ブロックチェーン技術等を用いた
デジタルアイデンティティの活用に関する研究

報告書

補足資料

【公表版】

令和３年３月

株式会社野村総合研究所

目次

第1章 アイデンティティに関わる技術及び運用の基礎

本章では、アイデンティティに関わる技術及び運用の基礎について整理する。現在新たなアイデンティティの思想/仕組みとして注目を集めている自己主権型アイデンティティ(Self-Sovereign Identity: SSI)及び分散型アイデンティティ(Decentralized Identity: DID)について理解するためには、従来のアイデンティティ管理モデルを理解することが必要となる。したがって、初めにアイデンティティの考え方について紹介した上で、従来主流となっているアイデンティティ管理の考え方について整理する。その上で、従来のアイデンティティモデルのリスクや課題について触れたうえで、その懸念に対応するモデルとしてのSSI/DID の考え方について概観する。

本章では以下の構成で検討を行う。1-1 では、アイデンティティやデジタルアイデンティティ、アイデンティティ管理の概念について整理する。その上で、アイデンティティ管理がどのように行われているのかについて、アイデンティティ管理の国際標準である ISO/IEC 24760 シリーズに基づいて整理する。次に、1-2 では、現在の主要なアイデンティティ管理モデルである Centralized（集中型）モデルや、フェデレーションモデルについて紹介した上で、これらモデルを支える主要な技術要素であるプロビジョニング管理、認証、認可、アイデンティティ連携について説明する。また、ガバナンス要素としての、ガバナンスフレームワークについても触れる。最後に 1-3 では、既存の集中型モデルやフェデレーションモデルにおける課題に対応する思想/仕組みとして注目されている SSI/DID の考え方について概観する。

1-1. デジタルアイデンティティとアイデンティティマネジメントシステム(IMS)

1-1-1. アイデンティティ/デジタルアイデンティティとは

アイデンティティに関わる用語や整理については、様々な組織・団体が規格やガイドライン等を作成・公表しているが、対象となっているスコープも異なり、また用語自体の定義も統一されていない。例えば、「デジタルアイデンティティ」の定義についても、国際的に統一された定義は存在せず[1]、各組織・団体が独自の定義付を行っているのが現状である。したがって、本調査において用いるアイデンティティに関連する用語について、その定義を最初に明確化しておくことは重要である。

本調査では、アイデンティティに関わる技術や運用に関して、概観を把握し観点を網羅的に整理するにあたり、「ISO/IEC 24760: IT Security and Privacy —A framework for identity management—」（以下、ISO/IEC 24760 シリーズ）に基づき、アイデンティティに関わる用語や仕組みに関する整理を行う。ISO/IEC 24760 シリーズは、情報システム管理を実現

[1] NIST SP 800-63-3 Digital Identity Guidelines, p. iv.

することを目的とした、アイデンティティ管理の概念と運用構造を規定した標準フレームワークとして広く参照されており、アイデンティティに関するグローバルの共通理解として位置づけられている。したがって、本調査においては、本規格で定義されている用語を用いる場合には、本規格における定義に従うこととする。

ISO/IEC 24760 シリーズでは、アイデンティティを「ある実体（エンティティ）に関連する属性（アトリビュート）の集合」と定義する。例えば、エンティティが人の場合、属性には以下のような情報が含まれる。

- ID/パスワード
- 基本的属性（氏名、性別、年齢、生年月日等）
- 利用履歴（購買履歴、位置情報、診療履歴等）
- 関係性/評判（信用情報、友達リスト等）

このような情報からも明らかな通り、アイデンティティはエンティティの社会活動（サービス利用や他者との関係構築）とともに成長していくものであり、このように変化・成長するアイデンティティのライフサイクル（ライフサイクルの詳細は 1-1-3.(3)にて詳述）を管理していくことが重要となる。アイデンティティのライフサイクルを管理していくことを、アイデンティティ管理といい、適切なアイデンティティ管理の仕組みを構築することが、金融機関を含めアイデンティティを取り扱う企業にとっては重要な課題となる。

特に、デジタル化の進展に伴い、アイデンティティ管理とはすなわちデジタルアイデンティティ管理の問題として議論されることが増えてきている。前述のとおりデジタルアイデンティティの定義は、各組織・団体について様々な定義がなされており、グローバルで統一的な定義がなされているわけではない。例えば、以下の組織ではデジタルアイデンティティを以下のように定義/説明している。

表 1-1：主要組織におけるデジタルアイデンティティの定義

組織	定義
米国政府[2]	デジタルアイデンティティとは、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である。（NIST, “SP 800-63 revision 3”）
英国政府[3]	デジタルアイデンティティとはあなたが誰であるかのデジタル表明である。（DCMS, “The UK digital identity and attributes trust framework”）

[2] US NIST, “SP 800-63 revision 3”, June 2017

[3] UK Department for Digital, Culture, Media & Sport, “The UK digital identity and attributes trust framework,” Feb. 2021. https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework

豪州政府[4]	デジタルアイデンティティとは、オンラインでやり取りする際に、エンティティを十分に識別できるようにするためのエンティティの電子的表現である。 (Australia, “The Trusted Digital Identity Framework”)
ITU[5]	デジタルアイデンティティとは、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。 (X.1252 “Baseline identity Management terms and definitions”)
World Bank[6]	デジタルアイデンティティとは、個人を一意に識別することができる電子的に捕捉され保存された属性および認証情報のセットである。デジタルアイデンティティは、次の 4 つの基本的な段階を含むライフサイクルの一部として作成・使用される。(a)エンロールメントとバリデーションを含む登録、(b)文書または認証情報の発行、(c)アイデンティティの認証、(d)サービス提供や取引のための認証。 (ID4D, “Technical Standards for Digital Identification Systems”)

このように様々な定義がなされているが、本調査では ISO/IEC 24760 シリーズのアイデンティティの定義を踏まえ、デジタルアイデンティティを「ある実体に関連する属性の集合の電子的な表現」と定義する。

デジタルアイデンティティの特徴は、現実世界における個人の属性情報をデジタル化することで、個人は利用するデジタルサービスに応じて、様々なデジタルアイデンティティを使い分けて利用することが可能になったことである。例えば、現実世界では「XX 一郎」として、企業に勤務し、生活を送りながら、デジタル世界においては、本名以外にも、勤務先の社員 ID や Xxichiro といったユーザ名でデジタルサービスを利用することも可能となり、利用するサービスによってデジタルアイデンティティを使い分けることができる。現実世界のアイデンティティと比較し、デジタルアイデンティティは容易に作成・利用できる点が特徴の一つであると言える。

[4] Australia, Digital Transformation Agency, “The Trusted Digital Identity Framework,” https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework

[5] ITU, X.1252 “Baseline identity Management terms and definitions”, April 2010

[6] ID4D, “Technical Standards for Digital Identification Systems”, 2018

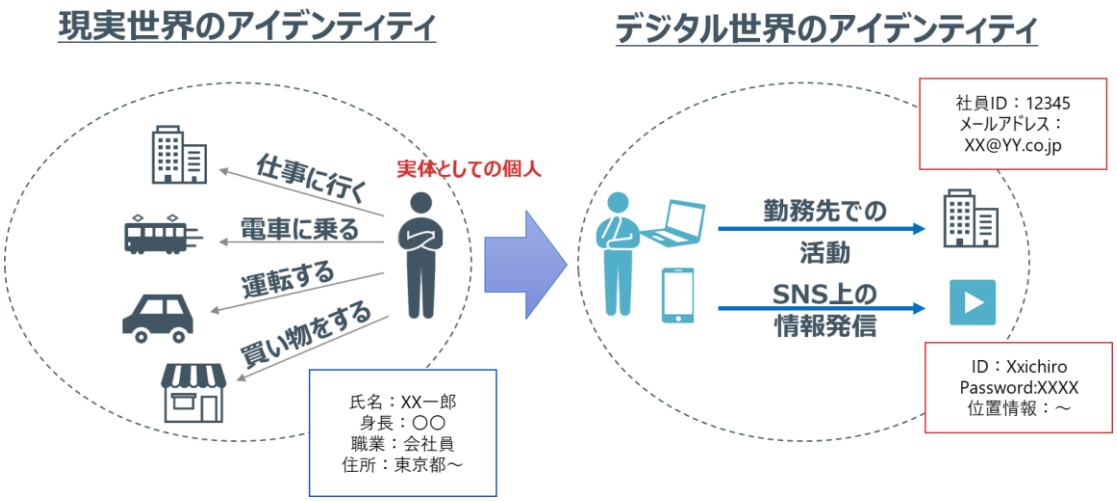


図 1-1：デジタルアイデンティティの利用イメージ

このように、ユーザにとってはリアルとデジタルのアイデンティティがつながることで、両方の世界を行き来しつつ多様なサービスの享受が可能になる。しかしながら、この実現には、両世界におけるアイデンティティの状態を管理する仕組み（アイデンティティ管理システム）が必要となる。

1-1-2. デジタルアイデンティティに関する主な検討団体

デジタルアイデンティティに関する標準化等について議論している主な団体および検討概要は以下の通り。

（1） ISO/IEC JTC 1

国際標準化機構(ISO)と国際電気標準会議(IEC)共同で、IT 分野の標準化を行うための組織として、JTC(Joint Technical Committee)1 を 1987 年に設置。JTC1 の配下にテーマ毎のサブコミッティ(SC)が設置されているが、主にアイデンティティ関連の規格を策定しているのは、情報セキュリティ・サイバーセキュリティおよびプライバシー保護を検討する SC27 である。SC27 では情報セキュリティマネジメントシステム(ISMS)などに関する ISO/IEC 27000 シリーズなどの規格が策定されており、アイデンティティ関連の主な規格も SC27 にて規格策定が進められている。

アイデンティティに関連する主な規格は以下の通り。

- ISO/IEC 24760-1:2019
  A framework for identity management — Part 1: Terminology and concepts

- ISO/IEC 24760-2:2015 (2020 年 12 月現在改定検討中)
  A framework for identity management — Part 2: Reference architecture and requirements
- ISO/IEC 24760-3:2016（2020 年 12 月現在改定検討中）
  A framework for identity management — Part 3: Practice
- ISO/IEC TS 29003:2018
  Identity proofing
- ISO/IEC 29115:2013
  Entity authentication assurance framework

また、その他アイデンティティ管理に関連し参照される主な規格は以下の通り。

- ISO/IEC 29100:2011
  Privacy framework
- ISO/IEC 29100:2011/AMD 1:2018
  Privacy framework — Amendment 1: Clarifications
- ISO/IEC 29101:2018
  Privacy architecture framework
- ISO/IEC 29146:2016
  A framework for access management
- ISO/IEC 29184:2020
  Online privacy notices and consent
- ISO/IEC 29191:2012
  Requirements for partially anonymous, partially unlinkable authentication

なお本調査においては、アイデンティティに関する用語やアーキテクチャ等については、ISO/IEC 24760 シリーズに基づく。ISO/IEC 24760 シリーズの詳細については、1-2 において詳述する。

（２） ITU-T

国際電気通信連合(ITU)は国連の専門機関の一つであり、無線通信や電気通信分野の標準化等の勧告を行う機関である。このうち、電気通信分野の標準化の勧告を行っているのが、ITU-T (ITU Telecommunication Standardization Sector)である。

ITU-T では、アイデンティティに関する勧告としては、以下が公表されている。これら勧告を参考に、（１）ISO/IEC JTC 1 で規格化されている。

- ITU-T X.1252 Recommendation: Baseline identity management terms and definitions[7] (2010/4/16 approved)
- ITU-T X.1253 Recommendation: Security guidelines for identity management systems[8] (2011/9/2 approved)
- ITU-T X.1254 Recommendation: Entity authentication assurance framework [9] (2020/9/3 approved)
- ITU-T X.1255 Recommendation: Framework for discovery of identity management information[10] (2013/9/4 approved)

また、各国における国家アイデンティティ・システムの構築のためのガイダンスとして、2018 年に「Digital Identity Roadmap Guide[11]」を公表している。

（３） ICAO

国際民間航空機関(ICAO)は、1944 年に設立された国連専門機関で、国際航空運送の安全・保安等に関する国際標準や勧告、ガイドライン等を作成している。

目視および機械読み取り可能な旅券（パスポートやビザなど）あるいは電子的機械可読旅行文書(eMRTD)については ICAO にて規格化されており、この規格に基づく作成が求められる。ICAO の規格については、例えば、後述する OpenID Foundation が策定する「OpenID Connect for Identity Assurance 1.0[12]」においても、アイデンティティアシュアランスにおいて ICAO コードに基づく国籍が用いられる等、デジタルアイデンティティの分野においても本規格等が用いられている。

なお、現在 ICAO 配下に「新技術ワーキンググループ(NTWG)」が設置されており、従来のドキュメントベースからスマホ等での身分証明書の提示を可能とするトラベルクレデンシャルに関する規格発行に向けた検討が進められている。NTWG は 2020 年 10 月に「Guiding Core Principles for the Development of Digital Travel Credential (DTC)[13]」を発

---

[7] ITU-T, https://www.itu.int/rec/T-REC-X.1252-201004-I

[8] ITU-T, https://www.itu.int/rec/T-REC-X.1253-201109-I/en

[9] ITU-T, https://www.itu.int/rec/T-REC-X.1254-202009-P/en

[10] ITU-T, https://www.itu.int/rec/T-REC-X.1255-201309-I

[11] ITU, “Digital Ideneity Roadmap Guide,” (2018)
https://www.itu.int/pub/D-STR-DIGITAL.01-2018

[12] OpenID Foundation, “OpenID Connect for Identity Assurance 1.0” (5 May 2020)
https://openid.net/specs/openid-connect-4-identity-assurance-1_0-ID2.html

[13] ICAO, “Guiding Core Principles for the Development of Digital Travel Credential (DTC)” (Oct. 2020)
https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Guiding%20core%20pri

行し、eMRTD と同程度のセキュリティ基準を満たすデジタルトラベルクレデンシャルの開発するための指針を公表している。

（４） W3C

W3C(World Wide Web Consortium)は、WWW で使用される各種技術の標準化推進を目的に設立された標準化団体。HTML や XHTML、CSS、DOM（Document Object Model）や XML（Extensible Markup Language）など多くの仕様を策定・公開している。

W3C では認証プロトコルの FIDO 2 の一部である WebAuthn 規格の仕様を所管している（WebAuthn の詳細については、1-2-4 で詳述）。また、分散型 ID（Decentralized Identifiers:DIDs）の規格の検討も進められている。本件に関連する主な規格は以下の通り。

- Verifiable Credentials Data Model 1.0[14]
- Decentralized Identifiers (DIDs) v1.0[15]

これら詳細については、第 3 章にて詳述する。

（５） IETF

インターネット技術タスクフォース(IETF)は 1992 年に設立された国際的非営利組織で、インターネットソサエティ(ISOC)のタスクフォース。TCP や IP、HTTP などの標準化を行っている。

IETF では、プロビジョニングプロトコルである SCIM(System for Cross-domain Identity Management)及び認可プロトコルである OAuth 2.0 の仕様を所管している。SCIM 及び OAuth 2.0 の詳細については、1-2-2 にて詳述する。

各国個別に独自のアイデンティティに関する規格やガイドライン等も策定されている。代表的な組織として米国や欧州の標準規格組織を挙げる。

（６）米国 NIST

アメリカ国立標準技術研究所(NIST)は商務省(Department of Commerce)傘下の米国の政府機関で、米国における各種標準を策定する組織である。

アイデンティティの分野については、「電子的認証に関するガイドライン」が策定されており、政府機関のみならず民間部門も含めて広く参照されるガイドラインとなっている。

---

nciples%20for%20the%20development%20of%20a%20Digital%20Travel%20Credential%20%20%28DTC%29.PDF

[14] W3C, https://www.w3.org/TR/vc-data-model/

[15] W3C, https://www.w3.org/TR/did-core/

電子的認証に関するガイドラインは以下の通り[16]。

- SP 800-63-3 (June 2017)[17]
  Digital Identity Guidelines
- SP 800-63A (June 2017)
  Enrollment and Identity Proofing
- SP 800-63B (June 2017)
  Authentication and Lifecycle Management
- SP 800-63C (June 2017)
  Federation and Assertions

（７）EU：CEN/CENELEC

欧州標準化委員会(CEN)は欧州規格を策定する非営利組織であり、主に EU 圏の国が参画している。なお、このうち電気分野については欧州電気標準化委員会(CENELEC)、通信分野については欧州電気通信標準化機構(ETSI)が欧州規格を策定している。

アイデンティティに関しては、CEN/CENELEC の JTC13/WG5 にて「Data Protection, Privacy and Identity Management」をテーマに検討がなされているが、直近ではブロックチェーン・DLT の検討グループである「Focus Group on Blockchain and Distributed Ledger Technologies」が設置され、そこでブロックチェーンや DLT を用いたデジタルアイデンティティに関する検討がなされている。2018 年には、勧告報告書が公表されている[18]。

（８）Kantara Initiative

Kantara イニシアチブは個人が自らの情報について取り扱いやすいようにしやすく、またデジタル経済における取引の円滑化のために活動することを目的として 2009 年に設立された非営利団体で、NIST SP 800-63-3 の適合についての第三者認証の実施や、仕様の土台を各種標準化団体に提案して標準仕様の策定にも貢献している[19]。

同イニシアチブが策定した代表的なフレームワークや仕様は以下の通り[20]。

---

[16] NIST, https://pages.nist.gov/800-63-3/

[17] SP 800-63-3 は、SP 800-3-4 への改定に向け、2020 年 6 月～2020 年 8 月まで改定に向けたパブリックコメントを募集していた。
https://csrc.nist.gov/publications/detail/sp/800-63/4/draft

[18] CEN/CENELEC, “Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies,” (Sep. 2018)
https://www.blockchaineconomia.es/wp-content/uploads/2018/11/Libro%20blanco%20estandarizaci%C3%B3n%20Bck.pdf

[19] Kantara Initiative, “About” https://kantarainitiative.org/about/

[20] Kantara Initiative, “The Rhythm of Kantara” https://kantarainitiative.org/about/

・ Kantara Trust Framework
・ Kantara User Management Access
・ Kantara Consent Receipt

Kantara User Management Access のメカニズムは IETF による”RFC 7591 OAuth 2.0 Dynamic Client Registration Protocol”に取り込まれ[21]、Kantara Consent Receipt は前述した ISO/IEC 29184:2020 “Online privacy notices and consent”においても例示されている。

（９）OIX

OIX（Open Identity Exchange）はアメリカの GSA（一般調達局）が ICF（Information Card Foundation）と後述する OIDF と、アイデンティティ情報のやり取りを法的および規定の観点で確立させるフレームワークを策定するために結んだパートナーシップをきっかけとして、オンライン上のアイデンティティにおける信頼向上を目的として 2010 年に発足した非営利団体である[22]。同団体は会合の実施、ケーススタディや白書の発行、そしてガイドの策定も行っており、軸となるガイドとしてはトラストフレームワークの在り方について描く「A Guide to Trust Frameworks and Interoperability」が策定途上にある[23]。

（１０）OASIS

OASIS (Organization for the Advancement of Structural Information of Standards) は 1993 年に SGML Open という名称として SGML（マークアップ言語の一種）を取り扱う製品間の互換性向上のためにベンダーや利用者によって発足したコンソーシアムが元で、SGML 以外の技術分野にも携わるようになったことから 1998 年に OASIS に改称した[24]。アイデンティティの分野については、多くのサービスで用いられている ID 連携プロトコルである SAML（Security Assertion Markup Language）の策定が代表的な活動として挙げられる[25]。

SAML 以外に OASIS が策定しているアイデンティティに関する仕様は以下の通り。

・ Authentication Step-Up Protocol and Metadata Version 1.0[26]

---

[21] IETF, “RFC7591 OAuth 2.0 Dynamic Client Registration Protocol” https://tools.ietf.org/html/rfc7591

[22] OIX, “About,” https://openidentityexchange.org/about

[23] OIX, “A Guide to Trust Frameworks and Interoperability” https://openidentityexchange.org/guide-trust-frameworks-interoperability

[24] OASIS, “About Us,” https://www.oasis-open.org/org/

[25] OASIS, “OASIS Security Services (SAML) TC,” https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[26] OASIS, “Authentication Step-Up Protocol and Metadata Version 1.0,” http://docs.oasis-open.org/trust-el/trust-el-protocol/v1.0/trust-el-protocol-v1.0.html (May 2017)

・ Biometric Identity Assurance Services (BIAS) SOAP Profile Version 2.0[27]
・ Electronic Identity Credential Trust Elevation Framework Version 1.0[28]
・ Identity Metasystem Interoperability (IMI) v1.0[29]
・ Identity Provider Discovery Service Protocol and Profile[30]

（１１）FIDO Alliance

FIDO（Fast Identity Online） Alliance は認証におけるパスワードへの依存を低減することを目的として 2013 年に発足し、前述した目的のための技術仕様の策定、仕様に準拠した製品の認定プログラムの実施、さらに成熟した技術仕様を他の標準化団体に申請するといった活動を行っている非営利団体である[31]。Windows や Android といった主要な OS、さらに Chrome、Firefox、Safari 等の Web ブラウザが FIDO Alliance による仕様の認定を受けており、既に多くのプラットフォームで利用することが可能となっている[32]。

FIDO Alliance が公開している認証に関する仕様は以下の通り。

・ FIDO Universal Second Factor (FIDO U2F)[33]
・ FIDO Universal Authentication Framework (FIDO UAF)[34]
・ Client to Authenticator Protocols (CTAP)[35]

FIDO の仕組みについては 1-2-2 にて詳述する。

（１２）OIDF

---

[27] OASIS, “Biometric Identity Assurance Services (BIAS) Soap Profile Version 2.0,” http://docs.oasis-open.org/bioserv/BIAS/v2.0/BIAS-v2.0.html (Jul. 2017)v

[28] OASIS, “Electronic Identity Credential Trust Elevation Framework Version 1.0,” http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/trust-el-framework-v1.0.html (May 2014)

[29] OASIS, “Identity Metasystem Interoperability Version 1.0,” http://docs.oasis-open.org/imi/identity/v1.0/identity.html (Jul. 2009)

[30] OASIS, “Identity Provider Discovery Service Protocol and Profile,” http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.html (Mar. 2008)

[31] FIDO Alliance, “Alliance Overview,” https://fidoalliance.org/overview/

[32] FIDO Alliance, “History of FIDO Alliance,” https://fidoalliance.org/overview/history/

[33] FIDO Alliance, “Universal 2nd Factor (U2F) Overview,” https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-overview-v1.2-ps-20170411.html (Apr. 2017)

[34] FIDO Alliance, “FIDO UAF Architectural Overview,” https://fidoalliance.org/specs/fido-uaf-v1.2-ps-20201020/fido-uaf-overview-v1.2-ps-20201020.html (Oct. 2020)v

[35] FIDO Alliance, “Client to Authenticator Protocol (CTAP),” https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html (Jan. 2019)

OIDF（OpenID Foundation）は 2007 年に発足し、OpenID のコミュニティと技術の実現、促進、保護に取り組んでいる非営利国際標準化団体である[36]。OIDF は OAuth 2.0 を土台とした ID 連携プロトコルである OpenID Connect 等の策定を行っているほか[37]、Windows Server 2016 以降の ADFS、Auth0、Okta、OpenAM といった様々なサービスへの規格準拠認定も行っている[38]。なお、OpenID Connect の仕組みについては 1-2-2 にて詳述する。

1-1-3. アイデンティティ管理システムとは

（1）用語集

本項では、アイデンティティ管理の考え方について ISO/IEC 24760 シリーズをもとに、アイデンティティ管理システム（IMS）のモデル（リファレンスアーキテクチャ）を示したうえで、本モデルにおける各アクターやステークホルダーの役割や責任等の考え方について整理を行う。

ISO/IEC 24760 シリーズでは、IMS の説明にあたり様々な専門用語が用いられているため、初めにこれら用語の定義を下表に記載する。

表 1-2：本調査で用いる基本概念の定義[39]

用語	定義
エンティティ（entity）	・ 明確に存在が区別されるドメインの運用目的に関連するアイテム
アイデンティティ(identity)	・ エンティティに関連するアトリビュートの集合
属性(attribute)	・ エンティティの特性または性質
アイデンティファイア(identifier)	・ ドメイン内のアイデンティティを一意に特徴付けるアトリビュートまたはアトリビュート群
リファレンスアイデンティファイア(reference identifier: RI)	・ ドメイン内のアイデンティファイアで、エンティティがドメイン内で認識されている間は同一で、エンティティが認識されなくなった後も、ポリシーで指定された期間は別のエンティティに関連づけられていないアイデンティファイア

[36] OpenID Foundation, “OpenID Foundation,” https://openid.net/foundation/

[37] OpenID Foundation, “OpenID Connect Core 1.0 incorporating errata set 1,” https://openid.net/specs/openid-connect-core-1_0.html

[38] OpenID Foundation, “Certified OpenID Connect Implementations,” https://openid.net/developers/certified/

[39] ISO/IEC 24760 part1 をもとに NRI 作成

ドメイン(domain)	・ アイデンティフィケーションやその他目的のために、エンティティがアトリビュートの集合を使用できる環境
アイデンティフィケーション(identification)	・ 特定のドメイン内のエンティティを他のエンティティと区別して認識するプロセス
アイデンティティ情報(identity information)	・ アトリビュート値の集合で、アイデンティティに関連するメタデータが任意で含まれる ・ ICT システムにおけるアイデンティティは、アイデンティティ情報として存在する
クレデンシャル(credential)	・ オーセンティケーションで使用するためのアイデンティティの表明 ・ 例えばユーザネーム、パスワード付ユーザネーム、PIN、スマートカード、トークン、指紋、パスポート等
オーセンティケーション(authentication)	・ ベリフィケーションの正式な（文書化され・組織によって認められた）プロセス。成功した場合、オーセンティケーテッドアイデンティティが生成される ・ オーセンティケーションのプロセスでは、ベリファイアによりエンティティから提供された一つあるいはそれ以上のアイデンティティアトリビュートが求められるLoA(level of assurance)を満たしているかをテストするプロセスが含まれる
オーセンティケーテッドアイデンティティ(authenticated identity)	・ エンティティのためにオーセンティケーション結果の記録が作成されたアイデンティティ情報
ベリフィケーション(verification)	・ 特定のエンティティに関連付けられたアイデンティティ情報が正しいことを確立するプロセス ・ ベリフィケーションのプロセスでは、ドメイン内のエンティティを認識するのにどのアトリビュートが必要かを決定した上で、決定された必要なアトリビュートが提示されているかや、正しいシンタックスを有しているか、定義された有効期間内のものか、そしてそれがエンティティに関連しているものであるかを確認する
バリデーション[40](validation)	・ 文書やクレデンシャル、またはアトリビュートが有効であることを確認するために、利用可能な最新の情報に基

[40] バリデーションについては、ISO/IEC 24760 シリーズで明示的な定義がなされていないため、ここでは ISO/IEC TS 29003 における定義を記載する。

	づき、イシュアまたはオーソリティのソースに確認を行うこと
アイデンティティマネジメント(identity management)	・ 特定のドメインにおけるアイデンティティのアトリビュートのライフサイクルや値、タイプ、任意のメタデータを管理するためのプロセスとポリシー
アイデンティティマネジメントシステム(identity management system: IMS)	・ 関連するメタデータを含むアイデンティティ情報を維持するためのポリシー、手順、技術、その他のリソースで構成されるメカニズム
アイデンティティプルーフィング(identity proofing)	・ 一定の LoA に達することを目的としたアイデンティティエビデンスに基づくベリフィケーション ・ 通常はエンロールメントの一環で行われる
アイデンティティエビデンス(identity evidence)	・ アイデンティティ情報が正当であると確認することを裏付ける情報
エンロールメント(enrollment)	・ エンティティを特定のドメイン内で認識させるプロセス
アイデンティティフェデレーション(identity federation)	・ ドメイン間のアイデンティフィケーションのためにどのようにアイデンティティ情報を交換および管理するかを規定した、2 つ以上のドメイン間の合意

（2）アイデンティティの 7 原則

適切なアイデンティティ管理を行うためには、いくつかの原則に基づいた設計・開発・運用が重要となる。例えば、元マイクロソフトのアイデンティティアーキテクトで、アイデンティティに関する国際的な議論に多大な影響を与えた Kim Cameron 氏は、デジタルアイデンティティの管理における「アイデンティティの 7 原則(Seven Laws of Identity)」を提唱している[41]。

表 1-3：アイデンティティの 7 原則

#	原則	内容
1	ユーザによる制御と同意	アイデンティティ・システムは、ユーザの同意がなければユーザを識別する情報を開示すべきではない

[41] Kim Cameron, “The Laws of Identity”
https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf
日本語訳は、崎村夏彦、「アイデンティティの 7 原則」を参照。
https://www.sakimura.org/2011/05/1104/

2	限定された用途で最低限の公開	最も安定し、長期にわたって使用できるソリューションとは、開示するアイデンティティ情報を最小限にし、情報へのアクセスを適切に制限するソリューションである
3	正当な関係者の身への情報開示	アイデンティティ・システムは、特定の状況において識別情報を必要とし、かつ入手できる正当な権利を持つ関係者のみに対して情報を開示するように設計されなければならない
4	方向づけられたアイデンティティ	アイデンティティ・システムは、公に使用する「全方位的」な識別子とプライベートで使用する「特定の方向性」を持った識別子の両方をサポートしなければならない。このことにより公共性を維持しながら不必要に関連付けの公開を防止できる
5	複数のアイデンティティプロバイダと技術の相互運用性	アイデンティティ・システムは、複数のアイデンティティプロバイダによって実行される複数のアイデンティティ技術の相互運用性を保持しなければならない
6	人間の統合	アイデンティティ・システムは、利用者たるユーザを分散システムの１つのコンポーネントとして定義しなければならない。明確なマンマシン・インターフェイスを策定してユーザを分散システムに統合し、アイデンティティを保護しなければならない
7	シンプルで一貫性のあるユーザエクスペリエンス	アイデンティティ・システムは、さまざまな状況下でのアイデンティティ・コンテキストの分離を可能にしつつも、一貫性のあるユーザとテクノロジーのインターフェースを提供しなければならない

アイデンティティの管理においては、これら 7 原則に基づくシステムの設計・開発・運用が重要となる。

（3）アイデンティティ管理システム（IMS）の仕組み

ISO/IEC 24760 では、アイデンティティ管理は上記のとおり、「特定のドメインにおけるアイデンティティの属性のライフサイクルや値、タイプ、任意のメタデータを管理するためのプロセスとポリシー」と定義される。ICT システムなどにおいて管理されるアイデンティティはアイデンティティ情報として管理されるため、これらアイデンティティ情報を適切に管理するためには、アイデンティティ情報を維持するためのポリシー、手順、技術、その他のリソースで構成されるメカニズム（＝アイデンティティ管理システム：IMS）が必要となる。具体的には、IMS は、管理的活動（アイデンティティ情報の管理やポリシー管理）とリソースアクセス管理（認証や属性情報の取得）が主な役割となる。

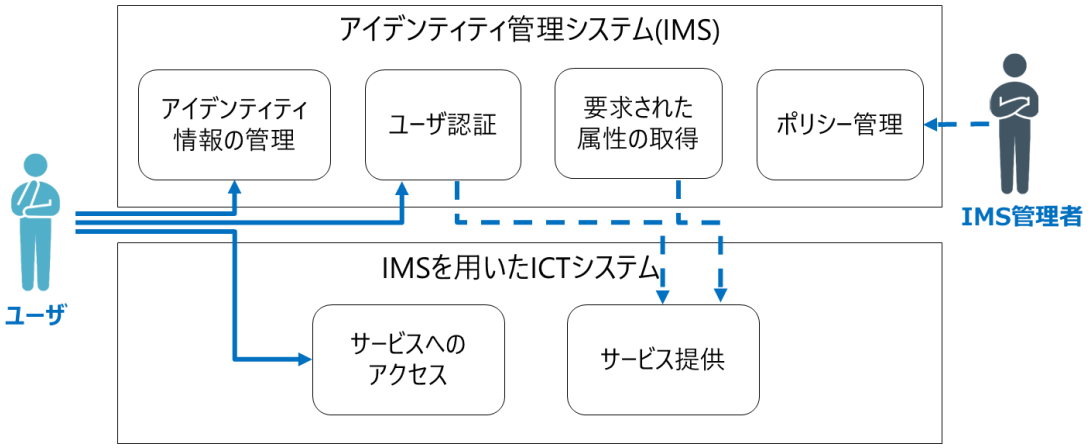


図 1-2：IMS の主な仕組み[42]

この中で重要な活動となるのは、アイデンティティ情報の管理におけるライフサイクル管理である。ISO/IEC 24760 シリーズでは、アイデンティティライフサイクルとして、以下の通り示される。

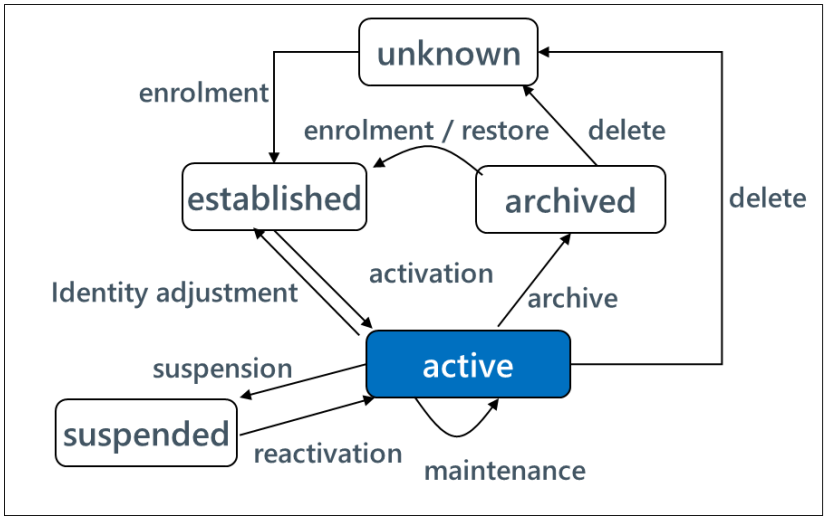


図 1-3：アイデンティティライフサイクル管理

図 1-3 における各ライフサイクルステージの定義は以下の通り。

[42] ISO/IEC 24760-2 をもとに NRI 作成。

表 1-4：IMS のライフサイクルステージの定義[43]

ステージ	定義
アンノウン Unknown	・ エンティティを識別するために用いられる情報がアイデンティティレジスタに存在しない状態。
エスタブリッシュド Established	・ エンロールメントプロセスにおいて必要なアイデンティティ情報が検証されている状態。リファレンスアイデンティファイア（表 1-2 定義参照）などの付加情報が生成され、情報が登録される（アイデンティティレジストレーション）。
アクティブ Active	・ IMS にアイデンティティ情報が存在し、エンティティがドメイン内で利用可能なサービスやリソースにアクセスできる状態。
サスペンデッド Suspended	・ IMS にアイデンティティ情報は存在するが、エンティティはドメイン内のリソースを利用できない状態。
アーカイブド Archived	・ アイデンティティレジスタにエンティティのアイデンティティ情報は存在するが、ドメイン内にエンティティが存在しない状態。エンティティのアーカイブド情報は再エンロールメントを行わない限り利用できない。エンティティが再エンロールした場合、アーカイブド情報はエンティティの新たなアイデンティティ（アーカイブド 情報を含む場合もある)をエスタブリッシュするために利用される。

また、各ライフステージ間における状態の定義は以下の通り。

表 1-5：各ライフステージ間の状態の定義

状態	定義
エンロールメント Enrolment	・ ベリファイド（verified）及びジェネレーテッド（generated）されたアイデンティティ情報に関するアイデンティティのアイデンティティプルーフィングとレジストレーションを行うこと
アクティベーション Activation	・ エンティティがドメイン内で提供されているリソースへのアクセスや、サービスを利用できるよう、アイデンティティレジスタで管理されている情報にアイデンティティ情報を付加すること
メンテナンス Maintenance	・ アイデンティティレジスタで管理されているエンティティのアイデンティティ情報をアップデートすること

[43] ISO/IEC 24760 part1

アイデンティティアジャストメント Identity adjustment	・ アイデンティティレジスタで管理されているエンティティのアイデンティティ情報をアップデートすることで、アクティベーション情報を新たな情報に修正すること
サスペンション Suspension	・ アイデンティティレジスタで管理されているエンティティのアイデンティティ情報の一部を一時的に利用できないようにすること。サスペンションは管理されているアイデンティティ情報へのアクセス権を削除することでなされる
リアクティベーション Reactivation	・ サスペンションの逆
デリート Delete	・ レジスタされたアイデンティティにおけるアイデンティティ情報の完全削除
アーカイブ Archive	・ アイデンティティレジスタにおけるエンティティのアイデンティティ情報の部分的削除のことで、情報は統計処理の目的でのみ利用でき、エンティティから付加情報が提供された場合のみ、関連エンティティとしてアクセス可能となる
エンロールメント・リストア Enrolment/restore	・ アイデンティティプルーフとして用いられるあるアイデンティティ情報がアイデンティティレジスタから取得されるエンロールメントプロセスのこと

IMS の適切な運用を考える際には、これらアイデンティティのライフサイクルにおける各アクションが適切に行われるようアイデンティティマネジメントを設計・構築することが求められる。IMS は、アイデンティティライフサイクルのステージによって、IMS を構成するアクターのロールやアクションが異なるため、IMS の仕組みを理解するためには、これらアクターについて理解することが重要となる。具体的には、以下のような多数なアクターによって IMS が運用・利用されている。

表 1-6：IMS に登場する主なアクター[44]

#	アクター	定義
1	プリンシパル (Principal)	・ IMS によりエンティティのアイデンティティ情報が保存、管理されているエンティティ
2	レジストレーションオーソリティ (Registration authority：RA)	・ エンロールメントやアイデンティティプルーフィング、アイデンティティレジストレーションに対して責任を負う特定のドメインにおけるエンティティ

[44] ISO/IEC 24760 シリーズ

3	アイデンティティ情報オーソリティ (Identity information authority：IIA)	・ アイデンティティの一つ以上のアトリビュート値の妥当性および／または正しさについて証明可能な記述を行うことができる特定のドメインに関連したエンティティ
4	アイデンティティ情報プロバイダ (Identity information provider：IIP)	・ 利用可能なアイデンティティ情報を提供するエンティティ ・ IIP の典型的なオペレーションは特定ドメイン内で認知されたエンティティのためにアイデンティティ情報を作成・維持すること。IIA が IIP の役割を担うこともある。
5	アイデンティティレジストレーションオーソリティ(Identity registration authority：IRA)	・ IMS においてアイデンティティレジスタにアイデンティティ情報を収集、記録、更新する際のオペレーションポリシーを整備、実施する義務や能力を有するアクター
6	アイデンティティアサーションプロバイダ (Identity Assertion Provider：IAP)	・ IAP はオーセンティケーション及び/又はアトリビュートを裏付ける責任を負う。ベリファイアとして活動し、アイデンティティレジスタにアクセスする
7	クレデンシャルイシュア/ クレデンシャルサービスプロバイダ (Credential Issuer/ Credential service provider：CSP)	・ クレデンシャルイシュアとは、特定ドメイン内のプリンシプルに対して、クレデンシャルを提供する責任を有するエンティティ ・ CSP とは、当該ドメインにおけるクレデンシャル管理の責任を負う、信頼されたエンティティ。CSP がクレデンシャルイシュアのロールを担う場合もある。
8	ベリファイア (Verifier)	・ ベリフィケーションを行うエンティティ
9	リライングパーティ (Relying party: RP)	・ 特定のエンティティのアイデンティティ情報のベリフィケーションに依拠するエンティティ
10	アイデンティティマネジメントオーソリティ (identity management authority：IMA)	・ 当該ドメインのアイデンティティマネジメントのためにビジネス目的を定義・調整するための責務と機能を有し、これら目的を達成するためのマネジメントポリシーを設定する
11	オーディター (auditor)	・ 文書化された方針や手順に従って運営されているかどうか、また、法律やその他の外部から課せ

		られた要求事項に準拠しているかどうかを確認する
12	レギュラトリーボディ (Regulatory body)	・ アイデンティティマネジメントシステムの運用を監督するために、法律、規制、または合意によって任務を与えられ、権限を与えられた機関
13	コンシューマ/シティズンリプレゼンテーティブ/アドボケート (Consumer/citizen representative or advocate)	・ 監視から消費者や市民を守るための活動や、プライバシー規制の改善のためにロビー活動を行う個人やグループ

これらアクターが IMS におけるアイデンティティライフサイクル管理の中でどのような役割を果たしているのかについて説明するにあたり、本調査では以下の 3 つのフェーズにおけるユースケースをもとに、IMS の運用の考え方について整理する。具体的には、IMS 内処理として登録処理（enrolment, activation）と更新処理（maintenance）、IMS 間処理として連携処理（federation）の 3 つのユースケースである[45]。

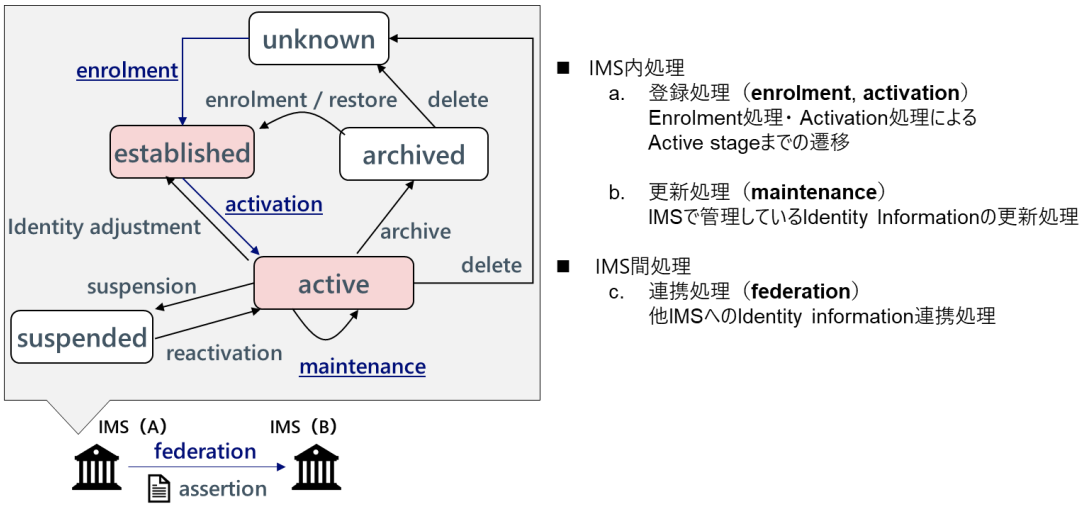


図 1-4：アイデンティティライフサイクル内の 3 ステージ

[45] 以降で記載する 3 つのユースケースに登場するアクターは表 1-6 に記載アクターのうち、主に#1-9 のアクターである。本ユースケースでは登場していないが、実際には IMS が適切に管理・運用されるためには、それらを管理・監督する#10-13 のアクターが存在している。

a. IMS 内処理：登録処理

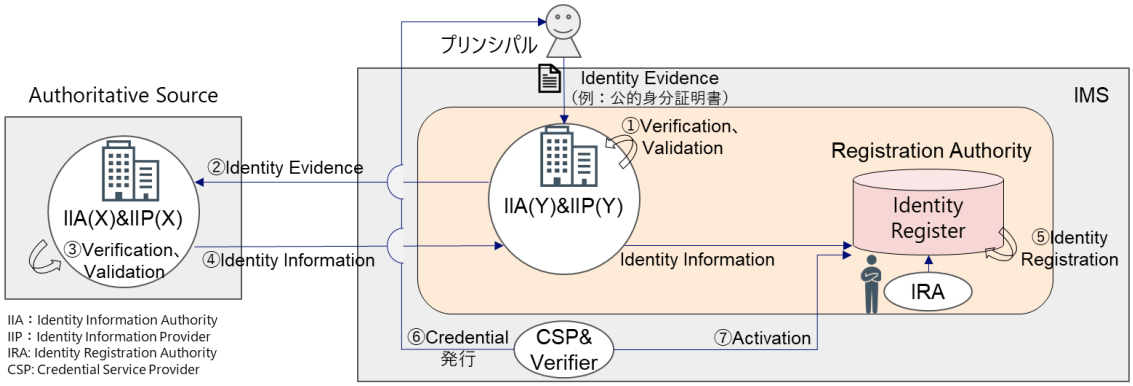


図 1-5：a. 登録処理（enrolment, activation）のフロー図

登録処理では、プリンシパルから提示されたアイデンティティエビデンスを受領した IMS は、プリンシパルのアイデンティティレジストレーションに必要な情報が揃っているかの確認を行う必要がある（＝アイデンティティプルーフィング）。アイデンティティプルーフィングにおいては、受領した情報が真正か（ベリフィケーション）ならびに有効か（バリデーション[46]）についての検証を行う（①）。

IMS は必要に応じてアイデンティティエビデンスの生成元である Authoritative Source に、アイデンティティエビデンスの照会を行い（②）、Authoritative Source でのバリデーション・ベリフィケーション実施を行った後（③）、その検証結果を返却してもらう（④）。そして検証結果を踏まえ、IMS 内で IRA が、アイデンティティレジスタに対しアイデンティティレジストレーションをおこなう（⑤）。

アクティベーションでは、プリンシパルが自身のアイデンティティ情報を参照・更新可能となるために必要なクレデンシャルを、CSP がプリンシパルに対し発行する（⑥）。併せて、同ドメインが提供するサービスとインタラクションできるようにすることで、IMS 内のアイデンティティ情報をアクティベート（⑦）させる。

[46] 一例として、公的個人認証サービスにおいては、発行した電子証明書の有効性検証機能を提供

b. IMS 内処理： 更新処理

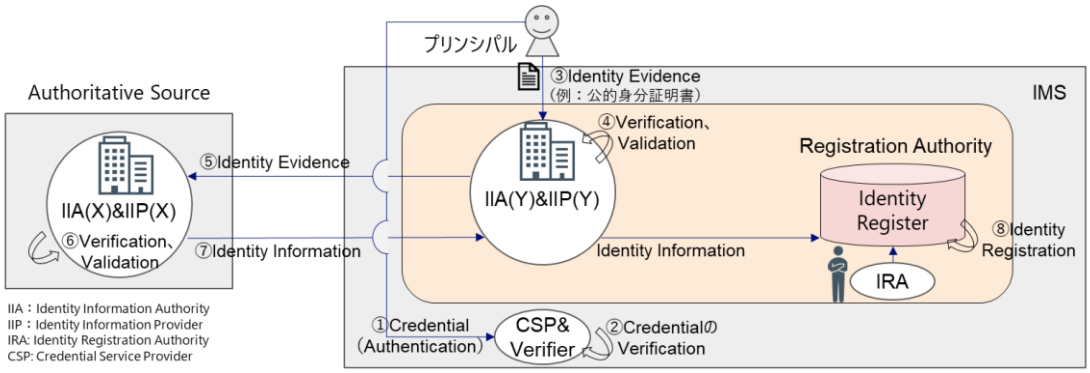


図 1-6：b. 更新処理（maintenance）のフロー図

更新処理では、プリンシパルは、クレデンシャルを用いたオーセンティケーション実行後、新たなアイデンティティエビデンスを更新し、IMS 上のアイデンティティ情報を更新する。まず、プリンシパルは CSP に対しクレデンシャルを送付（①）する。CSP では受領したクレデンシャルをベリフィケーションし、オーセンティケーションを行う（②）。その後、プリンシパルは新たなアイデンティティエビデンスを提示する（③）。その後、エンロールメント時と同様の処理を行い、アイデンティティレジスタに対しアイデンティティ情報を更新/修正する（④～⑧）。

c. IMS 間処理： 連携処理

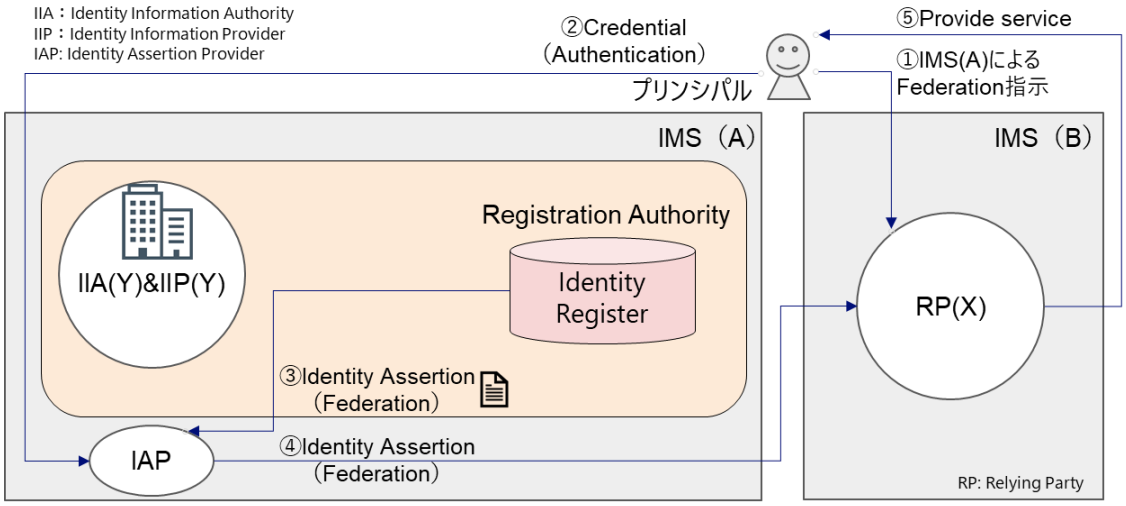


図 1-7：c. 連携処理（federation）

RP は、アイデンティティフェデレーションを行うことで、プリンシパルのオーセンティケーションを他ドメインの IMS に委ねることが可能となる（但し、事前に双方ドメインの IMA（Identity Management Authority）同士が、事前に両ドメイン間の ID 連携を許容している事が前提)。プリンシパルが IMS(B)に対するオーセンティケーションを、IMS(A)のアサーションを用い実施することを指示（①)、プリンシパルは IMS(A)に対し、クレデンシャルを渡しオーセンティケーションを実行する（②)。プリンシパルは自身のアイデンティティ情報を RP(X)に提供して良いか確認・同意を行い、アイデンティティアサーション（リライングパーティがオーセンティケーションで使用する、アイデンティティ情報オーソリティによるステートメント）の形で RP(X)に提供される（③、④)。RP(X)は受け取ったアイデンティティアサーションを踏まえ、自身のドメインにおけるプリンシパルへのサービス提供可否を判断し、提供可となった場合、プリンシパルにサービス提供を行う（⑤)。

（4）アイデンティティ管理のデジタル化

アイデンティティ情報のやり取りについては、依然として紙媒体等を用いたアナログでの処理を行っているシステムも多い（一例として、アイデンティティプルーフィングに用いられるアイデンティティエビデンスの連携手段として免許証のコピーを郵送する等)。

例えば、アナログの IMS の例として、ユーザ（プリンシパル）が金融機関での新規口座開設にあたり、本人確認書類として、公的身分証を提示し金融機関がコピーして確認、あるいはユーザがコピーして提出するといったことが想定される。いずれの場合も金融機関は提示された身分証のコピー（紙/画像データ）をもとに本人確認を実施しており、これはアナログの IMS であると考えられる。

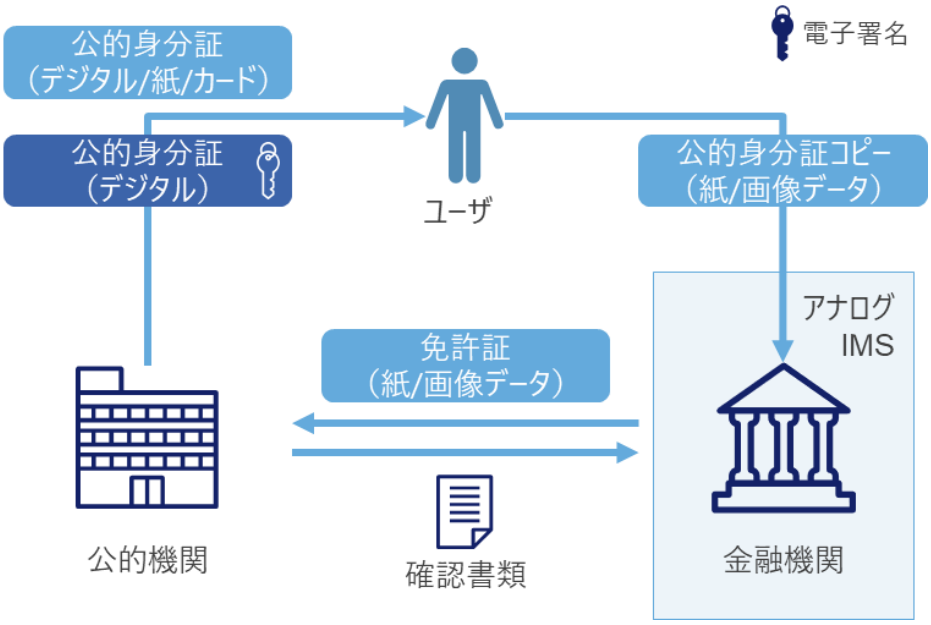


図 1-8：アナログの IMS（例）

これに対し、公的機関や金融機関等のデジタル化の進展に伴い、本人確認書類をコピー（紙/画像データ）ではなく、デジタルな公的身分証をそのまま金融機関に連携し、金融機関はそのマシンリーダブルな形式で連携された身分証の検証を行う、といった利用形態も増えてきている。

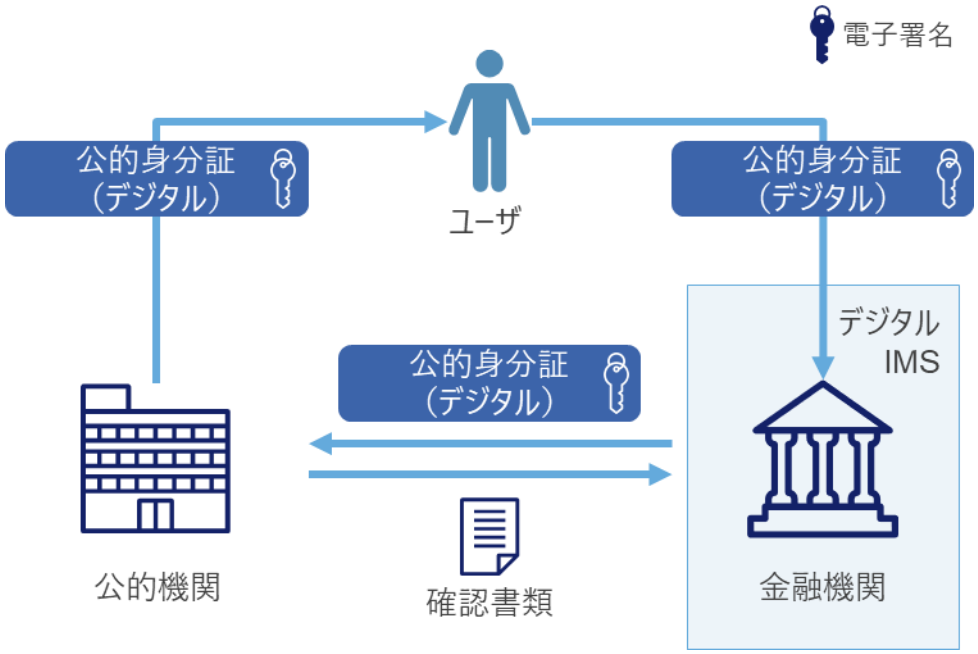


図 1-9：デジタルの IMS（例）

本調査では、IMS のデジタル化とは、このような相互のやりとりをデジタル化すること（例えば、マシンリーダブルな形式でのアイデンティティエビデンスの連携等）と捉え、2章以降において IMS のデジタル化の動向や課題等について整理する。

1-2.　主要な IMS モデルと構成要素

本節では、前節のアイデンティティに関連する概念定義を踏まえ、現在一般的に用いられる IMS モデルについて取り上げたうえで、そこで用いられている具体的な技術要素やガバナンス要素などについて整理する。

1-2-1. IMS の主要モデル

IMS のモデル/スキームとして、これまで/現在の代表的なものとしては Centralized（集中管理）モデルとフェデレーションモデルが挙げられる。

集中管理モデルでは RP と IdP が同一主体となり、個別にアイデンティティ管理とサービス提供を行い、ユーザはサービス毎にアイデンティティ管理が必要となっている。例えば、ユーザが A 銀行、B 銀行、C 銀行のオンラインバンキング用口座にアクセスする際、各行で作成したオンラインアカウントで個別にログインし、個別にオンラインバンキング口座にアクセスする場合は、集中管理モデルであるといえる。

フェデレーションモデルは、RP と IdP は別エンティティであり、ユーザは RP のデジタルサービスにアクセスする際、IdP のアイデンティティ情報を用いる。また、ユーザは RP 毎にログインする必要なく、特定の IdP のアイデンティティ情報をもとに、複数の RP にアクセスできる。例えば、ユーザが、A 銀行、B 銀行、C 銀行のオンラインバンキング用口座にアクセスする際、D 銀行が提供するアカウントを使って、A～C の各行のオンラインバンキング口座にアクセスできる場合は、フェデレーションモデルであるといえる。

図 1-10：代表的な IMS のモデル

インターネット上で様々なオンラインサービスが提供され始めた当初は、各サービス提供事業者が、単一の組織で展開された範囲で IMS を保持し、自社のポリシーに従ってアイデンディティの管理を行うのみであった。その後、複数の企業を横断しサービスの利用が当たり前となるにつれ、複数企業・組織の提供するサービスを横断的に使いたい場合等において、利用者のアイデンティティ情報を複数企業が連携して管理する体制を構築する必要が生じてきた。だが単一の IMS を複数企業・組織が管理するのは、責任分界点の問題や、各組織が求めるガバナンスやアイデンティティ管理の保証レベルに求める要件の摺り合わせ等を考慮すると、各企業・組織間での合意に要する労力が大きいという課題がある。またプライバシーの観点でも、単一の IMS 上でしか自らのアイデンティティを管理出来ない状況はリスクであり、対策が必要であった。

こうした課題を解決するため、IMS 間でアイデンティティ情報をやり取りする状況、すなわちフェデレーションモデルへと潮流が変化していった。フェデレーションモデルでは、IMS システム間ならびに利用者による自身のアイデンティティ情報の連携に対する操作への同意を以て、各 IMS の相互運用を実現し、利用者のアイデンティティの連携を行う。

また並行して、これらの基本原則を実現するために、IMS とそれに関連する技術の多様化も進み、プロビジョニングプロトコルとしての SCIM や ID 連携としての SAML および OIDC といった技術要素としての規格が策定され、標準として多くの IMS で用いられるようになった。次項では、これら規格の概要について記載する。

1-2-2. IMS モデルにおいて用いられる技術要素

IMS は複数の組織やサービスに跨って実装されるものであり、そこで用いられる技術の標準化は不可欠なものとなっている。このようなデジタルアイデンティティの標準化にはいくつかの動向と要素技術があり、主要なものをプロトコル毎に整理する。

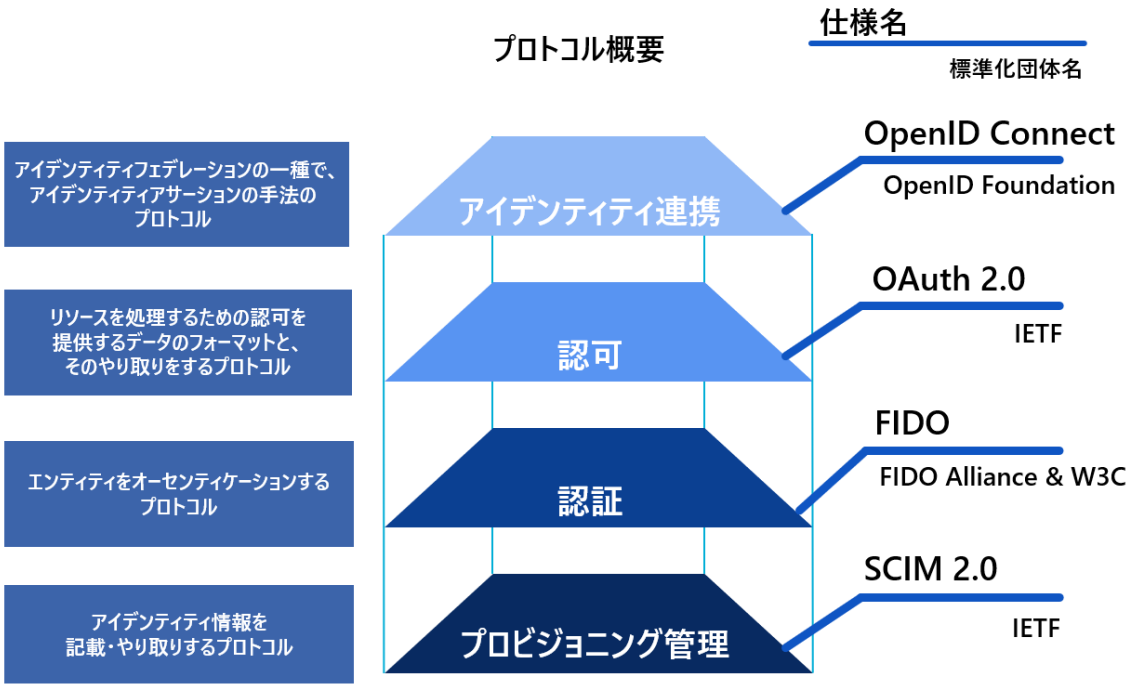


図 1-11　主要 IMS におけるプロトコル概要

各プロトコルを策定する団体および団体概要は下表のとおり。

表 1-7　各仕様と標準化団体概要

	プロビジョニング	認証		認可	アイデンティティ連携
仕様名	SCIM （System for Cross-domain Identity Management、当初は Simple Cloud Identity Management の略） 2.0	FIDO （Fast IDentity Online ）		OAuth 2.0	OIDC （OpenID Connect）
標準化団体	IETF（The Internet Engineering Task Force）	FIDO Alliance	W3C（World Wide Web Consortium）	IETF	OpenID Foundation

団体概要	インターネットに関連する標準技術仕様を策定する非営利国際標準化コミュニティ	FIDO の仕様策定、普及活動、FIDO 導入製品への認定プログラムを実施する非営利国際標準化団	World Wide Web の各種技術や規格を策定する非営利国際標準化団体	インターネットに関連する標準技術仕様を策定する非営利国際標準化コミュニティ	OpenID 技術の実現、促進、保護に取り組む非営利国際標準化団体

（1）プロビジョニング（SCIM 2.0）

プロビジョニングプロトコルとは、Web サイトやアプリケーション等のクライアントから Web アプリケーションのサービスプロバイダに、アイデンティティマネジメントシステム内で管理されているアイデンティティ情報に対しプロビジョニング（管理指示）を行うためのプロトコルを指す。プロトコルの登場の背景としては、インターネットの普及・拡大に伴い、単一のドメインだけに閉じず、横断的にアイデンティティ情報のプロビジョニングを行う必要が生じていたことがある。プロビジョニング処理の標準化を目指し、OASIS（Organization for the Advancement of Structured Information Standards）によって XML 形式で記述する SPLM（Service Provisioning Markup Language）の 1.0 が 2003 年に、2.0 が 2006 年に公開されていたものの、仕様の複雑さと相互互換性の悪さから普及しなかった[47]。それでも各種サービス間でのアイデンティティ情報のやり取り方法の標準化の需要はクラウドサービスの発展と利用機会の増加に伴って高まり、SCIM 1.0 が 2011 年に、1.1 が 2012 年に OWF（Open Web Foundation）内のワーキンググループによって公開された[48]。

SCIM はインターネットに関する標準技術仕様を策定してきた IETF に移管され、2015 年 9 月に公開された RFC7642、7643、7644 から構成される SCIM 2.0 では、アイデンティティ情報を共通のスキーマの JSON 形式で記述し、RESTful な Web API で CRUD に特化した処理を行うこと、といった事項が定められた[49]。SCIM は使い勝手の良いプロトコルとして利用の拡大が進み、各種サービスが SCIM に準拠や対応することで、Web サイトやアプリケーションは単一の方法に対応することで、多様なアプリケーションからのプロビジョニングが可能となった。

---

[47] 情報処理推進機構 『情報セキュリティ技術動向調査（2011 年上期）』 https://www.ipa.go.jp/security/fy23/reports/tech1-tg/a_08.html

[48] System for Cross-domain Identity Management “Specification SCIM 1.0 - Deprecated” “Specification SCIM 1.1” http://www.simplecloud.info/

[49] System for Cross-domain Identity Management, “Specification SCIM 2.0,” http://www.simplecloud.info/

SCIM 2.0 でのプロビジョニングの対象として、Web アプリケーションの IMS 内において JSON 形式で管理されているアイデンティティ情報（属性：アトリビュート）の群（「リソース」）が規定されている。SCIM 2.0 でやり取りされる「リソース」の記述項目は RFC7643 においてユーザ、グループ、企業ユーザ、サービスプロバイダ設定、リソースタイプの 5 つに分類されている。また、日時の表記など項目によっては互換性を持たせるためにフォーマットが規定されているものもある。ここでは例としてユーザでの「リソース」を以下に紹介する[50]。

表 1-8：SCIM 2.0 において「リソース」の種類がユーザである場合の属性（アトリビュート）例

属性名	配下属性名	概要
userName		サービスプロバイダにおいてログインなどにも用いられうるユーザ名
name	Formatted	フルネーム　例：“Mr. Kenta Christopher Yamada, II”
	familyName	性 例：”Yamada”
	givenName	名 例：”Kenta”
	middleName	ミドルネーム 例：”Christopher”
	honorificPrefix	敬称 例：”Mr.”
	honorificSuffix	接尾辞 例：”II”
displayName		表示名
nickName		ニックネーム
profileUrl		ユーザの Web サイト等のプロファイルへの URI
title		肩書
userType		組織とユーザの関係性（組織におけるユーザの種類）を示す値
preferredLanguage		サービスで表示する言語
locale		地域
timezone		タイムゾーン
active		アカウントの有効状態等
password		パスワード
emails	value	メールアドレス

[50] Internet Engineering Task Force, “Request for Comments: 7643 System for Cross-domain Identity Management: Core Schema,” https://tools.ietf.org/html/rfc7643

	display	正規化された表示用のメールアドレス
	type	メールアドレスの種類
phoneNumbers	value	電話番号
	display	正規化された表示用の電話番号
	type	種類
ims		インスタントメッセンジャー用のアドレス
	type	インスタントメッセンジャーのサービス
photos		ユーザの画像の URI
addresses	formatted	住所
	streetAddress	番地
	locality	都市・市区町村
	region	州・都道府県
	postalCode	郵便番号
	country	国
	type	住所の種類
groups		所属するグループ
entitlements		持つ権利等
roles		役割等
x509Certificates		電子証明書情報

上述した SCIM 2.0 として記述されたアイデンティティ情報の項目は、RFC7644 でデータのやり取りや操作の方法が定められている。SCIM のデータの受け渡し方法としては HTTP ベースの REST プロトコルと決められており、Web サービス間でのやり取りにも向いている。操作内容とリクエストメソッドの例を以下に紹介する[51]。

表 1-9：REST プロトコルでのリクエストメソッド

操作内容	リクエストメソッド
作成	POST
閲覧	GET
置換	PUT
削除	DELETE
更新	PATCH

[51] Internet Engineering Task Force, “Request for Comments: 7644 System for Cross-domain Identity Management: Protocol,” https://tools.ietf.org/html/rfc7644

また、SCIM 2.0 自体には認証や認可は備わっていないため、アイデンティティ情報の安全なやり取りのためには SCIM 2.0 とは別に規定される TLS クライアント認証、HOBA 認証、Bearer トークン、PoP トークン、Cookie、ベーシック認証等を例として挙げて、認証を実施することが必要だと RFC7644 では定められている[52]。

（2） 認証（FIDO）

認証プロトコルとは、アイデンティティを操作しようとするエンティティが、以前登録された際と同一のエンティティであることを確認する手法のプロトコルを指す。従来の一般的な認証プロトコルでは、ID とパスワードの組み合わせといったクレデンシャルをプリンシパルからネットワーク経由で IMS のベリファイアに送付し、ベリファイアにてベリフィケーションを実施している。このため、パスワードをネットワーク上でやり取りする必要があっただけでなく、通信内容の改ざんや、フィッシングサイト等でパスワードが窃取された場合になりすましや使いまわしをしているサービスへのリスト型攻撃のリスクもあった。このようなリスクに対応する為、クレデンシャルの窃取による不正ログインや、ユーザエクスペリエンスを低下させない多要素認証の仕様が求められていた。

新たに利用が広まっている FIDO は、標準的な公開鍵暗号方式を用いて堅牢な認証を実現可能としている。オンラインサービスへの登録時、ユーザのクライアントデバイスで新しい鍵ペアを生成し、秘密鍵はクライアントデバイスに保持し、公開鍵のみオンラインサービスに登録される。クライアントデバイスが秘密鍵を用いチャレンジに署名することにより、秘密鍵を保持していることをオンラインサービスに証明し、認証を行う。このため、機密情報である ID とパスワードの組み合わせをネットワーク上でやり取りせずともオーセンティケーションができ、認証器側でのベリフィケーションの結果は電子署名されることで通信経路での改ざんやなりすましから保護される。また、クライアントデバイスに保持された秘密鍵は、ユーザがデバイス上でロック解除を行うことで使用可能となる。ロック解除には、指紋認証、顔認証、暗証番号入力、2 段階認証デバイス挿入など、ユーザにとって使いやすく安全なアクションを採用可能である。FIDO についてはブラウザが FIDO Client として機能する FIDO2 の規格が公開され、大手ブラウザベンダも同規格に対応したことから、今後の利用拡大が期待されている。

FIDO の仕様策定と普及活動を担う FIDO Alliance は 2013 年に正式に発足し、2014 年にパスワードレス（UAF：Universal Authentication Framework）および二要素認証のプロトコル（U2F：Universal Second Factor）を公開した。その後、2019 年にインターネットに関連する標準技術仕様を策定する W3C により、Web ブラウザを FIDO クライアントと

---

[52] Internet Engineering Task Force, “Request for Comments: 7644 System for Cross-domain Identity Management: Protocol,” https://tools.ietf.org/html/rfc7644

して機能させ FIDO 認証器にアクセスする為の API 仕様を定義した、WebAuthn（Web Authentication API）[53]が策定された。加えて、FIDO クライアントと認証器間の通信仕様を規定した CTAP （Client to Authenticator Protocol）[54]が策定され、併せて FIDO2 と呼んでいる[55]。

FIDO Alliance による CTAP は Web ブラウザといったクライアントとベリフィケーションを実施する外部の認証器の間のプロトコルで、伝送経路は USB、NFC、Bluetooth を用いることができると定められている[56]。なお、Google の Android 7.0 以降や Microsoft の Windows Hello といった端末内蔵の認証方法は FIDO Alliance によって個別に FIDO2 の認定がなされている[57]。W3C による WebAuthn は Web ブラウザとサーバ側に組み込まれる仕様で、CTAP からのベリフィケーション結果の受け取りや伝達等を担っている。このように FIDO2 は利用者側の処理は FIDO Alliance による CTAP に準拠して認定された外部認証器や、または認定された内蔵認証器、Web 側の処理は W3C による WebAuthn と役割分担がなされて、両方が組み合わさることで認証方法として成り立っている。

FIDO2 を用いたサービスでのオーセンティケーション利用は事前に認証器側で鍵ペアの生成とサーバ側で鍵ペアの内の公開鍵の登録が必要で、登録の流れは以下の通り。

① ユーザが既存の認証手段でサービス側（RP）でログイン状態に遷移したうえで FIDO 登録をアプリケーションサーバに要求する。
② サービス側のアプリケーションサーバから FIDO サーバに要求を転送する。
③ サービス側の FIDO サーバがチャレンジ、ユーザ情報、RP 情報をまとめて PublicKeyCredentialCreationOptions としてアプリケーションサーバに送信する。
④ アプリケーションサーバからユーザ側の Web ないし NativeApp に PublicKeyCredentialCreationOption を送る。
⑤ ユーザ側の Web ないし NativeApp から PublicKeyCredentialCreationOption を OS ないし Web ブラウザに送る。
⑥ OS ないし Web ブラウザにて ClientData を生成しつつ、端末外部の認証器であれば CTAP で、内蔵認証器であれば端末内のプロトコルでチャレンジ、ユーザ情報、

---

[53] W3C, “Web Authentication: An API for accessing Public Key Credentials Level 1,” https://www.w3.org/TR/webauthn-1/

[54] FIDO Alliance, “Client to Authenticator Protocol (CTAP),” https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html

[55] FIDO Alliance 『仕様概要』 https://fidoalliance.org/仕様概要/?lang=ja

[56] FIDO Alliance, “Client to Authenticator Protocol (CTAP),” https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html

[57] FIDO Alliance, “FIDO® Certified Products,” https://fidoalliance.org/certification/fido-certified-products/

RP 情報、clientDataHash をまとめて authenticatorMakeCredential operation として送る。

⑦ 認証器によってユーザのベリフィケーションを行う。

⑧ 認証器内部で秘密鍵（Credential Private Key）と公開鍵（Credential Public Key）の鍵ペアを生成する。

⑨ 認証器秘密鍵（Attestation Private Key）と秘密鍵を用いて authenticatorMakeCredential operation から、公開鍵を含めた attestationObject を生成する。なお、attestationObject は認証器側にも保管する。

⑩ attestationObject を CTAP 等を経由して OS ないし Web ブラウザに送る。

⑪ OS や Web ブラウザから attestationObject と clientDataJSON を併せた AuthenticatorAttestationResponse を Web や NativeApp に送る。

⑫ Web や NativeApp から AuthenticatorAttestationResponse をアプリケーションサーバに送る。

⑬ アプリケーションサーバから FIDO サーバに AuthenticatorAttestationResponse を送る。

⑭ FIDO サーバにて AuthenticatorAttestationResponse の内容から、認証器の情報を FIDO Metadata Service 等に照会する。

⑮ FIDO Metadata Service 等から認証器のステータスや認証器公開鍵（Attestation Public Key）を含む Attestation Certificate を取得する。

⑯ 認証器秘密鍵と対になる認証器公開鍵で AuthenticatorAttestationResponse を検証しつつ、FIDO サーバ側のポリシーを満たす認証器であるかを確認する。

⑰ 公開鍵（Credential Public Key）と attestationObject をユーザ ID と紐付けて登録する。

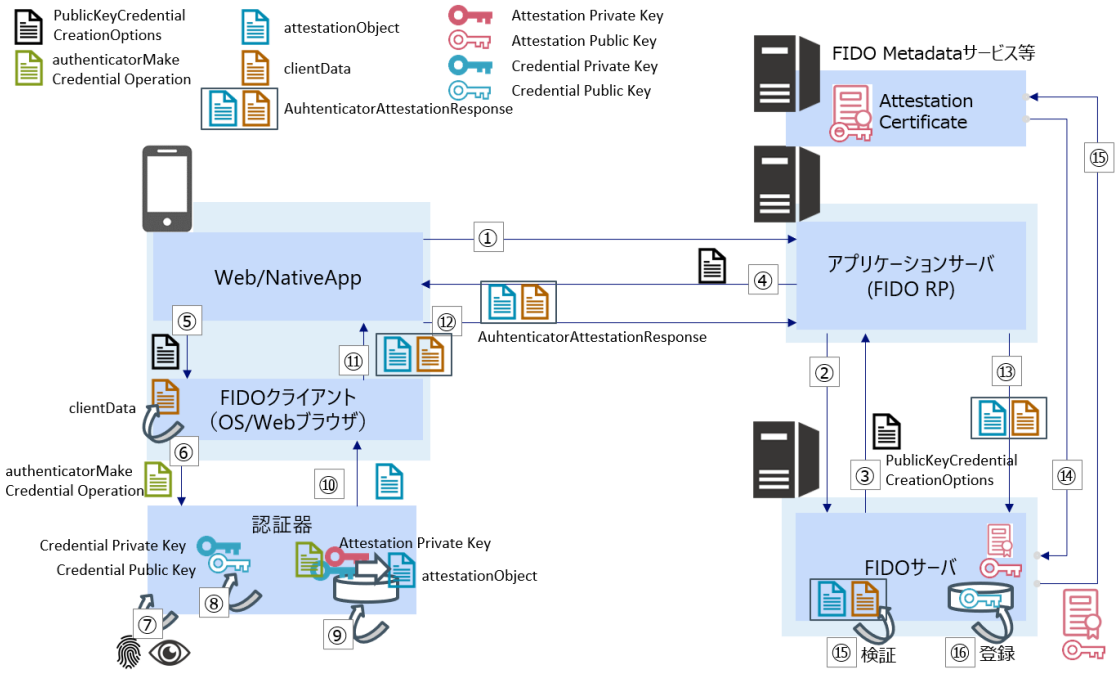


図 1-12：FIDO2 登録時の流れ[58]

登録が完了してからのサービスへのオーセンティケーションの流れは以下の通り。

① ユーザ側からログイン要求をサービス側（RP）に対して行う。
② サービス側のアプリケーションサーバから FIDO サーバに要求を転送する。
③ FIDO サーバからチャレンジと PublicKeyCredential を一意に特定可能な CredentialId を含む PublicKeyCredentialRequestOptions をアプリケーションサーバに送る。
④ アプリケーションサーバから PublicKeyCredentialRequestOptions をユーザ側の Web や NativeApp に送る。
⑤ Web や NativeApp から OS や Web ブラウザに PublicKeyCredentialRequestOptions を送る
⑥ OS や Web ブラウザは PublicKeyCredentialRequestOptions に含まれる CredentialId から登録時に使った認証器を確認し、端末外部の認証器であれば CTAP 経由で、内蔵認証器であれば端末内のプロトコルで relying party id とチャレンジが含まれる clientData のハッシュ値を送る。
⑦ 認証器によってユーザのベリフィケーションを行う。

[58] W3C, “Web Authentication: An API for accessing Public Key Credentials Level 1”をもとに NRI 作成

⑧ 認証器は relying party id から探索した当該サービス用の鍵ペアの秘密鍵で clientData のハッシュ値と、アプリケーションサーバの ID のハッシュ値等を含む authenticatorData を合体させて署名した signature を生成する。

⑨ 認証器から、authenticationData と signature を CTAP 等を経由して OS や Web ブラウザに送る。

⑩ OS や Web ブラウザから clientDataJSON、authenticator Data、signature を併せた AuthenticatorAssertionResponse を Web や NativeApp に送る。

⑪ Web や NativeApp から AuthenticatorAssertionResponse をアプリケーションサーバに送る。

⑫ アプリケーションサーバから FIDO サーバに AuthenticatorAssertionResponse を送る。

⑬ FIDO サーバにて AuthenticatorAssertionResponse が正しく署名されているかを登録している認証器公開鍵を用いて検証する。

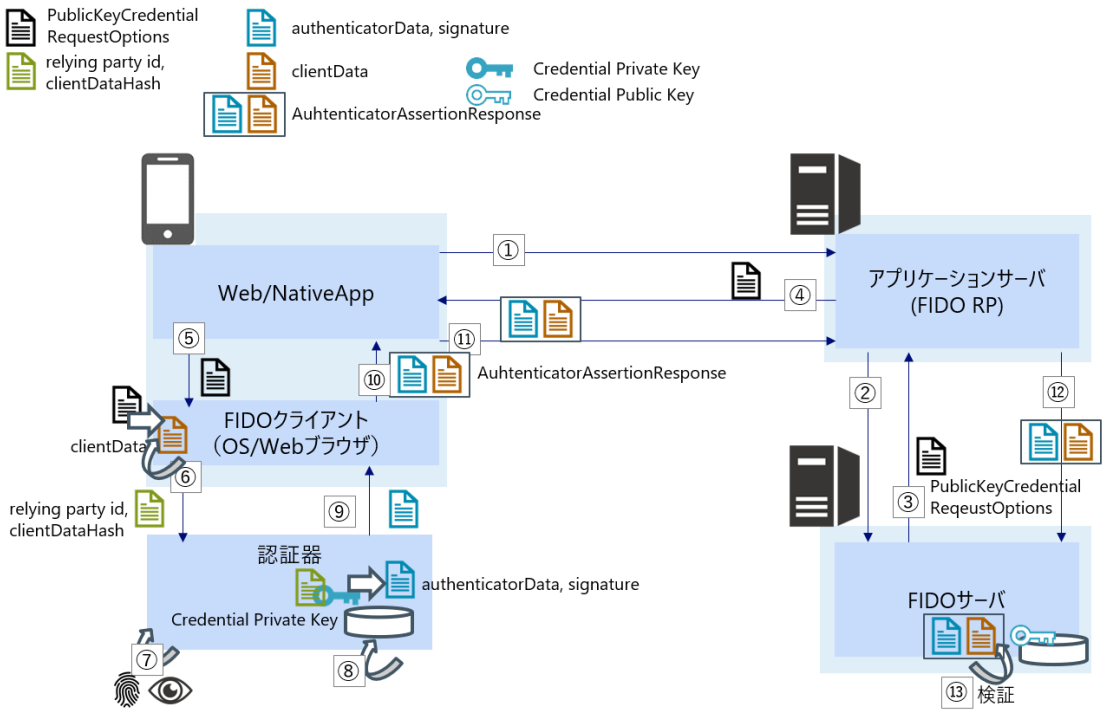


図 1-13：FIDO2 オーセンティケーション時の流れ[59]

FIDO2 の WebAuthn は主要なブラウザで対応しており、ベリフィケーションの認証器についても Android 7.0 以降や Windows Hello といった多くの利用者の端末に備わってい

[59] W3C, “Web Authentication: An API for accessing Public Key Credentials Level 1”をもとに NRI 作成

る指紋認証や顔認証機能を用いることができる。さらに、Web サービスとしては Google、Yahoo! Japan、LINE など主要なサービス事業者が実装し、認証プロトコルとしての FIDO の展開が期待されている。

（3） 認可（OAuth 2.0）

認可プロトコルとは、データやサービスといったリソース[60]を処理するための認可を提供するデータのフォーマットと、そのやり取りをするプロトコルを指す。一般的に使われている OAuth 2.0 は 2012 年に IETF によって RFC6749 と RFC6750 として公開されたものを根幹としている。これは 2006 年時点でアクセス権限を委譲するための標準的な API が存在していなかったことから、そのようなプロトコルを必要とした有志によって策定と公開がされた OAuth Core 1.0 が原点である[61]。

OAuth 2.0 といった認可プロトコルは、特定のリソースにアクセスさせたいアプリケーションに対して、認可の概念を定義した OAuth プロトコルが規定されるまでは ID とパスワードといったクレデンシャルを委ねる必要があった状況から、権限が限定された別のクレデンシャルを提供させるだけで済むようにさせたことでいくつかの問題点を解決した[62]。具体的な問題点としては、アプリケーションに平文のパスワードといったクレデンシャルを保存させてしまうことでアプリケーション側の情報漏えいによってリソースに全面的にアクセスできるクレデンシャルを流出させうることや、アプリケーションに不必要なリソースへのアクセス権限までも与えてしまうといったことが挙げられる。また、アプリケーションによるアクセスを確実に止めさせるにはクレデンシャル（パスワード）を変更する必要があるという問題も存在していた。OAuth 2.0 であれば、このような問題に対してはアプリケーションに与えていた個別のトークンを無効化するだけで済むということで解決する。

OAuth 2.0 では権限が限定された個別のクレデンシャル（トークン）を提供し、アプリケーションの情報漏えい時には全面的な権限を持つクレデンシャルまでは流出せず、不必要なリソースへのアクセスも制限でき、任意のタイミングでクレデンシャルを無効にすることが可能になった。また、同仕様ではリソースの所有権を持つエンティティ（リソースオーナー)、リソースをリソースオーナーに代わって保持と保護するサーバ（リソースサーバ)、リソースオーナーの認可を得たうえでリソースにアクセスしようとするアプリケ

---

[60] OAuth, “Terminology Reference,” https://www.oauth.com/oauth2-servers/definitions/

[61] OAuth, “Introduction,” https://oauth.net/about/introduction/

[62] Internet Engineering Task Force, “Request for Comments: 6749 The OAuth 2.0 Authorization Framework,” https://tools.ietf.org/html/rfc6749

ーション（クライアント）、そして認可のやり取りの機能を提供する認可サーバに役割が分担されている[63]。OAuth 2.0 の大まかな流れは以下の通り。

① リソースにアクセスしたいクライアントがリソースオーナーに対して認可を要求する。
② リソースオーナーはクライアントに、クライアントへの認可を表す認可グラントを提供する。
③ クライアントは自らの情報と共に認可サーバに認可グラントを提示し、アクセストークンを要求する。
④ 認可サーバはクライアントのオーセンティケーションを行い、認可グラントの正当性を確認し、正当なものであることが確認できればアクセストークンをクライアントに対して発行する。
⑤ クライアントはリソースサーバに対してアクセストークンを提示したうえでリソースへのアクセス要求を行う。
⑥ リソースサーバはアクセストークンの正当性を確認し、確認できればリソースへのアクセスをクライアントに提供する。

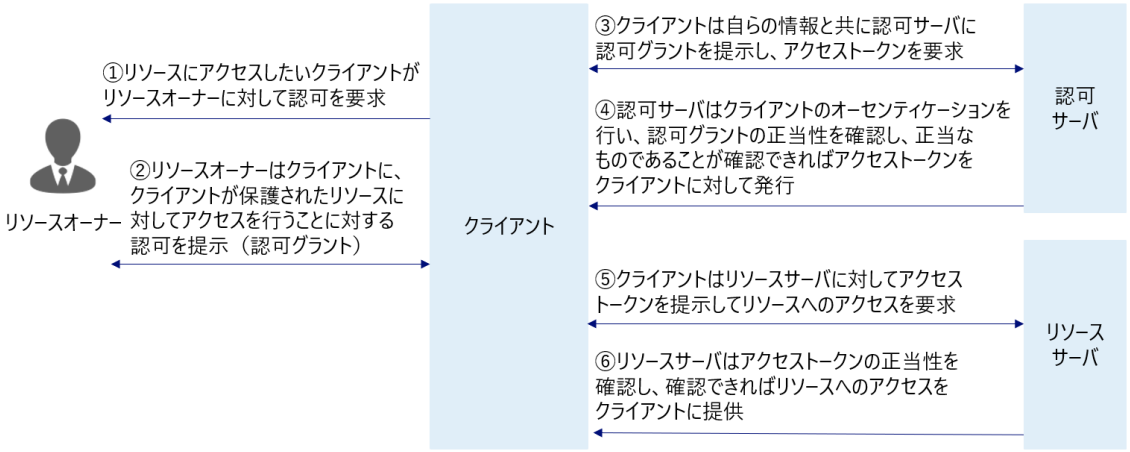


図 1-14：OAuth 2.0 の概観の流れ[64]

なお、リソースオーナーがクライアントに対してリソースへのアクセスを行うことに対する認可を表す認可グラントは認可コード、インプリシット、リソースオーナーパスワー

[63] Internet Engineering Task Force, “Request for Comments: 6749 The OAuth 2.0 Authorization Framework,” https://tools.ietf.org/html/rfc6749
[64] Internet Engineering Task Force, “Request for Comments: 6749 The OAuth 2.0 Authorization Framework,” https://tools.ietf.org/html/rfc6749 をもとに NRI 作成

ドクレデンシャル、クライアントクレデンシャルの 4 種類が RFC6749 では定義されており[65]、さらに OAuth 2.0 での拡張としてのアサーション[66]とデバイス[67]、OpenID Connect での拡張としての CIBA（Client Initiated Backchannel Authentication Flow）[68]とハイブリッドフロー[69]の認可グラントが存在する。それぞれの概要は以下の通り。

表 1-10：認可グラントの種類と概要

認可グラントの種類	概要
認可コード	クライアントがリソースオーナーを認可サーバにリダイレクトさせ、認可サーバがリソースオーナーをオーセンティケーションした上で発行され、リソースオーナーがクライアント側にリダイレクトされた際に届けられる。
インプリシット	クライアントがブラウザ上で実行させる場合を想定。 認可サーバがクライアントのオーセンティケーションを行わず、リソースオーナーからクライアントに対して直接アクセストークンが認可グラントとして提供される。
リソースオーナー パスワードクレデンシャル	クライアントとリソースオーナーの間の信頼性が高く、他の認可グラントが利用できない場合に用いられる。 ID とパスワードが認可グラントとして使われ、クライアントが認可サーバに対してアクセストークンを要求する一度だけ用いられ、要求後は破棄される。
クライアント クレデンシャル	クライアントがリソースオーナーである場合や、リソースがクライアントの管理下にある場合等で用いられる。 認可サーバによるクライアントのオーセンティケーションのみでアクセストークンが提供される。

[65] Internet Engineering Task Force, “Request for Comments: 6749 The OAuth 2.0 Authorization Framework,” https://tools.ietf.org/html/rfc6749

[66] Internet Engineering Task Force, “Request for Comments: 7521 Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants,” https://tools.ietf.org/html/rfc7521

[67] Internet Engineering Task Force, “Request for Comments: 8628 OAuth 2.0 Device Authorization Grant,” https://tools.ietf.org/html/rfc8628

[68] OpenID Foundation, “OpenID Connect Client Initiated Backchannel Authentication Flow - Core 1.0 draft-03,” https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0.html

[69] OpenID Foundation, “OpenID Connect Core 1.0 incorporating errata set 1,” https://openid.net/specs/openid-connect-core-1_0.html

アサーション	アイデンティティアサーションを認可グラントとして用いる。認可サーバはアイデンティティアサーションの正当性を確認できる必要がある。
デバイス認可	画面表示とインターネットへの接続は出来るが、入力のインターフェースが限られている端末がクライアントの場合に用いられる。 認可サーバから端末側にベリフィケーション用の URI とコードを送信し、端末がその URI とコードを表示させ、リソースオーナーがその URI にアクセスし、必要に応じてオーセンティケーションを経てからコードを入力することでアクセストークンが提供される。
CIBA （Client Initiated Backchannel Authentication Flow）	クライアント側が直接リソースオーナーに認可グラントを要求せず、認可サーバに対して通信を行い、認可サーバがリソースオーナーのベリフィケーションを実施したうえでクライアントにアクセストークンを提供する。
ハイブリッドフロー	認可サーバとは別にアクセストークンを発行するサーバがある方式。クライアントが認可サーバに通信を行い、認可サーバがリソースオーナーのベリフィケーションとアクセス認可の同意取得を行い、認可コードがクライアントに渡される。クライアントは認可コードをアクセストークン発行サーバに渡し、アクセストークン発行サーバからアクセストークンを受け取る。

認可サーバによって認可グラントの正当性の確認とクライアントのオーセンティケーションが完了して発行されるアクセストークンには、クライアントがアクセスできるリソースの範囲や期間といった情報の取得方法や、その情報自体が格納されている場合もある。そして、リソースサーバがアクセストークンの正当性を確認できた場合はクライアントに対してリソースへのアクセスを提供する。

認可グラントの種類は複数あるが、Web サービス等で実装されるのは認可コードが多く、参考として認可コードでの流れを以下に示す。

① リソースにアクセスしたいクライアントが、クライアント識別子、アクセスを要求するリソースの範囲、認可サーバからの結果のリダイレクト先 URI の情報をリソースオーナーのユーザエージェントに渡し、ユーザエージェントが認可サーバに遷移する。

② 認可サーバによってリソースオーナーのオーセンティケーションと、クライアントに対してリソースへのアクセスを承諾するかの確認が行われる。
③ リソースオーナーがクライアントによるリソースへのアクセスを承諾した場合、認可サーバが認可コードを発行して、①で受け取ったリダイレクト先 URI に対してリソースオーナーのユーザエージェントを経由して提供する。
④ クライアントは自らの情報と共に認可サーバに認可コードを提示し、アクセストークンを要求する。
⑤ 認可サーバはクライアントのオーセンティケーションを行い、認可コードの正当性を確認し、正当なものであることが確認できればアクセストークンをクライアントに対して発行する。
⑥ クライアントはリソースサーバに対してアクセストークンを提示したうえでリソースへのアクセス要求を行う。
⑦ リソースサーバはアクセストークンの正当性を確認し、確認できればリソースへのアクセスをクライアントに提供する。

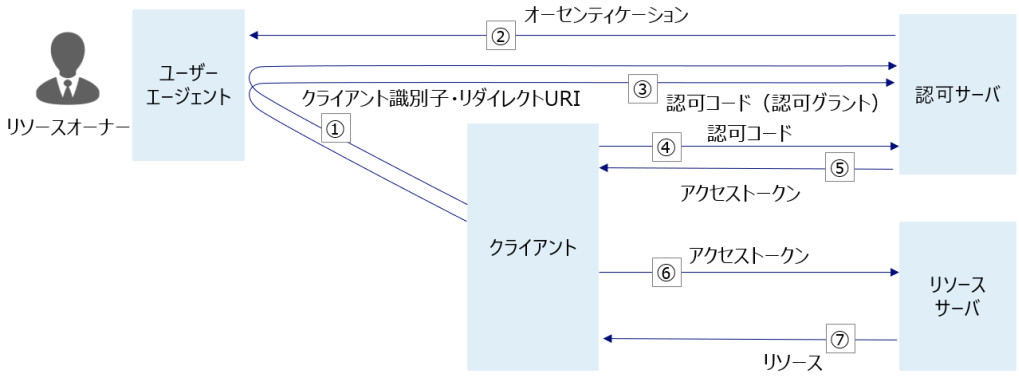


図 1-15：認可コードでの大まかな流れ[70]

また、OAuth 2.0 には安全性向上のための機能拡張の仕様やセキュリティ上のベストプラクティスもいくつか公開されており、代表的なものとしては認可コードの横取り攻撃を防ぐための RFC 7636 の PKCE（Proof Key for Code Exchange by OAuth Public Clients）[71]、ネイティブアプリ向けの実装に関する RFC 8252 の OAuth for Native Apps[72]、そして BCP（Best Current Practice）[73]等が挙げられる。

---

[70] Internet Engineering Task Force, “Request for Comments: 6749 The OAuth 2.0 Authorization Framework,” https://tools.ietf.org/html/rfc6749 の 4.1 Authorization Code Grant をもとに NRI 作成
[71] Internet Engineering Task Force, “Request for Comments: 7636 Proof Key for Code Exchange by OAuth Public Clients,” https://tools.ietf.org/html/rfc7636
[72] Internet Engineering Task Force, “OAuth 2.0 for Native Apps,” https://tools.ietf.org/html/rfc8252
[73] OAuth, “OAuth 2.0 Security Best Current Practice,” https://oauth.net/2/oauth-best-practice/

（4） ID 連携（SAML, OpenID Connect）

ID 連携プロトコルとは、アイデンティティフェデレーションの一種であり、アイデンティティアサーションの手法のプロトコルを指す。代表的なプロトコルとしては SAML（Security Assertion Markup Language）と OIDC（OpenID Connect）が存在する。SAML は OASIS によって 2002 年に 1.0 が公開され、2005 年には最新の 2.0 が公開された[74]。OIDC は 2007 年に発足した OpenID Foundation によって 2014 年に公開された仕様で、前述の OAuth 2.0 を土台としてアイデンティティアサーションを可能としたものになっている[75]。両者はともにエンティティ（ユーザ）の認証結果（オーセンティケーテッドアイデンティティ）や属性情報をアイデンティティマネジメントシステムから RP に連携する（アイデンティティアサーション）という役割を果たす。先に登場した SAML は事前に公開鍵とメタデータの交換を行った上でフェデレーションを行う必要があり、また XML 形式を重視したマークアップ言語の為、より軽量な言語を用いたフェデレーションのプロトコルの登場が期待されていた。OIDC は XML ではなく JSON 形式での軽量なデータ記述を採用した点、RESTful なプロトコルでやり取りが可能と定められている。また、SAML が Web ベースのアプリケーションでの利用を主眼として設計されているのに対して、OIDC はネイティブアプリやモバイルアプリへの対応も見据えられ、より単純に実装が可能となっている[76]。本項ではより広範囲での実装が可能で、今後展開が進んでいくことが見込まれる OIDC を代表的な ID 連携プロトコルとして解説する。

OIDC は「OAuth 2.0 プロトコルの上にシンプルなアイデンティティレイヤーを付与したもの」[77]で、これは OAuth 2.0 がリソースを利用させるための認可付与を取り扱うことを主眼としていたことに対して、認可を行う OpenID Provider（OP、OAuth 2.0 での認可サーバ）によるユーザのオーセンティケーションの結果の取得や、ユーザのアイデンティティ情報もリライングパーティ（RP、OAuth 2.0 でのクライアント）が取得できるようにするという構成になっている。OIDC によって、RP は認可の取得だけでなく、認可サーバである OP にオーセンティケーションを代行してもらうことも可能になる。OP によるオーセンティケーションの情報は JSON Web Token（JWT）形式の「ID トークン」として RP に提供され、RP は ID トークンからトークンの発行元、有効期限、発行日時、オーセンティケーションが実施された日時といった内容を確認できる。また、エンティティ

---

[74] OASIS, “SAML V2.0 Executive Overview,” https://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf

[75] OpenID Foundation, “What is OpenID Connect?,” https://openid.net/connect/

[76] OpenID Foundation, “How does OpenID Connect relate to SAML?,” https://openid.net/connect/faq/

[77] OpenID Foundation, “OpenID Connect Core 1.0 incorporating errata set 1,” https://openid-foundation-japan.github.io/openid-connect-core-1_0.ja.html

（ユーザ）についての情報の部分集合であるクレーム（Claim）[78]は、OAuth 2.0 でのリソースサーバへの要求と同じようにアクセストークンを用いて取得することも、ID トークン自体に格納して OP から RP に直接提供することも可能とも定められている。

