

# 京都工芸繊維大学における利用者原簿 管理基盤の強化と連携サービスの構築

京都工芸繊維大学 情報科学センター

○永井孝幸,山岡裕美,榊田秀夫

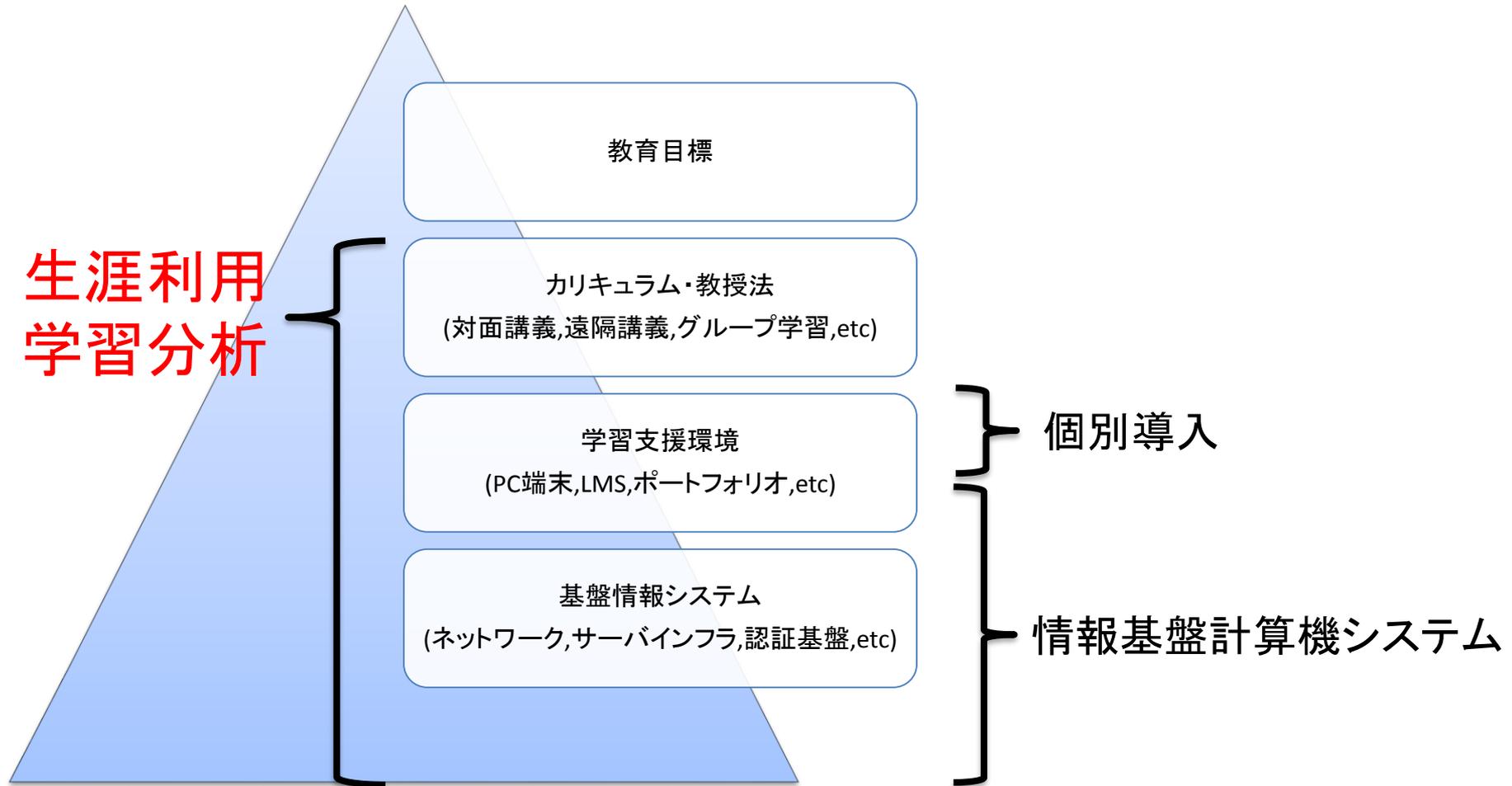
2018/06/16 北海道大学

# 内容

- 2018年3月に全学情報システムリプレース
  - 認証基盤の強化(生涯ID・学認対応)
  - 情報共有サービスの強化(権限管理)
- 前システム(System9)での課題
- 生涯ID対応
- 利用者原簿管理システム(Group+Talent)
- 連携サービス概要

