Kyushu University 100th 2011
知の新世紀を拓く

UPKIシングルサインオン実証実験
～Shibbolethを利用した大学間認証連携の実現～

九州大学･報告書
開かれた研究教育活動のための情報基盤
－オープン･安全･信用の実現に向けて－

中國真教, 笠原義晃, 伊東栄典, 岡村耕二, 井上仁, 鈴木孝彦 *
片岡真, 牧瀬ゆかり, 香川朋子, 井上創造 **
* 九州大学情報統括本部, ** 九州大学附属図書館

九州大学

1. はじめに

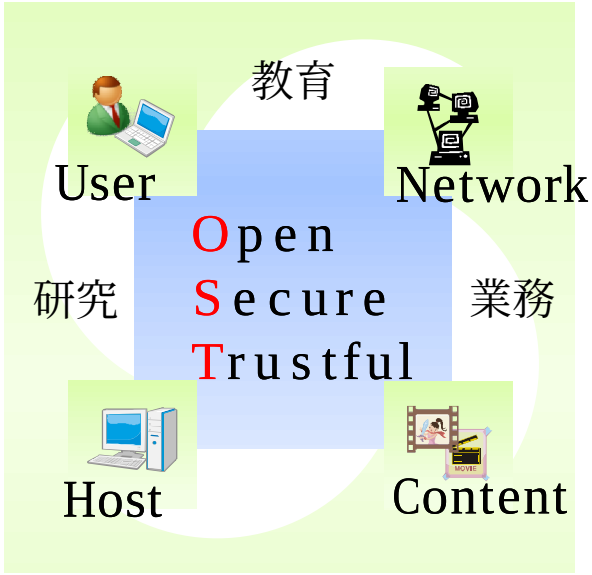
九州大学は2006年からUPKIプロジェクトに参画しています。国立情報学研究所や全国の参加大学と連携しつつ，全学共通認証基盤の構築，eduroamへの参加，NIIサーバ証明書配布プロジェクトの積極的な利用等を進めてきました。今年度にはSSO実証実験に参加し，大学間におけるサービス連携のための研究開発を進めています。

開かれた研究教育活動のための情報基盤の整備

～情報通信におけるオープン，安全・安心，信用の向上～

ユーザ
- 利用者のアカウント管理
- 利用者認証機構の整備
- 認証機構の高度化
- *Shibboleth SSO*

ホスト
- 計算機の信用性向上
- 通信の安全性向上
- *Shibboleth SSO*



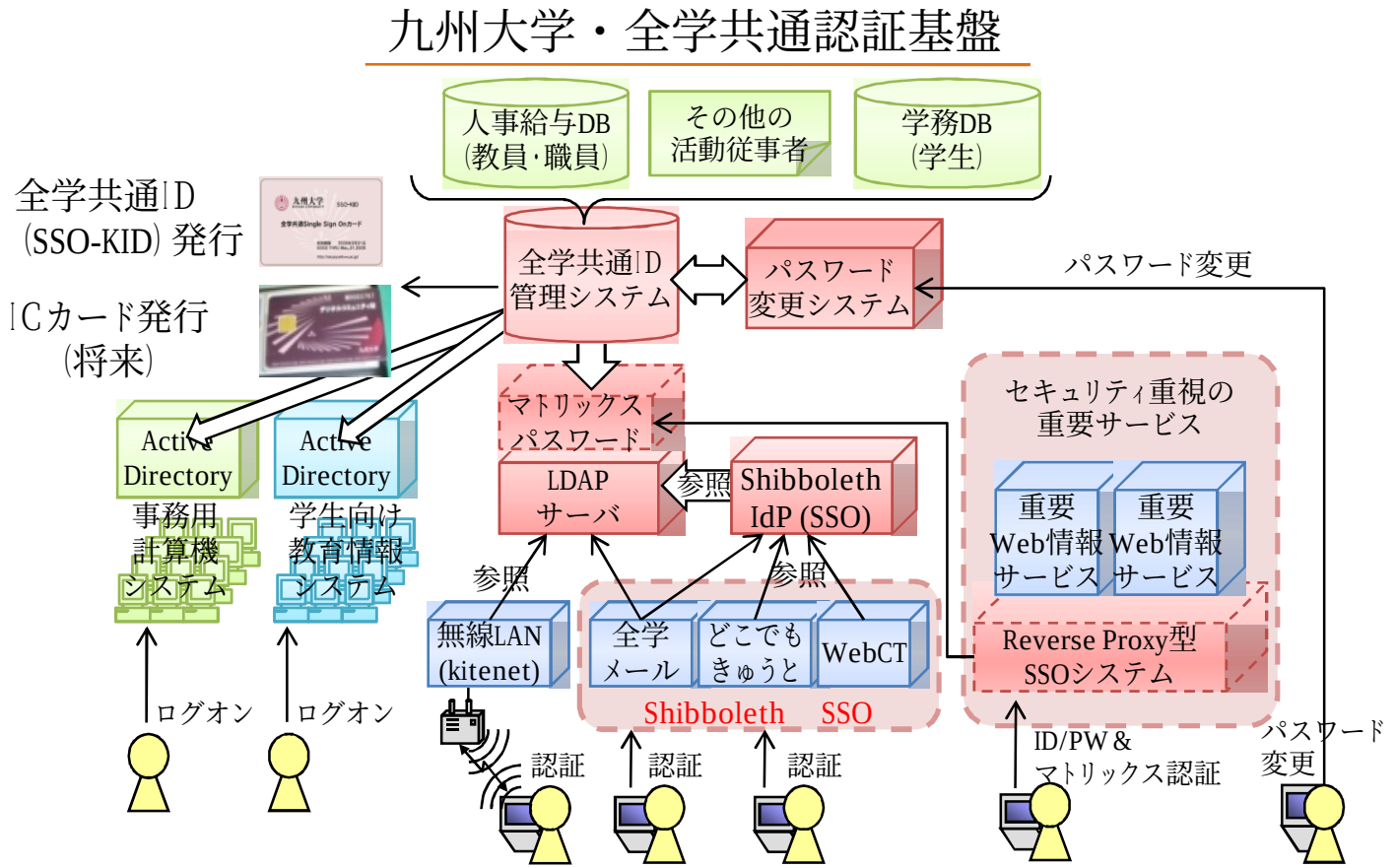
ネットワーク
- 安全･安心なネットワーク
- ネットワーク接続時の機器認証，利用者認証
- 来訪者にも便利

