点で、一部の実装に問題が生じている。

デジタル資格情報を支える技術は、難しいグレーゾーンにある。サービスが、認証中や認可中などにデータを見ることができれば、そのデータを保存し、利用して、場合によっては関連づけるか、あるいは将来的に販売することすらできる。1つのコンポーネントが単独で個人を識別することはできないかもしれないが、複数のシステムのコンポーネントとインタラクションを組み合わせれば、識別できるかもしれない。

このセクションでは、技術自体を通じてこれら資格情報に影響を及ぼすプライバシー関連の問題の一部に着目する。

4.2.1 プロトコルに内在する限界

デジタル環境は技術に左右されるが、法令で全てのユースケースを保護できないのと

[111] 世界銀行ID4D。『実務者ガイド（Practitioner's Guide）』。2023年4月1日にアクセス。https://id4d.worldbank.org/guide/creating-good-id-system-presents-risks-and-challenges-there-are-common-success-factors

[112] Waldman, Ari Ezra、『認知バイアスとダークパターン、「プライバシーパラドックス」（Cognitive Biases, Dark Patterns, and the 'Privacy Paradox）』（2020年）。Articles & Chapters。1332. https://digitalcommons.nyls.edu/fac_articles_chapters/1332

[113] 例えば、『Verifiable Credentials Data Model v1.1』4.7証明（署名）、https://www.w3.org/TR/vc-data-modelの注記を参照。

同様に、技術で全ての課題を解決することはできない。技術は全てのトランザクションを記録、監査、制御しなければならない厳格な規制環境に対応すると同時に、トランザクションを完全に個人の自由裁量に委ねる必要がある消費者環境にも対応しなければならない。オフライン・遠隔シナリオも、リアルタイムでの妥当性確認に依存することができないため難しい。悪意のある者（バッドアクター）に資格情報が不適切に利用されるリスクは技術で軽減できるが、完全に排除することはできない。

4.2.2 生体認証技術

生体認証、特に顔認識は個人とそのデジタル資格情報を照合する手段として人気が高まっている[114]。全てが開発者の予想どおりに機能するとき、個人にとっての利便性は高い。顔認識は、政府が提供している新たなオンラインツールとオンサインサービスを住民が活用する上で最も簡単な方法だと政府が考えることが多く、また所持する資格情報などを本人と強く結びつけることで不正を最大限防ぐ強力な方法でもあると実感している政府は多い。だが、一部システムの正確性には相変わらず問題がある。

生体認証は、その生物学的特性と行動特性に基づく個人の自動認識であり、確率的なものである[115]。全ての生体認証システムはタイプI（誤合致）エラーとタイプII（誤非合致）エラーを起こす。この寄与要因はユースケースや試料の質、環境、人口動態など枚挙にいとまがない。カメラが制約のない環境で、また変な角度で遠距離から作動する、顔認識の内密での非協力的な監視への応用は、主体が制御環境で固定された距離から認識されることをオプトインする出入国eGateとは異なるエラー率をもたらす。例えば、電話アプリなどの検証サービスはいまだに人間の表現型の網羅に苦しんでいる[116]。自撮り写真は厳しい照明条件や魚眼レンズ効果（被写体が近すぎる）、オクルージョン（帽子や暗い眼鏡など）に悩まされることが多く、参照写真は、権威源に基づくものでない場合、照合精度と身元不正利用リスク（例：写真のモーフィング）の双方に影響し得る。

生体認証でシステムに対する認証ができる場合に個人の得られる利便性は大きいが、この技術は大きなプライバシーの懸念を伴う。生体認証データがデバイスから出るというシナリオで、個人の生体認証データの詳細を収集・保存することは、そのデータの安全が適切に守られない場合、大きなプライバシーリスクとなる。その生体認証データが第三者のシステムで、唯一の認証データとして利用され、そのデータをセントラルレポジトリに照らしてチェックし、何らかの方法で個人を承認するか、承認しないかを判断するとしたら、懸念ははるかに大きくなる[117]。

---

[114] Shaheed, Kashif、Aihua Mao、Imran Qureshi、Munish Kumar、Qaisar Abbas、Inam UllahおよびXingming Zhang。『生理学に基づく生体認識システムに関する体系的レビュー：現在と今後のトレンド（A Systematic Review on Physiological-Based Biometric Recognition Systems: Current and Future Trends）』。*Archives of Computational Methods in Engineering* 28, no. 7 (2021): 4917–60. https://doi.org/10.1007/s11831-021-09560-3.

[115] ISO/IEC 2382-37:2022 情報技術 — 用語 — 第37部：生体認証。ISO/IEC JTC 1/SC 37。スイス・ジュネーブ：ISO、2022年3月。https://www.iso.org/standard/73514.html.

[116] Zukarnain, Z.A.; Muneer, A.; Ab Aziz, M.K。モバイルアイデンティティの認証の安全確保手法：問題と解決策、課題（Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges）。Symmetry 2022, 14, 821. https://doi.org/10.3390/sym14040821

[117] Bertocci, Vittorio。『2つの生体認証スタイルの話（A Tale of Two Biometrics Styles）』。Auth0 – ブログ、2023年3月10日。

直接的にはプライバシーの懸念ではないが、生体認証データを変更するにあたっての課題が有用性とセキュリティ関連の懸念を招いている。パスワードは比較的簡単に変更できるが、生体認証データの変更はこれより難しいことが多い。バイオハッシング（biohashing）や取消可能な生体認証（revocable biometrics）といった概念の研究が進められているが、政府がこれらの技法をどの程度利用しているかは不明である[118]。

米国には国家レベルのプライバシー法もなければ、生体認証に特化した国内法もない[119]。 各州が、自州で営業する企業を対象とした独自の法律を制定している。例えば、イリノイ州が当初、2008年に制定した生体認証情報プライバシー法は、生体認証情報の悪用とそれに伴うプライバシーへの影響に関する懸念に焦点を当てている。ただし、同法は州・地方政府とその契約者を対象から除外している。

GDPRのある欧州でさえ、加盟国は生体認証データに異なる保護策を義務づける可能性がある[120]。また、幅広い条項で「国家安全保障」や「防衛」、「治安」上の懸念がある場合には、同意なしに個人データを処理することをEU加盟国に認めているが、これら「国家安全保障」などの用語は、ひいき目に見ても、定義がきちんとなされていない[121]。

結局のところ、生体認証は資格情報と個人を結び付けるために政府に多用されているが、その保護の具体と利用に伴うリスクは大きな懸念である。なお、政府が特定の取引以外の場面で「1対多数」の照合により個人を識別する用途は、本稿の対象外である。

4.2.3 認証と認可のプロトコル

先に指摘したように、デジタル資格情報を発行する政府はSAML、OAuth／OpenID Connect、そしてVerifiable Credentialsといった少数のプロトコル群を重視している。一方、プライバシーへの影響という点で、これらプロトコルは、文書化の仕方だけでなく、プロトコルアーキテクトによる理解のされ方も異なる。

---

https://auth0.com/blog/a-tale-of-two-biometrics-styles/.

[118] 例えば、Prabhu, D、S. Vijay BhanuおよびS. Suthir。『クラウドコンピューティング環境向けの、プライバシーを守るステガノグラフィベースの生体認証システム（Privacy Preserving Steganography Based Biometric Authentication System for Cloud Computing Environment）』。Measurement: Sensors 24 (2022): 100511. https://doi.org/10.1016/j.measen.2022.100511およびLoh, Jia-Chng、Geong-Sen Poh、Jason H. M. Ying、Hoon Wei Lim、Jonathan PanおよびWeiyang Wong。『PBio：生体認証テンプレートの安全な共有を通じて組織をまたいだ生体認証サービスを実現（PBio: Enabling Cross-Organizational Biometric Authentication Service through Secure Sharing of Biometric Templates）』、2020年11月10日。https://eprint.iacr.org/2020/1381を参照。

[119] 米国上院司法委員会では現在、提案がなされているが（2020年8月に提出された「S.4400 – 全国生体認証情報法（2020年）（S.4400 - National Biometric Information Privacy Act of 2020）」）、進展がみられていない点に留意されたい。https://www.congress.gov/bill/116th-congress/senate-bill/4400を参照。

[120] Ross, Danny。『生体認証データを処理する？GDPRに従い、慎重な処理が必要（Processing Biometric Data? Be Careful, under the GDPR）』。International Association of Privacy Professionals、2017年10月13日。 https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/.

[121] Human Rights Watch。『EU一般データ保護規則』、2018年6月6日。https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation.

SAMLは、プライバシーを仕様の、文書化された基本的な部分として設計された。2002年のSAML 1.0の発行以降、この標準はセキュリティとプライバシーに完全に焦点を当てた別途の文書を含んでいた[122]。これが更新され、新たに2つの連続する版「SAML1.1」と「SAML2.0」が発行された[123]。これは、一般的に利用される認証標準のなかで、プライバシーを最も厳格に扱うものの1つである。

IETFで策定されたOAuth仕様群については、RFC 6793「Privacy Considerations for Internet Protocols」に相当する、正式なプライバシー検討（privacy considerations）が欠けている[124]。
それは、当初の中核的な仕様がアイデンティティ情報を全く含んでおらず、委任認可にしか焦点を当てていなかったためかもしれない。もっとも、これらの仕様にはセキュリティ考慮事項が含まれており、セキュリティ上の不備はプライバシー面の影響にもつながり得る。それでも、OAuth 2.0の脅威とセキュリティを扱うRFC 6819でも、プライバシーへの直接の言及は、次の一文を除けばほとんどない。 OAuth 2.0モデルの脅威とセキュリティに特化したRFC（「OAuth 2.0脅威モデルおよびセキュリティ考慮事項（OAuth 2.0 Threat Model and Security Considerations）」（RFC 6819））ですら、「注記：いかなる実装もデバイスの識別子利用によるプライバシーへの潜在的影響を考慮しなければならない」という文言以外に、プライバシーに直接言及していない[125]。

OpenID Foundationで作成した中核的なOpenID仕様は プライバシー考慮事項セクションを含んでいるものの、関係仕様のほとんどはこれを含んでいない（例外は「OpenID 2.0 to OpenID Connect Migration 1.0」）。中核的仕様にプライバシー考慮事項セクションを設けることは、建設的なアクションであるが、強固なプライバシーフレームワークの全ての要素（ファクト）となると、その仕様自体の性質上、いくつかの重要な能力が制約される。。OIDCのトランザクションはポイントインタイムのトランザクションであり、非機能的な要素を仕様に落とし込む能力を制限する。OECDプライバシーガイドラインの原則のうちの2つである同意および選択肢、そしてデータ最小化はある程度含まれているが、目的の正当性や収集制限、利用、保持、開示、正確性および質、個人参加、情報セキュリティなどの他の原則は対象から外れている。これらの項目は、利用時点を別にして、ポリシーなど法的あるいは契約上のフレームワークで記載されることが期待される。

W3Cが定めたVerifiable Credentials仕様も、幅広いプライバシー考慮事項セクションを

---

[122] 『OASIS Security Assertion Markup Language (SAML) のセキュリティとプライバシーの考慮事項（Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML)）』、OASIS、2015年3月15日。https://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf.

