認証連携IDサービス利用ガイド（管理者向け）

利用方法

1. 利用申請

本システムの利用を希望される機関の管理者の方は、eduroam JP申請システムより利用申請をお願いします。
なお、認証連携IDサービスにおいて申請機関からのアクセスを許可する手続きの都合上、先に機関IdPにおいて属性情報送信の設定をして頂き、その後一度、eduPersonTargetedID取得のため、実際にアクセスいただけますと（所属機関では現在アカウント発行機能が利用できない旨のメッセージが出ますが）助かります。
（eduPersonTargetedIDが送られてきていない旨のメッセージが出る場合は、IdP側の設定ができていないことを示します。）

なお、設定の初期値は以下の通りです。必要に応じて変更をお願いします。

- 学生によるアカウント発行不可
- 学生が発行するアカウントのレルムは教職員と同じ
- 教職員によるビジター向けアカウント発行不可（発行可能最大数が1週間・1か月とも０）

2. IdPが送信するべき属性

認証連携IDサービス（entityID: https://federated-id.eduroam.jp/shibboleth-sp ）では以下の属性を利用しますので、IdPから送信するように設定をお願いします。

属性	用途	
o (organization)	機関を識別するため。（必須）	
eduPersonTargetedID	利用者を識別するため。（必須）	個人識別のための属性です。利用者がログインすると、eduPersonTargetedIDのハッシュ値部分がログインIDとしてサイト上に表示されます。 なお、eduroam 利用者に対するインシデントが発生した場合、eduPersonTargetedID に基づいて利用者を特定して頂くことになりますので対応関係の記録などのご配慮をお願いいたします。(Shibboleth IdPの場合の参考情報)
eduPersonAffiliation	教職員・学生を識別したID発行のため。（選択）	教職員(faculty/staff)と学生(student)の識別に利用します。学生については、学生に対するアカウント発行可否、最長有効期限が適用されるとともに、ビジターアカウントの発行ができません。また、機関管理者からの操作による、年度更新確認の対象となります。属性情報がメンバー(member)または無指定（値なし）の場合は、ビジターアカウントの発行はできませんが、学生としての制限（発行可否、最長有効期間制限、年度更新確認）も適用されません。なお、属性値はシステム内には記憶されず、ログインするたびに参照され、その属性値に従った制限が適用されます。
eduPersonEntitlement	機関管理者権限の確認。（選択）	**管理者としてログインするためには、eduPersonEntitlement属性を適切に設定する必要があります。属性設定にあたって NIIへの申請等は必要ありません。** 機関管理者の識別に利用します。機関管理者としてアク セスする人に対して、IdP にて次の値を設定してください: urn:mace:gakunin.jp:entitlement:federated-id.eduroam.jp:site-admin また、発行済みアカウントの確認と失効のみが可能なサブ機関管理者としてアクセスする人に対しては、以下の値を設定してください: urn:mace:gakunin.jp:entitlement:federated-id.eduroam.jp:site-subadmin

送信されている属性情報の確認は次のURLにアクセスすることで可能です: https://federated-id.eduroam.jp/secure/

2.1 IdPへの設定例

学認参加IdPへの設定例は以下のとおりです。

本設定例は学認配布のテンプレート(*1)をベースとした設定ファイルに追加することを想定しております。
　Shibboleth IdPインストール時に作成されるデフォルトの設定ファイルや、独自の設定ファイルをご利用の場合には動作しない可能性がありますので、その場合は適宜読み替えて設定してください。
　(*1) IdP構築関連ファイル
　　https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=12158262

2023/11/28更新　Shibboleth IdP v4版

```
--------attribute-resolver.xmlに追加--------------
   <AttributeDefinition xsi:type="Mapped" id="eduPersonEntitlementForEduroamFedID">
        <InputDataConnector ref="myLDAP" attributeNames="uid" />
        <DefaultValue passThru="false"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:eduPersonEntitlement" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7" friendlyName="eduPersonEntitlement" encodeType=
"false" />
        <ValueMap>
             <ReturnValue>urn:mace:gakunin.jp:entitlement:federated-id.eduroam.jp:site-admin</ReturnValue>
             <SourceValue>test002</SourceValue>
             <SourceValue>ID2</SourceValue>
             <SourceValue>ID3</SourceValue>
        </ValueMap>
    </AttributeDefinition>

--------attribute-filter.xmlに追加--------------
<!-- Policy for Eduroam FederatedID -->
<AttributeFilterPolicy id="PolicyforEduroamFederatedId">
<PolicyRequirementRule xsi:type="Requester" value="https://federated-id.eduroam.jp/shibboleth-sp" />
   <AttributeRule attributeID="eduPersonTargetedID">
       <PermitValueRule xsi:type="ANY" />
   </AttributeRule>
   <AttributeRule attributeID="organizationName">
       <PermitValueRule xsi:type="ANY" />
   </AttributeRule>
   <AttributeRule attributeID="eduPersonAffiliation">
       <PermitValueRule xsi:type="ANY" />
   </AttributeRule>
   <AttributeRule attributeID="eduPersonEntitlementForEduroamFedID">
       <PermitValueRule xsi:type="ANY" />
   </AttributeRule>
</AttributeFilterPolicy>
```

