旧：IdPセッティング

旧：設定と接続テスト

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。

- OpenLDAPの設定（貴学でIdPをインストールする場合のみ）
  - 学認で利用するスキーマの導入
- Shibbolethの設定
  1. relying-party.xml（★）
     主な設定内容: entityIDの設定、メタデータ自動ダウンロードの設定
  2. handler.xml（★）
     主な設定内容: ログインのしくみの設定
     ⇒TypeをUsernamePasswordとし login.config を参照するだけ。
  3. login.config（★）
     主な設定内容: 認証先のLDAP設定
     （ldapURL，baseDn， userFilter，subtreeSearch，SSL）
  4. 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)
  5. 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。
- サーバ証明書の申請と設定
  1. サーバ証明書の取得とApacheの設定（★）
  2. メタデータの作成と提出（★）
  3. Back-Channelの設定

- 接続テスト
  - テストSPを利用した接続テスト（★）

※ 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-access.log**
  IdPのアクセスログです。IdPへのアクセス日時やアクセス元といった情報が含まれます。
  フォーマット：

```
requestTime | remoteHost | serverHost|serverPort | requestPath
```

- **/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/logging.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Tomcat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。「Xerces-JのClassNotFoundはlocalhost*にしか出力されない」「TLSのログはcatalina.outにしか出力されない」のようなこともあります（逆に複数ログに記録されるものもありますが）ので、くれぐれも3つのファイル全て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。

- **$CATALINA_BASE/logs/catalina.out**
- **$CATALINA_BASE/logs/localhost.<日付>.log**
- **$CATALINA_BASE/logs/catalina.<日付>.log**

構築後のカスタマイズ

- 属性管理（登録、変換、リリース方法）

- 新規SPの登録方法
- ユーザアクセスのロギング
- 認証方法の変更、設定（証明書による認証）
- LDAPの新規作成方法
  本ページ先頭の「OpenLDAPの設定」の項をご覧ください。
- StoredIDを利用するための設定
- IdPアップデート手順 (*はセキュリティフィックス)
  - 2.3.0(*) 情報交換ML:00346 情報交換ML:00348
  - 2.3.2(*) 情報交換ML:00366 不具合対策方法:情報交換ML:00415
  - 2.3.5 情報交換ML:00414 情報交換ML:00419
  - 2.3.6(*)
  - 2.3.8
  - 2.4.0(*)
  - 2.4.1,2.4.2(*) 情報交換ML:00855
  - 2.4.3(*) 情報交換ML:00876
  - 2.4.4(*) 情報交換ML:00915
  - 3.0.0以上 情報交換ML:00879, 情報交換ML:00880, GakuNinShare:Shibboleth IdP 3, シボレス実習活用編, 貴学にてIdPv4をインストールする場合の構築手順
- メタデータ記載の証明書更新手順（IdP）

ノウハウ

- 既存システムへの変更点を最小限にしたまま eduPerson 形式での属性受け渡しの実現方法（含：Mapped AttributeDefinition等による属性マッピング方法）
  （2008年度実証実験にて大阪大学提供）
- OpenSSO と Shibboleth 2.0 の SAML 2.0 連携
  （2008年度実証実験にて大阪大学提供）
- プライバシを考慮したID受け渡し（含：データベースを用いたeduPersonTargetedIDの提供方法）
  （2008年度実証実験にて京都産業大学提供）
- ロードバランサー配下のシボレスIdP環境設定に関する検証実験
  - IdPサーバにおけるTerracottaサーバ、Terracottaクライアント（Tomcat）の自動起動について
  - IdPサーバにおけるTerracottaサーバ、Terracottaクライアント（Tomcat）の起動確認について
- Active DirectoryにおけるeduPersonスキーマ（拡張スキーマ）の利用
  （成城大学提供）
- Active Directoryにおけるツリー情報をePSAに利用する方法（含：Script AttributeDefinitionによる属性変換方法）
  ※ Active DirectoryをLDAPサーバとしてShibboleth IdPと連携する場合は、Shibboleth Wikiの以下のページもご参照ください。
  ⇒LdapServerIssues
- Google Appsの接続方法
  （山形大学提供）
- ユーザ同意取得システム：uApprove JP
- 特定SPに対するユーザ毎のアクセス制限（FPSPプラグイン）
- Shibboleth用多要素認証導入のための技術ガイド（学認春CAMP2014 金沢大学資料）
  Shibboleth IdPの認証機能を拡張するための導入として、最適な資料です。
- IdPのホスト名変更に関する注意点

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