SPにまつわる仕様書と調達
～SPのシボ化を調達した場合～

岡山大学情報統括センター
河野圭太

岡山大学
OKAYAMA UNIV.

目次

- Shibboleth IdP
  - 導入経緯、運用状況
- 統合認証化
  - 体制、歩み
- SP追加の学内調整
- シボ化の方法
- シボ化の状況
- 知見

岡山大学
OKAYAMA UNIV.

Shibboleth IdP導入経緯

- 統合認証システムの一部として導入（2010年）
  - 当初は学認SPとの接続用として意識
  - 現在は学内SPの認証にも積極的に利用
  - 構築は統合認証システムの導入業者（調達）
  - 導入後の運用は学内で実施（業者による支援あり）
    - 新規SPの追加対応など

岡山大学
OKAYAMA UNIV.

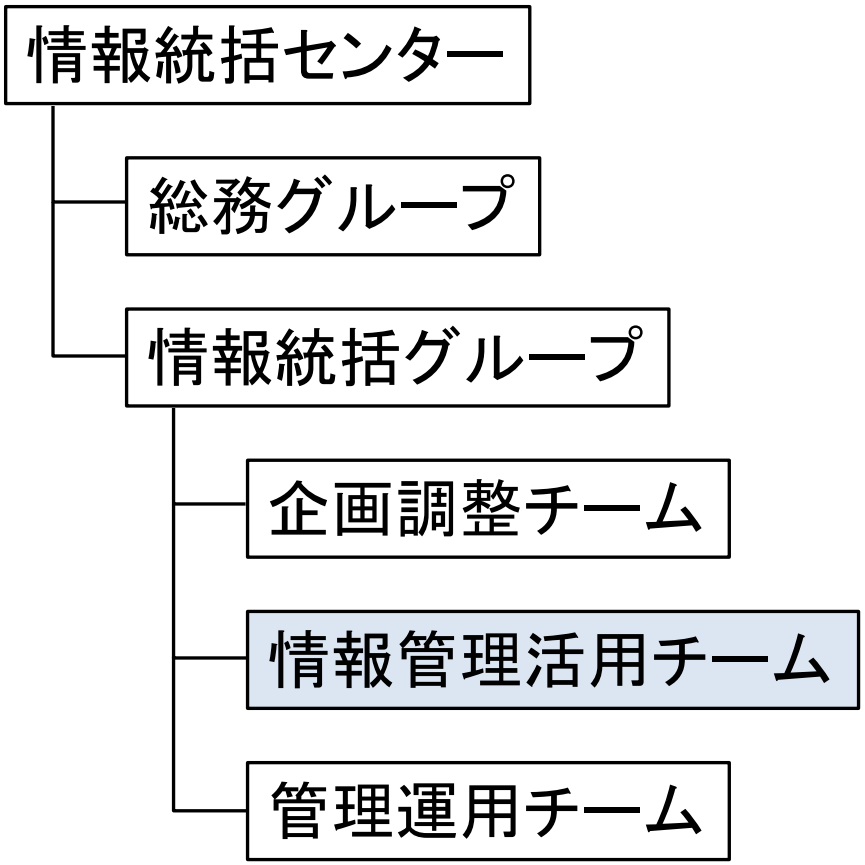
Shibboleth IdP運用状況

- 保有ID数
  - 学生：約14,000（学部生、大学院生、研究生・・・）
  - 教職員：約5,000（非常勤を含む）
  - 卒業生・退職者：約3,000/年（今年度より）
- 連携SP数
  - 学内SP：19
  - 学認SP：17

これらを単一IdPで運用

岡山大学
OKAYAMA UNIV.

組織・人員体制



統合認証プロジェクト
教員（常勤1）
職員（常勤2、非常勤1）
（全員他プロジェクトも兼務）

⇩

Shibboleth関連
教員（常勤1）
職員（常勤1※、非常勤1）
※専門職員

岡山大学
OKAYAMA UNIV.

統合認証化の歩み

- 統合認証システムの導入（2010年）
  - ID・パスワードの統一からSSO（認証の統合）へ
  - スモールスタート（ボトムアップ的なアプローチ）

既存システム：主にリバプロ型SSO製品による連携
新規システム：主にShibbolethによる連携

（ID統一によるメリットよりも
ID変更によるデメリットが
意識されるのを避けるため
（利用者・システム管理者））

岡山大学
OKAYAMA UNIV.

