学認技術運用基準（Ver. 2.1）

目　次

本基準は、国立情報学研究所学術認証運営委員会（以下「委員会」という。）が実施する学術認証フェデレーション「学認」において、委員会が提供するシステムと、学認に参加する Identity Provider（以下「IdP」という。）、ならびに、Service Provider（以下「SP」という。）が備えるべき技術・運用基準を示すものである。

本基準中の「しなければならない」(MUST)、「してはならない」(MUST NOT)、「必須である」(REQUIRED)、「するものとする」(SHALL)、「しないものとする」(SHALL NOT)、「すべきである」(SHOULD)、「すべきではない」(SHOULD NOT)、「推奨される」(RECOMMENDED)、「してもよい」(MAY)、および「任意である」(OPTIONAL) のキーワードは、RFC 2119 に記述されているとおりに解釈する。

1. SAML 技術標準

学認で利用する SAML 技術標準は、OASIS で規定する次の仕様に基づくものとする。

1.1) SAML 2 Core
(http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)
SAML2.0 コンフォーマンスに関する技術要件及び構成する一連の文書について規定。

1.2) SAML 2 Profiles
(http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)
システム間で利用する識別子やバインディングサポート、証明書や鍵の利用について規定。

1.3) SAML 2 Metadata
(http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)
メタデータを標準化された方法で記述するための規則について規定。

2. プロトコル

本基準では、学認に参加する IdP および SP（以下「エンティティ」という）が可能な限り幅広いサービスを提供できるように設計を行っている。そのため、学認に参加する全てのエンティティは、学認内において統一されたプロトコルを利用すべきである。利用されるプロトコルは、認証要求と認証応答のそれぞれにおいて以下に示す要件を満たすものとする。

なお、学認では、フェデレーション内で利用するソフトウェアとして、上記プロトコルの実装例である Shibboleth を利用することが推奨される。

2.1) 認証要求

HTTP-bound SAML プロトコルの認証要求（Authentication Request）メッセージは、SAML 技術標準「SAML 2 Profiles 」4.1.3、および、4.1.4 に定める Web Browser SSO Profile の仕様を満たす実装とすべきである。

2.2) 認証応答

SAMLアサーションを含むHTTPにバインドした認証応答(Authentication Response)メッセージは、SAML技術標準「SAML 2 Profiles 」4.1.3、および、4.1.4に定めるWeb Browser SSO Profileの仕様を満たす実装とすべきである。

また、認証応答メッセージ、もしくは、認証アサーションのいずれかに対して、署名をすべきである。さらに、認証アサーションに対して、暗号化をすべきである。

2.3) Shibboleth

Shibboleth は、Shibboleth Consortium(http://shibboleth.net)が開発、提供するSAML をベースとするソフトウェアである。

・Shibboleth 2 (https://wiki.shibboleth.net/confluence/display/SHIB2/Home) およびそれ以降

- IdPは2.4.3以上、SPは2.5.3以上を推奨

ただし、海外 SP 等のサービスを利用することを目的として、SAML1 プロトコルおよびShibboleth1.3プロトコルを利用してもよい。

3. 属性情報

属性情報は、各エンティティが利用者への認可の判断を行うために使用する情報である。

学認で利用可能な属性情報については、本定義に添付する「属性情報仕様一覧」を参照することとする。

3.1) 属性情報の利用

学認で定義されている全ての属性はユニークなURI名を持っている。各エンティティは利用したい属性について、可能な限り本定義に添付する「属性情報仕様一覧」から選択して利用すべきである。

もし、利用したい属性が「属性情報仕様一覧」に存在しない場合は、各エンティティは委員会に新規属性の追加を申請することができるものとする。申請された新規属性の追加については、委員会において検討し、委員会が決定するものとする。

なお、学認を介することのない、あるいは、学内のプライベートなフェデレーションのみで利用する場合にはこれ以外の属性を利用してもよい。

http://middleware.internet2.edu/dir/docs/draft-internet2-mace-dir-saml-attributes-latest.pdf

3.2) 属性情報の信頼性

IdPは、自機関に所属する利用者の属性を保証すべきである。また、自機関に所属しない利用者の属性を保証すべきではない。例えば、A大学のIdPがB大学の学生の属性を保証すべきではない。ただし、自機関に所属しない利用者を自機関が管理する場合、SPに対する不正なアクセスが発生しないよう特に属性管理に注意することで、そのような利用者の属性を保証してもよい。

