人間中心のデジタルアイデンティティ:

政府関係者向け

v1.1

主任編集：Elizabeth Garber、Mark Haine

2023年10月13日

引用：

E・GarbarおよびM・Haine（編集者）「Human-Centric Digital Identity: for Government Officials」

OpenID Foundation（2023年9月25日）

日付	改定
2023年10月13日	バージョン1.1に改定。共同ブランドパートナーであるMyData Globalを付録Dに追加。
2023年9月25日	最終版 バージョン1を公開。
2023年9月18日	パブリックコメントの検討と受領。編集前。図表類のフォーマットを行う予定。
2023年7月7日	パブリックコメント用ドラフトを公開。
2023年4月14日	専門家によるレビュー

寄稿組織

本稿のメッセージの形成のため、見識と内容を提供してくれた以下の方々に感謝する。彼らの貢献なくして本稿は成立しなかった。（敬称略）

- Dave Birch
- Julie Dawson
- Heather Flanagan
- Gail Hodges
- Nishant Kaushik (confirmed)
  Henk Marsman
- Nat Sakimura
- Golda Velez
- Kaliya Young

目次

目次 **3**

エグゼクティブサマリー **4**

編集者について 5

主な用語 **6**

第1部：アイデンティと政府の役割 **10**

背景 10

本稿の意義 5

第2部：現代のデジタルアイデンティティパラダイム **11**

パラダイム1と2：政府発行のeID 17

パラダイム3および4：政府が支援するマーケットプレイス 23

パラダイム5：新興のウォレットベース型パラダイム 26

重要な考慮事項 30

第3部：デジタルアイデンティティシステムに関する推奨事項 **33**

原則の統一 33

柱1：人間中心 34

柱2：戦略的設計とガバナンス 40

柱3：安全でプライバシーを保護するアイデンティティシステム 46

柱4：国際間の相互運用性の実現 49

結論とまとめ **52**

Appendix A – 進化する脅威モデル **54**

付録B – デジタルアイデンティティ原則の整合 **56**

付録C：OECD原則のチェックリスト機能 **58**

付録D：人間中心のデジタルアイデンティティにおける役割を担う非営利団体 **64**

付録E：プライバシーとセキュリティに関するベストプラクティス **67**

エグゼクティブサマリー

法的身分識別システムは、市民生活や経済活動への個人の参加を可能にする。そのおかげで、企業は発展でき、社会は回っている。また、これらは個人、組織、そして（近年では）モノの間の信頼関係構築に不可欠な要素であることが多い。国連世界人権宣言第6条[1]「法の下において人として認められる権利」は、実質的に、政府が教育・医療・投票・結婚・旅行など様々な権利を保障する土台を形成している[2]。 自己決定権やプライバシーでさえ、政府が個人を集団から区別する存在として識別することに依存していると言える。この依存関係こそが、国連が2030年までに普遍的な法的身分証明と出生登録を達成する持続可能な開発目標（SDG 16.9）を設定した理由である[3]。

このような経緯から、マッキンゼー[4]、ビル＆メリンダ・ゲイツ財団[5]、世界経済フォーラム[6]、世界銀行などの組織による有力な分析にも後押しされ、多くの国（および国家や地域をまたぐ組織）が現在、デジタルアイデンティティシステムやエコシステムの構築を目指している[7]。しかし、あらゆるアイデンティティシステムの設計、導入、展開、継続的管理には本質的なリスクが内在しており、デジタル化はそのリスクを増大させる[8]。

本稿の第1部および第2部では、これらの課題を検討し、グローバルの状況を調査することで、今日のデジタルアイデンティティシステムのパラダイム全体でみられる主な動向をまとめる。第3部では、既存の原則に基づいた文献を踏まえ、政府関係者がデジタルアイデンティティシステムの設計、実装、管理に必要なトレードオフを管理する際の推奨事項をまとめる。重要な点は、万能な解決策は存在しない、即ち、複数のシステムが並行して存在し得るし、単一の技術やアーキテクチャ、またはガバナンスの手法が万能薬となるわけでない、という考え方である。故に本稿ではOECDの最近のデジタルアイデンティティのガバナンスに関する勧告を踏まえ、政府関係者に以下を推奨する。

- デジタルアイデンティティシステムが人権確立を支え、維持し、促進するように設計する。その際、目的に適合した市民登録・法的身分システムを基盤とすること
- バリューセンシティブ[1]な人間中心の設計（Human-Centered Design：HCD）プロセスに従うこと

[1] （訳注）設計プロセスにおいて、プライバシー、公平性、信頼、尊厳といった、人間にとって重要な「価値観」を取り込むアプローチ

- バリューセンシティブHCDを技術的・制度的フレームワーク要件へ転換する戦略的アプローチを採用すること
- セキュリティ・バイ・デザインおよびプライバシー・バイ・デザインのベストプラクティスを優先すること
- 目的に適合したデジタルアイデンティティエコシステムを支えるオープン標準の成熟化に取り組むこと

(推奨事項全体については**表5**を参照のこと。本稿には複数の付録を付けている、これは、必要に応じて新たな非営利組織や策定されつつある新規基準を追加する「生きた文書」として維持するためである)

編集者について

本稿はOpenID Foundation (OIDF)から委託され、11の組織の協力(協力組織参照)により共同出版された。主任編集者はOIDF、OIX、その他の標準策定コミュニティのメンバーである。彼らはまた、OIDFおよび非OIDF標準を活用する営利事業も有している。本稿は厳密な調査とインタビューの過程を通じて、技術やアーキテクチャに関する偏りを最小限にしようと努めている。そのうえで、OIDFのビジョンは、人々が選択した場所で自らのアイデンティティを主張できるよう支援することであり、そのミッションは安全で相互運用性があり、プライバシーを保護するアイデンティティ標準の創出において、グローバルコミュニティをリードすることである。本稿に寄稿した非営利団体および専門家は全員、以下のような望みを共有している。1）アイデンティティデータの転送には安全で証明済みのプロトコルを使用する、2）国境を越えた相互運用性を実現する、および3）公共部門と民間部門が利益を実現し、堅牢なデジタルアイデンティティインフラへ移行しやすくする。

主な用語

本稿で使用する用語の多くは、文脈により異なった意味を持つ。すなわち、様々な分野や組織が、同じ概念に対して独自の用語体系を発展させてきた。例えば、社会科学者、国際開発者コミュニティのメンバー、または企業のセキュリティ確保を担当する最高情報セキュリティ責任者にとって、「アイデンティティ」は異なる意味を持つ。また、人や文化によっても意味が異なる。しかし、これらグループはすべて、人間中心のアイデンティティシステムの開発に価値を付加することができる。

本稿では以下の組織の定義を参考にしている。

- 国際連合経済社会局 「“Guidelines on the Legislative Framework for Civil Registration, Vital Statistics, and Identity Management（住民登録、人口動態統計及びアイデンティティ管理に対する法的組みに関するガイドライン）」[9]
- 国際連合　無国籍の地位に関する*1954*年条約[10]
- 国際連合　*1951*年の難民の地位に関する条約[11]
- 国際連合　無国籍状態に関する国連ガイドライン[12]
- OECD　デジタルアイデンティティのガバナンスに関する理事会勧告[13]

本規約は政府間協力により合意された用語の一貫した使用を保証する。追加された用語や注釈が加えられた用語もある。

法的身分証明（国連）	出生後に正式な戸籍登録機関による登録及び証明書発行により付与される氏名、性別、出生地、出生年月日など、個人のアイデンティティの基本的特性。出生届がない場合、法的な身分証明は法律上認定された証明機関により付与されることもある。戸籍登録機関による死亡証明書の発行により必要とされるからである。 [国連] 加盟国は、法的身分証明の付与及び身元証明書の発行について第一義的な責任を負う。難民に対する法的身分証明を付与する責任は、国際的に承認され権限を委任された機関に委ねられることもある。
デジタルアイデンティティ（OECD）	電子的に取得・保存された属性および／または資格情報であり、ユーザーの性質、特徴、または主張を証明するために使用可能で、必要に応じて当該ユーザーの一意的な識別を支援するもの。 なお、OECDの定義には含まれてはいないが、法人、機器、その他の人間以外も同様に識別されなければならない。
デジタルアイデンティティエコシステム（OECD）	政策立案者、規制当局、政府監督機関、デジタルアイデンティティソリューション提供者、資格情報発行者、サービス提供者、ユーザーなど、デジタルアイデンティティシステムに関わる様々な主体。このエコシステムには、異なる領域特化型のソリューションと関連した主体が含まれることがある。
デジタルアイデンティティシステム（OECD）	政策、規制フレームワーク、トラストフレームワーク、技術基準、役割と責任を含む、デジタルアイデンティティソリューション、資格情報、属性がユーザーに提供され、サービスプロバイダーによって信頼されるシステム全体。
市民登録（国連）	人口に関連する生命事象の発生と特性を、法令または規制に基づき法的要件に従って継続的、恒久的、義務的、および普遍的に記録する制度。 ・・・このプロセスは重要事象の発生事実を確立し、証明書という形式で法的文書を提供する・・・登録官が発行する書類または電子形式の文書・・・
法的地位	国連やOECDの文書において「法的地位」に関する単独の定義は見つかっていない。ただし本稿では、国籍に関する状態、身分上の状態、難民認定の状態、および無国籍者（以下に定義）といった概念をふくむものとして使用する、
国籍に関する状態（無国籍に関する国連のガイドライン）	「国籍に関する状態は、個人がパスポートや身分証明書の申請、公的部門における合法的居住や雇用の取得、投票権の行使、兵役義務の履行、政府サービスへのアクセスを試みる際に重要となる。」 各国には国籍付与に関する独自の法的根拠があり、国際的な定義がない点に留意されたい。
身分上の状態（国連）	一般に、婚姻状態や年齢など個人の社会における法的地位。身分上の状態により、個人の法的能力や責務、権利、および個人間の義務が決まることがある。

無国籍者（国連1954年条約）	いかなる国の法律の適用下においても、その国の国民とみなされない者。
資格情報 (OECD)	運転免許証、身分証明書、許可証、資格証明書など、資格発行者が発行し、電子的に記録された利用者に関する信頼できる確認済みの情報の集合。 なお、OECDの定義では「信頼性のある」とされているが、必ずしもそうとは限らない。資格情報は複数の組織によって発行される場合もあれば、自分で発行することもある。本来的には信頼性はこの用語に含まれる意味ではない。
デジタルアイデンティティソリューション(OECD)	ユーザーが属性や資格情報の保存、取得、共有ができ、オンラインまたはオフラインサービスにおける認証に使用される有形および／または無形の単位。
属性 (OECD)	氏名、生年月日、出生地、固有識別子など、ユーザーに帰属する検証済みの性質または特徴（例：個人識別番号、社会保障番号、会社登録番号）、および住所。
認証 (OECD)	情報通信システムにおいて、ユーザー、デバイス、またはその他のエンティティが主張する身元の有効性と確実性を確立するための機能。
トラストフレームワーク（OECD）	デジタルアイデンティティエコシステム内での信頼を促進する目的で、デジタルアイデンティティソリューションプロバイダーが従う共通要件の集合。要件は保証レベル（LoA）ごとに分類することができる。
資格情報発行者（OECD）	公共・民間を問わず、ユーザーに資格情報を発行するあらゆる主体を指す。
難民（1951年国連難民条約）	人種、宗教、国籍、特定の社会的集団への所属、または政治的意見に基づく迫害を受けることに対する十分な根拠のある恐れにより、出身国へ帰還することができない、または帰還を望まない者。

図1：人権関連のアイデンティティ

巻末の注参照[14、15、16、17]

第1部：アイデンティと政府の役割

背景

政府及び政府間組織は、以前から政府目標の発表、個人の権利の擁護、社会全体のダイナミクスの支援において人を識別することが果たす需要な基本的役割を認識してきた[18]。具体的には、法的身分証明は、国家が個人を認識し、その法的地位（ボックス1参照）に基づいて基本的ニーズを満たすサービスを提供する基盤を形成する[19]。住民登録に関する法と手続きは、この法的身分証明を支える基盤を提供する。多くの社会的人道的成果の実現可能性と、人権を保障する法的な承認の重要性を踏まえ、国連は2030年までに世界が法的身分証明持てるようにするという、持続可能な開発目標（SDGs: Sustainable Development Goals）を設定している（SDG 16.9）。
世界銀行によれば、現在の法的権利のギャップは少なくとも8億から10億人に達している[20]。ただしこの数値は、登録されてはいるが十分な書類を持たない人々を見落としている可能性がある。

ボックス１：法的地位

政府は法的地位（例：出生登録時の市民、適正手続きを経た亡命希望者または難民）を付与する。法典はその地位に基づき権利、義務などを規定する。

本稿では「法的地位」という用語は、市民的地位、国籍上の地位、難民、無国籍者、その他政府が付与し得る地位を包括する概念として用いる。

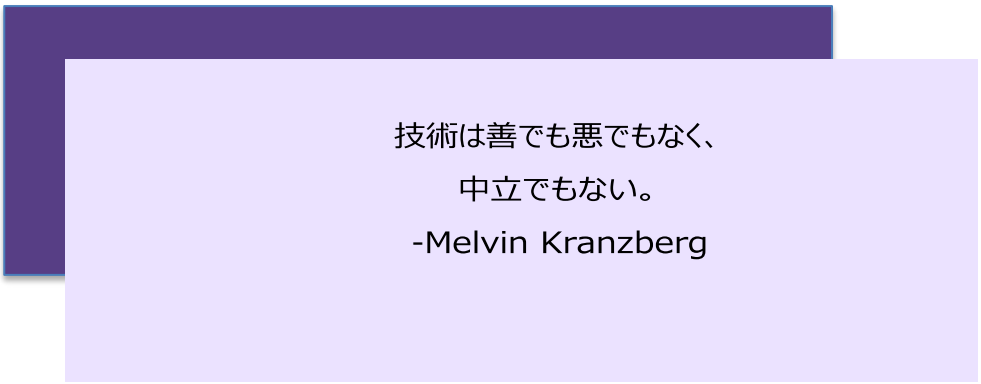
こうした社会的、人道的目標達成への期待により、世界各地で政府主導による取り組みが多数立ち上げられており、多くの取り組みでデジタルアイデンティティ技術、ソリューションおよびシステムが注目されている。しかし、法的身分証明の研究者であるBronwen Manby博士の2021年の論文が指摘しているように、全ての施策が同じ目標や方針を有しているわけではない[21]。政府の目的は、安全保障、安定性と国土強靭化を経た成長に至るまで多岐にわたっている。主権を有する政府とその所属機関の目標は多岐にわたるだろうし、政府に助言する非営利団体や民間企業も同様であろう[22]。**表1**に、多様な目標達成のためデジタルアイデンティティ技術を提案する、政府主導の研究および計画事例を示す。

表1：政府によるアイデンティティ施策で認識されている利点

	政府の動機	研究と取り組み
機会へのアクセス	**経済的関与と生産性** カウンターパーティの信頼により経済活動が可能になり、包摂性を支援し、コスト(詐欺など)を削減	McKinseyは、本人確認(デジタルIDを含む)へのアクセスがGDPの3-13%の成長をもたらすと推定
	金融安定性 デジタルアイデンティティが国際的な資金移動を支援し、麻薬、武器、人身売買などの不正な資金の流れに対抗	FATF(金融活動作業部会)は、信頼性の高い独立した本人確認システムが金融包摂の促進と不正な資金の流れの阻止を支えると主張
政府リソースへのアクセス	**行政サービス** 市民が受給資格のある行政システムへのアクセスを確保。詐欺を削減し、効率的なサービス提供を実現	世界中の文化的に適切なアプローチが多数存在(Part 2参照)
	給付と支援 市民、難民、亡命希望者、危機時の事実上の無国籍者を支援	Bill and Melinda Gates Foundationの報告によると、パキスタンの生体認証対応NADRAプログラムにより、女性が現金給付を受け取りやすくなった
国家安全保障	**サイバーセキュリティ** 堅牢なアイデンティティ&アクセス管理が、政府システム、サプライチェーン、国家の基盤インフラのサイバーセキュリティを支える	EU Cybersecurity ActとBiden政権のNational Cybersecurity Strategyは、デジタルアイデンティティを重要な実現要素として位置づけ
	物理的セキュリティ 市民、非市民、悪意ある行為者を識別することで、政府が物理的セキュリティを提供可能に	米国国土安全保障省は、航空旅行の安全性向上の取り組みとしてモバイル運転免許証(mDL)を挙げている
	政治的安定性 詐欺や誤情報が民主的プロセスに不安定化をもたらす	2023年、エストニアの有権者の50%以上がデジタル投票を実施 多くのアフリカ諸国(ナイジェリア、ガーナなど)が選挙の安全性確保のために生体認証を活用

巻末の注参照[23、24、25、26、27、28、29]

前述したように、表1, に示した多様な動機に加え、すべての人に法的な身分証明を与えるという目標（国連SDG 16.9）[30]も相まって、多くの政府が近年の技術革新を活用し、デジタルアイデンティティの資格情報、システム、およびエコシステム (主な用語参照) の構築を目指す動きが加速している。



あらゆる技術には、肯定的と否定的な結果が生じる可能性がある。デジタルアイデンティティの場合、技術は、特定の国家が法的身分証明に対して採用している手法（法的、手続き的、技術的）に既に存在する何らかの人権に否定的な影響を増幅させる力を持つ[31]。さらに、あらゆる技術は必然的に、たとえその価値観が明示的であれ、暗黙的であれ、あるいは無意識的なものであれ、結果に影響を及ぼす一連の価値観を内包している[32]。

表1に示した多くの取り組みは批判の対象になり、担当者が対処すべき重大なリスクを伴う。例えば、デジタルアイデンティティシステムが社会に広く浸透するにつれ、サイバーセキュリティインシデントの影響には、大規模なセクター横断的な機能停止や、悪意あるアクターへの膨大な量の個人データの流出が含まれることが考えられる。このようなレベルのサイバーセキュリティインシデントは2018年にインドのAadhaarシステムで発生し、史上3番目に大きなサイバーセキュリティインシデントとなった[33]。その他のこれまで知られているアイデンティティシステム侵害インシデントは、世界中で発生しており、しかも国によりアーキテクチャが異なっている（例：アルゼンチン[34]、ナイジェリア[35]、韓国[36]、エストニア[37]、オーストリア[38]）。生体
技術の収集・保存・利用が拡大するにつれ、必然的に安全でない、あるいは脆弱なソリューションの影響も拡大する。個人が虹彩や顔の輪郭、指紋を置き換えるよりも、数字列を置き換える方が容易なのだ[39]。デジタルアイデンティティシステムが膨大な個人データの「門番」として機能する中、こうした侵害は個人への広範な被害をもたらし、大規模なデータ損失や詐欺が発生すれば社会全体に及ぶ可能性がある。

政府とその協力者は、デジタルアイデンティティデータの取り扱い方次第で、さらなる被害を引き起こす可能性がある。倫理的な配慮を欠いたデータ処理が大規模に行われた場合、影響は社会全体に及び、意図せず人権を損なうことにもなりかねない[40]。この倫理的な配慮を欠く処理には、人々の生活に影響を与える偏ったアルゴリズムによる判断（例：保険、雇用、賃貸契約等の重要な決定に影響する保護特性）やその他の形式の社会的操作が含まれる[41]。

歴史上、法的身分証明システムにより可能となった意図的な人権侵害の事例は数多く存在する。これには、市民の監視、選挙権の剥奪、追放、国籍の剥奪、あるいは虐殺を実行するためにアイデンティティデータを悪用した事例が含まれる。現代史の事例としては、ミャンマーにおける身分証明書の利用によるロヒンギャ民族の追放と国籍剥奪[42]、米国における黒人や先住民の有権者の選挙権剥奪を目的とした身分証明取得の意図的制限[43]、インドのアッサム州における100万人超の市民権剥奪[44]、ドイツ第三帝国及びドイツ民主共和国政権による過剰なデータ収集の影響[45]がある。こうした被害が意図的な政策、政権交代、あるいは不十分な内部統制の結果によるものかは様々だが、制度設計者はそれらの可能性を考慮に入れざるを得ない。さらにこれらのリスクの発生確率と影響は技術によって増幅される可能性があるため、人権団体は以前から国連や世界銀行などの組織が推進する善意のデジタルアイデンティティソリューションの潜在的な悪用について懸念を表明している[46]。

普遍的に適用できる単一の政府モデルが存在しないように、単一のアイデンティティシステムがどこでも機能するわけではない。国とその国民には、適切な解決策に影響を与える独自の歴史、社会的構造、政府への期待、文化がある[47]。しかしながら、本稿は学際的な文献に基づき、歴史に根ざし、人々の関係性や社会的文脈を考慮して、現実のニーズに応えるように設計・構築されたアイデンティティシステムこそが、より持続可能であり、社会に一層大きな利益をもたらす可能性があると論じる。

本稿の意義

具体的な社会的利益実現への約束によって推進され、数多くの技術的進歩に支えられて、各国政府はデジタルアイデンティティシステムを構築または再構築する野心的なプロジェクトに着手している。しかし、このようなわかりやすい言い回しには膨大な量の複雑さが含まれている。「政府」という用語は、アイデンティティシステムに関与する多くの層、機能、機関の存在を隠している。本稿はそれらすべてを対象としている。

個別の主体による行動がエコシステムに予期せぬ影響を及ぼす可能性があるため、広い視野が不可欠である[48]。前述の通り、公共部門のあらゆる主体（個々の公務員、機能単位とその協力者、あるいは組織全体を問わず）は、政府のどの層（超国家的、国家的、地域的、地方的）にあっても、アイデンティティに関する独自の視点、すなわち、法的身分証明（および関連する証明事項）または資格情報の発行、法的身分の付与または定義（該当する場合）、属性の管理、認証、およびアクセスとアクションを承認する活動に関して、独自のアプローチを有する。それらのシステムは往々にして、コミュニケーション能力、すなわち当事者間の信頼を確立し、個人が特定の権利を有することを検証する能力を必要とする。多くの公共および民間セクター主体がこのエコシステムに対して正当な利害関係を持つ。小さな構成要素やプロトコルは、それぞれ、無数の技術的・政策的・ガバナンス上の決定によって形作られる。前述の通り、このような複雑なネットワークにおける決定はそれぞれ、ある価値体系を支持し、あるいは生み出すものである。

