

SpringerLinkに関する情報

- Springerの利用プロトコル： SAML2.0
- SpringerのSAML実装： OpenAM
- Springerへの属性送信の設定例：
SpringerのentityIDは <https://fsso.springer.com> ですが、このSPは属性を必要とせず、IdPのentityIDを見て機関の確認をしていますので、attribute-filter.xmlの設定は不要です。

IdPが送出するTransient IDについての注意

SpringerはentityIDを見ているため属性情報の送出は不要です。しかし、SpringerではTransient IDが送出されない場合にはIdPでの認証後に以下のようにエラーとなることがわかっています。



学認で提供している構築手順による標準的な設定の場合はすべてのSPに送信されますが、Transient IDの送出先を制限している場合には対象となるentityIDへTransient IDが送出されるようになっていくかご確認ください。以下のコマンドで確認することも可能です。出力の<saml2:NameID ...>の部分のFormat属性がFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"であることを確認してください。

```
$ /opt/shibboleth-idp/bin/aaccli.sh --principal="ユーザ名" --requester="https://fsso.springer.com" --saml2
```

IdPメタデータに記載する証明書についての注意

IdPが有効期限切れの証明書をアサーションの署名に使っているとエラーになることが確認されていますので、期限内に[メタデータ記載の証明書更新手順 \(IdP\)](#)の手順に従って証明書を更新するようご注意ください。

なお、以前はIdPのメタデータに複数の証明書が記載されている場合にエラーとなっていたましたが、現在はこの問題は解消されていることが確認できています。

IdPが送出するAuthentication Context Classについての注意

また、IdPが生成するアサーションに含まれるAuthentication Context Class (Authentication Method)にも制限があります。技術ガイドに沿って構築したIdPであれば問題ありません (PasswordProtectedTransport になります) が、この部分をカスタマイズしている場合はご注意ください。

Authentication Context Classを確認するには、以下のURLの <IdPのentityID> の部分をご自身のIdPに変更してアクセスし、認証してください。
<https://attrviewer20.gakunin.nii.ac.jp/Shibboleth.sso/DS?entityID=<IdPのentityID>&authnContextClassRef=urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified&authnContextComparison=minimum&target=/Shibboleth.sso/Session>
そうするとAuthentication Context Classが以下のような形で表示されます。

Authentication Context Class: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

この値が以下の値以外の場合、Springerでは上記と同じエラーが表示されます。

- urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
- urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard
- urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken
- urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI
- urn:oasis:names:tc:SAML:2.0:ac:classes>Password
- urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
- urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
- urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract
- urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony
- urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword
- urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
- urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered
- urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony
- urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI

- urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
- urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
- urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig
- urn:oasis:names:tc:SAML:2.0:ac:classes:X509
- urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony
- urn:oasis:names:tc:SAML:2.0:ac:classes:PGP
- urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword
- urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
- urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport
- urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI
- urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalTelephony