IdP･SP構築状況と SSOへの期待

山口大学･大学情報機構･メディア基盤センター

佐伯　徹郎, 王　躍, 永井　好和, 久長　穣

YAMAGUCHI UNIVERSITY

実験目的

- 山口大学大学情報機構メディア基盤センターでは，利用者･提供者（管理者）にとって利用しやすい，独自の統一認証を導入しているが，UPKI SSO実証実験においてはShibbolethを利用した大学間の認証連携を実現しようとしているので，そのための必要な技術や制度等の検証とノウハウの蓄積を目的として実証実験に参加した。

SSO連携実験内容

- IdP･SPの構築
- メタデータ自動更新実験 (IdP･SP)
- メタデータの署名と検証の実験 (IdP･SP)
- ArpViewerの利用

IdP･SPの構築

- 山口大学 Shibboleth-IdP
  - https://idp.cc.yamaguchi-u.ac.jp/
- 山口大学 Shibboleth-SP
  - https://sp.cc.yamaguchi-u.ac.jp/

  Apache

  https://sp.cc.yamaguchi-u.ac.jp/secure/

  Plone

  https://sp.cc.yamaguchi-u.ac.jp/

IdP･SPの構築環境 (1/2)

- IdPサーバ（1台）
  - CPU：Core2Quad 2.40GHz
  - メモリ：16GB
  - HDD：2TB
  - OS：CentOS 5.1
  - 主なソフト：OpenLDAP, Apache, Tomcat, Java

IdP･SPの構築環境 (2/2)

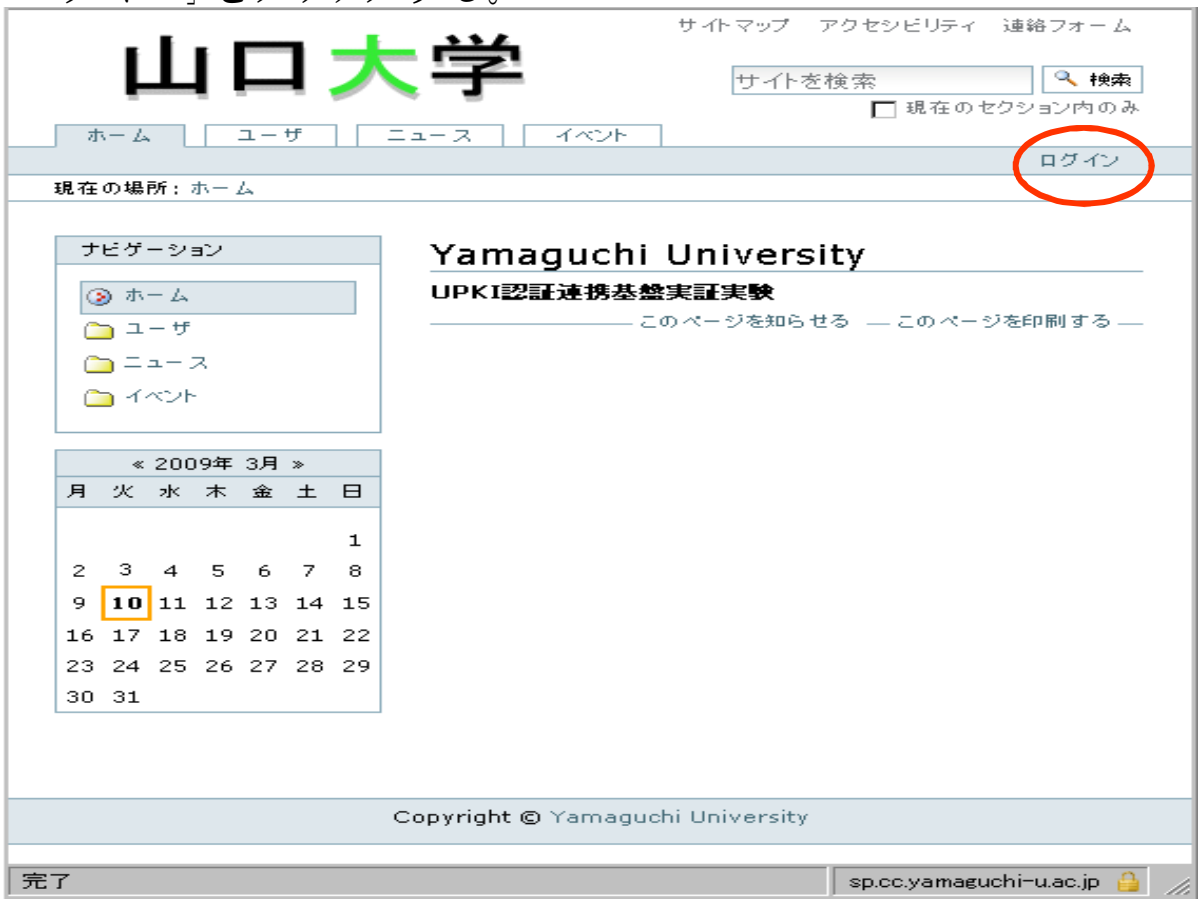
- SPサーバ（1台）
  - CPU：Core2Quad 2.40GHz
  - メモリ：16GB
  - HDD：2TB
  - OS：CentOS 5.1
  - 主なソフト：Apache, Plone, Tomcat, Java