コンテンツ
- 学内から発信するコンテンツの信用性保証
- 学外コンテンツの利用
- *Shibboleth SSO*

4つの分野で活動

1.1 ユーザ：全学共通認証基盤の構築

情報サービスにおける利便性・安全性・信用性を向上するために，全構成員を対象とする利用者認証基盤を整備しました。学生には以前からID発行および認証機構が存在していましたが，H17年から教職員へのID発行を実現しました。また，学内に散在していた各種情報サービスと，構築した全学共通認証基盤を連携させ，安全かつ便利な利用者認証環境を実現しました。

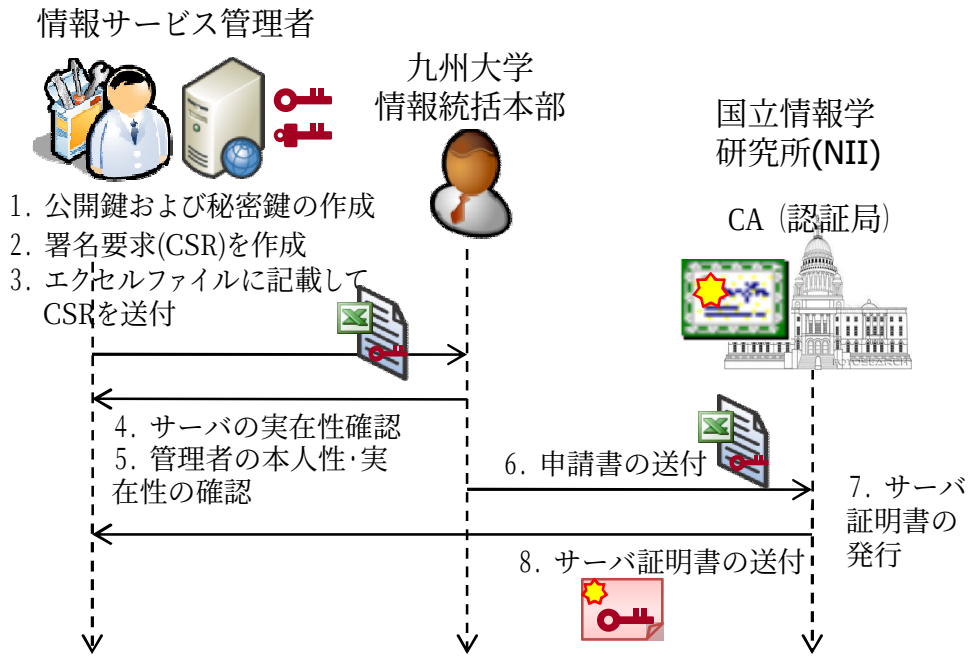


1.2 ホスト:サーバ証明書発行支援, 認証機能提供

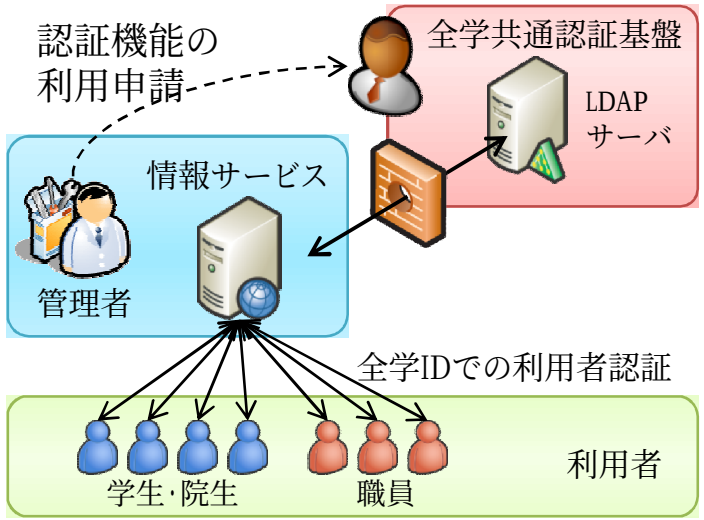
ホストの信用性と通信の安全性向上のために, サーバ証明書の発行を支援しています。国立情報学研究所のサーバ証明書発行プロジェクトに参加し, 学内の情報サービスに対しサーバ証明書を発行しました (2008年11月現在で, 45個を受付け)。

また, 学内の全学的な情報サービスを対象に, 全学共通IDによる利用者認証機能を提供しています (2008年11月現在で5個のサービスが利用)。

サーバ証明書の発行受付



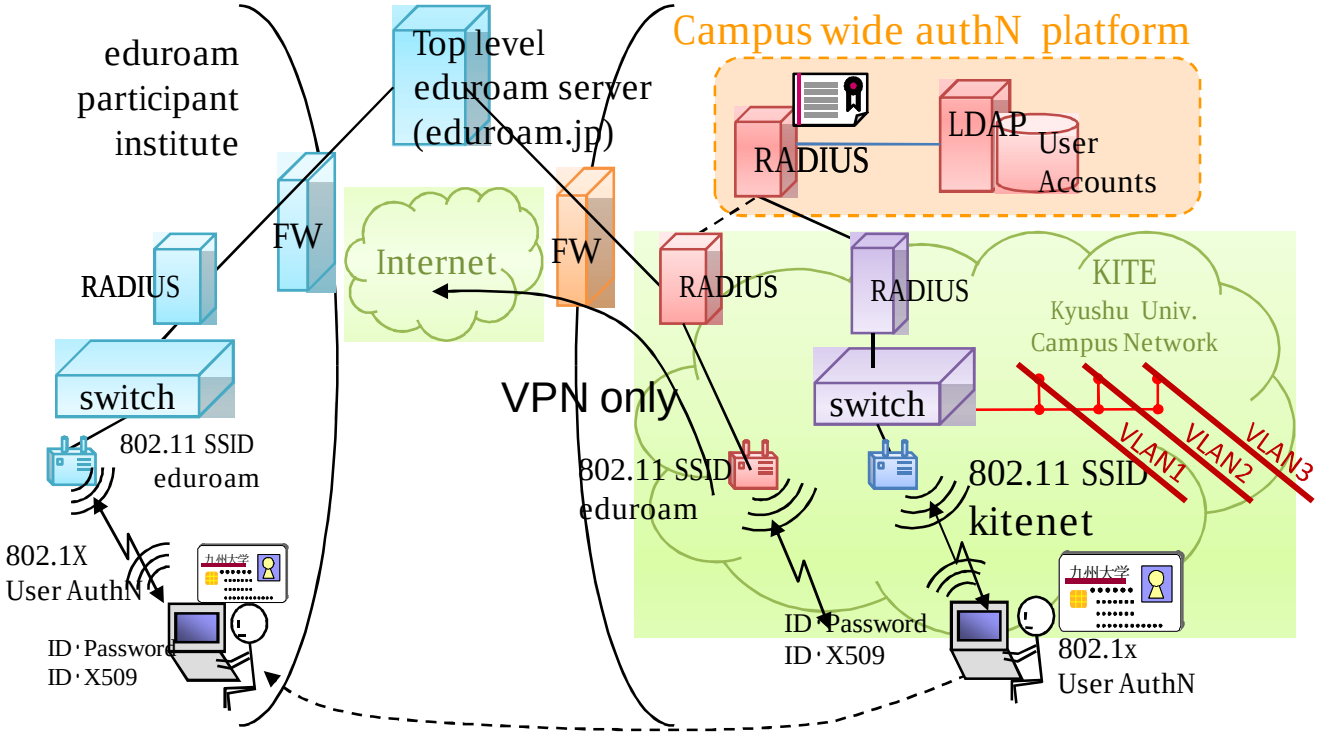
学内サービスへ利用者認証機能提供



1.3 ネットワーク：802.1Xネットワーク環境

大学内無線LANアクセスサービス（通称kitenet）では，802.1X認証に本認証基盤を利用しています。認証基盤用LDAPとRADIUSの連携システムは，eduroamなどその他のRADIUS認証サービスとの連携を考慮して構築しています。kitenetやeduroamは，学内者および来訪者も想定した構成になっており，オープンなネットワーク環境が実現できています。

kitenetおよびeduroamの構成図



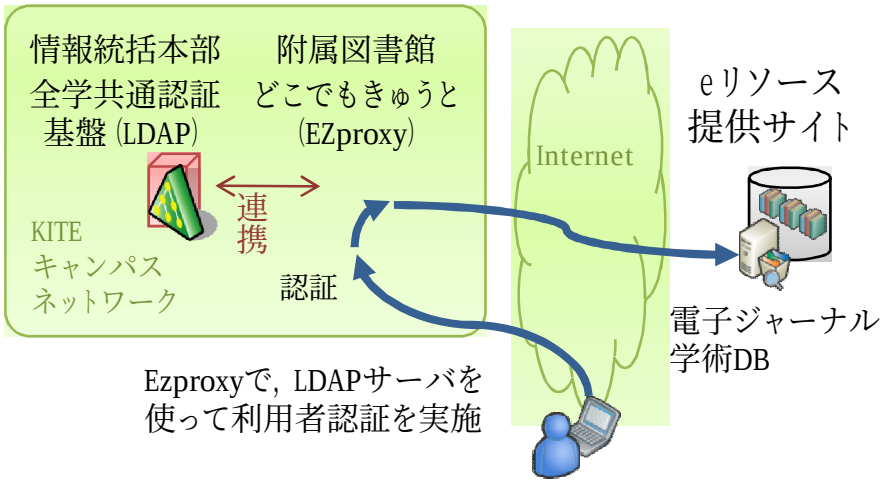
1.4 コンテンツ：学外からの利用，信用性保証

学内からのみアクセスが許されている契約電子ジャーナルに対し，学外からの利用を可能にするために，認証基盤と連動するEZproxyを用意しました。これに「どこでもきゅうと」と名付けてサービスを提供しています。現在，EZproxyのSSO対応を行っています。

