

SAML2でバックチャネル接続エラー

SAML2でIdPに接続したときに下記のようなバックチャネルの接続エラーが発生することがあります。

```
2012-11-16 17:45:00 ERROR Shibboleth.AttributeResolver.Query [6]: exception during SAML query to https://idp.example.ac.jp:8443/idp/profile/SAML2/SOAP/AttributeQuery: CURLSOAPTransport failed while contacting SOAP endpoint (https://idp.example.ac.jp:8443/idp/profile/SAML2/SOAP/AttributeQuery): connect() timed out!
2012-11-16 17:45:00 ERROR Shibboleth.AttributeResolver.Query [6]: unable to obtain a SAML response from attribute authority
```

→上記のエラーはIdP(idp.example.ac.jp)のattribute-filter.xmlに接続元SPへの属性送出設定がない(属性が受け渡されない)とき、SAML2でBack-Channelポートにfallbackするため発生します。IdP側のファイアウォールなどでBack-Channel(ポート8443)への接続が許可されていない場合にタイムアウトとなることがあります。いずれにしろ設定により属性は渡されませんので、このエラーによる実害は（ブラウザ表示の遅延以外は）特にありません。

→SAML2対応IdPのみ接続するときに「SPでBack-Channelを使用しないようにする設定」を以下に記載します。学認外のIdPと連携する場合など、SAML1で属性受け渡しをする可能性があるときは属性取得できなくなりますので、SAML2でかつBack-Channelを利用しないときだけに用いてください。

- /etc/shibboleth/shibboleth2.xml で次の部分をコメントアウト

```
<!-- Use a SAML query if no attributes are supplied during SS0. -->
<!--
<AttributeResolver type="Query" subjectMatch="true"/>
-->
```