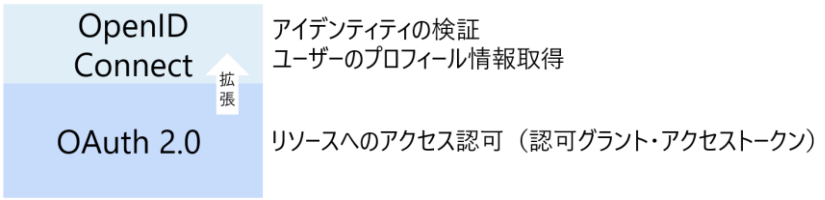


図 1-16：OAuth 2.0 と OIDC の関係概要[79]

OIDC でクライアントがオーセンティケーションの結果とユーザのアイデンティティ情報を取得するまでの大まかな流れは以下の通りである[80]。なお、前述した通り③の ID トークンにユーザの情報を格納することも可能だと OIDC では定められている。

① RP が OP（OAuth 2.0 での認可サーバ）に対して要求を出す。
② OP はユーザのオーセンティケーションを行う。
③ OP が ID トークンとアイデンティティ情報へのアクセストークンを RP に対して発行する。
④ RP はユーザのアイデンティティ情報を保持しているリソースサーバ（OP と同一の場合もある）に対してアクセストークンを提示したうえでアイデンティティ情報の要求を行う。
⑤ リソースサーバはアクセストークンの正当性を確認し、確認できればユーザの情報の集合体であるクレームを RP に提供する。

---

[78] OpenID Foundation, “OpenID Connect Core 1.0 incorporating errata set 1,” https://openid.net/specs/openid-connect-core-1_0.html

[79] OpenID Foundation, “What is OpenID Connect?,” https://openid.net/connect/ をもとに NRI 作成

[80] OpenID Foundation, “OpenID Connect Core 1.0 incorporating errata set 1,” https://openid.net/specs/openid-connect-core-1_0.html

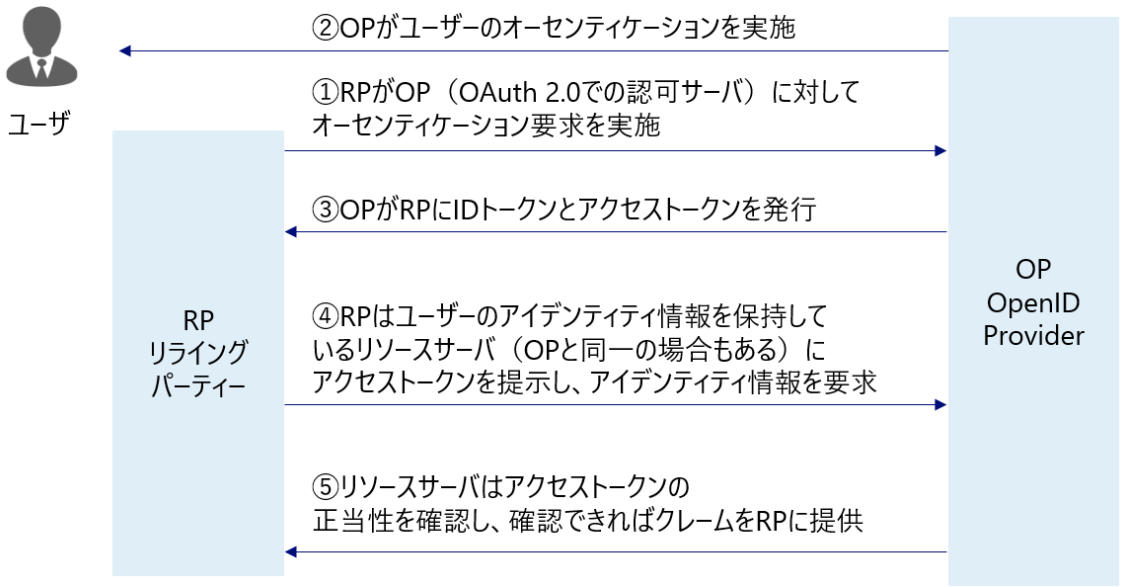


図 1-17：OIDC の大まかな流れ[81]

OIDC でのオーセンティケーション方法の種類は複数あり、参考として認可コードでの流れを以下に示す。

① エンドユーザが RP にログイン要求をする。
② RP が、クライアント識別子、アクセスを要求するリソースの範囲、OP からの結果のリダイレクト先 URI の情報をエンドユーザのユーザエージェントに渡し、ユーザエージェントが OP に遷移する。
③ OP はユーザのオーセンティケーションと、RP に対してアイデンティティ情報へのアクセスを承諾するかの確認が行う。
④ エンドユーザが RP によるアイデンティティ情報へのアクセスを承諾した場合、OP が認可コードを発行して、②で受け取ったリダイレクト先 URI に対してエンドユーザのユーザエージェントを経由して提供する。
⑤ RP は自らの情報と共に OP に対して認可コードを提示したうえで ID トークンとアクセストークンの要求を行う。
⑥ OP は RP のオーセンティケーションを行い、認可コードの正当性を確認し、正当なものであることが確認できれば ID トークンとアクセストークンを RP に対して発行する。

[81] OpenID Foundation, “OpenID Connect Core 1.0 incorporating errata set 1”の 1.3 Overview https://openid.net/specs/openid-connect-core-1_0.html をもとに NRI 作成

⑦ RP はアイデンティティ情報を保持しているリソースサーバ（OP と同一の場合もある）に対してアクセストークンを提示したうえでアイデンティティ情報へのアクセス要求を行う。

⑧ リソースサーバはアクセストークンの正当性を確認し、確認できればアイデンティティ情報へのアクセスをクライアントに提供する。

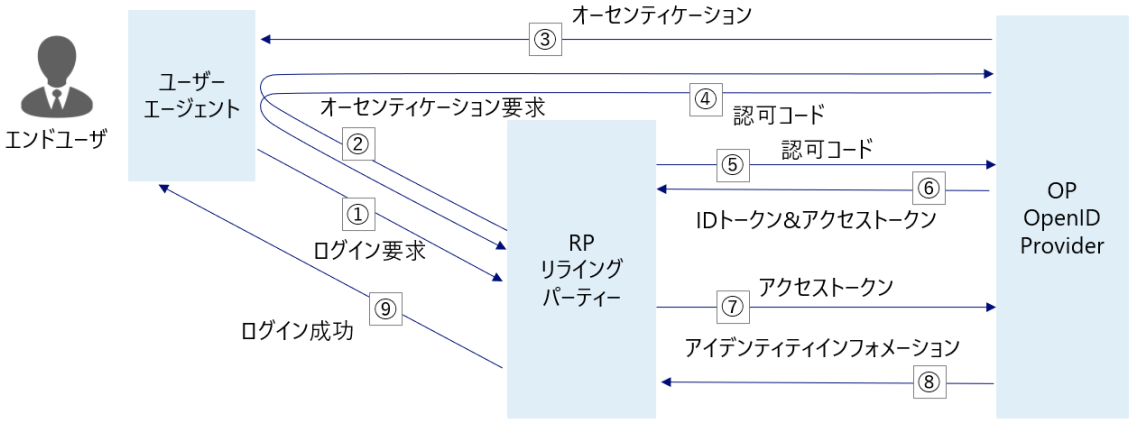


図 1-18：認可コードでの OIDC の大まかな流れ[82]

上述した OIDC の手順によって、RP が ID トークンもしくはアイデンティティ情報を保持しているリソースサーバからエンティティについての情報の集合体であるクレームとしてアイデンティティアサーションできうる記述項目を以下に紹介する。なお、OP はこれらの一部を RP に提供しない場合も、逆にここに記載されていない属性を提供する場合もある。

表 1-11：OIDC におけるクレーム例

クレーム名	概要
sub	OP によってユーザを識別するための値
name	フルネーム
given_name	名
family_name	性
middle_name	ミドルネーム
nickname	ニックネーム
preferred_username	ユーザが定めるユーザ名
profile	プロファイルへの URL

[82] OpenID Foundation, “OpenID Connect Core 1.0 incorporating errata set 1”の 3.1 Authentication using the Authorization Code Flow https://openid.net/specs/openid-connect-core-1_0.html をもとに NRI 作成

picture	プロファイル画像の URL
website	Web サイトやブログへの URL
email	ユーザが登録したメールアドレス
email_verified	メールアドレスのベリフィケーションがなされたか（true ないし false）
gender	ジェンダー
birthdate	生年月日
zoneinfo	タイムゾーン
locale	地域
phone_number	ユーザが登録された電話番号
phone_number_verified	電話番号のベリフィケーションがなされたか（true ないし false）
address	住所
updated_at	クレームが最後に更新された日時

1-2-3. デジタルアイデンティティのガバナンスフレームワーク

IMS を適切に運用していくにあたっては、標準プロトコル等の技術要素だけではなく、ガバナンスの要素も踏まえた設計・運用が重要となる。デジタルアイデンティティのガバナンスに関するルールとして、諸外国では「トラストフレームワーク」という名称で策定・公表されているものが多い。例えば、国際非営利団体の Open Identity Exchange(OIX)は、トラストフレームワークを「ユーザや組織、サービスそしてデバイスが相互にトラストできるようにするためのルール体系に基づきガバナンスされたアイデンティティトランザクションのための環境」と定義し、以下の項目についてのルール/ガイドを作成・公表している。

表 1-12　OIX のトラストフレームワークで規定される構成要素[83]

構成要素	項目
原則	
トラストマークと UX	
役割と義務	
一般ルール	記録保存と監査証跡
	不正行為とサイバーコントロール
ユーザサービス	デジタルアイデンティティの選択
	ID の作成＆管理

[83] OIX," OIX Guide to Trust Frameworks(version 0.1 Beta)"をもとに作成。

	トラストの獲得と提示
	同意
	ヘルプ＆サポート
リライングパーティサービス	アイデンティティサービスへのユーザアクセス
	レクエスト＆レスポンス(API)
	RP による ID 保証
	ライアビリティ
	サービスレベル
	ヘルプ＆サポート
トラストルール	プルーフィング
	アイデンティティ保証
	認証
	適格性保証
技術・セキュリティ要件	セキュリティルール
	エコシステム参加者のトラストレジストリ
	証跡の記録と提示
	リクエスト及びレスポンススキーム
相互運用性	内部の相互運用性
	外部の相互運用性
ガバナンス	トラストフレームワークの構築と管理
	トラストフレームワークの強制力
	トラストフレームワークの認証
	トラストフレームワークの運用

このように多くの国では政府機関や民間事業者等が適切に IMS を運用するためのガバナンスフレームワーク（トラストフレームワーク）を策定・発行しており、現在主に以下のようなガバナンスフレームワークが策定・利用されている。なお、日本においては、犯罪収益移転防止法や携帯電話不正利用防止法、電子署名法等で本人確認に関する要件は規定されているが、デジタルアイデンティティ全般のガバナンスフレームワークは存在していない。

表 1-13　デジタルアイデンティティの主なガバナンスフレームワーク

分類	国	発行組織	ガバナンス フレームワーク	概要

政府	米国	NIST	NIST SP800-63 シリーズ(2017)	アメリカ国立標準技術研究所(NIST)は商務省(Department of Commerce)傘下の米国の政府機関で、米国における各種標準を策定する組織。 アイデンティティの分野については、「電子的認証に関するガイドライン」が策定されており、政府機関のみならず民間部門も含めて広く参照されるガイドラインとなっている。 電子的認証に関するガイドラインは以下の通り 。 SP 800-63-3 (June 2017) Digital Identity Guidelines SP 800-63A (June 2017)Enrollment and Identity Proofing SP 800-63B (June 2017)Authentication and Lifecycle Management SP 800-63C (June 2017)Federation and Assertions
	EU	European Commission (DG CONNECT)	eIDAS	eID（電子本人確認）とｅトラストサービス（電子署名、電子シール、タイムスタンプ、電子配布、ウェブサイト認証等）について定めたもので、EU加盟国に法律として適用される。 (2014 年 7 月 23 日批准) 2020 年 7 月に eIDAS 改定に向けたパブリックコンサルテーションを開始。
	豪州	デジタルトランスフォーメーション庁	Trusted Digital Identity Framework	豪州のデジタルトランスフォーメーション庁は、2018 年 2 月に Trusted Digital Identity Framework(TDIF)を公表。デジタルアイデンティティサービスのプロバイダの認証の基準やルールを規定。
	英国	デジタル・文化・メデ	UK Digital Identity and	2021 年 2 月にしたデジタルアイデンティティを活用する事業者（アイデン

		ィア・スポーツ省	Attributes Trust Framework	ティティサービスプロバイダー、アトリビュート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ー、リライングパーティ）向けのガイドライン（アルファ版)。将来的にプロバイダの認証を行うことを目指し、必要となる要件などについて明記。
団体	カナダ	DIACC	Pan-Canadian Trust Framework (PCTF) 1.0 alpha (Nov. 2020)	・DIACC はカナダ財務省のタスクフォースでの提言を受け 2012 年に設立された非営利団体。 ・PCTF はカナダの政府機関や民間事業者がデジタルアイデンティティを利用する際のフレームワークとして策定。
	—	OIX	OIX Guide to Trust Framework version 0.1 BETA (July 2020)	・OIX は 2010 年に発足した非営利団体。米国政府の要望により、OpenID Foundation と Information Card Foundation の資金等をもとに設立。 ・トラストフレームワークは、デジタルアイデンティティを活用する事業者向け、原則や内容、責任などについて具体的に既定。
	—	Sovrin	The Sovrin Governance Framework (SGF)	・Socrin Foundation は、2016 年に設立された非営利組織。Sovrin ID や分散ネットワークである Sovrin Network の開発を運用を目的に設立。 ・SGF は Sovrin Networkno グローバルでの利用を目的に策定され、利用原則やポリシー、Trust Assurance Framework などが含まれる。

デジタルアイデンティを適切に運用するにあたっては、各国の法規制等への遵守と併せて、これらガバナンスフレームワークへの遵守も期待される。

1-3.　自己主権型/分散型アイデンティティ

1-3-1. 既存主要モデルへの懸念

1-2-1 で整理した通り、現在主流となっているフェデレーションモデルは、国内外の企業・組織、そして個人ユーザに浸透し、デジタルアイデンティティの利便性は向上してきた。しかしながら、その結果協力な顧客接点を持つ一部の大手プラットフォーム事業者にユーザ情報が集約され、大手プラットフォーム事業者に対する安全なアイデンティティ管理への懸念が指摘されるなど、課題も出てきている。

フェデレーションモデルのような特定のアイデンティティプロバイダ（IdP）に依存することのリスクとしては、例えば①IdP にアカウント停止されるリスク（悪意ある IdP が故意に停止したり、倒産等で停止される等）であったり、②（悪意を持った）アイデンティティプロバイダにアイデンティティを改ざんされるリスクなどが想定される。このような懸念を解決するためのアイデンティティ管理の思想として、「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）」が近年注目を集めている。

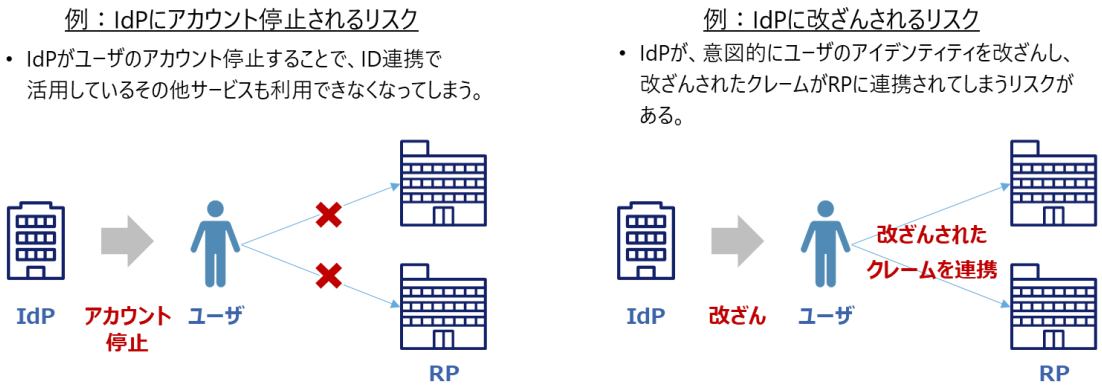


図 1-19：　既存 ISM モデルのリスク（例）

1-3-2. SSI/DID の概要

SSI とは、アイデンティティの管理主体が介在することなく、個人が自分自身のアイデンティティをコントロールできるようにすることを目指す思想である[84]。この思想のもと、SSI

[84] 例えば、Sovrin 財団は、SSI を以下のように定義している。
「自己主権型アイデンティティ（Self-Sovereign Identity：SSI）とは、行政当局の介入を受けずに個人が自分のアイデンティティを所有・管理すべきであると認識するデジタルムーブメントを表す言葉です。SSI は、人々がデジタルの世界で、オフラインの世界と同じ自由と信頼の能力を持って交流することを可能にする。」

では、ユーザが自分の属性情報に関するコントロール権を確保の上、信頼できる組織から発行された本人の属性情報を取得し、ユーザの許可した範囲でサービスプロバイダー等の組織（RP）に連携する。

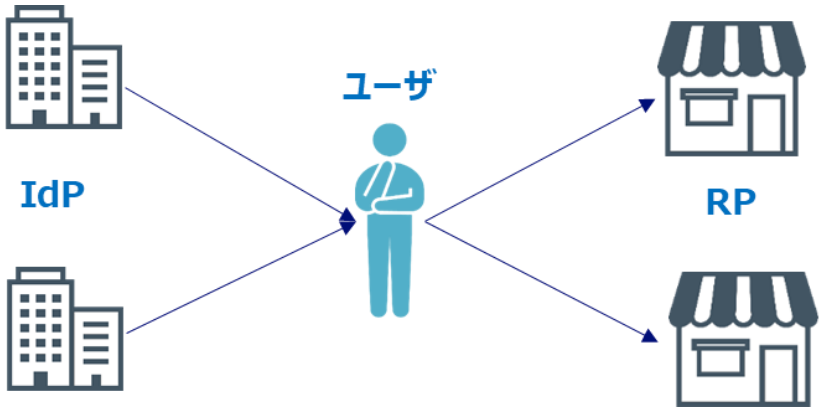


図 1-20：SSI の概念図

自分自身でデジタルアイデンティティを自己制御できることを目的とする SSI に対し、分散型アイデンティティ（Decentralized Identity:DID）は、ユーザのデジタルアイデンティティが特定の IdP 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である。実現にあたり、ブロックチェーン等の分散レポジトリの活用が提唱されることが多い[85]。

Sovrin Foundation, “What is self-sovereign Identity?,” Dec. 2018
https://sovrin.org/faq/what-is-self-sovereign-identity/

[85] 例えば、分散型アイデンティティのホワイトペーパーを公表しているマイクロソフトは以下のように定義している。
「分散型アイデンティティとは、ユーザ名などの識別子を、自己所有の独立した ID に置き換え、ブロックチェーンや分散型台帳技術を用いてデータ交換を可能にする」
Microsoft,
https://www.microsoft.com/en-us/security/business/identity-access-management/decentralized-identity-blockchain

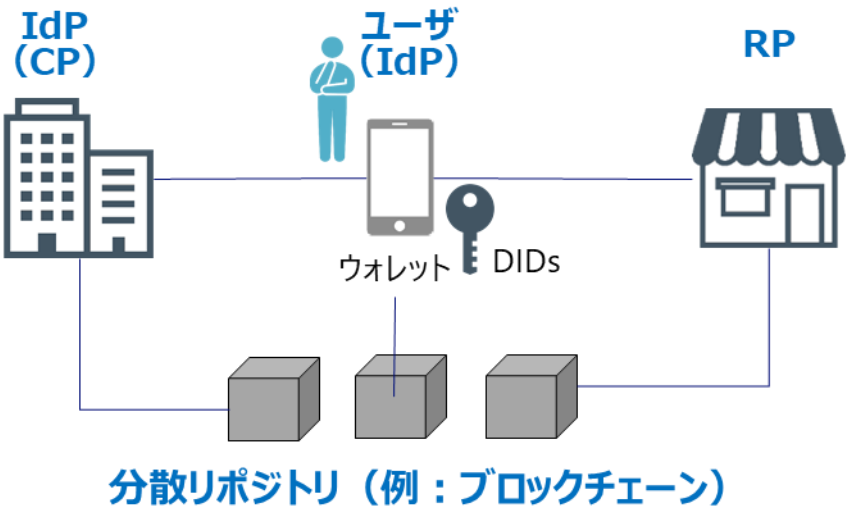


図 1-21：DID の概念図

1-1-3 で紹介した「アイデンティティの 7 原則」を提唱した、Kim Cameron 氏は、「アイデンティティの 7 原則」をベースにした以下の「SSI の 7 原則」を提示している。

表 1-14：SSI の 7 原則[86]

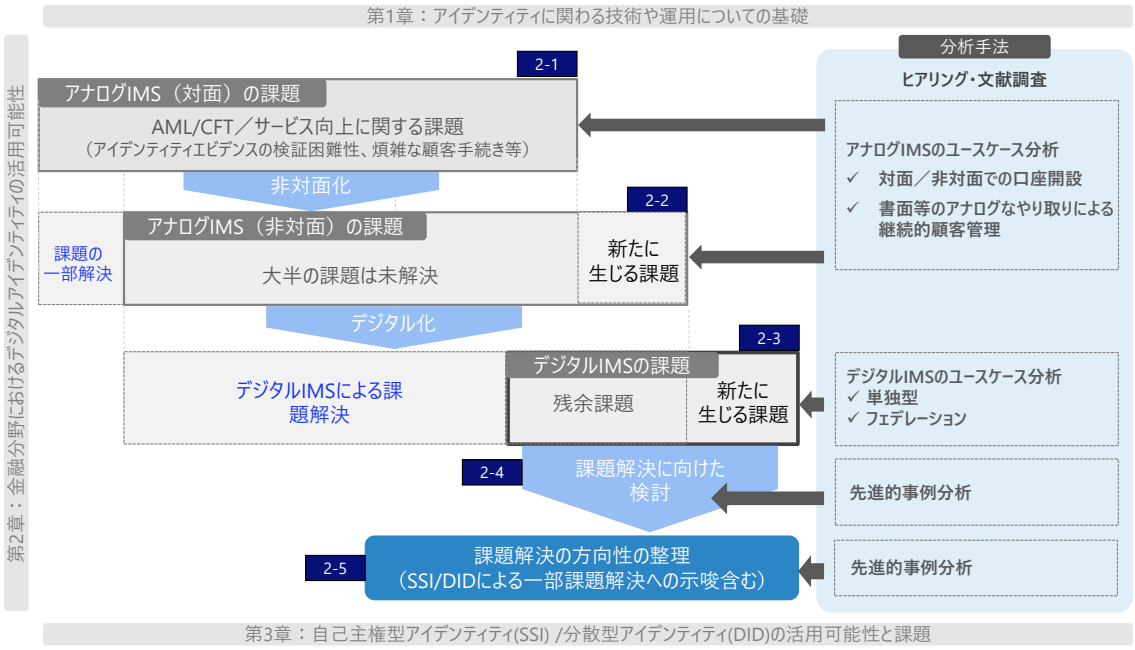
#	原則	内容
1	ユーザによる制御と同意	アイデンティティ・システムは、ユーザの同意がなければユーザを識別する情報を開示すべきではない
2	限定された用途で最低限の公開	最も安定し、長期にわたって使用できるソリューションとは、開示するアイデンティティ情報を最小限にし、情報へのアクセスを適切に制限するソリューションである
3	正当な関係者の身への情報開示	アイデンティティ・システムは、特定の状況において識別情報を必要とし、かつ入手できる正当な権利を持つ関係者のみに対して情報を開示するように設計されなければならない
4	方向づけられたアイデンティティ	アイデンティティ・システムは、公に使用する「全方位的」な識別子とプライベートで使用する「特定の方向性」を持った識別子の両方をサポートしなければならない。このことにより公共性を維持しながら不必要に関連付けの公開を防止できる

[86] 崎村夏彦、「The Law of Identity in SSI Era by Kim Cameron」をもとに NRI 作成。
https://nat.sakimura.org/2020/06/23/the-law-of-identity-in-ssi-era-by-kim-cameron/

5	**「アイデンティティハブ」の統合**	**ユーザは、プロバイダ間で一貫した方法で自分自身を表現し、アイデンティティを使用することができ、同時にコンテキスト間でアイデンティティを分離することができる**
6	**長期のアイデンティティの安定性に向けた DID の統合**	**個人データを事業者に依存しない形で保管したうえで、アイデンティティ事業者を存続させ、サービスとの関係を維持する**
7	人間の統合	アイデンティティ・システムは、利用者たるユーザを分散システムの 1 つのコンポーネントとして定義しなければならない。明確なマンマシン・インターフェイスを策定してユーザを分散システムに統合し、アイデンティティを保護しなければならない

アイデンティティの 7 原則のうち、「#5 複数のアイデンティティプロバイダと技術の相互運用性」と「#7 シンプルで一貫性のあるユーザエクスペリエンス」が、「#5 アイデンティティハブの統合」と「長期のアイデンティティの安定性に向けた DID の統合」に置き換わっていることが分かる。この 2 点が示唆することの詳細については改めて第 3 章にて詳述する。

第２章　金融サービスにおけるデジタルアイデンティティの活用可能性



第 1 章では、デジタルアイデンティティに関わる技術動向の概要を整理した。デジタルアイデンティティの活用が進展している一方で、IdP への情報の一極集中などの課題も指摘され、アイデンティティ管理の形態に変化が起きているという社会全体の流れについても概観した。

本章では、第 1 章の考察を元に、金融という特定分野でのデジタルアイデンティティの活用可能性と課題について論じる。金融分野におけるデジタルアイデンティティの活用を論じるにあたっては、金融機関におけるアイデンティティ管理の概略を理解する必要がある。そのため、まず、2-1 で、金融機関におけるアイデンティティ管理がどのような局面で実施されているのか、その実態を明らかにする（例：AML/CFT 対応、顧客へのサービス提供）。その上で、アイデンティティ管理の各局面において、従来の対面・アナログのプロセスによるアナログアイデンティティ管理を想定して課題を抽出する。ただし、足下では、金融機関によっては非対面でのアイデンティティ管理に重心を移している先も増えてきており、ネット専業の銀行や証券会社だけでなく、店舗を中心にサービスを提供する金融機関についても、非対面での口座開設や取引を積極的に推奨している。これを受けて、2-2 では、非対面でのアイデンティティ情報等のやりとりをアナログで行うアイデンティティ管理の課題について検討を行う。

次いで、2-3 では、2-1、2-2 で挙げられた課題の解決方策を検討する。アナログ中心の IMS の課題のいくつかについては、その解決のためにデジタル化が必要と考えられる。こ

こでは、デジタル IMS への移行で従来のアナログ IMS における課題がどのように解決されるのか、一方でデジタル IMS を活用しても残る、あるいは新たに発生する課題を整理する。

以上の 2-1 から 2-3 の分析の結果、デジタル IMS 活用時の課題として、利用する業務に応じた IAL の定義やデジタルアイデンティティ連携時における責任分界等の法的課題、セキュリティ確保等の技術的課題、新しい業務への投資等のビジネス面の課題、等が明らかとなった。2-4 では、これらの課題に対しての解決、取り組み事例を、主に海外事例を素材として整理する。ここで挙げられている先進事例は、わが国における取組を考えるにあたって大いに参考になるものと考えられる。

最後に 2-5 では、2-4 の事例等を参考にしながら、2-3 で挙げられた課題に対する解決の方向性を提示するとともに、ステークホルダーの視点での課題解決の意味や課題解決の過程で新たに発生すると考えられる利害関係を整理する。これにより、複数のステークホルダー間の利害を調整しながら解決に取り組む、マルチステークホルダーアプローチによる解決が必要な課題が抽出されることになる。

本章での検討、分析の結果として得られる結論は以下のようなものである。すなわち、金融分野においてもデジタルアイデンティティの重要性は認識されており、現状の金融機関のアナログ IMS に対する課題解決への期待も大きいことから、今後、金融分野におけるデジタルアイデンティティの普及に向けた取り組みは進んでいく可能性が高い。しかしながら、デジタル IMS の導入にあたっては、後述の通り、導入前や導入後に多くの課題が生じる。一部の課題については、ステークホルダー間で利害調整が必要となるものも存在することから、その解決には、SSI/DID の活用を含め、マルチステークホルダーアプローチによる合意形成を通じて課題解決を模索する必要がある。

調査方法について

本金融分野におけるデジタルアイデンティティの活用については、規制面、顧客利便性向上や金融機関のコスト削減といった様々な観点から、多様な立場の関係者が関心を寄せている。本研究では、ステークホルダーを切口に、規制当局側の立場、民間側の立場から、金融分野におけるデジタルアイデンティティ活用のユースケース、ユースケースにおける活用の効果という観点で整理・分析を行った。なお、ユースケース分析にあたっては、金融機関の中でも銀行（預金取扱金融機関）の業務を主に想定した調査分析を実施した。

具体的な手法としては、以下の 3 つの方法を中心に調査分析を実施している。

① 国内・海外有識者へのヒアリング調査
② デジタルアイデンティティ関連調査研究論文の文献調査
③ デジタルアイデンティティを活用した先進的事例の分析

① 国内・海外有識者へのヒアリング調査

アイデンティティ管理の課題については、金融機関が日々直面し、その課題解決の必要性を実感しているものである。そこで、本章の調査分析では、アイデンティティ管理における業務上の課題、法的課題、技術的課題の抽出、およびデジタルアイデンティティ活用における先進事例調査実施のため、下記のとおり、多分野の対象先に対してヒアリングを実施している。

表 2-1　国内・海外有識者へのヒアリング調査内容

区分	対象先	主なヒアリング内容
国内	金融機関 法曹関係者 ソリューションベンダー	• AML/CFT 業務を中心とした、アイデンティティ管理の現状業務の課題 • デジタルアイデンティティ活用についての現在の取り組み・課題・今後の展望 • デジタルアイデンティティ活用時の法的・技術的課題
海外	金融機関 政府当局/関連団体 国際機関 業界団体 標準化団体 個別ベンダー	• デジタルアイデンティティ活用に関する現在の取り組み・課題・今後の展望 • 顧客利便性向上に資する具体的な活用事例とその課題 • リスクベース・アプローチの高度化や金融包摂に向けてのインプリケーション • 規制整備/規制対応の状況・今後の展望 • 技術標準化動向

② デジタルアイデンティティ関連調査研究論文の文献調査

既存研究の整理にあたり、民間側の立場においては、2010 年代後半頃から個別金融機関（BBVA[87]、MasterCard[88]等）や標準化団体（OIX[89] 等）、民間コンサルティング会社（PwC[90]、Mckinsey Global Institute[91] 等）において研究がなされてきた。その後、業界団体等でも研究が進展し、2019 年に、70 カ国を超える国の 500 近い民間の金融機関が参加する Institute of International Finance（IIF）が、デジタルアイデンティティと金融分野の関係についてシリーズ論文 Digital Identities in Financial Services を公表した[92][93][94]。本シリーズは、現時点でのデジタルアイデンティティに関わる民間分野での活用可能性に関する研究を包括的にとらえているため、同シリーズ及び参照文献を調査する形で整理を進めた。一方、規制当局側は、前述の IIF 論文の中でも言及があったマネー・ローンダリング対策（AML）につき、FATF が 2020 年 3 月に公表した Guidance on Digital Identity を軸に、本文及び参照文献を中心に調査を行った。

上記規制当局側の立場および民間側の立場の双方から研究対象論文を選定することにより、デジタルアイデンティティの活用において関係するステークホルダーの視点から、既存

---

87 BBVA, “Digital Identity: the current state of affairs” （Feb. 2018）
https://www.bbvaresearch.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf

88 Mastercard, “Digital Identity ： Restoring Trust in a Digital World” （ Mar. 2019 ）
https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf

89 OIX, “The value of digital identity to the financial service sector” （Dec. 2016）
https://oixuk.org/wp-content/uploads/2017/01/The-value-of-digital-identity-to-the-financial-service-sector-Summary.pdf

90 PwC, “The Future of Onboarding” （Dec. 2016）
https://www.pwc.com/il/he/bankim/assets/pwc-the-future-of-onboarding.pdf

91 MGI, “Digital identification: A key to inclusive growth” （Apr. 2019）
https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth#

92 IIF, “Digital Identities in Financial Services Part 1: Embedding in AML Frameworks” （Aug. 2019）
https://www.iif.com/Portals/0/Files/content/Innovation/08272019_iif_digital_id_part_1.pdf

93 IIF, “Digital Identities in Financial Services Part 2: Responsible Digital Identities, The Key to Creating More Inclusive Economies” （Oct. 2019）
https://www.iif.com/Portals/0/Files/content/Innovation/10142019_responsible_digital_ids.pdf

94 IIF, “Digital Identities in Financial Services Part 3: The Business Opportunity for Digital Identity” （Mar. 2020）
https://www.iif.com/Portals/0/Files/content/Innovation/03_06_2020_%20difs.pdf

研究を包括的に整理を行った。具体的には、FATF と IIF のほか、OIX、 WorldBank 等のデジタルアイデンティティ分野で研究成果をあげている団体の研究結果に対する調査も行った。

金融分野におけるデジタルアイデンティティ活用に係る既存研究の主な対象文献を以下に示す。

表 2-2　調査を行った主な文献一覧

組織名	立場	組織概要	レポート名	公表日	目的・位置づけ
PwC	民間	ロンドンを本拠地とする会計監査、ディールアドバイザリー、ビジネスコンサルティング、税務、法務などに手掛ける総合ファーム	The Future of Onboarding[95]	2016 年	Onboarding プロセスについて、デジタルアイデンティティ活用の現状及び展望を整理し、エストニアや Gov.UK Verify を事例として挙げ、特に Gov.UK Verify については、バイオメトリックスを活用した認証の高度化やコスト削減効果について言及。また、効果的で継続的なモニタリングを可能にするために十分な情報を収集することの重要性についても言及
BBVA	民間	スペイン・バスク自治州・ビルバオに本社を持つ銀行グループ	Digital Identity: the current state of affairs[96]	2018 年 2 月	デジタルアイデンティティの重要性を経済活動、金融活動、社会活動の発展の側面から分析し、有効なアイデンテ

[95] The Future of Onboarding
https://www.pwc.com/il/he/bankim/assets/pwc-the-future-of-onboarding.pdf

[96] Digital Identity: the current state of affairs
https://www.bbvaresearch.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf

					ィティソリューションのあり方を議論
OIX	民間	UK を拠点とする、ID セクターで協力するためのコミュニティを作成し、ID トラストを推進する	The value of digital identity to the financial service sector[97]	2016 年	信頼できるオンライン取引を可能にするために、金融サービス部門で直面している課題に対し、政府公認のデジタル ID の活用が解決策になるかを、顧客調査等の実施により検証
			Digital Identity in the UK: The cost of doing nothing[98]	2018 年	デジタルアイデンティティの適用において、適用した場合の効果・利益と利用しない場合に今後発生する追加コストを比較検証
IIF	民間	1983 年に設立され、70 カ国を超える国の 500 近い民間の金融機関が参加する国際的組織。金融業界の健全な発展のためのリスク管理や支援を行い、業界を代表する機関として、金融に関する規制や	DIGITAL IDENTITY: KEY CONCEPTS[99]	2019 年 7 月	デジタルアイデンティティに関する 3 部構成の論文を発表する前のイントロ。デジタルアイデンティティの特徴等の概説
			Digital Identities in Financial Services Part 1: Embedding in	2019 年 8 月	デジタルアイデンティティを AML に活用する方法について、各国規制当局者や金融機関等のステークホルダーが考慮すべき点の考察

[97] The value of digital identity to the financial service sector
https://oixuk.org/wp-content/uploads/2017/01/The-value-of-digital-identity-to-the-financial-service-sector-Summary.pdf

[98] Digital Identity in the UK: The cost of doing nothing[98]
https://oixuk.org/wp-content/uploads/2018/04/Cost-of-Doing-Nothing-FINAL3v3b.pdf

[99] DIGITAL IDENTITY: KEY CONCEPTS
https://www.iif.com/Publications/ID/3425/IIF-Series-on-Digital-Identity---Key-Concepts

		基準の導入を政策当局などに提唱	AML Frameworks[100]		
			Digital Identities in Financial Services Part 2: Responsible Digital Identities, The Key to Creating More Inclusive Economies[101]	2019年10月	金融機関がデジタルアイデンティティを活用し、金融包摂を推進するための検討事項を、新興国での取組事例等を交えて考察
			Digital Identities in Financial Services Part 3: The Business Opportunity for Digital Identity[102]	2020年3月	デジタルアイデンティティが、金融機関に新たなビジネス機会をどのように 創出していくかを考察
FATF	規制当局	1989 年に開催されたアルシュ・サミットでの経済宣言を受けて設立された、マネー・ローンダリング対策における	FATF （2013-2017），Anti-money laundering and terrorist financing measures and	2017年11月	金融犯罪対策の有効性を損なうことなく金融包摂の目標を達成するための AML/CFT 措置の設計指針を提供すること、を目的とした2013年FATFガイダン

[100] Digital Identities in Financial Services Part 1: Embedding in AML Frameworks[100]
https://www.iif.com/Portals/0/Files/content/Innovation/08272019_iif_digital_id_part_1.pdf

[101] Digital Identities in Financial Services Part 2: Responsible Digital Identities, The Key to Creating More Inclusive Economies
https://www.iif.com/Portals/0/Files/content/Innovation/10142019_responsible_digital_ids.pdf

[102] Digital Identities in Financial Services Part 3: The Business Opportunity for Digital Identity
https://www.iif.com/Portals/0/Files/content/Innovation/03_06_2020_%20difs.pdf

		国際協調を推進するための政府間組織	financial inclusion - With a supplement on customer due diligence[103]		スの補完版。リスクに応じたレベルの顧客確認による顧客受入等を、デジタルアイデンティティィに特化せず議論
			Guidance on Digital Identity[104]	2020年3月	政府機関、金融機関、デジタルアイデンティティサービスプロバイダー向けに、デジタルアイデンティティのAMLに活用する際の考慮次項・検討指針等を広範囲に提供。新規口座開設時の検討事項を中心に、継続的顧客管理や他社によるデジタルアイデンティティ発行も範囲として検討
ACAMS	民間	金融犯罪対策に従事するプロフェッショナル向けの世界最大の会員制組織	Digital Identity and Financial Crimes[105]	2019年9月	デジタルアイデンティティソリューションにより、適切なAMLモニタリングをどのようにして確保できるかの考察
World Bank	国際団体	World Bank Groupは、貧困削	Public Sector Savings and	2018年	政府が提供するデジタルIDシステムが公共部

[103] FATF （2013-2017）, Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence
https://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf

[104] Guidance on Digital Identity
http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf

[105] Digital Identity and Financial Crimes
https://www.acamstoday.org/digital-identity-and-financial-crimes-2/.

Group ID4D		減と持続的成長の実現に向けて、途上国政府に対し融資、技術協力、政策助言を提供する国際開発金融機関 ID4D は World Bank Group に属し、グローバルな知識と専門性を分野横断的に提供し、各国がデジタル ID システムの変革の可能性を実現できるよう支援を実施	Revenue from Identification Systems:Opportunities and Constraints[106]		門にコスト削減や収入を生み出す（あるいは制限する）可能性のある特徴、メカニズム、条件など、公共部門がデジタル ID システムへの投資を行う際の潜在的な財政的利益を分析するためのフレームワークを構築することを目的に発行
			Private Sector Economic Impacts from Identification Systems[107]	2018 年	政府が提供する、あるいは政府が認知した ID システムが民間セクターにもたらすコスト削減と収益創出の機会を検討するための分析フレームワークを提供すること目的に発行

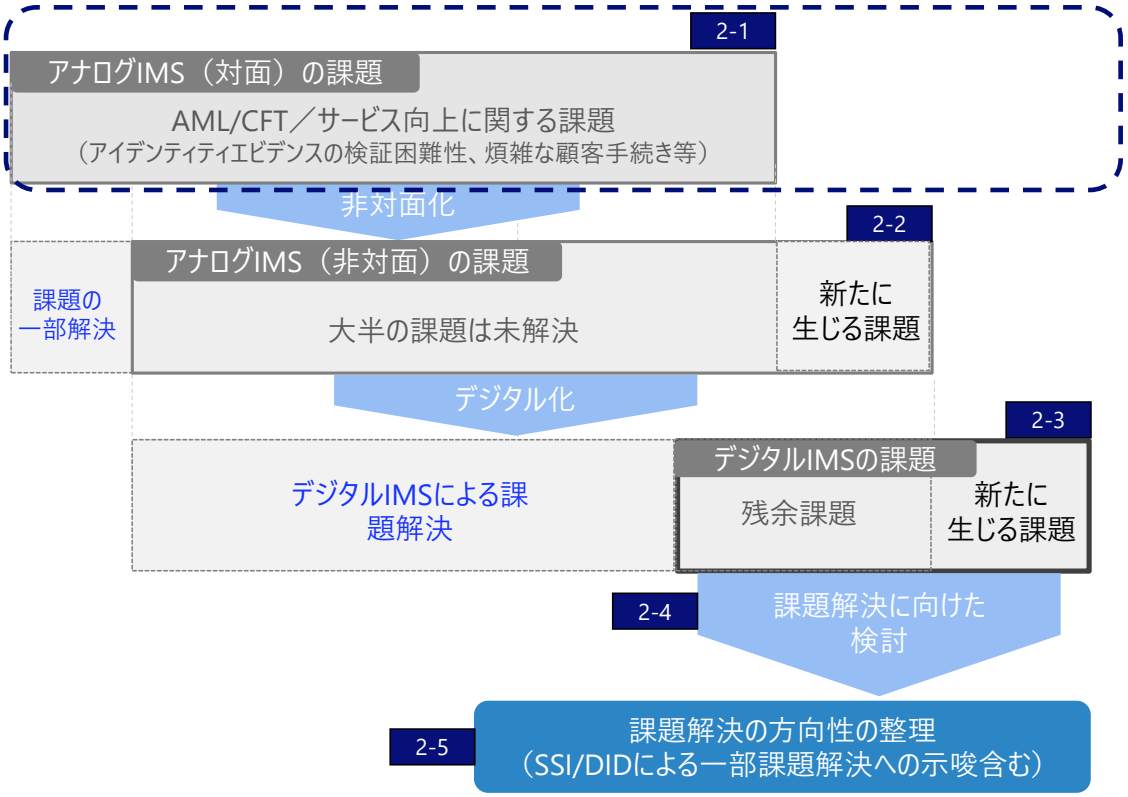
③ デジタルアイデンティティを活用した先進的事例の分析

アイデンティティ管理の課題解決に向け、デジタルアイデンティティの活用が期待されているが、海外各国を中心に、先進的な取組事例も見られる。これらの事例を整理し、アイデンティティ管理の課題解決に向けた示唆を抽出・整理した。

[106] Public Sector Savings and Revenue from Identification Systems:Opportunities and Constraints https://documents1.worldbank.org/curated/en/745871522848339938/pdf/Public-Sector-Savings-and-Revenue-from-Identification-Systems-Opportunities-and-Constraints.pdf

[107] Private Sector Economic Impacts from Identification Systems https://elibrary.worldbank.org/doi/pdf/10.1596/31828

2-1. 金融機関のアイデンティティ管理の現状と課題



本節では、金融機関におけるアイデンティティ管理の現状実態とその課題について、既存の調査研究や今回実施したインタビューを通じて、抽出、整理を行っていく。なお、本章においてアイデンティティ情報とは、１章と同様に、「ICT システムなどにおいて管理されるアイデンティティ（ある実体に関連する属性の集合の表現）」を指す。 具体的には、氏名・住所・生年月日等のユーザ属性、ユーザの識別子、取引履歴等を指す。また、本章において、アイデンティティ管理とは、１章で定義した「アイデンティティ管理システム（IMS） を通じた活動」を指す。具体的には、アイデンティティ情報の管理や、各サービスから要求された属性の提供等を指す。

2-1-1. 金融機関におけるアイデンティティ管理業務の現状

１）アイデンティティ管理の概略と本章の調査対象分野

金融機関においては、AML/CFT や顧客サービスの高度化という観点で、顧客のアイデンティティ管理の重要性が高まっている。各種規制への適切な対応、正しい顧客属性情報に基づくサービスの提供やレコメンデーション等を実施するにあたって、アイデンティティ管理の品質は業務の品質に重大な影響を及ぼすことになる。同様に、規制当局にとっても、金

融機関の規制遵守や顧客への適切なサービス提供・顧客保護の観点等からアイデンティティ管理は重要であり、顧客にとっても、自分たちが受けるサービスがテーラーメードでより良いものになりうるという観点で重要である。

また、2020 年の新型コロナウイルス感染症の拡大の影響を受けて、デジタル空間でのアイデンティティ管理の重要性が高まっていることも指摘されている[108]。パンデミックを契機とした犯罪、例えば詐欺、サイバー犯罪、財政資金や国際的な資金援助の搾取等が増加している。さらに、COVID-19 対策としての外出や対面接触機会の抑制の結果、オンラインサービス、経済刺激策や破産スキームの悪用等のリスクも増大している。

以上のような問題意識に基づき、本調査では、以下を主な検討対象とする。

① AML/CFT 規制対応

② 利用者の最善の利益に沿った商品・サービスの提供のため

なお、AML/CFT 規制対応については、その一部である本人確認に関する業務を中心に検討する。

表 2-3 本章の調査対象分野[109]

政策目標	主な対応事項	アイデンティティ管理との関連
金融システムの安定と金融仲介機能の発揮の両立	AML/CFT 規制対応	取引時確認、顧客フィルタリング、リスク評価、判断・対応
利用者保護と利用者利便の両立	利用者の最善の利益に沿った商品・サービスの提供	アイデンティティ情報を活用した顧客サービスの向上

2）分析の概要

金融機関におけるアイデンティティ管理業務は、業務の実施タイミングとしては、「onboarding（登録処理）」と「ongoing（更新処理）」に区分される。また、業務の目的として、「AML/CFT 規制対応」と「顧客サービスの向上」の二つが主に想定される。よって、本節では、業務の実施タイミングと業務の目的から、下図のように業務を以下の３つに分類する[110]。この３つの業務分類ごとに、業務の詳細とその課題を提示する。

---

[108] FATF, “COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses May 2020”, http://www.fatf-gafi.org/publications/methodsandtrends/documents/covid-19-ml-tf.html

[109] 金融検査・監督の考え方と進め方 （検査・監督基本方針）
https://www.fsa.go.jp/news/30/wp/supervisory_approaches_revised.pdf を元に NRI 作成

[110] B①顧客サービスの向上を目的とした onboarding（登録処理）については、時系列的に存在し得ないため、上記分類からは除外

onboarding：口座開設時の業務を意味し、本章においては下図の①を指す
（本章の範囲では顧客サービスの向上を目的とした業務には口座開設時の業務がないため、 用語集記載の onboarding due diligence（口座開設（取引時確認） を意味する）
ongoing　　：口座開設完了後の業務を意味し、本章においては下図の②と③を指す
なお、 用語集記載の ongoing due diligence（継続的顧客管理）は②を指す

図 2-1　本章で検討する業務の分類

また、各分類の業務の概略は以下の通りである。

表 2-4　業務分類毎のアイデンティティ管理業務概略

業務の分類			業務の概略
onboarding	①口座開設（取引時確認）		顧客の口座開設申込～金融機関による審査・開設判断
ongoing	②継続的顧客管理	定期的顧客情報調査	口座保有顧客に対する定期的な属性変更確認
		取引受付時確認	顧客からの取引申込～金融機関によるリスク確認と取引可否判断
		取引モニタリング（事後）	金融機関による顧客の取引傾向分析と顧客リスクの再評価
	③社内外のアイデンティティ情報を活用したサービス提供		金融機関による顧客アイデンティティ情報の収集・分析と顧客サービス向上に資する取り組み（テーラーメードのサービス提案等）

2-1-2. 対面・アナログ IMS の主な課題　①口座開設（取引時確認）

金融機関において、アイデンティティ管理業務のうち口座開設時の業務は、AML/CFT 規制対応の観点からも非常に重要で基本的な業務となっており、具体的には次のようになっている。

表 2- 5　口座開設業務の概要

業務プロセス	本業務での内容	概要
申込受領	口座開設申込書等受領	• 口座開設申込書類およびアイデンティティエビデンス（定義は次頁参照）を顧客から受領
取引時確認	本人確認・取引目的等の確認	• アイデンティティエビデンスの真正性（申込者本人の正しい情報であること）および有効性（アイデンティティエビデンスが有効であること）を確認し、取引目的および実質的支配者（法人の場合）等もあわせて確認
顧客フィルタリング	顧客フィルタリング	• 反社会的勢力や制裁対象等のリストとの照合、および、取引目的や属性との整合性検証や実質的支配者の確認を通じて、反社会的勢力や制裁対象者等による口座保有を防止
分析・評価	顧客リスクの評価	• 取引形態や顧客属性、商品・サービスの特性等を踏まえて AML リスク等の分析を行い、必要に応じて追加確認を実施
判断・対応	口座開設通知 or 疑わしい取引の届出	• 口座開設の承認と顧客への通知、もしくは口座開設の謝絶と必要に応じて疑わしい取引の届出

なお、本章において、アイデンティティエビデンスは「各法域で認められている本人確認書類/法人確認書類」とする。アイデンティティエビデンスとしては代表例として以下のようなものが挙げられる。

a　個人顧客の本人確認書類
- 運転免許証
- パスポート
- 国民 ID カード（例：日本におけるマイナンバーカード）
- 在留カード・特別永住者証明書（例：米国のグリーンカード）　等

b　法人顧客の確認書類等
- 登記事項証明書
- 印鑑登録証明書

- 上記のほか官公庁発行書類等で法人の名称及び本店又は主たる事務所の所在地の記載があるもの

（法人の担当者・代表者・実質的支配者の本人確認書類は個人顧客と同じ）

先述の業務プロセス分類ごとに、口座開設に関するアイデンティティ管理の課題を整理すると以下のようになる。

業務プロセス	AML/CFTに関する課題(金融機関/当局)	サービス向上に関する課題(顧客/金融機関)
申込受領	・申込情報やアイデンティティエビデンスの情報をデータ化する負担	・新興国における遠隔地居住者の金融包摂 ・顧客の来店負担 ・顧客の書類記入負担 ・顧客の事務処理待ち時間 ・金融機関毎に同様の口座開設申込を行う負担
取引時確認	・アナログのアイデンティティエビデンスの検証困難性 ・オペレーショナルコスト(書類保管コスト) ・他社で検証済の顧客を一から検証する負担	
顧客フィルタリング	・他社で検証済の顧客を一から検証する負担	
分析・評価		
判断・対応		

図 2-2　口座開設（取引時確認）業務に係る課題

a　AML/CFT に関する課題（金融機関／当局）

（ア）申込情報やアイデンティティエビデンスの情報をデータ化する負担

アイデンティティエビデンスを元にスクリーニング等の検証を行うためにはデータ化が必要であり、手入力によるデータ負担が発生する[111]。

（イ）アナログのアイデンティティエビデンスの検証困難性

顧客情報確認において、アイデンティティエビデンスの真正性・有効性を照会・確認するには、本来、アイデンティティエビデンス発行元・金融機関・顧客の 3 者を巻き込んだフローの構築が必要である。そして、各アイデンティティエビデンスの発行元は異なるため、アイデンティティエビデンス毎にフローの構築が必要となる。

[111] IIF, “Digital Identities in Financial Services Part 1: Embedding in AML Frameworks” （Aug. 2019）
https://www.iif.com/Portals/0/Files/content/Innovation/08272019_iif_digital_id_part_1.pdf

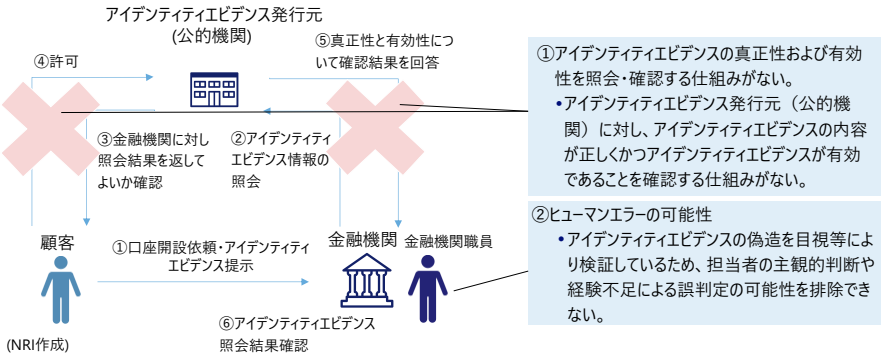


図 2-3　アイデンティティエビデンスの真正性・有効性を確認するフロー

しかし、金融機関は実務上、①アイデンティティエビデンスの真正性および有効性を照会・確認する仕組みがない、②ヒューマンエラーの可能性、という 2 つの課題を抱える。我が国においてもアナログのアイデンティティエビデンスの真正性・有効性を照会・確認するフローは構築されていないのが現状である。（免許証は IC 格納された情報により真正性検証可能、マイナンバーカードは公的個人認証の仕組を使い真正性・有効性検証が可能であるが、いずれもデジタル化されたもの）

なお、我が国におけるアイデンティティエビデンスの真正性・有効性検証可否は以下のようになっており、人の目に頼った真正性・有効性検証が大宗である。

表 2-6　本邦におけるアイデンティティエビデンスの真正性有効性検証可否

対面/非対面	アイデンティティエビデンス	検証可否	
		真正性	有効性
対面	免許証	○[112]	×
	マイナンバーカード	○	○
	その他証明書	×	×
非対面	証明書の紙コピー	×	×
	証明書画像	×	×
	証明書画像+本人容貌写真	○[113]	×
	免許証（IC チップ読み取り）	○[112]	×

112 犯罪収益等移転防止法第 6 条第 1 項第 1 号ヘ

113 犯罪収益等移転防止法第 6 条第 1 項第 1 号ホ

	マイナンバーカード（IC チップ読み取り）	○	○[114]

○：IC等に保存されたデータを元に照合可能　×：人の目で判断

(ウ)オペレーショナルコスト（書類保管コスト）

書類の保管や郵送に関わるコスト負担が生じている。

(エ)他社で検証済の顧客を一から検証する負担

金融機関ごとに口座開設時のアイデンティティ管理を行う場合、業務上の重複が大量に発生することになる。

b　サービス向上に関する課題（顧客／金融機関）

(ア)新興国における遠隔地居住者の金融包摂

近隣に支店が存在しないような新興国等においては、対面取引のため支店に出向かないといけないことから、遠隔地の支店への訪問が困難な顧客が排除されることになる。

(イ)顧客の来店負担

来店可能な顧客についても、支店への来店負担が発生する。

(ウ)顧客の書類記入負担

(エ)顧客の事務処理待ち時間

支店での書類の記入や手続きの待ち時間などで顧客に負担を掛けている。

(オ)金融機関ごとに同様の口座開設申込を行う負担

ある金融機関において口座開設済であっても、別の金融機関に口座開設する際に既存口座の情報を利用できず、一から口座開設手続きを行う必要がある。

[114] マイナンバーカードによる本人確認のうち、IC チップに記録された公的個人認証用の署名用電子証明書を使用

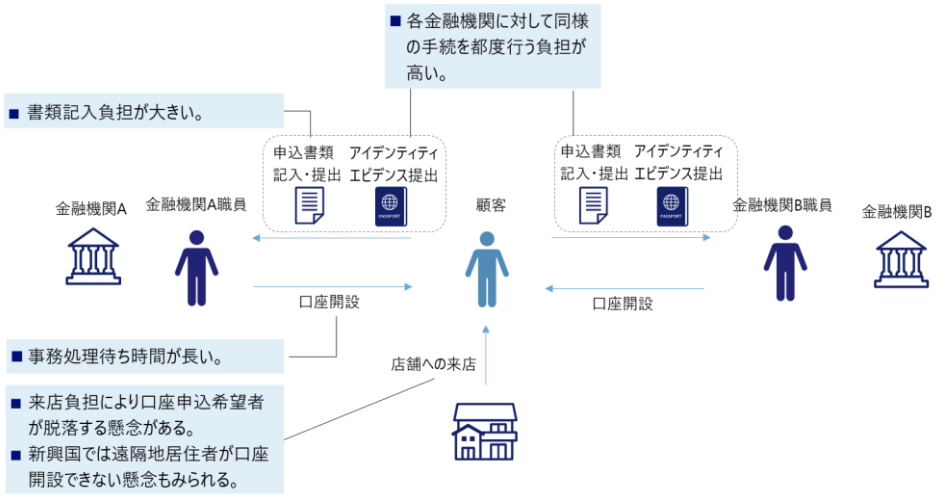


図 2- 4　対面・アナログ IMS での口座開設における顧客の主な課題

2-1-3. 対面・アナログ IMS の主な課題　②継続的顧客管理

AML/CFT 規制対応のため、顧客のライフサイクル全般を通して適切なアイデンティティ管理が求められる。

表 2- 7　継続的顧客管理業務の概要

業務プロセス	本業務での内容	概要
申込受領	<定期的顧客情報調査> 顧客情報収集・更新	• 顧客リスクに応じた頻度にて定期的に顧客情報を収集（郵送、架電等）し、顧客情報を更新
	<取引受付時確認> 取引申込受領	• 取引申請書類を顧客から受領
取引時確認	<取引受付時確認> 当人認証・取引内容確認	• 取引申請者の当人認証を行い、かつ、取引目的や金額等の取引内容を確認
顧客フィルタリング	<定期的顧客情報調査> 顧客フィルタリング	• 反社会的勢力や制裁対象等のリストとの照合、および、取引目的や属性との整合性検証や実質的支配者の確認を通じて、反社会的勢力や制裁対象者等による口座保有を防止
	<取引受付時確認> 顧客フィルタリング	
分析・評価	<定期的顧客情報調査> 顧客リスクの再評価	• 取引形態や顧客属性、商品・サービスの特性等を踏まえて AML リスク等の分析を行い、必要に応じて追加確認を実施
	<取引受付時確認>	

	取引リスクの評価	
	<取引モニタリング（事後）> 取引モニタリング	• 過去の取引パターン等と比較して異常取引の検知、調査、判断を行い、当該顧客のリスク評価に反映
判断・対応	<定期的顧客情報調査> 取引リスクの低減 or 疑わしい取引の届出 or 関係の継続	• 顧客リスクの再評価を踏まえ、取引金額等の閾値を厳格化する等の取引リスク低減措置を実施し、必要に応じ疑わしい取引の届出提出
	<取引受付時確認> 取引受付 or 疑わしい取引の届出	• 取引の受付、もしくは取引の謝絶と必要に応じて疑わしい取引の届出提出
	<取引モニタリング（事後）> 取引継続 or 疑わしい取引の届出	• 取引の継続、もしくは必要に応じて疑わしい取引の届出提出（疑わしい取引の届出提出の上で、取引を継続し、顧客をモニタリングする事例も含む）

これらの業務プロセス分類ごとに、継続的顧客管理に関するアイデンティティ管理の課題を整理すると以下のようになる。

図 2- 5　継続的顧客管理業務に係る課題

a　AML/CFT に関する課題（金融機関／当局）

（ア）取引申請書類をデータ化する負担

スクリーニング等の検証を行うためにはデータ化が必要であり、手入力によるデータ負担が発生する。

(イ)大量の顧客に対する検証事務負担

(ウ)アナログの顧客情報収集郵電費・データ化負担

アナログの顧客情報収集郵電費・データ化負担が生じる。また、大量の顧客に対する検証負担も大きい。

b　サービス向上に関する課題（顧客／金融機関）

(ア)郵便物の返送手続負担

アナログでのやり取りに伴う手続き負担が発生する。

(イ)取引時のセキュリティリスク（パスワード盗取など）

当人認証不正は以下のもの等が認識されている[115]。

- パスワードリスト型攻撃・フィッシング等によるインターネットバンキング等のユーザーID・パスワードの盗取
- 内部者によるユーザーID・パスワード等のデータ盗取

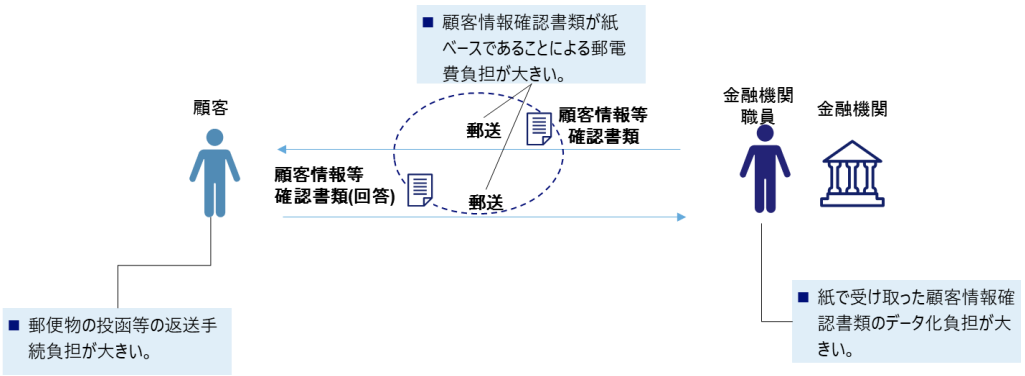


図 2- 6　定期的顧客情報調査におけるアナログ IMS に起因した諸課題

2-1-4. 対面・アナログ IMS の主な課題　③社内外のアイデンティティ情報を活用したサービス提供

アイデンティティに紐づく情報の収集・分析により、テーラーメードのサービス提案等、顧客サービス向上の取り組みが可能になる。

---

[115] Guidance on Digital Identity
http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf

表 2-8　社内外のアイデンティティ情報を活用したサービス提供業務の概要

業務プロセス	本業務での内容	概要
分析・評価	自社内のアイデンティティ情報収集	• 自社内において、取引情報等顧客に紐づく情報を収集
	他社からのアイデンティティ情報収集	• 他社から、金融/非金融の取引情報、非伝統的情報（顧客のサイトアクセス・位置情報、SNS）等、顧客に紐づく情報を収集
	アイデンティティ情報分析	• 収集した情報から、顧客のファイナンスニーズ等を分析（例：顧客の EC サイト購入履歴から教育ローンのニーズがいつ発生するか分析する等）
判断・対応	提供サービス選定/提案	• 分析結果に基づき、顧客にとって最適なサービスを選定し顧客へ提案

データの利活用に関する課題としては以下のようなものが挙げられる。

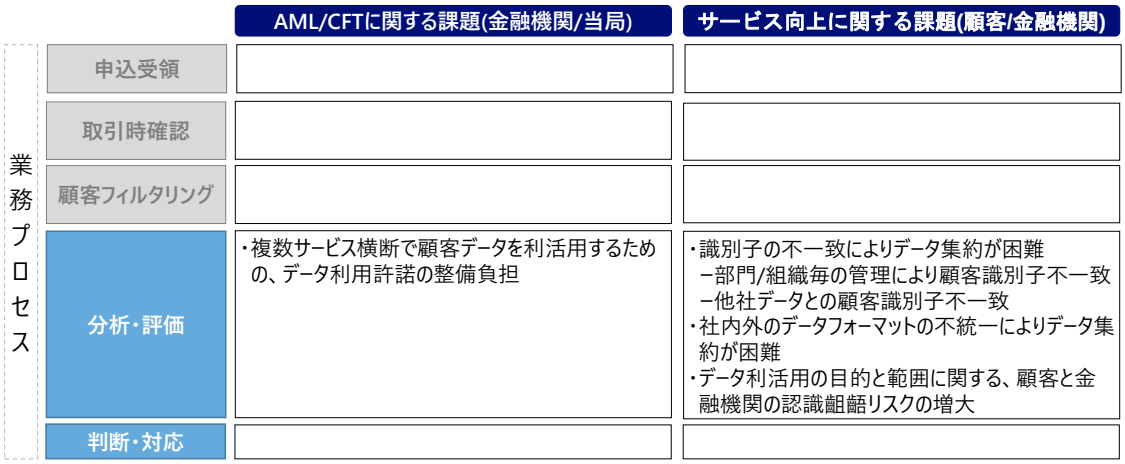


図 2-7　社内外のアイデンティティ情報を活用したサービス提供業務に係る課題

(ア) 識別子の不一致によりデータ集約が困難

および

(イ) 社内外のデータフォーマットの不統一によりデータ集約が困難

アイデンティティ管理に関する課題として、分析対象のデータベース間の顧客識別子（顧客 ID）やデータフォーマットの不一致が挙げられる。

（例：顧客識別子の不一致）

- 金融機関と他社の間の顧客識別子の不一致：各社で顧客 ID を発行・管理するため不一致が発生

・ 金融機関内の各部門間で顧客識別子の不一致：歴史が長く合併等を行っている金融機関にみられるケースであるが、社内の部門毎等で個別に顧客 ID を発行しているため不一致が発生。部門毎の分断は顧客 ID を管理しているシステムの分断によっているケースが多い

金融機関における情報分析業務に関して、複数の文献でデータの部分最適化に関する課題が指摘されている。

・ 銀行の管理会計は縦割りの部門軸であったため、事業部門・プロダクトごとに管理された膨大な数の業務によってマスターデータは部分最適化が進み、横串での管理が困難な状況[116]
・ データ設計に関するルールがなく、システム毎にコード体系や粒度が異なり、データの体系を揃えるのに負担が大きくコストも大きいため、分析に有用なデータを提供することができない[117]

社内データが部分最適化されると、顧客識別子やデータフォーマットが部門毎やシステム毎に異なる場合があり、サービス向上に向けた顧客軸での横断的なデータ分析を十分に行えない、という課題が発生していると考えられる。

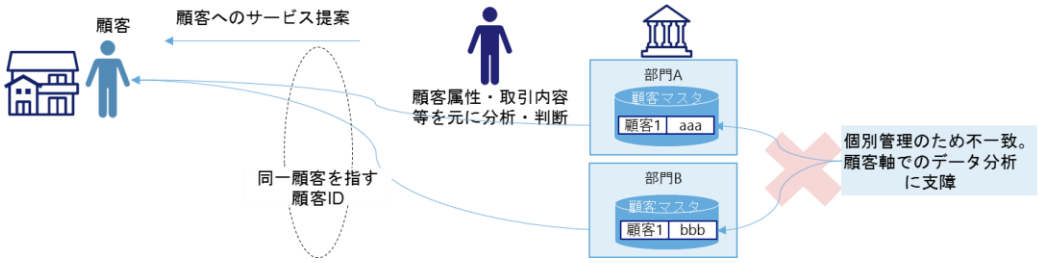


図 2-8　データ管理における顧客識別子の不整合

(ウ) データ利活用の目的と範囲に関する、顧客と金融機関の認識齟齬リスクの増大

不十分な顧客への説明により、顧客同意がないままデータ活用されるリスクが高まる。

---

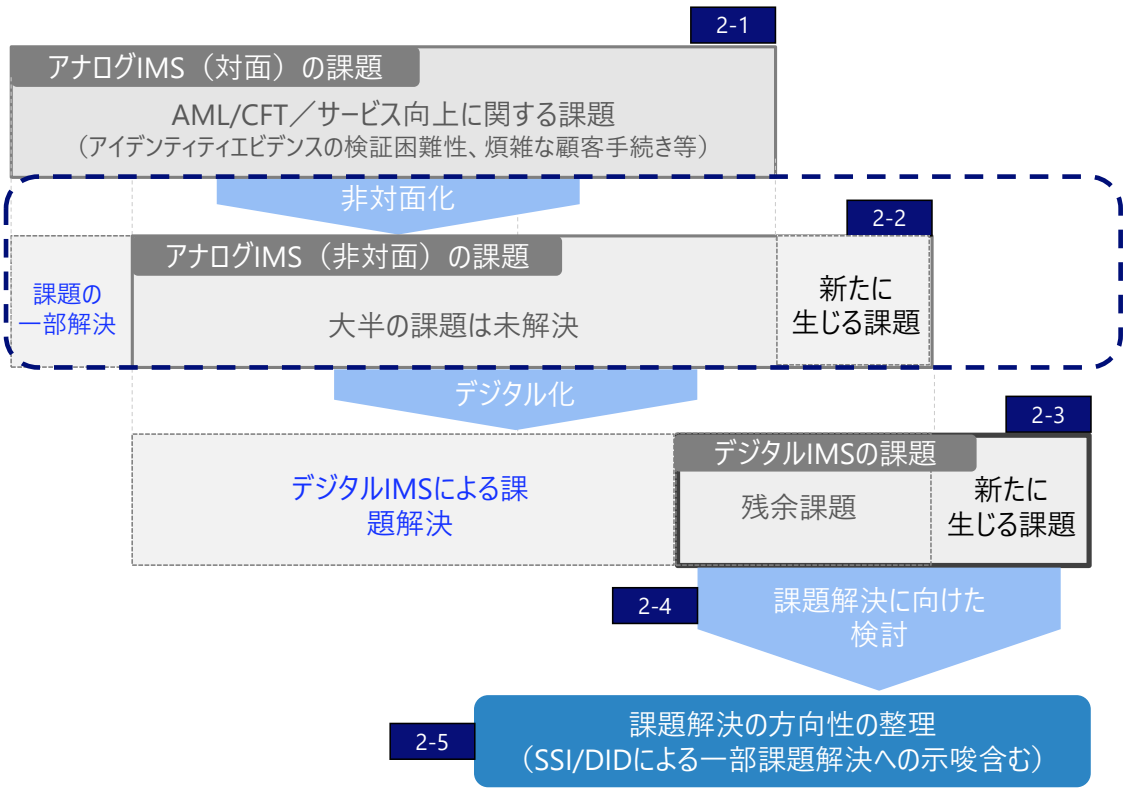
[116] The Finance「FINANCE FORUM 金融機関に求められるデータ利活用の実践」より抜粋 https://thefinance.jp/event/finance-forum-200528

[117] デロイトトーマツ「金融機関におけるデータを活用した意思決定の高度化 2016」 https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/financial-services/bk/jp-fi-data-utilization.pdf

(エ)複数サービス横断で顧客データを利活用するための、データ利用許諾の整備負担

顧客との間のデータ利用許諾は契約の都度、利用目的を明示する形で説明を行う必要がある場合がある。

2-2. onboarding プロセスの非対面化の進展



2-1 で見たように、対面や郵送での紙のアイデンティティエビデンスを用いたアイデンティティ管理により、金融機関・顧客に多くの負担が発生している。顧客においては、店舗への来店時間や申込書類記入負担が生じており、金融機関においても、紙のアイデンティティエビデンスを用いての目視による本人確認事務や、書類の郵送・保管等のコスト負担（書類の保管は個人情報を含むため厳重な管理が求められる）等が負荷となっていることは前述の通りである。

これに対して、近年、多くの金融機関では、主に onboarding プロセスにおいて郵送や画像、ビデオを利用したアイデンティティ管理を行うことで、対面業務の課題の解消を図っている。本節では、これらの非対面化によって解消される、あるいは解消されない、onboarding プロセスにおけるアイデンティティ管理業務の課題を検討する。

2-2-1. onboarding プロセスの非対面化の進展

金融機関においては、オンライン取引の増加や eKYC 等のリモート onboarding に関する本人確認規定の整備、民間ベンダーによるソリューション提供の拡充等を背景に、非対面化が進行している。このような非対面化の進展は、アイデンティティ管理業務のプロセ

スや内容に変革をもたらしている。

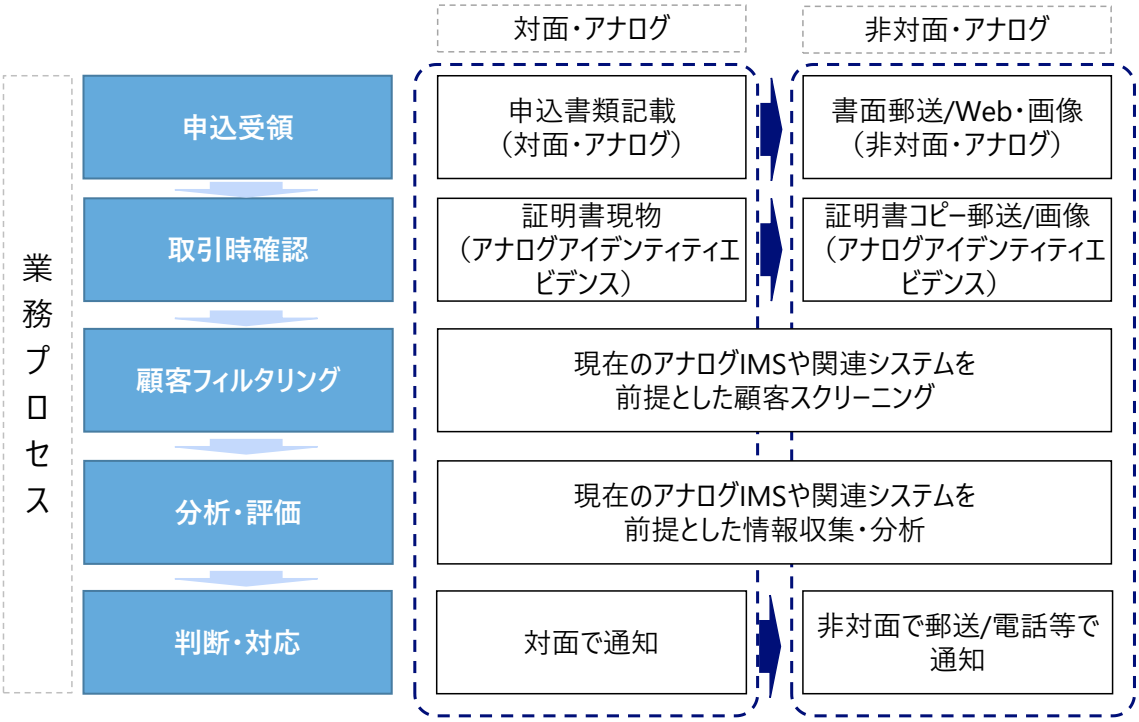


図 2-9　非対面化によるアイデンティティ管理の業務プロセスの変化

2-2-2. 非対面化による課題の一部解消と新たな課題の発生

onboarding 業務での非対面化の進展は、これまでの対面によるアイデンティティ管理の課題の一部を解消することに寄与している。具体的には、顧客サービスの面での課題となっていた、「顧客の来店負担」「顧客の事務処理待ち時間」等については、顧客自宅での手続きが可能になることから、課題の解消に大きく寄与している。一方、アイデンティティ管理業務の一部が対面から非対面へと移行することで、新たな課題が生じることも避けられない。

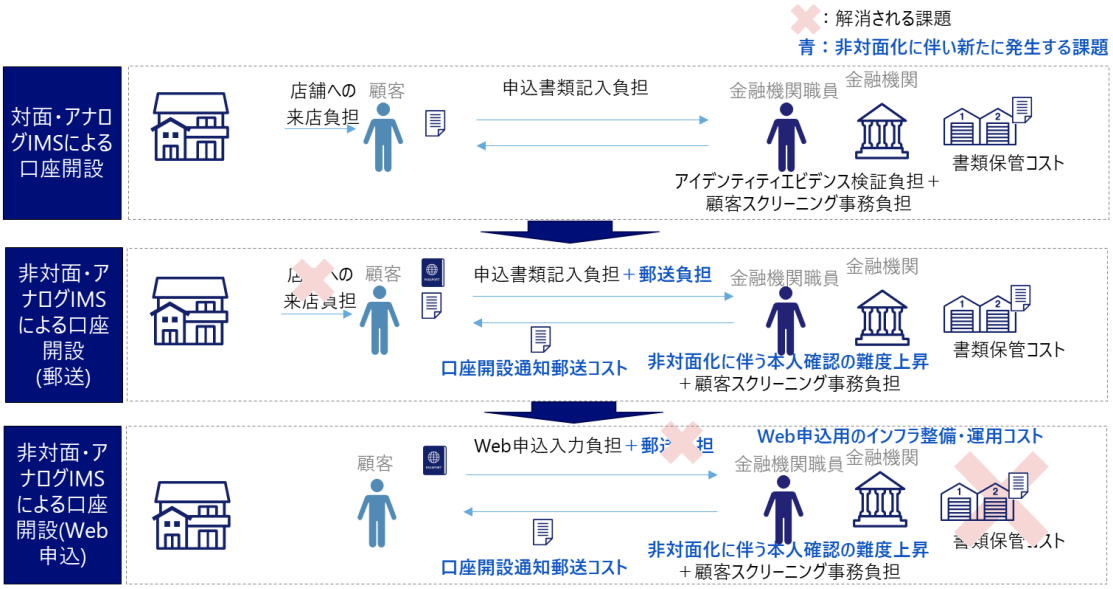


図 2- 10　対面・アナログ IMS の非対面化による課題の一部解消

凡例　文字：非対面化により解消される対面・アナログIMSの課題
青字：非対面化により新たに生じる課題

業務プロセス	AML/CFTに関する課題(金融機関/当局)	サービス向上に関する課題(顧客/金融機関)
申込受領	・~~申込情報~~やアイデンティティエビデンスの情報をデータ化する負担 ・Web申込用のインフラ整備・運用コスト	・~~新興国における遠隔地居住者の金融包摂~~ ・~~顧客の来店負担~~ ・~~顧客の書類記入負担→Web申込入力負担~~ ・~~顧客の事務処理待ち時間~~ ・金融機関毎に同様の口座開設申込を行う負担
取引時確認	・アナログ・アイデンティティエビデンスの検証困難性 ・~~オペレーショナルコスト(書類保管コスト)~~ ・他社で検証済の顧客を一から検証する負担 ・非対面化に伴う本人確認の難度上昇	
顧客フィルタリング	・他社で検証済の顧客を一から検証する負担	
分析・評価		
判断・対応	・所在確認のための口座開設通知郵送コスト	

図 2- 11　非対面化後も残る課題と非対面化により新たに発生する課題

(ア) 非対面化による本人確認の難度上昇

- 非対面取引は、対面取引と比較して、金融機関側が他人へのなりすましを看破する手段が限定されることから、本人確認の精度が低下するリスクを孕んでいる。取引の相手方と直に対面しないことで、性別、年代、容貌、言動等を直接確認することで容易に確認できる筈の情報を確認できないまま本人確認を行ってしまうことになる。これにより、本人特定事項の偽りや他人へのなりすましの有無を判断することが困難となるものである。また、顧客本人ではなく、ア

イデンティティエビデンスの偽変造等についても認識することが難しい傾向がある。アイデンティティエビデンスのコピーにより本人確認を行う場合には、その手触りや質感を感知できないことなどがその要因である。非対面での onboarding 業務において、アイデンティティエビデンスの真正性・有効性の検証が不十分にしかできないアナログ IMS を利用している限りにおいては、当該リスクを低減することが困難であり、非対面化により生じる／拡大するリスクが存在することに留意する必要がある。このため、対面取引との比較で言えば、一般的には、非対面での onboarding については、より高リスクなものとして金融機関が認識している傾向にある。取引の相手方と直に対面せずに行う取引であることから、同人の性別、年代、容貌、言動等を直接確認することにより、本人特定事項の偽りや他人へのなりすましの有無を判断することが困難となる可能性がある。

- アイデンティティエビデンスのコピーにより本人確認を行う場合には、その手触りや質感から偽変造の有無を確認することが困難となる可能性がある。

犯罪収益移転危険度調査書[118]でも、危険度の高い取引形態の一つとして非対面取引に言及している。

（イ）Web 申込入力負担

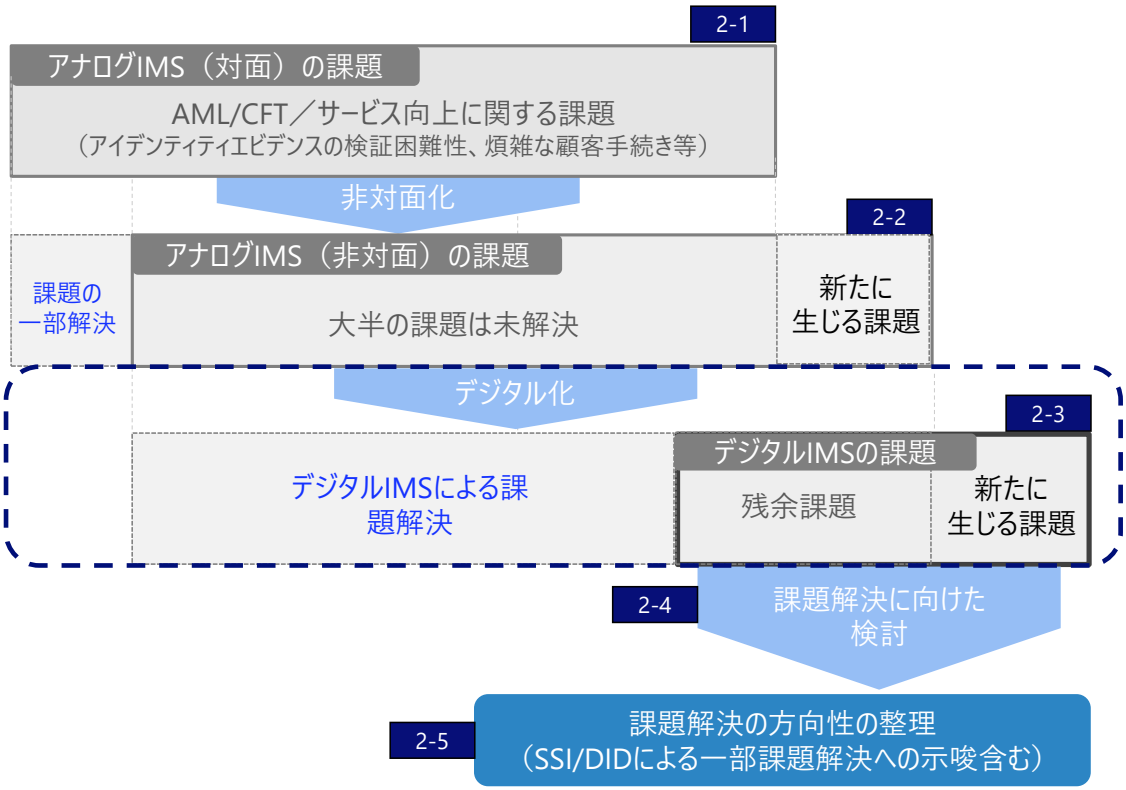
非対面での口座開設申込時には顧客は Web 等で申込入力を行う必要がある。申込時には、写真撮影や画像保存・アップロードといった負担が発生する。

（ウ）所在確認のための口座開設通知郵送コスト

非対面での口座開設実施時に、金融機関は口座申込者の届出住所に対して転送不要郵便を送付して口座開設申込者の所在確認を行うため、郵送コストが負担となる。

[118] 国家公安委員会『犯罪収益移転危険度調査書（令和 2 年度版）』（https://www.npa.go.jp/sosikihanzai/jafic/nenzihokoku/risk/risk021105.pdf）

2-3. デジタル IMS の活用可能性



近年の社会全体のデジタルシフトは2020年の新型コロナウイルス感染症の影響により一層の加速を見せている。これにより、金融取引のデジタル化も進展しているが、AML 等のコンプライアンスの観点からも、デジタル空間における本人性の確認がより重要であることは、前節までに分析したアナログによるアイデンティティ管理の課題からも明らかである。顧客サービス面でも、手続がデジタルで完結する利便性高い UX が金融においても徐々に普及し、デジタル化への顧客の期待が高まっている。

そこで、本節では、デジタル IMS に移行することで、従来のアナログでの IMS における課題がどのように解決されるのか、一方でデジタル IMS を活用しても残る、あるいは新たに発生する課題を整理していく。

2-3-1. 金融機関のデジタルアイデンティティ活用の重要性

金融機関においては、ネット金融機関の登場、拡大とネット取引の増加等を背景として、eKYC 等のリモート onboarding に関する本人確認規定の整備や民間ベンダーによるソリューション提供が進み、IMS のデジタル化が進行しつつある。本節において IMS のデジタル化とは、アイデンティティ情報の相互のやりとりをデジタル化すること（例えば、マシンリーダブルな形式でのアイデンティティエビデンスの連携等）

IMS のデジタル化の進展は、アイデンティティ管理業務のプロセスや内容に変化をもたらしている。

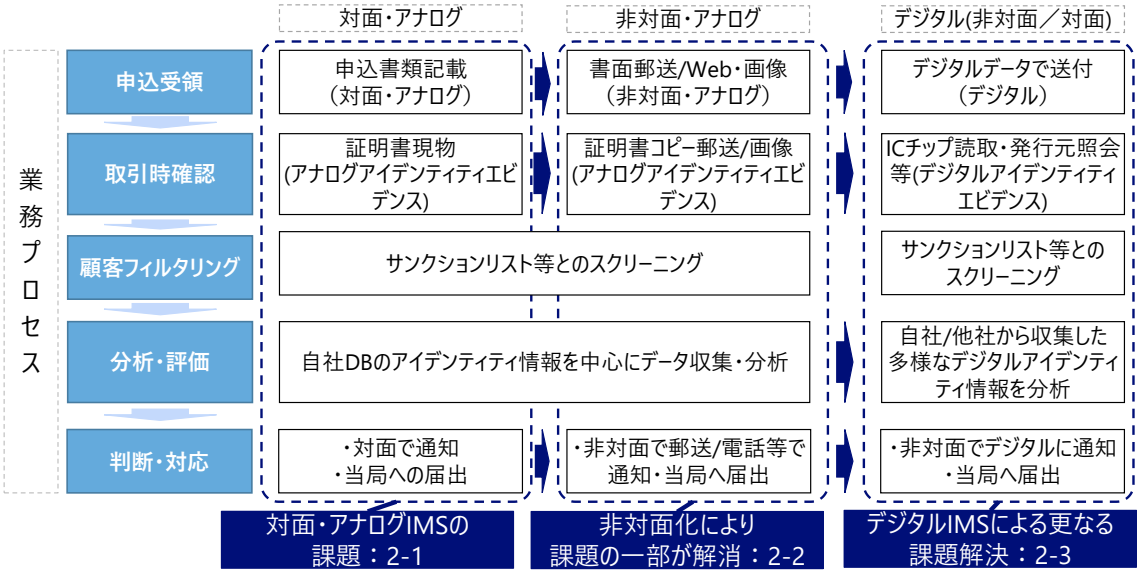


図 2- 12　IMS のデジタル化によるアイデンティティ管理の業務プロセス変化

金融機関の IMS がデジタル化されることで、onboarding、ongoing の各業務について、AML/CFT 高度化、コスト削減、顧客サービス向上が期待できる。ここでは、これらのメリットについて、主要なものを整理する。顧客の本人確認のプロセスについては、多くの国や地域で厳格に定められており、金融機関は多額のコストを掛けてこれに対応してきたが、デジタルアイデンティティを活用することで、アイデンティティエビデンスの精査・確認をより高精度、低コストで実現する動きが生じている。

2-3-2. 分析対象ユースケース

金融機関におけるデジタルアイデンティティ管理の課題を抽出するにあたって、2-1 で行った業務の分類毎にユースケースを設定し、当該ユースケースに沿って、金融機関自体を含むステークホルダーそれぞれの視点で課題の洗い出しを行う。

なお、「口座開設（取引時確認）」については、口座開設時の ID 連携の進展度合いを複数想定し、（1-1）自社でデジタルアイデンティティエビデンスを利用するパターンと、（1-2）アイデンティティエビデンスは利用せず他社で作成済のデジタルアイデンティティを利用するパターンの 2 パターンに分けて分析を行う。

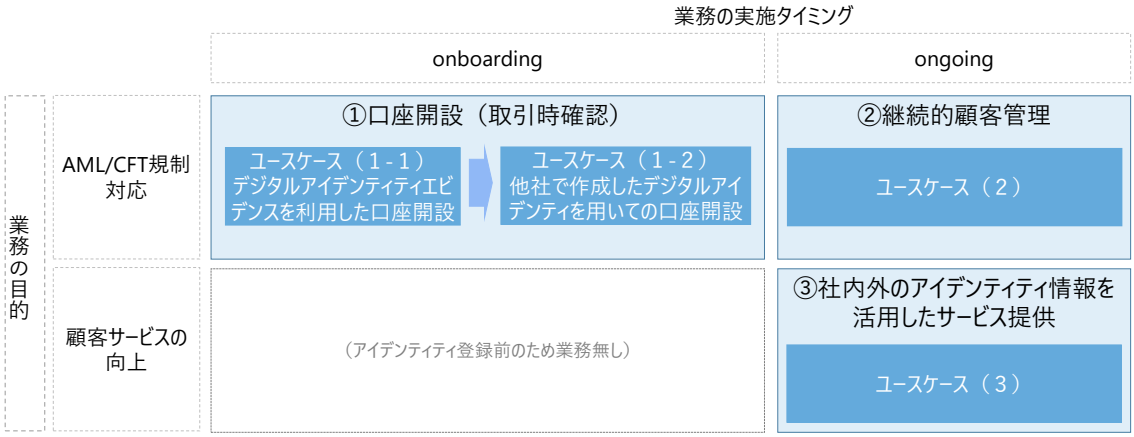


図 2-13　分析対象ユースケースの位置づけ

2-3-3. ユースケース分析

1）ユースケース （1 - 1） デジタルアイデンティティエビデンスを利用しての口座開設

業務の概要 （デジタル化による変化）

マシンリーダブルでデジタルに検証可能なアイデンティティエビデンスを用いて本人確認を行い口座開設することを想定する。これまでの非対面型でアナログなアイデンティティエビデンスを用いた口座開設との相違は下図に表される。

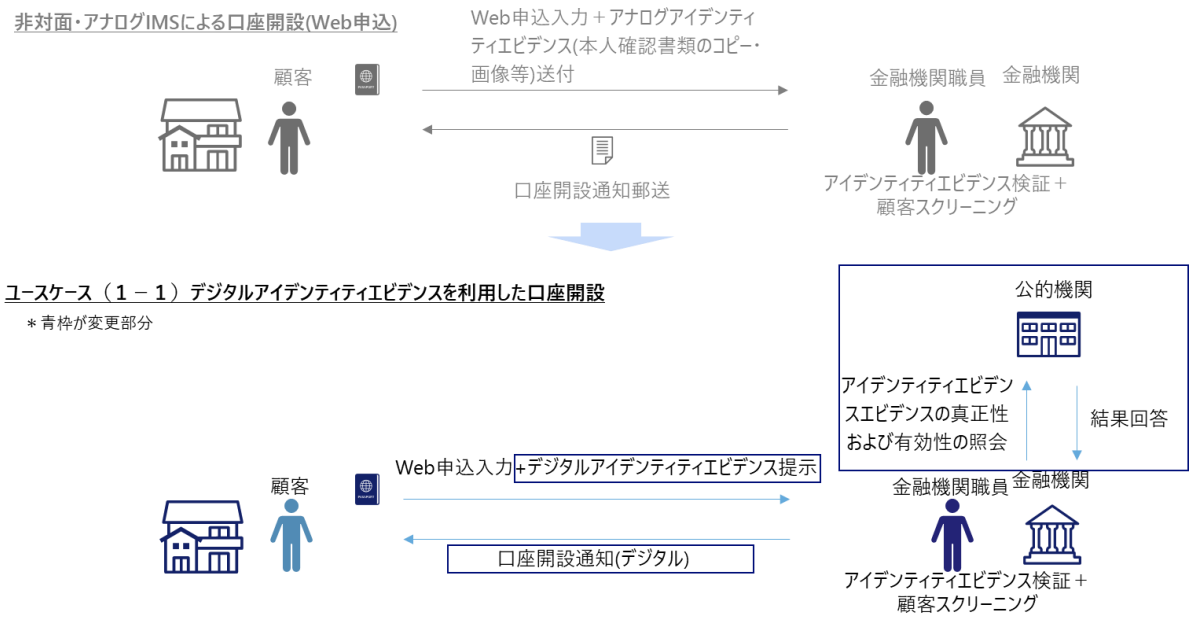


図 2- 14 デジタルアイデンティティエビデンスを利用しての口座開設業務

デジタル IMS 化により解決される課題

マシンリーダブルでデジタルに検証可能なアイデンティティエビデンスが用いられることで、以下の課題については、解消もしくは程度の低減につながるものと想定される。

- アイデンティティエビデンスの情報のデータ化を行う負担
  アイデンティティエビデンスがデジタル化されて金融機関に提供されることにより、金融機関サイドでのデータ化は不要になる。
- アナログのアイデンティティエビデンスの検証困難性
  マシンリーダブルでデジタルに検証可能なアイデンティティエビデンスの利用により、アイデンティティエビデンスの正しさを発行機関に照会し確認する仕組みが確立することを前提に、アイデンティティエビデンスの真正性確認に要する事務負担が軽減されるためである。

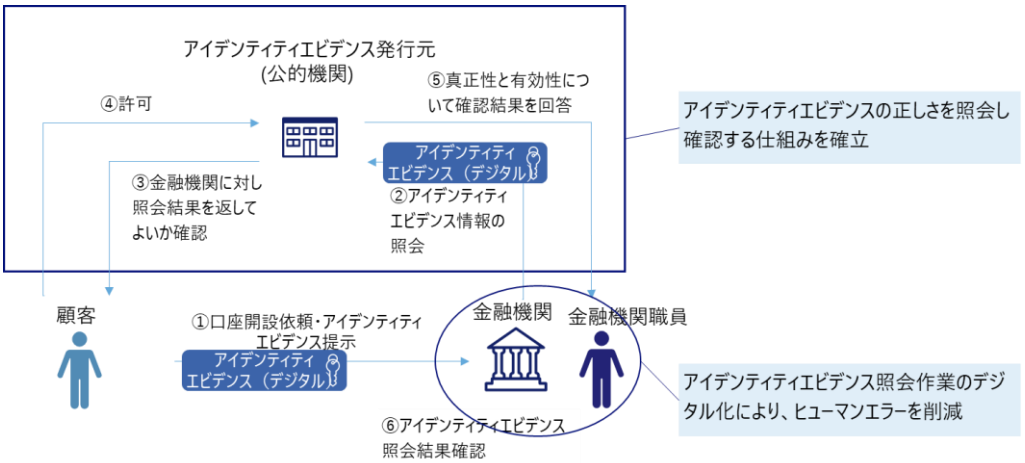


図 2- 15　デジタル化によるアイデンティティエビデンスの検証困難性の低下

- 非対面化に伴う本人確認の難度上昇

  デジタル IMS による真正性・有効性の確認により、アイデンティティエビデンス改ざんによるなりすましリスクが、アナログアイデンティティエビデンスとの対比で軽減されうる。また、生体情報等とのバインドにより、当人認証精度が向上しなりすましリスクが軽減されうる（インドの Aadhaar 等（2-4 参照））。

- 所在確認のための口座開設通知郵送コスト

  デジタルアイデンティティエビデンスとして国民 ID を利用する場合、国民 ID の住所を正として情報のアップデートを速やかに取り込む仕組みの構築を行うことで、郵便による確認を不要とすることが可能になる（シンガポールの事例（2-4 参照））。あるいは、顧客の取引時の位置情報等を参考に届出住所を確認する仕組みを構築することで、郵便による確認を不要とする（みずほ銀行等の実施した FinTech 実証実験ハブ支援案件「端末の位置情報や顔認証技術を活用した Digital ID による本人認証および継続的顧客管理に関する実証実験」で検証（2-4 参照））などの対応も可能。

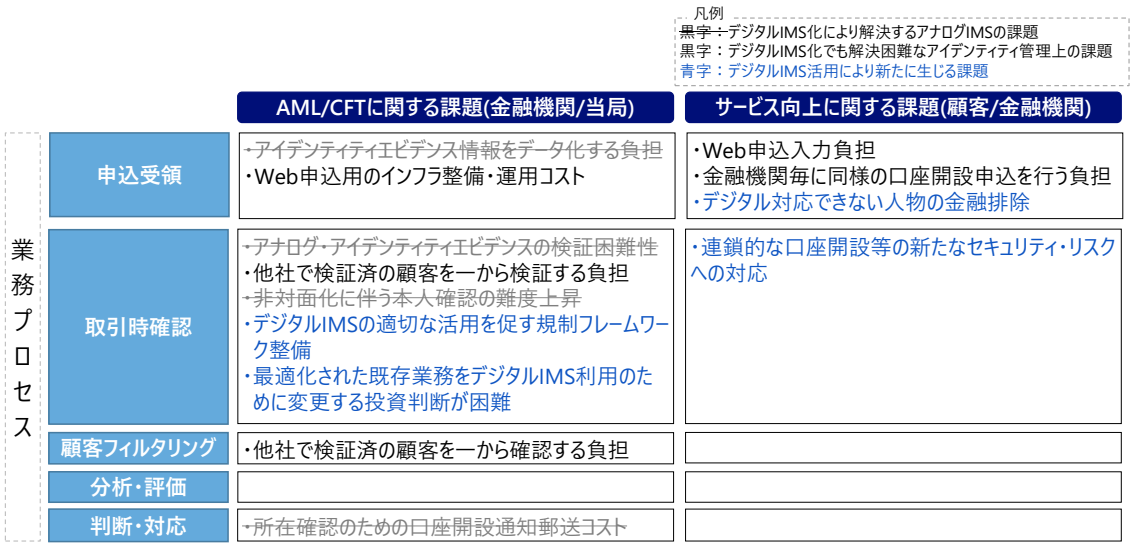


図 2- 16　口座開設のデジタル IMS 化により解消される課題と新たに発生する課題まとめ

新たに発生する課題

アナログ特有の課題が解決する一方で、デジタル化による新たな課題も発生する。

- デジタル対応できない人物の金融排除

  携帯電話・スマートフォン等の未普及、インターネットアクセスが可能な地域が限定的など、デジタルインフラの活用が難しい地域がある中でのデジタル化の推進は、新たな金融排除を生む可能性がある。

- デジタル IMS の適切な活用を促す規制フレームワーク整備

  FATF は、規制目的に適した IAL（Identity Assurance Level）が担保されるよう、以下①または②に該当するデジタル IMS を採用するよう提唱している[119]。

  ① 政府により顧客管理への利用を許可されたもの

  ② 堅牢性や IAL が政府や政府認可機関により保証もしくは監査され、かつ AML/CFT の観点から十分な IAL が提供されるもの

[119] FATF, “Guidance on Digital ID (2020)”
http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html

