令和４年度デジタル取引環境整備事業（「Ｔｒｕｓｔｅｄ Ｗｅｂ」の実現に向けた技術動向調査）

Trusted Webに係る海外動向調査報告書

2023年3月30日

株式会社エヌ・ティ・ティ・データ経営研究所

目次

1. 調査の背景・目的等

1.1 調査の背景・目的

仕様書の抜粋部分

Covid-19を契機に社会全体のデジタルトランスフォーメーション（DX）が加速し、サイバーとフィジカルが融合していく中で、様々な社会活動のデジタル化が進む「デジタル社会」に移行している。しかしながら、フェイクニュースやプライバシーリスク等の様々な課題が顕在化し、“一握りの巨大企業への依存”でも、“監視社会”でもない第三の道を模索することが必要となっている。このような中で、デジタル社会の基盤として発展してきたインターネットとウェブでは、データの受け渡しのプロトコルは決められているが、Identity管理も含め、データ・マネジメントの多くはプラットフォーム事業者など各サービスに依存し、サイロ化され、外部からの検証可能性が低く、「信じるほかない」状況となっている。

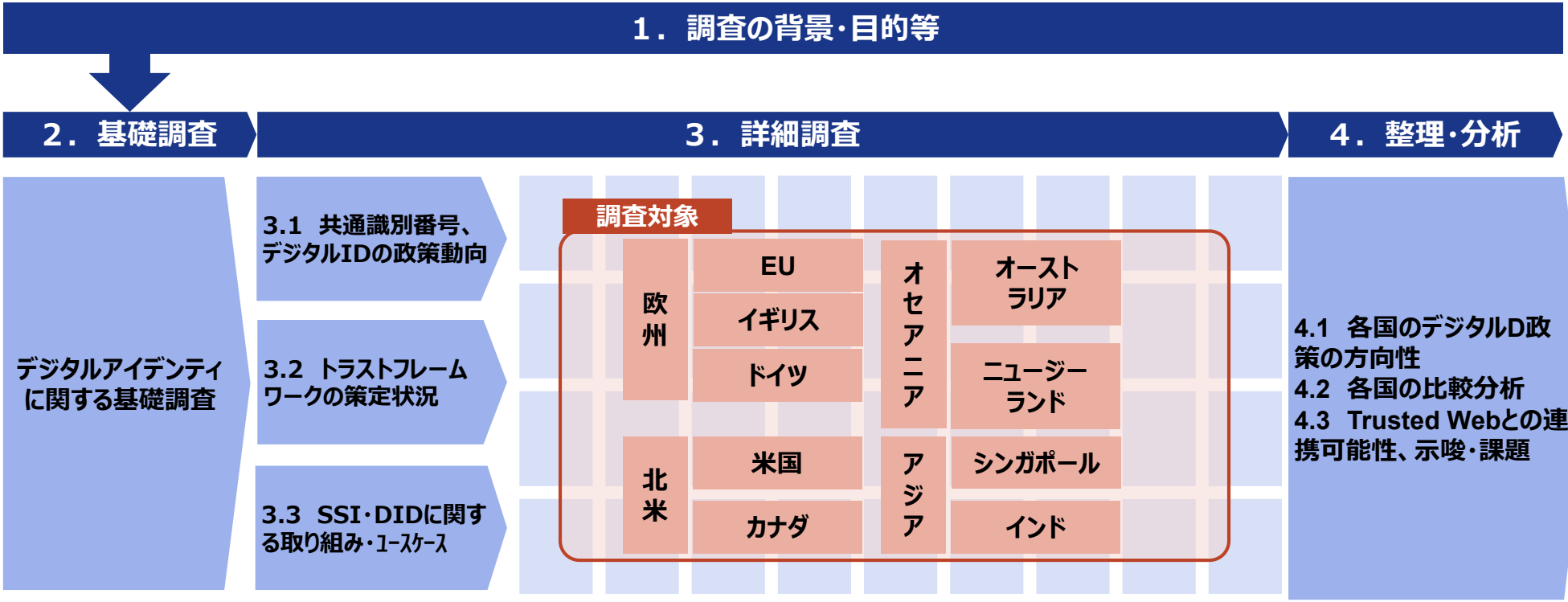
こうした中、2020年6月のデジタル市場競争会議における「デジタル市場競争に係る中期展望レポート」の提言を受け、データ・フリー・フロー・ウィズトラスト（DFFT）の具現化も視野に、2020年10月、内閣官房において「Trusted Web推進協議会」が発足した。

- Trusted Webでは、データ及びそのやり取りの検証可能領域を拡大するとともに、ユーザー（個人・法人等）による主体的なデータコントロールを可能にすることによって、デジタル社会の信頼性（Trust）の向上を目指している
- 本調査では、そのようなTrusted Webの実現を推進するため、諸外国における類似の取り組み動向を調査し、Trusted Webとの連携可能性や実現に向けた示唆を抽出することを目的とした

調査の全体像

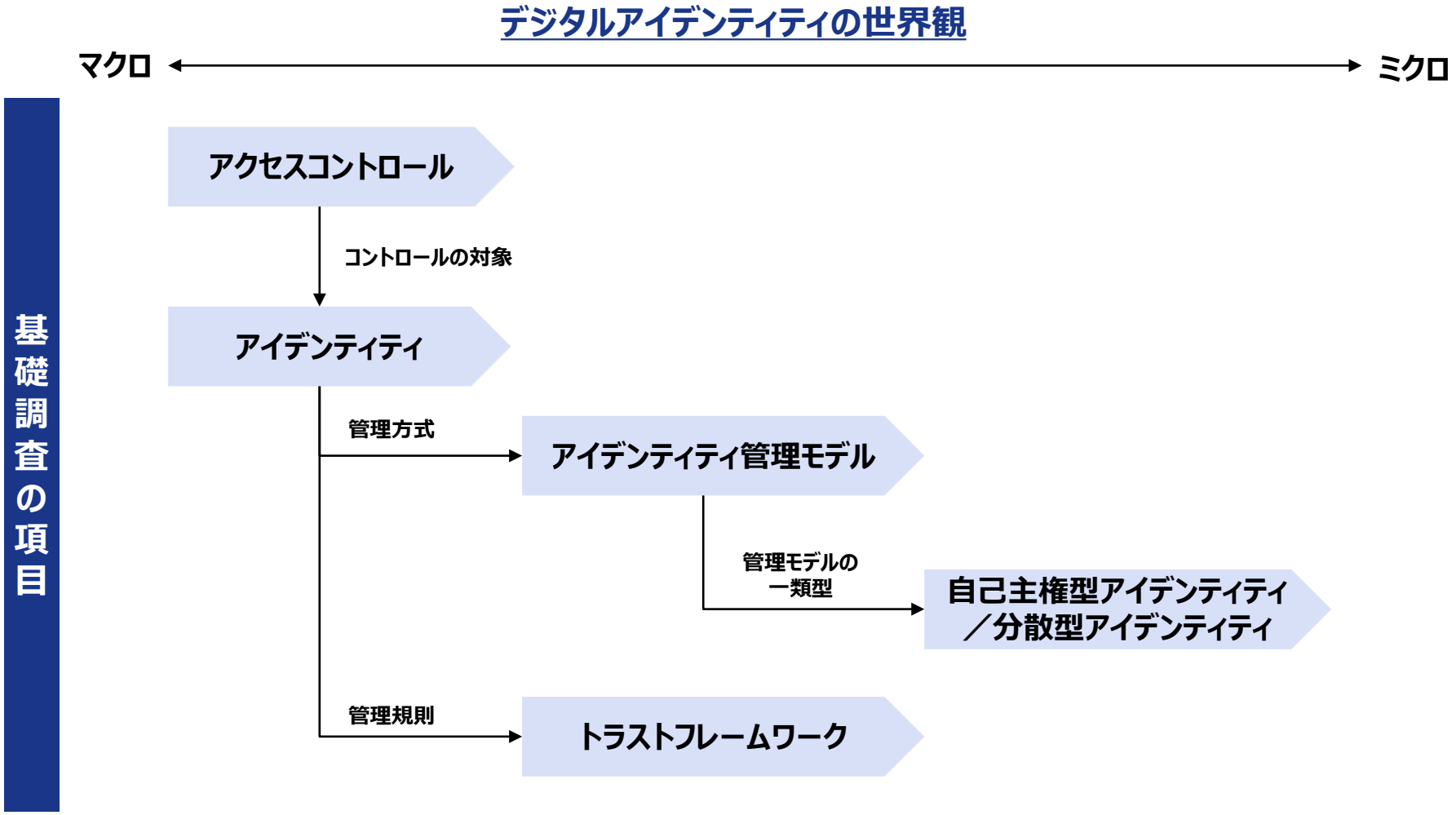
- デジタルアイデンティ周辺の基礎調査を整理するとともに、各国・地域の共通識別番号・デジタルIDに関する政策動向、トラストフレームワークの策定状況、自己主権型/分散型アイデンティティに関する取り組み状況及びそれらを活用したユースケースの3項目を個別テーマとして調査する
- 調査結果を基に各国・地域の制度・取り組みを横並びで整理・分析することによって、Trusted Webとの親和性が高く連携可能性のある国・地域・取り組み、Trusted Webの実現に向けた課題・示唆等を抽出する

調査の全体イメージ



基礎調査について

Trusted Webの問題意識は、デジタル社会の通信基盤たるインターネット・Webにおけるアイデンティティ管理に重点が置かれていることから、3章で実施する自己主権型IDや分散型ID等の各論の調査を行う上で必要となるデジタルアイデンティティ全体の世界観の基礎調査について整理した



詳細調査について

Trusted Webの問題意識は、デジタル社会の通信基盤たるインターネット・Webにおけるアイデンティティ管理に重点が置かれていることから、本調査の対象とする諸外国の取り組みについては、デジタルID周辺の動向、特に自己主権型/分散型アイデンティティに関する動向及びそれらに関連したユースケースについて調査を実施した

- **共通識別番号・デジタルIDに関する政策動向**
  データやサービスへのアクセスする際の「識別」・「認証」の手段となる共通識別番号やデジタルIDに係る諸外国の政策の変遷や最近の動向について調査を実施した
- **トラストフレームワークの策定状況**
  デジタルID及びデジタルIDに紐づくデータの利活用を含むアイデンティティ管理においては、データを取り扱う主体や、その果たすべき役割、セキュリティ基準などについて、いわゆるトラストフレームワークとして参照すべき法律・規則が定められている。諸外国のトラストフレームワークの策定状況や規定されている内容について調査を実施した
- **自己主権型／分散型アイデンティティに関する取り組み・ユースケース**
  中央集権的なID情報の管理への懸念に対するソリューションとして、Trusted Webにおいても参照されている自己主権型アイデンティティ（Self-Sovereign Identity: SSI）、分散型アイデンティティ（Decentralized Identity: DID）に関する諸外国の取り組み動向、及び関連技術の利活用事例（ユースケース）について調査を実施した

詳細調査における調査対象国・地域について

調査対象国・地域については、欧州・北米・オセアニア・アジア各地域の中でデジタルIDに関する議論や利活用が盛んであり、先行事例の見られる国・地域を抽出した

調査対象国・地域

国・地域		選定のポイント
欧州	EU[1]	• EU加盟国間での識別・認証に利用可能なデジタルIDであるeIDやeIDを活用したトラストサービスについて規定したeIDASの改正提案、その中で取り組まれているdigital identity wallet構想など、関連取組多数
	イギリス	• 政府が民間のIDプロバイダに認定を行い、公共サービスにおいて利用可能とするGOV.UK Verifyや共有トラストフレームワークであるUK digital identity and attributes trust frameworkの策定を推進
	ドイツ[1]	• eIDカード（電子身分証）を使った公共サービスの利用推進やSSIの実現に向けた政府プロジェクトを積極的に実施
北米	米国	• 連邦政府機関がデジタルIDサービスを実装するためのガイドラインであるNIST SP-800-63の策定、州・企業の単位でSSI、DIDに関する取り組み多数
	カナダ	• デジタルIDを安全に活用するためのフレームワークであるPan-Canadian Trust Frameworkの策定やブリティッシュコロンビア州におけるDIDs（分散型識別子）の活用など、関連取組多数
オセアニア	オーストラリア	• デジタルIDシステム内のプロバイダーとサービスに対する規則・標準を示したフレームワークであるTrusted Digital Identity Frameworkの策定、デジタルIDエコシステムの実現に向けた取組など
	ニュージーランド	• ニュージーランドにおけるデジタルIDサービスの法的な枠組みを規定したDigital Identity Trustframeworkの策定など
アジア	シンガポール	• 国民識別番号（NRIC、FIN）を利用した基盤であるSingpassの構築及びそれを中心としたデジタルIDサービス活用事例
	インド	• 顔写真、指紋、虹彩及び氏名住所などの登録と12桁のID番号を付与する共通識別番号Aadhaarの構築と、デジタルIDサービスへの利活用

1）EUはEUとしての取組のみを調査対象とし、ドイツはEUの取組とは直接的に関連のないドイツ独自の取組を調査対象とする

整理・分析について

**整理・分析にあたっては、調査結果を踏まえて各国のデジタルID政策の方向性を整理し、その中でもTrusted webと共通した課題を解決し得るSSI／DIDに関する取り組み状況が活発的な国・地域について比較を行う
さらにSSI/DIDを推進する政策動向について分析することで、Trusted Webとの連携可能性、実現に向けた示唆の抽出を試みる**

調査結果の整理・分析イメージ

4.1 調査結果を踏まえた各国のデジタルID政策の方向性の整理	4.2 各国の比較分析	4.3 Trusted Webとの連携可能性、示唆・課題
• 各調査テーマの結果を各国ごとに整理・一般化した上で、国ごとのデジタルID政策の方向性について整理する	• 前段階での整理結果を踏まえ、特にSSI／DIDの取り組みが比較的活発な国・地域について比較を行う • その後共通識別番号・デジタルID・トラストフレームワークの観点からSSI／DIDの取り組みに影響を及ぼしていると思われる事項を分析する	• 前段階で分析したSSI／DIDの取り組みに影響を及ぼしている事項、及びこれまでの調査結果から、Trusted Webとの連携可能性、取り組みに対する示唆・課題を抽出する

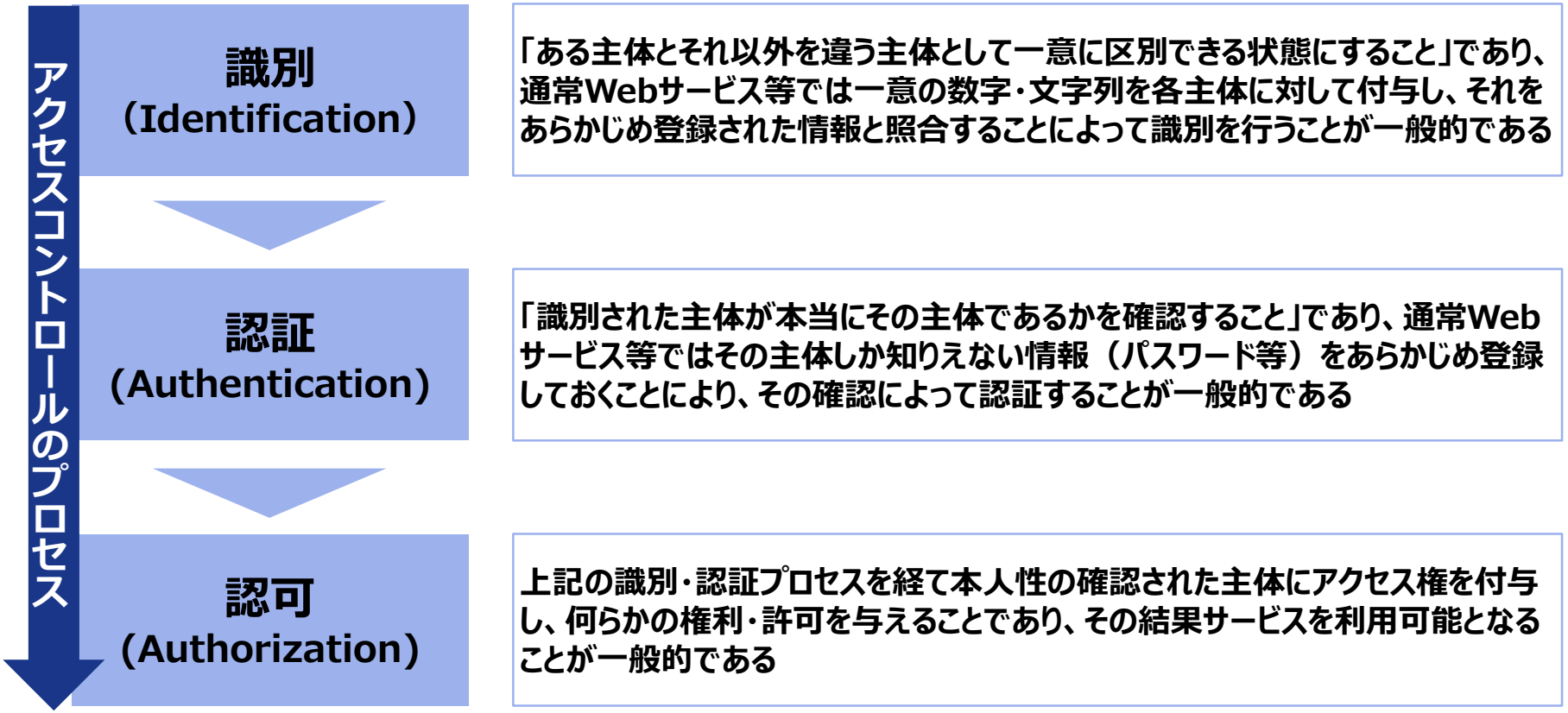
2. デジタルアイデンティに関する基礎調査

2.1 アクセスコントロールとトラスト

ユーザーがインターネットやWebを通じてデータやサービスへアクセスする際には、識別・認証・認可の各プロセスを経て、そのアクセスを適切に制御（コントロール）することで、ユーザー及びユーザーに紐づく各種データのトラスト[1]を保証している

1） TrustedWebにおける「トラスト：Trust」の定義：事実の確認をしない状態で、相手先が期待したとおりに振る舞うと信じる度合い

アクセスコントロールにおける識別・認証・認可のプロセス

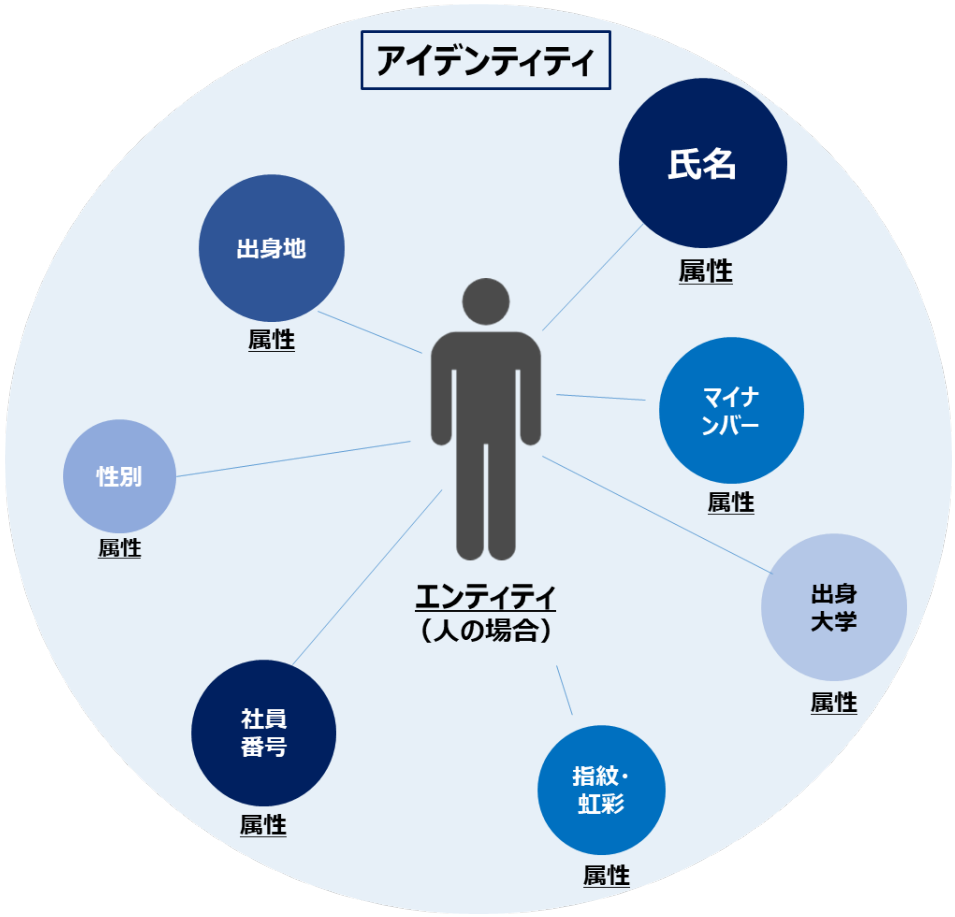


参考）JISハンドブック、ISO/IEC 24760-1

2.2 アイデンティティ

アクセスコントロールにおいては、ある主体（エンティティと呼ぶ）にまつわる属性情報を識別・認証することによりアクセスの認可を与える。ISO/IEC24760-1では、エンティティに関連する属性情報のことをアイデンティティ（identity：ID）と定義している

アイデンティティとエンティティ・属性情報の関係性



参考）ISO - ISO/IEC 24760-1:2011 - 情報技術 — セキュリティ技術 — ID 管理のフレームワーク — パート 1: 用語と概念

2.2 アイデンティティ：デジタルアイデンティティ

アイデンティティのデジタル表現（コンピュータ上で処理可能な表現）をデジタルアイデンティティ（デジタルID）と呼んでいる。近年、ユーザー（個人・法人等）はデジタルIDを利用して様々なデータやデジタルサービスにアクセス可能になっている

各国・機関におけるデジタルアイデンティティの定義

国・機関	定義
米国	オンライン・トランザクションに従事する対象者の固有の表現（US, NIST SP 800-63 revision 3）[1]
カナダ	あるコンテキスト内でサブジェクトを一意に識別するデジタル表現の一種で、ユーザーがオンラインサービスにアクセスする際にサブジェクトを表現するために排他的に提示/使用するもの(DIACC, Pan-Canadian Trust Framework Glossary)[2]
ITU（国際電気通信連合）	デジタル・コンテキストの中で個人を識別できるほど詳細なエンティ ティのデジタル表現である。(ITU, X.1252 “Baseline identity Management terms and definitions”）[3]
英国	デジタルアイデンティティは、個人として、または組織の代理人として行動する人のデジタル表現である。（The UK digital identity and attributes trust framework）[4]

出所）
1 https://www.nist.gov/identity-access-management/nist-special-publication-800-63-digital-identity-guidelines
2 https://diacc.ca/trust-framework/
3 https://www.itu.int/rec/T-REC-X.1252-202104-I/en
4 https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version#what-are-digital-identities

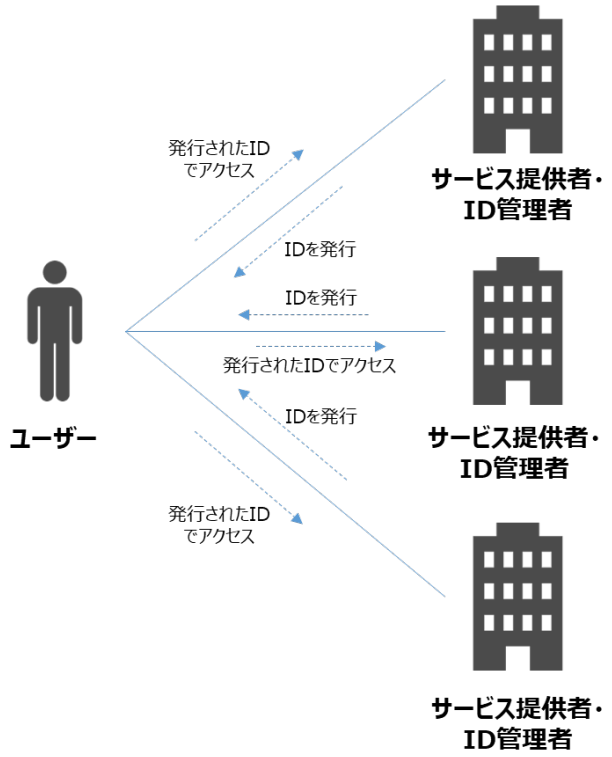
2.3 アイデンティティ管理モデル：現行の管理形態

現行のインターネット・webサービスにおいては、サービスを提供する企業等、ユーザー以外の主体がデジタルIDの発行・管理を担う、集中型や連邦型モデルの管理形態が一般的に採用されている

アイデンティティの管理形態

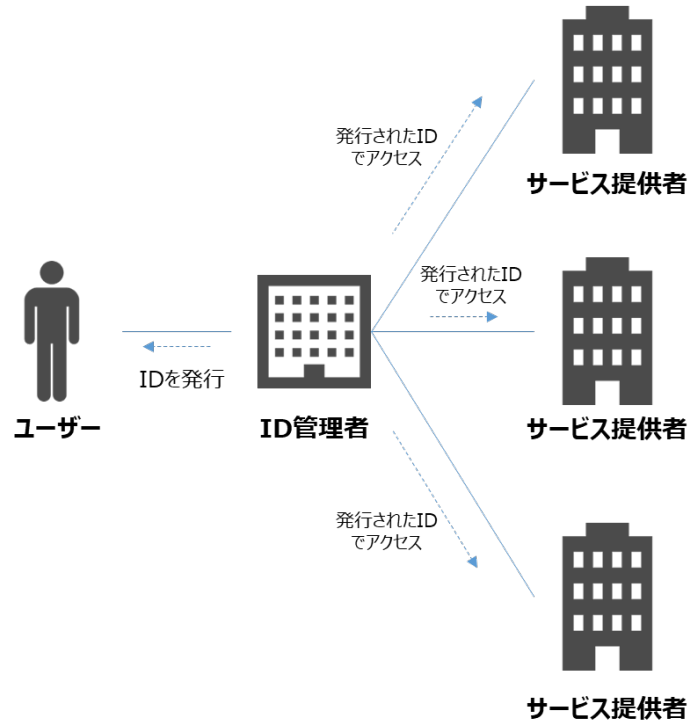
Centralizedモデル（集中型）

ユーザーのID情報は各サービス提供企業が個別に管理
ユーザーはサービスごとに発行されたIDで各サービスにアクセス



Federatedモデル（連邦型）

ユーザーのID情報はある特定の企業で管理
ユーザーは上記の企業から発行されたIDを使用して、連携している複数のサービスにアクセスできる



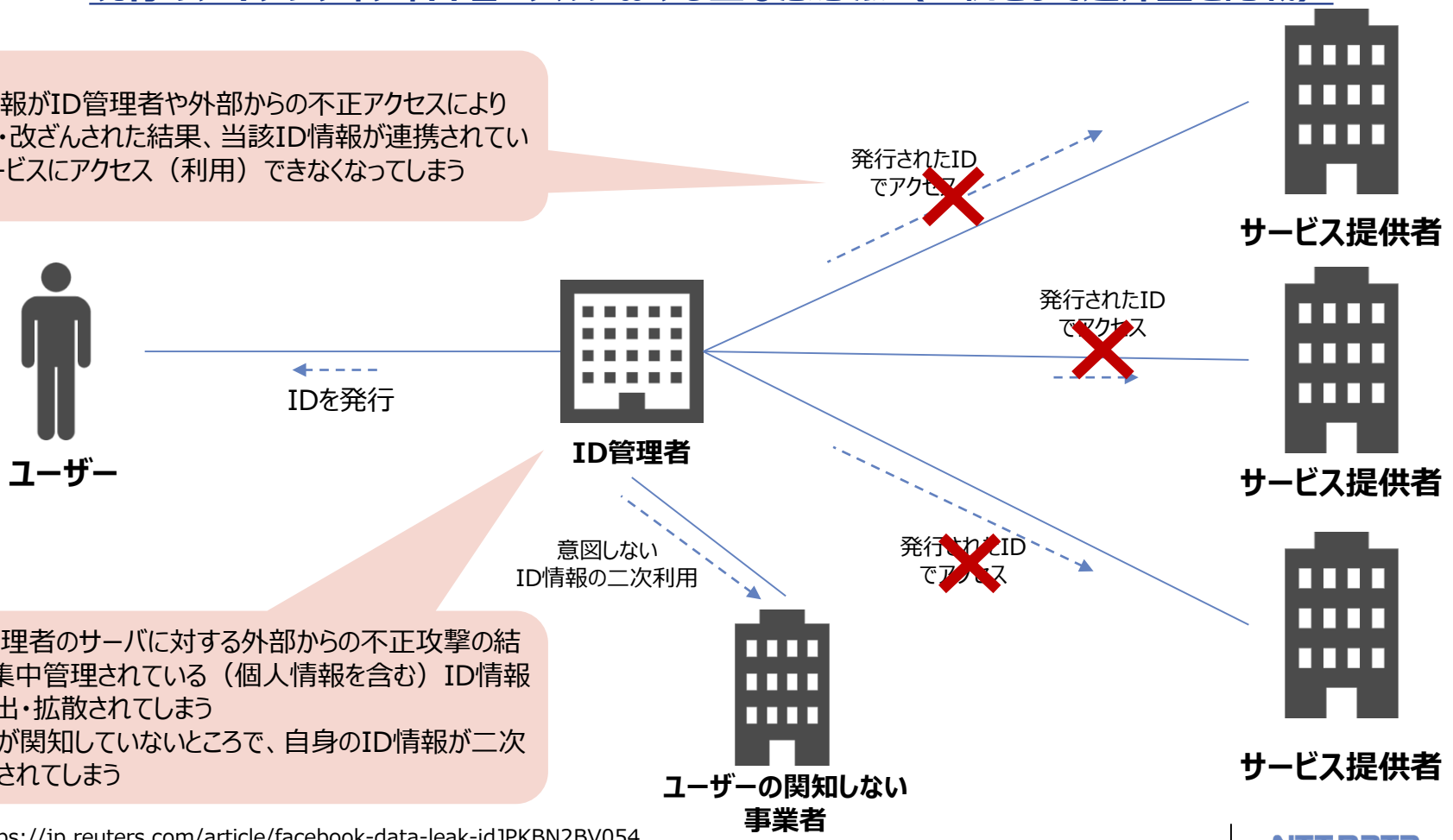
参考）http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

2.3 アイデンティティ管理モデル：現行のアイデンティティ管理モデルにおけるペインポイント

現状広く採用されている集権型及び連邦型アイデンティティ管理モデルにおいては、ユーザーのID情報をユーザー以外の主体（特に一部の巨大なIT企業）により集中管理されていることで、ユーザーの意図しないところでID情報が無効・改ざんされるリスクが懸念される。事実2021年の旧Facebook社（現Meta Platforms社）における個人情報漏洩などの事件[1]が発生しており 、効率的にID情報を管理できる反面リスクが顕在化している

現行のアイデンティティ管理モデルにおける主な懸念点（一例として連邦型を記載）

- ID情報がID管理者や外部からの不正アクセスにより無効・改ざんされた結果、当該ID情報が連携されているサービスにアクセス（利用）できなくなってしまう



- ID管理者のサーバに対する外部からの不正攻撃の結果、集中管理されている（個人情報を含む）ID情報が流出・拡散されてしまう
- 自分が関知していないところで、自身のID情報が二次利用されてしまう

出所）1 https://jp.reuters.com/article/facebook-data-leak-idJPKBN2BV054

2.4 トラストフレームワーク

アイデンティティ情報の管理や利活用においては、デジタルIDの発行主体等のステークホルダーの定義、その果たすべき役割、セキュリティ基準などについて、参照すべき法律・規則等が定められていることが多く、一般的に「トラストフレームワーク」の名称で諸外国において策定・公表されている

調査対象としている諸外国のトラストフレームワーク

国・地域		フレームワークの名称
欧州	EU	Electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC（eIDAS）
	イギリス	The UK digital identity and attributes trust framework
	ドイツ	IDunionネットワーク（Trust over IPスタック）
北米	米国	Identity Ecosystem framework
		NIST-SP800-63
	カナダ	Pan-Canadian Trust Framework
オセアニア	オーストラリア	Trusted Digital Identity Framework
		Trust ID Framework
	ニュージーランド	Digital Identity Trust Framework
		Identity Management Standard
アジア	シンガポール	NDI Stack
	インド	India Stack

2.5 自己主権型アイデンティティ／分散型アイデンティティ

集中型・連邦型のような現行のアイデンティティ管理形態におけるペインポイントを解決するモデルとして、自己主権型アイデンティティ（Self-Sovereign Identity: SSI）や分散型アイデンティティ（Decentralized Identity: DID）が参照されている。一部のレポートではSSI／DIDをそれぞれ「ユーザー自身のID情報管理を目指す考え方／特定のID情報管理者に依存しない仕組み」としているが、明確に定義されたSSI／DIDの使い分けが確認できなかったため、本調査では「特定の管理主体に依存することなく、既存のシステムに比して分散的にID情報が管理されている状態」を指す同一のものとしてSSI／DIDを扱う

SSI／DIDに関する諸機関での考え方

自己主権型アイデンティティ（SSI）	• ID情報の管理主体が介在することなく、ユーザー本人のID情報をユーザー自身がコントロールできることを目指した考え方。自己主権型IDのシステムではデジタルIDウォレット（自身のID情報を保管し、自身の判断に基づいて必要な相手に必要なID情報を提示することのできる製品・サービス）を用いて、自身のID情報の真正性を証明することができる（SovrinFoundation[1]）
分散型アイデンティティ（DID）	• ブロックチェーン等の分散台帳技術を活用してプライバシーを保護し、安全にデータ交換を行うシステムであり、自己主権型アイデンティティと同様の考え方（Microsoft[2]） • 自分自身でデジタルIDを自己制御できることを目指す思想であるSSIに対し、ユーザのデジタルIDが特定のID管理者に依存しないよう、その依存度を下げることを目的とする仕組み（野村総合研究所、レポート[3]） • 分散型アイデンティティによってプラットフォーム事業者に依存しない自由な競争環境とサービス連携を実現できる一方、不正対策や法執行に課題がある。信頼できる安全なDIDの利用環境を整備し、プライバシー保護や国境を越えた相互運用性の確保には多国間の連携が必要となる。個と個をつなぐことを目指す Web3.0 では、中央集権的な枠組みによらない ID の確立が必要である（デジタル庁、Web3.0 研究会レポート[4]）

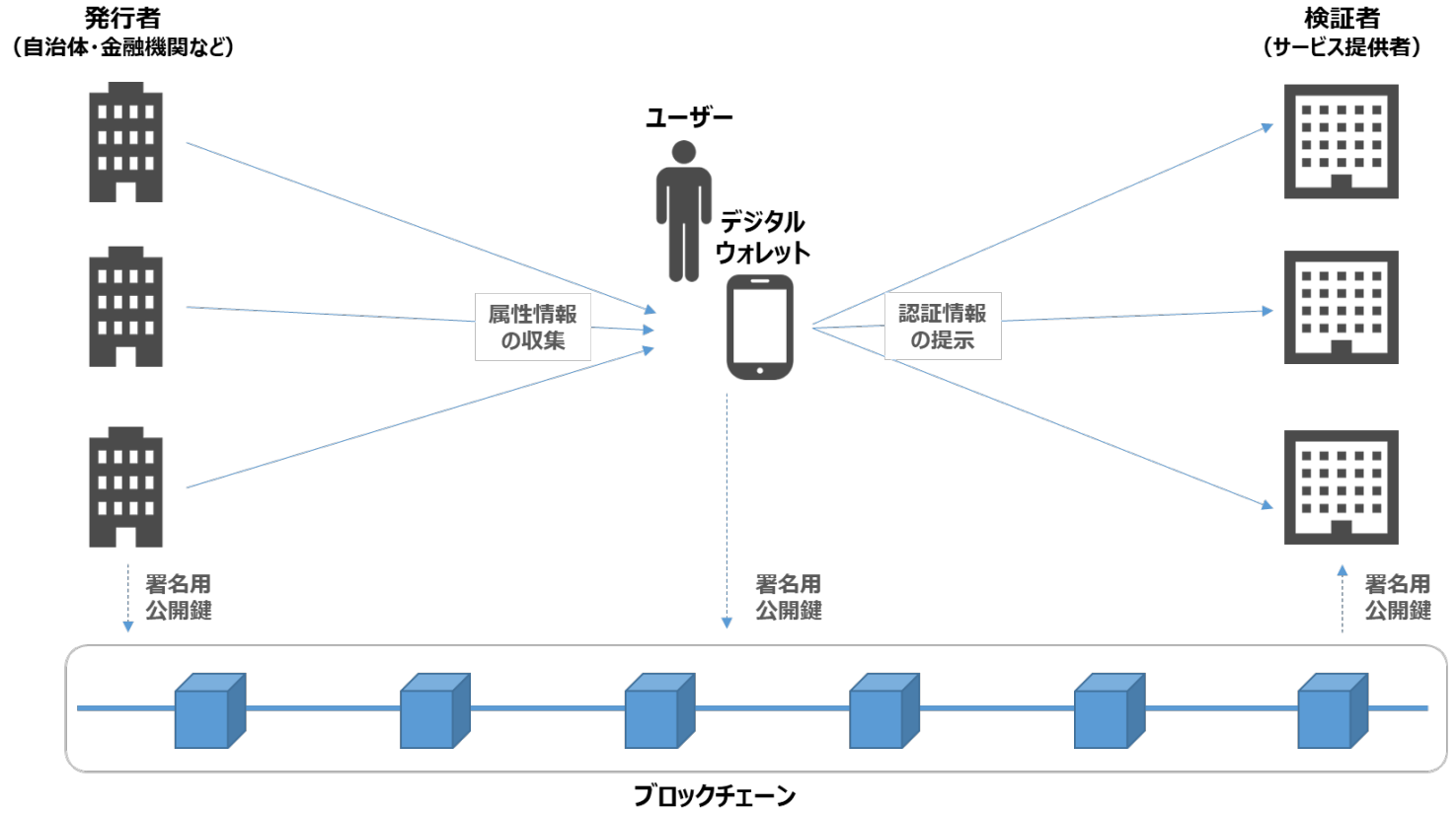
出所）1 https://sovrin.org/what-is-ssi/
2 https://www.microsoft.com/en-us/security/business/solutions/decentralized-identity
3 https://www.fsa.go.jp/policy/bgin/ResearchPaper_NRI_ja.pdf
4 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/a31d04f1-d74a-45cf-8a4d-5f76e0f1b6eb/a53d5e03/20221227_meeting_web3_report_00.pdf

2.5 自己主権型アイデンティティ／分散型アイデンティティ：SSI/DIDの実装スキーム

SSI/DIDとしては、デジタルウォレットで個人のID情報及び属性情報を保管し、ブロックチェーン等の分散台帳技術を活用した非改ざん性を担保して情報のやり取りを行う実装スキームが一般的に示されている

SSI／DIDの実装スキームイメージ

ID情報に含まれる属性情報（口座番号等）を信頼が担保された発行者から収集し、デジタルウォレットで自己管理
ユーザーの意思により必要な情報をサービス提供者に提示して認証を受ける
ブロックチェーンにより各やり取りにおけるデータ改ざんを防止



Microsoft（https://www.microsoft.com/en-us/security/business/solutions/decentralized-identity）を参考にNTTデータ経営研究所にて作成

2.5 自己主権型アイデンティティ／分散型アイデンティティ：SSI/DIDの実装スキーム

本報告書で主に用いる「ウォレット」については、EU等で推進されているデジタルIDウォレットと同義であり、ユーザーがID情報を自分自身で管理（保管・提示）することが可能なアプリケーション・サービスのことを指す
現在流通しているYahoo!ウォレットやApple社のウォレットなどの電子決済管理アプリケーションとは一部機能は重複するものの主用途が異なり、また保管されている情報をコントロールしている主体が自分自身か特定のID管理事業者かという点でも違いがある

電子決済管理ウォレット（例：Yahoo!ウォレット）

クレジットカードや銀行口座情報を登録し、各種サービスの支払い及び代金の受け取りを行うことができる

Yahoo!ウォレットで利用可能なサービス例

デジタルIDウォレット（例：EUDIW）

ユーザーの自身のウォレットに保管されたID情報を銀行に対し提示し口座開設等の申請プロセスを行うことができる

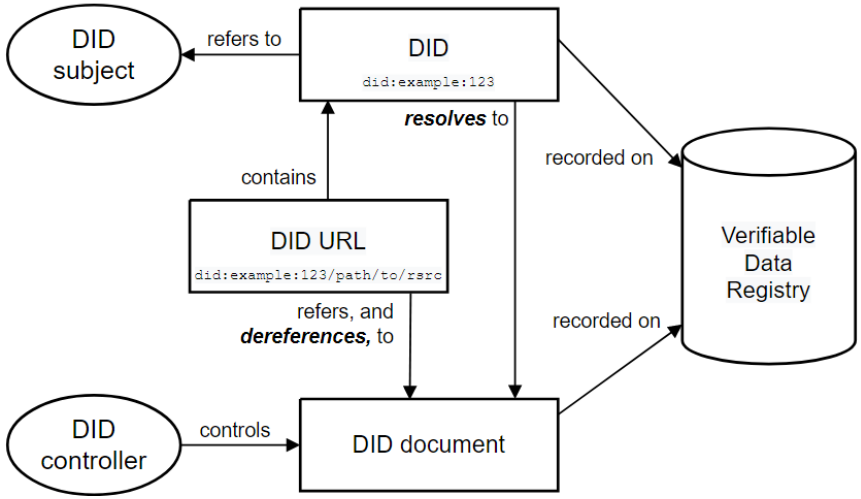
出所）1 https://wallet.yahoo.co.jp/guide/about/index.html
2 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

2.5 自己主権型アイデンティティ／分散型アイデンティティ：SSI/DIDの実装手段・参照規格

SSI/DIDの実装手段・規格としては、国際標準化機関であるW3CのDecentralized Identifiers（DIDs：分散型識別子）v1.0とVerifiable Credentials（VCs：検証可能な資格情報） v1.1が参照されている

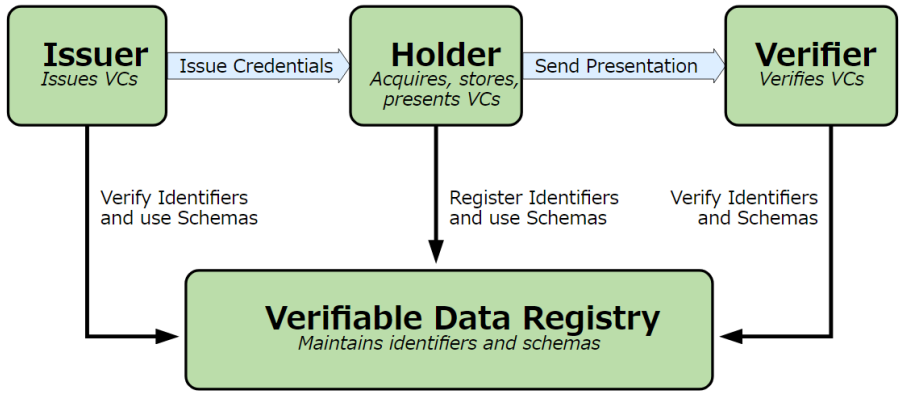
Decentralized Identifiers（DIDs）[1]

- サブジェクト（人、組織、モノ等）自身が特定のレジストリやIDプロバイダーから分離されたグローバルに一意な識別子（DID）を発行・活用するための仕様を規定する国際標準であり、DIDの形式やそのメタデータを記録したDID Document、及びそれらが登録される検証可能なデータレジストリ、DID Documentの検索・取得を行うDID Resolverといった要素から構成される



Verifiable Credentials（VCs）[2]

- 運転免許証などの資格情報について、インターネット・Web上でその内容を検証することができる資格情報を発行・提示・検証するための仕様を規定する国際標準であり、ある資格情報を発行するIssuerと、それを受け取るエンティティであるHolder、資格情報の提示を受けるVerifierが、検証可能なデータレジストリを介して発行・提示・検証を行うデータモデルとなっている



出所)
1 https://www.w3.org/TR/did-core/
2 https://www.w3.org/TR/vc-data-model/

3.詳細調査結果：

3.1 共通識別番号・デジタルIDに関する政策動向

3.2 トラストフレームワークの策定状況

3.3 自己主権型／分散型アイデンティティに関する取り組み・ユースケース

3.1 詳細調査結果：共通識別番号・デジタルIDに関する政策動向

3.1.1 欧州（EU、ドイツ、イギリス）における調査結果

現在に至るまでの変遷（共通識別番号）

EUにおいては欧州全体としての統一的な識別番号は存在せず、加盟国に依っている現状である

EU加盟国における共通識別番号の例

国	共通識別番号
エストニア	2000年に制定された国民登録法に基づき、11桁の数字である国民番号が内務省の所管で付番されている[1]
オーストリア	2004年に制定された電子政府によって、国民の共通識別番号が規定されており、出生時に付番される国民登録番号であるZMR-Zahl、それを暗号化したSource PIN、アプリケーションで割り当てられるssPINによって各セクターでの識別がなされている[2,3]
フィンランド	1960年代に個人識別コード（HETU）が導入されており、フィンランド国内外で出生したフィンランド国民に対して発行されている[4]
スウェーデン	1947年に導入された個人識別番号（PIN）が国税庁から国民に対して発行されている[2]

出所）
1 https://www.soumu.go.jp/main_content/000731090.pdf
2 https://www.cas.go.jp/jp/seisaku/npu/policy03/pdf/20100629/20100629_syakaihosyou_haihu_4.pdf
3 https://xtech.nikkei.com/it/article/COLUMN/20080125/292090/
4 https://dvv.fi/henkilotunnus

現在に至るまでの変遷（デジタルID制度）

EUにおいては単一の欧州規模のデジタルIDが採用されることはなかったが、2014年にeIDASの制定以降、EU加盟国間でオンラインサービスにおいて利用できるデジタルID（eID）の導入が加盟国ごと任意で進められた他方、eIDの提供が任意でかつその普及が十分でなかったことから、2021年のeIDAS改正提案（eIDAS2.0）において、デジタルウォレット（EUDIW）の提供を加盟国に義務付け、eIDを含めた属性証明書・公的文書をモバイルデバイスで利用可能とした

eSignature Directive
EU域内の電子契約において、適格な電子署名の有効性を、物理的な書面の署名と同等の法的効力と認める指令（directive）。2014年のeIDASの成立によって廃止された

1999

2014

eIDAS 1.0[1]
eSignatire Directiveの内容を推し進め、EUにおける電子商取引の統一した基準を制定するもの。加盟国間で利用できる電子本人認証であるeIDと、電子署名・eタイムスタンプといった電子サービスであるトラストサービス等について規定している

2021

eIDAS 2.0（改正提案）[2,3]
eIDAS 1.0のフレームワークを改善する改正提案。EUDIWの提供を加盟国に義務付け、eIDを含めたID、属性証明、公的文書の格納・利用を可能にするとともに、新たなトラストサービスへの対応、技術に関する下位規則の整備義務化などを提案している

出所）
1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
2 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281
3 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0290

eIDASの概要

元々制定されていた「電子署名指令（1999/93/EC）」から内容を推し進め、EUの電子商取引に統一した基準を設けるために制定され、2016年7月に適用開始された
主に電子本人認証である「eID」と、電子署名・eタイムスタンプといった電子サービスである「トラストサービス」の要件、法的効力、セキュリティ等について規定しており、トラストサービス事業者（TSP）は、監督機関から評価を受けることによって、加盟国間で同等の法的効力を得る適格トラストサービス事業者（QTSP）に認定されトラステッドリストに載せられることとなっている[1]

eIDASの章構成	概　要		
1．総則			
2．電子本人確認（eID）	eID		・オンラインで本人確認を実施する ・加盟国間で相互に通知・承認し使用する
3．トラストサービス	トラストサービス	電子署名	・書類等の電子データに署名として用いられ、手書き署名と同等の効力を保証する
4．電子文書		eシール	・電子データの発行元・完全性を保証する
5．権限移譲・実施規則		eタイムスタンプ	・ある時間に特定のデータが存在していたことを保証する
6．末則		電子登録配送サービス	・第三者間での確実なデータ送受信、送受信日時・送受信者の識別等を保証する
		ウェブサイト認証	・ウェブサイトの信頼性・正当性を保証する

出所）
1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

eIDASの改正提案

改正の背景・課題

■ **見直しの結果明らかになった課題を背景に、2021年6月に欧州委員会へeIDAS 2.0が立法提案された[1]**

- EU加盟国の中で通知され、承認されたeIDスキームは19事例のみであり、eIDのEU市民への普及率は59%に留まっていた（稼働していないeIDASノードが存在する、eIDASネットワークに接続している公共サービスの数が限られていたなど）
- eIDASでは、技術的中立性を保つために下位規則で技術要件を十分に示すことができておらず、トラストサービス事業者の間で解釈に相違が発生し、エラーが生じていた
- 既存のeIDAS 1.0では、教育・銀行・航空など様々な分野のニーズ（セクター・ドメインごとに要求される属性情報）やブロックチェーンなど新たな技術に対応できていなかった

改正提案の概要

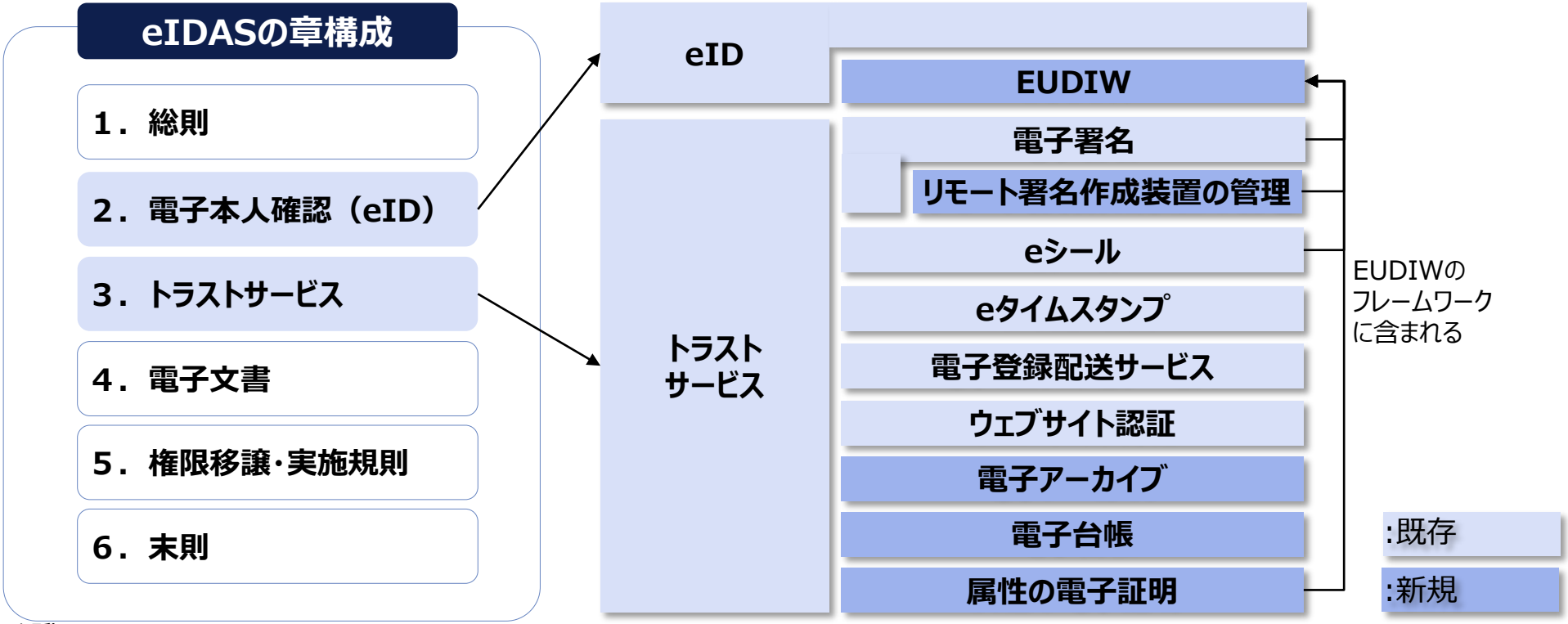
主な改正内容	概要
EUDIWの枠組み設定	• 全EU市民が利用可能な、新たなeIDの枠組みを整備し、発行を義務付ける • EU加盟国間での個人識別、属性情報の電子証明等が可能となる
トラストサービスの拡充	• 既存のトラストサービスに加え、電子アーカイブ、電子台帳（ブロックチェーン）、属性情報の証明などのトラストサービスを追加して定義、規定する
下位規則の整備	• eIDASに適用される技術の基準を規定する、下位規則の整備を義務付ける 例：EUDIWの認証基準、身元と属性の検証に関する基準、適格証明書の基準、属性証明とその確認の基準等
ブラウザ対応	• ブラウザは、EUの認定Web認証用証明書（QWAC）の認識を義務付ける（信頼性を向上）

出所）
1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281

eIDAS改正の影響

- 既存のトラストサービスの一部である電子署名、eシール及び新たに追加された属性情報の電子証明などはEUDIWの機能としてフレームワークに含まれることとなり、EUDIWは電子アーカイブや電子台帳といった新たなトラストサービスの導入と併せて、物理的な文書を必要としないデジタル証明手段をEU市民に提供するとされている[1]
- 技術に関する下位規則の整備の義務化は、トラストサービス事業者の間での認識統一が容易になり、技術的エラーの減少に寄与するものと思われる

eIDAS改正による、eID・トラストサービスへの新規追加項目



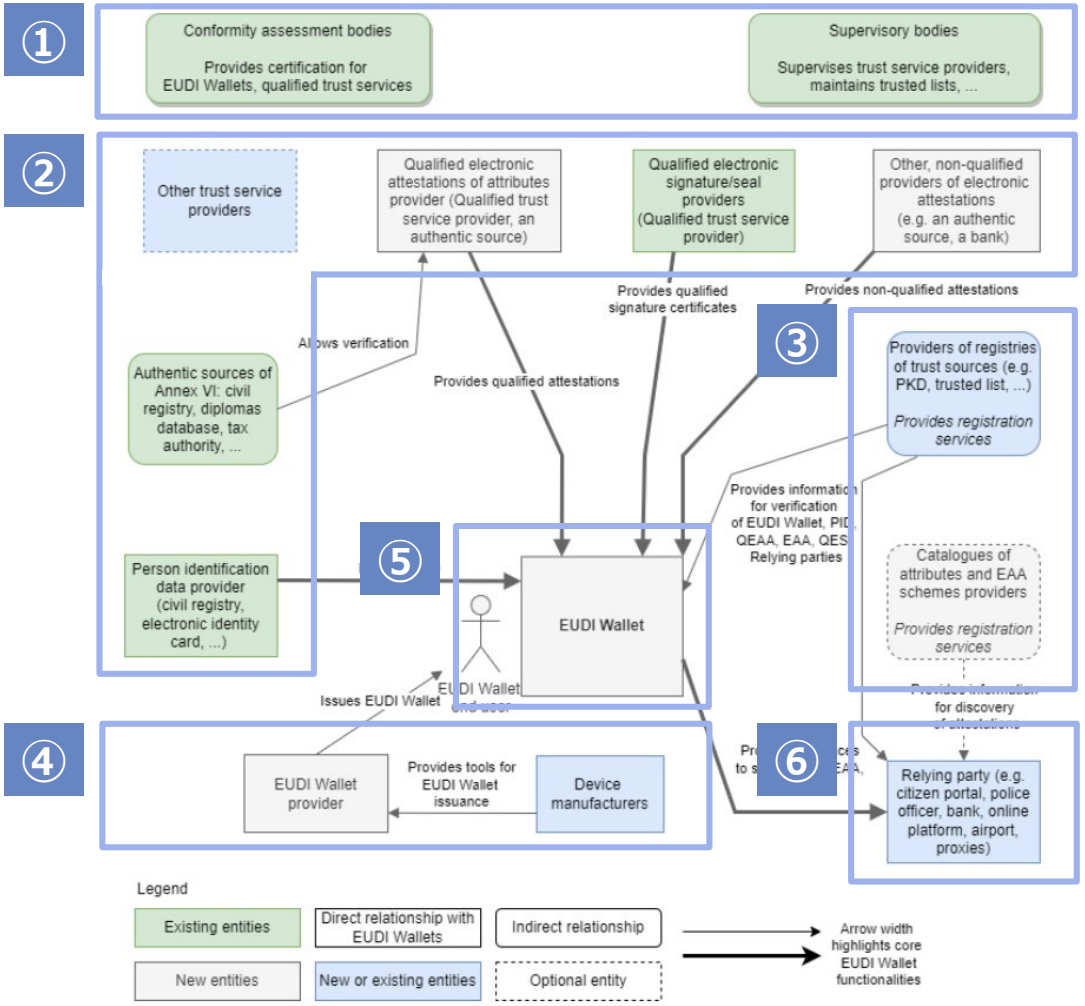
出所）
1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0290

EU
ドイツ
イギリス

EUDIWのエコシステム

eIDASの専門家グループは、EUDIWの概念に関する理解を促進するため「EUデジタルIDアーキテクチャとリファレンスフレームワーク」[1]を公開しており、その中で説明されているEUDIWのエコシステムではエンドユーザーが中心に据えられIDや資格情報をコントロールする構造がうかがえる

EUDIWのエコシステム



① EUDIWやトラストサービス事業者、トラステッドリストの適合性評価を行い、その管理監督を行う機関

② エンドユーザーのEUDIWに格納する各種情報（個人ID、属性情報の証明書）や、電子署名機能を提供する、トラストサービス事業者等の活動

③ EUDIWと、それを提示される当事者（Relying Party）の双方に検証のための情報提供が行われる
Walletの発行者やトラストサービス事業者がその役割を担う予定

④ EUDIWの発行と、必要なツールの製造
EUDIWは国もしくは国の指定した機関によって発行するとされる

⑤ EUDIWとそのエンドユーザー

⑥ EUDIWを提示される当事者（Relying Party）

出所）
1 https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline

eID（1）

eIDは2014年に成立したeIDAS1.0によって規定される、EU加盟国間で公共オンラインサービスへのアクセス時に本人確認を行うことのできるデジタルIDであり、加盟国はeIDASのネットワークに接続する国内のeIDスキームを指定し、それを他の加盟国へ通知することでピアレビューを受け、相互に承認されたならば利用可能となる[1,2]

eIDの通知・承認

- 通知には、当該加盟国（もしくは委任を受けた国）の公共機関が提供するeIDスキームであり、かつ一つ以上のオンラインサービスに既に利用できること、eIDASの下位規則に定める保証レベル（LoA）を満たしていることなどが必要となる
- 当該加盟国の通知するeIDスキームが、他の加盟国において承認されるには、当該eIDスキームの保証レベルが、他の加盟国で対象となるオンラインサービスと同等、もしくはそれ以上の保証レベルを満たすことが必要となる
- eIDASスキームにおける本人確認プロセスの保証レベルは、下位規則CIR (EU) 2015／1502によって規定されており、登録、本人確認のプロセスにおいて満たすべき要件を規定し、レベルをLowからHighまでの3段階に区分している

CIR (EU) 2015／1502に規定される保証レベルの一例

Low	Substantial	High
Webページでの自己申告登録によって実行され、本人確認が行われることが無い	Lowに加え、 • 国の認可したID文書によって登録内容の真正性を確認する • 少なくとも2つ以上の要素の認証手段を使用する	Substantialに加え、国の認める写真、もしくは生体認証IDを使用する

出所）
1 https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+Levels+of+Assurance
2 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002

eID（2）

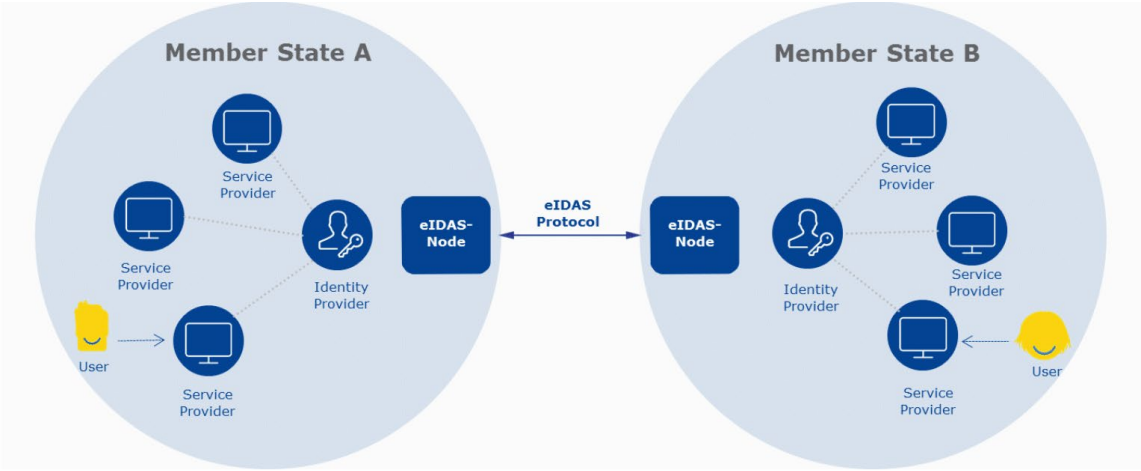
EU
ドイツ
イギリス

eIDの利用に伴う加盟国間の通信を行うために、各国はeIDASノードを実装する必要がある
eIDASノードは下位規則CIR (EU) 2015／1501においてその要件が規定されているが、具体的に使用する技術等は指定されてはおらず、実装の参考となるサンプルソフトウェアが欧州委員会から提供されている[1,2]

eIDASノードの実装

- 加盟国は、eIDスキームの通知と利用を行うにあたり、加盟国間で相互接続されるeIDASノードを実装する必要がある。eIDASノードは、ある加盟国のeIDスキームと、別の加盟国との間で通信を行うためのコネクター等からなるソフトウェアコンポーネントであり、各国は実装者（公的機関）を指名する必要がある
- 各国のeIDASノードの実装者は、eIDスキームを提供するアイデンティティプロバイダと、eIDによって本人確認を行うサービスプロバイダ等がeIDASネットワークに接続するための支援を行うこととなっている

eIDASノードを通じた加盟国間のeID利用



1 加盟国Aの市民が加盟国Bのオンラインサービスを利用する際、本人認証を要求される

2 加盟国Aの市民はAのeIDを持っているため、認証要求は、加盟国AのIDプロバイダー(IdP)に、eIDASノードを介して送信される

3 認証結果は加盟国Bのオンラインサービスプロバイダに返され、認証が完了し、市民はサービスへのアクセスを続行できる

出所）
1 https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?pageId=467109829
2 https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?pageId=467109866

eID（3）

eIDASの成立以来、2021年6月時点で14カ国から19のeIDスキームが通知されており、EU住民の約60%をカバーしている。しかしeIDの通知は加盟国の義務ではなかったことから加盟国間のeID利用状況に差異が生じ、また民間サービスやモバイルでの利用をeIDASで規定していなかったため、使用が煩雑でビジネスケースが限られたとの評価を受け、eIDAS改正提案の理由の一つとなった[1,2]

欧州委員会の公表している通知されたeIDスキームの例

Overview of pre-notified and notified eID schemes

Please find below information about the pre-notified and notified eID schemes under eIDAS:

タイトル	Member State	Title of the scheme	eID means under the scheme	Level of assurance	Status	Date	OJEU
Czech Republic	Czech Republic	National identification scheme of the Czech Republic	CZ eID card	High	NOTIFIED	13 Sep 2019	2019/C 309/09
Estonia	Republic of Estonia	Estonian eID scheme: ID card Estonian eID scheme: RP card Estonian eID scheme: Digi-ID Estonian eID scheme: e-Residency Digi-ID Estonian eID scheme: Mobiil-ID Estonian eID scheme: diplomatic identity card	— ID card — RP card — Digi-ID — e-Residency Digi-ID — Mobiil-ID — Diplomatic identity card	High	NOTIFIED	07 Nov 2018	2018/C 401/08
France	French Republic	French eID scheme "FranceConnect+ / The Digital Identity La Poste"		Substantial	NOTIFIED	02 Feb 2021	2021/C 522/03
Italy - eID	Republic of Italy	Italian eID based on National ID card (CIE)	Italian eID card (Carta di Identità elettronica)	High	NOTIFIED	13 Sep 2019	2019/C 309/09
The Netherlands (DigiD)	The Kingdom of the Netherlands	DigiD	DigiD Substantieel DigiD Hoog	Substantial, High	NOTIFIED	21 Aug 2020	2020/C 276/02
Sweden	The Kingdom of Sweden	Swedish eID (Svensk elegitimation)	BankID Freja eID (Notified) EFOS	Substantial and High	NOTIFIED	14 Dec 2020	2022/C 78 I/02

出所）
1 https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_2664
2 https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

現在に至るまでの変遷

ドイツではプライバシー侵害の懸念等の理由から国民共通番号の導入に至っておらず、行政分野ごとに異なる個人識別番号（租税識別番号や医療被保険者番号など）を用いて行政手続きを行っている
2021年4月に公布された登録現代化法に基づき、一定の制約の元で租税識別番号を行政分野横断で活用できる仕組みの整備が進められている

連邦住民登録法案（1970年代）
行政事務の効率化を目的として、行政分野で個人を識別する番号の導入（連邦住民登録法案）が検討されたが、プライバシー侵害の懸念により成立に至らなかった。

1970年代

1983

国勢調査の自紙にあたり、汎用的な個人を識別する番号を利用することは連邦憲法に違反する可能性を示唆するドイツ連邦裁判所の判決が下る。以降、複数の行政間で個人を識別する可能性がある共通的な番号の導入は違憲であるとの見解もあり、共通番号そのものの検討もされてこなかった。

2021

RegMog：登録現代化法（2021年4月～）
連邦政府・州・地方自治体における行政サービスをオンラインで提供するためのポータルサイト（連邦ポータル）の整備が進められている。

行政分野ごとに異なる個人識別番号が導入され、2022年時点においても、適用されている。
- IdNO：税務識別番号（2003年）
- KVNR：医療保険者番号（2003年）
- 年金保険番号
- 介護保険番号　等

登録現代化法

2021年4月に公布されたドイツの法律であり、オンラインアクセス法の改正及びID番号法の制定について規定している。2017年に制定されたオンラインアクセス法により、連邦政府と州は2022年末までに行政ポータルサイトを介した行政サービスの電子的提供が義務付けられていた

改正オンラインアクセス法

- 既存の税務識別番号を活用して、**法的根拠又は本人の同意がある場合に公的機関間でのデータ交換を可能**とするとともに、データ保護の観点から**データコックピットを導入すること**等が規定されている。
  - データコックピットとは、**本人**が、自身のデータについて**どの機関がどのデータ要素をどのような目的で処理したかをインターネットで確認できるもの**であり、日本においてはマイナンバーと紐づけられた特定個人情報の提供状況を確認することのできる情報提供等記録開示システムに相当するものと考えられる。
- 税務識別番号を利用する理由としては、既に共通識別番号として広く普及していること、ランダムな識別番号であり番号自体には個人に関する情報が含まれていないこと、及び他人に簡単に知られるものではないことが挙げられている。またオンラインアクセス法では、連邦政府、州政府、地方自治体は、575の管理サービスをオンラインで提供することが規定されている。

ID番号法

- ID番号法においては、行政手続上のデータを特定の自然人へ明確に割当てること、データの質の向上を実現すること、公的機関保有データの再提出を削減することを目的として制定されている。
- 主な規定
  - 人口登録簿、外国人登録簿、運転免許証登録簿等の総数 51 の登録簿へ税務識別番号を追加する旨
  - 各種登録簿の把握・各機関への税務識別番号等の送信（各機関とのデータのやり取りにおける仲介役を担う）・プロジェクト管理等を行う機関として登録現代化官庁を設置する旨
  - 連邦中央税務局が保存する個人データとして税務識別番号、姓、旧姓、名、生年月日、出生地、性別、及び国籍等を基本データとして規定する旨
  - 2 年ごとに連邦データ保護・情報自由受託官による登録現代化官庁への監査を実施する旨
  - 3 年ごとに連邦内務建設国土省による登録現代化官庁のデータ処理に関する評価及び連邦議会への報告を行う旨
  - ID番号法施行後 5 年目に専門家の関与の下での評価及び連邦議会への報告・提言する旨　等

現在に至るまでの変遷

ドイツではデジタル認証手段としてeIDカードが2010年から導入されており、16歳以上のドイツ国民に対して取得が義務付けられている。共通識別番号とは関連が見られないことから、共通識別制度とデジタルIDは別個の取り組みとして推進されていると想定される
2017年の連邦法改正により、eIDカードの発行時に電子署名機能を付与することが可能となり、登録現代化法によって整備されている行政サービスオンラインポータルサイトにおいても、eIDカードを用いた本人認証機能を使用することができるとされている[1]

eIDカードの導入（2010年～）
署名法（1997年）によって行政手続きにおける電子署名による申請を推進しようとしたものの使用の難しさから普及せず、新たな電子的本人証明手段として導入された[2]
共通識別番号の記載はされていない

連邦法改正（2017年）
eIDカードの発行時に電子署名機能を付与することが可能となる。

2010年 2017

～2017年
電子的な個人認証（利用者証明用電子証明書）の機能を含む電子署名機能の利用にあたって、eIDカードの取得とは別に、電子署名機能のアクティブ化の手続が必要とされていた。

出所）1 https://dl.ndl.go.jp/view/download/digidepo_12295665_po_02920002.pdf?contentNo=1
2 https://dl.ndl.go.jp/view/download/digidepo_8747938_po_02610004.pdf?contentNo=1

eIDを用いた個人認証の推進

ドイツでは電子政府に向けた取組やeIDAS等の欧州指令に基づき、2010年以降、eIDを用いた行政・民間サービスにおける個人認証を推進している[1]

eIDカード

- 認証の際、eID カードと6 桁の PINの2 つの認証要素を使用する
- eID カードのチップには、保持者の個人データが保有されており、このデータの保護に係るセキュリティアンカーと保持者の認証の役割を果たす
- 関連するキーが保存されており、それを用いて認証を行う。また、PINの入力を行うことで、利用者の同意を表す役割も果たす

保有されているデータ
• 苗字 • 出生名（任意） • 名前 • 博士号 (任意), • 誕生日 • 出生地 • 住所 • 有効期限 等

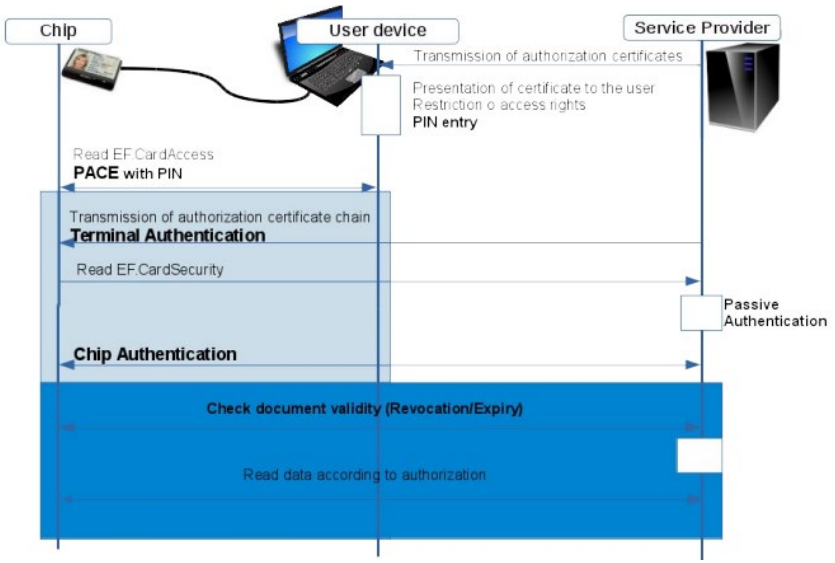
出所）
1 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_Whitepaper.pdf?__blob=publicationFile&v=1
German eID based on Extended Access Control v2 Overview of the German eID system version1.0（20 February 2017）

eIDを用いた個人認証の仕組み

個人認証にあたり、eIDASに準拠する形で認証の仕組みを構築している
利用者は、カードリーダー等にeIDカードをかざし、PINを入力することで個人認証を行い、サービスプロバイダーはeIDサーバーと連携し、eIDの登録情報と照合を行う[1]

認証の仕組み

- 個人認証に当たっては、ドイツ連邦情報セキュリティ局（BSI、連邦内務省の下級機関）等をトラストアンカーとする承認PKIに基づき発行される認証証明書と、カードに格納されている証明書を突合してeIDの有効性・公証性の確認を行っている



eIDカードを使った個人認証を行う際は、eIDカードと、読取り媒体としてのスマートフォン又はカードリーダー、専用のアプリ・ソフトウェアのAusweisApp2が必要となる

- 証明書の検証が行われた後、ICカードに格納された所有者の情報のアクセスが承認されるが、この承認も一定期間のみ有効であり、かつeIDカードの所有者はサービスプロバイダーが読み取ることができる情報を、より少なく制限することも可能となっている（例えば18歳以上のみが閲覧できるインターネットサイトであるならば、年齢情報のみを要求することができる）
- また、サービスプロバイダー側がeIDカードに格納された情報を読み取る際には、データは全て暗号化されて送信される

出所）
1 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_Whitepaper.pdf?__blob=publicationFile&v=1
German eID based on Extended Access Control v2 Overview of the German eID system version1.0（20 February 2017）

現在に至るまでの変遷

イギリスにおいては1939年に身分証明書として利用できるIDカード（国民識別番号）が導入されたが、提示を強制された事に対する反対運動から1953年に廃止された。その後2003年のIdentity Card Actで統一的なIDカード（国民識別番号）の導入を再検討したもののプライバシーへの懸念等から廃止され、NINO、NHS Number等行政分野毎に異なる識別番号を利用する状態が継続している

National Resistration Act (国民登録法)[1]
第2次世界大戦の緊急措置として、国家登録簿に基づき身分証明書として利用できるIDカードが発行されたが、警察への身分証の提示を拒否した人物が起訴された事件を契機として、反対運動が起き1953年に廃止された

Identity Card Act [2]
イギリスに在住する16歳以上の個人について、生体認証を含む個人情報を国民ID登録簿（NIR）に登録し、個人にID登録番号を付与するとともに、これに基づくIDカードを発行することを規定した法律
2010年、保守党・自由民主党の連立政権によって身分証明書法が可決されことでIDカードは廃止された

1939 1948 1996 2003

NINO(国民保険番号) [3]
国民保険及び社会保障制度において国民を識別するために使用される番号
一部税制においても参照番号として利用されている

NHS Number（国民医療制度番号） [4]
医療サービスにおいて、登録ユーザーに割り当てられる固有の番号であり、英国の国営医療制度であるNHSにおいて患者の医療記録の管理に用いられる。1996年に一般に導入された

出所）1 https://www.familyhistory.co.uk/national-registration-1915-1939/
2 https://researchbriefings.files.parliament.uk/documents/LLN-2016-0002/LLN-2016-0002.pdf
3 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/530003/snap-s1-intro.pdf
4 https://www.closer.ac.uk/wp-content/uploads/CLOSER-NHS-ID-Resource-Report-Apr2018.pdf

参考）経済安全保障法制に関する有識者会議 内閣官房 経済安全保障法制準備室 説明資料

主な共通識別番号の概要

イギリスにおいては国民保険制度、公衆衛生・医療といった目的別に、主にNINOとNHS Numberが識別番号として用いられている

現在利用されている共通番号制度

NINO（国民保険番号）[1]

- 2文字の接頭辞（アルファベット）と6の数字、1文字の接頭辞で構成される個人固有の識別子であり、1948年に制定された国民保険制度とともに運用が開始された
- 国民保険料の記録、社会保障給付、税額控除などにおいて利用され、主に歳入関税庁、雇用先、労働年金省、普通預金口座のプロバイダーなどに対して提供される

NHS Number[2]

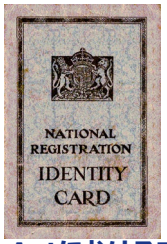
- イギリスの国営医療サービスであるNHSにおいて利用される、10桁の数字からなる識別番号であり、NHSのデータベース等において患者の識別、診療記録の管理に用いられる

過去利用されていた共通番号[3]

National ID Card

- 1939年に制定された国民登録法に基づき、全ての国民に登録を義務付けた国民登録簿が作成され、IDカードが発行された
- 第二次世界大戦の間の安全対策、及び戦後の食糧配給等に用いられていたが、1951年に警察へのIDカード提示を拒否した男性が起訴された事件を契機として制度への批判が高まり、1952年に国民登録法の廃止に伴い利用されなくなった

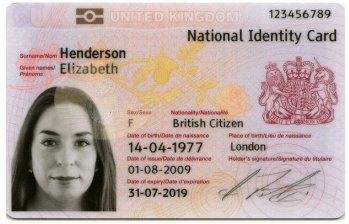
発行されたNational ID Card



Identity Card Act

- 米国の911同時多発テロ事件を契機としたIDカードの重要性の高まりを受けて、2004年にIDカード法（Identity Card Act）提案され、2006年に成立した
- 生体情報を含む国民ID登録簿を構築し、それに基づいたIDカードを発行することが規定され、2009年に先行的に発行が開始されたが、費用対効果や国民のプライバシーを侵害する可能性などが問題視され、2010年の政権交代とともに廃止された

Identity Card ActにおけるIDカード



出所）
1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/530003/snap-s1-intro.pdf
2 https://www.closer.ac.uk/wp-content/uploads/CLOSER-NHS-ID-Resource-Report-Apr2018.pdf
3 https://researchbriefings.files.parliament.uk/documents/LLN-2016-0002/LLN-2016-0002.pdf

現在に至るまでの変遷

イギリスにおいてはデジタル個人認証手段は長らく整備されてこなかったが、2016年のGOV.UK Verifyによる個人認証手段が整備された。しかし利用可能なサービスが制限されていること、認証手続きが煩雑であることなどからIDプロバイダーの離脱が相次ぎ、GOV.UK Verifyは2023年に廃止予定であり代替手段としてThe UK digital identity and attributes trust frameworkに基づいたデジタルID認証手段が整備されつつある

GOV.UK Verify[1]
銀行や郵便局、スーパーマーケットなどの民間企業が発行するIDを公共サービスにアクセスする際の本人認証手段として活用する仕組みとして2016年5月に本格運用を開始した
しかし利用可能なサービスが制限されていること、認証手続きが煩雑でコストが増加する等の課題が顕在化し、IDプロバイダーの離脱が相次いでいる

2016

2021

The UK digital identity and attributes trust framework[2]
様々なアプリケーションでのデジタルIDの作成と使用を促進するために設計された、相互運用可能なトラストフレームワーク
デジタル ID 、属性情報が、任意のエンティティによって信頼されることを保証する

出所）
1 https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify
2 https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework

Gov.UK Verify

概要

- 政府の認定を受けたIDプロバイダ（IDP）が発行するIDを活用して公共サービスへアクセスする際の、本人認証の仕組み
- 利用者は複数のIDPの中から自分が利用する事業者を選択・登録を行う
- GDS（英国政府デジタルサービス）が主導していたが、現在所管はDCMS（The Department for Digital, Culture, Media & Sport）に移っている
- ユーザーエクスペリエンスが不十分であることや、関係省庁が必ずしも協力的ではないこと、民間サービスプロバイダが求める要件水準を満たさないなどの理由から当初の想定ほど普及は進んでいない状況である

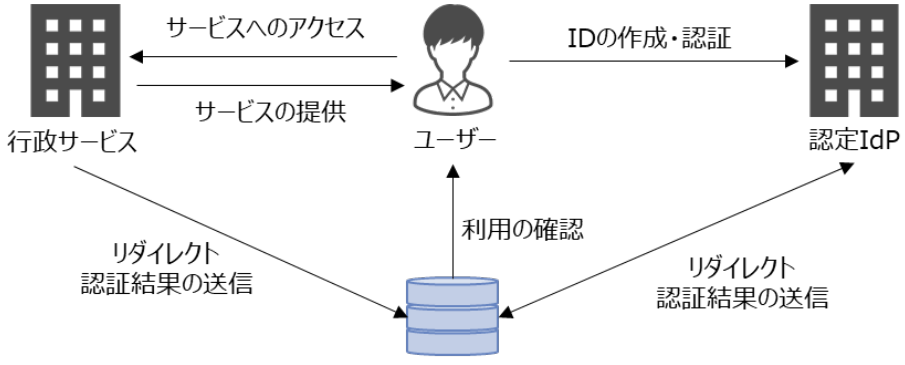
IDPの変遷

- 最初の入札でPost Office Ltd, Verizon、Experian、Digidentity、Mydex CICの5社が認定企業された後、Barclays,GB Group,Morpho,Royal Mailが加わった
- その後認定企業が英国政府との契約を更新せず、現在のIDプロバイダーはDigidentityとPost Office Ltdのみとなっている

提供サービス

- 2020年時点では約20種類のサービスが利用可能であったが、現在の提供サービスは以下の7種類に留まっている
  ①Rural Paymentsの利用　②運転免許証情報を記載した通行証をスマートフォンに追加　③自動車運転免許の申請④DBSベーシックチェック（犯罪歴）の申し込み　⑤住宅ローン証書へのサイン　⑥Total Rewards Statementにサインインする　⑦イングランドで登録ソーシャルワーカーになるための本人確認申請
- 現在は新規のアカウント作成は停止しており、2023年4月までにサービスへのアクセス停止が予定されている

Gov.UK Verifyのスキーム図



The UK digital identity and attributes trust framework①

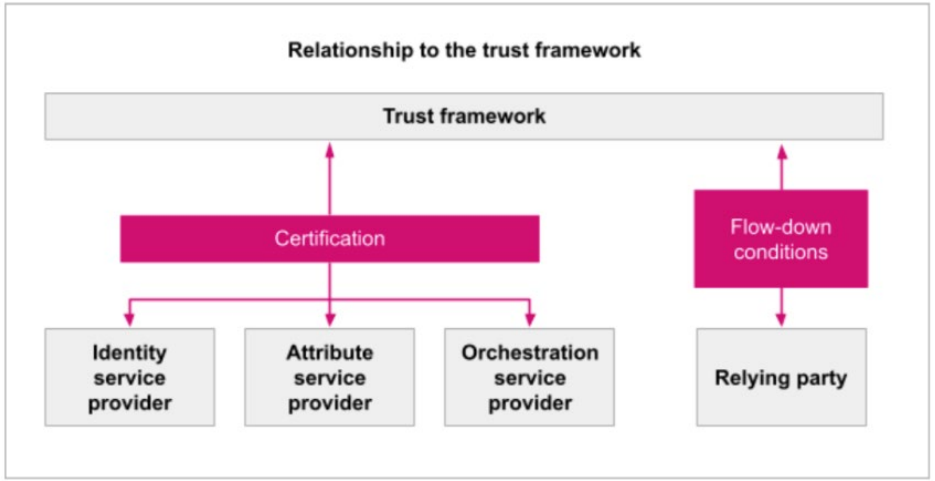
概要[1]

