

デジタル社会におけるアイデンティティ証明を支える
Verifiable Credentials の概要と規格開発の動向

決済機構局 山田のど夏、新崎卓、清水智子、岡部恒多

Bank of Japan Review

2026年3月

デジタル化の進展に伴い、自分のアイデンティティをデジタル技術を用いて安全かつ確実に証明する重要性が高まっている。こうした背景のもと、Verifiable Credentials (VC、検証可能な属性証明) が注目を集めている。VCは、デジタル署名による真正性の確保や改ざん防止機能を備えた汎用的かつ機械可読なデジタル証明書であり、新型コロナワクチンの接種証明書で使用されたほか、金融実務への応用も含めた幅広い領域での活用が検討されている。この間、各種団体でVCに関する規格開発が進められており、例えば国際標準化機構 (ISO) ではVCの一形態である検証可能な取引主体識別子 (vLEI) の国際規格を2024年10月に発行した。本稿では、VCの概要や活用事例、規格開発の動向を概説する。

はじめに

デジタル化の進展に伴い、プライバシーの侵害やなりすまし、データ改ざん等のリスクが増大しており、「自分が何者であるか」——すなわち、自分のアイデンティティ——をデジタル技術を用いて安全かつ確実に証明する重要性が一段と高まっている。また、それと同時に、社会全体の利便性向上の観点からは、提示された証明書を迅速に検証可能な仕組みが求められている。

こうした社会的な要請に応える技術として、Verifiable Credentials (VC、検証可能な属性証明) が注目を集めている。VCを活用することで、個人や企業は、自分の属性——例えば証明書保有者の身元に関する情報や資格・権利に関する情報——を安全かつ信頼性の高い形で示すことができる。

VCの利活用に向けた取組みは様々な領域で進み始めている。新型コロナワクチンの接種証明書で活用されたほか、更なる利活用の拡大に向けて、わが国を含む各国政府や業界団体・民間企業でも検討が進められている。同時に、VCに関しては、各種団体で規格開発が進んでおり、国際標準化機構 (ISO) では、VCの一形態である検証可能な取引主体識別子 (verifiable Legal Entity Identifier: vLEI) の国際規格を2024年10月に発行した。

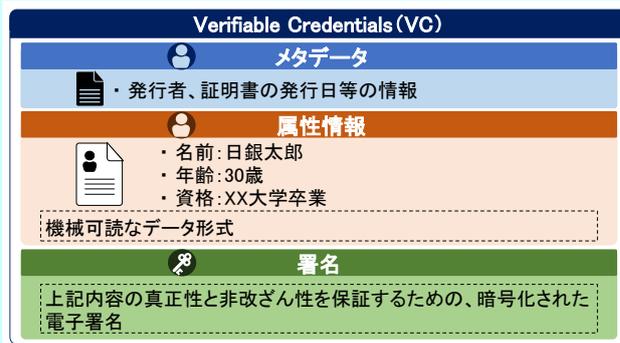
本稿では、まずVCについて、その概要、技術的な特徴点および活用事例について説明する。次にVCの規格開発の動向を概観したうえで、具体例としてvLEIを紹介する。

VCについて

(VCの概要)

VC¹とは、デジタル署名による真正性の確保・改ざん防止機能を有し、汎用的かつ機械可読なデータ形式として設計された、デジタル証明書である。具体的には、VCは、発行者等の情報に関するメタデータ、所有者の属性情報および証明書の真正性・非改ざん性を確保するデジタル署名で構成されており、これらは各種のデータ形式 (SD-JWT、mdoc等) で表現される (図表1)。

