自己主権型/分散型アイデンティティ
技術調査ホワイトペーパー

TOYOTA CONIQ

TOYOTA CONIQ **Alpha**, Inc.

目次

図表一覧

1. はじめに

1.1.背景

書籍「さよなら、インターネット」に、このような記述があります[1]。

「わたしたちのデジタルアイデンティティは自身のコントロールから離散し、
自分自身の所有物ではなくなった。(〜中略〜)あなたがある日、
ソーシャルネットワークアカウントすべて削除したとしても、
あなたの個人のデータはインターネット上に残り続ける。」

デジタルとリアル（オンラインとオフライン）が融合する今、この不都合な真実はインターネットばかりではありません。私たちの個人のデータを含むデジタルアイデンティティは、多くの場所で危険に晒されています。

私たちがオンライン上でサービスを受けたり何かを購入したりするために、多くの場合「自分は誰か」という情報を伝える必要があります。この「自分は誰か」というデジタル化された情報をデジタルアイデンティティといいます。

デジタルアイデンティティの普及や整備が進むにつれ、私たちの今日の生活は便利になった一方で、次のような問題が増えてきました。

- 企業は自社サービスをオンラインで提供する際、顧客を囲い込むことを目的に自社アカウントの登録を促し、ビジネスで活用することを念頭にできるだけ多くの顧客情報を集めようとします。何かしらのチケットをリアルの窓口で買う時は求められることはないのに、オンライン購入では住所・氏名・年齢・職業等チケット購入には必要ない個人のデータまで入力を求められる、といったことがその一例です。本来、生活者が企業に個人情報を提供する際には、提供する個人のデータが何に使われるかを理解した上で、サービスを享受されるために必要であると納得した上で、提供すべきものです。
- 今日、生活者は利用するサービスごとに ID とパスワードを登録する必要があり、それぞれの企業に個人のデータを登録します。デジタルのサービスだけでなく、最近はリアル店舗でもオンライン活用が増え、生活者自身、どこに何の情報を登録しているか、利用するために必要な ID とパスワードは何だったかを全て覚えて管理することが簡単ではなくなりました。
- こうしたことを理由に、生活者は 1 つの ID とパスワードを複数のサービスで使い回すことが多くなりました。そして、 1 つの ID とパスワードの漏洩が、複数のサービスに影響を及ぼすような問題が、世界各国で起きるようになりました。
- その解決策として、特定企業のアカウントを用いて外部のサービスにログインできる認証連携の仕組みが開発されました。しかし、当該特定企業は、生活者がどの外部サービスを使っているのかを把握できてしまいます。さらに、当該特定企業のアカウントが何

らかの理由で強制的に利用停止になってしまった場合、認証連携の仕組みでログインできていたサービス全てを利用できなくなる新しいリスクが生まれてしまいました。

このような問題を解決するために、あなたのアカウントの管理をどこかに託すのではなく、あなたが自ら管理する仕組みが考えられています。実現する方法として、生活者が自らのデータに関するコントロール権を確保して生活者が許可した範囲で提供できるようにする自己主権型アイデンティティ（SSI: Self-Sovereign Identity）と呼ばれる思想と、生活者のアカウントが特定企業等に依存しないように依存度を下げることを目的とした分散型アイデンティティ（DID: Decentralized Identity）と呼ばれる技術が注目を集めています。

例えば、次のようなことが可能になります。

- 自らが管理するアカウントを使ってさまざまなサービスを利用できることで、特定企業によって利用サービスが把握されることや、アカウントの強制停止で複数のサービスが利用できなくなることを回避できる
- どの企業・サービスに、何の情報を提供するかを、自分の意志で決められる
- 自分の情報の保管場所や活用先を自ら選択できる

このように、便利かつ安心・安全なデジタル社会にむけて、自己主権型/分散型アイデンティティの仕組みを、生活者に“選択肢”として提供することが大事だと考えます。

1.2.目的

本書は、既存の ID 技術に基礎理解や関心があり、上記のようなライフスタイルを提案する「自己主権型/分散型アイデンティティ」についてキーワードは聞いたことがあるが、どのようにビジネスに適用すれば良いか困っている、ビジネスの企画・推進、または、その決裁に関わる方を想定読者とします。また、本書を通じて、自己主権型/分散型アイデンティティを用いたデジタル社会を実現させるための、「技術理解支援」と、「社会実装にむけての課題の提言」を行うことを目的とします。

これらの前提のもと、本書は、以下の構成をとります。

「ビジネス適用」の観点では、第２章「自己主権型/分散型アイデンティティのユースケース」にて自己主権型/分散型アイデンティティを用いたデジタル社会を実現させるためのユースケースを記述します。

第２章で挙げたユースケースに関連する「技術理解支援」の観点では、第３章「自己主権型/分散型アイデンティティを構成する要素（アーキテクチャ）」にて４つのレイヤーから成り立つ構成要素の概要を記述します。

「社会実装に向けての技術課題の提言」の観点では、本書で取り扱う４つの各レイヤー（後述）について、今後の技術選択を進める上での論点を、第４章「今後の展望」として記述します。

2. 自己主権型/分散型アイデンティティのユースケース

本章では、自己主権型/分散型アイデンティティで実現されるデジタル社会での体験について、２つのユースケースを用いて説明します。

まず、本章で用いる最低限の技術用語を下表にまとめます。詳細な技術解説は「3 自己主権型/分散型アイデンティティを構成する要素」をご参照ください。

用語	説明
VC	VC（Verifiable Credentials）とは「検証可能なクレデンシャル」と訳されます。VC は物理的な「クレデンシャル」が表すものと同じ情報を保持し、デジタル署名等の技術を用いて改ざんを防止し信頼性を高くしたもののことです。VC は身分証明証やチケット等（例えば、運転免許証、航空券、ホテルの予約情報）を、暗号学的に検証できるようにしたものです。
デジタル ID ウォレット	デジタル ID ウォレットは、VC を受領・保管・提供するために、所有者が使うものです。
所有者	デジタル ID ウォレットや VC を利用する者（アクター）のことです。本章の例では、移動体験を通して様々なサービスを享受する者が該当します。
発行者	デジタル ID ウォレットの所有者へ VC を発行する者（アクター）のことです。本章の例では、宿泊・運転・決済等をする際に必要な VC を発行するマイナポータルアプリやクレジットカードアプリが該当します。
検証者	デジタル ID ウォレットの所有者から VC を提供され、VC が発行者から所有者へ正しく発行された VC であるか検証する者（アクター）のことです。本章の例では、移動体験を通して様々なサービスを提供するための旅行代理店アプリやレンタカーキーシステムが該当します。

特に発行者・所有者・検証者と呼ばれる３つの登場人物は、通常は以下のようなやりとりで VC を受け渡します。

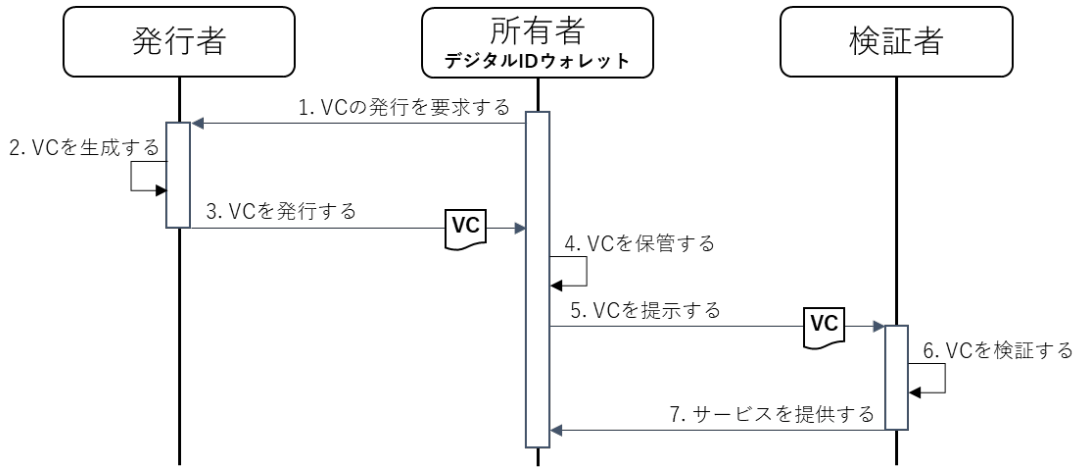


図 1 VC の受け渡しに関与する登場人物（発行者・所有者・検証者）

2.1. 移動体験におけるユースケース（チケットのデジタル化）

2.1.1. ユースケース概要

旅行代理店が提供するパッケージ旅行を予約し、電車・バス・レンタカー等を、デジタル ID ウォレットを通じて利用する移動体験を対象としたユースケースです。

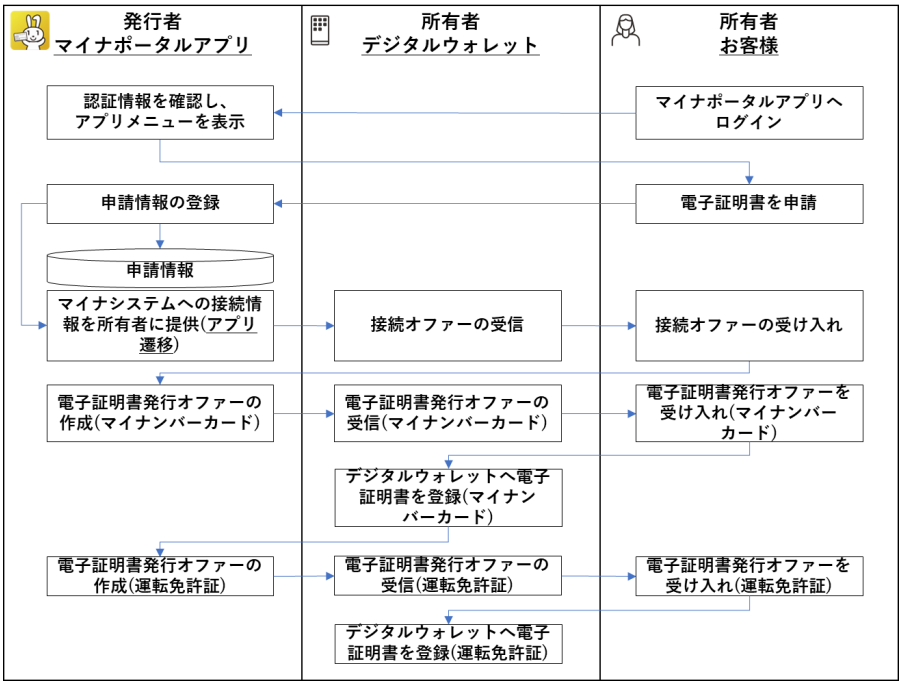
本ユースケースでは、移動体験（チケットのデジタル化）を検証するためのデモアプリを通じて、デジタル ID ウォレットで管理された VC を用いた移動体験を再現しています。（技術解説は「3.4.1 デジタル ID ウォレットの機能」を参照）

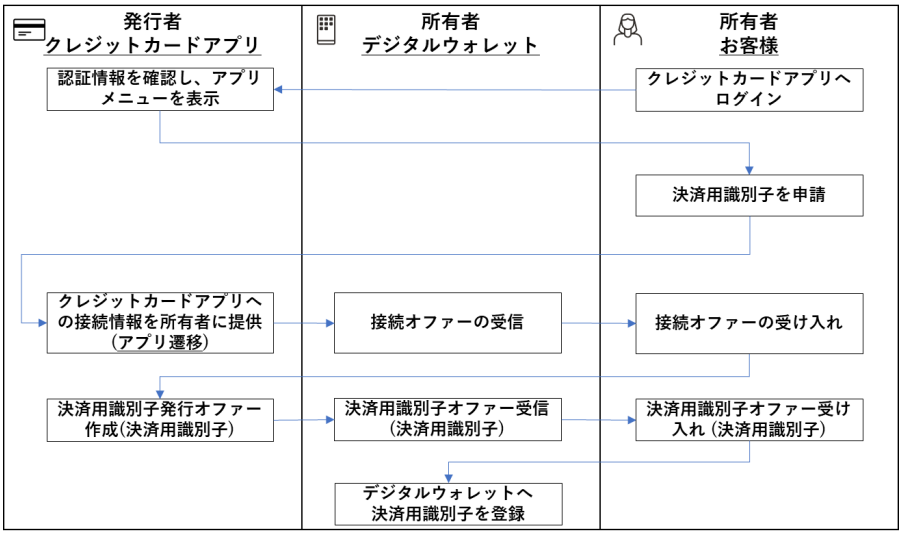
1. **VC の発行**
   所有者が、宿泊・運転・決済等をする際に必要な VC を、デジタル ID ウォレットに発行。（技術解説は「3.3.1 検証可能なクレデンシャルの受け渡しとフォーマット」を参照）
2. **VC の提供**
   デジタル ID ウォレットから、決済に必要な情報を、旅行代理店アプリに提供。（技術解説は「3.4.2 通信プロトコルの類型」の 1.遠隔型を参照）
3. **サービスの利用**
   所有者のデジタル ID ウォレットにある旅程表を使って、各種サービスや施設を利用。（技術解説は「3.4.2 通信プロトコルの類型」の 1.遠隔型を参照）