- 英国政府が定めた個人及び個人に関する情報を証明できるサービスをより簡単かつ安全に使用可能にすることを目的としたトラストフレームワークで、デジタルIDおよび/または属性情報を提供する際に遵守すべき一連のルールが規定されている
- 2021年にプロトタイプ「アルファ」を発表、その後2022年6月に「ベータ」版としてアップデートしている。ベータ版では、アルファ版で規定された役割のタイプに当てはまらない組織が出たことを踏まえ、サブ役割を追加する等より実態に合わせた更新を行った
- 組織間で同様のトラストフレームワークに基づいてデジタルIDを作成・運用することでデジタルIDを再利用できるコンセプトを目指し、OpenID Connect, W3C VC core v1.1などのデータ交換・技術標準などの業界アプローチと矛盾しないよう設計されている
- オープン環境で共同開発を行うためにGithub上にデジタルIDに紐づけられる属性情報のデータ・スキーマのドラフトがアップロードされている[2]
- フレームワークの評価のために、サンドボックス形式の演習を含むライブテストを行い、各組織によるフレームワークの理解・サービス改良を促進している

スキーム

- フレームワークにおける役割はIDサービスプロバイダー、属性サービスプロバイダー、オーケストレーションサービスプロバイダ、スキームオーナー及びユーザーの5種類が規定され、それぞれがフレームワークに準拠した認定を受けることによって、参加者間で相互運用可能なデジタルIDサービスのスキームが構築される

トラストフレームワークと参加者の関係



- **identity service providers（IDサービスプロバイダー）**
  - ✓ ユーザー（のデジタルID）の証明・検証を行う
  - ✓ ID検証を行うソフトウェア（モバイルアカウントの検証機能、生体認証対応の身元確認機能など）の開発を行う主体も該当する
- **attribute service providers（属性サービスプロバイダー）**
  - ✓ IDに紐づく属性情報（パスポート、運転免許証、出生証明書などの文書やデータベースにある属性情報や携帯電話番号、銀行口座、クレジットスコア、住宅ローンなど）の作成、収集、検証を行う主体であり、個人のデータストアやデジタルウォレットなどのソフトウェアを指す
- **orchestration service providers**
  - ✓ テクノロジインフラストラクチャ（分散型台帳など）の提供を通じて、トラストフレームワークの参加者間でデータを安全に共有する
- **scheme owners**
  - ✓ デジタルIDと属性情報を使用するためのスキームを作成及び実行する
  - ✓ 民間部門（サービス）におけるスキームについてはISO 17021:2012やISO / IEC 17065:2012などの標準を使用して、UKAS（英国認証機関認定審議会）の認定を受けることやスキームのデータ保護影響評価（DPIA：Data protection impact assessments）を完了していること等が求められる

出所）
1 https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version
2 https://github.com/Alastairtreharne1/Digital_Identity

The UK digital identity and attributes trust framework②

The UK digital identity and attributes trust frameworkでは、スキームとその参加者（各サービスプロバイダ等）の役割、及び各参加者が遵守すべきルールについて、英国政府のグッドプラクティスガイド（GPG）や国際標準を参照する形で規定している

The UK digital identity and attributes trust frameworkの章構成及び規定内容

1. 閣僚からの序文 ～ 9. トラストフレームワークを実行するユーザー	トラストフレームワークのエディトリアルな情報や、使用される用語、フレームワークに参加することによって得られる企業・ユーザーにとってのメリットについて
10. 組織がフレームワークに参加する方法	フレームワークにおける各ロールの役割、スキームについて
11. IDサービスプロバイダのルール	英国政府のGPG45を活用して身元確認を行うことについて
12. 属性サービスプロバイダのルール	属性情報の生成と、個人・組織へのバインド方法のガイダンス、属性情報の品質スコアリングについて
13.IDサービスプロバイダと属性サービスプロバイダの共通ルール	ID、属性サービスプロバイダに共通した、認証器による検証の方法、アカウントの管理、サービスの廃止要領等について
14. オーケストレーションサービスプロバイダのルール	オーケストレーションサービスプロバイダは15項に従うこと
15. 全てのサービスプロバイダの共通ルール	データモデルの相互運用性や、暗号化技術、及び組織の情報セキュリティ、リスク管理などの運用面のルール、参照すべき標準などについて
16. 規格、ガイダンス、法律の表	各項目にて示された規律・ガイダンス・法律を整理した表

出所）1 https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version#who-runs-the-trust-framework

3.1 詳細調査結果：共通識別番号・デジタルIDに関する政策動向

3.1.2北米（米国、カナダ）における調査結果

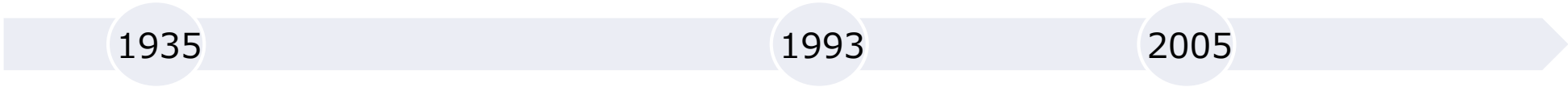
現在に至るまでの変遷

米国のID政策においては、従来から利用されている社会保障番号に代わる統一的な国民ID制度を模索しているものの未だ実現していない

社会保障法（社会保障番号）（1935～）[1]
当初社会福祉分野での活用を見越して制定された識別番号だが、行政・民間幷利用分野が拡大されていった

1970年代以降、社会保障番号の漏洩、なりすまし、詐欺が問題化

Real ID Act（2005～）[3,4,5]
911テロ以降、セキュリティ強化を目指し検討されている国民IDカードの連邦統一基準延期され、未だ施行されていない



Health Security Card（1993）[2]
クリントン政権において発行が検討されたが、実現しなかった全国民対象の健康医療IDカード

出所）
1 https://www.ssa.gov/history/ssn/ssnchron.html
2 https://www.heritage.org/health-care-reform/report/guide-the-clinton-health-plan
3 https://archive.epic.org/privacy/id_cards/#state
4 https://www.dhs.gov/xlibrary/assets/nprm_realid.pdf
5 https://www.jetro.go.jp/biznews/2022/12/df2ee82495881873.html

主な共通識別番号の概要

米国では全国民に共通した識別番号は存在しないものの、連邦政府の発行した社会保障番号（SSN）が行政・民間の広いサービスで利用されている他、公的な本人確認に利用可能な識別手段としては州政府発行の運転免許証や市民IDカードなどが用いられている

連邦政府の管轄する識別制度

社会保障番号（SSN）[1]

- 連邦政府機関である社会保障局が管轄する9桁の番号であり、当初は社会保障給付金の支給など、社会保障分野での利用を目的として1935年に制定されたが、その後段階的に利用範囲が拡大し、金融・税務などを含む幅広い行政・民間の分野で活用され、事実上の国民識別基盤となった歴史的経緯があり、州政府発行の運転免許取得にも必要となる
- しかし社会保障番号を使ったなりすましによる不正受給や情報漏洩が度々発生し、代替的な識別子を求める動きは継続されている

PIVカード[2]

- 連邦政府機関の職員に発行されるIDカードであり、セキュリティ強化の面からICチップの規格などが定められている

州政府の管轄する識別制度

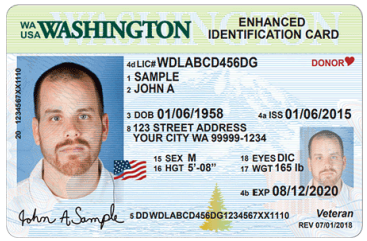
運転免許証[3]

- 米国の運転免許証の発行は連邦以下の州政府の管轄であり、発行条件や形式は州により異なる

市民カード[4,5]

- 州政府発行の身分証として州政府IDカードがあるほか、自治体発行としてNY市のIDNYCカードなどが存在する

ワシントン州IDの例



出所）
1 https://www.ssa.gov/history/ssn/ssnchron.html
2 https://www.ipa.go.jp/security/fy21/reports/tech1-tg/b_07.html
3 https://www.chicago.us.emb-japan.go.jp/con_realID.htm
4 https://www.dol.wa.gov/driverslicense/IDdesigns.html
5 https://www.nyc.gov/site/idnyc/about/about.page

社会保障番号に係る諸問題

米国においては、従来から存在する社会保障番号（SSN）が広範に個人認証に利用され、行政・民間サービスの双方で利用範囲が拡大されていたが、ワンストップの9桁の番号で多数の認証に利用されたことから、漏洩・なりすましなどの問題により、行政機関・民間企業のSSN収集制限や、SSNを含むプライバシー保護法が成立した

1935年の社会保障法によって社会保障番号が制度化され、当初は社会保障プラグラムにおける個人認証を目的としていたものの、米国内での身分証明として行政・民間の双方で広範に利用されるようになった

1960年代以降、社会保障番号の漏洩などによる盗難情報を利用したなりすまし・給付金詐欺、不正口座開設などが社会問題化

社会保障番号の提供・利用を含むプライバシー保護法が成立し、近年ではデジタル空間におけるプライバシー法の成立が民主党政権の公約に掲げられている

・プライバシー法（1974年）

・社会保障番号機密法（2000年）

・米国連邦データプライバシー法案（2019年）

社会保障番号に代わる識別制度の模索

米国では、社会保障番号に代わる統一された国民IDの発行が試みられているもののプライバシーの観点などから廃止されてきた経緯があり、9.11同時多発テロ以降、テロ対策強化のため試みられているReal ID法についても施行は延期されている

米国において実現していない国民IDの試み

Health Security Cardの発行（1993年）[1]

- クリントン政権期に、クリントン・ヘルスプランの一環として全国民に医療・健康サービスを受ける権利を保障するためのIDカードの発行が試みられた
- しかし、制度を検討する政府内タスクフォースの審議状況が不透明であったことや、健康保険業界からの反対、連邦政府が全国民にIDカードを発行することによるプライバシーの観点からの批判を受け、実現しなかった

Real ID Act（2005年～）[2,3,4]

- 9.11同時多発テロ事件において、実行犯が州政府発行のIDによって航空機に搭乗していたことから、連邦政府が統一したIDの基準を設ける法案として提起された
- 内容としては、州政府の発行する運転免許証の発行条件に連邦政府としての統一基準を設けるものであり、発行申請における写真、生年月日、住所、SSNなどの収集情報を統一し、政府機関が管理することでセキュリティを強化するとされた
- しかし、運転免許証が統一国民IDとなることや、政府機関の情報管理がプライバシー侵害にあたるなどの反対にあい、その導入は繰り返し延期され、現在は新型コロナウィルス蔓延によるロックダウン下での身分証明に既存の運転免許証システムが必要であることから、2025年まで施行が延期されている

出所）
1 https://www.heritage.org/health-care-reform/report/guide-the-clinton-health-plan
2 https://archive.epic.org/privacy/id_cards/#state
3 https://www.dhs.gov/xlibrary/assets/nprm_realid.pdf
4 https://www.jetro.go.jp/biznews/2022/12/df2ee82495881873.html

現在に至るまでの変遷

米国ではオンラインサービスの普及に伴い、デジタルIDの活用に係るエコシステムやステークホルダーの定義、フレームワークの作成などに向けた政策が実施されている

NSTIC（2011～）[1,2]
オンラインID管理における参加者・役割を定義するとともに、IDプロバイダーや属性情報提供者といった、参加者の責任に対して「公正な情報取り扱い原則」を定め、プライバシーを保護したID識別・認証を推進する

2011

2021

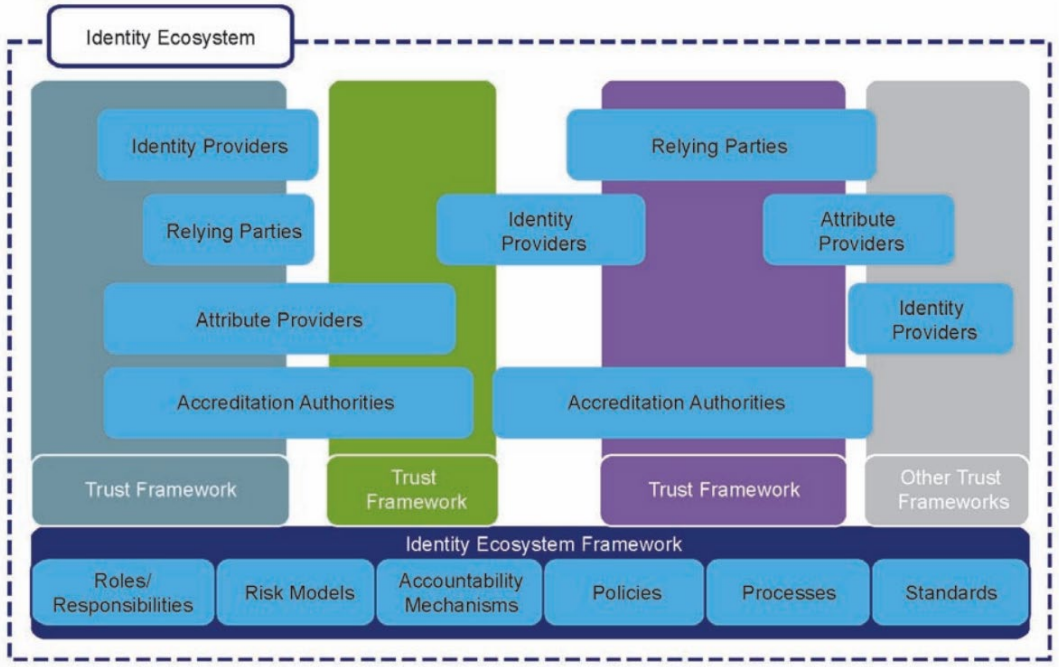
IDIA（2021～）[3,4]
デジタルIDのインフラ整備を進めるための超党的な法案であり、法制化されれば、連邦政府は官民協力のもと、タスクフォースの設立、デジタルIDフレームワークの作成などを行う

出所）
1 https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
2 https://www.aclu.org/news/national-security/dont-put-your-trust-trusted-identities
3 https://www.congress.gov/bill/117th-congress/house-bill/4258/text?r=81
4 https://findbiometrics.com/new-us-digital-identity-act-expected-pass-paving-way-next-gen-id-70702/

NSTIC

米国政府が2011年に発表した「サイバースペースにおける信頼あるアイデンティティのための国家戦略」[1,2]（NSTIC）は、オンラインID管理における参加者・役割を定義（アイデンティティエコシステム）するとともに、IDプロバイダーや属性情報プロバイダーといったエコシステムの各参加者に対して「公正な情報取り扱い原則」(FIPPs)を定め、よりプライバシーを保護した識別・認証環境を推進するイニシアチブである

NSTICの定めるアイデンティティエコシステムの概要



トラストフレームワーク

- IDプロバイダー、Relying Party（依拠当事者）、属性情報提供者、認定当局などの参加者が共通認識をもって連携するコミュニティを指す
- 各参加者は複数のトラストフレームワークを横断して参加している場合もあり、下記のアイデンティティエコシステムフレームワークを基礎として相互運用性を確保するとしている
- 証明情報の格納先（ウォレット等にあたる）としてID媒体（ID medium）という用語を用いている

IDエコシステムフレームワーク

- 相互運用性を持たせるための標準やリスクモデル、プライバシーポリシー・要件など、基礎となるもの

出所）
1 https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
2 https://www.aclu.org/news/national-security/dont-put-your-trust-trusted-identities

The Improving Digital Identity Act of 2021 (IDIA)

米国では2021年6月にデジタルIDのインフラ整備を進めるための超党的な法案「The Improving Digital Identity Act of 2021 (IDIA)」[1,2]が下院監視・政府改革委員会での検討後下院での可決が見込まれ2022年現在上院へも提出されており、法制化されれば連邦政府は官民協力の下、以下のような事項の実施を求める予定である

IDIAにおける実施事項

Improving Digital Identity Task Forceの設立

連邦、州、準州等の機関が、物理的IDとデジタルID資格情報間のセキュリティを強化する安全な方法を開発するための政府全体の取り組みの確立、調整を行うタスクフォースを大統領府に設置する

デジタルアイデンティティイノベーション助成金

デジタル ID 検証を可能にする高度で安全かつ相互運用可能なシステムの開発支援、及び運転免許証やその他のID資格情報提供システムのアップグレード用として、州、地方、先住民族等に助成金を支給する

デジタルIDフレームワークの作成

NISTは、連邦、州および地方自治体がデジタル ID検証をサポートするサービスを提供する際に従うべきガイドとして、標準、方法論、手順およびプロセスのフレームワークの作成と定期的な更新を行う

会計検査院による調査

合衆国会計検査官（GAO）は法律施行後1年以内に、デジタルIDの採用の増加および普及による推定・潜在的な費用効果の調査や、非政府組織による社会保障番号の収集と保持に関する法的規制要件の分析を行う

出所）
1 https://www.congress.gov/bill/117th-congress/house-bill/4258/text?r=81
2 https://findbiometrics.com/new-us-digital-identity-act-expected-pass-paving-way-next-gen-id-70702/

現在に至るまでの変遷

カナダでは社会保険番号が国民識別番号として活用されているがその使用用途は制限されており、身元証明には運転免許証やパスポート等の証明書が使用されている。統一的な国民IDカードを発行する制度は一時期検討されたものの、プライバシーの侵害等懸念が表明され実現していない

社会保険番号（1967～）[1]
当初税務申告の目的で使用が開始された、後に米国の社会保障番号等と同様に国民識別番号として活用されるようになった

1967

2003

National ID Card（2003）[2,3,4]
米国の911同時多発テロを受け、統一的な国民IDカードの発行を検討したが、プライバシー面等の懸念から反対を受け実現しなかった

出所）
1 https://www.canada.ca/en/employment-social-development/services/sin.html
2 https://www.priv.gc.ca/en/opc-news/speeches/2003/02_05_a_030318/
3 https://cippic.ca/index.php?q=en/national-id-cards
4 https://www.cbc.ca/news/canada/national-id-cards-slammed-at-immigration-hearing-1.358706

主な共通識別番号の概要

カナダにおいては、社会保険番号（SIN）が共通の国民識別番号として存在しているが、その利用目的は法的に制限されているため一般的な身分証明で使用されることはなく、パスポートや市民権証明書、各州の管轄で発行される運転免許証、健康カード等が主に利用されている[1]

連邦政府の管轄する識別番号制度

社会保険番号（SIN）[2]

- 連邦政府のサービス省が発行する9桁の番号であり当初は税申告の利用目的で発行開始されたが、その後就労や政府の公共サービスの利用に役割が拡大された
- SINの提供機会は、就職での採用時、利子の付随する銀行口座開設、政府プログラムへのアクセスなどに制限されており、一般的な身元証明（携帯電話の利用、ローンの申請、物件を借りる際）では必ずしも提供する必要はない
- 過去はプラスチック製のSINカードを発行していたが現在は廃止され、紙のSINレターが発行されている

一般的に用いられる識別手段

運転免許証[3]

- カナダの運転免許証の発行は州政府の管轄であり、発行条件や形式は州により異なる

健康カード[4]

- カナダ保険法の規定に基づき州政府の管轄で発行するカードであり、各州の健康医療プログラムで負担される健康・医療サービスへのアクセスに必要となる。カバーする医療サービスの範囲や、発行条件、形式は州により異なる

ケベック州健康カードの例

出所）
1 https://www.ramq.gouv.qc.ca/en/citizens/health-insurance/using-card
2 https://www.canada.ca/en/employment-social-development/services/sin.html
3 https://www.canada.ca/en/immigration-refugees-citizenship/services/new-immigrants/new-life-canada/driving.html
4 https://www.canada.ca/en/health-canada/services/health-cards.html

National ID Card

過去、カナダにおいて統一的な国民IDカードの制度化に関する議論は存在したが、プライバシー権の侵害や、費用の面から反対を受け実現しなかった[1,2,3]

National ID Card

- 米国の9.11同時多発テロによる安全保障要求の高まりを受け、2003年にカナダ市民権移民局を中心として、カナダ政府議会において協議された統一的な国民IDカードの発行制度
- カナダ在住者の氏名、生年月日、出生地、性別、住所、身体的属性などの情報を表示したプラスチックカードに、ICチップが備え付けられ、指紋や網膜パターンなどの生体認証データを含める可能性についても言及されていた
- 単一の全国的な証明書による利便性の向上や、セキュリティの強化などが利点として挙げられていたが、一つのカードに膨大な個人情報が集約されることによる危険性、政府が国民の生体情報を大規模に収集するプライバシー侵害の懸念などから、プライバシーコミッショナーや各州政府、ブリティッシュコロンビア市民自由協会などからの反対を受け、実現しなかった

出所）
1 https://www.priv.gc.ca/en/opc-news/speeches/2003/02_05_a_030318/
2 https://cippic.ca/index.php?q=en/national-id-cards
3 https://www.cbc.ca/news/canada/national-id-cards-slammed-at-immigration-hearing-1.358706

現在に至るまでの変遷

カナダでは財務省タスクフォースの提言からDIACCの設立を経て、共通的なトラストフレームワークであるPCTFを構築することで、官民双方のデジタルID活用を推進している

the Task Force for the Payments System Review （2010～2012）
財務省がカナダ経済がデジタル決済システムに移行するためのタスクフォースを立ち上げ、政府、企業、消費者団体、金融セクターなどからなるワーキンググループで議論し、提言を実施した

2010

2014

DIACC（2014～）
先のタスクフォースの提言を受け、政府・民間企業から構成される非営利組織であるDIACCがデジタルIDソリューションとサービスを実現するための研究開発に取り組むこととなった

PCTF（2020～） [1,2]
カナダの官民組織がデジタルアイデンティティを安全に活用するためのガバナンスモデルとしてDIACCが2020年にPCTF v1.0を発表した

2020

2022

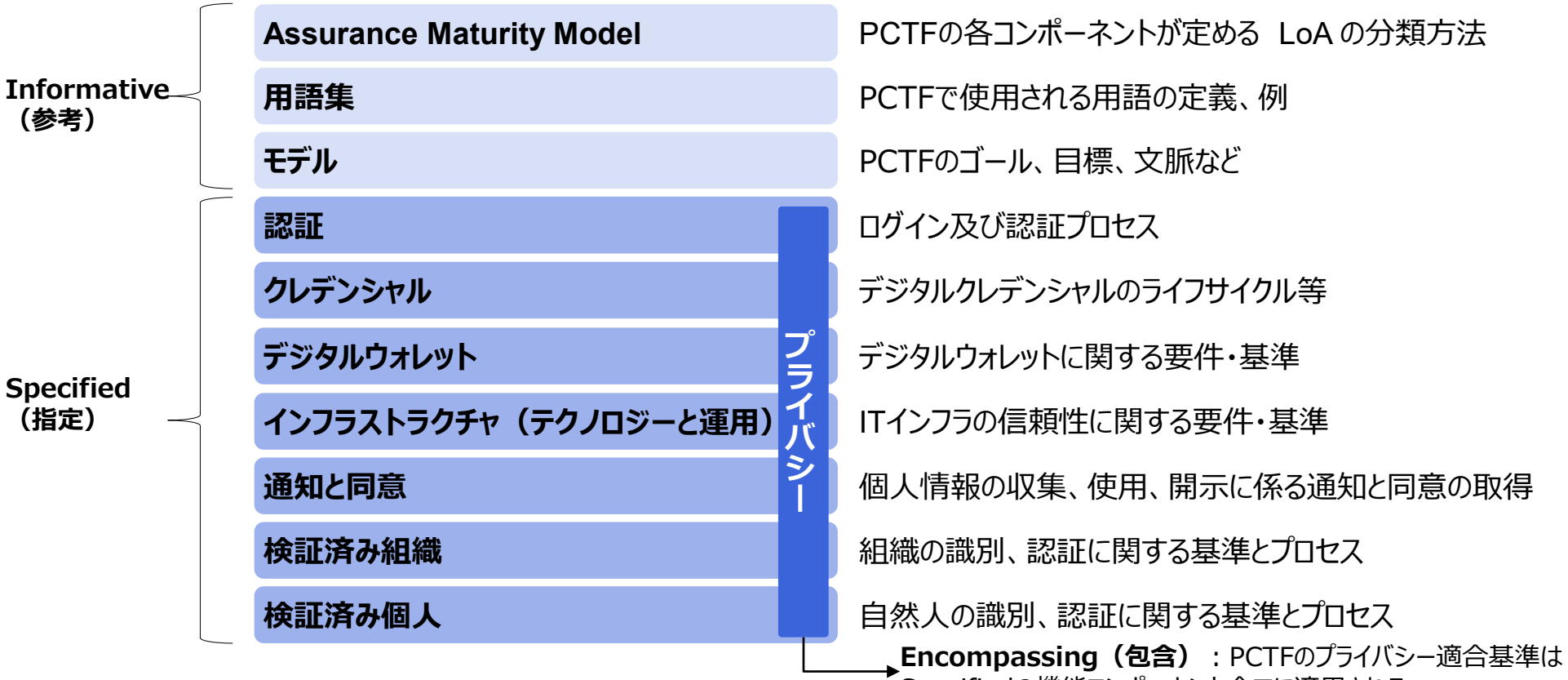
Digital Ambition 2022（2022～） [3]
カカナダの今後3年間のデジタル戦略計画を2022年8月に発表し、優先事項と主要なアクションについて述べ、その中で「既存の州のプラットフォームと統合された連邦デジタルIDプログラム」に取り組むとしている

出所）
1 https://diacc.ca/
2 https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation_V1.0.pdf
3 https://tnc.news/2022/08/10/digital-identity-program1/

DIACCによるPCTFの策定

カナダにおいては、政府・民間企業から構成される非営利組織であるDIACC（カナダデジタル識別認証評議会）がデジタルIDソリューションとサービスを実現するための研究開発に取り組んでおり、IACCは、カナダの官民組織がデジタルアイデンティティを安全に活用するためのガバナンスモデルとしてPCTF（Pan-Canadian Trust Framework）を開発し、2020年11月にPCTF 1.0 alphaを発表した。PCTFは、カナダのデジタルアイデンティティ管理における原則や基準、デジタルIDの作成、管理、提供に係る一連のプロセスなどを定義しており、デジタルIDに関係する公共・民間のステークホルダー、研究者などに参照されることを目的としている[1]

PCTFの構成要素（構造）



出所）
1 https://diacc.ca/trust-framework/

Digital Ambition 2022

カナダ政府は、カナダの今後3年間のデジタル戦略計画のレポートである「Canada's Digital Ambition 2022」を2022年8月に発表し、優先事項と主要なアクションについて述べており、その中で「既存の州のプラットフォームと統合された連邦デジタルIDプログラム」が必要であるとし、主要なアクションとして「共通・安全なデジタルIDフレームワークの策定」「デジタルIDプログラムの確立」などを挙げているが、アクションの具体的な詳細は示されていない[1,2]

DIACCはDigital Ambition 2022を歓迎するとともに、連邦政府に対し州・準州とのデジタルIDイニシアチブの連携を強化することを2022年10月の予算協議において勧告している[3]

Digital Ambition 2022におけるデジタルIDへの言及

Canada' Digital Ambition 2022

- **戦略テーマ１：テクノロジーとオペレーションの卓越性**
- **戦略テーマ２：データを活用したデジタルサービスとプログラム**
  - **優先事項2.1：データと情報価値の最大化**
  - **優先事項2.2：デジタルサービス提供のための安全な共通ソリューションの構築と使用**
  - **優先事項2.3：戦略的資産としてのデータと情報の管理と使用**
- **戦略テーマ３：行動可能なデジタル政策と戦略**
- **戦略テーマ４：資金調達、人材、文化の構造進化**

優先事項2.2を達成するためのアクション：
行政デジタルサービスを改善するためのプラットフォーム整備におけるデジタルIDに関するアクションが含まれている

・デジタルIDフレームワークに関するパブリックコンサルテーションの開始
・デジタルIDへの共通で安全なフレームワークの開発
・政府とやり取りをするためのデジタルIDプログラムの確立

出所）
1 https://tnc.news/2022/08/10/digital-identity-program1/
2 https://www.canada.ca/en/government/system/digital-government/government-canada-digital-operations-strategic-plans/canada-digital-ambition.html#toc5
3 https://diacc.ca/2022/10/

Digital Ambition 2022

Digital Ambition 2022において「既存の州のプラットフォームと統合された連邦デジタルIDプログラム」に取り組むと述べられ、オンタリオ州やブリティッシュコロンビア州では州ごとのデジタルIDシステムに取り組んでいること等から、それらと連携とした連邦型のデジタルIDシステムを連邦政府が想定していることが伺える

カナダにおける連邦デジタルIDプログラムに関する情報・事例

オンタリオ州デジタルID[1]
オンタリオ州政府は、民間企業と連携した州の住民向けのデジタルIDサービスの開発・提供を実施しており、W3C、DIF、ToIP、OIDFなどに準拠した分散型・自己主権型IDのモデルを採用している

ブリティッシュコロンビア州：BCデジタルトラスト[2]
ブリティッシュコロンビア州政府は、VCを発行・検証するためのソフトウェアや、オープンソースのデジタルIDウォレットであるBCウォレット及び州政府等の発行した資格情報を検索・入手できるパブリックディレクトリである「OrgBook BC」の開発・提供を行っている

カナダ銀行協会（Canadian Bankers Association：CBA）の提言[3,4]
- カナダの公認銀行を代表する業界団体として研究・政策提案などを行うCBAは、カナダにおけるフェデレーションデジタルIDスキームの構築を提案している
- CBAは、カナダの将来的なデジタルIDシステムに関するホワイトペーパーである「カナダのデジタルIDの未来 - フェデレーテッドアプローチ」において、「カナダでは連邦政治構造から、連邦政府と州政府の両方がIDインフラの各部分を処理しているため、集中的なIDシステムではなくフェデレーテッド・アプローチが望ましい」旨述べている

出所）
1 https://www.ontario.ca/page/ontarios-digital-id-technology-and-standards?utm_source=newsroom&utm_medium=email&utm_campaign=%2Fen%2Frelease%2F1000787%2Fontario-releases-technology-and-standards-for-digital-identity&utm_term=media
2 https://digital.gov.bc.ca/digital-trust
3 https://mobileidworld.com/Canadian-bankers-voice-support-federated-national-digital-identity-scheme-030209/
4 https://cba.ca/embracing-digital-id-in-canada

3.1 詳細調査結果：共通識別番号・デジタルIDに関する政策動向

3.1.3 オセアニア（オーストラリア、ニュージーランド）における調査結果

現在に至るまでの変遷

オーストラリアには日本のマイナンバーカードに該当するような国民共通番号制度は現状存在せず用途に応じて複数の番号を使い分けている状況であり、統一的な国民識別制度は過去検討されたもののいずれも実現しなかった

Tax File Number（1930～）
納税にあたって個人及び組織を一意に識別するために用いられる

1930

1985

Australia Card（1985~1987）
統一的な識別制度であるオーストラリアカードを導入するための法案が議会に提出された。この法案はIDカードの使用を強制するものではなかったが、事実上強制的な仕組みであると上院で民主党等が反対票を投じ否決され、1987年に廃案となった

2005

Identity Card（2005~2006）
2005年半ばのロンドン同時爆破事件とコーネリア・ラウの拘束に関するレポートを受け、オーストラリアカード以来、再び政治課題として浮上した。同2006年にメリットよりもデメリットの方が大きいとして導入は見送られた

2006

Smart card / access card（2006~）
2006年4月、ハワード政権時に17枚の医療・社会サービスカードに変わるアクセスカードが閣議決定された。2008年から2年間の登録機関を経て、段階的に導入される予定となっていたが、2007年11月、ラッド労働党政府下でプロジェクトの終了が報告された

2010

Health Care Identifier（2010）[1]
医療提供者と医療を求める個人を一意に識別する識別子で名前・生年月日・性別が基本情報として登録されている

出所）
1 https://www.health.gov.au/topics/health-technologies-and-digital-health/about/healthcare-identifiers

主な共通識別番号の概要

オーストラリアには日本のマイナンバーカードに該当するような、国民共通番号制度は現状存在せず、用途に応じて複数の番号を使い分けている

オーストラリアで使用されている番号制度

【国の管轄】

■ Healthcare Identifier（HI、医療識別子）[1]：

- 医療提供者と医療を求める個人を一意に識別する識別子で名前・生年月日・性別が基本情報として登録されている
- Healthcare Identifiers Regulations 2010で規則が定められ、現在はHealthcare Identifiers Regulations 2020の規定で運用中
- Individual Healthcare Identifier（**IHI**）、Health Provider Identifier-Individual **(HPI-I)**、Health Provider Identifier-Organisation（**HPI-O**）の3種類の識別子が割当られており、それぞれヘルスケアシステム内での個人の識別、患者ケアの提供に携わる医療提供者の識別、療サービスを提供する組織の識別に用いられている
- IHIはオーストラリアの全国的なデジタル健康記録プラットフォームである**My Health Record(MHR)への登録に活用**されている

【州の管轄】

■ Birth certificate（出生証明）[2]：

- 登録番号の設定は州で行われるため、州ごとに番号の桁数も異なる
（例：クイーンズランドは5桁、南オーストラリア州は8桁）
- 州によっては、登録時期によって登録番号がない場合もある
（例：クイーンズランドは1996年7月1日より前の出生証明書に登録番号はない）

■ Driver licence（運転免許証）[3]：

- 州ごとに発行されるが運転免許証の共通の設計基準はない
- 基本情報として、顔写真・名前・住所・生年月日・カード番号が登録されている

クイーンズランドの運転免許証

出所）
1 https://www.health.gov.au/topics/health-technologies-and-digital-health/about/healthcare-identifiers
2 https://www.usi.gov.au/students/identification/australian-birth-certificate
3 https://austroads.com.au/drivers-and-vehicles/registration-and-licensing/australian-driver-licensing

実現しなかった統一的な国民識別制度

オーストラリアでは過去に国民IDカードの実現を目指した提案があったが、いずれも批判を受けて失敗している[1]

Australia Cardの提案（1985-1987）

- 1985年、ボブ・ホーク労働党政権時に提出された「オーストラリア税制改革：白書草案」の中で、全国的な身分証明システムとして提案された
- オーストラリアカードの主な目的は課税制度と連邦給付の支払いによる歳入の損失防止にあり、カードによって情報の照合が容易になり、銀行口座の開設、投資、不動産の売買、求職など、さまざまな取引でカードを作成する必要があるため、脱税、社会保障費の不正受給、不法滞在者が減ると主張された
- 1986年10月にオーストラリアカード（IDカード）を導入するための法案が議会に提出された。この法案はIDカードの使用を強制するものではなかったが、事実上強制的な仕組みであると上院で民主党等が反対票を投じ否決され、1987年に廃案となった

Identity cardの提案（2005-2006）

- 2005年半ばのロンドン同時爆破事件とコーネリア・ラウの拘束に関するレポートを受け、オーストラリアカード以来、再び政治課題として浮上した
- オーストラリアカード法案に反対していたハワード首相は、2005年7月15日のぶら下がり取材時に国民IDカードは「我々に必要な鎧の一つかもしれない」と述べ、2006年1月に国民IDカードの有効性、コスト、プライバシーへの配慮などを検討する委員会が設置されたが、同2006年4月にオーストラリア政府はメリットよりもデメリットの方が大きいとして国民IDカードの導入を見送った

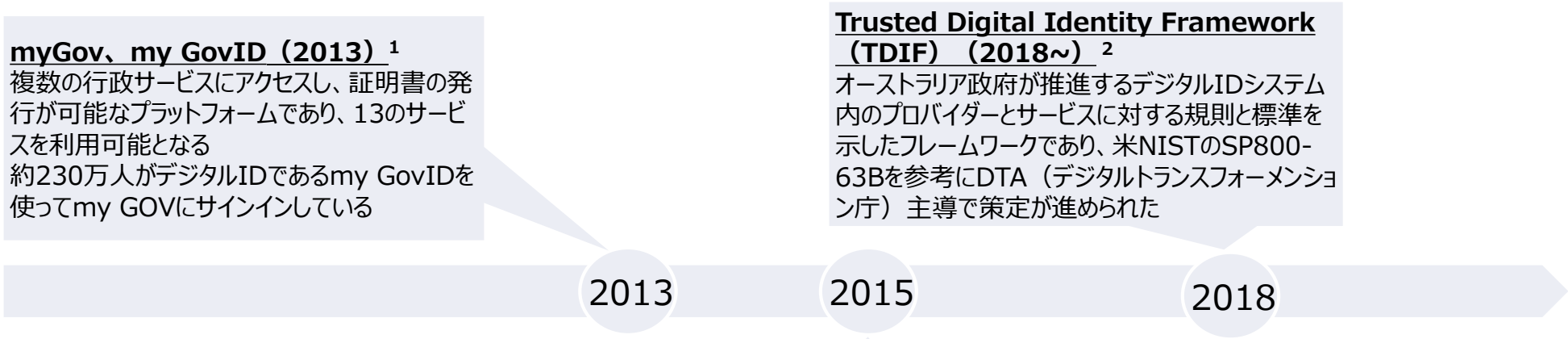
Smart card / access cardの提案（2006-2007）

- 2006年4月、ハワード政権時に17枚の医療・社会サービスカードに変わるアクセスカードが閣議決定された
- アクセスカードにはカード所有者の名前、デジタル写真、署名、カード番号が記載、カード内のマイクロチップには、写真、住所、生年月日、子供やその他の扶養家族の詳細が保存されていた。
- アクセスカードは2008年から2年間の登録機関を経て、段階的に導入される予定となっていたが、2007年11月、ラッド労働党政府下でプロジェクトの終了が報告された

出所）
1 https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Publications_Archive/archive/identitycards

現在に至るまでの変遷

オーストラリア政府のデジタルIDを活用した取り組みは、行政サービスの効率的な利活用促進に向けた取組から、デジタルIDシステムやトラストフレームワークといった全体的なIDガバナンスの構築に向けた取り組みへ移行している



出所）
1 https://my.gov.au/en/about
2 https://www.digitalidentity.gov.au/system-partners

オーストラリア政府のデジタルIDに関する取組

オーストラリア政府は、デジタル経済戦略の中でデジタルIDに関する取組の推進について言及しており、これまではデジタルIDを活用した行政サービスの効率的な利活用促進に向けた取組が中心であったが、現在はデジタルIDシステムやトラストフレームワークといった、全体的なIDガバナンスの構築に向けた計画が推進されている[1]

～2020までのデジタルID関連の取組

信頼性の高いオンラインIDに向けた取組		政府による「文書認証サービス（Document Verification Service）」利用の奨励
		政府が民間サードパーティのデジタル認証手段を利用することを検討
ID関連の行政サービスの状況	My Health Record（2012年～）	投薬、副作用、アレルギー、予防接種歴などの健康情報プラットフォーム。 Individual Healthcare Identifier（IHI）を用いて登録可能。約2,290万人が登録。
	myGov（2013年～）	複数の行政サービスにアクセスし、証明書の発行が可能なプラットフォーム。 約1,980万人がアカウント登録済。13のサービスを利用可能 約230万人がデジタルIDであるMyGovIDを使ってMygovにサインインしている

～2030までのデジタルID関連の取組計画

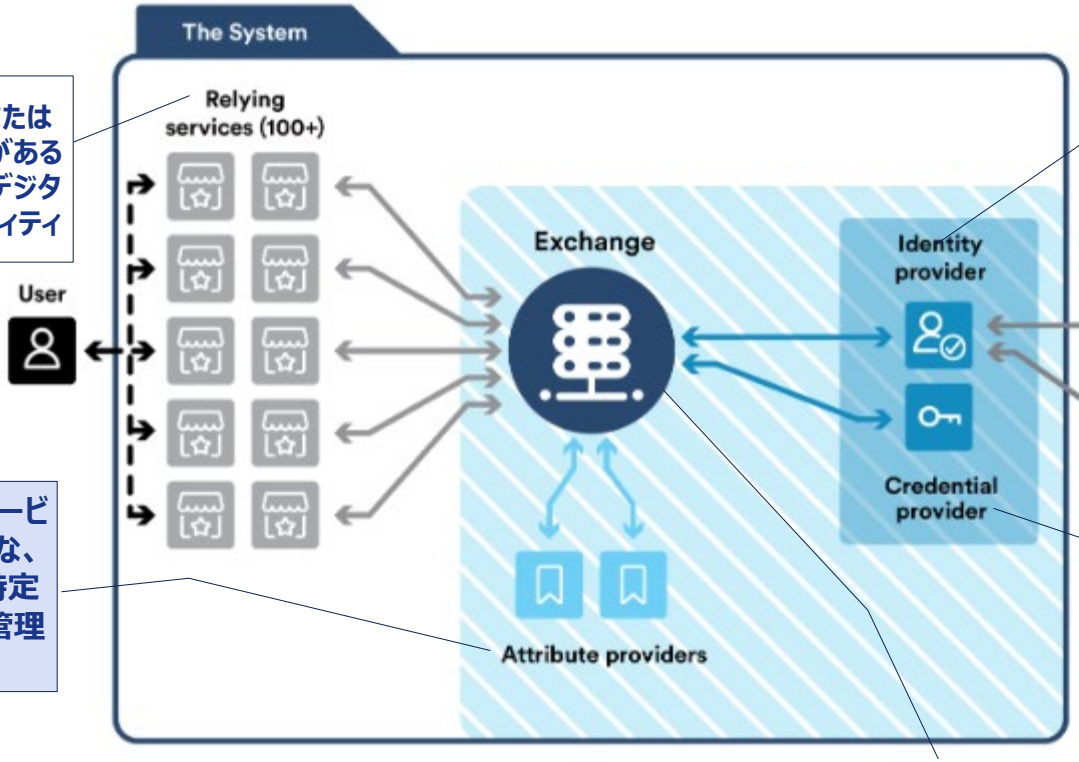
Digital Identity System（デジタルIDシステム）	• 政府および経済界全体からのサービスへの安全かつシンプルなアクセスのためのデジタル・アイデンティティ・システムの利用を拡大 ➢ デジタルIDは既に230万人以上のオーストラリア人と120万円社の企業が75以上の政府サービスを活用する際に利用されており、政府はデジタルIDシステムの構築に21-22年度予算として約2億5,660万ドルを投資している。
Trusted Digital Identity Framework（TDIF）	• オーストラリアのデジタルID制度のルールを定めたもので、人々がオンライン・サービスにアクセスすることをより容易かつ安全にし、年間31億ドル以上の経済的損失をもたらすと推定されるID犯罪に対する保護を強化するもの • 政府は、プライバシー、セキュリティ、および詐欺防止のメカニズムを組み込み、参加することを選択した人々の信頼と信用を構築するための法整備を進める予定としており、民間企業や他の政府へのフレームワークの展開を推進していくとしている

出所）
1 https://my.gov.au/en/about

デジタルIDシステム

デジタルIDシステムは、政府のオンラインサービスにアクセスする際に自分自身を安全･安心に証明する方法として、完全任意（非強制的）で、自らがコントロール可能であることを要件に2015年に取組が開始された。デジタルIDシステムを支えるトラストフレーム（TDIF）に基づいて、4種類の認定参加者（Identity providers、Credential providers、Identity exchange、Attribute providers ）を定めている[1]

オーストラリア政府が進めるデジタルIDシステムの全体像とTDIFの認定範囲



デジタルIDを使って身元または属性情報を確認する必要があるシステムを介してオンラインデジタルサービスを提供するエンティティ

サービスプロバイダーがサービスを提供するために必要な、個人、法人等に関する特定の「属性情報」の生成、管理を行うエンティティ

オンラインサービスの利用を希望する人に対して、身元確認するためのデジタルIDを作成し管理する認定を受けたエンティティ

認証サービス（文書認証サービス（DVS）や顔認証サービス（FVS）など）

システムで使用されるパスワードやその他形式の認証資格情報を処理するエンティティ

デジタルIDシステム内のエンティティ間の相互連携を担うエンティティ

TDIFの規定範囲

：TDIFの認証参加者

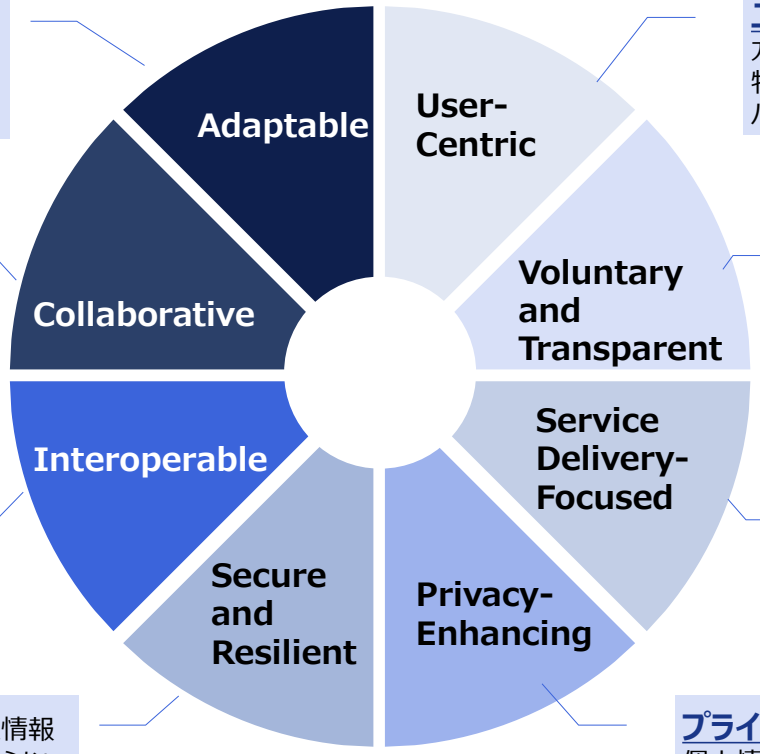
出所）
1 https://www.digitalidentity.gov.au/system-partners

オーストラリア
ニュージーランド

Trusted Digital Identity Framework（TDIF）

TDIFはオーストラリア政府が推進するデジタルIDシステム内のプロバイダーとサービスに対する厳格な規則と標準を示したフレームワークであり、米NISTのSP800-63Bを参考にDTA（デジタルトランスフォーメンション庁）主導で策定が進められ2018年に公表された[1]

TDIFの指導原則（Guiding principles）



適応性：このフレームワーク進化するコミュニティの期待やビジネス、技術、法律、社会的ニーズの変化に迅速に対応できるように、適応性と柔軟性を備えている必要がある

ユーザー中心：個人と組織が簡単かつ信頼された方法でデジタルサービスにアクセスすることを保証する。特に個人には、デジタルIDプロバイダーやサービスプロバイダーを柔軟に選択できるようにする必要がある

共同作業：政府と企業のそれぞれの長所と専門性が最適に活用できるように、公共部門、民間部門、そしてより広いコミュニティ間の活発なコラボレーションを奨励すること

自主性と透明性：デジタルIDへのアクセスと使用に関するコントロールを個人に与える。また認定参加者はクレデンシャルの使用を記録し、権限を与えられた者のみが記録にアクセスできるようにすることを義務付ける

相互運用性：他のトラストフレームワークや国内外のIDサービスと相互接続し、エコシステムの利点が最大限に個人と機関に行き渡るようにする

サービス提供に重点：認定参加者はユーザーに選択肢と利便性を提供する必要があり、またコストはどの利用者にとっても中立であるべきである

セキュアかつレジリエント：ユーザーの個人情報は外部の脅威から保護され、安全でなければならない。認定参加者は政府の厳しいセキュリティ基準を満たし、リスクの特定と軽減を行うことを保証する必要がある

プライバシーの向上：認定参加者がユーザーの個人情報を収集、開示する際は、ユーザー同意を得て、プライバシー法等の慣行に則っていることを保証する必要がある

出所）
1 https://www.digitalidentity.gov.au/sites/default/files/2022-03/TDIF%2002%20Overview%20-%20Release%204.6%20%28Doc%20Version%201.3%29.pdf

TDIFの機能要件

TDIFの認定参加者の役割に応じて適用される機能要件として、不正管理、プライバシー、保護セキュリティ、ユーザ体験、技術テストなどが定められている[1]

TDIFの機能要件

不正管理（Fraud Control）	認定参加者への申請者に対して適用される最低限の不正管理基準を定めており、基本的には連邦不正管理フレームワーク（CFCF：the Commonwealth Fraud Control Framework）への準拠を求めている（TDIFで定める要件とCFCFの最新版で規定されている要件に矛盾がある場合はCFCFを優先するとされている）。
プライバシー（Privacy）	認定参加者への申請者に対して適用される情報取扱要件を定めている。4つの認定種別に共通して課される要件として、オーストラリアプライバシー原則（APPs）を含むプライバシー法に基づく義務、オーストラリア政府機関プライバシーコード、関連する州または地域のプライバシーに関する法律への準拠を定めている。
保護セキュリティ（Protective Security）	申請者がアイデンティティ・サービスに対して最低限保証することが求められる保護セキュリティ水準を定めている。基本的には、オーストラリアサイバーセキュリティセンター（ACSC）が定めた政府の保護セキュリティポリシーフレームワーク（PSPF）及び情報セキュリティマニュアル（ISM）への準拠が求められる。
ユーザー体験（User Experience）	アイデンティティ・サービスのユーザビリティやIDプルーフィングの流れ、認証の流れについての要件を定めている。具体的には全てのタイプの申請者に対して、ユーザビリティの要件としてアイデンティティシステムの構築に当たりレスポンシブwebデザイン手法の採用やエンドツーエンドのジャーニーマップの作成等を義務付けている
技術テスト（Technical testing）	ユーザビリティテストのテストプランと実施に関する要件を定めている（ただし申請者とユーザーでインタラクションがないことをDTAに証明することができる場合のみは例外）。テストプランの要件としては、全てのタイプの申請者に対してテストの目的、ユーザビリティの目標・指標、テストへの参加人数、募集方法、ユーザビリティテストから得られた知見の実装方法等の作成などが求められている

出所）
1 https://www.digitalidentity.gov.au/sites/default/files/2022-03/TDIF%2004%20Functional%20Requirements%20-%20Release%204.6%20%28Doc%20Version%201.5%29_0.pdf

（補足）TDIFの認定事業者

Identity providers

サービス名称	プロバイダー名称	IPL*	認定日
Digital iD	Australia Post	IP2 (Standard)	2019年5月17日
myGovID	Australian Tax Office	IP1, IP2 (Basic, Standard) IP3 (Strong)	2019年5月30日 2021年8月8日
OCR Labs	OCR Labs	IP2 (Standard) IP3 (Strong)	2021年7月8日 2022年3月7日
ID	Mastercard	IP1+ (Basic)	2022年7月21日

* IPL：Identity proofing levels。作成可能なIDの証明レベルを示す。
IDを使用するサービスが求めるレベルとして、Basic（IPL1、1+）、Standard（IPL2、2+）、Strong（IPL3）の5段階が設定されている

Credential providers

サービス名称	プロバイダー名称	CL**	認定日
Digital iD	Australia Post	CL2	2019年5月17日
myGovID	Australian Tax Office	CL2	2019年5月30日
ID	Mastercard	CL2	2022年7月21日

** CL：Credential levels。認証プロセスにおける保証レベル。IPLごとに適したクレデンシャルレベルとしてCL1～CL3の3段階が設定されている

Identity exchange

サービス名称	プロバイダー名称	サポートしている規格	認定日
Exchange	Services Australia	OpenID Connect 1.0、SAML	2019年5月13日
connectID	eftpos	OpenID Connect 1.0	2021年9月15日
ID	Mastercard	OpenID Connect 1.0	2022年6月10日

Attribute providers

サービス名称	プロバイダー名称	作成される属性	認定日
Relationship Authorisation Manager (RAM)	Australian Tax Office	Business authorisations	2019年6月20日
myGov	Services Australia	myGov LinkID	2021年8月25日

TrustID FrameworkとTDIF

DTAの策定したTDIFとは別に、オーストラリアの決済業界の調整機関であるAPC（オーストラリア決済評議会）は、民間企業に向けたデジタルIDフレームワークであるTrustID Frameworkを策定しており、TrustID FrameworkとTDIFの相互運用性を確保することで、政府・民間双方が発行するデジタルIDが利用可能なネットワークの実現を目指している[1,2,3,4]

TrustID Frameworkの概要

- DTAの「myGovID」や「DigitaliD」などのTDIF認定下のデジタルIDが金融サービス分野での幅広い採用が期待できないと考えられたことを一因として、2019年6月にAPC（オーストラリア決済評議会）によって策定された
- TrustID Frameworkは、オーストラリアの民間企業が提供するデジタルIDソリューションの信頼性、相互運用性を高めるために、組織が製品やサービスの設計と構築において遵守するための一連のルールとガイドラインを提示するものである
- APCはDTAを協力して、Trust ID FrameworkとTDIFの相互運用性を確保し、最終的には政府・民間のデジタルIDサービスで相互運用可能なネットワークを促進するとしている
- APCの事務局的役割を果たすAPN（オーストラリア決裁ネットワーク）は、TrustID Frameworkのガバナンス構造についてコンサルテーションを行った

※APCは、APNとRBA（オーストラリア準備銀行）の共同決議によって2014年に発足した

出所）
1 https://www.itnews.com.au/news/banks-prepare-to-issue-mygov-compatible-digital-identities-532768
2 https://www.rba.gov.au/publications/annual-reports/psb/2020/retail-payments-regulation-and-policy-issues.html
3 https://www.auspaynet.com.au/insights/Trust-ID
4 https://www.australianpaymentscouncil.com.au/wp-content/uploads/2019/12/APC_Annual_Review_2019.pdf

（補足）デジタルIDシステム関連のサービス①

IDMatch（Verification Service）[1]

- オーストラリア内務省によって提供されている、国・州・準州など政府機関によって発行された身分証明書に記載されている個人情報を、パスポート、運転免許証、出生証明書などの既存の政府記録と比較して、**個人情報の有効性を検証することができるオンラインシステム**
- 連邦政府、州、準州政府はIDの共有とマッチングを促進するために2017年に**政府間協定**を締結している
- 政府機関が発行したEOI（Evidence of Identity）文書を権限のある機関が電子的に検証行う**DVS**（Document Verification Service, 2009年～）と政府記録上の画像と照合することで本人確認を可能とする**FVS**（Face Verification Service, 2016年～）、身元不明者の身元確認等に活用可能な**FIS**（Face Identification Service, 2017～）を提供している
- DVSは120を超える連邦、州、準州の機関と1,100を超える民間組織によって活用されている。他方、FVS/FISを利用できるのは政府機関のみ（FISについては法執行機関のみ）である

MyGov（Attribute Provider Service）[2,3]

- 複数の行政サービスに単一のアカウントでオンラインアクセスできるデジタルプラットフォーム。現在は、子育て、生活サポート、老後サポート、仕事、教育、ヘルスケア等、約13のサービスが利用可能である
- 2013年から提供が開始され、政府の執行機関である**Services Australia**により運用されている
- myGov アカウントを myGovサービスにリンクさせるために使用される属性としてMyGov LinkIDを生成する
- 2022年にモバイルアプリがリリースされ、**生体認証によるログイン機能**と**デジタルウォレット**が搭載された。今後は同アプリのデジタルウォレットに**メディアケアカード**（健康保険証）等も追加できるようになるとされている
- myGovの利用にはユーザー登録が必要だが、後述する**myGovIDアプリ**による認証も可能である

出所）
1 https://www.idmatch.gov.au/for-organisations
2 https://my.gov.au/en/about
3 https://www.biometricupdate.com/202212/australia-launches-mygov-digital-identity-mobile-app-at-long-last

（補足）デジタルIDシステム関連のサービス②

myGovID（Identity and Credential Provider Service）[1]

- オーストラリア政府のWebサイトやオンラインサービスにおける認証アプリケーションとして、オーストラリア税務局（ATO）及びDTA（Digital Transformation Agency）によって開発され、2019年にリリースされた
- AusKey（2010年にATOからリリースされた政府オンラインサービスへの認証アプリケーション）をはじめ連邦政府や地方自治体で使用されていた様々な認証方法がmyGovIDに統合された
- myGovID（アプリ）には氏名、生年月日、メールアドレスなど、ユーザーの主要なID情報が保存されており、既存の政府記録と照合される
- myGovIDはTDIFと認証サービスの利用者のIDを保証するためのデジタル鍵、証明書の使用方法を規定したGatekeeper Public Key Infrastructure Frameworkに準拠している
- アプリ上でIDの強度（Basic、Standard、Strong）を選択でき、求めるIDの強度によって必要な情報は異なる。またIDの強度によってアクセス可能なオンラインサービスが制限される

DigitaliD（Identity and Credential Provider Service）[2]

- 2016年にオーストラリア郵便公社からリリースされたモバイルベースの認証アプリ
- DigitaliDを使用して、郵便サービス利用時の身元証明や連携先のオンラインサービスへの認証に利用できるほか、アルコール購入時の年齢確認等、様々な民間企業サービスでも利用可能。また、写真付き身分証明証としても使用できるとされている
- ビジネス視点でのユースケースとしては、クライアントの身分証明書の迅速な照会・検証による新規顧客のオンボーディングコストの削減やマネーロンダリング防止、制裁対象者やリスクの高い個人の特定に利用できるとされている

出所）
1 https://www.mygovid.gov.au/
2 https://www.digitalid.com/personal

現在に至るまでの変遷

ニュージーランドでは統一的な共通識別番号は採用されておらず、税務、医療、教育といった目的別に異なる識別番号を使用する状態が続いている

IRD number（1952～）[1]
国内の税制を所管しているIRD（内国歳入庁）から発行される識別子であり、主に納税管理に使用され、銀行口座の開設や就労の際に必要となる

1952

NHI number（1993～）[2]
ニュージーランド保健省が所管する、国民が医療サービスを利用する際に必要となる識別子であり、出生時、もしくは医療サービスの利用時に付番される
個々の患者の識別と医療記録の管理に使用されるとともに、国家予防接種登録簿（NIR）などのデータベースへ医療従事者がアクセスする際に利用される

1993

NSN number（2010～）[3]
ニュージーランド教育省の所管する、全ての学生に対して付番される一意の識別子であり、ニュージーランドで就学する学生の識別・出席の管理、成績の記録、統計目的などで利用される

2014

出所）
1 https://www.ird.govt.nz/managing-my-tax/ird-numbers
2 https://www.health.govt.nz/our-work/health-identity/national-health-index/nhi-information-health-consumers/national-health-index-questions-and-answers#bused
3 https://www.education.govt.nz/school/managing-and-supporting-students/national-student-number-nsn-for-schools/

主な共通識別番号の概要

ニュージーランドにおいては一般的な運転免許証やパスポート等のほか、アルコールの販売・購入において年齢を証明するKiwiアクセスカードなどが識別手段として用いられ、識別番号としてはIRD番号、NHI番号、NSNなど複数存在しており、それぞれ税務、医療、教育といった目的別に使用されている

一般的に用いられる識別手段

- ニュージーランド国内では、一般的に運転免許証、パスポート、銃器免許証、出生証明書及び市民権証明書などが身分証明に用いられている[1]

Kiwiアクセスカード[2,3]

- アルコールの販売・購入において年齢を証明するためのカードであり、また写真付き身分証明書として運転免許証、パスポートなどの代替として用いることができる。ニュージーランドのホスピタリティ産業、商業宿泊施設の業界団体であるホスピタリティ・ニュージーランドによって2019年から発行されている

Kiwiアクセスカード

ニュージーランドの識別番号制度

IRD（内国歳入庁）番号[4]

- ニュージーランド国内の税制を所管しているIRD（内国歳入庁）から発行される識別子であり、主に納税管理に使用され、銀行口座の開設や就労の際に必要となる
- 納税者である個人（自然人）と、企業及び組織（法人）向けに異なるIRD番号が必要となる

NHI（国民健康指数）番号[5]

- ニュージーランド保健省が所管する、国民が医療サービスを利用する際に必要となる識別子であり、出生時、もしくは医療サービスの利用時に付番される
- 個々の患者の識別と医療記録の管理に使用されるとともに、国家予防接種登録簿（NIR）などのデータベースへ医療従事者がアクセスする際に利用される

NSN（全国学生番号）[6]

- ニュージーランド教育省の所管する、全ての学生に対して付番される一意の識別子であり、ニュージーランドで就学する学生の識別・出席の管理、成績の記録、統計目的などで利用される

出所）
1 https://www.nzta.govt.nz/driver-licences/getting-a-licence/identification
2 https://kiwiaccess.co.nz/
3 https://www.dia.govt.nz/identity-check
4 https://www.ird.govt.nz/managing-my-tax/ird-numbers
5 https://www.health.govt.nz/our-work/health-identity/national-health-index/nhi-information-health-consumers/national-health-index-questions-and-answers#bused
6 https://www.education.govt.nz/school/managing-and-supporting-students/national-student-number-nsn-for-schools/

統一的な識別子付与に対する制限

ニュージーランドではプライバシー法（2020年に改正）によって、個人に対して機関を横断した統一的な識別子を付与することを制限している[1,2]

1993年プライバシー法における固有識別子の原則

- 機関は、機関がその機能の1つまたは複数を効率的に実行できるようにするために、**その識別子の割り当てが必要でない限り、個人に一意の識別子を割り当ててはならない**
- 政府機関は、2007 年所得税法のサブパート YB の意味する関係者である場合を除き、**その機関の知る限り、別の機関によってその個人に割り当てられた一意の識別子を個人に割り当ててはならない**

2020年プライバシー法における固有識別子の原則

- 機関（A）は、A がその機能の1つまたは複数を効率的に実行できるようにするために**その識別子が必要な場合にのみ、その運用で使用するために一意の識別子を個人に割り当てることができる**
- A は、A の知る限り、**別の機関（B）によってその個人に割り当てられた一意の識別子と同じ一意の識別子を個人に割り当てることはできない**
    - A と B は、2007 年所得税法のサブパート YBの意味における関連者である
    - 一意の識別子は、統計または研究目的で A によって使用され、他の目的では使用されない

出所）
1 https://www.legislation.govt.nz/act/public/1993/0028/latest/DLM297038.html
2 https://legislation.govt.nz/act/public/2020/0031/latest/LMS23376.html

現在に至るまでの変遷

ニュージーランドでは、行政サービスの利用を効率化するためのRealMe、Identity Checkなどが提供されているほか、2018年からはDigital Identity Programmeが実施され、デジタルIDシステムやトラストフレームワークといった、全体的なIDガバナンスの構築に向けた取り組みを実施している

RealMe（2011～）[1]
ニュージーランド内務省（DIA）の提供するデジタルIDサービスであり、単一のアカウントをによる複数の公共サービスへのログインや、検証済みIDの作成が可能

2011

Digital Identity Programme（2018～2020）
ニュージーランド政府は、デジタルIDに新しいテクノロジーを活用し、市民のニーズと期待に応えるために適切な規則と環境を設定する方法を2018年から2年間調査した。
その結果、トラストフレームワーク法案や、デジタルIDシステムの推進といった取り組みが行われることとなった

2018

Identity Check（2022～）[2]
DIAによって開発され2022年9月からパイロットが行われているID検証サービスであり、オンラインの身元証明において、入力された個人情報を政府データベースの情報と比較することで検証を行う

2022

出所）
1 https://www.realme.govt.nz/privacy/identity-verification-service-privacy-statement/
2 https://www.dia.govt.nz/identity-check

The Digital Strategy for Aotearoa

ニュージーランド政府の主要なDX戦略である「The Digital Strategy for Aotearoa（マオリ語でニュージーランドの意）」[1]の３つの戦略テーマの一つである「政府・企業のデジタル信頼性の向上」において、デジタルアイデンティティ・トラストフレームワークの策定が重点的取り組み事項となっており、デジタルアイデンティティ・トラストフレームワークの策定法案は、2021年12月に政府で承認された

The Digital Strategy for AotearoaにおけるデジタルIDの取り組み

The Digital Strategy for Aotearoa（政府のDX政策方針）

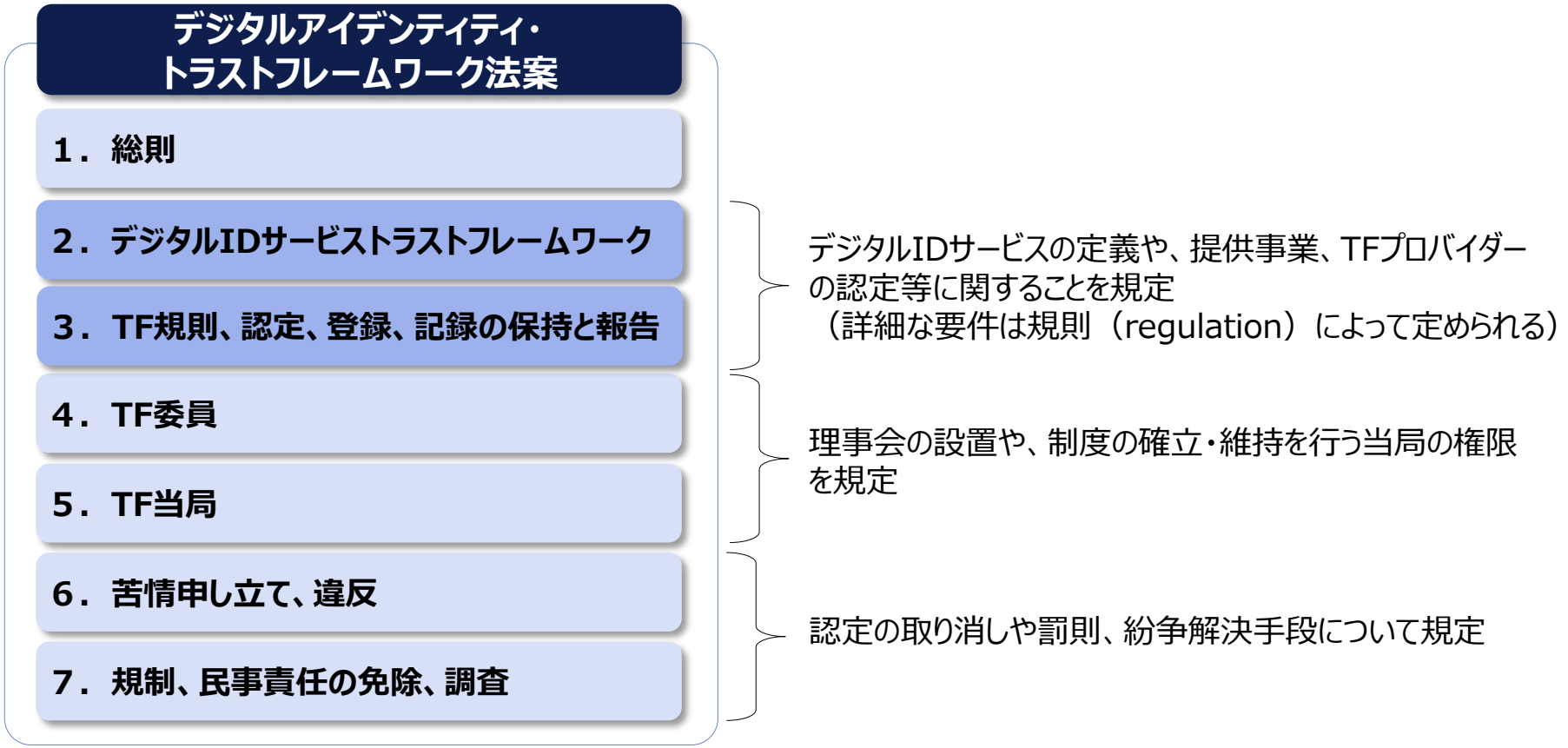
戦略的テーマ		
	①信頼：政府・企業のデジタル信頼性の向上	政府機関向けのクラウド導入
		サイバーセキュリティ戦略
		デジタルアイデンティティ・トラストフレームワーク
		⋮
	②包摂：デジタル・インクルージョンの向上	高齢者へのデジタルスキル教育・サポート
		農村部のデジタル接続
		⋮
	③成長：デジタル・イノベーション、生産性向上	

出所）
1 https://www.digital.govt.nz/dmsdocument/237~the-digital-strategy-for-aotearoa/html#focus-areasmahi-tika-trust

デジタルアイデンティティ・トラストフレームワーク法案

デジタルアイデンティティ・トラストフレームワーク法案は、ニュージーランドにおけるデジタルIDサービスの法的な枠組みを規定するものであり、デジタルIDサービスの定義などを定めるほか、法律の認定を受けた信頼できるデジタルIDサービス事業者を「TFプロバイダー」として定義・登録するなどの仕組みを定めている[1]

デジタルアイデンティティ・トラストフレームワーク法案の構成

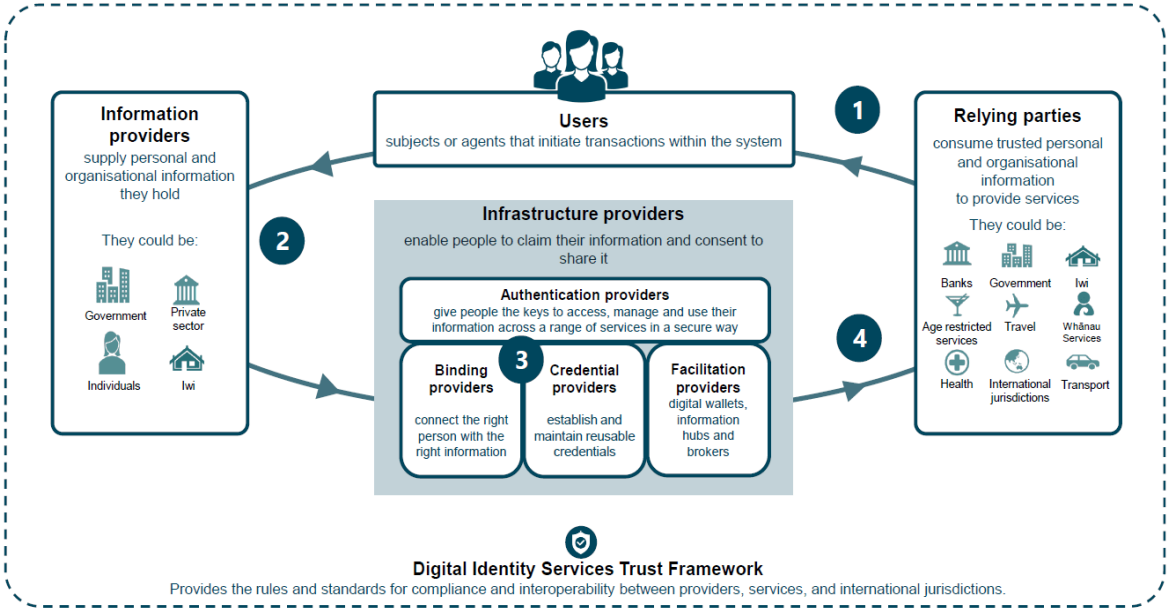


出所)
1 https://www.parliament.nz/en/pb/bills-and-laws/bills-proposed-laws/document/BILL_116015/digital-identity-services-trust-framework-bill

デジタルIDシステム

政府はデジタルIDサービスにおける各ステークホルダー（個人やサービスプロバイダー）の定義、役割、相互作用について示したエコシステムとして、デジタルIDシステムを提案している[1]

ニュージーランドにおけるデジタルIDシステム



① サービスプロバイダー（Relying Party）はユーザーがサービス利用するための要件（特定の情報）をユーザーに伝える。ユーザーは自身の情報を（安全な方法で）共有されることをサービスプロバイダーに許可する

② ユーザーの情報を保持する情報提供者（information providers）（政府、銀行、個人、電力会社など）がユーザーに情報を提供する

③ 各インフラストラクチャプロバイダーが連携し、バインディング（情報と個人（ID）の紐づけ）、認証プロセスを通じて、ユーザーが安全かつ確実に、情報の要求とシェアを可能にする

④ ファシリテーションプロバイダーにより、ユーザーが資格情報（クレデンシャル）をサービス事業者に共有し、サービスにアクセスすることや、トランザクションの完了作業を支援する

出所)
1 https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/digital-identity-system/

政府提供のデジタルIDサービス

ニュージーランドの政府機関の提供するIDサービスとしては、内務省の提供するRealMe、Identity Checkがあり、連携する行政･民間のサービスでログイン及び本人認証、ID情報の検証に使用されている

政府機関の提供するデジタルIDサービス

RealMe[1]

- ニュージーランド内務省（DIA）の提供するデジタルIDサービスであり、2011年から稼働している。
- 提供サービスは、単一のアカウントを作成することで、複数の公共サービスへのログインを可能にするRealMe Loginと、政府のデータベースと照合された検証済みのデジタルIDを作成するRealMe Verifiedの二つに分かれている

Identity Check[2]

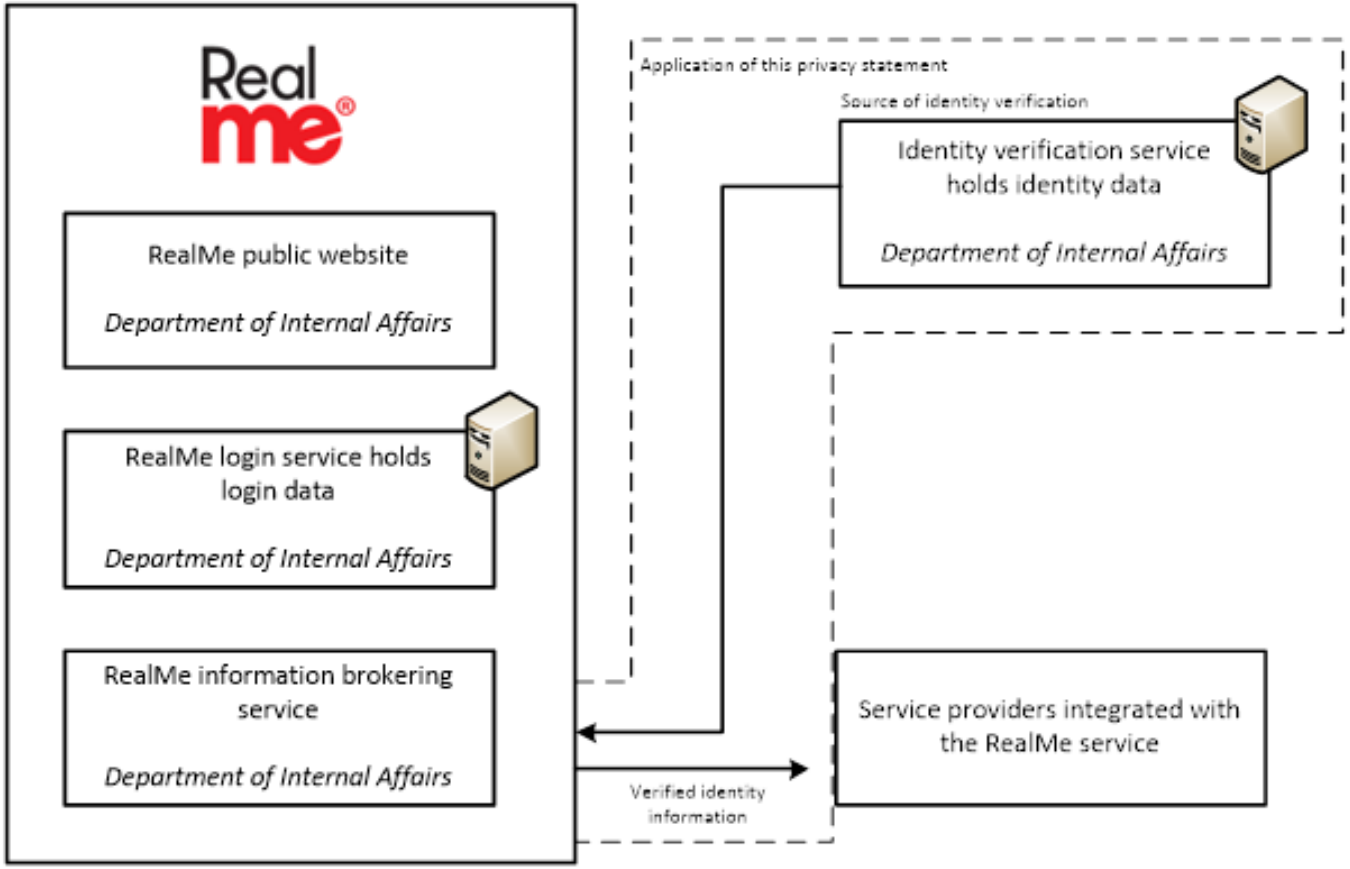
- DIAによって開発され2022年9月からパイロットが行われているID検証サービスであり、オンラインの身元証明において、入力された個人情報を政府データベースの情報と比較することで検証を行う
- RealMeの検証済みID作成と同じ仕組みを利用しており、オンラインサービスの身元証明プロセスの中で、IDチェック用のページにリダイレクトされることで動作する
- パイロットとして、Kiwiアクセスカードの申請にはIdentity Checkが活用されている

出所）
1 https://www.realme.govt.nz/privacy/identity-verification-service-privacy-statement/
2 https://www.dia.govt.nz/identity-check

RealMeのデータ管理主体

RealMeで運用されるログインデータやアイデンティティデータは政府（Department of Internal Affairs : DIA）がデータソースを保持しており、政府主導での管理がなされているものとみられる[1]

RealMeのサービスと保持するデータの関係図



出所)
1 https://www.realme.govt.nz/privacy/identity-verification-service-privacy-statement/

3.1 詳細調査結果：共通識別番号・デジタルIDに関する政策動向

3.1.4アジア（シンガポール、インド）における調査結果

現在に至るまでの変遷

シンガポールにおいては、英国統治下の1948年に制定された緊急登録法を契機として国民の登録・管理が始まり、1965年の国民登録法成立以降一意の識別番号が国民に対し付番されている。1966年以降は国民登録システムに基づくIDカード（NRIC）の発行が始まり、1991年には現在のクレジットカードサイズのIDカードに更新され国民の共通識別手段として継続して用いられている[1,2,3]

緊急登録法（1948年）
英国統治下で不法移民に対する取り締まりのため、12歳以上の全ての居住者を登録し、身分証明書を発行した

1948

1966

国民登録法（1965年～）
1965年のシンガポール独立後、より詳細な人口統計を記録するための再登録が始まり、共通のIDカードとしてNRICが発行される

1966年以降発行されていた身分証明書がクレジットカードサイズのIDカードに更新され、現在の形になる

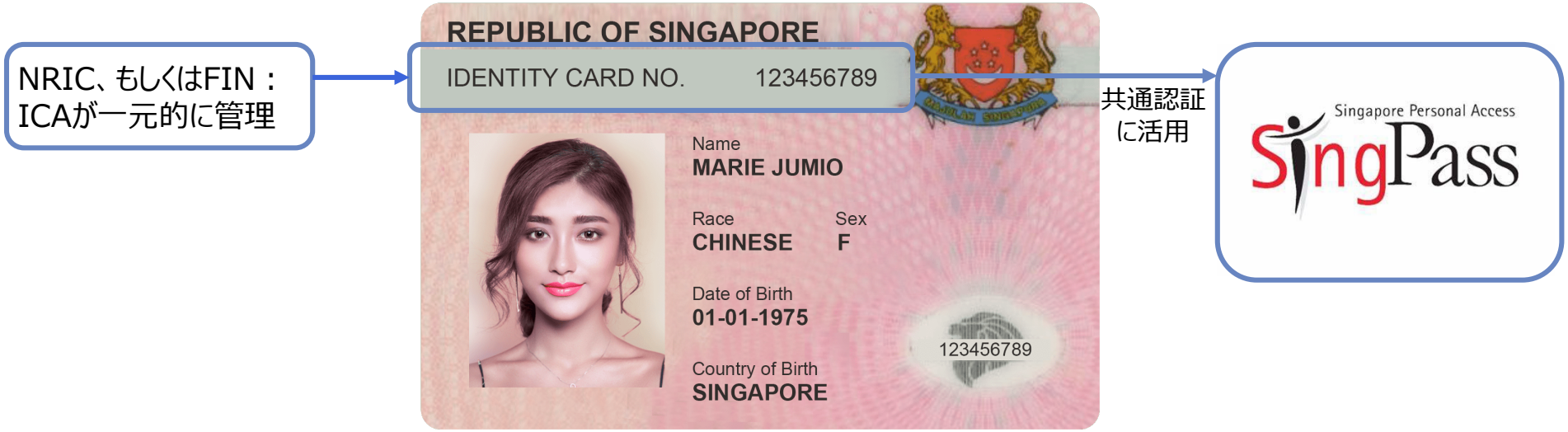
1991

出所）
1 https://eresources.nlb.gov.sg/history/events/07ffb260-e535-4dbb-a946-fa3403f47e72
2 https://www.ica.gov.sg/about-us/our-history/faf
3 https://www.dreamimmigrationsg.com/singapore-nric-number-national-registration-identity-card

NRIC、FIN

- シンガポールでは、シンガポール入国管理局（ICA）が管理する個人識別番号カード（非ICカード）があり、国民および居住者の登録が義務付けられている
- 個人識別番号には、シンガポール国民および永住者向けの国民登録番号カード(National Registration Identification Card：NRIC)、および外国人居住者登録番号（Foreign Identification Number: FIN)の2種類があり、NRICが付与されている場合、シンガポール国民および永住者は15歳になった時点で、氏名、性別、生年月日、民族、住所、血液型、写真、指紋・虹彩等をICAに登録している
- NRICとFINを使用した政府の運営する共通認証システムとしてSingpassが2003年に導入されている[1,2]

ICA発行の個人識別カードの一例



出所）
1 https://www.ica.gov.sg/documents/ic/registration
2 https://www.jri.co.jp/MediaLibrary/file/report/jrireview/pdf/11717.pdf

現在に至るまでの変遷

シンガポールでは、政府機関ごとに異なっていたオンラインサービスの認証システムを統一するため、前述の国民識別番号を利用した認証システムであるSingpassが2003年より導入された。その後2018年にモバイルアプリであるSingpass Mobileが提供され、行政・民間の両分野でのデジタル認証に幅広く活用されている

Singpass[1]（2003年～）
政府機関のオンライン認証方法の統一のために2003年に導入された共通認証システムであり、当初は前述の個人識別番号とパスコードによって認証していた

2003

2018

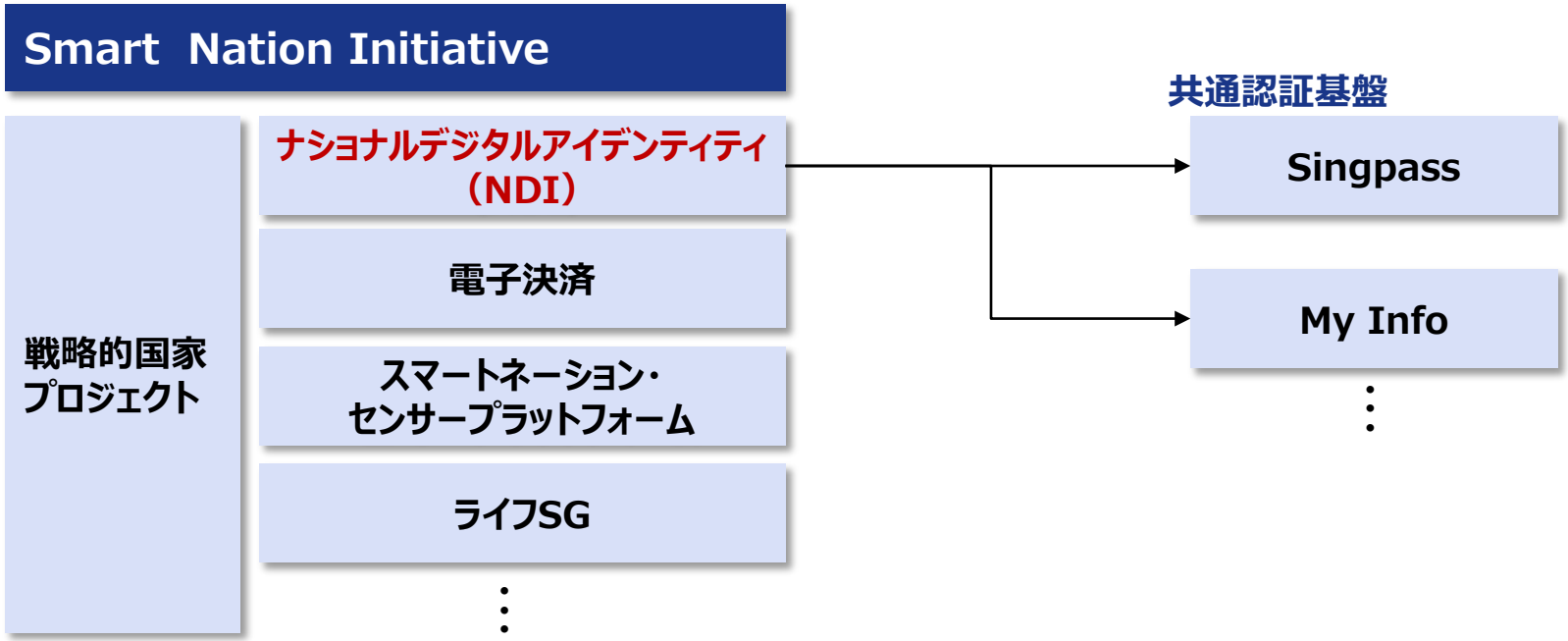
Singpass Mobile（2018年～）
政府技術庁 (GovTech)によって開発されたスマートフォンアプリであり、Singpassの認証を、スマートフォンアプリ上で指紋・顔認証・パスコードによって行うことができる。ID提示、ドキュメントの保管、電子署名など様々なサービスが利用できるようになっている

