検証可能な資格情報によるデジタル学生証の試作

糸川 諒[1,a)]　伊東 栄典[2]

概要：スマートフォンの普及に伴い，スマートフォンでの資格情報提示の検討が進んでいる。多くの大学で IC カード学生証・職員証が発行され，券面情報で名前や所属組織の確認と，IC による施設入館や図書貸出に利用されている。我々はスマートフォンで利用するデジタル学生証・職員証について検討している。W3C (World Wide Web Consortium) は検証可能な資格情報 (Verifiable Credentials, 以下 VC) の仕様を提供している。学生証を VC として発行することで，デジタル身分証を実現できる。VC の検証により，建物入館，図書貸出，出席確認に実現できる。本稿では，デジタル学生証の要求要件分析，試作システムの設計・実装・評価について報告する。

キーワード：学生証・職員証, 検証可能な資格情報, スマートホン, 認証基盤

A prototype of digital student ID with verifiable credentials

Ryo Itokawa[1,a)]　Eisuke Ito[2]

Abstract: With the spread of smartphones, smartphone based credentials are considered. University student/staff ID is realized as IC card, and the card is used as not only ID card using printed text to onfirm holder's name and organization, but also it is used as enterance key for buildings, book lending in library. We are considering digital student/staff ID that can be used on smartphones. W3C (World Wide Web Consortium) has published specifications for Verifiable Credentials (VC). By issuing a student/staff ID as a VC, a digital ID can be realized on smartphone. By verifying VC, it can be implemented for keys for building entry, book lending, and attendance confirmation. This paper reports our prototype of digital student/staff ID with VC. We also report requirements, design and implementation for digital ID, and evaluate our prototype system.

Keywords: student/staff ID, verifiable credentials, smartphone, user authentication system

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。多くの大学で，IC カード学生証・職員証が発行され，本人確認や施設入室等に用いている。IC カードは軽量薄型かつ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による代替について検討している [1]。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)[2] の仕様を提供している。この仕様に基づく VC を学生証・職員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。サービス機関が認めれば学割発行にも利用できる。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）。

[1] 九州大学工学部電気情報工学科
[2] 九州大学情報基盤研究開発センター
[a)] itokawa.ryo.975@s.kyushu-u.ac.jp

本論文の構成は以下の通りである。第 2 節で VC の技術動向を述べる。第 3 節で，デジタル学生証の方針および設計を述べる。第 4 で，試作システムを評価する。最後に第 5 で，まとめと今後の課題を述べる。

2. VC 関連動向

スマートフォンなどの端末で，デジタルに個人情報証明書として扱う検証可能な資格情報 (VC) が検討されている [3]。W3C は VC の仕様 [2] を公開している。この仕様では，主体として発行者 (Issuer)・保持者 (Holder)・検証者 (Verifier) と，Verifiable Data Registry を定義している。発行者は所有者に資格情報 (Credential) を電子的に発行し，所有者は資格情報を端末に保持する。検証者は所有者の資格情報を暗号技術を用いて電子的に検証する。この仕様では，VC の属性情報は JSON 形式で格納される。他者に提示する場合，JSON 形式を JWT(JSON Web Token)[4] に変換して QR コードなどで提示する。属性情報の真正性確認には暗号方式・暗号鍵・電子署名を用いる。

VC の実例にデジタル庁・厚生労働省のワクチン接種証明 [5] がある。ワクチンの接種証明書には SHC(Smart Health Cards) 方式 [6] が用いられている。このアプリでは，マイナンバーカードでの本人確認後，デジタル庁のサイトから接種証明情報を格納した JWT(JSON Web Token) および JWS(JSON Web Signature) 形式のデータを入手する。この JWT データが VC になる。アプリで，他社の接種証明を検証できる。QR コードで表示された VC (JWT データ) を読み取り，電子署名が正しいものかを確認する。VC 内に記載された URL（デジタル庁の Web サイト）から公開鍵を入手し，電子署名の正しさ (=改竄が無いこと) を確認できる。

