岡山大学 ケーススタディ

～ 生涯IDを考慮した統合認証の取り組み ～

岡山大学情報統括センター
河野圭太

岡山大学
OKAYAMA UNIV.

国立大学法人岡山大学

- 組織
  - 11学部、1コース
  - 7大学院
- 人員
  - 学生　　学部生　　約10,000名
    大学院生　　約3,000名
  - 教職員　　常勤　　約2,600名

岡山大学
OKAYAMA UNIV.

情報統括センター

- 組織
  - 平成22年4月　2つの組織を統合
    - 総合情報基盤センター　ネットワーク、教育・研究
    - 学術情報部情報企画課　事務
- ミッション
  - 情報戦略から大学経営を支援
  - 高度な情報環境を整備
  - 情報セキュリティ・情報倫理遵守を推進

岡山大学
OKAYAMA UNIV.

生涯メール

- 平成21年4月～
  - 卒業・退職時に新規メールアカウントを付与
  - ID・パスワードを**Gmail**で管理
    - 卒業生（Gmail）　　@s.okadai.jp
    - 退職者（Gmail）　　@t.okadai.jp
- 平成24年4月～
  - 在籍時のメールアカウントを継続利用
  - ID・パスワードを**統合認証システム**で管理
    - 学生（Gmail）　　@s.okayama-u.ac.jp
    - 教職員（オンプレミス）　　@okayama-u.ac.jp

岡山大学
OKAYAMA UNIV.

統合認証システム

- 沿革
  - 平成22年4月　　仮運用開始（教職員）
  - 平成22年6月　　本運用開始（教職員）
  - 平成22年10月　　仮運用開始（学生）
  - 平成23年4月　　本運用開始（学生）
  - 平成24年4月　　本運用開始（卒業生・退職者）

- 現在の連携システム
  - 学内　　ネットワーク、メール、教育用PC、
    学務システム、e-Learning　他多数
    （来年度、事務システムも連携予定）
  - 学外　　学認

岡山大学
OKAYAMA UNIV.

岡大ID

- 岡山大学の統合ID
  - システムID　　個人を識別するためのID
    - ランダムな英数字
    - 岡大ID、メールアドレスの**初期値**（変更可能）
  - 岡大ID　　システムを利用するためのID
    - 任意の文字列（変更可能）
  - 原則1人1ID
    - 学部生→大学院生→卒業生
    - 教職員→退職者

岡山大学
OKAYAMA UNIV.

運用開始

- スモールスタート（ただし、基盤はしっかり）
  - HP社IceWallによる教職員向けSSO（4システム）

- ID・パスワードの通知（既存の教職員）
  - 仮運用開始（アナウンスのみ）
    - 教育・研究用システム（メール）のID・パスワード
  - 本運用開始（学内便）
    - 教育・研究用システム利用者　　新規パスワード
    - 事務システム利用者　　新規ID・パスワード

岡山大学
OKAYAMA UNIV.

初年度の対応

- 翌年の教育・研究用システム更改への準備
  - 統合認証システムとの連携
    - センターIDから岡大IDへ
- 既存のLDAP認証からの移行
  - 学認等、新規を含めて20システムと連携
  - 業者の支援を利用
    - 連携システム担当者との打ち合わせ（準備、細部の詰め）
    - 統合認証システム側の設定作業

本格運用の開始に伴う問題

- ID（およびメールアドレス）の規則
  - ランダムな英数字 or 任意の文字列
  - 個人を推測困難
    - メールの送受信、メーリングリストの作成
      → システムエイリアス（従来ルールのアドレス）
      メーリングリスト（グループ）管理システム
      学生岡大ID検索システム（常勤教職員向け）
    - 一部システム（WebClass）でのID検索
      → 学生番号による検索機能
- IDの名称

岡山大学
OKAYAMA UNIV.