3.3) 属性情報の検証

SP は、受信する全ての属性情報が、信頼するオーソリティから発行されたものであることを検証すべきである。

3.4) 属性情報の種別

SP は、各サービスを提供する際に、必要となる属性情報及び当該属性情報の種別について利用者に明示すべきである。種別については“必須(required)”、“推奨(recommended)”、“任意(optional)”とし、属性情報の利用目的とともに明確に記載することが推奨される。

SP は提供するサービスで必要な属性情報について、別途定める申請書によりフェデレーション事務局まで申請するものとする。

なお、委員会は各 SP がどの属性情報を利用するか、各エンティティに対して通知を行うものとする。

3.5) スコープ

スコープは、原則として EntityID に記載しているドメインと一致しなければならない。各 IdP ではメタデータにこのスコープを明示するとともに、スコープ付きの属性を利用する際には、同じスコープによって利用しなければならない。また、SP ではアサーションによって受信した属性のスコープを、IdP のメタデータに記載されているスコープと比較して判断するものとする。

4. メタデータ

学認において利用するメタデータは、次に定めるとおりとする。

4.1) メタデータの仕様

SAML 2 のメタデータ仕様 （ 1.3) SAML 2 Metadata に記述。）にしたがった仕様とすべきである。

4.2) メタデータの種類

学認では、以下の２種類のメタデータを利用する。

・エンティティメタデータ：
　　各エンティティの情報を記載するメタデータ

・フェデレーションメタデータ：
　　学認に参加する全てのエンティティメタデータを含むメタデータ

4.3) エンティティメタデータの提出

学認に参加する全ての機関は、各エンティティのエンティティメタデータを委員会に提出しなければならない。

4.4) エンティティメタデータの内容

学認の各参加機関は、自身のサーバを証明するためのサーバ証明書やメタデータに関し、証明書更新やメタデータ記載内容に変更があった場合は、速やかに変更した最新版のメタデータを委員会に提出しなければならない。
また、メタデータの<ContactPerson>要素のように、個人情報の入力が必要になる箇所については、例えば、E-Mail アドレスには担当グループアドレスを記載する等、可能な限り個人が特定できる情報を表示しないことが推奨される。
なお、委員会に提出されたエンティティメタデータは、これに記載される個人情報を含めてWeb（リポジトリ）で公開することとしている。そのため、運用責任者はエンティティメタデータ提出時、あるいは、申請時にエンティティメタデータに記載された情報の公開を了承したものとみなす。
委員会では、各機関から提出されたエンティティメタデータを下記の目的のみに利用するものとする。

- エンティティメタデータ記載事項の検証
- 学認の運用、管理、運営
- フェデレーションメタデータへの追加、更新
- 学認各参加機関へのフェデレーションメタデータの配布、Web（リポジトリ）上での公開
- Discovery Service（以下「DS」という。）、IdP、および、SP への登録

4.5）エンティティメタデータの<Organization>要素

IdP は、提出するエンティティメタデータにおいて、<Organization>要素に下記を記載すべきである。

SP は、提出するエンティティメタデータにおいて、<Organization>要素に下記の内<OrganizationName xml:lang="en">を記載すべきである。さらに、その他の要素を記載してもよい。

- <OrganizationName xml:lang="en">：機関の英語正式名称
  特に、IdP の場合は、IdP を運用する機関の名称と一致しなければならない。
- <OrganizationName xml:lang="ja">：機関の日本語正式名称
  特に、IdP の場合は、IdP を運用する機関の名称と一致しなければならない。
- <OrganizationDisplayName xml:lang="en">：エンティティの英語正式名称
  特に、IdP の場合は、DS に表示する文字列とする
- <OrganizationDisplayName xml:lang="ja">：エンティティの日本語正式名称
  特に、IdP の場合は、DS に表示する文字列とする
  さらに、IdP が１機関内で複数存在する場合は、これらを区別できるようにすべきである

4.6）エンティティメタデータの ID

委員会は、フェデレーションメタデータ作成時に、提出された各エンティティメタデータを区別するための ID を、各エンティティメタデータの<EntityDescriptor>の ID 属性として付与してもよい。

4.7) フェデレーションメタデータの作成と公開

委員会は、提出された全てのエンティティメタデータについて検証を行い、さらに、フェデレーションメタデータに追加、検証、署名を行い、最新のフェデレーションメタデータを作成しなければならない。

