IMES DISCUSSION PAPER SERIES

検証可能クレデンシャルにおける本人紐づけを巡る論点：適用事例にみる対応方法と金融分野への含意

佐古和恵（さこかずえ）

Discussion Paper No. 2024-J-22

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

日本銀行金融研究所が刊行している論文等はホームページからダウンロードできます。
https://www.imes.boj.or.jp

IMES Discussion Paper Series 2024-J-22
2024 年 12 月

検証可能クレデンシャルにおける本人紐づけを巡る論点：適用事例にみる対応方法と金融分野への含意

佐古 和恵 *

要　　旨

検証可能クレデンシャル（Verifiable Credential: VC）とは、ある対象（人、モノ、組織など）の属性情報の正しさを発行者が保証する電子的な証明書であり、その技術的な中核はデジタル署名である。VC は属性証明の汎用的なツールとして、社会で流通する情報の信頼性を向上させる潜在能力を持ち、金融をはじめとするさまざまな産業分野において活用が期待される。他方、VC はデジタル・データゆえに、従来の紙の証明書と異なり、実活用にあたり注意すべき点がある。例えば、ある人物から「自分の証明書」として「〇山 A 子」と記載された証明書が送られてきたが、相手は本当に〇山 A 子なのだろうか。あるいはその証明書を B 県が発行したと記載されているが、本当に B 県が発行したものなのだろうか。このような、(1) 証明書の提示者実体が証明書に記載された提示者と同一人物であることの紐づけと、(2) 証明書の発行者実体が証明書に付与されたデジタル署名の発行者と同一であることの紐づけにおける正確性確保は、技術のみでは解決できない課題である。そこで本稿では、エンティティ（実体）と VC に記載された情報との紐づけにおける正確性確保の論点を解説したうえで、VC の適用事例としてワクチン証明書と資格証明書を紹介し、金融分野などの産業応用における VC の有用性と運用上の留意点について考察する。

キーワード：検証可能クレデンシャル、デジタル・アイデンティティ、認証、公開鍵
JEL classification: O31、O35、Z00

* 早稲田大学理工学術院教授（E-mail: kazuesako@aoni.waseda.jp）

本稿は、筆者が日本銀行金融研究所客員研究員の期間に行った研究をまとめたものである。本稿の作成に当たっては、副島豊氏（SBI 金融経済研究所）、菅和聖氏、金融研究所スタッフから有益なコメントを頂戴した。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

目　次

１．はじめに

分散型デジタル・アイデンティティとは、単一の管理機関に依存することなく、個人の属性を管理したり、対面またはオンラインで電子的に属性を証明したりする考え方である。佐古[1]では、分散型デジタル・アイデンティティを実現するための中核的な技術要素として、World Wide Web Consortium（W3C）[1]で仕様が策定されている検証可能クレデンシャル（Verifiable Credential: VC）について紹介した。分散型デジタル・アイデンティティの文脈において、VC は、適格な機関が個人の属性を保証するための証明書として利用される。例えば、運転免許や学校卒業などの資格証明、ワクチン接種証明といった用途が検討されている。また、属性の概念を拡張すれば、本人宛の請求書や明細書、契約書も VC として表現できる。さらに、個人の属性に限らず、組織やモノの属性を保証する証明書として VC を活用することも可能である。したがって、VC は単独でデジタル・クレデンシャル（電子的に発行された証明書、対となる概念は紙の証明書）として社会で流通する情報の信頼度を向上させる潜在能力を持つ。このため、VC は金融分野をはじめ、さまざまな産業分野において、属性証明の汎用的なツールとして活用できると期待される。

他方、VC はデジタル・データゆえに、従来の紙の証明書とは異なり、実活用にあたって注意すべき点がさまざまに存在する。とりわけ、紙の証明書においても潜在的に存在していたものの、デジタル・データによる証明書を提示する場面で顕著に現われる課題が、以下の 2 つの「紐づけ」である。1 つ目は、証明書に記述された情報と、個人や組織などの実体との「紐づけ」における正確性確保である。2 つ目は、証明書に記載された発行者情報と、証明書を発行した組織の実体との「紐づけ」の正確性確保である [2]。これらの課題は、VC に関する技術的対応のみで解消されるものではなく、利用目的や用途に応じた運用面での対応が必要となる。このため、これらの課題は学術界や産業界において広く認識されていながらも、正面から取り扱うことが難しく、現時点においても課題解決には至っていない。そこで本稿では、情報と実体の紐づけ方法と確保される正確性について考察することとしたい。

VC において考慮すべき紐づけは、図 1 に示すように、2 種類ある。1 つ目は、証明書（VC）に記載された属性情報が、VC を提示している人物（実体）に関す

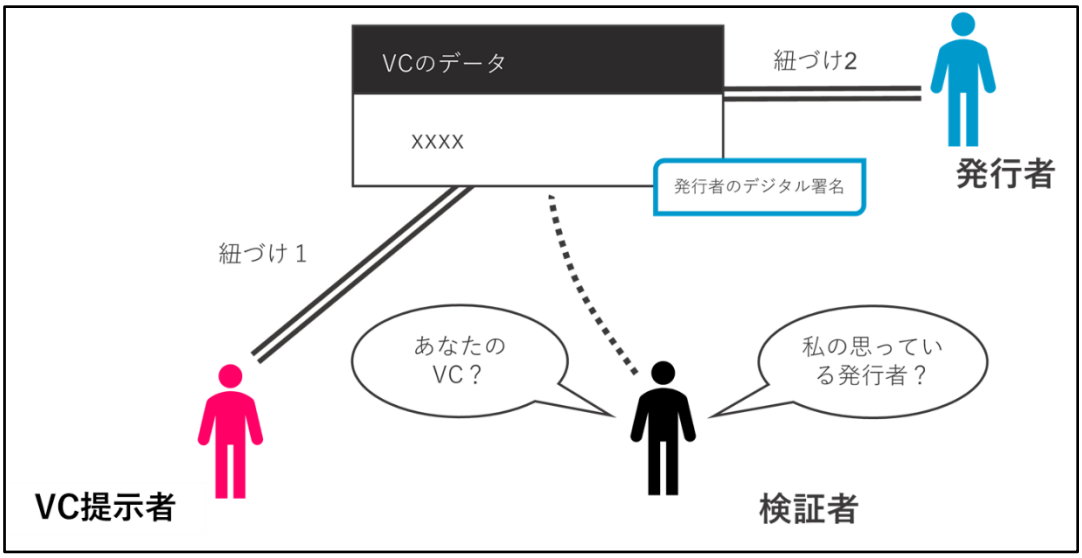
---

[1] W3C は、World Wide Web で使用される各種技術の標準化を推進するために設立された標準化団体である。

[2] より厳密には、後段で述べる通り、属性情報を証明する主体としての発行者の適格性も何らかの手段で確認する必要がある。この論点は、紙のデータにも存在し、デジタル・データに特有なものではない。また、利用目的に応じて適切な解決方法が異なると考えられるため、本稿では、この問題には深くは立ち入らず、可能な限り紐づけの論点に焦点を当てる。

るものであることの確認（紐づけ）である。例えば、目前で VC を提示する相手が B 県民であることを検証したい場合を考える。「〇山 A 子さんが B 県在住である」との属性情報が記載された VC が提示された際には、VC を提示した人物が〇山 A 子さんであることを別途確認できれば、VC の提示者が B 県在住であることを検証できる。2 つ目は、VC に記載されている証明書（VC）の発行者情報が、実際に VC を発行した人物や組織（実体）であることの確認（紐づけ）である。例えば、「〇山 A 子さんが B 県民である」と書かれた VC の発行者情報に「B 県」と記載されていた場合には、実際に B 県が発行したものであることを確認する必要がある。以上をまとめると、VC を提示された検証者は、なんらかの所定の手続きに従い、VC の提示者の本人確認と、発行者の確認の 2 つの紐づけを行う必要があるといえる。

図 1 2 つの紐づけ



デジタル・データの作成者を特定する方法の 1 つにデジタル署名技術があるが、デジタル署名さえあればこの問題が解決できる、と考えるのは早計である。例えば、先ほどの例の場合、デジタル署名が B 県によって発行されたことを確認するためには、デジタル署名を検証するための公開鍵が本当に B 県のものであることを別途確認する必要がある。

このように、VC の利用において、検証者が信頼できる紐づけの仕組みを確立することは容易ではない。この難しさは、組織や人などの名称の情報を以って、その名称を冠した実世界における組織や人などのエンティティ（実体）に関する事項を保証することが容易ではないことから生じる。より一般化すれば、属性と実体の紐づけの問題の本質は、エンティティをデジタル・データによって認証するための信頼できる情報をどのように確保するか、という問題である。ウェブ・

サイトにおける暗号通信では、公開鍵基盤（Public Key Infrastructure: PKI）が広く利用されていることも視野に入れつつ、さらに幅広い応用が想定されているVC でどのような仕組みが適切かを検討する必要がある。

