大阪大学

シングルサインオン実証実験
中間報告会　発表資料

大阪大学における認証連携用IdPの構築

- 既存の認証基盤をどのように連携させるか
  - ディレクトリサーバをShibboleth IdPのレポジトリとして転用する
  - Access ManagerをShibboleth SPとSAML2.0で連携させる

- 実証実験参加の目的
  - 既存の認証基盤への変更点を最小限に抑えつつ認証連携を実現する方法の調査
    - Shibboleth2.0 IdPにおける既存レポジトリ利用
    - OpenSSOとShibboleth2.0 SP の連携
    - Access ManagerとShibboleth2.0 SPの連携

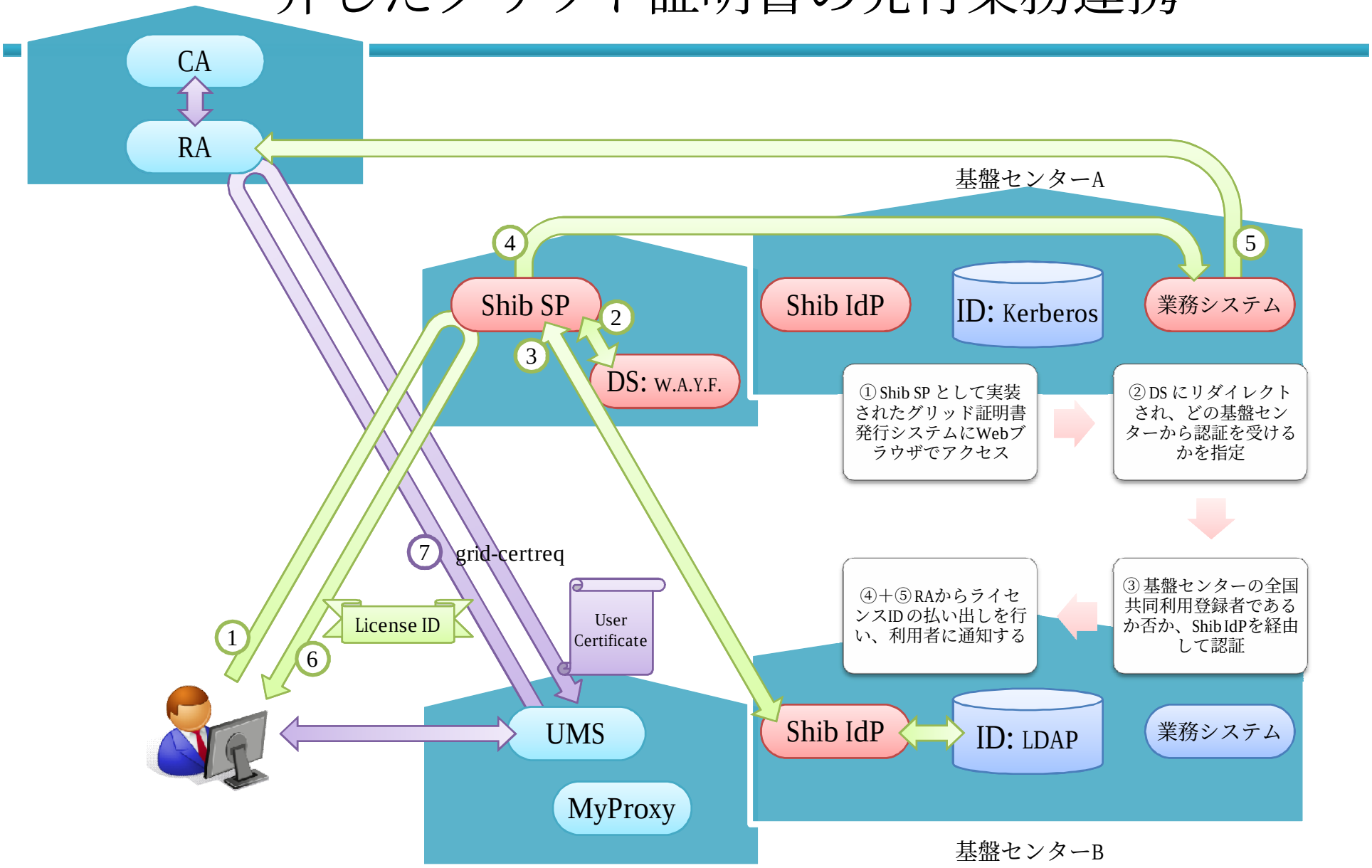
Shibboleth IdPにおける既存レポジトリの利用

- Shibboleth IdP導入時に必要な作業
  - 既存ディレクトリサーバにeduPersonスキーマ導入
  - eduPersonAffiliation等の値を設定
- Shibboleth IdPの属性マッピング機能で省略
  - 例）categoryCode = 8 or 9 の場合 eduPersonAffiliation = faculty に設定
    - Mapped AttributeDefinition
      - XMLファイルにマッピングを記述
      - 変更には再起動が必要
    - RelationalDatabase DataConnector
      - RDBにマッピングを記述
      - RDBの管理コストが増える
        - » SQLiteを用いることで管理コストを抑える

OpenSSOとShibboleth2.0 SPの連携

- OpenSSO
  - SunのIdP製品「Access Manager」のオープンソース版
  - SAML2.0，OpenIDのサポート
  - JMSを用いた冗長化機能
- SAML2.0での連携
  - GUIで設定可能
    - SPの追加
    - ディレクトリサーバの属性のアサーションへの追加
- 注意点
  - NameIDFormat問題
    - Shibboleth SPは現状“urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified”を扱えず“urn:oasis:names:tc:SAML:2.0:attrname-format:uri”を指定する必要がある
    - OpenSSOのデフォルトはunspecified
      - DefaultIDPAttributeMapper.java　を修正する必要がある
  - 属性マッピング機能
    - オープンソース版は機能不足（自前実装が必要）なので製品版で調査中

MICSプロファイルを満たすShibboleth IdP/SPを介したグリッド証明書の発行業務連携



基盤センターをまたがるVO形成の支援