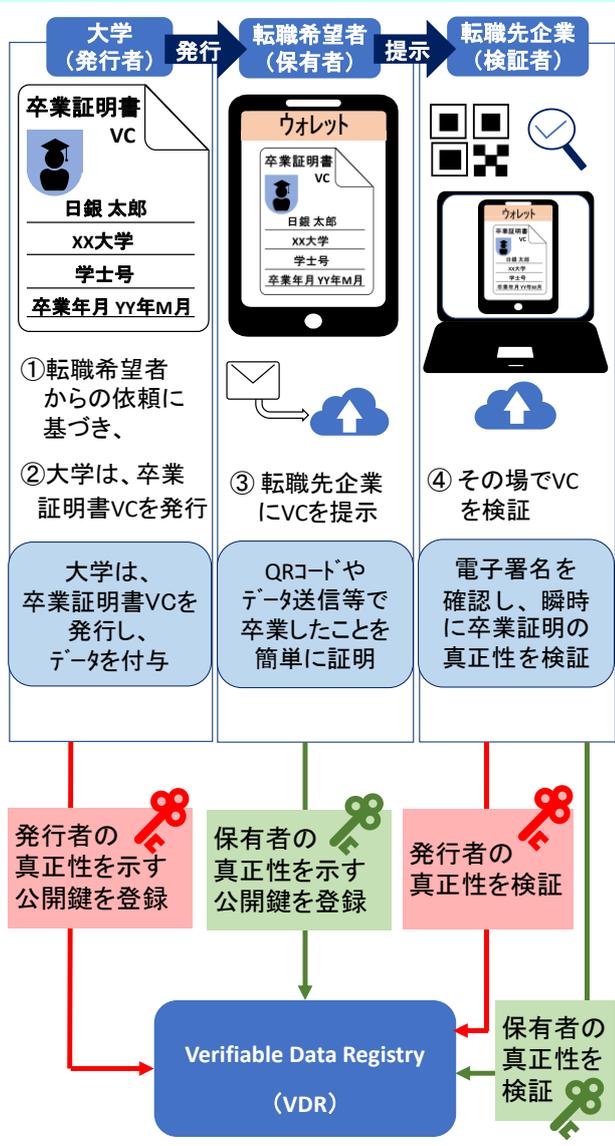
【図表1】VCの構造



(注) World Wide Web Consortium (W3C) 規格書等より筆者作成。

VC の利用に関する具体的なイメージを掴むために、転職希望者が大学から発行された卒業証明書(VC)を転職先企業に提示する事例を考えたい。具体的なプロセスは、次のとおりである(図表2)。

【図表2】VC の利活用の具体的なイメージ



(注) デジタル庁資料等より筆者作成。

まず、①大学卒業資格を有する転職希望者は、卒業証明書(VC)の発行を大学に依頼する。次に、②依頼を受けた大学は、卒業証明書の発行者として、大学の秘密鍵で署名したVCを転職希望者のウォレット²(VCの受取り・保存・提示を行うためのアプリケーション)に送付する。そして、③転職希望者は、自分のウォレットを用いて自分の秘密鍵で署名したうえで、転職希望先の企業に卒業証明書(VC)を提示する。最後に、④企業は受け取った卒業証明書(VC)の真正性について、大学および転職希望者の公開鍵をもとに検証を行

う。この際、2つの秘密鍵を用いて行われた署名の真正性は、Verifiable Data Registry (VDR)³と呼ばれるブロックチェーンやWebサーバ等に登録された、秘密鍵の保有者に関する検証可能なデータにより確保されている。この一連の流れを通じて卒業証明書(VC)の真正性が検証される。この例でみられるように、VCの大きな特徴は、VC保有者の属性情報の真正性を担保した上で、利便性が高い形で情報をやり取りできる点にある。

この仕組みは「IHVモデル」と呼ばれるVCの基本的な枠組みに基づいている。IHVモデルは、VCを使用した仕組み全体を「発行者(Issuer)」、「保有者(Holder)」、「検証者(Verifier)」という三者の役割で説明するモデルであり、三者の頭文字から「IHVモデル」と呼ばれる。発行者はVCを発行する主体、保有者は発行されたVCを管理する主体、検証者は提示されたVCの内容を確認し、真正性を検証する主体である。卒業証明書の取得・提示・検証の例で言えば、発行者が大学、保有者が転職希望者、検証者が転職希望先の企業に当たる。これら三者がそれぞれの役割を果たすことで、仕組み全体が成り立っている⁴。新型コロナワクチン接種証明書や米国におけるモバイル運転免許証⁵では、IHVモデルをベースにVCの実装が行われている。

