

金融庁 御中

# 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

---

株式会社野村総合研究所  
NRIセキュアテクノロジーズ株式会社

2021年3月31日



# 調査の背景と目的

## ■ 調査の背景

- 近年、技術革新に伴い金融サービスのデジタル化が急速に進展しており、多様な金融サービスが様々なデバイスやプラットフォームを通じて提供されるようになってきている。こうした動きに対応すべく、金融庁においては、「金融デジタルイゼーション戦略」を策定し、データ利活用や顧客のプライバシー保護といった課題に取り組んでいるところである。
- こうした中、金融サービスをデジタル化する上で不可欠な構成要素の一つがデジタルアイデンティティであると指摘されている。サービスの提供形態によらず、金融サービス提供者は利用者保護、マネーロンダリング・テロ資金供与防止等の観点からアイデンティティの適切な取り扱いが求められるが、金融サービス提供者が顧客を適切かつ効率的に識別した上で、利用者の属性やニーズに応じたきめ細やかなサービスを提供するためには、適切なフレームワークに基づくデジタルアイデンティティ・システムを構築することが期待されている。
- 足下、デジタルアイデンティティの技術開発や標準化に向けた様々な取組がみられており、そうした動向を適時適切に把握することは重要となる。さらに、近年、その発行と利用が中央的に管理されたデジタルアイデンティティに関するプライバシーの懸念、個人情報保護規制への対応、ロックイン回避及び金融包摂実現の必要性等を踏まえ、ユーザ自らがアイデンティティを管理する自己主権型／分散型アイデンティティ（SSI/DID）の議論も活発になっている。SSI/DIDの構築にあたっては、ブロックチェーン技術等を用いた分散型アーキテクチャが望ましいとの指摘もあるところ、こうした新たな動向にもフォワードルッキングに対応する必要がある。
- デジタルアイデンティティ領域については、ブロックチェーンを含め認証技術、アクセス制御技術、暗号化技術など多様な技術コンポーネントや、その運用体制及びガバナンスなど、幅広い論点について理解を深めるとともに、関与する様々なステークホルダーとの対話が必要となる。

## ■ 調査の目的

- そこで、本調査研究においては、国際共同研究の一環として、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に関する研究を行うこととする。金融規制当局として、今後の金融デジタル化を見据え、デジタルアイデンティティ・システムの現状把握及び、望ましいデジタルアイデンティティ・システムの在り方やその運用についての方向性を検討するために実施するものである。

# 目次

## 第1章 アイデンティティに関わる技術や運用についての基礎

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)

1-2. 主要なIMSモデルと構成要素

1-3. 自己主権型アイデンティティモデル

## 第2章 デジタルアイデンティティに係る金融規制当局や関連団体及び学術的な既存の研究・検討状況および金融サービスにおける活用可能性

2-1. 金融機関のアイデンティティ管理の現状と課題

2-2. onboardingプロセスの非対面化の進展

2-3. デジタルIMSの活用可能性

2-4. 課題解決（先進的事例からのインプリケーション）

2-5. 課題解決の方向性の整理

## 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)

3-1. SSI/DIDの概要

3-2. SSI/DIDの実現に必要な構成要素

3-3. SSI/DIDの先行事例/PoC事例

3-4. SSI/DIDの長所と実現に向けた課題

3-5. SSI/DID活用時の金融規制上の論点

## 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

4-1. 本章の構成

4-2. 各課題のステークホルダーとその関心事項

## 謝辞・免責事項

### ■謝辞

- 本報告書作成にあたっては、米国OpenID Foundation・崎村夏彦理事長、早稲田大学・佐古和恵教授、慶応義塾大学・鈴木茂哉特任教授、米ジョージタウン大学・松尾真一郎研究教授から有益な助言やコメントを得た。
  - ・ また、金融庁のご担当者からも有益な示唆・助言をいただいた。
- もともと、本報告書に関する内容の誤りは、すべて受託者である株式会社野村総合研究所並びにNRIセキュアテクノロジーズ株式会社に帰する。

### ■免責事項

- 本報告書の内容は金融庁の公式見解を示すものではない。
- 本報告書で記載している過去または現在の事実以外の内容については、本稿執筆時点で入手可能な情報に基づいた見通しであり、実際の動向等は種々の不確定要因によって変動する可能性がある。

## 用語集

■ 下記用語は主にISO/IEC 24760シリーズ\*1)に則る。

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
アトリビュート(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
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
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、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
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。
バリデーション (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づき、イシュー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

\*1) ISO/IEC 2460は以下の3部から構成される。

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

ISO/IEC 24760-2:2015 A framework for identity management — Part 2: Reference architecture and requirements

ISO/IEC 24760-3:2016 A framework for identity management — Part 3: Practice

## 用語集

- 下記用語は「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」および関連法規制に則る。また一部海外事例にて使用した用語は海外規定を参照する。

用語	定義
疑わしい取引の届出 <sup>*1)</sup>	<ul style="list-style-type: none"><li>・ 犯収法<sup>*2)</sup>の特定事業者に該当する金融機関等が、特定業務に係る取引について、当該取引において收受した財産が犯罪による収益である疑いがあるかどうか、又は顧客等が当該取引に関し組織的犯罪処罰法<sup>*3)</sup>第10条の罪若しくは麻薬特例法<sup>*4)</sup>第6条の罪に当たる行為を行っている疑いがあるかどうかを判断し、これらの疑いがあると認められる場合においては、速やかに、政令で定めるところにより、政令で定める事項を届け出る義務（犯収法第8条第1項、同法施行令<sup>*5)</sup>第16条）。</li></ul> <p>(参考：FATF勧告20<sup>*6)</sup>)</p> <ul style="list-style-type: none"><li>・ 金融機関が、資金が犯罪活動の収益ではないか、又はテロ資金供与と関係しているのではないかと疑うか又は疑うような合理的な根拠を有する場合には、法律または規制に基づいて、その疑いを金融情報機関(FIU)に速やかに届け出ること。</li></ul>
金融包摂 <sup>*7)</sup>	<ul style="list-style-type: none"><li>・ 個人や企業が、信頼があり持続可能な方法により、取引、支払、貯蓄、与信、保険といった要望を満たしかつ有益な金融商品やサービスを手頃な価格で利用可能なこと。</li></ul>

\*1) マネロン・テロ資金供与対策ガイドラインに関するよくあるご質問 (FAQ) [https://www.fsa.go.jp/news/r2/2021\\_amlcft\\_faq/2021\\_amlcft\\_guidelines\\_FAQ.pdf](https://www.fsa.go.jp/news/r2/2021_amlcft_faq/2021_amlcft_guidelines_FAQ.pdf)

\*2) 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>

\*3) 組織的な犯罪の処罰及び犯罪収益の規制等に関する法律 <https://elaws.e-gov.go.jp/document?lawid=411AC0000000136>

\*4) 国際的な協力の下に規制薬物に係る不正行為を助長する行為等の防止を図るための麻薬及び向精神薬取締法等の特例等に関する法律 <https://elaws.e-gov.go.jp/document?lawid=403AC0000000094>

\*5) 犯罪による収益の移転防止に関する法律施行令 <https://elaws.e-gov.go.jp/document?lawid=420CO0000000020>

\*6) The FATF Recommendations <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>

\*7) The World Bank Financial Inclusion <https://www.worldbank.org/en/topic/financialinclusion>

## 用語集

用語	定義
口座開設 (取引時確認) <sup>*1)</sup> onboarding due diligence	金融機関等が顧客と取引を行うに当たって、当該顧客がどのような人物・団体で、団体の実質的支配者は誰か、どのような取引目的を有しているか、資金の流れはどうなっているかなど、顧客に係る基本的な情報を適切に調査し、講ずべき低減措置を判断・実施すること。
継続的顧客管理 <sup>*2)</sup> ongoing due diligence	継続的に顧客情報更新や当該顧客が実施する取引内容等を検証し、顧客リスクを再評価するとともにリスク低減措置を判断・実施する一連の流れ。
実質的支配者 <sup>*3)</sup>	法人である場合において、その事業経営を実質的に支配することが可能となる関係にあるもの。
顧客フィルタリング <sup>*2)</sup>	取引前やリストが更新された場合等に、取引関係者や既存顧客等について反社会的勢力や制裁対象者等のリストとの照合を行うことなどを通じて、反社会的勢力等による取引を未然に防止することで、リスクを低減させる手法。いわゆるネームスクリーニングという業務も含む。
取引モニタリング <sup>*2)</sup>	過去の取引パターン等と比較して異常取引の検知、調査、判断等を通じて疑わしい取引の届出を行いつつ、当該顧客のリスク評価に反映させることを通じてリスクを低減させる手法。
リスクベース・アプローチ <sup>*1)</sup>	金融機関等が、自らのマネロン・テロ資金供与リスクを特定・評価し、これをリスク許容度の範囲内に実効的に低減するため、当該リスクに見合った対策を講ずること。

\*1) 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/2021\\_amlcft\\_guidelines.pdf](https://www.fsa.go.jp/common/law/amlcft/2021_amlcft_guidelines.pdf)

\*2) \*1)およびマネロン・テロ資金供与対策ガイドラインに関するよくあるご質問 (FAQ) を参考に定義

\*3) 犯罪による収益の移転防止に関する法律施行規則 <https://elaws.e-gov.jp/document?lawid=420M60000f5a001>

## 用語集

用語	定義
AAL <sup>*1)</sup>	• Authentication Assurance Level : 認証プロセス自体、および認証コードと特定個人の識別子の紐付けの頑強性
AML/CFT <sup>*2)</sup>	• Anti-Money Laundering and Combating the Financing of Terrorism : マネー・ローンダリング及びテロ資金供与対策
eKYC <sup>*3)</sup>	• electric Know Your Customer : オンラインで完結する自然人の本人特定事項の確認方法
IAL <sup>*1)</sup>	• Identity Assurance Level : 個人のアイデンティティを確信を持って決定するためのアイデンティティ証明プロセスの頑強性
FATF <sup>*2)</sup>	• Financial Action Task Force : 金融活動作業部会
KYC <sup>*4)</sup>	• Know Your Customer : 顧客確認のプログラム
LEI <sup>*5)</sup>	• Legal Entity Identifier : 取引主体識別子
LoA <sup>*6)</sup>	• Level of Assurance : 受領した個人のアイデンティティに対する信頼度
NPI <sup>*5)</sup>	• Natural Persons Identifier : 自然人識別子

\*1) NIST Special Publication 800-63-3 Digital Identity Guidelines

(日) <https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3-ja.html> (英) <https://pages.nist.gov/800-63-3/sp800-63-3.html>

\*2) 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

(日) [https://www.fsa.go.jp/common/law/amlcft/2021\\_amlcft\\_guidelines.pdf](https://www.fsa.go.jp/common/law/amlcft/2021_amlcft_guidelines.pdf) (英) [https://www.fsa.go.jp/common/law/amlcft/en\\_amlcft\\_guidelines.pdf](https://www.fsa.go.jp/common/law/amlcft/en_amlcft_guidelines.pdf)

\*3) 「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令」の公表について <https://www.fsa.go.jp/news/30/sonota/20181130/20181130.html>

\*4) 銀行の顧客確認に関するガイダンス <https://www.fsa.go.jp/inter/bis/f-20011004-2.html>

\*5) 日本銀行決済機構局ISOパネル (第1回) [https://www.boj.or.jp/paym/iso/iso\\_panel/data/isop201127.pdf](https://www.boj.or.jp/paym/iso/iso_panel/data/isop201127.pdf)

\*6) eID Documentation <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Levels+of+assurance>



# 第1章 アイデンティティに関わる技術や運用についての基礎

---

# 1. 本章の概要

---

# 本章の概要

### 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)

- アイデンティティとは「ある実体に関連する属性の集合の表現」であり、常に変化・成長するアイデンティティの状態を管理するための仕組みとして、アイデンティティマネジメントシステム（IMS）が必要となる。IMSとは、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のことである。
- デジタルアイデンティティとは「ある実体に関連する属性の集合の電子的な表現」である。従来のIMS間のアイデンティティ情報のやり取りについては、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依然として多かったが、デジタルアイデンティティの活用により、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）を目指す動きも出てきている（＝IMSのデジタル化）。

### 1-2. 主要なIMSモデルと構成要素

- 現在の主要なIMSモデルは、Centralizedモデルや、フェデレーションモデルであるが、これらモデルを支える技術要素として、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関するプロトコルの技術標準が策定されている。
- また、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。例えば、欧州ではeIDAS規則として法制化されていたり、米国や英国、カナダなどでもデジタルアイデンティティを適切に設計・開発・運用・利用していく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）が策定されており、これら法規制やフレームワークに準拠したデジタルアイデンティティの活用が求められている。

### 1-3. 自己主権型アイデンティティモデル

- 既存のIMSモデルには、（悪意を持った）IdPにアカウント停止されるリスクや、（悪意を持った）IdPにアイデンティティを改ざんされるリスクが指摘されており、これら懸念に対応するモデルとして、「自己主権型アイデンティティ(Self-Sovereign Identity: SSI)」、「分散型アイデンティティ(Decentralized Identity: DID)」が提唱されている。
- SSIモデルが提示する①認証と属性の分離、②選択的なクレーム提示、③Unlinkability、④過去取得したクレームの再提示・検証が可能、といった特徴により、既存モデルの懸念を解消する可能性を有している。

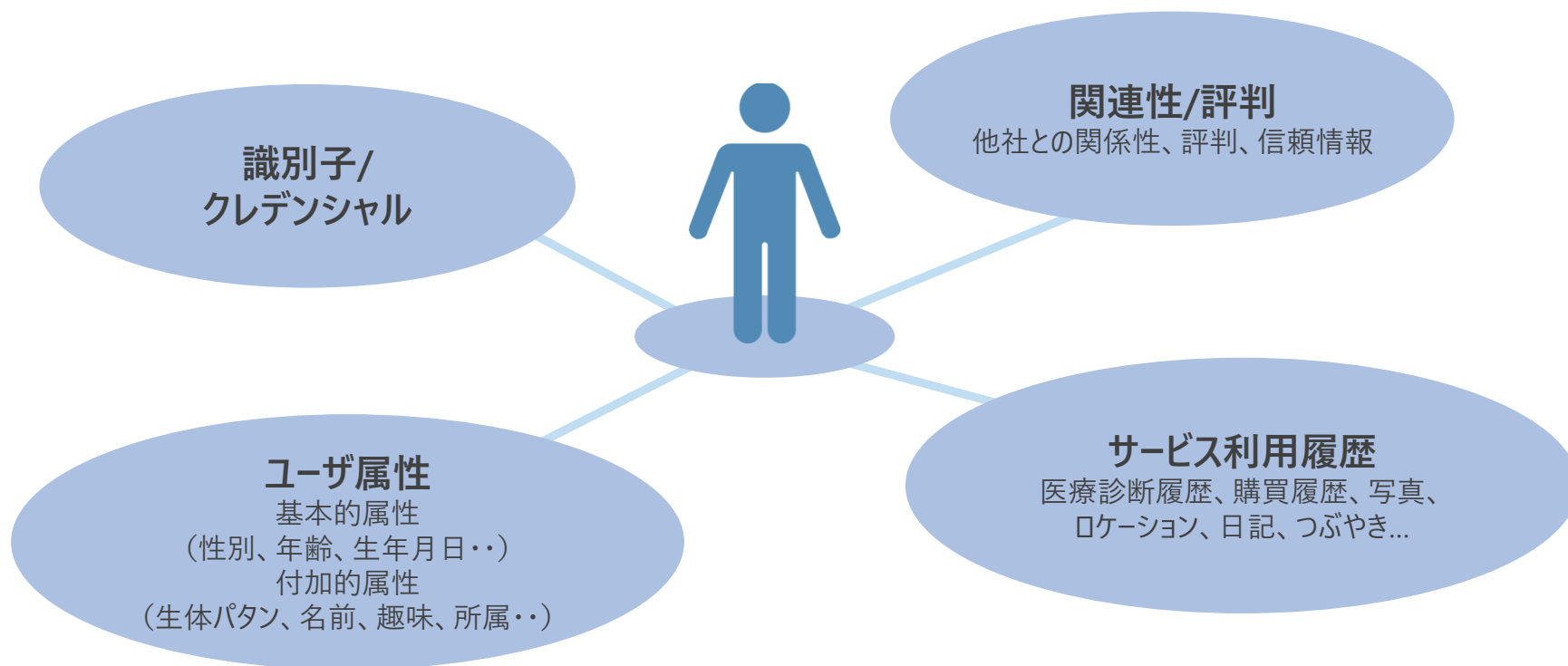
## 1-1. デジタルアイデンティティとアイデンティティマネジメントシステム(IMS)

---

## アイデンティティとは

- 「アイデンティティ」とは、「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」（ISO/IEC 24760）である。なお、エンティティは人だけでなく、組織やモノも含まれる。
- 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。

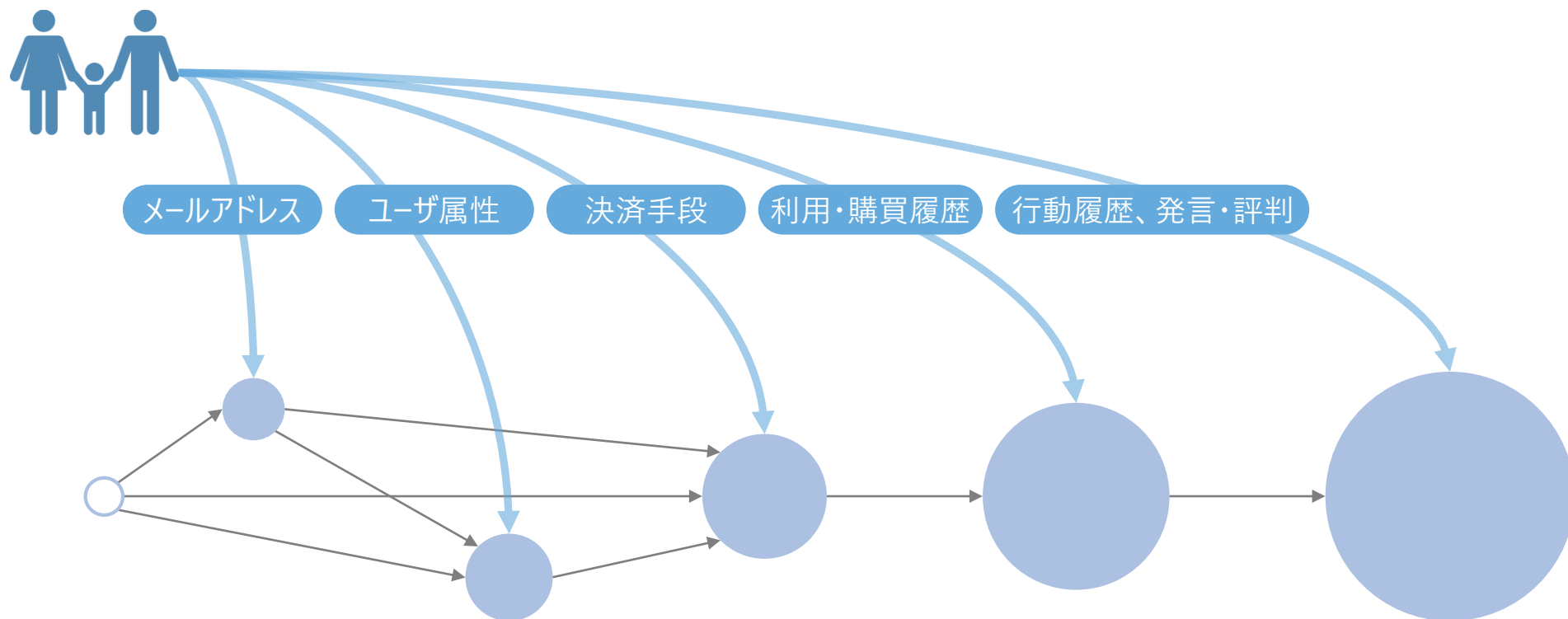
### 人のアイデンティティに含まれる属性例



## アイデンティティの特徴

- サービス利用や関係性とともに属性も増えるため、アイデンティティは一定のものでなく、属性の増加・変更に伴い変化・成長していく点が特徴である。

### アイデンティティの変化・成長例



## 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)

### デジタルアイデンティティとは

- 「デジタルアイデンティティ」は、各国・機関において様々な定義がなされているが、グローバルで定まっていないため、本調査では、ISO/IEC 24760のアイデンティティの定義(p.3)に沿って「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。

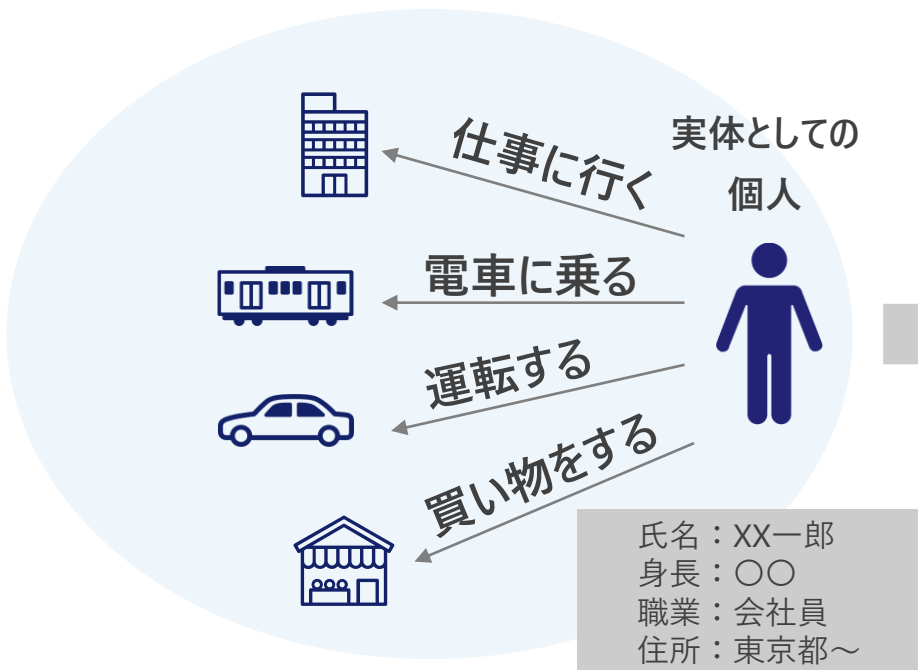
#### 主要組織におけるデジタルアイデンティティの定義例

団体	デジタルアイデンティティの定義
米国政府	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。 (US, "NIST SP 800-63 revision 3")
英国政府	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現である。 (UK, "The UK digital identity and attributes trust framework")
豪州政府	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	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。(ITU, X.1252 "Baseline identity Management terms and definitions")
World Bank	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。(ID4D, "Technical Standards for Digital Identification Systems")

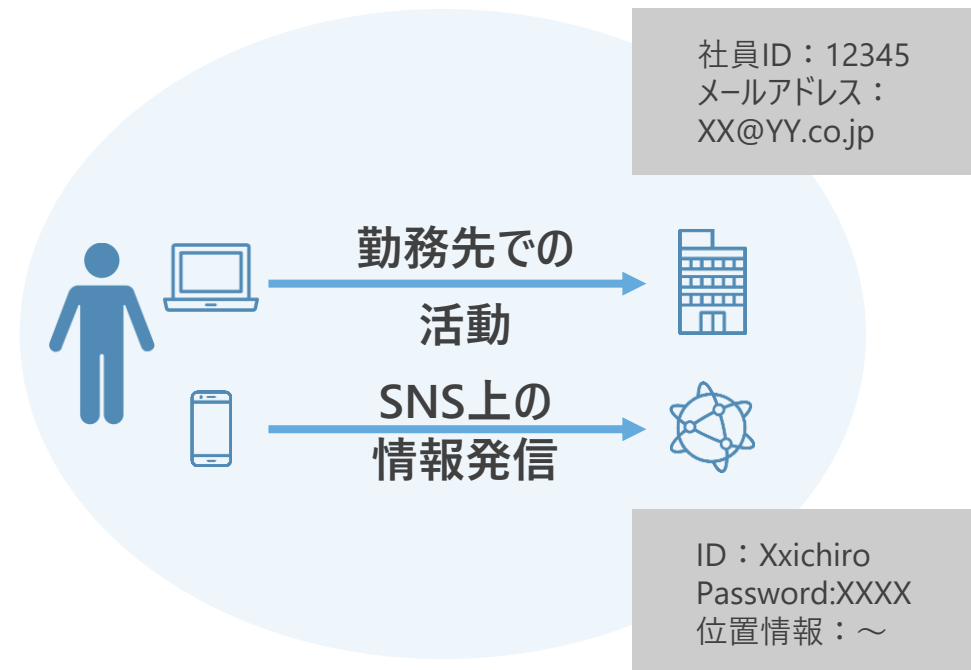
## デジタルアイデンティティの特徴

- 現実世界における個人の属性を容易にデジタル化できるようになったことで、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。
- 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。

### 現実世界のアイデンティティ



### デジタル世界のアイデンティティ



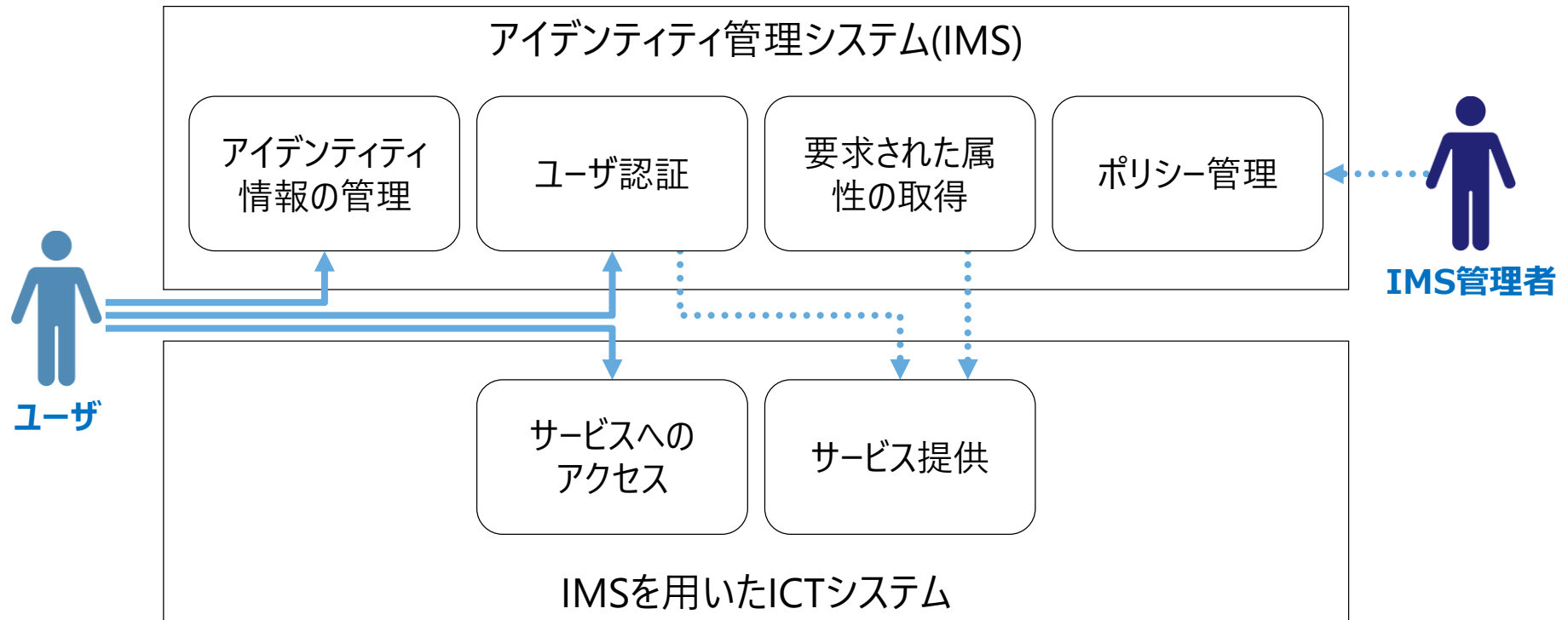


## 1-1. デジタルアイデンティティとアイデンティティマネジメントシステム(IMS)

### アイデンティティ管理システム(IMS)とは

- 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。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。
- 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活動（認証や属性情報の取得）が主な役割。

#### IMSの主な仕組み



## 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)

### 「アイデンティティの7原則」

- 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キム・キャメロン氏は、アイデンティティの管理での「**アイデンティティの7原則 (Seven Laws of Identity)**」を提唱している。
- IMSにおいてもこれら原則に基づく設計・開発・運用をしていくことが重要である。

#	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	正当な関係者のみへの情報開示	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イスを提供しなければならない

出所) Kim Cameron, "The Laws of Identity" <https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>

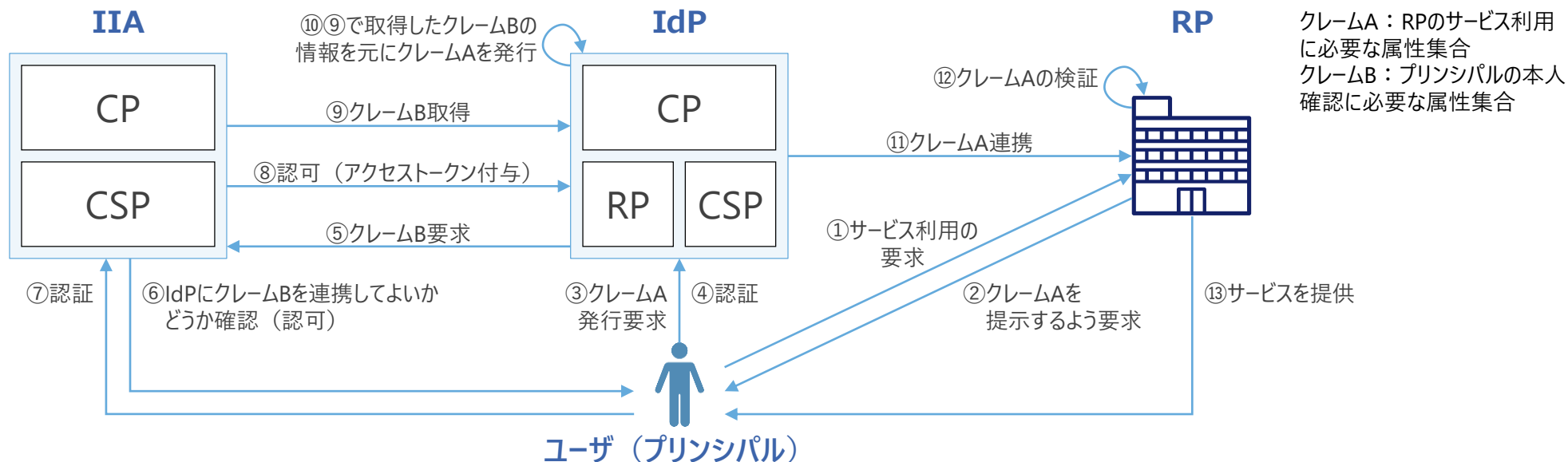
日本語訳は、崎村夏彦、「アイデンティティの7原則」 <https://www.sakimura.org/2011/05/1104/> を参照



## 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)

### IMSを構成する主要アクター

- IMSを構成する主要アクターとして、サービス提供事業者であるリライティングパーティへのクレーム（エンティティの属性集合のうちの一部）連携時（＝フェデレーションモデル）を例とすると、以下のアクターが存在する。



#	アクター (ロール)	定義
1	プリンシパル (Principal)	IMSにより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	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属性値の妥当性および／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エンティティ
3	アイデンティティプロバイダ (Identity Provider : IdP)	<ul style="list-style-type: none"> <li>利用可能なアイデンティティ情報を提供し、アイデンティティ情報を作成・維持するエンティティ。IIAがIdPの役割を担う場合もある</li> <li>アイデンティティ情報プロバイダ (Identity information provider : IIP)とも呼ばれる。</li> </ul>
4	クレデンシャルサービスプロバイダ (Credential Service Provider : CSP)	クレデンシャル（認証時に利用するアイデンティティの表明。例えばユーザID、パスワード）の管理責任を負う、信頼済みエンティティ。
5	クレームプロバイダ (Claims Provider: CP)	クレームを提供するエンティティ
6	リライティングパーティ (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

## 1-2. 主要なIMSモデルと構成要素

---

## 集中型モデルとサードパーティIdP/フェデレーションモデル

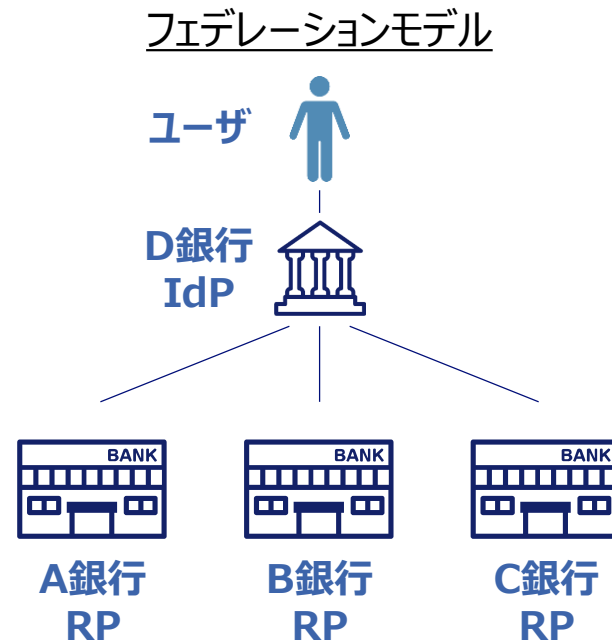
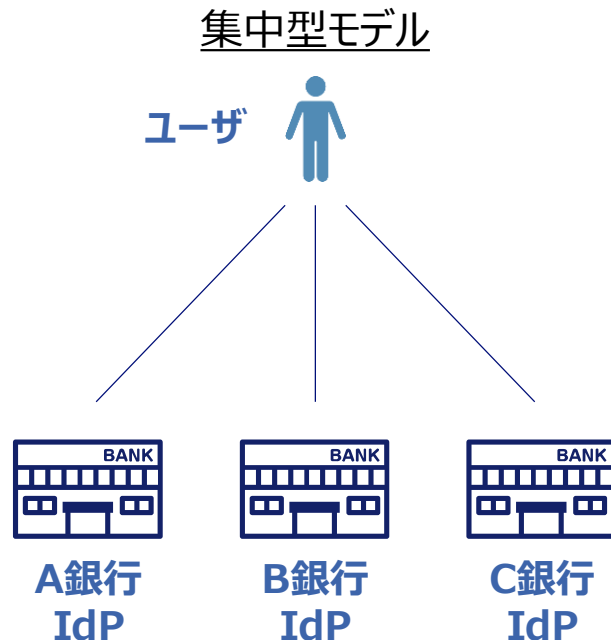
■ IMSのモデル/スキームとして、これまで/現在の代表的なものとしては以下の2つのモデルが挙げられる。

### ● Centralized (集中型) モデル

- RPがIdP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う。ユーザはサービス毎にアイデンティティ管理が必要  
例：ユーザはA銀行、B銀行、C銀行のオンラインバンキングにアクセスする際、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にアクセスする。

### ● フェデレーションモデル

- 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。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：ユーザは、A銀行、B銀行、C銀行のオンラインバンキングにアクセスする際、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にアクセスする。

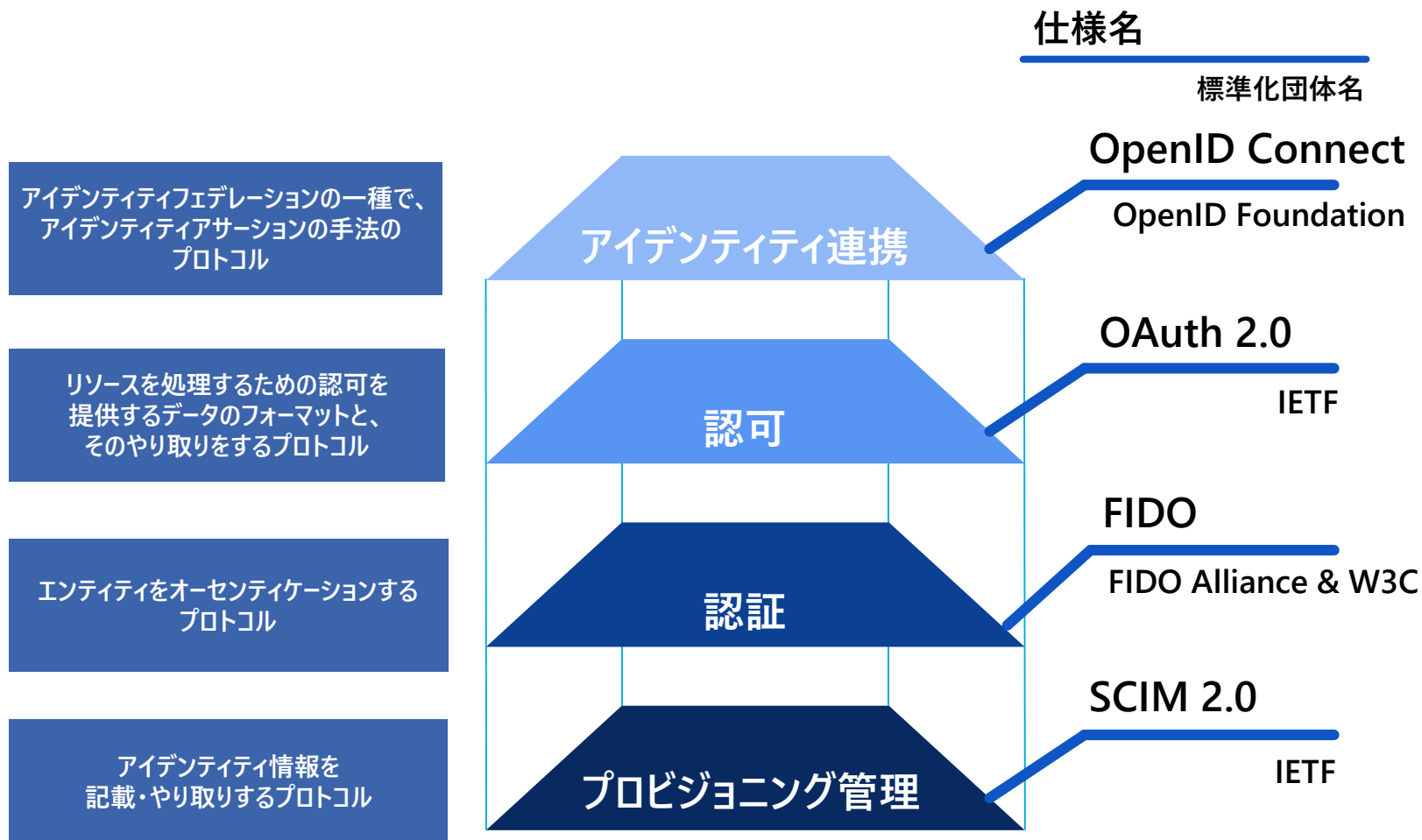


## 1-2. 主要なIMSモデルと構成要素

### 主要IMSモデルにおいて用いられる主な技術要素

- デジタルアイデンティティの活用において用いられているプロトコルと代表的な仕様は以下の通り。

#### プロトコル概要



## 1-2. 主要なIMSモデルと構成要素

# プロビジョニング管理：SCIM 2.0とは

### ■ SCIM 2.0 (System for Cross-domain Identity Management 2.0)

- 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、IMS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の仕様。

#### 登場の背景

- 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管理指示（プロビジョニング）を行う必要が生じた。
- プロビジョニング処理の標準化を目指し、SPLM（Service Provisioning Markup Language）というプロトコルが策定されたが、SPLMは仕様が複雑かつ相互運用性が悪く普及しなかった一方、クラウドサービスの発展と利用機会の増加に伴い、使い勝手の良い新たな仕様が必要となった。

#### 仕様の特徴

- 2015年に公開された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形式で記述すること、RESTfulなWeb APIでCRUDに特化した処理を行うこと、といった拡張性は持ちつつもシンプルな仕様とすることで、使い勝手の良いプロトコルとして利用の拡大が進んだ。
- 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。

#### 仕様の詳細

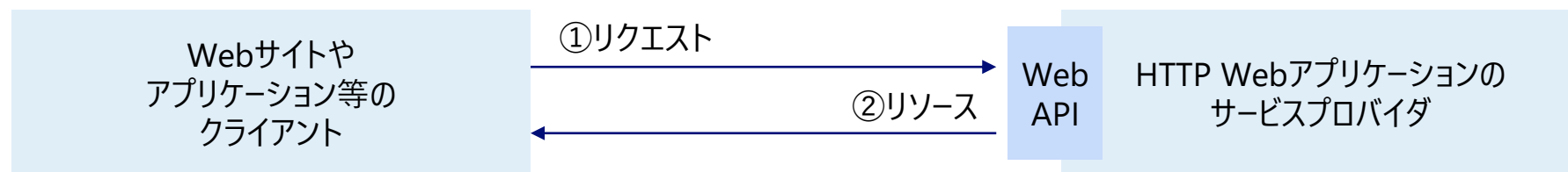
- SCIM 2.0は、Webサイトやアプリケーション等のクライアントが、HTTPのRESTプロトコルのリクエストメソッドを用いて、プロビジョニング（管理指示）を行うことができる。
- 指示の対象として、WebアプリケーションのIMS内においてJSON形式で管理されているアイデンティティ情報（属性（アトリビュート））の群（「リソース」）が規定されている。



## 1-2. 主要なIMSモデルと構成要素

## プロビジョニング管理：SCIM 2.0とは

## SCIM 2.0によるプロビジョニング処理概要



## ①RESTプロトコルでのリクエストメソッド

操作内容
作成
閲覧
置換
削除
更新

## ②「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		ユーザ名
name	Formatted	フルネーム 例：“Mr. Kenta Christopher Yamada, II”
	familyName	姓 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

## 1-2. 主要なIMSモデルと構成要素

### 認証：FIDOとは

#### ■ FIDO (Fast IDentity Online)

- 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、多要素認証を行うためのプロトコルの仕様。

#### 登場の背景

- 従来のIDとパスワードの組み合わせを用いたオーセンティケーション方式は、ネットワーク上での盗聴、ベリファイアへの不正アクセス、フィッシングサイト等による中間者攻撃でのクレデンシャル窃取、リスト型攻撃、といったリスクが存在していた。
- これに対応する為、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。

#### 仕様の特徴

- FIDOプロトコルは、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。
- 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。

#### 仕様の詳細

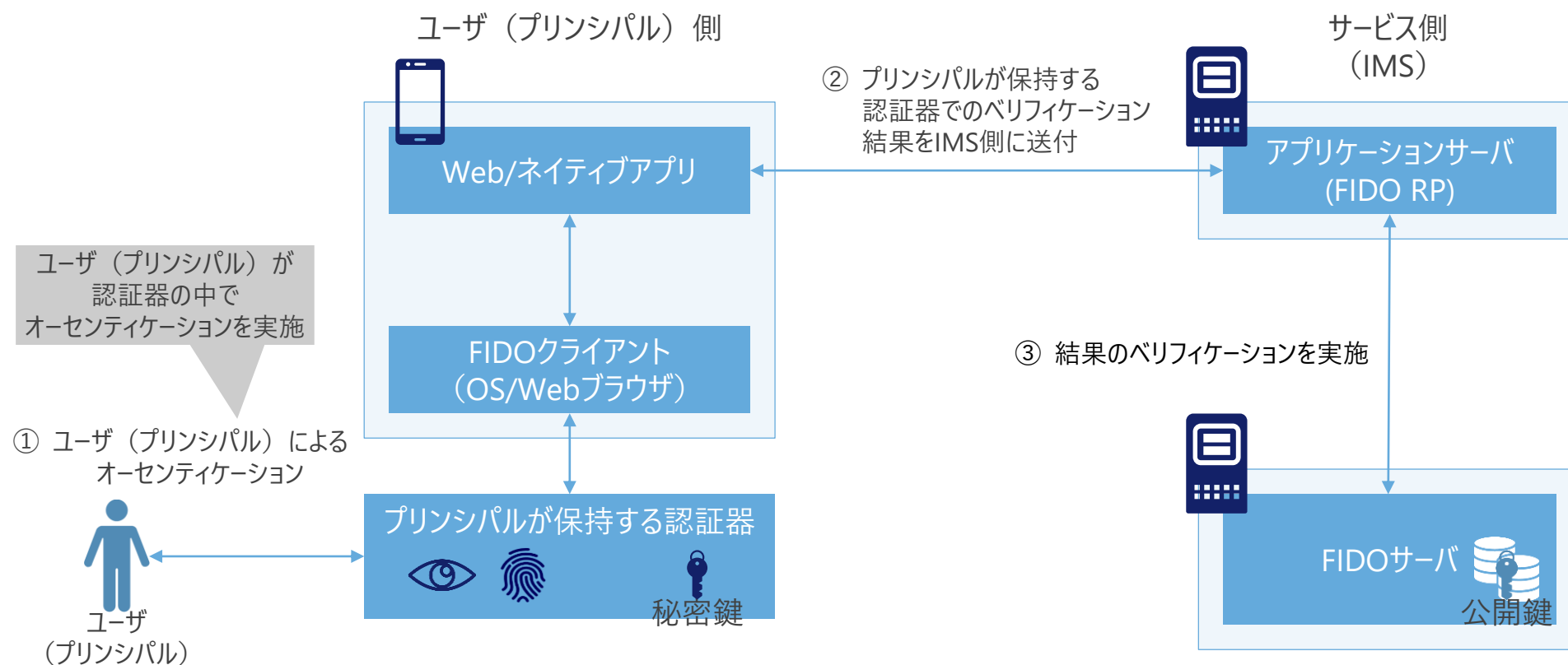
- FIDOの仕様策定と普及活動を担うFIDO Allianceでは、当初はUAF（Universal Authenticator Framework）、U2F（Universal Second Factor）と呼ばれる仕様策定を行った。
- その後、インターネットに関連する標準技術仕様が策定するW3Cにより、WebブラウザをFIDOクライアントとして機能させFIDO認証器にアクセスする為のAPI仕様が定義した、WebAuthn（Web Authentication API）が策定された。加えて、FIDOクライアントと認証器間の通信仕様が規定したCTAP（Client to Authenticator Protocol）が策定され、併せてFIDO2と呼んでいる。

## 1-2. 主要なIMSモデルと構成要素

## 認証：FIDOとは

- 秘密鍵はクライアントデバイス（認証器）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。

## FIDO2でのオーセンティケーション概観



## 1-2. 主要なIMSモデルと構成要素

### 認可：OAuth 2.0とは

#### ■ OAuth 2.0

- データ（例：アイデンティティ情報）やサービスといったリソース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ためのプロトコルの仕様。

#### 登場の背景

- 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、特定のリソースに対し処理させたいアプリケーション等に対し、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。
- このため、アプリケーションの情報漏えい時にリソースに全面的にアクセスできるクレデンシャル（パスワード）も流出されうるリスク、不必要なリソースへのアクセス権限までも付与する危険性、アプリケーションによるアクセスを制限（停止）する方法がクレデンシャルの変更に限定される、等の課題があった。
- このため、権限を限定とした個別のクレデンシャルを付与可能で、リソースのオーナーによって任意のタイミングでアクセスも制限できる仕様が求められていた。

#### 仕様の特徴

- OAuth 2.0は、アクセス権限を委譲する、認可という考えで規定されたOAuth 1.0から発展されている。
- 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。

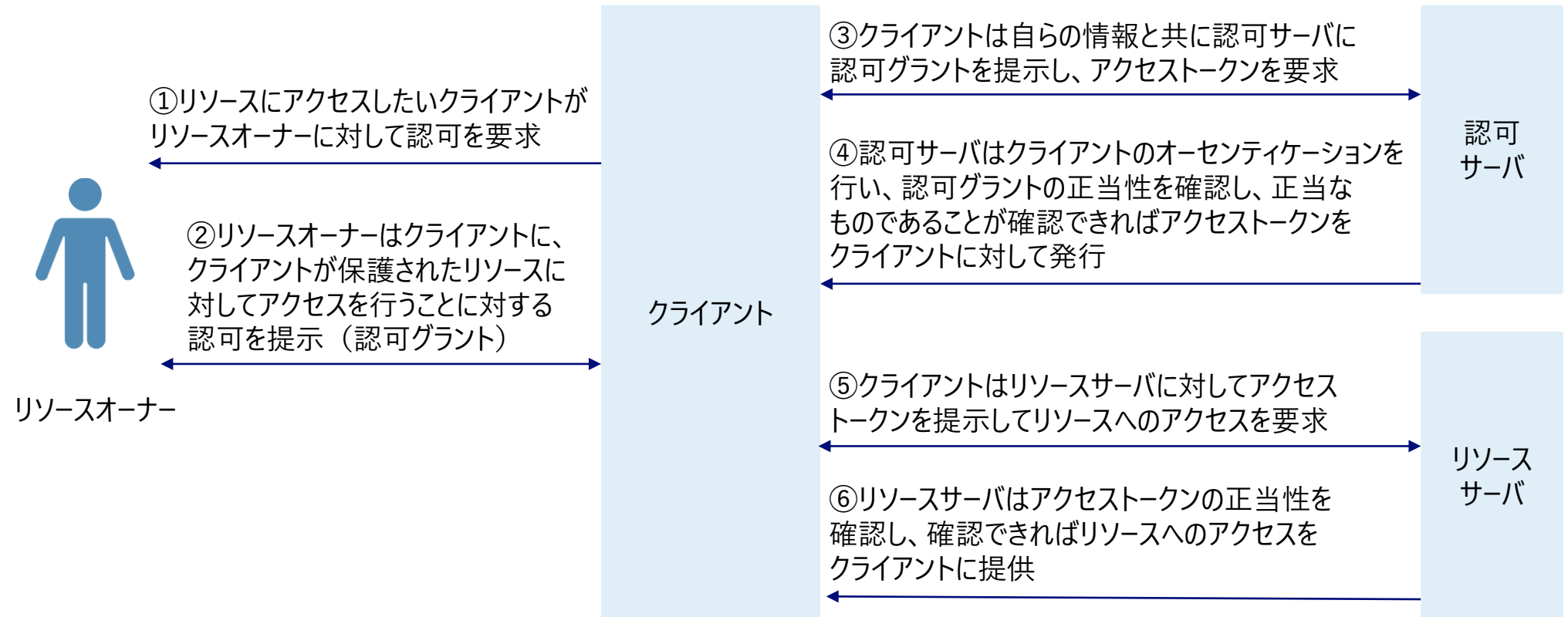
#### 仕様の詳細

- OAuth 2.0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ーション等（クライアント）、認可のやり取りの機能を提供する認可サーバに役割を分担している。

## 1-2. 主要なIMSモデルと構成要素

## 認可：OAuth 2.0とは

## OAuth 2.0の概観の流れ



## 1-2. 主要なIMSモデルと構成要素

## アイデンティティ連携：OpenID Connectとは

## ■ OpenID Connect

- IMSが他のIMSに対してアイデンティティ情報を渡す、アイデンティティフェデレーションを行うためのプロトコルの仕様。

## 登場の背景

- Webサービスにおけるシングルサインオンの需要等に対し、IMS同士のフェデレーションの実現手段として、SAML（Security Assertion Markup Language）と呼ばれるプロトコルが策定された。
- 同プロトコル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、より軽量の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。

## 仕様の特徴

- OpenID ConnectはOpenID FoundationによってOAuth 2.0を土台として2014年に公開され、XMLではなくJSON形式での軽量の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な点などから、広く利用されるようになった。

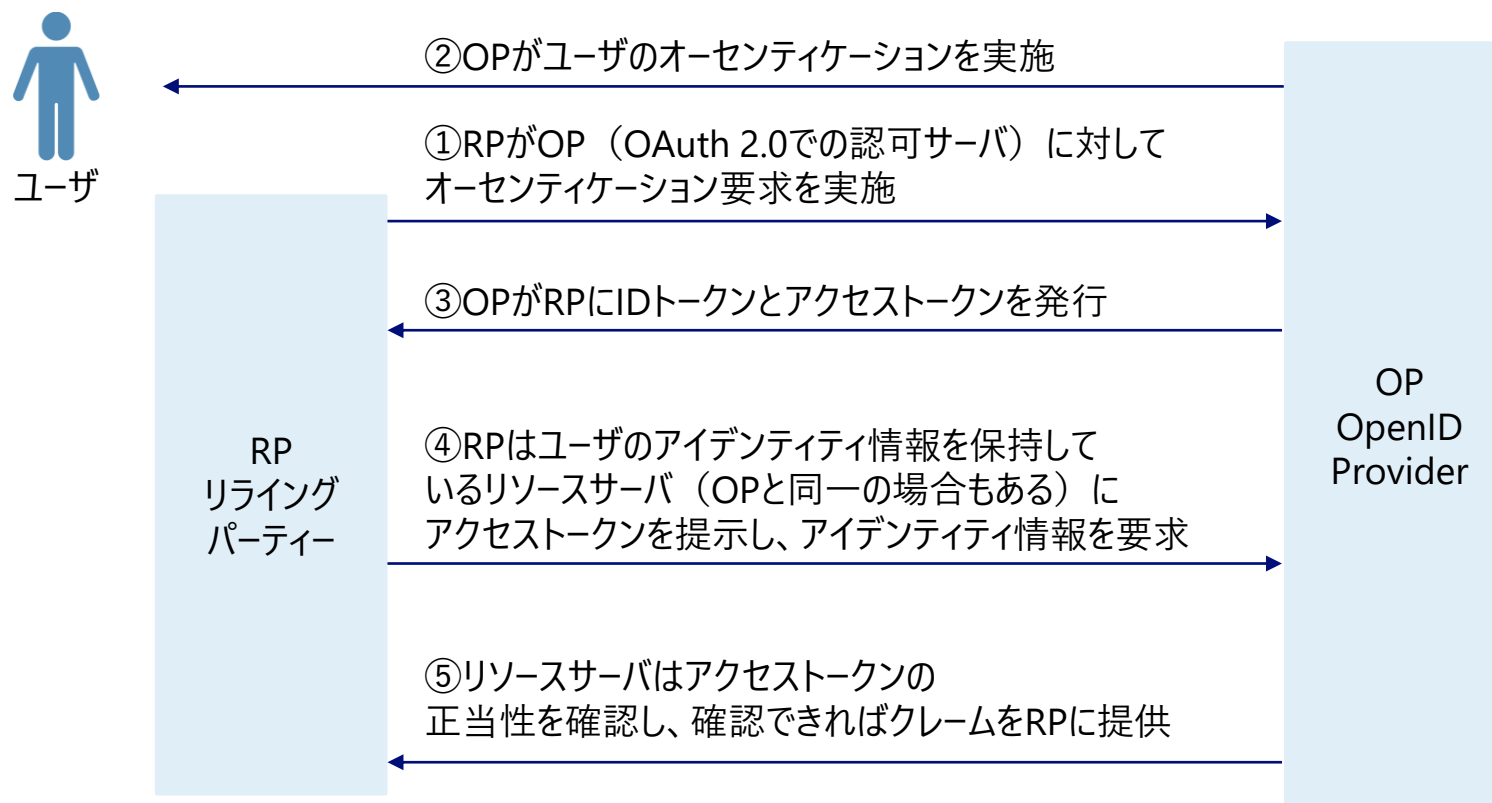
## 仕様の詳細

- OpenID Connectは OAuth 2.0 認可プロセスに認証の概念を拡張することで、セキュアなID連携とAPI連携を利用可能としている。
- リライティングパーティー（OAuth 2.0でのクライアント）はOpenID Provider（OAuth 2.0での認可サーバ）からのユーザのオーセンティケーションの結果やアイデンティティ情報が含まれる「IDトークン」と呼ばれるJSON Web Token（JWT）を受け取るか、もしくはリソースサーバから、ユーザ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情報を受け取る。

## 1-2. 主要なIMSモデルと構成要素

## アイデンティティ連携：OpenID Connectとは

## OpenID Connectの処理概観



## 1-2. 主要なIMSモデルと構成要素

# 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（トラストフレームワーク）

- 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。

### OIXのトラストフレームワークで規定される構成要素

構成要素	項目	構成要素	項目	構成要素	項目
原則		リライディングパー 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	技術・セキュリ ティ要件	セキュリティルール
トラストマークとUX			レクエスト&レスポンス(API)		エコシステム参加者のトラストレジス トリ
役割と義務			RPによるID保証		証跡の記録と提示
一般ルール	記録保存と監査証跡		ライアビリティ		リクエスト及びレスポンススキーム
ユーザサービス	不正行為とサイバーコントロール	トラストルール	サービスレベル	相互運用性	内部の相互運用性
	デジタルアイデンティティの選択		ヘルプ&サポート		外部の相互運用性
	IDの作成&管理		ブルーフィンギ	ガバナンス	トラストフレームワークの構築と管理
	トラストの獲得と提示		アイデンティティ保証		トラストフレームワークの強制力
	同意		認証		トラストフレームワークの認証
ヘルプ&サポート	適格性保証		トラストフレームワークの運用		



## 1-2. 主要なIMSモデルと構成要素

### 諸外国におけるデジタルアイデンティティに関する主なガバナンスフレームワーク

- 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、各IMS運営主体はこれらを踏まえたガバナンスの態勢構築が求められている。
- 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。

#### 諸外国におけるデジタルアイデンティティに関する主なガバナンスフレームワーク

国	発行組織	ガバナンスフレームワーク	概要
米国	NIST	NIST SP800-63シリーズ (2017)	<ul style="list-style-type: none"><li>アメリカ国立標準技術研究所(NIST)は、「電子的認証に関するガイドライン」としてSP800-63シリーズを策定しており、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。</li></ul>
EU	欧州委員会	eIDAS規則	<ul style="list-style-type: none"><li>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)</li></ul>
豪州	デジタルトランスフォーメーション庁	Trusted Digital Identity Framework	<ul style="list-style-type: none"><li>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ーの認証の基準やルールを規定。</li></ul>
英国	デジタル・文化・メディア・スポーツ省	UK Digital Identity and Attributes Trust Framework	<ul style="list-style-type: none"><li>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、リライティングパーティ）向けのガイドライン（アルファ版）。将来的にプロバイダー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。</li></ul>
カナダ	DIACC ※非営利団体	Pan-Canadian Trust Framework (PCTF) 1.0	<ul style="list-style-type: none"><li>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。</li><li>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。</li></ul>
-	OIX ※非営利団体	OIX Guide to Trust Frameworks	<ul style="list-style-type: none"><li>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。</li><li>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。</li></ul>

## 1-3. 自己主権型アイデンティティモデル

---

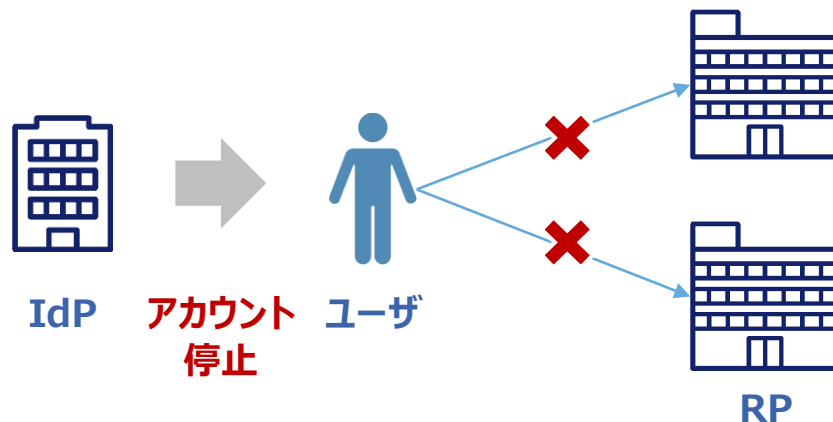
### 1-3. 自己主権型アイデンティティモデル

## フェデレーションモデルに対する懸念

- 現在フェデレーションモデルが主流となっており、IdPへの依存度が高まっている。
- しかしながら、特定のIdPに依存することに対する懸念点も指摘されている。例えば、以下のようなリスクが顕在化した場合、ユーザに与える影響は甚大である。
  - ① IdP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）
  - ② （悪意を持った）IdPにアイデンティティを改ざんされるリスク
- これら懸念を解決しうる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)」と、その仕組みとして「分散型アイデンティティ(Decentralized Identity: DID)」が提唱されている。

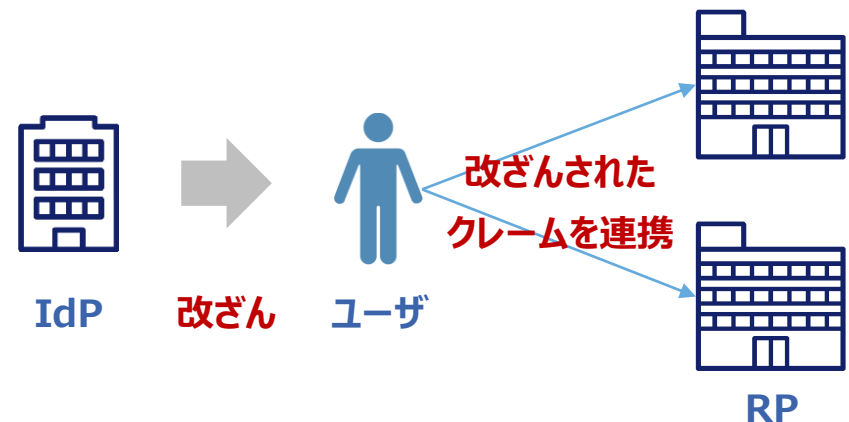
#### 例：IdPにアカウント停止されるリスク

- IdPがユーザのアカウント停止することで、ID連携で活用している其他サービスも利用できなくなってしまう。



#### 例：IdPに改ざんされるリスク

- IdPが、意図的にユーザのアイデンティティを改ざんし、改ざんされたクレームがRPに連携されてしまうリスクがある。

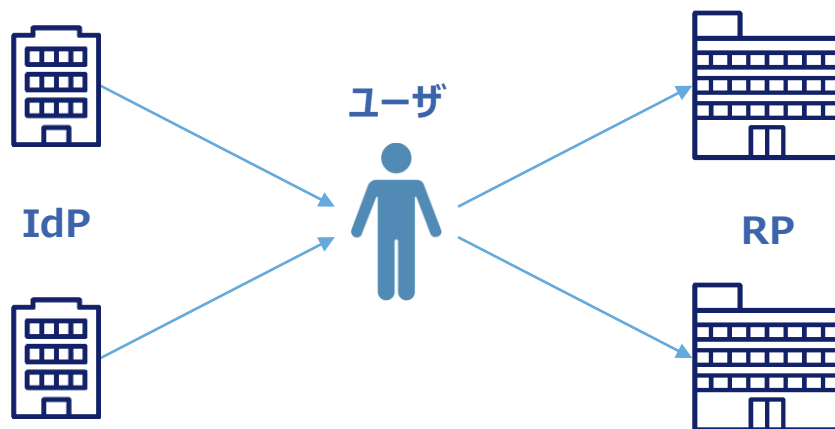


## 自己主権型アイデンティティ/分散型アイデンティティとは

### ■ 自己主権型アイデンティティ(Self-Sovereign Identity: SSI)

- 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旨とする思想(※1)。
- 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RPに連携する。

