デジタル学生証発行における身元確認方法の検討

糸川, 諒
九州大学システム情報科学研究府

山口, 嵩史
九州大学システム情報科学研究府

伊東, 栄典
九州大学情報基盤研究開発センター

出版情報：研究報告インターネットと運用技術（IOT）. 2024-IOT-66 (1), pp.1-6, 2024-07-12. Information Processing Society of Japan
バージョン：

デジタル学生証発行における身元確認方法の検討

糸川 諒[†1,a)]　山口 嵩史[†1,b)]　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) の仕様を提供しており，VC でデジタル学生証は実現できる。学生証を VC で発行する際，発行時の本人確認および利用者認証が問題となる。多くの大学ではオンラインサービスの利用者認証に ID・パスワード認証だけを用いている。パスワード認証は盗用等の脆弱性があるため，個人情報であるデジタル学生証発行に課題がある。マイナンバーカードを用いて，本人確認を強化する方法を検討した。本稿ではマイナンバーカードによる本人確認強化手法を述べる。

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 study of Identity Verification Methods for Digital Student ID

Ryo Itokawa[†1,a)]　Takashi Yamaguchi[†1,b)]　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), and digital student IDs can be realized with VC. When issuing student IDs as VCs, identity verification and user authentication become problems. Most universities only provide ID and password authentication for online services. Password is vulnerable by thefting, so PW authN is not better to issue digital student IDs. Therefore, we have considered a method to enhance the identity verification process using the Japanese My_Number Card. This paper describes a method to strengthen identity verification using My Number cards.

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][2]。標準化団体 W3C (World Wide Web Consortium) は検証可能な資

†1 現在，九州大学システム情報科学研究府
Presently with Grad. S. of ISEE, 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) itokawa.ryo.975@s.kyushu-u.ac.jp
b) yamaguchi.takashi.228@s.kyushu-u.ac.jp

格情報 (Verifiable Credentials。以下，VC)[3] 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）。

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 節で利用者認証と本人確認の概要を述べる。第 4 節で，デジタル学生証の方針および設計を述べる。第 5 節で，デジタル学生証における本人確認の方針および設計を述べる。第 6 で，試作システムを評価する。最後に第 7 で，まとめと今後の課題を述べる。

2. VC 関連動向

2.1 VC 事例

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 [4]。W3C は VC の仕様 [3] 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)[5] 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 [6] がある。ワクチン接種証明には SHC(Smart Health Cards) 方式 [7] 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。

アプリでは他者の接種情報を検証できる。他社が表示した QR コードから VC (JWT データ) を読み取り，電子署名が正しいか確認することで検証している。VC 内に記載された URL（デジタル庁のサイト）から公開鍵を入手し，電子署名の正しさ (=改竄が無いこと) を確認する。なお，2024 年 3 月末でワクチン接種証明アプリは終了している。

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 [8] 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。

デジタル学生証・職員証についても検討や開発が進んでいる。金沢大学では専用アプリを試験している [9]。ただし印字されたプラスチックカードが正式な学生証で，アプリは身分証との位置づけである。

2.2 VC の選択開示

資格情報には多くの情報が含まれており，本人確認などの利用用途に応じて情報を選択し，すべての情報を開示したくない場合がある。例えば，健康保険証を本人確認書類として提出する際には，保険者番号や被保険者等記号，QR コードを画像編集や付箋を用いてマスキングする必要がある。このような資格情報の選択開示は，デジタル資格証の枠組みである VC でも検討されている。

W3C の Verifiable Credential Data Model が示すエコシステムでは，Issuer（発行者）が Holder（保有者）に対して VC を発行し，その後 Holder が VC の内容の全てまたは一部を Verifiable Presentation（検証可能なプレゼンテーション）として Verifier（検証者）に渡す。Issuer は VC を発行する際，データにデジタル署名を付け，この署名により，VC が Issuer から発行されたものであることを確認でき，データの改竄も検出可能である。しかし，Holder が VC の一部のみを Verifier に提示したい場合，署名が無効になる問題がある。これに対処するために提案されたのが Selective Disclosure JWT（SD-JWT）である。

