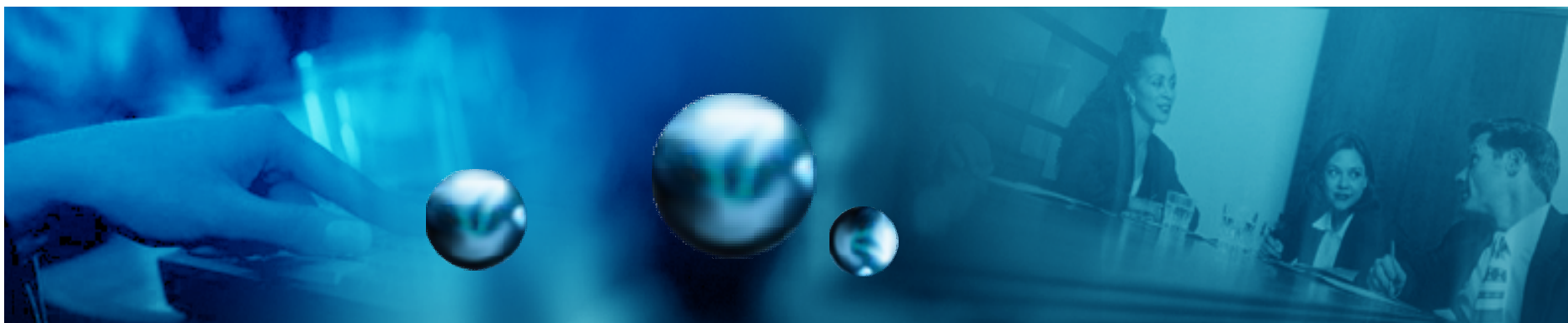


SSO実証実験の報告書

(東工大SSOとShibbolethの連携)



国立大学法人 東京工業大学



構築関連の報告

テスト用LDAPサーバの構築完了

数名のアカウントのみ登録

アカウント情報は『ID関連』以外は適当

テスト用IdPサーバの構築完了

CentOS 5.2 + Apache2.2 + Tomcat6 + shibboleth-idp-2.0.0

テスト用SPサーバの構築完了

CentOS 5.2 + Apache2.2 + shibboleth-sp-2.1(C++版でコンパイル)

Shibbolethの挙動確認

取得データの表示アプリ (PHP)

東工大ユーザ限定のShibboleth連携アプリの入り口 (リンク集等) を想定



東工大SSOとShibbolethの連携

連携の基本方針

東工大SSOにログインできれば簡単に東工大IdPへもログイン可能であること

東工大SSOからログアウトすれば東工大IdPからもログアウトされること

東工大SSOにログインすればShibbolethのDSによるIdP選択を省略できること

実装概要

東工大IdPのコンテンツを東工大SSOの保護下に設定

東工大SSOは認証済みユーザIDをHTTP Headerに埋め込むように設定

東工大IdPはHTTP Headerに埋め込まれたユーザIDで自動的にログインするように設定 (RemoteUserAuthServletを利用)

東工大SPにおいて東工大IdPを常に参照するように設定したリンク集を作成

連携イメージ (From 東工大SSO) (前)

PKI認証 (ICカードの機能)

[東工大ポータル \(TOP\)](#)



東工大ポータル (MENU)

[illegible]



TokyoTech Portal

http://portal.titech.ac.jp




ログアウト



一般システム

-  [Webメール \(Web Mail\)](#)
-  [学内ネットワークアクセス \(SSL-VPN\)](#)
-  [無線LANアクセス \(Wireless LAN\)](#)
-  [TOKYO TECH OCW講義資料入システム](#)
-  [パスワード変更 \(Password change\)](#)
-  [姓名読み登録 \(Name Registration\)](#)
-  [\(カードリーダー認証のみ\) 物品等請求システム](#)
-  [講義支援システム](#)
-  [リモートオフィスシステム](#)



東工大 外部提供

-  [図書館蔵書\(個人PC用\)ICカード認証のみ](#)
-  [図書館蔵書\(個人PC用\)ICカード認証のみ](#)
-  [図書館蔵書\(個人PC用\)ICカード認証のみ](#)
-  [図書館蔵書\(個人PC用\)ICカード認証のみ](#)

ICカードに印刷

	A	B	C	D	E	F	G	H	I	J
1	F	H	C	F	A	Q	R	Q	B	C
2	K	E	C	F	G	H	R	J	Y	X
3	I	E	Y	J	T	M	X	F	N	R
4	K	V	L	M	R	H	R	M	J	H
5	D	H	N	O	P	W	X	Q	X	V
6	A	B	C	D	E	F	G	X	D	I
7	E	Y	J	T	M	X	F	N	R	K

東京工業大学
The University of Technology

TokyoTech Portal

<http://portal.titech.ac.jp>

GSIC

Please input your account & password.

Account

Password

- ・ 上記の入力は『半角』で、かつ英字に関しては『大文字・小文字』の区別を必要とする。
- ・ 次ページのマトリクス入力では『半角』であれば『大文字・小文字』の区別は不要。

アカウント・パスワード認証 &マトリクス認証

Entrust IdentityGuard: [B1] [H7] [J3]

Shibboleth連携の入り口へのリンクをクリック

連携イメージ (From 東工大SSO) (後)

Shibboleth連携の入り口



Shibboleth.