名称変更

- 平成23年4月　名称変更を実施
  - 教育・研究用システムとの連携開始のタイミング

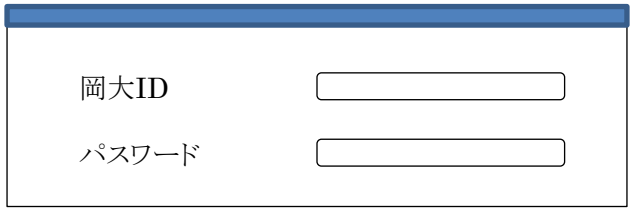
当初	現在
岡大ID	システムID
別名ID	岡大ID

岡山大学
OKAYAMA UNIV.

名称変更

- 平成23年4月　名称変更を実施
  - 教育･研究用システムとの連携開始のタイミング

当初	現在
岡大ID	システムID
別名ID	岡大ID

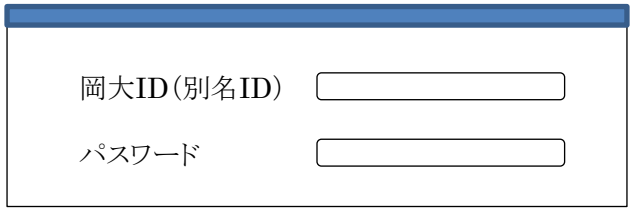


岡山大学
OKAYAMA UNIV.

名称変更

- 平成23年4月　名称変更を実施
  - 教育・研究用システムとの連携開始のタイミング

当初	現在
岡大ID	システムID
別名ID	岡大ID

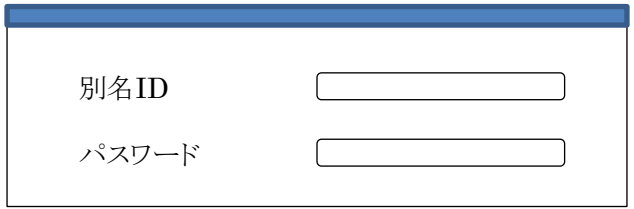


岡山大学
OKAYAMA UNIV.

名称変更

- 平成23年4月　名称変更を実施
  - 教育・研究用システムとの連携開始のタイミング

当初	現在
岡大ID	システムID
別名ID	岡大ID



岡山大学
OKAYAMA UNIV.

名称変更

- 平成23年4月　名称変更を実施
  - 教育・研究用システムとの連携開始のタイミング

当初	現在
岡大ID	システムID
別名ID	岡大ID

未だに当初の名称で呼ばれる場合も
（通知はがきの記載）

岡山大学
OKAYAMA UNIV.

利用者情報

- 大学情報DBから利用者情報を取得
  - 大学情報DBプロジェクト
    - 学内情報の一元的な取扱い
  - 構成員DB
    - 学務システム（学生マスタ）から
    - 人事システム（教職員マスタ）から

  システム間連携にはInfoteria社ASTERIA WARPを利用
  → ノン・プログラミングで構成変更可能

岡山大学
OKAYAMA UNIV.

教職員情報

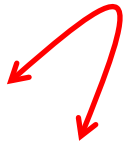
- 人事(給与)システム
  - 全教職員を管理するシステム　→　×
  - 給与支払い等に用いるシステム　→　○
    - 含む（構成員）　学長、理事、・・・、部長、課長、・・・、教授、・・・、**非常勤講師、TA、RA**
      → 総務課等と調整
    - 含まない（準構成員）　派遣職員、秘書
      → 申請ベース

着任時から利用できるよう、月末に翌月分のデータを取得し、自動作成
（ただし、もっと早くから欲しいという要望もある）

岡山大学 OKAYAMA UNIV.

岡大IDの利用者

- それぞれに許可されたシステムを利用可
  - 学生　　在学生
    卒業生
  - 教職員　　在職者　　構成員
    準構成員・・・申請書
    退職者
  - ゲスト　　短期（原則1日）・・・Web申請
    長期（原則最長30日）・・・申請書



識別可能

岡山大学
OKAYAMA UNIV.