SSIの概念図

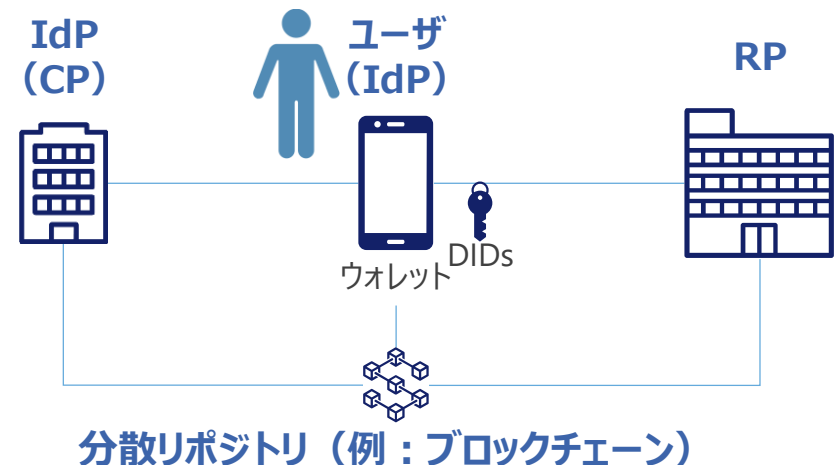


### ■ 分散型アイデンティティ(Decentralized Identity: DID)

- 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指す思想であるSSIに対し、分散型アイデンティティは、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が目的とする仕組み。
- 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以下のように定義している(※2)。

「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」

DIDの概念図



※1 : Sovrin Foundation, <https://sovrin.org/faq/what-is-self-sovereign-identity/>

※2 : Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access-management/decentralized-identity-blockchain>

### 1-3. 自己主権型アイデンティティモデル

## SSIの7原則

- 「アイデンティティの7原則 (Seven Laws of Identity)」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「SSIの7原則」を提示している。
- アイデンティティの7原則から、**主に原則 5 及び 6 がSSI版として更新**されている。本更新内容の詳細は3章で詳述。

#	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	正当な関係者のみへの情報開示	• 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できる「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	「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

出所) 崎村夏彦、「The Law of Identity in SSI Era by Kim Cameron」を基にNRI作成

<https://nat.sakimura.org/2020/06/23/the-law-of-identity-in-ssi-era-by-kim-cameron/>

## 第2章 金融分野におけるデジタルアイデンティティの活用可能性

---

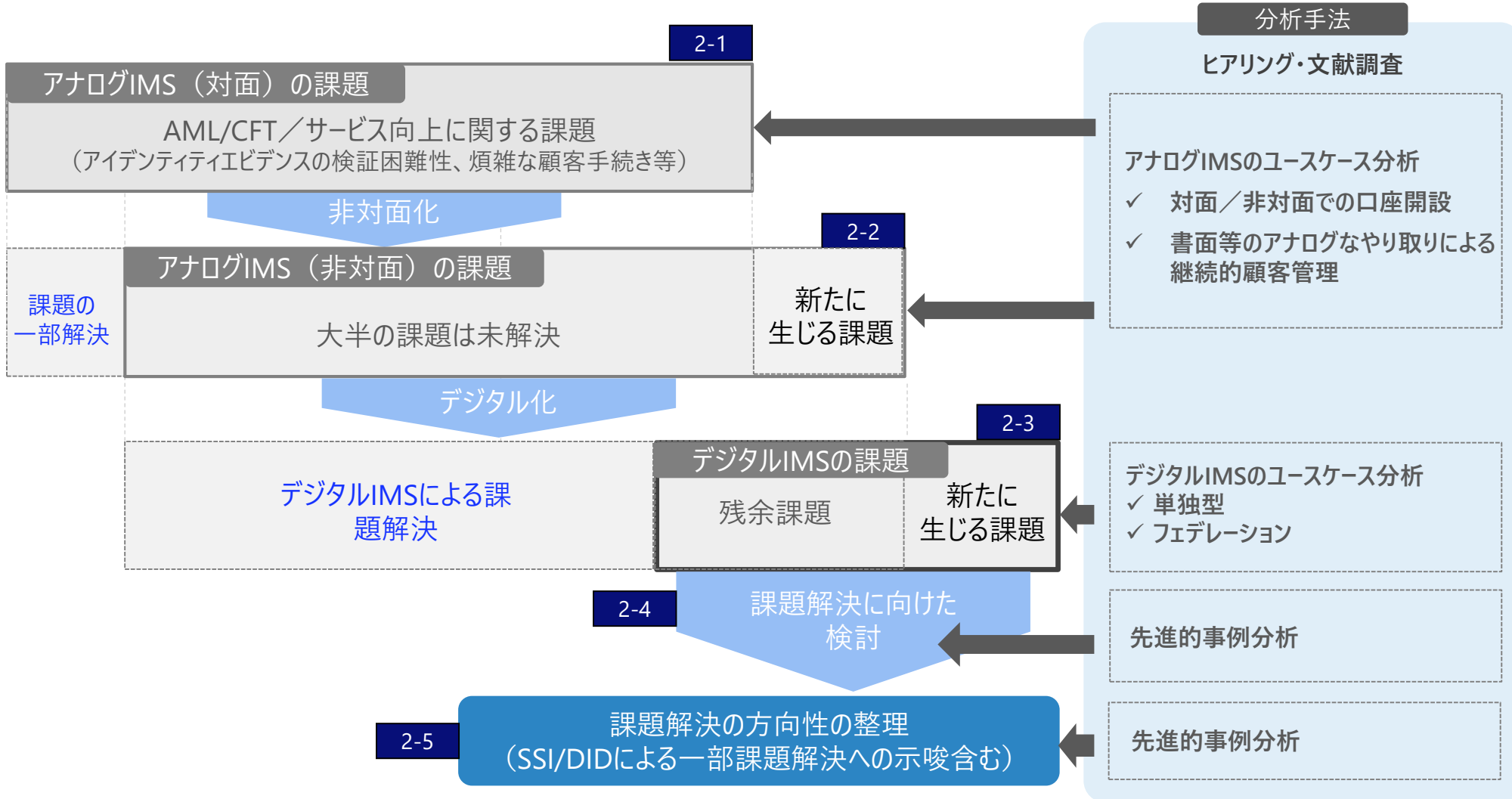
## 2. 本章の概要

---

## 2. 本章の概要

# 本章の流れ

第1章：アイデンティティに関わる技術や運用についての基礎



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)の活用可能性と課題



## 2. 本章の概要

### 調査方法

- 次節以降で述べる各種課題の抽出や課題解決の方向性の調査にあたっては主に以下の手法を用いた。
  - 国内・海外有識者へのヒアリング調査
  - 文献調査
  - 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
- 調査の対象・観点
  - 金融分野におけるデジタルアイデンティティ活用に関連する多様なステークホルダーを対象にヒアリング、および各ステークホルダーが発行した文献の調査を実施した。
  - 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業務分析を実施した。

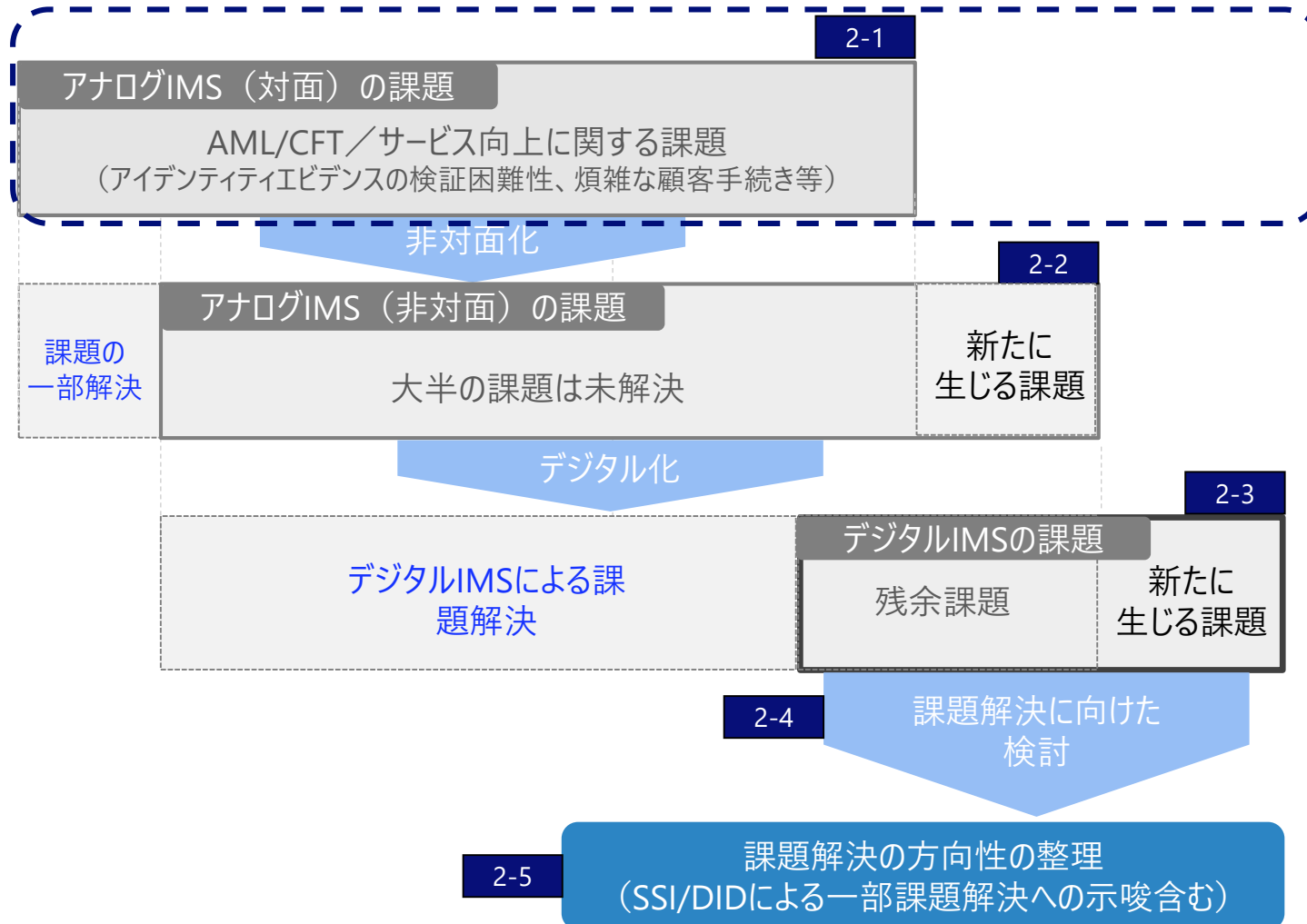
#### 調査対象先と調査の観点

調査対象先		課題抽出/課題解決の方向性調査の観点
国内	金融機関 法曹関係者 ソリューションベンダー	<ul style="list-style-type: none"><li>● 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</li><li>● 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</li><li>● デジタルアイデンティティ活用時の法的・技術的課題</li></ul>
海外	金融機関 規制当局/関連団体 国際機関 業界団体 標準化団体 ソリューションベンダー	<ul style="list-style-type: none"><li>● 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</li><li>● 顧客利便性向上に資する具体的な活用事例とその課題</li><li>● 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</li><li>● 規制整備/規制対応の状況・今後の展望</li><li>● 技術標準化動向</li></ul>

## 2-1. 金融機関のアイデンティティ管理の現状と課題

---

## 本節での議論対象



# アイデンティティ管理業務の概略

### ■ 本章の調査対象分野

- 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。
- 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。
- 本章では、アイデンティティ管理との関連が大きいと考えられる分野を主な調査対象として選定した。
- 本人確認が法令で定められる等、アイデンティティ管理が最も厳格に求められるAML/CFT規制対応について、その一部である本人確認に関する業務を中心に議論する。
- 加えて、利用者の最善の利益に沿った商品・サービスの提供を目標とする、多面的なアイデンティティ情報を活用した顧客サービスの向上にも言及する。

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、分析・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・サービスの提供のための努力	アイデンティティ情報を活用した顧客サービスの向上

出所：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](https://www.fsa.go.jp/news/30/wp/supervisory_approaches_revised.pdf) を元にNRI作成

## 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

### アイデンティティ管理業務の概略

#### ■ 本章で検討する業務の分類

- 前頁の対象分野について、本章で検討する業務の種類を、業務の目的と業務の実施タイミングから、3種類に分類する。
- なお、ここでの「onboarding」「ongoing」は業務の実施タイミングの分類を意味し、以降の頁でも同様とする。
  - 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、用語集に記載の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、用語集に記載のongoing due diligence (継続的顧客管理) は②を指す。

		業務の実施タイミング	
		onboarding	ongoing
業務の目的	AML/CFT規制対応	①口座開設 (取引時確認)	②継続的顧客管理
	顧客サービスの向上	(アイデンティティ登録前のため業務無し)	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

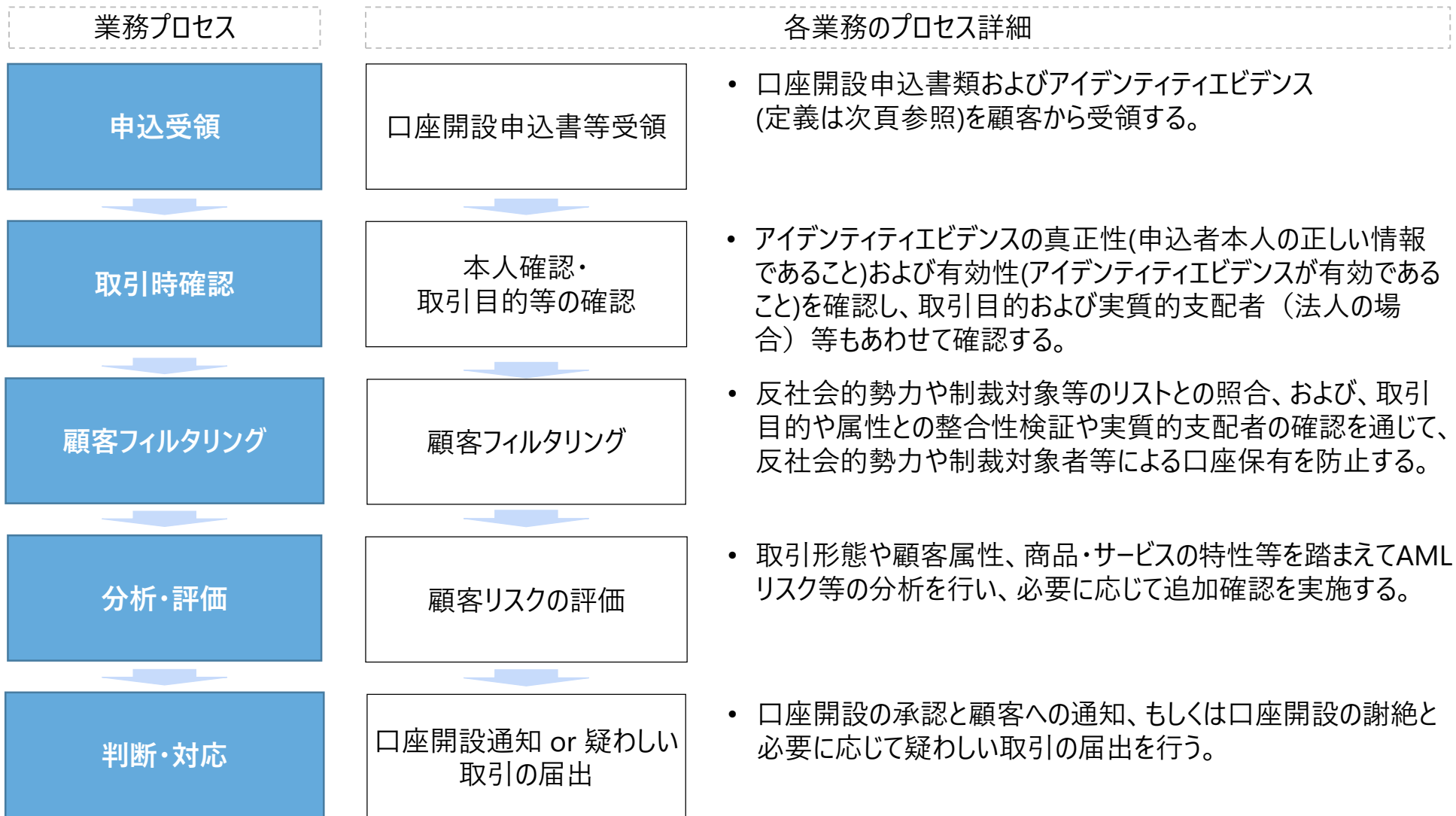
業務分類毎のアイデンティティ管理業務概略

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
	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
ongoing	②継続的顧客管理 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 (テラーメイドのサービス提案等)

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## アイデンティティ管理業務の詳細 ①口座開設（取引時確認）

### 口座開設（取引時確認）の業務プロセス



## 補足：本章におけるアイデンティティエビデンスの定義と具体例

- 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・エビデンスの一例

個人/法人	概要
個人	<ul style="list-style-type: none"><li>• 本人確認書類<ul style="list-style-type: none"><li>✓ 運転免許証</li><li>✓ パスポート</li><li>✓ 国民IDカード(例：日本におけるマイナンバーカード)</li><li>✓ 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</li></ul></li></ul>
法人	<ul style="list-style-type: none"><li>• 法人確認書類<ul style="list-style-type: none"><li>✓ 登記事項証明書</li><li>✓ 印鑑登録証明書</li><li>✓ 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</li></ul></li><li>• 担当者・代表者・実質的支配者の本人確認書類<ul style="list-style-type: none"><li>✓ 個人と同様</li></ul></li></ul>

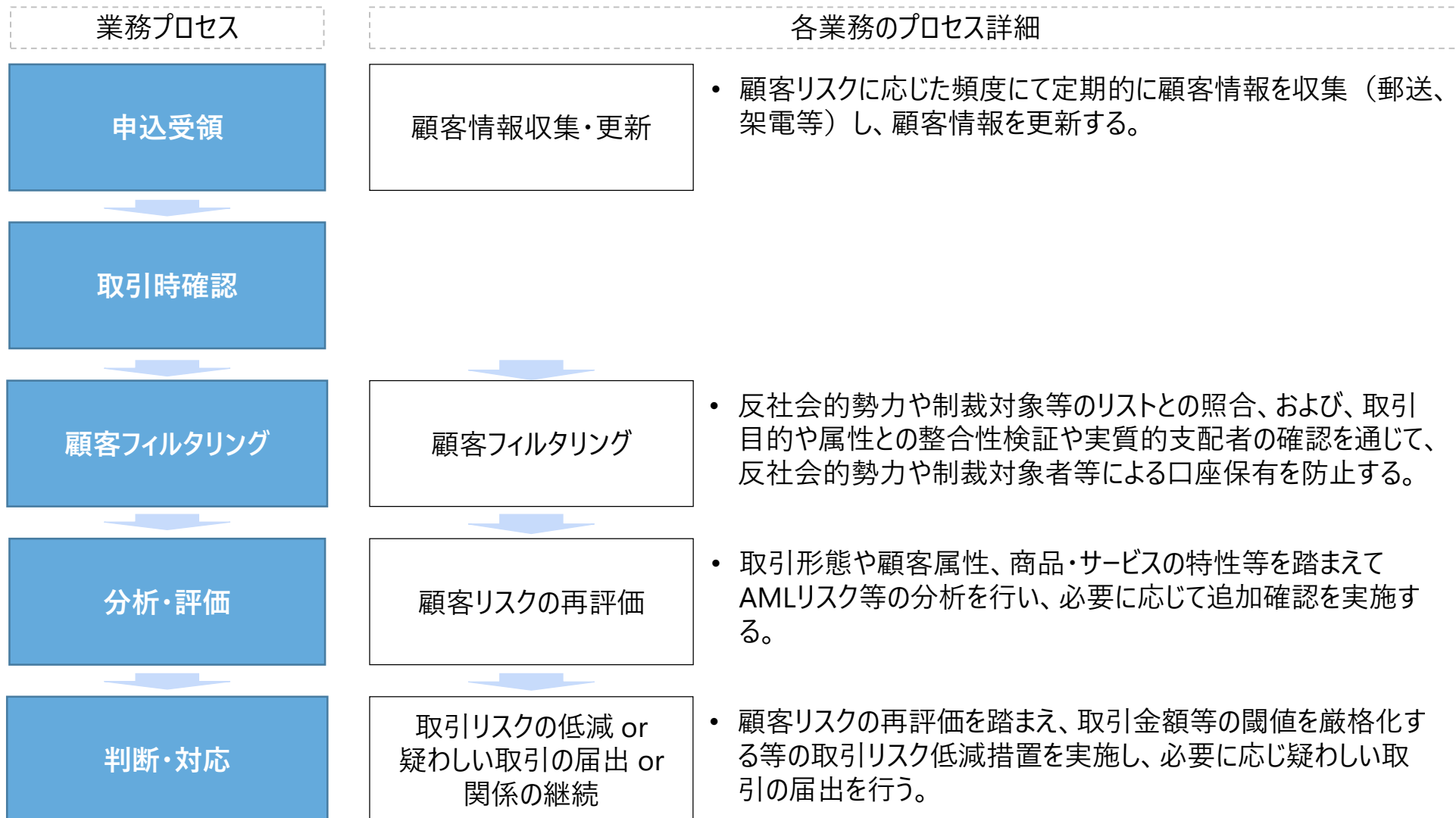
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## アイデンティティ管理業務の詳細

### ②継続的顧客管理

### ②-1 定期的顧客情報調査

#### 定期的顧客情報調査の業務プロセス

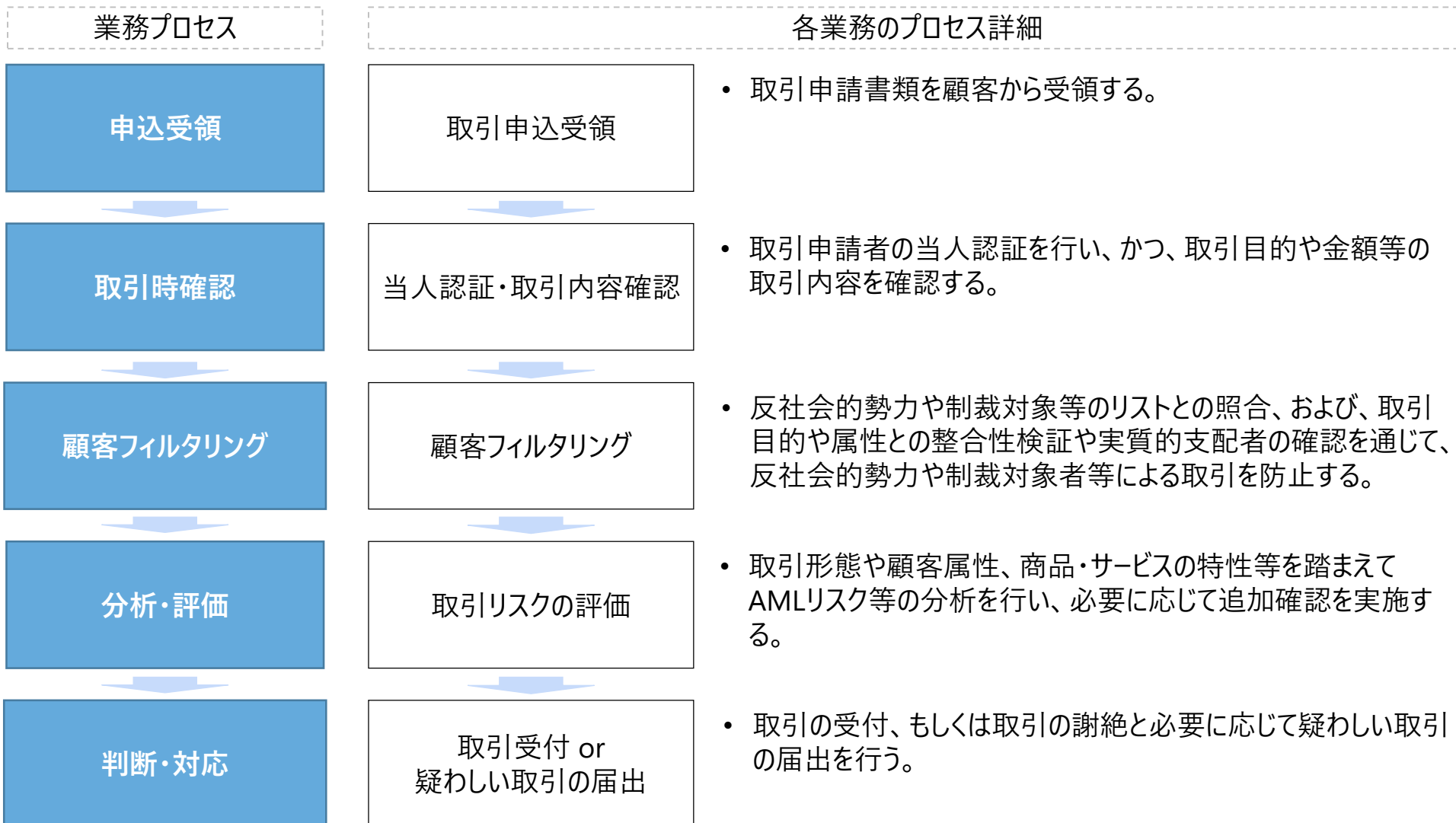




	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## アイデンティティ管理業務の詳細 ②継続的顧客管理 ②-2 取引受付時確認

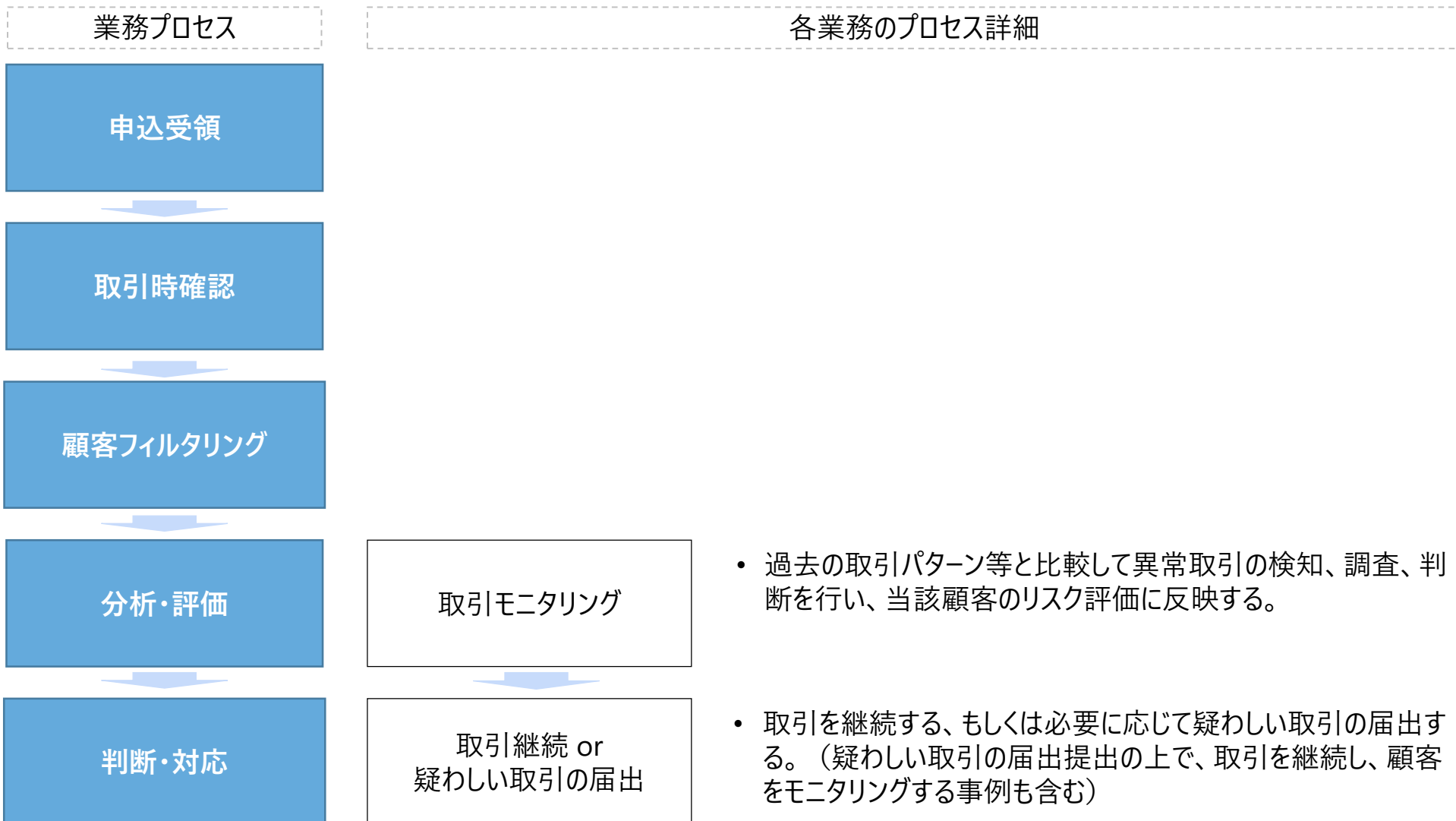
### 取引受付時確認の業務プロセス



	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## アイデンティティ管理業務の詳細 ②継続的顧客管理 ②-3 取引モニタリング(事後)

### 取引モニタリング(事後)の業務プロセス



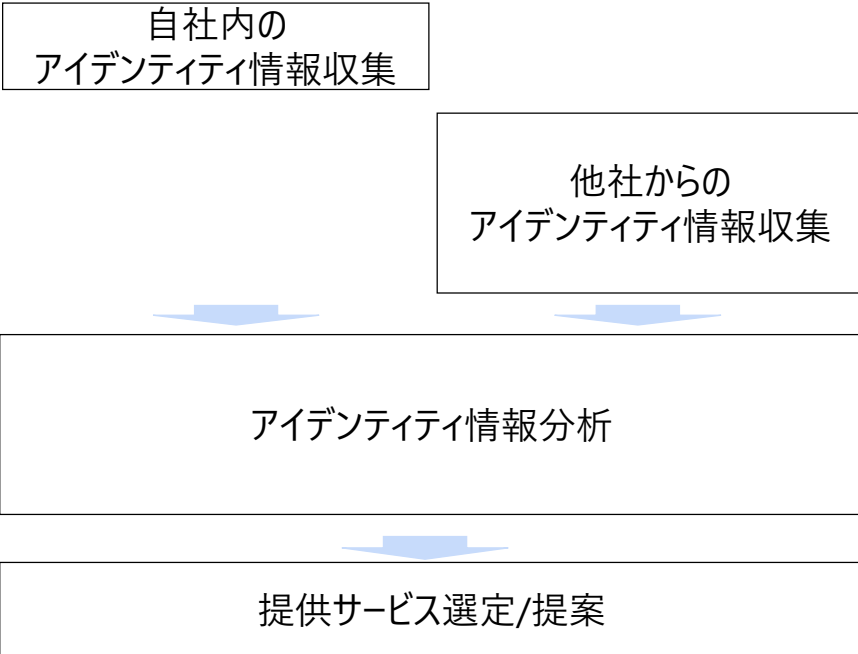
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 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

### アイデンティティ管理業務の詳細 ③社内外のアイデンティティ情報を活用した顧客サービス向上

- 顧客に紐づく社内外の多様なアイデンティティ情報の収集・分析により、テラーメイドのサービス提案等、顧客サービス向上に資する取り組みを実施する。

#### 社内外のアイデンティティ情報を活用した顧客サービス向上の業務プロセス



- 自社内において、取引情報等顧客に紐づく情報を収集する。
- 他社から、金融/非金融の取引情報や非伝統的情報(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する。
- 収集した情報から、顧客のファイナンスニーズ等を分析する。(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)
- 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を行う。

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 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

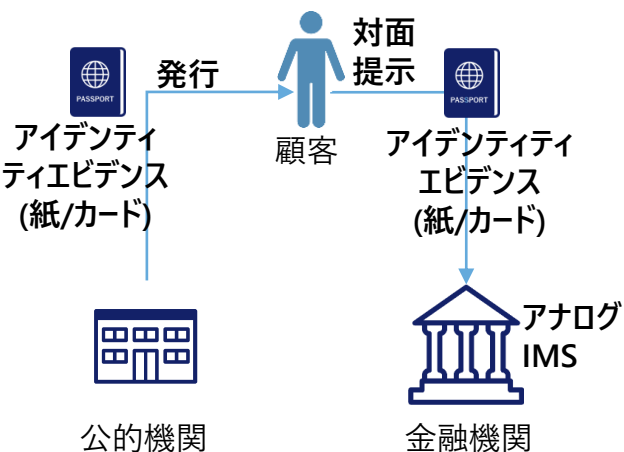
### 依然としてアナログ中心のアイデンティティ管理業務

■ アナログのアイデンティティエビデンス\*の対面利用、書面の郵送による手続き等、アナログ中心の業務を実施している。

\* アナログのアイデンティティエビデンス：紙・カード・画像等、エビデンスの情報をデータとして読み取ることができないアイデンティティエビデンスを指す

#### 口座開設（取引時確認）

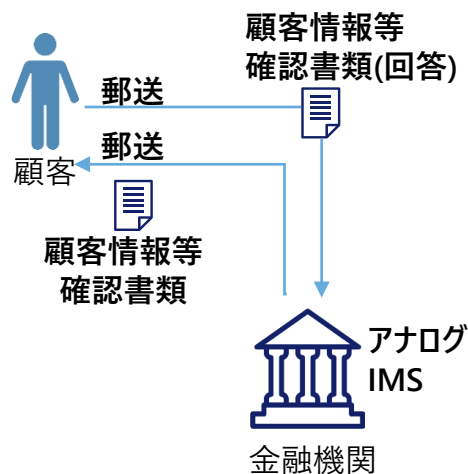
- 顧客はアナログのアイデンティティエビデンスを金融機関に対面で提出している。
- 金融機関は当該エビデンスを元に本人確認を実施している。



\*公的機関へのアイデンティティエビデンスの真正性および有効性照会は、アナログのアイデンティティエビデンスでは行われていない

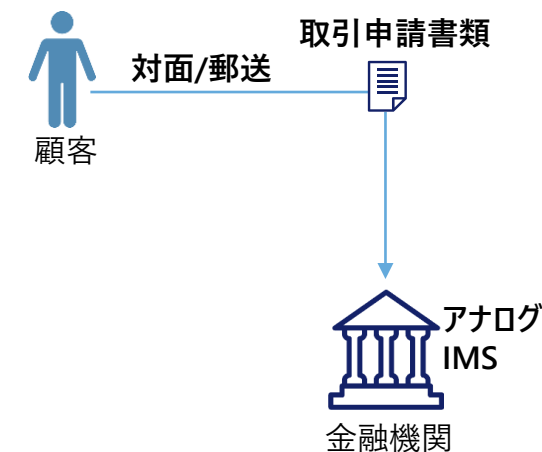
#### 継続的顧客管理（定期的顧客情報調査）

- 金融機関は顧客情報等確認書類を顧客に郵送している。
- 顧客は顧客情報等確認書類(回答)を金融機関に郵送している。
- 金融機関は本人確認と属性変更登録を実施している。



#### 継続的顧客管理（取引受付時確認）

- 顧客は対面または郵送で金融機関に取引を申請している。
- 金融機関は当該エビデンスを元に本人確認を実施している。



	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

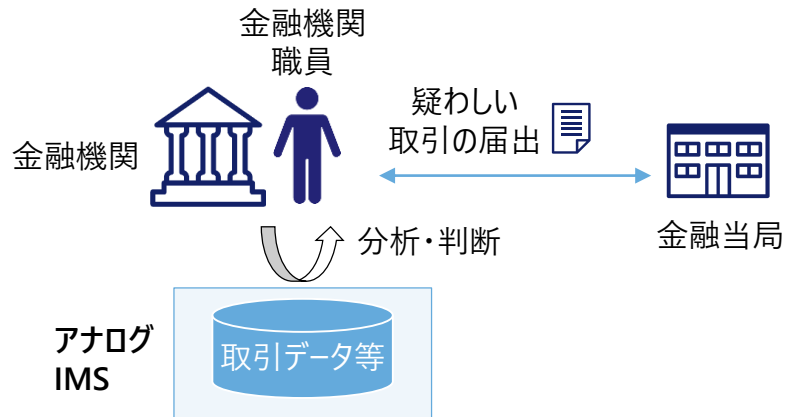
## 2-1-1. 金融機関におけるアイデンティティ管理業務の現状

### 依然としてアナログ中心のアイデンティティ管理業務

- 自社の取引データ等を利用して、分析・評価を実施している。

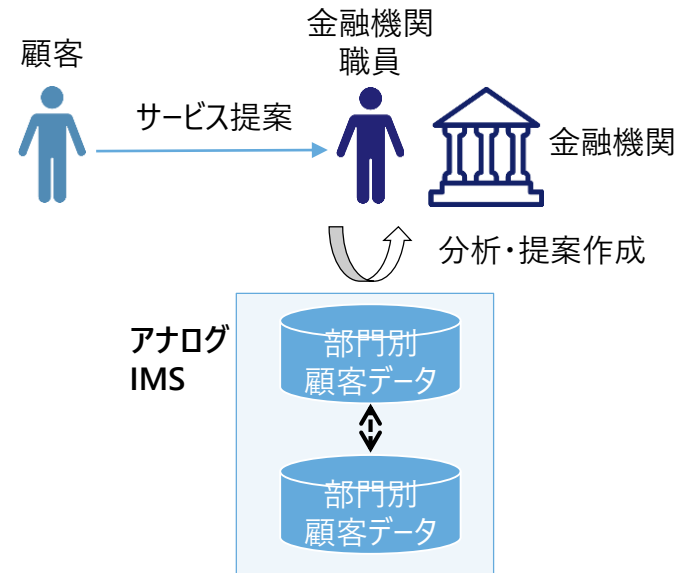
#### 継続的顧客管理（取引モニタリング(事後)）

- ・金融機関はサンクションリスト等および金額等の閾値や顧客の取引傾向から異常取引を検知している。
- ・金融機関は検知した異常取引の内容を精査し、精査結果に応じて顧客リスクを再評価している。
- ・金融機関は検知した異常取引が疑わしい取引に該当する疑いがある場合は、疑わしい取引の届出を実施している。



#### 社内外のアイデンティティ情報を活用した顧客サービス向上

- ・金融機関は顧客の属性や取引傾向を分析し、顧客に適したサービスを選定／設計している。
- ・金融機関は顧客にサービスを提案している。



	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 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）

### ①口座開設（取引時確認） 課題の概要

- 金融機関におけるアイデンティティ検証困難性や、顧客の事務負担が主な課題である。
- 次頁以降で主要課題（下表ハイライト部分）について詳述する（その他の課題については補足資料参照）。

		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	<ul style="list-style-type: none"> <li>・申込情報やアイデンティティエビデンス情報をデータ化する負担</li> </ul>	<ul style="list-style-type: none"> <li>・新興国における遠隔地居住者の金融包摂</li> <li>・顧客の来店負担</li> <li>・顧客の書類記入負担</li> <li>・顧客の事務処理待ち時間</li> <li>・金融機関毎に同様の口座開設申込を行う負担</li> </ul>
	取引時確認	<ul style="list-style-type: none"> <li>・アナログのアイデンティティエビデンスの検証困難性</li> <li>・オペレーショナルコスト(書類保管コスト)</li> <li>・他社で検証済の顧客を一から検証する負担</li> </ul>	
	顧客フィルタリング	<ul style="list-style-type: none"> <li>・他社で検証済の顧客を一から検証する負担</li> </ul>	
	分析・評価		
	判断・対応		

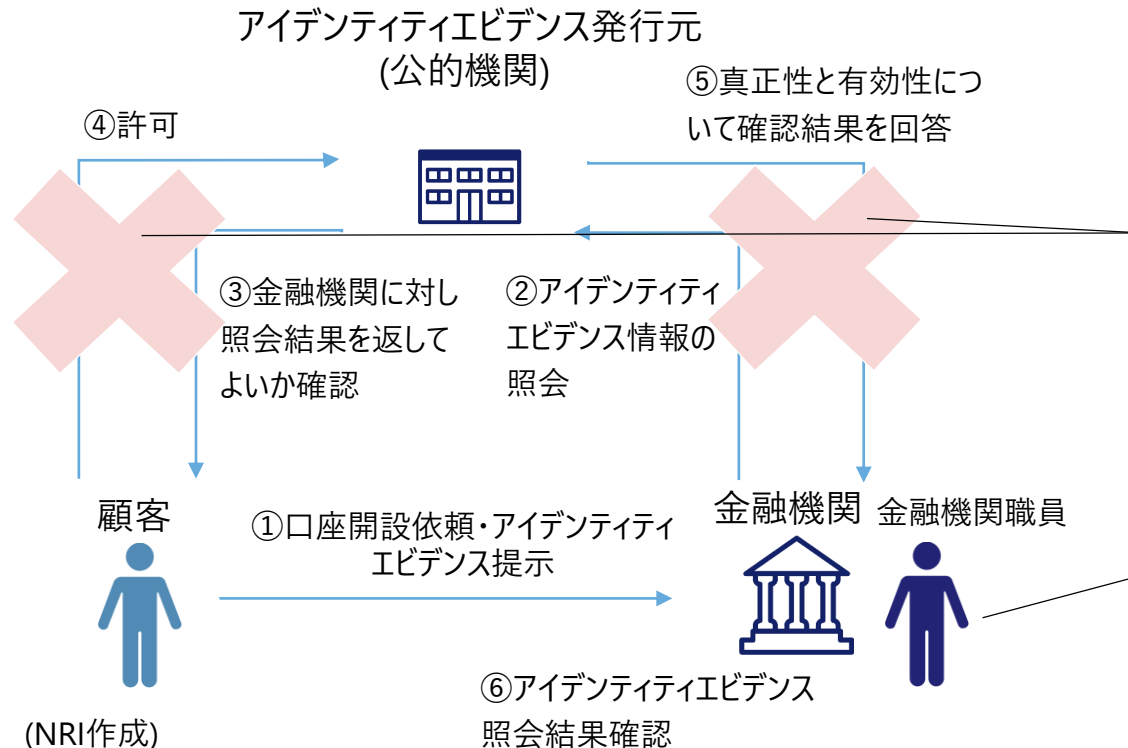
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 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）

# 【AML/CFT】アナログのアイデンティティエビデンスの検証困難性

- 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。
- なお、①の仕組みは、日本においても現状構築されていない。（次頁参照）

### 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（口座開設時）



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。  
 ・アイデンティティエビデンス発行元（公的機関）に対し、アイデンティティエビデンスの内容が正しくかつアイデンティティエビデンスが有効であることを確認する仕組みがない。

②ヒューマンエラーの可能性  
 ・アイデンティティエビデンスの偽造を目視等により検証しているため、担当者の主観的判断や経験不足による誤判定の可能性を排除できない。

(NRI作成)

## 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）

### 参考：日本の主要なアイデンティティエビデンスにおける真正性および有効性の検証状況

- 人の目に頼った真正性および有効性の検証が太宗である。
- なお、免許証とマイナンバーカードは、デジタルアイデンティティエビデンス（ICチップ情報等）の利用により真正性および有効性検証が機能的には可能だが、実務での活用拡大に関してはコスト面や運用面での課題が指摘されている。
  - 免許証はICチップに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みを使い真正性および有効性の検証が可能である。
  - 実務での活用に関しては、国内金融機関や有識者へのヒアリングにおいて、ICリーダーの準備コストや参照用暗証番号を忘れていた等、幅広い活用に向けた課題が意見として挙がっている。

#### 本邦におけるアイデンティティエビデンスの真正性および有効性検証可否

対面/ 非対面	アイデンティティエビデンス	真正性および有効性の検証状況	
		真正性	有効性
対面	免許証	○*1)	×
	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	○*2)	×
	免許証（ICチップ読み取り）	○*1)	×
	マイナンバーカード（ICチップ読み取り）	○	○*3)

\*1)犯罪収益等移転防止法第6条第1項第1号へ

○：IC等に保存されたデータを元に照合可能 ×：人の目で判断

\*2)犯罪収益等移転防止法第6条第1項第1号ホ

\*3)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



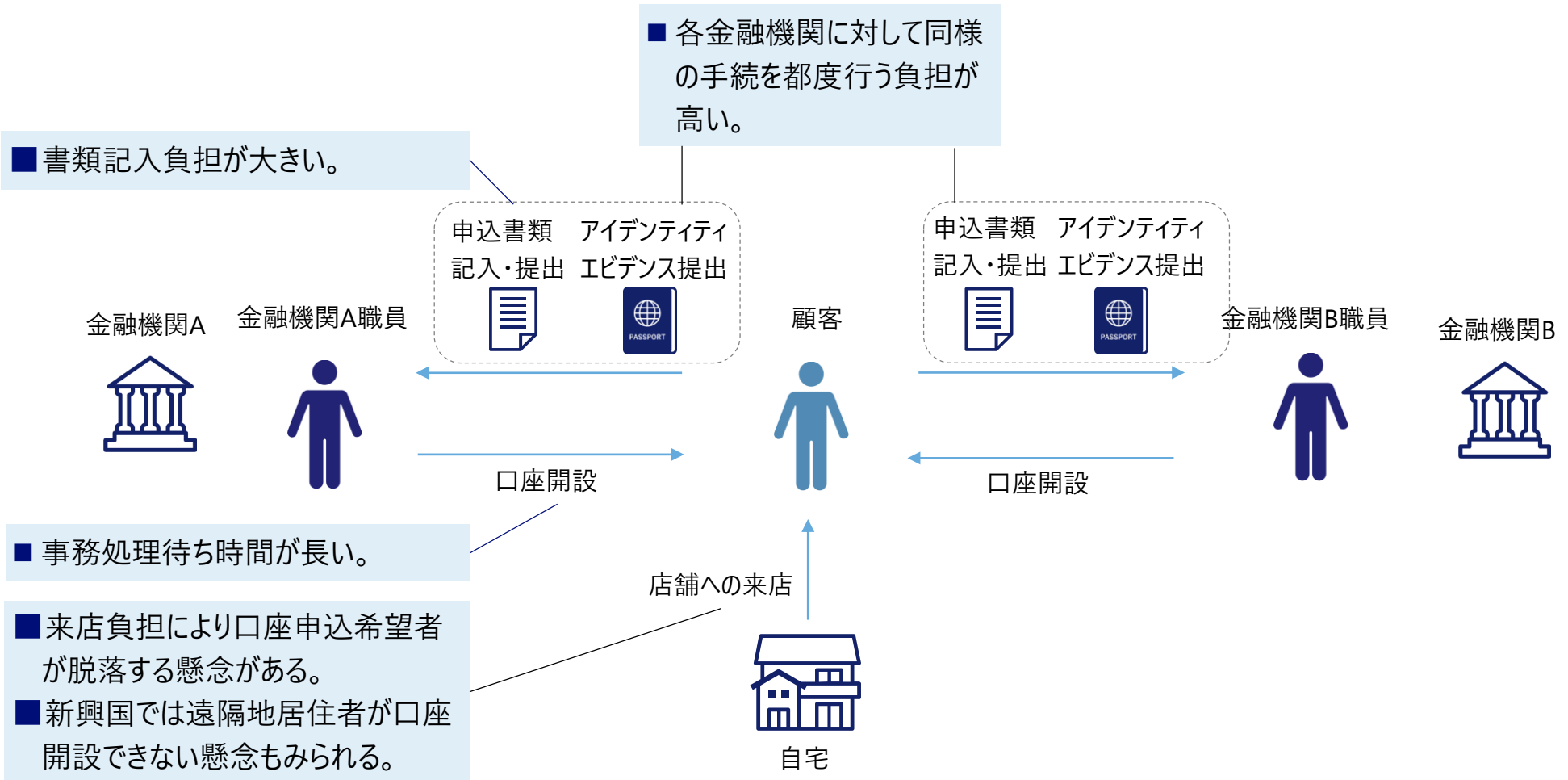
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 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）

# 【サービス向上】情報のアナログなやり取りに起因する顧客手続の諸課題

- 来店や書類記入等、顧客にとって様々な手続負担がある。

### 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

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

②継続的顧客管理 課題の概要

- AML/CFTにおける金融機関および顧客の事務負担等が挙げられる。
- 次頁以降で主要課題（下表ハイライト部分）について詳述する（その他の課題については補足資料参照）。

		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	・取引申請書類をデータ化する負担 <b>取</b>	・郵便物の返送手続負担 <b>定</b>				
	取引時確認	・大量の顧客に対する検証事務負担 <b>定</b>	・取引時のセキュリティリスク <b>取</b> (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						
	分析・評価	・アナログの顧客情報収集郵電費・データ化負担 <b>定</b>	<div style="border: 1px dashed gray; padding: 5px;">                     凡例  <table border="1" style="margin-left: 20px;"> <tr> <td><b>定</b></td> <td>…定期的顧客情報調査</td> </tr> <tr> <td><b>取</b></td> <td>…取引受付時確認</td> </tr> </table> </div>	<b>定</b>	…定期的顧客情報調査	<b>取</b>	…取引受付時確認
	<b>定</b>	…定期的顧客情報調査					
<b>取</b>	…取引受付時確認						
判断・対応							

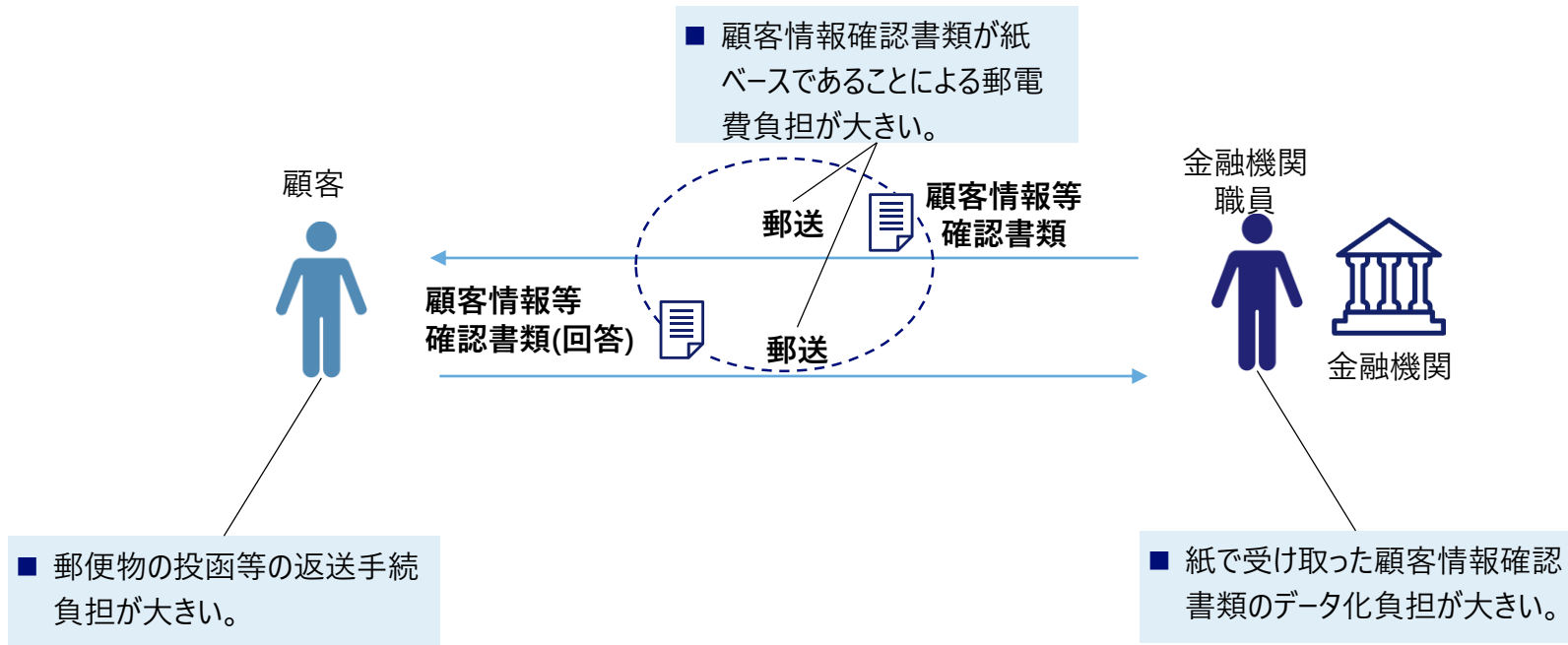
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-1-3. 対面・アナログIMSの主な課題 ②継続的顧客管理

### 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

- 定期的顧客情報調査においては、顧客と金融機関の間の書面によるやり取りに起因した事務負担やコスト負担の課題が発生している。

#### 定期的顧客情報調査における諸課題



	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

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

③アイデンティティ情報を活用したサービス提供 課題の概要

■ データ利活用にあたってのデータ集約に課題がある。次頁で詳述する。

		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		
	取引時確認		
	顧客フィルタリング		
	分析・評価	<ul style="list-style-type: none"> <li>複数サービス横断で顧客データを活用するための、データ利用許諾の整備負担</li> </ul>	<ul style="list-style-type: none"> <li>識別子の不一致によりデータ集約が困難               <ul style="list-style-type: none"> <li>部門/組織毎の管理により顧客識別子不一致</li> <li>他社データとの顧客識別子不一致</li> </ul> </li> <li>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</li> <li>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</li> </ul>
	判断・対応		

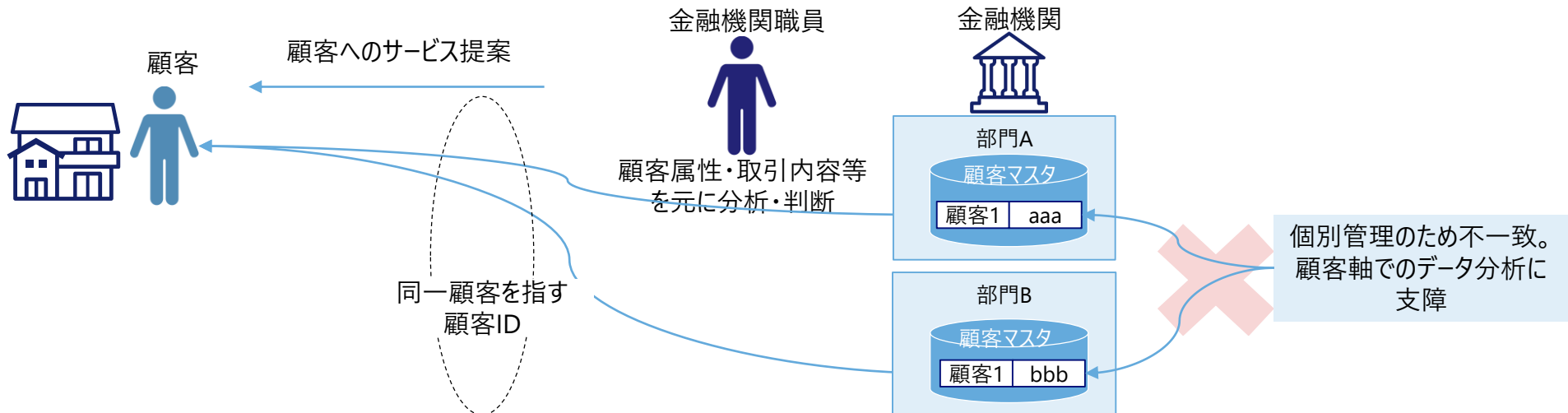
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

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

### 【サービス向上】顧客識別子やデータフォーマットが社内で不統一でありデータ利活用が困難

- 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であるとの指摘が国内金融機関実務者から上がっている。<sup>\*1)</sup>
  - 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という問題も有識者から指摘されている。<sup>\*2)</sup>
- 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。
- 関連する課題として、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等サービス毎になっている場合があり、その場合、顧客軸での横断的な分析にはデータ利用許諾の確認が必要なケースがあると考えられる。また、その際の不十分な顧客への説明により、顧客が顧客自身が望まないデータ利活用を懸念する可能性がある。

#### データ管理における顧客識別子の不整合



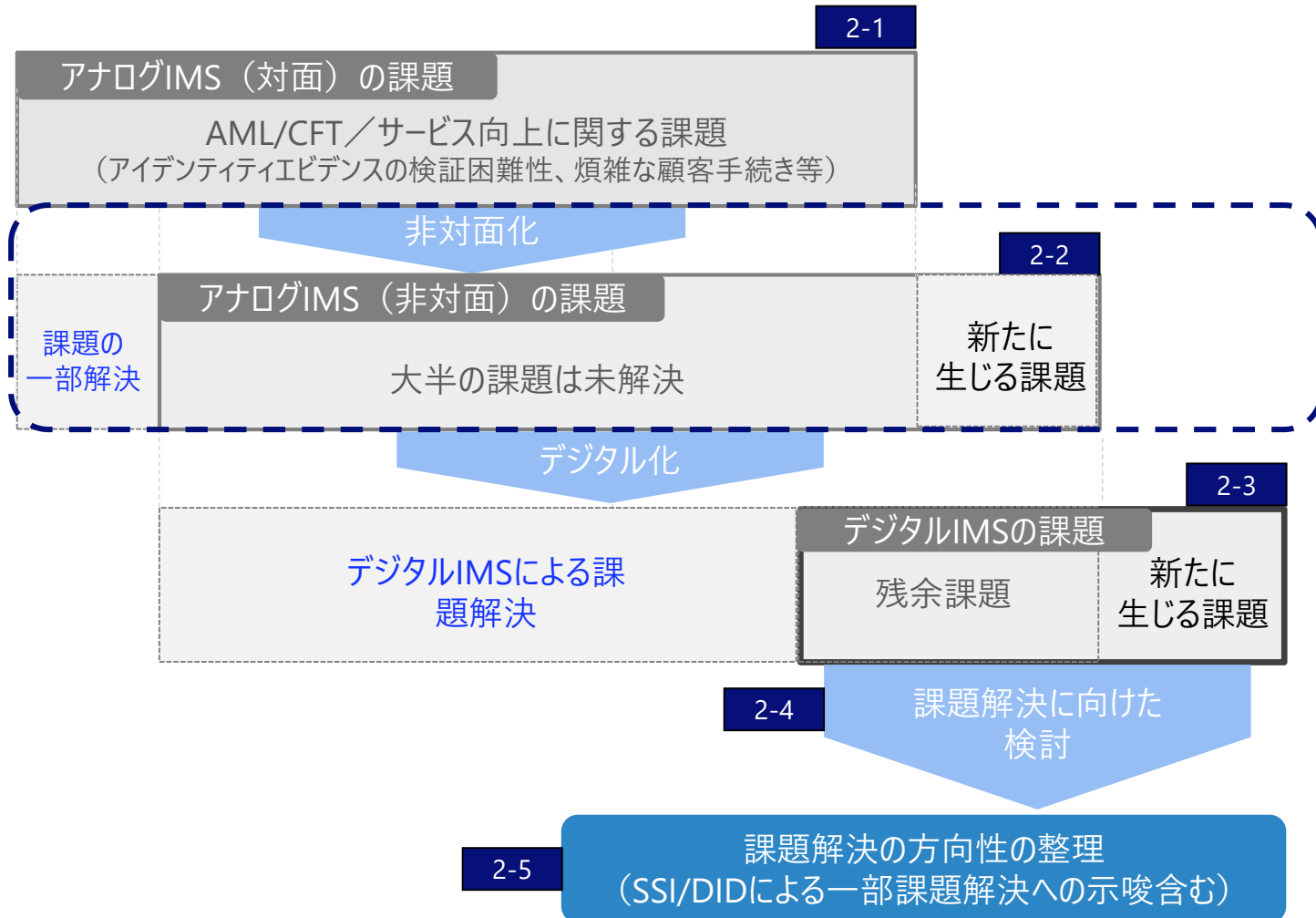
\*1)FINANCE FORUM 金融機関に求められるデータ利活用の実践より抜粋 <https://thefinance.jp/event/finance-forum-200528>

\*2)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>

## 2-2. onboardingプロセスの非対面化の進展

---

## 本節での議論対象



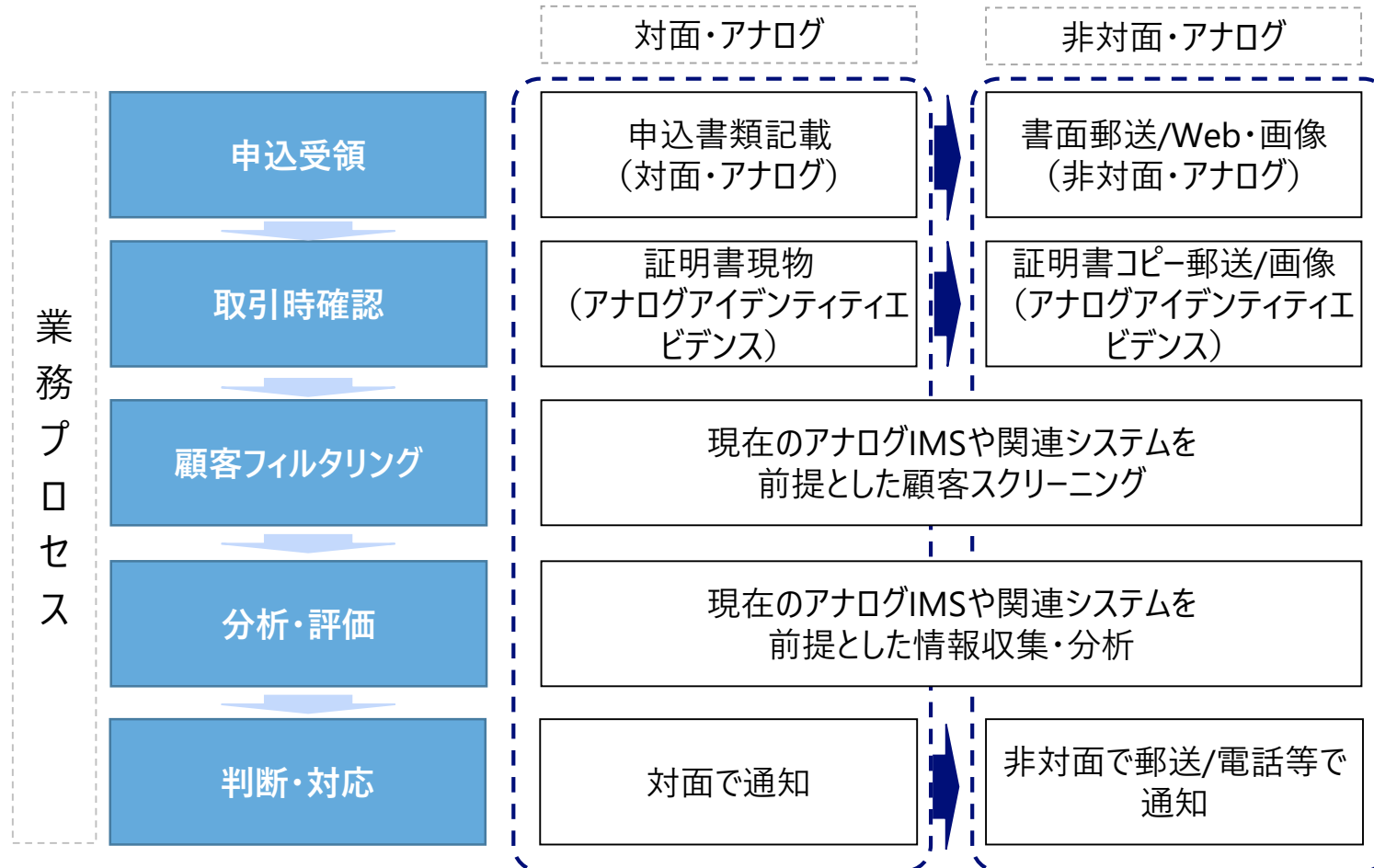
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-2-1. onboardingプロセスの非対面化の進展