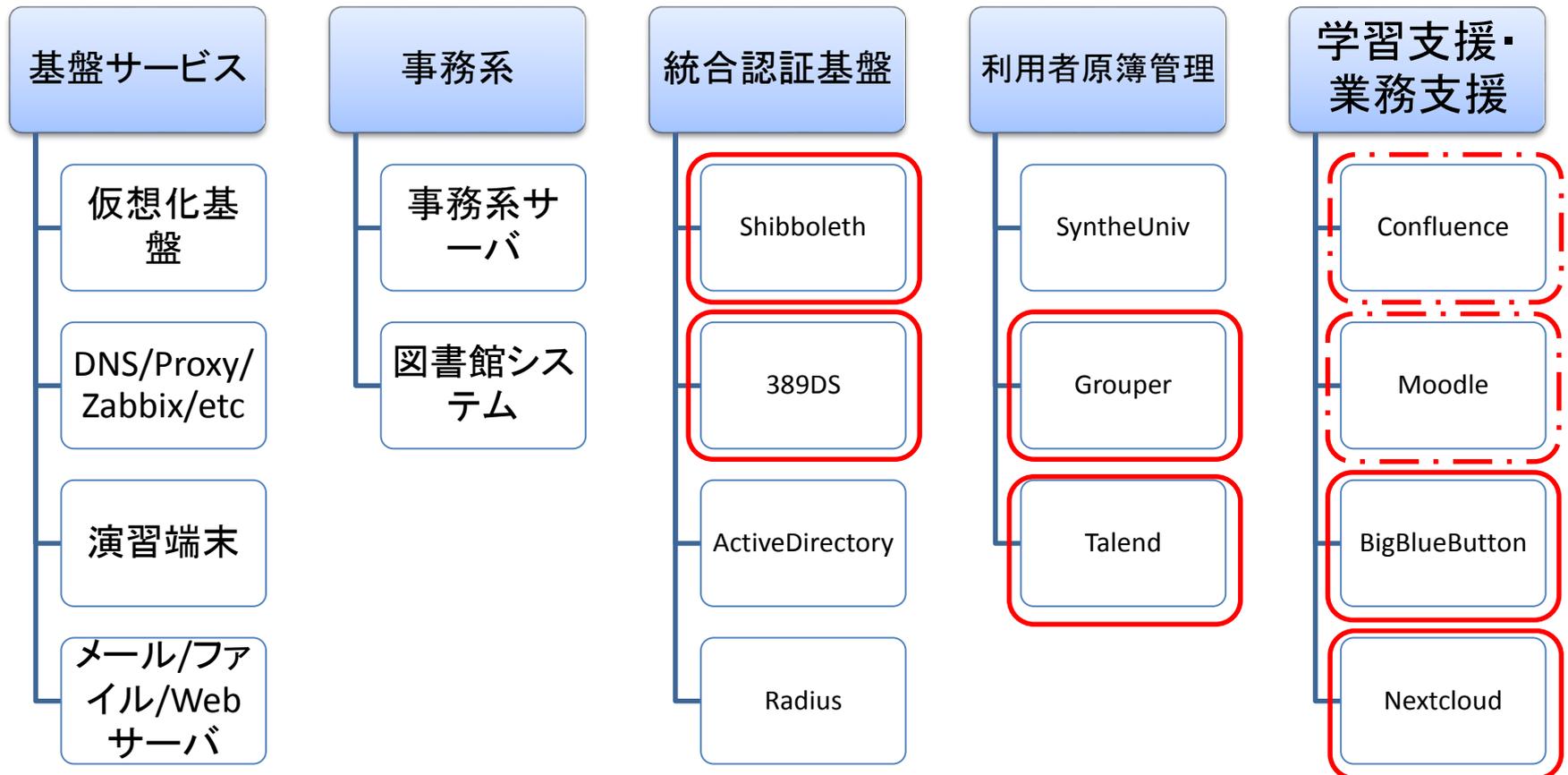


# 学習支援情報システムの観点から



# System10概要

## 導入内容＋構築範囲



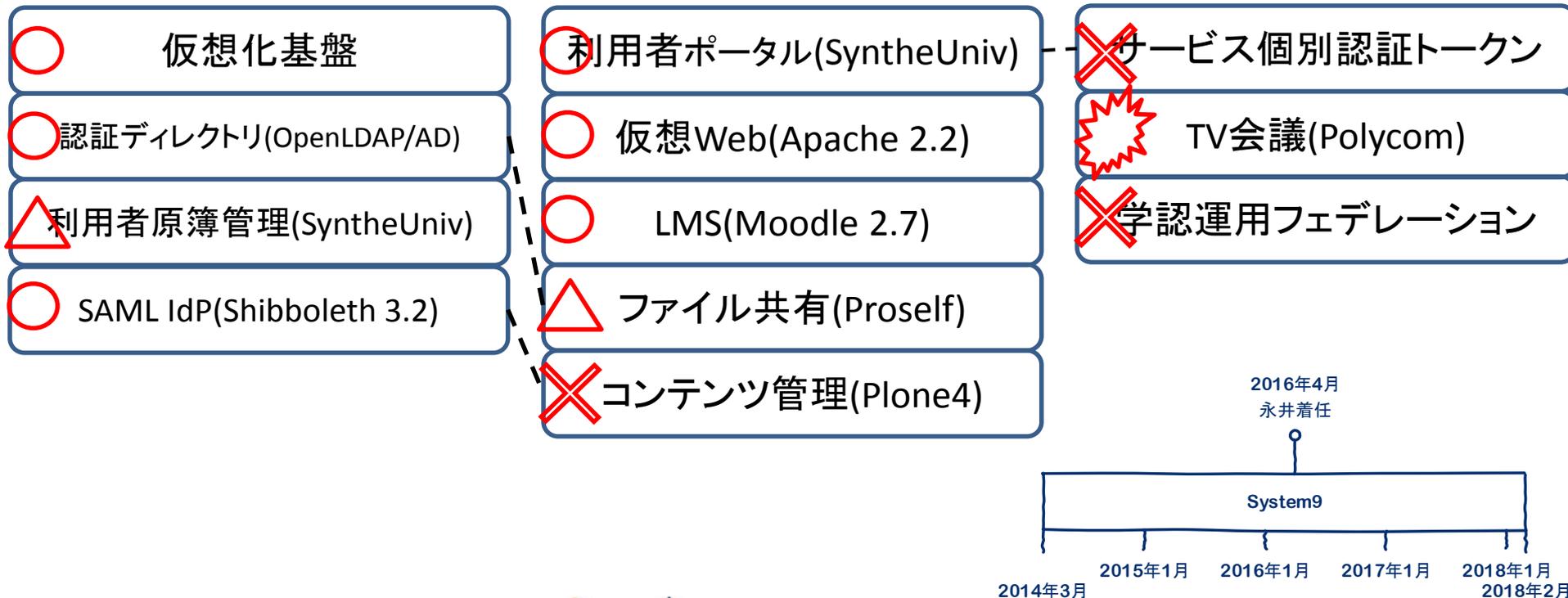
# 仕様検討時点の状況

## System9 + 既存サービス

### 実現サービス

### コアサービス

### 強化サービス



# System10サービス構成

- 実現サービス,情報共有サービスを強化

実現サービス

コアサービス

強化サービス

仮想化基盤

認証ディレクトリ(389DS/AD)

利用者原簿管理(SyntheUniv)

★CAS/SAML IdP(Shibboleth 3.3)

★グループ/資格管理(Grouper 2.3)

★データ連携(Talend)

利用者ポータル(SyntheUniv)

仮想Web(Apache 2.4)

LMS(Moodle 3.1)

ファイル共有(Nextcloud 12)

コンテンツ管理(Confluence)

★Web会議(BigBlueButton)

★生涯ID用LMS(Moodle 3.1)

★全文検索(Solr 6.6)

★学認SP連携

運用設計＝「いつ誰が何をやるか」



# 生涯IDの導入(2016)

- 既存ID: CISアカウント
  - 教職員: 氏名を元に自分で指定
  - 学生: 学生番号から自動附番(ex. b8122001)
    - 10年毎に重複発生 (Moodle運用で問題発生)
- 生涯ID: 工織大パーソナルID
  - ランダムID: u+数字6桁+英字(ex. u123456z)
  - 「生涯メールサービス」用に企画
    - u123456z@univ.kit.ac.jp宛のメールを転送
    - 認証用アカウントとしては配付せず

