W3C VCを用いたデジタル学生証発行システムの試作と評価

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：インターネットと運用技術シンポジウム論文集. 2024, pp.75-76, 2024-11-28. Information Processing Society of Japan
バージョン：

[ポスター発表] 研究報告

W3C VCを用いたデジタル学生証発行システムの試作と評価

糸川 諒[1,a)]　山口 嵩史[1,b)]　伊東 栄典[2,c)]

Prototyping and Evaluation of a Digital Student ID Issuer using W3C VC

1. はじめに

スマートフォンの普及に伴い，資格情報を表示する新たな仕組みの検討が進んでいる．筆者らが所属する九州大学では現在，IC カードを用いた学生証と職員証を発行しており，特定施設への入室に IC カード学生証・職員証を利用している．IC カードは軽量かつ耐久性に優れているものの，発行時の材料費や人件費などのコストや紛失・盗難のリスクが課題として存在している．我々は IC カード学生証および職員証の機能をスマートフォンで代替する方法について研究を進めている．

以前の研究 [1] では，W3C が提供する検証可能な資格情報（Verifiable Credentials、以下 VC）[3] の仕様に基づいた学生証の実現可能性について議論した．また論文 [2] で身元情報確認にマイナンバーカードを用いる手法を検討した．VC によるデジタル学生証実現により，標準仕様に基づく電子的本人確認が可能となり，学内外の様々な場面での利便性向上やコスト削減が期待される．

本研究では，デジタル学生証システムの発行機能を具体的に実装し，その実行可能性や効果を評価する．特に，LDAP と Keycloak[4] を用いた認証プロセスに注目し，システムの実装結果に基づいてさらなる改良点や今後の展望を検討する．最終的には，より使いやすく安全なデジタル学生証システムの構築を目指す．

2. デジタル学生証発行機能の実装

2.1 デジタル学生証実装概要

試作したデジタル学生証システムを図 1 と表 1 に示す．試作システムは発行局 (Issuer)，認証システム (IdP)，および学生のスマートフォンで構成されている．

発行局では，デジタル学生証の発行を行う．認証システムは Keycloak を用いて構成されており，学生証発行時の認証プロセスを担当する．中央のスマートフォンは，デジタル学生証の発行および保持に使用するデバイスである．発行局および認証局 (Keycloak) と連携しながら，最終的に発行される学生証を保持する．

以前は認証システムに Shibboleth IdP を使用する [1] としていた．しかし，今回の試作では認証システムに Keycloak を用いた．Keycloak は，多くの大学が用いる SAML プロトコル [5] に対応するだけでなく，近年普及しつつある OIDC（OpenID Connect）や OAuth などの認証技術にも対応できる．Keycloak ならば将来の拡張や他システムとの互換性が高まるため，より柔軟な対応が可能になる．

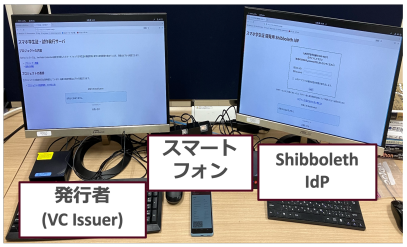

図 1　デジタル学生・試作システム

表 1　試作システムの構成内容

	Issuer	IdP	Smartphone
Machine	Beelink MINI-S12 N95		Sony Xperia ACE-2 SO-41B
OS	Ubuntu 24.04		Android
Middle ware	Flask 3.0.3	Open LDAP 2.6.7 Keycloak 25.0.4	Flutter App -

2.2 デジタル学生証の発行手続き

論文 [1] で提案したデジタル学生証発行手続きを試作システムとして実装した．実装した学生証発行機能手続きを示す．

- Keycloak を用いた認証局での利用者認証および属性情報取得

[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
[2] 九州大学情報基盤研究開発センター
Research Institute for IT, Kyushu U.
[a)] itokawa.ryo.975@s.kyushu-u.ac.jp
[b)] yamaguchi.takashi.228@s.kyushu-u.ac.jp
[c)] ito.eisuke.523@m.kyushu-u.jp

- Keycloak は ID・PW で LDAP サーバに BIND
- 認証成功後に LDAP から利用者の属性情報を取得
- Keycloak は SAML レスポンスを発行局に返す

• 発行局による学生証 VC 作成
- SAML レスポンス (利用者の属性情報) をデコード
- 属性情報から学生証 VC payload (JWT) 作成
- 秘密鍵で JWT に電子署名して JWS 作成

