



Kumamoto University

学認対応認証基盤とユーザID体系移行用 CASゲートウェイの構築

CLE/CE/SITE研究会(2013/12/15 琉球大学)

○永井 孝幸, 杉谷 賢一, 河津 秀利

中野 裕司(熊本大学)

今回の話

- 生涯IDの導入
 - 「個人(≠身分,契約)」に対してユーザIDを割り当て
- 技術・組織両面からの取り組み
 - IdAM(Identity and Access Management)の話
 - ユーザディレクトリ再構築
 - 学認(Shibboleth認証)対応
 - ユーザID体系移行用CASゲートウェイの開発

教訓:「シングルサインオン環境と生涯IDはセットで導入しましょう」



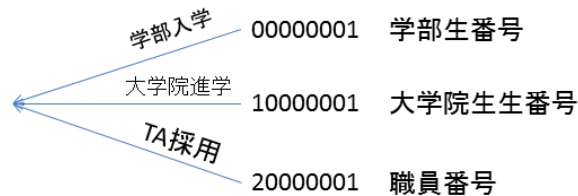
情報環構想2010

- キャンパス環境の高度化・セキュリティ強化
 - 「熊本大学ID(生涯サポート)の導入と熊本大学ポータル」の拡充



れています。卒業生との関係の継続、企業等外部の共同研究者、保護者や大学の支援者、地域社会へのサービス向上等を考え、生涯継続利用できる熊本大学IDを付与し、個々の利

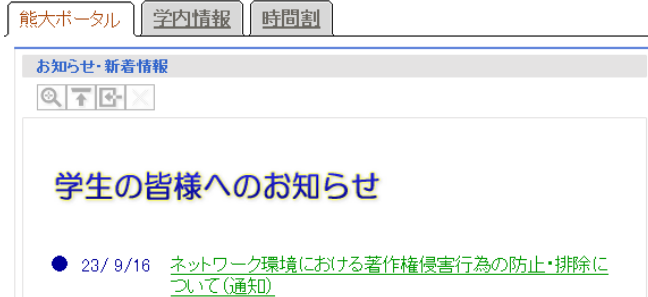
- 既存IDの問題
 - 身分・契約毎にIDを発行



既存ユーザID

「ワンストップサービス」にならない(なってない)

熊本大学ポータル
Kumamoto University

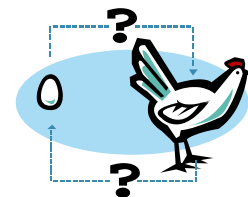


熊本大学ID(生涯ID)

- 英字＋数字からなる9桁のランダムID
 - 例: AB0123456
 - 既存IDは8桁。英字の出現位置も異なる。
- 既存システムで生涯ID運用できるか？
 - ユーザ区分の判別、ID書式チェックに影響あり
 - 「ユーザID順≠学生番号順」問題
 - 改修が絶望的なシステムあり(例: 給与・人事系)
- 新サービスのみ生涯ID利用？
 - 既存IDが多数派→ほとんど導入が見込めない



