IdPv4セッティング

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。（IdPv2の旧IdPセッティング、IdPv3の旧IdPセッティング）

- 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. 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， bindDNCredential）
  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(IdPv4)
     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。
  9. IdPのサービス動作状況の確認

- 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

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, |
```

- **/opt/shibboleth-idp/logs/idp-consent-audit.log**
  利用者が属性送信もしくは利用規約(ToU)に同意した場合、もしくは拒否した場合、もしくは同意内容を変更した場合に記録されます。

ただし、CentOS 7においてidp-process.logに出力されるべきログがTomcat起動当初に限って誤って **/var/log/messages** に出力される場合があるようですので、上記ファイルで確認できない場合はこちらもご参照ください。messagesへの出力はフォーマットが若干異なり以下のようになります。日付、ホスト名の後の" server: "がポイントです。

```
Mar 15 19:26:18 machine1 server: 2019-03-15 19:26:18.612 [ WARN] : net.shibboleth.ext.spring.config.
StringBooleanToPredicateConverter: ...
```

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。上記ファイルが見当たらない場合は/opt/shibboleth-idp/dist/conf/logback.xml との差分を確認してください。

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。
- eduPersonTargetedIDにStoredIDを利用するための設定
- メタデータ記載の証明書更新手順（IdP）
- IdPアップデート手順
- SPにおけるAES-GCM暗号対応状況

ノウハウ

- 特定SPに対するユーザ毎のアクセス制限（IdPv2のFPSPプラグイン相当）
- 送信属性同意機能の設定について（IdPv2のuApprove JPプラグイン相当。新規構築の場合はデフォルトで有効化されています）
- IdPのホスト名変更に関する注意点

以下のノウハウは主にIdPv2向けですが、IdPv3向けにも有用な情報がありますのでご参照ください。

- 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）
- 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）
- 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。

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