デジタル学生証の標準様式と発行シナリオ（mdoc 版）

2025-04-16

Editt
佐藤周行（NII）
鈴木彦文（NII）

1. はじめに

大学等における学生証や職員証は身分証として従来から信頼性で高い評価を得てきた。その信頼性の高さにより、偽造は大きなニュースになる。最近のオンライン完結型のサービスを目指す教育 DX では、証明書のデジタル化が重要な要素となる。従来得ていた高い信頼度をそのままにして運用するには、様々な技術のサポートが必要である。

特に身分証として利用する場合には、券面情報の真正性に加えて、本人所持の保証が必要である。後者は、貼付された顔写真と所持人の顔の突合が従来からなされてきたが、認証技術の応用により、より信頼性の高い確認が可能になってきた。

デジタル身分証の利用には、サービスを提供する側（検証者）の視点が欠かせない。デジタル身分証を各大学が個別に定める仕様で実装した場合、検証者は個別対応を求められる。現状はそうなってきており、このままでは検証者の経済的な負担が大きくなる。デジタル学生証の標準仕様の制定は急務である。

mdoc は、ISO/IEC18013-5 として制定された国際標準である。これらの規格に従ってデジタル認証アプリやモバイルデジタル運転免許証が公開・公開予定である。身分証の要件をこの上に立って定めることは、標準化の観点からも重要である。

mdoc は、実装に際してスマートフォン内のセキュアエレメントの利用等により、強い本人所持証明ができる。デジタル認証アプリやモバイルデジタル運転免許証が mdoc を採用しているのも、この機能が利用できることが大きい。　身分証として利用するということは、デジタル世界における認証トークンとしてデジタル学生証を利用できる可能性を持つということでもある。認証トークンとして必要な uid に相当するデータを格納しておくことでこれが可能になる。この点からもデジタル学生証に必要な機能を定める。さらに、認証トークンとしての利用は、デジタル学生証を起点とする派生 ID の生成を可能にする。この際の信頼の起点となれるように、属性の値保証とともに所持証明を与えることが本質的に必要である。

本稿は、mdoc を利用してデジタル学生証を発行、運用するにあたり、発行の際の標準を定めるものである。具体的には、発行に際して券面情報を送出する属性プロバイダ、mdoc のエレメント、また SaaS として発行を外部に委託する場合の契約上の留意点について、標準仕様を定める。

2. 発行モデルと属性プロバイダ

発行は本人が大学に申請し、大学は発行側（大学内又は大学外の発行サーバ）に対して必要な属性を送出する。発行された mdoc 形式のデジタル学生証は、スマートフォン等に格納し、本人所持証明ができる状態にする。本人所持証明には、mso が利用できる。

発行には、顔写真を含む属性が必要だが、これらは通常 IdP が扱うものではない。NII は[1]で属性の標準仕様を定めた。デジタル学生証の発行サーバは、標準仕様に従って送出される属性を使用して、mdoc 形式の身分証を発行する。

発行されたデジタル学生証は、検証者に選択的提示を経て、学生証の属性の全部または一部を提示し、検証者にサービスを要求する。検証者は、通常のサービスプロバイダの他に組織の IdP であってもよい。この場合、デジタル学生証は認証トークンとして利用することになる。認証トークンとして利用するとき、派生 ID のソースとなっても良い。

デジタル学生証には高い信頼度が求められることを述べたが、それを保証するのが属性プロバイダが送出する属性の保証度と、送出を要求する際に組織 IdP から求められる IAL/AAL である。これらの保証度は十分高いものでなければならない。

3. 学生証を mdoc で発行するための標準属性

附録 A.に、[1]で定めた属性プロバイダの持つべき標準属性を載せる。発行の際はこの全部または一部を利用する。

属性プロバイダからは送出されないが、発行に必要なデータとして、発行組織の代表者名と対応する、ISO/IEC18013-5 で定める形式の電子署名用証明書と、視覚的に訴えるものとして組織のロゴがある。これらは発行側で、あらかじめ用意しておくべきである。

4. 属性プロバイダから送出される属性と mdoc の標準属性のマッピング

mdoc 側は学生証用の名前空間と、その中の要素名を定める。具体的に、属性プロバイダから送出される属性とのマッピングの形で以下に定義する。mdoc の基本となる名前空間は org.iso.23220.1 である。拡張として org.iso.23220.1.jp.gakunin.1.id を定める（現時点で申請はしていない）

ソース属性	mdoc element ID	Namespace	Type
sn	family_name_latin1	23220.1	L
jasn	family_name_unicode	23220.1	U
givenName	given_name_latin1	23220.1	L
jaGivenName	given_name_unicode	23220.1	U
displayName	display_name_latin1	23220.1	L
jaDisplayName	display_name_unicode	23220.1	U

eduPersonAffiliation	person_affiliation	拡張	L
eduPersonScopedAffiliation	person_affiliation	拡張	L
gakuninScopedPersonalUniqueCode	personal_id	拡張	L
o	issuing_authority_latin1	23220.1	L
jao	issuing_authority_unicode	23220.1	U
ou	organizational_unit_name_latin1	拡張	L
jaou	organizational_unit_name_unicode	拡張	U
gakuNinEnrollDate	issue_date	23220.1	FD
gakuNinExpiryDate	expiry_date	23220.1	FD
gakuNinBirthDate	birth_date	23220.1	FD
jpegPhoto	portrait	23220.1	B
eduPersonPrincipalName	document_number	23220.1	L
mail	email_address	23220.1	L