また、これを各参加機関に公開しなければならない。

フェデレーションメタデータの有効期間は１４日間とし、これをフェデレーションメタデータ内に、<EntitiesDescriptor>要素の validUntil 属性で記載しなければならない。

また、委員会は有効期間内にフェデレーションメタデータを更新しなければならない。

フェデレーションメタデータのグループ名（＝<EntitiesDescriptor>要素の Name 属性）と、公開 URL は下記とする。

Name="GakuNin"

公開 URL＝"https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml"

4.8) フェデレーションメタデータの取得と設定

各参加機関は、4.7)で学認から公開されるフェデレーションメタデータを取得して、エンティティに設定すべきである。

4.9) フェデレーションメタデータの更新

古いフェデレーションメタデータを利用したエンティティでは、他のサイトとの連携ができなくなるだけではなく、そのエンティティのセキュリティレベルの低下につながる可能性がある。そのため、各参加機関はフェデレーションメタデータの定期的な更新を行うことが強く推奨される。この頻度は１回／日程度とする。また、この更新頻度を長く設定している場合においては、少なくともフェデレーションメタデータの validUntil 属性で記述された有効期限より前に更新を行うことが強く推奨される。

4.10) フェデレーションメタデータ署名の検証

各参加機関は 7.1)に規定される署名用の証明書にて、フェデレーションメタデータの署名を検証することが強く推奨される。

5. ディスカバリサービス（Discovery Service）

委員会は、学認に参加する全てのエンティティが、最適な方法で認証情報を確認することを可能とするため、ディスカバリサービスを提供するものとする。

5.1) ディスカバリサービスの URL

学認で提供するディスカバリサービスの URL は以下のとおりである。

https://ds.gakunin.nii.ac.jp/WAYF

5.2) ディスカバリサービスのプロトコル

以下に定められる SAML2 向けのプロトコル、および SAML1 向けに定められた Shibboleth1.3

プロトコルを用いる。
Identity Provider Discovery Service Protocol and Profile
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf

6. フェデレーション構築、運用サポート

学認に参加する各エンティティは、各々の判断において本基準で規定するプロトコルをサポートするソフトウェア製品を選択して利用することが可能である。

学認では、参加する各機関の IdP、SP 構築に際して、必要に応じて技術サポートを実施するが、商用製品に対するサポートは実施しないものとする。

7. 証明書の利用

学認では、各エンティティの信頼性を担保するため、証明書を利用することとする。

7.1) フェデレーションメタデータ署名用の証明書

委員会は、公開、配布するフェデレーションメタデータに対して XML 署名を行うものとする。なお、この署名に利用する証明書は、学認が管理、運用する自己署名証明書を利用するものとする。また、署名に使用する証明書については、各機関がフェデレーションメタデータの署名を検証する目的のため、学認から各エンティティに安全に配布すべきである。ただし、この証明書を直接配布せずに Web（リポジトリ）上で公開してもよい。

フェデレーションメタデータ署名用の証明書の公開 URL は下記とする。

公開 URL＝”https://metadata.gakunin.nii.ac.jp/gakunin-signer-2010.cer”

7.2) フェデレーションメタデータ署名用の証明書の検証

各エンティティは、fingerprint が下記の値と異なる署名用証明書を用いてはならない。これを確認するため、各エンティティは下記の値を用いて署名用証明書を検証することが推奨される。

フィンガープリント(SHA-1)
＝9F:8D:13:CB:E3:93:57:59:E1:81:8F:A4:26:A5:FD:60:AB:C5:01:00

最新の値は、Web サイト＝
”https://meatwiki.nii.ac.jp/confluence/display/GakuNinShibInstall/signer”
に掲載する。

7.3) 信頼する認証局

各エンティティが XML 署名や TLS 相互認証を行うための証明書は、以下に掲げる学認が信頼する認証局から発行された証明書を利用しなければならない。

－国立情報学研究所オープンドメイン認証局
https://certs.nii.ac.jp/（サービス案内ウェブページ）
－UPKI オープンドメイン認証局
(UPKI オープンドメイン証明書自動発行検証プロジェクトより発行されたもの。2015 年 6

月 30 日プロジェクト終了）
https://upki-portal.nii.ac.jp/docs/odcert （プロジェクトホームページ）
－WTCA に準拠した商用認証局であり、かつ委員会が認めた認証局
－大学のキャンパス認証局等のローカル認証局であり、かつ委員会が認めた認証局

