検証可能な資格情報によるデジタル学生証基盤の設計

山口, 嵩史
九州大学大学院システム情報科学研究府

糸川, 諒
九州大学工学部

伊東, 栄典
九州大学情報基盤研究開発センター

出版情報：IPSJ SIG Technical Report. Information Processing Society of Japan
バージョン：

[ポスター発表] 研究報告

検証可能な資格情報によるデジタル学生証基盤の設計

山口 嵩史[1,a)]　糸川 諒[†1,b)]　伊東 栄典[†2,c)]

A study on information infrastructure for digital student/staff ID using verifiable credential

1. はじめに

スマートフォンの普及に伴い，スマートフォンで資格情報を表示する仕組みの検討が進んでいる．九州大学では IC カード学生証・職員証を発行しており，特定施設の入室に IC カードを用いている．またカード券面に名前や所属組織等が印字されるため身分証に利用できる．IC カードは軽量薄型で耐タンパ性を備えたデバイスであるものの，費用と紛失盗難時の問題がある．そもそも IC カードの費用と印字作業の費用は必要である．紛失の場合，再発行カードの費用と再発行まで入館できない．盗難されると個人情報漏洩や，権限の無い他者による入館の危険性もある．携行の際は交通系など他の IC カードとの併用の面倒さも有る。

我々は IC カード学生証・職員証が持つ機能のスマートフォンでの代替方法について検討している．なお，以降では簡略化のため学生証のみに言及する（職員証でも同様の議論が適用できる）．標準化団体 W3C (World Wide Web Consortium) は検証可能な資格情報 (Verifiable Credentials. 以下，VC)[1] の仕様を提供している．この仕様に基づく VC を学生証として実現することで，電子的な本人確認が可能となる．VC の検証で，建物入館の可否，授業での出席確認などを実現できる．鉄道各社が認めれば，定期券や学割切符発行時の確認にも利用できる。

2. 検証可能な資格情報の動向

近年，認証技術として注目されている検証可能な資格情報 (VC) は，デジタル的な個人情報の証明書として機能する [2]．W3C VC 仕様 [1] では，発行者 (Issuer) が保持者 (Holder) に対して発行した証明書を，検証者 (Verifier) が検証可能とする仕組みが策定されている．この三つの主体以外に，Verifiable Data Registry が存在し，識別子や鍵，その他関連データの作成や検証の仲介を行う．VC に記載されている属性情報は，JSON 形式のデータである JWT(JSON Web Token)[3] で表現される．

VC はデジタル庁のワクチン接種証明書 [4] の SMART Health Cards(SHC)[5] や，慶應義塾大学が実施した次世代デジタルアイデンティティ基盤に関する実証実験 [6] に活用されている．この実証実験では慶應義塾大学の学生を対象に在学証明書や卒業証明書をスマートフォンに発行した．

3. 設計

デジタル学生証の画面を図 1 に示す．画像部分は従来からの身分証として提示する氏名・学生番号・所属学部などを表示する．QR コード部分が VC である．

図 1　デジタル学生証想定図

検討した学生証発行および検証機構の設計を述べる．設計したシステムでは Shibboleth を認証を用いる．システムの構成要素を以下に列挙する．

- 保持者：VC 保持者で学生（と職員）が該当.
- 発行者：VC 発行主体で大学が該当.
- IdP　：構成員の属性情報を提供する Shibboleth IdP.
- 検証者：提示された VC の検証主体．入館処理の機器や，学割発行者等が該当.

九州大学の学内認証基盤には Shibboleth IdP が導入されている．提案システムを実装する場合，発行者と検証者の

[1] 九州大学システム情報科学研究府
Grad. S. of ISEE, Kyushu U., Fukuoka 819-0395 Japan
[†1] 現在，九州大学工学部
Presently with School of Eng., Kyushu U., Fukuoka 819-0395 Japan
[†2] 現在，九州大学情報基盤研究開発センター
Presently with Research Institute for IT, Kyushu University
[a)] yamaguchi.takashi.228@s.kyushu-u.ac.jp
[b)] itokawa.ryo.975@s.kyushu-u.ac.jp
[c)] ito.eisuke.523@m.kyushu-u.jp