行政にオンラインで個人を識別し認識する一貫したアプローチを含む包括的な戦略が欠如すると、市場主導のソリューションが台頭してくる。しかし、これらは機能が限定的である。近年の米国史におけるこうした傾向を分析した業界団体Better Identity Coalition （BIC）は、オンライン上で “その人が本当に本人か” を確実に確認できる検証可能な情報に対するニーズが満たされなかった結果、プライバシーやデータセキュリティ上の弱点（魅力的なデータプール、ソーシャルエンジニアリング攻撃の足掛かり、ユーザーの行動に対する様々な追跡手法など）を持つ市場主導型ソリューションが、十分なチェックがされないまま台頭してきた経緯を明らかにしている（図2参照）[49]。脆弱性、社会的ニーズ、そして責任の分散という多様性を考えると、個々の公務員が直面する課題は理解できる。しかしこれは、Windley（2023年）がいう「フィッシング攻撃、詐欺、複雑性、摩擦は、人間がアイデンティティソリューションにどう関与するかを考慮しなかった結果である」と言える[50]。

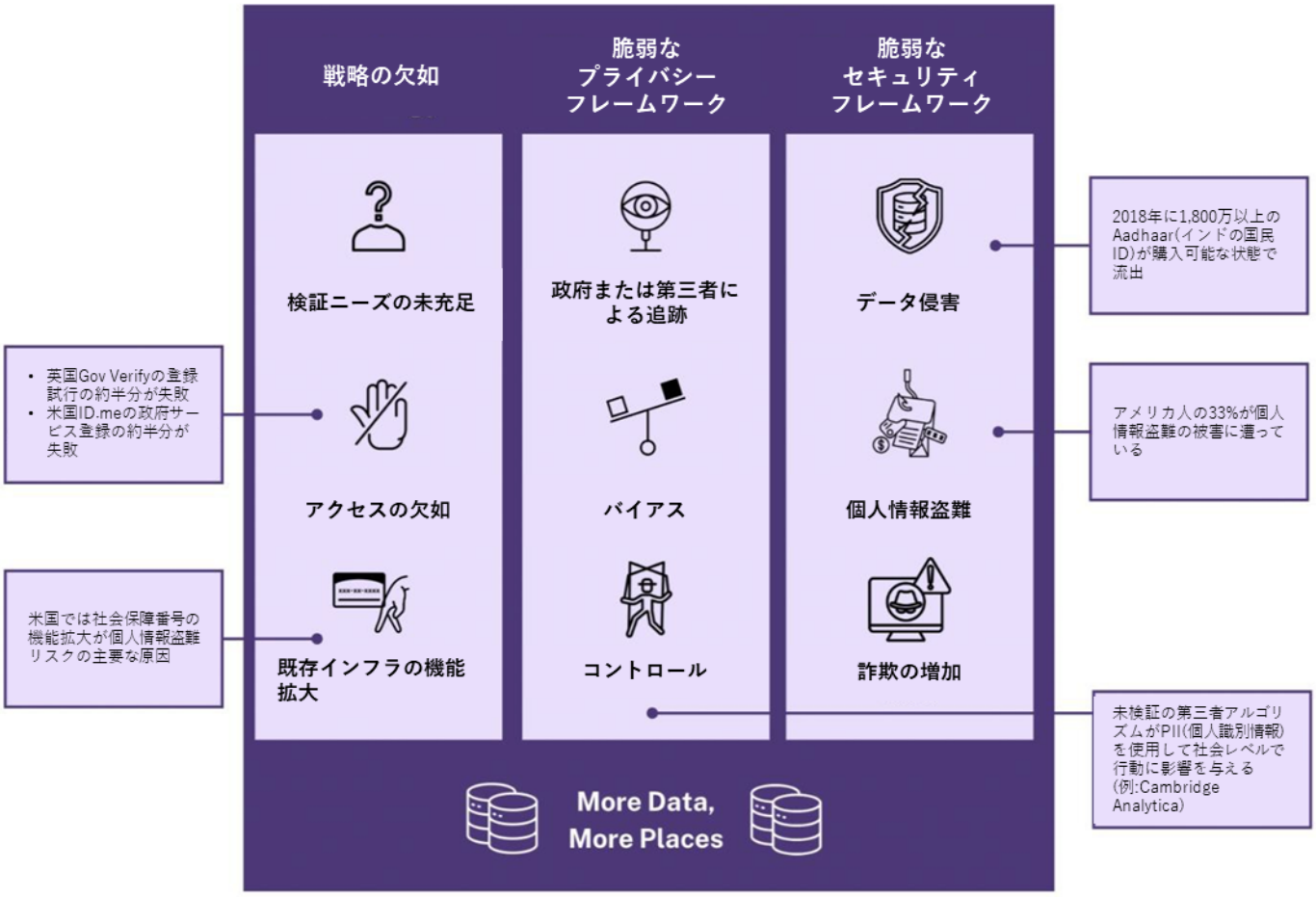


図2：脆弱なデジタルアイデンティティ戦略の意図しない結果

巻末の注参照[51, 52, 53, 54, 55, 56, 57]

脆弱なデジタルアイデンティティ戦略に起因するとされる弊害の多くは、未成熟な法制度、規制、あるいはその他のガバナンスのフレームワークに根本原因があることが多い[58]。図2のデータポイントは、戦略的なギャップが単に技術的な性質のものだけではなく、むしろ制度的文脈によって可能になったり悪化したりし、さまざまな形態の被害をもたらす可能性があることを示している。被害には、行政サービスの利用低迷[59]、政府が保有する個人情報の漏洩[60]、個人データベース侵害による身元情報盗用[61]、選挙干渉[62]、政府による（過度な）監視[63]などが含まれる。法的フレームワークの欠如は、損害が発生する状況を作るだけではない。プライバシーやセキュリティを専門とする法律学者は、情報漏洩に関するセキュリティ法のような[64]単純に組織単位の成果に焦

点を当て起草された法律は、組織が社会全体に悪影響を及ぼすような個別行動をもたらすと主張している[65]。これらの教訓は、あらゆるデジタルアイデンティティシステムにとって重要であり、特に民間セクターの参加者を巻き込んで、政府システム内のデータへのアクセスを可能にするシステムにおいてはなおさらである。

デジタルアイデンティティシステムの設計において、政府関係者はハイリスクで複雑な領域を調査している。本稿は、既存の学際的な関連文献の詳細なレビューにより作成されており、上記のような状況にある関係者のためのリソースを提供する。本稿のグローバルな範囲は、多くの正当なアプローチが共存するという前提に基づいた「万能型」アプローチを意味するものではない。むしろ、多くの課題が共通したものであり、国内および国境を越えた協力が必要であることを示唆している。第2部では、今日の政府が運用するシステムにおけるデジタルアイデンティティパラダイムを背景に、これらの課題を調査する。
第3部では、原則に基づいた既存の文献を統合し、国内に適応しつつ国境を越えて相互運用可能な、人権を尊重するデジタルアイデンティティシステムの構築に、政府がどう取り組むべきかについての議論を深める。これらの知見を得るため、著者らは北米、欧州、アジア、英国、アフリカの各政府機関および非政府組織の代表者へのインタビューを実施した。

人々にとってのデジタルアイデンティティシステムの意味

本稿は政府関係者向けだが、人の権利を尊重するデジタルアイデンティティシステムを実現するには、人と社会を軸に据える必要がある。「アイデンティティ」という用語自体、多義的であり、文脈によって異なる意味を持つ。社会科学者が用いる概念は、コンピュータ科学者やシステム管理者が重視する概念とは異なる。一方では、「アイデンティティ」は具体的な財産形態をとり（「私のアイデンティティが盗まれた」のように）、他方では、特にデジタル領域では、流動的で絶えず変化し、動的な関係性に依存する[66]。こうした相互依存的な「アイデンティティ」の概念は、それなりに正当な目的を果たす。本稿において「アイデンティティ」とは、個人が自分は誰かを他者に伝えるあらゆる方法を指す。個人は複数の相手に対して、自らのアイデンティティの異なる側面（時には競合し矛盾するものさえ）を正当に主張する選択が可能である。しかし「アイデンティティ」は他者との関係性の中で生じるため、相互依存的な意味合いを持つ。それは同時に、ある当事者が他者を認識する方法でもある[67]。

法的身分証明は、特に、個人が政府やその他の当事者から認識されることを可能にする。また権利、特権、アクセス権、説明責任の基盤を形成する。法律には、個人が法的地位に基づいて主張できる権利と特権について書かれている。
例えば、市民として認識されると保護され、権利（投票や福祉など）が与えられ、地域内の移動、資源へのアクセス、経済活動への参加が可能になる[68]。持続的な法的身分証明へのアクセスがなければ、法的地位の主張に苦労し、教育、医療、金融サービス、あるいは日常生活の他の多くの側面で排除されることが多くなる[69]。

デジタルであるか否かにかかわらず、アイデンティティシステムは全ての人々に等しく機能するわけではない。前述の通り、デジタル技術への移行は既存のアナログシステムにおける格差や人権問題を深刻化させる可能性がある。人にはデジタルアイデンティティシステムを利用する能力（または意欲）に影響を与える、異なるアクセシビリティに対するニーズや好みがある。例えば、携帯電話はより広範な包摂の機会を創出する一方で、一部の人々にとっては障壁となる。その使用を義務化することは、視覚障害を持つ人々、学習上の差がある人々、携帯電話を持たない人々などを排除する可能性がある。また、アーンスト・アンド・ヤングの「Connected Citizen Report」で概説されている「プライバシー擁護者」群のように、単に政府に自身のデータを預けることを信頼しない人々も存在する[70]。

こうした個人差に加え、デジタルアイデンティティシステムの設計では、生涯を通じて生じ得る大きな状況の変化も考慮しなければならない。これを怠ると、社会の主流から取り残された脆弱な集団に甚大な被害をもたらす恐れがある。例えば、英国ではアイデンティティおよび認証管理と連携した医療通知システムが、意図せず家庭内暴力の加害者として元パートナーや子供の追跡を可能にしてしまった事例がある[71]。

図3：アイデンティティおよびデジタルアイデンティティシステムにおける高リスク関係者

巻末の注参照[72]

第2部：現代のデジタルアイデンティティパラダイムでは、現在存在するデジタルアイデンティティシステムの種類を調査する。これらのエコシステムを検討するにあたり、システムの実装が様々な社会集団や前述した事例などの関係をどのように支えているか、あるいは損なう可能性があるかについて検討することは価値がある。本稿で

は一定の分析を提供するものの、国際的または特定の地域内における利害関係者やリスクに晒されているコミュニティに関する詳細な検討に代わるものではない。

第2部：現代のデジタルアイデンティティパラダイム

文化、インフラ、制度的準備状況、政治構造、経済的インセンティブなど、様々な要因の違いにより、世界各地で多様なデジタルアイデンティティシステムが生まれている。その他の文化的要因の中でも、各国の戸籍制度と法的身分証明の歴史は現在の状況と、デジタルソリューションがそれを補完する適切な方法を決定づけている[73]。

2016年、Consult Hyperionはデジタルアイデンティティシステムの基本形に関する詳細な分析を発表した[74]。本章ではこの研究を根拠として、その後の市場構造の変化に関する情報と微妙な差異を追加する。特に、最新の図表は市場が両極で進化したことを反映しており、生体認証とウォレットベースのモデルが著しい進展を遂げている。以下のセクションで、これらのモデルの性質と、代表的な実装例に関する簡潔な考察を併せて探求する。

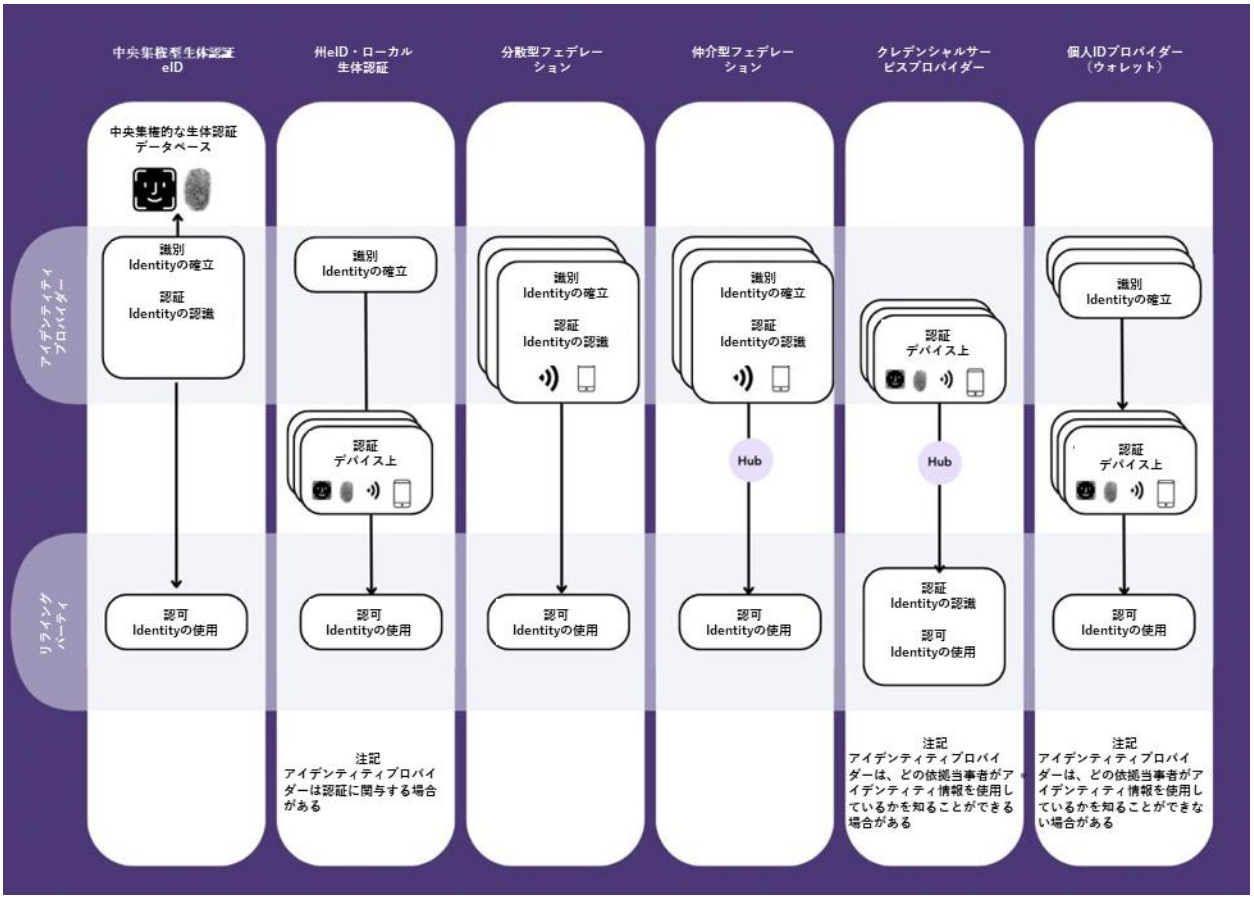


図4：デジタルアイデンティティアーキテクチャモデル

図4はConsult Hyperionの「デジタルアイデンティティ課題分析」（以下に説明）を参照している[75]。

本稿の冒頭で定義した「デジタルアイデンティティシステム」には様々な解釈が可能だが、「デジタルアイデンティティ」という用語がこれらのパラダイム間で異なる意味を持つことを認識することが重要である。最も重要な違いは、あるモデルではデジタルアイデンティティが政府によって発行・承認されるのに対し、他のモデルでは、政府発行の証明書に含まれる法的身分証明書の検証を経て、民間事業者によって作成されるという点である。本稿の目的に沿った「デジタルアイデンティティシステム」は、個人が自身の法的身分証明に関連した情報（必ずしも同一ではない）をデジタルで主張するという形式も包括する。

図4には、多くの技術的な細部の違いが含まれている。主な相違点は、アイデンティティプロバイダーの性質、生体認証の利用（特に認証における利用）、中央ハブの有無、そして「ウォレット」とも呼ばれることが多い**個人IDP**（個人用アイデンティティプロバイダー）の存在に関わるものである。デジタルアイデンティティシステムは多くの場合、政府が発行する基盤（アンカー）としての資格情報に依存している。このアンカーは、スマートカード内の電子要素や、パスポートなどの物理的証明書に埋め込まれたチップの形を取る場合がある。インドやウガンダ[76]などでは、政府が集中管理する生体認証データを利用して本人確認を行うことで、同一人物が複数の資格情報を用いて政府サービスを利用する可能性を抑止している（「**中央生体認証付きeID**」）。一方、他のシステムでは、生体情報はユーザーの手元に保持され、スマートカードやモバイルデバイスなどに格納される（「**国家型eID**」および「**個人型IDP**」モデル）。

さらに、ノルウェー[77]やカナダ[78]などでは、個人およびその政府発行書類の厳格な審査を経て発行される民間の資格情報を基盤としたデジタルアイデンティティシステムが発展している（「**分散型フェデレーション**」）。これらのシステムでは、さまざまな認証方式を採用する複数のフェデレーション型アイデンティティプロバイダーが分散して存在している。これらのプロバイダーは、トラストフレームワーク内で定められた法的・規制的なフレームワークの下で、生体認証データの収集、保存、利用に関する判断を行っている。また、ユーザーが中央のステートレスなハブ（「**仲介型フェデレーション**」）やマーケットプレイスを介して、ユーザーが多数の安全なアイデンティティ／認証プロバイダー（「**資格情報サービスプロバイダー**」）の中から選択できる仲介型市場を構築しようという動きもある。さらに、分散型アイデンティティ標準が成熟するにつれて、政府は「**個人型IDP**」やウォレット型のエコシステム構築を進めている。このモデルでは、政府機関や各種の資格情報発行者が相互運用可能なウォレットに電子アイデンティティ（eID）を発行し、ユーザーはそれを用いてさまざまな場面で身元を証明できる[79]。理論上、ウォレットには複数の政府発行または民間発行の資格情報を保持できるため、前述のeIDモデルとは異なる特徴を持つ。

図4では、これらのアーキテクチャモデルを「中央集権型」から「非中央集権型」といった単純な尺度で配置していないことに留意する必要がある。そのような分類は、現実の構造を過度に単純化してしまうためである。各モデルでは、資格情報発行者と、監査などの目的でデータを保存する必要のあるリライングパーティ（または検証者）の双方のデータベースに、多量のアイデンティティ情報が格納されている。また、データの保存場所や認証の実装に関する技術的な選択、およびどの当事者がデータを閲覧・修正・管理できるかといったガバナンス上の選択も存在する。例えばウォレットベースのモデルでは、ウォレットプロバイダー（例：デバイスメーカー）が資格情報を閲覧、保存、失効または管理できる範囲は、ポリシーによって定められる。技術的設計は、それらのポリ

シーを遵守するように構築されなければならない。逆に、利用可能なアーキテクチャの特性やリスクに応じて、ガバナンスおよびポリシーを策定する必要がある。

Consult Hyperionの報告書は、図4に示された各モデルについて、脆弱性、脅威、実行可能な軽減策の観点から分析し、いずれのモデルにも不適切な実装や悪用の可能性が存在することを指摘している[80]。表2はこの分析を踏まえ、追加的なリスクおよび軽減策を提示するとともに、アーキテクチャの違いによっては共通の脆弱性があること、またトレードオフの判断における重み付けが異なることを説明している。

表2 - アーキテクチャモデルと関連リスク／軽減策

	主要な脅威	緩和策
中央集権型 生体認証eID	• 生体認証データの侵害により、取り返しのつかないID盗難につながる • 政府による監視が可能になり、過度なデータ収集が行われる • 第三者データ受領者による利用者追跡が可能になる • 悪意のあるRP（Relying Parties）に個人情報が渡される	• セキュリティ基準に生体認証保護（例：バイオハッシング）を含める • 強力な法的枠組みにおけるデータ最小化とプライバシー保護 • 第三者に渡される一意の識別子 • RP（RP）のルール、管理、監査/執行の実践を設定
ローカル 生体認証eID	• 過度なデータ収集による政府監視が可能になる • データ侵害 • 第三者データ受領者による利用者追跡が可能になる • 悪意のあるRPに個人情報が渡される	• 強力な法的枠組みにおけるデータ最小化とプライバシー保護 • ガバナンスフレームワークに組み込まれた強力な最小セキュリティ基準 • 第三者に渡される一意の識別子 • RPのルール、管理、監査/執行の実践を設定
分散型 フェデレーション	• 悪意のあるRPに個人情報が渡される • IDPによる不適切なプライバシー慣行 • IDPでのデータ侵害 • IDPのプライバシーとセキュリティに関する消費者の選択が不明確	• RPのルール、管理、監査/執行の実践を設定 • データ保護基準（技術を含む）、執行、契約 • ガバナンスフレームワークにおける強力な最小セキュリティ基準 • 強力な最小基準とガバナンスと結びついた透明性
仲介型 フェデレーション	• ハブのアーキテクチャが追跡のリスクを生み出す • 悪意のあるRPに個人情報が渡される • IDPによる不適切なプライバシー慣行 • IDPまたはハブでのデータ侵害 • IDPのプライバシーとセキュリティに関する消費者の選択が不明確	• ハブはステートレスであり、データを保存しない必要がある • RPのルール、管理、監査/執行の実践を設定 • データ保護基準（技術を含む）、執行、契約 • ガバナンスフレームワークにおける強力な最小セキュリティ基準 • 強力な最小基準とガバナンスと結びついた透明性
クレデンシャル サービス プロバイダー	• ハブのアーキテクチャが（ハブによる）追跡のリスクを生み出す • 認証のみでは本人確認が容易にならない • トリプルブラインドモデルでは、発行者と検証者が互いを信頼しない可能性がある • システム内のプロバイダーの種類に包摂が限定される	• ハブはクレデンシャルがどこで使用されたかに関するデータを保存してはならない • エコシステム内の他の場所での本人確認のための最小基準 • 強力なガバナンスフレームワークと執行モデルを整備 • 包摂を促進するために多様なプロバイダーを確保（銀行だけでなく）
個人 IDプロバイダー （ウォレット）	• エコシステム内のすべての当事者（発行者、保有者、ウォレット、検証者、RP、オンチェーン/オフチェーン、ユーザー）間で信頼を確立することが困難であり、プライバシーと安全性の慣行を理解する必要がある • エンドユーザーが秘密鍵を記憶/維持することに依存	• 当事者間の信頼を確立、維持、取り消すためのスケーラブルなモデルを開発 • 法律で支えられた強力な最小プライバシーとセキュリティ基準 • 安全な復旧オプションと代替手段を提供