本稿では、VC における紐づけの正確性確保に焦点をあてる。まず、VC における実体との紐づけ方法について解説する。次に、既に社会で実用されているVC などデジタル・クレデンシャルの適用事例を紹介し、それらの紐づけの正確性確保の方法を述べる。1 つ目の適用事例は、デジタル庁が発行する「新型コロナウイルス感染症予防接種証明書（以下、「ワクチン証明書」と呼称）である。2 つ目の適用事例は、大学や学会、資格検定機関など多くの組織が発行を開始している「資格証明書」である。なかでも、本稿では、Open Badge[2]と呼ばれる証明書の規格に沿った事例を紹介する。これに加えて、Open Badge をベースに、発行された資格証明書のセキュリティを高めるためにブロックチェーンを活用する blockerts[3]と呼ばれる規格に沿った事例も紹介する。これらの適用事例において、紐づけの正確性確保のために配慮されている点を述べたうえで、注意を払うべき点について考察する。

本稿の構成は以下のとおりである。2 節では VC の基礎を解説する。3 節では実体との紐づけにおける正確性確保の問題について解説する。4 節と 5 節では、VC などデジタル・クレデンシャルの適用事例として、それぞれワクチン証明書と資格証明書を紹介するとともに、紐づけにおける正確性確保への配慮について述べる。6 節は、金融業界を始めとした産業分野における VC の有用性および、実活用に向けた留意点について考察する。7 節は結びである。

２．検証可能クレデンシャルとは

検証可能クレデンシャル（VC）とは、ある対象（人、モノ、組織など）の属性情報の正しさを発行者が保証する電子的な証明書であり、W3C において、そのデータ・モデルと標準的な利用方法が制定されている[4]。

（１）デジタル・クレデンシャルと紙の証明書の比較

電子的に発行された証明書（デジタル・クレデンシャル）と、紙の証明書の大きな違いは、その検証方法である。

紙の証明書は、検証者である受取手が目視で検証することが多いため、目視等により偽造や改ざんが検出できるよう作成されている。発行者の適格性確認は、検証者が証明書に記載されている発行者を適格な人・組織であることをあらかじめ知っていることが前提となる。そのもとで、検証者は、証明書が偽造されていないことを目視で確認することにより、証明書の紙面に記載された発行者情報を正しいものとみなす。対象との紐づけは、対象の識別子が記載された真正の

（偽造されていない）証明書であることの確認と、必要に応じて別の身分証明書を提示し、両者に同一の識別子が記載されていることの確認となる。

一方、電子データは、その性質上、複製、偽造、および改ざんが容易であり、とくに、目視では偽造や改ざんに気付けないという共通認識がある。このため、目視に頼らない検証手続きとして、VC ではデジタル署名が提供される。暗号学的なデジタル署名を導入すれば検証手続きは自動化されるが、上述のように、デジタル署名を検証するための公開鍵と発行者、および対象の紐づけにおける正確性確保の問題は残存する（この論点は 3 節で述べる）[3]。このほか、VC の場合にも、発行者の適格性を確認する必要がある。

（２）公開鍵基盤が存在するもとでの VC の必要性

VC が電子的な証明書であるならば、VC の概念を導入して新たに規格を制定する必要はなく、X.509[4]ベースの公開鍵基盤から取得できる公開鍵証明書を VC として流用すればよいと考えることもできるかもしれない。しかし、この考え方は、以下の理由から適当とはいえないため、VC の導入と普及の方策が検討されている。

イ．証明内容の差異

現在普及している公開鍵証明書は、「このエンティティに対応する公開鍵は○○である」という命題のみを証明するものである。一方 VC は、公開鍵に限らない属性を証明するものであるため、公開鍵証明書よりも証明事項の範囲が広い。

この点、X.509 ベースの属性証明書は、「このエンティティの属性は△△である」という命題を証明するものである。属性証明書は、公開鍵を持つエンティティの属性を補足的に証明する仕組みとして規定されていたが、公開鍵証明書ほど普及しなかった[5]。また、属性証明書は、公開鍵証明書と併用することが想定されているため、VC のように単独での利用ができない。

ロ．証明内容の提示方法

公開鍵証明書ならびに属性証明書は、証明書全体をそのまま検証者に見せる

---

[3] 本稿では深く立ち入らないが、検証手続きが正しく実行されていることの確認も重要である。例えば、検証用のソフトウェアを用いる場合、その動作の妥当性を確認することは実務的には重要である。

[4] X.509 は、公開鍵証明書の標準規格の一つであり、RFC5280 において規定されている。

[5] 普及しなかった理由は定かではないが、属性証明書は公開鍵証明書と併用することが想定されており、当時、公開鍵証明書は個人より組織やサーバを対象とするものが多かったため、属性を証明する手段として、より手軽な方式があったからではないかと推察される。

という提示方法しか想定されていない。このため、証明書に記述された内容のうち、開示する部分を提示者が選択できる「選択的開示」という機能が検討されていない。

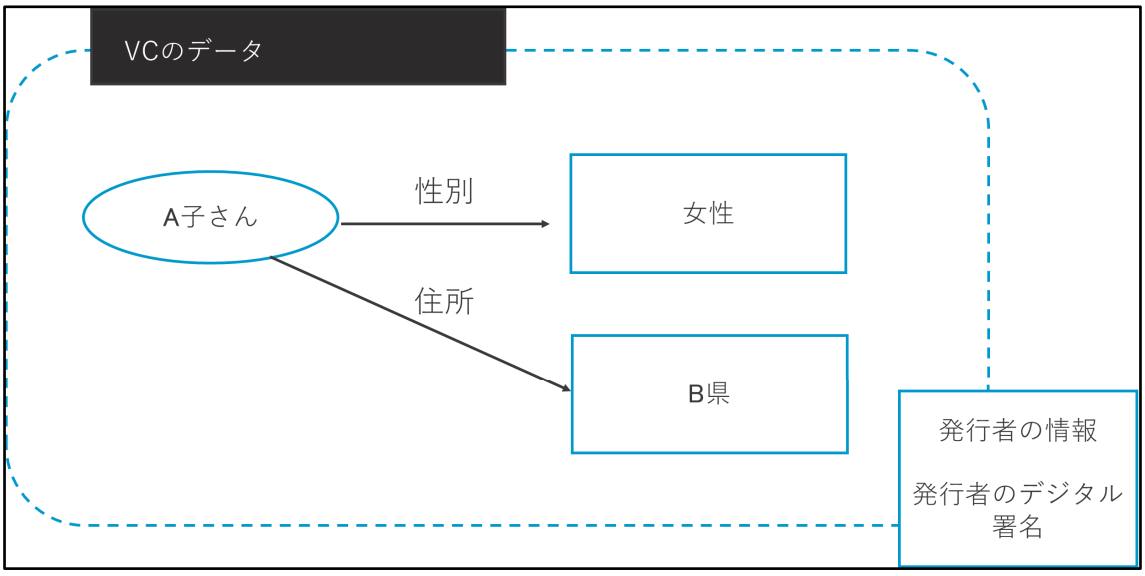
ハ．厳格な運用

公開鍵証明書は、対象のエンティティに対応する公開鍵の真正性を保証する観点で設計された仕様であり、厳格な運用が規定されている。そのため、必ずしも対象のエンティティが公開鍵を持たなくても良いようなユースケースに転用する場合には、管理・運用コストが見合わないと考えられる。

（３）VC の構成要素と検証手続き

VC に格納される情報の基本的な構成要素は、次のとおりである。まず、対象（Subject）を示す識別子と、その対象の属性情報（Attribute）についての記述（Claim）、および、この記述の内容を保証する人や組織（Issuer、以下では発行者）の情報がある。さらに、対象に関する記述と発行者情報に対して、発行者がデジタル署名を付与したものが VC である。例えば、A 子さんという対象について、性別が女性であり、住所が B 県であると記述された VC は図 2 のようになる。

図 2 VC の構成要素



VC の所有者（Holder、多くの場合は VC の発行を受けた対象者）は、必要に応じて VC を第三者に提示する [6]。VC を提示された検証者（Verifier）は、デジ

[6] 2 節（5）で紹介するように、VC そのまま見せるのではなく、情報を追加したり加工して VC を提示することは検証可能なプレゼンテーション（Verifiable Presentation）と呼ばれる。

タル署名などの正当性を所定の手続きに従って検証する。検証者が実施すべき事項は主に以下の 4 つである。

a） 発行者の適格性確認 : VC に記載されている発行者がその属性に関するお墨付きを与える主体として適格な人・組織であることを何らかの方法で確認する。
b） 発行者の公開鍵の入手 : 適格な人・組織である場合には、何らかの方法で発行者の正しい公開鍵を入手する。
c） 署名検証：VC が、VC に記載されている発行者により発行され、属性情報の記述が改ざんされていないことを確認するために、発行者の公開鍵を用いてデジタル署名を検証する。
d） 情報と提示者の紐づけ：VC に記載されている属性情報が、VC を提示している人に関する情報であることを何らかの方法で確認する。

（４）デジタル・クレデンシャルの変遷

本節（4）では、デジタル・クレデンシャルの例として、Open Badge の変遷について述べる。Open Badge は、1EdTech[7]が定める技術標準規格[2]であり、2022 年までに 7 千万枚以上のデジタル・クレデンシャルが Open Badge として発行されている[5]。Open Badge に記載される個人の属性は、主に資格に関するもの（資格情報）であり、本人が獲得した資格により、就職や昇格などに優位に働くことが期待されているものである。

バージョン 2 にあたる現行の Open Badge v2 には、大きく分けて Hosted Badge と Signed Badge の 2 種類があり、それらの検証方法には大きな違いがある。

