

NIIオープンハウス2012 学認セッション

「学認にまつわる仕様書の書き方と調達の仕方」

IdPを独自構築した事例 ー 愛媛大学の場合 ー

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

スケジュール概要

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

IdP構築に必要な知識・スキル

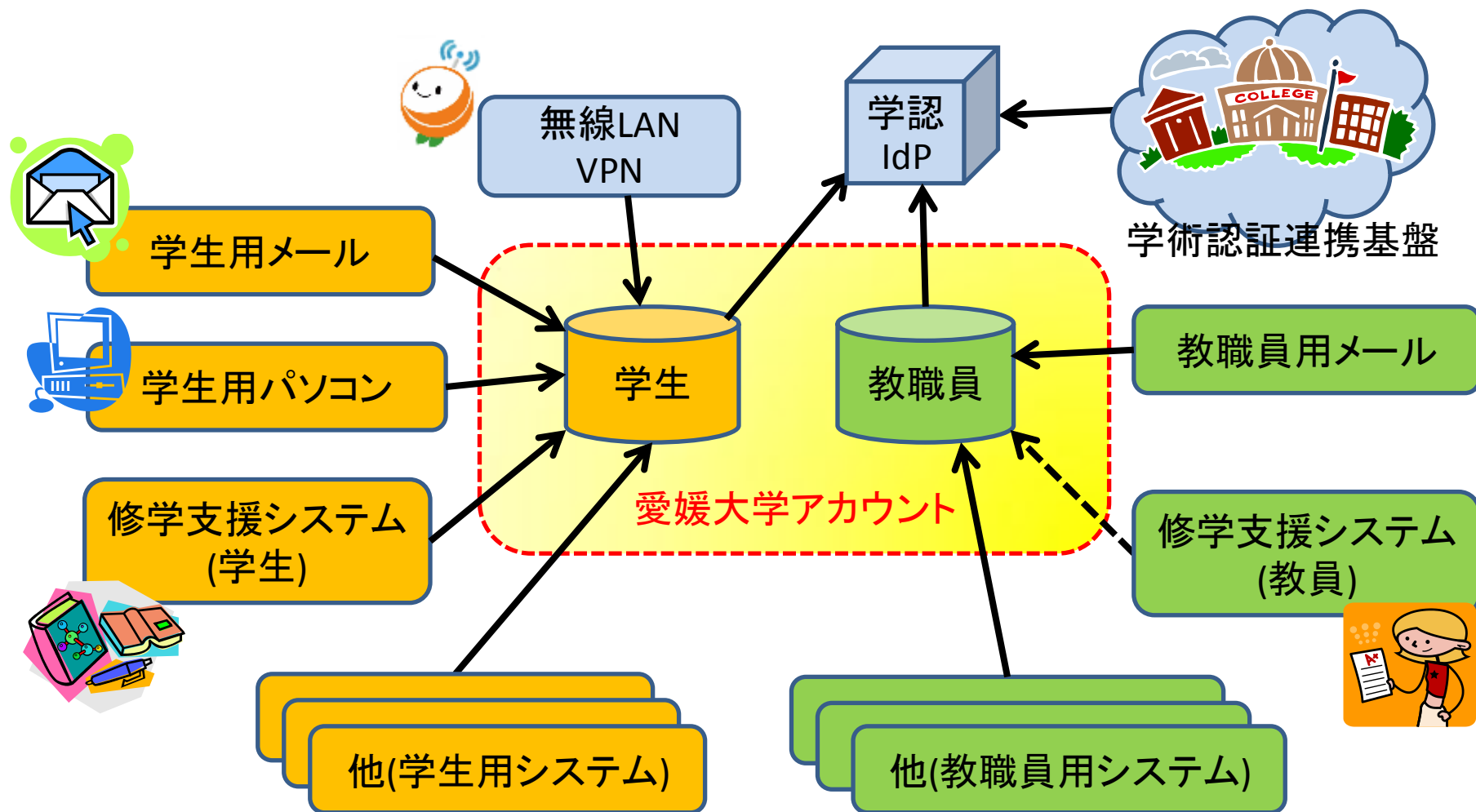
講演者の経歴

- ◆ 2010年5月以前
システムエンジニアとして主に金融系の業務アプリケーションを開発
- ◆ 2010年6月以降
愛媛大学総合情報メディアセンターにて技術員として
主に情報基盤システムの運用・管理に従事

