学認技術運用基準（Ver. 2.7）

（平成 25 年 10 月 17 日
学術認証運営委員会決定）

改正　平成29年 3月 8日
平成29年11月8日
平成31年 3月29日
令和2年2月28日
令和3年2月10日
令和5年 2月15 日

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、ServiceProvider（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、1.2) 記載の SAML 技術標準「SAML 2 Profiles 」 4.1 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 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 Project / 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 Identity Provider 4
（https://wiki.shibboleth.net/confluence/display/IDP4/Home）、Shibboleth Service Provider 3（https://wiki.shibboleth.net/confluence/display/SP3/Home）およびそれ以降
- IdP は 4.2.1 以上、SP は 3.2.2 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」を参照するものとする。

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。

3.2) 属性情報の信頼性

IdP は、自機関もしくは機関の設置した組織（以下、「機関の組織」という。）としての参加の場合は当該組織（以下あわせて、「自機関・組織」という。）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・組織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・組織に所属しない利用者を自機関・組織が管理する場合、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がサブドメインであるようなドメイン名、もしくは entityID に記載しているドメイン名と一致するものでなければならない。また、このドメイン名は原則として自機関・組織が所有するものでなければならない。ただし、entityIDに記載しているドメインが自機関・組織の所有するものでない場合は、スコープは自機関・組織が所有するドメイン名、もしくはそのサブドメイン名を用いるものとする。機関の組織の場合は組織を包含する機関が所有するドメインのサブドメイン名を利用してもよい。

以下に許可されるスコープの例を示す。

例１）機関としての申請の場合

自機関保有のドメイン：example.ac.jp

entityIDのホスト部：idp.example.ac.jp

スコープ：example.ac.jp または idp.example.ac.jp

例２）機関の組織としての申請の場合

例１の機関の設置した組織保有のドメイン：example-b.org

entityIDのホスト部：idp.example-b.org

スコープ：example-b.org または idp.example-b.org（組織のドメインを使用）

sub1.example.ac.jp または sub2.example.ac.jp 等（機関のドメインを使用）

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に対しては、同じスコープを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。

また、次に該当する機関は2つ目もしくはそれ以上のスコープを利用することができる。自機関が実施要領第5条第一号もしくは第二号に該当する機関を設置している場合、かつ当該機関に所属する利用者を管理している場合、当該機関に対応するスコープを利用することができる。この場合も、各IdPではメタデータにこのスコープを明示しなければならない。

以下に複数のスコープの例を示す。

例）大学Bを設置する法人Aとして参加する場合

法人Aとしてのスコープ：example-a.ac.jp

大学Bとしてのスコープ：example-b.ac.jp

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および機関の組織(以下あわせて、「参加機関・組織」という。)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・組織は、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、各参加機関・組織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・組織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 entityID

学認の各参加機関・組織は、提出するエンティティメタデータにおいて、<EntityDescriptor>の entityID 属性として、IdP または SP を一意に決定する識別子を記載しなければならない。

entityID の値は、https スキームを用いた URL 形式が推奨される。

URL 形式の entityID のホスト部はドメイン名（FQDN）でなければならない。このドメイン名は当該参加機関もしくは機関の組織の場合は組織を包含する機関の所有するドメイン配下のものであることが推奨されるが、参加機関もしくは機関の組織の場合は組織を包含する機関が自ら所有していないドメインのものであっても、所有者から承認を得ている場合や、その

他委員会が適当と認めた場合は、当該ドメイン名を利用してもよい。

4.6）エンティティメタデータの証明書

エンティティメタデータに記載する証明書は 7.4)の要件を満たさなければならない。

学認の各参加機関・組織は、7.4)に該当する証明書を更新する場合、他のエンティティに新しい証明書の情報が伝播するまで必要な期間を設けて、新旧の証明書を併記することが推奨される。

また、記載する証明書に関連する秘密鍵が危殆化した場合は、遅滞なく当該証明書を削除しなければならない。

4.7）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。なお、IdP、SPともに、機関の組織としての参加の場合は組織を設置した機関の名称とする。

