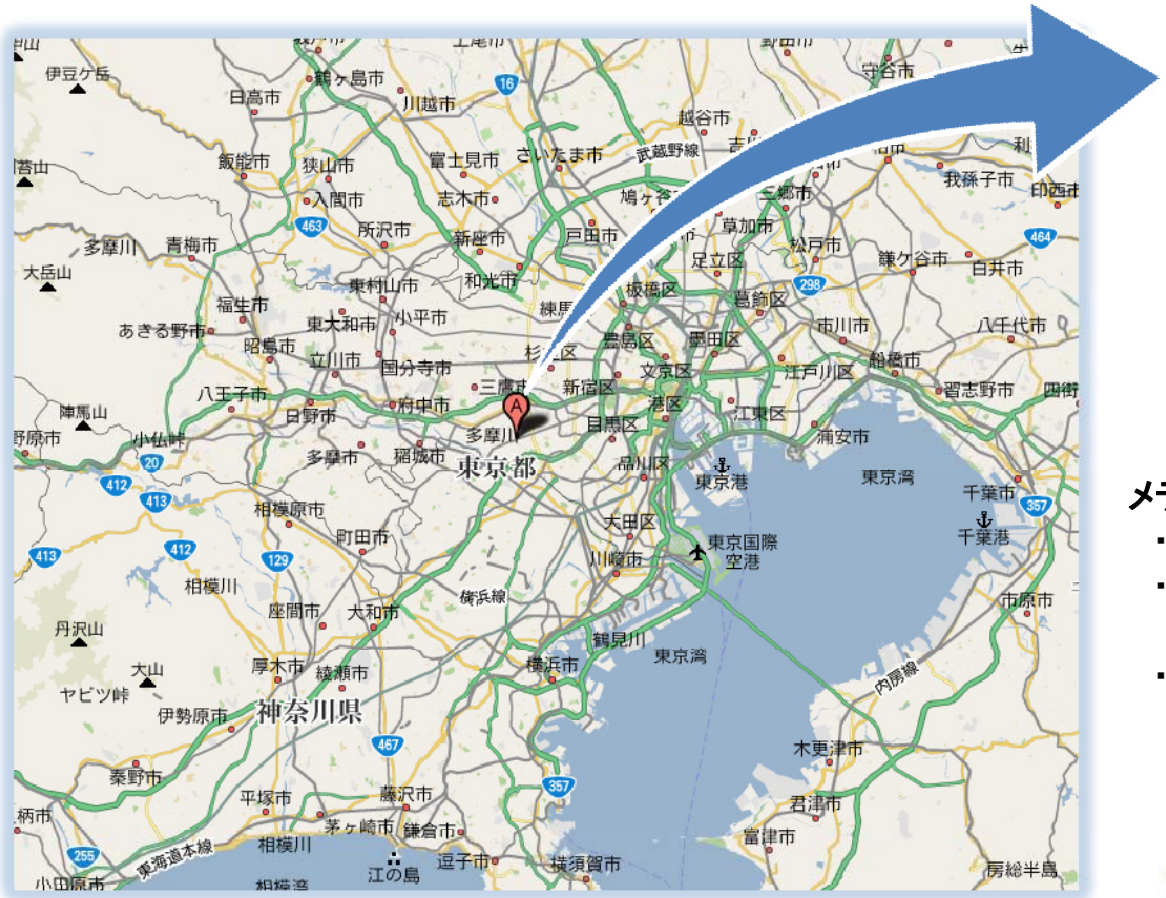
SSO 基盤構築のための Shibboleth-Driven Approach

Dec. 13th, 2010

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あり
・学部生：5,854 人，大学院生：145 人　(2010/05/01 現在)



メディアネットワークセンター
・大学の情シス+語学教育サポート
・専任 9名，派遣・委託 7 名

・そのうち IT 基盤設計・構築・運用
チームは専任 2 名，委託 1 名
派遣 1 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.

