Shibboleth から始めた学内 SSO 環境

～GakuNin 参加後の 1 年を振り返る～

成城大学メディアネットワークセンター

五十嵐　一浩

成城大学の紹介

・東京都世田谷区の私立文系大学
・1 Campus に 4 学部，同一敷地内に幼小中高
・学部生：5,805 人，大学院生：141 人　(2011/05/01 現在)

メディアネットワークセンター

・大学の IT 基盤設計・構築・運用
・PC, CALL 教室管理・運用
・学内ユーザーサポート
　（教員・学生・事務）
・専任 8名，契約・派遣・委託 6 名

SEIJO! University

そもそもの発端

・2007 年頃より 学内 IC カード導入検討開始
・2008 年夏 学内 PKI インフラ構築の必要性から，NII 様主催の軽井沢セミナーに参加

→ 学内 PKI 構築のハードルの高さを痛感.

→ 一方，学内では Felica ベースで対応アプリケーションを無理やり募集するといった強引な IC カード導入計画が進められていた.

→ 最終的に IC カード導入予算は付かず，中途半端なシステム導入の回避には成功.

研修の成果は？

・学術基盤構築・運用におけるリソース共有の重要性を再認識
- 中規模の文系大学単独では可能性に限界がある.
- 大学の構成員は「成城の学生だけ」を Care していればいいのか？

・忘れてしまいがちな Give & Take の精神
- 成城大学として，どのような貢献が可能（もしくは必要）なのか？

・研修参加者間でのヒューマン・ネットワークの拡張
- 情報センター等技術職員研究会への参加

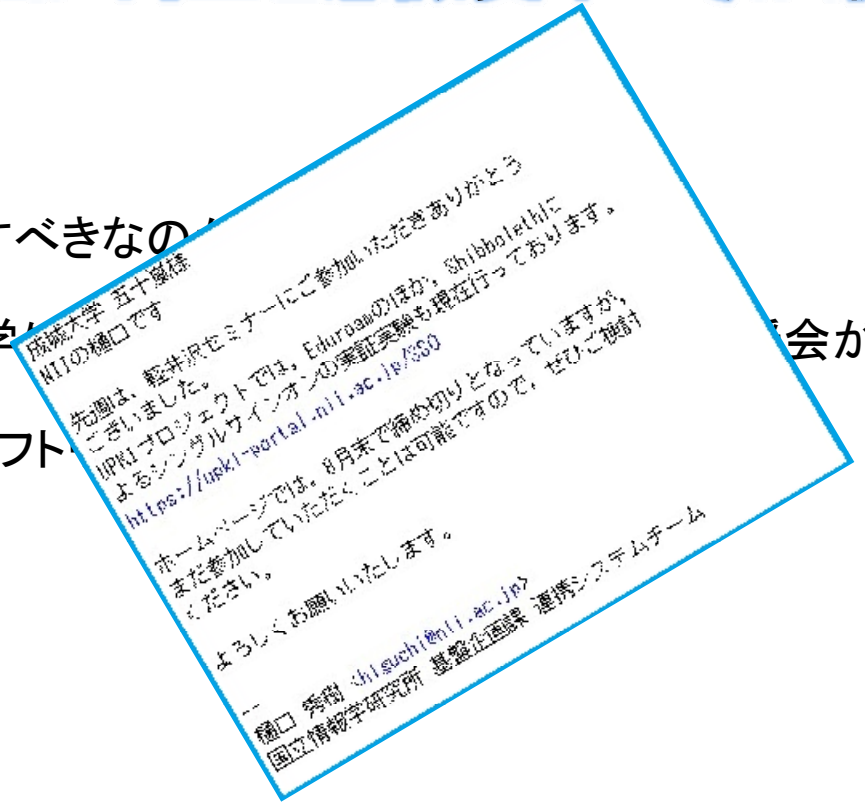
SEIJO! University

モチベーション向上と意識変革こそが最大の成果物

・何から着手すべきなの

・eduroam は学 会がうるさそう…

・提供できるソフト



Shibboleth の情報収集開始

→ 情報交換会にて曽根原先生や山地先生と出会う

「Shibboleth IdP は **Filter** !」

SEIJO! University

成城大学での認証基盤再考の背景

・認証基盤整備が遅れていた成城大学では，SSO を意識しない部署毎の Web サービス導入が始まった.