7.4）秘密鍵の危殆化
各エンティティは、エンティティが利用している秘密鍵が危殆化した場合、直ちに委員会に通知するとともに、関連する証明書を失効し、遅滞なく新たな証明書の再発行をもって代替の措置を行わなければならない。

7.5）ダイレクト SOAP 接続
SP がダイレクト SOAP 接続要求を行う場合には、XML 署名や TLS 相互認証を実装するべきである。

8. セキュリティ

学認においてセキュリティを確保するため、学認に参加する各エンティティは、本項に定める以下の事項について遵守しなければならない。

8.1）利用者 ID の管理
全ての利用者情報は、当該の機関が発行・管理している、有効なアカウントの情報でなければならない。
また、各エンティティにおいて、利用者 ID の有効期間が終了した場合、あるいは、利用者から利用意思の撤回があった場合には、遅滞なくその利用者 ID の利用を停止しなければならない。

8.2）利用者 ID の再利用
eduPersonPrincipalName、および eduPersonTargetedID に関して、かつて利用されていたが、現在利用されていない利用者 ID を他者が使用する場合は、最終の利用時から最低 24 ヶ月間は再利用すべきではない。

8.3）ID 利用者の同一性の保証
前項における再利用の場合を除いて、IdP では、同一 ID でのアクセスが同一人物からによることを保証するための方策を講じなければならない。

8.4）SP における ID 利用
ID を利用してサービスを提供する SP では、データベースでの ID 誤割当や振分アルゴリズムによるコリジョン等に十分に注意しなければならない。

8.5）利用者情報の維持管理
SP は、利用者情報について、個人情報の保護、情報の最新性の確保、情報漏えいのリスク回

避の観点から、必要最低限の分を超えて保持しないことが推奨される。
なお、サービスを提供するうえで個人情報を保持する必要がある場合には、利用者にその旨を明示しなければならない。

8.6）利用者の同意
各エンティティにおける属性の取扱い、特に属性の送受信時には、利用する属性の明示、および利用目的の明示を行い、本人同意を取得する等の機能を利用してもよい。

8.7）ログの保管
サービスへのアクセスログについては、最低3ヶ月保管することが推奨される。また、アクセスログの保管期間を定めることが推奨される。

8.8）参加機関の責任
学認に参加する各参加機関は、相互に協力して認証連携を実現することとする。そのため、各参加機関では自らが送信する情報の信頼性や正確性について努力義務を負うものとする。ただし、その限りにおいて、故意または重大な過失によるものを除き、送信した情報の信頼性や正確性に不備があったことにより生じた損害について責任を負わないものとする。
なおこの規定は、参加機関の間で送受する情報の信頼性や正確性についての責任に関し別途の取りきめをすることを妨げるものではない。

9. 学認運用エンティティ
委員会は、学認の運用に必要な学認 IdP の運用、および、各参加機関が運用接続試験を行うための属性表示サービスの提供を行うものとする。

9.1）学認 IdP
学認 IdP は、SP に対して以下の目的で運用するものとする。
・フェデレーションの運用で必要となる SP へのアクセス
・SP との接続確認
学認 IdP のエンティティ ID は、以下とする。
エンティティ ID ＝ ″https://idp.gakunin.nii.ac.jp/idp/shibboleth″
学認 IdP は、委員会がフェデレーションの運用のために必要と認めた者のアカウントを保持するものとする。学認 IdP は、例外的に、接続確認のために SP が利用するテストアカウントを保持してもよい。テストアカウントの発行については、別途定める。

9.2）属性表示サービス
SAML2 プロトコル、および、SAML1 プロトコルによる接続試験のため、それぞれのプロトコルで送信可能な全ての属性を表示するサービスであり、各参加機関が利用可能とする。
Attrviewer20：
エンティティ ID ＝ ”https://attrviewer20.gakunin.nii.ac.jp/shibboleth-sp”
プロトコル＝SAML2

Attrviewer13：

エンティティ ID ＝ ”https://attrviewer13.gakunin.nii.ac.jp/shibboleth-sp”

