九州大学におけるUPKI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

出版情報：2009-12. 国立情報学研究所
バージョン：
権利関係：

Kyushu University 2011
100th Anniversary

事例紹介

九州大学におけるUPKIの取り組み

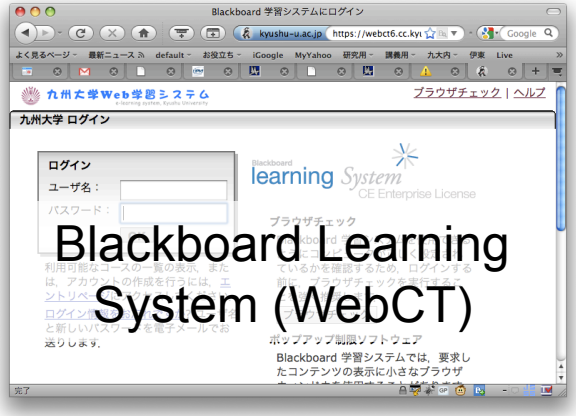
伊東栄典
九州大学情報統括本部
ito.eisuke.523@m.kyushu-u.ac.jp

KYUSHU UNIVERSITY

目次

1. はじめに

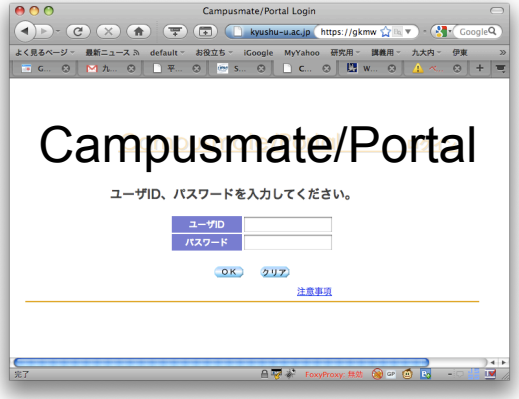
- 認証を要する情報サービスの増大
  - 認証用ID/PWの増加
- 認証作業が面倒になった
  - 利用者：ID/PWが複数あって，どれかわからない
  - 管理者：アカウント管理が，面倒
  - CIO：安全性（セキュリティ）の低下
- 統一的な基盤が必要


Blackboard Learning System (WebCT)


Microsoft Office SharePoint Server


教員業績DB

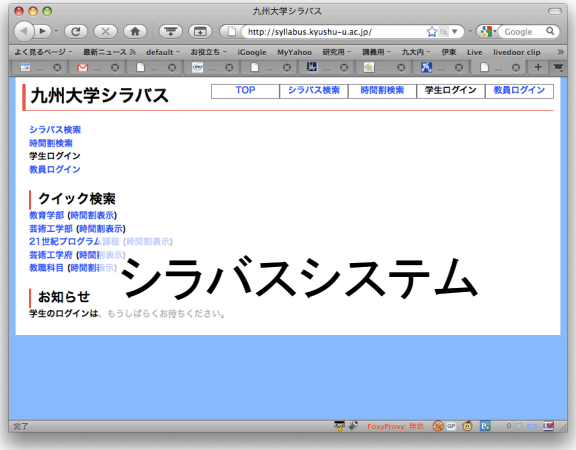

全学基本メール
Mirapoint Web Mail


Campusmate/Portal


Netacademy2
英語学習


九州大学機関リポジトリ
QIR
（附属図書館）


Campusmate-J
成績登録・確認


シラバスシステム

本発表の内容

- 九州大学の事例を紹介
  - 学内の認証統合
    - 全学共通認証基盤の方針・内容
  - 学外の認証連携へ
    - Shibboleth SSOの取り組み
    - UPKI Federationへの参加

