KYUSHU UNIVERSITY 2011
100th Anniversary

UPKI シンポジウム

九州大学の取り組み

伊東栄典
九州大学情報基盤研究開発センター
ito.eisuke.523@m.kyushu-u.ac.jp

KYUSHU UNIVERSITY

1. はじめに

1. はじめに
2. 九州大学全学共通認証基盤
3. Shibboleth IdPの構築
4. フェデレーションへの参加
5. おわりに

1. はじめに

- 大学向けICTサービスの問題
  - サービスの多様化
  - 効率化，省エネ，コンプライアンス
- 認証を要する情報サービスの増大
  - 認証用ID/PWの増加
  - 認証作業が面倒になった
    - 利用者：ID/PWが複数あって，どれかわからない
    - 管理者：アカウント管理が，面倒
    - CIO：安全性（セキュリティ）の低下
  - 統一的な基盤が必要
- 九州大学の全学認証基盤についての取り組みを紹介

2. 九州大学全学共通認証基盤

1. はじめに
2. 九州大学全学共通認証基盤
3. Shibboleth IdPの構築
4. フェデレーションへの参加
5. おわりに

2.九州大学全学共通認証基盤

- 九州大学の中期的情報政策
  －安全・安心な全学情報基盤の整備と九州大学e-University の実現を目指して－
  - 2007年2月5日に策定
  - 10個の基幹システムの整備を目標化

基幹システム	実現すべき機能・サービス
①教育・研究支援システム	研究用計算機システム，教育用計算機システム，ITサテライト拠点（情報サロン），e-Learning システム，学生用パソコンの充実等
②情報ネットワークシステム	高速で安全な学内情報ネットワーク，情報セキュリティ対策，全学無線LANサービス，ネットワーク監視等
③電子認証システム	全学共通ICカードシステム，全学共通個人認証システム，SSO（シングルサインオン）等
④遠隔講義・遠隔会議システム	遠隔講義システム，遠隔会議システム，遠隔ミーティング，パソコンTV会議等
⑤学外情報発信システム	オープンコースウエア（OCW），機関リポジトリー等
⑥サーバホスティングシステム	メールサーバホスティング，Webサーバホスティング，FTPサーバホスティング，サーバハウジング等
⑦全学情報共有システム	全学ポータル，全学グループウエア，全学電子掲示板等
⑧電子事務(e-Jimu)システム	電子申請，電子手続き，電子決裁システム，文書管理システム，事務情報提供サービス等
⑨業務システム	学務情報システム，図書館システム，人事給与システム，財務会計システム，経営シミュレーション等
⑩全学ソフトウエア管理システム	ソフトウエアのオンライン配布，全学ライセンスの一元管理，ソフトウエアパッチのオンラインサービス等

九州大学 全学共通認証基盤

- 目的
  - 認証における煩雑さを解消
  - 情報サービスの利便性・信頼性・安全性を向上
  - （大学活動の生産性向上）
- ３つのサービス
  - 全学共通IDの発行・管理
  - 認証機能の提供
  - サーバ証明書の申請受付