Consult Hyperionのデジタルアイデンティティ課題分析[81]より改編

このConsult Hyperionの報告書のリスク軽減策は、プライバシーと人権保護を促進するという目的を前提としている。また、保護策を定義・統制・執行する制度的フレームワークが、技術的実装と並行して成熟することを要求する。

したがって、グローバルな基本形を理解するには、アーキテクチャモデルとガバナンス類型を合わせて分析する必要がある。

シンガポール金融管理局は、完全な**民間ガバナンス**から完全な**公共ガバナンス**まで、4つのガバナンス類型（図5）を明確に示している[82]。これらモデルの間には、民間コンソーシアム、**政府主導型ガバナンス**、**官民共同ガバナンス**モデルなど、さまざまな程度の協力関係が存在する。

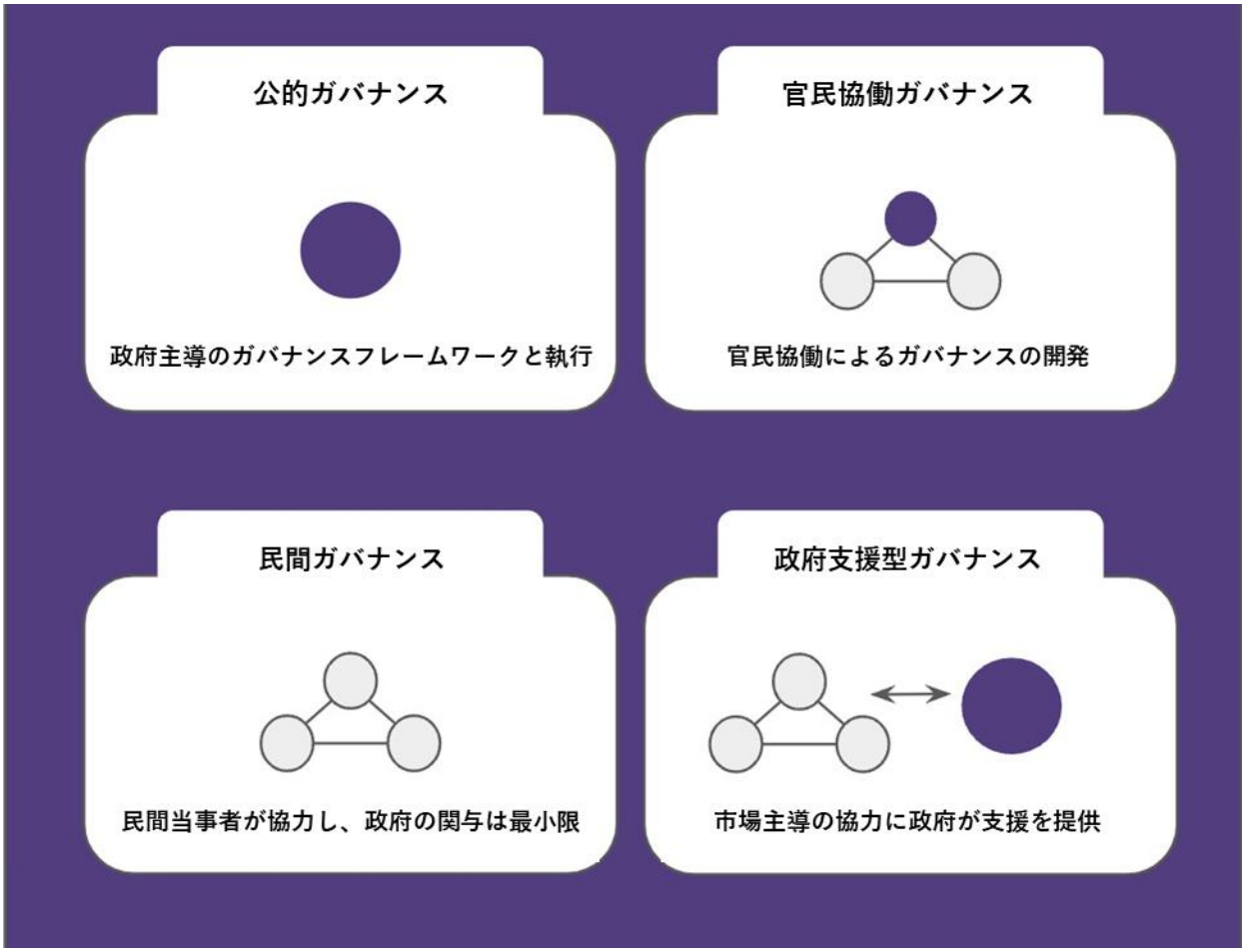


図5：ガバナンス類型

より厳密かつ詳細なトラストフレームワークの比較については、OIX – A Guide to Trust Frameworks for Smart Digital ID[2] [83]を参照されたい。

なお、前述の技術アーキテクチャモデル（図4）が自己完結型のデジタルアイデンティティシステムを記述しているのに対し、上記のガバナンスモデルの類型（図5）は、単一システムから複数のエコシステムが相互作用するネットワークに至るまで、複数のレベルに適用可能である点に留意されたい。ただし、ガバナンスと技術を組み合わせることで、興味を引く一連のパラダイムが浮上する。

2 （訳注）Open Identity Exchangeは2026年1月現在、運営を停止している

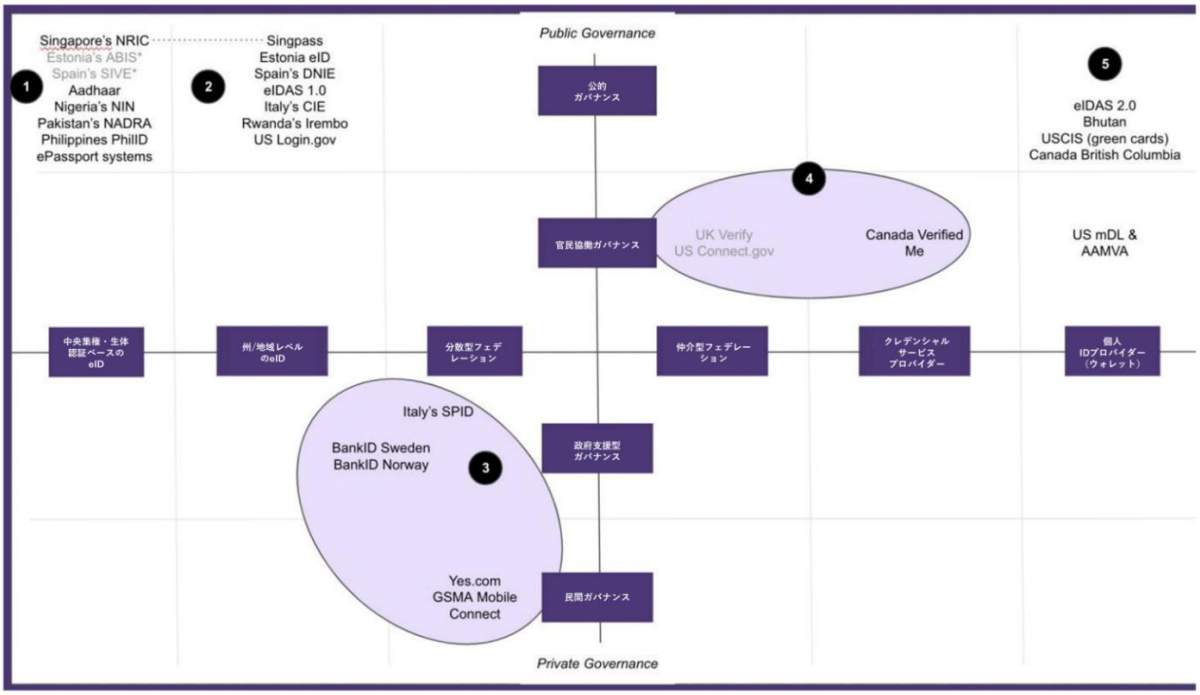


図6：デジタルアイデンティティパラダイム – 技術とガバナンス

以下のセクションで、上図で示した5つのパラダイムを検討する。

パラダイム1と2：政府発行のeID

政府公認スキームの大半は、完全な公共ガバナンスに支えられた電子アイデンティティの基本形に該当する。ただし生体認証データの取り扱いにおいて、多くのスキーム間で顕著な技術的差異が存在する。パラダイム1は、インドのAadhaarや世界銀行主導の多くの新興開発プログラムモデルに代表され、生体情報の収集と遠隔保管（本稿では「集中管理」と定義）を伴う。この生体情報の保管により、政府は各個人が1つのIDのみを有し、資源（例：給付金）が常に適切な対象者に届くことを保証する。

また、個人は紛失・盗難にあった身分証明書をデータベースで照会できるため、再度取得することができる。この意味で、政府の中央生体認証データベースが認証機関として機能することが求められる。つまり政府はそれらの属性がどこで使用されたかを把握できるようになる。したがってこのアーキテクチャでは、データの損失や潜在的な監視の影響を防ぐため、プライバシー規則とデータセキュリティ対策の強化が必要となる。

一方、シンガポールのSingpass[84]、エストニアのeID[85]、およびパラダイム2に代表されるその他のアーキテクチャでは、通常、ローカルな生体認証ストレージが採用されている。つまり、生体情報は、ユーザーが管理するデバイスまたは機械読み取り可能なカードに保存される。後者の場合、政府が取引において「アイデンティティプロバイダー」の役割を果たす場合でも、認証（ユーザーがそのアイデンティティに対応する唯一の人物であることの証明）はローカルデバイス上で行われる。このような場合、政府が個人のアイデンティティ使用状況を把握できる範囲に一定の制限が設けられる。

重要な点は、図6が示すように、個人が有するローカル（デバイスまたはスマートカード）生体認証への依存が大きいデジタルアイデンティティシステムを採用している政府の多くは、市民および／または非市民の生体データを保存するアイデンティティシステムも維持していることである。シンガポールのNRIC、エストニアのABIS、スペインのSIVEシステムがこれに含まれる。戦略的かつ効果的に実装すれば、システム間の境界や日常生活で個人が使用するデジタル識別子により、アイデンティティデータの機密性と整合性を維持することができる。

しかし、システム間、特に新興システム間の境界は必ずしも明確ではなく、法的に規定されているわけでもない。法的基盤やトラストフレームワークの構築がデジタルIDの技術的実装に遅れをとっている国（インド[86]、ナイジェリア[87]、ウガンダ[88]など）では、プライバシー擁護団体が重大な損害を指摘している。この格差は、米国が社会保障番号を導入した際、その使用に関する十分な法的制限を設けなかった結果、アイデンティティの盗用が発生した事例[89]と似ている。こうした制度的フレームワークが成熟しない限り、人々は監視やその他の被害に晒されるリスクがある。法的・制度的フレームワークの詳細については、3.2節を参照されたい。

INインド、Aadhaar[90]

概要	Aadhaarは世界最大のデジタルアイデンティティシステムであり、インド経済の多くの側面を支える多層構造のもとにある[91]
法的身分証明との関係	Aadhaarはインドにおける個人の一意性と居住を証明するものである。特定の法的地位に伴う権利を保証するものではない。
実装機関	インド固有識別番号庁（UIDAI） 2018年最高裁判所によるAadhaarの使用に関する判決[92]
実施年／成熟度	2009年 – 高度に成熟した技術；市民・機関による高い採用率；民間セクター全体での広範な適用。未成熟な制度的フレームワークでの実施。UIDAIは依然として自己規制機関として機能している[93]。
規模	12億件
生体認証	あり – 中央保管の指紋、顔テンプレート、虹彩スキャン
提供サービス	政府サービス全般で利用可能 2018年の最高裁判決の範囲内で、民間企業はAadhaarを基盤としたAPIを利用して以下が可能： - 金融サービス商品の提供 - 電子署名の取得と確認 - モバイル口座保有者の確認 - KYC（本人確認）の実施 - 従業員の認証
標準およびプロトコル	XML API[94]（Aadhaarプロトコルの多くは自社開発）
主な特徴	99%超の成人が登録済み 州政府は9年間で2兆ルピー（240億米ドル）を節約[95]
課題	• 過去に類のない規模のデータ漏洩[96] • 政府による監視の報告[97] • 偽ID作成の報告[98]

NGナイジェリア、国民識別番号（NIN）[99]

概要	国家アイデンティティ管理委員会（NIMC）は、2007年NIMC法第23号により設立され、ナイジェリアの国家アイデンティテデータベースの運営、同法対象者の登録、固有の国民識別番号（NIN）の割り当て、および汎用多目的カード（GMPC）の発行を行う。
法的身分証明との関係	NINは全国民が必須であり、個人の一意性と居住地を確立する。NIMCは人に関するあらゆる情報を結合し、それにより「個人のアイデンティティを確立・検証する」。したがって、法的地位の記録にも使用される可能性がある。
実装機関	NIMCはNINシステムの運営・統治を担う データプライバシー法は2023年7月に成立した[100]
実施年／成熟度	2007年 –技術情報はAadhaarほど充実していないが、同様の制度的背景（立法・ガバナンス）を有する
規模（個人識別数）	16歳以上の全市民に義務付けられている 2022年12月時点で9,260万件のNINが発行されている
生体認証	あり ー指紋と顔認証。国のDNAデータベースとの連携提案が報告されている[101]
提供サービス	公共、金融、民間サービスなど多様な分野で統合運用。 宿泊、医療、旅行、保険、金融商品、インターネットアクセス、雇用、学術機関、専門機関、福祉、不動産など様々な取引へのアクセスに必須[102]
標準とプロトコル	OSIA仕様に準拠したRESTful API[103] [104]
主な特徴	有権者名簿の精度向上
課題	プライバシーへの懸念による初期段階での（任意の）採用率の低さ[105] SIMカードへのNIN登録の政府による義務化が新型コロナ感染者数の増加につながった[106]

SG シンガポール、NRICおよびSingpass[107]

概要	「Singpassは、日常生活におけるあらゆる安全な取引ニーズに対応する信頼できるデジタルアイデンティティである」
法的身分証明との関係	Singpassは法的身分証明に基づいて国が保証するデジタルアイデンティティであり、「法令により物理的な書類が要求される場合を除き」全機関が受け入れている[108]
実装機関	シンガポール政府技術担当庁
実施年／成熟度	2003年 – Singpass開始 2017年 – NRIC 2018年 – SingpassアプリとNRICの連携 高度に成熟した技術、利用状況、ガバナンス
規模	登録ユーザー数：450万人[109]
生体認証	あり[110] ● NRICでは生体認証登録が必須（顔、指紋、虹彩） ● Singpass登録には顔認証またはMFAが必須。 ● 多くのSingpassサービスは個人のデバイスベースの認証に依存しているが、合法的な目的を持つ公的・民間組織はデータベース照合を行うIdentiface APIサービスを利用できる。
提供サービス	2000種のサービス／700組織。民間セクターは以下のSingpass APIと連携が可能。 ● ログイン ● 認証 ● 署名 ● 生体認証サービス
標準とプロトコル	OAuth2およびDPoP、PKCE、QR（圏外）
主な特徴	● 97%の採用率[111] ● 「MyInfo」サービス利用による申請時間の80%削減[112] ● 1,400以上のデジタルサービスを提供し、340以上の政府機関および民間組織を支援
課題	プライバシーに関する批判も一部存在する[113]

ITイタリア、電子身分証明書 (CIE)[114]および公的デジタル身分証明システム (SPID)[115]

概要	CIE – 電子身分証明書 SPIDは、基礎書類を審査する民間IDプロバイダーのネットワークを通じて公的・民間サービスを接続する公的デジタルアイデンティティシステムである
法的身分証明との関係	CIEは法的身分証明と法的地位を証明するもので、パスポートの代わりに使用される。SPIDは別の法的身分証明形態から派生したものである。
実装機関	GDPRおよびNIS2セキュリティ指令に基づいたデジタルイタリア庁（AGID） による規制
実施年／成熟度	2016年 – 成熟した技術。個人および民間組織によるSPIDの採用率は50%になる。 欧州のGDPR、eIDAS、およびAGIDが維持するフレームワークに基づいた成熟したガバナンス体制である。
規模（個人識別数）	3,000万人／全成人の50%[116]
生体認証	個人のデバイス内で使用される個人の生体認証が許可される
提供サービス	検証済みアイデンティティに対するリライングパーティ（RP） 認定属性
標準およびプロトコル	SAML2 – 現行インスタンス向け OAuth2およびOpenID Connect – 準備中、2023年に展開予定
主な特徴	9社のアイデンティティプロバイダー 導入促進のためインセンティブ制度を導入
課題	現時点で否定的な事例は確認されていない

パラダイム3および4：政府が支援するマーケットプレイス

一部の区域では、政府発行のデジタルアイデンティティ資格情報に加え、政府が民間運営のデジタルアイデンティティシステムの活性化（または調達）を推進している。例えばノルウェー、スウェーデン、フィンランドなど北欧諸国では、銀行ベースのデジタルアイデンティティシステムが銀行の顧客確認（KYC－Know-Your-Customer）プロセスを活用し、広く採用・利用されているBankID資格情報を発行している。政府は様々な用途にこれらのシステムを使用することで支援しており、金融規制当局がその利用を監督している。

北欧のBankIDモデルと同様に、カナダのInteracシステム（旧SecureKey）は銀行レベルの顧客識別に依存している。ただし、その「三重盲検」技術構造により、個人データが中央ハブ経由でRPには伝送されることはない。しかも、既に確立され安全性が証明されてい身元を認証に使用することができる。カナダのモデルはさらに、カナダデジタル識別認証評議会（DIACC）が官民セクターの会員費を通じて資金を調達し、民間業界全体で「Pan Canadian Trust Framework」の開発・維持に取り組んでいるという点で、BankIDとの差別化を図っている。このフレームワークは、カナダのデジタルアイデンティティシステムについて、技術中立的な原則と主なガバナンスに関する勧告を明確にするものである[117]。

その他の政府による支援施策としては、英国のGOV.UK Verify[118]があり、デジタルIDのための連合型または仲介型市場の構築を目指していた。しかし、この種の実装計画のいくつかは目標（特に普及率）を達成できず、内容が再検討されている。

NOノルウェーのBankID[119]

概要	BankIDはノルウェーの全銀行で使用されており、オンライン上で安全かつ簡潔な本人確認を求める組織や企業も利用することができる。
デジタルアイデンティティとの関係	銀行は法的身元確認を行う。法的地位の付与や伝達は行わない。
実装機関	以下を含む、強力な金融規制当局と全国的な法規制のフレームワークにおける民間実装機関（BankID取締役会） - 欧州一般データ保護規則（GDPR[120]） - 電子署名及び信託サービス[121]
実施年／成熟度	2004年 – エンドユーザー間の高い採用率を伴う、高度に成熟した技術。強力な立法と執行機関により支えられた成熟したガバナンス。
規模（個人識別情報）	430万件
生体認証	デバイス固有の生体認証技術（パスキー対応）を導入中[122]
提供サービス	IDPは銀行間で共有される民間事業体が提供。 RPは銀行、政府機関、民間企業。
標準とプロトコル	OAuth2およびOpenID Connect
主な特徴	高い国民の支持率 詐欺の削減率：1%から0.00042%へ
課題	● ノルウェー国外のサービスは利用できず、国際間の利用もできない。 ● 普及率の高さから銀行資格情報の共有が懸念される（デバイス生体認証導入の推進要因となっている）[123]

CA カナダのInteracシステム（旧SecureKey）

概要	Interacは「三重盲検」方式のサインインサービス（資格情報サービスプロバイダー）および検証サービス（国が関与しない中央ハブにより、ユーザーは銀行でログインまたは認証が可能）を提供。
法的身分証明との関係	銀行が法的IDを検証する。法的地位の付与や伝達は行わない。
実装機関	Pan Canadian Trust Framework[124] 個人情報保護および電子文書法（PIPEDA）[125]に基づく
実施年／成熟度	SecureKey Technologiesは2008年に設立され、カナダの全ての大手銀行に口座を持つ大多数のカナダ人にサービスを提供するまでに成熟した。その後、Interacからライセンスを受け、Avast（現Gen Digital）に買収された。
規模	年間2億件の個別取引を処理し、カナダの成人人口の大半を支えている。
生体認証	銀行認証プロトコルを活用
提供サービス	認証を行う認証サービスプロバイダー 本人確認 政府サービスおよび認証済み民間事業体で利用可能
標準とプロトコル	検証サービスは、成熟したBankIDフェデレーションと分散型技術[126]を組み合わせたものであり、Hyperledger Fabric[127]を含む
主な特徴	銀行、ユーザー、政府による非常に高い採用率プライバシー保護技術
課題	現時点で否定的な事例は確認されていない

パラダイム5：新興のウォレットベース型パラダイム

欧州における初期のeIDAS法はパラダイム2に完全に適合していており、その進化形が注目すべき最終パラダイムである。EU域内の相互運用性と市民のデジタルアクセシビリティ確保を目的として生まれたこの新規制は、全加盟国に対し「欧州デジタルIDウォレット」（EUDIウォレット）の発行を義務付ける。これは政府発行の資格情報とその他資格情報の両方を保持できる「個人IDプロバイダー」型のアーキテクチャである。規制当局は、銀行やその他のサービスプロバイダーを含む一定規模以上の民間事業体に対し、これらの資格情報の受け入れを義務付ける方針である[128]。なお、米国や中国の大手テクノロジー企業から登場しているような特定の民間主導型「ウォレット」サービスは、パラダイム5に最も適合する可能性が高く、今後、世界に定着する基準に影響を与える潜在的な可能性がある。

