

# 高等教育機関における証明書のデジタル化 留意すべき事項と今後目指すべき方向性

富士榮 尚寛<sup>1),2)</sup>, 阿部 涼介<sup>3)</sup>, 坂口 菊恵<sup>4)</sup>, 貞弘 崇行<sup>2)</sup>, 佐藤 周行<sup>5)</sup>, 鈴木 茂哉<sup>3)</sup>,  
野田 文香<sup>4)</sup>

- 1) 一般社団法人 OpenID ファウンデーションジャパン
- 2) 伊藤忠テクノソリューションズ株式会社 みらい研究所
- 3) 慶應義塾大学大学院 政策・メディア研究科
- 4) 独立行政法人 大学改革支援・学位授与機構
- 5) 大学共同利用期間法人 情報・システム研究機構 国立情報学研究所

naohiro.fujie@ctc-g.co.jp

## Digitalization of Academic Certificates; Matters, and Future Directions

Naohiro Fujie<sup>1),2)</sup>, Ryosuke Abe<sup>3)</sup>, Kikue Sakaguchi<sup>4)</sup>, Takayuki Sadahiro<sup>2)</sup>, Hiroyuki Sato<sup>5)</sup>,  
Shigeya Suzuki<sup>3)</sup>, Ayaka Noda<sup>4)</sup>

- 1) OpenID Foundation Japan
- 2) ITOCHU Techno-Solutions Corporation
- 3) Keio University
- 4) National Institute for Academic Degrees and Quality Enhancement of Higher Education
- 5) National Institute of Informatics

### 概要

高等教育機関が発行する証明書は多岐にわたる。諸外国においてはデジタル化と国境を跨いだ相互運用が試行され始めており、遠からず日本の機関も国外の機関との相互運用を迫られることになる。現在、相互運用に必要な資格枠組みの標準化は UNESCO 規約をベースに、デジタル化方式の標準化は OpenBadge や検証可能な資格情報 (Verifiable Credentials) に関連する技術等により実装が進んでいる。それらの状況を踏まえ日本国内の高等教育機関を含む関係機関においては、国際標準に準拠した資格枠組みの定義およびデジタル化方式について検討・決定を行うことが重要である。

## 1 はじめに

諸外国においては高等教育機関が発行する資格証明の国境を跨いだ相互運用・利活用に関する議論が活発に行われている。しかし日本国内においては資格に関する枠組みについて合意された標準が存在せず、各機関が発行した学位や単位に関する整理は進んでいない。また、相互運用を実現するために重要な役割を果たすデジタル技術に関しても個別の機関単位で採用技術が異なるなど、国内においても相互運用可能な状態となっていない。

一方で 2024 年 4 月にデジタル庁が欧州連合と締結した日 EU デジタルパートナーシップ協定における重点領域に教育分野における資格証明の相

互運用が盛り込まれるなど、国際的な相互運用の流れへの参加は避けられるものではなくなってきている。

本書においては 1.資格枠組み、2.デジタル技術の標準化の動向の分析を行い、今後の国際連携に向け国内の機関が実施すべき事項について論じる。

## 2 学術機関と発行する証明書の区分

学術機関が発行する証明書は多岐にわたる。相互運用について分析を行う前に高等教育機関を含む学術機関の区分、発行する証明書の区分の明確化を行うことが重要である。

### 2.1 学術機関の区分

本書における学術機関 (いわゆる学校) とは、

学校教育法<sup>1)</sup>、および国立大学法人法<sup>2)</sup>に規定される国立大学法人および独立行政法人国立高等専門学校機構、地方独立行政法人法<sup>3)</sup>に規定される公立大学法人、私立学校法<sup>4)</sup>に規定されている学校法人を指すものとする。具体的には、幼稚園、小学校、中学校、義務教育学校、高等学校、中等教育学校、特別支援学校、大学及び高等専門学校が該当する。

## 2.2 学術機関における証明書の区分

大まかに区分して、1. 学術機関が証明書発行機関としてその役割を果たし学習者等に対して発行する学修に関する証明書、2. 民間等の機関が発行し学術機関がその履修証明を利活用するための証明書、3. その他学術機関が発行し民間事業者等が利用する証明書の3種類が存在する。それぞれの証明書は以下の通り整理される。