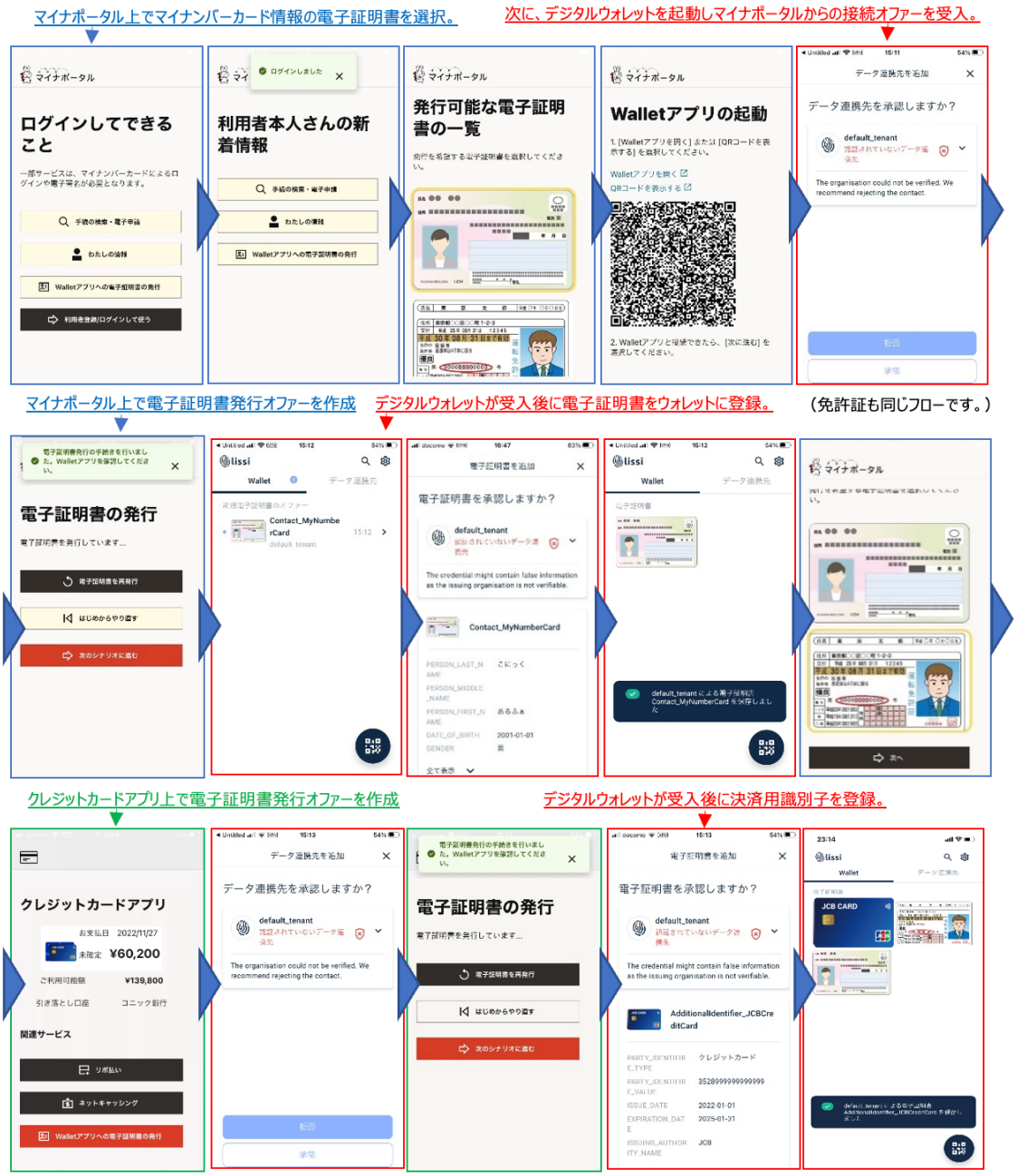
2.1.2. フロー

1. VC の発行

所有者が、宿泊・運転・決済等をする際に必要な、マイナンバーカード内に格納された基本４情報（氏名・住所・生年月日・性別）を含む電子証明書（公的個人認証）、運転免許証、決済用識別子に関する VC を、デジタル ID ウォレットに発行します。







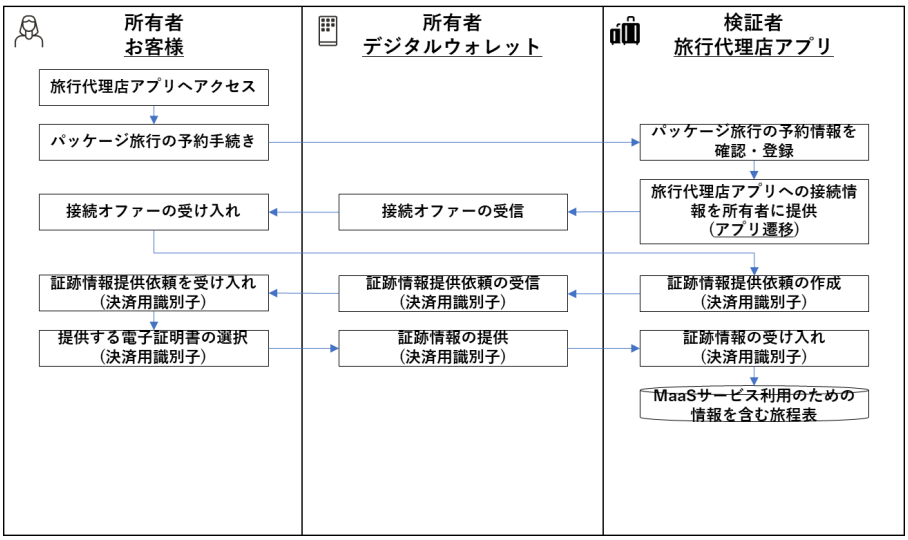
凡例　赤：電子ウォレット　青：マイナポータル　緑：クレジットカードアプリ　紫：旅行アプリ

図２移動体験におけるユースケース（チケットのデジタル化）のフロー－VC の発行

※マイナポータル部分については [2]をもとに作成

2. VC の提供

所有者のデジタル ID ウォレットから、決済に必要な決済用識別子を、旅行代理店アプリに提供し、旅行パッケージを購入します。旅程表等を入手し、所有者のデジタル ID ウォレットに発行します。



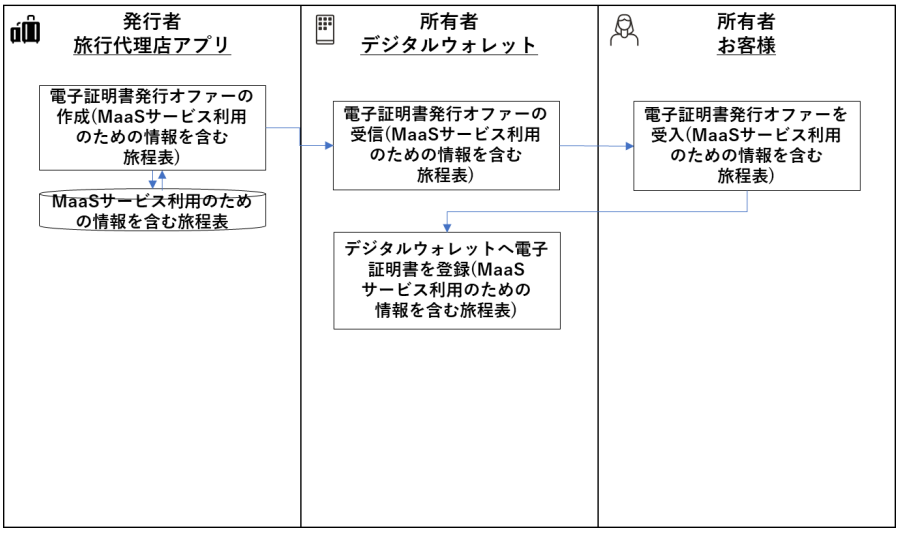


図３移動体験におけるユースケース（チケットのデジタル化）のフロー－VC の提供

3. **サービスの利用**

所有者のデジタル ID ウォレットに発行した各種チケット（鉄道乗者券、飛行機搭乗券、レンタカーのデジタルキー、ホテルルームキー）を使って、各種サービスを利用します。

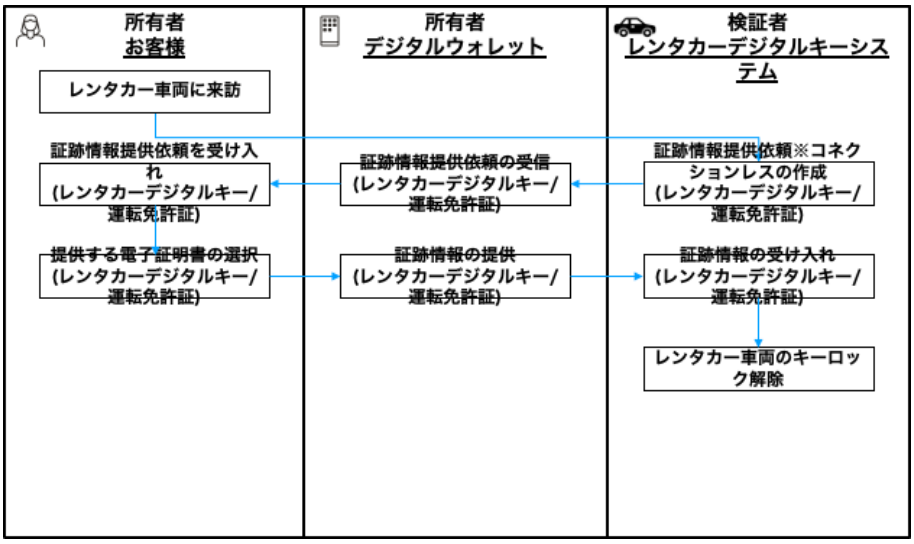


図４移動体験におけるユースケース(チケットのデジタル化)のフロー – サービスの利用

2.1.3. VC 関係図

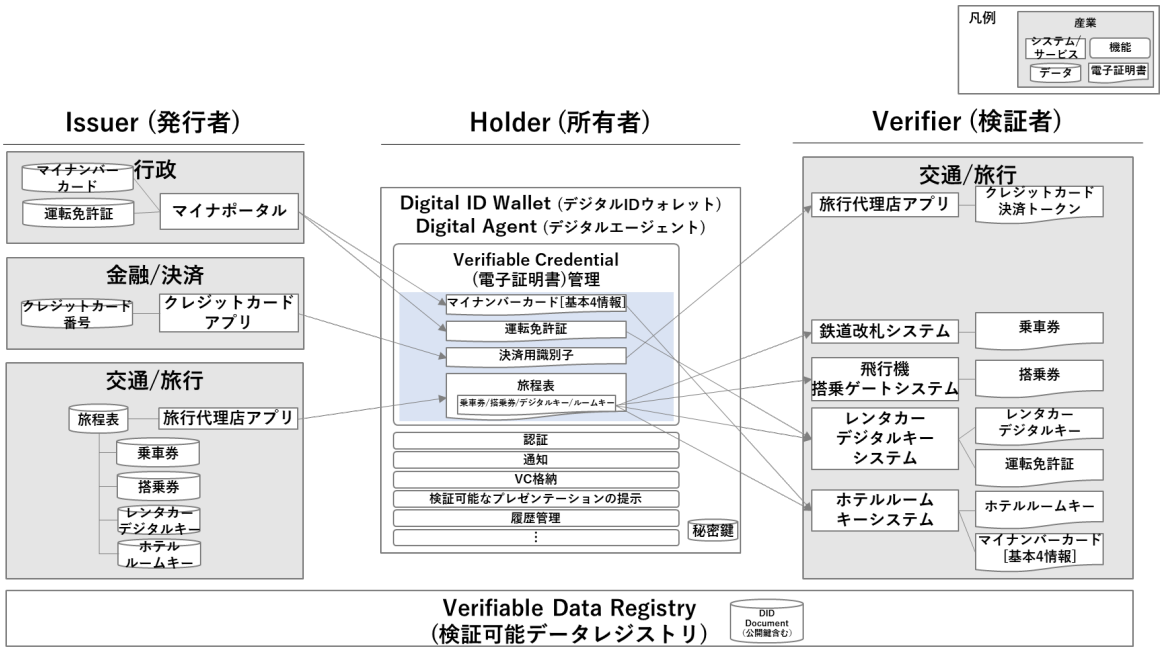


図 5 移動体験におけるユースケース(チケットのデジタル化)の VC 関連図

- 発行者と VC
  - 行政: マイナポータルから、マイナンバーカード内に格納された基本 4 情報(氏名・住所・生年月日・性別)を含む電子証明書（公的個人認証）と運転免許証に関する VC を、所有者に発行します。
  - 金融/決済: クレジットカード会社が管理する会員システムから、決済用識別子に関する VC を、所有者に発行します。
  - 交通/旅行: 旅行会社が管理するシステムから、パッケージ旅行に含まれるチケットに関する VC を、所有者に発行します。
- 検証者と VC
  - 交通/旅行: 移動体験を提供する各社が、決済情報、乗車券、搭乗券、運転免許証、ホテルルームキー等を検証し、サービスを提供します。