また，学内から発信されるコンテンツの信用性保証の仕組みを研究開発しています。機関リポジトリのようなコンテンツ蓄積・発信が普及するにつれ，コンテンツの信用性を保証する仕組みが重要となります。そこでPENSと名付けた信用性保証システムを開発しています。

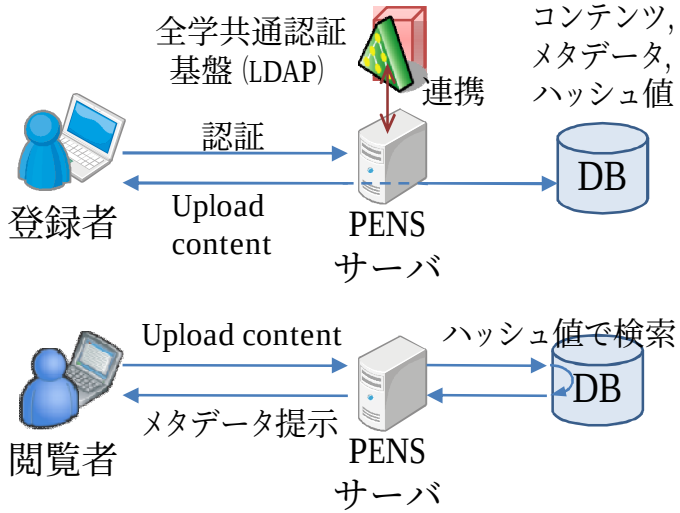
どこでもきゅうと EZproxyを用いたコンテンツ利用

EZproxy経由で，学外からのeリソースへのアクセスを実現



PENSシステム（開発中） コンテンツの信用保証の仕組み

作成者，発行日時，発行元，改竄の有無をチェック



2．UPKIシングルサインオン実証実験

UPKIシングルサインオン実証実験で3つの活動を行いました。

1. Shibboleth SSOに適する情報サービスの調査
2. Shibboleth SSO環境の整備
   - 試験用IdP，SPの構築
   - EZproxyおよびWebCTのShibboleth化
   - 本サービス用IdPの構築
3. Shibboleth SSO環境を用いた研究開発
   - コミュニティ認可機構
   - 要認証サービスのマッシュアップ

