徳島大学における Shibboleth実装とその運用

2011年11月15日

徳島大学　上田哲史

徳島大学からの報告

- 本学の「学認」参加自体は，学認の名称決定以前から…

- ただし，
- 本日時点で運用フェデレーションには至っていない
- ➔技術的な問題によるものではない
- ➔技術的には，学認採用のShibbolethを運用中

- そこで，
- 徳島大学でのShibboleth運用に関する工夫等を報告
- ➔「学認」等の枠組み展開への寄与

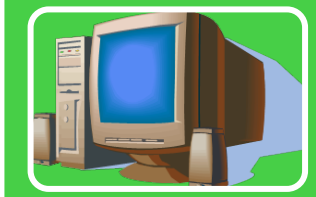
アウトライン

1. 要認証システム
2. 要認可システム
3. Shibboleth化
4. 属性処理上の工夫
5. 運用および今後の展開

要認証システム

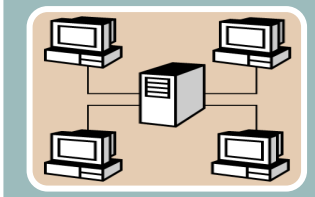
アプリケーション

- 要認証WEBシステムでのログイン
- メールシステムでの認証
- その他クラ／サバ系アプリケーションの認証



オペレーティングシステム

- Windows系OSへのログイン
- MacOSへのログイン
- NWドメインへのログイン



ネットワーク

- 無線LANでの認証
- VPNの認証
- 有線NW上の認証

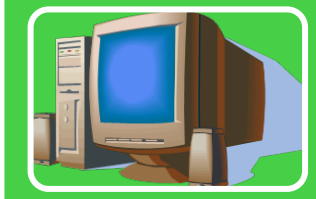
佐賀大，
広島大
など

※従来異なる認証を要していた要認証システムの連携が始まる

要認証システム

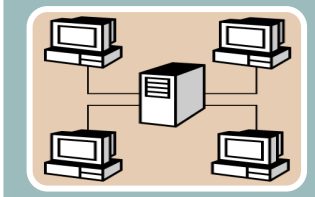
アプリケーション

- 要認証WEBシステムでのログイン
- メールシステムでの認証
- その他クラ／サバ系アプリケーションの認証



オペレーティングシステム

- Windows系OSへのログイン
- MacOSへのログイン
- NWドメインへのログイン



ネットワーク

- 無線LANでの認証
- VPNの認証
- 有線NW上の認証

※検討中：認証統合の範囲，認証順序，認可方法

例）ネットワーク

【徳島大学における2011年秋時点のネットワーク認証】

- 対象NW：**無線**LAN, VPN
  （802.1x機器があれば有線も同一制御可能）

- 利用者からの**申請方式**を採用
  （セキュリティポリシー，内規に従う）

- パスワードは一定期間有効で，再申請制
- アカウントは**WEB申請**
  （OSのID・PWDとは異なるものを発行）

Shibboleth化

システム固有の前提条件

- 例）人事給与システム
  - 基本的に人事課職員のみがアクセスするシステム
  - 特に堅牢なセキュリティ条件下での運用が求められる
- 例）履修登録システム
  - 基本的には学生が利用するシステム
  - 履修選択範囲は，それぞれの学生によって異なる
  - 学務部の事務職員は学生よりも強い権限でのアクセスが必要

- 何でもかんでも統合認証でSSO！？
- 実現可能性を十分検討した上で設計と実装を行う
- 少なくとも認可の仕組みが整理されていない状況での統合認証利用化は時期尚早