出所）
1 https://www.smartnation.gov.sg/media-hub/press-releases/singpass-factsheet-02032022

Smart Nation Initiative、NDI

- シンガポール政府は、テクノロジーによる国家の課題解決構想として、Smart Nation Initiativeを実行している。Smart Nation Initiativeによる課題解決を実現するための基盤として、戦略的国家プロジェクトを定めており、その中にはID管理に係るプロジェクトである「ナショナルデジタルアイデンティティ（NDI）」[1]が存在する
- NDIは国民が公共・民間のサービスを利用するための共通のデジタルIDスキームを創る取り組みであり、シンガポール政府技術庁（GovTech）によって推進されている。NDIの取り組みによる成果として、後述する共通認証基盤であるSingpass、個人情報の一元登録・認証サービスであるMy Infoなどが存在している

政府のDX政策方針

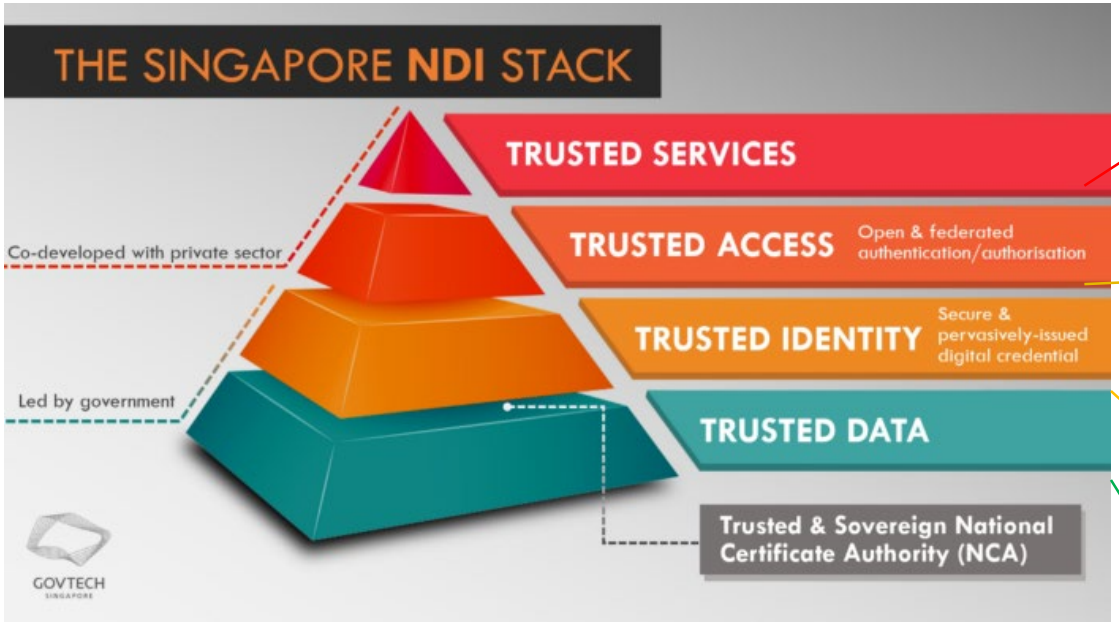


出所）
1 https://www.smartnation.gov.sg/initiatives/strategic-national-projects/national-digital-identity

NDI Stackのレイヤー構造

シンガポール技術庁（Govtech）は、NDIの取り組みをNDI Stackの概念によって構造化している。NDI Stackの中では、My Info、Singpassなどの信頼性の高いデータとIDを提供するTrusted Data、Trusted Identityレイヤーを基盤として、その上に信頼性ある認証方式とサービス統合を行うAPIといったTrusted Access、Trusted Serviceレイヤーを構築しており、政府主導の取り組みを基盤として民間部門と連携した認証・サービスを提供していることが分かる[1,2,3]

NDI Stackの構造



Trusted Service
公的機関、民間企業にAPIを提供し、サービス統合を可能にする

Trusted Access
法律や、Singpass Mobileの多要素認証のような信頼性ある認証技術標準によって公的機関・民間企業ASP（アプリケーションサービスプロバイダ）の信頼性を担保する

Trusted Identity
Singpassによって、高い保証を備えた基本的IDスキームを提供する
現在は政府中心の中央集権型だが、分散型モデルを検討する

Trusted Data
My Infoによって、信頼できるデータソースを市民・企業に対して提供する

：民間との共同領域　　：政府主導の領域

出所）
1 https://medium.com/ndi-sg/stack-x-webinar-national-digital-identity-stack-introduction-to-ndi-34b5dbed9565
2 https://www.globalgovernmentforum.com/wp-content/uploads/Singapore-NDI-slides_comp.pdf
3 https://www.tech.gov.sg/media/technews/giving-every-citizen-a-unique-digital-identity

Singpassの概要

- Singpass[1]は政府機関のオンライン認証方法の統一のために2003年に導入された共通認証システムであり、当初は前述の個人識別番号とパスコードによって認証していたが、2018年に政府技術庁（GovTech）によってSingpassの認証をスマートフォンアプリ上で行うことのできるSingpass Mobileを導入した
- Singpass MobileによってSingpassの認証基盤を活用したID提示、ドキュメントの保管、電子署名など様々なサービスが利用できるようになっている。またSingpass Mobileのサービス用APIは企業向けに公開されており、開発者はそれを活用することによって自社のサービスとSingpassの認証基盤を統合することができ、海外企業のAPI統合実績も存在する

Singpass Mobileによって利用できるサービスの例

サービス	概要
デジタルIC	• Singapass Mobileアプリによって、ユーザーのデジタルIDカードを表示することができる
ドキュメントウォレット	• Covid-19の検査証明などの政府発行文書をポータルから入手し、それを表示することができる • 対応する文書の種類は順次拡大予定
電子署名	• 電子文書に表示されているQRコードを読み取ることによって、Singpass認証による電子文書への署名が可能になる
My Info（My Info Bussiness）	• Singapass認証によって共有する範囲を指定・同意したうえで、政府機関と個人情報を共有することができ、サービス利用の都度個人情報を入力する必要がなくなる • 民間企業向けにはMy Info Bussinessが存在し、官民合わせて800以上のデジタルサービスがMyInfoを通じて個人情報を取得し、手続き時間を80%短縮しているとされる
SG verify	• 相手から提示されたQRコードを読み取り、本人確認に必要な情報を同意のうえ相手に提供（送信）できる • 2019年の個人データ保護法の改正により、企業の個人識別番号の収集が禁止されたため、導入された

出所）
1 https://www.smartnation.gov.sg/media-hub/press-releases/singpass-factsheet-02032022

Singpassの活用事例・導入効果

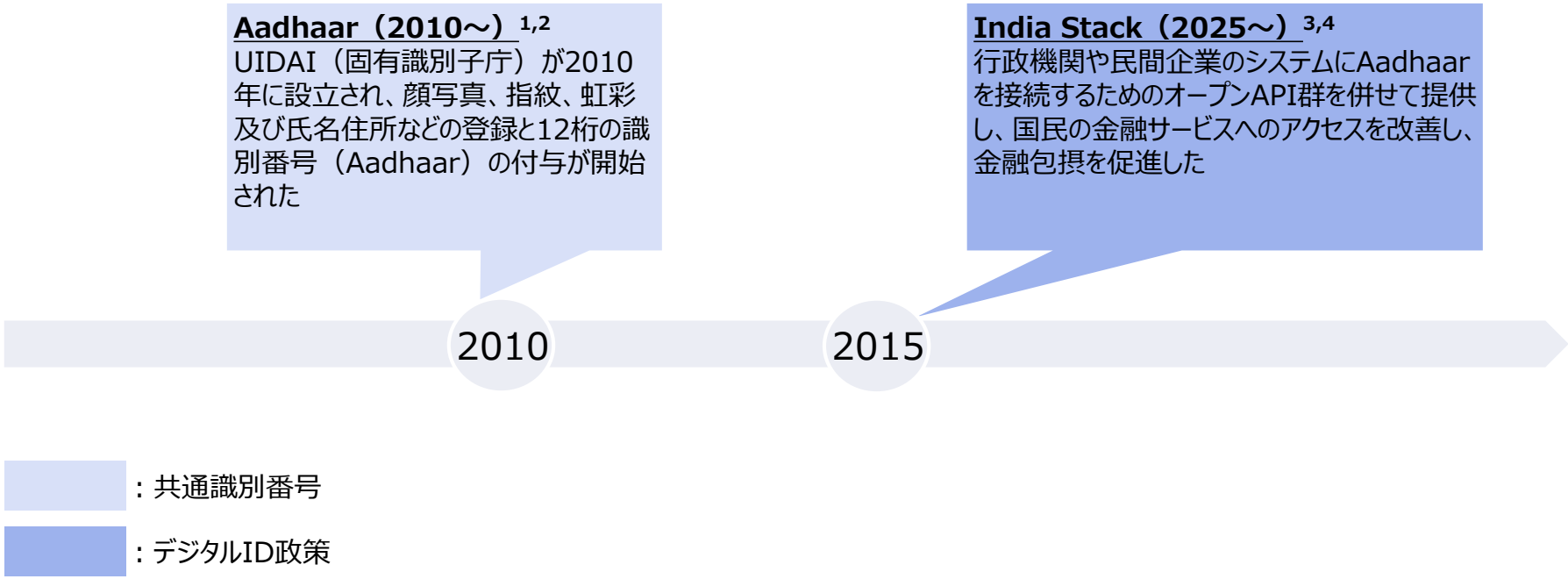
Singpass[1]のサービスAPIを基軸とした各種認証サービスは以下のような活用事例で成果を示している

Singpassのサービス API	活用事例の概要・導入の効果
MyInfo	• My Infoによる個人情報の共有は政府機関、民間企業の800以上のサービスで利用可能となっており、My Infoの利用によってユーザーの申請時間が平均で最大80%短縮され、データ品質の向上により、企業側の承認率も最大15%向上した。1日200,000件の取引が発生している • 個人による利用の他に、企業向けのMy Infoビジネスでは、企業のプロファイルや財務状況などの情報を共有することにより、ビジネス助成金の申請などの130以上の公共サービスに接続し、手続きを簡略化できる
SG verify	• SG VerifyによるQRコードを用いた非接触での対面の本人確認、個人情報の転送は、病院での新規患者登録、トレーニングプロバイダへの対面登録プロセスで利用されている
SafeEntry	• コロナ禍において重要なサービス拠点への物理的なチェックインにSingpassのSafeEntryAPIを利用し、NRIC、FIN、携帯電話番号などのエントリーした個人の記録を行っている
顔認証	• 顔認証APIは、納税・ビジネスサービスセンターや中央積立基金などの政府系サービスセンターへのログインに試験的に運用されており、以前は文書で平均10分かかっていた身元確認プロセスが数秒以内に完了するようになるなどの効果が確認されている • スマホをもっていない者でも利用できるため、デジタルインクルージョンを推進している

出所)
1 https://www.smartnation.gov.sg/media-hub/press-releases/singpass-factsheet-02032022

現在に至るまでの変遷

インド政府は、顔写真、指紋、虹彩及び氏名住所などの登録によって12桁の識別番号（Aadhaar番号）を国民に付与し、Aadhaarを基礎とした国民ID基盤であるIndia Stackを構築している。Aadhaar以前はインド国民の約17%しか銀行口座を保有しておらず、金融アクセスの格差が社会問題となっていた

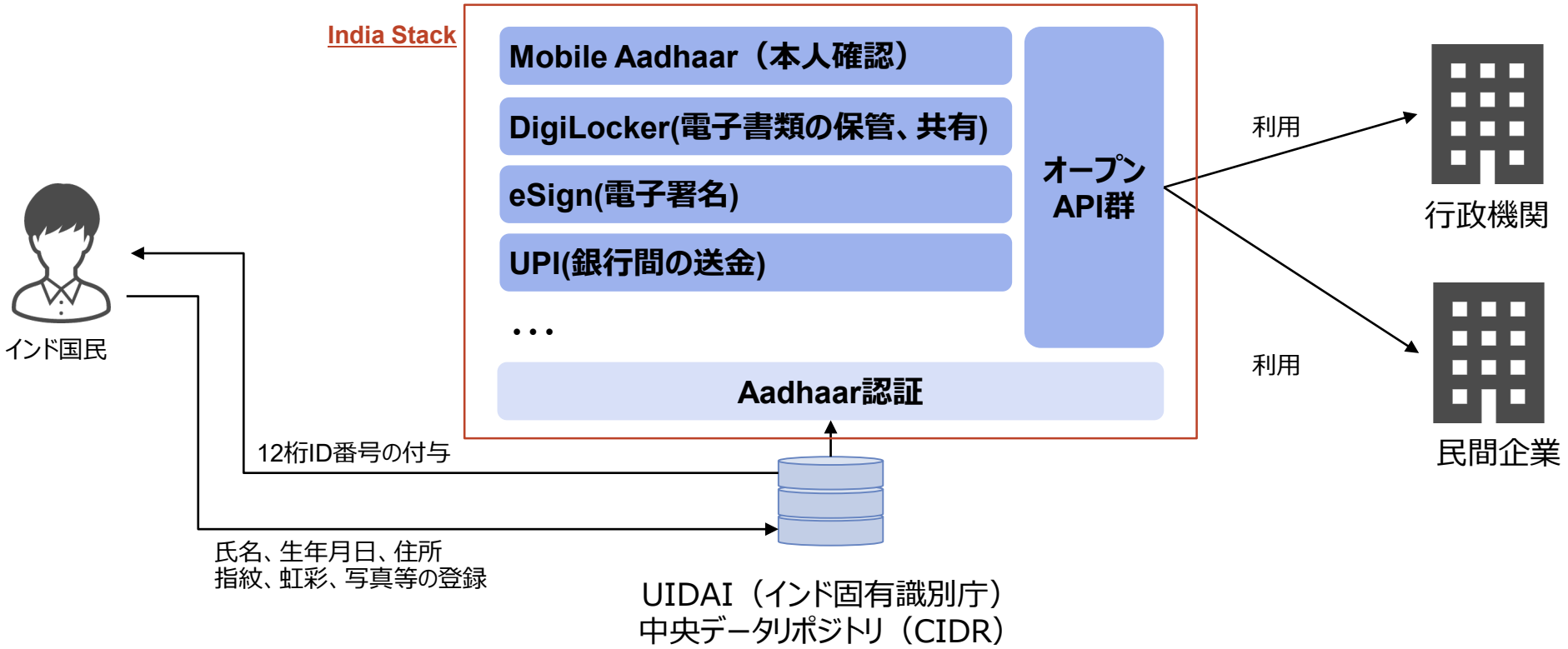


出所）
1 https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar.html
2 https://www.dqindia.com/exploring-application-of-blockchain-quantum-for-aadhaar-uidai-ceo/
3 https://info.thoughtworks.com/rs/199-QDE-291/images/India-Stack-DrivingTransformation-TWLiveIndia2019.pdf
4 https://indiastack.org/data.html

Aadhaar、India Stack

インドではAadhaarを基盤として、行政機関や民間企業のシステムにAadhaarを接続するためのオープンAPI群を併せたIndia Stackと呼ばれるID基盤が政府によって提供され、広範に活用されている
2019年時点でAadhaarにはインド国民の95%が登録しており、India StackのAPIにはAadhaarを活用して本人確認を行うMobile Aadhaar、電子文書の保管･共有を行うDigiLocker、電子署名を可能にするeSignなど多数存在している[1,2]

AadhaarをIndia Stackの概要



出所）
1 https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar.html
2 https://www.dqindia.com/exploring-application-of-blockchain-quantum-for-aadhaar-uidai-ceo/

India Stackのレイヤー構造

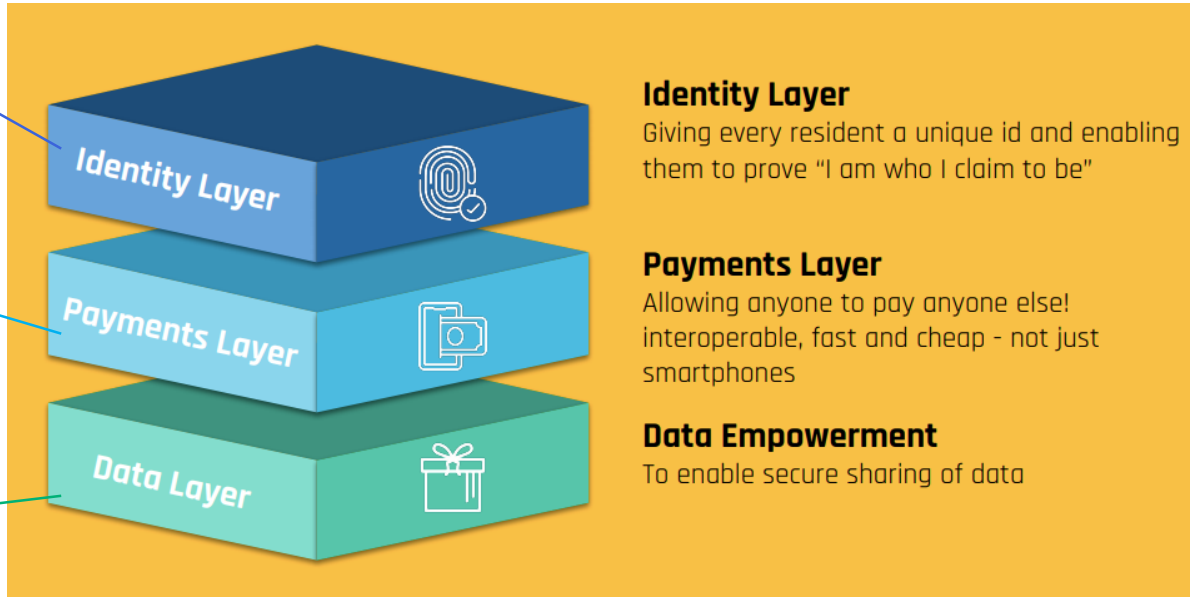
インド政府は国民ID基盤であるIndia Stackを3つのレイヤーに分けて概念を整理している。Aadhaarを基盤として、個人の識別・認証を可能とするIdentity Layer、金融取引を可能とするPayments Layer、個人データの保管・共有を可能とするData Empowermentからなり、Aadhaar認証を基盤としたAPIの活用により、デジタル経済にインド国民を包摂する構造を持っていることが確認できる[1,2]

India Stackの構造

Identity Layer
個人を識別・認証することを可能にする。Aadhaar認証やeKYC、電子署名を行うAPIが該当する

Payments Layer
Aadhaar認証を基盤として電子的な金融取引・社会保障給付を可能とする。APBやUPIなどの送金・振込APIが該当する

Data Empowerment
個人データの安全な管理・共有を可能とする。電子文書を保管するDigilockerなどのAPIが該当する



出所）
1 https://info.thoughtworks.com/rs/199-QDE-291/images/India-Stack-DrivingTransformation-TWLiveIndia2019.pdf
2 https://indiastack.org/data.html

Aadhaarの懸念点

Aadhaarはインド国民の戸籍管理や住民登録が不十分であった環境に対して、IDを使用する経済活動に国民全体を包摂する役割を果たし広範に利用されているものの、単一のデータベースで大量の個人情報・生体情報を保持しているなどの点で、以下の様な懸念が生起・指摘されている

プライバシー権の問題[1,2]

- Aadhaarによる個人情報・生体情報の収集は、導入以降国民のプライバシー権を侵害しているという批判に晒され、2018年の最高裁判決で民間企業による利用が制限されたものの、2019年の大統領令及び法改正で同意の基であれば民間での利用が再開されることとなった

セキュリティの問題[3]

- Aadhaarを巡るIDの取り扱いやセキュリティ体制の不備から、導入以降外部の不正アクセスや行政機関が誤ってAadhaar情報を公表するなどして、個人情報流出の問題が生起している

実質的登録義務化の問題[4]

- 社会保障給付金などの福祉プログラムを受けるためにAadhaar番号が必須であり、その利便性の高さから、Aadhaarへの登録が実質的に義務化（強制）されているという批判がある

出所）
1 https://www.theweek.in/news/india/2018/09/26/aadhaar-through-the-years-quick-timeline.html
2 https://www.afpbb.com/articles/-/3140401
3 https://www.newsweekjapan.jp/stories/world/2017/10/13-12_3.php
4 https://www.dailymail.co.uk/indiahome/indianews/article-4993558/Death-11-year-old-India-sparks-debate-tying-welfare-identity-card.html

3.1 詳細調査結果：共通識別番号･デジタルIDに関する政策動向

3.1.5共通識別番号･デジタルIDの政策動向に関する総括

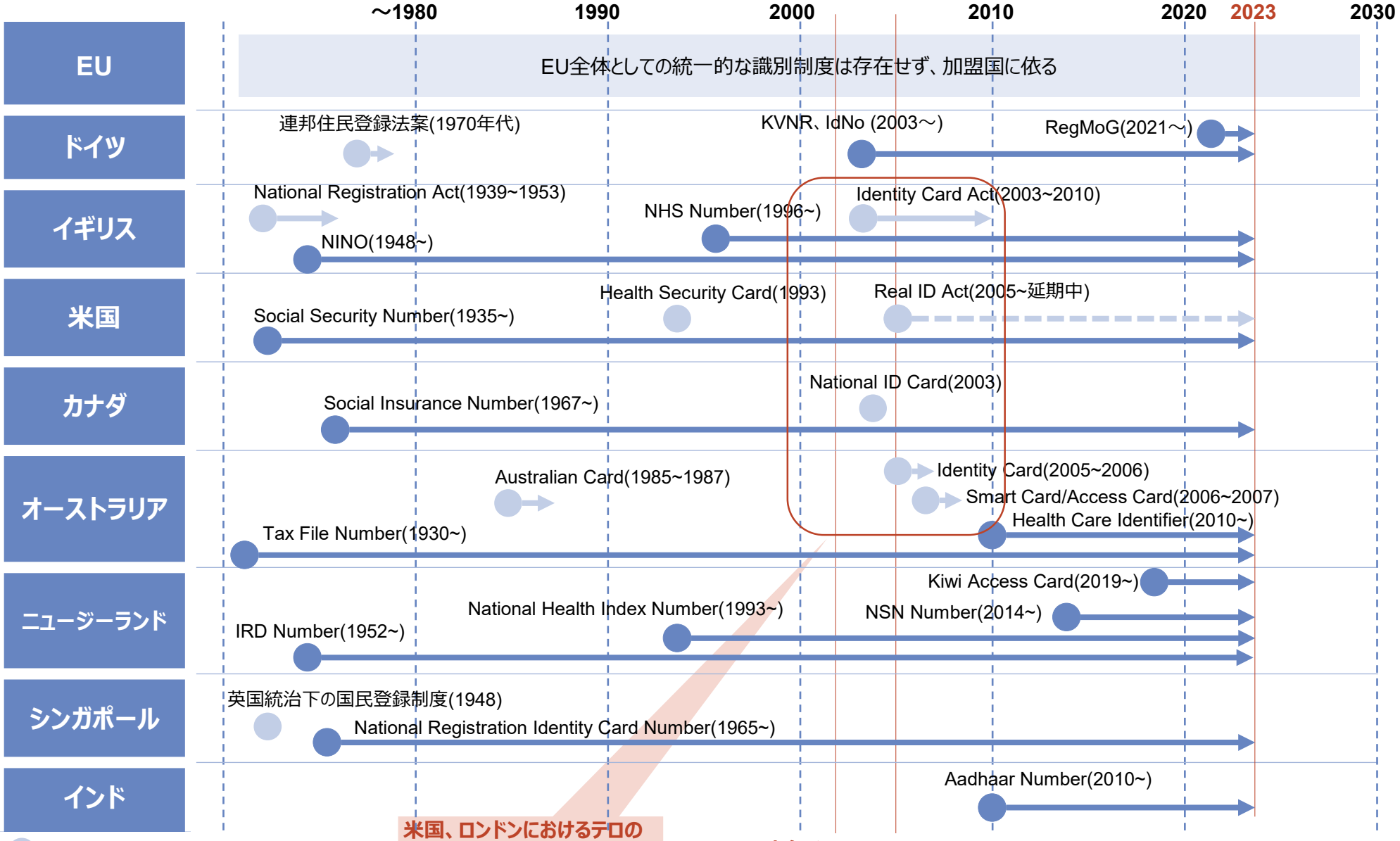
3.1.5 共通識別番号・デジタルIDに関する政策動向に関する総括

共通識別番号の導入状況

- 調査対象国のうち**シンガポール、インドにおいては全国民を対象とした統一的な識別制度が存在**している
- その他の国においては過去存在したか、もしくは検討されたもののプライバシーに関する懸念から廃止されており、**目的・分野別に異なる識別子を使用**している

国・地域		政府主導の共通識別番号の導入状況
欧州	EU	• EU全体としての**統一的な識別制度は存在せず、加盟国に依る**
	ドイツ	• **行政分野ごとに異なる個人識別番号を用いている**が、2021年4月に公布された登録現代化法に基づき一定の制約の元で**租税識別番号を行政分野横断で活用できる仕組みの整備**が進められている
	イギリス	• 統一的な国民識別制度であるNational ID Cardが過去存在した。またIdentity Card Actが検討されたことがあるものの実現せず、NINO、NHS Numberなど**社会保障、医療といった目的別に異なる識別番号を使用**している
北米	米国	• 従来から存在する**社会保障番号（SSN）が広範に個人認証に利用され、行政・民間サービスの双方で利用範囲が拡大**された • 社会保障番号に代わる**統一的な共通識別番号を模索しているものの、未だ実現してはいない**
	カナダ	• 社会保険番号が国民識別番号として活用されているが、その使用用途は制限されており、身元証明は運転免許証やパスポート等の証明書が使用されている • **統一的な国民IDカードを発行する制度は一時期検討されたものの、プライバシーの侵害等懸念が表明され実現していない**
オセアニア	オーストラリア	• 米国の社会保障制度や日本のマイナンバーカード、シンガポールの国民番号に該当するような国民共通番号制度は現状存在しないため、Health Care identifierやTax File Numberなど**用途に応じて複数の番号を使い分けている** • 過去に**国民IDカードの実現を目指した提案があったが、いずれも批判を受けて失敗**している
	ニュージーランド	• 一般的な運転免許証、パスポート等のほか、アルコールの販売・購入において年齢を証明するKiwiアクセスカードなどが識別手段として用いられる • 識別番号としてはIRD番号、NHI番号、NSNなど複数存在しており、それぞれ**税務、医療、教育といった目的別に使用**されている。統一的な識別子の付与はプライバシー法によって制限されている
アジア	シンガポール	• 英国統治下の1948年に制定された国民登録制度を契機として登録・管理が始まり、**1965年の国家登録法成立以降、一意の識別番号が国民に対し付番**されている • 1966年以降国家登録システムに基づくIDカード（NRIC）の発行が始まり、1991年には現在のクレジットカードサイズのIDカードに更新され、国民の共通識別手段として継続して用いられている
	インド	• 2010年から顔写真、指紋、虹彩及び氏名住所などの登録と**12桁のID番号（Aadhaar番号）を付与**し、国民ID基盤であるAadhaarを構築している

共通識別番号の導入状況：各国の変遷（補足）



：廃止されたか実現していないもの

：現在も利用されているもの

デジタルID政策の状況①

- 調査対象国のうちシンガポール、インドにおいては既存の統一的な共通識別子を基盤とした広範なデジタルIDサービスを政府が提供している
- その他の国においては政府が主導してトラストフレームワークを策定することにより、民間IDプロバイダーに対し認定を付与して公共サービス・民間におけるオンライン認証に活用している

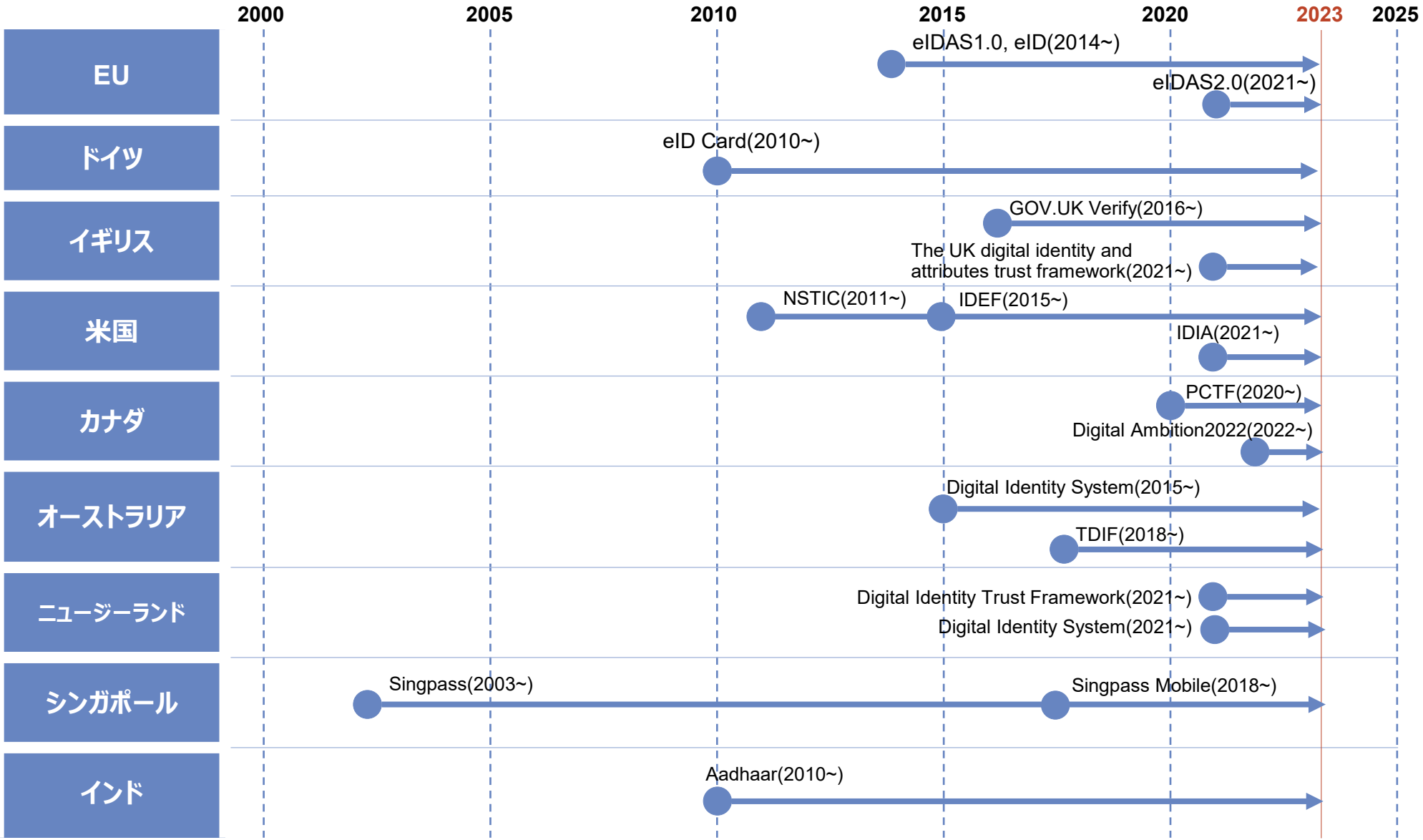
国・地域		デジタルID政策の状況
欧州	EU	• EU加盟国間で公共オンラインサービスへのアクセス時に本人確認を行うことのできるデジタルIDであるeIDがeIDASによって2014年から規定されている • 2021年のeIDAS改正提案（eIDAS2.0）においてモバイルウォレット（EUDIW）の提供を加盟国に義務付け、eIDを含めた属性証明・公的文書を格納・利用可能にすることでフレームワークの改善を図っている
	ドイツ	• eIDカードが2010年から導入されており、16歳以上のドイツ国民に対して取得が義務付けられている。2017年の連邦法改正により、eIDカードの発行時に電子署名機能を付与することが可能となった
	イギリス	• 政府の認定を受けたIdPが発行するIDを活用した公共サービスアクセス時の本人認証の仕組みであるGOV.UK Verifyを2016年5月に本格運用を開始したが、事業者の離脱が相次ぎ2023年に廃止予定である • 2021年にThe UK digital identity and attributes trust frameworkを策定し、トラストフレームワークを採用する機関の間でデジタルIDを相互運用できるよう、一連のルールを規定している
北米	米国	• 2011年にホワイトハウスの発表したNSTICに基づき、そのビジョンであるIdentity Ecosystemを規定するとともに、トラストフレームワークとしてIDEFを策定した • 連邦政府機関がデジタルIDサービスを実装する際のガイドラインとしてNIST SP800-63を策定し、官民問わず多くの組織から参照されている • 2021年に、デジタルIDのインフラ整備を進めるための超党的な法案としてIDIAを提出し、現在審議中である。法制化されれば、連邦政府は官民協力のもと、各種施策の実施を求める予定である
	カナダ	• 政府・民間企業から構成される非営利組織であるDIACCがカナダの官民組織がデジタルアイデンティティを安全に活用するためのガバナンスモデルとしてPCTF（Pan-Canadian Trust Framework）を策定している • カナダの今後3年間のデジタル戦略計画であるDigital Ambition 2022において既存の州のプラットフォームと統合された連邦デジタルIDプログラムに取り組むと発表した

デジタルID政策の状況②

- 調査対象国のうち**シンガポール、インドにおいては既存の統一的な共通識別子を基盤とした広範なデジタルIDサービスを政府が提供**している
- その他の国においては政府が主導して**トラストフレームワークを策定することにより、民間IDプロバイダーに対し認定を付与**して公共サービス・民間におけるオンライン認証に活用している

国・地域		デジタルID政策の状況
オセアニア	オーストラリア	• 2015年から、政府のオンラインサービスにアクセスする際に安全な認証を行うための取り組みとして、**デジタルIDシステムを推進しており、それを支えるトラストフレームワークとしてTDIFを策定**している • TDIFはデジタルIDシステム内のプロバイダーとサービスに対する規則と標準を示したフレームワークで、米NISTのSP800-63Bを参考にDTA（デジタルトランスフォーメンション庁）主導で策定が進められ、2018年に公表された
	ニュージーランド	• **Digital Identity Trust Frameworkによって、デジタルIDサービスの法的な枠組みを規定**し、認定を受けた信頼できるデジタルIDサービス事業者を「TFプロバイダー」として定義・登録するなどの仕組みを定めている • 政府はデジタルIDサービスにおける各ステークホルダー（個人やサービスプロバイダー）の定義、役割、相互作用について示したエコシステムとして、デジタルIDシステムを提案している
アジア	シンガポール	• 政府機関ごとに異なっていたオンラインサービスの認証システムを統一するため、前述の**国民識別番号を利用した認証システムであるSingpassが2003年より導入**された • その後2018年にモバイルアプリであるSingpass Mobileが提供され、行政・民間の両分野でのデジタル本人認証に幅広く活用されている
	インド	• Aadhaarを基盤として、行政機関や民間企業のシステムに**Aadhaarを接続するためのオープンAPI群を含めた国民ID基盤であるIndia Stackが広範に活用**されている

デジタルID政策の状況：各国の変遷（補足）



デジタルID政策の状況：各国の変遷（補足）

	欧州			北米	
	EU	ドイツ	イギリス	米国	カナダ
～2010～	・eIDAS成立(2014年)	・身分証明書法施行により電子証明書を使った個人認証を実施(2010年)	・保守党・自由民主党連立政権への政権交代、Identity Card Actの廃止(2010年)	・NSTICの発表(2011年)	・財務省主導でthe Task Force for the Payments System Reviewを提言(2011~2012年) ・DIACCの設立(2014年)
2015～	・eIDAS施行(2016年)	・行政サービスオンラインアクセス改善のためオンラインアクセス法(OZG)施行(2017年) ・eIDカード法(eIDKG)施行によりEU加盟国、EEA締約国の非ドイツ国民もドイツ国内でeIDカードが利用可能に(2019年)	・GOV.UK Verifyの利用開始(2016年)	・国家サイバーセキュリティ強化委員会がID管理改善を含むレポートを発表(2016年) ・Covid-19流行下で補助金給付におけるなりすまし等ID詐欺の被害拡大(2019年)	
2020～	・eIDAS見直し、パブリックコメントの開始(2020年2月) ・欧州のデジタル化移行への目標を示したデジタルコンパス2030発表(2021年3月) ・eIDAS Evaluation Report 発出(2021年6月) ・eIDAS2.0立法提案(2021年6月)		・GOV.UK Verify の2023年廃止を発表(2021年2月) ・The UK digital identity and attributes trust framework アルファ版発表 (2021年2月) ・The UK DIATF ベータ版発表(2022年6月)	・IDIA立法提案(2021年6月)	・PCTF v1.0発表(2020年) ・Digital Ambition 2022の発表(2022年8月)

デジタルID政策の状況：各国の変遷（補足）

	オセアニア		アジア	
	オーストラリア	ニュージーランド	シンガポール	インド
～2010～	・AUSkeyの導入(2010年)	・RealMeの導入(2011年)	・Signpassの導入(2003年)	・Aadhaarの導入(2010年) ・最高裁による、社会保障給付の為のAadhaar登録義務化取り止め命令(2014～2015年)
2015～	・Digital Idenity Systemの開始（2015年） ・DTAがTrusted Digital Identity Framework（TDIF）発表（2018年） ・AUSkeyの廃止、myGovIDへの統合(2019年) ・APCがTrustID Framework発表(2019年)	・DIAの主導でDigital Identity Programmeによる調査の実施（2018～2020年）	・My Infoの導入(2016年) ・Singpass Mobileの導入(2018年)	・Aadhaar 法成立(2016年) ・サービス提供等にあたりAadhaar番号提供の強制は違法とする最高裁判決(2019年)
2020～	・運転免許証・職業資格等のデジタル資格情報をDigital Idenity System に含めることに連邦政府・州・準州で合意(2023年)	・Digital Identity Trust Frameworkの立法提案(2021年) ・The Digital Strategy for Aotearoaの発表(2022年8月)	・sgIDの開発(2020年)	・Aadhaar改善の取り組み(Aadhaar2.0)(2021年)

デジタルID政策の状況ー共通識別番号を使用したデジタルIDサービス（補足）

- **調査対象国のうちシンガポール及びインドは、統一的な共通識別番号を基盤としたデジタルIDサービスであるSingpass、Aadhaarを提供している**
- **両サービスは認証基盤と他組織のシステムを接続するためのAPIの公開により、認証、ドキュメントの保管・提示、電子署名といった多様なサービスをワンストップで利用可能にしているが、中央集権的な仕組みからプライバシー等に係る懸念が生じている**

	Singpass	Aadhaar	My Gov ID（比較）
所管	シンガポール政府技術庁（GovTech）	インド政府固有識別子庁（UIDAI）	・オーストラリア税務局 ・デジタルトランスフォーメーション庁
導入年度	Singpass：2003年 Singpass Mobile：2018年	2010年	2019年
使用している共通識別子	シンガポール国民に対して付番されるNRIC番号、及びFIN（外国人居住者が対象）を利用することによって利用できる	インド国民に対して顔写真、指紋、虹彩及び氏名住所などの登録とともに付与されるID番号であるAadhaar番号によって利用できる	メールアドレス、パスポート、運転免許証、ビザなどにより登録する
概要・提供サービス	• Singpassを認証基盤としてモバイルアプリであるSingpass Mobileが提供され、Singpassの認証基盤を活用したID提示、ドキュメントの保管、電子署名など様々なサービスが利用できるようになっている • Singpass Mobileのサービス用APIは企業向けに公開されており、開発者はそれを活用することによって自社のサービスとSingpassの認証基盤を統合することができる。海外企業のAPI統合実績も存在する	• Aadhaarを基盤として、行政機関や民間企業のシステムにAadhaarを接続するためのオープンAPI群であるIndia Stackと併せて広範に活用されている • 2019年時点でAadhaarにはインド国民の95%が登録しており、India StackのAPIにはAadhaarを活用して本人確認を行うMobile Aadhaar、電子書類の保管・共有を行うDigiLocker、電子署名を可能にするeSignなど多数存在している	• 登録に使用する識別手段によりIDの強度が変わり、利用できるサービス範囲が異なる • myGovポータルで約13の政府サービスを利用できるほか、学生ポータル、税務申告、予防接種証明書アプリにおける認証などに使用できる • 民間企業向けのAPIの公開などは行っていない
懸念	2018年にSingpassがシステム障害により停止したことで、Singpassの法人版であるCorpassが停止し、一部の外国人労働者の労働許可証の発行が出来ず、帰国する事態となった	単一のデータベースで大量の個人情報・生体情報を保持していることによるプライバシー、情報流出の問題や、実質義務化の懸念がある	

3. 詳細調査結果：

3.1 共通識別番号・デジタルIDに関する政策動向

3.2 トラストフレームワークの策定状況

3.3 自己主権型／分散型アイデンティティに関する取り組み・ユースケース

トラストフレームワーク（再掲）

アイデンティティ情報の管理や利活用においては、デジタルIDの発行主体等のステークホルダーの定義、その果たすべき役割、セキュリティ基準などについて、参照すべき法律・規則等が定められており、一般的に「トラストフレームワーク」の名称で諸外国において策定・公表されている

調査対象としている諸外国のトラストフレームワーク

国・地域		フレームワークの名称
欧州	EU	Electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC（eIDAS）
	イギリス	The UK digital identity and attributes trust framework
	ドイツ	IDunion Network（Trust over IP Stack）
北米	米国	Identity Ecosystem Framework
		NIST-SP800-63
	カナダ	Pan-Canadian Trust Framework
オセアニア	オーストラリア	Trusted Digital Identity Framework
		Trust ID Framework
	ニュージーランド	Digital Identity Trust Framework
		Identity management standards
アジア	シンガポール	NDI Stack
	インド	India Stack

トラストフレームワーク調査方針

Trusted Web で定めている要件（合意形成やトレース等）を充足させるためには技術的なプロトコルでは充足できない箇所が散見される中、ガバナンスで補完する重要性がTrusted Web推進協議会等で議論されている中で再認識されている。以上を踏まえて、諸外国で定められているトラストフレームワークの構成・規定する内容について調査を行った。また、認証保証レベルを定めているものについては、政府機関、民間企業から多く参照されている米国のNIST SP 800-63[1]との比較を行った

調査対象のトラストフレームワーク

1	EU	Regulation 910/2014 : eIDAS（2.0）
2	ドイツ	IDunion Network
3	イギリス	The UK digital identity and attributes trust framework
4	米国	Identity Ecosystem Framework ：IDEF
5		NIST SP 800-63
6	カナダ	Pan-Canadian Trust Framework : PCTF
7	オーストラリア	Trusted Digital Identity Framework : TDIF
8		Trust ID Framework
9	ニュージーランド	Digital Identity Trust Framework
10		Identity management standards
11	シンガポール	NDI Stack
12	インド	India Stack

参考）1 https://learn.microsoft.com/ja-jp/azure/active-directory/standards/nist-overview

3.2 詳細調査結果：トラストフレームワークの策定状況

3.2.1 欧州（EU、ドイツ、イギリス）における調査結果

Regulation 910/2014 : eIDAS

2016年、EUの電子商取引に統一した基準を設けることを目的として Regulation 910/2014（eIDAS）が適用された。2020年に実施した初期影響評価とパブリックコメントのフィードバックを踏まえて2021年6月、eIDAS 2.0 への改定提案がされた。[1]eIDAS 2.0 では新たに「EUDIW」「リモート署名作成装置の管理」「電子アーカイブ」「電子台帳」「属性の電子証明」の項目が追加された他、「The commission shall/may」として各項目の要件や規則の整備を求めている

eIDAS 2.0 の構成要素

大項目	小項目	「The commission shall/may」	概要
総則	EUDIW	運用上の仕様と参照する技術要件 /認証基準リストの公開 /認証機関の基準 /通知フォーマットの仕様	• オンラインで本人確認を実施する • 加盟国間で相互に通知・承認し使用する
電子本人確認（eID）	電子署名	電子署名用の適格証明書の基準 /電子署名の検証基準 /電子署名の適格保存サービスの基準	• 書類等の電子データに署名として用いられ、手書き署名と同等の効力を保証する
	リモート署名作成装置の管理	電子署名作成デバイスの管理のための適格サービスの要件	• 署名者に代わって電子署名作成データを生成/管理を行う • 認証は5年間の脆弱性評価を条件として、2年間有効
トラストサービス	eシール	高度なeシールの基準 /eシール作成デバイスの管理のための適格サービスの要件	• 電子データの発行元・完全性を保証する
	eタイムスタンプ	データへの日付と時刻のバインドおよび正確な時間ソースに関する標準の要件	• ある時間に特定のデータが存在していたことを保証する
電子文書	電子登録配送サービス	電子登録配送サービスのデータ送受信の基準	• 第三者間での確実なデータ送受信、送受信日時・送受信者の識別等を保証する
権限移譲・実施規則	ウェブサイト認証	Webサイト認証の適格証明書の規格、仕様	• ウェブサイトの信頼性・正当性を保証する
末則	電子アーカイブ	電子アーカイブサービスの基準 ※電子アーカイブサービスの基準のみ「may」	• ドキュメントの完全性・出所の正確性・法的特性を保証する電子データの保存・送受信を行うサービスを指し示す
	電子台帳	一連のデータの実行及び登録並びに作成のプロセスに関する基準	• データの一意性・真正性・正しい時系列的な順序付けの保証を受けることができるサービスを指し示す
Annex	属性の電子証明	なし	• 紙の形式で合法的に発行された証明と同じ法的効力を有する • 加盟国間で相互に認識される

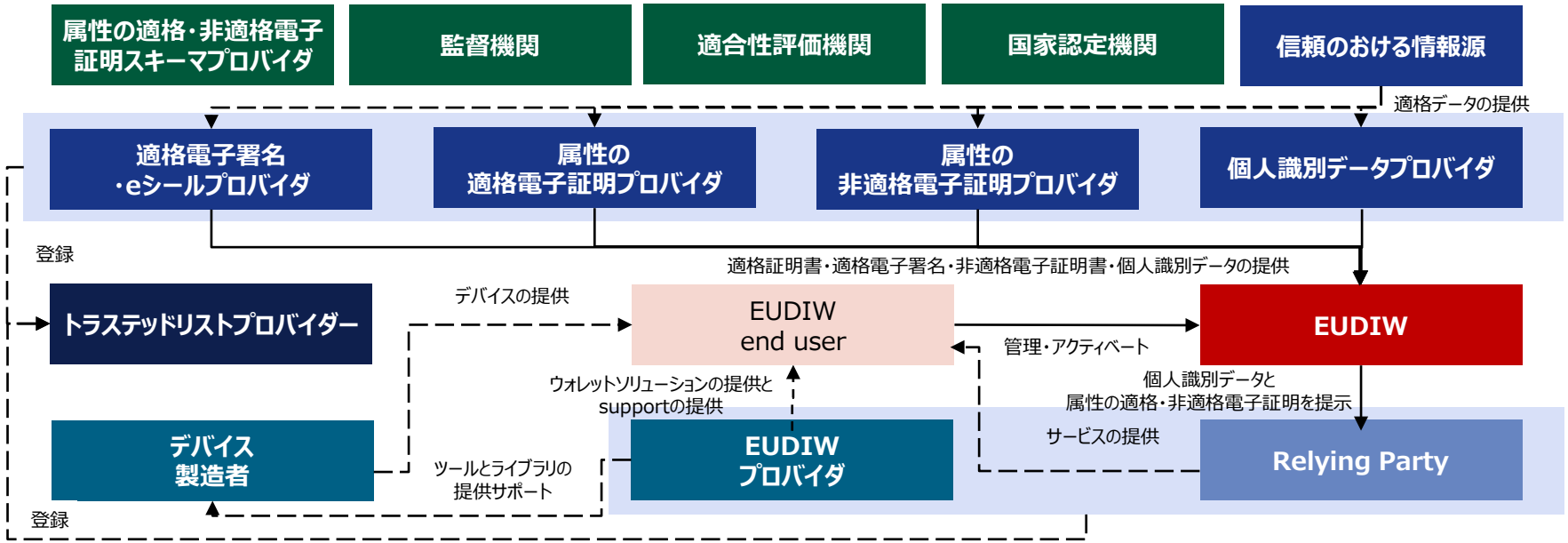
凡例 ■：Trusted Web との関連があると考えられる項目　■：Trusted Web との関連が薄いと考えられる項目

出所）
1 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281&from=EN

European Digital Identity Wallet : EUDIW

EUDIWアーキテクチャ・リファレンスフレームワーク（ARF）は、2023年2月10日に最終版が公開された。[1]必要な個人識別データと属性の電子的証明をユーザーに対して透過的で追跡可能な方法で安全に要求・取得・保存・選択・結合・共有することを求めており、またW3C VCs、SD-JWTなどの標準を参照していることなどからも、自己主権型アイデンティティ（Self Sovereign Identity）の実現を志向していることが伺える。

EUDIW ARFの構成



凡例
- EUDIWとそのエンドユーザー
- EUDIWに格納する各種情報（PID、属性情報の証明書）や、電子署名機能を提供する、トラストサービス事業者等の活動
- EUDIWの発行と、必要なデバイスの製造をする機関
- 各プロバイダの現在、過去の情報を提供する
- EUDIWを提示される当事者（Relying Party）
- EUDIWやトラストサービス事業者、トラステッドリストの適合性評価を行い、その管理監督を行う機関

実線：アーキテクチャ・リファレンスフレームワークのスコープ
点線 ：アーキテクチャ・リファレンスフレームワークのスコープ外

出所）
1 https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

（補足）NIST SP 800-63とeIDASの比較

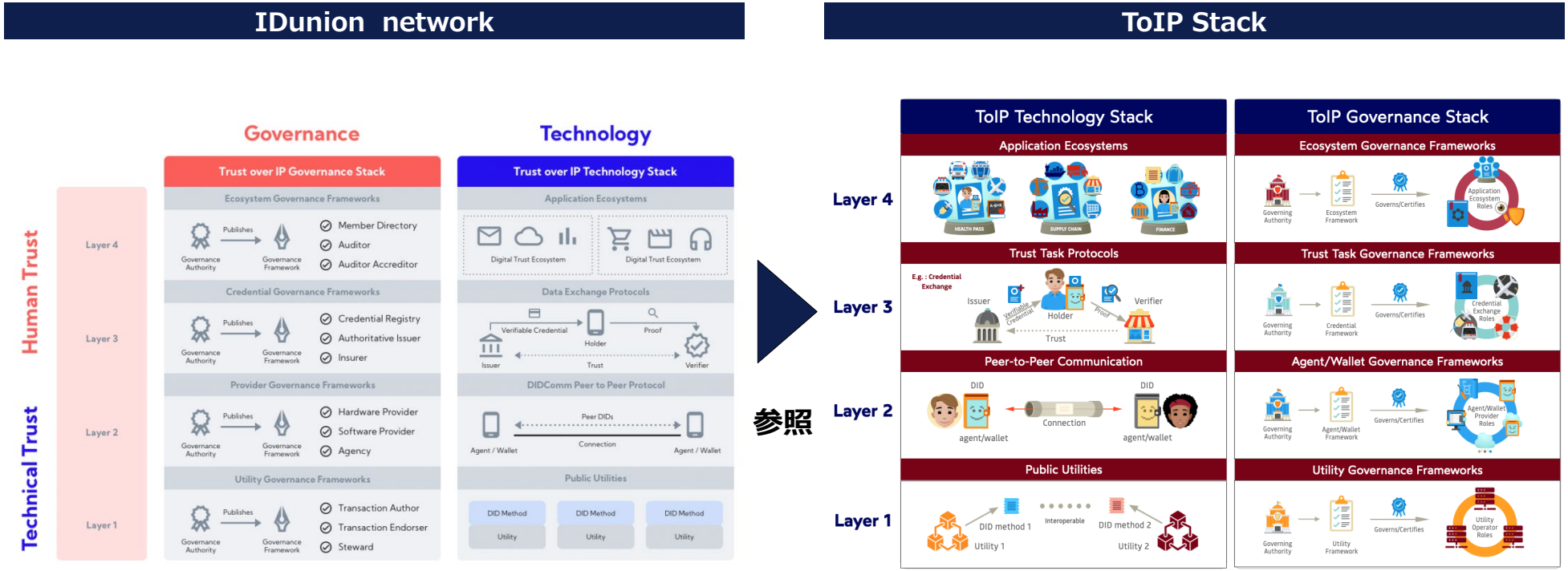
	NIST SP 800-63-3		eIDAS[1]	
本人確認（ID Proofing）の厳密さ、強度	Identity Assurance Level（IAL）		Identity proofing and verification (natural person)	
	IAL1	本人確認不要、自己申告での登録でよい	Low	主張されたアイデンティティを表す加盟国によって認識されたエビデンスを所持していると見なす
	IAL2	サービス内容ごとに識別に用いられる属性をリモートまたは対面で確認する必要あり	Substantial	主張されたアイデンティティを表す加盟国によって認識されたエビデンスを所持していると見なし、エビデンスが本物か確認を実施する
	IAL3	識別に用いられる属性を対面で確認するかつ検証担当者は有資格者である必要がある	High	主張されたアイデンティティを表す加盟国によって認識された写真もしくは生体認証のエビデンスを所持していることを確認し、「信頼のおける情報源」のもつ情報と照合し確認を実施する
認証プロセスの強度	Authenticator Assurance Level（AAL）		Issuance, delivery and activation	
	AAL1	単要素認証	Low	1つ以上の認証要素を利用する必要がある
	AAL2	2要素認証が必要（2要素目の認証手段はソフトウェアベースのもので可）	Substantial	2つ以上の認証要素を利用する必要がある
	AAL3	2要素認証が必要、かつ2要素目の認証手段はハードウェアを用いたもの（ハードウェアトークン等）が必要	High	Substantialに加えて重複や改ざん、および攻撃の可能性が高い攻撃者から保護する（具体的な技術の記載は無し）
フェレデーション（ID情報の連携）をする際のデータのやり取りの強度	Federation Assurance Level（FAL）		該当なし	
	FAL1	認証結果データへの署名		
	FAL2	署名に加え、データの送付対象のみが復号可能な暗号化の実施		
	FAL3	ユーザーごとの鍵と認証結果のデータを紐づけて送付し、送付先はユーザーの認証結果に紐づく		

出所）
1 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R1502&from=EN#d1e150-7-1

IDunion

2020年8月よりテストを開始した IDunion[1] は、ショーケースプログラム「Secure Digital Identities」の一環としてドイツの連邦経済エネルギー省が資金提供をしているデジタルアイデンティティインフラストラクチャを構築することを目的としたプロジェクトである。そのトラストフレームワークであるIDunion networkはTrust over IP Foundation（ToIP）*1の ToIP Stack[2]をリファーしている

IDunion networkとToIP Stackの関係



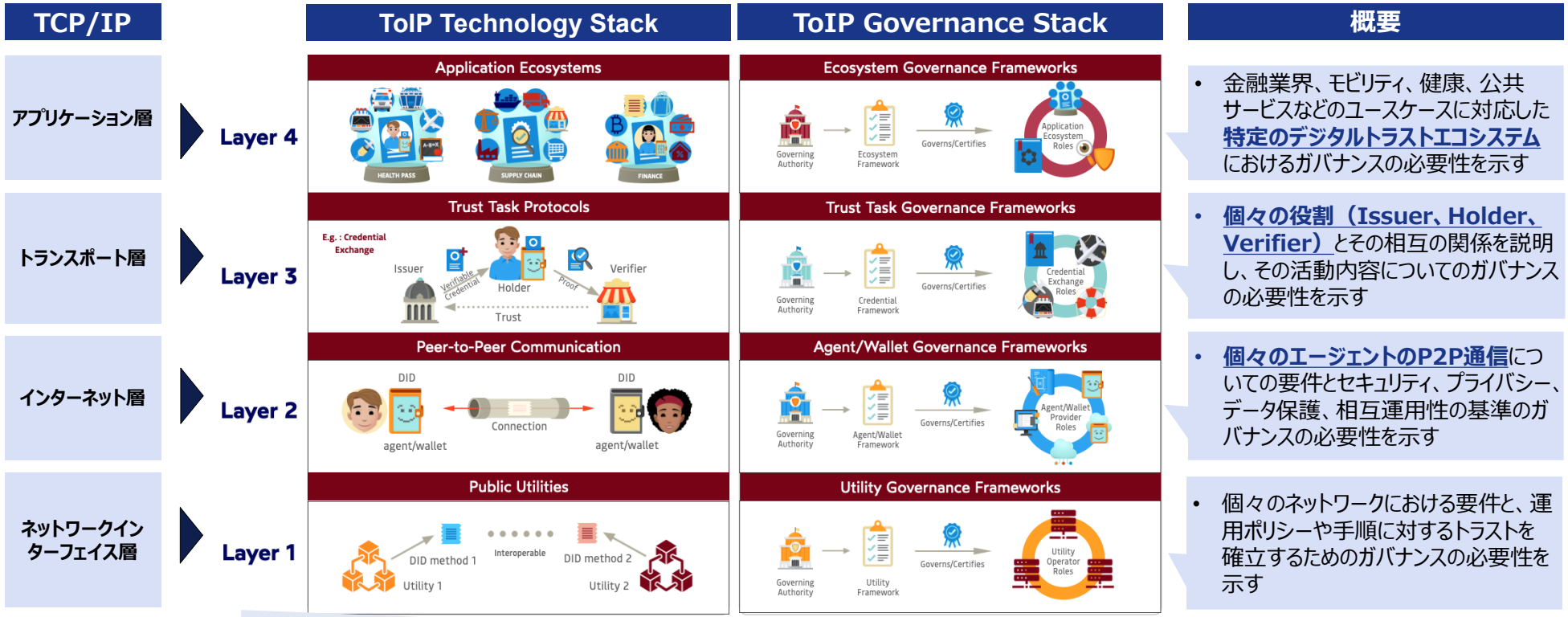
*1 Trust over IP Foundation（ToIP）は2020年5月に発足したLinux Foundationにホストされた分散型デジタルトラストのための相互運用可能なアーキテクチャの作成に取り組む組織である

出所）
1 https://idunion.org/?lang=en
2 https://www.trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf

IDunion：ToIP Trust Framework

ToIP Stack は、デジタル・ネットワークもしくはネットワーク上でのトラストを確立する方法を簡素化・標準化することを目的として、テクノロジー（マシンレイヤーでの暗号化による検証可能性）と、ガバナンス（法律・ビジネス・社会レイヤーでの人間のアカウンタビリティ）の2軸と、TCP/IPスタックの構造に着想を得た4層の整理の組み合わせによって構成されるコンセプトである[1,2,3]

ToIP Stackの構成と各レイヤーの概要



「各階層は、インターネット上の各デバイスが TCP/IP スタックのインスタンスを実行するのと同様に、プロトコルの標準 “スタック” のインスタンスになる」と記載があり、TCP/IPのレイヤーとイコールにはならないが、構造の要素を参考にしていると思われる

出所）
1 https://github.com/trustoverip/TechArch/blob/main/spec.md#1-introduction
2 https://www.trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf
3 https://trustoverip.org/wp-content/uploads/ToIP-Governance-Architecture-Specification-V1.0-2022-12-21.pdf

ToIP Technology Stack

ToIP Technology Stack は、暗号化による検証可能性について各レイヤーにおけるコンセプトを示しており、コンセプトのベースとなる技術として W3C DIDs の実装を明示していることが特徴的である[1,2]

ToIP Technology Stackの構成

構成	概要	詳細
Layer 4 **アプリケーションエコシステム** **Application Ecosystems**	エンドユーザーに価値を提供するために、1~3のレイヤーの上に構築する必要があるマーケットアプリケーションのための要件を定義する	• DIDとVCを利用してアプリケーションを構築し、デジタルトラストエコシステムを構築
Layer 3 **トラストタスクプロトコル** **Trust Task Protocols**	VCのデータ交換フォーマットとプロトコルを使用して、世界中の任意のIssuer-Holder-Verifier間での要件を定義する	• IssuerによるDIDと公開鍵のデータレジストリ（ブロックチェーン等）への書き込み • Issuerによる署名 • Verifierによるクレデンシャル保有証明の要求 • Verifierによる公開鍵を用いた検証
Layer 2 **P2Pコミュニケーション** **Peer-to-Peer Communication**	個人、組織、デジタルな “モノ” が標準的なP2Pプロトコル上（DIDcomm など）でデジタルクレデンシャルのやり取りをするために必要な要件を定義する	• データウォレットはDIDsを用いて直接通信することが可能。台帳に記録されることはない • Holderのデータウォレットは常にHolderの管理下にあり、データウォレットがHolderに代わって行動するときはHolderの同意のもとに実行する。Issuer, Verifierのデータウォレットはクラウドベースのサービスを含むあらゆるコンピューティングデバイスで実行可能 • 接続を通じてデータが交換されるとプライバシーは保護され、接続は将来の相互作用のために保持される
Layer 1 **パブリックユーティリティーズ** **Public Utilities**	分散型識別子(W3C DIDs)用のパブリックに読み取り可能で検証可能なデータストレージネットワーク（ブロックチェーン、分散型台帳技術など）の要件を定義する	• 分散型識別子（DID）は、デジタル・アイデンティティの確立と検証可能なクレデンシャルの共有に使用されるグローバルにユニークな文字列で、中央集権的なレジストリを必要としない。DIDは必要な限り永続的に維持される • 公開鍵やその他のデータを含む DID 文書を保管するために、DID method に対応した Verifiable Data Registry を整備する。ブロックチェーン、分散型台帳、分散型ファイルシステム、データベースなどを使用することが可能

出所）
1 https://github.com/trustoverip/TechArch/blob/main/spec.md#1-introduction
2 https://www.trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf

ToIP Governance Stack

ToIP Governance Stack は、Public Utilityの運用ポリシー・手順、デジタルエージェントのセキュリティ・プライバシー・データ保護・相互運用性の基準、Issuer-Holder-Verifier間の各活動それぞれのガバナンスの必要性を示すとともに、それらを束ねた上位概念である「デジタルトラストエコシステム」の策定の必要性を説明している[1,2,3]

ToIP Governance Stackの構成

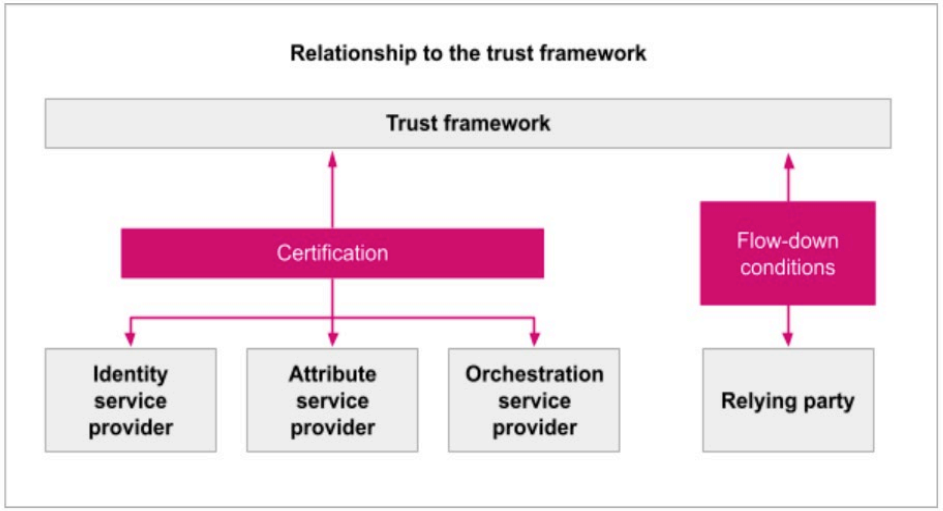
構成	概要	詳細
Layer 4 **エコシステムフレームワーク** Ecosystem Framework	**トラストの拡大** ガバナンスは、あらゆる規模の信頼エコシステムのメンバー間の信頼を促進する	• 下位 3 レイヤーすべてにわたるデジタルトラストエコシステム全体の運用を可能にするポリシーとルールを確立するための「エコシステムガバナンスフレームワーク」が必要であるとしている • エコシステムガバナンスフレームワークは、トラストマーク、トラストレジストリ、ユーザビリティ要件、認証プログラム、およびエコシステム全体の整合性と健全性を確保するために必要な他のメカニズムを規定することもできる
Layer 3 **トラストタスク ガバナンスフレームワーク** Trust Task Governance Framework	**信頼性** 標準的なルールを順守することで、デジタルクレデンシャルはHolderがVerifierと信頼関係を築くことを可能にする	• 提示されたVC証明に基づいてVerifierが判断を下すために必要なすべての情報を持てるようにするクレデンシャル・ガバナンス・フレームワークが必要である • クレデンシャル・ガバナンス・フレームワークと、 Issuer-Holder-Verifier間の4ステップ（前頁参照）を組み合わせることであらゆる規模のデジタルトラストエコシステムにスキームを適用可能になる
Layer 2 **エージェント・ウォレット ガバナンスフレームワーク** Agent/Wallet Governance	**認証** データウォレットは、セキュリティ、プライバシー、データ保護に関する標準規格に準拠して構築される	• デジタルウォレットとその間に通信するデジタルエージェントのセキュリティ、プライバシー、データ保護、相互運用性の基準を確立するために、ウォレット/エージェントガバナンスのフレームワークが必要である
Layer 1 **ユーティリティ ガバナンスフレームワーク** Utility Governance Framework	**合意形成** Verifiable Data Registry のセキュリティとインテグリティを保証するガバナンス	• Public Utility（ブロックチェーンや分散型台帳など）の運用に用いられるポリシーや手順に対するトラストを確立するためのガバナンスフレームワークが必要であるとしている • なおガバナンスフレームワークは、用いるDID ユーティリティによって大きく異なる可能性がある 例）パブリックパーミッションレスブロックチェーン（Bitcoin,イーサリアム等）は、パブリックパーミッションドブロックチェーン（Sovrin等）よりもアルゴリズム駆動型のガバナンスとなる

出所）
1 https://github.com/trustoverip/TechArch/blob/main/spec.md#1-introduction
2 https://www.trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf
3 https://trustoverip.org/wp-content/uploads/ToIP-Governance-Architecture-Specification-V1.0-2022-12-21.pdf

The UK digital identity and attributes trust framework の概要

The UK digital identity and attributes trust framework（The UK DIATF）は、DCMS*1により策定が進められている英国のトラストフレームワークである。2022年6月、2021年発表の「アルファ」版から「ベータ」版へアップデートを実施。実態に即したサブロールの追加や生体認証技術要件の追加、トラストマークの発行などの記載が追加された。並行して2022年6月に就労権・賃貸・犯罪歴の確認を対象にした「デジタルアイデンティティドキュメント検証テクノロジ （IDVT）」を開始している[1]

The UK DIATFの参加者



identity service providers（IDサービスプロバイザー）

ユーザー（のデジタルID）の証明・検証を行う
ID検証を行うソフトウェア（モバイルアカウントの検証機能、生体認証対応の身元確認機能など）の開発を行う主体も該当する

attribute service providers（属性サービスプロバイダー）

IDに紐づく属性情報（パスポート、運転免許証、出生証明書などの文書やデータベースにある属性情報や携帯電話番号、銀行口座、クレジットスコア、住宅ローンなど）の作成、収集、検証を行う主体であり、個人のデータストアやデジタルウォレットなどのソフトウェアを指す

orchestration service providers

テクノロジインフラストラクチャ（分散型台帳など）の提供を通じて、トラストフレームワークの参加者間でデータを安全に共有する

scheme owners

デジタルIDと属性情報を使用するためのスキームを作成及び実行する
民間部門（サービス）におけるスキームについてはISO 17021:2012やISO / IEC 17065:2012などの標準を使用して、UKAS（英国認証機関認定審議会）の認定を受けることやスキームのデータ保護影響評価（DPIA：Data protection impact assessments）を完了していること等が求められる

*1 DCMS：英国 デジタル・文化・メディア・スポーツ省

出所）
1 https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version#what-are-digital-identities

3.2.1 トラストフレームワークの策定状況

The UK DIATFの構成[1]

組織がフレームワークに参加する方法	各ロールの説明、スキームの例について紹介	
アイデンティティサービスプロバイダのルール	デジタルアイデンティティの作成	グッドプラクティスガイド45「誰かの身元を証明して確認する方法」を参照する
属性サービスプロバイダのルール	属性の理解	属性の品質、属性の共有について記載
	属性の作成	属性の作成、個人・組織へのバインド、属性の共有について記載
	属性の品質評価	属性のスコアリングについて記載
アイデンティティサービスプロバイダと属性サービスプロバイダの共通ルール	再利用可能なデジタル ID/属性サービスの作成	グッドプラクティスガイド44「認証器を使用してオンラインサービスを保護する」を参照するよう記載
	デジタル ID アカウントと属性アカウントの管理	アカウント取り消し・一時停止・閉鎖・回復・変更のためのプロセスが必要であると記載
	製品・サービスが包括的であることの確認	Equality Act 2010 に準拠し誰も除外されないよう検討することを記載
	製品・サービスがアクセシブルであることの確認	英国政府のアクセシビリティ規制に従う必要があることを記載
	製品・サービスの廃止	製品・サービスを廃止する際の通知と一定期間の猶予確保の必要を記載
全てのサービスプロバイダの共通ルール	提供する製品・サービスの相互運用性の確保	OIDC、W3C VCs data modelsなどの規格と競合しないデータスキーマを提供
	権限を委任された人物による行動の可否	権限の委任について、各サービスが許可するか判断する必要があることを記載
	苦情・紛争への対応	苦情・紛争処理のプロセスが必要
	スタッフとリソース	参加する組織が備えていなくてはいけないスタッフ・リソースについて記載
	暗号化と暗号技術	暗号化および暗号化技術に関する業界標準とベストプラクティスに従う必要がある
	サービス・品質管理	サービス・品質管理のため目標とプロセスを記載したドキュメントを作成する必要がある
	情報管理	ISO/IEC 27001:2017などに準拠した情報管理システムが必要である
	情報セキュリティ	ISO/IEC 27001:2017などの情報セキュリティ管理システムが必要である
	リスク管理	ISO/IEC 27005:2018 などのリスク管理フレームワークが必要である
	不正管理	不正管理に関するベストおラクティスへの準拠を求める
	インシデントへの対応	インシデント管理・ロギングに関する国家サイバーセキュリティーセンターガイダンスへの準拠が必要
	ユーザーに対する製品・サービスの明確な説明	ユーザーに対する製品・サービスの明確な説明を求める
	プライバシーおよびデータ保護規則	英国GDPRへの準拠を求める記載の中に「データの最小化」についても言及有り
	記録の保持	英国GDPRに準拠した記録の保管と破棄を求める
	証明書利用者との連携	フレームワーク内の他組織のサービス・製品を利用する「証明書利用者」と合意することを求める
	禁止事項	違法行為の禁止について記載
規律・ガイダンス・法律の表	各項目にて示された規律・ガイダンス・法律を整理した表	

出所）

凡例 ■：Trusted Web との関連があると考えられる項目　■：Trusted Web との関連が薄いと考えられる項目

1 https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity#when-to-check-someones-identity

The UK DIATFの認定

DIATFに参加を希望する機関は認証機関によって評価[1]を受け認定される必要があり、現在認定を受けたアイデンティティサービスプロバイダは35事業者存在する。また現在は英国認証機関認定審議会（UKAS）が認証機関を担っているが、今後はUKASにより認定された機関が認証を実施*1する

評価プロセス

Step00	DIATFにおいて担うロールと、認定したいスキームを決め、DCMS認定チームに連絡し事前評価を受ける
Step01	認証機関リストから認証機関を選択し連絡。認証のため契約を交わす
Step02	既存の認証が実施されているか確認できるエビデンスを認証機関に提出
Step03	認証機関が申請に対し評価を実施するか決定
Step04	評価の実施にあたりサービス説明の文書、基準文書を提出する
Step05	認証機関によりエビデンスの評価が実施される
Step06	認証機関内の監査人による独立した評価による判断を実施
Step07	要件を満たした機関はWebサイトにて公開される
Step08	認証機関により毎年サーベイランス評価が実施される
Step09	公平・平等な認証がなされているかを確認するため、全ての認証に対しDCMSによる定期的な保証を実施
Step10	認証機関は定期的（四半期に1回程度）認証評価数と、結果のレポートをDCMSに提出する

認定されたアイデンティティサービスプロバイダー覧（認定日）*2

- Yoti and Post Office EasyID（2022年11月2日）
- HooYu Limited（2022年6月6日）
- TrustID Limited（2022年6月13日）
- Digital Identity Net UK Limited （2022年12月3日）
- Paycasso Verify Ltd trading as Xydus （2022年6月27日）
- Sterling (EMEA) Limited （2022年7月5日）
- T4 Communications UK Ltd T/A Rightcheck （2022年7月7日）
- Deloitte LLP （2022年7月22日）
- Credas Technologies Ltd （2022年9月7日）
- Amiqus Resolution Ltd （2022年8月11日）
- Digidentity B.V. （2022年8月31日）
- CDD Services Ltd T/A Spotlite Business Services （2022年9月21日）
- OCR Labs Global Limited （2022年9月22日）
- uComply Limited （2022年9月26日）
- GB Group PLC （2022年10月20日）
- Marston Holdings Ltd （2022年9月14日）
- Onfido Limited （2022年9月29日）
- ID Pal Limited （2022年10月20日）
- Northrow Limited （2022年10月21日）
- Atlantic Data （2022年10月21日）
- Checkback International Group incorporating Vetting Solutions Centre Ltd （2022年10月27日）
- Datachecker Limited （2022年11月16日）
- Thirdfort Limited （2022年11月22日）
- Experian Limited （2022年11月30日）
- Nuggets Ltd （2022年12月2日）
- Konfir （2022年12月13日）
- Persona Identities Inc （2022年12月13日）
- Virtual Signature ID Validate Ltd （2022年12月7日）
- Mastercard UK Management Services Limited （2022年12月13日）
- Target Professional Services (UK) Limited （2022年12月21日）
- mypensionID Limited （2022年12月21日）
- Veridas Digital Authentication Solutions, S.L. （2022年12月21日）
- Due Diligence Checking Limited （2023年1月9日）
- iPassport （2023年1月18日）
- PPAC Solutions LTD （2023年2月6日）
- Fragomen LLP /DISC（2023年3月14日）

*1 現在下記の5機関が認証機関としての認定をうけるためのパイロット評価プログラムに申請している
Age Check Certification Services Ltd trading as Digital ID Systems Certification/Amtivo Group Limited trading as British Assessment Bureau and Certification Europe/BSI/Kantara/NQA
*2 令和5年3月27日時点での確認

出所）1 https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/trust-framework-certification

（補足）NIST SP 800-63とThe UK DIATFの比較

	NIST SP 800-63-3		The UK DIATF[1]	
本人確認（ID Proofing）の厳密さ、強度	Identity Assurance Level（IAL）		‘verification’ check	
	IAL1	本人確認不要、自己申告での登録でよい	1	静的情報による知識ベース検証の実施
	IAL2	サービス内容ごとに識別に用いられる属性をリモートまたは対面で確認する必要あり	2	対面・リモートでの写真付きエビデンスとの照合 / 生体認証による確認の実施 / 複数の動的情報による知識ベース認証の実施　のいずれかを実行する必要がある
	IAL3	識別に用いられる属性を対面で確認するかつ検証担当者は有資格者である必要がある	3	対面・リモートでの写真付きエビデンスとの照合 / 生体認証による確認の実施のどちらかを実行する必要がある
			4	生体認証による確認の実施を実行する必要がある
認証プロセスの強度	Authenticator Assurance Level（AAL）		The quality of authenticator	
	AAL1	単要素認証	Low	パスワード・暗証番号・静的情報による知識ベース検証・発行方法不明のトークン・処理方法不明の生体認証
	AAL2	2要素認証が必要（2要素目の認証手段はソフトウェアベースのもので可）	Medium	自動作成され、安全に保存されたパスワード・暗証番号 動的情報に基づく知識ベース検証 改竄・間違った人に発行されていないことがわかっているトークン
	AAL3	2要素認証が必要、かつ2要素目の認証手段はハードウェアを用いたもの（ハードウェアトークン等）が必要	High	アカウントを作成したユーザー以外に属さなかった認証器 業界標準*1を満たすことを証明するために独立してテストされたトークン キャプチャに関して業界標準*2を満たすことを確認するために独立してテストされたプロセス・システムをもつ生体認証
フェレデーション（ID情報の連携）をする際のデータのやり取りの強度	Federation Assurance Level（FAL）		該当なし	
	FAL1	認証結果データへの署名		
	FAL2	署名に加え、データの送付対象のみが復号可能な暗号化の実施		
	FAL3	ユーザーごとの鍵と認証結果のデータを紐づけて送付し、送付先はユーザーの認証結果に紐づく		

*1 COMMON CRITERIA、FIDO、NIST SP FIPS 140-2など
*2 ISO/IEC 19795-1:2006、ISO/IEC 30107-1:2016など

出所）
1 https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services/giving-users-access-to-online-services#choosing-an-authenticator

3.2 詳細調査結果：トラストフレームワークの策定状況

3.2.2北米（米国、カナダ）における調査結果

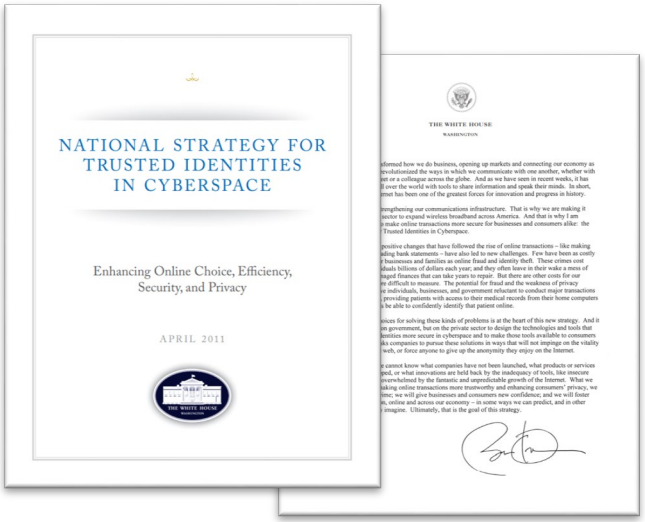
米国
カナダ

Identity Ecosystem

Identity Ecosystem[1]は2011年に、ホワイトハウスが発表した「NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE（NSTIC）」[2]のビジョンを具体化したものであり、「匿名から完全認証、低価値から高価値までのトランザクションを安全にサポートするユーザー中心のテクノロジー、ポリシー、および既存の合意された標準」を規定している。その後、2015年にNSTIC IDESG*1によってIdentity Ecosystem Framework（IDEF）[3]が策定された

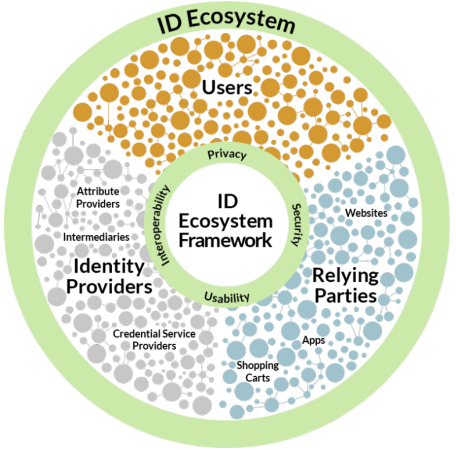
NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE

「NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE（NSTIC）」とは「個人、企業、その他の組織が機密性の高い取引をオンラインで行う際に、より大きな信頼とセキュリティを享受できる未来」をビジョンに掲げたホワイトハウスのイニチアチブである



Identity Ecosystem

Identity Ecosystemは「NSTIC」のビジョンである「個人、企業、その他の組織が機密性の高い取引をオンラインで行う際に、より大きな信頼とセキュリティを享受できる未来」が実現した姿として提唱されている概念である



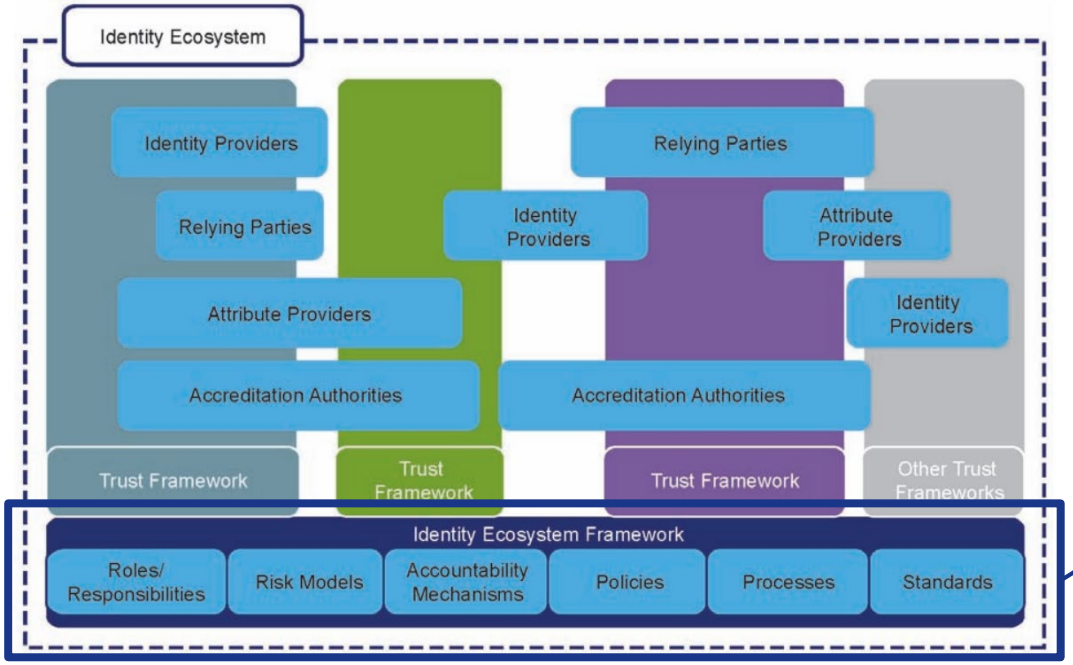
*1 NSTIC IDESG（ID Ecosystem Steering Group）はアイデンティティエコシステムフレームワーク(IDEF)のポリシー、標準、認定プロセスの開発を管理することにより、この使命を達成するために作成された民間部門主導の組織である。現在はKantara initiativeに移管し、RIUP WGとして存続している。