3．Shibboleth SSOに適する情報サービスの調査

学内向けの情報サービスについて，Shibboleth SSOの対象に適するもの，適さないものを検討しました。各サービスが，利便性を重視するものか，それともセキュリティを重視するかで分類し，また情報サービスの設置場所が学内のものか，学外のものかで分類しました。分類して検討した結果，利便性を重視するサービスにShibboleth SSOを適用することが良いと判断しました。

	利便性重視	セキュリティ重視
学内	• Campusmate-portal （学生向けWebポータル） • GraceMail（学生向けWebメール） • WebCT（eラーニングシステム） • きゅうとMy Library（図書館Webシステム，貸出更新，貸出状況確認，文献複写/貸借申込など） • どこでもきゅうと（Ezproxyによる学外からのeリソース利用）	•学務システム（履修登録･成績管理） •財務システム（予算管理，物品購入）
学外	• 学術機関向けWebメール(Google Apps, MS Live, Yahoo) • RefWorks (文献リスト管理)	（現在のところ，サービスは存在しない）

Shibboleth SSO環境に適したサービス

Shibboleth SSO導入の利点

- 学内向けサービスの改善
  - 利用者の利便性向上
    - 一度の認証で，複数のサービスが利用
    - 学外･学外を意識する必要がなくなる（利用時は，かならずIdPで認証）
  - 管理作業の効率化
    - 外部サービス(SaaS)での認証を一本化
  - セキュリティの問題
    - 複数レベルを設定できるのか
      - 低セキュリティレベルサービスの認証はID/PWだけで，
      - 高セキュリティレベルサービスの認証は，他の方法をするなど
- 大学間フェデレーションによる効率化
  - eリソース（電子ジャーナルなど）の団体利用など
  - 利用者のすそ野が増えれば，現在は対応していないサービスがSaaS化される可能性もある
- 大学間でのサービス連携の可能性
  - 認証レベル･方式が共通化すれば，その基盤上にサービスを提供可能
  - 大学間のサービスを組み合わせた，新しいサービスが構築できる可能性