### 2.2.1 学術機関が証明書発行機関としてその役割を果たし学修者等に対して発行する証明書

高等教育機関が発行する学修に関する証明書は、学術教育において扱われる学位（博士・修士・学士など）と職業教育において扱われる称号（高度専門士、専門士など）に分類される。後述のマイクロクレデンシャルとの対比では、マクロクレデンシャルと称される。

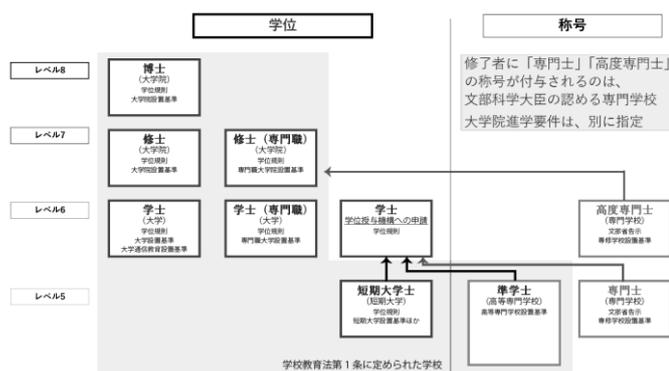


図 1 高等教育機関の授与する学位・称号と日本の教育資格枠組み（試案）との対応

### 2.2.2 民間等の機関が発行し学術機関がその履修証明を利活用するための証明書

学術機関が学位認定を行うために他の学術機関や民間の機関が発行する学修歴証明（いわゆるマイクロクレデンシャル）を利用するケースが存在する。主にリカレント教育の文脈等で利活用さ

れる証明書であり、例を挙げると TOEIC や TOEFL 等の語学資格や履修証明プログラムなどが挙げられる。また、新たな取り組みとして、専門職大学設置基準の中で社会人としての実務経験の単位変換が盛り込まれている。なお、本分野についてはデジタル化の試みが進められており、一般社団法人日本オープンオンライン教育推進協議会 (JMOOC)<sup>1)</sup>や JV-Campus<sup>2)</sup>における OpenBadge<sup>3)</sup>の利活用などが典型である。

### 2.2.3 その他学術機関が発行し民間事業者等が利用する証明書

電子ジャーナル等を利用するために学術機関に所属していることを証明する ID 連携の枠組み（学術認証フェデレーション、学認）や、公共交通機関等が学割や通学定期を発行するために必要な通学経路証明や在学証明（学生証など）も学術機関が発行する証明書の1類型とすることができる。

## 3 デジタル化と相互運用の現状

相互運用を検討するにあたり、関連するステークホルダーの洗い出しを行う必要がある。その上で、相互運用を実現するための要件の整理を行う。

前項に示した学術機関が扱う各種証明書を国内外・産学を問わず他機関と相互に運用するためには、大きく分けて2つの要件が存在する。

- 資格枠組み、機関の適格性認定の枠組み<sup>4)</sup>等に互換性があること
- 各種証明書を効率的・効果的に相互利用するための仕組みが存在すること（典型的には標準仕様に則ったデジタル化の推進）

本項ではステークホルダーおよび各要件について現状を整理する。

### 3.1 関連するステークホルダー

相互運用性を考える上で関連するステークホルダーとして以下が挙げられる。

表 1 関連するステークホルダー

区分	役割	例（シナリオ）
発行機関	学修証明を発行する	大学などの学術機関（学位などの発行） 民間事業者（TOEIC や IT 資格などの発行）

<sup>1</sup> <https://www.jmooc.jp/>

<sup>2</sup> <https://www.jv-campus.org/>

<sup>3</sup> <https://www.ledtech.org/standards/open-badges>

<sup>4</sup> 法的もしくはシステム的な適格性認定を行う仕組みを指す（トラストフレームワークと表現されることもある）

認定機関	発行機関の認定を行う	文部科学省など発行機関を認定する機関（学校教育法に則って認定） 発行機関が運用ルールに則ってシステム運営していることを認定する機関（学認における国立情報学研究所(NII)の役割が該当）
検証機関	学修証明を検証する	大学などの学術機関（留学・入学時など） 厚生労働省・ハローワーク（就業支援など） 民間事業者（学割・通学定期など）