要認可システム

（１）システムアクセスを認めるユーザが統合認証に乗っている全員ではないケース

➔システムへの人単位の認可制御

　例）先の例の人事給与システム

（２）アクセスを認められたユーザがアクセスできるコンテンツが，そのシステムの全部ではなくて一部制限があるケース

➔コンテンツへの人単位の認可制御

　例）先の例の履修登録システム

発想の転換

ログイン➔認証＝認可の時代は終焉

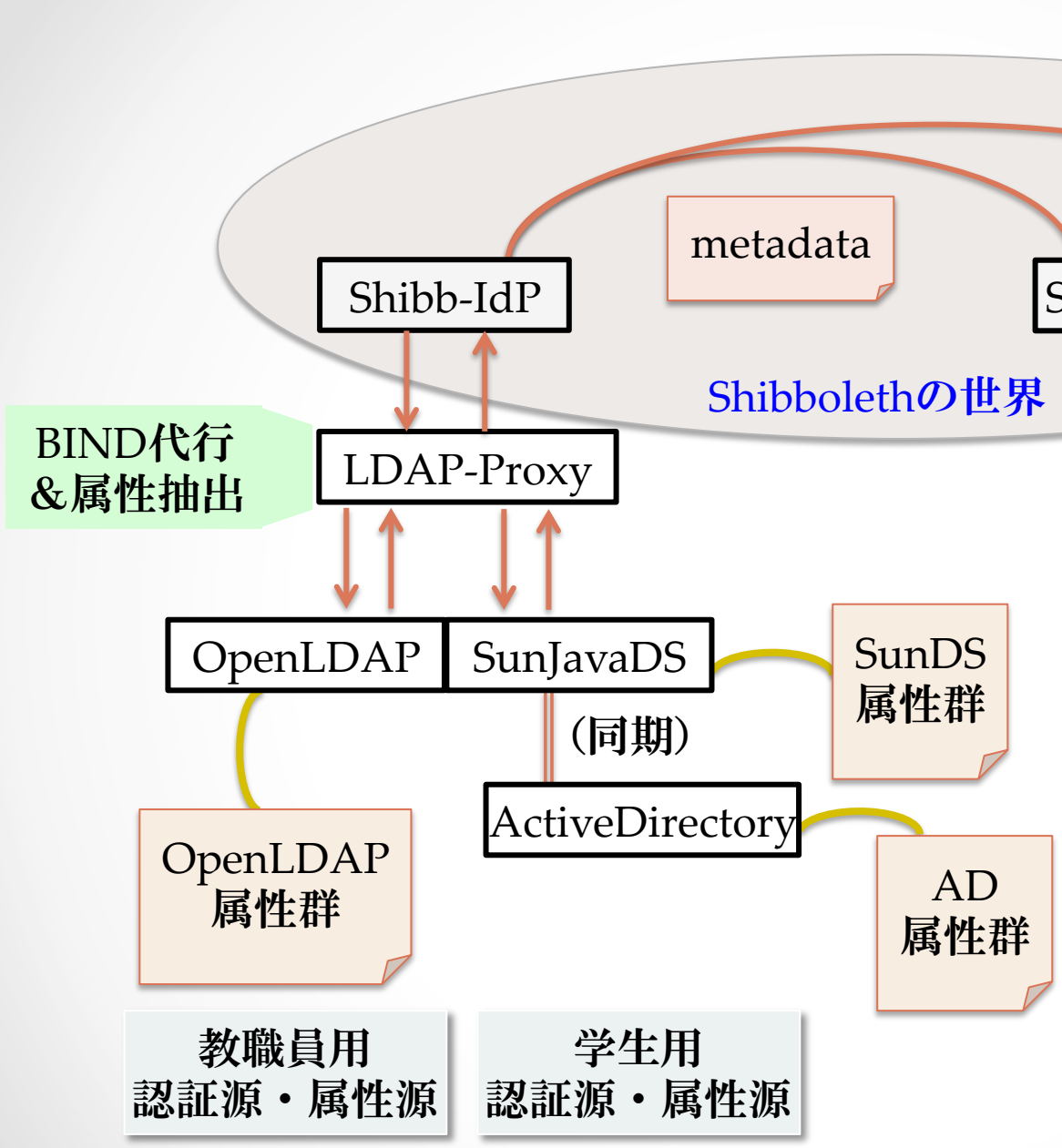
■スタンドアロンシステムの場合
- ログイン時の認証と認可は同義とした設計思想のものも多い
- システム内部で認可を実現しているものも多い

■統合された外部認証で認証源を実現する場合
- ログイン時の認証によるシステムアクセスは同義では扱えない
- システム内部の認可も今後は共通的に扱えるようにすべき

スタンドアロンのシステムを集めてSSO・認証連携だけ考えてShibbolizeせず，よく考えた実現・対応が大切

Shibboleth化

SSO実現＋認可制御



【2011年秋時点でのSPの例】
- Moodle（OSS-LMS）
- Joruri（OSS-CMS）
- 商用リバプロ
- ソフトダウンロード（独自開発）
- OpenPNE（OSS-SNS）
- WebDAV

など

（2011年秋時点）
徳島大学Shibboleth環境

属性管理に関する現況調査

（A）教職員の属性

- OpenLDAPにて実装
- 25属性

（B）学生の属性

- 実装：ActiveDirectory＋SunJavaDirectoryServer
- ADからDirectoryServerに同期する時点でフィルタリング
- 10属性

課題

1）バックエンドがADとLDAPで異なる

2）（A）と（B）で構築経緯も異なるため格納方針・内容が異なる

3）存在しない属性もある

運用状況

- SPの範囲
  - 学内学習管理システム（Moodle：OSS-LMS）
  - 連携大学間用学習管理システム（Moodle：OSS-LMS）
  - ポータルシステム（Joruri：OSS-CMS）
  - 商用リバプロシステム（IceWall）
  - ソフトウェア配信システム（独自開発）
  - 健康診断システム（独自開発）　など
- 試作したもの，予定等
  - ネットワーク利用申請システム（構築中）
  - SNS（OpenPNE：OSS-SNS，試作済み）
  - ネットワークリソース監視システム（試作済み）

今後の展開

- 学認の試行フェドから運用フェドへの展開検討

- クラウドに対応したSAML連携の展開
- 統合認証・SS〇の範囲の検討
- 認可制御の方針決め