研修の成果物は？

・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.
- 大学構成員は「自大学の学生だけ」を Care していればいい？

・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（or 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

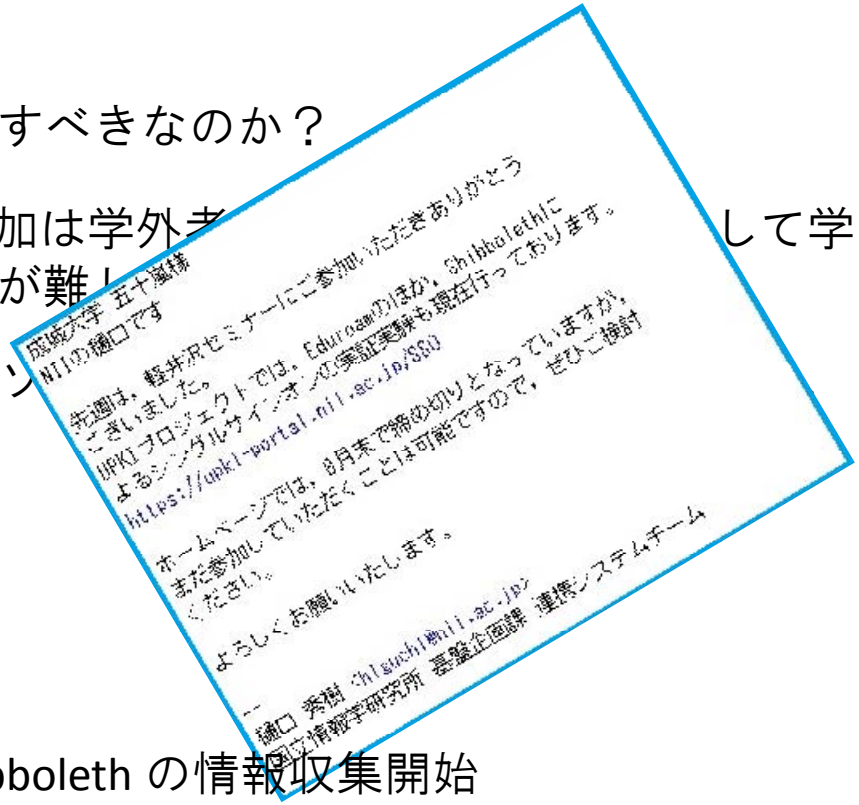
SEIJO! University

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か？

・eduroam 参加は学外者 して学内コンセンサス
を得ることが難し

・提供できるソ



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 の解

・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のもとに）

学内の **Shibbolize** 完了を待って **GakuNin** へ参加するのではなく，
GakuNin 参加を原動力として学内 **Web** サービスの **SSO** 化を促進 .

→ 既存認証基盤へ影響を与えず，サービス拡張が可能
(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

導入前の苦労

「とにかく，あるものだけで **(Idp** を**)** つくる！」というリソース制約

1. H/W
   → 幸い仮想化されたサーバーファームがあったので活用
2. IdP 構築作業
   → UPKI サイトの技術ガイド
3. LDAP データソース
   → 既存 Windows Active Directory に直接接続
   → 山形大学伊藤先生の Active Directory 環境構築事例を参考に.
   Active Directory スキーマ拡張については Internet2 サイト参照.

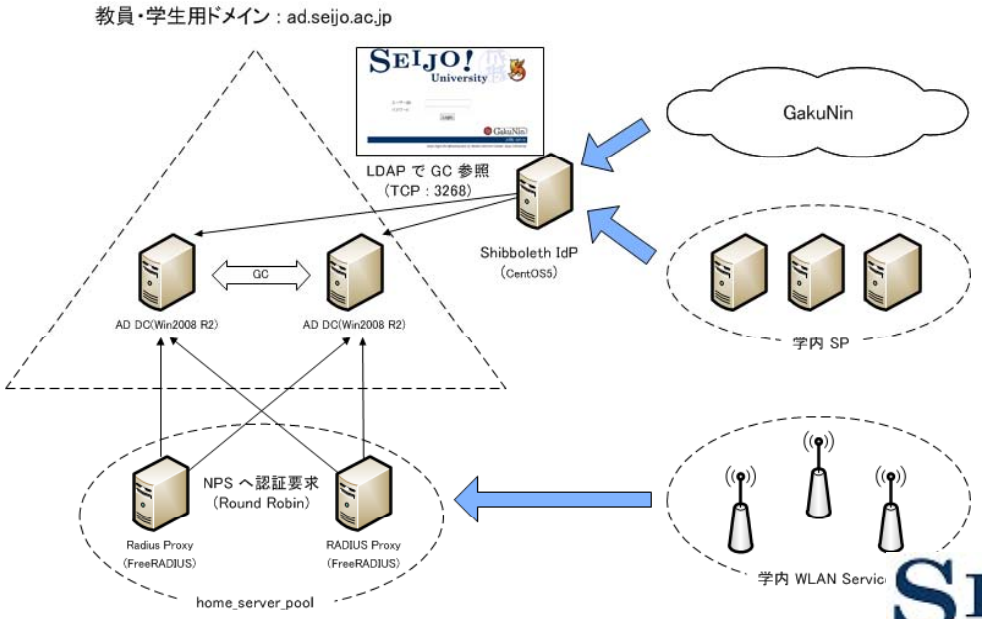
→ その他，情報交換 ML 等，多くの皆様のおかげで無事テストフェデレーション参加準備が完了.