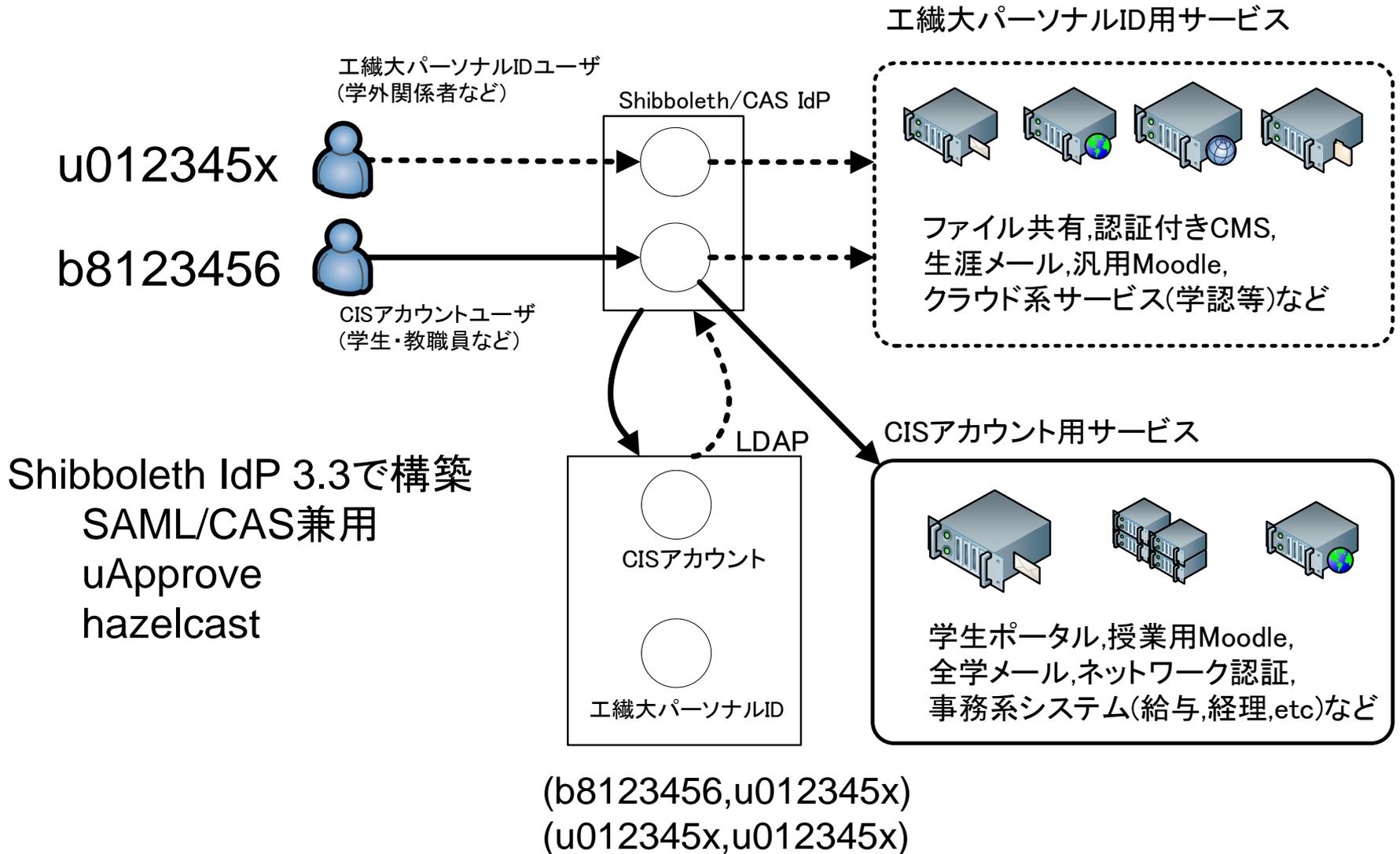


# 生涯ID活用までの道のり

- 名寄せ作業+附番  学認IdP構築で先行作業
  - 内部進学者/科目履修生/教職員
- 認証基盤
  - 既存サービスと生涯IDサービスの共存
- サービス利用資格管理
  - 卒業してもアカウントは消えない(コストモデル修正)
  - 組織構造と独立な区分(非階層的)
- 個人情報保護



# 生涯ID対応IdP



# サービス利用資格管理

- 利用資格グループにユーザを登録

# xxxxxxxx, People, cis.kit.ac.jp

dn: uid=xxxxxxx,ou=People,dc=cis,dc=kit,dc=ac,dc=jp

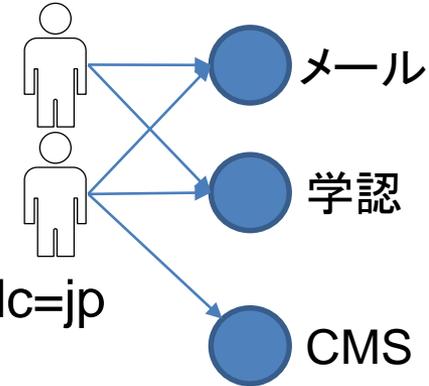
memberOf: cn=kit:user:category:12,ou=Grouper,...

memberOf: cn=service:microsoft:imagine:standard:user,...

memberOf: cn=service:cis:conuence:user,ou=Grouper,...

memberOf: cn=kit:entitlement:cis:service:eduroam,...

memberOf: cn=kit:sig:cis:koho-scommittee,ou=Grouper,...

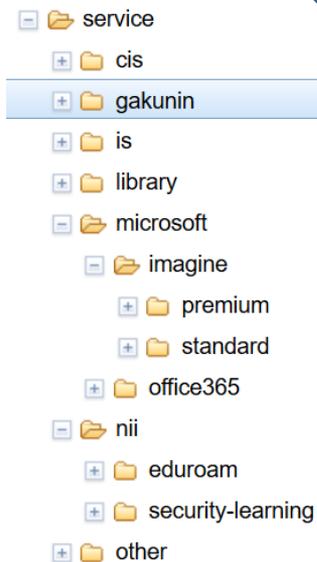


- グループ管理にGrouperを利用

– GUI+DB連携+REST API



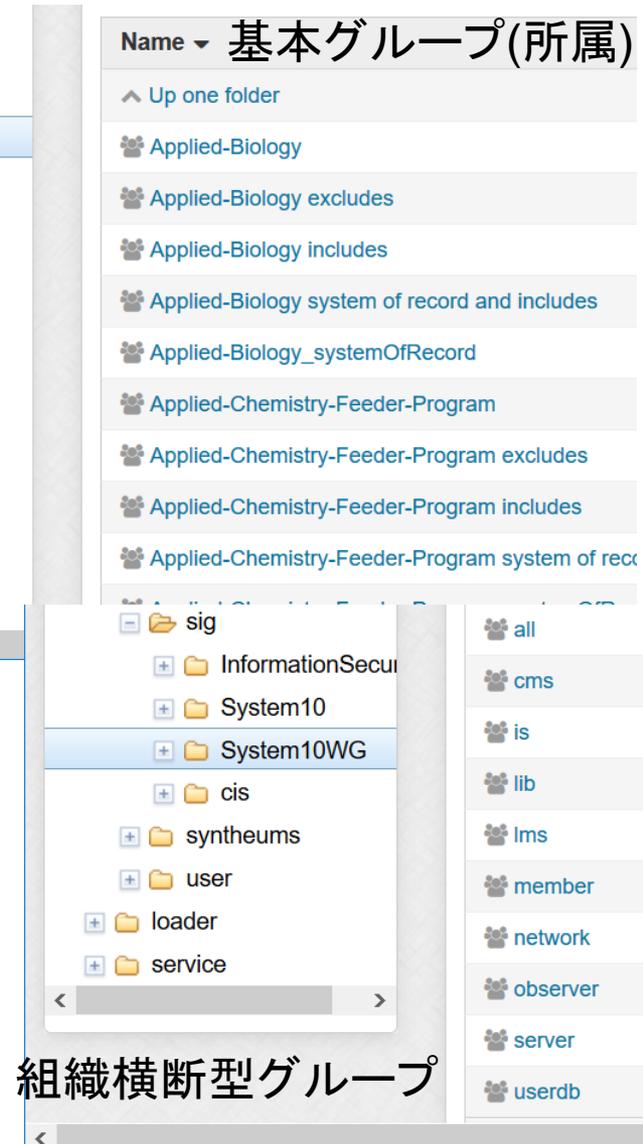
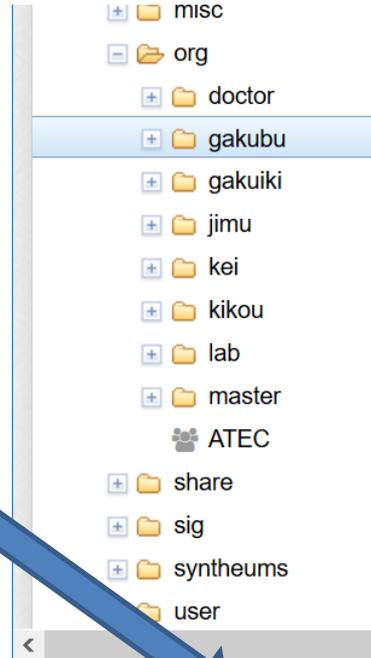
# Grouperを用いたグループ管理



