SINET＆学認 クラウド利用説明会
「 学認参加大学における活用事例の紹介」

愛媛大学における学認参加と利用状況

愛媛大学　総合情報メディアセンター
事務課　情報基盤チーム　技術員
増田　隆司

愛媛大学

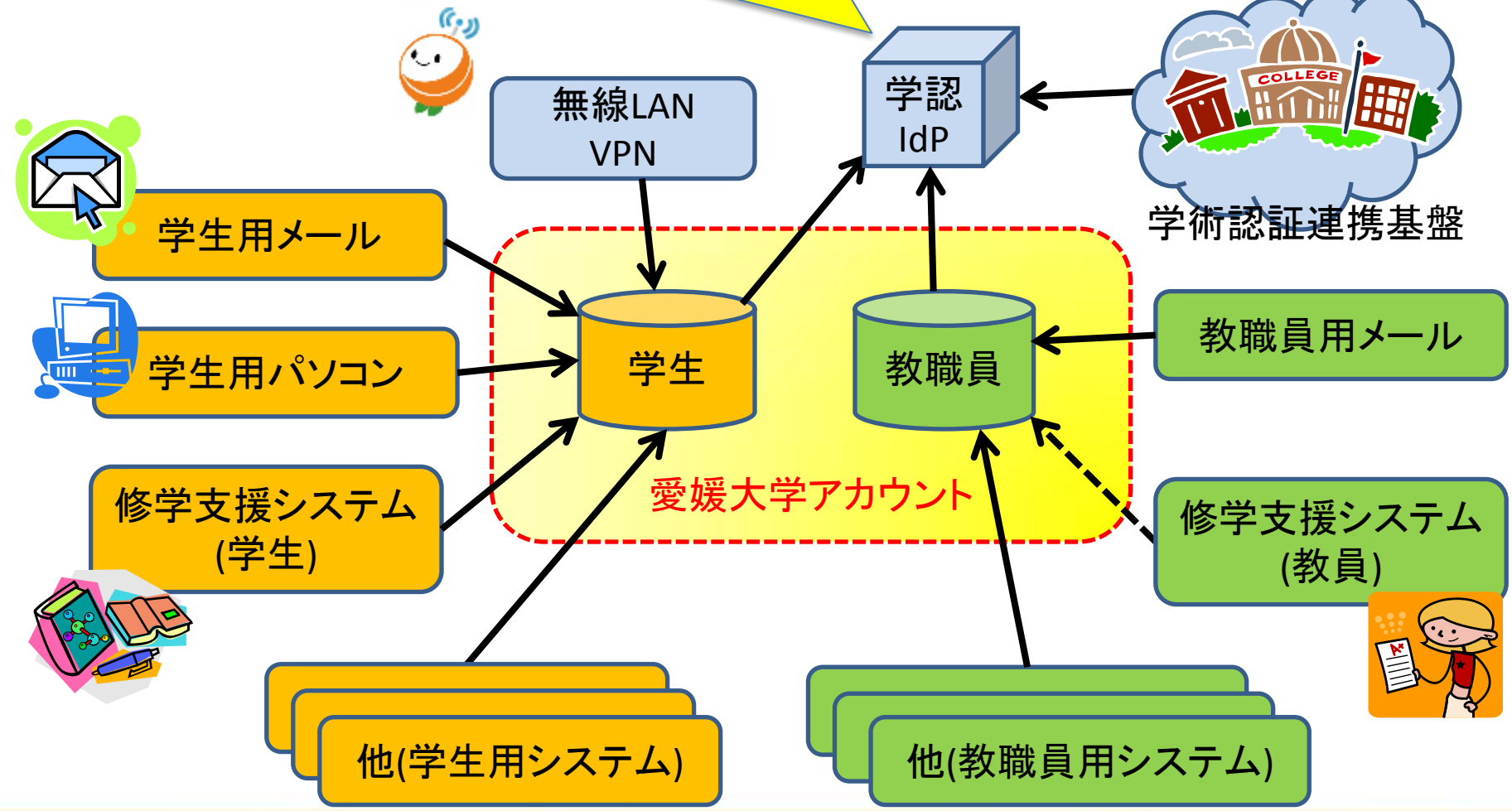
愛媛大学の紹介

- 愛媛県松山市に本拠地を置く国立の総合大学
- 6学部の他、各機構、各センター、附属学校園、附属病院が4キャンパスに分布
- 学生数：約10,000人
- 教職員数：約3,000人（非常勤を含む）