熊本大学ID導入プラン



- 「鶏と卵」: 熊本大学IDの普及を優先
 - ID利用者を増やさないとシステム対応が進まない

1. 学認(Shibboleth認証)対応

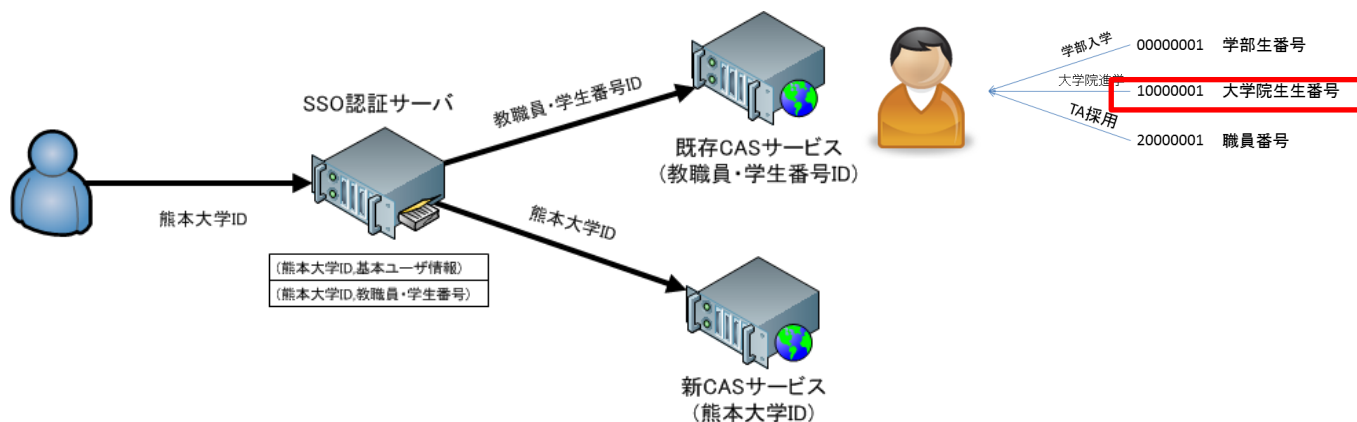
- 学外連携(外部サービス,クラウド)に利用



GakuNin

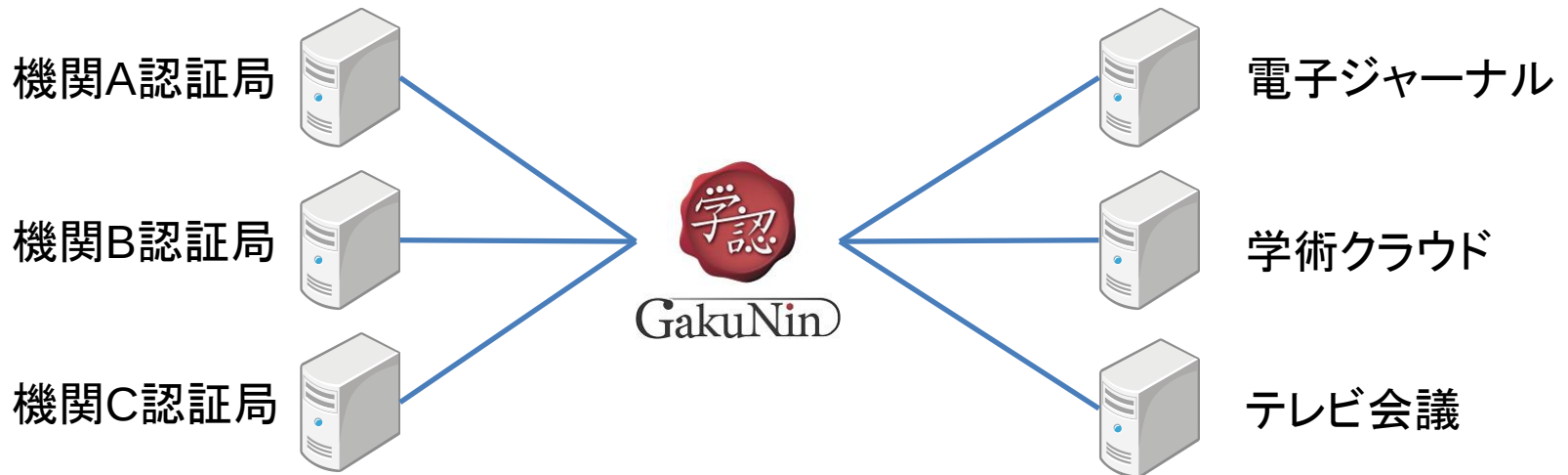
2. 認証ゲートウェイ構築

- ログインIDとユーザIDを分離→透過的移行支援



まずは学認の話

- ShibbolethはOSSだから導入簡単？  Shibboleth.
 - インストール・初期設定はNIIの研修でOK
 - 運用の相談はupki-fed MLでOK
 - 学認を介して相互信頼関係を確立



技術ではなく情報管理の問題



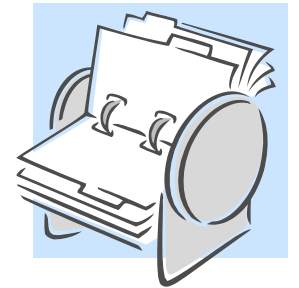
学術認証フェデレーション(学認)

- 機関認証局(IdP)+サービス提供者(SP)
 - 相互信頼のもとで成り立つ仕組み
 - 運用ガイドラインの遵守
 - 「利用者を一意に識別するID」「ユーザ職種属性」の保証
 - 「個人情報保護」も忘れずに(ユーザ自身の同意・オプトイン)
- 熊本大学の取り組み
 - テストフェデレーション参加(2008)後、進展無し
 - SSO認証基盤としてCASを導入済み(2006)
 - SSO基盤として二重投資するメリットが不明



ユーザディレクトリの構築

- 学認用ID(ePPN): 熊本大学IDの「ハッシュ値」
- 熊本大学IDからユーザ属性は分からない
 - 学認だけならstudent,faculty,staff,memberの区分
 - 大学ポータルで使うなら
 - 所属・職種・氏名・メールアドレス・履修科目
 - グループウェアで使うなら
 - 「部局Aの教授職以上のみ許可。でも事務は例外。」
 - 人事・学務DB上の区分コードでは対応できない
 - 本来なら「担当業務DB」が必要