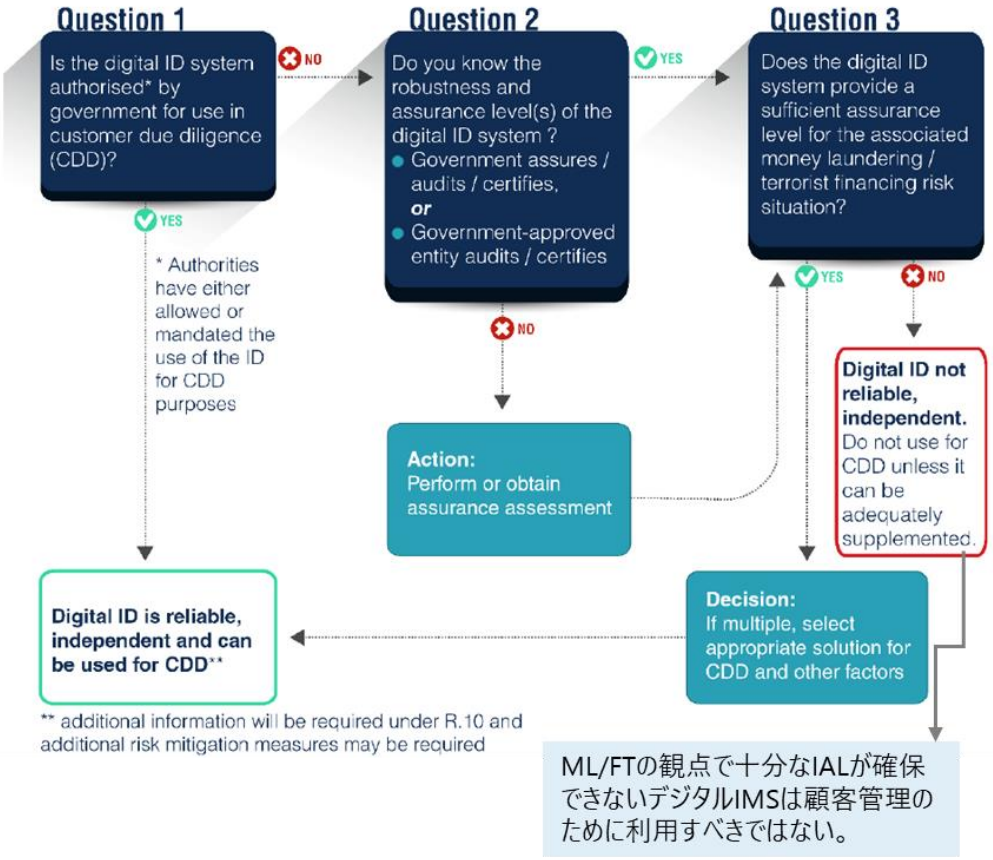


図 2- 17　FATF 提唱の AML/CFT 目的でのデジタル IMS の採否決定プロセス

加えて、FATF は、適切な IAL が担保されたデジタル IMS の下では、リスクベース・アプローチが可能となり、AML/CFT の高度化や金融包摂に寄与する点について言及している。一般に高リスクに分類非対面取引においても、適切なデジタル IMS に依拠する場合は、標準レベルもしくは低レベルのリスクになる可能性がある 119。本人確認規定（や継続的顧客管理規定）等の規制要件は、金融機関が信頼性の高いデジタル IMS をリスクに応じて適切に使用できるように規定されるべきだが、eID が推奨されている EU（ドイツ）などを除き、本人確認規定とアイデンティティ保証フレームワークとの接合が行われている法域は限定的である。一部の有識者からは、eKYC を導入したにも関わらず、画像確認技術の限界等から却って IAL が下がっているのではないか、といった指摘もあった。

表 2-9　各国の本人確認規程根拠と IAL との接合状況

	日本	アメリカ	英国	ドイツ	シンガポール	ニュージーランド
本人確認規程根拠	犯罪収益移転防止法で本人確認方法について規定	愛国者法で連邦レベルでの本人確認方法を規定、州法もこれに準拠	基本法となる概要を規定、政府デジタルサービスガイダンス等で詳細化	Money Laundering Act（GwG）で総論を規定、詳細は別に個別の法で定める	マネロンおよびアンチテロリズム法で規定	Identification Management Standards にて規定
対面での本人確認	原則写真付公的証明書					業態毎に水準を規定し、いずれの組み合わせでも水準を満たせば良い
非対面での本人確認の特例	ビデオ通話と公的証明書での確認も可	金融機関が定めることを要請	非対面での確認の規定無し	ビデオ通話での確認方法も詳細規定	非対面の場合の代替手段を列挙	必要水準が低い業態では非対面でも追加措置不要
アイデンティティ保証フレームワーク（IAL）との接合	無	無	無（Good Practice Guide45 が eIDAS と接合するもガイドライン留まり）	GwG 解釈ノートにて eIDAS 準拠を規定	無	無

（ご参考）国民番号制度	あり（マイナンバー※）	一部あり（SSN）	なし（2010年にIDカード法廃止）	あり	え	一部あり（IRD）

※マイナンバーの利用は、現在、社会保障、税金、災害対策の３つに厳しく限定されており本人確認には利用できない

- eIDが推奨されているEU（ドイツ）を除き、本人確認規定とアイデンティティ保証フレームワークとの接合は無い。
- シンガポールは政府ID利用への統一化により、実質的にアイデンティティ保証レベルを均一化している。
- EUではonboardingへのeIDの活用が検討され、金融分野における技術・ガバナンスともeIDAS規則に準拠することを前提として議論が進んでいる。
- 米国でもNIST（米国立標準技術研究所）がSP-800-63A[120]においてIAL、AALを規定しているが、米国・EUのように公的なアイデンティティ保証フレームワークが規定されている法域は限定的である。（下図参照）

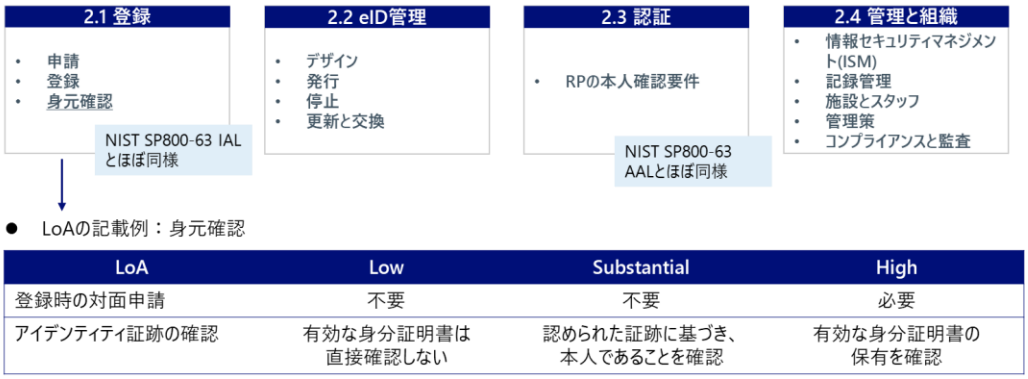


図2-18　（参考）米国・EUのアイデンティティ保証フレームワーク

[120] “CONFORMANCE CRITERIA for NIST SP 800-63A ENROLLMENT AND IDENTITY PROOFING and NIST SP 800-63B AUTHENTICATION AND LIFECYCLE MANAGEMENT （June 2020）” https://www.nist.gov/system/files/documents/2020/07/02/800-63A%20Conformance%20Criteria_0620.pdf

- 最適化された既存業務をデジタル IMS 利用のために変更する投資判断が困難

  デジタルアイデンティティエビデンスを利用するためには整備コスト・業務を変えるコスト等の負担が発生するが、これらのコストは小さくないため、そのコストを賄うのに十分なコスト削減・顧客獲得等の効果を示すためには金融機関内の部門を跨いだ金融機関全体としての効果を洗い出す必要があり、効果を取りまとめ投資の合意を得る負担は大きい。また、デジタルアイデンティティエビデンスの普及状況等、現状明確でない将来も勘案の上で初期投資の判断を行う必要があることも難しい点である。

  上記のイニシャルコストの問題に加え、継続的なセキュリティ強化等、ランニングコストの負担を鑑みた投資判断も重要である。

- 連鎖的な口座開設等の新たなセキュリティリスクへの対応

  業務プロセスがデジタルで完結するため、セキュリティホールが発見されると次々と不正利用を行われる懸念がある。偽造方法が確立すれば、アナログエビデンスと比較し、デジタルエビデンスの方が偽造エビデンスを多数作成しやすいと考えられるためである。文献[121]では、デジタル ID ネットワークには、偽の ID がシステムにアップロードされる可能性によるリスクが依然として存在し、本物の情報と偽物の情報を組み合わせて新しい ID を作成する合成 ID や、偽の ID は、デジタル ID ネットワークの onboarding プロセスを狙った攻撃の懸念が指摘されている他、悪質な従業員が偽の ID をシステムにアップロードする可能性も指摘されており、セキュリティに対する懸念は存在する。

2）ユースケース（1 - 2） 他社で作成したデジタルアイデンティを用いての口座開設

業務の概要 （デジタル化による変化）

口座開設時に、他社で作成したデジタルアイデンティを用いることによって、顧客の 2 社目以降の口座開設に係る負担の軽減、金融機関のアイデンティティエビデンス検証負担削減等の効果が期待される。これまでの非対面型でアナログなアイデンティティエビデンスを用いた口座開設との相違は次図に表される。

[121] “Digital Identity and Financial Crimes”
https://www.acamstoday.org/digital-identity-and-financial-crimes-2/

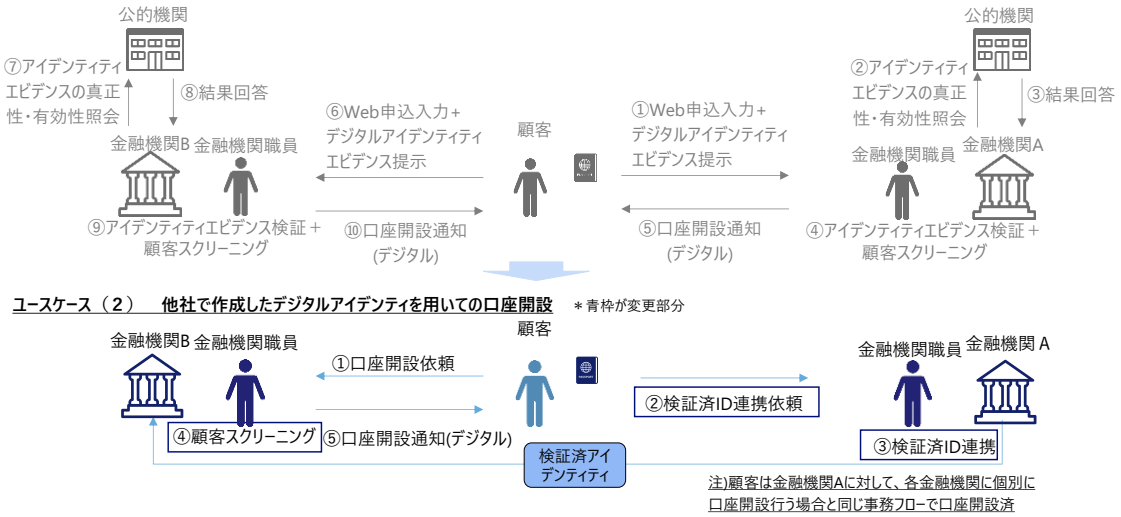


図 2- 19　他社作成のデジタルアイデンティティの活用業務

デジタル化により解決される課題

他社のアイデンティティエビデンスを利用することで、以下の課題については、解消もしくは程度の低減につながるものと想定される。

- 金融機関毎に同様の口座開設申込を行う負担
  顧客サービス面での改善が期待できる。
- 他社で検証済の顧客を一から確認する負担
  他社での検証結果を利用することで金融機関サイドの負荷も軽減される。

凡例
~~黒字：ユースケース（１-２）への移行により解決するユースケース(1)の課題~~
黒字：ユースケース（１-２）への移行でも解決困難なユースケース(1)の課題
青字：ユースケース（１-２）により新たに生じる課題

業務プロセス	AML/CFTに関する課題(金融機関/当局)	サービス向上に関する課題(顧客/金融機関)
申込受領	・Web申込用のインフラ整備・運用コスト ・ID連携当事者間のビジネスモデル・責任分界の未整備	・Web申込入力負担 ~~・金融機関毎に同様の口座開設申込を行う負担~~ ・デジタル対応できない人物の金融排除 ・煩雑なID連携仕様への対応負担 ・ID連携の同意管理負担
取引時確認	~~・他社で検証済の顧客を一から検証する負担~~ ・デジタルIMSの適切な活用を促す規制フレームワーク整備 ・最適化された既存業務をデジタルIMS利用のために変更する投資判断が困難	・連鎖的な口座開設等の新たなセキュリティ・リスクへの対応 ・特定の金融機関(IdP)への依存リスクが高まる
顧客フィルタリング	~~・他社で検証済の顧客を一から検証する負担~~	
分析・評価		
判断・対応		

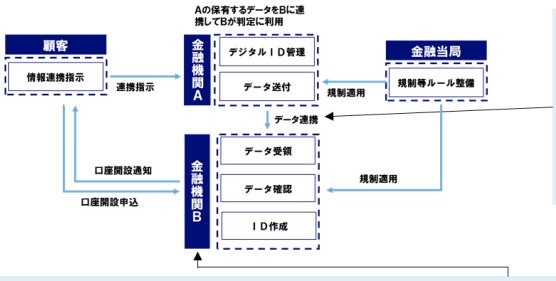
図 2- 20　ユースケース（１-１）（自社のみ）からユースケース（１-２）（他社作成デジタル ID を利用）への移行により解消される課題と新たに発生する課題まとめ

新たに発生する課題

口座開設申込における金融機関・顧客の更なる省力化が図られる一方、当事者間の責任分界の未整備等の課題が発生する。

- ID 連携当事者間のビジネスモデル・責任分界の未整備

  データ過誤による問題発生時の賠償責任分担が折り合わないという課題が発生する。また、責任分界とその対価のミスマッチも生じる。



【論点２】金融機関A(IDの出し手)のデータに過誤があり、それが原因で金融機関B(IDの受け手)側で問題が発生した場合の処置

- IDの出し手のデータに過誤があり、IDの受け手に損害を与えた場合における損害賠償責任等を検討する必要がある。
- 損害賠償の額については、論点1で言及した責任の範囲や、過誤の理由(IDの出し手の管理不備、サイバーテロ、顧客の提供情報に誤りあり、等)により異なる。

【論点１】金融機関A(IDの出し手)から金融機関B(IDの受け手)に連携された顧客の本人確認やKYCの責任

以下２パターンが考えられ、当事者間でやり取りされる対価等を勘案し責任範囲を検討する必要がある。

#	パターン	想定される各参加者の業務
1	金融機関A(IDの出し手)に責任	・金融機関Bは連携された情報を本人確認済情報として利用する。(責任小) ・金融機関Aの責任範囲は、顧客データを直近化して確認の上連携する等大きくなると考えられる。(責任大) かつ、金融機関Aへの過度な依存により金融機関BのKYC能力の弱体化、ひいては業界全体のKYC弱体化を懸念する意見もある。
2	金融機関B(IDの受け手)に責任	・金融機関Bは受領情報を参考に、自ら本人確認を再度実施する。(責任大) ・金融機関AはID情報を参考情報として連携する。(責任小)

図 2- 21　ID 連携当事者間の責任分界に係る論点

- 煩雑な ID 連携仕様への対応負担

  ID 連携にあたっては、仕様が共通化していることが望ましいが、各金融機関の業務の差異等から、多数の仕様が乱立している。

- ID 連携の同意管理負担

  ID 連携の内容と範囲について金融機関等 ID 提供者（IdP）と顧客との同意管理が不十分であり、個人情報保護法令に違反するリスクがある。

- 特定の金融機関（IdP）への依存リスク

  顧客が他社で作成したアイデンティティを用いての口座開設を複数金融機関に対して行うと、顧客の検証済アイデンティティ提供金融機関（下図金融機関 A）に対する依存度が高まり、これに伴うリスクが懸念される。下図の金融機関 A での検証に問題が発生した場合、ID 連携先である下図の金融機関 B のサービスに影響が発生する。

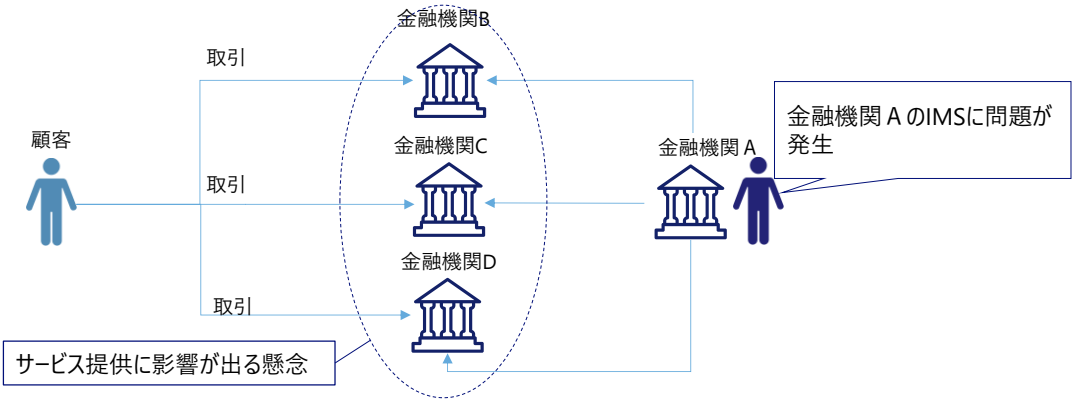


図 2- 22　IdP である金融機関に不具合が発生した場合の影響

3）ユースケース（２）継続的顧客管理

業務の概要　（デジタル化による変化）

デジタル IMS 化により金融機関⇔顧客のやり取りもアナログからデジタルに変化する。さらに、デジタル IMS 化により他社データを活用した分析も実施されることが予想される。

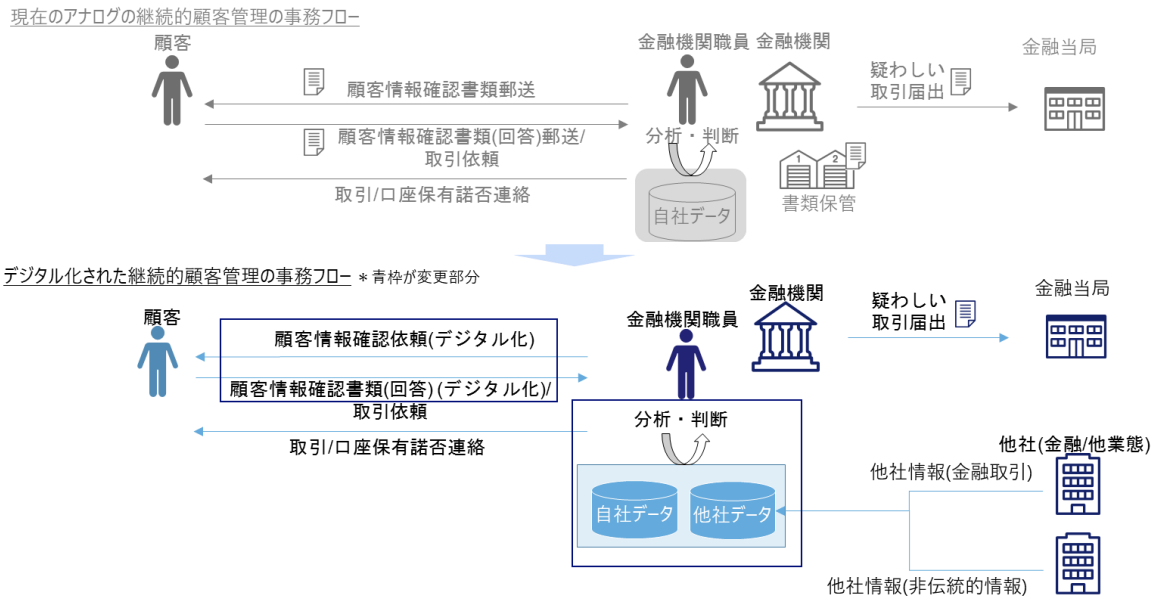


図 2- 23　デジタル化された継続的顧客管理業務

デジタル化により解決される課題

継続的顧客管理におけるデジタル IMS により、以下の課題が解消、低減されると想定される。

- 取引申請書類をデータ化する負担
  （既述）
- 郵便物の返送手続負担
  アイデンティティエビデンスや取引諾否に関する郵便物のやり取りの減少が期待できる。
- 大量の顧客に対する検証事務負担
  アイデンティティエビデンスがデジタル化されることで、多数の顧客に対応する金融機関の負担が大幅に削減される。
- 取引時のセキュリティリスク（非対面でアクセス時のパスワード盗取など）
  パスワードに加え生体認証等活用により、アクセス情報の盗難による被害等のセキュリティリスクが削減される。
- アナログの顧客情報収集郵電費・データ化負担
  顧客と金融機関間のやりとりがデジタル化されることで、郵送・データ化が不要となる。

デジタル化により高度化される業務

- リスクベース・アプローチの高度化
  FATF はデジタルアイデンティティに関するガイダンスにて、デジタルアイデンティティによる新たな技術を活用したリスク低減措置の高度化の可能性へ言及している。[122]
  - 顧客に紐づく情報の拡大
    - ジオロケーション、IP アドレス、取引に利用したデジタルデバイスの ID 等
    - インターネットや携帯電話等の様々なチャネルを通じて得られる追加情報
  - 広範な情報を用いた顧客の行動分析
    - アクセスしている人物に対する本人認証の強化
    - 異常なもしくは疑わしい取引検知の強化
  - 金融包摂
    - 新興国における従来の公的書類（パスポート、運転免許証等）の代替手段

[122] FATF, “Guidance on Digital Identity (2022)”
http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html

- 新興国におけるデジタルアイデンティティの保証レベルに応じた金融サービスの提供

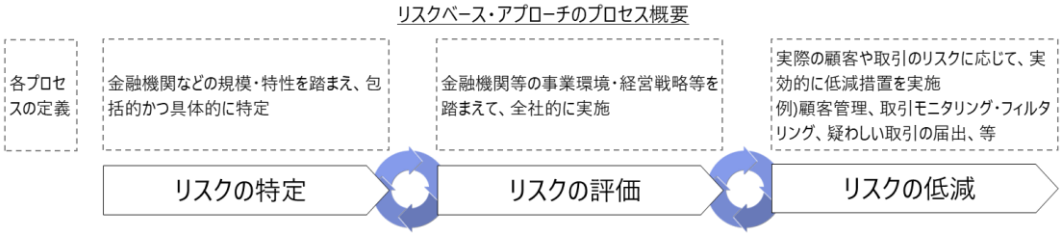


図 2- 24　リスクベース・アプローチのプロセス概要

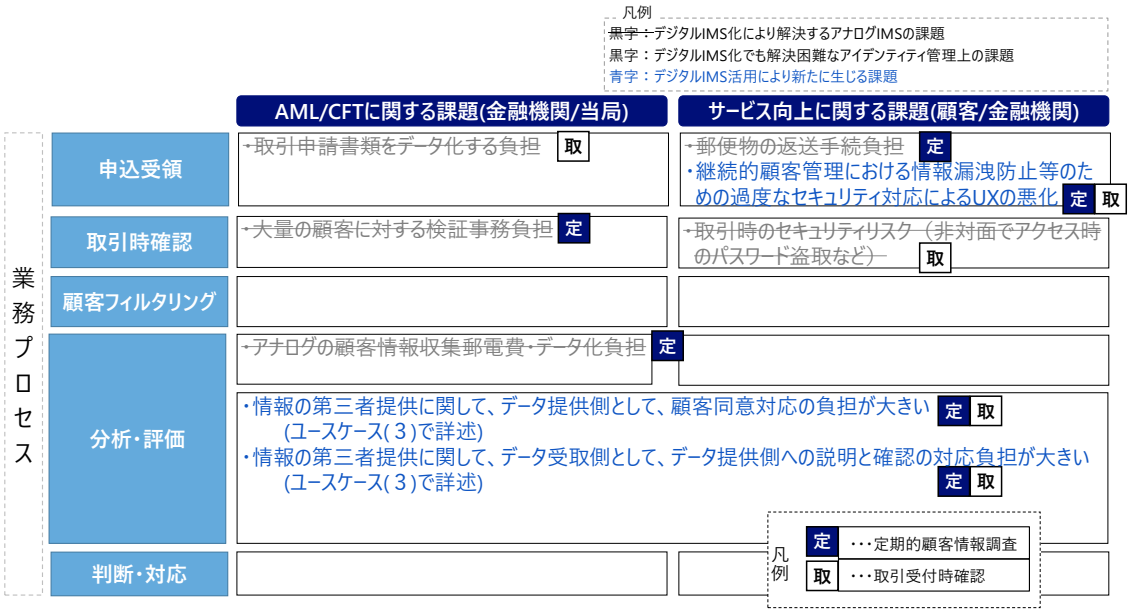


図 2- 25　継続的顧客管理におけるアナログ IMS のデジタル IMS 化により解消される課題と新たに発生する課題まとめ

新たに発生する課題

リスクベース・アプローチの高度化やコスト削減が図られる一方、他社データ利活用に対する課題が新たに発生する。

- 継続的顧客管理における情報漏洩防止等のための過度なセキュリティ対応による UX の悪化

  情報漏洩への対応が過度になった場合に、UX の低下が生じる可能性がある。

- 情報の第三者提供同意管理負担

  情報の第三者提供に関して、データ提供側として、顧客同意対応の負担が大きい。また、データ受け取り側として、データ提供側への説明と確認の対応負担が大きい。（ユースケース（３）で詳述）

4）ユースケース（3）他社情報を活用したサービス提供

業務の概要　（デジタル化による変化）

デジタル IMS 化により他社保持データも含めたアイデンティティ情報の収集・活用が容易となり、顧客に対し、より最適なテーラーメードサービスの提供等が期待される。

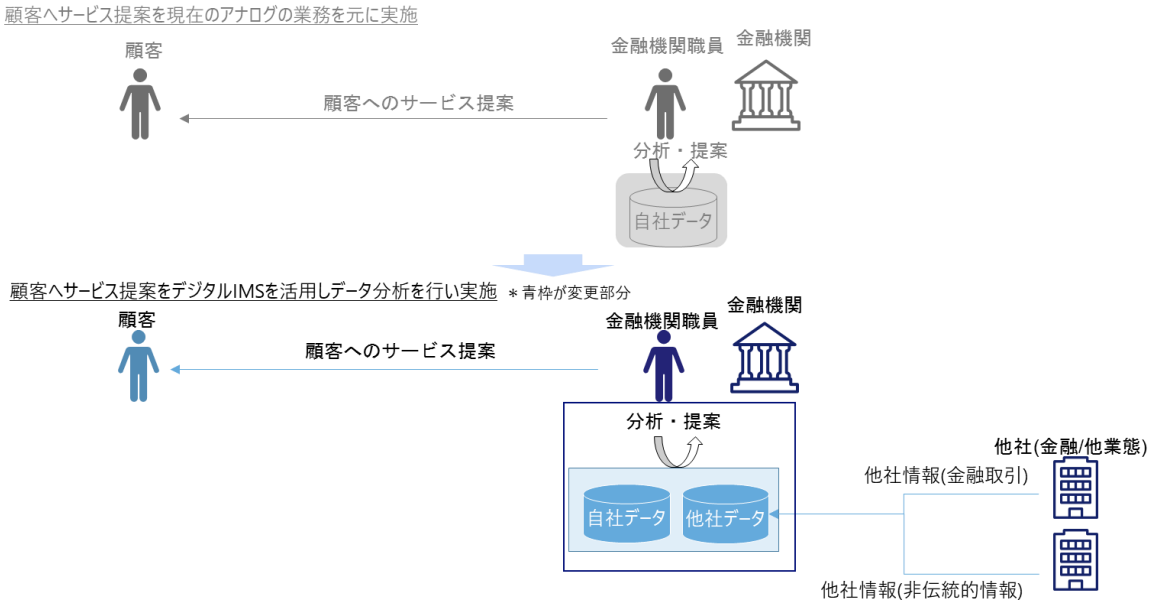


図 2- 26　他社情報活用のイメージ

デジタル化により解決される課題

他社情報を活用したサービス提供におけるデジタル IMS により、以下の課題が解消、低減されると想定される。

- 識別子の不一致によりデータ集約が困難

  他社データとの顧客識別子不一致が解消されることにより、各社の顧客 DB で持つ顧客識別子を、デジタル IMS 上で顧客を一意に表す顧客識別子に紐づけて管理することが可能になる。さらに、このような外部との識別子の一致をドライバーにして社内の各部門での識別子の統合とデータ利活用を促進する。

  ただし、データ利活用の促進に当たり、顧客のアイデンティティ情報の紐づけは解決策の一部であり、データを横串で利用できるよう顧客とのデータ利用許諾規定を見直す等、引き続き残る課題がある。

  なお、アイデンティティ情報の連携は、社内の部門間から企業間に広がることが期待されるが、効率的連携には連携仕様の整備が重要である。この点、デジタル IMS においては、1 章で述べた OpenID Connect®等のアイデンティティ連携仕様の活

用により、アイデンティティ情報の連携はより行いやすくなることが期待される。（下記左図参照）

また、前述の通り、金融機関においては個別最適化されたデータ・システムが多数存在しているケースもあるため、現実的には、下記右図のように、業務や利用目的が近いシステムに対し部分的に統一を図っていくことで段階的に成果を出していく形が考えられる。

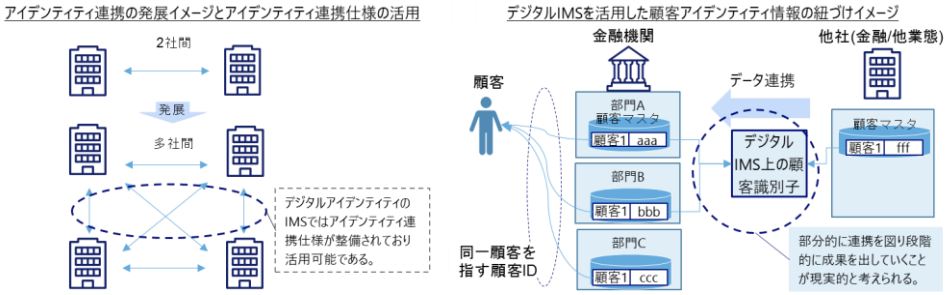


図 2- 27　デジタル IMS を活用した顧客識別子の統一

凡例
黒字：デジタルIMS化により解決するアナログIMSの課題
黒字：デジタルIMS化でも解決困難なアイデンティティ管理上の課題
青字：デジタルIMS活用により新たに生じる課題

業務プロセス	AML/CFTに関する課題(金融機関/当局)	サービス向上に関する課題(顧客/金融機関)
申込受領		
取引時確認		
顧客フィルタリング		
分析・評価	・複数サービス横断で顧客データを利活用するための、データ利用許諾の整備負担 ・情報の第三者提供に関して、データ提供側として、顧客同意対応の負担が大きい ・情報の第三者提供に関して、データ受け取り側として、データ提供側への説明と確認の対応負担が大きい	識別子の不一致によりデータ集約が困難 ー部門/組織毎の管理により顧客識別子不一致 ー他社データとの顧客識別子不一致 ・社内外のデータフォーマットの不統一によりデータ集約が困難 ・データ利活用の目的と範囲に関する、顧客と金融機関の認識齟齬リスクの増大
判断・対応		

図 2- 28　他社情報を活用したサービス提供のデジタル IMS 化により解消される課題と新たに発生する課題まとめ

新たに発生する課題

他社保持データも含めたアイデンティティ情報の収集・活用が容易となる結果、他社から情報を受け取り利用するためのルール整備に関する課題が発生する。

- 情報の第三者提供に関して、データ提供側として、顧客同意対応の負担が大きい

情報共有に対するプライバシーへの配慮が不十分で個人情報保護法令違反リスクがある。

- 情報の第三者提供に関して、データ受け取り側として、データ提供側への説明と確認の対応負担が大きい

  情顧客情報を受け取る金融機関についても、データの出し手に対するデータ取得経緯等の確認負担やデータ利活用の目的・内容等をデータ提供側に説明し、理解を得る負担等が発生する。

2-3-4. その他技術的課題

これまで述べてきた、3 つのユースケースには分類が難しいが既存研究等で指摘されている技術的課題として以下のようなものが挙げられる。

1）サイバーセキュリティ・データセキュリティに係る課題

課題の概要	課題の詳細
デジタル ID 集中による サイバーセキュリティ 脅威の増大	ID プロバイダがデジタル ID を集中管理すると、犯罪者から大量のデジタル ID を一度に狙われるリスクが高まる。より高いセキュリティレベルが求められる[123]。
オンライン ID 窃盗	ID がデジタル化されると、オンラインでの ID 窃盗のリスクが高まる。デジタル ID の導入と並行して ID 管理に対するセキュリティレベルの向上も必要である[124][125]。
トラストアンカーの 突然死	身元確認が第三者によって実施される場合、トラストアンカーの身元確認プロセスに障害が発生すると、影響範囲が広がり、エコシステム全体に影響を与えることになる[126]。

[123] “Digital Identities in Financial Services Part 2: Responsible Digital Identities, The Key to Creating More Inclusive Economies（Oct 2019）“
https://www.iif.com/Portals/0/Files/content/Innovation/10142019_responsible_digital_ids.pdf

[124] FATF, “Guidance on Digital Identity （2020）”
http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html

[125] OIX “The value of digital identity to the financial service sector （Dec 2016）”
https://openidentityexchange.org/networks/87/item.html?id=202

[126] DG-FISMA, “ASSESSING PORTABLE KYC/CDD SOLUTIONS IN THE BANKING SECTOR”
https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/assessing-portable-kyc-cdd-solutions-in-the-banking-sector-december2019_en.pdf

インサイダーの脅威	ID プロバイダがデジタル ID を集中管理することで、内部の犯行者が現れるリスクが高まる。ID プロバイダ内部のアクセス権限の管理レベル、セキュリティレベルの向上が求められる。[123]
記録の完全性	ある企業で作成したデジタル ID を他者が利用し、何らか問題が発生した場合、責任の所在を明確にする必要があるため、デジタル ID の作成や更新の記録が完全でなければならない[127]。

２）認証・認可に係る課題

課題の概要	課題の詳細
申請者が ID の真の所有者であることの確認	バイオメトリクスの活用、ID データベースの検証・取消リストの活用など、より高度な技術で、申請者が ID の真の所有者であることを確認する必要がある。120
認証技術の有効性についての継続的な測定	継続的認証技術の測定方法が成熟していないため、ID に紐づけられる属性が変化する可能性がある。分析システムは ID が詐欺等により悪用されることを示唆するリスク・シグナルを検知できる可能性がある。[124][125]

2-3-5. 金融機関からのデータ参照先に関する課題

１）法人の実質的支配者確認に関する課題をめぐる動向

本調査において、法人の実質的支配者の確認負担が大きいという意見が金融機関から提示されているが、現状 FATF は、2019 年 10 月公表の「best-practices-beneficial-ownership-legal-persons」[128]において、FATF の相互審査で示された各国の実情を鑑み、実質的支配者確認において、複数の情報を組み合わせて判断する手法を推奨しており、ある程度の確認負担の発生はやむを得ない側面もある。

[127] DG-FISMA, “Report on existing remote on-boarding solutions in the banking sector” https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf

[128] FATF best-practices-beneficial-ownership-legal-persons (Oct.2019) https://www.fatf-gafi.org/media/fatf/documents/best-practices-beneficial-ownership-legal-persons.pdf

表 2- 10　FATF が推奨する実質的支配者情報収集のアプローチ[129]

#	アプローチ名称	概要	実質的支配者の照会先	
1	the Registry Approach	登記簿に実質的支配者に関する 最新の正しい情報を集約 （できる仕組みづくり）	登記簿	
2	the Company Approach	各会社が実質的支配者に関する 最新の正しい情報を管理 （できる仕組みづくりと政府からの要求）	各会社	
3	the Existing Information Approach	既存の情報源を利用	外部の情報源	会社登記情報やその他の種類の登記簿 （土地、自動車、移動可能な財産の登記簿など）
				金融機関や DNFBP[130]
				その他の当局（監督官庁や税務当局）、証券取引所が保有する情報、商業データベース、など

むしろ、FATF においてもこうした対応が推奨されている根本的な課題としては、法人の実質的支配者確認における実質的支配者情報の確からしさを担保する仕組みが確立されていないこと、であると考えられる。

このような課題に対し、各国それぞれが制度の整備等を実施、検討している。

例えば、日本では、法務省民事局において、犯罪収益移転防止法施行規則第１１条第２項第１号の実質的支配者（以下 BO）を対象として、商業登記所が BO リストの保管と写しの交付をする制度が検討されている。

（令和２年７月法務省民事局「商業登記所における法人の実質的支配者情報の把握促進に関する研究会取りまとめ概要」より）

[129] “FATF best-practices-beneficial-ownership-legal-persons”（同上）を元に NRI 作成

[130] 指定非金融業者及び職業専門家（Designated non-financial businesses and professions）

- 日本では、公証人の行う定款認証における株式会社等の BO の申告制度により、会社設立時に公証人による BO 情報確認が行われている。
- 今後の課題は、①法人の設立後における継続的な BO の把握及び②公的機関が把握した BO 情報への捜査機関等によるアクセス。
- 専門性を有する商業登記所の登記官が実質的支配者を確認するハブとなって統一的に判断を行うことにより、個々の金融機関が窓口でその都度確認を行っている現状に比べ、運用の統一性及び一定レベルの判断水準が担保されることにより信頼性が向上するとされている。

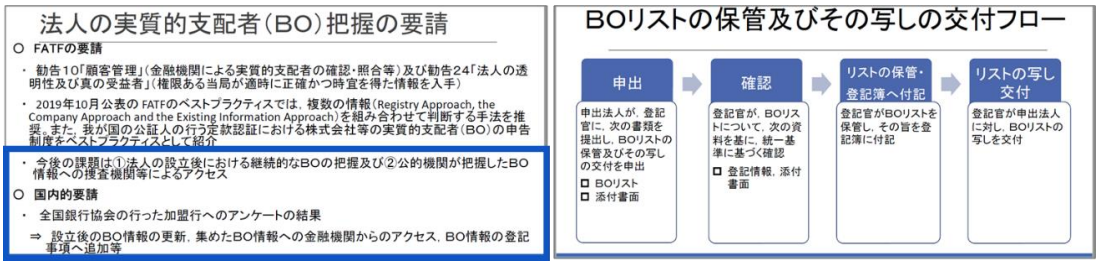


図 2- 29　我が国における法人の実質的支配者把握の要請と商業登記所による保管と写しの交付案[131]

2）クロスボーダー取引の諸課題をめぐる動向

FSB が 2020 年 4 月に G20 に提示したクロスボーダー送金の改善に向けた取り組み[132]の第一次報告書[133]では、クロスボーダー送金は、高コスト、低速、限定的なアクセス、透明性不足といった課題に直面している点が指摘されている。同報告書では、法規制や監督フレームワークに関わる論点として、多様な法的・規制慣行を持つ複数の国・地域をまたいでクロスボーダー送金を行う際の摩擦が指摘されている。

コンプライアンスの質を損なうことなく、また、適切な監督を確保しつつ、AML/CFT やその他のコンプライアンスプロセスの効率性を改善しコストを削減するために、どのような取り組みが考えられるか検討すべきとしている。

---

[131] 法務省「商業登記所における法人の実質的支配者情報の把握促進に関する研究会取りまとめ概要」http://www.moj.go.jp/content/001324012.pdf

[132] 2020 年 2 月の G20 財務大臣・中央銀行総裁会議において、優先事項としてクロスボーダー送金の改善に取り組んでいくことを決定。金融安定理事会（FSB）に対し、市場インフラ委員会（CPMI）等と協力して 2020 年 10 月までにクロスボーダー送金の改善に向けた工程表（ロードマップ）作成を要請

[133]FSB, “Enhancing Cross-border Payments Stage 1 report to the G20,Apr 2020” https://www.fsb.org/wp-content/uploads/P090420-1.pdf

関連する議論として、2021 年 6 月に改正された FATF 解釈ノートにより暗号資産の移転時に課せられる通知義務（いわゆるトラベルルール）に関しても、各国の AML/CFT 法令の導入が進むと共に、差異に対する対応は FATF 自身も課題と認識している[134]。これらのことから、クロスボーダー取引におけるアイデンティティ管理上の課題は、 AML/CFT 規制の国家毎の差異や、FATF 基準及びその他の規制・監督上の要件を実施する際の国境を越えたデータ共有への法的な障壁（各国のデータ保護規制等）、等法規制面のものが主であると考えられる。（金融機関のアナログ IMS がデジタル IMS 化されることで解決されるものではないと考えられる。）

加えて、FSB の第一次報告書では、“企業のための法人識別子（LEI）及び個人のためのデジタル ID の使用の拡大”といったデジタルアイデンティティに関する取り組みがあげられており、これは、金融機関が個人・法人についてのアイデンティティ情報をより効率的に確認するための周辺情報の整備の取り組みであると考えられる。

国内金融機関に対するヒアリングにおいても、クロスボーダー取引における国を跨いだ顧客の情報収集の負担の声はあり、期待される施策であると考えられる。

FSB における課題解消に向けた取り組み

FSB は、 2020 年 7 月に課題改善のための 19 の構成要素（Building Blocks, 以下「BB」）を特定した第二次報告書を公表。 2020 年 10 月には BB ごとの検討ロードマップを第三次報告書として公表している[135]。

デジタルアイデンティティに関わる課題については、下図の BB5、BB6、BB8、BB16 を中心に議論がなされている。

[134] ACAMS Today「暗号資産・暗号資産交換業者に関する新たな FATF 基準についての 12 か月レビュー」におけるトラベルルールの課題,Nov 2020
https://www.fsa.go.jp/frtc/kikou/2020/FSA_article_ACAMSToday2020_Sept-Nov.pdf

[135] FSB, “Enhancing Cross-border Payments Stage 3 roadmap （13 October 2020） “
https://www.fsb.org/wp-content/uploads/P131020-1.pdf

図 2- 30　フォーカスエリアおよび関連するビルディングブロック[136]

2-3-6. デジタル IMS 活用による課題の解消と発生

1）デジタル IMS 化により解決されるアナログ IMS の課題

これまで見たように、デジタル IMS 化によって、アイデンティティエビデンスの検証負担等の事務負担リスクベース・アプローチ等、その大多数が解消する。

一方、社内の複数サービスのデータや他社データを利活用するためのデータ利用許諾等、データ利活用に関する課題は引き続き残る。

なお、金融機関からのデータ参照先に関する課題については、アナログ IMS の課題ではないため下表には記載していない。

凡例
文字：デジタルIMSにより解消される非対面・アナログIMSの課題

業務プロセス	AML/CFTに関する課題(金融機関/当局)	サービス向上に関する課題(顧客/金融機関)
申込受領	~~・アイデンティティエビデンス情報をデータ化する負担~~ ・Web申込用のインフラ整備・運用コスト	・Web申込入力負担 ~~・金融機関毎に同様の口座開設申込を行う負担~~ ~~・郵便物の返送手続負担~~
取引時確認	~~・アナログ・アイデンティティエビデンスの検証困難性~~ ~~・他社で検証済の顧客を一から検証する負担~~ ~~・非対面化に伴う本人確認の難度上昇~~ ~~・大量の顧客に対する検証負担~~	~~・取引時のセキュリティリスク（非対面でアクセス時のパスワード盗取など）~~
顧客フィルタリング	~~・他社で検証済の顧客を一から検証する負担~~	
分析・評価	~~・アナログの顧客情報収集郵電費・データ化負担~~ ~~・自社データのみを利用した犯罪検知の限界~~ ・複数サービス横断で顧客データを利活用するための、データ利用許諾の整備負担	~~・識別子の不一致によりデータ集約が困難~~ ~~・部門/組織毎の管理により顧客識別子不一致~~ ~~・他社データとの顧客識別子不一致~~ ・社内外のデータフォーマットの不統一によりデータ集約が困難 ・データ利活用の目的と範囲に関する、顧客と金融機関の認識齟齬リスクの増大
判断・対応	~~・所在確認のための口座開設通知郵送コスト~~	

図 2- 31　デジタル IMS 活用により解消される課題と残される課題

136　同上（日本語は NRI 抄訳）

2）デジタル IMS 化により新たに発生する課題

2-3 のユースケース分析で見たように、デジタル IMS 活用で新たにいくつかの課題が生じる。

		AML/CFTに関する課題(金融機関/当局)	サービス向上に関する課題(顧客/金融機関)
業務プロセス	申込受領	・ID連携当事者間のビジネスモデル・責任分界の未整備	・デジタル対応できない人物の金融排除 ・煩雑なID連携仕様への対応負担 ・ID連携の同意管理負担 ・継続的顧客管理における情報漏洩防止等のための過度なセキュリティ対応によるUXの悪化
	取引時確認	・デジタルIMSの適切な活用を促す規制フレームワーク整備 ・最適化された既存業務をデジタルIMS利用のために変更する投資判断が困難	・連鎖的な口座開設等の新たなセキュリティ・リスクへの対応 ・特定の金融機関(IdP)への依存リスクが高まる
	顧客フィルタリング		
	分析・評価	・情報の第三者提供に関して、データ提供側として、顧客同意対応の負担が大きい ・情報の第三者提供に関して、データ受け取り側として、データ提供側への説明と確認の対応負担が大きい	
	判断・対応		

図 2- 32　デジタル IMS 化により新たに発生する課題

3）デジタル IMS の課題

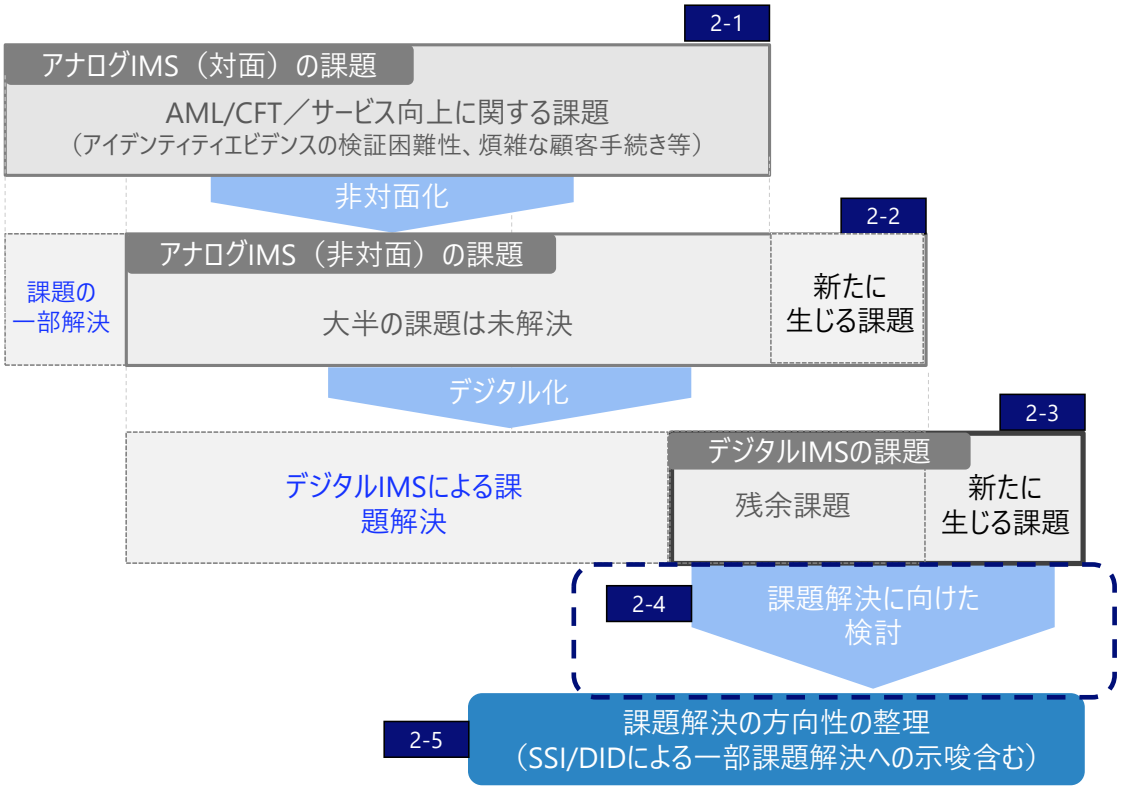
1)、2）を合わせ、デジタル IMS としての課題は以下の 9 点になる。

なお、8）9）は本調査においては課題の提示にとどめ、次節以降の記載を割愛する。

表 2- 11　デジタル IMS 化でも解決しなかったアイデンティティ管理上の課題およびデジタル IMS 化により新たに発生する課題一覧

課題の観点	課題
1）IAL	・デジタル IMS の適切な活用を促す規制フレームワーク整備
2）ID 連携 （責任分界を中心に）	・ID 連携当事者間のビジネスモデル・責任分界の未整備 ・特定の金融機関（IdP）への依存度が高まる
3）プライバシー （同意管理・ データミニマイゼーション）	・ID 連携の同意管理負担 ・複数サービス横断で顧客データを利活用するための、データ利用許諾の整備負担 ・情報の第三者提供に関して、データ提供側として、顧客同意対応の負担が大きい ・情報の第三者提供に関して、データ受け取り側として、データ提供側への説明と確認の対応負担が大きい ・データ利活用の目的と範囲に関する、顧客と金融機関の認識齟齬リスクの増大
4）金融包摂	・デジタル対応できない人物の金融排除
5）相互運用性	・煩雑な ID 連携仕様への対応負担
6）新しい業務へ移行するための投資判断	・最適化された既存業務をデジタル IMS 利用のために変更する投資判断が困難
7）金融機関からのデータ参照先に関する課題	・法人の実質的支配者確認に関する課題 ・クロスボーダー取引の諸課題
8）その他ビジネス上の課題 （UX 改善、IT インフラ整備）	・Web 申込入力負担 ・継続的顧客管理における情報漏洩防止等のための過度なセキュリティ対応による UX 悪化 ・連鎖的な口座開設等の新たなセキュリティリスクへの対応 ・社内外のデータフォーマットの不統一によりデータ集約が困難
9）その他技術的課題	・2-3-4 に記載の一連の技術的課題

2-4. デジタル IMS の課題解決（先進的事例）



アナログによる IMS の抱える課題について、デジタル IMS はその多くを解決するものの、デジタル化に関わらず残される課題、デジタル化による新たな課題が発生することを前節で提示した。本節では、そのようなデジタル IMS が抱える課題について、どのような解決の方策があるのか、諸外国等の先進事例を見ることで検討していく。

2-4-1. 先進事例と対応する課題

デジタル IMS の課題解決においては、欧米先進国だけでなく、東南アジア、南アジア等のデジタル化が進んでいる国においても参考になる事例が存在する。この節では、幅広く事例を参照していくことで、課題解決への示唆を得ていくこととする。

表 2- 12 デジタル IMS の課題と参考事例

課題の観点	事例
1） IAL	①EU、②シンガポール、③インド、④英国
2） ID 連携 （責任分界を中心に）	⑤ID 連携サービス ⑥標準化団体の取り組み

3） プライバシー （同意管理・ データミニマイゼーション）	本課題については、SSI/DID による課題解決が期待されている分野であるため、 3 章で詳細を議論する
4） 金融包摂	③インド
5） 相互運用性	⑨オーストラリア、⑥標準化団体の取り組み
6） 新しい業務へ移行するための 投資判断	⑤ID 連携サービス
7） クロスボーダー取引の諸課題	クロスボーダー取引(越境金融)について、 以下 2 事例 ⑦民間発行 ID、⑧欧州大手金融機関

2-4-2. 先進事例の内容

（1）EU における金融規制とアイデンティティ保証フレームワーク（eIDAS）の接合に向けた取組み

EU においては、欧州委員会が公共サービス向け規定である eIDAS の民間サービスにおける適用可能範囲の拡大を検討している。金融機関が EU における越境金融サービスの提供に向けて eIDAS に準拠したデジタル ID を提供することにより EU における金融機関間の IAL 統一化が促進される見込みである。

また eIDAS の適用拡大と合わせて、次期 AML 指令もしくは AML ルールブックへ顧客確認プロセスの統一規定追加が検討されている。これにより EU 加盟各国の国内 AML/CFT 法規制へ反映され、EU における金融機関間の顧客確認プロセス統一化が促進される見込みである。

表 2- 13 事例① EU における金融規制とアイデンティティ保証フレームワーク（eIDAS）の接合に向けた取り組み

対象課題	1） IAL
課題対応の方向性 ＜対応前＞	・ eIDAS の LoA(IAL)と金融における本人確認・顧客管理の対応が EU レベルでは取れず、加盟国の規制に委ねられた結果、規制がパッチワーク化しコンプライアンスコストが増大している状況である。 ・ プライバシー保護については、GDPR との対応が検討されているが、論点の指摘に留まる。
＜対応後＞	・ eIDAS の民間サービスにおける適用範囲を拡大することにより、民間サービスにおける IAL の統一化が促進される見込みである。

	・次期 AML 指令制定もしくは AML ルールブック改訂時に eIDAS を踏まえた統一顧客管理規定が制定され、加盟各国の AML/CFT 規定へ反映される。 ・プライバシー保護は、EU 内におけるデータ共有可能な範囲が欧州委員会より発表される見込みである。
背景・成功要因	・欧州委員会の主導により 2016 年の施行以来 eIDAS が公共サービスへ広く導入されて来た。 ・AML 指令の強制力により、加盟各国の AML/CFT 規制改訂が 30 年に渡り継続的に実施されて来た。
成果	・eIDAS の民間サービス適用拡大および顧客管理規定の統一化により、加盟国間の越境金融サービスが促進される見込みである。 ・顧客管理規定の統一化により、加盟各国の AML/CFT が強化される見込みである。
今後の課題	・EU 域外の越境金融サービス促進に向けて、EU 域外との相互運用性を図れるか。 ・統一顧客管理規定が国内法化された際、KYC プロセス全体として加盟国間で調和を図れるか。

EU におけるデジタル ID 活用は、2010 年の EU 成長戦略「欧州 2020」の一環として ICT 戦略「欧州デジタルアジェンダ」の公表に端を発し（2015 年のデジタル単一市場（DMS）戦略により発展的解消）、2014 年の eIDAS 規制採択、2015 年の欧州決済サービス指令（PSD2）採択に見られる金融規制へ波及してきている。

表 2- 14　EU におけるデジタル ID 活用の経緯

時期	できごと	補足
2010 年	EU の成長戦略「欧州 2020」の一環として、ICT 戦略「欧州デジタルアジェンダ」を公表	DSM に発展的解消
2013 年	2014-20 年の EU 予算として、Connecting Europe Facility（CEF）が採択	eID の活用が CEF の取り組みの 1 つとして規定
2014 年	eIDAS 規則採択	施行：2016 年 7 月

2015 年	デジタル単一市場（DSM）戦略が公表	eIDAS は構成要素の位置付け、EU 加盟国間の越境取引の eID 活用重視
2015 年 11 月	PSD2（欧州決済サービス指令）採択	97 条で SCA（安全な顧客認証）の要求、98 条にて EBA が SCA の RTS（規制技術基準）の策定を規定 eID は法的義務ではない（推奨に留まる）
2017 年	DG FISMA において eID/KYC エキスパートグループ設置	eIDAS 下での識別・認証ツールに基づく、越境での eID および KYC ポータビリティの活用促進手法を検討
2017 年 11 月	PSD2 の SCA に関する RTS が EBA から公表	電子的支払いに対する認証方式の厳格化を規定
2018 年 7 月	AMLD5（第 5 次アンチマネー・ローンダリング指令）施行	eID の利用が推奨はされるものの LoA のレベルについては規定なし
同上	CEF の枠組において、DG Connect から eBanking における eID 活用に関する報告書が公表	銀行セクターにおける eID の活用可能性や規制上の論点（主要規制と eID との関係性等）について整理
2019 年 12 月	上記 eID/KYC エキスパートグループの報告書が完成（公表は 2020 年 3 月）	金融における eIDAS を含むデジタル ID の活用に関する 2 つの政策文書を発行 ・Report on existing remote on-boarding solutions in the banking sector ・ASSESSING PORTABLE KYC/CDD SOLUTIONS IN THE BANKING SECTOR: The case for an attribute-based & LoA-rated KYC framework for the digital age （2019.12）
2020 年 7-10 月	eIDAS 改正に向けたパブリックコンサルテーション	改正案は 2021 年夏頃に公表予定
2020 年 9 月	Digital Finance Strategy for Europe 公表	以下 3 つを規定

		・ 2021 年 Q3 までに他の金融機関等の実施した顧客確認への依拠を可能とするガイドラインを整備 ・ AML/CTF 規制の EU ワイドでの統一 ・ eIDAS 規制の民間 ID への拡張

なお、金融機関間の顧客確認プロセス統一化に関して、DG-FISMA は前述の 2019 年 12 月政策文書[137]において EU の現状を以下のように整理している。

・eIDAS が AMLD5 や PSD2 で参照されているが、金融機関の依拠すべき LoA に関して EU レベルのガイドラインはない。また顧客確認は LoA の確認に限られないため各加盟国が独自に規定している。

・顧客確認は単に LoA を確認するだけではなく AML 等の固有の確認事項があるため、結果として詳細はクロスボーダーの場合を含め、各加盟国における独自のアプローチに委ねられている。

また、同文書において本人確認及び顧客確認に必要な属性要素および継続的顧客管理に向けた各要素の更新頻度を提唱している。

・コアアイデンティティ属性（永続的または非常に安定した属性）：最低で 10 年

・ステータスまたはグッドスタンディング属性（変化しうる属性）：金融機関の判断

・コンタクト属性（不可避的に変化がある属性）　　：変化が発生次第

137 “ASSESSING PORTABLE KYC/CDD SOLUTIONS IN THE BANKING SECTOR: The case for an attribute-based & LoA-rated KYC framework for the digital age （2019.12）”
https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/assessing-portable-kyc-cdd-solutions-in-the-banking-sector-december2019_en.pdf

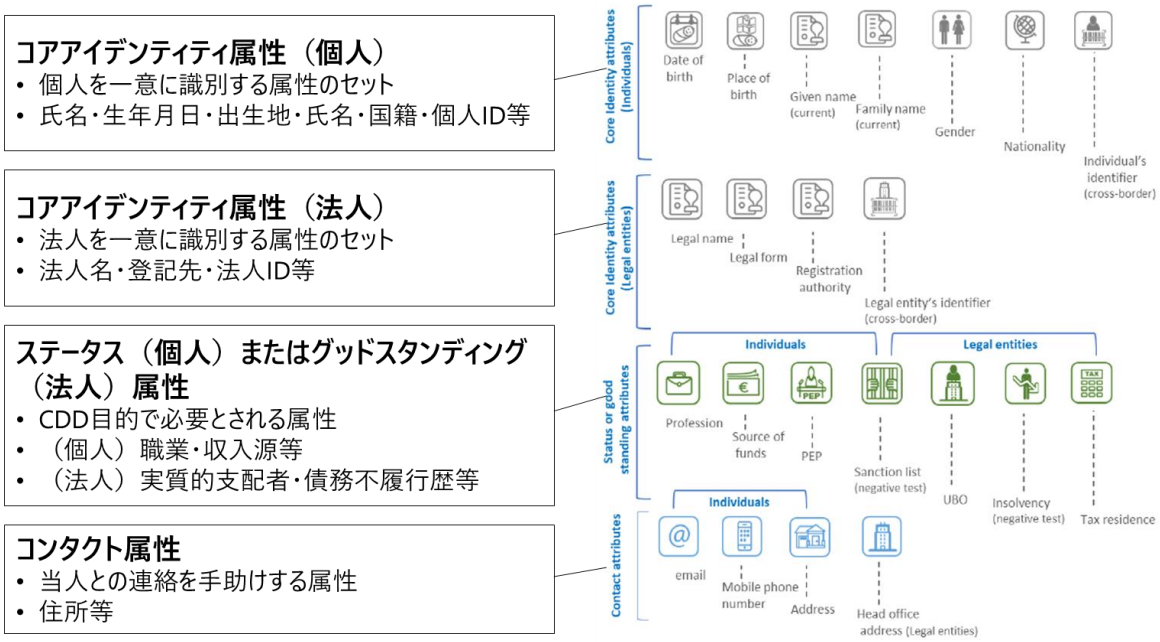


図 2- 33 DG-FISMA の提唱する属性要素分類

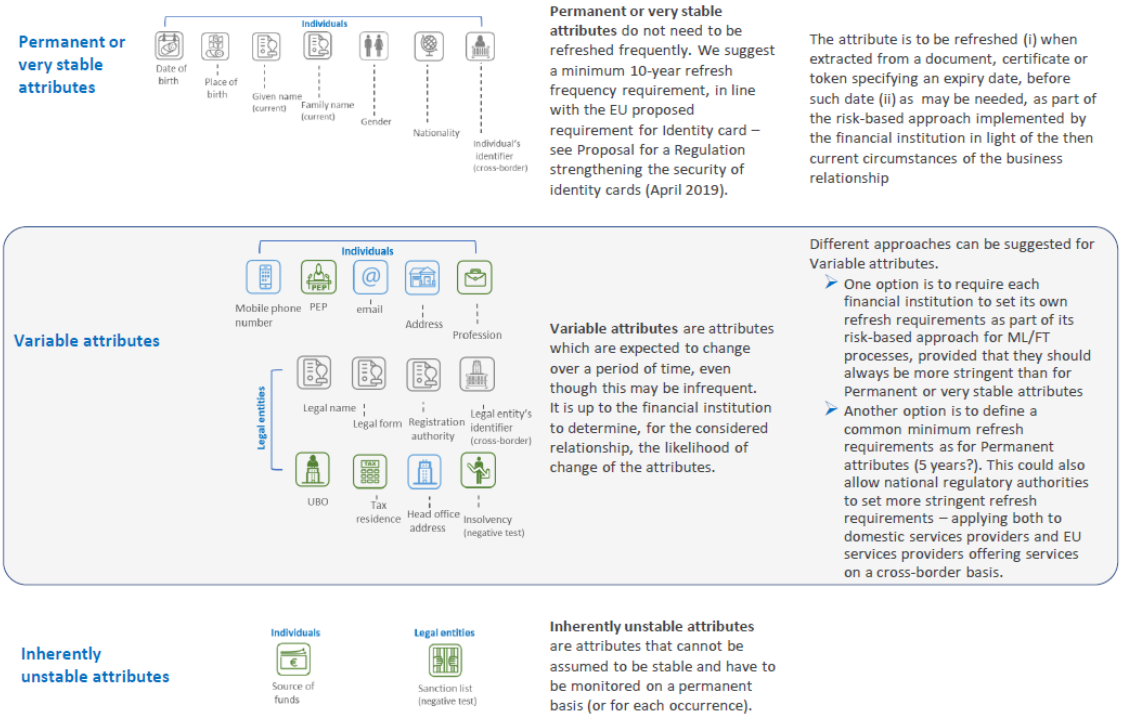


図 2- 34 DG-FISMA の提唱する属性要素更新頻度

（2）シンガポールにおける国民 ID を活用した onboarding の効率化

シンガポールにおいては 1948 年の国民 ID 導入以降、政府の主導で国民 ID の推進、普及が進められてきた。特に、政府オンラインサービス利用のための共有認証システムとして 2003 年に導入された SingPass は、多段階認証や生体認証の導入、さらに 2018 年の民間サービスへの開放により普及が促進された。

金融機関はこの認証基盤を活用し onboarding の効率化を実現している。

表 2- 15 事例②シンガポールにおける国民 ID を活用した onboarding の効率化

対象課題	1） IAL
課題対応の方向性 ＜対応前＞	・SingPass は政府オンラインサービス利用のための共有認証システム、MyInfo は行政サービス間の共通個人情報登録システムとして中央集権型プラットフォームで提供開始されるも、民間に開放されず。 ・一方で MAS 626 および解釈ノートにより非対面における本人確認書類や確認手法は細目化されていた。
＜対応後＞	・SingPass および MyInfo を民間サービスへ開放することにより、民間サービスは政府所有の本人確認情報を利用可能となり、法域内の IAL 統一が促進された。 ・生体情報や多要素認証追加、情報更新を政府主導で実施することにより、プラットフォームを利用する金融サービスの IAL を一律にボトムアップしている。
背景・成功要因	・政府の強力な主導により 20 年近くに渡り国民 ID が推進、普及されてきた。 ・SingPass が 2018 年、MyInfo が 2017 年に民間サービスへ開放された。
成果	・大手金融機関の新規オンボーディングがリモート化、オンボーディングコストも削減された。 ・リモートオンボーディング時の顧客情報を政府データから連携し入力項目を削減することでドロップ率が改善された。
今後の課題	・SingPass や MyInfo を AML/CFT へ利用出来ず、金融機関が独自に蓄積・検証したデータで対策を実施している。 ・国民 ID や長期滞在ビザを所有しない人が口座開設や金融サービスを利用するハードルはむしろ上がっている。

SingPass 導入の経緯

Singapore Personal Access（SingPass）は 2003 年に個人版、2016 年に法人版（Singpore Corporate Access)、2018 年からは SingPass Mobile を導入し、民間サービスへも開放された。2003 年導入当初の SingPass は行政オンラインサービスへアクセスするために国民 ID とパスワードを組み合わせた簡易な仕組みであったが、2015 年の 2 段階認証、2018 年の SingPass Mobile を利用した指紋認証や顔認証の導入により強化が図られている。また 2020 年 9 月には iProov 社の顔認証技術を採用[138]し、政府機関のキオスク端末における認証も可能とすることでスマートフォンを保有しない層の取り込みが図られている。

MyInfo 導入の経緯

MyInfo は行政サービス間で重複するデータの登録を防止する“Tell Us Once”サービスとして 2016 年に個人向けが、2018 年に MyInfo Business として法人向けが導入された。また 2017 年には民間サービスへ開放され、口座開設やクレジットカード申請への適用が開始された。代表的な例としては、M1 Remit 社のクロスボーダー送金、DBS 社および OCBC におけるクレジットカード申請、UOB における普通および当座預金口座、カーローンやクレジットカードのオンライン申請へ採用されている[139]。

NDI の構築

Smart Nation 政策のとして SingPass および MyInfo を基盤とした官民共通のデジタル認証基盤 NDI が構築中である。NDI Stack は 4 層で構成され、下位 2 層は政府主導によるトラストデータ（MyInfo）およびトラスト ID（SingaPass)、上位 2 層は官民協働によるトラストフレームワークおよびトラストサービスである。

なお、2019 年に Personal Data Protection Act が施行されたことにより国民 ID の収集、利用、保管、開示が原則禁止されたため、SG Verify の導入も始まっている。

---

[138] Businesswire “Singapore Government Extends National Digital Identity Programme With Face Verification Solution From iProov and Toppan Ecquaria” （September 22, 2020）
https://www.businesswire.com/news/home/20200921005898/en/Singapore-Government-Extends-National-Digital-Identity-Programme-With-Face-Verification-Solution-From-iProov-and-Toppan-Ecquaria

[139] Smart Nation Singapore “National Digital Identity （NDI） ”
https://www.smartnation.gov.sg/what-is-smart-nation/initiatives/Strategic-National-Projects/national-digital-identity-ndi

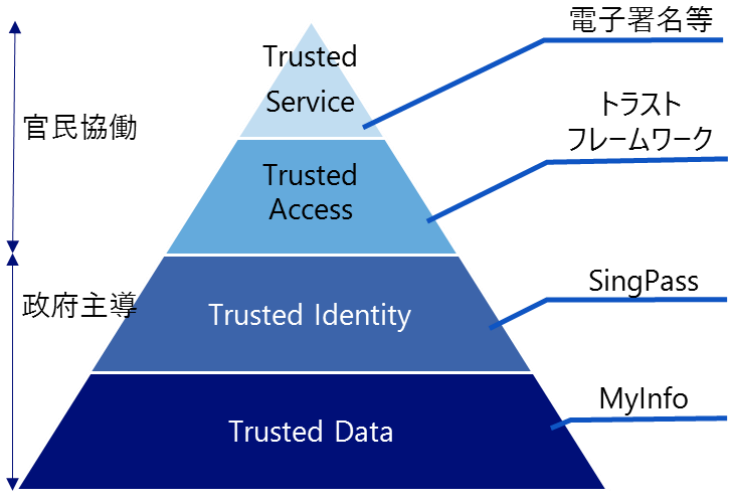


図 2- 35　NDI Stack の概要[140]

表 2- 16 シンガポールにおける国民 ID 普及の経緯

時期	できごと
1948 年	国民 ID の導入
2003 年	SingPass の導入 （国民 ID とパスワードによる行政サービスの利用）
2014 年	Smart Nation 構想
2015 年	SingPass へ 2 段階認証の導入
2016 年	MyInfo の導入
2017 年	MyInfo を民間サービスへ開放
2018 年	SingPass を民間サービスへ開放 SingPass Mobile の導入 （スマホによる指紋認証、顔認証が可能化）
2020 年	SingPass および MyInfo を基盤とした官民共通のデジタル認証基盤 NDI（National Digital Identity）を導入

[140] GovTech ウェブサイトを基に NRI 作成

（3）インドにおける India Stack を活用した民間サービスの拡大[141]

インドでは政府がデジタル決済化を主導し、Aadhaar を核とした認証決済基盤・India Stack を整備した。これにより India Stack を活用した民間サービス展開とともに爆発的に登録・利用が進んだ。

なお、Aadhaar について、導入以来プライバシーに関する批判があり、2018 年 9 月の最高裁判決により、Aadhaar による本人確認の民間利用が制限された。それまで Aadhaar 認証や eKYC を 積極的に活用してきた民間企業に対する影響が大きいため、モディ政権は大統領令（2019 年 3 月）とその後の Aadhaar 法の改正（2019 年 7 月）により、本人の同意のもとであれば民間企業も Aadhaar を本人確認に利用可能とした。民間企業は、本人が同意しなかった場合の Aadhaar 以外の本人確認方法を用意するなど、改正 Aadhaar 法に沿った対応を行っている。

表 2- 17 事例③インドにおける India Stack を活用した民間サービス

対象課題	1） IAL 4） 金融包摂
課題対応の方向性 ＜対応前＞	・低所得者層や遠隔層への社会保障、給付金の不正受給や中抜きが問題となっており、政府は全国民に識別番号を付番し給付金を国民の口座へ直接振込む形を目指していた。 ・識字率が 70%程度であったことから、生体認証の利用が検討されていた。
＜対応後＞	・政府は全国民への識別番号を付番と給付金直接振込を目指し、NPCI や UIDAI などの公的機関を設立し、Aadhaar、および、Aadhaar を ID とした認証・決済・口座登録機能 （”India Stack”）を公的基盤として開発・提供した。 ・モディ政権の「デジタルインド計画」により、Aadhaar および India Stack の登録・利用が爆発的に進んだ。
背景・成功要因	・政府がデジタル決済化を主導し、Aadhaar を核とした認証決済基盤・API 基盤（India Stack）を整備。 ・政府がデジタル決済の利用を拡大するための政策や法的整備を実施。 （2015 年に発表されたデジタル化政策「Digital India」の下、国民皆銀行口座プロジェクト、Aadhaar 法、等）

[141] 環太平洋ビジネス情報 RIM「India Stack：インドのデジタル化促進策にみる日本のマイナンバー制度への示唆」（2019 Vol.19 No.75）
https://www.jri.co.jp/MediaLibrary/file/report/rim/pdf/11416.pdf

対象課題	1） IAL 4） 金融包摂
成果	・登録は義務ではないものの現在成人の 99%以上が Aadhaar に登録している。 ・金融包摂が進み、公的証明を持っていない貧困層、農村部の遠隔層も金融サービスを利用できるようになった。 ・給付金の中抜き、さらにはマネー・ローンダリング、地下経済（脱税）の取り締まりも強化できた。
今後の課題	・プライバシー：銀行口座やＰＡＮカードとの紐付けは登録の「義務」につながり、各自が持つ 12 桁の番号を他者に知らせることはプライバシーの侵害であるとの指摘あり。 ・セキュリティ：システムがサイバー攻撃された場合、全ての登録データが危険にさらされるとの指摘あり。

インドにおける Aadhaar 拡大の経緯

低所得者層や遠隔層への社会保障と不正受給対策をきっかけとして、政府主導で決済のデジタル化が進められることとなった。偽造身分証明書や二重登録による不正受給、仲介機関による横領などが横行し、給付金・補助金が正当な受給者に届きづらかったため、国民すべてに識別番号を付番し、給付金を直接国民の口座に振り込めるようにすることを目指し、2007 年から活動母体が形成された[142]。

その後 2009 年に Aadhaar プロジェクトが開始され、2010 年からは Aadhaar をデジタル ID とした認証決済基盤・API 集合体（India Stack）を政府が提供したことで爆発的に登録・利用が進んだ。登録は義務ではないものの現在成人の 99%以上が登録している。

[142] COVID-19 in India - GOI's Economic Package for Self-Reliant （May 2020）, USDA（United States Department of Agriculture）
https://apps.fas.usda.gov/newgainapi/api/Report/DownloadReportByFileName?fileName=COVID-19%20in%20India%20-%20GOI%27s%20Economic%20Package%20for%20Self-Reliant%20India%20-%20Food%20and%20Agriculture%20Items_New%20Delhi_India_05-23-2020

表 2- 18 インドにおける Aadhaar 拡大の経緯[143][144][145]

時期	できごと
政府と銀行協会によるデジタル決済化主導の運営母体が形成される	
2007 年	PSS 法により、RBI（インド準備銀行（インドの中央銀行））がすべての決済システム（証券決済システムは除く）の認可・監督権限を持つ
2008 年	RBI がインド銀行協会と共同で NPCI（National Payment Council of India）を設立し、インドのリテール決済システムの運営母体となる。
Aadhaar プロジェクトが開始される	
2009 年	UIDAI（Unique Identification Authority of India）が設立され、Aadhaar プロジェクトが開始される。
”India Stack”と呼ばれる、Aadhaar を ID とした様々な認証・決済・口座登録機能および API が、公的基盤として開発・提供される	
2010 年	本人か否かを照会できる Aadhaar 認証（Aadhaar Authentication）機能が提供される。
2011 年	行政 機関が社会保障給付金・補助金をその口座宛てに送金することを可能にする APB（Aadhaar Payment Bridge）機能が提供される。
2011 年	Aadhaar 番号と生体認証だけで基本的な銀行取引を可能にする AEPS （Aadhaar Enabled Payment Systems）機能が提供される。
2012 年	個人情報照会機能である Aadhaar eKYC 機能が提供される。
モディ政権の「デジタルインド計画」「国民皆銀行口座プロジェクト」によりデジタル決済化が加速され、基盤である Aadhaar への登録や利用が加速される。	
2014 年	モディ政権がデジタルインド計画を発表する。電子決済の推進によるキャッシュレス化が重要な柱となる。
2014 年	モディ政権が国民皆銀行口座プロジェクトの導入を発表する。2015 年 3 月末までに 7500 口座を目標とする。

143 FinTech 時代の決済改革－英国とインドの取組み（2017 年 5 月）,野村資本市場研究所
http://www.nicmr.com/nicmr/report/repo/2017/2017spr05.pdf

144 環太平洋ビジネス情報 RIM（2019 年）,日本総合研究所
https://www.jri.co.jp/MediaLibrary/file/report/rim/pdf/11416.pdf

145 インドの銀行、国民 ID と口座のひも付けに苦戦,日本経済新聞
https://www.nikkei.com/article/DGXMZO21929200V01C17A0FFE000/

2016 年	Aadhaar 法が成立し、銀行口座は Aadhaar との紐づけを義務化される（紐づいていない口座は凍結される）
2016 年	UPI（Unified Payment Interface）と BBPS（Bharat Bill Payments System）がサービス開始される。
2017 年	Aadhaar Pay がサービス開始される。

India Stack とは

India Stack はインドにおけるデジタル ID 基盤の総称である。これは 3 つのレイヤーに分かれており、①個人をデジタル上で特定する ID レイヤー、②電子的な決済手段を提供するペイメントレイヤー、③自己のデータ管理を可能にするデータレイヤーの 3 つに分けられる。

①はデジタル ID、e-KYC、電子署名を、②は共通決済インターフェース、決済データ交換基盤、ID をベースとした決済サービスを、③は自己データへのアクセス管理機能、データ保存、銀行口座データの統合管理機能などを司る。

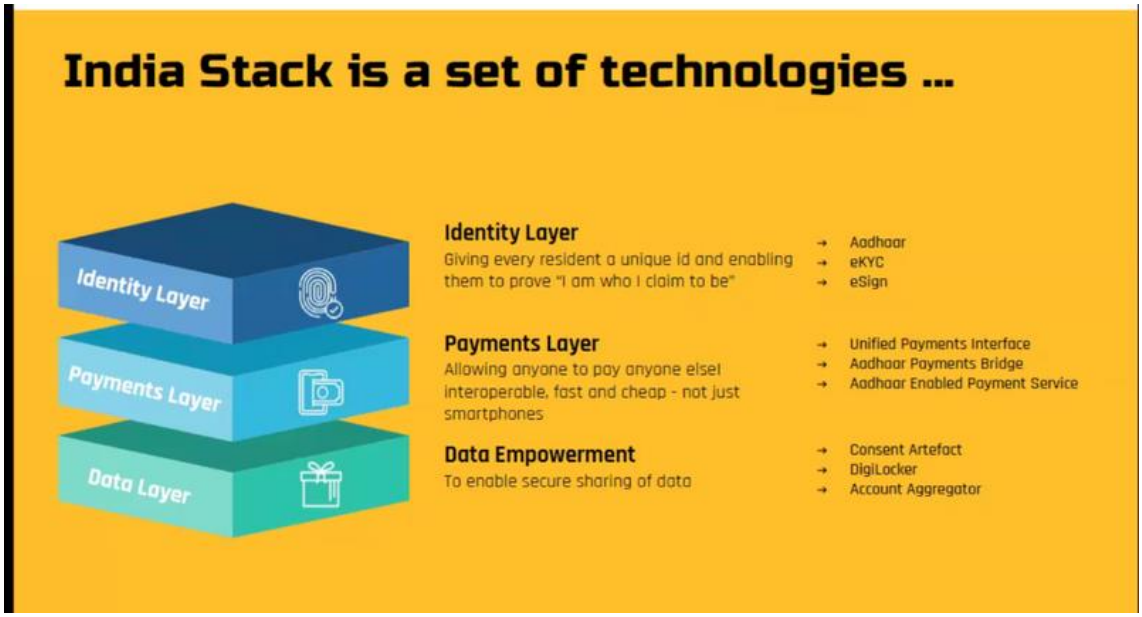


図 2- 36　India Stack の構成概要[146]

金融包摂措置

A）公的身元証明書を持たない層に対する措置

[146] オープンソースとしての行政デジタル ID フレームワーク（India Stack と MOSIP）
https://note.com/hiroki_yoshida/n/n1fcfb36d229f

UIDAI Aadhaar 登録プロセスは、公的身元証明書を持たない層に対し、柔軟な身分証明要件を備えており、生体認証に頼って一意性を確立している。

具体的には、全国各地にある認可された登録機関（主に州政府、中央省庁、銀行、公共部門組織）で、ソフトウェアと生体認証キャプチャおよびその他の機器を使用して、対面で登録を実施している。

登録時には中核となる属性を確認するために公的身元証明書を確認するが、不保持者には以下の対応も実施している。

- 家族の長が、必要な身元確認書類を使用して Aadhaar に登録し、登録中に家族を紹介すれば、家族は Aadhaar に登録することが可能
- 必要書類がない場合は、登録機関または地域の UIDAI オフィスの仲介で、登録センターで利用可能な紹介者または証明者を利用して登録行うことも可能

B）デジタルインフラ未整備の農村部における金融取引事例[147]

インドの国民の大多数は農村部で暮らしており、周囲に金融機関の支店/ATM がなく顧客もモバイル端末を持っていない。そこで、金融機関が派遣したエージェントが顧客の生体認証操作と顧客との現金の受け渡しを行うことで、金融機関の支店/ATM 網を整備することなく、農村部の国民へ金融サービスを提供している。

＜例：出金の場合＞

生体認証で本人確認して顧客へエージェントから現金を渡した後、顧客口座からエージェント口座へ振込処理を行う。

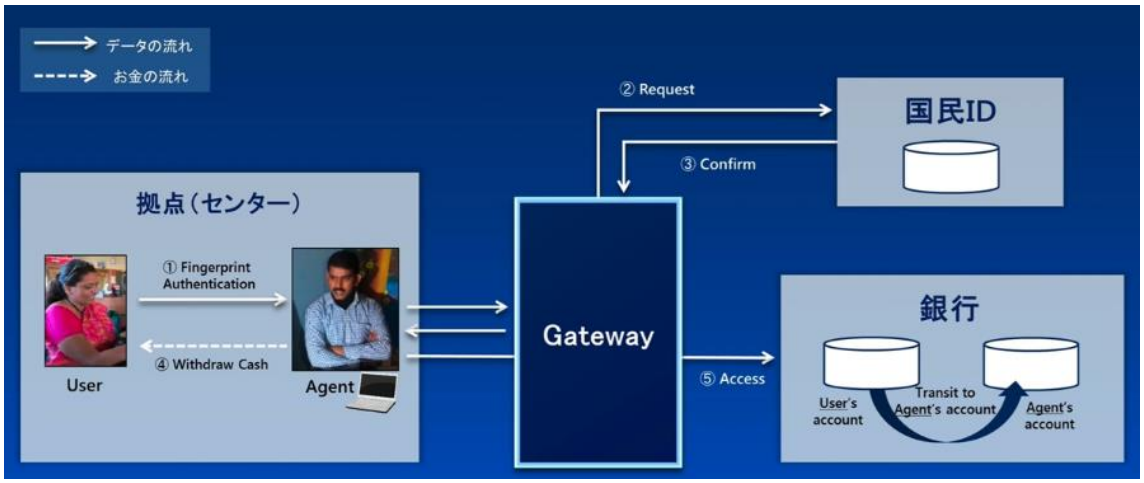


図 2- 37 デジタルインフラ未整備の農村部における金融取引事例

[147] 政府インターネットテレビ　スーパーシティ／スマートシティフォーラム 2019「インドにおけるアドハー成功の秘訣と金融サービス」https://nettv.gov-online.go.jp/prg/prg19513.html

（4）英国における国民 ID の代替策としての GOV.UK Verify 導入

英国においては国民 ID の導入を過去に複数回図るものの、いずれも失敗に終わっている。例えば 2006 年 3 月に成立した Identity Card Act 2006 は、政府による国民の管理、監視に対する懸念が根強く、2010 年の政権交代を機に 2011 年 1 月に廃止されている。代替策として 2011 年に Identity Assurance Service プロジェクトが発表され、公共サービスを利用する際の本人確認手段として民間が発行する ID 活用するための基盤 GOV.UK Verify が導入された。

しかし GOV.UK Verify においても IdP の撤退が相次ぎ、成功しているとは言い難い状況である。これは本人確認成功率が低くサービス数も増加しないことから利用者数が当初想定ほど伸びず、また高コストでもあったためである。政府から IdP として参加する民間企業へ資金支援も行われているが、撤退に歯止めは掛かっていない。

表 2- 19 事例④英国における国民 ID の代替策としての GOV.UK Verify 導入

対象課題	1） IAL
課題対応の方向性 ＜対応前＞	・ID カード法を制定し英国に 3 か月以上滞在する 16 歳以上の個人に ID 登録番号および ID カードを発行。 ・EU 域内パスポートとしての利用に加え、民間サービス利用時の本人証明として利用可能。 ・政府による管理や監視社会に対する強い危機感等のため ID カード法を廃止。
＜対応後＞	・民間企業が発行する ID を公共サービスへアクセスする際の本人認証手段として活用。 ・各個人が選択した IdP から GOV.UK Verify を通じて公共サービスを利用可能。 ・政府による国民 ID の集中管理に代わり、個人へ IdP の選択、利用、中止の権利を付与。
背景・成功要因	・政府横断的にデジタルサービスを担う GDS （Government Digital Service）が主導。 ・IdP として参加する民間企業に対して政府から一人当たり 20 ポンド[148]の資金を支援。（2021 年 10 月まで）

[148] Gobernmentcomputing “Commercial concerns push two IDPs away from Verify as it heads towards private sector delivery” （11 OCTOBER 2018）
https://www.governmentcomputing.com/identity/news/commercial-concerns-push-two-idps-away-verify-heads-towards-private-sector-delivery

成果	・GOV.UK Verify を利用して 22 種類の公共サービスを利用可能（2020 年 1 月現在）。 ・7 社の認定事業者（2014 年 10 月現在）と 600 万人が利用中（2020 年 1 月現在）。
今後の課題	・当初想定に利用者数やサービス数が未達かつコスト増のため、IdP が相次いで撤退し 2020 年 3 月現在 2 社へ減少。 ・主要銀行がデジタルアイデンティティを独自発行もしくは TISA 等の業界団体による規定等、代替策の検討が進展。

GOV.UK Verify の概要

GOV.UK Verify は eIDAS フレームワークの Level2 に相当する認証基盤である。公共サービスへアクセスする際に、GOV.UK Verify を経由して各個人が選択した認定 IdP に対して本人確認を実施する仕組みである。

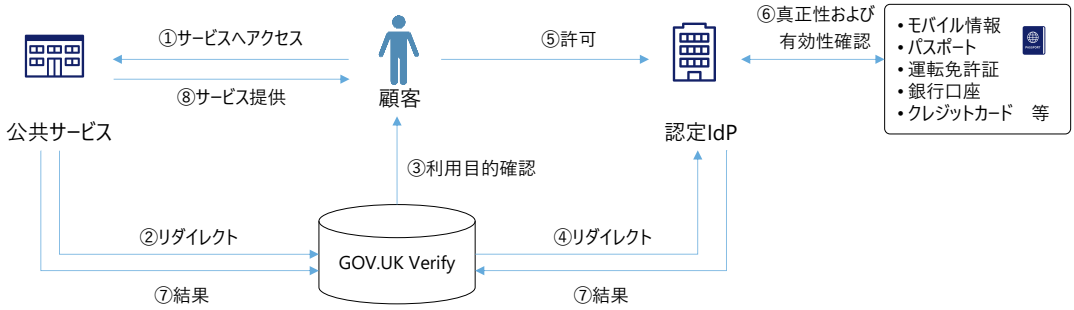


図 2- 38 GOV.UK Verify における本人確認フロー[149]

2019 年 3 月に発行された National Audit Office によるレポート“Investigation into Verify”によると利用者数、サービス数、本人確認成功率、利益のいずれの指標においても 2016 年に設定した目標値に遠く及ばないことが分かる。政府による資金支援は 2021 年 10 月まで延期されたが IdP の撤退は止まらず、2020 年 3 月現在残り 2 社まで減少している。

表 2- 20 National Audit Office による GOV.UK Verify の調査[150]

指標	2020 年目標	実績（2019 年 2 月）
利用者数	2,500 万人	360 万人
サービス数	46	19

[149] GOV.UK ウェブサイトを基に NRI 作成

[150] National Audit Office report （March 5, 2019）
https://www.nao.org.uk/report/investigation-into-verify/

本人確認成功率	90%	48%
利益	£873M	£217M

（5）ID 連携サービスにおける責任分界

責任分界における先進的 3 事例を表 2- 21 に整理する。いずれの ID 連携サービスにおいてもプラットフォームを介して ID が連携される点は共通である。

しかし連携される ID に対する責任分界は、ID 連携サービス 1 および ID 連携サービス 2 が認証レベルに応じて IdP の責任を規定しているのに対し、ID 連携サービス 3 は RP が全責任を負う点において異なる。

また料金体系は ID 連携サービス 1 が責任分界に紐づけて価格設定を行っているのに対し、ID 連携サービス 2 および ID 連携サービス 3 は全データが有料である。

表 2- 21 事例⑤ID 連携サービスにおける責任分界

サービス	ID 連携サービス 1	ID 連携サービス 2	ID 連携サービス 3
提供地域	欧州	北欧	日本
内容	eIDAS の適格トラストサービスプロバイダ(QTSP）として本人確認済情報（クレーム）を連携	官民双方のサービスに利用出来る統一 ID を全市民へ提供	事業者が eKYC を実現するために金融機関が保有する本人確認済情報を連携
連携可能な属性項目	OpenID Connect®の規定もしくは OpenID Connect for Identity Assurance®規定の仕様に準拠	口座開設に必要な属性に加えて AML/CFT 要件を満たす属性項目	非公開
主な参加者	IdP：法域内の金融機関 RP ：非公開	IdP：法域内の金融機関 RP ：小売、法域内の金融機関、政府サービス	IdP：法域内の金融機関 RP ：非公開
料金体系	本人確認済み情報：有料 本人確認未済情報：無料	認証レベル高情報：有料 認証レベル低情報：有料	本人確認済み情報：有料 本人確認未済情報：－
責任分界	本人確認済情報：IdP 責任 本人未確認情報：RP 責任	認証レベル高：IdP 責任 認証レベル低：RP 責任	RP が全責任 ※参考情報の位置付けのため

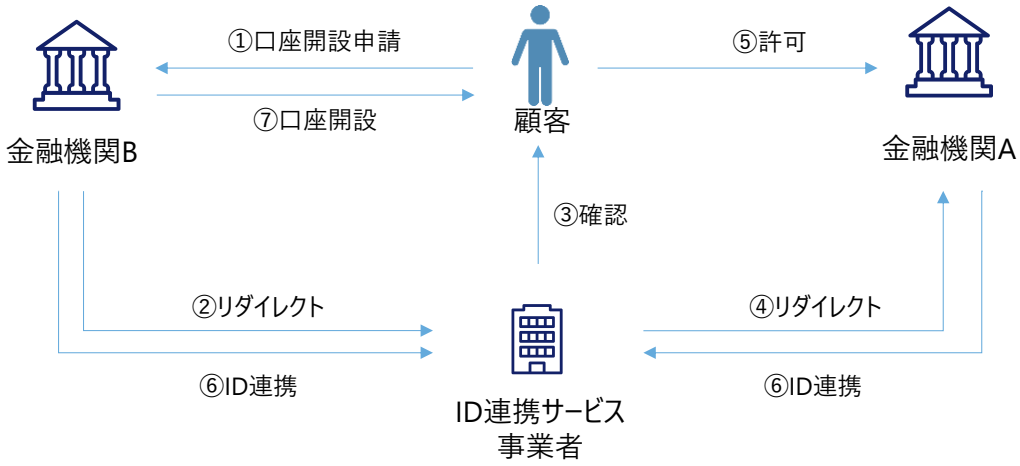


図 2- 39 他社で作成したデジタルアイデンティティを用いた口座開設フロー[151]

[151] 各社インタビューを基に NRI 作成

（6）標準化団体の取り組み

（6）-1　金融当局として特に注視すべき標準化動向

金融機関のアイデンティティ管理業務に影響が大きいと思われる標準化活動を、各々の標準化活動が解決に資する課題とあわせて下表に示す。

表 2- 22　金融当局として特に注視すべき標準化活動

団体名	検討グループ	活動概要	ステータス	注視すべき観点	対象課題
ISO	ISO TC 68 Financial services SC8 Reference data for financial services WG4	ISO 17442-2：Legal entity identifier（LEI）（取引主体識別子）の規格策定	活動終了	LEI は金融取引における法人を特定する識別子であり、活用等も議論されている	2-3-5 金融機関からのデータ参照先に関する課題
	ISO TC 68 Financial services SC8 Reference data for financial services WG7	ISO/DIS 24366：Natural Person Identifier（NPI）（自然人 ID）の規格策定。	第一版の作成に向けて議論中	NPI は個人の識別子であり現在第一版検討中であるが、LEI と同様に活用の動きが議論されている	2-3-5 金融機関からのデータ参照先に関する課題
OIDF	eKYC& Identity Assurance WG	ID 連携プロトコル“ OpenID Connect”を拡張し、属性情報に加え、確認方法等を表すメタデータを連携する規格の仕様検討を実施	Implementation Draft2 公開済	個人の検証済属性のメタデータ連携、法人関係者の情報連携等、AML 規制対応強化につながるユースケースが検討されている	2）ID 連携

	FAPI WG	FAPI（Financial-grade API）1.0 の策定	FAPI 1.0 最終版発行済（2021） FAPI2.0 Implementation Draft1 発行済	英国 Open Banking における PSD2 対応等、幅広く活用されている	5） 相互運用性
OIX	・Digital ID for AML ・Banks in the Identity Market	金融機関の AML 業務の活用等、金融特有の課題を議論	検討中	AML 等、金融特有の取組を実施中	5） 相互運用性

（6）-2　OpenID Foundation eKYC & Identity Assurance WG

活動概要

事業者間で行われる ID 連携における連携技術仕様について、属性情報に加えて、ID の信頼性の根拠となるメタデータ（検証の根拠とした法令・検証方法等）の連携や、法人関連の詳細情報の連携を実現する連携技術仕様を開発し、AML 規制対応や不正防止等の対策強化に寄与している。

表 2- 23 事例⑥OpenID Foundation eKYC & Identity Assurance WG の取り組み

対象課題	2） ID 連携（責任分界を中心に）
課題対応の方向性 ＜対応前＞	・本 WG において事業者間の連携技術仕様を整備するも、連携される ID に対する信頼の前提となる、法令や契約に基づく属性検証ルール、検証状態、検証方法等を連携できず。 ・法人についても、法人詳細情報や法人の代理として活動する自然人（代表者等）の情報を連携できず。
＜対応後＞	・本 WG において、ID 連携プロトコル“OpenID Connect”を拡張し、属性情報に加え、それがどのように確認されたかを表すメタデータを連携することが可能となるよう ID 連携仕様を策定。 ・法人については、法人の代理として活動する自然人の情報の連携から、仕様検討を実施中。

背景・成功要因	・デジタル化の進展による、デジタル空間における規制強化要請。
成果	・ID に関するメタデータの付与、法人詳細情報の連携により、AML 規制対応や不正防止等の対策強化を実現。
今後の課題	・他国の法令に基づく ID を信頼できるものとして金融機関業務に利用できるよう法令・ガイドラインに定める等、技術仕様に対応した法制度の整備。

活動内容[152]

eKYC & Identity Assurance WG において、ID 連携プロトコル OpenID Connect を拡張し、属性情報に加えてそれがどのように確認されたか（法令や契約に基づく属性検証ルール、検証方法等）を表すメタデータを連携するためのデータフォーマット規格 OIDC4IDA の仕様検討を実施している。

また法人については、法人の代理として活動する自然人の情報の取得を実現する Authority Claims の連携技術仕様を検討している。

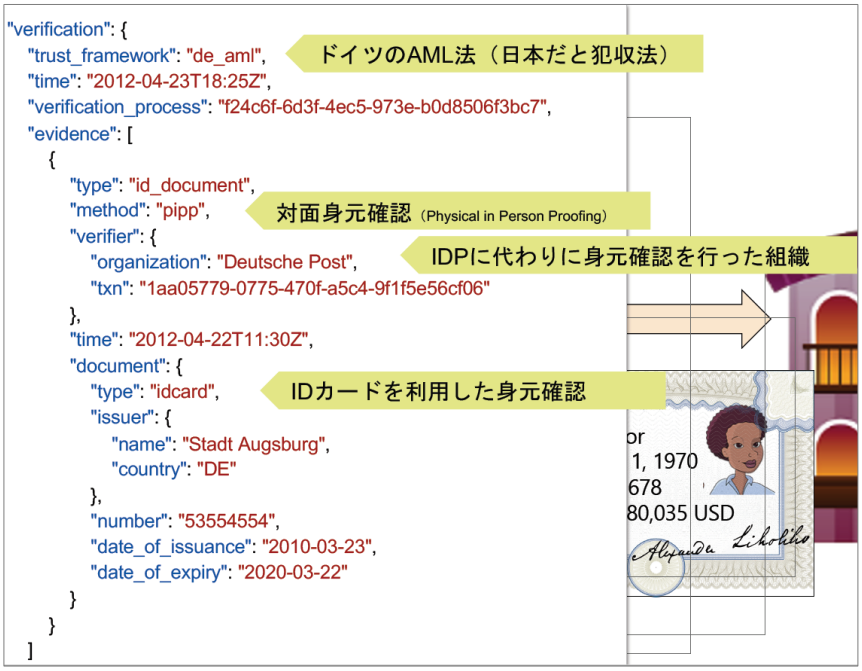


図 2- 40 自然人における ID 連携仕様イメージ

[152] Open ID Foundation Japan における KYC に関する取組概要（2021）
https://www.slideshare.net/oidfj/openid-foundationjapankyc-openid-bizday-14

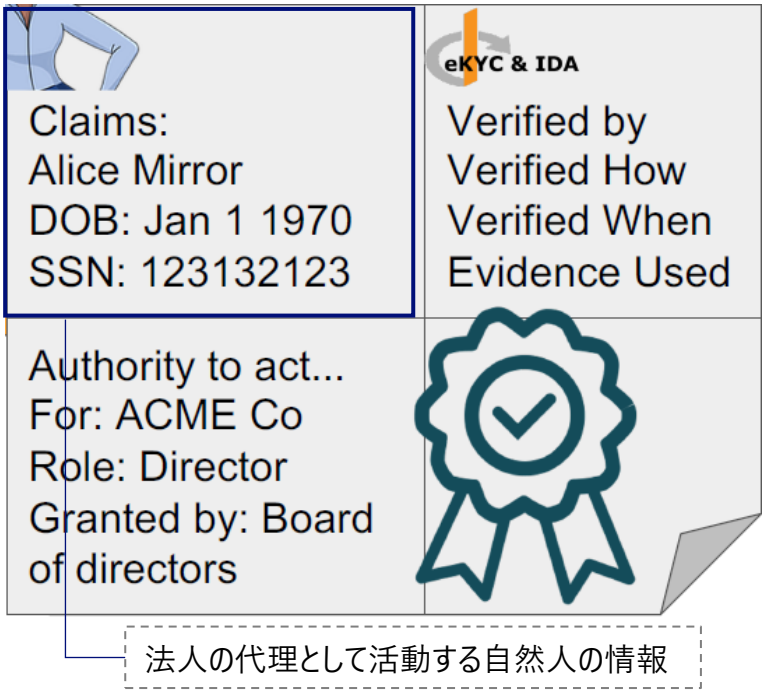


図 2- 41 法人における ID 連携項目イメージ（赤枠部分が現在検討中の情報）

（6）-3　OpenID Foundation FAPI WG

活動概要

OpenID Foundation の FAPI WG は、より安全性の高い Financial Grade の API 仕様である「Financial-grade API」の検討を行う WG である。OAuth で保護された REST/JSON モデルの API を開発し、英国 Open Banking における PSD2 対応等で利用されている。

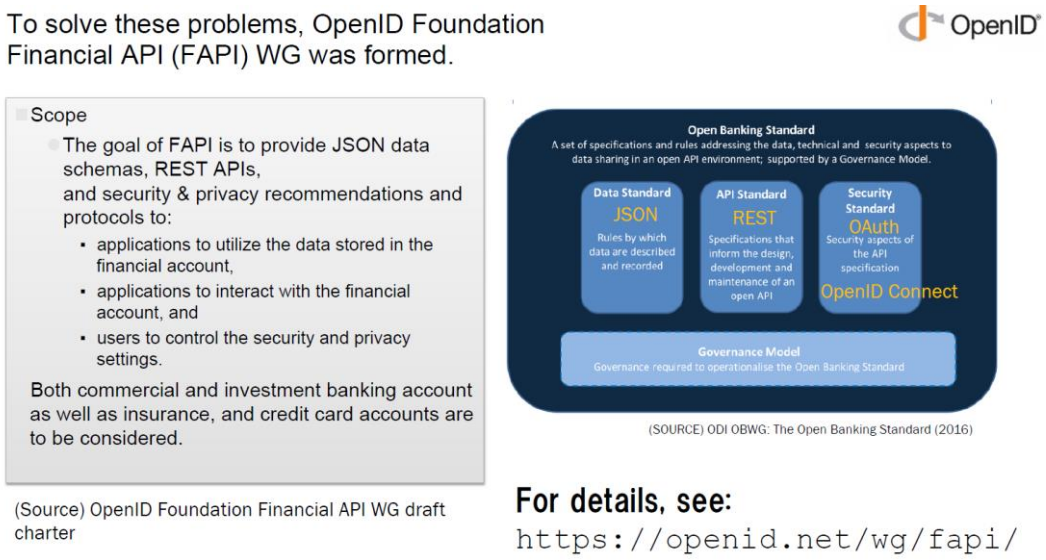


図 2- 42 OpenID Foundation　FAPI WG の活動スコープ[153]

[153] Open ID Foundation Financial API WG（2017 Jun）
https://www.slideshare.net/nat_sakimura/openid-foundation-fapi-wg-june-2017-update

図 2- 43 英国における FAPI 採用についての OIDF ニュースリリース[154]

活動マイルストーン

FAPI1.0 は 2021 年 3 月に最終仕様が確定されている。[155]

FAPI2.0 は 2020 年 12 月に ID1（Implementer's draft1）を発行し、現在も継続開発中。ID2 や Final の発行時期は未定である。

参加機関

IT ベンダー、Finteck 企業が参加し、ISO・IEC のリエゾン組織ともなっている。

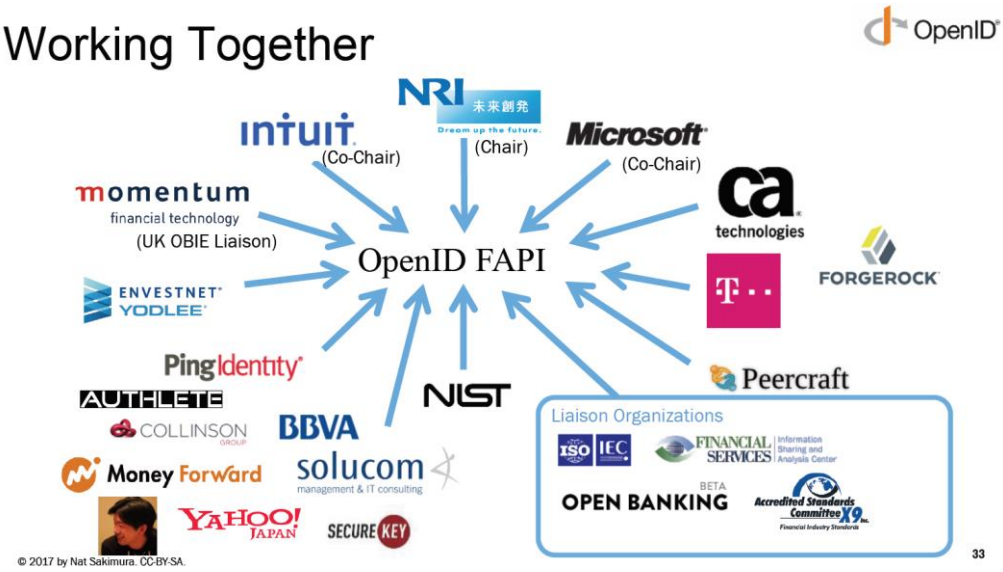


図 2- 44　FAPI プロジェクト参加機関[156]

採用事例

- 英国　　：CMA9+で採用済
- オーストラリア　　：ソフトローンチ済

[154] 英国における FAPI 採用についての OIDF ニュースリリース
https://openid.net/2018/07/12/the-uk-open-banking-implementation-entity-adopts-the-openid-foundation-financial-grade-api-fapi-specification-certification-program/

[155] OpenID, FAPI 1.0 Part 1 and Part 2 are now Final Specifications
https://openid.net/2021/03/12/fapi-1-0-part-1-and-part-2-are-now-final-specifications/

[156] Open ID Foundation Financial API WG（2017 Jun）
https://www.slideshare.net/nat_sakimura/openid-foundation-fapi-wg-june-2017-update

- 日本：全銀協の報告書に、詳細仕様が発行された際は各銀行において同仕様への準拠や準拠に向けた方針等が示されることが望ましい旨記載されている

- ロシア　　：採用に向けて取組中（暗号アルゴリズム変更が必要な可能性）
- ブラジル　　：採用に向けて取組中

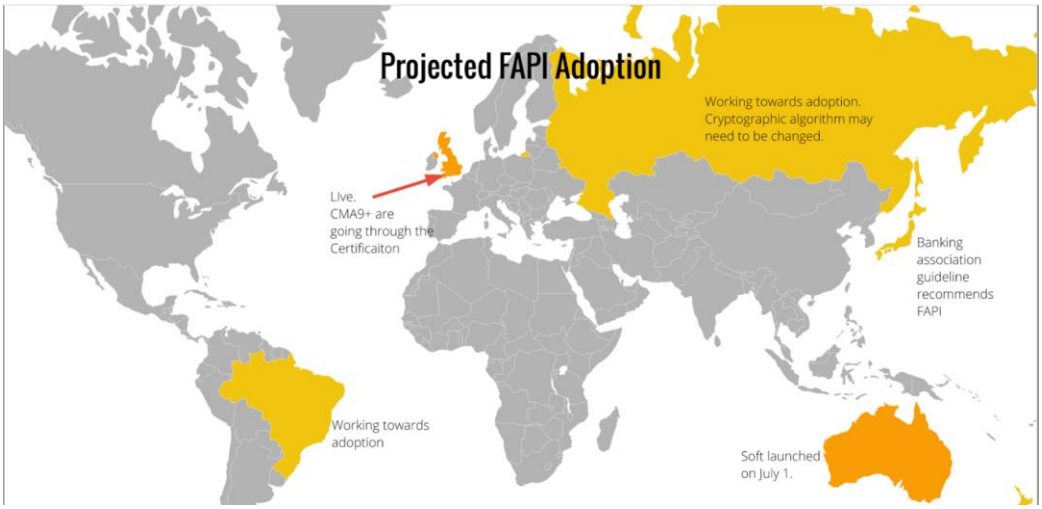


図 2- 45　FAPI 採用事例[157]

（6）-4　Open Identity Exchange （OIX）

1 章で紹介した OIX（2010 年に、米国政府の要望により、OpenID Foundation と Information Card Foundation の資金等をもとに設立された非営利団体）は、2020 年 6 月に「Digital Identity for AML KYC in the UK」と題したレポートを発行した。同レポートは、JMLSG（Joint Money Laundering Steering Group、英国の共同マネー・ローンダリング運営グループ）がガイダンス（Prevention of money laundering/combating terrorist financing, Guidance for the UK Financial Sector）を更新し、本人確認のために eIDAS 準拠のデジタルアイデンティティを利用することを容認したことを受け、発行されたものである。

同レポートの中、本人確認に eIDAS 準拠のデジタルアイデンティティを利用するためには、デジタルアイデンティティが業界として認定され、かつ、金融機関が ID プロバイダ・ブローカーの信頼性を簡単に判別できる必要があるとしており、そのためにはトラストスキームの確立が最善の方法であるとしている。トラストスキームの責務・型・運営形態について、以下のように提言している。

---

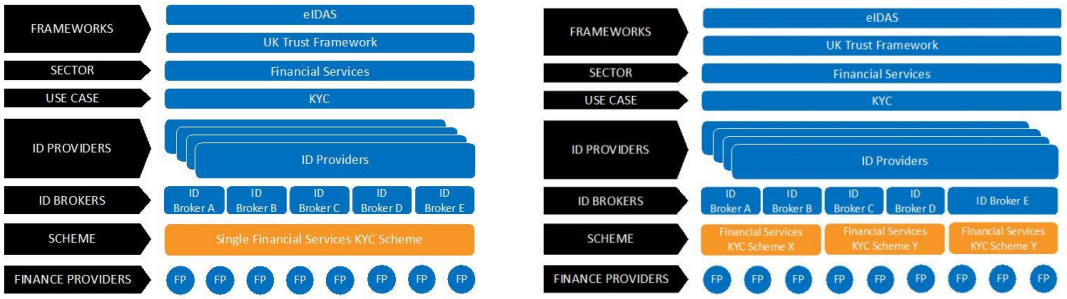
[157] Global Adoption of FAPI Among Open Banking Standards... And Beyond （2020 年 9 月 22 日）https://fapi.openid.net/wp-content/uploads/2020/09/20200922-Global-Adoption-of-FAPI-EN_Nats-FDX-Keynote.pdf

トラストスキームの責務

- デジタルアイデンティティとブローカーの両方について、
  評価基準のミニマムスタンダードの定義
- 非 eIDAS デジタルアイデンティティの準拠性評価方法の定義
- ブローカーがどのようにコンプライアンスを評価されるかの定義
- 上記基準への適合性の評価
- 上記基準に準拠していることの公表
- コンプライアンスプロセスに関する市場教育
- あらゆる問い合わせや苦情への対応

トラストスキームの型

単一型と複数型が考えられるが、複数型は市場を複雑に企業や消費者を混乱させる可能性があるため、単一型が望ましい



Single Trust Scheme	Multiple Trust Schemes
• Single, clear authority for Digital ID accreditation for financial services firms to trust	• Each different scheme may have different rules and standards that, whilst meeting guidelines, mean firms need to make assessments of different competing schemes.
• Consistent consumer experience across all ID providers	• Different experiences depending on the Scheme UX rules.
• Central consumer messaging of how the ID process works, supported by a TrustMark	• Varying consumer messaging and different TrustMarks (competing brands) result in consumer confusion.
• Single accreditation process for ID Providers and ID Brokers simplifies the process and compliance, lowering costs and encouraging new market entrants.	• Multiple accreditation processes for ID Providers and ID Brokers complicates the process and compliance, increasing costs and creating a barrier to entry for new market entrants.
• Central place to go to handle disputes	• No central place for disputes or arbitration.
• No-commercial agenda	• Possible commercial agendas of competing Schemes.