### 3.2 資格枠組み

前項に挙げた各種証明書について、現状の資格枠組みの互換性に関する現状を以下に記載する。

#### 3.2.1 学術機関が証明書発行機関としてその役割を果たし学修者等に対して発行する証明書

学位・称号について、2024年9月現在、日本国内では大学改革支援・学位授与機構（NIAD-QE）がUNESCO規約<sup>5</sup>をベースに次頁に挙げる教育資格枠組み（試案）<sup>5</sup>として取りまとめを試みており、同じくUNESCO規約に準拠している対欧州をはじめとする国々との国際的な相互運用性を確保するためには最も適していると考えられる。事実、欧州におけるEQF（European Qualifications Framework）とのレベルマッピングなど、既に国際連携に関する試みが実行されている。NIAD-QEはUNESCO規約に基づき学校教育法に規定されている高等教育機関（約4,700校）の一覧を保有し、海外の教育機関との対応を公開するセンター（NIC-Japan<sup>6</sup>）を管理している。

ただし現状の課題として、

- 各学術機関における個人の学修歴のデータ化、保管期間のルールの整備が進んでいないこと
- 他国等の機関との間で連携するためのデジタル・インターフェイスの整備は進んでいないこと

が挙げられ、国際連携を含む展開の妨げとなっ

ている。



図 2 日本の教育資格枠組み（試案）

#### 3.2.2 民間等の機関が発行し学術機関がその履修証明を利活用するための証明書

OpenBadge を代表例としてデジタル化は進んでいる一方で、マイクロクレンジンシャルの資格枠組みとの対応については標準化が非常に困難な領域である。職業資格やコンピテンシーなどスキル証明については多岐に渡るため類型化が困難であること、民間資格のレベルの読み替え（TOEIC xxx 点 ↔ 英検 x 級）や単位への変換（英文科では TOEIC xxx 点が要件、他の学科ではそこまで求めない、等）が事情によって様々である等の課題の存在が主な要因である。

まずは国もしくは機関単位でマイクロクレンジンシャルとマクロクレンジンシャルとのマッピングルール（単位への読み替え）を整備し、その上でマクロクレンジンシャルの資格枠組みの互換性確保に付随する形での国際的な相互運用性の実現が期待される。

#### 3.2.3 その他学術機関が発行し民間事業者等が利用する証明書

主に大学等の学術機関が参加する認証・ID シス

<sup>5</sup> 学位授与機構「日本の教育資格枠組み（試案）」  
[https://niadqe.jp/information/higher-education-](https://niadqe.jp/information/higher-education-degree-2/)

[degree-2/](https://niadqe.jp/information/higher-education-degree-2/)

<sup>6</sup> <https://www.nicjp.niad.ac.jp/>

テムのフェデレーション（学認）は国際的な相互運用性を確保するために Kantara Initiative<sup>7</sup>が定める Identity Assurance Framework に準拠する Level of Assurance (LoA) のレベル1（クラシック）の認定を受けた Trust Framework を策定・運用しており、InCommon<sup>8</sup>、eduGAIN<sup>9</sup>等の国外のフェデレーションとの相互運用を実現している。さらに、NIST SP800-63(-3)の基準を学術機関向けに解釈した学認 IAL2/AAL2 を策定し、実現可能性のための実証実験が始まっている。

一方で、在学証明や通学証明など国内に限られた範囲のみで通用すれば良い証明書も存在し、それらの証明書については国際的な相互運用については検討の必要性は少ない。また、国内の民間企業で広く利用されるためには一定の資格枠組みの標準化は必要となるが、学位とは異なり学校教育法により認定された学術機関であることのみを証明できれば十分な場合も多い。

