日本銀行ワーキングペーパーシリーズ

デジタルアイデンティティと取引・決済

小島怜*

鳩貝淳一郎**
junichirou.hatogai@boj.or.jp

No.25-J-7
2025 年 6 月

日本銀行
〒103-8660　日本郵便（株）日本橋郵便局私書箱 30 号

* 前・決済機構局
** 決済機構局

デジタルアイデンティティと取引・決済*

小島 怜[1]・鳩貝 淳一郎[2]

2025 年 6 月

■要　旨■

経済のデジタル化が進んだ現代では、インターネットを介してサービスを利用するシーンがますます増えている。事業者がユーザーに対してサービスを届けるには、属性情報などから構成されるアイデンティティをデジタルな形式で適切に用いることが必要である。

近年、こうしたデジタルアイデンティティの管理が、少数のメジャーなサービス事業者に担われるようになってきていることから、プライバシー、サービス利用の継続性、データに対するコントロールといった観点から、リスクやデメリットも指摘されている。こうした状況下で、特定の主体への依存を避ける形でアイデンティティを構成し、ユーザーが自身でコントロールする「自己主権型アイデンティティ」の考え方が、注目を集めている。

本稿では、自己主権型アイデンティティに関連した要素技術である「検証可能クレデンシャル」や「分散型識別子」などを説明し、これらを活用した社会実装の試みを紹介した上で、こうしたアイデンティティのあり方が、経済活動の中でも取引や決済の領域にとって重要であり、経済取引や決済の将来像を検討する際にも示唆がある旨を示す。

* 本稿の作成にあたっては、松尾真一郎氏（バージニア工科大学研究教授/ジョージタウン大学研究教授）から有益なコメントを頂いた。ここに記して感謝したい。ただし、ありうべき誤りは筆者らに属する。また、本稿の内容や意見は、筆者ら個人に属するものであり、日本銀行の公式見解を示すものではない。

[1] 前・決済機構局

[2] 決済機構局＜E-mail; junichirou.hatogai@boj.or.jp＞

１．はじめに

経済のデジタル化が進んだ現代では、インターネットを介してサービスを受けるシーンはますます増えている。事業者がユーザーに対してサービスを届けるには、ユーザーの属性情報などから構成されるアイデンティティを、デジタルな形式で適切に用いることが必要である。近年、既存のデジタルアイデンティティの仕組みに対して、特定の主体への依存を避ける形でアイデンティティを構成する試みが注目を集めている。こうした試みは、経済活動、とりわけ取引や決済の領域に長期的に大きな影響を与える可能性がある。

本稿では、こうした認識のもと、個人ユーザーのデジタルアイデンティティを念頭に、まず２節で既存のデジタルアイデンティティのあり方を概観する。３節では、これに対する新しいアイデンティティの考え方として「自己主権型アイデンティティ」を紹介し、要素技術と社会実装の試みを説明する。４節では、こうしたデジタルアイデンティティのあり方が、取引や決済の領域にとって重要であり、これらの将来像を検討する際にも示唆がある旨を示す。

２．既存のデジタルアイデンティティのあり方

アイデンティティという語は多義的であるが、国際標準化の推進機関であるISO/IEC のドキュメントにおける定義によれば、「ある実体に関連する属性の集合」[3]である。ここで言う「属性」とは、ユーザーの名などの身元の情報や、資格・権利の情報などのことである。具体的には、個人については、どんな名前で、住所はどこで、身長・体重はどのくらいで、どんな人相で、いつ生まれて、どんな趣味で、どんな免許や資格を持っていて、どんなサブスクリプションの契約をしていて…と様々な特徴を持っている。ここでは、こうした身元情報や資格情報などを属性と呼び、属性の集合体をアイデンティティと呼んでいる。アイデンティティは法人にとっても重要な概念だが、本稿では個人を検討の対象とする。

アイデンティティについてもう少し具体的なイメージを掴むために、村の住民にのみ商品券を渡すことを考える。住民が少なければ、人相で個人を特定できるだろう。もっとも、覚えられる人相の数は有限であるし、忘れてしまうこともある。これを解決する手段として、事前に村役場が証明書を発行しておき、現場において券面記載の住所などを確認すれば、適切に商品券を渡すことができるだろう。

人相や証明書などのいわば物理的なアイデンティティは、当事者による目視

[3] ISO/IEC 24760-1, https://www.iso.org/obp/ui/#iso:std:iso-iec:24760-1

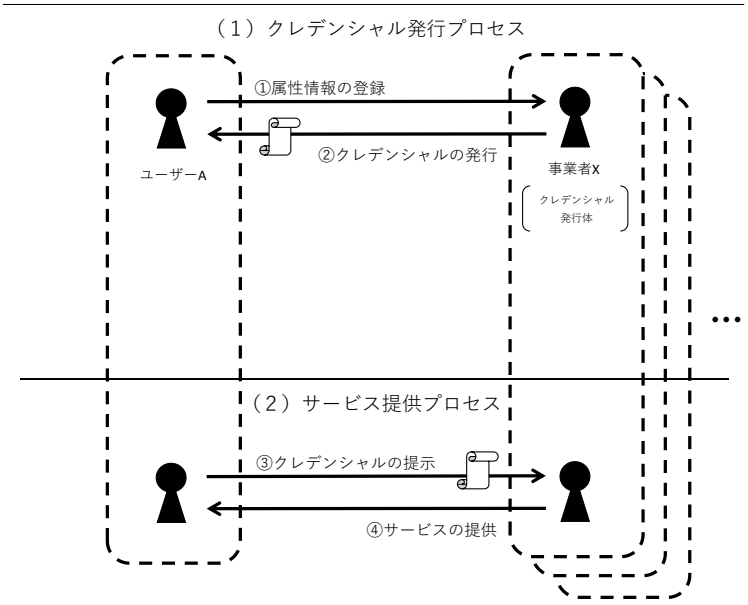
確認に依存していたり、処理件数に限界があったり、遠隔地とのやり取りに向かないという限界がある。スマートフォンなどの端末やネットワークを介してサービスが提供されることの多い今日では、物理的なアイデンティティではサービスの提供ができない可能性や、提供できたとしてもユーザー体験を大いに損ねる可能性がある。そこで、アイデンティティをコンピューターで処理できるようデジタルな形式で表現した「デジタルアイデンティティ」が活用されている。

