

学術機関の発行する証明書のための標準属性とその利用シーン

2025-04-02

Editor:

佐藤周行 (NII)

鈴木彦文 (NII)

1. はじめに

大学 DX の名のもとに、大学内外のさまざまなリソースをデジタルの形で提供することが当たり前のように議論されるようになった。教育、研究に関係するものについては特に議論が盛んである。

歴史上、大学がさまざまな場面で信頼の起点となってきたことから、大学の業務として学生や教職員に関する各種事項を証明することが重要であると認識されている。学生証が世界で一定のレベルで受容されているのは、世界的に大学が業務として行う「証明」に信頼がおかれていることを意味する。これら証明業務は、大学等が人手をかけてその真正性を担保してきた。自然、出頭しての本人確認等、コストがかかるものであった。近年、これらのデジタル化が議論の俎上に上ってきた。オンラインサービスの提供に大学等の証明を与えて、より利便性を高めるのが目的とされた。証明の対象としては、学生の身分証明、在学証明から、卒業生に対する卒業証明、在学事項証明、また一番複雑なものとして成績証明がある。証明を起点として学生や教職員にベネフィットを与えるビジネスは日本においても広く展開されているが、物理的なカードや紙面で発行される証明書の代わりにデジタル形式で証明書が発行されることが今後期待される。

この際に問題になるのは、従来、証明書におかれてきた信頼を維持することである。デジタルデータには本質的に偽造やコピーの危険が伴う。これらの可能性を排除しておくことが、証明書のデジタル化には本質的に重要である。この技術のために電子署名に加えて、所持証明技術が応用される。証明業務はこれらの技術の上に立っている。

証明書のデジタル化に際し、業務を効率化することも必要である。従来、大学等が独自で行っていた業務は、デジタル化によって証明業務の需要が増すと、業務の負荷が高くなることが予想される。証明書の発行業務を標準化し、さらに発行された証明書が標準的な形式を持つことが、サービスを提供する側にとっての本質的な利益になる。前者では、証明書を発行する業務を SaaS として展開するときに、各大学等から属性として提供されるデータが統一された形式を持つことが必要である。後者では、証明書を評価してアクションを起こす事業者は、統一された証明書の形式を要求するの

は当然である。

国立情報学研究所（NII）は、2024 年度、各種証明書のデジタル化のための各種実証実験に技術を提供してきた。具体的には、Felica Networks 社が展開したデジタル学生証の PoC のために使用属性の標準案を提供し

(<https://www.felicanetworks.co.jp/other-businesses/student-id.html>) た。さらにデジタル庁が JR 西日本とともに行ったデジタル在学証明書のために発行のための属性の標準案を提供した

(https://www.westjr.co.jp/press/article/items/250324_00_press_Mynumbercard_gaku_seikatuyou.pdf)。これらの経験を踏まえ、証明書発行のための標準属性セットの策定には大きな意味があるという結論に至った。

本稿では、求められる標準化のうち、証明書の発行業務を標準化するために、各大学等から送出されるデータの標準形式を定める。送出属性は従来の IdP から送出されてきた属性の範囲を大きく超えるため、IdP を拡張した属性プロバイダの構築とその運用を提案する。その信頼度を定めるため、従来の認証の保証度（IAL/AAL）に加えて、属性の保証度を議論する。さらに、具体的な利用シーンに即して身分証として使われるケース、証明書として文面を評価することを想定するケース、オンラインサービス利用のために認証トークンとして使われるケースそれぞれについて必要な属性と保証度を議論する。

2. 関連する技術と研究

学術機関で用いる属性を定めたもののうち、代表的なものは eduPerson[1]である。主としてオンラインでアサーションを交換するときの標準スキーマとして定義されている。各種証明に使うことは想定されていない。これを特に日本語に拡張したものが GakuNin スキーマ[2]である。これも各種証明に使うことを想定したものではない。

これらとは別に、学術機関で使う属性を LDAP スキーマとして定義したものに EU で定める SCHAC [3] がある。ここで定められている属性を見ると、各種証明を表現するためのものが概ねそろっている。SCHAC に準拠し、言語環境情報を日本語に設定することで SCHAC を標準属性セットとして使うことができる。ただ、GakuNin スキーマはその運用方針を取らず、日本語に関しては別途属性名を定めることにしている。今回はその方針に従い、また最小限の属性セットを定めることで証明書発行のための属性セットの性格付けを明らかにすることを目指す。

SCHAC を標準属性セットとして使用する場合は、日本と EU の文化の違いを吸収しきれない可能性があることである。たとえば、日本の在学証明に標準的に記載される入学年度についての記述がない。

3. 対象となる証明書と利用シーン

大学で発行される証明書のうち、具体的に以下を対象にする。

3.1 身分証

1. 学生証
2. 職員証

これらは、証明書の本人所持証明が必要になる。所持証明ができれば、オンラインサービスの際の認証トークンとして利用することが可能になる。このための属性を考慮する。

3.2 その他の証明書

1. 在学証明書
2. 卒業証明書

これらは、証明書の本人所持証明が必ずしも必要ではない。所持証明が必要な場合は、別途手段を講じる。具体的には、他の証明書と属性値を突合させる、使用に当たって認証を求める等が考えられる。そのための属性を併せて考慮する。