# onboardingプロセスの非対面化の進展

- eKYC等のリモート・オンボーディング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の拡大に伴い、非対面化による課題解決の動きがみられる。

### 非対面化による業務プロセスの変化





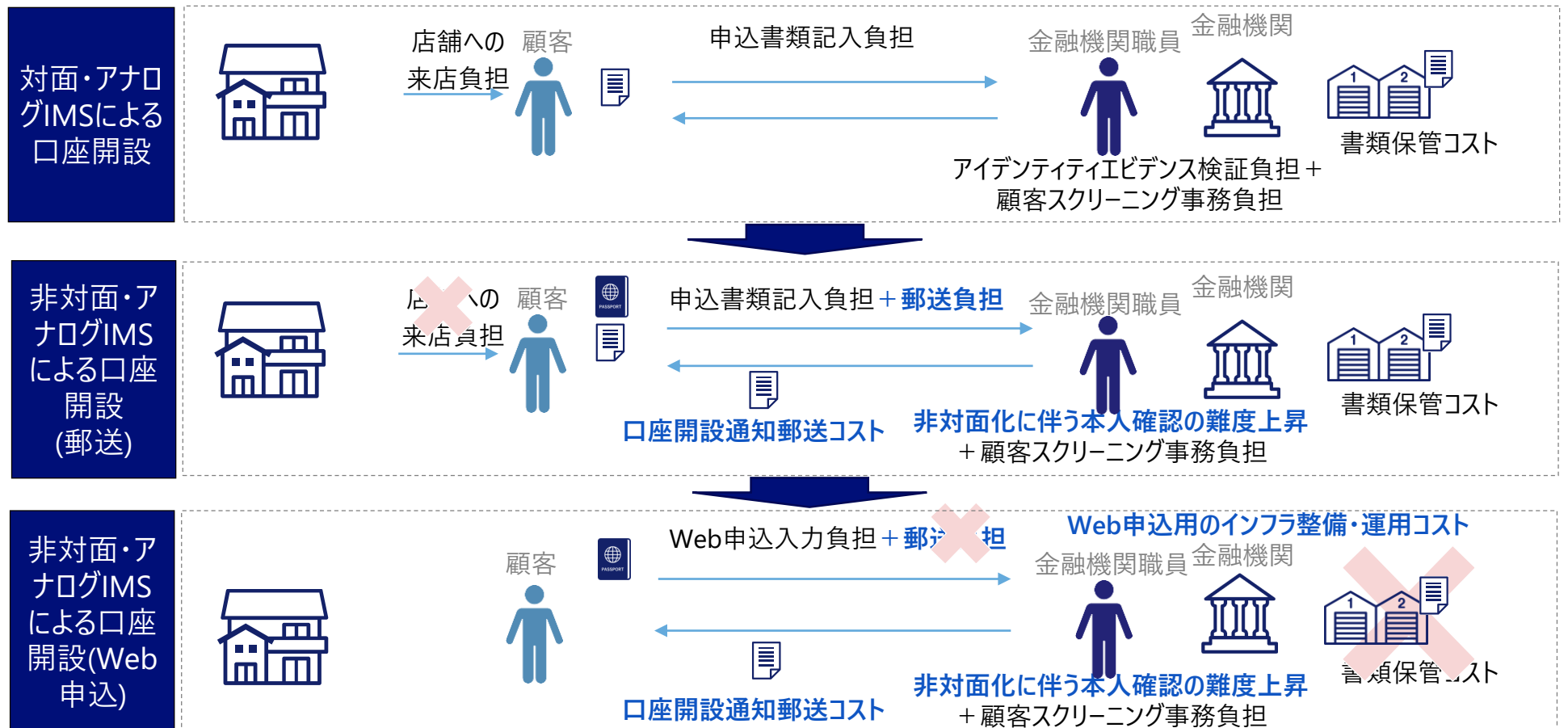
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-2-2. 非対面化による課題の一部解消

# 非対面化による対面・アナログIMSの課題の一部解消

- 顧客・金融機関の一部事務負担は削減されるが、非対面化に伴う本人確認の難度上昇や、本人所在確認のための口座開設郵送通知コスト、Web申込用のインフラ整備・運用コスト（Web申込に対応する場合のみ）が新たに発生している。

対面・アナログIMSの非対面化による課題の一部解消 ✖：解消される課題 ■：非対面化に伴い新たに発生する課題



	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

### 2-2-3. 非対面化後も残る課題

## 非対面化後も残る課題

- 非対面化後も、顧客の事務負担と金融機関の書類保管コスト以外の課題は解消されないまま残存するほか、本人確認の難度上昇等の新たな課題も発生している。
- 次頁以降で主要課題(下表ハイライト部分)について詳述する(その他の課題については補足資料参照)。

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	<ul style="list-style-type: none"> <li>・申込情報やアイデンティティエビデンス情報をデータ化する負担</li> <li>・Web申込用のインフラ整備・運用コスト</li> </ul>	<ul style="list-style-type: none"> <li>→新興国における遠隔地居住者の金融包摂</li> <li>→顧客の来店負担</li> <li>→顧客の書類記入負担→Web申込入力負担</li> <li>→顧客の事務処理待ち時間</li> <li>・金融機関毎に同様の口座開設申込を行う負担</li> </ul>
取引時確認	<ul style="list-style-type: none"> <li>・アナログ・アイデンティティエビデンスの検証困難性</li> <li>→オペレーショナルコスト(書類保管コスト)</li> <li>・他社で検証済の顧客を一から検証する負担</li> <li>・非対面化に伴う本人確認の難度上昇</li> </ul>	
顧客フィルタリング	<ul style="list-style-type: none"> <li>・他社で検証済の顧客を一から検証する負担</li> </ul>	
分析・評価		
判断・対応	<ul style="list-style-type: none"> <li>・所在確認のための口座開設通知郵送コスト</li> </ul>	

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-2-4. 非対面化により新たに発生する課題

### 【AML/CFT】非対面化に伴う本人確認の難度上昇

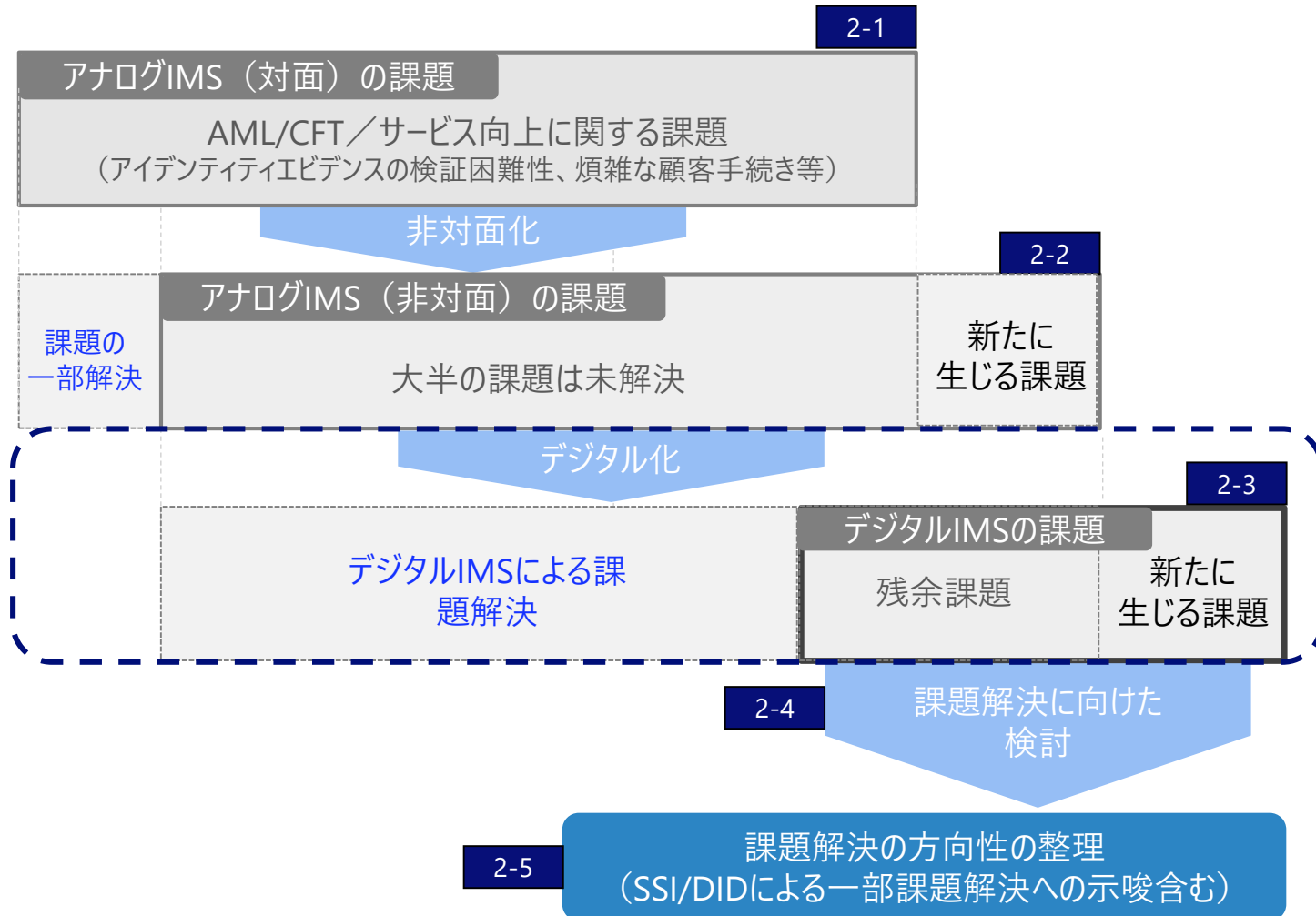
- 非対面取引は、対面取引と比較して、金融機関側が他人へのなりすましを看破する手段が限定されることから、本人確認の精度が低下するリスクを孕んでいる。
  - 取引の相手方と直に対面しないことで、性別、年代、容貌、言動等を直接確認することで容易に確認できる筈の情報を確認できないまま本人確認を行ってしまうことになる。これにより、本人特定事項の偽りや他人へのなりすましの有無を判断することが困難となる。
  - また、顧客本人ではなく、アイデンティティエビデンスの偽変造等についても認識することが難しい傾向がある。アイデンティティエビデンスのコピーにより本人確認を行う場合には、その手触りや質感を感知できない。
- 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、一般的には、非対面取引は対面取引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。犯罪収益移転危険度調査書<sup>\*1)</sup>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。

\*1) 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

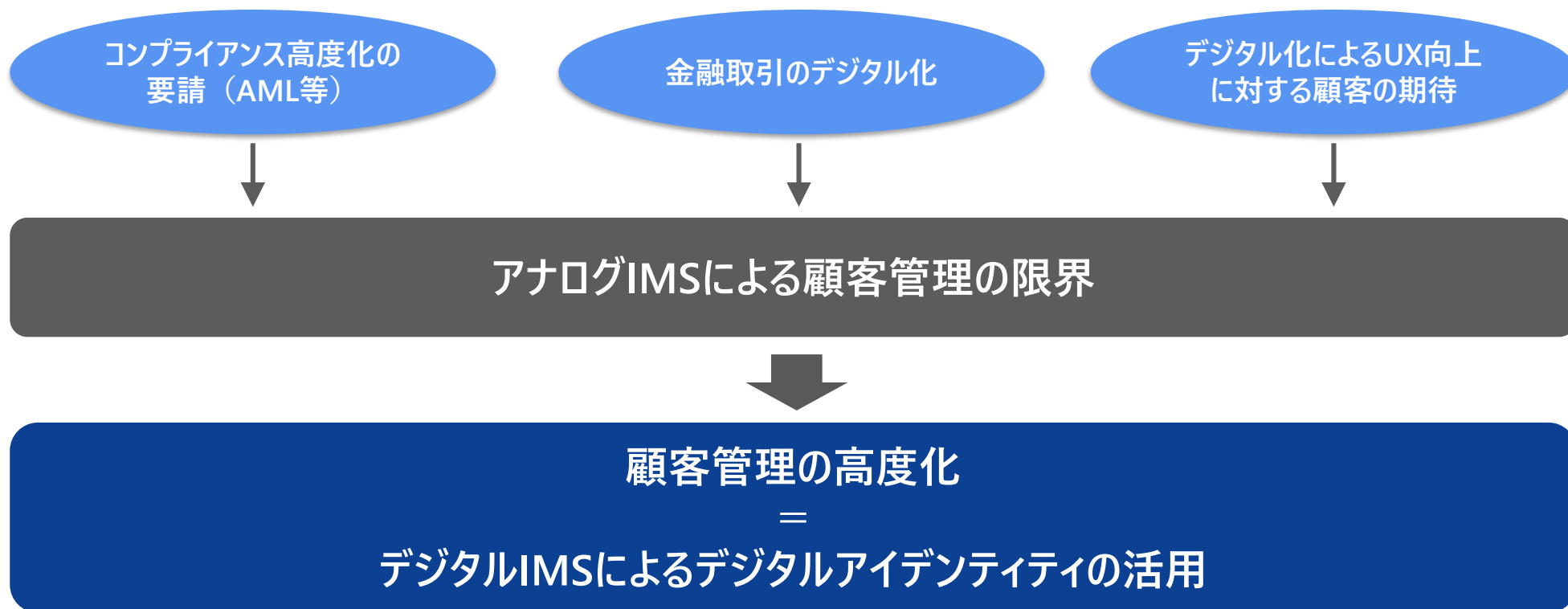
---

## 本節での議論対象



## 金融機関のデジタルアイデンティティ活用の重要性

- コロナ禍において社会全体のデジタルシフトが加速し、金融取引のデジタル化も急速に進展する中で、AML等のコンプライアンスの観点から、デジタル空間における本人性の確認がより重要になっている。
- 手続き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。
- 前節で整理した、金融機関が直面しているアナログIMSの課題解決として、デジタルIMSの活用が期待されている。



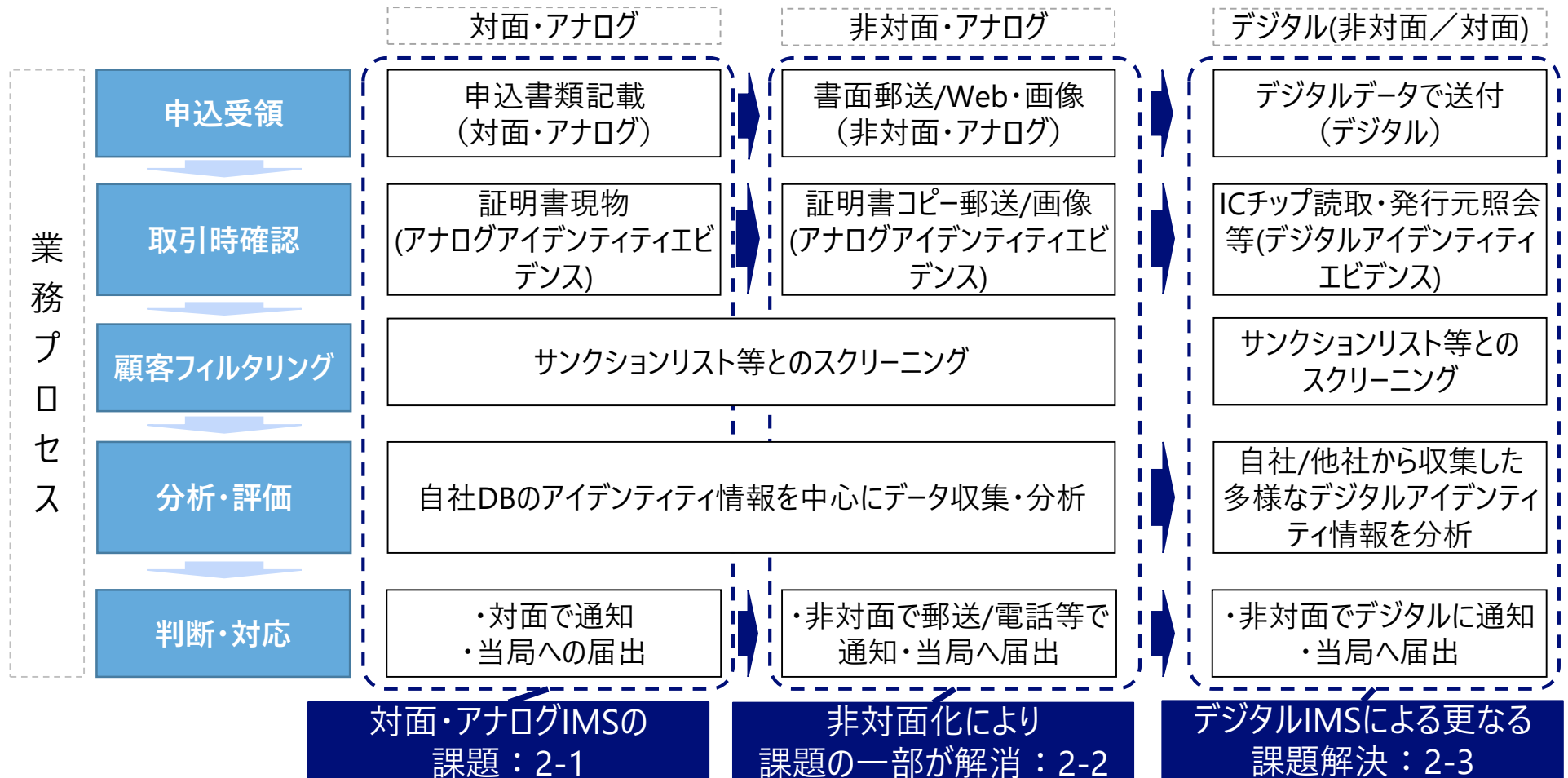
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 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

### IMSのデジタル化

- IMSのデジタル化：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を指す。  
(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)

デジタル化によるIMSの業務プロセスの変化



	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-3-2. 分析対象ユースケース

### 分析対象ユースケース

- 2-1-1の業務分類の単位でユースケースを設定して分析を行う。
- なお、onboardingプロセスについては、口座開設時のID連携が進むと想定し、  
（1-1）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。

#### 分析対象ユースケースの位置付け

#### 業務の実施タイミング

		onboarding	ongoing
業務の目的	AML/CFT規制対応	<p>①口座開設（取引時確認）</p> <p>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た口座開設</p> <p>➔</p> <p>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ティを用いたの口座開設</p>	<p>②継続的顧客管理</p> <p>ユースケース（2）</p>
	顧客サービスの向上	<p>（アイデンティティ登録前のため業務無し）</p>	<p>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</p> <p>ユースケース（3）</p>



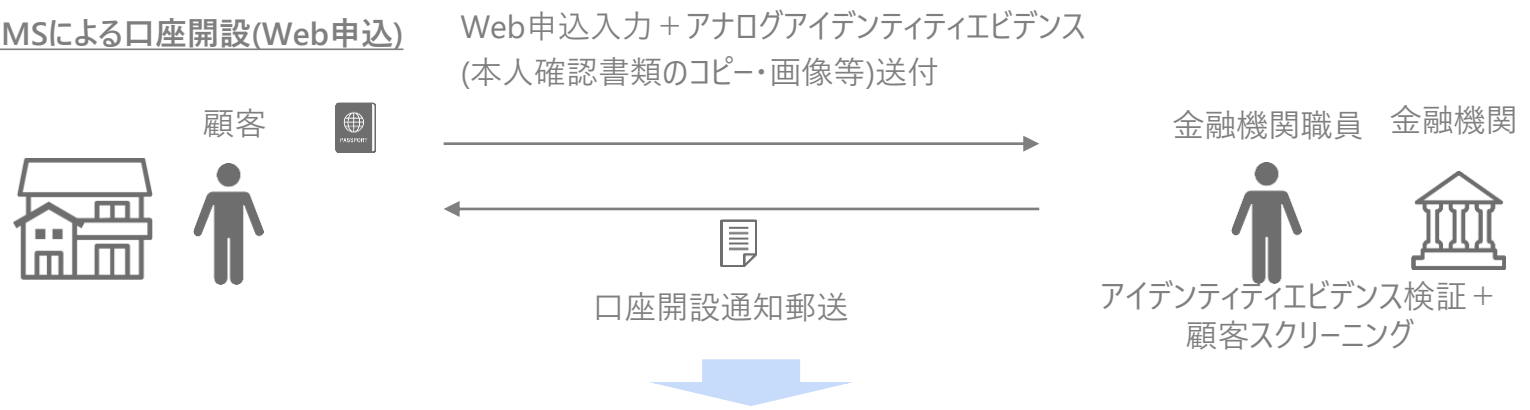
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-3-3. ユースケース分析 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た口座開設

### ユースケースの概要

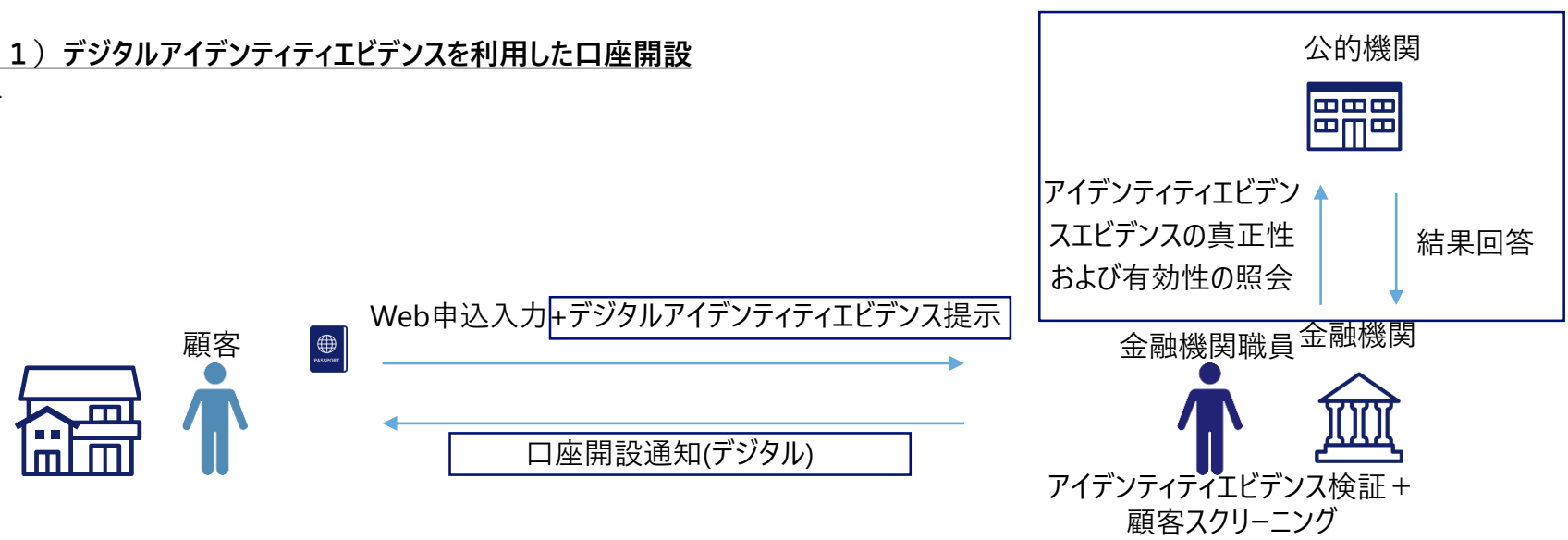
■ マシンリーダブルでデジタルに検証可能なアイデンティティエビデンスを用いて本人確認および口座開設処理を行う

#### 非対面・アナログIMSによる口座開設(Web申込)



#### 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た口座開設

\* 青枠が変更部分



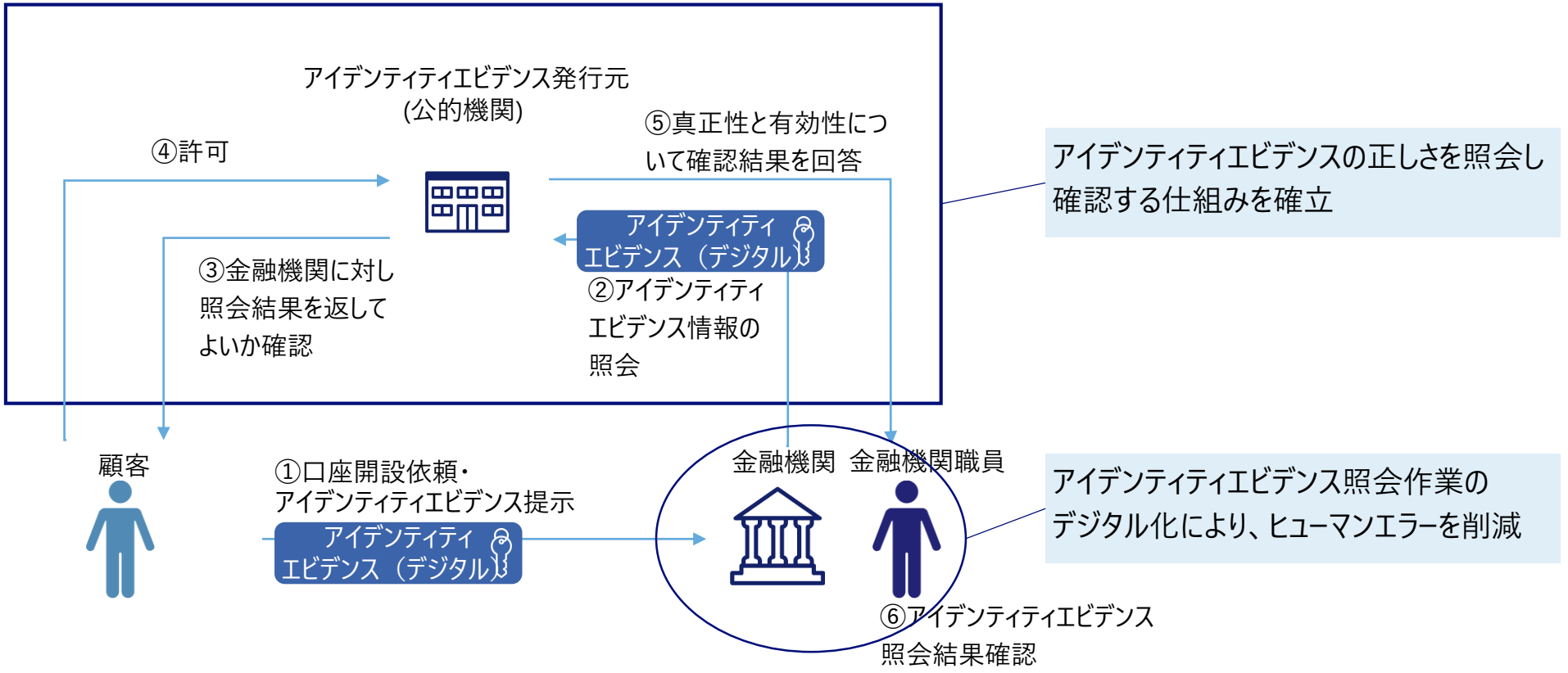
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

### 2-3-3. ユースケース分析 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

## デジタルIMSによる課題解決：アナログのアイデンティティエビデンスの検証困難性の解消

- 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活用により、アナログIMSにおけるアイデンティティエビデンスの検証困難性等諸課題が解消される。

デジタルIMSにおけるアイデンティティエビデンスの真正性および有効性を確認するフロー（口座開設時）



	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-3-3. ユースケース分析 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た口座開設 デジタルIMSによる課題解決：その他アナログIMSの諸課題の解決

### アナログIMSにおける口座開設時の課題

#### 非対面化に伴う本人確認の難度上昇

非対面取引は、対面と比較すると、他人へのなりすましを看破する手段が限定されるため、本人確認の精度が低下するリスクがある。

#### 所在確認のための口座開設通知郵送コスト

非対面口座開設実施時には、口座開設申込者の届出住所確認のために、転送不要郵便を送付し所在確認を行うため、郵送コスト負担が大きい。

### デジタルIMSによる解決策

- デジタルIMSによる真正性および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軽減される。
- 生体情報等とのバインドにより、提示されたアイデンティティエビデンスが口座開設を申し込んできた本人であることを確認する精度が向上し、なりすましリスクが軽減される。
- 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の住所を正として国民ID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。
- 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。

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

### 2-3-3. ユースケース分析 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た口座開設 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

- AML等規制対応の高度化や、口座開設申込における金融機関の省力化が図られる。
- 一方、デジタルIMSを活用した本人確認手法の整備等、新たな課題が発生する。
- 次頁以降で主要課題（下表ハイライト部分）について詳述する（その他の課題については補足資料参照）。

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

#### 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

		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	<ul style="list-style-type: none"> <li>アイデンティティエビデンス情報をデータ化する負担</li> <li>Web申込用のインフラ整備・運用コスト</li> </ul>	<ul style="list-style-type: none"> <li>Web申込入力負担</li> <li>金融機関毎に同様の口座開設申込を行う負担</li> <li>デジタル対応できない人物の金融排除</li> </ul>
	取引時確認	<ul style="list-style-type: none"> <li>アナログ・アイデンティティエビデンスの検証困難性</li> <li>他社で検証済の顧客を一から検証する負担</li> <li>非対面化に伴う本人確認の難度上昇</li> <li>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</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> </ul>
	顧客フィルタリング	<ul style="list-style-type: none"> <li>他社で検証済の顧客を一から確認する負担</li> </ul>	
	分析・評価		
	判断・対応	<ul style="list-style-type: none"> <li>所在確認のための口座開設通知郵送コスト</li> </ul>	

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-3-3. ユースケース分析 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た口座開設 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の整備（1 / 2）

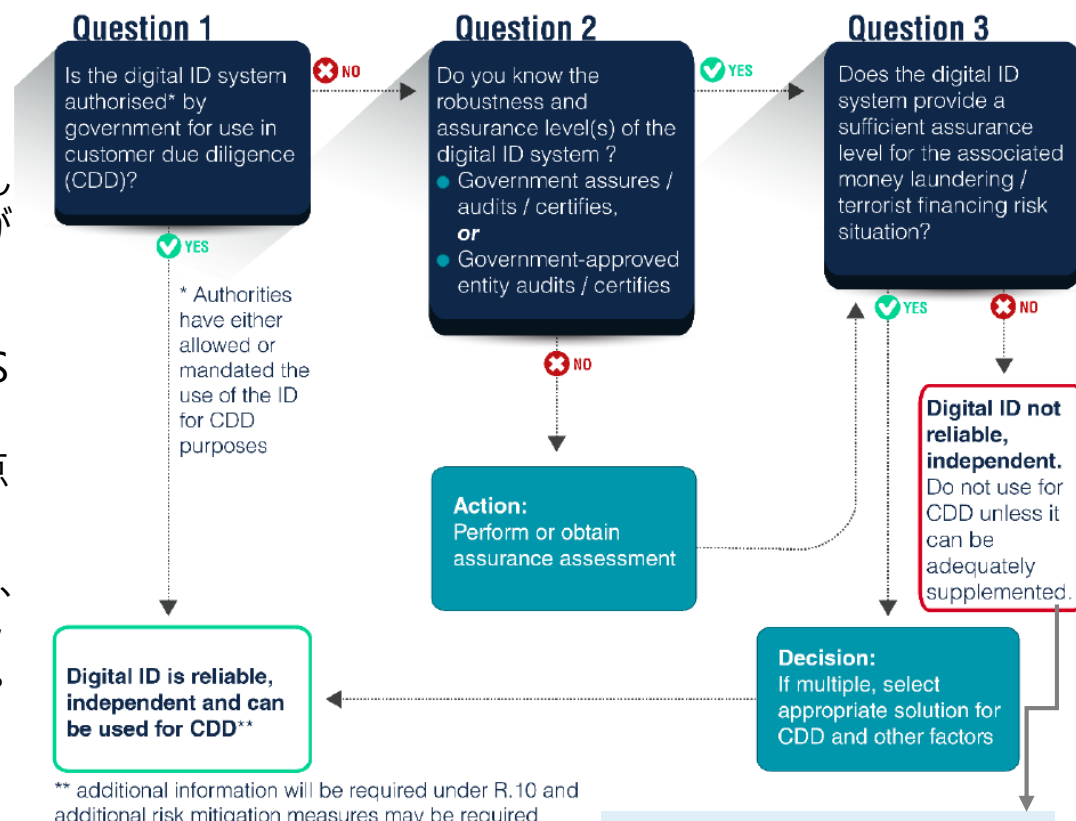
■ FATFは、規制目的に適したIAL（Identity Assurance Level）が担保されるよう、デジタルIMSの採否基準として以下を提唱している。

- ①政府により顧客管理への利用を許可されたもの  
または
- 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

■ 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への寄与する利点に言及している。

- 一般に高リスクに分類される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、標準的もしくは低リスクなレベルのリスクになる可能性がある\*1)。

FATFが提唱するAML/CFT目的でのデジタルIMSの採否決定プロセス\*1)



ML/FTの観点で十分なIALが確保できないデジタルIMSは顧客管理のために利用すべきではない。

\*1) GUIDANCE ON DIGITAL IDENTITY(Mar 2020)

<http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html>

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

### 2-3-3. ユースケース分析 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た口座開設

## 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の整備（2 / 2）

- 適切なIALの整備には、IALと本人確認規程との接合が重要であるが、現時点では、eIDが推奨されているEU（ドイツ）を除き、本人確認規定とIALとの接合は無い。
  - EUではonboardingプロセスへのeID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規則への準拠を前提として議論が進んでいる。
  - シンガポールは政府ID利用への統一化により、実質的にIALを均一化している。

	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POCA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	あり	一部あり (IRD)

※なお、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

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-3-3. ユースケース分析 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たの口座開設 （参考） 米国・EUのアイデンティティ保証フレームワーク

- 米国：NIST (米国立標準技術研究所) がSP-800-63A<sup>\*1</sup>)においてIAL、AALを規定している。
- EU：eIDASにてLoA (Levels of Assurance) を規定している。
- 米国・EUのように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。

### eIDASの本人確認時のLoA



LoA	Low	Substantial	High
登録時の対面申請	不要	不要	必要
アイデンティティ証跡の確認	有効な身分証明書は直接確認しない	認められた証跡に基づき、本人であることを確認	有効な身分証明書の保有を確認

\*1) CONFORMANCE CRITERIA for NIST SP 800-63A ENROLLMENT AND IDENTITY PROOFING and NIST SP 800-63B AUTHENTICATION AND LIFECYCLE MANAGEMENT [https://www.nist.gov/system/files/documents/2020/07/02/800-63A%20Conformance%20Criteria\\_0620.pdf](https://www.nist.gov/system/files/documents/2020/07/02/800-63A%20Conformance%20Criteria_0620.pdf)

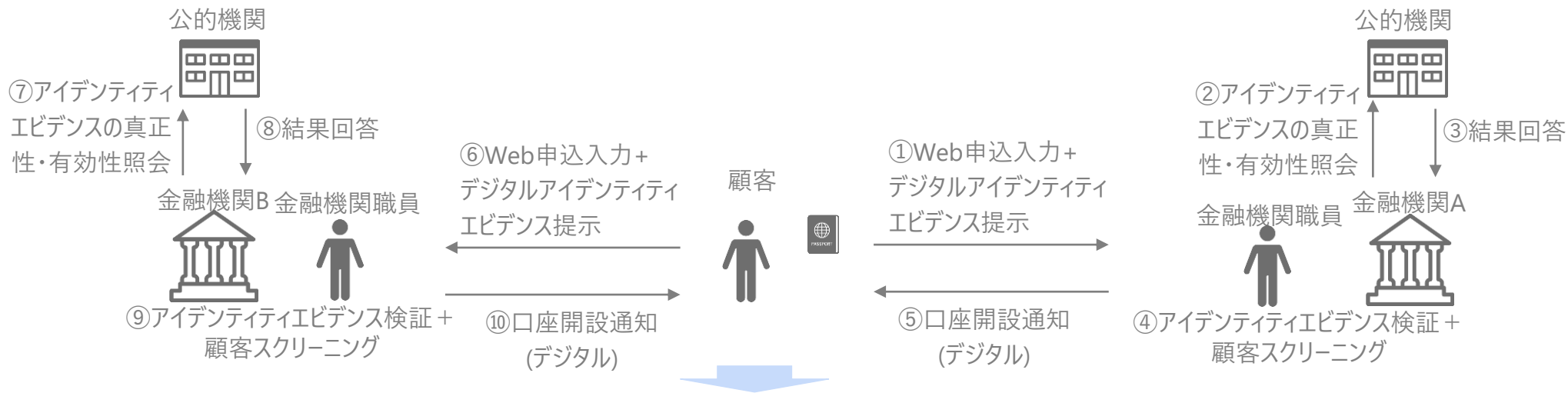
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

### 2-3-3. ユースケース分析 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ティを用いての口座開設

## ユースケースの概要

- 既存の金融機関口座のデジタルアイデンティティを用いて別の金融機関の新規口座を開設する。
- 顧客の口座開設負担軽減、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。

各金融機関に対して個別に口座開設を行う場合の事務フロー



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

\* 青枠が変更部分



注)顧客は金融機関Aに対して、各金融機関に個別に口座開設を行う場合と同じ事務フローで口座開設済



	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

### 2-3-3. ユースケース分析 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ティを用いての口座開設

## ユースケース(1-1)(自社のみ)からユースケース(1-2)(他社で作成したデジタル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

- 口座開設における金融機関・顧客双方の更なる省力化が図られる一方、当事者間の責任分界等の課題が発生する。
- 次頁以降で主要課題(下表ハイライト部分)について詳述する(その他の課題については補足資料参照)。

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

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

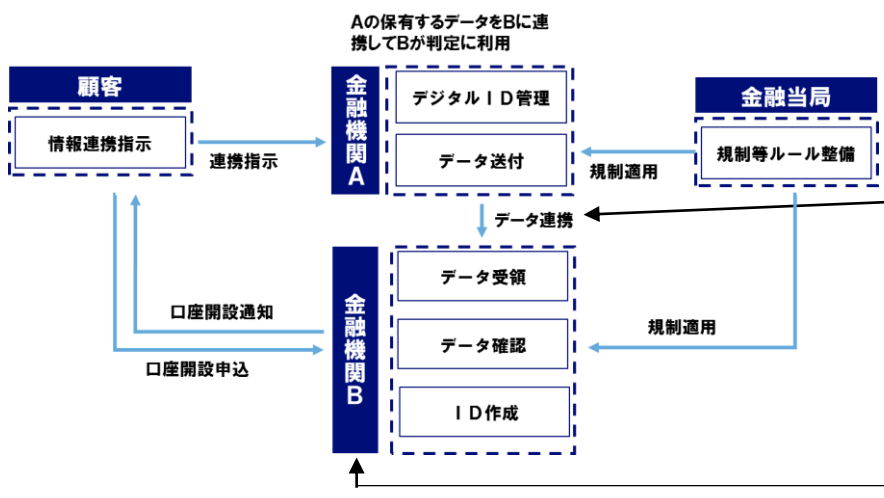
		AML/CFTに関する課題(金融機関/当局)	サービス向上に関する課題(顧客/金融機関)
業務プロセス	申込受領	<ul style="list-style-type: none"> <li>Web申込用のインフラ整備・運用コスト</li> <li>ID連携当事者間のビジネスモデル・責任分界の未整備</li> </ul>	<ul style="list-style-type: none"> <li>Web申込入力負担</li> <li>金融機関毎に同様の口座開設申込を行う負担</li> <li>デジタル対応できない人物の金融排除</li> <li>煩雑なID連携仕様への対応負担</li> <li>ID連携の同意管理負担</li> </ul>
	取引時確認	<ul style="list-style-type: none"> <li>他社で検証済の顧客を一から検証する負担</li> <li>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</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> <li>特定の金融機関(IdP)への依存リスクが高まる</li> </ul>
	顧客フィルタリング	<ul style="list-style-type: none"> <li>他社で検証済の顧客を一から検証する負担</li> </ul>	
	分析・評価		
	判断・対応		

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

### 2-3-3. ユースケース分析 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ティを用いての口座開設

## 【AML/CFT】ID連携当事者間のビジネスモデル・責任分界の整備にまつわる課題

- ID連携にあたっては当事者間の役割・責任を明らかにする必要があり、検討が必要な主な論点は下表の2点である。
- いずれにおいても、責任の範囲は当事者間でやり取りされる対価を考慮して検討されることが考えられる。



**【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	<ul style="list-style-type: none"> <li>・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)</li> <li>・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)</li> <li>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。</li> </ul>
2	金融機関B(IDの受け手)に責任	<ul style="list-style-type: none"> <li>・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)</li> <li>・金融機関AはID情報を参考情報として連携する。(責任小)</li> </ul>

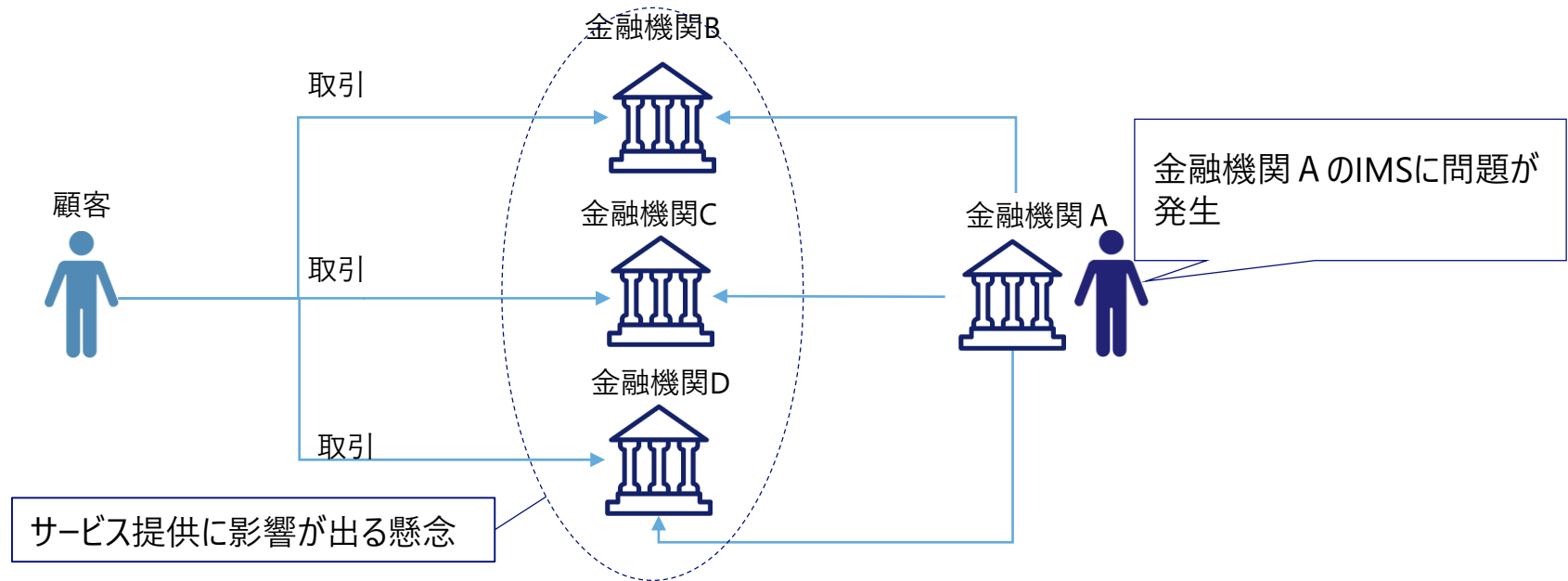
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

### 2-3-3. ユースケース分析 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ティを用いての口座開設

## 【サービス向上】特定の金融機関(IdP)への依存リスクが高まる

- 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場合、IDの出し手(下図金融機関A)に対する依存度が高まる可能性があり、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連携先の金融機関のサービスに影響が発生する。

IdPである金融機関に不具合が発生した場合の影響



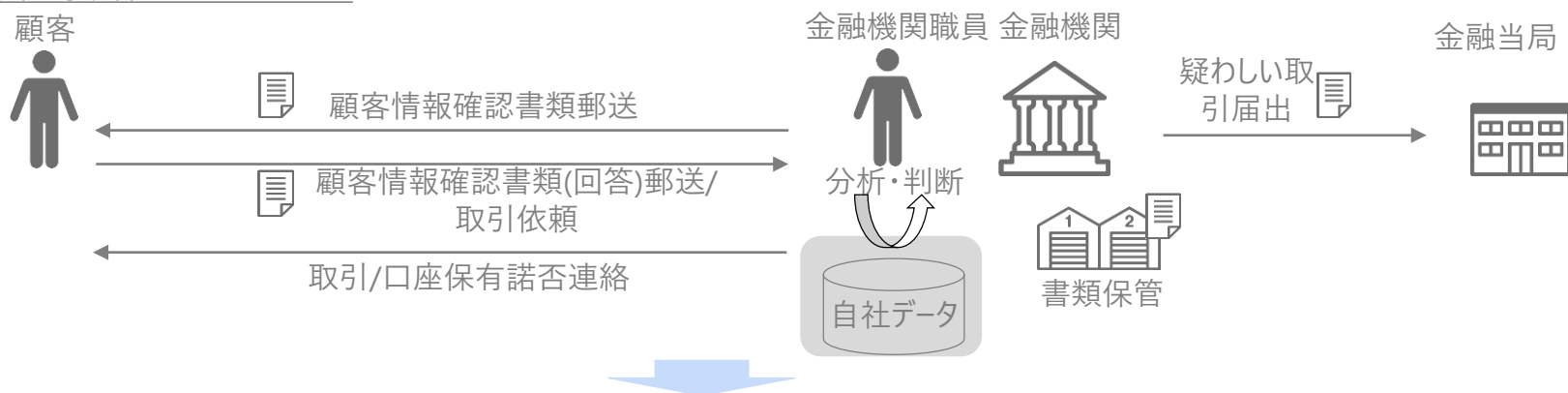
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-3-3. ユースケース分析 ユースケース（2）継続的顧客管理

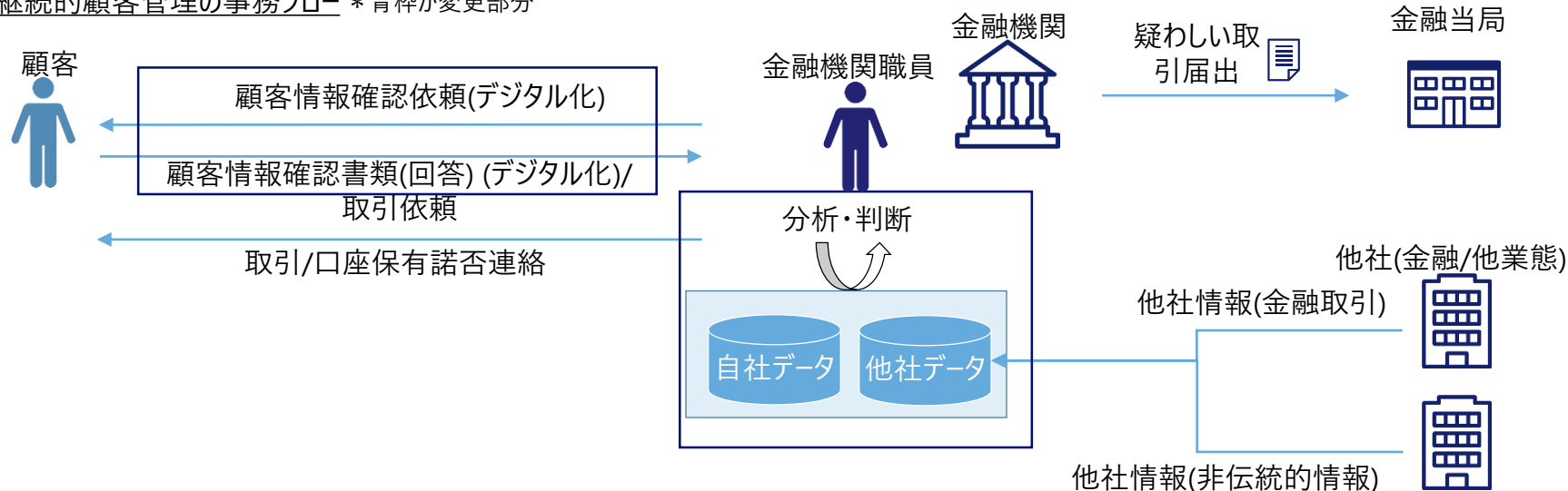
### ユースケースの概要

- デジタルIMS化により金融機関と顧客のやり取りがデジタル化され、金融機関・顧客双方の事務負担が削減される。
- デジタルIMS化により他社データを活用した分析の実施が現状より容易になることが期待される。

現在のアナログの継続的顧客管理の事務フロー



デジタル化された継続的顧客管理の事務フロー \* 青枠が変更部分



	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

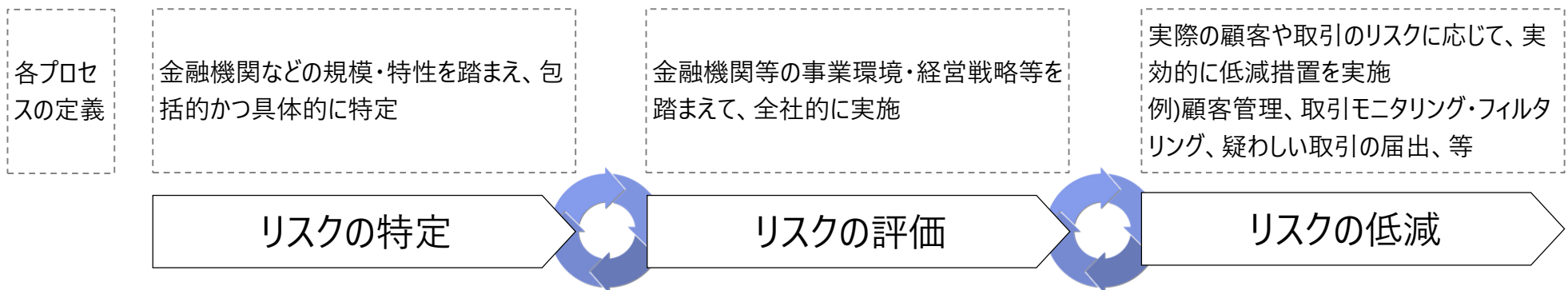
## 2-3-3. ユースケース分析 ユースケース（2）継続的顧客管理

# デジタルIMS化によるリスクベース・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\*1)。

- 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
  - ・ 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

### リスクベース・アプローチのプロセス概要



\*1) FATF Guidance on Digital Identity (March 2020)

<http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html>

### 2-3-3. ユースケース分析 ユースケース（2）継続的顧客管理

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 継続的顧客管理のデジタルIMS化により解消される課題と新たに発生する課題

- 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

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

		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	<ul style="list-style-type: none"> <li>取引申請書類をデータ化する負担 <b>取</b></li> </ul>	<ul style="list-style-type: none"> <li>郵便物の返送手続負担 <b>定</b></li> <li>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 <b>定 取</b></li> </ul>
	取引時確認	<ul style="list-style-type: none"> <li>大量の顧客に対する検証事務負担 <b>定</b></li> </ul>	<ul style="list-style-type: none"> <li>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） <b>取</b></li> </ul>
	顧客フィルタリング		
	分析・評価	<ul style="list-style-type: none"> <li>アナログの顧客情報収集郵電費・データ化負担 <b>定</b></li> <li>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 <b>定 取</b> (ユースケース(3)で詳述)</li> <li>情報の第三者提供に関して、データ受取側として、データ提供側への説明と確認の対応負担が大きい <b>定 取</b> (ユースケース(3)で詳述)</li> </ul>	
	判断・対応		

凡例

<b>定</b>	…定期的顧客情報調査
<b>取</b>	…取引受付時確認

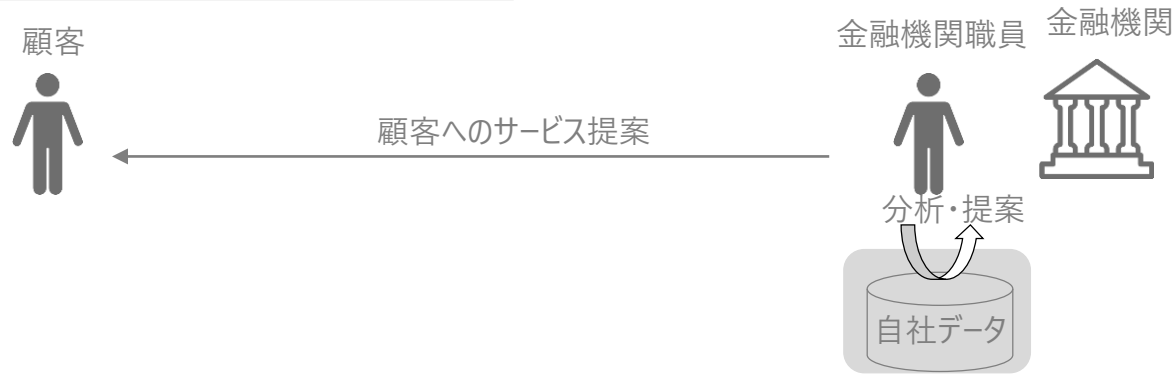
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

### 2-3-3. ユースケース分析 ユースケース（3）他社情報を活用したサービス提供

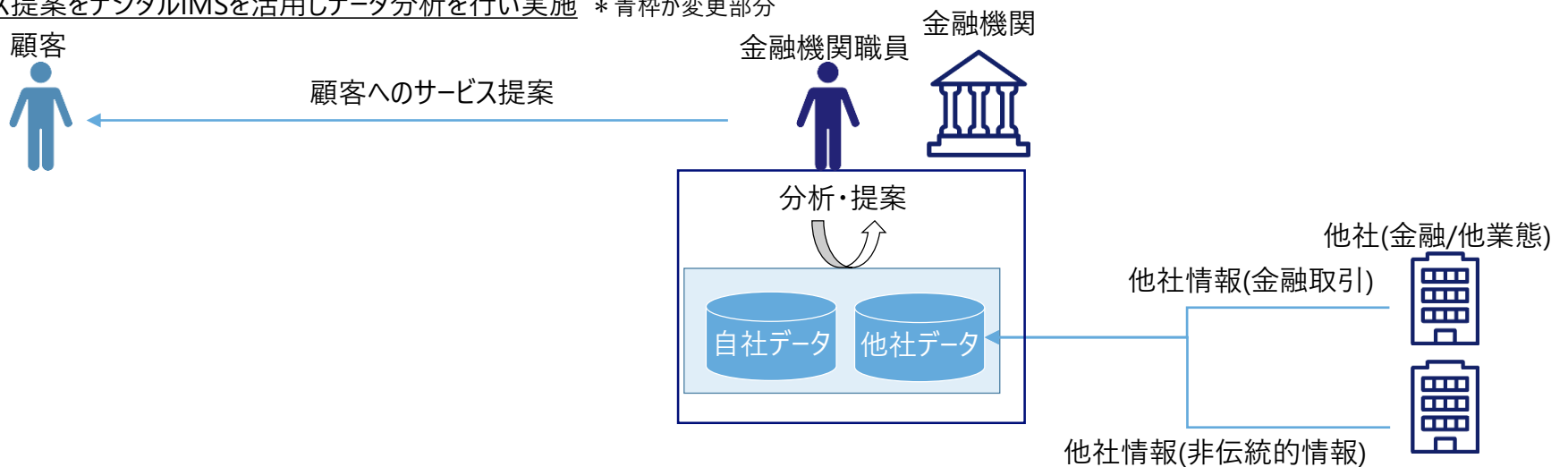
## ユースケースの概要

- 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イドサービスの提供等が期待される。

顧客へサービス提案を現在のアナログの業務を元を実施



顧客へサービス提案をデジタルIMSを活用しデータ分析を行い実施 \* 青枠が変更部分



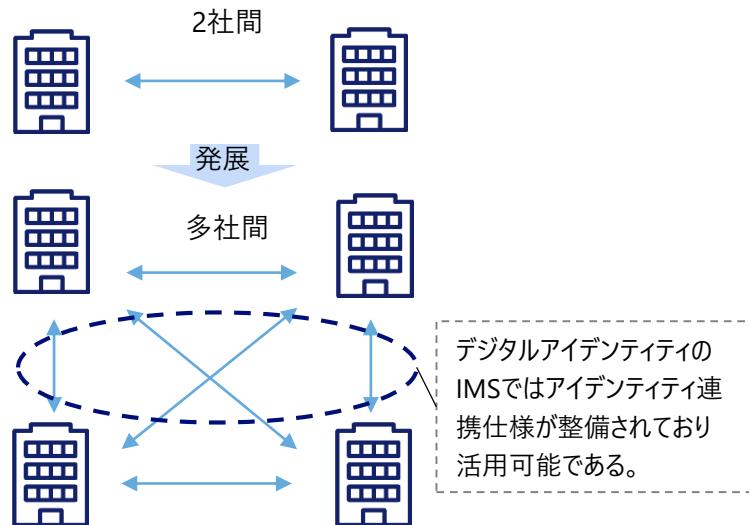
	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

### 2-3-3. ユースケース分析 ユースケース（3）他社情報を活用したサービス提供

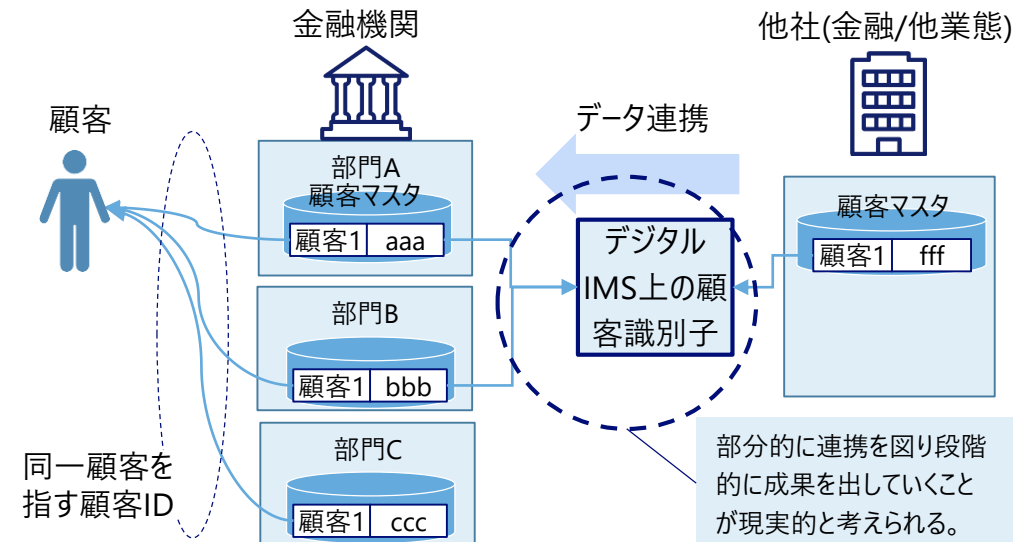
## デジタルIMSによる課題解決：顧客のアイデンティティ情報の部門間/会社間の紐づけ

- 社内の各部門のDBが持つ顧客のアイデンティティ情報や他社が持つ顧客のアイデンティティ情報を、デジタルIMS上の共通の顧客識別子に紐づけて管理することで、社内でのデータ利活用の促進が期待される。
  - 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、2-1-4.で言及したように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、業務や利用目的に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。
- 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。

アイデンティティ連携の発展イメージとアイデンティティ連携仕様の活用



デジタルIMSを活用した顧客アイデンティティ情報の紐づけイメージ





## 2-3-3. ユースケース分析 ユースケース（3）他社情報を活用したサービス提供

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

### 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

- 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。
- 次頁以降で主要課題(下表ハイライト部分)について詳述する(その他の課題については補足資料参照)。

#### 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

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	<ul style="list-style-type: none"> <li>・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</li> <li>・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</li> <li>・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</li> </ul>	<ul style="list-style-type: none"> <li>・識別子の不一致によりデータ集約が困難</li> <li>・一部門/組織毎の管理により顧客識別子不一致</li> <li>・他社データとの顧客識別子不一致</li> <li>・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</li> <li>・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</li> </ul>
判断・対応			

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-3-3. ユースケース分析 ユースケース（3）他社情報を活用したサービス提供

### 【サービス向上】他社情報の活用に関する諸課題

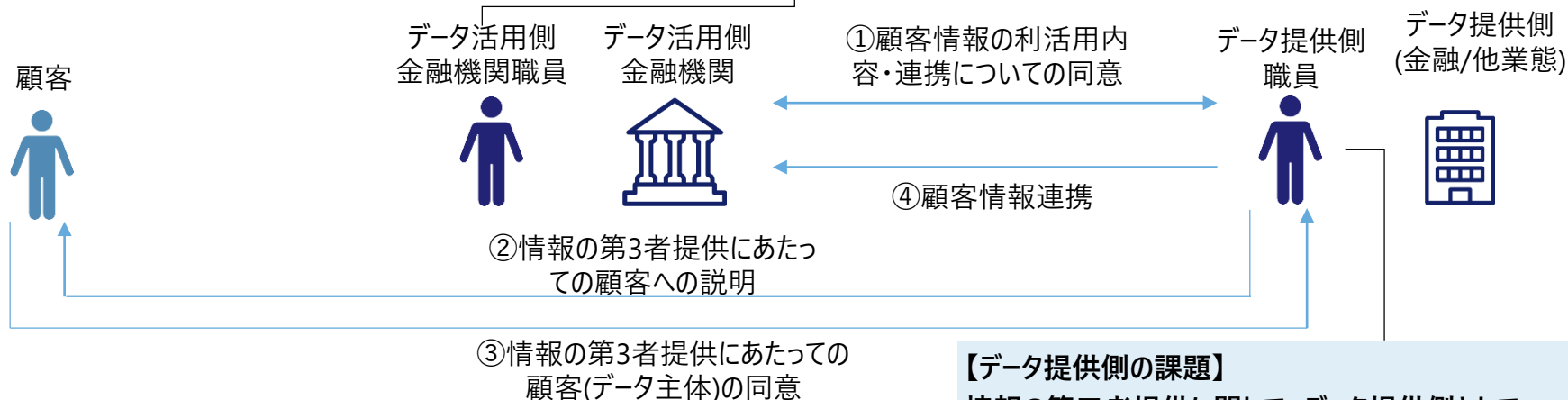
- データ利活用が企業を跨いで行われるようになると、複数サービス横断で顧客データを利活用するためのサービス利用許諾整備負担に加え、データ提供側/データ利活用側双方に、情報の第三者提供に関する対応負担が発生する。