経緯

2005年 2006年 2007年 2008年 2009年 2010年 2011年

九州大学

UPKI参画　**学内認証基盤の整備**

LDAP導入　パスワード管理装置導入　全学共通認証事業室設置　全学共通ID発行

多数のサービスで認証統合

学内無線LAN
kitenet（認証付き）

フェデレーション

Shibboleth IdP
学内向け試行運用

Reverse Proxy SSO導入
（マトリックスパスワード認証）

全学基本メール開始

？

NII

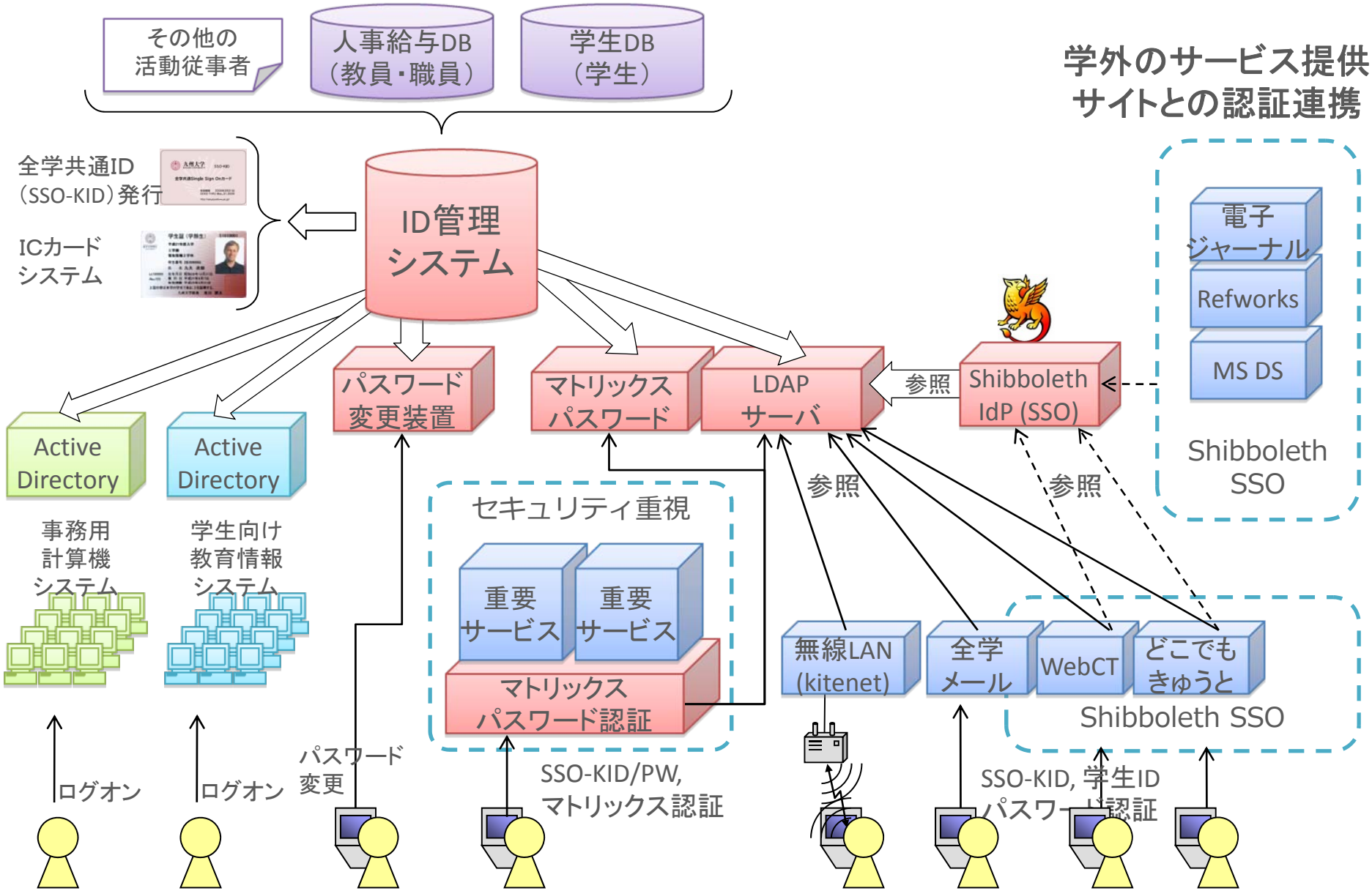
UPKI開始　UPKI Initiative　サーバ証明書 →

eduroam.jp →

GRID →

SSO実証実験 → UPKI-Fed 試行運用 → 学術認証フェデレーション

九州大学全学共通認証基盤　システム構成



アカウント数

	学生・院生・非正課生	職員	その他
登録利用者数	18,000	7,700	200～400
毎年の入れ替わり数	3,600（ほとんど4月）	1,000（ほとんど4月）	不明（今年から開始）

その他：派遣等，他機関からの出向者，名誉教授，学外非常勤講師，臨床教授

3. Shibboleth IdPの構築

1. はじめに
2. 九州大学全学共通認証基盤
3. Shibboleth IdPの構築
4. フェデレーションへの参加
5. おわりに

3. Shibboleth IdPの構築

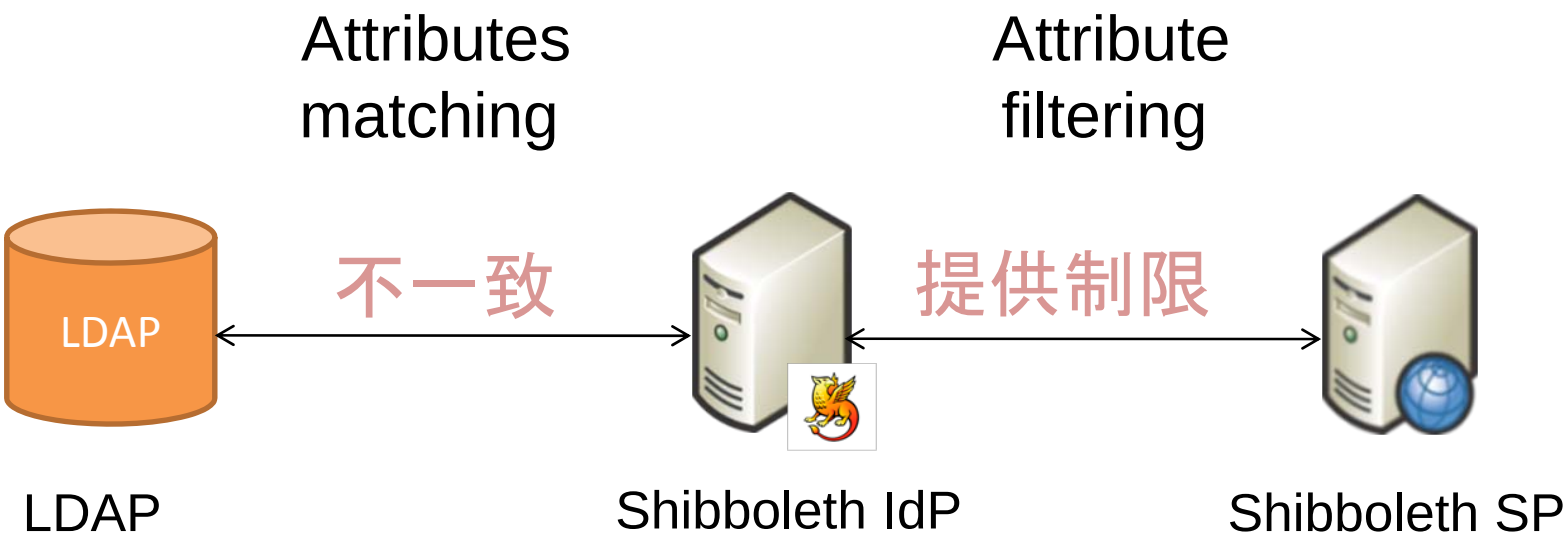
- Shibboleth IdPを構築
  - 学内サービスでのシングルサインオン実現
  - 外部のSaaS系サービスの利用
  - 大学間認証連携

