

eduPersonTargetedID

仕様

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【SAM L1】	"urn:oid:1.3.6.1.4.1.5923.1.1.1.10"
name【SAM L2】	"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の値はそれぞれ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=

属性定義の例（attribute-resolver.xml）

```
<!-- Attribute Definition for eduPersonTargetedID (computedID) -->
<resolver:AttributeDefinition xsi:type="ad:SAML2NameID" id="eduPersonTargetedID"
    nameIdFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
    sourceAttributeID="computedID">
    <resolver:Dependency ref="computedID" />
    <resolver:AttributeEncoder xsi:type="enc:SAML1XMLEObject" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" encodeType="false" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2XMLEObject" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" friendlyName="
eduPersonTargetedID" encodeType="false" />
</resolver:AttributeDefinition>
```

```
<!-- Computed targeted ID connector -->
<resolver:DataConnector id="computedID" xsi:type="dc:ComputedId"
    generatedAttributeID="computedID"
    sourceAttributeID="uid"
    salt="*****YOUR_SALT*****">
    <resolver:Dependency ref="myLDAP" />
</resolver:DataConnector>
```