#### 情報の第三者提供における顧客からの同意取得フローと課題

##### 【データ活用側の課題】

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

- データ提供者側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



##### 【データ提供側の課題】

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

- 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

## 2-3-4. その他技術的課題

### その他技術的課題

- 以降では、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を挙げる。

課題分類	課題の概要	課題の詳細
サイバー セキュリティ ・データ セキュリティ	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プロバイダーがデジタル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。 <sup>*1)</sup>
	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。 <sup>*2)*3)</sup>
	Authoritative Sourceの突然死	身元確認が第三者によって実施される場合、Authoritative Source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。 <sup>*4)</sup>
	インサイダーの脅威	IDプロバイダーがデジタル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プロバイダー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。 <sup>*1)</sup>
	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、何らかの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。 <sup>*4)*5)</sup>

\*参考文献は次頁にまとめて記載

## 2-3-4. その他技術的課題

### その他技術的課題

課題分類	課題の概要	課題の詳細
認証 ・認可	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。 <sup>*4)</sup>
	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。 <sup>*2)*3)</sup>

\*1) 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](https://www.iif.com/Portals/0/Files/content/Innovation/10142019_responsible_digital_ids.pdf)

\*2) Guidance on Digital Identity (March 2020) <http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html>

\*3) OIX The value of digital identity to the financial service sector (Dec 2016) <https://openidentityexchange.org/networks/87/item.html?id=202>

\*4) 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](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)

\*5) 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](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)

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-3-5. 金融機関からのデータ参照先に関する課題

# 【AML/CFT】法人の実質的支配者確認に関する課題をめぐる動向

- 国内金融機関に対するヒアリングにおいても、法人実質的支配者の確認負担が高いという意見が出ている。
- 現状、FATFは、2019年10月公表の「best-practices-beneficial-ownership-legal-persons」\*1)において、FATFの相互審査で示された各国の実情を鑑みると、実質的支配者確認において、複数の情報(下表参照)を組み合わせる手法を推奨しており、確認負担自体はやむを得ない側面もある。
- 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。

### FATFが推奨する実質的支配者情報収集のアプローチ\*2)

No.	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*3) 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

\*1)FATF, best-practices-beneficial-ownership-legal-persons, Oct 2019

<https://www.fatf-gafi.org/media/fatf/documents/Best-Practices-Beneficial-Ownership-Legal-Persons.pdf>

\*2)\*1)を元にNRI作成

\*3) 指定非金融業者及び職業専門家 (Designated non-financial businesses and professions)

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-3-5. 金融機関からのデータ参照先に関する課題

# 【AML/CFT】法人の実質的支配者確認に関する課題をめぐる動向

- 前頁の課題に対し、各国で制度の整備等が検討されている。例えば、日本では以下の検討が進んでいる。
  - 法務省民事局で、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）
    - ・ 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。

### 法人の実質的支配者（BO）把握の要請

#### ○ FATFの要請

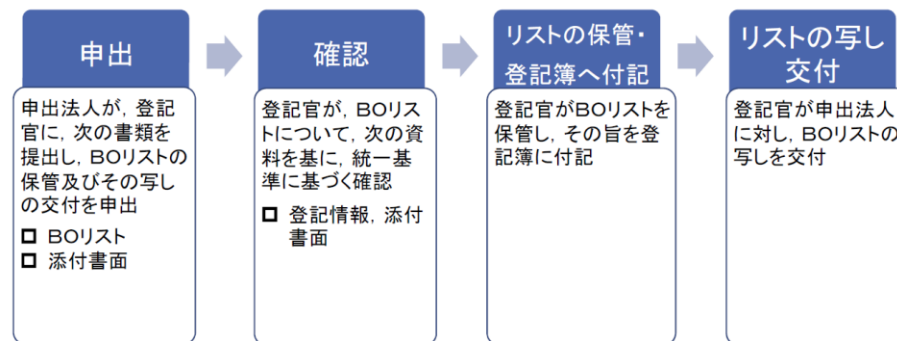
- ・ 勧告10「顧客管理」（金融機関による実質的支配者の確認・照合等）及び勧告24「法人の透明性及び真の受益者」（権限ある当局が適時に正確かつ時宜を得た情報を入手）
- ・ 2019年10月公表のFATFのベストプラクティスでは、複数の情報（Registry Approach, the Company Approach and the Existing Information Approach）を組み合わせる手法を推奨。また、我が国の公証人の行う定款認証における株式会社等の実質的支配者（BO）の申告制度をベストプラクティスとして紹介

- ・ 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

#### ○ 国内的要請

- ・ 全国銀行協会の行った加盟行へのアンケートの結果  
⇒ 設立後のBO情報の更新、集めたBO情報への金融機関からのアクセス、BO情報の登記事項へ追加等

### BOリストの保管及びその写しの交付フロー



	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-3-5. 金融機関からのデータ参照先に関する課題

### 【AML/CFT】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<sup>\*1)</sup>の第一次報告書<sup>\*2)</sup>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。
- 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<sup>\*3)</sup>
  - ⇒ 以上から、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基準およびその他の規制・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(各国のデータ保護法制等)、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<sup>\*2)</sup>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。

\*1) 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

\*2) FSB, Enhancing Cross-border Payments Stage 1 report to the G20, Apr 2020 <https://www.fsb.org/wp-content/uploads/P090420-1.pdf>

\*3) 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](https://www.fsa.go.jp/frtc/kikou/2020/FSA_article_ACAMSToday2020_Sept-Nov.pdf)

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-3-5. 金融機関からのデータ参照先に関する課題

# 【AML/CFT】クロスボーダー取引の諸課題をめぐる動向

### ■ 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。<sup>\*1)</sup>
- 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。

### 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<sup>\*1)</sup>

#### フォーカスエリアE：新しい決済インフラ等の潜在的な役割の模索

- BB17：新たな多面的プラットフォームの実現可能性検討
- BB18：グローバルステーブルコインの健全性促進
- BB19：国際性を持たせたCBDC設計

#### フォーカスエリアD：データの質の向上およびSTP化の促進

- BB14：メッセージフォーマットとしてISO 20022の統一版の採用
- BB15：データ交換のためのAPIプロトコルの調整
- BB16：プロキシ登録による一意識別子の確立



#### フォーカスエリアA：クロスボーダー送金の改善に向けた官民共同コミットメントの構築

- BB1：共通ビジョン・目標の策定
- BB2：国際的ガイダンス・原則の履行
- BB3：海外送金サービスレベルの共通基準設定

#### フォーカスエリアB：規制・監督・オーバーサイト枠組みの調和

- BB4：規制・監督・監視の枠組み調整
- BB5：AML/CFT規制の一貫かつ包括的な適用
- BB6：データフレームワークの見直し
- BB7：安全な送金コリドーの促進
- BB8：KYCおよびID情報の共有促進

#### フォーカスエリアC：クロスボーダー送金市場のニーズに応じた既存の決済インフラ等の改善

- BB9：PvP決済の促進
- BB10：決済システムへの（直接）アクセス改善
- BB11：（中銀間の）互恵的な流動性供給手続きの模索
- BB12：（主要な決済システムの）稼働時間延長
- BB13：決済システム間の相互接続推進

<sup>\*1)</sup> 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>



	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## 2-3-6. デジタルIMS化により解決されるアナログIMSの課題 ユースケース分析結果まとめ

# デジタルIMS化により解決されるアナログIMSの課題 ユースケース分析結果まとめ

- アイデンティティエビデンスの検証負担等、事務負担の課題が多数解消されている。
- 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	<ul style="list-style-type: none"> <li>→アイデンティティエビデンス情報をデータ化する負担</li> <li>・Web申込用のインフラ整備・運用コスト</li> </ul>	<ul style="list-style-type: none"> <li>・Web申込入力負担</li> <li>→金融機関毎に同様の口座開設申込を行う負担</li> <li>→郵便物の返送手続負担</li> </ul>
取引時確認	<ul style="list-style-type: none"> <li>→アナログ・アイデンティティエビデンスの検証困難性</li> <li>→他社で検証済の顧客を一から検証する負担</li> <li>→非対面化に伴う本人確認の難度上昇</li> <li>→大量の顧客に対する検証負担</li> </ul>	<ul style="list-style-type: none"> <li>→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)</li> </ul>
顧客フィルタリング	<ul style="list-style-type: none"> <li>→他社で検証済の顧客を一から検証する負担</li> </ul>	
分析・評価	<ul style="list-style-type: none"> <li>→アナログの顧客情報収集郵電費・データ化負担</li> <li>→自社データのみを利用した犯罪検知の限界</li> <li>・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</li> </ul>	<ul style="list-style-type: none"> <li>→識別子の不一致によりデータ集約が困難</li> <li>→部門/組織毎の管理により顧客識別子不一致</li> <li>→他社データとの顧客識別子不一致</li> <li>・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</li> <li>・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</li> </ul>
判断・対応	<ul style="list-style-type: none"> <li>→所在確認のための口座開設通知郵送コスト</li> </ul>	

	onboarding	ongoing
AML	①口座開設	②継続的管理
サービス		③サービス提供

## デジタルIMS化により新たに発生する課題 ユースケース分析結果まとめ

■ デジタルIMS化により、以下の課題が新たに発生する。

		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	<ul style="list-style-type: none"> <li>ID連携当事者間のビジネスモデル・責任分界の未整備</li> </ul>	<ul style="list-style-type: none"> <li>デジタル対応できない人物の金融排除</li> <li>煩雑なID連携仕様への対応負担</li> <li>ID連携の同意管理負担</li> <li>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</li> </ul>
	取引時確認	<ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> <li>特定の金融機関(IdP)への依存リスクが高まる</li> </ul>
	顧客フィルタリング		
	分析・評価	<ul style="list-style-type: none"> <li>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</li> <li>情報の第三者提供に関して、データ受取側として、データ提供側への説明と確認の対応負担が大きい</li> </ul>	
	判断・対応		

## 2-3-8. 課題まとめ

# 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

- 課題は、下表の9つの観点に整理される。
- なお、8) 9) は、本調査においては課題の提示にとどめ、次節以降の記載は割愛する。

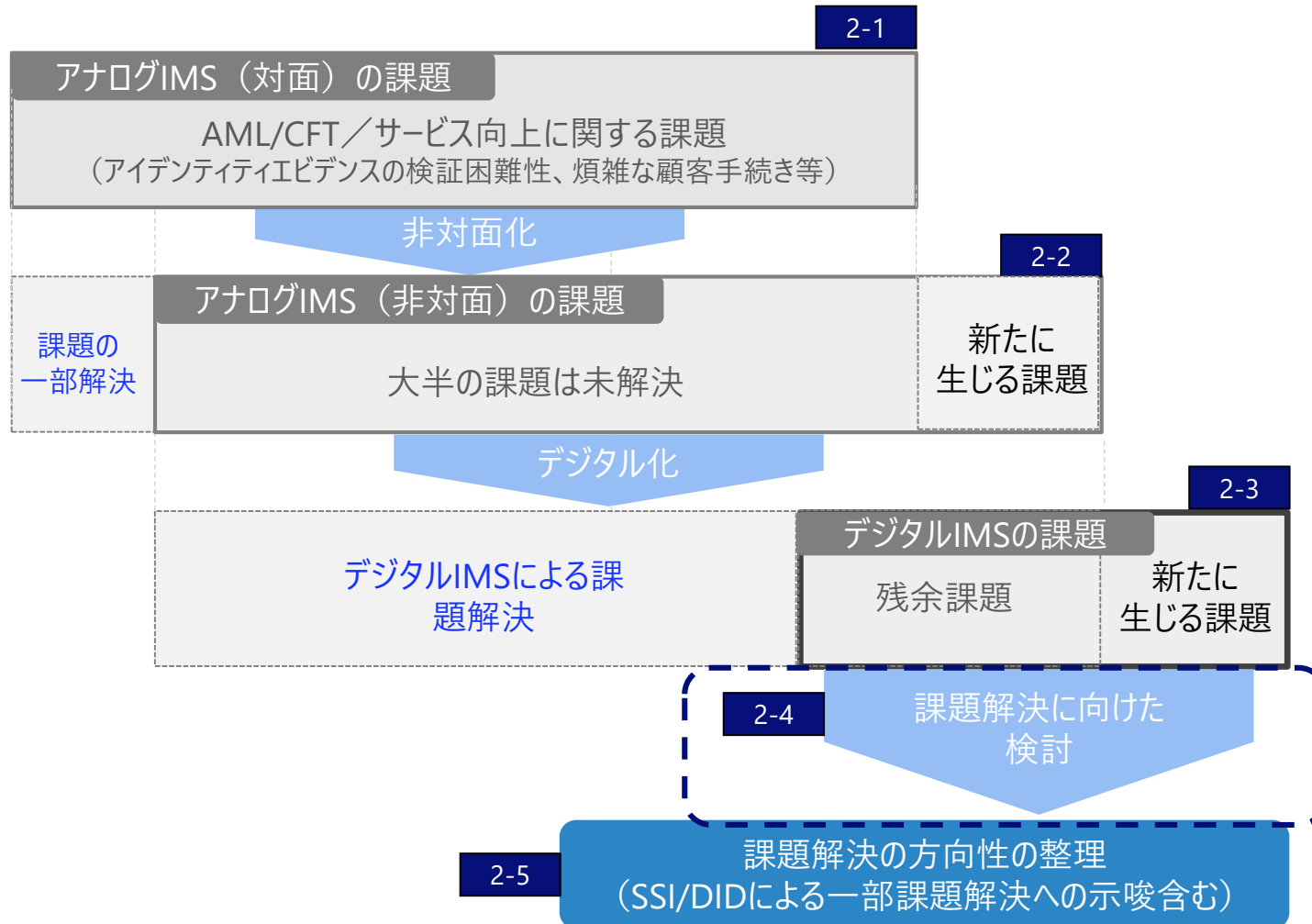
課題の観点	課題
1) IAL	・デジタルIMSの適切な活用を促す規制フレームワーク整備
2) ID連携（責任分界を中心に）	・ID連携当事者間のビジネスモデル・責任分界の未整備 ・特定の金融機関(IdP)への依存度が高まる
3) プライバシー （同意管理・データミニマイゼーション）	・ID連携の同意管理負担 ・複数サービス横断で顧客データを利活用するための、データ利用許諾の整備負担 ・情報の第三者提供に関して、データ提供側として、顧客同意対応の負担が大きい ・情報の第三者提供に関して、データ受け取り側として、データ提供側への説明と確認の対応負担が大きい ・データ利活用の目的と範囲に関する、顧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. 課題解決（先進的事例からのインプリケーション）

---

## 2-4. 課題解決（先進的事例からのインプリケーション）

### 本節での議論対象



## 2-4. 課題解決（先進的事例からのインプリケーション）

### 課題解決に向けた先進事例の活用

- 前節で挙げた通り、デジタル化されたIMSの構築・運用には様々な課題があるが、諸外国においてはこれらの課題に取り組む先進的事例もみられる。
- 本節では前節で挙げた、デジタルIMS化でも解決しなかったアナログIMSの課題、デジタルIMS化により新たに発生する課題について、下表の通り、取組事例から課題解決の示唆を得る。
  - なお、7) は、金融機関からのデータ参照先に関する課題のうち、海外での先進事例が見られるクロスボーダー取引の諸課題への対応のみを取り上げる。

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、 <b>3章で詳細を議論する</b>
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. 課題解決（先進的事例からのインプリケーション）

### ①EU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

- EUでは公共サービス向けであるeIDASの民間サービスにおける適用可能範囲の拡大を検討中である。
- 合わせてAML指令の改訂による顧客管理規定の統一化も検討中である。

#### 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。
- 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

- 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が規定され、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。

## 2-4. 課題解決（先進的事例からのインプリケーション）

## 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

- AML/CFT高度化（例：リモートオンボーディング）やクロスボーダー取引改善などを目的に、eIDASに基づくeIDの金融セクターでの活用に向けた検討が進展している状況である。

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（推奨にとどまる）。
2017年	DG FISMAにおいてeID/KYCI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（別紙：詳細レポート参照）
2019年12月	上記eID/KYCI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つの報告書 <sup>*1)*2)</sup> （別紙：詳細レポート参照）
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	①2021年Q3までに他の金融機関等の実施した顧客管理への依拠を可能とするガイドラインを整備、②AML/CTF規制のEUワイドでの統一、③eIDAS規制の民間IDへの拡張、を規定。

\*1) 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](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)

\*2) 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](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)



## 2-4. 課題解決（先進的事例からのインプリケーション）

# ①EU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

■ DG-FISMAは本人確認及び 顧客管理に必要な属性要素を提唱\*1)している。

### コアアイデンティティ属性（個人）

- 個人を一意に識別する属性のセット
- 氏名・生年月日・出生地・氏名・国籍・個人ID等

### コアアイデンティティ属性（法人）

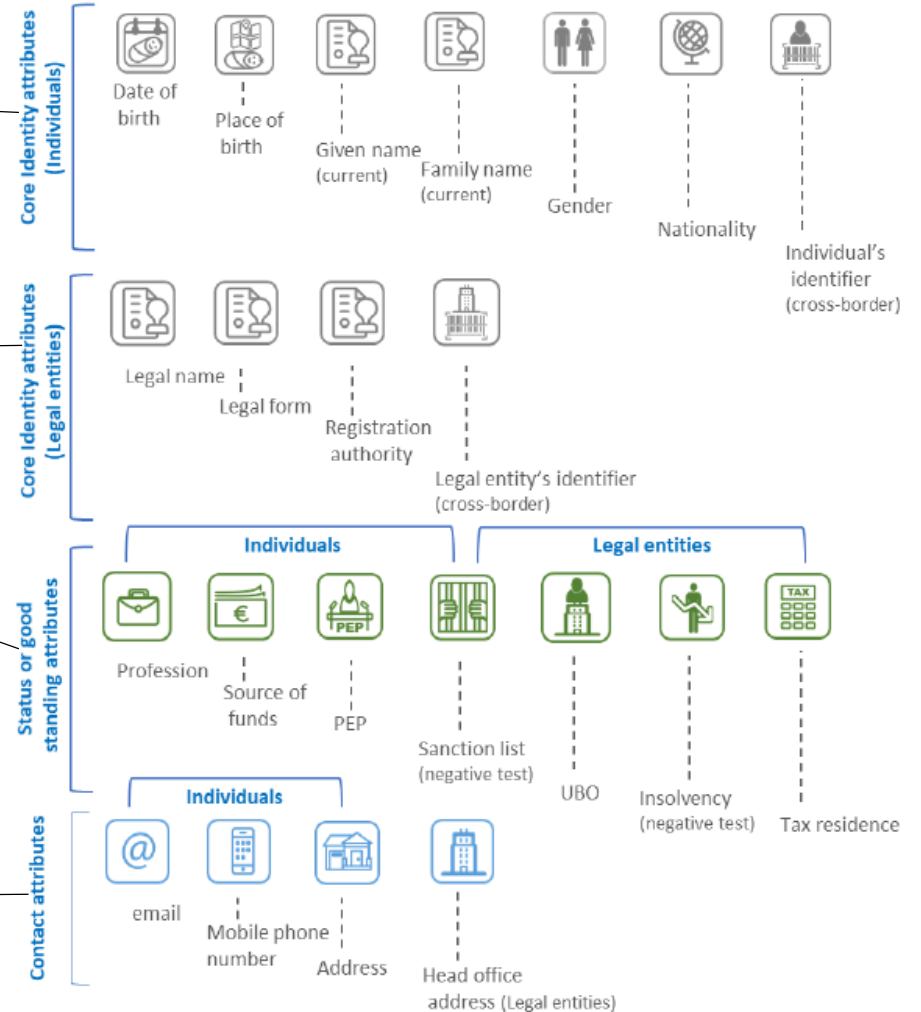
- 法人を一意に識別する属性のセット
- 法人名・登記先・法人ID等

### ステータス（個人）またはグッドスタンディング（法人）属性

- 顧客管理目的で必要とされる属性
- （個人）職業・収入源等
- （法人）実質的支配者・債務不履行歴等

### コンタクト属性

- 当人との連絡を手助けする属性
- 住所等



\*1) 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](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)

## 2-4. 課題解決（先進的事例からのインプリケーション）

### ②シンガポールにおける国民IDを活用したonboardingプロセスの効率化

- シンガポールでは政府が国民IDを20年近くに亘り推進、普及させてきた。
- この基盤を活用し、大手金融機関はonboardingプロセスの効率化に大きく成功している。

#### 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、普及されて来た。
- ✓ SingPassが2018年、MyInfoが2017年に民間サービスへ開放された。

#### 成果

- ✓ 当該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、各金融機関が独自蓄積・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。

## 2-4. 課題解決（先進的事例からのインプリケーション）

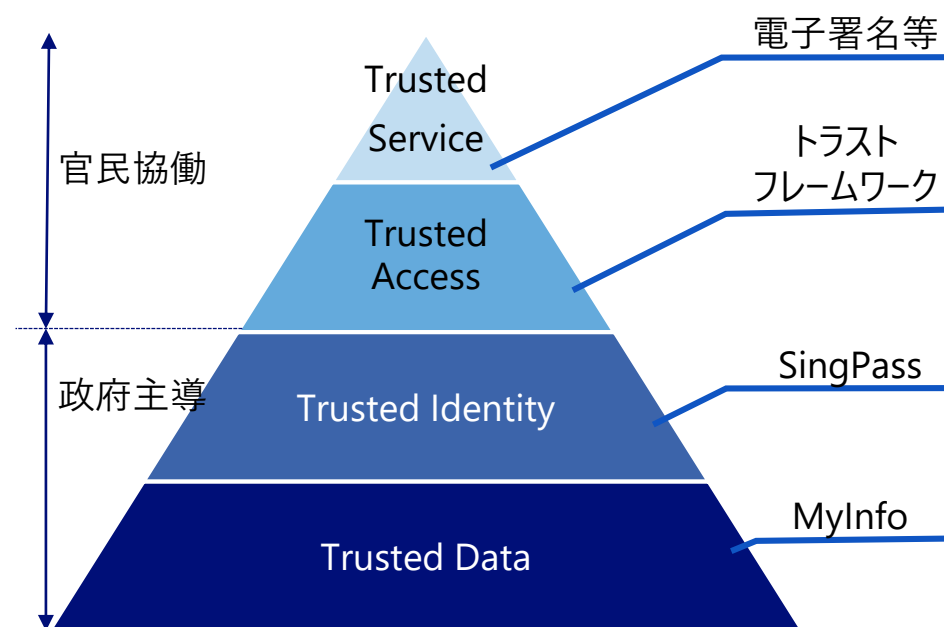
### ②シンガポールにおける国民IDを活用したonboardingプロセスの効率化

- 国民IDを基にしたSingPassによる行政サービス利用に端を発し、SingaPassの認証強化、セキュリティ強化を実施している。
- さらにSingPassおよびMyInfoを基盤にした官民共通のデジタル認証基盤NDIを構築、推進している。

国民IDの普及の経緯

NDI Stackの概念

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) を構築



## 2-4. 課題解決（先進的事例からのインプリケーション）

### ③インドにおけるIndia Stackを活用した民間サービスの拡大

- 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。
- 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、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が、その後Aadhaar法の改正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なった。

<b>課題対応の方向性</b>	<p style="text-align: center;">対応前</p> <ul style="list-style-type: none"> <li>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。</li> <li>なお、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。</li> </ul>	<p style="text-align: center;">対応後</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>
<b>背景・成功要因</b>	<ul style="list-style-type: none"> <li>✓ 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）を整備した。</li> <li>✓ 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した。 （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）</li> </ul>	
<b>成果</b>	<ul style="list-style-type: none"> <li>✓ 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。</li> <li>✓ 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。</li> <li>✓ 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。</li> </ul>	
<b>今後の課題</b>	<ul style="list-style-type: none"> <li>✓ プライバシー：銀行口座やPANカードとのひも付けは登録の「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がある。</li> <li>✓ 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がある。</li> </ul>	

出所) Digital Financial Services (April 2020) <https://documents1.worldbank.org/curated/en/750421502949470705/pdf/118736-BRI-EMCompass-Note-42-DFS-Challenges-and-Opportunities-PUBLIC.pdf>  
 NNA アジア取材ノート「国民皆番号、商機と危うさ生む改革」(2017年9月号) [https://www.nna.jp/nnakanpasar/backnumber/170901/feature\\_001](https://www.nna.jp/nnakanpasar/backnumber/170901/feature_001)

## 2-4. 課題解決（先進的事例からのインプリケーション）

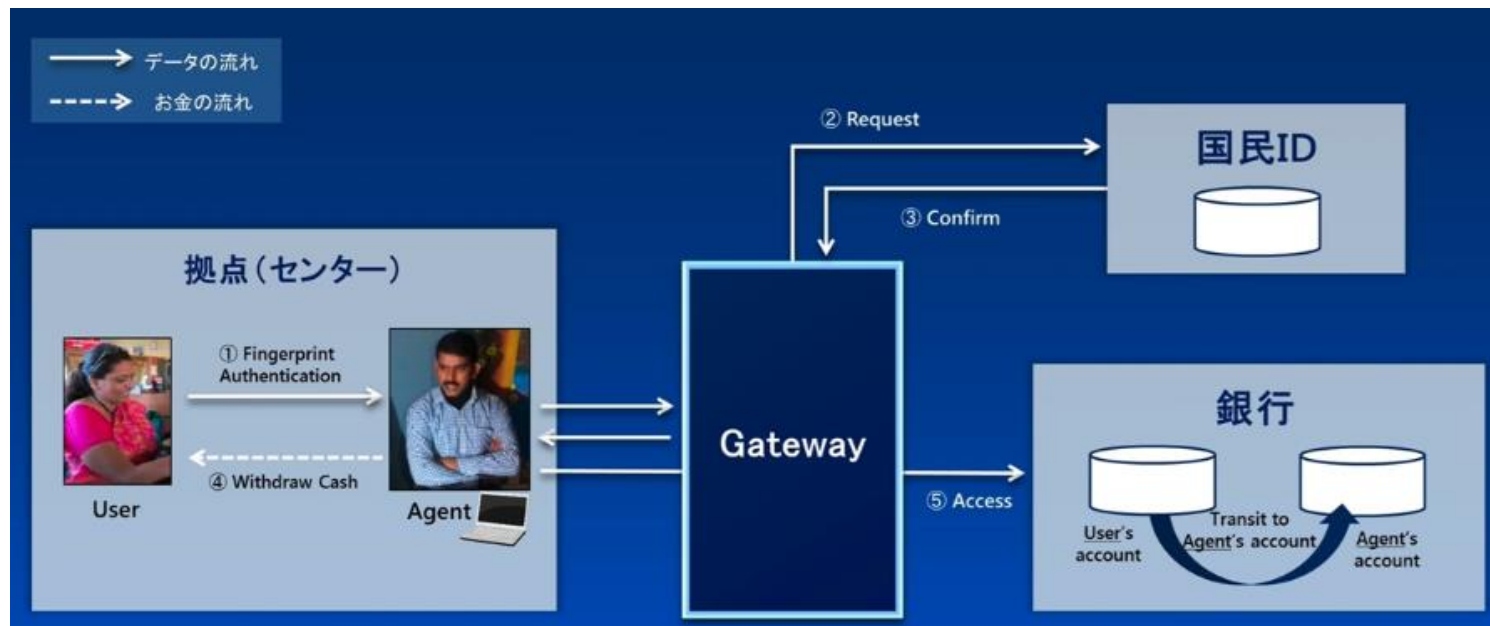
### ③インドにおけるIndia Stackを活用した民間サービスの拡大

#### ■ デジタルインフラ未整備の農村部での金融取引事例\*1)

- 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。



\*1)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>

## 2-4. 課題解決（先進的事例からのインプリケーション）

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

- 英国では国民IDの普及に複数回失敗し、代替策としてGOV.UK Verify（詳細後述）を導入した。
- しかし利用者数、サービス数、本人認証成功率、利益いずれも未達であり、IdPの撤退が始まっている。

<p><b>課題対応の方向性</b></p>	<p>対応前</p> <ul style="list-style-type: none"> <li>• 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カードを発行した。</li> <li>• 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とした。</li> <li>• 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カード法を廃止した。</li> </ul>	<p>対応後</p> <ul style="list-style-type: none"> <li>• 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できるようGOV.UK Verifyを整備した。</li> <li>• 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とした。</li> <li>• 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、中止の権利を付与した。</li> </ul>
<p><b>背景・成功要因</b></p>	<ul style="list-style-type: none"> <li>✓ 政府横断的にデジタルサービスを担うGDS (Government Digital Service)が導入を主導した。</li> <li>✓ 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<sup>*1)</sup>の資金を支援した。（2021年10月まで）</li> </ul>	
<p><b>成果</b></p>	<ul style="list-style-type: none"> <li>✓ GOV.UK Verifyを利用して22種類の公共サービスを利用可能とした（2020年1月現在）。</li> <li>✓ 7社の認定事業者（2014年10月現在）と600万人が利用中である（2020年1月現在）。</li> </ul>	
<p><b>今後の課題</b></p>	<ul style="list-style-type: none"> <li>✓ 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社へ減少した。</li> <li>✓ 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している。</li> </ul>	

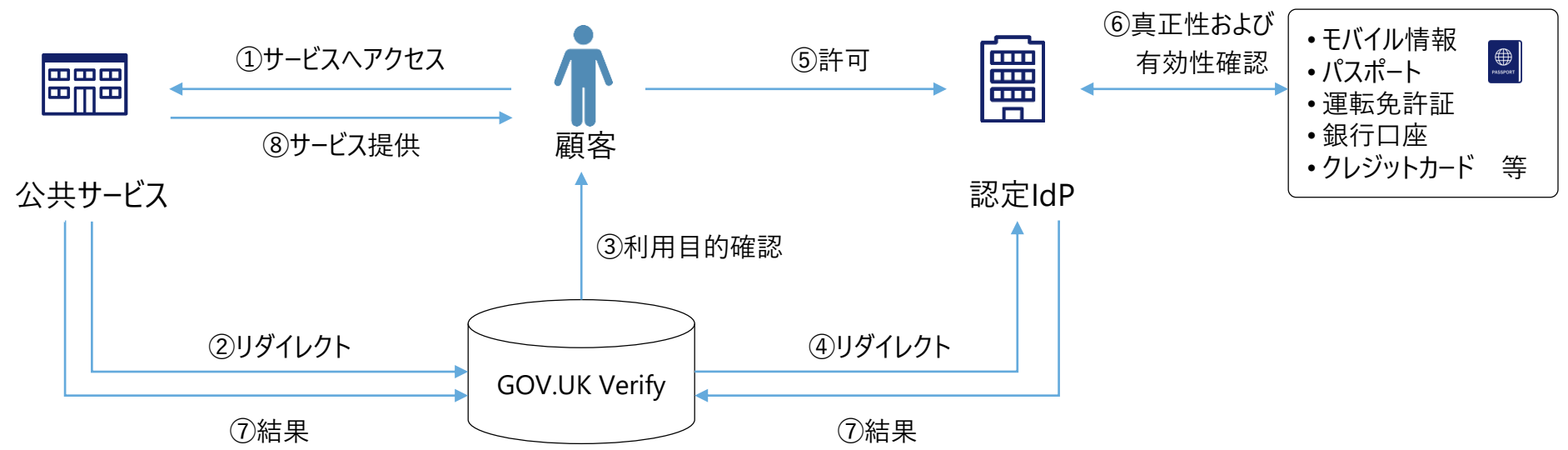
\*1) <https://www.governmentcomputing.com/identity/news/commercial-concerns-push-two-idps-away-verify-heads-towards-private-sector-delivery>

## 2-4. 課題解決（先進的事例からのインプリケーション）

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

- 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る。
- 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。

アイデンティティの真正性・有効性を確認するフロー



## 2-4. 課題解決（先進的事例からのインプリケーション）

## ⑤ID連携サービスにおける責任分界

- ID連携サービス1および2においては 本人確認済みもしくは高認証レベルの情報に限定してIdPが責任を負う。
- ID連携サービス3においては参考情報の位置付けのため、RPが責任を負う。

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

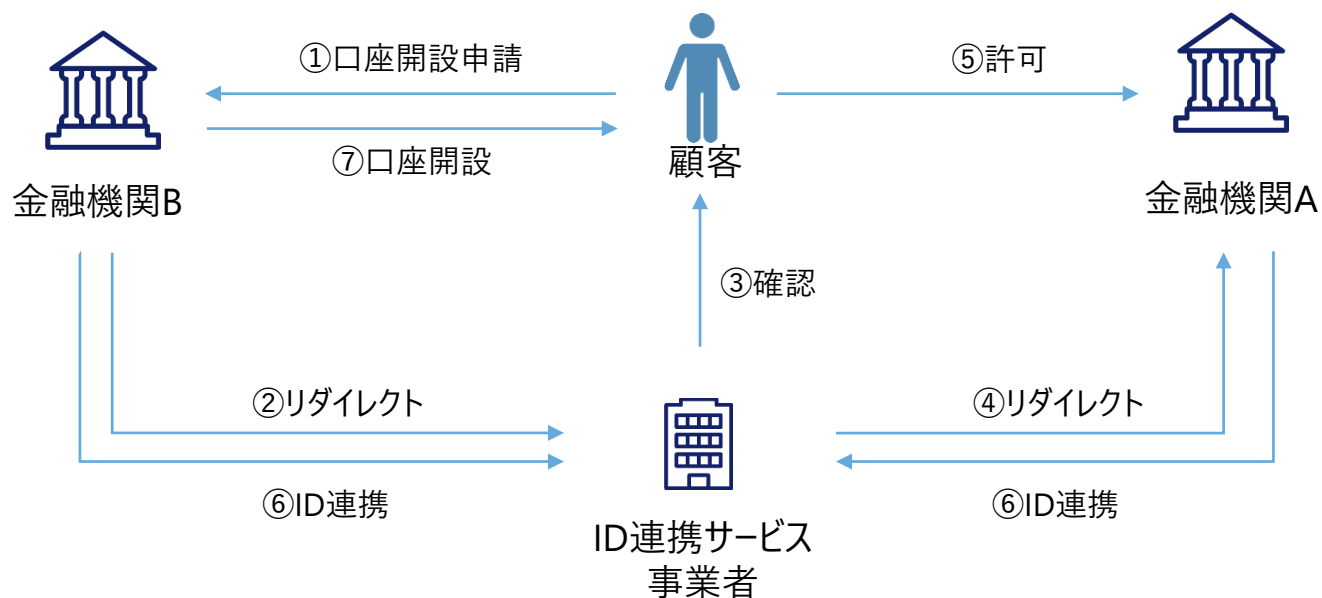


## 2-4. 課題解決（先進的事例からのインプリケーション）

### ⑤ ID連携サービスにおける責任分界

- ID連携サービス 1 ～ 3 のいずれもID連携サービスの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。
- 連携されるIDに対する責任分界はID連携サービスにより異なる。
- 連携されるIDの対価もID連携サービスにより異なる。

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



## 2-4. 課題解決（先進的事例からのインプリケーション）

## ⑥標準化団体の取り組み 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。

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	<ul style="list-style-type: none"> <li>ISO 17442-2 : Legal entity identifier (LEI)(取引主体識別子)の規格策定</li> </ul>	活動終了	<ul style="list-style-type: none"> <li>LEIは金融取引における法人を特定する識別子であり、AMLへの活用等も議論されている</li> </ul>	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	<ul style="list-style-type: none"> <li>ISO/DIS 24366 : Natural Person Identifier (NPI)(自然人ID)の規格策定。</li> </ul>	第一版の作成に向けて議論中	<ul style="list-style-type: none"> <li>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AML等への活用の動きが議論されている</li> </ul>	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	<ul style="list-style-type: none"> <li>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</li> </ul>	Implementation Draft2公開済	<ul style="list-style-type: none"> <li>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高度化につながるユースケースが検討されている</li> </ul>	2) ID連携  (詳細後述)
	FAPI WG	<ul style="list-style-type: none"> <li>FAPI(Financial-grade API) 1.0の策定</li> </ul>	FAPI2.0 Implementation Draft1発行済	<ul style="list-style-type: none"> <li>英国Open BankingにおけるPSD2対応等、幅広く活用されている</li> </ul>	5) 相互運用性
OIX	<ul style="list-style-type: none"> <li>Digital ID for AML</li> <li>Banks in the Identity Market</li> </ul>	<ul style="list-style-type: none"> <li>金融機関のAML業務の活用等、金融特有の課題を議論</li> </ul>	検討中	<ul style="list-style-type: none"> <li>AML等、金融特有の取組を実施中</li> </ul>	5) 相互運用性

## 2-4. 課題解決（先進的事例からのインプリケーション）

## ⑥標準化団体の取り組み OpenID Foundation eKYC &amp; Identity Assurance WG

- 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。

## 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<sup>®</sup>”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連携仕様を策定した。
- 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連携から、仕様検討を実施中である。  
(以上詳細次頁)

## 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の要請に基づき検討を行った。

## 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している。

## 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が必要である。

## 2-4. 課題解決 (先進的事例からのインプリケーション)

# ⑥標準化団体の取り組み OpenID Foundation eKYC & Identity Assurance WG

### ■ 活動概要

- 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
- 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中

自然人におけるID連携仕様イメージ




```

"verification": {
  "trust_framework": "de_aml",
  "time": "2012-04-23T18:25Z",
  "verification_process": "f24c6f-6d3f-4ec5-973e-b0d8506f3bc7",
  "evidence": [
    {
      "type": "id_document",
      "method": "pipp",
      "verifier": {
        "organization": "Deutsche Post",
        "txn": "1aa05779-0775-470f-a5c4-9f1f5e56cf06"
      },
      "time": "2012-04-22T11:30Z",
      "document": {
        "type": "idcard",
        "issuer": {
          "name": "Stadt Augsburg",
          "country": "DE"
        },
        "number": "53554554",
        "date_of_issuance": "2010-03-23",
        "date_of_expiry": "2020-03-22"
      }
    }
  ]
}

```

出所：OpenID 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>

法人におけるID連携項目イメージ (青枠部分が現在検討中の情報)

 <p><b>Claims:</b>        Alice Mirror        DOB: Jan 1 1970        SSN: 123132123</p>	 <p>Verified by        Verified How        Verified When        Evidence Used</p>
<p>Authority to act...        For: ACME Co        Role: Director        Granted by: Board of directors</p>	

法人の代理として活動する自然人の情報

出所：同左

## 2-4. 課題解決（先進的事例からのインプリケーション）

## ⑦ 民間発行IDによるクロスボーダー取引

- 現在は法域内における民間IDの浸透を最優先し、当該IDを利用した本格的なクロスボーダーには未進出である。
- 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。

課題対応  
の方向性

## 現在

- 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<sup>\*1)</sup>の双方に準拠しているため、隣接他法域においても利用可能だが、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。

## 新eIDAS制定後

- 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<sup>\*2)</sup>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。

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、同法域規制当局の権限が弱体化している。

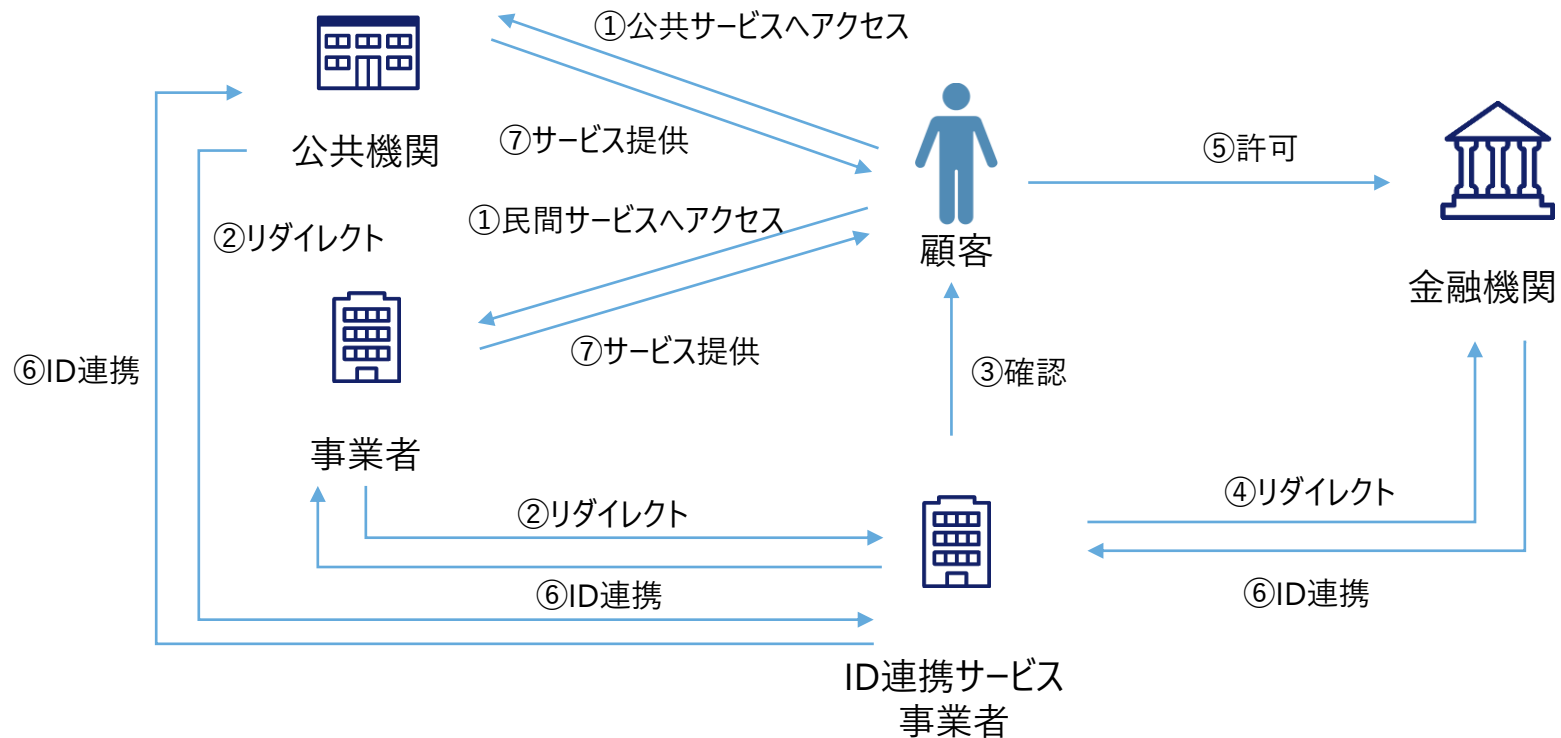
\*1) 電子署名に関する指令（2016年7月にeIDASへ置換） <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0093>

\*2) 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/#/>

## 2-4. 課題解決（先進的事例からのインプリケーション）

## ⑦ 民間発行IDによるクロスボーダー取引

- 金融機関において口座開設を行うことによりIDが発行される。
- 当該IDを用いて公共サービスや事業者サービスを利用することが可能である。

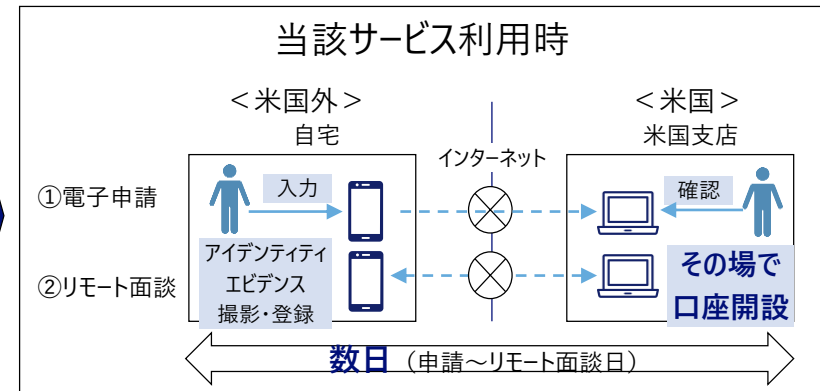
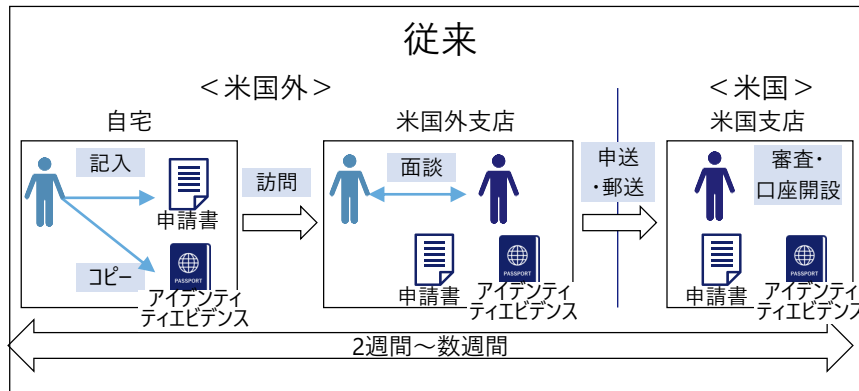
金融機関が作成したデジタルアイデンティティを用いたID連携フロー

## 2-4. 課題解決（先進的事例からのインプリケーション）

## ⑧ 欧州大手金融機関によるクロスボーダー口座開設

- 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、欧州大手金融機関は一部顧客限定で国外からのリモート口座開設サービスを提供している。
- 対象を上位ステータス口座保有顧客に限定することで、非対面リスクを抑制している。

## 課題対応の方向性



## 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り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。

## 2-4. 課題解決（先進的事例からのインプリケーション）

### 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が利用されないと見込み、TrustID frameworkを策定した。
- 中銀・金融業界に加えDTAが参加し、金融系IdPによるID連携・統一を目的としてしている。

#### 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等、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。



## 2-4. 課題解決（先進的事例からのインプリケーション）

## ⑨オーストラリアにおける官民サービスの相互運用

- PSB（Payment System Board）は、金融システムのリスク管理・決済システムの効率化・競争の促進を検討するRBA内の委員会であり、決済業界との調整機関としてAPCを設立した。
- APCは政府IDの代替としてTrustID frameworkを策定し、さらにTDIFとの相互運用性を持たせることで、官民双方のサービスへのアクセスを可能とした。
- DTA・豪中銀も関与してTrustIDフレームワークを策定した背景には、政府としてもTDIF上のIdPであるDTAのmyGovIDや郵便公社のDigitaliDが金融サービス内で広く採用されることを期待するのが難しくなったことがある、という意見も見られている。



（参考）TrustID frameworkに参加している組織（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

**その他サービス**

- Coles Group Ltd（小売）
- Woolworths Ltd（小売）
- Optus（通信）
- Australian Postal Corporation（郵便公社）

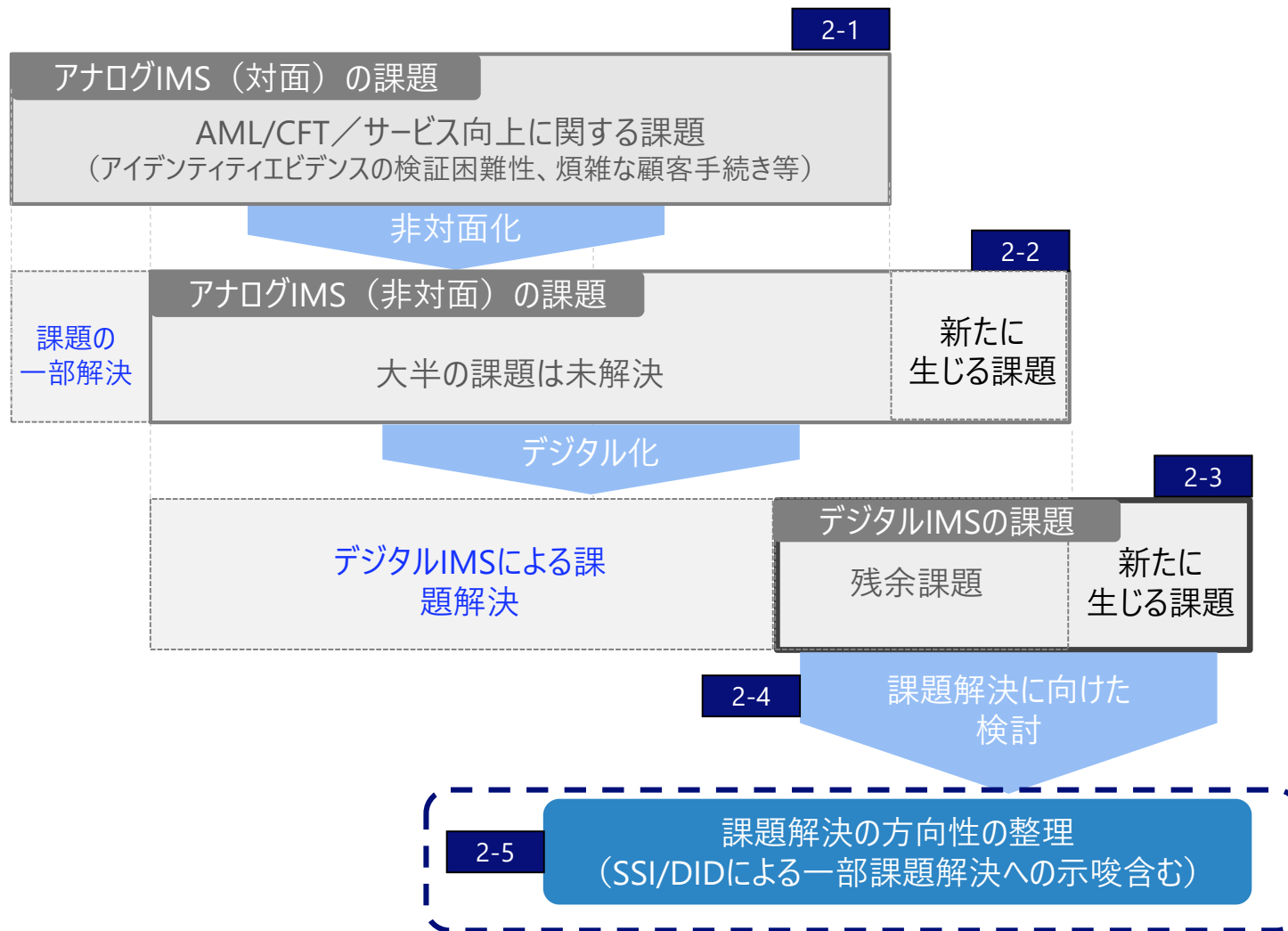
**行政機関等**

- Digital Transformation Agency
- Reserve Bank of Australia

## 2-5. 課題解決の方向性の整理

---

## 本節での議論対象



### 本節の検討事項の概要

- 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、諸外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。  
(2) ID連携の課題の一部および(3) プライバシーの課題の一部が該当する)
  
- 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

# 本節の検討対象課題一覧

- 2-3-8.で整理した、下表の課題を対象とする。

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 ・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

カテゴリ	課題	課題詳細	取り組み事例と得られた示唆
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	<ul style="list-style-type: none"><li>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<sup>*1)</sup></li><li>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。</li></ul>	<ul style="list-style-type: none"><li>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。</li><li>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・③事例)</li><li>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。</li><li>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(①事例)。</li></ul>

\*1)FATF Guidance on Digital Identity (March 2020) <http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html>

## 2) “ID連携” の課題詳細と取り組み事例・得られた示唆

カテゴリ	課題	課題詳細	取り組み事例と得られた示唆
2) ID連携	<ul style="list-style-type: none"> <li>・ID連携当事者間のビジネスモデル・責任分界の未整備</li> </ul>	<ul style="list-style-type: none"> <li>・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。 <ul style="list-style-type: none"> <li>・ 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。</li> <li>・ 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</li> <li>・ 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</li> <li>・ 上記3点の責任分界に見合う対価の合意</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>・ 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(⑤事例)。 <ul style="list-style-type: none"> <li>-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</li> <li>-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</li> <li>-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</li> </ul> </li> </ul>
	<ul style="list-style-type: none"> <li>・特定の金融機関(IDプロバイダー)への依存度が高まる</li> </ul>	<ul style="list-style-type: none"> <li>・顧客が、ある金融機関(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。</li> <li>・更に、IDプロバイダー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を被る可能性が有り、影響の拡大が懸念されると考えられる。</li> </ul>	<ul style="list-style-type: none"> <li>・特定のIDプロバイダー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。</li> </ul>

### 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

カテゴリ	課題	課題詳細	取り組み事例と得られた示唆
3) プライバシー	<ul style="list-style-type: none"> <li>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</li> <li>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</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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。</li> <li>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。                     <ul style="list-style-type: none"> <li>データ利活用に関する顧客への説明実施負担</li> <li>同意記録の作成・保管等の顧客との同意管理負担</li> </ul> </li> </ul> <p>(データ提供側の負担)</p> <ul style="list-style-type: none"> <li>データ利活用に関する顧客への説明実施負担</li> <li>同意記録の作成・保管等の顧客との同意管理負担</li> </ul> <p>(データ受け取り側の負担)</p> <ul style="list-style-type: none"> <li>データの出し手に対するデータ取得経緯等の確認負担</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>
	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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。                     <ul style="list-style-type: none"> <li>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。</li> <li>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</li> <li>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。</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。<sup>*1)</sup></li> </ul>

\*1) 日本IT団体連盟による「情報銀行」の認定制度 <https://www.tpdms.jp/system/index.html>



## 4) “金融包摂” の課題詳細と取り組み事例・得られた示唆

カテゴリ	課題	課題詳細	取り組み事例と得られた示唆
4) 金融包摂	・デジタル対応できない人物の 金融排除	<ul style="list-style-type: none"> <li>• 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。<sup>*1)</sup> <ul style="list-style-type: none"> <li>– 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</li> </ul> </li> <li>• 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。           <ul style="list-style-type: none"> <li>– デジタル化されていない人々の年齢層を見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、間違っただ操作に対する恐怖、例えば誤ってボタンを押してしまい間違っただ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</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• 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           <ul style="list-style-type: none"> <li>– 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シンガポール・③インドの事例)</li> <li>– 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)</li> </ul> </li> <li>• 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</li> <li>• 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</li> </ul>

\*1)FATF Guidance on Digital Identity (March 2020) <http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html>

## 5) “相互運用性” の課題詳細と取り組み事例・得られた示唆

カテゴリ	課題	課題詳細	取り組み事例と得られた示唆
5) 相互運用性	・煩雑なID連携仕様への対応負担	<ul style="list-style-type: none"> <li>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。 <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>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(⑩オーストラリアの事例)</li> <li>左記は、主に一つの法域の範囲を想定した課題であるが、国をまたいだ技術仕様の相互運用性に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。 <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> </ul> </li> <li>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。 <ul style="list-style-type: none"> <li>(例) FDX(Financial Data eXchange)<sup>*1)</sup> <ul style="list-style-type: none"> <li>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</li> <li>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 <ul style="list-style-type: none"> <li>(FDXのCertificateのテスト手順) <ol style="list-style-type: none"> <li>1次試験：OIDF Certificate(FAPI ConformanceTest)</li> <li>2次試験：各国個別要件に応じたテスト</li> </ol> </li> </ul> </li> </ul> </li> </ul> </li></ul>

\*1)FDX Press-Release “Financial Data Exchange, OpenID Foundation Take Step Towards Global Standard for Financial Data Sharing” (March 2019)

<https://openid.net/2019/04/02/financial-data-exchange-openid-foundation-take-step-towards-global-standard-for-financial-data-sharing/>

## 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

カテゴリ	課題	課題詳細	取り組み事例と得られた示唆
6) 新しい業務へ移行するための投資判断	<p>・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</p>	<p>・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。</p> <ul style="list-style-type: none"> <li>- 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。</li> <li>- 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。</li> <li>- 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。</li> </ul>	<ul style="list-style-type: none"> <li>・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(⑤事例(ID連携))。</li> <li>・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*1)も加味した、包括的な施策としてとらえる考え方もある。</li> <li>・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*2)、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*1)、がそれぞれ文献で指摘されている。</li> </ul>

\*1)Private Sector Economic Impacts from Identification Systems <https://elibrary.worldbank.org/doi/pdf/10.1596/31828>

\*2)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>

## 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

カテゴリ	課題	課題詳細	取り組み事例と得られた示唆
7) クロスボーダー取引の諸課題	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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。</li> <li>FSB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。 <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>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(2-3-5【AML/CFT】クロスボーダー取引の諸課題をめぐる動向 参照)</li> <li>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(⑦事例)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(⑧事例)等の個別の動きが見られる。</li> </ul>

## 2-6. 本章の結論

### 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、フェデレーションモデルのアイデンティティマネジメントシステムになりつつあり、デジタルアイデンティティの活用が進んでいくと考えられる。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(IDプロバイダー)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)

---

## 3. 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

#### 3-1. SSI/DIDの概要

- 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した。
- 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。したがって、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した。その結果、
  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 (Unlinkabilityの確保) 、
  4. デジタルアイデンティティの長期の保管・利用が可能、という4つの特性の導出を行った。

#### 3-2. SSI/DIDの実現に必要な構成要素

- SSI/DIDに関する複数の標準化団体が提唱する実現方式を俯瞰し、3-1.で導出した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・整理を行った。

#### 3-3. SSI/DIDの先行事例/PoC事例

- SSI/DIDに関して、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を中心に取組内容について整理した。

#### 3-4. SSI/DIDの長所と実現に向けた課題

- SSI/DIDの長所と実現に向けた課題について整理した。SSI/DIDは3-1で挙げた4つの特性を活用することで、①自己主権の獲得②プライバシーへの配慮③利便性の向上／業界全体のコスト抑制、といったメリットが期待出来る。
- 他方、課題としては、①技術②法的/制度③運用④ビジネスの観点で継続検討が必要な課題が存在する。

#### 3-5. SSI/DID活用時の金融規制上の論点

- 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検討を行った。SSI/DID独自の論点として、①ウォレットに対する金融規制の考え方、②新たな本人確認情報に対する法的手当て、の観点から整理した。

## 3-1. SSI/DIDの概要

---



### 「3-1. SSI/DIDの概要」の要旨

#### ■ SSIと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旨とする思想」である。
- DIDとは、「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が目的とする仕組み」のことである。

#### ■ SSI/DIDの特性

- SSI/DIDに関する定義を踏まえ、以下4点の特性を導出した。

実現すべき項目	項目概要
認証と属性の分離	<ul style="list-style-type: none"><li>● 特定IdPへの依存度を下げするため、Recognition（当人認証）とSelfness（属性）を分離</li><li>● クレームプロバイダー（CP）からDIDと紐づける形で属性を発行し、その後DIDを用いてライティングパーティ（RP）に対し認証を行うことで、クレームの連携を行う</li></ul>
分散した属性の活用・選択的な提示	<ul style="list-style-type: none"><li>● 複数CPからのクレーム取得・連携</li><li>● ウォレットからRPに対し選択的に提示する</li></ul>
提示先の秘匿（Unlinkability）	<ul style="list-style-type: none"><li>● ウォレットを介したクレームの連携を行うことで、CPに対し、クレームの送付先となるRPを秘匿しつつクレームの連携を行う</li></ul>
長期のデジタルアイデンティティの保管・利用	<ul style="list-style-type: none"><li>● 発行されたクレームの検証に用いる資材を分散リポジトリに長期保管することで、仮にCPが存在しなくなった場合でも、過去に発行されたクレーム検証が可能（分散リポジトリにブロックチェーンなどImmutableな性質を持つ技術を採用することで、検証に必要な資材の完全性・透明性を確保する方式を提案する標準化団体も存在）</li></ul>

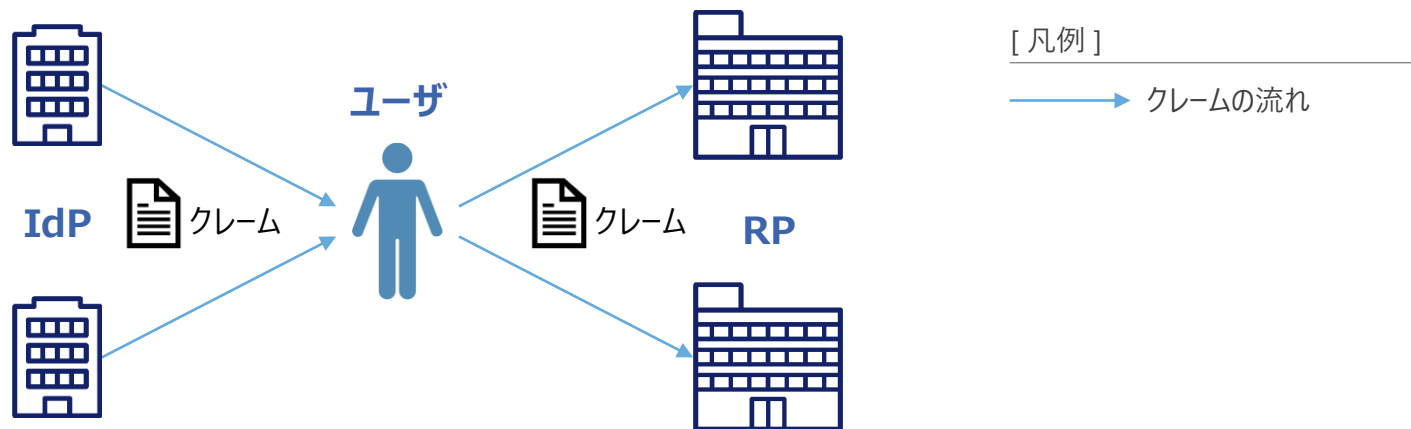
## 自己主権型アイデンティティ (SSI) とは

- 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旨とする思想(※)。

※ : Sovrin Foundation, <https://sovrin.org/faq/what-is-self-sovereign-identity/>

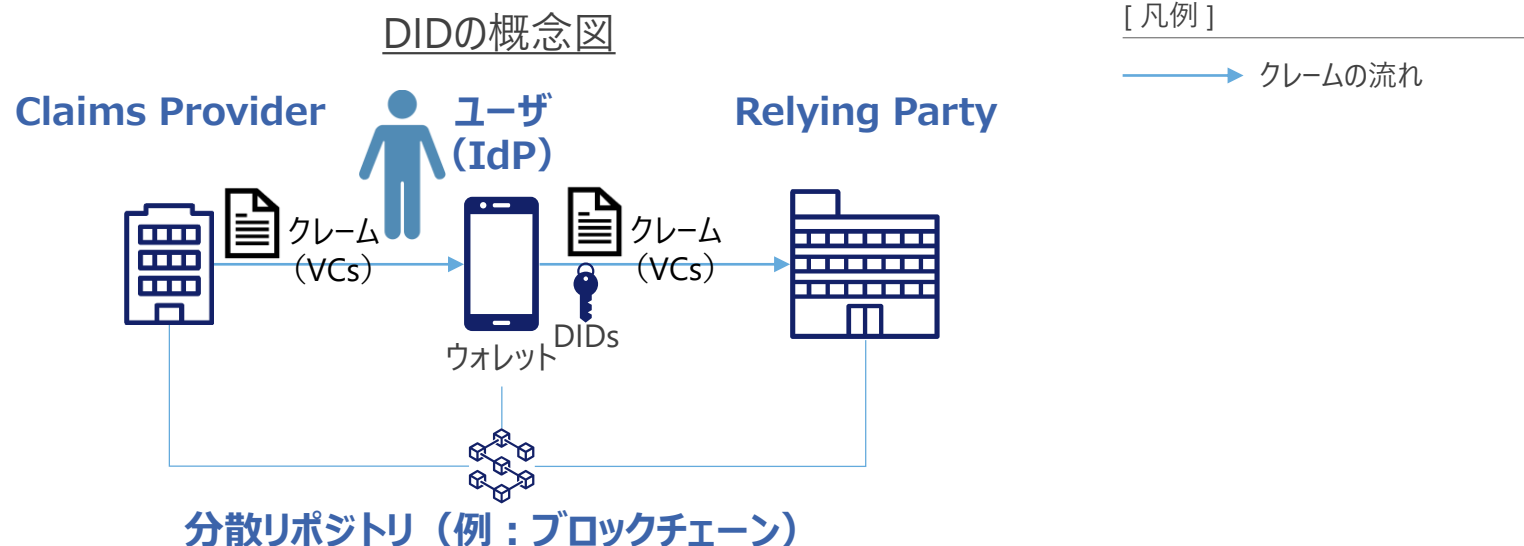
- ユーザが自分の属性情報に関するコントロール権を確保の上、信頼できる組織から発行された本人の属性情報を取得し、ユーザの許可した範囲でRP等に連携できるようにする。