・SSO 化を希望するユーザーの声も弱かったため，商用製品を導入するには予算確保が困難であった.

・大学が契約している電子ジャーナルの利便性向上については，図書館担当者も含め，より簡便な仕組みが求められていた.

・肝心な学生からの SSO 化要望を組み上げる仕組みも存在しなかった.

Shibboleth から始めてみよう.

[Pros]

・導入予算不要の為，センター主導の Small Start で基盤構築可能.

・GakuNin へ参加すれば NII 様提供の Web サービスも有効活用できる.
→ Casify ? or Shibbolize ? の答え

・図書館システム連携のトリガーになると期待.

[Cons]

・各部署管轄の既存 Web サービス改修にはコストがかかってしまう.

SEIJO! University

Shibboleth IdP 先行構築のアプローチ

（SSO 基盤が存在しないという前提）

学内の Shibbolize が完了してから GakuNin へ参加ではなく,
GakuNin へ参加してから学内 Web サービスを段階的に Shibbolize .

→ 既存認証基盤へ影響を与えず，サービス拡張可(DreamSpark, Fshare etc)

→ 外的要因による管理対象属性の整理促進

→ ユーザーに SSO の便利さを部分的にでも体感してもらえる.

→ 特に成城の場合，実装しないと話が進まない.

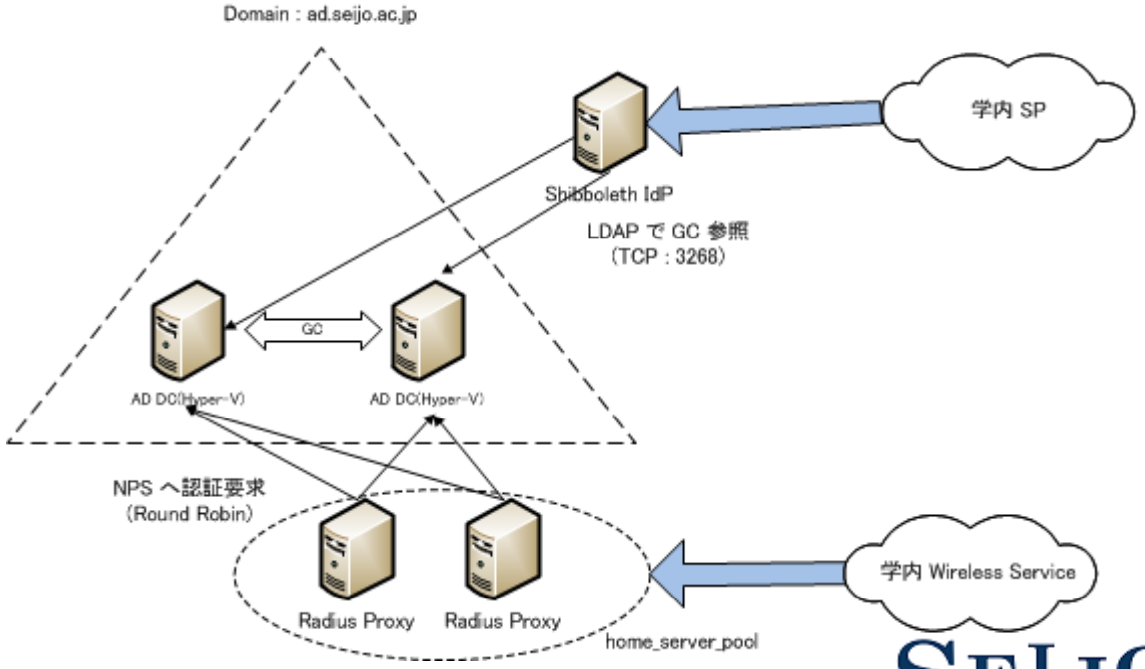
→ 他大学の学生が利用できるサービスを成城の学生達が利用できない
　となれば，それは管理者である自分の責任.