デジタルアイデンティティの枠組みでは、資格情報などの属性を書き込んだデジタルな形式の証明書を「クレデンシャル」、クレデンシャルを発行し内容を保証する主体を「クレデンシャル発行体」と呼ぶ。現代において、インターネットを介したサービスのユーザーは、典型的には、クレデンシャル発行体に属性情報を登録して、クレデンシャルを発行してもらい、サービス事業者に提示してサービスを受ける。

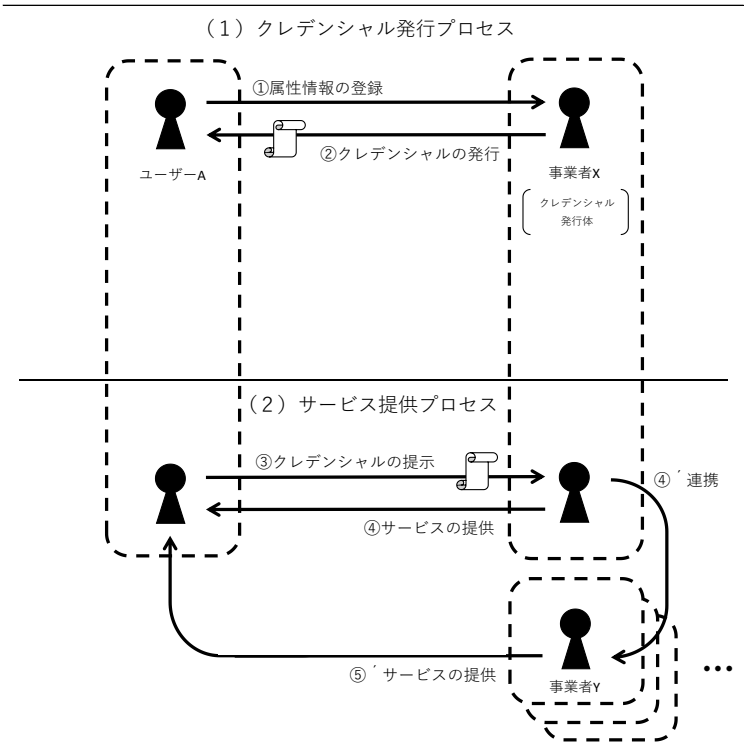
デジタルアイデンティティの管理モデルとしては、まず、事業者がクレデンシャル発行、認証・認可、サービス提供を一貫して行う「集中型モデル」がある（図表１左)。プロセスをやや詳しくみると、まず、①ユーザーが、自身の属性情報をサービス事業者に伝達して登録する。②サービス事業者はユーザーの属性情報を管理し、クレデンシャルを発行する。③ユーザーはサービスを利用する際に、事業者にクレデンシャルを提示し、④事業者は登録されている情報と照合し、これに基づいてサービスを提供する。

（図表 1）集中型モデルとフェデレーションモデルの比較

【集中型モデル】



【フェデレーションモデル】



デジタル化が進展し、インターネットを介して利用可能なサービスが増えるにつれ、複数のサービスにおいて横断的にアイデンティティを利用するニーズが高まってきた。こうしたなかで、メジャーなサービス事業者＝クレデンシャル発行体[4]が、ユーザーのアイデンティティ情報を他のサービス事業者に連携する「フェデレーションモデル」（Federated identity model）が普及してきた（図表１右)。典型的には、メジャーなSNSサービスのアカウントを用いて、他社サービスの認証が行われる事例などがある。

このモデルでは、ユーザーのアイデンティティ情報が幅広いサービスで用いられるようになり、利便性が向上する一方で、クレデンシャル発行体となるサービス事業者にアイデンティティの管理を依存する形となっている。現在主流となっているこのモデルが内包するリスクとして、たとえば、以下が指摘されている。

① サービス利用の継続性に関するリスク

特定の組織の判断や過失によりアイデンティティの提供や連携が停止されることで、サービスを利用できなくなる可能性がある。

② サービス利用にかかるプライバシーに関するリスク

ユーザーは自身が使用する多様なサービスについて、その利用状況を特定のクレデンシャル発行体である事業者に知られることになり、こうしたプライバシー情報の集中自体がリスクを含んでいると指摘される。また、過失または故意により、ユーザーの意に反して、他の事業者にもアイデンティティが連携される可能性がある。

③ アイデンティティ情報の改ざん・流出のリスク

特定の組織がアイデンティティ管理を担うことになり、この管理が十分でない場合は、外部からの攻撃などにより改ざん・流出するリスクがある。その場合、事業者ごとにアイデンティティ管理を行っている状況よりも、特定の組織によって収集されるアイデンティティ情報が多いため、影響が大きくなる可能性がある。