卒業生・退職者を含む運用

- 毎年約4,000IDが増加
- 卒業・退職後もShibbolethを利用
  → そのままでは学認も利用可
  → **IdP側で**認可制御が必要

参考：学術認証フェデレーションシステム運用基準（Ver 1.2）、http://www.gakunin.jp/

  - FilterPerSPを拡張し、認可制御
    - ORに加えて、ANDによる条件指定
    - 当該SPに送信しない属性を用いた条件指定

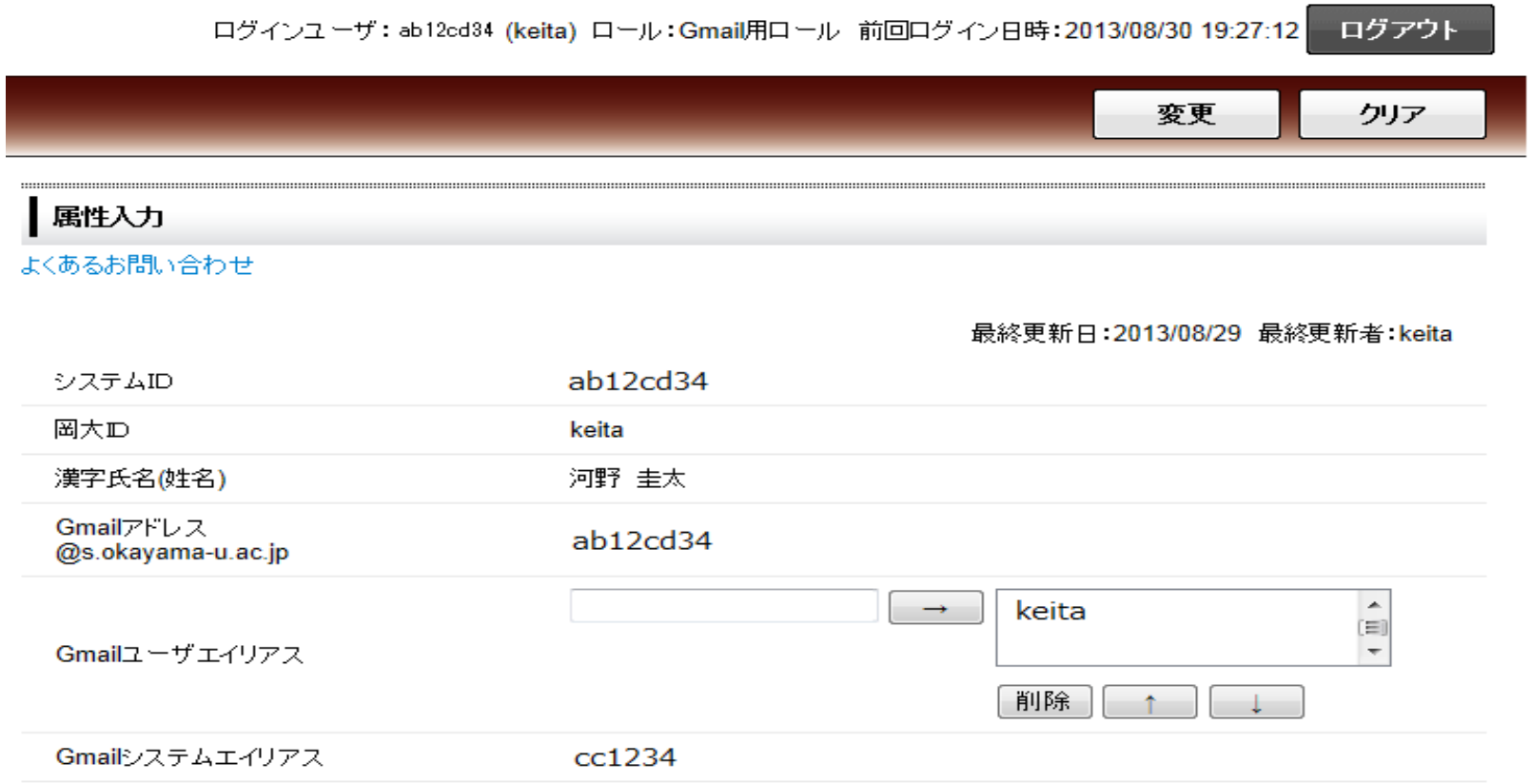
参考：FPSPプラグイン、https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=12158554