[123] F. Hirsch他。OASIS Security Assertion Markup Language (SAML) V2.0のセキュリティとプライバシーの考慮事項（Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0）。OASIS SSTC、2005年3月。文書ID saml-sec-consider-2.0-os。http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf。

[124] Cooper, A.、Tschofenig, H.、Aboba, B.、Peterson, J.、Morris, J.、Hansen, M.およびR. Smith、『Privacy Considerations for Internet Protocols（インターネットプロトコルのプライバシーに関する考慮事項）』、RFC 6973, DOI 10.17487/RFC6973、2013年7月、<https://www.rfc-editor.org/info/rfc6973>.

[125] Lodderstedt, T., Ed.、McGloin, M.およびP. Hunt、『OAuth 2.0脅威モデルおよびセキュリティ考慮事項（OAuth 2.0 Threat Model and Security Considerations）』、 RFC 6819, DOI 10.17487/RFC6819の58ページを参照。2013年1月、<https://www.rfc-editor.org/info/rfc6819>.

含んだ中核的仕様である[126]。この仕様群の比較的新しい仕様として、デジタルウォレットに関するEUの取り組みから特に注目されているが、実装ガイドラインなど関係文書はプライバシーに関するいかなる特別な注記も含んでいない。

4.2.4 Fast IDentity Online (FIDO)

FIDO Allianceとその仕様は認証プロセスで利用できるセキュリティ機能を著しく向上させてきた。これが定めた認証フレームワークとプロトコルは、FIDO Universal Second Factor (FIDO U2F)とFIDO Universal Authentication Framework (FIDO UAF) 、Client to Authenticator Protocols (CTAP)の3つである。CTAPはW3CのWeb Authentication (WebAuthn)仕様を補完するものであり、合わせてFIDO2と呼ばれる[127]。

これらは、認証のセキュリティを向上させており、また生体認証データの取り扱い要件を含んでいる。当該データはユーザーの制御の下、デバイス内に保存しておかなければならず、オンデバイスアプリケーションは各ウェブサイトに一意のキーを提供して、ウェブサイトをまたいだユーザーのトラッキングを防止しなければならない。FIDO2は、プロトコル層でプライバシー機能を組み込む好例である。

FIDO AllianceはFIDO資格情報の利用と実装に焦点を当てた一連のプライバシー原則を発行してきた。これも、標準の策定にどのようにプライバシーの視点を組み込むかを示す、興味深いモデルである[128]。

4.2.5 データを検証する

住民と組織がアイデンティティ情報を信頼できるようにする上で不可欠な要素は、検証済みのクレームである。検証済みクレームは、保証されたアイデンティティ情報を提供する。しかし、その情報をどのように共有するかの詳細は、まだ策定途上である。OpenID Foundation eKYC and Identity Assurance（eKYC & IDA）ワーキンググループは「確認済みのアイデンティティ情報、すなわち検証済のクレームと、その検証の仕方および各々のクレームの維持管理方法に関する情報の通信を標準化する、OpenID Connectの拡張版の策定」に力を入れている[129]。

検証済みのクレームに対応する能力は、特にプライバシーに関係してくる。この能力は、システムに対する十分な信頼を実現させることができ、それにより、その個人についてアサートされていることのクロスチェックをするためにさらに多くの情報を収集する主観的な必要性を軽減することができるはずである。プログラムを通じて情報を検証する能力がなければ、政府発行のデジタル資格情報は、対応することが期待されている多様な用途をうまく満たすことができない。現在検討されている技術は、資

[126] 『Verifiable Credentials Data Model v1.1』、https://www.w3.org/TR/vc-data-model.

[127] FIDO Alliance。『FIDO2 -ユーザー認証仕様の概要（FIDO2 - User Authentication Specifications Overview）』。2023年4月29日にアクセス。https://fidoalliance.org/specifications/.

[128] FIDO Alliance。『プライバシー原則』。2023年5月4日にアクセス。https://fidoalliance.org/fido-authentication/privacy-principles/.

[129] OpenID Foundation。『EKYC & Identity Assurance WG』。2023年4月1日にアクセス。https://openid.net/wg/ekyc-ida/.

格情報にあるデータの、組織による利用の仕方に対処しようとしていない[130]。その代わりに、この技術は組織が必要とする情報を表現することと、データ最小化原則を守ることを可能にすると考えられる。

関連仕様はまだ策定段階にある。仕様が完成して実運用されるまで、この機能は、これら資格情報を支える技術におけるギャップのままである。

4.2.6 技術に関するポリシーを比較する

どのような資格情報を受け入れるかについて、全ての組織のルールが同じわけではない。これは、合法性と同様に、技術の大きな問題となっている。Open Identity Exchange (OIX)は、本格的な信頼フレームワークで、ポリシーから技術まで、どのような点を考慮する必要があるかに焦点を当てている。その1つに、relying partyへの情報の提示時に適用する必要が生じる可能性のあるさまざまな制約にどのように対処するかがある。技術的なポリシーの記述がそれぞれ異なるため、少なくとも現時点では、産業（医療や金融サービス、教育など）と国・地域をまたいだ資格情報の検証と利用ができない。OIXは以下の領域での特定の資格情報機能の標準化で将来これが可能にならないか模索している[131]。

- 資格情報を発行するにあたり、利用者の本人確認（identity proofing）をどのように行うか
- 認証器を利用者にどのようにひも付け（バインド）し、認証器が資格情報を提示する主体として正当であることをどのように保証（主張）するか
- どのようにデータをフォーマットするか

オープンソースポリシーの記述言語はさまざまあるが、1つのエンティティから別のエンティティへのポリシーの記述の伝達を含んだものは1つもない[132]。OpenID Foundation eKYC & IDAワーキンググループの『Advanced Syntax for Claims』草案の執筆者は、RegoやJSONlogic、場合によってはその他を用いて書くことを検討してきたが、いまだに次のステップについて議論している[133]。資格情報の検証は、検証を行うエンティティと、そのエンティティが資格情報のどのような情報を要求しているか、その要求の形式に左右される。現在はそのいずれも、セキュリティとプライバシーの基本的原則に対応した形で共有することができない。

限界の一端は、情報のより詳細な共有と妥当性確認を可能にする高度な暗号アルゴリズムへの依存の高まりにある。選択的開示全般と、特にゼロ知識証明を中心に据えた

---

[130] Fett, Daniel、『OIDC Advanced Syntax for Claims (ASC) - クレームと選択的停止／削除の変化（OIDC Advanced Syntax for Claims (ASC) - Transformed Claims & Selective Abort/Omit）』、プレゼンテーション、2021年5月12日、https://danielfett.de/download/oidc-advanced-syntax-for-claims.pdf

[131] Open Identity Exchange。『OIX -ワーキンググループ』。2023年5月3日にアクセス。https://openidentityexchange.org/workgroups.

[132] De Coi、Juri LucaおよびDaniel Olmedilla。『信頼管理とセキュリティ、プライバシーポリシーの言語のレビュー（A Review of Trust Management, Security and Privacy Policy Languages）』、*Secrypt* (2008): 483-490およびWorld Wide Web コンソーシアム。『PolicyLangReview -ポリシー言語利益団体（PolicyLangReview - Policy Languages Interest Group）』、2009年5月20日。https://www.w3.org/Policy/pling/wiki/PolicyLangReviewを参照。

[133] Haine, Mark。『EKYC & IDA WGレポート』。*OpenID Foundation*。日付不明。 https://openid.net/wordpress-content/uploads/2021/09/OIDF_eKYC-WG-Update_Mark-Haine-Daniel-Fett.pdf.

策定が、プライバシーの強力な可能性をいくつか切り開いてきた。一部のテスト実装で実現されてきたが、これら実装には、新たなアルゴリズムに対応し、かつ数値演算を処理できるだけの強力なデバイスOSとハードウェアが必要となる[134]。

高度な暗号技術を必要としないアプローチもある。IETFのOAuthワーキンググループの草案「Selective Disclosures for JWTs (SD JWTs)」に記載されているハッシュベースのアプローチとISO/IEC 18013-5（モバイル運転免許証）に定義されているmdocsである[135]。 同様に、リンク不可能性（unlinkability）や述語（predicate）は、高度な暗号技術なしに実現できる場合がある。だが、結局のところ、適合性テストや実施、罰則のメカニズムがなければ、ISO/IEC 18013-5の「保持する意図（intent to retain）」のようなメカニズムですら、容易に偽装でき、実際にはデータを保持できてしまう。

4.2.7 データの相関関係と再利用

OECDのプライバシー原則にある利用制限と目的明確化には、サービスは自らが述べる利用目的に必要なデータのみを収集しなければならないと記載されている。このような考え方は、世界の標準や法令の一部に盛り込まれているが、解釈にはギャップがある。個人が自分の政府発行のデジタル資格情報を旅行目的で利用する場合、旅行サービスがその情報を利用して利用者体験をさらに高めることは、不適切なのだろうか。その線引きは常に明確とはかぎらない。常に法律に違反しないようにすることに関心を持つ組織は、プライバシーステートメントやエンドユーザーライセンス契約に、法律で義務づけられていることを記載するが、これらステートメントは難解だとの悪名が高い[136]。個々人は識別や認証、認可を受ける新たな方法に直面して、自分のプライバシーを脅かす新たな脅威にどう対処していいかわからないと感じている。

> *「しかし、空港での生体認証など新興の旅行関連技術には、機微性が極めて高いとされる、顔・網膜画像や指紋、音声認識（すなわち生体認証データ）など新たな種類の情報の収集と利用、保存が必要となる。旅行者が空港での処理を目的とした自分の生体認証データの共有をオプトアウトする選択肢がなかったと感じる場合や、自分の生体認証データの収集・利用前にそれを適切に知らされたり、同意を求められたりしなかったと感じる場合があるかもしれない（Street 2019）。」– Athina Ioannou、Iis P. TussyadiahおよびGraham Miller、Journal of Travel Researc*[137]

---

[134] Bertocci, VittorioおよびDaniel Fett。『プライバシー保護策とSD-JWTに関するDaniel Fett（Daniel Fett on Privacy-Preserving Measures and SD-JWT）』。Auth0、2022年9月29日。https://identityunlocked.auth0.com/public/49/Identity%2C-Unlocked.--bed7fada/3bbcbab8.

[135] Fett, Daniel、Kristina YasudaおよびBrian Campbell。『JWT (SD-JWT)の選択的開示（Selective Disclosure for JWTs (SD-JWT)）』。IETF Datatracker、2023年3月13日。https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/.

[136] Zhang, Yibo、Tawei WangおよびCarol Hsu。『GDPRの自主的実装とプライバシーステートメントの可読性が顧客の情報開示意向と信頼に与える影響（The effects of voluntary GDPR adoption and the readability of privacy statements on customers' information disclosure intention and trust）』。*Journal of Intellectual Capital* 21, no. 2 (2020): 145-163.

[137] Ioannou, Athina、Iis P. TussyadiahおよびGraham Miller。『それはプライベート！旅行者のプライバシー考慮事項とオンラインデータ開示を理解する（That's Private! Understanding Travelers' Privacy Concerns and Online Data Disclosure）』。*Journal of*

Travel Research 60, no. 7（2021年9月1日）：1510–26. https://doi.org/10.1177/0047287520951642.

デジタルアイデンティティ全般と、特に政府発行のデジタル資格情報の領域でみられるギャップの多くと同様、このギャップは技術の限界と現行規則の制約の両方に関連する領域に入る。

4.2.8 デジタル資格情報

デジタルアイデンティティプロトコルに関わる話で（明示されない場合であっても）どの資格情報を使うのか、そこに含まれる個人識別可能なデータの量、そして情報の一部または全部を開示できるかどうかが前提となる。デジタルアイデンティティプロトコルで用いられる資格情報の種類はアイデンティティトークンからW3C Verifiable Credentials、ISO/IEC 18013-5 mdocs、そしてSD-JWT VCまで幅広い。技術上の制約という観点では、各資格情報標準は、その設定次第でプライバシー上の利点にもリスクにもなり得る。

ISO/IEC 18013-5（モバイル運転免許証）は端末登録の選択肢と、プライバシー保護手法に関する実装者向けガイダンスを盛り込んだ附属書が含まれる。だが、端末が登録されず、ガバナンスポリシーがなく、ガバナンスが実施されなければ、資格情報からrelying partyに送られるデータが悪用されるリスクがある。

Trust Over IPはポリシーを用い、技術とポリシーのスタックを一本化して設定の選択肢を狭めることでこの課題への対処を目指している。実装者が全て同じ資格情報の形式とプロトコル、ルールに従えば、システム内やシステム間の相互運用性を実現でき、場合によっては一部のプライバシー面のメリットがシステム内でより偏りなく得られるようになる。

World Wide Web コンソーシアムが作成したVerifiable Credentials Data Model仕様も、包括的なプライバシー考慮事項セクションを含んだ中核的仕様である[138]。この仕様群の比較的新しい仕様として、デジタルウォレットに関するEUの取り組みから特に注目されているが、実装ガイドラインなど関係文書はプライバシーに関するいかなる特別な注記も含んでいない。

OpenID for Verifiable Credentials (OIDC4VC)は仕様群に新たに加わり、OAuthとOpenID Connectをベースとし、Decentralized Identity Foundationの標準を活用してモジュール型アプローチを実装者に提供する。実装者はOIDC4VC の柔軟性を利用して、幅広いユースケースに対処し、また実装間の相互運用性を可能にするプロファイルを開発することができる。例えば、実装者はOIDC4VC内でmdocsを利用するかどうかを選ぶことができ、また開始チャネルと提示チャネルや、ユースケースに最適なのは高信頼プロファイルか低信頼プロファイルかも選ぶことができる。このアプローチは、単一の「スタック」と実装アプローチを提案し、設定の選択肢をより限定するISO/IEC 18013-5（モバイル運転免許証）やTrust Over IPとは異なる。

4.3 規則と標準で見過ごされている保護策

[138] 『Verifiable Credentials Data Model v1.1』、https://www.w3.org/TR/vc-data-model.

政府発行のデジタル資格情報では、プライバシー配慮が民間部門とは異なる基準で扱われがちである。これは理解できると同時に、憂慮すべき問題である。政府の要件と責任は全く異なる。これら資格情報にアイデンティティの高度な妥当性確認と検証が必要である上に、住民のデータのセキュリティ確保が期待されることで、プライバシー保護策の実装には独自の難しさがある。

保護策が法律で定められているものの、政府機関を対象範囲外としている事例に、民間エンティティにしか適用されないイリノイ州生体認証情報プライバシー法（BIPA）がある[139]。州や地方の政府機関や裁判所とそのメンバー（事務官や判事、裁判官など）は含まれていない[140]。対照的に、シンガポールには行政サービスに適用されるセキュリティとプライバシーに関する要件を定めた、幅広い「公共セクター（ガバナンス）法（PSGA）」がある。米国のNIST SP 800-63は中間的な位置づけで、連邦レベルでのみ準拠が義務化されている。一方で、州によってプライバシー法制の作り方や、政府機関に適用するかどうかは大きく異なる。

標準と規制には、対面のオンデバイス要件しか規定していないものもある。先にISO/IEC 18013-5とISO/IEC 27553-2について述べたときに指摘したように、データが保存されているデバイスからそのデータが出る必要が生じる可能性のある遠隔（リモート）シナリオを想定した要件や制約の記述は、まだ草案段階にあるか、検討中である。

4.3.1 インドのデジタル個人データ保護法案（2022年）

インドでオンラインプライバシーに対応した法的取り組みの1つが、インド議会で審議中の新デジタル個人データ保護法案である。議会は2022年8月に前の同法案を撤回しており、これは2度目の取り組みとなる。Aadhaarシステムでは10億人を超える住民に資格情報を提供しており、このシステムなどオンラインサービスから取得された個人データがどのように利用されるかについての懸念には、個人が自らのデータ保護について救済を求められるよう、法的保護によって一部対処する必要がある。

全ての法律は妥協の産物であり、デジタル個人データ保護法案に対しては、プライバシー擁護派がいまだに政府自体からの保護の強化を強く訴えている[141]。政府による監視という問題が大きな懸念点であることに変わりはない[142]。同法案が明確にオフラインデータとペーパーベースのデータの収集を対象から除外していることで、紙の記録

[139] Institute for Legal Reform。『ILR Briefly：不適切な組み合わせ：イリノイ州と生体認証情報プライバシー法- ILR（ILR Briefly: A Bad Match: Illinois and the Biometric Information Privacy Act – ILR）』。ILR、2021年10月21日。 https://instituteforlegalreform.com/research/ilr-briefly-a-bad-match-illinois-and-the-biometric-information-privacy-act/.

[140] 『生体認証情報プライバシー法』。イリノイ州議会、2008年10月3日。 https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.（訳注：2026年05月01日時点はリンク切れ）

[141] Sherman, Justin。『インドの新データ法案はプライバシーの寄せ集め（India's New Data Bill Is a Mixed Bag for Privacy）』。Atlantic Council、2022年11月23日。 https://www.atlanticcouncil.org/blogs/southasiasource/indias-new-data-bill-is-a-mixed-bag-for-privacy/.

[142] Mathi, Sarvesh。『データ保護法案が監視を合法化。政府に改革の意思なし：Stakeholders #NAMA（Data Protection Bill Legitimises Surveillance, Govt Has No Intent of Reforms: Stakeholders #NAMA）』。MediaNama、2022年12月20日。 https://www.medianama.com/2022/12/223-dpdp-bill-2022-enables-govt-surveillance-discussion/.

をデジタル化したデータも保護されるのかといった疑問が残る[143]。

同法案は、他地域のプライバシー法に共通するいくつかの原則と、適法性、公平性、透明性、目的制限、データ最小化、正確性、保存制限、説明責任といった原則（他地域の法制およびOECDプライバシーガイドラインに共通）に基づき設計されている。だが、政府によるモニタリング自体や、デジタル化されたデータの例のグレーゾーンに関しては、これら原則をどのように適用するかが、保護策案には間違いなく欠落している。

4.3.2 シンガポールの個人データ保護法と公共セクター（ガバナンス）法

シンガポールは、政府を対象としたプライバシーとセキュリティの要件をきちんと文書化して明確に定めている数少ない国の1つである。PDPAはプライベートセクターにおけるデータ保護責任の法的フレームワークを定めるのに対して[144]、PSGAは公共セクターを対象とした、それに相当する法的フレームワークである[145]。PDPAが同意に焦点を当て、PSGAがサイバーセキュリティ面に多く触れるなど、制御のレベルが異なる[146]。 別個の法的フレームワークがあることは、シンガポールのプライバシーを取り巻く環境をより透明なものにするという点でプラスとなる一方、公共セクターとプライベートセクターのプライバシー保護に著しい相違が生じているという点でマイナスとなる。

行政サービスによくあることだが、主流となるテーマは監視に関する懸念である[147]。PSGAは、利用の同意、あるいは利用を知らせることすらなくても、政府部局間で幅広くデータを共有することを認めている。どのようなデータが収集されたのか、また政府がそれをどのように利用したのかを、個人が知るための法的手段はないように見受けられる。Singpassが非常に多くのサービスのユビキタスな資格情報の役割を果たしており、収集される可能性のあるデータ量は莫大である。

---

[143] Nandle, Ravin。『インドのデジタル個人データ保護法案（2022年）：前のPDPBの一新となるか（India's Digital Personal Data Protection Bill 2022: Does It Overhaul the Former PDPB?）』International Association of Privacy Professionals、2022年11月22日。https://iapp.org/news/a/indias-digital-personal-data-protection-bill-2022-does-it-overhaul-the-former-pdpb/. s

[144] Lim, Chong Kin。『シンガポール - データ保護概要（Singapore - Data Protection Overview）』、OneTrust DataGuidance、2022年5月。https://www.dataguidance.com/notes/singapore-data-protection-overview.

[145] シンガポール政府スマートネーションデジタル政府オフィス（SNDGO）。『政府の個人保護法と政策』。2023年4月1日にアクセス。https://www.smartnation.gov.sg/about-smart-nation/secure-smart-nation/personal-data-protection-laws-and-policies. （訳注：2026年05月01日時点はリンク切れ）

[146] Singapore Management University Newsroom。『このソーシャルメディアとデータ侵害の時代におけるプライバシーの立ち位置とは（Where Does Privacy Stand in This Age of Social Media and Data Breaches?）』。2019年5月13日。https://news.smu.edu.sg/news/2019/05/13/where-does-privacy-stand-age-social-media-and-data-breaches

[147] Choo, JuliaおよびAnngee Neo。『PAP政府による個人データの利用と悪用（The Use and Abuse of Personal Data by the PAP Government）』。New Naratif、2022年6月7日。https://newnaratif.com/the-use-and-abuse-of-personal-data-by-the-pap-government/.

4.3.3 GDPRとNIS2、eIDAS

GDPRとNIS2、eIDAS 2.0はいずれも個人データに関連するが、プライバシーは、これら規則の指針となる設計上の考慮事項の1つにすぎない。GDPRはEU加盟国の市民と居住者に幅広いプライバシー保護を提供することから、世界のプライバシー関連規則の「ゴールドスタンダード」に挙げられることが多い。一方、NIS2は重要なデジタルインフラのレジリエンス向上により大きな焦点を当てている。NIS2の要件はデータレベルの保護より、システムレベルのセキュリティに重点を置いているため、相反する要件となり、個人データのプライバシーに影響を及ぼすかもしれない[148]。また、デジタルアイデンティティに焦点を当てる規則である電子身分証の新枠組みは、データ主体が管理するデータ共有モデルを構築することで、第三者へのデータ共有に関して一般データ保護規則が課す制約との調整を図っている。

これらなどEU規則がいずれもアイデンティティ領域、そして必然的に政府発行のデジタル資格情報に影響を及ぼすことから、プライバシーを取り巻く環境に矛盾とギャップが生じるリスクが大きい。

技術的視点から、国家ウォレット（national wallet）の重視は、ウォレット自体が単一障害点（Single point of failure）になることを示唆する。何らかの理由でウォレットを利用できない個人は、物理的な運転免許証やパスポートのコピーの共有など、プライバシー強化機能の弱いプロセスに頼らざるを得ないかもしれない。また、ウォレットを載せる技術要件自体は規定されていないため、端末ベンダが政府発行者かrelying party、検証者、そしてもっと言えば個人と並ぶアイデンティティエコシステムを構成するもう1つの要素となっており、実証可能な信頼モデルを設計する際には、この点も考慮に入れなければならない。

4.3.4 米国の連邦・州プライバシー法

米国は包括的な全国規模のプライバシー法がない数少ない国の1つである。その代わりに、医療データや財務データなど特定の情報やセクターを対象とした法律がある。このギャップへの対処に、カリフォルニアやユタ、コロラド、バージニア、コネチカットなどさまざまな州が着手しているが、その取り組みにはまとまりと一貫性がない。IAPP（International Association of Privacy Professionals）はこの複雑な状況の動向把握に関心を持つ個人向けに「U.S. State Privacy Legislation Tracker」を提供している[149]。

---

[148] NIS2とGDPRがお互いにどのように関係し合っているかについて詳しくは、Perray, RomainおよびPilar Arzuaga。『EUと英国全体でサイバーセキュリティを規制する- McDermott Will & Emery（Regulating Cybersecurity across the EU and the UK - McDermott Will & Emery）』。McDermott Will & Emery、2023年1月。https://www.mwe.com/insights/regulating-cybersecurity-across-the-eu-and-the-uk/を参照。

[149] Anokhy Desai。『US State Privacy Legislation Tracker』。IAPP Resource Center、2023年3月31日。International Association of Privacy Professionals。2023年4月1日にアクセス。https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

新たなプライバシーリスクを招いている事例

GDPRに記載されたアクセス権では、EU居住者が主体アクセス要求（SAR）をほとんどの組織に送ることを認めている。これを受けて、これら組織は自らが保有する当該居住者に関する全個人データのコピーを1カ月以内に渡す必要がある。GDPRは、「アクセスを要求するデータ主体の身元を確認（アイデンティティを検証）するためにあらゆる合理的な手段を」用いることができるとしているが、それ以上の規定をしていない（Rec. 64）。GDPRは要求者の身元を確認（アイデンティティを検証）することになる組織に関するさらなるガイダンスを提供していない。実際、GDPRはさらに、SARが提出されている場合、組織は個人の特定に役立つデータをそれ以上収集することができないとしている。

Blackhat USA 2019で紹介された論文では、執筆者のJames PavurとCasey Knerrが、GDPRの「アクセス権」プロセスが、権限のない第三者に機微な情報をさらすことで、いかにデータ窃取を招くおそれがあるかを述べている[149]。

これは、個人のプライバシーを守るために設計された法律がうっかり招いている大きなプライバシーリスクである。[150]

5 将来に向けた拡大についての提言

各国政府は、デジタルトランスフォーメーションが多くの便益をもたらすと謳っている。経済成長から行政サービスの効率性と透明性の向上まで、その理想を実現するには、デジタルトランスフォーメーションをフルスピードで推し進めなければならない。より詳細なレベルでは、質の高い検証済みの資格情報を発行することで、政府は、以下などの魅力的な成果を約束する。

- 個人が自らのデータ開示をコントロールできるようにすること
- 全関係者によるデータ最小化の義務化
- relying partyに説明責任を求める法令
- 取引の監査ログの可能性と権利を主張する能力
- 不正行為の最大限の抑止と、それに伴うコスト削減
- 直接的な政府のユースケース以外の領域への拡張の可能性

これらは目指すに値する目標ではある。しかし、それぞれを切り離して達成することはできず、その実現も決して保証されているわけではない。

これらの目標は、複数のトレードオフの中で成り立っており、そのため政府は、効率化の必要性、変化する人口構成に伴うデジタルサービスへの期待、相反する個人の行

[150] Pavur, JamesおよびCasey Knerr。『GDPArrrrr：プライバシー法を利用してアイデンティティを盗む（GDPArrrrr: Using Privacy Laws to Steal Identities）』。Blackhat USA 2019 Whitepaper、2019年。https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf.

動、そしてプライバシー要求の間で、バランスを取ることに苦慮している[151]。一方、技術の側でも、同じニーズと、プロトコルが支えられることには基本的な限界があるという現実との折り合いをつけようとしている。

その結果、政府とプライベートセクターの両方が、きわめて複雑な環境を管理しようとして、分散型モデルではなく、アイデンティティデータをより中央集中的に保管する方向へ向かっている。

規則はしばしば、同意取得のような対応を求める。その結果、民間部門では、外部の情報源—たとえそれが政府発行のデジタル資格情報やそのウォレットであっても—に依拠するより、サービスを内製化する方が安全な選択肢になりやすい[152]。加えて、組織の垣根を超えた相互運用性に必要な技術標準群と技術仕様群の複雑化自体が、政府を含め、デジタル環境で活動をしようとするあらゆる組織の大きな負担となっている。

規則が複雑な技術的実装を余儀なくし、国境をまたいだ複雑性を招く。その結果、このシステムに対する個人の信頼が低下し、混沌とした状況を利用する悪意のある事業者（バッドアクター）につけいる隙を与えている。どうすれば政府や市民社会、標準化団体、開発者が協力してシステムに秩序をもたらすことができるのか。 要件が複雑すぎるときに、どうすればこのマルチウェイ型信頼モデルのステークホルダーがよりシンプルなソリューションを個人に提供できるのか。このセクションでは、政府や技術者、市民社会のメンバーに向けた、政府発行のデジタル資格情報のプライバシーを取り巻く環境を改善できる方法に関する提言を紹介する。これら提言は、先に述べたこの環境に関する知見に基づいている。

[151] 例えば、国際連合。『2022年電子政府調査：デジタル政府の未来（E-Government Survey 2022: The Future of Digital Government）』。国際連合、2022年。United Nations, 2022. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2022の120ページを参照。

[152] この一般的な例は、フェデレーテッドログイントランザクションのユーザーの同意を登録するため、ウェブベースの認証と認可のフローを仲介することを目指すブラウザベンダの進行中の取り組みである。W3C Federated Identity Community Group で検討中の著作物である、Identity Community Group。World Wide Web Consortium。『フェデレーテッドアイデンティティコミュニティグループ（Federated Identity Community Group）』。2023年4月2日にアクセス。https://www.w3.org/community/fed-id/を参照。

5.1 セキュリティとプライバシーの基本

提言のサマリ：セキュリティとプライバシーの基本	
5.1	政府は、すでに確立され、国際的に認められたプライバシーフレームワークを用いてデジタルアイデンティティシステムに関する策定する際の参考とすべきである。
個人主体性	
5.1.1	政府は、他の、場合によっては無関係なアクションを可能にするために政府が欲しがる情報に焦点を合わせるのではなく、個人がシステム上で行い得るさまざまな手続きのために、個人からどのような情報を実際に取得する必要があるのかを考えなければならない。
5.1.1	個人は、情報に基づく選択を行う主体性を持たなければならないが、システムのデフォルトは最もプライバシーを強化するものであるべきである。
システムの透明性	
5.1.2	政府は、個人から監査人まで全ての関係者が、企業が要求する情報が、確立されたプライバシーフレームワークの標準原則に適合しているかを検証できるように、消費者保護法を改正することを検討すべきである。
5.1.2	各政府は、最低限、自らと、政府発行のデジタル資格情報を利用する（公共と民間、両方の）当事者向けの監査要件を策定しておくべきである。全てのrelying partyをレビューの対象とし、また、いつ、どのようにデータを利用および保持するかに責任を負わせるべきである。
データ最小化	
5.1.3	政府および市民社会、組織は、ある特定の種類のトランザクションに最低限必要となる、適切な一連のデータとはどのようなものかについて見解を一致させるべきである。
選択的開示	
5.1.4	OSベンダ、コンピュータハードウェアメーカー、標準開発者に至るすべての関係者が、標準開発者の担当者全員が選択的開示に必要な技術を広く利用できるようにする取り組みに参加しなければならない。

先に述べたOECDプライバシー原則とISO/IEC 29100にあるいくつかの概念を、デジタルシステム内のプライバシーに関するあらゆる議論の土台とすべきである。これら原則は目新しいものではなく、また政府やプライベートセクターの組織はこれを一から作り直すか、あるいは自らの法的・技術的システムに組み込みたいと思うものだけをこのなかから都合のよいものだけを選んで組み込む傾向にある。

政府発行のデジタル資格情報に関しては、これら原則を基本原則として、計画と設計の初期段階で組み入れるべきである。

政府はNIS2やNISTサイバーセキュリティフレームワーク、EUサイバーレジリエンス法案に記載されているものなど、最新のサイバーセキュリティのベストプラクティスを精査すべきである[153]。これが、「合理的な安全保護策で、データの損失や不正アクセ

[153] NIS2指令、http://data.europa.eu/eli/dir/2022/2555/oj、国立標準技術研究所。『サイバーセキュリティフレームワー

ス、破壊、利用、改変、開示などのリスクから個人データを守るべきである」とするOECD 安全保護の原則（Security Safeguards Principle）を順守する上で役立つ。その国がOECD加盟国であろうと、なかろうと、政府がそのシステムで個人データをどのように保護するかに関するこれら原則は（保護の適切さを測る）妥当な基準となる。
政府は自らがデジタルエコシステムで最も重要なデータ管理者であり、そのため、説明責任の原則（「データ管理者は上記の原則を実行するための措置を順守していることに責任を負うものとする」）に対して責任を負う必要があることを常に頭に置いておくべきである。

5.1.1 個人主体性

同意とユーザー制御は、デジタル資格情報の民間による発行と利用に対する規制で強く対処されている項目であるが、おそらく、規制当局が意図した効果は表れていない[154]。同意はOECDの収集制限と利用制限、個人参加の各原則でもカバーされている。デジタル資格情報の政府による発行と利用は、行政サービスにとってさえ、いつ、どのように同意を要請するかのレベルを押し上げている。政府は、他の、場合によっては無関係なアクションを可能にするためにどのような情報を望むのかに焦点を合わせるのではなく、システムで講じる必要があるさまざまなアクションのために、個人からどのような情報を実際に取得する必要があるのかを考えなければならない。

例えば、政府は、自らが要請するものと、個人が許可するものが合致する場合には、サービスがさらなる同意の要請をする必要がないよう、個人がデータ公開のデフォルトを設定できる、データ開示の同意管理サービスを検討してもよいかもしれない。別の選択肢として、デバイスの各ウォレットへの同意記録実装を義務づけることも考えられる（ISO/IEC 18013-5に取り入れられた仕組み）。個人のデフォルトがサービスの要件と合致しない場合、サービスはどのような情報を、なぜ要請しているか説明し、異なる道を選択する機会をその個人に提供する必要が出てくる可能性もある。その個人には、自分のデジタルフットプリントを最小限に抑えるための選択的開示の選択肢を与えられるべきである[155]。

個人は主体性を持たなければならないが、同時に、不必要な選択という負担を負わされてはならない。デフォルトは常に合理的で、個人に対して行われる要求を最小限にとどめるものであるべきであり、またプライバシーの最良の選択は常に、最も簡単なものであるべきである。

ク| NIST（Cybersecurity Framework | NIST）』。米国商務省国立標準技術研究所。2023年4月2日にアクセス。https://www.nist.gov/cyberframework、および欧州委員会。『サイバーレジリエンス法』。Shaping Europe’s Digital Future、2022年9月15日。https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

[154] 詳しくは、Cate, Fred H.およびMayer-Schönberger, Viktor、『ビッグデータ社会の通知と同意（Notice and Consent in a World of Big Data）』（2013年）。Maurer Facultyの論文。2662。 https://www.repository.law.indiana.edu/facpub/2662を参照。

[155] 例えば、AAMVAのmDL実装ガイドラインとデータ最小化および選択的開示に関する具体的なガイダンス（AAMVA’s mDL implementation guidelines and the specific guidance on Data Minimization and Selective Disclosure）。AAMVA。『モバイル運転免許証実装ガイドライン1.2 - 米国自動車管理者協会 – AAMVA（Mobile Driver’s License Implementation GuidelinesAmerican Association of Motor Vehicle Administrators – AAMVA）』、2023年1月。27～29ページ。https://www.aamva.org/assets/best-practices,-guides,-standards,-manuals,-whitepapers/mobile-driver-s-license-implementation-guidelines-1-2を参照。

5.1.2 システムの透明性

ユーザー制御という概念と相まって、政府は信頼を高めるため、自らのシステムの透明性の構築を進めている。自らのサービスがコード層に至るまで何をしているかを示すことで、この取り組みを行っている場合もあれば[156]、個々人が読み、利用することで、政府がそのシステムに関してどのような情報を開示しているかを確認できる文書化ツールやサービスツールに頼っている場合もある。これによってOECDの公開原則と目的明確化原則が関わってくるが、それでもこれら原則の扱いはそれぞれ全く異なる。

例えば、Aadhaarシステムでは居住者がウェブサイトから自分のアイデンティティの認証履歴をチェックできる。だが、Aadhaar技術自体は*プロプライエタリな（非公開の独占的な）集中管理システムとして運用されている[157]。一方、SingpassはGitHubレポジトリでAPIソースコードを世界に公開している[158]。

米国カリフォルニア州はサイバーセキュリティ監査要件の見直しを進めており、これが透明化に向けたその取り組みの強力な一部となるかもしれない[159]。これとは対照的に、GDPRには正式な監査要件が全くない。また、第三者監査は、政府であれ、企業であれ、組織が自らの順守状況を評価する手助けとなり便利だが、監査結果が公表されたときにしか、透明性の尺度とはならない。

とはいえ、政府は、自らが発行する資格情報がプライベートセクターで利用される場合には特に、企業が要求する情報が実際に必要最小限のものであるかどうかを個人には判断できないことを認識しなければならない。個人データの要請に至る企業の意思決定の透明性は皆無かそれに近い。政府は、個人から監査人まで全ての関係者が、標準原則に適合しているかを検証できるように、消費者保護法を改正することを検討すべきである。

各政府は最低限、自らと、政府発行のデジタル資格情報を利用する（公共と民間、両方の）当事者向けの監査要件を策定しておくべきである。全てのrelying partyをレビューの対象とし、また、いつ、どのようにデータを利用および保持するかに責任を負わせるべきである。例えば、シンガポールでは、relying partyの説明責任がSingpassシステムの中心的要素である[160]。イタリアでは、どの新relying partyもシステムへのアクセスが許可される前にチェックを受け、少額の料金が課せられる。

---

[156] シンガポール政府。『Singpass』。GitHub。2023年4月2日にアクセス。https://github.com/singpassを参照。

[157] Privacy International。『IDシステムを分析：Aadhaar（ID Systems Analysed: Aadhaar）』、2021年11月19日。https://privacyinternational.org/case-study/4698/id-systems-analysed-aadhaar.

[158] 『Singpass』、https://github.com/singpass.

[159] カリフォルニア州。『よくある質問（FAQ）– カリフォルニア州プライバシー保護局（CPPA）（California. “Frequently Asked Questions (FAQs) - California Privacy Protection Agency (CPPA)）』。2023年4月2日にアクセス。https://cppa.ca.gov/faq.html.

[160] シンガポール個人データ保護委員会。『PDPC | 責任（PDPC | Accountability）』。2023年4月2日にアクセス。https://www.pdpc.gov.sg/accountability.

5.1.3 データ最小化

世界各地の規則でも謳われている基本的なセキュリティのベストプラクティスは、ISO/IEC 29100プライバシーフレームワークに「データの処理は、明確化された目的に必要な最小限にとどめるべきである」と記載されたデータ最小化の原則である。もちろん、直接必要なものの解釈はさまざまにでき、法律面と技術面、両方の実施メカニズムはばらばらに適用されているか、完全に欠如している。今もなお、個人のデータプライバシーを守る最も強力な方策の1つは、個人データを全く収集しないことである。

政府は、個人データのいくつかの基本属性について、公的な情報源（オーソリティ）であるという独自の立場にある。出生記録や実名、国籍（市民権）は、政府が自国の市民や居住者のために生成するデータのほんの一例にすぎない。例えば、インドのAadhaarシステムは人口動態データの4つの項目（氏名と年齢、性別、住所）と、任意で2つの項目（携帯番号と電子メールアドレス）しか収集しない。しかし、政府は必ずしも自らの権限の範囲ではないデータも多く集める可能性が高い。政府機関が多様性や公平性に対応できているか否かを評価するため、人種や性別、性的指向などのデータを収集しているが、そのデータが情報源となり、政府自体が重要だとするその他の目的（公共の安全など）に利用される可能性もある[161]。

米国国立標準規格研究所（NIST）は、NIST Special Publication 800-53『情報システムと組織向けのセキュリティとプライバシー管理（Security and Privacy Controls for Information Systems and Organizations）』で米国政府向けのガイドラインを作成してきた[162]。これは、全ての米国政府機関にデータの収集と取り扱いに関する厳格なガイドラインを提供するものである。

シンガポールはさまざまな原則を重視し、「プライバシーに配慮した設計（Privacy-conscious design）」の原則（「Singpassアプリプロファイルで機微なデータを容易に非表示にできるようにすることで、出先でのトランザクション時に自分のプライバシーを確保する」）でデータ最小化に暗に対応している[163]。個人のSingpassデータの一部を要求するサービスからは、その情報は非表示にできるものの、銀行口座情報などから、かなりの量のデータがサービスには保存されている。

欧州データ保護会議（EDPB）のガイドラインは、データ最小化を検討する際に考慮すべき設計要素を把握するための優れた手引きとなる[164]。

---

[161] 例えば、『レズビアンおよびゲイ、バイセクシュアル、トランスジェンダー、クィア、インターセックスの個人の平等の向上（Advancing Equality for Lesbian, Gay, Bisexual, Transgender, Queer, and Intersex Individuals）』。*Federal Register - the Daily Journal of the United States Federal Government*、*2022年6月15日*。https://www.federalregister.gov/documents/2022/06/21/2022-13391/advancing-equality-for-lesbian-gay-bisexual-transgender-queer-and-intersex-individualsのLGBTQ＋に関する情報と大統領府でのデータ収集に関する指摘を参照。

[162] Force, Joint Task。『情報システムと組織向けのセキュリティとプライバシー管理（Security and Privacy Controls for Information Systems and Organizations）』。CSRC、2020年12月10日。https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[163] シンガポール政府。『Singpass -原則』。2023年4月2日にアクセス。https://www.singpass.gov.sg/main/principles/.

[164] 欧州データ保護会議。『データ保護バイデザインおよびバイデフォルトVersion 2.0第25条の1つのガイドライン4/2019を採択（Adopted 1 Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0）』、2020年10月20日、21～23ページ。https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.

とはいえ、大規模なデータ最小化を支えるには、もっと多くの対応を講じる必要がある。政府と市民社会、組織はある特定の種類のトランザクションに最低限必要となる、適切な一連のデータとはどのようなものかについて見解を一致させるべきである。例えば、銀行は政府発行のデジタル資格情報が真正なものであることの検証と、個人の氏名と生年月日の収集、その資格情報の期限のみとする」と規定することで、それ以外の情報の収集を禁止できる。

各relying partyを、それが収集できる情報の内容に応じて認証し登録すれば、定められた法令に従い、それに従って技術でデータ最小化を実行できるかもしれない。

5.1.4 選択的開示

データ最小化と同意など基本的な原則を推進する規則を補完するには、選択的開示ツールの開発をさらに推進しなければならない。先に述べたように、資格情報からデータの一部のみを開示する手段を提供するこれら技術は、高度な暗号アルゴリズムか、策定中の新標準のいずれかに依拠している。ゼロ知識証明に用いられる高度なアルゴリズムは政府の承認を受けておらず、またほとんどのモバイルデバイスハードウェアがこれに対応していない。だが、その代替として、SD-JWT のアプローチのようなソルト付きハッシュベースのアプローチは、政府の承認を受け、かつ、モバイルデバイスも対応する署名アルゴリズムと共に用いることができる。SD-JWT のようなソルトとハッシュベースのスキームはまだ草案ステータスにあるが、本書発行時点では、選択的開示と高いセキュリティレベルの両立を図る唯一の方法である[165]。

OSベンダとコンピュータハードウェアメーカー、標準開発者に至るまで、すべての関係者が選択的開示に必要な技術を広く利用できるようにする取り組みに参加しなければならない。

5.2 今も続く懸念に対処する

政府発行のデジタル資格情報を利用するシステムにセキュリティとプライバシーの基本的要素が組み入れられるなか、個人が求めるプライバシーと技術の能力、そして政府が行っているトレードオフの間のギャップを埋めるために、政府と技術者が対処しなければならない構造的な懸念がある。

提言のサマリ：今も続く懸念に対処する	
監視	
5.2.1	政府は自らのシステムとサービスを中心に、プライバシーとセキュリティの基本原則を支持し、厳守する姿勢を示す努力をもっとしなければならない。
多様性と公平性、包摂性（DEI）	

pdf.（訳注：原稿よりURL更新。。2026年05月01日時点）

165 これら資格情報で選択的開示を実現できるか否かと、どのように実現するかに関する情報を含め、資格情報の形式の違いについて詳しくは、現在策定中の資格情報比較マトリクス（Credential Comparison Matrix）。
https://docs.google.com/spreadsheets/d/1Z4cYfjbbE-rABcfC-xab8miocKLomivYMUFibOh9BVo/edit#gid=1590639334を参照。

5.2.2	政府と技術者は公平性を規則に落とし込み、いかに技術を向上させてより多様性に富んだユーザー基盤を支えるかを検討して、DEI関連の問題を改善する努力をもっとしなければならない。
Single Point of Failure（SPOF）	
5.2.3	政府はあらゆる手を尽くして、自らの管理下にあるデータを守り、single point of failureを避け、生体認証データの保存時には、忘れずに情報にバイオハッシングを施さなければならない。
正当な行為者による不適切な利用	
5.2.4	政府に、自らの資格情報の利用に伴い収集する個人データの利用に責任を負わせるには、個人と社会がその利用について知ることができるレベルのシステムの透明性を、おそらくは第三者監査人の利用により確保しなければならない。
持続可能な保護	
5.2.5	非政府組織（NGO）は、デジタルアイデンティティシステムが採用するマルチステークホルダーの信頼モデルの全当事者と連携して、プライバシー保護の質を低下させる法改正の影響を和らげる効果を世界的に発揮できるソリューションづくりを先導しなければならない。

5.2.1 監視

プライバシーと行政システムについて考察する論文や調査報告書の多くは、政府による監視の可能性に対する懸念を含む。より安全で効率的な社会というビジョンを実現するために、収集するあらゆるデータを利用していると極めてオープンに発信する政府もある。

政府は、公正な民主主義への支援と、人権の擁護者としての役割を改善するのであれば、特に自らのシステムやサービスにおいて、プライバシーとセキュリティの基本原則を支持し、厳守する姿勢を示す努力をもっとしなければならない。

5.2.2 多様性と公平性、包摂性

多様性と公平性、包摂性（DEI）はプライバシーと近い関係にあるが、それ自体として独立した研究を要するほど独自性があり、プライバシーとは別に、研究する必要がある。政府発行のデジタル資格情報の利用は、技術へのアクセスや技術を利用する能力だけでなく、技術を利用したいという意欲まで、多くの要素に依存するが、その要素は万国共通ではない。

DEIへの影響も、監視に関する懸念につながっている。マイノリティや、それ以外の理由で周縁化された集団の個人は、デジタル資格情報の利用を含めた行政サービスの利用が政府によるトラッキングやネガティブなアクションにつながるという懸念を共有する。

この懸念が実際に問題となる一例として、DEI・プライバシー擁護派は、アルゴリズム

による排除の問題を挙げる。政府がサービスへのアクセスに関わる意思決定の支援へのAI利用を進めるにつれ、アルゴリズムによる排除（algorithmic exclusion）が大きな懸念となってきた。キャサリン・タッカー博士（Dr. Catherine Tucker）はこのアルゴリズムによる排除を、不良データやデータの欠損が原因で、「アルゴリズム処理から人々が排除されることにより生まれる結果で、アルゴリズムがその人たちに関する予測をできないことを意味する」と定義している[166]。

行政サービスがデジタル資格情報に依存している場合には、その資格情報を取得できない個人はその行政サービスの恩恵から排除される可能性が高い。

NIST SP 800-63-4草案に盛り込まれた公平性の新たなガイドラインなどの取り組みは、この種の排除を防ごうとしているが、DEIの問題は社会全体で取り組まなければならない課題であることに変わりはない。政府と技術者は公平性を規則に落とし込み、いかに技術を向上させてより多様性に富んだユーザー基盤を支えるかを検討して、これらの問題を改善する努力をもっとしなければならない。

5.2.3 Single Point of Failure（SPOF）

これら資格情報に一定レベルの検証（有効性確認）期待が、政府による大量の個人データの収集を招いている。おそらく自明のことだが、それに伴う必然的な懸念として、政府がそのデータをどのように保護するかという問題がある。Aadhaarシステムの場合、一元管理されたデータの侵害で、10億件を超える記録が流出した可能性がある。他の行政システムへの侵入では、生体認証データが侵害被害に遭った。

政府はあらゆる手を尽くして、自らの管理下にあるデータを守り、単一障害点（Single Point of Failure）を避け、生体認証データの保存時には、情報に慎重にバイオハッシングを施さなければならない（バイオハッシングについて詳しくは、4.2.2「生体認証技術」を参照）。

5.2.4 正当な行為者による不適切な利用

（決して万国共通ではない）プライバシー法の順守を義務づける規則の対象に政府が入っている場合であっても、公共の安全や国家安全保障の旗の下に、必ず強力な例外が設けられている。その時の政権によって、合法的なアクションと悪用の境界線は変わりやすい。この懸念は、持続可能な保護に関わる問題の一部と、政府による監視に関する懸念を反映している。

政府が資格情報の利用を通じて収集した個人データの運用について、説明責任を果たさせるためには、個人や社会がその利用状況を把握できるよう、第三者監査人の活用などを通じて、システムに一定の透明性を確保しなければならない。

---

[166] Tucker, Catherine。『ワーキングペーパー　アルゴリズムによる排除：スパースデータとデータ欠損に対するアルゴリズムの脆弱性（Working Paper Algorithmic Exclusion: The Fragility of Algorithms to Sparse and Missing Data）』。The Center on Regulation and Markets at Brookings、2023年2月。https://www.brookings.edu/wp-content/uploads/2023/02/Algorithmic-exclusion-FINAL.pdf.

