O-014

ブロックチェーン・アカウントに紐づいた Verifiable Credentials の枠組みと証明書可視化

Verifiable Credentials Framework and Certificate Visualization Associated with Blockchain Accounts

石坂 匠 †　　和﨑 克己 ††
Takumi Ishizaka　Katsumi Wasaki

1　はじめに

現状，証明書として多く用いられている紙などの物理的な媒体では，証明内容の真偽を正確に検証できず，経歴の詐称等を防ぐことが難しい．これを解決するための手段として Verifiable Credentials という考え方がある．Verifiable Credentials とはオンライン上で検証可能なデジタル署名された証明書のことで，証明書（claim）の発行元や日時を正確に検証することができる．本研究では，ブロックチェーン・アカウント上で Verifiable Credentials を管理できる Universal Profiles(ERC725/735 LUKSO) という分散型 ID の実装を例とし，第三者検証可能かつ個人アカウントでの claim 管理が可能な枠組みと、資格証明の可視化の仕組みを提案する．

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り，それを個人で保管したり提示したりして使っている．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 は経歴等の個人情報をオンライン上で検証可能な形で管理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可能にする．

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．利用主体と Claim の関係性を図 1 に示す。

Holder（保有者）
Claim 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 Claim 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．

† 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

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 Claim をやり取りすることで，Verifiable Credentials を実現する．例えば Holder は試験などで獲得した資格を Issuer から Claim としてレジストリで受け取り，必要になれば自分の制御の元 Verifier に Claim を提示できるようになる．Claim を受け取った Verifier はその Claim が 信頼できる Issuer から発行され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 Claim，Issuer の情報などを書き込むため，悪意を持った情報の書き換えなどが行えない信頼のおけるデータベースである必要がある．

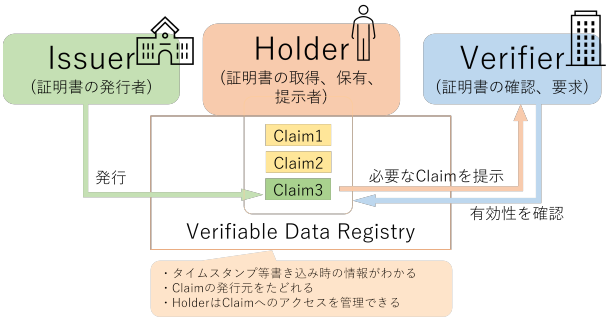

図 1　Verifiable Credentials のエコシステム

2.3　DID とは

DID とは分散型 ID を意味し，管理主体が介在することなく自らのデジタルアイデンティティを保有、コントロールできるというものである [1]．デジタルな個人情報を非中央集権的に管理することで，特定の機関への依存や意図しない情報漏洩を防ぐことができる．Verifiable Credentials の利用には Issuer や Holder のアイデンティティが必要になるが，これは DID で実現されることが望ましい．

3　Universal Profiles

3.1　Universal Profiles とは

Universal Profiles とは、LUKSO プラットフォームで運用されているアイデンティティを持った分散型のブロックチェーンアカウントである。Ethereum での標準規格として検討されていた ERC725/ERC735 を拡張したものであり、自己主権型のアカウントとして情報の管理やトランザクションを行うことが特徴である．

3.2 Universal Profiles の構成要素

Universal Profiles の構成要素として大きな役割を果たしているのは主に LUKSO での標準規格である LSP0 と LSP6 である．LSP0 は ERC725 を使ったアカウントを実現する規格であり，アカウントがブロックチェーン上の任意のアドレスまたはスマートコントラクトと対話できるようにする ERC725X と，スマートコントラクトに制限なくデータを保存できるようにする ERC725Y で構成される [3]．LSP6 は LSP0 の所有者として機能し，ERC725Account のストレージからアドレスのアクセス許可を読み 取り，そのアクセス許可に基づいてアクセスを制限するキーマネージャである．アクセス許可は変更することができ，どのアドレスにどのようなアクセス権限を与えるか設定することができる

3.3 Verifiable Credentials における役割

2.2 節で述べた Verifiable Data Registry は，改ざんが困難かつトランザクション情報が残るブロックチェーンによって実現することができる． また Issuer や Holder の DID は Universal Profiles で実現することができる．Universal Profiles には LSP6 によるアクセス権限の制御機能があるため Claim の管理にも適している．これらのことから，Verifiable Credentials のエコシステムをすべて LUKSO で管理できることがわかる．