図 2- 46　トラストスキームの単一型と複数型の比較[158]

[158] Global Adoption of FAPI Among Open Banking Standards... And Beyond （2020 年 9 月 22 日）
https://fapi.openid.net/wp-content/uploads/2020/09/20200922-Global-Adoption-of-FAPI-EN_Nats-FDX-Keynote.pdf

トラストスキームの運営形態

トラストスキームの運営方法としては、非営利組織とし金融業界の承認と支援を受ける形が適当。また、トラストスキームの組織形態としては、新たな別組織としてもよいし、金融サービスまたは ID サービスの既存の非営利組織に付属させるのもよい。

（6）-5　LEI の活用検討状況

FSB が 2019 年に公表した Peer Review レポート[159]によると、LEI は規制目的などの当局活動、貿易などの民間活動、様々な分野で活用されている。多くの FSB 参加国・法域で、LEI の取得や促進に関するルールが導入済みである。

LEI のユースケース

リーマンショックへの対応として、多くの国でデリバティブ取引報告、市場監督、与信先管理、リスク管理などの分野で LEI を活用する制度の導入が既に進められている。また、国際送金時に LEI をより活用するための検討の動き等もある。（図 2- 47 LEI の活用参照）

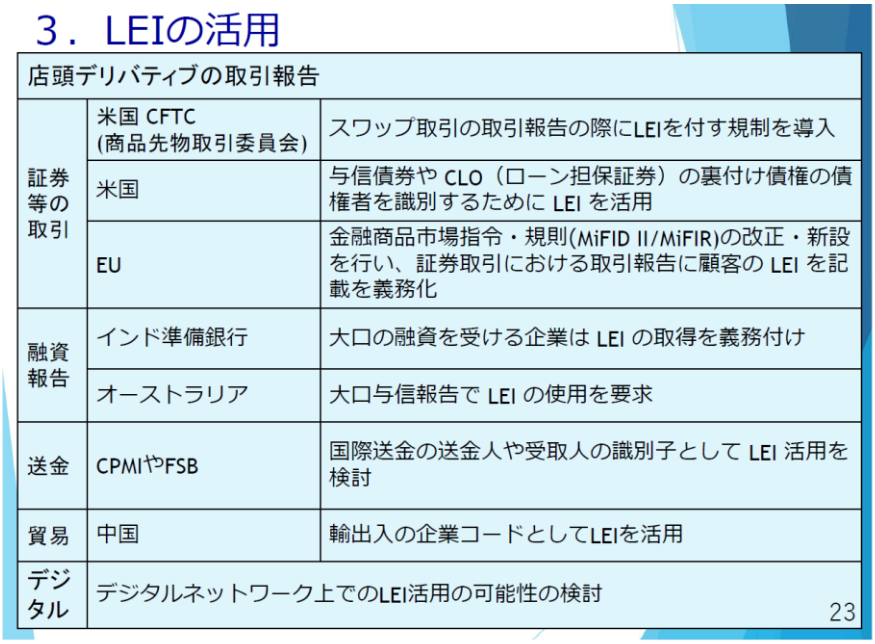


図 2- 47 LEI の活用[160]

[159] FSB：Thematic Review on Implementation of the Legal Entity Identifier - Peer Review Report （May 2019）
https://www.fsb.org/wp-content/uploads/P280519-2.pdf

[160] 2020 年 11 月 24 日日本銀行決済機構局 ISO パネル第一回資料
https://www.boj.or.jp/paym/iso/iso_panel/data/isop201127.pdf

これらの動きを受け、法人識別子として徐々に広まりを見せ始めている状況である。現状事例はないが、LEI に対して法人実質的支配者情報を付与し共有・管理を行うことがなされれば、AML における法人実質的支配者情報の収集効率化につながると期待される。

また関連する動きとして、本邦では、公証人法改正により法人登記時の実質的支配者届出を義務付け、その共有を検討している[161]。

[161] 法務省民事局：商業登記所における法人の実質的支配者情報の把握促進に関する研究会取りまとめ概要（Jul 2020） http://www.moj.go.jp/content/001324012.pdf

（7）民間発行 ID によるクロスボーダー取引

北欧では全国民を対象とした国内外の官民サービスへ利用可能な民間発行 ID サービスがある。eID および eSignature[162]に準拠しており、EU トラステッドリスト[163]にも掲載されている。なお、他国の同様のサービスとの相互運用性を有するが、現在は法域内における ID の浸透を最優先する方策を取っているため、当該 ID を利用した本格的なクロスボーダー取引には未進出であり、新 eIDAS 制定により EU 全域において当該 ID が利用可能となった後にクロスボーダーサービスへの本格進出予定である。

表 2- 24 事例⑦民間発行 ID によるクロスボーダー取引

対象課題	7） クロスボーダー取引の諸課題
課題対応の方向性 ＜対応前＞	・当該 ID 発行時は金融機関の店頭に赴く必要がある。 ・当該 ID は eID および eSignature の双方に準拠しており、隣接法域の民間発行 ID との相互運用性を有するが、クロスボーダーには実質的に未進出である。 ・政府 ID もかつて存在したが、現在は当該 ID が官民双方のサービスに利用可能である。
＜対応後＞	・現 eIDAS 規則第 24 条が改訂され、店頭に赴かずに当該 ID の発行が可能となる見込みである。 ・EU トラステッドリスト認定に伴い、EU 全域における利用が可能になる予定である。 ・当該法域政府が独自 eID（政府 ID）を発行予定だが、民間発行 ID の補足的な位置付けで当該 ID の優位性が継続する見込みである。
背景・成功要因	・提供サービスのリスクに応じた認証レベルの選択が可能である。 ・当初から隣接法域の ID との相互運用性を担保した設計を実施した。
成果	・当該法域の大半の成人市民に普及している。（本格的なクロスボーダーは未導入） ・民間企業が発行した ID を用いて法域内外の官民サービスを利用可能である。

[162] 電子署名に関する指令（2016 年 7 月に eIDAS へ置換） https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0093

[163] EU 加盟国が適格と認めたサービスプロバイダーの一覧 https://webgate.ec.europa.eu/tl-browser/#/

	・
今後の課題	・欧州委員会による当該 ID への権限が強まる一方、法域規制当局の権限が弱体化している。

当該 ID は法域内の金融機関において口座開設を行うことにより発行される。一旦 ID が発行されると、法域内の共通 ID としてオンライン公共サービスや非金融を含む民間サービスへのアクセスに利用可能となる。

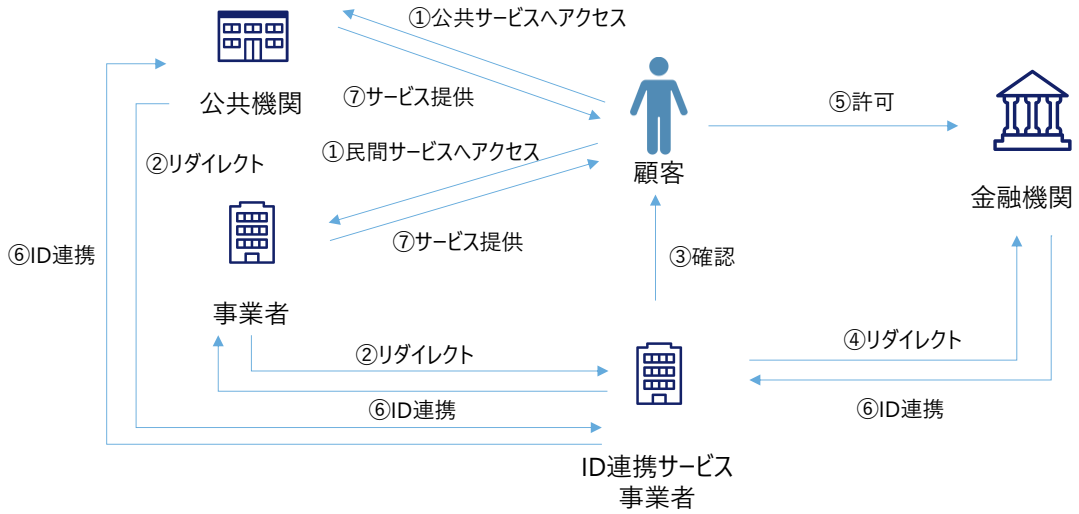


図 2- 48 金融機関が作成したデジタルアイデンティティを用いた ID 連携フロー

（8）欧州大手金融機関によるクロスボーダー口座開設

欧州大手金融機関においては、ファイヤーウォール規制および個人情報保護規定等の制約がない法域間に限定し、他法域から非対面による口座開設を可能としている。

元々上位ステータス口座の情報が法域間で共有されていたこと、また既存の上位ステータス口座を利用した他法域における上位ステータス口座開設の仕組みがあったことを背景に、デジタルアイデンティティを活用してリモート onboarding を実現したサービスである。

表 2- 25 事例⑧欧州大手金融機関によるクロスボーダー口座開設

対象課題	7） クロスボーダー取引（越境金融）
課題対応の方向性 ＜対応前＞	・既存顧客が他法域において口座開設を行う場合は一から口座開設申請する必要があった。 ・居住する法域の欧州大手金融機関支店に赴き、申請書やアイデンティティエビデンスを支店経由で他法域の支店へ申送・郵送する必要があり、口座開設まで 2 週間から数週間を要した。
＜対応後＞	・口座情報を他法域の支店へ連携することにより、簡易なリモート手続きが可能となった。 ・自宅からオンラインで申し込むことが可能となり、かつリモート面談を併用することにより、数日での口座開設が可能となった。
背景・成功要因	・ファイヤーウォール規制および個人情報保護規定等の制約がない法域間では、上位ステータス口座を保有する顧客の情報がグローバルで共有されていた。 ・当該顧客情報を活用した他国での口座開設の仕組みが存在した。
成果	・上位ステータス口座を保有する米国外在住顧客が簡易なリモート手続きにより短期で口座開設が可能になった。 ・米国における上位ステータス口座数が増加している。
今後の課題	・他法域でのサービス実現ニーズがあるものの、ファイヤーウォール規制および個人情報保護規定等の制約がある法域間、デジタルアイデンティティを活用できていない法域での実現は困難である。

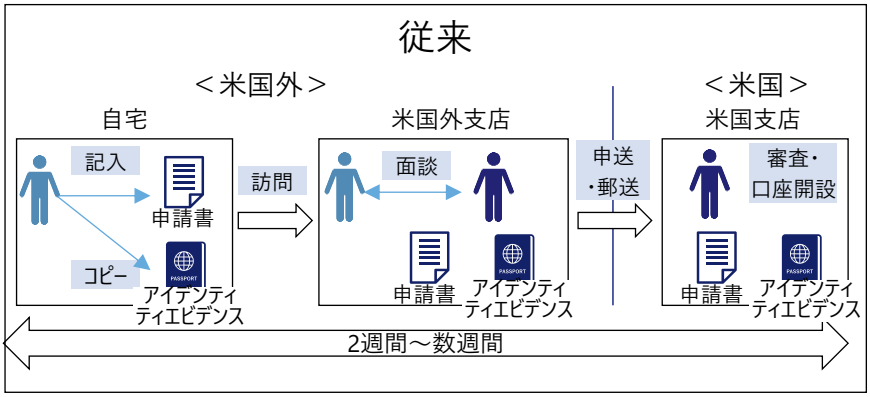


図 2- 49 欧州大手金融機関米国における従来の口座開設フロー[164]

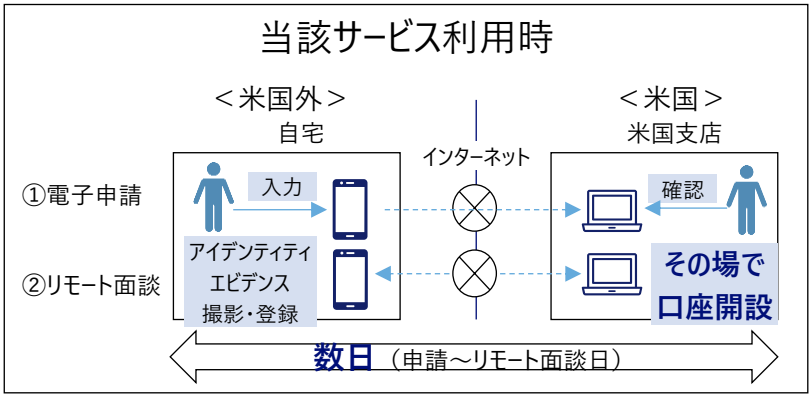


図 2- 50 欧州大手金融機関米国における当該サービスを利用した口座開設フロー[165]

[164] 欧州大手金融機関ウェブサイトを基に NRI 作成

[165] 欧州大手金融機関ウェブサイトを基に NRI 作成

(9) オーストラリアにおける官民サービスの相互運用

オーストラリア政府は金融業界で myGovID 等の政府 ID の利用が拡大しないと見込み、TrustID framework を作成した。TrustID framework にはオーストラリア中央銀行、金融業界に加えて DTA（デジタルトランスフォーメーション庁）が参加し、金融系 IdP による ID 連携や統一を目的としている。

表 2- 26 事例⑨オーストラリアにおける官民サービスの相互運用

対象課題	5） 相互運用性
課題対応の方向性 ＜対応前＞	・DTA(デジタルトランスフォーメーション庁)を主体に TDIF の策定や、TDIF 上の IdP として myGovID(DTA)や DigitaliD（郵便公社）を認証していた。 ・しかし TDIF は処理に時間を要することや、様々な制約が設けられていることから金融サービスへの適用が進まなかった。
＜対応後＞	・APC（Australia Payment Council）が設計する TrustID framework に TDIF との相互運用性を持たせることで相互にサービスアクセス可能になる見込みである。 ・民間企業が発行する ID を TDIF および TrustID framework 双方で稼働させることで IdP と民間や政府機関 RP 間の本人確認ハブとして機能させている。
背景・成功要因	・TrustID framework の策定に DTA および豪中銀が参画し TDIF との相互運用性を担保した。 ・郵政公社を巻き込むことにより民間企業が発行する ID による行政 ID 管理を可能とした。
成果	・民間企業における顧客 ID 管理や認証と、政府からの給付金受領などの国民 ID 管理との双方に利用が可能となった。 ・住宅ローン申請時の属性データの証明など、高付加価値のユースケースにおけるコスト節約を図ることが可能となった。
今後の課題	・TrustID Framework は TDIF から、民間企業が発行する ID は TDIF および TrustID Framework の双方から認証を受けていない。 ・民間企業が発行する ID 以外に商用フレームワークの提供がなく、また本格的な商業運用はこれからである。

APC は様々なサービスのデジタル ID がそれぞれに生成・管理されていることを問題視しており、経済の非効率化・顧客管理の高リスク化を TrustID framework により解消しようとしている。APC は TrustID framework 上で運用される民間セクターのプロバイダによるデジタル ID が、最終的には政府サービスへのアクセスに使用できる、またその逆も同様に可能であるように設計している。

表 2- 27 TDIF と TrustID framework の比較

	TDIF	TrustID framework
策定主体	DTA （内閣府内に設置）	APC
設置	内閣府内	AusPayNet（金融業界団体）と RBA（豪準備銀行）の合弁
対象	政府・地方自治体が中心 民間にも拡大	金融機関を中心とした民間部門
目的	デジタル経済全体のコスト削減 人々と政府の関係を合理化 イノベーション・効率・柔軟性の向上	様々なデジタル ID が生成・管理されていることによる経済的な非効率の解消、民間企業の顧客管理リスク等の解消
認証対象	IdP 等に対して条件を規定 myGovID および DigitaliD 認証済み	不明

TrustID framework にはオーストラリアの金融機関を中心に Visa や Mastercard などのグローバルな決済事業者、郵便公社や小売・通信などのサービス業、DTA や RBA などの行政機関等が参加している。

表 2- 28 TrustID framework 参加組織（2019 年時点）

銀行	Australia and New Zealand Banking Group Ltd Bendigo & Adelaide Bank Ltd Commonwealth Bank of Australia National Australia Bank Ltd Suncorp-Metway Ltd Westpac Banking Corporation
決済	eftpos Payments Australia Ltd MasterCard Asia/Pacific （Australia） Pty Ltd Visa AP （Australia） Pty Ltd PayPal Pty Ltd

	Cuscal Ltd
その他	Coles Group Ltd（小売） Woolworths Ltd Optus Australian Postal Corporation
行政機関	Digital Transformation Agency Reserve Bank of Australia

TrustID Framework をベースとした主要ユースケースとしては eftpos の ConnectID が挙げられる。eftpos はオーストラリア郵便公社と提携して、ID プラットフォーム connect ID の PoC を実施しており、ユーザに容易な ID 管理・本人確認・ペイメント等を提供している。

表 2- 29 eftpos ConnectID の概要

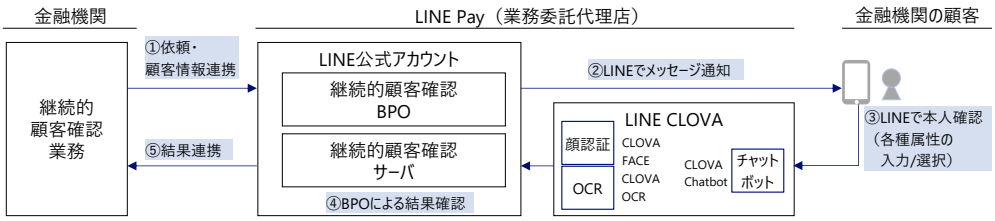
概要	豪郵便公社や政府・銀行などの IdP と e コマース業者や政府機関 RP との間の本人確認のハブとして機能するプラットフォーム
TrustID との関係性	ConnectID は TrustID framework および TDIF 上で稼働するよう設計されている。 ・ ConnectID は、eftpos が提供するプラットフォームサービス ・ TrustID および TDIF は要件定義、参加者の役割と運用責任の定義、データの使いやすさ、プライバシー、セキュリティ、相互運用性に関する保証等を提供
パートナー（予定含む）	IdP：豪郵便公社、myGovID、その他銀行、小売 RP：小売、政府機関
ユースケース	民間企業：顧客の ID 管理と認証（年齢確認、住所特定、銀行口座情報等） 政府　　：政府からの給付金等の受け取りに関する国民の ID 管理

（コラム）日本におけるデジタル IMS 活用の萌芽事例

（1） LINE CLOVA の AI 技術を活用した金融機関向け銀行口座保有者の継続的顧客管理サービス[166]

金融機関が行う従来の継続的顧客管理方法では、郵送物の手配と配送に費用と手数がかかる上、顧客による書類の記入や返送がされにくいため、銀行口座管理の安全性、効率化が課題とされている。LINE Pay と LINE CLOVA は、金融機関から委託を受け、LINE 公式アカウント上で、対象顧客に対する本人確認依頼の通知、トーク画面内での本人確認、確認結果の金融機関へのフィードバックを行う。この仕組みにより、口座保有者の継続的な顧客確認を完全にオンライン化し、金融機関のオペレーションの DX に貢献できる。サービスは 2021 年夏ごろの開始が予定されている。

表 2- 30　LINE CLOVA の AI 技術を活用した金融機関向け銀行口座保有者の継続的顧客管理サービスの概要

名称	LINE Pay 社　銀行口座の継続的な顧客確認サービス
提供開始日	2021 年夏ごろ開始予定
対象課題	継続的顧客管理のための金融機関の対応コスト （郵電費、顧客とのコミュニケーション、情報確認・更新作業等
解決の方向性	LINE のインターフェースおよび内部機能（LINE Pay の口座情報管理機能と LINE のメッセージ機能）を活用して顧客への通知・顧客からの更新情報収集・登録作業をデジタル化し、UX 向上とコスト削減を両立する
仕組みの概要	
参加者	✓ 金融機関：継続的顧客確認の委託元、既存顧客データの連携 ※具体的な金融機関名は現時点で非公開 ✓ 金融機関の顧客：LINE インターフェース上で顧客属性情報の更新内容を入力 ✓ LINE Pay：顧客への通知と顧客属性情報の更新管理、金融機関への顧客属性情報フィードバック

[166] LINE Pay 社のホームページから NRI 作成

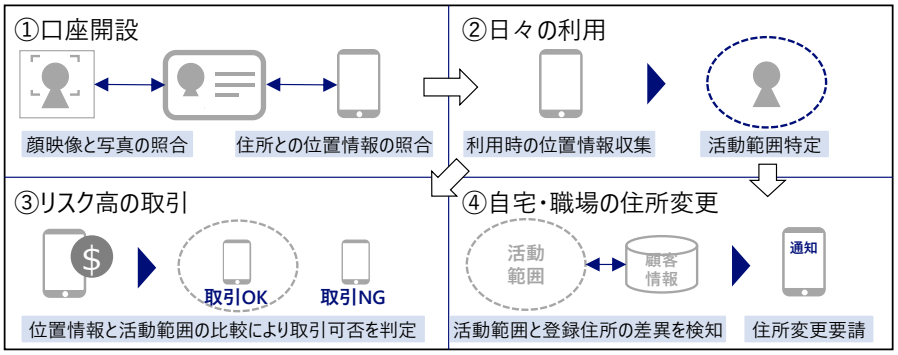
(2)「インターネットバンキングにおける本人認証」および「継続的顧客管理」のシステム基盤構築実証実験[167]

現在主流の二要素認証では不正アクセスの完全排除は困難であり、また、顧客のユーザビリティも高いとは言えない。そこで、株式会社みずほ銀行、グーグル・クラウド・ジャパン合同会社、株式会社野村総合研究所、大日本印刷株式会社の 4 社は、顧客の利便性を損なわないままセキュリティを高めるため、スマートフォン、タブレット、ノートパソコン等のモバイル端末の位置情報（ジオロケーション）や顔認証技術を活用した、デジタルアイデンティティによるインターネットバンキングにおける本人認証および継続的顧客管理のシステム基盤構築とサービスの実現に向けた実証実験を行った。実験結果はまもなく第一次最終報告として公表される予定である。

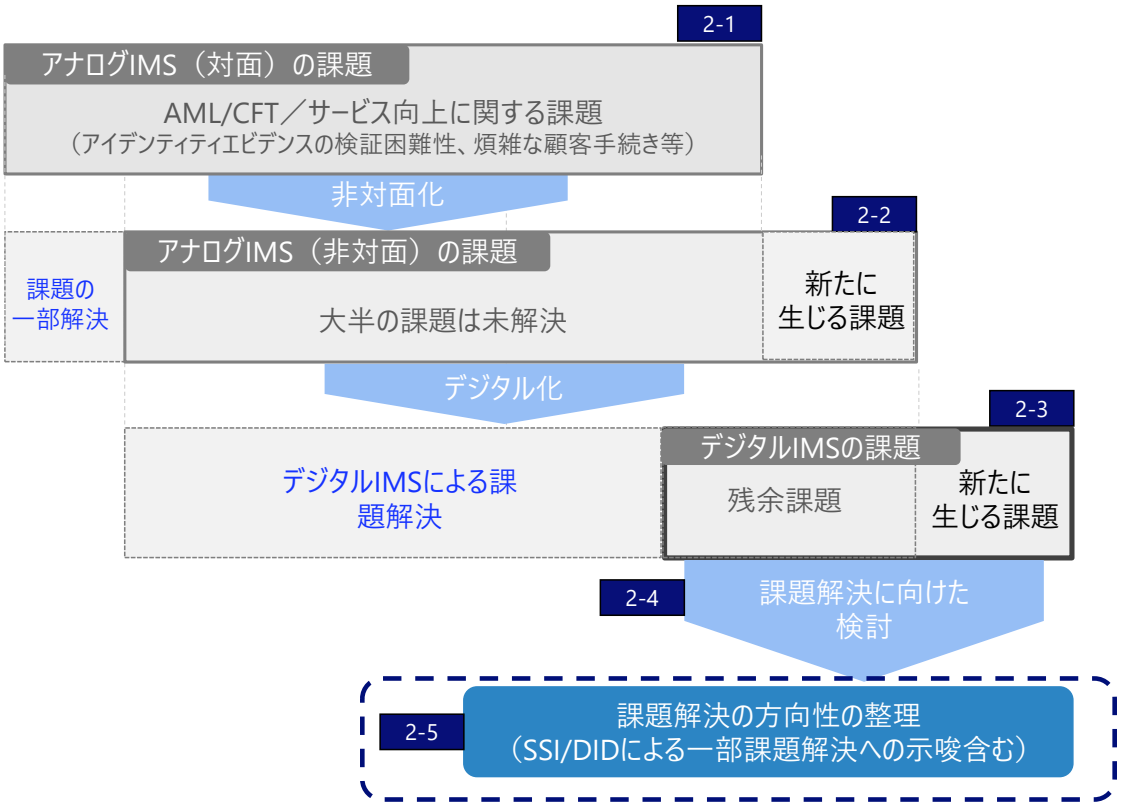
表 2- 31 「インターネットバンキングにおける本人認証」および「継続的顧客管理」のシステム基盤構築実証実験の概要

実証実験名称	インターネットバンキングにおける本人認証」および「継続的顧客管理」のシステム基盤構築実証実験
実施期間	2020 年 5 月～2020 年 10 月
対象とする課題	パスワード等の「知識」と専用カード等の「所有物」の二要素認証がはらむ、「他人に渡るリスク」「紛失／忘却リスク」
解決の方向性	位置情報（※） ・顔認証という「本人しか持ちえない情報」「紛失／忘却リスクがない情報」の利用 （※）位置情報の利用・・・自宅住所等での端末操作を認証の制約とすること
実施内容	① テストシステムの構築 ② 口座開設～送金～登録情報変更のシナリオに沿って顔認証・位置情報の登録/変更とモバイル端末からの認証をテスト ③ 認証の精度や認証ルールなど、実現に向けた技術・制度課題を整理

[167] みずほ銀行のホームページから NRI 作成

想定活用事例	
参加者	✓ みずほ銀行：本実証実験の設計、効果検証等 ✓ グーグル・クラウド・ジャパン：当実証実験における技術支援の提供 ✓ 野村総合研究所：インターネットバンキングにおけるアプリおよびサーバーシステムの構築 ✓ 大日本印刷：顔認証技術を活用した本人確認機能の提供、API 連携による顔認証機能・eKYC 機能の構築
成果	✓ まもなく第一次最終報告のため、詳細は非公表

2-5. 課題解決の方向性の整理



デジタル IMS の構築・運用に向けた様々な課題の解決に向けては、前節で取り上げた通り、海外各国において課題に取り組む先進的事例がみられた。

本節では、2-3-8 で挙げた「デジタル IMS 化でも解決しなかったアイデンティティ管理上の課題およびデジタル IMS 化により新たに発生する課題」に対し、 2-4 で挙げた事例等を元に課題解決の方向性を改めて整理する。

なお、SSI/DID の活用により解決が期待される課題については、3 章で課題解決の方向性を引き続き検討する。以下が該当する。

2）ID 連携の課題の一部

3）プライバシーの課題の一部

一方、課題解決の方向性に従い具体的に課題解決を推進するにあたっては、複数のステークホルダーが存在し、各々異なる関心事項を持っていることが想定される。課題解決推進上の課題については、4 章にて、想定されるステークホルダーおよび関心事項を整理し、解決のアプローチを検討することとする。

2-5-1. 本節の検討対象課題一覧

本節における課題解決の方向性整理の対象は、2-3-8 で整理した下表のとおりとする。

表 2- 24 本節で検討対象とする課題一覧

課題の観点	課題
1） IAL	・デジタル IMS の適切な活用を促す規制フレームワーク整備
2） ID 連携（責任分界を中心に）	・ID 連携当事者間のビジネスモデル・責任分界の未整備 ・特定の金融機関（IdP）への依存度が高まる
3） プライバシー（同意管理・データミニマイゼーション）	・ID 連携の同意管理負担 ・複数サービス横断で顧客データを利活用するための、サービス利用許諾の整備負担 ・データ提供側として、情報の第 3 者提供に関する顧客同意対応負担が大きい ・情報の第 3 者提供に関して、データ受け取り側としての対応負担が大きい ・データ利活用の目的と範囲に関する、顧客と金融機関の認識齟齬リスクの増大
4） 金融包摂	・デジタル対応できない人物の金融排除
5） 相互運用性	・煩雑な ID 連携仕様への対応負担
6） 新しい業務へ移行するための投資判断	・最適化された既存業務をデジタル IMS 利用のために変更する投資判断が困難
7） クロスボーダー取引の諸課題	・AML/CFT 規制の国家毎の差異や、FATF 基準及びその他の規制・監督上の要件を実施する際の国境を越えたデータ共有への法的な障壁

2-5-2. 各課題の解決の方向性

1）”IAL” の課題詳細と取り組み事例・得られた示唆

表 2- 25 デジタル IMS の適切な活用を促す規制フレームワーク整備
課題詳細と課題解決の方向性

対象課題	・ デジタル IMS の適切な活用を促す規制フレームワーク整備

課題詳細	・AML/CFT 等の規制目的に適した IAL が担保されるデジタル IMS の利用が必要であると、FATF のガイダンスで指摘されている[168]。 ・適切な IAL の整備には、IAL と本人確認規程が接合している状態（＝金融機関が信頼性の高いデジタル IMS をリスクに応じて適切に使用できるように本人確認規程が規定されている状態）が望ましい。しかし、現在は、各法域にてアイデンティティエビデンスに対する規定は存在するものの IAL との明確な紐づけは行われていない等、改善の余地があると考えられる。
取り組み事例と得られた示唆	・適切な IAL の設定および IAL と接合した AML/CFT 規制等の整備を行うことが対策として考えられる。 ・整備のアプローチとして、信頼性の高い ID を広く活用することを前提とし、それを可能とする AML 規制を整備するという方策が事例からは示唆される。(2-4 事例（2）シンガポールにおける国民 ID を活用した onboarding の効率化、および　（3） インドにおける India Stack を活用した民間サービスの拡大) ・具体的な AML/CFT 規制等の整備に当たっては、技術革新の取り込み等を鑑み、各金融機関に工夫の余地を持たせることが必要と考えられる。 ・また、IAL 整備の範囲についても、本人確認に特化せず、AML 対応に必要な顧客属性の保証レベルまで踏み込む等の対応も考えられる（2-4 事例（1）EU における金融規制とアイデンティティ保証フレームワーク（eIDAS）の接合に向けた取り組み)。

2）”ID 連携”　の課題詳細と取り組み事例・得られた示唆

表 2- 26　ID 連携当事者間のビジネスモデル・責任分界

課題詳細と課題解決の方向性

対象課題	・ID 連携当事者間のビジネスモデル・責任分界の未整備
課題詳細	・金融機関間等で ID 連携を実施する際に、以下の点が未整備であると ID 連携ビジネスが立ち行かない点が指摘されている。

[168]Guidance on Digital Identity　(2020)
http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html

	- ID の出し手が ID 連携に当たり保証する責任範囲（身元確認にとどまるのか（IAL：ID Proofing)、身元確認にとどまらない KYC の範囲とするか（＋Due Diligence)、等）の明確化。 - データ過誤により、顧客もしくは ID 連携を受けた金融機関において何らかの損害が発生した場合の責任分界 - 新規口座開設や継続的顧客管理を実施するためには、実務として許容できるデータの鮮度が必要になるため、ID 連携する際のデータの鮮度を担保するためのルール・責任を明確化する必要がある - 上記 3 点の責任分界に見合う対価の合意
取り組み事例と得られた示唆	・関係者間協議により、以下のような責任分界の明確化が必要と考えられる（2-4　事例（5）ID 連携サービスにおける責任分界）　。 - ID の出し手が ID 連携に当たり保証する責任範囲の明確化 - 新規口座開設や継続的顧客管理を実施するためには、実務として許容できるデータの鮮度が必要になるため、ID 連携する際のデータの鮮度を担保するためのルール・責任を明確化 - データ過誤により顧客もしくは ID を利用した金融機関において何らかの損害が発生した場合の責任分界の明確化

表 2- 27　特定の金融機関（ID プロバイダー）への依存度の高まり
課題詳細と課題解決の方向性

対象課題	・特定の金融機関（ID プロバイダー）への依存度の高まり
課題詳細	・顧客が、ある 1 金融機関（以下、ID の出し手）が発行したアイデンティティを用いての口座開設を複数金融機関に対して行うと、ID の出し手に対する依存度が高まり、リスクが懸念される。例えば、ID の出し手の検証に問題が発覚した場合等、ID 連携先の金融機関全てのサービスに停止等の影響が出る懸念があると考えられる。 ・更に、ID プロバイダである金融機関に問題が発生すると、当該金融機関の発行した ID に依存しているユーザが一括で被害にあう可能性が有り、影響の拡大が懸念されると考えられる。
取り組み事例と得られた示唆	・特定の ID プロバイダへの依存度を下げるためには、3 章で取り上げられた通り、SSI/DID が課題解決策の一つと考えられるため、3 章で議論を継続する。

3）”プライバシー”　の課題詳細と取り組み事例・得られた示唆

表 2- 28　情報提供時の同意管理の整備

課題詳細と課題解決の方向性

対象課題	・データ提供側として、情報の第三者提供に関する顧客同意対応負担が大きい ・情報の第三者提供に関して、データ受け取り側としての対応負担が大きい ・複数サービス横断で顧客データを利活用するための、サービス利用許諾の整備負担
課題詳細	・個人情報保護法制上、ID 連携の際、連携元と連携先との間で情報の第三者提供に関する同意管理が必要である。 ・情報の第三者提供に関する同意管理について、ID 連携の拡大に伴い以下のような対応負担が増大すると考えられる。　（データ提供側の負担） - データ利活用に関する顧客への説明実施負担 - 同意記録の作成・保管等の顧客との同意管理負担 （データ受け取り側の負担） - データの出し手に対するデータ取得経緯等の確認負担 - データ利活用の目的・内容等をデータ提供側に説明し、理解を得る負担
取り組み事例と得られた示唆	・法令対応であるので、各国の個人情報保護法制に則った対応を実施する必要があると考えられる。 ・中長期的には、SSI/DID の仕組みを活用し、顧客が自己主権により各社とデータ利活用について同意する形とすることで、第 3 者提供という形態自体を見直し、負担削減を図るという考え方もあるため、3 章で検討を継続する。

表 2- 29　データ利活用の目的と範囲に関する、顧客と金融機関の認識齟齬リスクの増大

課題詳細と課題解決の方向性

対象課題	・データ利活用の目的と範囲に関する、顧客と金融機関の認識齟齬リスクの増大
課題詳細	・国内有識者ヒアリングにて、以下の点が課題として指摘されている。 - 金融機関等からのデータ利活用に対する説明が不明瞭であると、顧客は自らが意図しないデータ利活用がなされてしまう懸念がある。 - 一方、特に個人においては、金融機関からの説明を完全に理解し金融機関が説明通りにデータ利活用しているか確認することは困難、という側面もある

	- 結果として、とりあえず同意してしまい、顧客の意図しないデータ利活用を認めてしまうケースもある。
取り組み事例と得られた示唆	・形式的な同意取得ではなく、利用者が提供したデータが、金融機関等においてどのように使われるかを顧客が正しく認識できる管理機能を金融機関が提供する必要があると考えられる。 ・加えて、上記管理機能自体が正しく機能していることを確認するため、第三者による金融機関の監査も必要と考えられる。 ・また、情報銀行という形態も解決策の一つとなりうる。情報の管理を情報銀行に委ねる形で、情報銀行側で責務を負いデータ提供を実施する。消費者団体が情報銀行の認定制度を設ける事例もみられる[169]。

（補足）情報銀行認定制度について （以下、日本ＩＴ団体連盟ＨＰより抜粋）

認定者

日本 IT 団体連盟（以下、IT 連盟）

一般社団法人。IT 関連団体の連合体として、我が国の IT 産業の健全な発展に貢献するとともに、世界最高水準の IT 社会の構築を目指すため、政府との双方向のコミュニケーションを実現しながら積極的に提言等を行い，もって我が国の経済・社会，国民生活の向上に寄与することを目的に設立

制度概要

IT 連盟による「情報銀行」の認定制度は、「情報信託機能の認定に係る指針」（総務省・経済産業省「情報信託機能の認定スキームの在り方に関する検討会」）および同指針を踏まえて IT 連盟として策定した情報セキュリティ対策やプライバシー保護対策等に関する認定基準に適合していることを審査。当該認定を受けた「情報銀行」事業者およびサービスは、安心・安全な「情報銀行」として、消費者がその個人情報を信頼して託せられる「情報銀行」であることをアピールすることが可能。当該認定は任意であり、情報銀行事業に必須のものではない。

認定の運用体制

「情報銀行」認定に関するスキームについては、「情報信託機能の認定に係る指針」を踏まえ、「情報銀行」認定における独立性、中立性、公平性などを担保しつつ、責任ある認定を行うことができるガバナンス体制で運用。

[169] 日本 IT 団体連盟（以下、IT 連盟）による「情報銀行」の認定制度
https://www.tpdms.jp/system/index.html

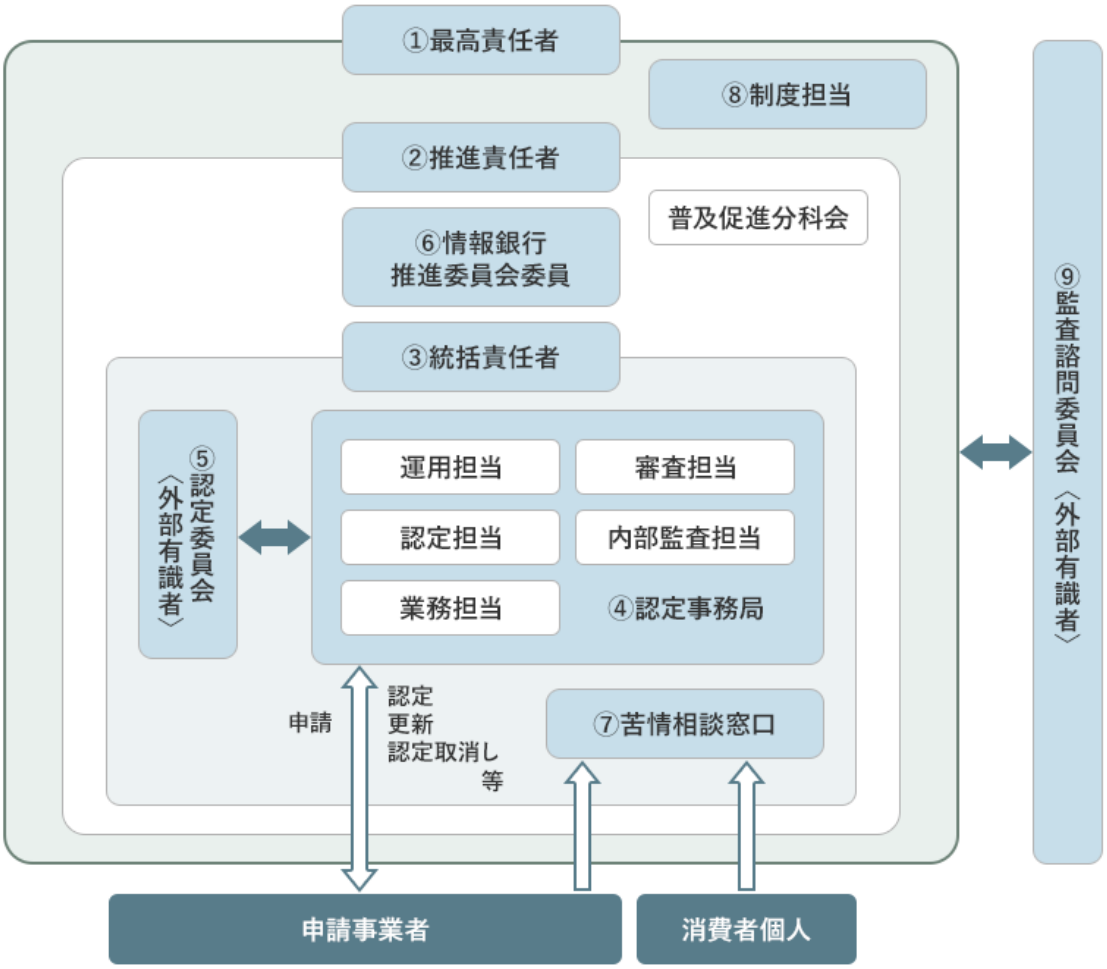


図 2-19 情報銀行認定運用体制図

① 最高責任者：認定機関を代表し、認定制度の企画立案及び認定業務等による「情報銀行」推進等認定機関の運営に関する責任を保持

② 推進責任者：認定業務、問合せ・苦情等対応業務及び普及促進業務等「情報銀行」推進に関する責任を保持

③ 総括責任者：認定業務並びに申請事業者及び消費者個人等からの問合せ・苦情等対応業務を総括し、執行の責任を保持

④ 認定事務局：下記担当者で構成され、認定業務を実施

運用担当：認定業務運営における品質維持等を実施

業務担当：申請受付、認定証発行等を実施

認定担当：認定判定用報告書の作成等を実施

審査担当：書類審査等、審査計画書及び審査報告書の作成等を実施

内部監査担当：認定業務運営について内部監査を実施

⑤ 認定委員会：上記④の認定判定用報告書等により認定基準への適合性評価、認定判定を実施
⑥ 情報銀行推進委員会委員：上記⑤の結果を踏まえ認定決議、認定判定を実施
⑦ 苦情等相談窓口：申請事業者及び消費者個人等からの問合せ・苦情等対応を実施
⑧ 制度担当：指針の見直し等を踏まえた認定制度の企画立案等の検討を実施
⑨ 監査諮問委員会：認定機関の運営に関する公平性等の監査諮問を実施

4）”金融包摂” の課題詳細と取り組み事例・得られた示唆

表 2- 30 デジタル対応できない人物の金融排除
課題詳細と課題解決の方向性

対象課題	・デジタル対応できない人物の金融排除
課題詳細	・デジタルインフラ整備状況の観点からの金融排除懸念について、FATFのガイダンスでは以下の指摘がされている。[170] - 携帯電話・スマートフォン等が十分普及していない、インターネットアクセスが可能な地域が限定的、等の理由からデジタルインフラの活用が難しい地域においては、デジタル化の推進が金融排除を生む懸念がある ・デジタルに対するリテラシーの観点の金融排除懸念について、海外有識者へのヒアリングでは以下が指摘されている。 - デジタル化されていない人々の年齢層を見てみると高齢者の方が多く、彼らがデジタルサービスの利用、携帯電話の銀行アプリの利用に躊躇する理由は、間違った操作に対する恐怖、例えば誤ってボタンを押してしまい間違った場所に送金してしまうなどの恐怖等の精神的障壁である
取り組み事例と得られた示唆	・各国の金融機関の業務整備状況や各国の政治体制等に応じた方針での対応になると考えられる ・金融で活用できるデジタルアイデンティティインフラ（アイデンティティ管理インフラや決済インフラ）を国を挙げて整備し、全国民をデジタルに取り込む方針（2-4 事例（2）シンガポールにおける国民 ID

[170] Guidance on Digital Identity （2020）
http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html

	を活用した onboarding の効率化、および　(3) インドにおける India Stack を活用した民間サービスの拡大) ・既存の業務も活用しアナログ・デジタル両方の形での受入を行う方針（日本等先進国） ・マイノリティに対して、オペレーションの代理を行う職務（既存の行政書士に近い役割）を設け、運用対処を行う方策も考えられる ・デジタル化により AML 規制対応の強化を図っている側面もあるため、AML 規制強化と金融包摂のバランスを取った対応が必要と考えられる

5）”相互運用性”　の課題詳細と取り組み事例・得られた示唆

表 2- 31　煩雑な ID 連携仕様への対応負担

課題詳細と課題解決の方向性

対象課題	・煩雑な ID 連携仕様への対応負担
課題詳細	・国内有識者ヒアリングにて、ID 連携負担に関する以下の課題が指摘されている。 - 各金融機関が独自の仕様でデジタル IMS を実装してしまうと、金融機関間で ID 連携を行う際に、各金融機関の接続の度に別の技術仕様に基づく接続対応が必要となる。 - これは接続負担の増大につながり、結果、ID 連携の拡大につながらず ID 連携がビジネスとして立ち行かない、顧客がデジタルアイデンティティを広く活用できず、社会全体にデジタルアイデンティティが普及するスピードが上がらない、といった結果を招く。
取り組み事例と得られた示唆	・技術仕様や関連する法制度の整備を官民の連携により対応し、社会全体への幅広い普及を目指す事例もみられる（(9) オーストラリアにおける官民サービスの相互運用) ・本課題は、主に一つの法域の範囲を想定した際の問題意識からあがった課題であるが、国をまたいだ技術仕様の相互運用性ついても同様であり、グローバルで ID 連携仕様の標準化が進められている（(6)　標準化団体の取り組み)。国内有識者ヒアリングにおいても、以下が指摘されている。 ✓ 各国毎に別々の仕様になるだけでも実装負荷は膨大となる。 ✓ このため、国際標準一本化はより望ましい姿と、ベンダー等からはとらえられている。

	✓ ベンダーは、各国仕様に応じた実装は非常に煩雑と考えており、積極的に ISO 活動等のグローバルな標準化活動に参画している。 ・また、標準の策定にとどまらず、Certification Program の策定等、標準への準拠性を検証し正しく普及させる仕組みも出てきている。 （例）FDX（Financial Data eXcahnge）[171] ✓ 準拠性を機械的に検証可能な仕組みも提供し、標準準拠の認定を実施 ✓ グローバルに共用できる部分と各国制度等による部分を各々検証 ✓ （FDX の Certificate のテスト手順） 1 次試験：OIDF Certificate（FAPI ConformanceTest） 2 次試験：各国個別要件に応じたテスト

6）”新しい業務へ移行するための投資判断” の課題詳細と取り組み事例・得られた示唆

表 2- 32　デジタル IMS 利用のための投資判断
課題詳細と課題解決の方向性

対象課題	・最適化された既存業務をデジタル IMS 利用のために変更する投資判断が困難
課題詳細	・国内有識者ヒアリングにて、以下の課題が指摘されている。 - デジタル IMS 利用のための初期投資は、アナログ IMS からの移行期間中は純粋に追加コストとなり、最適化された現行業務を変更してまで対応するインセンティブを見つけることが難しい。 - セキュリティ対応等は、技術進歩に合わせて継続的に投資することが必要であるが、どこまで最新技術を追いかけるための投資を行うべきか、判断できない。 - 新たな取り組み単体での収益化計画策定は困難。既存プロセスからの移行に伴う既存コスト圧縮等を加味した計画を作らねばならない。

[171] OpenIDFoundation “Financial Data Exchange, OpenID Foundation Take Step Towards Global Standard for Financial Data Sharing” （April 2019）
https://openid.net/2019/04/02/financial-data-exchange-openid-foundation-take-step-towards-global-standard-for-financial-data-sharing/

取り組み事例と得られた示唆	• 自らの持っているアイデンティティ情報の収益化によるコスト回収は対策の一つとして考えられる（2-4　事例（5）ID 連携サービスにおける責任分界)。 • ID 連携事業単体で投資を回収するという収益回収モデルではなく、既存のオペレーションコスト低減や盗難・不正行為の減少による対応コスト低減などのコスト低減効果[172]も加味した、包括的な施策としてとらえる考え方もある。 • また、アイデンティティエビデンスとして国民 ID を活用する場合、国・当局は国民 ID の整備コストについてインフラコストに加えて普及コストの観点からも検討する必要があること[173]、金融機関は国民 ID のルール整備状況や普及状況に応じて手戻りのない投資が重要であること [5]、がそれぞれ文献で指摘されている。

＊上述の説明で参照している 2 文献「WorldBankGroup, Private Sector Economic Impacts from Identification Systems」・「WorldBankGroup, Public Sector Savings and Revenue from Identification Systems:Opportunities and Constraints」の主な論点については章末の参照文献を参照

７）”クロスボーダー取引の諸課題”　の課題詳細と取り組み事例・得られた示唆

表 2- 33　クロスボーダー取引に関する法的課題
課題詳細と課題解決の方向性

対象課題	・ AML/CFT 規制の国家毎の差異や、FATF 基準及びその他の規制・監督上の要件を実施する際の国境を越えたデータ共有への法的な障壁
課題詳細	・ 金融機関は一定額を超えた海外送金には送金元・送金先に関する情報の収集を求められている。 ・ FSB[174]では、海外送金時の送金元・送金先確認について、以下のような法的障壁があるとしている。

[172] Private Sector Economic Impacts from Identification Systems
https://elibrary.worldbank.org/doi/pdf/10.1596/31828
[173] Public Sector Savings and Revenue from Identification Systems:Opportunities and Constraints
https://documents1.worldbank.org/curated/en/745871522848339938/pdf/Public-Sector-Savings-and-Revenue-from-Identification-Systems-Opportunities-and-Constraints.pdf
[174] Enhancing Cross-border Payments Stage 1 report to the G20,Apr 2020
https://www.fsb.org/wp-content/uploads/P090420-1.pdf

	- 各国における AML/CFT 規制の差異により、本人確認の厳格さのレベルが異なり、情報の信頼性に懸念がある。 - 送金元・送金先に関する個人情報を国境を越えて共有する必要がある際に、各国のデータ保護法制が障壁となる場合がある。
取り組み事例と得られた示唆	・FSB においては、左記課題の解消を目指した対応ロードマップを作成し、対応方針の議論を継続（P.61 参照）[175] ・各金融機関・法域においては、EU という広域で利用できる eID を用いてクロスボーダー取引の効率化を図ろうとする動きや、顧客を富裕層と限定することで、業務負担を許容し外国からの口座開設を受け入れる動き等の個別の動きが見られる（(5) ID 連携サービスにおける責任分界)。

[175]Enhancing Cross-border Payments Stage 3 roadmap （13 October 2020）（日本語は NRI 抄訳）
https://www.fsb.org/wp-content/uploads/P131020-1.pdf

2-6.本章の結論

- 金融分野においてもデジタルアイデンティティの重要性は認識されており、また、信頼性の高いデジタル IMS の構築により、AML 規制対応強化の実現とともに、アイデンティティエビデンスの検証負担等アナログを理由とした業務負担が多数解消されることが期待されることを確認した。

- このため、1 章で述べたデジタルアイデンティティ概論と同様、アナログでの処理→アイデンティティマネジメントシステムのデジタル化→ Federation モデルのアイデンティティマネジメントシステムという流れをたどり、デジタルアイデンティティの活用が進展していくと考えられる。銀行が IdP となる事例もあり、かつ IdP としての役割への期待が大きいことも、この流れを後押しすると考えられる。

- この実現のためには、規制整備、責任分界、技術仕様の整備、プライバシー、金融包摂への配慮、新しい業務へ移行するための投資、といった課題の解決が求められる。本章では、先行事例等を参考にしつつ課題解決の方向性の整理を行ったが、実際の課題解決に当たっては規制当局・金融機関・顧客といったステークホルダー間の協議による推進が求められる。協議推進上の課題の解決については 4 章で引き続き議論を行う。

また、デジタル IMS の課題として指摘された特定の金融機関（IdP）への依存に対する対応やプライバシーの課題については、SSI/DID の活用によってさらなる改善が図られる期待がある。この点は、3 章で引き続き議論を行う。

第 3 章　自己主権型アイデンティティ(SSI)/分散型アイデンティティ(DID)

本章の概要

本章では、自己主権型アイデンティティ(SSI)と呼ばれる思想と、その実現手段として検討されている分散型アイデンティティ（DID）に関する議論動向について整理する。

SSI モデルによる IMS は、現時点で確立した標準が存在しない。そのため、まず 3-1 では、代表的なユースケースを踏まえつつ、本調査における DID を用いた SSI/DID の想定実装イメージを定義する。その上で 3-2 では、複数の標準化団体が提唱する実現方式を俯瞰し、SSI/DID の特性の実現において技術面・統制面の両観点から必要な構成要素の抽出と整理を行う。続いて、3-3 では、SSI/DID の先行事例/PoC 事例について整理する。特に先進事例として注目されている、カナダの Verified.me 及びスペインの Alastria_ID/Dalion について詳細に整理する。これらの整理を踏まえ、3-4 では SSI/DID の長所と実現に向けた課題を導出する。そして、3-5 では SSI/DID を金融取引に活用する際に必要となる金融規制上の論点について考察する。

3-1. SSI/DID の概要

3-1-1. SSI/DID の全体像

自己主権型アイデンティティ（Self-Sovereign Identity：SSI)とは、1 章で記述したようにアイデンティティの管理主体が介在することなく、個人が自分自身のアイデンティティをコントロールできるようにすることを目指す思想を指す[176]。SSI ではユーザが自分の属性情報に関するコントロール権を確保の上、信頼できる組織から発行された本人の属性情報（クレーム）を取得し、ユーザの許可した範囲で RP 等に連携できるようにする。従来のモデルでは、IdP 及び RP はユーザのアイデンティティ情報を保持・管理する必要があったが、SSI の思想では、IdP はアイデンティティ情報の発行者（Issuer）のみの役割を担うことが想定される。

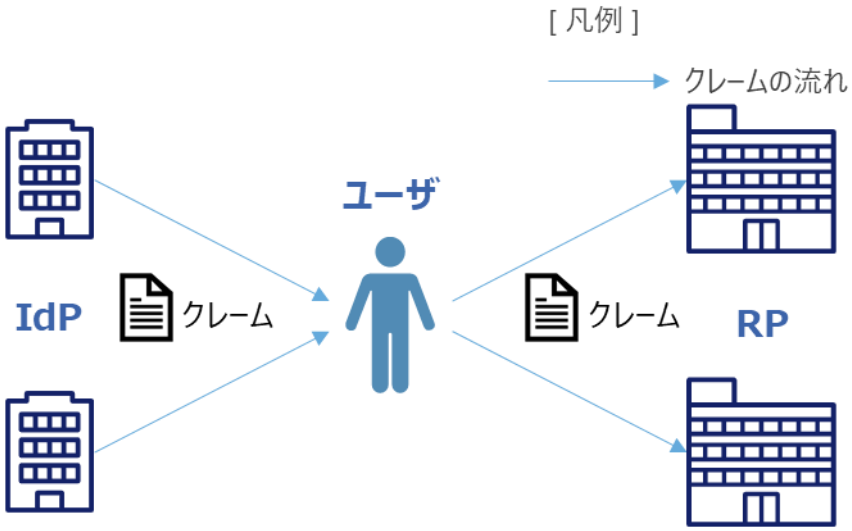


図 0-1：SSI の概念図

自分自身でデジタルアイデンティティを自己制御できることを目的とする SSI に対し、分散型アイデンティティ(Decentralized Identity: DID)は、ユーザのデジタルアイデンティティが特定の IdP 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。

実現にあたり、ブロックチェーン等の分散レポジトリの活用が提唱されることが多く、例えば、分散型アイデンティティのホワイトペーパーを公表しているマイクロソフトは「分散型アイデンティティとは、ユーザ名などの識別子を、自己所有の独立した ID に置き換え、

[176] Sovrin Foundation, "What is self-sovereign Identity?," (December 2018), https://sovrin.org/faq/what-is-self-sovereign-identity/

ブロックチェーンや分散型台帳技術を用いてデータ交換を可能にすることで、プライバシーの保護や取引の安全性を確保することができるトラストフレームワーク」と定義している[177]。

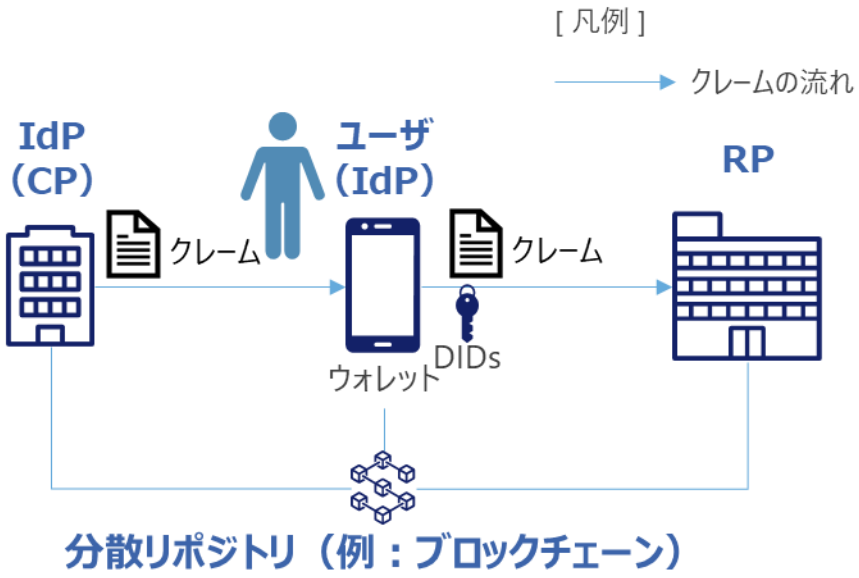


図 0-2：DID の概念図

なお、SSI の思想の実装にあたり、例えば World Wide Web Consortium(W3C)においては、Decentralized Identifiers (DIDs)と Verifiable Credentials (VCs)という二つの仕様が検討されている。これら仕様の詳細については 3-2-2 にて詳述するが、SSI/DID における各種用語は検討団体によって用いる用語が異なる。本調査での SSI/DID に関する概念の名称は 1-1 にて ISO/IEC24760-1 と OpenID Connect Core 1.0 を基にした「IMS を構成する主要アクター」での用語を基本は引き続き用いつつ、W3C 等による図表や仕様の説明では当該団体ごとの用語を用いるため、以下の通りに対応させる。

表 0-1：本調査と W3C による SSI/DID に関する用語

#	本調査での用語	W3C による用語	本調査での用語の定義	W3C での用語の定義※
1	クレーム（Claim）	Verifiable Credential	アイデンティティであるエンティティの属性集合のう	暗号学的に検証可能な作成者を持ち、改ざんや盗み見が

[177] Microsoft, "Own your digital identity," https://www.microsoft.com/en-us/security/business/identity-access-management/decentralized-identity-blockchain

			ちの一部の属性集合	わかる（tamper-evident）エンティティの属性集合
2	クレームプロバイダー (Claims Provider: CP)	Issuer	クレームを提供するエンティティ	クレームを主張（assert)、クレームから Verifiable Credential を生成、Verifiable Credential をホルダーに送るエンティティ
3	リライングパーティ (Relying Party: RP)	Verifier	特定のエンティティのアイデンティティ情報のベリフィケーションに依拠するエンティティ	Verifiable Credential を受け取る エンティティ

3-1-2. SSI で実現すべき項目

1 章で提示したように Kim Cameron 氏は「アイデンティティの 7 原則」をベースにした「SSI の 7 原則」を提示しており、原則 5 （「『アイデンティティハブ』の統合」）および原則 6 （「長期のアイデンティティの安定性に向けた DID の統合」）が更新されている。原則 5 の「アイデンティティハブの統合」とは、ユーザは、プロバイダ間で一貫した方法で自分自身を表現し、アイデンティティを使用することができ、同時にコンテキスト間でアイデンティティを分離することができることである。原則 6 の「長期のアイデンティティの安定性に向けた DID の統合」とは個人データを事業者に依存しない形で保管したうえで、アイデンティティ事業者を存続させ、サービスとの関係を維持することである。

各標準化団体では、実現のプロトコルとアプローチは異なるものの、原則 5 と原則 6 の実現すべき項目手段として、いずれも”認証と属性情報の分離“、”分散した属性情報の活用と選択的な提示”、”提示先の秘匿（Unlinkability）”、そして”長期のデジタルアイデンティティの保管と利用”という 4 つの特性を想定していると考えられる。

SSI についての理解を深めるために、本項では従来の IMS モデルにおける課題と、その課題を解決することができると考えられている SSI モデルについて、具体的なユースケースをもとに説明する。ここで想定するユースケースは、就職活動時に就職先に卒業証書（あ

るいは成績証明書等）を提示する場合であり、具体的には下記図のような処理フローが想定される。

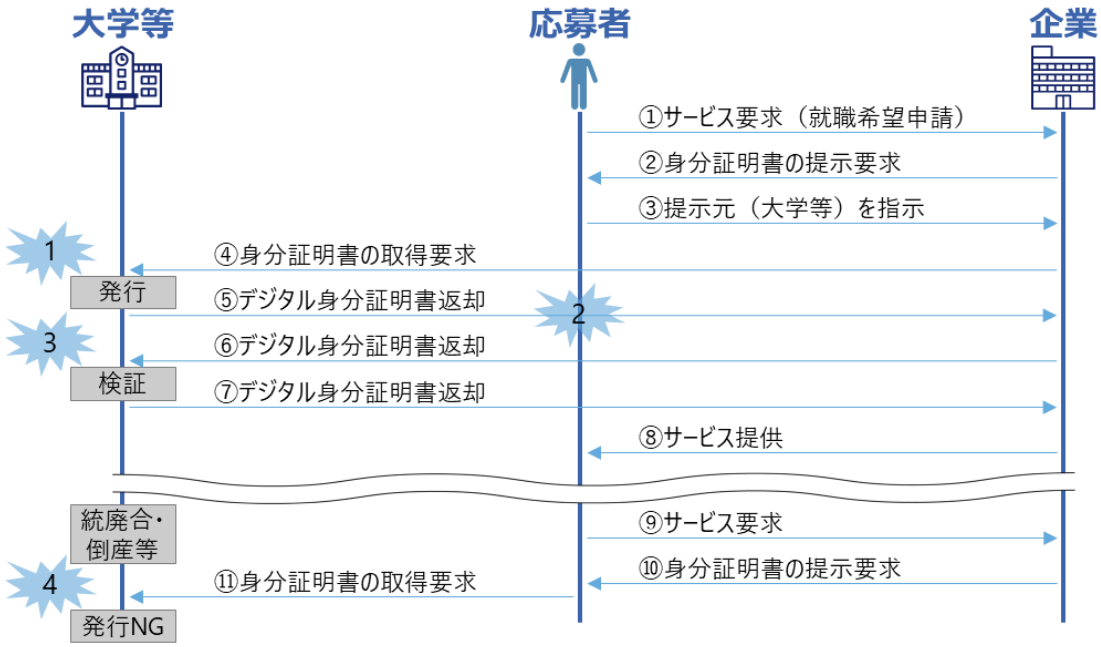


図 0-3：既存モデルで就職活動時に就職先に卒業証書を提示するケース

既存モデルではクレームの管理を大学等の ID プロバイダに強く依存しており、上図の番号と対応させて下記に示すリスクが例として想定される。

1. クレーム（身分証明書）提示の際、大学等においてユーザ認証が必要となる。大学等にアカウント停止措置を受けることで身分証明書の取得が困難となる。
2. 企業側に提示する情報について応募者にコントロール権がない。
3. どの企業に応募しているか、大学等に知られてしまう。
4. 大学が将来的に統廃合や倒産等で消滅した場合、当該大学から証明書が発行不可能となってしまう。

SSI のモデルは、本項で述べた 4 つの特性（1. 認証と属性の分離、2.分散した属性の活用・選択的な提示、3. 提示先の秘匿、4. 過去取得したクレームの再提示・検証が可能）を用い、これら既存モデルの課題を解消する可能性を有していると考えられる。SSI モデルで就職活動時に就職先に卒業証書を提示するケースは以下の通り。

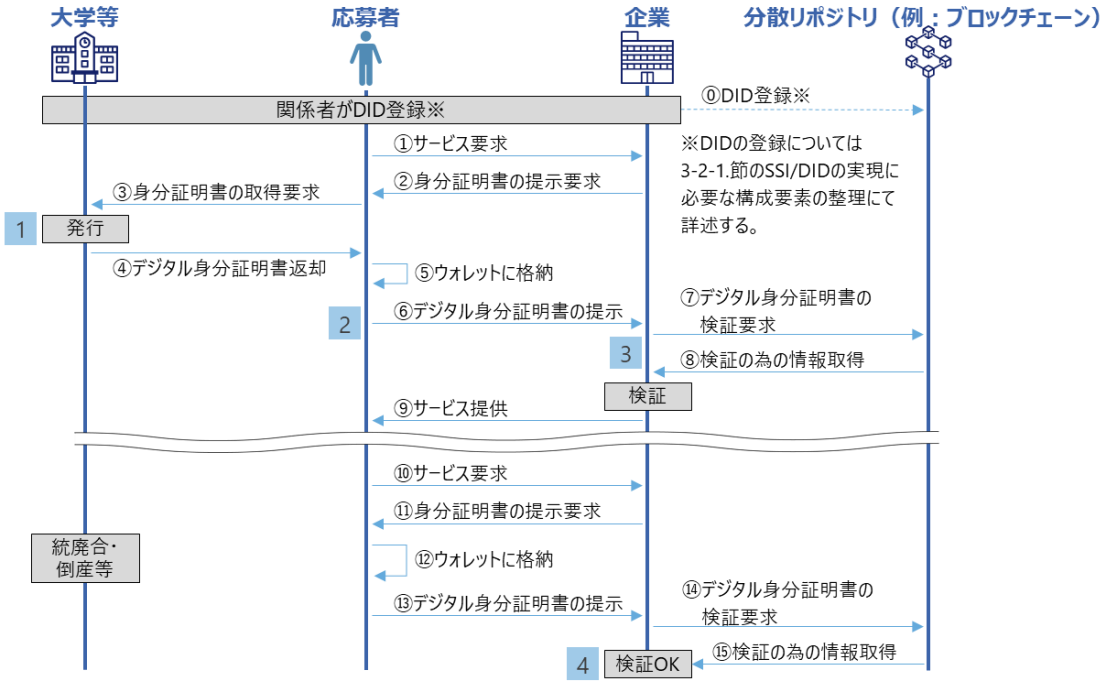


図 0-4：SSI モデルで就職活動時に就職先に卒業証書を提示するケース

次に、上の図で示した 4 つの特性についてそれぞれ詳述するとともに、各特性がどの様に既存モデルの課題解決に貢献するかを述べる。

1. 認証と属性の分離

“認証と属性の分離”とは、Recognition（当人認証）と Selfness（属性情報）の分離を意図する。これにより、ユーザの持つ「ウォレット」と呼ばれるデータ保管場所がハブとなり各企業にデータを連携するハブ＆スポークの形をとることが可能となることで、既存モデルの課題である ID プロバイダへの依存度を下げた形で、分散型のデータ連携が可能となる。また、「ウォレット」を介した分散型のデータ連携が可能になるということで、自分の個人情報を自らがコントロールし、各企業へ必要な情報を連携しながら価値提供も可能となる。

実現のためには、Peer to Peer の対向認証に必要となるクレデンシャル情報（識別子・シークレット）と連携される属性情報の分離を行う必要がある。またその実現手段として分散型アイデンティティ（DID）と呼ばれる方式が、様々な標準化団体で検討されている。同方式を用いることで、ID プロバイダがアカウント停止を行った際に自らの属性情報が取得できなくなる点を回避できるようになるほか、クレームプロバイダー（上図においては大学）以外にウォレットにもクレーム（属性情報）を保持しておくことが可能となる。また分散型台帳技術（DLT）や長期署名等を用いたヒストリカルな署名を付与することで、ID プロバイダによる改ざんが困難となり、当該時刻におけるデータの真正性を保証する。

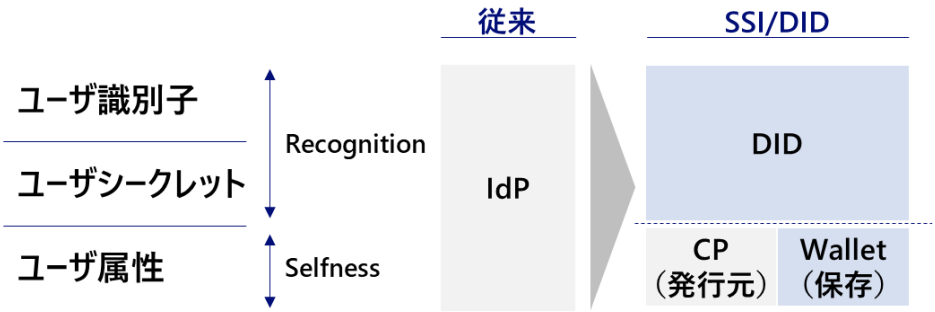


図 0-5：アイデンティティ構成要素とアイデンティティの管理

2. 分散した属性情報の活用・選択的な提示

分散した属性情報の活用・選択的な提示とは、点在する CP からクレームを収集し、ユーザが意図したクレームのみを RP に展開可能なことを意図する。例えば W3C の規定する「Verifiable Credentials Data Model」では、ユーザ（Holders）が、”Issuer”と呼ばれる役割を担うエンティティ（CP）からクレームを検証可能な形で発行してもらい、それを自身のウォレットに格納する。その後、自身の望むクレームのみを”Verifier”と呼ばれるエンティティ（RP）に連携し、クレームの発行元や真正性等を検証して貰うことで、提供したクレームに応じたサービスや機能を供与して貰うモデルが検討されている。

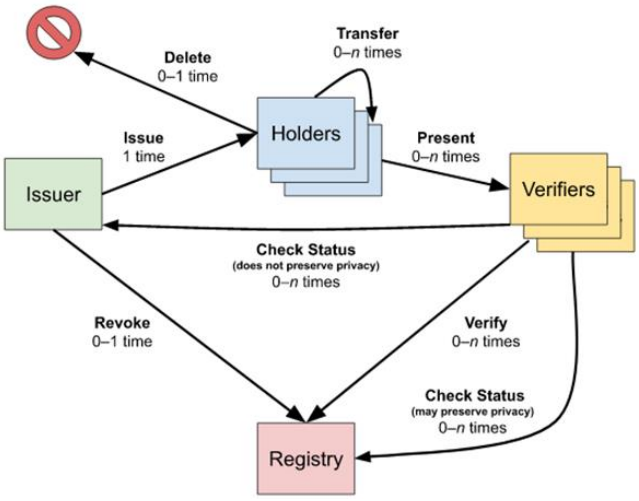


図 0-6：Verifiable Credentials Data Model における
Verifiable Credential のライフサイクル[178]

またその際、ユーザは CP から取得した Verifiable Credential を束ね自身のペルソナのサブセットとして提示（Verifiable Presentation と呼ばれる）が可能なモデルが示されている。

[178] W3C, "Verifiable Credentials Data Model 1.0 - 5.1 Lifecycle Details," (November 2019), https://www.w3.org/TR/vc-data-model/

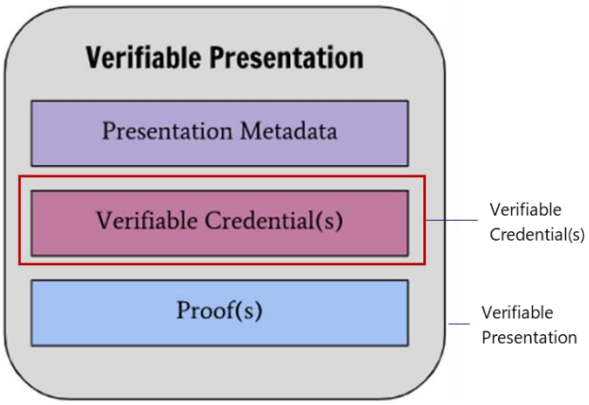


図 0-7：Verifiable Credentials Data Model における VC・VP の概要図[179]

3. 提示先の秘匿（Unlinkability）

提示先の秘匿（Unlinkability）とは、ユーザが CP に、その RP に発行したクレームを連携したか知られることなく、クレームの連携・検証が可能なことを意図する。これはクレームを受け取った RP は、その真正性を検証（Verify）する必要があり、その際に付与された署名値の検証に用いる検証鍵を、クレーム発行元である CP に照会してしまうと、クレームの連携先が露呈する恐れが背景にある。RP に対し、分散リポジトリ等で展開されたメタデータを参照し検証鍵を取得させることで、上記 CP から見て、クレームを発行した「ユーザ」とその連携先である「RP」が紐付くことを回避し、CP-RP Unlinkable[180]も満たす。

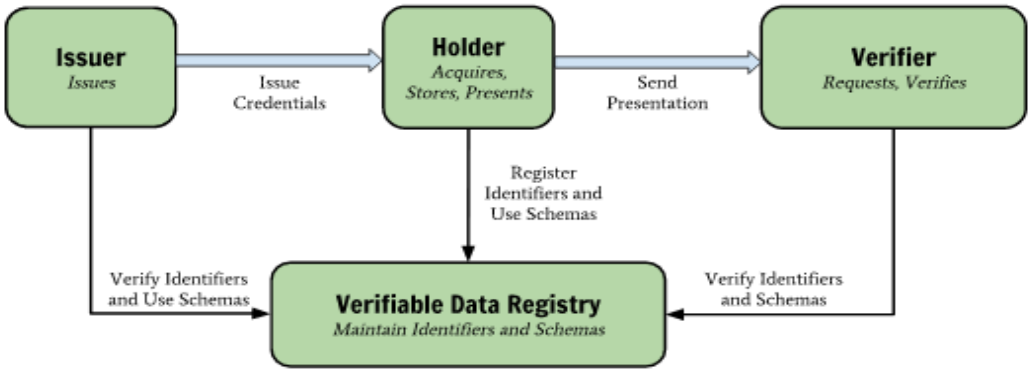


図 0-8：ホルダーを介したクレーム連携概要&RP におけるクレーム検証の仕組み[181]

---

[179] W3C, "Verifiable Credentials Data Model 1.0 - 3.2 Credential, 3.3 Presentations," (November 2019), https://www.w3.org/TR/vc-data-model/

[180] ISO, "Information security, cybersecurity and privacy protection - Requirements for attribute-based unlinkable entity authentication," https://www.iso.org/standard/72018.html

[181] W3C, "Verifiable Credentials Data Model 1.0," (November 2019), https://www.w3.org/TR/vc-data-model/

4.　長期のデジタルアイデンティティの保管・利用

長期のデジタルアイデンティティの保管・利用とは、一度 CP によって発行されウォレットに格納されていたクレームが、CP の状態に関わらず、継続的に利用可能な状態を維持することを意図する。例えば発行元が大学等の場合、統廃合により CP が存在しなくなる可能性がある。その場合でも、過去発行されたクレームが正当な（真正性が保証された）ものであることが確認可能となる。また、仮に CP がクレーム発行後に内容の改ざんを企図したとしても、過去時点で発行されたクレームの真正性検証が可能である。

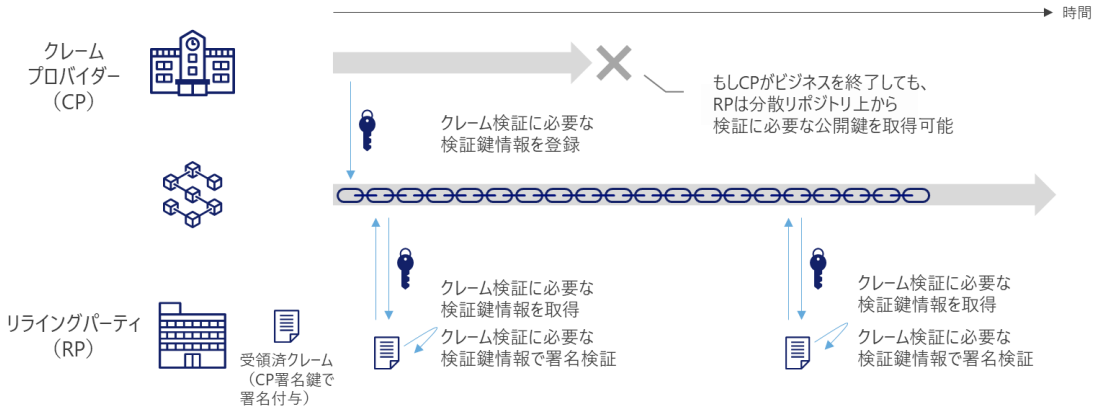


図 0-9：長期のデジタルアイデンティティの保管・利用の概観

3-2. SSI/DID の実現に必要な構成要素

構成要素の整理としては、SSI モデルによる IMS は、現時点で確立した標準が存在しないものの、各標準化団体が提唱するモデルいずれも前述の 4 つの特性が共通的に登場する。本調査では、代表的なユースケースを踏まえつつ、この特性を実現するための処理フローを定義した。

技術面での整理としては、SSI モデル実現方法として、各団体が上述の処理フロー実現のために策定しているプロトコルとその概要の整理を行った。

統制面での整理としては、IMS トラストフレームワークの実務者向けガイドである OIX Guide to Trust Framework を元に、SSI モデルにおいてステークホルダーに求められる役割と、充足すべき統制要件の整理を行った。

3-2-1. SSI/DID の実現に必要な構成要素の整理

3-1-2 で述べたユースケースを対象に、DID の生成およびクレーム連携処理に関する処理フローを定義した。

処理フローは”DID の登録処理”と”クレームの連携処理”の 2 つから構成される。”DID の登録処理”はホルダー[182]が DID の ID Proofing を行い、Activation 処理が完了し、DID が有効状態に遷移するまでの処理を指す。”クレームの連携処理”は、ホルダーが DID を取得後 IdP となり、CP とホルダー間, 及びホルダーと RP 間でのクレーム連携処理を指す。

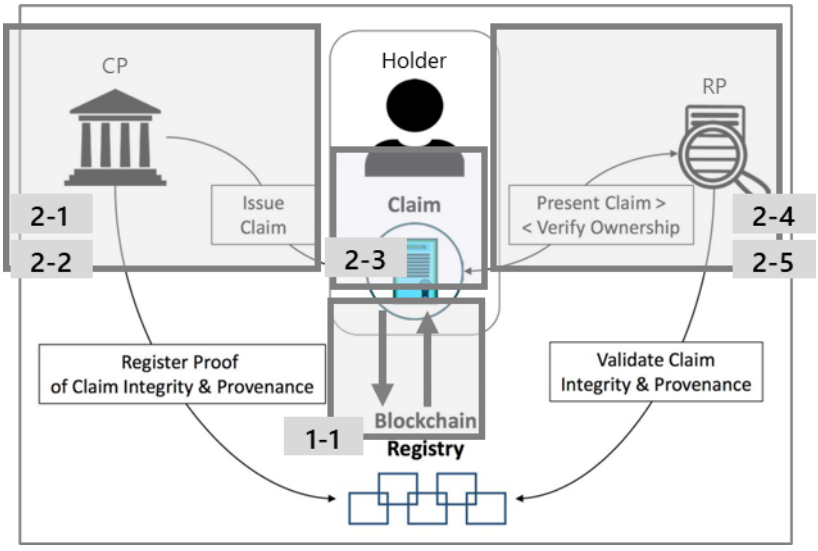


図 0-10：DID の登録処理とクレームの連携処理の概観[183]

[182] 本報告書では SSI/DID においてクレームを授受するユーザの役割をホルダーと表記する。

[183] decentralized-id.com 資料を基に作成

“DID の登録処理”では、ホルダーが自身の DID およびメタデータの生成と登録を行う。また、CP、RP についても、予めそれぞれの DID の生成と登録が完了しているものとする。（1-1）。

“クレームの連携処理”は CP 上のユーザとユーザ自身の DID の Binding 処理（2-1）、クレーム発行（2-2）、ウォレットへのクレーム格納（2-3）、RP に対するユーザ認証[184]（2-4）、そしてクレーム連携の処理（2-5）から構成される。

1. CP 上のユーザと DID の Binding 処理（2-1）では、ユーザが CP 内の Credential Service Provider に対し認証を実行する。CP がユーザから”ユーザの DID を保持・管理していることを示す情報”を受け取り、DID を操作しているエンティティと、CP 上のアカウントを操作しているエンティティが同一であることを確認した上で、Binding する。
2. クレーム発行（2-2）では、CP が Binding で受け取った情報を利用し、クレーム発行要求してきたエンティティ（RP）に対するクレームである点を検証した上で、クレームを発行する。
3. ウォレットへのクレーム格納（2-3）では、クレーム発行で取得したクレームをユーザがウォレットに格納・保持する。
4. RP に対するユーザ認証（2-4）では、ユーザが RP に対し、ユーザの DID の登録処理における DID およびメタデータを用いて認証を行う。
5. クレーム連携の処理（2-5）では、まず RP に対するユーザ認証で対向の認証が完了後、ユーザがウォレットへのクレーム格納で取得したクレームを連携する。そのうえで RP は、受領したクレームが、RP に対するユーザ認証で認証したユーザの DID と Binding され発行されたクレームか（Verification）、および連携されたクレームは有効か（Validation）を検証する。

DID の登録処理での DID およびメタデータ（Authentication Credential 含む）の生成と登録（1-1）では、ユーザは、自身のクレーム連携の為に用いる分散型アイデンティティ（DID）を、RA を介して生成・登録を実施する（①）。そして、従前の IMS と同じく、何らかの ID Proofing を行った上で、DID 及び関連メタデータを生成と登録する。また DID 生成時には、DID の所有者であることを示すために用いられる秘密鍵・公開鍵の鍵ペアも生成される（②）。

[184] 本章では 1 章で定義した「オーセンティケーション」を「認証」と表記する

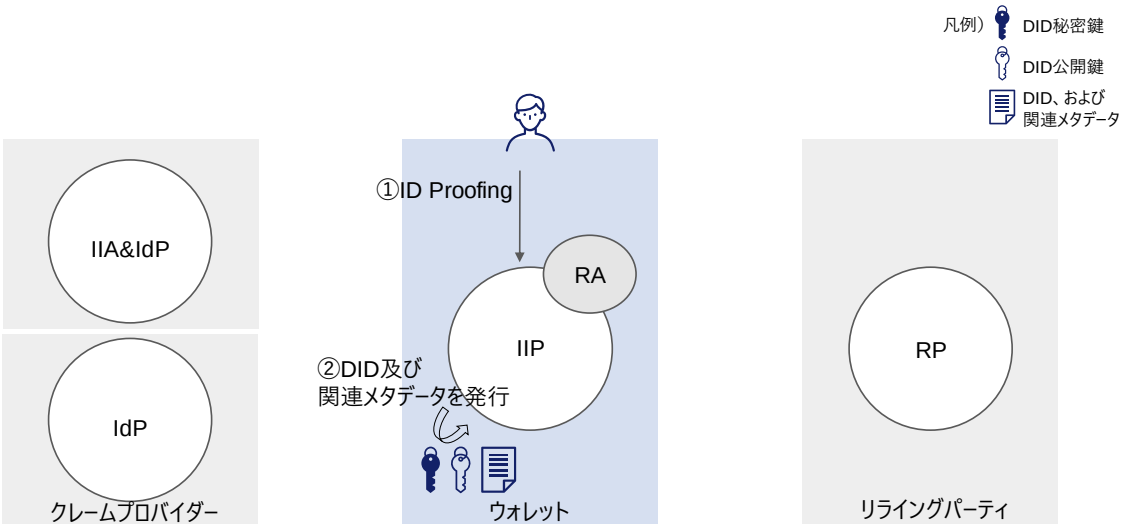


図 0-11：DID の登録処理

CP 上のユーザと DID の Binding 処理（2-1）では、CP が、ユーザから提示された DID 所有者情報と、CP 上にある Active なユーザの Identifier 間の Binding を実施する。

まず、ユーザは、CP の IdP で Authentication を行うとともに（①）、CP に対しクレーム発行要求を行う。その際併せてユーザは ”ユーザの DID を保持・管理していることを示す情報” を提示し、DID 所有者であることを証明する（②）。

その後、CP の IdP は、①，②の結果に問題が無ければ IdP の管理する Identifier とクレーム発行要求をしてきたユーザとの Binding を行う（③）。

なお、Binding における考慮事項については、補論 1 を参照のこと。

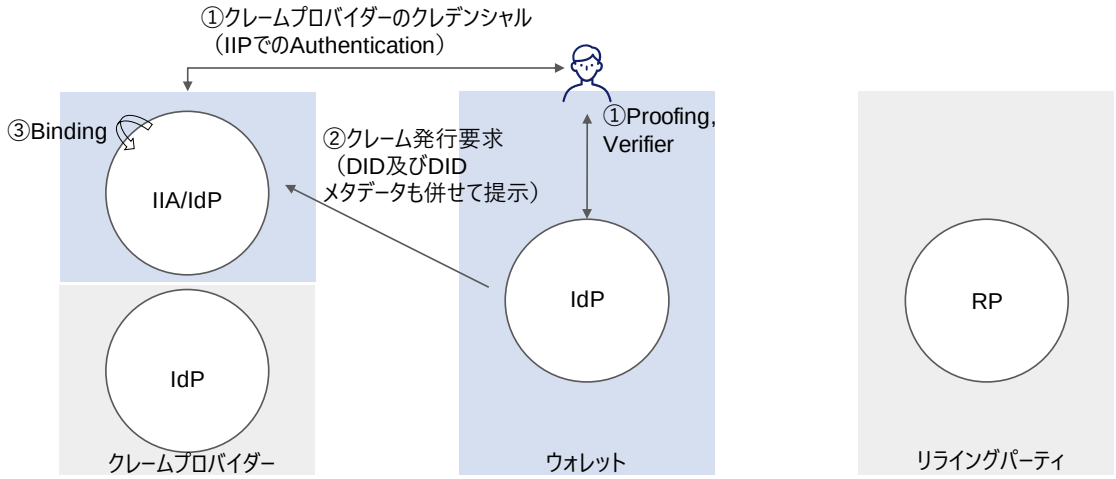


図 0-12： クレームの連携処理（2-1. CP 上のユーザと DID 所有者の Binding）

クレーム発行（2-2）では、Binding 内容を踏まえ、CP は、DID 向けのクレームを発行し、ウォレットに送付する（①）。またその際、下図の様に、複数 IdP からクレームを収集することも有りうる。その際、収集先の IdP は、別に IIA が存在するケースもあれば、IIA と IIP を兼ねるケースも存在する。また、ユーザ自身が属性情報を主張しクレーム（自己証明のクレーム）として発行するケースも存在する（下図クレーム(K)参照）。