これは、EU全域の法律により支援される最大規模の事例でが、世界でも多くの取り組みが行われている。ブータン王国は、ウォレットベースの国家デジタルアイデンティティシステム（NDI）を開始した[129]。また、北米では、ウォレットベースのエコシステムを構築するための複数の取り組みが進行中である。具体的な取り組みとしては、ブリティッシュコロンビア州政府による市民向けウォレットと検証可能な「個人資格情報」の発行[130]、米国市民移民局（USCIS）によるグリーンカード発行[131]、ISOと米国自動車管理者協会（AAMVA）によるモバイル運転免許証（mDL）の標準化・管理化への取り組み[132]などが含まれる。

これらは全て「ウォレットベース」のエコシステムではあるものの、同一ではない点に留意する必要がある。この分野には多くの新たな基準や技術が生まれている。これらの初期段階のプログラムは信頼の確立、通信プロトコル、データの共有・保存など、重要な差別化による違いを成熟させようと努めている。

さらに、あらゆるシステムと同様、その存在は法的身分証明やプライバシー・データセキュリティなどの保護を付与する特定の国の法的基盤に関連している。

EU 欧州のeIDAS 2.0

概要	EU市民および居住者に調和したデジタルIDとウォレットを提供する[133]。
法的身分証明との関係	eIDASは、加盟国間で法的地位を付与・伝達する法的身分証明システムを基盤とする。
実装機関	eIDAS 1→2 GDPRおよびNIS2セキュリティ指令に基づく eIDAS 2.0の規制は、技術的フレームワークやパイロット事業と並行して進化している。
実施年 / 成熟度	● 未施行[3] / 大規模パイロット事業実施中 / デジタルウォレットの設計・選定に向けた国家レベルの取り組み ● GDPRおよびNIS2に基づく中程度の成熟度。取引相手信頼の確立・維持・失効に関する拡張可能なモデルの開発を継続中。
規模	初期段階 – 数百万のEU市民に影響する4つの大規模パイロット事業を開始
生体認証	生体認証は1対1照合に利用可能
提供サービス	提供される資格情報に依存する様々な配信コンポーネントと機会
標準とプロトコル 詳細はEUのアーキテクチャ参照フレームワークを参照[134]	W3C VCデータモデル[135] OpenID for Verifiable Credentials Issuance[136] OpenID for Verifiable Presentations [137] Self-Issued OpenID Provider v2 [138] ISO 18013-5 (mDL) [139] SD-JWT[140] JSON-LD with LD Proofs (optional） [141]
主な特徴	エンドユーザーによる制御とプライバシーに対する先見的なアプローチ 業界および標準化団体との広範な連携
課題	未提供；内容の多くが検討中

[3] （訳注）2026年加盟国がEUDIウォレットの提供を開始(予定)

US 米国USCISデジタル永住者カード[142]

説明	USCISは米国の合法的な移民制度を管理。検証可能な資格情報として導入と計画を実施中である。
法的身分証明との関係	特定の法的地位に関する（取得後の）法的なアイデンティティ形式。まだ広く使用・受け入れられていない。
実装機関	USCISはグリーンカードを発行し、既存の権限に基づいてこれらのデジタルグリーンカードを発行する。本プログラムを直接規制する国家レベルのプライバシー法やアイデンティティ・トラスト・フレームワークは存在しない。
実施年／成熟度	2023年
規模（個人識別情報）	米国では1,290万人が物理的なグリーンカードを所持[143]しているが、デジタルカードプログラムはまだ稼働していない。
生体認証	デジタルグリーンカードには写真も含む。 グリーンカードを申請する際、申請者の写真と指紋が採取され、政府のシステムに保存される。
提供サービス	デジタルグリーンカードを発行し、国境で受け入れる。これらのカードは、所持者によるその他の身元確認に使用できる。
標準とプロトコル	米国国立標準技術研究所（NIST）ガイドラインW3C VCデータモデル[144] および W3C DID Core[145] VC-APIにより既存の政府システムに接続 クレデンシャルハンドラーAPIによる資格情報の送受信
主な特徴	国土安全保障省の科学技術局は、中核的なDIDおよびVCデータモデル標準開発に資金を提供していた。現在、ベンダー共通の適合試験を支援している。 個人のプライバシー支援 • IDの使用場所を政府が追跡できないアーキテクチャ • 選択的属性開示の実現 • 発行された資格情報の検証者による使用状況を個人が把握できる構造 競争的なエコシステムと個人の選択の支援 • 個人の識別子選択 • 個人のウォレット選択
課題	未提供；内容の多くが検討中

USCA 北米モバイル運転免許証（mDL）

米国自動車管理者協会主導による

概要	米国もカナダも単一の国家アイデンティティシステムはないが、モバイル運転免許証のデバイスウォレットへの組み込みなど、運転免許証の管理基準については協力している。
法的身分証明との関係	運転免許証は政府発行の身分証明書として広く認められているが、法的身分証明やステータスを証明するものではない。
実装機関	AAMVA
実施年／成熟度	米国国立標準技術研究所（NIST）は2016年からmDLパイロット事業を実施している[146] モバイル運転免許証に関するISO規格（**ISO 18013-5**）は2021年8月18日に承認され、同年9月30日に公表された アリゾナ州、カリフォルニア州、コロラド州、ジョージア州、アイオワ州、メリーランド州、ユタ州でTSAが適合するmDL認証を採用している（2023年9月現在）[4]。
規模（個人識別情報）	データなし
生体認証	運転免許証を確認する担当官または職員が運転者の写真を共有する
提供サービス	主に法の執行および航空旅行関連での、運転資格および身分証明書としての使用を目的としている。
標準およびプロトコル	ISO 18013-5 NISTガイドライン
主な特徴	モバイル運転免許証は、特にデジタルおよびアプリ間通信チャンネルで提示される場合、ユーザー体験を向上させる。ただし、対処すべきプライバシーおよびベンダーロックインに関する懸念が生じる[147]。
課題	ISO18013-5 mDL標準は対面提示を規定する。オンライン提示に関する標準（検証可能提示向けOpenIDを定義するISO 18013-7やBrowser API関連作業）は未成熟で支援が必要。一方、一部のウォレットは独自の提示モデルを構築しており、以下のよう懸念が生じている。 ● ベンダーロックイン ● ウォレットプロバイダーによる個人識別情報（PII）へのアクセス・保存・追跡をガバナンスモデルがどう防ぐか ● ブラウザやサードパーティ検証機関によるオンライン上のデータ照合

[4] （訳注）2026年1月時点では10州以上に拡大している。

重要な考慮事項

あらゆる技術と同様、デジタルアイデンティティシステムも誤用・悪用・不適切な実装の可能性を内包している。また、第1部で指摘したように、（意図してもしなくとも）結果を決定づける価値観が内在している。政府は、（本稿が主張する人権の維持と促進を中心とすべき）あらゆるプロジェクトの目標について、リスクや軽減策およびトレードオフを戦略的に追及する必要がある。体系的に考えると、これには様々なユースケース、特に個人や法人がデジタルIDデータの交換に依存する（あるいは依存する可能性のある）リスクが高い状況に対応する設計が含まれる。人々を保護し危害を防止するため、基盤となる法的身分証明システム、政府が発行する機能的なデジタルアイデンティティシステム（モバイル運転免許証など）、政府から得たIDに由来するデジタルアイデンティティシステム（BankIDなど）が、これらの使用例や状況の支援を目的としてどのように連携すべきかを検討することは極めて重要である。

表3：ステークホルダータイプ別トレードオフの目安（網羅リストではない）

ステークホルダー	主なニーズ	トレードオフ
 General Public	• 私のアイデンティティに対応したアクセス権とサービス（法的地位を含むがこれに限定されない） • 信頼性の証明 • アイデンティティ詐称、盗難の防止 • 透明性と監査可能性 • 個人データの管理 • データ収集方法および人間の行動に影響するデータ利用方法に対する広範な保護	利便性とセキュリティ・プライバシーのバランス データの最小化とデータ収集（例：不正対策） データ破棄とデータ保持（例：監査目的）
 Children	• 上記と同様 • 保護者／後見人との対応、委任、および廃止 • その他の被害の防止（例：オンライン上の年齢確認）	データの最小化 と データ保護
 Undocumented & Stateless	• 法的に有効なID • 回復可能なID	包含と管理されたアクセス 包含 と プライバシー・データの最小化
 Family Migration	• 相互運用可能なIDと法的地位の越境認識 • 取消不能な家族関係	相互運用性 と プライバシーおよびデータの最小化 不可逆性と柔軟性
 Under Threat (various contexts)	• 法的地位（難民としての地位など）決定プロセス • 個人に関する機密データ • 個人の日常活動 • アイデンティティ置換	プライバシーとアクセス
 Disability & Carers	• アクセス可能性とサポート • 委任と廃止	プライバシー、アクセス、不正対策がすべて緊張関係にある可能性
 Legal Entities	• 不正対策 • ユーザー確認のためのデータ受信 • データの保護 • 規制への準拠	データ収集・保持（特に不正対策のため）とデータの最小化・破棄

システム内のユーザーの異なるニーズを認識するには、価値観に基づくトレードオフの決定が必要であり、また、特定のトレードオフに伴うリスクを軽減する設計、展開、運用戦略を定義する必要がある。これらの決定では、技術的設計選択に伴う制度的ルールと、それらの管理・執行方法を考慮しなければならない。例えば、アイデンティティの閲覧・保存を制限する法的境界を明文化することで、ネットワーク参加者、技術者、標準設計者は技術的、手続き的に遵守すべき範囲を理解できる。リスク軽減には、技術（および進化する社会文化的規範）に歩調を合わせた法律、執行、ガバナンスフレームワークが不可欠である。

当然ながら、「トレードオフ」は二者択一を意味するものではない。設計者は重点を置くべき領域を決定する必要があり、今日出現している標準と技術は、各スケール内で実装者が利用できる柔軟性と活動範囲を拡大している。しかし、新たなツールが出現すると、脅威もまた出現する。例えば、生体認証の取得精度を高め、保存容量を増加させる技術は、生体認証情報の盗難リスクを高め、人々に前例のない衝撃を与えることも考えられる。付録Aでは、ある領域の進歩が技術的スタックの他の部分に新たな課題を引き起こした事例を示している。
実装者は脅威モデルを継続的に評価し、利用可能な最善の対策を取り入れる必要がある。今日の最も単純な技術的、アーキテクチャ的なリスク軽減戦略には以下のようなものがある。

- 保存時および転送時に可能な限り暗号化を実施する（特に個人を特定可能な情報）
- 生体データを保護するバイオハッシングその他の暗号化処理する（保存する場合）
- 最新FIDO2（およびその進化形）標準への準拠する
- データの相関を回避するため、RPまたはサードパーティごとに固有の識別子を使用する
- 認証用の中央ハブが存在する場合、それはステートレス（状態を持たない）であるべきであり、個人情報を静止状態で保存してはなりません。

次章では、権利を尊重するデジタルアイデンティティシステムの導入において、政府が価値観や原則に基づくトレードオフを判断する指針となる文献を調査・整理する。

第3部：デジタルアイデンティティシステムに関する推奨事項

原則の統一

政府発行の身分証明書および政府主導のエコシステムに関する文献は、本稿の知見と一致するいくつかの主要テーマに集約される(付録B –デジタルアイデンティティ原則の統一参照)。これらの文献は人権と民主主義の理念に基づいており、政府はあらゆるシステムに内在するリスクとトレードオフを慎重に検討する、戦略的で人間中心のアプローチを取るべきであること示唆している。

本稿は特に、2023年の「デジタルアイデンティティのガバナンスに関するOECD理事会の勧告[148]」を支持する。同勧告は関連文献の大半を統合している (付録C – チェックリストとしてOECDデジタルアイデンティティ勧告も参照). 本章はOECDの包括的作業を支える柱に加え、ID2020[149]、世界銀行のID4D[150]、世界経済フォーラム[151]、スマートデジタルIDのトラストフレームワークに関するOIXガイド[152]など影響力があるこれまでの研究からの知見、ならびにDIACCなどの成熟したトラストフレームワークに基づいて作成されている[153]。本稿は新たなフレームワークを構築するというより、むしろこれらの原則に基づくモデルが収束する重要なテーマ（図7）について、より深い関与に向けて具体的な推奨事項を示す。

図7：テーマ別推移章事項とOECDの柱との対応

以下の推奨事項は、政府がこれらの原則を「どのように」実現できるかについての議論を深めるため、最新の文献をまとめたものである。表5にそれらを要約する。

柱1：人間中心

デザインは至る所に存在し、デザインは力であり、デザインは政治的である[154]。

デジタルアイデンティティシステムを通じて人権と人間の繁栄を促進するため、政府は 第1部に示した定義が示唆するように、「アイデンティティ」が文脈に依存する概念であることを認識すべきである。場合により、特に組織にとっては、それが比較的独立した静的な概念（すなわち、個人がアクセス管理のために認識可能な単一のアイデンティティを持つ）であると捉えることは有益であろう。一方、人々が時間をかけて無数の個人や組織と関わる文脈では、「アイデンティティ」は動的で関係性に基づくものである。第1部では、組織中心に席巻した技術や法的フレームワークが、個人やコミュニティへの実害を招いた（あるいは防止できなかった）と論じた。2003年に拡張ソーシャルネットワークがユーザー中心のデジタルアイデンティティシステムを要求して以来、同様の理念を推進する動きはさらに広がっている[155]。情報システム、社会科学、開発に関わる研究者らは、データジャスティスに取り組むグローバルなアプローチを求めている[156]。カナダデジタルアイデンティティ認証評議会（DIACC）とヒューマンテクノロジー財団（HTF）による2022年11月の報告書[157]は、政府が人間中心の原則を包含したアイデンティティのソリューションを設計するプロセスに言及している。その多くはID2020[158]、ID4D[159]、Women in Identity[160]、世界経済フォーラム[161]などの権利擁護団体や、Trust over IP Foundation[162]、MyData Global[163]などの組織が推進する原則と一致している。直近のOECD勧告では、実在する人間と社会（アイデンティティ技術に依存する企業やその他のサービスを含む）のニーズが最優先事項と位置付けられている[164]。本稿は、第1部で推奨した人権基盤を土台とし、標準に裏打ちされた包括的で価値に配慮した人間中心の設計（Human-Centered Design）へのアプローチを推奨する。

人権基盤

第1部では、政府はその影響の大きさを踏まえ、たとえ他の利益が有効な推進力となるか否かにかかわらず、人権の維持と促進を明確な目的として、アイデンティティシステム（デジタルアイデンティティシステムを含む）およびエコシステムを設計すべきであると論じた。そのためには、確立された人権のフレームワークに照らして、リスクと機会を分析する必要がある。即ち、デジタルアイデンティティシステムの検討は、それが法的身分証明、法的地位、および住民登録とどのような関係（あるいは潜在的な関係）を持つかという文脈の中で行われなければならない。これらの概念は相互に深く結びついているものの、混同してはならない。

これらの概念が結びついているのは、あらゆる分析において「世界人権宣言」第6条（法的承認を受ける権利）および持続可能な開発目標（SDGs）16.9（すべての人に法的な身分証明を）を含める必要があるからであり、いずれも法的身分証明に焦点を当てているためである。さらに、このような分析では、アイデンティティシステム（デジタルアイデンティティシステムを含む）が、現在および将来にわたり存在する国際的な人権フレームワークを構成する条約や協定における、あらゆる義務の履行をどのように支援できるかも考慮すべきである。これらの法的フレームワークには、たとえば「難民の地位に関する条約」[167]、「無国籍に関する条約」[168]、「証人保護に関する条約」[169]、「児童の権利に関する宣言」[170]などが含まれる。このような分析は、国連が発行している文献群、特に前述の資料群、なかでも「Guidelines on the Legislative Framework for Civil Registration, Vital Statistics, and Identity Management Systems（戸籍登録、重要統計およびアイデンティティ管理システムの立法的フレームワークに関するガイドライン）」[171]を出発点とすべきである。

人間中心の設計

政府が人権を保護するという目標を達成するためには、オープンで反復的かつ信頼性のあるデジタルアイデンティティシステムの設計プロセスにおいて、システムの利用者（および法人などの他の社会的ステークホルダー）が中心的な役割を果たす必要がある[172]。このようなアプローチは、システムが目的に適ったものとなることを確保する上で重要である。なぜなら、システムが投資に見合うだけの利用が得られない可能性があるためである。例えば、英国議会は最近、1億5400万ポンドを投じたGov.UK Verify プログラムを中止した。理由は、利用率が想定の6分の1にとどまり、登録率も38～50%だったためである[173]。

人間中心の設計（HCD）とは、「人々のためにソリューションを開発する学問」である[174]。本稿では、「ユーザー中心」や「個人中心」ではなく「人間中心」という表現を採用している。それは、他の用語では捉えきれないより広範な視野を伝えられると考えるからである（もっとも、本稿で用いられる多くの用語と同様、その意味は文脈によって左右される可能性がある）。たとえば、HCDプロセスは単にユーザーインターフェースに的を絞ったものではなく（また、対象ユーザーのみに限定したものでもなく）、複数のステークホルダーコミュニティを横断し、体系的に良好な成果を導くことを目的としている[175]。HCDの研究者であるKlaus Krippendorf氏は、2004年の論文において、HCDは「多くの個人や文化的概念が、技術との途切れないインターフェースへと展開することを可能にする」ことに関心を持つと論じている[176]。

このプロセス自体、本稿では言及していない多くの手法やツールの支援を受けて開発されている場合もあり、システムを利用する人々の共感を育むため、広い包摂性と深い関与が求められている。プロトタイプの開発と設

計ー試験の繰り返しがその理解を深め、拡大する。このプロセスはユーザー体験のデザインだけでなく、一連の選択肢の提供（「ワンサイズが全てに合うわけではない」[177]）、リスク分析、リスク軽減策、およびトレードオフの判断にも影響を与える。これにより実装者は前提を検証し、普及や利用を促進する要因について実質的な知識を得ることができる。例えば、英国の研究者らは、スーパーマーケットの買い物客の70%程度が、再利用可能なデジタルIDより匿名のフェイシャルスキャンによる年齢確認を好むことを明らかにした[178]。さらに、HCDは物事がうまくいかない場合のシナリオ、つまり詐欺や個人情報の盗難に対する救済メカニズムといった「不幸な経路」も考慮に入れる。

包括性

デジタルIDシステムはプロセスの簡素化と利便性の向上を約束する一方で、全稼働寿命を通して異なるニーズを持つ各種コミュニティを包含し、変化を見越して設計されなければならない。マッキンゼーが指摘するように、デジタルアイデンティティシステムへの包括的なアクセスは人々に大きな機会をもたらすと考えられる[179]。アーンスト・アンド・ヤングの「Connected Citizen Report」で言及されているようなペルソナ開発が有用だろう[180]。しかし表3に示す通り、誤った解決策により格差が拡大し、排除が助長され、さらには抑圧の手段となり得るおそれがある人々が多数存在する。

OECDは、政府が提供する選択肢を利用できない、あるいは利用しないことを選択する人々を含む脆弱な層への配慮を行っている[181]。Secure Identity Allianceは2021年の報告書で、包括的実践につながる広範な関与について注目すべき事例をいくつか紹介している。これには、フランスにおける特定の職業向けの革新的なアイデンティティソリューション、アゼルバイジャンにおける政府推奨技術の導入を望まない、あるいは導入できない人々への対応策、オーストラリアにおける家庭内暴力の被害者向けウォレットなどが含まれる[182]。「アイデンティティの排除がもたらす人への影響（The Human Impact of Identity Exclusion）」は、このように多くの人が、書類の再発行や善意に基づくアイデンティティシステムの利用時に、一見したところ克服が困難な課題に直面していると指摘している。これらの問題は、経済的排除や、より広範なアクセスの欠如につながる[183]。真に全ての権利を代表するためには、実装者は人間の経験をすべて視野に入れた設計を行う必要があり、その際、取り残されたコミュニティや「エッジケース」のシナリオを、設計の初期段階から考慮することが求められる。これらの人々は、HCDプロセスの早い段階で特定し、連絡を取る必要がある。

Bボックス2：チャンピオンユースケース例

国際社会には、デジタルアイデンティティ技術を活用して大規模なアクセスと包摂を実現する多くの機会がある。本稿では、最も複雑な「チャンピオン」ユースケースをいくつか含め、そうした技術が各状況で人権をいかに強化できるか、また法的アイデンティティと制度的フレームワークがどこで進化する必要があるかを定義することを推奨する。

家族関係

家族構成員間の絆、例えば親と子、あるいは養育者と子の関係は普遍的に適用されるものであり、普遍的に複雑である（「委任」として知られる）。実際の世界では、感情的な親子間の「絆」はよく理解されている。しかし、その絆を主張する仕組みは機能不全に陥っており、現行の基準やフレームワークでは不十分である。

各国は自国の児童保護政策の実施に苦慮している[1]。この問題は複雑で、詐欺、虐待、同意、管理リスクが蔓延している。結果として、親や養育者がサービスに登録し利用する能力には障壁が立ちはだかる。

この課題を「チャンピオン」ユースケースとして解決するための協働により、組織が結束して家族支援を実現し、長年の問題に対処することが可能になる。

国境を越えて

多くのアイデンティティ関連文献は、デジタルアイデンティティシステムが市民や定住者をいかに支援するかを中信としている。これは、自国民の中の脆弱な集団に対する善意を前提としていると言える。しかし実際には、無国籍者や事実上の無国籍者（自国政府から抑圧を受けた、同化を迫られた、あるいは人権保護の責任を放棄された人々）が数百万単位で存在する。国連人権宣言がすべての人に適用されることを考えると[1]、本稿は、こうした人々のためにアクセス可能で相互運用性のある識別システムを開発するため、各国政府が国際的に協力することを推奨しなければ義務を怠ったと言える。こうした取り組みで重要なことは、個人が認められた法的地位を獲得し、世界経済に参加できるようにすることである。

バリューセンシティブ設計

前述のHCDの定義が示唆するように、システムの使いやすさや普及は重要だがそれだけでは目標として不十分である[184]。このように焦点が狭義だと、採用したシステムが人々の利益を損なう恐れがある[185]。「粘着性のある」誤情報を拡散するアルゴリズム[186]や、サードパーティーアプリによる銀行口座データのスクリーンスクレイピングがその例だ[187]。このような場合、エコシステムは人とコミュニティを保護し、認識できず制御できない危害に直面した際の彼らの権利を強化しなければならない。これらの理由から、このHCDプロセスが価値の可視化、トレードオフの判断、ガバナンスの強化を目標とすることは不可欠である（便利で有用な技術の導入は無論のこと）。したがって、バリューセンシティブ設計（VSD）の調査と実践を組み込むことは機能として有益であり、HCDプロセスが正しい情報を導くことを保証する[188]。

