

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



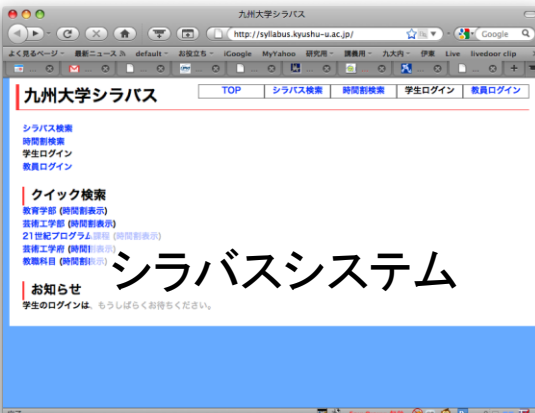
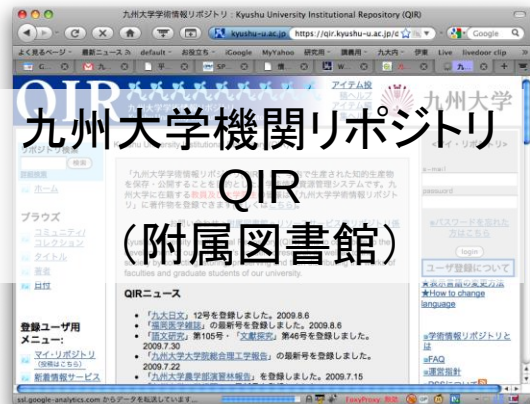
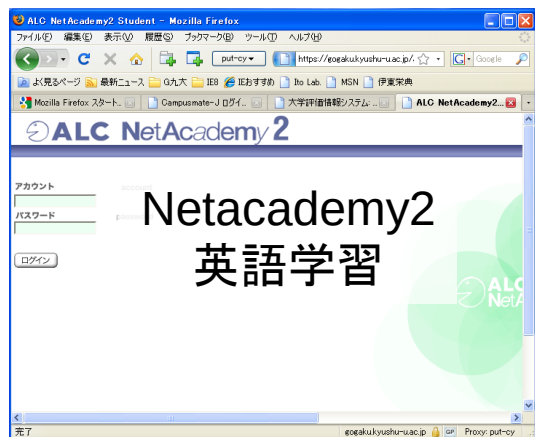
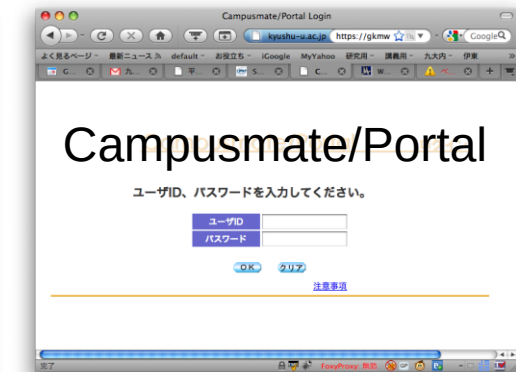
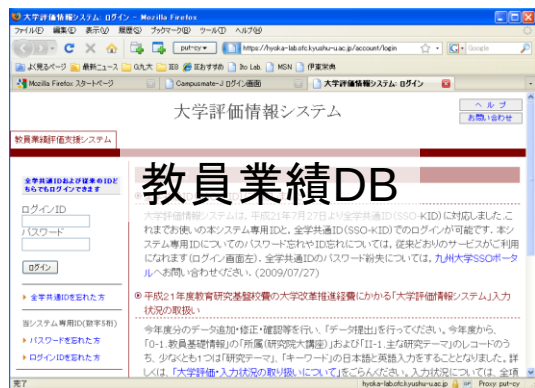
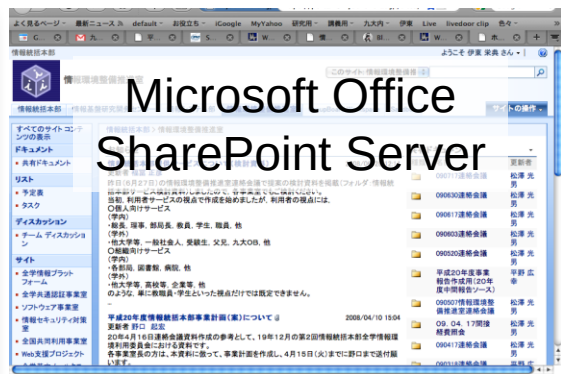
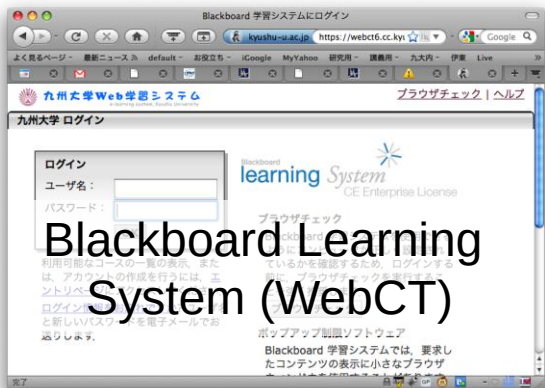
KYUSHU UNIVERSITY

