認証連携導入の諸問題(1) Shibboleth

- 米国教育機関を中心とした利用実績
- 属性によるリソース制限
- (UPKI参加大学への)サーバ証明書の無料配布
- uPortal、Moodle等の大型アプリケーションが対応

↑このような優れた特徴を持つシステムであるが…
最大の問題は「**初期設定の煩雑さ**」にある

- 複数のシステムの集合体である(tomcat,ant,openldap,Shibboleth)
  - 設定ファイルやログが分散する
  - 各デーモン間の依存関係を把握しにくい
- 大学毎に導入レベルが異なり、足並みが揃わない
- NII説明会資料に従えば導入は決して難しくないが、それは「VMwareイメージの配布」という親切なサービスがあったからこそ
  - 「そこまでしないと実証実験を完遂してもらえないのでは」という意識が窺える
  - Windows xpがゲストOSの場合、配布されたVMイメージはそのままでは動作しない
- 各大学の実情に合わせた運用を行う場合、VMイメージの利用だけでは「絶対に」終わらない
- 学内既存認証システムとの仲介を行うミドルウェアを開発する必要があり、Shibbolethのアーキテクチャに対する深い理解が求められる

認証連携導入の諸問題(2) SAML

- .NET Passportのような集中モデルと違い、プライバシや可用性への懸念が少ない
- OpenIDのような「緩すぎる連携」でない
- 仕様が変わりにくく、安定している(SAML 2.0は2005年に標準化)
- クロスドメインの制約を越えられる
- シングルログアウトが可能
- 名寄せ回避のための匿名識別子あり
- 携帯電話から使える識別子(Artifact Binding)あり
- 日本大学によるGoogle Appsのような大規模事例あり

↑このような魅力を持つ技術仕様であるが…
最大の問題は「**入手可能な情報の少なさ**」にある

- 公式ドキュメント以外では、読むものがひじょうに少ない
- XMLによるメッセージ交換を行っていることもあり、仕様書は大部にわたる
- 「仕様書はProfiles→Bindings→Assertions and Protocolsの順で読め」のようなノウハウはあるが、それらは一部の人達の間に閉じられている
- 解決策は
  - Liberty Alliance技術セミナやIdentity Conferenceへの積極参加
    - 年に1～2回のシンポジウムでは足りない
    - UPKI参加大学の中だけではあまり情報共有が行われていない
  - 手軽に試せる実装、ライブラリの提案

認証連携導入の諸問題(3)
キラー・アプリケーションへの渇望

- 「UPKI認証連携でないとできない」アプリケーションは何か?
- 「属性に基づく許可」が生きる場面は?
- 「単位互換」の話題はしばしば出るが、これは技術よりも政治の問題
- ScienceDirectやRefWorksの学外利用は既存技術で可能
- 無線LANのイベント利用も一時アカウントの発行で可能
- 「○○のためなら、多少の手間を乗り越えてでも認証連携したい」という目標が必要

Shibboleth実現へのインセンティブ

●文科省などの補助金が獲得しやすくなること
– シボレスを前提としたサービスを考えてみる

●大学間の競争力が増すこと
– 私立大学では「横並び」は許されない
– ICT：特色ある学習支援環境の整備が急務

●国家的な学術情報インフラとして位置づけること
– 国策として、国力アップのための研究・教育戦略を考えるべき

●コアコンピタンス（強み）とドメイン（立ち位置）を決めること
– 何で戦うか？どこで戦うか？
– インフラは共有化、サービスは差別化

●セッション内の行動記録が一元的に取得できること
– 知的利用行動がライフログのように丸ごと記録可

●Open IDが使える、ケータイやiPhone3Gでも使えること
– Google世代、ケータイ世代の学生にフォーカスする