IdP･SPの構築についてのコメント (苦労した点など)

- 手順書にいくつかの誤りが含まれていた。
  - IdP手順書 (Ver.1.2) はかなり改善されているが, SP手順書 (Ver.1.2) の方は誤りがまだ多いようだ
- 設定項目が多いが, 確認方法の記述は少なかった。
  - 設定ミスが起こりやすい
- 設定ファイルの意味についての説明は少なかった。
  - 混乱してしまうことも

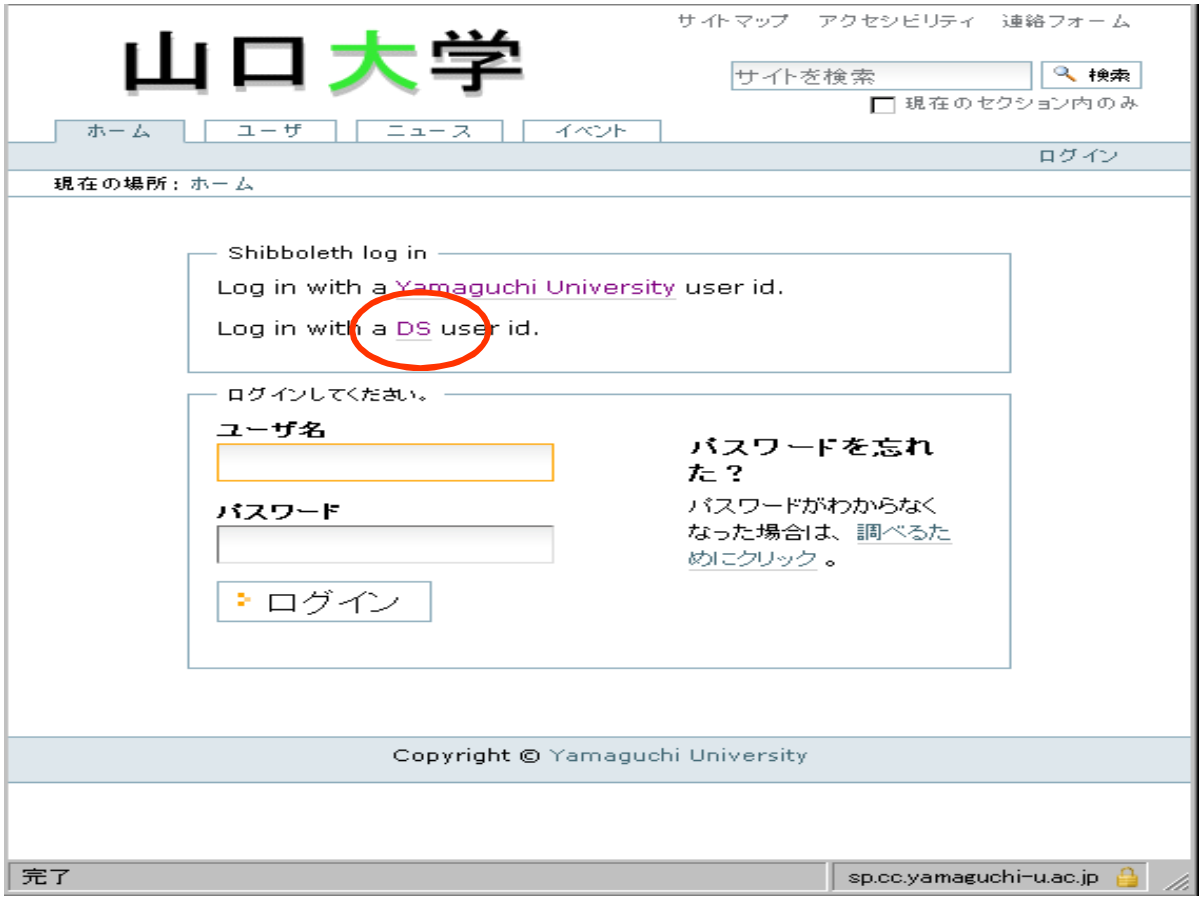
IdP･SPの構築実験結果（接続例1/5）

① 本学Ploneサイト https://sp.cc.yamaguchi-u.ac.jp/ にアクセスし、「ログイン」をクリックする。



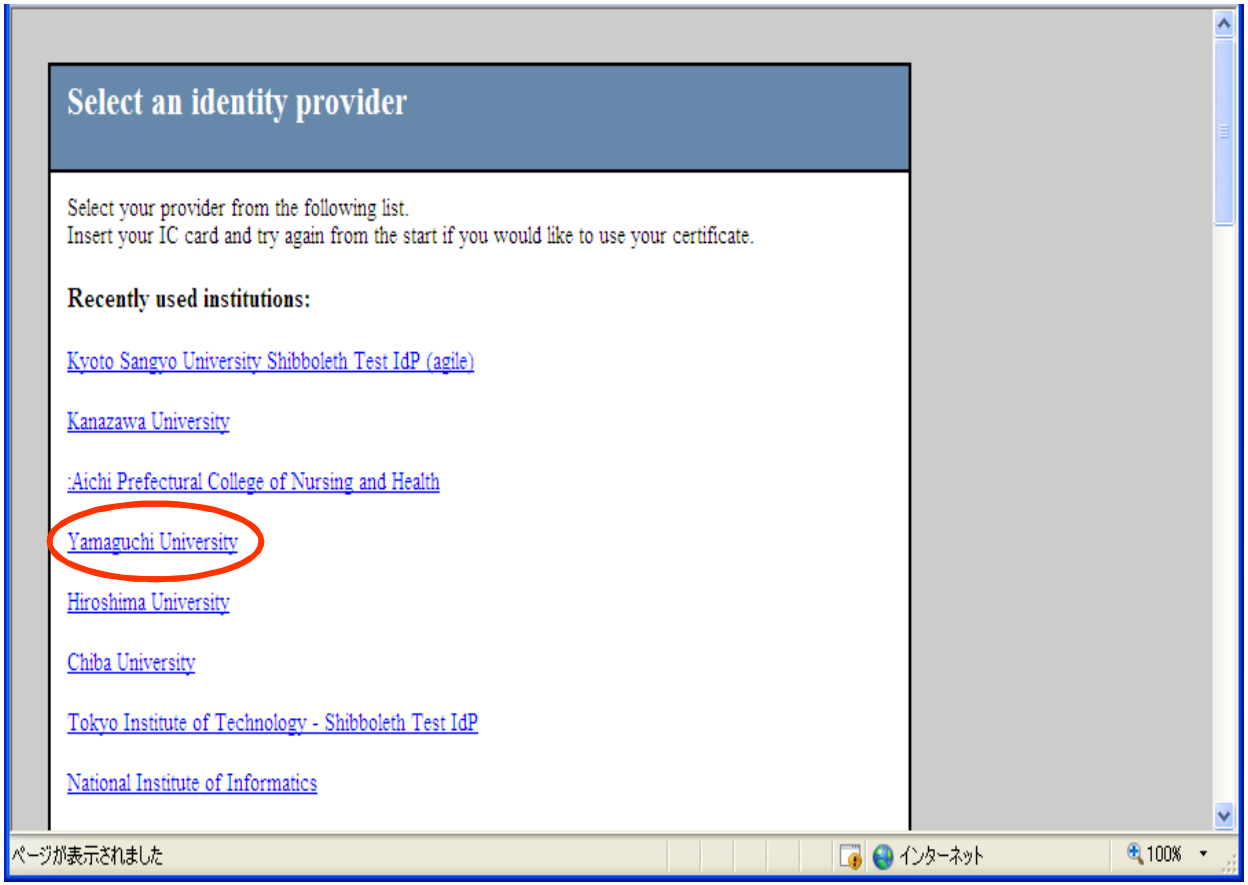
IdP･SPの構築実験結果 (接続例2/5)