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）

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 →

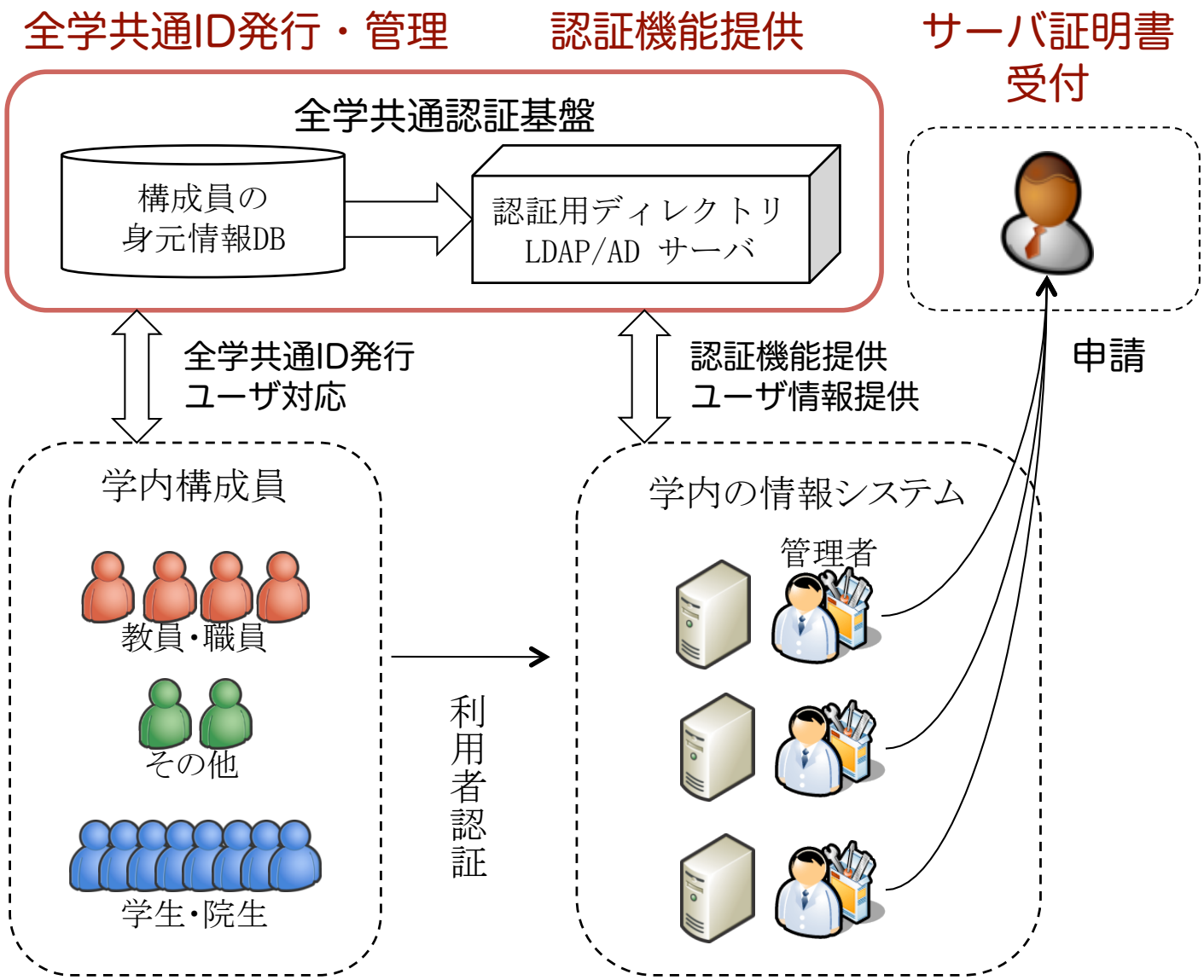
SSO実証実験 → UPKI-Fed 試行運用 → UPKI-Fed 学術認証フェデレーション →

2. 九州大学 全学共通認証基盤

- 認証における煩雑さを解消
- かつ，情報サービスの利便性・信頼性・安全性を向上

- 学内向け情報サービスにおける，認証を統合
- 九州大学　情報統括本部 全学共通認証事業室
  - 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

