O-006

署名された複数のアクティビティに基づく Verifiable Credentials の発行・検証プロセスの枠組み

A Framework for Verifiable Credentials Issuance and Verification Process Based on Multiple Signed Activities

石坂 匠 †　　和﨑 克己 ††
Takumi Ishizaka　Katsumi Wasaki

1　はじめに

Verifiable Credentials(VCs) とは，検証可能な資格証明のことであり，特定の発行者によって Claim が示されたことを証明できるものである．現状、VC について W3C による規約やそれに基づくサービスが存在しているが，VC が発行される根拠や過程については不透明なものが多い．例えば，教育現場で VC を活用する場合，学生の評価が教員によって発行されたことを VC で保証することが可能になっても，その VC の内容は個々の教員の信頼性に依存しており，内容の検証までは外部から行うことができない．プライバシーの観点から根拠となる情報をそのまま開示することも望ましくない．このように，現状では VC に記された評価や判定について，内容の正しさを保証することが難しい．本研究では，複数の活動記録を根拠として VC を発行する仕組みや，その検証方法について提案する．ブロックチェーン技術や暗号技術を用いることで，改ざんや情報漏洩を防ぎつつこの仕組みを実現する。主に教育機関での利用を想定し、成績評価や修了証発行のプロセスをプライバシーに配慮しつつより信頼性の高いものにする。

2　Verifiable Credentials

2.1　Verifiable Credentials とは

Verifiable Credentials とはオンライン上で検証可能なデジタルな証明書のことである [1]．通常，証明書の多くはカードや紙といった物理的な媒体である．この方法では「証明書が信頼できる機関から発行され資格情報が偽造されていない」ということを正確に検証するのは難しい．Verifiable Credentials は資格情報にかかわる主体の ID や署名情報などを信頼性の高いデータレジストリ上で管理し，検証可能な形で資格証明を発行することで，これらの問題を解決し，資格情報が信頼できるものかどうか第三者が判断できる仕組みを実現する．

2.2　Verifiable Credentials のエコシステム

Verifiable Credentials を利用する主体は以下の三つが存在する [2]．なお資格情報を Claim と呼ぶ．

Holder（保有者）
VC を取得，保有，提示する主体．例として学生，従業員，顧客などが考えられる．

Issuer（発行者）
Holder に対し Claim を認め VC を発行する機関．例として教育機関，企業，政府などが考えられる．

Verifier（検証者）
Issuer に VC の提示を要求し，検証を行う機関．例として雇用主，Web サービスなどが考えられる．

これらの主体が検証可能なデータベースである Verifiable Data Registry を通じて ID やスキーマ，署名情報の管理や検証を行うことで Verifiable Credentials を実現する．その流れを図 1 に示す．例えば Holder は試験などで獲得した資格を Issuer から 署名された VC として受け取る．必要になれば Holder は必要な VC に署名をし Verifiable Presentation(VP) として Verifier に提示する．VP を受け取った Verifier はその VP の Holder と Issuer による署名を検証し，悪意のある改変も行われていないことを Verifiable Data Registry から確認することができる．Verifiable Data Registry は Holder ごとの識別子や Issuer の情報，VC スキーマなど VC の信頼性を確保するための情報を管理するため，悪意を持った情報の書き換えなどが行えないブロックチェーンなどの信頼性の高いデータレジストリである必要がある．

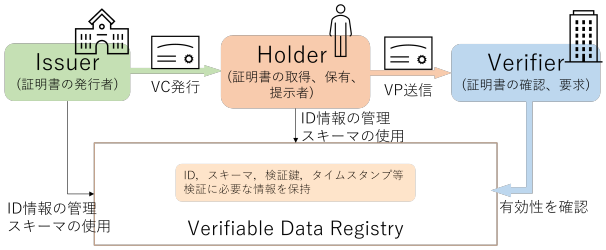

図 1　Verifiable Credentials にかかわる主体と情報の流れ

3　複数のアクティビティを根拠とした VC 発行・検証

3.1　Evidence の記載方法

W3C による Verifiable Credentials Data Model v2.0 の Advanced Concepts では，検証者に向けた Claim の裏付けを示すために VC の json ファイル内に “evidence” というキーを設定する方法が示されている．このキーでは，Claim の根拠となるようなデータを示すことができ，そのデータの URL や名前，ハッシュ値などを VC に記載することで Claim の内容の信頼性を向上させる役割を果たす．

† 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

3.2　活動証明をもとにした修了証 VC の発行・検証

evidence キーを設定することで Claim の内容の根拠を示すことができるが，この根拠にもまた信頼性が必要である．教育現場での活用を考えると根拠となるデータのプライバシーにも配慮しなければならない．これらの要件を満たす方法として，根拠のデータを署名付きの VC として管理し，それらのハッシュや署名情報を Evidence として記載する方法が考えられる．

修了証発行を例に，活動証明 VC に基づいた VC の発行や検証の流れを図 2 に従い説明する．①まず Issuer である教員は，Holder である学生の修了条件にかかわるデータを，活動が行われるごとに署名して記録する．このデータは通常プライバシーの観点から外部には非公開にされるべきものであるため，学内サーバーで保管する．②活動証明 VC が記録される際，同時にオープンなブロックチェーン上にハッシュ値が記載されるようにする．これによってブロックチェーン上には活動証明に対応するハッシュ値とタイムスタンプが同時に記録されるため，各活動証明の改ざんを防いだり，各活動が定期的に行われていたことなどを示すことができるようになる．ブロックチェーンへの書込みは，活動証明 VC 発行の際に自動でスマートコントラクトで処理が行われるようにする．③修了に必要な条件が揃ったら，教員はブロックチェーンに記載された各活動証明のハッシュ値や ID，署名者の情報を Evidence として VC に記載し署名された修了証 VC を学生に対して発行する．④学生が Verifier に提示を求められたら修了証 VC に自分の署名を追加し修了証 VP として提示を行う．⑤Verifier は受け取った VP を，ブロックチェーン上の DID や対応する検証鍵，VC スキーマを使って検証する．これに加え，Evidence の情報がブロックチェーン上に記録されており要件を満たしていることも確認する．もし修了証 VC の内容に疑義が出た場合は，Verifier が Issuer に申し立てを行うことで，活動証明 VC の提示を求め修了証に対し正当な根拠であるかどうかを確かめることができる．この時，対応するブロックチェーン上のハッシュ値との一致も確認することで改ざんを防ぐことができる．

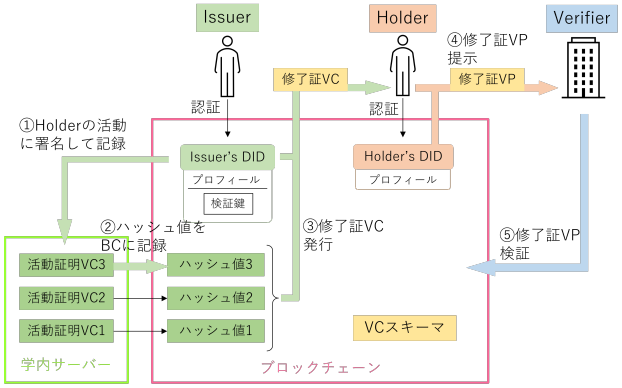

図 2　活動証明 VC をもとにした修了証 VC の発行・検証

3.3　修了証 VC 発行の自動化

量的な評価の計算結果に基づいて修了証 VC が発行される場合，事前定義した条件に従って修了証 VC 発行プロセスを自動化することができる．これにより修了証発行時の不整合を防ぐことが可能になる．

4　ゼロ知識証明を用いた VC 発行

4.1　ゼロ知識証明

ゼロ知識証明とは，何か特定のことを証明したいときに，その証明したいこと以外の何の知識も伝えることなく当該事項を証明する手法である [3]．特に VC においては，すべての内容を明かさず特定の属性のみの情報を提示する選択的開示や，スコアを明かさず特定のスコア以上であることを示す範囲の証明などで活用できる．技術的には BBS 署名や zk-SNARK などによって実現されている．これを応用し，複数のアクティビティを根拠とした VC 発行をする際，根拠となるデータの値は開示せず「演算が正当に行われ結果が特定の条件を満たしている」ということだけを証明できれば，プライバシーに配慮しつつ Claim の内容の信頼性を向上させることができる．

4.2　zkML とは

zkML（Zero-Knowledge Machine Learning）とは、機械学習のモデルや入力データを開示せずとも、推論結果の正当性を示すことができる手法である．機械学習計算のアウトソーシングでの信頼確保が可能になり，金融での信用ランク算出や医療データの活用などが期待される．zkML を実現するツールの一つである EZKL は，Pytorch などで作られたモデルを回路形式に変換し，zk-SNARK の手法を用いることで機械学習のゼロ知識証明を実現している [4]．

4.3　zkML を用いた VC 発行

大学講義などでの評価方法の一つとして，レポートが 6 割，テストが 4 割といったような各活動のスコアに重みをつけ全体の評点を決めるという方法がある．線形回帰のモデルを用いることで機械学習でもこのような評価方法が可能になり，かつ EZKL で作成された証明を VC の Evidence として記載すれば VC 発行の根拠となった各活動のスコアは隠しつつも最終評価の算出が適切に行われたことを検証可能にできる．将来的には，教員が評価した量的な内容だけでなく，自然言語や映像データなど様々なものを評価対象にして zkML を用いた VC 発行を行うことにより，より多角的でプライバシーにも配慮した信頼性の高い教育システムの構築が可能になると考える．

5　まとめと今後の課題

複数のアクティビティに基づく VC の発行・検証について，教育機関での活用を例にブロックチェーン技術やゼロ知識証明を用いて実現する方法を提案した．今後の課題として，検証システムの実装方法やモデルの透明性の確保について検討していく必要がある．

参考文献

[1] LASTRUST. Verifiable credentials とは？, May 2020. https://lastrust.io/2020/06/05/whatis-did-web3/.
[2] W3C. Verifiable credentials data model v2.0, June 2024. https://www.w3.org/TR/vc-data-model-2.0/#ecosystem-overview.
[3] 有限責任監査法人トーマツ. ゼロ知識証明入門. 株式会社翔泳社, 2021.
[4] EZKL. The ezkl system, 2025. https://docs.ezkl.xyz/.