Web情報サービスの対応方法

	学内サーバ	学外サービス (SaaS, ASP)
利便性重視（低セキュリティ）	• 全学基本メール（Webmail） • WebCT (e-Learning) • 全学ライセンスソフト提供 • 全学ポータル 分散認証型SSO Shibboleth (SAML)	• 電子ジャーナル • RefWorks • Google Apps
安全性重視（高セキュリティ）	• 財務会計システム • 学務情報システム（成績管理） ID/PW認証とマトリックス認証 Proxy型SSO	？

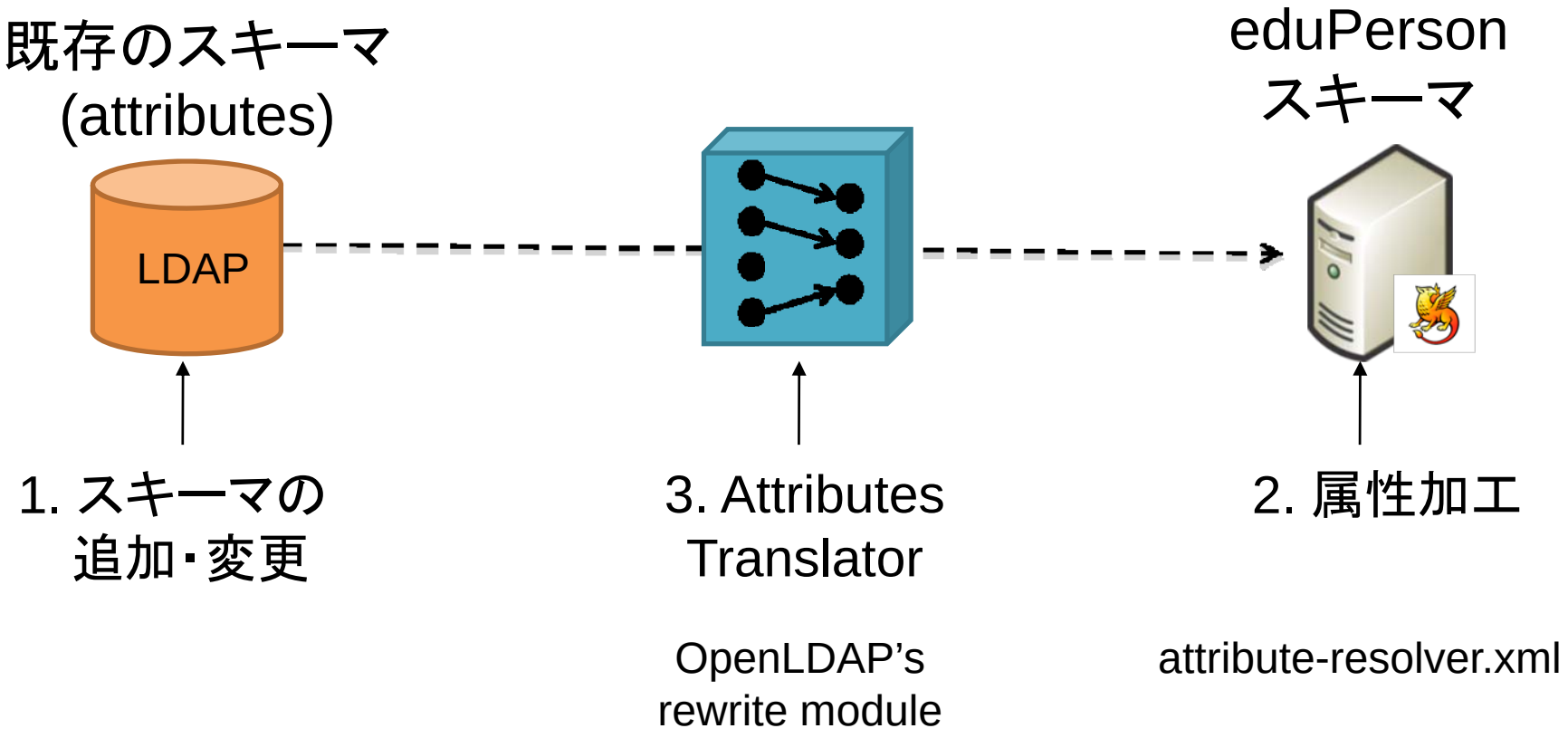
Shibboleth IdP構築における問題

- 2つの問題



Attribute mismatchの解決手法

- 3 つの解決手法