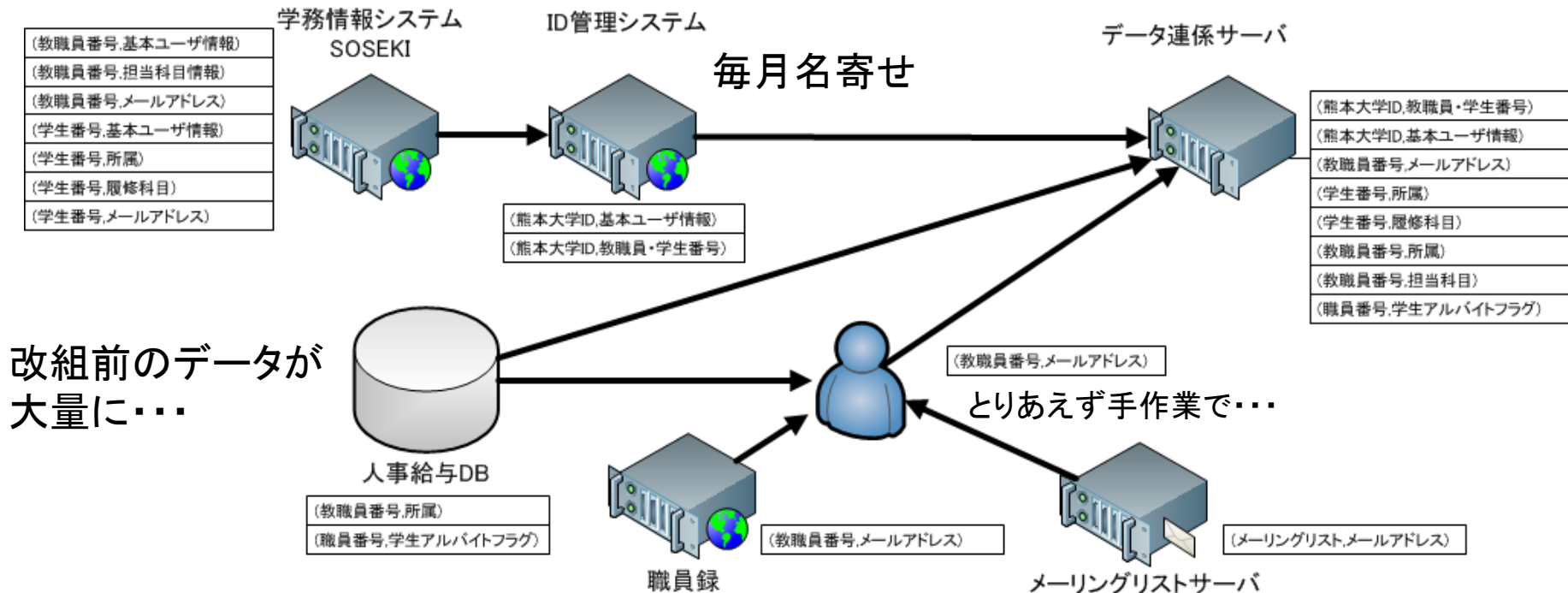


そもそも全学共通のLDAPサーバが無かったので一から構築



アカウント原簿の作成

- 人事給与DB＋学務DBからデータ集約
 - 熊大IDひもづけ: ID管理システムで毎月名寄せ
 - メールアドレス: 「kumamoto-u.ac.jp」のみ収集

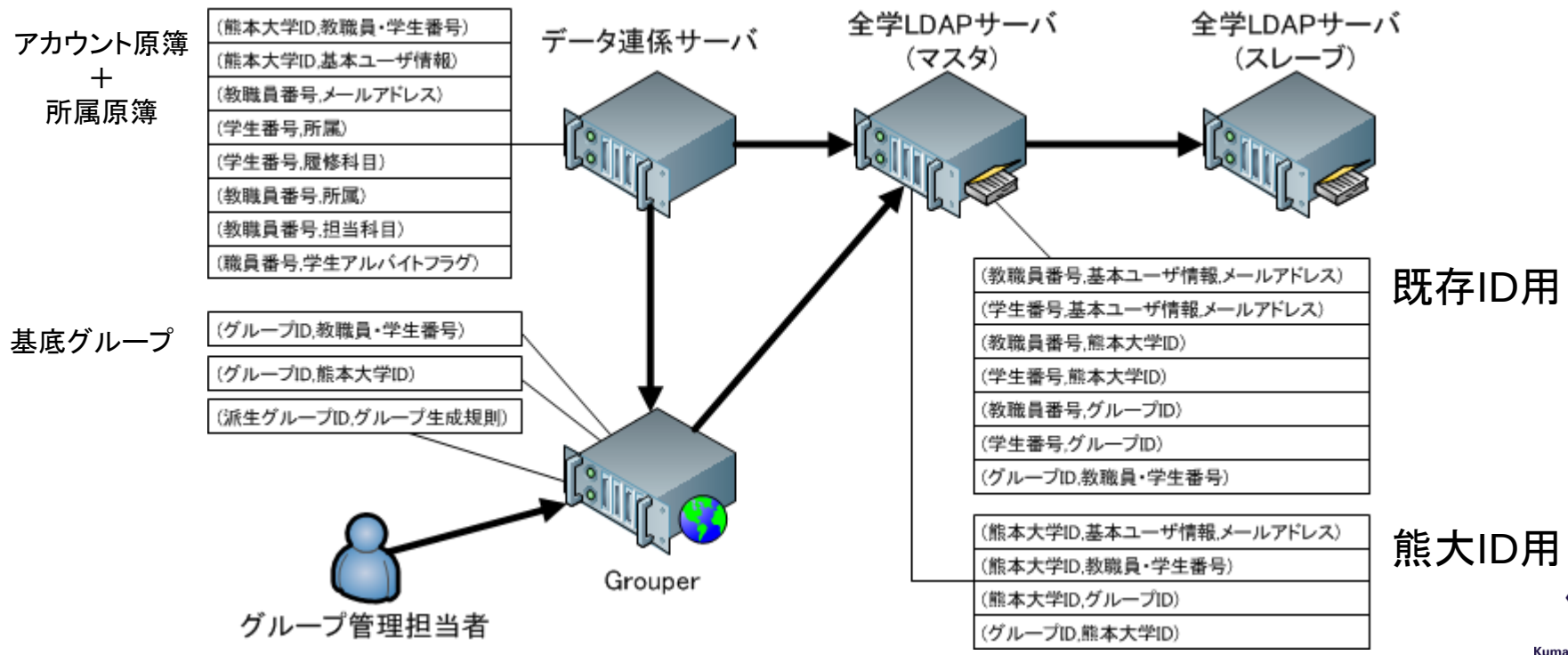


ユーザディレクトリシステム構成

- 389DirectoryServer(商用版:RedHat DS)
 - 元FedoraDS(元Netscape DS)



- Grouper:基底グループの和・差・積に対応



Grouper



- Internet2発祥のグループ管理用ツールキット
 - DBデータ取り込み→グループ更新→LDAP同期
 - CLI,WebServiceAPI対応,uPortal・Sakai連携
 - グループ毎に管理者割り当て可能

Internet2 Grouper™

Welcome Log out

My enrollment
My memberships
Join groups
My responsibilities
Manage groups
Create groups
My tools
Explore
Folder workspace
Group workspace
Entity workspace
Lite UI
Help

EXPLORE

Browse groups hierarchy ⓘ

You can look for groups throughout the hierarchy.
(You might not be able to see some groups if you lack appropriate privileges.)