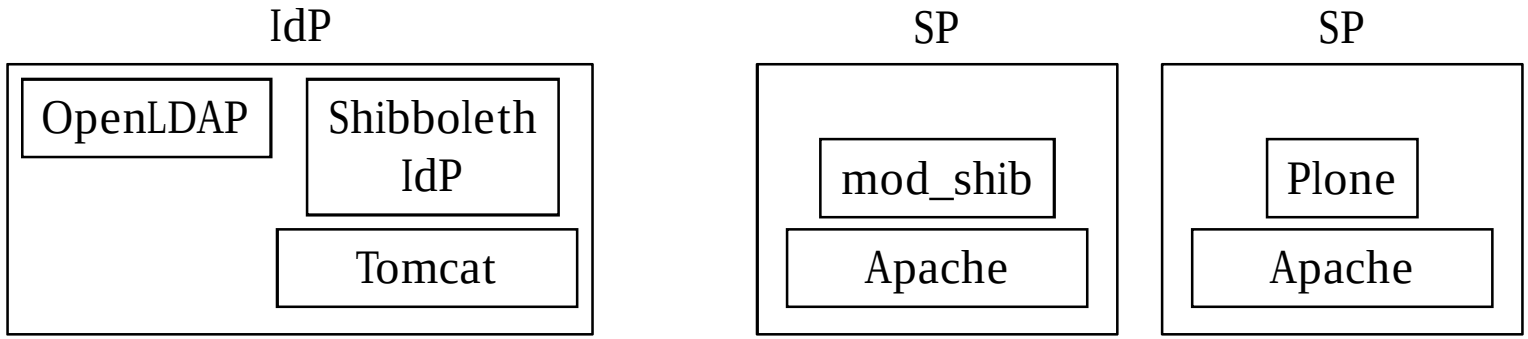
4. Shibboleth SSO環境の整備

○ 試験用IdPの構築

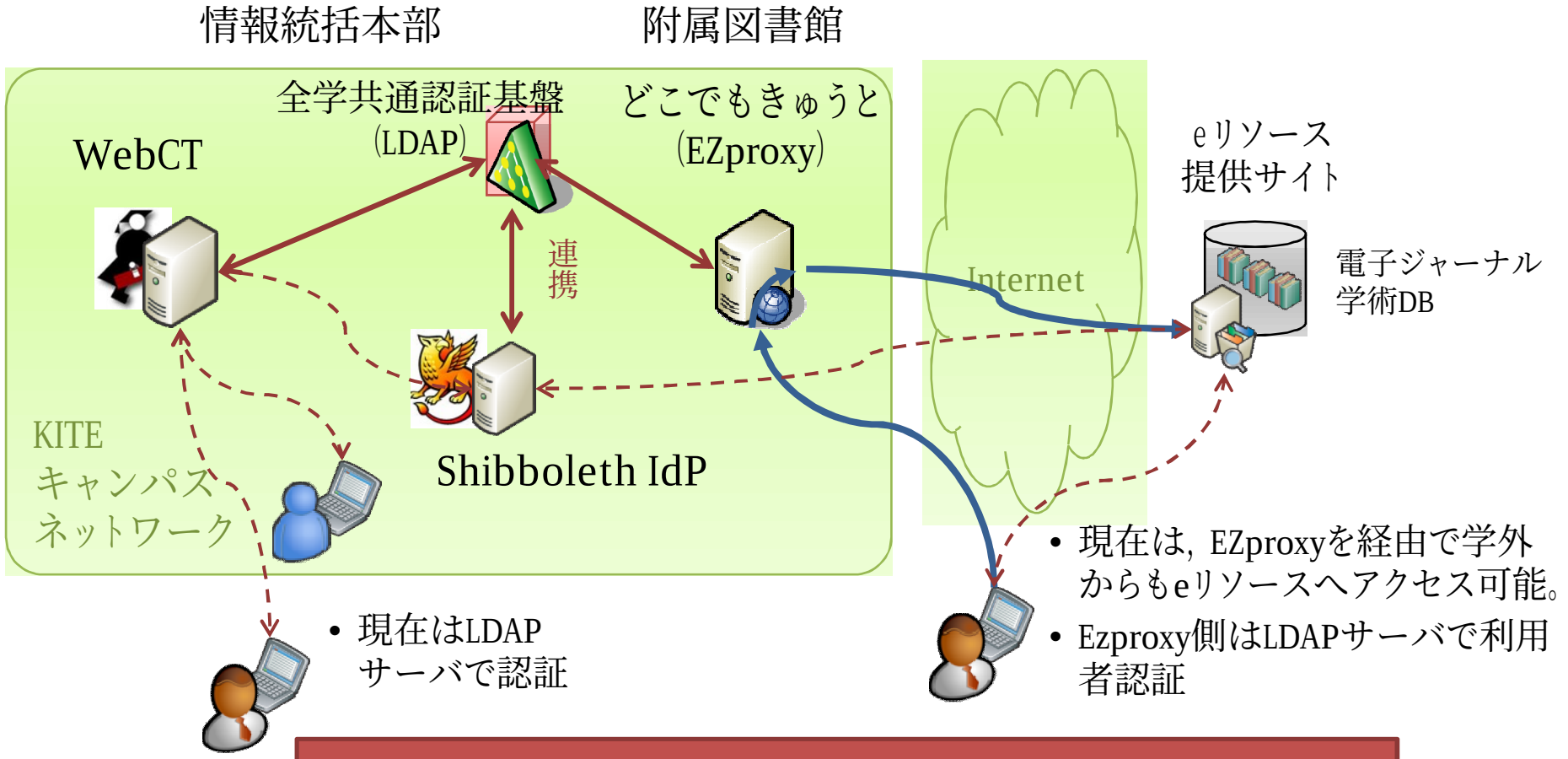
NIIが提供している Vmware イメージを利用して，試験用のIdP（upki-idp.cc.kyushu-u.ac.jp）を構築しました。このさい，OpenLDAPで利用者情報提供サーバを構築し，IdPと接続しました。また，利用者のアカウントとしては，実験用の仮アカウントを作成しました。

○ 試験用SPの構築

SPとして，いくつかの環境を調査しました。まず，NIIが提供する VMware イメージを用いたSP (upki-sp1.cc.kyushu-u.ac.jp)を構築しました。Web CMSであるPloneを用いたShibboleth環境も構築しました。また，Apache Webサーバに Shibboleth認証モジュールである mod_shib を導入し，それを用いた環境も構築しました。



