設定（IdP）

設定

以下の※を一読した上で次の手順を順に実行してください。

- Shibbolethの設定
    1. metadata-providers.xml
       主な設定内容: メタデータの参照設定（自動ダウンロードなど）
    2. idp.properties
       主な設定内容: entityIDやScopeなどIdPの設定（証明書や認証方法も含む）
    3. ldap.properties
       主な設定内容: 認証先LDAPの設定
       （ldapURL，useStartTLS, baseDN， subtreeSearch, userFilter， bindDN）
    4. saml-nameid.properties
       主な設定内容: idp.persistentIdの設定
    5. secrets.properties
       主な設定内容: LDAPのパスワード（bindDNCredential）やsaltの設定
    6. attribute-resolver.xml
       主な設定内容: IdPで取り扱う属性情報の設定
       属性情報の取得元の設定(LDAP，ComputedID等)
    7. attribute-filter.xml
       主な設定内容: attribute-resolverで設定した属性情報のうち 送信する属性を各SP毎に設定。
    8. 属性送信同意画面の設定（IdP）
       主な設定内容: V4.1以降デフォルトで無効化された属性送信同意機能を有効化。

- サーバ証明書の申請と設定
    1. サーバ証明書の設定

ログ確認（※）

※ 設定ファイルを変更したら必ずプロセスを再起動しログを確認すること

実習環境ではIdPのログは以下に出力されます。

- **/opt/shibboleth-idp/logs/idp-process.log**
  IdPの動作ログです。IdPのエラーや警告が記載されます。IdPの動作に問題が発生した場合には、まずこちらを参照下さい。
- **/opt/shibboleth-idp/logs/idp-audit.log**
  IdPからSPへの送信ログです。発生日時、相手側ID、送信した属性といった情報が含まれます。
  フォーマット：

```
auditEventTime | requestBinding | requestId | relyingPartyId | messageProfileId |
assertingPartyId | responseBinding | responseId | principalName | authNMethod |
releasedAttributeId1,releasedAttributeId2, | nameIdentifier | assertion1ID,assertion2ID, |
```

なお、これらログファイルに関する設定は、/opt/shibboleth-idp/conf/logback.xmlにあります。

上記のログファイルでエラーの原因が特定できない場合、以下に挙げたJettyのログファイルをご確認ください。どのファイルにどのような内容が書き出されるかは定かではありませんが、service.xmlやinternal.xmlの記述ミスのような低レベルなエラーがこれらに出力されます。2つのファイルをチェックするようにしてください。経験上有益な情報を含んでいるものから順に書いています。

- **/opt/jetty-base/logs/<日付>.jetty.log**
- **/opt/jetty-base/logs/access.log**

このページに探している情報がない場合、下記のWikiスペースにも有益な情報が掲載されていますので、あわせてご覧ください。
⇒meatwiki:GakuNinShare