Browse or list groups ⓘ

Current location is:
Root: course: 2013

50 Change page size
Showing 1-50 of 8589 items

- 2013-05-13461-Special-Lecture-on-Regional-Sciences-B
- 2013-05-33904-Special-Lecture-on-Linguistics
- 2013-05-61900-Basic-Seminar-of-Modern-World-System-C
- 2013-07-05600-Selected-Topics-in-Human-Geography
- 2013-07-08595-Seminar-in-Instruments-BII
- 2013-07-09370-Basics-in-Design-I

Types

grouperLoader

<u>grouperLoaderAndGroups</u>	
<u>grouperLoaderDbName</u>	grouper_group
<u>grouperLoaderGroupQuery</u>	select group_name,readers,updaters from grouper_group.grouper_group where groupType='staff'
<u>grouperLoaderGroupsLike</u>	
<u>grouperLoaderGroupTypes</u>	addIncludeExclude
<u>grouperLoaderIntervalSeconds</u>	
<u>grouperLoaderPriority</u>	
<u>grouperLoaderQuartzCron</u>	0 30 2,19 * * ?
<u>grouperLoaderQuery</u>	select group_name,subject_id from grouper_group.grouper_member where groupType='staff'
<u>grouperLoaderScheduleType</u>	CRON
<u>grouperLoaderType</u>	SQL_GROUP_LIST



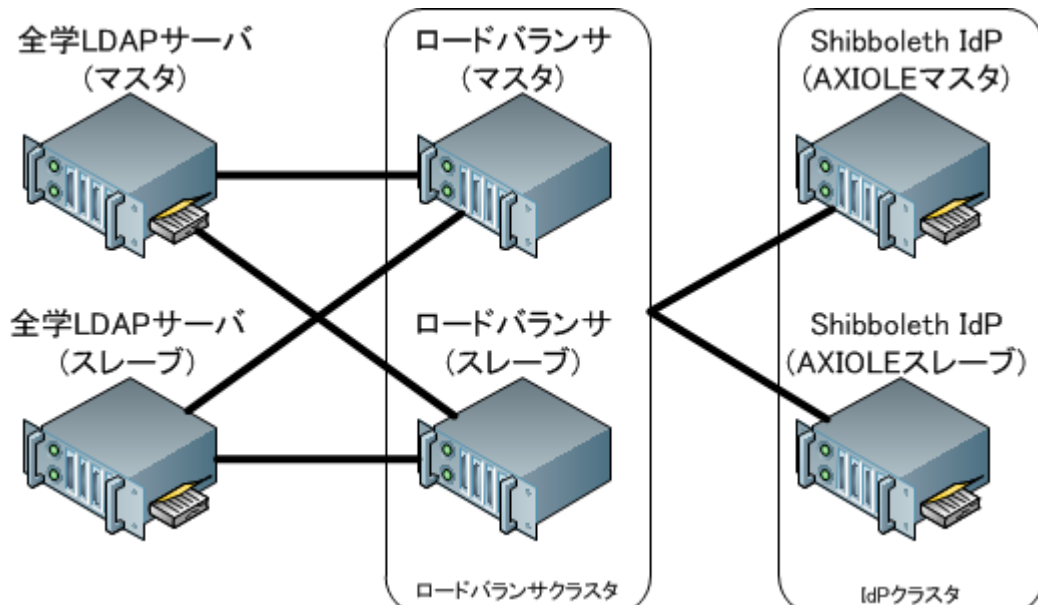
学認用グループの定義

- 教員・職員・学生って一体誰のこと？
 - 付属学校の教職員は？ 附属病院のスタッフは？
 - TAは職員？
 - 雇用契約上は「有期雇用職員」
 - 対外的にも「熊本大学の職員」とみなす？？？
 - 幽霊職員問題(卒業したTAが帳簿に残存)
 - 電子ジャーナル利用契約との整合性
- 現状
 - 「学生＋常勤の教職員」で運用開始(2013/12)
 - その他のケースはWGで継続審議



今回導入した学認用IdP

- AXIOLEアプライアンスによる冗長構成
 - Shibboleth IdP + uApproveJP相当
 - 学認用属性定義は一部JavaScriptを利用