３．自己主権型アイデンティティのコンセプトと取り組み

本節では、既存のデジタルアイデンティティに対する新しい考え方として「自己主権型アイデンティティ」を紹介し、要素技術として「検証可能クレデンシャ

[4] この文脈では、「アイデンティティプロバイダー」と呼ばれる。

ル」と「分散型識別子」を説明する。また、これらを活用した社会実装の試みをいくつか挙げ、課題と留意点を説明する。

３－１　自己主権型アイデンティティの考え方

上記のリスクは、経済・社会のデジタル化の進展とともに大きくなる。近年、こうしたリスクを軽減しうるデジタルアイデンティティの管理モデルとして「自己主権型アイデンティティ」（Self-Sovereign Identity、SSI）が提唱されている。これは、管理主体が介在することなく、個人が自身のアイデンティティを自らコントロールすべきという思想である。自己主権型アイデンティティの考えに基づいた管理モデルは、以下のような特徴を備えることが期待される[5]。

①　自身に関する属性のデータを自ら把握し、制御する

自己主権型アイデンティティの考え方においては、提示を求められる情報を自ら構成し、サービス事業者に共有する。ここでは、本人が認識しないまま必要以上の情報をサービス事業者に収集されることがない。また、サービスを利用しているという事実を、サービス事業者以外に知られることがない。

②　他者の都合でアイデンティティの利用を制限されない

自己主権型アイデンティティでは、特定の主体に依存しない形で、自身の属性について他者に証明することができる。アイデンティティの利用について、特定の主体の都合や過失により制限されることがない。クレデンシャルの発行体の関与を必要としないことで、可用性の観点でもメリットがある。

以下では、自己主権型アイデンティティに関連が強い技術である「検証可能クレデンシャル」と「分散型識別子」をみていく[6]。続いて、それらを活用する取り組みをいくつか取り上げる。

３－２　自己主権型アイデンティティに関連の深い技術

自己主権型アイデンティティの実現を目指す文脈で、要素技術として「検証可能クレデンシャル」と「分散型識別子」が重視されている。

---

[5] どういったアイデンティティのあり方であれば「自己主権」的なのかについては、様々な考え方がある。この点につき、たとえば、Christopher（2016）は「自己主権型アイデンティティの 10 原則」として、「コントロール」、「アクセス」、「透明性」、「永続性」、「ポータビリティ」、「同意」といった原則を挙げている。

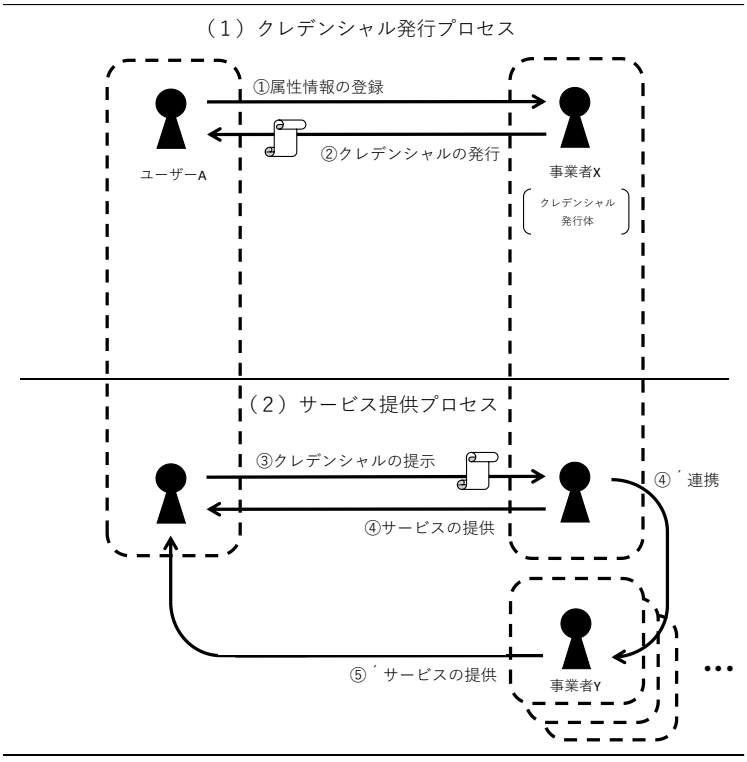
[6] どちらの技術も、標準化団体である W3C（World Wide Web Consortium）によって技術標準として勧告されている（W3C, 2022）。