目次

1. はじめに
2. 九州大学 全学共通認証基盤
3. SS0環境の構築
4. Shibboleth SS0
5. UPKI Federation
6. おわりに

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



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 SS0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

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

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)

?

学内無線LAN
kitenet (認証付き)

全学基本メール開始

UPKI開始 UPKI Initiative サーバ証明書

eduroam.jp

GRID

SSO実証実験

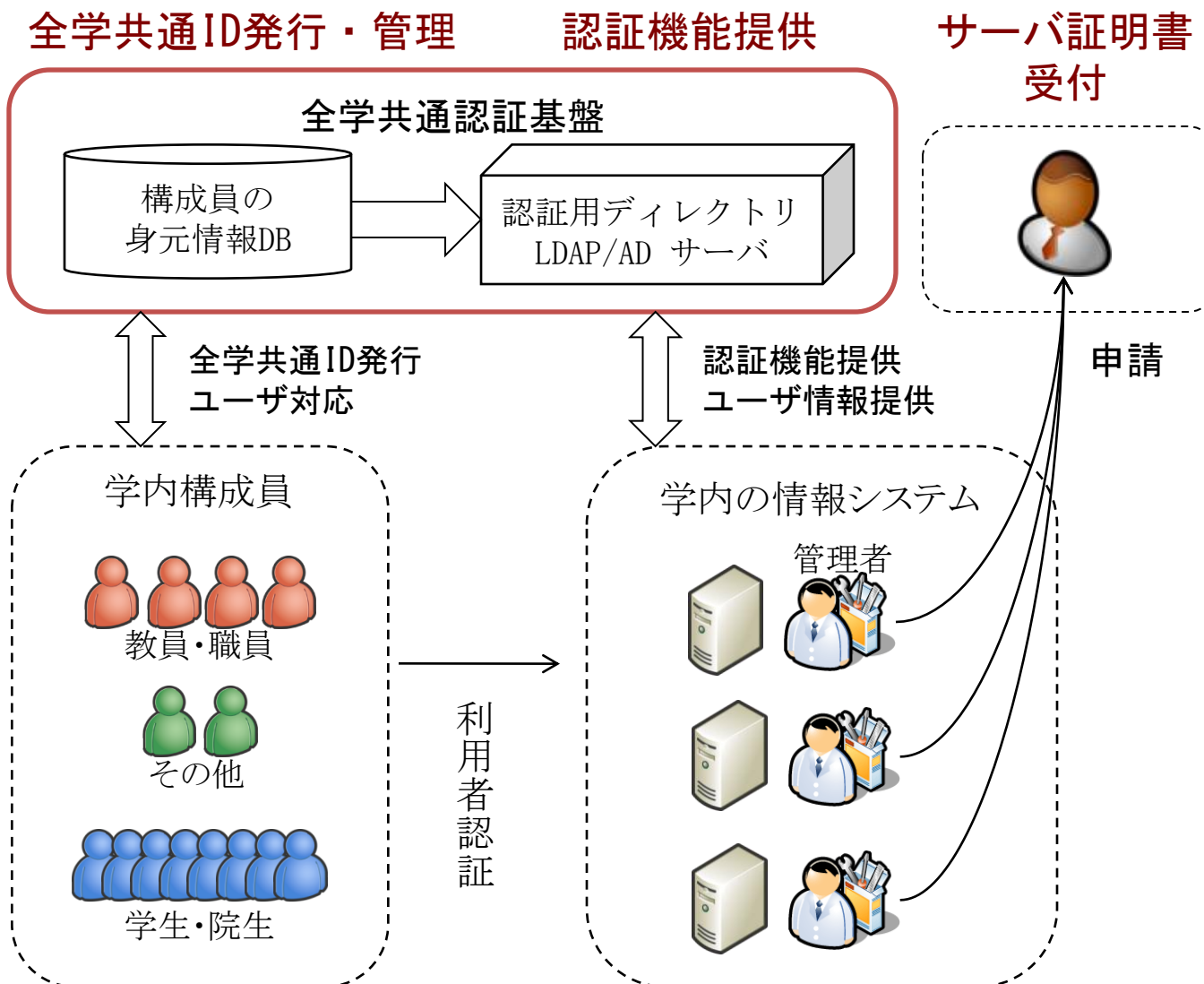