出所）
1 https://idefregistry.edufoundation.kantarainitiative.org/what-is-the-id-ecosystem/
2 https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
3 https://idesg.org/The-ID-Ecosystem/Identity-Ecosystem-Framework/Development-of-the-IDEF.html

Identity Ecosystem

IDEFはIdentity Ecosystemを構築する相互運用性標準、リスクモデル、プライバシーと責任のポリシー、要件、および説明責任メカニズムの包括的なセットであり、IDEFは産業セクターごとに策定されているトラストフレームワークとは別に、各産業セクターを横断して満たすことが求められる/推奨される要件として Baseline Functional Requirements を規定している[1,2]

Identity EcosystemとIdentity Ecosystem Frameworkの関係



Identity Ecosystem Framework

※図は2011年4月時点のものであり、2015年に策定されたIDEFの構成要素と異なる部分が存在している

出所）
1 https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
2 https://idefregistry.edufoundation.kantarainitiative.org/idef-knowledge-base/

IDEFの構造

IDEF は Identity Ecosystem は各レイヤーにおける参加主体の担うべき Roles と行うべきActivity を規定している Functional model と、Identity Ecosystem の参加主体が必ず満たさなければならない、または推奨されている要件を定義している Baseline Functional Requirements によって構成されている[1,2]

IDEFの構造

Functional model

	Activities:	Roles:
Governance & Accountability	Policy, Rule & Requirement Development Certification Accreditation Assessment/Audit	Accreditation Body Certification Body Assessors/Auditors Community of Interest
Interoperability	Activities: Stds. Development Spec Development Exchange	Roles: Standards Development Body Specification Development Body Interoperability Providers
Administration and Operations	Activities: Redress Recovery Enterprise Governance & Policy Development	Internal Audit Service Optimization Updates (Periodic & Event Based)
Functional	Core Operations: Registration Credentialing Authentication Authorization Trans. Intermediation	Roles: Users Identity Providers Credential Service Providers Registration Authorities Intermediaries Attribute Providers Relying Parties

×

Baseline Functional Requirements

Privacy	オンライン取引において、利用者の情報を必要な分だけを収集し、収集した情報を利用者の同意のもとに慎重かつ適切に取り扱うための方法を定めた要件
Security	オンライン取引において、オンライン・アイデンティティ・データを保護するために用いられるべき手段、他者による不正アクセスを防止する手段、および回復できる手段を定義する要件
Interoperability	企業や利用者がインターネット上の異なるオンラインサービス間でアイデンティティデータを利用するための技術や手続きの基準を定義する要件
Usability	オンラインサービスやアイデンティティ情報の制御を適切に使いやすくし、できるだけ多くのユーザーに対して透明性を持たせるための基準を定めた要件
Best Practice	現在IDEFの要求事項ではなく、推奨事項であるが、将来的には要求事項に含めることが検討される可能性がある

出所）
1 https://idefregistry.edufoundation.kantarainitiative.org/docs/IDEF-Functional-Model-v1.0_MOD-2.pdf
2 https://idefregistry.edufoundation.kantarainitiative.org/idef-knowledge-base/

米国
カナダ

IDEF Functional modelの詳細①

Governance&Accountability Layer はコミュニティやアクター間で IDESG の機能要素を実行するためのルール・ガイドライン・要件を作成・監視・実施するエンティティが存在するレイヤーである。Administration and Operations Layer とは異なり、エンティティ内部のガバナンスではなく、エンティティ間の取り組みに特化している[1]

Governance & Accountability Layer	ポリシー / ルール / 要求事項 / 開発	• 特定のコミュニティ内でのアイデンティティおよびアイデンティティ技術の使用を管理するための規則、要件およびポリシーを特定または採用することを含む、トラストフレームワークを作成するプロセス
Interoperability Layer	認定（Accreditation）	• エンティティがトラストフレームワークの認証又は評価活動を実施する能力があることを評価、承認及び正式に承認するためのプロセス
Administration and Operations Layer	認証（Certification）	• 製品またはサービスのプロバイダがトラストフレームワークに定義された要件を満たしているかどうかを評価、検証、判断するプロセス
Functional Elements Layer	評価・監査	• トラストフレームワークまたはコミュニティのルール、ポリシー、要件に対するエンティティの適合性をレビューし、証拠を収集するプロセス

出所）
1 https://idefregistry.edufoundation.kantarainitiative.org/docs/IDEF-Functional-Model-v1.0_MOD-2.pdf

凡例 ■：Trusted Web との関連があると考えられる項目 ■：Trusted Web との関連が薄いと考えられる項目

米国
カナダ

IDEF Functional modelの詳細②

Interoperability Layer は、Identity Ecosystem内のエンティティが通信し、アイデンティティを交換する能力を確立し、維持するための機能である[1]

Governance & Accountability Layer		
Interoperability Layer	標準策定	• コミュニティ内またはエコシステム全体で使用される アイデンティティ技術の標準および手順の標準を作成するプロセス
	仕様開発	• コミュニティ内の参加者が アイデンティティデータをどのように主張し交換するかを定義する仕様およびプロファイルを作成するプロセス
	交換	• 特定のコミュニティ内またはエコシステム全体の参加者間でクレデンシャルのポータビリティをサポートするために、技術的な（セマンティックを含む）相互運用性を促進するプロセス
Administration and Operations Layer		
Functional Elements Layer		

出所）
1 https://idefregistry.edufoundation.kantarainitiative.org/docs/IDEF-Functional-Model-v1.0_MOD-2.pdf

凡例 ■：Trusted Webとの関連があると考えられる項目 ■：Trusted Webとの関連が薄いと考えられる項目

米国
カナダ

IDEF Functional modelの詳細③

Administration and Operations Layer は IDESG の中核的な運営と機能を管理・支援することを目的とした活動を実施するレイヤーである。Functional model 内のいずれかのRoleを果たす Identity Ecosystem の全参加者は Administration and Operations Layer の Activity も実施する[1]

Governance & Accountability Layer	Redress	• エンティティおよび組織が、ID システムの運用およびプロセス中に発生したエラーを調整するプロセス • すべてのエコシステム・サービス・プロバイダは、リドレス活動を実行しなければならない
Interoperability Layer	Recovery	• セキュリティまたはプライバシーに関するイベント（データ侵害、サービスの中断など）の後に、組織がクレデンシャル、属性、および他の ID サービスの可用性と継続性を確保するためのプロセスと手順 • すべてのエコシステム参加者は、復旧活動を実行する責任がある
Administration and Operations Layer	Enterprise Governance & Policy Development	• エンティティが、中核となる業務や機能の適切な遂行を支援するために必要な方針・ルール（法的契約ポリシー、データ保護ポリシー、セキュリティポリシー、個人情報保護ポリシーなど）を策定し、実施するプロセス
Functional Elements Layer	Internal Audit	• エンティティの規則、ポリシー、要件への適合性を確認しその証拠を収集するプロセス
	Service Optimization	• 組織がサービスの改善のため内部および外部からのインプット（例：標準規格、顧客調査、外部ガバナンス/規制）を取り込み、統合をするプロセス
	Updates (Periodic & Event Based)	• エンティティがアカウント、属性、クレデンシャル、および他の ID 情報を更新して、資格の適格性を決定するプロセス • 定期的な性質、またはイベントベース（例：結婚、サブスクリプションの終了など）である場合がある

出所）
1 https://idefregistry.edufoundation.kantarainitiative.org/docs/IDEF-Functional-Model-v1.0_MOD-2.pdf

凡例 ■：Trusted Web との関連があると考えられる項目 ■：Trusted Web との関連が薄いと考えられる項目

米国
カナダ

IDEF Functional modelの詳細④

Functional Elements Layerは、オンラインアイデンティティ関連インタラクションで発生する可能性のある基本的な操作（機能要素）で構成され、「コア・オペレーション」としてグループ化されている。なおオンラインアイデンティティ関連インタラクションにおいて各機能要素は必ず呼び出されるわけではない他、model 内で各機能要素の実行順番は明示的に定められていない[1]

Governance & Accountability Layer	登録	• クレデンシャルの発行または関連付けを目的として、デジタルアイデンティティを確立するプロセス • アプリケーション /属性管理 /属性検証 /適格性判断 を行う
Interoperability Layer	クレデンシャリング	• 確立されたデジタル・アイデンティティとクレデンシャルを結びつけるプロセス • クレデンシャルプロビジョニング /トークン結合 /属性結合 /取り消し を行う
Administration and Operations Layer	認証	• デジタルアイデンティティを主張するために使用される1つまたは複数のクレデンシャルの有効性を判断するプロセス • 認証要求 /クレデンシャル提示 /クレデンシャル検証 /認証決定 を行う
Functional Elements Layer	承認	• リソースへのアクセスに関する特定の要求を許可または拒否するプロセス • 承認要求 /属性制御 /属性検証 /承認決定 を行う
	トランザクションの操作	• トランザクション間の結合を制限し、クレデンシャルのポータビリティを促進するプロセスおよび手順 • Blinding /仮名化・匿名化 /プロトコル変換 を行う

出所）
1 https://idefregistry.edufoundation.kantarainitiative.org/docs/IDEF-Functional-Model-v1.0_MOD-2.pdf

凡例 ■：Trusted Web との関連があると考えられる項目 ■：Trusted Web との関連が薄いと考えられる項目

IDEF Baseline Functional Requirements[1]の詳細①

米国
カナダ

Privacy	データの最小化	個人情報の収集・使用・送信・保存を最小限にしなくてはならない。また、IdPはデータの最小化をサポートするために様々な粒度の情報要求に対応する技術的な仕組みの提供をしなくてはならない
Security	目的の制限	収集・使用・送信・保存した個人情報の使用をそのトランザクションの指定された目的にのみ制限しなくてはならない
Interoperability	属性の最小化	トランザクションにおいて特定の属性を収集する必要性を評価しなくてはならない。実行可能な限り、エンティティは属性ではなくユーザーに関するクレームを収集・生成・使用・送信・保存しなくてはならない
Usability	資格情報の制限	トランザクションに必要な場合とトランザクションに関連するリスクまたは関連する当事者へのリスクに対して適切である場合のみを除いてユーザーのクレデンシャルを要求してはならない
Best Practice	データ集約リスク	個人情報が収集・生成・使用・送信・保存されるシステムプロセスにおいて個人情報の集約によるリスクの評価を行うとともに、そのリスクを最小限に抑えるようにシステム・プロセスを設計する必要がある
	使用上の注意	個人情報をどのように収集・生成・使用・伝送・保管するかを説明する簡潔で意味のあるタイムリーなコミュニケーションをユーザーに提供しなくてはならない
	ユーザーデータコントロール	ユーザーが個人情報にアクセス・訂正・削除できるよう適切な仕組みを提供しなくてはならない
	サードパーティの制限	ユーザーが自身の個人情報の取扱いについて選択する際に、その選択は当該のエンティティが個人情報を送信する第三者に対して効果的に伝達されなくてはならない
	ユーザーへの変更通知	ユーザーの個人情報の収集・生成・使用・伝送・保存するサービスまたはプロセスに重要な変更があった場合はユーザに通知し同意を得る他、その変更により生じるリスクを軽減するための措置を提供しなくてはならない
	ユーザーによる登録拒否	ユーザーは登録の拒否、クレデンシャルのプロビジョニングの拒否、クレデンシャルの提示の拒否、自分の属性・クレームの公開を拒否する機会を得なくてはならない
	提供が任意の個人情報	トランザクションに先行してどの個人情報が必須で、どの個人情報が任意であるかを利用者に明確に示さなくてはならない
	匿名	実行可能な場合は常にエンティティは匿名、有効な属性を持つ匿名、偽名、または適切な場合は一意に惜別されるIDシステム及びプロセスを使用しなければならない
	リスクに比例したコントロール	ユーザーの個人情報の処理または使用に関する管理はその処理または使用のリスクの程度に見合ったものでなければならない
	データの保持と廃棄	個人情報の保持はユーザーに機能・サービスを提供し管理するために必要な時間に制限し、不要になった個人情報は適切な業界標準・法的要件に従い廃棄しなくてはならない
	属性の分離	可能な限り識別子データは属性データから分離されなければならない

出所）
1 https://idefregistry.edufoundation.kantarainitiative.org/idef-knowledge-base/privacy

凡例 ■：Trusted Web との関連があると考えられる項目 ■：Trusted Web との関連が薄いと考えられる項目

IDEF Baseline Functional Requirements[1]の詳細②

米国
カナダ

Privacy
Security
Interoperability
Usability
Best Practice

セキュリティ対策	アイデンティティ管理機能およびサービスをサポートするシステムに適切かつ業界で認められている情報セキュリティ基準・ガイドライン・慣行を適用しなくてはならない
データの整合性	認証データおよび属性値を含むアイデンティティデータの機密性と完全性を保護するために業界で受け入れられた手法を実施しなくてはならない
クレデンシャルの複製	クレデンシャル及びトークンを発行または管理する事業者は不正な開示及び複製から保護するために業界で認められているプロセスを実施しなくてはならない
クレデンシャルの保護	クレデンシャル・トークンを発行または管理するエンティティは業界で認められているデータの完全性を個人及び他のエンティティがクレデンシャルおよびトークンデータのソースを検証できるようにしなくてはならない
クレデンシャルの発行	クレデンシャル・トークンは適切かつ意図されたユーザーにのみ付与されるように設計された方法で発行または管理を行わなくてはならない
クレデンシャルの一意性	クレデンシャルを発行または管理するエンティティは認証のために各アカウントのペアがそのネームスペース内で一意に識別可能であることを保証しなければならない
トークン制御	ユーザーを認証するエンティティはユーザーが有効なトークンを管理していることを証明するために業界で認められた安全なプロトコルを使用しなければならない
多要素認証	ユーザーを認証するエンティティはパスワードを補強する、またはパスワードの代替となる認証メカニズムを提供しなければならない
認証リスク評価	エンティティは認証メカニズム及びサポート・プロセスの選択についてリスク評価プロセスを設けなければならない
アップタイム	デジタルアイデンティティ管理機能を提供し実施する事業者は、そのサービスの有効性に関して表明した保証を維持するために確立したポリシーとプロセスを持たなくてはならない
鍵管理	アイデンティティ管理の一部として暗号化ソリューションを使用する事業者は業界で受け入れられている慣行に一致するポリシー及びプロセスを実装しなければならない
復旧と再発行	クレデンシャルおよびトークンを発行するエンティティはセキュリティを維持しクレデンシャル・トークンの再発行・後進・復旧のためのメソッドと、オリジナルの登録・クレデンシャル操作を保証するメソッドを実装しなくてはならない
撤回	クレデンシャルまたはトークンを発行するエンティティはクレデンシャルおよびトークンを無効化するためのプロセスと手順を設けなくてはならない
セキュリティログ	デジタルアイデンティティ管理システムを実行するエンティティはシステム監査、必要に応じてセキュリティ調査、規制要件をサポートする方法でトランザクションとセキュリティ・イベントを記録しなくてはならない
セキュリティ監査	情報セキュリティ方針及び手順、ログ、インシデントレポート、クレデンシャル喪失発生のレビューを含む追加要件への準拠について定期的に監査を実施し、方針・手順の有効性を定期的に見直さなくてはならない

出所)
1 https://idefregistry.edufoundation.kantarainitiative.org/idef-knowledge-base/security

凡例 ■ : Trusted Web との関連があると考えられる項目 ■ : Trusted Web との関連が薄いと考えられる項目

IDEF Baseline Functional Requirements[1]の詳細③

米国
カナダ

Privacy	第三者認証	エンティティはサードパーティによって認証された外部ユーザーを受け入れることができなければならない
Security	サードパーティのクレデンシャル	エンティティは複数の目的および複数の受信者のために消費できるコンテンツおよび方法を使用してクレデンシャルまたはアサーションを発行しなければならない
Interoperability	標準化されたクレデンシャル	IDESGスタンダードレジストリにリストされている公開の標準に準拠した形式、またはIDESGスタンダードインベントリにリストされている非占有仕様に準拠して、クレデンシャルまたはアサーションを発行しなければならない
Usability	標準化されたデータ交換	デジタルアイデンティティ管理機能を実行する組織は公開された基準に適合するアイデンティティ関連データを通信および交換するシステム及びプロセスを使用しなければならない
Best Practice	文書化されたプロセス	エンティティは、内部およびエンティティ間の取引を含め、デジタルアイデンティティ管理機能を実施する際に、文書化されたビジネス方針およびプロセスを採用しなければならない
	第三者のコンプライアンス	サードパーティ・サービス・プロバイダとしてデジタルアイデンティティ管理機能を実行するエンティティは他のエンティティおよび関連する機能に適用されるIDESG基本要件のそれぞれを遵守しなければならない
	ユーザーの救済	エンティティがIDESG基本要件に準拠しないことによって損害を受けたと考えるユーザーのために効果的な救済メカニズムを提供し、促進しなければならない
	アカウンタビリティ	エンティティは、監査・検証・確認のためのメカニズムを提供することによるIDESG基本要件への準拠について説明責任を負わなければならない

出所）
1 https://idefregistry.edufoundation.kantarainitiative.org/idef-knowledge-base/interoperability

凡例 ■：Trusted Webとの関連があると考えられる項目 ■：Trusted Webとの関連が薄いと考えられる項目

IDEF Baseline Functional Requirements[1]の詳細④

米国
カナダ

Privacy	ユーザビリティの実践	デジタルアイデンティティ管理機能はユーザー中心の設計と業界で認められている適切なユーザビリティガイドラインとプラクティスを各プロセスに適用しユーザビリティ評価によって特定した重大な欠陥を修正する必要がある
Security	ユーザビリティ評価	エンティティは、デジタルアイデンティティ管理機能で実行する通信・インターフェイス・ポリシー・データトランザクション・およびエンドtoエンドプロセスの使いやすさを評価する必要がある
Interoperability	平易な文言	デジタルアイデンティティ管理機能でユーザーに提示される情報は、一般オーディエンスのまたはトランザクションの特定されたターゲットオーディエンスが理解しやすい明確でわかりやすい言葉でなければならない
Usability	ナビゲーション	デジタルアイデンティティ管理機能でユーザーに提供されるすべての選択肢・経路・インターフェース・およびオファリングは、ユーザーによって明確に識別できなければならない
Best Practice	アクセシビリティ	すべてのデジタルアイデンティティ管理機能は、実行可能な限り多くのユーザーがアクセスできるように合理的な配慮をしなければならず、アクセシビリティに関するすべての適用法および規制を遵守しなければならない
	ユーザビリティのフィードバック	デジタルアイデンティティ管理機能で提供されるすべてのプロセスは、ユーザビリティに関するユーザーのフィードバックを容易に収集するためのメカニズムを提供しなければならない
	ユーザー要件	ユーザー要件を収集するための公開標準・法的要件が存在する場合、デジタルアイデンティティ管理機能はユーザーに早期段階でインタフェースおよびアクセシビリティ要件を文書化し表現するための構造的な機会を提供する必要がある

出所）
1 https://idefregistry.edufoundation.kantarainitiative.org/idef-knowledge-base/usability

凡例 ■：Trusted Web との関連があると考えられる項目 ■：Trusted Web との関連が薄いと考えられる項目

IDEF Baseline Functional Requirements[1]の詳細⑤

米国
カナダ

Privacy	推奨されるポータビリティ	エンティティは、アイデンティティアカウントのポータビリティを可能にするサービスとシステムを利用する必要がある
Security	推奨されるデータ交換基準	デジタルアイデンティティ管理機能を実行する組織はIDESG標準レジストリにリストされている公開オープン標準、レジストリに実行可能なオプションがない場合は IDESG標準インベントリにリストされている非占有仕様に適合するアイデンティティ関連データを通信および交換するシステムおよびプロセスを利用するべきである
Interoperability	推奨される分類基準	エンティティは属性の意味的な相互運用性を可能にするために、安定し公開された共通の分類法を利用すべきであり、そのような標準が確立されているコミュニティ内で運用する場合は、それらの分類法のための公開されたオープンな標準を使用すべきである
Usability	推奨されるプロセスモデル	エンティティはデジタルアイデンティティ管理機能のために安定し、公開された共通の形式モデルおよびビジネス・ プロセスを採用すべきであり、そのような標準が確立され、それらの機能に適切である場合には、 それらのモデルおよびプロセスに公開オープン標準を使用するべきである
Best Practice	推奨されるモジュール性	エンティティは、デジタルアイデンティティ管理機能にモジュール式アイデンティティコンポーネントを実装することが推奨される
	推奨されるフェデレーション基準	アイデンティティフェデレーション内でデジタルアイデンティティ管理機能を実施する場合、エンティティは、そのフェデレーションが設定した最低基準に従って、公開されたポリシーおよび明示的に要求されるシステム ルールにすべての実質的側面で準拠すべきである
	推奨される法令順守	デジタルアイデンティティ管理機能を実施する場合、エンティティは関連機能に適用されるすべての法律および規制を実質的にすべて遵守すべきである
	推奨される品質管理	エンティティはデジタルアイデンティティ管理機能で使用する個人情報の必要な品質を、それらの機能のリスクと関係するユーザーへのリスクを含む情報に基づいて決定するべきである
	推奨されるテクノロジーの適用	実行可能な限り、プライバシー要件とポリシーは技術的な仕組みによって実装されるべきで ある。これらの技術的なプライバシー管理は技術スタックの中で可能な限り低い位置に置かれるべきである。
	推奨される 個人情報提供拒否の結果	エンティティは、ユーザーが必須および任意の個人情報の提供を拒否した場合の結果について、ユーザーに簡潔で明確な通知を行うべきである
	推奨される属性要求クエリ	デジタルアイデンティティ管理機能を行うエンティティは、ユーザーが自分の属性とその使用方法に関する独自の要件を文書化し伝える機会を永続的に提供するべきである。エンティティはユーザーが自分の属性を共有することに同意するよう求められる前に、 要件に関するそれらのコミュニケーションに対して誠実な応答を提供するべきである

出所）
1 https://idefregistry.edufoundation.kantarainitiative.org/idef-knowledge-base/best-practices

凡例 ■：Trusted Web との関連があると考えられる項目 ■：Trusted Web との関連が薄いと考えられる項目

IDESG Standards Registry & Inventory

IDESG Standards Registry & Inventory とは、IDESGによって指定された各基準のリストである。認証は「SAML」「OpenID Connect」、認可は「OAuth 2.0」、リスクマネジメントは「NIST SP 800-37」、セキュリティ・プライバシー管理は「NIST SP 800-53」、情報セキュリティマネジメントは「ISO 27002」がそれぞれ指定されている[1,2]

IDESG Standards Registry & Inventoryで指定された標準

SAML		• XMLをベースにしたシングルサインオンを実現するためのフェデレーション形式のプロトコルの仕様
NIST SP 800-37		• 情報システムのライフサイクルにそったリスクマネジメントフレームワークを提供するドキュメント
NIST SP 800-53		• セキュリティとプライバシーの管理策の包括的かつ柔軟なカタログ • システムの影響レベル（低、中、高）ごとにセキュリティ管理ベースラインと、影響レベルに関係なくシステムに適用できるプライバシーベースラインを提供
OpenID Connect 1.0		• JSONをベースにしたシングルサインオンを実現するためのフェデレーションの形式のプロトコルの仕様
OAuth 2.0 認証フレームワーク (RFC 6749)	RFC 6750	OAuth 2.0 承認フレームワーク: ベアラー トークンの使用
	RFC 6819	OAuth 2.0 脅威モデルとセキュリティに関する考慮事項
	RFC 7009	OAuth 2.0 トークンの取り消し
	RFC 7591	OAuth 2.0 動的クライアント登録プロトコル
	RFC 7592	OAuth 2.0 動的クライアント登録管理プロトコル
	RFC 7636	OAuth パブリック クライアントによるコード交換の証明キー
ISO 27002		• 情報セキュリティマネジメントのベストプラクティスを提供するドキュメント

出所）
1 https://www.idesg.org/The-ID-Ecosystem/Registry.html
2 https://www.intellilink.co.jp/column/security/2019/111900.aspx

凡例 大項目 : 小項目 : 概要

米国
カナダ

（参考） IDEF Registry

IDEF Registry[1]はオンラインアイデンティサービスプロバイダー、およびアイデンティティクレデンシャルを認証するアプリケーションの所有者/運用者のための単一のウェブプレゼンスであり、登録を希望するサービスは自ら申請し、自己評価をする

IDESG Registryの登録状況

サービス名	概要	コアオペレーション
Authen2cate	• クラウド、Web、VPN、およびモバイル リソースにシングルサインオン (SSO)、多要素認証、およびアイデンティティ 管理サービスを提供する、フルサービスのセキュリティで保護されたクラウド ベースの アイデンティティ管理ソリューション	登録 / クレデンシャリング / 認証 / 認可 / 仲介
MYDIGIPASS	• MYDIGIPASS はアイデンティティの証明、認証、フルフィルメント、および強力な認証サービスを提供する包括的なデジタルアイデンティティ管理ソリューション • ハードウェアトークンやモバイルアプリなど、複数のタイプのオーセンティケーターをサポート	登録 / クレデンシャリング / 認証
Persona Trust	• 公証人および認定された信頼できるエージェントによるオンラインリモート電子身元証明を世界中で提供	登録
Identity Gateway	• 米国の退役軍人、第一対応者、およびその他の指定されたグループ (資格のある当事者) のメンバーに、リモートでアイデンティティを確認するためのシンプルで安全な方法を使用して、完全なエンドツーエンドのアイデンティティの証明および資格情報管理サービスを提供	登録 / クレデンシャリング / 認証
Norton Secure Login	• FICAM*1 認定のクレデンシャル サービス プロバイダー (CSP) ID プロバイダー サービスであり、保証レベル (LOA) 1、2、および 3 のすべての ID 証明、強力な認証機能、および規制された業界の認定と要件を満たす高保証認証を提供	登録 / クレデンシャリング / 認証
MorphoTrust eID	• 運転免許証のトラストを受け継ぐ、eGovサービス用の消費者管理型オンラインID	登録 / クレデンシャリング / 認証 / 認可
PRIVO-Lock and the PRIVO iD Platform	• ファミリーフレンドリーなシングルサインオン機能をもつアイデンティティと同意の管理製品およびサービス • 企業が合法的に若年層の消費者と直接取引することを可能にする	登録 / クレデンシャリング / 認証 / 認可 / 仲介
Direct Certificates	• ダイレクトアドレスのデジタル証明書とダイレクト組織証明書を提供 ※ダイレクトアドレスは XXXX@AA.com のような直接個人に紐づくもの	登録 / 資格証明
PDS:Authenticator	• リストに記載（最終更新2016年）があったが、現在は異なるサービスとなっている模様（TozID Authenticator）	認証 / 登録 / クレデンシャリング / 認可 / 仲介
UMBC Retriever Stories	• メリーランド大学ボルチモア校のコミュニティ (同窓生、教職員、学生、地域コミュニティの友人) が UMBC 内外での経験を共有するためのオンライン スペース	認可 / クレデンシャリング / 資格

*1 FICAM：Federal Identity, Credential and Access Management は、共通のICAM（Identity, Credential, and Access Management ）プロセスを設計、計画、実行するための連邦政府の企業向けアプローチである。企業の アイデンティティプロセス、プラクティス、ポリシー、および情報セキュリティ規則を提供する

出所）
1 https://idefregistry.edufoundation.kantarainitiative.org/registry/

NIST SP-800-63の構成

SP-800-63 とは2017年6月NIST（米国国立標準技術研究所）が発表した、デジタルアイデンティティサービスを実装する連邦政府機関向けの技術要件であり、特にデジタル認証で使用するためのアイデンティティの登録と検証について重点が置かれているドキュメントである。連邦政府機関向けの技術要件であるため、民間企業等が順守すべき標準ではないものの、連邦政府機関以外の組織が参照する行為は自由である。各保証レベルの選択方法を記載した SP 800-63-3 Digital Identity Guidelines[1,2] / 身元確認保証レベル（IAL）を規定する SP 800-63A /当人認証保証レベル（AAL）を規定する SP 800-63B / 連携情報保証レベル（FAL）を規定する SP 800-63C の4文書で構成される[3,4]

NIST SP-800-63の構成

SP 800-63-3 Digital Identity Guidelines	• 一般的な Identity Framework および、デジタルシステムにおける Authenticator, Credential, Assertion の利用について概観し、リスクベースプロセスに基づく各 Assurance Level の選択方法について述べている
SP 800-63A Enrollment and Identity Proofing	• ユーザーが申請者として新規登録する際に、クレデンシャルサービスプロバイダーが行う本人確認の強度を示す身元確認保証レベル（IAL : Identity Assurance Level ）のそれぞれのレベルにおける要件を記載している
SP 800-63B Authentication and Lifecycle Management	• 既に登録済みのユーザーがログインする際の認証プロセス（単要素認証・多要素認証、認証手段）の強度を示す当人認証保証レベル（AAL : Authenticator Assurance Level）のそれぞれのレベルにおける要件を記載している
SP 800-63C Federation and Assertions	• OpenID Connect ID Token や SAML Assertion などの Assertion のフォーマットやデータやり取りの仕方など認証連携の強度を示す連携情報保証レベル（FAL : Federation Assurance Level）のそれぞれのレベルにおける要件を記載している

出所）
1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
2 https://www.jipdec.or.jp/eventseminar/event/u71kba0000009o56-att/nist_sp_800-63-3.pdf
3 https://www.nccoe.nist.gov/sites/default/files/2023-01/digital-identity-guidelines-kickoff-revision-4-presentation.pdf
4 https://www.jipdec.or.jp/library/report/20171127.html

米国
カナダ

SP 800-63A : Enrollment and Identity Proofing

SP 800-63A[1,2] は、ユーザーが申請者として新規登録する際にクレデンシャルサービスプロバイダーが行う本人確認の強度を、身元確認保証レベル（ Identity Assurance Level : IAL ）として、IAL1 IAL2 IAL3 の3段階で整理し要件を定義している文書である[3,4]

IAL : Identity Assurance Levels の概要と要件

IAL1	本人確認不要、自己申告での登録でよい
IAL2	サービス内容により識別に用いられる属性をリモートまたは対面で確認する必要がある
IAL3	識別に用いられる属性を対面で確認する必要があり、確認書類の検証担当者は有資格者が行う必要がある

Requirement	IAL1	IAL2	IAL3
存在	要件なし	対面および非監視下のリモート	対面および監視下のリモート
収集	要件なし	Identity Resolution に必要最低限な範囲に限定する データ照会の助けになる属性の収集を含めてもよい	IAL2 に同じ
エビデンス*1	収集しない	Issuing Source が実施した Proofing および検証の強度により以下の組み合わせとなる • 1つの SUPERIOR もしくは STRONG なエビデンス • 2つの STRONG なエビデンス、もしくは1つの STRONG なエビデンスと2つの FAIR なエビデンス	• 2つの SUPERIOR なエビデンス もしくはIssuing Source が実施した Proofing および検証の強度によって以下の組み合わせとなる • 1つの SUPERIOR もしくは STRONG なエビデンス、 • 2つの STRONG なエビデンスと1つの FAIR なエビデンス
正当性確認	確認なし	それぞれのエビデンスを、エビデンスと同じ強度のプロセスで確認しなければならない	IAL2 に同じ
検証	検証なし	STRONG の強度のプロセスによって検証する	SUPERIOR の強度のプロセスによって検証される
住所確認	要件なし	必須。Enrollment コードを任意の Address of Record に送信、通知は Enrollment コードとは別の経路で送信する	必須 Proofing の通知は郵便住所に対して送信する
生体情報収集	なし	任意	必須
セキュリティ管理	N/A	SP 800-53*2 Moderate 基準 (もしくはそれ相当の連邦 / 業界標準)	SP 800-53 High 基準 (もしくはそれ相当の連邦 / 業界標準).

*1 エビデンスの強度はSP800-63A 5.2 Validating Identity Evidenceにて **Superior Strong Fair Weak Unacceptable** の5種類に定義されている
*2 「SP 800 53 ：情報システムおよび組織のためのセキュリティ管理策とプライバシー管理策」はセキュリティとプライバシーの管理策の包括的かつ柔軟なカタログである。システムの影響レベル（低、中、高）ごとに3つのセキュリティ管理ベースラインと、影響レベルに関係なくシステムに適用できるプライバシーベースラインを提供している

出所） 1 https://openid-foundation-japan.github.io/800-63-3-final/sp800-63a.ja.html
2 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf
3 https://www.jipdec.or.jp/library/report/20171127.html
4 https://www.jipdec.or.jp/library/report/20201215_01.html

SP 800-63B : Authentication and Lifecycle

SP 800-63B[1]は、既に登録済みのユーザーがログインする際の認証プロセス（単要素認証・多要素認証、認証手段）の強度を当人認証保証レベル（Authenticator Assurance Level : AAL）として3段階（AAL1 AAL2 AAL3）の整理で要件を定義しているドキュメントである[2,3]

AAL : Authenticator Assurance Level の概要と要件

AAL1	セキュアな認証プロトコルを用いた単一要素認証（例：パスワード）でよい
AAL2	承認された暗号通信技術*1を用いたセキュアな認証プロトコルを用いて、二つの異なる認証要素の保持・管理していることの証明に基づく多要素認証が必要である
AAL3	承認された暗号通信技術を用いたセキュアな認証プロトコルを用いて、二つの異なる認証要素の保持・管理していることの証明に加え、Verifier Inpersonation（検証者偽装）*2 耐性のあるハードウェアベース（例：パスワード等でアクティブにしたIPhone のFace ID）の認証要素であることを（鍵所有証明：Proof of Possession*3) を必要とする

要件	AAL1	AAL2	AAL3
許可されている Authenticator タイプ	記憶シークレット /ルックアップシークレット /アウトオブバンド /単一要素OTPデバイス /多要素OTPデバイス/単一要素暗号ソフトウェア /単一要素暗号デバイス /多要素暗号ソフトウェア /多要素暗号デバイス	• 多要素 OTP デバイス • 多要素暗号ソフトウェア • 多要素暗号デバイス • ルックアップシークレット/アウトオブバンド /単一要素 OTP デバイス /単一要素暗号ソフトウェア /単一要素暗号デバイス のいずれか2つの組み合わせ	• 多要素暗号デバイス/単一要素暗号デバイスを記憶シークレットと併用 • 多要素OTPデバイス(ソフトウェアまたはハードウェア) を単一要素暗号デバイスと併用 • 多要素 OTP デバイス(ハードウェアのみ) を単一要素暗号ソフトウェアと併用 • 単一要素 OTP デバイス(ハードウェアのみ)を多要素暗号ソフトウェア と併用 • 単一要素 OTP デバイス(ハードウェアのみ)を単一要素暗号ソフトウェア 及び記憶シークレットと併用
FIPS 140*4 確認	Level 1 (政府機関のVerifier)	Level 1 (政府機関のAuthenticator及びVerifier)	Level 2 総合 (多要素Authenticator) Level 1 総合 (Verifier及び単一要素暗号デバイス) Level 3 物理セキュリティ (全てのAuthenticator)
再認証	30 日	12 時間 または 30 分 の非活動 再認証に用いるにはどちらかの認証要素でもよい(MAY)	12 時間 または 15 分 の非活動 両方の認証要素をつかうものとする(SHALL)
セキュリティ統制	SP 800-53 低度のベースライン(または等価)	SP 800-53 中度のベースライン(または等価)	SP 800-53 高度のベースライン(または等価)
中間者攻撃耐性	必須	必須	必須
検証者なりすまし耐性	不要	不要	必須
検証者危殆化耐性	不要	不要	必須
リプレイ耐性	不要	必須	必須
認証意図	不要	推奨	必須
記録保持ポリシ	必須	必須	必須
プライバシー統制	必須	必須	必須

*1 FIPS （Federal Information Processing Standardization : 連邦情報処理標準） ないしは NIST Recommendation に 指定もしくは採用されているアルゴリズムおよび技術を指す
*2 登録済みユーザーの情報を取得しなりすますために攻撃者が認証プロトコルで検証者になりすますシナリオを指す
*3 アクセストークンの発行対象者とアクセストークンの利用者が同一であることを API アクセス時に確認することで、不正にアクセストークンを取得した攻撃者によるアクセスを防ぐという概念
*4 FIPS 140（Federal Information Processing Standardization 140）は米国政府の暗号モジュールに関するセキュリティ要件の使用を規定する標準規格

出所）1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
2 https://openid-foundation-japan.github.io/800-63-3-final/sp800-63c.ja.html
3 https://www.jipdec.or.jp/library/report/20171127.html

米国
カナダ

（参考）AAL要件の各項目の概要について

許可されている Authenticator タイプ[1]

Authenticator	概要	例
記憶シークレット	ユーザー自身が記憶するもの	パスワード、PIN等
ルックアップシークレット	認証したい人と認証情報を払い出す側との間で共有されるシークレット	乱数表、リカバリーコード等
アウトオブバンド	別経路を介して安全に通信できるもの	SMSによる認証コードの送信、QRコード読み取り
単一要素OTPデバイス	何らかのアクティベーションを必要としないOTP生成デバイス	Touch IDや、マスターパスワードによりアクティベートする必要のないOTPアプリ
多要素OTPデバイス	単一要素OTPデバイスに、さらに二要素目の入力によるアクティベーションを追加したもの	Touch IDや、マスターパスワードによりアクティベートする必要のあるOTPアプリ
単一要素暗号ソフトウェア	単一要素ソフトウェア暗号Authenticatorは、ディスクあるいは"ソフト"媒体に記録された暗号鍵	パスワード保護のない端末ごとのクライアント証明書
多要素暗号ソフトウェア	単一要素暗号ソフトウェアに、二要素目の入力によるアクティベーションを追加したもの	指紋認証を行うことで有効化されるクライアント証明書
単一要素暗号デバイス	保護された暗号鍵を用いて認証を行うハードウェアデバイスを指す	FIDO U2F のUSBキー等
多要素暗号デバイス	単一要素暗号デバイスに、二要素目の入力によるアクティベーションを追加したもの	指紋認証などによってアクティベートを行わなければ使用できないFIDOのUSBキー等

出所）
1 2021/07/06 次世代認証連携検討作業部会「学認でのAAL2について」

AAL各要件の概要[2,3]

各要件名	概要
再認証	登録済みユーザのセッションは定期的な再認証が行われる必要がある
セキュリティ統制	SP 800-53 または等価な連邦政府機関 あるいは業界標準で定義されているセキュリティ統制の高度な基準の中から適切に調整されているセキュリティ統制を採用する必要がある
中間者攻撃耐性	攻撃者が2つの通信当事者の間に配置され、それらの間を移動するデータを傍受および/または変更する攻撃への耐性
検証者危殆化耐性	Verifierが安全に検証できない状況に陥ることへの耐性
リプレイ攻撃耐性	攻撃者が以前にキャプチャしたメッセージを(正当な要求者と検証者の間で)再生して、その要求者になりすまして検証者に、またはその逆を行うことができる攻撃への耐性
認証意図	認証プロセスはにおいてSubjectが明示的に各認証や再認証の要求に応じる必要がある場合、その意図を明らかにする
レコード保持ポリシー	準拠法,規則,及び任意の国立公文書記録管理局(NARA)のレコード保持スケジュールを含むポリシに合致するそれぞれのレコード保持ポリシに従う必要がある
プライバシー統制	SP 800-53で定義された適切に調整されたプライバシコントロール、または他の等価な業界標準を採用する必要がある

出所）
2 https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3.html
3 https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.ja.html

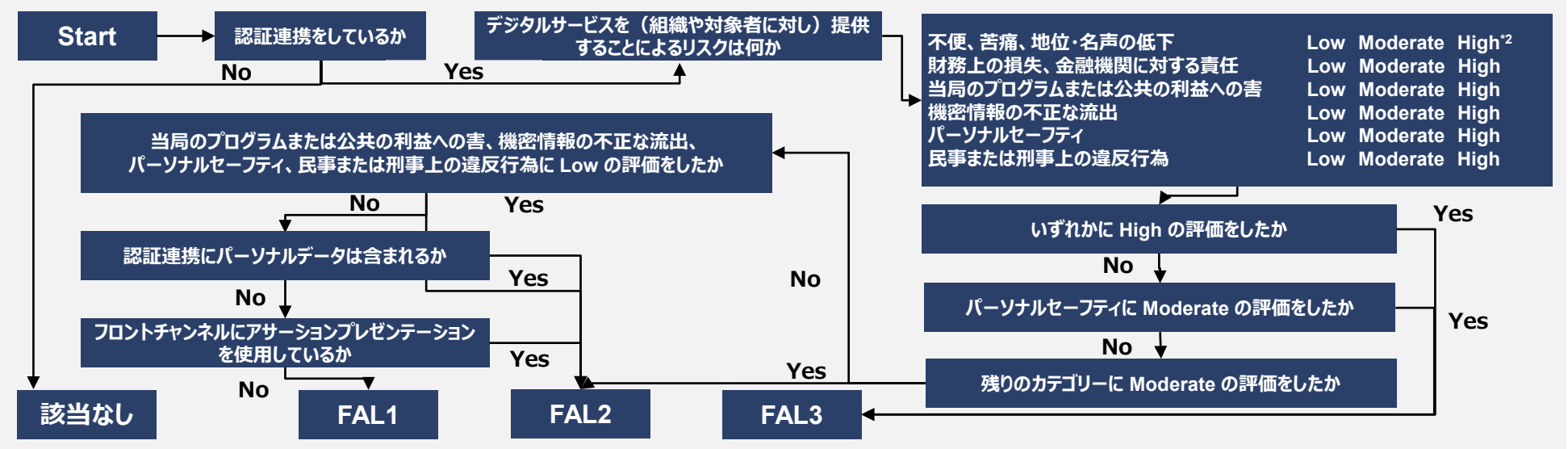
米国
カナダ

SP 800-63C : Federation and Assertions

SP 800-63C[1]は、OpenID Connect ID Token や SAML Assertion などの Assertion[*1] のフォーマットやデータやり取りの仕方といった認証連携の強度を、連携情報保証レベル（Federation Assurance Level : FAL）として3段階（FAL1 FAL2 FAL3）の整理で要件を定義しているドキュメントである[2,3,4,5]

FAL : Federation Assurance Level の概要とレベル選択フロー

FAL1	アイデンティティプロバイダが承認された暗号技術を用いて Assertion に署名する必要がある
FAL2	署名に加え対象認証機関のみが復号可能な暗号化を行う必要がある。個人情報が Assertion に含まれる場合はFAL2以上になる
FAL3	FAL2に加え、Holder-of-Key Assertion（ユーザごとの鍵と、アイデンティティプロバイダーが発行したAssertionを紐づけて認証機関に送り、認証機関はユーザがそのAssertionに紐づいた鍵を持っているか（ユーザの正当性）を確認する）を用いる必要がある



*1 アイデンティティプロバイダが認証機関（RP）に送る認証結果データ
*2 各選択肢の影響度はFIPS199「連邦政府の情報および情報システムに対するセキュリティ分類規格」に準拠している。 Low：「限定的な悪影響」 Moderate：「重大な悪影響」 High：「致命的・壊滅的な悪影響」

出所） 1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf
2 https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.ja.html
3 https://www.jipdec.or.jp/library/report/20171127.html
4 https://www.ipa.go.jp/files/000025321.pdf
5 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

SP 800-63-4

2022年12月、SP 800 63-3 が発表された2017年当時から現在に至るまでのデジタル環境の変化に対応するため、「公平の向上」「利用者の選択の重視」「不正行為や高度な脅威の防止」「アドレスの実装に関する教訓」を目的としたドラフト（SP 800-63-4）[1,2,3,4]の公開がされている。最終化は2024年春-夏頃を予定しており、「Note to Reviewers」という項目を設け、2023年3月までドラフトへのコメントを募集している[5]

NIST SP-800-63-4 改訂の目的

公平性の向上	• 63-3 では組織のリスクマネジメントの視点のみであったが、個人・コミュニティへのリスクマネジメントも求める記載 • デジタルサービスを受ける資格のある人すべてにサービスを提供することの難しさ等「任務遂行のリスク」について記載 • 一部の人口に対して不当な扱いとならないか継続的なモニタリングを求める記載
利用者の選択の重視	• 顔認証技術など生体認証は利用できない人も存在するため（例：農作業に従事し指紋が消えてしまった）、そのような人たちであってもサービスが利用できるように複数の authenticator オプションを用意する必要があると記載
不正行為や高度な脅威の抑止	• 新しい攻撃を考慮したリスクと脅威モデルの更新 • フィッシングに強い認証の新しいオプションの提供、登録プロセスに対する自動的な攻撃を防ぐための要件の導入について記載 • Verifiable Credentials や Mobile driver’s licenses などの新しい技術の導入も記載
アドレスの実装に関する教訓	• 2020年に行ったフィードバックから得た指摘事項への反映として、「FAL の見直し」「Trusted Referees の詳細」「アイデンティティ属性バリデーションソースの明確化」「住所確認要件の改善」について記載

出所）
1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.ipd.pdf
2 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63A-4.ipd.pdf
3 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.ipd.pdf
4 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63C-4.ipd.pdf
5 https://www.nist.gov/identity-access-management/roadmap-nist-special-publication-800-63-4-digital-identity-guidelines

SP 800-63-4 [1]「Note to Reviewers」で募集されたコメント

本人確認と登録 **Identity Proofing and Enrollment**	• 顔認証を必要としない無人の完全リモートのアイデンティティ証明ワークフローの追加する際に、それはどのような技術・方法によって実現されるのか • デジタルエビデンス（例：モバイルドライバーライセンス、Verifiable Credentials）をさまざまなアイデンティティ証明に統合する方法にはどのようなものがあるのか • CSP が不正検出、対応、および通知能力を確立し維持するための一連の要件を指定することの影響、利点、およびリスクは何か ➢ 基本的な規範的要件として組み込むべき既存の不正チェック（死亡日など）または不正防止技術（デバイスの指紋採取など）はあるか。あるとすれば、それらはどの程度の保証レベルで適用可能か？ ➢ 不正分析やリスクスコアリングのような新しい手法は、今後どのように研究・標準化され、ガイダンスに統合され得るのか ➢ これらの手法に付随して、プライバシーや公平性についてどのような配慮が必要か • 生体検知（Liveness detection）と入力データ攻撃検知（Presentation Attack Detection）のための現在のテストプログラムは、実装と技術の性能を評価するのに十分か否か • アイデンティティ検証のために提案された生体認証技術要件は、生体認証技術の実装にどのような影響を及ぼすのか
リスクマネジメント **Risk Management**	• デジタルアイデンティティのリスクを企業のリスクマネジメントと統合するためには、どういったガイダンスや指針を追加提供するべきか • 保証レベルの選択プロセスおよびデジタルアイデンティティリスクマネジメントモデルに、公平性・プライバシー・ユーザビリティの観点はどのように統合することができるのか • リスク分析および不正行為軽減技術は、それぞれのアイデンティティ保証レベルの選択にどのように統合されうるのか。また、全体的なアイデンティティリスクを軽減する能力について、どのように認定し定量化できるのか
認証とライフサイクル管理 **Authentication and Lifecycle Management**	• FIDOパスキー、Verifiable Credentials、モバイルドライバーライセンスなどの新しい認証モデルや技術は、ガイドラインで十分に取り上げられ、適切な対応がなされているのか。また関連するセキュリティ、プライバシー、ユーザビリティの潜在的な利点とリスクは何か • AAL2およびAAL3認証のガイドラインに定義されているフィッシング対策は明確かつ十分か • セッション管理のしきい値と再認証の要件は、エージェントや組織でどのように実装されているか。NISTは、アプリケーション、ユーザ、ミッションのニーズに基づいて閾値を提供もしくはセッションの長さをエージェントに委ねたりする必要があるか • 本編で提案された生体認証技術の性能要件は、生体認証技術の実世界での実装にどのような影響を与えるか
本人確認と登録 **Federation and Assertions**	• ガイドラインでこれまで議論されていなかったアイデンティティおよびプロビジョニング API の使用を考慮するために、どのような追加のプライバシー考慮事項（例：同意の取り消し、使用の制限）が必要になるか • FAL3の実用的な実装を可能にするために、更新されたテキストと「バインドされたオーセンティケータ」の導入の記載は明確か。また更新されたガイダンスに基づき、どのような複雑さや課題が予想されるか

出所） 1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.ipd.pdf

Pan-Canadian Trust Framework（PCTF）の概要

- 2020年11月、DIACC（カナダデジタル識別認証評議会）*1は、カナダの官民組織がデジタルアイデンティティを安全に活用するためのガバナンスモデルとして PCTF（Pan-Canadian Trust Framework）1.0 alpha[1]を発表した
- PCTFは、カナダのデジタルアイデンティティ管理における原則や基準、デジタルIDの作成、管理、提供に係る一連のプロセスなどを定義しており、デジタルIDに関係する公共・民間のステークホルダー、研究者などに参照されることを目的としている
- デジタルアイデンティティサービスがPCTFの基準に準拠しているかを判断する認証プログラムとして「Voilà Verified Trustmark Program」[2]を定めている

PCTFの構成要素

Informative 参考	Assurance Maturity Model		PCTFの各構成物が定める LoA の適切な分類方法について記載している
	用語集		PCTFで使用される用語の定義、例
	Model		PCTFのゴール、目標、文脈など
Specified 指定	プライバシー	認証	ログイン及び認証プロセスに関する基準の定義
		クレデンシャル	デジタルクレデンシャルのライフサイクル等に関しての基準を定義している
		デジタルウォレット	デジタルウォレットに関する要件・基準を定義している
		インフラストラクチャー	ITインフラの信頼性に関する要件・基準を定義している
		通知と同意	個人情報の収集、使用、開示に係る通知と同意の取得に関する基準の定義している
		検証済み組織	組織の識別、認証に関する基準とプロセス
		検証済み個人	自然人の識別、認証に関する基準とプロセス

*1 DIACC（カナダデジタル識別認証評議会）はデジタルIDソリューションとサービスを実現するための研究開発に取り組む政府・民間企業から構成される非営利組織である。

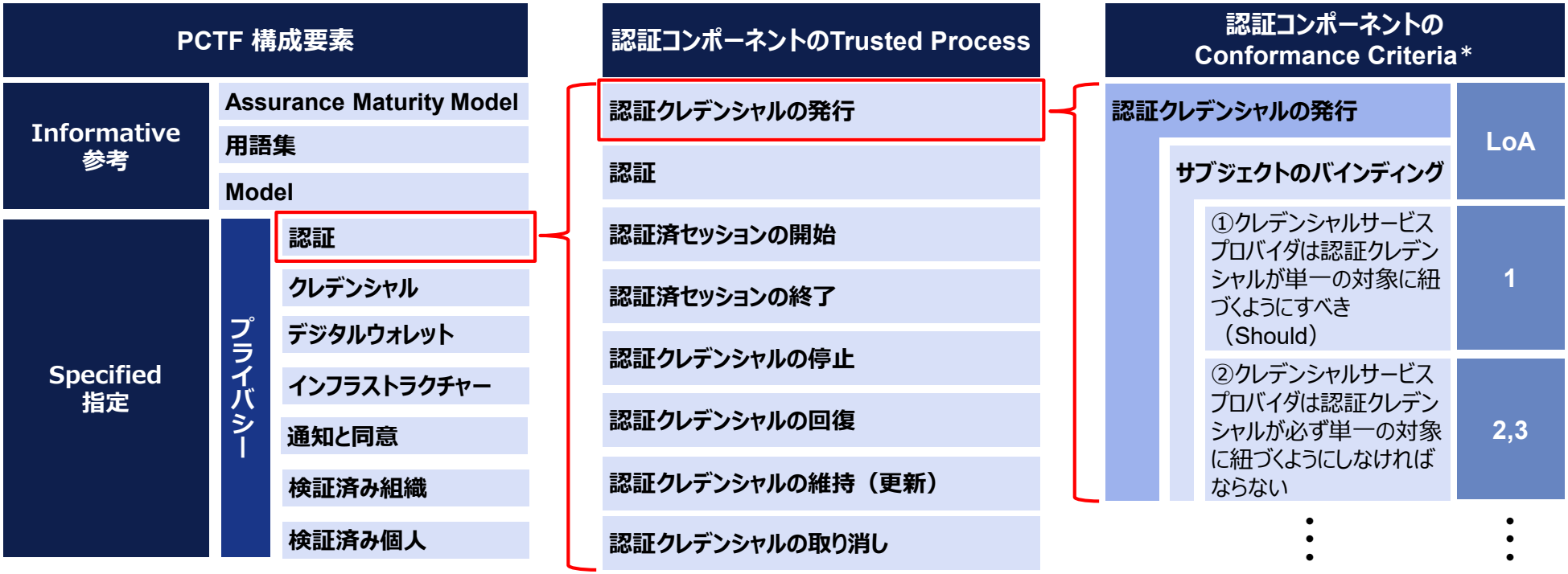
出所）
1 https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation_V1.0.pdf
2 https://diacc.ca/

米国
カナダ

Pan-Canadian Trust Framework（PCTF）の概要

PCTFは、各構成要素がそれぞれの領域（認証、クレデンシャル等）における細分化されたプロセス（Trusted Process）と、それに応じた適合基準（Conformance Criteria）を定め、LoAを算定する仕組みとなっている。最終的には各構成要素でのLoAをもって、Assurance Maturity Modelに定めるアプローチ方法によってサービス全体のLoAが決定される[1]

コンポーネントとプロセス、適合基準の対応関係（例：認証コンポーネント）



出所）
1 https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation_V1.0.pd

PCTF コンポーネント規定されるプロセス① デジタルウォレット[1]

Wallet Instantiation and Security Processes	デジタルウォレットの生成	• Verifierが検証可能なウォレットを作成するプロセス。作成には、携帯電話または携帯電話以外のデバイスへのソフトウェアのインストール、またはサーバーでのウォレットのインスタンスの生成が含まれる場合がある
	デジタルアイデンティティウォレットの登録	• 保有者が発行者、検証者、検証可能データレジストリにウォレットを登録するプロセス。登録完了後、Holderは、Issuer、Verifier、または検証可能データレジストリの登録サービスにより永続的に管理できる登録済みデジタルウォレットを持つことになる
	認証	• 所有者がクレデンシャルをデジタルアイデンティティウォレットにバインドするための認証管理を確立するプロセス。このバインドは、所有者がデジタルアイデンティティウォレットを管理し、そのウォレットにバインドされたクレデンシャルを所有、管理、提示する権限があることを保証する
Credential Management and Use Processes	VCの要求	• ウォレット所持者は発行者にクレデンシャルを要求するプロセス • クレデンシャル要求の前提条件として、デジタルアイデンティティウォレットの属性、検証済み人物の記録、およびバインド の記録を検証することで、要求の保証を強化することができる
	VCの保管	• 検証可能なクレデンシャルがデジタルアイデンティティウォレットで保護され保管されるプロセス • 高レベルの保証が必要な場合は、クレデンシャルを保護する前提条件としてのプロセスおよび技術を実装することができる
	VCの管理	• デジタル・ウォレットに保管されるクレデンシャルと属性 が正確かつタイムリーな情報を含むことを保証し、以下の操作を行うプロセス ➢ 更新：クレデンシャルのIssuerを通じて、VCの属性を最新にする手順 ➢ 失効の通知：IssuerがVCを失効させた際に、VCのHolderに通知する手順 ➢ 期限切れの通知：IssuerがVCの期限切れのタイミングでVCのHolderに通知する手順 ➢ 復元：IssuerまたはデジタルアイデンティティウォレットHolderがVCを復元するために使用する手順 ➢ 削除：デジタルアイデンティティウォレット所有者がVCを削除する手順 （※デジタルアイデンティティウォレットにバインドされたHolderのみが利用できる）
	VCの表示	• デジタルウォレットからクレデンシャルを取得し、所有者に表示するプロセス
	VCのレンダリング	• セキュアなクレデンシャルの特定の状態または条件を確立し、人間が読み取り、理解できるフォーマットで表示するプロセス
	証明の提示	• デジタルウォレットはVerifierの証明要求を満たすために、保有者（ウォレットの所有者） のクレーム（署名済みクレデンシャル）の証明を互換性のあるフォーマットでVerifierに提示できなければならない ➢ 互換性は主に「クレデンシャルの形式」「署名スキーム」「要求されたクレームごとに許容されるIssuer」「**選択的開示の可否**」を指す • 理想的にはウォレット（及びIssuer）は固定された1回の交換だけでなく、ウォレットと検証者双方のポリシーを満たす双方向のネゴシエーションプロセスをサポートすることが望ましい • 証明(Proof)とは、要求されたクレームを改ざん不可能な状態で提示し、検証者が適切な暗号処理により検証することができるものである。選択的開示がサポートされる場合、Verifierが要求した特定の請求項のみを共有することができるようにせねばならない。そうでない場合は証明要求を満たすために必要なクレデンシャル一式を共有しなければならない • 証明書要求を受理する前に、保有者は要求された情報をVerifierに送ることに同意しなければならない。Holderがアクセスできる監査ログには、トランザクションの時間、要求され、提示されたクレーム、Verifierの詳細、Success Status 、および提供された場合は受領が記録されなければならない。**オプションとして、監査ログは永続し、同意を確認し取り消す方法を提示することができる**
Consent Processes		• PCTFの構成要素における「通知と同意 (前スライドを参照)」にて規定される

出所）
1 https://diacc.ca/wp-content/uploads/2022/05/PCTF-Digital-Wallet-Component-Overview-Draft-Recommendation-V1.0.pdf

凡例 大項目 : 小項目 : 概要

PCTF コンポーネントで規定されるプロセス② 検証済み個人[1]

ソースの確立 **Establish Sources**	• アイデンティティの検証および/または確認に使用できるアイデンティティ証拠のソース、および これらのソースの保証を決定するために実施されるプロセス • 通常、デジタルアイデンティティシステムは、特定のコンテキストでアイデンティティを検証する要件をサポートし、目標確保レベルを満たすために、さまざまなソースを使用する
アイデンティティの解決 **Identity Resolution**	• アイデンティティ情報の使用によって対象集団内の対象者の一意性を確立するプロセス • 責任ある機関は、アイデンティティ属性の観点から独自のアイデンティティ解決要件として特定の集団内の他の対象者から対象者を一意に識別するために必要な一連のアイデンティティ属性を指定し定義する
アイデンティティの確立 **Identity Establishment**	• 後続のプログラム、サービス、および活動において他者が依拠しうるアイデンティティの証拠（Verified Person Record）をプログラム／サービス集団内に作成するプロセス
アイデンティティバリデーション **Identity Information Validation**	• 権威ある当事者*1によって確立されたID情報と比較して、対象に関するアイデンティティ情報の正確性を確認するプロセス • 「ソースの確立」プロセスから取得したエビデンスに基づいて、主張されたアイデンティティ情報が存在し、有効であるかどうかを判断する • このプロセスは、ユーザーが自身のアイデンティティ情報を使用していることを保証するものではないことに注意する。対象者が使用しているアイデンティティ情報は、権威あるソースからのアイデンティティエビデンスと比較した場合に正確であることのみを保証する
本人確認 **Identity Verification**	• 提示された本人確認情報がユーザーの管理下にあることを確認するプロセス • 本人確認とは関係のない個人情報を使用する場合があることに留意すべきである • 「ソースの確立」で確認されたエビデンス、およびユーザとのインタラクションから取得されたアイデンティティエビデンスを使用して、主張されたアイデンティティがユーザに属するかどうかを判断することができる
エビデンス検証 **Evidence Validation**	• 提示されたエビデンス（物理的または電子的なもの）が受け入れられる、または認められるかを確認するプロセス
本人提示 **Identity Presentation**	• ある人が時間的に連続した存在であることを動的に確認するプロセス
アイデンティティの維持 **Identity Maintenance**	• 対象者について記録されたアイデンティティ情報が、要求に応じて正確、完全、かつ最新であることを保証するプロセス • このプロセスは、以前に実施したアイデンティティ情報の検証およびアイデンティティ検証の有効性に影響を与える可能性のある事象を扱う 例：被検証者を立証するために使用したエビデンスが変更・期限切れ・取り消しとなり、検証者記録が無効となった場合など

*1 権威ある当事者：参加者（PCTF準拠組織）が、依拠当事者に保証レベルによってアイデンティティ情報またはアイデンティティエビデンスを提供するロール

出所）1 https://diacc.ca/wp-content/uploads/2020/09/PCTF-Verified-Person-Component-Overview-Final-Recommendation_V1.0.pdf

凡例 大項目 ：概要

米国
カナダ

PCTF コンポーネント規定されるプロセス③ 検証済み組織[1]

組織アイデンティティの確立 **Organizational Identity Establishment**	• 組織アイデンティティのレコードを作成するプロセス • 他の関係者は、その後のプログラムやサービスの提供のために、このレコードに依拠することができる • 特定の対象集団に属する組織を一意に区別するためのアイデンティティ情報が含まれ、一意性の程度は責任権限者以外の関係者を満足させるものではない可能性がある
組織アイデンティティの発行 **Organizational Identity Issuance**	• 組織アイデンティティのエビデンスを作成し、組織に提供するプロセス • 組織アイデンティティの基礎的エビデンスは、公共部門組織レジストリによって発行される • 組織アイデンティティの文脈的エビデンスは、公的機関または民間企業によって発行される
組織アイデンティティの解決 **Organizational Identity Resolution**	• 組織のアイデンティティ情報を使用することにより、集団の中で組織を固有なものとして確立するプロセス • 各プログラムまたはサービスが、その管轄内で組織のアイデンティティの解決を達成するために必要な組織のアイデンティティ属性のセットを指定する
組織アイデンティティのバリデーション **Organizational Identity Validation**	• 責任ある機関によって確立された組織に関するアイデンティティ情報の正確性を確認するプロセス • 文脈的/基礎的なエビデンスを使用して、主張された組織のアイデンティティが存在し、有効であることを判断する • このプロセスの意図は、組織のアイデンティティ情報が目的に対して正確かつ信頼できることを保証するための確立された方法を、依拠当事者に提供すること
組織アイデンティティの検証 **Organizational Identity Verification**	• 提示された組織アイデンティティ情報が、提示を行う組織に関連することを確認するプロセス • 検証は、組織アイデンティティのバリデーションとは別のプロセスであり、異なる方法を採用し、アイデンティティに関連しない組織情報の収集を必要とする場合がある
組織アイデンティティの維持 **Organizational Identity Maintenance**	• 組織について記録されたアイデンティティ情報が、必要な限り正確、完全、かつ最新であることを保証するプロセス • 組織のアイデンティティ情報に変更が生じた場合にアイデンティティ情報を開示する、アイデンティティ通知もプロセスに含まれる。なおアイデンティティの通知は、アイデンティティ情報がリスク要因にさらされたことを示す場合もある
組織アイデンティティのリンク **Organizational Identity Linking**	• 同じ組織のアイデンティティ情報の2つ以上のセット/インスタンスを関連付けるプロセス

出所）
1 https://diacc.ca/wp-content/uploads/2020/09/PCTF-Verified-Organization-Component-Overview-Final-Recommendation-V1.0-1.pdf

PCTF コンポーネントで規定されるプロセス④ 通知と同意[1]

通知文の作成 **Formulate Notice**	• 収集される情報について説明するステートメントを生成するプロセス • 必要な情報は、適用される法律、政策及び契約上の要件に基づいており以下を含むものの限定はされず、対象者には通知の形で提示される 1. どのような個人情報が収集、使用、または開示されるのか 2. 情報の収集、使用、開示、または保存の目的 3. 情報の開示先（状況に応じて、組織、個人、またはその両方） 4. 要求された個人情報の情報源（開示組織または対象者） 5. 情報の取扱い及び/又は保護方法 6. 通知が適用される期間 7. 通知が適用される管轄または当局の下 8. 収集に関する対象者の質問に答えることができる権限を有する者の連絡先 9. 関連する管轄区域の関連する法律、政策、および規制によって要求される追加情報
同意の要求 **Request Consent**	• 対象者に通知を提示し、対象者が通知の内容に基づいて同意を受け入れる/拒否するための機能を提供し、意味のある同意を決定するプロセス • 同意を要求された対象者が、同意する権限を有することを確認することを意図している • このプロセスは、対象者を認証し、対象者の身元を確認し、同意の意思決定を行う対象者の権限を確認するために、PCTF の他のコンポーネント（例：認証、検証された人物、検証された関係）で定義されたトラステッドプロセスを利用する
同意の記録 **Record Consent**	• 通知条件と対象者の同意判断の記録を作成するプロセス • **記録は永続的。対象者がその後同意を取り消した場合でも、履歴参照用に保持されることがある。**保持は法律または規制の対象となることがある • 保存される可能性のある通知条件の例には、「対象者に関する情報」「同意を提供した公認機関」「通知が提示された日時」「提示された通知のバージョン」など、保存される可能性のある同意決定情報の例としては「対象者が行った決定とともに通知条件」「同意した日時」「同意の有効期限」がある • **同意の記録には、対象者が共有に同意したデータの種類に関する情報を保管すべきであるが、対象者のデータを含むべきではない** • 通知条件と同意の決定情報の保管/保持は、記録された同意が適用される法域の法律及び規則に従わなければならない • 同意の決定が保存されると、同意の決定に関連する当事者に同意の決定が通知される • 同意の記録は、関連する法規制に準拠する限り、不要になった時点で破棄することができる
同意の管理 **Manage Consent**	• 同意の決定のライフサイクルを管理するプロセス ➢ **同意の確認** 保存された同意の決定の詳細を対象者および承認された審査担当者*1が見ることができ、 適切かつ適用可能なプライバシー慣行に従い、関連する法律、規則、およびポリシーを尊重する ➢ **同意の更新** 対象者又は認定機関が、目的の変更又は前回の同意から状況が変化する可能性のある期間が経過したことに基づき、以前に保存した同意の決定から修正した同意の決定を確立する場合 設定された有効期限に基づき、同意の決定を失効させること。- **対象者が積極的に同意を撤回することを含む** ➢ **同意の取り消し** 他の事象（例:詐称等により同意が不正であることが判明した場合など）に起因する同意を取り消す状況 • 同意の管理プロセスは、「同意の記録」プロセスを通じて保存することが可能

*1 承認された審査者は、同意の影響を受ける参加者（すなわち、開示組織、要求組織、規制機関又は 政策担当者）である。また、監査のための規制機関や監視委員会も含まれる

出所）

1 https://diacc.ca/wp-content/uploads/2020/09/PCTF-Verified-Organization-Component-Overview-Final-Recommendation-V1.0-1.pdf

Voilà Verified Trustmark Program

- **2022年10月、DIACCはデジタルアイデンティティサービスがPCTFの基準に準拠しているか判断する認証プログラム「Voilà Verified Trustmark Program」[1,2]を正式に開始した**
- **4名の専門家のボランティア*1によって構成される Voilà Verified Trustmark Oversight Board (TOB) が独立して運営を行う**
- **アセッサー・Readiness advisor によって認定されたサービスは3年間有効なトラストマークが付与され、「Voilà Verified Program Public Directory」に公開される**

認定プロセス

申請

- 興味のあるサービスまたはネットワーク事業者は、Voila Verifiedプログラムに登録し、アプリケーション・パッケージを提出
- アプリケーション・パッケージはTOBによって審査され、審査段階への移行を確認
- 申請者がDIACC認定アセッサーを選択し、アセスメントを実施

アセスメント

- DIACC認定アセッサーが、PCTFのコンポーネントに対する申請者のサービス/ネットワークの適合性を判断する第三者評価を実施
- TOBは、アセスメントレポートを独自に品質評価し、申請者を認定するかを最終的な決定を行う

認定

- DIACCは、認定したサービスやネットワーク事業者に3年間のTrustmarkを付与し、毎年監督アセスメントを実施
- 検証書類、ライセンス契約書、トラストマークロゴを提供
- 認定したサービスやネットワーク事業者はVoilà Verified Program Public Directoryに記載される

認定されたサービス

認定事業者	概要	認定日	Role	トラストマーク
Kimble and Associates LLC (DBA Kuma)	プライバシーとセキュリティに関するコンサルティングファーム	2022/06/20	Assessor Readiness advisor	
Schellman Compliance LLC	IT 監査とコンプライアンス証明を提供する会社	2022/10/20	Assessor Readiness advisor Tasting Laboratory	
CHYP USA, Inc. (Consult Hyperion)	デジタルアイデンティティ、インターネット上のトラストを扱うコンサルティングファーム	2023/01/27	Readiness advisor	

*1 政府情報セキュリティ・サイバーセキュリティ担当副大臣補佐、seedot(サイバーセキュリティ企業)CEO、Business Law Group, Vancouver（弁護士事務所）シニアパートナー、オーストリア工科大学デジタル安全セキュリティセンターテーマ別コーディネーター/シニアエンジニアおよび研究プロジェクトマネージャー の4名からなる

出所）
1 https://diacc.ca/voila-verified/
2 https://diacc.ca/2022/10/18/voila-verified-trustmark-program-is-live-duty-of-care-a-top-priority/

（補足）NIST SP 800-63とPCTFの比較

	NIST SP 800-63-3		PCTF[1]	
本人確認（ID Proofing）の厳密さ、強度	Identity Assurance Level（IAL）		Identity assurance levels (IAL)	
	IAL1	本人確認不要、自己申告での登録でよい	IAL1	自己申告
	IAL2	サービス内容ごとに識別に用いられる属性をリモートまたは対面で確認する必要あり	IAL2	識別に用いられる1つ以上のエビデンスをリモートで確認をする
	IAL3	識別に用いられる属性を対面で確認するかつ検証担当者は有資格者である必要がある	IAL3	識別に用いられる2つ以上のエビデンスを対面（もしくは同等の方法）で確認するエビデンスを発行した機関が適切かどうかの確認、もしくは検査官による検査を実施する
			IA 4	識別に用いられる3つ以上のエビデンスを確認する※実施方法は現在定義なしエビデンスを発行した機関が適切かどうかの確認、もしくは検査官による検査を実施する
認証プロセスの強度	Authenticator Assurance Level（AAL）		Authentication assurance levels (AAL)	
	AAL1	単要素認証	AAL1	単純なセッション （HTTP クッキー、デバイスポスチャー*1・デバイス管理システムなど）
	AAL2	2要素認証が必要（2要素目の認証手段はソフトウェアベースのもので可）	AAL2	ユーザー名とパスワードの組み合わせなどの共有された秘密共有鍵による鍵所有の暗号化証明
	AAL3	2要素認証が必要、かつ2要素目の認証手段はハードウェアを用いたもの（ハードウェアトークン等）が必要	AAL3	非対称鍵による鍵所有の暗号化証明
			AAL4	シールドハードウェアトークン / Trusted Platformモジュールに格納される鍵検証された生体認証
フェレデーション（ID情報の連携）をする際のデータのやり取りの強度	Federation Assurance Level（FAL）		該当なし	
	FAL1	認証結果データへの署名		
	FAL2	署名に加え、データの送付対象のみが復号可能な暗号化の実施		
	FAL3	ユーザーごとの鍵と認証結果のデータを紐づけて送付し、送付先はユーザーの認証結果に紐づく		

*1 従来からのID/パスワードによる認証に加え、アクセスするのに使用している端末のセキュリティ状態などをチェックして、条件に合致しない場合はアクセスを許可しない機能

出所）
1 https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=26776#appC

3.2 詳細調査結果：トラストフレームワークの策定状況

3.2.3オセアニア（オーストラリア、ニュージーランド）における調査結果

Trusted Digital Identity Framework（TDIF）

Trusted Digital Identity Framework（TDIF）[1]は、2018年に公表されたオーストラリア政府が推進するデジタルIDシステム内のプロバイダーとサービスに対する厳格な規則と標準を示した認定フレームワークである。「認定プロセス」「機能要件」「ロール要件」「フェデレーションのオンボーディング要件」「認定の維持」などの13文書で構成されている

TDIFの構成

01. 用語集 / 02. 概要	
03. 認定プロセス	TDIF認定を取得するために申請者が完了する必要のあるプロセスと要件を定義している
04. 機能要件	不正防止、プライバシー、保護セキュリティ、ユーザーエクスペリエンス、技術テストなど、認定された役割に適用される要件の概要を示す
04A. 機能ガイダンス	機能要件に定められた要件を満たすための申請者向けガイダンス
05. ロール要件	認定されたロールに適用されるユーザー用語とライフサイクル管理要件を定義している
05A. ロールガイダンス	ロール要件に定められた要件を満たすためのガイダンス
06. フェデレーションのオンボーディング要件	申請者の ID システムがオーストラリア政府の ID フェデレーションへのオンボードを承認されたときに満たす必要がある要件として機能要件、技術統合テスト要件、運用義務、および ID 交換の認定要件の概要を示す
06A. フェデレーションのオンボーディングガイダンス	要件に定められた要件を満たすための申請者向けガイダンス
06B. OpenID Connect 1.0 profile	IDフェデレーション内で OpenID Connect 1.0 がどのように使用されるかを説明する文書
06C. SAML 2.0 profile	IDフェデレーション内で SAML 2.0 がどのように使用されるかを説明する文書
06D. 属性プロファイル	IDフェデレーション内で使用される属性と、OpenID Connect 1.0 プロファイル・SAML 2.0 プロファイルでどのようにマップされるかを説明する文書
07. 認定の維持	認定プロバイダーがTDIFの認定を維持するために、最初の認定日から1年後までに完了しなければならないプロセスおよび要件を定義している

凡例 ■：Trusted Web との関連があると考えられる項目　■：Trusted Web との関連が薄いと考えられる項目

出所）
1 https://www.digitalidentity.gov.au/tdif#accredited

TDIFの機能要件（再掲）[1]

TDIFの認定参加者の役割に応じて適用される機能要件として、不正管理、プライバシー、保護セキュリティ、ユーザ体験、技術テストなどが定められている

TDIFの機能要件

不正管理（Fraud Control）	認定参加者への申請者に対して適用される最低限の不正管理基準を定めており、基本的には連邦不正管理フレームワーク（CFCF：the Commonwealth Fraud Control Framework）への準拠を求めている（TDIFで定める要件とCFCFの最新版で規定されている要件に矛盾がある場合はCFCFを優先するとされている）。
プライバシー（Privacy）	認定参加者への申請者に対して適用される情報取扱要件を定めている。4つの認定種別に共通して課される要件として、オーストラリアプライバシー原則（APPs）を含むプライバシー法に基づく義務、オーストラリア政府機関プライバシーコード、関連する州または地域のプライバシーに関する法律への準拠を定めている。
保護セキュリティ（Protective Security）	申請者がアイデンティティ・サービスに対して最低限保証することが求められる保護セキュリティ水準を定めている。基本的には、オーストラリアサイバーセキュリティセンター（ACSC）が定めた政府の保護セキュリティポリシーフレームワーク（PSPF）及び情報セキュリティマニュアル（ISM）への準拠が求められる。
ユーザー体験（User Experience）	アイデンティティ・サービスのユーザビリティやIDプルーフィングの流れ、認証の流れについての要件を定めている。具体的には全てのタイプの申請者に対して、ユーザビリティの要件としてアイデンティティシステムの構築に当たりレスポンシブwebデザイン手法の採用やエンドツーエンドのジャーニーマップの作成等を義務付けている
技術テスト（Technical testing）	ユーザビリティテストのテストプランと実施に関する要件を定めている（ただし申請者とユーザーでインタラクションがないことをDTAに証明することができる場合のみは例外）。テストプランの要件としては、全てのタイプの申請者に対してテストの目的、ユーザビリティの目標・指標、テストへの参加人数、募集方法、ユーザビリティテストから得られた知見の実装方法等の作成などが求められている

出所）
1 https://www.digitalidentity.gov.au/sites/default/files/2023-03/tdif_04_functional_requirements_-_release_4.8.pdf

TDIF フェデレーションのオンボーディング要件

TDIFの認定参加者がフェデレーションに参加する要件として、「技術要件」「属性サービスプロバイダ要件」「アイデンティティエクスチェンジ*1要件」「属性要件」が定められており、具体的な技術としてOpenID Connect 1.0 とSAML 2.0 の使用を前提としている

フェデレーションのオンボーディング要件

技術要件	共通機能要件	統合技術要件（OpenID Connect 1.0 /SAML 2.0 の実装要件)、セキュリティ要件、機能的データ要件、監督機関への報告要件、をそれぞれ示している
	技術試験要件	機能要件（前頁参照）にて示した要件
	機能固有の技術的な統合要件	Identity resolution（ペアワイズアイデンティファー、重複排除）についての要件を示す
属性サービスプロバイダ機能要件	技術要件	属性スキーマの要件、アイデンティエクスチェンジの生成するペアワイズアイデンティファーの使用要求、APIの提供、REST APIの要件などを示す
	監査記録	属性サービスプロバイダの監査ログに含まれる必要があるものについての要件を示す
アイデンティティエクスチェンジ要件	統合要件	監査ID、監査履歴・コンシューマー履歴・ユーザーダッシュボード、属性サービスプロバイダの統合（APIでの呼び出し等）、アイデンティプロバイダの選択機能の実装についての要件を示す
	フェデレーションプロトコルマッピング要件	OIDC/SAML-OIDC/SAMLの仲介時の保証レベルのマッピングを示す
属性要件	計算された属性	属性セット内の属性から、アルゴリズムを用いて動的に導き出される属性についてサポートする要件を示す
	属性サービスプロバイダの属性	属性サービスプロバイダ自身の属性が公開されることに関する要件を示す
	属性共有ポリシー	属性共有ポリシーに従った形での属性の開示を定める
	属性データプレゼンテーション	アイデンティティフェデレーションに参加する際の属性データ表現についての要件を示す

*1 アイデンティティエクスチェンジ：ID フェデレーションのメンバー間の ID 属性とアサーションの流れを伝達、管理、調整するTDIF公認の組織または政府機関を指す

凡例 ■：Trusted Web との関連があると考えられる項目 ■：Trusted Web との関連が薄いと考えられる項目

出所） 1 https://www.digitalidentity.gov.au/sites/default/files/2023-03/tdif_06_federation_onboarding_requirements_-_release_4.8.pdf

TDIF認定事業者（再掲）

Identity providers

サービス名称	プロバイダー名称	IPL*	認定日
Digital iD	Australia Post	IP2 (Standard)	2019年5月17日
myGovID	Australian Tax Office	IP1, IP2 (Basic, Standard) IP3 (Strong)	2019年5月30日 2021年8月8日
OCR Labs	OCR Labs	IP2 (Standard) IP3 (Strong)	2021年7月8日 2022年3月7日
ID	Mastercard	IP1+ (Basic)	2022年7月21日

* IPL：Identity proofing levels。作成可能なIDの証明レベルを示す。
IDを使用するサービスが求めるレベルとして、Basic（IPL1、1+）、Standard（IPL2、2+）、Strong（IPL3）の5段階が設定されている

Credential providers

サービス名称	プロバイダー名称	CL**	認定日
Digital iD	Australia Post	CL2	2019年5月17日
myGovID	Australian Tax Office	CL2	2019年5月30日
ID	Mastercard	CL2	2022年7月21日

** CL：Credential levels。認証プロセスにおける保証レベル。IPLごとに適したクレデンシャルレベルとしてCL1~CL3の3段階が設定されている

Identity exchange

サービス名称	プロバイダー名称	サポートしている規格	認定日
Exchange	Services Australia	OpenID Connect 1.0、SAML	2019年5月13日
connectID	eftpos	OpenID Connect 1.0	2021年9月15日
ID	Mastercard	OpenID Connect 1.0	2022年6月10日

Attribute providers

サービス名称	プロバイダー名称	作成される属性	認定日
Relationship Authorisation Manager (RAM)	Australian Tax Office	Business authorisations	2019年6月20日
myGov	Services Australia	myGov LinkID	2021年8月25日

（補足）NIST SP 800-63とTDIFの比較

オーストラリア
ニュージーランド

	NIST SP 800-63-3		TDIF[1]	
本人確認（ID Proofing）の厳密さ、強度	Identity Assurance Level（IAL）		Identity proofing levels（IP）	
	IAL1	本人確認不要、自己申告での登録でよい	IP1	ID検証不要（自己申告）
	IAL2	サービス内容ごとに識別に用いられる属性をリモートまたは対面で確認する必要あり	IP1+	ID検証に１つのID文書（携帯番号等）が必要
	IAL3	識別に用いられる属性を対面で確認するかつ検証担当者は有資格者である必要がある	IP2	2つ以上のID文書（パスポート、出生証明書等）が必要
			IP2+	2つ以上のID文書と本人の真正性確認（生体認証等）
			IP3	2つ以上のID文書（うち一つは顔写真入り）と本人の真正性確認（生体認証等）
			IP4	4つ以上のID文書（うち一つは顔写真入り）と本人の真正性確認（生体認証等）と対面でのインタビューへの出席
認証プロセスの強度	Authenticator Assurance Level（AAL）		Credential level（CL）	
	AAL1	単要素認証	CL1	単要素認証 IP1にのみ適用可能
	AAL2	2要素認証が必要（2要素目の認証手段はソフトウェアベースのもので可）	CL2	2要素認証（CL1にワンタイムパスワードの追加等） IP1~3に適用可能
	AAL3	2要素認証が必要、かつ2要素目の認証手段はハードウェアを用いたもの（ハードウェアトークン等）が必要	CL3	2要素認証とハードウェア認証が必要 IP1~4に適用可能
フェレデーション（ID情報の連携）をする際のデータのやり取りの強度	Federation Assurance Level（FAL）		該当なし	
	FAL1	認証結果データへの署名		
	FAL2	署名に加え、データの送付対象のみが復号可能な暗号化の実施		
	FAL3	ユーザーごとの鍵と認証結果のデータを紐づけて送付し、送付先はユーザーの認証結果に紐づく		

出所）
1 https://www.digitalidentity.gov.au/sites/default/files/2023-03/tdif_05_role_requirements_-_release_4.8.pdf

TrustID Framework（再掲）

DTAの策定したTDIFとは別に、オーストラリアの決済業界の調整機関であるAPC（オーストラリア決済評議会）は、民間企業に向けたデジタルIDフレームワークであるTrustID Frameworkが策定しており、TrustID FrameworkとTDIFの相互運用性を確保することで、政府・民間双方が発行するデジタルIDが利用可能なネットワークの実現を目指している[1,2,3,4]

TrustID Frameworkの概要

- DTAの「myGovID」や「DigitaliD」などのTDIF認定下のデジタルIDが金融サービス分野での幅広い採用が期待できないと考えられたことを一因として、2019年6月にAPC（オーストラリア決済評議会）によって策定された
- TrustID Frameworkは、オーストラリアの民間企業が提供するデジタルIDソリューションの信頼性、相互運用性を高めるために、組織が製品やサービスの設計と構築において遵守するための一連のルールとガイドラインを提示するものである
- APCはDTAを協力して、Trust ID FrameworkとTDIFの相互運用性を確保し、最終的には政府・民間のデジタルIDサービスで相互運用可能なネットワークを促進するとしている
- APCの事務局的役割を果たすAPN（オーストラリア決裁ネットワーク）は、TrustID Frameworkのガバナンス構造についてコンサルテーションを行っている

※APCは、APNとRBA（オーストラリア準備銀行）の共同決議によって2014年に発足した

出所）
1 https://www.itnews.com.au/news/banks-prepare-to-issue-mygov-compatible-digital-identities-532768
2 https://www.rba.gov.au/publications/annual-reports/psb/2020/retail-payments-regulation-and-policy-issues.html
3 https://www.auspaynet.com.au/insights/Trust-ID
4 https://www.australianpaymentscouncil.com.au/wp-content/uploads/2019/12/APC_Annual_Review_2019.pdf