サービス利用資格グループ

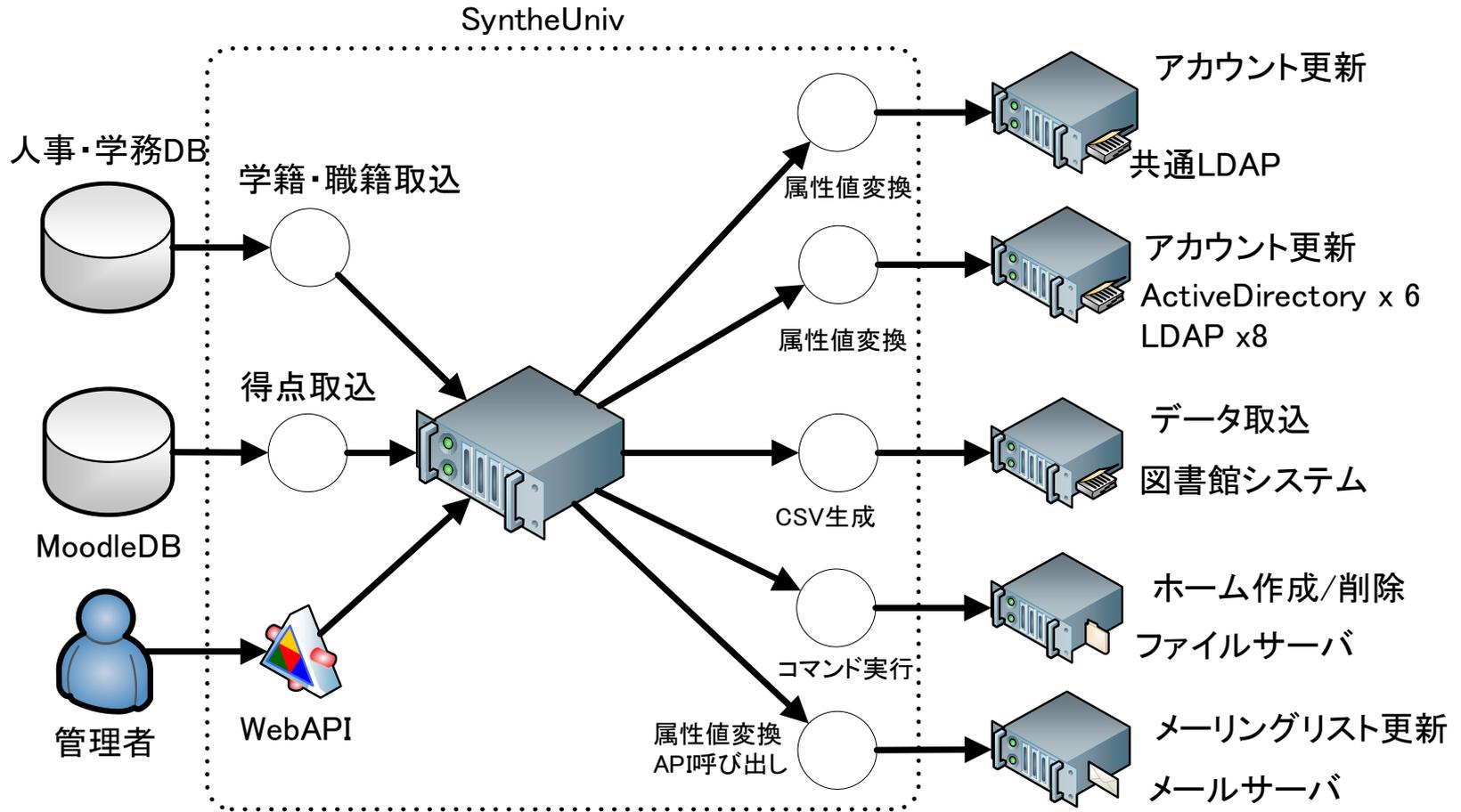


京都工芸繊維大学  
KYOTO INSTITUTE OF TECHNOLOGY



組織横断型グループ

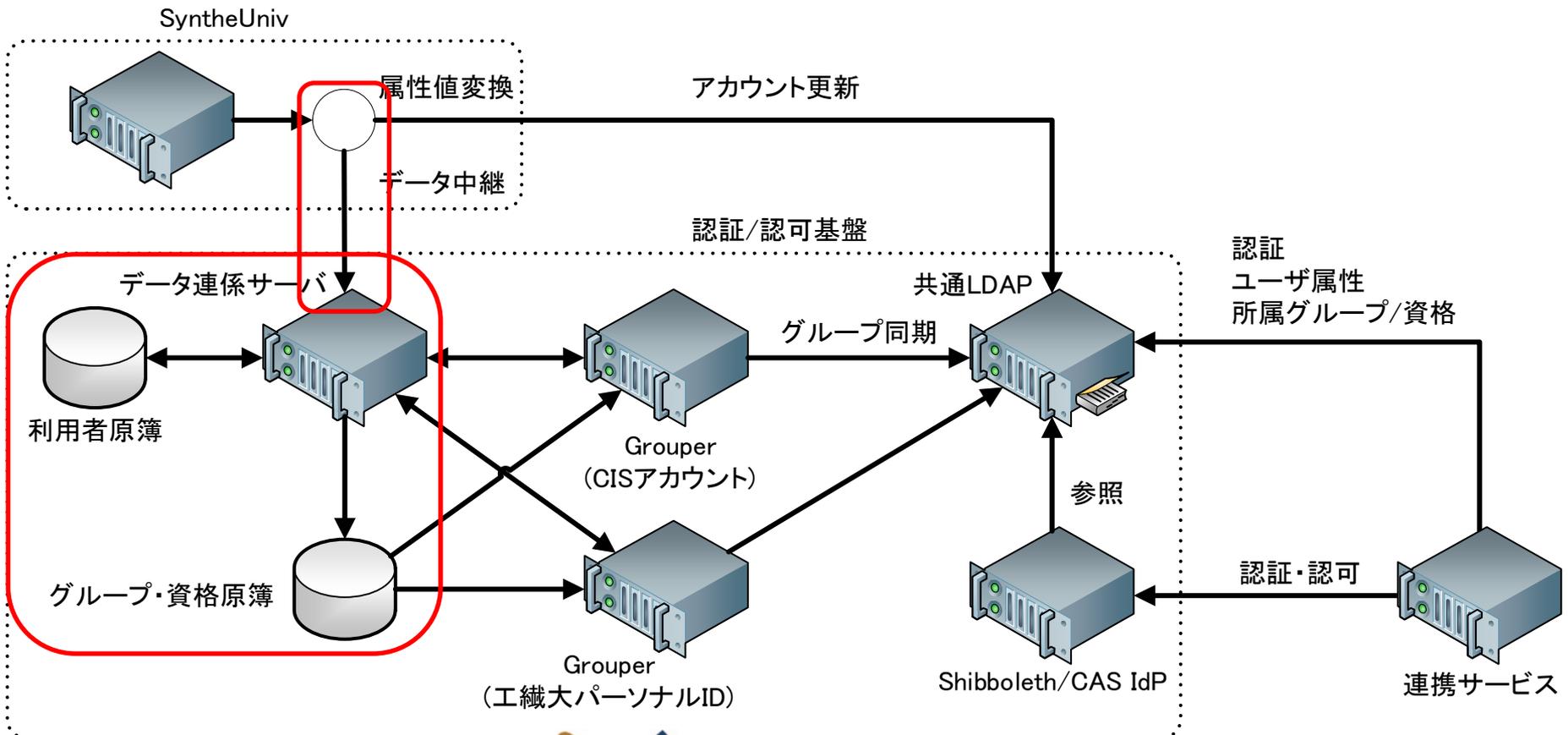
# アカウント情報連携



○ ベンダー独自モジュール(受信側サーバに導入)

# 認証認可基盤構成

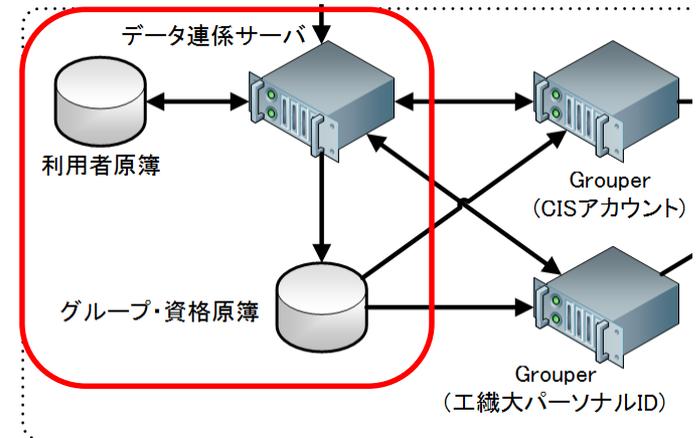
- 開示情報に基づきデータ中継モジュール開発



# データ関係サーバの役割

- 基本グループ原簿の生成