② 「DS」を選ぶ。



IdP･SPの構築実験結果 (接続例3/5)

③ 「Yamaguchi University」を選ぶ。



IdP･SPの構築実験結果 (接続例4/5)

④ ユーザ名とパスワードを入力する。

IdP･SPの構築実験結果 (接続例5/5)

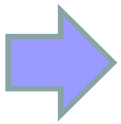
⑤ ログインユーザの属性情報を確認する。

IdP･SPの構築実験結果

- IdP
  - ◆NIIのDSとの連携
  - ◆本学のSP (Apache, Plone)，他大学 (金沢大学, 産業技術大学院大学, 徳島大学)のSP，NIIのSP（Plone1･2, Moodle, CiNii）への接続･SSO
- SP（Apache，Plone）
  - ◆NIIのDSとの連携
  - ◆本学のIdP，NIIのIdPからの接続･SSO

メタデータ自動更新実験 (SP･IdP)

- IdP･SPの設定を変更し，常にリポジトリに配置される最新のUPKI-Fedメタデータを定期的に自動ダウンロードして利用



更新作業が頻繁になることや
更新時の作業ミスを排除

メタデータ自動更新実験結果

■ IdP

◆UPKI-Fedメタデータリポジトリとの連携

IdP･SPのメタデータファイルのタイムスタンプにより,
更新を確認

■ SP

◆IdPと同様

メタデータの署名と検証の実験 (SP･IdP)

- フェデレーション全体のメタデータに署名し，ダウンロードしたサイトで検証

⇒ メタデータの改ざん可能性による
フェデレーション全体に及ぶ
信頼性の低下を防止

メタデータの署名と検証の実験結果 (不正な署名の検証例)

IdP

17:09:32.484 ERROR [edu.internet2.middleware.shibboleth.common.config.BaseService:187] - Configuration was not loaded for shibboleth.RelyingPartyConfigurationManager service, error creating components. The root cause of this error was: Signature trust establishment failed for metadata entry

SP

2009-03-06 18:56:39 ERROR OpenSAML.Metadata.Chaining : failure initializing MetadataProvider: SignatureMetadataFilter unable to verify signature at root of metadata instance.

ArpViewerの利用実験

- ArpViewerの導入

  ⇒ IdPからSPへ送付する
  ユーザ自身の属性内容を確認可能

ArpViewerの利用実験結果（属性内容の確認例）

今後への期待（展望）

- インストールは ports, rpm化
- ユーザ属性の整合性（属性セマンテクス）
- 連携認証の共通ポリシー
- 提供できるサービスの展開

いつでも（つど事務手続きをしなくても），
どこでも（どの大学に行っても），安全・
安心して，自大学にアクセスできる，
UPKI の実現へ