必要な知識・スキル

- ◆ OSのセットアップ(愛媛大学ではCentOS)
 - ◆ 必要なソフトウェアのセットアップ
 - ◆ LDAP, スキーマに関する知識
 - ◆ IdPの設定
 - ◆ ログ解析
- ⇒経験、知識不足のため
理解と構築に時間を要した。

愛媛大学の認証環境



発生した問題

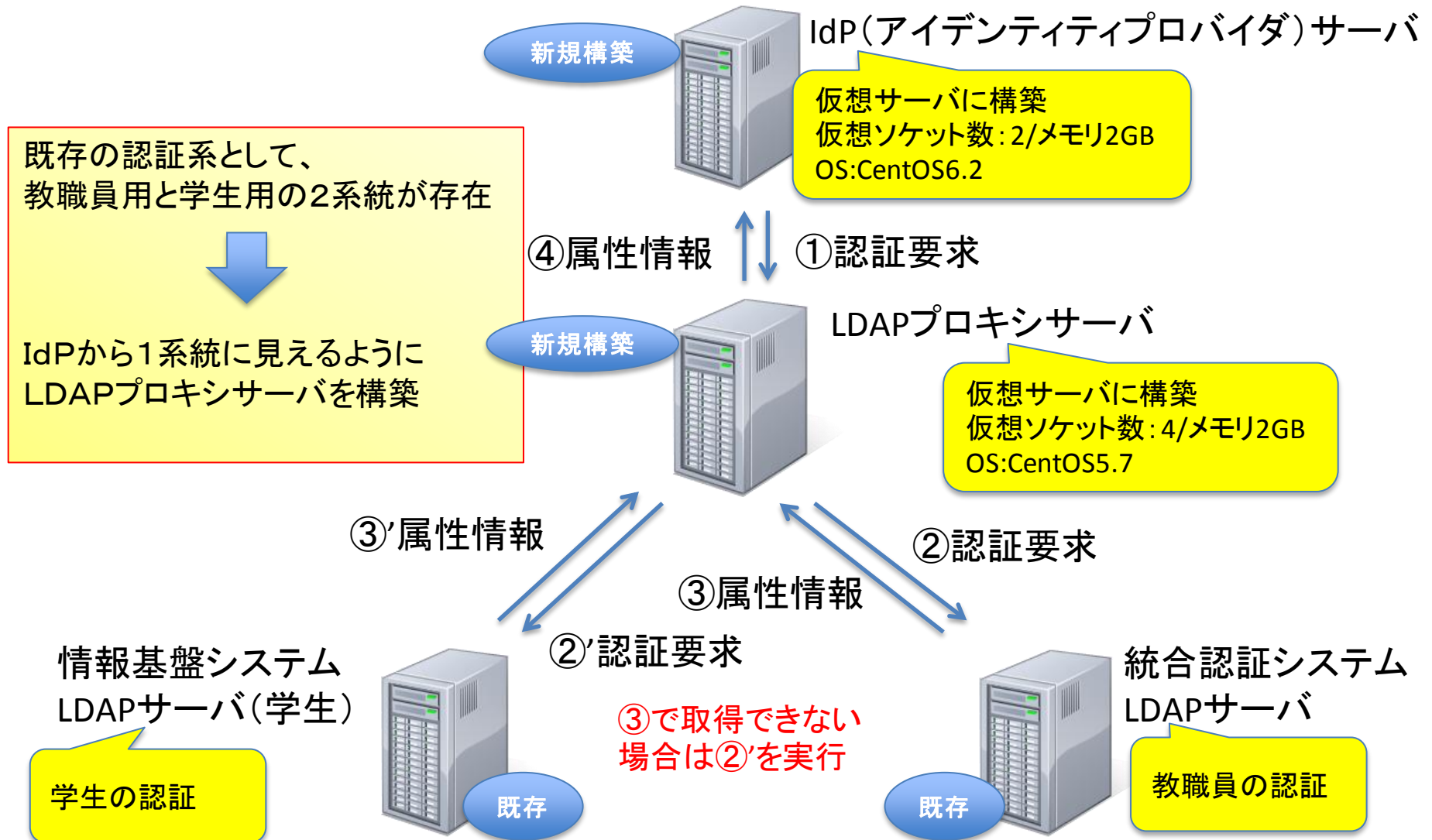
非システムのな問題

- ◆「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。

システムのな問題

- ◆愛媛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。

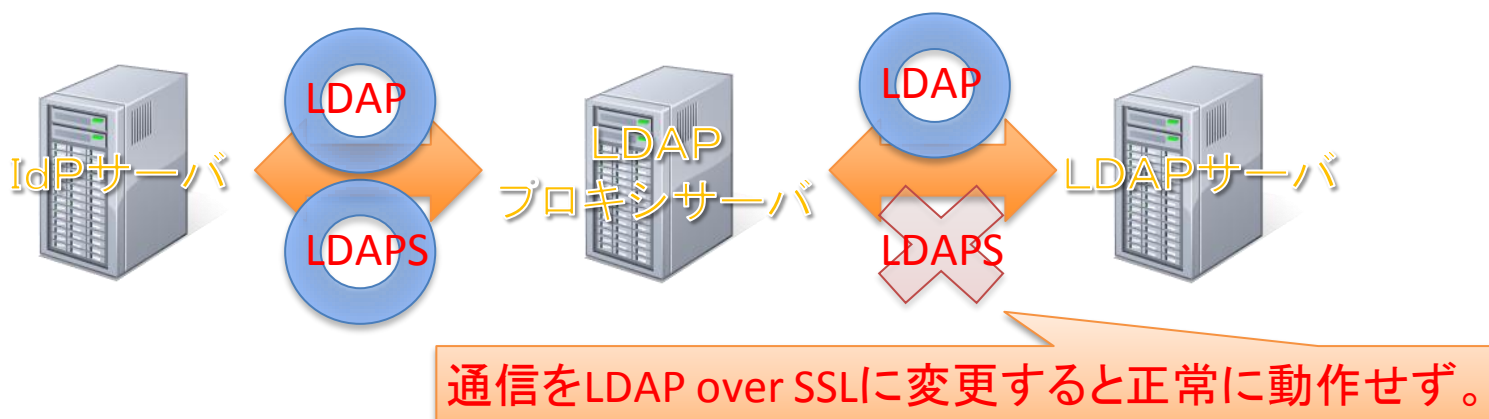
認証環境の構成



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

(赤字斜体が要対応)

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

IdPサーバの構築

OSのセットアップ、Apache+mod_ssl,OpenLdapのインストールまでできれば、NIIの学認ホームページの技術ガイドに記載されている内容だけでほぼ構築可能

主な設定ファイル	主な設定内容
relying-party.xml	entityIDの設定 メタデータ自動ダウンロードの設定
handler.xml	ログインのしくみの設定 ⇒TypeをUsernamePasswordとしlogin.configを参照するだけ。
login.config	認証先のLDAP設定 (LdapURL, baseDN, userFilter, subtreeSearch, SSL)
attribute-resolver.xml	IdPで取り扱う属性情報の設定 属性情報の取得元の設定(LDAP, ComputedID等)
attribute-filter.xml	attribute-resolverで設定した属性情報のうち 送信する属性を各SP毎に設定。

設定ファイルを変更したら必ずプロセスを再起動しログを確認

⇒ /opt/shibboleth-idp/logs/idp-process.log

今後の課題

- ◆ 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

Ehime University - Gakunin Login Page - Windows Internet Explorer

https://... Ehime University - Gakunin...

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)



愛媛大学

学認ログインページ

Ehime University GakuNin Login Page



ここは愛媛大学の学術認証フェデレーションログインページです。
学術認証フェデレーションの詳細については[こちら](#)を参照してください。

学認では、ご利用するサービスによっては個人情報をサービスプロバイダに送信します。ご了承の上ご利用ください。各サービスにて送信される個人情報など、詳細は[こちら](#)でご確認ください。

学 生 : 情報基盤システムのユーザID・パスワードを入力してください。
教職員 : 全学メールのユーザID・パスワードを入力してください。

User ID :

Password:

Login

SPに個人情報を
送信する旨を記載



Shibboleth.



ユーザへの送信属性通知

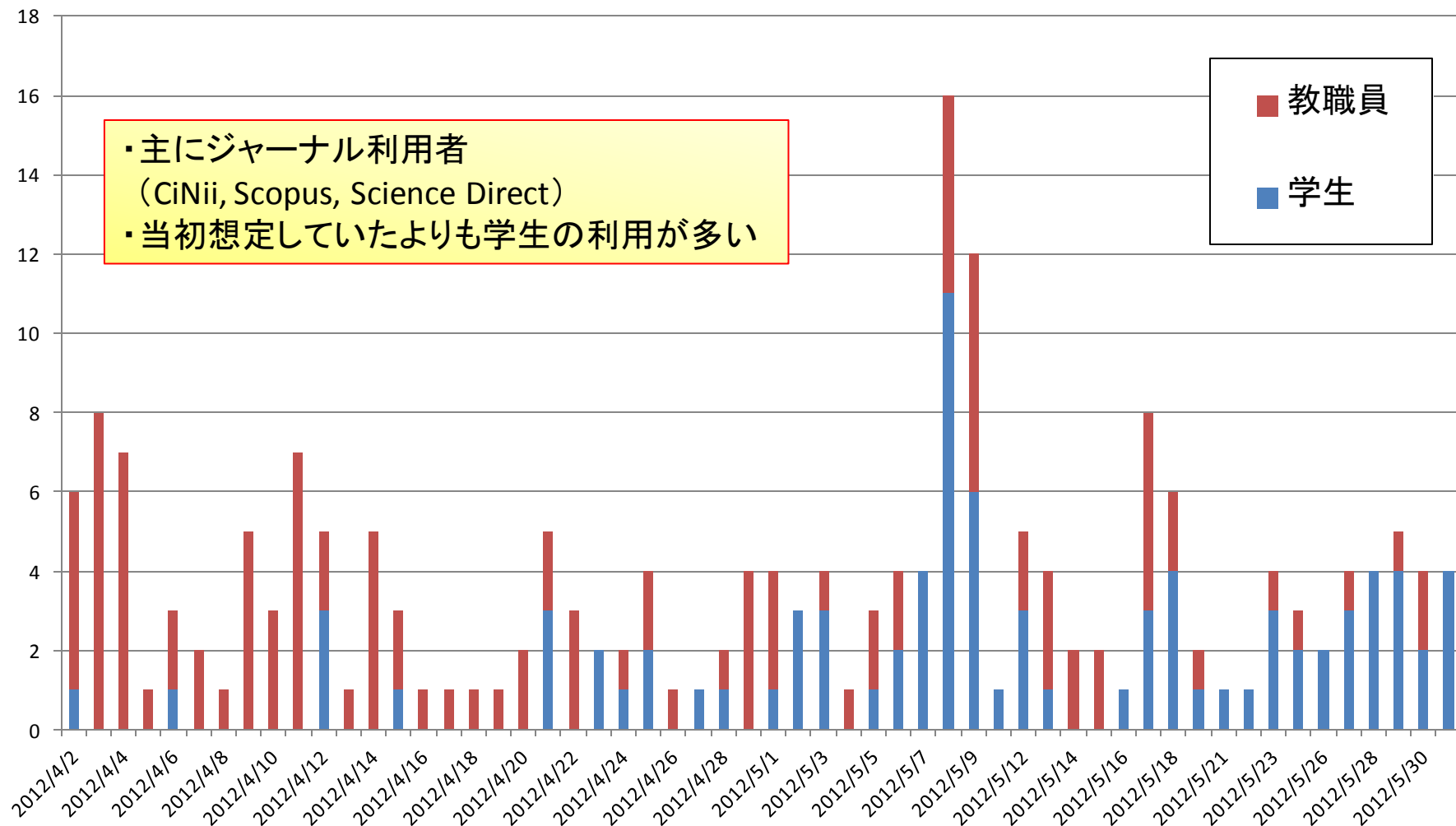
属性名では一般ユーザに
解り辛い、各属性を
右図のように

- ・「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	●			●	●

利用状況



※同一日に同一IDで同一SPを利用しているものはカウント対象外