SEIJO! University

Shibboleth 稼働までの経過

・2009 年 12 月　テストフェデレーション参加
・2010 年　3 月　教員・学生の認証環境統合（別ドメインで運用してい）
・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
（GakuNin 参加については，センター委員会の事業計画説明時に報告し，委員会の承認を得た．）
・2010 年　5 月　GakuNin への参加承認
・2010 年　7 月　学内 Web サービスの Shibboleth 化着手

■成城大学認証基盤



SEIJO! University

現在進行中のタスク

■成城大学としてできること（１）

→　公開 SP を独自開発・提供するだけの体力はない為,
　関連ベンダーに Shibboleth 化を強く要望していく

・語学 e-learning アプリケーション（商用）の Shibboleth 化共同開発
　ALC 社 NetAcademy2 で Reverse Proxy 経由の SSO
　2011 年 4 月よりサービスイン

・電子ジャーナルの Shibboleth 対応を図書館と共同で要望中

・学生用 Portal 構築と Shibboleth 化検討

■成城大学としてできること（２）

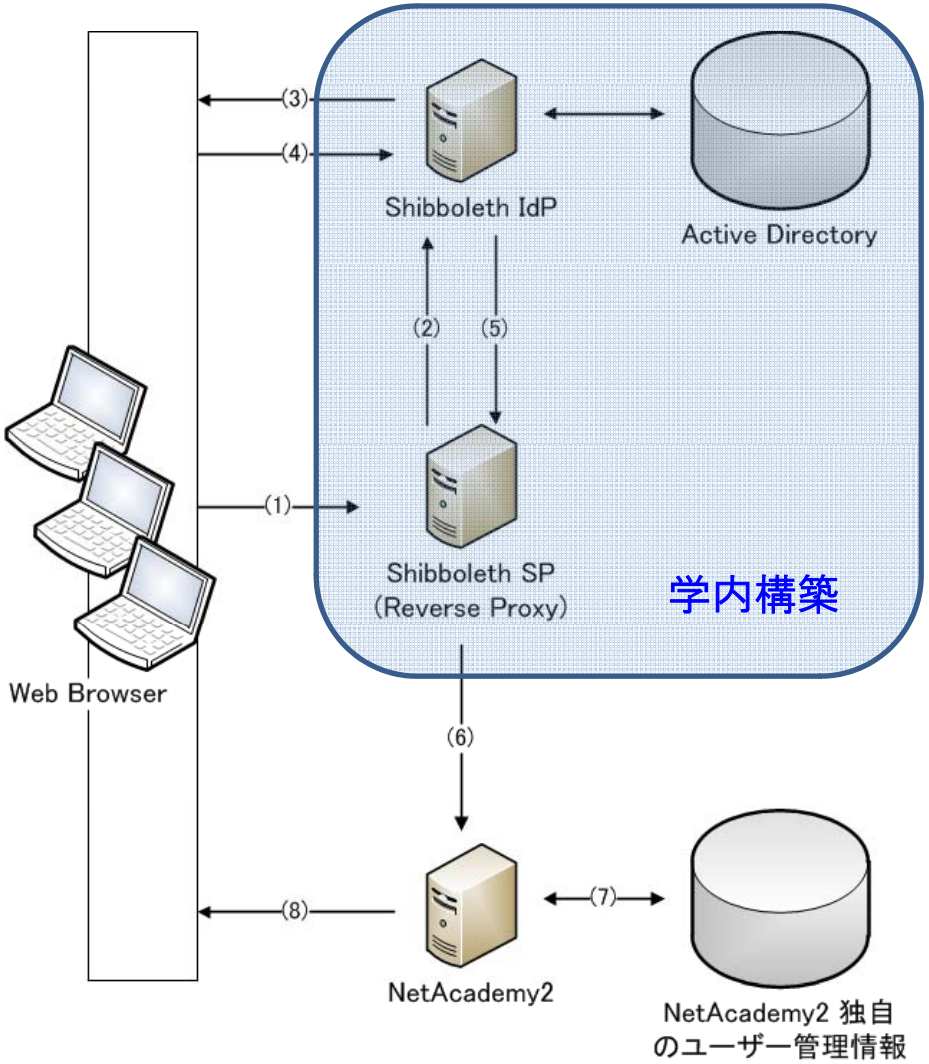
→　内部開発 Know-How の公開

・Yahoo! Mail Academic Edition(学生用メール) の AEAuth 認証を Shibbolize
　LDAP 経由での認証とは別の入り口で実装