2017/9/25修正　Shibboleth IdP v3.2以降対応版

```
--------attribute-resolver.xmlに追加--------------
<resolver:AttributeDefinition xsi:type="ad:Mapped" id="eduPersonEntitlementForEduroamFedID" sourceAttributeID="uid">
    <resolver:Dependency ref="myLDAP" />
    <resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:dir:attribute-def:eduPersonEntitlement" encodeType="false" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7" friendlyName="eduPersonEntitlement" en
codeType="false" />
    <ad:ValueMap>
         <ad:ReturnValue>urn:mace:gakunin.jp:entitlement:federated-id.eduroam.jp:site-admin</ad:ReturnValue>
         <ad:SourceValue>ID1</ad:SourceValue>
         <ad:SourceValue>ID2</ad:SourceValue>
         <ad:SourceValue>ID3</ad:SourceValue>
    </ad:ValueMap>
</resolver:AttributeDefinition>


--------attribute-filter.xmlに追加--------------
<!-- Policy for Eduroam FederatedID -->
<AttributeFilterPolicy id="PolicyforEduroamFederatedId">
<PolicyRequirementRule xsi:type="Requester" value="https://federated-id.eduroam.jp/shibboleth-sp" />
   <AttributeRule attributeID="eduPersonTargetedID">
       <PermitValueRule xsi:type="ANY" />
   </AttributeRule>
   <AttributeRule attributeID="organizationName">
       <PermitValueRule xsi:type="ANY" />
   </AttributeRule>
   <AttributeRule attributeID="eduPersonAffiliation">
       <PermitValueRule xsi:type="ANY" />
   </AttributeRule>
   <AttributeRule attributeID="eduPersonEntitlementForEduroamFedID">
       <PermitValueRule xsi:type="ANY" />
   </AttributeRule>
</AttributeFilterPolicy>
```

ID1, ID2, ID3の部分は、機関管理者としてedurPersonEntitlementを送信するユーザのIDに置き換えて、必要な人数分だけ記入してください。

※2017/9/19以前の記述はIdPv3系では正常に動作しない可能性がございます。
※2017/9/20更新版では、IdPv3.2系列で動作しない可能性がありますので、現在のバージョンに差し替えてください。こちらは3.2および3.3の両系列で動作します。
※Shibboleth IdP v3.1以前をご利用の場合は、IdPをアップデートいただくか、適宜読み替えて設定してください。

3. 機関管理者ログイン

本サービスサイトからログインを行うと まず学術認証フェデレーションの認証が要求されます。 認証が成功すると、メニューが表示されます。管理者としてログインした場合は、以下の「管理者機能」のメニューが追加されます。

- 所属機関の発行アカウント状況確認機能
- 所属機関の学生アカウント発行可否設定機能
- 所属機関の学生アカウント継続確認機能
- 所属機関の学生アカウント利用期間上限設定機能
- 所属機関の学生アカウントのレルム区別設定機能
- 所属機関の本人用アカウント発行数上限設定機能
- ビジター用アカウント発行数上限設定機能（利用範囲制限なしに対応）
- ビジター用アカウント発行数上限一時緩和機能

3.1. 所属機関の発行アカウント状況確認機能

所属機関の利用者が発行したアカウントの一覧の確認と失効ができます。一覧はアカウントの発行者ごとに表示され、発行者はeduPersonTargetedIDで区別されます。

発行者を識別するIDとしてeduPersonTargetedIDのハッシュ値の部分のみが表示されます。たとえばハッシュ値としてABCDEF1234567890が見えている場合、IdPから送信されているeduPersonTargetedIDは