5.2.5 持続可能な保護

政府は変わる。選挙や政変などに伴う変化で、ある国や地域が、1つの政治体制や政党から別のそれに変わる。ある政権で存在していた法律が、別の政権では無効にされたり、悪用されたりすることもある。残念ながら、これらは、あらゆる統治制度に伴うリスクであり、政府は変わる可能性があり、時間とともに変わっていくだろうが、それは必ずしも市民や居住者の生活を向上させる変化とはかぎらない。そのため、法令が特にデジタルアイデンティティに関して、個人のプライバシーを支えるものとなるよう気を付けていたとしても、それだけでは決して十分ではなかろう。

だからこそ、規制と共に技術を進化させ、お互いにバランスを取り、お互いを制御する役割を果たすことができるようにしなければならない。OECDや国際連合、世界銀行などの非政府組織（NGO）と、Secure Identity Alliance （SIA）やGlobal Legal Entity Identifier Foundation（GLEIF）、OpenID Foundation、World Privacy Forumなどの組織は、政府から標準化団体、そしてプライベートセクターの技術者まで、マルチステークホルダーの信頼モデルの全当事者と連携して、世界的に機能し、かつプライバシー保護を損なう法改正の影響を緩和するソリューションへと導かなければならない。

5.3 新たな懸念に先手を打つ

政府や市民社会、技術者が議論をしている今も続く懸念に加え、技術の進歩に伴い新たな懸念が浮上してきた。増え続けるデータの量と利用を人工知能で把握する取り組みが、政府とプライベートセクターでみられる全てのアイデンティティシステムに関係する問題として拡大している。アイデンティティエコシステムの全ステークホルダーは、このような新たな問題についてよく考え、先手を打ってそれがもたらすギャップを埋める必要がある。これを特に浮き彫りにするのが、戦争のデジタル領域への拡大である。下に示した提言は、本書の発行時点で専門家コミュニティにある程度よく理解されていたリスクに対処しているが、世間一般に知られているリスクを全てカバーしているわけではない。今後の版で新たなリスクが追加される可能性もある。例えば、政府が選定した暗号標準に量子コンピューティングが及ぼす影響を懸念する実務家は多いが、現時点でアプローチに関する見解は一致していない。

提言のサマリ：新たな懸念に先手を打つ	
デジタル戦争	
5.3.1	技術者と政府は、デジタルアイデンティティシステムとサービスを、軍事活動のニーズに対応しながらも、本書に記載するセキュリティとプライバシーの基本的機能の多くに準拠した設計にしなければならない。
ディープフェイク	
5.3.2	技術者と政府は、既存の保護策をすり抜ける新たな方法を支える技術の進歩がもたらす脅威に常に気を付け、迅速に対応しなければならない。
メタバース	

5.3.3	政府と技術者は、メタバースのようなイマーシブ技術がプライバシーに及ぼす影響にもっと迅速に対応しなければならない。
生成AIと大規模言語モデル	
5.3.4	政府と技術者は、可能であればAIベースの新たなセキュアシステムの開発を通じて、AI強化型攻撃との闘いに労力を集中させなければならない。

5.3.1 デジタル戦争

ほぼ全てのプライバシー法令は、公共の安全のためにはプライバシーを停止・保留する条項を含む。国が戦争状態になると、これが最も顕著となる。

Lothar FritschおよびSimone Fischer-Hübnerは、その論文『プライバシーとセキュリティが次なるモノの戦場（BoT）に及ぼす影響に関する調査（Implications of Privacy & Security Research for the Upcoming Battlefield of Things）』で、「モノの戦場（BoT）」の文脈で考えたときの、今後25年間にわたるプライバシーの未来に焦点を当てた[167]。

技術者と政府は、デジタルアイデンティティシステムとサービスを、戦闘のニーズに対応しながらも、本書に記載するセキュリティとプライバシーの基本的特性の多くに応じた設計にしなければならない。

> *「データの真正性がますます重要な社会的関心事となっているため、中央への信頼（central trust）を必要とせずに、データベースを共同で維持管理できる体制は、非常に深い関わりがある。同様に、十分な保護策のない中央管理システムはsingle point of failureである。センサー測定に対する信頼と運用の協調的な実施は、防衛と市民の安全に不可欠である。システムのコンセンサスとアルゴリズムに関する説明責任、コンポーネントの正常な機能の検証の確保と文書化は今後、コネクテッドデバイス（接続されたモノ）とその制御システムの重要な特性となる。安全なロギング技術が、運用の機密性を保持しながら、異常を調べる一助となるかもしれない。」– L. FritschおよびS. Fischer-Hübner, Journal of Information Warfare*[168]

プライベートセクターと軍事技術（自律型ドローンなど）の重なり合いは、プライバシーとセキュリティの考慮を社会のあらゆる面に組み込まなければならないことを示唆する。軍事転用の可能性は、あらゆるレベルでチェックとバランスを考慮しなければならないことを示唆する極めて大きな懸念点である。

---

[167] Fritsch, L.、Fischer-Hübner, S.（2019年）。プライバシーとセキュリティが次なるモノの戦場（BoT）に及ぼす影響に関する調査（Implications of Privacy & Security Research for the Upcoming Battlefield of Things）。Journal of Information Warfare, 17(4)。https://www.diva-portal.org/smash/get/diva2:1306652/FULLTEXT02

[168] 同上、78ページ

5.3.2 ディープフェイク

デジタル環境では、ディープフェイク（人工知能と機械学習（AI/ML）を利用して作成された本物そっくりの画像と動画）の脅威が増している。AI/ML技術の進歩に伴い、不正行為事案や偽造事案でディープフェイクが出現し、法執行機関にとって難しい課題となってきた[169]。

ディープフェイクの作成に利用される技術が、資格情報の遠隔利用シナリオ（ISO/IEC 27533で想定されているユースケースなど）における犯罪活動にも利用されうることは想像に難くない。（ISO/IEC 18013-5やOAuth Selective Disclosure、OpenID for Verifiable Presentationsを含め、本書で述べたものなどの取り組みで）標準に従った情報の交換を保護する技術的信頼性が向上しつつある中でも、ディープフェイクが、生体認証証明プロセスや生体認証による認可といったエンドツーエンドの実装の別の部分に対する信頼を損ねかねない。要するに、ディープフェイクのような他の技術が進化して、保護策をすり抜ける新たな方法を見つけるようになってきたのである[170]。

技術者と政府は、既存の保護策をすり抜ける新たな方法を支える技術の進歩がもたらす脅威に常に気を付け、迅速に対応しなければならない。

5.3.3 メタバース

「メタバース」という概念は近年、大きな注目を集めてきたが、想像の域を出ない構想あると考える人はいまだに多い。

> *メタバースはユビキタスなバーチャル世界の相互連結網（interconnected web）であり、部分的に物理的世界と重複し、またこれを強化している。これらバーチャル世界は、アバターとなったユーザーがお互いにつながり、交流することや、拡張性と同時性、一貫性を持つイマーシブな環境でユーザー生成型コンテンツを体験、消費することを可能にする。経済システムが、メタバースへの貢献に対するインセンティブを与えている[171]。*

この用語が今後も使われるか否かにかかわらず、デジタル世界がよりイマーシブな体験を含むようになっているという考え方は想像に難くない。だが、それが政府発行のデジタル資格情報とプライバシーにどのような意味を持つのかは、数多くの疑問と懸念を示唆するが、しかし答えはほとんど見つかっていない[172]。完全にデジタルな世界

---

[169] Frederick Dauer、『ディープフェイクの時代の法執行機関（Law Enforcement in the Era of Deepfakes）』、 *Police Chief Online*、 2022年6月29日.

[170] 『JWTs (SD-JWT)の選択的開示（Selective Disclosure for JWTs (SD-JWT)）』、" https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/ and "OpenID for Verifiable Credentials," https://openid.net/openid4vc/.

[171] Weinberger, Markus。『メタバースとは？ - 質的メタ統合に基づく定義（What Is Metaverse?—A Definition Based on Qualitative Meta-Synthesis）』。*Future Internet* 14, no. 11（2022年10月28日）：310。 https://doi.org/10.3390/fi14110310.