・<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。なお、IdP、SPともに、機関の組織としての参加の場合は組織を包含する機関の名称とする。

・<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し、原則として機関の英語名称とする。ただし、実施要領第５条第四号に基づく参加組織は、参加組織またはかかるプロジェクトの英語名称とする。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。

・<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し、原則として機関の日本語名称とする。ただし、実施要領第５条第四号に基づく参加組織は、参加組織またはかかるプロジェクトの日本語名称とする。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。

4.8）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。

4.9）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・組織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“

委員会は、学認利用の一時休止を届け出た参加機関・組織があった場合、もしくは、学認への参加を一時停止する参加機関・組織があった場合、当該参加機関・組織のエンティティメタデータを一時的にフェデレーションメタデータから除外するものとする。

また、公開 URL の末尾にクエリ部"?generation=N"（N は任意の桁数の数字）を付与した URL を用いてもよい。委員会は、クエリ部付きのアクセスに対して、異なる署名用証明書もしくは暗号アルゴリズム等を用いたメタデータを提供することができる。

4. 10）フェデレーションメタデータの取得と設定

各参加機関・組織は、4.9)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. 11）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・組織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. 12）フェデレーションメタデータ署名の検証

各参加機関・組織は 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。

特に 7.3)に定める署名用証明書移行期間においては、7.3)に示す Web サイトに記載された署名用証明書とメタデータ公開 URL の対応関係を参照し、これに従った適切な署名用証明書および URL を用いること。

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、各参加機関・組織の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、原則として、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、証明書を利用するものとする。

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、この署名に使用する証明書は、学認が管理、運用する自己署名証明書を使用するものとする。また、署名に使用する証明書については、各参加機関・組織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-2017.cer”

ただし、7.3)に定める更新された署名用証明書の提供のために上記公開 URL の数字部分を変更してもよい。

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、7.3)に定める更新された署名用証明書および更新前の署名用証明書を除いて 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-256)

=5E:D6:A8:C5:E9:30:49:3F:B4:BA:77:54:6A:FB:66:BA:14:7D:CB:50:5B:EF:0F:D9:7C:26:04:C2:D9:36:FD:81

7.3）フェデレーションメタデータ署名用の証明書の更新

委員会は、緊急時に本基準の改訂を待たずにフェデレーションメタデータ署名用の証明書を更新してもよい。

7.1)の公開 URL および 7.2)のフィンガープリントの最新の値は、下記の Web サイトに掲載する。

Web サイト

＝”https://meatwiki.nii.ac.jp/confluence/display/GakuNinShibInstall/signer”

この際、委員会は各エンティティが設定変更を行うための移行期間を設定することができ

る。移行期間中は原則として更新前の証明書で署名されたメタデータおよび更新後の証明書で署名されたメタデータの両方を提供するものとする。移行期間および移行期間内のメタデータ公開URLと署名証明書の対応関係等移行スケジュールは上記Webサイトに掲載するものとする。移行期間は原則として1年以内とする。

委員会は、移行期間終了後速やかに4.9)に定める公開URL全てにおいて更新された署名用証明書で署名されたフェデレーションメタデータを公開しなければならない。

各エンティティは、移行期間の設定がある場合は移行期間内に、もしくは取得した検証可能なフェデレーションメタデータの有効期限が切れる前に、本基準掲載のフェデレーションメタデータ署名用の証明書情報との差異について、事務局への確認等、他の情報源により真正性を確認したうえで、更新することが強く推奨される。また委員会は、できるだけ速やかに本基準を改訂し証明書情報を更新するものとする。

7. 4）信頼する証明書

各エンティティが XML 署名やXML 暗号化、TLS 相互認証を行うための証明書は、その信頼性を担保するために、以下に掲げる条件を満たさなければならない。なお、ここで「エンティティにマッチする」とは、当該エンティティのメタデータに含まれる entityID、<SingleSignOnService>、<AssertionConsumerService>に示されるエンドポイントのいずれかのドメイン名が、当該証明書においてRFC 6125 に規定された検証をパスすることをいう。ただし、IdPにおいては上記いずれも自機関・組織もしくは機関の組織の場合は組織を包含する機関が所有するドメインでない場合は、 3.5)に定めるスコープと一致するドメイン名もしくは当該ドメイン配下の任意のドメイン名が上記検証をパスする場合も「エンティティにマッチする」とみなし、同条件ではこのような証明書を用いることが推奨される。ただしこの場合、証明書の更新では原則として同一のドメイン名を用いるものとする。