以下のユーザ情報が <https://register-ci.nii.ac.jp/shibboleth-sp> に送信されます。

ユーザ情報	
jaOrganizationName	熊本大学
eduPersonTargetedID	

ユーザ情報送信に同意できない場合はブラウザを開いてください。

☐ 今後、この画面を表示しません。
どのサービスに対してもユーザ情報(上記以外のユーザ情報も含む)を送信することに同意します。

確認

eduPersonAffiliation属性定義(抜粋)

```
<ad:Script><![CDATA[
importPackage(Packages.edu.internet2.middleware.shibboleth.common.attribute.provider);
eduPersonAffiliation = new BasicAttribute("eduPersonAffiliation"); eduPersonAffiliation.getValues().add("member");
if (typeof memberOf != "undefined" && memberOf != null ){
    count = memberOf.getValues().size(); shibPrefix = "cn=shibboleth"; shibPrefixLength = shibPrefix.length;
    facultyGroup="cn=shibboleth:faculty,ou=kugroups,dc=kumamoto-u,dc=ac,dc=jp";
    staffGroup="cn=shibboleth:staff,ou=kugroups,dc=kumamoto-u,dc=ac,dc=jp";
    studentGroup="cn=shibboleth:student,ou=kugroups,dc=kumamoto-u,dc=ac,dc=jp";
    for ( i = 0; i < count; i++ ){
        value = memberOf.getValues().get(i);
        if(value.substring(0,shibPrefixLength) != shibPrefix) continue;
        if(value == studentGroup) eduPersonAffiliation.getValues().add("student");
        else if(value == facultyGroup) {
            eduPersonAffiliation.getValues().add("faculty"); eduPersonAffiliation.getValues().add("staff");
        } else if(value == staffGroup) eduPersonAffiliation.getValues().add("staff");
    }
}
]]></ad:Script>
```

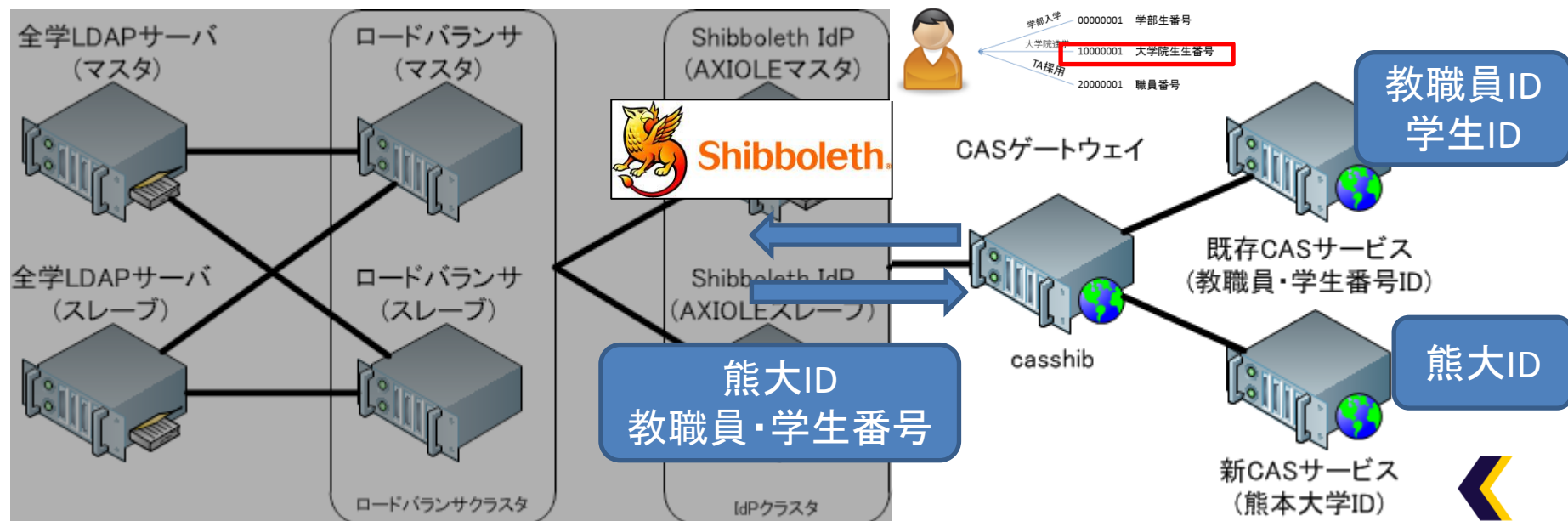
Grouperで管理

所属LDAPグループ(Grouperで管理)に応じて属性値を動的割当



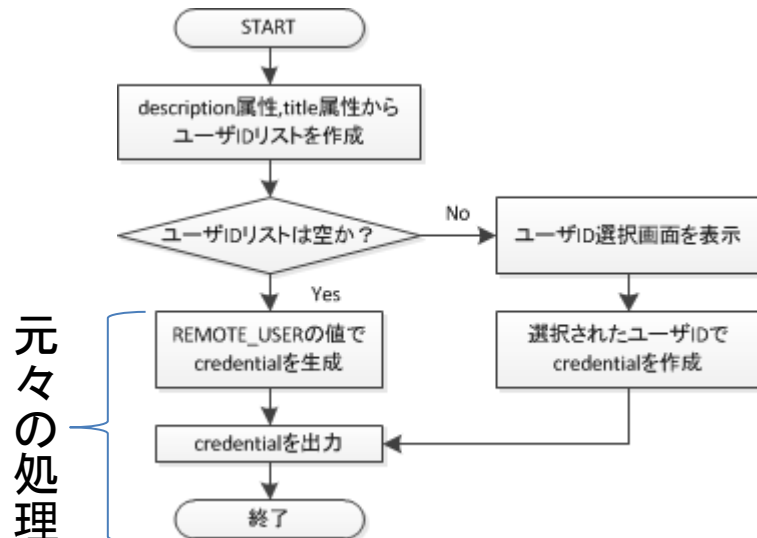
CASゲートウェイの実装

- casshibにユーザID選択機能を実装
 - UC MercedによるCAS-Shibbolethゲートウェイ実装
 - CASクライアントから見るとCASサーバ
 - Shibbolethサーバから見るとShibbolethクライアント



ユーザID選択機能の実装

- remoteAuthenticateアクションを改造
 - REMOTE_USER:熊本大学ID
 - description属性:教職員・学生番号(LDAPで紐付)
 - title属性:アプリ固有アカウント(IdPで付加)



Languages: [English](#) | [Japanese](#) | [Chinese](#)

 **Kumamoto University**
統合認証システム

ユーザ名を選択してください

ユーザ名:

☐ acc00039 ← description属性

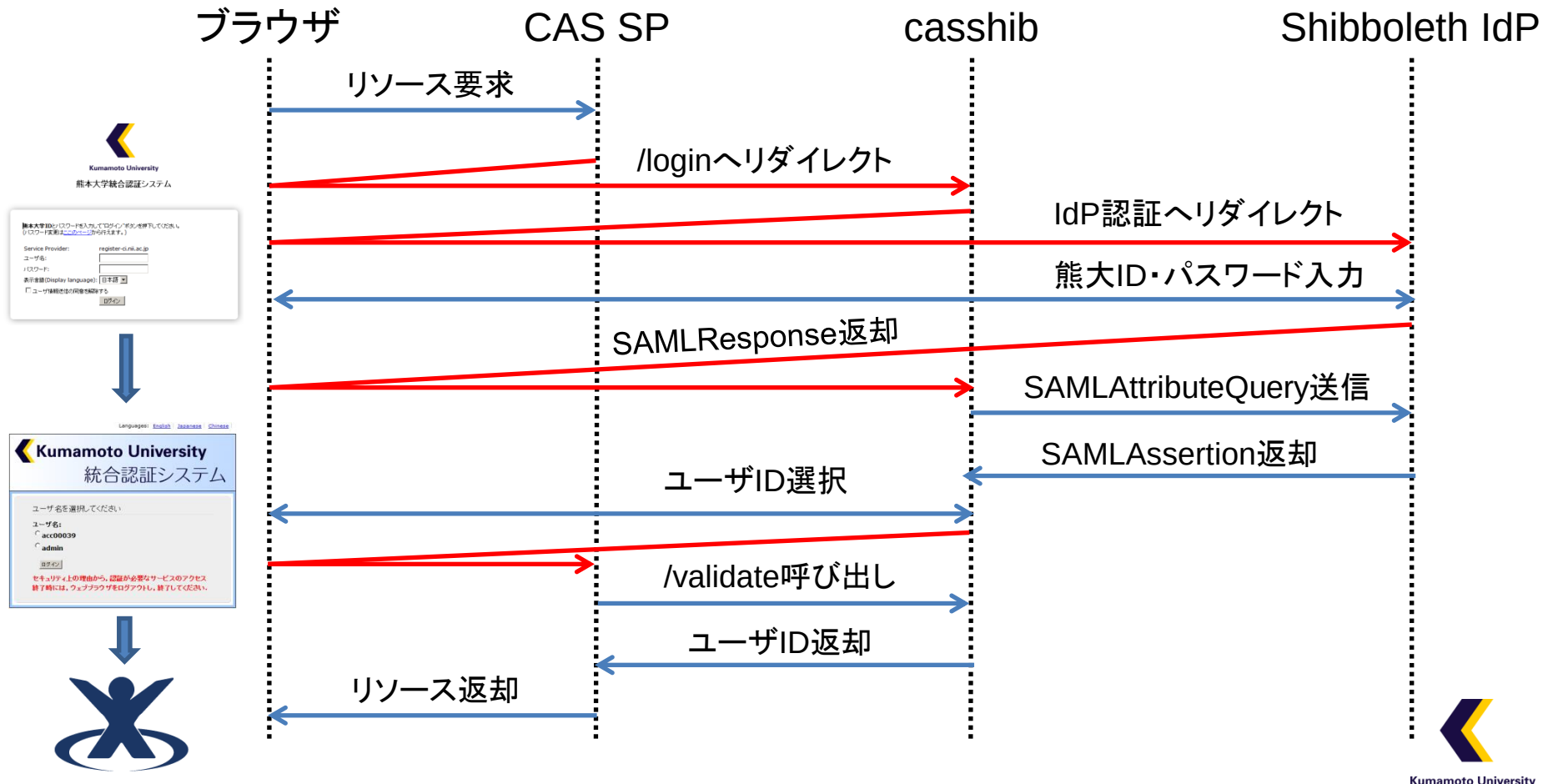
☐ admin ← title属性

セキュリティ上の理由から、認証が必要なサービスのアクセス
終了時には、ウェブブラウザをログアウトし、終了してください。

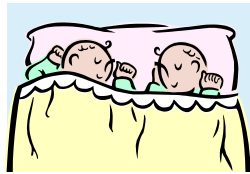


初回認証・ユーザID選択時の動作

- 教職員・学生番号の選択は1回だけ(で運用?)