### 3.3 デジタル化の取り組み

相互運用を効率的・効果的に実現するためには資格枠組みの互換性に加えて証明書をやり取りするための方法を定義する必要があり、デジタル化はそのための重要な要素となる。

デジタル化を検討する際、以下の構成要素について決定し合意することが必要となる。

- データモデル
- トランスポートプロトコル
- トラストフレームワーク

なお、決定に当たっては特定のベンダ技術へのロックインを防止することが非常に重要であり、デジュール・フォーラムを問わず国際的に標準として認められ広く活用されている技術を選定し、監査可能性の観点からもオープンソース技術による実装を前提とすべきである。

以下にデジタル化を行う上で検討が必要となる各構成要素について記載する。

#### 3.3.1 データモデル

取り扱う証明書のみならず、発行者、認定者、検証者のエンティティや関連して取り扱われる全てのデータに関する以下の項目についてステークホルダーが合意する必要がある。

- スキーマ: 取り扱うデータセットに含まれ

るべきデータ項目・形式(数値・文字列等)

- データの意味: 取り扱うデータセットに含まれるデータの値の解釈方法
- コンテナ形式: データセットのフォーマット (JSON、XML 等)
- 署名形式 (データにデジタル署名を施す場合): 署名アルゴリズム
- 選択的開示等の付加機能の要否

なお、現時点で主流となっているデータモデルの標準は大きく分けて mdoc (ISO/IEC 18013-5:2021<sup>10</sup>)、および Verifiable Credentials (W3C/VC<sup>11</sup>、IETF/SD-JWT-VC<sup>12</sup>)である。mdoc に関しては Apple や Google のウォレットがサポートすることを表明しているため利用者にとっては利便性が高い一方で、Apple/Google ウォレットの実装が公開されていない（クローズドソース）であること、現時点においては実装できるベンダが特定のベンダに集中する傾向にあることから、mdoc のみをサポートすることは推奨されない。事実、欧州におけるデジタルアイデンティティウォレットの実装ガイドラインでは mdoc と Verifiable Credentials の両方をサポートすることとされているため、日本国内においても同様にオープンソースでの発行者・ウォレット・検証者の実装が可能な状態を目指す必要がある。

また、対象とする証明書の種別によっては上記に挙げたデータモデル標準の上位に定義されたデータモデルやスキーマ標準が存在することがある。その場合、基盤となる下位レイヤーの標準がどのような状態でどのように変化するのかを正しく見極めた上で技術選定を行う必要がある。例えばマイクロレデンシャルとして広く利用されている OpenBadge の次世代バージョンである version 3 は W3C Verifiable Credentials Data Model version 2.0 の上位レイヤーに構成される。しかしながら、W3C において Verifiable Credentials Data Model version 2.0 は 2024 年 9 月時点では勧告候補のドラフト状態であり、今後の仕様が変わる可能性があり、慎重な見極めが必要となる。

#### 3.3.2 トランスポートプロトコル

関係ステークホルダー間で証明書を受け渡す方法についてステークホルダーが合意する必要がある。

<sup>7</sup> <https://kantarainitiative.org/>

<sup>8</sup> <https://incommon.org/>

<sup>9</sup> <https://edugain.org/>

<sup>10</sup> <https://www.iso.org/standard/69084.html>

<sup>11</sup> <https://www.w3.org/TR/vc-data-model/>

<sup>12</sup> <https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/>

ある。例えば API 等のインターフェースの仕様、通信方式等が該当する。これらの方式を検討する上では対面および非対面（オンライン）の両方のシナリオを想定して適切なプロトコルを選定することが重要となる。

前述のデータモデルを扱うにあたり、現時点で主流となっているトランスポートプロトコルには ISO/IEC 23220 シリーズ<sup>13</sup>、OpenID for Verifiable Credential Issuance<sup>14</sup>、OpenID for Verifiable Presentations<sup>15</sup>が存在する。特にオンラインのシナリオにおいてはデータモデルの種別に依存がない（mdoc、Verifiable Credentials についてもサポートしている）OpenID 系のプロトコルを利用することが望ましく、欧州においても OpenID 系プロトコルが採用されている。

なお、前述のとおりデータモデルおよびトランスポートプロトコルの標準規格も複数存在するため、それらを組み合わせたプロファイルを定義し、相互運用を行う対象の間において合意するのが合理的である。同じく欧州においては High Assurance Interoperability Profile (HAIP)<sup>16</sup>を利用するプロファイルとして定めている。

