「学認技術運用基準」新旧対照表(v2.4 : v2.5)

v 2.4	v2.5	備考
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 3.3.0 以上、SP は 2.6.0 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。	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 Identity Provider 3 (https://wiki.shibboleth.net/confluence/display/IDP30/Home)、Shibboleth Service Provider 3 (https://wiki.shibboleth.net/confluence/display/SP3/Home) およびそれ以降 - IdP は 3.4.0 以上、SP は 3.0.0 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。	変更 変更
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。	3.2）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。	追加 追加 追加
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	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の所有するものでない場合は、スコープは自機関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。	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当該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）	追加 追加 追加 追加 追加
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。	4.3）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。	追加
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	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	追加

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	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	変更 追加
4.5）エンティティメタデータの entityID 学認の各参加機関は、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	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	追加

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。	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・組織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・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。	追加 追加
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。	4.6）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。	追加
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。 ・<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。	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包含する機関の名称とする。 ・<OrganizationName xml:lang=”ja”>：機	追加

・<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。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。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。 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。	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。	追加 追加 追加
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。	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。	追加

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があった場合、もしくは、学認への参加を一時停止する機関があった場合、当該参加機関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。	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。	追加 追加 追加
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。	4.10）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。	追加
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	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	追加

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。	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。	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。	追加
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、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。	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。	追加
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。	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。	追加

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。	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。	
7.4）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。	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。	追加
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。	8.1）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。	変更
8.8）参加機関の責任	8.8）参加機関・組織の責任	追加

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ものとする。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。	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。	変更 追加 追加
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。 各参加機関は当該アクセスについて予め承諾するものとする。	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。	 追加
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	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	 追加 変更
9.3）属性プロバイダ(mAP)	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	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	追加 修正
別紙 1. 学認　属性情報仕様一覧 5. eduPersonPrincipalName 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	別紙 1. 学認　属性情報仕様一覧 5. eduPersonPrincipalName 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。また、特に同一のスコープを複数の IdP で用いている場合は別人に同じ識別子が割り当てられないようにするべきである。 設定例：t-ninsyo2009@b-univ.ac.jp	変更 追加
別紙 1. 学認　属性情報仕様一覧 10. surname 説明等	別紙 1. 学認　属性情報仕様一覧 10. surname 説明等	

設定例： Ninsh o Yama da	設定例： Ninsho Yamada	修正
別紙 1. 学認　属性情報仕様一覧 12. givenName 説明等 設定例： Tar o Jiro	別紙 1. 学認　属性情報仕様一覧 12. givenName 説明等 設定例： Taro Jiro	修正
別紙 1. 学認　属性情報仕様一覧 14. displayName 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	別紙 1. 学認　属性情報仕様一覧 14. displayName 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	修正