<IdPのentityID>!https://federated-id.eduroam.jp/shibboleth-sp/!ABCDEF1234567890

となります。

機関管理者は、当該機関に属する利用者が発行したアカウントの失効を行うことができますが、機関管理者がアカウントを失効させた場合は、失効を行った管理者に関する情報が記録されます。

なお、有効期限が切れているアカウントは、すでに無効となっているため、失効操作はできません。

アカウントの失効情報は、一日に一回、認証サーバと同期を行いますが、すぐに失効情報を反映したい場合は「失効反映」をクリックしてください。

一覧表示では改ページの機能は実装されておりませんが、1万件表示して支障がないことを確認しています。多数のアカウントの一覧表示に関して支障が発生するようであればお知らせください。

「有効アカウントの一括取得」サブメニューより、有効アカウントの一覧をCSVでダウンロードできます（ダウンロードするアカウントの条件を指定してフィルターをかけることができます）。また、「アカウントの一括失効」サブメニューより、CSVをアップロードすることで、一括失効を行うことができます。一括失効したいアカウントの指定は、ダウンロードしたCSVの1列目のフラグを1にしてアップロードすることで行います。なお、一括失効作業は 1,000 アカウントまでとなっています。

3.2. 所属機関の学生アカウント発行可否設定機能

利用者が学生（eduPersonAffiliationがstudent）の場合の、アカウント発行可否を切り替えます。初期値は発行不可です。

3.3. 所属機関の学生アカウント継続確認機能

学生に対して、年度ごとの継続確認を行う場合に利用します。「学生アカウント継続確認開始機能」を実行してから「学生アカウント継続確認終了機能」を実行するまでの間、学生がログインした場合に、継続確認が行われます。学生の利用者が継続確認期間中にログインすると、その時点で有効なeduroamのアカウントがある場合に、継続確認を促すメッセージが表示され、「継続利用」か「失効」かを選択します。継続確認期間終了後に、確認がなされなかった、あるいは、失効を選択した学生利用者が発行したアカウントについて、一斉失効が行われます。

管理者が「学生アカウント継続確認開始機能」をクリックすると、学生利用者に対して、継続確認を行う期間等を通知するためのメッセージが入力できます。このメッセージは、前述の学生の利用者が継続確認期間中にログインした際に表示される、継続確認を促すメッセージとともに表示されます。

3.4. 所属機関の学生アカウント利用期間上限設定機能

3か月から1年までの間で1か月単位で設定することが可能です。初期値は3か月です。

3.5. 所属機関の学生アカウントのレルム区別設定機能

学生が発行するアカウントのレルムと、教職員が発行するアカウントのレルムを区別できるようにします。区別を有効にした場合、教職員に対しては、従来通りレルムとして「DDD.f.eduroam.jp」が用いられますが、学生に対してはレルムとして「DDD.s.eduroam.jp」 が利用されます。これにより、たとえば機関内での学生と教職員の接続先ネットワークを別にするなどの制御に活用することができます。管理者メニューで設定を変更すると、それ以降に発行される学生のアカウントのレルムが変更されます。発行済みのアカウントは元のレルムのまま有効ですので、必要に応じて失効処理と再発行依頼をしてください。

3.6. 所属機関の本人用アカウント発行数上限設定機能

機関毎に設定することが可能です。初期値は5です。0を指定することでビジター用アカウントのみ発行可能とすることができます。

3.7. ビジター用アカウント発行数上限設定機能

各利用者（教職員に限る）がビジター用に発行可能な（同時に有効な）アカウント数の上限（最大有効期間 1 週間、最大有効期間 1 か月、それぞれについて）をシステム上で直接設定できます。初期値は、いずれも0です（発行不可）。最大有効期間 1 か月のアカウント数の上限のみを設定することも可能です。

3.8. ビジター用アカウント発行数上限一時緩和機能（代理認証機能）

大きな会議の開催時など、まとまった数のビジター用アカウントが必要な場合に、特定の利用者（教職員に限る）に対して、発行できる（同時に有効な）ビジター用アカウントの数を一時的に緩和させることができます。通常時のビジター用アカウントの発行は不可としつつ、発行数上限一時緩和機能を用いて、一時的に特定の利用者にビジター用アカウントの発行を許可することも可能です。期間上限は最長13ヶ月まで設定できます。また、代理認証機能この機能の利用範囲制限なしアカウント作成によって実現されています。