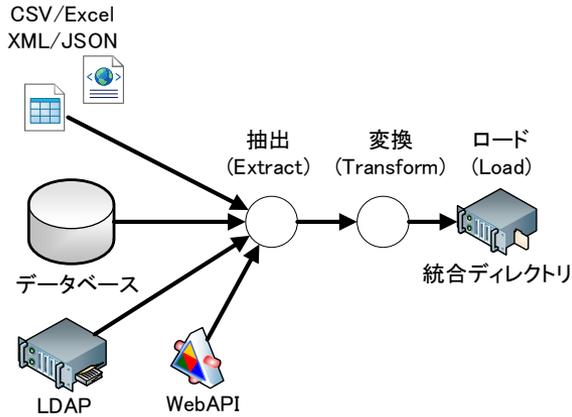
- 職種・学籍別グループ
- 所属別グループ
- 研究室配属済み学生



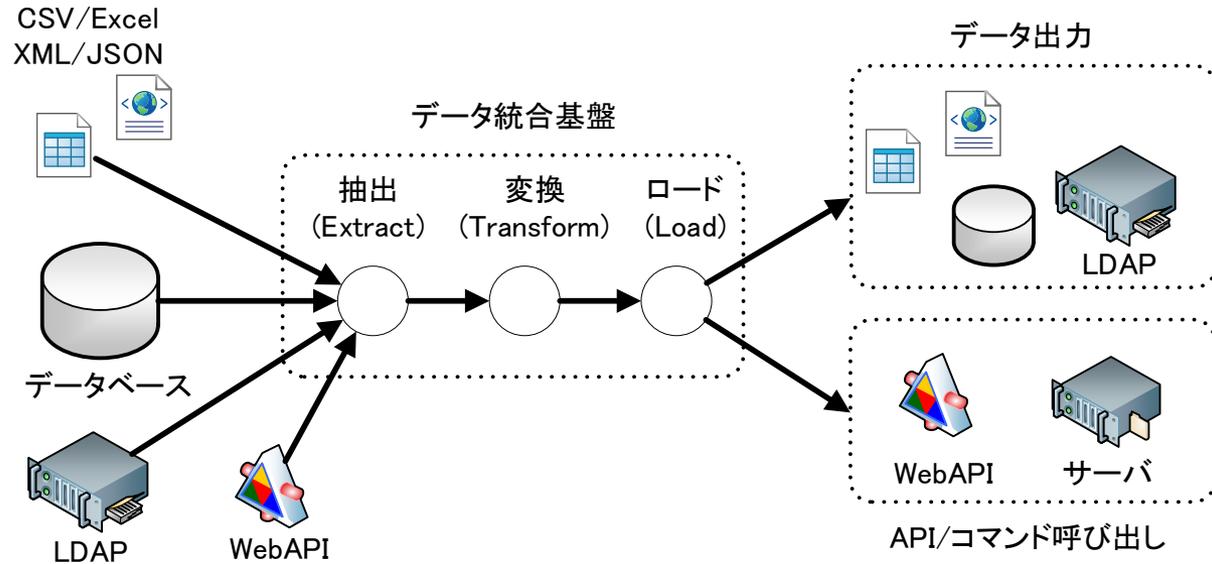
- 工織大パーソナルID用グループ自動生成

- CISアカウント用グループを自動変換
  - ランダムIDで直接メンバー管理するのは厳しい

# データ関係基盤



統合ディレクトリ方式  
(Identity Management系)



データハブ方式  
(ETLツール, データ解析系)

- OpenIdMは両方式対応しているがクローズドに...
  - midPointが同等品(未評価)