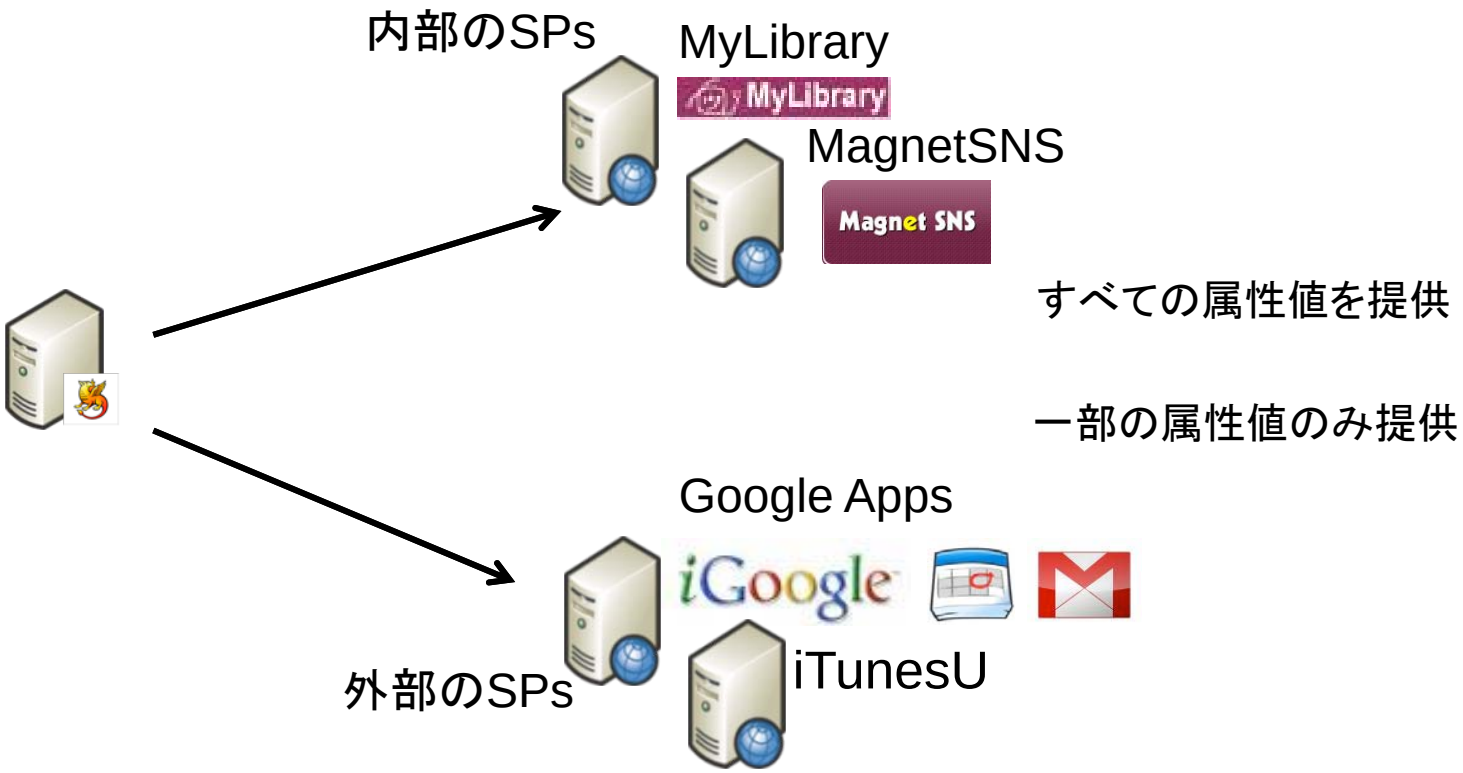


Attribute mismatch解決手法の比較

	既存のスキーマ構成を変更	Shibboleth側で属性加工	Attribute Translatorを利用
SP	○	○	○
利用者	○	○	○
IdP（管理者）	・属性管理システムに変更	○	・Attribute Translatorを新たに構築
利点	・一度設定してしまうと運用が簡単 ・新たなサーバを構築する必要なし	・属性管理システムに変更を加える必要なし ・新たなサーバを構築する必要なし	・設定が簡単 ・属性管理システムに変更を加える必要なし
問題点	・属性管理システムの変更にかかるコスト ・既存のサービスを変更する必要が発生する可能性あり	・設定が煩雑	・管理サーバ数増加のため管理者の負担が増加