→ UPKI-Fed
試行運用

→ 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

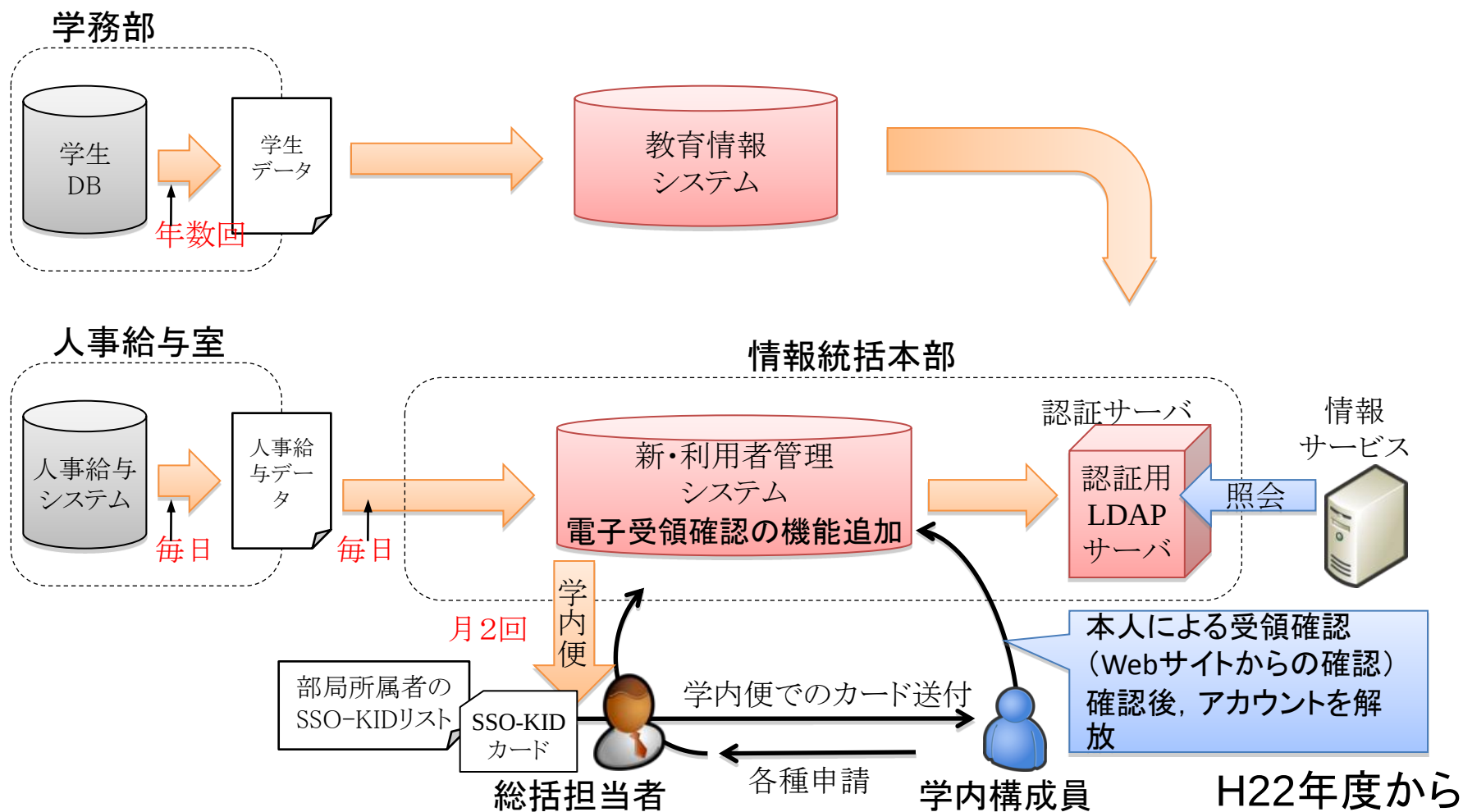
九州大学 全学共通認証基盤



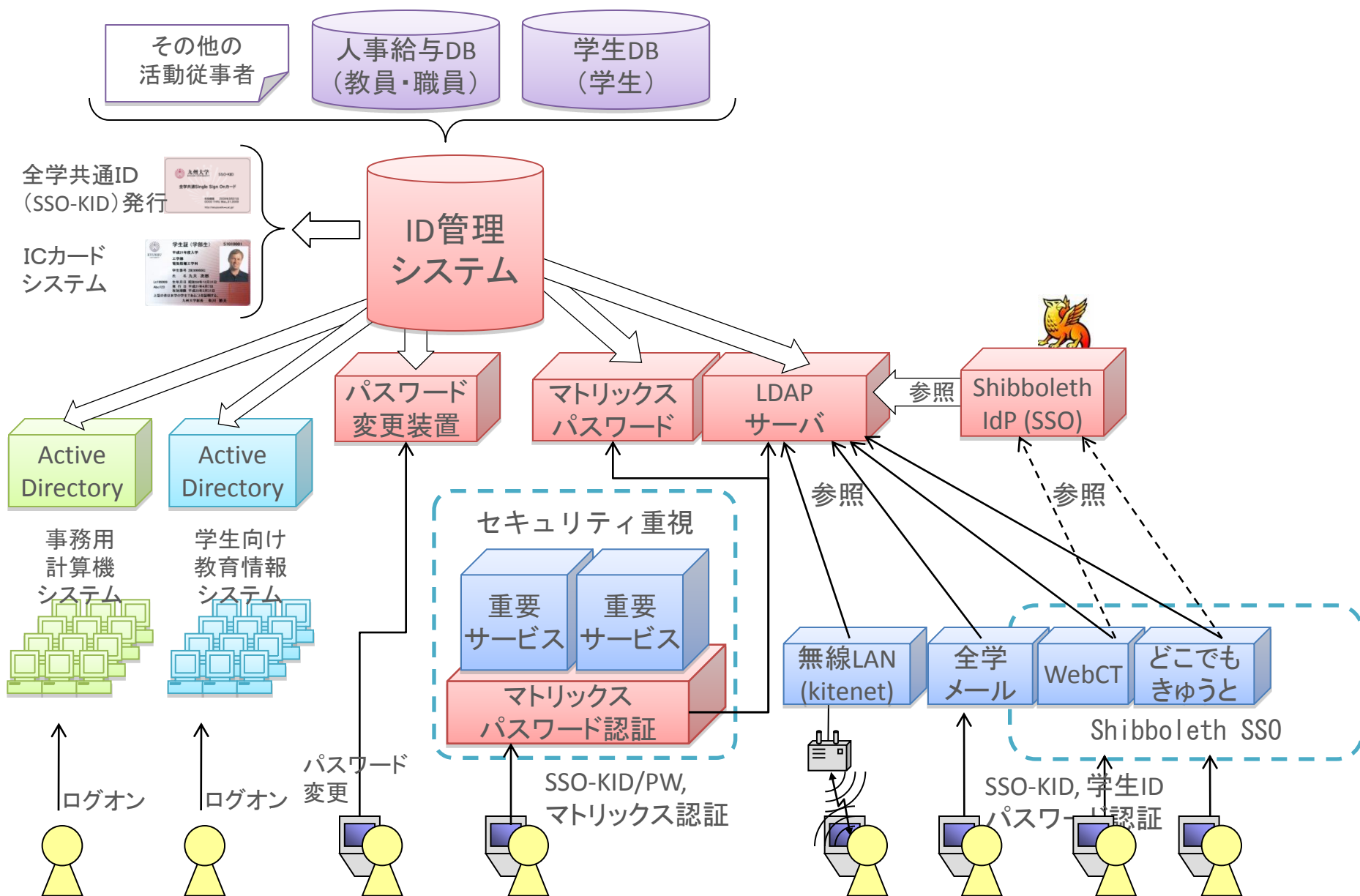
対応サービス

- ▶ 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)