### 3.3.3 トラストフレームワーク

各種証明書の解釈は前述の資格枠組みの相互運用性により解決されるべきであるが、デジタル化に際して主に運用面でのルールを規定し合意することが必要となる。一般的にこれらのルールをトラストフレームワークと呼び、以下の事項を規定・合意する。

- 発行者・検証者の認定要件（適格性、データの管理状態、証明書の発行・失効条件等）
- 認定後の管理・監査要件（適格状態の維持確認サイクル）
- 認定者の適格性（認定機関自体が適切であること）

例えば、国内においては学校教育法に基づき高等教育機関として認定された機関の一覧を NIAD が管理しており、7年毎に機関別認証評価（学位を適切に授与しているかどうか等）を行っている（専門学校など一部例外あり）が、実際のデータのメ

ンテナンスが当該ルールによって実施されていることを監査する仕組み・体制を含め検討し合意を行う必要がある。

先にも述べた、NII が運営する学術認証フェデレーションは加入機関のアイデンティティ基盤が適切にシステム運営されていることを確認・認定するトラストフレームワークを持っており、かつ国際連携しているため、デジタル資格証明を発行する際は本トラストフレームワークを拡張する形で実装を始めるのが適切だと考えられる。

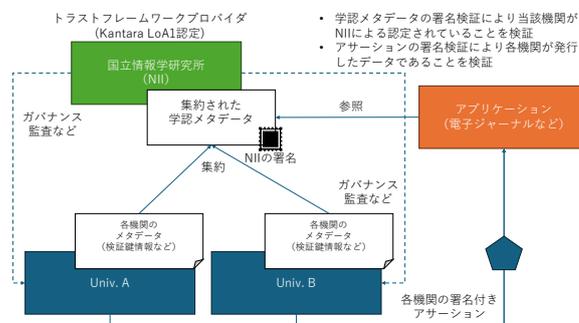


図 3 学認トラストフレームワークの仕組み

なお、デジタル資格証明に利用される Issuer/Holder/Verifier (IHV) モデルにおいては、OpenID Federation<sup>17</sup>のメタデータディスカバリの仕組みを応用する（メタデータを NII から各機関へチェーンさせるなど）ことで同様の効果を得ることができると考えられる。

ここまで挙げた各種要素について検討・合意をすることにより、以下のとおり相互運用性が確保された状態を実現することが可能となる。

- 発行機関が発行した証明書を検証機関が検証可能な状態（真正性の検証<sup>18</sup>）
- 発行機関が発行した証明書を検証機関が確認可能な状態（スキーマの検証<sup>19</sup>）
- 発行機関が発行した証明書を検証機関が判断可能な状態（適格性の検証<sup>20</sup>）
- 証明書の発行機関が認定期間によって認められた機関であることを検証機関が検証可能な状態（真正性の検証）
- 証明書の発行機関が認定期間によって認められた機関であることを検証機関が確

<sup>13</sup> <https://www.iso.org/standard/74910.html>

<sup>14</sup> [https://openid.net/specs/openid-4-verifiable-credential-issuance-1\\_0-ID1.html](https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-ID1.html)

<sup>15</sup> [https://openid.net/specs/openid-4-verifiable-presentations-1\\_0-ID2.html](https://openid.net/specs/openid-4-verifiable-presentations-1_0-ID2.html)

<sup>16</sup> [https://openid.net/specs/openid4vc-high-](https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-sd-jwt-vc-1_0.html)

[assurance-interoperability-profile-sd-jwt-vc-1\\_0.html](https://openid.net/specs/openid-federation-1_0.html)

<sup>17</sup> [https://openid.net/specs/openid-federation-1\\_0.html](https://openid.net/specs/openid-federation-1_0.html)