SSIの概念図



## 分散型アイデンティティ (DID) とは

- 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が目的とする。
- 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」  
(Microsoft) ※ : Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access-management/decentralized-identity-blockchain>
- DIDの実装にあたり、例えばWorld Wide Web Consortium(W3C)においては、以下二つの技術が検討されている。
  - Decentralized Identifiers (DIDs)
  - Verifiable Credentials (VCs)

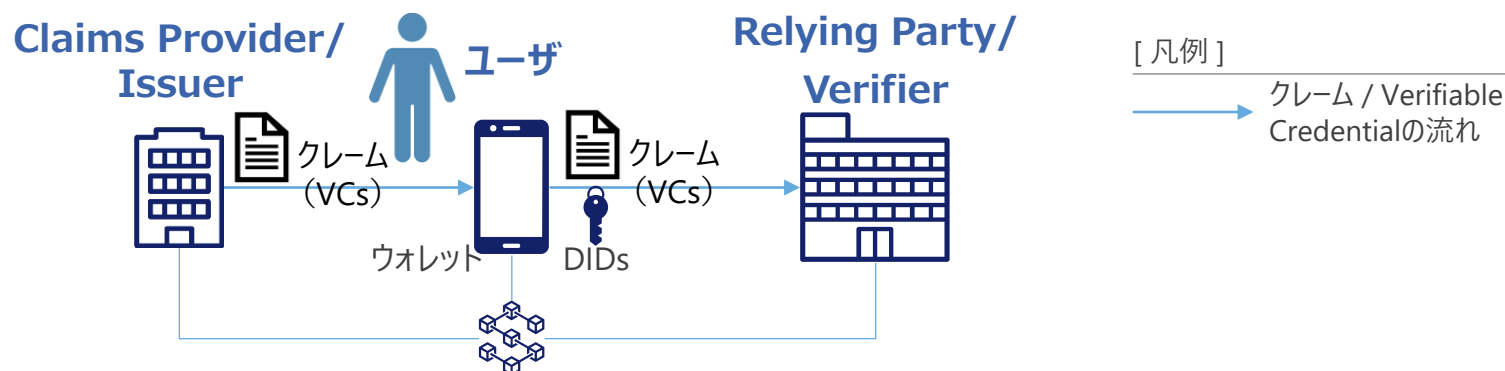


### 3-1-1. SSI/DIDの全体像

## 本調査と標準化団体でのSSI/DIDに関する用語

- SSI/DIDについては3-2-2.項で挙げる標準化団体等がそれぞれ仕様の策定を進めており、SSI/DIDにおける概念の名称についても団体によって表す用語が異なる。
- そのため、本調査でのSSI/DIDに関する概念の名称は1-1.節にて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。

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ちの一部の属性集合	暗号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) な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バ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

※ 出所) Verifiable Credentials Data Model 1.0 1.2 Ecosystem Overview <https://www.w3.org/TR/vc-data-model/> を基にNRI作成

## 「SSIの7原則 (Seven Laws of Identity)」と本章の整理方針

- 1-3.節でも示した通り、キムキャメロン氏は「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、具体的には、原則 5 及び 6 が更新されている。
- 以降本章では、この2点の原則を踏まえ、SSI/DIDの構成要素について整理していく。

#	原則	内容
1	ユーザによる制御と同意	<ul style="list-style-type: none"> <li>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</li> </ul>
2	限定された用途で最低限の公開	<ul style="list-style-type: none"> <li>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</li> </ul>
3	正当な関係者のみへの情報開示	<ul style="list-style-type: none"> <li>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</li> </ul>
4	方向づけられたアイデンティティ	<ul style="list-style-type: none"> <li>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</li> </ul>
5	「アイデンティティハブ」の統合	<ul style="list-style-type: none"> <li>ユーザは、プロバイダー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</li> </ul>
6	長期のアイデンティティの安定性に向けたDIDの統合	<ul style="list-style-type: none"> <li>個人データを事業者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</li> </ul>
7	人間の統合	<ul style="list-style-type: none"> <li>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</li> </ul>

## SSI/DIDで実現すべき項目

- 各標準化団体（W3C、DIF、OpenID Foundation等）では、実現の Protokol は異なるものの、SSIの7原則の項番 5「アイデンティティハブ（※）の統合」および項番 6「長期のアイデンティティの安定性に向けたDIDの統合」の実現すべき項目手段として、いずれも以下の4項目について言及している。



実現すべき項目	項目概要
認証と属性の分離	<ul style="list-style-type: none"><li>• 特定IdPへの依存度を下げるため、Recognition（当人認証）とSelfness（属性）を分離</li><li>• クレームプロバイダー（CP）からDIDと紐づける形で属性を発行し、その後DIDを用いてライティングパーティ（RP）に対し認証を行うことで、クレームの連携を行う</li></ul>
分散した属性の活用・選択的な提示	<ul style="list-style-type: none"><li>• 複数CPからのクレーム取得・連携</li><li>• ウォレットからRPに対し選択的に提示する</li></ul>
提示先の秘匿（Unlinkability）	<ul style="list-style-type: none"><li>• ウォレットを介したクレームの連携を行うことで、CPに対し、クレームの送付先となるRPを秘匿しつつクレームの連携を行う</li></ul>
長期のデジタルアイデンティティの保管・利用	<ul style="list-style-type: none"><li>• 発行されたクレームの検証に用いる資材を分散リポジトリに長期保管することで、仮にCPが存在しなくなった場合でも、過去に発行されたクレーム検証が可能（分散リポジトリにブロックチェーンなどImmutableな性質を持つ技術を採用することで、検証に必要な資材の完全性・透明性を確保する方式を提案する標準化団体も存在）</li></ul>

（※）アイデンティティハブとは、「個人データの管理をユーザの手に委ねる、分散化されたオフチェーンの個人データストア」のこと。

出所) Microsoft, "Identity Hubs as personal datastores" (Mar. 2019)

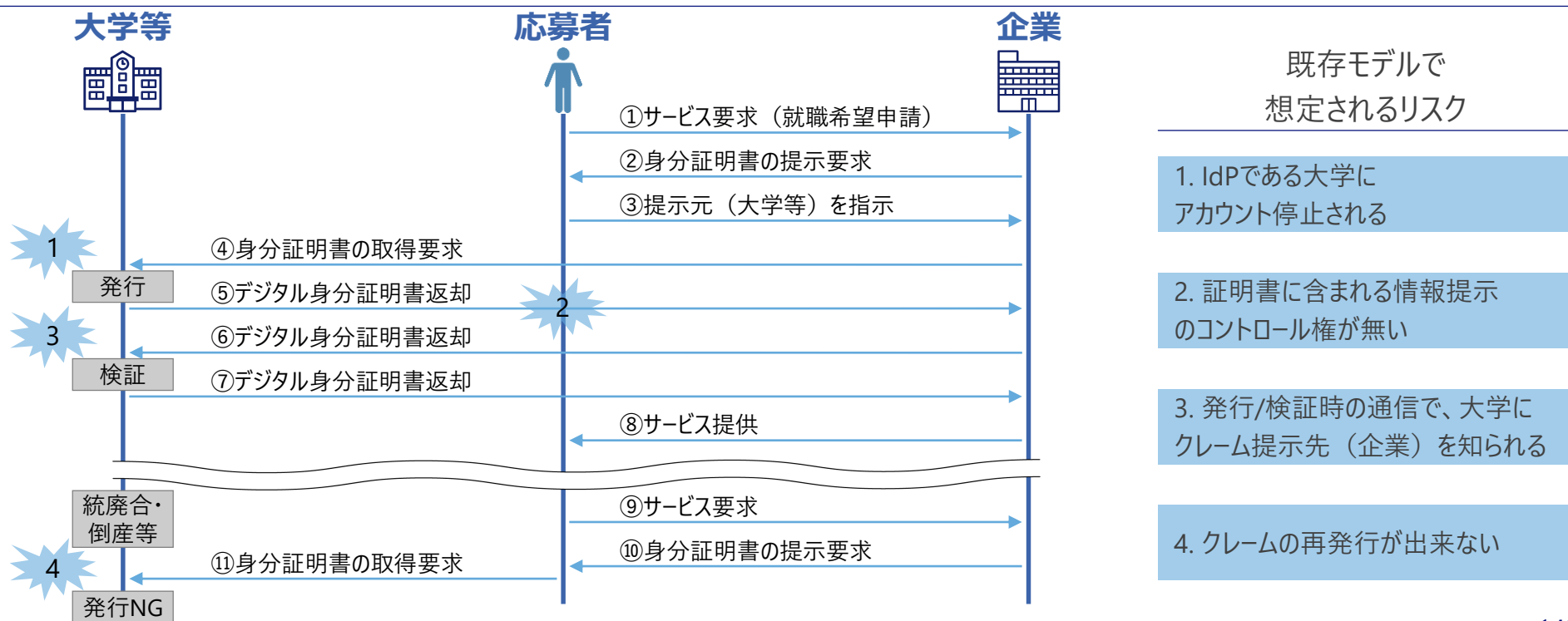
<https://techcommunity.microsoft.com/t5/azure-active-directory-identity/identity-hubs-as-personal-datastores/ba-p/389577>

## ユースケース：就職活動時に就職先に卒業証書を提示【既存モデル】

- 就職活動者が、希望企業に対して必要な書類（本ケースでは大学の卒業証書や成績証明書等）を提示するというユースケースにおいて、現在のFederationを用いた既存モデルでは、以下のようなフローにて処理されるのが一般的。
- 既存モデルでは、クレームの管理を大学等のIdPに強く依存しており、例えば下記に示すリスクが想定される。
  - クレーム提示の際、大学等においてユーザ認証が必要となる。アカウント停止措置等により身分証明書の取得が困難となる。
  - 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。
  - どの企業に応募しているか、大学等に知られてしまう
  - 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

※) 例えば、XX年に〇〇大学を卒業したことだけを提示したいのに、成績や応募者の個人情報等が含まれてしまう等懸念がある。

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

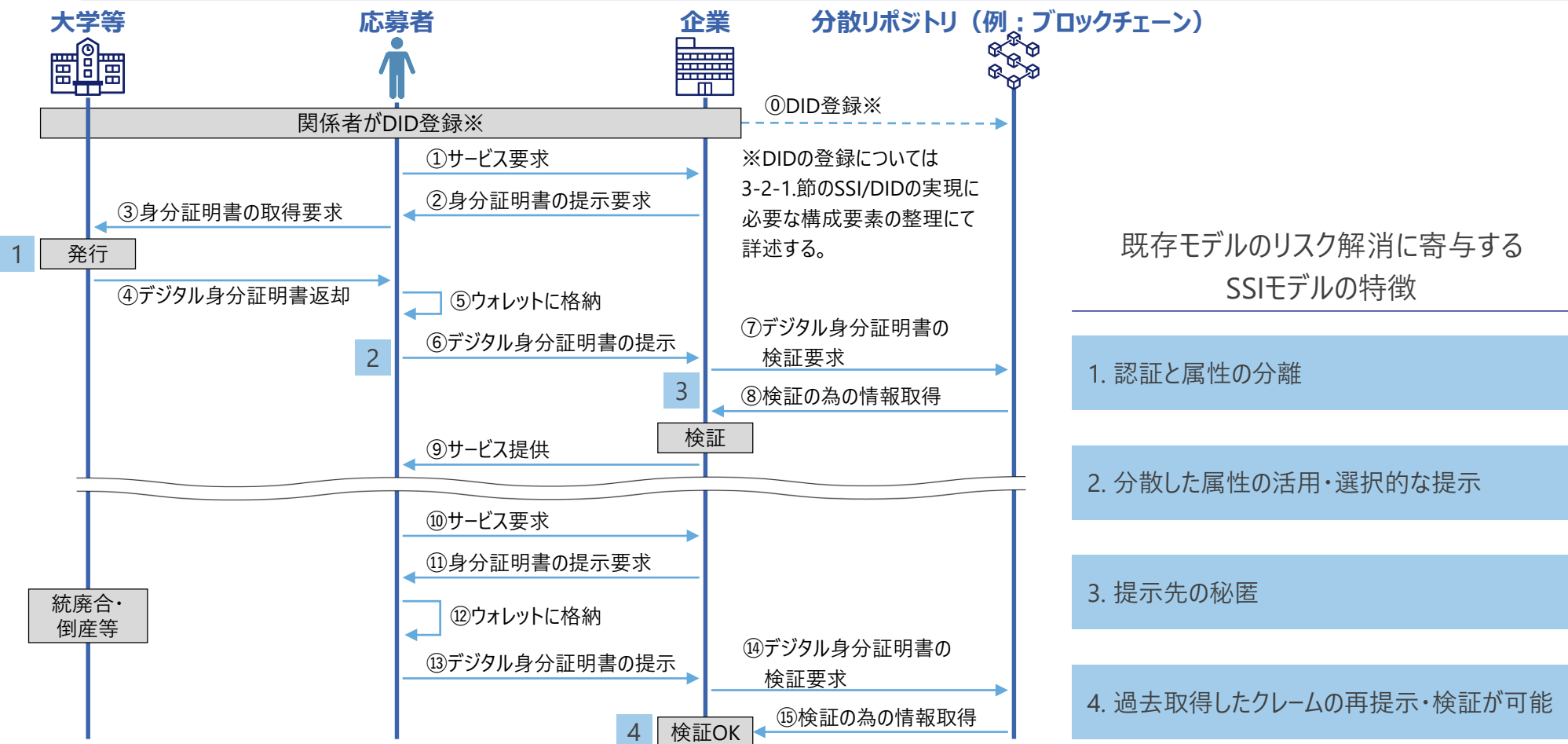


### 3-1-2. SSI/DIDで実現すべき項目

## ユースケース：就職活動時に就職先に卒業証書を提示【SSIモデル】

- SSIのモデルは、これら既存モデルの課題を解決できるモデルであると言われる。具体的には、SSIモデルが提示する  
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、といった特徴により、既存モデルの懸念を解消する可能性を有している。

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





## SSI/DIDで実現すべき項目 – 1. 認証と属性の分離

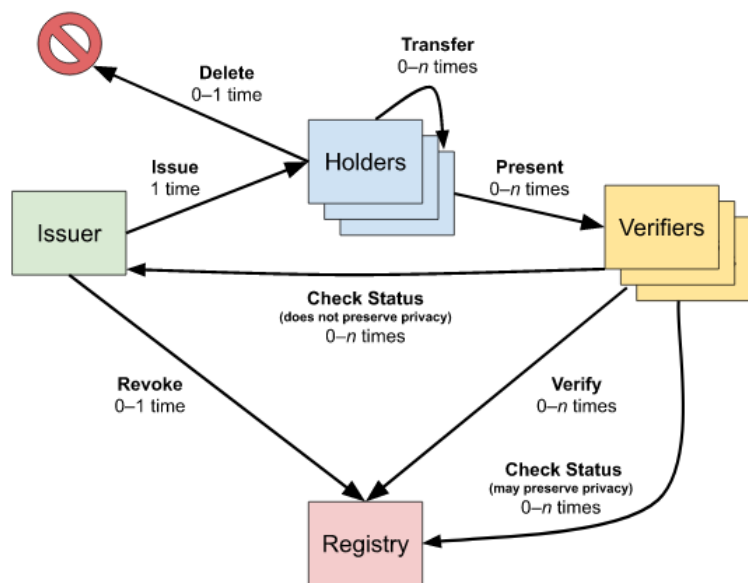
- 「認証と属性の分離」とは、Recognition（当人認証）とSelfness（属性）の分離を意図する。
  - 分散型のデータ連携が可能
    - ユーザの持つ「ウォレット」と呼ばれるデータ保管場所をハブとして、取得したクレームを様々なRPに対し連携することが可能となった。その結果、自分の個人情報を自らがコントロールし、各企業へ必要な情報を連携しながら価値提供が可能となる。
    - Peer to Peerの対向認証に必要となるクレデンシャル情報（識別子（ユーザID等）・シークレット（パスワード等））と、連携される属性を分離する。
  - 既存モデルの抱えるリスクを解消
    - IdPが行う不合理なユーザアカウント停止等により、ユーザが自らの属性情報を取得できなくなる課題があった。これに対し、ユーザがDIDを使うことで、アカウント停止の回避が可能となる。
    - CP以外にウォレットにもクレームを保持。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、当該時刻におけるデータの真正性が保証可能となる（IdPによる改ざんが困難）。



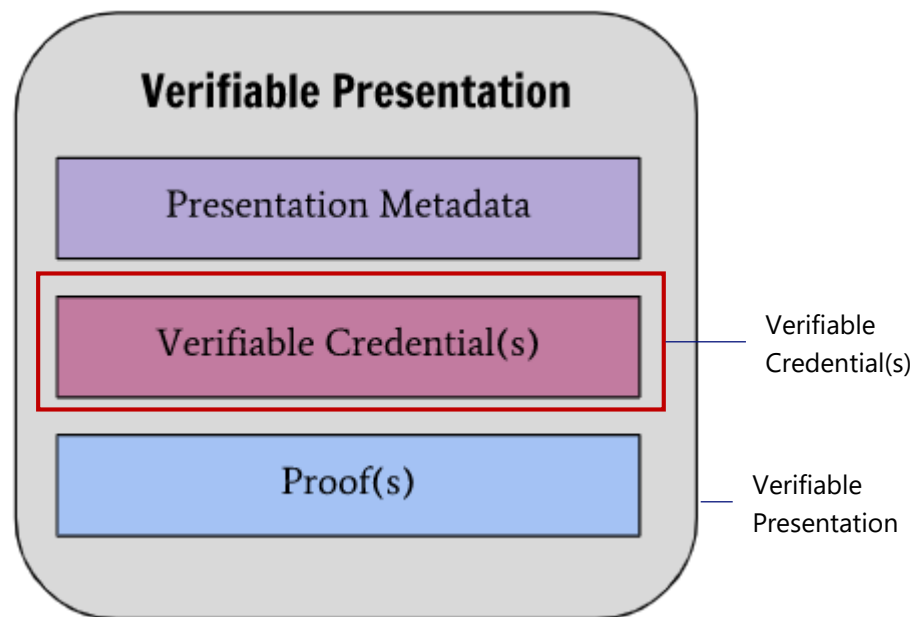
## SSI/DIDで実現すべき項目 – 2. 分散した属性の活用・選択的な提示

- 「分散した属性の活用・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の規程する「Verifiable Credentials Data Model」では、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。

Verifiable Credentials Data Modelにおける  
Verifiable Credentialのライフサイクル



Verifiable Credentials Data Modelにおける  
Verifiable Credential(s)とVerifiable Presentationの概要図



※W3Cにおいては、クレームを検証可能な形で発行する役割を「Issuer」、クレームを受領し発行元や真正性等を検証する役割を「Verifier」として定義

## SSI/DIDで実現すべき項目 – 3. 提示先の秘匿（Unlinkability）

- 「提示先の秘匿（Unlinkability）」とは、ホルダーがCPに、発行されたクレームをどのRPに連携したか知られることなく、クレームの連携・検証が可能であることを意図する。
  - クレームを受け取ったRPは、その真正性を検証（Verify）する必要がある。その際、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。
  - 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する（CP-RP Unlinkable※を満たす）。

※ ISO/IEC FDIS 27551記法に準拠

Holderを介したクレーム連携概要、およびRPにおけるクレーム検証の仕組み

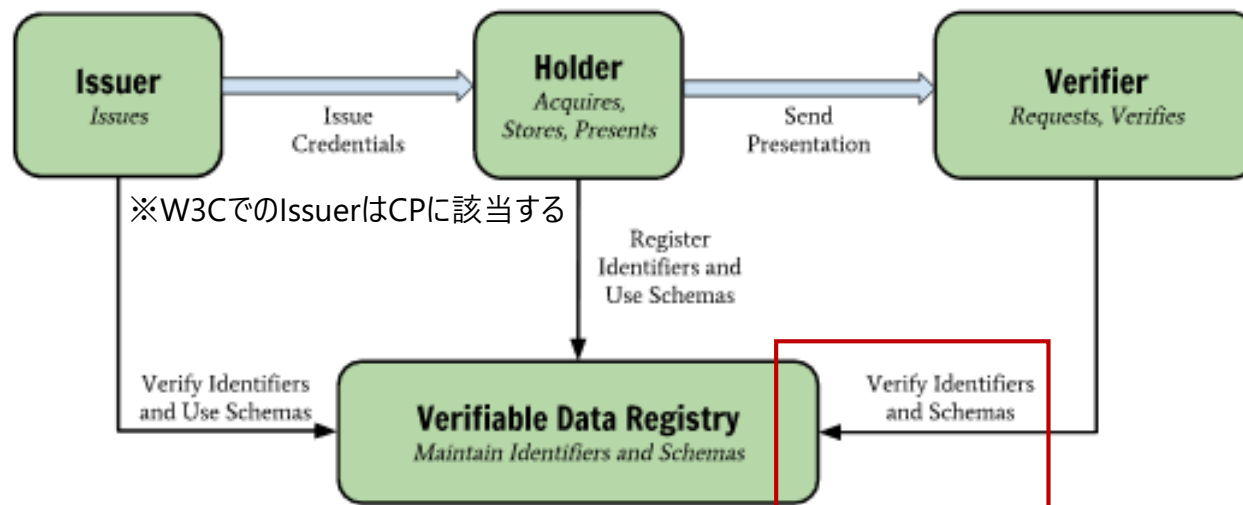
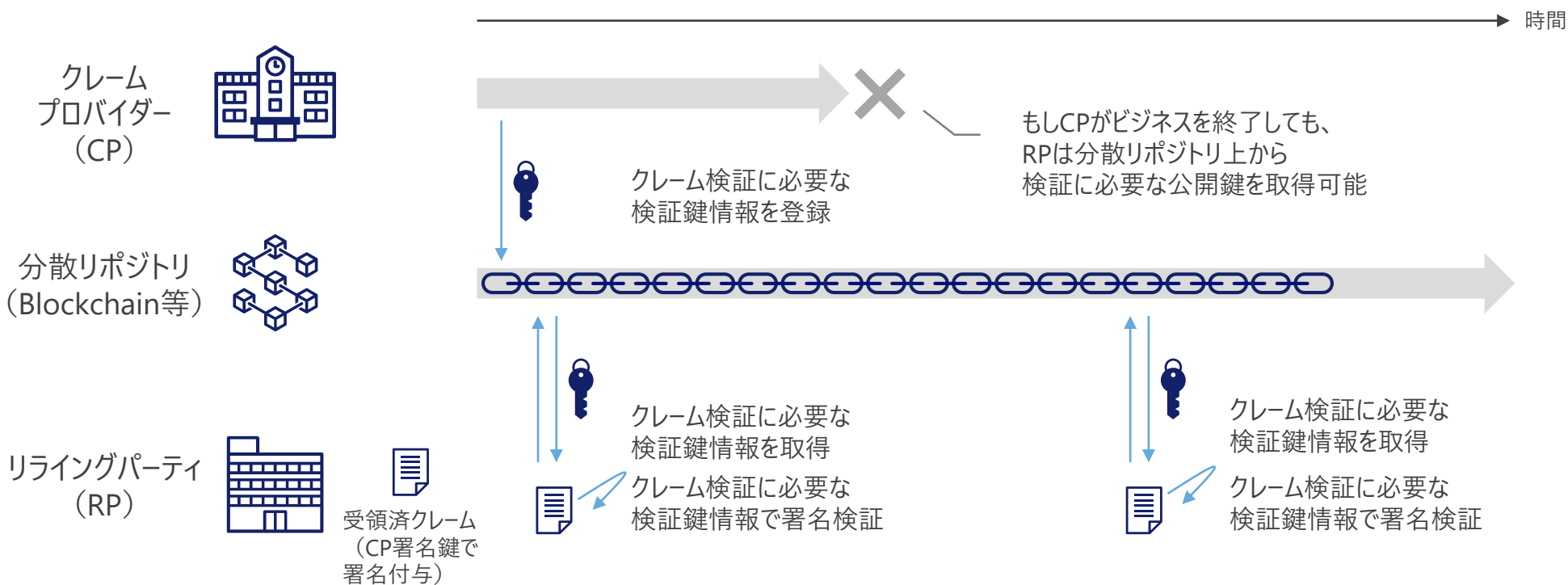


Figure 1 The roles and information flows forming the basis for this specification.

## SSI/DIDで実現すべき項目 – 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（CP）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ものである（真正性が保証されたものである）ことが確認可能。
  - 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。

### 長期のデジタルアイデンティティの保管の概観



## 3-2. SSI/DIDの実現に必要な構成要素

---

### 「3-2. SSI/DIDの実現に必要な構成要素」の要旨

#### ■ 構成要素の整理

- 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

- 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を整理した。
- 相互運用性の動向として、団体間での動向（OpenID Foundation / DIFにおけるリエゾン協定）、仕様策定の動向（Presentation Exchange/DID Comm, CHAPI/Verifiable Presentation Request Specificationの仕様統合）等、一部で協調・収斂の動きもある。但しデータモデルに関する議論は一定検討にあがっているものもあるが、Communication LayerやUtility Layerについては、今後更なる収斂の動きが期待される状況にある。

#### ■ 統制面での整理

- SSIモデルのIMS運用に参加するステークホルダー間でアイデンティティインフォメーションの連携を行う際、相互に信頼を維持した上でデータの連携を行う必要がある。そのためには、「トラストフレームワーク」と呼ばれる、仕組みに参加したステークホルダーを定義し、各ステークホルダーが役割と義務を適切に担うことで、系全体の信頼性を担保するやり方が存在する。
- 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では、SSIモデルに特徴的なアクターであるホルダーを含める形で、各ステークホルダーの定義と付随するロールの定義を行っている。同ガイドを元に、SSIモデルにおいてステークホルダーに求められるロールと、充足すべき統制要件の整理を行った。
- その結果、統制要件自体は、従来の集中型・Federation型モデルのIMSから変わらない一方、どのステークホルダーがどのロールを担うかにより、従来のモデルでは想定されなかったステークホルダー間の利害衝突が発生し得る点が明らかになった。

## 処理フローの定義

- 3-1-2.項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。

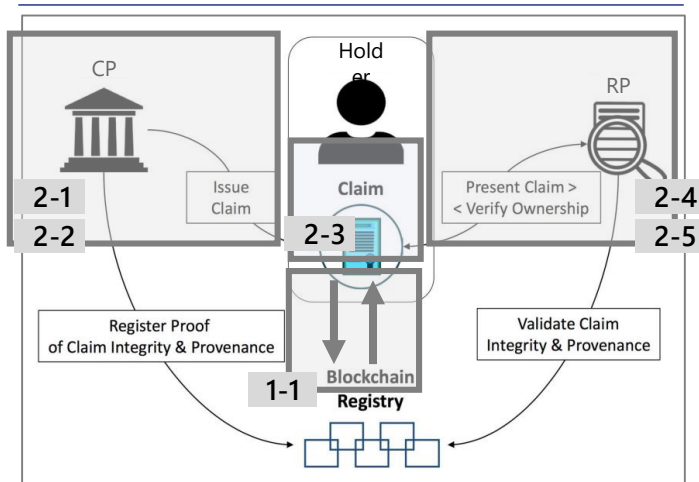
### 1. DIDの登録処理

ホルダーがID Proofingを行い、DIDのActivation処理が完了し、DIDが有効状態に遷移するまでの処理を行う。

### 2. クレームの連携処理

ホルダーがDIDを取得後にIdPとなり、CP / ホルダー間, 及びホルダー / RP間でのクレーム連携処理を行う。

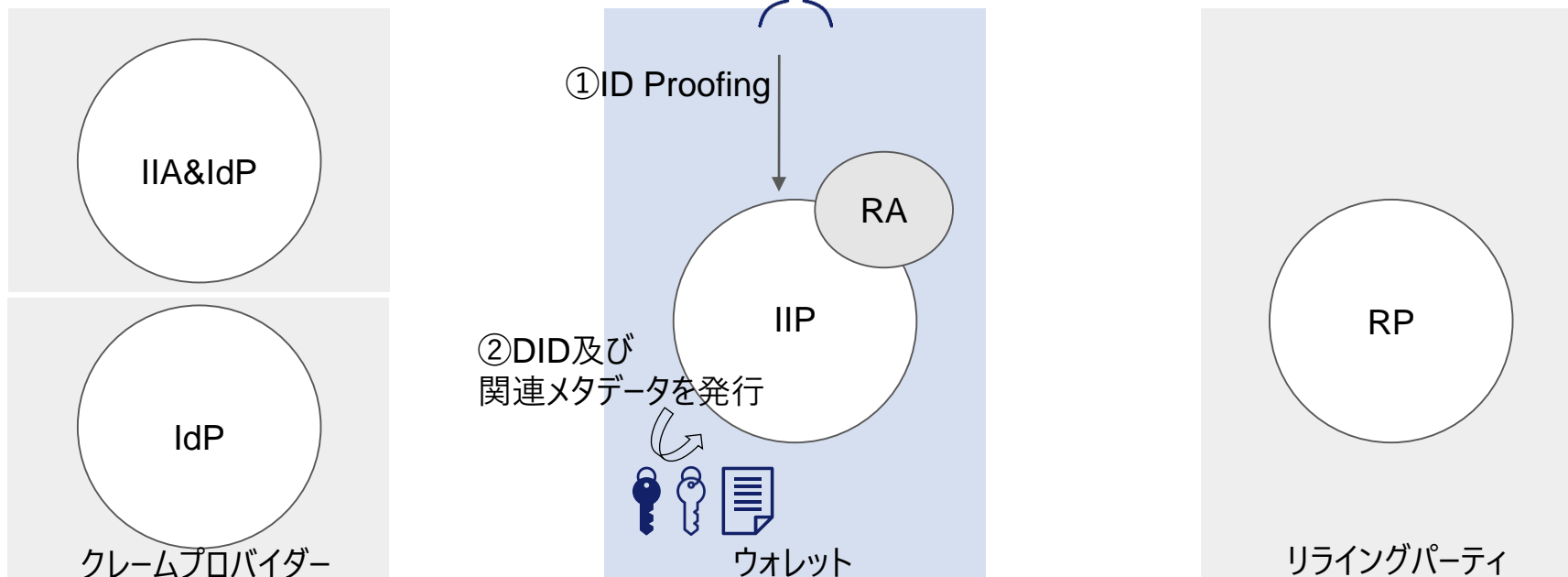
DIDの処理フローの概観



処理	処理概要
1. DIDの登録処理 (DIDが有効状態に遷移するまでの処理)	
1-1. DIDおよびメタデータの生成・登録	DIDおよびメタデータの生成・登録を実施
2. クレームの連携処理	
2-1. CP上のユーザとDID所有者のBinding	<ul style="list-style-type: none"> <li>ユーザがCP内のCSPに対し認証を実行</li> <li>CPは、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を実施</li> </ul>
2-2. クレーム発行	2-1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
2-3. ウォレットへのクレーム格納	2-2) で取得したクレームをウォレットに格納・保持
2-4. RPに対するユーザ認証	ウォレットとRP間で、1-1) のDIDおよびメタデータを用い対向認証
2-5. クレーム連携	<ul style="list-style-type: none"> <li>2-4)で対向の認証が完了後、2-3)で取得したクレームを連携。</li> <li>RPは、受領したクレームが、2-4)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</li> </ul>

## 処理フローの定義 – 1. DIDの登録処理 (1-1. DIDおよびメタデータの生成・登録)

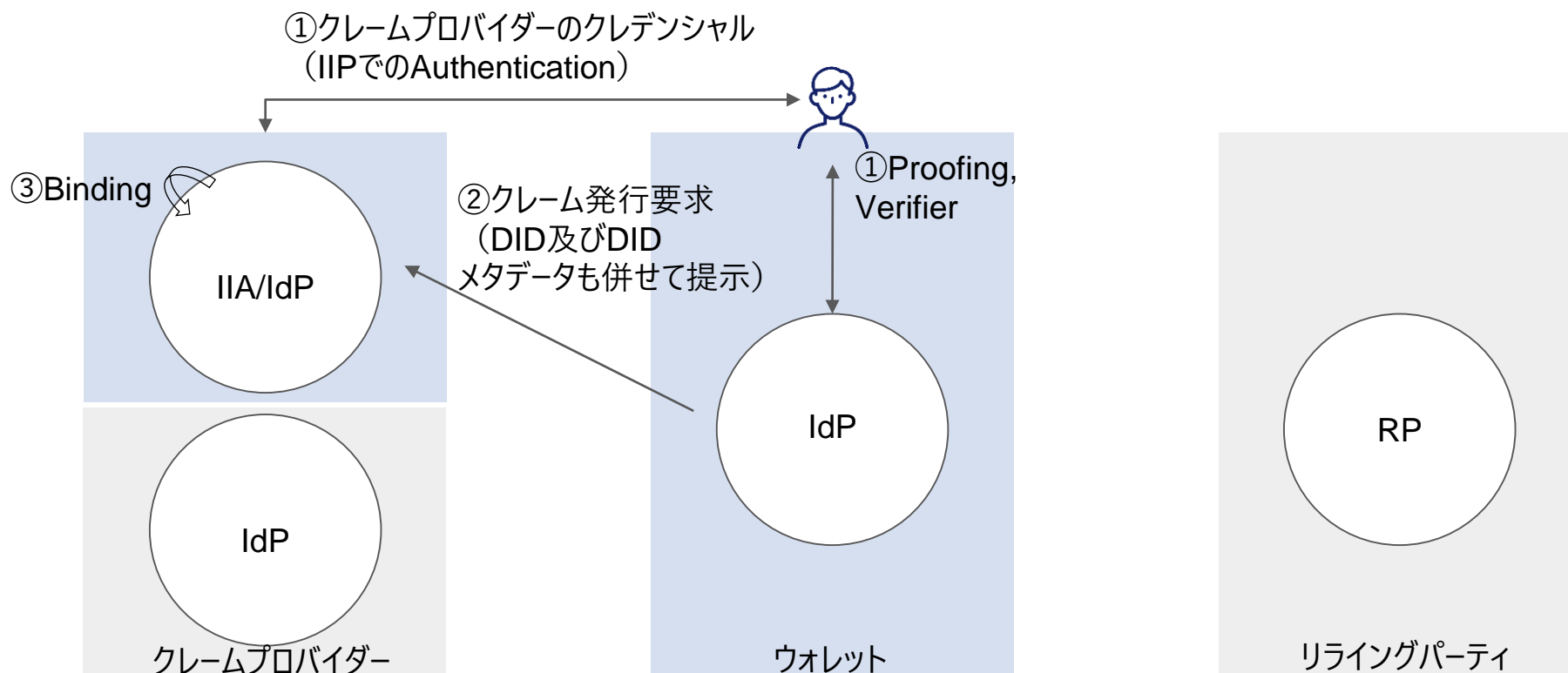
- ① ユーザは、自身のクレーム連携の為に用いる分散型アイデンティティ(DID)をRegistration Authority (RA) を介し、生成・登録を実施する。
- ② 従前のIMSと同じく、何らかのID Proofingを行った上で、ユーザがウォレットの機能を使い、DID及び関連メタデータを発行する (DID生成時には、DIDの所有者であることを示すために用いられる秘密鍵/公開鍵の鍵ペアも生成)。





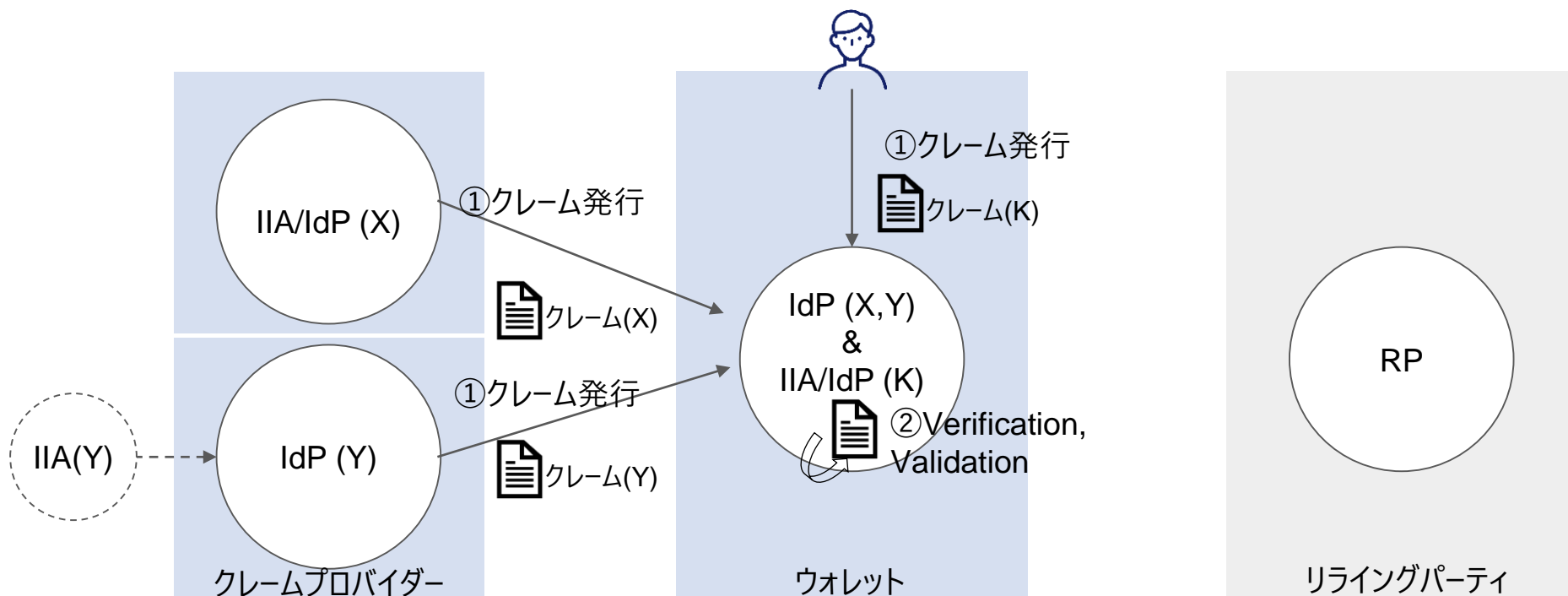
## 処理フローの定義 – 2. クレームの連携処理 (2-1. CP上のユーザとDID所有者のBinding)

- クレームプロバイダーが、ユーザから提示されたDID所有者情報と、クレームプロバイダー上にあるActiveなユーザのIdentifier間のBindingを実施する。
  - ユーザは、クレームプロバイダーのIdPでAuthenticationを行うとともに (①)、クレームプロバイダー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)。
  - クレームプロバイダーの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HolderとのBindingを行う (③)。



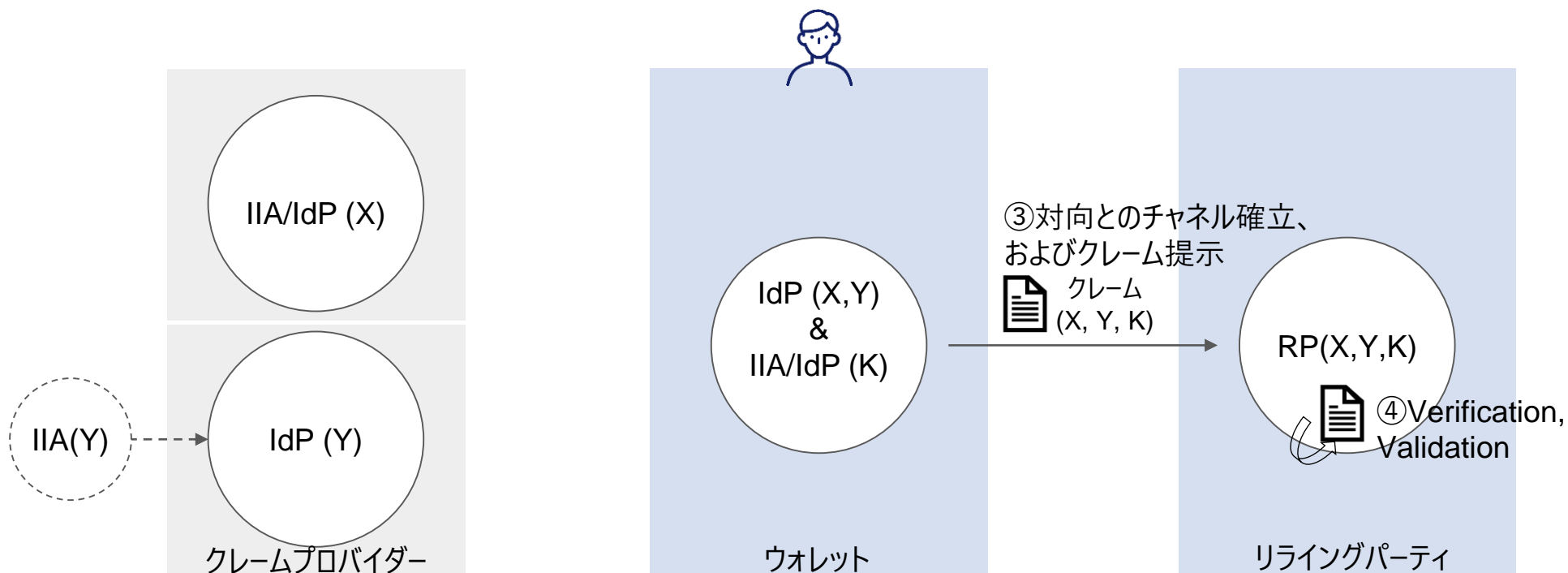
## 処理フローの定義 – 2. クレームの連携処理 (2-2. クレーム発行、2-3.ウォレットへのクレーム格納)

- 2-2. クレーム発行：Binding内容を踏まえ、クレームプロバイダーは、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。
  - 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。
  - 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 (下図クレーム(K)参照)。
- 2-3. ウォレットへのクレーム格納：ホルダーは受領したクレームの真正性・有効性検証を行い、ウォレットに格納 (②)。



## 処理フローの定義 – 2. 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)

- 2-4. RPに対するユーザ認証：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 (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。
- 2-5. クレーム連携：ユーザは保持するクレームから提示を許容したもののみリライティングパーティに提示 (③)。リライティングパーティは、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。



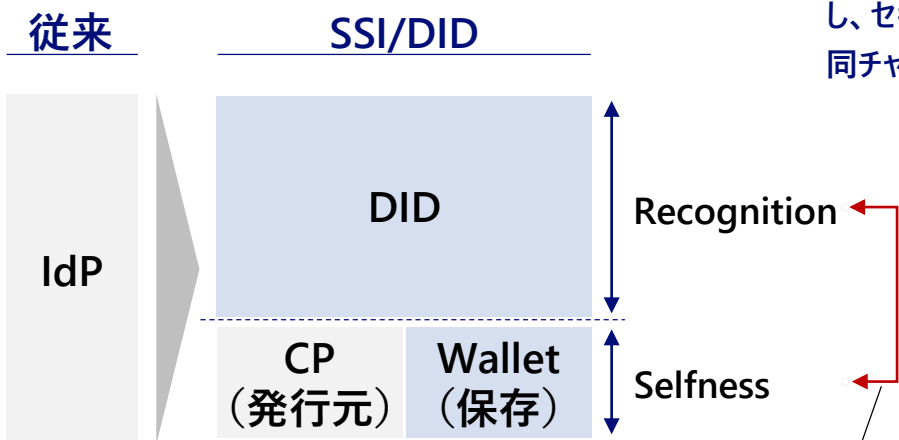
## (参考) Bindingにおける考慮事項 – Bindingの必要性

■ 3-1-2. 項で述べた通り、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。（次頁で詳述）

“当人認証”と“属性”の分離に伴う Binding の実施

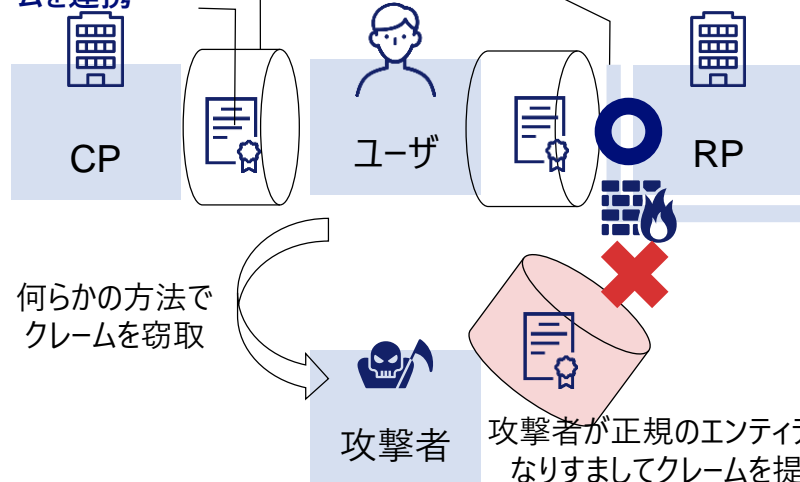
“Binding”による窃取したクレームを用いた“なりすまし”の防止



クレーム発行時の段階で、何らかの方法でBindしていることを暗号的証明可能とする必要がある

対向のエンティティをDIDを用いて認証し、セキュアなチャネルを確立  
同チャネルを介し、クレームを連携

RPが、“対向のエンティティ”と“クレームの発行対象”が紐づいているか暗号的証明がなされているか検証



何らかの方法でクレームを窃取

攻撃者

攻撃者が正規のエンティティになりすましてクレームを提示

## (参考) Bindingにおける考慮事項 – Bindingの方式

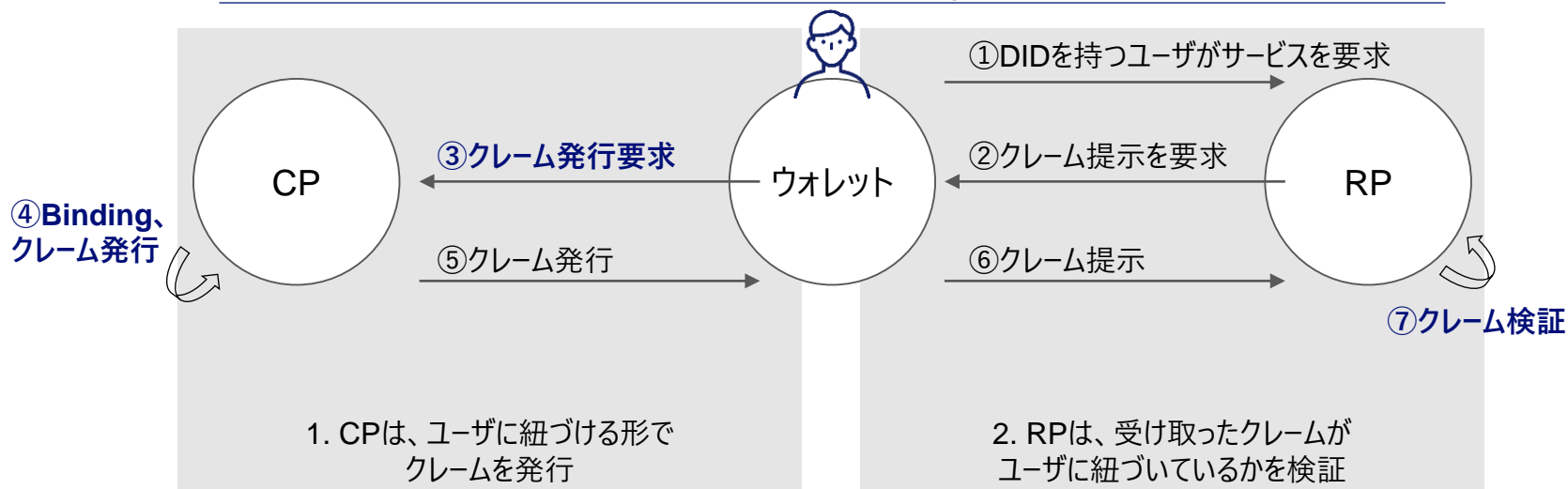
■ ユーザとクレームを“Binding”のためには、下記2点が必要となる。

1. CPがクレームを発行する際、相對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。
2. RPがクレームを受領する際、相對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。

■ 上記実現のためには、以下の処理が必要となる。

- クレーム発行要求時：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（処理③）
- クレーム発行時：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（処理④）
- クレーム検証時：ユーザのウォレットを介しクレームを受け取ったRPは、そのクレームが、相對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（⑦）。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。

### クレーム発行時におけるBindingの考慮箇所



## (参考) Bindingにおける考慮事項 – Bindingの実装例

- 例えば OpenID Foundationの策定する “OpenID Connect Claims Provider”<sup>\*1)</sup>では、それぞれ以下の処理を規定している。
  1. 前頁の「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」<sup>\*2)</sup>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。
  2. 前頁の「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（Universally Unique Identifier）やDIDの識別子、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。

#### 処理③：クレーム発行要求と、DID所有者との紐付け・確認

##### 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

#### 処理④/⑦：クレームと、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

DID識別子

##### クレーム上での紐付情報記載例<sup>\*1)</sup>

```
{ (中略)
  "credentialSubject": {
    "id": "urn:uuid:dc000c79-xx (中略)",
    (中略)
  }
}

{ (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）


\*1) “OpenID Connect Credential Provider”, <http://lists.openid.net/pipermail/openid-specs-ab/attachments/20210528/2f163c71/attachment-0001.bin>

\*2) “OpenID Connect Core 1.0 incorporating errata set 1”, <https://openid.net/specs/openid-connect-core-1.0.html#RequestUriParameter>

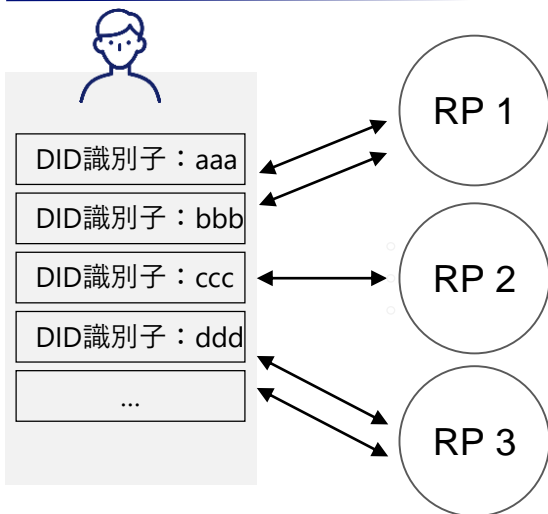
## (参考) Bindingにおける考慮事項 – DID識別子を用いたBinding時の懸念 (1 / 3)

- 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、下図の様に複数の使い方が想定される。このうち、RP毎に異なるDID識別子を使用する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 (次頁にて詳述)。

### DID識別子の使い方

凡例)  同一のDID識別子を利用

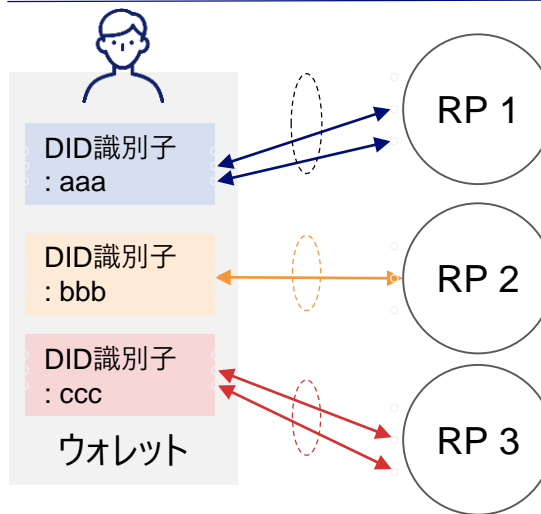
#### “Ephemeral” なDID識別子の利用ケース



- RP毎に異なるDID識別子を利用
- 同じRPでも毎回異なるDID識別子を利用 (One-use)

DID識別子による名寄せ懸念無し

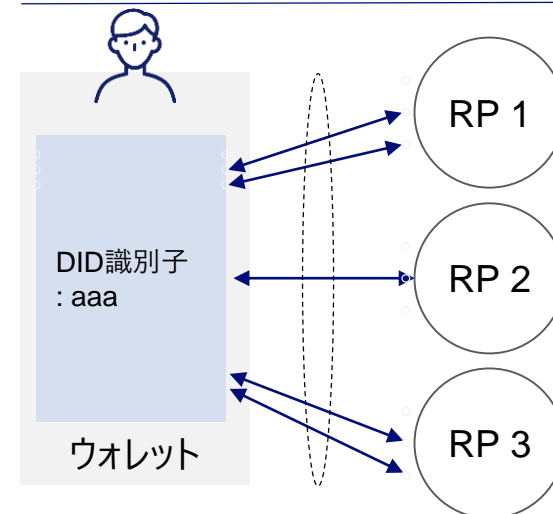
#### “Pairwise” なDID識別子の利用ケース



- RP毎に異なるDID識別子を利用
- 同じRPに対しては、毎回同じDID識別子を利用

RP毎にDID識別子を変えることでRP間による名寄せを回避したい

#### “Omni Directional” なDID識別子の利用ケース



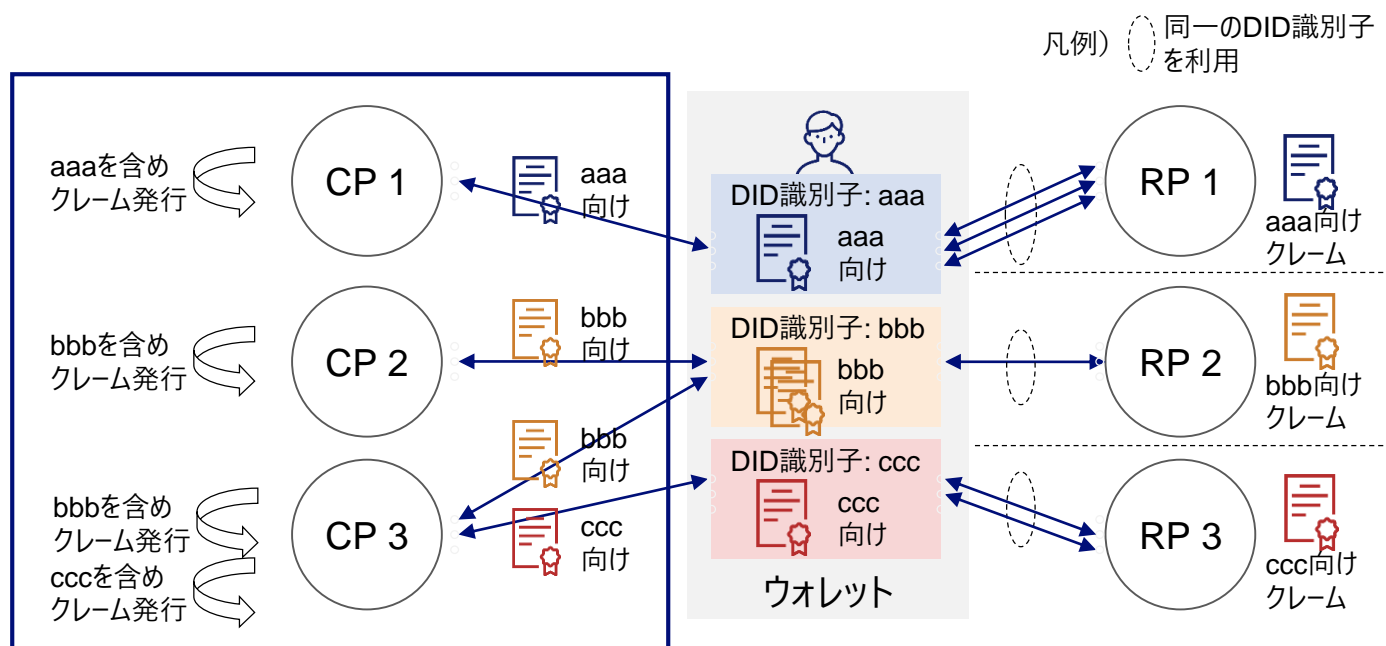
- RP毎に同じDID識別子を利用
- 同じRPに対しては、毎回同じDID識別子を利用

RP間で名寄せされる前提で利用

## (参考) Bindingにおける考慮事項 – DID識別子を用いたBinding時の懸念 (2 / 3)

- 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。

“Pairwise” なDID識別子利用におけるクレーム連携のイメージ



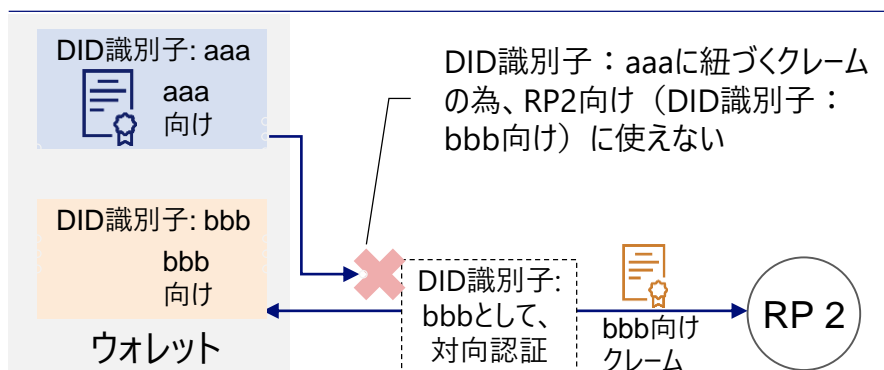
CPは、指定されたDID識別子をクレームにBindingして、クレーム発行を行う必要がある。



## (参考) Bindingにおける考慮事項 – DID識別子を用いたBinding時の懸念 (3 / 3)

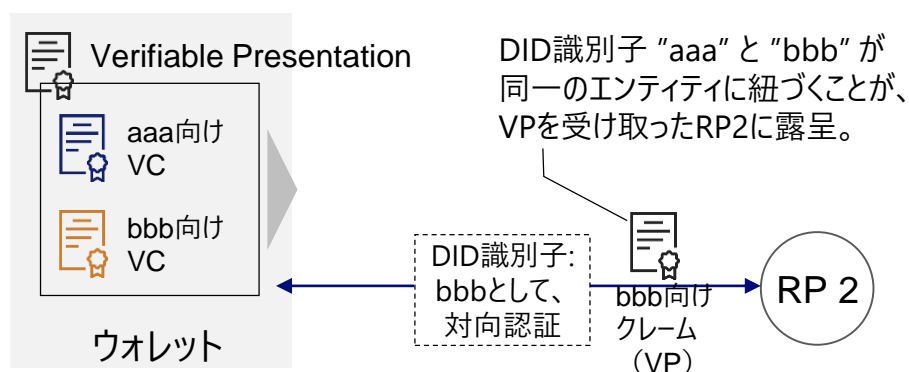
- RP2 のサービス利用におけるオンボーディング時、ユーザはまずRP2 向けにDID識別子を発行し、クレーム提示の準備を始める。その際、既に発行済のクレームを使おうとしても、同クレームはRP1 向けに新たに作成したDID識別子と紐付いていない為、新たにクレームを取り直す必要が生じる (DID識別子に応じたDynamicなクレームの生成・取得が必須となり、3-1-2.項で述べた「長期のデジタルアイデンティティの保管・利用」の特性への制約となる懸念がある)。
- また、W3C Verifiable Credentials Data Model 1.0のVerifiable Presentation (VP) では、複数VCを格納可能と規定されている\*1)。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。

懸念①：Staticなクレームの利用が困難



- 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)

懸念②：クレーム集約時に、包含するクレームと紐づいているDID識別子同士が、紐付いてしまう



- 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。

\*1) "Verifiable Credentials Data Model 1.0", <https://www.w3.org/TR/vc-data-model/>

## (参考) Bindingにおける考慮事項：サマリー

- 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。

#### Bindingにおける要件

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)

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)

#### DID識別子を用いたBindingにおける懸念事項

- 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、過去にウォレット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.項で述べた「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)
- 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<sup>\*1)</sup>)、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)

\*1) "Verifiable Credentials Data Model 1.0", <https://www.w3.org/TR/vc-data-model/>

### 3-2-2. 技術構成要素に対する各標準化団体の議論動向

## 技術構成要素の各標準化団体の検討仕様

- 以下ユースケースを対象に、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を行う。

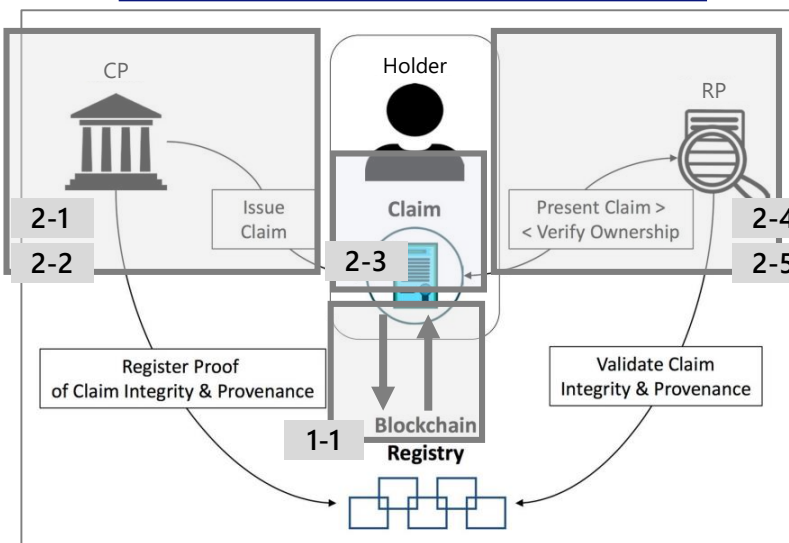
#### 1. DIDの登録処理

ユーザがID Proofingを行い、DIDのActivation処理が完了し、DIDが有効状態に遷移するまでの処理を行う。

#### 2. クレームの連携処理

ホルダーがDIDを取得後にIdPとなり、CP / ホルダー間、及びホルダー / RP間でのクレーム連携処理を行う。

SSI/DIDの処理フローの概観



処理	処理概要
1. DIDの登録処理（DIDが有効状態に遷移するまでの処理）	
1-1. DIDおよびメタデータの生成・登録	DIDおよびメタデータの生成・登録を実施
2. クレームの連携処理	
2-1. CP上のユーザとDID所有者のBinding	<ul style="list-style-type: none"> <li>ユーザがCP内のCSPに対しAuthenticationを実行</li> <li>CPは、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を実施</li> </ul>
2-2. クレーム発行	2-1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
2-3. ウォレットへのクレーム格納	2-2) で取得したクレームをウォレットに格納・保持
2-4. RPに対するユーザ認証	ウォレットとRP間で、1-1) のDIDおよびメタデータを用い対向認証
2-5. クレーム連携	<ul style="list-style-type: none"> <li>2-4)で対向の認証が完了後、2-3)で取得したクレームを連携。</li> <li>RPは、受領したクレームが、2-4)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</li> </ul>

### 3-2-2. 技術構成要素に対する各標準化団体の議論動向

## 技術構成要素の各標準化団体の検討仕様

点線で囲われた仕様は、他団体で定義された仕様を参照する方針を意味する

#	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

※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、策定途上など今後記載内容の変動が想定されたため、本調査では詳細の記述を割愛する。



### 3-2-2. 技術構成要素に対する各標準化団体の議論動向

## OpenID Foundationによる実現アプローチ

- 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（当人認証）を行った上で、ユーザをハブとするクレーム連携の仕様の策定を進めている。
- 属性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とのリエゾン締結し共に議論を進めている。

### OpenID Connect Core 1.0 – Self Issued OpenID Provider

#### 7. Self-Issued OpenID Provider TDC

OpenID Connect supports Self-Issued OpenID Providers - personal, self-hosted OPs that issue self-signed ID Tokens. Self-Issued OPs use the special Issuer Identifier <https://self-issued.me>.

The messages used to communicate with Self-Issued OPs are mostly the same as those used to communicate with other OPs. Specifications for the few additional parameters used and for the values of some parameters in the Self-Issued case are defined in this section.

---

#### 7.1. Self-Issued OpenID Provider Discovery TDC

If the input identifier for the discovery process contains the domain `self-issued.me`, dynamic discovery is not performed. Instead, then the following static configuration values are used:

```
{
  "authorization_endpoint":
  "openid",
  "issuer":
  "https://self-issued.me",
  "scopes_supported":
  ["openid", "profile", "email", "address", "phone"],
  "response_types_supported":
  ["id_token"],
  "subject_types_supported":
  ["pairwise"],
  "id_token_signing_alg_values_supported":
  ["RS256"],
  "request_object_signing_alg_values_supported":
  ["none", "RS256"]
}
```

NOTE: The OpenID Foundation plans to host the OpenID Provider site <https://self-issued.me/>, including its WebFinger service, so that performing discovery on it returns the above static discovery information, enabling RPs to not need any special processing for discovery of the Self-Issued OP. This site will be hosted on an experimental basis. Production implementations should not take a dependency upon it without a subsequent commitment by the OpenID Foundation to host the site in a manner intended for production use.

---

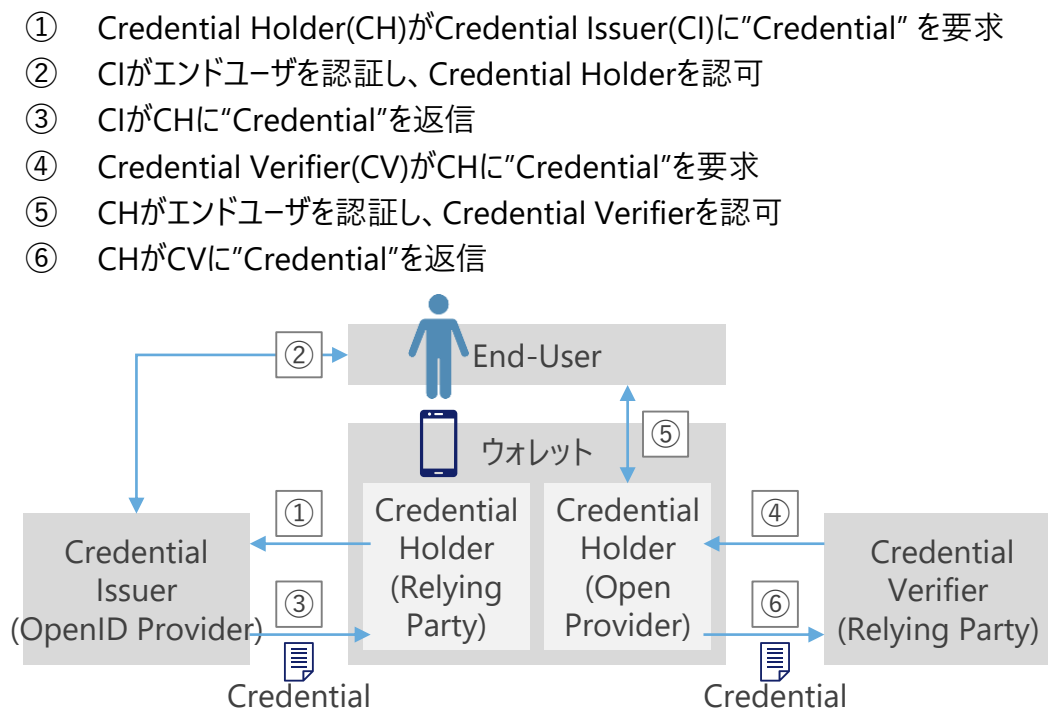
#### 7.2. Self-Issued OpenID Provider Registration TDC

When using a Self-Issued OP, registration is not required. The Client can proceed without registration as if it had registered with the OP and obtained the following Client Registration Response:

```
client_id
redirect_uri value of the Client.
client_secret_expires_at
0
```

NOTE: The OpenID Foundation plans to host the (stateless) endpoint <https://self-issued.me/registration/1.0/> that returns the response above, enabling RPs to not need any special processing for registration with the Self-Issued OP. This site will be hosted on an experimental basis. Production implementations should not take a dependency upon it without a subsequent commitment by the OpenID Foundation to host the site in a manner intended for production use.

### OpenID Connect Credential Provider



※生成されるCredentialとDID間のBindingは、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る

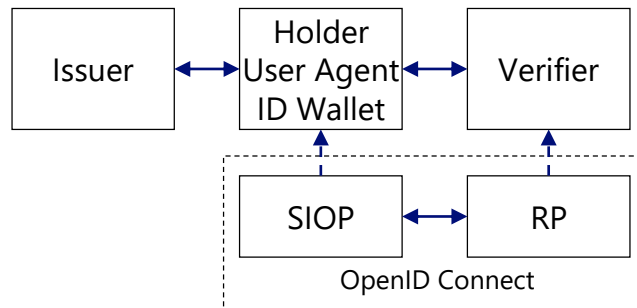
### 3-2-2. 技術構成要素に対する各標準化団体の議論動向

## DIFによる実現アプローチ

- 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/提示が可能な仕様策定も行っている。

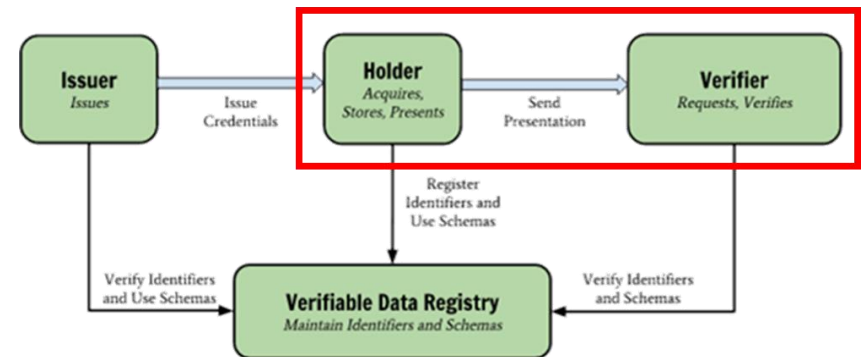
#### OpenID Foundationとのリエゾン背景（OIDC選択理由）

- Well-known and mature
- Widely used, and has a big community
- Enterprises are familiar with OIDC
- Simple and light-weight
- Flexible and extensible through profiles
- Additional (optional) support for credentials/ claims exchange
- Based on work incubated at RWOT, and IIW



#### クレーム要求/提示に関する仕様策定（Presentation Exchange）

- HolderおよびRP間におけるProofの要求/提示を規定
- 以下の形式に対応することでOpenID Connect, DID Comm、Credential Handler APIを介し連携可能
  - JSON Web Tokens (JWTs)
  - Verifiable Credentials (VCs)
  - JWT-VCs

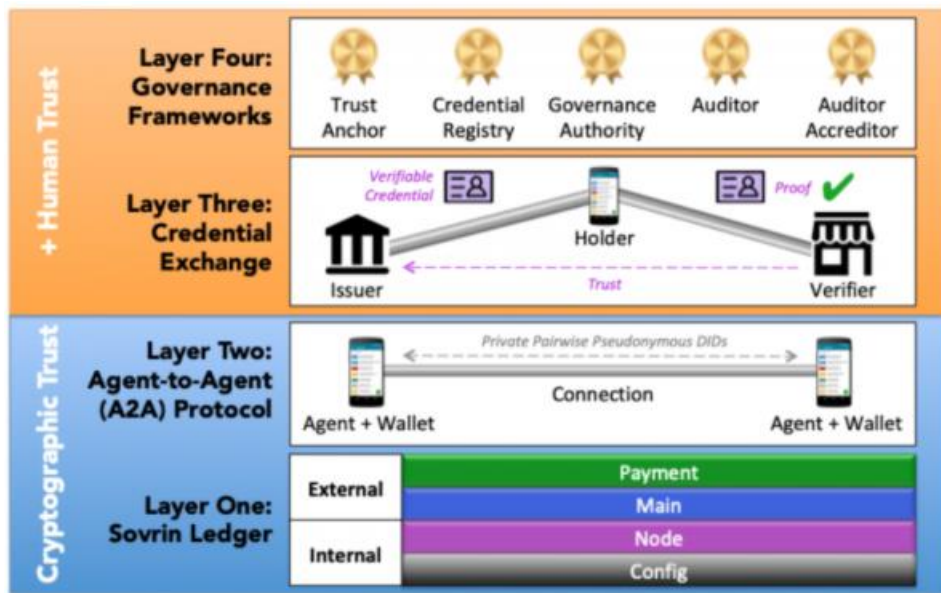


### 3-2-2. 技術構成要素に対する各標準化団体の議論動向

## Sovrinによる実現アプローチ

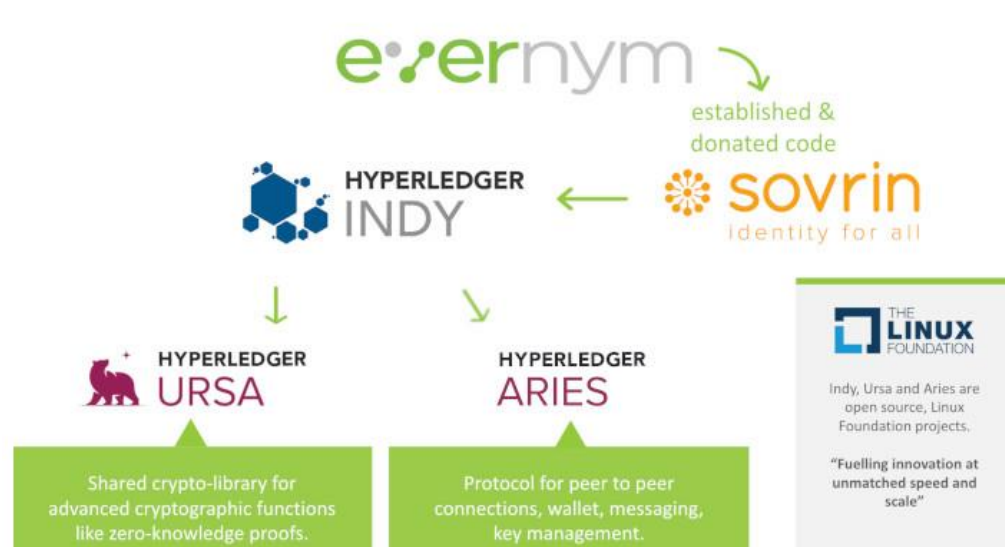
- Sovrin Foundationは、SSIモデルの実現に必要な「Sovrin Governance Framework」を規定し、法的協定や用いる技術仕様・標準・ポリシー、同フレームワークのポリシー適合性評価のための基準とプロセス等を定義している。また、同フレームワーク内では、構成スタックとして「Sovrin Stack」と呼ばれる4層のLayerを定義している。
- 規範的な構成要素として、W3CのDIDs、VC Data Model、DID Method 1.0 Specificationが言及されている。また、DID/DID Document管理の為に分散台帳技術としては、Evernym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。
  - 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。

Sovrin FoundationによるSovrin Stack図



出所) Sovrin Foundation  
<https://sovrin.org/wp-content/uploads/Sovrin-Governance-Framework-V2-Master-Documents-V2.pdf>  
<https://sovrin.org/2020-how-ssi-went-mainstream/>

Hyperledger Indy及び関連プロジェクトの設立経緯



出所) Evernym Hyperledger Aries: The Next Major Step Towards Interoperable SSI  
<https://www.evernym.com/blog/hyperledger-aries/>



### 3-2-3. 各標準化団体の検討仕様

## 各仕様の概要

- 本項では、以下の仕様の概要についてまとめる。

なお、A-2) OpenID Connect Claims Aggregationについては、セキュリティ考慮事項の項がTBDとなっており、本調査では課題については記述を割愛する。

#	団体名	仕様名
A-1)	OIDF	OpenID Connect Core
A-2)	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 0.1
C-1)	DIF	Self-Issued DID Profile for OpenID v1.0
C-2)	DIF	Presentation Exchange
D-1)	Hyperledger	Aries RFC 0023: DID Exchange Protocol 1.0
D-2)	Hyperledger	Aries RFC 0036: Issue Credential Protocol 1.0
D-3)	Hyperledger	Aries RFC 0037: Present Proof Protocol

## A-1) OpenID Connect Core

- OpenID Connect Core（以下、「OIDC」と記述）はOpenID Foundationにより2014年に策定された仕様であり、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。
- 同仕様の中で、ユーザ自身がIdPとして振る舞う「Self-Issued OpenID Provider」（以下「SIOP」と記述）という方式が言及されている。
  - OIDC Core Ch.7 Self-Issued OpenID Provider
    - 「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。
    - 同方式を用いることで、既存のIdP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。

## OpenID Connect Core 1.0 - SIOP

### 7. Self-Issued OpenID Provider TOC

OpenID Connect supports Self-Issued OpenID Providers - personal, self-hosted OPs that issue self-signed ID Tokens. Self-Issued OPs use the special Issuer Identifier <https://self-issued.me>.

The messages used to communicate with Self-Issued OPs are mostly the same as those used to communicate with other OPs. Specifications for the few additional parameters used and for the values of some parameters in the Self-Issued case are defined in this section.

#### 7.1. Self-Issued OpenID Provider Discovery TOC

If the input identifier for the discovery process contains the domain self-issued.me, dynamic discovery is not performed. Instead, then the following static configuration values are used:

```
{
  "authorization_endpoint":
  "openid:",
  "issuer":
  "https://self-issued.me",
  "scopes_supported":
  ["openid", "profile", "email", "address", "phone"],
  "response_types_supported":
  ["id_token"],
  "subject_types_supported":
  ["pairwise"],
  "id_token_signing_alg_values_supported":
  ["RS256"],
  "request_object_signing_alg_values_supported":
  ["none", "RS256"]
}
```

NOTE: The OpenID Foundation plans to host the OpenID Provider site <https://self-issued.me/>, including its WebFinger service, so that performing discovery on it returns the above static discovery information, enabling RPs to not need any special processing for discovery of the Self-Issued OP. This site will be hosted on an experimental basis. Production implementations should not take a dependency upon it without a subsequent commitment by the OpenID Foundation to host the site in a manner intended for production use.

#### 7.2. Self-Issued OpenID Provider Registration TOC

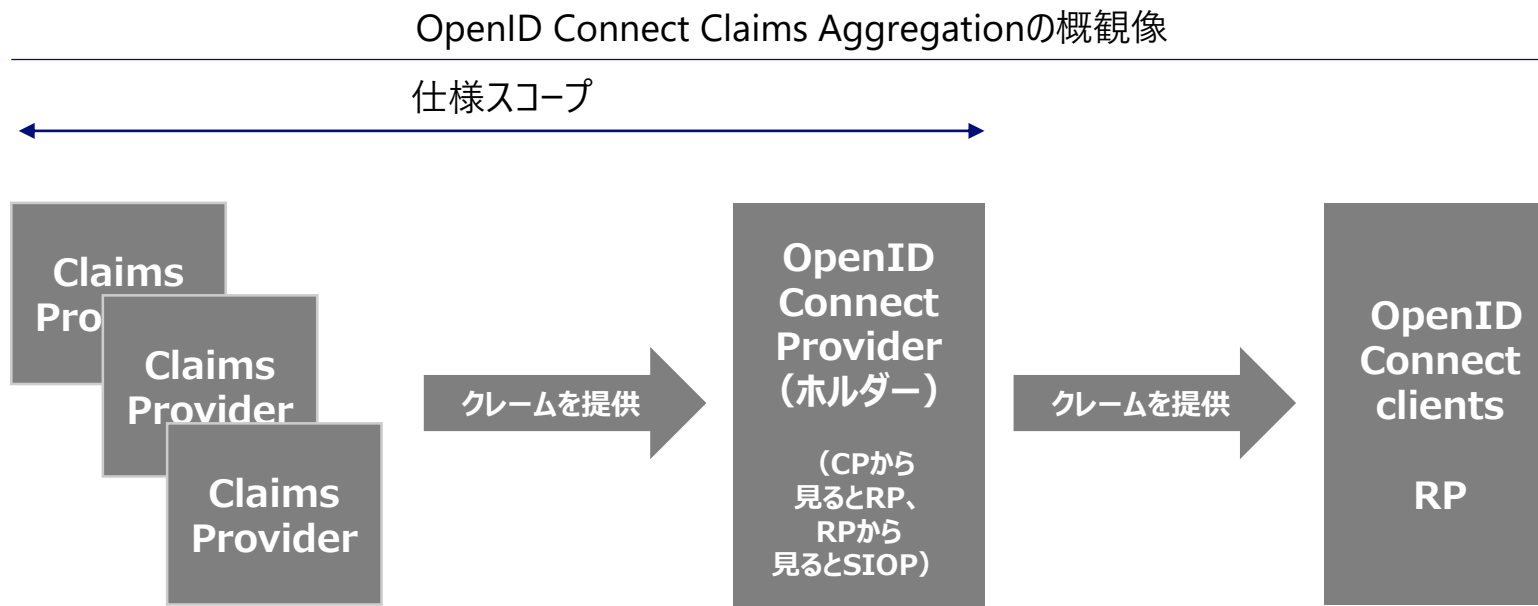
When using a Self-Issued OP, registration is not required. The Client can proceed without registration as if it had registered with the OP and obtained the following Client Registration Response:

```
client_id
redirect_uri value of the Client.
client_secret_expires_at
0
```

NOTE: The OpenID Foundation plans to host the (stateless) endpoint <https://self-issued.me/registration/1.0/> that returns the response above, enabling RPs to not need any special processing for registration with the Self-Issued OP. This site will be hosted on an experimental basis. Production implementations should not take a dependency upon it without a subsequent commitment by the OpenID Foundation to host the site in a manner intended for production use.

## A-2) OpenID Connect Claims Aggregation

- 本仕様は、クレームプロバイダーから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を規定している。
  - OpenID Providerは、Claims Provider（以下、「CP」）に対して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、Relying Party（以下、「RP」）の役割を果たす。
  - 同仕様では、CPからOpenID Connect Providerにクレームが提供されるまでの処理が仕様策定範囲であり、OpenID Connect ProviderからRelying Partyへのクレーム提供は仕様策定範囲外となる。
  - OpenID Providerはエンドユーザのすべてのクレーム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に共有できる。

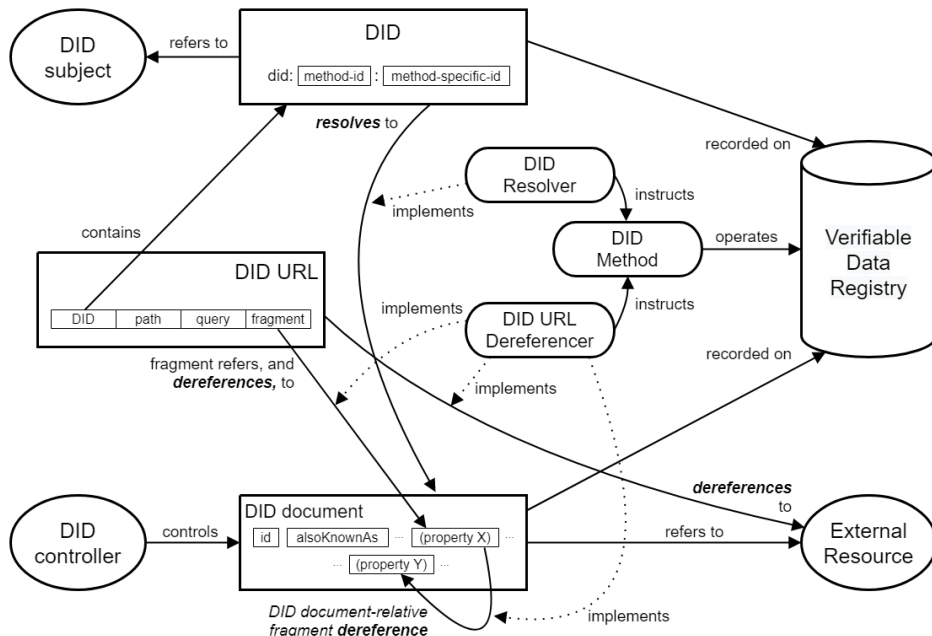


### 3-2-3. 各標準化団体の検討仕様

## B-1) Decentralized Identifiers (DIDs) v1.0

- DIDs v1.0はDIDのシンタックス、データモデル、プロパティ、シリアル化された表現、DIDの操作およびDIDが表すリソースを解決するプロセスを規定している（下表参照）。
- 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的な識別子を、分散型アイデンティファイア(DID)として定義している。

Decentralized Identifiers (DIDs) v1.0



出所) Decentralized Identifiers (DIDs) v1.0

規程対象	概要
DIDs とDID URLs	DIDはスキーム(did)、メソッド識別子(method identifier)、DID methodから生成される識別子(method-specific identifier)の3パートから構成されるテキスト形式の文字列。DIDは永続的で不変であり、非活性化後も再利用されないことが要求される。
DID Subjects	DIDによって識別されるエンティティ。DID Controllerである場合もある。人、グループ、組織、物理的、論理的なものでも可能。
DID Documents	DID関連のメタデータ、公開鍵による検証方法、DID subjectとのやり取りに関連したサービスを示す抽象的なデータモデル。
DID Methods	Verifiable Data Registriesを使って、DIDとそれに関連したDID Documentsを生成、解決、後進、非活性化する方法を指定する。
DID Controllers	DID ControllerはDID Methodで定義されるように、DID Documentを変更可能なエンティティで、人、組織、自律型ソフトウェア。
Verifiable Data Registries	分散台帳、分散ファイルシステム、データベース、P2Pネットワーク、信頼できるストレージのことで、DIDの記録やDIDドキュメントの生成に必要なデータを返すシステム。
DID resolverとDID resolution	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。当該処理をDID resolutionと呼ぶ。
DID URL dereferencers と DID URL dereferencing	DID URL間接参照は、DID URL(および関連メタデータ)を入力として受け取り、リソース(および関連メタデータ)を出力として生成するソフトウェア、ハードウェアコンポーネント。当該処理をDID URL 間接参照(リファレンス先参照)と呼ぶ。

## B-1) Decentralized Identifiers (DIDs) v1.0 – 課題と新たな取り組み

- セキュリティ考慮事項として、下記点が挙げられている。

考慮事項	概要(1/2)
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。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。

## B-1) Decentralized Identifiers (DIDs) v1.0 – 課題と新たな取り組み

- セキュリティ考慮事項として、下記点が挙げられている。

考慮事項	概要(2/2)
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。

## B-1) Decentralized Identifiers (DIDs) v1.0 – 課題と新たな取り組み

- プライバシー考慮事項として、下記点が挙げられている。

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かもしれない。
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 1.0

- 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上でクレデンシャルを表現するためのメカニズムを提供する。学歴資格、医療データ、銀行口座等の第三者が検証したmachine-readableな各種個人情報情報をWeb上で表現することを可能にする。

Verifiable Credentials Data Model 1.0

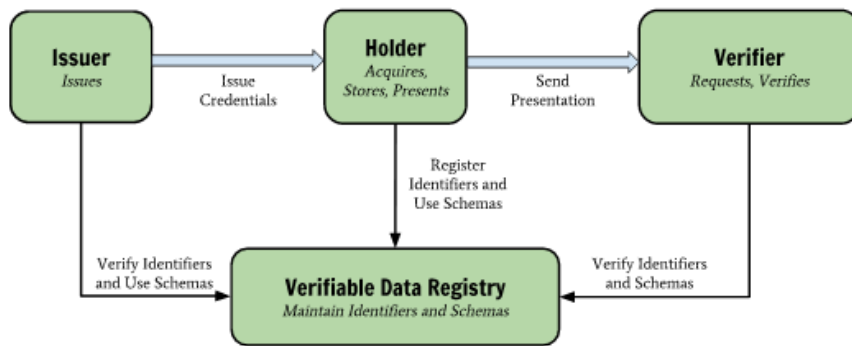


Figure 1 The roles and information flows forming the basis for this specification.

Actor	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



## B-2) Verifiable Credentials Data Model 1.0 – 課題と新たな取り組み

- セキュリティ考慮事項として、下記点が挙げられている。

考慮事項	概要
Cryptography Suites and Libraries	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。
Content Integrity Protection	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。
Unsigned Claims	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。
Token Binding	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。
Bundling Dependent Claims	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。
Highly Dynamic Information	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。
Device Theft and Impersonation	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。 <ul style="list-style-type: none"> <li>・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</li> <li>・Credential Repositoryでパスワード、生体または多要素認証を有効にする</li> <li>・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</li> <li>・別のハードウェアベースの署名デバイスを使用する</li> <li>・上記のすべてまたは任意の組み合わせをとる</li> </ul>

## B-2) Verifiable Credentials Data Model 1.0 – 課題と新たな取り組み

- プライバシー考慮事項として、下記点が挙げられている。

考慮事項	概要(1/3)
Personally Identifiable Information	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。
Identifier-Based Correlation	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。
Signature-Based Correlation	Verifiable Credentialの内容は、proof フィールドを使用して保護される。このフィールドのプロパティは、複数のセッションまたはドメインにまたがって同じ値が使用され、値が変更されない場合、相関関係のリスクが大きくなるため、署名とメタデータを毎回再生成することが推奨される。
Long-Lived Identifier-Based Correlation	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。
Bundling Dependent Claims	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。
Device Fingerprinting	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。
Favor Abstract Claims	Verifiable Credentialの受信者は、取引に必要な以上の PII を明らかにすることができないよう、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。

## B-2) Verifiable Credentials Data Model 1.0 – 課題と新たな取り組み

- プライバシー考慮事項として、下記点が挙げられている。

考慮事項	概要(2/3)
The Principle of Data Minimization	<p>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。</p>
Bearer Credentials	<p>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。</p>
Validity Checks	<p>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</p> <ul style="list-style-type: none"> <li>• Holderの専門職免許のステータス</li> <li>• ライセンスの更新日又は失効日</li> <li>• 個人の下位資格</li> <li>• HolderとHolderが交流しようとしている事業者間の関係</li> <li>• Holderに関連する地理的位置情報</li> </ul> <p>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せん。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。</p>
Storage Providers and Data Mining	<p>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、人や組織別プロフィー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。</p> <ul style="list-style-type: none"> <li>• 顧客情報を第三者に販売しないサービスプロバイダー</li> <li>• サービスプロバイダー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</li> <li>• 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</li> </ul>

### 3-2-3. 各標準化団体の検討仕様

## B-2) Verifiable Credentials Data Model 1.0 – 課題と新たな取り組み

- プライバシー考慮事項として、下記点が挙げられている。

考慮事項	概要(3/3)
Aggregation of Credentials	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。
Usage Patterns	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。
Sharing Information with the Wrong Party	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。
Frequency of Claim Issuance	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。
Prefer Single-Use Credentials	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。
Private Browsing	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。ブラウザベンダー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

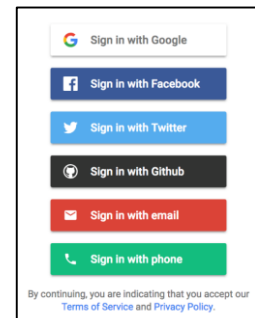
- Credential Handler API (CHAPI) はブラウザ上でクレデンシャルの要求および保管に関するイベントをハンドリングするAPIであり、Payment Handler APIとCredential Management APIの2つをベースとして構成されている。
- 本仕様では、下記の点を目的として規定されている。
  - ユーザのクレデンシャルの利用をより簡単かつ安全にする。
  - ユーザがウォレットプロバイダーを選択できるようにする。
  - Webアプリ開発者に標準的なウォレットAPIを提供する。
- その他にもOAuth 2.0/OIDCにおけるNASCAR problemの解決なども規定されている。

### Credential Handler API策定のタイムライン

- W3C CCG (Credentials Community Group) にて仕様が公開。
  - 2014年 - Identity Credentials protocolが提案
  - 2017年 - Web Payments HandlerがDave Longleyによって提案
  - 2017年 - CHAPIがDave Longleyによって提案
  - 2017年 - CHAPIがW3C CCGで仕様の策定が進められる

### NASCAR problem

- NASCAR problemはサードパーティのアイコンやブランドがウェブサイト上に集まり視覚的なノイズとなる問題である。具体例としては、Payment UIやサインインUIなどが挙げられている。



## B-3) Credential Handler API

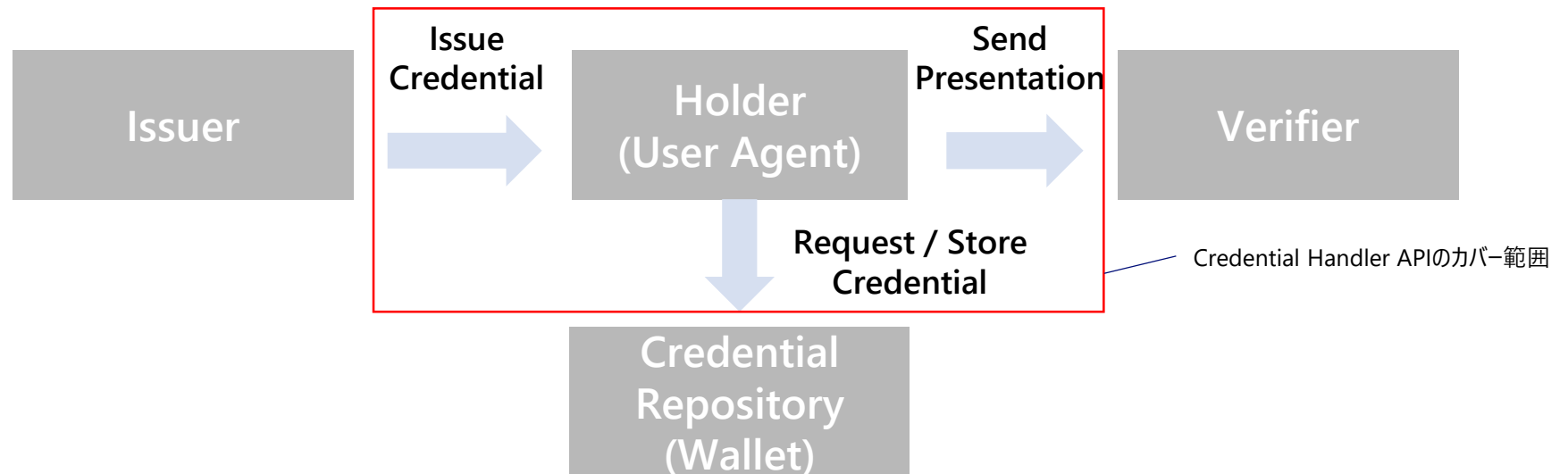
### ■ 処理内容

- CredentialRequestEventやCredentialStoreEventといったCredentialの要求や保管に関するイベントが定義。
- オリジンベースでCredentialの要求および保管のイベントを処理。

### ■ ロール

- Credential Repository (Wallet): ユーザのCredentialの保管と要求を処理。
- Credential Issuer (Issuer): ユーザにCredentialを発行。
- Credential Verifier (Verifier): ユーザにCredentialを要求。
- Mediator (User Agent): Credentialの保管と要求を仲介。

Credential Handler APIの概観像



## B-3) Credential Handler API – 課題と新たな取り組み

- セキュリティおよびプライバシー考慮事項として、下記点が挙げられている。

考慮事項	概要
ユーザ環境に関する情報	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 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 0.1

- Confidential Storageでは、暗号化されたデータをストレージプロバイダーで保管、インデックス作成、検索するためのプライバシーを尊重したメカニズムを提供する。これは、個人や組織が、ストレージプロバイダーがデータを閲覧、分析、集計、再販できないようにデータを保護したい場合に有用である。このアプローチは、アプリケーションデータがポータブルであり、ストレージプロバイダーのデータ侵害から保護されていることを保証する。

### Confidential Storageエコシステム概観

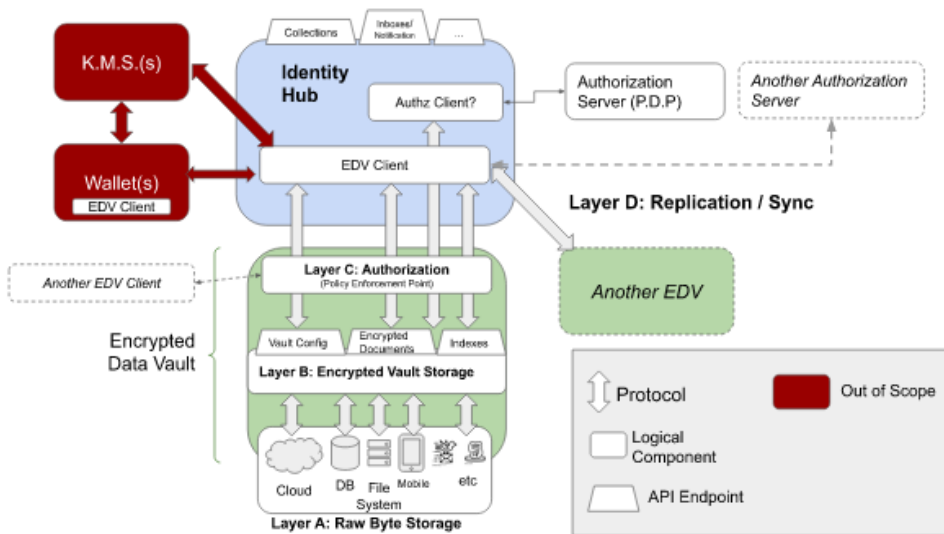


Figure 1 Confidential Storage layers

要件	概要
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。



## B-4) Confidential Storage 0.1 – 課題と新たな取り組み

- セキュリティ考慮事項として、下記点が挙げられている。

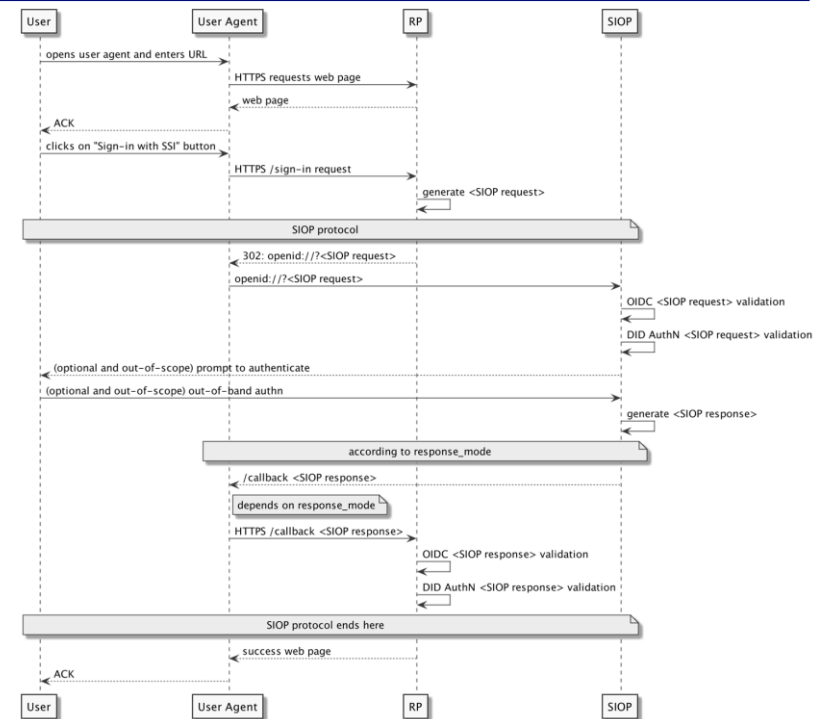
考慮事項	概要
Malicious or accidental modification of data	<ul style="list-style-type: none"> <li>サービスプロバイダーはEncrypted Data Vault内のデータを読み取ることはできないが、サービスプロバイダーが暗号化データを削除、追加、変更することは可能である。暗号化データの削除、追加、変更は、data vault内のデータのグローバルマニフェストを保持することで防げる。</li> </ul>
Compromised vault	<ul style="list-style-type: none"> <li>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。</li> </ul>
Data access timing attacks	<ul style="list-style-type: none"> <li>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。</li> </ul>
Encrypted data on public networks	<ul style="list-style-type: none"> <li>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。</li> </ul>
Unencrypted data on server	<ul style="list-style-type: none"> <li>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。</li> </ul>
Partial matching on encrypted indexes	<ul style="list-style-type: none"> <li>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。</li> </ul>
Threat model for malicious service provider	<ul style="list-style-type: none"> <li>悪意のあるサービスプロバイダーによる以下の攻撃が考えられる。 <ul style="list-style-type: none"> <li>✓ 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</li> <li>✓ 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</li> <li>✓ 暗号化されたデータの追加・削除・変更</li> <li>✓ 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</li> <li>✓ 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</li> </ul> </li> </ul>

## C-1) Self-Issued DID Profile for OpenID v1.0

- Self-Issued DID Profile for OpenID (SIOP DID) は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 \*1)にOpenID Connectを使用するための仕様である。
- RPはWebアプリケーションが想定されており、モバイルアプリケーションやデスクトップブラウザからIdentity Walletアプリケーションを起動して利用する。
- 全体的な処理フローはOIDC Core 7. Self-Issued OpenID Providerにしたがって行われる。

SIOP DID処理フロー

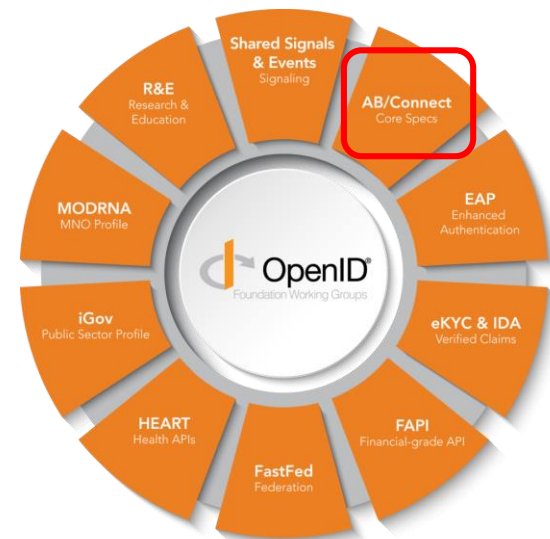
1. UserはRPにアクセス
2. RPは"Sign-in with SSI"ボタンを返し、Userがこれを押下するとSIOP Requestが生成
3. SIOP Request (openid://?<SIOP request>)によりSIOPが起動
4. SIOPはOIDC/DID AuthNに従ってSIOP requestを検証しSIOP responseを生成
5. response\_modeの指定に従ってRPにSIOP Responseがわたされる
6. RPはOIDC/DID AuthNに従ってSIOP responseを検証する。



### 3-2-3. 各標準化団体の検討仕様

## C-1) Self-Issued DID Profile for OpenID v1.0 – 課題と新たな取り組み

- 2020年11月9日 OIDFとDIFのLiaison Agreement締結に伴い、SIOP DIDの作業は一時停止することが表明されている。
  - 今後はOIDF AB/Connect WGによってOIDC Coreの7. SIOPの改訂が進められる。
  - AB/C WGによるSIOP仕様の作業が完了した後、DIF Authentication WGで作業が再開される予定である。



### OpenID Foundationにおける議論

Requirements for OIDC Self-Issued OpenID Providerに記載のScopeを中心に議論。

#### ■ Scope

- A. SIOP request
- B. SIOP response
- C. Key recovery and key rotation
- D. Trust model between RP and SIOP
- E. Issuance of the claims
- F. Privacy protection

### DIFにおける議論

2021年1月 DIF Face to Faceコミュニティイベントにおいて仕様検討状況を公表。

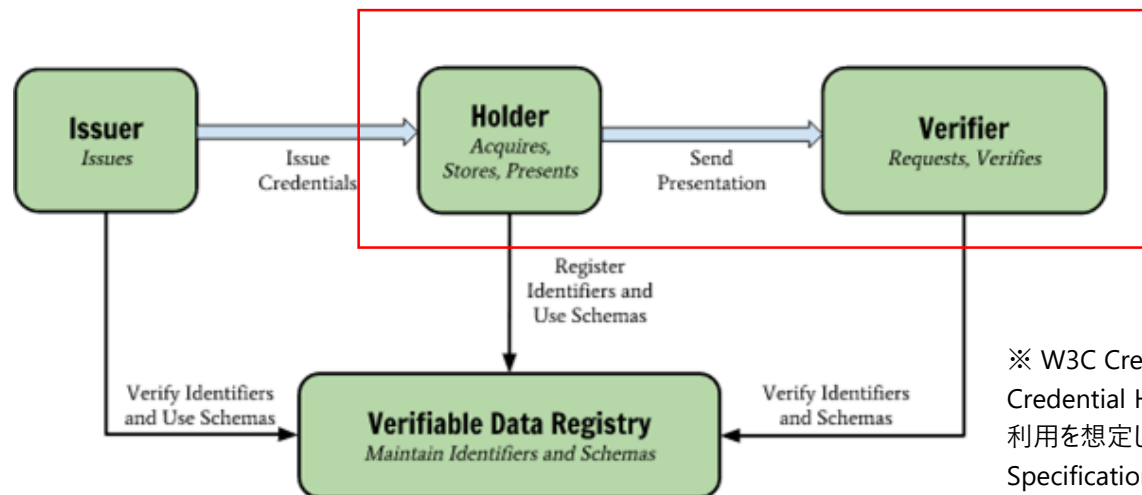
#### ■ Current Draft

- 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

- Presentation ExchangeはVerifierがProofの要件を明確にするためのデータフォーマットおよびHolderが要件に沿ってProofを提示するためのデータフォーマットを定義する。
- Presentation Exchangeはクレームフォーマットやトランスポートプロトコルに依存しないメカニズムとすることで冗長な処理、コード、手間を省くことを目的としている。
- サポートしているClaimフォーマットおよびトランスポートプロトコルの一例は以下の通りである。
  - クレームフォーマット: JSON Web Token (JWT) 、 Verifiable Credential (VC) 、 JWT Verifiable Credential (JWT-VC)
  - トランスポートプロトコル: OpenID Connect、 DIDComm、 Credential Handler API

Presentation Exchangeの概観像



※ W3C Credential Community Groupにて Credential Handler APIでの利用を想定したVerifiable Presentation Request Specificationが別途存在

## C-2) Presentation Exchange – Presentation Definition & Presentation Submission

- HolderおよびVerifier間におけるProofの要求と提示は以下の用語で定義される。
  - **Presentation Definition:** Verifierが必要とするProofを定義。
  - **Presentation Request:** VerifierからHolderに対するPresentation Definitionの転送方法を定義。
  - **Presentation Submission:** Verifierが指定したPresentation Definitionに従ってProofを提示する方法を定義。

### Presentation Definitionオブジェクトを用いた定義例

```
{
  "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"
        }]
      }
    ]
  }
}
```

### Presentation Submissionオブジェクトを用いた定義例

```
{
  // 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]"
      }
    ]
  }
}
```

## C-2) Presentation Exchange – 課題と新たな取り組み

### ■ セキュリティ考慮事項

- 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。<sup>\*1)</sup>
- 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。<sup>\*1)</sup>

### ■ 今後の取り組み

- 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。<sup>\*2)</sup>
- GitHubのIssue上ではPresentation Exchangeがサポートするトランスポートプロトコルである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。<sup>\*3) \*4)</sup>

\*1) Security Considerations, <https://github.com/decentralized-identity/presentation-exchange/issues/204>

\*2) I1W30 CHAPI and DID Comm 101, <https://docs.google.com/presentation/d/1qPbwx9IXwPlgsZgS2XPXeGgstxrixnC8n0E2I4cxVc8/edit>

\*3) What does PE look like within OpenID Connect? #101, <https://github.com/decentralized-identity/presentation-exchange/issues/101>

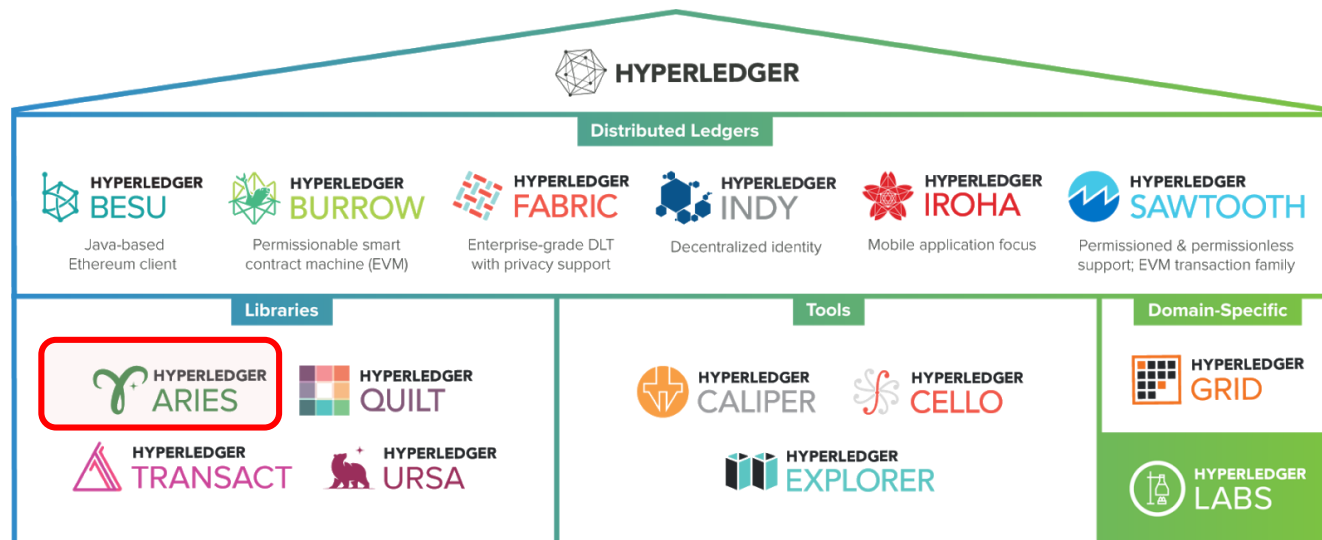
\*4) Examples that show support for regular OIDC flow, <https://github.com/decentralized-identity/presentation-exchange/issues/92>

### 3-2-3. 各標準化団体の検討仕様

## D) Aries RFC

- Hyperledger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 Ariesプロジェクトはmessage exchangeプロトコル、エージェントのアーキテクチャおよびテストの定義や共有を目的としている。
  - Aries プロジェクトを構成するコンセプトと機能はHyperledger aries-rfcs GitHubリポジトリで文書化されている。
  - Aries RFCはconcepts (すべてのプロトコルにまたがる背景情報) とfeatures (特定のプロトコルの仕様) の2つのグループで定義されている。
  - Hyper Ledger Indyには、indy-hipeと呼ばれるaries-rfcに相当するリポジトリが別途存在する。

### HyperledgerプロジェクトにおけるHyperledger Ariesプロジェクトの立ち位置



### 3-2-3. 各標準化団体の検討仕様

## D-1) Aries RFC 0023: DID Exchange Protocol 1.0

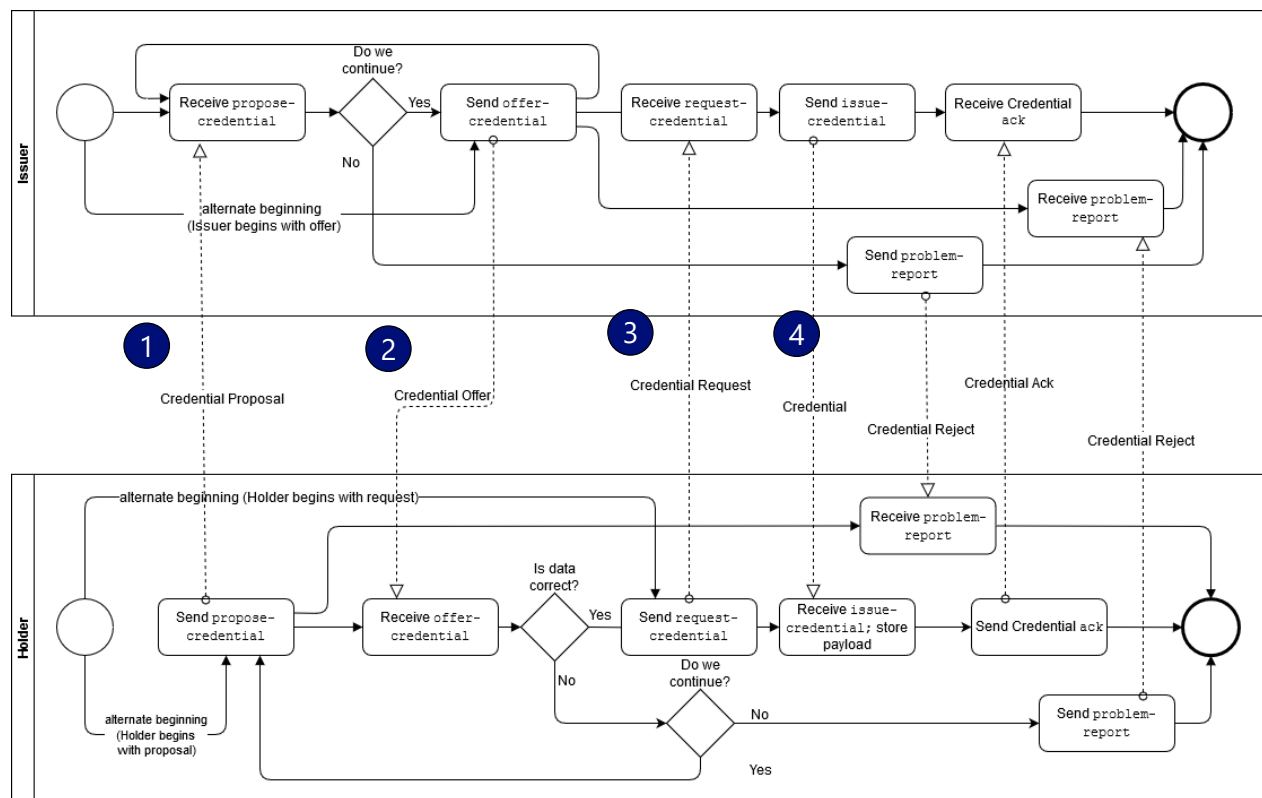
- 本仕様では、Agent間でDIDを交換するためのプロトコルを規定している。
- 以下の2つのロールを規定している。
  - Requester  
invitationメッセージを受信し後、またはPublic DIDからの暗黙的な招待を使用して、このプロトコルを開始する当事者。
  - Responder  
invitationの送信者または暗黙的な招待をもつDIDの発行者。DIDCommを介して他のAgentと対話できる必要がある。
- 処理フローの概要は、以下の通りである。
  1. Responderはout-of-band protocolからのinvitationメッセージやResponderのPublic DIDに含まれる招待メッセージを使用して、Requesterに自身の情報を提供する。
  2. Requesterは受け取った情報を元にDIDとDID DocumentをリクエストメッセージとしてResponderに送信する。
  3. Responderは送信されたDID Documentに含まれる情報を使用してDIDとDID Document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 1.0

- 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。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 つのロールを扱っている。

1. HolderからIssuerに対して送信されるプロトコルを開始する際のリクエスト。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リクエスト。
2. IssuerがHolderに対して送信する提供予定のクレデンシャルや価格に関する連携情報。
3. HolderからIssuerに対して送信されるクレデンシャルを要求するリクエスト
4. Credential Requestに対するクレデンシャルを含むレスポンス





## D) Aries RFC – 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。<sup>\*1)</sup>
- 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。<sup>\*2)</sup>

\*1) Drilling down: Co-development, <https://medium.com/decentralized-identity/drilling-down-co-development-in-the-open-765a86ab153f>

\*2) Setting Interoperability Targets, <https://blog.identity.foundation/setting-interoperability-targets/>

### 3-2-4. 統制構成要素の概要

## 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（トラストフレームワーク）

- 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、規制当局向けにAML等の分野における適切な規制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ガイドとして活用可能と述べられている。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、ガバナンス面での考慮事項の整理を行う。

OIXのトラストフレームワークで規定される構成要素

構成要素	項目	構成要素	項目	構成要素	項目
1. 原則		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	8. 技術・ セキュリティ要件	セキュリティルール
2. トラストマークとUX			レクエスト & レスポンス(API)		エコシステム参加者の トラストレジストリ
3. 役割と義務			RPによるID保証		証跡の記録と提示
4. 一般ルール	記録保存と監査証跡		ライアビリティ		リクエスト及びレスポンススキーム
	不正行為とサイバーコントロール		サービスレベル	9. 相互運用性	内部の相互運用性
5. ユーザ サービス	デジタルアイデンティティの選択	ヘルプ & サポート	プルーフニング		外部の相互運用性
	IDの作成 & 管理	7. トラスト ルール	アイデンティティ保証	10. ガバナンス	トラストフレームワークの構築と管理
	トラストの獲得と提示		認証		トラストフレームワークの強制力
	同意		適格性保証		トラストフレームワークの認証
ヘルプ & サポート			トラストフレームワークの運用		

### 3-2-4. 統制構成要素の概要

## 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	<ul style="list-style-type: none"><li>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. リライティングパーティ、3. フレームワーク、の順)</li><li>1.ユーザに関し4つの原則 (4Cs) を定義する。 (Convenience, Choice, Control, Confidence)</li></ul>
2. トラストマークとUX	<ul style="list-style-type: none"><li>User, RP, Evidence Issuer が見てトラストフレームワーク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)</li><li>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。)</li></ul>
3. 役割と義務	—
4. 一般ルール 記録保存と監査証跡	<ul style="list-style-type: none"><li>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。<ul style="list-style-type: none"><li>▶ 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</li></ul></li></ul>
不正行為とサイバーコントロール	<ul style="list-style-type: none"><li>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、担うロール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<ul style="list-style-type: none"><li>▶ 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</li></ul></li></ul>

### 3-2-4. 統制構成要素の概要

## トラストフレームワークの構成要素概要

	構成要素	概要
5. ユーザサービス	デジタルアイデンティティの選択	<ul style="list-style-type: none"> <li>自身のニーズに適したIdPの選択、他IdP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。</li> </ul>
	IDの作成 & 管理	<ul style="list-style-type: none"> <li>Identityのライフサイクル管理、特にクレデンシャル、Account Recovery、属性更新時のRPへの通知等の対応が可能なこと。</li> </ul>
	トラストの獲得と提示	<ul style="list-style-type: none"> <li>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。</li> </ul>
	同意	<ul style="list-style-type: none"> <li>利用者同意の元属性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。</li> </ul>
	ヘルプ & サポート	<ul style="list-style-type: none"> <li>IdP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。</li> <li>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。</li> </ul>
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	<ul style="list-style-type: none"> <li>RPによるTrustmark選択が可能なこと。</li> </ul>
	レクエスト & レスポンス(API)	<ul style="list-style-type: none"> <li>IdP/Verifier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。</li> </ul>
	RPによるID保証	<ul style="list-style-type: none"> <li>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。</li> </ul>
	ライアビリティ	<ul style="list-style-type: none"> <li>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。</li> </ul>
	サービスレベル	<ul style="list-style-type: none"> <li>Trust schemeやBrokerによる差別化・競争力の保持が可能なこと。</li> </ul>
	ヘルプ & サポート	<ul style="list-style-type: none"> <li>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。</li> <li>保証メカニズムによる差別化が図れること。</li> </ul>

### 3-2-4. 統制構成要素の概要

## トラストフレームワークの構成要素概要

構成要素	概要
7. トラストルール プルーフィング	<ul style="list-style-type: none"><li>• 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。</li><li>• 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。</li></ul>
アイデンティティ保証	<ul style="list-style-type: none"><li>• 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。</li><li>• 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。</li></ul>
認証	<ul style="list-style-type: none"><li>• 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。</li><li>• 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。</li></ul>
適格性保証	<ul style="list-style-type: none"><li>• 適格性保証のため、Eligibility Evidence の Validation・Verificationを行う。</li></ul>

### 3-2-4. 統制構成要素の概要

## トラストフレームワークの構成要素概要

	構成要素	概要
8. 技術・セキュリティ要件	セキュリティルール	<ul style="list-style-type: none"><li>• 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)</li></ul>
	エコシステム参加者のトラストレジストリ	<ul style="list-style-type: none"><li>• 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。</li></ul>
	証跡の記録と提示	<ul style="list-style-type: none"><li>• 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。</li><li>• ゼロ知識証明への対応を行うか考慮すべき。</li></ul>
	リクエスト及びレスポンススキーム	<ul style="list-style-type: none"><li>• 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ム定義が必要。 (特に複数Evidence Issuerをサポートするトラストフレームワークでは重要となる)</li><li>• OI DF／W3C等グローバルに定義されたスキームを考慮すべき。</li><li>• 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ムの為のキュレーターを実装すべき。</li></ul>



## トラストフレームワークの構成要素概要

構成要素	概要
<p>9. 相互運用性 内部の相互運用性</p>	<p>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。</p> <ul style="list-style-type: none"> <li>➤ Application of Principles</li> <li>➤ Trustmark Rules</li> <li>➤ Trust Rules and model, but perhaps leave the setting of acceptable scores within the model for particular use cases to <u>the trust scheme</u>.</li> <li>➤ Technical Rules such as used of common levels of Security and common Schemas</li> </ul>
<p>外部の相互運用性</p>	<p>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。</p> <ol style="list-style-type: none"> <li>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</li> <li>2) ノードアプローチ※を通じた、エージェントが多数フレームワークの整合性と互換性を独立に評価し、複数トラストフレームワークが相互に信頼しあう</li> <li>3) IdPやevidence verifier等当事者の、複数のトラストフレームワークへの準拠</li> </ol> <p>※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”)</p> <p>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。</p> <ul style="list-style-type: none"> <li>➤ Application of Framework Principles</li> <li>➤ Trustmark Rules</li> <li>➤ Trust Rules</li> <li>➤ Record Keeping</li> <li>➤ Fraud Controls</li> <li>➤ Response Schema</li> <li>➤ Security Standards</li> </ul>

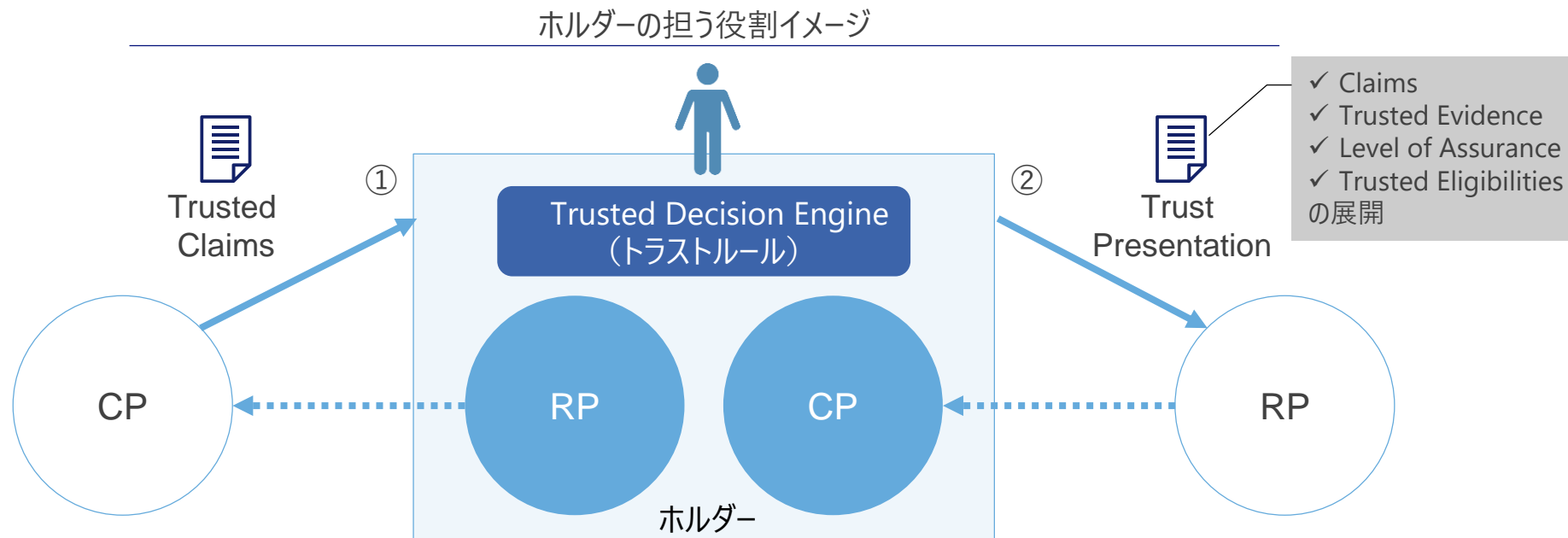
## トラストフレームワークの構成要素概要

	構成要素	概要
10. ガバナンス	トラストフレームワークの構築と管理	<ul style="list-style-type: none"> <li>• トラストフレームワーク生成者として5モデル定義 (事例)               <ul style="list-style-type: none"> <li>1) Independent Governing Entity 1) DIACC</li> <li>2) Consortium of Participating Entities 2) CA/Browser Forum</li> <li>3) Single Participant Governing Entity 3) 単一ID Provider, GOV.UK Verify</li> <li>4) Non-Governing Standards or Certification Organization 4) Kantara Initiative, tScheme</li> <li>5) Mutual Agreement Among All 5) - (個別の管理主体は存在せず)</li> </ul> </li> </ul>
	トラストフレームワークの強制力	<ul style="list-style-type: none"> <li>• 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。               <ul style="list-style-type: none"> <li>1) 民間セクター：契約メカニズムによる強制力</li> <li>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</li> <li>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）</li> </ul> </li> </ul>
	トラストフレームワークの認証	<ul style="list-style-type: none"> <li>• 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）</li> <li>• 認定手法は以下の通り（各レベルは別紙にて詳述）。               <ul style="list-style-type: none"> <li>➢ Self-Assessment</li> <li>➢ Verified Self-Assessment</li> <li>➢ Approved</li> <li>➢ Certified</li> </ul> </li> </ul>
	トラストフレームワークの運用	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 統制機能の例として、以下に分類。               <ul style="list-style-type: none"> <li>➢ Governance and Policy Development</li> <li>➢ Policy Enforcement</li> <li>➢ Participating Entity Management</li> <li>➢ Network Evolvement</li> <li>➢ Trust Framework Operations</li> </ul> </li> </ul>

### 3-2-4. 統制構成要素の概要

## SSIモデルにおけるトラストフレームワークの適用イメージ

- 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。
  - ① CPからクレームを受け取る、「RP」としての役割を担う
  - ② 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つの役割を担うことで、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。そのため、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。詳細は3-4.節にて詳述する。



### 3-3. SSI/DIDの先行事例/PoC事例

---

### 「3-3. SSI/DIDの先行事例/PoC事例」の要旨

- 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、カナダの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、立ち上げ時はIdPとしての金融機関と、サービスプロバイダー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。
  
- 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. SSI/DIDの先行事例/PoC事例

## 金融機関が関与する主な取組事例

- 現在特に海外を中心にSSI/DIDに関連する様々な取組が進められているが、その多くは実証レベルであり、実際のサービスなどに適用されているものは少ないのが現状。
- 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。

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。 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、ワンズオンリーによる利便性を提供する。 現在は、実証実験の段階であり、2021年5月にリリース予定である。
スペイン	Veridas (BBVAとdas-Nanoの合併会社)	金融	BBVA/Bankia/Renta 4 Banko	高度な生体認証機能(顔、声、指紋等)の提供 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している。
		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している。
ドイツ	Deutsche Bank	行政・銀行・ヘルスケア等	Deutsche 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IdPとして参加	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である。
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認証イニシアティブの一環としてIdP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にしている。

出所：各社プレスリリース等をもとにNRI作成

### 3-3. SSI/DIDの先行事例/PoC事例

## 金融機関が関与する主な取組事例

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
グローバル	Master Card (カード)	通信会社の顧客のID管理	Optus (通信会社)		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を提供する。
		大学の試験における本人確認	郵便公社 ディーキン大学	デジタルIDプラットフォームの提供	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することが出来る。
		行政のデジタルID連携	北マケドニア共和国		北マケドニア国民が日常のさまざまな活動で使用できる、ローカルのデジタルIDと関連トラス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ある。
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	他事業者間の属性の連携・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 伊藤忠テクノロジーソリューションズ 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。

出所：各社プレスリリース等をもとにNRI作成

### 3-3. SSI/DIDの先行事例/PoC事例

## 金融機関が関与する主な取組事例

- 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以下2事例について詳述する。

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	選定理由
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。 主要7銀行が保有する本人確認情報等を生保等に連携。	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。
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分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する。 現在は、実証実験の段階であり、2021年5月にリリース予定である。	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。



## Canada: Verified.Me

- 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属性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の分散型アイデンティティ標準(W3C DIDs and Verifiable Credentials)に準拠している。
- 本サービスは、消費者は無料で利用できる。（App StoreやGoogle Playからアプリをダウンロードして利用）

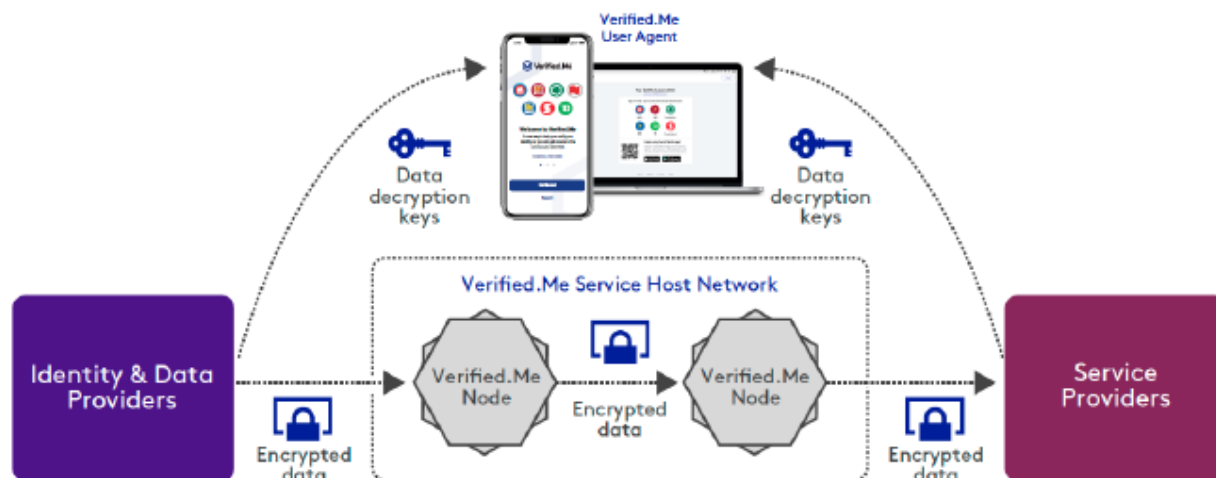
Verified.Meのサービス概念図



## Canada: Verified.Me

- Verified.Meの基本的な仕組みは以下の通り。

### Verified.Meの仕組み



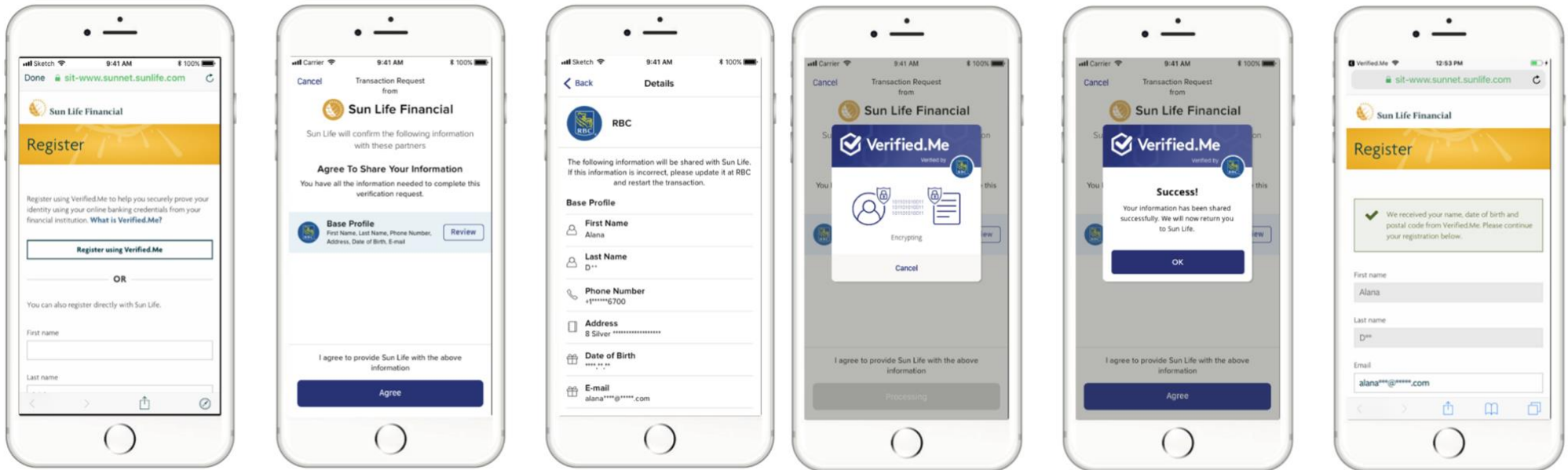
- アイデンティティ&データプロバイダー(IdPs)
  - ユーザに関する特定の情報を生成または保持する Verified.Me に参加するカナダの適格組織。IdPの例としては、金融機関、信用情報機関、電気通信プロバイダー、およびその他の適格なトラステッドソースが該当
- リライングパーティ(RP)またはサービスプロバイダー
  - Verified.Me に参加するカナダの適格な組織であり、Verified.Me を通じてユーザに特定の情報の提供を求める。Verified.Meは、サービスプロバイダーが、主体に対してサービスや製品を提供する際のアイデンティティや適格性をバリファイするのを支援する
- 金融機関のアイデンティティ&データプロバイダー（金融機関、または「サービス・ホスト」）
  - カナダの主要金融機関 7 社は、Verified.Me サービスへのアクセスを希望するサブジェクトの認証、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。サービスホストは、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 ユーザーエージェント
  - ユーザが 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）を介してユーザの属性の共有に同意するために提供されるツール

### 3-3. SSI/DIDの先行事例/PoC事例

## Canada: Verified.Me

- 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。

### Verified.Meの利用イメージ



- 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

## Canada: Verified.Me

- Verified.Meの主な特徴としては、以下の点が挙げられる。

#### 【サービスが創出された背景】

- 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おり、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銀行側にあった。

#### 【SSI/DIDとしての特徴】

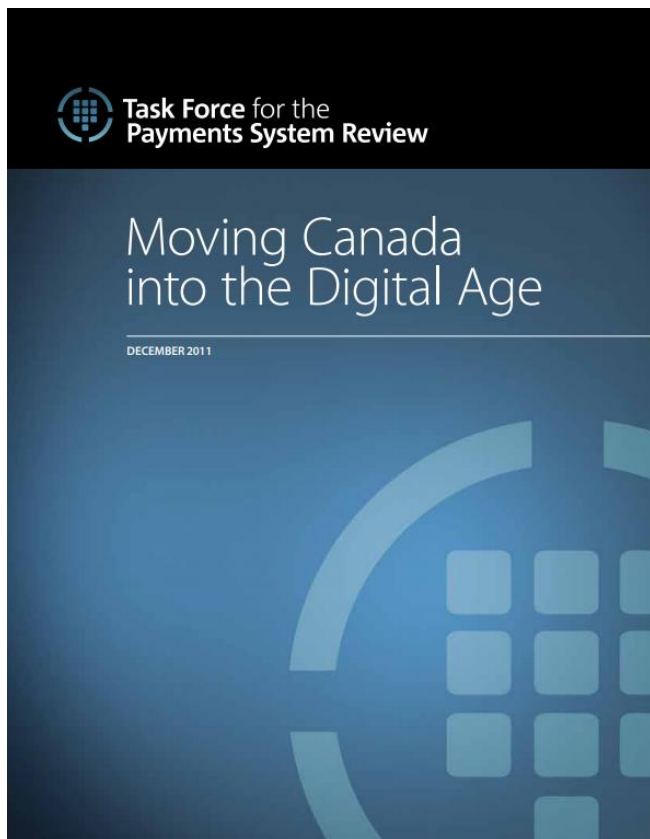
- 本サービスはSSIに基づくモデルではあるが、一般のSSIよりも更に厳しいモデルを取っている。SecureKey社はこれを「Triple Blind」と呼ぶ。すなわち、本サービスモデルに参画する3者（Identity & Data Provider, Service Provider, Network Operator）のいずれもが、ユーザが連携する情報がどこからどこに提示されるのか分からないような設計となっている。一般にSSIのモデルは、リライティングパーティ側はこのIdentity情報が使われているのかについては制限しないため、この点でより強固なプライバシー設計となっている。

#### 【ユースケース】

- 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。

## 【参考】カナダのデジタルアイデンティティ

- 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り組んでいる。
- 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。



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頼りに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。

- 上記提言の3点目の提言を踏まえ、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。

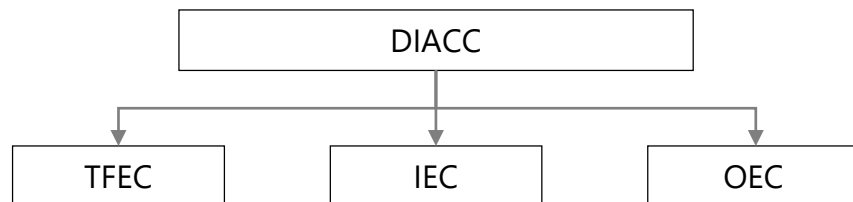
### 3-3. SSI/DIDの先行事例/PoC事例

## 【参考】DIACC (Digital ID & Authentication Council of Canada)

- DIACCの参加メンバーと主な取組みは以下の通り。
- 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。



### DIACC内に設置されているコミッティ



TFEC : Trust Framework Expert Committee  
IEC : Innovation Expert Committee  
OEC : Outreach Expert Committee

### DIACCの官民での取組み



#### Outreach: 情報収集・共有

- Connect, develop, and strengthen outreach that informs Canadian and global trends.
- Gain early input and view into local and international efforts including GDPR, PSD2, UNCITRAL, and more.
- Provincial members are first to be considered as venues for DIACC and IdentityNORTH events.



#### Innovation: ユースケースの企画、PoC実施

- Connect, share, develop, and strengthen service and product strategies.
- Drive use cases to gain visibility, input, and recognition.
- Test viabilities and accelerate innovation via design challenges, proofs of concepts, applied research, and more.



#### Interoperability: 相互運用性、ベスパラ輸出

- Connect, influence, and deliver public/private sector collaborative standards, agreements, and programs to secure interoperability.
- Map impactful use cases to evolving standards and practices to secure Canadian digital identity.
- Lead and gain early insights and strategic opportunities for interoperability.
- Share Canadian standards globally and bring best global practises to our community.

### 3-3. SSI/DIDの先行事例/PoC事例

## 【参考】PCTF(Pan-Canadian Trust Framework)とSSI/DIDへの対応

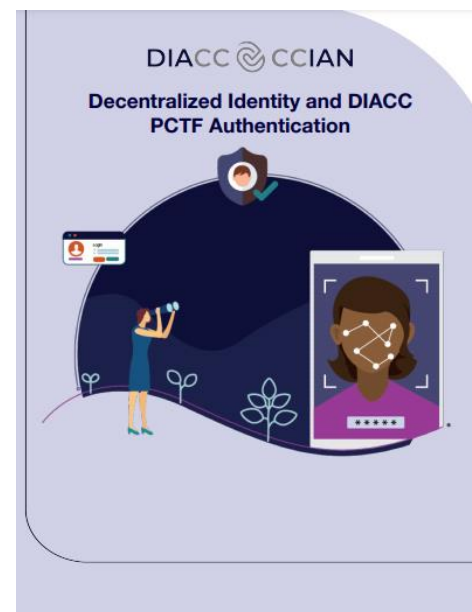
- DIACCは、カナダの官民組織がデジタルアイデンティティを安全に活用するためのガバナンスモデルとしてPCTFを開発し、2020年11月にPCTF 1.0 alphaをローンチ。
- PCTFは、アイデンティティ管理を既存のアナログからデジタルに移行する際に求められる基本原則や基準を策定し、政府機関や事業者がリファレンスアーキテクチャとして参照できるようにすることを目的に策定。
- 法的強制力はなく準拠は任意であるが、デジタルアイデンティティのトラストフレームワークとして、カナダ国内のみならずグローバルでも注目されている。
- また、2021年2月に分散型アイデンティティがどのようにPCTF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。

【PCTFの構成要素】



出所) [https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation\\_V1.0.pdf](https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation_V1.0.pdf)

【DIDに関するガイドライン】



出所) <https://diacc.ca/wp-content/uploads/2021/02/Decentralized-Identity-and-DIACC-PCTF-Authentication.pdf>

## 【参考】PCTF準拠状況のセルフアセスメント

- 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果たしている。
- 例えば、前述のVerified.Meについて、SecureKey社は以下のセルフアセスメント結果を公表。

### DIACC Identity Networks Paper Verified.Me by SecureKey Technologies Inc., Self-Assessment



This document is intended to be used by identity network providers that want to demonstrate how their solution fits into the framework and requirements as described in the "Making Sense of Identity Networks" whitepaper. This self-assessment is an informal way to illustrate the concepts discussed in the whitepaper and has been reviewed by Consult Hyperion to ensure it is objective, accurate, and aligns with the framework.

#### 1. Introduction

Verified.Me is a service (live and in production as of May 1, 2019) offered by SecureKey Technologies Inc., in conjunction with a consortium of seven of Canada's major financial institutions – BMO, CIBC, Desjardins, National Bank of Canada, RBC, Scotiabank and TD.

Verified.Me is a privacy-respecting digital identity and attribute sharing network. The service simplifies identity verification processes by allowing individuals (subjects) to share identity and attribute information from trusted sources (including financial institutions, mobile operators, credit bureau, and government) with the services that they wish to access.

The network is based on permissioned distributed ledgers operated by the consortium. It is built using the IBM Blockchain Platform which is based on Linux Foundation's open source Hyperledger Fabric and is aligning with W3C decentralized identity standards, to enable interoperability with other networks. SecureKey's Triple Blind® approach means that no network participant alone, including SecureKey, can have a complete view of the user journey - the subject can't be tracked.

The service is free for consumers to use, either using their web browser, or by downloading the mobile app through the App Store (iOS) or Google Play (Android).



### 3-3. SSI/DIDの先行事例/PoC事例

## Spain: Alastria\_ID/Dalion

- Alastria\_IDはSSIでのデジタルアイデンティティのモデルで、Dalionはスペインの金融事業者等によってAlastria\_IDを基にサービス化されているプロジェクトの名称である。

### ■ Dalion参加企業

- Alastria、銀行、保険会社、エネルギー事業者、IT開発事業者

Dalionプロジェクト参加企業・団体  
(Santander社プレスリリースより)

### ■ プロジェクト概観

- 2019年に開始、2020年にPoCを実施、2021年5月サービス提供開始予定
- AlastriaのEthereum-Quorumブロックチェーン上で動作（開発時点）

### ■ 利用者へのメリット

- 個人の情報を自ら管理可能
- 新規サービス登録・利用時の情報入力の手間削減（KYCといった検証含む）
- アイデンティティ盗難対策

### ■ 参加企業へのメリット

- 利用者登録の手続きなどの効率化
- 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



銀行



保険



MAPFRE



エネルギー



CaixaBank



証券取引所運営

ITサービス



### 3-3. SSI/DIDの先行事例/PoC事例

## Spain: Alastria\_ID/Dalion

### DNI 3.0カード例

- スペインに関連するデジタルアイデンティティの取り組みは以下の通り。

- DNI (Documento Nacional de Identidad) 3.0 <sup>\*1)</sup>

- スペイン政府（国家警察総局）が発行 従来のDNIeから2015年頃より移行
- 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
  - ・ 格納データ：氏名等情報、顔写真、サイン、指紋、電子署名証明書、DNI証明書
- 身分情報の提示や電子署名の付与等に使用可能



画像出典：[https://www.dnielectronico.es/PDFs/uso\\_nfc.pdf](https://www.dnielectronico.es/PDFs/uso_nfc.pdf)

- Alastria\_ID

- 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<sup>\*2)</sup>
  - ・ 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
- 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の自己主権型アイデンティティ基盤<sup>\*3)</sup>
- 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が目的<sup>\*3)</sup>
  - ・ スペインの標準化団体（UNE）に提示、欧州電気標準化委員会にも提出され、さらにESSIF (European Commission's Self-Sovereign Identity Initiative) にも示唆を与えた<sup>\*4)</sup>

- Dalion <sup>\*4)</sup>

- 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
- サンタンデル銀行を含めた多数の銀行業、保険業、証券市場等が参画し、地方自治体や大学等のオブザーバーも参加
- 検証済みの属性の受け渡し、つまり他銀行等による身分検証結果を転用可能にして身分検証の手間削減が目標

\*1) スペイン国家警察総局 <https://www.dnielectronico.es>

\*2) Alastria <https://alastria.io/>

\*3) Alastria\_ID GitHub <https://github.com/alastria/alastria-identity/wiki>

\*4) サンタンデル銀行によるDalionプロジェクトのプレスリリース <https://www.santander.com/en/press-room/press-releases/2020/11/ten-spanish-companies-join-forces-to-promote-digital-identity-using-blockchain-technology>

### 3-3. SSI/DIDの先行事例/PoC事例

## Spain: Alastria\_ID/Dalion

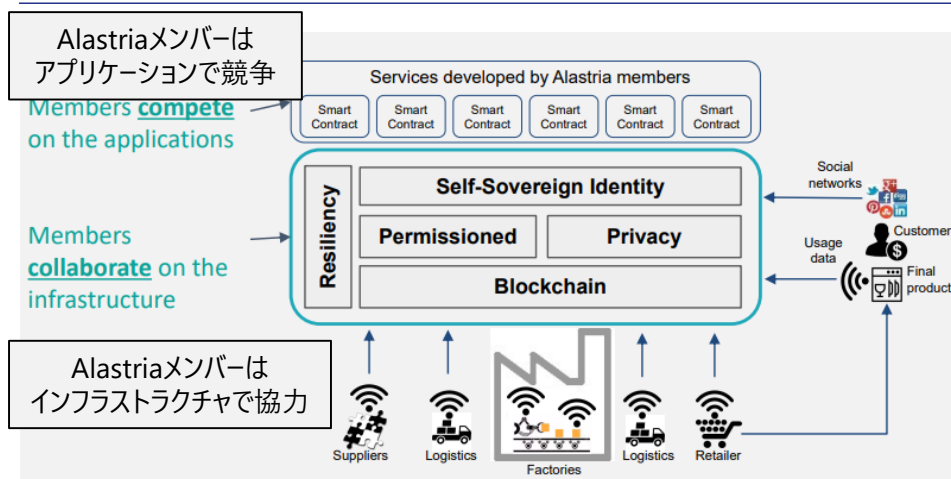
#### ■ Alastria\_IDとはAlastriaのアイデンティティ委員会によるデジタルアイデンティティのプロジェクト

- Alastria参加メンバーが運営するブロックチェーン上で動くSSIのモデル
- 欧州圏での法的有効性を持った自己主権型のデジタルアイデンティティのインフラストラクチャと開発フレームワークを提供

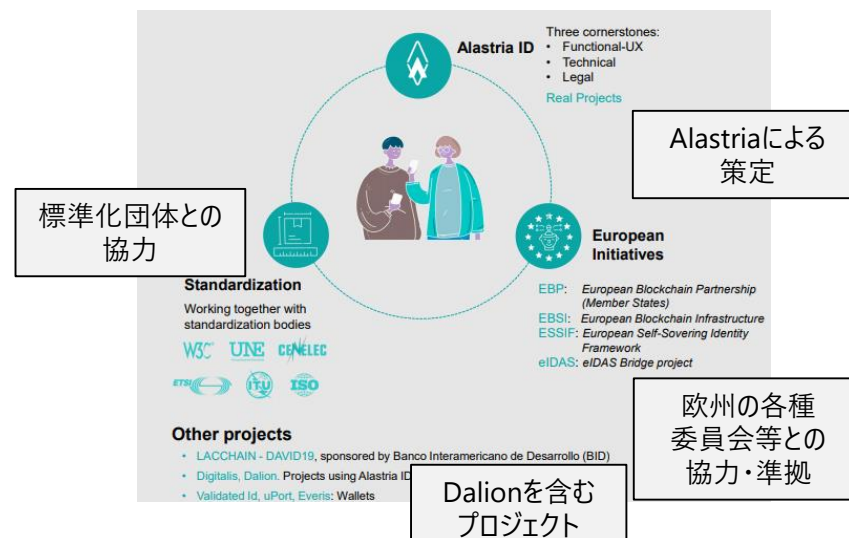
#### ■ 以下の欧州圏の基準等に準拠

- 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
- GDPR対応としてEUBOFと欧州議会によるブロックチェーンとGDPRについてのレポート
- eIDAS規制

#### Alastria\_ID 役割分担



#### Alastria\_ID 特徴



出所)

"Alastria Digital Identity An ongoing project"

<https://portal.r2docuo.com/alastria/document?L3110FC15F>

"Alastria\_ID" GitHub <https://github.com/alastria/alastria-identity/wiki>

出所) "Alastria ID Compatibility and interoperability"

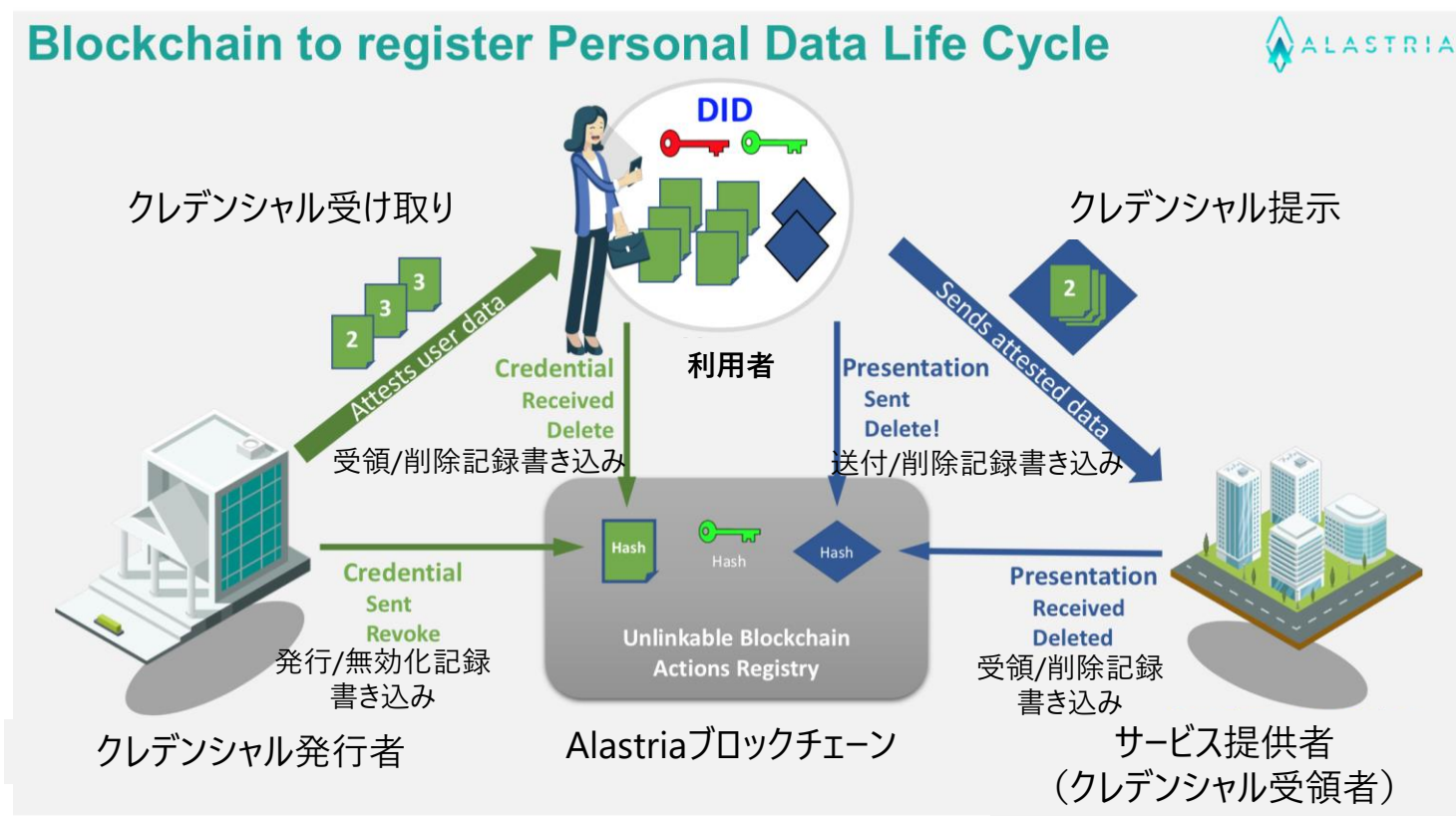
<https://portal.r2docuo.com/alastria/document?L097EBB43D>

### 3-3. SSI/DIDの先行事例/PoC事例

## Spain: Alastria\_ID/Dalion

- Alastria\_IDは一般的なSSI/DIDと同様にクレデンシャル発行者（Issuers）、利用者（User）、クレデンシャル受領者（Service Provider）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。

Alastria\_ID 利用概観図



## 3-4. SSI/DIDの長所と実現に向けた課題

---

## 「3-4. SSI/DIDの長所と実現に向けた課題」の要旨

- SSIモデルの長所ならびに実現に向けた課題は、それぞれ以下の通り。
  - 長所は、主にIdPへの依存度を下げること、自己制御権の獲得やプライバシーへの配慮実現可能な点が挙げられる。また、複数クレームプロバイダー間を、ユーザのウォレットをハブに連携するトポロジーを取ることで、業界全体のオンボーディングコスト抑制に寄与する点が期待出来る。
  - 実現にむけた課題は、新たなモデルであるが故の技術・法的/制度・運用面で生じる新規課題克服、ならびにビジネスにおける新規取り組みに向けてのオーバーヘッドへの考慮や適合ユースケース探索が挙げられる。

SSIモデルにおける長所

種類	概要
自己制御権の獲得	<ul style="list-style-type: none"> <li>• IdPによるロックアウト制約を回避</li> <li>• IdPによる発行後クレームの内容改ざんを回避</li> </ul>
プライバシーへの配慮	<ul style="list-style-type: none"> <li>• 既存IdPでの処理の最小化</li> <li>• 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</li> <li>• 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）</li> </ul>
利便性の向上／業界全体のコスト抑制	<ul style="list-style-type: none"> <li>• 取得済クレームを用いた複数リライティングパーティへの展開（利便性向上）</li> <li>• 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</li> </ul>

SSIモデルの実現に向けた課題

種類	概要
技術	<ul style="list-style-type: none"> <li>• SSI/DIDを構成する各レイヤーのトラストアンカー整理・実装</li> <li>• 複数仕様の併存における相互運用性の考慮</li> <li>• 新規策定されるプロトコルに対するセキュリティ実装の確保</li> </ul>
法的/制度	<ul style="list-style-type: none"> <li>• 政府および政策立案者の関与</li> <li>• データ保護制度</li> <li>• プライバシー対策</li> </ul>
運用	<ul style="list-style-type: none"> <li>• 規制当局や弁護士、公証人の技術の理解</li> <li>• 標準化の推進</li> <li>• トラストフレームワークの整備・開発</li> <li>• ライアビリティの明確化</li> </ul>
ビジネス	<ul style="list-style-type: none"> <li>• 現行IT/デジタルシステムの適応</li> <li>• 個人の導入/ユースケースの検討</li> </ul>

### 3-4-1. SSI/DID活用のメリット

## SSIモデルのメリット

■ SSIモデルは、下記項目へのメリットが期待される（下線は2章で言及したデジタル化加速における課題）。

■ 各メリット獲得のためには、SSI/DIDの4つの特性が必要不可欠となる。

SSIモデルのメリット

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	<ul style="list-style-type: none"> <li>悪意を持ったIdP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</li> <li>以下の実現により、IdP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               <ul style="list-style-type: none"> <li>✓ クレームを自身のウォレットに取得</li> <li>✓ 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</li> </ul> </li> </ul>	●	●		●
プライバシーへの配慮	<ul style="list-style-type: none"> <li>既存IdP内での処理の最小化（Recognition処理に限定）</li> <li>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</li> <li>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）</li> </ul>	●	●	●	
利便性の向上／業界全体のコスト抑制	<ul style="list-style-type: none"> <li>一度取得したクレームを複数リライティングパーティに展開が可能（顧客の利便性向上に寄与）</li> <li><u>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</u></li> </ul>	●	●		

### 3-4-1. SSI/DID活用のメリット

## 先行事例におけるSSIモデルのメリット

■ SSIモデルのメリットに関して、3-3.で取り上げたカナダのVerified.Meでの対応状況は以下の通りと考える。

#### 先行事例での実現例

メリット	SSI/DIDの特性との対応				先行事例（Canada Verified.Me）での実現例 ※公開情報等をもとにNRI考察
	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	●	●		●	<ul style="list-style-type: none"> <li>認証と属性の分離は、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。</li> <li>分散情報活用・選択的提示は、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。</li> <li>長期の保管・利用については、実施有無含め詳細不明。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。</li> </ul>
プライバシーへの配慮	●	●	●		<ul style="list-style-type: none"> <li>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。</li> <li>分散情報活用・選択的提示は、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。</li> <li>提示策の秘匿については、RPに対してどのIdPから取得した属性が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。</li> </ul>
利便性の向上／業界全体のコスト抑制	●	●			<ul style="list-style-type: none"> <li>認証と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。</li> <li>分散情報活用・選択的提示は、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かるコストを大幅に削減できている。</li> </ul>



### 3-4-2. SSI/DIDの課題 - (1) 技術面での課題

## 技術的課題

#### ■ SSI/DIDを構成するレイヤーにおける技術的課題

- DIDを構成する各レイヤにおいて、トラスト、相互運用性、セキュリティの観点で課題を整理する。

※ウォレットアプリケーションの信頼性にも関与

SSIモデルのレイヤーごとの課題観点での技術的課題

レイヤー		トラストアンカー	相互運用性	セキュリティ			
Claim Presentation Layer		バリデーション/ベリフィケーション/ 透明性の確保					
Claim Issuance Layer							
Wallet Layer	Local Storage	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	データフォーマットの統一 スキーマ共通	モデル間・メソッド間における 相互運用性への考慮	プロトコルの認定・規格適合性の確認 (Certificate, Conformance Test)	Cryptographic Agility	Formally provable
	WebApp						
	クラウド						
Transport/Communication Layer		DID cryptographic private keyの トラスト確保※					
Discovery Layer		Universal Resolverの追跡性、 透明性、トラストアンカー担保					
Utility Layer		アイデンティファイア生成の スキーマにおけるAuthority Model					

### 3-4-2. SSI/DIDの課題 - (1) 技術面での課題

## 【参考】実現方式に伴う技術的課題の対象仕様

- 標準化団体によってレイヤーの実現方式は異なる。既存方式の活用・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検討が必要となる。
- 実現方式は下記組み合わせに限定されるものではなく、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（例えば3-2節で述べたOIDF/DIFリエゾン協定等）

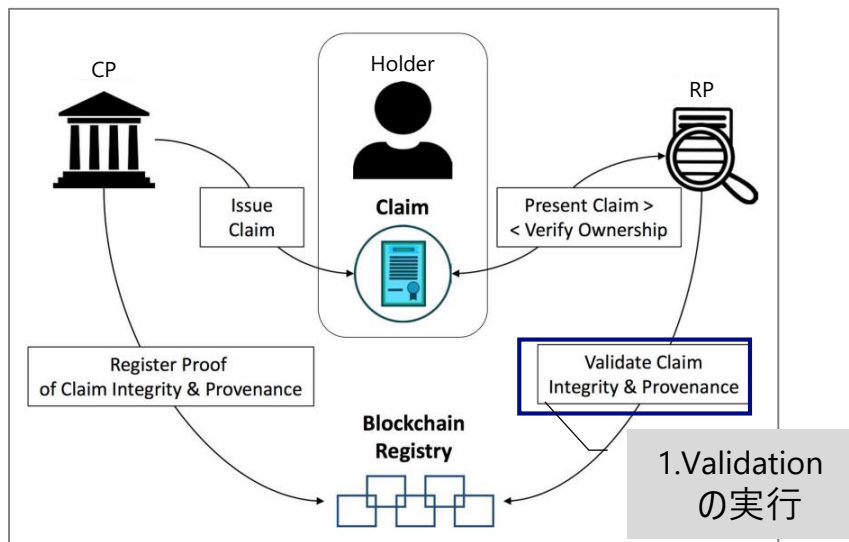
レイヤー		モデル			
		OIDC		DID/VC	
Claim Presentation Layer		OpenID Connect	OpenID Connect	Presentation Exchange VP Request Spec	Aries : Present Proof Protocol 1.0
Claim Issuance Layer		JWT (JSON-LD, ZKP表現方式としても対応)	VC Data Model (VC / VP / ZKP)	VC Data Model (VC / VP / ZKP)	Aries : Issue Credential Protocol 2.0
Wallet Layer	Local Storage	ベンダ実装依存	ベンダ実装依存	Confidential Storage	ベンダ実装依存
	WebApp			ベンダ実装依存	
Transport/ Communication Layer		REST http(s)	OIDC SIOP	REST http(s)	OIDC SIOP
Discovery Layer		OIDC Discovery WebFinger .well-known	OIDC Discovery WebFinger .well-known	DID Comm/ CHAPI	Aries : DID Exchange Protocol 1.0
Utility Layer		DNS/Domain	DNS/Domain	NFC/BLE/QR/http(s)	
				DID Resolution	
				DIDs	

### 3-4-2. SSI/DIDの課題 - (1) 技術面での課題

## 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

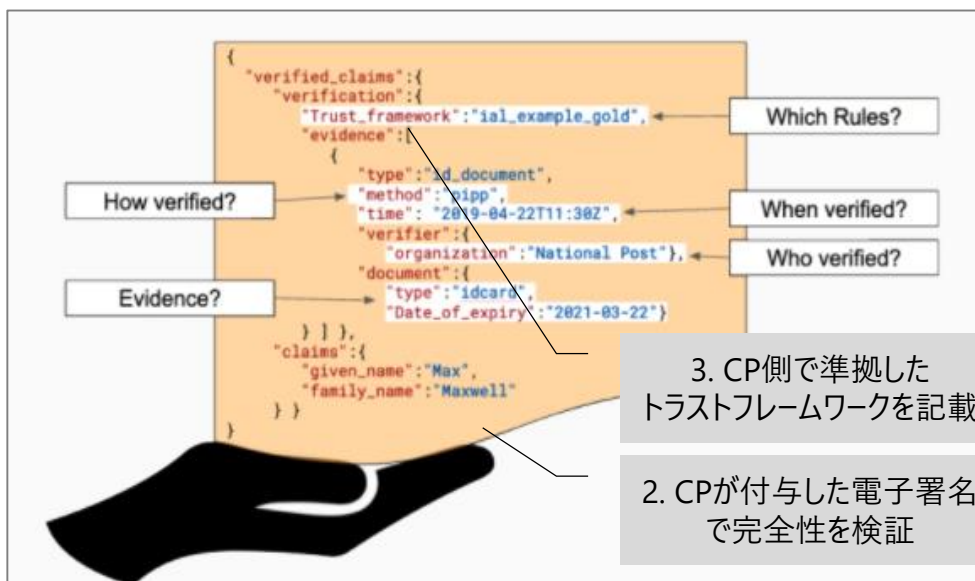
- SSI/DIDはクレームに対し、1. 有効状態（失効されていない）かを確認するバリデーション、2. 改ざんされていないかを検証するベリフィケーション、3. 生成時に準拠したトラストフレームワークが確認できる透明性、の確保が重要となる。
  1. ブロックチェーン等の分散リポジトリ上にクレームの失効情報を展開し、RP側で参照する、といった実現方式が考えられる。一方で、CRL\*で用いられている有効期限切れの情報は排除される等サイズ肥大化への対処措置を、ブロックチェーンの様にImmutableな特性を持つ方式で実現する場合は、実装面での考慮が必要となる。 \* CRL: Certificate Revocation List (RFC5280)
  2. 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。
  3. 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。

#### 分散リポジトリへのValidation実施



出所) decentralized-id.com資料を基に作成

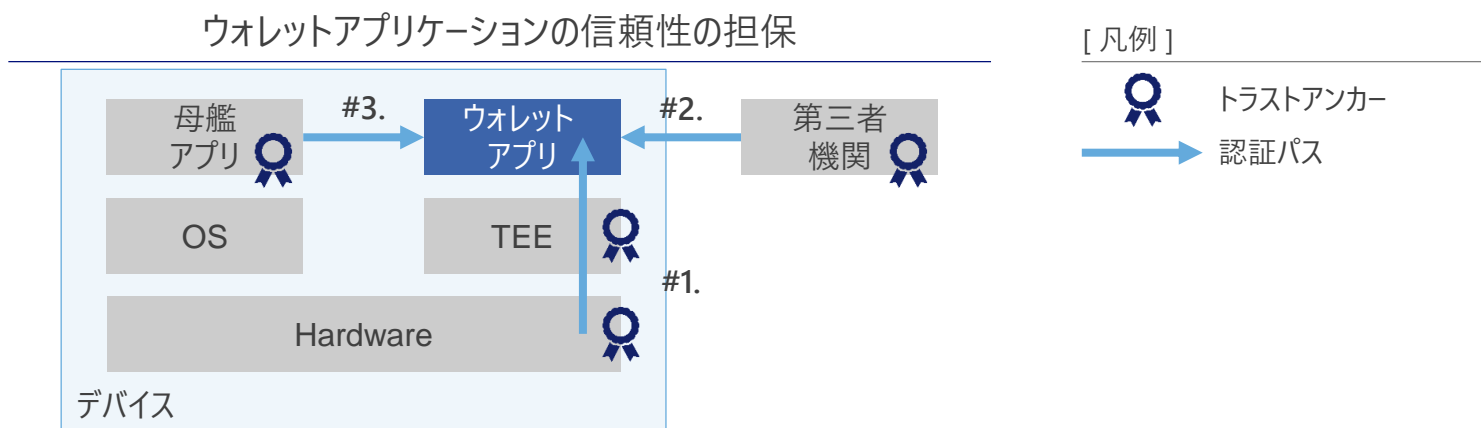
#### OIDC4IDAを用いたクレームのベリフィケーション・透明性の確保



出所) OpenID Foundation “eKYC & Identity Assurance WG”

## ウォレットアプリケーションの信頼性の担保

- アプリの信頼性確保（保証）には、保証の起点となりうるトラスタンカーからの認証パスチェーン確保が必要となる。想定されるトラスタンカー候補として、例えば以下の表の3つの手法が想定される。
- エコシステムとしての提供を考慮すると、#1.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。

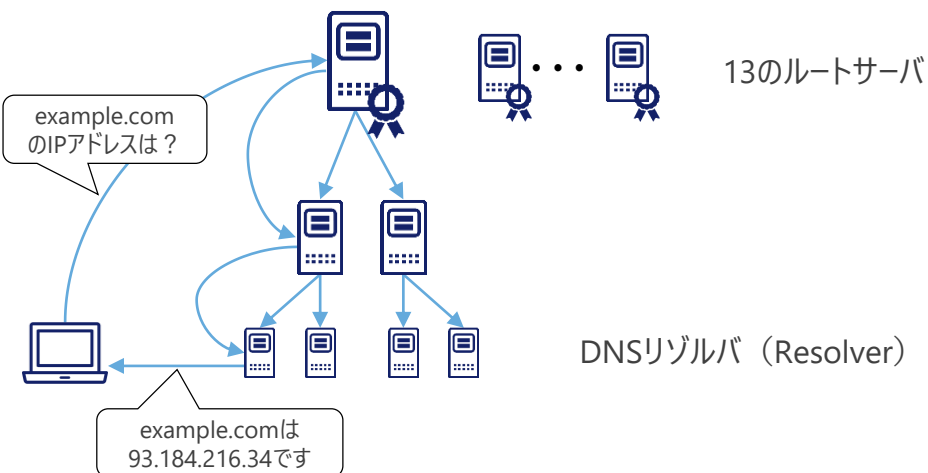


#	手法	概要	課題
1.	デバイス内の下位レイヤーからの認証パスチェーン構築	OS/TEEなどセキュアエレメント内に格納された署名鍵を使って処理結果への署名・署名検証を実施し、下位レイヤーからの信頼を構築	<ul style="list-style-type: none"> <li>• 特定モデル/製品への依存が発生</li> <li>• ポータビリティ確保が困難</li> <li>• HW/OSベンダーの協力が不可欠</li> </ul>
2.	第三者機関による評価プログラムを通じた評価	iOSのApp Store、AndroidのGoogle Play Store等の第三者機関がアプリを確認	<ul style="list-style-type: none"> <li>• 第三者機関の検証プログラムに依存</li> <li>• 別チャンネルからの取得によるバイパスが可能</li> <li>• 第三者機関の意向によるウォレットアプリ排除</li> </ul>
3.	母艦アプリ等からの呼出し（Deeplink等）	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	<ul style="list-style-type: none"> <li>• 母艦アプリのプリインストールが必要（事後導入の場合、#2.と同様の考慮が必要）</li> </ul>

## Universal Resolverの追跡性や透明性、トラストアンカーの担保

- SSI/DIDのUniversal Resolverのトラストアンカーの担保と、追跡性や透明性の確保が課題となりうる。
  - 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。
    - 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。
    - グローバルにおける一意性を担保する等の要件を想定した場合、その類似性から例えばICANNにおけるドメイン取得時の管理等と同等の運用・管理要件が想起される。

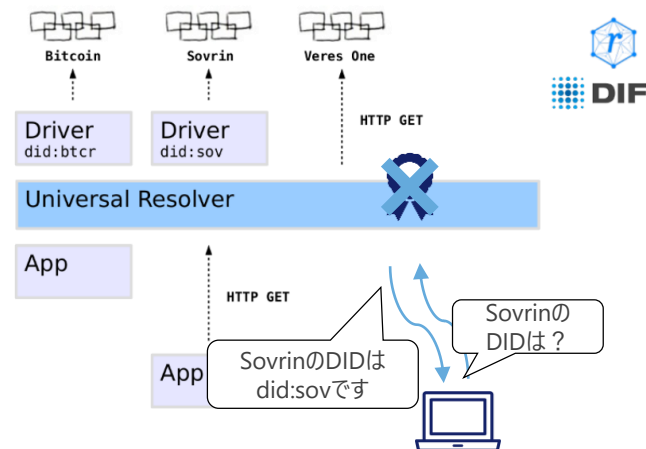
DNSの解決 (Resolve) 概観



ルートサーバが、下位DNSリゾルバ (Resolver) の  
トラストアンカーとして振る舞う

出所) NRI作成

Universal Resolverの概観



Universal Resolverが  
トラストアンカーとして振る舞う必要がある

出所) <https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c>

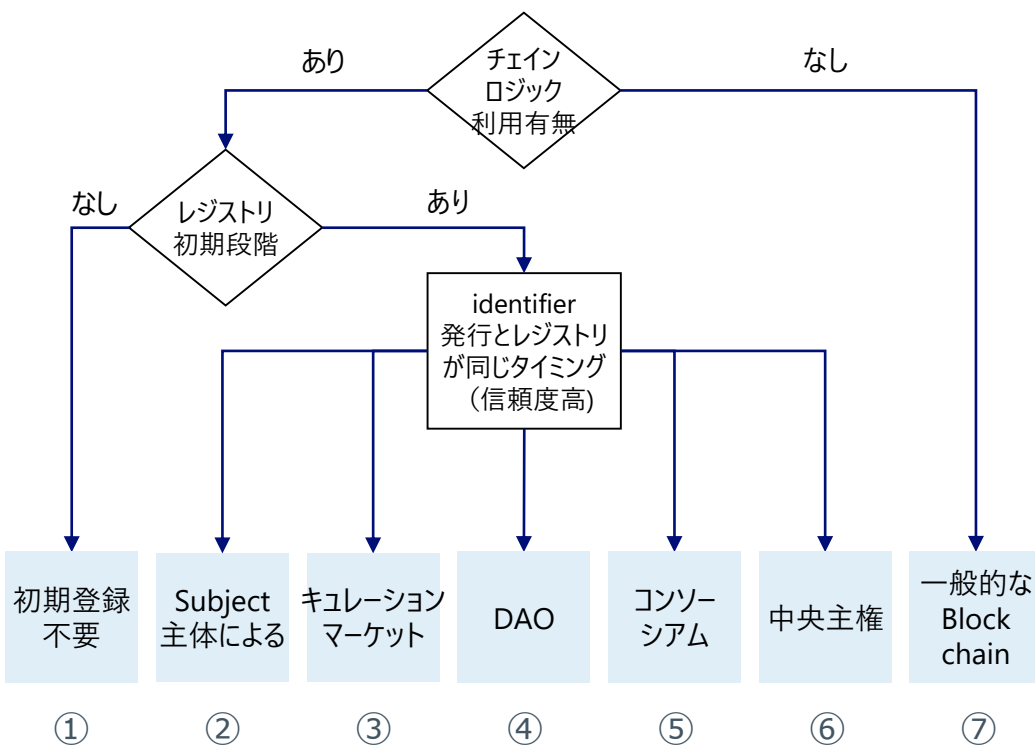
### 3-4-2. SSI/DIDの課題 - (1) 技術面での課題

## アイデンティファイア生成におけるスキーマのAuthority Model

■ Authority ModelとSSI思想との相反（ Subjective consensus ） が起こりうる。

- 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。
- 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・統制を効かせるかの考慮が必要となりうる。

Identifier のレジストリモデル



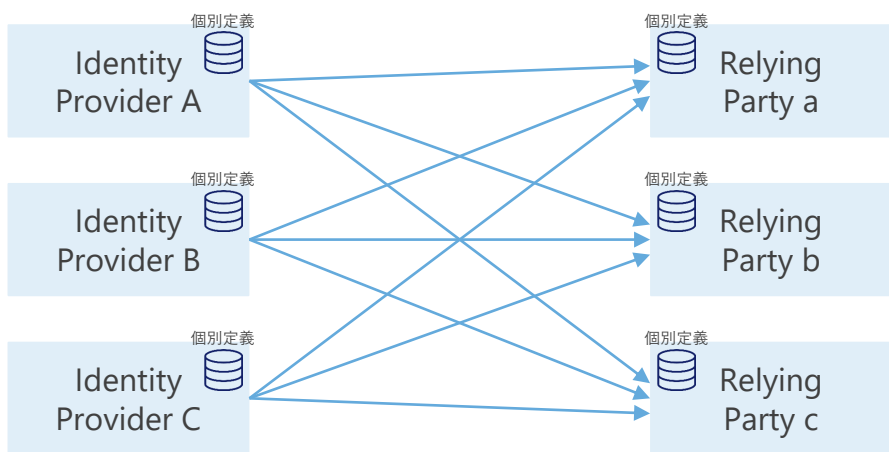
#	種類	特徴	
①	初期登録不要	特定の状況下のみでアイデンティファイアを台帳に登録	
②	Subject (主体)	自己登録で、Issuerが発行したクレデンシャルを受け取るエンティティであるSubjectがレジストリを管理	
③	Curation market	③～⑤は参加者による許可の実装管理の度合いにより変動しうる	
④	DAO (Decentralized Autonomous Organization) (分散自律団体)		<ul style="list-style-type: none"> <li>• Curation market：レジストリの判断を参加者が投票で決める</li> </ul>
⑤	Consortium (共同事業体)		<ul style="list-style-type: none"> <li>• DAO：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</li> <li>• Consortium：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</li> </ul>
⑥	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	
⑦	一般的なブロックチェーン (チェーンロジックなし)	チェーンロジック（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	

### 3-4-2. SSI/DIDの課題 - (1) 技術面での課題

## フォーマット、スキーマ、プロパティ等の共通化・統一化

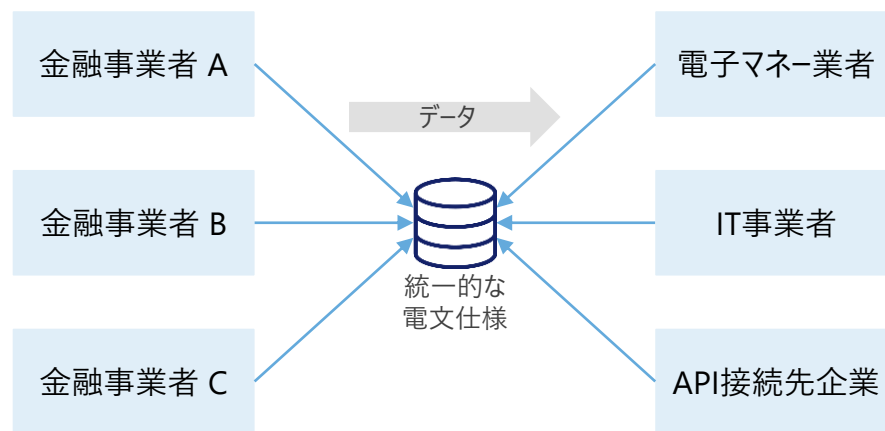
- フォーマット、スキーマ、プロパティ等の統一化がなされていない状態だと、データ連携時における個別スキーマの参照や独自のパース処理実装等、開発が非効率となるため、極力仕様の共通化・統一化が進むことが望ましい。
  - 共通化・統一化に際しては、標準技術仕様としての策定範囲と、業界・業種等ユースケースに応じた関連団体等で定める範囲との、境界を意識した策定範囲の議論が必要となる。
- OpenID Connectや金融API等ではフォーマットの統一とスキーマが共通されることで、データの受け渡しを容易化。
  - OpenID Connectにおけるクレームのやり取りで広く用いられるJWT（JSON Web Token）は、RFC7519として策定されて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。
  - 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。

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



スキーマ、フォーマット、プロパティ、パラメータ等が異なるとデータ授受のための開発が非効率（個別開発が発生）

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



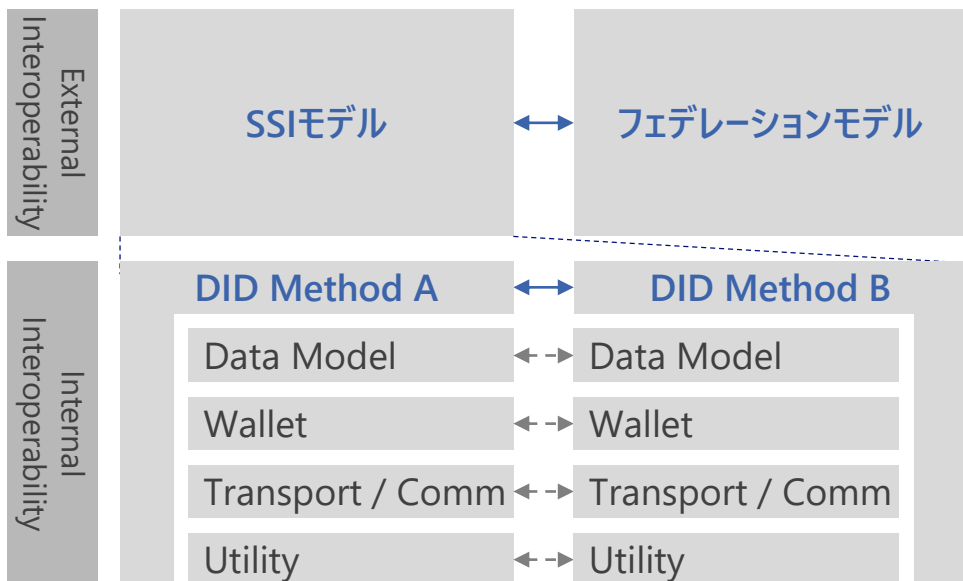
電文仕様を統一することでデータ授受における仕様を標準化

### 3-4-2. SSI/DIDの課題 - (1) 技術面での課題

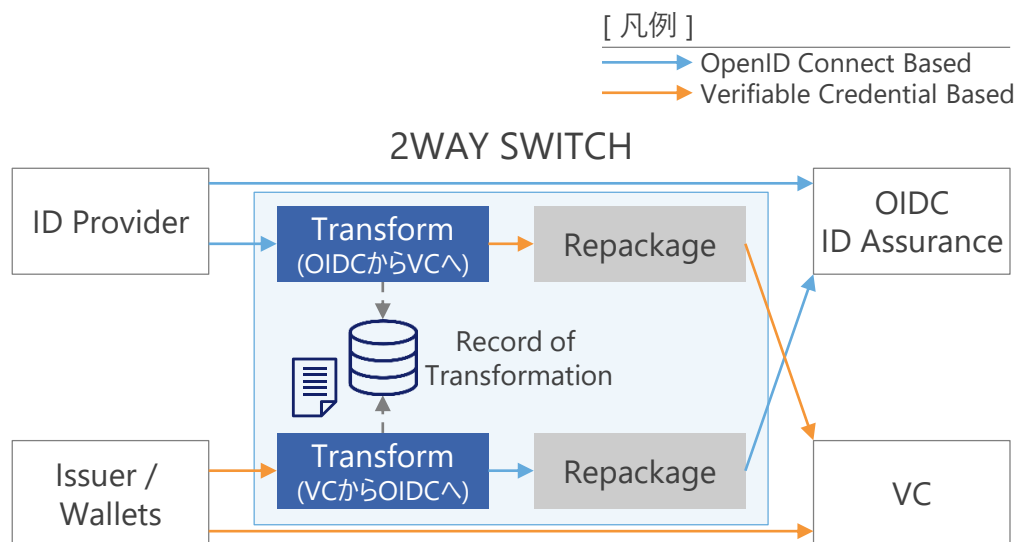
## モデル間・メソッド間における相互運用性への考慮

- クレーム連携では、異なるモデル間での相互運用性（External Interoperability）、あるいは共にSSIモデルであっても利用しているメソッド間での相互運用性（Internal Interoperability）への考慮が必要。
  - 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。
  - 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・リゾーブ・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。
- 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、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。

総合運用性の考慮対象例



モデルのスイッチング事例イメージ





## 3-4-2. SSI/DIDの課題 - (1) 技術面での課題

### DIDの認定や規格適合性

■ 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

- 1章で紹介したFIDOのUAF、U2F、FIDO 2 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。
- 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。

#### OpenID Foundationから提供されている規格適合性テストイメージ

The screenshot shows a test result that has failed. At the top, there are two red bars: the first says "INTERRUPTED" and the second says "FAILED". Below this, the test details are listed:

- Test Name: oidcc-client-test-3rd-party-init-login
- Variant: client\_auth\_type=client\_secret\_basic, request\_type=request\_object, response\_type=code, response\_mode=form\_post, client\_registration=static\_client
- Test ID: 7XsfXd1ZAg0QAWA
- Created: Tue Apr 20 2021 20:56:01 GMT+0900 (日本標準時)
- Description: The client is expected to register with a valid 'initiate\_login\_uri'. The user is sent to that url, which should result in the RP redirecting the user to the authorization endpoint and the normal 'happy path' sequence completing.

At the bottom, the results summary shows: SUCCESS 4, FAILURE 1, WARNING 0, REVIEW 0, INFO 1.