SEIJO! University

Shibboleth 導入の経緯

・2009 年 12 月　テストフェデレーション参加
・2010 年　3 月　教員・学生認証環境統合
・2010 年　4 月　運用フェデレーション用 IdP 構築と GAKUNIN へ参加申請
・2010 年　5 月　GAKUNIN への参加承認
　　MS DreamSpark，NII Fshare, eduroam-shib 等活用
・2011 年　4 月　ALC NetAcademy2 の Shibboleth 認証統合
　　Yahoo!Mail Academic Edition の Shibboleth 認証統合

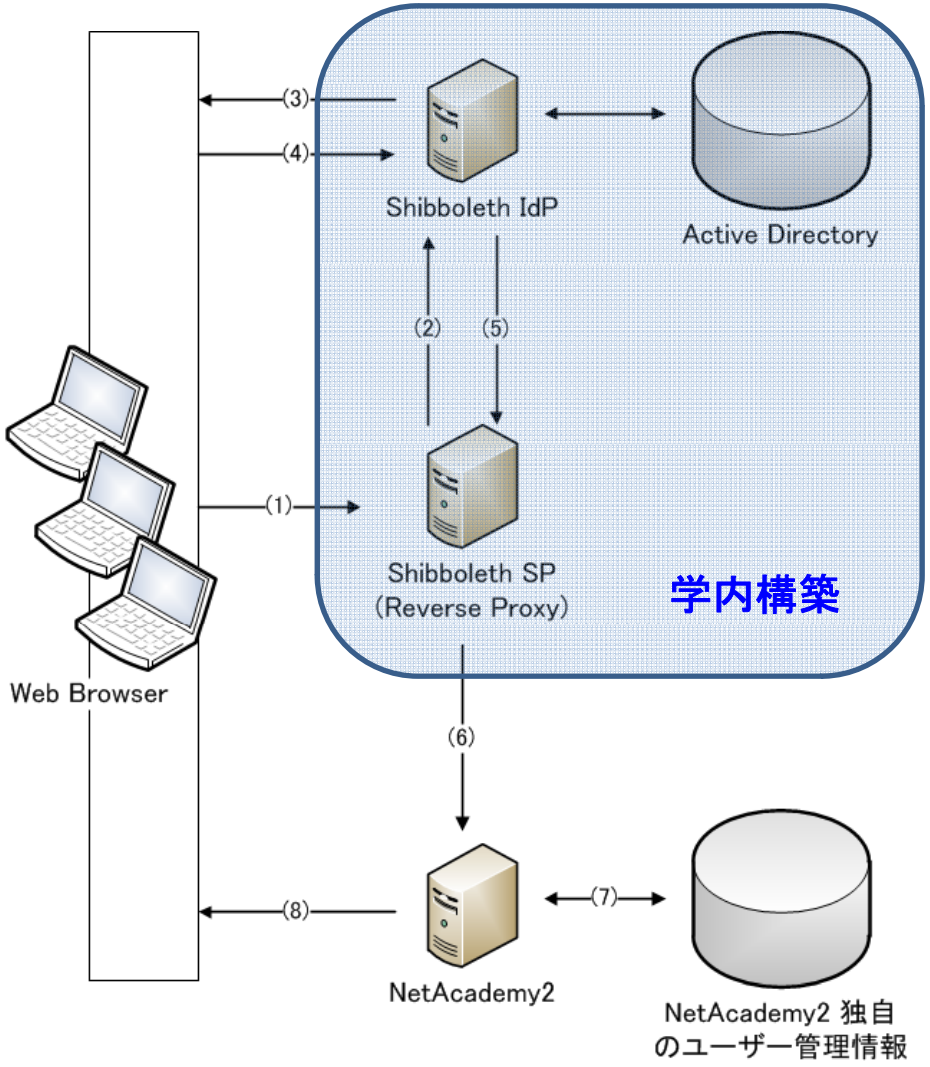
■成城大学認証基盤構成



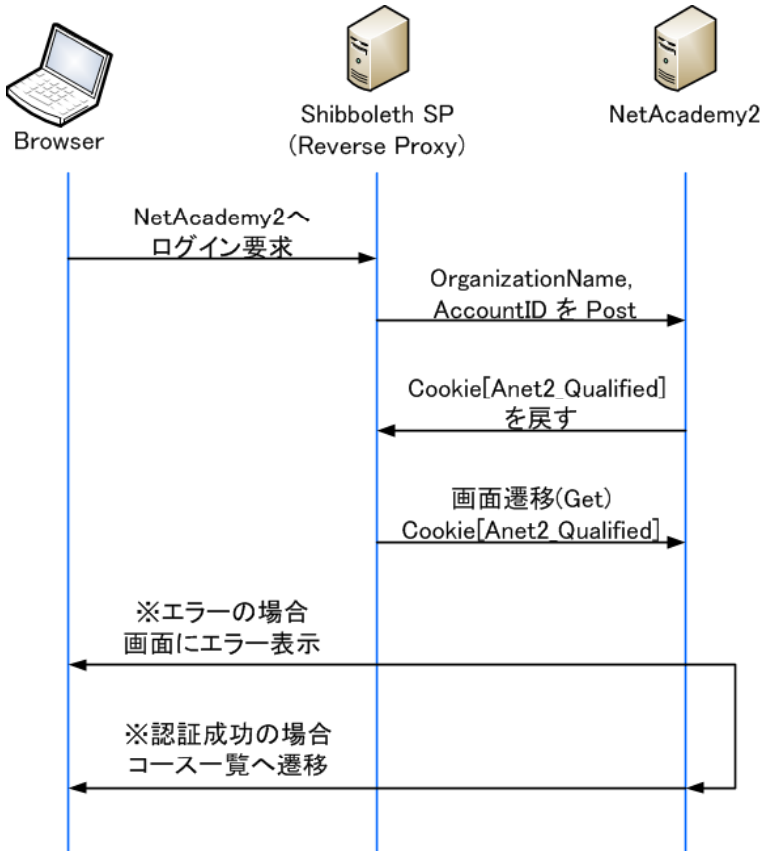
SEIJO! University