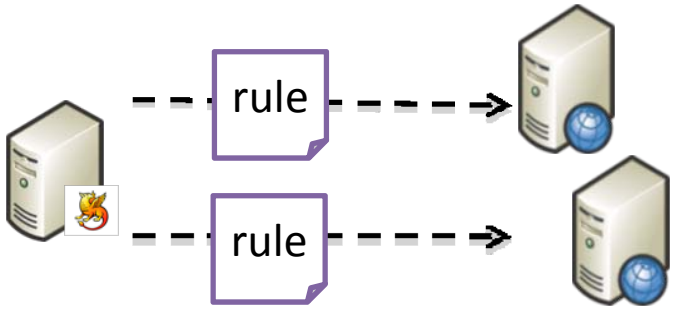
Attribute filtering

- 外部SPには属性情報を一部しか提供しない

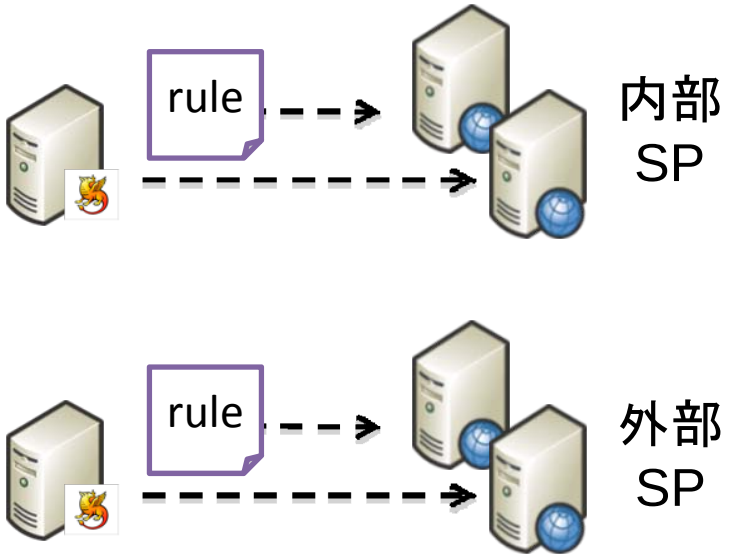


Attribute filteringの解決手法

1. SPごとに属性提供ルール



2. 複数のIdPs

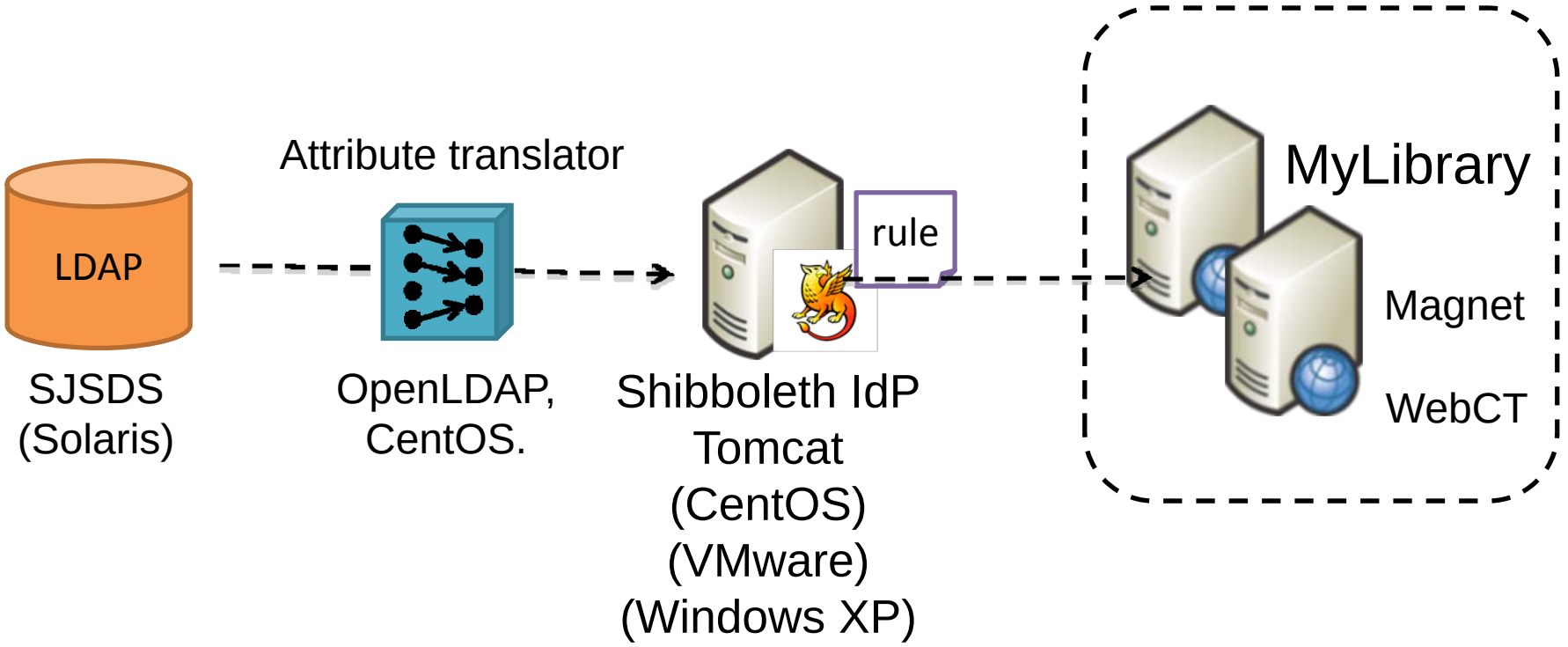


Attribute filtering解決手法の比較

	1. SPごとにルールを記述（attribute filter利用）	2. 複数IdPを構築
SP	○	○
利用者	○	・2回以上認証操作が必要
IdP	○	・IdPサーバを新たに構築
利点	・新たなサーバを構築する必要なし	・設定が簡単
問題点	・設定が煩雑	・管理サーバ数増加のため管理者の負担増

