ユーザアクセスのロギング

ユーザアクセスのロギング

IdPの運用において、インシデント発生時の対応のためには、ユーザ認証の記録をログファイルに出力しておくことが必要となります。特に、SPに対してeduPersonPrincipalNameのような個人識別可能な属性を渡さない場合は、セッションの識別子やeduPersonTargetedIDなどが手がかりとなります。

IdPにおいてログに記録するための一つの方法としては、attribute-resolver.xmlに以下のような定義を追加（<AttributeResolver></AttributeResolver>の内側)する方法があります(Shibboleth IdP 3.2.1以降で動作確認)。

● eduPersonTargetedIDの定義でComputedIDを用いている場合

以下の例では、指定したSP（ここでは https://shiken-sp00.nii.ac.jp/shibboleth-sp）に対して送信される属性のみがログに記録されます。

Shibboleth IdP V4以降向け

```
<AttributeDefinition id="eduPersonTargetedIDLogging" xsi:type="ScriptedAttribute">
    <!-- Inputs that provides the source attribute. -->
    <InputDataConnector ref="computedID" attributeNames="computedID" />
    <InputAttributeDefinition ref="eduPersonPrincipalName" />
    <Script><![CDATA[
        logger = Java.type("org.slf4j.LoggerFactory").getLogger("net.shibboleth.idp.attribute");

        if ( resolutionContext.attributeRecipientID.equals("https://shiken-sp00.nii.ac.jp/shibboleth-sp") ) {
            logger.info(
                "eduPersonPrincipalName : " + eduPersonPrincipalName.getValues().get(0).getValue()
                    + '@' + eduPersonPrincipalName.getValues().get(0).getScope()
                + " , eduPersonTargetedID : " + computedID.getValues().get(0)
                );
        }
    ]]></Script>
</AttributeDefinition>
```

Shibboleth IdP 3.xでJava 8 以降の場合

```
    <resolver:AttributeDefinition id="eduPersonTargetedIDLogging" xsi:type="Script" xmlns="urn:mace:shibboleth:2.0:resolver:ad">

      <!-- Dependency that provides the source attribute. -->
      <resolver:Dependency ref="computedID" />
      <resolver:Dependency ref="eduPersonPrincipalName" />

      <Script><![CDATA[
                 logger = Java.type("org.slf4j.LoggerFactory").getLogger("net.shibboleth.idp.attribute");

           if (  resolutionContext.attributeRecipientID.equals("https://shiken-sp00.nii.ac.jp/shibboleth-sp") ) {
               logger.info(
                      "eduPersonPrincipalName : " + eduPersonPrincipalName.getValues().get(0).getValue()
                             + '@' + eduPersonPrincipalName.getValues().get(0).getScope()
                      + " , eduPersonTargetedID : " + computedID.getValues().get(0)
                     );
           }
      ]]></Script>
    </resolver:AttributeDefinition>
```

Shibboleth IdP 3.xでJava 7 の場合

```
        <resolver:AttributeDefinition id="eduPersonTargetedIDLogging" xsi:type="Script" xmlns="urn:mace:shibboleth:2.0:resolver:ad">


          <!-- Dependency that provides the source attribute. -->
          <resolver:Dependency ref="computedID" />
          <resolver:Dependency ref="eduPersonPrincipalName" />

          <Script><![CDATA[
               importPackage(Packages.org.slf4j);

               logger = LoggerFactory.getLogger("net.shibboleth.idp.attribute");

               if (  resolutionContext.attributeRecipientID.equals("https://shiken-sp00.nii.ac.jp/shibboleth-sp") ) {
                   logger.info(
                          "eduPersonPrincipalName : " + eduPersonPrincipalName.getValues().get(0).getValue()
                                  + '@' + eduPersonPrincipalName.getValues().get(0).getScope()
                           + " , eduPersonTargetedID : " + computedID.getValues().get(0)
                         );
               }
          ]]></Script>
        </resolver:AttributeDefinition>
```

定義を追加したあと、Tomcatの再起動を行い設定を反映してください。

idp-process.logに次のようなメッセージが出力されるようになります。なお、ログレベルはINFOになっていますので、logback.xmlの設定も必要に応じて調整してください。

```
2016-08-31 13:57:02,281 - INFO [net.shibboleth.idp.attribute:-2] - eduPersonPrincipalName : test001@nii.ac.jp , eduPersonTargetedID :
LkDwL3dNSb9FBr3TNP0g3D9F7mk=
```

● eduPersonTargetedIDの定義でStoredIDを用いている場合

上の例で `computedID` を全て `storedID` に置き換えてください（置き換える個所には下線を引いています）。

参考：eduPersonTargetedIDでComputedIDを使う方法は eduPersonTargetedID に記載されています。