佐賀大学における
シングルサインオン実証実験報告

佐賀大学
総合情報基盤センター
江藤博文

はじめに

- 佐賀大学における、シングルサインオン実証実験の状況について報告
- Web インターフェイスを使ったネットワーク利用認証Opengateへの組み込み
  - ネットワーク利用をポータルへのゲートウェイに
- その他のアプリケーションの構築状況

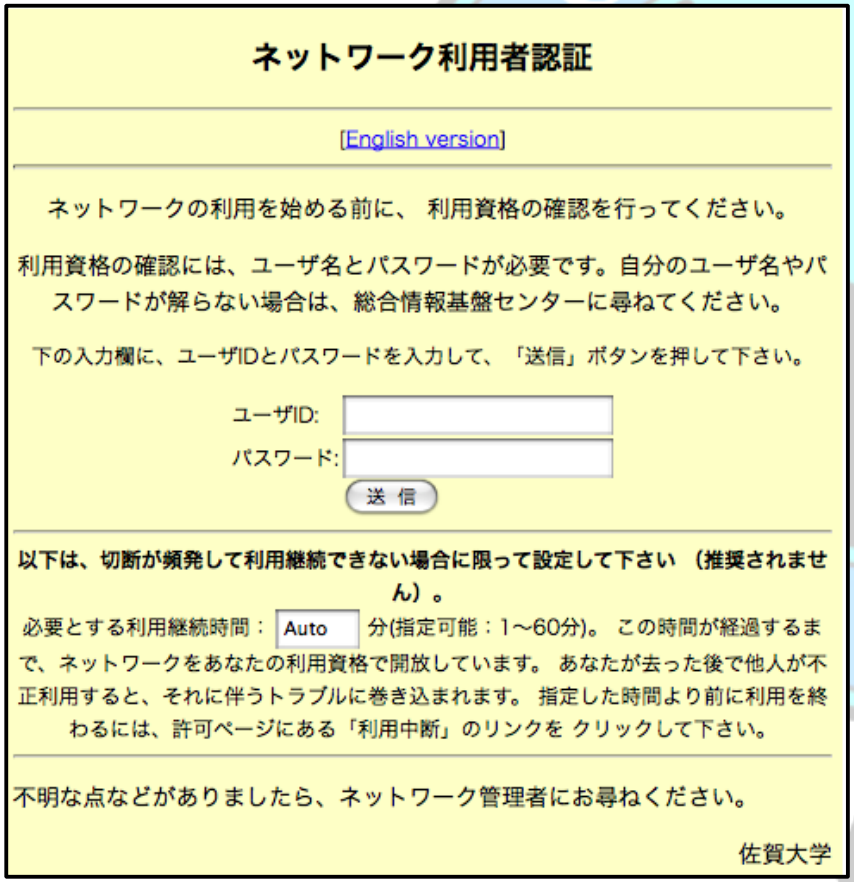
佐賀大学での取り組み

- 共通的情報システムのシングルサインオンによる統合を計画
  - 利用者情報統合をさらに推進
- ネットワーク認証システムOpengateをシングルサインオン化
  - ネットワーク利用がシングルサインオンとなる
- Opengateから大学ポータルへ呼び込む
  - ネットワーク利用開始直後にポータルを表示

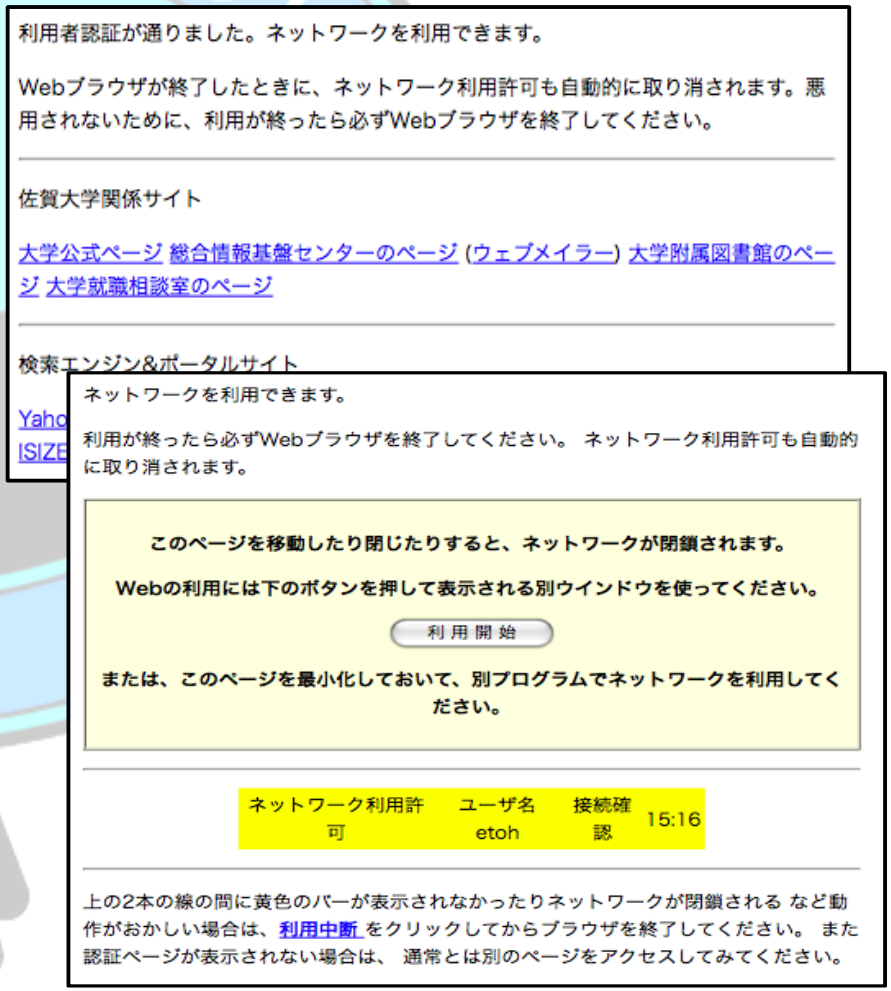
Shibboleth対応Opengateの開発

- Opengate
  - 佐賀大学で開発、運用しているネットワーク利用者認証システム
  - 学生などの持ち込み端末の利用に使用
  - 佐賀大学内に全学規模で導入
- 利用方法
  - 利用者のブラウザ起動後の任意のページへのアクセスを横取りし、認証ページを表示
  - 認証後、ファイアウォールを開き、ネットワーク利用を開始
  - 同時にログイン状況、利用案内のページを表示
    - 利用案内ページをポータルとする可能性
  - ブラウザ終了をネットワーク終了ととらえ、ファイアウォールを閉鎖