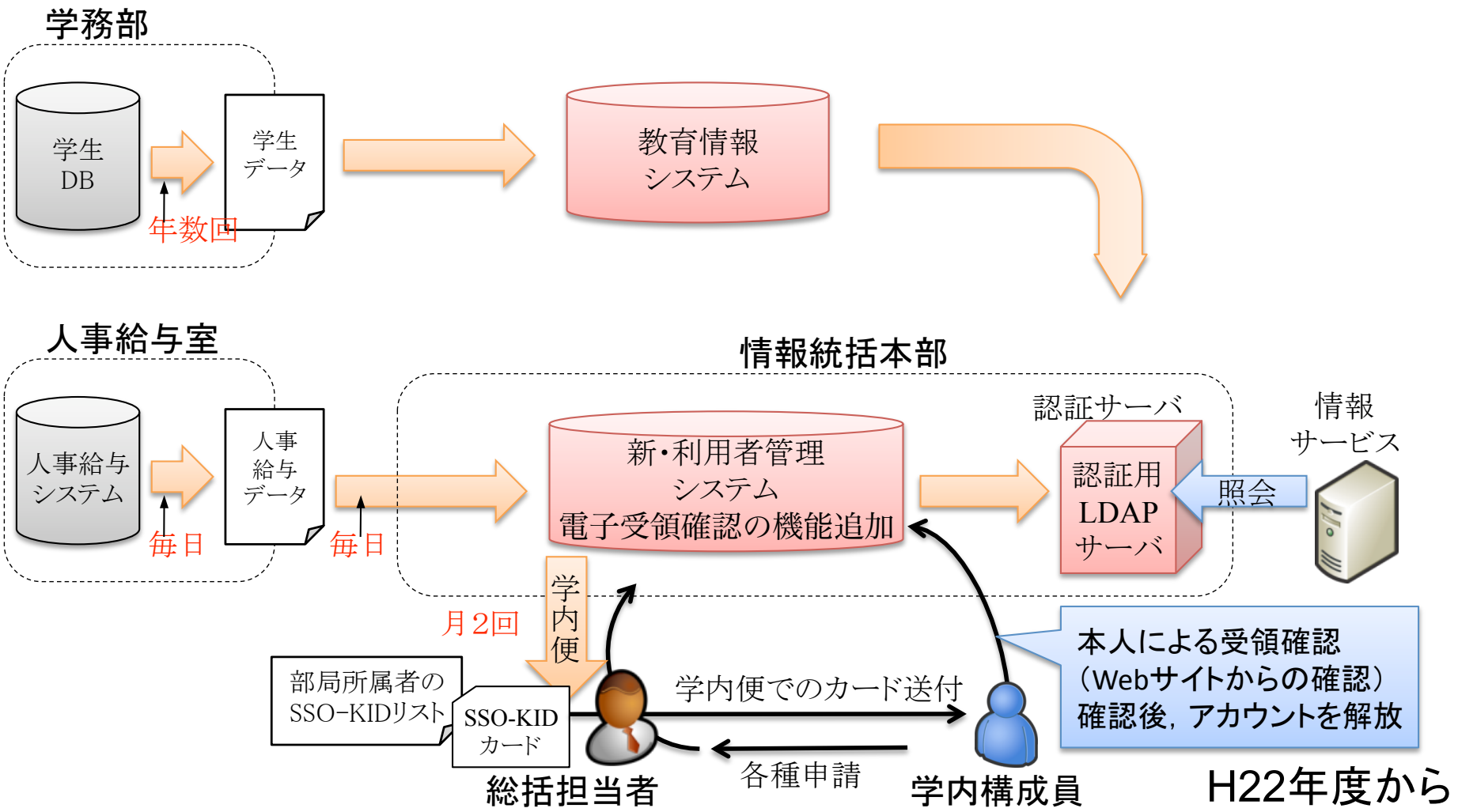
九州大学 全学共通認証基盤



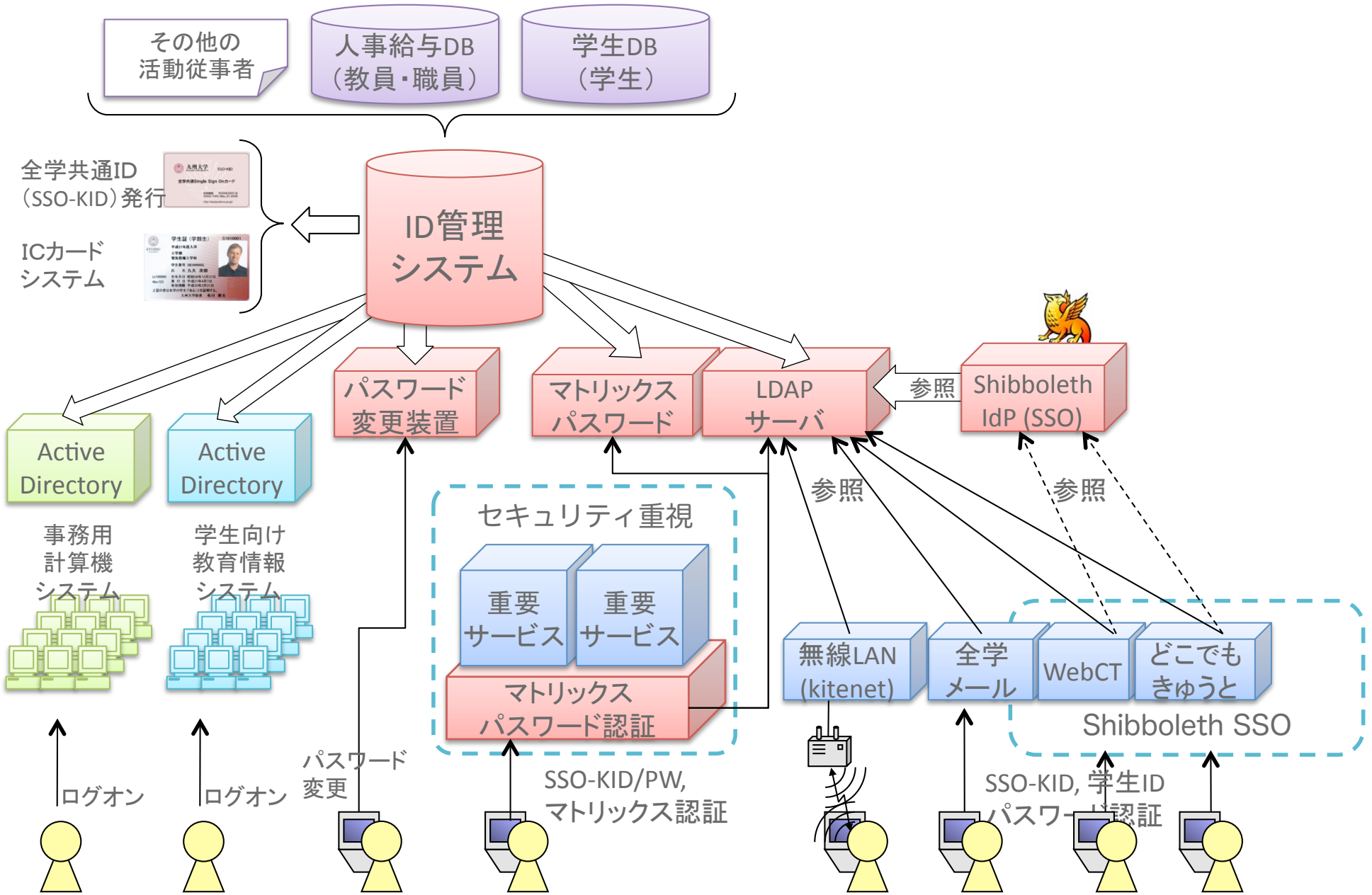
対応サービス

- 教育情報システム，学生用メール，学生ポータル
- kitenet（無線LANアクセス）
- 九州大学シラバス
- 全学ライセンスソフト （マイクロソフト，セキュリティ対策ソフト）
- WebCT （Web学習システム）
- NetAcademy 2 （英語学習システム・ 言語文化研究院提供）
- どこでもきゅうと （附属図書館電子ジャーナル利用）
- スペース管理システム （施設部）
- 全学基本メール
- 学務情報システム（学務部）
- 大学評価・教員業績評価支援システム（大学評価情報室）
- 事務用計算機システム（事務LAN接続端末の認証）
- ICカード職員証Web申請