エコシステムの設計に価値を組み込むことは単純な作業ではない[189]。とはいえ、研究者らは人工知能のような新興技術のニーズを支援するため、VSDツールを改良している[190]。表4にいくつかの考察を概説する。

表4：HCDプロセス上のバリューセンシティブ実装

人間中心設計のフェーズ	価値重視設計の意義
誰にリーチするのか? ステークホルダー・マッピング コミュニティのためのHCD目標設定 ペルソナの開発	広範で社会横断的なステークホルダー・グループ 学際的な研究者 価値観と緊張関係を表面化させるために設計された質的調査手法
何を知る必要があるのか? 既存および新規のインサイトの収集 ジャーニー・マッピング	
障壁と機会の特定 ラピッド・インクワイアリー(迅速な調査) 情報の統合	• 価値の緊張関係を技術的、手続き的、法的、またはその他の方法で交渉・管理する必要がある領域を特定する
アイデアとプロトタイピング アイデアの創出 プロトタイプの構築	• 要件に価値観を組み込む • 交渉戦略の文書化
測定と改善 パイロット実施と反復	• 提供されたパイロットまたはプログラムの「組み込まれた」価値観を評価(および対処)するための研究手法

巻末の注参照[191]

このプロセスは、デジタルアイデンティティシステムがバランスの取れた価値観を基盤とし、技術の目的は実在の人々が世界と関わる能力を強化することを保証することである[192]。特に、広範な価値観を列挙するだけでなく、要件を特定し、避けられないトレードオフの意思決定を価値観に基づいて調整する方向へと進んでいる。

人間中心の標準

オープンで堅牢に策定された標準は、技術や制度を成熟させ、社会のニーズを満たし、その価値観を支えることを可能にする。しかし、それらの標準は開発に携わるワーキンググループの価値観を反映する。アイデンティティシステムの標準化を主導する非営利組織やワーキンググループは、社会全体を反映した堅牢かつ公平な標準を策定するため、グローバルな多様性と包括性を備えている必要がある。こうした組織はそのことを自覚し、明確に示す必要がある。

政府は積極的に関与することで支援できる。標準化団体の使命を支援し、協力し、自らのニーズを明確に伝えることで、ワーキンググループがそれらに対応できるようにすべきである。例えば、「チャンピオン」ユースケース（前述の親子間の「デジタルの絆」など）を実現するためには、標準化団体は、最も活発な参加者（多くの場合、グローバルノースの大規模民間企業）だけでなく、特にグローバルサウスにおける政府関係者や多国間機関からの要件も理解する必要がある。以下のセクションでは、人間中心の価値観に基づき、アイデンティティエコシステムの重要な要素であるセキュリティ、プライバシー、相互運用性、および強力なガバナンスを推進する組織、ワーキンググループ、および一連の標準に焦点を当てる。

アイデンティティ業界から生まれた２つのグローバルな取り組みが、周縁化された人々を包摂するアイデンティティシステムのためのガイドライン策定特に取り組んでいる。Women in Identityは、アイデンティティの包摂に関する国際的な行動規範を策定中であり[193]、ID2020は、移民、無国籍者、および権利が脅かされている人々の権利の促進に中心としている。

人間中心のアイデンティティシステム実現に向けた推奨事項

1. デジタル技術が格差の是正や権利の促進に果たす役割を含め、アイデンティティシステムに関する人権分析を策定・維持する。
2. アイデンティティエコシステムのステークホルダーグループを幅広く、かつ包括的に関与させる。
3. ステークホルダーグループに対するリスクと便益を反映し、価値観に配慮したHCDプロセスに従って中核的価値観から着手する。
4. 価値観に基づくトレードオフの判断とリスク軽減戦略を定義する。
5. これらの価値に基づく優先事項を達成する標準を成熟させるため、標準化団体と連携する。
6. 特に、Women in Identity Code of ConductおよびID2020と連携し、脆弱な立場や周縁化された集団を考慮したアイデンティティシステムの設計を採用する。
7. 大規模なユーザー要件を明確にする「チャンピオン」ユースケース（例：親子間、無国籍者などの「デジタルの絆」）において協働 し、相互運用可能なデジタルアイデンティティ基盤に関するグローバルな協力を可能にする。

柱2：戦略的設計とガバナンス

「体系的な問題は、構造的に対処すれば、無数のばらばらな問題よりはるかに容易に改善できる」[194]

デジタルアイデンティティの技術アーキテクチャとガバナンスには、有効なアプローチが多く存在するが、第2部では、図2で示したような意図しない結果を回避するため、重要なトレードオフの判断とその緩和策を明確にている。政府およびアイデンティティシステムが社会で果たす役割の複雑性を踏まえ、OECDはデジタルアイデンティティソリューションの設計にあたり、協調的かつ戦略的なアプローチを推奨している。前述の人間中心設計プロセスは、エコシステムの目標と戦略を形作る価値観を明らかにするものである。これを踏まえ、政府はデジタルアイデンティティシステムの技術、導入、継続的運用を方向付けるための制度的支援層を構築する必要がある(図8参照）。これらはもちろん、人権フレームワークと法的身分証明や法的地位を規定する法律を基盤として構築される。

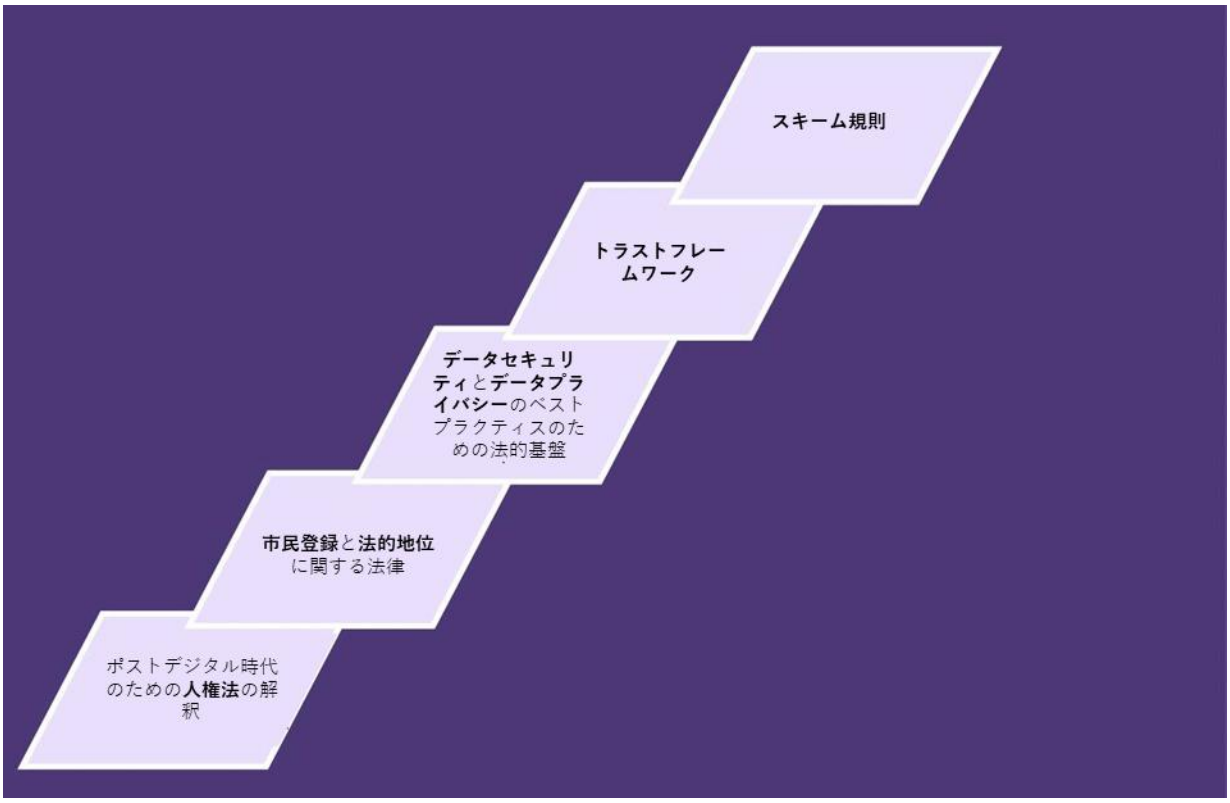


図8：ガバナンス強化のための制度的フレームワークの層

これらの層には、法的基盤の強化（または設計）、トラストフレームワークの定義、および強力な継続的ガバナンスの確保が含まれる。

法的基盤

OECD勧告の限界の一つは、法的身分証明、データセキュリティ、データ保護、およびプライバシーに関する法律が存在し、かつその目的に適合しているということを前提としている点にある。この前提は、必ずしも常に正しいとは限らない。しかし、第2部で述べたように、これらの法的基盤は、あらゆるデジタルアイデンティティエコシステムに内在するリスクを軽減し、欠陥のある法的身分証明制度やインフラから生じる危害や人権問題を防止する上で極めて重要である[195]。したがって、これらの基盤では、技術が発展に歩調を合わせて進化していく必用がある。これには、既存の基準を新たな文脈に適用すること、さらには新たな基準を策定することが含まれる。

特にデータセキュリティ[196]およびプライバシー法[197]に関しては、学者らはガバナンスシステムと制度的保護設計において人間中心のアプローチを求めている。多くの論者は、デジタルアイデンティティシステムを含む新興技術を支える法的基盤が、個人を十分に保護しておらず、現代に適した人権解釈を取り入れていないと指摘している。エリザベス・レニエリスは先駆的な著書『Beyond Data』において、欧州の一般データ保護規則（GDPR）が世界で最も進んだプライバシー法であるとしながら、大量の匿名化・仮名化データが新興技術に取り込まれることで社会全体に及ぼす影響（少なくとも一般人にとっては予測不能な影響）を考慮すると、個人にデータ管理の負担を過度に負わせていると論じている。アルゴリズムによる偏りや大規模操作といった被害を防ぐためには、新興技術に関連する人権法について、現代的な再解釈が求められる[199]。

もっとも、ポストデジタル時代の人権を再定義する国際的取り組みと歩調をあわせ、立法側でも実現できることはある。学者のソロヴェとハーツォグは、現代のセキュリティ法が事後調査や責任追及を重視するあまり、体系的な予防を促す仕組み作りを損なっていると指摘する[200]。彼らは、プライバシー・バイ・デザインとセキュリティ・バイ・デザインを企業活動に不可欠な慣行とする包括的なアプローチにより、法が人々をよって、法が人々をより適切に保護できると主張している。こうした基盤を整えることでは、場当たり的な対策や個別的な解決策がもたらす意図せざる悪影響を最小化できるだろう。

本稿は下記の文献（特にy Renieris氏、Solove氏及びHartzog氏）を参照し、アイデンティティエコシステムの法的基盤に関して以下の2件を推奨する。

1. 推奨事項1（上記参照）に基づき、政府は国際ガバナンス、人権団体、市民社会、学界、民間セクターと連携し、新興技術に関する人権アジェンダを支える法的フレームワークをいかに適応させるかを定義する措置を講じなければならない。

2. これらの権利を保証し、組織的なデータ管理と利用可能な最適なプライバシーおよびセキュリティ対策の導入を求める柔軟なガイドラインを確立するため、各国のプライバシーおよびセキュリティ関連法を改正する。

トラストフレームワーク

プライバシーセキュリティ法は、戦略的なデジタルアイデンティティシステムの基盤的要素であるが、それだけでは意図された価値体系を十分に維持することはできない。条約や法律の改正には当然時間がかかるため、過度に規範的な要件を課さないことは妥当である。しかしながら、セクター横断的かつ社会全体に及ぶ潜在的なリスクと便益を踏まえる、各国はデジタルアイデンティティシステムを専用のガイドラインと独立した監視を必要とする重要な国家インフラとして位置づけつつある[201]。このことが、OECD原則がステークホルダーによって定義された人間中心の要件に基づき、強固なトラスフレームワークの策定を特に推奨する理由である。Open Identity Exchangeの『トラストフレームワークガイド』で定義されている通り、このフレームワークはエコシステム固有の原則・役割・規則・義務を定義し、それらを継続的なガバナンスと執行モデルに組み込む場である(図9)参照[202]。こうしたフレームワークは詳細でありながら柔軟性を備えていることが求められる。基盤となる法的・規制的フレームワークを補完するよう設計されているためである。さらに、運用を支える契約や技術要件に不可欠な情報を提供するという役割も果たす。

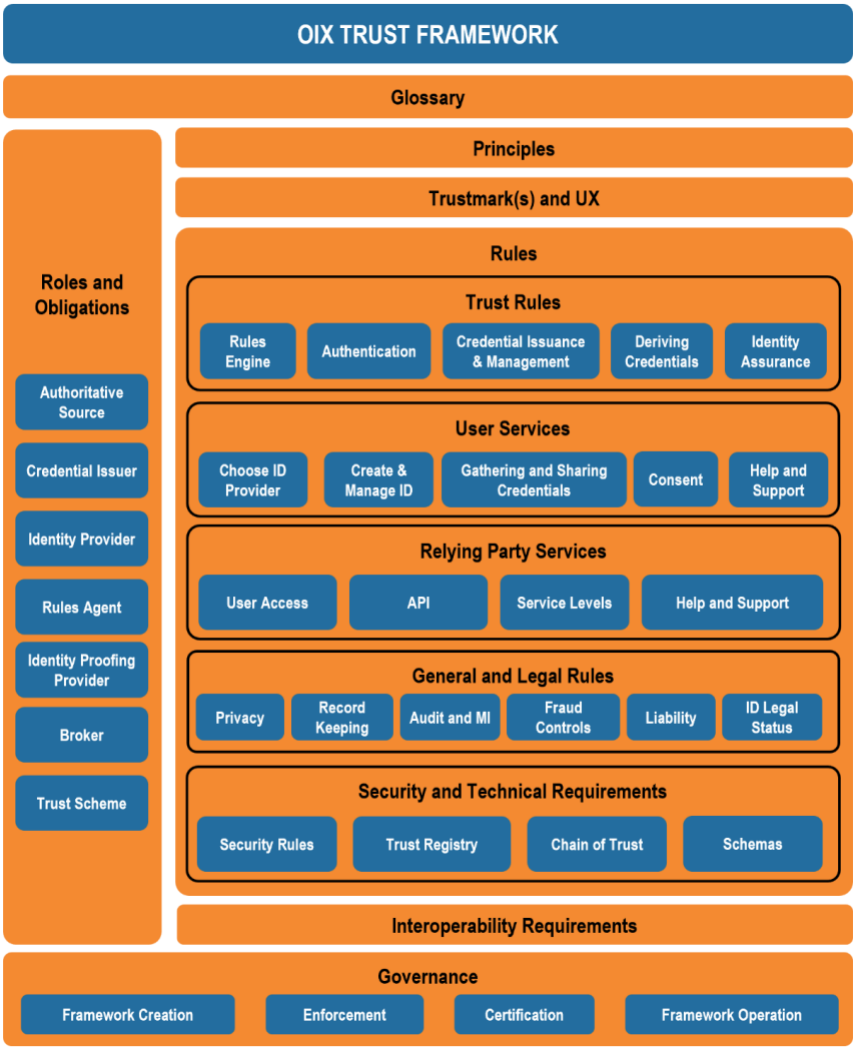


図9：OIXデジタル信頼フレームワークガイド（出典：OIX[203]）

市民に権限を与え、活気ある民間部門を支える強力なアイデンティティエコシステム構築が必要であることから、各国は官民連携によるデジタルアイデンティティトラストフレームワークの開発を加速させている[204]。例えば、カナダの「Pan-Canadian Trust Framework（PCTF）」は、民間企業と政府関係者が共同で開発した成果物であり、多様なデジタルアイデンティティシステムやアーキテクチャに対するガイドラインを提供している。アーキテクチャは大きく異なるが、ウォレットベースのブリティッシュコロンビア州のアイデンティティエコシステムの運営者と、Interacが運営する銀行ベースのVerified.meエコシステムの運営者は、いずれもDIACCに参加し、PCTFの推進に寄与している。

この取り組みには継続的な努力と投資が求められるが、合意された価値観の範囲内で革新を進める複数のアイデンティティエコシステムを生み出す可能性がある。

重要なのは、こうした合意された価値観が、システムの展開方法やその後の管理や評価の在り方を含め、トラストフレームワークのあらゆる側面に浸透している必要があるという点である。善意に基づいて設計されたシステムであっても、システムの導入が意図した価値観と整合していない場合、個人に悪影響を及ぼすことがある。例えばウガンダでは、国民アイデンティティの義務化が完全導入前に実施され、未登録者への適切な対応が欠如した結果、医療サービスや高齢者向け給付を受け取れなくなったことが報告されている[205]。意図しない被害のさらなる事例は、Center for Human Rights and Global Justiceによる「Paving a Digital Road to Hell」（地獄へと向かうデジタル道路を舗装する）に示されている[206]。これが、Centre for Internet and Societyが、トラストフレームワークの包括性評価において、権利ベース、規則ベース、およびリスクベースの検証を推奨する理由である[207]。最後に、エコシステムが意図した通りに機能し続けることを保証するため、導入後の市民およびすべてのステークホルダーに生じる費用と利便性についての分析は、HCDプロセスで導出された価値観に基づいて慎重に設計し実施すべきである[208]。

戦略的な設計と強固なガバナンスに関する推奨事項

1. ポストデジタル時代に向けた国連人権規約の解釈について国際的に協働し、既存の法的フレームワークがこの解釈にどの程度対応しているかを評価する
2. これらの権利を保障し、プライバシー・バイ・デザインおよびセキュリティ・バイ・デザインのベストプラクティスに基づく組織的なデータ管理を義務付けるため、国家および地域レベルのプライバシーセキュリティ関連法規を構築・整備する
3. デジタルアイデンティティを重要インフラと位置付け、必要に応じて国家、超国家、および地方レベルの戦略（および関連投資）を策定する
4. OIXの支援のもと、優先順位付けされた人間中心の価値観をエコシステムガイドラインへ転換するデジタルアイデンティティトラストフレームワークの官民連携に時間と資源を投入する
5. トラストフレームワークにエコシステムの設計、実装、管理、評価の各側面を組み込む

柱3：安全でプライバシーを保護するアイデンティティシステム

第3と第4の柱は、デジタルアイデンティティシステムの原則に基づく文献の全てが、セキュリティ、プライバシー、および相互運用性に大きな重要性があることを反映している。本章では、複雑なテーマであり多くの専門論文や教科書などで扱われているセキュリティとプライバシー関連のその他のリソースについて簡単に言及する。

データセキュリティは、デジタルアイデンティティシステムが意図する全ての利点を支える基盤である。これには個人、集団、コミュニティ、民間組織、政府機関など、アイデンティティを保有する者、あるいはそれを検証する必要のある全ての主体への便益が含まれる。このようなアイデンティティ整合性への依存度を、特にあらゆるサプライチェーンに内在する広範な公的および私的相互依存性と併せて考えると、セキュリティはいまや企業の社会的責任（CSR）の基本的な要素となっている[209]。政府関係者は、デジタルアイデンティティシステムを導く立法やトラストフレームワークといった制度的フレームワークが、エコシステム内の全てのアクターにプライバシーとセキ

ュリティのインセンティブを創出するよう、細心の注意を払わねばならない[210]。欧州のNIS2指令[211]は立法のテンプレートとなり得る。また米国NISTの草案SP800-63-4は、アイデンティティシステムの保護に向けた包括的フレームワークを提供する[212]。このテーマに関心のある読者は、これらから始めることを推奨する。

セキュリティは本質的にプライバシーと関連しているが、両者は同一ではない。セキュリティとはデータを含む組織の資産を保護する方策であり、プライバシーはそもそもデータの収集・処理・保管に関わる問題である[213]。両者は対立することもある。例えば、詐欺やサイバー犯罪対策には、行為者の特定や、時には不審な活動に関するデータの保持と共有が必要となる。こうした緊張関係は、立法レベルやトラストフレームワークレベル（実際、NIST草案SP800-63-4[5]はこれを目的としている）を含む（ただしこれらに限定されない）複数のレベルで均衡を図り、必要に応じて方針、手順、技術的制御等を通じて緩和されなければならない。

OECDは、これらのニーズの均衡を図るためのベストプラクティスの出発点として、一連のプライバシー原則[214]を策定した。この原則は以下の8つのトピックを網羅しており、欧州の一般データ保護規則（GDPR）[215]の第5条で定められたもの、およびあらゆる国が批准可能な2018年欧州評議会個人データ処理に関する個人保護条約（第108号）に沿った内容となっている[216]。

1. 収集の制限
2. データの品質
3. 目的の特定
4. 利用目的の限定
5. セキュリティ対策
6. 透明性
7. 個人の参加
8. 説明責任

付録D-Eに、世界中での実施を支援する、安全でプライバシーを強化するデジタルアイデンティティ標準を開発する機関およびワーキンググループを記載した。新たなデジタルアイデンティティシステムのプライバシーに関する考慮事項について深く掘り下げたい読者には、本稿の姉妹論文である「Government-Issued Digital Identity Credentials and the Privacy Landscape」（政府発行のデジタル身分証明資格とプライバシー環境）を推奨する。本稿では、これらの具体的な課題を、世界的な法律、実装、ギャップ、トレードオフ、およ

[5] （訳注）SP800-63-4は、2025年8月に正式に出版された

び既知の問題を解消または改善するための明確な勧告という観点から探求している。

セキュリティとプライバシーに関する推奨事項

1. データセキュリティは企業の社会的責任（CSR）の基盤的要素であり、すべてのプロセス（開発・調達プロセス等）に組み込まれるべきであるという考え方を推進する。
2. 既存のベストプラクティス文書を参照する（現時点では以下を含む）。
    a. 法令：欧州のNIS2およびGDPR
    b. トラストフレームワーク：NIST SP800-63-4
    c. プライバシー：OECDプライバシー原則、GDPR、欧州評議会条約108
3. 「政府発行のデジタルアイデンティティ認証とプライバシー環境」を参照し、現行法やベストプラクティスがまだ対応していないリスクとアプローチを検討する
4. 選択したセキュリティプロトコルが正式なセキュリティ分析手法を用いて検証され、すべての弱点が対処されていることを確認する。
5. エコシステム参加者が、望ましい成果が実際に達成されることを保証するための、明確で実証的に測定可能かつ義務的な認証および適合プロセスを有していることを確認する。