附属図書館　「どこでもきゅうと」(EZproxy)
情報統括本部　WebCT



今後は，Shibbolteh IdPによるSSOに期待

5．Shibboleth SSO環境を用いた研究開発

二つの研究開発を行っています。

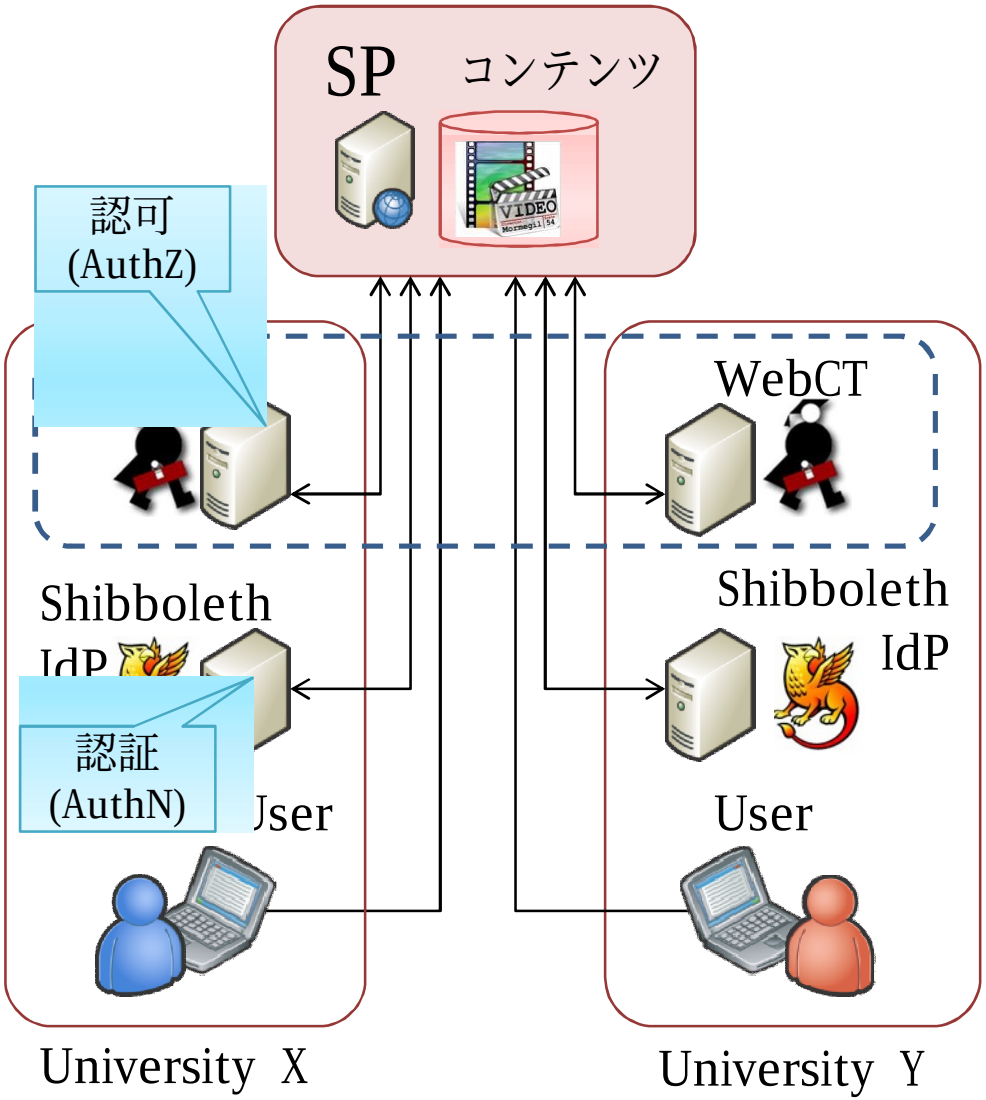
- コミュニティ認可機構
  - 大規模な人員ディレクトリを用いた属性認可が適用しずらい，小規模グループでの情報共有のための認可機構
  - 小規模なグループとして，SNSのコミュニティや，eラーニングシステムWebCTの受講者グループを利用
- 要認証サービスのマッシュアップ
  - 認証を要するサービスの増加と，SaaSと呼ばれる外部サービスの内部利用が背景にある。
  - 認証を要するサービスを，複数組み合わせるための仕組みを検討