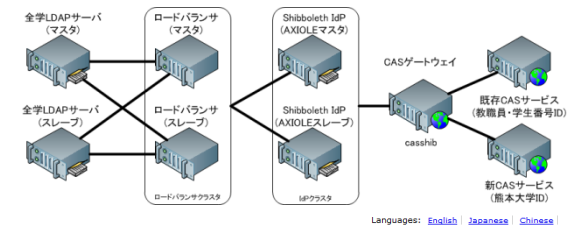
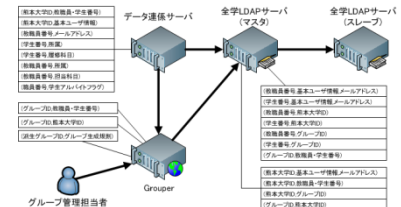


運用状況

- 熊本大学ID: 56,265件発行(2013/10時点)
 - 教職員(1997年度以降),学生(1999年度以降)
 - 自動名寄せ失敗は月に数件(カナ氏名表記揺れ)
- ユーザディレクトリ
 - 職種・部局グループ(約800グループ) 
 - 学部・学科・専攻グループ(約186グループ)
 - 開講科目受講生・教員グループ(17140グループ)
 - 一回の同期に2時間(チューニング前は>12時間)
- casshib-3.5.2aの冗長構成テスト中 
 - ehcache + Terracotta

まとめ

- 今回は生涯ID用認証基盤を構築
 - 学認対応 + CASゲートウェイ構築
 - オープンソースで構築可能
 - 学内認証CAS・Shibboleth両対応
- 演習室端末環境は手つかず
- 熊大IDの普及
 - 熊大ID対応サービスの立ち上げ
 - 「NATあるからIP V6要らない」的シナリオの回避
- 情報のライフサイクル管理



Languages: [English](#) | [Japanese](#) | [Chinese](#)



