科学の健全な発展のために

72246424 仁戸田晃

概要 科学の発展のために研究者としての自分がすべきだと考えていることを、自分の現在の研究と関連づけて述べる。先に自分の研究内容である「デジタル学生証における発行者の秘匿と真正性検証の両立」について背景および前提知識とともに述べ、その後、研究の持ちうる倫理的課題について論じる。

1 研究の概要

学生証の提示は、学生であることを確認するために広く用いられている手法であるが、プライバシーの観点などから学生証の発行者を秘匿してしまうと、学生証の真正性が担保できなくなってしまう。そこで、検証可能な証明書である Verifiable Credentials を用い、学校群を包括する群を導入したアプローチをとることでこの問題を解決する。

2 背景

2.1 学生であることの確認

日常生活で、学生割引に適用や、学生限定のイベントなど、学生であることを確認したい・されたい場面は多く存在する。その場合、現在用いられているのは主に学生証・在籍証明証など、所属機関による所属証明の提示や、学校発行のメールアドレスを用いた認証であり、本研究では学生証に着目する。一般の学生証には、学校名、名前、学部、学籍番号、顔写真、など様々な属性が記載されているが、学生証を提示する人は、プライバシーの観点などから必要外の情報を提供したくないことがあるということも想像できる。

2.2 Verifiable Credentials

学生証の一形態として、Verifiable Credential (以下、VC と呼称) を用いたものがある。Verifiable Credentials は、暗号学的な手法で改ざん検知、および作成者が誰であるかの検証を可能にした Credential のこと、すなわち検証可能な証明書のことであり、ここでの Credentail とは発行者によって発行された、対象となる主体に対する何らかの主張 (Claim) の組と定義される。Claim は、対象となる主体にまつわる「属性：値」のペアである。VC においては、発行者（Issuer）によって発行された VC を、保有者（Holder）が検証者（Verifier）に提示する IHV モデルが取られている。なお、VC の示す主張の対象としての Subject と、VC の Holder は必ずしも同じである必要はない。Subject と Holder が異なる例として、子供に対して発行された VC をその保護者が保管する場合などが挙げられる。Holder が VC を Verifier に提示する際、Holder が、複数の VC を合わせ、VP が正しいことを示す Proof および Holder であることを示す Proof を含んで提示する Verifiable Presentations (以下、VP と呼称) という形式をとることもできる。また、Holder は VC および VP を任意のタイミングで任意の属性を含んだ形で提示することもでき、任意の属性の提示を可能にする技術として選択的開示が存在する。

2.3 VC の一例

VC を適用できる事例として、運転免許証が挙げられる。運転免許証において先ほどの IHV モデルを適用すると、Issuer は各都道府県公安委員会であり、Holder は運転免許証を交付され保持する人であり、Verifier は時と場合により異なりうる。レンタカー会社が車を貸し出す時に運転免許証を確認する場合があるかもしれないし、アルコール等を購入する際に年齢確認を行うために小売業者が運転免許証を確認する場合があるかもしれない。また、選択的開示も可能である。Holder が年齢確認をされる場合、最低でも顔写真と生年月日の項目があれば必要十分であると想定され、名前や住所などの情報は開示する必

要はない。この場合、選択的開示を用いることで、顔写真と生年月日という 2 つの属性が適切な Issuer によって主張され、改ざんされていないことを Verifier は暗号学的に検証することができる。

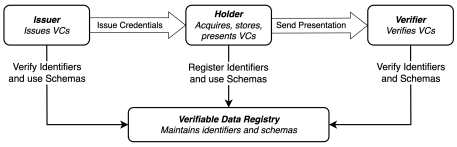

図 1　IHV モデル

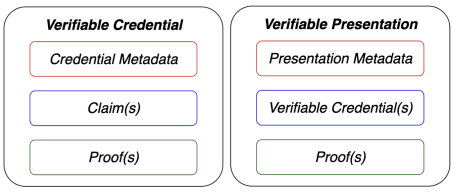

図 2　VC および VP

1. 番号付き箇条書き
2. 番号付き箇条書き

- 箇条書き
- 箇条書き

3　研究目的

3.1　hoge

画像を図 3 に示す。

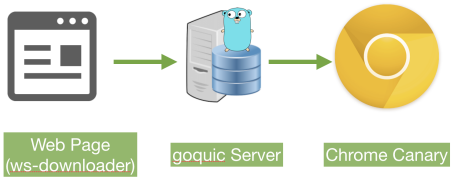

図 3　画像の例

3.2　fuga

fugafuga