Hosted Badge では、サーバが保有する情報を参照することでユーザの資格情報を確認する（図 3 における「サーバ保有情報による資格確認」）。すなわち、ユーザが所有している Open Badge にはホスト・サーバへの URL のみが記載されており、検証者は記載された URL にアクセスして得た資格情報を確認する。

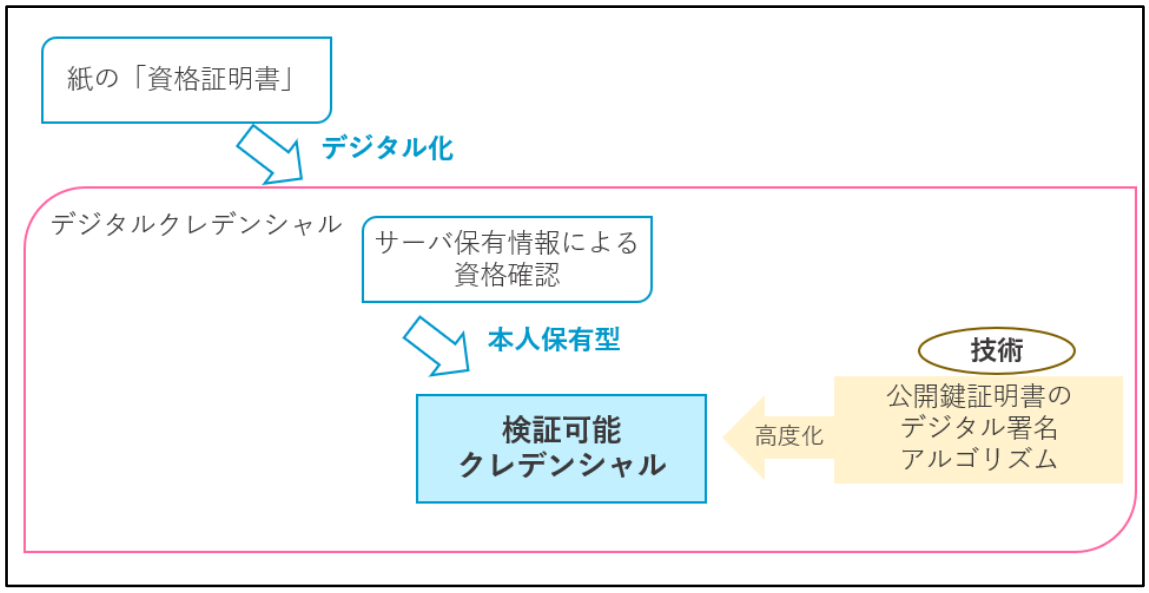
Hosted Badge には、いくつかの課題がある。まず、発行した Open Badge の資格情報およびその検証手段を提供するために、ホスト・サーバを常時稼働させる必要がある。また、ホスト・サーバは、どの検証者が誰に発行した Open Badge を検証したかという情報を掌握できるため、プライバシー確保の観点から懸念が残る。このほか、ホスト・サーバの情報が改ざんまたは消去された場合には、既発行の Open Badge の内容をホスト・サーバ側で改ざんしたり失効させられる点も懸念される。さらに、Open Badge に記載されているホスト・サーバの URL

[7] 2022 年に IMS Global から改名した教育向けのデジタル・クレデンシャルのエコシステムを推進する認証団体。メンバーは 33 か国、1,000 団体以上。

や、アクセスして得た資格情報には、デジタル署名等による保護がないことから、それらが改ざんされていたとしても検知できないという問題もある。このように様々な懸念が指摘されてはいるが、Hosted Badge は汎用のブラウザで誰でも URL から検証できるため、以下で述べる Signed Badge に比べて広く普及している。

Signed Badge は、Open Badge のデータに資格情報を含めたうえで、発行者のデジタル署名を付与したものである。ホスト・サーバに関する上記の懸念は払しょくされる反面、デジタル署名の検証に専用のソフトウェアが必要となる。

図 3 デジタル・クレデンシャルの変遷



最新バージョンである Open Badge v3 では、Hosted Badge の仕様を廃止し、Signed Badge の発展版にあたる VC の仕様を採用することが決定した。この仕様変更は、他人が運営するホスト・サーバに依存することなく、資格情報を証明したい本人が「提示する資格情報」と「提示する相手」を自身でコントロールし、受取側が資格情報を直接検証できる運用形態に移行するトレンドを汲んだものである[8]。また、W3C の標準である VC の仕様を採用することにより、Open Badge 専用の検証プログラムは不要となり、VC 用の検証プログラムを利用できるようにもなった。

Open Badge v2 の Hosted Badge から Open Badge v3 への変化は、デジタル社会における情報の正しさを確保する方法の変化であると捉えることができる。す

[8] これまでは、アイデンティティ・プロバイダが本人に関する情報を検証者であるサービス提供者に渡す形態が多かったが、近年は、同情報を検証可能クレデンシャルとして、本人がサービス提供者に直接提供する分散型デジタル・アイデンティティが注目されている。

なわち、従前は「発行者（ホスト・サーバ)」に、ある情報の正しさを保証させることによって、その情報の正しさを確認していた。この方法は、ある意味で堅実ではあるが、情報を開示する範囲と相手についての判断責任を発行者が負うことになるため、適切な情報管理を確保するためのサーバ運用（特に検証用のサーバ運用）や組織対応の面で運用上のコストが大きい。このコストは、正しさを保証したい情報にデジタル署名を付与し、どの情報を誰に開示するのかをユーザに判断させることで、取り払うことができると期待される。

ただし、デジタル署名技術の利用だけで、ホスト・サーバに直接確認する方式と同等の情報の正しさが自動的に確保されるわけではない。デジタル署名を検証するための公開鍵が、適格な発行者により公開されたものであることを確認することが重要である[9]。何故ならば、任意のデータについて、なんらかのデジタル署名を付与することは誰にでも可能だからである。デジタル署名の検証が、資格情報の証明手続きのなかで意味を持つためには、デジタル署名が適格な発行者により発行されたものであることを確認する必要がある。

（５）検証可能なプレゼンテーション

紙の証明書を提示する方法は、検証者に紙面全体を見せる方法のみであるが、デジタル・クレデンシャルの場合には、複数の提示方法がありうる。例えば、他人の証明書を提示するなりすましを防止するために、本人確認情報（デジタル署名など）を追加して提示する方法や、単一または複数の証明書のうち検証者に必要な属性情報だけを抜き出して提示する方法が考えられる。このように、さまざまな形で VC の内容を提示する際のデータ・フォーマットを、検証可能なプレゼンテーション（Verifiable Presentation: VP）と呼ぶ。VC のデータ形式とは別に、VP のデータ形式が W3C で制定されている。

VP を提示する際には、VP の作成者が VC の保有者と等しいことを検証可能とする必要がある。VC 保有者の公開鍵が VC に記載されている場合には、同公開鍵を用いて VP に付与されたデジタル署名を検証することにより、VP の作成者が VC 保有者と等しいことを確認することができる。

（６）VC の特徴的な機能

VC は、付与する発行者のデジタル署名技術として、高機能なものを採用することにより、機能を拡張できる。例えば、選択的開示機能を持つデジタル署名技

[9] サーバに直接確認する方式であっても「正しい」サーバに確認しているかどうかを別途確認する必要はある。

術[10]を採用した場合には、VP において不必要な情報を提示することなく[11]必要事項のみ証明することができる。図 2 の例であれば、検証者に対して「性別」の情報を秘匿しつつ、「B 県在住」であることのみを開示し、さらに、この情報（を含む元の VC）に B 県のデジタル署名が付与されていることも保証できる。また、大小関係などの記述内容についての性質を証明する機能も付与できる。例えば、あるテストの得点が 88 点であるとの成績データに関する VC を保有する状態で、実際の得点を開示することなく、得点が 85 点以上であったことのみを提示することもできる。この性質の証明には、ゼロ知識証明[12]と呼ばれる暗号技術が活用される。

３．VC における実体との紐づけ方法について

2 節（1）で述べたとおり、VC の検証においては、対象の属性情報と対象実体との紐づけ、発行者情報と公開鍵との紐づけの正しさを確認することが求められる。これは、他人の VP を悪意あるユーザが窃取して提示するなりすましのリスクや、不正な発行者により VC が偽造されるリスクに対処するためである。そこで、本節では、VC の検証における紐づけの方法について検討を行う。なお、VC の提示方法には対面と非対面（オンライン）があり得るが、本稿では、例として個人が対面で VC を提示する場合と、組織がオンラインで VC を提示する場合について考察する。

個人が対面で提示する際、検証者が対象の存在や名前などを既に知っている場合には、その対象の名前が記載された証明書（VC）の提示により対象の紐づけは完了する。しかし、対象の存在を知らない場合には、別途、対象の本人確認が必要となる。その場合の典型的な手段は、本人のみが保有すると想定されるパスポート等の身分証明書の提示である。証明書（VC）に本人の顔写真が掲載されている場合には、検証者の目前にいる対象との容貌の一致により、証明書（VC）と対象の実体が紐づいていることが確認できる（生体認証）。オンラインで組織

---

10 例えば、BBS 署名[6]など。

11 従来のデジタル署名技術を用いて選択的開示を可能とする方式として、IETF において SD-JWT（Selective Disclosure JSON Web Token）が標準化されている。この方法では、相異なる属性情報を選択して VP を作成することにより、選択的開示を実現できる。ただし、VP には、作成元となった VC を特定可能にする情報（具体的には VC に付与されたデジタル署名値そのもの）を含めて、検証者に提示する必要がある。このため、このデータ値を手掛かりに、複数の VP が同一の VC から作成されたことを知ることができるため、名寄せされるリスクがある。なお、IETF については脚注 32 も参照のこと。