推奨事項4および5に関する詳細な文献については、シュトゥットガルト大学のWebインフラストラクチャモデル[217]およびNISTの適合性試験概要[218]を参照されたい。

柱4：国際間の相互運用性の実現

デジタルアイデンティティシステムはエコシステムの内外および政府間の関係を支える基盤であることから、原則に基づくデジタルアイデンティティに関する文献は、セクター横断的かつ国境を越えた相互運用性の促進と整合している。これは、個人が特定の政府とどのように関わるかを定義するだけでなく、政府システムが他の領域において、信頼できる関係のライフサイクル（確立、維持、終了、失効）をどのように、またどのような範囲で可能にするかを定義することを意味している[219]。

相互運用可能なエコシステム標準

目標達成のためには、法的・組織的な相互運用性に加えて、技術的・セマンティックな相互運用性も必要である[220]。具体的には次のような領域が該当する。

- エコシステム内の主体間における相互信頼の確立
- 個人、主体、デバイスの識別（後者2つは本稿の主題ではないが、人間のアイデンティティとの識別・相互作用、あるいはその代理としての識別が必要）
- プロトコルレベルにおける標準化されたインターフェース
- 既存の国家および超国家レベルの身元保証基準・政策の整合化
- データとメタデータ（情報内容と形式）[221]の調和、セキュリティ慣行と構成

相互運用性の実現に向けて、各組織は組織全体にわたる取り組みの整合を図るために連携を開始している。Trust Over IP Foundationは分散型技術を用いたインターネットへの信頼に関する共通基準構築を目指している[222]。非営利団体MyData Globalは、2019年以降、個人データにおける「相互運用性の旅（journey of interoperability）」を様々な主体と進めてきた[223]。さらに、Global Assured Identity Networkを主導する非営利団体は、既存の信頼エコシステムを橋渡しし[224]、その他の取り組みは付録E-Fに記載されている。

政府はオープン標準の開発を促進し、各層間の相互運用性を可能にする認証を義務付ける上で重要な役割を担っている。例えば、欧州連合のアーキテクチャ参照フレームワーク[225]は、検証可能な資格情報のためのOpenIDなど、その戦略が重視する価値に基づく優先事項を満たす新たな標準群の成熟を積極的に支援している。また、目標を支える適合性および認証に向けた道筋の検討も進めている。同様に、米国土安全保障省科学技術局内のSilicon Valley Innovation Programは、W3CのCredentials Community Groupによるロードマップ作成に強い影響力を発揮してきた。具体的には、Citizenship and Traceability

Vocabularies、JSON-LD、および検証可能な資格情報認証向けのLD署名（LD Signatures for Verifiable Credentials）の継続的な開発と成熟を支援している。さらに、ベンダーを介さない直接的な協力は、政府にコスト削減、ベンダーロックインの最小化、およびセキュリティ強化をもたらし、バリューセンシティブHCDプロセスで明らかになった価値観と目標を支える、より安全で効果的な（すなわち成熟した）システムへの迅速な発展を促している。

強調すべき重要な点は、認定と適合性の役割である。エコシステム参加者にこれらへの遵守が義務付けられなければ、どれほど優れた標準や政策であっても意味をなさない。そのようなエコシステムは、標準や政策が本来軽減を目的としているセキュリティ、プライバシー、および相互運用性のリスクに対して脆弱な状態に置かれる。適合性試験だけでは万能ではないものの、不可欠な手段である。

上記の事例やOECD勧告同様、本稿は政府に対し、これらをオープンスタンダードとして開発するよう強く促す。このような透明性があるアプローチは、エコシステムの長期的な安定性と持続可能性を約束する[226]。要するに、政府はアイデンティティソリューションを開発するオープンスタンダードコミュニティとの継続的かつ直接的な関与と支援を通じて、より多くの利益をより迅速に提供することができるようになる (付録D-E参照）。

相互運用性に関する推奨事項

1. 政策フレームワークと技術標準の整合を図った開発を促進する。
2. 優先事項を共有し、オープンスタンダードコミュニティと直接連携して、優先事項に対応する標準を成熟させる。
3. 官民連携の強化、透明性と信頼の向上、成熟化プロセスの加速を図るため、オープンスタンダードへの参加を推進する。
4. 主要なエコシステム標準および政策に対する必須の認定および適合性試験を導入する。

結論とまとめ

デジタルアイデンティティシステムによって社会や政府にもたらされる機会は膨大である。その点では複雑さとリスクも同様に膨大である。政府がデジタルアイデンティティエコシステムを通じて人権を持続・促進するには、人間中心の協働によって技術・制度設計の全層に中核的な価値を組み込む必要がある。

表5：推奨事項のまとめ

柱1：人間中心のアイデンティティシステム
デジタル技術が格差解消と権利促進において果たす役割を含め、アイデンティティシステムの人権分析を開発・維持する。
アイデンティティエコシステムのステークホルダーグループを幅広く、かつ包括的に関与させる。
ステークホルダーグループに対するリスクと便益を反映し、価値観に配慮したHCDプロセスに従って中核的な価値観から着手する。
価値に基づくトレードオフの判断とリスク軽減戦略を定義する。
価値に基づく優先事項を達成する標準の成熟を目指し、標準化団体と連携する。
特に、Women in Identity Code of ConductおよびID2020と連携し、脆弱な集団や周縁化された集団を考慮したアイデンティティシステムの設計を採用する。
大規模なユーザー要件を明確にする「チャンピオン」ユースケース（例：親子間の「デジタルの絆」、無国籍者、その他）において連携し、相互運用可能なデジタルアイデンティティインフラ基盤に関するグローバルな協力を可能にする。
柱2：戦略的設計とガバナンス
国際的に協力して、デジタル時代以降の国連人権規約を解釈するとともに、国際的に協力するとともに、既存の法的フレームワークがこの解釈にどの程度対応しているかを評価する。
人権を保証し、プライバシー・バイ・デザインおよびセキュリティ・バイ・デザインのベストプラクティスを通じた組織的なデータ管理責任を義務付けるため、国および地域レベルのプライバシー・セキュリティ関連法規を構築または発展させる。
デジタルアイデンティティを、必要に応じて国家、超国家、および地方レベルの戦略を必要とする重要なインフラとして扱う。

OIXガイドの支援の下、優先順位付けされた人間中心の価値観をエコシステム全体のガイドラインへ転換するデジタルアイデンティティトラストフレームワークに関する官民連携に時間と資源を投入する。
トラストフレームワークに設計、実装、管理、および評価の各側面を組み込む。
柱3：安全かつプライバシーを保護するアイデンティティシステム
さらに、データセキュリティは企業の社会的責任の一部であり、すべてのプロセス（開発・調達プロセス等）に組み込むべきであるという考え方を推進する。
既存のベストプラクティス文書を参照する（現時点では以下を含む）。 ● 法令：欧州のNIS2およびGDPR ● トラストフレームワーク：NIST SP800-63-4 ● プライバシー：OECDプライバシー原則、GDPR、欧州評議会条約108
「Government-Issued Digital Credentials and the Privacy Landscape」を参照し、現行法やベストプラクティスで未対応のリスクやアプローチを確認する。
選択したセキュリティプロトコルが正式なセキュリティ分析手法を用いて検証され、すべての弱点に対処していることを確認する。
エコシステム参加者が、望ましい成果を実際に達成することを保証するための、明確で実証的に測定可能かつ義務的な認証および適合プロセスを有していることを確認する。
柱4：国際間の相互運用性の実現
政策フレームワークと技術標準の整合を図った開発を促進する。
優先事項を共有し、オープンスタンダードコミュニティと直接連携して、それらの優先事項に対応する標準を成熟させる。
官民連携の強化、透明性と信頼性の向上、成熟化プロセスの加速を図るため、オープンスタンダードへの参加を推進する。
主要な標準と政策に対する必須の認証および適合性試験を導入する。

Appendix A – 進化する脅威モデル

– 技術が生まれ成熟するにつれて、人間中心の関係性を設計したアイデンティティエコシステムへの移行はますます現実味を帯びてきている。地球上の半数以上の人々がネットワークに接続したモバイルデバイスを利用しており[227]、またデバイスはその使用者／所有者を認識できる高感度カメラレンズ、センサー、その他の生体認証機能を備え、それらは日々進化している。かつてはデータの保存自体が克服しがたい課題だったが、今日では、組織がそのデータをクラウド上でも安全に保存・管理できるようになっている。

このような操作を安全に行うには、バイオハッシングのような新たな暗号化技術と手法が必要である。また、暗号技術、クラウドコンピューティング、および安全なメッセージングプロトコルの進歩により、機密情報の漏洩リスクを低減したデータ転送が可能になっている。下の表は、多くのデジタルアイデンティティ技術の進歩が脅威モデルを変革しているかを示している。

技術的進歩	成熟度	技術が支援するアイデンティティ上の課題	技術上の課題
JOSE	確立済み	標準的な署名または暗号化方式によるアイデンティティデータの通信	これらのオブジェクトの操作と処理
X509認定書	確立済み	特定情報のアサート	静的性質
SAML2	確立済み	安全なシングルサインオン、特に企業のWebケース向け	XMLベースのペイロードとウェブブラウザ中心のインターアクション サードパーティの追跡
OAuth2 Suite	確立済み	安全な情報交換	サードパーティの追跡 コンセント・ハッキング
OpenID Connect Suite	確立済み	安全なID情報交換	サードパーティの追跡 コンセント・ハッキング
モバイルデバイス	確立済み	ローカル認証によるデジタル携帯型識別子へのアクセス	デバイス依存のクロスデバイスフロー
生体認証の取得	成長過程	認証重複	安全なデータ保管 プライバシー

クラウドコンピューティング	確立済み	大規模保管の確保	アクセス制御
安全な生体認証ストレージ 例：バイオハッシング	新興	生体認証の確保	プライバシー／利用規約
FIDO 2	成長過程	安全なフィッシング対策認証	法的身分証明へのユーザーのリンク
パスキー	新興	携帯型ユーザー認証	鍵の来歴、アサーション およびクラウドベースのセキュリティ確保、ユーザー体験
Shared Signals Framework	新興	デジタルアイデンティティエコシステム内のエンティティ間の重要イベントの伝達	データ共有に関する合意の必要性
Verifiable Credentials	新興	完全性をデジタル署名で保証された主体に関する情報を表現するデータモデル	信頼当事者による利用
分散型識別子	新興	公開鍵素材とエンドポイントを提供する分散型PKIを支援するデータモデル	
信頼レジストリ	新興	ガバナンスフレームワークに準拠する主体を記録するガバナンス機関の支援	水平および垂直スケーリング エコシステム内のアクターによる発見
選択的開示	新興	エンドユーザーのプライバシー制御	依存当事者による利用

付録B – デジタルアイデンティティ原則の整合

テーマ	ID2020[228]	ID4D[229]	WEF[230]	DIACC & HTF[231]	OECD[232]
人間中心					
人間中心の結果となる設計	X	x		X	x
ユーザー（子ども、脆弱な立場の人々、後見人を含む）向け設計	X	x	x	X	x
サービスプロバイダー向け設計	X			X	x
偽名アイデンティティへの対応	X			X	x
ユーザーの選択と制御	X	x	x	x	x
インクルージョン					
ユニバーサルアクセス／障壁の除去	X	x		x	x
任意／非強制	x	x		x	x
一意性／永続的な識別子	x	x			x
携帯型 / 回復力（常にアクセス可能）	x			x	x
戦略的ガバナンスと設計					
重要／戦略的国家インフラ					x
独立した監視		x			x
透明性のある政策	x			x	x
明確な説明責任	x	x	x	x	x
公民連携					x
市民の参加／対話				x	x
アクセス可能なオンボーディングと規制サンドボックス					x
長期的持続可能性		x	x	x	x
環境への影響					x
安全、プライバシー保護					
データの最小化 / 選択的開示	x	x	x	x	x
集約／相関の防止	x				x
プライバシー・バイ・デザイン	x	x	x	x	x
最低限のセキュリティ基準	x	x	x	x	x
プライバシーおよびセキュリティに関する法令、規制、ガイドラインの遵守					x
国際間相互運用性					
対応可	x	x			

テーマ	ID2020[228]	ID4D[229]	WEF[230]	DIACC & HTF[231]	OECD[232]
人間中心					
人間中心の結果となる設計	x	x		X	x
ユーザー（子ども、脆弱な立場の人々、後見人を含む）向け設計	x	x	x	X	x
サービスプロバイダー向け設計	x			X	x
偽名アイデンティティへのー対応	x			X	x
ユーザーの選択と制御	x	x	x	x	x
インクルージョン					
ユニバーサルアクセス／障壁の除去	x	x		x	x
任意／非強制	x	x		x	x
一意性／永続的な識別子	x	x			x
携帯型／回復力（常にアクセス可能）	x			x	x
戦略的ガバナンスと設計					
重要／戦略的国家インフラ					x
独立した監視		x			x
透明性のある政策	x			x	x
明確な説明責任	x	x	x	x	x
公民連携					x
市民の参加／対話				x	x
アクセス可能なオンボーディングと規制サンドボックス					x
長期的持続可能性		x	x	x	x
環境への影響					x
安全、プライバシー保護					
標準への適合	x	x			x
ベンダーロックインの防止	x	x			x
セクター間相互運用性	x			x	x
技術的相互運用性 (国際)	x	x	x	x	x
法的相互運用性 (国際)	x				x

付録C：チェックリストとしてのOECD原則

ユーザー中心かつ包括的なデジタルアイデンティティの開発

II. 加盟国には、**ユーザーとサービス提供者のニーズに応えるデジタルアイデンティティシステムを設計・実装することを推奨する。**この目的のため、以下を実施する必要がある。

☐ デジタルアイデンティティシステムの設計、導入、または改良を検討する際、デジタル成熟度や既存のデジタルアイデンティティ開発状況を含む国内の状況を考慮する。

☐ サービス設計手法を活用し、デジタルアイデンティティシステムがユーザーのニーズに応え、アクセス可能で倫理的かつ公平な成果を達成するようにする。特に以下を重視する。

- ☐ ユーザー、サービスプロバイダー、その他の関係者のニーズの特定
- ☐ デジタルアイデンティティのライフサイクルにおけるエンドツーエンドのユーザー体験への考慮
- ☐ 運用パフォーマンスを測定し、必要に応じてデジタルアイデンティティシステムとソリューションの繰り返しの改善

☐ 以下のユーザーの観点から携帯デジタルアイデンティティソリューションの開発を促進する。

- ☐ 場所（対面、遠隔、あらゆる政府レベル、国境を越えた利用を含む）
- ☐ 技術：インターネット接続速度や品質に制約されない、最も便利なデバイス、モバイル端末、通信媒体の利用が可能
- ☐ セクター：公共サービスへのアクセスに加え、必要に応じて広範な経済活動へのアクセスを可能とする

☐ プライバシー保護と同意に基づくデジタルアイデンティティソリューションの開発を促進し、ユーザーが自身の属性や資格情報に対する所有権を強化し、共有する属性・資格情報の内容、タイミング、共有先をより容易かつ安全に制御できるようにする。

III. 加盟国は、**デジタルアイデンティティへのアクセスと利用における障壁を最小化し、包括性を優先することを推奨する。**この目的のため、以下を実施する必要がある。

☐脆弱な立場にある人々や少数派を含む全ての層が、それぞれのニーズに応じて安全で信頼できるデジタルアイデンティティソリューションを利用できるよう、デジタルアイデンティティのライフサイクル全体におけるアクセシビリティ、手頃な価格、使いやすさ、公平性を追求する。

☐デジタルアイデンティティソリューションへのアクセスや利用を希望しない、またはできない人々に対して、公共・民間セクターを含む必須サービスへのアクセスが制限または拒否されないように措置を講じる。

☐デジタルアイデンティティシステムの設計、開発、導入の全段階において、包括的かつ協調的なステークホルダーの関与を促進し、透明性、説明責任、およびユーザーのニーズと期待との整合性を図る。

☐デジタルアイデンティティの利点と安全な利用方法、ならびにデジタルアイデンティティシステムがユーザーを保護する仕組みについての認識を高めるとともに、リスクを認知し、潜在的な危害の軽減策を示す。

☐デジタルアイデンティティソリューションへのアクセスや利用が困難な人々に対し、適切な経路を通じて支援が提供されるような措置を講じるとともに、ユーザー のスキルと能力を構築する機会を確認する。

☐デジタルアイデンティティシステムの有効性を、包括性とデジタルアイデンティティへのアクセス・利用障壁の最小化に焦点を当てて監視・評価し、公表する。

デジタルアイデンティティのガバナンス強化

IV.加盟国には、**デジタルアイデンティティに対して戦略的なアプローチを取り、デジタルアイデンティティエコシステム全体における役割と責任を定義することを推奨する。**この目的のため、以下を実施する必要がある。

☐ 公共部門および広範な経済界におけるデジタルアイデンティティの利点を実現し、リスクを軽減するための長期的なビジョンを戦略として、またはより広範な戦略の一部として策定する。

☐ 国家レベルの戦略的なリーダーシップと実施に関する監督を確保し、デジタルアイデンティティエコシステムにおける国内の役割と責任を定義し、周知する。

☐ 関連性および適用可能性に応じて、政府機関および各レベルの管轄当局間の協力と調整を促進する。

☐ 政府機関、あらゆるレベルの政府における管轄当局、および該当するその他の関連主体が、ユーザーの権利保護や包摂性の優先を含むデジタルアイデンティティエコシステムの管理・監視・保護に責任を負うよう措置を講じる。

☐ 適切な場合、イノベーションと競争を促進し、代替モデルや技術の潜在的価値を探求する健全なデジタルアイデンティティソリューション市場の発展を支援することにより、官民セクター間の連携を促進する。

☐ 国家または地域レベルのトラストフレームワークを確立するか、該当する場合は関連する地域のとらすとフレームワークと連携し、デジタルアイデンティティソリューションプロバイダーが遵守できる共通要件（サイバーセキュリティ要件を含む）を、異なる保証レベル（LoA）に対して設定し、デジタルアイデンティティエコシステム内の信頼構築を促進する。

☐ デジタルアイデンティティシステムの規制と監督に関する明確な責任を確立し、ユーザー及び関係者の権利が保護され、紛争解決、救済、回復のための適切かつ効果的なメカニズムが整備されるようにする。

☐ 技術選択の環境への影響と、デジタルアイデンティティライフサイクルを通した全ての関係者のコストを反映した継続的な投資の必要性を考慮し、持続可能で強靭なデジタルアイデンティティシステムを推進する。

☐ 新たなニーズ、脅威、リスク、および機会に対応できるように、デジタルアイデンティティシステムを監督する。

V.加盟国は、**デジタルアイデンティティシステムへの信頼を確保するため、プライバシー保護とセキュリティの優先を推奨する。**この目的のため、以下を実施する必要がある。

☐ 信頼できるデジタルアイデンティティシステムの設計においてセキュリティを基盤と認識し、デジタルアイデンティティソリューション提供者及びソリューションが、定義された保証レベル（LoA）と整合的および／またはリスクベースアプローチと整合的な方法で、ユーザー、サービスプロバイダーや社会を（潜在的なアイデンティティ盗難や改ざんを含む）あらゆる脅威からの保護のため、関連する全ての要件の遵守を確認する。

☐ ユーザー制御、プライバシー、およびデータ保護をデジタルアイデンティティシステムの基本原則とし、インフォームドコンセント、完全性、機密性、選択的開示、目的の限定、個人データの収集・利用制限を含む「プライバシー・バイ・デザイン」および「プライバシー・バイ・デフォルト」アプローチの採用を促進する。これには、生体認証データを含む特別なカテゴリーの個人データの悪用を防ぐための特定の基準やメカニズムの必要性を考慮することも含まれる。

☐ サービス間でのデータセットの集約や、ユーザーが異なったサービスにアクセスするためにデジタルアイデンティティソリューションを利用した場合、不要な個人データの痕跡が残留しないようにする。

☐ 既存データの保護およびプライバシー法に基づく説明責任義務を履行する。

☐ デジタルアイデンティティソリューションを通じて共有される属性や資格情報が正確、完全、最新かつ関連性を保つような強固な仕組みを導入する。

☐ デジタルアイデンティティシステムの設計・利用において、子どもや脆弱な立場にある人々、および少数派を安全に受け入れて保護する方法に関する具体的なニーズを特定する。

☐ 必要に応じて、ユーザーがデジタルアイデンティティソリューションによる代理人の指名、および代理権の委任を可能にする法的承認メカニズムの確立を検討する。これにより、ユーザー自身が可視化・管理・追跡可能な形で代理人の行動を保証する。

☐ デジタルアイデンティティシステムの設計および関連するその他の措置において、オープンスタンダードとオープンソースソフトウェアの利用を促進し、単一のハードウェアまたはソフトウェアベンダーへの依存に伴うユーザー、サービスプロバイダー、および社会へのリスクを軽減する。

VI.加盟国は、**相互運用性を実現するため、法的・規制上のフレームワークを調整し、資源を提供することを**推奨する。この目的のため、以下を実施する必要がある。

☐ 適切な場合、デジタルアイデンティティシステムに関する国内政策・法令・規則・ガイドラインにガバナンス、責任、プライバシー、回復力、セキュリティなどの課題を網羅し、場所・技術・セクターを超えた相互運用性と移植性を促進・支援するようにする。

☐ 関連する全てのセキュリティ要件を遵守する限り、デジタルアイデンティティソリューションが技術・ベンダー中立であることを保証し、国際的に認められた技術標準と認証の利用を促進する。

☐ デジタルアイデンティティシステムに参加するための支援を目的としたリソースカタログ（共通技術コンポーネント、文書化、適切な技術サポートなど）へのサービスプロバイダーによるアクセスを提供する。