（検証可能クレデンシャル）

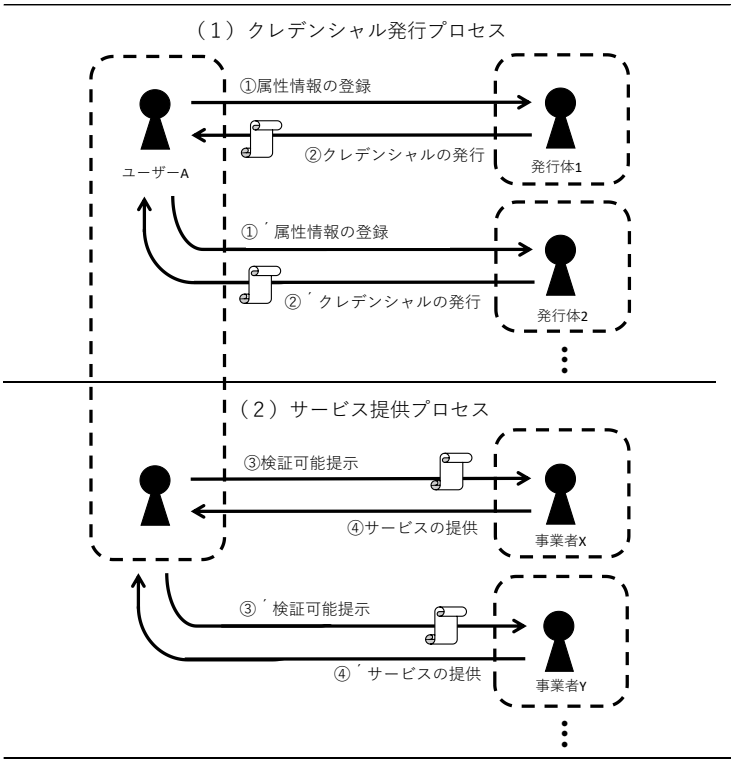
検証可能クレデンシャル（Verifiable Credential、以下「VC」）は、信頼できる主体によって個人に発行され、個人がサービス提供事業者などに「検証可能提示」という形態で提示し、記載された属性につきその事業者が機械的に確認できるものである。以下、前述のフェデレーションモデルとの比較を念頭に、検証可能提示のプロセスを説明する（図表 2 右）。

（図表 2）フェデレーションモデルと検証可能クレデンシャル（VC）の比較

【フェデレーションモデル】



【検証可能クレデンシャル（VC）】



まず、ユーザーは、クレデンシャル発行体から VC の発行を受ける（①、②）。ユーザーは、ユーザーが提示したい内容を含む VC、この VC に対しユーザーが行ったデジタル署名などをあわせて、サービス事業者に提示する（検証可能提示、③）。サービス事業者は、クレデンシャル発行体に問い合わせることなく、クレデンシャルが当該発行体により発行されたこと、内容が発行時から改ざんされていないことなどを確認し、サービスを提供する[7]（④）。

[7] 具体的には、ユーザーから VC の提示を受けたサービス事業者は、クレデンシャル発行体の公開鍵を取得してデジタル署名を検証し「クレデンシャルが確かにその発行体により発行されたこと」を確認する。続けて、ユーザーの公開鍵を用いてデジタル署名を検証し、内容が発行時から改ざんされていないこと確認する。より詳細には、佐古（2023）を参照。

この仕組みにおいては、クレデンシャル発行体の関与がない状態で、サービス事業者が認証・認可を行うことができる。また、ユーザーは、VC が含む属性情報のうち、「そのサービスを受けるために必要な範囲のみ」をサービス事業者に開示することや（選択的開示）、複数の VC を組み合わせて検証可能提示を行うことができる。また、VC とゼロ知識証明[8]の技術を組み合わせて、「サービス事業者に対し属性を開示しなくても、サービスの提供を受ける」ことも目指されている。

（分散型識別子）

一般に、サービス提供のためには、ユーザーを他のユーザーと区別して認識する必要があり、このために識別子が正しく割り振られることが重要である。既存のアイデンティティ管理の枠組みでは、単一の組織が一元的に重複がないよう識別子を発行することが一般的である。

これに対して、分散型識別子（Decentralized Identifier）は、特定の組織に依存しない形で割り振られる識別子とその管理枠組みである[9]。分散型識別子では、識別子を付与する対象（DID サブジェクト）が自ら採番し割り振るのが特徴である[10]。これにより、外部から削除されたり変更されたりされず、自己主権的な性質を備えている。また、通常の仕組みでは番号を発行した主体が個人と識別子の紐づけを証明するが、分散型識別子では、個人と識別子との紐づきの証明に非対称鍵暗号を用いることが主に想定され、信頼される特定の主体への依存を前提にしない形となっている。

なお、個人がルールに従わずに割り振ると、同じ識別子が存在してしまう可能性があるが、分散型識別子では DID メソッドと呼ばれる形式に従いレジストリ（検証可能データレジストリ）に登録することで、重複を避けている[11]。DID メソッドは多数あるが、たとえば、識別子およびその付随情報（識別子と個人との紐づきを証明・検証するための暗号的な鍵の情報など）を、変更できない形で公開するモデルがある。具体的な方法として、自身がアクセス権を持つ Web サーバーでの公開や、ブロックチェーンなどの共有されたストレージ上に記録することが挙げられる[12]。こうした形での公開が可能であれば、重複を避けて識別子

---

8 ゼロ知識証明は、ある主張が真であることを、真であること以外の知識を他者に伝えることなく説得する技術である。解くのが困難とされる問題について解を知っていることを他者に示すが、その際、解についての知識を一切他者に与えない。

9 W3C が 2022 年 7 月に標準規格として勧告した。

10 識別子の対象は法人やモノなど、個人以外のものを対象としうる。本稿では、個人のアイデンティティのみ扱う。

11 DID メソッドの中には、レジストリへの登録を想定しないものも存在する。

12 分散型識別子に非対称鍵暗号の公開鍵を紐づけておくことで、ある分散型識別子が自身

を付与できる。

このようなことが適切に行えたとすると、特定の主体による管理への依存度合いを下げつつ適切に個人を識別し、それに基づいた認証を実行できる。

３－３　自己主権型アイデンティティの社会実装の試み

自己主権型アイデンティティの考え方に基づいた技術について、社会実装を目指す例も出てきている。本節では、VC や分散型識別子を活用しようとする事例や、これとは異なるアプローチで自己主権的性質を備えようとする試みを取り上げる。