2.2. 移動体験におけるユースケース（マーケティングプラットフォーム）

2.2.1. ユースケース概要

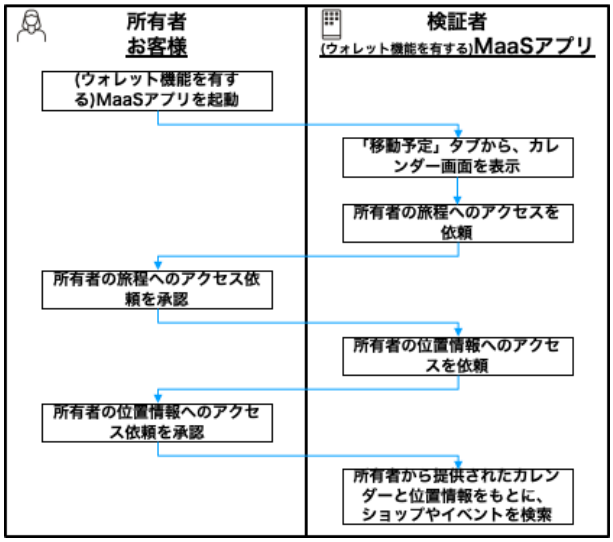
旅行者が持つスマートフォン内にインストールされた、デジタル ID ウォレット機能を有する MaaS アプリに旅行者の予定と位置情報を提供することで、旅行先の地域で使用可能なクーポンが提案される移動体験を対象としたユースケースです。

本ユースケースでは、以下のポイントについて検証するためのデモアプリを通じて、デジタル ID ウォレット機能を有する MaaS アプリで管理された VC を用いた移動体験を再現しています。（技術解説は「3.4.1 デジタル ID ウォレットの機能」を参照）

1. **旅程と位置情報の提供**
   所有者の旅程（カレンダー）と、位置情報を、デジタル ID ウォレット機能を有する MaaS アプリに提供。
2. **VC のレコメンデーション**
   デジタル ID ウォレット機能を有する MaaS アプリが、所有者から提供された旅程（カレンダー）・位置情報をもとに、旅行先の地域で使用できるクーポンをレコメンド。
   所有者は、デジタル ID ウォレットにクーポンの VC を格納。（技術解説は「3.5.1 識別子（DID）の仕様」を参照）
3. **サービスの利用**
   所有者は、デジタル ID ウォレット機能を有する MaaS アプリからレコメンドされたクーポンを用いて、各種サービスや施設を利用。（技術解説は「3.4.2 通信プロトコルの類型」の 2.近接型を参照）

2.2.2. フロー

1. **旅程と位置情報の提供**
   所有者の旅程（カレンダー）と位置情報を、デジタル ID ウォレット機能を有する MaaS アプリに提供します。



デジタルウォレット機能付きの MaaS アプリに、スマートフォンのカレンダー情報と位置情報、そして、旅程の情報提供を許可します。

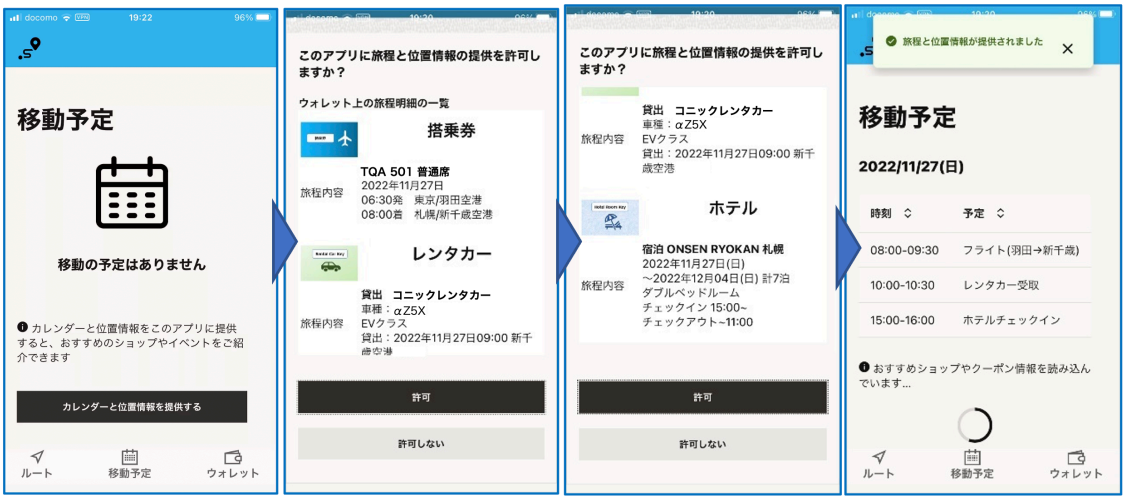
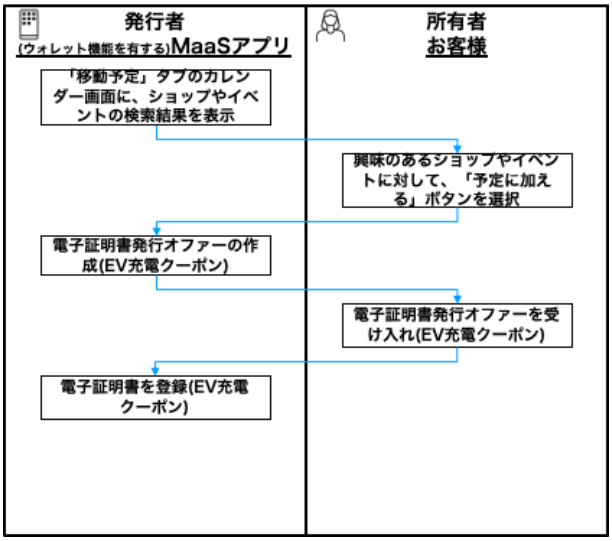


図 6 移動体験におけるユースケース（マーケティングプラットフォーム）のフロー - VC の提供

2. VC のレコメンデーション

デジタル ID ウォレット機能を有する MaaS アプリが、所有者の旅程（カレンダー）と位置情報から、旅行先の地域で使用できるクーポン（レストランで使える EV 充電クーポン）に関する VC を、所有者のデジタル ID ウォレットに発行します。



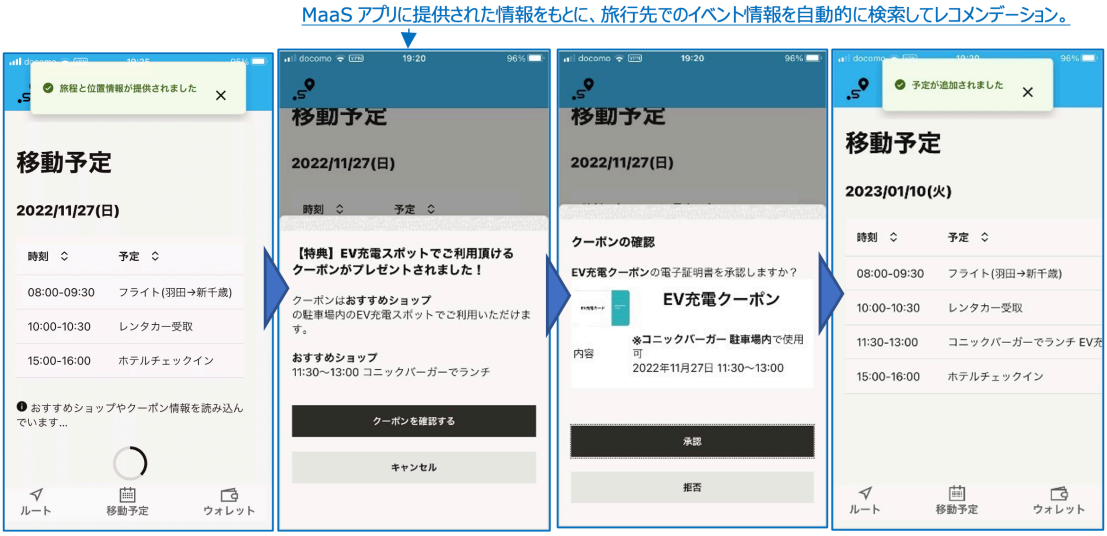
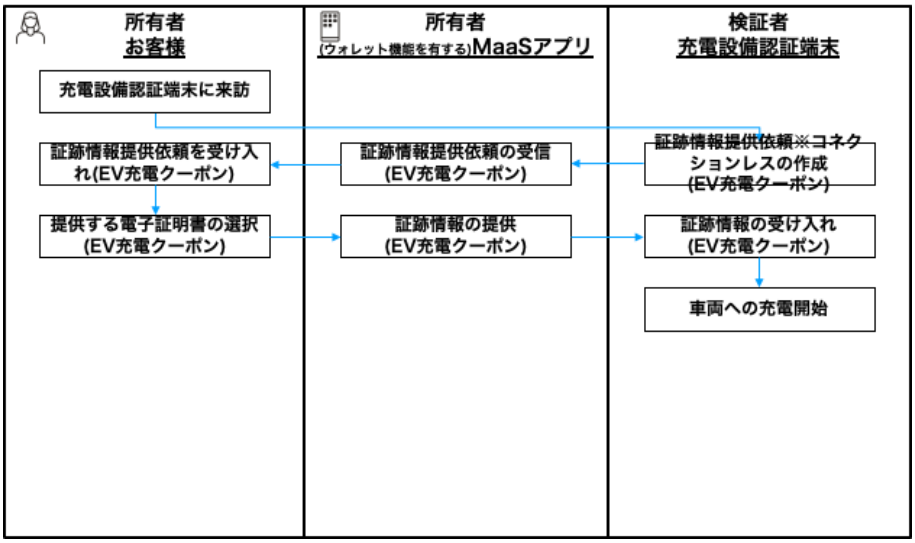


図 7 移動体験におけるユースケース（マーケティングプラットフォーム）のフロー - VC のレコメンデーション

3. **サービスの利用**

所有者のデジタル ID ウォレットから、EV 充電クーポンを、レストランの駐車場に設置された充電設備認証端末に提供します。



充電スタンドの QR コードを MaaS アプリ（ウォレット内蔵）で読取り、ウォレット内に保存された EV 充電クーポンを使用。

図 8 移動体験におけるユースケース（マーケティングプラットフォーム）のフロー - サービスの利用

2.2.3. VC 関係図

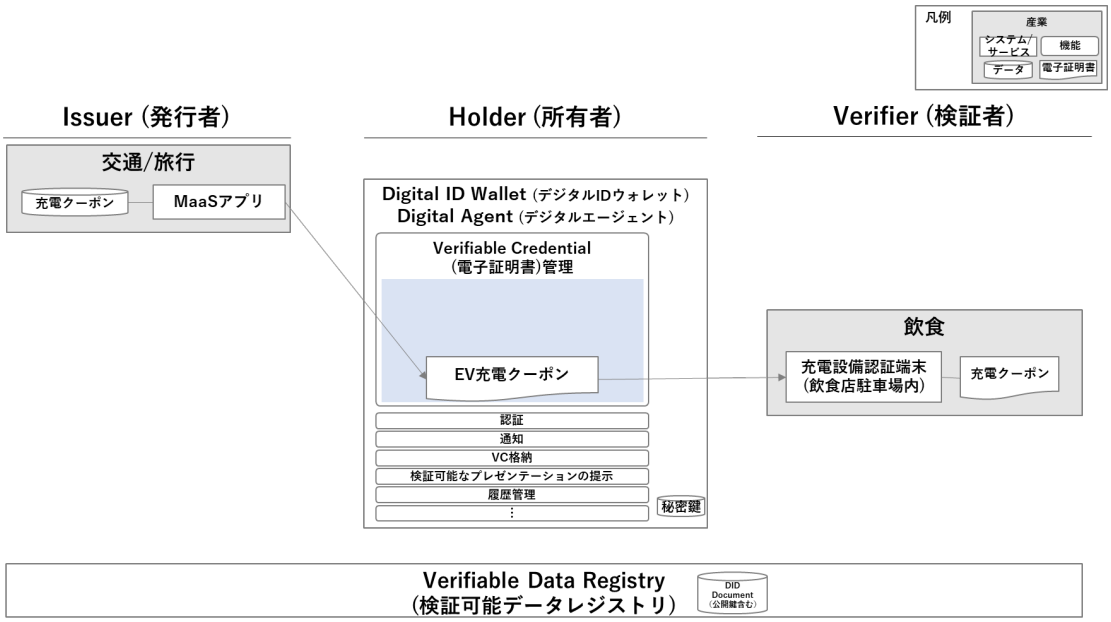


図 9 移動体験におけるユースケース（マーケティングプラットフォーム）の VC 関連図

- 発行者と VC
    - 交通/旅行: デジタル ID ウォレット機能を有する MaaS アプリから、旅行先の店舗等で使用できるクーポンに関する VC を、所有者に発行します。
- 検証者と VC
    - 交通/旅行デジタル ID ウォレット機能を有する MaaS アプリが、所有者の旅程（カレンダー）と位置情報を検証し、マーケティングのためのレコメンデーションエンジンへの学習データとして取り扱います。
    - 飲食: 旅行先の地域で使用できるクーポンを検証し、EV 充電サービスを提供します。