個人属性の管理

- 統合認証管理システム
  - 「ロール」による権限管理
    - 教職員用ロール（基本属性の一部）
    - メール用ロール
    - ネットワーク用ロール　他
  - 容易な管理属性の追加（好きなだけ）
    - スモールスタートからの拡張を実現

岡山大学
OKAYAMA UNIV.

Gmail用ロール


ログインユーザ：ab12cd34 (keita) ロール：Gmail用ロール 前回ログイン日時：2013/08/30 19:27:12
ログアウト
変更
クリア
属性入力
よくあるお問い合わせ
最終更新日：2013/08/29 最終更新者：keita
システムID
ab12cd34
岡大ID
keita
漢字氏名(姓名)
河野 圭太
Gmailアドレス
@s.okayama-u.ac.jp
ab12cd34
Gmailユーザエイリアス
→
keita
削除
↑
↓
Gmailシステムエイリアス
cc1234

他システムとの連携

- 情報連携
  - CSV（モジュール提供）
  - LDAP
- 認証連携
  - Shibboleth（推奨中）
  - HP社IceWall
  - LDAP

岡山大学
OKAYAMA UNIV.

連携システム

- 情報統括センター管理
  - ネットワーク、メール、教育用PC　他
- 他部局管理
  - 学務システム、e-Learning　他

→　連携の度に打ち合わせを実施
システム担当者
（システム納入・保守業者）

岡山大学
OKAYAMA UNIV.

Shibboleth化

- 開発システム等
  - ハードルは低い（担当者の作業でも多数の実績）
    - パッケージ、インストーラの利用
    - 作業（設定）マニュアルの提示
    - （Shibbolethの動作説明）
  - **内製システムの開発も容易に**
    - 学生岡大ID検索システム　他
- パッケージ製品等
  - カスタマイズコストがかかる場合も

Shibboleth化に伴う問題（1）

- 携帯電話への対応（Cookie問題）
  - Gmail、WebClassに影響
  - WebClass
    - LDAPによるローカル認証を併用

最終的に、スマートフォンの普及に頼ることに・・・

岡山大学
OKAYAMA UNIV.

Shibboleth化に伴う問題（2）

- ログアウト（シングルログアウト）問題
  - ログアウトしてもログアウトしない！
  - 3つのセッションの違い
    → どこまでログアウトしたい？
    - Shibboleth IdP（SSOサービス）　30分
    - Shibboleth SP　8時間（1時間）
    - アプリケーション

    今のところ、終了時にブラウザを閉じるよう指導

岡山大学 OKAYAMA UNIV.

学認との連携

- 学認の利用
  - SP（電子ジャーナル、ネットワーク利用等）
    - 利用数はまだまだ（おそらく認知度も）
  - **Shibboleth運用ノウハウ**
- 学認への期待
  - 利用必須システムの学認対応
    → 岡山大学は（ほぼ）学認Ready!
    （ID・パスワードの普及）
    認知度を高めたい

岡山大学
OKAYAMA UNIV.

学認との連携に伴う問題

- 個人属性の取り扱い
  - 個人情報の第三者提供（SPへの属性送信）
    → 平成25年9月　uApprove.jpを利用開始予定

参考：uApprove.jp、https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=13501031

Terms of Useを用いたコンプライアンス確認

確認項目　関連法令・諸規則等の遵守
（セキュリティポリシー等）
適切なセキュリティ対策の実施

確認頻度　年に1回程度（予定）

まとめ

- 岡山大学における統合認証の取り組み
  - 運用、情報連携・管理、認証連携

- 学認への参加
  - まずはIdPの構築を
    - 冗長化、FilterPerSP、uApprove.jp、StoredID

岡山大学
OKAYAMA UNIV.