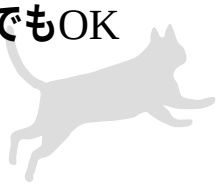
名古屋大学におけるIdPの構築

名古屋大学情報連携基盤センター
平野　靖

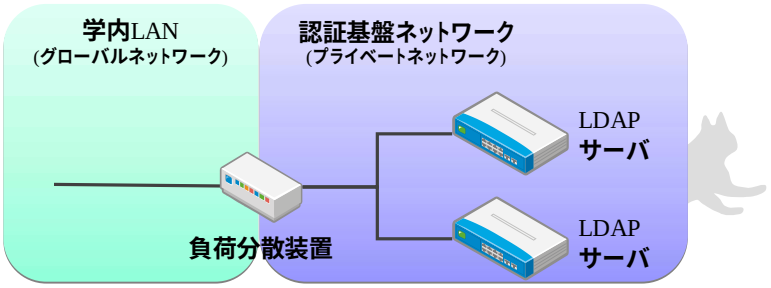
ＵＰＫＩシングルサインオン実証実験への参加状況

- IdP：構築済み
  - 全学のユーザ認証基盤を参照
- SP：未構築
  - 現在のところ，UPKI-Fed参加機関にのみアクセスOKなコンテンツが見つからない
    - 学内のみOK or 世界中の誰でもOK
  - e-learningやVOなど



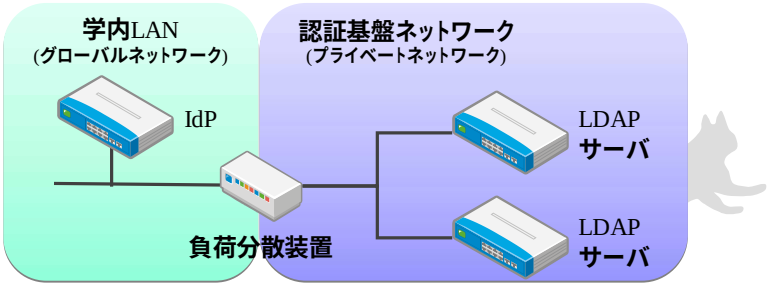
名大のユーザ認証基盤の構成

- 複数台のLDAPサーバ＋負荷分散装置
  - LDAPサーバ：ユーザの認証情報を格納
    - Solaris 9 (UltraSPARC IIIi)
    - Sun Java System Directory Server Enterprise Edition



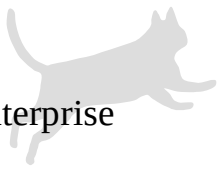
構築したIdPの構成

- Solaris 9 (UltraSPARC IIIi) + Shibboleth
  - 既存の認証基盤がSolarisで運用されており，技術職員がSolarisに慣れている
- IdP外部のLDAPサーバを参照



構築したIdP

- IdP
  - Solaris 9
  - Tomcat 6.0.18
  - Apache 2.2.6
  - shibboleth-idp-2.0.0
- LDAPサーバ
  - Solaris 9
  - Sun Java System Directory Server Enterprise Edition



名大のユーザ認証基盤

- LDAPサーバ
  - CASサーバの認証DB
  - 非Webアプリのためのユーザ認証
- 負荷分散装置
- CAS(Central Authentication Service)サーバ
  - Webアプリに対するSSO
  - 学内(情報連携統括本部外も含む)で運用される情報サービスのユーザ認証

SWITCH

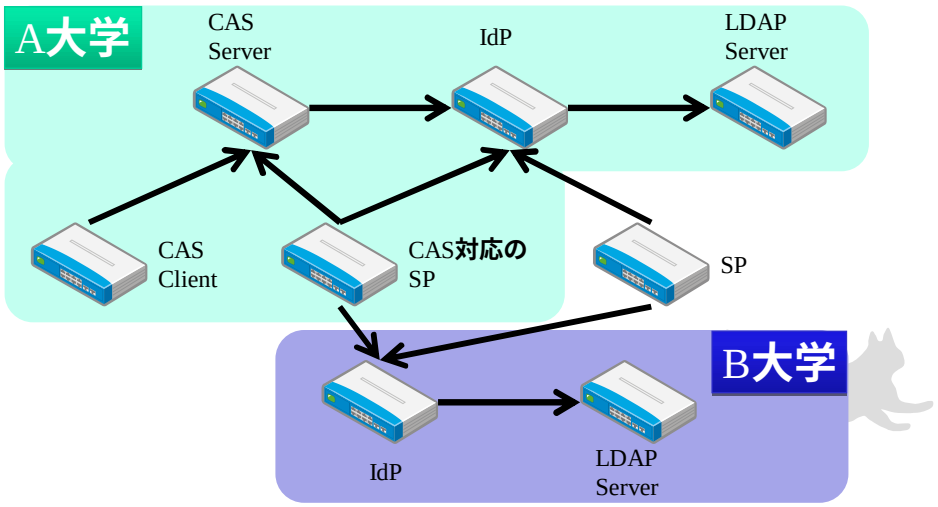
- スイスの大学が共同で設立した団体
- スイスの大学に対するネットワークサービスを提供
  - インフラ，e-Learning，Grid，認証・認可基盤 (Authentication and Authorization Infrastructure (AAI))，・・・
- Shibbolethベースの認証・認可フェデレーションを構築
  - スイス国内75%の大学が利用

CASのShibboleth対応：SWICHによる実装

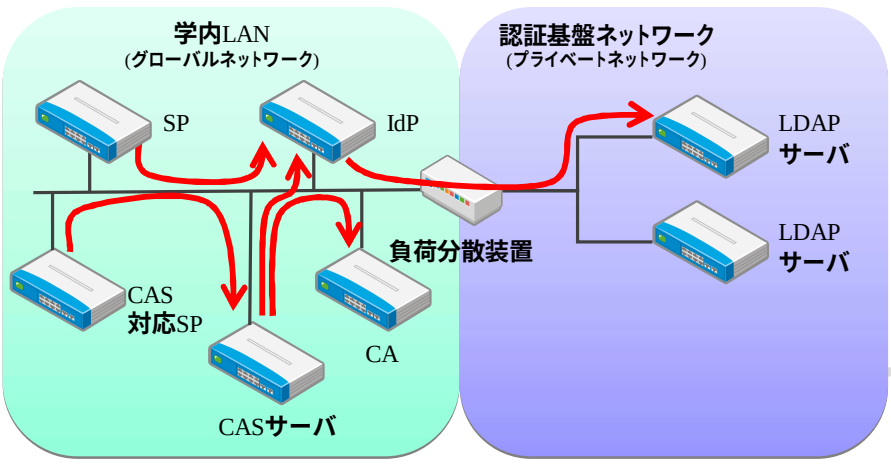
- CASの認証DBとしてIdPを参照
- ShibbolethのWebアプリをCAS対応に
- https://www.switch.ch/aai/docs/shibboleth/SWITCH/1.3/idp/install-cas.html
  - CAS Server 2.0.12
  - Shibboleth 1.3

} 少し古い

CASのShibboleth対応：SWICHによる実装



検証実験環境



今後の計画

- CAS Ver.3とShibboleth Ver.2.1での検証
- CASの認証DBとしてLDAPサーバとIdPの両方を使えるかの検証
- 名大版CASとの連携