IdP運用状況

システム構成



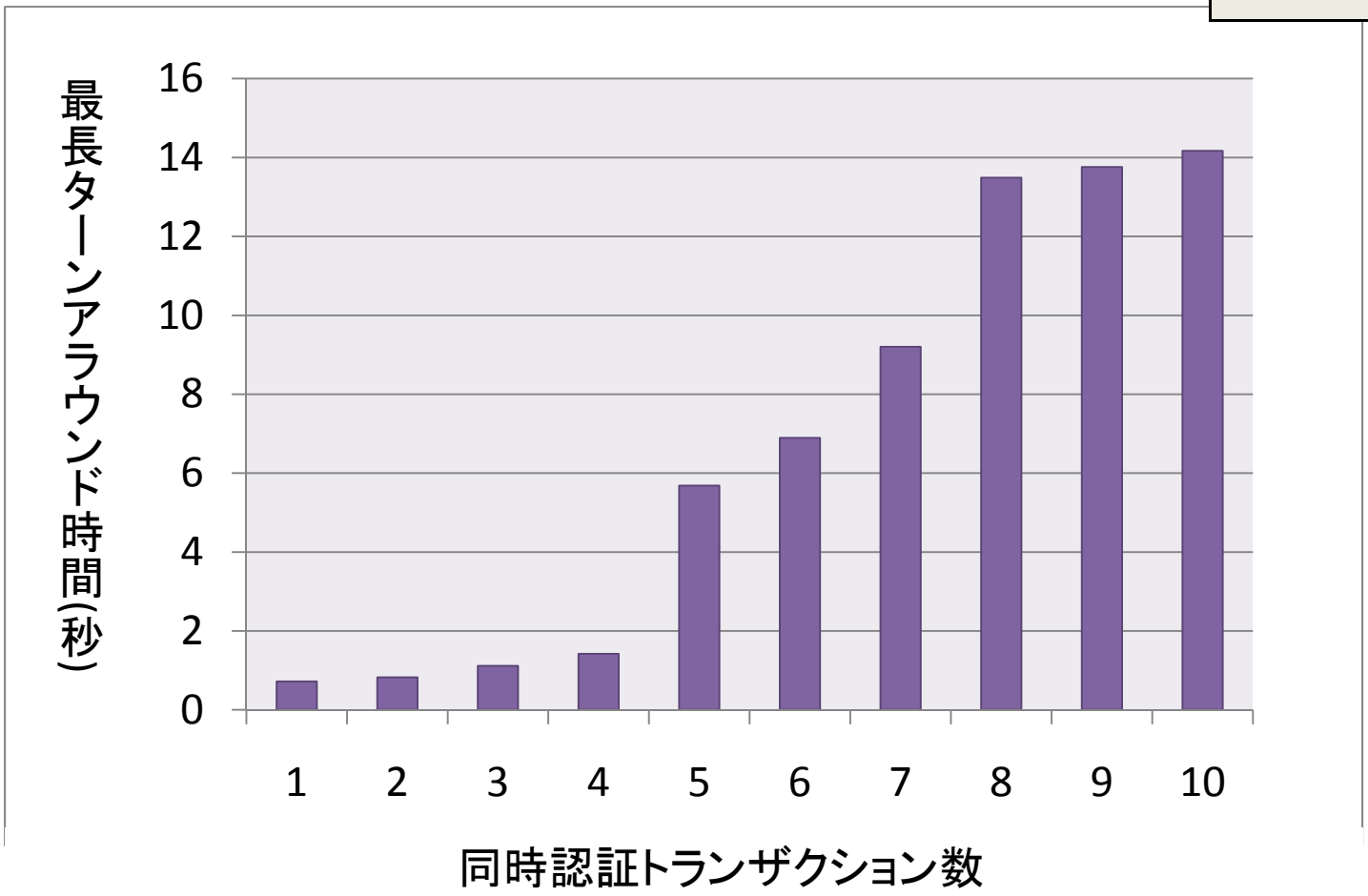
Kyushu University Library
http://www.lib.kyushu-u.ac.jp/