SD-JWT では，選択的開示の対象となるデータを元のデータ集合から切り離し，代わりにそのダイジェスト（ハッシュ値）をデータ集合に埋め込む。このダイジェストを含むデータ集合に Issuer が署名を行い，署名付きデータ集合と切り離したデータの中から選択したデータを一緒に Verifier に渡すことで，開示しないデータの改竄防止と検証を可能にする。

SD-JWT の具体的な実装方法として，JWT（RFC 7519）を利用する。データに対する署名と選択的開示のためのダイジェストの計算には，データ名・データ値にランダムなソルトを加えてハッシュ化を行うことで，元データの推測を防ぎつつ，安全にデータを開示することができる。

3. 本人確認と利用者認証

3.1 本人確認

対面の本人確認は古くから行われてきた。最も古くからある対面での本人確認方法は，信頼できる人が発行する紹介文書や証明書を確認する方法であろう。この方法は，個人的な信頼関係を基にしており，血縁や地縁の繋がりが強い場合に有効である。しかし，縁者でない人や関係の薄い人は信頼性を確保することが難しく，詐欺や偽造のリスクが存在する。

次の方法は，政府などの信頼できる第三者が発行する証明書による確認方法である。公的機関が発行するため信頼性が高く，統一形式で扱いやすい利点がある。ただし証明書の有効期限や偽造のチェックは必要である。

対面での本人確認方法として，証明書に記載された情報（氏名，住所，年月日）を見て，一つひとつ会話で確認する方法がある。直接対話により不審な点や矛盾を確認でき，その場でのフィードバックが可能である。この方法は入国時の本人確認などで利用されている。確認作業の時間や，職員の判断力に依存するという課題がある。

近年のデジタル技術の進歩により，電子的な本人確認方法も進化している。まず，電子証明書 (Digital Cetrificate) の利用がである。政府が発行するデジタル ID やマイナンバーカードを利用することで，オンラインでの迅速かつ正確な身元確認が可能となる。具体的には，受付窓口に専用の読み取り機を設置し，マイナンバーカードやその他のデジタル ID をスキャンして確認する。

指紋や顔認証などの生体情報で，本人確認の精度を高めることができる。生体情報はコピーが困難なため，なりすましの問題が少ない。ただし指紋デバイスや顔認証アプリと，生体情報の事前登録が必要になる。

オンライン事前登録による効率化もある。来訪者が事前にオンラインで身元情報を登録し，登録情報を持つことで，窓口における対面での確認作業を効率化できる。例えば市役所では，役所のウェブサイトに事前登録フォームを設置し，必要情報を入力させること実現している。

3.2 利用者認証との比較

本人確認と，オンラインでの利用者認証は，似ているが微妙に異なる。利用者認証とは，サービスやシステムにアクセスする際に正当な利用者であることを確認するプロセスである。オンラインバンキングのログインやスマートフォンのロック解除などがこれに該当する。一方，本人確認とは個人が特定の本人であることを確認するプロセスのことである。銀行口座の開設時の身分証明書提示やオンラインサービスの登録時の身分証明書アップロードなどがこれに該当する。どちらのプロセスも，ともにセキュリティを高め，不正行為を防ぐためのものであるけれど，利用者認証はサービスへのアクセス権の確認を目的とし，本人確認はサービス利用者の身分の証明を目的としている点で異なる。

本稿で扱う学生証は，本人確認が可能な，公的な身分証明書の役割を持つ。従来の IC カード学生証と同様にデジタル学生証にも同じ機能が求められる。そのためデジタル学生証発行時には，発行時に申請者が本物の学生であることを確認し，不正発行や身分詐称を防ぐための本人確認が必要である。デジタル学生証の発行手続きはオンラインで行われるため，本人確認もオンラインで行う必要がある。また，正当な所有者がアクセスしていることを確認するためのデジタル学生証の利用者認証をスマホのロック機能や学生証アプリの利用開始時に指紋認証や顔認証を用いることで，さらなるセキュリティ強化が可能である。

4. 方針と設計

4.1 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 [3] 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 [4]。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。