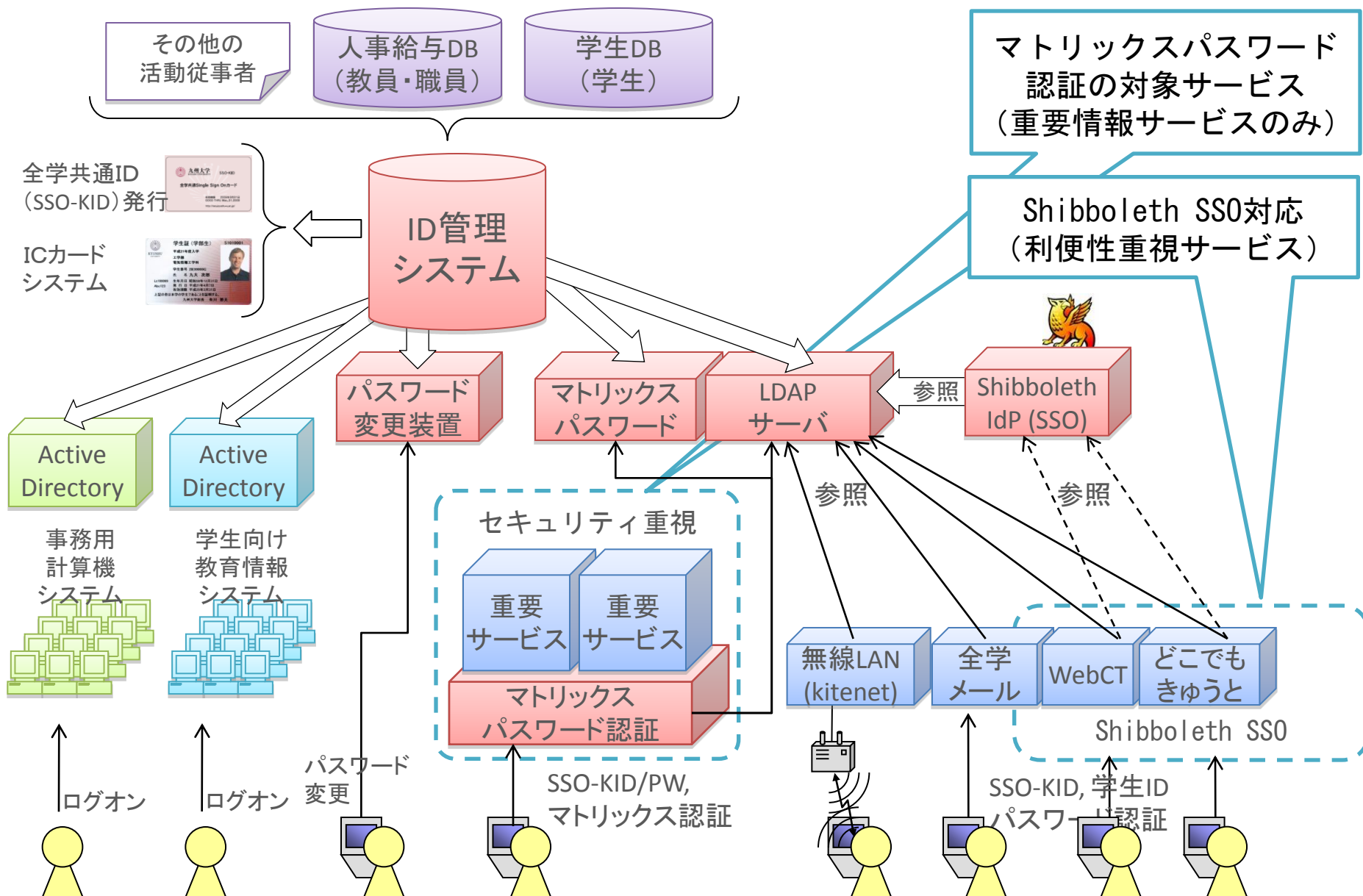
3. SS0環境の構築

- ▶ 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SS0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