その後、ウォレットへのクレーム格納（2-3）では、ユーザは受領したクレームの真正性・有効性検証を行い、ウォレットにクレームを格納する（②）。

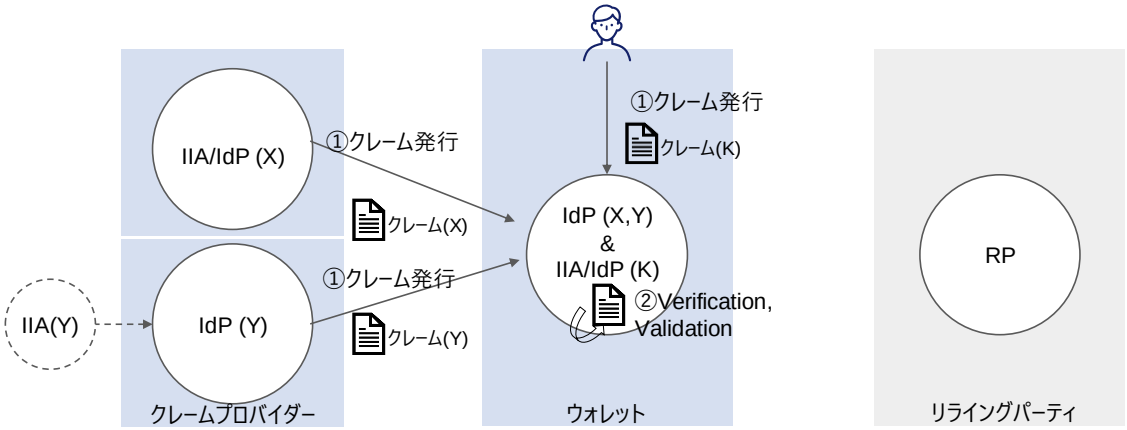


図 0-13：クレームの連携処理（2-2. クレーム発行、2-3.ウォレットへのクレーム格納）

RP に対するユーザ認証（2-4）では、DID と関連メタデータを用い、ウォレットと RP 間でセキュアなチャネルを確立する（③）。対向認証の技術仕様は、各標準化団体が多様な仕様を策定しているが、概して 1-1. で生成した秘密鍵/公開鍵ペアを用いた、公開鍵暗号方式に基づく形を提唱している。クレーム連携の処理（2-5）では、ユーザは保持するクレームから許容したもののみ RP に提示する（③）。RP は、受領したクレームの真正性・有効性検証を行い（④）、問題なければユーザにサービスを提供する。

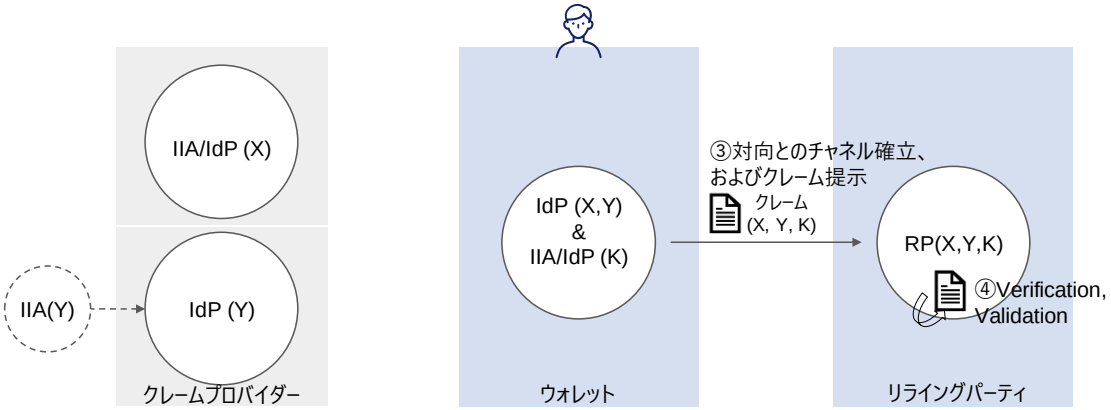


図 0-14：クレームの連携処理（2-4. RP に対するユーザ認証、2-5. クレーム連携）

3-2-2. 技術構成要素に対する各標準化団体の議論動向

前述した DID の登録処理とクレームの連携処理を対象に、各標準化団体の規定している仕様がどこを対象としているかのマッピングは以下の通り。なお、※が付いた仕様は 2021 年 4 月 1 日時点で他仕様との統合や重複などにより今後記載内容が変動することが想定されたため、本調査では詳細の記述を割愛する。

表 0-2：技術構成要素の各標準化団体の検討仕様（2021 年 4 月時点）

#	A) OpenID Foundation	B) W3C/W3C-CCG	C) DIF	D) Sovrin (hyperledger、Linux Foundation)
1-1) DIDおよびメタデータの生成・登録	A-1) OpenID Connect Core (SIOP) OpenID Self Issued Identifiers ※	B-1) Decentralized Identifiers (DIDs) v1.0	B-1) Decentralized Identifiers (DIDs) v1.0 C-1) Self-Issued OpenID Connect Provider DID Profile v0.1	B-1) Decentralized Identifiers (DIDs) v1.0
2-1) クレームプロバイダー上のユーザとDIDのBinding処理	OpenID Connect Credential Provider ※	B-2) Verifiable Credentials Data Model 1.0 BBS+ Signatures 2020 ※	OpenID Connect Credential Provider ※	D-1) Aries RFC 0023: DID Exchange Protocol 1.0 Hyperledger Ursa
2-2) クレーム発行及びウォレットへの送付	A-1) OpenID Connect Core (SIOP)	B-1) Decentralized Identifiers (DIDs) v1.0 vp-request-spec (W3C-CCG) ※	B-1) Decentralized Identifiers (DIDs) v1.0 C-1) Self-Issued OpenID Connect Provider DID Profile v0.1	B-1) Decentralized Identifiers (DIDs) v1.0 D-1) Aries RFC 0023: DID Exchange Protocol 1.0 D-2 Aries RFC 0036: Issue Credential Protocol 1.0
2-3) ウォレットへのクレーム格納	A-3) OpenID Connect Claims Aggregation	B-2) Verifiable Credentials Data Model 1.0 B-1) Decentralized Identifiers (DIDs) v1.0 B-3) Credential Handler API (W3C-CCG)	B-2) Verifiable Credentials Data Model 1.0 B-1) Decentralized Identifiers (DIDs) v1.0	B-2) Verifiable Credentials Data Model 1.0 B-1) Decentralized Identifiers (DIDs) v1.0
2-4) RPに対するユーザ認証	A-1) OpenID Connect Core (SIOP)	B-4) Confidential Storage 0.1 B-1) Decentralized Identifiers (DIDs) v1.0	B-4) Confidential Storage 0.1 B-1) Decentralized Identifiers (DIDs) v1.0	B-1) Decentralized Identifiers (DIDs) v1.0
2-5) クレーム連携	A-1) OpenID Connect Core (SIOP)	B-1) Decentralized Identifiers (DIDs) v1.0 vp-request-spec (W3C-CCG) ※ B-3) Credential Handler API (W3C-CCG)	DID-SIOP ※ B-1) Decentralized Identifiers (DIDs) v1.0 C-1) Self-Issued OpenID Connect Provider DID Profile v0.1 C-2) Presentation Exchange	B-1) Decentralized Identifiers (DIDs) v1.0 D-3) Aries RFC 0037: Present Proof Protocol 1.0

W3C としては DID の実現手段として、Decentralized identifiers（DIDs）と呼ばれる、個人や組織が信用するシステムを使用して自身の識別子を生成し、暗号証明（電子署名、プライバシー保護生体認証プロトコルなど）を使用して当該識別子を認識できるように設計された新しいタイプのグローバルに一意な識別子を用いた、クレームの連携のためのメカニズムを策定している。なお、DIDs についての詳細は後述する。

また、Verifiable Credentials Data Model 1.0 では、Verifiable Credential（VC）、Verifiable Presentation（VP）と呼ばれるクレームのデータモデルを定義しており、ユーザのプロパティを表現する為のデータに関する定義や、VC と VP のライフサイクルモデルが規定されている。

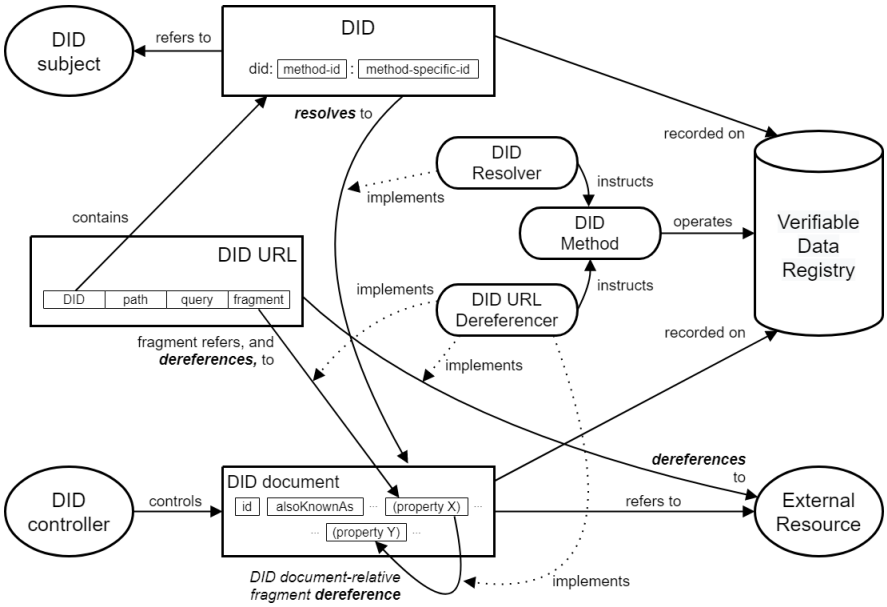


図 0-15：Decentralized Identifiers (DIDs) v1.0[185]

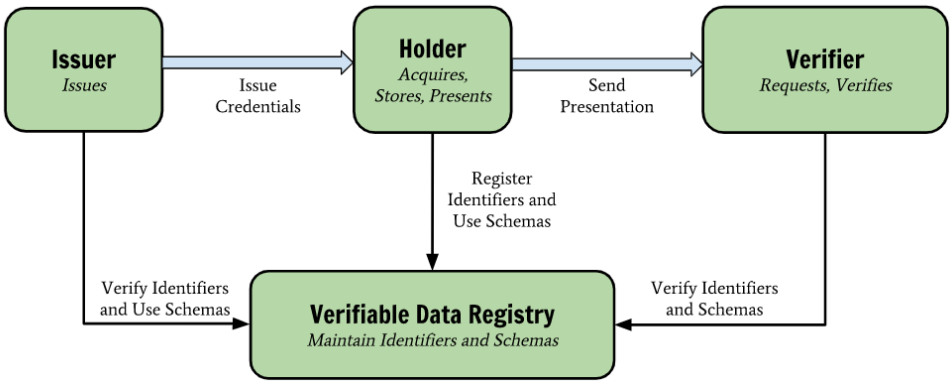


図 0-16：Verifiable Credentials Data Model 1.0[186]

OpenID Foundation は既存仕様の中にある「Self-Issued OpenID Provider」を使い、ユーザが OpenID Provider として機能し Recognition を行った上で、ユーザをハブとするクレームの連携を図る仕様の策定を進めている。クレームのデータモデルについては、W3C の DIDs を包含する形で拡張を検討しており、DID との Binding に関する部分についても、DIF とのリエゾンを締結し、共に議論を進めている。なお、生成される Credentials（クレーム）と DID 間の Binding は、下記の OpenID Connect Credential Provider での①要求時に OpenID Connect Core 1.0 で規定された”Signed Request Object”での実現を想定してい

185 W3C, "Decentralized Identifiers (DIDs) v1.0," (June 2021), https://w3c.github.io/did-core/

186 W3C, "Verifiable Credentials Data Model 1.0," (November 2019), https://www.w3.org/TR/vc-data-model/

る。OpenID Foundation による OpenID Connect Credential Provider での処理の流れは以下の通り。

① Credential Holder（CH）が Credential Issuer（CI）に”Credential” を要求
② CI がエンドユーザを認証し、認可を取得
③ CI が CH に“Credential”を返信
④ Credential Verifier（CV）が CH に”Credential”を要求
⑤ CH がエンドユーザを認証し、認可を取得
⑥ CH が CV に”Credential”を返信

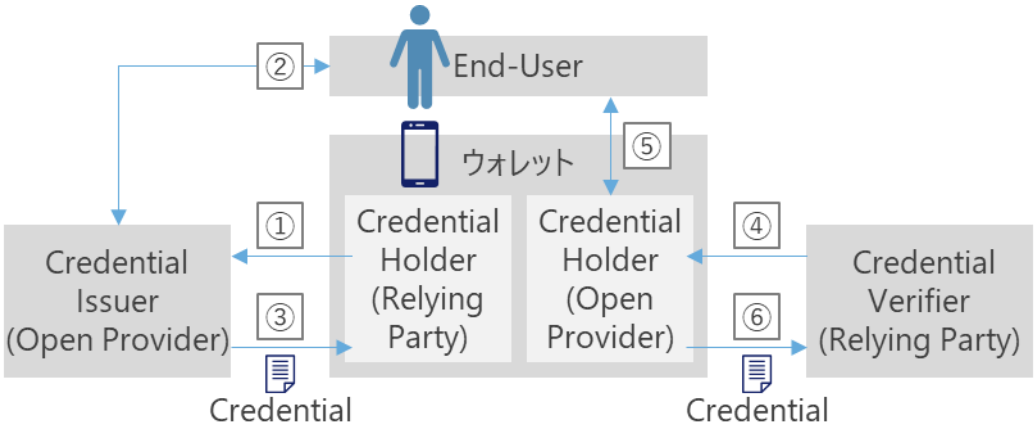


図 0-17：OpenID Connect Claims Aggregation の過程

DIF は当初、ホルダーの概念と、先述の DIDs や OpenID Connect と組み合わせる為の仕様を検討していたが、OpenID Foundation が広範に活用されている点や高い拡張性持っている点などから、2020 年 11 月に OpenID Foundation とリエゾン協定を結び、上記実現のために OpenID Connect を用い仕様拡張する方針とした。他にも複数 Working Group が仕様策定を行っており、一例として、トランスポートプロトコルやクレームのデータフォーマットに依存しない、ホルダーから RP へのクレーム要求や提示が可能な仕様策定も行っている。なお、OpenID Foundation とのリエゾン背景、すなわち OIDC 選択理由としては以下を挙げている[187]。

- 良く知られていて成熟した仕様である
- 広く利用されており、大きなコミュニティが存在する
- OIDC に精通した企業が多く存在している

[187] Oliver Terbu, "Using OpenID Connect with Decentralized Identifiers," (May 2019), https://medium.com/decentralized-identity/using-openid-connect-with-decentralized-identifiers-24733f6fa636

- シンプルかつ軽量である
- 柔軟性及び拡張性がある
- クレデンシャル/クレームの交換をオプションとしてサポートしている
- RWOT や IIW で開発されたものがベースとなっている

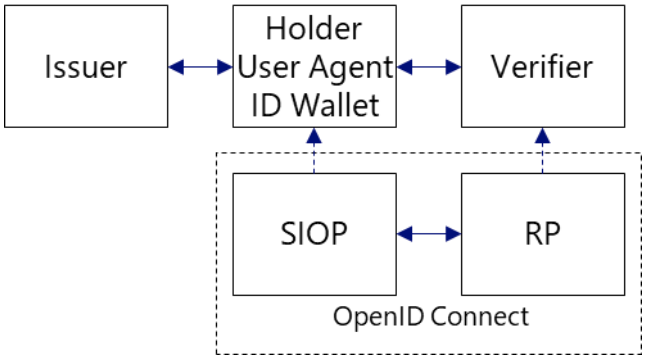


図 0-18：DIF にとっての OpenID Connect

Sovrin Foundation は、SSI モデルの実現に必要な「Sovrin Governance Framework」を規定し、法的協定や用いる技術仕様・標準・ポリシー、同フレームワークのポリシー適合性評価のための基準とプロセス等を定義している。また、同フレームワーク内では、構成スタックとして「Sovrin Stack」と呼ばれる 4 層の Layer を定義している。

規範的なの構成要素として、W3C の DIDs、VC Data Model、DID Method 1.0 Specification が言及されている。また、DID/DID Document 管理の為の分散台帳技術としては、Evernym 社が Sovrin Network の立ち上げとコード提供を行った後、オープンソースプロジェクト「Hyperledger Indy」として展開されている。Hyperledger Indy としては Peer to Peer Connection / Wallet / Messaging / KeyManagement プロトコルを規定した Aries プロジェクト、ZKP の様な暗号機能のための暗号ライブラリ提供を目的とした USRA プロジェクトといった拡張仕様に対しても、Contributor として貢献している。

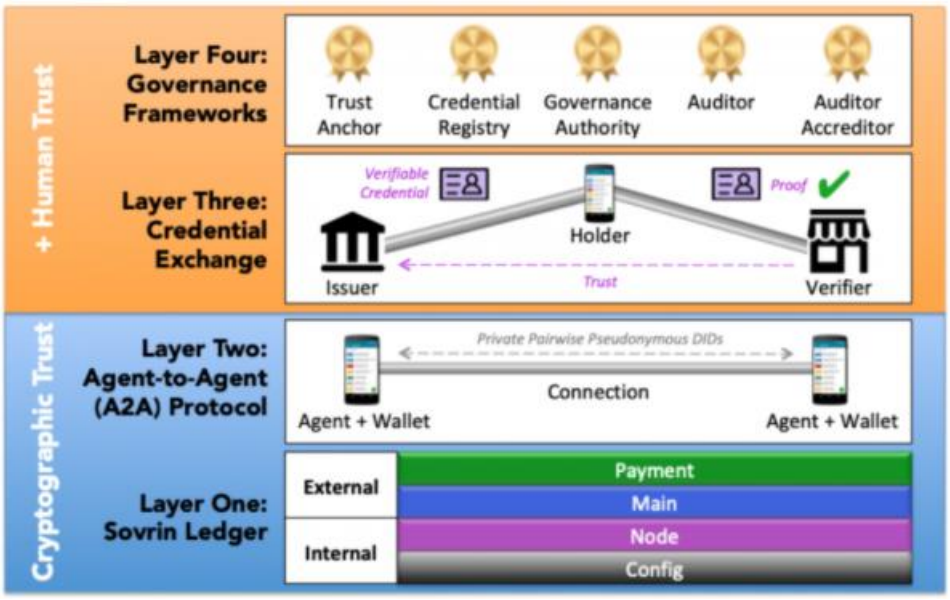


図 0-19：Sovrin Foundation による Sovrin Stack 図[188]

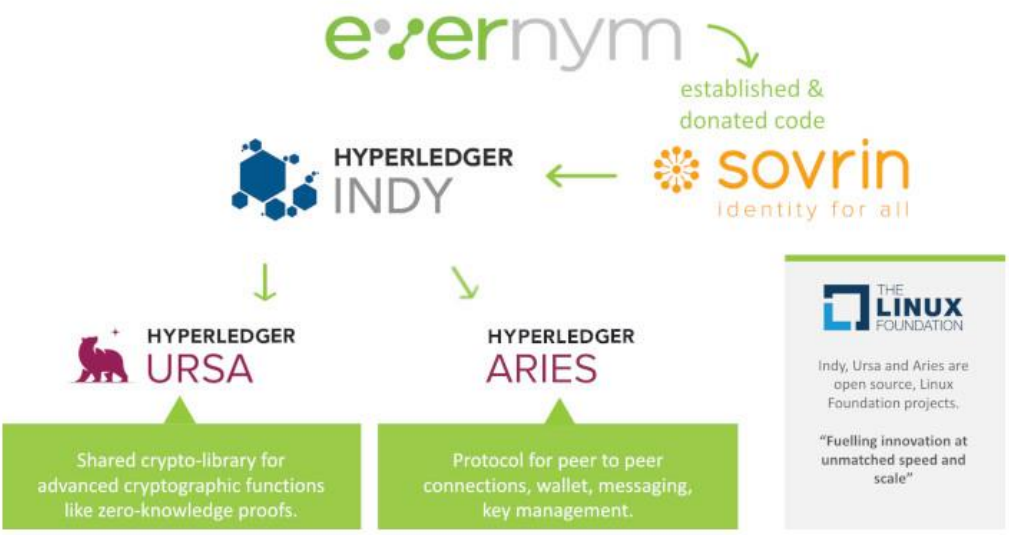


図 0-20：Hyperledger Indy 及び関連プロジェクトの設立経緯 [189]

[188] Sovrin Foundation, "2020 - How SSI Went Mainstream," (January 2021), https://sovrin.org/2020-how-ssi-went-mainstream/

[189] Evernym, "Hyperledger Aries: The Next Major Step Towards Interoperable SSI," (May 2019), https://www.evernym.com/blog/hyperledger-aries/

3-2-3. 各標準化団体の検討仕様

本節では、技術構成要素の検討仕様のうち、以下の仕様の概要についてまとめる。

表 0-3：各標準化団体の検討仕様

#	団体名	仕様名
A-1)	OIDF	OpenID Connect Core
A-2)	OIDF	OpenID Self Issued Identifiers
A-3)	OIDF	OpenID Connect Claims Aggregation
B-1)	W3C	Decentralized Identifiers (DIDs) v1.0
B-2)	W3C	Verifiable Credentials Data Model 1.0
B-3)	W3C	Credential Handler API
B-4)	W3C, DIF	Confidential Storage
B-5)	W3C	JSON-LD
B-6)	IETF	JSON Web Message
C-1)	DIF	Self-Issued OpenID Connect Provider DID Profile v0.1
C-2)	DIF	Presentation Exchange
C-3)	DIF	Key Event Receipt Infrastructure
C-4)	DIF	Sidetree
D-1)	Hyperledger	Aries RFC 0023: DID Exchange Protocol
D-2)	Hyperledger	Aries RFC 0036: Issue Credential Protocol
D-3)	Hyperledger	Aries RFC 0037: Present Proof Protocol
E-1)	Trust over IP Foundation	Trust over IP
F-1)	Evernym	Decentralized Key Management System

（A-1）OpenID Connect Core[190]

OpenID Foundation による OpenID Connect Core の詳細は 1 章で説明済みのため割愛し、同仕様の Chapter 7 で言及されているユーザ自身が ID プロバイダとして振る舞う Self-Issued OpenID Provider（SIOP）という方法について説明する。「SIOP」は、自身が self-hosted な OpenID Provider として振る舞う。SIOP を用いることで、自身が OP として振る舞い、クレームを連携するための Recognition に必要なクレデンシャル管理が可能となる。そして、同方式を用いることで、既存の ID プロバイダへの依存を下げることに繋がり得るため、SSI の思想の実現手段の一つとして、昨今注目されている。

[190] OpenID Foundation, "OpenID Connect Core 1.0 incorporating errata set 1 - 7.Self-Issued OpenID Provider," (November 2014), https://openid.net/specs/openid-connect-core-1_0.html#SelfIssued

（A-2）OpenID Self Issued Identifiers

OpenID Self Issued Identifiers とは OpenID Foundation AB/Connect ワーキンググループにて策定中の、OIDC 環境における self-issued identifiers への対応を定義する仕様である。Self-issued identifiers とは、OpenID Connect Core 1.0 の第 7 章において規定されている、自らホストして自己署名を行った ID トークンを発行する OP による識別子のことを指す

サブジェクト（ユーザ）の識別子について、OpenID Connect 仕様での Key ID はクレームにおける”sub”として定義される。この”sub”は URL（URI）として定義され、DID も含むいかなる形式の URL が許容される。ただし、URL は OIDC の JWT への署名鍵を安全に再発行する方法を提供する必要がある。

クレームの連携先となる RP を選択するための方法の前提として、ユーザがブラウザ経由でアクセスし、その中で認可フローを開始するのが典型的な手法として挙げられている。標準の方法としては OpenID Connect Core 1.0 の第 7 章にて規定されている”openid://”スキーマ以外のスキーマを利用することも認められている。

本仕様では、ユーザは認証手段が用いられなくなったり紛失したりした場合でも識別子を用いてユーザ個人のリソースにアクセスすることを想定している。そのため、ユーザは異なる鍵を有効化して自身のリソースに紐づける必要がある。

また、Signed Claims として、属性やその他のデータは JSON Object Signing and Encryption 形式でまとめて格納されて署名されると規定されている。Signed Claims には General Claims と Client Bound Claims の二種類が規定されている。General Claims は UserAgent が発行する、クライアントやサブジェクトに紐づかない、発行時のセッション情報と言った Claim 等がある。Client Bound Claims は ID トークンをセッショントークンとして用いる場合が想定されており、ユーザエージェントとクライアント間で生成されるか以前のやり取りでキャッシュされた Claim を用いると規定されている。なお、Client Bound Claims の JSON Object Signing and Encryption 形式のヘッダは前述の通り DID を含みうる”sub”を参照し、その”sub”の鍵で署名を行う。他に、ユーザの識別子情報を運ぶための Id トークンは OIDC の ID Token を基にして同トークンの必須項目を全て含み、UserAgent が発行すると規定されている。

本仕様の課題としては、そもそも OpenID Connect Core とは別の仕様にするべきかどうかの議論がなされていることが挙げられる 。また、OpenID Self Issued Identifiers では、ユーザエクスペリエンスの懸念についてもいくつか挙げられている。まず、OIDC が”openid://”スキーマを用いるため、携帯端末でのカスタムスキーム指定時の特定のアプリ立ち上げの機能を用いることが可能で、デスクトップ端末ではブラウザの拡張機能やプラグインによって提供できる。デスクトップ端末でブラウザを利用時に拡張機能が使えない場合は、QR コードの生成については本仕様の対象外のため、QR コードで（SIOP のユ

ーザエージェントへ）遷移させることを検討することが第一に挙げられている。また、カスタムスキームに複数のアプリが登録されている時、Android は開くアプリを選択できるが、iOS は挙動が未定義のため、SIOP 利用に限らないが iOS 端末では SIOP の機能を使わせないといった対応になりうる懸念も上げられている。なお、その場合の緩和策としては専用のアプリを起動させたうえで読み込ませる QR コードを用いるという方法が提示されている。

本仕様では、ユーザが自らのアイデンティティを管理する責任も負うものの、ユーザはセキュリティに関して深く考慮しないことを前提に、どの識別子の発行方法もユーザの管理自体やその回復を助けられるようにすることが重要だとされている。

本仕様では、ユーザ間でのプライベートな情報のやり取りが暗号化されることを必須としている。

（A-3）OpenID Connect Claims Aggregation[191]

OpenID Connect Claims Aggregation とは、OpenID Foundation Connect WG にて策定中の、複数の CP から OpenID Connect クライアントへアグリゲート（集約）されたクレームを提供するための処理方法の仕様である。この仕様によって、ユーザは単一の OpenID Connect Provider（OP）に複数のクレームを集約させて、様々な RP に個別ではなくまとめてクレームを提供させることができるようになる。

OpenID Connect Claims Aggregation において OP は、大元のクレームを発行する CP に対してはクライアントとして登録し、必要なユーザ情報に対して OIDC 認証リクエストを行うことにより、 RP としての役割を果たすことでクレームを受け取り、集約して要求元のクライアント（RP）にまとめたクレームを提供する。具体的な流れとしては以下の通り。

① OP が CP を検出する。なお、本仕様は OpenID Connect Discovery 1.0 にて規定されている CP からのレスポンスに、署名されたクレームを提供する URL を示す claims_endpoint が必須の、JWS での署名や JWE での暗号化のアルゴリズムを任意のメタデータとして追加されることを規定している。
さらに、OIDC for Identity Assurance に対応している場合は、OIDC for Identity Assurance の 7 節で規定されているように対応機能を提示することも必須である。

② OP が CP にクライアントとして登録される。
本仕様では OpenID Connect Dynamic Client Registration 1.0 での Dynamic Registration 等で行われることを挙げている。

③ CP への認証リクエストを、PKCE と共に OpenID Connect Code Authorization Flow に沿って出す。

---

[191] OpenID Foundation, "OpenID Connect Claims Aggregation,"
https://bitbucket.org/openid/connect/src/master/openid-connect-claims-aggregation/openid-connect-claims-aggregation-1_0.md

④ CP からクレームを取得する。
⑤ OP から要求元の RP に集約されたクレームを返す。
⑥ RP は集約されたクレームの有効性を検証（Validate）する。
1. 集約されたクレームが暗号化されている場合には、RP が OP と予め定めた鍵とアルゴリズムで復号する。
2. CP の発行者識別子が含まれる iss（issuer）Claim はクライアントが信頼しているものであることを確認する。
3. uid の値はクライアントの公開署名鍵のフィンガープリントを base64url でエンコードされたものであることが必須である。
4. クライアントは、iss（issuer）Claim に発行者にて登録されている cliend_id の値が、aud（audience）Claim にオーディエンスとして含まれることを検証（validate）することが必須である。なお、aud（audience）Claim には複数の要素を配列に含むこともできる。また、集約された Claims にクライアントが有効なオーディエンスとして記載されていない場合か、クライアントによって信頼されていない追加のオーディエンスが記載されている場合は当該の集約されたクレームを拒否することが必須である。
5. クライアントは集約されたクレームの署名を JWT の alg ヘッダーパラメータで指定されたアルゴリズムを用いて JWS に従って検証（validate）し、その際には集約されたクレームの発行者（OP）が提供した鍵を用いることが必須である。

OP はユーザのすべてのクレームの情報を一元化して収集できるため、 CP と RP が直接クレームをやり取りする必要がなく、ユーザは OP を介して取得したクレーム情報を他の RP に共有させることが出来る。

（B-1）Decentralized Identifiers (DIDs)[192]

DID v1.0 は、個人や組織が信用するシステムを使用して自身の識別子を生成し、暗号証明（電子署名、プライバシー保護生体認証プロトコルなど）を使用して当該識別子を認識できるように設計された新しいタイプのグローバルに一意な識別子を用いた、クレームの連携のためのメカニズムを策定する仕様である。同仕様の中で、分散型アイデンティティファイア（DID）と呼ばれる個人や組織が信用するシステムを使用して自身の識別子を生成し暗号証明（電子署名、プライバシー保護生体認証プロトコルなど）を使用して認証可能となるグローバルに一意な識別子が規定されている。

フェデレーションモデルで用いられる識別子とは対照的に、DIDs は中央集権型の登録機関、ID プロバイダ、認証局から分離されるように設計されている。一つの DID（a DID）は、任意の subject（人、組織、モノ、データモデル等）と関連づけることができる。また、

[192] W3C, "Decentralized Identifiers (DIDs) v1.0," (June 2021), https://w3c.github.io/did-core/

DID Controller は特定 IdP からの許可を必要とせずに DID の制御（DID Document の作成、更新、非アクティブ化)可能であることを証明できる。DID は DID subject と DID Document を関連付けた URIs であり、その subject と関連した信頼できるやり取りを可能とする。

DID Document は DID subject を記述するデータセットで、暗号化ツール、検証方法、サービスエンドポイントを示すことができ、DID subject がデータモデルのような情報リソースの場合には、DID subject 自体を含むことがある。

DID の作成者は、信頼するコンピューティングインフラ(Verifiable Data Registries)上で動作する特定タイプの DID を設計できる。特定タイプの DID の仕様は DID method と呼ばれる。DID を使用したアプリケーションやシステムの作成者は、特定のユースケースに最も適した DID method をサポートできる。DID resolver は DID を入力として受け取り、DID Documents を出力するソフトウェア、ハードウェアコンポーネントである。(図 0-15 を参照)。

DID パラメータは、DID Method から完全に独立しており、すべての DID に対して同じように機能する。オプションのパラメータがサポートされている場合、それらは、サポートしている DID Method 全体で一様に動作することが期待される。

表 0-4：DID パラメーター一覧

パラメータ名	サポート	説明
relative-ref	必須	サービスエンドポイントのリソースを識別する相対 URL 参照は、service パラメータを使って DID Document から選ばれる
service	必須	service ID によって DID Document からサービスを識別する
version-id	任意	DID Document の特定バージョンを識別する
version-time	任意	DID Document の特定バージョンのタイムスタンプを識別する
hl	任意	完全性を保護するための DID Document のリソースハッシュ

入力メタデータを DID resolver に渡すことで同じ機能を表現できる場合には、DID パラメータは使用しないことが予想される。

また、DID URL は標準的な DID 構文の拡張により、特定のリソースを配置する標準的な URI 構成要素(path, query, fragment)を組み込む。DID path/ query は一般的な URI と同一である。DID fragment は、DID Document または外部リソースへの参照として method から独立した形で使用される

DID URL の一部である DID パラメータは，どのようなリソースが識別されるかを指定するために使用されるべきであるのに対し，DID URL の一部ではない入力メタデータは，そのリソースがどのように解決されるか，あるいは参照を解除されるかを制御するために使用される

相対 DID URL は、DID Document 内の did:<method-name>:<method-specific-id> で始まらない URL 値である。URL の内容は、通常、同じ DID Document 内のリソースを参照する。相対 DID URL は，必要以上に冗長になりがちな絶対 URL を使用することなく，DID Document 内の検証方法やサービスを識別するために使用される。

DID Document の最上位レベルのコアプロパティは次の通り。

表 0-5：DID Document のコアプロパティのパラメータ

パラメータ名	サポート	説明
id	必須	DID subject は DID Document の最上位にある id プロパティで表現される
alsoKnownAs	任意	DID subject は異なる目的または異なる時刻に複数の識別子を持つことができる。2 つ以上の DID が同じ DID subject を識別するために alsoKnownAs プロパティを使用できる
controller	任意	DID Document に DID controller を示すプロパティを含めてもよい
verificationMethod	任意	DID subject または関係者とのやりとりの認証/認可に使用されるプロパティ。本プロパティには、id, type, controller,特定の検証方法を示すプロパティを含まなければならない。検証方法に使用できる公開鍵には、RSA, ed25519, secp256k1, Curve25519, JWK がある。例えば、verificationMethod が公開鍵の場合、鍵の身元を示す本プロパティの controller は、上述の DID controller であるとは限らない
authentication	任意	DID subject の認証方法を指定する(埋め込み、または参照可)。DID controller の認証には、controller の値

		に関連付けられたエンティティの DID Document authentication プロパティを用いる必要がある
assertionMethod	任意	Verifiable Credential 発行のように、DID subject のクレーム表現方法を指定する
keyAgreement	任意	受信者との間で安全な通信チャネルを確立するなど、DID subject への情報の暗号化方法を指定する
capabilityInvocation	任意	HTTP API への認可など、DID subject が暗号化特性を呼び出す際に使用できる仕組みを指定する
capabilityDelegation	任意	HTTP API への認可を委譲するなど、DID subject が暗号化特性を他の相手に委譲する際に使用できる仕組みを指定する
service	任意	サービスへのポインタを指定する。本プロパティには、id, type, serviceEndpoint プロパティを含まなければならない

DID Document では、JSON、JSON-LD、および CBOR 用の構文が提供されるが、XML や YAML 形式のデータモデルを使用してもよい。Producers はドキュメントのメタデータにてメディアタイプを介してどの表現が使用されたかを示さなければならない。Consumers は DID Document の内容のみではなく content-type フィールドを介して DID Document の表現を決定しなければならない。

表 0-6：DID Document でのデータモデル

表現	説明
JSON	JavaScript Object Notation の略、resolver のメタデータでは、content-type は application/did+json と表現される
JSON-LD	JSON for Linking Data の略、resolver のメタデータでは、application/did+ld+json と表現される
CBOR	Concise Binary Object Representation の略、JSON 互換でサイズをより小さくエンコードすることで処理性能を向上できる

DID Method は、異なる Verifiable Data Registries で本仕様の実装手段を提供する。DID method の仕様は、正確に 1 つのメソッド名(method-specific-id)で識別され、メソッド固有の DID スキームを定義しなければならない。DID Method の割り当てや承認を管理する中央機関が存在しないため、特定メソッドの一意性を確実に知る方法はないが、DID Methods

Registry に非公認リストが維持されているため、新規 DID メソッド仕様の実装者は自身のメソッド名をそこに追加することが推奨される。

DID Document 上で実行可能な操作について、操作する当事者の権限はメソッド固有のものである。例えば、DID Method は次のような認可の実装方法を定義しなければならない。

- controller プロパティを使用
- 更新/非活性操作の認可に authentication プロパティ配下の verification methods を使用
- DID Document の他の構造を、例えば、DID Document 更新に capabilityInvocation で指定した verification method を使用
- DID Document を使用せずにメソッドに組み込まれたルールを使用

また、DID メソッド仕様には次のような操作が規定されている。

表 0-7：DID メソッド仕様での操作

操作	概要
Create	DID controller が verifiable data registry 上の DID およびそれに関連する DID Document を作成する方法
Read/Verify	DID resolver が DID を使用して verifiable data registry から DID Document を要求する方法
Update	DID controller が verifiable data registry 上の DID ドキュメントを更新する方法
Deactivate	DID controller が verifiable data registry 上の DID を非アクティブ化する方法、または非アクティブ化が不可能であることを宣言する方法

DID resolution は、適用される DID Method の "Read "操作を使用して DID を DID Document に解決する。

```
resolve ( did, did-resolution-input-metadata )
     -> ( did-resolution-metadata, did-document, did-document-metadata )

resolveRepresentation ( did, did-resolution-input-metadata )
     -> ( did-resolution-metadata, did-document-stream, did-document-metadata )
```

図 0-21：DID resolution の例[193]

DID URL 間接参照機能は、DID URL を、DID メソッド、メソッド固有識別子、パス、クエリ、フラグメントなど、DID URL の構成要素に応じた内容を持つリソースに参照する。

```
dereference ( did-url, did-url-dereferencing-input-metadata )
        -> ( did-url-dereferencing-metadata, content-stream, content-metadata )
```

図 0-22：dereference の例[194]

DID resolver は、少なくとも 1 つの DID Method 用の DID 解決関数を実装すること、および少なくとも 1 つの適合表現(JSON/ JSON-LD/ CBOR など)で DID Document を応答する関数を実装しなければならない。

セキュリティ考慮事項は次の通り。

表 0-8：DIDs のセキュリティ考慮事項

考慮事項	概要
DID Resolver の選択	DID Method Registry は、DID Method 名とそれに対応する DID Method 仕様のリストである。実装者は、特定の DID Method 名と対応する DID Method 仕様を義務付ける中央機関が存在しないことを考慮する必要がある。DID Resolver が DID Method を正しく実装しているか疑問がある場合、DID Specification Registry から十分な情報を得たうえでどの DID Resolver の実装を使用するか決定することができる。
DID および DID Document の証明	自己署名された DID Document 上で検証された署名は DID のコントロールを証明するものではなく、DID Document がタイムスタンプを付与されてから改ざんされていないこと、タイムスタンプが生成された時点で DID controller が署名に使われた秘密鍵をコントロールしていたことを証明するだけである。
公開鍵のコントロールの証明	DID Document の公開鍵に対応する秘密鍵のコントロールを証明する方法には、静的な方法と動的な方法がある。

[193] W3C, "Decentralized Identifiers (DIDs) v1.0 - 8.1 DID Resolution," (January 2021), https://www.w3.org/TR/2021/WD-did-core-20210131/#did-resolution

[194] W3C, "Decentralized Identifiers (DIDs) v1.0 - 8.2 DID URL Dereferencing," (January 2021), https://www.w3.org/TR/2021/WD-did-core-20210131/#did-url-dereferencing

	静的な方法は、DID Document を秘密鍵で署名する方法であり、DID Document が登録された時点の秘密鍵のコントロールを証明する。もし DID Document が署名されていない場合には、DID Document に記述された公開鍵のコントロールは動的に証明する必要がある。
認証と Verifiable Claims	DID および DID Document は、本質的に PII（個人を特定できる情報）を持たない。DID を実世界、例えば、DID と同じ subject を持つクレデンシャルを用いて人や会社などにバインディングするプロセスは、この仕様の範囲外である。
認証サービスのエンドポイント	DID Document が、DID subject の認証または認可を目的としたサービスエンドポイントを公開している場合、そのサービスエンドポイントでサポートされている認証プロトコルの要件を遵守することは、サービスエンドポイントの提供者、対象者、または要求する当事者の責任である。
否認の禁止	DID および DID Document 更新の否認を禁止することは、対象が不正な更新を監視していること、DID method のアクセス制御機構に従って悪意ある更新をもとに戻せることを想定してサポートされる。
DID Document の変更通知	DID Document への不正な変更に対する一つの緩和策は、変更時に DID subject を監視し、積極的に通知することである。これは、メールアドレスにパスワードリセット通知を送信することによって、従来のユーザ名／パスワードのアカウント乗っ取りを防止することをサポートすることに類似している。DID の場合、このような通知を生成する仲介レジストラやアカウントプロバイダーは存在しないが、DID が登録されている Verifiable Data Registry が直接変更通知をサポートしている場合、サブスクリプションサービスを DID controller に提供することができる。DID controller がサードパーティの監視サービス頼る場合、別の攻撃のベクトルを組み込むことになる。
鍵および署名の有効期限	分散型アイデンティティアーキテクチャでは、鍵または署名の有効期限切れポリシーを強制する中央機関は存在しない。DID resolver と当事者は、鍵が使用された時点で有効期限が切れていないことを検証する必要がある。
鍵の失効と復旧	暗号鍵失効の発生を定義するのは DID method に任されている。さらに、DID method の仕様は、鍵の回復を可能にするための信頼されたパーティの定足数のサポートを可能にすることも期待され

	ている。DID method 仕様におけるアクセス制御および鍵復旧は、第二の復旧手順を保持することによって鍵の危殆化から保護するタイムロック機能を含めることもできる。
Human-Friendly な識別子の役割	Human-Friendly な識別子を DID にマッピングする(そして、検証され、信頼される方法でそれを行う)問題は、この仕様の範囲外である。
不変性	不変性がサイバーセキュリティ上の利点をもたらすという考え方は、特にキャッシングに関連する。グローバルな真のソースに結び付いた DID method では、DID Document の最新バージョンを常に検索可能である。しかしキャッシュレイヤーが存在する場合、オブジェクトの属性が実際には異なっているのに実際に存在すると信じてしまい悪用される可能性がある。
DID Document 内の暗号化データ	DID Document のすべてまたは一部を暗号化することは、長期的にデータを保護する適切な手段ではない。同様に、暗号化データを DID Document に配置することは、個人を特定できる情報を含む適切な手段ではない。この点から、暗号化データが DID Document に含まれる場合、実装者は、DID との関連付けを望まないエンティティの公開鍵で暗号化しないことが大切である。

プライバシー考慮事項は次の通り。

表 0-9：DIDs のプライバシー考慮事項

考慮事項	概要
個人を特定できる情報（PII）を非公開にする	DID メソッド仕様が、すべての DID と DID Document が公開されている public verifiable data registry のために書かれている場合、DID Document には個人データが含まれないことが重要である。すべての個人データは、DID subject の管理下にあるサービスエンドポイントの後ろに保管されるべきである。個人データは、ＤＩＤ Document 内の公開鍵記述によって識別され、かつ安全に保護された通信チャネルを使用して、プライベートな P2P で交換できる。また、個人データが不変の分散型台帳に書き込まれないため、DID subject や依頼者は GDPR の忘れられる権利を実行できる。
DID の相関リスクと別名 DID	DID は相関関係に使用されるかもしれないため、DID controller は、対となるユニークな DID を使用することで、このプライバシーリスクを軽減できる。各 DID は別名として機能する。

DID Document の相関リスク	別名 DID の相関防止保護は、対応する DID Document 内のデータを相関させることができれば容易に打ち破られる。例えば、複数の DID Document で同じ公開鍵記述または独自サービスエンドポイントを使用することは、同一 DID の使用と同程度の相関情報が提供される。エンドポイントプライバシーのためのより良い戦略としては、多くの異なる subject によって数千、数百万のＤＩＤでエンドポイントを共有することが考えられる。
subject へのタイプの割り当て	DID subject のタイプおよび性質を、明示的、あるいは推論によって示すために使用できるプロパティを DID Document に追加することは危険である。そのようなプロパティは、個人を特定できる情報や相関可能なデータが DID Document 内に存在するだけでなく、特定の操作や機能性に含まれたり除外されたりするような方法で特定の DID をグループ化するために使用できる。これらのリスクを最小化するために、DID Document 内のすべてのプロパティは、DID の使用に関連する暗号材料、エンドポイント、または検証方法を表現するためのものであるべきである。
プライバシー群	DID subject が群の中で他と区別がつかない場合、プライバシーを利用できる。デジタルフィンガープリントを減らすためには、要求側の実装で共通設定を共有し、有線プロトコルでネゴシエートされたオプションを最小限に抑え、暗号化されたトランスポートレイヤーを使用し、メッセージを標準的な長さにパディングする。

（B-2）Verifiable Credentials Data Model[195]

Verifiable Credential は暗号学的に検証可能な作成者を持ち、改ざんや盗み見がわかる(tamper-evident)エンティティの属性集合であり、Verifiable Credentials Data Model は暗号的に安全で、プライバシーを尊重し、machine-readable な方法で、Web 上で Verifiable Credential を表現するためのメカニズムを提供する仕様である。例えば、学歴資格、医療データ、金融口座、およびその他の第三者が検証した machine-readable な各種個人情報を Web 上で表現することを可能にする。

Verifiable Credential Data Model のエコシステムにおけるコアアクターの役割とその関係性について説明する。

表 0-10：Verifiable Credentials Data Model のエコシステムでの役割

[195] W3C, "Verifiable Credentials Data Model 1.0," (November 2019), https://www.w3.org/TR/vc-data-model/

役割	概要
Holder	1 つ以上の verifiable credential を保有し、それらから verifiable presentation を生成するエンティティが担う役割 例：学生、従業員、顧客
Issuer	1 つ以上の subject に関するクレームから作成した Verifiable Credential を Holder に送信するエンティティが担う役割 例：企業、非営利団体、業界団体、政府、個人
Subject	生成されるクレームのエンティティ 例：人、動物、物 多くの場合、Verifiable Credential の Holder が Subject であるが、親（Holder）が子供（Subject）の Verifiable Credential を所持することや飼い主（Holder）がペット(Subject)の Verifiable Credential を所持することもある
Verifier	1 つ以上の Verifiable Credential を受信するエンティティが担う役割 オプションとして Verifiable Presentation 内で受信することもある 例：雇用者、セキュリティ担当者、ウェブサイト
Verifiable Data Registry	識別子、鍵、Verifiable Credential スキーマ、失効登録、Issuer 公開鍵など、Verifiable Credential の使用に必要なその他関連データの作成と検証を仲介するシステムが担う役割 例：信頼されたデータベース、分散型データベース、政府 ID データベース、分散型台帳

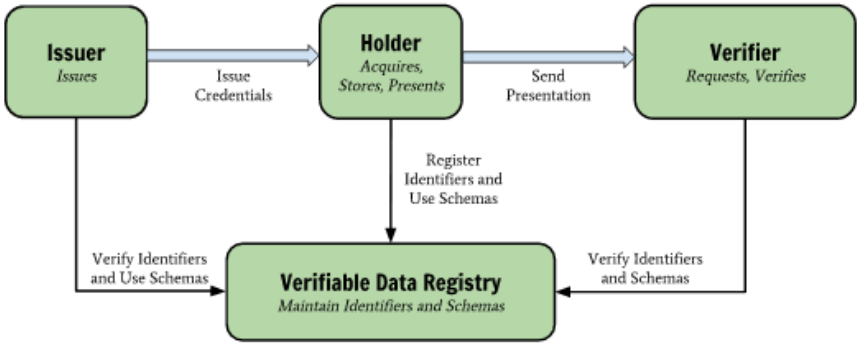


Figure 1 The roles and information flows forming the basis for this specification.

図 0-23：Verifiable Credentials Data Model1.0 の外観像

Verifiable Credential は暗号でその発行を証明する改ざん防止可能な(tamper-evident)クレームとメタデータのセットである。Verifiable Credential の例として、デジタル従業員証、デジタル出生証明書、デジタル学歴証明書がある。

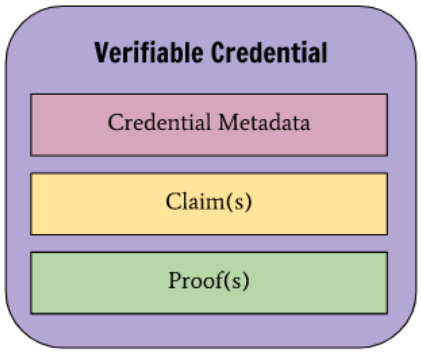


Figure 5 Basic components of a verifiable credential.

図 0-24：Verifiable Credential の構成要素

Verifiable Presentation は 1 つ以上の Verifiable Credential から表現されるデータであり、データの作成者を検証可能にする。Verifiable Credential の Holder は Verifiable Presentation を生成して Verifier に共有することで Verifiable Credential の所持を証明することができる。

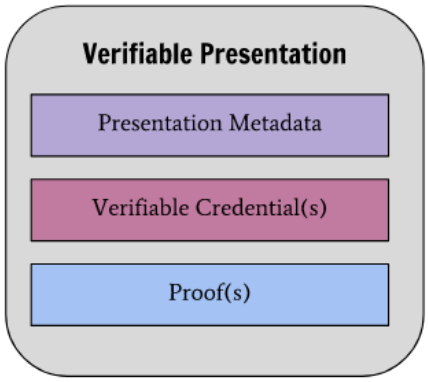


Figure 7 Basic components of a verifiable presentation.

図 0-25：Verifiable Presentation の構成要素

この仕様では、Verifiable Credential または Verifiable Presentation の転送プロトコルは定義されていないが、他の仕様でエンティティ間の転送方法を規定している場合には、この Verifiable Credential データモデルを適用できる。また、この仕様では、認証フレームワークは定義されていない。Holder、Verifiable Credential の Issuer、Verifiable Credential の内容、およびその独自ポリシーを考慮にいれて、Verifiable Credential または Verifiable Presentation 検証後に Verifier が行う事項も定義していない。

Verifiable Credential の信頼モデルは次のとおりである。

- Verifier は受け取ったクレデンシャルを発行した Issuer を信頼する。この信頼構築のために、クレデンシャルには、Issuer がクレデンシャルを生成した Proof(つまり Verifiable Credential)が含まれる必要がある。もしくは、Issuer が Verifiable Credential を生成したこと、かつ、Verifiable Credential が転送または保管時に改ざんされていないことを明確に証明する方法で送信される必要がある(Verifier のリスクアセスメントによっては、この信頼は弱まる可能性がある)
- すべてのエンティティは Verifiable Data Registry が改竄を防止しどのデータがどのエンティティによって管理されているかを記録していることを信頼する
- Holder および Verifier は、Issuer が Subject について正当なクレデンシャルを発行し適切な時に素早く失効することを信頼する
- Holder は、Repository がクレデンシャルを安全に保管し、Holder 以外には公開せず、保管中に破損、紛失しないことを信頼する

セキュリティ考慮事項は次の通り。

表 0-11：Verifiable Credentials Data Model のセキュリティ考慮事項

考慮事項	概要
暗号スイートとライブラリ	暗号スイートとライブラリには使用期限があり、最終的には新たな攻撃や技術の進歩にさらされることになる。本番システムは、このことを考慮に入れ、暗号スイートやライブラリの簡単かつ積極的にアップグレード、既存クレデンシャルの無効化や更新の仕組みを確認する必要がある。クレデンシャルを処理するシステムの長期的な実行可能性を確保するためには、定期的な監視が重要である。
コンテンツの完全性の保護	Verifiable credential には外部データへの URL が含まれることが多い。Verifiable credential 外に存在するリンク先のコンテンツは、Verifiable Credential の証明の保護から外れるため、改竄から保護されていないことが多い。コンテンツへのリンクの完全性を保護したい場合は、コンテンツの完全性を強制する URL スキームを使用することが推奨される。
未署名のクレーム	この仕様では、いかなる種類の署名または証明も含まないクレデンシャルを生成することができる。これらのタイプのクレデンシャルは、中間ストレージ、または自己主張された情報に有用であることが多く、これは Web ページのフォームに記入することに似ている。実装者は、これらのタイプのクレデンシャルが、作成者不

	明、もしくは信頼できないため、検証ができないことに注意が必要である。
トークンバインディング	Verifier は、自身が Verifiable Presentation の意図された受信者であり、 中間者攻撃のターゲットではないことを確認する必要がある。トークンバインディング(Token Binding [RFC8471])のようなアプローチは、Verifiable Presentation のリクエストと応答を結びつけることでプロトコルを安全にできる。
プライバシー群	このシステムでは、暗号化できないフィールドがいくつかある。例えば、データに関連付けられたバージョン番号から、データの更新頻度を知ることができる。暗号化されたコンテンツに関連付けられた識別子により、サーバは document 間で識別子を関連付けることで知識を得ることができます。実装では、暗号化なしで保存される情報量を最小限に抑えることが推奨される。
依存クレームのバインディング	Issuer がクレデンシャル内の情報を細分化する、または選択的な開示を可能にする署名スキームを使用することはベストプラクティスである。細分化の場合、Issuer によって安全に行われなければ、Holder が Issuer が意図していない方法で異なるクレデンシャルを束ねる可能性がある。
動的な情報	Verifiable Credential が動的な情報に対して発行される場合、実装者は有効期限が適切に設定されていることを確認する必要がある。Verifiable Credential の有効期間は、Verifiable Credential に含まれる情報に対するユースケースおよび予想される有効期間に応じた適切な期限を設定することが重要である。
デバイスの窃盗となりすまし	Verifiable Credential がデバイスに保存されており、そのデバイスが紛失または盗難にあった場合、攻撃者が被害者の Verifiable Credential を使用してシステムにアクセスできる可能性がある。この種の攻撃を緩和する方法としては、以下のようなものがある。 ・デバイスでパスワード、PIN、パターン、または生体認証による画面ロック解除保護を有効にする ・Credential Repository でパスワード、生体または多要素認証を有効にする ・暗号鍵にアクセスするときにパスワード、生体または多要素認証を有効にする ・別のハードウェアベースの署名デバイスを使用する ・上記のすべてまたは任意の組み合わせをとる

プライバシー考慮事項は次の通り。

表 0-12：Verifiable Credentials Data Model のプライバシー考慮事項

考慮事項	概要
個人を特定できる情報	Verifiable Credential に含まれる一部のデータは Verifier と共有されるときプライバシー侵害の影響を受ける可能性がある。政府発行の識別子、配送先住所、およびフルネームなどの個人を特定できるデータは、エンティティの決定、追跡、および関連付けに使用できる。生年月日と郵便番号などの個人を特定できないと思われる情報であっても、組み合わせによって強力な相関性を持つ。このような特性を持つデータを共有する際には、Holder に警告することが強く推奨される。また、Issuer は、可能な限り、プライバシー保護する Verifiable Credential を提供することを強く推奨する。
識別子ベースの相関関係	Verifiable Credentials の Subject 識別子は、長期間、複数 Web ドメインにまたがって使用されると相関関係のリスクが増加する。
シグネチャーベースの相関関係	この仕様では、いかなる種類の署名または証明も含まないクレデンシャルを生成することができる。これらのタイプのクレデンシャルは、中間ストレージ、または自己主張された情報に有用であることが多く、これは Web ページのフォームに記入することに似ている。実装者は、これらのタイプのクレデンシャルが、作成者不明、もしくは信頼できないため、検証ができないことに注意が必要である。
永続的なの識別子ベースの相関関係	Verifiable Credential には、個人を関連付けるために永続的に使用可能な能識別子が含まれることがある。Holder にソフトウェアを提供する組織はこれらの情報が共有されたときに Holder に警告することが求められる。
依存クレームのバインディング	Issuer がクレデンシャル内の情報を細分化する、または選択的な開示を可能にする署名スキームを使用することは、 ベストプラクティスであると考えられる。細分化の場合、Issuer によって安全に行われなければ、Holder は Issuer が意図していない方法で異なるクレデンシャルを束ねることがある。
デバイス・フィンガープリント	インターネットおよび Web 上の個人を追跡、関連づける外部メカニズムが存在する。Internet protocol (IP) address tracking, web browser fingerprinting がある。Verifiable Credential を使用してもこれらの追跡技術は防止できない。Verifiable Credential と一緒に

	使用することで新たな相関関係が生まれる可能性がある。プライバシーを尊重するシステムでは、Verifiable Credential が使用されている場合には、これらの追跡技術を使用しないことが推奨される。
抽象クレーム	Verifiable Credential の受信者は、取引に必要以上の PII を明らかにすることがないよう、Issuer は必要最小限なセットに制限することを検討すべきである。クレデンシャルに PII を入れないように、subject に関する具体的な情報を提供せず Verifier のニーズを満たす抽象プロパティを使用する。
データ最小化の原則	プライバシー侵害を防止するためのベストプラクティスとして、要求された情報、および受信した情報を必要最小限に制限することが認められている。Verifiable Credential では、Issuer にとってのデータ最小化は Verifier が使用する必要最低限のデータに限定することである。また、Verifier にとってのデータ最小化はサービスアクセス時に要求される情報の範囲を制限することである。Verifier は特定の取引が発生に必要な情報のみを要求することが求められる。
Bearer Credential	Bearer Credential は、コンサートチケットのようなプライバシーを強化する情報であり、Bearer Credential の Holder には、Holder の機密情報を漏らすことなく特定のリソー スを利用する権利が与えられる。Bearer Credential は、その共有が大きな経済損失やレピュテーション低下を招かない低リスクケースで使用されることが多い。複数のサイトで同じ Bearer Credential を繰り返し使用すると、これらのサイトが結託して Holder を不正に追跡したり、相関関係を持たせたりする可能性がある。Bearer Credential の Issuer は、Bearer Credential が単一使用、個人特定情報を含まないこと、過度に相関性がないことを確実にしなければならない。
妥当性のチェック	Verifiable Credential の処理時に、Verifier は以下のような有効性チェックが期待される ・Holder の専門職免許のステータス ・ライセンスの更新日又は失効日 ・個人の下位資格 ・Holder と Holder が交流しようとしている事業体間の関係 ・Holder に関連する地理的位置情報 これらのチェックプロセスにより、Holder のプライバシー侵害につながる情報漏洩が発生する可能性がある。例えば、失効リストを

	チェックするような単純な操作では、特定の事業者が Holder と対話しようとしている可能性が高いことを Issuer に通知することができます。これにより、Issuer が知識なしで結託して個人を関連付けできる可能性がある。Issuer は、クレデンシャルごとに固有の失効リストのような、プライバシー侵害につながる可能性のあるメカニズムを検証プロセス中に使用しないことが求められる。
ストレージプロバイダーとデータマイニング	Holder が Issuer から受け取る Verifiable Credential はどこかに保存する必要がある（例えば、Credential Repository）。Verifiable Credential 内の情報は本質的に機密性が高いことから、Holder はデータマイニングの対象となることがある。Verifiable Credential の無料保存を謳うサービスは、実際には個人データをマイニングして、人や組織別プロファイルを構築したい組織に販売している可能性がある。データマイニングおよびプロファイリングのための効果的な緩和策には、以下のものがある。 ・顧客情報を第三者に販売しないサービスプロバイダ ・サービスプロバイダがクレデンシャルの内容を表示できないように verifiable credential を暗号化するソフトウェア ・顧客管理デバイスに verifiable credential をローカル保存し想定外に顧客情報をアップロード、分析しないソフトウェア
クレデンシャルの集約	Verifiable Credential の集約はプライバシーリスクであり、エコシステムすべての参加者はデータ集約のリスクを認識する必要がある。例えば、2 つの Bearer Credentials（1 つはメールアドレス、もう 1 つは Holder が 21 歳以上であることを示す）が複数のセッションに渡って提供された場合、Verifier は、その個人の年齢関連情報だけでなく、一意の識別子を持つようになる。これにより Holder のプロファイリングが容易になり、時間の経過とともに多くの情報が漏洩する。また、クレデンシャルの集約は、複数のサイト間で互いに結託して行われた場合、プライバシー侵害につながる可能性がある。解決策は、技術的なものではなく、ポリシー的な傾向がある。Holder が自分の情報が集約されることを望まない場合、Holder は自身が送信する Verifiable Presentation の中でその旨を表現しなければならない。
利用パターン	プライバシー保証に努力しても、実際に Verifiable Credential を使用すると、匿名化が解除されてプライバシーが失われる可能性がある。同じ Verifiable Credential が、同じ Verifier に複数回提示されると、Verifier は Holder が同一だと推測できる。同じ Verifiable

	Credential が異なる Verifier に提示されると、それらの Verifier が結託するか、第三者が両 Verifier の取引記録にアクセスできる。また、第三者は、Verifiable Credential を提示した個人が両サービスで同一人物であると推測できる。つまり、アカウントは同一人物によって管理されていることがわかる。
誤った相手との情報共有	Holder が Verifier と情報共有を選択した場合、Verifier が悪意を持って、Holder に危害を加えるような情報を要求する場合がある。例えば、Verifier が Holder や銀行からだまし取るために銀行口座番号を要求し、他の情報とともに使用される可能性がある。Issuer は、Holder が誤った Verifier にクレデンシャルを送信した場合においても被害が拡大しないよう、可能な限り多くの情報を直接ではなく トークン化して含めるべきである。
クレームの発行頻度	利用パターンは特定の種類の動作に相関させることができる。この相関関係の一部は、Holder が Issuer の知識がない Verifiable Credential を使用すると緩和される。しかし、Issuer は、Verifiable Credential を短期間で自動更新することで、この保護を無効にできる。Holder にソフトウェアを提供する組織は、Holder が有効期限の短いクレデンシャルを繰り返し使用すると、行動の相関が生じる可能性がある場合には、Holder に警告する必要がある。Issuer は、使用パターンを相関させるような方法でクレデンシャルを発行することを避けるべきである。
シングルユースのクレデンシャル	プライバシーを尊重するシステムでは、Verifier とのやりとりに必要な情報のみを Holder が開示することを要求する。Verifier は、開示要求が満たされたことを記録し、開示された機密情報は破棄する。しかし、規制上の負担や長期保存識別子がそれを妨げている場合がある。Verifiable Credential エコシステムの設計では、可能な限り 1 回のみ利用される Verifiable Credential を優先することで、プライバシーを尊重する努力が必要である。
プライベートブラウジング	理想的なプライベートブラウジングでは、PII が明らかにされることはない。ブラウザベンダごとにプライベートブラウジングの扱いが異なり、ブラウザによってはこの機能が全くない場合もある。多くのクレデンシャルには PII が含まれているため、プライベートブラウジングモードでクレデンシャルやプレゼンテーションを使用したい場合、この情報が明らかになる可能性があることを警告する必要がある。

（B-3）Credential Handler API[196]

Credential Handler はクレデンシャルの要求と保存のイベントを処理するためのイベントハンドラであり、Credential Handler API は、ユーザが信頼できるサードパーティの Web アプリケーションをクレデンシャルリクエストおよびクレデンシャルストレージのハンドラーとして指定できるようにする API である。

ホルダーが User Agent としてブラウザを利用する際、Issuer からの CredentialStoreEvent または、Verifier からの CredentialRequestEvent を処理するイベントハンドラとして機能する。

Credential Repository はユーザに代わってクレデンシャルの要求と保存を処理できる Web アプリケーションである。この仕様は、Credential Request と Credential Storage を処理するための新しい Web プラットフォーム機能を定義する。

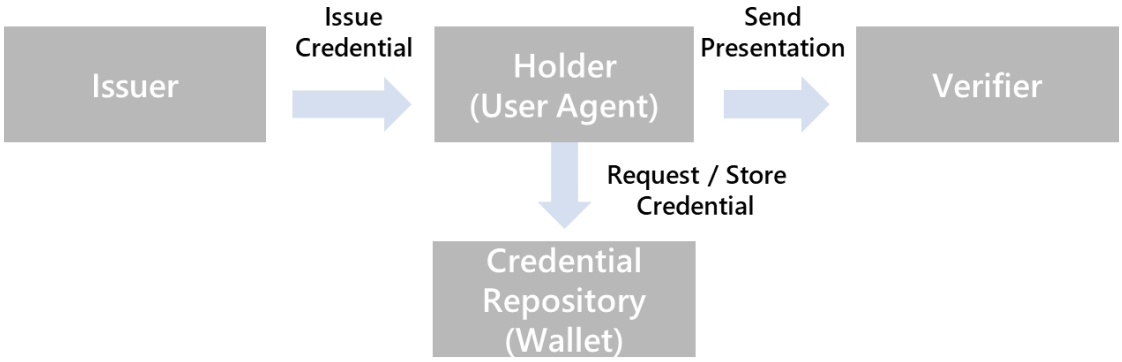


図 0-26：CHAPI の全体像[197]

Credential Request について、次のフローが想定されている。

1. オリジンは、サポートされているクレデンシャルタイプのセットのためのクレデンシャルリクエストとストレージのために、ユーザに許可を要求する。例としては、デジタルウォレットプロバイダーサイトを訪れたユーザは、そのオリジンから Credential Handler を登録するように促される。
2. Credential Handler は Service Worker コードで定義される。
3. Service Worker の登録時に、CredentialManager を使用して以下をセットする
   （ア）有効な WebCredential タイプのリスト
   （イ）ハンドラーが特定の WebCredential タイプをサポートする条件
   （ウ）Credential Handler によってサポートされる hints の表示に使用される情報

[196] W3C, "Credential Handler API 1.0," (March 2021), https://w3c-ccg.github.io/credential-handler-api/

[197] W3C, "Credential Handler API 1.0," (March 2021), https://w3c-ccg.github.io/credential-handler-api/

4. Credential Handler との対話には、2 つのエントリポイントがある。Relying Pary (Verifier) が Credential Management Level1 の get() メソッドを WebCredentialRequestOptions を指定して呼び出す場合と、Issuer が Credential Management Level 1 の store()メソッドを呼び出す場合の 2 つである。これらの両方のケースでは、User Agent は、Relying Party によって受け入れられた WebCredential タイプを、登録された Credential Handler によってサポートされたものと比較しながら、候補となるクレデンシャルヒントのリストを割り出す。
5. User Agent はユーザに対し、登録された Credential Handler の候補の hints を選択肢として表示する。User Agent は登録時に提供された情報（ラベルやアイコン)、ウェブアプリから利用可能な情報を使用してこれらの選択肢を表示する。
6. ユーザが hint を選択すると、User Agent は、hint が登録されている Service Worker の Credential Management で CredentialRequestEvent または CredentialStoreEvent を発行する。CredentialRequestEvent には、クレデンシャルタイプ固有のオプションを含む CredentialRequestOptions およびオリジンや選択されたヒントなどの追加情報が含まれる。
7. CredentialRequestEvent または CredentialStoreEvent が有効化されると、Credential Handler は Credential Request または Credential Storage を処理するために必要なステップを実行し、適切な WebCredential を Relying Party または Issuer に返す。ユーザとの対話が必要な場合、Credential Handler は、その目的のために context-specific なウィンドウを開くことができる。
8. User Agent は、Credential Handler がリクエストの処理を終了すると、非同期的に応答を受け取る。応答は WebCredential またはリクエストが拒否された場合は NULL である。

本仕様のセキュリティならびにプライバシーの観点における課題は以下の通り

- User Environment に関する情報
  Credential Handler API はユーザの登録済み Credential Handler に関する情報を共有しない。オリジンからの情報は、ユーザの同意がある場合のみ Relying Party と共有されるべきである
- クレデンシャル送信前のユーザの同意
  この仕様の目標の一つは、クレデンシャルを送信するために必要なユーザの操作を最小限にすることである。一方で、User Agent は、ユーザの同意なしに Web サイトを呼び出してクレデンシャルを要求し、それをサイレントに受け取ることを可能にする構成を許可してはならない
- 安全な通信
  Credential Handler は Service Worker コードで定義されており、Service Worker の

Security Consideration[198]についての考慮が必要となる。
また、WebCredential セキュリティはこの仕様の範囲外であり、それらの管理をサポートする Credential Handler によって対処される必要がある

- Credential Repository の信頼性
  User Agent は、セキュリティの問題を引き起こす Credential Handler を利用不可としてよい。セキュリティ上の理由で Credential Handler が利用できない場合、User Agent は Credential Handler の開発者に（コンソールやメッセージを通じて）根拠を提供するべきであり、混乱を避けるためにユーザに通知することもできる。
- データ検証
  Relying Party は Credential Management API を通じて受信した WebCredential データが期待通りであることを検証する必要がある
- プライベートブラウジングモード
  Credential Management API が”private browsing mode”で起動された場合、User Agent は、プライベートコンテキストで Credential Handler を起動する必要がある。これにより、一般的に、サイトが以前に保存された情報にアクセスするのを防ぐことができる。
  また、ユーザがオリジンにログインするか、詳細を再入力する必要がある

（B-4）Confidential Storage[199]

Confidential Storage では、暗号化された分散型データストレージのためのプライバシー保護プロトコルを設計することが可能であり、幅広い実用的なアピールができることが期待されている。

下図は、コンポーネントの種類とその役割を示している。Encrypted Data Vault は、低レベルの暗号化ストレージの役割を果たす。

198 W3C, "Service Workers 1 - 6.Security Considerations," (November 2019), https://www.w3.org/TR/service-workers-1/#security-considerations

199 W3C, "Confidential Storage 0.1," (April 2021), https://identity.foundation/confidential-storage/

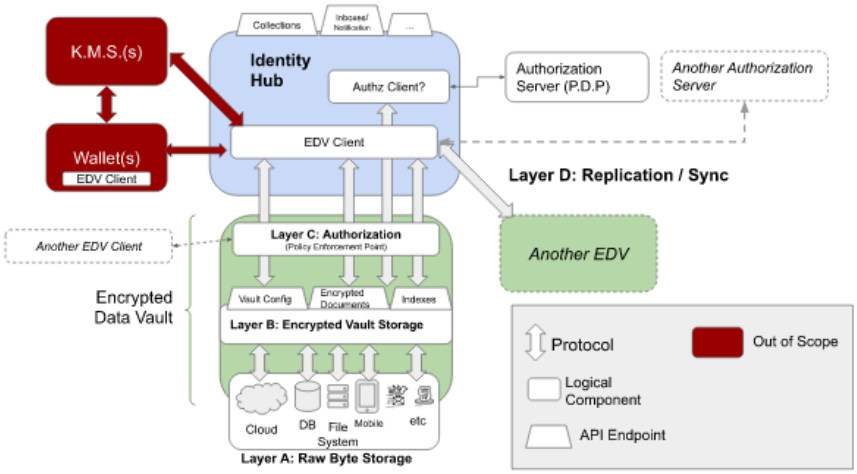


Figure 1 Confidential Storage layers

図 0-27：Confidential Storage のエコシステム概要[200]

表 0-13：Confidential Storage のエコシステムでの役割

役割	説明
data vault controller	data vault の作成、管理、削除によってエンティティが実行する役割。このエンティティは、管理下の data vault に対して、ストレージエージェントへの権限付与や取り消しする責任がある。
storage agent	data vault 内のデータ作成、更新、および削除することにより、エンティティが実行する可能性のある役割。このエンティティは、通常、data vault controller によって data vault にアクセスするための権限が付与される。
storage provider	エンティティが data vault controller に raw data storage mechanism を提供することで実行する役割。保管時および storage provider 間の転送中にデータは暗号化されているので、エンティティはデータを見ることはできない。

要件は以下の通り。

表 0-14：Confidential Storage の要件

要件	概観

[200] W3C, "Confidential Storage 0.1 - 1.2 Ecosystem Overview ," (April 2021), https://identity.foundation/confidential-storage/#ecosystem-overview

Privacy and multi-party encryption	エンティティのデータのプライバシーを確保して、storage provider を含む無認可パーティがアクセスできないよう、データ転送中（ネットワーク上）と保管中（ストレージ上）の両方で暗号化されている必要がある。データは複数のエンティティと共有される可能性があるため、暗号化メカニズムが複数のパーティへのデータ暗号化をサポートすることも必要である。
Sharing and authorization	システムは、1 つの必須の認証スキームを指定するだけでなく、他の代替認証スキームを許可することが期待されている。
Identifiers	システムは識別子に依存しないものでなければいけなく、一般的には、URN や URL の形をした識別子が好ましい。
Versioning and replication	情報の継続的バックアップが求められる。システムは少なくとも 1 つの mandatory versioning strategy と mandatory replication strategy をサポートすることが必要であるが、他の alternate versioning strategy と replication strategies も可能にすることが求められる。
Metadata and searching	本システムを利用して大量のデータを保存し、効率的かつ選択的に検索することが求められる。そのためには、暗号化された検索機構が必要である。クライアントがデータにメタデータを関連付けて検索できるようにすることが重要である。
Protocols	このシステムは様々な動作環境に常駐することができるので、少なくとも 1 つのプロトコルが必須であるが、他のプロトコルも設計によって許可されていることが重要である。

セキュリティ考慮事項は次の通り。

表 0-15：Confidential Storage のセキュリティ考慮事項

考慮事項	説明
Malicious or accidental modification of data	サービスプロバイダは Encrypted Data Vault 内のデータを読み取ることはできないが、サービスプロバイダが暗号化データを削除、追加、変更することは可能である。暗号化データの削除、追加、変更は、data vault 内のデータのグローバルマニフェストを保持することで防げる。
Compromised vault	Encrypted Data Vault は、data controller(復号鍵と適切な認証情報を保持しているエンティティ）が誤って攻撃者にアクセスを許可した場合に危殆化する可能性がある。例えば、被害者が誤って攻撃者に vault 全体へのアクセスを許可したり、暗号化キーを誤操作したりす

	る可能性がある。攻撃者がシステムにアクセスできると、vault の構成を変更、削除、変更できる。
Data access timing attacks	通常、サーバがエンティティの身元や、そのエンティティが Encrypted Data Vault にアクセスする目的を特定することは困難であるが、エンティティが Encrypted Data Vault にアクセスした際に漏洩するアクセスパターンや大まかなファイルサイズ、その他の情報に関連するメタデータは常に存在する。
Encrypted data on public networks	すべての暗号化方式が最終的には破られると仮定することは、データを保護する際の安全な仮定である。サーバが暗号化されたデータを保存するためのストレージ戦略として、いかなる種類の public storage network も使用することは推奨しない。
Unencrypted data on server	このシステムでは、暗号化できないフィールドがいくつかある。例えば、データに関連付けられたバージョン番号から、データの更新頻度を知ることができる。暗号化されたコンテンツに関連付けられた識別子により、サーバは document 間で識別子を関連付けることで知識を得ることができます。実装では、暗号化なしで保存される情報量を最小限に抑えることが推奨される。
Partial matching on encrypted indexes	暗号化されたテキストフィールドの部分一致やスカラー範囲の検索など、暗号化されたインデックスでは利用できない、検索システムでは一般的な操作がある。これらの機能は、将来的にはゼロ知識暗号化スキームを使用して追加されるかもしれない。
Threat model for malicious service provider	悪意のあるサービスプロバイダによる以下の攻撃が考えられる。 ・vault 内の情報にアクセスしているエンティティの相関関係 ・ファイルサイズやアクセスパターンに応じて、vault に保管されているファイルの種類についての推測 ・暗号化されたデータの追加・削除・変更 ・暗号化されたデータに設定された認証ポリシーを実行しない ・暗号化されたデータを未知の外部システムに流出させる

（B-5） JSON-LD[201]

JSON-LD 1.1 は、Linked Data をシリアライズするための JSON ベースのフォーマットを定義した仕様である。この構文は、すでに JSON を使用しているシステムに容易に統合できるように設計されており、JSON から JSON-LD へのスムーズなアップグレードパスを提供する。主に、Web ベースのプログラミング環境で Linked Data を使用することで相互

[201] W3C, "JSON-LD 1.1," (July 2020), https://www.w3.org/TR/json-ld11/

運用可能な Web サービスを構築し、Linked Data を JSON ベースのストレージに格納する方法を意図している。JSON-LD は JSON と互換性があるため、現在利用可能な多数の JSON Parser やライブラリを再利用することができる。

Linked Data は、異なるドキュメントや Web サイト間で標準的なデータのネットワークを作成する方法の一つである。これにより、アプリケーションは Linked Data の 1 つの部分から始まり、Web 上の異なるサイトでホストされている Linked Data の他の部分へ埋め込まれたリンクを辿ることができる。

JSON-LD は、JSON が提供するすべての機能に加えて、以下の機能を導入している。

- IRIs（Internationalized Resource Identifiers）を使用した JSON オブジェクトのための普遍的な識別子メカニズム
- 異なる JSON ドキュメント間で共有されているキーをコンテキスト（JSON-LD ドキュメントを解釈するための一連のルール）を介して IRIs にマッピングすることでキーの曖昧性を解消する方法
- JSON オブジェクトの値が Web 上の別のサイトのリソースを参照するメカニズム
- 文字列にその言語で注釈を付ける機能
- データ型と日付や時刻などの値を関連付ける方法
- ソーシャルネットワークなどの 1 つ以上の有向グラフを 1 つの文書で表現するための機能。

JSON は軽量で言語に依存しないデータ交換フォーマットである。JSON のデータには他のデータソースと競合するキーが含まれている可能性があるため、異なるソースからの JSON を統合することは困難である。さらに、JSON には、Web 上の基本的な構成要素であるハイパーリンクのサポートが組み込まれていない。**図 0-28** において、name は”Manu Sporny”という人の名前であり、”homepage”はその人のホームページが含まれていることは人間にとっては明らかである。しかし、機械はこのような直観的な理解を持っておらず、人間であってもこのような表現の曖昧さを解決することが難しい場合がある。

図 0-28：サンプル JSON ドキュメント A[202]

[202] W3C, "JSON-LD 1.1 - 3.Basic Concepts," (July 2020), https://www.w3.org/TR/json-ld11/#basic-concepts

Linked Data および一般的な Web では、曖昧性のない識別のために IRIs を使用している。IRIs を使用することで、他の開発者が使用する可能性のあるデータに曖昧性のない識別子を割り当て,その用語が何を意味するのかの定義を得ることができる。このプロセスは IRI dereferencing として知られている。

図 0-29 はすべてのプロパティが IRIs で明確に識別され、@id キーワードで明示的にマークされている。これは、非常に具体的な JSON-LD ドキュメントだが、人間の開発者にとっては冗長で作業が困難な状態である。この問題に対処するために**図 0-30** のようにコンテキストの概念を導入している。

```
{
  "http://schema.org/name": "Manu Sporny",
  "http://schema.org/url": {
    "@id": "http://manu.sporny.org/"
    ↑ The '@id' keyword means 'This value is an identifier that is an IRI'
  },
  "http://schema.org/image": {
    "@id": "http://manu.sporny.org/images/manu.png"
  }
}
```

図 0-29：サンプル JSON-LD ドキュメント B[203]

context は terms を IRIs にマッピングするために使用される。context は JSON-LD ドキュメントに直接埋め込むか、URL を使用して参照することができる。

[203] W3C, "JSON-LD 1.1 - 3.Basic Concepts," (July 2020), https://www.w3.org/TR/json-ld11/#basic-concepts

```
{
  "@context": {
    "name": "http://schema.org/name",
    ↑ This means that 'name' is shorthand for 'http://schema.org/name'
    "image": {
      "@id": "http://schema.org/image",
      ↑ This means that 'image' is shorthand for 'http://schema.org/image'
      "@type": "@id"
      ↑ This means that a string value associated with 'image'
        should be interpreted as an identifier that is an IRI
    },
    "homepage": {
      "@id": "http://schema.org/url",
      ↑ This means that 'homepage' is shorthand for 'http://schema.org/url'
      "@type": "@id"
      ↑ This means that a string value associated with 'homepage'
        should be interpreted as an identifier that is an IRI
    }
  }
}
```

図 0-30：JSON-LD Example Context[204]

セキュリティの観点における課題は以下の通り。

- JSON-LD は JSON がベースとなっているフォーマットであるため RFC 8259 The JavaScript Object Notation (JSON) Data Interchange Format セクション 12 についての考慮が必要になる
- JSON-LD は有向グラフのための純粋なデータ交換フォーマットであることを意図しているため、JavaScript の eval()のようなコード実行機構に渡されて解析されるべきではない
- JSON-LD ドキュメントを処理する際には、リモートコンテキストやフレームへのリンクが自動的に追従し、ユーザがそれぞれのファイルに対して明示的に要求しなくてもファイルが転送される。リモートコンテキストが第三者によって提供されている場合、第三者が利用パターンや同様の情報を収集してプライバシーの問題につながる可能性がある
- HTTP のような安全でない接続を介して Web からロードされる JSON-LD コンテキストは、攻撃者によって改竄されるリスクがある。ミッションクリティカルな目的でリモートコンテキストを利用するアプリケーションは、リモートコンテキストを使用できるようにする前に、リモートコンテキストを調査し、キャッシュすることを推奨する

[204] W3C, "JSON-LD 1.1 - 3.Basic Concepts," (July 2020), https://www.w3.org/TR/json-ld11/#basic-concepts

- JSON-LD は長い IRIs を短い文字列に置き換えることができるため、JSON-LD ドキュメントが処理された際、結果として得られるデータが受信者のリソースをすべて消費する可能性がある
- JSON-LD は使用できる IRIs スキームに制限を設けておらず、vocabulary-relative IRIs は IRIs の解決ではなく文字列の連結を使用しているため、参照を逸脱した場合、悪意のある IRIs を構築される可能性がある
- 将来的にキャッシュおよび取得されたコンテンツがリモートのサーバから取得されたデータと一致することを保証する手段として SRI（Subresource Integrity）が組み込まれる可能性がある

プライバシーの観点における課題は以下の通り。

- 外部コンテキストの取得は JSON-LD プロセッサの動作を公開し、中間ノードが取得したリソースのイントロスペクションを通じてクライアントアプリケーションをフィンガープリントすることを可能にし、中間者攻撃の機会を提供することになる。これを防ぐためには、パブリッシャはリモートコンテキストをキャッシュすることを検討するか、documentLoder を使用してそのようなコンテキストのローカルバージョンを維持するべきである

（B-6）JSON Web Message[205]

JSON Web Message（JWM）はアプリケーションレベルのメッセージを JSON エンコードして、様々なトランスポートプロトコル上にて転送する。JWM は実装を容易にするため、すでに広く使用されている JOSE family を拡張して安全なメッセージングシステムの基盤を提供する仕様である。

JWM は RFC7516 JSON Web Encryption（JWE）で完全性及び機密性を実現し、RFC 7515 JSON Web Signature（JWS）でメッセージを否認可能なデジタル署名と関連付けることが可能である。JWM は様々な送信者及び受信者に対応するために利用可能な署名・暗号アルゴリズムの種類が多いという点において JSON Web Token（JWT）と異なる。

[205] Internet Engineering Task Force, "JSON Web Message," (January 2020), https://tools.ietf.org/id/draft-looker-jwm-01.html

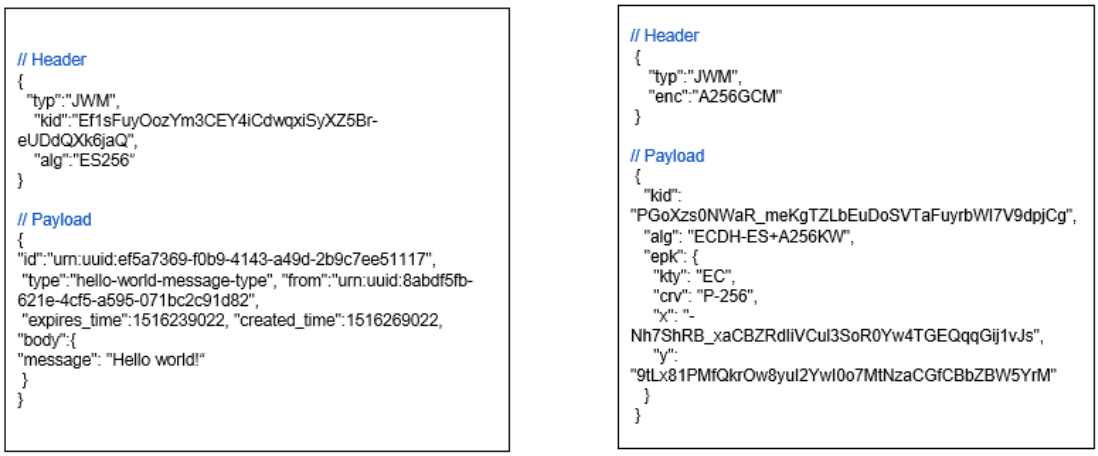


図 0-31：JSON Web Message の例[206]

本仕様のセキュリティの観点における課題は以下の通り。

- JWM の内容は、その内容が暗号で保護され、信頼の決定に必要なコンテキストにバインドされていない限り信頼することはできない。
- ネストされた JWM は署名と暗号化の両方が可能であればどのような順序でも適用可能である。
- JWS および JWE におけるセキュリティ考慮事項が適用される。
- プライバシーの観点における課題は以下の通り。
- JWM はセンシティブなプライバシー情報を含む場合がある。この場合、情報が開示されることを防ぐために、「暗号化された JWM を利用し受信者を認証」、「TLS のような暗号化された経路上で送信」などの対策をしなければならない。

（C-1）Self-Issued DID Profile for OpenID[207]

Self-Issued DID Profile for OpenID（SIOP DID）は DIF Authentication Working Group にて公開されている、Web アプリケーションに Identity Wallet を統合するための汎用的な方法として DID AuthN に OpenID Connect を使用するための仕様である。

SIOP DID 公開時に DIF が OIDC を選択した理由は以下のとおりである。[208]

- 良く知られていて成熟した仕様である

---

[206] Internet Engineering Task Force, "JSON Web Message - 2.JSON Web Message (JWM) Overview," (January 2020), https://datatracker.ietf.org/doc/html/draft-looker-jwm-01#section-2

[207] DIF, "Self-Issued OpenID Connect Provider DID Profile v0.1," https://identity.foundation/did-siop/

[208] Oliver Terbu, "Using OpenID Connect with Decentralized Identifiers," (May 2019), https://medium.com/decentralized-identity/using-openid-connect-with-decentralized-identifiers-24733f6fa636

- 広く利用されており、大きなコミュニティが存在する
- OIDC に精通した企業が多く存在している
- シンプルかつ軽量である
- 柔軟性及び拡張性がある
- クレデンシャル/クレームの交換をオプションとしてサポートしている
- RWOT や IIW で開発されたものがベースとなっている

プロトコルの処理フロー概要は以下のとおりである。SIOP DID のフローは OIDC Self-Issued OpenID Provider 仕様に従って Implicit フローで行われる。

1. ユーザは RP にアクセスする
2. RP は”Sigin-in with SSI”ボタンを返し、User がこれを押下すると SIOP Request が生成
3. SIOP Request (openid://?<SIOP request>) により SIOP が起動
4. SIOP は OIDC/DID AuthN に従って SIOP request を検証し SIOP response を生成
5. response_mode の指定に従って RP に SIOP Response がわたされる
6. RP は OIDC/DID AuthN に従って SIOP response を検証する。

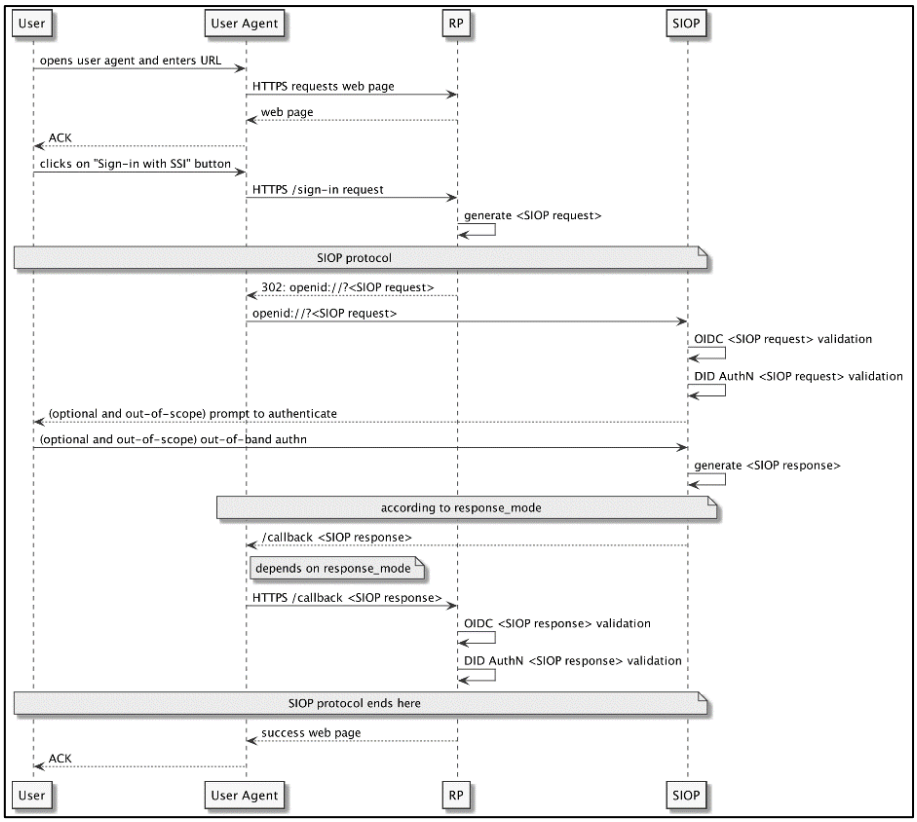


図 0-32：SIOP の処理フロー概要像[209]

2020 年 11 月 9 日 OIDF と DIF はリエゾン契約を締結に伴い、DIF による SIOP DID の作業を一時停止することを表明した。今後は OIDF AB/Connect Working Group によって OIDC Core 7 章 Self-Issued OpenID Provider の改訂が進められる。AB/Connect Working Group で作業が再開される予定となっている。

2021 年 1 月の DIF F2F Virtual コミュニティイベントにて関連仕様のステータスが以下の通り公表された。

- OpenID Connect Claims aggregation (adopted)
- OpenID Self Issued Identifiers (adopted)
- Self-Issued OpenID Provider v2 draft01 (adopted)
- OpenID Connect Credential Provider
- Smart Credentials
- Portable Identifiers: WIP

（C-2）Presentation Exchange[210]

Presentation Exchange は Verifier が Proof の要件を明確にするために利用可能な Presentation Definition および、Holder が Presentation Definition に従って Proof を提出するために使用可能な Presentation Submission のデータ形式を体系化する仕様である。クレームをやり取りするアイデンティティ・システムにおいて一般的なアクティビティは Holder と Verifier 間の Proof の要求と提出である。このフローにおいて、Verifier が Proof の要件を定義する方法および Holder が要件に合わせて Proof をエンコードする方法が必要である。これら主要な 2 つのステップを容易にするメカニズムが必要が仕様の背景にある。

Presentation Exchange はクレームの形式およびトランスポートプロトコルに依存しないように設計されている。つまり、クレームの形式を JSON Web Token (JWT)、Verifiable Credential (VC)、JWT-VC としたうえで、OpenID Connect (OIDC)、DIDComm、Credential Handler API で伝達することが可能である。

Presentation Exchange はトランスポートプロトコルや特定のエンドポイントなどのデータを伝達する方法を示す仕様ではないが、他の仕様やプロジェクトのフローにおいて Presentation Exchange で定義されたデータ形式の利用を奨励している。

---

[209] DIF, "Self-Issued OpenID Connect Provider DID Profile v0.1 - 3.Protocol Flow," https://identity.foundation/did-siop/#protocol-flow-0

[210] DIF, "Presentation Exchange," https://identity.foundation/presentation-exchange/

DIF Presentation Protocol 以外の Presentation Protocol として、Verifiable Presentation Request Specification v0.1[211]が W3C CCG (Credential Community Group)で公開されている。これらの仕様は次期に統合されていく旨が IIW30 のセッション 101 Session: Verifiable Credential Handler (CHAPI) and DIDComm[212]で述べられている。

Presentation Definition は Verifier が必要とする Proof を明確にするためのオブジェクトである。Presentation Definition は、必要な Proof の形式と詳細を記述する入力と、オプションの選択ルールのセットで構成される。ホルダーが要件を満たす様々なタイプの Proof で柔軟に対応することができるようにする。

Presentation Definition は VP, OIDC, DIDComm, CHAPI などのプロトコルでラップされて伝達されることが想定されている。

```
{
  "comment": "Note: VP, OIDC, DIDComm, or CHAPI outer wrapper would be here.",
  "presentation_definition": {
    "id": "32f54163-7166-48f1-93d8-ff217bdb0653",
    "input_descriptors": [
      {
        "id": "wa_driver_license",
        "name": "Washington State Business License",
        "purpose": "We can only allow licensed Washington State business",
        "schema": [{
          "uri": "https://licenses.example.com/business-license.json"
        }]
      }
    ]
  }
}
```

図 0-33：Presentation Definition オブジェクトを用いた定義例[213]

Presentation Definition オブジェクトは以下のパラメータで構成される。

表 0-16：Presentation Definition オブジェクトのパラメータ

パラメータ名	サポート	説明
id	MUST	UUID などの一意の識別子

[211] W3C, "Verifiable Presentation Request Specification v0.1," (April 2021), https://w3c-ccg.github.io/vp-request-spec/

[212] IIW, "101 Session: Verifiable Credential Handler (CHAPI) and DIDComm," https://iiw.idcommons.net/101_Session:_Verifiable_Credential_Handler_(CHAPI)_and_DIDComm

[213] DIF, "Presentation Exchange v1.0.0 - 4.Presentation Definition," https://identity.foundation/presentation-exchange/#presentation-definition

name	MAY	Presentation Definition が何に関係するかを記述する human-friendly な名前。
purpose	MAY	Presentation Definition の入力が要求される目的を記述した文字列。
format	MAY	Verifier が処理可能な Claim フォーマットを Holder に通知するための値（jwt, jwt_vc, jwt_vp など）。
submission_requirements	MAY	Submission Requirement Format に準拠した値。この値が存在しない場合は、input_descriptors 配列に含まれるすべての入力が Submission に必要となる。
input_descriptors	MSUT	Descriptor オブジェクトの配列。Submission_requirements が存在しない場合、input_descriptors は入れ何時に含まれるすべての入力が Subimission に必要となる。

Presentation Submission は、Verifier が Presentation Definition で指定した要件に従って、Verifier への Proof の提示を統一するためのオブジェクトである。

```
{
  // NOTE: VP, OIDC, DIDComm, or CHAPI outer wrapper properties would be here.
  "presentation_submission": {
    "id": "a30e3b91-fb77-4d22-95fa-871689c322e2",
    "definition_id": "32f54163-7166-48f1-93d8-ff217bdb0653",
    "descriptor_map": [
      {
        "id": "banking_input_2",
        "format": "jwt_vc",
        "path": "$.verifiableCredential[0]"
      },
      {
        "id": "employment_input",
        "format": "ldp_vc",
        "path": "$.verifiableCredential[1]"
      },
      {
        "id": "citizenship_input_1",
        "format": "ldp_vc",
        "path": "$.verifiableCredential[2]"
      }
    ]
  }
}
```

図 0-34：Presentation Submission オブジェクトを用いた定義例[214]

Presentation Submission オブジェクトは、presentation_submission プロパティとしてデータフォーマット内に配置されなければならない。

Presentation Submission オブジェクトは以下のパラメータで構成される。

表 0-17：Presentation Submission オブジェクトのパラメータ

パラメータ名	サポート	説明
id	MUST	UUID などの一意の識別子。
definition_id	MUST	Submision を Definition にリンクするための値。有効な Presentation Definition の id でなければならない。
descriptor_map	MUST	Input Descriptor Mapping オブジェクトの配列。

Presentation Submission を埋め込む場所はプロトコルごとに以下のように定義されている。

表 0-18：プロトコルごとの Presentation Submission の埋め込み場所

Target	Location
OpenID	top--level
DIDComms	ルートオブジェクト配下の presentations-attach.data.json
VP	top-level
CHAPI	ルートオブジェクトは以下の data

現時点で本仕様にセキュリティ考慮事項の記載は存在しない。セキュリティ考慮事項のセクション追加は GitHub の Issue で取り上げられている。また、Issue 上では、Holder が Verifier からの要求に自動応答する場合、Verifier が複数回 Presentation Exchange を実行することで Holder のプロファイリングが可能になり、プライバシー保護の目的が失われることが懸念されている。

Presentation Exchange と役割が酷似した仕様として Verifiable Presentation Request Specification という仕様が W3C CCG から公開されており、統合または共存が検討されている。GitHub の Issue 上では Presentation Exchange がサポートするトランスポートプロ

[214] DIF, "Presentation Exchange v1.0.0 - 4.Presentation Definition," https://identity.foundation/presentation-exchange/#presentation-definition

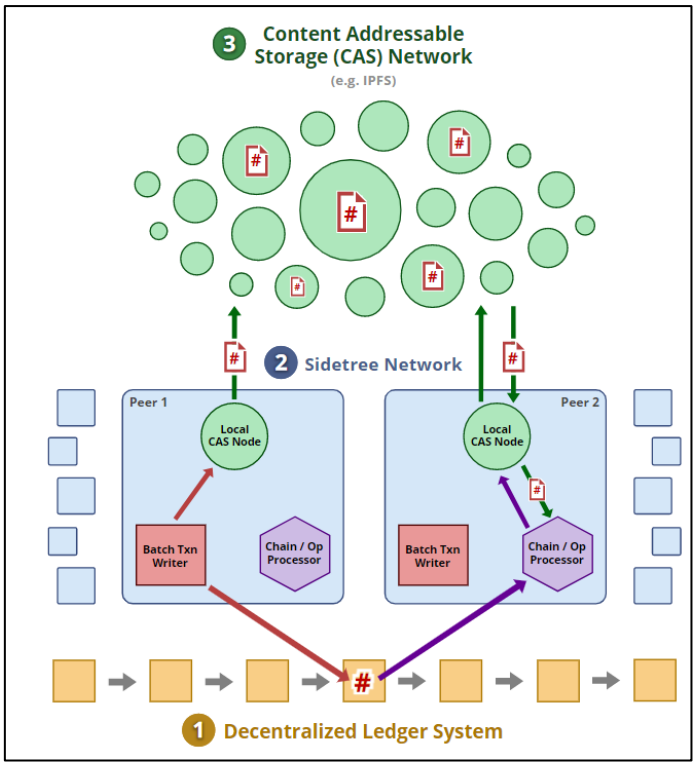
トコルである OpenID Connect 利用時の処理フローなどに関する質問がいくつか上がっている。

（C-3）Sidetree[215]

Sidetree はブロックチェーンのセカンドレイヤー技術であり、スケール可能な DPKI（Decentralized Public Key Infrastructure）ネットワークを構築するためのプロトコルである。このプロトコルにより、ユーザは第三者機関を必要とせずグローバルで一意の識別子を作成し、関連するメタデータを管理することができる。なお、利用される識別子は W3C DID に準拠している。

Sidetree を構成する要素については以下の通りである。

- Decentralized Ledger System…DID や DID Document を書き込む Bitcoin などの基盤
- Sidetree Network…Sidetree ノードで形成され、トランザクションの監視や書き込みを実行するネットワーク。これらのノードは、データをフェッチして CAS に再配置する。
- Content Addressable Storage（CAS）Network…IPFS など CAS（Content-Addressable Storage）で形成されたネットワーク