愛媛大学
マスコット
キャラクター
「えみか」

愛媛大学の認証環境

2012年4月から27SP（現在28SP）利用可能な状態でサービス開始。



サービス開始までのスケジュール

2011年

- 8月　NII情報処理技術セミナー受講
- 10月　学認へ参加する方針を部署内で決定
- 12月　学認への参加が学内で承認される

2012年

- 1月　認証環境構築開始
- 2月1日　テストフェデレーションにて検証開始
- 3月9日　運用フェデレーションへ参加申請
- 3月16日　運用フェデレーションへの申請承認
- 3月19日　図書館と連携し電子ジャーナルの学認利用申請開始
  （対象ジャーナル数：10）
- 4月2日　教職員・学生へのサービス開始

発生した問題

非システム的な問題

- 「学認とは？」を説明してもよくわからないという人や誤解されるケースが多々発生。
- 学認に参加するためにシステム構築が必要ということが学内で認識されていなかった。

システム的な問題

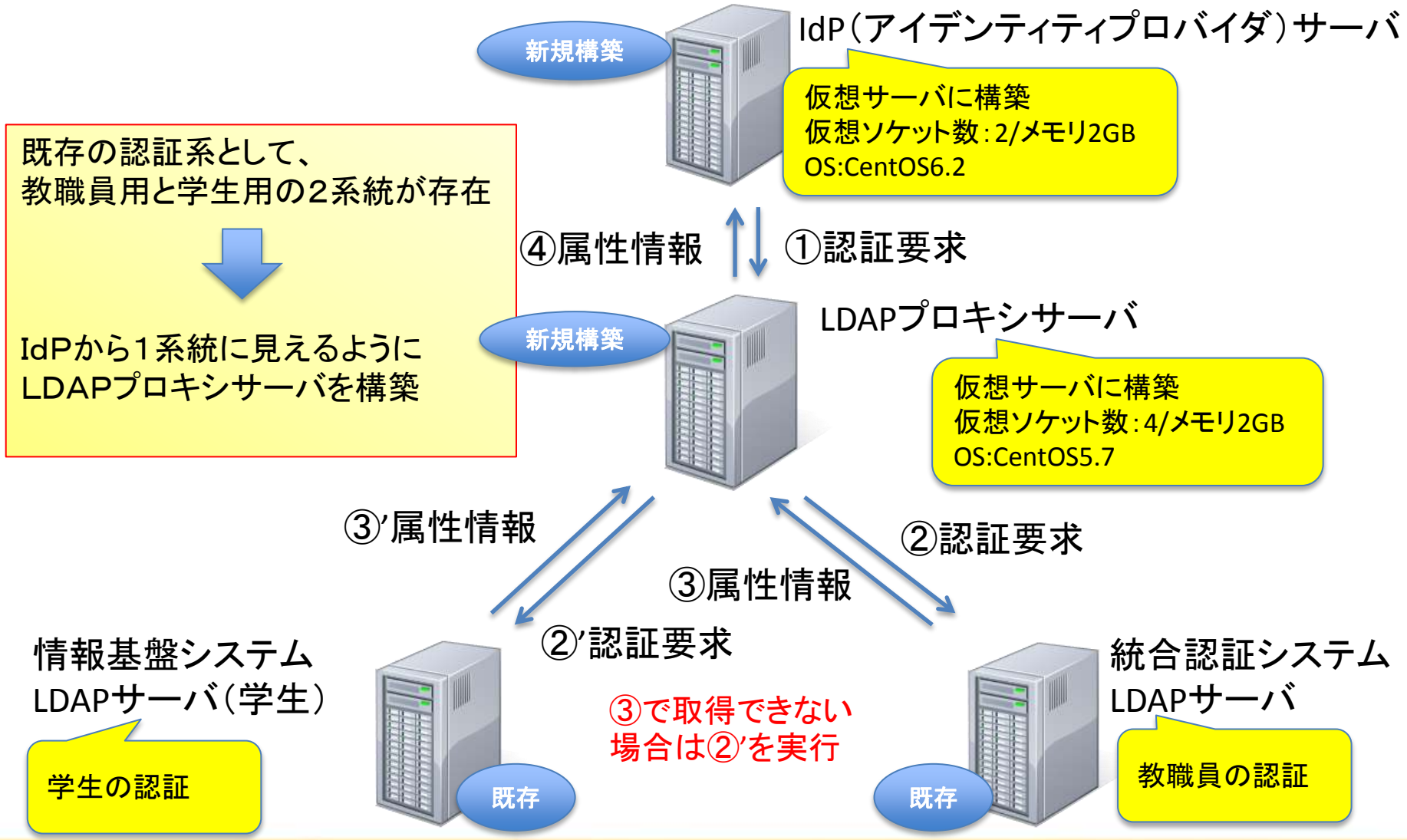
- IdPから直接参照可能なLDAPは1つだけだが、大学の認証系は教職員用と学生用が存在。