ID管理のデータフロー



九州大学全学共通認証基盤　システム構成とデータフロー（H21年度）



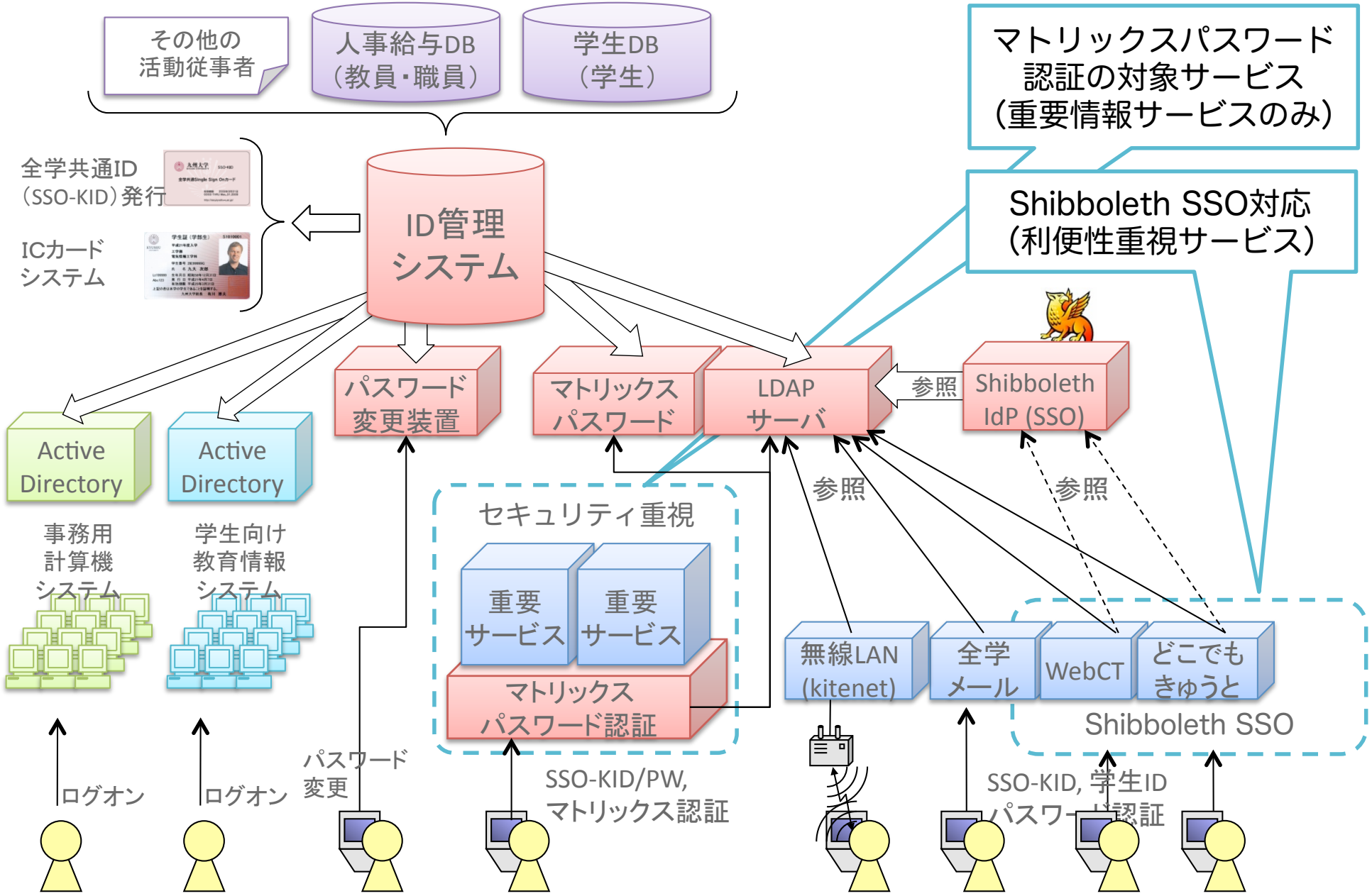
3. SSO環境の構築

- ID統合による安全性（セキュリティ）の問題
  - 一つのID/PWで，全サービスが利用できて便利になった
    - ID/PWが破られると，全サービスを利用されてしまう
  - 学内の情報サービスに，LDAPで認証機能を提供
    - 情報サービス側にID/PWを入力する
    - 情報サービスが破られると，ID/PWを盗まれるかも
  - 安全性（セキュリティ）の考慮が必要
- まだSSOになっていない。
  - Single ID/PWにはなったけれども
- 安全かつ便利なシステムが必要
  - セキュリティレベルに応じたシステムが必要

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)
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	?
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