運転免許証のデジタル化も検討されている。ISO はモバイル運転免許証仕様 [7] の策定および公開をしており，いくつかの国や行政単位でモバイル運転免許証の実証実験がされている。

学生証や職員証についても開発や検討が進んでいる。金沢大学では専用アプリによるデジタル学生証を試験している [8]。ある企業は，デジ学 [9] と名付れたアプリを作成・販売している。

3. 方針と設計

3.1 方針

デジタル学生証の実装方針を以下に示す。

- なるべく IC 学生証が持つ機能を継承
- 最初は実装しやすい簡易な構成
- なるべく既存の認証基盤を利用
- 1 つの大学だけでも運用可能な構成
- 将来，他大学や外部組織との連携を想定

W3C VC 仕様 [2] では発行者 (Issuer)・保持者 (Holder)・検証者 (Verifier) と，Verifiable Data Registry を定義している。Verifiable Data Registry にブロックチェーンネットワークも検討されている [3]。ブロックチェーンの維持には複数ノード稼働が望ましい。しかし 1 大学での運用を考えると，ブロックチェーン用ノード群の維持は過剰であろう。簡易な構成である中央集権型サーバで，学生証 VC 発行と，学生証 VC の検証支援を行う構成にする。

デジタル学生証を VC で実現するには，学生証データが検証可能でなければならない。学内の建物入館や出席確認に VC を使う場合，検証方法が非公開でも問題ない。他大学や外部組織でも検証可能とするには，検証機能の仕様を公開し，かつ共通化する必要がある。例えば学生が交通機関の学割を使う場合，デジタル学生証を検証可能とする必要があるだろう。

3.2 デジタル学生証の VC 構造

デジタル学生証の VC 構造は，デジタル庁のワクチン接種証明の VC 構造と援用する。つまりデジタル学生証の核となる VC データは JSON で記述する。VC データに電子署名を付与し，データの完全性（改竄がないこと）を保証する。署名に用いる秘密鍵に対応する公開鍵の URL は，学生証 VC に含める。現用 IC カード学生証の券面情報に含まれるデータは，VC に含める。

表 1 デジタル学生証 VC 構造

項目	説明
発行者	大学名，学長名（公印画像）
所属	学部学科
氏名	漢字氏名，カナ氏名，英字氏名
生年月日	西暦年月日
有効期限	西暦年月日
学生番号	文字列
Login ID	必要ならば記載
電子署名	署名アルゴリズムと署名データ
公開鍵 URL	署名用の秘密鍵に対応する公開鍵

学生証のテキスト情報を信頼するには，学生証の顔写真と所有者（学生）の顔を見比べての同一人物確認が必要である。そのためデジタル学生証には「顔写真」が必要である。ただし顔写真データはデジタル学生証のアプリ内に保存するだけで，VC データには格納しない予定である。VC データは他者に渡す可能性があるため，プライバシー保護のために顔写真を VC に含めない。

3.3 VC 発行手順

設計方針として，既存認証基盤の利用と，1 つの大学で運用可能な構成を上げている。そのため，日本の多くの大学で利用されている Shibboleth IdP を利用する。Shibboleth 認証では，IdP で利用者認証が成功すると，SAML Response

に利用者の属性情報を含めて返信できる。そこで学生証 VC 発行に Shibboleth IdP での認証を用いる。認証成功後に返る SAML Response に記載された属性情報を，学生証 VC 発行局で JWT 形式に変更し，所有者（学生）に VC として発行する。図 1 に検討中の学生証 VC 発行手順案を示す。