[215] DIF, "Sidetree v1.0.0," https://identity.foundation/sidetree/spec/

図 0-35：Sidetree の概要像[216]

ION は Sidetree プロトコルを活用したパブリックかつパーミッションレスな DID ネットワークであり、ブロックチェーンに依存しない Sidetree プロトコルを Bitcoin 上に実装し、Content-Addressed Storage を IPFS 用いて実装している。トランザクションはハッシュでエンコードされており、ION ノードはハッシュに関連付けられた DID 操作のバッチを IPFS 経由で取得、保存、複製するために使用する。

ION および ION がベースにしている Sidetree プロトコルの開発は DIF で行われている。2021 年 3 月に ION の v1 が完成し、Bitcoin のメインネットでローンチされたことがマイクロソフトから発表された。ION はパーミッションレスなシステムであり、誰もが ION ノードを運用することができる。運用される ION ノードが多ければ多いほど ION ネットワークは強固なものになる。今後、他の企業や組織と協力して ION ノードの本番インフラの活用を図っていくとしている。

（C-4）Key Event Receipt Infrastructure

Key-Event Receipt Infrastructure（KERI）はキーイベントを受け取り管理するインフラであり、マイクロレジャーとしての役割を持つ。キーイベントは鍵の生成、鍵のローテーション、署名などのイベントを指している。DIF Identifiers & Discovery Working Group が主導しているプロジェクトであり、以前は W3C Decentralized Identifier Working Group で仕様検討されていた。

KERI の特徴は以下の通りである。

- 自己証明付き識別子
  Self-certifying identifier（SCID）という公開鍵にバインドされた唯一の識別子であることを暗号技術のみ（ブロックチェーンを必要としない）で証明することができる識別子を利用する。これにより、第三者に依存することなく KERI 識別子のコントロールを証明することができる。
- 自己証明キーイベントログ
  ペアを変更する度にログファイルに署名されたメッセージを書き込む。これにより、鍵ペアを変更する際に第三者に依存することなく新しい公開鍵のコントロールを証明することができる。
- キーイベントログの証人
  KERI キーのイベントログのコピーを自身で保管することも、他の目撃者に自身のコピ

[216] DIF, "Sidetree v1.0.0 - 7.Network Topology," https://identity.foundation/sidetree/spec/#network-topology

ーを署名したうえで保管してもらうことも可能である。これにより、現在の公開鍵を管理しており不正をしていないことを示す追加の証拠を提供する。

- 鍵の漏洩を防ぐシンプルかつ安全でスケーラブルなプリローテーション
  KERI は次に利用する秘密鍵を隠すためのソリューションを持っている。これにより、次に利用する秘密鍵を安全にロックすることができ、現在利用している秘密鍵が危殆化した場合においても自身を守ることができる。なお、秘密鍵の盗難自体を防ぐことはできない。
- システムに依存しない検証
  KERI 識別子とイベントログは Self-certifiying である。これにより、KERI 識別子と鍵は”ledger-locked”ではないため、あらゆる台帳、分散データベース、Verifiable Data Registry 上で検証することが可能である。
- 委任された自己証明書によるエンタープライズレベルの鍵管理
  KERI 識別子は委任が可能であり、識別子で親子関係を持つことができる。KERI 識別子と鍵の委任により、あらゆる規模と複雑さの階層構造を拡張して管理することが可能である。
- GDPR の忘れられる権利との互換性
  KERI インフラでは不変な台帳を利用する必要がない。これにより、KERI イベントログはセキュリティを損なうことなく削除することができるため GDPR に準拠することが可能である。

（D）Hyperledger Aries RFC

以下の（D-1）から（D-3）までを策定している Hyperledger Aries RFC[217]とは、Hyperledger Aries プロジェクトを構成するコンセプトや機能で文章化されているものである。Hyperledger Aries 自体は Linux Foundation がサポートするブロックチェーンを構築するためのプロジェクトである Hyperledger の一部であり、クレデンシャルの作成、送信および保存に焦点を当てた再利用かつ相互運用可能なツールキットを提供する。

なお、Hyperledger プロジェクトには Aries の他に Hyperledger Indy や Ursa などが存在している。Hyperledger Indy は分散アイデンティティのために特別に実装されたブロックチェーンである。Indy は Distributed Ledger Technology（DLT）の実装と、DLT とやり取りをするためのアプリケーションのためのインターフェースを提供している。Hyperledger Ursa は暗号化パッケージを提供するプロジェクトであり、Indy および Aries における処理で利用されている。Ursa は非常に複雑な暗号処理を様々なプロジェクトにおいて再利用可能にし、セキュリティを向上させるための重要な役割を担っている。

---

[217] Hyperledger, "Hyperledger Aries RFC," https://github.com/hyperledger/aries-rfcs

（D-1）Aries RFC 0023: DID Exchange Protocol[218]

DID Exchange Protocol 1.0 は Agent 間で DID を交換するためのプロトコルを規定している。本仕様では Requester および Responder の 2 つのロールが定められている。Requester は Invitation メッセージを受信または Public DID からの暗黙的な Invitation を使用してこのプロトコルを開始する当事者である。Responder は、Invitation の送信者または暗黙的な Invitation を持つ DID の発行者であり、DIDComm を介して他の Agent と対話をする。

プロトコルの処理フローの概要は以下の通りである。

1. Responder は Invitation メッセージを使用して Requester に自身の情報を提供する。
2. Requester は受信した情報を元に DID と DIDDocument をレスポンスメッセージとして Requester に送信する
3. Responder は送信された DIDDocument に含まれる情報を使用して DID と DIDDocument をレスポンスメッセージとして Requester に送信する。
4. Requester はレスポンスメッセージを受信したことを通知するメッセージを Responder に送信する

（D-2）Aries RFC 0036: Issue Credential Protocol[219]

Issue Credential Protocol はクレデンシャルの発行に使用されるメッセージを形式化するプロトコルである。このプロトコルは特定のクレデンシャルの形式に依存するものではない。対応するクレデンシャルの形式の一例としては、JWT、JSON-LD、ZKP などがある。また、このプロトコルに適合していないクレデンシャルの形式を使用する場合は GitHub から Issue を提起することができる。

このプロトコルでは、Issuer と Holder の 2 つのロールを扱う。

---

[218] Hyperledger, "Aries RFC 0023: DID Exchange Protocol 1.0," (May 2021), https://github.com/hyperledger/aries-rfcs/blob/master/features/0023-did-exchange/README.md

[219] Hyperledger, "Aries RFC 0036: Issue Credential Protocol 1.0," (November 2020), https://github.com/hyperledger/aries-rfcs/blob/master/features/0036-issue-credential/README.md

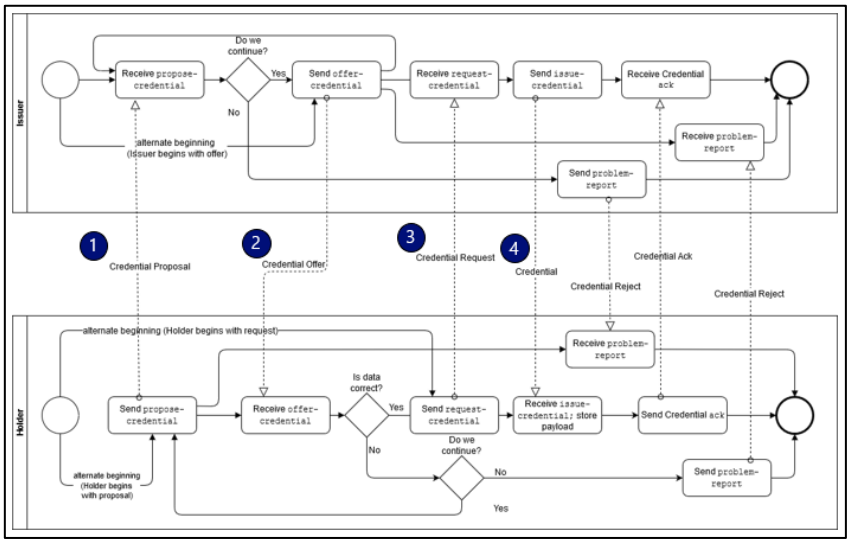


図 0-36：Issuer Credential Protocol 1.0 の概要像[220]

プロトコルの処理フローの概要は以下のとおりである。

1. Holder から Issuer に対してプロトコルを開始するためのリクエストが送信される。または、Holder が Issuer に対して要求するクレデンシャルを指定するためのリクエストが送信される。
2. Issuer が Holder に対して提供予定のクレデンシャルに関する情報を送信する。
3. Holder から Issuer に対してクレデンシャルを要求するためのリクエストが送信される。
4. 要求されたクレデンシャルに対するレスポンスを送信する。

（D-3）Aries RFC 0037: Present Proof Protocol[221]

Present Proof Protocol は Proof の提示に使用されるメッセージを形式化するプロトコルである。このプロトコルは検証可能なクレームを提示するためのメッセージについてのものであり、特定の提示メカニズムに依存するものではない。ただし、バージョン 1.0 の段階でサポートされている提示メカニズムは Hyperledger Indy のみである。

このプロトコルでは、Verifier と Prover の 2 つのロールを扱う。

---

[220] Hyperledger, "Aries RFC 0036: Issue Credential Protocol 1.0," (March 2020), https://github.com/hyperledger/aries-rfcs/blob/master/features/0036-issue-credential/credential-issuance.png

[221] Hyperledger, "Aries RFC 0037: Present Proof Protocol 1.0," (November 2020), https://github.com/hyperledger/aries-rfcs/tree/master/features/0037-present-proof

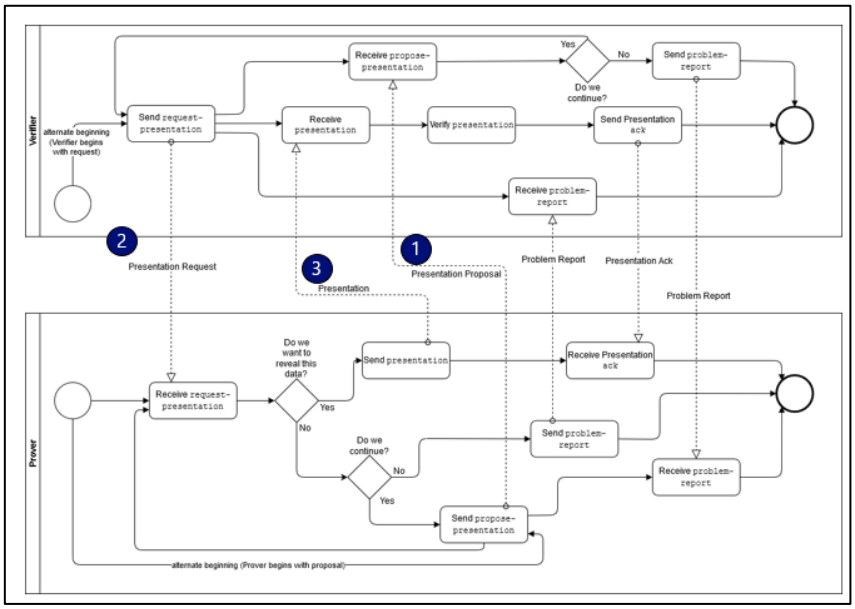


図 0-37：Presentation Proof Protocol の概要像[222]

プロトコルの処理フローの概要は以下の通りである。

1. Prover から Verifier に対して Proof Presentation を開始するためのメッセージが送信される。
2. Holder から Issuer に対してクレデンシャルを要求するリクエストが送信される
3. Verifier から Prover に対して署名済みの Presentation が含まれるレスポンスが送信される。

（D）Aries RFC の課題と新たな取り組み

Aries と DIF は共同で DID Communication ワーキンググループを主催しており、Aries を中心に構築されたエコシステムだけでなく、分散型 ID コミュニティ全体の通信プロトコルの仕様策定に参加している。Aries は独自に Aries interoperability profile という Conformance Test のプロファイルを所持している。ただし、これは Aries のプロトコルやアーキテクチャが正常に実装されていることを示すためのものである。ここでの相互運用性とは、他の Aries システムとの相互運用性や標準的な VC データモデルに対する Aries の共通解釈と、その解釈に基づいてコミュニティが定義したプロトコルへの適合性を意味している。W3C CCG は W3C のコア仕様に関するテストスイートとして VC-HTTP-API Test Suite および DID core Test Suite に取り組んでいる。Aries interoperability profile は独自のインフラに焦点を当てており、ブロックチェーンベースの ZKP システムプライバシー保証

222 Hyperledger, "Aries RFC 0037: Present Proof Protocol 1.0," (March 2020), https://github.com/hyperledger/aries-rfcs/blob/master/features/0037-present-proof/credential-presentation.png

に焦点を当てている。この焦点は W3C テストスイートに取って代わるものではなく、補完するものである。

（E-1）Trust over IP[223]

Trust over IP（ToIP）は開発者がデジタル通信ネットワーク上で信頼された関係を確立するために実装できる標準的なアーキテクチャを定義している。”identity layer”の最終的な目的はエンティティの識別だけでなく、相互作用に必要な信頼を促進することであるため、このスタックを Trust over IP と呼んでいる。

ToIP はテクノロジーとガバナンスの両方を包含する 2 つの並列スタックである。これは、デジタルトラストはテクノロジーだけでは達成できず、人間とテクノロジーが一緒に働くことによってのみ達成できるということを反映している。なお、ToIP スタックは特定のガバナンスフレームワークを定義するものではない。むしろ、オンラインでの過渡的なトラストを促進するために、普遍的に参照され、理解され、消費されうるデジタルガバナンスフレームワークをどのように設計し、実装するかのメタモデルである。ガバナンスを定義するためのアプローチは、人間とレイヤー2 でソフトウェアエージェントが、トラストの境界の中でも境界を越えてトラストの決定を下すことを容易にする。

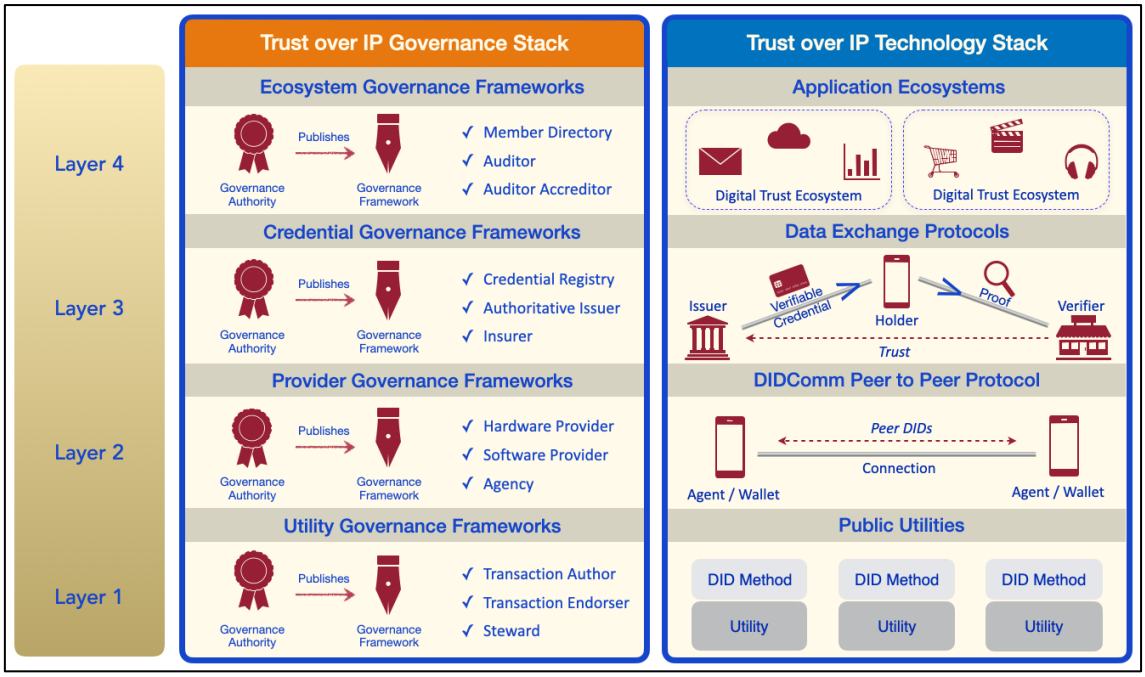


図 0-38：The ToIP stack[224]

[223] Hyperledger, "0289: The Trust Over IP Stack," (May 2021), https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0289-toip-stack/README.md

[224] Hyperledger, "0289: The Trust Over IP Stack," (June 2020), https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0289-toip-stack/img/fig-1-toip-full-stack-2020-05-06.png

2020 年 5 月に Linux Foundation はデジタルアイデンティティの標準化を実現するためのコンソーシアム「Trust over IP（ToIP）Foundation」の立ち上げを発表した。ToIP Foundation は、政府、非営利団体、金融、ヘルスケア、エンタープライズソフトウェアなどのプライベートセクターが Linux Foundation と協力し、デジタル時代の消費者や企業のための普遍的なセキュリティとプライバシープロトコルを強化することを目的としている。

（F-1）Decentralized Key Management System[225]

Decentralized Key Management System（DKMS）は Distributed Ledger Technology における利用を想定した鍵管理の新しいアプローチである。従来の PKI では集中型の認証局により証明書が発行されていたが、DKMS におけるトラストのルートは DID をサポートする分散台帳およびプロトコルになる。DKMS は CKMS の派生であり、NIST 800-130 をもとに CKMS 要件の DKMS への適用が図られている。

DKMS は DID レイヤー、Cloud レイヤー、Edge レイヤーの 3 つのレイヤーで構成される。DID レイヤーは分散台帳や分散型のプロトコルを介して登録及び解決される DID で構成されたレイヤーである。Cloud レイヤーは通信を仲介する手段を提供し、暗号化されたピアツーピア通信を可能にするサーバーサイドのエージェントで構成される。Edge レイヤーは ID 所有者が直接利用し、秘密鍵の生成及び保存をするローカルデバイス、エージェント、ウォレットで構成される。

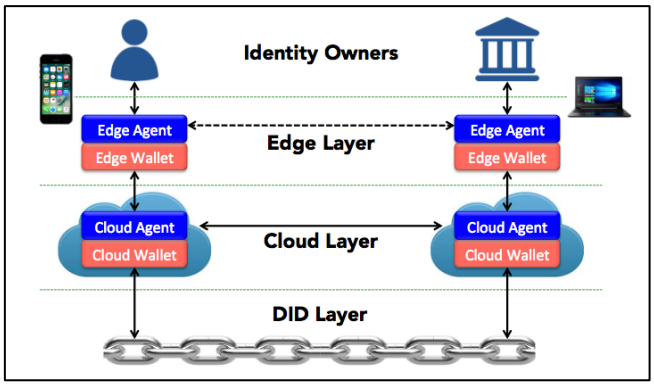


図 0-39：DKMS の概要像[226]

[225] Hyperledger, "DKMS (Decentralized Key Management System) Design and Architecture V4," (August 2020), https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0051-dkms/dkms-v4.md

[226] Hyperledger, "DKMS (Decentralized Key Management System) Design and Architecture V4 - 3.High-Level Architecture," (August 2020), https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0051-dkms/dkms-v4.md#3-high-level-architecture

DKMS による鍵管理では NIST 800-130 に定義される鍵タイプ（マスター鍵、暗号鍵、データ鍵）に加え、以下の鍵タイプが Credential Exchange プロトコルに必要な鍵タイプとして含まれる。

- Agent policy keys
- DID keys
- Link secret
- Wallet encryption keys
- Wallet permission keys

各鍵タイプにおける鍵紛失からのリカバリについては以下の通り。

表 0-19：DKMS での鍵タイプごとの鍵紛失からのリカバリの影響と要求事項

鍵のタイプ	影響	要求事項
Agent policy key	Agent は Agent Policy Registry を更新できなくなる	Agent Policy Registry からアクティブな Agent Policy Key を取消し、代替 Agent に新しい Agent Policy Key を発行できるバックアップ Agent Policy Key を所持している必要がある。
DID Key	Agent はチャネルを介して認証できなくなり、キーをローテーションできなくなる	暗号化されたバックアップから回復可能でなければならない
Link Secret	所有している Verifiable Credential の Proof を生成できなくなったり、同じ ID で Credential を発行できなったりする	暗号化されたバックアップから回復可能でなければならない
Credential	Credential の Issuer に連絡し、再認証したうえで Issuer に既存の Credential の取り消しを要求する必要がある	暗号化されたバックアップから回復可能であるべき
Relationship State Recovery	Key Loss のシナリオによる Relationship State の回復は	上記のキー損失シナリオのいずれかによる関係状態の

	dead drop mechanism により可能	回復は、デッドドロップメカニズムを介して有効になる

各鍵タイプにおける鍵侵害からのリカバリについては以下の通り。

表 0-20：DKMS での鍵タイプごとの鍵侵害からのリカバリの影響と要求事項

鍵のタイプ	影響	要求事項
Agent Policy Key	攻撃者が Agent を使用して Owner になりすまし、Proof を提示したり、Policy Registry を変更したりできる。	Owner はなりすましを防ぐためにデバイスの取り消しができる必要がある。また、侵害された鍵を Agent Policy Registry から取消し、新しい Agent Policy Key を代替 Agent に発行することを許可されたバックアップ Agent Policy Key を持っている必要がある。
DID Key	攻撃者がチャネルを使用して所有者になりすますだけでなく、所有者が起こったことに気付く前に攻撃者がキーをローテーションした場合、所有者をそれ以上使用できないようにロックアウトできることを意味する。 キーを定期的にローテーションさせると、この攻撃対象領域が最小限に抑えられる。	Owner は侵害が発見されたときに手動でローテーションをトリガーできる必要がある。 Owner は、アクションを承認するために複数の Agent が必要なため、単一の侵害された Agent トが鍵を取り消すことができない複数の Agent 間で拡散信頼モデルを実装する必要がある。
Link Secret	攻撃者が Verifiable Credential を受信するときに Owner になりすますか、Proof の提示に既存の	Owner は自分の資格情報を取り消して、新しいリンクシークレットで再発行するように要求する必要がある。

	資格情報を使用する可能性があることを意味します。攻撃者が「PROVE」認可を持つ Agent も使用できない限り、Verifier は認証されていない Agent を検出できる。	
Credential	攻撃者が Verifiable Credential の属性を学習したことを意味する。攻撃者が Link Secret と許可された Agent を侵害することもできなければ、資格情報を主張することはできないため、唯一の損失は基盤となるデータの制御となる。	
Relationship State Recovery	Key Compromise のシナリオによる Relationship State の回復は dead drop mechanism により可能。	

3-2-4. 統制構成要素の概要

1 章で紹介した Open Identity Exchange(OIX)のトラストフレームワークは、特定技術要素に寄らず、欧州の eIDAS、英国の Verify、カナダの PCTF、インドの Aadhaar 等の教訓も踏まえ、AML 等の分野における適切な規制要件定義に際して、トラストフレームワークとの関連性の理解を促す規制当局向けのガイドとして活用可能と述べられている[227]。また、SSI への適用も想定されている。

こうした特性を考慮し、本調査では、ガバナンスにおける構成要素として、同フレームワークにて規定された項目を踏まえた整理を行う。同時に、SSI モデルにおける、ガバナンス面で考慮事項の整理を行う。

表 0-21：OIX のトラストフレームワークで規定される構成要素[228]

[227] OIX, "OIX Guide to Trust Frameworks V0.1 BETA," (June 2020), https://openidentityexchange.org/networks/478/item.html?id=364

[228] OIX, "OIX Guide to Trust Frameworks V0.1 BETA," (June 2020), https://openidentityexchange.org/networks/478/item.html?id=364

構成要素	概要
1. 原則	
2. トラストマークと UX	
3. 役割と義務	
4. 一般ルール	記録保存と監査証跡
	不正行為とサイバーコントロール
5. ユーザサービス	デジタルアイデンティティの選択
	ID の作成＆管理
	トラストの獲得と提示
	同意
	ヘルプ＆サポート
6. リライングパーティサービス	アイデンティティサービスへのユーザアクセス
	レクエスト＆レスポンス(API)
	RP による ID 保証
	ライアビリティ
	サービスレベル
	ヘルプ＆サポート
7. トラストルール	プルーフィング
	アイデンティティ保証
	認証
	適格性保証
8. 技術・セキュリティ要件	セキュリティルール
	エコシステム参加者のトラストレジストリ
	証跡の記録と提示
	リクエスト及びレスポンススキーム
9. 相互運用性	内部の相互運用性
	外部の相互運用性
10. ガバナンス	トラストフレームワークの構築と管理
	トラストフレームワークの強制力
	トラストフレームワークの認証
	トラストフレームワークの運用

表 0-22：トラストフレームワークの構成要素概要

構成要素	概要

1. 原則		マルチステークホルダーのニーズを考慮するにあたっての優先順位を定義する。 （1.ユーザ、2. RP、3. フレームワーク、の順） ユーザに関し 4 つの原則（4Cs）を定義する。 （Convenience, Choice, Control, Confidence）
2. トラストマークと UX		User, RP, Evidence Issuer が見て Trust Framework の運用がなされているのを認識可能とするシグナルを定義する。（シンボル・フレーズなど） 包括的なトラストマークを作成する、或いはトラストマーク表示時にフレームワーク間の総合合意を一覧表示することで、フレームワーク間の Interoperability を示すことも可能。 （例：フレーズ、単語、シンボル等。類似事例では、決済におけるカードブランド等がある。）
3. 役割と義務		—
4. 一般ルール	記録保存と監査証跡	データトラッキングとトラストフレームワークの完全性確保の為、以下に関する監査記録の保持が必要。 データの生成、更新、削除、Evidence の収集・提示、保証の評価（アセス）、クレデンシャルの発行と利用
	不正行為とサイバーコントロール	トラストフレームワーク内の ID エコシステム全体を、サイバー攻撃や ID 詐欺から保護する必要がある。また、トラストフレームワークに参加するエンティティは、担う役割に応じ不正やサイバーリスクの管理に何らかの責任を持つ。 不正に対する防御、不正行為の検知、当事者への通知・報告、不正行為の防止活動を行う機関同士の攻撃情報共有、影響の局所化・対象 ID の閉鎖、対処・復旧、証跡の取得、起訴・調査のための証跡の提示等。
5. ユーザサービス	デジタルアイデンティティの選択	自身のニーズに適した ID プロバイダの選択、他 ID プロバイダへのアサーション展開可否、一度オンボーディングを完了したエンティティの再アク

		セス時における適切な Recognition 実施等が可能なこと。
	ID の作成＆管理	Identity のライフサイクル管理、特にクレデンシャル、Account Recovery、属性情報更新時の RP への通知等の対応が可能なこと。
	トラストの獲得と提示	Evidence の保持、RP の求める保証レベルの充足。理想は、利用者が保証レベルを意識せず使えるのが望ましい。
	同意	利用者同意の元属性情報の連携が可能なこと。共有・利用履歴の閲覧権・データ削除権を利用者が有すること。
	ヘルプ＆サポート	Identity Provider がいつでも変更可能なこと、またその際 Identity Proofing 情報のポータビリティを有すること。 クレデンシャルが危殆化した際、RP への通知や、クレデンシャルの復旧が可能であること。
6. リライングパーティサービス	アイデンティティサービスへのユーザアクセス	RP による Trustmark 選択が可能なこと。
	レクエスト＆レスポンス(API)	CP と RP の選択に制約を受けない、インターフェース定義やリクエスト・レスポンスの定義が明確であること。
	RP による ID 保証	Identity Assurance Model の定義、RP による利用者（が意識しなくて保証レベルを済むための）のガイドがあること。
	ライアビリティ	責任モデル、障害時の責任、フレームワークのルール逸脱時に課せられる責任、訴訟、調停・仲裁人の必要性に関する整理がなされていること。
	サービスレベル	Trust scheme や Broker による差別化・競争力の保持が可能なこと。
	ヘルプ＆サポート	RP 内アカウントへのアクセスの継続性を維持した状態での IDP の移植性・選択の自由の実現、コンプライアンス・苦情処理の対応が可能なこと。 保証メカニズムによる差別化が図れること。
7. トラストルール	プルーフィング	ID Proofing の技術要素として、Validation, Verification, Identity Risk Assessment を定義。

		Identity Assurance Assessment への Proofing Score 割り当てにも言及。 フレームワーク間の相互運用性においては、Proofing Score の一致／同等性判断で実現される可能性がある。
	アイデンティティ保証	Identity Assurance Process において、保証レベルの定義付け、本人確認・当人認証の保証レベル、バインディング処理を考慮する必要がある。 フレームワーク間の相互運用性においては、保証レベルの一致／同等性判断で実現される可能性がある。
	認証	信頼性／evidence／適格性のレベルを RP に提示する為、および Digital Identity を maintain するため、クレデンシャルを用いた当人認証処理を行う必要がある。 継続的なトラストの確認（Evidence の有効性検証[validation]および再検証[reverified]）を考慮すべき。
	適格性保証	適格性保証のため、Eligibility Evidence の Validation・Verification を行う。
8. 技術・セキュリティ要件	セキュリティルール	フレームワーク内の当事者に適用されるルールの定義と、その遵守が必要。 （休止中のデータ、トランジット中のデータ、運用セキュリティ管理に関するルール規定を行う必要がある）
	エコシステム参加者のトラストレジストリ	参加する当事者を管理するためのレジストリ実装・記録・チェックが必要。
	証跡の記録と提示	Evidence の収集・生成・提示フェーズでどの様に evidence proof の履歴が記録されるかを定義すべき。また履歴は改ざんされない様、暗号技術の考慮も必要となる。 ゼロ知識証明への対応を行うか考慮すべき。
	リクエスト及びレスポンススキーム	Identity Evidence と eligibility information が一貫した方法で RP に提示される様、リクエスト／レスポンスのスキーマ定義が必要。

		（特に複数 Evidence Issuer をサポートする Trust Framework では重要となる） OIDF／W3C 等グローバルに定義されたスキーマを考慮すべき。 Evidence Type によってはローカライゼーションが必要となるが、フレームワークはそれに備え、ローカルに適用可能なスキーマの為のキュレーターを実装すべき。
9. 相互運用性	内部の相互運用性	ユースケース・セクター間での相互運用性達成のため、トラストフレームワークレベルでのルール設定に準拠させる、或いは当事者に個別の複数 scheme に準拠してもらうことで達成。 トラストフレームワークレベルで設定すべきルールとして、以下を述べている。 ● Application of Principles ● Trustmark Rules ● Trust Rules and model, but perhaps leave the setting of acceptable scores within the model for particular use cases to the trust scheme. ● Technical Rules such as used of common levels of Security and common Schemas
	外部の相互運用性	他トラストフレームワークとの外部相互運用性の実現手段として、下記 3 点に言及。 １）相互合意。フレームワークが保証するトラストを相互に認識。 ２）ノードアプローチ※を通じた、エージェントが多数 framework の整合性と互換性を独立に評価し、複数 trust framework が相互に信頼しあう ３）IDP や evidence verifier 等当事者の、複数の trust framework への準拠。 ※ノードアプローチは、各フレームワークが共通に合意されたルールに従うことを必要とするのみであり、フレームワーク間の大量の相互運用性実現のための効率的な手段としている。いわゆる”Framework of frameworks”）

		相互運用性で考慮すべき設計・実装ポイントとして、以下を述べている。 ● Application of Framework Principles ● Trustmark Rules ● Trust Rules ● Record Keeping ● Fraud Controls ● Response Schema ● Security Standards	
10. ガバナンス	トラストフレームワークの構築と管理	トラストフレームワーク生成者として5モデル定義 1）Independent Governing Entity 2）Consortium of Participating Entities 3）Single Participant Governing Entity 4）Non-Governing Standards or Certification Organization 5）Mutual Agreement Among All	（事例） 1）DIACC 2）CA/Browser Forum 3）単一 ID Provider, GOV.UK Verify 4）Kantara Initiative, tScheme 5）-（個別の管理主体は存在せず）
	トラストフレームワークの強制力	ルール遵守の為の強制力として、下記3つのケースを想定。 1）民間セクター：契約メカニズムによる強制力 2）政府セクター・政府スポンサー：法令・規則等による強制力 3）官民パートナーシップ：ハイブリッド（主要原則は法律準拠、特定要件は契約で執行等）	
	トラストフレームワークの認証	トラストフレームワークに参加するエンティティの認証。（トラストフレームワークが定義する義務を果たしている証跡として） 認定手法は以下の通り（各レベルは別紙にて詳述）。	

		● Self-Assessment ● Verified Self-Assessment ● Approved ● Certified
	トラストフレームワークの運用	トラストフレームワーク（TF）の開発・維持に責任を持ち課題発生時に修正する TF Provider が必要。 統制機能の例として、以下を言及。（各レベル差異は別紙にて詳述） ● Governance and Policy Development ● Policy Enforcement ● Participating Entity Management ● Network Evolvement ● Trust Framework Operations

出所：OIX Governance framework をもとに NRI 作成

Open Identity Exchange（OIX）のトラストフレームワークでは、デジタルアイデンティティ管理において必要な構成要素、並びにその実現に必要な役割と義務が述べられている。同フレームワークでは、SSI モデルに対するアプローチについても言及されているが、役割と義務の考え方が変わるのではなく、誰が担うか、という点で従来のモデルと異なると述べている。具体的には、ホルダーが以下の役割を担う点である。

- CP からクレームを受け取る、「RP」としての役割を担う
- RP に対し、①で取得したクレームを展開する、「CP」としての役割を担う

ホルダーが上記 2 つの役割を担うとなると、トラストフレームワークの構成要素でのガバナンスの要件の大半を実現する必要が生じる。しかし、多数の一般のユーザにガバナンス要件を厳守させること等は困難だと考えられるため、実運用を考慮すると、監査対応やクレデンシャルの管理、Liability の整理等、克服すべき課題が存在する。識者からは、ホルダーであるユーザ自身が、ウォレットを提供する事業者に役割と責任を委ねて担わせることが望ましいという意見もあった。詳細は 3-4 にて詳述する。

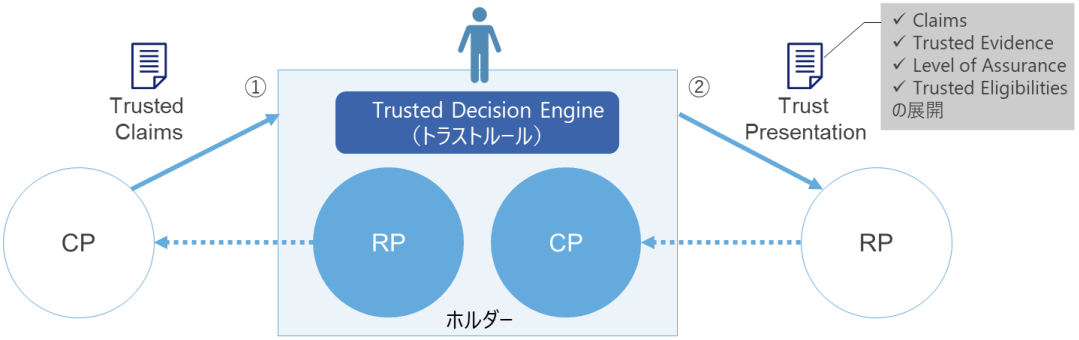


図 0-40：ホルダーの担う役割イメージ[229]

[229] 「OIX Quarterly Workshop - 15th Dec 2020」での資料をもとに NRI が作成

3-3. SSI/DID の先行事例/PoC 事例

現在国内外において金融機関等が関与する SSI/DID を用いた様々な実証実験が進められている。金融機関等が SSI/DID に関心を持っている背景として、主に顧客の登録手続きの効率化や AML 対策の観点で取り組んでいることが分かった。

ただし、現在のところこれら取組の多くは実証レベルであり、実サービスとして取り入れられているのは、カナダ Verified.Me などごく少数にとどまる。Verified.Me は、コンソーシアム型としてスタートし、現時点ではアイデンティティプロバイダとしての金融機関と、サービスプロバイダとしての政府機関や一部の生保会社のみが参画するモデルである。したがって、ユーザの利用シーンを一定程度限定することで、SSI のコンセプトを実現している。なお、ガバナンス準拠という観点では、DIACC が策定する PCTF に準拠している点が特徴であると言える。

また、今後の実用化に向けて特に EU で注目されている取組の一つが、スペインを中心に検討が進められている Alastria_ID を用いたプロジェクトで、代表的なものとして Santander 社が推進するプロジェクト Dalion が挙げられる。Alastria は EU の GDPR や eIDAS への準拠を謳っており、EU の厳しい規制に準拠できるソリューションとして位置づけられている。ただし、Alastria 自体は Alastria_ID の技術フレームワークを開発・提供しているのみで、実際のユースケースは Dalion 等の個別のプロジェクトでの検討が進められている。各プロジェクトにおいて、参画するステークホルダーがどのような責任分界のもとビジネスモデルを構築するのかは現時点では明らかになっておらず、今後の課題になっていると考えられる。

3-3-1. 金融機関が関与する主な取組事例

。SSI/DID に関連して金融機関が関与している主な取組みとして以下の事例がある。

表 0-23：金融機関が関与する SSI/DID の主な取組事例[230]

国	金融機関	ユースケース	パートナー	金融機関の役割	概要
カナダ	カナダ主要 7 行	行政や生保等	SecureKey Technologies	銀行は IdP として参加	カナダ主要 7 銀行がコンソーシアムを構築し、Verified.me というサービスを 2019 年 5 月より提供。

[230] 各社プレスリリース、公表情報をもとに NRI 作成。

					主要 7 銀行が保有する本人確認情報等を生保等に連携。
スペイン	Banco Santander	レンタカー・保険・ローンの申し込み、行政への申し込み	CaxiaBank、MAPFRE(保険)、Repsol(エネルギー)、Alastria (非営利ブロックチェーンコンソーシアム)	ジョイントベンチャーが ID プラットフォームの役割を果たし、銀行本体は IdP として参加	安全で信頼性の高い ID プラットフォームにより、ユーザが個人情報をより細かく自らで制御できるようにすることで、プライバシーの保護と、ワンスオンリーによる利便性を提供。 現在は、実証実験の段階であり、2021 年 5 月にリリース予定。
	Veridas（BBVA と das-Nano の合弁会社)	金融	BBVA/Bankia/ Renta 4 Banko	高度な生体認証機能（顔、声、指紋等)、セキュリティの保護	銀行口座の開設や、オンライン取引時の生体認証などの機能を、BBVA を含めた各金融機関等に提供。
		行政	ナバラ州政府（スペイン）		行政手続きのオンライン化・顔識別技術による国境の管理・安全で高速の本人確認などの機能をナバラ州に提供。
ドイツ	Deusche Bank	行政・銀行・ヘルスヘア等	Deusche Bahn, Daimler, Lufthansa	ジョイントベンチャーが ID プラットフォームの役割を果たし、銀行本体は	他企業と出資して作り上げた Verimi が、デジタル ID プラットフォームとして、ID を一つに集約する役割を担い、銀行・行政・ヘルス

				IdP として参加	ケア・モビリティ・オンラインゲーム等にデジタル ID を用いたユースケースを提供する予定
英国	Barclays	行政（国民年金の受け取り等）	イギリス政府	GOV.UK のアイデンティティと連携	政府の GOV.UK 認証イニシアチブの一環として ID プロバイダと認定されており、ID 連携がなされているため、イギリス政府のサービスをうけるにあたっての本人確認を簡単化。
グローバル	MasterCard（カード）	通信会社の顧客の ID 管理	Optus（通信会社）	デジタル ID プラットフォームの提供	Optus は、MyOptus アプリをダウンロードしている約 600 万人の顧客に MasterCard の ID サービスを導入し、デバイスの購入・アカウントの変更・追加サービスの購入などに使用できる安全でポータブルなデジタル ID を提供。
		大学の試験における本人確認	郵便公社ディーキン大学		郵便公社の ID・アプリと、ディーキン大学のポータルサイトを用いてオンラインで試験を受ける学生の本人確認を実施可能。
		行政のデジタ	北マケドニア共和国		マケドニア国民が日常のさまざまな活動

		ル ID 連携			で使用できる、ローカルのデジタル ID と関連トラストサービスを提供することを目的としている。最初のアプリケーションの中には、新しい銀行口座のリモート開設をサポートする e-KYC 機能や新しい携帯電話アカウントが存在。
日本	JCB	本人確認・属性変更手続き等	富士通	決済や認証機能や、事業者間の資金精算などの運営スキームの知見を提供	ユーザ ID 情報の連携と活用を可能にするプラットフォームの共同開発の検討と、プラットフォームを活用した新たなサービスやビジネスモデルの検討を 2019 年 10 月より開始。
	JCB みずほ銀行	他事業者間の属性情報の連携・流通	富士通	JCB・みずほ銀行が保有する参加者の情報を各社から本人に開示。同時に、同システムを通して、参加者から開示された本人の情報を受領	2020 年 4 月から 2021 年 1 月に、複数事業者が持つ情報の管理や信頼性向上の観点から、ID 情報の相互運用モデルに関する実証実験を実施。

	JCB	オンライン身分証明書	慶應義塾大学 伊藤忠テクノソリューションズ Japan Digital Design 西日本電信電話 BlockBase	提供する決済サービスとの連携等	慶應義塾大学の学生を対象に在学証明書や卒業見込証明書などをスマートフォンアプリへ発行する、次世代デジタルアイデンティティ基盤の実証実験をマイクロソフトと連携して2020年10月から開始。

上記の主な取組事例のうち、国内外の有識者ヒアリングにおいて金融分野における SSI/DID の事例として示されることが多かったカナダの事例と、スペインの Banco Santander の事例について詳述する。カナダの事例の選定理由としては、既にサービスとして提供されており、金融分野における SSI/DID のユースケースの代表的な事例としてグローバルで認識されているためである。スペインの事例の選定理由としては、EU における SSI/DID の取組における先進的な取組みとして位置づけられているためである。

3-3-2. カナダ: Verified.Me

(1) Verified. Me の概要

カナダでは、SecureKey Technologies 社が、カナダの主要金融機関 7 社（BMO, CIBC, Desjardins, National Bank of Canada, RBC, Scotiabank and TD）のコンソーシアムと共に、Verified.Me というサービスを 2019 年 5 月から提供している。

Verified.Me は、プライバシーを尊重した「デジタルアイデンティティ・属性情報共有ネットワーク」である。本サービスは、ユーザがサービスにアクセスするために、トラステッドソース（金融機関、携帯電話事業者、信用情報機関、政府など）から、アイデンティティやアトリビュート情報を共有できるようにすることで、アイデンティティベリフィケーションプロセスの簡素化を実現できるものとして位置づけられている。

本ネットワークは、コンソーシアムが運営する許可型の分散型台帳をベースにする。具体的には、Linux Foundation のオープンソースである Hyperledger Fabric をベースにした IBM Blockchain Platform を使用して構築されており、他のネットワークとの相互運用性を可能にするために、W3C の標準（W3C DIDs and Verifiable Credentials）に準拠している。本サービスは、消費者は App Store や Google Play からアプリをダウンロードして無料で利用できる。

図 0-41：Verified.Me のサービス全体像[231]

Verified.Me の基本的な仕組みは以下の通り[232]。

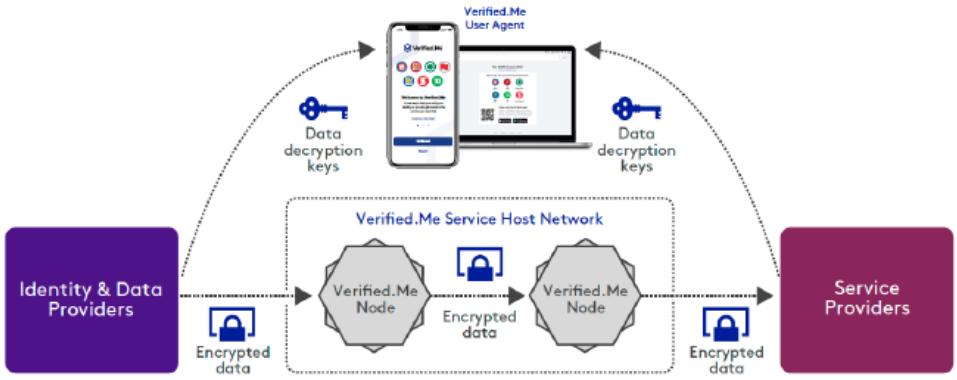


図 0-42：Verified.Me の仕組み[233]

アイデンティティ＆データプロバイダー）（IDPs）はサブジェクトに関する特定の情報を生成または保持する Verified.Me に参加するカナダの適格組織である。IDP の例としては、金融機関、信用情報機関、電気通信プロバイダ、およびその他の適格なトラステッドソースが該当する。

---

[231] DIACC, "DIACC Identity Networks Paper Verified.Me by SecureKey Technologies Inc., Self-Assessment," https://diacc.ca/wp-content/uploads/2020/05/DIACC-Identity-Networks-Paper-Self-Assessment_SecureKey-VerifiedMe.pdf

[232] DIACC, "DIACC Identity Networks Paper Verified.Me by SecureKey Technologies Inc., Self-Assessment," https://diacc.ca/wp-content/uploads/2020/05/DIACC-Identity-Networks-Paper-Self-Assessment_SecureKey-VerifiedMe.pdf

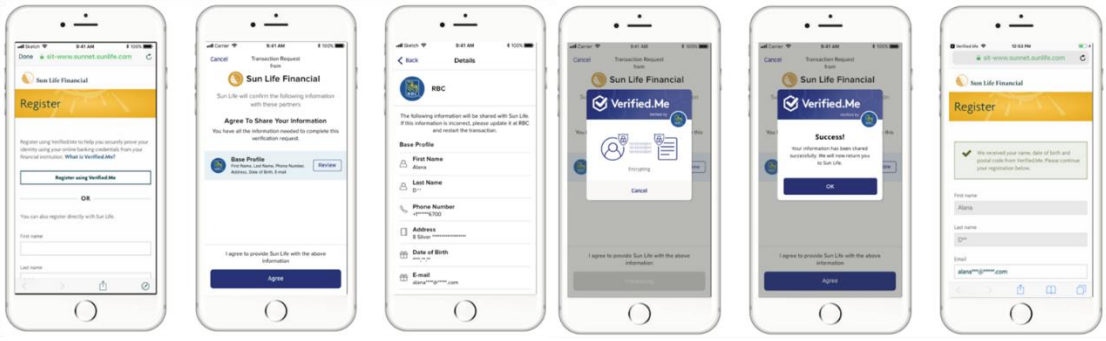
[233] DIACC, "DIACC Identity Networks Paper Verified.Me by SecureKey Technologies Inc., Self-Assessment," https://diacc.ca/wp-content/uploads/2020/05/DIACC-Identity-Networks-Paper-Self-Assessment_SecureKey-VerifiedMe.pdf

リライングパーティ(RP)またはサービスプロバイダは、Verified.Me に参加するカナダの適格な組織であり、Verified.Me を通じてユーザに特定の情報の提供を求める。Verified.Me は、サービスプロバイダが、主体に対してサービスや製品を提供する際のアイデンティティや適格性をベリファイすることを支援する。

金融機関の IDPs は、カナダの主要金融機関 7 社で、Verified.Me サービスへのアクセスを希望するサブジェクト（ユーザ）の認証、およびネットワークのコアコンポーネントのホスティングを担当する。一部の金融機関はサービスホストとしてネットワーク上の分散ノードを運営し、一次 IDP としても機能する

Verified.Me のユーザエージェントは、サブジェクトが Verified.Me ネットワークにアクセスし、ネットワーク（モバイルアプリまたは Web ブラウザ）を介してサブジェクトの属性情報の共有に同意するために提供されるツールである。

Verified.Me の利用イメージとして、生保会社（Sun Life Financial）契約時に、銀行（RBC）の本人確認情報を連携して利用する際は以下のような流れで情報が連携される。



・ 生保会社のサイトから“Register using Verified.Me”を選択
・ Verified.Meに登録されているアイデンティティ情報を選択（この場合はRBC）
・ RBCに登録されているアイデンティティ情報を確認
・ 連携を実行
・ RBCのアイデンティティ情報の連携が成功
・ 生保会社に情報が連携され、登録完了

図 0-43：Verified.Me のサービス利用イメージ[234]

Verified.Me のサービスが創出された背景として、カナダでは、口座開設時に対面での本人確認を実施している点、KYC 情報の更新をしないと口座が凍結されてしまうという事情もあり銀行の本人確認情報が鮮度・精度ともに高い状態になっている点が挙げられ、銀行としてもこうした KYC 情報を上手く活用するという発想があった。

SSI/DID としての Verified.Me の特徴は、本サービスが SSI に基づくモデルではあるが、一般の SSI よりも更に厳しいモデルを取っていることである。SecureKey 社はこれを「Triple Blind」と呼ぶ。すなわち、本サービスモデルに参画する 3 者（Identity & Data Provider,

[234] iPhone in Canada, "Verified.Me App Launches in Canada: Digital Identity Service for Big Bank Customers," (May 2019), https://www.iphoneincanada.ca/news/verifiedme-launch-canada/

Service Provider, Network Operator）のいずれもが、ユーザが連携する情報がどこからどこに提示されるのか分からないような設計となっている。一般に SSI のモデルは、リライングパーティ側はどこの Identity 情報が使われているのかについては制限しないため、この点でより強固なプライバシー設計となっている。

ユースケースとしては、主なサービス利用者（サービスプロバイダー）は、政府機関や生保等に限られているが、Nationwide な ID インフラとなることを目指している。

（2）カナダのデジタルアイデンティティ概要

カナダでは、政府・民間企業とで構成される DIACC（Digital ID & Authentication Council of Canada）が、デジタルアイデンティティと認証フレームワークの開発に取組んでいる。DIACC の設立の背景には、カナダ財務省が、デジタル時代の金融システムの見直しを目的に立ち上げた「決済システムレビュータスクフォース」が 2011 年 12 月に策定した報告書がある。本報告書では、以下の提言がなされている[235]。

> カナダの決済システムを大幅に近代化するためには、消費者の行動から会計ソリューション、政府がサービスを提供する際に依拠している手続きに至るまで、さまざまな分野で変化が必要である。産業界は、不確実性や協調性の欠如もあって、変革を実施していない。したがって、カナダ政府は、以下のような行動をとることで、変化をリードする必要がある。
> - すべての政府機関のサプライヤーと受益者に電子請求書と電子支払（EIP）を導入する。
> - 民間企業と協力してモバイルエコシステムを構築する。
> - 近代的な決済システムを支え、カナダ人のプライバシーを保護するために、「デジタルアイデンティフィケーションおよびオーセンティフィケーション（DIA）」制度の構築を推進する。

本提言を踏まえ、検討組織として官民組織による非営利組織として DIACC が 2012 年に設立された。DIACC は財務省のタスクフォースの提言などが背景にあることから、メンバー企業には金融機関等も多く占める[236]。

---

[235] Task Force for the Payments System Review, "Moving Canada into the Digital Age," (December 2011), https://www.canada.ca/content/dam/fin/migration/n12/data/12-030_1-0_eng.pdf

[236] 設立初期時の DIACC ボード組織は以下の組織。
TD Bank Group, CIBC, BMO, ScotiaBank, Rogers, TELUS, Government of Canada, Province of Ontario, Province of British Columbia, Equitable Bank, RBC, Interac, Equifax, Canada Post, BlackBerry, Desjardins, SecureKey, Central 1 Credit Union

DIACC 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 Pan-Canadian Trust Framework (PCTF)を開発し、2020 年 11 月に PCTF 1.0 alpha の運用をローンチしている[237]。PCTF は、アイデンティティ管理を既存のアナログからデジタルに移行する際に求められる基本原則や基準を策定し、政府機関や事業者がリファレンスアーキテクチャとして参照できるようにすることを目的に策定されている[238]。PCTF には法的強制力はなく準拠は任意であるが、デジタルアイデンティティのトラストフレームワークとして、カナダ国内のみならずグローバルでも注目されている。

図 0-44：PCTF の構成要素[239]

また、DIACC は 2021 年 2 月に分散型アイデンティティがどのように PCTF に準拠するのかについてのガイドラインも公表している[240]。

なお、デジタルアイデンティティサービスを提供する事業者は、PCTF への準拠状況をセルフアセスメントし、その結果を公表することで、利用者への安全性等に関する説明責任を

DIACC, "Digital ID & Authentication Council of Canada Launched," (May 2014), https://diacc.ca/2014/05/12/digital-id-authentication-council-canada-launched/

[237] DIACC, "DIACC 2020 Year-End Achievements and Milestones," (December 2020), https://diacc.ca/wp-content/uploads/2020/12/DIACC-Year-End-Achievements-and-Milestones-2020-Final.pdf

[238] DIACC, "Pan-Canadian Trust Framework Model," (September 2020), https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation_V1.0.pdf

[239] DIACC, "Pan-Canadian Trust Framework Model," (September 2020), https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation_V1.0.pdf

[240] DIACC, "Decentralized Identity and DIACC PCTF Authentication," (February 2021), https://diacc.ca/wp-content/uploads/2021/02/Decentralized-Identity-and-DIACC-PCTF-Authentication.pdf

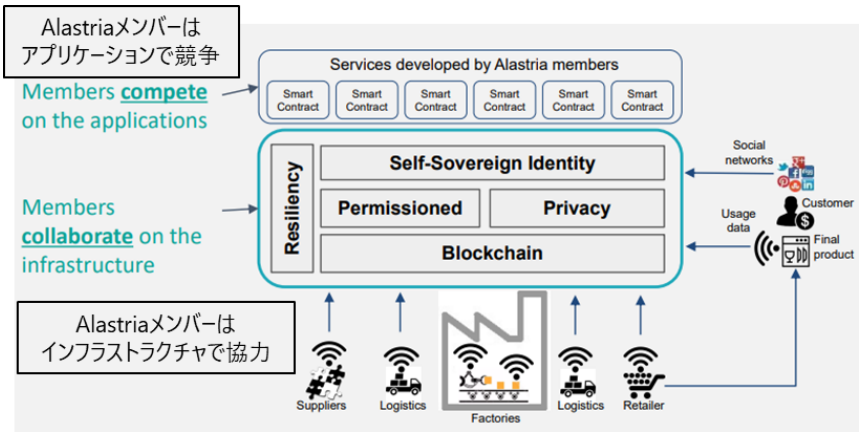
果たしている。例えば、前述の Verified.Me について、SecureKey 社もセルフアセスメント結果を公表している[241]。

3-3-3. スペイン: Alastria/ Dalion

スペインでは、スペイン政府によるデジタルアイデンティティとして DNI(Documento National de Identidad)の他に、Alastria による SSI のデジタルアイデンティティのモデルとして Alastira_ID が存在し、Alastria_ID をベースとしたプロジェクトとして Dalion が始動している。

DNI 3.0 とは、スペイン政府（国家警察総局）が発行する身分証明書である[242]。従来の DNIe から 2015 年頃より移行しており、IC チップによって接触型ないし非接触型（NFC）でデータを利用可能である。格納データは、氏名等情報、顔写真、サイン、指紋、電子署名証明書、DNI 証明書で、身分情報の提示や電子署名の付与等に使用可能である。

一方で、Alastria_ID は、2017 年に発足した非営利団体の Alastira により、2018 年からプロジェクトが開始された SSI のデジタルアイデンティティのモデルである[243]。Alastria のメンバー数は 550 近くで、主にスペイン（一部はイタリアやドイツ）の金融業含む企業、公共機関、大学等が参加している。Alastria_ID そのものは Alastira のメンバーによって運営されるブロックチェーンを用いたオープンソースモデルかつ EU 圏での法的有効性を持つ自己主権型アイデンティティ基盤でもある[244]。



---

241 DIACC, "DIACC Identity Networks Paper Verified.Me by SecureKey Technologies Inc., Self-Assessment," (May 2020), https://diacc.ca/wp-content/uploads/2020/05/DIACC-Identity-Networks-Paper-Self-Assessment_SecureKey-VerifiedMe.pdf

242 スペイン国家警察総局, "Dni y Pasaporte," https://www.dnielectronico.es

243 Alastria https://alastria.io/

244 Alastria, "AlastriaID," https://github.com/alastria/alastria-identity/wiki

図 0-45：Alastria_ID の役割分担[245]

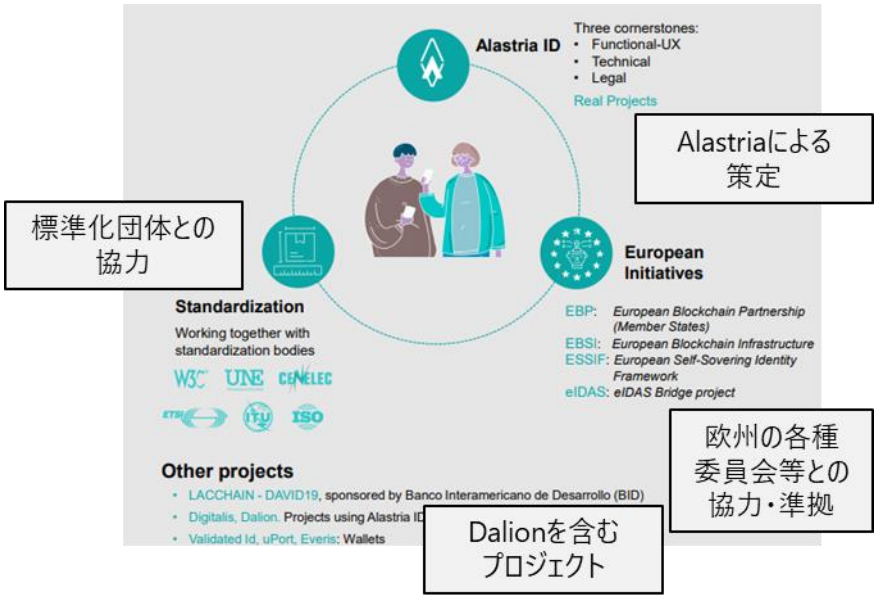
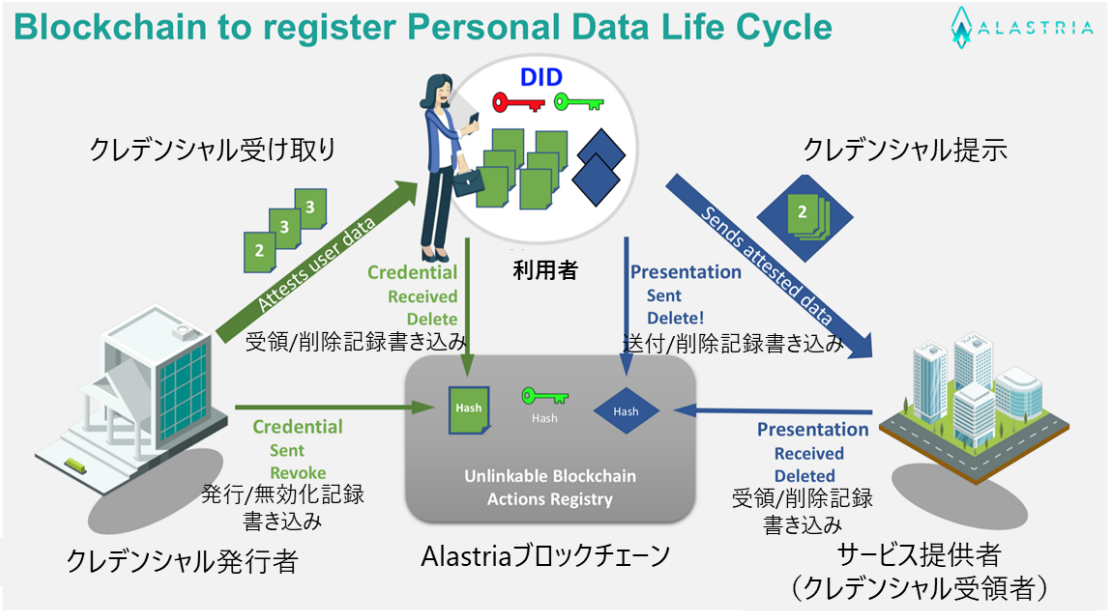


図 0-46：Alastria_ID の特徴[246]



[245] Alastria, "Alastria Digital Identity An ongoing project," (September 2019), https://portal.r2docuo.com/alastria/document?L3110FC15F

[246] Alastria, "Alastria ID Compatibility and interoperability," https://portal.r2docuo.com/alastria/document?L097EBB43D

図 0-47：Alastria_ID 利用概観図[247]

Alastria_ID は欧州圏においての法的有効性を持った自己主権型デジタルアイデンティティのインフラと開発フレームワーク提供を目的とし、スペインの標準化団体（UNE）や欧州電気標準化委員会に提出され、さらに ESSIF（European Commission's Self-Sovereign Identity Initiative）にも影響を与えている[248]。EU 圏における法的有効性を確保するため、eIDAS 規制、ブロックチェーンを用いた自己主権型アイデンティティのフレームワークとしての欧州委員会による SSI eIDAS 法的レポート、EUBOF（EU Blockchain Observatory and Forum）による e-Identity ワークショップレポート、EUBOF と欧州議会によるブロックチェーンと GDPR に関するレポート等に準拠している。

また、Alastira_ID は一般的な SSI/DID と同様にクレデンシャル発行者（Issuers）、ユーザ、サービスプロバイダーに役割分担がなされ、クレデンシャルに関する操作などが Alastria のブロックチェーンに書き込まれ、ブロックチェーン上の記録を用いてクレデンシャルの真正性を検証することができる。

Dalion は Alastria_ID をベースとしたプロジェクトで、2019 年に開始し、2020 年に PoC を実施し、2021 年 5 月にサービス提供開始予定である[249]。サンタンデール銀行を含めた多数の銀行業、保険業、証券取引所等が参画し、地方自治体や大学等もオブザーバー参加している。検証済みの属性情報の受け渡し、つまり他銀行等による本人確認結果を転用可能にして本人確認の手間削減が目標となっている。なお、開発時点では Alastria の Ethereum-Quorum ブロックチェーン上で動作する。

Dalion の利用者へのメリットとしては、個人の情報を自ら管理できること、新規サービス登録・利用時の情報入力の手間が削減されること、アイデンティティ盗難対策などが挙げられる。参加企業へのメリットとしては、利用者登録手続などの効率化、悪意ある利用者による詐称対策、参加企業間の新規ビジネスモデルの開発とユーザエクスペリエンス向上が挙げられる。

3-4. SSI/DID の長所と実現に向けた課題

---

247 Alastria Blockchain Ecosystem, "La identidad digital de Alastria presenta su primer MVP," (March 2020), https://alastria-es.medium.com/la-identidad-digital-de-alastria-presenta-su-primer-mvp-696750d687ac

248 Santander, "Ten Spanish companies join forces to promote digital identity using blockchain technology," (November 2020), https://www.santander.com/en/press-room/press-releases/2020/11/ten-spanish-companies-join-forces-to-promote-digital-identity-using-blockchain-technology

249 Santander, "Ten Spanish companies join forces to promote digital identity using blockchain technology," (November 2020), https://www.santander.com/en/press-room/press-releases/2020/11/ten-spanish-companies-join-forces-to-promote-digital-identity-using-blockchain-technology

3-4-1. SSI/DID 活用のメリット

SSI モデルを用いる主要なメリットとしては、1．自己制御権の獲得、2．プライバシーへの配慮、3．利便性の向上と業界全体のコスト抑制、の 3 点が期待される。

1. 自己制御権の獲得とは、自身が ID プロバイダとなりクレームの管理を行うことで、CP が発行した自身のクレームに対する自己制御権を獲得することを意図する。例えば、以下のような点が上げられる。
   (ア) 悪意を持った ID プロバイダによるアイデンティティ停止措置を受けなくなる
   (イ) クレームを自身のウォレットに取得しておき、(クレームの真正性検証に必要な) CP の署名検証鍵を、耐改ざん性を有し信頼できる形で保持可能な分散リポジトリ等に長期保管することで、CP の動態に依存せずユーザの意図せぬ更新（改ざん）を受けない、クレームの保持・展開が可能となる
2. プライバシーへの配慮とは、既存 ID プロバイダ内での処理を最小化（Recognition 処理に限定）し、データ連携における明確な同意管理やデータミニマイゼーション実現策としての活用、そして自身の意思で保持するクレーム削除を行うことで「忘れられる権利」行使の実現策としての活用可能となることを意図する。
3. 利便性の向上と業界全体のコスト抑制とは、一度オンボーディングを行ったクレームを複数 RP に対し活用することで、オンボーディングの機会を減らし、利便性向上と業界全体のコスト抑制に貢献することを意図する。ユーザのウォレットをハブに複数 CP/RP 間でクレームが連携されることで、上記実現が期待される。

上述の SSI モデルでのメリットと、3-1-2 で述べた SSI/DID の 4 つの特性の対応関係は以下の通りとなる。

表 0-24：SSI/DID モデルのメリットと SSI/DID の特性との対応

メリット	概要	SSI/DID の特性との対応			
		認証と属性の分離	分散情報活用・選択的提示	提示先の秘匿	長期の保管・利用
自己制御権の獲得	悪意を持った ID プロバイダによるアイデンティファイアのロックアウト処置を受けない。 以下の実現により、ID プロバイダの動態に依存しない／ユーザの意図せぬ更新（改ざん）を受	○	○		○

	けない、クレームの保持が可能となる。 ● クレームを自身のウォレットに取得。 ● クレームプロバイダーの署名検証鍵（クレームの真正性検証に必要な）を耐改ざん性を有し信頼できる形で保持可能な分散リポジトリ等に長期保管。				
プライバシーへの配慮	既存 ID プロバイダ内での処理の最小化（Recognition 処理に限定)。 データ連携における明確な同意管理やデータミニマイゼーション実現策としての活用、自身の意思で保持するクレーム削除を行うことで「忘れられる権利」行使の実現策としての活用。 クレームプロバイダーに対し、クレーム提示先の秘匿が可能（Need to know の原則を遵守可能)。	○	○	○	
利便性の向上／業界全体のコスト抑制	一度取得したクレームを複数リライングパーティに展開が可能（顧客の利便性向上に寄与)。 複数クレームプロバイダーからのデータ連携を可能にすることで、業界全体でのオンボーディングコスト抑制に寄与。	○	○		

上記のそれぞれのメリットについて、3-3-2 で取り上げたカナダの Verified.Me での対応状況を SSI/DID の特性ごとに述べる。

自己制御権の獲得のメリットとして、認証と属性の分離がなされることで、ユーザエージェントにて格納された属性はユーザのコントロール下になっており、CP の管理外となっている。分散情報活用・選択的提示については、ユーザエージェントにて選択的提示を可能と

する実装がなされている。長期の保管・利用については、実施有無含め詳細不明である。なお、本特性を有するその他事例としては、例えば、慶應義塾大学が JCB 等と取り組む「オンライン身分証明書」のユースケースでは「永続的に検証可能な属性提供基盤」が一つの特徴と位置付けられている。

プライバシーへの配慮のメリットとして、認証と属性の分離については、既存 IDP 内での処理の最小化（認証処理に限定）する機能が実装されている。分散情報活用・選択的提示については、ユーザエージェントにて選択的提示を可能とする実装がなされており、ユーザ同意に基づく処理を実現している。提示策の秘匿については、RP に対してどの IdP から取得した属性か分からないような匿名処理を実現する機能が実装されている。

最後に、利便性の向上と業界全体のコスト抑制認証のメリットとして、属性の分離については、取得したクレームがユーザエージェントに格納され、複数の RP にクレーム展開可能な実装となっている。分散情報活用・選択的提示については、複数 CP からデータ連携を可能とすることで RP 側での本人確認にかけるコストを大幅に削減できるようになっている。

3-4-2. SSI/DID の技術面の課題

SSI/DID の技術面の課題については、DID を構成する各レイヤーにおいて、トラスト、相互運用性、セキュリティの観点で以下の通り整理を行った。

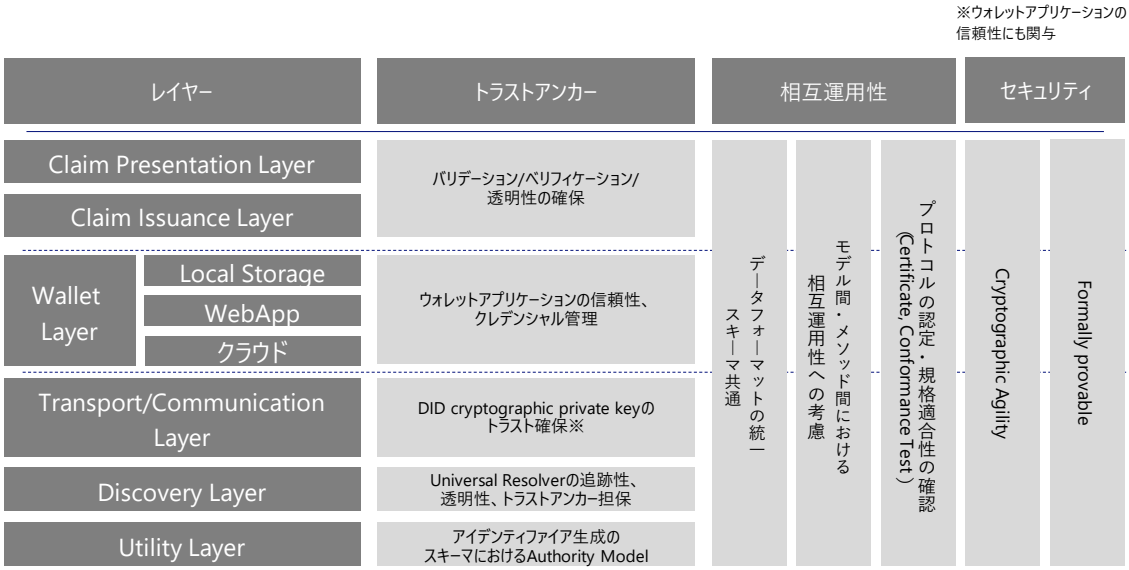


図 0-48：SSI/DID モデルの技術面の課題

また、標準化団体によってレイヤーの実現方式は異なり、既存方式の活用と展開における課題と、新規方式検討における課題の両面から技術的課題への対策の検討が必要となる。各レイヤーに対する実現方式例として、例えば以下のような組み合わせが考えられる。

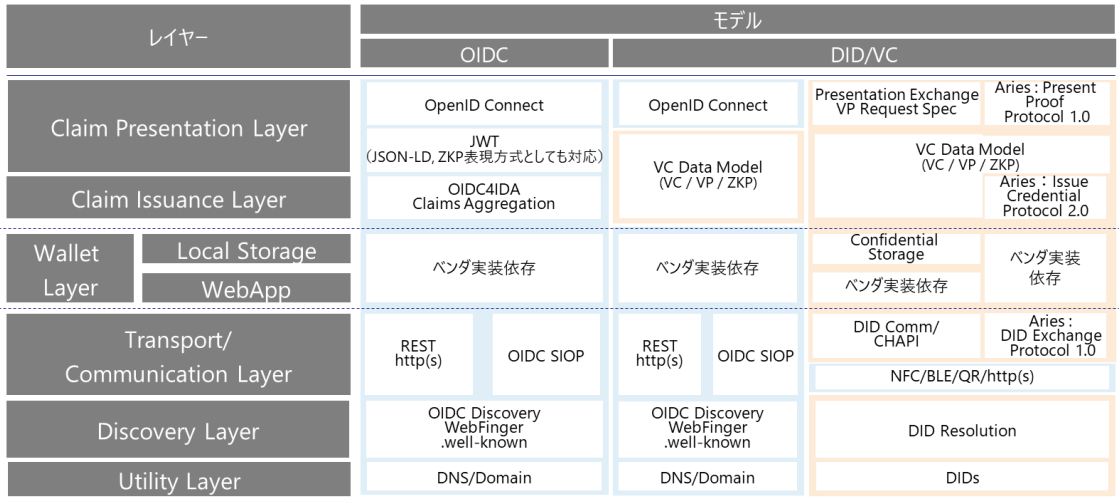


図 0-49：各レイヤーに対する実現方式例

なお、実現方式は上の図の組み合わせに限定されるものではなく、例えば 3-2 で述べた OIDF と DIF リエゾン協定等、各標準化団体においても各スタックに対する実現方式の組み換えに関する議論が行われている。

（1）バリデーション/ベリフィケーション/透明性の確保

SSI/DID の技術面の Claim Presentation と Claim Issuance レイヤーでのトラスト観点での課題として、クレームに対するバリデーション、ベリフィケーション、透明性の確保が挙げられる。SSI/DID はクレームに対し、有効状態（失効されていない）かを確認するバリデーション、改ざんされていないかを検証するベリフィケーション、生成時に準拠したトラストフレームワークが確認できる透明性、の確保が重要となる。バリデーションについては、ブロックチェーン等の分散リポジトリ上にクレームの失効情報を展開し、RP 側で参照する、といった実現方式が考えられる。一方で、Certificate Revocation List （CRL）で用いられている有効期限切れの情報は排除される等サイズ肥大化への対処措置を、ブロックチェーンの様に Immutable な特性を持つ方式で実現する場合は、実装面での考慮が必要となる。ベリフィケーションについては、クレームに対し、CP が署名を実施、RP が署名検証を行うことでの実現方式が考えられる。そして、透明性についてはクレーム自体に、生成時に CP が準拠した法的要求事項、トラストフレームワーク、商業的合意等を記載し、RP が内容を確認可能とする ”OpenID Connect for Identity Assurance” プロトコル等、透明性を持つ仕様活用による実現方式が検討されている。

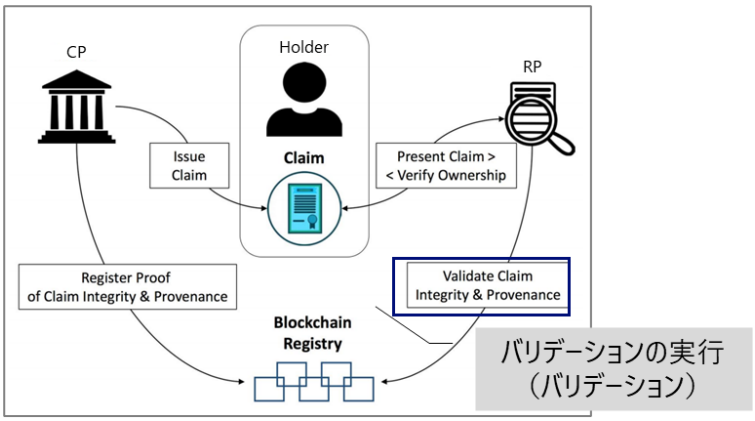


図 0-50：分散リポジトリへのバリデーション実施[250]

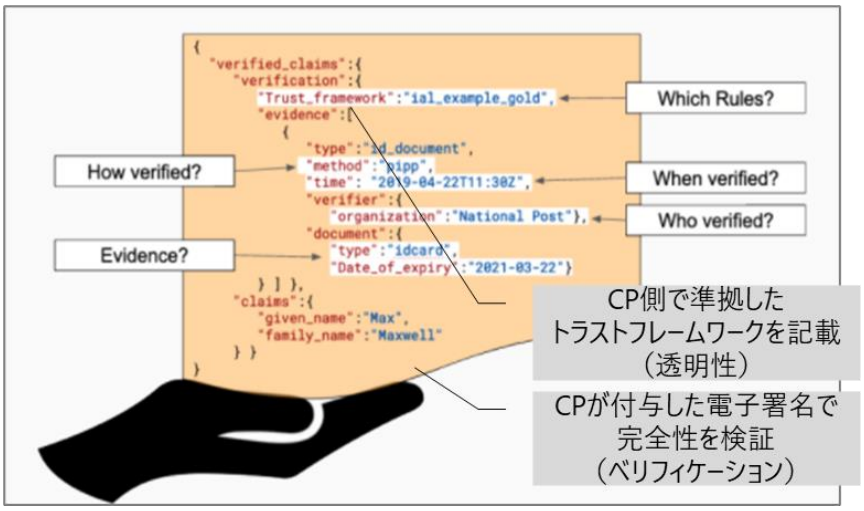


図 0-51：OpenID Connect for Identity Assuranace を用いたクレームの ベリフィケーション・透明性の確保[251]

（2）ウォレットアプリケーションの信頼性、クレデンシャル管理

ウォレットレイヤーでのトラストの観点においての課題としては、ウォレットアプリケーションの信頼性の担保が挙げられる。ウォレットアプリケーションの信頼性確保（保証）には、保証の起点となりうるトラストアンカーからの認証パスチェーン確保が必要となる。想定されるトラストアンカー候補として、例えばデバイス内の下位レイヤーからの認証パスチェーン構築、第三者機関による評価プログラムを通じた評価、そして Deeplink 等を用いた母艦アプリ等からの呼出しが挙げられる。

---

250 decentralized-id.com 資料を基に作成

251 OpenID Foundation, "eKYC & Identity Assurance WG," https://openid.net/wg/ekyc-ida/

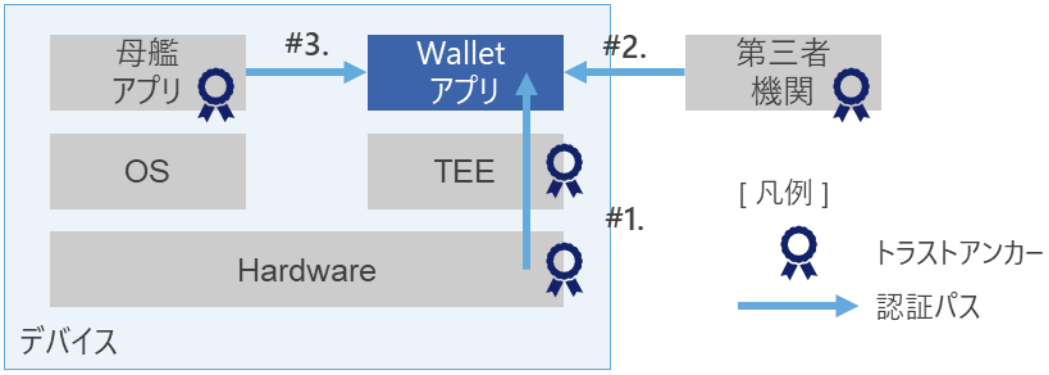


図 0-52：ウォレットアプリケーションの信頼性の担保

デバイス内の下位レイヤーからの認証パスチェーン構築は、OS/TEE などセキュアエレメント内に格納された署名鍵を使って処理結果への署名・署名検証を実施し、下位レイヤーからのトラストを構築する。この方法では、特定モデルや製品への依存が発生すること、ポータビリティ確保が困難であること、そしてハードウェアや OS ベンダーの協力が不可欠であることが課題として挙げられる。

第三者機関による評価プログラムを通じた評価は、iOS の App Store、Android の Google Play Store 等の第三者機関がアプリを確認する。この方法での課題としては、第三者機関の検証プログラムに依存すること、別チャネルからの取得によるバイパスが可能であること、そして、第三者機関の意向によるウォレットアプリの排除があり得ることが挙げられる。

Deeplink 等を用いた母艦アプリ等からの呼出しは、ウォレットをミニアプリとして、信頼された母艦アプリから呼び出すことである。この方法を事後導入で行う場合は第三者機関による評価プログラムを通じた評価と同じ課題が想定されるほか、事後導入でなければ母艦アプリのプリインストールが必要となる。

エコシステムとしての提供を考慮すると、デバイス内の下位レイヤーからの認証パスチェーン構築が望ましい。他方、同仕様の実現には、ハードウェアや OS ベンダー等のプラットフォーマーの協力が不可欠となる。

（3）Universal Resolver の追跡性、透明性、トラストアンカー担保

Transport/Communication と Discovery レイヤーでのトラスト観点の課題としては、Universal Resolver の追跡性や透明性とトラストアンカーの担保が挙げられる。これはすなわち DNS のルートサーバからの DNS 解決と同様な Resolver のトラストアンカーの担保を行う方法の議論が起こりうることである。エコシステムとしての可用性維持や信頼性担保への考慮が必要になるほか、ICANN におけるドメイン取得時の管理等、同等の運用・管理要件が想定される。

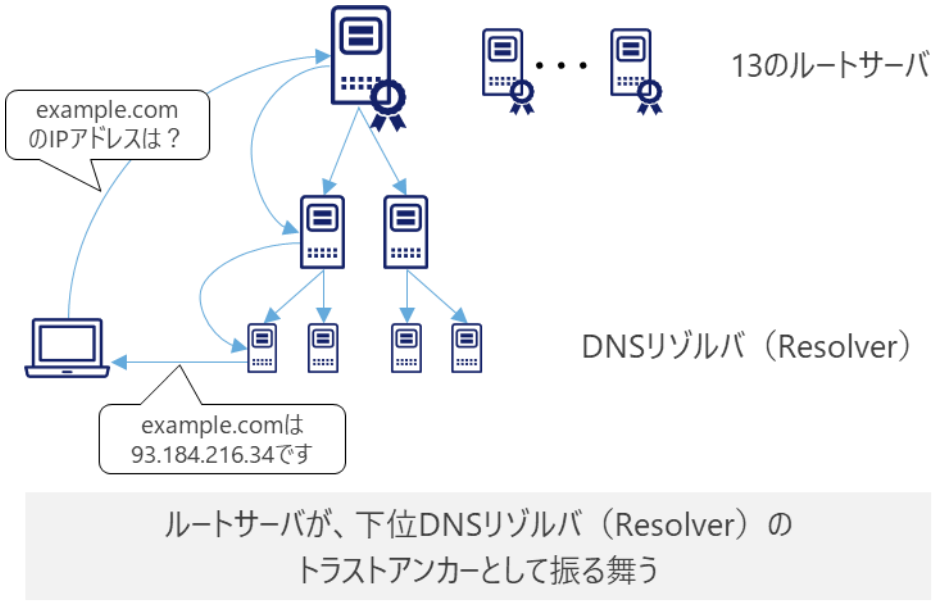


図 0-53：DNS の解決（Resolve）概観

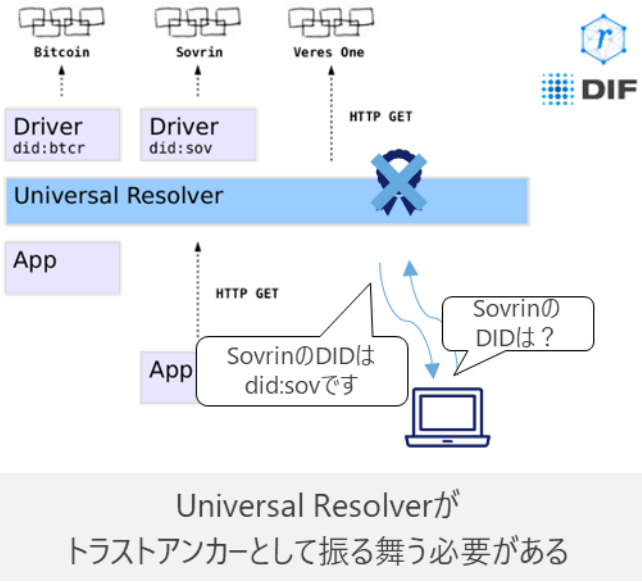


図 0-54：Universal Resolver の概観[252]

（4）アイデンティファイア生成のスキーマの Authority Model

[252] Markus Sabadello, "A Universal Resolver for self-sovereign identifiers," (November 2017), https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c

Utility レイヤーのトラストの観点での課題としては、アイデンティファイア生成におけるスキーマの Authority Model が挙げられる。これは、Authority Model と SSI 思想との相反（Subjective consensus）が起こりうることである。既存の IDP によるアイデンティティ生成時においては、複数の Authority Model が存在するが、SSI/DID で自己主権となった場合においても、どこまでレジストリに権限を持たせるかや、統制を効かせるかの考慮が必要となりうる。

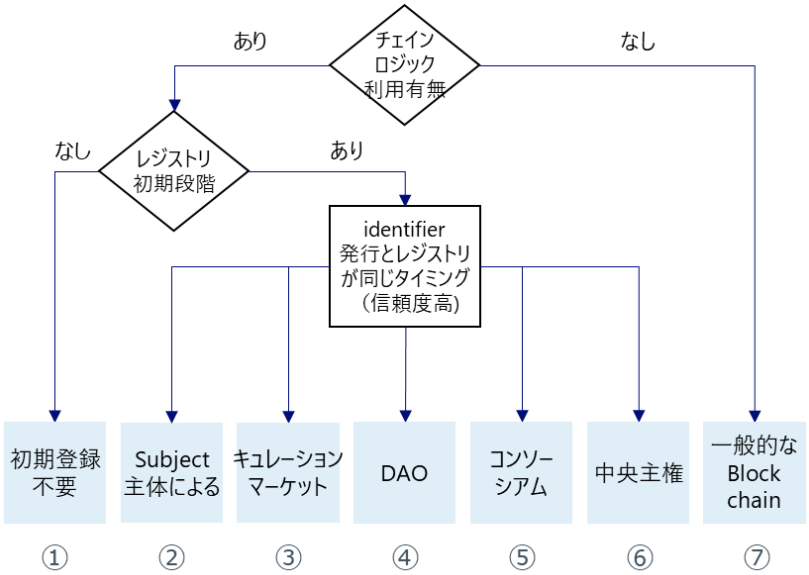


図 0-55：Identifier のレジストリモデル [253]

Identifier のレジストリモデルの種類と特徴は以下の通り。

表 0-25：Identifier のレジストリモデルの種類と特徴[254]

種類	特徴
初期登録不要	特定の状況下のみでアイデンティファイアを台帳に登録する。
Subject（主体）	自己登録で、CP が発行したクレデンシャルを受け取るエンティティである Subject がレジストリを管理する。

[253] NIST, "A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems," (January 2020), https://csrc.nist.gov/publications/detail/white-paper/2020/01/14/a-taxonomic-approach-to-understanding-emerging-blockchain-idms/final

[254] NIST, "A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems," (January 2020), https://csrc.nist.gov/publications/detail/white-paper/2020/01/14/a-taxonomic-approach-to-understanding-emerging-blockchain-idms/final

Curation market	参加者による許可の実装管理の度合いにより変動しうる。 Curation market はレジストリの判断を参加者が投票で決める。 DAO は単一ではないエンティティがチェーン上のレジストリとロジックを用いて管理する自己持続可能な組織型構成。 Consortium は政府、企業、個人（自身）以外のエンティティがレジストリの判断を担う。
DAO (Decentralized Autonomous Organization)（分散自律団体）	
Consortium（共同事業体）	
中央主権	単一ないし一体化したエンティティがレジストリを管理する。
一般的なブロックチェーン （チェインロジックなし）	チェインロジック（例：スマートコントラクト）のない一般的なブロックチェーンを使ったアイデンティティ登録が行われる。

（5）データフォーマットの統一スキーマ共通

レイヤーを問わず、相互運用性の観点での課題として、まずはフォーマット、スキーマ、プロパティ等の共通化や統一化が挙げられる。フォーマット、スキーマ、プロパティ等の統一化がなされていない状態だと、データ連携時における個別スキーマの参照や独自のパース処理実装等、開発が非効率となるため、極力仕様の共通化や統一化が進むことが望ましい。なお、共通化や統一化に際しては、標準技術仕様としての策定範囲と、業界・業種等ユースケースに応じた関連団体等で定める範囲との、境界を意識した策定範囲の議論が必要となる。

OpenID Connect や金融 API 等ではフォーマットの統一とスキーマが共通されることで、データの受け渡しを容易化している。具体的には、OpenID Connect におけるクレームのやり取りで広く用いられる JWT（JSON Web Token）は、 RFC7519 として策定され、スキーマとしてアイデンティティインフォメーションの各種データや扱い方法のフォーマットを定め、相互運用性を保っている。また、日本でも『電子マネー分野のオープン API に係る電文仕様標準』が策定され、接続事業者によるデータ利用を推進している。

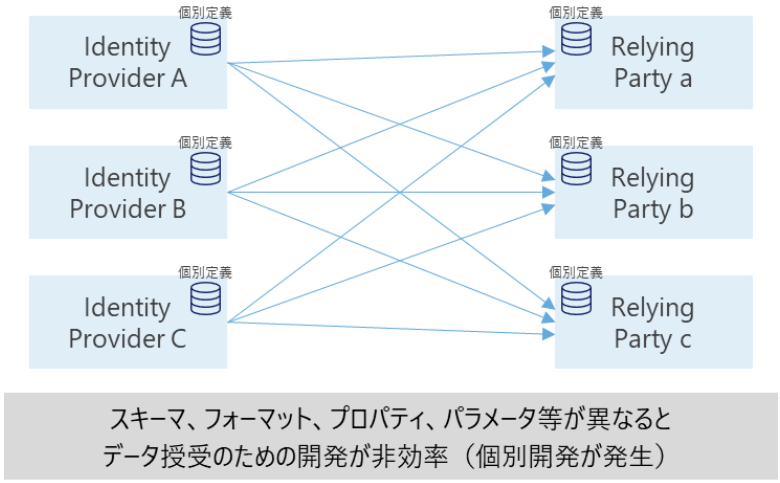


図 0-56：個別フォーマット・スキーマ等が定義された状態でのデータ連携

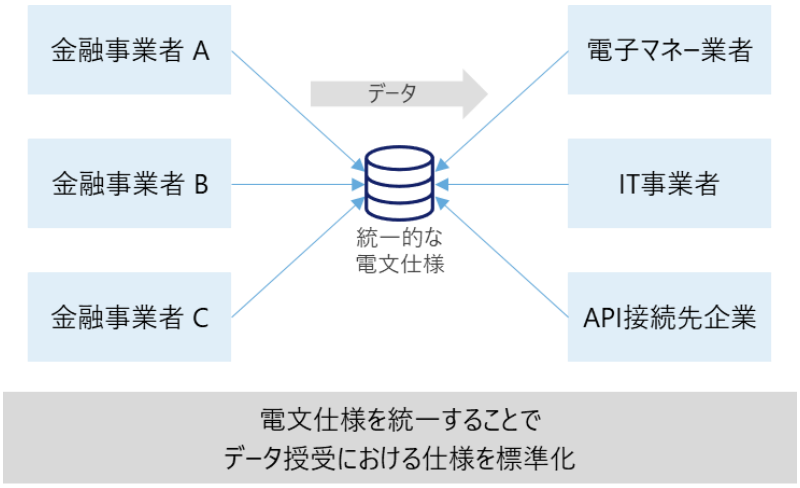


図 0-57：統一フォーマット・スキーマ等が定義された状態でのデータ連携

（6）モデル間・メソッド間における相互運用性への考慮

相互運用性の観点でのもう一つの課題としては、モデル間やメソッド間における相互運用性と、スケーラビリティへの考慮が挙げられる。具体的にはクレーム連携では、異なるモデル間、さらに SSI モデルでも異なるメソッドを意識した相互運用性の確保が必要となることがある。既存事業者のインターフェースにおいてフェデレーションモデルの SSI/DID の相互運用性が考慮する場合、SSI/DID への対応が追加投資となりうる。また、SSI/DID では DID メソッドごとに DID スキーム、DIDs と DID ドキュメントの生成・リゾルブ・更新・無効化の方法が定められており、スキームや方法が異なる場合には連携処理が困難となる。

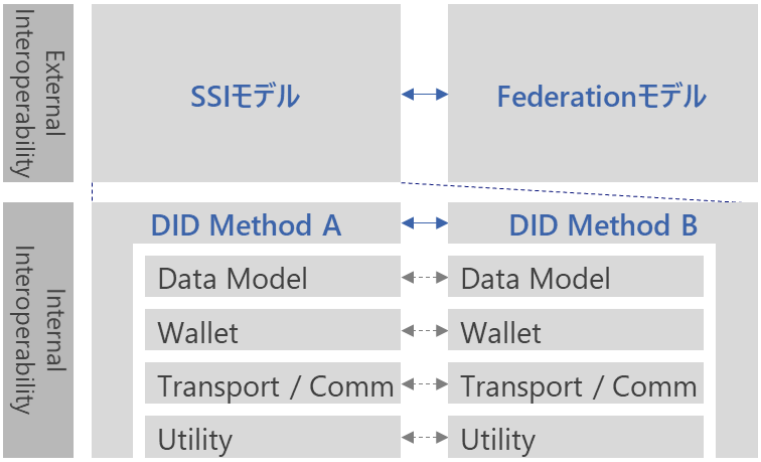


図 0-58：総合運用性の考慮対象例

SSI モデルとフェデレーションモデルの互換性を持つためには、以下の図の Gateway 機能を持ったモジュールによるスイッチング等の変換処理の考慮が必要となる。他方、SSI モデルは多数の仕様策定が進んでおり、対応するメソッド数によっては、スイッチング機能開発や運用コストが膨大となる懸念がある。

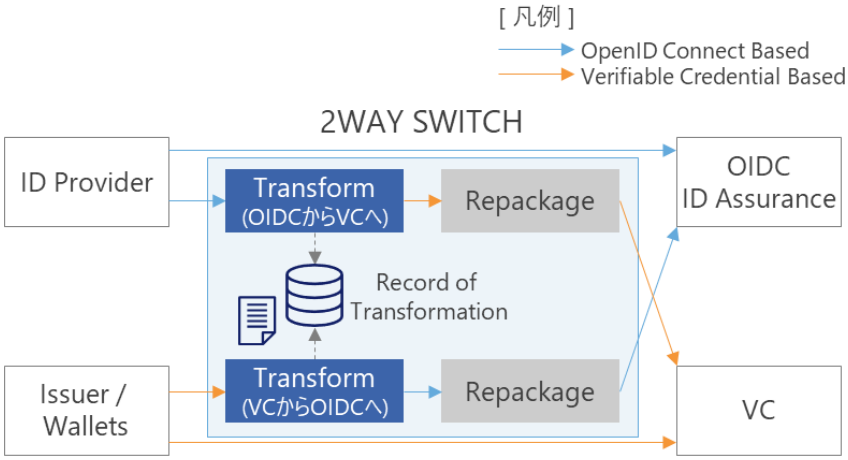


図 0-59：モデルのスイッチング事例イメージ[255]

（7）プロトコルの認定・規格適合性の確認（Certificate, Conformance Test）

相互運用性の観点で、DID の認定や規格適合性も課題として挙げられる。既存の標準技術での取り組み同様に、標準化推進の為の施策として、相互運用性や仕様充足性等、透明性を具備し実装負荷を抑える認定制度や規格適合性テストの提供の考慮が望ましい。標準の認定と規格適合性確認の事例としては、1 章で紹介した FIDO の UAF、U2F、FIDO 2

[255] OIX Quarterly Workshop - 15th Dec 2020 を基に NRI 作成

は適合性、相互運用性、セキュリティ機能を FIDO Alliance によって認定するプログラムが提供されている。また、認定プログラムの一環として自己評価を行うテストツールが提供されており、実装が仕様に準拠していることを確認できる。認定プログラムによって、例えば FIDO2 認定サーバは異なるベンダーによって製造されて認定された任意の FIDO2 認証器を用いられるようになる等、相互運用性が担保されている。他には、OpenID Foundation によって策定されている OpenID Connect や FAPI（Financial-grade API）についても、実装での相互運用性の担保のために規格適合性テストの提供と認定プログラムの実施がなされている。規格適合性テストでは HTTP のリクエストやレスポンス、サーバ設定や鍵の確認等、仕様に照らし合わせて動作を検査する。

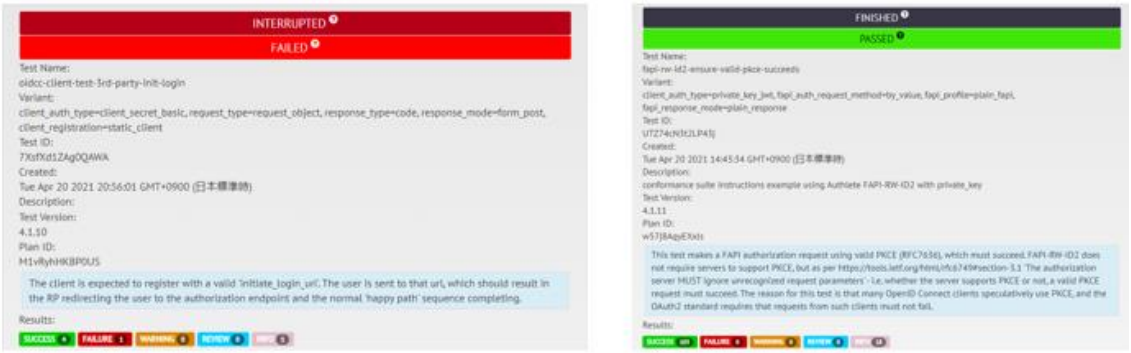


図 0-60：OpenID Foundation から提供されている規格適合性テストイメージ[256]

（8）Cryptographic Agility

セキュリティ観点の課題としては、Cryptographic Agility への考慮が挙げられる。一般的にアルゴリズムは経時で危殆化のリスクが高まる。危殆化時には、電子署名や暗号化を施された情報に対する改ざんやなりすましの脅威を招くため、長期のクレーム利用を想定したユースケースでは、アルゴリズム危殆化を想定し、安全なアルゴリズムへの移行に対する考慮を要する。3-1-2 で述べた「長期のデジタルアイデンティティの保管・利用」実現には、クレームプロバイダーが存在しない状況も考慮した仕組みが必要となる。

3-2 で述べた処理フローを踏まえると、少なくとも①対向認証・経路暗号、②クレーム、③クレーム検証に必要な情報、の 3 か所において、用いられるアルゴリズムに対する危殆化への考慮が必要となる。

①の対向認証・経路暗号は動的な要求に基づく処理であり、移行対応の主体であるクレームプロバイダー・ホルダー・サービスプロバイダーが存在する前提での、当事者の対応（新しい暗号アルゴリズムへの切り替え等）を整理する必要がある。

---

256 OpenID Foundation, "OpenID Foundation conformance suite," https://www.certification.openid.net/

一方で、②のクレームと③のクレーム検証に必要な情報は、過去生成された情報も対象となる。危殆化の対応主体エンティティの一つであるクレームプロバイダーが既に存在しない可能性を考慮した対処が必要となる。例えば③のクレーム検証に必要な情報では、パブリックブロックチェーン向けの手法として、ハッシュアルゴリズムが危殆化した場合でも、信頼できる第三者機関が存在せずとも対応可能な手法が提唱されている。例としては、新規アルゴリズムで新ブロックを生成し、危殆化したアルゴリズムを用いて過去に生成されたブロックの有効性を、拡張することが挙げられる[257]。