九州大学全学共通認証基盤　システム構成とデータフロー（H21年度）



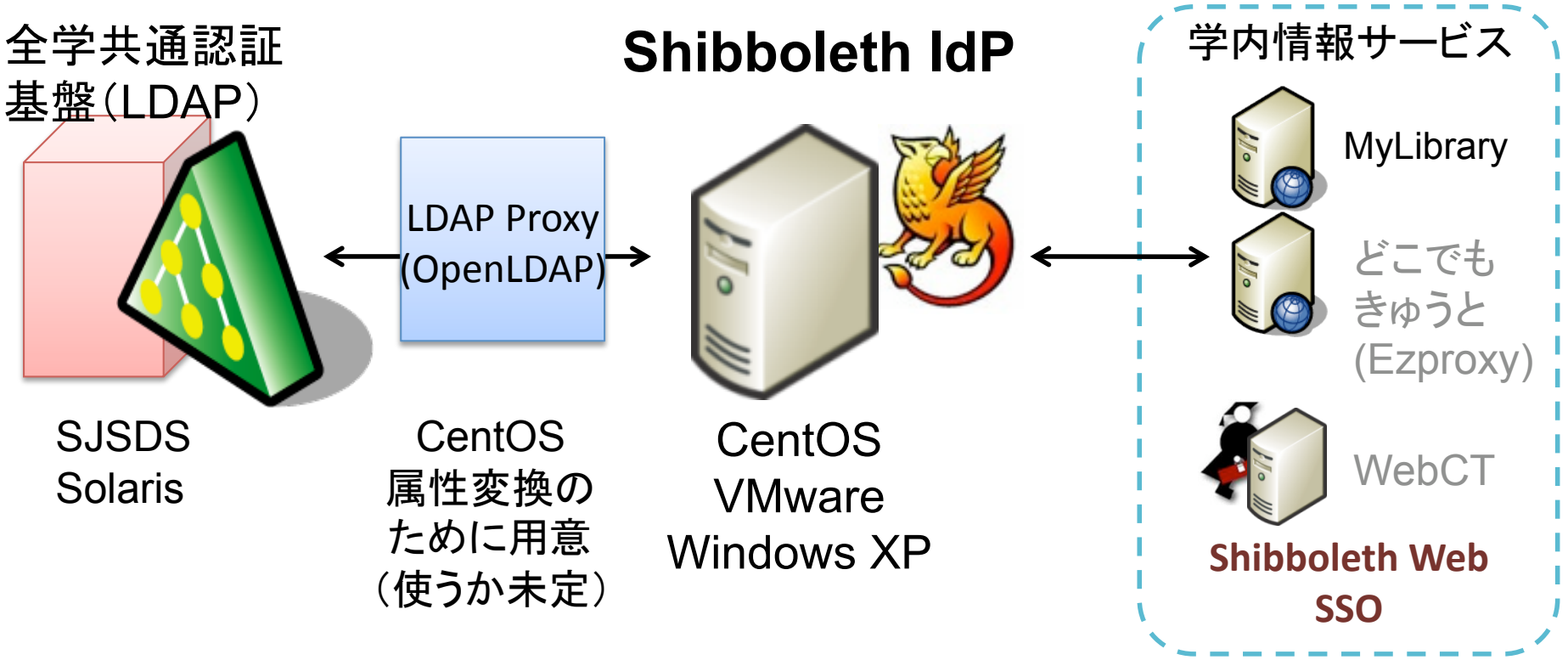
マトリックスパスワード認証

- Reverse Proxy SSO
- 利用者は職員のみ
- 重要サービスのみ
  - 学務情報システム（成績登録）
- マトリックスパスワード
  - IC職員証の券面に印刷