紙媒体の証明書と比較すると、VCの活用には様々な利点がある。上記の事例では、VCを活用することにより、発行者である大学および保有者である転職希望者にとっては紙ベースの卒業証明書の発行および取得負担が軽減され(郵送等による証明書の取寄せが不要、取得日数の削減等)、企業にとっては証明書の真正性を担保することができるため、偽造による被害のリスクを抑え、かつ迅速に確認作業を進めることが可能となる。VCを活用することで、証明書の真正性を確保しつつ、発行者、保有者、検証者それぞれの利便性が大きく高まることが期待される。

(VCの技術的な特徴点)

VCの技術的特徴の一つは、データ形式の柔軟性である。多様な属性情報をVCに取り込むことが可能となるように、データ形式が各種の規格によって標準化されている。また、VCは、保有者に帰属する多様な属性情報を、検証者に対し、全部ではなく選択的に開示することに対応しており、

個人情報の保護やプライバシーの向上を図れる点も大きな特徴である⁶（図表3）。

さらに、VCは、従来の電子証明書（EC）とは異なり、中央集権的なデータベースを必ずしも必要としない。保有者が自らのVCを提示し、検証者がその電子署名を確認するだけで属性情報の検証が完結する。このように、情報管理の構造が、従来の電子証明書と比べて、より分権的になっていることもVCの大きな特徴である。

【図表3】VCと従来の電子証明書（EC）の比較

特徴	比較	内容
概要	VC	主体の持つ属性を証明
	EC	この主体がこの鍵の持ち主である証明
フォーマットの柔軟性	VC	・柔軟性が高い ・多様な属性・資格情報が含まれる
	EC	・固定的 ・単一の属性情報しか取り扱えない
選択的開示	VC	選択的開示に対応
	EC	選択的開示に非対応
情報管理の構造	VC	中央集権的なデータベースを必要としない
	EC	中央集権的なデータベースを必要とする
使用例	VC	・新型コロナワクチン接種証明書 ・卒業証明書VCの例に照らすと、卒業証明書の真正性を担保
	EC	・マイナンバーカードの署名機能 ・卒業証明書VCの例に照らすと、大学の公開鍵の真正性のみを担保

（注）各種資料より筆者作成。

（VCの活用事例）

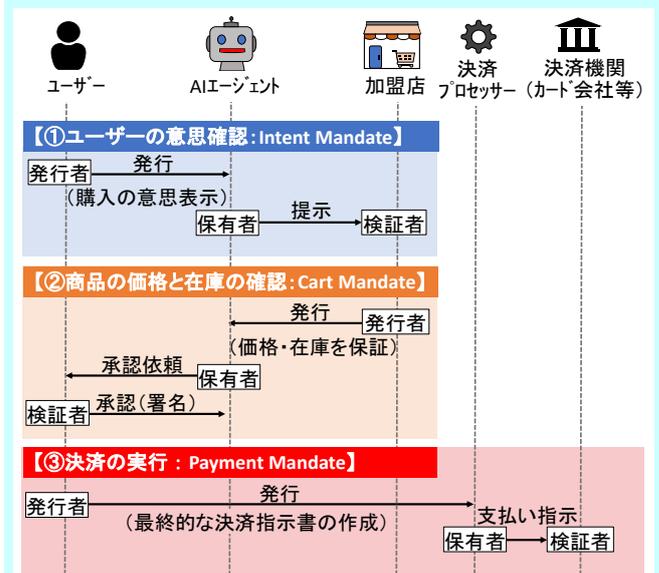
上述のとおり、新型コロナワクチンの接種証明書や米国におけるモバイル運転免許証など、VCの社会実装は既に進んでいる。今後の利活用を展望する事例として、以下の2つを紹介する。

1つ目は、本邦における事例として、DID/VC共創コンソーシアム（DVCC）で検討されているスキームが挙げられる⁷。金融機関の預金口座開設に当たっては、本人確認手続きがその都度行われる。DVCCでは、この手続きが口座開設申込者と金融機関双方にとって負担が大きいという現状を踏まえ、犯罪による収益の移転防止に関する法律（犯罪収益移転防止法）に基づいた本人確認の結果をVCとして発行し、申込者が必要な場面で別の金融機関に提示可能な仕組み（本人確認結果の二次利用）を検討している。具体的には、口座開設申込者が、ある金融機関との取引時における本人確認の結果をVC（「取引時確認VC」と命名されている）として管理し、公的個人認証等を活用

して本人確認を実施した結果（同、「署名検証結果VC」と併せて、この2つのVCを新たに預金口座を開設しようとしている別の金融機関に提示することで、口座開設実務の厳格性と簡便性が両立するスキームの実現を目指している。

2つ目は、AIエージェントを用いた商取引への活用である。AIエージェントとは、ユーザーの意図や指示を基に自律的に各種処理や取引を実行するプログラムを指し、商取引においてはユーザー指示に基づき、自動的に商品の在庫検索や取引処理を実行する。IT企業大手であるGoogleは、2025年9月、AIエージェントによる安全な商取引を実現するための仕組みである「Agent Payments Protocol（AP2）」を公表⁸。商取引にAIエージェントを活用することで、例えば複数のオンラインストアでユーザーにとって最適な商品を検索し、安全かつ簡便に購入することが可能となることを目指している。AP2では、商取引の各段階——ユーザーの意思確認、商品の価格と在庫の確認、決済の実行——でMandateと呼ばれる3種類のVCを用いて情報処理の内容を確実に確認することで、AIエージェントによるユーザーの指示に反する処理を防いだり、取引のプロセスの証跡を確実に残したりすることを可能とし、結果として取引全体の安全性を確保することを企図している（図表4）⁹。AIエージェントを用いた新たな商取引の領域において、VCは安全性と信頼性の確保の基盤技術となり得ると考えられる。

【図表4】Google AP2の概要



（注）Google ホームページ等より筆者作成。

VC の更なる利活用に向けた取組みは、民間だけでなく、各国政府でも進められている。日本では 2025 年にデジタル庁が VC の利活用に向けた検討会¹⁰を設置。現在、別の会議体¹¹において、住民票の写しや就労証明書の発行をユースケースとして取り上げ、仮にこれら証明書を VC として発行した場合の論点整理を行っている。また、欧州では、スマートフォンなどのデバイスに利用者のデジタル証明書を格納し、行政手続きや民間サービスの利便性を高めることを目的に、2026 年末までに「欧州デジタル ID ウォレット (EU Digital Identity Wallet : EUDIW)」の導入が予定されている。EUDIW に格納される証明書の裏付けとなる技術として VC が採用されている。EUDIW の導入に向けては、複数のパイロット実験が実施されており、「POTENTIAL¹²」というパイロット実験では、銀行口座の開設やモバイル運転免許証の発行など 6 つの領域について、EU 加盟 19 か国とウクライナにおいて官民 140 以上の参加者が関わる形で実証実験が行われた。EUDIW 実装のための枠組みや法制度面の整備も含め、2026 年末の導入に向けた取組みが進められている。

VC に関する規格開発の動向と具体例

VC の規格開発の動向を概観すると、World Wide Web Consortium (W3C) が 2017 年に検証可能な情報の概念を提唱¹³した後、2019 年に「Verifiable Credentials Data Model 1.0」を勧告として公表し、VC の基本的な仕組みを標準化した。また、Internet Engineering Task Force (IETF) は、データに署名や暗号化を施す方法を定めた規格「Jason Web Token (JWT)」に選択的開示機能を追加した「Selective Disclosure for JSON Web Tokens」(RFC 9901) を 2025 年に発行した。さらに、OpenID Foundation は、VC の発行プロトコルを定めた「OpenID for Verifiable Credential Issuance 1.0 (OID4VCI)」と VC の提示プロトコルを定めた「OpenID for Verifiable Presentations 1.0 (OID4VP)」などの規格を 2025 年に発行している。このほか、ISO/IEC 第一合同技術委員会 (JTC1) においても、オフライン利用にも対応したモバイル運転免許証の国際規格を ISO/IEC 18013-5 として 2021 年に発行し、さらに汎用化した規格として ISO/IEC 23220 シリーズの開発を進めている。

