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

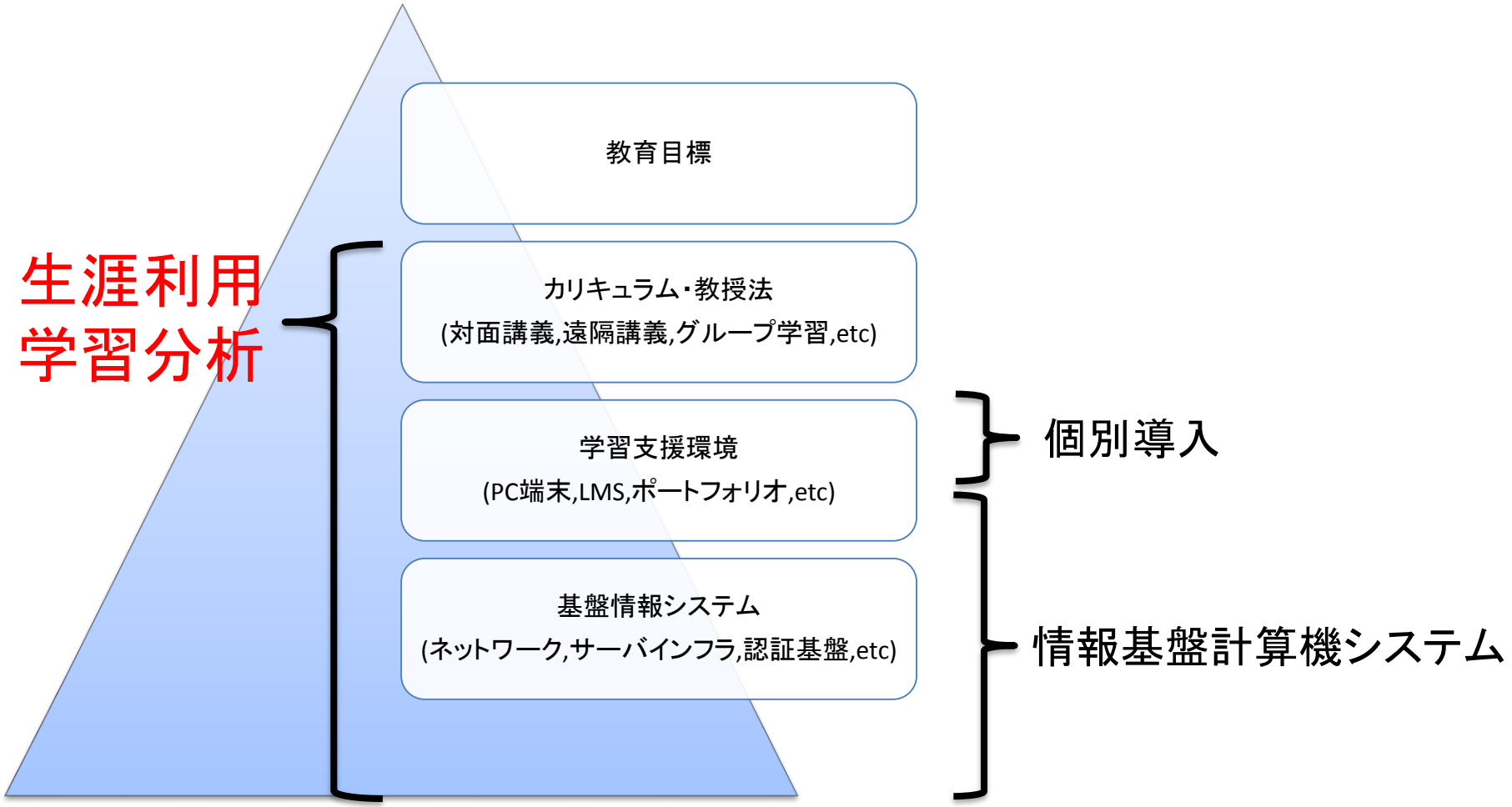
京都工芸繊維大学 情報科学センター
〇永井孝幸,山岡裕美,桝田秀夫

2018/06/16 北海道大学

内容

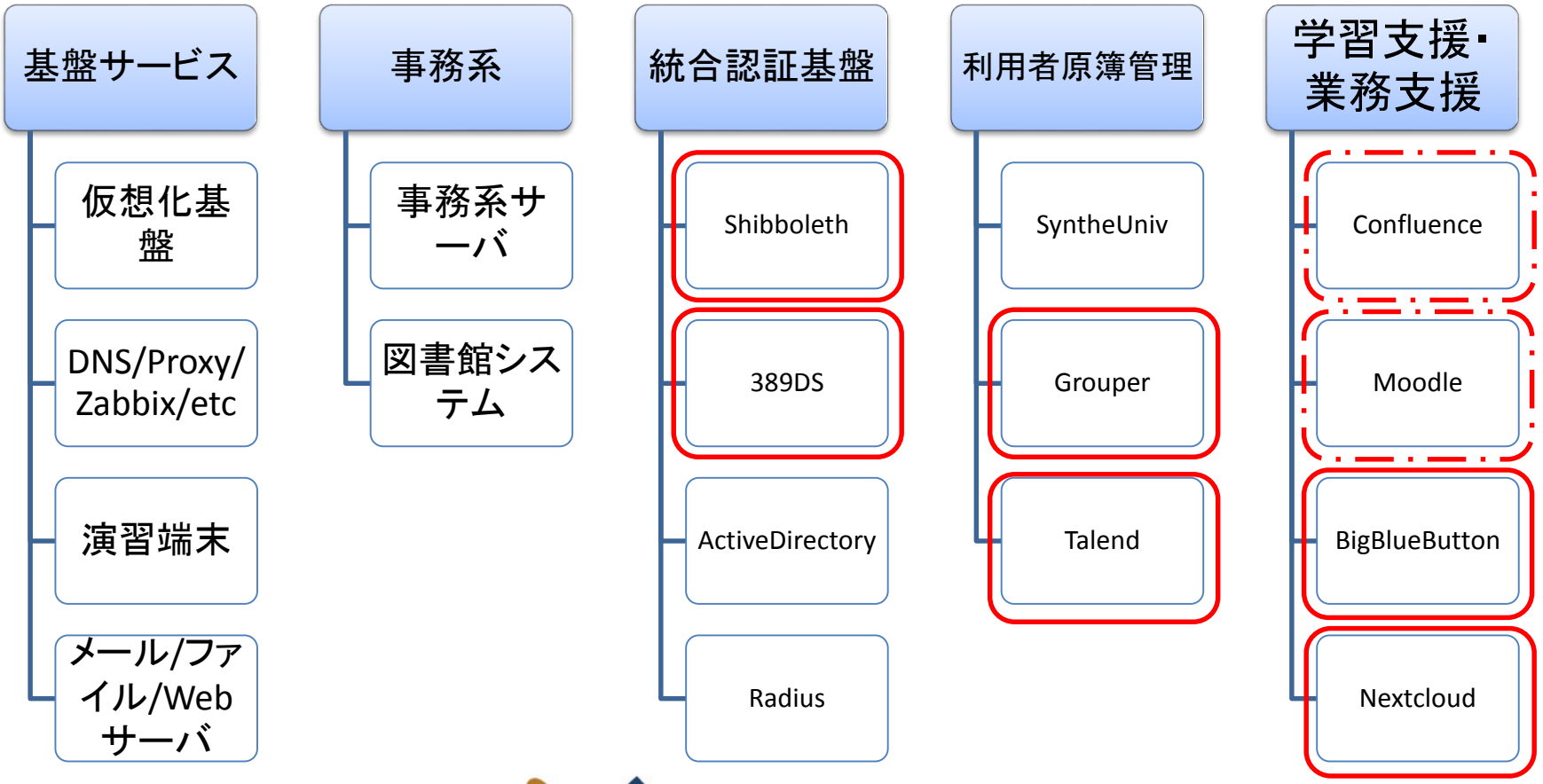
- 2018年3月に全学情報システムリプレース
  - 認証基盤の強化(生涯ID・学認対応)
  - 情報共有サービスの強化(権限管理)
- 前システム(System9)での課題
- 生涯ID対応
- 利用者原簿管理システム(Grouper+Talend)
- 連携サービス概要