☐ 新興技術のリスクと機会、および相互運用性に影響を与える可能性のあるデジタルアイデンティティシステムの更新を探求するための安全で管理された環境を提供する、規制サンドボックスなどのメカニズムの創設を支援する。

☐ デジタルアイデンティティエコシステム全体において、既存の国内規則および国際的に認められた技術基準への準拠状況を適切に監視し報告する。

デジタルアイデンティティの国際利用の実現

VII.加盟国には、**様々な越境シナリオにおけるユーザーとサービスプロバイダーの進化するニーズへの認識を推奨する。**この目的のため、以下を実施する必要がある。

☐ 異なる管轄区域における属性および／または資格情報の共有を必要とする活動を認識することにより、状況とユーザーの経験に基づいて、デジタルアイデンティティシステムの国際相互運用性における優先的なユースケースを特定する。

☐ 国際協力により、他管轄区域のサービス提供者がデジタルアイデンティティソリューションを認識・統合・信頼するために必要な要件を特定する。

☐ デジタルアイデンティティシステムの国際相互運用性および関連ユースケースに伴うリスクを特定し、必要に応じて軽減策を採用する。

VIII.加盟国には、**他国のデジタルアイデンティティシステム及び発行されたデジタルアイデンティティに対する信頼の基盤を確立するため、国際的に協力することを推奨する。**この目的のため、以下の措置を講じる必要がある。

☐国境を越えたデジタルアイデンティティを支援するため、相手国や活動と適切かつ適用可能な形で連携する連絡窓口を国内で指定する。

☐ 既存の法的要件、トラストフレームワーク、技術基準の一貫性、互換性、または同等性を評価・マッピングする、自由貿易協定を通じた協働の可能性を探る、越境規制実験の機会を特定するなど、デジタルアイデンティティシステムの越境相互運用性を可能にする国際的な規制協力に取り組む。

☐ 国際的な技術標準策定作業への参加、経験とベストプラクティスの交換、イノベーションプログラムの調整を通じて、デジタルアイデンティティエコシステム全体の関連ステークホルダーと連携し、二国間および多国間協力に取り組む。

☐デジタルアイデンティティの越境相互運用性が、外国ユーザーが必須サービスや商業取引にアクセスする際に不当な差別的扱いに利用されないようにする。

☐ 国際間の取引におけるデジタルアイデンティティ利用に関連する責任の根拠の明確化に取り組む。

☐ 国際間の公共サービスにおいては、サービスへのアクセスを試みるユーザーの識別とデジタル識別情報の整合性を確保するため、必要に応じて、海外の特定の公共機関に保存されているアイデンティティ属性と、デジタル識別プロセスを通じて共有されたユーザーの属性または情報を照合できるようにする。

☐以下の実現に向けて必要な段階を概説するロードマップを作成する。

- ☐ 国内で認められたデジタルアイデンティティソリューション及び関連した属性または資格情報を国際的に利用可能とする。
- ☐ 相手国のデジタルアイデンティティソリューションおよび関連属性または資格情報を国内で認証する。

付録D：人間中心のデジタルアイデンティティにおける役割を担う非営利団体

この付録は我々が維持・更新する「流動的な付録」である。レビュー担当者は、本稿のメッセージに沿った組織の追加を提案することができる。

組織	ミッションとウェブサイト
Decentralized Identity Foundation	私たちは共に新たなアイデンティティエコシステムを構築しています。 個人、組織、アプリ、デバイス向けの、オープンで標準ベースの分散型アイデンティティエコシステムの基盤となるコンポーネントの開発にご参加ください。
DIACC	DIACCは、デジタル経済においてカナダの価値観と視点を保護し促進することが極めて重要であると考えています。DIACCは、以下の原則を指針として、私たちの使命とビジョンを支援しています。
EBSI - European Blockchain Services Infrastructure	European Blockchain Services Infrastructure （EBSI）は、ブロックチェーン機能を活用した公共の利益を目指しています。EBSIは欧州委員会とEuropean Blockchain Partnershipによるイニシアチブです。
FIDO Alliance	FIDO Allianceは、世界におけるパスワード依存の過度な依存を減らすための認証標準という明確な使命を持つオープンな業界団体です。 認証およびデバイス認証のための標準の開発、利用、および準拠を推進しています。
Global Assured Identity Network -技術実証 (OIDF) -政策ワーキンググループ (OIX)[6]	150名以上の共同執筆者が発表した2021年版GAIN Digital Trust白書は、高信頼性アイデンティティ保証のためのグローバルな相互運用ネットワーク構築を提唱しています。OpenID Foundationの会長である崎村 夏彦氏が欧州アイデンティティ会議でこのような国際協力を発表した際、著者らが共有するビジョンを「人々が互いを信頼できるインターネット」と表現しています。
Global Legal Entity Identifier Foundation (GLEIF)	取引相手に関する意思決定をよりスマートに、低コストで、信頼性の高いものにします。
ID2020 (Ethical Identity)	ID2020は、パートナーを通じて、デジタルアイデンティティの将来の方向性を決定するマルチステークホルダーの連携を推進しています。提携者として、安全、セキュリティ、相互運用性、および個人の管理が、設計によってデジタルアイデンティティシステムに組み込まれるよう取り組んでいます。
IETF Internet Engineering Task Force	IETF の全体的な目標は、インターネットの機能を向上させることです。

6 （訳注）Open Identity Exchangeは2026年1月現在、運営を停止している

	その使命は、インターネットの設計、使用、管理の方法に影響を与え、インターネットの機能を向上させるような、高品質で関連性の高い技術およびエンジニアリング文書を作成することです。これらの文書には、プロトコル標準、現在のベストプラクティス、および様々な情報文書が含まれます。 IETF のいくつかのグループは、ユーザー中心の アイデンティティ に活用されるプロトコルに取り組んでいます。
ISO国際標準化機構	ISO（国際標準化機構）は、168 の国家標準化機関が加盟する、独立した非政府国際機関です。 加盟機関を通じて専門家を結集し、知識を共有し、合意に基づく自主的な市場関連国際規格を開発することで、イノベーションを支援し、地球規模の課題に対する解決策を提供しています。 本稿は、ISO 18013-5「モバイル運転免許証」も大きく依存しています。
Kantara Initiative	私たちは、アイデンティティと個人データの信頼性の高い利用の向上に焦点を当てたグローバルコミュニティです。私たちのワーキンググループは、個人情報やアイデンティティの収集、保存、利用に関するイノベーション、標準化、ベストプラクティスの開発に取り組んでいます。
MyData Global	MyData Global の目的は、個人データに関する自己決定権の向上を通じて個人に力を与えることです。 MyData Global は、個人データに関する人間中心のパラダイムというビジョンを共有し、その最先端を推進する、個人データ専門家や組織によるグローバルコミュニティの形成を支援しています。
NIST米国国立標準技術研究所	経済的安全性の強化と生活の質の向上につながる測定科学、標準、技術の進歩を通じて、米国のイノベーションと産業競争力を促進しています。 NIST SP800-63-4 は最新のデジタルアイデンティティ ガイドラインです。
OASIS	IDTrustクラスターは、ユーザー中心の ID に関連する標準に関わっています。
Open Identity Exchange (OIX)[7]	OIX は、アイデンティティ分野に携わるすべての関係者が連携・協力し、相互運用可能な信頼できる アイデンティティに必要なガイダンスを開発するコミュニティです。トラストフレームワークの定義と教育を通じて、すべての個人が信頼され、世界的に受け入れられるアイデンティティを実現するためのルール、手段、および信頼を構築しています。

[7] （訳注）Open Identity Exchangeは2026年1月現在、運営を停止している

OpenID Foundation	当ファウンデーションのビジョンは、人々が選択した場所で自分のアイデンティティを主張できるよう支援することです。その使命は、安全で相互運用性があり、プライバシーを保護するアイデンティティ標準の策定において、グローバルコミュニティをリードすることです。
Open Wallet Foundation	OWF は、オープンで安全、かつ相互運用が可能なデジタルウォレットソリューションのグローバルな普及を推進するとともに、政府諮問委員会を通じて専門知識と助言バイスを提供する、企業および非営利団体によるコンソーシアムです。 OWF は、発行者、ウォレットプロバイダー、および依存当事者が、ユーザーの選択、セキュリティ、プライバシーを保護する実装を起動するために使用できる、標準ベースの OSS コンポーネントに関する協力を通じて、デジタルウォレット技術のベストプラクティスを設定することを目指しています。
Secure Identity Alliance	アイデンティティの真の可能性を解き放ち、人、経済、社会の繁栄を実現します。
Trust Over IP Foundation	インターネット・デジタル・トラストのための完全なアーキテクチャを開発します。 そして、すべての人にとってより良いインターネットを実現します。
国連開発計画（UNDP） - Regi-Trust	発見と検証のためのDigital TRUST Infrastructure（Regi-TRUST）は、国連開発計画（UNDP）が主催・運営するインフラプロジェクトです。このプロジェクトは、ドメインネームシステム（DNS）とそのセキュリティ拡張機能という既存のインターネットインフラを活用し、信頼できるサービスの発見と検証を可能にする一連のツールを開発・提供することを目的としています。
W3C Credentials Community Group	本グループはW3Cの知的財産権（IPR）傘下にありますが、W3Cスタッフの最小限のサポートのもと、完全にボランティアにより運営されています。CCGが作成する仕様は「公式」なW3C勧告ではない。多くの仕様はCCGから、公式なW3Cワーキンググループやその他の標準化開発組織での作業へと移行します。
W3C 公式ワーキンググループ	W3Cは、ウェブの長期的な成長を保証するプロトコルとガイドラインを開発することで、ウェブの潜在能力を最大限に引き出す取り組みを主導しています。 分散型識別子（DID）、JSON-LD、Verifiable Credentials
Women In Identity	Women in Identityは、世界中の市民、社会および経済の発展を可能にする普遍的なアクセスを実現するため、多様なチームによるソリューションを構築するデジタルアイデンティティ産業を牽引しています。

付録E：プライバシーとセキュリティに関するベストプラクティス

この付録は、当方が維持・更新する「流動的な付録」である。レビュー担当者は、本稿のメッセージに沿った組織の追加を提案することができる。

FIDO Alliance	FIDO2[8]	フィッシング耐性のある認証への移行に向けたベストプラクティスガイドライン
GDPR	欧州一般データ規則	個人データの保護、処理、移動に関する規則
NIS 2	欧州指令	EU全域で共通のサイバーセキュリティ水準を確立する立法
NIST	SP800-63-4	デジタルアイデンティティガイドライン
	Cybersecurity Framework	ビジネス上の推進要因を用いてサイバーセキュリティ活動を導き、組織のリスク管理プロセスの一環としてサイバーセキュリティリスクを考慮することに重点を置く。
OECD Privacy Principles	Legal Instrument 0188	プライバシー保護および個人データの越境流通に関する勧告
OpenID Foundation	OpenID Connect Core	上記のPAは、ユーザージャーニーにおけるエンドユーザーの承認を得て、トランザクション固有の署名付きアサーションを提供する
	OIDC FAPI Profile	FAPIプロファイルは、OIDC実装者およびエコシステムが明確に定義された脅威を軽減するために使用できる、実績のあるセキュリティ設定を提供する
	OIDF ASC[9]	初期段階の仕様であり、OpenID Connectにおけるデータ最小化によるプライバシー強化を目的としている
	OpenID4VC	新興の仕様として、検証可能な認証やmDLなどの署名付きデジタル資格情報の交換を標準化して保護する取り組みである
	OpenID SSF	Shared Signals Frameworkは新たな仕様で、認証および認可段階の後にアクションが取られる可能性のあるイベント（不正が疑われる場合など）を迅速かつ効率的に通知することを可能にする

[8] （訳注）2026年1月現在は、パスキー（passkey）とも呼ばれる

[9] （訳注）OpenID Connect Advanced Syntax for Claimsのこと

	OIDC4IDA	OpenID Connect for Identity Assuranceは、特定のエンドユーザーに対して実施された本人確認保証プロセスを標準化および詳細に記述することを可能にし、依存当事者は処理をより深く理解することができる

[1] Image sourced from United Nations. *Universal Declaration of Human Rights*, 2015. e-book. 14-15.
[2] See, for example, United Nations Office of the High Commissioner of Human Rights. "Fact Sheet No.2 (Rev.1) The International Bill of Human Rights." Accessed September 1, 2023.
[3] United Nations Development Program. " "The SDGs in Action."" UNDP (Accessed June 26, 2023.)
[4] White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., Mccarthy, M., and Sperling, O. "Digital Identification: A Key to Inclusive Growth," McKinsey Global Institute (2019)
[5] Bill and Melinda Gates Foundation. "Digitization for Improved Governance: Financial Services for the Poor" (August, 2021)
[6] O'Halloran, D., George, M., Duda, C. Leong, C., Johnson, J., and Keeling, J. "Digital Identity Ecosystems: Unlocking New Value." World Economic Forum (2019)
[7] World Bank Group. "Principles on Identification for Sustainable Development: Toward the Digital Age (English)" Washington, D.C.: World Bank Group (2022)
[8] See, for example Center for Human Rights and Global Justice. "Paving a Digital Road to Hell." Center for Human Rights and Global Justice: New York University School of Law (2022).
[9] United Nations. "Guidelines on the Legislative Framework for Civil Registration, Vital Statistics and Identity Management." New York (2022)
[10] United Nations High Commissioner for Refugees. "Text of the 1954 Convention relating to the Status of Stateless Persons." New York (1954)
[11] United Nations High Commissioner for Refugees. "Convention and Protocol Relating to the Status of Refugees." New York (1967)
[12] United Nations High Commissioner for Refugees. "Convention on the Reduction of Statelessness." (1967)
[13] OECD. "Recommendation of the Council on the Governance of Digital Identity" Legal Instruments 049 (1967)
[14] United Nations. *Universal Declaration of Human Rights*, 2015. e-book. 14-15
[15] World Bank. "ID4D Global Dataset – volume 21: Global ID Coverage Estimates." (2023)
[16] UNICEF. "The State of the World's Children: Children in a Digital World" (2017)
[17] PwC, "Global Economic Crime and Fraud Survey 2022: Protecting the Perimeter," (2022)
[18] Szreter, S. "The Right of Registration: Development, Identity Registration, and Social Security – a Historical Perspective." *World Development,* 35, no. 1 (2007), https://doi.org/10.1016/j.worlddev.2006.09.004 as cited in Manby, B. "The Sustainable Development Goals and 'Legal Identity for All': 'First Do No Harm' *World Development*, 139 (2021)
[19] See, for example Wenz, K. M., Palacios, R.J. and Lantei, S. "Incentives for Improving Birth Registration Coverage: A Review of the Literature." *Identification for Development*. Washington D.C.: World Bank Group. (2017)
[20] Clark, J., Diofasi, A., and Casher, C "850 million people globally don't have ID - why this matters and what we can do about it" *World Bank Blogs* (Feb 6, 2023)
[21] Manby, B. "850 million people globally don't have ID - why this matters and what we can do about it" 139 (2021)
[22] United Nations. *Universal Declaration of Human Rights*, 2015. e-book. 14-15.

[30] United Nations Development Program "The SDGs in Action." UNDP (Accessed June 26, 2023)
[31] Manby, Bronwen. 'The Sustainable Development Goals and "Legal Identity for All": "First, Do No Harm"'. World Development 139 (2021). https://doi.org/10.1016/j.worlddev.2020.105343.
[32] Brey, Philip. 2010. 'Values in Technology and Disclosive Computer Ethics'. In *Cambridge Handbook of Information and Computer Ethics*, edited by Luciano Floridi, 41–58. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511845239.004.
[33] Nair, P. "Aadhaar breach report: Reactions on freedom and privacy" CSO Online (Jan 11, 2018)
[34] Cimpanu, C. "Hacker steals government ID database for Argentina's entire population" The Record (October 17, 2021)
[35] Sahara Reporters "EXCLUSIVE: Hacker breaks into NIMC Server, Steals Over Three Million National Identity Numbers of Nigerians" Sahara Reporters: New York (January 10, 2022)
[36] Thomson, I. "South Korea faces $1bn bill after hackers raid national ID database" The Register (October 14, 2014)
[37] Jennings, R. "Estonian Hacker Steals 300,000 Government ID Photos" Security Boulevard" (July 30, 2021)
[38] Reuters, "Dutch hacker obtained virtually all Austrians' personal data, police say" Reuters (January 25, 2023)
[39] Weinert, A. "Biometrics, Keep Your Fingers Close" Microsoft (May 26, 2020)
[40] Renieris, E.M. *Beyond Data*, MIT Press: New York (2022)
[41] O'Neil, C. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy,* New York: Penguin (2017) and Rainie, L. and Anderson, J. "Code-Dependent: Pros and Cons of the Algorithm Age" Pew Research Center (February 8, 2017)
[42] Holzl, V. "Identity and belonging in a card: how tattered Rohingya IDs trace a trail toward statelessness" The New Humanitarian (March 1, 2018)
[43] Shah, P. and Smith, R. S. "Legacies of Segregation and Disenfranchisement: The Road from Plessy to Frank and Voter ID Laws in the United States" *RSF: The Russell Sage Foundation Journal of the Social Sciences* Vol 7, No 1 (February 2021) pp. 134-146
[44] Masiero, S. "A new layer of exclusion? Assam, Aadhaar and the NRC" *London School of Economics Blogs* (September 12, 2019)
[45] Martin, M. "Germany's new e-ID cards raise hackles over privacy" Reuters (November 10, 2010)
[46] Center for Human Rights and Global Justice "Paving a Digital Road to Hell" Center for Human Rights and Global Justice: New York University School of Law (June 2022)
[47] Abouharb, M. Rodwan and Daveed Gartenstein-Ross. "The Civicness of Nations: Measuring Expectations of Government." *International Studies Quarterly*, vol. 55, no. 4, 2011, pp. 1099–1120.
[48] Sheldrake, P. "Human Identity: the Number One Challenge in Computer Science" (2022) Accessed on August 23, 2023
[49] Better Identity Coalition "Better Identity in America: A Blueprint for State Policymakers" Better Identity Coalition (2022), p. 5-6
[50] Windley, P. J. Learning Digital Identity: Design, Deploy, and Manage Identity Architectures O'Reilly Media, Inc (January 2023), p. 37

[51] Khaira, R. "Rs 500, 10 minutes, and you have access to billion Aadhaar details" The Tribune (January 3, 2018)
[52] Donnan, S. and Bass, D. "How Did ID.me Get Between You and Your Identity" *Bloomberg Businessweek* (January 20, 2022)
[53] UK Public Accounts Parliamentary Committee "Accessing public services through the government's Verify digital system" (May 8, 2019)
[54] Wilson, C. "No, You Can't Have My Social Security Number: why using SSNs for identification is risky and stupid" *Slate.com* (July 14, 2009)
[55] FirstPost "Aadhaar security breaches: Here are the major untoward incidents that have happened with Aadhaar and what was actually affected" Firstpost (January 16, 2018)
[56] Maiero, S. "Digital identity as platform-mediated surveillance" *Big Data and Society,* 10(1) (January 3, 2023)
[57] Confessore, N. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far" New York Times: London (April 4, 2018)
[58] Burt, C. "Nigeria ID4D head calls for stronger legal framework to support digital ID consistency" *Biometric Update.com* (November 30, 2022)
[59] See, for example UK Public Accounts Parliamentary Committee "Accessing public services through the government's Verify digital system" (May 8, 2019) and Donnan, S. and Bass, D. "How Did ID.me Get Between You and Your Identity" *Bloomberg Businessweek* (January 20, 2022)
[60] Khaira, R. "Rs 500, 10 minutes, and you have access to billion Aadhaar details" The Tribune (January 3, 2018)
[61] Consumer Financial Protection Bureau "Equifax data breach settlement" Accessed on September 1, 2023
[62] Confessore, N. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far" New York Times: London (April 4, 2018)
[64] Solove, D. J. and Hartzog, W. *Breached! Why Data Security Law Fails and How to Improve It* Oxford University Press (March 1, 2022)
[65] Renieris, E.M. *Beyond Data* MIT Press: New York (2022)
[66] See, for example, Sheldrake, P. "Human Identity: the Number One Challenge in Computer Science" (2022) Accessed on August 23, 2023
[67] Andrieu, J. "A Primer on Functional Identity" Web Of Trust (November 18, 2019)
[68] United Nations "Human Rights Instruments" United Nations (Accessed on Jun 25, 2023)
[69] Woman in Identity "Code of Conduct: the Human Impact of Identity Exclusion" Women in Identity (Accessed on June 25, 2023)
[70] Bertrand, A. and McQueen, J. "How can digital government connect citizens without leaving the disconnected behind?" Ernst and Young (February, 24, 2021)
[71] Oppenheim, M. "How NHS is inadvertently telling domestic abusers where they can track down their victims" The Independent (February 16, 2022)
[72] Figure 3 references include:
World Bank. "ID4D Global Dataset – volume 21: Global ID Coverage Estimates." (2023)
United Nations Refugee Agency "Statelessness around the world" Accessed on September 5, 2023
United Nations Refugee Agency "1 percent of humanity displaced: UNHCR Global Trends Report" (June 18, 2020)
AARP "1 in 5 Americans Now Provide Unpaid Family Care" (July 15, 2022)