3.3 今回、対象外とする証明書

成績証明書は、大学が発行する証明書の中で発行プロセスが最も複雑なものである。このデジタル化は OpenBadge[4]を含めて他で精力的に論じられており、本稿では検討の対象外とする。

4. 発行モデルと関係者

4.1 従来の IdP/SP モデル

従来のアイデンティティ連携では、処理がオンラインで行われることを前提としている。利用者は IdP にアクセスして自分の属性情報を RP に提供し、RP はそれを評価する。この時に IdP と RP が直接間接に同じトラストに参加し、オンラインで情報を共有するモデルになっている。

4.2 IHV モデルにおける証明書の役割

これに対して、IHV モデル (three party model) では、発行者と検証者がオンラインで結合していることを要求しない。VDR を通じて同じトラストに参加していることを確認するものの、検証の対象になるのは、所持者の持つ文書である。文書の発行者が信頼できることが VDR で保証される。また、検証対象の文書が保持者のものであることが求められる時にどう保証するかも問題になる。保持者の視点からは、検証として文書を要求する側が信頼のおけるものであるかどうか確認しなければならない。これらの事項は検討が始まっており、特に EUDIW の ARF[5]でウォレットの運用のためのアーキテクチャが提案されている。

4.3 信頼の起点

属性は属性プロバイダから提供されることを想定するが、これを学務又は人事 DB と直結させて運用すべきである。IAL についても、同様の議論があり、IAL2 以上での運用には、直結性を条件としてきた[6]。属性を提供するのが学務又は人事 DB であることを考えると、これ「のみ」を信頼の起点として、組織が真正性を保証するようにすべきである。

4.4 SaaS としての証明書発行システム

証明書発行システムの運用の負担がどの程度になるのかは、様々な要素を考える必要があるが、外部事業者発行を委託することも一つの手段である。その際に、機関は、CoC (Code of Conduct) の確認をするとともに、署名者 (通常学長レベル) 情報の交換と署名のための電子証明書の運用委託について前もって契約を結ばなければならない。この議論は別稿で行う。

5. 標準属性

以上の対象証明書と利用シナリオをカバーするように、証明書発行のための標準属性セットを以下に定める。定めるときは、その属性の信頼の起点と表現スキーマを併せて記す。

5.1 事項証明に使われるもの

5.1.1 本人に関する属性

姓： sn, jasn

名： givenName, jaGivenName

その他の名前情報： displayName, jaDisplayName

誕生日： gakuninBirthDate

これらの属性は、本人情報ではあるが、機関は責任を持って値を保証しなければならない。日本では、通常高校からの持ち上がりの情報でこの値が設定され、十分信頼できるものとみなされている。displayName は、本人の申し出をそのまま、または本人がセルフサービスで設定することを許容するものがある。この属性が送出された場合、利用する側は組織がどの程度の保証度を与えるかについての運用には注意すべきである。

5.1.2 機関が保証する属性

機関名： o, jao

部局名（複数）： ou jaou

身分： eduPersonAffiliation eduPersonScopedAffiliation

身分証番号（学生証番号）： gakuninScopedPersonalUniqueCode

入学日時： gakuninEnrollDate

有効期限： gakuninExpiryDate

これらは、機関で管理する学務または人事 DB に格納されているはずの情報である。

5.2 身分証として使うときに必要になる属性

顔写真： jpegPhoto

5.3 オンライン利用での認証トークンとして利用するときに必要な属性

ePPN: eduPersonPrincipalName

email: mail

これらは、オンライン利用時に認証トークンとして身分証を利用するときに、R&S[7]として送出が求められるものである。この値を保証するのは、機関の IdP である。IdP の値は学務又は人事 DB を信頼の起点とすることを前提とし、さらに ePPN は、IdP 自身が採番し、信頼の起点とならなければならない。

これらを附録 A にまとめる。

6. 実装に当たってのノート

6.1 アサーション作成時に定義する必要のある属性

送出データの信頼度を表現するために、属性プロバイダは、以下の値を送出してもよい。

保証度 eduPersonAssurance

IAL 確認手段 gakuninIdentityAssuranceMethodReference

6.2 LDAP 以外で DB を構築する際のノート

IdP のバックエンドにいる DB として LDAP を用いるのは一般的であるが、それ以外の DB を用いることもある。現時点でも SQL が採用されていることを観察している。

この場合、OU 等、複数の値の設定を許すものについて発行者と IdP が何らかの取り決めをすることが求められる。本稿では規定しないが、名前空間に倣って :: を区切り記号としてもよい。

6.3 属性の信頼度

証明書の性格上、記載事項は、属性プロバイダが高い保証度を以て送出しなければならない。信頼度の高い運用をされている学務又は人事 DB に格納されているか、そこから直接計算される属性に高い保証度を設定するのは合理的である。その他の場合、学生等のセルフサービスで属性を設定できるようにしているところがあるが、その部分の保証度を高く設定してはならない。高い保証度を持つ属性については属性プロバイダの運用ポリシーとして記載しなければならない。

