

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 穰

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 (苦勞した点など)

- 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)

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。

The screenshot shows the Yamaguchi University website interface. At the top, there is a search bar and a navigation menu. The 'ログイン' (Login) button is circled in red. Below the navigation menu, there is a calendar for March 2009, with the date '10' highlighted. The footer contains the copyright notice 'Copyright © Yamaguchi University' and the URL 'sp.cc.yamaguchi-u.ac.jp'.

山口大学

サイトマップ アクセシビリティ 連絡フォーム

サイトを検索 検索

現在のセクション内のみ

ホーム ユーザ ニュース イベント

ログイン

現在の場所: ホーム

ナビゲーション

- ホーム
- ユーザ
- ニュース
- イベント

Yamaguchi University

UPKI認証連携基盤実証実験

このページを知らせる — このページを印刷する —

Copyright © Yamaguchi University

完了 sp.cc.yamaguchi-u.ac.jp

IdP・SPの構築実験結果 (接続例2/5)

「DS」を選ぶ。

山口大学

サイトマップ アクセシビリティ 連絡フォーム

サイトを検索

現在のセクション内のみ

ホーム ユーザ ニュース イベント

ログイン

現在の場所: ホーム

Shibboleth log in

Log in with a [Yamaguchi University](#) user id.

Log in with a **DS** user id.

ログインしてください。

ユーザ名

パスワード

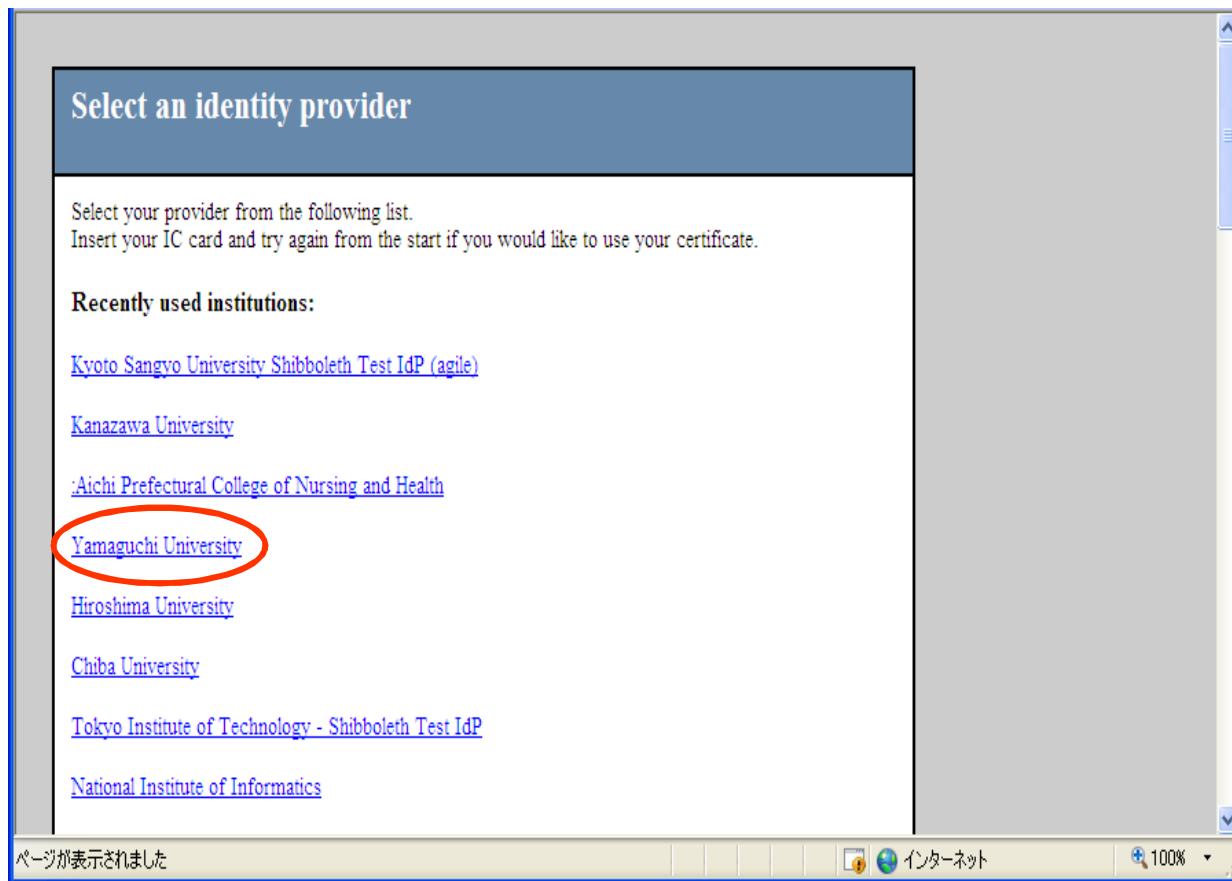
パスワードを忘れた?
パスワードがわからなくなった場合は、[調べるため](#)にクリック。

Copyright © Yamaguchi University

完了 sp.cc.yamaguchi-u.ac.jp

IdP・SPの構築実験結果 (接続例3/5)

「Yamaguchi University」を選ぶ。



IdP・SPの構築実験結果 (接続例4/5)

ユーザ名とパスワードを入力する。

山口大学  Shibboleth.

Yamaguchi University
Shibboleth Identity Provider Login
UPKI認証連携基盤実証実験

サイトを利用するには、ユーザ名とパスワードが必要です。

ユーザ名:

パスワード:

Copyright © [Yamaguchi University](http://yamaguchi-u.ac.jp)

完了 idp.cc.yamaguchi-u.ac.jp 

IdP・SPの構築実験結果 (接続例5/5)

ログインユーザの属性情報を確認する。

The screenshot shows the Yamaguchi University website interface. At the top, the university name '山口大学' is displayed in large green characters. To the right, there are links for 'サイトマップ', 'アクセシビリティ', and '連絡フォーム'. Below the name is a search bar with the text 'サイトを検索' and a '検索' button. A navigation menu includes 'ホーム', 'ユーザ', 'ニュース', and 'イベント'. A user profile bar shows the user 'test_eppn_1' with a 'ログアウト' link, which is circled in red. The main content area features a 'ナビゲーション' sidebar with links to 'ホーム', 'ユーザ', 'ニュース', and 'イベント'. Below this is a calendar for March 2009, with the date '10' highlighted. The main content area displays 'Yamaguchi University' and 'UPKI認証連携基盤実証実験'. At the bottom, there is a copyright notice 'Copyright © Yamaguchi University' and a status bar with '完了' and the URL 'sp.cc.yamaguchi-u.ac.jp'.

山口大学

サイトマップ アクセシビリティ 連絡フォーム

山口大学

サイトを検索 検索

現在のセクション内のみ

ホーム ユーザ ニュース イベント

test_eppn_1 ログアウト

現在の場所: ホーム

ナビゲーション

- ホーム
- ユーザ
- ニュース
- イベント

Yamaguchi University

作成者 admin — 最終変更日時 2008年10月13日 16時23分

UPKI認証連携基盤実証実験

このページを知らせる — このページを印刷する —

Copyright © Yamaguchi University

完了 sp.cc.yamaguchi-u.ac.jp

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)

 **UPKI認証連携基盤**

[SSO実証実験](#)

This is the Digital ID Card to be sent to 'https://upkishib1.nii.ac.jp':

Digital ID Card	
eduPersonAffiliation	faculty
principalName	test_eppn_115
organizationName	test_o
organizationalUnit	science

Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future.

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