  ⇒LDAPプロキシサーバを構築。

  ⇒当初、LDAPプロキシが正常に動作せず。

- 既存のLDAPに登録されている属性情報が不足しているものやRFCに準拠してしないものが存在。

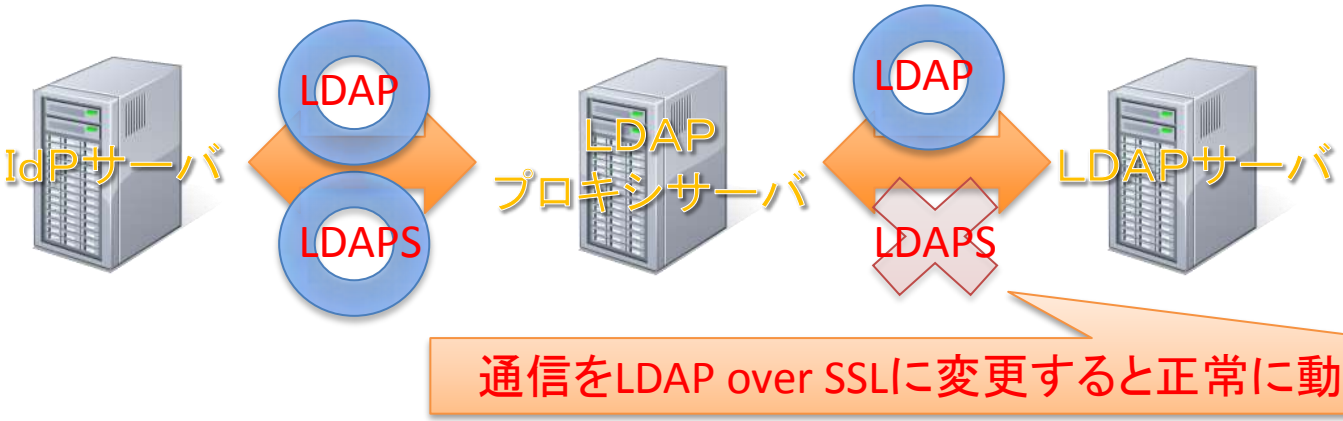
認証環境の構成


新規構築
IdP（アイデンティティプロバイダ）サーバ
仮想サーバに構築
仮想ソケット数：2/メモリ2GB
OS:CentOS6.2
既存の認証系として、
教職員用と学生用の2系統が存在
IdPから1系統に見えるように
LDAPプロキシサーバを構築
④属性情報
①認証要求
新規構築
LDAPプロキシサーバ
仮想サーバに構築
仮想ソケット数：4/メモリ2GB
OS:CentOS5.7
③'属性情報
②認証要求
③属性情報
②'認証要求
情報基盤システム
LDAPサーバ（学生）
学生の認証
既存
③で取得できない
場合は②'を実行
既存
統合認証システム
LDAPサーバ
教職員の認証