3. 自己主権型/分散型アイデンティティを構成する要素

本章では、自己主権型/分散型アイデンティティを構成する要素について、４つのレイヤーから概要を記述します。それぞれのレイヤーについて、概要とサービス展開にあたっての考慮事項を示します。

3.1.自己主権型/分散型アイデンティティの構成要素と４つのレイヤー

自己主権型/分散型アイデンティティを構成する要素は下図の通りです。構成要素には諸説ありますが [3]、本章では、2021 年に出版された書籍「Self-Sovereign Identity」 [4]を参照し、下図の４つのレイヤーを一例として取り上げます。

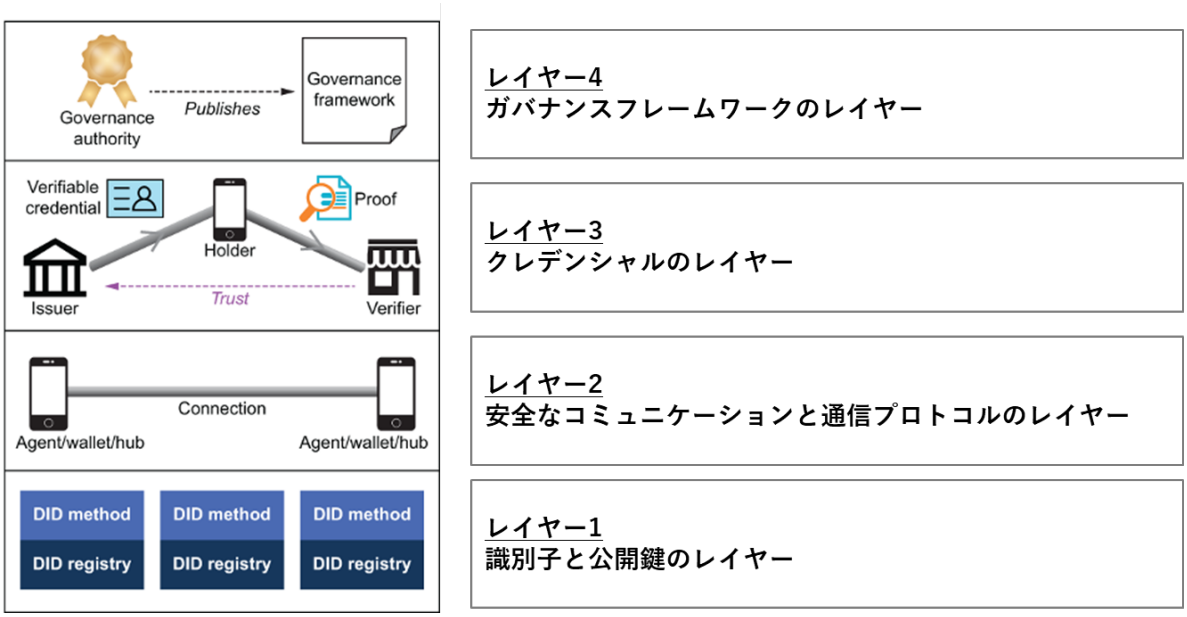


図 10 自己主権型/分散型アイデンティティを構成する要素

４つのレイヤーが正しく作用することで、個人や組織が自己主権型/分散型アイデンティティを正しく利用できるようになります。これにより、下図のように信頼を確保した情報流通を行うことができます。

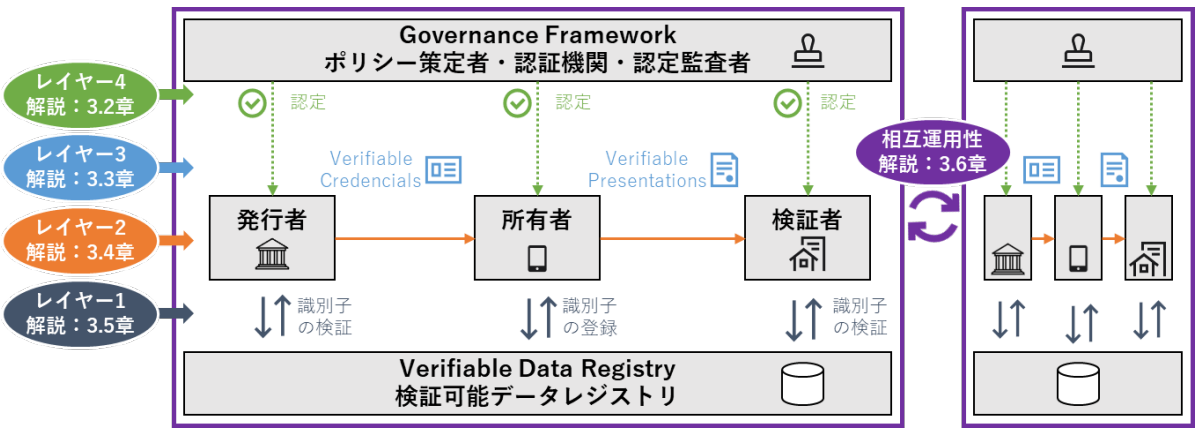


図 11 信頼を確保した情報流通

- **レイヤー4 ガバナンスフレームワーク**
  検証者が「検証可能なクレデンシャル」に関連する信頼について答えることを可能とするためのレイヤーです。行政機関や業界団体等の管理運営団体が、情報流通時の信頼を保証するために、「その信用状況を誰が審査し、どのような根拠をもってそれを担保するか」についてのポリシーや契約を定めます。

- **レイヤー3 クレデンシャル**「検証可能なクレデンシャル」の相互運用性をサポートするためのレイヤーです。発行者、所有者、検証者と呼ばれる登場人物（前述）の間で、身分証明書や航空券、ホテルの予約情報といった「検証可能なクレデンシャル」の発行・提供・検証について取り扱います。

- **レイヤー2 安全なコミュニケーションと通信プロトコル**
  参加者間での信頼されたコミュニケーションを確立するためのレイヤーです。「検証可能なクレデンシャル」を管理するデジタル ID ウォレットと、デジタル ID ウォレットを介した発行者・所有者・検証者間の通信プロトコルについて取り扱います。

- **レイヤー1 識別子と公開鍵**
  識別子と公開鍵が定義と管理されるレイヤーです。各個人や組織等を同じ DID の仕組みの中で一意にする識別子（DID）の仕様と、識別子（DID）に紐づく情報（DID ドキュメント）を、発行者や検証者からも参照できるような形で管理する方法を取り扱います。

以降の章では、それぞれのレイヤーについて、概要を示した上で、取りうる選択肢を類型化しながら説明します。また、それぞれのレイヤーの相互運用についても記述します。

3.2.レイヤー4 ガバナンスフレームワーク

レイヤー4 ガバナンスフレームワークでは、組織やプロセスを用いた人間による信頼について説明します。

3.2.1. ガバナンスフレームワークの概要

ガバナンスフレームワーク（※本書では「トラストフレームワーク」を「ガバナンスフレームワーク」として扱います）は、法規制やフレームワークに準拠して参加者がデジタルアイデンティティを適切に設計・開発・運用・利用していくために、行政機関や業界団体等によって策定されます。

ガバナンスフレームワークでは、どのような組織体でガバナンスプレーヤーと主要プレーヤーを構成するかを定めます。また、どのようなガバナンスの枠組みを整備するかを定めます。組織構成とガバナンス整備の観点のもと、以下を基本的な構成要素として定めることで、持続的なガバナンスを実現します（図 12）。

ガバナンスフレームワークの基本的な構成要素

- 関連する組織体系の役割 [5]
    - ガバナンスプレーヤー
        - Policy Maker: ガバナンスフレームワークのポリシー策定者
        - Governance Framework Provider: 全体のガバナンスを管理する国家認定機関
        - Assessor: 第三者機関として、加盟者のポリシーへの準拠を審査する適合性評価機関
    - 主要プレーヤー
        - Identity Provider: アイデンティティ情報を管理し提供する機関（IdP）
        - Service Provider: アイデンティティ情報をもとにサービスを提供する機関（SP）
        - User: ID 情報の所有者として Identity Provider に ID 情報を登録し、Service Provider に ID 情報の提供を許可することでサービスを利用する一般利用者
- 組織の関係性
- 組織がカバーすべき範囲
- 業務内容を定める、保証すべき信頼性のレベルに応じた規則（ポリシー）

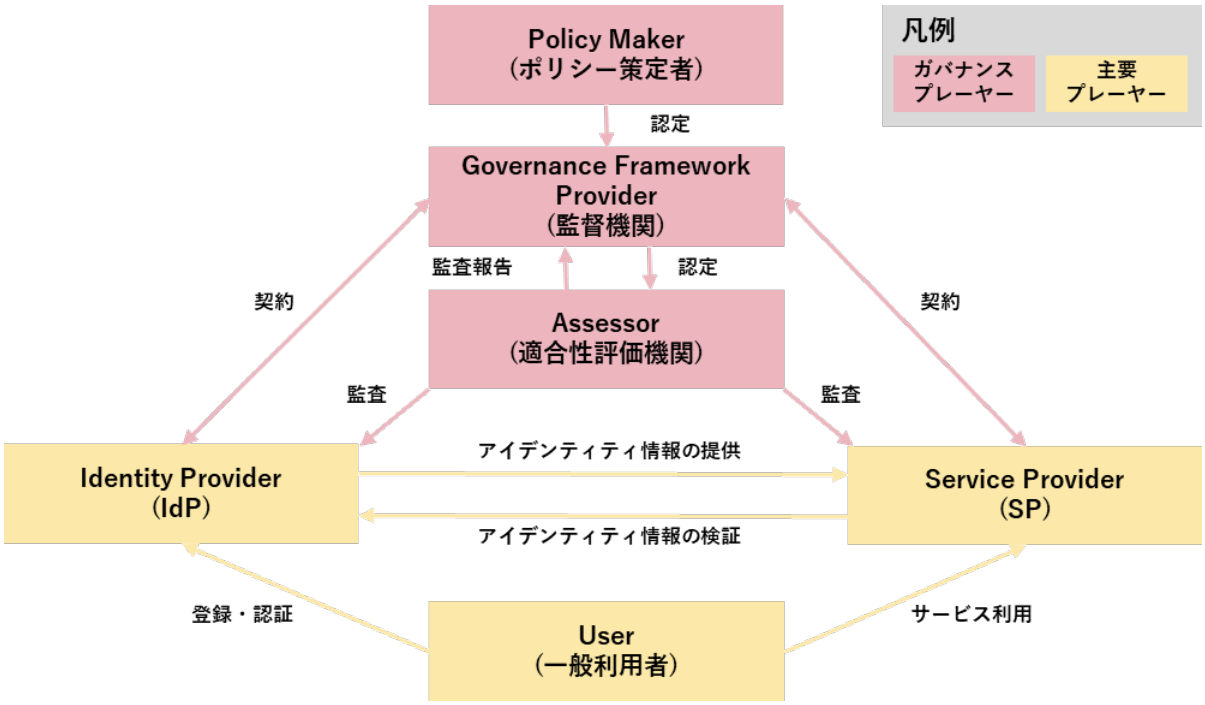


図 12 ガバナンスフレームワークの基本形 ※[5]より引用・編集

3.2.2. ガバナンスフレームワークの事例

ここでは、ガバナンスフレームワークの事例として、欧州における電子商取引のための規則 eIDAS について説明します。

eIDAS は、欧州委員会による、ヨーロッパ域内における電子商取引のための電子識別、認証、電子サイン等、トラストサービス [6] [7]に関する規則（（EU）No 910/2014）です。法制面では、欧州デジタルアイデンティティフレームワークの設立として元々の eIDAS を改正する規則（（EU）No 2024/1183）が 2024 年 5 月に施行されました。本書では、この 2024 年 5 月に施行された規則をその通称での eIDAS 2.0 と記します。技術面では、eIDAS 2.0 でのデジタル ID ウォレットを踏まえたリファレンスアーキテクチャ ARF が 2023 年 2 月に公開、2024 年 3 月には V1.3.0 へ改訂されています [8]。eIDAS 2.0 の社会実装に向けた取り組みに関しては「4.1.1 実社会・ビジネスにおける適用事例」で後述します。

図 12 に示すように、eIDAS では欧州委員会がポリシー策定者として eIDAS 規則を法制度として策定します。これを根拠として、EU 加盟国ごとのガバナンスフレームワークでは、図 12 の凡例に示すようにガバナンスプレーヤーを設置し、主要プレーヤーを管理します。