デジタルアイデンティティ・トラストフレームワーク

デジタルアイデンティティ・トラストフレームワーク法案[1,2]は、ニュージーランドにおける個人・組織間取引に対するデジタルIDサービスの法的な枠組みを規定するものである。デジタルIDサービスの定義等を定めるほか、要件を満たした信頼できるデジタルIDサービス事業者を「TF（トラストフレームワーク）プロバイダー」として登録する仕組みを定めている

デジタルアイデンティティ・トラストフレームワーク法案

総則	TFの定義	• デジタルIDサービス信頼フレームワークまたは信頼フレームワークとは、個人と組織間の取引に対するデジタルIDサービスの提供を規制するためにこの法律によって確立された法的枠組みを意味する
デジタルIDサービス トラストフレームワーク	認定マーク	• TFプロバイダーは、TF理事会によって承認された認定マークを使用して、提供する認定サービスを識別することができる
	信頼フレームワーク外のデジタル ID サービス	• 認定されていないデジタルIDサービスを提供することを認める • TFプロバイダーは認定されていない認定サービスとデジタルIDサービスの両方を提供可能
TF規則、TFプロバイダの認定・登録・記録の保持と報告	TF規則	• TFプロバイダは規則として定められる「識別管理」「プライバシー・守秘義務」「セキュリティとリスク」「情報・データ管理」「共有とファシリテーション」の各要件を全て満たす必要がある • 2023年2月時点で各要件の詳細は未策定の模様
	TFプロバイダー認定	• 認定申請、申請に必要な情報（TF規則の充足、犯罪歴がないこと等）、TF当局による認定判断、認定決定の通知に関して定めている • 認定期間の設定は未策定の模様である。また、現時点での認定取り消しの条件は認定後12か月以内にサービスが開始されないことである
	TFレジスタ	• TFレジスタは、利用者がサービス事業者がTFプロバイダーとして認定されているかどうかを判断し、認定されている場合はその認定のステータスと履歴を判断するために用いられる • TF当局によって認定されたプロバイダとIDサービスをTF当局が登録し、維持・管理を行う
	TFプロバイダーによる記録の保持と報告	• TFプロバイダは活動に関する必要な情報を収集し、保管し、定期的・要求に応じてTF当局に提供しなくてはならない • 2023年2月時点で、必要な情報の要件、情報保管期間は未設定
TF委員会		
TF当局		
苦情申し立て、違反		
規制、民事責任の免除、調査		

凡例 ■：Trusted Webとの関連があると考えられる項目 ■：Trusted Webとの関連が薄いと考えられる項目

出所）1 https://www.parliament.nz/en/pb/bills-and-laws/bills-proposed-laws/document/BILL_116015/digital-identity-services-trust-framework-bill
2 https://www.legislation.govt.nz/bill/government/2021/0078/latest/whole.html#LMS496284

Identification Management Standards

Identification Management Standards[1] は、2021年4月に内務省によって策定されたニュージーランドにおけるアイデンティティ管理の標準である。「情報保証基準」「バインディング保証基準」「認証保証基準」「フェデレーション保証基準」と各保証レベルを決定する「識別リスクアセスメント」により構成されている。それぞれの保証が連携して機能することで組織が適切なエンティティに関する適切な情報を持っていることを保証するとともに、アイデンティティ詐欺のリスクを最小限に抑えることが目的。対象は公共・民間・組織・個人で、準拠は任意である[2]

Identification Management Standards の構成

識別リスクアセスメント Assessing identification risk	• サービスもしくはトランザクションの識別リスクアセスメントを実施する方法を提供するドキュメント • 識別リスクを ①誤った情報の提供によるリスク（情報保証基準） ②誤った紐づけによるリスク（バインディング保証基準、認証保証基準） の2種類にわけ、リスクがもたらす結果のカテゴライズ*1と、インパクト*2、現在組織が提供している施策*3の3要素から評価し、保証レベルを決定する
情報保証基準 Information Assurance Standard	• 収集された情報がエンティティの適格性（eligibility）もしくは能力（capability）に関して、正確な判断に適していることを保証するための具体的な管理方法を提供する基準 • 基準と実装ガイドラインの2ドキュメントで構成される
バインディング保証基準 Binding Assurance Standard	• 個人情報の盗難を防止することを目的として、エンティティがエンティティ情報および認証器と適切に結合していることを保証するための具体的な管理方法を提供する基準 • 基準と実装ガイドラインの2ドキュメントで構成される
認証保証基準 Authentication Assurance Standard	• 1つまたは複数の認証器が、権限を有する保有者によって依然として保有され、かつ単独で管理されていることを保証するために用いられる管理方法を提供する基準 • 基準と実装ガイドラインの2ドキュメントで構成される
フェデレーション保証基準 Federation Assurance Standard	• 他者が依拠するクレデンシャルを提供する当事者、またはプレゼンテーションファシリテーションメカニズムを提供する当事者*4に対して追加の管理方法を提供する基準 • 基準と実装ガイドラインの2ドキュメントで構成される

*1 リスクのカテゴライズを「金融的な損失/責任」「機密情報の不正な開示」「資格、識別、評判の損失/損害」「その他の損失/責任」の4分類で評価する
*2 問題が発生した際に受ける影響について、それぞれの機関がもつリスクフレームワークに基づき、「Rare」「Unlikely」「Possible」「Likely」「Almost certain」の5段階に当てはめ評価を行う
*3 現時点で各組織が講じている施策を「予防的：事象または結果の発生を阻止する」「是正的・縮小的：事象や結果の発生を阻止するのではなく、影響の程度を軽減する」「検出：事象を特定することで、今後発生しないように是正措置を講じる」「指令的・阻害的：ルール、ポリシー、トレーニングの実施もしくは価値が薄いとして施策を実施しない」の4分類に分け評価を行う
*4 1つ以上のクレデンシャルを依拠当事者に提示することを容易にするメカニズムを提供する

出所）1 https://www.digital.govt.nz/standards-and-guidance/identification-management/
2 https://www.digital.govt.nz/standards-and-guidance/identification-management/guidance/assessing-identification-risk/

Identification Management Standards – ① 情報保証基準の詳細

情報保証基準はRelying Party(RP)を対象として、収集された情報がエンティティの適格性（eligibility）もしくは能力（capability）に関して、正確な判断に適していることを保証するための具体的な管理方法を提供する基準である。LOAとして1~4 レベルの Information Assurance（IA）を定めており、識別リスクアセスメントによってレベル分けがなされ、一部の要件ではレベルに応じた内容への準拠を求めている

情報保証基準のうちレベルごとの要件を定めるもの[1]

	情報検証に必要なエビデンス	エビデンスの「質」	エビデンスの登録ステータス	不正対策*1
IA 1	エンティティをエビデンスとして使用する必要がある	エンティティをエビデンスとして受け入れる必要がある	適用されない	適用されない
IA 2	少なくとも作成の一部に信頼できるソースのコピーを参照しているエビデンスを選択する必要がある	エビデンスを「額面通り」に受け取る必要がある	適用されない	適用されない
IA 3	少なくとも信頼できるソースのコピーであるエビデンスを選択する必要がある	手動で識別されること、またはエビデンスを再現できるように独自の知識を必要とする物理的なセキュリティ機能を含める必要がある	エビデンスの発行者、または同等のサービスプロバイダと登録ステータスを確認する必要がある	「不正対策手法」を適用する必要がある
IA 4	信頼できるソース、もしくは同等とみなされる信頼できるソースに継続的に同期されたリンクを持つエビデンスを選択する必要がある	エビデンスが体系的に識別され、信頼できる通信チャネルを通じてアクセスされることを基準とする必要がある	エビデンスの発行者、または同等のサービスプロバイダと登録ステータスを確認する必要がある	「不正対策手法」を適用する必要がある

*1 「不正対策ガイドライン」は2023年3月現在作成中のため詳細は不明

出所

1） https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-management-standards/information-assurance-standard/

凡例 ■：大項目 ■：適用される内容 ■：適用されない内容

Identification Management Standards – ② バインディング保証基準

バインディング保証基準はRPを対象に個人情報の盗難を防止することを目的として、エンティティがエンティティ情報および認証器と適切に結合していることを保証するための具体的な管理方法を提供する基準である。LOAとして1~4 レベルの Binding Assurance（BA）を定めており、識別リスクアセスメントによってレベル分けがなされ、一部の要件ではレベルに応じた内容への準拠を求めている

バインディング保証基準のうちレベルごとの要件を定めるもの[1]

	エンティティバインディングの要件			オーセンティケータバインディングの要件
	バインディングファクター	不正対策*2	バインディングの維持	仕様
BA 1	適用されない	適用されない	5年に1度エンティティバインディングテストを実施し、BAと一致しているか確認する必要がある	適用されない
BA 2	少なくとも1つのバインディングファクター*1タイプ、もしくは同等以上の保証レベルの既存の認証器/クレデンシャルを使用する必要がある	適用されない	5年に1度エンティティバインディングテストを実施し、BAと一致しているか確認する必要がある	適用されない
BA 3	少なくとも2つのバインディングファクタータイプ、もしくは同等以上の保証レベルの既存の認証器/クレデンシャルを使用する必要がある	「不正対策手法」を適用する必要がある	生体認証要素を伴わない限り5年に1度エンティティバインディングテストを実施し、BAと一致しているか確認する必要がある	認証器発行者もしくは同等のサービスプロバイダに対して、認証器が使用不可となる事象発生の有無について確認してもよい
BA 4	知識/所有のいずれかと生体認証ファクター、もしくは同等以上の保証レベルの既存の認証器/クレデンシャルを使用する必要がある	「不正対策手法」を適用する必要がある	生体認証要素を伴わない限り5年に1度エンティティバインディングテストを実施し、BAと一致しているか確認する必要がある	認証器発行者もしくは同等のサービスプロバイダに対して、認証器が使用不可となる事象発生の有無について確認する必要がある

*1 バインディングファクター：エンティティが知っていること（知識ファクター）、エンティティが持っているもの（所有ファクター）、エンティティが何か、または行う何か（生体認証ファクター）の3種類が存在する
*2 「不正対策ガイドライン」は2023年3月現在作成中のため詳細は不明

出所
1）https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-management-standards/binding-assurance-standard/

凡例 ■：大項目 ■：適用される内容 ■：適用されない内容

Identification Management Standards – ③ 認証保証基準

認証保証基準とはRPを対象に、認証器が権限を有する保有者によって依然として保有され、かつ単独で管理されていることを保証するために用いられる管理方法を提供する基準である。LOAとして1~4 レベルのAuthentication Assurance（AA）を定めており、識別リスクアセスメントによってレベル分けがなされ、一部の要件ではレベルに応じた内容への準拠を求めている

認証保証基準のうちレベルごとの要件を定めるもの[1]

	契約条件	契約条件のリマインド	共有の制限	アカウント無効化	物理的な所有ファクターの防止	認証試行回数上限	推測・開示された知識ファクターの防止	所有ファクターによるなりすまし防止	スプーフィング[2]の防止	生体認証	スプーフィング*1の防止	生体認証での誤検知対策	生体認証での誤検知対策
AA 1	説明してもよい	任意	適用されない	適用されない	適用されない	試行回数上限を10回とし、15分試行を制限する	適用されない	非物理的な課題への予測不可能な応答を実施してもよい	「人」から直接生体認証の応答を受け取るための制御をしてもよい	適用されない	「人」から直接生体認証の応答を受け取るための制御をしてもよい	適用されない	適用されない
AA 2	説明する必要がある	実施する必要がある	適用されない	適用されない	適用されない	試行回数上限を5回とし、30分試行を制限する	適用されない	非物理的な課題への予測不可能な応答を実施する必要がある	「人」から直接生体認証の応答を受け取るための制御をする必要がある	適用されない	「人」から直接生体認証の応答を受け取るための制御をする必要がある	適用されない	適用されない
AA 3	説明する必要がある	実施する必要がある	2つの異なるファクター実装をする必要がある	30回認証に失敗した際にアカウントを無効にし、調査を実施する	別のタイプの認証要素と組み合わせる	試行回数上限を5回とし、30分試行を制限する	所有/生体認証ファクターと組み合わせる必要がある	非物理的な課題への予測不可能な応答を実施する必要がある	「人」から直接生体認証の応答を受け取るための制御をする必要がある	適用されない	「人」から直接生体認証の応答を受け取るための制御をする必要がある	訓練されたオペレータによる手動比較、体系的比較のいずれか	手動比較をする際は、別のファクターと組み合わせる必要がある
AA 4	説明する必要がある	実施する必要がある	生体認証と、異なるファクターを実装する必要がある	30回認証に失敗した際にアカウントを無効にし、調査を実施する	生体認証を2要素目として組み合わせる	試行回数上限を5回とし、30分試行を制限する	生体認証ファクターと組み合わせる必要がある	非物理的な課題への予測不可能な応答を実施する必要がある	「人」から直接生体認証の応答を受け取るための制御をする必要がある	生体認証ファクターサンプルを対面・リモートで取得し、活性チェックを実装する必要がある	「人」から直接生体認証の応答を受け取るための制御をする必要がある	体系的比較を実施する必要がある	別のファクターと組み合わせる必要がある

*1 スプーフィング：なりすましの試み（例：録音、マスク、化粧または補綴物など）

出所
1）https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-management-standards/authentication-assurance-standard/

凡例 ：大項目 ：適用される内容 ：任意の内容 ：適用されない内容

Identification Management Standards – ④ フェデレーション保証基準

フェデレーション保証基準とは、クレデンシャルを提供する当事者、またはプレゼンテーション・ファシリテーションメカニズムを提供する当事者に対して追加の管理方法を提供する基準である。他の基準と異なり、LoAは存在しない

フェデレーション保証基準[1]

要件	項目	概要
資格情報を確立するための要件	クレデンシャルのリスクの把握	クレデンシャルが不正なアクセスや使用から適切に保護されていると保有者が信じるためには、クレデンシャルプロバイダーが複数のコンテキストで使用された場合にクレデンシャルがもたらすリスクを理解し、軽減する必要がある
	クレデンシャルの保証レベル	資格情報の確立に対する一貫したアプローチの必要性と、RPがデンシャルクレデンシャルプロバイダーが本物であることを知る必要がある
	プライバシー保護	フェデレーションメカニズム*1による、保有者が予期・望まない可能性のあるデータの可用性に対してプライバシー保護をする必要がある
	包括的	クレデンシャルプロバイダーはワイタンギ条約*2に基づく責任やデジタルインクルージョンなどの義務を負い、エンティティが対等な立場で参加できるようにしなくてはならない
	クレデンシャルの維持	関連性と完全性の維持のための活動としてクレデンシャルの更新・中断・取り消しの手段を提供する必要がある
ファシリテーション・メカニズム[2]を確立するための要件	ファシリテーションメカニズムのリスクの把握	ファシリテーションメカニズムのリスクとしてリンクできるクレデンシャルの数が増えるにつれて、情報の蓄積に注意を柄う必要があることなどを把握する必要がある
	バインディング保証基準の維持	接続時に個々のクレデンシャルのバインディング保証レベルが低下していないことが「確実」である必要がある
	プライバシー保護	フェデレーションメカニズムによる、保有者が予期・望まない可能性のあるデータの可用性に対してプライバシー保護をする必要がある
	ファシリテーションメカニズムの維持	関連性と完全性の維持のための活動としてクレデンシャルの追加・削除・キャンセル・喪失/侵害の報告等の手段を提供する必要がある
ファシリテーションプロバイダによるクレデンシャル提示の要件	一貫性と認識された方法	RPがクレデンシャルの整合性を信頼するために、クレデンシャルが一貫性のある認識された方法で確立および提示されていることを知っている必要がある
	プライバシー保護	データの最小化や許可の提供などのプライバシー原則*3の積極的な適用を行う必要がある
	プレゼンテーション内容の保全	クレデンシャル保持者がクレデンシャル対象情報をRPへ提供することを許可する場合、両者は同じ情報をRPが受信することを信頼できるようにする必要がある
	プレゼンテーションの調査を可能にする	クレデンシャルの提示プロセスにおけるさまざまな関係者の匿名性、仮名性、および盲検化を可能にする

*1 ファシリテーションメカニズム：証明書利用者からの要求に応じて 1 つ以上の資格情報 (完全または部分的) の提示を容易にできるメカニズム。Realme やデジタルウォレットも含まれる
*2 ワイタンギ条約：1840年、英国とマオリ族間で締結された条約。https://www.newzealand.com/jp/feature/treaty-of-waitangi/
*3 プライバシー原則：Privacy Act 2020 and the Privacy Principles 。組織や企業がお客様の情報を収集、保存、使用、共有する方法を規定している法律

凡例
：大項目
：小項目
：概要

出所
1）https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-management-standards/federation-assurance-standard/

（補足）SP 800-63とIdentification Management Standardsの比較

	NIST SP 800-63-3		Identification Management Standards[1]
本人確認（ID Proofing）の厳密さ、強度	Identity Assurance Level（IAL）		
	IAL1	本人確認不要、自己申告での登録でよい	該当なし
	IAL2	サービス内容ごとに識別に用いられる属性をリモートまたは対面で確認する必要あり	
	IAL3	識別に用いられる属性を対面で確認するかつ検証担当者は有資格者である必要がある	
認証プロセスの強度	Authenticator Assurance Level（AAL）		Authentication Assurance（AA）
	AAL1	単要素認証	AA1 単要素認証
	AAL2	2要素認証が必要（2要素目の認証手段はソフトウェアベースのもので可）	AA2 2要素認証
	AAL3	2要素認証が必要、かつ2要素目の認証手段はハードウェアを用いたもの（ハードウェアトークン等）が必要	AA3 生体認証もしくは2要素認証
			AA4 2要素認証が必要 うち1つは活性チェックにより実装された生体認証である必要がある
フェレデーション（ID情報の連携）をする際のデータのやり取りの強度	Federation Assurance Level（FAL）		
	FAL1	認証結果データへの署名	該当なし
	FAL2	署名に加え、データの送付対象のみが復号可能な暗号化の実施	
	FAL3	ユーザーごとの鍵と認証結果のデータを紐づけて送付し、送付先はユーザーの認証結果に紐づく	

出所
1）https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-management-standards/authentication-assurance-standard/

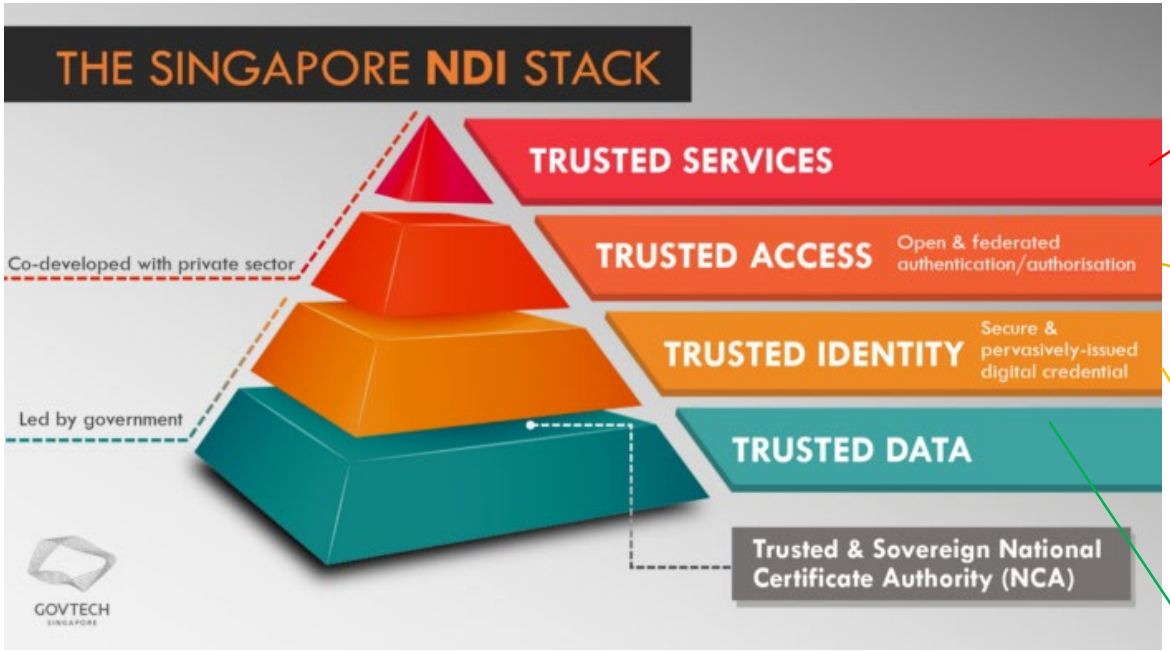
3.2 詳細調査結果：トラストフレームワークの策定状況

3.2.4アジア（シンガポール、インド）における調査結果

NDI Stack の構造（再掲）

シンガポール技術庁（Govtech）は、NDIの取り組みをNDI Stackの概念によって構造化している。NDI Stackの中では、My Info、Singpassなどの信頼性の高いデータとIDを提供するTrusted Data、Trusted Identityレイヤーを基盤として、その上に信頼性ある認証方式とサービス統合を行うAPIといったTrusted Access、Trusted Serviceレイヤーを構築しており、政府主導の取り組みを基盤として、民間部門と連携した認証・サービスを提供していることが分かる[1,2,3]

NDI Stackの構造



Trusted Service
公的機関、民間企業にAPIを提供し、サービス統合を可能にする

Trusted Access
法律や、Singpass Mobileの多要素認証のような信頼性ある認証技術標準によって公的機関・民間企業ASP（アプリケーションサービスプロバイダ）の信頼性を担保する

Trusted Identity
Singpassによって、高い保証を備えた基本的IDスキームを提供する
現在は政府中心の中央集権型だが、分散型モデルを検討する

Trusted Data
My Infoによって、信頼できるデータソースを市民・企業に対して提供する

：民間との共同領域　　：政府主導の領域

出所）
1 https://medium.com/ndi-sg/stack-x-webinar-national-digital-identity-stack-introduction-to-ndi-34b5dbed9565
2 https://www.globalgovernmentforum.com/wp-content/uploads/Singapore-NDI-slides_comp.pdf
3 https://www.tech.gov.sg/media/technews/giving-every-citizen-a-unique-digital-identity

India Stack（再掲）

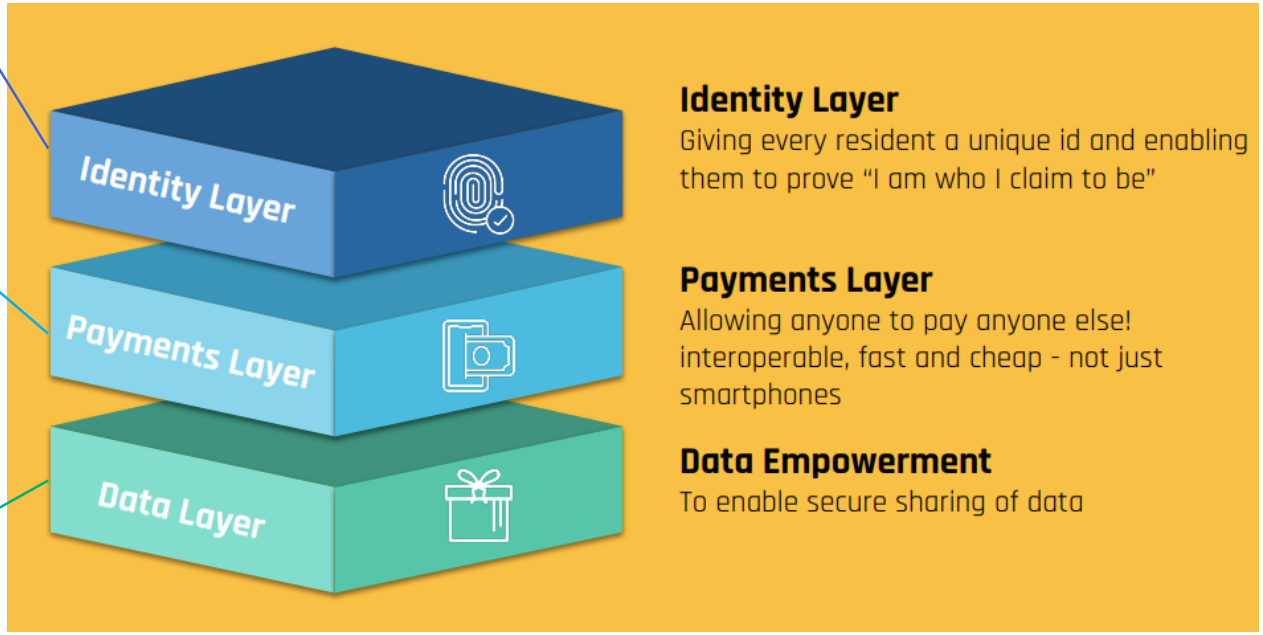
インド政府は国民ID基盤であるIndia Stackを3つのレイヤーに分けて概念を整理している。Aadhaar認証を基盤として、個人の識別・認証を可能とするIdentity Layer、金融取引を可能とするPayments Layer、個人データの保管・共有を可能とするData Empowermentからなり、Aadhaar認証を基盤としたAPIの活用により、デジタル経済にインド国民を包摂するための構造を持っていることが確認できる[1,2]

India Stackの構造

Identity Layer
個人を識別・認証することを可能にする。Aadhaar認証やeKYC、電子署名を行うAPIが該当する

Payments Layer
Aadhaar認証を基盤として電子的な金融取引・社会保障給付を可能とする。APBやUPIなどの送金・振込APIが該当する

Data Empowerment
個人データの安全な管理・共有を可能とする。電子文書を保管するDigilockerなどのAPIが該当する



出所）
1 https://info.thoughtworks.com/rs/199-QDE-291/images/India-Stack-DrivingTransformation-TWLiveIndia2019.pdf
2 https://indiastack.org/data.html

3.2 詳細調査結果：トラストフレームワークの策定状況

3.2.5トラストフレームワークの策定状況に関する総括

各トラストフレームワークのスコープ

トラストフレームワークのスコープについては、法律・規則としてのルールを定めるものから、システムのコンセプトを規定するもの、国のID利活用の指針を概念化したもの等様々ある

各トラストフレームワークのスコープ

国・地域		名称	スコープ
欧州	EU	Regulation 910/2014 : eIDAS（2.0）	EUの電子商取引に統一した基準を設けることため、eID、EUDIW及びトラストサービスの法的効力・要件について規定している
	ドイツ	IDunion Network	ネットワーク上でのトラストを確立する方法を簡素化・標準化することを目的として、テクノロジー（マシンレイヤーでの暗号化による検証可能性）と、ガバナンス（法律・ビジネス・社会レイヤーでの人間のアカウンタビリティ）をTCP/IPスタックの構造に着想を得た4層で整理している
	イギリス	The UK digital identity and attributes trust framework	英国における個人及び個人に関する情報を証明できるサービスをより簡単かつ安全に使用可能にすることを目的として、デジタルIDおよび/または属性情報を提供する際に遵守すべき一連のルールが規定されている
北米	米国	Identity Ecosystem Framework : IDEF	米国政府の推進するIdentity Ecosystemを構築する相互運用性標準、リスクモデル、プライバシーと責任のポリシー、要件、および説明責任メカニズムを包括的に規定している
		NIST SP 800-63-3 NIST SP 800-63-4	デジタルアイデンティティサービスを実装する連邦政府機関向けの技術要件であり、特にデジタル認証で使用するためのアイデンティティの登録と検証について規定している
	カナダ	Pan-Canadian Trust Framework : PCTF	カナダのデジタルアイデンティティ管理における原則や基準、デジタルIDの作成、管理、提供に係る一連のプロセスなどを定義しており、デジタルIDに関係する公共・民間のステークホルダー、研究者などに参照されることを目的としている
オセアニア	オーストラリア	Trusted Digital Identity Framework : TDIF	オーストラリア政府が推進する「デジタルIDシステム内」のプロバイダーとサービスに対する厳格な規則と標準を規定している
		Trust ID Framework	オーストラリアの民間企業が提供するデジタルIDソリューションの信頼性、相互運用性を高めるために、組織が製品やサービスの設計と構築において遵守するための一連のルールとガイドラインを規定している
	ニュージーランド	Digital Identity Trust Framework	ニュージーランドにおける個人・組織間取引に対するデジタルIDサービスの法的な枠組みを規定している
アジア	シンガポール	NDI Stack	デジタルID活用に係る国の指針を概念化したものであり、Singpass, My Infoの活用、APIによる接続が前提となっている
	インド	India Stack	デジタルID活用に係る国の指針を概念化したものであり、Aadhaarの活用、APIによる接続が前提となっている

トラストフレームワークの一般化

トラストフレームワークの策定状況に関する総括にあたっては、トラストフレームワークそのものの特性と規定している内容について一般化し整理することで、トラストフレームワークごとの比較を行い、国・地域の傾向・特徴を分析することとした

各国のトラストフレームワークの一般化

フレームワークのメタ的特性	策定主体		政府・民間どちらの主導か、もしくは共同しているか
	罰則の有無		法で規定されているか、フレームワークの遵守に強制力があるか
	認定の有無		フレームワーク遵守のインセンティブがあるか
フレームワークで規定する内容	原理・原則		提供するサービスやプロセス、機能要件
	ガバナンス	ステークホルダーの定義・要件	スキームへの参加者の役割・責任等について規定しているか
		プロセスの定義・要件	登録、認証、認可、ID連携等のプロセスの要件を規定しているか
		コンポーネントの定義・要件	ウォレット、プロトコル、レジストリ等のコンポーネントの要件を規定しているか
	テクノロジー	特定の技術の参照・指定	特定の技術標準・仕様の参照を行っているか
		独自の技術仕様の規定	フレームワーク内で独自の技術仕様を規定・参照しているか

（補足）一般的なトラストフレームワークの策定プロセス

トラストフレームワークのメタ的特性の比較

強制力（法律で規定）を有しているものはeIDAS（EU）のみである
また、一部の国ではトラストフレームに基づく認定制度を設け、トラストフレームワークへの準拠を促している
インド・シンガポールにおいては、国のID利活用に係るコンセプトを示すのみで、明確な要件やサービススキームについては規定をしていない

トラストフレームワークのメタ的特性の比較

国・地域		トラストフレームワーク名称	策定主体	強制力	認定	認定を行う主体
欧州	EU	Regulation 910/2014 ：eIDAS（2.0）	政府主導	強制	有	加盟国の適合性評価機関による認定
	ドイツ	IDunion Network	官民共同	任意	無	
	英国	The UK digital identity and attributes trust framework	政府主導	任意	有	政府主導で民間企業・団体による認定
北米	米国	Identity Ecosystem Framework ：IDEF	政府主導	任意	無*1	
		NIST SP 800-63	政府主導	任意	無	
	カナダ	Pan-Canadian Trust Framework : PCTF	官民共同	任意	有	DIACCの専門家ボランティア（TOB）による認定
オセアニア	オーストラリア	Trusted Digital Identity Framework : TDIF	政府主導	任意	有	DTA認定チームによる認定
		Trust ID Framework	民間主導	任意	有	詳細不明
	ニュージーランド	Digital Identity Trust Framework	政府主導	任意	有	認定制度は政府当局によって運営されるが、認定主体は不明
		Identity management standards	政府主導	任意	無	
アジア	シンガポール	NDI Stack	政府主導	任意	無	
	インド	India Stack	政府主導	任意	無	

*1 自己評価によるレジストリへの登録あり

トラストフレームワークのメタ的特性の比較 - 強制力の違い

現時点において、準拠に強制力を持つトラストフレームワークは eIDAS のみであり、多くのトラストフレームワークは強制力を持たず、任意で各フレームワークのエコシステムに参加することを求めている

各トラストフレームワークにおける強制力の違い

国・地域		トラストフレームワーク名称	強制力	判断根拠とした記載の日本語訳
欧州	EU	Regulation 910/2014 : eIDAS（2.0）	強制	この規則は**その全体が拘束力を持ち**、すべての加盟国に直接適用されるものとする[1]
	ドイツ	IDunion Network	任意	IDunion研究プロジェクトは、セキュアデジタルIDショーケースプログラムの一環として、連邦経済気候行動省によって資金提供されている[2]
	英国	The UK digital identity and attributes trust framework	任意	プロバイダが他の**The UK DIATF 参加者とのみデータを共有することは義務付けない**[3]
北米	米国	Identity Ecosystem Framework : IDEF	任意	アイデンティティ・エコシステムへの**参加を希望するエンティティ**が、確立された参加要件を理解し、各要件への自らの準拠を評価できるようにすることを目的とし、自己評価プログラムを用意している[4]
		NIST SP 800-63	任意	政府機関のシステムに対しては権限を持つ**当局からの承認なしに適用されることは無い**。民間事業者は契約上の義務がない限り**参照は自由**である[5]
	カナダ	Pan-Canadian Trust Framework : PCTF	任意	PCTFは、常に**自由に利用**できレビューと採用が可能なオープンパブリックリソースである[6]
オセアニア	オーストラリア	Trusted Digital Identity Framework : TDIF	任意	事業者は認定を受けることを**選択する**ことができる[7]
		Trust ID Framework	任意	Trust ID フレームワークへの参加は現在開発中の認定要件を満たす**すべての組織に開かれている**[8]
	ニュージーランド	Digital Identity Trust Framework	任意	TFプロバイダは**認定外のサービスも提供可能**である[9]
		Identity management standards	任意	義務としての遵守を求められる場合は**契約・内閣による委任・法律などのプロセス**を要する。義務でない場合は**グッドプラクティスとして遵守**してもよい[10]
アジア	シンガポール	NDI Stack	任意	ナショナル・デジタル・アイデンティティ（NDI）は戦略的国家プロジェクトであり、市民がよりスムーズで安全な取引を行えるよう、さまざまなソリューションを**提供**している[11]
	インド	India Stack	任意	India Stack とは、人口規模でのアイデンティティ、データ、決済といった経済的プリミティブを解放することを目的とした、**一連のオープンAPI**と**デジタル公共財**[12]の呼称である

出所）
1 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN
2 https://idunion.org/ueber-uns/?lang=en
3 https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version#feedback-received-and-updates
4 https://wiki.idesg.org/wiki/Business_Value_Models
5 https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information
6 https://diacc.ca/trust-framework/pctf-overview/
7 https://www.digitalidentity.gov.au/tdif#accredited
8 https://www.auspaynet.com.au/insights/Trust-ID
9 https://www.legislation.govt.nz/bill/government/2021/0078/latest/whole.html#LMS459587
10 https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-management-standards/applying-the-standards/
11 https://www.developer.tech.gov.sg/products/categories/digital-identity/
12 https://indiastack.org/index.html

凡例 ：強制 ：任意 ：不明

トラストフレームワークのメタ的特性の比較 - 認定制度の違い

一部の国ではトラストフレームワークに基づく認定制度を設け、トラストフレームワークへの準拠を促している

各トラストフレームワークにおける認定制度の違い

国・地域		トラストフレームワーク名称	認定	判断根拠とした記載の日本語訳
欧州	EU	Regulation 910/2014 : eIDAS（2.0）	有	各加盟国は、自らが責任を負う適格信託サービス提供者に関する情報及び当該加盟国が提供する**適格トラストサービスに関する情報を含むトラステッドリストを作成し、維持し、及び公表**する[1]
	ドイツ	IDunion Network	無	
	英国	The UK digital identity and attributes trust framework	有	The UK digital identity and attributes trust framework への参加を希望する組織は、**認定を受ける**必要がある[2]
北米	米国	Identity Ecosystem Framework : IDEF	無	アイデンティティ・エコシステムへの参加を希望するエンティティが、確立された参加要件を理解し、各要件への自らの準拠を評価できるようにすることを目的とし、**自己評価プログラム**を用意している[3]
		NIST SP 800-63	無	
	カナダ	Pan-Canadian Trust Framework : PCTF	有	**Voilà Verified** は、デジタルアイデンティティサービスがPan-Canadian Trust Framework（PCTF）に準拠しているかどうかを判定する最初で唯一の**認証プログラム**[4]
オセアニア	オーストラリア	Trusted Digital Identity Framework : TDIF	有	オーストラリア政府のデジタルアイデンティティシステムがオーストラリア政府を超えて拡大する準備ができているかどうかをテストする一環として、**TDIFの下で多くの企業を認定**している[5]
		Trust ID Framework	有	Trust ID フレームワークへの参加は**現在開発中の認定要件を満たす**すべての組織に開かれている[6]
	ニュージーランド	Digital Identity Trust Framework	有	TFプロバイダーは、TF理事会によって**承認された認定マーク**を使用して、この法律に基づいて認定されている提供する認定サービスを識別することができる[7]
		Identity management standards	無	
アジア	シンガポール	NDI Stack	無	
	インド	India Stack	無	

出所）
1 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN
2 https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/trust-framework-certification
3 https://wiki.idesg.org/wiki/Business_Value_Models
4 https://diacc.ca/voila-verified/
5 https://www.digitalidentity.gov.au/tdif#accredited
6 https://www.auspaynet.com.au/insights/Trust-ID
7 https://www.legislation.govt.nz/bill/government/2021/0078/latest/whole.html#LMS459587

凡例 ：有 ：無

トラストフレームワークの比較 – ステークホルダーの違い

分散型を志向している IDunion Network とそれ以外のトラストフレームワークとでステークホルダーの記載について相違がみられる。また。The UK DIATF と PCTF 、Identity management standards についてはインフラを提供する主体についても言及している

各トラストフレームワークにおけるステークホルダーの抜粋*

国・地域		トラストフレームワーク名称	データ主体	発行者	検証者	インフラ提供者
欧州	EU	Regulation 910/2014 ：eIDAS（2.0）	申請する 自然人または法人	認定トラスト サービスプロバイダ	relying parties	無
	ドイツ	IDunion Network	Holder	Issuer	Verifier	無
	英国	The UK digital identity and attributes trust framework	users	identity service providers attribute service providers	relying parties	orchestration service providers
北米	米国	Identity Ecosystem Framework ：IDEF	user	Identity provider Credential provider Attribute provider	relying party	無
		NIST SP 800-63	Applicants subscribers	Credential Service Provider	Verifier relying party	無
	カナダ	Pan-Canadian Trust Framework : PCTF	User	Identity Provider Credential Service Provider Identity Attribute Provider	relying party	Network Facilitator
オセアニア	オーストラリア	Trusted Digital Identity Framework : TDIF	User	Identity providers Credential Service providers Attribute Service providers	Relying Party	無
		Trust ID Framework	不明	不明	不明	不明
	ニュージーランド	Digital Identity Trust Framework	users	TF providers	relying parties	無
		Identity management standards	Entity	Credential provider	relying parties	Facilitation Provider
アジア	シンガポール	NDI Stack	無	無	無	無
	インド	India Stack	無	無	無	無

＊各ステークホルダーは参照先のトラストフレームワークにおける名称で記載している

凡例 ：分散型 ：連邦型 ：無 ：不明

トラストフレームワークの規定する内容の比較

規定している内容では、法的な枠組み・ステークホルダー等を規定する戦略（上位概念）的な側面の強いものと、プロセス・コンポーネント、特定の技術の適用についても規定する網羅的／システム寄りのフレームワークとに分かれる

国・地域		名称	ガバナンス			テクノロジー	
			ステークホルダーの定義・要件	プロセスの定義・要件	コンポーネントの定義・要件	特定の技術の参照・指定	独自の技術仕様の規定
欧州	EU	Regulation 910/2014 : eIDAS（2.0）	トラストサービスプロバイダ等を定義	–	EUDIWの提供について義務化	–	–
	ドイツ	IDunion Network	Issuer-Holder-Verifier間の活動を規定	VCのフォーマットとプロトコルを使用したデータ交換プロセスを規定	ブロックチェーンやDLT、デジタルエージェントについて規定	W3C DIDsの実装を明示	–
	イギリス	The UK digital identity and attributes trust framework	デジタルID、属性情報を提供する際のステークホルダーについて規定	デジタルID、属性情報を提供するプロセスについて規定	–	NIST、ISO/IEC、W3C、OIDFなどの標準を参照	–
北米	米国	Identity Ecosystem Framework : IDEF	アイデンティティプロバイダ、クレデンシャルプロバイダ、属性プロバイダ、RPなどを定義	–	–	SAML、OpenID Connect、OAuth 2.0などの技術標準を参照	–
		NIST SP 800-63-3 NIST SP 800-63-4	サブスクライバ、アプリカント、RP等の参加者を定義	アイデンティティの登録と検証プロセスを規定	AALで認証デバイスについて規定	W3C VCsやmDL等の技術について記載検討	–
	カナダ	Pan-Canadian Trust Framework : PCTF	参加するエンティティとその役割について定義している	デジタルIDの作成、管理、提供に係る一連のプロセスを定義	デジタルウォレット・インフラ等のコンポーネントの要件を定義	–	–
オセアニア	オーストラリア	Trusted Digital Identity Framework : TDIF	4種類の認定参加者を規定	アイデンティティ証明のライフサイクルプロセスについて定義	–	OpenID Connect 1.0 /SAML 2.0 の実装要件を規定	–
		Trust ID Framework	詳細不明	詳細不明	詳細不明	詳細不明	詳細不明
	ニュージーランド	Digital Identity Trust Framework	デジタルIDサービス事業者の種別・提供サービス等について規定	–	–	–	–
		Identity management standards	–	–	–	–	–
アジア	シンガポール	NDI Stack	政府と民間事業者の協働を示す	–	–	–	Singpass, My Infoの活用、APIによる接続が前提
	インド	India Stack	民間事業者・行政サービスとの接続を示す	–	–	–	Aadhaarの活用、APIによる接続が前提

トラストフレームワークの規定する内容の比較

規定している内容では、法的な枠組み・ステークホルダー等を規定する戦略（上位概念）的な側面の強いものと、プロセス・コンポーネント、特定の技術の適用についても規定する網羅的／システム寄りのフレームワークとに分かれる

国・地域		名称	ガバナンス			テクノロジー	
			ステークホルダーの定義・要件	プロセスの定義・要件	コンポーネントの定義・要件	特定の技術の参照・指定	独自の技術仕様の規定
欧州	EU	Regulation 910/2014 : eIDAS（2.0）	トラ	–	EUDIWの提供について義務化	–	–
	ドイツ	IDunion Network	ISS	トとプロトコルを使換プロセスを規定	ブロックチェーンやDLT、デジタルエージェントについて規定	W3C DIDsの実装を明示	–
	イギリス	The UK digital identity and attributes trust framework	デジタルID、属性情報を提供する際のステークホルダーについて規定	デジタルID、属性情報を提供するプロセスについて規定	–	NIST、ISO/IEC、W3C、OIDFなどの標準を参照	–
北米	米国	Identity Ecosystem Framework : IDEF	Identity Ecosystem の参加主体を定義	–	–	SAML、OpenID Connect、OAuth 2.0などの技術標準を参照	–
		NIST SP 800-63-3 NIST SP 800-63-4	サブスクライバ、アプリカント、RP等の参加者を定義	アイデンティティの登録と検証プロセスを規定	AALで認証デバイスについて規定	W3C VCsやmDL等の技術について記載検討	–
	カナダ	Pan-Canadian Trust Framework : PCTF	参加するエンティティとその役割について定義している	デジタルIDの作成、管理、提供に係る一連のプロセスを定義	デジタルウォレット・インフラ等のコンポーネントの要件を定義	–	–
オセアニア	オーストラリア	Trusted Digital Identity Framework : TDIF	4種類の認定参加者を規定	アイデンティティ証明のライフサイクルプロセスについて定義	–	OpenID Connect 1.0 /SAML 2.0 の実装要件を規定	–
		Trust ID Framework	詳細不明	詳細不明	詳細不明	詳細不明	詳細不明
	ニュージーランド	Digital Identity Trust Framework	デジタルIDサービス事業者の種別・提供サービス等について規定	–	–	–	–
		Identity management standards	–	–	–	–	–
アジア	シンガポール	NDI Stack	政府と民間事業者の協働を示す	–	–	–	Singpass, My Infoの活用、APIによる接続が前提
	インド	India Stack	民間事業者・行政サービスとの接続を示す	–	–	–	Aadhaarの活用、APIによる接続が前提

戦略的側面

網羅的／システム的側面

（補足）各トラストフレームワークの特徴

国・地域		名称	特徴
欧州	EU	Regulation 910/2014 : eIDAS（2.0）	EUDIWアーキテクチャ・リファレンスフレームワークでは個人がウォレットでIDや資格情報をコントロールすることのできる、**自己主権型アイデンティティに近しい傾向が伺える**
	ドイツ	IDunion Network	**W3C DIDsでの実装を明示**し、ブロックチェーンや分散型台帳の運用ポリシーや手順、デジタルエージェントのセキュリティについて規定している
	イギリス	The UK digital identity and attributes trust framework	**W3C VCs**のデータモデルや**OIDC**規格と競合しない独自のデータスキーマの作成を行う。なお具体的な技術アーキテクチャ等は示していない
北米	米国	Identity Ecosystem Framework : IDEF	IDESG Standards Registry & Inventoryに準拠する標準規格のリストを公開しており、**SAML・OpenID Connect・OAuth 2.0が記載**されている
		NIST SP 800-63-3 NIST SP 800-63-4	**アイデンティティの登録と検証プロセスを規定**しており、**W3C VCs や mDL についての記載を追加するか検討**している
	カナダ	Pan-Canadian Trust Framework : PCTF	デジタルウォレットやインフラストラクチャについてのコンポーネントを定義したドキュメントが存在。技術進歩に適応するため具体的な技術の明記はしていない
オセアニア	オーストラリア	Trusted Digital Identity Framework	Web 2.0 型のフレームワークであり、フェデレーションに関する具体的な技術要件として**OpenID Connect 1.0、SAML 2.0**の記載がある
		Trust ID Framework	詳細未公表につき不明
	ニュージーランド	Digital Identity Trust Framework	法案であり認定制度を設けることを明示しているものの、**Digital Identity Trust Frameworkで認定されていないデジタルIDサービスを提供することを認めて**おり、認定QTSP以外の事業者を認めないeIDASと比較し緩やかな法案である
		Identity management standards	アイデンティティ管理における情報の正確性、バインディングプロセス、認証、フェデレーションの標準を示している
アジア	シンガポール	NDI Stack	政府主導の領域（Singpass、My Info）と民間事業者と協働するサービス・アプリケーション領域の体制が示されている
	インド	India Stack	Aadhaarを基盤として、APIで民間事業者・行政サービスと接続することで国民の金融包摂を図ることが概念化されている

（補足）各トラストフレームワークの参照先

国・地域		名称	特徴
欧州	EU	Regulation 910/2014 : eIDAS（2.0）	特定の標準の参照は確認できない
	ドイツ	IDunion Network	フレームワーク自体がToIP Stackをリファーしており、その中でもW3C VCs、OpenID Connect、IETF SAMLなどの標準を参照している
	イギリス	The UK digital identity and attributes trust framework	各参加主体とそれらに共通するルール・ガイドラインとして、mDL、情報管理、暗号化アルゴリズムに関するISO/IEC標準やOpenID Connect、W3C VCs、NIST サイバーセキュリティフレームワーク、SP 800-175B等の多数の国際標準を参照している
北米	米国	Identity Ecosystem Framework : IDEF	IDESG スタンダードレジストリにおいて参照すべき標準として、認証はSAML、OpenID Connect、認可はOAuth 2.0、リスクマネジメントはNIST SP 800-37、セキュリティ・プライバシー管理はNIST SP 800-53、情報セキュリティマネジメントはISO 27002が指定されている
		NIST SP 800-63-3 NIST SP 800-63-4	W3C VCs及びISO/IEC 18013-5:2021（mDL）に対応した記載の追加をSP 800-63-4への改訂で検討している
	カナダ	Pan-Canadian Trust Framework : PCTF	デジタルウォレットの相互運用性のためにサポートすべき標準の例としてW3C VCs、DIDsを紹介しているほか、認証プロセスやクレデンシャルのライフサイクルなどでNIST SP 800-63を参照している
オセアニア	オーストラリア	Trusted Digital Identity Framework	IDフェデレーションにおけるSAML、OpenID Connectの活用に関する文書が存在するほか、参加者のロール要件において、生体認証バインディングについてISO/IEC 30107-1、CSPの満たすべき要件としてNIST SP 800-63Bなどを参照している
		Trust ID Framework	特定の標準の参照は確認できない（詳細不明）
	ニュージーランド	Digital Identity Trust Framework	特定の標準の参照は確認できない
		Identity management standards	特定の標準の参照は確認できない
アジア	シンガポール	NDI Stack	特定の標準の参照は確認できない
	インド	India Stack	特定の標準の参照は確認できない

（補足）トラストフレームワークの規定する内容の整理

地域・国			欧州		
			EU	ドイツ	イギリス
名称			Regulation 910/2014：eIDAS（2.0）	IDunion Network	The UK digital identity and attributes trust framework
策定主体			欧州委員会（政府主導）	資金提供：連邦経済気候行動省 主体：民間企業、政府機関、教育機関（官民共同）	デジタル文化・メディア・スポーツ省（政府主導）
強制力の有無			強制（EU加盟国に適用）	任意	任意
認定の有無			EU加盟国はトラストサービスの認定事業者のトラステッドリストを作成し、公開する義務を負う	なし	現在35事業者が認定サービスプロバイダとして登録・公開（認証機関についても現在5機関の申請あり
原理・原則			EUの電子商取引に統一した基準を設けることを目的として策定	世界中で使用でき、ヨーロッパの価値観と規制に基づいた分散型ID管理のためのオープンエコシステムを作成すること	人々が自分が誰であるか、または自分自身に関する情報を証明できるサービスをより簡単かつ安全に使用できるようにすること
ガバナンス	ステークホルダーの定義・要件		eIDにおけるノード実装者やトラストサービスプロバイダ等の役割・責任を規定	Issuer-Holder-Verifier間の役割の定義とガバナンスを規定している	デジタルID、属性情報を提供するステークホルダーについて規定している
	プロセスの定義・要件		なし	VCのフォーマットとプロトコルを使用したデータ交換プロセスを規定している	各ステークホルダーがデジタルID、属性情報を提供するプロセスについて規定している
	コンポーネントの定義・要件		EUDIWの提供について義務化している ※eIDASの外部だがEUDIWアーキテクチャ・リファレンスフレームワークは**自己主権型アイデンティティに近しい傾向が伺える**	**ブロックチェーンや分散型台帳の運用ポリシーや手順、デジタルエージェントのセキュリティについて規定**している	なし
テクノロジー	特定技術の参照・指定	分散型ID関連	なし	**W3C DIDs**	**W3C VCs**
		一般的な認証・認可	なし	**OpenID Connect** **LDAP** **SAML**	**OpenID Connect**
		レジストリ	なし	**Hyperledger Indy**	なし
	独自の技術の参照・指定		なし ※eIDASノード導入のためのサンプルソフトウェアを開発している	なし	なし

（補足）トラストフレームワークの規定する内容の整理

地域・国			北米		
			米国		カナダ
名称			Identity Ecosystem Framework：IDEF	NIST SP-800-63-3 NIST SP-800-63-4	Pan-Canadian Trust Framework：PCTF
策定主体			NSTIC IDESG（民間主導） 現在はKantara Initiativeに移管	NIST：米国国立標準技術研究所（政府主導）	DIACC：カナダデジタル識別認証評議会（官民共同）
強制力の有無			任意	任意	任意
認定の有無			なし ※自己評価によるIDEF Registry への登録はある	なし	Voilà Verified Trustmark Program によってPCTFへの準拠を認定している
原理・原則			NSTICにおいて示された「個人、企業、その他の組織が機密性の高い取引をオンラインで行う際に、より大きな信頼とセキュリティを享受できる未来」の実現	デジタルアイデンティティサービスを実装する連邦機関のための技術的要件の提供	サービスとネットワークの信頼を検証することにより、現在および将来のカナダのデジタルアイデンティティエコシステムのイノベーションニーズを満たす
ガバナンス	ステークホルダーの定義・要件		Identity Ecosystem の参加主体の担うべき役割と必要なアクション、及びプライバシー・セキュリティ等の要件を定義している	デジタルアイデンティティモデルとして、サブスクライバ、アプリカント、RP等の参加者を定義している	PCTFの中のクレデンシャル等のコンポーネントにおいて、参加するエンティティとその役割について定義している
	プロセスの定義・要件		なし	デジタル認証における**アイデンティティの登録と検証プロセスを規定している**	デジタルIDの作成、管理、提供に係る一連のプロセスなどを定義している
	コンポーネントの定義・要件		なし	AALで許可されている認証デバイスについて規定している	**デジタルウォレット、インフラ等のコンポーネントの要件を定義**している
テクノロジー	特定技術の参照・指定	分散型ID関連	なし	**W3C VCs・mDL**について記載を検討	**W3C VCs、DIDs**
		一般的な認証・認可	**SAML** **OpenID Connect** **OAuth 2.0 など**	なし	なし
		レジストリ	なし	なし	なし
	独自の技術の参照・指定		なし	なし	なし

（補足）トラストフレームワークの規定する内容の整理

地域・国			オセアニア			
			オーストラリア		ニュージーランド	
名称			Trusted Digital Identity Framework：TDIF	Trust ID Framework	Digital Identity Trust Framework	Identification Management Standards
策定主体			DTA：デジタルトランスフォーメーション庁（政府主導）	APC：オーストラリア決済評議会（民間主導）	ニュージーランド政府（政府主導）	ニュージーランド 内務省（政府主導）
強制力の有無			任意	任意	任意	任意
認定の有無			4種類の認定参加者を規定し、TDIFの認定事業者リストを公表している	Trust ID フレームワークへの参加は現在開発中の認定要件を満たすすべての組織に開かれている（詳細未公表）	認定を受けたデジタルIDサービス事業者を「TFプロバイダー」として定義・登録する	なし
原理・原則			ユーザー中心、自主性と透明性、プライバシーの向上等の8つの指導原則を持っている	詳細未公表につき不明	個人および組織に安全で信頼できるデジタルIDサービスを提供する法的枠組みを確立する	組織が適切なエンティティに関する適切な情報を持っていることを保証し、ID詐欺のリスクを最小限に抑えるため
ガバナンス	ステークホルダーの定義・要件		4種類の認定参加者を規定し、それぞれの機能要件について定義している		デジタルIDサービス事業者の種別・提供サービス等について規定している	なし
	プロセスの定義・要件		ロール要件において、アイデンティティ証明のライフサイクルプロセスについて定義している		なし	なし
	コンポーネントの定義・要件		なし		なし	なし
テクノロジー	特定技術の参照・指定	分散型ID関連	なし		なし	なし
		一般的な認証・認可	OpenID Connect 1.0 SAML 2.0		なし	なし
		レジストリ	なし		なし	なし
	独自の技術の参照・指定		なし		なし	なし

（補足）トラストフレームワークの規定する内容の整理

地域・国			アジア	
			シンガポール	インド
名称			NDI Stack	India Stack
策定主体			GovTech：政府技術庁（政府主導）	UIDAI：固有識別子庁（政府主導）
強制力の有無			任意	任意
認定の有無			なし	なし
原理・原則			不明	不明
ガバナンス	ステークホルダーの定義・要件		政府主導の領域（Singpass、My Info）と民間事業者と協働するサービス・アプリケーション領域の体制が示されている	Aadhaarを基盤として、APIで民間事業者・行政サービスと接続することで国民の金融包摂を図ることが概念化されている
	プロセスの定義・要件		なし	なし
	コンポーネントの定義・要件		なし	なし
テクノロジー	特定技術の参照・指定	分散型ID関連	なし	なし
		一般的な認証・認可	なし	なし
		レジストリ	なし	なし
	独自の技術の参照・指定		Singpass, My InfoとのAPI接続	AadhaarとのAPI接続

3. 詳細調査結果：

3.1 共通識別番号・デジタルIDに関する政策動向

3.2 トラストフレームワークの策定状況

3.3 自己主権型／分散型アイデンティティに関する取り組み・ユースケース

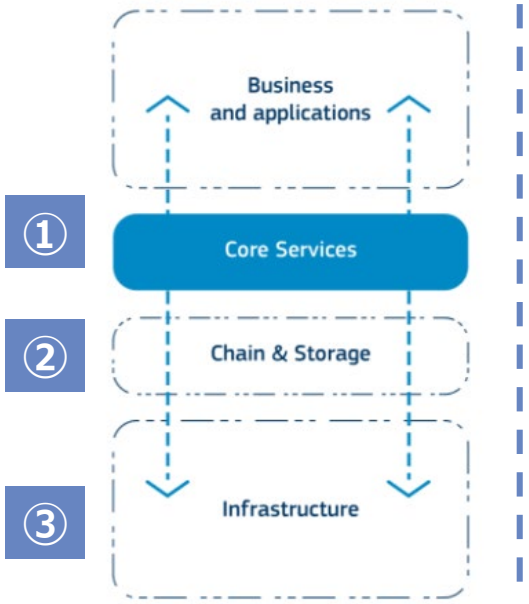
3.3 詳細調査結果：自己主権型／分散型アイデンティティに関する取り組み

3.3.1欧州（EU、ドイツ、イギリス）における調査結果

EBSI

- 欧州ブロックチェーンパートナーシップ（EBP）は欧州委員会と連携し、ヨーロッパ全土に分散したノードのブロックチェーンネットワークを構築するイニシアチブである「欧州ブロックチェーンサービスインフラストラクチャ（EBSI）」を実行しており、各ノードはEBPが指定した各加盟国当局によって運用されている[1]
- EBSIプラットフォームのアーキテクチャは①「コアサービス層」、②「チェーン・ストレージ層」、③「インフラ層」の３層から構成されている。EBSIはプラットフォームが対応するアプリケーションとして、VCやデジタルウォレットを挙げており、EU Digital Identityのアーキテクチャ・リファレンスフレームワークに関する文書にも、一部のユースケースにEBSIが活用できる旨記載されている[2]

EBSIプラットフォームのアーキテクチャ



① **コアサービス層**
アプリケーションを開発する第三者へ提供される、EBPによって定義された要件への準拠を保証するインターフェース（API）のセット

② **チェーン・ストレージ層**
EBSIによってサポートされている、ブロックチェーンとオフチェーンストレージプロトコル

③ **インフラ層**
ブロックチェーンネットワークへの接続を提供するもの

出所）
1 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI
2 https://webgate.ec.europa.eu/regdel/web/meetings/2409/documents/6689

EBSIとeIDASの連携

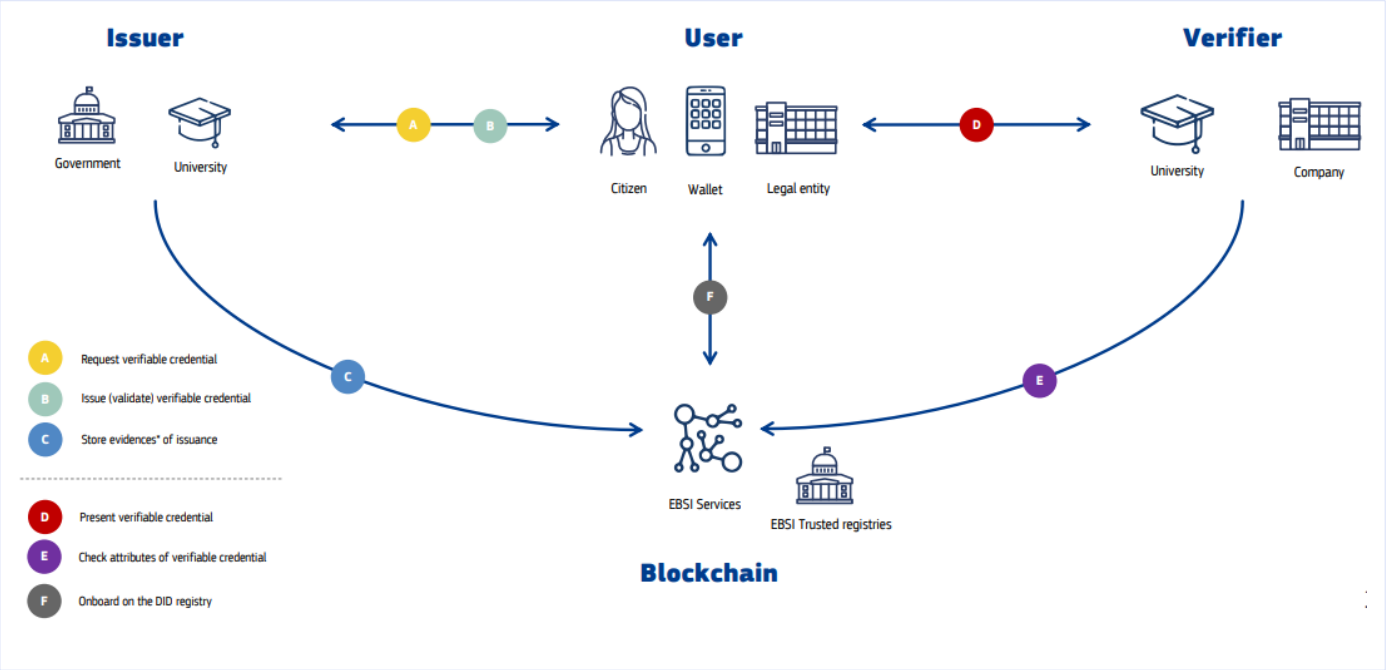
- EBSIのプロジェクトの一つとして、「欧州自己主権アイデンティティフレームワーク（ESSIF）」によってブロックチェーンを用いたSSIの検討が進められており、その中でSSI eIDAS bridgeというコンポーネントが開発されている
- SSI eIDAS bridgeは、ブロックチェーンによって、issuerによる検証可能な資格情報（VC）の発行・電子署名と、verifierによるVCの検証の橋渡しをする機能であり、eIDASが規定するトラストサービス等をSSIのエコシステムに組み入れるものである
- ESSIFは、その活動の中で「eIDASなど既存のブロックを統合/調整する」と述べており、eIDASとEBSIの構築するブロックチェーンは相互に活用されるものと思われる

SSI eIDAS bridgeのイメージ図

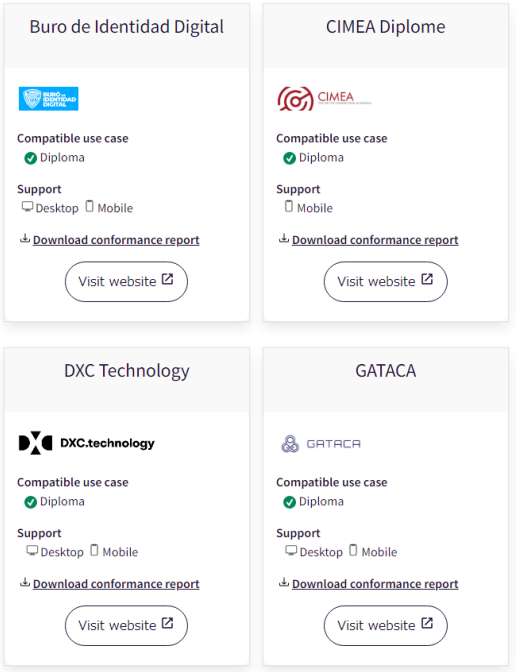
EBSIの想定される活用例

- EBSIの一般的な活用例としては、デジタルウォレットなどのサービスとEBSIのブロックチェーン、レジストリを活用した学生―企業間の検証可能な資格情報（学位）のやり取りなどが想定されている。EBSIはウォレットプロバイダーに対して、仕様の公開とコンフォーマンステストを提供し、2021年には85件のウォレットプロバイダーから申請を受け、10件以上のプロバイダに対するテストが開始された
- EBSIは、EBSIのブロックチェーンインフラと検証可能な資格情報、ウォレット等の組み合わせによって、開示範囲の選択を可能にするとしている[1]

EBSIを活用したVC交換のユースケース図



EBSI準拠のウォレットの例[2]



出所）
1 https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi
2 https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Conformant+wallets

eIDASとEBSI、ESSIF、eSSIF-Labの関連性

EUのSSIに関係した政策、取り組みであるeIDASとEBSI、ESSIF、eSSIF-Labのプロジェクトそれぞれに、相互接続性に関する情報がみられた

相互に関連するEUのID政策、取り組み

EBSI ESSIF	• EBSIの仕様にはeIDASのフレームワーク（eID、トラストサービス）とEBSIプラットフォームを連携させるためのeIDAS Bridge APIが存在している。（現在はアーカイブ化されている）[1] • ESSIFのSSI eIDAS BridgeとeIDAS Bridge APIが同一のものであるかは不明だが、ESSIFひいてはEBSIの構築するブロックチェーンインフラとeIDASの規定するID、サービスはある程度の相互接続性を有しているとみられる
eSSIF-Lab	• eSSIF-Labは、SSIを促進するプロジェクトに対し欧州委員会から資金提供を行うプログラムである • 大きくオープンソースのSSIインフラの開発に貢献するプロジェクトと、商用領域でマーケットとSSI技術を統合するプロジェクトに分かれ、2022年現在で合計63プロジェクトに資金提供している • eSSIF-Labは、資金提供したプロジェクトの成果物は実装の際、EBSI、ESSIFや米国のDHS-SVIP（国土安全保障省シリコンバレーイノベーションプログラム）との相互接続性テストを実行するとしている[2]

出所）
1 https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/%5Barchived%5DeIDAS+Bridge+API#:~:text=What%20is%20the%20eIDAS%20Bridge%20API%20service%20This,Decentralised%20Identifiers%2C%20or%20DIDs.%20Why%20we%20need%20it
2 https://essif-lab.github.io/framework/docs/ssi-standards

EUの取り組みで参照される国際標準

EBSI（ESSIF）、eSSIF-Labのそれぞれに、W3C、DIF、IETF、ToIPといった主要な国際標準規格への参照、サポートが見られた

各取り組みで参照される技術・標準

EBSI ESSIF	• EBSIはブロックチェーン基盤に、Linux Foundationのオープンソースのブロックチェーンフレームワークである、Hyperledgerを使用している • EBSIのシステム中で使用される識別子、データモデルには、W3C Decentralised Identifiers (DIDs), W3C Verifiable Credentials (VCs), W3C Verifiable Presentations (VPs), OpenID Connectなどを基にしているとされる[2] • EBSIは電子署名、eシールのなされたVC、VPのやり取りにおける規格として、IETFのJSON Web Signature、JSON Web Token、JSON Web Keyを現在サポートしている。また、eIDASの定める中で最も高レベルのセキュリティが担保された電子署名レベルであるAdESのセキュリティレベルにJSON形式で適応させたJAdESをサポートしている
eSSIF-Lab	• eSSIF-Labは、eSSIF-Labの構築するSSIインフラはW3C、Aries、DIF、ToIPの技術と相互接続性がなければならないとしている • また、ほとんどのeSSIF-Labの資金提供の対象者は、それらの国際標準化活動に積極的に参加していると活動報告で述べられている[3]
eIDAS（参考）	• 技術下位規則の整備は、現状では改正提案の原文にも、「eIDAS2.0の発効から12か月以内に●●に必要な規格の参照番号を定めるものとする」と記載されているのみ

出所）
1 https://essif-lab.eu/wp-content/uploads/2021/03/essif-booklet_last-version.pdf
2 https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Playbook
3 https://cordis.europa.eu/project/id/871932/reporting

EUDIWに関する公共調達情報

欧州委員会による公共調達事業の中にデジタルIDに関する開発・調査事業が確認でき、その内容は「EUのデジタルアイデンティティフレームワークを提案」「EUDIWを開発、実装する手段を提供」と記載されており[1]、先述のEU Digital IdentityやEUDIWの検討に大きく関係するものと思われる

デジタルIDに関する公共調達の概要

項目	概要
調達元	欧州委員会、通信ネットワーク・コンテンツおよび技術総局(CONNECT)
件名	Belgium-Brussels: Framework Contract for Fixed Price and Quoted Time and Means for Development, Consultancy and Support for the European Digital Identity Wallet （ベルギー-ブリュッセル:欧州デジタルアイデンティティウォレットの開発、コンサルティング、サポートのための固定価格と見積り時間および手段の枠組み契約）
実施内容（抜粋）	欧州のデジタルアイデンティティフレームワークの提案と、共通の組合ツールボックスに関する欧州委員会の勧告に基づいて、欧州デジタルアイデンティティウォレットを開発および実装する手段を提供する。ウォレットおよびその他の関連コンポーネントは、欧州のデジタルアイデンティティの枠組みに関する規則の要件を実施するために、加盟国およびその他の利害関係者に提供される。2022年末には、大規模なパイロットテストが実施される予定である。
調達価格	最大2億6千万ユーロ（約37億円）
入札開始日	2022年7月25日

出所）
1 https://ted.europa.eu/udl?uri=TED:NOTICE:309685-2022:DATA:EN:HTML&tabId=3

（補足）EUDIWに関連する公共調達で参照される標準

EU
ドイツ
イギリス

EUDIWに関係するEUの公共調達事業は、eIDASに定めるEUDIWの具体化のためのプロトタイプ開発等を実施するものであり、参照される技術が公募資料に記載されている[1]

公共調達で参照される標準

調達事業の概要	• 本事業は、EUDIWのプロトタイプウォレットの開発・実装を通じて、EUデジタルアイデンティティフレームワークの策定や、共通ツールボックス（2022年10月上旬公開予定）の策定にも携わるものである • エコシステムの補助ソフトウェア開発や、2022年第4四半期～2023年第4四半期までの、EU加盟国への実装も事業範囲に含まれている
参照される技術・標準	事業の技術選定基準には、以下のような参照すべき技術・標準が列挙されている • SAML（ユーザー認証を行うためのマークアップ言語規格） • CTAP（デバイスの近距離通信インターフェース） • OAuth（アクセス権限認可プロトコルの標準） • OpenID Connect（ oAUTH を拡張したアイデンティティ認証プロトコル） • DIDComm（DIDを使用したメッセージコミュニケーション等の仕様） • ISO/IEC 18013-5:2021– mDL（モバイル運転免許証の規格） • AnonCreds（検証可能な資格情報のデファクト標準） • W3C DIDs • W3C VCs

出所）
1 https://etendering.ted.europa.eu/cft/cft-documents.html?cftId=10237

EUDIWに関するパイロットプロジェクト-1

欧州委員会は2022年2月、EUDIWの試験運用を行うためにパイロットプロジェクトの募集を行った。[1]パイロットプロジェクトは2022年10月に発表される予定の共通ツールボックスに基づいた、「モバイル運転免許証」「決済」「eHealth」「教育・職業資格」等のテーマに焦点を当てたものが募集された[2]

パイロットプロジェクトの募集概要

項目	概要
調達元	欧州委員会、デジタルヨーロッパプログラム（DIGITAL）
件名	Support to the implementation of the European Digital Identity Framework and the implementation of the Once Only System under the Single Digital Gateway Regulation（ヨーロッパのデジタルアイデンティティフレームワークの実装とシングルデジタルゲートウェイ規制の下でのワンスオンリーシステムの実装へのサポート）
実施内容（抜粋）	EUDIWとそのエコシステムの試験的実装、およびワンスオンリーの原則に関連する優先分野でのユース ケースの試験的実施、および参照技術、標準、コンポーネント、ソリューションの検証を行う。ユースケースは、EBSIなどの電子台帳を活用した資格情報の交換といった分散型テクノロジーに基づいて構築される場合がある。 ウォレット、資格情報の発行国及び依拠当事者の国としてEUの3カ国以上が含まれている必要がある。 ＜優先分野＞ **・モバイル運転免許証**：運転免許資格の提示・証明を行う **・決済**：オンラインや実店舗での商品・サービスに対する支払いを行う **・eHealth**：個人の医療記録等のヘルスデータにアクセスするための証明を行う **・教育・職業資格**：公的機関または民間企業に対して、教育・職業資格を証明する **・その他**：デジタル旅行証明書や社会保障等の分野
入札開始日	2022年2月22日
提案期限	2022年8月17日

出所）
1 https://www.biometricupdate.com/202202/tender-launched-for-european-digital-identity-wallet-pilots
2 https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-deploy-02-electronic-id

EUDIWに関するパイロットプロジェクト-2

前記のパイロットプロジェクトについて、2022年12月に欧州委員会は5つの国際コンソーシアムの提案を採択したことを発表した[1]

採択されたパイロットプロジェクトの概要

コンソーシアム名	取り組み分野	パイロットプロジェクトの概要
DC4EU	教育・社会保障	デジタルIDウォレットを活用した、欧州域内における基本的な教育資格や専門資格、欧州健康保険証（EHIC）などの発行・利用を行う 出所）https://www.dc4eu.eu/
EU Digital ID Wallet Consortium（EWC）	旅行・支払い	旅行者が欧州域内を旅行するにあたり、チケットやパスポート、就労資格などの旅行証明書をデジタルIDウォレットで携帯し、オンラインでの支払いを行う 出所）https://eudiwalletconsortium.org/
Vector	教育・社会保障	市民と組織が、教育・社会保障に関する検証可能な資格情報をEBSIの分散型レジストリを使用した形でやり取りを行うユースケースを検証する 出所）https://wiki.sunet.se/display/Projekt/VECTOR
POTENTIAL	モバイル運転免許証 eHealth その他	デジタルIDウォレットを使用し、行政手続き、口座開設、電子署名、電子処方箋、SIMカード登録、モバイル運転免許証の提示等のユースケースを検証する 出所）https://www.digital-identity-wallet.eu/
NOBID	決済	デジタルIDウォレットを使用して、PSD2＊に基づく本人確認及び取引を実行し、販売店や個人に対する支払いを行う 出所）https://www.nobidconsortium.com/our-proposal/

＊PSD2（欧州決済サービス指令第2版）： 2015年に成立した国際市場における決済サービスについて定めた欧州議会指令であり、銀行が顧客本人の同意に基づいて、口座情報にアクセスするAPIを第三者（Fintech企業等）に提供することを可能にする

出所）
1 https://wiki.sunet.se/display/Projekt/EUDIW

ユースケース：DC4EU_教育資格・社会保障データの管理

分野：教育・行政
フェーズ：PoC
EU
ドイツ
イギリス

概要

- 欧州委員会は2022年2月、EUDIWの試験運用を行うために、パイロットプロジェクトの募集を行い、2022年12月に5つの国際コンソーシアムの提案を採択したことを発表した[1]
- DC4EUは教育及び社会保障の分野でパイロットを行い、eIDやEUDIリファレンスウォレット、ブロックチェーンを活用した市民によるデータコントロール、プライバシーの向上を図るとしている[2]

エンティティ

- 国家機関（ユースケースの関連領域や加盟国間の連携を主導）
- 公的・民間の依拠当事者
- 専門教育資格、健康保険証（EHIC）発行主体
- ウォレットユーザー（EU市民及び居住者）

使用されている技術

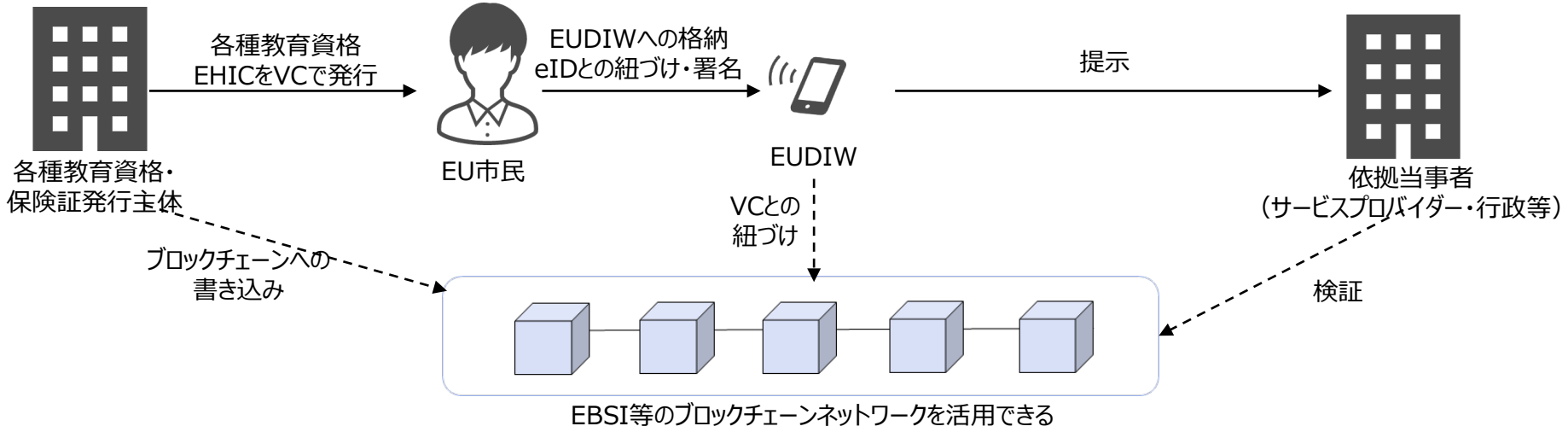
- W3C VCs、ブロックチェーン（EBSI）

扱う属性情報

- eID、専門教育資格、健康保険証（EHIC）等

ペインポイント	提供する価値
信頼性の高い電子認証手段へのアクセスができない	ブロックチェーンを電子認証手段に適用したセキュリティの向上
個人データの共有をユーザーがコントロールすることができない	EUDIWへのVCの発行に依るデータコントロールの実現

ビジネスモデル



※パイロットの詳細が不明であるため、コンソーシアム発表の情報を基にEUDIWのリファレンスモデルなどで補足

出所）
1 https://wiki.sunet.se/display/Projekt/EUDIW
2 https://dc4eu.eu/#toggle-id-4

ユースケース：EWC_欧州域内旅行での情報提示

分野：旅行・小売
フェーズ：PoC
EU
ドイツ
イギリス

概要

- 欧州委員会は2022年2月、EUDIWの試験運用を行うために、パイロットプロジェクトの募集を行い、2022年12月に5つの国際コンソーシアムの提案を採択したことを発表した
- EWC（EUDIWコンソーシアム）は、欧州域内の旅行における旅客機へのチェックイン、ショッピングの支払いなどをEUDIWで資格情報をコントロールすることにより検証するとしている

エンティティ

- 国家機関（ユースケースの関連領域や加盟国間の連携を主導）
- 公的・民間の依拠当事者
- 属性情報、資格情報及び認証プロバイダ
- ウォレットユーザー（EU市民及び居住者）

使用されている技術

- 不明

扱う属性情報

- 旅行者情報、支払い資格情報、企業ID等

ペインポイント

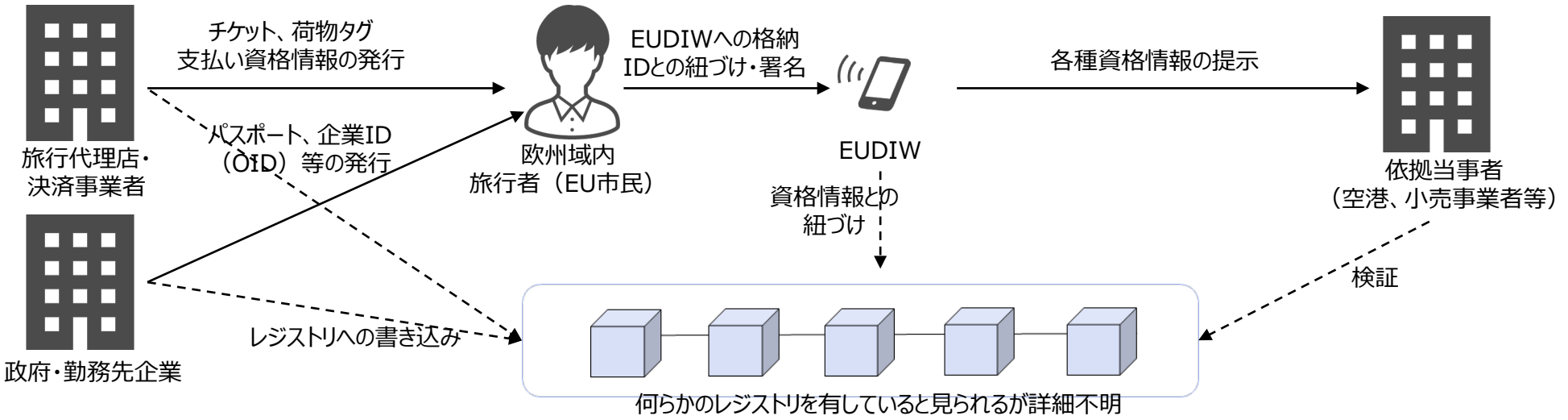
旅行において必要な全てのID、資格情報を管理することが煩雑である

加盟国間で使用できない資格情報等が存在する

提供する価値

チケットやパスポート、企業・国の個人ID、支払資格情報などを国境を跨ぎEUDIWで一括管理、提示できる

ビジネスモデル



※パイロットの詳細が不明であるため、コンソーシアム発表の情報を基にEUDIWのリファレンスモデルなどで補足

出所）
1 https://wiki.sunet.se/display/Projekt/EUDIW
2 https://eudiwalletconsortium.org/

ユースケース：Vector_教育資格・社会保障データの管理

分野：教育・行政
フェーズ：PoC
EU
ドイツ
イギリス

概要

- 欧州委員会は2022年2月、EUDIWの試験運用を行うために、パイロットプロジェクトの募集を行い、2022年12月に5つの国際コンソーシアムの提案を採択したことを発表した[1]
- VectorはDC4EUと同様に教育及び社会保障の分野でパイロットを行うが、EBSIからの支援を受けたパイロットプロジェクトと並行しており、ESSPASS、EHIC、EUROPASSなどのプロジェクトとも連携するとしている[2]

エンティティ

- 国家機関（ユースケースの関連領域や加盟国間の連携を主導）
- 公的・民間の依拠当事者
- 専門教育資格、健康保険証（EHIC）発行主体
- ウォレットユーザー（EU市民及び居住者）

使用されている技術

- W3C VCs、W3C DIDs、ブロックチェーン（EBSI）

扱う属性情報

- eID、専門教育資格、健康保険証（EHIC）等

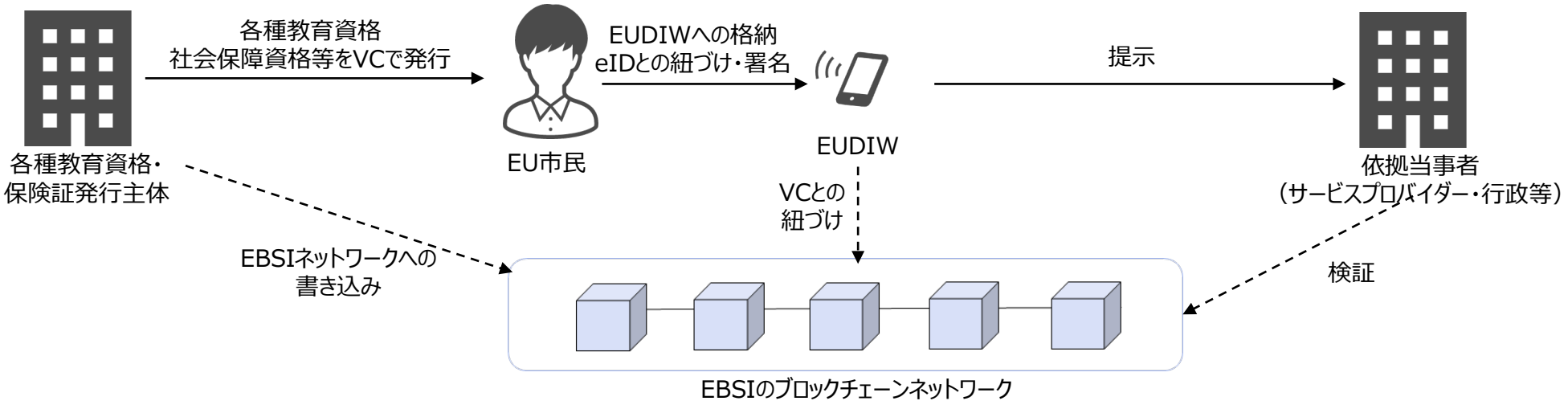
ペインポイント

信頼性の高い電子認証手段へのアクセスができない
個人データの共有をユーザーがコントロールすることができない

提供する価値

ブロックチェーンを電子認証手段に適用したセキュリティの向上
EUDIWへのVCの発行に依るデータコントロールの実現

ビジネスモデル



※パイロットの詳細が不明であるため、コンソーシアム発表の情報を基にEUDIWのリファレンスモデルなどで補足

出所）
1 https://wiki.sunet.se/display/Projekt/EUDIW
2 https://wiki.sunet.se/display/Projekt/VECTOR