12 ゼロ知識証明は、一方の当事者（証明者）が、別の当事者（検証者）に対して、ある命題が真であることを、命題が真であること以外の一切の情報を漏らさずに、証明することを指す。

が VC を提示する場合には、商業登記電子証明書[13]や、後述するドメイン認証を用いた確認で紐づけることができる。個人の場合と異なり、プライバシーに配慮する点が少なく、既存の仕組みが活用できる。ただし、検証者がしっかり相手組織の適格性を別途確認する必要がある。

このように、紐づけの方法にはいくつかの方法があり、本節（1）で次のイ.～ホ.をそれぞれ紹介する。

イ．　検証者にとって既知の識別子による紐づけ
ロ．　対象本人のみが所有すると想定される身分証明書などによる紐づけ
ハ．　生体情報による紐づけ
ニ．　公開鍵と秘密鍵のペアを用いた紐づけ
ホ．　ドメイン名を使った URL 配下にある情報による紐づけ

上記のイ．からニ．は主に個人を紐づけるときに用いられる手法である。対象が組織の場合には、主にニ．とホ．が用いられる。本節（2）では、ニ．とホ．を用いて、発行者組織の紐づけ方法を紹介する。

（１）対象実体の紐づけについて

イ．検証者にとって既知の識別子による紐づけ

この方法では、検証された VP に記載の識別子である、対象の名前やメール・アドレス、所属組織を特定するドメイン名などと、検証者の知識を照合することで対象の紐づけを行う。この方法は、検証者が所有者の存在を認識しており、かつ、その名前やメール・アドレスやドメイン名との対応関係についての知識を持っていることが前提である。例えば、眼前の人物の名前が「〇山 A 子」であることを検証者が事前に知っている状況を考える[14]。このときに、検証された VP から抽出された VC に「〇山 A 子さんは B 県に在住である」と記載され、適切なデジタル署名が付与されていたら、目の前の人物（実体）と VC の属性情報を紐づけ、眼前の人物が B 県に在住していることが確認できる。

---

13 法務省が商業登記に基づいて発行する電子証明書。詳しくは以下の URL を参照。
https://www.moj.go.jp/MINJI/minji06_00028.html

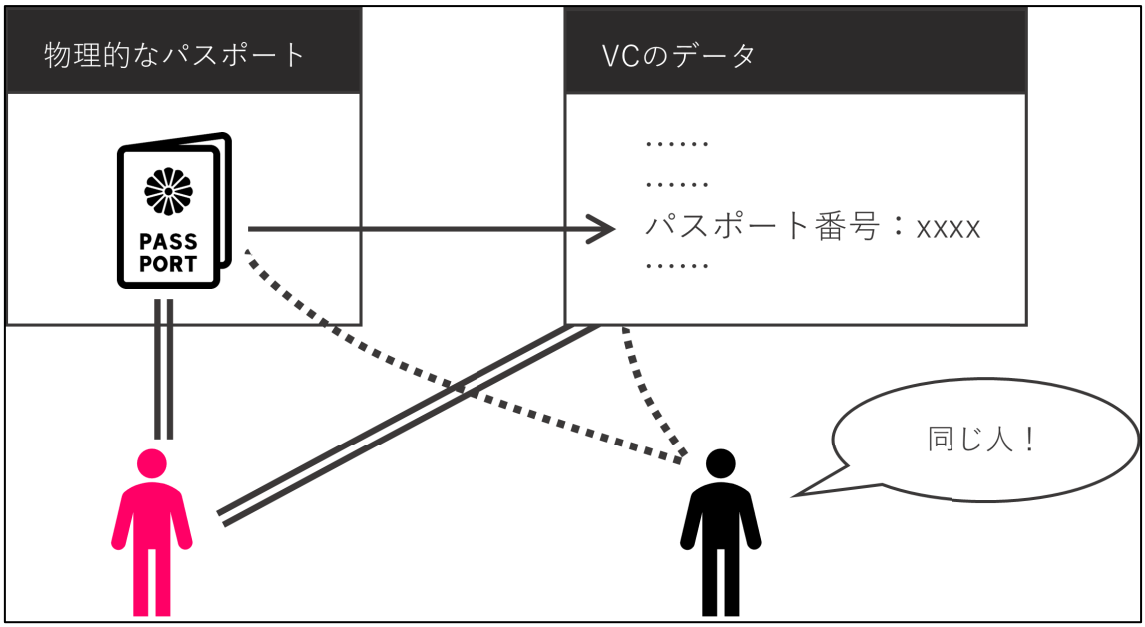
14 対面の場合に、眼前の人物の「名前を知っている」状態とは、対象人物（実体）の存在が既知であり、かつその人物の名前を認識している状態を表す。オンラインの場合に、対象人物の「メール・アドレスを知っている」状態とは、対象人物（実体）の存在が既知であり、かつ対象人物がそのメール・アドレスの唯一の利用者であることを何らかの事情で認識している状態を表す。例えば、過去に、そのメール・アドレスにメールを送信し、対象人物から返信メールが届いたといった経験により醸成された認識が該当する。

また、企業や団体の場合にはドメイン名を使うこともできる。例えば、「△△会社は××認定を受けました」、という内容を示す VC において、△△会社のドメイン名を記載することにより△△会社を特定することも可能である。ただし、検証者が対象の人物の名前やメール・アドレス、ドメイン名を知らない場合には、これら識別子の情報を使っても紐づけはできない。

ロ．対象本人のみが所有すると想定される身分証明書などによる紐づけ

この方法では、対象は、本人のみが所有すると想定される身分証明書など[15]（例えば、パスポート、運転免許証）を検証者に提示する。検証者は、身分証明書などに記載されている識別子と、対象が提示した VP から抽出された VC に記載された識別子を照合することで紐づけを行う（図 4）。この方法は、検証者と対象が初対面のケースであっても有効である。後述するワクチン証明書が、このケースに該当する。ただし、ある人物（標的）の VC とその人物名義の身分証明書を攻撃者が同時に保有している場合には、攻撃者は標的に紐づけられること（なりすまし）が可能になってしまう点には注意を払うべきである。

図 4 本人のみが所有する身分証明書などによる紐づけ



ハ．生体情報による紐づけ

この方法は、VC に記載された、対象の指紋や容貌についての生体情報を対象

15 身分証明書なども、適格な発行者から発行されている必要がある。

実体との紐づけに利用する。対象は、VP を検証者に提示する。検証者は、VP を検証したあと、VP から VC に記載された生体情報（登録顔画像など）を抽出し、眼前の提示者から得られた生体情報と照合する。なお、オンラインで照合する場合には、通信相手である提示者本人の生体情報が入力されていることを担保する必要がある。この担保がない場合には、提示者本人ではない他人の顔画像などを入力することにより、なりすましが可能になってしまう。

二．公開鍵と秘密鍵のペアを用いた紐づけ

この方法は、検証された VP から抽出された VC に記載された公開鍵に対応する秘密鍵を、対象のみが保有していることを利用して紐づけを行う（図 5）。まず、対象は、公開鍵と秘密鍵のペアを生成する。次に、公開鍵を VC に記載し、秘密鍵は機密情報として自身で保管する。検証者は、チャレンジ・レスポンス方式と呼ばれる方法[16]で、VC の所有者が公開鍵に対応する秘密鍵を保有していることを、秘密鍵の情報を得ることなく検証する。検証者は、VC の所有者実体が、VC の公開鍵に対応する秘密鍵の所有者であると確認でき、属性情報と VC の所有者実体を紐づけられる。

なお、検証された VP から公開鍵を抽出した後に、チャレンジ・レスポンス方式で本人確認を行う方法のほかに、VP を生成する前に検証者からあらかじめチャレンジを送付してもらい、秘密鍵を用いたレスポンスの情報（保持者のデジタル署名）を VP に含める方法もある。

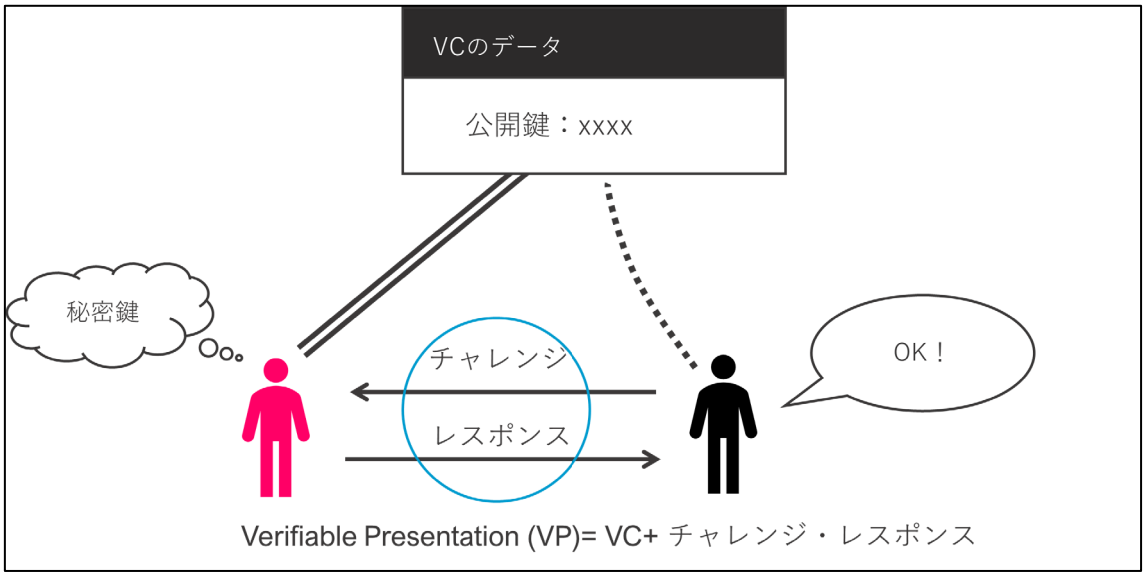
この検証の手続きを実行するには、チャレンジとレスポンスの情報を送受信するデバイスが必要である。また、この方式の安全性は、秘密鍵が VC の所有者によって安全に管理され、その機密性が保たれているとの前提に依拠している。