プロトコル＝SAML1

別添１．学認　属性情報仕様一覧

1.organizationName

名　　称	organizationName
概　　要	利用者の所属する機関名称を英字で表わします。
参照スキーマ	RFC4519, RFC2256 (LDAPv3)
name 【SAML1】	"urn:mace:dir:attribute-def:o"
name 【SAML2】	"urn:oid:2.5.4.10"
friendlyName	o
属性値 or 形式	文字列（１バイトコード)
照合順序	caseIgnoreMatch
複数値	単一値
説明等	機関名称を英字で表わした属性です。 設定例： Abcdef University National Institute of Informatics

2.jaOrganizationName

名　　称	jaOrganizationName
概　　要	利用者の所属する機関名称を日本語で表わす
参照スキーマ	GakuNin.Schema
name 【SAML1】	未定義
name 【SAML2】	"urn:oid:1.3.6.1.4.1.32264.1.1.4"
friendlyName	jao
属性値 or 形式	文字列 (Unicode/UTF-8)
照合順序	caseIgnoreMatch
複数値	単一値
説明等	学認で新規に定義する属性です。 値はUnicode 文字列ですので、機関名称を日本語表記で記載することが可能です。 設定例： あいうえお大学 国立情報学研究所

3.organizationalUnitName

名　　称	organizationalUnitName
概　　要	機関内所属名称を英字で表わす
参照スキーマ	RFC4519, RFC2256 (LDAPv3)
name 【SAML1】	"urn:mace:dir:attribute-def:ou"
name 【SAML2】	"urn:oid:2.5.4.11"
friendlyName	ou
属性値 or 形式	文字列（１バイトコード）
照 合 順 序	caseIgnoreMatch
複 数 値	単一値
説 明 等	設定例： Faculty of Technology Cyber Science Center

4.jaOrganizationalUnitName

名　　称	jaOrganizationalUnitName
概　　要	機関内所属名称を日本語で表わす
参照スキーマ	GakuNin.Schema
name 【SAML1】	未定義
name 【SAML2】	"urn:oid:1.3.6.1.4.1.32264.1.1.5"
friendlyName	jaou
属性値 or 形式	文字列 (Unicode/UTF-8)
照 合 順 序	caseIgnoreMatch
複 数 値	単一値
説 明 等	学認で新規に定義する属性です。 値はUnicode 文字列ですので、機関内所属名称を日本語表記で記載することが可能です。 設定例： 工学部 サイバーサイエンスセンター

5.eduPersonPrincipalName

名　　称	eduPersonPrincipalName
概　　要	フェデレーション内の利用者を一意に定めます。
参照スキーマ	eduPerson Object Class Specification (200806)
name	“urn:mace:dir:attribute-def:eduPersonPrincipalName”

【SAML1】	
name 【SAML2】	“urn:oid:1.3.6.1.4.1.5923.1.1.1.6”
friendlyName	eduPersonPrincipalName
属性値 or 形式	[各 IdP で一意な、かつ、永続的な識別子]@[Scope]
照 合 順 序	caseIgnoreMatch
複 数 値	単一値
説 明 等	フェデレーション内で一意な、かつ、永続的な利用者識別子。「機関内で一意な利用者識別子」とスコープを合わせることで、フェデレーション内での一意性を保証します。IdP は、フェデレーションに参加する全ての SP に対して同じ値を送信します。 なお、属性値のローカルパート部に「@」を含めることはできません。 設定例：t-ninsyo2009@b-univ.ac.jp

6.eduPersonTargetedID

名 称	eduPersonTargetedID
概 要	フェデレーション内の利用者を匿名で表わす
参照スキーマ	eduPerson Object Class Specification (200806)
name 【SAML1】	″urn:mace:dir:attribute-def:eduPersonTargetedID″
name 【SAML2】	″urn:oid:1.3.6.1.4.1.5923.1.1.1.10″
friendlyName	eduPersonTargetedID
属性値 or 形式	<IdP の entityID>!<SP の entity>![各 IdP 内で一意、各 SP 毎に異なる特定不可能な、かつ、永続的な識別子]、256 バイト以下
照 合 順 序	caseExactMatch
複 数 値	複数値
説 明 等	フェデレーション内で一意な、かつ、SP サイト毎に異なる永続的な利用者識別子です。これは、SP 間での利用者の特定を防ぐことを目的としていて、識別子の値はハッシュ等によりユーザの特定が不可能であることが要求されます。 フォーマットは、<IdP の entityID>、<SP の entityID>、およびハッシュ化等によって匿名化した識別子を”!”で結合したものです。 設定例： https://idp.sample.ac.jp/idp/shibboleth!https://sp.sample.ac.jp/shibboleth-sp!+Lxxl7QLnCkaKguy5xjNLRBkdDc=