The screenshot shows a test result that has passed. At the top, there are two bars: a dark grey bar saying "FINISHED" and a green bar saying "PASSED". Below this, the test details are listed:

- Test Name: fapi-rw-id2-ensure-valid-pkce-succeeds
- Variant: client\_auth\_type=private\_key\_jwt, fapi\_auth\_request\_method=by\_value, fapi\_profile=plain\_fapi, fapi\_response\_mode=plain\_response
- Test ID: UTZ74cN3tLP43j
- Created: Tue Apr 20 2021 14:43:34 GMT+0900 (日本標準時)
- Description: conformance suite instructions example using Authlete FAPI-RW-ID2 with private\_key
- Test Version: 4.1.11
- Plan ID: w57J8AqyEXxls

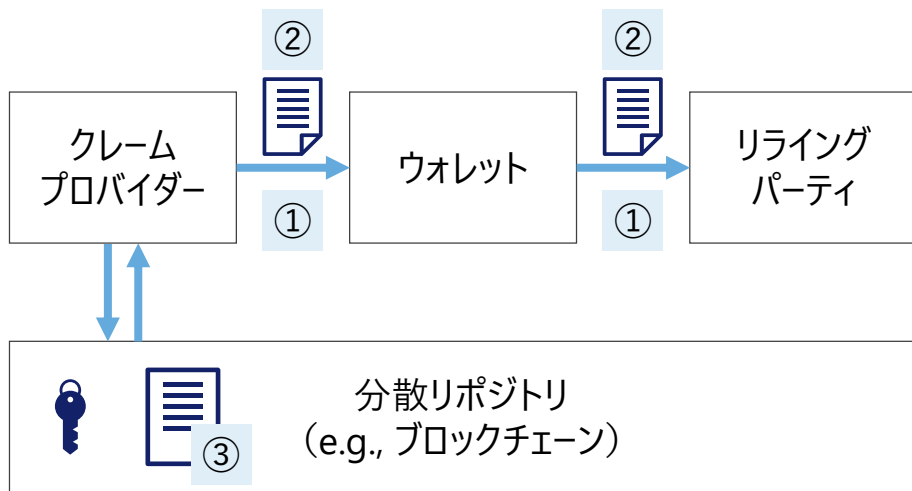
A text box below the description explains: "This test makes a FAPI authorization request using valid PKCE (RFC7636), which must succeed. FAPI-RW-ID2 does not require servers to support PKCE, but as per https://tools.ietf.org/html/rfc6749#section-3.1 The authorization server MUST ignore unrecognized request parameters - i.e. whether the server supports PKCE or not, a valid PKCE request must succeed. The reason for this test is that many OpenID Connect clients speculatively use PKCE, and the OAuth2 standard requires that requests from such clients must not fail."

At the bottom, the results summary shows: SUCCESS 103, FAILURE 0, WARNING 0, REVIEW 0, INFO 13.

## Cryptographic Agilityへの考慮

- 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項で述べた「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。

### Cryptographic Agilityの考慮対象



- ①通信経路（対向認証・経路暗号）
- ②クレーム
- ③クレーム検証のための情報（eg, DID、DID Doc等）

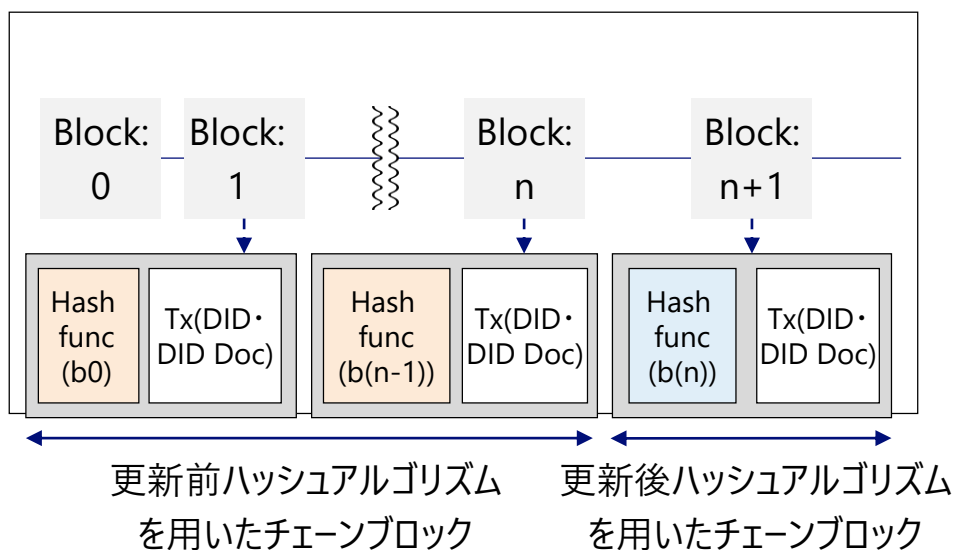
- 3-2節で述べた処理フローを踏まえると、少なくとも①対向認証・経路暗号、②クレーム、③クレーム検証に必要な情報、の3か所において、用いられるアルゴリズムに対する危殆化への考慮が必要。
- ①は動的な要求に基づく処理であり、移行対応の主体であるクレームプロバイダー・ホルダー・リライティングパーティが存在する前提での、当事者の対応（新しい暗号アルゴリズムへの切り替え等）を整理する必要がある。
- 一方で、②・③は、過去生成された情報も対象となる。危殆化の対応主体エンティティの一つであるクレームプロバイダーが既に存在しない可能性を考慮した対処が必要となる。
- 例えば③では、パブリックブロックチ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（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\*）

### 3-4-2. SSI/DIDの課題 - (1) 技術面での課題

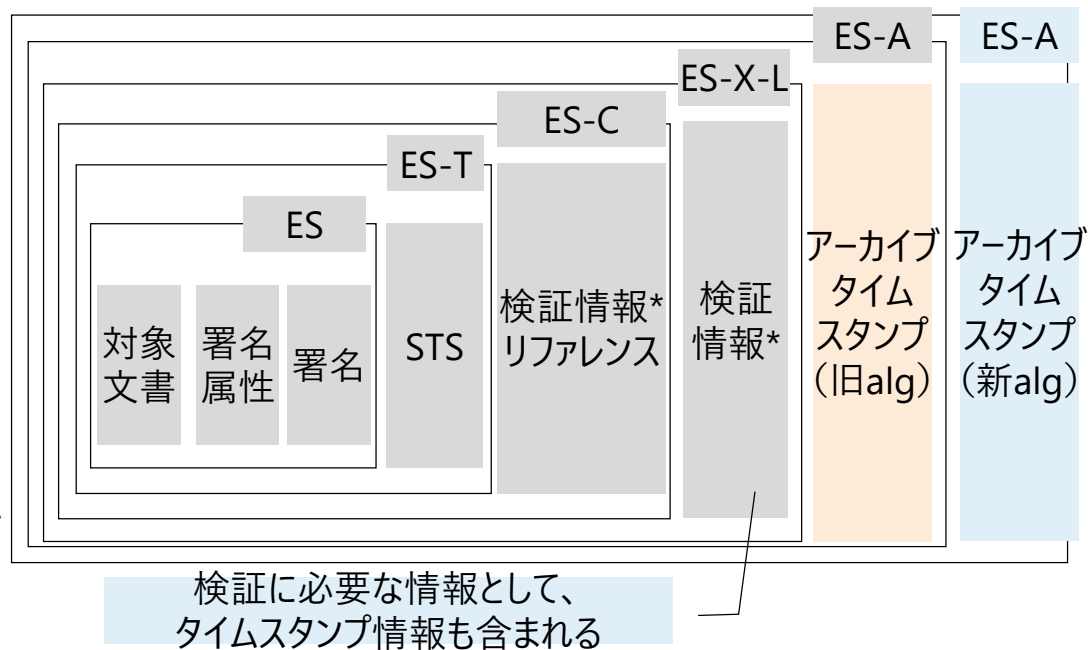
## 【参考】ハッシュアルゴリズム危殆化時の移行方式 (Blockchain方式・長期署名方式)

- ブロックチェーンを用いる場合、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。
- DID実現時には、ブロックチェーンだけでなく、長期署名方式を用いた分散リポジトリ等における実装も想定される。長期署名方式では、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。

Blockchainにおけるアルゴリズム移行方式



長期署名方式 (CAeSの例)



## 3-4-2. SSI/DIDの課題 - (1) 技術面での課題

### 形式検証によるセキュリティの担保

- 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。
- 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。

#### ISO/IEC 9798に対する形式検証適合と検出脅威例

検証対象の  
ISO/IEC 9798 Series

ISO/IEC 9798で言及されている考慮すべき  
Thread Model

- ISO/IEC 9798-1:2010
- ISO/IEC 9798-2:2008
- ISO/IEC 9798-3:1998
- ISO/IEC 9798-4:1999
- ISO/IEC 9798-2:2008/Cor 1:2010
- ISO/IEC 9798-3:1998/Cor 1:2009
- ISO/IEC 9798-3:1998/Amd 1:2010
- ISO/IEC 9798-4:1999/Cor 1:2009

1. Man-in-the-middle attacks
2. Replay attacks
3. Reflection attacks
4. Forced delay attacks

形式検証を適合

検出した脅威

対策

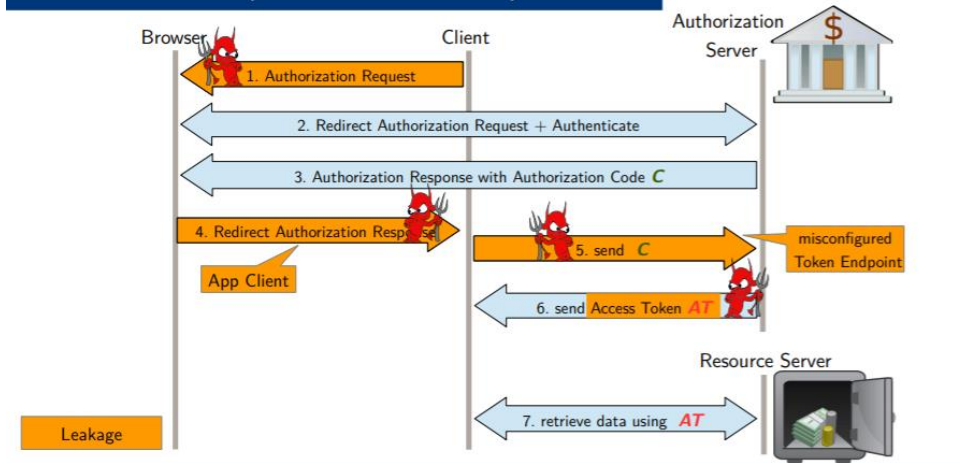
1. Role-mixup attacks
2. Type flaw attacks
3. Reflection attacks

1. Tagging
2. Removing ambiguity of optional fields
3. Explicitly stating assumptions on Spec

- ISO/IEC 9798シリーズに対し仕様内で言及されたThread Modelを踏まえ検証。
- Role-mixup attacks、Type flaw attacks、Reflection attacksの懸念を抽出。併せて、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、解決のためのfixを提示。
- 検証対象となるモデルを定義の上、Attackerモデルを定義し、検証を実施。
- Read / Read-Write 両Profileに対し形式手法を展開。
- Attackerモデルとして、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漏洩を定義。

#### 形式検証の概要とFAPIにおける検証事例

##### Attacker Model (Read-Write Profile)



### 3-4-2. SSI/DIDの課題 - (2) 非技術面での課題

## SSI/DIDの非技術面での課題

■ SSI/DIDの非技術面での課題として、以下の観点が考えられる

項目	観点	概要
1)法的/制度上の課題	政府および政策立案者の関与	<ul style="list-style-type: none"><li>SSIに対応した国民ID文書の提供を技術的・法的枠組みにも対応できるよう、制度上の課題に対応する必要がある。</li><li>例えば、SSI/DIDに対応した電子署名や電子取引の規制、および電子文書などの検証可能な証明書として位置づける等。</li></ul>
	プライバシー保護	<ul style="list-style-type: none"><li>SSIを推進・指示する人々のデータ、権利、プライバシーを保護するためのデータ保護規制に向けた既存制度の見直しや必要に応じて改定が必要。例えば、ウォレット操作のための秘密鍵を保護する権利を検討する等。</li><li>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、個人/機密データが分散台帳に登録されてしまう危険性がある。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。</li></ul>
2)運用上の課題	トラストフレームワーク	<ul style="list-style-type: none"><li>欧州連合の eIDASのような適格ID プロバイダー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。</li></ul>
	ライアビリティ	<ul style="list-style-type: none"><li>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の想定が不明瞭。</li></ul>
3)ビジネス上の課題	現行のIT/デジタルシステムの適応	<ul style="list-style-type: none"><li>SSI/DIDを利用可能とする、クレデンシャルの発行や検証を可能にするために、現在のITシステムの移行や新規システム構築が必要となる場合があるが、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。</li></ul>
	個人の導入/ユースケースの検討	<ul style="list-style-type: none"><li>現状SSI/DIDは広く普及しておらず、企業や政府が継続して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。</li></ul>

### 3-4-2. SSI/DIDの課題 - (2) 非技術面での課題

## 1) 法的/制度上の課題の課題詳細と取り組み事例・得られた示唆

■ 各課題の詳細および課題解決にあたり参考となる取組事例は以下の通り。

カテゴリ	課題	課題詳細	参考となる取り組み事例
1) 法的/制度上の課題	・政府および政策立案者の関与	<ul style="list-style-type: none"><li>・ SSI/DIDに対応したナショナルIDの提供を法的に対応できるよう、制度上の課題に対応する。</li><li>・ 例えば、SSI/DIDに対応した電子署名や電子取引の規制、および電子文書などの検証可能な証明書として位置づける等の検討が必要ではないか。</li></ul>	<ul style="list-style-type: none"><li>・ EUでは欧州委員会がEBP(European Blockchain Partnership)と共同で取り組むEBSI(European Blockchain Service Infrastructure)イニシアティブにおいて、欧州SSIフレームワークであるESSIF<sup>*1)</sup>(European Self-sovereign Identity Framework)の検討が進められており、eIDASへの適合を目的としてeIDAS Bridge<sup>*2)</sup>の策定等が行われている。</li></ul>
	・ プライバシー保護	<ul style="list-style-type: none"><li>・ SSIを推進・指示する人々のデータ、権利、プライバシーを保護するためのデータ保護規制に向けた既存制度の見直しや必要に応じて改定が必要。</li><li>・ 例えば、ウォレット操作のための秘密鍵を保護する権利を検討する等。</li><li>・ 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、個人/機密データが分散台帳に登録されてしまう危険性がある。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。</li></ul>	<ul style="list-style-type: none"><li>・ 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な米国ワイオミング州は、ブロックチェーン関連の法律をいくつも制定しているが、この中で、「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」時の条件を限定する追加条文案が提案され、個人の「秘密鍵」を守る権利の保護強化を目指す動きとして注目を集めた。</li><li>・ Sovrin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として、Sovrin Legerへの書き込みを行うTransaction Authorsに関し、Permissioned Write Access policesでは法人のみが書き込み可能とし、個人は書き込みをできないようにする旨ガバナンスフレームワークに規定している。</li></ul>

\*1) European Commission, <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505734>

\*2) European Commission, <https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about>

## 【参考】政府および政策立案者の関与：EUにおける取組事例

- 法的/制度上の課題のうち、現在国内外で最も検討・議論が進んでいる問題の一つが、SSI/DIDに対応した電子署名や電子取引の規制、および電子文書などの検証可能な証明書として位置づけるための検討。
- 例えばEUでは、SSI/DIDとeIDASの接合に向けた検討が欧州委員会で進められている。
  - eIDASでは、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が本eIDASに適用されるかが論点となっている。
  - 本点については、eIDASをSSIEコシステムのトラストフレームワークと位置付ける、eIDAS Bridge<sup>\*1)</sup>や、欧州SSIフレームワークであるEBSI ESSIF<sup>\*2)</sup>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。

### 事例：eIDAS Bridge

- 欧州委員会は、eIDASをSSIEコシステムのトラストフレームワークとして利用可能にするために、eIDAS Bridgeを開発。
- eIDAS Bridgeは、イシュアのVerifiable credentialへの署名プロセスを支援し、ペリファイアのクレデンシャルのペリフィケーションプロセスにおけるイシュアのDIDの背後にいるイシュア（本プロジェクトでは法人を対象）の特定を支援する。eIDAS Bridgeを「渡る」ことにより、Verifiable credentialのトラストが証明される仕組み。



\*1) eIDAS Bridge詳細 <https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about>

\*2) ESSIF詳細 <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pagelid=262505360>

### 【参考】プライバシー保護：米国ワイオミング州の法案

- 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を推進していくにあたっては、このような思想やアーキテクチャの推進を後押しする制度が必要となる。
- 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。

#### 事例：米国ワイオミング州の法案

- 米国ワイオミング州は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、ブロックチェーン関連の法律をいくつも制定している。
- この中で、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ている。
- 本法案は、2021年4月に否決されているが、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。

#### 「秘密鍵の開示(Disclosure of private cryptographic keys)」

#### 34-29-107. 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。



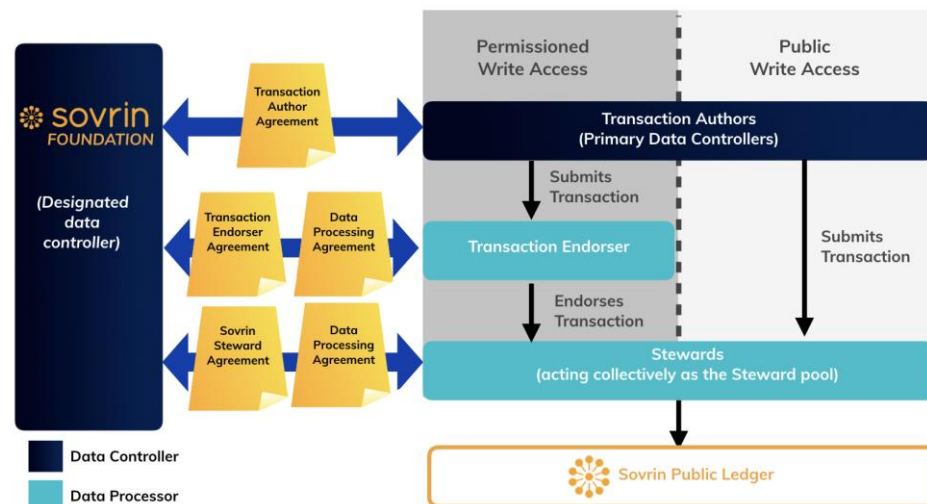
## 【参考】プライバシー保護：Sovrin財団の取組

- SSI は既存の多くのプライバシー問題を解決することができるものとして注目されている。例えば、代表的なものとしては、EUの一般個人データ保護規則（GDPR）の第17条で規定される忘れられる権利等への対応等に関しては、SSI/DIDにより個人はデジタル情報にリンクされた自分の情報をコントロールすることができるため、ユーザにとっても、また unnecessary 個人データの管理が不要となるデータ管理者にとっても有益なソリューションとなる可能性がある。
- しかしながら、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。

### 事例：Sovrin財団の取組

- Sovrin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右図のように整理している。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、法人のみが書き込み、個人は書き込みできない。Sovrinこの理由の一つに、以下を挙げている。

“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。”



### 3-4-2. SSI/DIDの課題 - (2) 非技術面での課題

## 2)運用上の課題の課題詳細と取り組み事例・得られた示唆

カテゴリ	課題	課題詳細	参考となる取り組み事例
2)運用上の課題	・トラストフレームワーク 運用制度	<ul style="list-style-type: none"> <li>欧州連合の eIDASのような適格 IdP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。</li> </ul>	<ul style="list-style-type: none"> <li>例えば、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した「SSI eIDAS Legal Report」が発行されている。<sup>*1)</sup></li> </ul>
	運用スキームの整理	<ul style="list-style-type: none"> <li>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る。</li> <li>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。</li> </ul>	<ul style="list-style-type: none"> <li>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は、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。ただし、課題詳述に挙げた統制機能などの一部はまだ議論・策定段階のものもある。</li> </ul>
	運用業務の遂行	<ul style="list-style-type: none"> <li>TF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。</li> <li>TFの維持・活用に際し必要な統制機能として、下記点が挙げられる。 <ul style="list-style-type: none"> <li>参画団体の管理・認定</li> <li>策定ポリシーの執行</li> <li>フレームワークの運用</li> <li>他TFとの相互運用性確立</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>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<sup>*1)</sup>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・実装することで、相互運用性を確保している。</li> </ul>

\*1) European Commission - SSI eIDAS Legal Report : [https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI\\_eIDAS\\_legal\\_report\\_final\\_0.pdf](https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf)

## 2)運用上の課題の課題詳細と取り組み事例・得られた示唆

カテゴリ	課題	課題詳細	参考となる取り組み事例
2)運用上の課題	・ライアビリ 責任分界点 ティ	<ul style="list-style-type: none"> <li>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の想定が不明瞭。</li> <li>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。</li> </ul>	<ul style="list-style-type: none"> <li>OIXではトラストフレームワークの中で、SSIモデルへの対応についても触れており、本課題についても論点となっている。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。</li> </ul>
	ユーザの保護・支援	<ul style="list-style-type: none"> <li>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。</li> <li>例えば、 <ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul> </li> <li>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。</li> </ul>	<ul style="list-style-type: none"> <li>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。</li> <li>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、ウォレットベンダー、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議論も出ている。</li> </ul>
	開発・運用コスト負担	<ul style="list-style-type: none"> <li>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。</li> </ul>	<ul style="list-style-type: none"> <li>SecurekeyのVerifie.Meでは、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。</li> </ul>

## 【参考】ライアビリティ：OIXのトラストフレームワーク

- SSI/DIDの運用上/ビジネス上の課題の中でもSSI/DID特有の課題として指摘されているが、ライアビリティの問題である。すなわち、SSIモデルに基づくサービスでは、何か問題が生じた場合の責任分界に関する整理が現時点では不透明である。
  - 従前の集中型・Federation型のIMSモデルでは、ライアビリティの問題については、IdP/RP間で直接調整・交渉を行うことで整理することとがるが、SSIモデルでは、ウォレットを制御するユーザ自身がIdPとして振る舞うため、従来のIdPである国や企業・組織等が果たしている責務等をユーザ自身が果たす必要が生じることとなる。
  - 実際には、全てのユーザ自身にその調整を期待するのは不可能であり、金融包摂の観点からも何らかの支援が必要となるが、その支援を、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の想定が不明瞭である。本課題を解決しない限り、ユーザは安心してSSIモデルのサービスを利用せず、またRPも責任が不明瞭なサービスを提供しないため、本課題の解決の方向性を考えることが、運用上/ビジネス上重要となる。

### 事例：OIXのトラストフレームワーク

- 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、トラストフレームワークを有効に活用・運用するために以下の機能を指摘する。

項目	概要
ガバナンスとポリシー策定	• トラストフレームワークのルール策定と修正、意志決定、利害関係者の協力・調整、基準・手続き管理、説明責任の仕組み作り
ポリシーの実施	• 既存ポリシーの遵守の確保、実施メカニズム、評価または監査の実施、変更とリリースの管理
参加団体の管理	• 参加事業体の管理と登録、認定とトラストマーク、サポート、紛争解決、請求書発行
ネットワークの発展	• ネットワークの成長とサポート、マーケティング、コミュニケーション、戦略の開発
トラストフレームワークの運営	• 参加事業体や利用者へのサービス提供

### 3)ビジネス上の課題の課題詳細と取り組み事例・得られた示唆

カテゴリ	課題	課題詳細	参考となる取り組み事例
3)ビジネス上の課題	・現行のIT/デジタルシステムの適応 既存スキームとの相互運用性	<ul style="list-style-type: none"> <li>・SSI/DIDを利用可能とするために、クレデンシャルの発行や検証を可能にする等、現在のITシステムの移行や新規システム構築が必要となる場合がある。</li> <li>・連携先の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が必要となる事が予想される。</li> </ul>	<ul style="list-style-type: none"> <li>・ 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。但し3-4-2項でも述べた通り、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。</li> </ul>
	新規投資の発生	<ul style="list-style-type: none"> <li>・新規スキーム構築のためのコスト負担が発生する。また、上述の既存スキームとの相互運用性への考慮が無い場合には、両スキーム独立しての運用となり、両系の維持・運用コストが発生する。</li> </ul>	<ul style="list-style-type: none"> <li>・ SecurekeyのVerifie.Meでは、金融機関は共同で出資してVerified.Meを構築するモデルを採用することで、自社単独開発と比較してコスト低減を実現。</li> </ul>
	・ユースケースの開拓	<ul style="list-style-type: none"> <li>・現状SSI/DIDは広く普及しておらず、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。</li> </ul>	<ul style="list-style-type: none"> <li>・ Sovrin Foundationにおいても、今後のユースケース開拓の継続必要性が議論されており、例えば、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*1)。</li> <li>・ 既にCovid-19関連の事例として、IATAの“Travel Pass” *2)によるデジタルの形で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。</li> </ul>

## 3-5. SSI/DID活用時の金融規制上の論点

---

### 3-5. SSI/DID活用時の金融規制上の論点

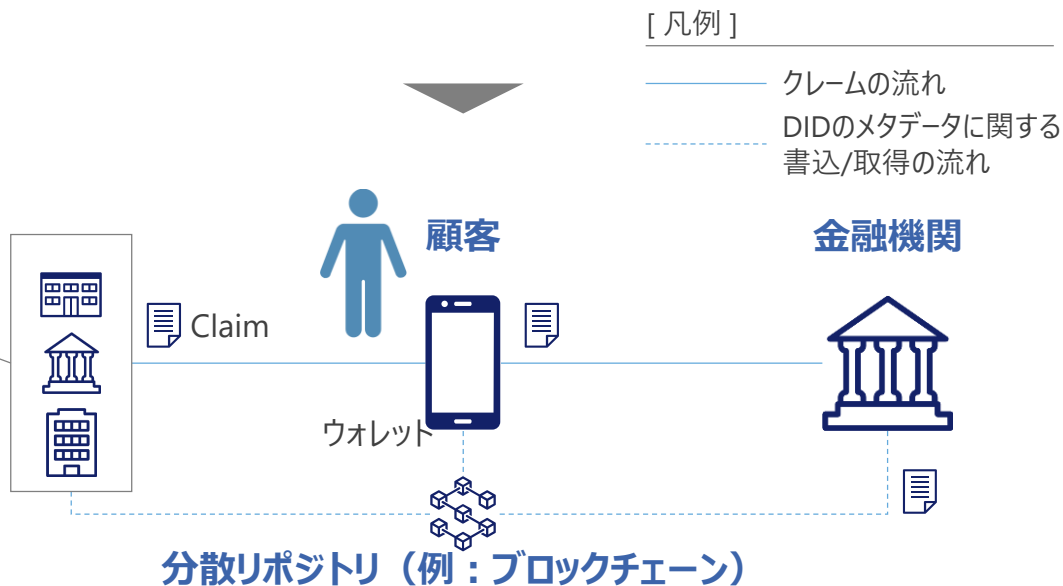
## 金融規制上の論点を検討する上でのSSI/DIDを活用したアイデンティティ管理の前提

- 前述のSSI/DIDモデルに金融取引主体を当てはめ、下段のモデルを検討の前提とする。
- 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。

(前述のSSI/DIDモデル (一般論))



(金融取引におけるSSI/DIDモデル)



### 3-5. SSI/DID活用時の金融規制上の論点

## SSI/DID活用モデルにおける金融規制上の論点の考え方

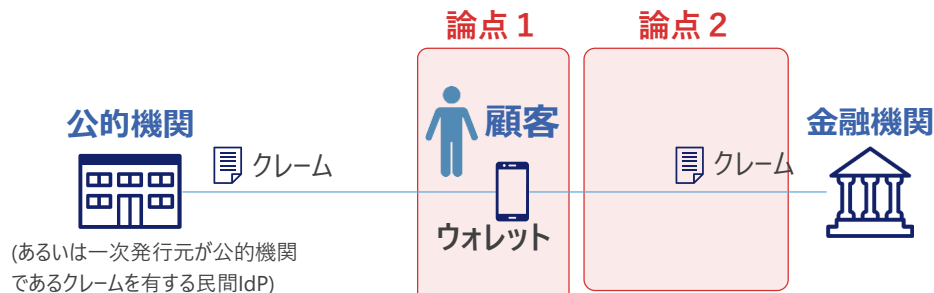
- 従来のデジタルアイデンティティ管理モデルとの大きな相違点は、以下2点である。
  - 相違点1) 金融機関へ連携されるクレームが全て顧客のウォレット起点になる
  - 相違点2) 金融機関へ連携されるデータが顧客が提示したクレームになる
- 上記2点に起因して、新たに金融規制の対象とする必要がある点を、論点として以降検討する。
  - 相違点1) についての論点：ウォレットに対する金融規制の考え方 (下図の論点1)
  - 相違点2) についての論点：新たな本人確認情報に対する法的手当て (下図の論点2)

従来のデジタルアイデンティティ管理モデル

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)、  
ユースケース(2) 継続的顧客確認/取引時確認



SSI/DIDを活用したデジタルアイデンティティ管理モデル



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





## 検討の前提と方法 (1) ウォレット運用形態のパターン

- ウォレット運用の形態を「データの運用管理主体」と「データの保管環境」の2軸で下図4パターンに分類し、ウォレット運用の形態の違いによる金融規制への影響を検討する。

No.	データの運用管理主体		データの保管環境	ウォレット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	<p>顧客 → データ処理 → 個人デバイスウォレット (DID, DID)</p>
2		委託先 (ウォレットプロバイダ)	ローカル	<p>顧客 → データ処理委託 → 委託先 → データ処理 → 個人デバイスウォレット (DID, DID)</p>
3		自己	クラウド	<p>顧客 → クラウドウォレット (DID, DID)</p>
4		委託先 (ウォレットプロバイダ)	クラウド	<p>顧客 → データ処理委託 → 委託先 → データ処理 → クラウドウォレット (DID, DID)</p>

## 検討の前提と方法 (2) 金融規制の実現可能性に関する評価項目

- 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認する必要がある。
- そのため、ウォレットに関して金融規制上問題となる以下3点について評価し、金融規制への影響を検討する。

①

ウォレット運用の  
信頼性

自身のIDと連携元のClaimのBindingが正しく行われ、顧客本人の正しい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

クレームの提示元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

金融犯罪捜査時の  
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ウォレット内のデータを捜査当局が調査できるかどうか

## ウォレットに対する規制の実現可能性評価結果

- 金融規制上は、現状では委託・クラウド型のウォレット運用形態が望ましいと考えられる。

規制の実現性	ウォレット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		
			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金融犯罪捜査時のウォレット内データ開示
↓	1	<p>自己/ローカル</p>	<p><b>低</b></p> <p>(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)</p>	<p><b>困難</b></p> <p>(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)</p>	<p><b>困難</b></p> <p>(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)</p>
	2	<p>委託/ローカル</p>	<p><b>高</b></p> <p>(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)</p>	<p><b>可</b></p> <p>(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)</p>	<p><b>困難</b></p> <p>(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)</p>
	3	<p>自己/クラウド</p>	<p><b>低</b></p> <p>(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)</p>	<p><b>困難</b></p> <p>(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)</p>	<p><b>可</b></p> <p>(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)</p>
	4	<p>委託/クラウド</p>	<p><b>高</b></p> <p>(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)</p>	<p><b>可</b></p> <p>(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)</p>	<p><b>可</b></p> <p>(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)</p>

## (補足) データの保管環境による金融犯罪捜査時等のウォレット内データ開示性の違い

- 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否した場合でも強制的に開示させる必要がある。
- 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、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。

パターンNo.	1	2	3
秘密鍵の保管環境	顧客のウォレット以外	顧客のウォレット	
ウォレットの保管環境	-	ローカル	クラウド
金融犯罪捜査時等のウォレット内データ開示	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。

## (ご参考) Amazon Web Service (AWS) の法律執行情報リクエストに対する考え方

- AWS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には、政府の要請に応じて必要な顧客情報を開示することとなっている。
  - 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、政府の要請に応じて顧客情報を開示する（下図赤線部）
  - なお、政府の要請に対しても必要な情報のみを文書で正式に要請された場合のみ開示する意思を示している。（下図青線部）

法律執行情報リクエストに対するAWSの説明ページ\*1)

### 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、政府の要請に応じ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。

\*1) <https://aws.amazon.com/jp/compliance/amazon-information-requests/>

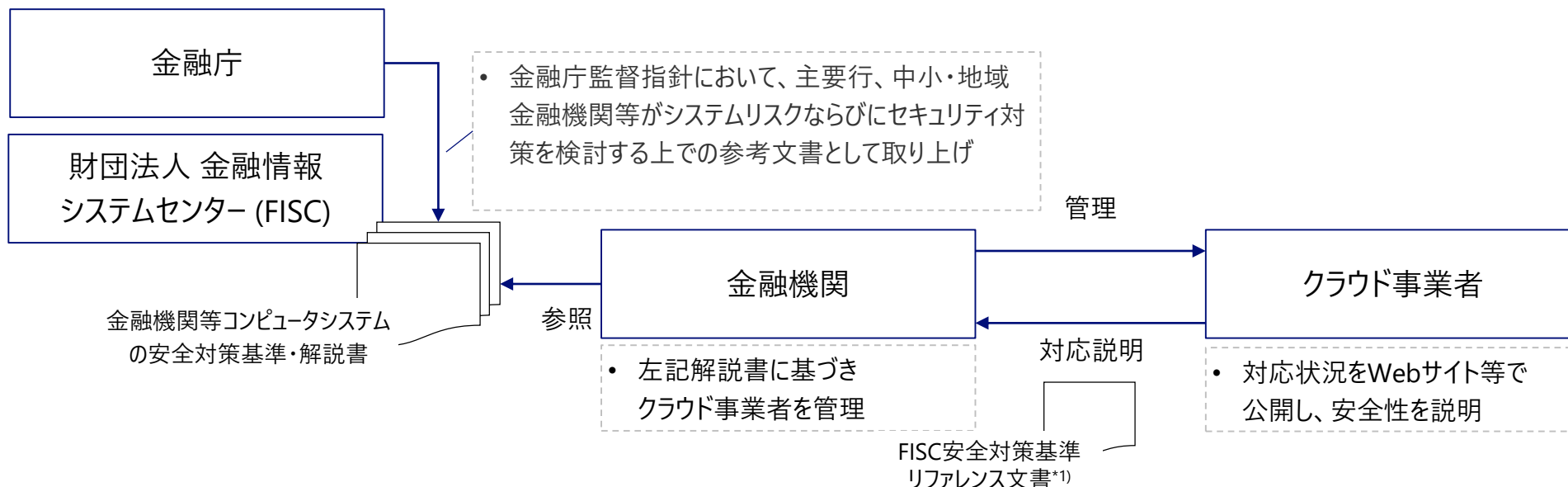
## ウォレットに対する金融規制の進め方についての示唆

- 金融機関に接続するウォレットを適切に規制する必要があるため、まず規制の難易度が最も低い「委託・クラウド型」に絞って金融利用を可能とするのが現実的と考えられる。
  - 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。
- 「委託・クラウド型」の場合、委託先であるウォレットプロバイダ、および、ウォレットプロバイダが利用するクラウドベンダを金融規制対象とする必要があると考えられる。
  - 一定の基準を満たしたウォレットプロバイダのみが金融機関へ接続できるよう、ルール化が必要と考えられる。
    - ・ 例えば、ウォレットプロバイダを登録制とし、登録済のウォレットプロバイダへ委託されたクレームのみ、口座開設や金融取引に利用可能とするよう、技術的に制限をかける、など。
  - ウォレットデータを保管するクラウドベンダが金融犯罪捜査時のデータ開示請求に対応できるよう、ルール化が必要と考えられる。
    - ・ 例えば、ウォレットプロバイダと同様、ウォレットデータを保管するクラウドサービスに対しても登録制とする、など
  - また、特定のウォレットプロバイダへの依存を回避するため、ウォレットプロバイダの変更が可能な状態（ポータビリティ）を確保する手当ても必要と考えられる。
- また、問題発生時の責任分界、金融犯罪捜査時のデータ開示請求について、あらかじめ定めておく必要があると考えられる。
- 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。(次頁に概略記載)
  - 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の間に契約関係はないものの、ウォレットプロバイダ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。

## (ご参考) 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

- 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、金融庁による金融機関の監督、金融機関によるパブリッククラウドサービスの評価、が行われている。

### 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



\*1) 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  
[https://d1.awsstatic.com/whitepapers/compliance/JF\\_Whitepapers/AWS\\_FISC\\_Guidelines\\_9thEdition.pdf](https://d1.awsstatic.com/whitepapers/compliance/JF_Whitepapers/AWS_FISC_Guidelines_9thEdition.pdf)

### 3-5. SSI/DID活用時の金融規制上の論点

## 論点2) 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がIdPとなるデジタルアイデンティティの形で行われることとなるため、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。
  - なお、デジタルアイデンティティとバインドされるClaimの発行元は、現状の発行元/ID連携元と同様と想定される。

#### 従来のデジタルアイデンティティとSSI/DIDにおける金融機関へ連携されるデータの形態と項目の比較

##### A) 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

	データの形態	データの項目
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
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Claim)	必要な項目のみ

##### B) 2章のユースケース (1-2) 口座開設 (ID連携) の場合

	データの形態	データの項目
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Claim)	各金融機関の本人確認用項目 (顧客に公開)



## 補論：フェデレーションモデルを用いたSSI/DID特性の充足可否

---

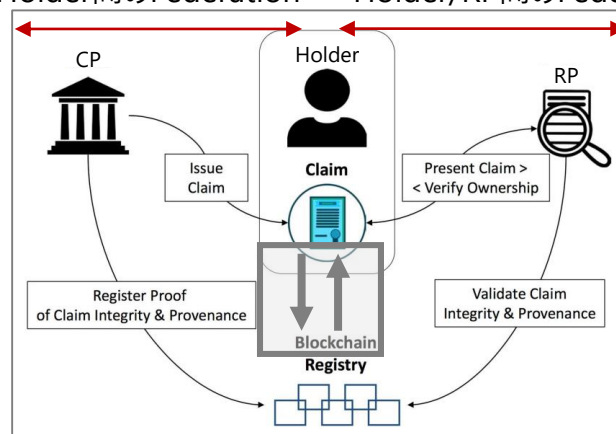
## (補論) フェデレーションモデルを用いたSSI/DID特性の充足可否

- 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IdPとなる形が考えられる。
- ユーザがIdPとなりクレームの連携を行う場合、どこにIdP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、フェデレーションモデル\* を2つ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、まずはフェデレーションモデルにおける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。

\*) Distributed / Aggregated Claims Modelの導入

### ローカルにIdP機能をデプロイする場合のSSIモデル実現像

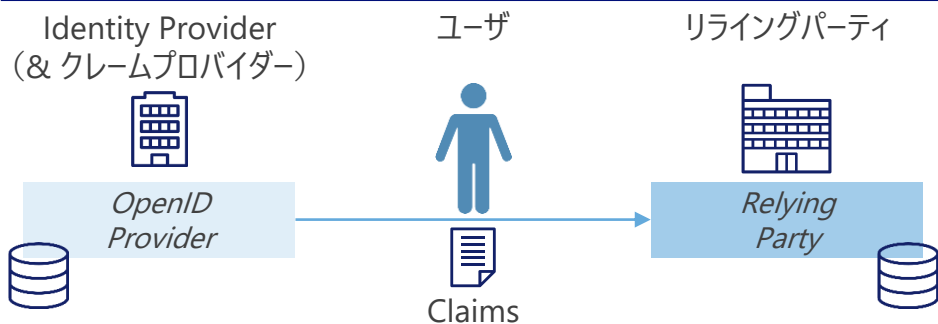
CP/Holder間のFederation    Holder/RP間のFederation



## (補論) フェデレーションモデルを用いたSSI/DID特性の充足可否

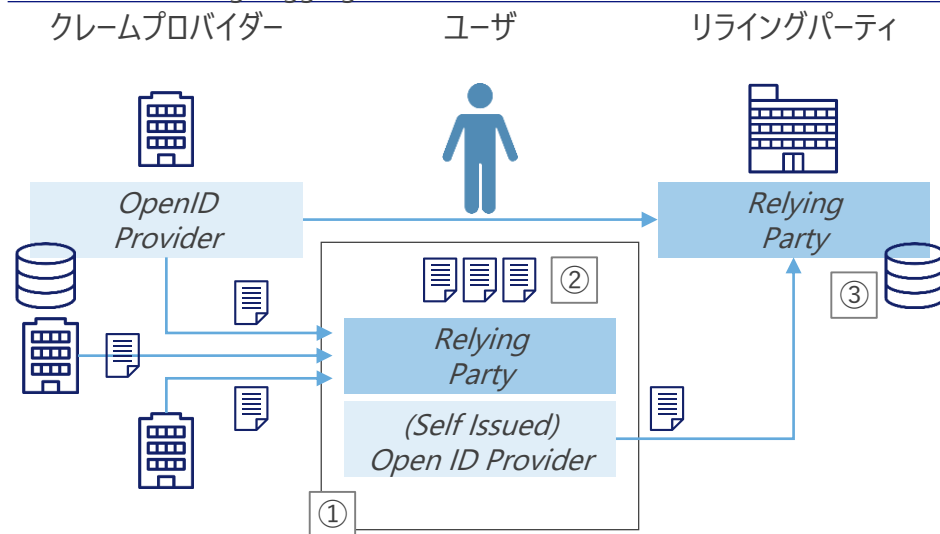
- OpenID Connectの仕様を用いトポロジーを変えることで、1. 認証と属性の分離、2. 分散した属性の活用・選択的な提示、3. 提示先の秘匿 (Unlinkability) の実装は可能である。

一般的なフェデレーションモデル



トポロジーを変えたフェデレーションモデル

(e.g., Aggregated / Distributed Claims Model)



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
	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
3. 提示先の秘匿 (Unlinkability)	Self-Issued Open Provider (SIOP)	ユーザ自身がIdPとなりCP/RP間の連携ではなく、ホルダー経由のクレーム連携が可能

## (補論) フェデレーションモデルを用いたSSI/DID特性の充足可否

- 4. 長期のデジタルアイデンティティの保管・利用については、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「CAAdES」、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。

### OpenID Connectでのクレームの仕様策定範囲

#### 5.7. Claim Stability and Uniqueness

The sub (subject) and iss (issuer) Claims, used together, are the only Claims that an RP can rely upon as a stable identifier for the End-User, since the sub Claim MUST be locally unique and never reassigned within the Issuer for a particular End-User, as described in Section 2.

(中略)

**All other Claims carry no such guarantees across different issuers in terms of stability over time or uniqueness across users, and Issuers are permitted to apply local restrictions and policies.**

出所) ETSI, ISO

### 長期署名規格例

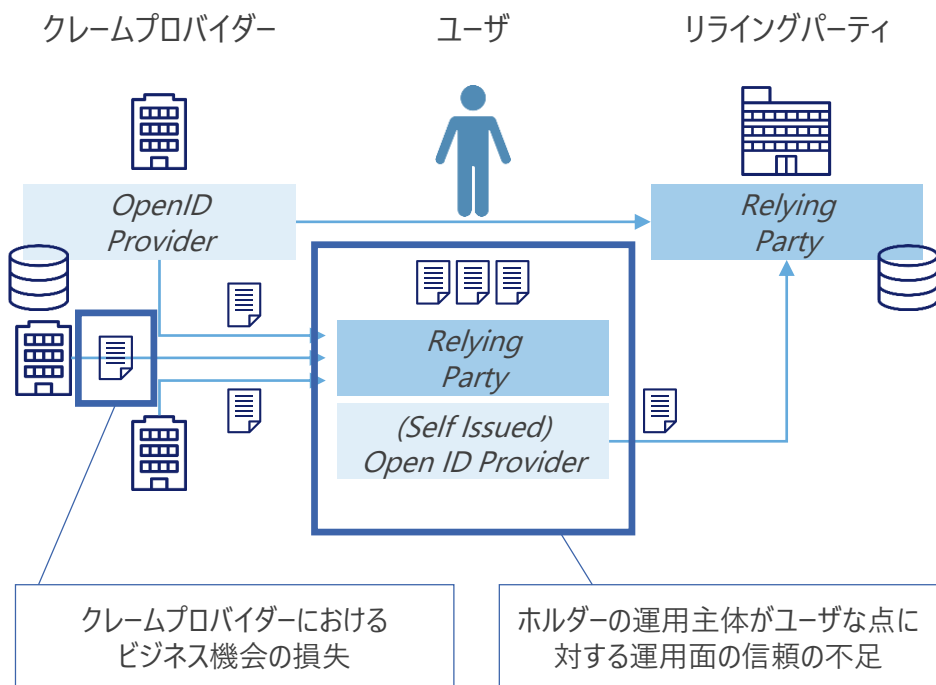
長期署名規格	対象 フォーマット例	主な規格 (Technical Specification)
CAAdES (CMS Advanced Electronic Signatures)	CMS, PKCS#7	ETSI TS 101 733 v2.2.1 (2013-04) ISO 14533-1:2014
XAdES (CMS Advanced Electronic Signatures)	XML	ETSI TS 101 903 v1.4.1 (2009-06) ISO 14533-2:2012
PAdES (PDF Advanced Electronic Signature)	PDF	ETSI 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)

## (補論) フェデレーションモデルを用いたSSI/DID実現における課題概観

- 前頁で述べた通り、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、サービスとして展開された事例※の調査・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。両面における課題はOpenID Connectに限らず、本項で述べた通り他のSSIモデル向け実装でも生じ得る課題である。

※) Linksafeによる分散型識別子の取得, neustarによるディレクトリサービス等

### フェデレーションモデルでのSSI/DID実現における課題箇所



### フェデレーションモデルの実サービスにおける課題例

- 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クレームプロバイダーによる、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、の運用・管理能力に対する懸念からクレームプロバイダー/リライングパーティホルダー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。

## 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

---

## 4 - 1. 本章の構成

---

### 本章の構成

#### ■ 本章の目的

- 本章では、第1章から3章で実施した分析を総括して、今後の課題について分析する。
- 具体的には、SSI/DIDを含むデジタルアイデンティティの活用にあたってさらに検討を要する分野、つまり今後、規制当局やエンジニア、事業者といった様々なステークホルダー関与の下で議論を進めるにあたっての論点の特定を行う。

#### ■ 本章の分析方法

- 上記の論点の特定について、まずは各章での検討の結果、現状明確な解決の方向性が示されていない論点を特定するとともに、これらの課題について、各ステークホルダーが持っている関心事項（Concern）を整理する（4-2）。



## 4 - 2. 各課題のステークホルダーとその関心事項

---

## 4-2. 各課題のステークホルダーとその関心事項

### 本節の構成

- 本頁以降では、2章、3章で挙げられた各課題に対する課題解決の方向性と、各課題に関するステークホルダーとその関心事項を検討する。
- 課題解決の方向性は、2-4節で取り上げた先進事例、3章での議論を参考に整理を行った。
- ステークホルダー／関心事項については、課題解決の方向性に影響を与えるステークホルダー・目的を洗い出し、潜在的な利害関係を整理した。
- 結果として、SSI/DIDに関連する課題であるか如何によらず、ステークホルダー間での利害関係を調整する必要があると思われる論点が複数存在し、マルチステークホルダーアプローチによる解決の必要性を示唆する結果となった。
- 第2章の課題を4-2-1、第3章の課題を4-2-2で分割して扱い、それぞれ以下の内容を記載する。両者には一部重複する課題（責任分界等）もあるが、ステークホルダーが異なっているため、別に記載した。

#### 4-2-1. デジタルアイデンティティの活用に向けた課題とステークホルダの関心事項

- 2章で挙げた課題の解決、および2章で挙げた課題をSSI/DIDで解決する際のステークホルダーおよび関心事項の抽出・整理を行った。

#### 4-2-2. SSI/DIDの活用に向けた課題とステークホルダの関心事項

- SSI/DIDを活用する際のステークホルダー・関心事項の抽出・整理を行った。

## 4-2-1. デジタルアイデンティティの活用に向けた課題とステークホルダの関心事項

### 1) “IAL”の課題解決の方向性とコンフリクト

カテゴリ	課題	課題解決の方向性	ステークホルダー	関心事項
1) IAL	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>適切なIALの設定およびIALとリンクしたAML規制の整備を行う。整備のアプローチとして、信頼性の高い国民IDを広く活用することを前提とし、それを可能とするAML規制の整備も考えられる。(②・③事例)</li> <li>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(①事例)。</li> </ul>	<ul style="list-style-type: none"> <li>金融当局</li> <li>金融機関</li> <li>顧客</li> </ul>	<ul style="list-style-type: none"> <li>プリンシプルベースで技術革新も取りこんだ対応の促進</li> <li>信頼性の高いID活用によるAML高度化</li> <li>信頼性の高いID活用によるAML高度化</li> <li>自社責任範囲の明確化のためのルール明確化</li> <li>利用できるアイデンティティの選択肢の豊富さ</li> </ul>

#### 4-2-1. デジタルアイデンティティの活用に向けた課題とステークホルダの関心事項

### 2) “ID連携”の課題解決の方向性とコンフリクト

カテゴリ	課題	課題解決の方向性	ステークホルダー	関心事項
2) ID連携	・ID連携当事者間の ビジネスモデル・責 任分界の未整備	<ul style="list-style-type: none"> <li>関係者間協議による、責任分界の明確化 (⑤事例)</li> <li>-デジタルIDを用いたKYC共有化を実現した際、各種チェック等を行う最終責任を明確化</li> <li>-新規口座開設時や継続的顧客管理実施時にデータの最新化が求められるため、その担い手・責任を明確化</li> <li>-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</li> </ul>	<ul style="list-style-type: none"> <li>金融当局</li> <li>金融機関 (デジタルIDの出し手/受け手)</li> <li>顧客</li> <li>ソリューションベンダー</li> </ul>	<ul style="list-style-type: none"> <li>規制監督の観点から責任の明確化</li> <li>ビジネス観点からの自社責任範囲の限定</li> <li>不利益を被った際の補償の観点から責任の明確化</li> <li>ビジネス観点からの自社責任範囲の限定</li> </ul>
	・特定の金融機関 (IdP)への依存度が高まる	<ul style="list-style-type: none"> <li>特定のIdP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。</li> <li>一方、3章で検討した通り、金融規制の実施においては、SSI/DIDのデータの運用管理はWalletベンダーに委託、Walletの管理環境はクラウドにあるといった、より信頼性のある管理体制の構築が望ましいという側面がある。</li> </ul>	<ul style="list-style-type: none"> <li>金融当局</li> <li>大手金融機関</li> <li>金融機関</li> <li>顧客</li> <li>Walletベンダー</li> <li>クラウドベンダー</li> </ul>	<ul style="list-style-type: none"> <li>より信頼性のある管理体制の構築</li> <li>IdPとしてID連携ビジネスの収益拡大</li> <li>RPとしてIdPに依拠することでコンプライアンスコストを低減</li> <li>特定IdPに依存しない管理</li> <li>収益拡大</li> <li>運用の自由度</li> <li>収益拡大</li> <li>運用の自由度</li> </ul>

#### 4-2-1. デジタルアイデンティティの活用に向けた課題とステークホルダの関心事項

### 3) “プライバシー”の課題解決の方向性とコンフリクト

カテゴリ	課題	課題解決の方向性	ステークホルダー	関心事項
3) プライバ シー	<ul style="list-style-type: none"> <li>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</li> <li>情報の第三者提供に関して、データ受取側として、データ提供側への説明と確認の対応負担が大きい</li> </ul>	<ul style="list-style-type: none"> <li>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者提供という形態を回避し、負担削減を図る。</li> </ul>	<ul style="list-style-type: none"> <li>個人情報保護当局</li> <li>金融機関・事業者（情報連携相手）</li> <li>顧客</li> </ul>	<ul style="list-style-type: none"> <li>顧客のプライバシー保護</li> <li>SSI/DIDによる情報の第3者提供にかかる対応負担削減</li> <li>新しい仕組みへの移行負担</li> <li>法令順守</li> <li>プライバシー保護</li> <li>新しい仕組みへの移行負担</li> <li>同意事項の明確化</li> </ul>
	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>事業者からのデータ利活用に関する説明内容の確からしさを、第3者による監査等でカバーする必要がある。</li> </ul>	<ul style="list-style-type: none"> <li>個人情報保護当局</li> <li>金融機関</li> <li>金融機関を監査する第三者機関</li> <li>顧客</li> </ul>	<ul style="list-style-type: none"> <li>顧客のプライバシー保護</li> <li>法令に従った対応の実施</li> <li>負担の少ない対応</li> <li>データ利活用促進</li> <li>規制遵守状況の確認</li> <li>法令に従った対応の実施</li> <li>プライバシーの確保</li> <li>法令に従った対応の実施</li> </ul>

## 4) “金融包摂”の課題解決の方向性とコンフリクト

カテゴリ	課題	課題解決の方向性	ステークホルダー	関心事項
4) 金融包 摂	・デジタル対応できない人物の金融排除	<ul style="list-style-type: none"> <li>・各国の現状の金融機関の業務整備状況や各国の政治体制等応じて対応</li> <li>– デジタルアイデンティティを活用した金融に必要なインフラ(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に基づき対応(②シンガポール・③インドの事例)</li> <li>– 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)</li> <li>・金融当局および金融機関はデジタル化によりAMLの高度化を図っている側面もあるため、AMLの高度化と金融包摂のバランスを取った対応が必要</li> </ul>	・金融当局	<ul style="list-style-type: none"> <li>・金融包摂の実現（特に新興国）</li> <li>・AML/CFTの高度化</li> </ul>
			・政府当局	・デジタル化の推進
			・金融機関	<ul style="list-style-type: none"> <li>・AML/CFTの高度化</li> <li>・経済性</li> </ul>
			・顧客	・金融サービスの円滑な利用

## 5) “相互運用性”の課題解決の方向性とコンフリクト

カテゴリ	課題	課題解決の方向性	ステークホルダー	関心事項
5) 相互運用性	・煩雑なID連携仕様への対応負担	・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(⑨オーストラリアの事例)	・金融当局	・政府IDを発行するような政府機関と民間の連携によるトラストフレームワークの策定などを通じたID連携環境の整備
			・標準化団体	・技術仕様策定 ・グローバル標準、コスト負担の大きい技術仕様
			・金融機関	・ソリューション利用 ・グローバル標準、コスト負担の大きい技術仕様
			・ソリューションベンダー	・ソリューション提供 ・グローバル標準、コスト負担の大きい技術仕様

## 6) “新しい業務へ移行するための投資判断”の課題解決の方向性とコンフリクト

カテゴリ	課題	課題解決の方向性	ステークホルダー	関心事項
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	・投資額を費用対効果の面から妥当なもの とするため以下等を検討 -インフラの共同利用によるコスト削減 -国として整備を進めるよう官の巻き込み -ID連携による収益化(⑤事例)	・金融当局	・AML高度化等の観点から、デジタルID の利用促進
			・金融機関	・効果に見合った投資
			・ID流通プラット フォーム提供者	・インフラ整備に妥当な対価の徴取



## 7) “クロスボーダー取引の諸課題”の課題解決の方向性とコンフリクト

カテゴリ	課題	課題解決の方向性	ステークホルダー	関心事項
7) クロス ボーダー 取引の 諸課題	<ul style="list-style-type: none"> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• 広域に適用可能なeIDを活用し取引時確認の統一化を行い、かつ広域に対して取引時確認統一化と平仄を合わせたAML指令を整備(①EU・⑦北欧の事例)のように、クロスボーダーを行う法域間での協調による対応が一つのアプローチとして考えられるか。</li> </ul>	<ul style="list-style-type: none"> <li>• 金融当局</li> <li>• 金融機関</li> <li>• 顧客</li> </ul>	<ul style="list-style-type: none"> <li>• 規制フレームワーク／トラストフレームワークの整備</li> <li>• コスト削減のため法域間の規制ギャップ減少</li> <li>• 利便性確保</li> </ul>

## 4-2-2. SSI/DIDの活用に向けた課題とステークホルダの関心

### 1) 法的/制度上の課題

カテゴリ	課題	課題解決の方向性	ステークホルダー	関心事項
1) 法的/制度上の課題	<ul style="list-style-type: none"> <li>政府および政策立案者の関与</li> </ul>	<ul style="list-style-type: none"> <li>SSIに対応した国民ID文書の提供を技術的・法的枠組みにも対応できるよう、制度上の課題に対応する必要がある。</li> <li>例えば、SSI/DIDに対応した電子署名や電子取引の規制、および電子文書などの検証可能な証明書として位置づける等。</li> </ul>	<ul style="list-style-type: none"> <li>金融当局</li> </ul>	<ul style="list-style-type: none"> <li>金融サービスのデジタル化の推進</li> </ul>
			<ul style="list-style-type: none"> <li>金融機関</li> <li>ユーザ</li> </ul>	<ul style="list-style-type: none"> <li>自社サービスへのSSI/DIDの利活用促進</li> <li>利便性の向上とプライバシー強化</li> </ul>
	<ul style="list-style-type: none"> <li>プライバシー対策</li> </ul>	<ul style="list-style-type: none"> <li>SSI/DIDを活用時における人権等の権利保護に関する制度見直し等。</li> <li>例えば、ウォレット操作のための秘密鍵を保護する権利を設ける等。</li> <li>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、個人/機密データが分散台帳に登録されてしまう危険性がある。必要に応じて規制の見直しや、運用ガイドライン等の策定が求められる。</li> </ul>	<ul style="list-style-type: none"> <li>政府当局</li> <li>ユーザ/消費者団体</li> <li>金融当局</li> <li>金融機関/事業者</li> <li>ユーザ</li> </ul>	<ul style="list-style-type: none"> <li>金融犯罪等時の情報（例：秘密鍵）開示</li> <li>権利保護（例：表現の自由、人権）</li> <li>既存の各種規制・ガイドラインで未整備の論点・課題の特定</li> <li>各種法規制等に準拠したサービス・ソリューションの提供</li> <li>プライバシー対策が十分なサービス判断</li> </ul>

## 2) 運用上の課題

カテゴリ	課題	課題解決の方向性	ステークホルダー	関心事項
2)運用上の課題	<ul style="list-style-type: none"> <li>・トラストフレームワーク</li> </ul>	<ul style="list-style-type: none"> <li>・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。</li> </ul>	<ul style="list-style-type: none"> <li>・ 金融機関・事業者</li> </ul>	<ul style="list-style-type: none"> <li>・ 規制遵守・サービス拡大</li> </ul>
			<ul style="list-style-type: none"> <li>・ 各国規制当局</li> </ul>	<ul style="list-style-type: none"> <li>・ トラストフレームワークの規制整備</li> </ul>
			<ul style="list-style-type: none"> <li>・ ユーザ</li> </ul>	<ul style="list-style-type: none"> <li>・ 利便性確保</li> </ul>
	<ul style="list-style-type: none"> <li>・ライアビリティ</li> </ul>	<ul style="list-style-type: none"> <li>・ SSIモデルでは、Wallet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の想定が不明瞭。</li> </ul>	<ul style="list-style-type: none"> <li>・ 金融当局</li> </ul>	<ul style="list-style-type: none"> <li>・ 規制監督の観点から責任明確化</li> </ul>
			<ul style="list-style-type: none"> <li>・ ユーザ</li> </ul>	<ul style="list-style-type: none"> <li>・ 不利益を被った際の補償の観点から責任明確化</li> </ul>
			<ul style="list-style-type: none"> <li>・ デジタルIDの出し手/受け手の金融機関/ID流通プラットフォーム提供者/ウォレットプロバイダー</li> </ul>	<ul style="list-style-type: none"> <li>・ リスク回避の観点から責任回避</li> </ul>

## 2) 運用上の課題

カテゴリ	課題	課題解決の方向性	ステークホルダー	関心事項
2)運用上の課題	・標準化	・ DID や VC などが、IEEE、ISO、ITU、NIST などの標準化団体（SDO）に受け入れられ、標準として推奨されるようになることが必要である。	・ 標準化団体	・ 技術仕様整備
			・ 金融当局	・ 規制整備・技術の規制への適用評価
			・ ID流通プラットフォーム提供者、ウォレットプロバイダー	・ アイデンティティソリューション・機能の提供・事業化
			・ 金融機関	・ ソリューション利用

## 3) ビジネス上の課題

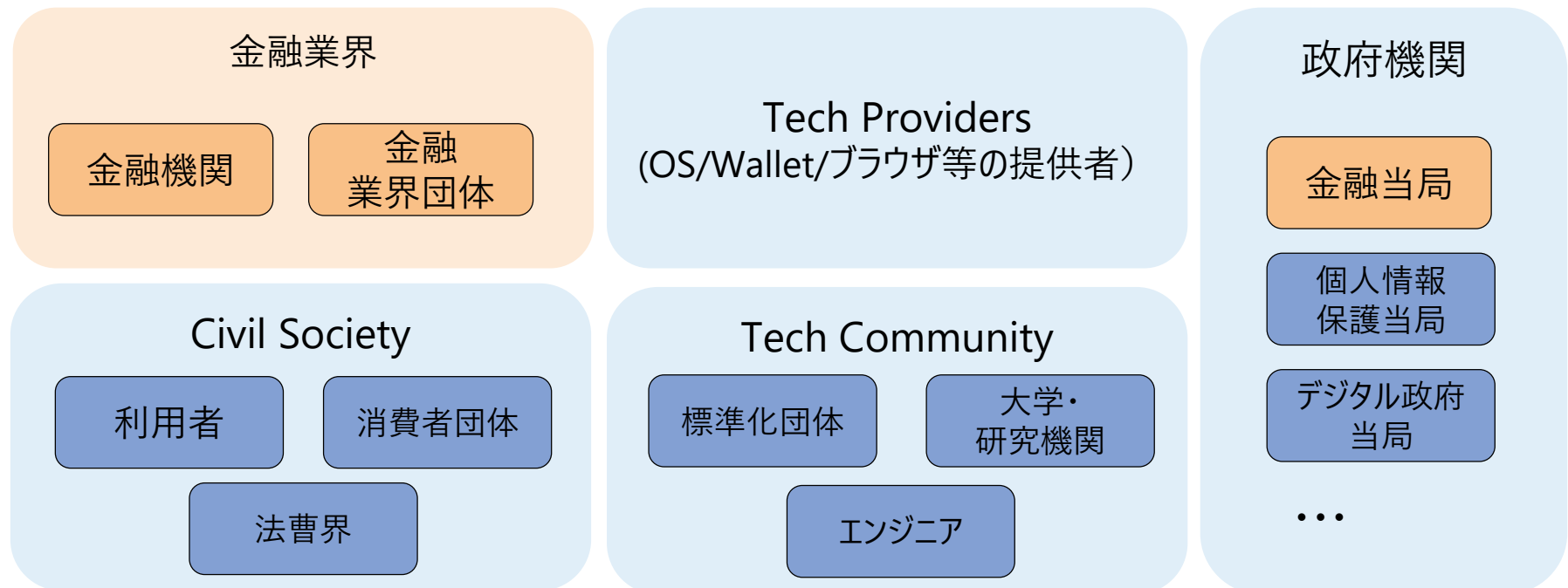
カテゴリ	課題	課題解決の方向性	ステークホルダー	関心事項
3) ビジネス上の課題	<ul style="list-style-type: none"> <li>• 現行のIT/デジタルシステムの適応</li> </ul>	<ul style="list-style-type: none"> <li>• SSI/DIDを利用可能とする、クレデンシャルの発行や検証を可能にするために、現在のITシステムの移行や新規システム構築が必要となる場合があるが、現状その投資に見合う利用が見込まれていない場合が多い。</li> </ul>	<ul style="list-style-type: none"> <li>• 各金融機関</li> <li>• 金融当局</li> <li>• ID流通プラットフォーム提供者・ウォレットプロバイダー</li> </ul>	<ul style="list-style-type: none"> <li>• 投資対効果の説明できる範囲で投資をとどめたい</li> <li>• 業界全体のオンボーディングコスト抑制の観点から、DIDの利用促進</li> <li>• インフラ整備に妥当な対価の徴取</li> </ul>
	<ul style="list-style-type: none"> <li>• 個人の導入/ユースケースの検討不足</li> </ul>	<ul style="list-style-type: none"> <li>• 現状SSI/DIDは広く普及しておらず、企業や政府が継続して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。さらに、SSIに適したアプリケーションの市場を開拓することも非常に重要。</li> </ul>	<ul style="list-style-type: none"> <li>• ユーザ</li> <li>• 消費者団体</li> <li>• 政府当局</li> <li>• 金融機関</li> <li>• ID流通プラットフォーム提供者、ウォレットプロバイダー</li> </ul>	<ul style="list-style-type: none"> <li>• サービスの円滑な利用</li> <li>• 消費者保護、デジタルディバイド回避</li> <li>• デジタル化の推進</li> <li>• 金融包摂の推進・AML規制強化</li> <li>• 参入障壁の排除</li> </ul>

#### 4-2-1/2. 各課題のステークホルダーとその関心事項

(参考) 金融業界は、今後、本調査で検討した論点を扱うにあたり、Tech Provider、Tech Community及び市民社会や金融以外の政府機関と課題解決を模索する必要がある。

- ステークホルダー (SH) の母集団として、デジタル競争本部で検討が進むTrusted Webの議論を参照した。
  - 「ステークホルダーには、従来のエンジニア、プラットフォーム事業者のみならず、サービス提供事業者、インフラ提供事業者、大学研究機関、利用者、消費者保護団体、シビルソサイエティ、法曹界、政府など様々なものを含む」  
(Trusted Web ホワイトペーパー Ver1.0、20頁)
- 上記を金融を念頭に置き換えて区分すると、次の通りとなる。金融業界は、4-2.で挙げた諸課題について、従来必ずしも交流の多くなかったステークホルダを含めて、議論を行って解決策を模索していく必要がある。

金融分野でのデジタルアイデンティティに関連する主なステークホルダ (オレンジ：従来の金融関連SH、青字：新たに加わるSH)



### (参考) マルチステークホルダーガバナンスの概要

- 金融庁「令和元年度：ブロックチェーン技術等を用いた金融システムのガバナンスに関する研究」では、分散型金融システムのガバナンスの検討において、「マルチステークホルダーガバナンス」の有効性について調査しているが、デジタルアイデンティティの課題についても、同様にマルチステークホルダーガバナンスが有効であると考えられる。
- 同調査研究報告書では、マルチステークホルダーガバナンスの長所について以下の通り整理している。

マルチステークホルダー型ガバナンスとは、ある事象に対する3者以上のステークホルダー（利害関係当事者）が、多様性とバランスを重視して構成され、それぞれが対等な立場で参加・議論できる会議を通じ、単体もしくは2者間では解決の難しい課題解決のために、合意形成などの意思疎通を図ることを目的とした、継続性のある統治メカニズム。

#### マルチステークホルダー型ガバナンスの長所

- マルチステークホルダー型ガバナンス（以下MSG）を実現するためには、まずもってマルチステークホルダーが集まった会議体が組成される必要がある。また、その会議体は、**多様性とバランスを重視**して組成される必要がある。
- 一方、会議体を構成するステークホルダーの多様性とバランスが担保されるためには、少なくとも**①ステークホルダーの直接的な利害、②担当者の社会的属性、③担当者の能力（ケパビリティ）**、等が明確に類型化されていなければならない。とりわけ①と②については、会議体全体を俯瞰したバランス（配分の均衡状態）が期待され、また③については一定以上の水準に達していることが要件となる。
- これを裏返せば、MSGを指向するということは、**当事者の役割が明らかにされる必要があること**を意味する。従って、前項（分散型金融システムがもたらす課題）の「課題の特定」で触れた、当事者の定義について、それが**明確にされることを事前に合意することが必要**となる。すなわち、分散型金融システムにおいてMSGの導入に合意するということは、分散型金融システムの当事者が自らの役割を相対化し、想定される全体の系の中での位置づけを明らかにしていくという営みに合意するということ、予め合意することになる。
- 一方、定義や役割が相対的に明確化されていけば、以下が可能となる。
  - **担うべき責任（あるいは免れるべき責任）の分解**
  - 責任に対する**当事者の有責性と限界領域**（無限と有限の区別）の設定
  - 分解された責任に基づく当事者同士の**分界点の設定**
- また、こうした役割と責任の特定が進めば、**①相互の尊敬（リスペクト）に基づく分業、②分業に基づく課題解決能力の向上、③MSGへの貢献のインセンティブ拡大**、が期待される。
- 具体的には、たとえば何らかのインシデントが発生した際、技術者、事業者、政府がそれぞれ**解決すべきことが役割分担**され、それぞれの責任において業務を**分業しながら効率的に課題解決に当たる**ことができる。また同時に、消費者を含めたステークホルダー間の**責任範囲の有限性**（免責の設定）について合意形成が図られれば、事業者を含めたステークホルダーのすべてにとって、**MSGへ貢献するインセンティブが形成**され、そうした**ガバナンス形態に基づく産業化が期待**される。