（VC と分散型識別子の活用事例）

カナダのブリティッシュ・コロンビア州は、デジタルガバメント推進の一環として、OrgBook BC というサービスを提供している。OrgBook BC は、各種の政府機関が企業等に対して VC の形式で発行したビジネス上のライセンスや許可証を、Web サービス上で検索可能にした実運用中の公開登録簿である。150 万以上の法人と 440 万件以上の VC が登録されている。このサービスは、VC と分散型識別子を扱う分散型台帳上に構築されることで、アイデンティティ管理が特定の組織に依存しない仕組みとなっている[13]。

金融分野に関連する事例としては、同国の Verified.Me が挙げられる。NPO の DIACC (Digital Identification and Authentication Council of Canada) が策定したフレームワークに基づき、SecureKey Technologies 社が、カナダの主要金融機関 7 社で構成されたコンソーシアムとともに、同サービスを 2019 年 5 月から提供している。ここでは、金融機関から成るコンソーシアムがアイデンティティ基盤を構成する分散型台帳を運営し、ユーザーは、金融機関、信用情報機関、通信事業者などに指示を送ることで、自身の属性をサービス事業者に提供できる。Verified.Me は、従来型のフェデレーションモデルのアイデンティティと自己主権型アイデンティティを組み合わせることで双方の利点を生かすよう設計したとされている。

（分散アプリケーションの開発に活用する試み）

VC や分散型識別子といった技術を活用し、分権化されたアプリケーションの開発を推し進める取り組みとして、「Web5」がある。Web5 は、決済サービス会社

と紐づくものであることを自身の秘密鍵を用いて暗号的に主張できる。

[13] また、このような分散型台帳を用いたアイデンティティ管理を、企業等でなく個人に適用する構想も進められている。

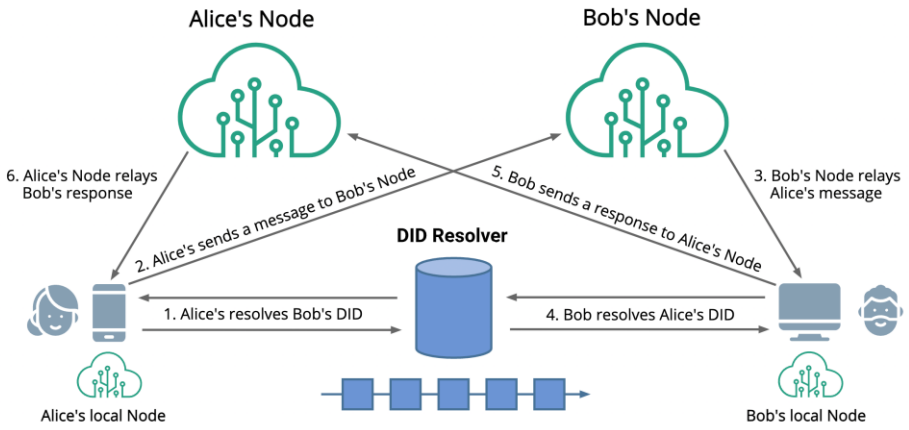
BLOCK（旧 Square）の子会社 T.B.D, Inc.が提案した、自己主権型アイデンティティの考え方に基づいた社会構想である。

ここでは、個人にまつわる様々なデータを、自身が管理するノード（Decentralized Web Node、以下「DWN」）で管理する（図表 3）。そのデータを用いて、個人の属性を他人に証明する際は、VC を活用する。

一般にウェブ上のサービスは、なんらかのアプリケーションソフトウェアから提供されることになるが、Web5 におけるサービス提供は DWA（Decentralized Web App）が担う。DWA は、DWN にアクセスしその情報を活用してサービスを提供するが、DWA がデータを保持するわけではなく、データはあくまで DWN に保存される。DWN の識別には、分散型識別子が活用される。

このようにサービスやアプリケーションから独立してデータが扱われることによる、サービス間のインターオペラビリティ（データのポータビリティ）の向上が、このアーキテクチャの利点の一つとされている[14]。

（図表 3）Web5 のネットワークトポロジー



（出展）「Decentralized Web Node」（https://identity.foundation/decentralized-web-node/spec/）

（ブロックチェーン上で個人の連続性を表現する試み）

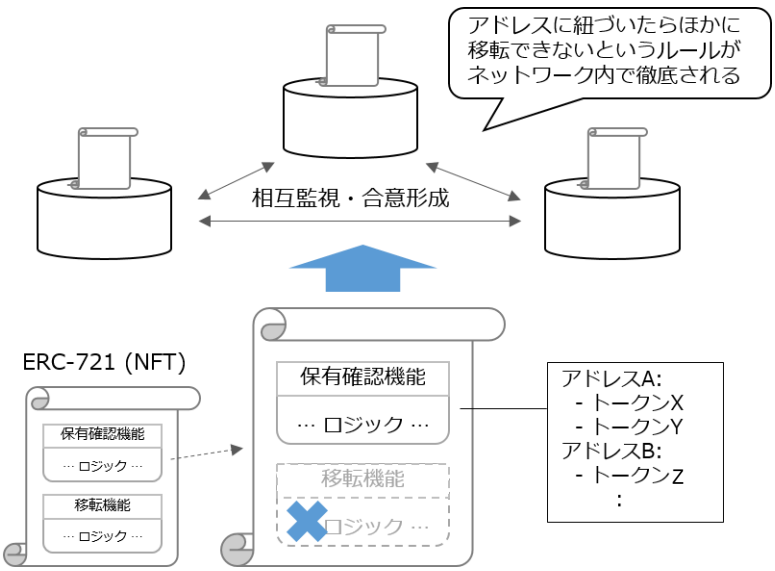
個人の身元などの情報を開示することなく、その個人の固有性・連続性の表現を試みるアプローチもある。以下では、ブロックチェーンの中でも、個人が身元や属性を明らかにせずに取引などを行うことが可能なパーミッションレスブロックチェーンにおいて、特定の主体に依存しないアイデンティティ管理の実現を目指す提案として、「ソウルバウンドトークン」を取り上げる。