7.eduPersonAffiliation

名 称	eduPersonAffiliation

概　　要	利用者の職種等を表します。
参照スキーマ	eduPerson Object Class Specification (200806)
name 【SAML1】	"urn:mace:dir:attribute-def:eduPersonAffiliation"
name 【SAML2】	"urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
friendlyName	eduPersonAffiliation
属性値 or 形式	"faculty", "staff", "student", "member"
照 合 順 序	caseIgnoreMatch
複　数　値	複数値
説　明　等	利用者の職位として、４つの値が利用可能です。IdP サイトでは、機関内の実際の詳細職位とのマッピングが必要です。いずれの値にも合致しない利用者については、この属性自体を送らないようにします。また、利用できる値は、「卒業生」等、必要に応じて追加することを予定しています。 設定例：staff, member

8.eduPersonScopedAffiliation

名　　称	eduPersonScopedAffiliation
概　　要	利用者が所属する機関内での職種を表します。
参照スキーマ	eduPerson Object Class Specification (200806)
name 【SAML1】	"urn:mace:dir:attribute-def:eduPersonScopedAffiliation"
name 【SAML2】	"urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
friendlyName	eduPersonScopedAffiliation
属性値 or 形式	文字列@スコープ、　文字列は下記の値： "faculty", "staff", "student", "member"
照 合 順 序	caseIgnoreMatch
複　数　値	複数値
説　明　等	利用者が所属する機関においてどのような関係であるかについて定義する属性です。設定する属性値は「eduPersonAffiliation」と同値ですが、@以降にスコープを付加します。 設定例：member@nii.ac.jp, student@nii.ac.jp

9.eduPersonEntitlement

名　　称	eduPersonEntitlement
概　　要	特定のアプリケーションを利用する資格情報を表します。
参照スキーマ	eduPerson Object Class Specification (200806)

name 【SAML1】	″urn:mace:dir:attribute-def:eduPersonEntitlement″
name 【SAML2】	″urn:oid:1.3.6.1.4.1.5923.1.1.1.7″
friendlyName	eduPersonEntitlement
属性値 or 形式	文字列（１バイトコード）
照　合　順　序	caseExactMatch
複　　数　　値	複数値
説　　明　　等	サービスを利用する資格情報を表しています。なお、本属性は SP サイトが受信する文字列を決定し、IdP サイトは SP サイト毎にその値を利用します。IdP サイトでは、SP サイトが決めるサービス利用資格に従い、各ユーザの属性として送信する値を設定します。 設定例：urn:mace:dir:entitlement:common-lib-terms

10. surname

名　　称	surname
概　　要	氏名（姓）を英字で表しています。
参照スキーマ	RFC4519, RFC2256 (LDAPv3)
name 【SAML1】	“urn:mace:dir:attribute-def:sn”
name 【SAML2】	″urn:oid:2.5.4.4″
friendlyName	sn
属性値 or 形式	文字列（１バイトコード）
照　合　順　序	caseIgnoreMatch
複　　数　　値	単一値
説　　明　　等	設定例： Ninsho Yamada

11. jaSurname

名　　称	jaSurname
概　　要	氏名（姓）を日本語で表わします。
参照スキーマ	GakuNin.schema
name 【SAML1】	未定義
name 【SAML2】	″urn:oid:1.3.6.1.4.1.32264.1.1.1″
friendlyName	jasn

属性値 or 形式	文字列 (Unicode/UTF-8)
照　合　順　序	caseIgnoreMatch
複　　数　　値	単一値
説　　明　　等	学認で新規に定義する属性です。値はUnicode 文字列ですので、氏名の“姓”を日本語表記で記載することが可能です。 利用例： 認証 山田

12.givenName

名　　称	givenName
概　　要	氏名（名）を英字で表わします。
参照スキーマ	RFC4519, RFC2256 (LDAPv3)
name 【SAML1】	″urn:mace:dir:attribute-def:givenName″
name 【SAML2】	″urn:oid:2.5.4.42″
friendlyName	givenName
属性値 or 形式	文字列（１バイトコード)
照　合　順　序	caseIgnoreMatch
複　　数　　値	単一値
説　　明　　等	設定例： Taro Jiro