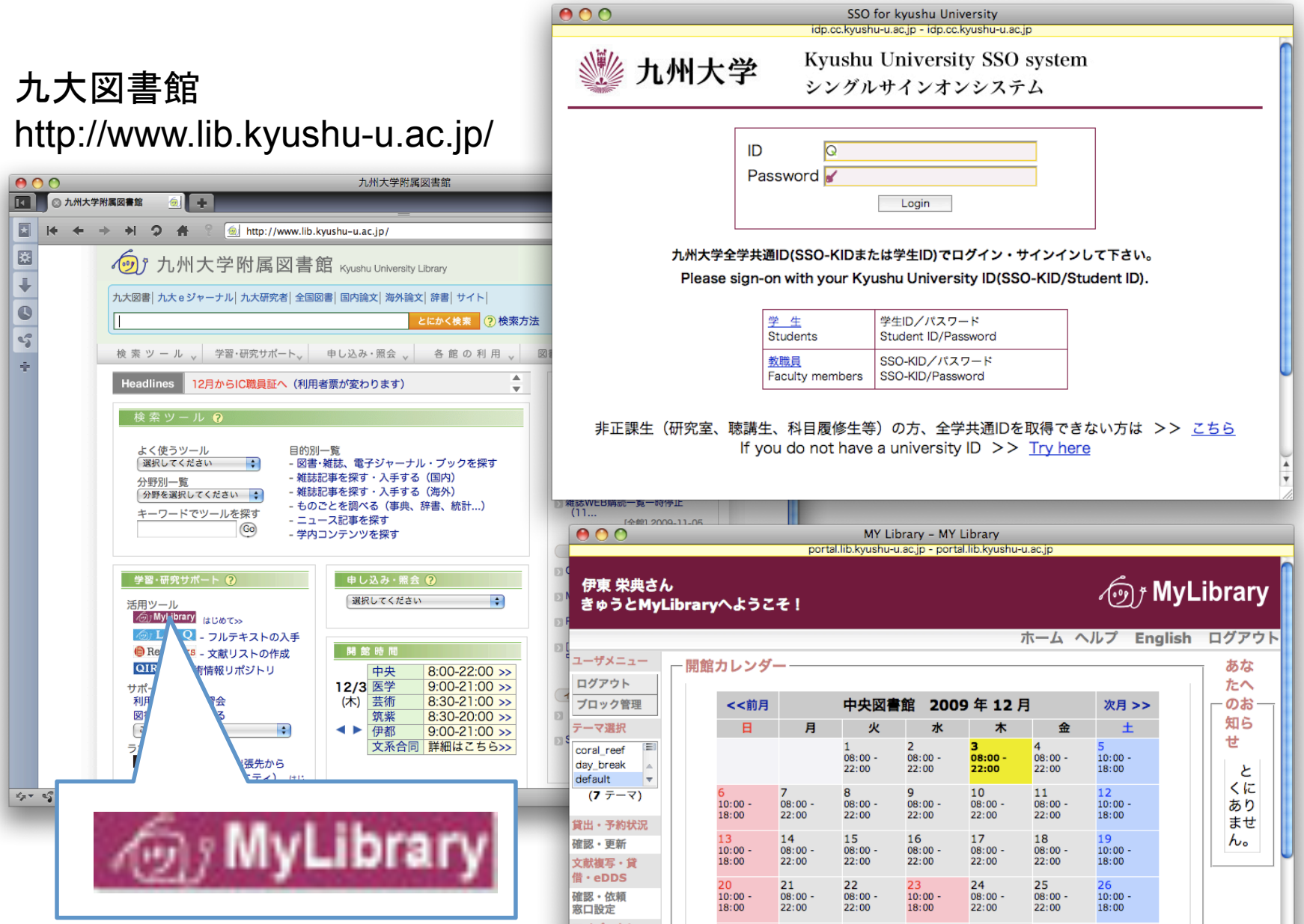
4. Shibboleth SSO

- 利便性重視のシステムは，ShibbolethでSSO環境を構築
  - セキュリティ的に良い
  - 全国標準になりつつある
  - 学外との連携，フェデレーションにもつながる