<sup>18</sup> 改竄されていないことを確認

<sup>19</sup> データ項目が揃っていることを確認

<sup>20</sup> 業務的に利用可能な状態であることを確認

認可可能な状態（スキーマの検証）

- 証明書の発行機関が認定期間によって認められた機関であることを検証機関が判断可能な状態（適格性の検証）

なお、国や規則によっては検証機関が認定機関によって認定を受けていることを発行機関や利用者によって検証できる必要がある場合も存在するため、相互運用を検討する相手ごとに確認を行う必要がある。この課題に対応するために OpenID Foundation<sup>21</sup>や Secure Identity Alliance<sup>22</sup>などの非営利団体や国連開発プログラムなどが協力して運営する国際的な相互運用を目指すコミュニティである SIDI Hub（Sustainably and Interoperable Digital Identity Hub）<sup>23</sup>の 2024 年度のテーマの一つとしても教育クレデンシャルが取り上げられており、日本国内からも取り組みへの貢献が期待される。

### 3.4 国際および国内の動向

ここまで見てきた資格枠組みおよびデジタル化に関する諸外国ならびに日本国内の取り組みの現状について記載する。

#### 3.4.1 国際動向

大きな潮流として、UNESCO 規約の存在もあり、マクロクレデンシャルの資格枠組みについてはある程度は整備が進んでいる。しかしながらデータ形式を含む互換性の担保の課題があり、国家間での相互運用・連携は進んでいない。

また、民間資格の単位変換などマイクロクレデンシャルとマクロクレデンシャルの紐づけについては各国ともに今後の課題となっている状態である。特に米国は OpenBadge を用いた民間資格やトレーニングを積極的に学術機関で活用する方向性で進んでいるが、他国においてはそこまで踏み込んだ社会実装には至っていない。特に推進の障壁となるのがマイクロクレデンシャルに関するビジネスモデルが描きにくい点である。例えば edX など有償でクレデンシャルを発行する事業者も、発行したクレデンシャルの利用先が増えない等の課題に直面しておりビジネス面では苦戦を強いられている。

表 2 諸外国における取り組み例（マイクロクレデンシャル）<sup>[6][7]</sup>

国	取り組み	特徴・課題
中国	CSSD（Center	卒業証書と学位証書の

<sup>21</sup> <https://openid.net/>

<sup>22</sup> <https://secureidentityalliance.org/>

	for Student Services and Development)	認証業務を一本化して対応。学習者の単位は各機関ではなく CSSD に先に登録され、その後各機関へ連携される。就職などの際も CSSD を通じてデータが提供される
韓国	生涯学習ポータル	単位銀行として統一的な可視化が進んでいる
欧州	Europass、EQF	資格枠組みの整理が進んでいる。学習者自身でマクロ・マイクロの各種クレデンシャルを登録する仕組み（Europass）となっている。マクロクレデンシャルに関しては機関登録も可能である。

#### 3.4.2 日本国内の動向

前述した通り、NIAD-QE が「日本の教育資格枠組み（試案）」を取りまとめているが、公式なものとして広く普及している状況ではない。また、特にマイクロクレデンシャルについては JV-Campus がキュレーションのためのプラットフォーム事業を展開、また JMOOC がオンラインコースの提供～履修証明の発行を行っている。他にも各大学の単位で独自の実装を行いデジタル学生証の提供を行うケースも散見される。

表 3 国内における資格証明の状況と課題

資格区分	状況	課題
学術機関が証明書発行機関としてその役割を果たし学習者等に対して発行する学修に関する証明書	NIAD-QE が「日本の教育資格枠組み（試案）」を取りまとめて発表している	公式な資格枠組みとして認知されていない
民間等の機関が発行し学術機関がその履修証明を利活用	JV-Campus、JMOOC、民間企業などが証明書	単位とのマッピングの整理が進んでいない

<sup>23</sup> <https://sidi-hub.community/>

用するための 証明書	( OpenBadge 等)を発行して いる 一部の大学(サイ バー大学や 産業能率大学 など)は外部資 格を単位とし て認定してい る	
その他学術機 関が発行し民 間事業者等が 利用する証明 書	大学毎に独自 の技術仕様で 実装している	標準的な仕組 みがない(標 準技術を利用 していないケ ースが多数存 在する) 民間事業者等 への展開が進 んでいない <sup>24</sup>