# Talendを使ったデータ連携



tPostgresqlConnection\_1

jName  
GID  
groupName  
stemPrefix  
stem  
servicePrefix  
affiliation  
comment

Var



式	Column
row1.servicePrefix	servicePrefix
row1.stem	groupStem
row1.affiliation	affiliation
row1.servicePrefix + ":" + row2.suffix	serviceStem

row2

Property	Value
Lookup Model	一回のロード
Match Model	All Matches
Join Model	Inner Join
Store temp data	false

式キー	Column
row1.affiliation	affiliation
	type
	suffix



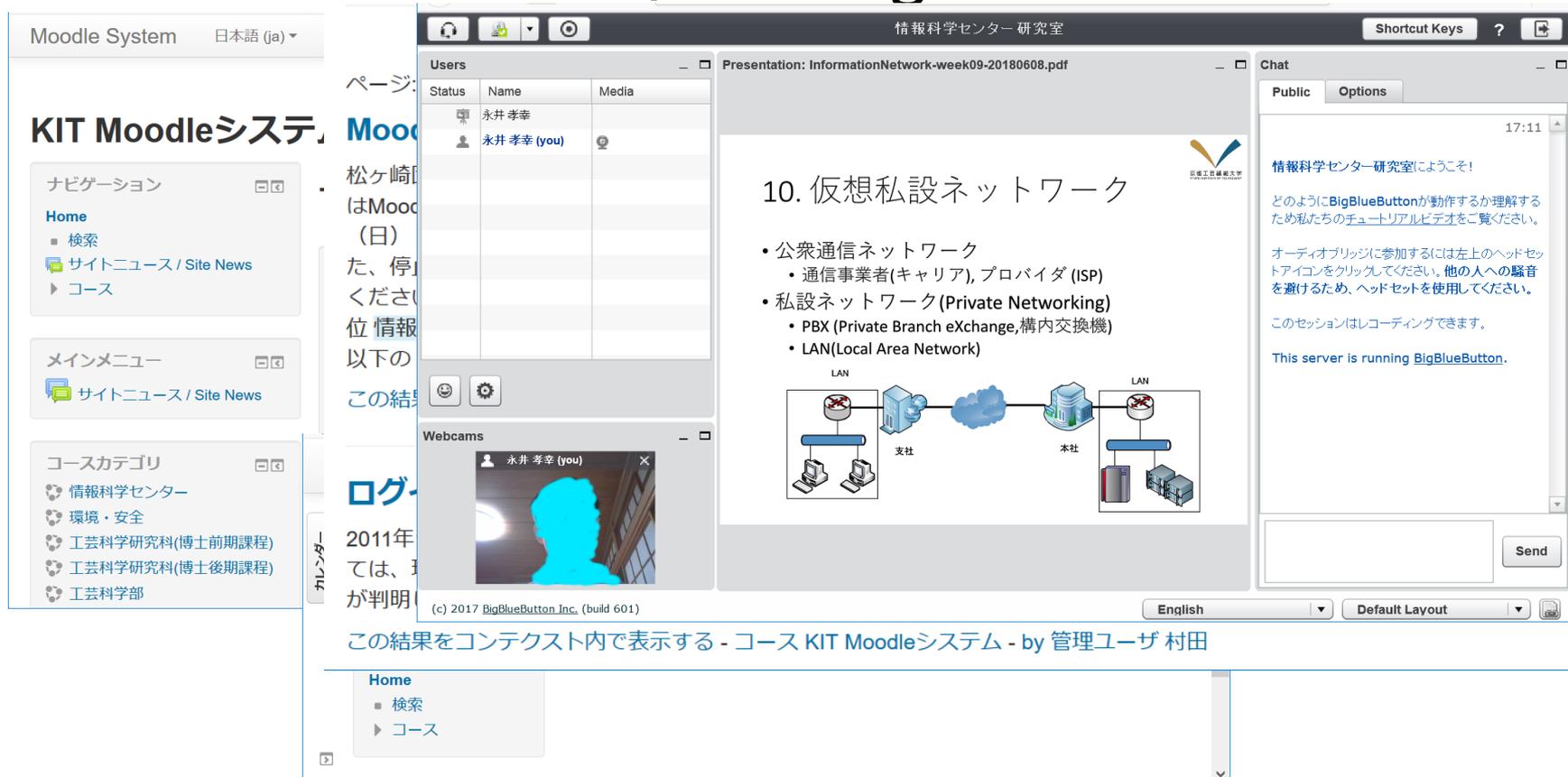
tPostgresqlCommit\_1



tPostgresqlRollback\_1

# Moodle 3.1 LTS

- 生涯ID対応+全文検索+BigBlueButton1.1



Moodle System 日本語 (ja) ▾

KIT Moodleシステム

ナビゲーション

- Home
- 検索
- サイトニュース / Site News
- コース

メインメニュー

- サイトニュース / Site News

コースカテゴリ

- 情報科学センター
- 環境・安全
- 工芸科学研究科(博士前期課程)
- 工芸科学研究科(博士後期課程)
- 工芸科学部

情報科学センター 研究室

Shortcut Keys ?

Users

Status	Name	Media
	永井 孝幸	
	永井 孝幸 (you)	

Webcams

永井 孝幸 (you)

10. 仮想私設ネットワーク

- 公衆通信ネットワーク
  - 通信事業者(キャリア), プロバイダ (ISP)
- 私設ネットワーク (Private Networking)
  - PBX (Private Branch eXchange, 構内交換機)
  - LAN (Local Area Network)