従来のOpengateの画面遷移



利用者認証



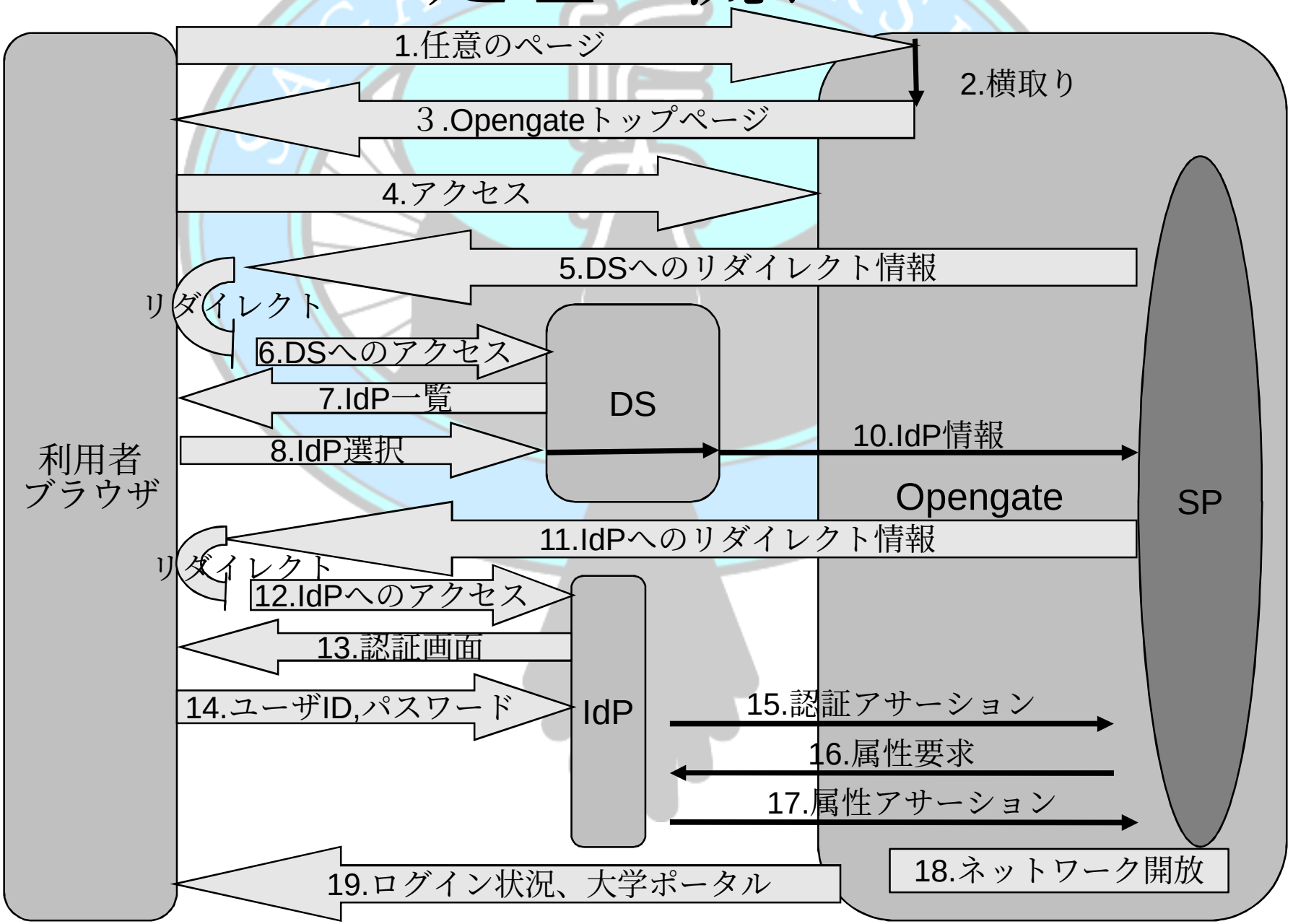
認証ページ

ネットワーク利用許可

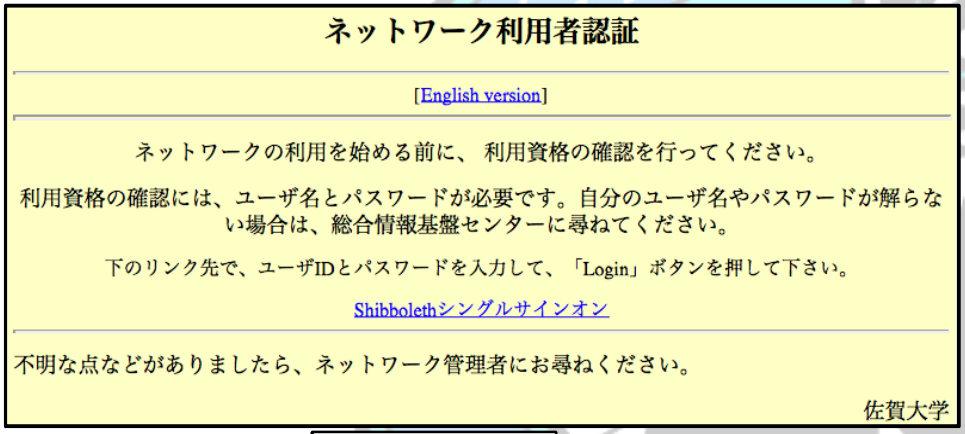
Shibboleth対応Opengate

- 現在のOpengateとの相違
  - Opengateそのものが認証を行わない
  - 初期画面はDSへのリンクのみを表示
- 利用の流れ
  1. 任意のページへのアクセスを横取り、初期画面を表示
  2. DSへのリンクで、DS画面へ移動
  3. 大学のIdPを選択し、IdP認証画面へ移動
  4. 認証後、ファイアウォールを開放、ネットワークの利用許可、ログイン状況と利用案内のページを表示
  5. ブラウザ終了でファイアウォール閉鎖

Shibboleth対応Opengateの処理の流れ

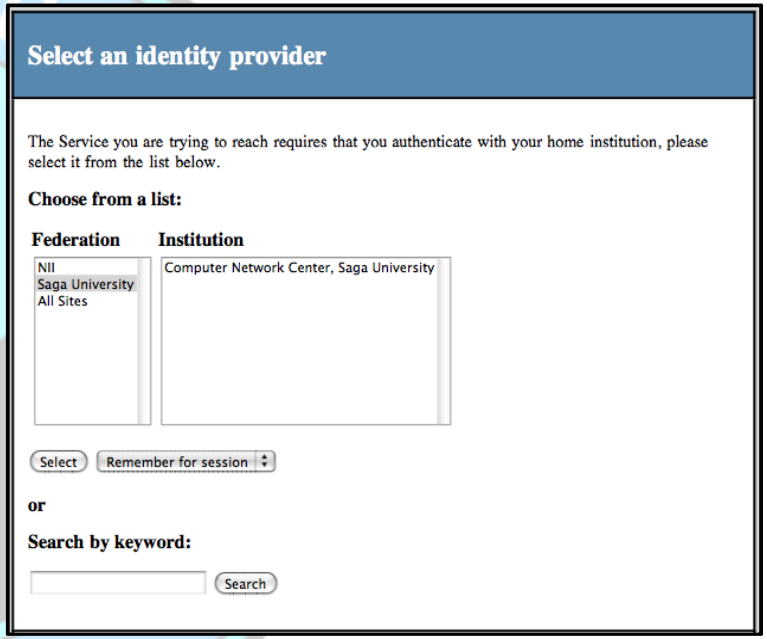


Shibboleth対応Opengate 画面遷移



初期画面

DSへ