SP追加の学内調整

- （初期）仕様書に統合認証化の記載を依頼
  - 運営委員会等で記載例とともに広報・周知

1　本学の統合認証システムと連携し、以下の機能を実現すること。
1-1　Shibbolethによるシングルサインオン連携
1-2　Shibbolethによる属性交換
（CSV連携またはLDAPによる属性取得）に基づくID管理
（2010年運営委員会資料より）

⇩

（見積提示業者と）打ち合わせに来てもらうことを依頼
「最終仕様を確定」

岡山大学
OKAYAMA UNIV.

打ち合わせ内容

- 利用者の範囲
  - 学生？教職員？その他？
- 利用属性
  - 種別？氏名？メールアドレス？
- 統合認証化の方法
  - Shibboleth
    - Shibbolethの動作、導入方法
    - シボ化のメリット（学認の存在）
  - （リバプロ型SSO製品）
  - ローカル認証存続の必要性

シボ化の方法

- シボ化（SAML対応）済
- Shibbolethミドルウェア利用
  - セッション利用
    - アプリケーションをShibboleth配下に配備
    - 環境変数から属性を取得
  - プロキシ利用
    - Shibboleth配下にログインプロキシを配備
    - アプリケーションのセッション（Cookie）を代理取得

詳細は学認HPを参照

SP導入状況

- 学内SP（19）
  - シボ化（SAML対応）済（4）
    - Gmail, WebClass, Moodle（2）
  - セッション利用（13）
    - 学務システム, 学士課程教育構築（Q-cum）システム
    - 情報共有システム, リユース情報提供システム
    - 教職員メールアドレス検索システム, 他
  - プロキシ利用（2）
    - ALC NetAcademy 2, 入試BIシステム
- 学認SP（17）

WebClassのシボ化

- 対応内容
  - シボ化済（オプション購入）
  - Shibboleth IdP設定のみ大学作業
- 対応期間
  - 数週間

岡山大学
OKAYAMA UNIV.

学務システムのシボ化

- 対応内容
  - セッション利用
  - （5つのうち）4つのサブシステムをシボ化
  - （複数）グループID利用から個人認証へ移行
    - 個人IDでの認証後にグループIDを選択
  - 携帯電話（スマホ除く）からの利用
    - LDAP認証
  - 既存のローカル認証との併用
- 対応期間
  - 他の改修も合わせ数ヶ月

岡山大学
OKAYAMA UNIV.

仕様書記載事項

・Shibbolethによるシングルサインオンを実現すること。
・JavaScriptおよびCookieを利用できない携帯電話からの認証にも対応すること。
・個人が複数のサブシステムIDを持つ場合には岡大IDによる認証後に利用するサブシステムIDを選択する機能を有すること。
・岡大IDとサブシステムIDの紐付を一括変更する機能を有すること。
・既存のローカル認証（携帯電話からの認証を含む）との併用を実現すること。ただし、機能を無効化できること。

（学務システム改修仕様書より抜粋）

岡山大学
OKAYAMA UNIV.

ALC NetAcademy 2のシボ化

- 対応内容
  - プロキシ利用（オプション購入）
  - プロキシプログラムのみ業者提供
  - プロキシサーバ構築、Shibboleth SP設定は大学作業
- 対応期間
  - 1週間程度

岡山大学
OKAYAMA UNIV.

知見

- シボ化の経験
  - とりあえず（IdP、）SPを構築してみることを推奨
    - 作業ボリュームを理解しておくことが大事
- 事前の打ち合わせ
  - （既製品の）シボ化にはそれなりにコストが必要
    - 標準で対応しているものは少ない
      → 打ち合わせに来てもらう体制づくり
  - 見積の妥当性を評価
    - 未知のものにはリスクを積まれやすい
    - まずはしっかりとした説明を

まとめ

- IdPの運用状況
- SPのシボ化
  - 新規システムを中心にボトムアップ的アプローチで実施
- 学内調整
  - とりあえず（初期）仕様書への記載、そして打ち合わせを
- SPのシボ化方法
  - シボ化済、セッション利用、プロキシ利用
- SP導入状況
  - 学内SP（19）, 学認SP（17）

岡山大学
OKAYAMA UNIV.