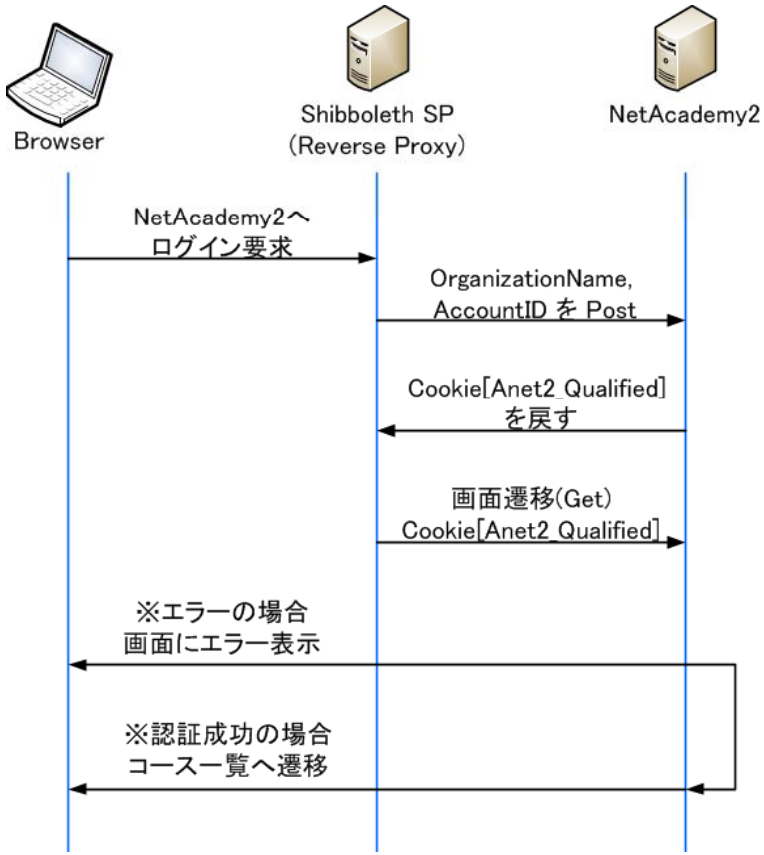
SEIJO! University

ALC NetAcademy2

■ 構成概要



■ 認証情報の受け渡し

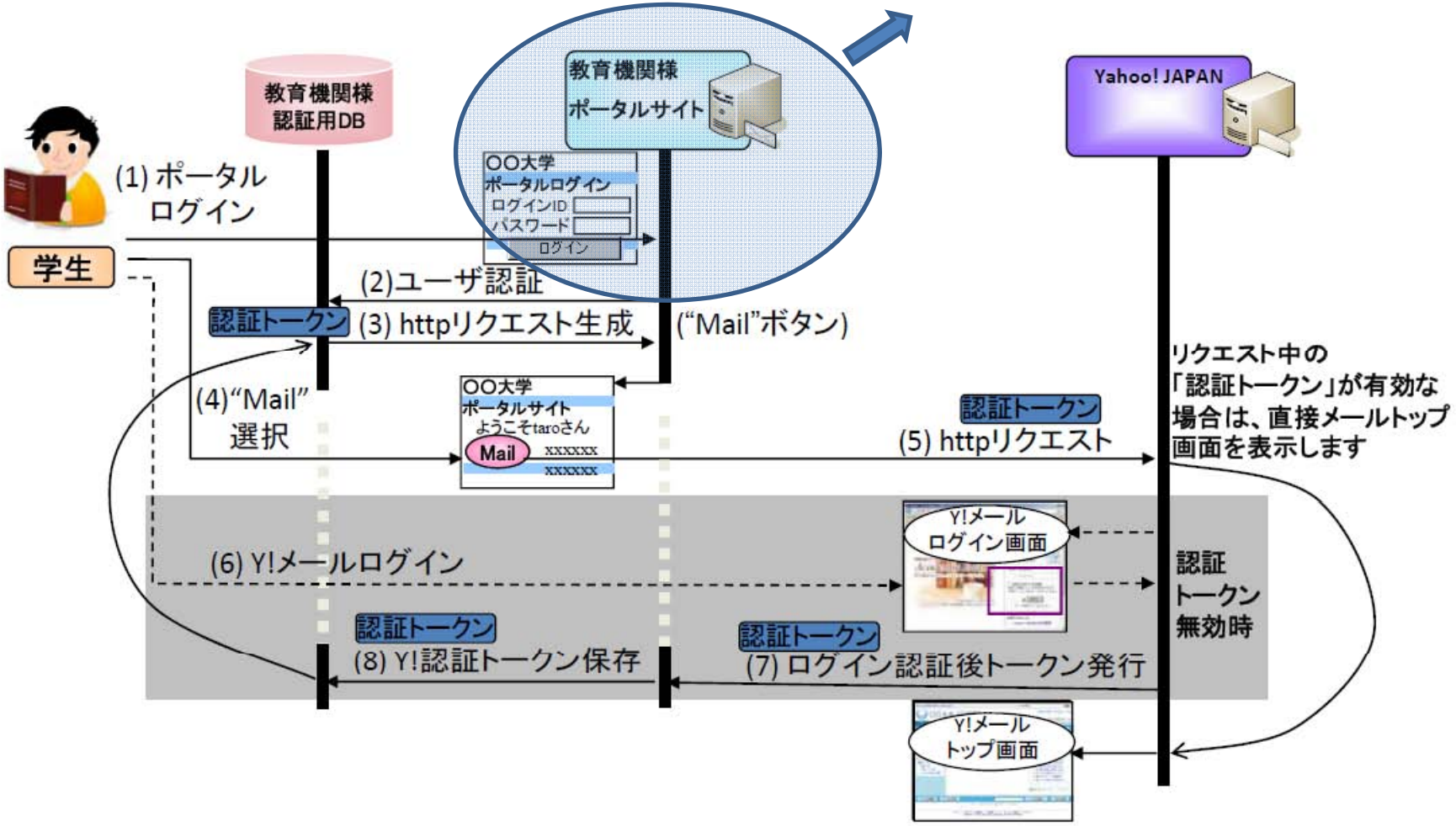


SEIJO! University

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

今後の課題

・Load Balancer を活用した IdP の冗長化(2011 年度予算申請中)
　SP の増加前に冗長化/負荷分散

・教員用 Webmail
　Shibboleth 対応実績のあるシステムへ更新検討中

・部署毎導入商用アプリケーションの Shibbolize
　SSO 実装の説得と予算確保(Campus Square,シラバスシステム etc)

・WLAN Service の認証一元化
　Opengate SSO は学内環境だけを考えると魅力的.
　eduroam や認証 switch によるネットワーク認証実装との兼ね合いも
　要検討

・組織改編も視野に入れたシステム設計/運用設計変更
　事務系システムや幼小中高は別の認証基盤
　組織横断的なアプリケーションを SSO 化するのが難しい
　(Cybozu Garoon は学園管轄…)

SEIJO! University