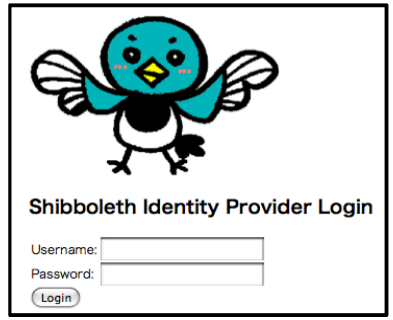


DS、IdP一覧画面

IdP選択

ログイン状況&利用案内画面

認証



IdP認証画面

Shibboleth対応Opengate

- Shibboleth対応の利点
  - ネットワークの利用開始とシングルサインオンを同時に実現することによる利便性向上
  - ポータルサイトに導く事による、大学からのスムーズな情報の提供が実現可能
  - NII シングルサインオン大学間連携による他大学の利用者へのサービス提供が実現可能
  - ネットワーク利用者認証システムであるOpengateを基本的情報システムへのアクセスゲートウェイに

課題

- ゲスト用認証
  - 現在のOpengateには学外者一時利用の認証を持っている
  - 学内の利用者とは別に、ゲスト認証用IdP構築が必要
- 他大学との認証連携
  - NIIの大学間の認証連携に連動することで、認証連携に参観している他大学のIdPで他大学の利用者の認証が可能
  - eduroamよりもローミングが容易可能
    - 利用者にとって容易