LDAPプロキシサーバの構築

IdPサーバからLDAPプロキシサーバへ問合せを行い、まず教職員用LDAPをサーチ、次に学生用LDAPをサーチし、認証が成功すれば必要な属性を返却する。

当初、CentOS6.2+OpenLDAP2.4で構築。



設定を色々と変更して試すがうまくいかないためNIIに相談。

CentOS5.7では正常に動作。
CentOS5.7で再構築。

IdPから送信が必要な属性

属性名	内容	取得元の例
mail	メールアドレス	LDAP
o	大学名(英字)	IdPでStaticに記載
ou	所属学部・部署(英字)	LDAP
sn	姓(英字)	LDAP
givenName	名(英字)	LDAP
displayName	氏名・表示名 (英字)	LDAP
eduPersonAffiliation	職種等・身分	LDAP
eduPersonPrincipalName	[ID]@ehime-u.ac.jp	IdPで生成
eduPersonEntitlement	SP利用資格情報	IdPでStaticに記載
eduPersonScopedAffiliation	[eduPersonAffiliation]@ehime-u.ac.jp）	IdPで生成
eduPersonTargetedID	[IdPのEntityID]+[SPのEntityID]+[ハッシュ化したID]	IdPで生成
jao	大学名(日本語)	IdPでStaticに記載
jaou	所属学部・部署(日本語)	LDAP
jasn	姓（日本語）	LDAP
jaGivenName	名（日本語）	LDAP
jaDisplayName	氏名・表示名(英字)	LDAP