構築と設置，学生と検証者向けのアプリケーション開発に焦点を当てれば十分である．そこで VC 発行と検証の処理手順を説明する．

3.1 VC 発行

VC 発行手順を以下に示す．

- 保持者は専用アプリを起動
- 可能なら NFC マイナカードで本人確認
- 専用アプリから発行者（大学）に VC 発行を要求
- 発行者は IdP へリダイレクト処理
- 保持者は IdP で ID とパスワードを入力に利用者認証
- 認証が通れば IdP は SAML[7] 形式で保持者の属性情報を発行者に返す
- 発行者は SAML の属性情報から JWT 形式の属性情報を作成
- 発行者の秘密鍵で JWT の署名を作成
- 発行者から保持者へ VC（デジタル学生証）を発行

現在の Shibboleth IdP はテキストの属性情報は返せるものの，顔写真情報は保持していない．大学は IC 学生証印字のための顔写真データを保有している．デジタル学生証の発行者に顔写真データを持たせる必要がある．

3.2 VC 検証

保持者は VC から提示用の形式である VP (Verifiable Presentation) を作成する．他者に使われないように VP の有効期限は短く，一定時間毎に更新する．検証者による検証作業はドアの開閉など近距離で行うと想定する．

VC 検証手順を以下に示す．

- 保有者は専用アプリを起動
- 専用アプ内でランダム数値を生成（暗号用の共通鍵として利用）
- 数値を鍵として VC 暗号化し，暗号化 VC と共通鍵から QR コードを生成
- 検証者は QR コードから暗号化 VC と暗号鍵を読出して VC を復号
- 検証者は VC の署名検証により，内部テキストを信用

3.3 他の検証方式との比較

資格情報の検証は，Blockchain や PKI クライアント証明書での実現も考えられる．Blockchain の場合，トランザクションを記録するノードが一定台数以上必要である．プライベートチェーンを用いる場合，ノード群の構築と管理・運用の手間がかかるし，ノード群の長期的な維持も問題になる．パブリックチェーンを用いる場合には，ノードの維持費は不要だけれど，処理のためのガス代（金額）が必要になる．

クライアント証明書を用いる場合，各学生に対してクライアント証明書の発行費用が必要になる．全学生への証明書を発行すると，大きな費用が必要である．クライアント証明書の秘密鍵利用時の PIN 管理も必要になる．

Blockchain とクライアント証明書どちらの場合も学生自身に秘密鍵の管理が委ねられる．学生側が秘密鍵を適切に管理することは容易ではなく，秘密鍵を紛失してしまう場合も考えられる．この場合，鍵情報の再登録や証明書の再発行でコストが再度発生する．

本論文で提案する Shibboleth を用いるシステムでは，既存 IdP を活用するため管理・運用が比較的容易である．また，Shibboleth IdP には構成員の情報が登録されているため，学生証の失効と再発行作業は簡便になる．学生による秘密鍵管理も必要もないうえ，退学時の学生証失効などの管理も大学側で行える．そのため提案システムは，先述した 2 つよりも現実的に優れていると考えている．

4. おわりに

今回，スマートフォン学生証を実現するために設計したシステムについて説明した．本論文で提案したシステムでは，発行者は Shibboleth を用いての VC を発行を行う．今後，検討した設計を基づく発行者システムとスマートフォン用のアプリを試作し，試作システムで動作検証を行う予定である．

参考文献

[1] W3C, Verifiable Credentials Data Model v1.1, 2022, https://www.w3.org/TR/vc-data-model/, 最終アクセス：2023/10/5.
[2] 仙道 頭洋, 小川 博久, Web3.0 時代のサイバーセキュリティ -インターネット経済のパラダイム転換に向けた課題と展望-：6. 分散型 ID とサイバーセキュリティ -進化するデジタルアイデンティティとそのセキュリティ-, 情報処理, vol.64, no.10, pp.e32–e36, 2023.
[3] M. Jones; J. Bradley; N. Sakimura, JSON Web Token (JWT), https://www.rfc-editor.org/rfc/rfc7519, 最終アクセス：2023/10/6.
[4] 厚生労働省, 新型コロナウイルス感染症予防接種証明書 (接種証明書) について, https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/vaccine_certificate.html, 最終アクセス：2023/10/6.
[5] SMART Health IT, SMART Health Cards, https://smarthealth.cards/en/, 最終アクセス：2023/10/6.
[6] 慶應義塾大学,「慶應義塾大学、次世代デジタルアイデンティティ基盤の実証実験を開始」, 2020-10-26, https://www.keio.ac.jp/ja/press-releases/files/2020/10/26/201026-1.pdf, 最終アクセス：2023/10/5.
[7] OASIS, Security Assertion Markup Language (SAML) V2.0 Technical Overview, http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html, 最終アクセス：2023/10/6.