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

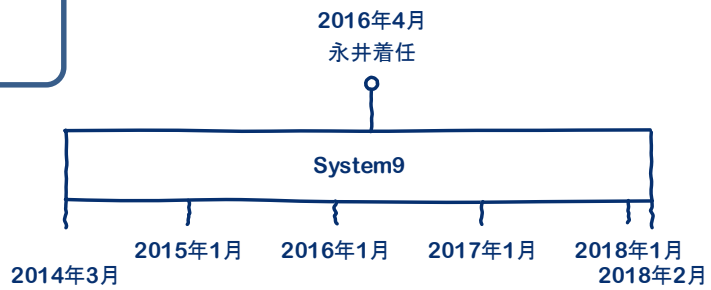


京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY

仕様検討時点の状況

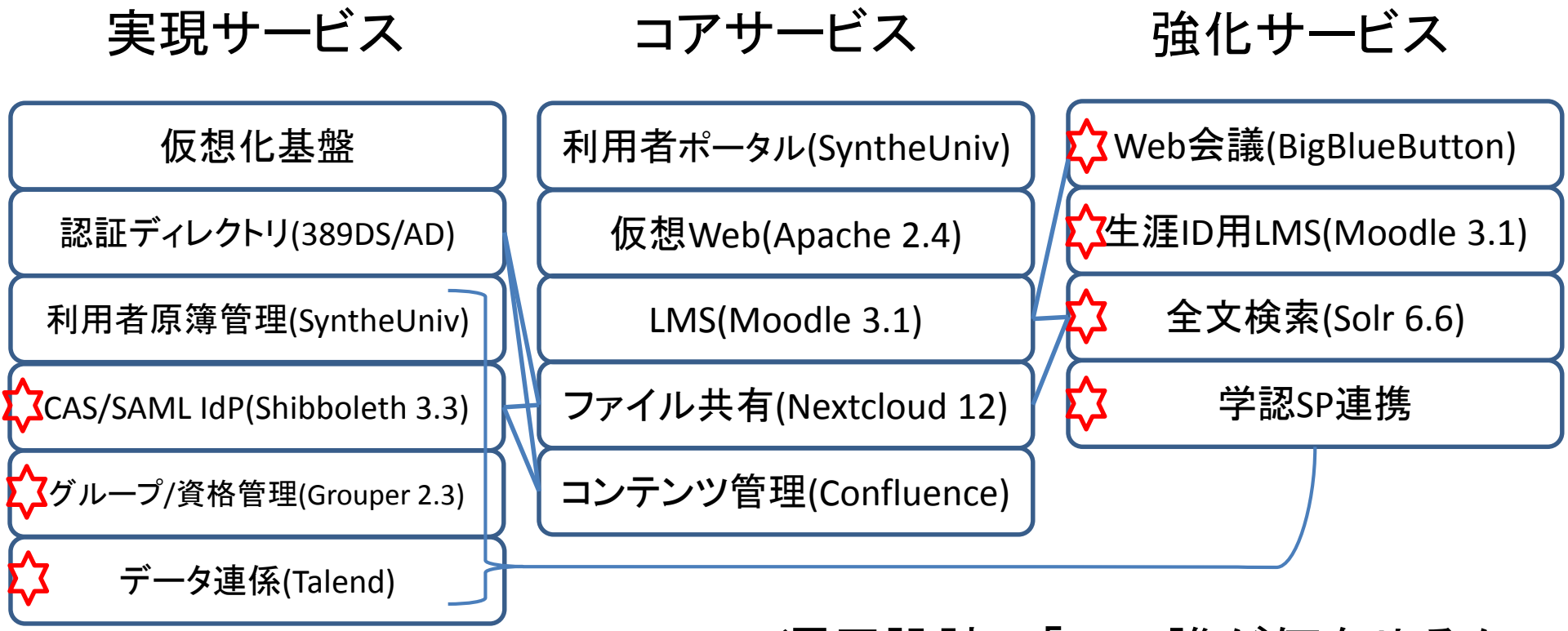
- System9 + 既存サービス

実現サービス	コアサービス	強化サービス
○ 仮想化基盤	○ 利用者ポータル(SyntheUniv)	× サービス個別認証トークン
○ 認証ディレクトリ(OpenLDAP/AD)	○ 仮想Web(Apache 2.2)	✸ TV会議(Polycom)
△ 利用者原簿管理(SyntheUniv)	○ LMS(Moodle 2.7)	× 学認運用フェデレーション
○ SAML IdP(Shibboleth 3.2)	△ ファイル共有(Proself)	
	× コンテンツ管理(Plone4)	



System10サービス構成

- 実現サービス,情報共有サービスを強化



運用設計＝「いつ誰が何をやるか」

京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY

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：工繊大パーソナル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

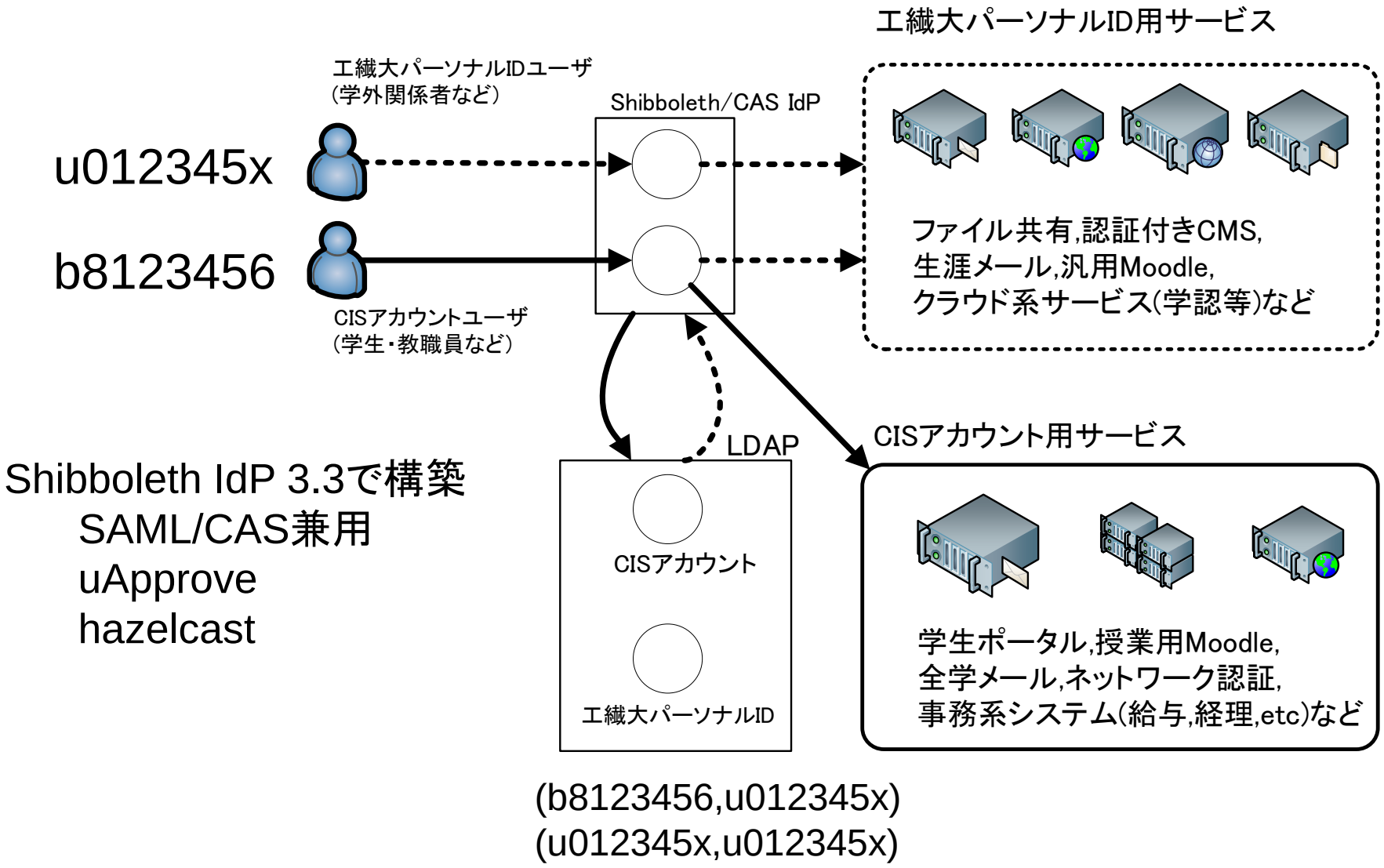
京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY

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

京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY

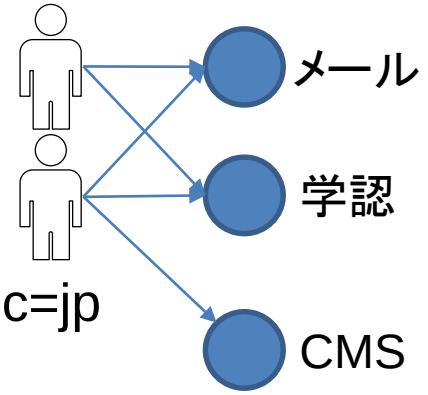
生涯ID対応IdP



Shibboleth IdP 3.3で構築
- SAML/CAS兼用
- uApprove
- hazelcast

(b8123456,u012345x)
(u012345x,u012345x)

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

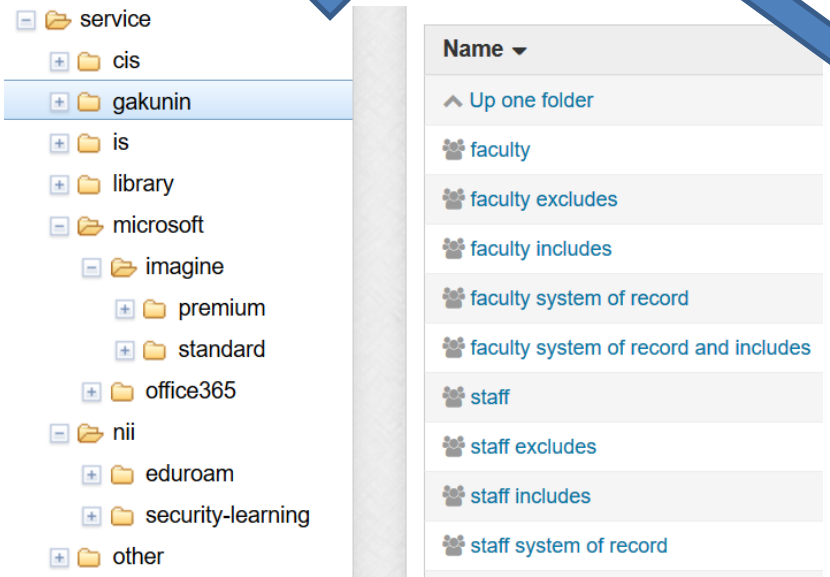
```
# xxxxxxxx, People, cis.kit.ac.jp
dn: uid=xxxxxxxx,ou=People,dc=cis,dc=kit,dc=ac,dc=jp
memberOf: cn=kit:user:category:12,ou=Grouper,...
memberOf: cn=service:microsoft:imagine:standard:user,...
memberOf: cn=service:cis:conuence:user,ou=Grouper,...
memberOf: cn=kit:entitlement:cis:service:eduroam,...
memberOf: cn=kit:sig:cis:koho-scommittee,ou=Grouper,...
```

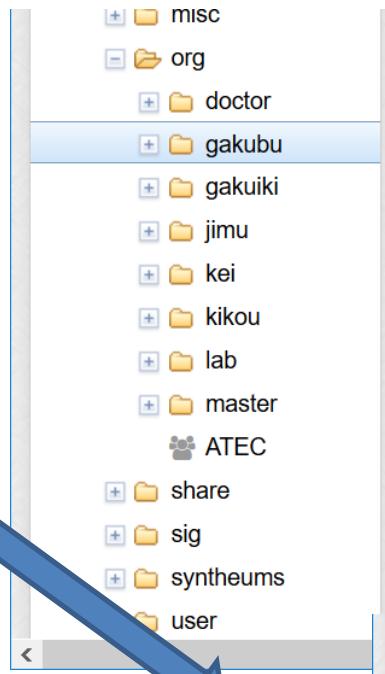
- グループ管理にGrouperを利用
  - GUI+DB連携+REST API

