SSO連携実験の中間報告
（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

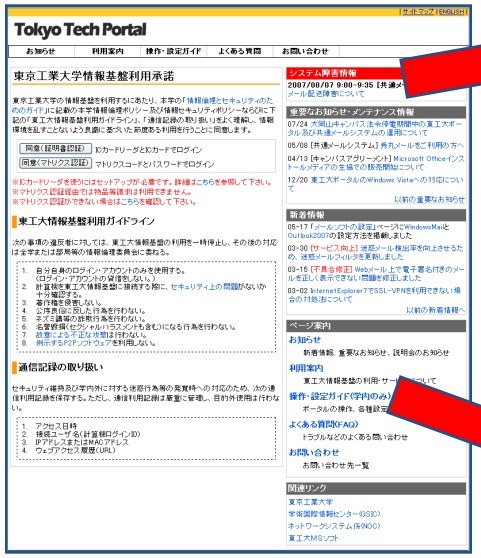
実装概要

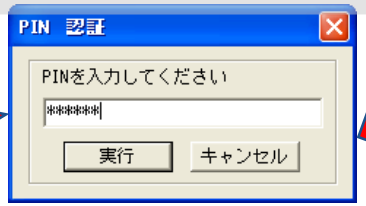
- 東工大IdPのコンテンツを東工大SSOの保護下に設定
- 東工大SSOは認証済みユーザIDをHTTP Headerに埋め込むように設定
- 東工大IdPはHTTP Headerに埋め込まれたユーザIDで
  自動的にログインするように設定（RemoteUserAuthServletを利用）
- 東工大SPにおいて東工大IdPを常に参照するように設定したリンク集を作成

連携イメージ（From 東工大SSO）（前）

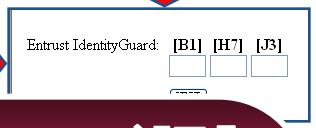
PKI認証（ICカードの機能）

東工大ポータル（TOP）

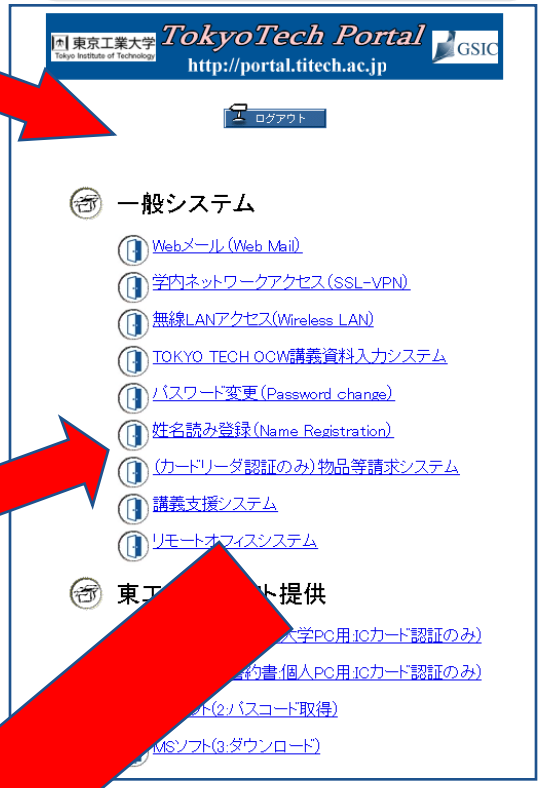




ICカードに印刷



東工大ポータル（MENU）



アカウント・パスワード認証 ＆マトリクス認証

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

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

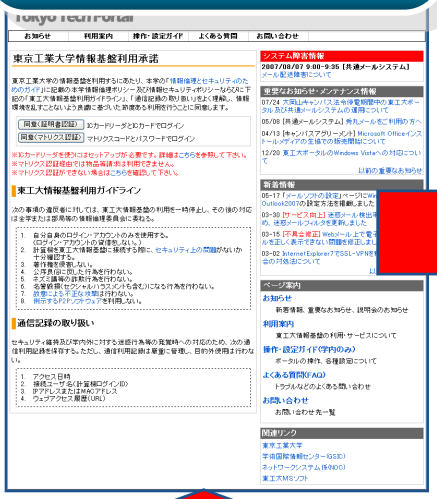
意図している機能

- 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

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

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）