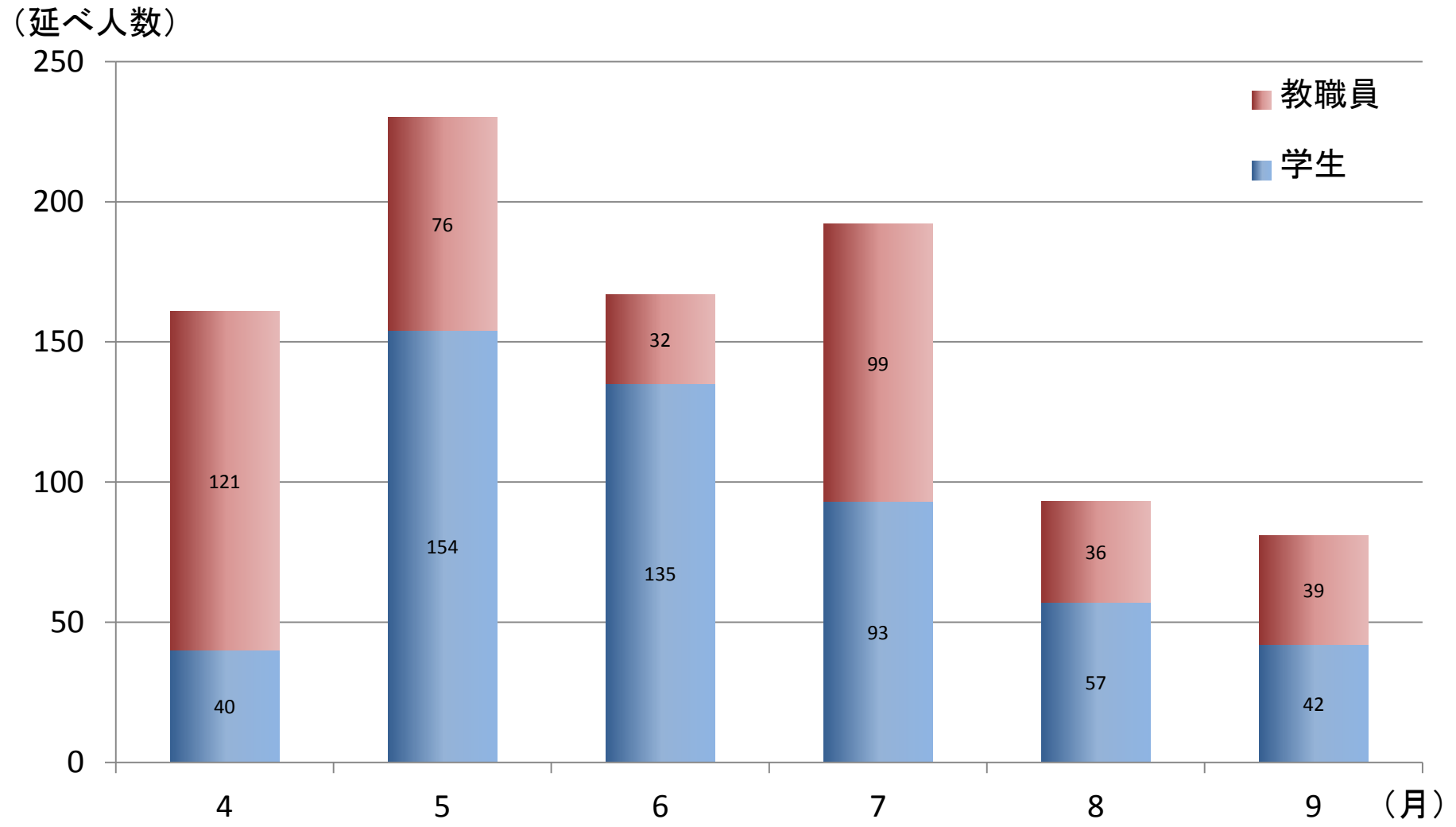
LDAP属性の整備

◆LDAPに必要な属性と整備前の状況

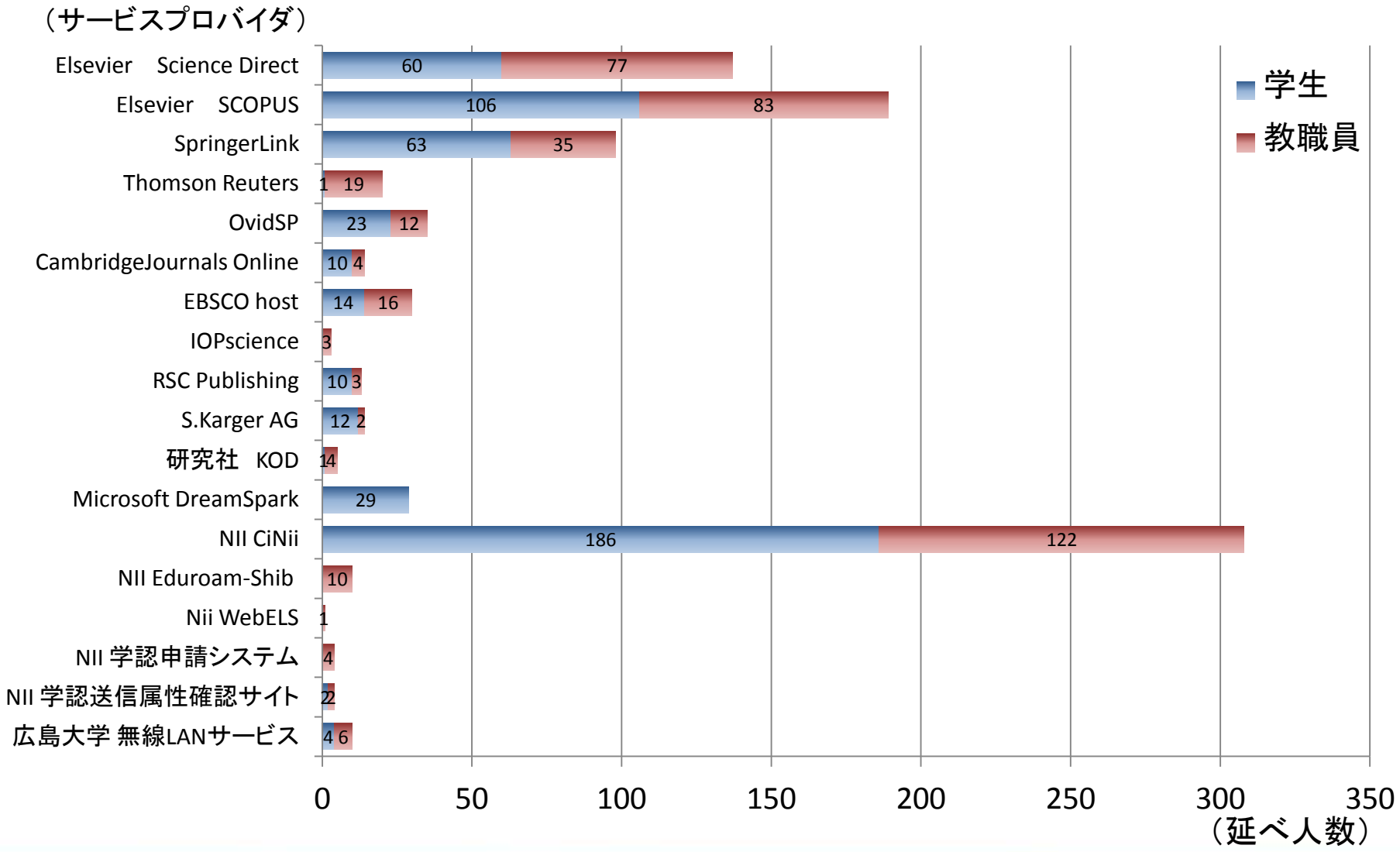
属性名	教職員用LDAP	学生用LDAP
mail	○	○
ou	全角文字（日本語）が設定	（属性なし）
sn	全角文字（日本語）が設定	○
givenName	全角文字（日本語）が設定	○
displayName	異なる属性名で設定あり	（属性なし）
eduPersonAffiliation	（属性なし）	（属性なし）
jasn	snに設定あり	（属性なし）
jaGivenName	givenNameに設定あり	（属性なし）
jaDisplayName	異なる属性名で設定あり	（属性なし）
jaou	ouに設定あり	（属性なし）