LAN 支社 本社 LAN

この結果をコンテキスト内で表示する - コース KIT Moodleシステム - by 管理ユーザ 村田

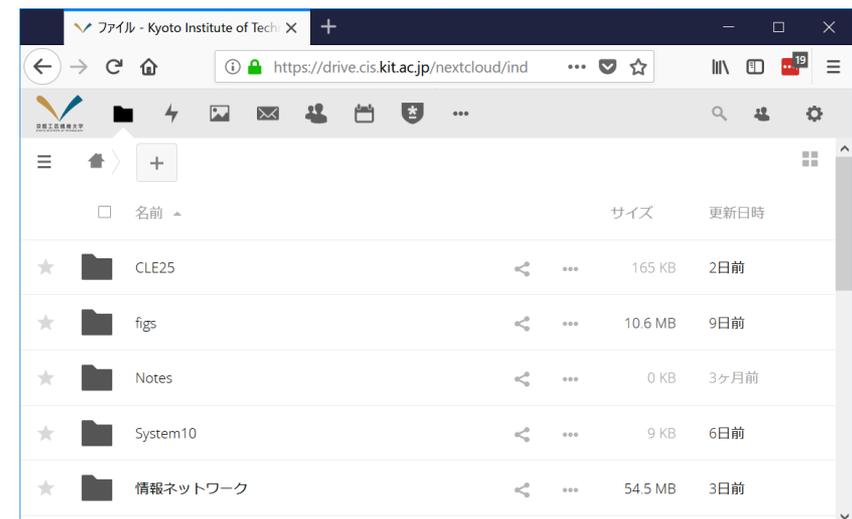
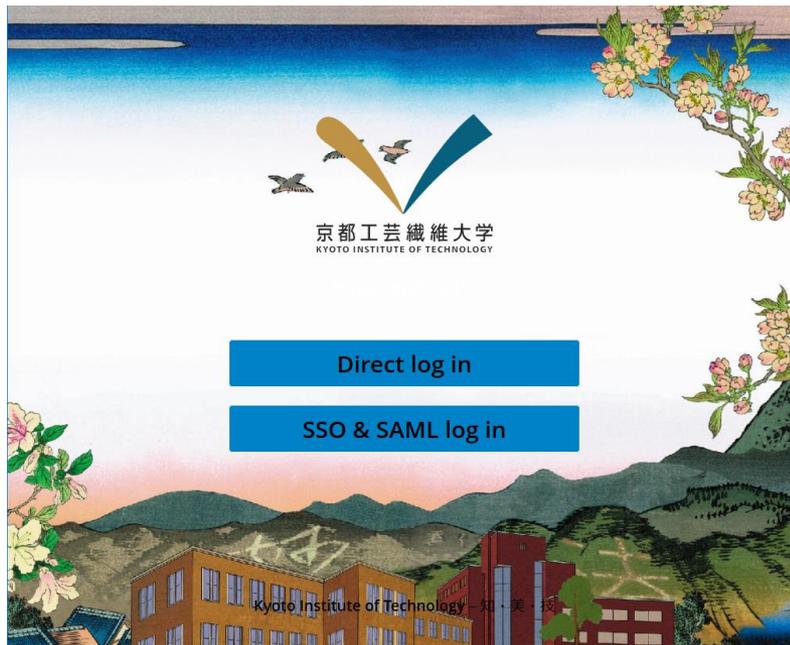
Home

- 検索
- コース

京都工芸繊維大学  
KYOTO INSTITUTE OF TECHNOLOGY

# Nextcloud 12

- SAML認証+生涯ID  
– 全文検索,LDAPグループ連携

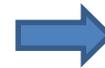


# Confluence 6.4

- 個人識別符号の匿名化
  - 生涯IDは一般ユーザ間では見せたくない



mod\_substituteで対策



Substitute

```
s{"user":{"type":"known",(.*)},"displayName":"(.*?)"|
{"user":{"type":"known",$1},"displayName":"@@hidden@@",
```

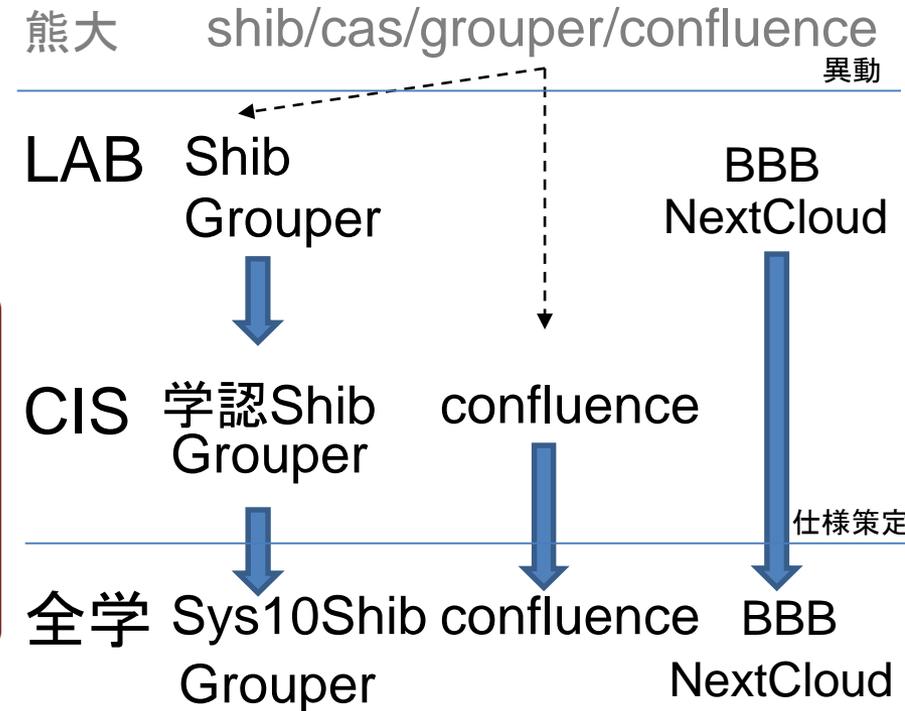
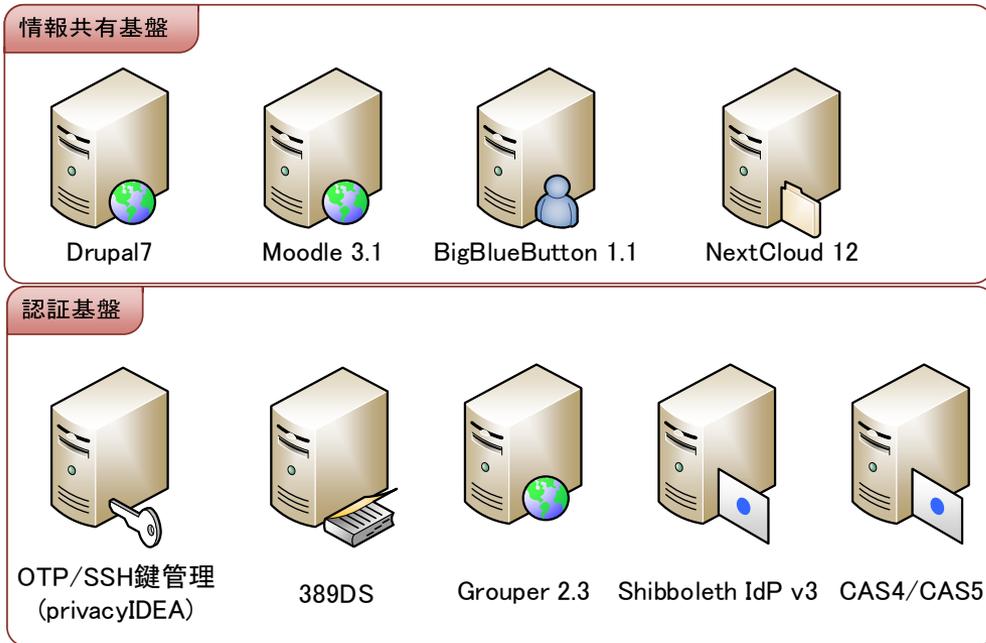
**Tamai Keisuke**



<https://info.cis.kit.ac.jp/wiki/display/~@@hidden@@>

# リスク低減策

- 段階的導入:研究室→センター→全学
- 技術検証環境:KVM/Docker+ansible



# グループウェアによる知識共有

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

名寄せ作業に必要なデータ関係 - x +

<https://confluence.cis.kit.ac.jp/pages/viewpage.action?pageId=7539881>

Confluence スペース ユーザー カレンダー 作成 ...