ガバナンスプレーヤーは EU 加盟国ごとに、国家認定機関（National accreditation body）、国家監督機関（National Supervisory Body）、適合性評価機関（Conformity Assessment Bodies）を設置します。国家認定機関と国家監督機関は適合性評価機関を認定・監査します。

主要プレーヤーは eIDAS 規則では「QTSP=適格トラストサービスプロバイダ」が挙げられます。適合性評価機関は各 QTSP の事業を監査します。これにより、主要プレーヤーの信頼性を高める工夫がされています。

eIDAS の特徴として、EU 各加盟国の QTSP が、トラステッド・リストに集約される点が挙げられます。トラステッド・リストとは、トラストサービスに必要な要素技術（電子署名や e シール等）ごとの、信頼のおける事業者の一覧です。トラステッド・リストは欧州委員会が Web サイトに公開しており [9]、EU 全体のトラストアンカーとして機能しています。

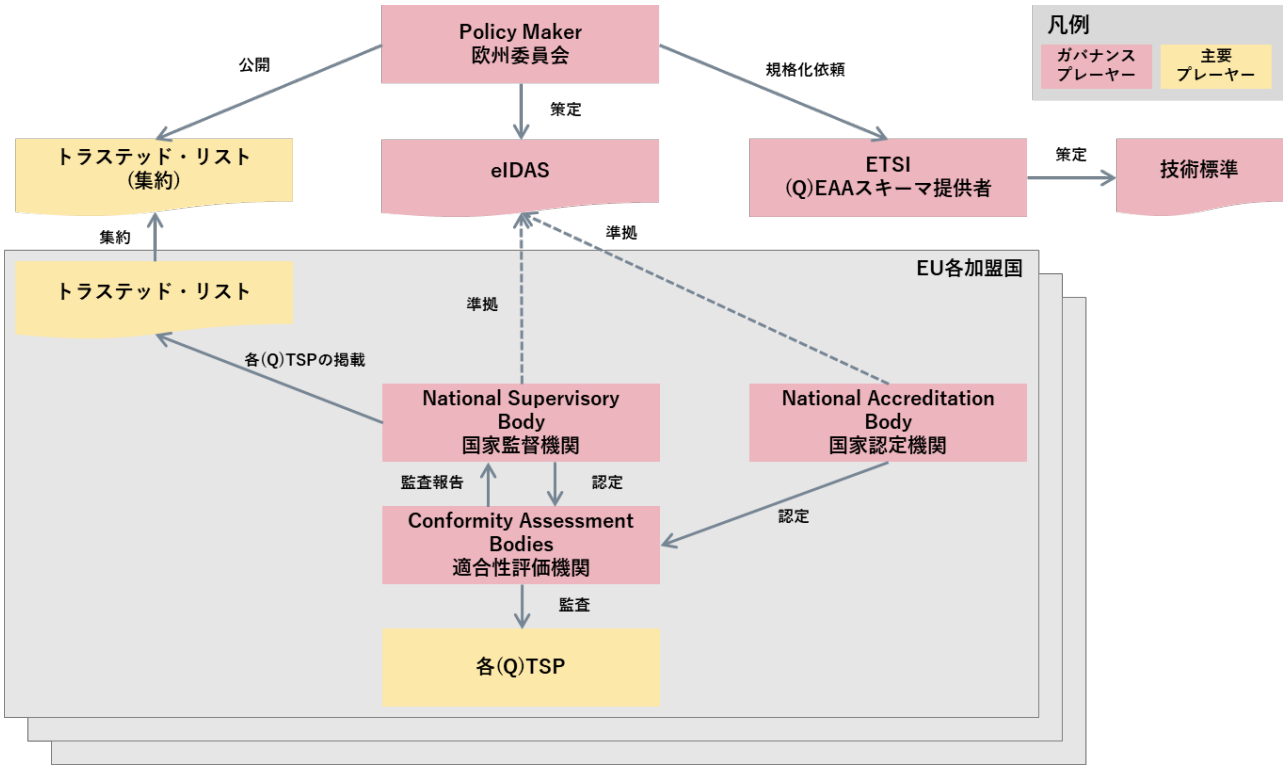


図 13 ガバナンスフレームワークの事例(eIDAS)

図 13 に示すように、トラステッド・リストを法制度のレベルで規定し、EU 加盟国間で合意している点が eIDAS の大きな特徴です。

3.2.1 項（一般論による整理）と 3.2.2 項（eIDAS の事例による整理）において、用語に相違があります。以下に参考情報として対応表を示します。

3.2.1 項（一般論による整理）	3.2.2 項（eIDAS の事例による整理）
Governance Framework	Trust Framework
Governance Framework Provider 監督機関	National Supervisory Body 国家監督機関
なし	National Accreditation Body 国家認定機関
Assessor 適合性評価機関	Conformity Assessment Bodies 適合性評価機関
Identity Provider IdP	Identity Provider IdP
Service Provider SP	Relying Party RP

3.3.レイヤー3 クレデンシャル

3.3.1. 検証可能なクレデンシャルの受け渡しとフォーマット

VC（Verifiable Credentials:検証可能なクレデンシャル）をデジタル上で受け渡すための基本的な考え方を、本項で説明します。

VC の受け渡しは、以下の図で示す、発行者、所有者、検証者と呼ばれる 3 つの登場人物の存在を前提としています（図 14）。なお、「レイヤー4 ガバナンスフレームワーク」で登場した、Identity Provider（IdP）は発行者に、Service Provider（SP）は検証者に、それぞれ対応します。

- **発行者は、所有者に、VC を発行する**
  (例) 行政機関は、所有者に、運転免許証を発行する
- **所有者は、検証者に、VC を、「検証可能なプレゼンテーション※」として提供する**
  (例) 所有者は、運転免許証を、レンタカー会社に提供する
  ※所有者に VC が紐づいていることを検証者が検証できるようなフォーマットで、一つないし複数の VC を組み合わせたもの
- **検証者は、所有者から提供された VC が、発行者から所有者へ正しく発行されたものかどうか検証する**
  (例) レンタカー会社は、運転免許証が、行政機関から所有者へ正しく発行されたものかどうか検証する

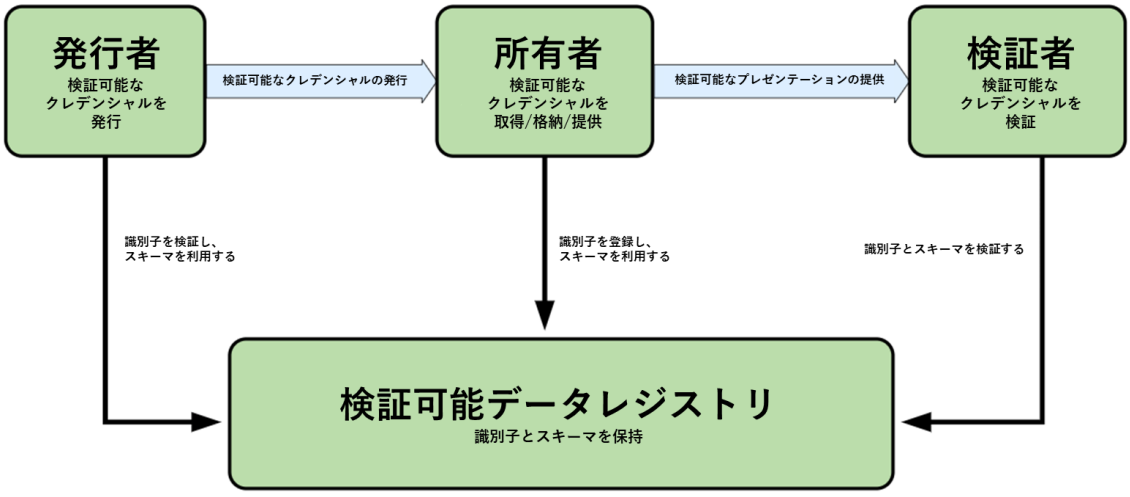


図 14 VC に関連する発行者、所有者、検証者の関係 ※ [10]より引用・翻訳

なお、所有者が VC をスマートフォン上に管理するためのデジタル ID ウォレットについては、「レイヤー2 安全なコミュニケーションと通信プロトコル」の項にて、VC 発行の根拠となる識別子やスキーマと呼ばれるデータを保持し、VC の発行や検証時に参照する、検証可能データレジストリについては、「レイヤー1 識別子と公開鍵」の項にて、それぞれ取り扱います。

VC の技術仕様は、Web 標準を開発する国際コミュニティ W3C がデータモデルを [10]、IETF が選択的開示（例えば、飛行機のチケットの VC に含まれている情報のうち、便名のみを検証者が分かるように提供する）に関するデータフォーマットを [11]、それぞれ策定しています。この他にも各要素技術の標準化団体が、VC に関心を示している状況と言えます [12]。

産業界においては、ワクチン接種証明やモバイル運転免許証等で活用が始まっています [13]。特に、モバイル運転免許証については、ISO/IEC 規格で定められたデータフォーマット mdoc に基づいた、mDL と呼ばれるモバイル運転免許証データが米国では既に一部の州で利用されているほか、その他の地域間でも共通的に利用されようとしています [14] [15] [16]。

3.3.2. 発行者と検証者の制限に関する類型

VC を取り扱うサービスやプラットフォーム（デジタル ID ウォレット等）を運営するにあたっては、発行者と検証者の参加をどの程度制限または許容するのか考慮する必要があります。

発行者の参加を制限する理由の一つは、VC は「発行者から所有者へ正しく発行されたものかどうか」をテクノロジー面から証明するのみであり、「発行者が信頼できるかどうか」は、VC 自体から知ることができないからです。

検証者の参加を制限する理由の一つは、所有者が検証者に提供する VC の情報が不適切に利用されないようにするためです。

ここでは、以下に示す発行者と検証者の参加方法の類型をもとに議論を進めます(図 15)。図 15 は、縦軸に参加者の種類(発行者・検証者)を、横軸に参加の制限の大きさ(特定対象者のみ・申請許可制・自由参加)をそれぞれ示しています。右側ほど参加の制限が小さく、誰もが参加可能な、パブリックに近い類型になります。

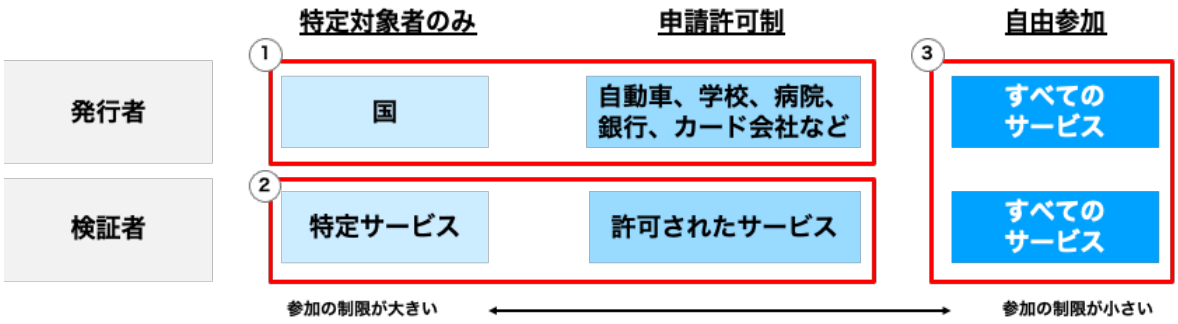


図 15 発行者と検証者の参加方法の類型

① **発行者が制限されている場合（特定対象者または申請許可制）**

検証者は、発行者の参加が制限されていない自由参加の場合よりも、所有者から提供される VC の中身の情報が高い信頼性を有している前提で、サービス提供することができます。

所有者は発行者の参加が制限されていない自由参加の場合よりも、高い信頼性を有した情報が含まれる VC をデジタル ID ウォレットに保管し、検証者に提供することができます。

例えば、発行者が運転免許証を取り扱う行政機関や、航空券を取り扱う航空会社に限られる場合、検証者は所有者から VC として提供される運転免許証や航空券が真正な内容であるとみなすことができます。
※先述の通り、VC は「発行者から所有者へ正しく発行されたものかどうか」をテクノロジー面から証明するのみであり、発行者（と所有者）が悪意を持って VC の中身を虚偽の内容で作成することは VC の技術だけでは防ぐことができません。したがって発行者を制限することは、虚偽の内容の VC が最終的に検証者に提供される可能性を減らす効果があり得ます。

② **検証者が制限されている場合（特定対象者または申請許可制）**
発行者は、所有者に発行した VC のデータが、情報管理が不十分な検証者に提供されてしまうことなどで所有者が被害に遭う懸念が減ります。
所有者は VC を検証者に提供する際、検証者の参加が制限されていない場合よりも、心理的ハードルを感じにくくなります。
例えば検証者が、旅行先の地域で MaaS サービスを提供する事業者等、デジタル ID ウォレットサービスの提供者から認証を受けていたり、とあるガバナンスフレームワークに適合したりする場合、所有者は、運転免許証や旅程に関するデータを、VC として、安心して MaaS 事業者に提供することができます。
※検証者の参加が制限されていれば、情報管理が不十分な検証者に所有者が VC を渡してしまうこと等による、情報漏えいや情報の不適切な利用などの被害に所有者が遭遇する可能性が下がることが期待されます。