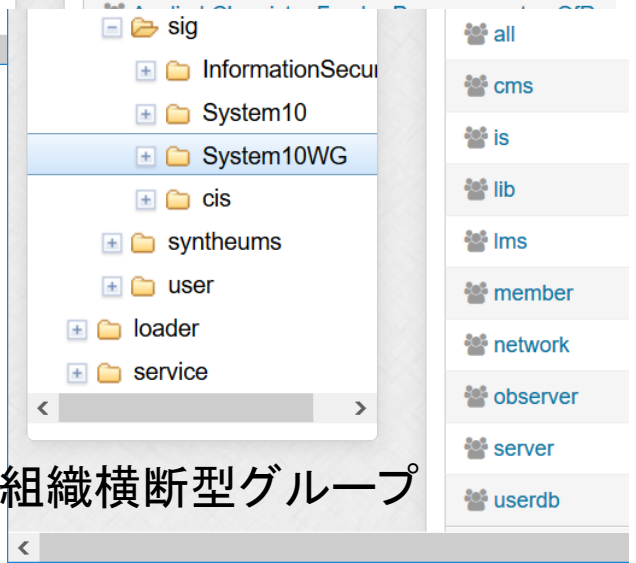
Grouper™

京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY

Grouperを用いたグループ管理





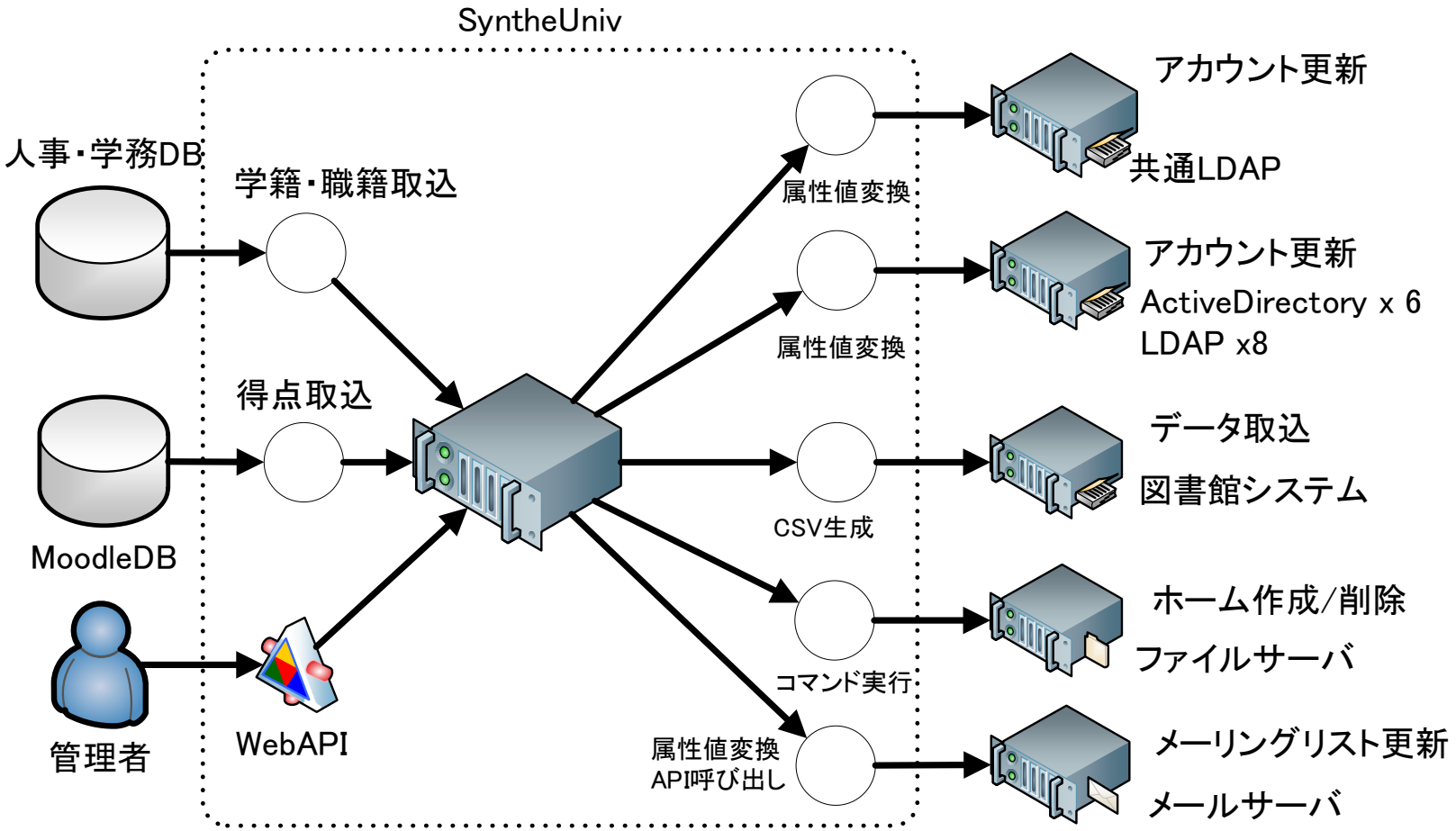


サービス利用資格グループ

京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY

組織横断型グループ

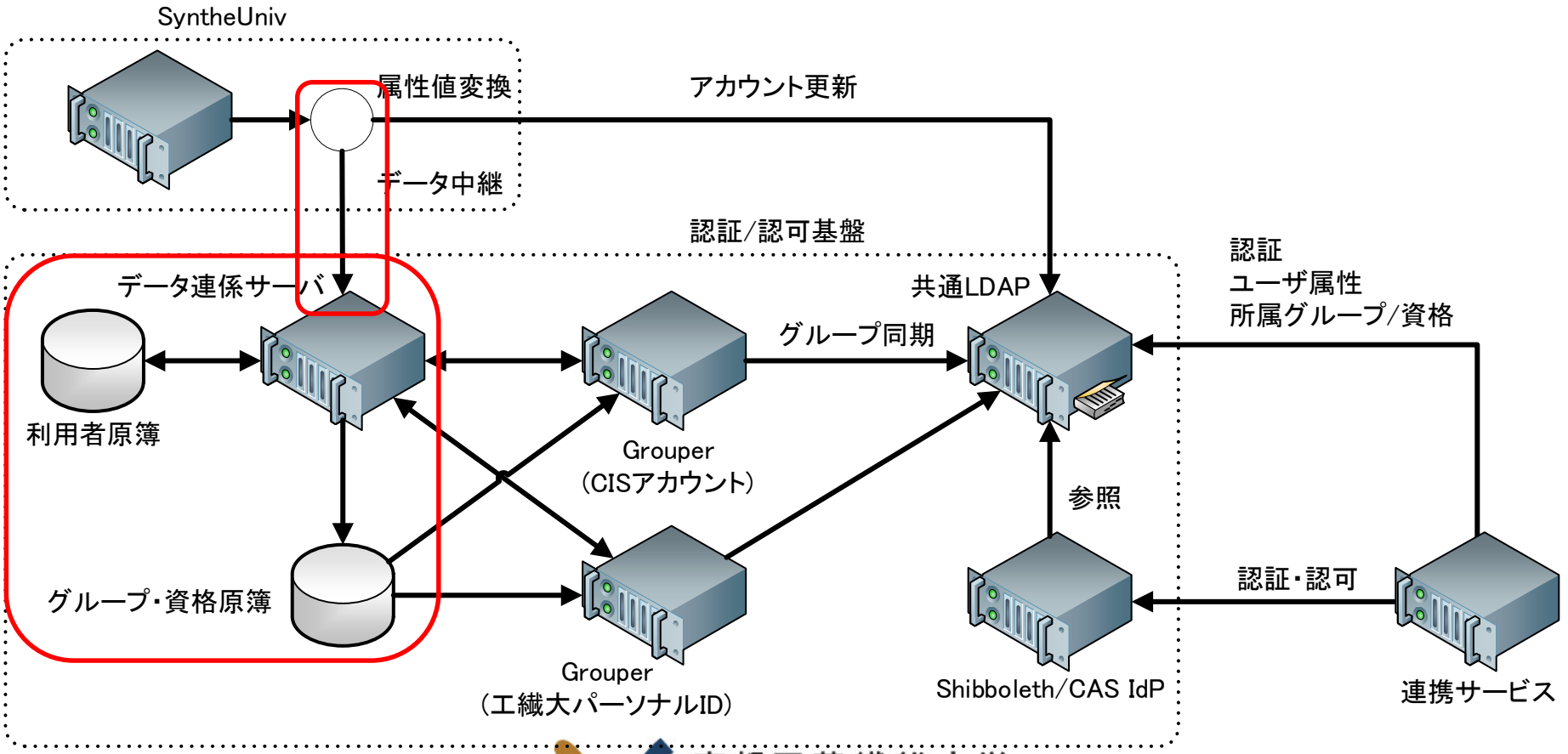
アカウント情報連携



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