東京工業大学

NII実証実験用 Shibboleth Test SP Top Page

Shibboleth連携済みアプリケーション一覧

アプリケーション	自動 ログイン	Top Page	概要	提供元
NII Plone1	自動 ログイン	Top Page	Test用ポータルサイト	NII
NII Plone2	自動 ログイン	Top Page	Test用ポータルサイト	NII
CiNii(ログイン実証実験用)	自動 ログイン	Top Page	論文情報ナビゲータ(本物) あくまでもログイン実証実験用として提供するものですので、 アクセス後の操作には十分注意願います。	NII
NII Moodle	自動 ログイン	Top Page	Test用E-Learningサイト	NII
MPS (Multiple Pointers System)	自動 ログイン	Top Page	複数ユーザが同時利用できるマルチマウスアプリケーション	産業技術大学院大学
File Transfer Service	自動 ログイン	Top Page	UPKIを用いたファイル送信サービス	金沢大学
環境変数一覧(テスト用)	自動 ログイン	Top Page	東工大専用の連携テストデバッグ用	東工大

連携されるデータ一覧

連携用ID (eppn)	GST00600@titech.ac.jp
連携用ID (REMOTE_USER)	GST00600@titech.ac.jp
連携用組織名 (o)	Tokyo Institute of Technology
連携用所属名 (ou)	Guest
連携用職名 (eduPerson_Affiliation)	faculty

意図している機能

各アプリの簡易紹介と注意事項

各アプリへの自動ログインリンク
(クリックするだけでログイン可能)

各アプリのTopPageへのリンク

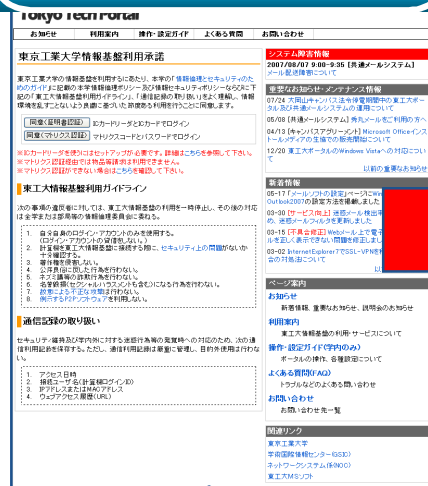
Shibbolethで連携されるデータの表示

連携イメージ (From 各Shibbolethアプリ)

各Shibbolethアプリ



東工大ポータル (TOP)



東工大ポータルにログイン後、
東工大IdPにリダイレクトされ、
該当Shibbolethアプリにログイン

東工大IdPに認証要求があると
東工大ポータルにリダイレクト

DS上で東工大IdPを選択

Shibbolethの通常の
認証スキームでも連携可能

2009/4/20



東工大SSOとShibbolethの連携に関する まとめと要望

東工大SSOとShibbolethの連携のまとめ

東工大SSOとShibbolethのクリックだけによるログイン連携を可能にした
(ユーザによるDS上でのIdP選択の必要性はない)

東工大SSOからログアウトすれば
その後の東工大IdPへの認証要求を全て遮断できるが、
各SPが持つ認証キャッシュの無効化に対する検討がまだ必要

NIIへの要望

今回構築した『Shibboleth連携の入り口』は一つのアプリケーションなので、
同様の機能を持つアプリケーションをNII側で管理運用することを検討してほしい
(ユーザにDS上でIdPを選択させることは避けた方が望ましい)
(各組織はまずこのアプリにログインさせる方式が管理・運用しやすい)



NIIからの連携確認依頼事項の進捗報告

Metadataの自動ダウンロード (IdP & SP)	設定済み
Metadataの署名検証 (IdP & SP)	設定済み
Elsevierとの接続テスト	未検証
各属性の学内LDAPとの接続性の検証	検証中
各属性のSPに対応したリリース制御	検証中
日本語属性の連携検証	未検証
個人情報提供に関する学内ポリシーの検証	協議中



学内LDAPサーバとの連携に関する 検討事項のまとめ

所属の英語名称を登録していない

所属コードからの変換を検討中

個人情報を含めない
eduPersonPrincipalNameの検討

一意であることを保障するために
LDAPの属性を追加して、
乱数を格納することを検討中

職種区分の厳密な定義が難しい

各大学で共通認識を持つ
必要がある上に、
振り分けルールが
複雑化する懸念もある

個人情報等の学内ポリシーのため、
下記の情報等が必ず提供できるかは
保障できない (現在協議中)
・氏名 / メールアドレス

提供できない情報を必須とする
SPの存在次第で、
なんらかの対応方針は検討する



Shibboleth連携に関する ポリシー的な検討事項&要望のまとめ

IdP内の利用ユーザとSPの間に
明確な契約が無いように見えるので、
IdP側の個人情報提供が
かなり難しく思える



SP側で利用する個人情報については、
ユーザへの利用用途の通知や
ユーザの同意を取ってから利用することを
SP側に義務付けてほしい

簡易なSPを運用するとしても、
ユーザ識別ID自体に
個人情報が含まれていたのでは、
SPの管理責任が
割に合わないほど負担に思える



個人情報を全く含まないで、
かつ、
ある期間(1年以上?)は
IdP内で必ず一意であると保障できる
ユーザ識別IDの提供を
IdP側に義務付けてほしい
(eduPersonPrincipalName?)

上記の要望を踏まえて、
利用属性のどれを個人情報として取り扱わなければならないかの統一的な区別を
フェデレーション内で作ることが可能かどうかもNII側で検討して欲しい