6.4 卒業生等の収容

卒業証明や在学事項証明は、大学を離れた人に対する重要なサービスである。しかし、現状の日本では、この種のサービスを展開するための DB の構築が進んでいない。さらに、サービスを開始するには、卒業生としての身元確認と、当人が本当に主張する卒業生であるかの確認についてのオンラインでの合理的な手法が確立されていないので、なりすましについてのリスクが無視できない。現状では、オンラインでの確認の開発が進んでいないことから、今回は卒業証明に関する属性の定義を見送る。将来卒業日時等に対応する属性を卒業生 DB で定義・運用することが必要になるだろう。

6.5 文字コードについてのコメント

日本語処理の場合、文字コードの問題は本質的なものとして悩みの種になってきた。特に SaaS として発行業務を請け負う場合、また RP に対してデジタル認証アプリ等他の証明書と突合して何かを証明する場合、文字コードの統一した運用基準が必要になる。特に、UTF-8 で定めのない文字を外字として運用することができないため、jaDisplayName 等を用いて、合理的な妥協策を講じる必要がある。

7. おわりに

本稿では、学術機関が証明書発行を可能にするような属性プロバイダを運用する場合に必要な標準属性セットを定義した。

参考文献

- [1] REFEDS: eduPerson <https://github.com/REFEDS/eduperson>
- [2] 学認: <https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=12158166>

[3] REFEDS:

<https://wiki.refeds.org/display/STAN/SCHAC+Releases?preview=/44957731/128909315/SCHAC%2B1.6.0-final.pdf>, 2022.

[4] Open Badges <https://openbadges.org/>

[5] EU Commission: EUDIW ARF, <https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/>

[6] 学認次世代認証連携検討作業部会: IAL2 の新学認での運用に当たって (案)

<https://gakunin.jp/sites/default/files/2021-11/IAL2%E3%81%AE%E6%96%B0%E5%AD%A6%E8%AA%8D%E3%81%A7%E3%81%AE%E9%81%8B%E7%94%A8%E3%81%AB%E5%BD%93%E3%81%9F%E3%81%A3%E3%81%A6%EF%BC%88%E6%A1%88%EF%BC%89.pdf>, 2021.

[7] REFEDS: Research and Scholarship, <https://refeds.org/category/research-and-scholarship>

附録

A. 属性一覧

Name	Schema	意味	文字コード
OID :			
sn	person	姓	Latin
OID: 2.5.4.4			
jasn	GakuNin	日本語姓	UTF-8
OID: 1.3.6.1.4.1.32264.1.1.1			
givenName	person	名	Latin
OID: 2.5.4.42			
jaGivenName	GakuNin	日本語名	UTF-8
OID: 1.3.6.1.4.1.32264.1.1.2			
displayName	inetOrgPerson	Latin での表示名	Latin
OID: 2.16.840.1.113730.3.1.241			
jaDisplayName	GakuNin	日本語表示名	UTF-8
OID: 1.3.6.1.4.1.32264.1.1.3			
gakuNinBirthDate	GakuNin	誕生日	Date
OID: 1.3.6.1.4.1.32264.1.3.3			
o	inetOrgPerson	組織名	Latin
OID: 2.5.6.4			
jao	GakuNin	日本語組織名	UTF-8
OID: 1.3.6.1.4.1.32264.1.1.4			
ou	inetOrgPerson	組織単位名	Latin
OID: 2.5.6.5			
jaou	GakuNin	日本語組織単位名	UTF-8
OID: 1.3.6.1.4.1.32264.1.1.5			
eduPersonAffiliation	eduPerson	職種等	Latin
OID: 1.3.6.1.4.1.5923.1.1.1.1 値は ("faculty", "staff", "student", "member")			
eduPersonScopedAffiliation	eduPerson	職種等	Latin
OID: 1.3.6.1.4.1.5923.1.1.1.9 (スコープは@で区切る)			
gakuninScopedPersonalUniqueCode	GakuNin	学生（職員）番号	Latin

OID: 1.3.6.1.4.1.32264.1.1.6			
gakuninEnrollDate	GakuNin	入学（採用）日	Date
OID: 1.3.6.1.4.1.32264.1.3.1			
gakuninExpiryDate	GakuNin	券面の有効期限	Date
OID: 1.3.6.1.4.1.32264.1.3.2			
jpegPhoto	inetOrgPerson	写真	Binary
OID: 0.9.2342.19200300.100.1.60			
eduPersonPrincipalName	eduPerson	Fed 内一意名	Latin
OID:1.3.6.1.4.1.5923.1.1.1.6			
mail	inetOrgPerson	メールアドレス	Latin
OID: 0.9.2342.19200300.100.1.3			
eduPersonAssurance	eduPerson	保証度	Latin
1.3.6.1.4.1.1466.115.121.1.15			
gakuninIdentityAssuranceMethodReference	GakuNin	IAL 確認手段	Latin
OID:			