－国立情報学研究所 UPKI 証明書発行サービスにより発行された証明書で、エンティティにマッチするもの

https://certs.nii.ac.jp/（サービス案内ウェブページ）

－WebTrust for Certification Authorities (WTCA)に準拠した認証局、かつ委員会が認めた認証局から発行された証明書で、エンティティにマッチするもの

－上掲の要件を満たす別の証明書を利用する Web サイトに配置することによって、当該エンティティとの紐付けが確認できた証明書

－大学のキャンパス認証局等のローカル認証局、かつ委員会が認めた認証局から発行された証明書で、エンティティにマッチするもの

－現に他国のフェデレーションに参加しているエンティティであって、運用上の制約により上掲の要件を満たす証明書が利用できないと認められる場合において、入手手段を含め委員会が認めた証明書

－その他委員会が特に認めた証明書

なお、失効した証明書は使用すべきではない。また、証明書は 3 年を目処に定期的に更新すべきである。

7. 5）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。

7.6）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。

7.7）複数証明書の取り扱い

各エンティティは、連携するIdPもしくはSPのエンティティメタデータに複数の証明書の記載がある場合は、これを適切に取り扱うべきである。例えば、IdPが複数の証明書を記載している場合、SPはいずれの証明書でXML署名されているアサーションも当該IdPからの正当なものと認識すべきであり、SPが複数の証明書を記載している場合、IdPはダイレクトSOAP接続においていずれの証明書が提示された場合も当該SPからのものと認識すべきである。

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、自機関・組織が発行・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。さらに同一のスコープを複数のIdPで用いている場合は、eduPersonPrincipalName等スコープ付きのID属性について、当該スコープを共用する全てのIdPの中で共通する各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・組織の責任

学認の各参加機関・組織は、相互に協力して認証連携を実現するものとする。そのため、各参加機関・組織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・組織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。

8.9）バージョンチェックの承諾

委員会は、実施要領第 17 条に基づきセキュリティ向上を目的として使用ソフトウェアのバージョン確認（パッチ適用の有無確認を含む）のため事前に通知の上各エンティティに対してアクセスすることができる。各参加機関・組織は当該アクセスについて予め承諾するものとする。

9 学認運用エンティティ

委員会は、以下の IdP/SP を運用するものとする。

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・組織が利用可能とする。

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

9.3) 属性プロバイダ(mAP)

利用者 ID(eduPersonPrincipalName)を伴った要求に対して、当該 ID に関する所属グループ情報(isMemberOf)等の属性を提供するサービスであり、各参加機関・組織が利用可能とする。

mAP:

エンティティ ID=”https://cg.gakunin.jp/idp/shibboleth”

プロトコル=SAML 2.0 Attribute Query の他、別途定める独自プロトコル

また、利用者がグループの作成・管理を行うための以下の SP を提供する。

mAP(SP):

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

プロトコル=SAML2

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	複数値
説　明　等	機関名称を英字で表わした属性です。ここで機関とは実施要領第5条各号に該当する機関を指します。機関の組織として参加している場合でも組織名称を用いることはできません。機関としての参加の場合、自機関に所属する利用者には自機関の機関名称を用いることが推奨されますが、第5条第三号として参加する機関は、下位機関に所属する利用者に対して下位機関名称を用いる、もしくは両方併記することができます。 SPは、一部のIdPについて本属性に複数の値が入り得ることにご注意ください。 本属性に複数の値を送信するIdPは、SPからいずれかの値に絞って単一値を要求され得ることにご注意ください。 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	複数値