System10利用者管理システムワーキング

ページ / System10利用者管理システムワーキング

## 名寄せ作業に必要なデータ関係

Nagai Takayuki が作成し、2018/01/05 に Yamaoka Hiromi が最終更新

データ	名寄せに必要な新規項目	想定作業	既存の問題
教務データ	旧学生番号がない学生の連携データについてpersonID項目の追加をお願いしたい	学務課: <ul style="list-style-type: none"> <li>SyntheUMS上で該当学生のpersonIDを特定</li> <li>情報科学センターにpersonID付きデータを送信</li> </ul> 教務DBに新たなカラムが追加できるかどうか確認する必要がある。 情報科学センター: <ul style="list-style-type: none"> <li>学務課の名寄せ作業に必要なSyntheUMS利用権限を設定</li> <li>personIDに基づいて既存アカウントと名寄せ</li> </ul>	旧学生番号がない学生の場合、センターでは名寄せ作業ができない 本人特定に必要な個人情報にアクセスできる学務課にてpersonID特定をお願いしたい 【旧学生番号がないケース】 <ul style="list-style-type: none"> <li>非正規生 → 正規生</li> <li>正規生 → 非正規生</li> <li>科目等履修生については、学務課様にて別帳簿で管理</li> </ul>
人事データ	連携データにpersonID項目の追加をお願いしたい	人事課: <ul style="list-style-type: none"> <li>SyntheUMS上で該当学生のpersonIDを特定</li> <li>情報科学センターにpersonID付</li> </ul>	

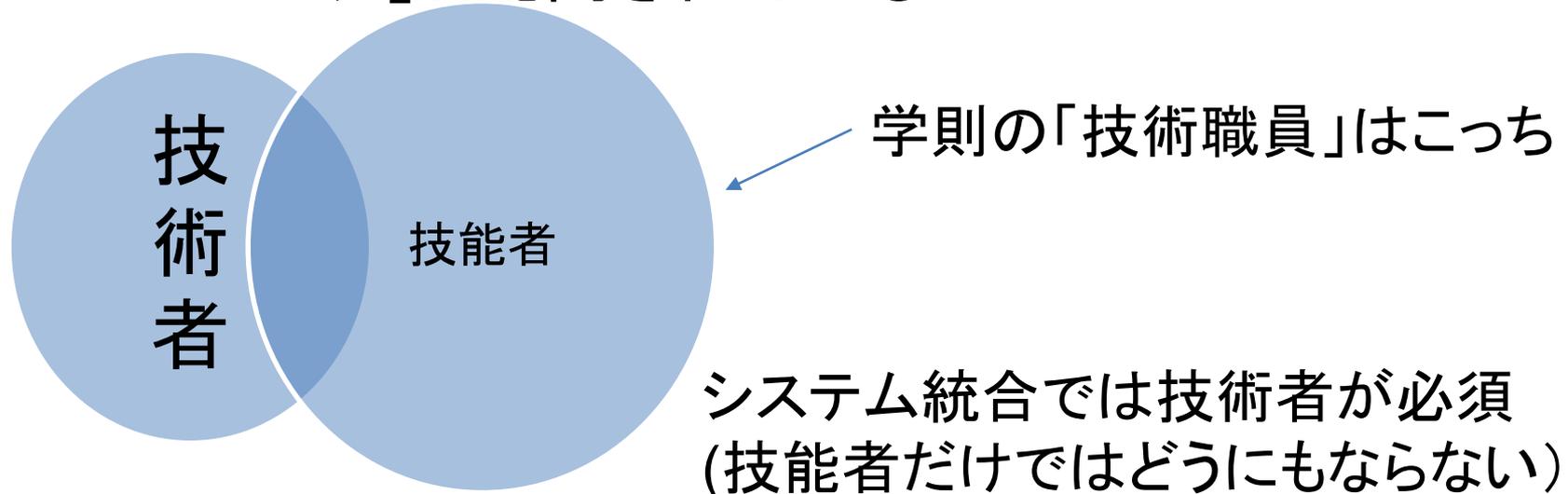
ページ ツリー

- 2017-11-14 ミーティング議事録
- 2017-11-30 ミーティング議事録
- 2017-12-18 ミーティング議事録
- 2018-01-22 ミーティング議事録
- データ関係課題
- ファイル一覧
- ミーティング議事録
- 統一アカウントの属性について
- 統一アカウント新設への対応について

スペース ツール

# 技術者と技能者

- 技術者：解決策を考案する人
  - アーキテクト、デザイナー
- 技能者：既定の作業を行う人
  - 「エンジニア」と混同されている



# 今後の課題

- 汎用ユーザポータル
- 多要素認証対応
- クラウド・コンテナ技術の活用
- 個人情報保護対応
  - GDPR対応まで必要？
- 調達方法の見直し
  - 一括更新はリスクと釣り合っているか？



# まとめ

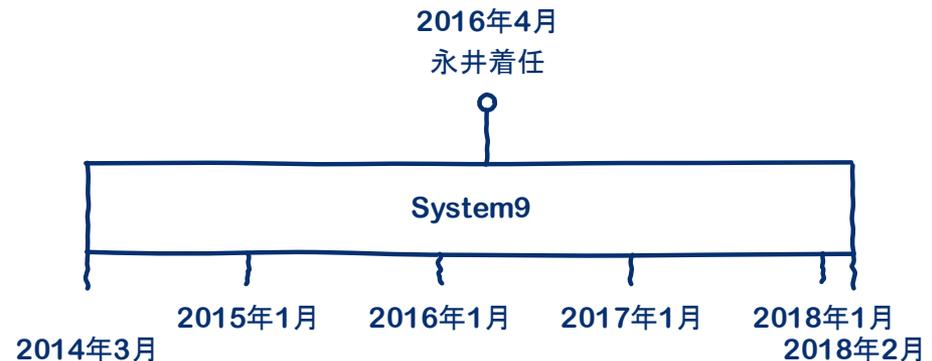
- システム導入≠サービス構築
  - コアサービス+実現サービス+運用設計
- 生涯IDの導入
  - 権限管理,データ関係基盤強化
- オープンソースの活用
  - 技術検証の先取り
  - リスク低減策(品質保証のコスト)



# 前提知識

- システム調達是一般競争入札方式
  - (例外を除き)特定製品の指名買いは出来ない
    - オープンソース製品は仕様に明記してもOK
  - 仕様充足審査+「評価ポイント/価格」で比較
- 情報科学センタースタッフ構成

区分	人数(外部出身)
専任教員	3 (3)
技術職員	6 (4)



# システム更新補足資料

## • 全体スケジュール



官報 号外政府調達第227号 平成29年12月1日

落札日 2017年10月13日

落札者 日本電気株式会社

落札価格 10,202,760円