14 目的の情報を扱うためのデータの構成や仕様が、DWA 間で共有されていることが前提となる。

アカウントやウォレットを「ソウル」と呼び、ソウルに半永久的に紐づく譲渡できないトークンを「ソウルバウンドトークン」(Soulbound Token、以下「SBT」)と呼ぶ[15]。SBT は、個人が身元や属性を明らかにせずに取引などを行うことが可能なパーミッションレスブロックチェーンにおいて、現実の身元の情報を示さないまま、その個人に紐づく特徴を表現する手段となる。たとえば、あるイベントへの参加者に SBT が発行されると、SBT が譲渡できないことによって、その保有者がイベント参加者であったことを示す証拠となりうる。これによって、イベントに参加した人だけが、後日に特典が得られるといったことが可能となる。ここでは、現実の身元の情報の開示は不要である。

具体的な実装例として、NFT (Non-Fungible Token) [16]のスマートコントラクトから、他者に移転する機能を除いたものを作成して用いる方法がある。パーミッションレスブロックチェーンに、移転機能を除いたスマートコントラクトを展開することで、SBT の「ロジック」がブロックチェーンに参加する各ノードに共有され、「トークンの発行」や「トークンとアカウント（アドレス）との紐づき」の確認が行えるようになる。このような形で、ブロックチェーンの相互監視のもと、SBT が「一度アカウントに紐づいたら他のアカウントに移らない」ことが徹底される（図表 4)。

（図表 4）譲渡不可能性の単純な実装方法



なお、この方法のみでは、秘密鍵を譲渡してしまうことでトークンを実質的に

[15] SBT の活用の可能性についてのホワイトペーパーが 2022 年に公表された（Ohlhaver, Weyl and Buterin, 2022)。
[16] ここでは ERC-721（Entriken et al., 2018）を想定する。

移転することについては制限されない。この点、Buterin and Schneider (2022) は、トークンを手放すと損失を被るといったインセンティブ設計により、ある程度こうした行動を抑制できるとしている。

SBT では、個々の属性の証明だけでなく、譲渡不可能性により個人についての不変性・連続性をもたらすものである。SBT により、現実の個人としての情報を開示することなく、デジタル上で活動を積み重ねそれを認知させることができ、このことで周囲とのより深い関係構築が可能になる。この点に着目した模索の事例もみられ、具体的には、保有する SBT を加味した重み付き投票の仕組みや、特定の管理主体を交えない、コミュニティによる秘密鍵のリカバリー（コミュニティリカバリー）等が提案されている[17]。

３－４　新しいデジタルアイデンティティにおける課題と留意点

紹介してきた取り組みは、目的やアプローチは異なるものの、自己主権的な情報の取り扱いを志向しており、特定のアプリケーションやサービスでの利用のみを前提とせず、広く通用するデジタルアイデンティティの確立を目指している点で共通している。

これらの試みは、デジタル社会における情報の取り扱いに関する、様々な選択肢を社会に提供することにつながると考えられるが、現時点で幅広く一般的に用いられるものとはなっていない。これらの新しいアイデンティティが広く社会に実装され活用されるには、クリアすべき課題や留意すべき点がある。

（依拠する主体の残存）

取りあげてきたデジタルアイデンティティの仕組みは、アイデンティティの提示やサービス提供について、当事者以外への依拠をなるべく減らす仕組みであるが、第三者の介在が全くないということではない。具体的には、分散型識別子の管理に Web サーバーを用いる場合、信頼される主体により運営される DNS や、HTTPS のための認証局への依存は前提となる。ストレージの可用性やアクセスポリシー等の影響も受ける。また、サービス提供の前提である認証の信頼性は、利用するデバイスやソフトウェア、またそれらを提供している事業者に強く依存する。たとえば、様々なアイデンティティを、自身が管理するひとつの環境（いわゆる「デジタルウォレット」など）に集約する場合、その環境を構成するデバイスやソフトウェアに欠陥があれば、その個人のアイデンティティ関連情報はリスクにさらされることになる。

---

17 秘密鍵を紛失した主体が所属する複数のコミュニティから、その主体とリアルタイムで交流のある個人を特定し、彼らの合意を得て秘密鍵を回復する仕組み。

（暗号技術に関する課題）

これまで説明した試みは、アイデンティティの提示やサービス提供について、当事者以外への依拠をなるべく減らすことを企図しているが、依拠のポイントを特定の主体から暗号技術に寄せているという解釈も可能である。したがって、暗号技術一般の課題、たとえば、暗号強度の検証、危殆化への対処、可監査性の担保などの課題を継承している。また、VC などの技術は、サービス事業者がその場で＝第三者の介在なく、暗号技術に基づいて検証するため、VC の適切な失効管理などの仕組みを備えない場合、十分な信頼を得られないこととなる。