連絡先 〒812-8581 福岡市東区箱崎6-10-1 九州大学情報管理室 092-642-3843

SSO-KID 9999999999

	1	2	3	4	5	6	7	8
A	00	11	22	33	44	55	66	77
B	88	99	98	76	54	32	10	98
C	76	54	32	10	98	76	54	32

0123456789

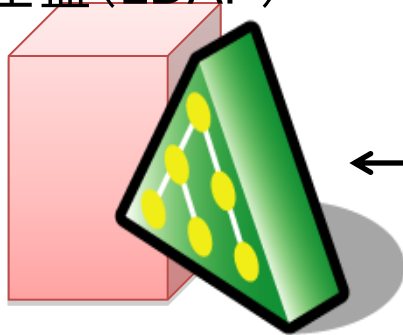
1 この証明書を紛失した場合は、直ちに交付者に届け出なければならない。
2 有効期限が切れた場合、または本学の職員で無くなったときは、直ちに交付者に返付しなければならない。

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

全学共通認証
基盤 (LDAP)



SJSDS
Solaris

LDAP Proxy
(OpenLDAP)

CentOS
属性変換の
ために用意
(使うか未定)

Shibboleth IdP



CentOS
VMware
Windows XP

学内情報サービス



MyLibrary



どこでも
きゅうと
(Ezproxy)



WebCT

**Shibboleth Web
SSO**



九大図書館

<http://www.lib.kyushu-u.ac.jp/>

九州大学附属図書館 Kyushu University Library

九大図書 | 九大eジャーナル | 九大研究者 | 全国図書 | 国内論文 | 海外論文 | 辞書 | サイト |

検索 ツール 学習・研究サポート 申し込み・照会 各館の利用

Headlines 12月からIC職員証へ (利用者票が変わります)

検索ツール

よく使うツール
選択してください

分野別一覧
分野を選択してください

キーワードでツールを探す (Go)

目的別一覧
- 図書・雑誌、電子ジャーナル・ブックを探す
- 雑誌記事を探す・入手する (国内)
- 雑誌記事を探す・入手する (海外)
- ものごとを調べる (事典、辞書、統計...)
- ニュース記事を探す
- 学内コンテンツを探す

学習・研究サポート

活用ツール

MyLibrary はじめて>>
フルテキストの入手
Re - 文献リストの作成
QIR 情報リポジトリ

申し込み・照会

選択してください

開館時間

中央	医学	芸術	工学	伊都	文系合同
8:00-22:00 >>	9:00-21:00 >>	8:30-21:00 >>	8:30-20:00 >>	9:00-21:00 >>	詳細はこちら>>

12/3 (木)

27 伊都 9:00-21:00 >>

文系合同 詳細はこちら>>

MyLibrary

SSO for kyushu University
idp.cc.kyushu-u.ac.jp - idp.cc.kyushu-u.ac.jp

九州大学 Kyushu University SSO system
シングルサインオンシステム

ID

Password

Login

九州大学全学共通ID (SSO-KIDまたは学生ID) でログイン・サインインして下さい。
Please sign-on with your Kyushu University ID (SSO-KID/Student ID).

学生 Students	学生ID/パスワード Student ID/Password
教職員 Faculty members	SSO-KID/パスワード SSO-KID/Password

非正課生 (研究室、聴講生、科目履修生等) の方、全学共通IDを取得できない方は >> [こちら](#)
If you do not have a university ID >> [Try here](#)

IdP

portal.lib.kyushu-u.ac.jp - portal.lib.kyushu-u.ac.jp

伊東 栄典さん
きゅうとMyLibraryへようこそ!

ホーム ヘルプ English ログアウト

ユーザメニュー

ログアウト
ブロック管理

テーマ選択

coral_reef
day_break
default
(7 テーマ)

貸出・予約状況

確認・更新
文献複写・貸借・eDDS
確認・依頼
窓口設定

マイブックシェルフ

貸出履歴一覧
ブックマーク
新着資料案内
登録・確認

開館カレンダー

<<前月 中央図書館 2009年12月 次月>>

日	月	火	水	木	金	土
		1 08:00 - 22:00	2 08:00 - 22:00	3 08:00 - 22:00	4 08:00 - 22:00	5 10:00 - 18:00
6 10:00 - 18:00	7 08:00 - 22:00	8 08:00 - 22:00	9 08:00 - 22:00	10 08:00 - 22:00	11 08:00 - 22:00	12 10:00 - 18:00
13 10:00 - 18:00	14 08:00 - 22:00	15 08:00 - 22:00	16 08:00 - 22:00	17 08:00 - 22:00	18 08:00 - 22:00	19 10:00 - 18:00
20 10:00 - 18:00	21 08:00 - 22:00	22 08:00 - 22:00	23 10:00 - 18:00	24 08:00 - 22:00	25 08:00 - 22:00	26 10:00 - 18:00
27 10:00 - 18:00	28 Closed	29 Closed	30 Closed	31 Closed		