[172] メタバースにおけるプライバシーとガバナンスに関する興味深い論文については、Fernandez, Carlos Bermejoおよび Pan Hui。『生活とメタバース、そして全て：メタバースにおけるプライバシーと倫理、ガバナンスの概要（Life, the Metaverse and everything: An overview of privacy, ethics, and governance in Metaverse）』。*2022 IEEE 42nd*

をうまく規制することはできるのか。政府発行のデジタル資格情報は、個人参加に関する確実性をある程度確保する必要があるのか。

政府にも、技術者にも、検討すべきプライバシー関連の疑問や技術的疑問がさまざまあり、また、限られた時間で実際的なソリューションを考案する必要もある。メタバースなど完全にデジタルなサービスの商業開発は個人に期待を抱かせる可能性が高く、事後的に制限を適用することは関係者全員にとって不快な経験となりかねない。

5.3.4 生成AIと大規模言語モデル

もう1つの新たな懸念領域は、生成人工知能（AI）と大規模言語モデル（LLM）である。ブログの投稿やソーシャルメディアのやり取り、主流メディアには、これらモデルの脅威と将来性の両方を考察する話題があふれている。

> *大規模言語モデル（LLM） AIは、大量のデータから自然言語のテキストを生成できるAIモデルを意味する用語である。大規模言語モデルはトランスフォーマーなどディープニューラルネットワークを利用して、何十億あるいは何兆もの言葉を学習し、いかなるトピックや分野のテキストも生成する。大規模言語モデルは分類や要約、翻訳、生成、会話などさまざまな自然言語タスクを実行することもできる。大規模言語モデルの例はGPT-3やBERT、 XLNet、EleutherAIなどである*[173]。

政府発行のデジタル資格情報とプライバシーという文脈で考えると、懸念はディープフェイクがもたらすそれと類似する（セクション3.3.2「ディープフェイク」を参照）。これに加え、生成AIが、行政サービスを含め、あらゆるオンラインシステムを標的にできる生成AIによってマルウェアの作成がいかに容易になるかについての考察からも懸念が浮かぶ[174]。

政府と技術者は、場合によってはAIベースのセキュリティ特化型の新システムの開発を通じて、AI強化型攻撃との闘いに労力を集中させなければならない。

5.4 市民社会の役割

市民社会は法律や政策、仕様についての知識ギャップを埋めるのに必要な専門知識と情熱を政府と標準策定組織の両方に与えている。先の「Privacy Considerations for

---

*International Conference on Distributed Computing Systems Workshops (ICDCSW)*において、272～277ページ。IEEE、2022年を参照。

173 『LLM AIに関する概念の概要（Concepts Overview for LLM AI）』。 Microsoft Learn、2023年4月4日。https://learn.microsoft.com/en-us/semantic-kernel/concepts-ai/.

174 Harr, Patrick。『生成AIが、私たちの知るサイバー攻撃の全てを変える（Generative AI Changes Everything We Know About Cyberattacks）』、Dark Reading。2023年2月23日。https://www.darkreading.com/vulnerabilities-threats/generative-ai-changes-everything-we-know-about-cyberattacks.

Internet Protocols（インターネットプロトコルのプライバシーに関する考慮事項）」のコールアウトで述べたように、コード（技術的であれ法的であれ）を作成している人は最善の意図を持っているものの、プライバシー領域の深い専門的知識がなく、その考慮に十分に対処できないことが多い。

IAPPは定期的に政府のコンサルテーション（意見公募）に回答しているが、Electronic Privacy Information Center(EPIC）も同様である。Privacy InternationalやElectronic Freedom Foundation (EFF)など、プライバシー問題に特化したいくつかの市民社会組織はこの領域で極めて活発に活動をしている。これは政府の文脈においてプライバシーを啓蒙し、擁護していく上での重要な要素である。ただ、これら組織は、技術標準の策定面での活動がさほど活発でないことが多い。この点は変える必要がある。

それを変えられる可能性がある手段の1つが、Internet Research Task ForceのPrivacy Enhancements and Assessments Research Group (Pearg)である[175]。IETFのパートナー組織であるInternet Research Task Force (IRTF)はインターネットが直面するより難しい問題の一部に関する研究を支援している。IRTFは標準設定組織ではないが、十分な関与があれば、プライバシー擁護派が標準設定プロセスの参考となる情報を提供できるようになる別の方法をもたらすかもしれない。

6 まとめ

政府はデジタルトランスフォーメーションを推進し、政府発行の質の高いデジタル資格情報を有権者に提供しているが、プライバシーについて「技術的に可能」というレンズを通して考え、また法令の設計でプライバシーを考慮に入れなければならない。政府は社会の脆弱な一員を守る注意義務を負い、この義務はこのデジタル技術時代で彼らを守ることにも及ぶ。いかに社会を守るかを考えるとき、政府は、保護を受ける権利があり、自ら決定を下し、安心してオンライン活動を行う主体性が認められるべき個人が社会を構成していることも忘れてはならない。個々人と社会全体が、必然的に委ねることになるデータを政府がどのように利用するかを懸念している。その懸念に対処するのは政府の責任である。

技術は、オンラインの世界におけるプライバシーの確保を可能にする役割を担う。プロトコル設計やハードウェアとソフトウェアの進歩、暗号アルゴリズムの進化を通じて、技術はプライバシーをより強化する環境を実現させるツールを提供する。これらのツールを完全に中立なものと見なし、これらがいかにプライバシーに影響を及ぼすような形で誤用または悪用されるおそれがあるかという脅威を無視してしまえば、回避できたはずの新たなプライバシーリスクを招くことになる。技術者はプライバシー意識を設計の中核に組み込まなければならない。

これら資格情報が現在、世界各地でどのように利用されているか、その範囲を考えると、プライバシーへの幅広い影響を完全に把握することはとてつもない難題である。

[175] 『Privacy Enhancements and Assessments Research Group (Pearg) 』。2023年4月1日にアクセス。https://datatracker.ietf.org/rg/pearg/about/.

市民社会はプライバシーを取り巻く環境を深く理解しており、特に政府と連携することを望んでいる。そのような連携は必要であるが、それだけでは十分でない。市民社会は技術開発に関与するとともに、技術者がプライバシーを取り巻く環境について現時点で認識できていない課題を把握する手助けをしなければならない。

そして最後に、個々人自身も、このシステムの改善を助ける一翼を担う。明確で実行可能かつ簡単な選択肢を提供することは政府とサービス、技術者の役割だが、個人も自らに与えられた選択肢を活用する必要があるだろう。

本書はこの領域の可能性に軽く触れただけである。資格情報を有権者に発行する政府はさらに増えている。技術者は常に新たなプロトコルとツールの開発に取り組んでいる。NGOと市民社会は世界各地でプライバシーやそれに関連する問題に対応している。私たち全員が、政府発行のデジタル資格情報の極めて複雑な環境と、プライバシーを取り巻く環境に対処する今、各セクションが思考を刺激し、より深い議論を促すことができたら幸いである。

7 付録A： OECDプライバシー原則の原文

https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188からコピー

収集制限の原則

7. 個人データの収集には制限を設けなければならず、いかなる個人データも適法で公正な手段によって、かつ、該当する場合には、データ主体が認識し、または同意した上で取得されなければならない。

データ内容の原則

8. 個人データはその利用目的に関係したものでなければならず、かつ、利用目的に必要な範囲で正確、完全であり、最新の状態に保たなければならない。

目的明確化の原則

9. 個人データの収集目的は、収集時より遅くない時点で明確化されなければならず、その後におけるデータの利用は、当該収集目的の達成、または当該収集目的と矛盾せず、かつ、目的の変更の都度明確化される他の目的の達成に限定されなければならない。

利用制限の原則

10. 個人データは、上記9.に従い明確化された目的以外の目的のために、開示され、閲覧に供され、その他の形で利用されてはならない。ただし、以下の場合は、このかぎりではない。

a) データ主体の同意がある場合、または

b) 法律により認められる場合

安全保護の原則

11. 個人データはデータの紛失、権限のないアクセス、破壊、利用、修正若しくは開示などのリスクに対し、妥当な安全対策により保護されなければならない。

公開の原則

12. 個人データに関わる進展（development）、実務上の取扱要領（practice）および方針（ポリシー）については、全般的に公開の政策が取られなければならない。個人データの存否および種類ならびにその主たる利用目的にのほか、データ管理者のアイデンティティおよび通常居住する場所を確認する手段を容易に利用できるようにしておかなければならない。

個人参加の原則

13. 個人は、以下の権利を有するものとする。

a) データ管理者が自分に関係するデータを保有しているか否かについて、当該データ管理者などに確認をとること、自分に関係するデータについて、

i. 合理的な期間内に、

ii. 仮に必要とする場合でも、過度にならない手数料で、

iii. 合理的な方法により、かつ、

iv. 本人が容易に理解できる形式で、

通知を受けること、

b) 上記の(a)および(b)の権利に基づく要求が拒否された場合には、その理由が示されること及び、そのような拒否に対して異議を申し立てることができること

c) 本人に関するデータに対して意義を申し立てること及び、その異議が認められた場合に、当該データを削除し、訂正、完全化、または補正すること。

責任の原則

14. データ管理者は上記の諸原則を実行するための措置を順守していることについて説明責任を負うものとする。

8 付録B：ISO/IEC18013-5とISO/IEC 29100のプライバシー原則

このセクションは、ISO/IEC 18013-5附属書Eの一部を要約したものの抜粋である。このプライバシー原則はISO/IEC 29100「プライバシーフレームワーク」をベースとしている。

8.1 プライバシー保護の原則

1. **同意および選択：**データ主体が自分の個人データの処理に同意していなければならない。
2. **目的の正当性および明確化：**データ主体が、自分の個人データが収集、処理および場合によって保存される目的を十分に認識していなければならない。
3. **収集制限：**データ管理者およびデータ処理者はその目的に必要なデータのみを収集し、これらの原則に整合する形でのみデータを収集しなければならない。
4. **データ最小化：**データ処理は明確化された目的に特に必要な範囲で最小限にとどめなければならない。
5. **利用、保持および開示の制限：**データ処理者は、明確化された目的以外の目的で、または他の原則に整合しない形で、データ主体の個人データを利用しては

ならない。

6. **正確性および質：**処理および保有されるデータの高い正確性がデータ主体の最善の利益となるため、データ処理者は正確性を確保するための対策を講じなければならない。
7. **公開性、透明性および通知：**同意の取得や、明確な通知の発出ならびに更新を含め、どのようなデータがどのように処理されているかをデータ主体が十分に把握できるようにしなければならない。
8. **個人参加およびアクセス：**データ主体が、自らの個人データの収集、同意、処理および保存管理に関与できるようにしなければならない。
9. **情報セキュリティ：**個人データは、データの紛失、不正アクセス、破壊、利用、改変または開示などのリスクから、安全対策により保護されなければならない。
10. **プライバシーコンプライアンス、責任および監査：**データ管理者およびデータ処理者は個人データ処理のあらゆる側面について説明責任を負い、データ主体に監査ログおよび監査可能性を提供しなければならない。