これらへの対策を、コストやユーザビリティ等の観点を踏まえ、アイデンティティのライフサイクル全体をスコープに入れたうえで検討する必要がある。

（個人による鍵管理の難しさ）

紹介した取り組みは、個人が安全に秘密鍵を管理できることを前提にしているものが多い。秘密鍵を格納しデジタル署名を発行するデジタルウォレットを活用するにしても、引き続きユーザーにリテラシーが求められるほか、ウォレット提供事業者への信頼の問題からは逃れられない[18]。

デバイスやソフトウェアに関して選択肢や透明性が確保できなければ、これらへのリスクを生じることとなるが、一方で、前述した、特定の主体への依存を前提としないコミュニティリカバリーなどのような仕組みの成熟が、こうした問題を解決していく可能性もある。

（プライバシー上の留意点）

サービス事業者へのデジタル形式での情報の提示はデータの複製を意味しており、事業者の手元に残る可能性がある。前述のゼロ知識証明をすべてのケースに用いることは、現時点で現実的ではない。これを解決するために、発行したクレデンシャルの失効管理や、データを扱うプロトコルやソフトウェア実行環境の検証方法など、多岐にわたる検討事項がある。

また、本稿で取り上げた取り組みのうち、パーミッションレスブロックチェーンを想定しているものも多いが、一般に、パーミッションレスブロックチェーンに書き込んだデータは変更できない。書き込む情報が暗号化されたデータや仮名であったとしても、暗号の危殆化、名寄せ、外部データとの紐づけなどにより、個人にとって残したくない情報となるリスクが残存する。したがって、分散型識別子、SBT などのパーミッションレスブロックチェーン上に記録されうるデータ

18 秘密鍵をカストディアンなどに集約する場合は、より直接に他者への依存が問題になる。

も、仮にそれ自体が重要な情報でなくても問題になりうる。

（コストとのトレードオフ）

自己主権型のアイデンティティは、依存する主体の分散化を志向しているが、これは処理の効率化などの集中のメリットを捨てることになり、仕組み全体のコスト増加につながりうる。

Web5 のモデルのようにデータを分散して扱うことは、データや計算資源が集約されず、スケールメリットを低減しうるため、全体としてコストがかかる可能性がある。データや計算資源が集約されないほか、分散された環境それぞれにおいて十分なセキュリティを個別に維持する必要がある。

VC や SBT で行いうるように、アイデンティティを構成するクレデンシャルの発行体を複数主体に分散させることを想定した場合、それらの発行体を信頼できるかを判断するクレデンシャル検証者のコストは相対的に高まる。

４．アイデンティティと取引・決済

デジタルアイデンティティは、デジタル空間における経済活動が重要となっていく中で、重要性を増していくものと考えられる。本節では、デジタルアイデンティティと取引や決済との関係を説明したうえで、将来に向けたインプリケーションに触れる。

４－１　取引や決済におけるアイデンティティの重要性

経済活動、とりわけ取引や決済において、円滑に資金が支払われ決済が完了することは重要である。取引が、お互い持ち寄った品物とお金を、対面で、同時に交換されるといったシンプルなものであれば、相手がどのような人間であるかを問う必要性は低い。しかし現実には、遠隔地取引、信用取引、代理を立てた取引など様々な取引の形態があり、これらの取引では、相手が信頼できるのか、どこにいるのか、問題があった時に連絡ができるのか、といったことを知っていることが前提になる。ここでは、関係者のアイデンティティが重要になってくる。

このようなアイデンティティの重要性は、経済・社会のデジタル化の進展に伴い、一層高まると考えられる。たとえば、インターネットを介した商取引では、取引相手は遠隔地におり、発注、発送、受け取り、支払い、着金などがすべて同時ということはなく、各段階に時間差がある。インターネットを介してサービスを提供する事業者も、アクセスしてきたユーザーがサービスを受ける資格があるのか、適切に確認する必要がある。デジタル形式でアイデンティティを扱うこ

とは、デジタル社会における経済取引の基盤と言える。

より直接的に決済とアイデンティティが関係している分野としては、マネー・ローンダリングなどへの対策がある。国際的な議論の中で、プライバシーなどとのバランスを踏まえつつ、対策の有効性向上の検討や実践が続いているが、こうした領域でもデジタルアイデンティティのあり方は重要な考慮事項となる。

加えて、決済にかかる情報は、それ自体が取引主体にとって重要な情報であり、アイデンティティを構成する重要な要素になりうる。アイデンティティが取引や決済の前提であると同時に、取引や決済から生成される情報はアイデンティティを構成しうる。取引や決済の関連情報が、特定の主体に集約されることなく経済活動ができることは、プライバシー意識の高まりの中で、ますます重要になってくると考えられる。

４－２　取引・決済の未来へのインプリケーション

上記のように、デジタルアイデンティティは、デジタル社会におけるサービス提供の基盤であり、マネロン対策などの社会的要請に応えるための前提である。また、取引・決済関係の情報が、デジタルアイデンティティを構成するという側面もある。取引・決済の将来像を考える際にも、以下の点も踏まえ、デジタルアイデンティティに関する試みについて丁寧にみていくことが重要である。