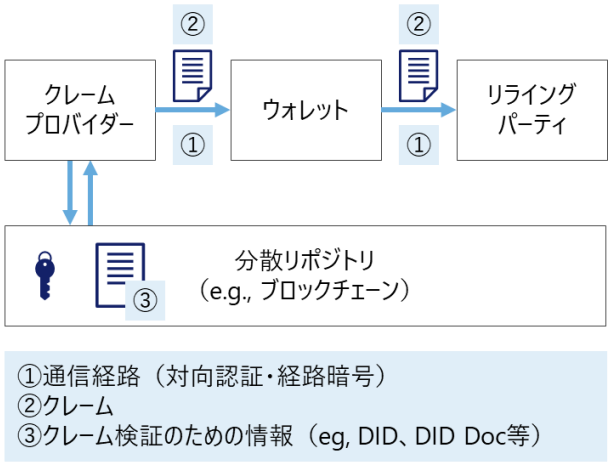


図 0-61：Cryptographic Agility の考慮対象

なお、ハッシュアルゴリズム危殆化時の移行方式について、Blockchain 方式と長期署名方式を参考として挙げる。

ブロックチェーンを用いる場合は、ハッシュアルゴリズムの危殆化が発生した場合でも、新しいハッシュアルゴリズムを用いたブロックの生成を行う（Hash(n)）ことで、過去のブロックの真正性を含めた形での証明が可能となる。

[257] Masashi Sato, Shin'ichiro Matsuo, "Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography," (September 2017), https://ieeexplore.ieee.org/document/8038516

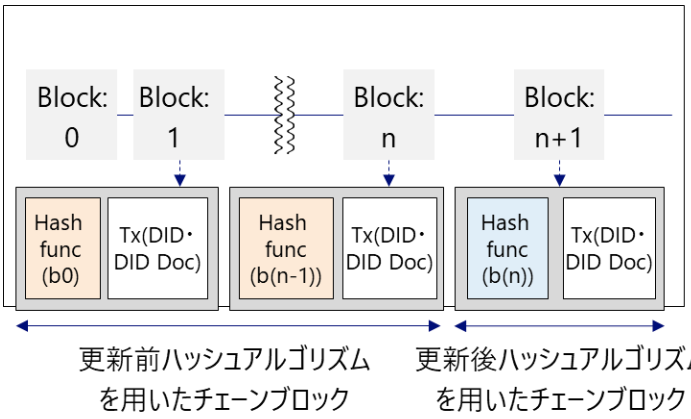


図 0-62：Blockchain におけるアルゴリズム移行方式

長期署名方式においても、新しいハッシュアルゴリズムを用いて再アーカイビングを行う方法が規定されている。一方で、同方式においては、公開鍵証明書の有効期限や、失効情報リスト（CRL）の発行時間等を鑑み、正確な時刻情報が必要となる点について留意が必要である。

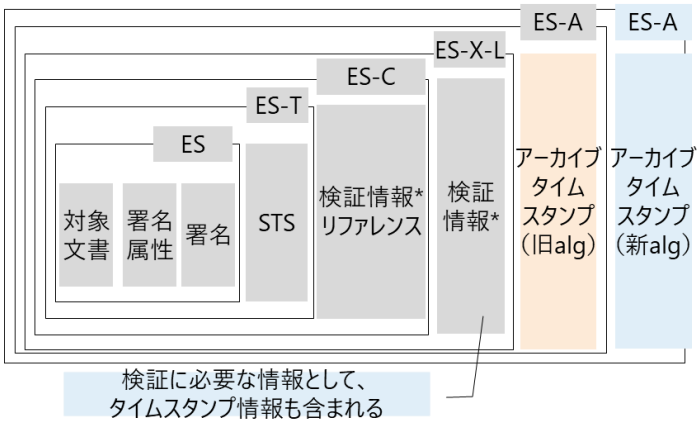


図 0-63：長期署名方式（CAdES の例）[258]

（9）Formally provable

セキュリティ観点のもう一つの課題としては、形式検証によるセキュリティの担保が挙げられる。プロトコル仕様策定は非常に複雑な作業であり、数学的な証明等を用いた脆弱性検知の手法によるサポートも期待されている。形式検証（Formal Verification）は、与えられた脅威モデルの中で多様な攻撃の可能性のあるシナリオに対する脆弱性の検出を行

[258] IETF, "CMS Advanced Electronic Signatures (CAdES)," (February 2008), https://datatracker.ietf.org/doc/html/rfc5126

う手法であり、ISO/IEC9798 における脆弱性検出や、 Financial-Grade API 評価など、多様なシーンにおいて利用実績のある手法である。

ISO/IEC 9798 に対する形式検証適合と検出脅威の事例では、ISO/IEC 9798 シリーズに対し同仕様内で言及された Thread Model を前提に Attack Model を定義し、形式検証が行われた。検証の結果、Role-mixup attacks、Type flaw attacks、Reflection attacks に対する懸念が抽出された。また同検証では、暗号化される保護対象へのタグ付けや Option Field の曖昧さ排除、前提条件の明文化など、抽出された懸念解決のための fix 提示とその有効性についても併せて示されている。[259]

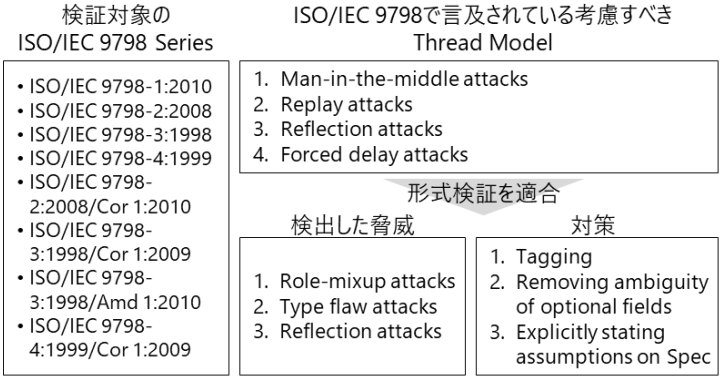


図 0-64：ISO/IEC 9798 に対する形式検証適合と検出脅威例

FAPI における検証事例では、検証対象となるモデルならびに Attacker モデルを定義し、検証が行われた。検証対象モデルは、Read/Read-Write 両 Profile として、また AttackerModel は、Read では認可リクエスト/認可レスポンス漏洩、Read-Write では攻撃者によるトークンエンドポイント制御/AT 漏洩、をそれぞれ対象として定義し、形式検証が行われた。[260][261]

---

[259] David Basin and Cas Cremers, "Evaluation of ISO/IEC 9798 ProtocolsVersion 2.0," (April 2011), https://people.cispa.io/cas.cremers/downloads/papers/BC2011-iso9798-v2.pdf

[260] Daniel Fett, Pedram Hosseyni, Ralf Kuesters, "An Extensive Formal Security Analysis of the OpenID Financial-grade API," (January 2019), https://arxiv.org/abs/1901.11520

[261] Daniel Fett, Pedram Hosseyni, Ralf Kuesters, "Formal Security Analysis of the OpenID Financial-grade API," (March 2019)

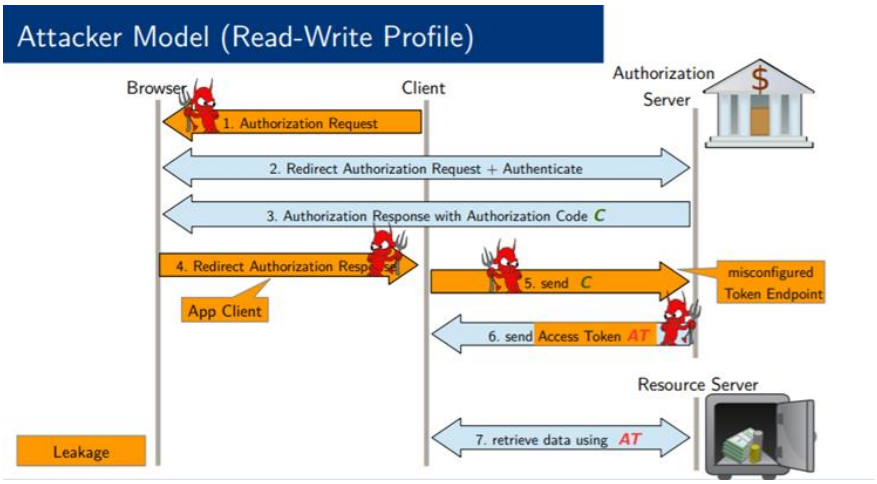


図 0-65：形式検証の概要と FAPI における検証事例

現在仕様策定中の SSI/DID の関連プロトコルについても、将来的な適用・検証が期待される。

3-4-3. SSI/DID の非技術面の課題

SSI/DID の非技術面での課題としては、法的と制度上の課題、運用上の課題、ビジネス上の課題に分類し、それぞれの中で以下の通りに観点が存在する。

表 0-26：SSI/DID の非技術面の課題

#	項目	観点
1)	法的と制度上の課題	政府および政策立案者の関与
2)		プライバシー保護
3)	運用上の課題	トラストフレームワーク
4)		ライアビリティ
5)	ビジネス上の課題	現行の IT/デジタルシステムの適応
6)		ユースケースの開拓

（1）政府および政策立案者の関与

政府および政策立案者の関与については、SSI に対応した公的 ID の提供に法的に対応できるよう、環境整備を行う必要がある。例えば、SSI/DID に対応した電子署名や電子取引の法制度整備や、電子文書などの検証可能な証明書の検討などが挙げられる。

これらは現在、国内外で最も検討・議論が進んでいる論点の一つであり、例えば EU では、2014 年に採択された eIDAS 規則に SSI/DID を対応させるための検討が行われている。eIDAS は、電子署名を含むトラストサービスと eID の法的効力を承認するもので、eID の認証結果を EU 加盟国各国で受け入れあうことができるため、SSI/DID が eIDAS

に適用されるかが SSI/DID の普及において重要な論点となっている。この点、eIDAS を SSI エコシステムのトラストフレームワークと位置付ける欧州委員会の eIDAS Bridge[262] や、欧州委員会が EBP(European Blockchain Partnership)と共同で取り組む EBSI(European Blockchain Service Infrastructure)イニシアチブ、欧州 SSI フレームワークである EBSI ESSIF [263]といった取組の中で具体的に検討されているところである。本取組では、例えば、eIDAS がどのように SSI の仕組みをサポートするのかについて法的な観点から検討した SSI eIDAS Legal Report[264]等を発行している。

なお、eIDAS Bridge は、イシュアの Verifiable credential への署名プロセスを支援し、ベリファイアに対しては、クレデンシャルの検証プロセスにおいて、DID の背後にある発行者（本プロジェクトの範囲内の法人）の特定を支援する。eIDAS Bridge を「渡る」ことにより、Verifiable credential が信頼できるようになる。

（2）プライバシー保護

プライバシー保護については、データ保護規制に向けた既存制度の見直しが必要となる可能性がある。

例えば、SSI/DID においては、ウォレットの操作を可能とする秘密鍵を保護することが最も重要となり、これが不必要に開示、提示されてしまった場合、個人データ漏えいと同様の人権被害を及ぼすこととなる。このような観点から法的・制度上の見直しの必要性等についての検討も必要となる可能性がある。例えばブロックチェーン関連事業を積極的に後押しする州の一つとして有名である米国のワイオミング州は、ブロックチェーン関連の法律をいくつも制定しており、その中で、デジタルアセットに関する法律（Section 34-29）への追加条文(34-29-107)として、「秘密鍵の開示」に関する条文案が示され、個人の「秘密鍵」を守る権利を保障するものとして注目を集めた[265]。本法案は、2021 年 4 月に否

---

[262] Joinup, "About SSI eIDAS Bridge," https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about

[263] ESSIF の詳細について EBSI の以下参照
https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505360

[264] European Commission, “SSI eIDAS Legal Report - How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market-” April 2020.
https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf

[265] 条文案は以下の通り。

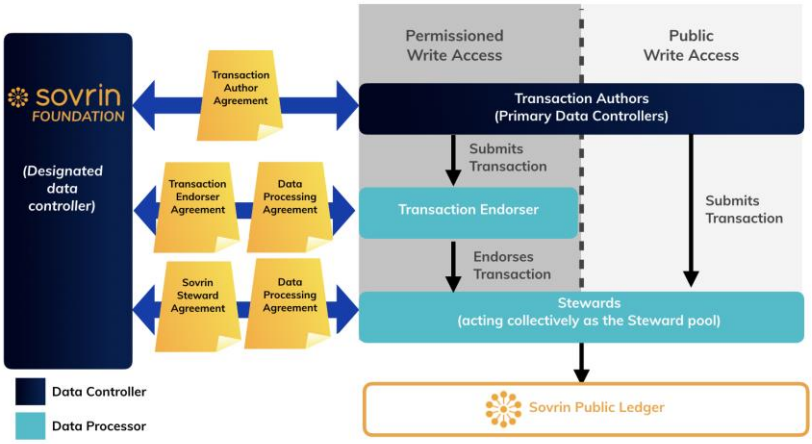
「秘密鍵の開示(Disclosure of private cryptographic keys)： 秘密鍵の作成、禁止（Production of private keys; prohibition.） 何人も、公開鍵がデジタル資産、その他の利益または権利に関して必要な情報を利用できないまたは開示できない場合を除き、秘密鍵がアクセスを提供するデジタル資産、その他の利益または権利に関連する本州の民事、行政、立法またはその他の手続きにおいて、秘密鍵を提示したり、秘密鍵を他の者に知らせたりすることを強制されない。本項は、秘密鍵がアクセスを提供するデジタル資産、その他の利益または権利を提示または開示すること、またはデジタル資産、その他の利益または権利に関

決されているが、秘密鍵を守る権利を保障する同様な法案は今後も世界各国で検討されることが想定される。

SSI/DID についての注目が高まってきているのは、各国のデータ保護法制度が強化され、組織における個人データ管理の重要性が高まっていることが要因の一つに挙げられる。SSI/DID の普及・浸透にあたっては、上述のような、思想やアーキテクチャの推進を後押しする環境整備が必要となるだろう。

また、SSI/DID に分散型台帳やブロックチェーンネットワークを利用する場合、分散台帳に登録される情報が個人データに該当するかどうかについての検討も重要となる[266]。必要に応じて規制の見直しや、利用する際の運用ガイドライン等の策定が求められる。例えば、SSI/DID にブロックチェーンが使用される場合は、個人データや PII の台帳への登録を確実に回避することが必要となる。この点に関して、今後 SSI/DID のユースケース等に応じてよい明確化、具体化していくことが必要であると想定される。

Sovrin 財団では、GDPR を想定したデータ保護法に準拠するためのリーガルフレームワークにおける主要なアクターの役割を以下の図のように整理している。



する情報を開示することを強制する合法的な手続きを禁止するものとは解釈されないものとする。」Select Committee on Blockchain, Financial Technology and Digital Innovation Technology, "Disclosure of private cryptographic keys.," https://legiscan.com/WY/text/SF0105/2021

[266] 例えば、欧州では公開鍵やトランザクションデータに該当するかどうかに関する検討がなされている。詳細は以下を参照。

CNIL, “Blockchain and the GDPR,” Nov 2018.
https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

European Parliamentary Research Service, “Blockchain and the General Data Protection Regulation,” July 2019
https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

図 0-66：Sovrin 財団の取組[267]

この中で、Sovrin Leger への書き込みを行う Transaction Authors に関し、現状 Permissioned Write Access polices では、法人のみが書き込め、個人は書き込みできない。Sovrin この理由の一つに、「これにより、個人データが Sovrin Ledger に書き込まれるリスクが軽減される。これは現在、Permissioned Write Access polices で禁止されているためである。Sovrin 財団は、不変的な公開台帳上の個人データに関する現在の規制の不確実性の下で、この保護が必要であると考える」と述べている[268]。

（3）トラストフレームワーク

トラストフレームワーク（TF）に関する課題としては、運用制度（TF の開発・選定)、運用スキームの整理（TF の維持)、運用業務の遂行（TF の定めるルールの執行）の観点があると考えられる。

運用制度については、欧州連合の eIDAS のような適格 ID プロバイダの認証を確立するために、国や地域の公的および民間のフレームワークを開発することが必要である。例えば（１）でも取り上げた「SSI eIDAS Legal Report」では、欧州委員会によって SSI の技術仕様に対し法的観点から適合性を評価し現行規則の改正等の必要性に言及されている。

運用スキームの整理については、トラストフレームワークの構築・管理・更新を維持・継続していく必要があり、誰が同活動に対し責任を負うか（公的/民間)、コスト負担やインセンティブ設計への考慮も必要となる。

運用業務の遂行については、トラストフレームワークは一度作成して完了するものではなく、その枠組みを継続的に維持・活用する必要がある。トラストフレームワークの維持と活用に際し必要な統制機能として、参画団体の管理や認定、策定ポリシーの執行、フレームワークの運用、他トラストフレームワークとの相互運用性確立が挙げられる[269]。

運用スキームの整理と運用業務の遂行について参考となる取り組み事例としては、OIX や DIACC などの団体が策定しているトラストフレームワークが、非営利組織として官民のステークホルダーが集まって構築されており、一定の運用スキームや運用業務遂行に向けた体制は整備されていることが挙げられる。ただし、課題詳述に挙げた統制機能などの

---

[267] Sovrin Foundation , "Data Protection and the Sovrin Governance Framework," https://sovrin.org/data-protection/

[268] Sovrin Foundation , "Data Protection and the Sovrin Governance Framework," https://sovrin.org/data-protection/

[269] OIX, "OIX Guide to Trust Frameworks V0.1 BETA," (June 2020), https://openidentityexchange.org/networks/478/item.html?id=364

一部はまだ議論・策定段階のものもある。また、SSI/DID 以外の分野では、例えば、参加事業者でコンソーシアムを形成する CA/Browser Forum[270]では、電子証明書を使った通信の安全性・利便性向上のためのガイドライン策定を行っている。同フォーラムには主要な Web ブラウザ開発ベンダーも参加しており、過去 EV SSL 証明書のガイドライン策定なども行っている。各社は同フォーラムでの議論を踏まえ、自社のブラウザ仕様実装の検討を行う一方、上述の協調領域における議論は統一的な仕様を策定や実装することで、相互運用性を確保している。

（4）ライアビリティ

ライアビリティの課題としては、責任分界点、ユーザの保護と支援、開発と運用コスト負担の観点がある。

責任分界点については、SSI モデルでは、ウォレットを制御するユーザ自身が IDP として振る舞うことで、従来であれば国・企業・組織等が果たすべき責務を一義的にはユーザ自身が果たす必要が生じる。このためユーザへの支援が重要となるが、誰がどの様に担うのか、またその責務や責任分界点、また有事の際の扱い等を考慮しておく必要がある。また、ステークホルダーの適切な参集がなされていない場合、本来考慮すべき担務の欠如や責任分界点があいまいとなる懸念がある。

OIX はこのような課題を解決するための一つのツールとして、トラストフレームワークの作成・活用を提唱しており、例えば責任分界点に関する議論はライアビリティの考慮事項として、言及されている（表 0-22、6. リライングパーティサービス）。

また、DIACC では、DID の PCTF への準拠の考え方についてのガイドラインが公表され、この中で本点への対応が課題である点についても触れられている。いずれも課題としては認識されているが、具体的な解決案などは議論中の課題となっている。

ユーザの保護と支援については、ユーザ自身の IT リテラシーも様々であり、社会インフラとしての金融においては、利用者包摂を意識した仕組み作りが期待される。例えば、トラストフレームワークに求める要件を準拠し、認定を受けた利用者に使いやすいソリューション提供が可能な事業者のみ参画可能とすることや、自身での管理が困難なユーザについては権限委任等による代行の仕組みを検討することといった、包摂やデジタルディバイドを意識した制度設計が期待される。なお、OIX Trust framework モデルでは、ウォレットが Issuer としても Verifier としても機能することを想定しており、AML 向けの Evidence の提示等、ウォレットが監査対応という役割を担うことを想定している。同モデルの検討においては、実ユースケースにおける上記役割の担い手として、ウォレットベンダ、3rd Party のサービス提供者等の想定があり得るのではないか、という議論も出ている。

---

[270] CA /Browser Forum, "About EV SSL," https://cabforum.org/about-ev-ssl/

そして、開発と運用コスト負担については、金融サービス全体でのオンボーディングコスト抑制に寄与する一方、誰がどのようなソリューション開発・運用コストの負担を担うかの整理が必要となる。これについては、SecureKey の Verified.Me が、金融機関も共同で出資して Verified.Me を構築するモデルを採用しているという取り組みが挙げられる。

（5）現行の IT/デジタルシステムの適応

SSI/DID を幅広く利用可能とするためには、クレデンシャルの発行や検証を可能にする等、現在の IT システムの更新や新規システム構築、更新・新規構築に係るコスト負担が必要となる場合が、現状その投資に見合う利用が見込まれていない場合が多い。既存システムが一律新規スキーム（SSI/DID 方式）に移行するとは考えにくく、当面は既存スキーム（Federation 方式）との併存を意識し両スキームへの対応と維持及び運用コストの負担が必要となる事が予想される。

OIX Trust Framework では、両スキームに対応するモデルのスイッチングハブを構成するモデルの構想を行っている[271]。但し 3-4-2 でも述べた通り、同実装には、モデル・メソッド間における相互運用性への考慮が重要となる。またスイッチングの対象メソッド実装が収斂せず複数仕様が乱立する場合、同改修の工数増に繋がることが予想される。

（6）ユースケースの開拓

ユースケースの拡大については、企業や政府が個人に対して使いやすいソリューションを提案することが必要となる。例えば Sovrin Foundation においても、今後のユースケース開拓の必要性が議論されており、Covid-19 の接種証明書や医療結果の証明への活用といった医療はじめ、金融・その他分野におけるクレデンシャルの活用拡大を予想している[272]。実際、既に Covid-19 関連の事例として、IATA の ”Travel Pass”によるデジタルの形での接種証明書の展開といった具体的な事例も出始めている[273]。

---

[271] OIX Quarterly Workshop - 15th Dec 2020

[272] IATA, "IATA Travel Pass Initiative," https://www.iata.org/en/programs/passenger/travel-pass/

[273] Sovrin Foundation , "2020 - How SSI Went Mainstream," (January 2021), https://sovrin.org/2020-how-ssi-went-mainstream/

3-5. SSI/DID 活用時の金融規制上の論点

本節では SSI/DID を金融取引に活用する際に想定される金融規制上の論点について考察する。考察にあたっては、3-1-1.項で記載した一般的な SSI/DID のモデル（**図 0-2**）に金融取引のステークホルダーを当てはめた、下図下段の「金融取引の SSI/DID モデル」を前提とする。

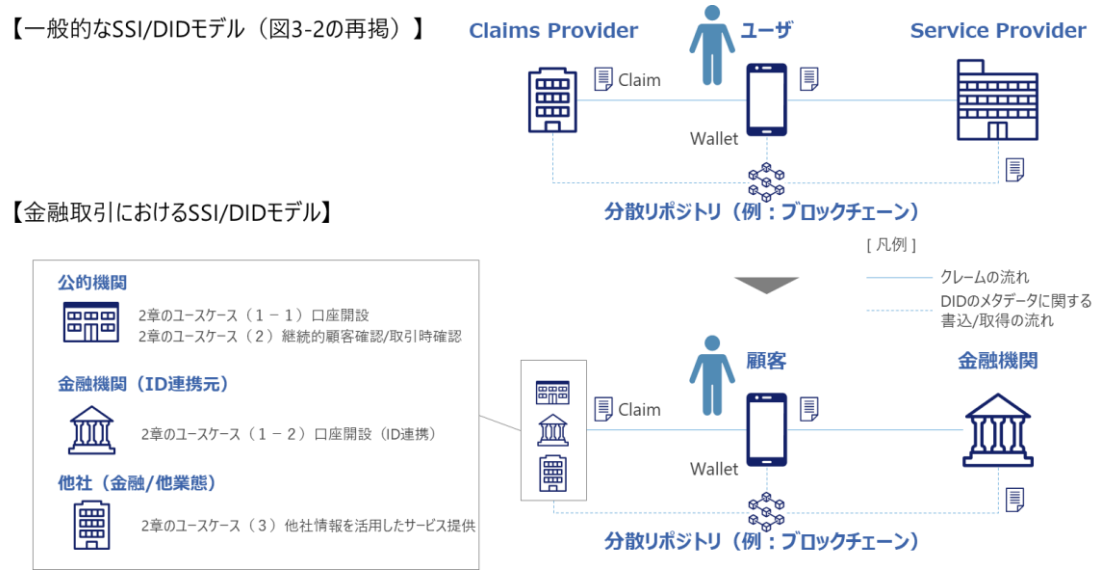


図 0-67：金融取引における SSI/DID モデル

なお、顧客から受け取ったクレームを金融機関は保管して利用できる前提とする。すなわち、金融機関における顧客データの分析業務は、都度ウォレットから情報を収集せずとも、金融機関に保管されたクレームを利用して実施可能とする。

3-5-1. 金融取引における SSI/DID モデルでのユースケース

図 0-67 を 2 章のユースケース別に記載すると、図 0-68 のように整理できる。

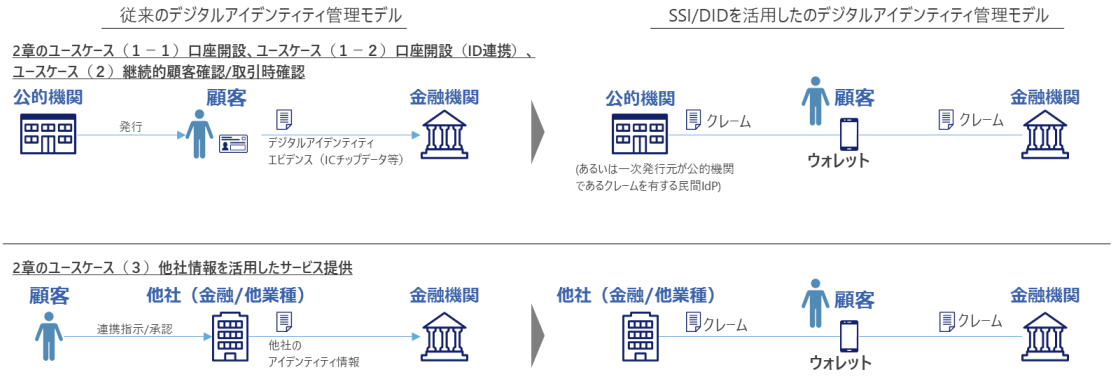


図 0-68：2 章のユースケース別の SSI/DID モデルと従来のモデルとの違い

2 章のユースケース（1－1）口座開設、ユースケース（1－2）口座開設（ID 連携)、およびユースケース（2）継続的顧客確認/取引時確認の場合、本人確認用のクレームを顧客が公的機関（あるいは一次発行元が公的機関であるクレームを有する民間 IdP）から受け取り、その中から新規に口座開設する金融機関が必要とする属性情報を選択（あるいは金融機関が求める属性情報を承認）してウォレットから金融機関へ連携する。新規に口座開設する金融機関は、ウォレットから連携された情報を元に本人確認を行う。（図 0-68 上段)。

2 章のユースケース（3）他社情報を活用したサービス提供の場合、顧客が自身のクレームを保有する他社から当該クレームを受け取り、その中から金融機関が顧客へのサービス提供のために必要とする属性情報を選択（あるいは金融機関が求める属性情報を承認）してウォレットから金融機関へ連携する。顧客へサービスを提供する金融機関は、ウォレットから連携された情報を元に顧客へ最適なサービスを提供する。（図 0-68 下段）

上述のいずれのパターンにおいても、従来のデジタルアイデンティティ管理モデルと比較した場合、SSI/DID を活用したデジタルアイデンティティ管理モデルの相違点は主に 2 点ある。

1 点目は、金融機関に連携される情報の連携元である。従来のデジタルアイデンティティ管理モデルでは、デジタルアイデンティティエビデンスは顧客の端末（IC チップリーダやスマートフォン等）から、ID 連携の場合は ID 連携元の金融機関/企業から連携されるが、SSI/DID を活用したデジタルアイデンティティ管理モデルではいずれも顧客のウォレットからの連携となる。

2 点目は、金融機関に連携される情報の作成者である。従来のデジタルアイデンティティ管理モデルでは、デジタルアイデンティティエビデンスや連携されるアイデンティティ情報は、公的機関、金融機関、企業等が作成したものであるが、SSI/DID を活用したデジタルアイデンティティ管理モデルでは、いずれも顧客がウォレット上で作成（顧客の保持するクレームの中から必要な属性を選択・提示）したものになる。

3-5-2. 金融規制上の論点

相違点 1 についての規制上の論点は、ウォレットに対する規制をどのようにかけていくか、である（図 0-69 の論点 1)。金融機関へ連携されるクレームが全て顧客のウォレット起点となるため、金融システム安定化のためには、ウォレットから提示されるクレームの安全性や調査・責任追及のルートを確保する必要がある。そのためにはウォレットに対して一定の規制を設ける必要があると考えられるが、誰に対してどのような規制をかけるべきか、を考察する。

相違点 2 についての規制上の論点は、新たな本人確認情報に対して必要な法的手当ての在り方、である（図 0-69 の論点 2)。ウォレットから金融機関へ連携される本人確認情報

や既存口座の情報が、金融機関の本人確認情報として法的に認める必要があるが、従来から認められている本人確認情報と違いを考慮し、法的にどのように認めればよいのかを考察する。なお、2 章のユースケースのうち、ユースケース（3）他社情報を活用したサービス提供については、連携時に本人確認を伴わないため、本論点の対象外とする。

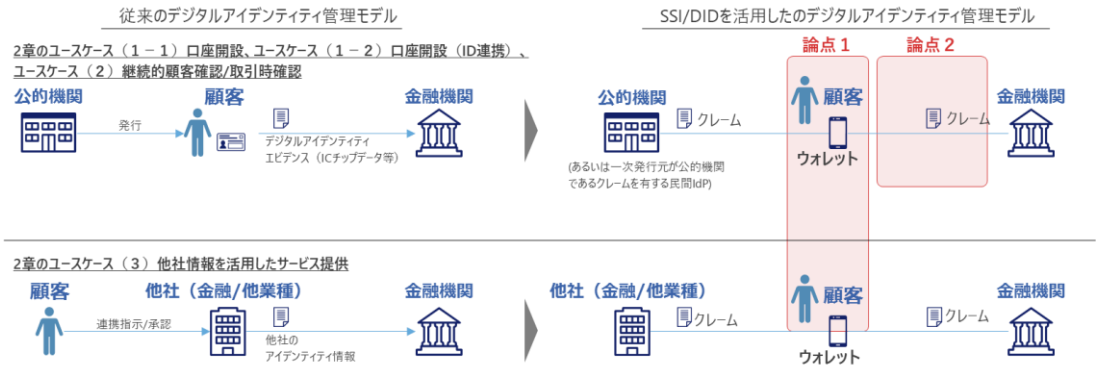


図 0-69：金融取引における SSI/DID 活用時の金融規制上の論点

3-5-3. ウォレットに対する規制の考え方

（1）検討の前提と方法　ウォレット管理形態のパターン

まず、「誰に対して」規制をかけるべきかを考察するため、ウォレットの管理形態をパターン分けし、各パターンにおける規制対象者を明らかにする。

ウォレットの管理形態は「データの運用管理主体」と「データの保管環境」の 2 軸で分類できる。「データの運用管理主体」とは、クレームの送受信や ID とクレームの Bind などウォレットデータ運用の、管理および実行者のことである。「データの運用管理主体」は、さらに「データ管理者」と「データ処理者」の 2 者に分類できる。「データ管理者」はデータの主権者である顧客自身である。データ処理者は顧客自身と、ウォレットプロバイダー等の委託先の 2 パターンが考えられる。「データの保管環境」とは、ウォレットデータが保管されるインフラ環境のことであり、顧客自身の個人デバイス（ローカル）とクラウド環境の 2 パターンが考えられる。したがって、ウォレットの管理形態のパターンは、「データの運用管理主体」2 パターンと「データの保管環境」2 パターンの掛け合わせで、計 4 パターンが考えられる。

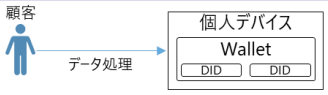
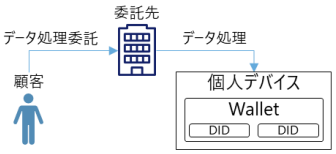
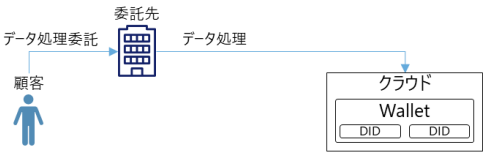
No.	データの運用管理主体		データの保管環境	Wallet運用形態のイメージ
	管理者	処理者		
1	自己（顧客）	自己	ローカル	
2		委託先（Walletプロバイダ）	ローカル	
3		自己	クラウド	
4		委託先（Walletプロバイダ）	クラウド	

図 0-70：ウォレット管理形態のパターン

（2）検討の前提と方法　規制の実現可能性に関する評価項目

次に、「どのような」規制をかけるべきかを考察するため、規制を通じて担保すべきウォレットに関する要件を整理する。各要件の実現性を評価し、評価結果に応じて現実的な金融規制の方向性を考察する。

ウォレットから連携されるアイデンティティ情報が規 AML/CFT 等の規制目的達成の観点から適切なものである必要があり、規制上の評価項目として、例えば①当人の情報が正しく（なりすまし等の不正無く）連携されるか、②問題発生時に責任を追及できるか、③問題発生時に対象データを調査できるか、の 3 つを検討する。評価項目名として、以降、①ウォレット運用の信頼性、②問題発生時の責任追及・対応、③犯罪捜査時のウォレット内データ開示、とする。

表 0-27：金融規制の実現可能性に関する評価項目

#	評価項目	評価項目の説明
1	ウォレット運用の信頼性	顧客自身の DID と CP のクレームの Binding が正しく行われ、当該クレームが金融機関へ連携できるかどうか
2	問題発生時の責任追及・対応	および最終責任者である顧客に対し、なりすまし等の不正利用時の責任追及や対応を求めることができるかどうか
3	犯罪捜査時のウォレット内データ開示	金融犯罪捜査時に、金融機関が保管していない Wallet 内のデータを捜査当局が調査できるかどうか

（3）ウォレットに対する規制の実現可能性評価結果

ウォレットの管理形態パターンごとに前述の評価項目で評価した結果を**エラー! 参照元が見つかりません。**に示す。

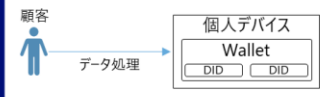
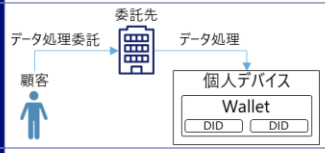
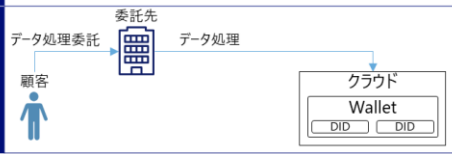
規制の実現性	Wallet運用形態のパターン	金融規制の実現可能性に関する評価項目		
		①Wallet運用の信頼性	②問題発生時の責任追及・対応	③金融犯罪捜査時等のWallet内データ開示
	1 自己/ローカル 	低 (運用信頼性の低さにより、なりすまし等不正利用の観点から懸念)	困難 (問題発生時の管理責任や対応を特に個人に対し求めるのは困難)	困難 (金融犯罪捜査時の顧客に対する強制的データ開示は難しい)
	2 委託/ローカル 	高 (委託先がデータ処理を行うため、自己運用と比較すると懸念は減少)	可 (委託先にも一定の責任を問う余地はあり、自己運用と比較し安定した運用が期待)	困難
	3 自己/クラウド 	低 (運用信頼性の低さにより、なりすまし等不正利用の観点から懸念)	困難 (問題発生時の管理責任や対応を特に個人に対し求めるのは困難)	可 (クラウドベンダの開示方針によっては、個人デバイスより実現性高)
	4 委託/クラウド 	高 (委託先がデータ処理を行うため、自己運用と比較すると懸念は減少)	可 (委託先にも一定の責任を問う余地はあり、自己運用と比較し安定した運用が期待)	可 (クラウドベンダの開示方針によっては、個人デバイスより実現性高)

図 0-71：ウォレットに対する規制の実現可能性評価結果

①ウォレット運用の信頼性については、ウォレット運用（データ処理）を第三者に委託する方が顧客が自己管理するよりも信頼性が高い、すなわちなりすまし等の不正利用がされ難いと考えられる。なぜなら、高いセキュリティ水準による豊富な運用実績を有する大手ベンダーによるウォレット運用の方が、自己管理による運用と比較して不正利用等のリスクが低いと考えられるためである。

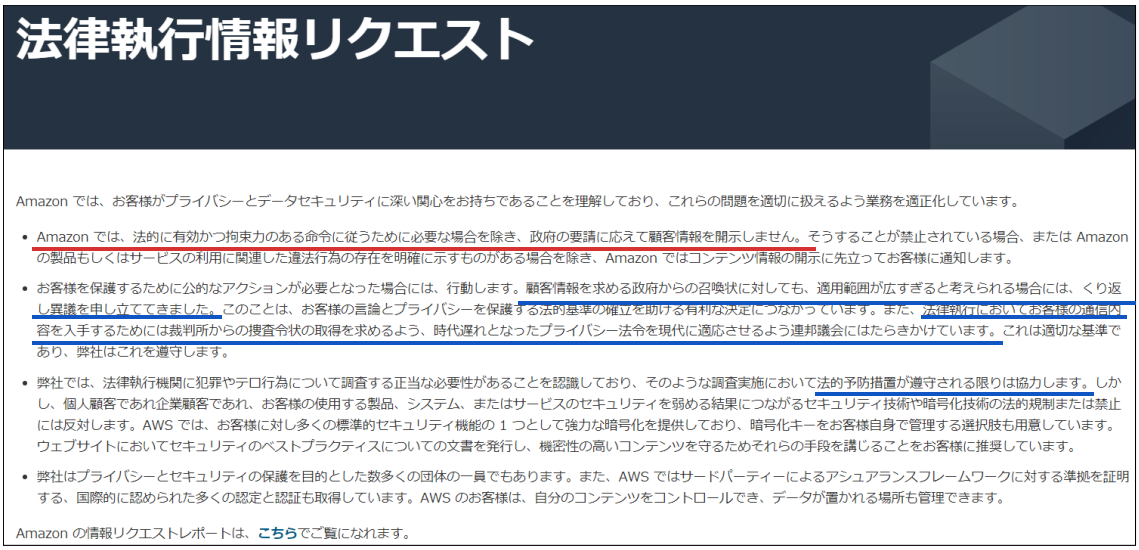
②問題発生時の責任追及・対応についても、ウォレット運用（データ処理）を委託する方が顧客が自己管理するよりも実現しやすいと考えられる。一般に、問題発生時の管理責任や対応を特に個人に対し求めるのは困難なため、自己管理の場合は問題解決に向けた動きを取りづらい。一方、管理を委託する場合、委託先にも一定の責任を問う余地はあり、自己運用と比較して効果的な責任追及が期待できる。

③犯罪捜査時等のウォレット内データ開示については、ウォレットデータをクラウド上で管理したほうがローカル管理するよりも実現性が高いと考えられる。

ウォレット環境がローカル（個人デバイス）の場合、秘密鍵がローカルにしかないため、犯罪捜査時に捜査当局が強制的にデータ調査することは難しい。一方、ウォレット環境がクラウドの場合、秘密鍵もクラウド上に存在するケースが多いため、ローカル管理に比べれば、クラウドベンダの金融犯罪調査時の情報開示方針によっては捜査当局が強制的にデータ調査できる余地があるといえる。

クラウドベンダの金融犯罪調査時の情報開示方針の事例として Amazon Web Service（AWS）の法律執行情報リクエストに対する考え方を紹介する。AWS は、法律執行情報リクエストに対する考え方を Web ページで公開しており、法的に有効かつ拘束力のある命令に従うために必要な場合には、政府の要請に応えて必要な顧客情報を開示する旨を表明している。具体的には「Amazon では、法的に有効かつ拘束力のある命令に従うために必要な場合を除き、政府の要請に応えて顧客情報を開示しません」（図 0-赤線部）とあり、逆説的に、法的に有効かつ拘束力のある命令に従うために必要な場合は、政府の要請に応えて顧客情報を開示する意思を示している。

なお、政府の要請に対しても必要な情報を文書で正式に要請された場合のみを開示する旨を表明している。具体的には「顧客情報を求める政府からの召喚状に対しても、適用範囲が広すぎると考えられる場合には、くり返し異議を申し立ててきました。」「法律執行においてお客様の通信内容を入手するためには裁判所からの捜査令状の取得を求めるよう、時代遅れとなったプライバシー法令を現代に適応させるよう連邦議会にはたらきかけています」「法的予防措置が遵守される限りは協力します」（図 0-青線部）とあり、たとえ政府からの要請であっても、文書での正式に要請された場合に限り調査に必要な情報のみを開示する意思を示している。



法律執行情報リクエスト

Amazon では、お客様がプライバシーとデータセキュリティに深い関心をお持ちであることを理解しており、これらの問題を適切に扱えるよう業務を適正化しています。

- Amazon では、法的に有効かつ拘束力のある命令に従うために必要な場合を除き、政府の要請に応えて顧客情報を開示しません。そうすることが禁止されている場合、または Amazon の製品もしくはサービスの利用に関連した違法行為の存在を明確に示すものがある場合を除き、Amazon ではコンテンツ情報の開示に先立ってお客様に通知します。
- お客様を保護するために公的なアクションが必要となった場合には、行動します。顧客情報を求める政府からの召喚状に対しても、適用範囲が広すぎると考えられる場合には、くり返し異議を申し立ててきました。このことは、お客様の言論とプライバシーを保護する法的基準の確立を助ける有利な決定につながっています。また、法律執行においてお客様の通信内容を入手するためには裁判所からの捜査令状の取得を求めるよう、時代遅れとなったプライバシー法令を現代に適応させるよう連邦議会にはたらきかけています。これは適切な基準であり、弊社はこれを遵守します。
- 弊社では、法律執行機関に犯罪やテロ行為について調査する正当な必要性があることを認識しており、そのような調査実施において法的予防措置が遵守される限りは協力します。しかし、個人顧客であれ企業顧客であれ、お客様の使用する製品、システム、またはサービスのセキュリティを弱める結果につながるセキュリティ技術や暗号化技術の法的規制または禁止には反対します。AWS では、お客様に対し多くの標準的セキュリティ機能の 1 つとして強力な暗号化を提供しており、暗号化キーをお客様自身で管理する選択肢も用意しています。ウェブサイトにおいてセキュリティのベストプラクティスについての文書を発行し、機密性の高いコンテンツを守るためそれらの手段を講じることをお客様に推奨しています。
- 弊社はプライバシーとセキュリティの保護を目的とした数多くの団体の一員でもあります。また、AWS ではサードパーティーによるアシュアランスフレームワークに対する準拠を証明する、国際的に認められた多くの認定と認証も取得しています。AWS のお客様は、自分のコンテンツをコントロールでき、データが置かれる場所も管理できます。

Amazon の情報リクエストレポートは、こちらでご覧になれます。

図 0-3：法律執行情報リクエストに対する AWS の説明ページ[274]

また、データの保管環境による犯罪捜査時等のウォレット内データ開示性の違いについて補足する。SSI/DID の仕組み上、基本的にはウォレットの秘密鍵がないとウォレット内のデータ開示はできない。しかし、犯罪捜査等に必要なデータは、顧客が秘密鍵の提供を拒

274 アマゾンウェブサービスジャパン株式会社、「法律執行情報リクエスト」
https://aws.amazon.com/jp/compliance/amazon-information-requests/

否した場合でも強制的に開示させる必要がある。したがって、犯罪捜査時等に捜査当局が特別に秘密鍵にアクセスできる必要があるため、犯罪捜査の観点からは、ウォレットはローカルデバイス内よりもクラウド上での管理が望ましいと考えられる。

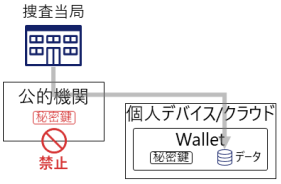
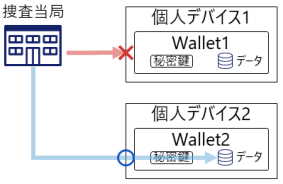
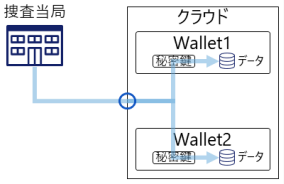
パターンNo.	1	2	3
秘密鍵の保管環境	顧客のWallet以外	顧客のWallet	
Walletの保管環境	–	ローカル	クラウド
金融犯罪捜査時等のWallet内データ開示	不可	困難	可
	秘密鍵はいかなる理由があろうと他人に管理させないということが基本的人権に沿った原則になる。（海外有識者からも指摘あり）	デバイスの管理主体が顧客自身のため、デバイスの種類や設定によっては、犯罪捜査に必要なデータをバックドアから取得しようとしても、アクセスできない可能性がある。	クラウドベンダにおける金融犯罪時のデータ開示の対応方針によっては、クラウドベンダ経由でのデータ開示が期待できる。
			

図 0-72：データの保管環境による犯罪捜査時等のウォレット内データ開示性の違い

上記結果をまとめると、ウォレットの管理は委託し、かつ、ウォレットデータはクラウド上で管理する運用形態の下で、ウォレットプロバイダー・クラウドベンダといった事業体に対する規制を通じてウォレット規制を実現する方が、ウォレット利用者やウォレットデータが格納された各デバイスを直接規制するよりも、規制の実行可能性がが高いと考えられる。

（4）ウォレットに対する金融規制の進め方についての示唆

自己管理・個人デバイスの場合、ウォレットアプリや操作の品質確保、犯罪捜査用バックドア確保の難易度が高いため、AML/CFT 等の規制目的達成の観点からは、規制の難易度が相対的に低いと考えられる「委託・クラウド型」に絞って SSI/DID の金融サービスでの利用を許容とするところから始めるのが現実的と考えられる。

「委託・クラウド型」の場合、ウォレット運用の信頼性を担保するため、委託先であるウォレットプロバイダー等を何らかの規制対象とする必要があるかもしれない。ウォレットプロバイダーについては、例えば、一定の基準を満たしたウォレットプロバイダーのみが金融機関へ接続できるようなルール化が必要とも考えられる。

また、「委託・クラウド型」でウォレット運用を行う場合、新たな課題として、特定のウォレットプロバイダーへの依存（ベンダーロックイン）が考えられる。顧客保護の観点から、ウォレットプロバイダーの変更が可能な状態（ポータビリティ）を確保する手当てが必要と考えられる。

なお、ルールの適用方法については、金融サービスにおけるパブリッククラウドの活用に対するガイドライン適用の事例が参考になると考えられる。パブリッククラウド活用の場合と異なり、ウォレットの場合は金融機関とウォレットプロバイダーの間に契約関係はないものの、ウォレットプロバイダーはビジネス上金融機関と接続する必要があるため、ガイドラインを遵守するインセンティブは働くと考えられる。

参考として、金融サービスにおけるパブリッククラウド活用に対するガイドラインの手当について紹介する。金融機関がパブリッククラウドを活用する場合、財団法人金融情報システムセンター （以下、FISC）により金融機関等の自主基準として策定された「金融機関等コンピュータシステムの安全対策基準・解説書」（以下、安全対策基準）をガイドラインとして参照することとなっており、同ガイドラインを鑑として、金融機関によるパブリッククラウドサービスの評価、金融庁による金融機関の監督、が行われている。

FISC 安全対策基準は、統制・実務・設備・監査の 4 分野について、システムの安全性に関する管理策が示されているものである。

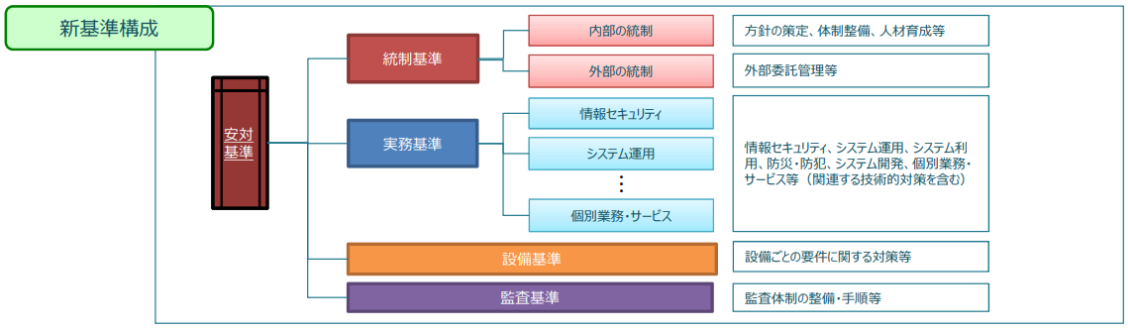


図 0-73：FISC 安全対策基準の構成[275]

FISC 安全対策基準は、金融機関におけるパブリッククラウドサービス管理基準の事実上の標準となっており、金融機関はパブリッククラウドサービスの評価・選定、および運用管理の際に、FISC 安全対策基準を満たしているかどうかの確認を行っている。

各クラウドベンダは FISC 安全対策基準に対する対応状況をリファレンス文書として Web サイト上で公開して安全性を説明しており、金融機関にとって上記確認のための材料となっている[276]。

---

[275] 公益財団法人 金融情報システムセンター、「安全対策基準（第 9 版）の改訂概要」（2017.12）
https://www.fsa.go.jp/singi/kessai_kanmin/siryou/20171220/04.pdf

[276] アマゾンウェブサービスジャパン株式会社、「金融機関向け AWS FISC 安全対策基準対応リファレンス」（2020.9）
https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_FISC_Guidelines_9thEdition.pdf

金融庁は監督指針において、金融機関等がシステムリスクならびにセキュリティ対策を検討する上での参考文書として FISC 安全対策基準を取り上げ、利用を後押ししている。また、金融機関の監査も同書に沿って実施されている。

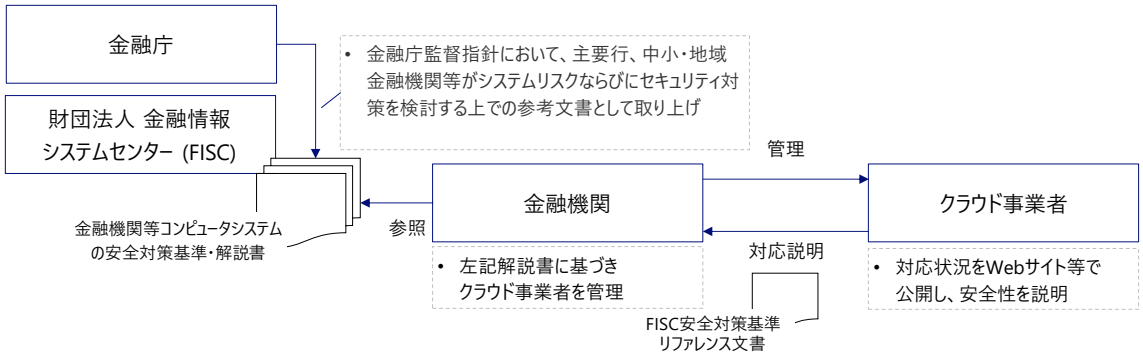


図 0-74：FISC 安全管理基準を鑑とした金融サービスにおけるパブリッククラウドサービスの安全性評価

3-5-4. 新たな本人確認情報に対する法的手当て

金融機関へ提示する本人確認情報が個人を IdP とするデジタルアイデンティティの形となるため、個人発行のデジタルアイデンティティをどのように法的に認めるか、が課題である。

アイデンティティエビデンスを顧客から金融機関へ連携する場合（表 0-28）、従来はマイナンバーカードや運転免許証等の本人確認書類に付帯するデジタルアイデンティティエビデンス（IC チップ等に記録された属性情報）の全項目を IC カードリーダやスマートフォンから金融機関へ連携する。一方、SSI/DID では口座開設に必要な属性情報を顧客がクレームの形でウォレット上に収集して自身の ID とバインドし、デジタルアイデンティティとして金融機関へ連携することとなる。

表 0-28 アイデンティティエビデンスを顧客から金融機関へ連携する場合[277]

デジタルアイデンティティの種類	データの形態	データの項目の項目
従来のデジタルアイデンティティ	デジタルアイデンティティエビデンス（IC チップ内のデータなど）	アイデンティティエビデンス記載全項目

[277] 2 章のユースケース（1－1）口座開設、ユースケース（2）継続的顧客確認/取引時確認の場合

SSI/DID	個人の発行した デジタルアイデンティティ （公的機関等のクレーム）	必要な項目

既存口座情報など金融機関の既存のデジタルアイデンティティを連携して口座開設する場合（表 0-29）、従来は連携元の金融機関から口座開設する金融機関へ直接 API 等で顧客の属性情報が連携される。一方、SSI/DID では口座開設に必要な属性情報を顧客がクレームの形で連携元金融機関からウォレット上に収集して自身の ID とバインドし、デジタルアイデンティティとして口座開設先の金融機関へ連携することとなる。

現在、多くの法域において、上記のようなクレームが本人確認に使用できる情報として規定されていないため、仮にこれらのクレームの使用を許容する場合には、何らかの法的手当てが必要と考えられる。

なお、デジタルアイデンティティにバインドされるクレームの一次発行元は、現状の発行元／ID 連携元と同様に、公的機関中心と想定される。

表 0-29　金融機関の既存のデジタルアイデンティティを連携して口座開設する場合[278]

デジタルアイデンティティの種類	データの形態	データの項目の項目
従来のデジタルアイデンティティ	金融機関（ID 連携元）の デジタルアイデンティティ	各金融機関の本人確認用項目（顧客には非公開）
SSI/DID	個人の発行した デジタルアイデンティティ （公的機関等と金融機関（ID 連携元）のクレーム）	各金融機関の本人確認用項目（顧客に公開）

[278] 2 章のユースケース（1－2）口座開設（ID 連携）の場合

3-1-2 で述べた通り、SSI/DID の特性として、 Recognition（当人認証）と Selfness（属性）の分離があげられる。一方で、この二つを分離する場合には、連携されたクレーム（属性）が、当人認証をしている相手（エンティティ）に関するものかどうかを判別可能とするため、紐付け（Binding）を行う必要がある。

具体的な懸念として、ユーザがクレームを RP に提示する際、RP は「そのクレームが相対しているユーザに対し発行されたクレームか」の検証を行う必要がある。この処理を行わない場合、窃取されたクレームを用いた ”なりすまし” が可能となる。

これを防ぐためにはクレーム発行要求の段階から、ユーザとクレームを ”Binding” する形で、クレーム発行を行う必要がある。

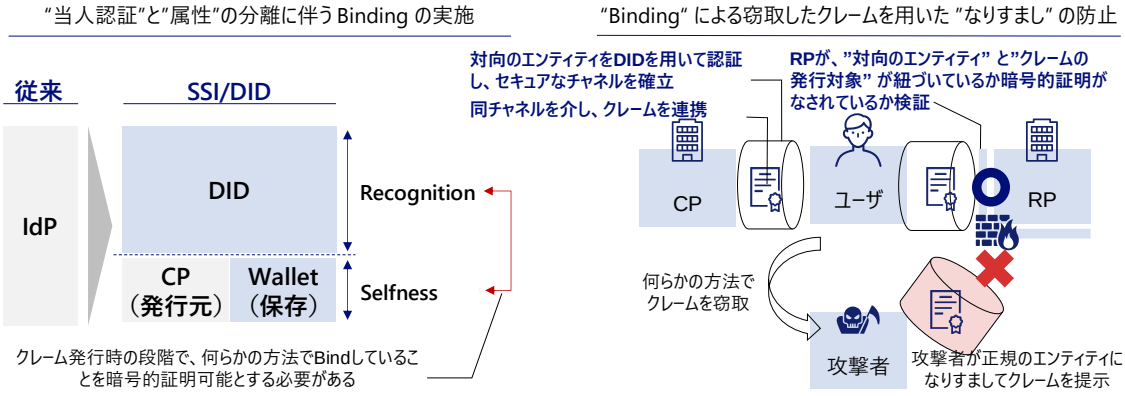


図 0-75：Binding の必要性

ユーザとクレームを ”Binding” のためには、次の 2 点が必要となる。まず、CP がクレームを発行する際、相対しているエンティティ（ユーザ）に対しクレームを発行する必要がある。次に、RP がクレームを受領する際、相対しているエンティティ（ユーザ）に対し発行されたクレームであることを検証する必要がある。

これらの実現のためには、以下の処理が必要となる。まず、クレーム発行要求時（処理③）で、ユーザに紐づく形で CP にクレームを発行して貰うため、後で RP が暗号的に証明されていることを検証可能な、何らかの形で自らのエンティティを示す情報を連携する。次に、クレーム発行時（処理④）では、CP は、処理③で受け取った情報に紐づける形でクレームの発行を行う。そして、クレーム検証時（処理⑦）では、ユーザのウォレットを介しクレームを受け取った RP が、そのクレームが相対しているユーザに紐づくものであることを、暗号的に証明されていることの検証を行う。これは、クレームが CP により発行されたものであることを電子署名を用いて検証を行う観点とは別に、考慮すべき観点である。

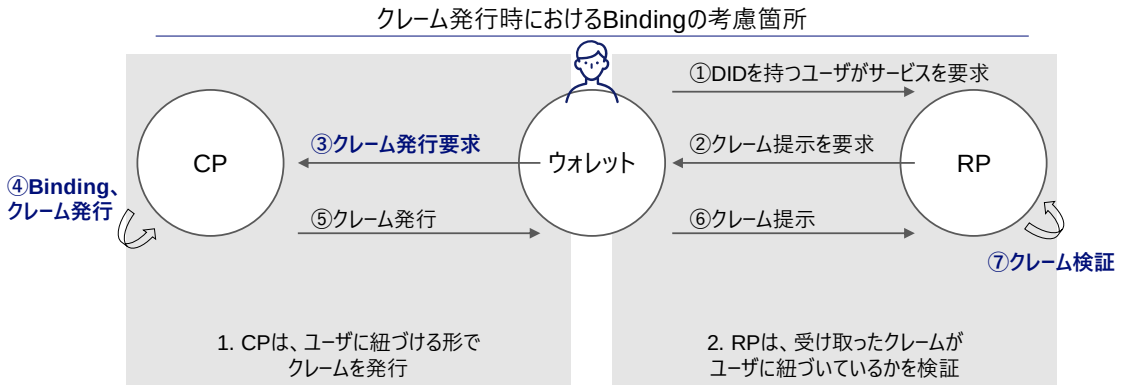


図 0-76：Binding の方式

例えば OpenID Foundation の策定する”OpenID Connect Claims Provider[279]“では、それぞれ以下の処理を規定している。

「処理③：クレーム発行要求」において、OpenID Connect Core の仕様中に登場する「Request Object[280]」という仕様を用い、リクエストの電文に対し DID 秘密鍵で署名を付与し、CP が署名を検証することで、このリクエスト電文が（DID 秘密鍵を操作可能な）DID 所有者から来たものか否かの判断を可能とする。

「処理④：Binding およびクレーム発行、処理⑦：クレーム検証」において、紐付情報として、ウォレットの UUID や DID 識別子（Decentralized Identifier） 或いは DID 公開鍵情報等をクレームに含めて発行することで、RP がクレーム受領時に、DID 所有者に紐づいたものかどうかの検証を可能とする。

279 OpenID Connect Credential Provider, http://lists.openid.net/pipermail/openid-specs-ab/attachments/20210528/2f163c71/attachment-0001.bin

280 “OpenID Connect Core 1.0 incorporating errata set 1”, https://openid.net/specs/openid-connect-core-1_0.html#RequestUriParameter

Credential Endpoint Request Parameters

```
POST /credential HTTP/1.1
Host: https://issuer.example.com
Authorization: Bearer  <access-token>
Content-Type: application/json
{
  "request": <signed-jwt-request-obj>
}
```

リクエスト内容に対し、Holderが自身の署名鍵
（DID秘密鍵）で署名付与

図 0-77：処理③：クレーム発行要求と、DID 所有者との紐付け・確認

エンティティとの紐付情報	

ウォレットに
関与するUUID
	{（中略）
	"credentialSubject":{
	"id": "urn:uuid:dc000c79-xx（中略）",
	（中略）
	}

DID識別子	{（中略）
	"credentialSubject":{
	"id": "did:example:1234",
	（中略）
	}

クレーム内の"credentialSubject" 値に対し、クレームの発行対象である
エンティティのメタデータを格納（例：UUID、DID識別子、DID公開鍵、等）

図 0-78：処理④、⑦：クレームと、DID 所有者との紐付け・確認

クレームに紐付情報を格納することでエンティティとクレーム間の紐付を証明可能となる一方、同情報を用いた不当な名寄せへの懸念についても、考慮・対策が必要となる。DID 識別子は、複数の使い方が想定される。このうち、RP 毎に異なる DID 識別子を資料する Pairwise では、クレームの種別によってはクレームに内包される DID 識別子の突合が可能となる懸念がある。

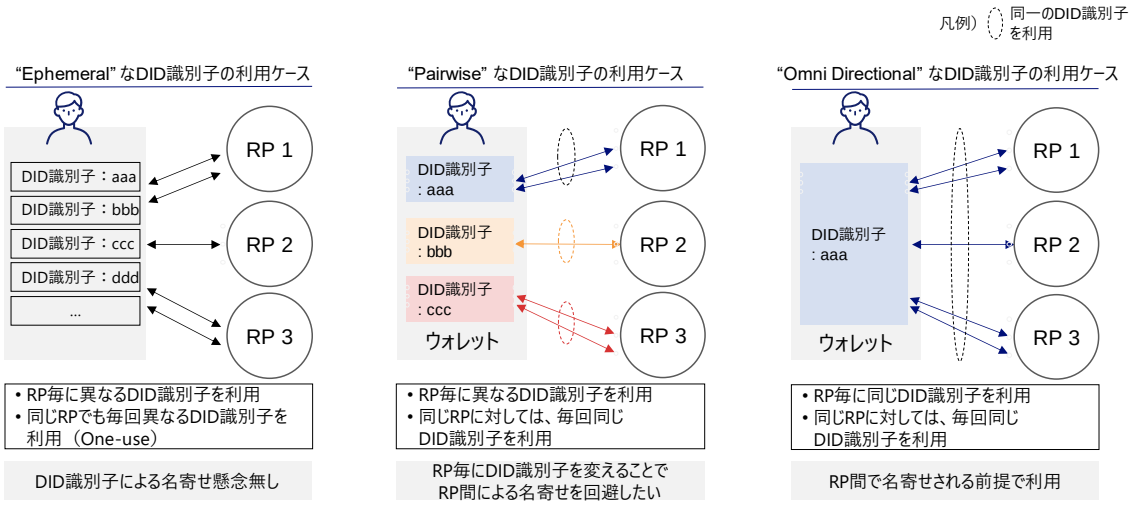


図 0-79：DID 識別子の使い方

Binding に“Pairwise”な DID 識別子を用いている場合、クレームに Bind される DID 識別子は RP に応じ異なる。故に、各 CP はクレーム生成の段階で、Bind する DID 識別子を意識し発行する必要がある。

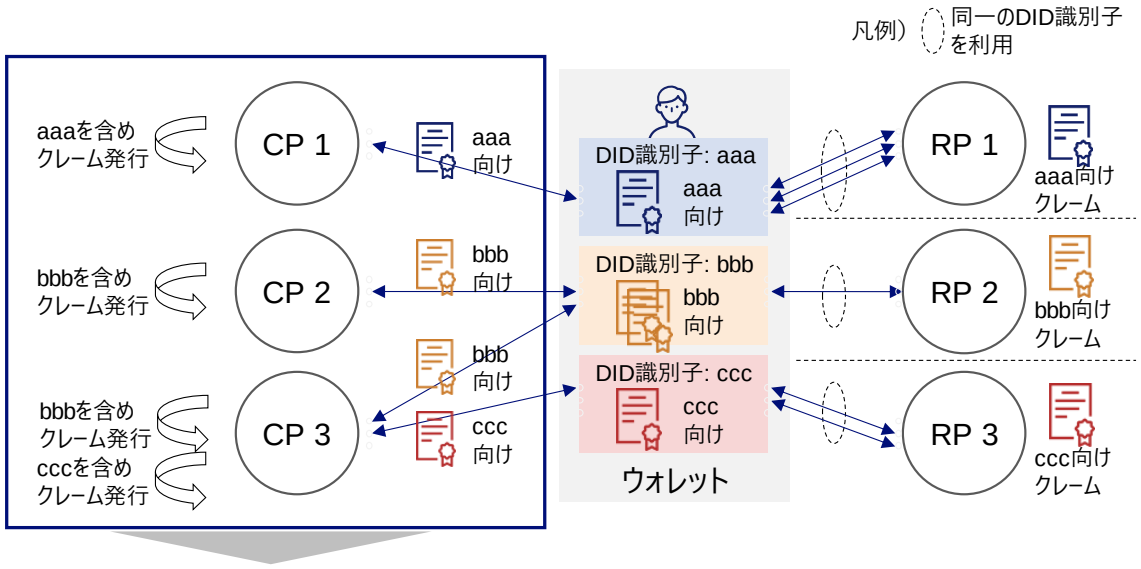
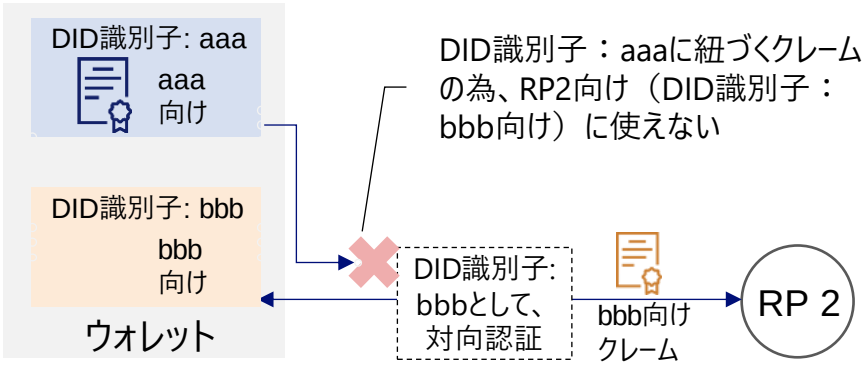


図 0-80：“Pairwise” な DID 識別子利用におけるクレーム連携のイメージ

例えば以下のケースでは、RP2 のサービス利用におけるオンボーディング時、ユーザはまず RP2 向けに DID 識別子を発行し、クレーム提示の準備を始める。その際、既に発行済のクレームを使おうとしても、同クレームは RP1 向けに新たに作成した DID 識別子と紐付いていない為、新たにクレームを取り直す必要が生じる（DID 識別子に応じた Dynamic なクレームの生成・取得が必須となり、3-1-2 で述べた「長期のデジタルアイデンティティの保管・利用」の特性への制約となる懸念がある）。

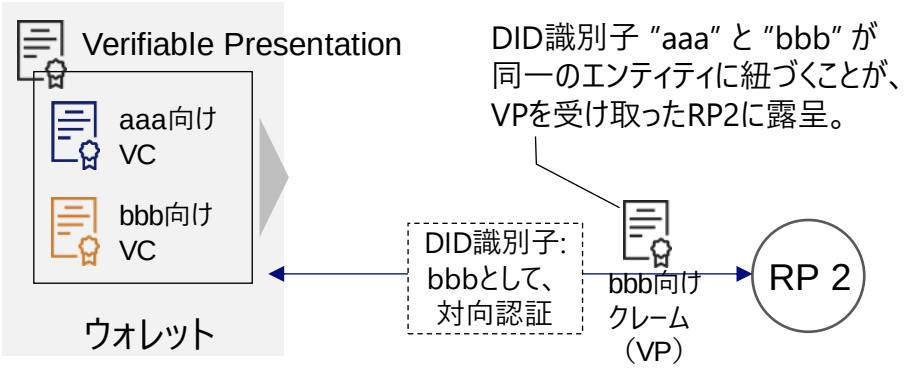


- RP2はウォレットのDID識別子を ”bbb” と認識し対向認証を行った上で クレーム連携を実施する。
- DID識別子 ”aaa” 向けのクレームでは”bbb” にBindされていないため、 RP2に対し使えない。改めて ”bbb” 向けの形でクレームの再発行が必要。 （クレームの ”Stock & Forward” が出来ず、SSIに求められる特性 「長期のデジタルアイデンティティの保管・利用」の実現が困難）

図 0-81：懸念①：Static なクレームの利用が困難

また、W3C Verifiable Credentials Data Model 1.0 の Verifiable Presentation（VP）[281]では、複数 VC を格納可能と規定されている。その際、VC に Binding されている DID 識別子が異なる場合、受領した RP2 において、それらの異なる DID 識別子が、「同一エンティティに紐づいている」と露呈してしまう。

[281] “Verifiable Credentials Data Model 1.0”, https://www.w3.org/TR/vc-data-model/



- RPが結託し上記のBindingに用いる紐付情報を突合することで、Pairwiseを用い異なるDID識別子をRPに応じ使い分けることで実現していた "RP+RP'-U Unlinkability" が損なわれてしまう。

図 0-82：懸念②：クレーム集約時における、包含するクレームと紐づく DID 同士の紐付

これまで述べた通り、Binding における考慮事項をまとめると以下の通りとなる。

プライバシーを考慮すると、 Binding 実現において以下 2 つの要件への考慮が必要である一方、識別性の高い情報をクレームに含めて発行するだけでは、Binding とプライバシー確保の両立は困難である。

表 0-30：プライバシーに配慮した Binding に求められる要件と懸念事項

Binding における要件	DID 識別子を用いた Binding における懸念事項
Dynamic なクレーム生成・取得ではなく、Static なクレームの連携が可能（Stock & forward）	・ Binding の為に、DID 識別子をクレームに含め発行を行う場合、RP との間で用いる DID 識別子が変わると、クレームの再発行が必要となる。 ・ 結果、過去に Wallet に格納していたクレームが意味をなさなくなる可能性があるため、3-1-2 で述べた「長期のデジタルアイデンティティの保管・利用」実現が困難となる懸念がある（毎回動的に CP にクレーム発行を要求する必要が生じ得る）
RP が結託し上記の Binding に用いる紐付情報を突合してもユーザの名寄せが出来ないこと（RP+RP'-U Unlinkability）	・ 複数クレームを含める形でのクレーム提示を想定している仕様もあるが（W3C Verifiable presentation[282]）、含まれるクレームに Bind された DID 識別子が異なる場合、それを受領した RP から見て、異なる DID 識別子が同じエンティティに紐づ

[282] "Verifiable Credentials Data Model 1.0", https://www.w3.org/TR/vc-data-model/

	くことが露呈する懸念がある（異なる DID 識別子を使い分けていても、名寄せの懸念がある）

SSI モデルでは、第三者がアイデンティティの管理主体に介在することなく、個人が自分自身のアイデンティティをコントロールできるようにする必要がある。この実現のため、属性に関するコントロール権を確保するため、ユーザ自身が ID プロバイダとなる形が考えられる。

ユーザが ID プロバイダとなりクレームの連携を行う場合、どこに ID プロバイダの機能をデプロイするかによって、トポロジーの実装は複数考えられる。仮に、「ウォレット」などのローカルマシンにデプロイする場合、Federation モデルを Distributed と Aggregated Claims Model を導入し、複合することでの実現アプローチが考えられる。実際、過去に同じトポロジーを持つサービスもデプロイされており、実現可能性が期待された。一方で、そうしたサービスが実際のビジネスにおいて広範に利用されているとは言い難い状況がある。

本項では、こうした背景を踏まえ、SSI モデルの課題整理に先立ち、まずは Federation モデルにおける SSI/DID の充足可否を整理の上、実際のビジネスにおける展開の阻害要因となる課題の整理を行う。

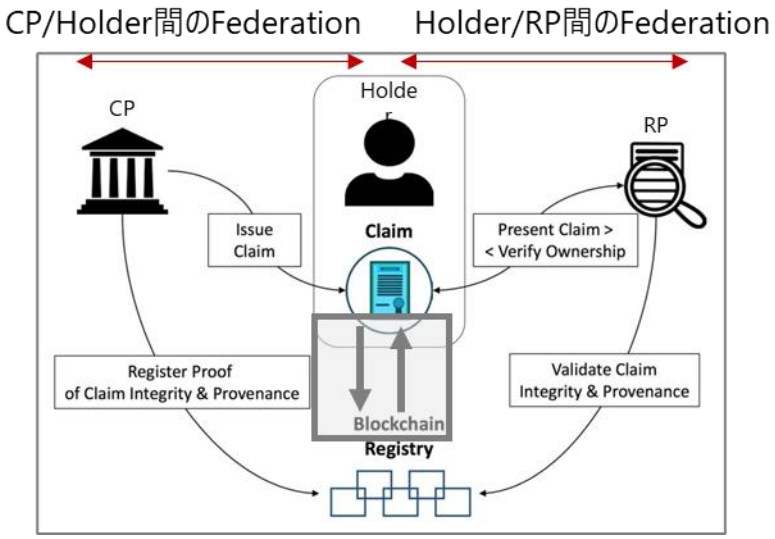


図 0-83：ローカルに ID プロバイダ機能をデプロイする場合の SSI モデル実現像[283]

OpenID Connect の仕様を用いることで、SSI/DID の特性である認証と属性の分離、分散した属性の活用と選択的な提示、提示先の秘匿（Unlinkability）は実装が可能である。

[283] decentralized-id.com 資料を基に作成

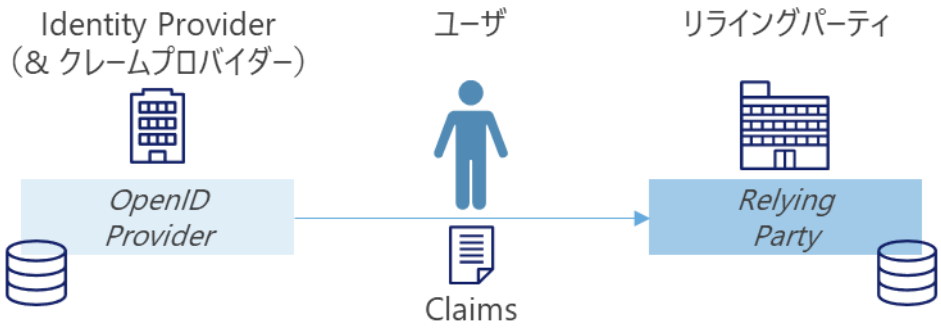


図 0-84：一般的な Federation モデル

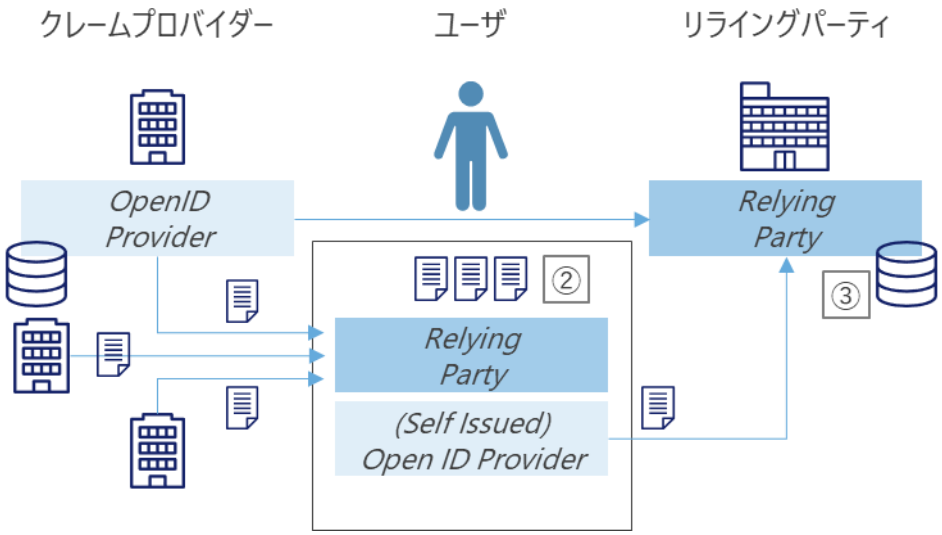


図 0-85：トポロジーを変えた Federation モデル
（e.g. Aggregated / Distributed Claims Model ）

表 0-31：SSI/DID の特性、OpenID Connect の対応仕様、実装概要

SSI/DID の特性	OpenID Connect の対応仕様	実装概要
①認証と属性の分離	Self-Issued Open Provider（SIOP）	ユーザ自身が IdP となることで、CP/ホルダー間、ホルダー/RP 間での Federation によるクレーム連携を実施。
②分散した属性の活用・選択的な提示	Aggregated Claims	複数の CP 上のクレームを集約。
③提示先の秘匿（Unlinkability）	Distributed Claims	ホルダーに収集したクレームから、RP に対し選択的にクレームを提示。

長期のデジタルアイデンティティの保管と利用の特性については、OpenID Connect の仕様策定範囲外となっており、実現する場合には、別途長期署名に関連した仕様等を組み合わせた実装の考慮が必要となる。長期署名の規格としては、PKCS#7 や CMS 等の署名フォーマットに対応した「CAdES」、XML 署名フォーマットに対応した「XAdES」、PDF 署名フォーマットに対応した「PAdES」等があり、また近年では JSON Web Token の署名フォーマットにも対応した、「JAdES」 も ETSI にて規定されている。

表 0-32：長期署名規格例

長期署名規格	対象 フォーマット例	主な規格 （Technical Specification）
CAdES （CMS Advanced Electronic Signatures）	CMS, PKCS#7	ETSI TS 101 733 v2.2.1 (2013-04) ISO 14533-1:2014
XAdES （CMS Advanced Electronic Signatures）	XML	ETSI TS 101 903 v1.4.1 (2009-06) ISO 14533-2:2012
PAdES （PDF Advanced Electronic Signature）	PDF	ETSI TS 102 778-1/2/3/4/5 (2009-07) ETSI TS 102 778-3 V1.2.1 (2010-07) ISO 14533-3:2017 ISO32000-2: 2020
JAdES （JSON Advanced Electronic Signature）	JSON	ETSI TS 119 182-1 V1.1.1 (2021-03)

OpenID Connect を踏まえた 4 つの特性をもつ IMS のデプロイ可能性を検討した結果、技術的な実装が可能ではないかという仮説を導出した。

仮説の裏付けとして、Linksafe による分散型識別子の取得や neustar によるディレクトリサービスといったサービスとして展開された事例の調査と確認を行った。機能面での充足は一定確認できたものの、ビジネス面、運営面の両面における課題から、広範に展開されず利用が広まっていない実態が明らかとなった。

ビジネス面の主な課題は、データブローカーに代表される CP による、データ提供機会の減少・連携先が秘匿される点に対する反発である。データ提供件数に応じた課金請求モデルを採るデータブローカーの立場では、ホルダーにクレームを格納し何度も提示可能となると、自分たちのビジネス機会の損失に繋がる。データブローカーは、自身のデータが

どこに連携されたかのナレッジを元にデータ提供元等ビジネス機会の拡大を図るが、リライングパーティを秘匿される事で、ニーズの把握が困難となる懸念がある。

運営面の主な課題は、ホルダーの運用主体を完全にユーザに委ねた場合、ホルダーの運用・管理能力に対する懸念から CP と RP からの信用を得られないケースがあり得る。

同モデルでは、ユーザがホルダーとしての運用・管理責任を負い、自らのクレデンシャルを管理する。ホルダーの運用・管理能力の不足や責任能力の欠如の懸念がある。特に Recognition に用いられる DID 鍵の運用・管理を行う点を考慮すると、当該能力の欠如への懸念は、提示される CSP としての提供サービス（認証）に対するトラスト欠如に繋がり得る。両面における課題は OpenID Connect に限らず他の SSI モデル向け実装でも生じ得る課題である。

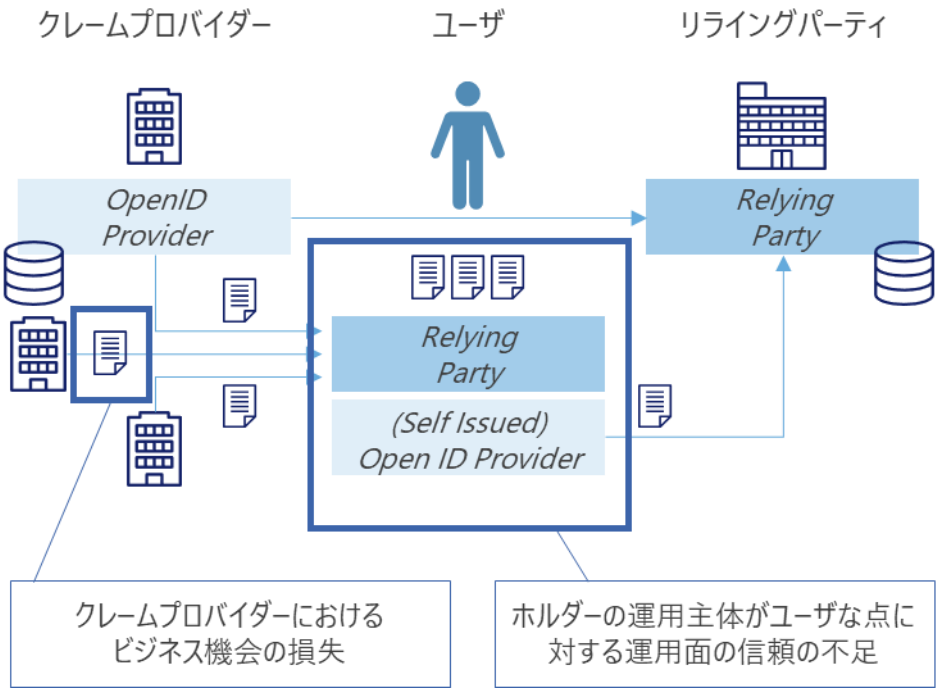


図 0-86：Federation モデルでの SSI/DID 実現における課題箇所

第４章　デジタルアイデンティティ活用に向けた今後の論点

（必要事項はすべて本編に記載したため、本資料では省略）

Appendix1　第 2 章の主な参照文献

本 Appendix は、2 章冒頭で言及した主な既存研究につき、その概要のうち、主に金融サービスに関わる部分を中心に概要を整理したものである。なお、文中の図表は、特段の注記がない場合はすべて各対象文献から抜粋したものである。

1. The Future of Onboarding （2016）

発行者

PwC

ロンドンを本拠地とする会計監査、ディールアドバイザリー、ビジネスコンサルティング、税務、法務などに手掛ける総合ファーム

本レポートの狙い

onboarding について、デジタルアイデンティティ活用の現状及び展望を整理し、グローバルな onboarding のスタンダードを整備し業界全体の効率化を図ることが重要である旨を提言

主な論点

- 金融機関の現状の onboarding プロセスにおける課題

現状、多くの金融機関で採用されているクライアント・オンボーディングのプロセスは、書類を集める、個別に信用調査機関に顧客の身元を確認する等の対応を行っているが、下図の課題がある旨指摘している。

・ 顧客から、即時の口座開設要請や来店せずに口座開設行いたい要請がある。
・ 金融機関における検証に非常に時間がかかる。
・ マニュアル作業であるため、KYC の検証強度が区々である。

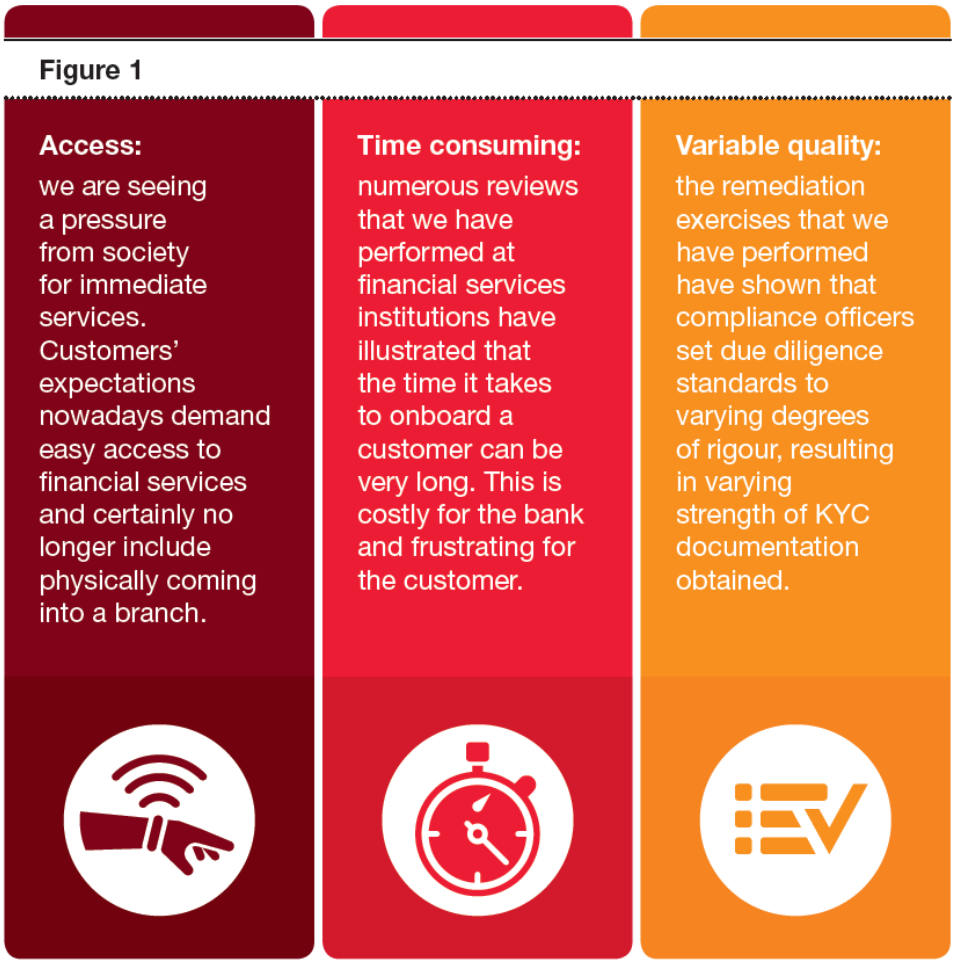


図 2- 51　onboarding プロセスにおける現状課題

- 課題解決に向けたデジタルアイデンティティの活用

  上記課題の解決事例として、本文献では以下を挙げている。

  ・ ノルウェーの BankID

  ノルウェーでは、公的機関と民間企業の両方で、BankID をデジタル ID として使用することが可能である。2016 年時点では、成人人口の 80%がデジタル ID を持っており、この銀行 ID を使用することで、個人は簡単に銀行口座を開設することができる。

  ・ オランダのデジタルアイデンティティ

  政府機関や医療機関に用途を限定してデジタルアイデンティティを活用

  ・ EU 全体の動き

  電子署名と電子 ID を認識するための単一の法的枠組みの確立（eIDAS）

  ・ 英国の GOV.UK Verify

  公的機関と民間部門の両方でデジタル ID を活用できるプラットフォームを整備

● GOV.UK Verify の金融機関の onboarding プロセスにおける活用の検討

本文献では、GOV.UK Verify の金融機関における活用について検証を実施している。結論としては、銀行の onboarding においてはいわゆる本人確認に加えて、制裁者リストとのスクリーニングや、個人の勤務先・収入等様々な情報を確認している点が、GOV.UK Verify が担保している本人確認との違いである旨が指摘されている。ノルウェーでは、銀行が ID プロイバイダーとしてこの点を担保しているため、デジタル ID の導入が成功している点を指摘している。

● GOV.UK Verify に必要な認証レベルの担保

本文献では、GOV.UK Verify が持つべきデジタルアイデンティティの保証レベルについても検討を行っている。その中で、バイオメトリックスの活用に触れている。英国では、デジタルアイデンティティの保証レベルは、英国政府の情報保証に関する国家技術機関である CESG（Communications-Electronics Security Group）と内閣府が作成した「グッド・プラクティス・ガイド」に記載されており、バイオメトリックスの活用は最高位のレベル 4 の保証レベルの確保につながると期待されている。

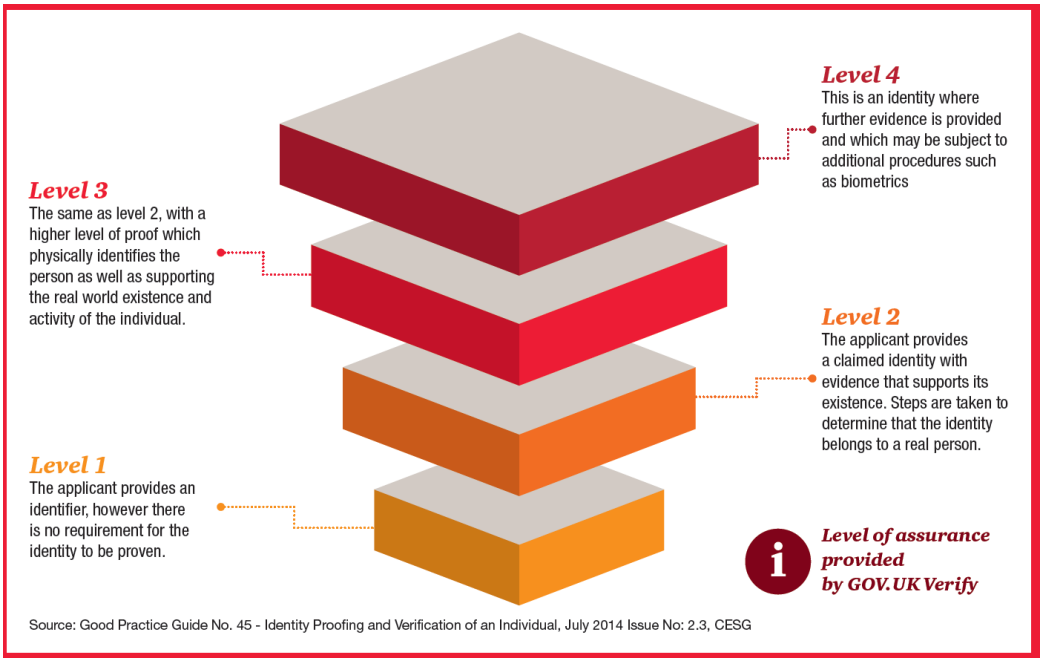


図 2- 52　CESG が定める保証レベル

また、バイオメトリックスの活用は、新たな規制である決済サービス指令 2（以下、PSD2：Payment Services Directive 2）への対応にもつながる点が指摘されている。

PSD2 は、「強力な顧客認証」というコンセプトを導入しており、これは顧客のアイデンティティを認証する際に 2 つ以上の独立した要素に基づいていることを求める。
・ 知識（ユーザーだけが知っているもの） - パスワード等
・ 所有（ユーザーだけが所有しているもの） - モバイルデバイス等
・ 固有性（ユーザーが持っている何か）-バイオメトリクス等
バイオメトリックスを認証要素として活用することが期待されている。

- 金融包摂への期待

本文献では、金融業界全体として、デジタルアイデンティティを活用した onboarding のスタンダードを作ることができるのではないかと提言を行っている。世界の金融業界全体のスタンダードとなる onboarding プロセスを構築することができれば、onboarding プロセスが未整備な途上国において速やかな体制の構築が期待でき、途上国国民の金融サービス活用が促進される点を指摘している。また、これは途上国の国民のみならず途上国の金融機関にも言えることであり、onboarding のスタンダードの導入により世界で金融機関の AML/CFT 等の規制対応の平準化が図られ、クロスボーダー取引の円滑化が期待される点が指摘されている。

- 今後にむけて

本文献では、本文献執筆時点（2016 年）から 24 か月以内でコンプライアンスコストが 55%上昇する旨を指摘している。本文献では、この解消に向けては、金融機関が個別対応を実施するのではなく、国際的なスタンダードを整備し業界全体としてコスト削減につながるように議論を推進すべきである旨を提言している。

2. Digital Identity:the current state of affairs （2018）

発行者

BBVA

スペイン・バスク自治州・ビルバオに本社を持つ銀行グループ

本レポートの狙い

デジタルアイデンティティ活用の現状と課題、今後の活用の方向性を整理しつつ、その中で銀行が果たすべき役割について考察

主な論点

- 本文献におけるデジタルアイデンティティの定義

  デジタルアイデンティティの定義は各種標準化団体等で行われており、その内容は多岐にわたるが、本文献では、デジタルアイデンティティを、“個人の実体をオンラインでの相互作用と結びつける属性のセット”と定義して議論を行っている。

- デジタルアイデンティティの信頼性を確保するためのアイデンティティ管理

  本文献ではデジタルアイデンティティの信頼性確保の重要性に触れつつ、信頼性を確保するためのアイデンティティ管理の方式について、現在のシステムは以下の要素に基づき各個人の単一のアイデンティティを確立する傾向がある旨言及している。

  ・ 個人が知っていること（パスワード、暗証番号、セキュリティコード ）
  ・ 個人が持っているもの（身分証明書、銀行カード ）
  ・ 個人がどのように見えるか、またはどのように行動するか（身体的／行動的特徴にまたがるバイオメトリクス）
  ・ 個人がどこにいるか（携帯電話番号、地理的位置情報、IP アドレス、ソーシャル・ネットワーク・サイト）

- アイデンティティプロバイダ

  本文献では、デジタル アイデンティティにはプロバイダが必要であるが、世界的に受け入れられている アイデンティティプロバイダは存在しない旨を指摘している。現状、主なアイデンティティプロバイダは以下の通りと述べている。

  ・ 公共部門

    伝統的に、物理的な世界では、政府が ID の主な提供者であった。公的機関によって管理されるパスポートや ID カード等の文書が例として挙げられる。国家 eID は、通常、政府サービスへのアクセスを提供するために発行される。

  ・ 民間部門

民間企業は、例えばオンラインバンキングのユーザ作成等において、自ら顧客を検証し、ID の提供を行っている。

・ フェデレートアイデンティティ

オンラインにおける ID 検証が必要なサービスの増加に伴い、複数のサービスプロバイダが提供する ID およびクレデンシャルを管理できる ID プロバイダ・システムが求められる状況となっていると、本論文では指摘している。フェデレートアイデンティティの事例として、本文献ではスウェーデンで多数の大手銀行が開発し、一般市民、当局、企業のメンバーが使用できるソリューション、BankID を挙げている。BankID ネットワークには、Danske Bank, ICA Banken, Ikano Bank, Länsförsäkringar Bank, Nordea, SEB, Skandiabanken, Sparbanken Syd, Svenska Handelsbanken, Swedbank, Ålandsbanken が含まれている。

● デジタルアイデンティティ普及のドライバー

本文献では、デジタルアイデンティティ普及のドライバーとして以下の点を挙げている。

・ ユーザがよりオンライン上で多く活動するようになるという行動の変化
・ オンライン上で様々な取引を行うために、オンラインにおける自らの信頼性を確保する必要性
・ オンライン上でのプライバシーの確保のための堅牢なデジタルアイデンティティシステム構築への期待
・ 生体認証・ビッグデータ分析等の新しい技術の活用
・ 現状業務と比較したコストの減少

● デジタルアイデンティティにおける銀行の役割

本文献では、銀行にとっての新たなビジネス機会として、さまざまなセクターにまたがるデジタルアイデンティティの信頼されるプロバイダになることが指摘されている。銀行の以下の特性が指摘されている。

・ 銀行は、身元確認の分野で長い経験を持っている。かつては物理的な世界で、そして今はデジタルの世界で、顧客のアイデンティティを確認するためのプロセス設計に取り組まなければならなかったため、ノウハウが蓄積されており、他の業界にその知識を提供することができる。
    ・金融機関は一般的に他の機関よりも消費者から信頼されている。
    ・銀行は、金融部門が規制されていることから、コンプライアンス対応に慣れている。銀行は規制により、マネー・ローンダリングを追跡するために、顧客のデューデリジェンスを行うことがますます求められるようになってき

ており、この規制を遵守するために培ったノウハウは外部に提供できるものとなっている。

一方、かかる期待がありながら銀行がプロバイダとなることを躊躇する要因として以下と指摘している。

・問題発生時の責任への懸念
・問題発生時のレピュテーション懸念
・プロバイダとなるためのシステム投資負担

● デジタルアイデンティティ活用上の課題

他の文献等でも指摘されているサイバーセキュリティや相互運用性の課題とともに、本文献では、ユーザのコントロールの欠如（情報のデジタル化に伴い、コピーにより容易にデータ取得が可能となり、ユーザーデータ利用のコントロールが難しくなる懸念がある）、を課題として挙げている。

● 今後への期待

バイオメトリックス等の新しい技術を活用したセキュリティ強化や相互運用性の確立に加え、自己主権型 ID への期待も述べられている。

ID 管理システムは進化しており、ユーザはますます自分の ID の使用を制御できるようになり、ユーザ中心の ID と呼ばれるものへと移行していくと述べられている。（下図参照）

・ 最初は、ユーザがサービスプロバイダから独立して ID プロバイダを選択できるようにすることで、ユーザがより多くの制御を得られるように開発される。
・ しかし、このシステムでは、ユーザは自分の ID のコントローラーまたは発行者に依存しなければならないため、セキュリ ティの問題が残る。セキュリティ当局は、サイバー攻撃の標的になりやすく、インサイダーと敵対者のいずれかからの悪用によりシステムのセキュリティが破壊されるリスクを指摘している。
・ 次のステップは、権限が多数の信頼されたアクターの間で分散される分散型 ID システムであろう。これは、しばしば自己主権型 ID と呼ばれるものである。分散型台帳技術の採用により、個人は自分のデータを取得、複製、移動、送信等のコントロールを自ら行うようになり、コントローラー、発行者、またはプロセッサに頼る必要がなくなると本文献では指摘している。また、自己主権型 ID のインフラ構築におけるブロックチェーン活用への期待も述べられている。