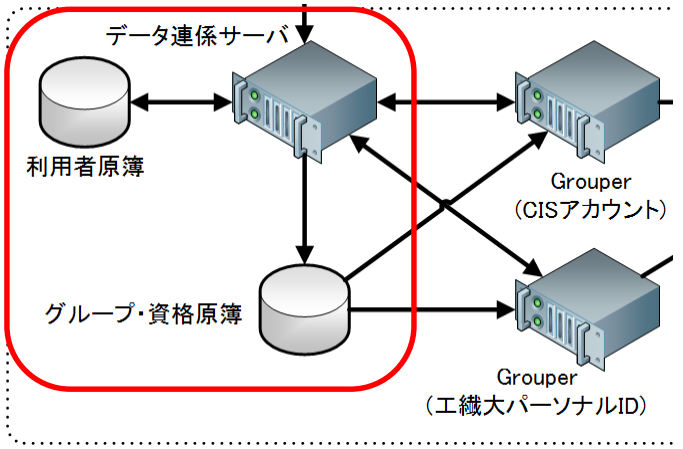
- 開示情報に基づきデータ中継モジュール開発



京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY

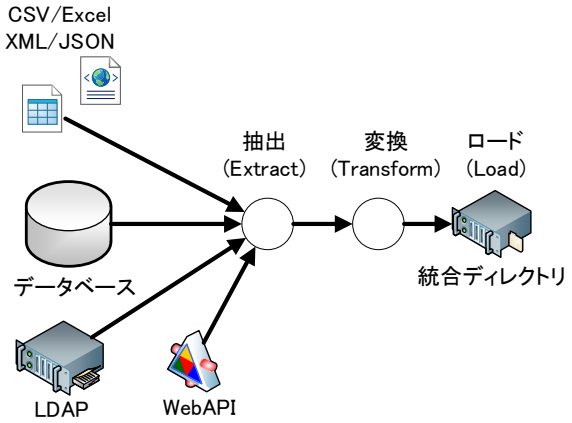
データ連係サーバの役割

- 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



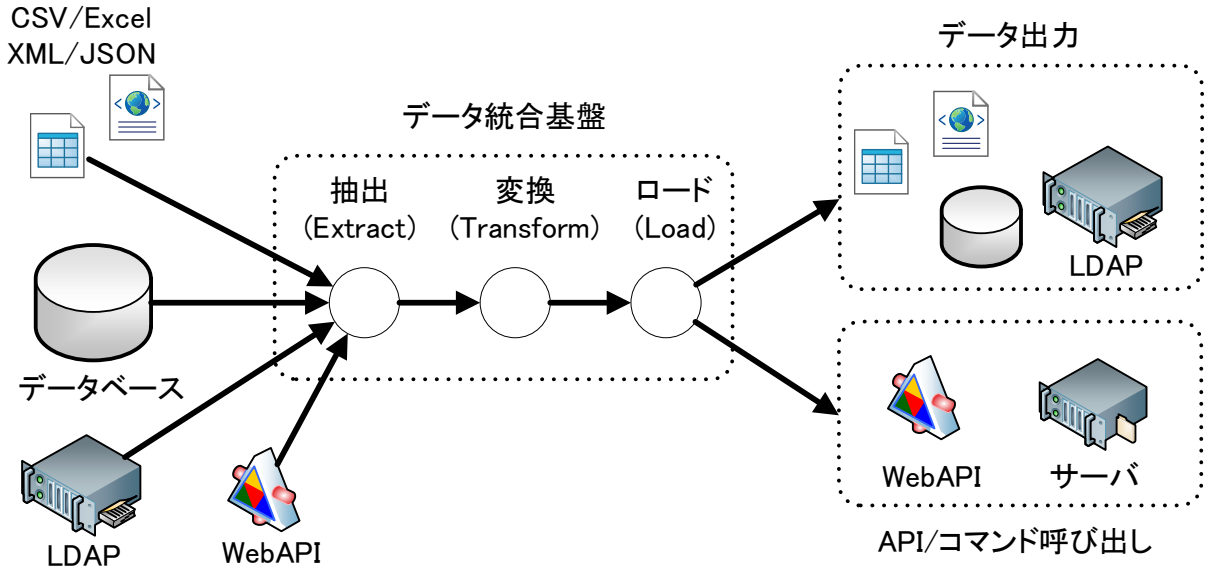
- 工織大パーソナルID用グループ自動生成
  - CISアカウント用グループを自動変換
    - ランダムIDで直接メンバー管理するのは厳しい