4.2 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。

4.3 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。

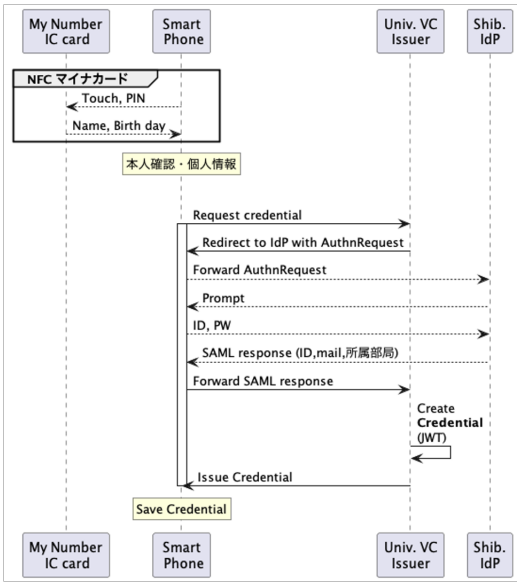

図 1 学生証 VC 発行手順の案

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。

4.4 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。

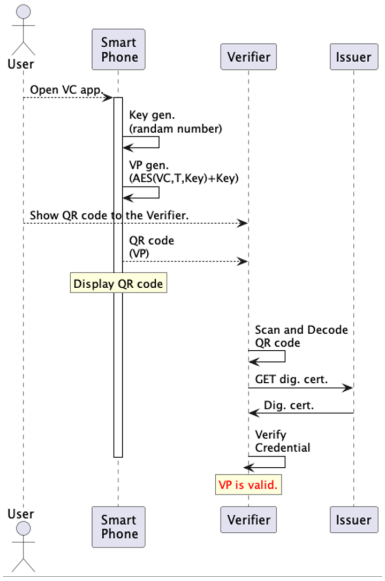

図 2 VC 検証手順の案

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 (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。

5. 本人確認の方針と設計

5.1 本人確認の方針

デジタル学生証発行手続きにおけるオンラインでの本人確認の方法を提案する。本人確認には，日本国政府が発行するマイナンバーカード [12] を利用する。マイナンバー

カードとは，日本に住民票がある人からの申請により無料で交付される，氏名，住所，生年月日，性別，マイナンバーが記載された，顔写真付きのプラスチック製のカードである。IC チップが搭載されており，4 つのアプリケーションを保有している。1 つ目が JPKI-AP，2 つ目が券面 AP，3 つ目が券面事項入力補助 AP，4 つ目が住基 AP である。

マイナンバーカードを用いた本人認証には大きく 2 つの方法が考えられる。1 つ目は内部にある基本情報と各大学が保持している利用者情報との照合であり，2 つ目は内部の電子証明書を用いた認証である。今回は簡単に実装できる，基本情報と利用者情報との照合を用いて，本人確認を行う。

5.2 本人確認の設計

先ほど説明した発行手順における身元確認の方法を設計する。専用アプリでスマートフォンの NFC 機能を用いてマイナンバーカード搭載の券面事項入力補助 AP と通信を行い，基本 4 情報（氏名，住所，生年月日，性別）を読み取る。その際には，マイナンバーカード発行時に作成した券面事項入力補助用暗証番号（数字 4 桁）が必要である。その後，VC 発行時に発行サーバにマイナンバーカードから読み出した基本 4 情報を送り，その情報と発行サーバ側で IDP 認証後に返る属性情報を照合して本人確認の検証を行う。

図 3 にマイナンバーカードとの通信手順を示す。

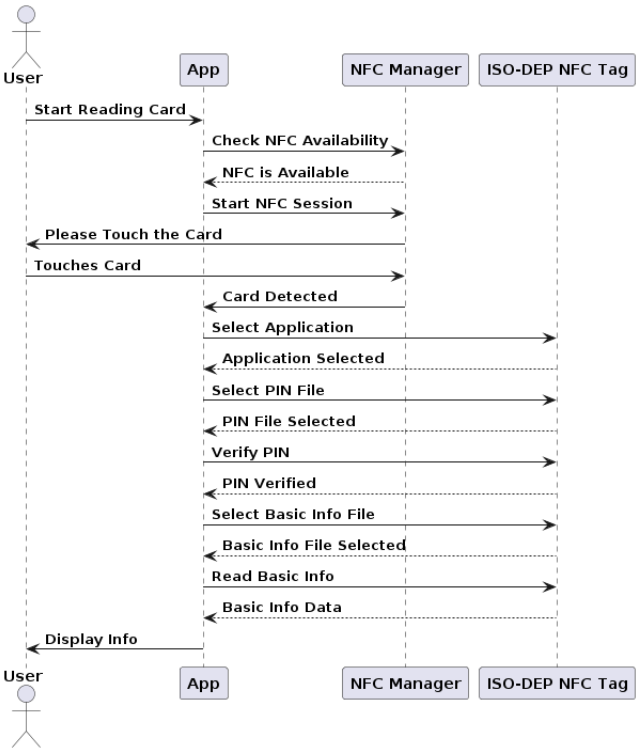

図 3 マイナンバーカードとの通信

属性情報の照合は (**??**) を用いて行う。照合の際，生年月日と性別に関しては一致または不一致の 2 パターンの結果しか存在しないため式 (1) で示すように正誤の 2 パターンに応じてそれぞれの属性に割り当てられた値に重みをかけた値が信頼度を表す。氏名に関してはミドルネームなど名前を表す要素数が人によって異なり，また部分的な一致が存在するため，それを考慮して名前要素の誤数に重みかけた値が信頼度を表すようにする。最終的に得られた信頼度の正負によって本人確認の検証結果を判断する。

$$r = w_1 x_1 + w_2 x_2 + w_3 x_3 \tag{1}$$

- r: 信頼度
- x_1: 名前要素の誤数（0〜N(N: 名前の要素数)）
- x_2: 生年月日の一致（-10, 1）
- x_3: 性別の一致（-1, 0）
- w_1: 重み（-100）
- w_2: 重み（100）
- w_3: 重み（100）

5.3 課題

マイナンバーカードを持たない日本人学生も存在する。所有しない学生が，本人確認が行えないため学生証を発行できないとなると，学生生活において多大な不利益を被る。そこで，本人確認ができた場合には学生証のプレミアム化などで差別化を図るか，マイナンバーカード以外の本人確認によるデジタル学生証発行の仕組みも必要である。

次に留学生の対応が必要である。留学生は在留カードを保持していることが多いため，在留カードでの本人確認も行いたい。

留学生の場合，在留カードやパスポートの表記と，大学への登録情報が異なる可能性がある。中国系の学生の場合，漢字氏名が，日本の漢字を用いる場合と，本国の漢字を用いる場合がありえる。西欧系の学生の場合，ミドルネームを登録する場合と，省略する場合がありえる。

他にも，名前や性別の変更の問題がある。筆者らが所属する九州大学では約 1 %の構成員が結婚などで氏名変更している。変更に応じてデジタル学生証の表記も変更させる仕組みが必要である。

6. 試作と評価

6.1 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。

Shibboleth IdP には，ジェイズ・コミュニケーション社の WisePoint IdP を利用する（共同研究で提供）。デジタ

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

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。執筆時点で IdP が本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 4　試作デジタル学生証の画面

本稿で考察したマイナンバーカードの読み取りは，専用アプリによる基本４情報の読み取りは出来ている。学生証アプリへのマイナカード読み取り機能は試している途中である。今後機能を実装し，式 (1) による確認方法を実現したい。

7. 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。デジタル学生証発行時の本人確認に，マイナンバーカードを用いる手法を提案した。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も説明した。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。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] 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の試作, 情報処理学会 火の国情報シンポジウム 2024, B5-3, Mar.13, 2024.
[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] SMART Health IT, SMART Health Cards, https://smarthealth.cards/en/, 最終アクセス:2023/10/6.
[8] 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.
[9] 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：2024/1/10.
[10] , 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：2024/1/10.
[11] 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.
[12] デジタル庁, マイナンバーカードとは | デジタル庁, https://www.digital.go.jp/policies/mynumber/pros-and-safety#insides, 最終アクセス:2024/5/17.
[13] TakahikoKawasaki(川崎 貴彦), SD-JWT (選択的開示のためのデータフォーマット) #VerifiableCredentials - Qiita, https://qiita.com/TakahikoKawasaki/items/cd2fbbb0bfcfab729d73, 最終アクセス:2024/6/6.