2008年度実証実験成果報告 大阪大学サイバーメディアセンター

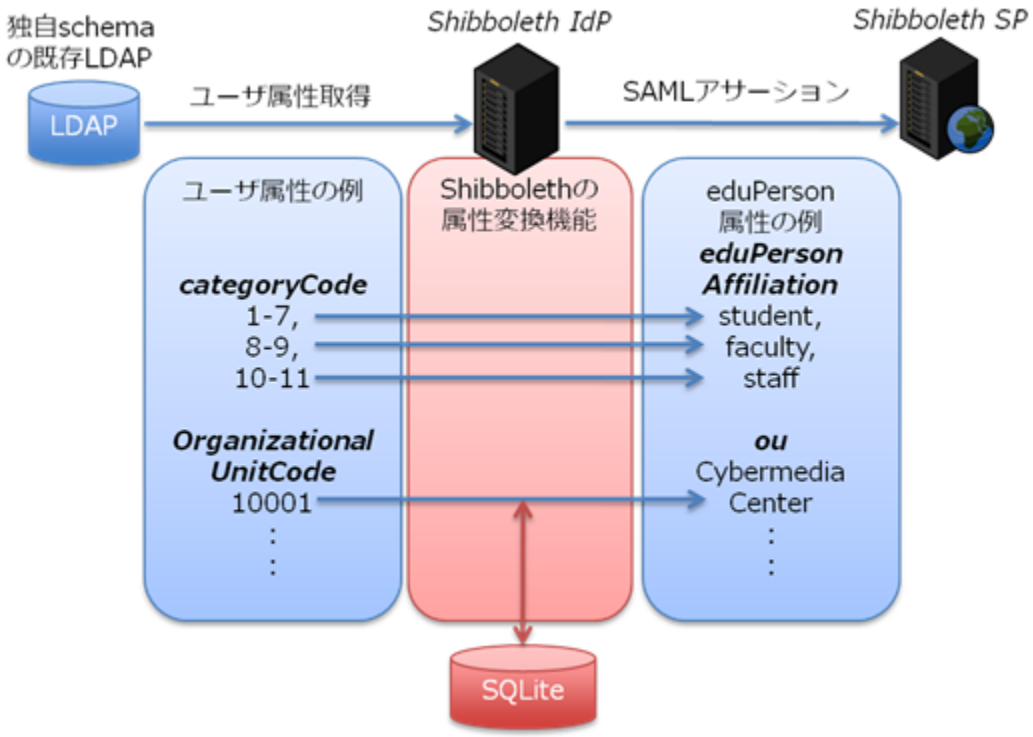
実証実験は平成20年度で終了しました。最新の情報は トップページ（技術ガイド） から参照ください。

認証連携用 IdP

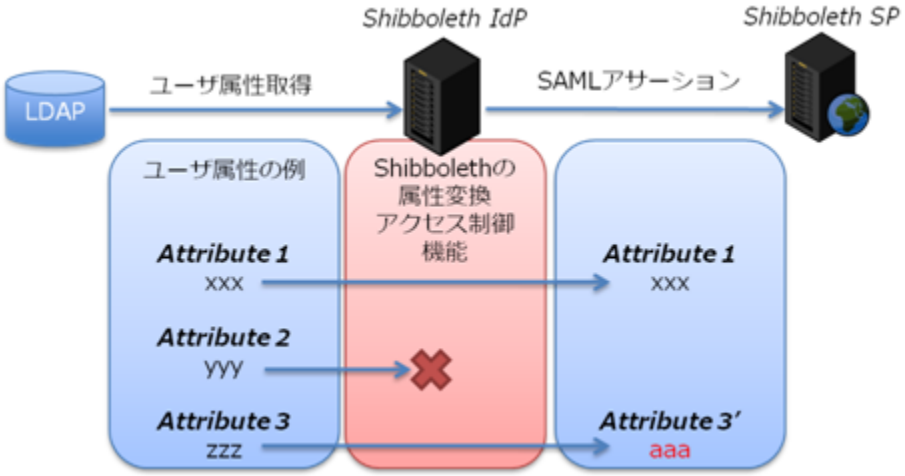
大阪大学サイバーメディアセンターでは、学内サービスの認証基盤として構築した全学IT認証基盤を大学間認証連携およびサービス連携の基礎として発展させるため、UPKI認証連携基盤の実証実験に参加し、既存の認証基盤の拡張方針について検討を進めています。

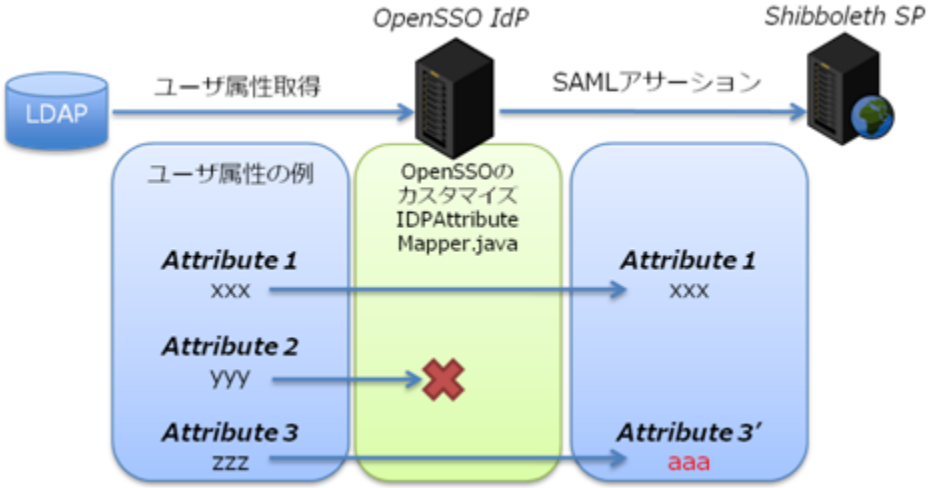
本センターでは特に既に認証基盤を構築した大学をターゲットとして、既存の認証基盤に対する変更を最小限に抑えた上で、UPKI認証連携基盤に参加 する方法について検討していきたいと考えています。ここでは本学の認証基盤を例に、UPKI認証連携基盤にシームレスに統合するためのアプローチについて 紹介していきます。