IdP

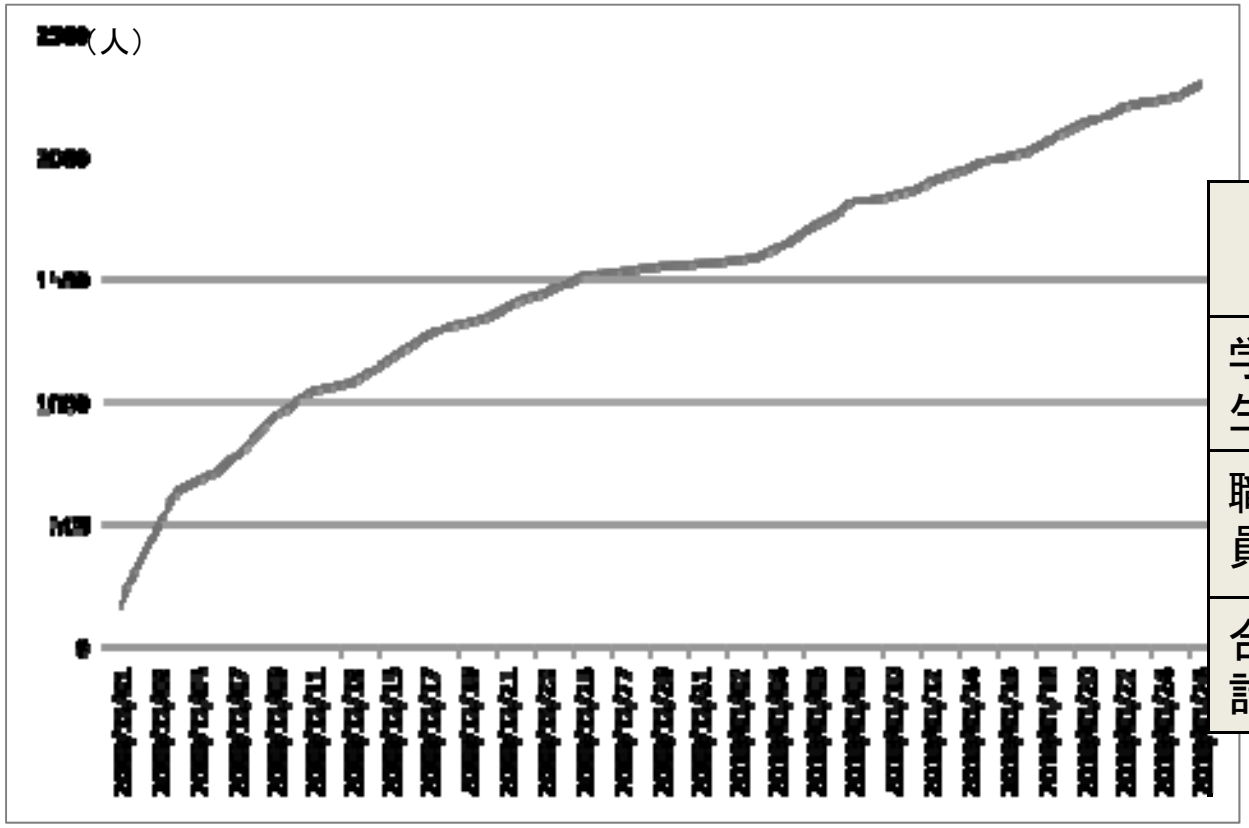
SP

処理速度の測定

試作環境	
OS	CentOS5.3
メモリ	256MB
CPU	Athlon 2.6GHz

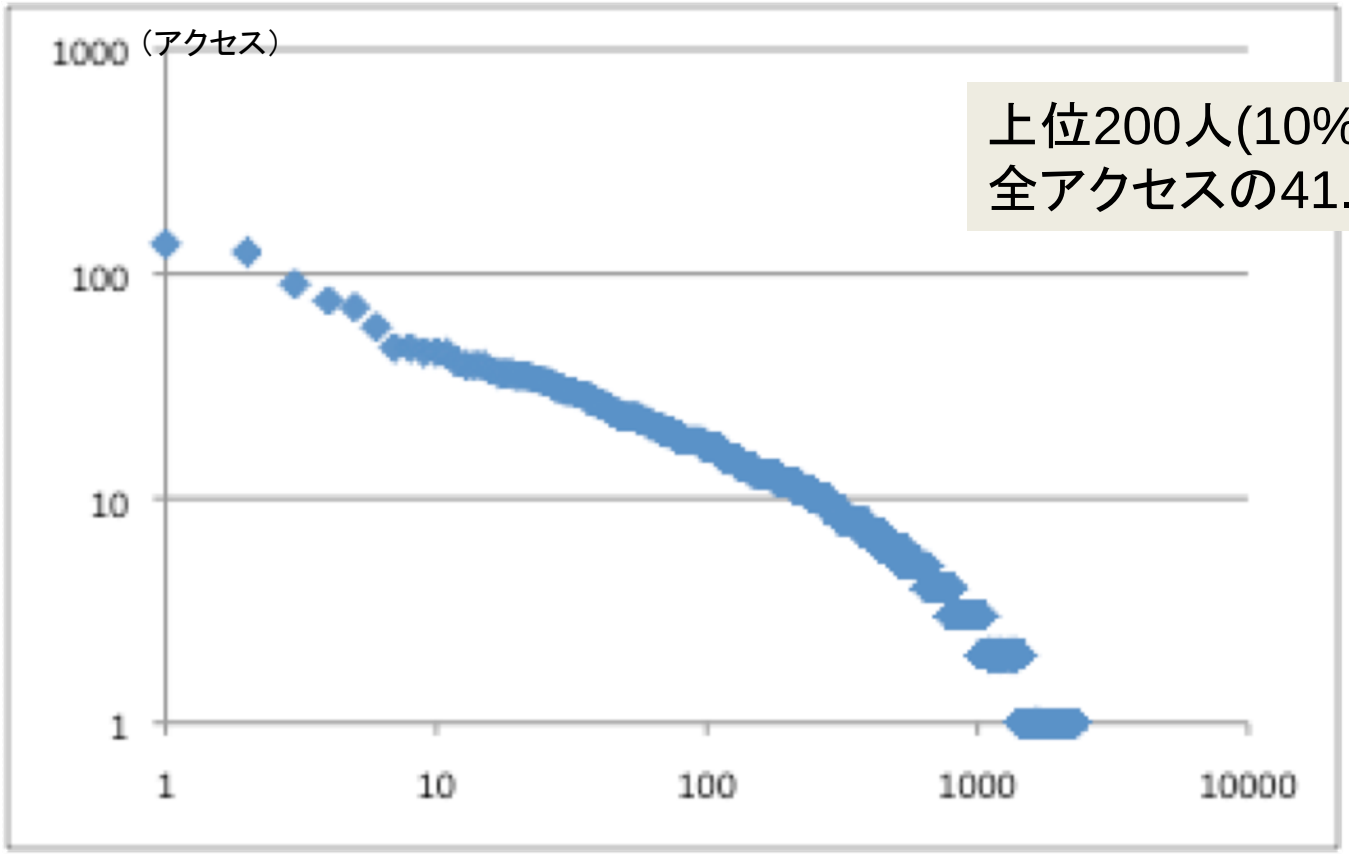


ユニークユーザ数



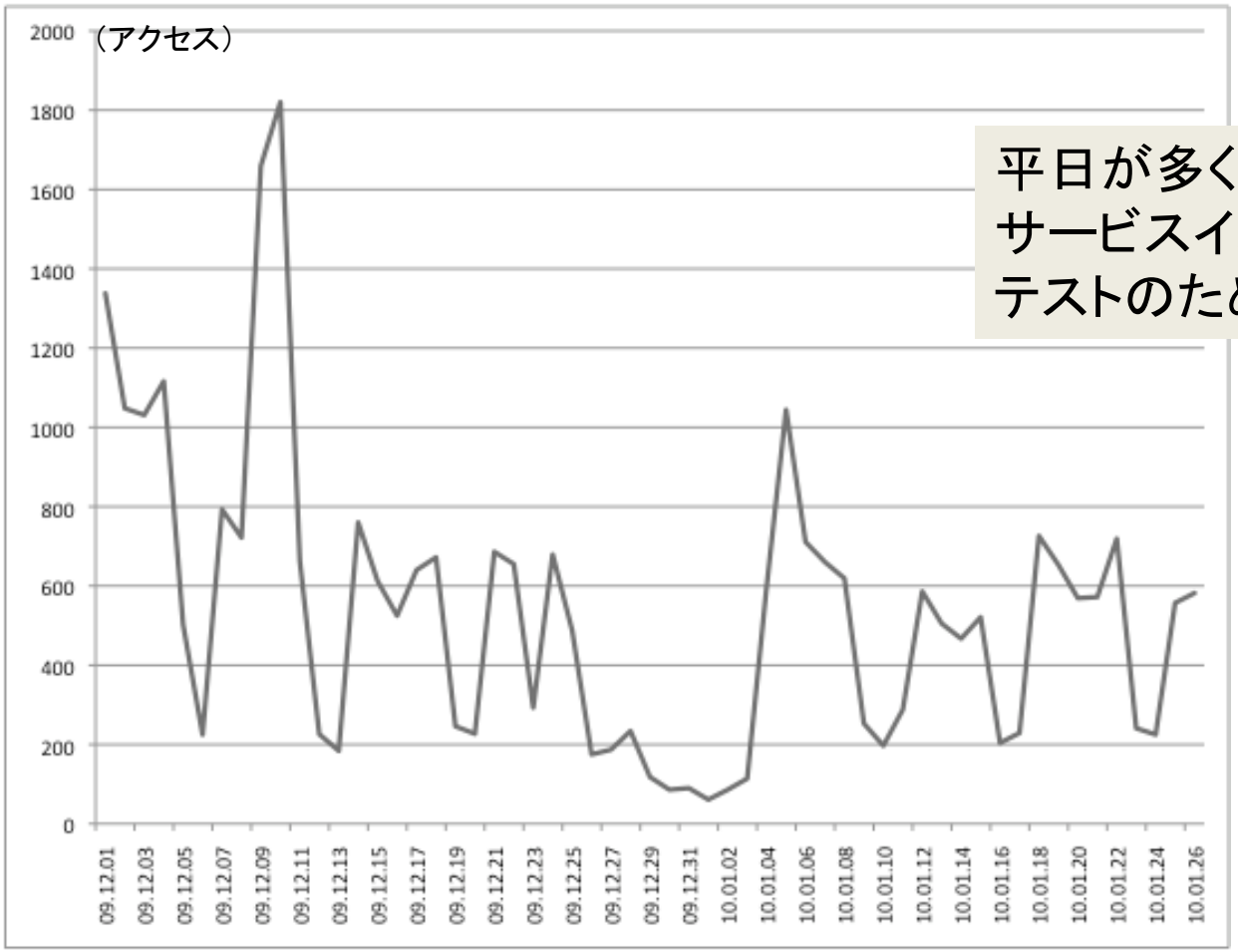
	利用者数	総数
学生	1815	18000
職員	467	7000 (2500)
合計	2291	25000

利用者・アクセス頻度



上位200人(10%)
全アクセスの41.2%

日毎のアクセス



平日が多く、土日が少ない
サービスイン直後は
テストのためアクセス数が多い

時間ごとのアクセス

学校にいる時間帯（午後）の
利用が多い

4. フェデレーションへの参加

1. はじめに
2. 九州大学全学共通認証基盤
3. Shibboleth IdPの構築
4. フェデレーションへの参加
5. おわりに

4. フェデレーションへの参加

- 2009年12月から，学内向けサービスへShibboleth IdPを試行提供
- 2010年，フェデレーション参加
  - 学外のサービスの利用
    - 全学情報環境利用委員会での承認
    - 九州大学内では試行的に，運用サーバへ参加
  - 来年度に向け，高性能サーバを準備
    - SP増加により，同時利用者数が増加する場合への備え
  - 年度末までにRefWorksに対応（予定・作業中）

5. おわりに

1. はじめに
2. 九州大学全学共通認証基盤
3. Shibboleth IdPの構築
4. フェデレーションへの参加
5. おわりに

5. おわりに

- 九州大学の認証基盤を紹介
  - 全学共通認証基盤
  - 情報統括本部・全学共通認証事業室
  - SSOの方針，Shibboleth IdP，運用結果
  - フェデレーションへの参加

今後の期待

- 認証サービスの増加
- 利用権を設定しているサービスの増加
  - 電子ジャーナル
  - データベース
  - ソフトウェア
  - Google Apps, Windows Live, Yahoo academic mail
  - その他コンテンツ
  - 電子書籍
- 要認証サービス間での連携