あなたへのお知らせ
とくありません。

貸出資料の返却日です。
予約資料の取置き期限日です。この日を過ぎると、予約資料を受け取ることができません。

SP

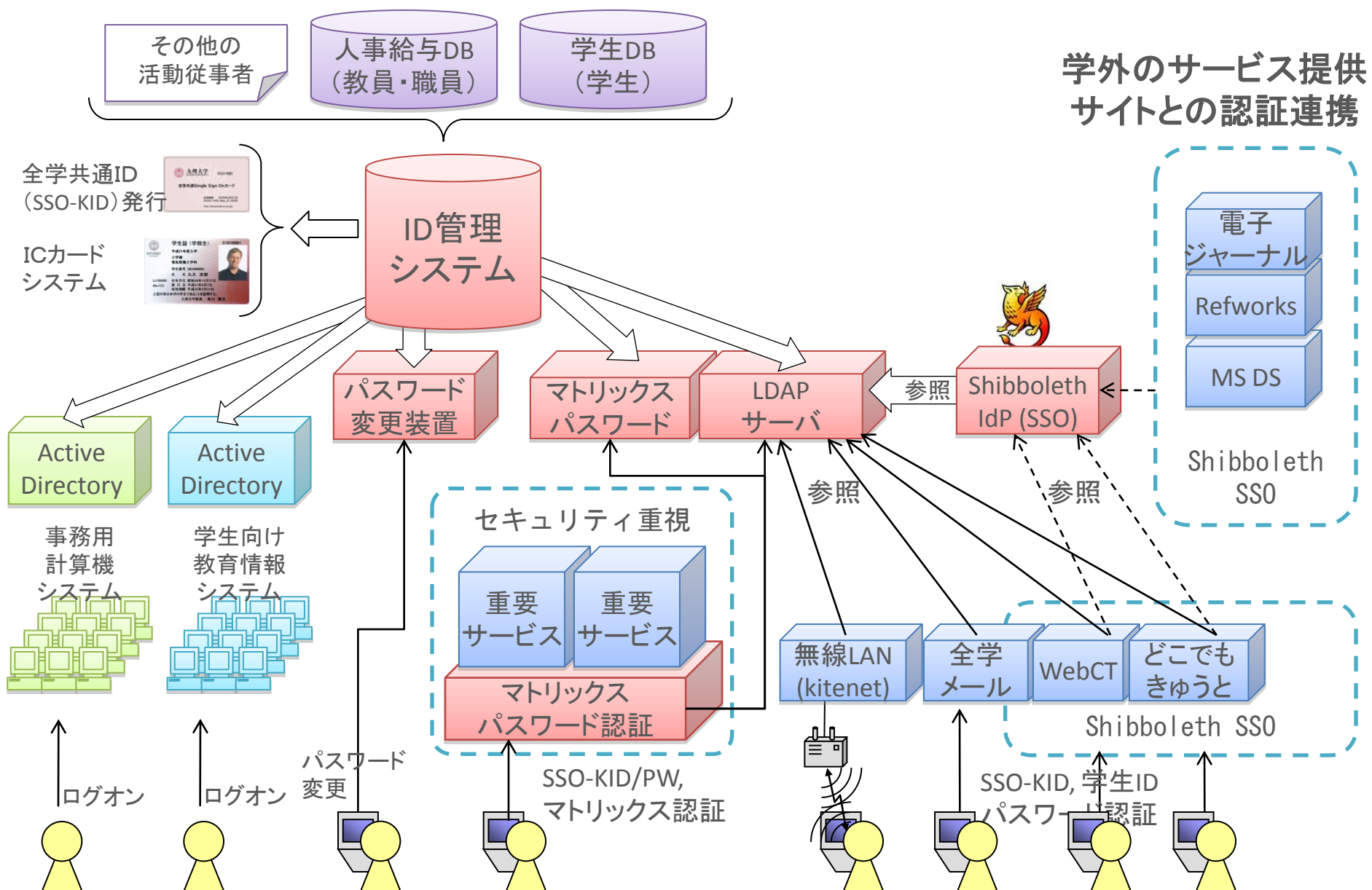
Shibboleth SS0の状況

- ▶ 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