13.jaGivenName

名　　称	jaGivenName
概　　要	氏名（名）を日本語で表わします。
参照スキーマ	GakuNin.schema
name 【SAML1】	未定義
name 【SAML2】	″urn:oid:1.3.6.1.4.1.32264.1.1.2 ″
friendlyName	jaGivenName
属性値 or 形式	文字列 (Unicode/UTF-8)
照　合　順　序	caseIgnoreMatch
複　　数　　値	単一値
説　　明　　等	学認で新規に定義する属性です。値はUnicode 文字列ですので、氏名の“名”を日本語表記で記載することが可能です。

	設定例： 太郎 次郎

14.displayName

名　　称	displayName
概　　要	英字氏名（表示名）を表します。
参照スキーマ	RFC2798 (inetOrgPerson)
name 【SAML1】	"urn:mace:dir:attribute-def:displayName"
name 【SAML2】	"urn:oid:2.16.840.1.113730.3.1.241"
friendlyName	displayName
属性値 or 形式	文字列（１バイトコード)
照 合 順 序	caseIgnoreMatch
複　数　値	単一値
説　明　等	主に、アプリケーション上で表示される英字氏名（表示名）として利用することが可能です。 設定例： Ninsho Taro Yamada Jiro

15.jaDisplayName

名　　称	jaDisplayName
概　　要	アプリケーション上に日本語で表わす氏名等（表示名）
参照スキーマ	GakuNin.schema
name 【SAML1】	未定義
name 【SAML2】	"urn:oid:1.3.6.1.4.1.32264.1.1.3"
friendlyName	jaDisplayName
属性値 or 形式	文字列 (Unicode/UTF-8)
照 合 順 序	caseIgnoreMatch
複　数　値	単一値
説　明　等	学認で新規に定義する属性です。 主に、アプリケーションで表示される日本語氏名（表示名）として利用することが可能です。 設定例： 認証太郎

	山田次郎

16.mail

名　　称	mail
概　　要	電子メール
参照スキーマ	RFC2798 (inetOrgPerson)
name 【SAML1】	"urn:mace:dir:attribute-def:mail"
name 【SAML2】	"urn:oid:0.9.2342.19200300.100.1.3"
friendlyName	mail
属性値 or 形式	文字列@ドメイン、256 バイト以下
照 合 順 序	caseIgnoreMatch
複　数　値	単一値
説　明　等	電子メールアドレスを設定することが可能です。 設定例：ninsho_taro@nii.ac.jp

17. gakuninScopedPersonalUniqueCode

名　　称	gakuninScopedPersonalUniqueCode
概　　要	教職員の教職員番号および学生の学籍番号を表す
参照スキーマ	GakuNin.schema
name 【SAML1】	未定義
name 【SAML2】	"urn:oid:1.3.6.1.4.1.32264.1.1.6"
friendlyName	gakuninScopedPersonalUniqueCode
属性値 or 形式	所属:識別番号@スコープ　(Unicode/UTF-8) 所属は、faculty、student など 識別番号は、学生番号、教職員番号など
照 合 順 序	caseIgnoreMatch
複　数　値	複数値
説　明　等	学認で新規に定義する属性です。 英数字は半角、日本語文字は全角で表記 設定例： faculty:12345@kyoto-su.ac.jp

	student:abcdefg@kyoto-su.ac.jp student:12あ3456@osaka-u.ac.jp

18.isMemberOf

名　　称	isMemberOf
概　　要	所属するグループ名を表す
参照スキーマ	eduMember Object Class Specification
name 【SAML1】	未定義
name 【SAML2】	"urn:oid:1.3.6.1.4.1.5923.1.5.1.1"
friendlyName	isMemberOf
属性値or形式	文字列（1バイトコード）
照合順序	caseExactMatch
複数値	複数値
説明等	利用者が所属するグループIDを、URI形式で表します。 設定例：https://voplatform.example.ac.jp/gr/FooGroup

＜参照URL＞

(1)「eduPerson and eduOrg Object Classes」

https://www.internet2.edu/products-services/trust-identity-middleware/eduperson-eduorg/

(2)「GakuNin.Schema」

https://meatwiki.nii.ac.jp/confluence/download/attachments/12158166/gakunin.schema?version=2&modificationDate=1382000918000&api=v2

(3)「eduMember Object Class Specification」

http://macedir.org/specs/internet2-mace-dir-ldap-group-membership-200507.html