3.4 証明書と付帯情報の可視化制御

Universal Profiles に紐づけられる情報は，基本的に JSON 形式である．視覚的にデザインされた証明書を PDF や画像ファイルで発行したい場合は，格納先の URL を JSON ファイル内で参照することで実現できる．格納先としては，通常のサーバーも使用可能だが，分散型ストレージである IPFS を利用することが望ましい．これを利用することで参照先も信頼性の高いストレージを指すことになるので，資格証明の信頼度が向上する．

4 Verifiable Credentials の活用に関する提案

Universal Profiles の利用を念頭に置き，Verifiable Credentials の活用を提案する．

4.1 マルチシグへの対応

資格証明は単一の機関から発行されることが多いが，複数の機関や人の署名に対応すれば発行方法の幅が広がる．例えば教育現場においては，複数指導員全員の署名をもって発行される修了証や，企業と担当教員の署名をもって発行される企業参画型授業の修了証などで利用が考えられる．

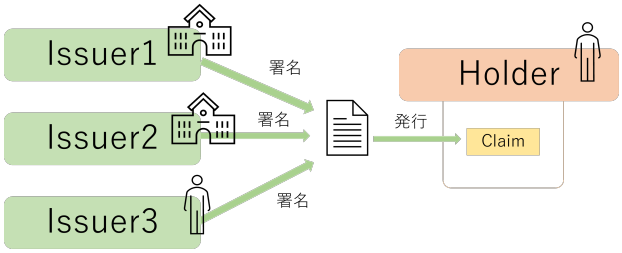

図 2 マルチシグによる Claim 発行

4.2 提示する Claim の選択

所持している Claim の中には，公にしたくない内容や提示先にとってポジティブでない内容が含まれている可能性がある．このため Claim の提示を求められた際に，Holder の意志で情報を適切に選択しその情報だけが提示されるようにする仕組みがあると良い．また一定の条件のもと選択された Claim を適切にまとめ可視化する機能によって，他の Verifier へ使いまわしが行えたり Verifier にとっての可読性を高めたりというメリットが得られる．

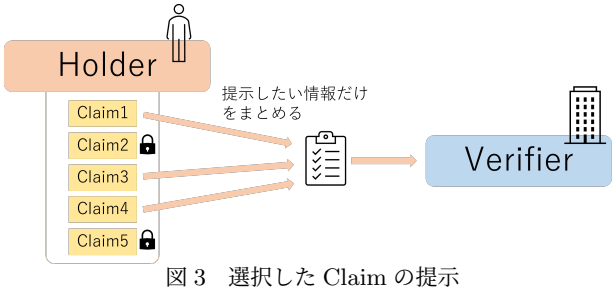

図 3 選択した Claim の提示

4.3 Claim の一括管理

前述した通り LUKSO プラットフォームの中で Verifiable Credentials の機能は完結できるが，別の仕組みを用いて Verifiable Credentials を実現するプラットフォームも考えられる．その際一人で複数のプラットフォームの情報を管理することになると，資格証明の比較が行いづらかったり，単純に管理が面倒なったりという問題が生じる．そこで複数のプラットフォームから自分の資格情報を引き出し，Universal Profiles の書式に合わせ変換・記録するアダプターがあれば，これらの問題を解決し利便性が高まる．

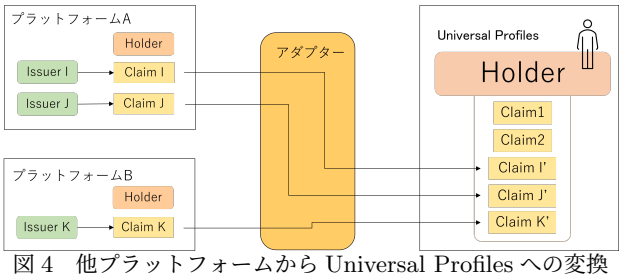

図 4 他プラットフォームから Universal Profiles への変換

5 まとめと今後の課題

Universal Profiles を利用した Verifiable Credentials について，枠組みと活用の提案を行った．今後の課題として，Claim の適切なフォーマットについての検討や他サービスとの連携方法について考えていく必要がある．

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] LUKSO. Universal profiles, June 2024. https://docs.lukso.tech/standards/universal-profile/introduction.