SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

検証可能なマッチング方式の一提案
A Proposal for a Verifiable Matching Method

福岡 尊 * 坂本 拓也 * 牛田 芽生恵 *
Takeru Fukuoka Takuya Sakamoto Mebae Ushida

キーワード DID, VC, ゼロ知識証明

あらまし

分散的アイデンティティ（Decentralized IDentity, **DID**）とは，中央集権的ではなく，分散的なアプローチで管理されるデジタル ID のことである．この DID により，個人にデジタル証明書を電子署名に施した形で発行し，またその個人が，検証可能な証明書を開示できる仕組みを実現できる（Self-Sovereign Identity, SSI）．発行されるデジタル証明書として考えられる例としては，学生証，卒業証明書，運転免許証など多岐に渡る．さらに，例えばデジタル卒業証明書であれば，個人の学歴の正しさを電子的に担保できるため，就職活動などの場で活用できる．この電子署名を施した証明書を **VC**（Verifiable Credential）と呼ぶ．

この DID/VC を用いた枠組みの一つの大きな特徴としては，DID はブロックチェーンのような記録媒体で残るため永続性が高く，そのため発行された学歴といった証明書は，その発行元が消失したとしても有効であることが挙げられる．この特徴はサステナブルな社会に貢献できるものであり，DID/VC を用いたエコシステムの実現を，様々なベンダーが目標としている．たとえばマイクロソフトは，Azure AD と Microsoft Authenticator を活用した DID/VC を実装し，2021 年 4 月からデモとして公開している [1]．こういったエコシステムの実現をより加速させるためには，DID/VC を活用した事例創出を想定した技術を創出することが有効である．

本論文では，DID/VC を活用する事例の一例として，マッチングサービスを念頭に置く．例えば学生が学歴を VC としてマッチング事業者に提示すれば，従来と比べより信頼のおける属性情報に基づいたマッチングを実現することができる．その一方で，マッチングを行う第三者に学生の情報が伝わってしまうという，プライバシー上の懸念が存在する．従来より，プライバシーを保護したうえでマッチングを行う技術は，様々な方面で研究されてきた．例えば Relational Hash[2] は，異なる 2 者が信頼できる第三者から鍵をそれぞれ受け取り，その鍵を用いてハッシュ関数を通すことによって，ハッシュする前の値を明かさずに，一致していたかをチェックすることを可能にする．この技術は属性を秘匿したままのマッチング処理を可能にするものの，ハッシュ化する前の平文に為された署名が有効かどうかを確認することは難しい．

本論文では，VC の VP における信頼性担保を保持しつつ，VC を秘匿した上でマッチングを実現する，一方式を提案する．Relational Hash とは異なり，各々が自らの鍵を作成し信頼できる第三者に預けた上でマッチングを行うことで，属性を秘匿する方式そのものを単純化することができ，従来のゼロ知識証明を援用することが可能となる．

参考文献

[1] https://docs.microsoft.com/ja-jp/azure/active-directory/verifiable-credentials/, 2021 年 12 月 8 日閲覧

[2] Mandal, Avradip, and Arnab Roy. “Relational hash”, The Role and Importance of Mathematics in Innovation. Springer, Singapore, 2017. 103-105.

* 富士通株式会社，〒211-8588 神奈川県川崎市中原区上小田中四丁目 1 番 1 号，Fujitsu Limited, 4-1-1 Kamikodanaka, Nakahara-ku, Kawasaki-shi, Kanagawa, Japan. 211-8588 fukuoka.takeru@fujitsu.com