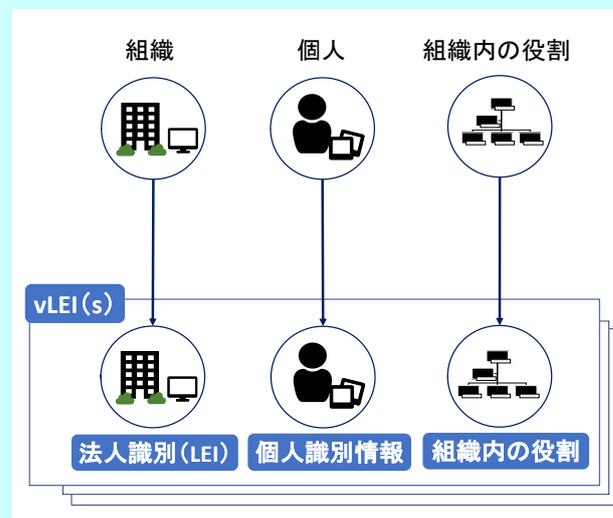
以下では、VC の規格開発の一例として、日本銀行が国内委員会の事務局¹⁴を務めている ISO/TC 68 (国際標準化機構・金融サービス専門委員会) において、2024 年 10 月に国際規格 (ISO 17442-3) として発行された「検証可能な取引主体識別子 (verifiable Legal Entity Identifier : vLEI)」を紹介する¹⁵。vLEI の大きな特徴は、後述するように、非営利組織のグローバル LEI 財団 (Global LEI Foundation : GLEIF) を頂点とするトラストチェーン構造が形成されており、エコシステム全体のガバナンス構造が明確化されている点である。

(vLEI の概要)

vLEI は、取引主体識別子 (Legal Entity Identifier : LEI)¹⁶を基礎としている。LEI は、金融商品の取引当事者 (法人、ファンド等) を識別するための国際的な識別子であり、英数字 20 桁のコードとして表現される。現在、LEI は、創設のきっかけとなった店頭デリバティブ取引の報告用途のみならず、決済指図などの他の金融分野、貿易分野をはじめとした非金融分野など、幅広い領域で利用されている。

vLEI は、LEI コードを含む法人のアイデンティティ、役職者のアイデンティティおよびその役職者が組織において果たす役割、を表した各種の VC を一つに結び付けた仕組みである。vLEI の直観的な理解としては、取引と紐づいた「法人情報 (LEI)、当該法人の役職者の名前と役職を入れ、デジタルに暗号署名され封緘された封筒」である (図表 5)。

【図表 5】 vLEI の概念図

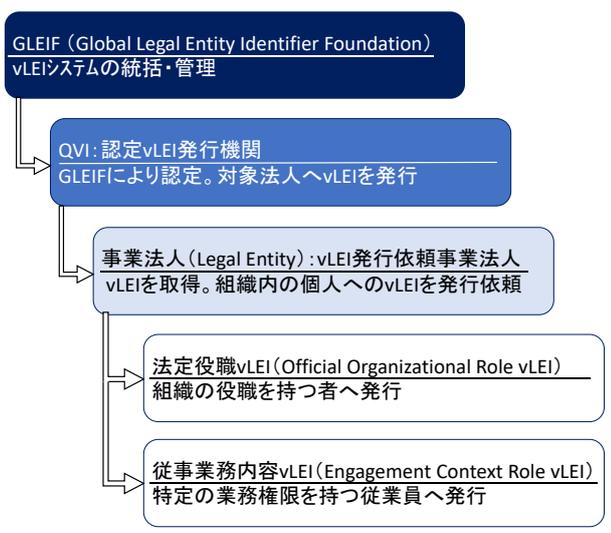


(注) GLEIF ホームページ等より筆者作成。

vLEIの特徴の一つは、GLEIFがvLEIに関するエコシステム全体のガバナンスを担っており、トラストチェーン——信頼の関係性を署名等の繋がりを辿ることで確認可能な仕組み——の基盤を提供している点である。一般的なVCでは、証明書の真正性は担保可能であるものの、VCの発行者の信頼性確保が課題となる。一方、vLEIについては、GLEIFがvLEIのエコシステムをデジタル的に検証可能な形で管理しており、システム全体のガバナンスを担うことで、vLEIの信頼性を高めている。

vLEIのトラストチェーンは、GLEIFがQVI(Qualified vLEI Issuer: 認定vLEI発行機関)を認定するとともにQVIのvLEIを発行し、QVIが対象法人にvLEIを発行、QVIあるいは対象法人が役職者に役職等に関するvLEI(法定役職vLEI、従事業務内容vLEI)を発行¹⁷するというもの(図表6)。

【図表6】vLEIのトラストチェーン



(注) 日本銀行 ISO パネル第9回 GLEIF 資料等より筆者作成。

このように、各レイヤーでvLEIを発行することで、入れ子構造のトラストチェーンを形成していることがvLEIの特徴である。川下にあるvLEI(例えば法定役職vLEI)を検証する際には、川上の内容(対象法人のvLEI等)も含める形で証明書の真正性を検証可能となっている。

vLEIのもう一つの特徴として、個人向けの利用を想定したVCと、使われている技術が異なる点が挙げられる。vLEIは、上述のトラストチェーンの構築とその検証を実現するため、データ形式、

セキュリティ¹⁸、データの伝送・表現¹⁹それぞれについて特徴的な技術を採用している。例えばデータ形式については、Authentic Chained Data Containers (ACDC) と呼ばれる、各種のvLEIによる入れ子構造の構築および複数の署名付き証明書の格納が可能な技術を採用している。また、これら技術はブロックチェーン等の外部台帳を必ずしも必要としないため、自己完結的にトラストチェーンを検証可能とすることで、エコシステム全体の安定性を高めている。

(vLEIの利活用の動向)

vLEIの主な機能は、①組織・人のアイデンティティの「認証」、②組織・人の報告データやコンテンツに対する「署名」、③組織・人に対する「権限付与」の3つである(図表7)。

【図表7】vLEIの用途

①「認証」	✓ 組織・人のアイデンティティをグローバルに認証 例: テレコム業界での迷惑メール・詐欺電話・ロボコール対策
②「署名」	✓ レポート、提出データ、コンテンツに対するデジタル署名 例: 欧州銀行監督機構(EBA)へのレポート・コンテンツ内容の証明
③「権限」	✓ 組織・人に対する権限をグローバルに許可 例: 組織として当局報告を行う際の権限認証

(注) 日本銀行 ISO パネル第9回 GLEIF 資料等より筆者作成。

こうした機能を機械可読な形で提供することで、なりすましや証明書の偽造リスクの防止と取引処理の自動化が実現できると期待されている。

現在、GLEIFによってグローバルに8社がQVIとして指定²⁰されており、上記の3つの機能を活かし、vLEIの具体的な利活用に向けた動きが進んでいる。金融当局向けの報告のような典型的な金融領域での活用²¹のみならず、通信における発信者認証による迷惑・詐欺電話対策やサプライチェーン管理(取引文書やデータに署名を行うことで、真正性を担保)、貿易金融取引(取引参加者の身元・権限をvLEIを用いて検証し、顧客審査コストを削減)など、様々な目的での利活用に向けた具体的な取り組みが進められている。

おわりに

本稿では、デジタル化の進展に伴い注目が高まっている VC について、その概要、技術的な特徴点や活用事例を概説した。また、各種業界団体・標準化団体による VC の規格開発を概観し、その一例として、2024 年 10 月に国際規格が発行された vLEI を紹介した。

VC という新しい技術がもたらす可能性は大きいと見込まれる。一方で、VC の更なる利活用を展望するに当たっては、多岐にわたる検討が求められる。例えば技術面では、様々な業界団体・標準化団体が VC の規格開発を進めていることで、VC の目的に応じて様々な規格やデータ形式が利用可能な状況となっている一方、複数の規格やデータ形式が併存することで、相互運用性の確保が論点となっている。また、運用面では、上述のとおり、正当な発行者により発行されたことに対する信頼性確保に関する課題のほか、VC を発行した後も、有効期限の管理、更新、属性変更に伴う再発行、さらには失効管理など、ライフサイクル

全体を通じた適切な運用プロセスが必要となる。これらに限らず、VC の更なる利活用に向けては、その導入に伴うリスクとその対応策を十分に検討する必要がある。

デジタル化社会において自分のアイデンティティを安全・確実かつ利便性の高い形で証明できるようにすることは、金融・決済の未来にとっても極めて重要な要素の一つであると考えられる。特に、デジタル化の更なる進展により様々なタイプのマネーが国境を越えて、これまで以上に高速で移動することが予想される。そうした中で、マネーを受払いする人や企業の情報もまた、安全・確実かつ利便性の高い形で証明・検証する必要性が高まるであろう。VC はそれに資する一手段になり得ると考えられる。

ISO/TC68 国内委員会事務局を務める日本銀行としては、今後も、VC に関する技術面の動向や利活用に向けた検討状況を適切に把握していきたい。

¹ World Wide Web Consortium (W3C) の「Verifiable Credentials Data Model v2.0」では、「改ざん防止機能を備え、作成者 (authorship) を暗号的に検証可能な属性情報 (筆者による仮訳) 」と定義されているが、本稿では VC に馴染みのない読者にも理解しやすい形で VC を定義した。

² W3C の「Verifiable Credentials Implementation Guidelines 1.0」では、利用者が VC を保管するソフトウェアを Repository と定義した上で、その一例としてウォレットを提示している。

³ VDR には、公開鍵のほか、スキーマと呼ばれる VC のデータ構造の定義、失効情報など、VC の検証に必要な情報が登録される。W3C の「Verifiable Credentials Data Model v2.0」では、VDR へ登録された情報について、改ざん検知可能であることや誰がどのようなデータを管理しているかの正確な記録であることが期待されているとしている。

⁴ 後述するように、一般的な VC では、VC が正当な発行者により発行されたものであることを十分に保証しない (言い換えると、正当でない発行者により発行された VC であることを排除できない) 場合がある。この場合、発行者の信頼性を確保するためには、信頼できる発行者のリスト (トラストリスト) の作成など別途の手当が必要である。

⁵ 米国のモバイル運転免許証は国際規格 ISO/IEC 18013-5 に基づいて発行されている。American Association of Motor Vehicle Administrators (AAMVA) から実装ガイドラインとして「Mobile Driver's License Implementation Guidelines」が発行されている。

⁶ この特徴の一方で、デジタル庁「属性証明の課題整理に関する有識者会議 (第 1 回)」(<https://www.digital.go.jp/councils/vc-diw-governance/2c9c78e4-4cb5-4ef0-a3e5-6fd461d0ef84>) の事務局説明資料では、VC に起因するプライバシーの侵害として、「VC は名寄せに利用されやすい情報 (Issuer の署名値等) を含むため、複数の Verifier が意図的に VC を共有し名寄せを行うことで、利用者

がプライバシーを侵害されるリスクが想定される。」とも指摘されている。

⁷ DVCC の取組みはデジタル庁「Verifiable Credential (VC/VDC) の活用におけるガバナンスに関する有識者会議 (第 1 回)」の議事録および資料を参照 (<https://www.digital.go.jp/councils/verifiable-credential-governance/5a5c145f-85f4-41a5-bc51-4e442c6154b8>)。

⁸ AP2 の概要は、Google ホームページを参照 (<https://cloud.google.com/blog/products/ai-machine-learning/announcing-agents-to-payments-ap2-protocol?hl=en>)。

⁹ AP2 には、ユーザー立ち合い型 (Human Present) とユーザー非立ち合い型 (Human Not Present) の 2 つがあるが、図表 4 では前者の概要図を示した。

¹⁰ 脚注 7 の会議体資料を参照。

¹¹ デジタル庁「属性証明の課題整理に関する有識者会議」(<https://www.digital.go.jp/councils/vc-diw-governance>)。

¹² POTENTIAL における各種取組みについては、下記 URL を参照 (<https://www.digital-identity-wallet.eu/>)。

¹³ W3C は、2017 年に「Verifiable Claims (後の Verifiable Credentials)」のデータモデルとその表現方法について標準化することを目指し、ワーキンググループを設立。その後、具体化に向けた検討が進められた。

¹⁴ 日本銀行決済機構局は、経済産業省に設置されている審議会である日本産業標準調査会 (Japanese Industrial Standards Committee : JISC) から委任を受けて、ISO/TC68 (金融サービス専門委員会) 国内委員会事務局の役割を担っている。ISO/TC68 国内委員会の取組み等は、下記 URL を参照 (<https://www.boj.or.jp/paym/iso/index.htm>)。

¹⁵ 日本銀行決済機構局は、2025 年 2 月に「ISO パネル (第 9 回) : 店頭デリバティブ取引の市場改革から外為業務等に広がる取引

主体識別子 (LEI) の活用可能性」を開催 (https://www.boj.or.jp/paym/iso/iso_panel/isop250228.htm)。vLEI に関する GLEIF からの説明のほか、vLEI を含めた LEI 全般に関するパネルディスカッションを実施した。

¹⁶ LEI は、リーマン・ショックの際に、グローバルな店頭デリバティブ取引の実態をマクロ的に把握できなかったことが取引の清算を遅らせ、危機を拡大させたとの反省に基づき創設された。LEI コードの運営主体は GLEIF が担っており、GLEIF は金融当局・中央銀行からなる規制監視委員会 (Regulatory Oversight Committee) によって監督されている。LEI は ISO 17442 として 2012 年 6 月に国際規格化されている。LEI の概要と導入の経緯については、橋本崇「金融サービスで用いる法人の ID ナンバーにかかる国際的議論の現状」(日銀レビュー2019-J-7、2019 年)を参照 (https://www.boj.or.jp/research/wps_rev/rev_2019/data/rev19j07.pdf)。

¹⁷ 法定役職 vLEI は、国際規格 ISO 5009 で定められた組織や法人を代表する個人の公的役割に基づいて発行される vLEI。一方、従事業務内容 vLEI は、それ以外の社内での役割 (例えば Chief Risk Officer) に対して発行されるもの。いずれについても、対象法人の情報を含んでいるが、法定役職 vLEI の発行は QVI が行う一方、従事業務内容 vLEI の発行は QVI と対象法人のいずれも可能である点に留意。

¹⁸ セキュリティについては、Key Event Receipt Infrastructure (KERI) という技術を採用。KERI は、外部のブロックチェーン等への依存を必須としない設計であるため、適用範囲の柔軟性を確保しやすいことに加え、次に使う鍵をあらかじめ決めて“予約”しておく Pre-rotation と呼ばれる仕組みにより、万一秘密鍵が盗まれた場合でも、なりすましに使われにくくすることを企図。

¹⁹ データの伝送・表現については、Composable Event Streaming

Representation (CESR) という技術を採用。署名などの暗号に関する情報 (改ざん検知や本人確認に使う情報) を含め、データのフォーマットを厳格に定義することで、データの構造と検証に必要な情報が崩れにくく、連続したデータを順に読み取って処理するような方式や機械処理に適した運用を志向している。

²⁰ QVI のリストは GLEIF のホームページを参照 (<https://www.gleif.org/ja/organizational-identity/get-a-vlei-list-of-qualified-vlei-issuing-organizations>)。本邦においては、TOPPAN エッジ社が 2025 年 9 月に QVI に認定された。

²¹ 欧州銀行監督機構 (EBA) は、バーゼル規制に基づく開示 (いわゆる第 3 の柱) に関する新しい報告要件の対応のために、vLEI を用いたパイロット実験を 2024 年から 2025 年にかけて実施。本実験では、vLEI を活用することで、効率的かつ改ざん不可能な形で報告者のアイデンティティを管理しつつ、金融当局と金融機関双方にとって対応負担を削減することが検討された。

日銀レビュー・シリーズは、最近の金融経済の話題を、金融経済に関心を有する幅広い読者層を対象として、平易かつ簡潔に解説するために、日本銀行が編集・発行しているものです。ただし、レポートで示された意見は執筆者に属し、必ずしも日本銀行の見解を示すものではありません。

内容に関するご質問等に関しましては、日本銀行決済機構局 決済システム課 情報技術標準化グループ (代表 03-3279-1111 内線 6887) までお知らせ下さい。なお、日銀レビュー・シリーズおよび日本銀行ワーキングペーパー・シリーズは、<https://www.boj.or.jp> で入手できます。