データ連係基盤



統合ディレクトリ方式

(Identity Management系)



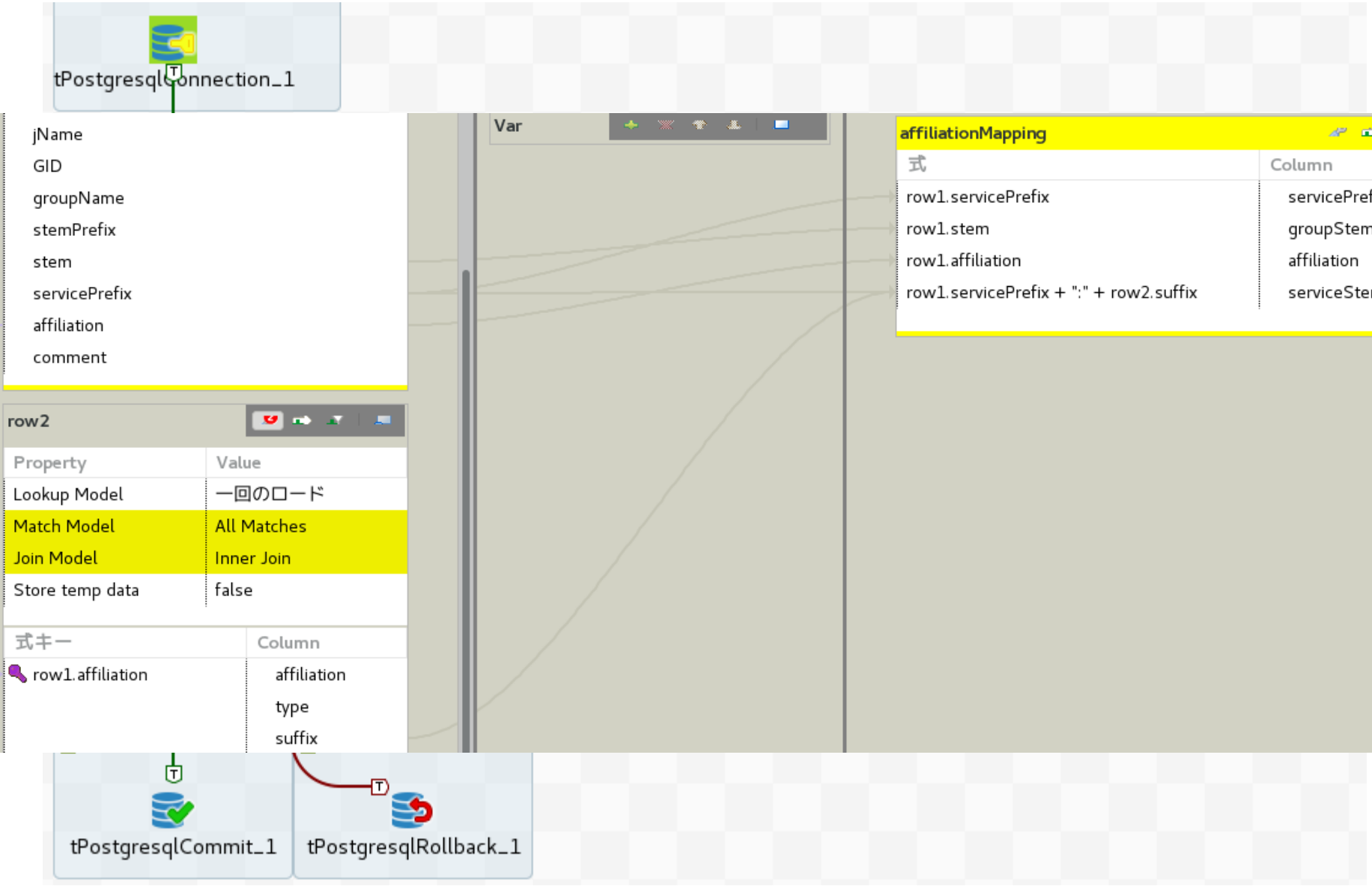
データハブ方式

(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)

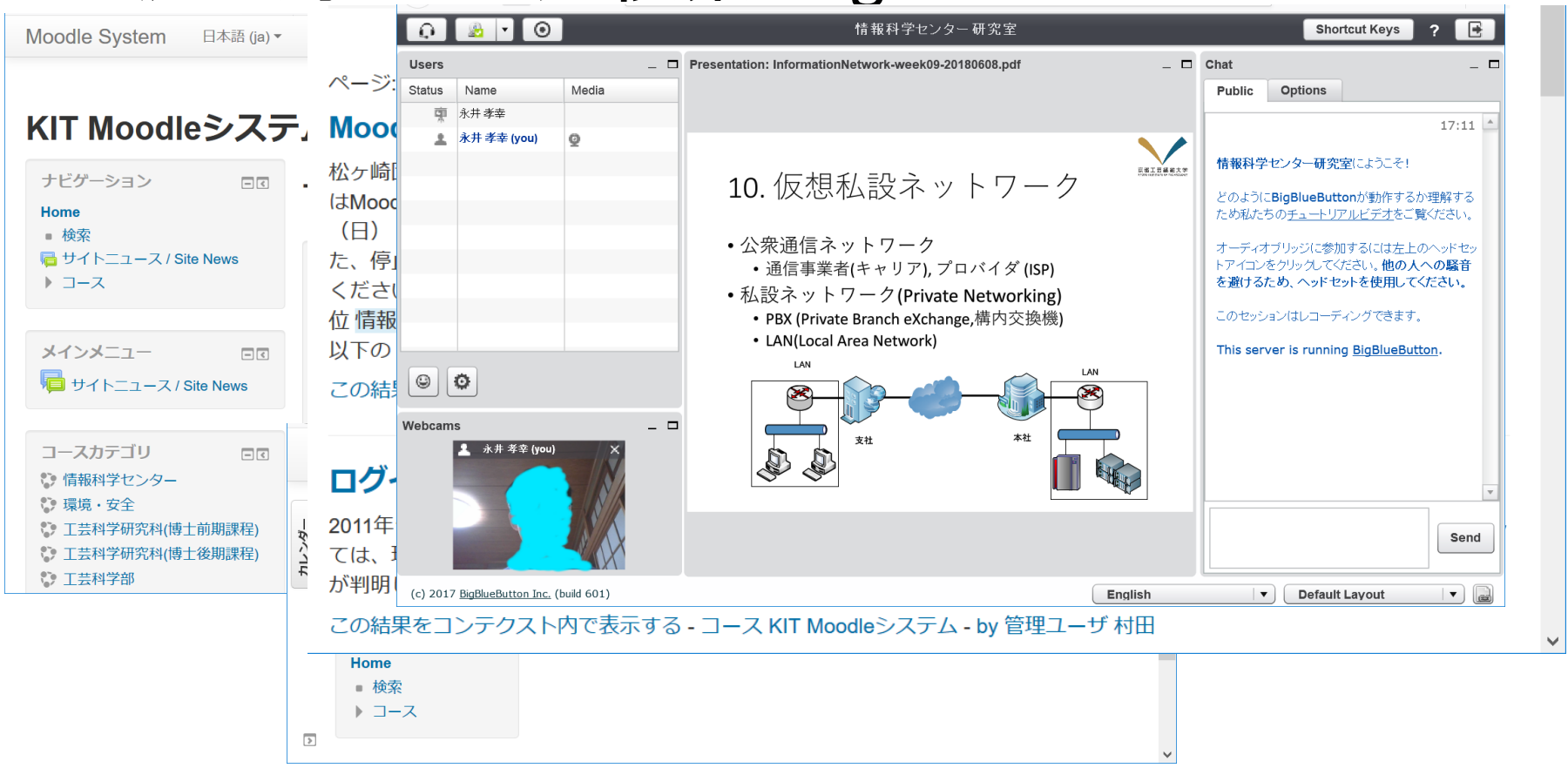
京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY

Talendを使ったデータ連係



Moodle 3.1 LTS

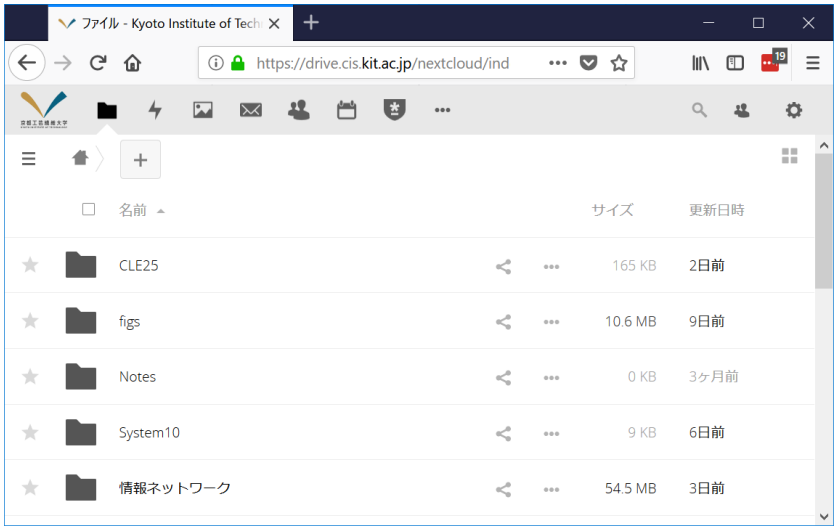
- 生涯ID対応+全文検索+BigBlueButton1.1



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



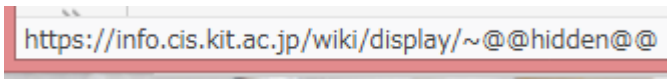
京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY

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

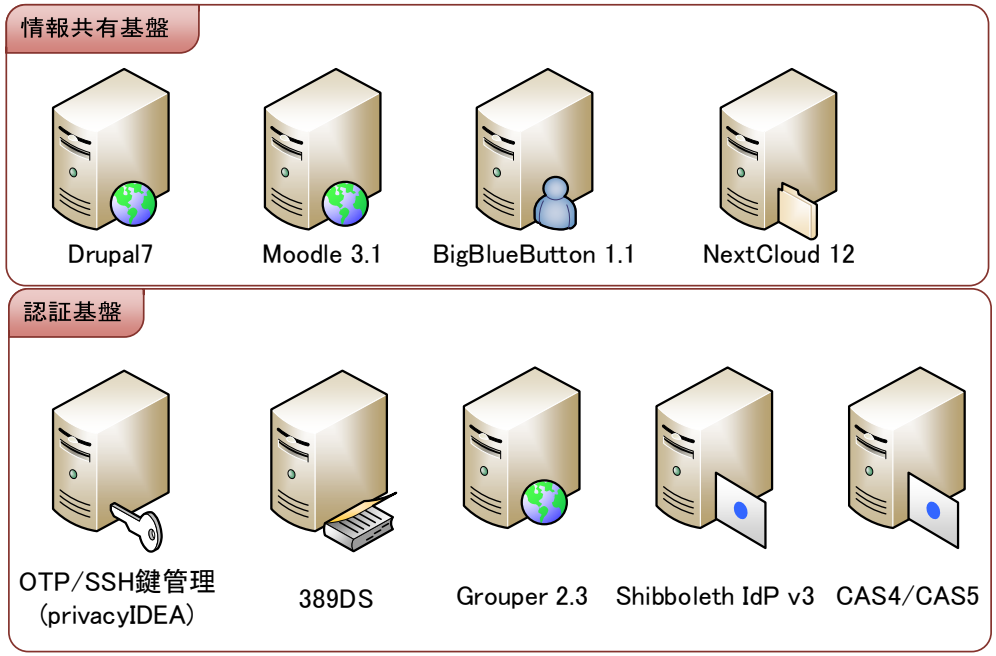
Substitute
s|{"user":{"type":"known",(.*?),"displayName":"(.*?)",|{"user":{"type":"known",$1,"displayName":"@@hidden@@",