（代替的な支払い手段の構成要素となる可能性）

既存のデジタルアイデンティティモデルの一つである、フェデレーションモデルのなかで、アイデンティティ連携を行うクレデンシャル発行体は、プラットフォーマーと呼ばれるメジャーなサービスの事業者が担っていることが多い。ユーザーにアイデンティティ管理に関する利便性を提供することで、プラットフォーマーの経済圏を強化している側面がある。こうしたプラットフォーマーのアカウントに、支払い手段が紐づいていることも多い。

ユーザーの同意のもとで、アイデンティティ情報や決済情報が適切に利活用され、サービスの利便性が向上することは有益だが、その仕組みに入らないという選択肢が残されていることも重要である。プラットフォーマーに対しユーザー自身の様々な情報を提供しないと、事実上、円滑な決済や取引ができないような状況は望ましくないだろう。アイデンティティ情報の提供を最小限にとどめるような支払い手段が、プラットフォーマーの提供する利便性の高い決済手段とともに、現実的な選択肢として社会に存在することは重要である[19]。自己主権

19 現金がそうした代替的な支払い手段のニーズの受け皿に結果としてなるかもしれない

型アイデンティティは、そうした代替的な支払い手段の重要な要素となる可能性がある。

（トークン化の中で自己主権型アイデンティティが発展する可能性）

近年、ブロックチェーン上の経済活動に関する動きとして、資金や資産の「トークン化」の動きがある。これは、資金や資産をブロックチェーンなどの基盤上で流通できる形態に変換するもので、これにより様々な資金と資産が、同じ基盤（または、相互運用性の高い複数の基盤）の上で流通することが目指されている。ステーブルコイン、セキュリティトークン、預金トークン、国債トークンなど、様々な資金・資産のトークン化の試みがある。もとより、自己主権型アイデンティティの実装を試みた事例には、ブロックチェーンを前提にしているものも多いが、上記のような資金・資産のトークン化の動きの中で、幅広い取引に活用されるようになる可能性がある。

ブロックチェーンではない伝統的な決済の仕組みにとっても、トークン化された資産や資金をどのように扱うか、またトークンが流通する新しい基盤との相互運用性についてどう考えるかという点は、重要なテーマとなりつつある。新しい基盤のアイデンティティ管理のあり方が自己主権型アイデンティティと親和的となる可能性があることを踏まえ、取引や決済の将来像を考える際に自己主権型アイデンティティの動向を意識して検討を進めることが重要である。

５．おわりに

本稿は、デジタルアイデンティティの管理の方法の中で、特定の主体への依存度を下げ、自分自身でコントロールすることを目指す自己主権型アイデンティティの動きに着目して、要素技術の解説と社会実装の事例紹介を試みた。そのうえで、デジタルアイデンティティのあり方が、経済取引や決済にとって重要であることを指摘した。

デジタル化社会におけるアイデンティティのあり方を考えることは、決済の未来を検討するにあたってもきわめて重要である。今後も、本稿で挙げたような自己主権型アイデンティティにかかる技術の動向や社会実装の試みを、適切にフォローすることが重要である。

が、社会のデジタル化が進み個人の取引がデジタルな領域で行われるようになると、現金で決済できる領域は小さくなる可能性がある。

参照文献

Buterin, V., & Schneider, N. (2022). *Proof of Stake: The Making of Ethereum and the Philosophy of Blockchains.* Seven Stories Press, Inc.

Christopher, A. (2016). *The Path to Self-Sovereign Identity*. Retrieved from https://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

Entriken, W., Shirley, D., Evans, J., & Sachs, N. (2018). *ERC-721 Non-Fungible Token Standard.* Retrieved from EIP-721: https://eips.ethereum.org/EIPS/eip-721

European Union. (2016). *General data protection regulation.*

International Organization for Standardization (ISO), and International Electrotechnical Commission (IEC). (2019). *ISO/IEC 24760-1: IT Security and Privacy —A framework for identity management — Part 1: Terminology and Concepts.*

Ohlhaver, P., Weyl, E. G., & Buterin, V. (2022). *Decentralized society: Finding web3's sould.* Available at SSRN 4105763.

Preukschat, A., & Reed, D. (2021). *Self-Sovereign Identity.* Manning Publications.

Province of British Columbia. (2024). *A public directory of organizations registered in BC*. Retrieved from OrgBook BC: https://orgbook.gov.bc.ca/search

T.B.D., Inc. (2022). *What is Web5?* Retrieved from tbd: https://developer.tbd.website/blog/what-is-web5

Temoshok, D., Proud-Madruga, D., Choong, Y.-Y., Galluzzo, R., Gupta, S., LaSalle, C., . . . Regenscheid, A. (2022). *NIST SP 800-063-4 -- Digital Identity Guidelines.* National Institute of Standards and Technology.

World Wide Web Consortium (W3C). (2022). *Decentralized Identifiers (DIDs) -- W3C Recommendation.* Retrieved from https://www.w3.org/TR/did-core

World Wide Web Consortium (W3C). (2022). *Verifiable Credentials Data Model v1.1 -- W3C Recommendation.* Retrieved from https://www.w3.org/TR/vc-data-model-1.1/

Worldcoin Foundation. (2024). *A New Identity and Financial Network.* Retrieved from Worldcoin Whitepaper: https://whitepaper.worldcoin.org/whitepaper-wld

佐古和恵. (2023). 分散型デジタルアイデンティティとは？ ～概念、仕組み、実現に資する技術と課題～. 日本銀行 IMES Discussion Paper, No.2023-J-8.