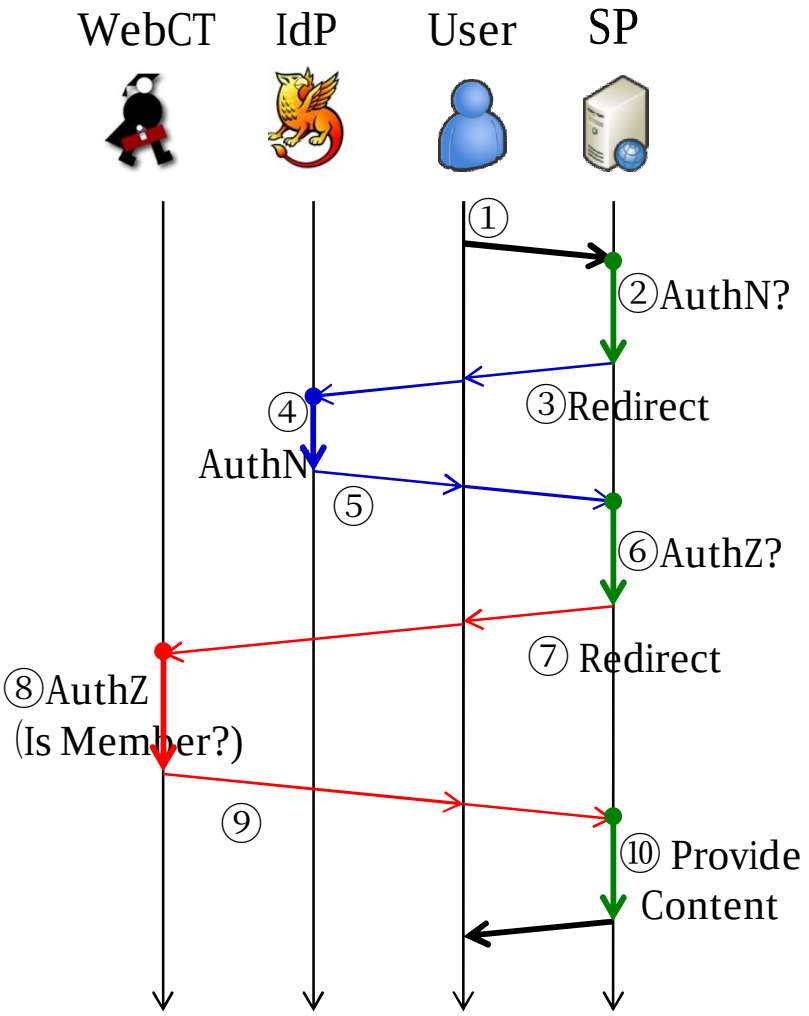
5.1 コミュニティ認可機構

サービスの提供において，細かなアクセス制御を行なうためには，認証だけでなく認可も必要です。認可とは，ある情報資源に対する閲覧･編集といった操作の権限設定を行う操作です。Shibbolothでは利用者の所属部局や性別といった属性に応じて認可制御を行う，属性認可機構が提提供されています。この属性認可は，利用者情報を均一かつ大規模に管理している情報サービスには適しています。しかし，利用者数が小規模な場合や，利用者の管理組織が複数の場合には適用が困難になります。利用者数が小規模な場合のために，Shibboleth化されたサービス内で構成されている「コミュニティ」を用いて認可を行う仕組みについて検討しました。

具体例として，WebCT内部で定義されたグループ情報（各講義の履修者情報）を得ることで，認可を行なうことを試みています。

組織間サービス連携のための，グループ･コミュニティを利用した認可機構





5.2 要認証サービスのマッシュアップ

複数のサービスを連携させ新しいサービスを提供するMashup技術があります。Mashupを利用したサービスは複数のサービスが，あたかも一つのWebサービスであるかのように見せることができます。従来，認証を要する情報サービスの組込みは困難でした。しかし，Shibboleth SSOを用いれば，認証に関する部分の障壁が下がり，要認証Web情報サービスでもマッシュアップを行うことが可能になると考えました。そこで，Shibboleth化された複数の情報サービスを連携するマッシュアップのための基盤について研究開発を行いました。


EA Mash UP - Windows Internet Explorer
http://noah.cc.kyushu-u.ac.jp/~abe/mashup/sample/
EA Mash UP
This is demo Mash Up services.
iKow
My Open Archive
mitter
iKnow! beta
noahnoahnoah
My Open Archive
Search
Recent entries
Share Your Video Experience.
mitter beta
最近見た動画
ページが表示されました
インターネット
100%

6. おわりに

九州大学では, NIIのCSI事業およびUPKIプロジェクトの開始に合わせて, H17年度より認証基盤の整備を進めてきました。その成果として, H19年度から全学共通認証サービスの提供を開始しました。

H20年度から始まったUPKIシングルサインオン実証実験では, 以下を実施しました。

1. Shibboleth SSOに適する情報サービスの調査
2. Shibboleth SSO環境の整備
3. Shibboleth SSO環境を用いた研究開発

今後, 以下を行う予定です。

- 実用サービスでのShibboleth SSO適用
  - コミュニティ認可機構
  - 要認証サービスのマッシュアップ
- 国内フェデレーションへの参加および協力
- Shibboleth SSOを用いたサービスについての研究開発