L: Latin U: UTF-8, FD: Full Date, B: BST

属性プロバイダは、属性の値を eduPersonAssurance をともに送出することにより一括して保証する。[1]で問題を指摘したが、displayName については、組織によって運用形態が異なることが予想されるので、別途 CrP（Credential Policy）により確認するべきである。

個人の属性の他に、組織が管理する以下の属性がある。これらは属性プロバイダからは提供されずに、発行側が管理する。

mdoc Element ID	Namespace	用途	学生証の時の値
issuing_authority_logo	拡張	大学ロゴ	大学の定めるもの
president_name	拡張	発行者	学長名
document_type	23220.1	証明書種類	学生証のときは STUDENT.1 職員証のときは ACADEMICEMPLOYEE.1 に固定
issuing_country	23220.1	発行国	JP

これらを附録 B にまとめる。

これらの要素名の他に、必要に応じて拡張をしても良い。例えば、誕生日が属性として送出されたら、それらから、18 歳以上等のフラグを表す属性を設定しても良い。この情報は age_over_NN として ISO/IEC 23220-1 に定義されているので、それに従わなければならない。また、document_type として STUDENT.1 と ACADEMICEMPLOYEE.1 以外の値を取

り、それが意味を持つようにしても良い。

認証トークンとして用いるときには ePPN を利用する。現状の R&S[2]では、ePPN は永続性を要求されていることに注意すべきである。また、R&S で要求する shared user identifier, person name, email address, affliation は属性プロバイダから送出可能になっていることを前提にして良いが、一部の属性が送出されない場合、部分的な属性を格納するのでも良い。

これら属性の全部または一部を券面情報とし、その値の真正性を保証するために、大学等が持つ電子証明書で全体を署名しなければならない。

5. 提示を許す検証者のリスト

認証トークンとして利用する際には R&S に従って属性を送出するので、組織が属しているフェデレーションが eduGain に参加している限り、問題にしない。

検証者が R&S を超える属性を要求する場合、デジタル学生証をその検証者に提示してよいかは学生証を運用する大学等で判断しなければならない。このとき、検証者の示す行動規範を評価しなければならない。さらに提示することを許容する検証者のリストを作成して管理しなければならない。この運用は学生証を格納するウォレット（大学アプリ）の機能として提供してよい。

6. 失効を含むライフサイクル管理

デジタル学生証発行側は、デジタル学生証の失効リストを管理しなければならない。失効は、学生の卒業、休退学、格納デバイスの紛失等によって任意のタイミングで起こり得る。発行側は、発行された学生証の document_number を適切に管理し、失効情報を適切な形で公開しなければならない。

7. セキュリティの考慮

学生証としての利用がオンラインに限定されず、券面の表示と視認によるなんらかの権限付与がなされることが予想される。その場合、視覚効果の高い大学ロゴを適切に含めて視認の効果を上げるべきである。

8. 学生証発行を外部委託する場合の留意事項

デジタル学生証の運用の負荷が高いと判断する場合、発行、運用を SaaS に外部委託してもよい。外部委託契約には、データ保護についての行動規範の提出を求め、それを評価しなければならない。

9. おわりに

デジタル学生証の発行に当たり問題となる属性と mdoc 要素名の定義を行った。さらに運用に当たっての留意点をあげた。

参考文献

[1] 佐藤, 鈴木 Ed. 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.

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

附録

A. 標準属性

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	UTF-8
OID: 1.3.6.1.4.1.5923.1.1.1.1　値は（"faculty", "staff", "student", "member"）			
eduPersonScopedAffiliation	eduPerson	職種等	UTF-8
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:			

B. mdoc 内でデジタル学生証（職員証）に利用する属性

mdoc element ID	Namespace	Type
family_name_latin1	23220.1	Latin
family_name_unicode	23220.1	UTF-8
given_name_latin1	23220.1	Latin
given_name_unicode	23220.1	UTF-8
displayName		Latin
jaDisplayName	拡張	UTF-8
person_affiliation	拡張	Latin
personal_id	拡張	Latin
issuing_authority_latin1	23220.1	Latin
issuing_authority_unicode	23220.1	UTF-8
organizational_unit_name_latin1	拡張	Latin
organizational_unit_name_unicode	拡張	UTF-8
issue_date	23220.1	Full Date
expiry_date	23220.1	Full Date
birth_date	23220.1	Full Date
portrait	23220.1	Binary

principal_name	拡張	Latin
uniq_code	拡張	Latin
email_address	23220.1	Latin
issuing_authority_logo	拡張	Binary
president_name	拡張	UTF-8
document_number	23220.1	Latin
document_type	23220.1	Latin
issuing_country	23220.1	Latin
age_over_NN *	23220.1	Latin

*）年齢認証情報。これを設定する場合はISO/IEC 23220-1の仕様に従わなければならない。