Shibboleth システム構成



九大図書館
http://www.lib.kyushu-u.ac.jp/



IdP

SP

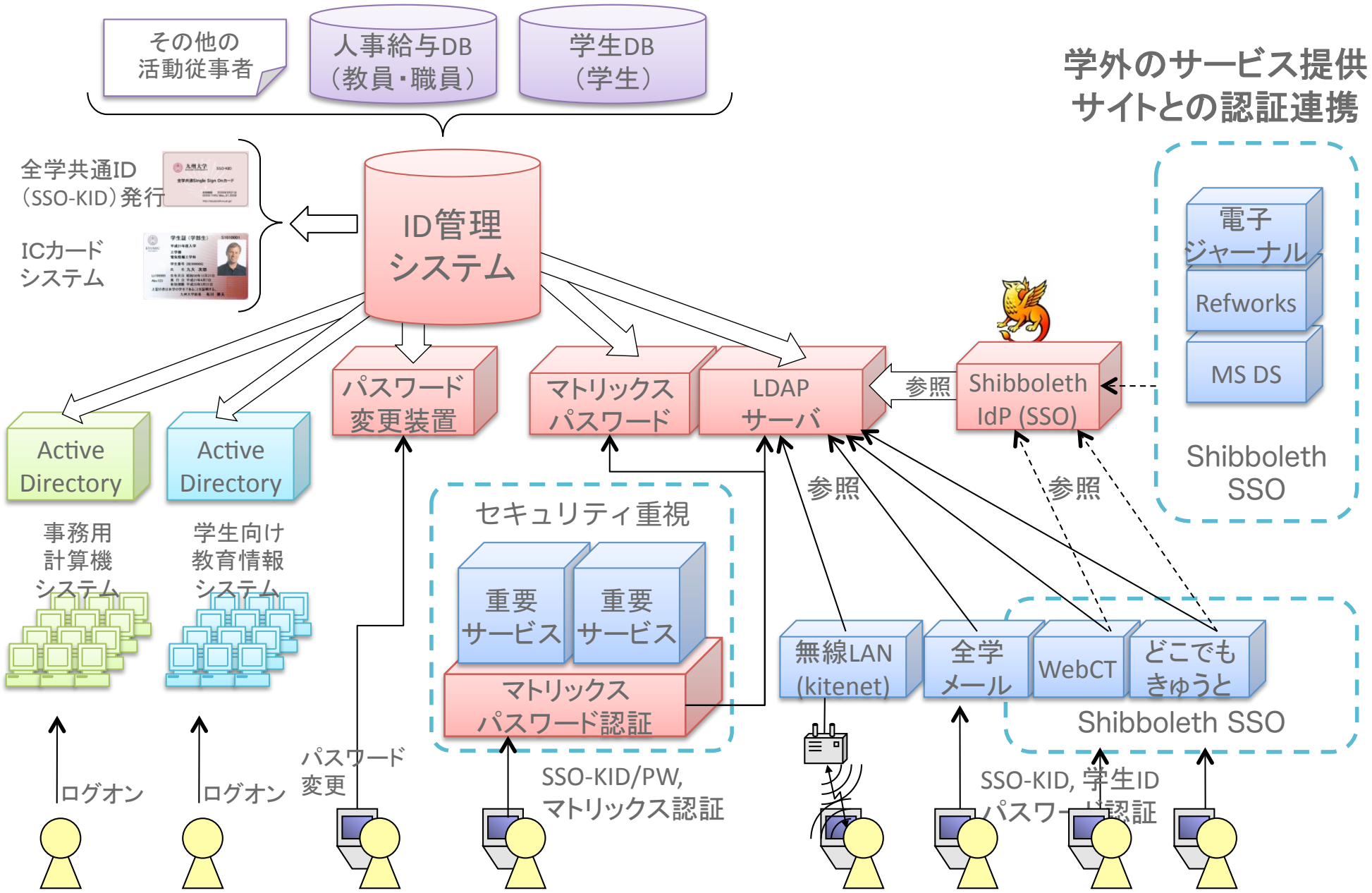
Shibboleth SSOの状況

- 始まったばかり(2009年12月1日にサービスイン)
  - 今の所，順調
- 利用者が増えると，処理できるかは不安
  - 高性能サーバに変更予定

4. UPKI Federation

- 学外組織提供のサービスが利用したい
  - 電子ジャーナル,
  - MS DreamSpark
  - (Google Apps)
  - その他，SaaS系のサービス
- 参加状況
  - テストフェデレーションに参加
  - 試行運用フェデレーションにも参加（予定）
    - 学内の合意形成が必要
    - 外部SPへ提供する属性情報の扱いについて，きちと検討する必要がある。

九州大学全学共通認証基盤　システム構成とデータフロー（H22年度）



JANET Training

- JANET
  - 英国の組織（学術ネットワーク運用から発展）
- 各種の研修コースを提供
  - そのなかのShibboleth IdP/SP構築研修に参加

- トレーニングの内容
  - テキストと，VM環境を与えられる（VMは持ち帰りOK）
  - ２日間（一日目：IdP，２日目：SP）
  - 一通り設定ができる
    - 予備知識が無いと，わからない

6. おわりに

- 九州大学の事例を紹介
  - 全学共通認証基盤
    - 全学共通ID
    - マトリックスパスワード認証装置
  - Shibboleth環境
  - フェデレーションへの参加状況