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

分散型アイデンティティの永続的利用とプライバシー保護
Privacy enhanced durable usage of decentralized identity

坂本 拓也* 牛田 芽生恵* 福岡 尊* 森永 正信*
Takuya Sakamoto Mebae Ushida Takeru Fukuoka Masanobu Morinaga

キーワード 分散型アイデンティティ，ブロックチェーン，ゼロ知識証明，アンリンカビリティ

あらまし

近年、分散型アイデンティティと呼ばれるオーソリティ(発行者)により確認されたアイデンティティ(自身の名前や住所、資格などの属性情報)のクレデンシャルを利用者自身で所有して第三者(検証者)に開示・証明することを可能にする仕組みが実現されつつある。アイデンティティを取り扱うことからプライバシーへの配慮が重要である。例えば、Hyperledger Indy では、ゼロ知識証明を使って、複数の属性値を含むクレデンシャルから一部の属性のみを開示する技術が搭載されており、さらには、同じ利用者が複数回、同じサービスにクレデンシャルを開示したとしても、同一人物の開示であることを識別できないアンリンカビリティも実現している。

分散型アイデンティティでは、クレデンシャルの証明を発行者による署名ベースで行うため、発行者の秘密鍵が漏洩した場合には再発行などのプロセスを踏む必要がある。しかし、出生証明書や卒業証明書など長期にわたっての利用する可能性があるクレデンシャルを考えた場合には、発行者主体がなくなっていて再発行できない場合もありうる。

永続的に利用するためには、ブロックチェーンが一つの解決策となる。例えば、ブロックチェーンにタイムスタンプ付きで、クレデンシャルを保存しておけば、検証者は漏洩が想定される日時以前のタイムスタンプを持つことを確認することで、クレデンシャルの正当性を検証できる。しかし、クレデンシャルをブロックチェーンに保存することは、プライバシー問題につながる。なお、クレデンシャルの代わりにハッシュ値を置くことで、属性そのものに対するプライバシーは強化できるが、複数回アクセス時のアンリンカビリティは達成されない。

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

そこで、ゼロ知識証明のデジタル署名の知識の証明とメンバーシップ証明を組み合わせることで、アンリンカビリティを実現する方法を提案する。デジタル署名の知識の証明は、クレデンシャルの開示時のアンリンカビリティの実現のために Hyperledger Indy で利用されている。メンバーシップ証明は、ある集合の中にある値が含まれていることを、その値を伝えることなく、証明することを可能にする。

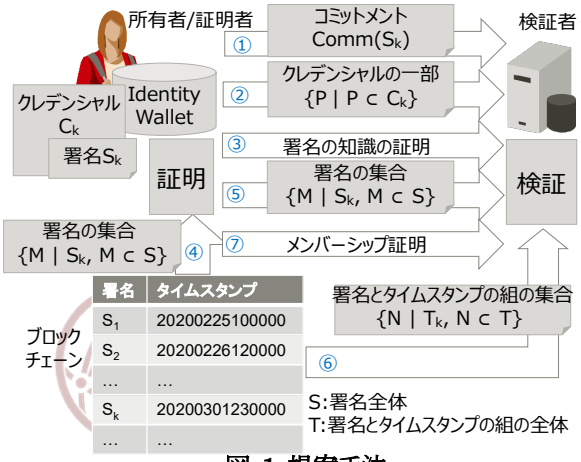

図 1 提案手法

図 1 に示すように、証明者は開示する署名のコミットメントを検証者に送った上で、クレデンシャル(一部でもよい)を開示して署名の知識の証明をすることでクレデンシャル開示部分の正当性を証明し、ブロックチェーンに保存された自身の署名を含む複数の署名を検証者に提供した上でその中に自身の署名が含まれることをメンバーシップ証明により証明する。これにより、自身の署名を一つに特定できないが、提供した署名のすべてがある日時以前のタイムスタンプであれば、自身の署名もそうであることが確認できることになる。

本提案により、ブロックチェーンによる永続的な利用とアンリンカビリティの実現の両立が可能となる。