O-005

Verifiable Credentials に基づく DID の信頼性確保と関係性取得によって形成するレビューシステム

A Review System Formed by Ensuring the Trustworthiness of DID and Acquiring Relationships Based on Verifiable Credentials

出合 祐喜 †　和崎 克己 ††
Yuki Deai　Katsumi Wasaki

1　はじめに

現在、レビューのような評価システムは信頼性の欠如が大きな課題となっている。特に、アカウントを大量に作成し評価の操作を行うサクラレビューや、対立している相手に不正確な情報を投稿する中傷的レビュー等が問題となっており様々なレビューサイトにおいて被害が確認されている [1]。しかし、このようなレビューを第三者が正当な主体が作成したものか、正しい情報であるかを検証する手段について既存対策はあるが十分ではなく、確認することは難しい。こうした背景を踏まえ、デジタル上で資格情報を検証可能な状態で保有、提示できる Verifiable Credentials（VC）を活用することで、レビューの信頼性を向上させる手法を提案する。本提案では、レビューを行う側・レビューされる側 (以降：レビュー者・被レビュー者）との関係性を VC を用いることで明確にし、レビュー閲覧時にその関係性を確認できる仕組みを構築する。こうすることで関係性を持たない者によるレビューを排除することができ、不正に作成されたアカウント・レビューを見分けることが可能となる。

2　背景技術

2.1　Verifiable Credentials（VC）

VC は検証可能な資格情報を意味し、卒業証書や診察記録等の資格情報を安全かつ信頼性を保ったままデジタル上で扱える仕組みとなる [2]。その原理について、VC は 3 つの主体の相互作用により運用される。このような VC のやり取りの構造と各主体の役割を、図 1 に示す。第一の主体は Issuer（発行者）で、これは VC を発行するものを指し資格情報等のデジタルデータの付与や、そのデータが正しいことを保証する。第二の主体は Holder（保持者）で、VC を受け取り管理するものを指し、VC の管理・保持・選択的な共有を行う。第三の主体は Verifier（検証者）で、VC を確認する第三者を指し、VC を受け取り検証を通してその正当性を確認する。図中に現れる DID（Decentralized Identity）については次節にて説明する。また、スキーマ（Schema）とは、VC の構造や属性等を定義するテンプレートのような役割を持ち、これにより発行者と検証者の間で VC について共通の理解を得られる。結果、検証者はスキーマから検証のルールを知ることができ、VC が適切な属性を持っているか、内容の整合性が担保されているか等を確認することが出来る。

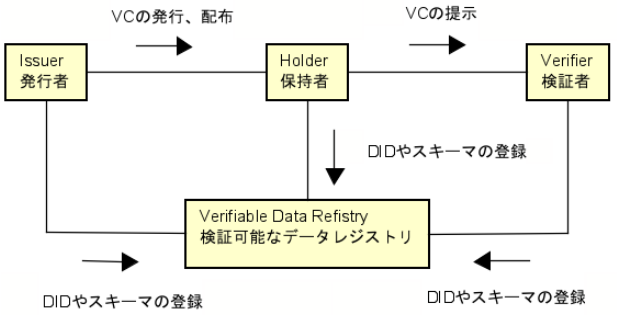

図 1　Verifiable Credentials の構造 [2]

2.2　Decentralized Identity（DID）

DID とは自己主権型の識別子を指す。従来の ID は ID の管理、発行を企業や政府等の中央集権的な機関が行っていたのに対し、DID はブロックチェーン等の分散台帳技術を用いることで、ID をユーザー自身が生成・管理できる（ブロックチェーンを用いらない手法もある）[2]。DID は VC を活用する上で重要な役割を果たす。VC は発行者・保持者・検証者によって構成されているが、検証者に信頼性が十分に高いことを検証するためにはそれぞれの関係者を一意かつ検証可能に識別できる手段が必要となる。この識別手段として DID を用いることにより、それぞれの関係者は固有の識別子を作成・保有することが可能となり、DID を基に互いに VC の正当性を証明し合うことが可能になる。また、DID は個人や組織が完全に自己管理できるため、自身の VC を安全かつ選択的に管理・共有できる。結果、プライバシーを保護しながら信頼性の高い情報を受け渡しを実現できる。

2.3　Universal Profiles（UP）

本研究では、レビュー者と被レビュー者の関係性を示すため DID と VC を安全かつ選択的に管理できる仕組みが必要である。そこで、LUKSO（Ethereum 互換のブロックチェーン）上で DID に紐づけて VC や NFT といった資産を管理できるスマートコントラクトシステム、Universal Profiles(UP)[3] を採用する。UP は、ERC725（VC を含むメタデータを管理）や ERC20（トークン管理）等の標準規格を用いることで安全に資産を保存、動的に管理することを可能にしている [3]。DID と VC を一元管理でき、資産を選択的に呼び出しや共有、検証することが可能という UP の特徴は提案システムの要件に合致しており、基盤として適切である。

† 信州大学大学院総合理工学研究科, Graduate School of Science and Technology, Shinshu University.
†† 信州大学工学部電子情報システム工学科, Department of Electrical and Computer Engineering, Faculty of Engineering, Shinshu University.