ユースケース：POTENTIAL_市民サービスへのアクセス改善

分野：交通・医療・金融・行政
フェーズ：PoC
EU
ドイツ
イギリス

概要

- 欧州委員会は2022年2月、EUDIWの試験運用を行うために、パイロットプロジェクトの募集を行い、2022年12月に5つの国際コンソーシアムの提案を採択したことを発表した[1]
- POTENTIALは金融、モビリティ、医療、行政などの面で実証を行うとしており、電子署名機能を活用した電子政府サービス利用や銀行口座開設、mDLの警察への提示、電子処方箋の提示などを例として挙げている[2]

エンティティ

- 国家機関（ユースケースの関連領域や加盟国間の連携を主導）
- 公的・民間の依拠当事者（金融機関、通信事業者、警察、電子行政サービス窓口等）
- 属性情報、資格情報及び認証プロバイダ（政府・行政機関・医療機関等）
- ウォレットユーザー（EU市民及び居住者）

使用されている技術

- mDL

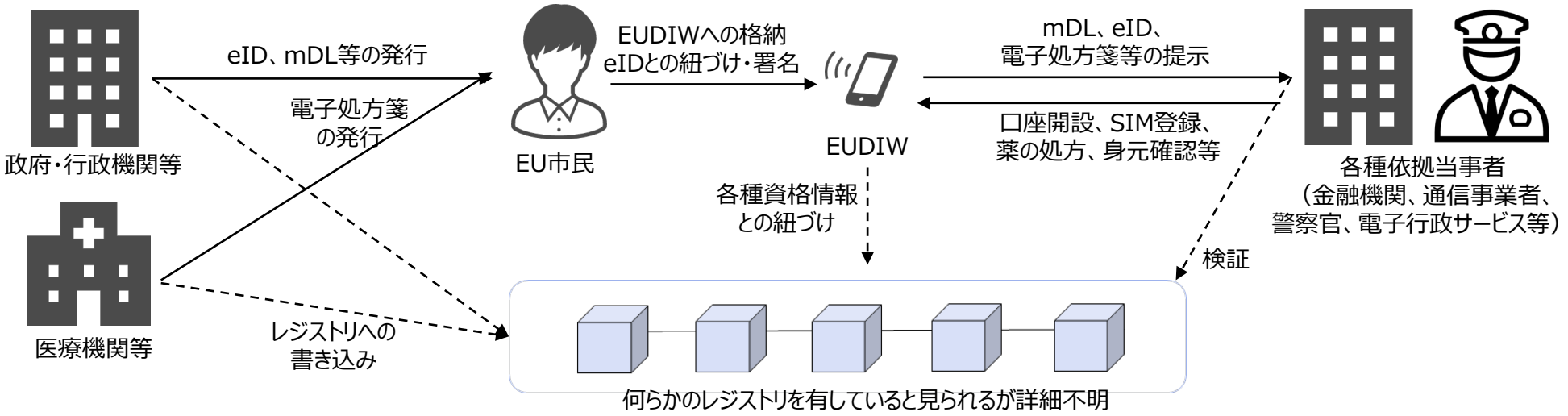
扱う属性情報

- eID、運転免許証（mDL）、処方箋情報等

ペインポイント

ペインポイント	提供する価値
物理的な証明書携行、手動での検証の手間	管理業務・認証プロセスにおけるコスト削減
加盟国間で使用できない資格情報等が存在する	加盟国間での相互運用性の向上

ビジネスモデル



※パイロットの詳細が不明であるため、コンソーシアム発表の情報を基にEUDIWのリファレンスモデルなどで補足

出所）
1 https://wiki.sunet.se/display/Projekt/EUDIW
2 https://www.digital-identity-wallet.eu/

ユースケース：NOBID_国内・国境を越えた電子決済の推進

分野：金融

フェーズ：PoC

EU
ドイツ
イギリス

概要

- 欧州委員会は2022年2月、EUDIWの試験運用を行うために、パイロットプロジェクトの募集を行い、2022年12月に5つの国際コンソーシアムの提案を採択したことを発表した
- NOBIDコンソーシアムは、EUDIWを用いた国内及び国境を跨いだ支払いに焦点を当て、SCT即時支払いや従来の口座間送金などのインフラに基づき、サービス提供者などの支払い要求に応える形で取引を行うとしている

エンティティ

- 国家機関（ユースケースの関連領域や加盟国間の連携を主導）
- 公的・民間の依拠当事者
- 属性情報、資格情報及び認証プロバイダ
- ウォレットユーザー（EU市民及び居住者）

使用されている技術

- 不明

扱う属性情報

- 口座情報等

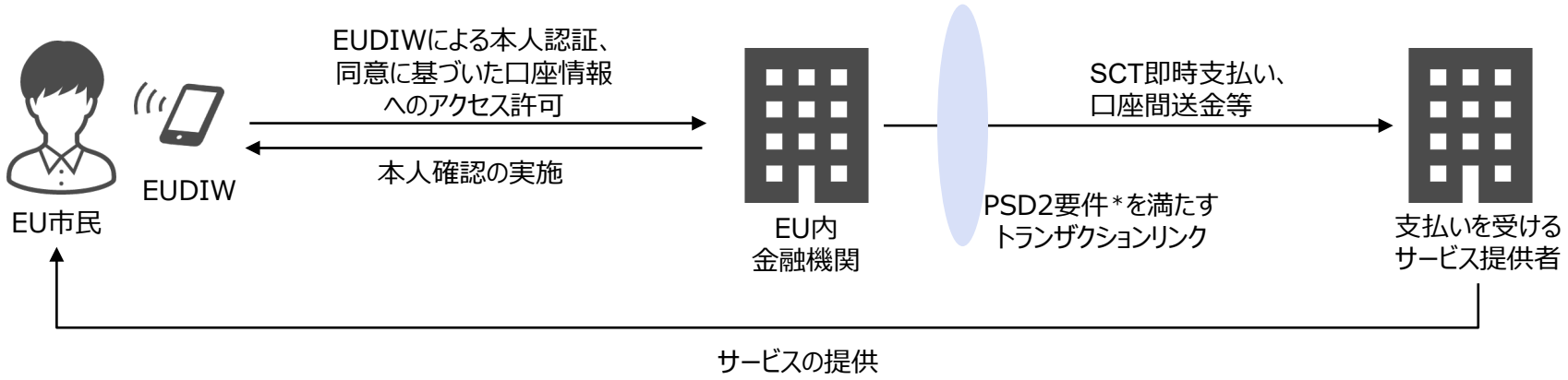
ペインポイント

不明（情報なし）

提供する価値

不明（情報なし）

ビジネスモデル



＊PSD2（欧州決済サービス指令第2版）： 2015年に成立した国際市場における決済サービスについて定めた欧州議会指令であり、銀行が顧客本人の同意に基づいて、口座情報にアクセスするAPIを第三者（Fintech企業等）に提供することを可能にする

出所）
1 https://wiki.sunet.se/display/Projekt/EUDIW
2 https://www.nobidconsortium.com/our-proposal/#_payment

SSIの実現に向けた政府プロジェクト

ドイツでは2020年以降、公共部門のデジタル化を推進するために、SSIのアプローチに基づくデジタルアイデンティティエコシステムの実現に向けた２つの取組を進めている

プロジェクト名称	所管	概要
SSIパイロットプロジェクト[1]	連邦首相府（Bundeskanzleramt）	• 2020年、メルケル首相と18人のドイツのビジネスリーダー（BMW、ドイツ鉄道、ドイツ銀行、Robert Bosch、ダイムラー：現メルセデス・ベンツ・グループなど）とがデジタルIDに関する意見交換を行った結果、同年12月に連邦首相府主導でデジタルIDエコシステムの構築に向けたSSIパイロットプロジェクトシリーズが開始された • 意見交換では、EU域外における大規模なプラットフォームがID市場に参入していることから緊密な協力関係が提案されるとともに、デジタル資格情報の交換と保管の標準を備えた包括的なエコシステムを構築する戦略の概要について説明された • 2020年12月、ドイツ連邦首相府主導の元、デジタルIDエコシステムにおけるSSIパイロットプロジェクトシリーズが開始され、ホテルのチェックイン手続きのデジタル化のユースケースに着手している
Secure Digital Identities ショーケース[2]	連邦経済エネルギー省（Bundesministerium für Wirtschaft und Energie：BMWi）	• 2020年、連邦経済エネルギー省（BMWi）は、イノベーションコンペティション「Showcase Secure Digital Identities」を開始し、スマートフォンを使って日常的にサービスプロバイダーや当局に対してデジタル認証を行う、新しいアイデンティティ・エコシステムの優れたアプローチを公募した • 2020年6月から11月にかけて、選ばれたコンソーシアムはコンペティションフェーズでプロジェクトアイデアの企画を行い、2021年4月からの実施フェーズではBMWiによって4つのショーケースプロジェクト（ID-Ideal、SDIKA、ONCE、IDUnion）が選定された

出所）
1 https://www.bundesregierung.de/breg-de/service/archiv/start-pilot-hotel-check-in-1914392
2 https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.htm

連邦首相府主導のSSIパイロットプロジェクト

2020年12月、ドイツ連邦首相府主導の元、デジタルIDエコシステムにおけるSSIパイロットプロジェクトシリーズが開始され、ホテルのチェックイン手続きのデジタル化のユースケースに着手している[1]

パートナー都市・企業

■ **企業**：ドイツ鉄道、ルフトハンザ、ロバート ボッシュ、BWI、Bundesdruckerei、ドイツ・ホスピタリティ社、モーテル・ワン社、リンドナー・ホテル社、等

技術的な構成要素

■ **デジタルウォレット**：デジタル ID や証明書、証書、承認、チケットなどのその他のデジタル資格情報を保存可能とする

ユースケース

■ **ホテルチェックインの簡素化**

- 企業の出張者が、ホテルにチェックインする際に係る身分証明等のプロセスをデジタルIDを活用して、簡素化する。
- ホテルのチェックインの際に必要となる私人の証明（会社の住所情報）と主権者の証明（身分証明書の属性情報）を企業とサービスプロバイダーからそれぞれ事前に取得し、デジタルIDウォレットに格納しておくことで、チェックインの際にホテル側から提示されるQRコードを読み取るだけでチェックインが可能となる。

出所）
1 https://www.bundesregierung.de/resource/blob/992814/1898280/d9819a40553a9543b9e8f3acb620b0c2/digitale-identitaet-neu-download-bundeskanzleramt-data.pdf

Secure Digital Identities ショーケース

2020年、連邦経済エネルギー省（BMWi）はドイツにおけるeIDASソリューションの開発と行政・（中小）企業・個人への利用促進を目的として「Secure Digital Identities」ショーケースを開始し、2021年にIDunionをはじめとする4つのショーケースプロジェクトを選定している[1]

Secure Digital Identities ショーケースプロジェクトの概要

コンペティション・フェーズ（2020年6~11月）

- Secure Digital Identitiesを実現するための説得力のあるコンセプトアイデアを開発し、実現可能性の観点から課題を明確にするとともに、実装フェーズで迅速かつ効率的に実施を進めるための条件を整備するフェーズ
- 11のプロジェクトがコンペの対象となり、専門家からなる審査員によって評価をされた

実装フェーズ（2021年4月～2024年12月）

- ユーザーが、スマートフォンを使用して日常生活でサービスプロバイダーや当局に対して自分自身をデジタルで識別可能とする相互運用可能なIDエコシステムの構築をめざす。
- 4つのショーケースプロジェクトは、公的機関や民間企業、IDサービスプロバイダー等、すべてのステークホルダーを考慮し、プロジェクト内及び4つのショーケースプロジェクト間の相互運用性にも焦点が当てられている。

- EMIL
- ID-Ideal
- IHRE-ID
- ONCE
- PeopleID
- SDI in NRW
- SDIKA
- SHIELD
- Smartphone ID +
- SSI für Deutschland （IDunion）
- STEREO

ID-Ideal
-セキュアなデジタルIDのマネジメント

ONCE
-シンプルなオンライン登録

SDIKA
–カールスルーエにおけるセキュアデジタルIDのショーケース

SSI für Deutschland （IDunion）
-自然人、法人、モノのためのIDエコシステム

出所）
1 https://www.digitale-technologien.de/DT/Navigation/EN/Foerderprogramme/Sichere_Digitale_Identitaeten/Programm/programm.html

ショーケースプロジェクト：ID-Ideal

4つのショーケースプロジェクトのうち、ID-Idealでは、現代において多数保有されているデジタルIDを単一の安全なデジタルIDに置き換えることで、IDの管理及びそれに関連するデータの主権やセキュリティ両方の維持を可能にすることを目指している[1]

パートナー都市・企業

- **都市・大学**：ミットヴァイダ市役所、ミットヴァイダ大学、ドレスデン技術経済大学
- **企業**：ミットヴァイダ銀行、KAPRIONテクノロジーズ(有)、SALTソリューションズ(有)

技術的な構成要素

- **デジタルウォレット**：デジタル ID や証明書、証書、承認、チケットなどのその他のデジタル資格情報を保存可能とする
- **ID-Ideal トラストフレームワーク**：デジタルウォレットを活用し、様々な当局や期間が発行するデジタルIDを受け入れたり、ユーザーが企業や公的機関に対して、自分自身のデジタル識別したデジタルIDを提示する等、相互にやり取りをする際に必要となる、標準化されたデジタルフォーマットやインターフェスをエコシステムとして提供する。

ユースケース

- **図書館における会員カードの自動登録**
  - 会員カードの申請について、デジタルIDを使用して会員カードの申請や個人情報の更新に関連するすべてのプロセスをオンライン上でワンストップで完結させる。
  - 従来、図書館の利用者や従業員が、紙またはオンラインにて手入力で登録していた会員情報をデジタルIDを使用することで、入力及び個人情報の登録・保管にかかる作業を省力化する。
- **公共交通等モビリティサービス利用のワンストップ登録**
  - バスや電車、タクシー、カーシェアリング、レンタサイクル等、地方自治体や民間企業により提供されているモビリティサービスの利用に際し、個人データやパス、割引資格、支払い情報等のデジタル証明書を利用可能とする。
  - それらを、デジタルウォレットに保存し、サービスごとにプロバイダーに提供することで、サービス毎に必要となる登録の手間を削減する。
- **住所変更に係る個人情報の自動再登録**
  - 市民が居住地を変更する際に発生する、公的機関（登記所や税務署等）や民間企業（銀行や保険会社等）における、住所の登録及び解除の手続きをオンライン上で完結させる。
  - ID-Idealは、市民の登録データを安全に保管し、法的に安全な手順でデータの変更を公的機関や企業に通知するウォレットを開発することで、市民の要求に応じて、必要となるデータが各機関に直接転送できる仕組みを構築する。

出所） 1 https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Use_Cases/Use_Case_1/Use_Case_1.html

ショーケースプロジェクト：ONCE

ONCEは行政、公共交通機関、観光・ホテル業向けのセキュアなデジタルID、デジタルIDアプリケーションの開発・実装を行うことを目的としたプロジェクトであり、スマートフォン・アプリによるID管理を軸に市民のIDデータに対するコントロールの強化を図っている[1]

パートナー都市・企業

- **都市**：ヘッセン州、バイエルン州、ノルトライン・ヴェストファーレン州の各都市
- **企業**：Bundesdruckerei、フランフォーファー研究機構、シュトゥットガルト大学技術経営研究所、ロバート・ボッシュ　他多数

技術的な構成要素

- **ONCE Wallet-App**：スマートフォンでのIDデータの管理・転送と、その後のアクセス管理による制御を可能にしている
- **バックエンドシステム**：デジタルIDのブロックとアップデートのための機能を提供している
- **ONCE ID Gateway**：IDデータを必要に応じてサービスプロバイダに転送を可能にしている
- **統合インターフェース**：オンラインサービスの運営者がIDデータを利用・検証可能にしている

ユースケース

- **運転免許証、自動車登録証等の確認作業への活用**
  - 運転免許証と車両登録のデジタル化により、警察が運転者の情報を検査する際に要する時間を大幅に短縮可能
  - 運転免許証は各免許当局のオンラインポータルで管理でき、運転免許の取り消しや新しい車両の申請は、自宅のデバイスから行うことが可能
  - レンタカーやカーシェアリングの利用時の身分証明書の提示・確認作業においても原本の提示を不要にすることで迅速化することが可能
- **公共施設の利用促進に向けた活用**
  - 博物館、プール、スポーツ施設、文化クラブ、公園、集会所等の公共施設の利用時にデジタルIDを用いることで確認・提示作業を迅速化する
  - 現時点で顔写真等の視覚的特徴を提示する機能がなく、今後ONCEの準拠ウォレットに認証された個人写真を実装することが期待されている
- **地域・自治体の特典サービスの利用促進への活用**
  - デジタルスパカードやゲストカードを導入することで、スマートフォンを経由して入場料の無料や割引等の観光サービスを受けることが可能となる
  - 従来、ホテルの宿泊客には提供されていなかった特典情報が、配信されるようになることで、宿泊客の満足度向上とともに、観光施設側は売上機会の創出につながる

出所）1　https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Use_Cases/Use_Case_3/Use_Case_3.html

ショーケースプロジェクト：SDIKA

SDIKAでは、市民や組織が場所に関係なく、さまざまなアプリケーション間で、行政や民間サービスにデジタル ID を用いてアクセスすることを可能とするエコシステムを構築することを目指している[1]

パートナー都市・企業

- **都市**：カースルーエ市（情報技術・デジタル局）
- **企業**：FZI情報技術研究センター、CASソフトウェア(株)、 INIT(有)、ISB(株)、Jolocom(有)

技術的な構成要素

- **SDI-X システム**：受け入れポイントで様々な発行者のデジタル ID を検証して使用することが可能となる。これによりクラウドベースで一元管理されたIDと自己管理されたID/SSIの両方が利用可能となる。各受け入れポイントがローカルのSDI-Xアダプターを介して接続する。

ユースケース

- **安全で迅速な骨髄提供**
  - ドナーがデジタルIDとしてウォレットに保存した情報を、ドナーの意思の下、必要な情報をドナーデータベースへ転送が可能となる。
  - これまで医療機関が手入力で登録していたドナー登録の作業が省力化されるとともに、医療機関とドナーで迅速な連携が可能となる。
- **ビジネスの立ち上げ加速**
  - 会社（ビジネス）を立ち上げるにあたり、創業期における登記や銀行口座の開設、日々の運営においても都度都度情報の入力や提示が求められるIDデータを、一か所に集約し何度も使いまわすことを可能にすることで、都度発生する作業を省力化する。
  - またePAの電子認証とも連携することで、申請者の認証とその後の手続きの迅速化を可能とする。
- **建築業の申請・許可プロセスの加速化**
  - 民間企業や行政等、様々なステークホルダーが参画する建築業において、デジタル化により申請・許可の管理プロセスをより適切に記録、追跡可能とすることで、加速化を図るとともに、透明性のある管理手法を実現する。

出所） 1 https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Use_Cases/Use_Case_4/Use_Case_4.html

ショーケースプロジェクト：IDunion

Idunionでは、ブロックチェーンベースの自己決定型IDシステム（SSI）を含む、エンドユーザーが自分のID情報を保存および管理でき、欧州及び国際ネットワークと相互運用可能な安全なデジタルIDのための分散型 IDエコシステムを開発することを目標にしている[1]

パートナー都市・企業

- **都市**：ケルン市
- **企業**：ベルリン工科大学、ING-ディバ銀行、ドイツテレコム、シーメンス、neosfer(有)、esatus(株)、ロバートボッシュ(有)等

技術的な構成要素

- **Self Sovereign Identity (SSI)**：ブロックチェーンベースの自己決定型IDシステム

ユースケース

- **サプライチェーンにおける効率的マスター管理データ**
  - 従来、取引等のために、企業のITシステムで主導で保管・管理していた、登記簿の情報や税金、会計データ等を、発行者のビジネスウォレット上に保管可能とすることで、情報の管理・更新に係る手間を省力化し、さらに取引プロセスの透明性を担保とする。
- **教育プログラムの記録やその証明の一元化**
  - 学士・修士課程、交換留学等の際に必要となるコース記録や成績証明書など、学生生活における様々な記録を、単一のデジタルウォレット保存することで、学生が、必要に応じて大学の管理者に送付することが可能となる。
  - 提出する機関に応じて様々な様式（紙、デジタル）で提出する必要があった、コース記録や各種証明書等をデジタルウォレットで保管し、そこから提出することで、データの管理や提出に係る作業を省力化する。
- **2要素認証なしでの安全な支払い（スマートチェックアウト）**
  - オンラインでモノを購入する際、注文手続きにおいて発生する個人情報や住所、支払い情報等の入力の手間を削減するためにブラウザやサービスプロバイダー上に保存しているデータをデジタルウォレットに保管することで、自分自身でアイデンティティ情報を管理することが可能となる。
  - データ保護関連のリスクの解消の他、販売者側は、入力の手間を起因とする注文キャンセルによる機械損失の減少に貢献する。

出所） 1 https://www.digitale-technologien.de/DT/Redaktion/EN/Standardartikel/sdi_use_case_2.html

SSIパイロットプロジェクト：ホテルチェックインの簡素化

分野：旅行

フェーズ：限定的に実運用

EU
ドイツ
イギリス

概要

- 企業の出張者が、ホテルにチェックインする際に係る身分証明等のプロセスをデジタルIDを活用して、簡素化する。ホテルのチェックインの際に必要となる私人の証明（会社の住所情報）と主権者の証明（身分証明書の属性情報）を企業とサービスプロバイダーからそれぞれ事前に取得し、デジタルIDウォレットに格納しておくことで、チェックインの際にホテル側から提示されるQRコードを読み取るだけでチェックインが可能となる[1]

エンティティ

- 費用負担主体：不明
- 価値提供主体：Bundesdruckerei（IDサービスプロバイダー）
- 参加者：企業（従業員）、ホテル

使用されている技術

- 不明

扱う属性情報

- 登記簿の情報や税金、会計データ等

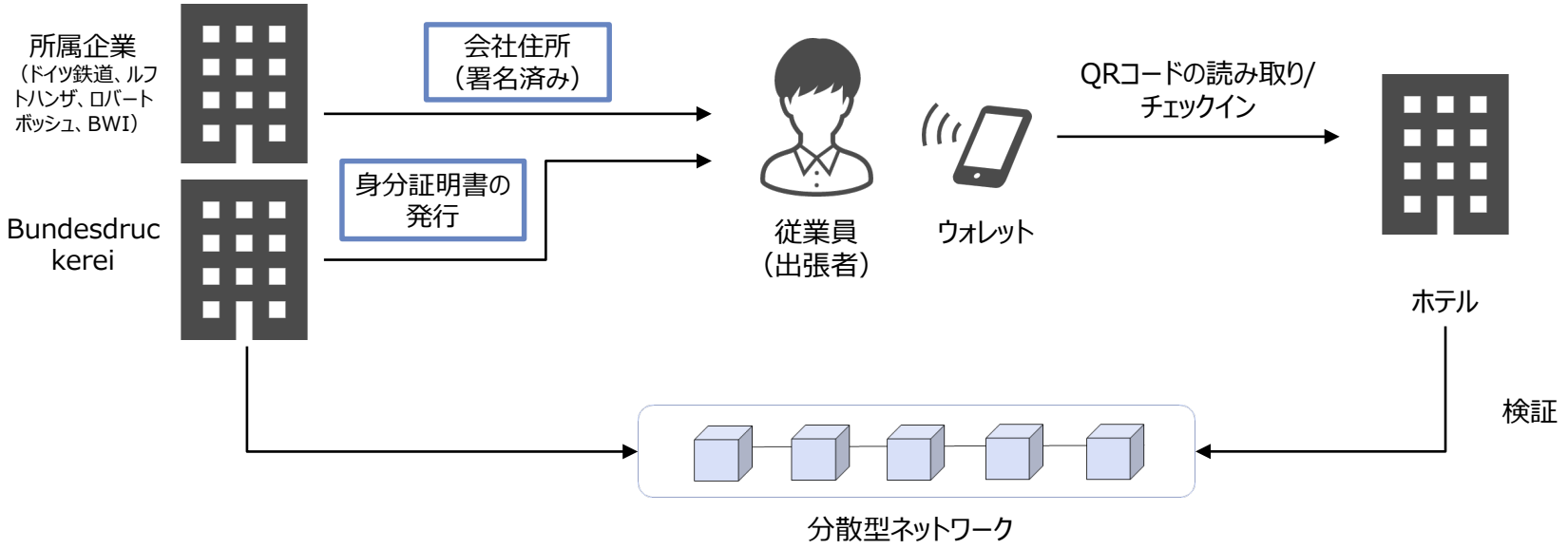
ペインポイント

ホテルのチェックインに係る本人確認とその証明に係る手続き

提供する価値

デジタルIDでの身分証明によるチェックイン手続きの簡素化

ビジネスモデル



出所）1 https://www.bundesregierung.de/resource/blob/992814/1898280/d9819a40553a9543b9e8f3acb620b0c2/digitale-identitaet-neu-download-bundeskanzleramt-data.pdf

ID-Ideal：図書館における会員カードの自動登録

分野：行政

フェーズ：PoC

EU
ドイツ
イギリス

概要

- 会員カードの申請について、デジタルIDを使用して会員カードの申請や個人情報の更新に関連するすべてのプロセスをオンライン上でワンストップで完結させる。
- 従来、図書館の利用者や従業員が、紙またはオンラインにて手入力で登録していた会員情報をデジタルIDを使用することで、入力及び個人情報の登録・保管にかかる作業を省力化する[1]

エンティティ

- 費用負担主体：不明
- 価値提供主体：ID-Ideal
- 参加者：図書館、公共施設

使用されている技術

- 不明

扱う属性情報

- 氏名、住所情報等

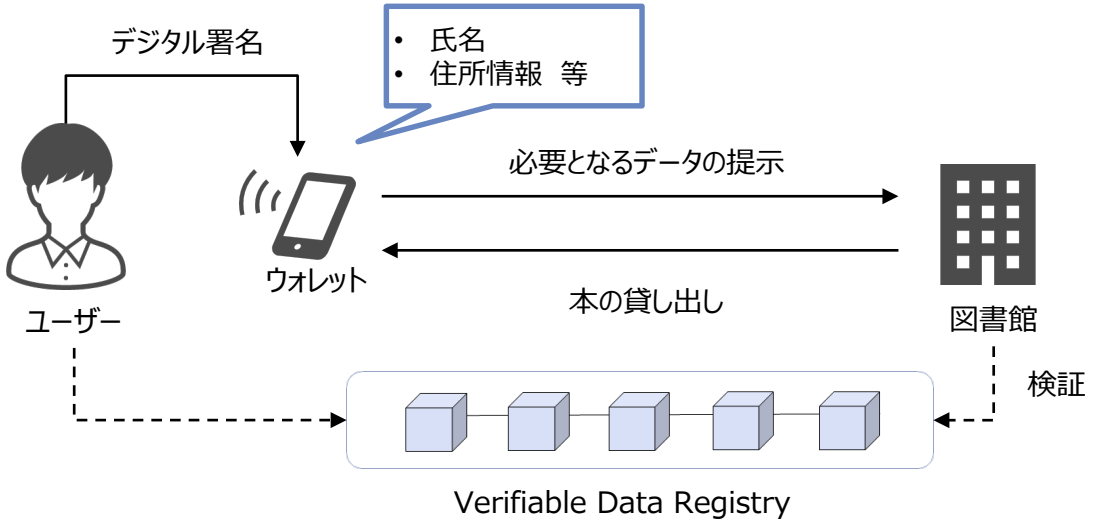
ペインポイント

会員カード作成更新に係る個人情報提示の手間

提供する価値

ユーザーの登録手続きの削減、図書館職員の登録手続きの削減

ビジネスモデル



出所）1　https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Use_Cases/Use_Case_1/Use_Case_1.html

ID-Ideal：公共交通等モビリティサービス利用のワンストップ登録

分野：交通
フェーズ：PoC
EU
ドイツ
イギリス

概要

- バスや電車、タクシー、カーシェアリング、レンタサイクル等、地方自治体や民間企業により提供されているモビリティサービスの利用に際し、個人データやパス、割引資格、支払い情報等のデジタル証明書を利用して、それらを、デジタルウォレットに保存し、サービスごとにプロバイダーに提供することで、サービス毎に必要となる登録の手間を削減する[1]

エンティティ

- 費用負担主体：不明
- 価値提供主体：ID-Ideal
- 参加者：公共交通機関、モビリティサービスプロバイダー

使用されている技術

- 不明

扱う属性情報

- パスや割引資格、支払い情報等

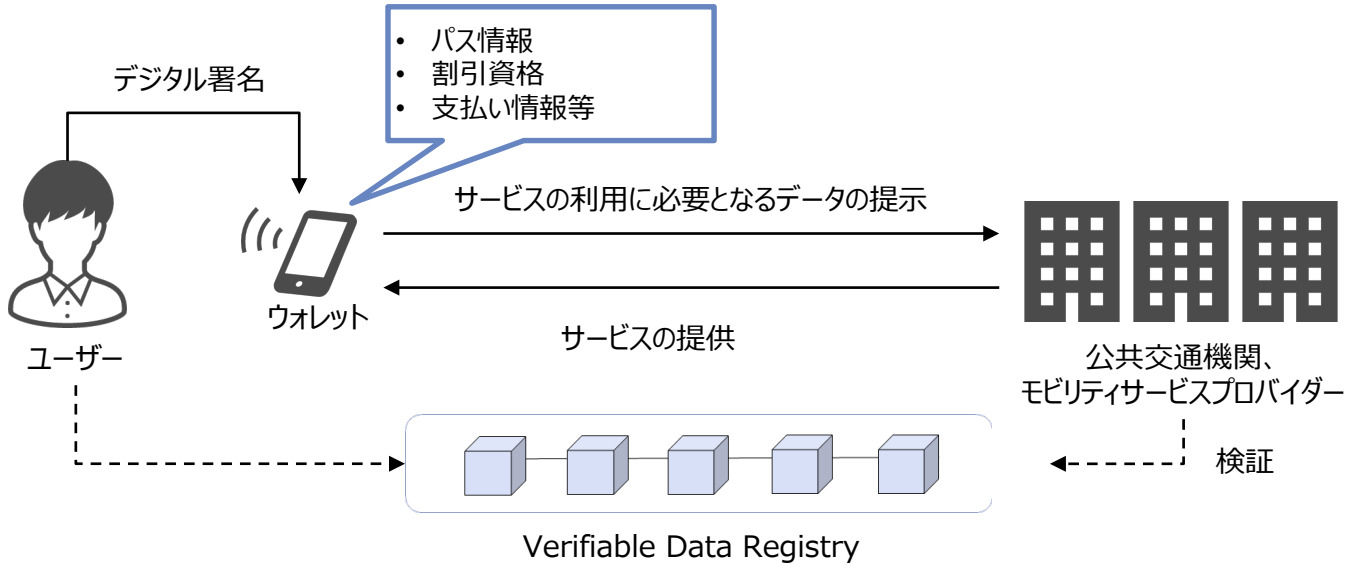
ペインポイント

利用するモビリティサービスごとに登録が必要となる

提供する価値

サービス毎に必要となるデータが提示されワンストップでの登録が可能となる

ビジネスモデル



出所） 1 https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Use_Cases/Use_Case_1/Use_Case_1.html

ID-Ideal：住所変更に係る個人情報の自動再登録

分野：行政
フェーズ：PoC
EU
ドイツ
イギリス

概要

- 現在、市民が居住地を変更する場合、公的機関（登記所や税務署等）や民間企業（銀行や保険会社等）において、登録または登録の解除が必要となり、多大な労力を要している
- 市民の登録データを安全に保管し、法的に安全な手順でデータの変更を公的機関や企業に通知するウォレットを開発することで、市民の要求に応じて、必要となるデータが各機関に直接転送できる仕組みを構築する[1]

エンティティ

- 費用負担主体：不明
- 価値提供主体：ID-Ideal
- 参加者：公的機関：登記所、税務署等、民間企業：銀行、保険会社等

使用されている技術

- 不明

扱う属性情報

- 住所情報

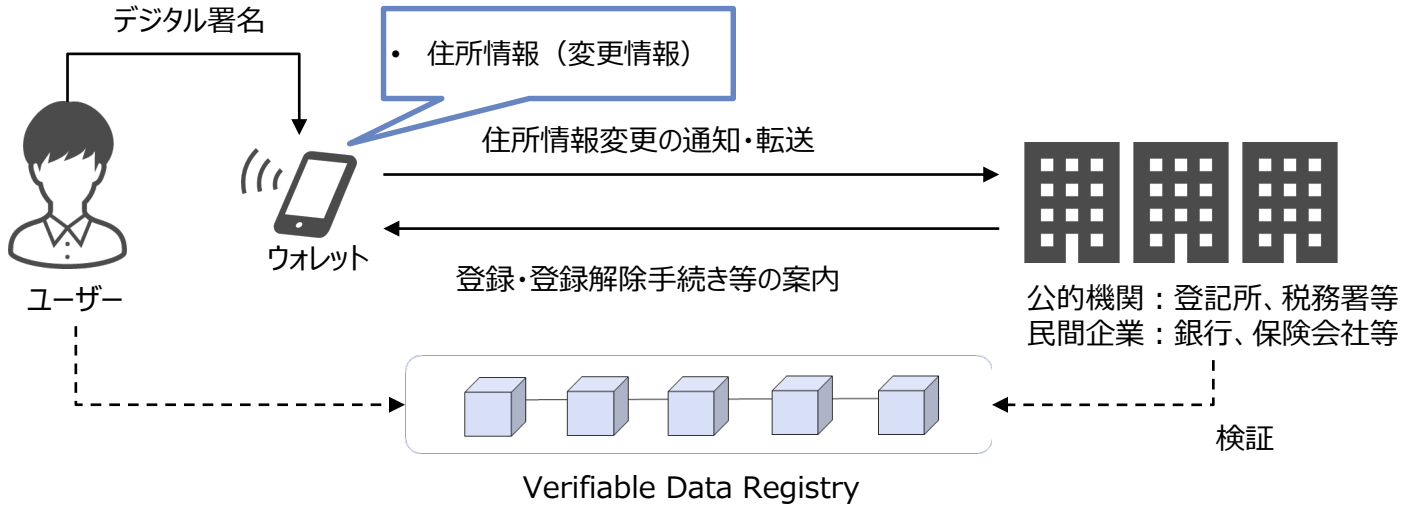
ペインポイント

住所変更のたびに発生する公的機関や企業への住所登録・解除手続きの手間

提供する価値

機関への更新情報の通知、情報の転送

ビジネスモデル



出所） 1 https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Use_Cases/Use_Case_1/Use_Case_1.html

ONCE：運転免許証、自動車登録証等の確認作業への活用

分野：交通・行政
フェーズ：PoC
EU
ドイツ
イギリス

概要

- 運転免許証と車両登録のデジタル化により、警察が運転者の情報を検査する際に要する時間を大幅に短縮可能
- 運転免許証は各免許当局のオンラインポータルで管理でき、運転免許の取り消しや新しい車両の申請は、自宅のデバイスから行うことが可能
- レンタカーやカーシェアリングの利用時の身分証明書の提示・確認作業においても原本の提示を不要にすることで迅速化することが可能[1]

エンティティ

- 費用負担主体：不明
- 価値提供主体：ONCE
- 参加者：各免許当局、サービスプロバイダー

使用されている技術

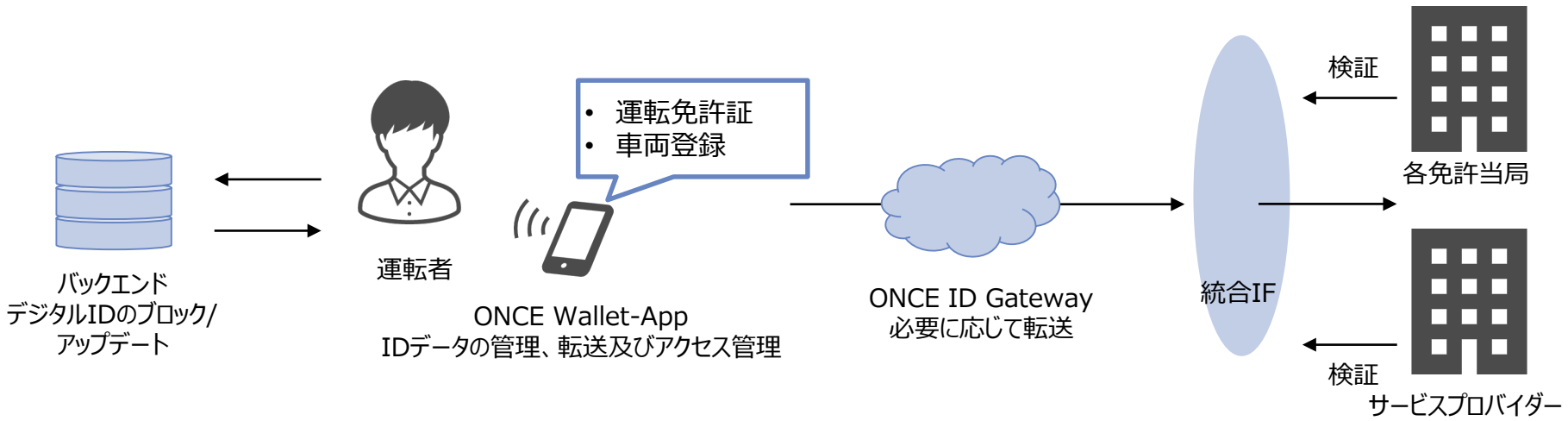
- ONCE Wallet-App、バックエンド、ONCE ID Gateway、統合IF

扱う属性情報

- 運転免許証情報

ペインポイント	提供する価値
警察やプロバイダーによる身分証明書の確認作業	デジタル化による確認時間の短縮
運転者による運転免許証の管理、申請等の手続き	オンラインでの管理による申請手続きの手間の削減

ビジネスモデル



出所） 1 https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Use_Cases/Use_Case_3/Use_Case_3.html

ONCE：公共施設の利用促進に向けた活用

分野：行政
フェーズ：PoC
EU
ドイツ
イギリス

概要

- 博物館、プール、スポーツ施設、文化クラブ、公園、集会所等の公共施設の利用時にデジタルIDを用いることで確認・提示作業を迅速化する
- 現時点で、EU及びEEAの市民向けのeIDカード及びサードパーティーのシステムには、顔写真等の視覚的特徴を提示する機能がなく、今後ONCEの準拠ウォレットに認証された個人写真を実装することが期待されている[1]

エンティティ

- 費用負担主体：不明
- 価値提供主体：ONCE
- 参加者：公共施設

使用されている技術

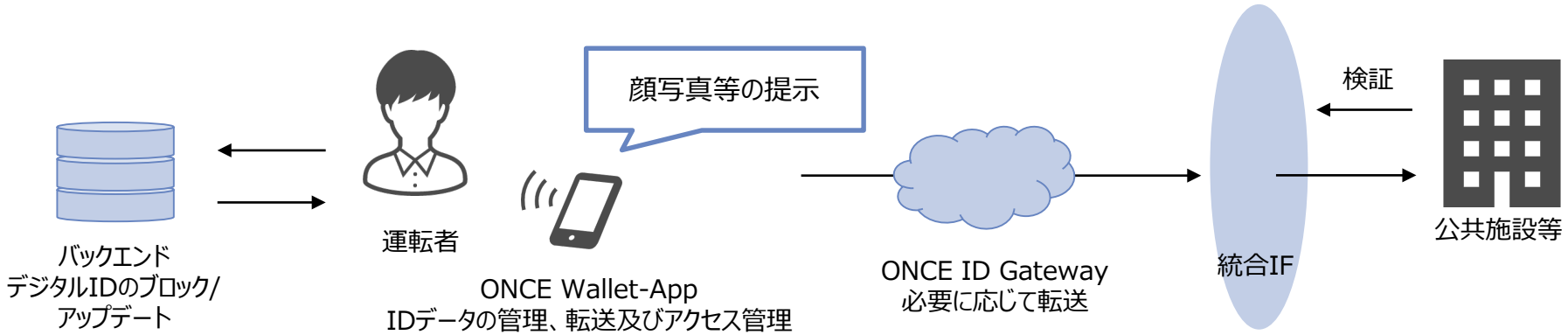
- ONCE Wallet-App、バックエンド、ONCE ID Gateway、統合IF

扱う属性情報

- 顔写真等の視覚情報

ペインポイント	提供する価値
公共施設利用時の確認・提示作業	ユーザー及び施設側の確認・提示作業の削減
顔写真等がないことによる追加の確認作業の発生	顔写真等の掲載による追加で発生する確認作業の抑止

ビジネスモデル



出所） 1 https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Use_Cases/Use_Case_3/Use_Case_3.html

ONCE：地域・自治体の特典サービスの利用促進への活用

分野：行政、旅行

フェーズ：PoC

EU
ドイツ
イギリス

概要

- デジタルスパカードやゲストカードを導入することで、スマートフォンを経由して入場料の無料や割引等の観光サービスを受けることが可能となる
- 従来、ホテルの宿泊客には提供されていなかった特典情報が、配信されるようになることで、宿泊客の満足度向上とともに、観光施設側は売上機会の創出につながる[1]

エンティティ

- 費用負担主体：不明
- 価値提供主体：ONCE
- 参加者：自治体、地域の観光施設、ホテル等

使用されている技術

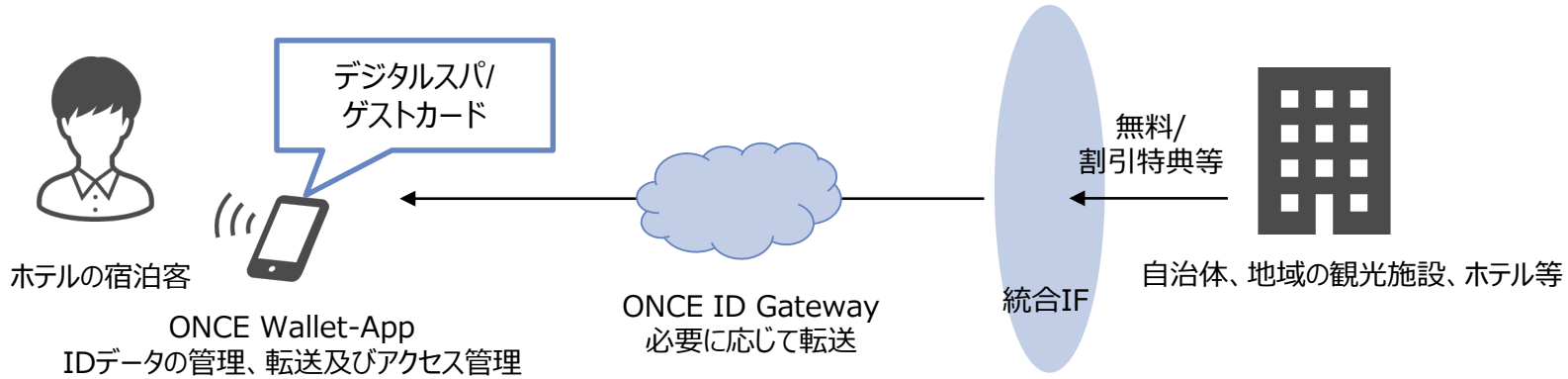
- ONCE Wallet-App、バックエンド、ONCE ID Gateway、統合IF

扱う属性情報

- ホテルや自治体、観光施設などのサービス情報、宿泊客の宿泊情報

ペインポイント	提供する価値
観光客/ツアリストとホテルの宿泊客でのサービス等に係る情報の格差	観光客/ツアリストとホテルの宿泊客への公平な情報配信
ホテル宿泊客にサービスが届かないことによる機械損失	サービスの利用機会、売上獲得機会の増加

ビジネスモデル



出所） 1 https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Use_Cases/Use_Case_3/Use_Case_3.html

SDIKA：安全で迅速な骨髄提供

分野：医療

フェーズ：PoC

EU
ドイツ
イギリス

概要

- ドナーがデジタルIDとしてウォレットに保存した情報を、ドナーの意思の下、必要な情報をドナーデータベースへ転送が可能となる
- これまで医療機関が手入力で登録していたドナー登録の作業が省力化されるとともに、医療機関とドナーで迅速な連携が可能となる[1]

エンティティ

- 費用負担主体：ドナーデータベース管理者（医療機関？）
- 価値提供主体：SDIKA
- 参加者：医療機関、ドナー

使用されている技術

- SDI-X システム

扱う属性情報

- ドナー登録に係る個人情報

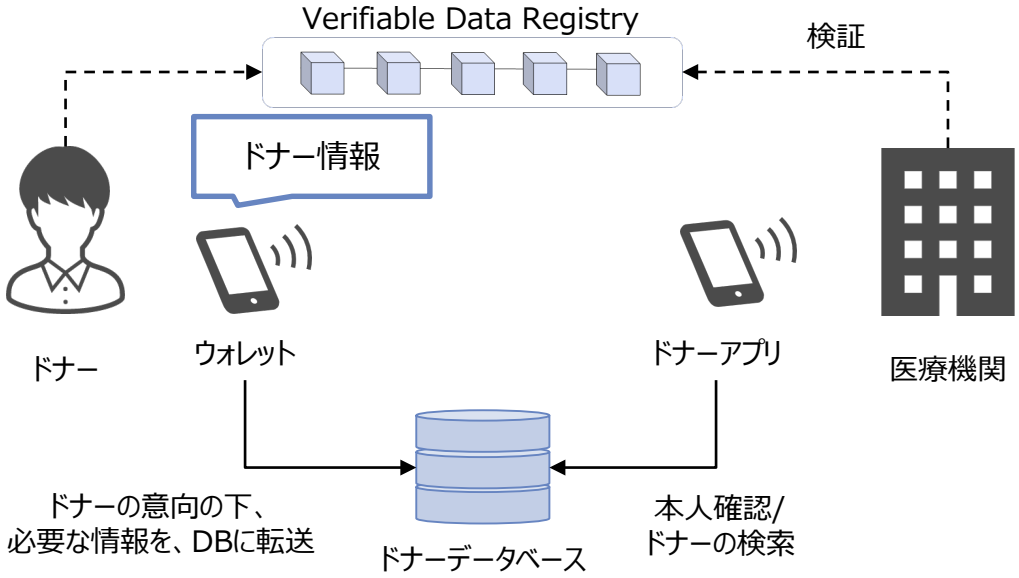
ペインポイント

医療機関等による手入力でのドナー登録作業

提供する価値

医療機関等によるドナー登録作業の省力化（ドナー側による代替）

ビジネスモデル



出所） 1 https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Use_Cases/Use_Case_4/Use_Case_4.html

SDIKA：ビジネスの立ち上げ加速

分野：行政、金融

フェーズ：PoC

EU
ドイツ
イギリス

概要

- 会社（ビジネス）を立ち上げるにあたり、創業期における登記や銀行口座の開設、日々の運営においても都度情報の入力や提示が求められるIDデータを、一か所に集約し何度も使いまわすことを可能にすることで、都度発生する作業を省力化する
- またePAの電子認証とも連携することで、申請者の認証とその後の手続きの迅速化を可能とする[1]

エンティティ

- 費用負担主体：個人/法人データベース管理者
- 価値提供主体：SDIKA
- 参加者：企業や個人事業主、銀行や登記所等

使用されている技術

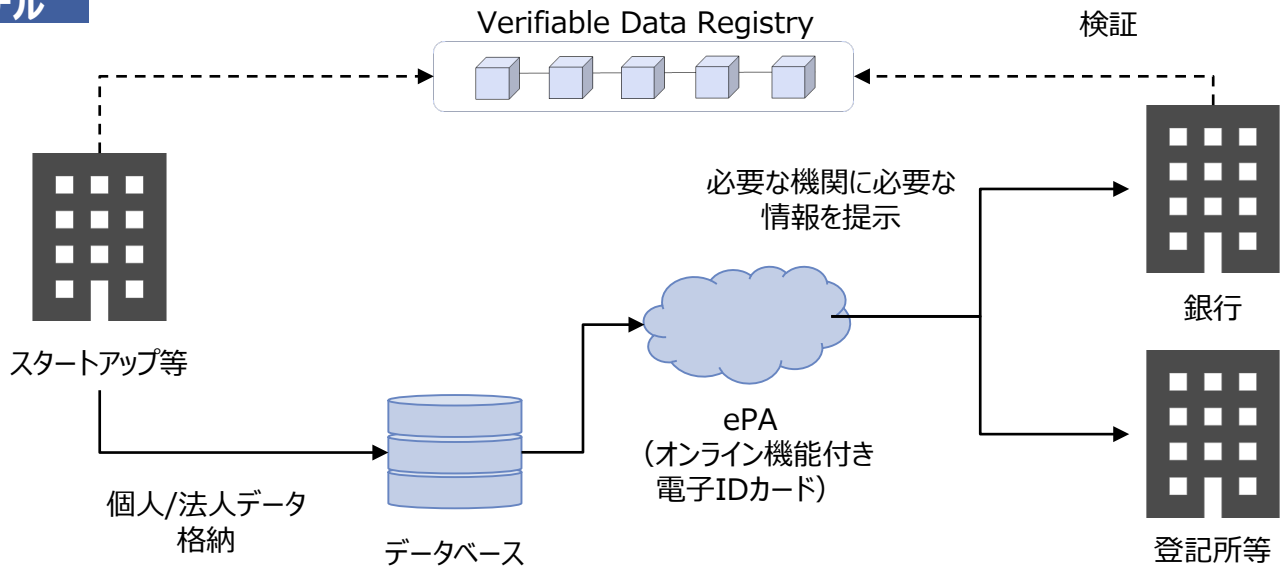
- SDI-X システム

扱う属性情報

- 創業や事業運営に係る個人/法人情報

ペインポイント	提供する価値
創業や事業運営において都度発生する関係機関への申請手続き	データを一元管理し、使いまわすことによる都度発生する作業の省力化
申請後、認証作業によるリードタイムの発生	電子認証システムと連携することによる後続プロセスの迅速化

ビジネスモデル



出所） 1 https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Use_Cases/Use_Case_4/Use_Case_4.html

SDIKA：建築業の申請・許可プロセスの加速化

分野：行政
フェーズ：PoC
EU
ドイツ
イギリス

概要

- 民間企業や行政等、様々なステークホルダーが参画する建築業において、デジタル化により申請・許可の管理プロセスをより適切に記録、追跡可能とすることで、加速化を図るとともに、透明性のある管理手法を実現する[1]

エンティティ

- 費用負担主体：不明
- 価値提供主体：SDIKA
- 参加者：建築士、施工事業者、自治体、行政機関

使用されている技術

- SDI-X システム

扱う属性情報

- 建築申請に係るステークホルダのアイデンティティ情報、役割や権限等

ペインポイント

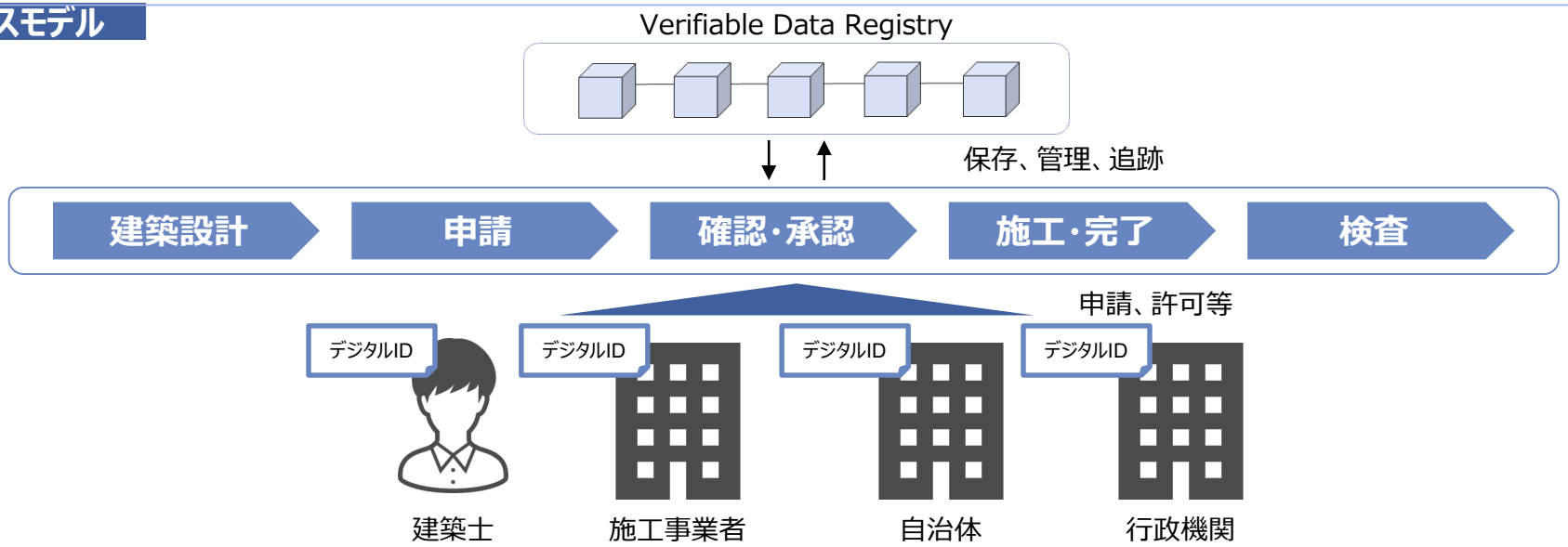
多岐に渡るステークホルダーが跨ることによるプロセス把握の困難

提供する価値

デジタルによるプロセスの見える化

トレーサビリティの向上による透明性の実現

ビジネスモデル



出所） 1 https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Use_Cases/Use_Case_4/Use_Case_4.html

IDunion：教育プログラムにおける記録やその証明の一元管理

分野：教育
フェーズ：PoC
EU
ドイツ
イギリス

概要

- 学士・修士課程、交換留学等の際に必要となるコース記録や成績証明書など、学生生活における様々な記録を、単一のデジタルウォレット保存することで、学生が、必要に応じて大学の管理者に送付することが可能となる
- 提出する大学別の機関に応じて様々な様式（紙、デジタル）で提出する必要があった、コース記録や各種証明書等をデジタルウォレットで保管し、そこから提出することで、データの管理や提出に係る作業を省力化する[1]

エンティティ

- 費用負担主体：不明
- 価値提供主体：IDUnion
- 参加者：学生、大学の管理部門等

使用されている技術

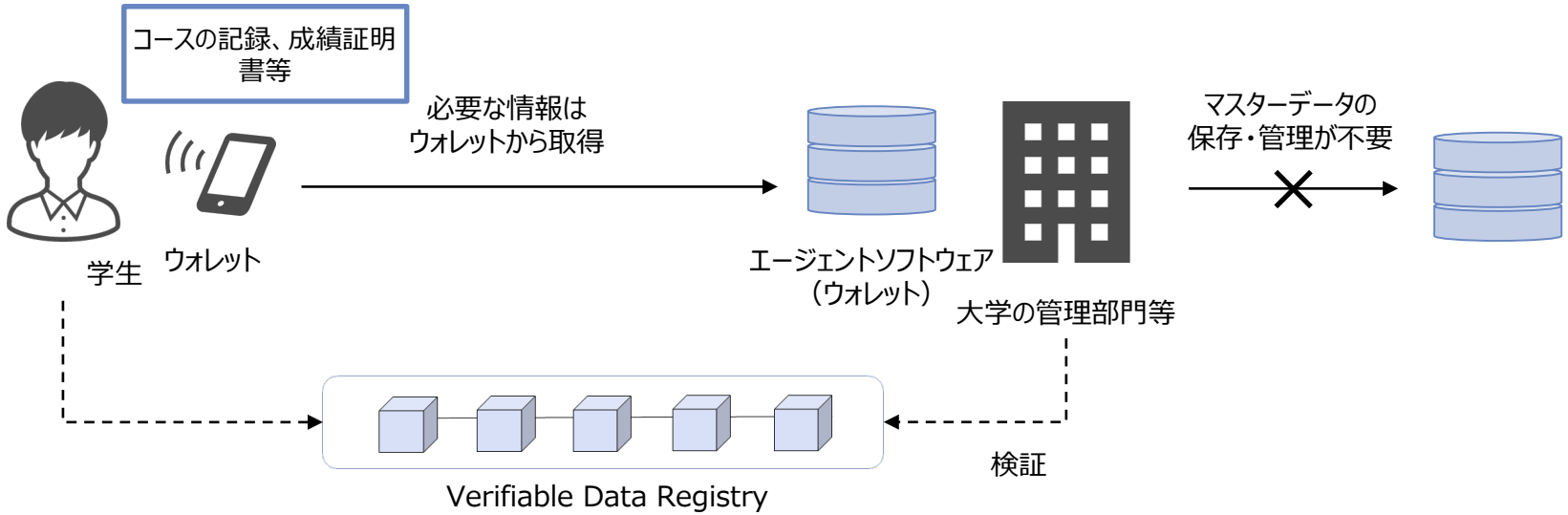
- 不明

扱う属性情報

- コースの記録、成績証明書等

ペインポイント	提供する価値
異なる機関へそれぞれの様式で証明書等の提出に係る手間	ウォレットで保管し、情報を取得可能にすることによる省力化
各機関側でのマスターデータの保存・管理に係る手間	ウォレット上で一元管理することによる省力化

ビジネスモデル



出所） 1 https://www.digitale-technologien.de/DT/Redaktion/EN/Standardartikel/sdi_use_case_2.html

IDunion：2要素認証なしでの安全な支払い

分野：小売

フェーズ：PoC

EU
ドイツ
イギリス

概要

- オンラインでモノを購入する際、注文手続きにおいて発生する個人情報や住所、支払い情報等の入力の手間を削減するためにブラウザやサービスプロバイダー上に保存しているデータをデジタルウォレットに保管することで、自分自身でアイデンティティ情報を管理することが可能となる
- データ保護関連のリスクの解消の他、販売者側は、入力の手間を起因とする注文キャンセルによる機械損失の減少に貢献する[1]

エンティティ

- 費用負担主体：不明
- 価値提供主体：IDUnion
- 参加者：一般消費者、オンラインサイト、サプライヤー/サービサー

使用されている技術

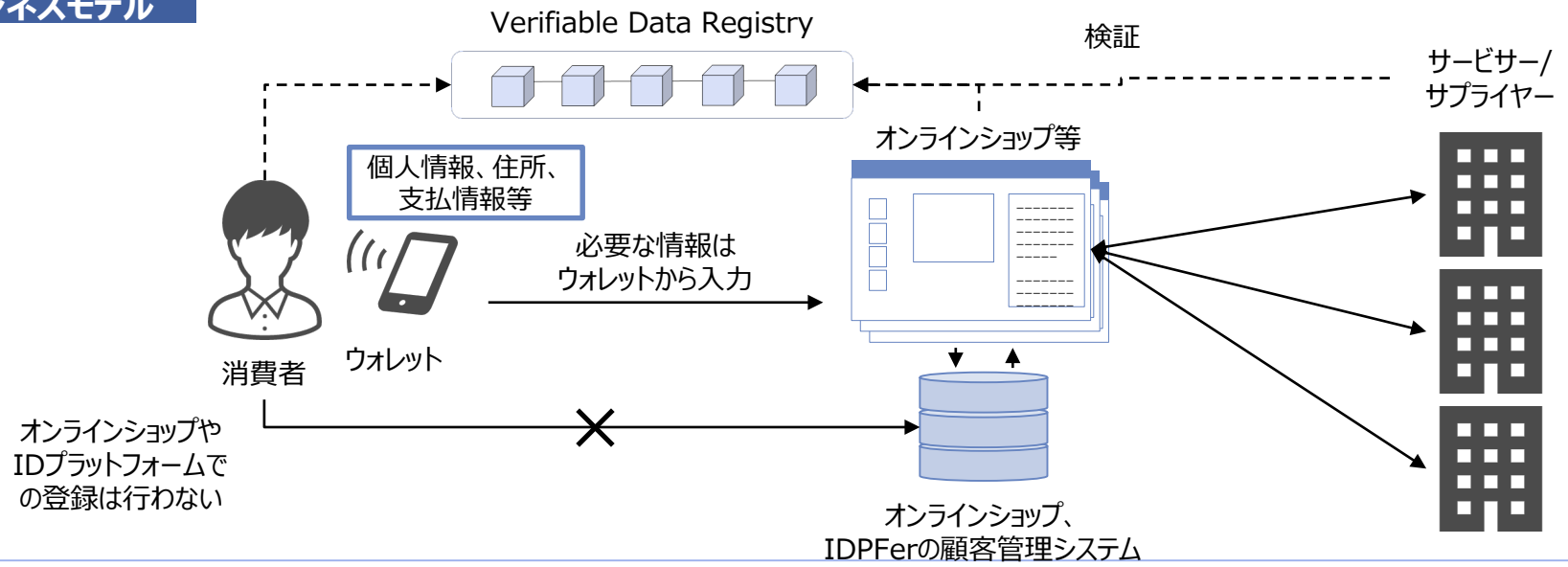
- 不明

扱う属性情報

- 個人情報、住所、支払情報等

ペインポイント	提供する価値
登録や注文手続きにおいて発生する個人情報等の入力に係る手間	都度発生する個人情報等の入力に係る手間の省力化
入力の手間を起因とする注文キャンセルによる機械損失	手続きの省力化による機械損失の削減
オンラインショップやIDPFerに管理させることによる心理的な不安	ウォレットで自分自身で管理することによる心理的安全性の確保

ビジネスモデル



出所） 1 https://www.digitale-technologien.de/DT/Redaktion/EN/Standardartikel/sdi_use_case_2.html

IDunion：サプライチェーンにおける効率的マスター管理データ

分野：サプライチェーン
フェーズ：PoC
EU
ドイツ
イギリス

概要

- 従来、取引等のために、企業のITシステムで主導で保管・管理していた、登記簿の情報や税金、会計データ等を、発行者のビジネスウォレット上に保管可能とすることで、情報の管理・更新に係る手間を省力化し、さらに取引プロセスの透明性を担保とする[1]

エンティティ

- 費用負担主体：不明
- 価値提供主体：IDUnion
- 参加者：企業（発行者）、取引先、公的機関等

使用されている技術

- 不明

扱う属性情報

- 登記簿の情報や税金、会計データ等

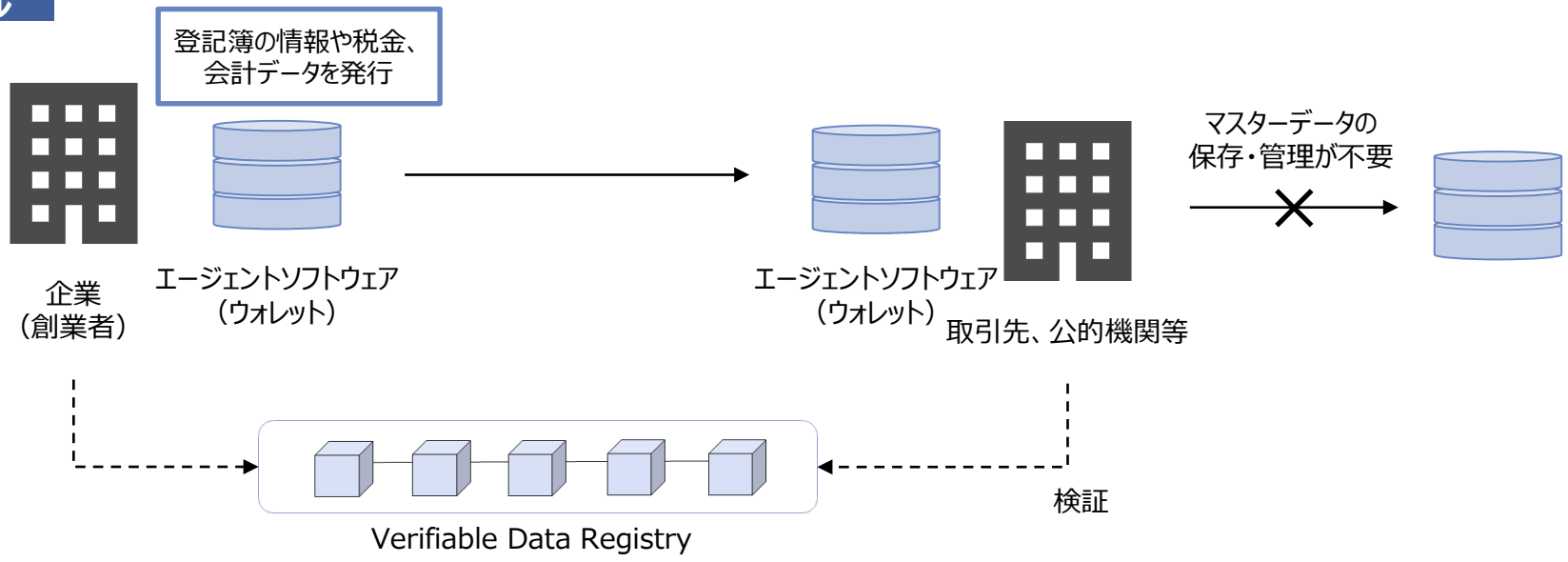
ペインポイント

企業活動における事務系情報等のマスターデータ保管に係る手間

提供する価値

発行者のウォレットに保管することによる提出先におけるデータの管理・更新手続き等の省力化

ビジネスモデル



出所） 1 https://www.digitale-technologien.de/DT/Redaktion/EN/Standardartikel/sdi_use_case_2.html

（補足）Business Partner Agent -Org. Wallet

IDunionの取り組みにおける「サプライチェーンにおける効率的マスター管理データ」は、Bosch I.O Gmbh社(Bosch社のIoT重視の子会社) のBusiness Partner Agentイニシアチブにおける Org. Wallet（組織のウォレット）という名称で情報公開されている[1]

Business Partner Agent

- Business Partner Agentは、Bosch社の研究プロジェクト「Economy of Things（モノの経済）」の中で実施されている、デジタルIDおよび分散型IDの原則に基づいて、企業間のデータ交換の改善を目的とする開発イニシアチブである
- 基本的に開発はオープンソースであり、成果物の機能仕様、ソースコード等はGitHub（https://github.com/hyperledger-labs/business-partner-agent）上で公開されている

Org. Wallet

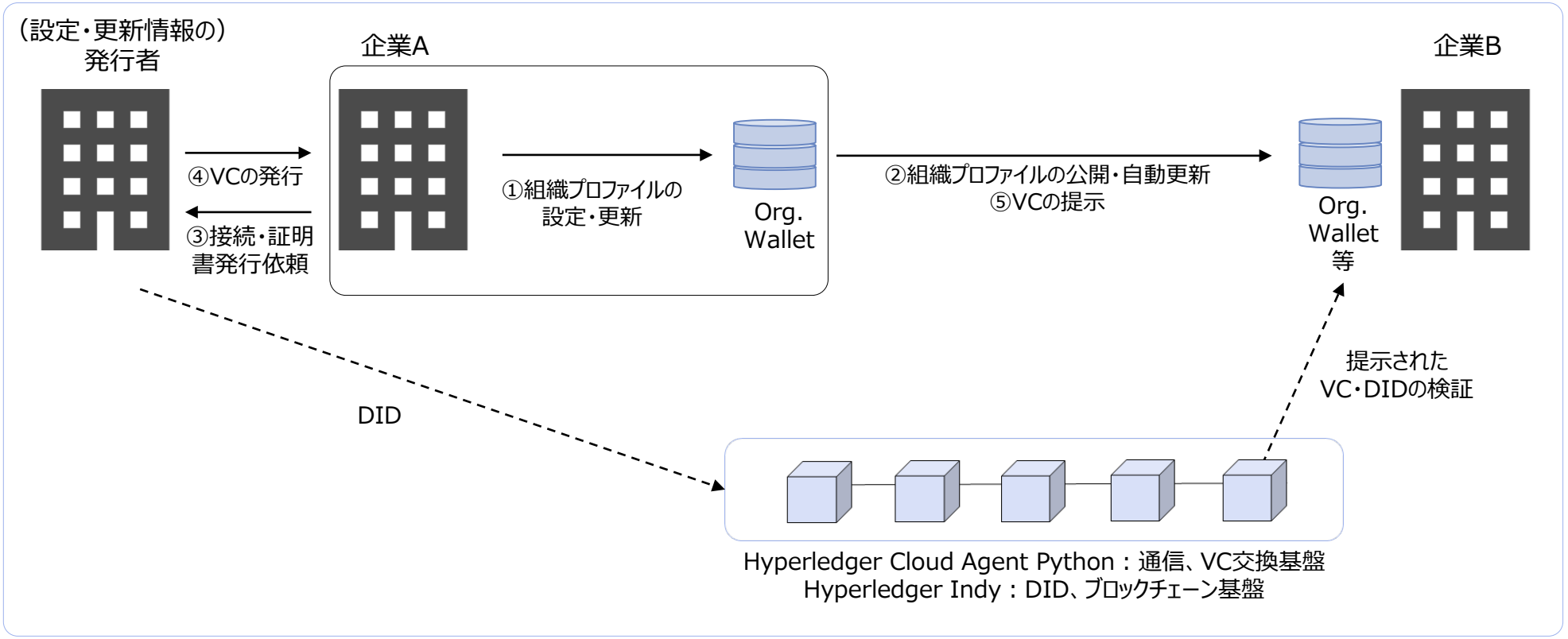
- Organization Walletは、Bosch社の提供する、組織のニーズに焦点を当てた企業向けデジタルウォレットである
- 自社のデータ（IDプロバイダーや信用調査会社による詳細な企業情報、住所、連絡先データ、銀行口座データ、認証機関(ISO、IATF等)発行の証明書等）をビジネスパートナーと交換し、顧客やサプライヤーからの受信データをシームレスに検証するためのツールを提供する

出所）
1 https://orgwallet.de/en/

（補足）Business Partner Agent -Org. Walletの概要

- **Bussiness Partner Agent（Org. Wallet）を使用する企業は、ウォレットアプリケーションを使用して自社のデータ及び証明書を検証可能な形でビジネスパートナーと共有できるようになる[1]**
- **Bussiness Partner Agent（Org. Wallet）の機能は、Hyperledger Indy（ID特化のDID、ブロックチェーン基盤）及びHyperledger Cloud Agent Python（VCのエコシステム基盤）上に構築されており、DID、VCは、W3C標準に準拠し、Hyperledgerに適合させた仕様となっている**

Bussiness Partner Agent（Org. Wallet）のスキーム図



出所）
1 https://orgwallet.de/en/

（補足）Business Partner Agent - Org. Walletの動作要領

EU
ドイツ
イギリス

Bussiness Partner Agent（Org. Wallet）のGithubリポジトリでは、登録～VCの提示までの動作デモ動画が公開されており、概ね以下のような順序で操作されることが確認できる[1, 2]

Bussiness Partner Agent（Org. Wallet）の動作要領

自社の登録	• パブリックDIDを発行し、組織プロファイル（企業名、住所、連絡先等）を登録 • この時点で組織のプロファイルはドキュメントとしてウォレットに格納される
ビジネスパートナーの追加	• 情報のやり取りをしたい企業等のパブリックDID、もしくはインビテーションを利用して、ビジネスパートナーを追加する　※ビジネスパートナーは、情報のやり取りをする相手の他、情報の検証を要求する相手も含まれる（銀行口座情報の検証を依頼する銀行など）
VCの格納	• （外部の認証を要する企業情報のやり取りをする場合）Issuerから発行された証明書などのドキュメントをウォレットに格納する 例）銀行口座情報のVCを銀行に依頼し、口座情報のVCを作成・追加
情報の送受信	• ビジネスパートナーを選択し、プレゼンテーション要求・応答に基づくVCの提示を行うことで、検証可能な情報のやり取りを行う • プレゼンテーション要求・応答はゼロ知識証明による選択的開示をサポートしているほか、ビジネスパートナーとのチャット機能も有する

出所）
1 https://labs.hyperledger.org/business-partner-agent/index.html
2 https://github.com/hyperledger-labs/business-partner-agent

ユースケース：my EGO

分野：保険
フェーズ：コンセプト

EU
ドイツ
イギリス

概要

- ドイツのデジタルID・SSIサービス提供企業であるmy EGOは、ブロックチェーンをベースとしたIDウォレット、Issuer、Verifier向けの発行・検証ゲートウェイなどを提供している[1]
- my EGOは、自動車関連データと自動車オーナーIDの紐づけによる、パーソナライズされた自動車保険の提供に自社サービスが活用できるとして、ユースケースの検討を行っている

エンティティ

- 費用負担主体：不明
- 価値提供主体：my EGO社
- 参加者：自動車オーナー、自動車関連企業、自動車保険企業

使用されている技術

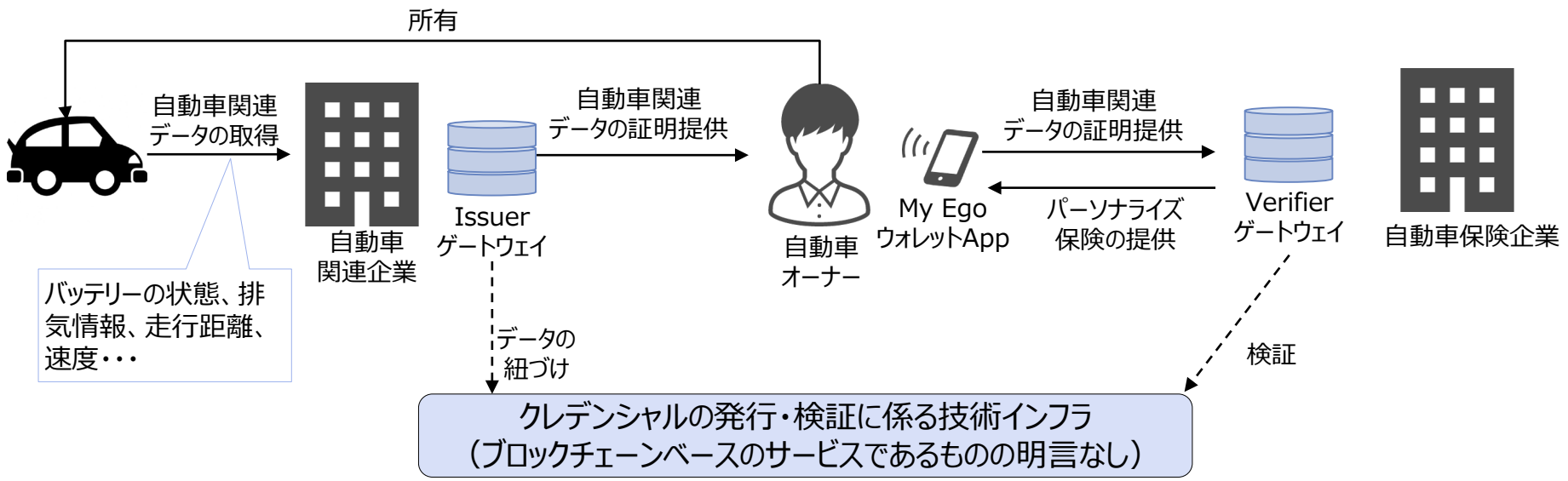
- W3C VCs、ブロックチェーン

扱う属性情報

- 自動車関連データ（走行距離等）、自動車保険申請に係る個人情報

ペインポイント	提供する価値
自動車保険の申請の煩雑さ	申請に係る情報をmyEGOで管理することで申請プロセスを簡略化
自動車関連データの主権が不明瞭	自己の権限でデータ管理を行うことができ、データの悪用を防止できる

ビジネスモデル

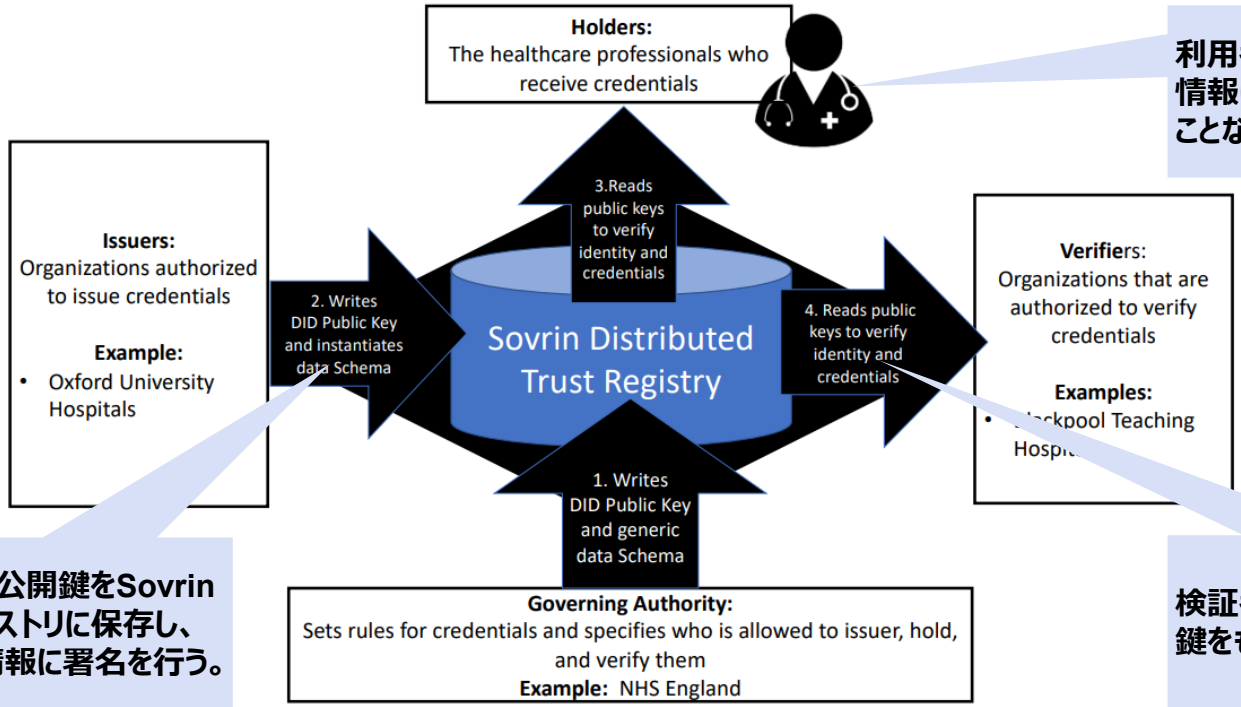


出所）
1 https://myego.io/usecase-automotive-mobility/

NHS Digital Staff passport

イギリスのNHS（国民保健サービス）は医療スタッフの異動等に伴う身分証明プロセスの効率化のため、W3C VCs/DIDsに準拠した医療従事者の証明書情報交換サービスであるNHS Digital Staff Passportを2020年から展開しており[1]、レジストリとしてHyperledger Indyをベースとしたsovrin Networkを使用しウォレットはEvernym社から提供を受けている[2]

NHS Digital Staff PassportにおけるSovrin Networkの活用



利用者（医療従事者）の個人情報はブロックチェーンに保存することなく、P2Pで通信を行う

参加する病院は公開鍵をSovrin Networkのレジストリに保存し、秘密鍵で証明情報に署名を行う。

検証者は分散型台帳上の公開鍵をもってID情報の検証を行う

出所）
1 https://transform.england.nhs.uk/information-governance/guidance/digital-staff-passport/
2 https://cpb-us-e1.wpmucdn.com/wordpressua.uark.edu/dist/5/444/files/2018/01/BCoE2022SS1FINAL.pdf

EU
ドイツ
イギリス

FCAによる規制サンドボックスの実施

FCA（金融サービス庁）は新たな技術やビジネスモデルを促進するために、企業が市場で実証を行う事のできる規制サンドボックス（Regulatory Sandbox）を実施しており[1]、規制サンドボックスの中でデジタルIDに関する実証が行われ、分散型アイデンティティ、SSIに関連した事例も含まれている[2]

規制サンドボックスにおける分散型アイデンティティ、SSIに関連した実証

参加企業等

- Fintech Delivery Panel　Partners※が申請主体となり、Deloitte、Evernym、Onfido等がメンバーとして参加した
- 2019年の規制サンドボックス第5コホートで申請が認められ実施された

取り組み概要

- 金融機関のKYCプロセスにおいて、消費者が分散型IDとVCを用いて身元の証明を行い口座を開設する実証を行い、規制要件への適合をテストした
- Evernymの提供する自己主権型のデジタルIDウォレット及びVCの発行プラットフォームとOnfidoのID検証SDKを用いて、金融機関の顧客オンボーディング、口座開設の効率化を図った

※イギリスにおけるフィンテックの推進を目的とした、金融機関、テック企業、規制当局、シンクタンク等の共同イニシアチブ

出所）
1　https://www.fca.org.uk/firms/innovation/regulatory-sandbox
2　https://www.evernym.com/onfido-deloitte/

ユースケース：映画館における「年齢証明」の簡易化

分野：エンタメ
フェーズ：実運用
EU
ドイツ
イギリス

概要

- 2022年5月、英国映画協会（UK Cinema Association）がDigital Identity and Attributes Trust Frameworkにおける認定アイデンティティサービスプロバイダー(IDSP)であるYotiとパートナーシップを締結し、Yotiアプリを使用して映画館における年齢を証明できるようにした
- イギリスの映画館利用者の約20%が9-14歳、約30%が15-24歳に属している一方、パスポートや運転免許証なしで年齢を証明することが非常に困難であるという課題解決を目指すもの[1，2]