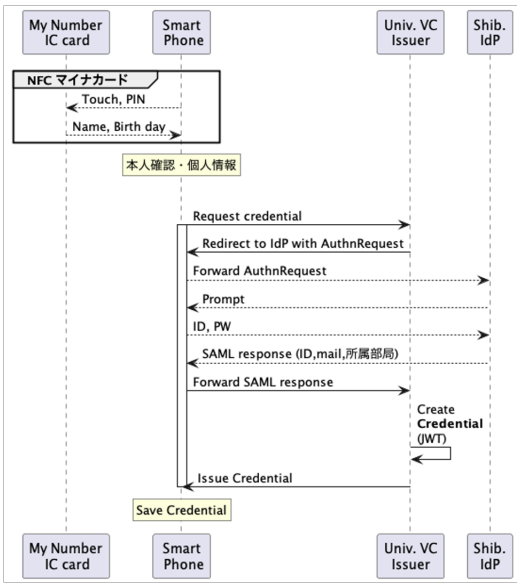

図 1　学生証 VC 発行手順の案

2024 年 1 月現在，筆者が所属する九州大学の IdP では，ID・パスワード認証しか提供していない。ID と PW が漏れると，他者の学生証情報を取得することが可能になる。IdP に多要素認証を含めるか，他の本人確認機構が必要である。可能ならマイナンバーカードによる本人確認を行いたい。

九州大学の Shibboleth IdP は，テキストで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。ただし IC 学生証印字のために顔写真データを大学は保有している。デジタル学生証発行局が顔写真データを保持し，学生証 VC 発行時に顔写真データを送付するか，スマートホンで撮影した顔写真を利用するかの手続きが必要になる。

3.4　VC 検証

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 検証では，保有者は VC を QR コードとして提示し，検証者は QR コードをデコードしたテキストを処理する。QR コードは画像として保存できるため，VC の JWT テキストの QR コード化ではなりすましが可能になる。なりすまし防止のため，5 分程度の一定時間毎に変化する仕組みを導入する。

図 2 に検証手順の案を示す。

一定時間毎に QR コード変化させるつつ，VC データを保護する方法として，所有者と発行者が共有する秘密情報

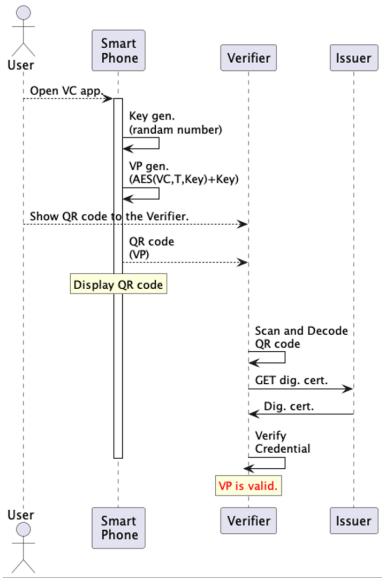

図 2　VC 検証手順の案

(seed) と時刻ベース OTP(One time password) を使う。ここで TOTP は，RFC6238 で定義される 6 桁数値である。検証者に渡す QR コードの値は，以下の値とする。

- UserID, TOPT
- VC ヘッダ
- VC を key で AES 暗号化した文字列
- VC の署名

検証者は所有者の QR コードをデコードする。VC ヘッダに埋め込まれた確認 URL(発行局) に，UserID と TOPT で key を問い合わせる。UserID と TOTP が正しければ key が返信される。返信された key で AES をデコードし，VC 内容を確認する。

所有者のアプリが作る key，また発行局が返す key の値は，ハッシュ値 $SHA_1(seed, T)$ とする。ここで T は，TOTP で用いる時刻情報である。

3.5　表示データの追加

現在の IC 学生証は，IC 機能 (NFC 機能) を用いずに，券面に印刷されたバーコードだけを使う場合もある。学生健康診断における受診者確認や，図書館への入館ゲートは，学生番号だけを確認している。バーコードや QR コードでの学生番号（学籍番号）表示も必要であろう。