ALC NetAcademy2 の Shibboleth 対応

■ 構成概要



■ 認証情報の受け渡し

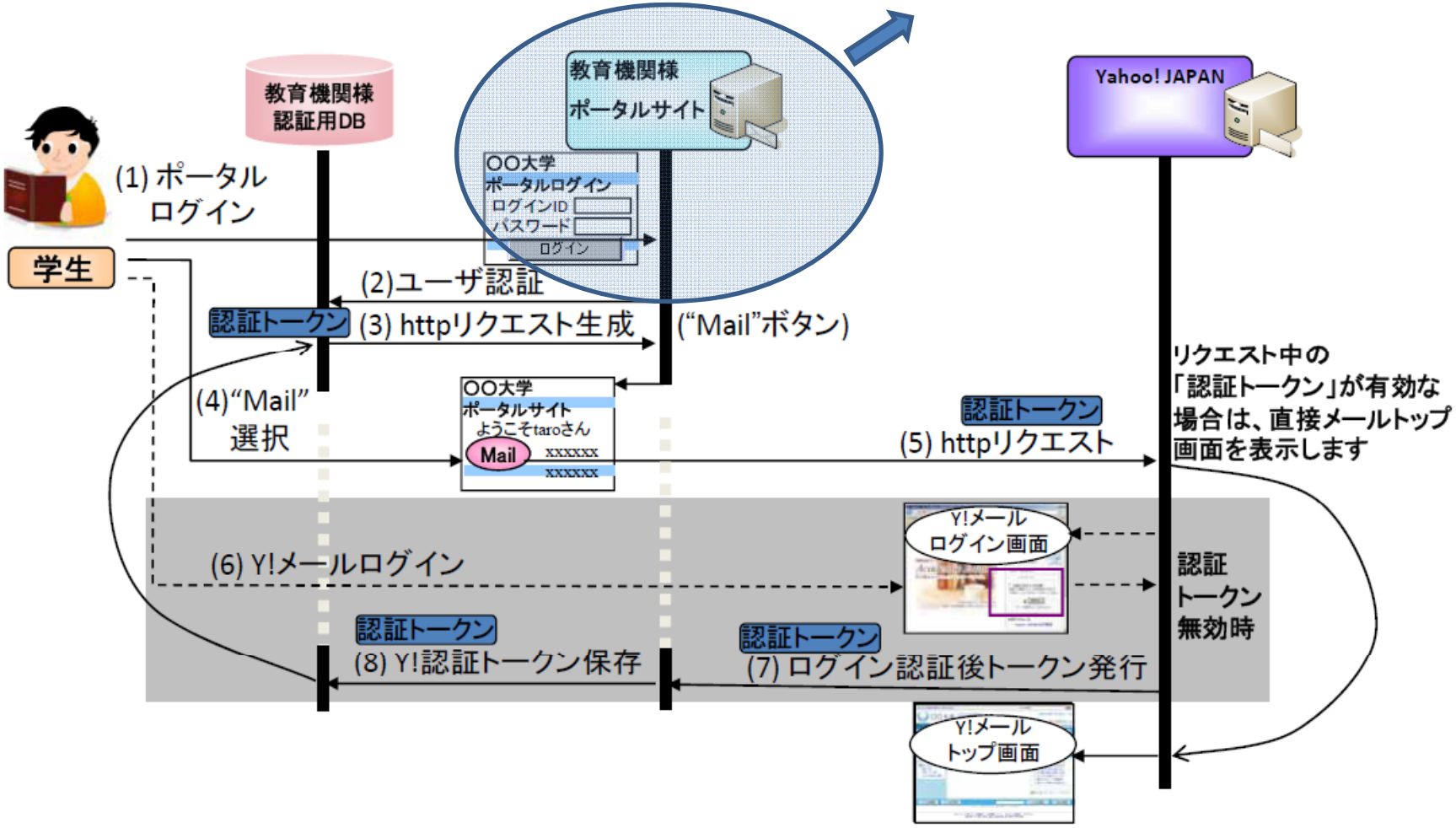


SEIJO! University

Yahoo!Mail Academic Edition + AEAuth

Yahoo! の API には $_SERVER[eppn] を渡す
$_SERVER[unscoped-affiliation] で利用者制限

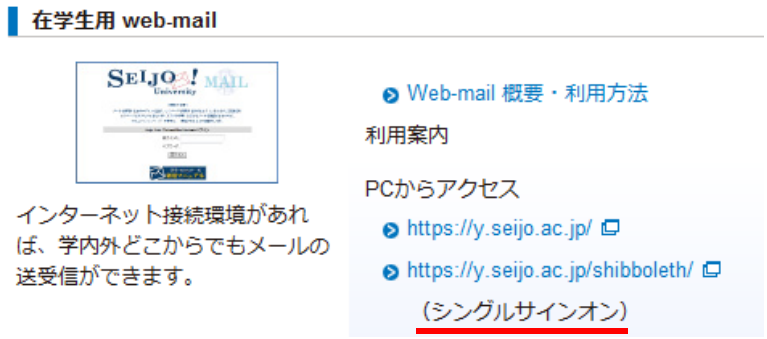
概要フロー



SEIJO! University

ユーザーからのフィードバック

- DreamSpark がすぐ利用できた！
- Fshare はうれしい機能，だが送信先の自由度が低い…
- eduroam-shib もうれしいが，首都圏外の出張先で利用できないことが多い
- 結局自分が利用したい電子ジャーナルは VPN 張らないといけない…
- ユーザーから反応がないが，実は便利に感じているのでは？
  Yahoo! Mail は 2011 年 4 月からこっそり SSO リンクを追加しただけだが，
  述べ 600 以上のログインあり



- 2011 年 4 月から SSO 化した ALC NetAcademy2 はログイン回数述べ 10,000 以上
  学習者人数も前年度比で約 35% 増加

SEIJO! University

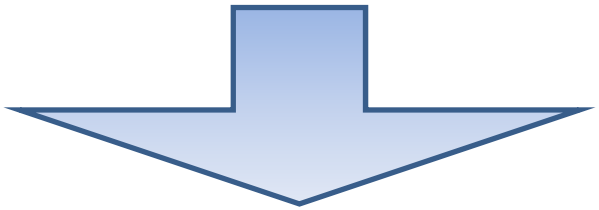
学内で SSO は普及したのか？

・Campus Square（学事システム）や Webclass（e-larning） 等の Web システムが独自認証.

・部署毎導入の商用アプリケーション SSO 化は実装優先順位が低い.

・しかしながら，ユーザーが SSO 非対応サービスを「不便」に感じはじめているのは事実である.