エンティティ

- 費用負担主体：英国映画協会
- 価値提供主体：Yoti
- 参加者：映画館ユーザー

使用されている技術

- AES-256暗号、フェイスキャプチャ

扱う属性情報

- 年齢証明情報

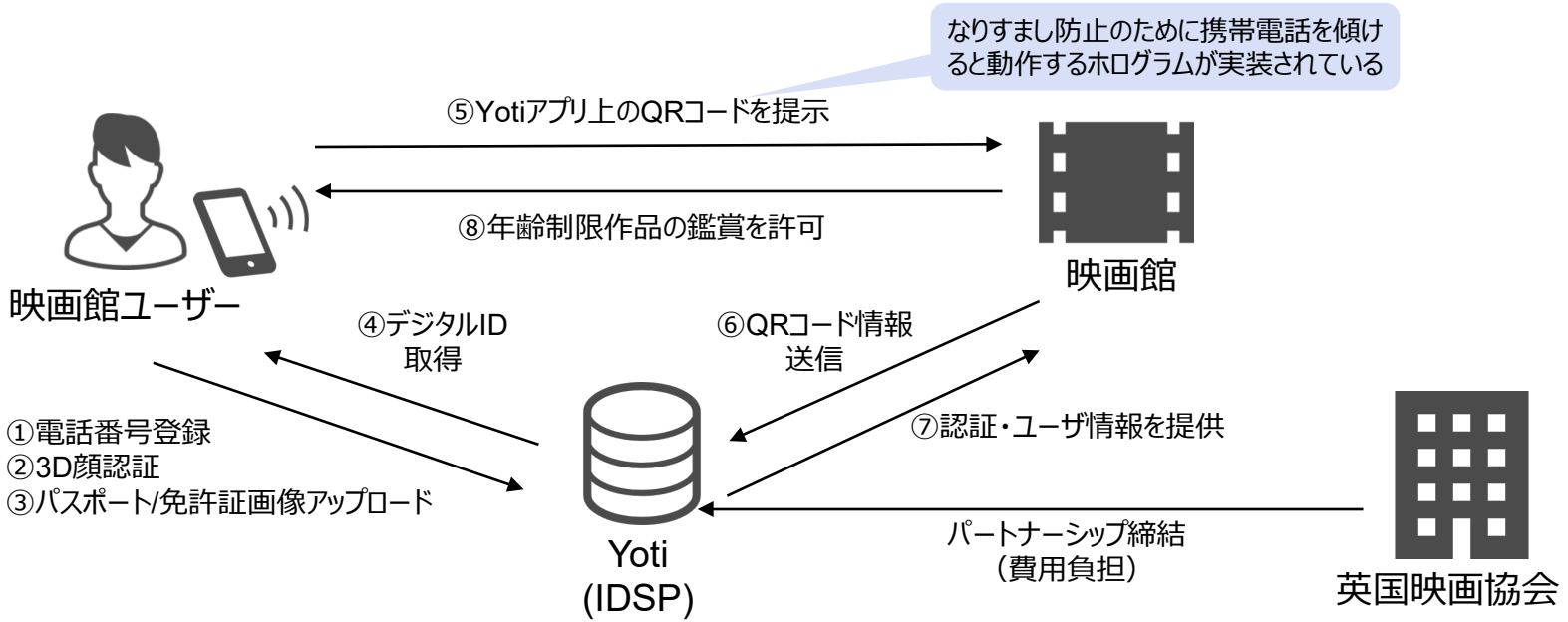
ペインポイント

年齢証明手段がパスポートや運転免許証しかない

提供する価値

モバイルアプリ導入による選択肢の増加

ビジネスモデル



出所）1 https://www.techuk.org/resource/uk-cinema-association-partners-with-digital-identity-provider-yoti-to-ease-proof-of-age-challenges-at-cinemas.html
2 https://www.cinemauk.org.uk/wp-content/uploads/2022/05/Yoti-Digital-ID-Scheme-Press-Release1.pdf

ユースケース：英国金融サービス向けのデジタルIDスキームの構築

分野：金融
フェーズ：PoC
EU
ドイツ
イギリス

概要

- イギリスの金融サービスにおける業界団体であるTISA（The Investing and Saving Alliance's）は、英国の金融サービスのデジタル化を推進するためのゲートウェイとして、デジタルIDスキームの開発・検証を実施しており、金融サービスプロバイダーが様々な認定IDプロバイダーからKYCのためにデジタルIDを活用できるようにすることを目指している[1]
- 2021年9月、金融サービスプロバイダー(Fidelity、MoneyHub、Profile Pensionなど)とIDプロバイダー(Post office、Yoti、Digidentity、OBidなど)とのPoCフェーズを完了した

エンティティ

- 費用負担主体： Innovate UK
- 価値提供主体：TISA、金融サービスプロバイダー、IdP

使用されている技術

- 不明

扱う属性情報

- 不明（金融サービスでのKYC属性情報）

ペインポイント

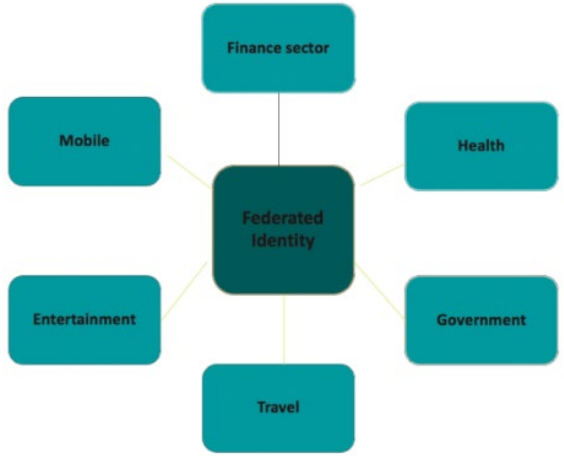
消費者の金融商品へのアクセス複雑性

提供する価値

シンプルかつ安全なアクセス手段の提供・コスト削減・効率化

ビジネスモデル

将来のデジタルアイデンティティの活用イメージ



- Innovate UK(ビジネス、エネルギー、産業戦略省が後援する部門外の執行機関)は、デジタルアイデンティティプロジェクトの研究段階を支援するための助成金をTISAに授与
- 同助成金は、金融サービスプロバイダーとIDプロバイダー間の安全なデジタルIDの使用と再利用をテストするPoCに活用され、主に以下のユースケースがテストされた
  - 当座貸越付き銀行口座の開設
  - ISA（ndividual Savings Account ：個人貯蓄口座）の申し込み
  - 年金の開設
- 将来的には、テクノロジー及び規格の相互運用性が担保された様々な分野において作成されたデジタルIDを活用することを目指している

出所）
1 https://www.tisa.uk.com/tisa-groups-projects/digital-id/

ユースケース：不動産に係るデジタルアイデンティティ活用

分野：不動産
フェーズ：実運用
EU
ドイツ
イギリス

概要

- イギリスIT企業のEtiveは、政府の技術支援施策であるInnovative UKの助成金を受け不動産取引に係るデジタルアイデンティティスキームを策定した
- スキームではEtiveの提供する、不動産に関する販売履歴、保険、エネルギー性能、メンテナンス状況などの情報管理や身元証明で不動産取引をサポートするプロパティログブック（PLB）を活用し、迅速な不動産取引を可能にするとしている[1，2]

エンティティ

- 費用負担主体： Innovate UK
- 価値提供主体：Etive
- 参加者：不動産の売買者、物件エージェント、銀行、英国土地登記

使用されている技術

- 不明

扱う属性情報

- 不動産に関する情報及び売買者の身元証明情報

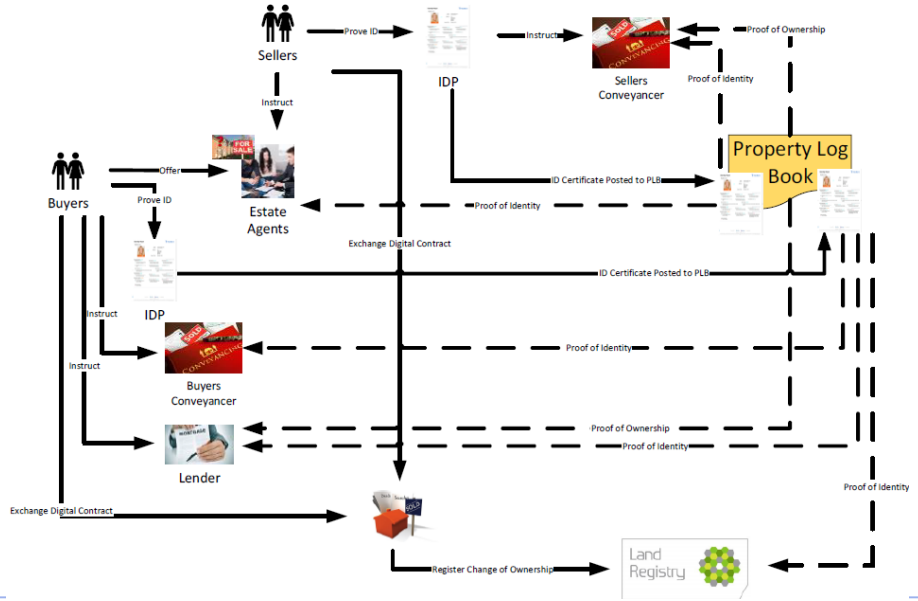
ペインポイント

不動産取引プロセスにおける時間の増加

提供する価値

デジタルID及びPLBによる各種情報確認の迅速化

ビジネスモデル



- 住宅売買における買い手（buyer）と売り手（seller）が不動産エージェントの仲介で売買プロセスを行う
- 売買プロセスの中で、IDプロバイダー経由で売り手、買い手双方の身元証明を行い、その結果をPLBに登録する
- 以降のローン手続きや不動産不動産登記の専門家（conveyancer）との契約手続きの際にはPLBに記録されたデータを基に照会する
- IDプロバイダはイギリスのIDサービスの標準であるGPG45に準拠している（eIDASにも準拠）

出所）
1 https://etive.org/wp-content/uploads/2021/01/A-Digital-Identity-Trust-Framework-and-Home-Buying-Selling__Public.pdf
2 https://etive.org/about/

ユースケース：医療従事者のオンボーディングトレーニングの効率化

分野：医療

フェーズ：PoC

EU
ドイツ
イギリス

概要

- 医療従事者が所有し、管理する分散型デジタルスタッフパスポート(DSP)を使用して、あるNHSトラスト*から別のNHSトラストへの簡単なデータ交換を可能にする
- 従来、医療従事者が英国内のNHSトラスト間で転勤する度に身分証明書や医療証明書を確認し、オンボーディングプロセスに最大7日間も要していたが、DSPを用いたソリューションを活用することでNHS組織間の職員の移動、医療行為の実施に係るプロセスが簡素化されるとしている[1]

*イングランドとウェールズの国民保健サービスにおける組織単位

エンティティ

- 費用負担主体（想定）：医療機関
- 価値提供主体：IdP（Evernym）
- 参加者：NHSトラストの医療従事者

使用されている技術

- ブロックチェーン、W3C VCs/DIDs

扱う属性情報

- 身元証明情報、医療関連資格、トレーニング記録

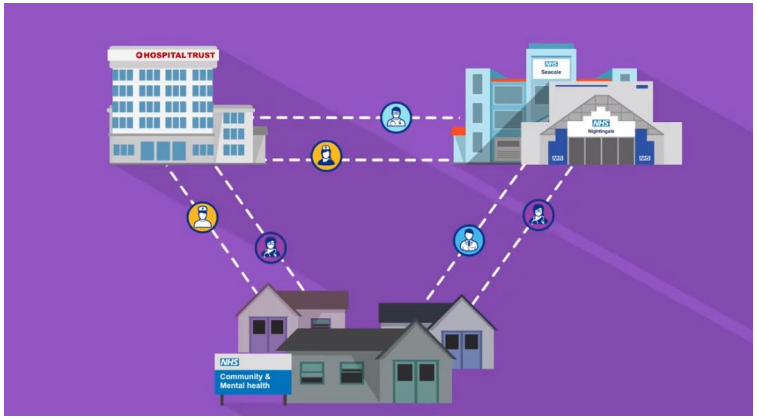
ペインポイント

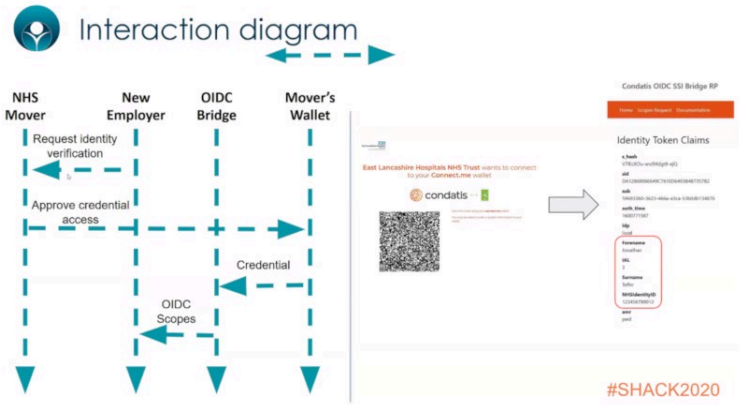
医療従事者の転勤におけるオンボーディングプロセスに時間を要する

提供する価値

デジタルID、検証可能な資格情報によるプロセスの迅速化

ビジネスモデル





- DSPは分散型技術に基づいて構築されており、医療従事者はEvernymのデジタルウォレットである Connect.Meを使用してモバイルデバイスにデジタルIDを暗号的に保持、各部門は身元、資格、トレーニング記録を証明する検証可能な資格情報を発行可能になる
- W3C標準ベースのアーキテクチャを採用しており、またSitekitやCondatisの検証アプリをConnect.MeとNHSの人事システムを統合しており、人事プロセスの大幅効率化を可能としている

出所）

1 https://www.evernym.com/blog/two-days-11-hacks-a-recap-of-the-nhs-staff-access-hackathon/

ユースケース：患者の「痛み」管理の効率化

分野：医療
フェーズ：PoC
EU
ドイツ
イギリス

概要

- 英国のディープテック企業であるMvine Ltd. の疼痛管理システム「MSERV」により、患者の感じる痛みをスコアリングし、効率的な患者の治療を行う試みが実施されている
- 患者は自身の感じる「痛み」を国際的に認知された標準的なアンケートであるQuality of Recovery-15に基づきスコアリングし、同システム通じてスコアが看護師を介さずに直接ペインチームに共有することで、従来よりも正確かつ迅速な治療を行うことが可能となる
- Barts Heart Centrerで、心臓手術後の回復強化(ERACS：Enhanced Recovery after Cardiac Surgery)イニシアチブの一環として試験されている[1]

エンティティ

- 費用負担主体（想定）：NHSイングランド病院
- 価値提供主体：Mvine Ltd.
- 参加者：患者、医療従事者

使用されている技術

- 不明

扱う属性情報

- 患者の感じる痛みのスコア

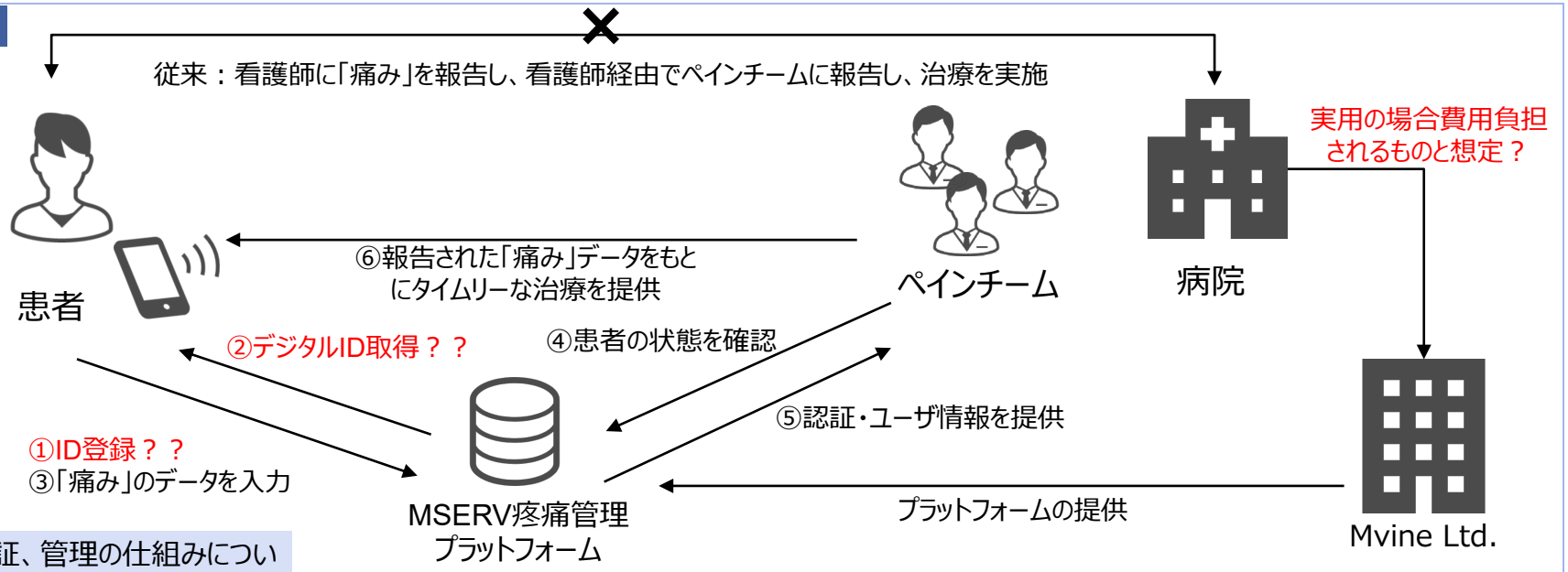
ペインポイント

患者が痛みを訴えてから処置までのタイムラグ

提供する価値

患者の痛みスコアデータ確認による処置の正確・迅速化

ビジネスモデル



※患者のデータの認証、管理の仕組みについての詳細は確認できなかった

出所） 1 https://www.techuk.org/resource/digital-identity-in-healthtech-use-case-for-mserv-pain-management-platform.html

3.3 詳細調査結果：自己主権型／分散型アイデンティティに関する取り組み

3.3.2 北米（米国、カナダ）における調査結果

社会保障番号の代替識別子の検討

米国では社会保障番号の漏洩事件などを通じて、代替的なIDを模索する動きは継続されており分散型IDを検討する動きも政府機関にはみられる

過去発生した社会保障番号の漏洩事件

内国歳入庁（IRS）への不正アクセス事件（2015年）

- サイバー攻撃により流出した社会保障番号を用いて、何者かがIRSの公開システムにおいて確定申告を行い、１万３千人分の税還付が詐取された

エキファックス社の情報漏洩事件（2017年）

- 米国３大消費者信用調査会社の１社であるエキファックス社がハッキングを受け、社会保障番号を含む大量の個人情報が流出し、1億4,300万人への影響があるものとみられている[1]
- 事件を受け、当時のトランプ政権は**社会保障番号の代わりとなる個人識別手段を検討**するように指示した[2]

社会保障番号の代替識別子の検討

- 2020年に米国のDHS（国土安全保障省）は、社会保障番号の収集と利用を減少させるため、カナダに本拠地を置くSecure Key Technologies社に193,000ドルを資金提供し、**社会保障番号の代替識別子を実装**する開発プログラムを実施した

- プログラムは、DHSのシリコンバレーイノベーションプログラム（SVIP）の下で実施され、SVIPのディレクターは「**分散型識別子（DID）などのW3C標準に基づくシステムを実装し**、個人を特定できる情報を明らかにせず、追跡目的で使用できない、グローバルに一意で無意味であるが解決可能で検証可能な識別子の発行を可能にする」と述べている[3]

出所）1 https://wired.jp/2017/09/26/massive-equifax-breach/
2 https://www.bloomberg.co.jp/news/articles/2017-10-04/OX9ZNO6K50XS01
3 https://www.dhs.gov/science-and-technology/news/2020/10/09/news-release-dhs-awards-alternative-identifier-social-security-number

米国各州におけるmDLの導入

米国ではルイジアナ州、コロラド州、アリゾナ州、カリフォルニア州など複数州でISO/IEC18013-5に基づくモバイル運転免許証（mDL）の導入及びテストを展開しており、個人のモバイルデバイスに保存された検証可能なデジタル運転免許証を、改ざん困難な形で必要な情報のみの提示を可能にするとしている[1]

ISO/IEC18013-5

- 2021年に成立したISO規格の国際標準であり、モバイル端末に格納されるモバイル運転免許証（mDL）を実装するためのインターフェース仕様を規定しており、mDLの発行元以外の者（他国の運転免許証発行機関、公共・民間サービスでの運転免許証による身元確認者等）がmDLの検証を可能とすることを目的としている[2]
- mDLによって、個人は物理的なIDを携行することなく、自身のデバイスで運転免許証を管理することができ、トランザクションに必要な属性情報のみを提示することが可能になる[3]

米国におけるmDLの導入

- ルイジアナ州、コロラド州、アリゾナ州は早期からmDLの導入に取り組んでおり、カリフォルニア州、ユタ州などが近年テストに着手している
- 米国運輸保安局（TSA）は、Apple社のウォレットアプリケーションをもってmDLのサポートを開始しており、アリゾナ州ではmDLを空港の保安検査で提示することが可能である

出所）
1 https://www.govtech.com/fs/california-moves-to-test-new-digital-drivers-licenses
2 https://www.soumu.go.jp/main_content/000779585.pdf
3 https://www.idemia.com/press-release/idemia-enables-acceptance-state-ids-and-drivers-licenses-apple-wallet-tsa-airport-checkpoints-2022-03-24#:~:text=The%20TSA%20will%20be%20the,Face%20ID%20or%20Touch%20ID

イリノイ州とEvernymの提携

イリノイ州政府は、自己主権型IDソリューションのプロバイダーであるEvernym社と提携し、分散型台帳技術を活用して、出生登録プロセスにおいてイリノイ州市民の自己主権型IDを作成する試みを2017年に発表した[1、2]

取り組みの概要

- イリノイ州政府は、2017年に自己主権型IDソリューションのプロバイダーであるEvernym社との提携を発表し、分散型台帳技術を活用して、イリノイ州市民の為の安全なデジタルIDソリューションを提供することを明らかにした
- 提案されているコンセプトでは、出生登録プロセスにおいてイリノイ州市民の自己主権型IDを作成するため、政府機関が法的氏名、生年月日、性別、血液型などの出生登録情報に暗号署名し、検証可能なクレームを作成するとしている
- 作成されたクレームは分散型台帳に分散型識別子という形で保存・暗号化され、その閲覧・共有は、ID 所有者または新生児の場合はその法的保護者の明示的な同意により許可され、企業や政府がイリノイ州市民を認証する際に使用できる

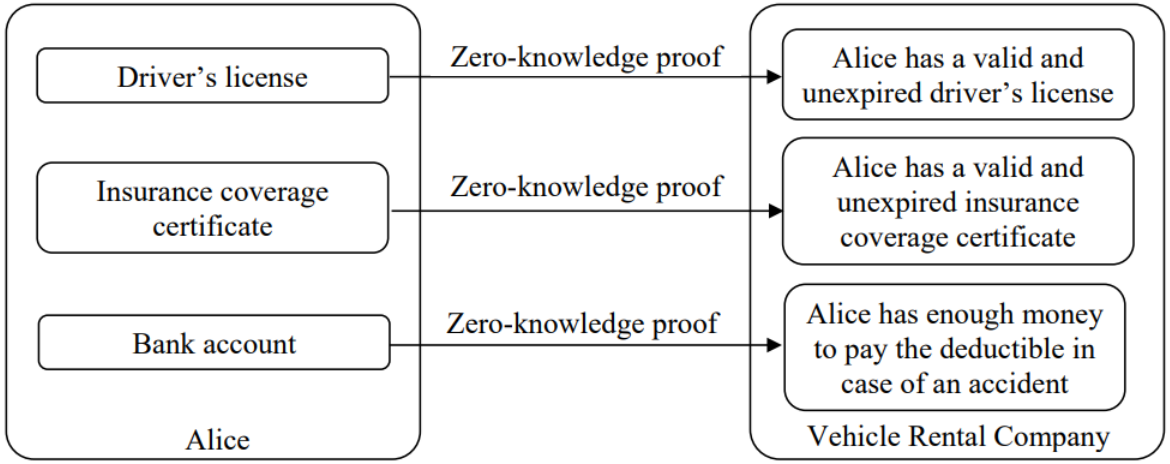
出所）
1 https://www2.illinois.gov/IISNews/14759-DCEO_Birth_Registration_Pilot_Release.pdf
2 https://www.govtech.com/data/illinois-announces-key-partnership-in-birth-registry-blockchain-pilot.html

米国
カナダ

NISTによるブロックチェーンID管理システムの検討

NISTは2020年1月14日にブロックチェーンベースのID管理システム(IDMS)に関するホワイトペーパーを公開した。NISTは従来の ID システムは通常、単一障害点の形成、相互運用性の欠如および大量のデータ収集やユーザー追跡の有効化などのプライバシーの問題があるが、ブロックチェーン技術には、これらの懸念を軽減する可能性があるとして、ブロックチェーンベースIDMSのアーキテクチャの分類アプローチ、想定されるユースケースなどを記載している[1]

NISTのホワイトペーパーに記載されたユースケースの例



ユースケース例：車のレンタルにおける最小情報開示

有効な運転免許証、保険証書、銀行口座情報などをウォレットアプリとオンチェーンストレージに格納し、それらを組み合わせて必要な最小情報（免許証・保険証書の保持、有効期限等）として自動車レンタル会社に提示することを想定している

より一般的には、MOBI（後述）などのブロックチェーンイニシアチブの推進するシステムの中に含まれる、料金支払いや駐車サービスなど、自動車産業のあらゆるエンティティが含まれるとしている

出所）
1 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01142020.pdf

ユースケース：MOBI

分野：交通

フェーズ：PoC

米国
カナダ

概要

- MOBIは米国に本拠地を置く、自動車産業におけるブロックチェーン技術等の利用・標準化を推進するコンソーシアムである
- 車両に固有のIDであるVIDとビークルウォレットを付与し、オーナーや製造元などのウォレットと連携させることにより、V2Xサービスへの利用や、CO2排気量、バッテリーに関するデータの連携を促進する取り組みを行っている[1]

エンティティ

- 費用負担主体：不明
- 価値提供主体：MOBI
- 参加者：ユーザー、政府機関、自動車メーカー、V2Xサービス提供企業

使用されている技術

- W3C VCs/DIDs、ブロックチェーン

扱う属性情報

- 車両登録証明、整備履歴証明、保険加入状況等

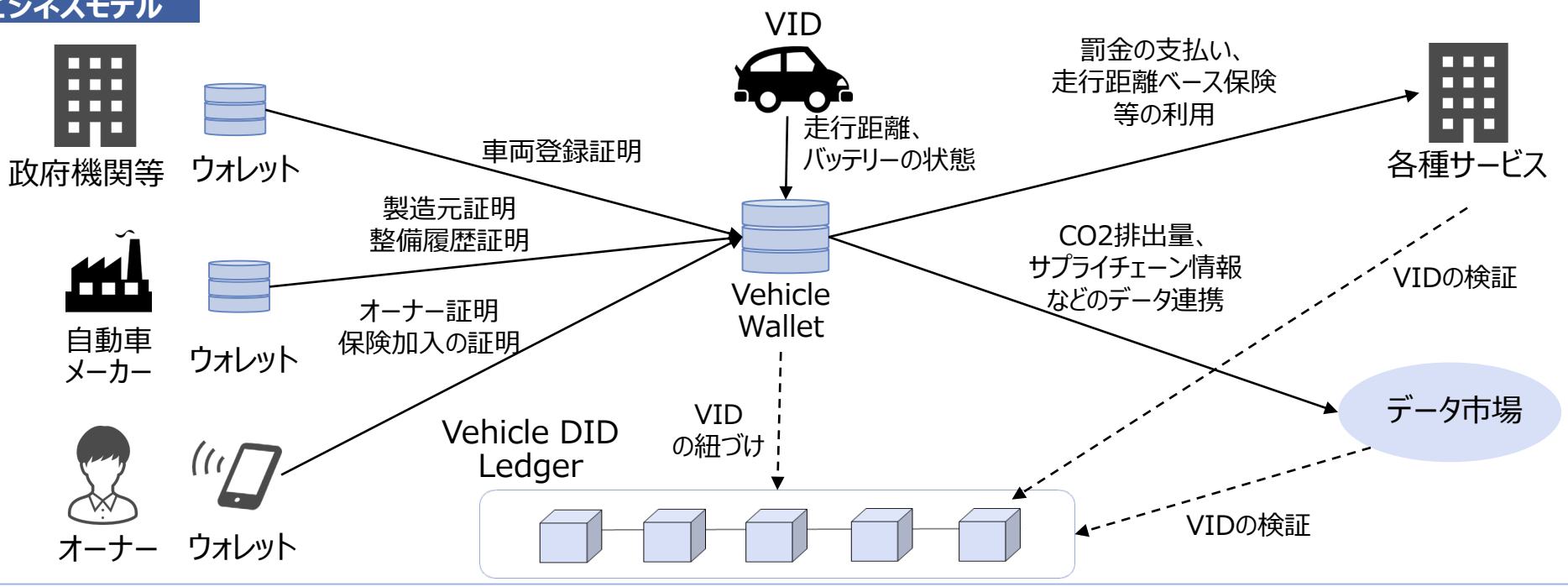
ペインポイント

車両に関するデータが分散管理されており、収集作業が煩雑

提供する価値

車両データをビークルをウォレットで管理し情報収集作業を簡素化

ビジネスモデル



出所）
1 https://dlt.mobi/

米国
カナダ

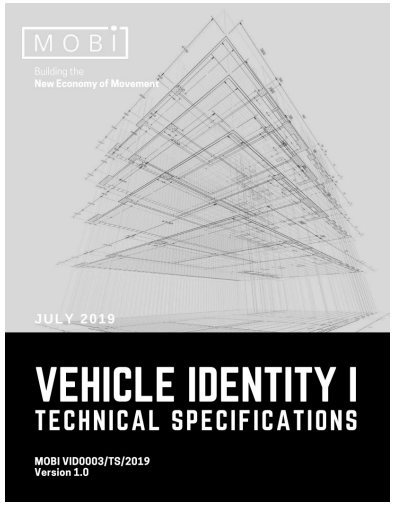
（補足）MOBIの国際標準規格準拠状況

MOBI（Mobility Open Blockchain Initiative）における車両に付与される固有IDであるVID標準にはバージョンⅠ、Ⅱが存在し、W3C VCs／DIDsへの言及が見られる[1]

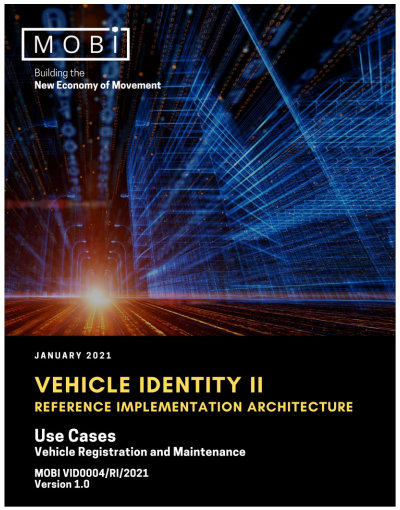
VIDのバージョンについて

- MOBIの公表しているVID標準には、2019年に公表されたVIDⅠと、2021年に公表されたVIDⅡが現状存在し、VIDⅠについては車両製造元での出生証明を付与し、VIDⅡでは政府の車両登録や、メンテナンス履歴の証明・追跡がスコープとなっている

VIDの準拠標準について



VIDI



VIDⅡ

- VIDⅠ、VIDⅡともに、公開されている部分は冒頭のサマリと用語定義のみで、本文はMOBIメンバーのみに公開されるとしている
- VIDⅠでは、備考として「一部明確な方法と要件を示すが、他の実装固有要素は、実装時の柔軟性を保持するために意図的に曖昧なままにしている」とし、その例としてW3CのDIDsと、他の統合IDプロトコルの対立を述べている
- しかし、用語定義の中でVCs、DIDsについてはW3Cで規定された標準である旨言及していることから、関連規格について認識しているものと思われる

出所）
1 https://dlt.mobi/

ユースケース：信用組合の身元証明効率化

分野：金融

フェーズ：実運用

米国
カナダ

概要

- 米国のEvernym社は、信用組合サービス組織であるBonifiに対して信用組合のメンバー証明VCの発行と、それを格納するデジタルウォレット、レジストリを含むMemberPassのシステムを構築するサポートを提供した
- 信用組合のメンバー認証に係る時間が80%減少するなどの効果を挙げた[1,2]

主体・ユーザー

- 費用負担主体：Bonifi（信用組合サービス組織）
- 価値提供主体：Evernym
- 参加者：信用組合及びメンバー（費用の負担は不明）

使用されている技術

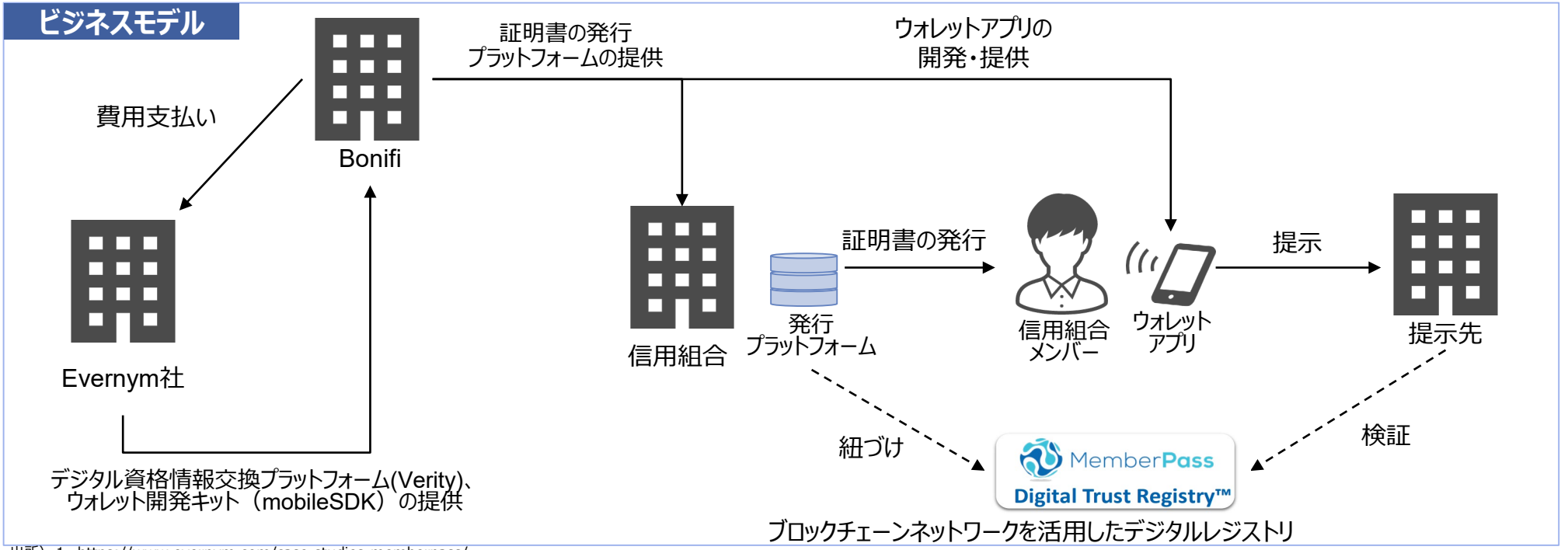
- W3C VCs

扱う属性情報

- 信用組合のメンバー資格

ペインポイント	提供する価値
従来の信用組合のセキュリティが不十分（簡単な本人確認質問など）	検証可能な信用組合メンバー資格情報の発行
信用組合のメンバー認証に時間を要する	デジタル資格情報の検証による認証の高速化

ビジネスモデル



出所）1 https://www.evernym.com/case-studies-memberpass/
2 https://secureservercdn.net/198.71.233.197/yxs.15e.myftpupload.com/wp-content/uploads/2020/05/052620-Trust-Registry-Flyer-v-Final-4.pdf

ユースケース：難民IDの提供

分野：医療

フェーズ：実運用

米国
カナダ

概要

- NGO団体のiRespondによって、個人識別手段を持たない難民に対して、分散型デジタルIDと医療サービス等へのアクセスが提供されている[1]
- 虹彩スキャン画像を12桁のID番号に変換してブロックチェーンネットワークに保存し、IDと紐づけられた医療記録はデータベースに保管される
- 虹彩スキャン画像のみが医療記録へのアクセスキーとなる[2]

エンティティ

- 費用負担主体：不明
- 価値提供主体：iRespond
- 参加者：ユーザー（難民）、医療機関

使用されている技術

- ブロックチェーン

扱う属性情報

- 医療記録

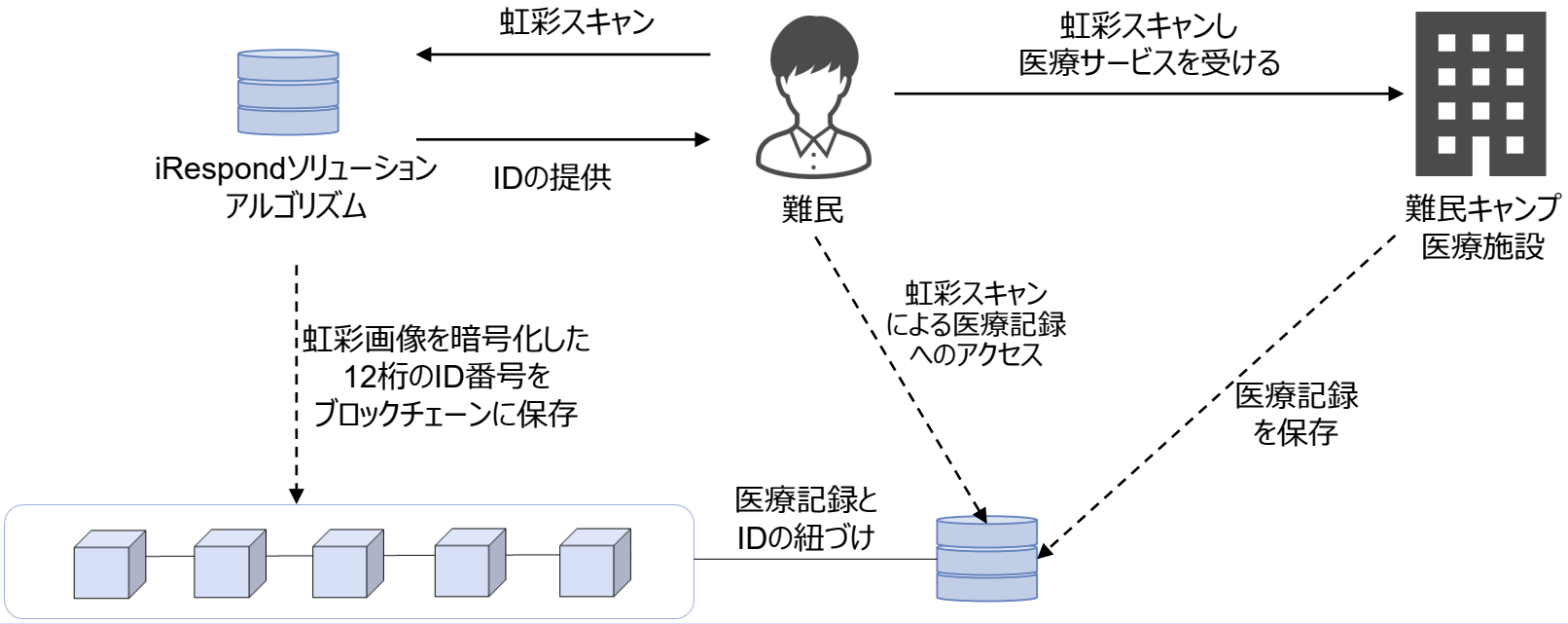
ペインポイント

難民は個人識別手段がなく十分な医療サービスが受けられない

提供する価値

IDを付与することで医療サービスを受けることが可能になる

ビジネスモデル



出所）1 https://www.irespond.org/
2 https://www.newsweek.com/2019/03/08/can-blockchain-finally-give-us-digital-privacy-we-deserve-1340689.html

オンタリオ州デジタルID

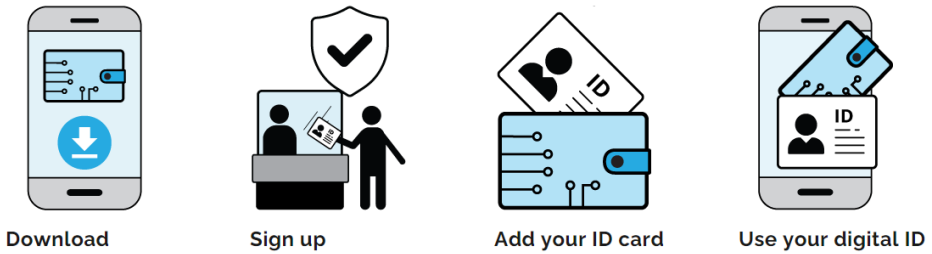
オンタリオ州政府は、民間企業と連携して州の住民向けのデジタルIDサービスの開発・提供を実施しており、W3C、DIF、ToIP、OpenID Connectなどに準拠した分散型・自己主権型IDのモデルを採用している

デジタルIDシステムの開発

- オンタリオ州政府は、2017年から州の中小企業イノベーションチャレンジ（SBIC）の一環として、オタワに拠点を置くBluink社を支援し、モバイルアプリであるeID-Meを開発した
- デジタルウォレットでのID管理をシステムの中心として、2021年後半からリリース予定としていた（オンタリオ州政府のWebサイトでは、リリースに向け準備中となっているが、Bluink社のHPではeID-Meは実稼働している）[1]

オンタリオ州デジタルIDの概要

- オンタリオ州住民は、モバイルアプリをインストールし、オンラインもしくは対面の確認でサインアップした後、デジタルウォレットに州政府発行の証明書を格納・提示することが可能となる
- W3CのVCモデルに準拠したプロセスで発行・提示・検証を行うとしている[2, 3]



オンタリオ州の準拠する技術・標準

オンタリオ州政府は準拠を検討している技術・標準を以下のとおり公開している[4]

データモデル
Verifiable Credential(W3C)

鍵管理
DID(W3C)

データ形式
JSON-LD(W3C)

DIDメソッド
・DID:WEB,DID:KEY(W3C)
・DID:PEER(DIF)

通信層
DIDCommV2(DIF)

ID標準
OIDC(OIDF)

相互運用性
・SIOP V2(OIDF),
・Presentation Exchange, Credential Manifest(DIF),
・ Aries Interop Profile 2.0(Hyper ledger)

署名形式
BBS+(BLS12-381), EdDSA(W3C)

出所）1 https://bluink.ca/blog/posts/press-release-bluinks-eid-me-brings-ontario-digital-identity-to-your-smartphone
2 https://toronto.ctvnews.ca/ontario-prepares-to-launch-digital-id-program-and-here-s-how-it-works-1.5577757
3 https://www.ontario.ca/page/digital-id-ontario
4 https://www.ontario.ca/page/ontarios-digital-id-technology-and-standards

ISEによる資金提供プログラム

カナダのイノベーション科学経済開発省(ISE)はInnovative Solution Canadaというイノベーター企業への資金提供プログラムを行っており、2019年に「User-Centric Verifiable Digital Credentials」と題し、個人が保有する、ポータブルかつ安全なデジタル資格情報：自己主権型IDソリューションを募集した[1, 2]

User-Centric Verifiable Digital Credentialsの公募概要

提案するソリューションの要件

- 国内またはグローバルに相互運用可能な検証プラットフォームで動作できるユーザー中心の検証可能なデジタルクレデンシャルを作成すること
- ユーザーのプライバシーとIDを保護する事
- W3CのDIDs/VCs、JSON-LDなどの標準に準拠したウォレット、エージェントを使用した検証可能なデジタル資格情報の作成・送信・保存をサポートすること
- PCTFその他（限定しない）のガイドラインに準拠していること

プロジェクトへの資金提供

- フェーズ１で最大150,000カナダドル、フェーズ2で最大1,000,000カナダドルの資金提供を行うとして提案を募集し、フェーズ1で適格とされた提案のみフェーズ2に進んだ

採択されたユースケース

- 最終的に6つのユースケースが公表されており、2021年に最終報告会と公開デモが実施された
- 採択されたベンダーにはオンタリオ州デジタルIDに関係するBluinkやVerified.Meの提供主体であるSecurekeyなどが含まれている

出所）1 https://canada-ca.github.io/ucvdcc/
2 https://ised-isde.canada.ca/site/innovative-solutions-canada/en/user-centric-verifiable-digital-credentials

OPCによる取り組み

カナダのプライバシー権の保護および促進を目的とした両院議会内の主体であるOPC（プライバシーコミッショナー事務局）は、デジタルIDの実装に係る研究への支援や、デジタルIDやプライバシーについてオンブズマンとの共同決議などを行っており[1]、特にデジタルIDエコシステムに関係する共同決議においては、中央集権的な仕組みを避け、個人の主権とプライバシーを重視するよう政府含むデジタルIDのステークホルダーに求めていることが分かる[2]

OPCによる取り組み例

プライバシーに関する研究支援

OPC は、2022年6月20日にプライバシー研究を支援する「Contributions Program」の一環として、社―ブルック大学に47,443カナダドルの給付を発表した。この研究プロジェクトは、カナダ企業において、従業員のプライバシー尊重や法令を順守しながら、クラウドベースのデータストレージを行うデジタルIDを実装する方法を検討するものであり、プロジェクトは、2023年3月末までに完了予定である

プライバシー監視の責任を負う連邦・州・準州のプライバシーコミッショナー及びオンブズマン共同決議

OPCは2022年9月21日にデジタルIDエコシステムにより、個人、企業および政府がIDを確認し、高度な効率性と信頼性を持ってオンラインで取引を行うためのオンブズマン決議を行った。決議の中では、デジタルIDエコシステムへの参加者に対する以下の様な提言・要求が述べられている

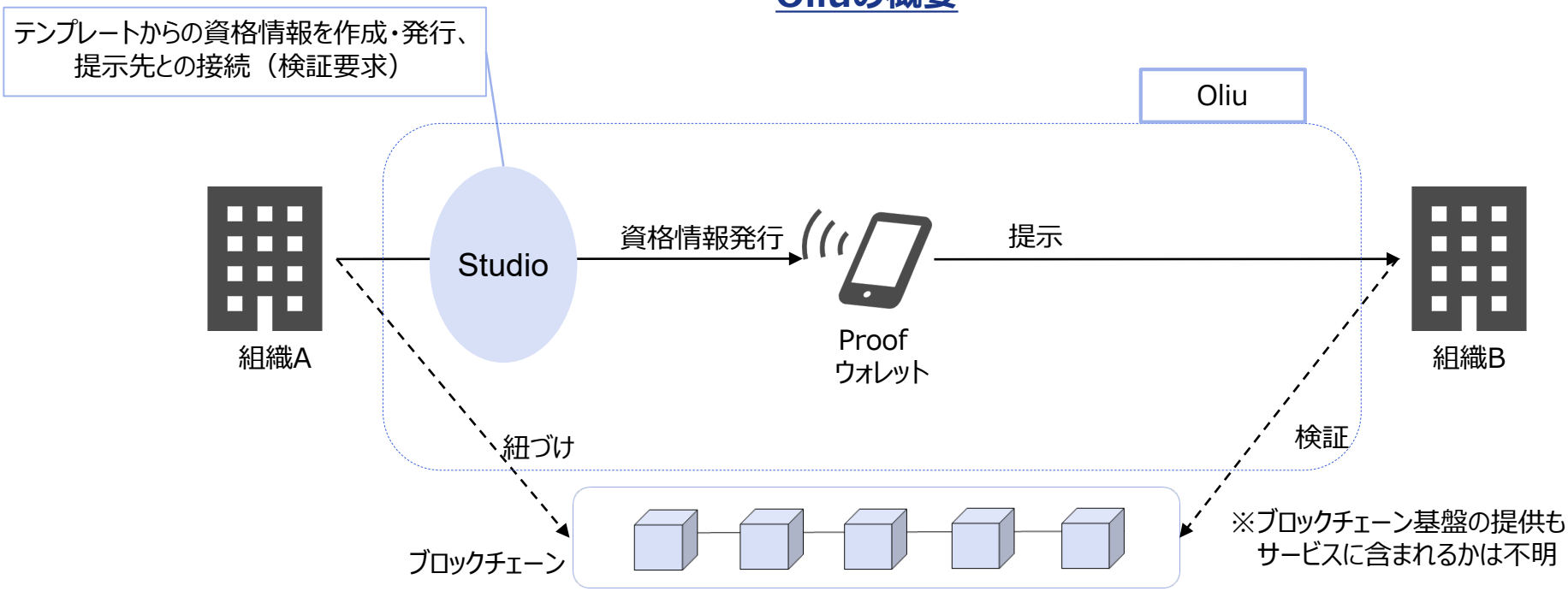
・デジタルIDエコシステムは中央データベースを構築すべきではない
・個人は自分の個人情報を管理する必要がある
・デジタルIDエコシステムへの個人の参加は、自発的かつ任意である必要がある
・・・・

出所）1 https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/cp_bg/
2 https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_220921_02/

政府とATB Ventures社の連携

- カナダの金融機関ATB Financialの研究部門であるATB Ventures社（DIACCのメンバー）は、2022年2月にカナダ政府と連携した国家デジタルトラストサービスのPoCをサポートするため、同社の自己主権型ID管理ソリューションプラットフォームである「Oliu」を提供し、9月に同プラットフォームを販売開始した[1]
- OliuはW3Cの各種標準に準拠し、ブロックチェーンを基盤とした資格情報を発行するためのノーコードで利用できるWebアプリケーションやAPIからなる「Studio」と、クレデンシャルウォレットである「Proof」からなり、デジタルクレデンシャルの発行、検証のための総合的なスイートであるとしている[2]

Oliuの概要



出所）
1 https://oliu.id/studio/
2 https://www.newswire.ca/news-releases/atb-ventures-r-launches-their-enterprise-software-platform-oliu-tm-to-organisations-today-accelerating-the-adoption-of-digital-identity-854314621.html

KTDIへの参加

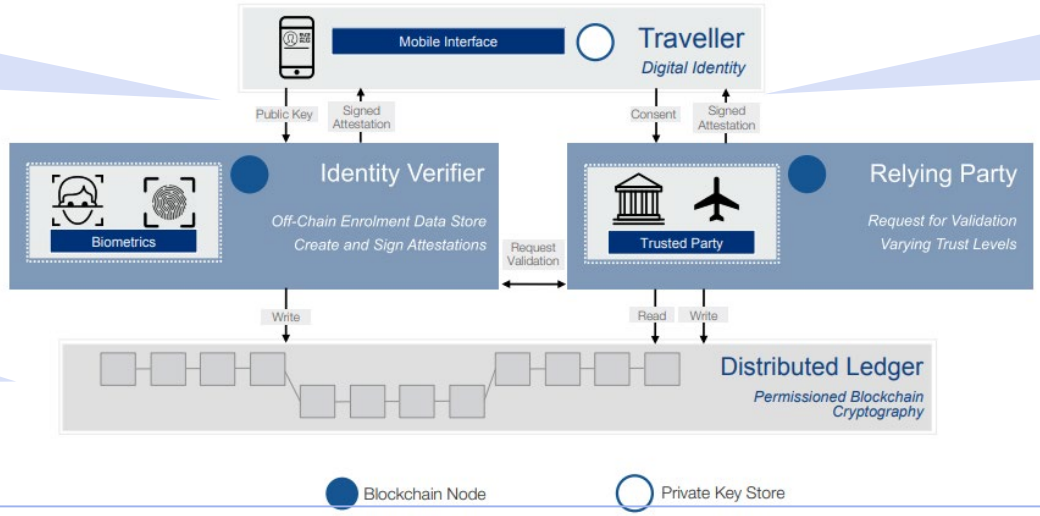
- **カナダ政府は、世界経済フォーラム（WEF）の主導する、世界旅行における旅行者IDを通じたセキュリティ強化を推進するイニシアチブであるKTDIにパートナーとして参加している[1]**
- **KTDIは、旅行者個人が検証されたID属性を自己管理できる分散型IDをコンセプトとしたグローバルコンソーシアムを結集するとしており、カナダ、オランダが政府として参加している[2]**

Known Traveller Digital identity(KTDI)パイロットの概要

- KTDIのパイロットグループは、カナダ政府とオランダ政府を中心として、エアカナダ、モントリオール空港、アムステルダム空港などが2018年から参加し、2019年に内部でのテストを実施した
- KTDIのプロトタイプでは、旅行者がパスポートや市民権、生体情報といった、信頼できるエンティティによって証明された検証済み資格情報をモバイルデバイスで管理し、旅行の各段階で（事前）提示することにより搭乗・出入国プロセスを迅速化し、また検証結果はKTDIプロファイルに追加されることで、当局のリスク管理の容易化などを実現するとしている[3]

KTDIのプロトタイプコンセプト

旅行者はパスポート情報や生体情報をモバイルアプリを通じて提供し、政府当局の検証を受けることでプロファイルが作られる



検証されたID情報は、旅行者の同意に基づき旅行の各段階で空港職員や国境当局に提示され・検証される

資格情報の識別子、発行・検証組織の公開識別子は暗号化され、分散型台帳に書き込まれる

出所）1 https://ktdi.org/
2 https://www.westernstandard.news/news/canada-one-of-two-countries-participating-in-wef-travel-digital-id-pilot-program/article_54eca963-702b-5652-8d83-76ad92bfd6f1.html
3 https://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf

ユースケース：Interac verification service

分野：金融

フェーズ：実運用

米国
カナダ

概要

- Interac社とカナダの金融機関により、デジタルID検証ネットワークであるInterac verification serviceが提供されている（※）
- Interac verification serviceは金融機関に登録しているIDや属性情報を、アプリケーションを通じて連携・提示・検証することを可能にするサービスで、政府サービスへのログインも可能である[1]

（※）2022年現在にInterac社によりSecureKey Technology社が買収され、Verified Meから名称変更した[2]

エンティティ

- 費用負担主体：不明
- 価値提供主体：SecureKey Technology社（当初）
- 参加者：ユーザー、金融機関、企業・政府等のサービス提供機関

使用されている技術

- DID（W3C）、ブロックチェーン（Hyperledger Fabric）

扱う属性情報

- 金融機関に登録している属性情報

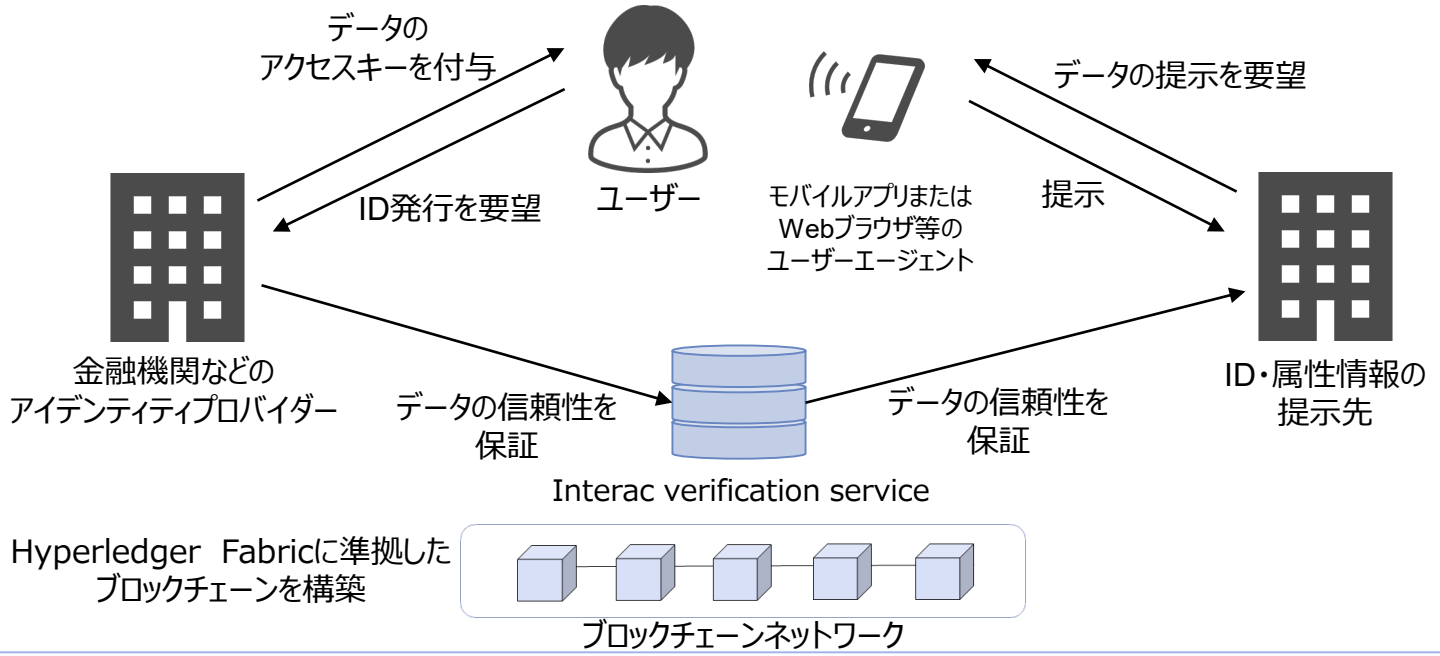
ペインポイント

電子メールでの個人情報のやり取りによる個人情報の盗難や詐欺の発生

提供する価値

安全かつ信頼性のある認証システムによる不正の排除

ビジネスモデル



出所）1 https://verified.me/
2 https://www.interac.ca/en/consumers/products/interac-verification-solutions/sign-in-service/

ユースケース：BCデジタルトラスト-OrgBookBC

分野：行政

フェーズ：実運用

米国
カナダ

概要

- ブリティッシュコロンビア（BC）州政府は、デジタルIDとVCに関するプロジェクトである「BCデジタルトラスト」を行っている
- BCデジタルトラストでは、VCを発行・検証するためのソフトウェアや、オープンソースのデジタルIDウォレットであるBCウォレット、及び州政府等の発行した資格情報を検索・入手できるパブリックディレクトリである「OrgBookBC」の開発・提供を行っている[1]

エンティティ

- 費用負担主体：不明
- 価値提供主体：BC州政府
- 参加者：ユーザー、市民サービス省

使用されている技術

- W3C VCs、ブロックチェーン（Hyperledger Aries、Indy、Ursa）

扱う属性情報

- 不明

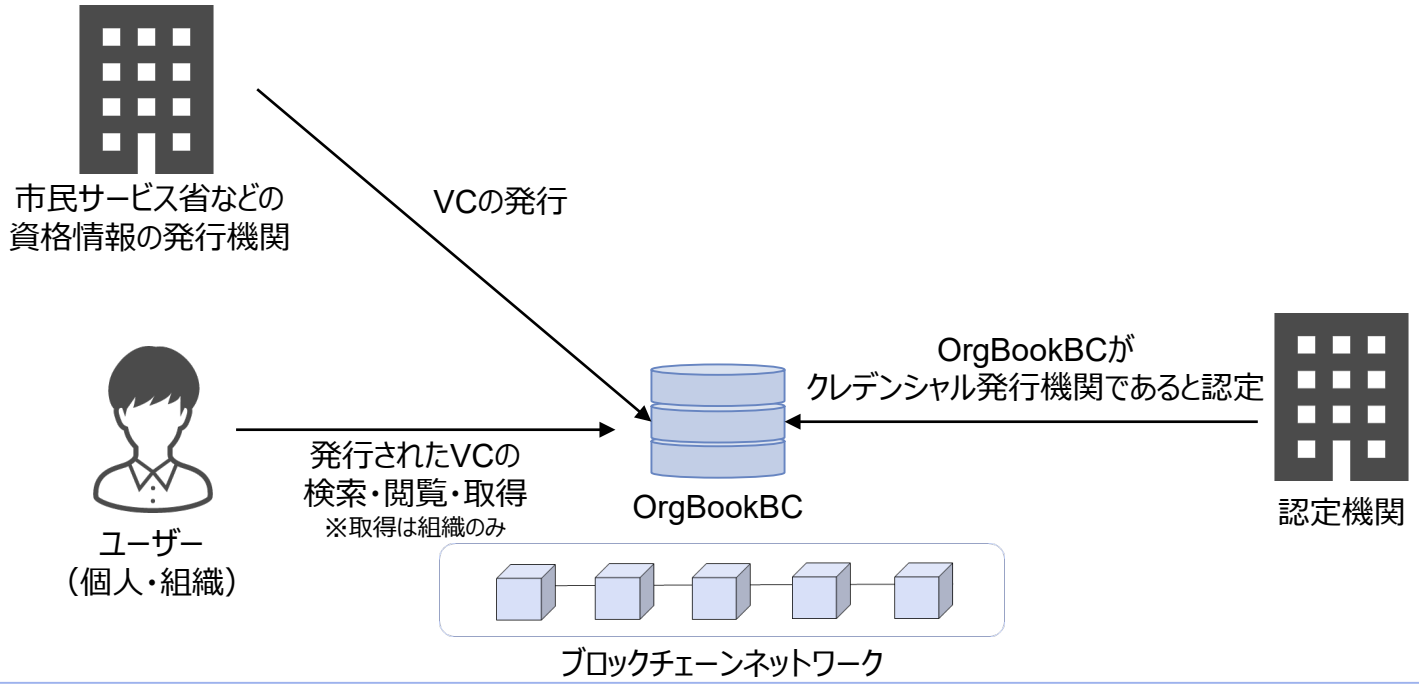
ペインポイント

証明書の発行・認証には時間と労力がかかる

提供する価値

証明書の発行・認証をシステム化することで時間と労力を削減

ビジネスモデル



出所）
1 https://digital.gov.bc.ca/digital-trust/projects-and-initiatives/orgbook-bc/

ユースケース：Nothern Block

分野：行政、旅行、金融、医療、サプライチェーン

フェーズ：実運用

米国
カナダ

概要

- Nothern Block社によって、企業向けのデジタルクレデンシャル管理・発行プラットフォームとWebベースのクラウドウォレットからなる「Orbit Enterprise」と、個人向けのデジタルクレデンシャル格納・提示を行うモバイルウォレットである「Orbit Edge Wallet」が提供されている
- 相互運用性の確保、ゼロ知識証明による選択的開示も可能とされている[1]

エンティティ

- 費用負担主体：不明
- 価値提供主体：Nothern Block社
- 参加者：ユーザー（個人、企業）

使用されている技術

- VC、DID（W3C、Anoncreds）、ブロックチェーン（Hyperledger）

扱う属性情報

- 運転免許証、パスポート等

ペインポイント

資格情報の発行機関が多数あり管理が煩雑

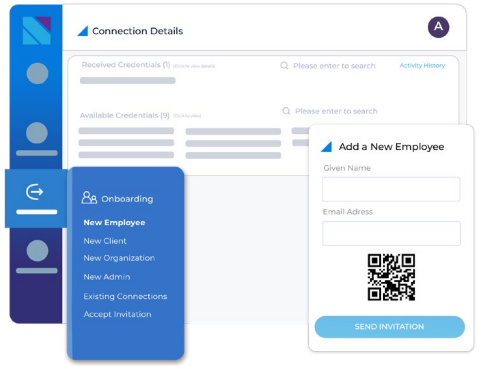
提供する価値

単一システムで多数の資格情報を管理することが可能

ビジネスモデル

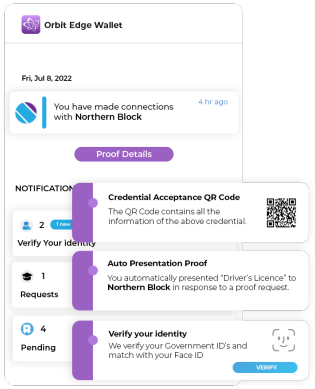
Nothern Blockの提供サービス

Orbit Enterprise



企業向けのデジタルクレデンシャル管理・発行プラットフォームとWebベースのクラウドウォレット

Orbit Edge Wallet



個人向けのデジタルクレデンシャル格納・提示を行うモバイルウォレット

出所）
1 https://northernblock.io/orbit-edge-wallet/

ユースケース：eID-Me

分野：行政・金融・小売・医療等

フェーズ：実運用

米国
カナダ

概要

- カナダのオタワに所在するBluink社は、身分証明書のスキャン・生体認証によって作成した検証済みのデジタルIDと、行政・企業のサービスを統合するソリューションであるeID-Meを提供している[1,2]
- eID-Meはオンタリオ州政府のデジタルIDにおいても使用されている[3]

エンティティ

- 費用負担主体：行政機関、民間企業（金融、小売、医療、旅行、法務、シェアリングエコノミーが例として示されている）
- 価値提供主体：Bluink社
- 参加者：行政・企業サービスのユーザー

使用されている技術

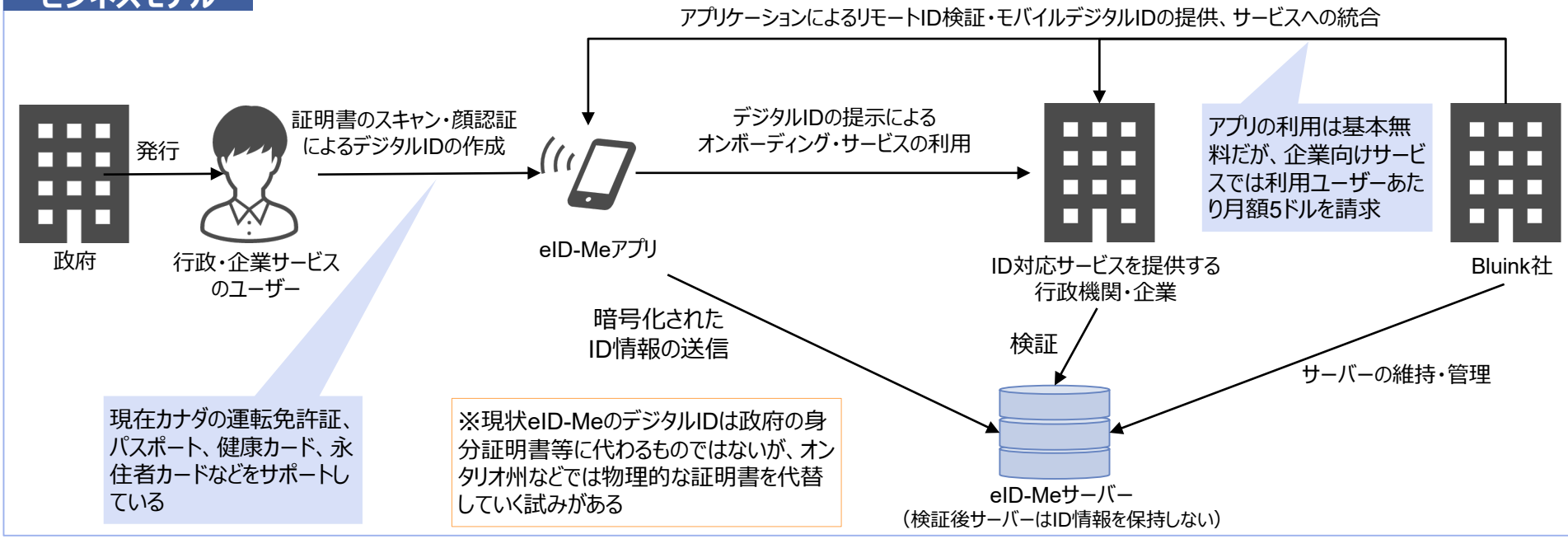
- W3C VCs, OpenID Connect, SAML

扱う属性情報

- 本人確認情報（政府発行証明書）

ペインポイント	提供する価値
ユーザーのなりすまし、ID詐欺のリスク	検証済デジタルID作成によるセキュリティ強化
サービスへのオンボーディングに係るコスト	登録の容易化による顧客体験向上、対面確認などのコスト削減

ビジネスモデル



出所）1 https://reviews.financesonline.com/p/bluink-enterprise/
2 https://bluink.ca/eid-me#solutions
3 https://docs.bluink.ca/eid-me/faq.html

3.3 詳細調査結果：自己主権型／分散型アイデンティティに関する取り組み

3.3.3 オセアニア（オーストラリア、ニュージーランド）における調査結果

連邦政府・州政府によるデジタル資格情報の活用

- **ニューサウスウェールズ（NSW）州の行政サービス提供主体であるService NSWは州政府の発行する資格情報をデジタルウォレットで管理することのできるアプリケーションを提供しており[1,2]、その取り組みの中で自己主権型／分散型IDに関する議論・計画が実施されている[3,4]**
- **2023年2月には、連邦政府と州・準州政府の間で国家のデジタルIDシステムにデジタル資格情報を含めるための契約に合意したことが報じられている[5]**

NSWデジタルID

Service NSWアプリ

- Service NSWが提供するスマートフォンアプリであり、ユーザーは州政府の発行する一部の資格情報を端末に保存し、表示することができる。利用にはオンライン行政サービスプラットフォームであるMyServiceNSWのアカウントと、セルフィーと2つ以上の身分証明書によるNSWデジタルIDの作成が必要となる
- 現状運転免許証、Covid-19デジタル証明書、個人事業主免許、船舶運転免許等12の資格情報が利用可能となっているおり、州政府のパートナー企業や政府機関で使用することができる。データモデルや準拠している技術標準は現状確認できなかった

自己主権・分散型IDへの言及

- 州政府はNSWデジタルIDについて、「NSWデジタルIDとそのパイロットでは、**暗号化された個人情報をデバイスに保管でき、政府や民間企業によって中央保持されることはない**。」「ウォレットによって**信頼され、分散化され、検証可能な資格情報を管理・共有できるようになる**」と述べている

連邦政府・州政府の連携

- NSW州政府は連邦政府との資格情報の連携についても検討中であるとしているが[2]、2023年2月に連邦政府が新しい国家デジタルIDシステムにデジタル資格情報を含めるために、州および準州との契約に合意したと報じられた
- これにより、**国際標準に基づいたデジタル資格情報をウォレットに保管し、全国的に使用可能になる**とされている

出所)
1 https://www.service.nsw.gov.au/transaction/get-started-digital-licences
2 https://www.nsw.gov.au/nsw-government/projects-and-initiatives/how-it-works
3 https://www.itnews.com.au/news/service-nsw-to-bring-facial-verification-to-digital-channels-572839
4 https://www.itnews.com.au/news/nsw-ready-to-pilot-decentralised-digital-id-587834
5 https://www.biometricupdate.com/202302/australia-and-state-govts-agree-on-digital-id-credential-sharing-deal

ユースケース：学生登録・本人確認プロセスの分散化

分野：教育

フェーズ：PoC

オーストラリア
ニュージーランド

概要

- Mastercardは、2020年にオーストラリア郵便公社のデジタルIDサービス（DigitaliD）とディーキン大学の学生登録及び本人確認プロセスと統合するパイロットを実施した
- 学生はDigitaliDを使用して大学のオンライン試験ポータルにアクセスすることができ、これはMastercardのネットワーク内のプロバイダーとのサービス統合作業に基づいて行われた[1]
- 銀行や政府機関などのリファレンスポイントによって検証された情報を個人がデバイスに保持することで、分散モデルを実現するとしている[2]

エンティティ

- 費用負担主体：不明
- 価値提供主体：オーストラリア郵便公社、Mastercard
- 参加者：ディーキン大学（学生）

使用されている技術

- 不明

扱う属性情報

- 大学の在籍証明（本人確認）

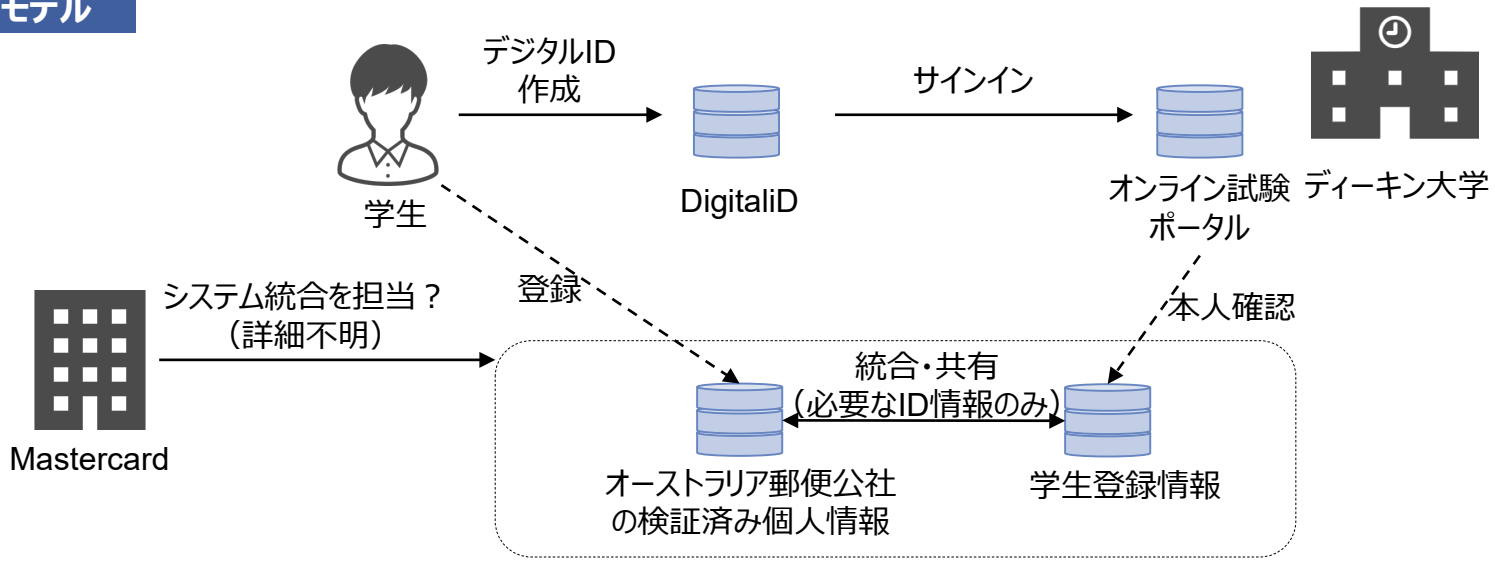
ペインポイント

一元的なIDデータベースの保持

提供する価値

分散型のIDモデルの導入（実験）

ビジネスモデル



出所） 1 https://www.zdnet.com/article/mastercard-expands-digital-id-trial-with-deakin-and-australia-post/
2 https://www.deakin.edu.au/about-deakin/news-and-media-releases/articles/deakin-and-mastercard-trialling-a-new-digital-identity-service2

ユースケース：OCR Labs

分野：不動産・金融・保険等
フェーズ：実運用
オーストラリア
ニュージーランド

概要

- オーストラリアのデジタルIDソリューション提供企業であるOCR Labsは、不動産・金融・保険等の企業向けの顧客本人確認サービスを提供している
- 顧客はフェイスキャプチャと身分証明書による登録でユーザーIDを作成・検証することができ、検証済みIDによって当該企業へのオンボーディング・本人認証が可能になる[1]
- OCR LabsはTDIFの認定を受けている

エンティティ

- 費用負担主体：企業（金融、不動産、保険等）
- 価値提供主体：OCR Labs
- 参加者：当該企業の顧客

使用されている技術

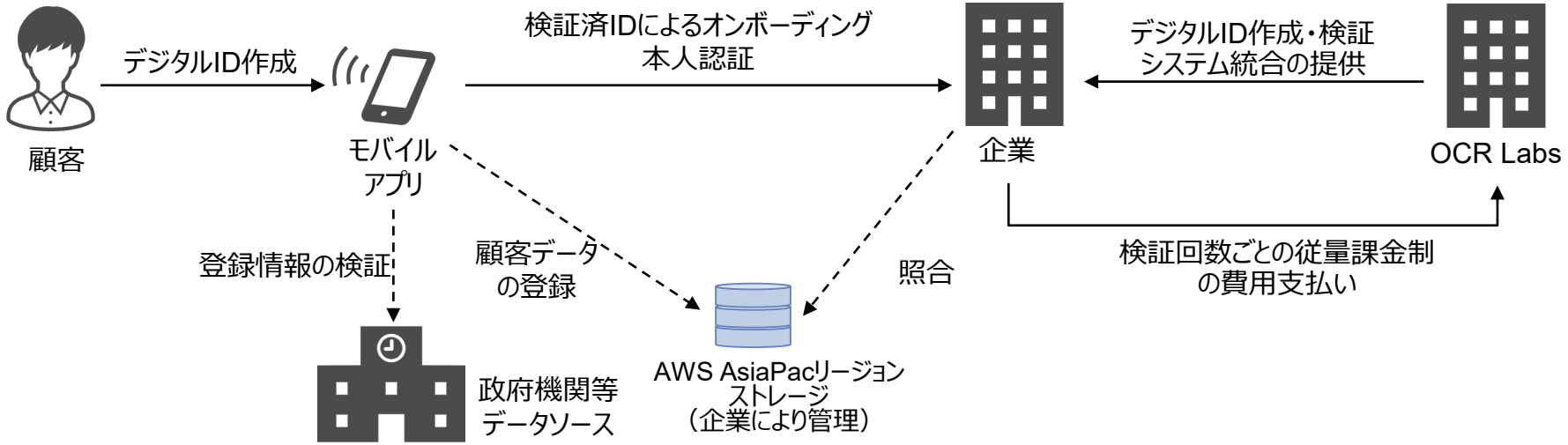
- 生体認証（フェイスキャプチャ）、OAuth

扱う属性情報

- 本人確認

ペインポイント	提供する価値
顧客のオンボーディング・本人確認に時間を要する	登録・検証の自動・高速化
ID詐称による不正	検証済デジタルIDによる不正の防止

ビジネスモデル



出所）
1 https://ocrlabs.com/technologies/id-verification

MATTRワクチンパス

- ニュージーランド政府保健省は2021年に、コロナウィルスのデジタルワクチンパスのプロバイダーとしてオークランドのIT企業であるMATTRを選定した
- MATTRは資格情報の生成・検証・管理などの各種デジタルIDサービスを提供する企業であり、DIF、OIDF、W3C、IETF等の主要な国際標準化団体のDID、VC関連規格をサポートしている[1, 2]
- デジタルワクチン接種証明書の仕様はGithubで公開されており、W3CのVCデータモデルやDIDweb、IETFのJson Web Keyなどオープンな国際標準に準拠している[3]

MATTRの提供するワクチンパス

出所）1 https://www.health.govt.nz/news-media/media-releases/technical-information-published-support-covid-19-vaccine-pass-and-verifiers
2 https://learn.mattr.global/docs/platform/supported-standards
3 https://github.com/minhealthnz/nzcovidpass-spec

ユースケース：MATTRワクチンパスの実装

分野：医療
フェーズ：実運用
オーストラリア
ニュージーランド

概要

- ニュージーランド政府保健省は2021年に、コロナウィルスのデジタルワクチンパスのプロバイダーに、オークランドのIT企業であるMATTRを選定した
- MATTRは資格情報の生成・検証・管理などの各種デジタルIDサービスを提供する企業であり、DIF、OIDF、W3C、IETF等の主要な国際標準化団体のDID、VC関連規格をサポートしている
- デジタルワクチン接種証明書の仕様はGithubで公開されており、W3CのVCデータモデルやDIDweb、IETFのJson Web Keyなどオープンな国際標準に準拠している

エンティティ

- 費用負担主体：ニュージーランド政府
- 価値提供主体：MATTR
- 参加者：ワクチン接種者、医療従事者

使用されている技術

- W3C、OIDF、DIF、IETFなどの各種標準に準拠（Github上に一覧）

扱う属性情報

- ワクチン接種記録

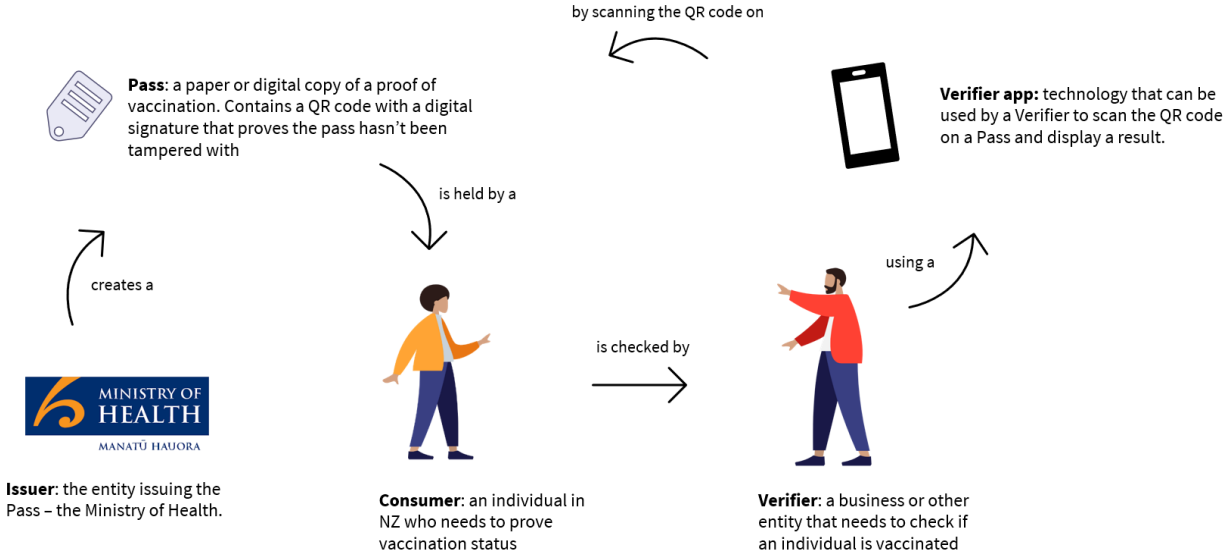
ペインポイント

正確なワクチン接種記録の確認が困難

提供する価値

改竄不可能なワクチン接種状況の証明・検証

ビジネスモデル



①ワクチンパスはニュージーランド保健省によって発行され、デジタル署名付きのQRコードが含まれる紙もしくはデジタル証明書形式で交付される

②ワクチン接種状況の確認が必要な場面で生活者（国民）はVerifierに対し紙もしくはデジタルで証明書を提示する

③Verifierは検証アプリケーションでQRコードをスキャンし、ワクチン接種状況を確認する

※各種データのやり取りは、W3CのVCデータモデルに基づいている

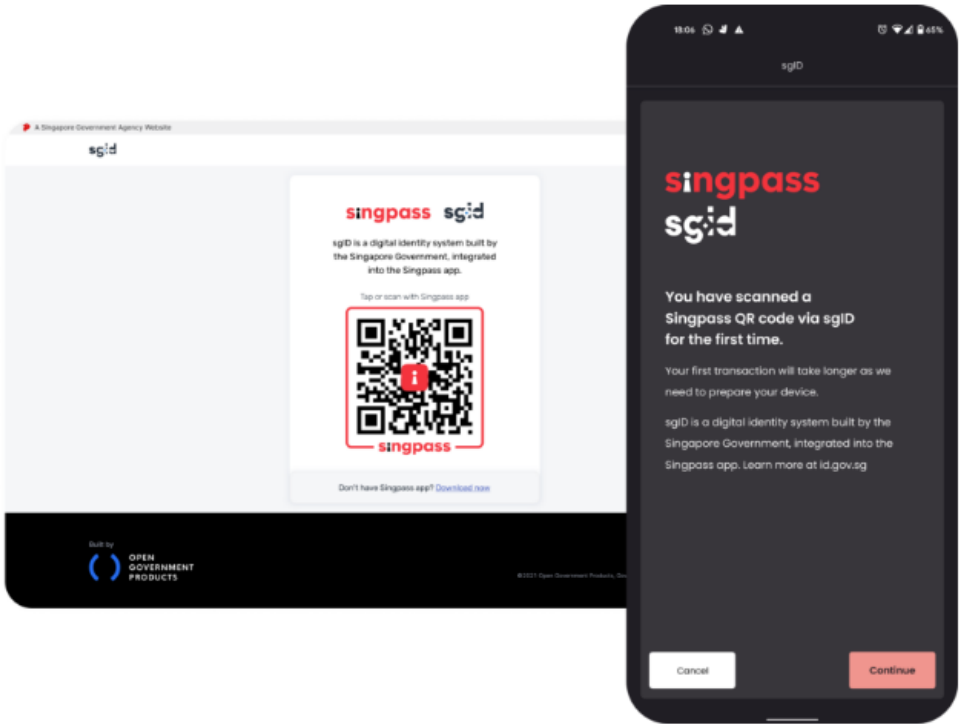
3.3 詳細調査結果：自己主権型／分散型アイデンティティに関する取り組み

3.3.4 アジア（シンガポール、インド）における調査結果

sgID

- sgIDは、GovTechによって開発されている、プライバシー保護に重点を置いた実験的な認証およびデータ共有サービスであり、一部の企業や政府機関で利用できる。sgIDはユーザーが認証を求められるビジネス・サービスごとに固有識別子（unique identifier）を発行するため、NRICなど単一の個人識別番号に依存しないとされる
- sgIDによる通信は、ゼロ知識プロトコルを用いてやり取りされ、またユーザーは認証・共有するデータをコントロールできることで安全性・自己主権性を高めているとされ、sgIDへのログインは、Singpass MobileのQRコードスキャンによって行われる[1, 2]