表 4 デジタル学生証の実装と利用技術の例

機関名	概要	ベンダ/利用 技術等
芝浦工業 大学 <sup>25</sup>	デジタル証明書を 発行	Digitary core Hyperledger Indy
東洋大学 <sup>26</sup>	デジタル証明書を 発行	Digitary core Hyperledge Indy
千葉工業 大学 <sup>27</sup>	NFT を使って学生 証を発行	Pitpa NFT
慶應義塾 大学 <sup>28</sup>	Verifiable Credentials を利用して学生証 を発行(実験)	Microsoft Verifiable Credentials
大阪大学 <sup>29</sup>	顔認証を使ったデ ジタル学生証	NEC Bio-IDiom
追手門学 院大学 <sup>30</sup>	学生向けアプリへ の学生証機能の導 入	不明

<sup>24</sup> 例) JR 東日本サイト: 電子化された学生証(デジタル学生証)につきましては、当社においては、旅客営業規則に定める『証明書』および『通学定期乗車券購入兼用の証明書』には該当せず、その効力は認められません。

[https://jreastfaq.jreast.co.jp/faq/show/3266?category\\_id=14&site\\_domain=default](https://jreastfaq.jreast.co.jp/faq/show/3266?category_id=14&site_domain=default)

<sup>25</sup> [https://web.sic.shibaura-it.ac.jp/Digital\\_certificate](https://web.sic.shibaura-it.ac.jp/Digital_certificate)

<sup>26</sup> <https://daigakujihou.shidaiaren.or.jp/pickup/pickups/4>

※過去のリリースを含む

※他にもデジタル学生証アプリ(もしくは基盤)を提供するベンダも存在している(例:株式会社ジェイ・エス・エス「MyID/がプリ!」<sup>31</sup>や株式会社Recept「proovy/学ナビ」<sup>32</sup>など)

#### 4 今後に向けて

学術機関が取り扱う証明書の国際的な相互運用を目標とすると、はじめに対象とする相手国と想定するシナリオ・ユースケースにおける証明書の種別やレベルを明確化した上で、両国の現在の状況を分析する必要がある。その上で、UNESCO規約や Verifiable Credentials などの資格枠組みとオープンなデジタル技術標準への準拠を基本として両国間での適用に向けた課題分析～導入に向けたステップを策定する必要がある。

なお、取り組みにあたり各国の機関や採用する技術の標準化を行う団体など、適切なステークホルダーの巻き込みが非常に重要となることは言うまでもない。

#### 参考文献

- [1] e-Gov 法令検索、学校教育法、第一章、第一条、令和5年4月1日施行  
<https://laws.e-gov.go.jp/law/322AC0000000026>
- [2] e-Gov 法令検索、国立大学法人法、第一章、第二条、令和6年4月1日施行  
<https://laws.e-gov.go.jp/law/415AC0000000112>
- [3] e-Gov 法令検索、地方独立行政法人法、第一章、第二条、令和6年6月12日施行  
<https://laws.e-gov.go.jp/law/415AC0000000118>
- [4] e-Gov 法令検索、私立学校法、第一章、第二条、令和5年5月8日施行  
<https://laws.e-gov.go.jp/law/324AC0000000270>
- [5] 高等教育資格承認情報センター「高等教育の資格の承認に関するユネスコの規約」  
<https://www.nicjp.niad.ac.jp/site/unesco-conventions.html>
- [6] 坂口 菊恵・中村 優、マイクロクレデンシャ

<sup>14/</sup>

<sup>27</sup> <https://www.it-chiba.ac.jp/topics/pr20220818/>

<sup>28</sup> <https://www.keio.ac.jp/ja/press-releases/2020/10/26/28-75892/>

<sup>29</sup> <https://www.cmc.osaka-u.ac.jp/?p=9531>

<sup>30</sup> <https://www.asahi.com/thinkcampus/article-110459/>

<sup>31</sup> <https://myid.co.jp/student-id-card/>

<sup>32</sup> <https://proovy.recept.earth/gakunavi>

ルと単位銀行、大学質保証フォーラム・ポスター展示

- [7] 坂口 菊恵、学修履歴データの通用性担保に向けた国際動向、大学等の質保証人材育成セミナー、令和5年3月13日

※脚注等の各 URL の最終アクセス・確認日：  
2024年9月30日