まだまだ基盤を管理するセンター主導で工夫できることもあるのでは？

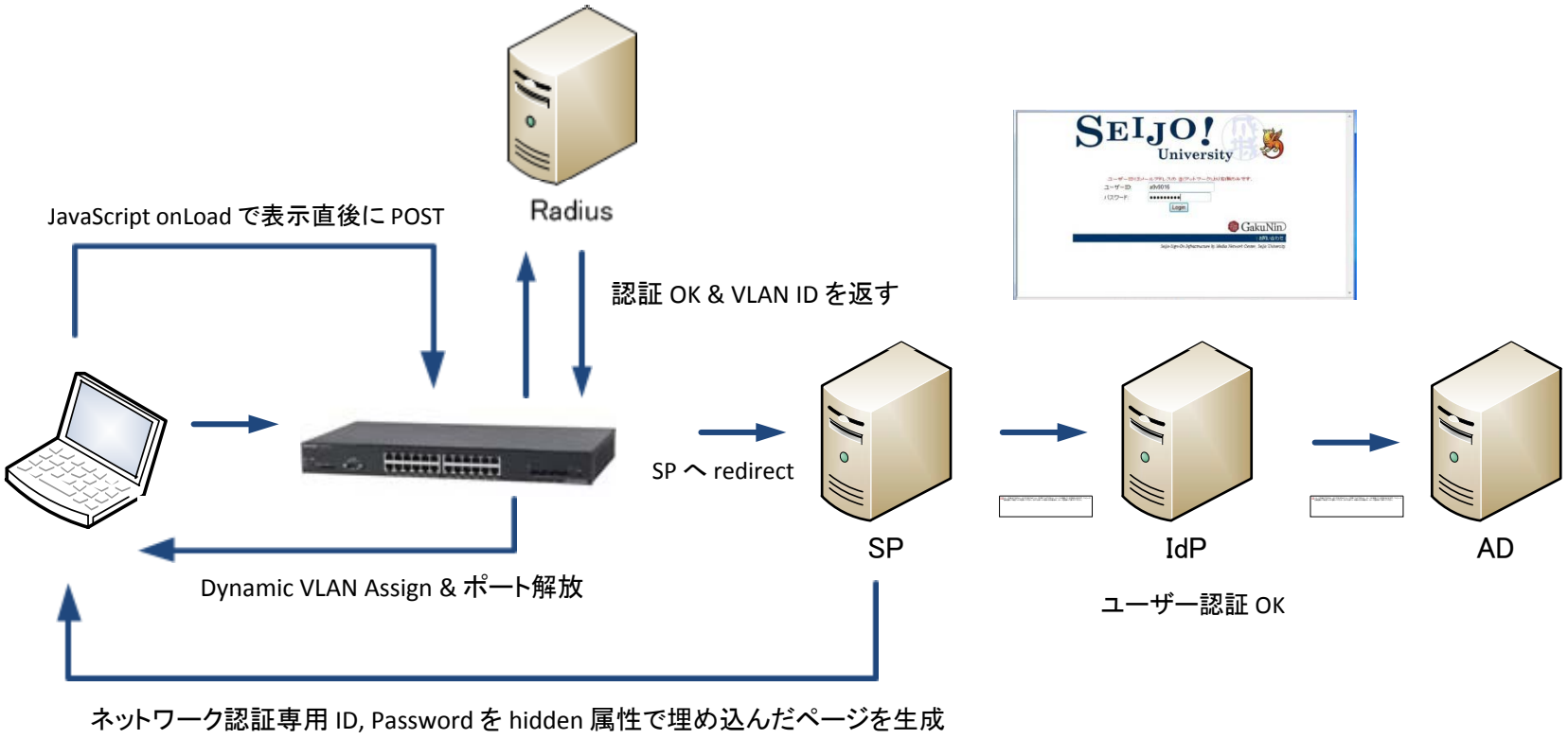


ネットワーク認証の SSO 化

SEIJO! University

Shibboleth ネットワーク認証の動作概要

(AlaxalA 社 AX2530S 利用：島ハブ経由の Dynamic VLAN 割当や, 中間証明書の Install が可能)



・個人のアカウント情報を利用しないので，Dynamic VLAN の管理も楽になり，情報漏洩時のリスクも最小限に抑えられる.
・SP と Radius を同一サーバーで構築することで，認証情報の同期や スイッチ ACL の設定も簡略化できる.

SEIJO! University

Shibboleth側の考慮点

・IdP, SP 共に，Session 中でクライアント IP Address のチェックをしているため，
Dynamic VLAN 割当により IP Address が変わってしまうと再認証を要求される.

IdP 側で Session IP check を無効にする！

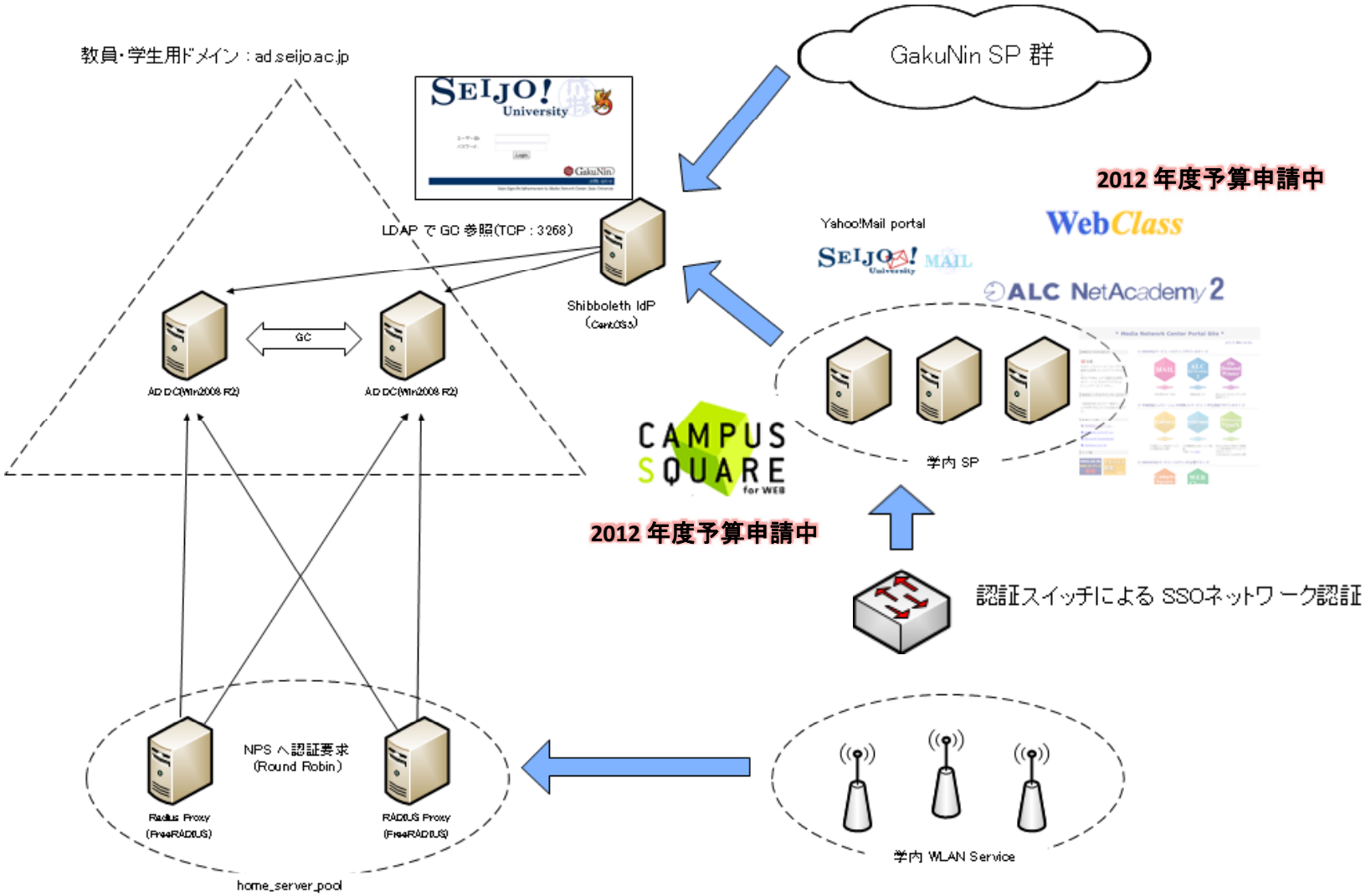
src/shibboleth-identityprovider-バージョン/src/main/webapp/WEB-INF/web.xml を編集して idp.war を rebuild

```
...
   <filter>
      <filter-name>IdPSessionFilter</filter-name>
      <filter-class>edu.internet2.middleware.shibboleth.idp.session.IdPSessionFilter</filter-class>
      <init-param>
         <param-name>ensureConsistentClientAddress</param-name>
         <param-value>false</param-value>
      </init-param>
   </filter>
...
```

※SP 側でも Session IP check を無効にできるが，別 SP 利用時に再認証要求されるので
実用性が低い.

SEIJO! University

2012 年度の成城大学認証基盤と SP



SEIJO! University