試作した発行局では，ID・パスワード認証でデジタル学生証を発行する．ID・PW 認証は弱いため，他者の学生証発行が可能となる恐れがある．今後はセキュリティ強化のために，マイナンバーカードやデジタル庁が提供する利用者認証システムを活用した，より厳格な本人確認プロセスの導入を検討している．加えて，専用アプリとの連携を強化し，学生証の発行や保持をより簡便かつ実用的に行う仕組みの構築により，システム全体のセキュリティ向上と実用性向上を目指したい．

3. 考察

試作した発行局では，デジタル学生証のデータを発行できた．VC 検証機構は今後作成予定である．ここではデジタル学生証発行に関する課題を議論する．

3.1 システム負荷

試作したデジタル学生証発行処理の負荷を考える．このシステムを評価するため，発行学生証の数を見積もる．九州大学では年間で学部生に約 2,500 枚，大学院生に約 1,100 枚，合計 3,600 枚の新規学生証が年度初め発行する．デジタル学生証の場合，署名用の秘密鍵の更新による再発行が必要になる．鍵の有効期限は年々短くなる傾向がある．鍵の有効期限が 1 年の場合，全学生 2 万人（学部生約 12,000 人，大学院生約 8,000 人）への再発行が必要となる．試作システムのミニ PC サーバでは，1 日で 2 万枚のデジタル学生証を発行できない．

2 つの対処方法を考える．1 つ目はクラウドの仮想マシン利用によるスケーリングである．発行数の多い時期には高性能な仮想マシン（VM）を用い，発行数の少ない平常時は低性能仮想マシンに切り替える．柔軟なスケーリングで，コストを抑えた安定運用を実現できる．2 つ目の対処方法は発行時期の分散である．新入生には 4 月初めに学生証発行が必要であるけれど，在校生への発行時期はずらすことが出来る．学部や学年ごとに発行期限を分散できれば，在校生に若干の不便を強いるものの，システム負荷を軽減できる．実運用する場合，これら 2 つの方法を考えつつデジタル学生証発行の負荷を軽減したい．

3.2 顔写真データ

現在，殆どの大学では物理カード学生証発行のために学生の顔写真データを保持している．しかしプライバシ保護の観点から，オンラインの LDAP や Active Directory には顔写真データを搭載していない．デジタル学生証に本人確認精度向上のために顔写真が必要である．より認証強固な認証手法を備えた LDAP や AD に顔写真データを搭載するか，別の顔写真リポジトリ構築が必要である．自撮り写真を用いる場合，本人の顔写真であることの証明も必要であろう．

3.3 その他課題

電子署名用の鍵管理も課題である．試作段階では鍵のバージョン管理を考慮していない．長期間の安定運用に，電子証明書を自動更新機構や，過去に用いた鍵の保持と参照機構も必要となる．

学生証のライフサイクルも考慮する必要がある．通常の入学卒業以外に，携帯電話紛失，アカウント盗難の対処が必要である．氏名変更や転学部についても考慮しなければならない．再発行の際，過去に発行したデジタル学生証を無効化も必要である．無効化は検証機構と組み合わせて考える必要がある．

4. おわりに

今回，デジタル学生証を実現するために実装したデジタル学生証の発行機能について説明し，実装した学生証発行システムに対する評価を行った．本論文で説明した学生証発行システムでは，Keycloak による認証を活用して学生証の発行を行う．今後は，デジタル学生証システムの検証機能の実装や，スマートフォンアプリを利用した発行および検証機能の試作を進め，その試作システムでの動作検証を行う予定である．

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, 情報処理学会 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, 山口嵩史, 伊東栄典: デジタル学生証発行における身元確認方法の検討, 情報処理学会 第 66 回 インターネットと運用技術研究会 (IOT66), pp.1-6, 2024.
[3] W3C, Verifiable Credentials Data Model v1.1, 2022, https://www.w3.org/TR/vc-data-model/, Accessed 2023/10/5.
[4] Cloud Native Computing Foundation, Keycloak, https://www.keycloak.org/, Accessed 2024/10/6.
[5] 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, Accessed 2023/10/6.
[6] M. Jones; J. Bradley; N. Sakimura, JSON Web Token (JWT), https://www.rfc-editor.org/rfc/rfc7519, Accessed 2023/10/6.