Kumamoto University
統合認証システム

ユーザ名を選択してください

ユーザ名:
acc00039
admin

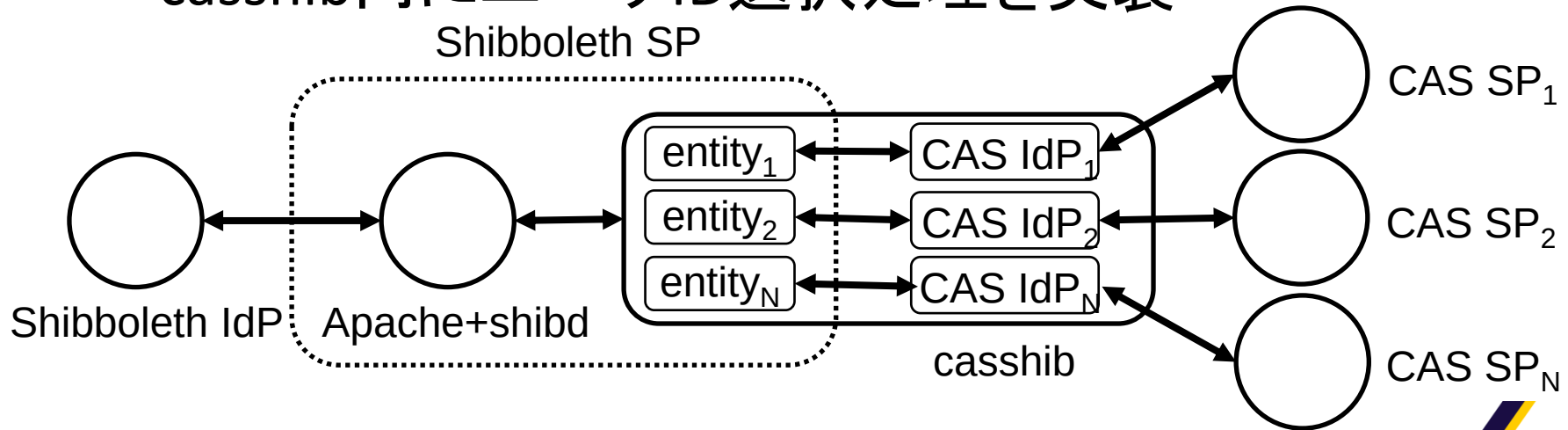
ログイン

セキュリティ上の理由から、認証が必要なサービスのアクセス
終了時には、ウェブブラウザをログアウトし、終了してください。



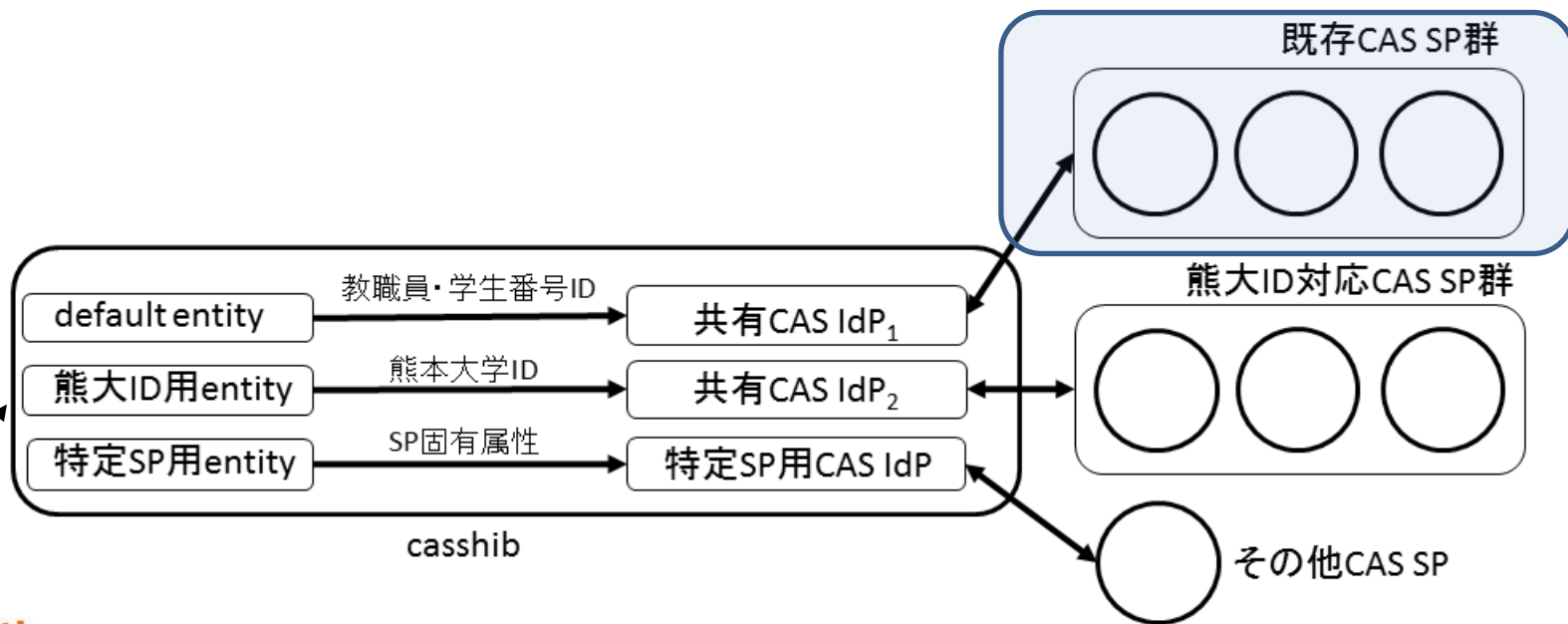
casshibの仕組み

- CASサーブレットをShibbolethの配下に置く
 - HTTPヘッダからユーザID・ユーザ属性を取得
 - 仮想的に複数のCAS IdPとして振る舞う
- Shibboleth IdPを改造したくない
 - casshib内にユーザID選択処理を実装



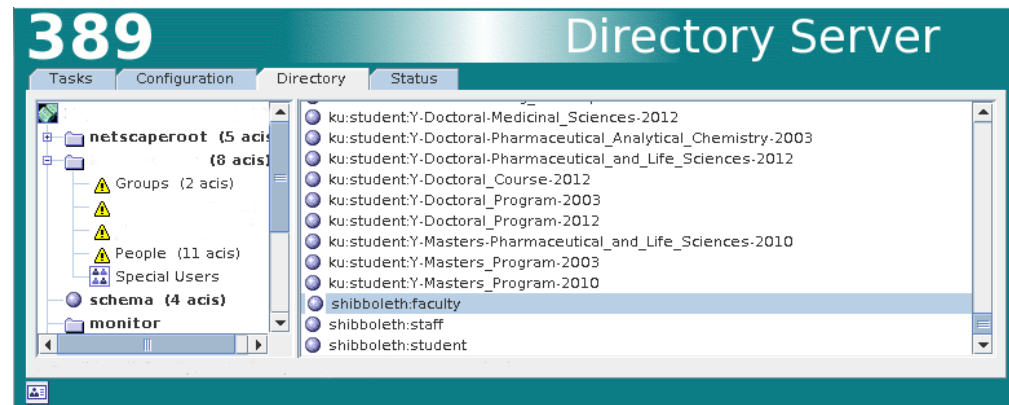
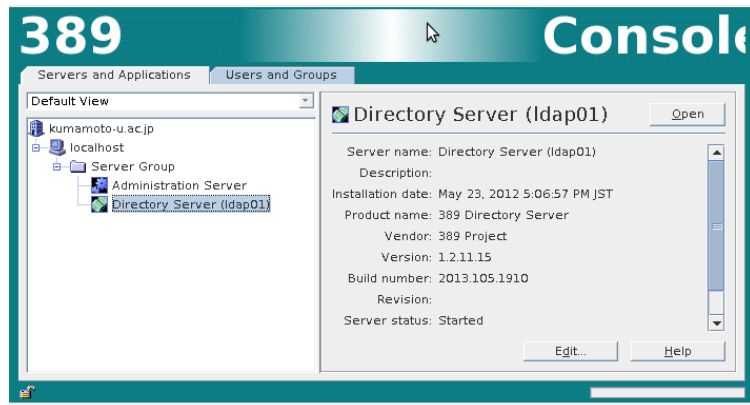
CASゲートウェイの運用

- 仮想IdP毎に異なるユーザ属性を保持できる
 - 教職員・学生番号用共用IdP : ID選択は1回だけ
 - アプリ固有IdP:熊大ID+追加属性を想定



付録:389DirectoryServer

- 389-console



- ドキュメント

- [Red Hat Directory Server](#)
- [389 Directory Server wiki](#)

付録: SP利用制限

```
<afp:AttributeFilterPolicy id="releaseAttributesToExternalSP">  
  <afp:PolicyRequirementRule xsi:type="basic:AND">  
    <basic:Rule xsi:type="basic:AttributeRequesterString"  
value="https://serviceURI/shibboleth-sp"/>  
    <basic:Rule xsi:type="basic:AttributeValueRegex"  
attributeID="eduPersonAffiliation"  
    regex="student|faculty|staff"/>  
  </afp:PolicyRequirementRule>  
  <afp:AttributeRule attributeID="eduPersonPrincipalName">  
    <afp:PermitValueRule xsi:type="basic:ANY"/>  
  </afp:AttributeRule>  
</afp:AttributeFilterPolicy>
```

ePAがstudent,faculty,staffの時のみ
ePP属性をSPに送出



付録：属性送出制限時の動作

- ユーザID等を送信しないのでSP側で棄却
 - 卒業生等休眠アカウントでの利用を防止



本システムの利用権限を満たしていません。

ご不明な点やご質問等がありましたら、下記までご連絡ください。

✉ mcu-sp-admin@nii.ac.jp

Copyright© National Institute of Informatics