3　レビューシステムの提案

3.1　関係性の導入による第三者証明可能性

関係性の取得方法については、DID とそれに紐づく VC を使って行う。前のセクションで述べたように DID と VC を活用することで資格情報を信頼できる形で第三者に証明することができる。例えば大学内での関係について、被レビュー者の DID からレビュー者と関係がある自身の VC（「被レビュー者：学生」と「レビュー者：教員」であれば学生証 VC 等）をレビュー者に一部共有して、レビュー者はレビュー本文と受け取った VC と自身の VC を比較し記録する。結果、第三者がレビューを確認する際、レビュー本文の信頼性をレビューに付与された VC の正当性を検証することで評価することができる。この仕組みにより、中傷的レビューやサクラレビュー目的で作成された不正なアカウントは信頼性の高い VC を持つことが難しく、検証の突破を困難にしている。また、VC から一致する情報を比較することで関係性の深さをある程度取得することが可能でありレビューの正確性、信頼性をさらに補強することが可能である。

3.2　レビューシステムの例

関係性の導入に基づくレビューシステムの例として、図 2 に人事選考時のフローを示す。レビュー作成から提出・検証に至るまでの一連の流れと各主体の役割を整理している。以下は就職活動の学生採用時の要件調査フローの各ステップである。

■選考情報から必要なレビュー確認（被レビュー者） 選考先が求めているレビューの関係性（先生やインターンの担当等）を調査する。

■レビューの要件提示（選考先）　提出が求められるレビュー内容と、レビュー作成者の VC 要件を提示する。

■レビュー依頼（被レビュー者）　要件に合う人にレビューを依頼する。その際、自身の VC から関係性取得に必要ない情報を隠し、所属や署名情報等必要最低限の情報を共有する。

■レビュー作成（レビュー者）　被レビュー者の人柄や行動について記述し、関係性のある VC（○○大学、××研究室、入学日、卒業日等）を付与してレビューと VC 情報をブロックチェーンに保存する。自身の VC、レビューを選考先の公開鍵で暗号化する。

■レビュー提出（被レビュー者）　必要な情報をまとめて選考先に提出する。自身の VC を選考先の公開鍵で暗号化する。

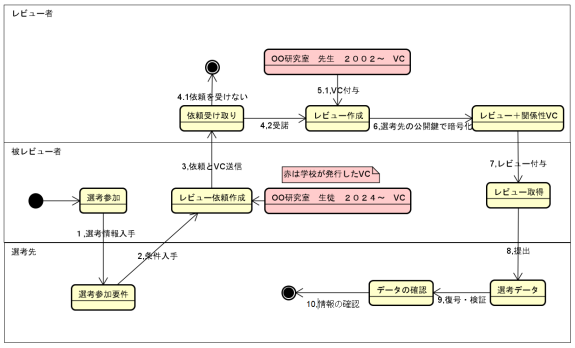

図 2　レビュー生成～検証及び人事選考・要件調査フロー

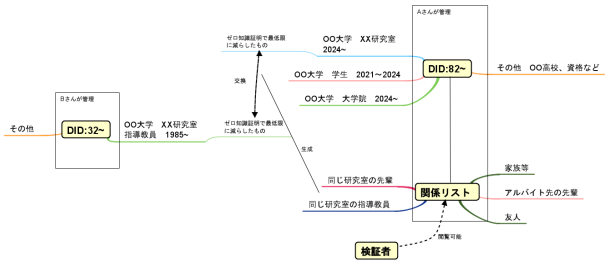

図 3　ZKP を用いて作成した関係性リストの概念図

■ レビュー検証（選考先）　レビュー、VC を復号し、ブロックチェーンで検証する。

4　関係性リストについて

レビューの信頼性を確保する手段の一つとしてレビュー者の DID に信頼できる VC が複数あるかを確認する方法がある。しかし VC の公開は個人の特定や悪用のリスクがある。それらを解決するため「関係性リスト（図 3）」を検討している。関係性リストとは、身近な関係性を持つ個人や組織と ZKP（ゼロ知識証明：ある情報の真偽を、内容を明かさずに証明する手法 [4]）を利用して VC から最低限の情報を交換し、例えば同じ大学、同じ研究室、一定期間同じ所属等の情報を第三者に証明する。関係性リストの証明とともに、一部の情報の秘匿機能も併せ持つことで、その DID が持つ関係性を一覧表示できる仕組みである。これは少ない情報から信頼できる関係性を示せるため個人を特定されるリスクが低く、悪用することが難しくなる。DID に紐づく関係性を部分的に公開していくことにより、信頼できる機関が発行した VC 同士の関係性が一定数あれば DID を信頼する等、DID の信頼を得る手段としての活用が考えられる。

5　まとめと今後の課題について

本研究は、DID と VC を組み合わせてレビューを第三者が検証できる枠組みを提示し、不正レビューによる信頼性の低下を技術的に克服する手法を提案した。これにより、既存課題の克服や、人事選考のような高い信頼性を必要とするレビューの実現を見出した。今後の課題としては、VC に含まれる個人情報の扱いや関係性リストの精査がある。前者については、関係性を示すために秘匿する情報、開示する情報を制定しシステムの枠組みを整備する必要がある。後者については、関係性リストの生成や発行、失効等についてより詳細に定義し、安全なモデルを構築及びレビューシステムへの活用を目指す。

参考文献

[1] 小久保 重信「はびこる偽レビュー業者、アマゾンが 1 万件超を提訴ー消費者欺くフェイク評価で金銭授受」『JBpress / Japan Innovation Review』2022-07-21. https://jbpress.ismedia.jp/articles/-/71067(June 2025)

[2] W3C, Verifiable Credentials Data Model v2.0 https://www.w3.org/TR/vc-data-model-2.0/ (June 2025)

[3] Universal Profiles, LUKSO Developer Docshttps://docs.lukso.tech/learn/overview (June 2025)

[4] ZK-SNARK: Definition & How It' s Used (Investopedia, 2024 改訂) https://www.investopedia.com/terms/z/zksnark.asp?utm_source=chatgpt.com(June 2025)