Singapass Mobileを通じたsgIDへのログイン画面



出所）1 https://www.id.gov.sg/
2 https://www.open.gov.sg/products/sgid/

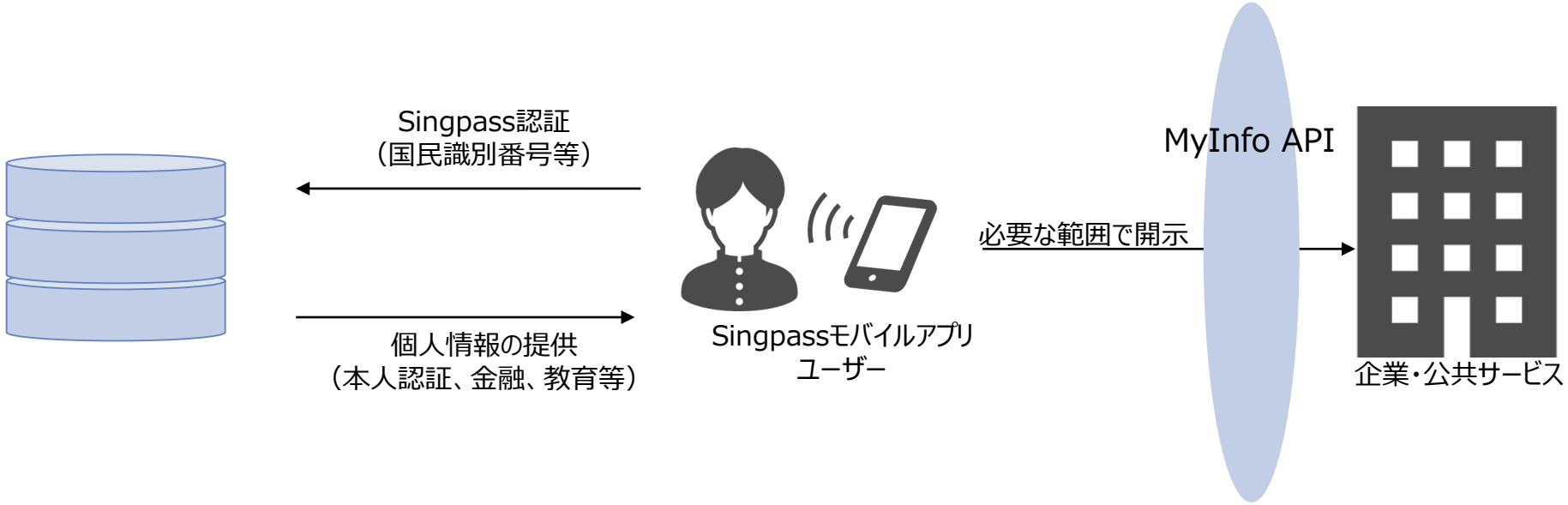
シンガポール
インド

分散型アイデンティティへの移行情報

GovTechのナショナルデジタルアイデンティティ（NDI）・ディレクターであるKendric Lee氏は、アラン・チューリング研究所が2022年7月に開催した公開セッションで、「Singpassで利用できるサービスのMyInfoはユーザーが自分のIDを制御する試みであり、ある程度フェデレーション型のエコシステムだが、W3CのDID、VCなどに基づく分散型モデルを検討している」旨述べた[1]

MyInfoの現状スキーム図

MyInfoは現状では個人のスマートフォンにインストールされたSingpassモバイルアプリから認証を行い、政府のデータソースから必要な個人情報を選択して、MyInfoAPIを通じて企業・公共機関へ開示・入力するスキームとなっている



出所)
1 https://www.biometricupdate.com/202207/singpass-incorporates-digital-identity-card-saves-36-per-onboarding-considers-decentralization

Project Guardian

シンガポール金融管理庁（MAS）は、2022年5月にブロックチェーンを活用した資産トークン化のユースケースを探求する金融業界との共同イニシアチブであるProject Guardianを発表し、その中で4つの主要な分野でユースケースを開発するパイロットを実施するとしており、その一つに「信頼ある分散型金融（DeFi）の環境のための、参加するエンティティの検証可能な資格情報を発行・検証する独立したトラストアンカー」が挙げられている[1]

Project Guardianで開発される４分野のユースケース

分野	開発するユースケースの概要
オープンで相互運用可能なネットワーク	パブリックブロックチェーンを使用し、デジタル資産を取引できるようにするオープンで、既存の金融インフラストラクチャとも相互運用可能なネットワークを構築する
トラストアンカー	独立したトラストアンカーの共通のトラストレイヤーを通じて、DeFi＊プロトコルを実行するための信頼ある環境を確立する。トラストアンカーは、DeFiプロトコルへの参加を希望するエンティティに検証可能な資格情報をスクリーニング、検証、発行する規制対象の金融機関である
資産のトークン化	デジタル伝送が可能な資産のセキュリティや、パブリックブロックチェーン上の預金受取機関によって発行されるトークン化された預金の利用を検討する
機関グレードのDeFiプロトコル	市場操作と運用リスクを軽減するために、DeFiプロトコルに規制上のセーフガードとコントロールを導入することを検討する

＊DeFi：ブロックチェーン上に構築された金融エコシステムの総称であり、既存の中央集権的な金融サービス管理主体（政府・銀行）の介在を必要としない仕組み。
ブロックチェーンによるスマートコントラクトや改ざん・不正の困難性によって、ユーザー同士の迅速かつセキュアな金融取引を実行可能にすると期待されている。

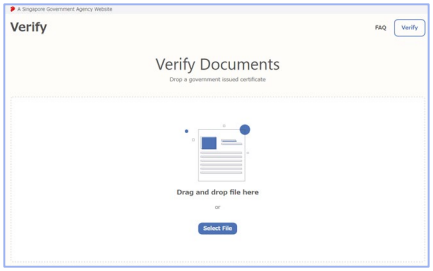
出所）
1 https://www.mas.gov.sg/news/media-releases/2022/mas-partners-the-industry-to-pilot-use-cases-in-digital-assets

Open Attestation

Govtechは、ブロックチェーンを利用した文書の発行・検証のオープンソースフレームワークである OpenAttestationを構築しており、下記のようなブロックチェーンを活用した各種証明書の発行・検証サービスを開発している

Verify

Verifyのアップロード画面



- GovTechの開発したデジタル公的証明書の検証システム
- シンガポール政府機関の発行する証明書には、固有のデジタルコードが紐付けられ、それは証明書の要約情報とともにブロックチェーン上で保存されている
- ユーザーはVerifyサイト上で証明書をアップロードし開くことによって、ブロックチェーン上の情報と対比が行われ、内容の改竄の有無・正式な証明書であるかを検証することができる

出所）https://www.verify.gov.sg/verify

Opencerts

検証された証明書の例

- GovTechとOpencertsコンソーシアムが開発した、デジタル卒業証明書の発行・検証システム
- Opencertsコンソーシアムに加盟する教育機関によって採用されており、ブロックチェーンを活用して改竄が困難な学術証明書を発行し、検証を可能にする
- 検証はVerifyと同様に、Opencertsのサイト上で証明書を開くことによって行うことができる

出所）https://www.developer.tech.gov.sg/products/categories/blockchain/opencerts/overview.html

SingpassとOpenAttestationの関連（補足）

SingpassとOpenAttestationの関連

- Govtechは、ブロックチェーンを利用した文書の発行・検証のオープンソースフレームワークであるOpenAttestationを構築しており、各種証明書の検証サービスであるOpencertsやVerfyは、OpenAttestationを利用した電子政府サービスである。（OpenAttestationはNDIとは別の取り組み）カナダもOpencertsを採用している[1]
- OpenAttestationでCovid-19の予防接種証明書を検証するサービスであるHealthcertsがSingpassアプリのドキュメントウォレットで表示できることから[2]、OpenAttestationによる文書の発行・検証はSingpassと連携していると思われる

参照される技術

- OpenAttestationは他のW3C　VCウォレットと相互運用性を持たせるべく、データモデルをW3Cの規格に合わせる予定であるとしている[3]
- その他、Singpassの一部における固有識別子を活用した認証サービスであるsgIDについては、使用している技術・参照規格などは確認できなかった

出所）1　https://www.openattestation.com/docs/docs-section/roadmap/v3/overview
2　https://gallery.openattestation.com/tag/health-certs
3　https://www.biometricupdate.com/202207/singpass-incorporates-digital-identity-card-saves-36-per-onboarding-considers-decentralization

シンガポール
インド

Aadhaarの補完に向けた取り組み

Aadhaarは生体情報を含む国民の個人情報を政府に提供する特性上、プライバシー侵害や情報流出への懸念に対する訴訟や、民間企業の利用に関する法改正などが度々生起していることから、Aadhaarを所管するUIDAIはAadhaarを補完する取り組みを行っている

Aadhaarを補完するための取組に関する情報

ブロックチェーン・量子コンピューティングの活用への言及

UIDAIのCEOは、2022年1月開催のIndia Digital Summit 2022で、Aadhaarのセキュリティ強化のため、ブロックチェーンや量子コンピューティング使用の可能性を探っていると発言した。Aadhaar 2.0では、エコシステムのセキュリティに重点を置き、自動化されたバイオメトリック・マッチング・ソリューションの高速化を図るとしている[1]

Aadhaar Notice and Consent Guidelinesの公開

UIDAIは2022年3月にAadhaar Notice and Consent Guidelineを公開している。
さまざまな官民組織の個人データの収集や処理を含む取引のシナリオに対処するために、通知や同意取得の実装に関するガイダンスを提供するものである[2]

デジタルID・映像KYC認証システムの開発

MeitY（インド電子情報技術庁）からの2億3,000万ルピーの支援をうけ、銀行研究所(IDRBT)、ハイデラバードの国際情報技術研究所、およびインド工科大学ビライ校などが、新しいブロックチェーンおよび機械学習ベースのデジタルIDと、ビデオKYC認証システムを開発中である。
このプラットフォームは、金融取引に必要なドキュメントを保存するデジタルウォレットとして、Aadhaarシステムの補完が可能としている[3]

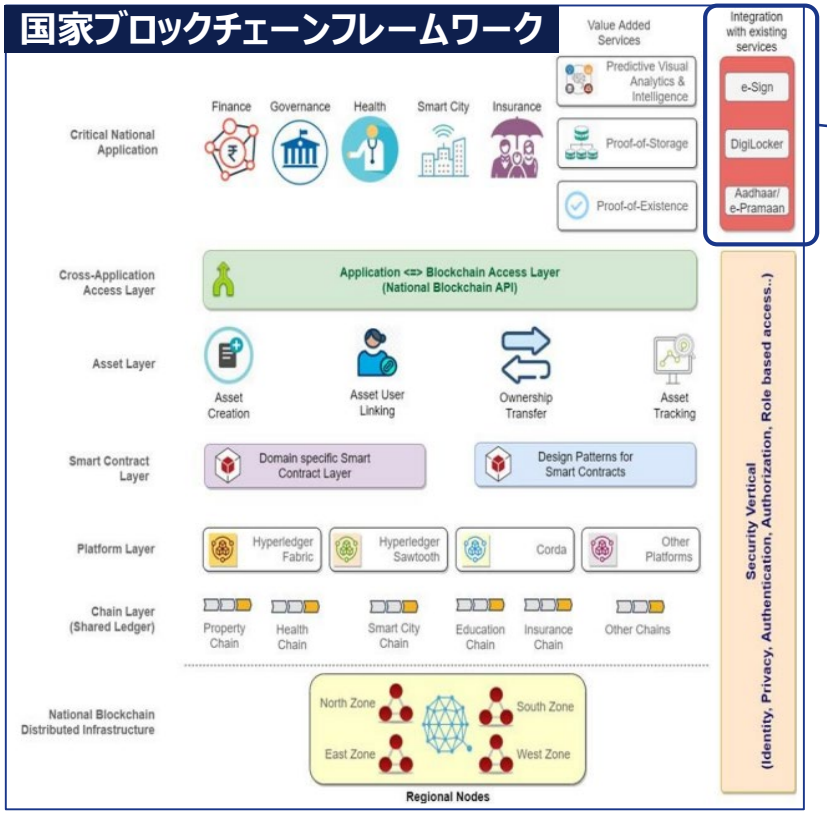
出所）1 https://www.dqindia.com/exploring-application-of-blockchain-quantum-for-aadhaar-uidai-ceo/
2 https://uidai.gov.in/images/resource/Final_Aadhaar_Notice_and_Consent_Guidelines.pdf
3 https://timesofindia.indiatimes.com/city/hyderabad/aadhaar-2-0-next-gen-digital-id-platform-being-built-by-city-based-research-bodies/articleshow/91110623.cms

NATIONAL STRATEGY ON BLOCKCHAIN

インド政府のMeitY（電子情報技術省）は2021年12月に「ブロックチェーンに関する国家戦略（NATIONAL STRATEGY ON BLOCKCHAIN）」を発表し、インド国内でのブロックチェーンの適用可能性や、開発作業の方向性、課題、及び参照モデルである国家ブロックチェーンフレームワークについて記述しており、その中でAadaarとブロックチェーンの接続可能性や、SSI／DIDについて言及されている[1]

NATIONAL STRATEGY ON BLOCKCHAINにおけるデジタルIDへの言及

国家ブロックチェーンフレームワーク



ブロックチェーンとAadhaar等の統合

インドの構築する国家レベルのブロックチェーンインフラの開発において参照するモデルとなる国家ブロックチェーンフレームワークにおいて、AadhaarやIndia StackのAPIなどの既存のアプリケーションとの統合可能性が述べられている

SSI、DIDへの言及

同文書では、インドでのブロックチェーン活用に関するパブリックコンサルテーションを行った結果から、実行可能な推奨事項を記載しており、その中では「自己主権型アイデンティティ、ゼロ知識証明・・・など、既存の関連技術を調査し、フレームワークの適切なレイヤーに統合する可能性がある」旨述べられている

出所）
1 https://www.meity.gov.in/writereaddata/files/National_BCT_Strategy.pdf

MeitY（電子情報技術省）ブロックチェーン技術センターオブエクセレンス

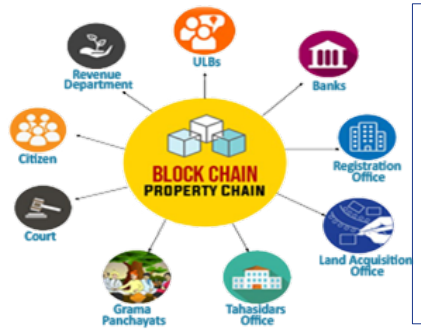
- インド政府のMeitY（電子情報技術省）は、全国的に調整された相互運用可能なブロックチェーンエコシステムを構築し、ブロックチェーンの実装を進めるためにブロックチェーン技術センターオブエクセレンス（CoE-BCT）を有している
- CoE-BCTは研究機関や政府と連携し、概念実証からプロダクトまでのブロックチェーンソリューションの開発と実装を進めており、以下の様なブロックチェーンプロダクトを実装している

CoE-BCTの開発したブロックチェーンプロダクト[1]

証明書チェーン（CC）

- ブロックチェーンを活用し、発行された証明書の記録・保管を行い、オンラインでのアクセス（取得）と検証を行うことを可能にする
- 教育試験委員会などで導入実績がある

プロパティチェーン（CC）

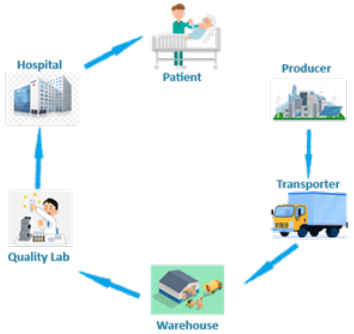


- ブロックチェーンを活用し、不動産の詳細と相続、売却、贈与などの取引を記録・参照可能にする
- カルナータカ州の提供するアプリケーションと統合実績がある

ドキュメントチェーン（DC）

- ブロックチェーンを活用し、カースト、収入、配給カード、運転免許証、出生・死亡証明書など、政府が発行した文書の保存と検索・検証を可能にする
- カルナータカ州の出生・死亡証明書、歳入庁の所得証明書などで導入実績がある

ロジスティクスチェーン（LC）



- ブロックチェーンを活用し、医薬品などの製造業者からサプライヤー、倉庫、病院にいたるまでの状態・取引を記録する
- カルナータカ州の医薬品物流倉庫協会での導入実績がある

出所）
1 https://blockchain.gov.in

ユースケース：Truscholar

分野：教育

フェーズ：実運用

シンガポール

インド

概要

- インドのTruScholar社はブロックチェーンネットワーク基盤をもってデジタル証明書インフラやクレデンシャルウォレット、分散型IDメカニズムを大学等教育機関に提供し、学術証明書の発行・失効等の記録管理、学習者IDの作成や、証明書の提示・検証を可能にするとしている[1]

エンティティ

- 費用負担主体：大学等教育機関
- 価値提供主体：Truscholar社
- 参加者：学生（費用負担なし）

使用されている技術

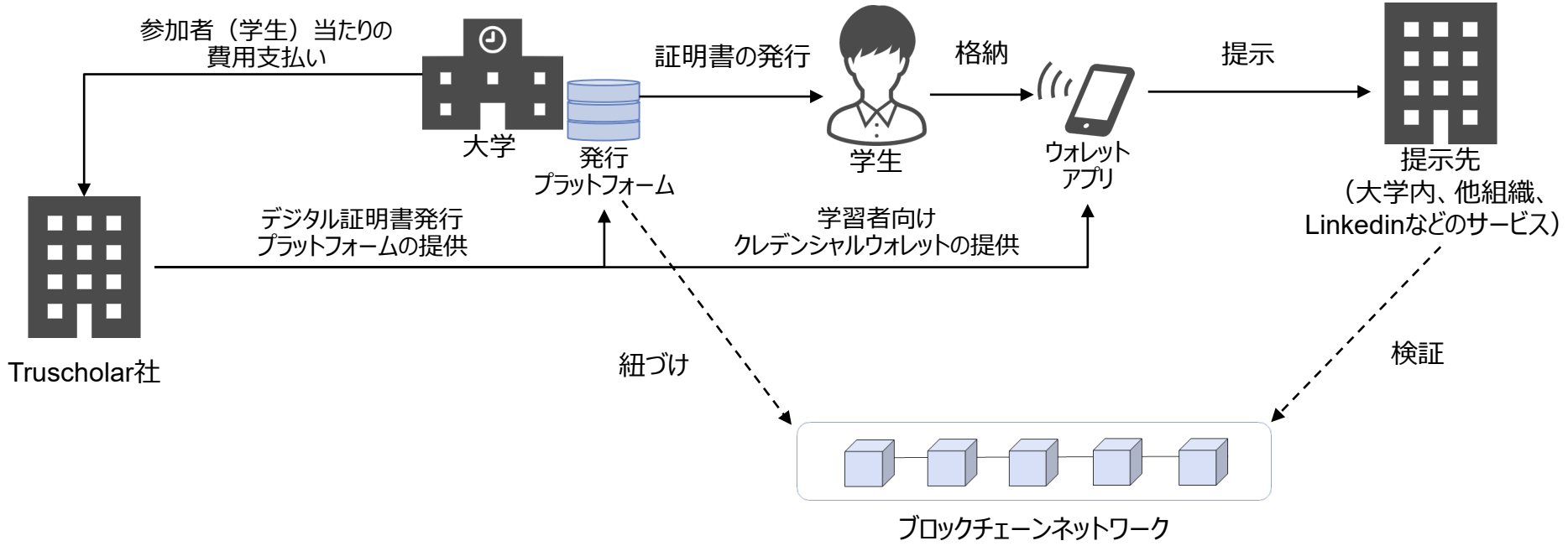
- ブロックチェーン（Hyperledger Fabric、Indy）

扱う属性情報

- 大学在籍証明、保有資格、卒業証明等

ペインポイント	提供する価値
教育機関の名前を悪用した不正な資格情報生成	改竄不可能なデジタル証明書の生成
学術証明書発行に時間を要する	デジタル証明書発行プラットフォームによるプロセスの高速化

ビジネスモデル



出所）
1 https://www.truscholar.io/student-support/

ユースケース：CRUBN

分野：教育、医療、金融

フェーズ：実運用

シンガポール
インド

概要

- インド工科大学カンプール校（IIT）発のSSIソリューション提供を行う団体であるTrentialは、同じくIIT発の非営利団体であるCRUBNとともに、SSIソリューションの提供を行っており、ブロックチェーンを基盤として、検証可能な資格情報の発行ポータル、デジタルIDウォレットの「Indisi Wallet」と、検証サービスを提供する
- ユーザーは資格情報の格納・選択的提示が可能である[1]
- 学術証明書の発行・格納・提示や、医療、金融サービスにおける使用などを想定している[2]

エンティティ

- 費用負担主体：病院・教育機関等資格情報の発行主体
- 価値提供主体： Trential、 CRUBN
- 参加者：資格情報の発行を受けるユーザー

使用されている技術

- ブロックチェーン

扱う属性情報

- 大学在籍証明、医療記録、運転免許証等

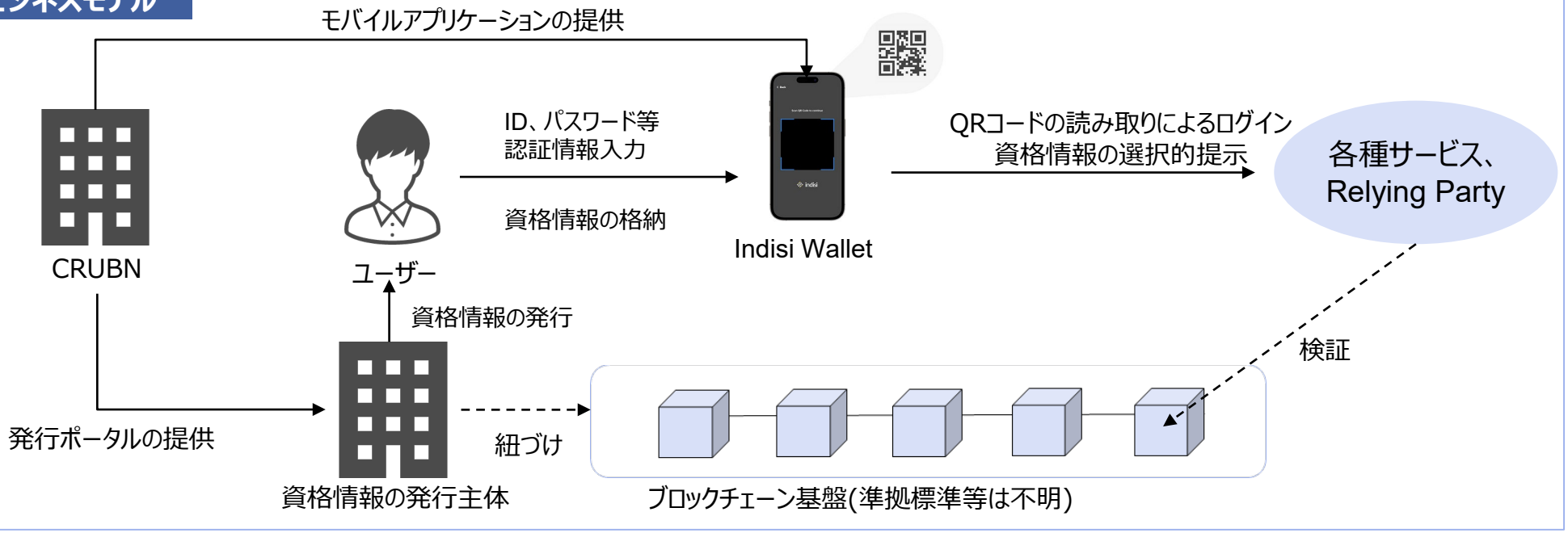
ペインポイント

教育機関の名前を悪用した不正な資格情報生成

提供する価値

改竄不可能なデジタル証明書の生成

ビジネスモデル



出所） 1 https://www.trential.com/digital-credentials
2 https://www.ssi.crubn.com/

3.3 詳細調査結果：自己主権型／分散型アイデンティティに関する取り組み
3.3.5 自己主権型／分散型アイデンティティに関する取り組みに関する総括

自己主権型／分散型アイデンティティに関する政府の取り組み

調査対象国の中で、欧州、北米、オセアニアにおいてはSSI／DIDの実現を支援するために政府による民間開発プログラムへの資金提供、実証環境の提供が行われている。シンガポール、インドでは民間主導の開発プログラムへの資金提供は確認できなかった。例えばシンガポールでは政府機関（GovTech）が既存の共通識別番号に囚われない分散型識別子（Unique ID）の検討を行っている。またインドでは政府機関（UIDAI）がブロックチェーンを活用した分散型ソリューション、選択的開示等の構想について検討をおこなっている。このようにシンガポール、インドでは政府機関自身によるSSI／DIDの考え方を取り入れた検討・技術開発を実施している傾向が見受けられた

	欧州		
	EU	ドイツ	イギリス
政府による取り組み	**ESSIF（2014年～）** EBSIの中のプロジェクトの一つであり、**相互運用可能な自己主権型IDフレームワークを実装し、必要な仕様を定義し、市民が単一の中央集権的な仕組みに依存することなく、独自のデジタルIDを作成、制御、および使用**できるようにすることを目指している ESSIFの中でSSI eIDAS bridgeというコンポーネントが開発されており、SSI eIDAS bridgeはブロックチェーンによって、issuerによるVCの発行、電子署名（シール）、verifierによるVCの検証の橋渡しをする機能であり、eIDASが規定するトラストサービス等をSSIのエコシステムに組み入れるものである **eSSIF-Lab（2020年～）** SSIを促進するプロジェクトに対し欧州委員会から資金提供を行うプログラムである 大きく**オープンソースのSSIインフラの開発に貢献するプロジェクトと、商用領域でマーケットとSSI技術を統合するプロジェクト**に分かれ、2022年現在で合計62プロジェクトに資金提供している 各プロジェクトは到達段階に応じて15,000～最大106,000ユーロの資金提供を受けることができ、総計5,600,000ユーロの資金提供を行うとしている eSSIF-Labは、資金提供したプロジェクトの成果物は実装の際、EBSI、ESSIFや米国のDHS-SVIP（国土安全保障省シリコンバレーイノベーションプログラム）との相互接続性テストを実行するとしている **EUDIWパイロットプロジェクト（2022年～）** 欧州委員会は2022年2月、**EUDIWの試験運用を行うためにパイロットプロジェクトの募集を行った**。パイロットプロジェクトは2022年10月に発表される予定の共通ツールボックスに基づいた「モバイル運転免許証」「決済」「eHealth」「教育・職業資格」等のテーマに焦点を当てた提案が募集された。基準を超えた提案のために合計46,640,478ユーロの予算が要求されるとしている	**SSIパイロットプロジェクト（2020年～）** **デジタル資格情報の交換と保管の標準を備えた包括的なデジタルIDエコシステムの構築**に向けたSSIパイロットプロジェクトシリーズが開始され、**ホテルのチェックイン手続きのデジタル化のユースケースに着手**している **Secure Digital Identities ショーケース（2020年～）** 連邦経済エネルギー省（BMWi）は、イノベーションコンペティション「Showcase Secure Digital Identities」を開始した。**スマートフォンを使って日常的にサービスプロバイダーや当局に対してデジタル認証を行う、新しいアイデンティティ・エコシステム**の優れたアプローチを公募し、**4つのショーケースプロジェクト（ID-Ideal、SDIKA、ONCE、IDUnion）が選**定された	**FCA 規制サンドボックス（2019年）** FCA（金融サービス庁）が新たな技術やビジネスモデルを促進するために、企業が市場で実証を行う事のできる規制サンドボックス（Regulatory Sandbox）を実施している 規制サンドボックスの中で**デジタルIDに関する実証が行われており、分散型アイデンティティ、SSIに関連した事例も含まれている** **NHS Digital Staff passport（2020年～）** ※ユースケース「医療従事者のオンボーディング効率化」 NHSが医療スタッフの異動等に伴う身分証明・医療証明プロセスの効率化のため、**W3C VC/DID標準に準拠した医療従事者の証明書情報交換サービス**を2020年から展開している。 ベースレジストリとして、Hyperledger Indyをベースとしたsovrin Networkを使用し、ウォレットはEvernymから提供を受けている。

3.3.5 自己主権型／分散型アイデンティティに関する取り組みに関する総括

自己主権型／分散型アイデンティティに関する政府の取り組み

	北米	
	米国	カナダ
政府による取り組み	**イリノイ州とEvernymの提携（2017年～）** イリノイ州政府は、自己主権型IDソリューション提供企業であるEvernymとの提携を発表し、**分散型台帳技術を活用してイリノイ州市民のための自己主権IDを提供する**ことを明らかにした **社会保障番号の代替識別子検討プログラム（2020年）** 2020年に米国のDHS（国土安全保障省）は、社会保障番号の収集と利用を減少させるため、カナダに本拠地を置くSecure Key Technologies社に193,000ドルを資金提供し、社会保障番号の代替識別子を実装する開発プログラムを実施した。 プログラムは、DHSのシリコンバレーイノベーションプログラム（SVIP）の下で実施され、SVIPのディレクターは「**分散型識別子（DID）などのW3C標準に基づくシステムを実装し、個人を特定できる情報を明らかにせず、追跡目的で使用できない、グローバルに一意で無意味であるが解決可能で検証可能な識別子の発行を可能にする**」と述べている **米国各州におけるmDLの導入（2021年～）** 米国ではルイジアナ州、コロラド州、アリゾナ州、カリフォルニア州など複数州で**ISO/IEC18013-5に基づくモバイル運転免許証（mDL）の導入及びテスト**を展開している	**オンタリオ州デジタルID（2017年～）** オンタリオ州政府は、民間企業と連携して州の住民向けのデジタルIDサービスの開発・提供を実施しており、**W3C、DIF、ToIP、OpenID Connectなどに準拠した分散型・自己主権型IDのモデル**を採用している **BCデジタルトラスト（2017年～）** ブリティッシュコロンビア（BC）州政府は、デジタルIDとVCに関するプロジェクトである「BCデジタルトラスト」を行っている **KTDIへの参加（2018年～）** カナダ政府は、世界経済フォーラム（WEF）の主導する、世界旅行における旅行者IDを通じたセキュリティ強化を推進するイニシアチブであるKTDIにパートナーとして参加している **ISEによる資金提供（2019年～2021年）** イノベーション科学経済開発省(ISE)はInnovative Solution Canadaというイノベーター企業への資金提供プログラムを行っており、2019年に「User-Centric Verifiable Digital Credentials」と題し、**個人が保有する、ポータブルかつ安全なデジタル資格情報：自己主権型IDソリューションを募集**した。 フェーズ１で最大150000カナダドル、フェーズ2で最大1000000カナダドルの資金提供を行うとして提案を募集し、フェーズ1で適格とされた提案のみフェーズ2に進んだ。 提案するソリューションの要件として、ユーザー中心でプライバシーが守られている事、**W3CのDID/VC、JSON-LDなどの標準に準拠していること、PCTFその他（限定しない）のガイドラインに準拠していること**などが提示された。 **カナダ政府とATB Ventures 社の実証実験（2022年）** カナダ政府はATB Ventures社と連携し、同社の自己主権型ID管理ソリューションプラットフォームである「Oliu」を活用した実証実験を行った

3.3.5 自己主権型／分散型アイデンティティに関する取り組みに関する総括

自己主権型／分散型アイデンティティに関する政府の取り組み

	オセアニア		アジア	
	オーストラリア	ニュージーランド	シンガポール	インド
政府による取り組み	**NSWデジタルID（2021年～）** ニューサウスウェールズ（NSW）州の行政サービス提供主体であるService NSWは州政府の発行する資格情報をデジタルウォレットで管理することのできるアプリケーションを提供しており、その取り組みの中で**自己主権型／分散型IDに関する議論・計画が実施されている** 2023年2月には、連邦政府と州・準州政府の間で国家のデジタルIDシステムにデジタル資格情報を含めるための契約に合意したことが報じられている	**MATTRワクチンパスの実装（2021年～）** ニュージーランド政府保健省は2021年に、コロナウィルスのデジタルワクチンパスのプロバイダーに、オークランドのIT企業であるMATTRを選定した MATTRは資格情報の生成・検証・管理などの各種デジタルIDサービスを提供する企業であり、DIF、OIDF、W3C、IETF等の主要な国際標準化団体**のDID、VC関連規格をサポート**している	**sgID（2020年～）** GovTechはNDIの実験的な拡張として、プライバシー保護に重点を置いた認証およびデータ共有を可能とするsgIDを開発している sgIDはユーザーが**認証を求められるビジネス・サービスごとに固有識別子（unique identifier）を発行するため、NRICなど単一の個人識別番号に依存せず安全性・自己主権性を高めている**とされる **My Infoの改善（2022年～）** NDI Stackの基盤となるMy Infoについて、NDIのディレクターは「MyInfoはやや中央集権的な、ある程度フェデレーション型のエコシステムだが**W3CのDID、VCなどに基づく分散型モデルを検討している**」旨述べている	**Aadhaar2.0の検討（2021年～）** Aadhaarを所管するUIDAIのCEOは、2022年にインドデジタルサミット2022において、Aadhaarを進化させたAadhaar2.0のビジョンに向け、ブロックチェーンと量子コンピューティングの使用可能性を模索していると発言した。**分散型レベルのソリューションを構築するためにブロックチェーンを活用する**と述べており、量子コンピューティングはレジリエンスあるセキュリティのために活用するとしている。 また、「Partial Authentication（部分的認証）」を検討しているとも発言し、「ある人がその地域に居住していることを確認したい時に、住所自体を確認する必要は無い」としていることから、**ゼロ知識証明に近い選択的開示の構想も検討**していると見られる。

3.3.5 自己主権型／分散型アイデンティティに関する取り組みに関する総括

自己主権型／分散型アイデンティティに関するユースケースの取り組み分野

ユースケースの取り組み分野では、金融、医療、行政などが比較的多く見られ、金融取引における本人確認（KYC）や、秘匿性の高い個人情報（医療情報）の交換などの面とSSI／DIDの親和性が高いことが想定される

国・地域		ユースケース	分野										
			金融	保険	不動産	医療	サプライチェーン	交通	教育	小売	エンタメ	旅行	行政
欧州	EU	DC4EU_教育資格・社会保障データの管理							●				●
		EWC_欧州域内旅行での情報提示								●		●	
		Vector_教育資格・社会保障データの管理							●				●
		POTENTIAL_市民サービスへのアクセス改善	●			●		●					●
		NOBID_国内・国境を越えた電子決済の推進	●										
	ドイツ	SSIパイロットプロジェクト：ホテルチェックインの簡素化										●	
		ID-Ideal：図書館における会員カードの自動登録											●
		ID-Ideal：公共交通等モビリティサービス利用のワンストップ登録						●					
		ID-Ideal：住所変更に係る個人情報の自動再登録											●
		ONCE：運転免許証、自動車登録証等の確認作業への活用						●					●
		ONCE：公共施設の利用促進に向けた活用											●

3.3.5 自己主権型／分散型アイデンティティに関する取り組みに関する総括

自己主権型／分散型アイデンティティに関するユースケースの取り組み分野

ユースケースの取り組み分野では、金融、医療、行政などが比較的多く見られ、金融取引における本人確認（KYC）や、秘匿性の高い個人情報（医療情報）の交換などの面とSSI／DIDの親和性が高いことが想定される

国・地域		ユースケース	分野										
			金融	保険	不動産	医療	サプライチェーン	交通	教育	小売	エンタメ	旅行	行政
欧州	ドイツ	ONCE：地域・自治体の特典サービスの利用促進への活用										●	●
		SDIKA：安全で迅速な骨髄提供				●							
		SDIKA：ビジネスの立ち上げ加速	●										●
		SDIKA：建築業の申請・許可プロセスの加速化											●
		IDunion：教育プログラムにおける記録やその証明の一元管理							●				
		IDunion：2要素認証なしでの安全な支払い								●			
		IDunion：サプライチェーンにおける効率的マスター管理データ					●						
		myEGO		●									
	イギリス	映画館における「年齢証明」の簡易化									●		
		英国金融サービス向けのデジタルIDスキームの構築	●										
		不動産に係るデジタルアイデンティティ活用			●								
		医療従事者のオンボーディング・トレーニングの効率化				●							
		患者の「痛み」管理の効率化				●							

3.3.5 自己主権型／分散型アイデンティティに関する取り組みに関する総括

自己主権型／分散型アイデンティティに関するユースケースの取り組み分野

ユースケースの取り組み分野では、金融、医療、行政などが比較的多く見られ、金融取引における本人確認（KYC）や、秘匿性の高い個人情報（医療情報）の交換などの面とSSI／DIDの親和性が高いことが想定される

国・地域		ユースケース	分野										
			金融	保険	不動産	医療	サプライチェーン	交通	教育	小売	エンタメ	旅行	行政
北米	米国	MOBI						●					
		Evernymの信用組合メンバー認証効率化	●										
		iRespondによる難民IDの提供				●							
	カナダ	Interac verification service	●										
		BCデジタルトラストーOrgBookBC											●
		Nothern Block	●			●	●					●	
		eID-Me	●			●				●			●
オセアニア	オーストラリア	オーストラリア郵便公社、大学、Mastercardの連携							●				
		OCR Labs	●	●	●								
	ニュージーランド	MATTRワクチンパス				●							
アジア	インド	Truscholar							●				
		CRUBN	●			●			●				
合計数			10	2	2	9	2	4	6	3	1	4	11

3.3.5 自己主権型／分散型アイデンティティに関する取り組みに関する総括

自己主権型／分散型アイデンティティに関するユースケースの実装フェーズ

調査したユースケースの9割以上がPoC、実運用の段階に達している事から、自己主権型／分散型アイデンティティに関する取り組みは、要素技術等のコンセプト検討の段階を脱し、試行的な取り組みを含めた実践段階にあることが想定される

国・地域		ユースケース	フェーズ		
			コンセプト	PoC	実運用
欧州	EU	DC4EU_教育資格・社会保障データの管理		●	
		EWC_欧州域内旅行での情報提示		●	
		Vector_教育資格・社会保障データの管理		●	
		POTENTIAL_市民サービスへのアクセス改善		●	
		NOBID_国内・国境を越えた電子決済の推進		●	
	ドイツ	SSIパイロットプロジェクト：ホテルチェックインの簡素化			●
		ID-Ideal：図書館における会員カードの自動登録		●	
		ID-Ideal：公共交通等モビリティサービス利用のワンストップ登録		●	
		ID-Ideal：住所変更に係る個人情報の自動再登録		●	
		ONCE：運転免許証、自動車登録証等の確認作業への活用		●	
		ONCE：公共施設の利用促進に向けた活用		●	

3.3.5 自己主権型／分散型アイデンティティに関する取り組みに関する総括

自己主権型／分散型アイデンティティに関するユースケースの実装フェーズ

調査したユースケースの9割以上がPoC、実運用の段階に達している事から、自己主権型／分散型アイデンティティに関する取り組みは、要素技術等のコンセプト検討の段階を脱し、試行的な取り組みを含めた実践段階にあることが想定される

国・地域		ユースケース	フェーズ		
			コンセプト	PoC	実運用
欧州	ドイツ	ONCE：地域・自治体の特典サービスの利用促進への活用		●	
		SDIKA：安全で迅速な骨髄提供		●	
		SDIKA：ビジネスの立ち上げ加速		●	
		SDIKA：建築業の申請・許可プロセスの加速化		●	
		IDunion：教育プログラムにおける記録やその証明の一元管理		●	
		IDunion：2要素認証なしでの安全な支払い		●	
		IDunion：サプライチェーンにおける効率的マスター管理データ		●	
		myEGO	●		
	イギリス	映画館における「年齢証明」の簡易化			●
		英国金融サービス向けのデジタルIDスキームの構築		●	
		不動産に係るデジタルアイデンティティ活用			●
		医療従事者のオンボーディング・トレーニングの効率化		●	
		患者の「痛み」管理の効率化		●	

3.3.5 自己主権型／分散型アイデンティティに関する取り組みに関する総括

自己主権型／分散型アイデンティティに関するユースケースの実装フェーズ

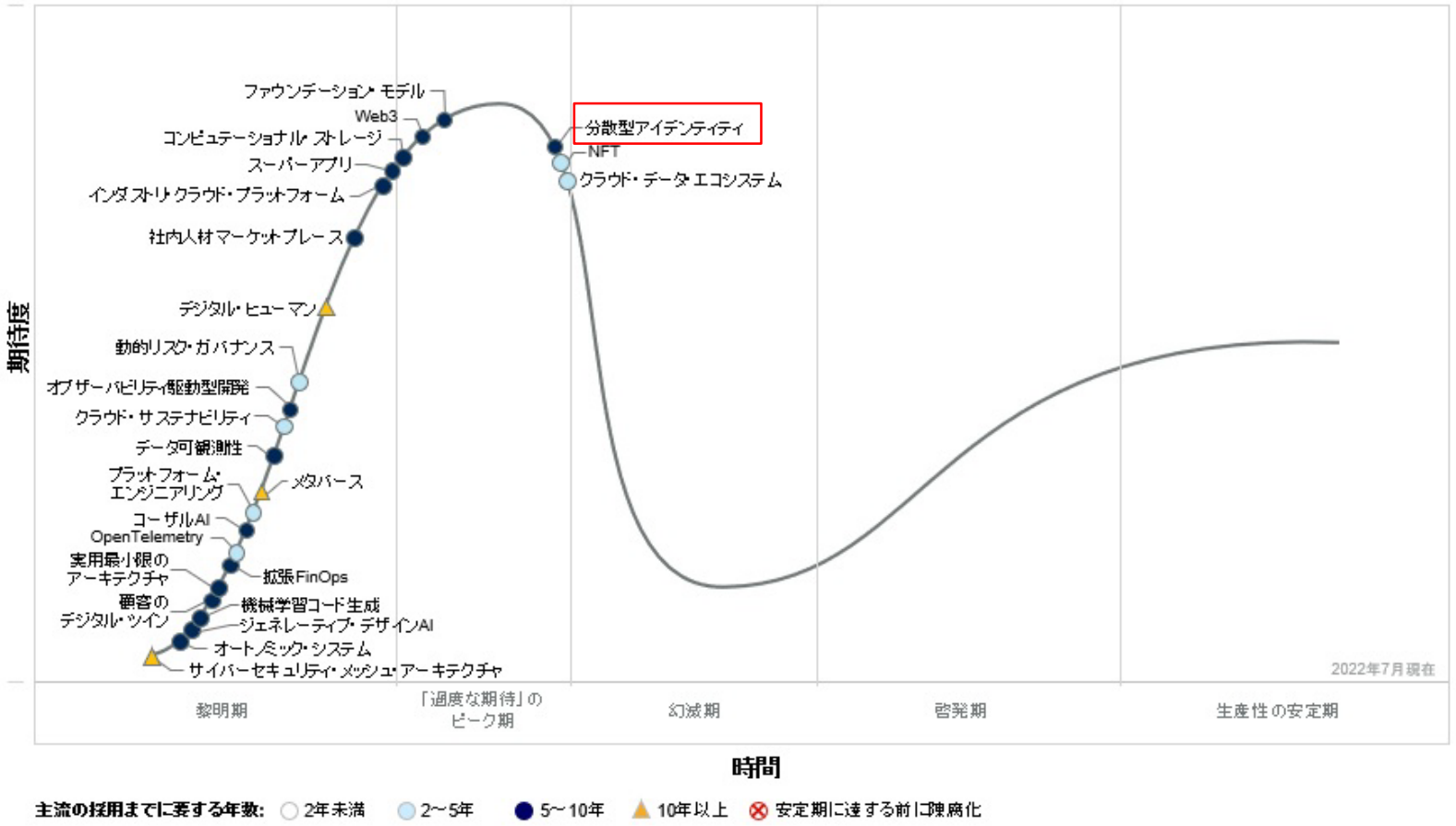
調査したユースケースの9割以上がPoC、実運用の段階に達している事から、自己主権型／分散型アイデンティティに関する取り組みは、要素技術等のコンセプト検討の段階を脱し、試行的な取り組みを含めた実践段階にあることが想定される

国・地域		ユースケース	フェーズ		
			コンセプト	PoC	実運用
北米	米国	MOBI		●	
		Evernymの信用組合メンバー認証効率化			●
		iRespondによる難民IDの提供			●
	カナダ	Interac verification service			●
		BCデジタルトラストーOrgBookBC			●
		Nothern Block			●
		eID-Me			●
オセアニア	オーストラリア	オーストラリア郵便公社、大学、Mastercardの連携		●	
		OCR Labs			●
	ニュージーランド	MATTRワクチンパス			●
アジア	インド	Truscholar			●
		CRUBN			●
合計数			1	22	13

自己主権型／分散型アイデンティティに関するユースケースの実装フェーズ（参考）

ガートナージャパンが2022年7月に発表した「先進テクノロジのハイプ・サイクル：2022年」においては、分散型アイデンティティは「黎明期」を抜け、「幻滅期」に入ろうとしており、実証や社会実装においてプロバイダーのもたらす成果によって普及に繋がるか否かの分岐に差し掛かっている事が伺える[1]

先進テクノロジのハイプ・サイクル：2022年



出所）
1 https://www.gartner.co.jp/ja/newsroom/press-releases/pr-20220816

4. 整理・分析

4.1 調査テーマを総括した各国のデジタルID政策の方向性

4.2 各国の比較・分析

4.3 Trusted Webとの連携可能性、示唆・課題

整理・分析の要領（再掲）

整理・分析にあたっては、調査結果を踏まえて各国のデジタルID政策の方向性を整理し、その中でもTrusted webと共通した課題を解決し得るSSI／DIDに関する取り組み状況が活発的な国・地域について比較を行うさらにSSI/DIDを推進する政策動向について分析することで、Trusted Webとの連携可能性、実現に向けた示唆の抽出を試みる

調査結果の整理・分析イメージ

4.1 調査結果を踏まえた各国のデジタルID政策の方向性の整理	4.2 各国の比較分析	4.3 Trusted Webとの連携可能性、示唆・課題
• 各調査テーマの結果を各国ごとに整理・一般化した上で、国ごとのデジタルID政策の方向性について整理する	• 前段階での整理結果を踏まえ、特にSSI／DIDの取り組みが比較的活発な国・地域について比較を行う • その後共通識別番号・デジタルID・トラストフレームワークの観点からSSI／DIDの取り組みに影響を及ぼしていると思われる事項を分析する	• 前段階で分析したSSI／DIDの取り組みに影響を及ぼしている事項、及びこれまでの調査結果から、Trusted Webとの連携可能性、取り組みに対する示唆・課題を抽出する

4. 整理・分析

4.1 調査テーマを総括した各国のデジタルID政策の方向性

4.2 各国の比較・分析

4.3 Trusted Webとの連携可能性、示唆・課題

EU

	調査結果	結論
共通識別番号 デジタルID	• EU全体としての**統一的な識別番号は存在せず、加盟国に依る** • EU加盟国間で公共オンラインサービスへのアクセス時に当人認証を行うことのできるデジタルIDである**eIDがeIDASによって2014年から規定**されている • **eIDAS改正提案（eIDAS2.0）においてモバイルウォレット（EUDIW）の提供を加盟国に義務付け**、eIDを含めた属性証明・公的文書を格納・利用可能にしている	• 統一的な識別番号を持たない • 相互運用性を持ったデジタルIDを法で規定している
トラスト フレームワーク の策定状況	**Regulation 910/2014：eIDAS（2.0）** • EUの電子商取引に統一した基準を設けるため、**eID、EUDIW及びトラストサービスの法的効力・要件**について規定しており、**OIX*2のTrust Frameworks for Smart Digital IDで参照**されている。 • **EU加盟国に規則（regulation）として直接適用される法的な強制力**があり、**適格なサービスプロバイダをQTSPとして認定**しEU加盟国間でのサービスを認めている。 • 規定内容については、**ステークホルダーの定義・要件が主であるが、コンポーネントとしてEUDIWの提供を義務付け**ている	• 政府主導でトラストフレームワークを策定 • 法的強制力、認定制度あり • トラストサービスにおけるステークホルダー、コンポーネントを規定している
SSI／DID に関する 取り組み・ ユースケース*1	• 政府の取り組みとして**eSSIF-Lab、ESSIFなどの開発プログラムが実施**されている • **SSIの実現を標榜するEUDIWの実装に向けたパイロットプロジェクト**を実施しており、金融・医療・交通・教育・旅行・行政等の多様な分野でPoCを実施している **件数** 5件　**分野** 金融、医療、交通、教育、小売、旅行、行政（7分野）　**フェーズ** コンセプト：0件 PoC：5件 実運用：0件	• SSI／DID実現に向けた政府支援が存在する • 多様な分野でユースケースの取り組まれている（7分野） • 取り組みとしてはPoC段階にある

デジタルID政策の方向性

- EUは国家共同体として統一的な識別番号は持たず、政府（欧州委員会）の下、強制力を持ったトラストフレームワークによってデジタルID及び関連サービス、コンポーネントに加盟国間での一定の相互運用性を担保するとともに、認定制度でその準拠にインセンティブを与えている
- SSIの実現を標榜するEUDIWやESSIF等開発プログラムの実施など、政府としてSSI／DIDの実現に注力している

＊1：EUDIWに関連した取組を抽出

＊2：OIX（Open Identity Exchange）：相互運用可能で信頼できるデジタルIDに関するガイダンスの開発を目的として2010年に米国で設立された非営利団体

ドイツ

	調査結果	結論
共通識別番号 デジタルID	• **行政分野ごとに異なる個人識別番号を用いている**が、2021年4月に公布された登録現代化法に基づき一定の制約の元で**租税識別番号を行政分野横断で活用できる仕組みの整備**が進められている • **eIDカードが2010年から導入されており、16歳以上のドイツ国民に対して取得が義務付けられている**	• 統一的な識別制度を持たない • デジタルIDの運用についてはeIDASに準拠している
トラスト フレームワーク の策定状況	**IDunion Network** • ネットワーク上でのトラストを確立する方法を簡素化・標準化することを目的として、テクノロジーと、ガバナンスを**TCP/IPスタックの構造に着想を得た4層で整理**している • **官民共同で策定され、その準拠は任意であり認定などの仕組みは無い** • ステークホルダー・プロセス・ガバナンスについて規定され、**ブロックチェーンやDLT、DIDs（W3C）の実装を明示している**	• 官民共同プロジェクトの中で策定 • 法的強制力、認定制度なし • ステークホルダー、プロセス、コンポーネントを規定し、特定の技術を指定
SSI／DID に関する 取り組み・ ユースケース	• 政府主導で**SSIパイロットプロジェクト、Secure Digital Identityショーケース**などのプロジェクトを実施しており、**積極的にPoCを実施**している **件数** 14件　**分野** 金融、保険、医療、サプライチェーン、交通、教育、小売、旅行、行政（9分野）　**フェーズ** コンセプト：1件 PoC：12件 実運用：1件	• SSI／DID実現に向けた政府の支援が存在する • 多様な分野でユースケースが取り組まれている（9分野） • 多くの事業はPoC段階にある

デジタルID政策の方向性

- プライバシーへの懸念から統一的な識別制度は持たず、国内で相互運用性あるデジタルID（eIDカード）を運用している
- トラストフレームワークは存在するが、IDunionの中で任意で参照されるものであり、法的な強制力はなく認定制度などの準拠へのインセンティブは設けていない
- SSIの実現を標榜するパイロットプロジェクトにおいてPoCを積極的に実施しており、SSI／DIDの実現に政府として取り組んでいることが伺える

イギリス

	調査結果	結論
共通識別番号デジタルID	• **過去に統一的な国民識別番号が存在した、もしくは検討されたことがあるものの廃止**された。現在は、社会保障、医療といった**目的別に異なる識別番号を使用**している • **民間IdPを行政サービスに活用するGOV.UK Verify**を2016年5月に本格運用開始したが、事業者の離脱が相次ぎ2023年に廃止予定である（OIXのTrust Frameworks for Smart Digital IDで参照されている） • The UK digital identity and attributes trust frameworkを策定し、**デジタルIDを相互運用できるよう、一連のルールを規定**している	• 統一的な識別番号は持たない • 相互運用性を持ったデジタルIDをトラストフレームワーク等によって規定している
トラストフレームワークの策定状況	**The UK digital identity and attributes trust framework** • 英国における個人及び個人に関する情報を証明できるサービスをより簡単かつ安全に使用可能にすることを目的として、デジタルIDおよび/または属性情報を提供する際に遵守すべき一連のルールが規定されている • **政府主導で策定され、その準拠は任意**となっているが、**フレームワークへの参加を希望する組織は認定を受ける必要**がある • **ステークホルダー・プロセスについて規定**し、W3C、OIDFなどの**標準を参照**している	• 政府主導でトラストフレームワークを策定 • 法的強制力なし、認定制度あり • ステークホルダー、プロセスを規定し、特定の技術標準を参照している
SSI／DIDに関する取り組み・ユースケース	• 政府主導で**FCAの規制サンドボックスやNHS Digital Staff passport**などのSSI／DIDに関連した取り組み、実証環境の提供を行っている **件数** 5件　**分野** 金融、不動産、医療、エンタメ（4分野）　**フェーズ** コンセプト：0件 PoC：3件 実運用：2件	• SSI／DID実現に向けた政府の支援が存在する • 金融・医療分野などの分野で取り組まれている • 主にPoC、実運用段階にある

デジタルID政策の方向性

- プライバシーへの懸念から統一的な識別番号は設けず、官民で相互運用性のあるデジタルIDを活用している
- トラストフレームワークに法的な強制力はないが、準拠することで認定を受けられるため、一定のインセンティブ設計が図られている
- 金融・医療などの分野でSSI／DIDに関連した取り組みを政府として実施している

米国

	調査結果	結論
共通識別番号デジタルID	• 従来から存在する**社会保障番号（SSN）が広範に個人認証に利用され、行政・民間サービスの双方で利用範囲が拡大**された。プライバシー等への懸念から**社会保障番号に代わる統一的な共通識別番号を模索**しているものの、未だ実現してはいない • NSTIC、IDIA法案及びNISTの標準などで**、政府としてのデジタルID利活用の方針を示し、エコシステムの形成・インフラ整備**を図っている	• 実質的な統一的識別番号（SSN）を活用しているが、プライバシー等の懸念から改善を実施 • 各種政策法規によって政府としてのデジタルID利活用の方針を示し、民間企業と協働している
トラストフレームワークの策定状況	**Identity Ecosystem Framework ：IDEF** • 米国政府の推進するIdentity Echosystemを構築するために、その参加主体の役割と必要なアクション、プライバシー・セキュリティ等の要件を定義している **NIST SP 800-63-3、SP 800-63-4** • デジタルIDサービスを活用する政府機関向けのガイドラインであるが民間でも任意で参照されており、特にデジタル認証で使用する登録・検証のプロセスに焦点を当てている	• 政府主導でトラストフレームワークを策定 • 法的強制力、認定制度なし • ステークホルダー、プロセス、コンポーネントを規定し、特定の技術標準を参照している
SSI／DIDに関する取り組み・ユースケース	• 社会保障番号に代わる**分散型の識別子（DID等）を実装する開発プログラム**への支援や、**各州における自己主権IDの実装、mDLの導入**などSSI／DIDに係る取り組みが連邦政府・州政府の主導で実施されている **件数** 3件　**分野** 交通、金融、医療（3分野）　**フェーズ** コンセプト：0件 PoC：1件 実運用：2件	• SSI／DID実現に向けた政府（連邦・各州）の支援が存在する • ユースケースはPoC、実運用段階にある

デジタルID政策の方向性

- 実質的な統一的識別制度としてSSNが活用されているものの、プライバシー・情報流出への懸念から改善を図っている
- NSTIC、IDIA等の法律及びNISTの標準で政府としてのデジタルID利活用方針を示すことで、民間企業にも参照可能となっている
- SSI／DIDに関連する支援・取り組みを連邦政府・各州政府双方で実施している

カナダ

	調査結果	結論
共通識別番号デジタルID	• **目的別の識別番号を使用**しており、統一的な国民IDカードを発行する制度が一時期検討されたものの、プライバシー等の懸念から実現していない • 政府・民間企業から構成される非営利組織であるDIACC主導で、**カナダの官民組織がデジタルアイデンティティを安全に活用するためのガバナンスモデルとしてPCTF（Pan-Canadian Trust Framework）を策定**している	• 統一的な識別番号は検討されたものの実現せず、目的別の識別番号を使用している • 相互運用性を持ったデジタルIDをトラストフレームワークによって規定している
トラストフレームワークの策定状況	**Pan-Canadian Trust Framework：PCTF** • **官民共同の非営利組織DIACCによって策定**され、カナダの**デジタルアイデンティティ管理におけるステークホルダー、デジタルIDの作成、管理、提供に係る一連のプロセス**などを定義しているほか、**ウォレットやインフラなどのコンポーネントも定義**している • **法的強制力は無く、任意で参照**されているが、**Voilà Verified 認定プログラム**によってその準拠にインセンティブを設けている • **OIXのTrust Frameworks for Smart Digital IDで参照**されている。	• 官民共同でトラストフレームワークの策定を進めている • 法的強制力なし、認定制度あり • ステークホルダー、プロセス、コンポーネントを規定しているが、特定の技術の参照・指定は無い
SSI／DIDに関する取り組み・ユースケース	• **ISEによる資金提供プログラムやATB Ventures社との実証実験、KTDIへの参加**など、SSI／DIDに関する取り組みは連邦政府として積極的に実施されている他、**オンタリオ州、BC州など州政府単位でも実施**されている **件数** 4件　**分野** 金融、医療、サプライチェーン、交通、旅行、行政（6/11分野）　**フェーズ** コンセプト：0件 PoC：1件 実運用：3件	• SSI／DIDに関連した取り組み・支援が連邦政府・各州政府の主導で実施されている • ユースケースは実運用の段階にある

デジタルID政策の方向性

- 目的別の識別番号を使用し、官民共同で相互運用性をもったデジタルIDをトラストフレームワークを規定している
- SSI／DIDに関連する支援・取り組みを連邦政府・各州政府双方で実施している

オーストラリア

	調査結果	結論
共通識別番号 デジタルID	• 過去に国民IDカードの実現を目指した提案があったがいずれも批判を受けて失敗し、Health Care identifierやTax File Numberなど用途に応じて複数の識別番号を使い分けている • 政府のオンラインサービスにアクセスする際に安全な認証を行うための取り組みとしてデジタルIDシステムを推進しており、それを支えるトラストフレームワークとしてTDIFを策定している	• 統一的な識別番号は検討されたものの実現せず、目的別の識別番号を使用している • 相互運用性を持ったデジタルIDをトラストフレームワークによって規定している
トラスト フレームワーク の策定状況	**Trusted Digital Identity Framework : TDIF** • オーストラリア政府が推進する「デジタルIDシステム」内のプロバイダーとサービスに対する厳格な規則と標準を規定している **Trust ID Framework** • オーストラリアの民間企業が提供するデジタルIDソリューションの信頼性、相互運用性を高めるために、組織が製品やサービスの設計と構築において遵守するための一連のルールとガイドラインを規定している	• 政府主導、民間主導双方のフレームワークが存在 • 法的強制力なし、認定制度あり • TDIFはステークホルダー、プロセスを規定し、特定の技術を参照している（Trusted ID Frameworkは詳細不明）
SSI／DID に関する 取り組み・ ユースケース	• NSW州におけるデジタルIDの取り組みの中で、自己主権型／分散型IDに関する議論・計画が実施されている **件数** 2件　**分野** 教育、金融、保険、不動産（4分野）　**フェーズ** コンセプト：0件 PoC：1件 実運用：1件	• 州政府による取り組みの中でSSI／DIDに関する議論が行われているほか、民間企業においてPoC、サービスが事例として存在する

デジタルID政策の方向性

- 統一的な識別番号は検討されたものの実現せず、目的別の識別番号を使用している
- 政府の主導するデジタルIDシステムのためのフレームワークであるTDIFと、民間主導で政府とのデジタルIDに相互運用性を持たせる取り組みが並行して行われている
- 州政府のデジタルIDに関連した取り組みの中でSSI／DIDと思われる議論が行われているほか、民間企業でのSSI／DIDに関するPoC、サービス事例が見られる

ニュージーランド

	調査結果	結論
共通識別番号 デジタルID	• IRD番号、NHI番号、NSNなど識別番号が複数存在しており、それぞれ**税務、医療、教育といった目的別に使用**されている • **Digital Identity Trust Frameworkによって、デジタルIDサービスの法的な枠組みを規定**しているほか、デジタルIDサービスにおける各ステークホルダーを示したエコシステムとしてデジタルIDシステムを提案している	• 目的別の識別番号を使用している • デジタルIDの法的な枠組みについて法律で規定している
トラスト フレームワーク の策定状況	**Digital Identity Trust Framework** • ニュージーランドにおける**個人・組織間取引に対するデジタルIDサービスの法的な枠組み**を規定しており、認定を受けた**信頼できるデジタルIDサービス事業者を「TFプロバイダー」として定義・登録**するなどの仕組みを定めている **Identity management standards** • 内務省の策定した、ニュージーランドにおける**アイデンティティ管理の標準であり、各保証レベルとそれを決定する識別リスクアセスメントにより構成**されている	• 政府主導でトラストフレームワークを策定している • 法的強制力なし、Trust ID frameworkには認定制度あり • Trust ID Frameworkはステークホルダーを規定している
SSI／DID に関する 取り組み・ ユースケース	• ニュージーランド政府保健省は2021年に、コロナウィルスのデジタルワクチンパスのプロバイダーに、オークランドのIT企業であるMATTRを選定した • MATTRワクチンパスはDIF、OIDF、W3C、IETF等の主要な国際標準化団体の**DID、VC関連規格をサポート**している **件数** 1件　**分野** 医療（1分野）　**フェーズ** コンセプト：0件 PoC：0件 **実運用：1件**	• 現時点で確認できたユースケースは1件のみであった • 政府の取り組みとして、デジタルワクチンパスに分散型IDを採用している

デジタルID政策の方向性

- 目的別の識別制度を使用し、デジタルIDについてはその法的な枠組みを規定しているほか、政府主導でアイデンティティ管理の標準を策定している
- SSI／DIDに関連する支援・取り組みとしては、政府によるデジタルワクチンパスへの分散型IDの選定が挙げられる

シンガポール

	調査結果	結論
共通識別番号デジタルID	• 1965年の国家登録法成立以降、**一意の識別番号が国民に対し付番**されている • **国民識別番号を利用した認証システムであるSingpassが2003年より導入**され、その後2018年にモバイルアプリであるSingpass Mobileが提供され行政・民間の両分野でのデジタル本人認証に幅広く活用されている	• 統一的な識別子を使用し、それを基盤としたデジタルIDサービスを政府が提供している
トラストフレームワークの策定状況	**NDI Stack** • **デジタルID活用に係る国の指針を概念化**したものであり、Singpass, My Infoの活用、APIによる接続が前提となっている • 法的強制力や認定制度は無く、**政府主導の領域（Singpass、My Info）と民間事業者と協働するサービス・アプリケーション領域の体制**が示されている	• 国としての指針を概念化しており、詳細な要件等は規定されておらず、強制力・認定制度も存在しない
SSI／DIDに関する取り組み・ユースケース	• sgIDの開発やMyInfoの改善などにおいて、単一の識別番号への依存を弱める、分散型モデルを検討するなどしている **件数** 0件　**分野** －　**フェーズ** コンセプト：0件 PoC：0件 実運用：0件	• 既存の政府提供のデジタルIDサービスの改善を図る中でSSI／DIDに関連したアプローチが見られる

デジタルID政策の方向性

- 統一的な識別制度を使用し、それを基盤としたデジタルIDサービスを政府主導で提供している
- フレームワークや法律によって細部の枠組みや要件を定めることは無く、デジタルID活用に係る国の指針をレイヤー構造で概念化するにとどまっている
- 既存の政府提供のデジタルIDサービスの改善を図る中でSSI／DIDに関連したアプローチを行っている

インド

	調査結果	結論
共通識別番号デジタルID	• 2010年から顔写真、指紋、虹彩及び氏名住所などの登録と**12桁のID番号（Aadhaar番号）を付与**し、国民ID基盤であるAadhaarを構築している • Aadhaarを基盤として、行政機関や民間企業のシステムに**Aadhaarを接続するためのオープンAPI群を含めた国民ID基盤であるIndia Stackが広範に活用**されている	• 統一的な識別子を使用し、それを基盤としたデジタルIDサービスを政府が提供している
トラストフレームワークの策定状況	**India Stack** • **デジタルID活用に係る国の指針を概念化したものであり、Aadhaarの活用、APIによる接続が前提**となっている • 法的強制力や認定制度は無く、**Aadhaarを基盤として、APIで民間事業者・行政サービスと接続することで国民の金融包摂を図る**ことが示されている • Aadhaarは**OIXのTrust Frameworks for Smart Digital IDで参照**されている。	• 国としての指針を概念化しており、詳細な要件等は規定されておらず、強制力・認定制度も存在しない
SSI／DIDに関する取り組み・ユースケース	• Aadhaarの改善（Aadhaar2.0）において、**分散型レベルのソリューションを構築するためのブロックチェーンの活用、ゼロ知識証明による選択的開示の検討**を行うとしている **件数** 2件　**分野** 金融、医療、教育（3/分野）　**フェーズ** コンセプト：0件 PoC：0件 実運用：2件	• 既存の政府提供のデジタルIDサービスの改善を図る中でSSI／DIDに関連したアプローチが見られる

デジタルID政策の方向性

- 統一的な識別制度を使用し、それを基盤としたデジタルIDサービスを政府主導で提供している
- フレームワークや法律によって細部の枠組みや要件を定めることは無く、デジタルID活用に係る国の指針をレイヤー構造で概念化するにとどまっている
- 既存の政府提供のデジタルIDサービスの改善を図る中でSSI／DIDに関連したアプローチを行っている

整理・分析

4.1 調査テーマを総括した各国のデジタルID政策の方向性

4.2 各国の比較・分析

4.3 Trusted Webとの連携可能性、示唆・課題

SSI／DIDの取り組み状況が比較的活発な国・地域の分析

SSI／DIDの取り組み状況では、欧州・北米、特にEU・ドイツにおいてSSI／DIDを標榜する政府の取り組み、開発プログラムに対する資金提供等が行われており、確認できたユースケースも多いことから、Trusted Webに対する示唆の抽出にあたっては欧州・北米地域の方向性を分析対象とすることとした

国・地域		政府におけるSSI/DIDに関連した動き		ユースケース件数	主なフェーズ
欧州	EU	• 政府の取り組みとして**eSSIF-Lab、ESSIFなどの開発プログラムが実施**されている • **SSIの実現を標榜するEUDIWの実装に向けたパイロットプロジェクト**を実施しており、金融・医療・交通・教育・旅行・行政等の多様な分野でPoCを実施している	政府による取り組み、開発プログラムへの資金提供が実施されている	10	PoC、実運用
	ドイツ	• 政府主導で**SSIパイロットプロジェクト、Secure Digital Identityショーケース**などのプロジェクトを実施しており、**積極的にPoCを実施**している		14	PoC
	イギリス	• 政府主導で**FCAの規制サンドボックスやNHS Digital Staff passport**などのSSI／DIDに関連した取り組み、実証環境の提供を行っている		5	PoC、実運用
北米	米国	• 社会保障番号に代わる**分散型の識別子（DID等）を実装する開発プログラム**への支援や、**各州における自己主権IDの実装、mDLの導入**などSSI／DIDに係る取り組みが連邦政府・州政府の主導で実施されている		3	PoC、実運用
	カナダ	• **ISEによる資金提供プログラムやATB Ventures社との実証実験、KTDIへの参加**など、SSI／DIDに関する取り組みは連邦政府として積極的に実施されている他、**オンタリオ州、BC州など州政府単位でも実施**されている		4	実運用
オセアニア	オーストラリア	• NSW州政府のデジタルIDの取り組みの中で、SSI／DIDに関する言及が見られる	政府による取り組みの中にSSI／DIDに関する言及が見られる	2	PoC、実運用
	ニュージーランド	• ニュージーランド政府保健省は2021年に、コロナウィルスのデジタルワクチンパスのプロバイダーに、オークランドのIT企業であるMATTRを選定した • MATTRワクチンパスはDIF、OIDF、W3C、IETF等の主要な国際標準化団体の**DID、VC関連規格をサポート**している		1	実運用
アジア	シンガポール	• sgIDの開発やMyInfoの改善などにおいて、単一の識別番号への依存を弱める、分散型モデルを検討するなどしている		0	–
	インド	• Aadhaarの改善において、**分散型レベルのソリューションを構築するためのブロックチェーンの活用、ゼロ知識証明による選択的開示の検討**を行うとしている		2	実運用

凡例

SSI／DIDの取り組みに影響を及ぼしていると思われる要素の分析-欧州・北米の方向性

- 欧州・北米ではプライバシーの侵害・情報流出への懸念から統一的な共通識別番号を持たず目的別に異なる識別番号を採用してきた。そのためシンガポールやインドのように共通識別番号をデジタルIDには活用せず、独立した検討が進められている。また、相互運用可能なデジタルIDを法律・フレームワークによって定義し、政府機関や民間企業がそれを参照する形での検討が進められている。そして相互運用可能なデジタルIDとして、ID情報の管理主体とは異なるプロバイダによって提供されるウォレットをもって個人データを管理できるような取り組みが存在することから、結果として特定のID管理者の介在が少なくなりSSI／DIDに関連した取り組みの素地を形成したと想定される
- トラストフレームワークではSSI／DIDの実装手法を含めた具体的な技術・コンポーネント等に言及している点が特徴的であり、その実装を促進していると想定される

調査テーマ	SSI／DIDの取り組みに影響を及ぼしていると思われる要素
共通識別番号	• 共通識別番号については、プライバシーの侵害・情報流出への懸念等から統一的な共通識別番号は使用されなかった、もしくは過去に採用・検討されたものの廃止され、目的別に異なる識別制度を使用する状況が共通している • 「ユーザー本人がID情報を管理する／特定のID管理者への依存度を下げる」というSSI／DIDの原則に対して、統一的な共通識別番号がもたらす政府によるID情報の一元管理という方向性は相反するものであるため、欧州・北米でSSI／DIDの導入が進んだ一つの要因と想定される
デジタルID	• デジタルIDについては、各国のデジタルID利活用のビジョンやエコシステムを法律・フレームワークの形で具体化・要件を規定し、政府機関や民間企業に参照されることによってデジタルIDの相互運用性を担保している点が共通している • これはシンガポール・インドにおいて統一的な共通識別子を基盤とした広範なデジタルIDサービスを政府が提供している例とは対照的に、上記の通り目的別の識別制度を使用している欧州・北米では結果的にそのような形をとる事になったと想定され、特定のID管理者への依存度を下げることにも貢献していると思われる
トラストフレームワーク	• トラストフレームワークについては政府主導もしくは官民共同で策定され、EUを除いて法的な強制力は持たず、認定制度を有するものとそうでないものは半数づつとなっている • 規定している内容については、ステークホルダー、プロセス、コンポーネントについて規定するか、特定の技術を参照・指定する網羅的／システム寄りのフレームワークとなっており、特にEU、ドイツ、イギリス、米国ではSSI／DIDの実装手法と通ずるW3C VCs／DIDsの参照や、EUDIWの提供を義務化している点が特徴的であり、SSI／DIDの実装を促進

整理・分析

4.1 調査テーマを総括した各国のデジタルID政策の方向性

4.2 各国の比較・分析

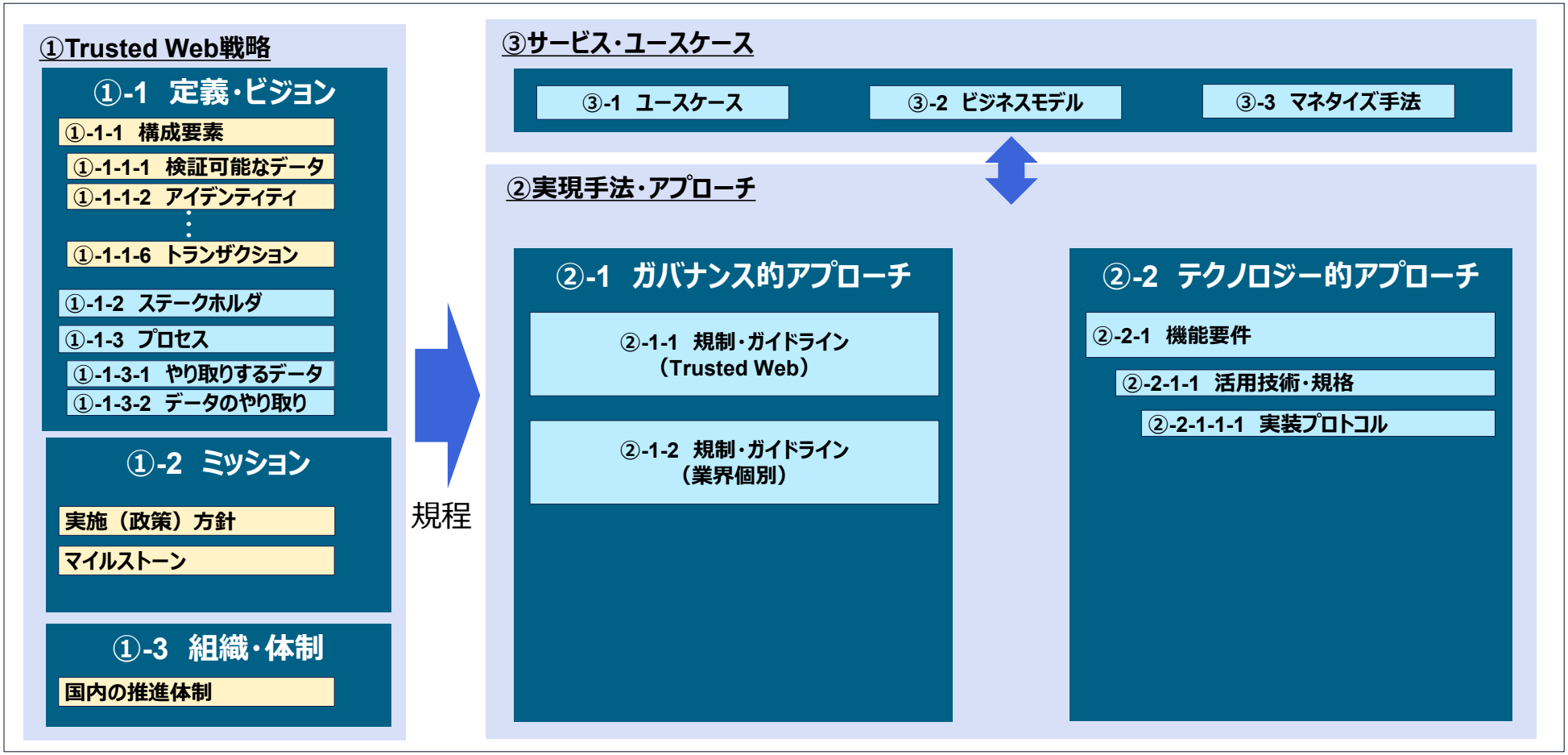
4.3 Trusted Webとの連携可能性、示唆・課題

Trusted Webとの連携可能性、示唆抽出の方針

示唆の抽出・整理にあたっては、Trusted Webの取り組みの構造を意識し、Trusted Webホワイトペーパーの骨子を参考にすることとして戦略・実現手法・アプローチ、サービス・ユースケース、外部との連携といった論点から分析を行うこととした

Trusted Web（WP）の全体像

規程　例示



Trusted Webとの連携可能性、示唆・課題

各国のデジタルID政策の方向性がSSI／DIDの取り組みに及ぼしている影響、及び個別の調査テーマの取り組み状況からTrusted Webの各論点について以下のような連携可能性、示唆・課題が得られた

論点① 戦略：Trusted Webを今後進めていくうえでのビジョン・推進体制

- 欧州・北米ではプライバシーの侵害・情報流出への懸念から統一的な識別番号を持たず、目的別に異なる識別番号を採用してきた。そのため共通識別番号をデジタルIDには活用せず、独立した検討が進められてきた。また相互運用可能なデジタルIDを法律・フレームワークの形で定義して政府機関や民間企業がそれを参照する形となった
  相互運用可能なデジタルIDとして、ID情報の管理主体とは異なるプロバイダによって提供されるウォレットをもって個人データを管理できるような取り組みが存在することから、結果として特定のID管理者の介在が少なくなりSSI／DIDに関連した取り組みの素地を形成したと想定される

- Trusted Webにおいても、課題の解決にはデータのコントロールに関する仕組みを前提としており、SSI／DIDは手法として有力と考えられる。EUDIWの提供やmDLの導入等SSI／DIDを推進する欧州・北米の取り組みはTrusted Webのユースケースとしても流用可能であり、今後ユースケースの規模を拡大し国際的なデータ連携を視野に入れる場合は当該国との連携等が考えられる

- 国境を跨いだID情報のコントロールを行う活動への参加・ユースケースの創出などはTrusted Webが国際的なデータ連携を視野に普及を進めるにあたって方向性の一つとして考えられる
  国際的データ連携のユースケース例としては、EUにおけるEU加盟国間でのEUDIW等SSIソリューションの運用実証や、デジタルワクチンパスの実装、オーストラリア政府のKTDIへの参加など、国境を跨いだ個人に主権あるID情報コントロールなどが一案として考えられる

Trusted Webとの連携可能性、示唆・課題

各国のデジタルID政策の方向性がSSI／DIDの取り組みに及ぼしている影響、及び個別の調査テーマの取り組み状況からTrusted Webの各論点について以下のような連携可能性、示唆・課題が得られた

論点② 実現手法：Trusted Webを実現するためのガバナンス・テクノロジー面のアプローチ

- 欧州・北米のトラストフレームワークにおいては、ステークホルダー、プロセス、コンポーネントの要件を規定しており、中でもカナダのISE資金提供プログラムでは、PCTFその他のガイドラインへの準拠を、応募の必須条件としている
  Trusted Webにおいても、ガバナンス面からエコシステムの参加主体（ステークホルダー）、プロセス（登録、認証、フェデレーション）、核となるコンポーネント（ウォレット等）について具体的に要件を規定する、もしくは実装で参考となる外部の標準を参照することにより開発実証・社会実装を促進し得ると思われる

- 欧米・北米のトラストフレームワークにおいては、5ヶ国中2ヶ国が政府・官民共同機関による認定制度、1ヶ国が民間企業による認定制度、１ヶ国が自己評価による登録制度を設け、その準拠に対してインセンティブを設けている（例：政府機関の認定したフレームワークに準拠することに依るトラストサービスに対する信頼性の確保、公共調達における応募資格としての活用）。Trusted Webにおいてもその仕様等に準拠していることを示す認定制度を導入することは、準拠へのお墨付きを（政府主導の）認定という形で得られることで、Trusted Webの考え方に共感する機関にとって活動参加へのインセンティブとなり得る

- 欧州・北米の取り組みにおいては、SSI／DIDの実装手法であるW3C VCs／DIDsなどの特定の技術の参照やウォレットのアーキテクチャなどを規定している。Trusted Webは前提として技術中立であるものの、テクノロジー面では特定の技術標準を参照・指定した事例を参考として紹介することによって、外部からの理解を促進し得ると思われる

Trusted Webとの連携可能性、示唆・課題

各国のデジタルID政策の方向性がSSI／DIDの取り組みに及ぼしている影響、及び個別の調査テーマの取り組み状況からTrusted Webの各論点について以下のような連携可能性、示唆・課題が得られた

論点③ サービス領域・ユースケース：親和性の高いサービス領域・ユースケースモデル等

- EUのEUDIWのパイロットプロジェクトにおいては、mDL、決済、ehealth、教育・専門資格といった試験的実装の優先分野を定めている。Trusted Webにおいても、実証事業等によるユースケース開発にあたっては、そのビジョン・ミッションとの親和性の高い分野に焦点を絞った開発を行うことによって、リソースの節用を図り費用対効果を向上させることができると思われる
  本調査ではSSI／DIDのユースケース分野としては金融、医療、行政などが比較的多く見られ、以下のような理由からSSI／DIDとの親和性が高いものと想定される
  - ✓ 金融分野においては、口座登録・金融取引における本人確認（KYC）が重視されており、コストを要している。そのため、特定のIdPを介在せずユーザーがID情報を提示・検証できるSSI／DIDの特性と親和性があると想定される
  - ✓ 医療分野においては健康情報など秘匿性の高い個人情報が扱われることが多く、プライバシーなどの面から、ユーザーによる主体的なID情報管理を可能にするSSI／DIDとの親和性があると想定される

- ドイツのSSIショーケースプロジェクトにおいては、各プロジェクトでパートナー都市・大学・企業等を定めて連携し、またカナダのオンタリオ州・BC州などで州政府単位のSSI／DID実装が見られる他、米国もmDLの試験導入を各州政府が行っている
  Trusted Webにおいてもユースケース開発の実効性を高めるためにはTrusted Webの解決する課題を明確化する必要がある。そのため例えば地域課題の解決という共通目的のために地方自治体及びその地方の教育機関・企業と連携したプロジェクトを実施することにより、実効性ある個別のユースケースの創出につながると思われることからユースケース検討単位の一つとして地方自治体が考えられる

Trusted Webとの連携可能性、示唆・課題

各国のデジタルID政策の方向性がSSI／DIDの取り組みに及ぼしている影響、及び個別の調査テーマの取り組み状況からTrusted Webの各論点について以下のような連携可能性、示唆・課題が得られた

論点④　外部との連携：今後Trusted Webと連携が期待される外部のシステム・団体等

- Trusted Webホワイトペーパーやユースケース調査結果のとおり、ブロックチェーンは自己主権・分散型アイデンティティ管理の実装・ユースケース開発において、検証可能なレジストリとしての役割を果たす可能性がある。実際、EUにおいてはEBSIのブロックチェーン基盤を検証可能なレジストリとして活用したEUDIWパイロットプロジェクトが行われている
  Trusted Webの実装・ユースケース開発においては、基盤となる可能性のあるインフラとして、技術中立的な立場は崩さずブロックチェーンの推進を行う団体等（例：BGIN）と連携することによりユースケース検討を深化させることができると思われる。連携方法の例としては、Trusted Webにおいて産業分野別のガバナンスが論点として議論されていることから、BGIN等団体の実施する分散型金融のガバナンスに関する議論において、Trusted Webのユースケース開発実証と連携した検討を行うことなどが考えられる
  他方、ブロックチェーンは暗号技術によってデータの改ざんを困難にするという特性上、検証可能な領域を拡大し得る反面運用コストが高額であるため、ブロックチェーンを実装・ユースケース開発に利用する場合はその必要性を明確にするとともに、サービサー・有識者を交え総合的に判断しコストの低減に取り組むべきである

- イギリスではFCAの行う金融市場での実証環境構築支援にデジタルIDに関する実証が行われており、分散型アイデンティティ、SSIに関連した事例が含まれている。
  Trusted Webにおいても産業分野別のガバナンスが論点として議論されている中、各産業分野で新しい技術やビジネスモデルを用いた事業活動を促進する他の取り組み（例：金融庁　規制のサンドボックス）に参加、連携することによって、産業分野別のガバナンス・導入にあたっての課題検討の深化や、多様なステークホルダーの巻き込みによってTrusted Webの普及を図ることができると思われる

NTT DATA

Trusted Global Innovator