・現状登録されているユーザの属性情報を修正
・新規ユーザに適用できるよう登録システムを改修

利用状況（2012年月別・延べ人数）



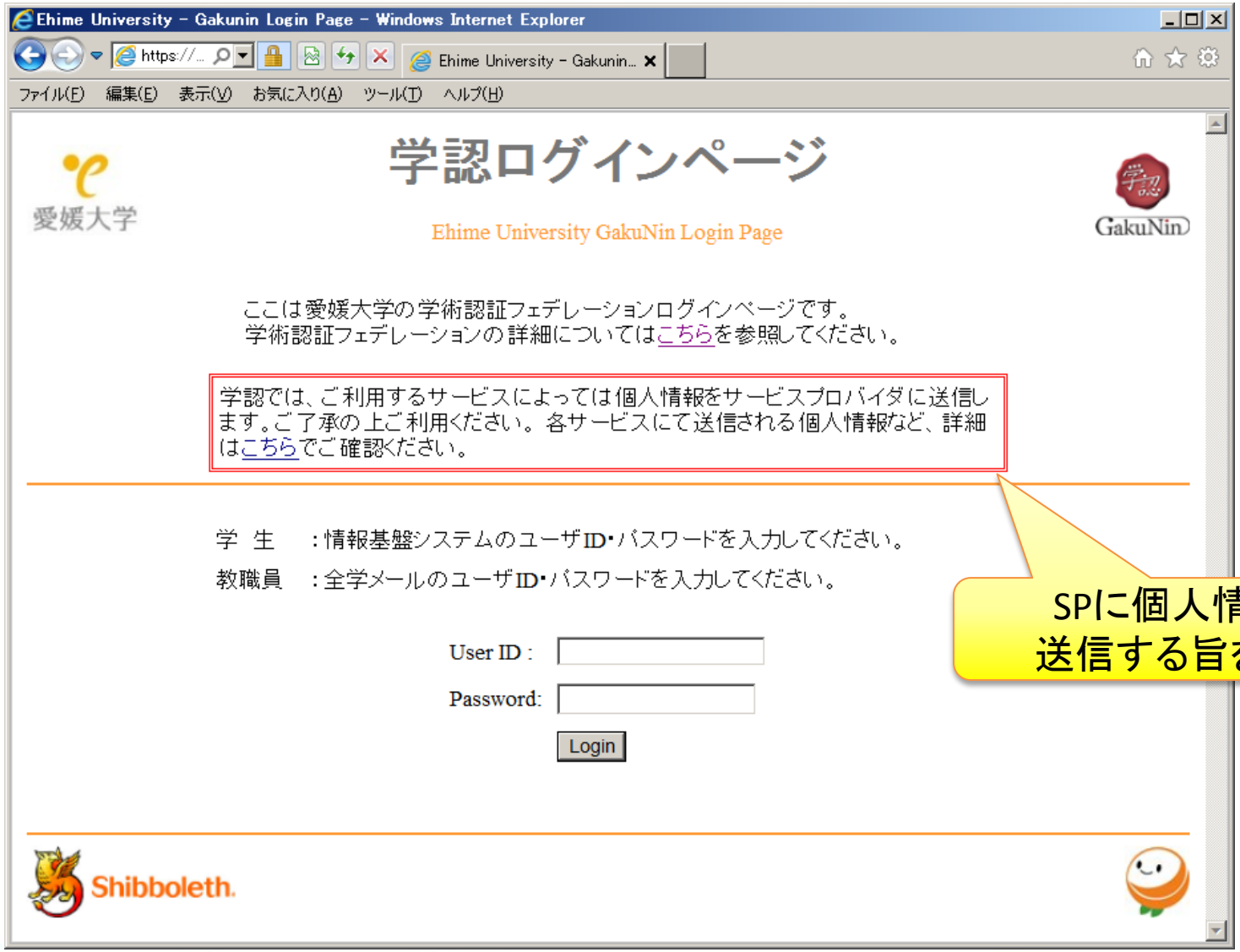
利用状況（SP別・延べ人数）



今後の課題

- ユーザへの周知と普及
  サービス開始から半年間で学認経由でサービスプロバイダを利用した人は
  学生86人（0.88%）、教職員55人（1.86%）と全学構成員の1%程度。
  ⇒ サービス開始時に全学アナウンスはしたがあまり認知されていない。
  VPNがある程度普及済。Wileyなど学認から利用できないものがある。
- eduPersonTargetedID生成時のStoredIDの使用
  ComputedIDの場合、ユーザIDをハッシュ化する際のアルゴリズムとして
  SHA-1を使用しており、低い確率($1/2^{80}$)ではあるが衝突が発生する
  可能性がある。
  ⇒運用開始時はComputedIDを使用。
- ユーザ同意取得システム　uAapprove.jpの適用
  学認ではSPに個人情報を送信するため、
  ユーザ同意を得て使用してもらうことが望ましい。
  ⇒運用開始時は導入せず、ログイン画面に注意書きと
  リンク先のホームページに詳細を記載して代替。

ログイン画面



SPに個人情報を
送信する旨を記載

ユーザへの送信属性通知

属性名では一般ユーザに解り辛いため、各属性を右図にように
- 「氏名」
- 「所属」
- 「身分」
- 「ユーザID」
- 「メールアドレス」

に分類して、
各SP毎に送信する情報に●印をつけてホームページに掲載。

組織等	サービス・利用方法	送信情報				
		氏名	所属	身分	ユーザID	メールアドレス
Elsevier（図）	Science Direct SCOPUS					
Springer（図）	SpringerLink					
Thomson Reuters（図）	Web of Knowledge EndNote Web			●		
Ovid（図）	OvidSP			●		
CUP（図）	CambridgeJournals Online			●		
EBSCO（図）	EBSCO host					
IOP（図）	IOPscience			●		
Royal Society of Chemistry（図）	RSC Publishing			●		
研究社(図)	KOD					
Microsoft	DreamSpark（注） 利用方法			●		
国立情報学研究所	CiNii（図）	●	●			●
	FaMCUs			●		
	Fshare					
	Eduroam-Shiba 利用方法					
	WebELS WebELS Learning利用方法 WebELS Meeting利用方法			●		
	edubase Cloud 利用方法				●	●
	学認申請システム				●	
	GakuNin mAP 利用方法	●			●	●
	meatwik 利用方法	●			●	●

今後の計画

認証システム

- 認証システムの次期リプレイス時に学生用と教員用の認証系を統合。
  IdPサーバにStoredID、uAapprove.jpを導入。
- IdPサーバ、LDAPサーバをクラウド移行しノンストップシステム化。

学内向けサービス

- 学内システム（メールシステム、e-ラーニングシステム、教務系システム等）について 順次Shibboleth対応を行い、愛媛大学IdPを経由して認証することで　学認サービスプロバイダと共にシングルサインオン化を図る。

学外者向けサービス

- 学内無線LANをeduroamに対応、もしくは学認SPとすることで、
  学外者の来訪時にゲスト利用を可能とする。
- e-ラーニングシステムの学認SP化によってeラーニングを利用した
  大学間連携講義への活用。