本方式は、検証者が対象人物について名前などの識別子を含めて何ら情報を持っていなくても有効な紐づけ方であり、デジタル・データに特有であるといえる。

---

16 チャレンジ・レスポンス方式とは、認証方法の一つである。本稿のケースの場合、まず、検証者は VC の所有者にチャレンジと呼ばれる情報を送る。次に、所有者は、（VC に記載してある公開鍵に対応する）秘密鍵の情報を用いてレスポンスと呼ばれる回答情報を作成し、検証者に返送する。検証者は、レスポンスが秘密鍵を使わなければ満たせない性質を持つことを、公開鍵とチャレンジの情報を使って検証する。この検証結果を以って、検証者は、所有者が秘密鍵の情報を持っていることを信頼する。なお、レスポンスの情報から、秘密鍵の情報を推定できないことが暗号学的な安全性の観点から重要である。

図 5 公開鍵と秘密鍵のペアによる紐づけ



ホ. ドメイン名を使った URL 配下にある情報による紐づけ

組織の多くはドメインを所有している。検証者を含めた多くの人々が、同ドメイン上のウェブ・サイトにより組織の存在を認識している状況であれば、ドメインを組織の実体との紐づけに利用できる。具体的には、VC に記載されている URL の情報を、対象（主として組織）の識別子として扱うことにより、対象実体と VC の属性情報の紐づけを行うものである。URL とはインターネット上の住所のようなものであり、企業などが排他的に利用するドメイン名をベースに構成される。例えば、VC に「https://〇〇〇.co.jp」などの URL が記載されており、それが C 社のドメインのものであることが知られていれば、C 社（実体）と VC との紐づけができる。これにより、VC に記載されている属性が C 社の属性であることを確認できる。また、検証者は、VC に記載されている組織の属性情報と、URL からたどれる組織のウェブ・サイトに掲載されている組織の情報とを照合することもできる。

この照合により、検証者は組織実体と属性情報を紐づけられる。URL は、イ. における既知の識別子による紐づけで使用する識別子とは異なり、インターネットから取得できるコンテンツで証跡を確認することが可能な識別子であるといえる。

（２）発行者の紐づけについて

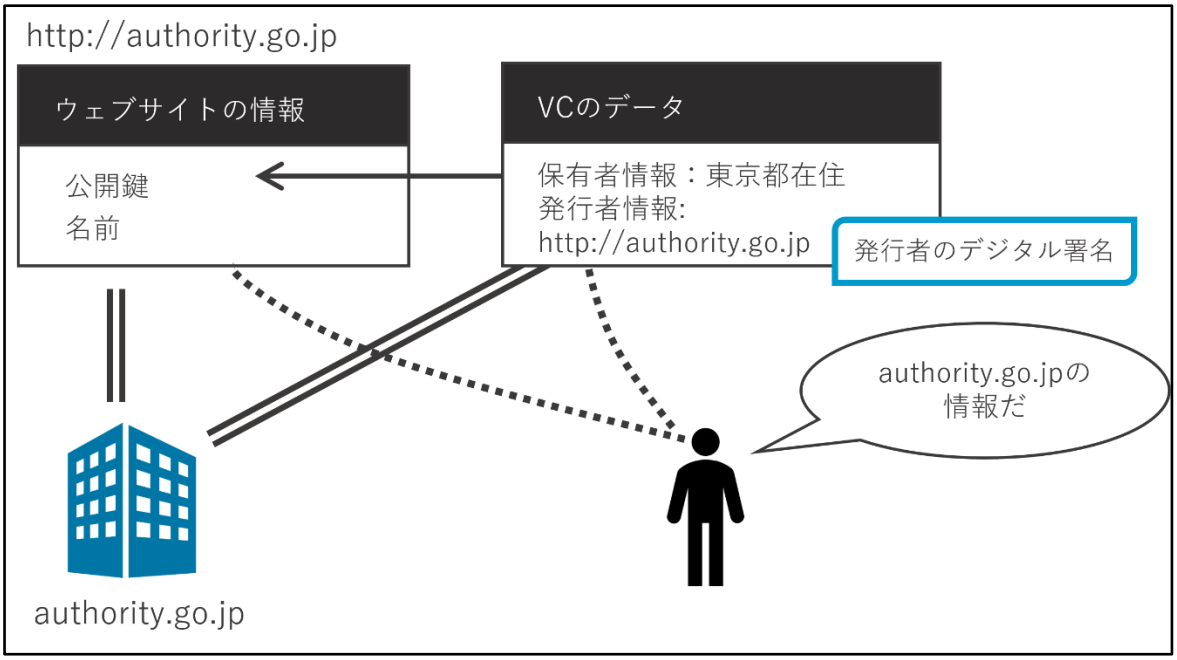
本節（2）では、VC に記載された発行者情報と発行者実体との紐づけについて述べる。発行者の紐づけ方法は、発行者により付与されたデジタル署名の検証のみである。発行者実体が作成した公開鍵を確実に入手することが紐づけの正

しさの確保につながる。

公開鍵の入手方法として、学術的には様々な方法が考案されている。例えば、X.509 の公開鍵証明書のように、信用できる第三者に発行者実体と公開鍵の対応関係を保証してもらう方法があるが、前述した通り、想定される用途が画一的かつ厳格な運用基準を満たす必要がある。他の方法として、発行者実体が責任をもって刊行する書籍などに公開鍵を掲示することも考えられる。

実用途でよく使われる方式は、URL を利用した紐づけである（図 6）。これは、本節（1）ニ．の方法と同ホ．の方法の組合せである。具体的には、VC の中に、発行者情報として発行者が排他的に利用するドメイン名を含む URL を記述しておき、その URL の参照先に発行者の公開鍵を格納しておく。この方法は前提として、URL に含まれるドメイン名を発行者実体が利用していることを検証者は予め知っている[17]必要がある。

図 6 URL による発行者の紐づけ



（3）VC 発行を委託する場合の留意点

VC を発行する技術力とノウハウがない企業にとって、発行業務を外部業者に委託する動機は強い。外部委託する場合には、発行者実体との紐づけを巡る落とし穴に注意を払う必要がある。

---

[17] 検証者が「ドメイン名を発行者実体が利用していることを知っている」状態は、ドメイン名を含む URL によるアクセス手段を提供することにより、発行者企業などが自社サービスを提供していることを経験的に知っている状態や、ドメイン名の登録情報を知っている状態を表す。

本節（2）では、発行者を紐づける手段としてURLの参照先に公開鍵を格納する方法を述べた。自組織が VC を発行する場合には、自組織のドメイン配下のURL 参照先に公開鍵を格納すればよい。これに対して、委託先業者が VC を代理発行する場合には、公開鍵の格納場所、および、公開鍵に対応する秘密鍵の実体的な管理者について注意深い検討を要する。

例えば、A 社の名義で VC が発行されるが、委託先業者 B が代理発行しているケースを考える。このとき、発行者情報として A 社の社名が書かれるが、公開鍵の在りかを参照するURLとしてB社のドメイン名がVCに記載されたとする。このケースでは、検証者は、VC に記載された URL から公開鍵を入手し、デジタル署名の検証も可能である。しかし、紐づけの正しさを確保する点で、以下のような3つの論点がある。

イ．なりすましの予防の検知

発行者としてVCに記載されているA社とは異なる組織が不正に発行したVCを検知するためには、検証手続きにおいて、公開鍵の格納領域を配下にもつドメイン名の登録者と発行者の社名が一致していることを確認する必要がある。ただし、上記の例のように、A 社の名義で委託先業者 B が VC を代理発行するようなケースもあるため、検証者にはこうした委託関係を予め知っていることが求められる。しかし、こうした前提を置くことは、多くの用途において現実的ではない[18]ことから、VC の発行を他社に委託する場合には、発行者実体との関係を検証者が認識できるような別途の仕組みが必要である。

ロ．ドメインの有効期限

A 社の公開鍵が委託先の B 社のドメインで管理される場合、委託先がそのドメインを管理する期間も重要なポイントである。紙の証明書では、証明書の検証に発行者の関与は基本的には不要である。他方、VC では、検証のたびに検証者が公開鍵を取得するための情報インフラを、発行者が継続的に提供し続けなければならない。

VC の用途が、被発行者にとって生涯有効となる卒業証書である場合には、何十年にもわたって検証用の環境を提供する必要が生じる。発行者（A 社）がこうした環境を提供することは実務上の重要な課題であるが、とくに、A 社が B 社に委託し、発行時に B 社のドメインを含む URL で公開鍵を提供する場合には、B 社のドメインを、A 社が責任をもって VC が利用される永きにわたって継続的

---

18 ドメイン名と企業実体との関係を認識する難しさは、適格な発信者と誤認させる紛らわしいメール・アドレスから発信されるフィッシング・メールに多くの人が騙されてしまう現状からも推察されるであろう。

に稼働させる必要がある。仮に、B 社がドメインを売却した場合には、発行済の VC が検証できなくなるおそれや、A 社名を騙った不正な VC が発行されるおそれがある。

ハ．秘密鍵の管理者

デジタル署名の作成に利用した秘密鍵の管理体制も重要な論点である。委託先が秘密鍵を管理する場合には、委託先の管理状況の適切性を、発行者が確認する必要がある。委託先が同一の秘密鍵（したがって、対応する公開鍵も同一）を用いて、複数の組織の VC を発行していた事例も報告されている[19]。このような秘密鍵の使いまわしを行うと、検証者は発行者を一意に特定することができなくなってしまう。

４．事例 1: 新型コロナウイルス感染症予防接種証明書

（１）概要

ワクチン証明書は、予防接種法に基づいて各市町村で実施された新型コロナワクチン接種の事実を公的に証明するものとして、被接種者からの申請に基づき発行されるものである[20]。

ワクチン証明書には、書面と電子証明書の 2 つの発行形態がある。このうち、電子証明書は、2 種類の国際規格に準拠したデータ・フォーマットで発行することが可能であり、その一つが VC を採用している SMART Health Cards である[21]。本稿では SMART Health Cards 規格に準拠した海外用について説明する。

（２）詳細

以下では、VC で表現されたワクチン証明書の詳細を項目別に記述する。各項目の記述を表 1 にまとめた。

---

19 2024 年「暗号と情報セキュリティシンポジウム（SCIS2024）」のナイト・セッションにおける報告。

20 https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/vaccine_certificate.html

21 SMART Health Cards は、民間 IT 企業の共同プロジェクト「VCI」が策定した健康証明書用の規格であり、国内用と海外用の両方のワクチン証明書で採用されている。もうひとつの国際規格は ICAO VDS-NC であり、海外用のワクチン証明書のみで採用されている。

表 1 ワクチン証明書の仕様

証明内容	対象に関するワクチン接種記録（接種年月日、ワクチンの種類・製品名・ロット番号など）
利用目的	海外での入国審査（パスポートとともにワクチン証明書を提示）、またはレストランへの入店
持ち主との紐づけ	VC 記載の対象の氏名 VC 記載のパスポート番号
発行者	厚生労働省
発行者の公開鍵	デジタル庁のドメイン配下の領域に格納
発行方法	マイナンバー・カードによる本人確認とパスポートの所有確認後、VC が政府のサーバから発行される。
VC 提示方法	アプリが QR コード形式で VC（属性情報、デジタル署名）を提示
検証方法	QR コードから読みだした VC のデジタル署名を上記の公開鍵で検証。検証が成功し、VC 記載の識別子のパスポートを対象が所持していれば、VC 記載の接種実績を受理する。

イ．証明内容

対象が接種したワクチンの種類や接種日時などの接種記録が含まれる。

ロ．利用目的

入国審査にあたり、海外用のワクチン証明書をパスポートとともに提示するほか、レストランなどワクチン接種証明が求められる場面で提示する。

ハ．発行者

ワクチン証明書に記載されている発行者は厚生労働省である。これは、ワクチン証明書の属性情報が、同省が管理するワクチン接種記録に基づくためである。

ニ．発行者の公開鍵と紐づけ

ワクチン証明書では、発行者を特定する識別子として、デジタル庁のドメイン名を含む URL が指定されている。この URL の参照先から署名検証用の公開鍵を入手することにより、検証者は発行者実体（デジタル庁）とワクチン証明書を紐づけることができる。ここで、デジタル庁のドメイン名 digital.go.jp を含む URL の参照先として公開鍵を自由に格納できる主体はデジタル庁しかいないことか

ら、この公開鍵が厚生労働省を含む政府のものであると確認できる[22]。この紐づけ方法は、3 節（2）で解説したとおりである。また、3 節（3）で述べた委託の落とし穴も回避されている点に留意されたい。

ホ．発行方法

ワクチン証明書の発行を希望する利用者は、まず、専用のスマートフォン・アプリをダウンロードし、マイナンバー・カードでログインおよび認証する[23]。アプリは、利用者が提示するパスポートを読み取り、そのパスポートに記載された個人名が、マイナンバー・カードの所有者に合致することを確認する。この照合が成功すると、利用者の接種記録がパスポート番号とともに記載されたワクチン証明書が VC として発行される。ワクチン証明書のデータはアプリ内に保存される。

このように、ワクチン証明書は、政府が配布する専用のスマートフォン・アプリによってのみ、発行の依頼および取得が可能である。

ヘ．提示方法

利用者は、専用アプリを起動して、ワクチン証明書の表示画面を検証者に提示する。表示画面には、ワクチン証明書に記載された属性情報と、ワクチン証明書を VC としてダウンロードできる QR コードが表示される。

なお、ワクチン証明書の表示画面には、属性情報とともに、時々刻々と変化する現在時刻が外縁部に表示される。この工夫は、過去に生成された他人のワクチン証明書のスクリーンショット等を提示することによる接種実績の詐称を、ある程度抑止すると見込まれる。また、この QR コードは、VP ではなく、ワクチン証明書の VC そのものである。

このように、ワクチン証明書は、政府が配布した専用のスマートフォン・アプリによってのみ提示されることが想定されている。

ト．検証方法

検証者は、提示された QR コードからワクチン証明書を VC としてダウンロードし、デジタル署名を入手する。ワクチン証明書には、対象を特定する氏名とパスポート番号が識別子として記載されている。対象との紐づけは、対象が所持するパスポートに記載されている氏名やパスポート番号などによって行われる。この紐づけの方法は、3 節（1）ロ．に相当する。

---

22 検証者は digital.go.jp がデジタル庁のドメインであることを知っていることが前提となる。

23 マイナンバー・カードは本人のみによって所持され、電子証明書の発行に必要な暗証番号も本人によって適切に管理されていることが前提である。

次に、本節（2）ニ．の方法により、政府の公開鍵を用いてデジタル署名を検証する。デジタル署名の正当性が確認できれば、対象との紐づけ確認のうえ、接種記録を受理することが想定されている。

５．事例 2: 資格証明書（Open Badge)

近年、オンラインで入学審査や就職審査が実施される場面が増えており、審査の際に提出されたデジタル・データの卒業証書や資格証明書が真正であることを確認するニーズが高まっている。もっとも、紙の証明書をスキャンした画像データから、証明書の偽造を検出することは困難であるため、検証可能性を持つデータ形式で発行された証明書が求められている。

デジタル・データの資格証明書の規格として、1EdTech が標準化している Open Badge が知られている。2 節（4）で述べたように、Open Badge には様々なバージョンがある。また、Hyland Credentials 社は、発行された Open Badge に関連する情報（ハッシュ値）をブロックチェーンに埋め込むプロセスを加えて改ざん耐性を持たせることにより、資格証明書の証拠性を補強する Blockcerts という方式を公開している。情報処理学会やデジタル庁など多くの組織も Open Badge v2 に Blockcerts を組み合わせた Open Badge を発行している。執筆時点（2024 年 3 月）で策定中の最新の Open Badge v3 は、VC の規格に準拠しており、千葉工業大学が規格策定に先立って卒業証書の発行に利用している [24]。

本節では、（1）Open Badge v2 の Hosted Badge、（2）Open Badge v2 に Blockcerts を組み合わせたもの、（3）Open Badge v3 の 3 種類について述べる（表 2）。これらのうち、（1）と（2）については、VC を利用していない。

表 2 Open Badge の概要

	Open Badge v2 Hosted Badge	Open Badge v2 + Blockcerts	Open Badge v3（執筆時点 2024 年 3 月の情報に基づく）
証明の内容	対象が資格を保有していること		
利用目的	求職や受験などに際して資格を提示すること （卒業証明書、TOEIC 結果、各種資格証明）		
持ち主との紐づけ	Open Badge に記載された対象の氏名、メール・アドレス、顔写真など		左記に加えて、持ち主の公開鍵の記載も検討中
発行者	資格発行者		

[24] 詳細はプレス・リリースを参照されたい（https://www.it-chiba.ac.jp/media/pr20220818.pdf）。

発行者の公開鍵	なし（発行者は署名しない）	ブロックチェーン・トランザクションの署名を検証する公開鍵を URL で指定	URL の他、分散型デジタル・アイデンティティ（Decentralized Identity）による特定も検討中
発行方法	対象のメール・アドレスに証明書ダウンロード用の URL を送付	Open Badge に、ブロックチェーン上の埋め込み位置と発行者のブロックチェーン用の公開鍵の情報を追記した JSON ファイルを作成し、保有者に送付。発行および送付方法は左記と同じ	未定
提示方法	Open Badge の JSON ファイルを共有		VP が活用される見込み
検証方法	Open Badge の JSON ファイルに記載された URL 参照先から、資格証明書の「原本」を入手し、その証明事項を受理する	ブロックチェーン上に Open Badge 記載のデータが埋め込まれており、かつ、そのデータに発行者のデジタル署名が付与されていることを検証	VP を検証する見込み

（１）Open Badge v2

イ．概要

Hosted Badge として発行される Open Badge v2 は、記載された対象が資格保有者であることを証明する目的で、資格発行者により発行される。Open Badge は卒業証明書や検定結果などを求職時や受験時に電子的に添付するような利用方法が想定されている。

検証者である Open Badge の受取側は、添付された Open Badge が、偽造または改ざんされておらず、正当な発行者により発行されたことを検証する。そのために、検証者は、Open Badge に記載された URL の参照先から、資格証明書の原本データを入手する。発行者により管理されているこの原本データを参照することにより、検証者は対象が資格保有者であることを確認できる。本節（1）では、ある学会が発行する Hosted Badge 型 Open Badge の事例[7]を紹介する。

ロ．発行者

発行者は学会である。

ハ．発行者の公開鍵

Hosted Badge は、公開鍵を利用しない。

ニ．発行方法

学会が発行する Open Badge では、発行時の対象実体との紐づけを対象の氏名

とメール・アドレスで行う。発行者は、このメール・アドレスに向けて、発行済の Open Badge をダウンロードできる URL を送る。この手続きにより、メール・アドレスを管理している対象実体だけが、Open Badge を入手できると想定している[25]。

Open Badge の記述には、対象を特定する情報（氏名、メール・アドレスなど）、および、対象に付与された資格、資格付与日などの属性情報が含まれる。さらに、資格を発行した組織名と原本データの所在を参照する URL も Open Badge に記載される。これらの情報を合わせた Open Badge が、JSON 形式の電子ファイルとして発行される。資格保有者である対象は、自身のメール・アドレスに送付された証明書ダウンロード用の URL から Open Badge（すなわち、JSON ファイル）を入手する。

ホ．提示方法

対象が資格保有者であることを第三者（検証者）に証明したい場合には、前述の JSON ファイルを検証者に提示する。

ヘ．検証方法

JSON ファイルを提示された第三者（検証者）は、JSON ファイルに記載された URL から、資格証明書の原本データを入手し、これを表示して目視で資格情報を確認する。持ち主との紐づけは、3 節（1）イ．の「検証者にとって既知の識別子による紐づけ」に相当する。

（２）Open Badge v2 の Blockcerts 補強版

イ．概要

本節（1）で述べた Hosted Badge 型の Open Badge v2 は、発行者が管理する原本データを参照することにより、検証者が対象の資格情報を確認するものであった。しかし、発行者が悪意を持って原本データを書き換えてしまうと、改ざんの事実を検出することができない。また、この方法では、発行者が原本データを参照するサービスが停止すると Open Badge も検証できなくなってしまう。

この問題に対処するため、ブロックチェーンに Open Badge に関連する情報を埋め込むプロセスを加えることにより、資格情報の証拠性を補強する Blockcerts

[25] なお、必ずしも発行者および検証者が持ち主の正しいメール・アドレスを知っているとは限らないので、発行および検証の手続きにおいて、紐づけの効果は限定的であると思われる。

という方式が公開されている。この補強版を、本稿では便宜上 Blockcerts Open Badge と呼ぶことにする。

Blockcerts Open Badge では、ブロックチェーンに Open Badge に関連する情報（ハッシュ値[26]）が埋め込まれ、その関連情報に発行者のデジタル署名が付与[27]される。Open Badge には、このデジタル署名を検証するための公開鍵の格納場所を参照する URL が記載される。検証者は、発行者が管理する原本データを参照できずとも、提示された JSON ファイルとブロックチェーン上の関連情報から、Open Badge が発行者によって発行され、偽造または改ざんがなされていないことを確認できる。また、発行者が悪意をもって原本データを改ざんした場合にも、検証者と対象は改ざんを検知できる。この意味において、資格情報の証拠性が補強されているといえる。

本節（1）で紹介した学会が発行する Open Badge にもこの補強がなされているため、以下ではこの例を紹介する。

ロ．発行者

発行者は、学会である。

ハ．発行者の公開鍵

ブロックチェーンのトランザクション・データに発行者のデジタル署名が付与される。そのデジタル署名を検証するための発行者の公開鍵の格納場所として、Open Badge の中に URL が掲載される。

ニ．発行方法

Hosted Badge と同様に、発行時の対象実体との紐づけは、対象の氏名とメール・アドレスで行う。

Blockcerts Open Badge には、Open Badge v2 に掲載される内容と同様の情報が含まれる。すなわち、対象を特定する情報（氏名やメール・アドレスなど）、対象の属性情報（対象に付与された資格、資格付与日）、資格を付与した組織名、原本データの所在を参照する URL などである。これに加えて、ブロックチェーン上にハッシュ値（の合算値）が掲載されているトランザクションの識別情報、

---

26 ブロックチェーンに Open Badge のデータそのものではなく、ハッシュ値を掲載する理由は、プライバシーへの配慮と、ブロックチェーンへの掲載の手数料の節約である。なお、個々の Open Badge のハッシュ値ではなく、複数の Open Badge ハッシュ値の合算値がトランザクション・データに掲載される。

27 ブロックチェーンの仕様により、トランザクションには発行者のデジタル署名が付与される。

合算に使われたその他のハッシュ値の情報、発行者のブロックチェーン用の公開鍵の情報が追記されている。これらの情報を記した JSON ファイルが資格証明書として発行される。

対象は、自身のメール・アドレスに送付される URL から資格証明書ダウンロード用のウェブ・サイトに接続し、Blockcerts Open Badge を入手する。

ホ．提示方法

対象が資格保有者であることを第三者（検証者）に提示したい場合には、前述の JSON ファイルを検証者に提示する。

ヘ．検証方法

JSON ファイルを提示された第三者（検証者）は、JSON ファイルに記載された URL の参照先から、資格証明書の原本データを入手し、資格証明書の内容を確認する。さらに、提示された Open Badge のデータから計算したハッシュ値（の合算値）と、ブロックチェーンに掲載されているハッシュ値（の合算値）を照合する。最後に、そのトランザクション・データに掲載された発行者のデジタル署名を検証する。これにより、正しい発行者により発行され、証明書が偽造または改ざんされていないことを確認できる。持ち主との紐づけは、3 節（1）イ.の「検証者にとって既知の識別子による紐づけ」に相当する。

（３）Open Badge v3

1EdTech は Open Badge v3 の仕様として、従来の独自のフォーマットではなく、W3C が策定した VC の仕様に基づくものを策定中である。執筆時点（2024 年 3 月）においては、仕様が確定していないため公開されている実装例もないが、類推した仕様を表 2（本節冒頭を参照）に記す[28]。

Open Badge v2、および Blockcerts Open Badge では、検証サーバの存在が不可欠であったが、VC の仕様を採用することにより、検証サーバやブロックチェーンにアクセスすることなく、検証者は VC を検証することが可能になる。

６．VC の実活用の展望と留意点

金融分野を始めとして、さまざまな産業分野においても、VC を有効に活用する余地があると期待される。以下に、VC が有用となりうる用途について、金融分野を中心に例示を試みる。

---

[28] Open Badge v3 の正式な仕様が 2024 年 5 月にリリースされた。詳しくは、以下の URL を参照。https://www.imsglobal.org/spec/ob/v3p0

① 金融機関が発行する各種証明書（例えば、取引証明書、振込証明書、口座残高証明書、預金入出金取引証明書）を VC で発行することが考えられる。これにより、VC の受領者はウェブ画面のスクリーンショットや、紙の証明書のスキャン・データよりも信頼性の高い形でオンラインの各種申請に利用できる。VC は、発行時からデジタル・データであるため転記が容易である。また、記述の正しさを第三者が検証できるため事務ミスの予防に役立つ。さらに、VC に記載する属性情報の規格が統一されていれば、金融機関ごとに異なる書面の様式に対処することが不要となる。

② 月次のクレジット・カード明細書を VC で発行することも考えられる。VC で実現できる選択的開示の機能を使うことにより、明細書の中で、必要な決済取引履歴のみを開示することにより、他の取引を伏せたまま組織内の経理処理に活用できる。

③ 金融機関側が VC の提示を受ける例としては、口座開設の申込者が金融機関に提示する本人確認のための資格情報を VC により提示する手続きが考えられる。

④ 決済事業においては、暗号資産・電子決済手段について取引経路の追跡を可能にするため、トラベル・ルールが FATF（金融活動作業部会）により導入された。このルールは、利用者の依頼を受けて暗号資産や資金を送付する側の暗号資産交換業者・電子決済手段等取引業者に対して、送付人・受取人に関する情報の受取側事業者への通知を義務づけたものである。この制度変更への対応においても、VC の活用により通知義務にかかる事務コストを軽減できる可能性がある。

⑤ メールのなりすましと改ざんの検知に VC を活用できる。金融機関や公的組織などになりすましたフィッシング・メールによる金融犯罪の被害が拡大するなか、メールにデジタル署名を付与する DKIM（Domain Keys Identified Mail）を導入する機運が高まっている[29]。

---

[29] フィッシング・メール対策として、送信者ドメインを認証する電子メールの認証プロトコルである DMARC（Domain-based Message Authentication Reporting and Conformance、RFC7489）を導入する機運が高まっている。DMARC は、送信者ドメインを認証する技術の標準である SPF（Sender Policy Framework）と DKIM をベースにしている。

なお、DKIM の運用においても、メールの送信元実体を特定して適格性を確認し、デジタル署名検証用の公開鍵を安全に取り込む仕組みが必要となる。このため、デジタル署名の発行者情報とその実体との紐づけにおける正確性確保が課題となる。

⑥ メディアが責任をもって発信する情報にVCを付与することにより、ニュースなどの信頼性の担保やフェイク・ニュース対策に活用できる。

⑦ 人口減少を迎えているわが国において、海外からの実習生を受け入れる場合に、VCを用いた実習生の経歴確認や、日本で蓄積した実績の保証に活用することも一案である[30]。

以上の用途は、あくまでVCの利用可能性を模索するための例示に過ぎないが、いずれの用途についても、エンティティとの紐づけにおける正確性確保の問題が残存している点には注意が必要である。この問題への対処を誤ると、デジタル署名とその検証枠組みが暗号学的に頑健であったとしても、なりすまし攻撃などへの脆弱性をもたらすおそれがある。

とくに、金融機関がVCを発行するケースでは、金融機関が行う本人確認における紐づけが正確性の源泉となるが、残余リスクもある。例えば、VCの発行時にライブ・カメラによるeKYCを組み合わせて本人を認証する場合には、eKYCがディープ・フェイク等の深層学習を悪用してなりすませる余地が残る。攻撃者の能力や攻撃コスト、対策の効果とコストを比較衡量しながら、金融機関が対応することが求められるであろう。

７．結語

デジタル情報と実世界の存在（実体）との紐づけを、実体に関して知りうる情報に限りがある第三者（検証者）が正しく行うことは容易ではない。この問題への対処は、高い信頼性を要する用途にも適したVCにおいて顕著に求められる。すなわち、VCの技術的本質はデジタル署名に過ぎず、デジタル署名が何らかの属性情報の証明書として機能するには、属性情報に加えて紐づけの正確性を担保するための適切な運用が必要となる。現時点では、この課題の完全な解決には至っておらず、目的や用途に応じて必要となる正確性を確保できるよう、さまざまな紐づけの仕組みが模索されている状況である。

本稿で紹介したとおり、VCは、ワクチン証明書や卒業証明書を始めとして、社会で信頼できるデジタル情報の伝達手段としてすでに活用されている。金融分野においてもVCの活用余地は大きいと期待される。金融機関がVCを発行する場合と、第三者が発行したVCを金融機関が検証する場合が考えられ、活用形態に応じて必要となる取組みは異なるであろうが、正確性確保のために、落とし穴に陥らず適切な仕組みを構築運用していくことの重要性は不変である。

---

30 このような適用例については、内閣官房・デジタル庁が実施している「令和4年度補正 Trusted Web 開発等推進事業に係る調査研究 Trusted Web ユースケース実証事業」[8]でも様々検討されている。

紐づけにおける正確性確保の課題に対して一定の解決策が見いだされ、各種証明書が紙と同等の安全性で電子的に発行されてインターネットで相互に受渡しできるようになれば、社会生活の利便性が向上することが期待される。将来、VC がより身近なものとなれば、より正確な情報の流通に寄与し、健全な社会に貢献できるものと考えている。

以　　上

参考文献

[1] 佐古和恵、「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～」、金融研究所ディスカッション・ペーパーNo.2023-J-8、日本銀行金融研究所、2023 年

[2] 1EdTech, “IMS Open Badges Home” (https://openbadges.org/、2024 年 3 月 4 日).

[3] Blockcerts, “About Blockcerts” (https://www.blockcerts.org/about.html、2024 年 3 月 4 日).

[4] W3C, “Verifiable Credentials Data Model v1.1,” W3C Recommendation, 2022 (https://www.w3.org/TR/vc-data-model/、2024 年 3 月 6 日).

[5] 1EdTech, “Badge Count 2022” (https://content.1edtech.org/badge-count-2022/、2024 年 3 月 4 日).

[6] Yamamoto, Dan, Yuji Suga, Kazue Sako, “Formalising Linked-Data Based Verifiable Credentials for Selective Disclosure” 2022 Security Standardisation Research Conference (SSR 2022), *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2022, pp. 52-65.

[7] 福田岐弦・水野重弦・渡邉　健・佐古和恵・寺田雅之・吉濱佐知子、「Blockcert OpenBadge 証明書に関する仕組みと考察」、第 103 回コンピュータセキュリティ研究会（CSEC 研究会）、2023

[8] みずほリサーチ&テクノロジーズ株式会社・ＳＢＩホールディングス株式会社・Originator Profile 技術研究組合・株式会社 DataSign、富士通 Japan 株式会社・株式会社 PitPa・株式会社電通国際情報サービス・Institution for a Global Society 株式会社・シミック株式会社・株式会社 ORPHE・一般社団法人情報サービス産業協会・大日本印刷株式会社「令和 4 年度補正 Trusted Web 開発等推進事業に係る調査研究　Trusted Web　ユースケース実証事業」、中間報告会資料、2024 年（https://www.toppan.com/ja/joho/social/trusted_web2023_koubo.html、2024 年 3 月 4 日）

[9] 富士榮尚寛、「分散型 ID と OpenID Foundation の活動概要」（ https://speakerdeck.com/fujie/fen-san-xing-idtoopenid-foundationnohuo-dong-gai-yao、2024 年 3 月 4 日).

補論 VC の標準化動向

VC をどのように表現し、どのようにやりとりするかについては、さまざまな標準化団体が標準化を進めている。富士榮 [9]を参考に、本稿に関係する VC の標準化動向を表 3 にまとめた。

表 3 関連標準

キーワード	技術仕様	策定団体	ステータス
データモデル	Verifiable Credentials Data Model v1.1	W3C	勧告
	Verifiable Credentials Data Model v2.0	W3C	策定中
証明	Data Integrity 1.0	W3C	CG Report
	JSON Web Proof	IETF	策定中
署名形式	JSON Web Signature	IETF	RFC
署名アルゴリズム	The BBS Signature Scheme	IETF	策定中
オブジェクト形式	JSON (JavaScript Object Notation)	IETF	RFC
	JSON－LD (JSON for Linked Data)	W3C	勧告
選択開示	Selective Disclosure for JWTs (SD-JWT)	IETF	策定中
	BBS　CryptoSuite v2020	W3C	策定中
プロトコル	OpenID for Verifiable Credential Issuance	OpenID Foundation	策定中
	OpenID for Verifiable Presentations	OpenID Foundation	策定中

W3C は、W3C Data Model として、オブジェクト形式 JSON-LD に基づいたデータ・フォーマットを規定している。最新の確定版はバージョン 1.1（v1.1）で、現在バージョン 2.0（v2.0）を策定中である。このフォーマットで記載される基本的な要素は、発行者（Issuer）、属性情報の記述（Claim）、その記述に対応する証明である。記述（Claim）には、対象（Subject）とその人がもつと宣言する属性（Attribute）が記載される。

なお、W3C Data Model では、発行者や対象をどう記述するか、また証明をどう生成するかについては規定しない。これらの記述方法、生成方法は別に標準化されているものを用いる。

証明に関しては、VC に付与する証明と、VP に付与する証明がある。VC に付与する証明は、発行者が全体に対してデジタル署名を付与する単純な証明であることが多い。一方で VP に付与する証明は、検証者が求める証明内容に基づいて、選択開示をした結果が正しいことを証明したり、署名者が異なる複数の VC から証明を導出したりするなど、複雑なものを含む場合がある。JSON-LD に基

づいた証明の記述方法は W3C の Data Integrity[31]で、JSON Web Token に基づいたものは IETF[32]の JSON Web Proof[33]で策定中である。署名形式に関しては JWS（JSON Web Signature）が IETF で策定されている。

上記の標準は、それぞれデジタル署名や証明にかかる記述方法の仕様を策定するものであり、署名アルゴリズムは別の標準で規定されている。RSA、ECDSA、EdDSA（Edward curve を用いた楕円曲線版 Schnorr 署名）などは IETF で規定されており、BBS 署名の標準化も開始されている[34]。

また、選択的開示の仕様は、IETF において任意の署名アルゴリズムに対応する SD-JWT と、W3C において JSON-LD 形式で BBS 署名に特化したプロジェクトがそれぞれ進行している。上述の IETF の JSON Web Proof でも検討されている。

上記は、主に VC や VP の記述方法についての標準であるが、これらの発行と提示のプロトコルの標準化は、IETF や W3C ではなく、OpenID Foundation[35]において策定が開始されている。具体的には、発行に関しては OpenID4VCI（OpenID for Verifiable Credential Issuance）と、OpenID4VP（OpenID for Verifiable Presentation）が策定されている。

---

31 https://www.w3.org/TR/vc-data-integrity/

32 IETF（Internet Engineering Task Force）は、インターネット技術の標準化を推進する非営利団体。IETF が策定した文書は、RFC（Request for Comments）として付番・公表される。

33 https://github.com/json-web-proofs/json-web-proofs,
https://www.ietf.org/archive/id/draft-jmiller-jose-json-web-proof-00.html

34 従来、BBS 論文に書かれていた方式を改良したものを BBS+署名と呼んでいたが、2023 年の論文で、当初の BBS 論文のままでも安全な署名方式であることが証明され、その後、BBS 署名と呼ばれることになった。

35 Open ID Foundation は、インターネット上のアイデンティティおよび API アクセス管理に関わる技術の標準化を目指す非営利団体。