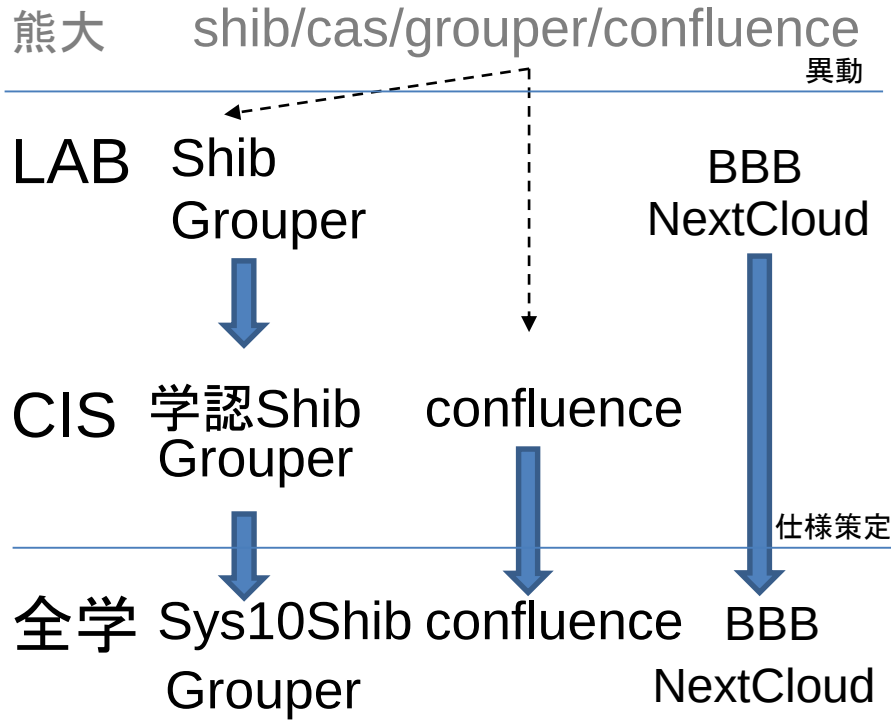


京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY

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





京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY

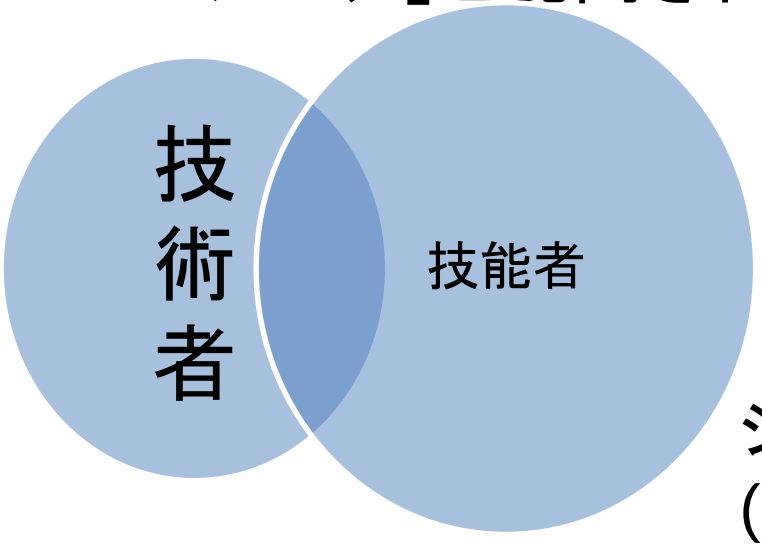
グループウェアによる知識共有

EduTech

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: • SyntheUMS上で該当学生のpersonIDを特定 • 情報科学センターにpersonID付きデータを送信 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: • 学務課の名寄せ作業に必要なSyntheUMS利用権限を設定 • personIDに基づいて既存アカウントと名寄せ	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】 • 非正規生 → 正規生 • 正規生 → 非正規生 • 科目等履修生については、学務課様にて別帳簿で管理
人事データ	連係データにpersonID項目の追加をお願いしたい	人事課: • SyntheUMS上で該当学生のpersonIDを特定 • 情報科学センターにpersonID付	

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



学則の「技術職員」はこっち

システム統合では技術者が必須
(技能者だけではどうにもならない)

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？

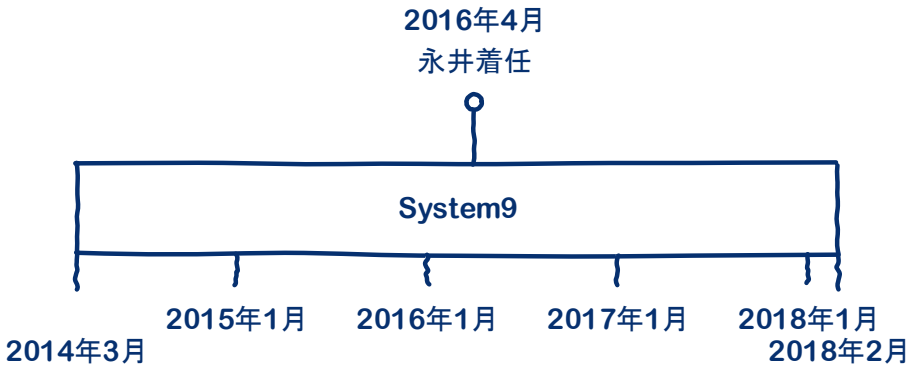
まとめ

- 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,データ連係基盤強化
- 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

- システム調達は一般競争入札方式
  - (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

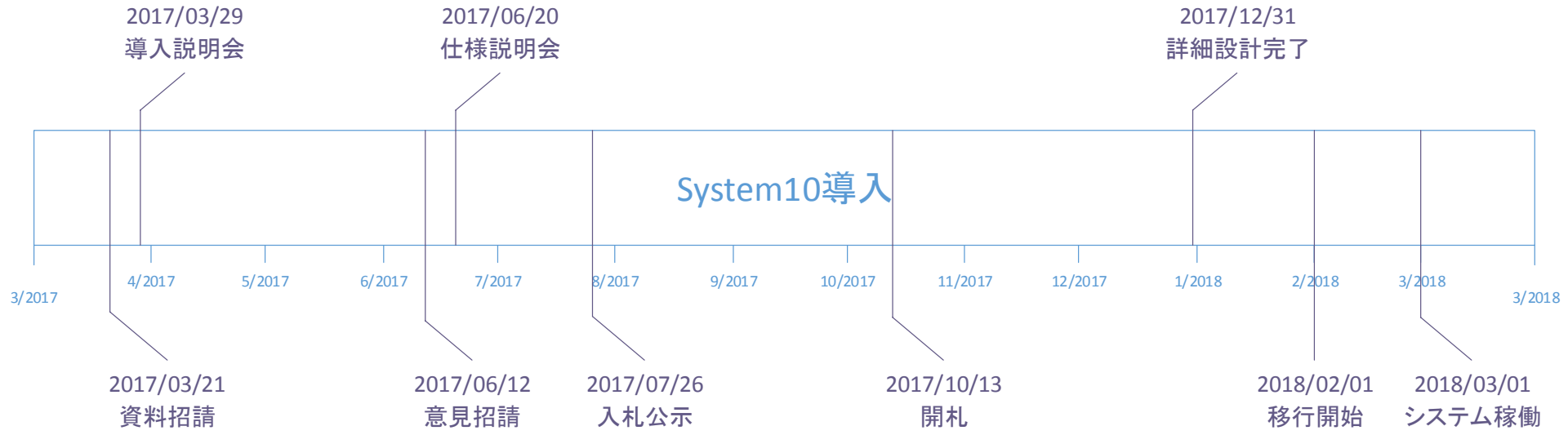
区分	人数(外部出身)
専任教員	3 (3)
技術職員	6 (4)



京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY

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

京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY