ＳＳＯ実証実験のためのIdP構築

東北大学における事例紹介

東北大学 情報部 情報推進課
安西　従道

東北大学における実証実験

- シングルサインオン(SSO)実証実験のための
  シンプルな環境を構築。

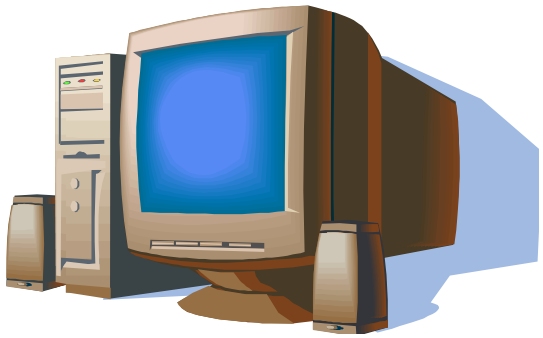
- IdPで使用するユーザ体系として、構築作業中
  の東北大ID（仮）の形式を参考に構築し、運用の
  テスト環境とする。

- 東北大ID環境におけるShibbolethによる、SSO
  導入のテストベッドとしても考える。

ハードウェア構成

- HP ProLiant ML110 G5

CPU	:	Xeon X3210 2.13GHz
Memory	:	2GB
HDD	:	SATA 3.5 250GB
CD or DVD	:	SATA DVD RW



ソフトウェア構成

- OS：CentOS 5.1 x86_64
- Java SE Development Kit (JDK) 6u7 (1.6)
- openssl 0.9.8b
- openLDAP 2.3.27
- Apache 2.2.3
- Apache ant 1.6.5
- Tomcat 6.0.18
- Shibboleth-idp-2.0.0

IdP構築作業概略

- 「IdP構築・運用手順書ver1.0」に従って作業。

  最新版は「IdP構築・運用手順書Ver1.2」(2008/09/23)

- UPKI「サーバ証明書発行・導入における啓発・評価プロジェクト」よりサーバ証明書を取得。

  UPKIポータルサイト サーバ証明書PJの各種掲載記事を参照し、作業を行った。

- LDAPデータとして、導入予定の「統合電子認証システム」で使用する形式に近いものを、テスト環境として作成。

  今回のテストにより問題なく使用出来ることが確認された。

- Metadataの自動更新に対応。

  2008年10月30日より対応。

IdP構築作業時のトラブル対応(1)

- Tomcat、shibbolethをdebugモードで起動し、情報収集。

Tomcat debugモードでの起動。
/etc/init.d/tomcat のファイルを変更。

```
#
# Start Tomcat
#
$DAEMON_HOME/bin/jsvc \
-debug \     ←追加
```

ログファイル
～/tomcat/logs/catalina.out

shibboleth debugモードでの起動。
/opt/shibboleth-idp-2.0.0/conf/logging.xml
のファイルを変更。
<level value="INFO" /> の箇所を
<level value="DEBUG" /> に変更

ログファイル
～/shibboleth-idp-2.0.0/logs/idp-process.log

- Tomcat 環境変数の修正。(IdP構築･運用手順書ver1.2では対応済み)

1. DAEMON_HOME
DAEMON_HOME=$CATALINA_HOME
2. CATALINA_BASE
CATALINA_BASE=$CATALINA_HOME

IdP構築作業時のトラブル対応(2)

- Metadata更新に関するトラブル。

  Metadataの取扱について、実証実験支援チームからの登録完了のメールと、SSO実証実験リポジトリWebページでのデータ更新にタイムラグがあり、結果 shibboleth の動作に不具合が発生する状態になった。
  このような問題については、Metadata自動更新によって改善されたものと思われる。

- shibboleth-idp-2.0.0/credentials に置いた秘密鍵の ファイルから、パスフレーズを削除。

  /opt/shibboleth-idp-2.0.0/credentials に置いた秘密鍵のファイルに、パスフレーズが有ると tomcat 起動時に idp.war ファイルのデプロイに失敗する現象が見られた。
  このため、以下のコマンドにより秘密鍵ファイルからパスフレーズを削除したファイルを作成し使用した。

  ```
  # openssl rsa -in xxxx.key -out xxxx.key.nonpas
  ```

今後の展望

- IdPについて、東北大IDを使用する運用形態を検討。

- 東北大学統合電子認証システム(構築作業中)での、Shibbolethを利用したSSO環境構築を検討。