③ **すべての発行者と検証者の参加が許容されている場合（自由参加）**
発行者、所有者、検証者間の自由な情報流通が可能な一方で、参加者に対するガバナンスは効きにくくなります。内容の真正性などが不確かな情報が含まれる VC が発行者から発行され、情報管理が不十分な検証者に VC のデータが提供されてしまうようになる恐れもあります。

3.4.レイヤー2 安全なコミュニケーションと通信プロトコル

3.4.1. デジタル ID ウォレットの機能

レイヤー2 では、VC の授受を行うウォレット（デジタル ID ウォレット）が言及されています [4]。デジタル ID ウォレットは、以下の図の赤枠に示す機能を主要なものとして有します (図 16)。

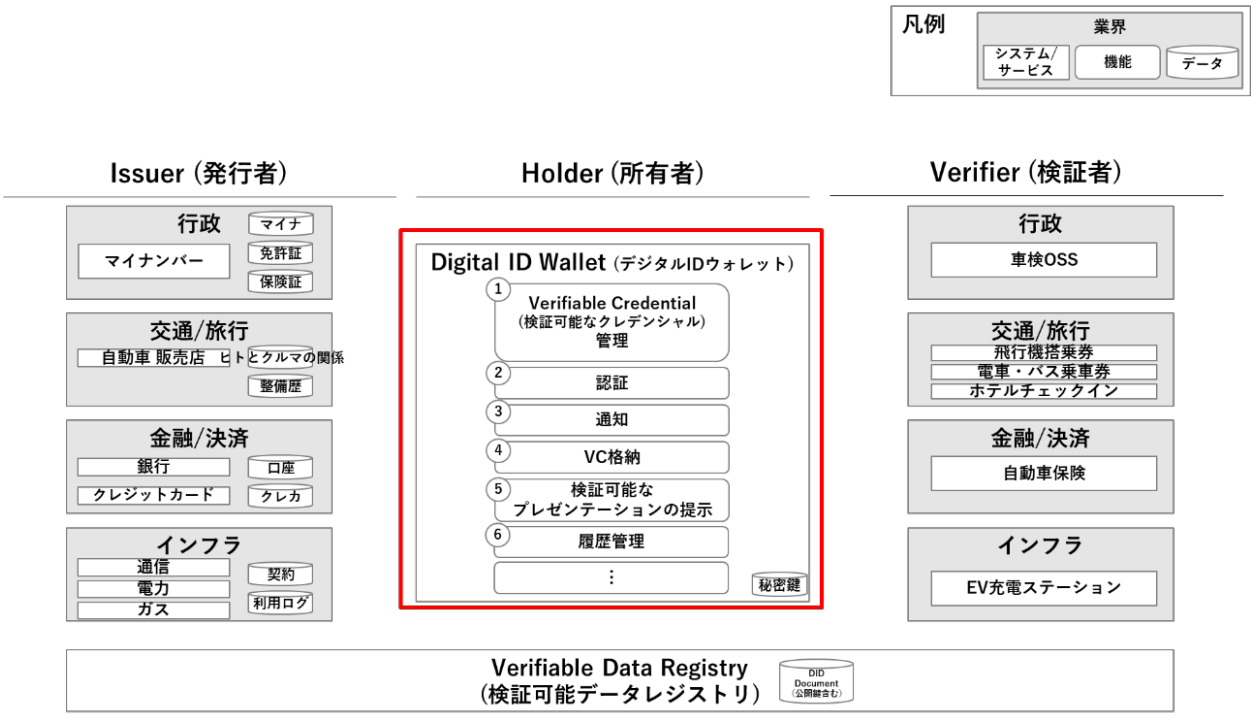


図 16 デジタル ID ウォレットの位置付けと主要な機能

1. **VC 管理**
   デジタル ID ウォレットに対して発行された VC を利用者が閲覧できるようにするほか、不要になったり有効期限が切れたりしたものを削除する機能
2. **認証**
   利用者がデジタル ID ウォレットを利用する際、パスコードや生体認証等によって認証する機能
3. **通知**
   発行者や、検証者が、所有者にプッシュ通知等を行う機能
4. **VC 格納**
   発行者がデジタル ID ウォレットに対して発行する VC を格納する機能
5. **検証可能なプレゼンテーションの提供**
   検証者が所有者から提供された VC が発行者から所有者へ正しく発行されたものかどうか検証できるように、検証可能なプレゼンテーションとしてデジタル ID ウォレットがデジタル署名を行い、デジタル ID ウォレットから検証者に対して提供する機能
   ※デジタル署名の根拠となる DID については、こちらの機能の中で管理されます。その仕組みについては、「レイヤー1 識別子と公開鍵」の項にて取り扱います。

6. **履歴管理**
   VC の格納や、検証可能なプレゼンテーションとしての提供といった処理の履歴を保持し、利用者が閲覧できるようにする機能

デジタル ID ウォレットとして実装が推奨される機能として、欧州においては、eIDAS 2.0 に基づいたリファレンスアーキテクチャである ARF（Architecture and Reference Framework）が 2023 年に公表されています。eIDAS 2.0 の ARF（Ver1.3）では、デジタル ID ウォレットのアーキテクチャについて、基本要素として暗号鍵管理、発行・交換・通信のプロトコル、データモデル、デジタル署名フォーマット等について記載されています [8]。各デジタル ID ウォレットプロバイダーはこれに準拠したデジタル ID ウォレットアプリケーションを公開することが見込まれます。また、ARF においても更新が継続しており、2024 年 5 月には Ver1.4 が公開されました。本書の執筆チームも、ARF を継続的に確認している他、実際のデジタル ID ウォレットサービスとして、ドイツの Lissi Wallet 等を調査しています [17]。

3.4.2. 通信プロトコルの類型

所有者は、デジタル ID ウォレットを発行者または検証者と通信させることで、VC の受け渡しを行います。ここでは、その際の通信プロトコルについて、以下に示す 2 つの類型を、代表例として取り扱います(図 17)。

これらの通信プロトコルによって、デジタル ID ウォレットの UI/UX には、大きな違いが生じます。実装においては、それぞれの特色を理解した上で、デジタル ID ウォレットの提供機能にあわせ、単一の通信プロトコルだけでなく、複数の通信プロトコルを組み合わせる等の考慮を行う必要があります。

図 17 通信プロトコルの 2 類型

1. **遠隔型**
   クライアント（所有者のデジタル ID ウォレット）とサーバー（事業者等が用意）間のデータやり取りに使用します。
   OpenID Foundation は、既存の Web サービスやモバイルアプリを大きく変更することなく、VC の受け渡しを行うことを目的としたプロトコル「OpenID for Verifiable Credentials」の仕様群の策定を進めています [18]。この仕様群には、「レイヤー3 クレデンシャル」の項にて挙げた、「VC の発行」に対応する「OID4VCI （OpenID for Verifiable Credential Issuance）」と「検証可能なプレゼンテーションの提供」

に対応する「OID4VP（OpenID for Verifiable Presentations）」が含まれます。
デジタル ID ウォレットから、他のモバイルアプリやブラウザで開いている Web サービスのページに VC のデータを提供する場合で遠隔型の利用が想定されます。まず、デジタル ID ウォレットから、モバイルアプリや Web サービスの裏側のサーバーに対して VC が提供されます。裏側のサーバーが VC を受け取ると、VC のデータを基にモバイルデバイス上のモバイルアプリや Web サービスのページの内容が更新されるような流れです。
また、遠隔型の通信プロトコルだけでなく、後述する近接型の通信プロトコルにも対応したデジタル ID ウォレットを使用するサービスも登場しています [19]。

2. **近接型**
   クライアント同士間のやり取りに使用します。インターフェースには、NFC、Bluetooth、QR コード等を使用します。
   QR コードについては、スマートフォンのカメラで QR コードを読み取り、クライアント同士の通信経路を確立し、VC を DID Comm 等の仕様を用いてやり取りする実装が見られます [17] [20]。

3.5. レイヤー1 識別子と公開鍵

3.5.1. 識別子（DID）の仕様

DID は、同じ DID の仕組みの中で、個人や組織を一意に識別するものです。DID は、自らが信頼したシステムを用いて生成することも可能としてデザインされています [21]。このような DID を用いて、自己主権型/分散型アイデンティティの考え方に適している識別子を設計できる可能性もあります。

本項の以下の記述では、W3C が定める仕様の詳細には触れず、DID の概念的な理解を助けるための要素を紹介します。

DID の生成には、いくつかの方法がありますが、ここでは以下の図 18 のように、発行者・所有者・検証者のデバイスが生成する公開鍵をもとに生成される場合を説明します。ここで、公開鍵は秘密鍵とともにデバイスが生成するもので、両者をあわせてキーペアと呼びます。キーペアのうち公開鍵は、その名の通り他者に公開や共有することを前提とする一方で、秘密鍵は、主にキーペアを発行したデバイス内のみで管理して秘密にしておくことを前提とします。両者は、暗号学的アルゴリズムにより紐付いています。

DID とその生成に用いた公開鍵は、DID ドキュメントと呼ばれるデータとして検証可能データレジストリ、すなわち、発行者・所有者・検証者が参照できるデータ置き場に格納されることもあります。

これらの関係を日常生活で例えると、印鑑に似ていると言えます。

- 秘密鍵は印鑑にあたり、印鑑を所持している人だけが書類に捺印できます。
- 公開鍵は印影にあたり、書類への捺印が印鑑（秘密鍵）を所持する本人によって行われたかどうか確認できます。
- DID ドキュメントは印影（公開鍵）と印鑑を所持している人を識別する情報（DID）を紐付けます。

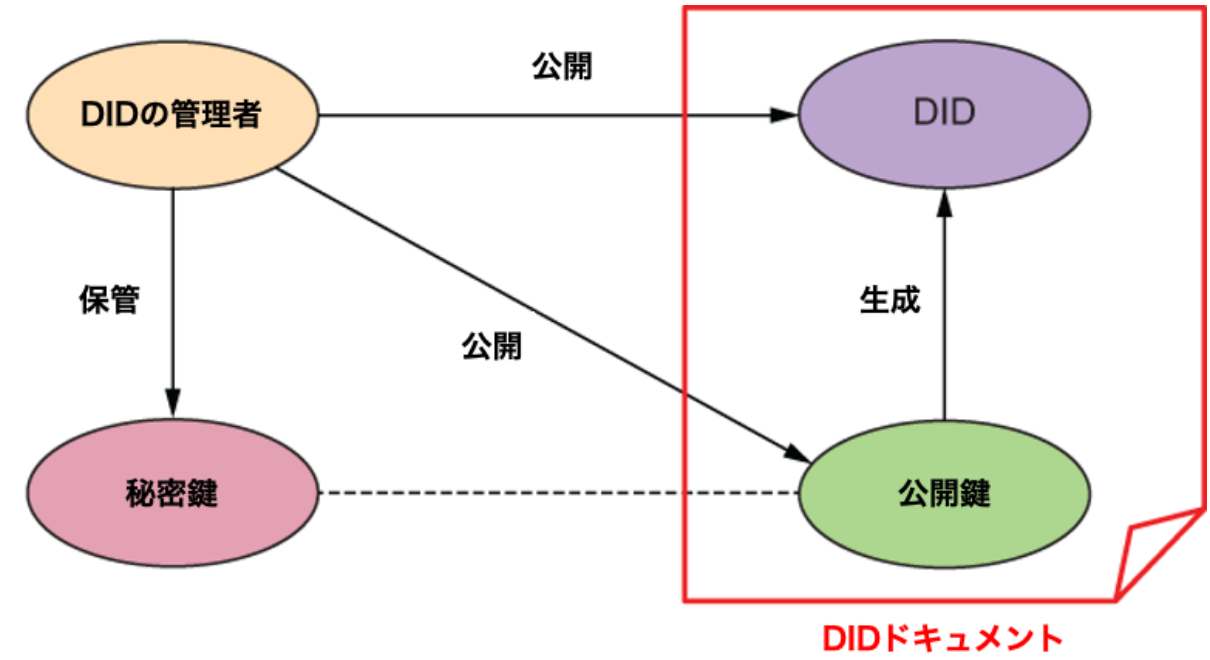


図 18 DID と公開鍵、DID Document の関係 ※[4]より引用・翻訳

検証可能データレジストリには、DID ドキュメントのほか、VC の定義情報(スキーマと呼ばれ、例えば、どの国の入国時でも共通で読み取れる「パスポート」のフォーマット等を指します)や、その失効に関わるデータ等が格納される場合もあります[10]。