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。ここで機関とは実施要領第5条各号に該当する機関を指します。機関の組織として参加している場合でも組織名称を用いることはできません。機関としての参加の場合、自機関に所属する利用者には自機関の機関名称を用いることが推奨されますが、第5条第三号として参加する機関は、下位機関に所属する利用者に対して下位機関名称を用いる、もしくは両方併記することができます。 SPは、一部のIdPについて本属性に複数の値が入り得ることにご注意ください。 本属性に複数の値を送信するIdPは、SPからいずれかの値に絞って単一値を要求され得ることにご注意ください。 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 【SAML1】	“urn:mace:dir:attribute-def:eduPersonPrincipalName”
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。「スコープ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しこの属性を送信するよう設定した全ての SP に対して、同一の ID であれば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仮名で表わす
参照スキーマ	eduPerson Object Class Specification (200806)
name 【SAML1】	"urn:oid:1.3.6.1.4.1.5923.1.1.1.10"
name 【SAML2】	"urn:oid:1.3.6.1.4.1.5923.1.1.1.10"
friendlyName	eduPersonTargetedID
属性値 or 形式	<saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" NameQualifier="IdPのentityID" SPNameQualifier="SPのentityID">[各IdP内で一意、SP毎に異なる特定不可能な、かつ、永続的な識別子]</saml2:NameID> ただし、NameID要素の内容(content)は256バイト以下、 NameQualifier/SPNameQualifierの値は1024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利用者の特定が不可能であることが要求されます。 この属性は他の属性と異なり属性値を文字列としてではなくXMLとして記述し、SPはXMLとして解釈します。つまりアサーション中の当該属性値の<や>等は実体参照には置換されずそのまま格納されます。

	なお、IdPから送信された値をShibboleth SPで取り出すと、<IdPのentityID>、<SPのentityID>、IdP内識別子を"!"で結合した形式となります。 Shibboleth SPでの属性値例： 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	"urn:oid:1.3.6.1.4.1.32264.1.1.1"
【SAML2】	
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

19. eduPersonAssurance

名　　称	eduPersonAssurance
概　　要	ID の保証レベルを表す
参照スキーマ	eduPerson Object Class Specification (200806)
name 【SAML1】	未定義
name 【SAML2】	"urn:oid:1.3.6.1.4.1.5923.1.1.1.11"
friendlyName	eduPersonAssurance
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	ID の保証レベルを、URI 形式で表します。 設定例：http://idm.example.ac.jp/LOA#sample

20. eduPersonUniqueId

名　　称	eduPersonUniqueId
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 (201305)
name 【SAML1】	未定義
name 【SAML2】	"urn:oid:1.3.6.1.4.1.5923.1.1.1.13"
friendlyName	eduPersonUniqueId
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。他の利用者に対して再利用してはなりません。IdP は、フェデレーションに参加しこの属性を送信するよう設定した全ての SP に対して、同一の ID であれば同じ値を送信します。 属性値のローカルパート部に用いることができるのは英数字（a-z, A-Z, 0-9）のみであり、最大長は 64 文字です。また、この属性は caseIgnoreMatch のため、大文字・小文字のみが異なる値を再利用することができません。 ローカルパート部は、氏名等を含まないランダムな値にすることが推奨されます。 設定例：0123456789abcdef@b-univ.ac.jp

21. **eduPersonOrcid**

名　称	eduPersonOrcid
概　要	ORCID 識別子を表す
参照スキーマ	eduPerson Object Class Specification (201602)
name 【SAML1】	“urn:mace:dir:attribute-def:eduPersonOrcid”
name 【SAML2】	"urn:oid:1.3.6.1.4.1.5923.1.1.1.16"
friendlyName	eduPersonOrcid
属性値 or 形式	文字列（1 バイトコード）
照 合 順 序	caseIgnoreMatch
複　数　値	複数値
説　明　等	利用者の ORCID 識別子を、URI 形式で表します。 設定例：http://orcid.org/0000-0002-1825-0097

＜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~~
「eduMember Object Class Specification」のリンク先が
学認事務局の意図するものと異なっていることを確認しております。（上記取り消し線部分）
大変恐縮ですが，当該URLにはアクセスしないようよろしくお願いいたします。