Shibboleth 2.0 の属性マッピング機能の検証



OpenSSO と Shibboleth 2.0 の SAML 2.0 連携

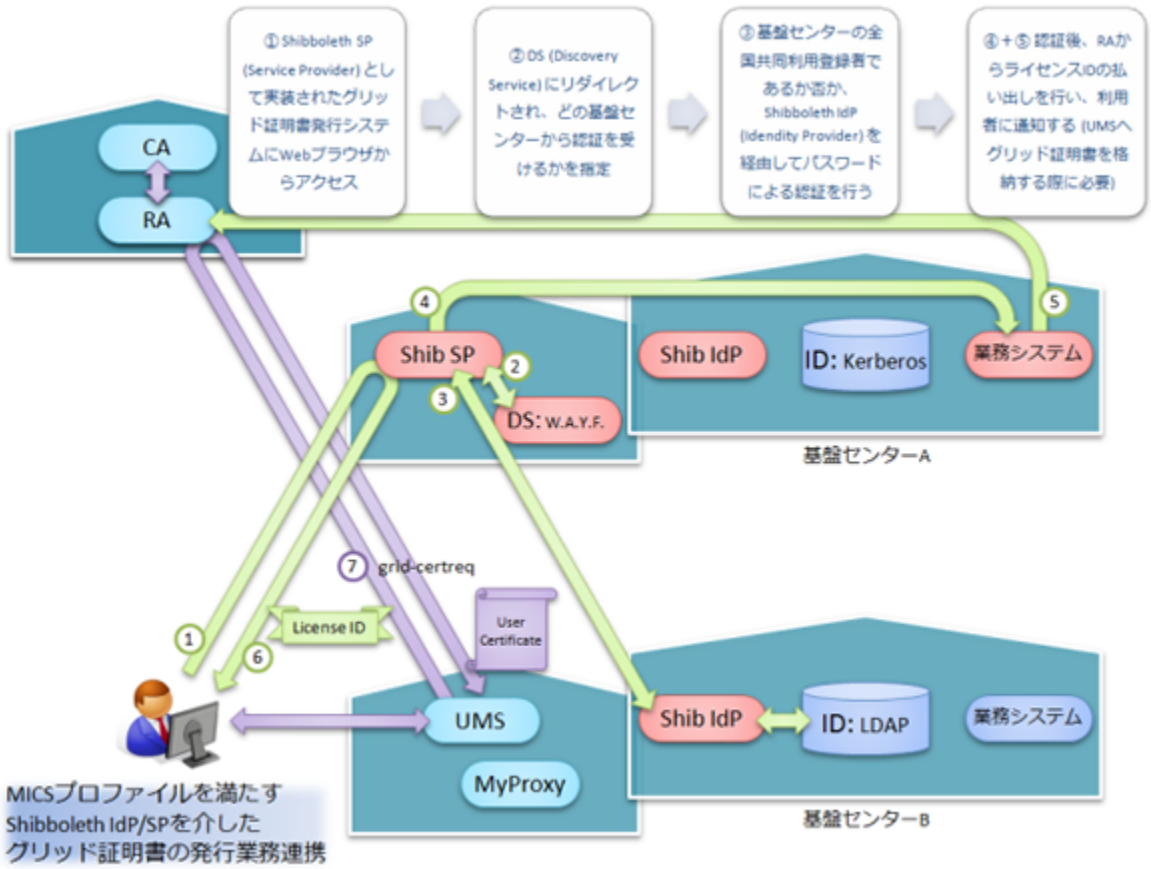




グリッド証明書発行SP

大阪大学サイバーメディアセンターでは、本センターの大規模計算機システムを利用するための既存の全国共同利用業務のIDデータベース (Microsoft ActiveDirectory≒Kerberos) に付随するShibboleth IdPを設置しました。さらに、当該IdPによる認可を受けた利用者に対して本センターのグリッド認証局からグリッド証明書を発行するために必要となるラ イセンスIDを自動的に払い出すSPを構築中です。

システムの構成イメージは次の図の通り:



1. Shibboleth SPとして実装されたグリッド証明書発行システムにWebブラウザからアクセス
2. DSにリダイレクトされ、どの基板センターから認証を受けるか指定
3. 基板センターの全国共同利用登録者であるか否か、Shibboleth IdPを経由してパスワードによる認証を行う
4. 認証後、RAからライセンスIDの払い出しを行い、利用者に通知する (UMSへグリッド証明書を格納する際に必要)

このように、NISやLDAP、ADSなどによる既存のIDレポジトリにShibboleth IdPを付随して設置し、本センターと業務協力関係を結ぶことで、これまでのような人手による事務作業を省略して、本センターが発行するグリッド証明書を 取得可能になります。また、このような業務フローはMICSプロファイルによる業務規定に合致するものと考えており、将来的にIGTF/APGrid PMAによってプロダクションレベルのグリッド証明書発行業務として認可され得るものです。

今回の実証実験の一環として、本システムの実験運用への参加にご興味のある方は、manabu （アットマーク） cmc.osaka-u.ac.jpまでご一報ください。