検証者は、所有者のデジタル ID ウォレットから提供された VC を検証するタイミングで、検証可能データレジストリにアクセスし、VC に対する信頼が公開鍵・秘密鍵のキーペアによって担保されていることを確認する場合もあります。例えば、「この乗車券は、とある鉄道会社から、所有者に正しく発行されたものである」といったものです(図 19)。

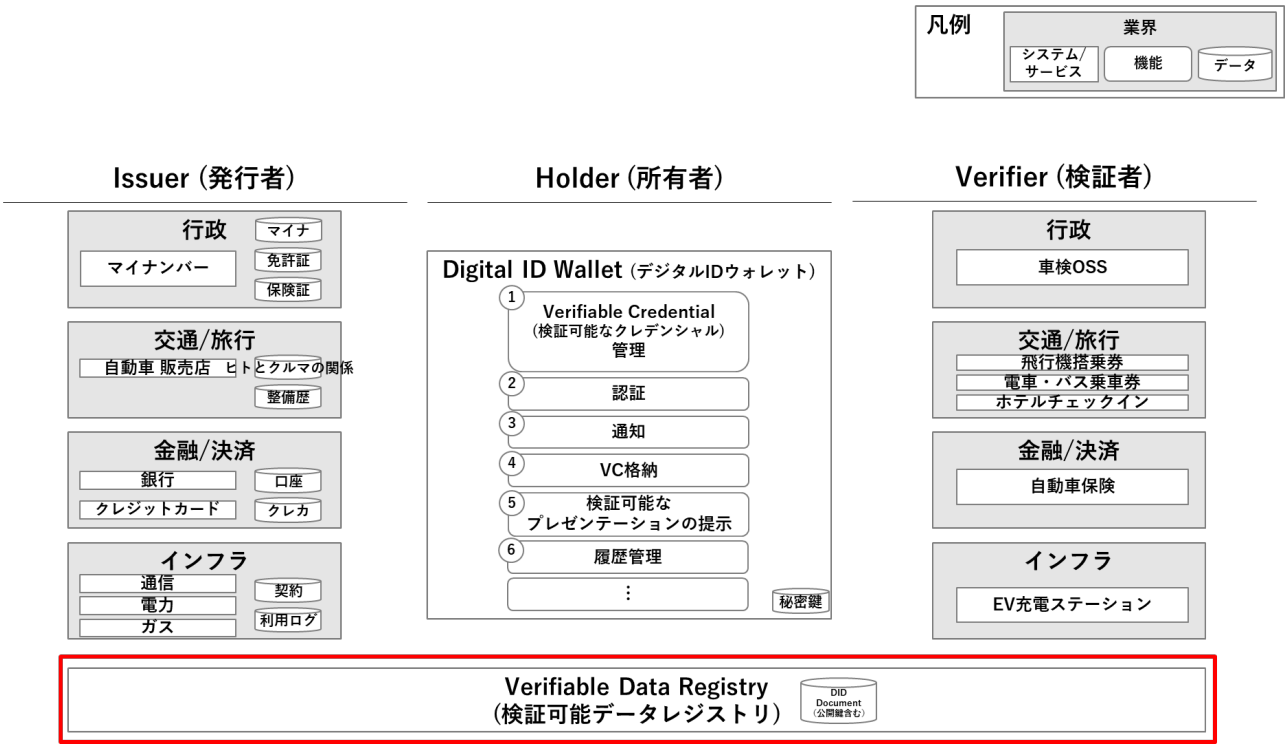


図 19 検証可能データレジストリの位置付け

公開鍵と DID ドキュメントの管理方法は、自己主権型/分散型アイデンティティのアーキテクチャにおけるテクノロジー面で根幹をなします。ここでは、公開鍵および DID ドキュメントの管理方法（※本書執筆時点でおよそ 200 が W3C に登録されています [22]）について、物理的な観点で主な類型を図 20 に示します。なお、公開鍵および DID ドキュメントの管理方法については物理的な観点以外にも権限といった他の観点も存在します。

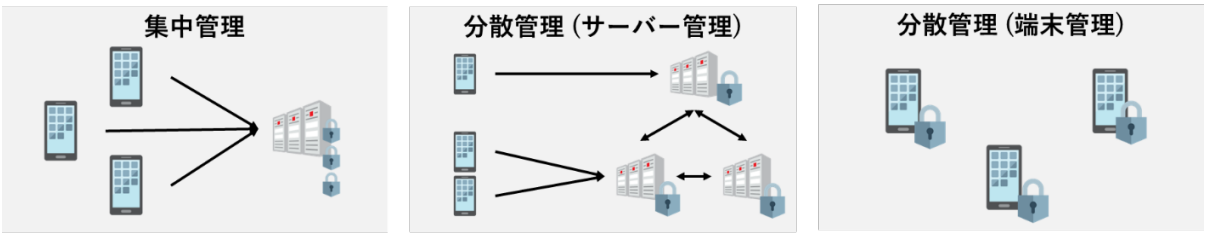


図 20 識別子(DID)管理の主な類型

1. **集中管理**
   公開鍵および DID ドキュメントを、一か所に集中して管理する方法です。
2. **分散管理 – サーバー管理**
   公開鍵および DID ドキュメントを、サーバーサイドで複数のデータベース等を用いて分散管理する方法です。
3. **分散管理 – 端末管理**
   公開鍵および DID ドキュメントを、スマートフォン等のモバイルデバイスで管理する方法です。

3.6.自己主権型/分散型アイデンティティの相互運用

ここまで述べてきたように、自己主権型/分散型アイデンティティには、４つのレイヤーが存在します。それぞれのレイヤーにおいて、フレームワークや技術標準が存在しています。

自己主権型/分散型アイデンティティの考え方や技術のもとでは、生活者はさまざまな事業者や業界、さらには国をまたいだサービスを、自らの意思で利用することが想定されます。例えば旅行シーンでは、飛行機・電車・レンタカーといったモビリティサービスを、スマートフォン上のデジタル ID ウォレットを用いて使用することになるでしょう。その際、各企業のサービスは、生活者が持つデジタル ID ウォレットを介して、情報の交換がスムーズに行われる、シームレスな体験として提供されることが望ましいでしょう。

企業が事業者や業界、国をまたいだサービスを提供していくためには、それぞれのレイヤーで採用する技術やガバナンスの仕組みを、まずは参加プレーヤー全員と合意する必要があります。つまり相互運用とは、参加プレーヤーが利用するシステムや機器を用いて情報を交換する際に、交換された情報を想定したとおりに使用できる共通な枠組みであると言えます。また、その後のプレーヤーの増加を見越して、可能な限り標準的な方法、すなわち相互運用が担保される方法を採用することが欠かせません。

このような相互運用は、「レイヤー4 ガバナンスフレームワーク」において参加プレーヤー間によるガバナンス面での合意を経て、「レイヤー3 クレデンシャル」「レイヤー2 安全なコミュニケーションと通信プロトコル」「レイヤー1 識別子と公開鍵」にあたるテクノロジー面に関する取り決めを行っていく方法が取られるでしょう。ただし、特にテクノロジー面についてはどの程度強制力を伴わせるかがポイントとなり、厳格さと自由度のバランスを取り、参加プレーヤーによるイノベーションを阻害しない取り決めが必要になります。

例えば eIDAS 2.0 では、「レイヤー4 ガバナンスフレームワーク」として、各国で効力を持つ法制度を制定しました。その後に、ARF として、本書執筆時点最新の Ver1.4 では「レイヤー3 クレデンシャル」「レイヤー2 安全なコミュニケーションと通信プロトコル」について、eIDAS 2.0 の取り組みで採用する技術標準の選定等を検討しています。

4. 今後の展望

4.1. 業界動向

本書の執筆時点において、自己主権型/分散型アイデンティティは、第３章「自己主権型/分散型アイデンティティを構成する要素」にて触れたように、比較的新しい考え方やテクノロジーであると言えます。したがって、実社会やビジネスへの適用は今まさに検討が進んでいる最中で、世界各地で PoC（概念実証）が行われている状況です。

ここでは自己主権型/分散型アイデンティティに関連する動向について、「実社会・ビジネスにおける適用事例」と「テクノロジーの標準化動向」の２つの視点から説明します。

4.1.1. 実社会・ビジネスにおける適用事例

実社会・ビジネスにおける適用事例/実装に向けた取り組みとして、３つを紹介します。

- SMART Health Card
  VCI 等の団体による、医療分野における VC の標準化を推進する取り組みで、すでに実社会・ビジネスに適用されています。
  ここ最近では、新型コロナウイルスのワクチン接種証明書が、この取り組みで標準化された VC の形式に沿って提供されています [13]。
  この取り組みは、主に「レイヤー3 クレデンシャル」に分類されます。

- eIDAS 2.0 Large Scale Pilot
  欧州では、第３章「自己主権型/分散型アイデンティティを構成する要素」で触れたように、eIDAS 2.0 に関連して、デジタル ID ウォレットを踏まえたリファレンスアーキテクチャ ARF の策定作業が進んでいます。また、ARF の社会実装に向けた取り組みとして、Large Scale Pilot と呼ばれる取り組みが、EU 各国でコンソーシアム型の協力体制を作りながら、展開されています [23]。具体的なユースケースとして、「行政サービスの利用」「モバイル運転免許証の提示」「法人間における Wallet を通じた商取引/情報取引」等を含む 11 個が挙げられ、これらのユースケースを、４つのコンソーシアム（POTENTIAL、NOBID、DC4EU、EWC）が担っています。
  Large Scale Pilot で得られた知見は、ARF にも反映され、社会実装と標準化の両輪が、今後も進んでいくと想定されます。

- Trusted Web
  Trusted Web は、2019 年に日本政府が提唱した、DFFT (Data Free Flow with Trust)の実現に向け、内閣官房デジタル市場競争本部が設立した Trusted Web 推進協議会による取り組みです。この取り組みでは、Trusted Web を、「特定のサービスに過度に依存せずに、データ自体とデータのやり取りを検証できる領域を拡大し、Trust を向上する仕組み」と位置づけており、本書の「1.1 背景」で示した考え方とも共通します。
  2022～2023 年度にかけて、「Trusted Web の実現に向けたユースケース実証事

業」が展開されており、「個人」「メディア」「ヘルスケア」「法人と行政庁」「サプライチェーン」「IoT」等をテーマにしたPoC（概念実証）が行われています[24]。国際的な相互運用の観点では、2023年4月のG7群馬高崎デジタル・技術大臣会合において、閣僚宣言として各国との連携が合意され、日本とその他の地域、特に欧州との検討が進んでいます。

4.1.2. テクノロジーの標準化状況

テクノロジーの標準化は、各業界団体等が、ワーキンググループという形で技術標準を策定しています。ここでは、第3章「自己主権型/分散型アイデンティティを構成する要素（アーキテクチャ）」で扱ったレイヤーごとに、テクノロジー面での主要な標準化の状況を一覧にします。

項番	レイヤー	取り組み名 (団体名)	ステータス
1	レイヤー4 ガバナンスフレームワーク	eIDAS 2.0 (欧州委員会)	Ver 2.0 として、Electronic Identification, Authentication and Trust Services の略で、電子識別、認証、電子サイン、およびトラストサービス等の管理/監査/基準に関する立法を提案
2	レイヤー3 クレデンシャル	Verifiable Credentials Data Model (W3C)	VC の仕様(v1.1)を、広く使用が可能な"Recommendation"として策定[10]
3		Selective Disclosure for JWTs (IETF)	"Active Internet-Draft"として、標準化文書(RFC)に向けて検討が進行中 [11]
4		mdoc/mDL (ISO/IEC JTC 1/SC 17)	ISO/IEC 規格として発行済(2021, 2023) [15] [16]
5	レイヤー2 安全なコミュニケーションと通信プロトコル	eIDAS2.0 Architecture and Reference Framework (欧州委員会等)	デジタル ID ウォレットのリファレンスアーキテクチャを策定[8]
6		OpenID for Verifiable Credentials (OpenID Foundation)	OpenID Connect の拡張仕様群として、VC の発行・提供に関する仕様群を、" Working Group Draft"として策定 [18]
8		Hyperledger Aries (Hyperledger Foundation)	近接型のデジタル ID ウォレットの機能/通信仕様を策定[25]
9		DID Comm (DIF)	DID を用いた近接型の通信プロトコルの標準仕様を策定[20]
10	レイヤー1 識別子と公開鍵	Decentralized Identifiers (W3C)	DID の仕様(v1.0)を、広く使用が可能な" Recommendation"として策定(2022) [21]
11		Hyperledger Indy (Hyperledger Foundation)	分散台帳を用いた識別子と公開鍵の管理仕様を策定[26]
12		Self-Issued OpenID Provider v2 (OpenID Foundation)	OpenID Connect の拡張仕様として、ユーザー自身が識別子等を発行するための仕様を、"Draft"として策定 [27]

表 1 テクノロジーの標準化状況

以上のようなテクノロジーの標準化に関する活動は、それぞれが独立性を持つ一方、他の活動に対して相互に影響を与えることが少なくありません。そのため、自己主権型/分散型アイデンティティが注目されるにつれ、こうした活動間の関連性を、整理する取り組みも行われるようになっています [28]。