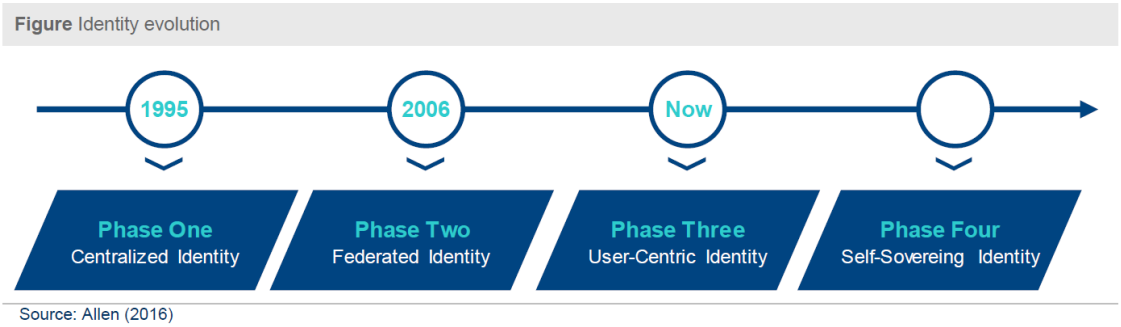


図 2- 53　デジタルアイデンティティの管理形態の変遷

3. The value of digital identity to the financial service sector （2016）

発行者

OIX（Open Id Exchange）

2010 年に設立された、ID 分野に関わるすべての人がつながり、協力し合い、相互運用可能で信頼できる ID に必要なガイダンスを開発するためのコミュニティ。 Trust Frameworks の定義と教育を通じて、すべての人が信頼でき、誰もが認める ID を持てるようにするためのルール、ツール、信頼を創造することを目的に活動

本レポートの狙い

英国において、金融サービス部門内で、信頼できるオンライン取引を可能にするために直面している課題に焦点を当て、デジタル ID の再利用が解決策になるかどうかを調査・分析すること。調査は、顧客や金融機関へのインタビューを通して実施された。

主な論点

- 金融サービス業界のアイデンティティニーズ

本文献執筆当時、英国金融業界は、今後 3 年間で、多くの英国および EU の指令、規制、イニシアチブを実施しなければならない状況にあった。

表 2- 32　2016 年当時の英国及び EU の指令・規制・イニシアチブ予定

Regulation / Initiative	Date of Implementation
EU Payment Account Directive （PAD）	September 2016
EU Fourth Money Laundering Directive （4MLD）aaa	June 2017
Open Banking （Competition and Markets Authority）	Early 2018
Second Payment Services Directive （PSD2）	January 2018
General Data Protection Regulation （GDPR）	May 2018

これらの変化の全体に共通して見られるテーマは、アイデンティティの問題であると本文献は指摘している。アカウントの開設や管理、支払いの開始、組織間での個人データの共有、あるいは顧客を保護し、個人情報の誤用や乱用、詐欺を防ぐためには、強力な顧客識別と認証が不可欠であると言及している。

- イギリス政府の動き

2016 年 5 月、英国政府は新しいデジタル ID スキーム“GOV.UK Verify”を正式に開始した。Gov.UK Verify は eIDAS フレームワークの Level2 に相当する認証技術で

あり、各個人が選択した IdP から GOV.UK Verify を通じて公共サービスへアクセスする際の本人認証手段である。

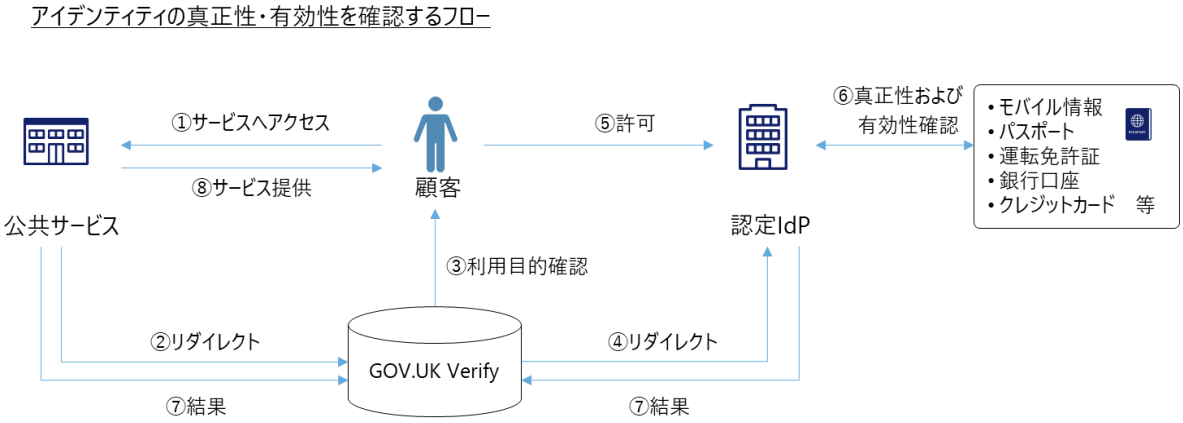


図 2- 54　GOV.UK Verify 認証フロー

出所）本文献の記述等を元に NRI 作成

- 本調査の実施内容

本文献では、英国政府が広く普及を目指している GOV.UK Verify を活用して銀行口座開設を可能とした場合の、顧客・金融機関のメリットや課題をインタビューにより検証した。

・ 顧客

全体的に、金融サービス取引における GOV.UK Verify ID の再利用という概念には大きな障壁はなかった。参加者は、現在の金融サービスの onboarding プロセスに不満を表明し、それを申請完了の障壁と見なしていた。参加者は、デジタル ID を使用することで、プロセスがより簡単に、より迅速に、より安全になると考えていた。

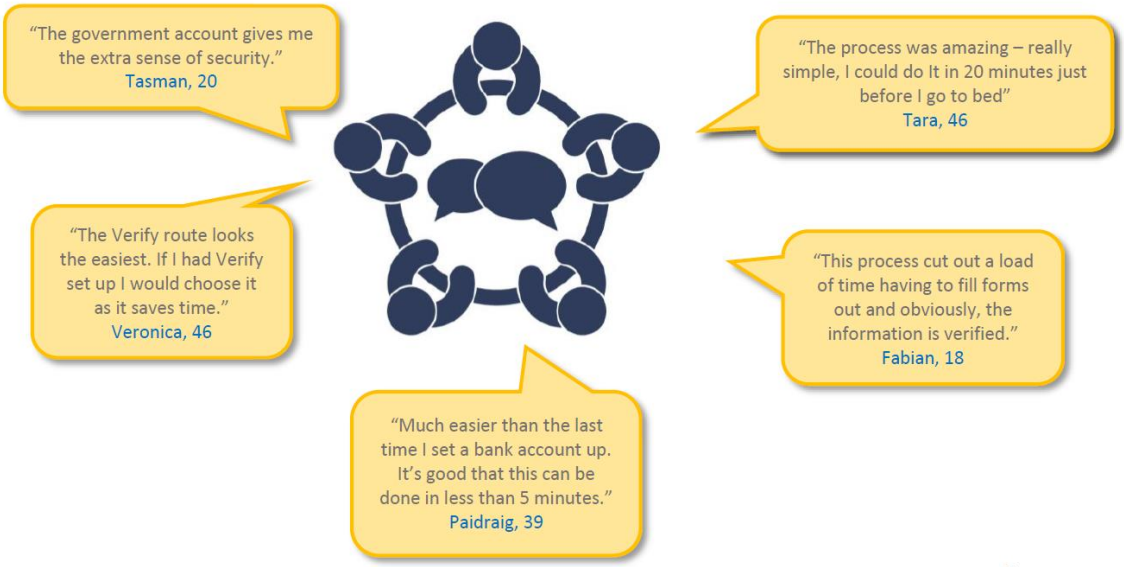


図 2- 55　本調査の顧客インタビューの回答例

- 金融機関
  - GOV.UK Verify ID を再利用することの強みは、最高水準で検証された強力な ID を提供できることにあると評価された。保証レベルがすでに確立されていたため、金融機関にとってはリスクが軽減された。統合されたアイデンティティモデルを使用することは、セクター横断的な市場内での相互運用性のため、ポジティブであると評価された。
  - 金融機関は、消費者の認識不足、規模、および GOV.UK Verify の再利用にあたっての商業的推進力がないように見えることについて懸念を表明した。金融機関はまた、収入証明、資金証明など、一部の取引を完了するために追加の ID 属性情報が必要になると感じていた。
  - ビジネスと顧客体験を向上させるための巨大な機会があると評価された。また、詐欺の減少と、顧客が詐欺に遭うのを防ぐためにデジタル ID の再利用が有用である可能性についても言及された。
  - 規制当局の承認がないこと、内閣府と財務省の間に明確な連携がないことが、このアプローチの主な脅威であると言及された。

- 結論

  調査の結論として以下の点が述べられている。
  - 広く採用され、目的に適合し、信頼され、標準に基づいたデジタル ID スキームは、金融サービス業界にとって重要な価値を持つ可能性がある。

- 顧客にとっては、金融機関との口座開設プロセスとその後の取引を簡素化することができる。
- 金融機関は、顧客の識別と管理に一貫したアプローチを提供し、口座開設や取引のコストを削減することができる。ポートフォリオ管理などの新しいサービスの提供を容易にし、既存サービスの提供を変革することができる。
- 産業界にとっては、決済等における、新しいユーザ中心のビジネスモデルを提供するための基盤として、標準に基づいたデジタル ID スキームを活用することが期待でき、差し迫った法律の要求に応えながら、顧客にとってより競争力があり、ダイナミックで魅力的な市場を創出することが期待できる。
- セクター横断的なスキームに対して政府や規制当局の承認を得ることは、デジタル ID スキーム構築のための重要な触媒となる。ユーザ調査を通じて、政府に承認された ID スキームを持つことの価値が示された。

4. Digital Identity in the UK: The cost of doing nothing（2018.4）

発行者

OIX（Open Id Exchange）

本レポートの狙い

英国における

・ デジタルアイデンティティに対応しない場合の潜在的なコストを明確化
・ 将来のデジタルアイデンティティニーズを形成する要因を特定
・ デジタルアイデンティティに対応しないコストが大きすぎて負担できない場合に備えた、海外事例に基づいた潜在的な解決策の探究

を実施し、コスト面からデジタルアイデンティティ導入推進の是非を検討

主な論点

● 英国のデジタルアイデンティティ活用の現状

本文献では、英国のデジタルアイデンティティ活用状況につき以下の通り言及している。

・ 政府独自の ID スキーム GOV.UK Verify の状況

GOV.UK Verify は政府デジタル・サービス（GDS）が開発を主導してきており、信頼性はあるものの、用途が公共サービスに限定されていることから利用者が当初の期待より伸び悩み、その結果利用可能サービスの拡大もなされないという悪循環に陥っている。

・ 民間セクターのデジタルアイデンティティの状況

民間セクターのデジタルアインデンティティが市場に出回っているが、普遍的に利用できるものはなく、多くは ID に関わる規制要件（金融規制等）を満たすことができていない状況である点が指摘されている。一例として、民間のデジタルアイデンティティ発行の際に利用者から受け入れている身元確認の文書が信頼性の高いものではないため、当該デジタルアイデンティティは規制対応が必要な金融サービス等には利用できないというケースが挙げられている。

・ デジタルアインデンティティ活用の障壁

GOV.UK Verify における属性の不足（民間サービスでの活用には氏名、住所、生年月日、性別の 4 つの属性のみでは不足）、問題発生時の責任、共通のルールの欠如等、他の文献でも指摘されている点に加え、英国の特徴として、政府 ID に対する懸念が挙げられている。10 年前に国民 ID カード計画が失敗したことは、国民 ID イニシアチブに対する継続的な国民の不信感に反映されており、データのプ

ライバシーとセキュリティに関する社会的な懸念の高まりと合わせて、将来のデジタル ID の利用に強い障壁を生み出す可能性がある点が指摘されている。

- デジタルアイデンティティ導入を行わないコスト

本文献では、デジタルアイデンティティ導入に向けた期待や課題を分析するとともに、デジタルアイデンティティ導入を行わずに現状の業務を継続した場合のコストも検討している。特に影響の大きい、金融分野についてはより具体的に分析が行われている。

・ KYC コストの増加

現在の AML および金融犯罪対策コストの上昇傾向が続く場合、銀行業界だけでも 2020 年末までに年間 25 億ポンドの追加コストがかかることになり、これは 50%の増加となる点が指摘されている。

・ 詐欺の被害の増加

オンラインでの ID 盗難被害等により、被害額が増加する点が指摘されている。

・ 機会損失のコスト

より多くの顧客データを収集し分析することで、収益機会に繋げることなどが期待される（次頁図参照）が、デジタル化を行わないことでこの機会を逸する懸念が指摘されている。

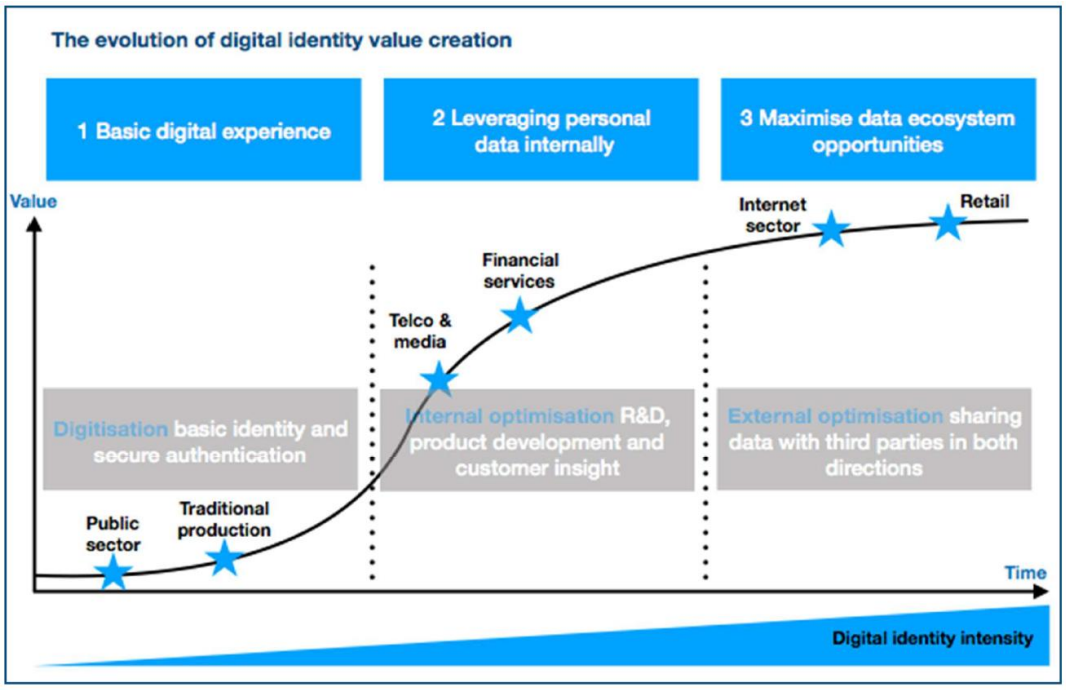


図 2- 56　デジタルアイデンティティを活用した価値創出イメージ

● デジタルアイデンティティ活用に向けた潜在的な解決策

本文献では、デジタルアイデンティティ活用に向けた潜在的な解決策を、海外事例を元に分析している。成功に向けては、民間部門（特に銀行部門）の関与の重要性や官民の協調の重要性等が指摘されている。（詳細次頁表）

● 結論

コンプライアンスコストの上昇等のすでに明らかになりつつある要素と、より詳細に分析したデジタルアイデンティティ導入コストを比較し、方針を決定すべきであると提言している。また、この決定は証拠を収集した上で、可能性の高いコストと利益の詳細な理解をもって行うべきである点も併せて提言している。

表 2- 33　デジタルアイデンティティ活用推進の成功要因・失敗要因

Success Factors	Failure Indicators
Private sector involvement （particularly banking sector） in the scheme design and delivery	Government-led with little or no private sector involvement
A shared vision for delivery between Government and industry, and clarity of roles	No shared vision, competing roles
Wide range and availability of services able to utilise the ID • Government / civil services • Private sector services	Limited service availability, lack of ubiquity
Banking services are accessible using the ID	Public services access only
High frequency of use - application to high-volume low-authentication purposes （e.g. website log-ins, age verification） and less frequent higher authentication uses （e.g. bank account opening）	Low frequency uses only
Existence of a mandatory ID for all citizens - e.g. social security number, national ID card.	Voluntary or no national ID scheme in existence.

An accepted history of national identity schemes	Public distrust of Identity schemes / 'big brother'
A national residential register	No central residential register
Available to be used via a variety of channels including Smart phone	e-Card-based only – particularly if a card-reader is also required
Low population states	Large population states
Using existing KYC data （particularly bank data） to actively enroll customers with an ID	'Organic' enrolment only
Public trust in the security of the scheme	Security breaches / questions
Public trust in how data will be used	Lack of trust in privacy rules
Liability model and trust framework addressed	The lack of clarity on liability
A clear business case - operational savings demonstrated and agreed by industry	Little economic benefit or high costs compared to current processes
Regulatory clarity / confidence	Regulatory ambiguity or barriers
Passive enrolment of customers - a smooth customer journey	Difficult or lengthy enrolment process - a poor customer journey
Well-connected / interoperable existing government IT and databases	Fragmented / unconnected / legacy govt systems
Well-connected citizenry （wifi, mobile, broadband adoption and coverage rates）	Unconnected societies （not that not all channels need to be well developed – e.g. mobile only schemes in Sub-Saharan Africa）
Barriers to access an ID removed or addressed	Low inclusion and low access rates
Strong public awareness and education – and govt and private sector working together to achieve this	Low awareness and or education level, or lack of joined up promotion.

5. Digital Identities in Financial Services Part 1: Embedding in AML Frameworks（Aug 2019）

発行者

IIF（Institute of International Finance）

1983 年に設立され、70 カ国を超える国の 500 近い民間の金融機関が参加する国際的組織。金融業界の健全な発展のためのリスク管理や支援を行い、業界を代表する機関として、金融に関する規制や基準の導入を政策当局などに提唱

本レポートの狙い

国際的な基準設定者や各国の規制当局が、デジタルアイデンティティをマネー・ローンダリング防止 （AML）フレームワークに組み込み、広く実用化し、金融犯罪に対する防御メカニズムを強化し、システムの 効率を高め、より包括的な AML フレームワークに貢献する方法について考察

主な論点

金融犯罪対策としてのデジタル ID のメリットと、規制当局等ルールメーカーが配慮すべき事項について述べられている。主なポイントは以下の通り。

- 金融犯罪対策としてのデジタル ID のメリット
  - 個人のアイデンティティを構成する固定の属性セットをまとめた単一のデータセットを作成し、中央のリポジトリ内に保存するか、その人物と交流のある機関（公共または民間）のネットワーク全体に保存することで、顧客のアイデンティティに関する単一の真実のバージョンを作成することができる。これにより、金融機関が保有する記録の完全性を強化することが可能であり、その結果、詐欺行為に対抗することができる。
  - また、デジタル化により、業務の効率化やデータの手入力等によるエラーの削減が可能になるとともに、デジタル ID をネットワーク内で共有することにより KYC の結果を金融機関間で共有することが可能となり業務の効率化が期待される。

- 規制当局が配慮すべき事項
  - テクノロジーに依存しないガイダンスの構築

    多くの選択肢を確保するため、どのソリューションを選択するかは、Digital ID を開発・使用する者の裁量に委ねられるべきであり、これらのソリューションは、金融犯罪に対抗するためのメリットに基づいて、基準と期待を満たしているかどうかでのみ判断されるべきものである。この実現のため、すべての国際的な基準設定

者は、開発中のアイデアについて民間部門と公的部門の間の緊密な協力を促進すべき

・ ソリューションに対する評価

ソリューションには、公的機関主導のもの、公的機関の支援や推奨を受けながら民間が主導で推進するもの（カナダの DIACC 等）、民間主導のものが存在する。このうち、民間主導のものについては、公的機関の支援や推奨を受けていないため、これらのソリューションを使用しても、（今のところ）AML 規則を満たすのに十分ではないと考えられているが、民間主導だから高リスクを一律に判断するのではなく、ID ソリューションが開発された場合に満たすべき基準を定めて評価を行っていくことが、イノベーション促進の観点からも重要である。

・ 民間企業と法執行機関の間のフィードバックループ

デジタル ID は、個人に一意に結びついた一連のデジタル属性として、効果的な情報共有エコシステムの構成要素となる可能性を秘めている。金融犯罪防止の分野では、より広範なデータ共有の議論が行われているが、デジタル ID を活用し、公共部門と民間部門が協力し、疑わしい活動に関する関連情報を共有することが考えられる。これにより、金融機関は業界の他のプレーヤーに脅威を警告することが可能となる。特に、同じ顧客を共有している金融機関の 1 つが FIU に報告する必要のある不正な行動を確認した場合に、他の金融機関を情報共有できることは金融犯罪防止上有効なソリューションである。

・ 業界全体としての AML 対応強化や効率化を実現するためのトラストフレームワーク・相互運用性の整備

現在、同一人物との取引を希望するすべての金融機関は、完全な本人確認と顧客確認プロセスを独自に実施しており、効率、データの質、情報の一貫性に明らかな欠点がある。これに対し、規制当局や標準化団体が AML/CFT に適用されるべき最低限の基準を十分に詳細に定義し、顧客確認を最初に実施した金融機関の実施基準が他社に開示されるといった、デジタル ID を広く共用し AML 対応強化や効率化を図ることが期待される。また、業界全体として効率化を図るためには、上記の通り基準を明確にしルールを共有することに加え、デジタル ID システム間の相互運用性を担保することが重要である。

・ デジタル ID 活用における IAL 整備の重要性

デジタル ID の普及をきっかけに、いわゆる「保証のレベル（IAL）」を含めた本人確認プロセスを再構築することが考えられる。現在の慣行とは対照的に、この概

念は、結果を決定する一連の固定された条件に依存するのではなく、リスクベースのアプローチを優先する。例えば、現行のガイダンスでは、「オール・オア・ナッシング」のルールとして、特定の種類の文書（パスポートなど）で本人確認を行うことを求めていることが多いが、保証のレベルに基づいて構築されたプロセスであれば、より柔軟に対応することができる。顧客は、自分の身元に関する主張の証拠としてさまざまなソースを提示することができ、金融機関は特定のケースのリスクに基づいてそれらを自由に受け入れることができる。これにより、金融機関は判断の際に、証拠の出所、誰が収集したか（政府、金融機関、第三者、または顧客が提供したもの）、独立したソースによって検証されているか、または顧客の自己開示のみに依存しているかなど、さまざまな要因を考慮することが可能となる。電子的な識別とその保証レベルに関する国際的な基準（NIST SP 800-63 や eIDAS ルールなど）がすでに存在しており、特に民間機関の間で使用される基準として、より広範な規模で活用することができる。

・ デジタル ID に問題が発生した際の責任分界やデジタル ID 共用のあり方の整理

ある金融機関が他金融機関に対して提供したデジタル ID に誤った情報が含まれており、それが原因で他金融機関においてマネー・ローンダリング等の問題が発生した際、他金融機関への賠償責任のあり方や、規制当局に対する法的責任や罰金支払責任等を明らかにする必要がある。

他社への依拠を幅広く認めれば認めるほど（例えば、ある金融機関で顧客確認実施済の顧客については他社では顧客確認不要とする等）問題発生時はリスクが連鎖的に波及するが、一方で、このリスクを回避するために、他社で顧客確認実施済みの顧客に対して他金融機関に一律で顧客確認再評価を義務付けると、効率化が図られないこととなるため、適切なバランスを検討する必要がある。

6. Digital Identities in Financial Services Part 2: Responsible Digital Identities,The Key to Creating More Inclusive Economies

発行者

IIF（Institute of International Finance）

本レポートの狙い

デジタルアイデンティティの活用が金融包摂にもたらす正負の影響や金融機関がデジタルアイデンティティのエコシステムに参画する意義について調査

主な論点

- デジタルアイデンティティと本人確認プロセスが金融包摂へ与える影響

世界銀行が 3 年ごとに提供している金融包摂に関する最大のデータセットである最新の 2017 年 Global Findex のデータでは、口座所有に対する障壁が下図の通り確認されている。

（赤枠がデジタルアイデンティティによる解消が期待されるもの）

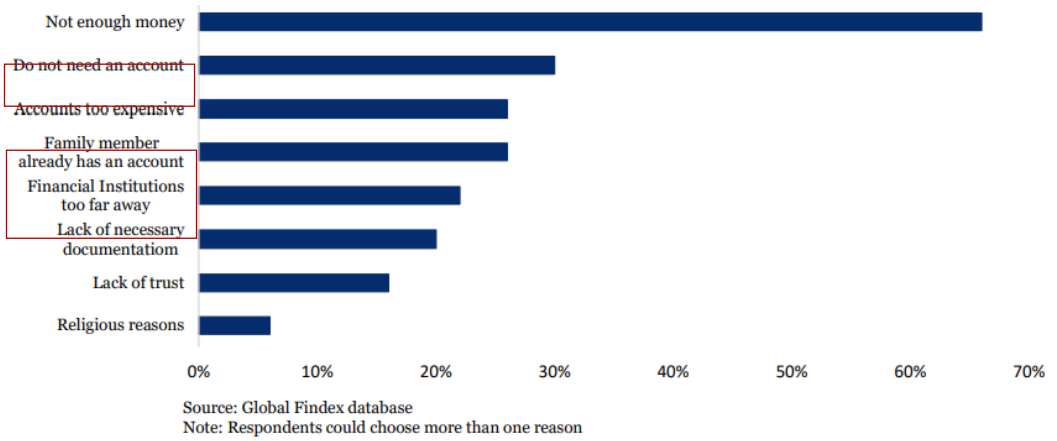


図 2- 57　金融包摂の阻害要因についての Global Findex 調査結果

デジタルアイデンティティが影響を与えることができる障壁として次のものが挙げられている。

・ 口座開設・維持管理費用が高すぎる

ほとんどの金融機関では、口座開設手数料と最低開設預金残高が必須条件となっているが、低所得者層にとっては負担が大きい。調査では、口座開設費用が高いことが口座所有の主な障壁となっていると回答した人は 26%に上った（この数字は中南米の一部の発展途上国では 60%に跳ね上がっている）。

・ 金融機関が遠い

伝統的な（ブリック＆モルタル）銀行モデルは運営コストが高いため、低所得者層への融資は困難である。また、多くの金融機関が農村部への支店網の拡大を避けているのも、コストの高さが理由の一つであり、これも包摂を妨げる大きな障害となっている

・ 口座開設に必要な書類を非保有

いくつかの国の規制当局は、金融機関が遵守することを義務づけられているKYC 手続きの一環として、オンボーディング文書の物理的なコピーを必要とする。通常、金融機関は、口座を開設するためには、住所を証明するものに加えて、法的な身分証明書（出生証明書、国籍証明書、パスポートなど）を持参することを求めている。必要書類の不足を挙げた回答者は 20%であった（Findex では 49%に達している）。

これらの課題に対する対策として、e-KYC などのデジタル認証の新技術が金融機関のリモート onboarding プロセスを加速させるために利用されている点を指摘している。これらの技術は、適切に導入されれば、新規の銀行顧客受け入れ時のオペレーション時間、コスト、および書類作成の要件を最小限に抑えることができ、大きな効果が期待できる点を指摘している。例として、いくつかのテクノロジー企業が電子的な e-KYC ソリューションを提供しており、銀行の新規顧客は携帯電話を介してオンボーディングを完了することができる点を挙げている。このような対応により、口座開設コストが削減され、書類作成の必要性がなくなり、銀行の支店や代理店ネットワークに容易にアクセスできない地方に住む潜在的に十分なサービスを受けていない人口層にとっては、長時間の来店時間を回避することが可能となる。

● 金融履歴データの欠如した顧客へのサービス提供

デジタルアイデンティティの金融包摂への活用について、金融履歴データの欠如した顧客へのサービス提供可能性についても述べられている。

低所得者層は通常、正式な収入証明がなく、クレジットヒストリーもなく、クレジットスコアもない「シン・ファイル・カスタマー」とみなされ、金融機関にとってはハイリスクな顧客となる。そこで、デジタルアイデンティティは、代替のデータソースを提供する上で重要な役割を果たすことが期待されている。本文献では、デジタルアイデンティティは、個人とその行動パターンを一意に識別するデジタル資格情報と属性のセットと定義され、この属性には、デジタル空間での行動に基づいて潜在的に銀行取引可能な顧客であるか判断するための代替データセットが存在する可能性が

ある。例えば、デジタル請求書支払いや携帯電話の料金支払い等、潜在的な顧客の支払いトランザクション履歴を分析することにより、金融機関は、顧客のデジタルフットプリントに基づいて代替データに基づくクレジットスコアを作成することが期待される。他に、デジタル税、補助金、電子商取引などが、歴史的に銀行口座を持たない消費者をプロファイリングするために使用できる代替デジタルデータセットの例として挙げられている。

- 経済への悪影響

  金融包摂をデジタル化により進めすぎることにより、債務不履行に陥るリスクが高まっているケースも本文献では指摘している。

  - テクノロジーを利用して取引処理の容易さを高めることは、管理が行き届いていない場合、特に金融リテラシーが低いことで知られる低所得者層にとって、金融の脆弱性を増大させる可能性がある点を指摘している。
  - テクノロジーやモバイル・プラットフォームを利用して、監督下にない形で簡単に金融にアクセスすることが悪影響を及ぼす可能性のある事例として以下が取り上げられている。
    - 中国のクレジットブーム：テクノロジーを介して担保されたクレジットが急増しており、無担保の消費者ローンは 2008 年以降、毎年平均 20%ずつ増加[284]
    - サハラ以南のデジタルクレジット：ケニアやタンザニアなどの国々で 2012 年以来、何百万人もの借り手にモバイルマネーを提供してきた M-Pesa のような取り組みが実施され、自動化された与信判断により、即日融資が可能となり、遠隔地からの支払いと返済が可能となったことで、モバイルマネーは多くの低所得者にとって効率的で便利なエコシステムとなった。結果、デジタル融資が急増し、借り手のうちタンザニアでは 56%、ケニアでは 47%がデジタルローンの返済が遅れたことがあり、タンザニアでは 31%、ケニアでは 12%が債務不履行に陥ったと報告されている[285]

- 現在の主要プレーヤーの持つ能力とデジタルアイデンティティ活用に求められる能力とのギャップ

---

[284] Luo, Han & Hu, *China's Generation Z Is Hooked on Credit,* Bloomberg, 31 July 2019, https://www.bloomberg.com/news/articles/2019-07-31/china-s-generation-z-is-hooked-on-credit

[285] Kaffenberger, Michelle, and Edoardo Totolo., A Digital Credit Revolution: Insights from Borrowers in Kenya and Tanzania, Working Paper, *CGAP*, 2018, Washington, D.C. https://www.cgap.org/sites/default/files/publications/Working-Paper-A-Digital-Credit-Revolution-Oct-2018.pdf

本論文では、金融のおける、デジタルアイデンティティ活用の主要なプレーヤーは、金融機関、テクノロジー企業、規制当局と指摘している。主要プレーヤーの間で共通の基準やポリシーがないことが、最近のデータ・プライバシーの問題や、安易で無責任なデジタル・ファイナンスによる消費者の債務不履行率の上昇といった状況を生んでいると指摘している。下図は、現在のエコシステムのプレーヤー各々が持つ能力をマップ化したものである。デジタルアイデンティティを活用した金融包摂を推進していくには以下の点が指摘されている。

生態系プレーヤーの属性	金融機関	テクノロジー企業	規制当局
信頼	✓	✗	✓
リスク管理	✓	✗	✓
代替データ	✗	✓	✓
規制された	✓	✗	−
人的資本	✗	✓	✗
消費者保護	✓	−	✓
金融リテラシー	✓	✗	✓
標準的な方針と規則	✗	✗	✗
技術インフラ	✗	✓	−

図 2- 58　各ステークホルダーの持つスペシャリティ

・ 金融機関は、代替データセットへのアクセスと分析を行う必要がある点が指摘されている。金融取引履歴が限られている低所得者層の代替クレジットスコアを作成する際に重要なデータとなるためである。

・ テクノロジー企業は現在、大規模な消費者セグメントに関する代替データセットを保有しており、俊敏なテクノロジー・インフラストラクチャを活用した経験豊富な人的資本（データサイエンティスト）を備えている。ただし、テクノロジー企業は金融に関するリテラシーが十分ではないため、規制され、信頼され、リスク管理経験が豊富な金融機関がデジタルアイデンティティの主要プレーヤーとなることは、重要であることが指摘されている。訓練を受けた銀行担当者が、金融知識のない銀行口座非保有層の顧客を教育し、金融の安定性を確保することの重要性は、デジタル・ファイナンスの世界においても変わらない点が指摘されている。

7. Digital Identities in Financial Services Part 3: The Business Opportunity for Digital Identity

発行者

IIF（Institute of International Finance）

本レポートの狙い

デジタルアイデンティティの発展と進化する市場が、金融サービスプロバイダにどのような新しいビジネスチャンスをもたらしているかを調査

主な論点

- カスタマーセントリシティに焦点を当てたデジタルトランスフォーメーション
  - 様々な業態の事業者が互いに接続して交流し、シームレスで便利な体験を通じて顧客に価値を生み出すことを可能にする「デジタル・プラットフォーム」が機会として考えられる。このエコシステムでは、消費者との関係を確立している信頼できる事業者が発行する複数のデジタル ID 属性（請求書や納税記録、財務諸表、通話データ記録など）によって ID を検証することができ、金融機関は、テクノロジー・プラットフォームの大規模な消費者基盤を活用しながら、ファイナンシャル・アドバイザーとしての役割を果たし、顧客へのサービス提供を最大限に支援することになると考えられる。
    例：個人の日々の支払いデータ等からファイナンスニーズを見つけ出し金融サービスを提供、データ分析し把握した類似する顧客の行動特性等を元に将来の顧客行動を予測し金融サービスを提案

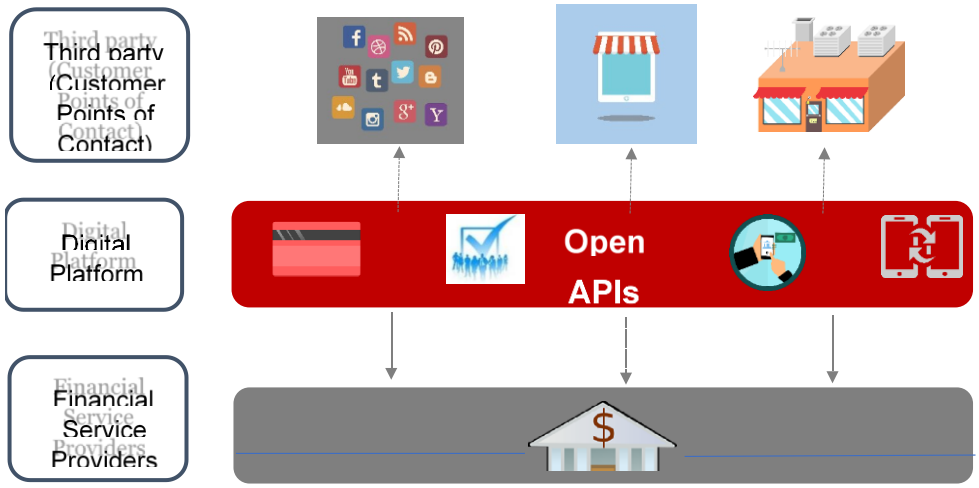


図 2- 59　他業態と連携した金融サービス提供イメージ

・ 業界を跨いだ様々な業種のデータを収集・分析することにより、よりパーソナライズされたサービスの提供も期待される。

● 金融機関の役割

・ 金融機関は、顧客データを確実に保護し、長年にわたって顧客との信頼関係を築いてきた確かな実績があり、機密性の高い金融データの性質上、業界ではセキュリティとプライバシーへの投資が相当なものとなっている。また、金融機関への信頼は、センシティブなデータ（リアルペイメント）を保護してきた長年の実績によっても強化されている。以上から、金融機関がデータ・スチュワードとしてデジタル・プラットフォームを監督することは理にかなっていると指摘

・ 金融機関のリスクおよび融資担当者は伝統的に門番としての役割を果たしており、信用記録、リスク選好度、規制上の許容度、経済見通しに基づいて金融機関の融資基準を調整している。また、コンプライアンス担当者は、違法な信用差別を引き起こすような行動やポリシーが意図しない結果を招くことに注意を払っている。これらのスキルにより、新しいエコシステムの中でも金融サービスプロバイダは重要な役割を果たすことになる点も指摘

● デジタル ID の利活用のための留意点

・ デジタル ID の利活用を促進するためには、データの共有を円滑に行う仕組みが必要であり、相互運用性の確保が重要である点を指摘。これは、データ利活用によるサービスの向上や規制対応強化（例：規制対応強化のための官民の情報のフィードバックループ構築）等のためにも重要である点を指摘

・ 金融機関社内の壁についても指摘。データ分析により自らの業務の欠点が明るみに出る懸念による社内の抵抗や、データ分析のためのインフラ整備の重要性を指摘

8. Guidance on Digital Identity （March 2020）

発行者

FATF（Financial Action Task Force）

1989 年に開催されたアルシュ・サミットでの経済宣言を受けて設立された、マネー・ローンダリング対策における国際協調を推進するための政府間組織

本レポートの狙い

各国当局、規制対象企業およびその他の関連するステークホルダーが、 FATF 勧告 10 に基づく顧客デューディリジェンス（顧客確認）を実施する際、 デジタル ID システムをどのように使用するかの意思決定を支援することを目的に発行

主な論点

- AML/CFT におけるデジタル ID システムの利点とリスク

（主な利点）

・ 信頼性のある独立したデジタル ID システムの構築により、オンボーディング時の顧客識別/検証や、継続的な顧客の口座へのアクセスの際に行う堅牢なデジタル認証による疑わしい取引検知の向上、等を通じたリスクベース・アプローチの実現。これにより、従来高リスクと判断されていた非対面取引も、標準的もしくは低レベルのリスクと評価される可能性

・ 特に発展途上国では、デジタル ID システムおよびデジタル金融サービスが金融包摂の中核的な推進要因として浮上しており、金融包摂への寄与が期待

・ 途上国では、政府から個人への支払い（G2P）がますますデジタル化され、救命のための支援がデジタル化された現金ベースで行われるケースが増加。これらの活動は取引口座へのアクセスが必要だが、デジタル ID システムを利用することで容易に

（主なリスク）

・ なりすまし、不正アクセス等のサイバーセキュリティ関連のリスク

・ 生体認証等の新しい技術が抱えるリスク（画像等を活用した偽装のリスク等）

・ デジタルアイデンティティが持つ生体認証を含むプライバシー情報の保護

・ デジタル技術へのアクセスの欠如や技術リテラシーの低さによる、金融排除のリスク

- リスクベース・アプローチの下、デジタル ID システムが十分な信頼性と独立性を備えているかどうかの評価

・ デジタル ID システムの使用が FATF 勧告 10 の（a）（信頼できる文書、データ等による顧客身元確認・照合）および（d）（継続的な顧客管理）の要件に合致しているかどうかを判断するために、政府、金融機関、およびその他の利害関係者は、以下の評価を行うべきと指摘。
・ デジタル ID システムが提供する保証レベルを、その技術、アーキテクチャ、およびガバナンスに基づいて理解し、その信頼性/独立性を判断する。
・ デジタル ID の保証レベルを考慮して、デジタル ID システムが適切な信頼性を持ち、潜在的な ML、TF、詐欺、その他の不正な資金調達のリスクに照らして独立しているかどうかを、リスクに基づいて判断する。
・ 規制対象企業が、顧客の識別と検証、および継続的なデューデリジェンスの目的でデジタル ID システムを使用するかどうかを決定する際の道筋を、次頁ローチャートにて提示

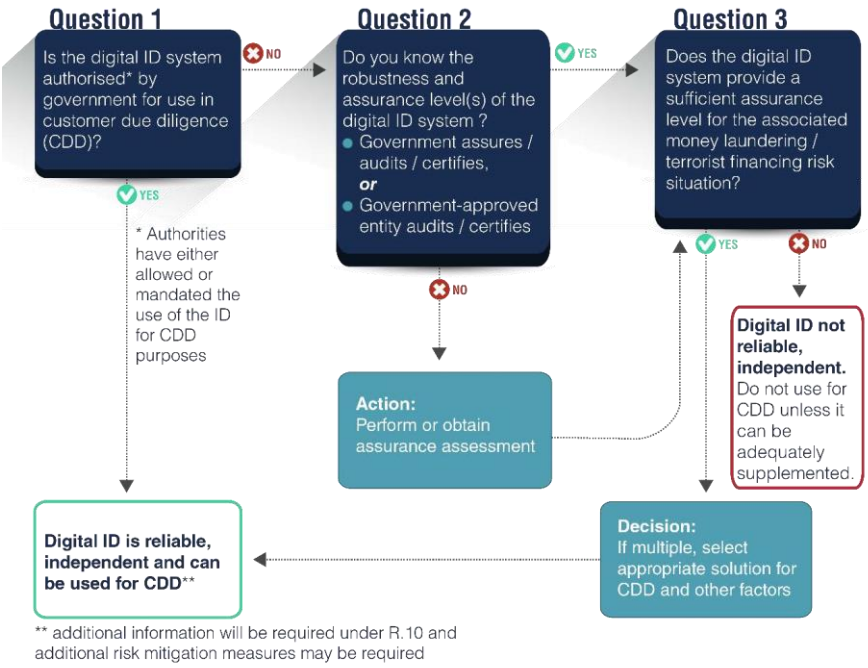


図 2- 60　AML/CFT 目的でのデジタル IMS の採否決定プロセス

9. Digital Identity and Financial Crimes（2019.9）

発行者

ACAMS（Association of Certified Anti-Money Laundering Specialists）

金融犯罪対策に従事するプロフェッショナル向けの世界最大の会員制組織。継続的な専門知識の学習、ACAMS コミュニティとの交流を通じて金融犯罪撲滅に取り組む個人と組織をサポート

本レポートの狙い

デジタルアイデンティティが金融サービスや金融犯罪にもたらす影響を考察

主な論点

- 本文献におけるデジタルアイデンティティの定義

本文献では、デジタルアイデンティティ（以下、デジタル ID）を“コンピュータシステムを通じて保存され、アクセス可能な個人に関するデータであり、市民および国民アイデンティティ（身分証明）と密接に関連しているもの”と定義している

- デジタル ID ネットワーク

世界中の多くの政府が、社会サービス提供の効率と精度の向上からデジタル運転免許証の発行まで、さまざまなシナリオに対応しようと、いくつかのデジタル ID ネットワークを立ち上げている。インドの Aadhaar ID やニュージーランドの RealMe などのプラットフォームの多くは、銀行口座の開設も可能である。Aadhaar ID、GOV.UK Verify、RealMe 等は、主に公共部門が資金を提供しているが、多くはデジタル ID 制度の実行に必要な技術を専門とする民間企業と提携している。

民間部門においても、デジタル ID ネットワーク構築の動きが技術の発展と共に見られ用としているところである。

- 金融サービスと金融犯罪への影響

・ 金融機関のメリット

金融機関がデジタル ID ネットワークに参加する主な利点は、従来の プロセスで実行する場合よりも低いコストでデジタル・チャネルを通じて正確に顧客を識別できる ことであると本文献では指摘されている。さらに、そう遠くない将来、デジタル ID ネットワークの主な利点は、金融機関がデジタル ID ネットワークにおける「トラスト・ブローカー」となることで識別プロセスを収益化する方向にシフトする可能性がある。これらの 2 つの利点の組み合わせにより、運用コストの削減と新たな利益の流れによる全体的な収益の増加がもたらされる一方で、顧客確認

（KYC）手続の合理化と監査可能性の増加により、金融犯罪対策強化の効果が高まる可能性があると指摘されている。

本文献では、KYC において下表のプロセスを想定しているが、紙ベースのドキュメントをベースにした現状業務は時間が非常にかかるものとなっている点を指摘している。デジタル ID の活用により、業務の効率化や、デジタル ID ネットワーク参加者間で信頼された情報をやり取りすることによるさらなる効率化が図られる点が指摘されている。

表 2- 34　KYC における主な業務プロセス

Action	Contextual Definition	Simplified Definition	Primary Responsibility	Traditional Method
Identity	Establish or link who or what （someone or something） is.	Link	Bank	Reliance on government-issued Identification documents or records.
Authenticate	Prove or show someone to be true or genuine.	Prove	Customer	Provide attributes to confirm one's identity such as PIN number, username, password, biometrics, etc.

・ 金融機関のリスク

デジタル ID 活用のリスクとして本文献は以下の点を指摘している。

1. データセキュリティ
2. ガバナンス
3. 認証の方法
4. トランザクション・モニタリング
5. 責任の所在

最初の２つのリスクは従前よりあるプライバシー保護に関連したリスクである。

後半の３つのリスク、すなわち、認証方法、取引の監視、責任は、金融犯罪のリスクに近いものである。デジタル ID ネットワークは、識別情報のセキュリティ、伝送、および追跡可能性を向上させることができるが、偽の ID または偽造 ID がシステムにアップロードされる可能性によるリスクは依然として存在する。本物の

情報と偽物の情報を組み合わせて新しい ID を作成する合成 ID や、偽の ID は、デジタル ID ネットワークの onboarding プロセスを狙った攻撃である。さらに、悪質な従業員が偽の ID をシステムにアップロードする可能性もある。このリスクの緩和策として、以下の対応が考えられる点、本文献では指摘している。

- 最低限の期間（例：6 ヶ月)、アカウントのデジタル ID ネットワークへのアクセスを制限する（口座開設早々に高額送金等をできないように）
- デジタル ID ネットワークへのアクセスを、最低限の資産または取引量の口座を持つ顧客に限定する
- デジタル ID ネットワークのみで入会した人には、信用限度を設けたり、高額商品へのアクセスを制限したりする
- 従来の金融犯罪プログラム（AML、詐欺など）による、デジタル ID ネットワークのみで開設された口座の取引監視の強化。

● 結論

金融機関におけるデジタル ID の活用は、前述の通りメリットがある一方で、活用の推進にあたってのリスクへの対応が求められる。今後の展望としては、異なるデジタル ID ネットワーク間の相互運用性の構築や、オープンソースのブロックチェーン技術などの可能な技術的変化の検討など、さらなるロードマップや戦略が必要であると考えられるが、デジタル ID ソリューションは、その可能性と重要性を無視することはできないため、追求する価値のある事業であると思われる。

10．Public Sector Savings and Revenue from Identification Systems:Opportunities and Constraints

発行者

World Bank Group ID4D

World Bank Group は、貧困削減と持続的成長の実現に向けて、途上国政府に対し融資、技術協力、政策助言を提供する国際開発金融機関である。

ID4D は World Bank Group に属し、グローバルな知識と専門性を分野横断的に提供し、各国がデジタル ID システムの変革の可能性を実現できるよう支援を実施している。

本レポートの狙い

政府が提供するデジタル ID システムが公共部門にコスト削減や収入を生み出す（あるいは制限する）可能性のある特徴、メカニズム、条件など、公共部門がデジタル ID システムへの投資を行う際の潜在的な財政的利益を分析するためのフレームワークを構築することを目的に発行

主な論点

政府がデジタル ID システムを構築することにより、公共部門にもたらすコスト削減と収益創出の機会について、デジタル ID システムが持つ 4 つの特徴を元に分析。

一方で、政府が提供するデジタル ID システムの構築の際に必要な事項（システムコスト、排除への対応等）についても併せて指摘。以下で詳述。

- 公共部門に最もインパクトを与えるデジタル ID システムの 4 つの特徴

Feature	Description	Key Benefits
Digitization	transition from paper to digital-based systems, including of databases, credentials, data transfer, etc.	• *Direct:* reduces operating and transaction costs • *Indirect*: enables unique ID, integration, digital authentication
Unique ID	creation of a unique identifier –often biometric-based–for each member of the target population	• *Direct:* eliminates duplicates; increases efficiency • *Indirect*: enables integration; boosts digital authentication
Integration and Interoperability	connections between different identification systems, including their ability to exchange information	• *Direct:* reduces operating and transaction costs; enables identity verification across databases, fee-charging
Digital Authentication	electronic process that uses one or more identity factors to prove that a person is who they claim to be	• *Direct:* decreases risk of impersonation; reduces transaction costs; enables fee-charging revenue models

図 2- 61　公共部門にインパクトを与えるデジタル ID システムの 4 つの主要な特徴

1. デジタル化

   ID ライフサイクル全体で紙ベースのシステムからデジタルシステムに移行することで、運営費や取引コストを削減

2. ユニークな ID

   母集団内の各個人に固有の識別子を作成することで、取引の効率を高め、不正の機会を削減

3. 統合および相互運用性

   ID システム間の統合、相互運用性、または依存関係を高めることにより、部門を跨いだ各種取引の効率を高める等の運用効率化を実現。また、公共部門で統一的な ID を作成・提供することが可能となり、民間へのより価値の高い ID 提供ビジネスの実現が可能に

4. デジタル認証

デジタル認証は、人が主張する人物であることを確実にする安全なプロセスを提供することで、 政府対個人（G2P）の支払いなどのさまざまな取引における ID 窃盗およびなりすましの事例を削減

- 上記の特徴が最大限に発揮されるための条件

  デジタル ID システムの信頼性と、全人口に占めるデジタル ID システムの利用者数の割合（カバレッジ）の重要性を指摘

  ・ ほとんどの場合、財政的利益が顕著になる前に、十分なカバー率が必要である。例えば、アジア開発銀行のある報告書では、カバー率が 50%以下の身分証明書システムは利用価値が低く、システムのカバー率が 80%以上になると官民のメリットが出始めるとしている（ADB 2016）。

  ・ カバー率と堅牢性の両方は、識別システム自体への投資によって大きく左右される。つまり、コスト削減や収入の機会を増やすためには、各国は識別システムにもより多くの費用をかけなければならない

- 上記の特徴に基づくコスト削減効果・収益効果を整理

	A. Decreasing Expenditures		B. Increasing Revenue	
Mechanism	**1. Reducing Fraud in G2P transfers**	**2. Reducing Administrative Costs**	**3. Increasing Tax Collection**	**4. Charging Fees**
Description	reducing ghosts, duplicates, ineligible beneficiaries, and impersonation	eliminating redundant systems and reducing transaction costs	identifying tax evaders and widening the tax base	to individuals for ID services and to third parties for verification/authentication
Location	• Payroll • Pensions • Safety nets • Targeted subsidies • Education • Health insurance, etc.	• Identity providers • Agencies or programs that require identity proofing, verification, authentication, or credentials	• Tax administration	• Identity provider

図 2- 62　デジタル ID システムによる公共部門のコスト削減と収益獲得のメカニズム

1. G2P トランスファーにおける不正行為の削減

   ・ 複数の受益者および幽霊受益者の排除

   十分な対象範囲と堅牢性があれば、固有の ID クレデンシャルまたはデータベースを G2P 受益者リストと統合することで、受益者のリストの重複を排除し、偽の受益者や死亡した受益者の排除が可能に

   ・ 無資格の受益者の識別

異なる ID システム間の相互運用性確保等により、異なるソース間での ID 属性の検証を容易にし、G2P プロバイダが無資格受給者を発見することが可能に

・タイでは、現金給付プログラムが国民 ID 番号を使用して、受益者の適格性を税金、職業、その他のデータベースと照合し、2970 万米ドルから 5940 万米ドルを節約

・ なりすましと漏洩の防止

堅牢なデジタル認証は、本人が主張する人物であることを確実にすることで、受益者のなりすましを減らし、不正を抑制。また、デジタル決済の仕組みと組み合わせることで、取引の電子的な証跡を残すことができ、漏洩を防止

2. 管理コストの削減

・ 取引コストの削減

ID の作成、検証、および認証には、個人と政府の間、および政府機関自体の間のさまざまな取引が伴います。紙ベースのシステムからデジタルシステムへの移行は、これらの取引の多くのコストを削減する可能性がある。さらに、これらの機能により、デジタル決済や電子政府サービスが可能となり、効率がさらに向上

・エストニアでは、電子身分証明書（eID）と X-Road データ交換レイヤーを含む身分証明書システムにより、身分証明書に関連する取引コストを削減し、オンラインサービスを促進することで、毎年 GDP の 2%を節約していると推定

・ 冗長なシステムの排除

十分な範囲および堅牢性を持つ デジタル ID システム間の相互運用性の確保または統合の実現により、重複したデータ収集の回避等を実現

3. 税収の増加

・ 固有の識別システムと税務管理を統合することにより、納税者の識別が改善され、課税ベースが拡大し、コンプライアンスが向上する可能性がある

4. 利用者料金の請求

・ 徴税の増加に加えて、ID システム、特に ID 検証および認証のためのデジタル・プラット フォームを備えた ID システムは、ID プロバイダが特定のサービスに手数料を請求できることに よって追加の収入源を生み出す可能性がある。

- しかし、手数料の徴収は ID プロバイダにとって重要な収入源であり、ある程度の財政上の自由性を提供するが、サービスへの過剰な課金は需要を減少させ、ID は普遍的な公共財であるべきだという原則を損なう可能性がある。

● 導入時の検討事項

・システムのコスト

- システム機能（デジタル化、固有 ID、システム間の統合と相互運用性、デジタル認証）を十分な堅牢性を持って導入し、人口の大部分に適用するためのコスト
- デジタル ID システムのメリットを最大化するために以下事項等を実現するコスト
  - ・デジタル ID を活用できるサービス（健康保険、税金など）のデジタル化
  - ・幅広く活用するための相互運用性のフレームワークや API インターフェースなどを作成
  - ・ICT バックエンドインフラ、全国のブロードバンド接続、POS デバイスなどへの投資を含む、デジタル認証インフラの展開
  - ・有料サービスモデルの導入のためのコスト（サービス用ウェブサイト準備、キャンペーン費等）

・その他には、デジタル化により排除される可能性のある社会的弱者等への配慮、例えば、ID 提供システムを有料化することは貧困層にとっては ID システムの利用の妨げになるため配慮が必要といった排除の抑止、複数データベースを統合して利用する際に業務に必要な最小限の情報にアクセスするといったプライバシーの配慮等が検討事項として挙げられている。

11. Private Sector Economic Impacts from Identification Systems

発行者

WorldBankGroup ID4D（No.10 と同様）

本レポートの狙い

政府が提供する、あるいは政府が認知した ID システムが民間セクターにもたらすコスト削減と収益創出の機会を検討するための分析フレームワークを提供すること目的に発行

主な論点

政府提供、あるいは政府が認知した ID システムについて、民間セクターにもたらすコスト削減と収益創出の機会について、デジタル ID システムが持つ 5 つの特徴を元に分析。一方で、政府提供、あるいは政府が認知した ID システムがもたらす経済的でメリットについても併せて指摘。以下で詳述。

- 民間部門にとって最もインパクトのある ID システムの 5 つの主要な特徴と主な利点

Feature	Description	Key Benefits
Digitization	transition from paper to digital-based systems, including of databases, credentials, data transfer, etc.	• *Direct:* reduces operating and transaction costs • *Indirect:* enables unique ID, integration, digital authentication
Unique ID	creation of a unique identifier –often biometric-based–for each member of the target population	• *Direct:* increases transaction efficiency; reduces fraud opportunities • *Indirect:* enables integration and queriability
Integration and Interoperability	connections between different identification systems, including their ability to exchange information	• *Direct:* increases transaction efficiency; facilitates queriability; reduces fraud opportunities • *Indirect:* incentivizes system adoption by incorporating a wider array of services into a given identity platform; encourages positive network effects
Queriability for Verification and Authentication	the ability of private sector companies to efficiently, securely, and consistently query and identification system for information	• *Direct:* increases transaction efficiency; facilitates effective private sector verification and authentication • *Indirect:* reduces private data liability costs; mitigates fraud opportunities; incentivizes value added services; encourages positive network effects
Public-Private Cooperation and Partnerships	the extent to which private sector companies are directly involved in the architecture and continued execution of identification systems	• *Direct:* enables private sector revenue generation for identity services

図 2- 63　民間部門にとってインパクトのある ID システムの 5 つの主要な特徴と主な利点

1. デジタル化
    - ID ライフサイクル全体で紙ベースのシステムからデジタルシステムに移行することで、 民間企業の運営費や取引コストを削減
2. ユニークな ID
    - 母集団内の各個人に固有の識別子を作成することで、取引の効率を高め、不正の機会を削減
3. 統合および相互運用性
    - ID システム間の統合、相互運用性、または依存関係を高めることにより、民間で行われる各種取引の効率を高め、民間企業からのデジタル ID に対する照会を容易にし、不正の機会を削減
4. 検証および認証のための照会性

・ 民間企業が効率的かつ安全に、一貫して ID システムに情報を照会できることで、取引の 効率が向上し、民間企業の効果的な検証および認証プロセスを促進

5. 官民パートナーシップ（PPP）

・ 国家レベルの ID システムの構築および継続的な実行に民間部門が直接参加することで、 取引効率が向上し、ID 関連サービスに対する民間部門の収益創出を実現

● 上記の特徴に基づくコスト削減効果・収益効果を整理

（1）コスト削減効果

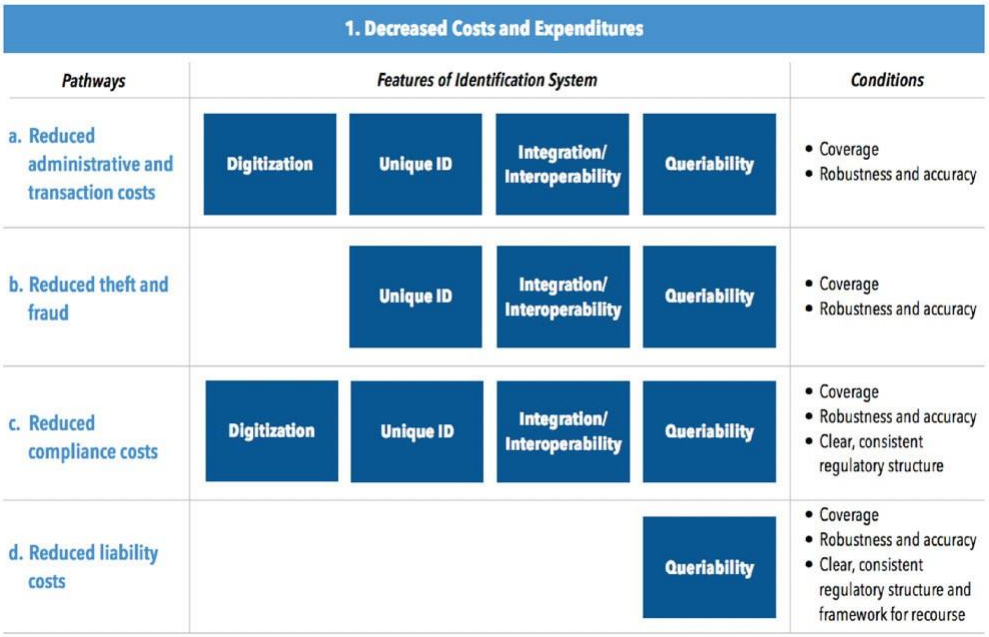


図 2- 64　デジタル ID システムの特徴がもたらすコスト削減効果

a. 管理・取引コストの削減

・ デジタル化により取引実行時のコストを削減

金融機関では、対面での取引にかかる平均コストは約 4.25 ドル、モバイル取引ではわずか 0.10 ドルにしかならないという試算あり。

インドでは、Aadhaar システムにより、第三者がユーザの本人確認等を遠隔かつ安全に検証可能に。Aadhaar システムの導入前、インドの平均的な企業のオンボーディングコストは約 1,500 ルピー（約 23 ドル）であったが、Aadhaar システムの照会性、デジタル化、相互運用性の向上により、オンボーディングコストはわずか 10 ルピー（約 0.15 ドル）にまで激減するという試算あり。

b. 盗難・不正行為の減少

- 効率的な照会メカニズムを備えた強力な本人確認システムにより、オンボーディングの際に消費者を正確に識別し、デジタル・プロセスを通じて検証されたアイデンティティと過去の金融行動とを関連付けることができれば、将来の詐欺被害を防ぐような分析が可能に。顧客のアイデンティティライフサイクルの中でも都度デジタルアイデンティティの検証を行うことにより、取引時点での不正を軽減。

c. コンプライアンスコストの削減

- マネー・ローンダリングなどの犯罪行為を抑止し、より広範な経済的安定性を促進しようとする政府からの要請に起因する事務コストの削減
  - [286]ヨーロッパでは、平均的な銀行の KYC コストは年間 6,000 万ドルで、個々の取引では、身元確認のために 10 ポンドから 100 ポンド（13.40 ドルから 134 ドル）のコストが発生

d. 個人情報を保有することによる責任コストの軽減

- 政府が支援する本人確認システムは、サイバー犯罪を阻止したり、個人データが危険にさらされないことを保証したりするものではないが、民間企業が保有する個人データを最小限に抑え、代わりに信頼できる政府システムへの問い合わせに頼ることができれば、企業のデータ漏洩のリスクと潜在的なコストを軽減することができる

（2）収益機会

[286] "Uncover the True Cost of Anti-Money Laundering & KYC Compliance. LexisNexis Risk, 2016. https://www.lexisnexis.com/risk/intl/en/resources/research/true-cost-of-aml-compliance-apac-survey-report.pdf

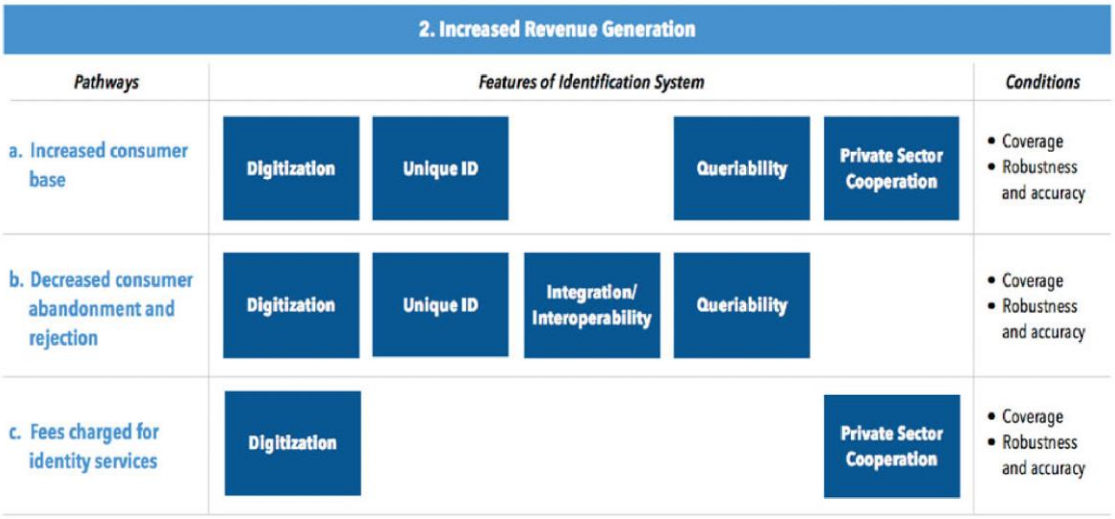


図 2- 65　収益増加の機会を可能にする識別システムの特徴

a. 顧客基盤の拡大

- 政府提供のデジタル ID システムの活用による、途上国においてより多くの国民を金融サービスに取り込むことが可能となる等、顧客基盤の拡大

b. 消費者の棄権と拒絶の減少

- onboarding プロセスの煩雑さ等に起因した顧客離脱の削減
  英国では、金融サービスの申し込みの 25%が、KYC プロセスの難しさなどの理由で放棄されていると推定。[287]電子商取引では、この数字は 3 倍に跳ね上がり、ほとんどの放棄はログインや支払いの確認プロセスで発生 [288]

c. アイデンティティに関連するサービスの料金

- 政府が支援する ID システムの提供に直接関与する企業が ID サービスの料金を請求する機会を獲得

● 負の経済的影響の可能性

---

[287] FStech “Know Your Compliance Costs” （June 2017）
https://www.fstech.co.uk/fst/mitek/Hyperion-Whitepaper-Final-for-Release-June2017.pdf

[288]"E-Commerce retailers are losing their customers because of this one critical mistake." *Business Insider,* 16 March 2016.
https://www.businessinsider.com/e-commerce-shoppers-abandon-carts-at-payment-stage-2016-3

・ 新しいデジタル ID システムの技術的導入に伴う統合コスト・維持コストが政府に発生

ジャマイカの 2017 年の国家 ID システム（NIDS）立ち上げプロジェクトでは、米州開発銀行から受け取った 6800 万ドルの資金のうち 500 万ドルが「官民の ID 認証の合理化」に充てられ、さらに 60 万ドルが「制度的能力と官民の連携」の改善に充当。[289]

・ 国家レベルの ID 政策の一貫性のない実施および施行は、民間部門に経済的非効率性を生み出す。

英国では、政府が変わった後の 2010 年に ID カード法案を放棄した。このプログラムには約 45 億ポンド（59 億ドル）が予定されていたが、カードのためにすでに 30 ポンド（39 ドル）を支払っていた 1 万 5,000 人の英国市民には返金されず

・ ID 関連のシステムおよび政策に大幅な変更が加えられると、サンクコストが失われ、企業は新たな短期または中期の統合およびコンプライアンスコスト、ならびに新たな非効率性に直面する可能性がある。国は、提案された ID 制度について官民の対話を促進し、新たな規制要件について民間との明確で一貫したコミュニケーションを優先することによって、これらの潜在的なコ ストを軽減し始めることができる。

[289] For a full profile on this status of Jamaica's NIDS project

Appendix2　各法域における金融法規制の状況

1. イギリス

イギリスにおける金融法規制は Proceeds of Crime Act（POCA）2002 を基本法として犯罪利益を幅広く定義し、POCA の改訂および他法規により補完する形式を取る。CFT に関しては POCA とは別に Terrorism Act（TA）2000 を規定し、テロおよびテロ資金供与に関して一元的に定義している。

また POCA および TA のいずれも細則化は行わず、Money Laundering Regulations やガイダンスにて身元確認等の関する細則を規定している。

【AML に関する法規制】

① POCA 2002[290]

全 12Part のうち Part7 にて AML を定義している。主として犯罪利益の定義に留め、身元確認等に関する具体的な規定までは言及していない。詳細な規定は後述の Money Laundering Regulations（MLR）に委ねている。

② POCA 2002 （Business in the Regulated Sector and Supervisory Authorities） Order 2003[291]

POCA2002 に対して監督対象の修正および監督官庁の追加を主としている。身元確認等に関する規定は追加していない。

③ POCA 2002 （Business in the Regulated Sector and Supervisory Authorities） Order 2007[292]

②同様、POCA2002 に対して監督対象の再修正および監督官庁の再追加を主としている。身元確認等に関する規定は追加していない。

④ Crime and Courts Act 2013[293]

従前の Serious Organised Crime Agency に代わり National Crime Agency を AML/CFT 調査機関として設立する旨を規定する。

---

290 legislation.gov.uk “Proceeds of Crime Act 2002” https://www.legislation.gov.uk/ukpga/2002/29/contents

291 legislation.gov.uk “The Proceeds of Crime Act 2002 （Business in the Regulated Sector and Supervisory Authorities） Order 2003” https://www.legislation.gov.uk/uksi/2003/3074/contents/made

292 legislation.gov.uk “The Proceeds of Crime Act 2002 （Business in the Regulated Sector and Supervisory Authorities） Order 2007” https://www.legislation.gov.uk/uksi/2007/3287/made

293 legislation.gov.uk “Crime and Courts Act 2013” http://www.legislation.gov.uk/ukpga/2013/22/contents/enacted

⑤ Serious Crime Act 2015[294]

POCA 2002 に対し没収財産に関する手続き等の修正を主としている。

【CFT に関する法規制】

① TA 2000[295]

従前の複数法規の法規にまたがっていたテロおよびテロ資金に関する規定に代わり、テロおよびテロ資金供与を一元的に定義している。TA の改訂および他法規により補完する形式を取る。

② Anti-terrorism, Crime and Security Act 2001[296]

2001 年 9 月 11 日のアメリカにおける同時多発テロを受けて成立。後に Section 23 が European Convention on Human Rights に準拠しないと判断され、Prevention of Terrorism Act 2005 に置き換えられた。

③ TA 2000 （Business in the Regulated Sector and Supervisory Authorities） Order 2003[297]

TA 2000 に対し監督対象セクターおよび非監督対象セクターを改訂。

④ TA 2006[298]

テロおよびテロ資金供与の定義を追加・修正。核の脅威の追記や厳罰化を合わせて実施。

⑤ TA 2000 （Business in the Regulated Sector and Supervisory Authorities） Order 2007[299]

③同様、TA 2000 に対して監督対象セクターおよび非監督対象セクターを再改訂。

---

294 legislation.gov.uk “Serious Crime Act 2015” https://www.legislation.gov.uk/ukpga/2015/9/contents/enacted

295 legislation.gov.uk “Terrorism Act 2000” https://www.legislation.gov.uk/ukpga/2000/11/contents

296 legislation.gov.uk “Anti-terrorism, Crime and Security Act 2001” https://www.legislation.gov.uk/ukpga/2001/24/contents

297 legislation.gov.uk “The Terrorism Act 2000 （Business in the Regulated Sector and Supervisory Authorities） Order 2003” https://www.legislation.gov.uk/uksi/2003/3076/contents/made

298 legislation.gov.uk “Terrorism Act 2006” https://www.legislation.gov.uk/ukpga/2006/11/contents

299 legislation.gov.uk “The Terrorism Act 2000 （Business in the Regulated Sector and Supervisory Authorities） Order 2007” https://www.legislation.gov.uk/uksi/2007/3288/made

【細則規定】

① MLR2017[300]

リスク別の身元確認方法 （顧客確認: 27~29, 33, EDD: 33~35, SDD: 37） および下記確認内容、取引時のタイミング （30） を規定。

（個人：28-（2））

- 顧客の身元確認が済んでいない場合は、顧客の身元確認を実施すること
- 既に身元確認が済んでいる場合は、当該顧客の身元を金融機関の担当者等が熟知している場合を除き、取引を行う者が顧客本人であるかの確認を実施すること
- 顧客の取引目的及び性質について、必要に応じて追加的に情報を入手し評価すること

（法人：28-（3）-（a））

- 法人登記名
- 法人番号もしくは他登記番号
- 登記住所、異なる場合は本社住所

（未上場法人：28-（4））

- 真の受益者の特定
- 関係者が真の受益者が誰であるかを認知していることを確認するため、真の受益者のアイデンティティを検証するために合理的手段を取ること
- 真の受益者が法人や信託会社、財団法人、類似する法的処置である場合は支配構造を検証するたえに合理的手段を取ること

② MLR2019[301]

MLR2017 に対して暗号資産交換業者等を対象に追加 （3-（1）-（b））、AMLD5 への準拠 （3-（1）-（c））、対象下限金額の変更 （13-（4）-（a）-（i）） を実施。

また身元確認においては必要な書類を例示し、個人においては運転免許証およびパスポートに言及。また電子的身元確認手段としてトラストサービス （Regulation （EU） No 910/2014） も例示。

③ Good Practice Guide 45

政府デジタルサービス局にて Good Practice Guide 45 を発行しているが、MLR と異なり適用は各業界団体および各金融機関の責任とされている。”How to prove and verify

---

[300] legislation.gov.uk “The Money Laundering, Terrorist Financing and Transfer of Funds （Information on the Payer） Regulations 2017” https://www.legislation.gov.uk/uksi/2017/692/contents/made

[301] legislation.gov.uk “The Money Laundering and Terrorist Financing （Amendment） Regulations 2019” https://www.legislation.gov.uk/uksi/2019/1511/contents/made

someone‘s identity”[302]および”Identity profiles”[303]にて Levels of Confidence として独自の 4 レベル（Low Confidence/Medium Confidence/High Confidence/Very High Confidence）を規定し、各レベルにおける確認点を満たした場合の加点手続きを規定している。

Very High Confidence を満たす本人各書類としては以下が例示されている。

- 国際民間航空機関（ICAO）の電子パスポート（e-Passport）の仕様に準拠した生体認証付きパスポート
- EU もしくは EEA 加盟国の ID カード（(EC) No2252/2004 に準拠、かつ生体情報を含む）
- 生体認証に基づく英国内居住許可証

④ The Joint Money Laundering Steering Group（JMLSG） Guidance[304]

JMLSG が HM Treasury 承認のもと、金融セクターに対して法規制の細分化を実施しているが、適用責任は各金融機関の判断に委ねられている。

顧客確認（Part1 Chapter5）にて、MLR2019 にて言及されている”electronic identification means”の具体例として eIDAS を挙げているが、IAL を含め一義的な規定はされていない。ただしデジタル ID 提供元が信頼に足る条件の 1 つとして eIDAS への準拠を挙げている。

2. ドイツ

ドイツにおける法規制は Money Laundering Act（GwG）を基本法とし GwG の解釈ノートよりデジタルアイデンティティ関連法規への紐づけがされている。主な細則としてはビデオ通話による身元確認手法を規定した Circular 3/2017 （GW） - video identification procedures、ID カードに関する細則を規定した German Act on Identity Cards and Electronic Identification が挙げられる。

またドイツ連邦銀行では eID のユースケースの検討も行われている。

---

[302] gov.uk “Guidance How to prove and verify someone's identity” （Updated 11 February 2021）
https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity

[303] gov.uk “Guidance Identity profiles” （Updated 11 February 2021）
https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/identity-profiles

[304] The Joint Money Laundering Steering Group（JMLSG） “Prevention of money laundering/ combating terrorist financing 2020 REVISED VERSION PART 1”
https://secureservercdn.net/160.153.138.163/a3a.8f7.myftpupload.com/wp-content/uploads/2020/07/JMLSG-Guidance_Part-I_-July-2020.pdf

① GwG[305]

② Interpretation and Application Guidance in relation to the German Money Laundering Act[306]

GwG および GwG の解釈ノートにおいて顧客管理手法を規定している。身元確認に関しては対面による身元確認として以下の細則を規定している。

- 対面時の身元確認における収集項目
  - 個人：氏名、出生地、生年月日、国籍、居住地
  - 法人：会社名/商号、法的形態、商業登記番号、登記住所、代表機関の構成員氏名
- 物理的な検証時に身元確認書類として認められる書類
  - ドイツ政府発行のパスポート、もしくは German Passport Act に準拠した写真付き書類
  - ドイツ政府が認める法域のパスポート
- GwG 解釈ノートにては同等なセキュリティを有する手法として以下を規定
  - 電子身分証明書 （German Act on Identity Cards and Electronic Identification）
  - 適格電子証明 （Regulation （EU） No 910/2014）
  - 電子識別スキーム （Regulation （EU） No 910/2014）
  - GwG にて規定する決済口座開設時の文書

③ Circular 3/2017 （GW） - video identification procedures[307]

目視による確認と口頭による対面コミュニケーションが取れる場合は身元確認が可能と解釈し、非対面による身元確認を追加規定している。映像による身元確認として主に以下の細則を規定している。

- 個人のみ対象
- 金融機関および外部委託先のオペレータが実施可能、またオペレータは精通しており年次研修の受講が必須
- オペレータをアクセスが限定された場所に配置

---

305 Bafin “GwG Money Laundering Act” https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/GwG_en.html

306 Bafin “Interpretation and Application Guidance in relation to the German Money Laundering Act” https://www.bafin.de/SharedDocs/Downloads/EN/Auslegungsentscheidung/dl_ae_auas_gw_2018_en.html

307 Bafin “Circular 3/2017 （GW） - video identification procedures” https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/2017/rs_1703_gw_videoident_en.html

- 身元確認書類の裏表や本人写真の撮影もしくはスクリーンショットの取得、およびそれらに対する明示的な同意
- 通信はリアルタイムかつ中断なしで十分な品質、またエンドツーエンドの暗号化が必要
- 身元確認書類は MRZ （機械可読領域を用いたチェックデジット確認） と光学的セキュリティが必要
- 身元確認書類の光学セキュリティの確認と形式的な特徴の確認が必要
- 身元確認書類のシリアル番号確認、損傷・偽造確認および水平もしくは垂直報告からの確認
- 身元確認書類に含まれる情報の妥当性および信頼性を確認
- 身元確認書類に含まれる個人情報の一致確認 （質問や観察）
- TAN （シーケンスナンバー） の送付と本人によるシステムへの TAN 入力

④ German Act on Identity Cards and Electronic Identification[308]

ID カードに含まれるデータおよび ID カードを本人特定情報として利用する場合に利用可能な内容（生体情報を含む）を規定している。具体的には Section5 にて以下の 12 項目を ID カードから取得可能な情報として規定している。ただし ID カード上には 1〜5 および 9〜12 のデータ、また指紋情報は ID カード保持者からリスクエストがあった場合のみ保管すると規定 （Section5 （5），（9））している。

1. 姓および旧姓
2. 名
3. 博士号
4. 生年月日および出生地
5. 写真
6. 署名
7. 身長
8. 目の色
9. 居住地（ドイツ外の場合は"no main residence in Germany"）
10. 国籍
11. 一意識別番号
12. 宗教名／芸名／筆名

また ID カード情報取得には以下の 2 段階を規定 （Section 18 （4））している。

- サービスプロバイダからの権限証明をカード保持者へ送信

[308] German Act on Identity Cards and Electronic Identification
https://www.gesetze-im-internet.de/englisch_pauswg/englisch_pauswg.html

・ カード保持者による PIN の入力

⑤ Use of electronic identification means （eIDs） in electronic payments and when opening a bank account[309]

ドイツ連邦銀行による口座開設への eID の適用可能性を法的面およびソリューション面から検討した文書。eIDAS への対応を明記し、eID の適用先として電子決済および口座開設をユースケースに検討しているが、ガイダンスの位置付けには至っていない。

3. シンガポール

Notice 626 およびそのガイドラインにて身元確認において必要な身元確認書類および確認手法を定義している。またガイドラインにおいては非対面における身元確認手法を細則化している。

一方、National Registration Act により国民認識番号として NRIC を設定している。さらに Smart Nation 政策として SingPass、MyInfo が National Digital Identity （PDPA に準拠した SG Verify） に統合、整備されつつある。

① Notice 626 Prevention of Money Laundering and Countering the Financing of Terrorism[310]

対面による身元確認における身元確認書類と収集する情報を以下のとおり規定している。

・ 対面による身元確認において収集する情報

個人：フルネーム （別名含む）、一意識別子 （ID カード番号、出生証明番号、パスポート番号）、住所、国籍

法人：会社名/商号、商業登記番号、登記住所、設立年月日

・ 対面による身元確認において必要な書類

写真付きの身元確認書類

② GUIDELINES TO MAS NOTICE 626 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM[311]

---

[309] Deutsche Bundesbank eID working group “Use of electronic identification means （eIDs） in electronic payments and when opening a bank account” https://www.bundesbank.de/resource/blob/826326/e8b63fa9701886ec99dee591bb7104f2/mL/bericht-eids-elekronischer-zahlungsverkehr-data.pdf

[310] MAS Notice 626 Prevention of Money Laundering and Countering the Financing of Terrorism https://www.mas.gov.sg/-/media/MAS/Notices/PDF/MAS-Notice-626--November-2015.pdf

[311] MAS “GUIDELINES TO MAS NOTICE 626 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM “

非対面による身元確認手法を以下のとおり細則化している。

- 非対面による身元確認手法
  - 銀行毎に非対面に伴う固有リスクを勘案した方針と手続きを定め、実施すること
  - 対面による顧客との接触がない場合は、対面と同等の顧客確認を実施すること
  - 個人のみ対象
- 非対面による身元確認手法は以下 1 つ以上を実施すべきと規定
  - 別途確認済みの居住先もしくは法人の電話番号による接触
  - 書簡もしくは適切な手法による顧客住所の確認
  - 顧客雇用先の人事部門への雇用状況確認 （本人同意が必要）
  - 他行から入手した取引明細による給与詳細の確認
  - 弁護士もしくは公証人による身元確認証明書
  - 他行の本人口座から引き出したチェックによる少額振込の依頼
  - 非対面ビジネスを行っている他行による信頼性のある身元確認

③ The National Registration Act of 1965[312]

16 歳以上の国民および永久許可証保持者に対して発行される National Registration Identification Card（NRIC）を規定している。（外国人向けには同様の FIN を別途規定）NIRC においては以下の情報を保持するが、他法域の国民識別カードと大きく異なる点はカードの表裏にこれら情報が記載されていることである。

また 2017 年からは ICA にて取引（パスポートの受取等）を行う際に虹彩データの収集が開始され、従前の指紋採取を補完することによる強化策を実施している。

- ID カード番号（バーコード含む）
- 写真（モノクロ）
- 英名
- （オプション）ピンイン、民族固有表記（中国語、ジャワ語、タミール語）
- 民族
- 生年月日
- 性別
- 出生国／地

---

https://www.mas.gov.sg/~/media/MAS/Regulations and Financial Stability/Regulations Guidance and Licensing/Commercial Banks/Regulations Guidance and Licensing/Guidelines/GUIDELINES TO MAS NOTICE 626 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM.pdf

[312] Singapore Status Online “The National Registration Act of 1965”
https://sso.agc.gov.sg/Act/NRA1965

- 右親指指紋
- 国籍
- 発行日
- 居住地

④ Singapore Personal Access（SingPass）

政府オンラインサービスを利用するための共通認証システムとして SingPass を導入し、2018 年からは SingPass Mobile を導入し民間サービスへも開放している。

SingPass は 2003 年に個人版、2016 年に法人版（Singapore Corporate Access）が導入されており、2003 年の SingPass 導入時は主に政府サービス毎に異なった ID の統合が主旨であった。NRIC と異なり取得は任意だが、2019 年 9 月現在で 380 万人が取得済みである。

また 2016 年までに Two-factor Authentication の導入によりセキュリティの強化、

2020 年 9 月には顔認証技術に iProov 社の顔生体認証技術を採用[313]し、スマートフォンを保有しない層を取り込み（政府機関のキオスク端末で認証可能）を図る。

2018 年には SingPass Mobile （SPM） を導入し、モバイルデバイスへの移行を促し、2020 年 3 月現在[314]、16 の民間企業が SPM と連携したログインポータルを構築済みである。

ただし金融機関からは AIA、Manulife、Prudential 等に留まり、銀行は NRIC と組み合わせた独自認証を実施している。

⑤ MyInfo

SingPass 同様に中央集中型で個人情報を記録する仕組みであり、2017 年には口座開設等の民間サービスへも開放している。

”Tell Us Once”サービスとして個人向けが 2016 年、法人向けの CorpPass が 2016 年、MyInfo Business が 2018 年にサービスを開始しているが、2016 年の導入時は行政サービス間で重複したデータの登録を防止することが主旨であり、SingPass の認証や本人同意を必要とする。

また 2017 年には民間サービスへ開放し、口座開設やクレジットカード申請への適用が開始され、法人の行政手続きはほぼ CorpPass による実施が可能である。

---

313 Businesswire “Singapore Government Extends National Digital Identity Programme With Face Verification Solution From iProov and Toppan Ecquaria” （September 22, 2020）
https://www.businesswire.com/news/home/20200921005898/en/Singapore-Government-Extends-National-Digital-Identity-Programme-With-Face-Verification-Solution-From-iProov-and-Toppan-Ecquaria

314 GOVTECH Singapore “SingPass Mobile hits one million users 31 MAR 2020”
https://www.tech.gov.sg/media/media-releases/singpass-mobile-hits-one-million-users

2020 年 11 月現在[315]では 110 の行政サービスに加えて 90 の民間サービスが採用、大手銀行等にも以下事例を含む採用が拡大している。

- M1 Remit 社のクロスボーダー送金
- DBS および OCBC におけるクレジットカード申請
- UOB における普通および当座預金口座、カーローンやクレジットカードのオンライン申請

⑥ Personal Data Protection Act （PDPA）

Smart Nation 政策により SingPass および MyInfo を統合した National Digital Identity を準備するも、2019 年の PDPA 施行により SG Verify への転換を図る。PDPA では民間企業による NRIC 収集・仕様・保管・開示が原則禁止されたため、身元確認手段向けに 2019 年 12 月に SG Verify を導入し NRIC の代替としての利用を開始している。口座開設やクレジットカード契約に利用可能である。

また 2019 年 8 月にはテクニカルガイドライン[316]を発表し、SG Verify を通してセキュアに個人情報を収集する仕組みを推奨している。PDPA 準拠のため企業側では部分的な NRIC 情報のみが取得可能である。

4. アメリカ

連邦法では Bank Secrecy Act （BSA）および USA PATRIOT Act を基本法とし、同法が定義する CIP にて身元確認書類や手法を規定している。

また連邦法はプリンシプルベースであり細則は州法に委ねられているが、州法においても基本的に細則化は実施していない。例えば最も AML/CFT の厳罰化が進む州の 1 つであるニューヨーク州では、DFS504 においてマネロン検知手法を規定しているが、身元確認は連邦法に定める CIP を踏襲するに留まる。

① BSA[317]

---

315 Smart Nation Singapore “National Digital Identity （NDI）” https://www.smartnation.gov.sg/what-is-smart-nation/initiatives/Strategic-National-Projects/national-digital-identity-ndi

316 Personal Data Protection Commission（PDPC） Singapore “TECHNICAL GUIDE TO ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR NRIC AND OTHER NATIONAL IDENTIFICATION NUMBERS” https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Technical-Guide-to-Advisory-Guidelines-on-NRIC-Numbers---260819.pdf?la=en

317 Office of the Comptroller of the Currency “Bank Secrecy Act （BSA）” https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html

AML/CFT 全般を規定し、細則は検査マニュアル[318]として FFIEC にて公開している。顧客確認の一部として金融機関における Customer Identification Program （CIP） の導入を規定するも、細則は USA PATRIOT Act に委ねる。

② USA PATRIOT Act[319]

CIP の細則を規定 （Section 326）する。ただし CIP 手法は金融機関の規模や業務次第とし、最低基準を規定するのみである。

③ CIP

対面による身元確認を前提に規定されており、非対面による身元確認は規定されていない。具体的には以下を規定する。

- 身元確認において最低限以下の情報収集
  - 個人：名前、生年月日、住所もしくは勤務先（ない場合は陸軍郵便局/海軍郵便局私書箱番号、最近親者もしくは代理人の住所もしくは勤務先)、納税者番号（アメリカ人）もしくは納税者番号/パスポート番号/外国人登録番号/政府発行の国籍もしくは居住が確認できる写真付き書類/同様の措置から 1 つ以上（非アメリカ人）
  - 法人：会社名、主たる事務所の所在地/現地事務所/その他物理的所在地
- 身元確認において必要な書類
  - 個人：政府発行の期限切れしていない国籍や居住が確認できる写真もしくは類似の措置のある書類（運転免許証やパスポート等）
  - 法人：存在証明書類（法人格付与証明書、政府発行の事業許可証、パートナーシップ契約書、信託証書等）
- 書類以外の身元確認手段
  - 消費者報告機関や公共データベース情報等との比較、他金融機関への照会、財務諸表の入手
- 上記手段で身元確認できない場合の例外措置
  - 署名者を含む口座管理者に関する情報との比較

また非対面を含む例外に対する措置の規定も金融機関に委ねられており、細則は規定されていない。非対面による身元確認は、身元確認書類以外による確認手段の例外の 1 つとして定義 （(a) - (2) - (ii) - (B) - (2)）されている。

- 詳細の規定はなく、金融機関による例外時の対処方法規定を要請

---

318 FFIEC Bank Secrecy Act/Anti-Money Laundering InfoBase
https://bsaaml.ffiec.gov/

319 USA PATRIOT ACT
https://www.govinfo.gov/content/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

・ 同列の例外：政府発行の写真付き書類を提示できない場合、提示された書類に精通していない場合、身元確認書類なしに口座開設した場合、書類による身元確認ができないリスクが高い環境で提示された場合

④ Part 504 of the Banking Superintendent's Regulations[320]

ニューヨーク州では Department of Financial Services（DFS）504 において DFS 監督下の金融機関に対して年次の順守証明を要請している。準拠法は BSA 等の連邦法であり、DFS への証明書提出手続きを主に規定し、AML/CFT に関する細則化は行っていない。

⑤ Final Rule on Transaction Monitoring and Filtering Programs[321]

DFS 監督下の金融機関に対して取引モニタリングおよびフィルタリングプログラムに特化して規定しており、身元確認に係る規定は対象外である。

⑥ Joint Statement Encouraging Innovative Industry Approaches to AML Compliance[322]

Financial Crimes Enforcement Network と Federal Banking Agency との共同声明。連邦政府として銀行および信用組合における革新的アプローチへの官民協働を促し、アプローチ実行時の 31 CFR 1010.970（例外、免除条項）の適用も示唆する。

5. ニュージーランド

【認証規格】

身元確認の標準規格として EOI（Evidence of Identity）が使用される。EOI（Evidence of Identity）規格はニュージーランド電子政府相互運用性フレームワーク（NZ e-Government Interoperability Framework）の一部であり、主にニュージーランドの政府機関が使用することを想定し、政府サービスを求める個人の身元を確立し、確認するためのプロセス要件を規定している。

各種認証目的に適用される規格・文書は以下のものが定められている。

表 2- 35　ニュージーランドで各種認証目的に適用される規格・文書

標準/文書名	目的

[320] New York State Department of Financial Services "Part 504 of the Banking Superintendent's Regulations"
https://www.dfs.ny.gov/industry_guidance/transaction_monitoring

[321] New York State Department of Financial Services "DFS ISSUES FINAL ANTI-TERRORISM TRANSACTION MONITORING AND FILTERING PROGRAM REGULATION The risk-based banking rule takes effect January 1, 2017."
https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1606301

[322] "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing"
https://www.fincen.gov/sites/default/files/2018-12/Joint Statement on Innovation Statement （Final 11-30-18）_508.pdf

オンラインサービスの認証基準ガイド	NZ の e-GIF 認証規格の概要を提供する。
身元の証明基準	政府機関の顧客のアイデンティティを確立するためのビジネスプロセスを指定する。オフラインとオンラインの両方のチャネルで提供されるサービスに適用される。
認証キーの強度規格	オンライン認証に使用する認証鍵と、認証交換に必要な保護を指定する。
身元確認記録のためのデータ形式の標準	政府機関が顧客 ID レコードで使用することができる一連の顧客情報データ要素のデータ形式を指定する。
パスワード標準	オンライン認証に使用するパスワードの要件を指定する。
その他の認証鍵規格	オンライン認証に使用する二要素認証鍵の要件を指定する。
NZ セキュリティアサーションメッセージング標準	認証アサーションを通信するためのメッセージング標準を指定する。
NZ セキュアウェブサービスのフレームワークと基準	セキュアな Web サービスと ID 関連のセキュアな Web サービスのためのメッセージング標準と参照パターンを指定する。
多要素認証のガイダンス	多要素認証の概要を提供する。他の認証鍵規格が開発された場合は、これに取って代わられる可能性がある。(NZ の e-GIF 規格外)
セキュリティアサーションメッセージングフレームワーク	セキュリティアサーションメッセージングの一般的な紹介。(NZ の e-GIF 規格外)

【個人の身元確認のプロセス】

各政府機関は個人にサービス提供する前に、EOI プロセスに基づき、下記4つのフェーズに沿ってサービス内容に必要な身元確認要件を確立する必要がある。

表 2- 36　ニュージーランドでの個人の身元確認プロセス

フェーズ	説明
リスクアセスメント	このフェーズでは、機関が提供するサービス内の ID 関連リスクのレベルを決定する。ID 関連のリスク評価の結果は、特定のサービスに EOI プロセスが必要な場合にはどのようなものがあるかを判断するのに役立つ。

設計・運用	このフェーズでは、リスク評価段階で特定されたサービスの ID 関連リスクのレベルに適切な EOI プロセスを設計することが含まれる。運用上適切な EOI プロセスが確実に実施されるようにガイダンスが必要な事項を提供する。
サービス提供	このフェーズでは、身元確認後に代理店がサービスを提供することになるため、本規格の対象外となる。
モニタリングと評価	このフェーズでは、各機関の EOI ビジネスプロセスと関連する成果が、リスクアセスメントフェーズの結果として確立された EOI プロセスの目標と一致していることを確認するために、EOI プロセスの継続的なモニタリングと定期的な評価を行う。

また、ID 関連リスクレベルを評価する際は下記のカテゴリ別に影響レベル、発生の可能性、リスクを Unlikely、Possible、Likely のレベル別に評価し、サービスの全体的なリスクレベルの評価が求められる。

表 2- 37　ニュージーランドでの ID 関連リスクレベル評価項目

結果カテゴリ	影響レベル	可能性	リスク
迷惑、苦痛、地位や名誉の毀損			
財務上の損失または負債			
機関のプログラムや公共の利益への弊害			
機密情報の無断公開			
個人の安全性			
機関の外部への流出			
全体のレベル			

【有効な文書・記録】

EOI 規格では身元確認の目的を A から E の 5 つと定義しており、また、各目的を満たすために使用できる文書・記録、またはその組み合わせも提示している。単独で認証が可能となる文書・記録、認証の補助的な文書・記録、また発行機関による確認や面接による属性確認、公的機関の利用履歴などの認証方法も提示されている。

A）アイデンティティが存在する

B）アイデンティティが生きている

C）提示者がアイデンティティとリンクしている

D）プレゼンターはアイデンティティの唯一の主張者である

E）コミュニティでのアイデンティティの使用

【独自の取組み】

各機関の ID 確認プロセスの効率性・正確性向上のため、政府は権威ある ID データソースを提供している。その代表例が身元確認サービス（IVS）とデータ検証サービス（DVS）である。

IVS は、パスポートにより確認可能な人物情報をオンラインで近似情報を提供することで、身元関連のリスクを伴うサービスへのアクセスの改善を図っている。EOI 規格で定める身元確認の目的のうち、申請者が ID の唯一の利用者であることを確認すること（目的 D）を除き、すべての目的を満たしている。IVS は特にオンライン・チャネルを使用したリアルタイムで高い信頼性で身元を確認する場面で推奨される。

DVS は、内務省が発行した文書（出生証明書、パスポート、市民権証明書など）の情報を、内務省のシステム内のソースデータと照合して検証できるようにする、安全な Web ブラウザベースのサービスである。顧客の身元やサービスを受ける資格を証明するプロセスの一部として、文書の提示を要求する政府機関をサポートするために設計されたもの（例：EOI 規格の目的 A を満たす；目的 B と C をサポートするため）。また、DVS は出生証明書の氏名変更の検証を通じて、提示者が身元の唯一の請求者であること（EOI 規格の目的 D）を立証するためにも使われる。

6. 日本

犯罪収益移転防止法により対面および非対面の身元確認の細則を規定する。マネー・ローンダリング及びテロ資金供与対策に関するガイドライン（AML/CFT ガイドライン）において顧客管理に係るミニマムスタンダード（対応が求められる事項／対応が期待される事項）を規定するも、身元確認に係る細則は規定していない。

① 犯罪収益移転防止法[323]

対面による身元確認時に必要な身元確認書類を規定する。

- 対面による身元確認手段として以下の写真付き書類を規定

運転免許証/運転経歴証明書
パスポート/乗員手帳
マイナンバーカード
在留カード・特別永住者証明書
各種福祉手帳
官公庁発行・発給の氏名・居住地・生年月日・写真付き書類

[323] e-gov 犯罪による収益の移転防止に関する法律
https://elaws.e-gov.go.jp/document?lawid=419AC0000000022

・ 対面における身元確認時の上記書類代替として以下写真無し書類から 2 点を規定

各種被保険者証/公務員共済組合の被保険者証/私立学校教職員共済制度の加入者証/国民年金手帳
児童扶養手当証書・特別児童扶養手当証書
母子手帳
印鑑登録証明書
住民票（写し）
戸籍謄本・抄本　等

また平成 30 年 11 月の改正によりオンライン身元確認を追加規定、さらに令和 2 年 4 月の改正により郵送による身元確認は本人限定受取時の写真付き書類の提示規定により規定を補強した。一方、対面による身元確認は写真無し書類 2 点による代替が継続して認められている。

・ 非対面による身元確認手段として郵送もしくは特定事業者が提供するソフトウェアの使用を規定

郵送による身元確認

- 身元確認書類の原本、法人：転送不要郵便の送付（第 6 条第 1 項第 1 号チ、リ）
- 身元確認書類の写し 2 種類（第 6 条第 1 項第 1 号リ）
- 身元確認書類の写しと補完書類の原本又は写し（第 6 条第 1 項第 1 号リ）

金融機関が提供するシステムを経由して以下のいずれかを送信

- リアルタイムビデオ通話等により身元確認書類と本人容貌画像の提示を受け、氏名・住居・生年月日・写真・厚みを確認（第 6 条第 1 項第 1 号ホ）
- 写真付き身元確認書類の IC 情報と本人容貌画像（第 6 条第 1 項第 1 号ヘ）
- 銀行等の顧客情報照会、もしくは他行振込を利用した他行の身元確認情報利用（第 6 条第 1 項第 1 号ト）

② 銀行法[324]

[324] e-gov　銀行法
https://elaws.e-gov.go.jp/document?lawid=356AC0000000059

銀行業務全般に関する規定のうち、第二十四条にて実質的に定期的な当局報告を規定し、AML/CFT に関する順守状況の報告を要請する。ただし口座開設や身元確認に関する細則は規定していない。

③ AML/CFT ガイドライン[325]

実質的に各業法を裏付けとして、金融機関等に対する AML/CFT に係るガイドラインを定義。顧客管理に関する規定にて身元確認に言及があるものの、細則規定はない。

④ 疑わしい取引の参考事例[326]

AML/CFT ガイドラインの解釈ノートに相当する。口座開設に関する言及はあるものの、取引時の検知観点が主旨であり、身元確認に関する記載はない。

---

[325] 金融庁　マネー・ローンダリング及びテロ資金供与対策に関するガイドライン
https://www.fsa.go.jp/common/law/amlcft/amlcft_guidelines.pdf

[326] 金融庁　疑わしい取引の参考事例
https://www.fsa.go.jp/str/jirei/