一時緩和する際は、以下の入力項目を設定します。

- 上限緩和有効化パスワード：利用者がこのパスワードを投入することで、一時的な緩和が有効になります。（通常時の個人管理のビジター用アカウントは発行できなくなります。発行済みのビジター用アカウントは継続して有効です。）緩和状態は、機関管理者がこの設定を削除するまで継続して有効です（利用者が自身で解除することはできません）。一度設定されたパスワードの変更はできません。変更のためには一旦削除して再設定してください。
- 発行数上限緩和値：一時的に緩和する発行数の上限を指定します。パスワードを投入した利用者による平常時に発行済みの個人管理のビジター用アカウントの数は積算されません。ID/Password に関しては 10万、EAP-TLS では 1千 まで指定可能です。なお、管理者が緩和設定を解除した後は、緩和適用中に発行されたビジター用アカウントの数は、個人管理のビジター用アカウント数には積算されません。再度異なる緩和設定の適用を受けた場合、前回の緩和設定によって発行されたビジター用アカウントの数は積算されません。
- 緩和可能ユーザ数：パスワードを投入することで、この緩和設定が適用される利用者数の上限を指定します。一般には1を指定します（最大30）。
- 利用範囲制限なしアカウント作成：「許可」を選択すると、アカウント発行機関限定の利用範囲制限がかからないアカウントも発行することが可能となります。「禁止」を選択すると、これまで通り、利用範囲制限のあるアカウントのみの発行となります
- メモ：この緩和設定によって発行されるビジター用アカウントの用途（会議名）などを記載しておくために利用できます。

機関管理者は設定を行った後、パスワードを、まとまった数のビジター用アカウントを発行したい利用者に通知してください。パスワードを受け取った利用者は、ビジター用アカウントの発行済みアカウント確認画面でパスワードを投入することで、緩和設定が適用されます。パスワード入力フィールドは、緩和設定が存在している場合にのみ出現します。（一度、パスワードを投入して緩和設定が有効になると、さらなるパスワードの投入はできなくなります。別のパスワードを投入して、別の緩和設定に切り替えることはできません。）緩和設定適用済みのユーザには、ビジター用アカウント発行機能のメニュー画面などで、その旨が表示されます。

3.9 ビジター用アカウントの利用範囲制限

ビジター用アカウントの利用範囲制限が適用されます。原則として、ビジター用アカウントを発行した機関のネットワークでのみ利用可能となりますが、複数の機関にまたがって利用させたい等のご要望がある場合は、ご相談ください（必ずしもご要望にお応えできるとは限りません）。

ビジター用アカウント発行数上限一時緩和機能において許可することにより、利用範囲制限のないアカウントの発行も可能となります。

改定履歴

2023/3	3.1. 所属機関の発行アカウント状況確認機能	（追加）一括失効の上限について
2024/3	3.8. ビジター用アカウント発行数上限一時緩和機能	（追加）代理認証機能の記述 （追加）発行上限数を 1,000 から数万へ（上限については開示していません） （追加）有効期間を13ヶ月
2024/3	2. IdPが送信するべき属性	（改定）属性に関する説明を表にまとめました
2024/3	2. IdPが送信するべき属性	（改定）注意事項を移動
2023/11	2.1 IdPへの設定例	（追加）Shibboleth 4 設定例
2022/4	3.6. 所属機関の本人用アカウント発行数上限設定機能	（追加）ビジターアカウントのみ発行させたい場合
2021/4	3.8. ビジター用アカウント発行数上限一時緩和機能	（追加）有効期間延長

2020/2	3. 機関管理者ログイン	（追加）所属機関の発行アカウント状況確認機能、所属機関の学生アカウントのレルム区別設定機能
2020/2	3.1. 所属機関の発行アカウント状況確認機能	（追加）CSV アップロードによる一括失効操作
2020/2	3.5. 所属機関の学生アカウントのレルム区別設定機能	（追加）学生・教職員をレルムで区別する
2019/4	3.8. ビジター用アカウント発行数上限一時緩和機能 3.9 ビジター用アカウントの利用範囲制限	（追加）利用範囲制限なしアカウント作成
2018/11	3.1. 所属機関の発行アカウント状況確認機能	（追加）失効操作の記録
2018/11	3.3. 所属機関の学生アカウント継続確認機能	（追加）年度更新時期の学生アカウントの継続確認
2018/4	3.9 ビジター用アカウントの利用範囲制限	（追加）利用範囲制限を適用
2017/9	2.1 IdPへの設定例	（追加）Shibboleth 3.2 設定例