4.2. 課題

ここでは、自己主権型/分散型アイデンティティを取り巻く、今後検討すべきいくつかの課題を例に、レイヤー毎に分類して記述します。

- **レイヤー４ ガバナンスフレームワーク**
  以下を担うような、管理運営団体等の運営主体の設立を検討する必要があります。
  - 協会等の管理運営団体の設立と業務内容の取り決め
  - 適合性評価機関の認定と業務内容の取り決め
  - 上記の業務を支えるポリシーの策定
  - コストの回収方法

- **レイヤー３クレデンシャル**
  業界にあわせたユースケースを想定し、以下を検討する必要があります。
  - ユースケース毎に共通で用いられる、スキーマと呼ばれる VC の仕様策定
  - ユースケース毎に異なる、発行者と検証者に対する参加の制限の有無と、制限自体の内容の取り決め
  - 既存の認証連携の仕様（OpenID Connect 等）との相互接続性の確保

- **レイヤー２ 安全なコミュニケーションと通信プロトコル**
  業界やユースケースにあわせた標準的な UI/UX が定まっていないため、以下を検討する必要があります。
  - UI/UX に大きな影響のある通信プロトコルの選択に関して、業界やユースケース毎にベストプラクティスを確立
  - 特に進化の早い UI の要素技術（本書執筆時点で主流である QR コードのほか、NFC、Bluetooth 等の活用が見込まれる要素技術）への順応
  - 個人だけでなく、法人やその従業員による利用を考慮した、デジタル ID ウォレットの提供形態

- **レイヤー１ 識別子と公開鍵**
  多数の DID ドキュメントの管理方法があるため、以下を検討する必要があります。
  - 相互運用に適した DID ドキュメントの管理方法

4.3.　今後の展望

本書の冒頭で述べた問題について、まさに近年、「個人情報が必要以上に収集され、意図しない用途に利用されるのではないか？」という懸念から、ヨーロッパの GDPR（一般データ保護規制）の導入や、日本での個人情報保護法改正等、世界的に個人情報保護管理に対する規制が強まっています。

個人が自身に関する情報の流通をコントロールできることを目指す自己主権型アイデンティティの思想と、その実現手段の一例として検討が進む分散型アイデンティティの技術は、今後益々注目を集めるでしょう。

また、日本政府が環境整備の方針を示している[29]分散型デジタル社会の世界において、各種産業における DX で主導的役割を担うために、自己主権型/分散型アイデンティティへの取り組みは、実現手段の一つとして、今後も継続的に議論がなされていくことが予想されます。

このような情勢下において、本書に示した自己主権型/分散型アイデンティティとそれに付随する４つのレイヤーにおける課題について早期に取り組むことが、分散型デジタル社会の実現、ならびに世界における日本の産業力の優位性向上に寄与することも期待されます。

自己主権型/分散型アイデンティティ 技術調査ホワイトペーパー

2024 年 8 月

企画・発行：トヨタ・コニック・アルファ株式会社

協力：　総合監修　株式会社ジェーシービー
第１章・第２章監修　日本オラクル株式会社
第３章監修　NRI セキュアテクノロジーズ株式会社

※ 本書 P.9～P.15 で使用した画面遷移の画像は、ドイツの Lissi GmbH 社から提供を受けた Lissi ID-Wallet を日本語化したプロトタイプアプリの画面を元に改変したものです

用語集

項番	用語	用語(和名)	定義
1	Assessor	適合性評価機関	Trust Framework Provider の認可のもと、第三者機関として、認証機関が定めるポリシーへの準拠を審査する機関。
2	Decentralized Identifier (DID)	分散型識別子	分散型アイデンティティ(DID: Decentralized Identity)とは異なる。同じ DID の仕組みの中で一意な識別子。 個人や組織が、自らが信頼できるシステムを使って自分の識別子を生成できるように設計されていることもある。デジタル署名等の暗号証明を用いて認証することにより、個人や組織がその識別子に紐づいていることを証明することが可能。 [24]より抜粋 ※一部改変
3	Wallet	デジタル ID ウォレット※ ※原文では”Wallet”だが、本文書ではアイデンティティを扱うため明示的に和名に「デジタル ID」を挿入	Verifiable Credential(検証可能なクレデンシャル)やキーマテリアルを受領、保管、提供、管理できるように Holder（所有者）が用いるエンティティ。 [30]より翻訳 ※一部抜粋
4	Holder	所有者	Verifiable Credential（検証可能なクレデンシャル）を保管し、Verifiable Credential（検証可能なクレデンシャル）から Verifiable Presentation（検証可能なプレゼンテーション）を作成することのできる個人や役割。[10]より翻訳
5	Identity Provider (IdP)	ID プロバイダ	アイデンティティ情報を管理し提供する機関。
6	Issuer	発行者	Verifiable Credential(検証可能なクレデンシャル)を作成し、Holder（所有者）に発行することのできる役割。 [10]より翻訳 ※一部改変
7	Policy Maker	ポリシー策定者	トラストフレームワークのポリシー策定者。 [31, 5]より抜粋
8	Self-Sovereign Identity (SSI)	自己主権型アイデンティティ	管理主体が介在することなく、個人が自分自身のアイデンティティをコントロールできるようにすることを目指す考え方。 管理者を介さずに自分自身でアイデンティティ情報を管理できることを重視している点が特徴。 [24]より抜粋
9	Service Provider (SP)	サービスプロバイダ	アイデンティティ情報をもとに、サービスを提供する機関。
10	Trust Framework Provider	認証機関	ID フェデレーションなどのガバナンスと管理を担当する機関。
11	Trust Service	トラストサービス	「トラストサービス」とは、通常有償で提供される電子サービスで、以下の内容から構成されるものをいう。 (a)電子署名、e シール、電子タイムスタンプ、電子書留サービス及びこれらのサービスに関連する証明書の作成、検証及び妥当性確認。 (b)ウェブサイト認証のための証明書の作成、検証及び妥当性確認。 (c)これらのサービスに関連する電子署名、e シールまたは電子証明書の保存。 [6] [7]より引用
12	User	一般利用者	サービス利用者。

13	Verifiable Credential (VC)	検証可能なクレデンシャル	物理的な「クレデンシャル」※が表すのと同じ情報をすべて表すことができ、加えてデジタル署名等の技術を用いることで、現実の物理的な「クレデンシャル」より改ざん防止性や信頼性を高くしたもの。 ※現実世界における、「クレデンシャル」の例 ・「クレデンシャル」の対象の識別に関する情報（例: 写真、名前、識別番号） ・発行機関に関連する情報（例: 市役所、国家機関、認証機関） ・「クレデンシャル」の種類に関する情報（例: オランダのパスポート、アメリカの運転免許証、健康保険証） ・発行機関が対象について主張している特定の属性情報（例: 国籍、運転可能な車両の種類、生年月日） ・「クレデンシャル」が何から派生したかに関する証跡 ・「クレデンシャル」の制約に関する情報（例: 有効期限、利用規約） [10]より翻訳
14	Verifiable Data Registry	検証可能データレジストリ	識別子、鍵、その他関連データとして例えば Verifiable Credential（検証可能なクレデンシャル）のスキーマ、失効レジストリ、Issuer（発行者）の公開鍵など Verifiable Credential（検証可能なクレデンシャル）の利用に必要なデータの作成と検証を仲介する場合もあるシステムの役割。 [10]より翻訳 ※一部抜粋
15	Verifiable Presentation (VP)	検証可能なプレゼンテーション	データの作成性が暗号検証プロセス後も信頼できる方式でエンコードされた、改ざん検知可能な Presentation（プレゼンテーション）。Presentation（プレゼンテーション）自体は、特定の Verifier（検証者）に共有される、一つ以上の Issuer（発行者）から発行された一つ以上の Verifiable Credential（検証可能なクレデンシャル）から派生したデータ。 [10]より翻訳 ※一部抜粋
16	Verifier	検証者	Verifiable Presentation（検証可能なプレゼンテーション）を要求、受領、検証するエンティティ。 [30]より翻訳 ※一部抜粋

参考文献

[1] 光. 武邑 , 恵. 若林, さよなら、インターネット, ダイヤモンド社, 2018.

[2] “マイナポータル,” [オンライン]. Available: https://services.digital.go.jp/mynaportal/.

[3] Trust over IP Foundation, “The ToIP Technology Architecture Specification,” [オンライン]. Available: https://trustoverip.org/our-work/technical-architecture/.

[4] D. R. Alex Preukschat, Self-Sovereign Identity, Manning Publications, 2021.

[5] OpenID ファウンデーション・ジャパン, “トラストフレームワーク WG,” [オンライン]. Available: https://www.openid.or.jp/working-group/tfwg/.

[6] THE EUROPEAN PARLIAMENT , THE COUNCIL OF THE EUROPEAN UNION, “REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC,” [オンライン]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32014R0910.

[7] 電子認証局会議, “トラストサービスとは,” [オンライン]. Available: https://www.c-a-c.jp/about/trust.html.

[8] European Commission, “The European Digital Identity Wallet Architecture and Reference Framework,” [オンライン]. Available: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework.

[9] European Commission, “EU Trusted List Browser,” [オンライン]. Available: https://webgate.ec.europa.eu/tl-browser/.

[10] W3C, “Verifiable Credentials Data Model v1.1,” [オンライン]. Available: https://www.w3.org/TR/vc-data-model/.

[11] D. Fett, K. Yasuda , B. Campbell, “Selective Disclosure for JWTs (SD-JWT),” [オンライン]. Available: https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/.

[12] 株式会社インターネットイニシアティブ, “Internet Infrastructure Review（IIR）Vol.52,” [オンライン]. Available: https://www.iij.ad.jp/dev/report/iir/052/02.html.

[13] “SMART Health Cards Framework,” Credential Modeling, [オンライン]. Available: https://spec.smarthealth.cards/credential-modeling/.

[14] 一般社団法人日本スマートフォンセキュリティ協会, “デジタル身分証の動向とセキュリティ対策について,” [オンライン]. Available: https://www.jssec.org/column/20231127.html.

[15] ISO/IEC JTC 1/SC 17, “ISO/IEC 18013-5:2021 Personal identification, ISO-compliant driving licence, Part 5: Mobile driving licence (mDL) application,” [オンライン]. Available: https://www.iso.org/standard/69084.html.

[16] ISO/IEC JTC 1/SC 17, “ISO/IEC 23220-1:2023 Cards and security devices for personal identification Building blocks for identity management via mobile devices Part 1: Generic system architectures of mobile eID systems,” [オンライン]. Available: https://www.iso.org/standard/74910.html.

[17] Neosfer GmbH, “Lissi Wallet,” [オンライン]. Available: https://www.lissi.id/for-users.

[18] OpenID Foundation, “OpenID for Verifiable Credentials - Overview,” [オンライン]. Available: https://openid.net/sg/openid4vc/.

[19] N. GmbH, “Lissi Connect Demo,” [オンライン]. Available: https://demo.lissi.id/.

[20] Decentralized Identity Foundation, “DIDComm Messaging v2.0,” [オンライン]. Available: https://identity.foundation/didcomm-messaging/spec/v2.0/.

[21] W3C, “Decentralized Identifiers (DIDs) v1.0,” [オンライン]. Available: https://www.w3.org/TR/did-core/.

[22] W3C, “DID Specification Registries,” [オンライン]. Available: https://w3c.github.io/did-spec-registries/#did-methods.

[23] European Commission, “EU Digital Identity Wallet Pilot implementation,” [オンライン]. Available: https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation.

[24] Trusted Web 推進協議会, “Trusted Web ホワイトペーパー Ver.3.0,” 2023. [オンライン]. Available: https://trustedweb.go.jp/documents/.

[25] Hyperledger Foundation, “Hyperledger Aries,” [オンライン]. Available: https://www.hyperledger.org/use/aries.

[26] Hyperledger Foundation, “Hyperledger Indy,” [オンライン]. Available: https://www.hyperledger.org/use/hyperledger-indy.

[27] K. Yasuda, M. Jones , T. Lodderstedt, “Self-Issued OpenID Provider v2 - draft 13,” [オンライン]. Available: https://openid.net/specs/openid-connect-self-issued-v2-1_0.html.

[28] A. Hughes , T. Lodderstedt, “Digital Credentials and Issuance Protocols A joint effort by the global community of experts,” [オンライン].

[29] デジタル庁, “デジタル社会の実現に向けた重点計画,” 2022. [オンライン]. Available: https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/d130556b/20220607_policies_priority_outline_05.pdf.

[30] OpenID Foundation, “OpenID for Verifiable Presentations - draft 20,” [オンライン]. Available: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html. [アクセス日: 11 6 2024].

[31] OpenID ファウンデーション・ジャパン, “組織におけるアイデンティティ管理の基本的な考え方,” [オンライン]. Available: https://www.slideshare.net/naohiro.fujie/ss-131091269.