また，ある大学の学生であることを証明するものの，自分の個人情報は渡さない仕組みも必要であろう。現段階の学生証 VC には，氏名・生年月日など個人を特定できる情報が多い。VC 全体を渡すのではなく，デジタル学生証を持つ個人が，本当に所属しているのか否かを発行局に問い合わせる仕組みも必要であろう。この仕組みも TOPT を用いて実現できる。

4. 試作と評価

4.1 試作システム

試作システムを，Linux サーバ 2 台と，Android スマートホンで作成している。サーバには https と電子署名には，国立情報学研究所の UPKI サーバ証明書を利用する。Linux サーバは，Shibboleth IdP サーバと，デジタル学生証発行局として運用する。

表 2 試作システムハードウェア

	発行局	IdP	スマートホン
機種	Beelink MINI-S12 N95		Sony Xperia ACE-2 SO-41B
OS	AlmaLinux 9.2		Android
Web	Apache 2.4		-
その他	Shibboleth SP	Open LDAP 稼働	Flutter App

本論文の執筆時点でサーバ 2 台は未完成である。Shibboleth IdP には，ジェイズ・コミュニケーション社との共同研究により，WisePoint IdP を利用させていただく予定である。デジタル学生証発行局は，Apache Web サーバ，Shibboleth SP モジュール，Python CGI プログラムとして実装中である。IdP が稼働していないため，スタブ発行局として，どの利用者 ID に対しても一つの学生証 VC データを返すだけの機能を実現している。IdP 稼働後には利用者 ID とパスワードによる認証と，SAML Response の属性情報からの VC 変換，および電子署名を実現する。

デジタル学生証は，Flutter を用いて Android アプリとして開発している。試作したデジタル学生証の画面を図?? に示す。アプリを起動し，「学生証発行」に移り，利用者認証が成功すると学生証 VC データを入手する。発行局から得た VC データを格納後，学生証表示モードに移ると，QR コード付きの学生証画面が表示される。

図 3 試作デジタル学生証の画面

他者の学生証 VC の検証モードも実装している。学生証の QR コードを撮影後，QR コード画像をデコードし，得た JWT 文字からヘッダ部，ペイロード部（学生証データ本体），電子署名に切り分ける。ヘッダ部に書かれた署名用のハッシュアルゴリズムで，ペイロード部分の値を計算する。またヘッダ部記載の URL から公開鍵を取得し，署名を検証する。検証が成功したら，学生証 VC が正しいと表示する。

なお，3 節で記述した「一定時間ごとに QR コードが変わる」という機能を本露文の執筆時点では実装できていない。この機能も今後実装予定である。

5. おわりに

本論文では検証可能な資格情報 (VC) によるデジタル学生証について述べた。システムの実現方針，VC 学生証発行手順の案，VC 学生証検証手順の案，および試作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 IdP 認証を用いての VC を発行を行う。検証手順については，今後も進化させていく必要がある。デジタル学生証発行システムと Android スマートホン用アプリを試作している。どちらも未完成であるため，今後も開発を続けつつ動作検証を行う予定である。

謝辞 共同研究として参加してくださるジェイズ・コミュニケーション社の皆様に感謝します。

参考文献

[1] 山口嵩史, 糸川諒, 伊東栄典: 検証可能な資格情報によるデジタル学生証基盤の設計, インターネットと運用技術シンポジウム論文集, vol.2023, pp.83-84, 2023.
[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] SMART Health IT, SMART Health Cards, https://smarthealth.cards/en/, 最終アクセス:2023/10/6.
[7] ISO/IEC 18013-5:2021, Personal identification ISO-compliant driving licence, 2021-10-4, https://www.iso.org/standard/69084.html, 最終アクセス:2024/2/2.
[8] 金沢大学, 「金沢大学身分証アプリ」試行運用の開始 | KU-NOTICES, https://note.w3.kanazawa-u.ac.jp/contents/615, 最終アクセス：2023/1/10.
[9] , デジタル学生証発行システム・学生証表示アプリ「デジ学」, https://www.digigaku.jp/, 最終アクセス：2023/1/10.
[10] 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.