課題

- 他大学のIdP変更への対応
  - Opengateでは、ネットワーク利用者認証前はファイアウォールを閉鎖
  - IdPへのみファイアウォールを開放
  - 他大学のIdP変更に対応するため、NII共有メタデータの情報を元に動的にファイアウォールを変更
- 属性情報
  - NIIと学内での必須属性が異なる
  - SP毎に提供する属性をIdP側で区別する設定

課題

- シングルログアウト
  - 現在のShibbolethはシングルログアウト未対応
  - ブラウザ終了により利用終了を判断
- 長時間放置によるのファイアウォール閉鎖
  - Opengateでは、長時間パケットが流れなくなると自動でファイアウォールを閉鎖
  - 再度IdPへアクセスにより、IdPの持続時間内では認証無しでネットワークが開放
  - IdP及びSPの持続時間を要検討
- IdPの負荷実験

IdP、SPの構築状況

- 本実証実験において、佐賀大学で行ったShibbolethに対応の各種アプリケーションの構築状況
  - IdP
  - SP
    - Plone
    - Moodle
    - Drupal
  - DS

IdP構築

- OS及び各種ソフトウェア
  - Solaris10 5/08
  - Tomcat 6.0.16
  - Apache 2.2.9
  - OpenLDAP 2.3.39
  - Ant 1.7.0
  - Java 1.5.0_17
  - Shibboleth idp 2.0.0

IdP構築

- メタデータ関連
  - フェデレーション全体のメタデータ設定
    - CiNii(NII論文情報ナビゲータ)、NII提供Plone、Moodleへのシングルサインオンを確認
  - フェデレーション全体のメタデータの自動受信設定
  - 署名付きフェデレーション全体のメタデータの自動受信設定、及び検証設定を確認

IdP構築

- LDAP関連
  - テストデータによる、シングルサインオン確認
  - 佐賀大学実運用LDAPからデータの一部を使用、実データによるシングルサインオン
  - eduPersonPrincipalName(eppn)の自動生成設定
    - uidを元にハッシュ値を生成
- その他
  - SPにより提供する属性区別
    - 学内向けSPにのみuidを提供

SP構築

- OS及び各種ソフトウェア
  - Ploneサイト
    - CentOS 5.1
    - Apache 2.2.3
    - Shibboleth sp 2.0
    - Plone 3.0.6
    - Python 2.4.4
  - Moodleサイト
    - FreeBSD 6.4
    - Apache 2.2.11
    - Shibboleth sp 2.1
    - Moodle 1.9.3
    - PHP 5.2.8
  - Drupalサイト(PHPベースのCMS)
    - WindowsXP Pro. SP3
    - Apache 2.2.11
    - Shibboleth sp 2.1
    - Drupal 6.8
    - PHP 5.2.6
    - PostgreSQL 8.3.1

SP構築

- メタデータ関連
  - フェデレーション全体のメタデータ設定
    - 佐賀大学SP上で、NII DSを選択後IdPの一覧表示でDSへの登録を確認
    - 佐賀大学SP上で、他大学のIdP認証画面で連携を確認
    - 佐賀大学SPログイン後、他のSPへのシングルサインオンを確認
  - フェデレーション全体のメタデータの自動受信設定
  - 署名付きフェデレーション全体のメタデータの自動受信設定、及び検証設定

DS構築

- 目的
  - 学内シングルサインオン環境整備による大学独自の認証連携ポリシーのDS
- OS及び各種ソフトウェア
  - CentOS 5.1
  - Tomcat 6.0.18
  - Apache 2.2.3
  - Ant 1.7.1
  - Java 1.6.0_07
  - Shibboleth ds 1.0.0

DS構築

- メタデータ関連
  - フェデレーション全体のメタデータ、佐賀大学IdP、SPメタデータ設定
    - NII 登録のIdPの一覧、佐賀大学IdP一覧表示を確認
    - 佐賀大学及び他大学のIdP選択後認証画面表示を確認