Freedom House “Freedom in the World 2023” (March, 2023)
United Nations Office on Drugs and Crime “Victim Assistance and Witness Protection” Accessed on September 10, 2023
World Health Organization “Disability” (March 7, 2023)
Huecker, M.R., King, K.C., Jordan, G.A., Smock, W. “Domestic Violence” National Library of Medicine. Last updated April 9, 2023.
[73] Breckenridge, K. and Szreter, S. "Registration and Recognition: Documenting the Person in World History" 39:3 (January 2014)
[74] Nyst, C., Pannifer, S., Whitley, E., Makin, P. "Digital Identity: Issue Analysis" version 1.6. Consult Hyperion (June 8, 2016)
[75] ibid
[76] Handforth, C. and Wilson, M. "Digital Identity Country Profile: Uganda" GSMA: London, UK (2019)
[77] BankID "About Us" BankID (Accessed on June 15, 2023)
[78] Interac "Access government services with Interac sign in service" Interac (Accessed on June 25, 2023)
[79] European Commission "The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework" v1.0.0
[80] Nyst, C., Pannifer, S., Whitley, E., Makin, P. "Digital Identity: Issue Analysis" version 1.6. Consult Hyperion (June 8, 2016) 161-175
[81] Nyst, C., Pannifer, S., Whitley, E., Makin, P. "Digital Identity: Issue Analysis" version 1.6. Consult Hyperion (June 8, 2016)
[82] Monetary Authority of Singapore "Foundational Digital Infrastructures for Inclusive Digital Economies" Singapore (April 2021)
[83] Open Identity Exchange (OIX) “Trust Frameworks for Smart Digital ID” (June 2022) [10]
[84] Singpass "Your improved digital ID to make life easy" Singapore: Singpass (Accessed June 26, 2023)
[85] e-estonia "e-Identity" (Accessed on July 3, 2023)
[86] Supreme Court of India "Writ Petition (Civil) No. 494 of 2012" New Delhi: Supreme Court of India (September 26, 2018) *See Also:* Varadhan, S. and Mohanty, S. "Supreme Court imposes curbs on use of Aadhaar" Reuters Technology News (September 26, 2018)
[87] Iruoma, K. "Got your number: Privacy concerns hobble Nigeria's digital ID push" Reuters (August 5, 2021)
[88] Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, and Unwanted Witness "Chased Away and Left to Die" (June 8, 2021)
[89] Puckett, C. "The Story of the Social Security Number" *Social Security Bulletin* 69 (2) U.S. Social Security Administration (2009)
[90] Unique Identification Authority of India "Usage of Aadhaar" (Accessed on July 3, 2023)
[91] Bill and Melinda Gates Foundation, “Digitization for Improved Governance: Financial Services for the Poor,” (2021) p.12-13
[92] Supreme Court of India "Writ Petition (Civil) No. 494 of 2012" New Delhi: Supreme Court of India (September 26, 2018) *See Also:* Varadhan, S. and Mohanty, S. "Supreme Court imposes curbs on use of Aadhaar" Reuters Technology News (September 26, 2018)
[93] Young, K. "Key Differences Between the U.S. Social Security System and India's Aadhaar System" New America (August 5, 2019)
[94] Unique Identification Authority of India "Aadhaar e-KYC API Specification - Version 2.0" (May 2016)

[10] （訳注）Open Identity Exchangeは2026年1月1日現在、組織は運営を停止している

[95] Business Standard "Aadhaar a 'bedrock' for govt welfare schemes, saved over RS 2trn" Business Standard (June 01, 2022)
[96] Nar, P. "Aadhaar breach report: Reactions on freedom and privacy" CSO (Jan 11, 2018)
[97] Henne, Kathryn. "Surveillance in the Name of Governance: Aadhaar as a Fix for Leaking Systems in India." *Information, Technology and Control in a Changing World*, June 22, 2019, 223–45.
[98] Kumar, A. (ed) "How fraudsters are using loopholes in Aadhaar system to create Fake IDs" India.com (March 18, 2023)
[99] National Identity Management Commission "National Identity Management Commission: providing assured identity" NIMC (Accessed on June 26, 2023)
[100] Nigeria Data Protection Commission "Nigeria Data Protection Bill, 2022" NDPC (Accessed June 26, 2023)
[101] Biometric Update "Nigeria's national biometric ID proposed to go digital, add DNA" Biometric Update (August 16, 2020)
[102] Federal Republic of Nigeria Official Gazette "Mandatory Use of the National Identification Number Regulations, 2017" Lagos: Federal Republic of Nigeria Official Gazette, 104: 121 (November 13, 2017)
[103] National Identity Management Commission "Enhanced NIMC Verification System v1.0" NIMC.gov (Accessed June 26, 2023)
[104] OSIA "Unlocking the ID Ecosystem with OSIA: a universal interoperability framework for innovation, competition, and sustainability" Accessed on September 21, 2023
[105] Iruoma, K. "Got your number: Privacy concerns hobble Nigeria's digital ID push" Reuters (August 5, 2021)
[106] McSweeney, E. "As Covid-19 cases rise in Nigeria, a government policy is creating crowds and chaos" CNN (February 10, 2021)
[107] Singpass "Your improved digital ID to make life easy" Singapore: Singpass (Accessed June 26, 2023)
[108] GovTech Singapore "All Government Agencies to Accept Singpass Digital IC from 1 November 2021" (October 28, 2021)
[109] Post, V. "The evolution of Singpass: How Singapore's national digital identity came about" KrAsia (April 27, 2023)
[110] Macellino, A. "Singpass introduces biometric face verification, Kofax integrates digital signatures" Biometric Update (December 17, 2020)
[111] Cooper, A., Marskell, J., and Chan, C.H. "National Digital Identity and Government Data Sharing in Singapore" The World Bank ID4D and Govtech Singapore (2022) pp xiv
[112] Ibid, pp 46
[113] En, T.J. "Singapore's flawed data privacy regime" New Naratif (June 11, 2018)
[114] Ministero dell'Interno "Electronic Identity Card (CIE)" Carta Identita Interno (Accessed on June 26, 2023)
[115] Agenzia per l'Italia Digitale "SPID Public Digital Identity System" (Accessed on June 26, 2023)
[116] Mascellino, A. "Italian national digital ID scheme reaches 30 million users milestone" Biometric Update (May 9, 2022)
[117] DIACC "Pan-Canadian Trust Framework" DIACC (Accessed June 26, 2023)
[118] UK Parliament "Accessing public services through the Government's Verify digital system" London: UK Parliament (May 8, 2019)

119 BankID "BankID: We ensure safe and secure identification and signing" BankID (Accessed June 26, 2023)
120 Official Journal of the European Union "Regulation (EU) 2016/679 Of the European. Parliament And Of The Council" (April 27, 2016)
121 Ministry of Local Government and Districts "Act on the Implementation of the EU Regulation on electronic identification and trust services for electronic transactions in the internal market" (June 15, 2018)
122 BankID "BankID with Biometrics" BankID (Accessed on June 27, 2023)
123 Hersey, F. "Digital parenting, minimized fraud and a 'just do it' attitude: Future Identity Festival" Biometric Update (November 17, 2021)
124 DIACC "Pan-Canadian Trust Framework" DIACC (Accessed June 26, 2023)
125 Office of the Privacy Commissioner of Canada "The Personal Information Protection and Electronic Documents Act (PIPEDA)" (Accessed on July 5, 2023)
126 Avast "Avast to Acquire SecureKey Technologies" PRNewswire (March 24, 2022)
127 SecureKey Technologies "Verifie[11]d Me: Your Identity in Your Control" (December 2019)
128 European Commission "Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity" COM(2021) 281 final. Brussels: European Commission (June 3, 2021)
129 Macdonald, A. "Bhutan launches self-sovereign biometric digital ID, crown prince first to enroll" Biometric Update (February 23, 2023)
130 British Columbia "Digital Credential Services" (Accessed on June 27, 2023)
131 John, A. "US Digital Immigration Credentials Overview" FedID Conference Slides (December, 2022)
132 International Organization for Standardization "ISO/IEC 18013-5 Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application" ISO (September 2021) 133 Council of the EU "European digital identity (eID): Council makes headway towards EU digital wallet, a paradigm shift for digital identity in Europe" Brussels: Press Release (December 6, 2022) 134 European Commission "The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework" v1.0.0
135 W3C "Verifiable Credentials Data Model v1.1" (March 3, 2022)
136 Lodderstedt, T., Yasuda, K., Looker, T. (eds) "OpenID for Verifiable Credential Issuance" OpenID Foundation (February 3, 2023)
137 Terbu, O., Lodderstedt, T., Yasuda, K., Looker, T. "OpenID for Verifiable Presentations - draft 18" OpenID Foundation (April 21, 2023)[12]
138 Yasuda, K., Jones, M., and Lodderstedt, T. "Self-Issued OpenID Provider v2" OpenID Foundation (January 1, 2023)
139 International Organization for Standardization "ISO/IEC 18013-5 Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application" ISO (September 2021)
140 Fett, D., Yasuda, K. and Campbell, B. "Selective Disclosure JWTs (SD-JWT)" IETF Draft
141 Sporny, M. Longley, D., Kellogg, K., Lanthaler, M., Champin, PA, Lindstrom, N. "JSON LD 1.1" W3C (July 16, 2020)[13]
142 John, A. "US Digital Immigration Credentials Overview" FedID Conference Slides (December, 2022)
143 Baker, B., Miller, S. "Estimates of the Lawful Permanent Resident Population in the United States and the Subpopulation Eligible to Naturalize: 2022" Homeland Security: Office of Immigration Statistics (October 2022)

11 （訳注）2026年1月1日現在、原文のURLは現在リンク切れ。アーカイブ等は確認できず

12 （訳注）OpenID for Verifiable Presentationsは、2025年9月、最終仕様が承認された（リンク）

13 （訳注）Selective Disclosure JWTs (SD-JWT)は、2025年11月、最終仕様が正式公開された（リンク）

144 W3C "Verifiable Credentials Data Model v1.1" (March 3, 2022)
145 W3C "Decentralized Identifiers (DIDs) v1.0" (July 19, 2022)
146 Thales "Gemalto wins U.S. Government Grant for DDL Pilot in Four Jurisdictions" Thales Group (November 14, 2016)
147 Hersey, F. "Digital ID Credentials come to the Apple Wallet, inform apps, but EU may cause friction" Biometric Update (October 4, 2022)
148 OECD, "Recommendation of the Council on the Governance of Digital Identity" Legal Instruments 0491 (2023)
149 ID2020 "ID2020 Technical Requirements" ID2020 Certification (April 28, 2019; Accessed June 26, 2023)
150 World Bank Group "Principles on Identification for Sustainable Development: Toward the Digital Age (English)" Washington, D.C.: World Bank Group (November 3, 2022)
151 O'Halloran, D., George, M., Duda, C. Leong, C., Johnson, J., and Keeling, J. "Digital Identity Ecosystems: Unlocking New Value" World Economic Forum (September 2021)
152 Mothershaw, N. "Trust Frameworks for [14]Smart Digital ID" The Open Identity Exchange (June 2022)
153 de Brisis M.M. and Brennan, J. "Universal Digital Identity Policy Principles to Maximize Benefits for People: A shared European and Canadian Perspective" DIACC and Human Technology Foundation (November 2, 2022)
154 Solove, D. J. and Hartzog, W. *Breached! Why Data Security Law Fails and How to Improve It* Oxford University Press (March 1, 2022), p.176
155 Planetwork "Augmented Social Network" (Accessed on June 27, 2023)
156 See, for example, Masiero, S. and Bailur, S. "Digital Identity for Development: the quest for justice and a research agenda" *Information Technology for Development*, 27:1, pp.1-12 (2021) Further sources can be found on the Global Data Justice website
157 de Brisis M.M. and Brennan, J. "Universal Digital Identity Policy Principles to Maximize Benefits for People: A shared European and Canadian Perspective" DIACC and Human Technology Foundation (November 2, 2022)
158 ID2020 "Manifesto" (Accessed on June 27, 2023)
159 World Bank Group "Principles on Identification for Sustainable Development: Toward the Digital Age (English)" Washington, D.C.: World Bank Group (November 3, 2022)
160 Woman in Identity "Code of Conduct: the Human Impact of Identity Exclusion" Women in Identity (Accessed on June 25, 2023)
161 O'Halloran, D., George, M., Duda, C. Leong, C., Johnson, J., and Keeling, J. "Digital Identity Ecosystems: Unlocking New Value" World Economic Forum (September 2021)
162 Trust Over IP Foundation "Overcoming Human Harm Challenges in Digital Identity Ecosystems" V1.0 Trust Over IP Foundation (November 16, 2022)
163 https://www.mydata.org/participate/declaration/ chapter 3
164 OECD, "Recommendation of the Council on the Governance of Digital Identity" Legal Instruments 0491 (2023)
165 See, for example Manby, Bronwen. 'The Sustainable Development Goals and "Legal Identity for All": "First, Do No Harm"'. World Development 139 (2021). https://doi.org/10.1016/j.worlddev.2020.105343. [copy attached, since this is not open access]
166 United Nations.*Universal Declaration of Human Rights*, 2015. e-book. 14-15

[14] （訳注）Open Identity Exchangeは2026年1月現在、運営を停止しており原文のURLは現在リンク切れ。アーカイブ等は確認できず

[167] United Nations High Commissioner for Refugees. "Convention and Protocol Relating to the Status of Refugees." New York (1967)
[168] United Nations High Commissioner for Refugees. "Text of the 1954 Convention relating to the Status of Stateless Persons." New York (1954)
[169] United Nations Office on Drugs and Crime "Victim Assistance and Witness Protection" Accessed on September 10, 2023
[170] United Nations "Convention on the Rights of the Child" (November, 1989)
[171] United Nations Department of Economic and Social Affairs "Guidelines on the Legislative Framework for Civil Registration, Vital Statistics, and Identity Management Systems" New York (2023) [172] de Brisis M.M. and Brennan, J. "Universal Digital Identity Policy Principles to Maximize Benefits for People: A shared European and Canadian Perspective" DIACC and Human Technology Foundation (November 2, 2022)
[173] UK Parliament "Accessing public services through the Government's Verify digital system" London: UK Parliament (May 8, 2019)
[174] Luma Institute "Innovating for People: Handbook of Human-Centered Design Methods" (February 22, 2021)
[175] unicef "Human Centered Design 4 Health" unicef (Last Accessed June 27, 2023)
[176] Krippendorf, Klaus "Intrinsic motivation and human-centred design" *Theoretical Issues in Ergonomics Science,* 5(1) (2004) 43-72 as cited in Sheldrake, P. "Once more with meaning – a review of a draft industry paper on human-centric digital identity" (August 14, 2023)
[177]de Brisis M.M. and Brennan, J. "Universal Digital Identity Policy Principles to Maximize Benefits for People: A shared European and Canadian Perspective" DIACC and Human Technology Foundation (November 2, 2022)
[178]Morrison, R. "UK supermarket digital ID trial success could see law changed" Tech Monitor (January 3, 2023)
[179]White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., Mccarthy, M., and Sperling, O., "Digital Identification: A Key to Inclusive Growth," McKinsey Global Institute (2019)
[180]Bertrand, A. and McQueen, J. "How can digital government connect citizens without leaving the disconnected behind?" Ernst and Young (February, 24, 2021)
[181] OECD, "Recommendation of the Council on the Governance of Digital Identity" Legal Instruments 0491 (2023)
[182]Secure Identity Alliance "Giving Voice to Digital Identities Worldwide: Key Insights and Experiences to Ovvercome Shared Challenges" Secure Identity Alliance (2021)
[183]Woman in Identity "Code of Conduct: the Human Impact of Identity Exclusion" Women in Identity (Accessed on June 25, 2023).
[184] See, for example Davis, Fred D. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology" MIS Quarterly 13 (3): 319–40.
[185]Ravenscraft, E. "How to Spot - and Avoid - Dark Patterns on the Web" Wired (July 29, 2020). [186]Myers, S.L. "How Social Media Amplifies Misinformation More than Information" New York Times (October 13, 2022).
[187]Pimintel, B. "Banks and fintechs agree: It's time for screen scraping to go. So what's next?" Protocol (October 5, 2021)[15]

[15] （訳注）2026年1月1日現在、原文のURLは現在リンク切れ。アーカイブ等は確認できず

[188] Winkler, T. and Spiekermann, S. "Twenty years of value sensitive design: a review of methodological practices in VSD projects" *Ethics and Information Technology,* 23, pp. 17-21 (March 2021)
[189] Van de Poel, I. "Embedding Values in Artificial Intelligence (AI) Systems." *Minds and Machines* 30, 385-409 (2020)
[190] Umbrello, S. and van de Poel, I. "Mapping Value Sensitive Design onto AI for Social Good Principles" *AI Ethics* 1(3) 283-296 (2021)
[191] Winkler, T. and Spiekermann. "Twenty yfears of value sensitive design: a review of methodologicalpractices in VSD projects" *Ethics and Information Technology,* 23 (2021) https://doi.org/10.1007/s10676-018-9476-2
[192] Marsman, Henk. "Is the Capabilities Approach Operationalizable to Analyse the Impact of Digital Identity on Human Lives." Data & Policy 4 (2022): e43. doi:10.1017/dap.2022.37.
[193] Woman in Identity "Code of Conduct: the Human Impact of Identity Exclusion" Women in Identity (Accessed on June 25, 2023)
[194] Solove, D. J. and Hartzog, W. *Breached! Why Data Security Law Fails and How to Improve It* Oxford University Press (March 1, 2022) p.191
[195] See, for example Manby, Bronwen. 'The Sustainable Development Goals and "Legal Identity for All": "First, Do No Harm"'. World Development 139 (2021). https://doi.org/10.1016/j.worlddev.2020.105343.
[196] Solove, D. J. and Hartzog, W. *Breached! Why Data Security Law Fails and How to Improve It* Oxford University Press (March 1, 2022) page number
[197] Renieris, E.M. *Beyond Data* MIT Press: New York (2022) page number
[198] Confessore, N. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far" New York Times: London (April 4, 2018) https://www.nytimes.com/2018/04/04/us/politics/cambridge- analytica-scandal-fallout.html
[199] Renieris, E.M. *Beyond Data* MIT Press: New York (2022)
[200] Solove, D. J. and Hartzog, W. *Breached! Why Data Security Law Fails and How to Improve It* Oxford University Press (March 1, 2022)
[201] Lips, S., Tsap, V., Bharosa, N, Draheim, D., Krimmer, R., and Tammet, T. "Management of National eID Infrastructure as a State-Critical Asset and Public-Private Partnership: Learning from the Case of Estonia (May 19, 2022)
[202] Mothershaw, N. "Trust Frameworks for Smart Digital ID" The Open Identity Exchange (June 2022)[16]
[203] Mothershaw, N. "Trust Frameworks for Smart Digital ID" The Open Identity Exchange (June 2022) [17]
[204] de Brisis M.M. and Brennan, J. "Universal Digital Identity Policy Principles to Maximize Benefits for People: A shared European and Canadian Perspective" DIACC and Human Technology Foundation (November 2, 2022)
[205] Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, and Unwanted Witness "Chased Away and Left to Die" (June 8, 2021)
[206] Center for Human Rights and Global Justice "Paving a Digital Road to Hell" Center for Human Rights and Global Justice: New York University School of Law (June 2022)
[207] Bhandari, V., Trikanad, S. and Sinha, A. "Governing ID: A Framework for Evaluation of Digital Identity" Centre for Internet and Society, India (January 22, 2020)
[208] van der Straaten, J. "Identification for Development It Is Not: Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable' - A Review" (November 20, 2020)

[16] （訳注）Open Identity Exchangeは2026年1月現在、運営を停止しており原文のURLは現在リンク切れ。アーカイブ等は確認できず

[17] （訳注）Open Identity Exchangeは2026年1月現在、運営を停止しており原文のURLは現在リンク切れ。アーカイブ等は確認できず

209 Easterly, J. "Congressional Hearing On Evolving the U.S. Approach to Cybersecurity: Raising the Bar Today to Meet the Threats of Tomorrow" Washington, D.C.: US House of Representatives - Homeland Security Committee (November 3, 2021)
210 Solove, D. J. and Hartzog, W. *Breached! Why Data Security Law Fails and How to Improve It* Oxford University Press (March 1, 2022)
211 "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)." European Union, December 14, 2020. http://data.europa.eu/eli/dir/2022/2555/oj.
212 NIST "SP 800-63-4 (draft) Digital Identity Guidelines" NIST (December 16, 2022)[18]
213 Solove, D. J. and Hartzog, W. *Breached! Why Data Security Law Fails and How to Improve It* Oxford University Press (March 1, 2022)
214 OECD. "Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data." OECD Legal Instruments, October 7, 2013. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.
215 "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)." European Union, May 4, 2016.
216 Council of Europe. "Convention for the protection of individuals with regard to the processing of personal data." Convention 108+. (June 2018)
217 University of Stuttgart "The Web Infrastructure Model (WIM)" https://www.sec.uni-stuttgart.de/research/wim (Last Accessed September 24, 2023)
218 https://www.nist.gov/itl/ssd/information-systems-group/overview-conformance-testing
219 Young, K. *The Domains of Identity* Anthem Press (June 25, 2020)
220 European Commission. Directorate General for Informatics. 2017. New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations. LU: Publications Office. https://data.europa.eu/doi/10.2799/78681
221 Open Identity Exchange. "OIX defines the need for clear, global data standards for identity information." August 29, 2023.[19]
222 Trust Over IP Foundation "Why Trust Over IP" Trust Over IP Foundation (November 16, 2022)
223 MyData Operators. https://mydata.org/operators. (Last Accessed September 24, 2023)
224 Garber, E., Mothershaw, N., Labriolle, S., and Comparin, D. "GAIN in 2023" (2023)
225 European Commission "The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework" v1.0.0
226 Theodorou, Y. "Modernising Digital-ID Systems: What Open Standards and Open-Source Software Really Mean" Tony Blair Institute for Global Change (December 15, 2022)
227 "The Mobile Economy - The Mobile Economy." 2022. The Mobile Economy. November 29, 2022. https://www.gsma.com/mobileeconomy/#key_stats.
228 "ID2020 Technical Requirements: v1.0" https://docs.google.com/document/d/1L0RhDq98xj4ieh5CuN-P3XerK6umKRTPWMS8Ckz6_J8/edit (Last Accessed September 24, 2023)
229 World Bank Group et al (2022) Principles on Identification for Sustainable Development https://www.idprinciples.org/

[18]（訳注）SP800-63-4は、2025年8月に正式に出版された（リンク）

[19]（訳注）Open Identity Exchangeは2026年1月現在、運営を停止しており原文のURLは現在リンク切れ。アーカイブ等は確認できず

[230] World Economic Forum. "Unlocking Identity Ecosystems: Unlocking New Value." (September 2021)
[231] "Universal Digital Identity Policy Principles to Maximize Benefits for People: A Shared European and Canadian Perspective." 2022. Digital ID & Authentication Council of Canada. November 2, 2022. https://diacc.ca/2022/11/02/policy-design-principles-to-maximize-people-centered-benefits-of- digital-identity/.
[232] OECD Privacy Principles, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491