岡山大学における
統合認証の取り組みと学認との連携

岡山大学情報統括センター
河野圭太

統合認証の取り組み（～2009）

- IDとパスワードの統一を推進
  - 教育研究支援情報システム：ID一括管理システム
  - その他システム：LDAP

断片的な統合認証が進行

- 課題
  - 全構成員を包含するID体系が存在しない。
    - 教育研究支援情報システムID（センターID）：全学生、全教員（2009年度以降）、一部職員
    - 学務システムID：全学生
    - 教員評価システムID：全教員
  - 進学や転学、身分変更に伴いIDが変更される。
  - セキュリティ対策箇所が分散化される。（安全性の低下）

教育系

学務系

教員系

統合認証の取り組み（2010～）

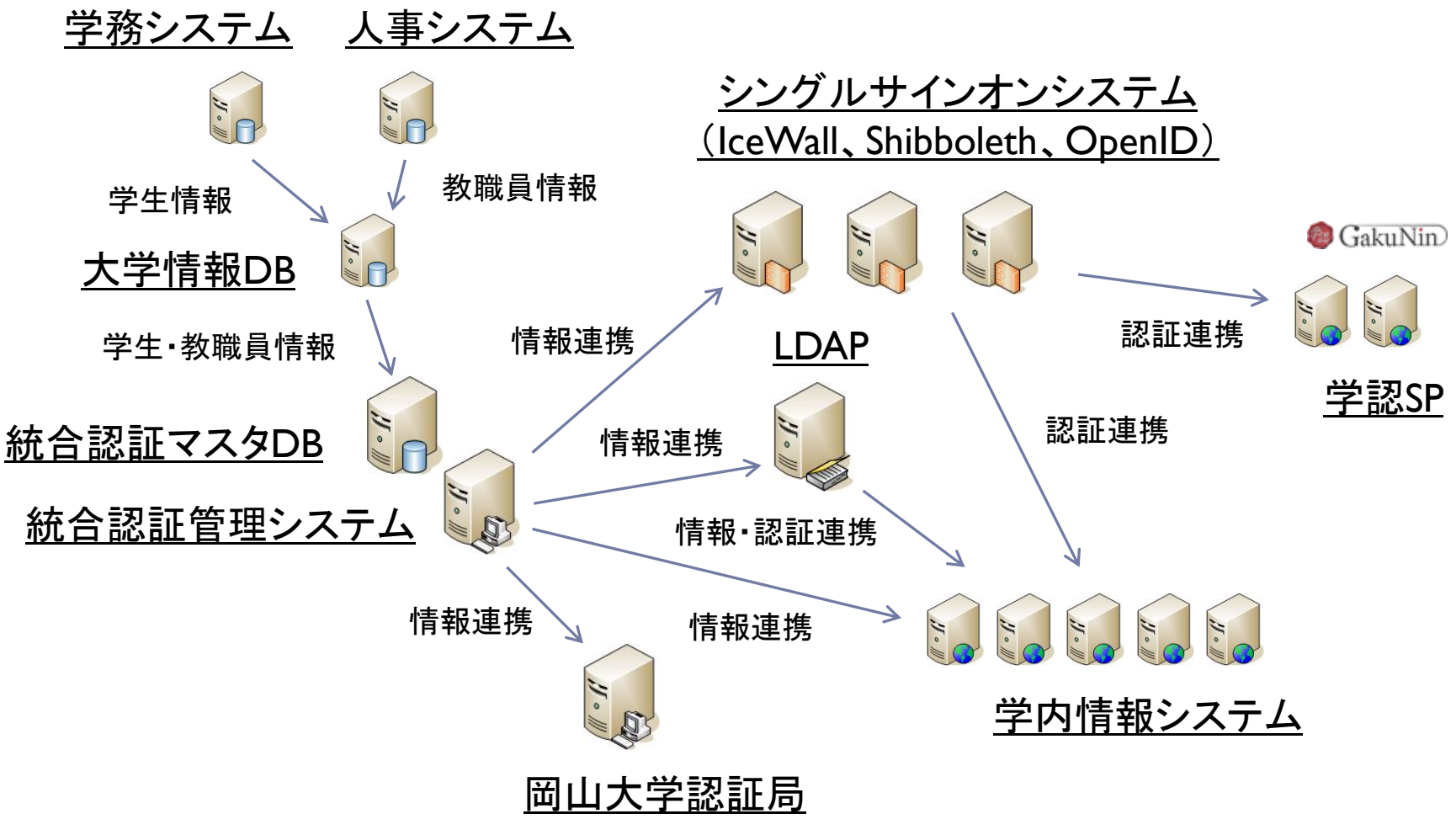
- 統合認証システムの運用を開始
  - 全構成員に対する統一的なID付与
    - 全ての学生、教員、職員が利用可能
    - 身分に依存しないID体系
  - IDの生涯利用
    - 進学、転学、身分変更の度にIDが変わらないように
    - 卒業、退職しても使えるIDを
  - シングルサインオン
  - 認証機構の統合
  - 学認との連携

<u>不変のIDによる学内（外）システムの統合利用</u>

岡大IDとシステムID、メールアドレスの関係

名称	用途	割り当てルール
システムID	個人を識別するために付与するID	ランダムな英数字
岡大ID	システムにログインするために利用するID	個人が設定した文字列（初期値は上記と同じランダムな英数字）
メールアドレス	メールアドレス	個人が設定した文字列@okayama-u.ac.jp（初期値は上記と同じランダムな英数字@okayama-u.ac.jp）

統合認証システムの構成



統合認証管理システム

- 大学情報DBと連動した岡大IDの自動生成
- 柔軟な権限（ロール）設定による個人属性の分散管理
- ワークフローによるサービス利用申請

管理属性の追加も容易に実現可

主な機能

- 岡大IDの変更
- メールエイリアスの設定
- 追加メールアドレスの申請
- ホスティングサービスの申請
- 岡大IDの登録
- 利用サービスの変更
- 各種申請の承認
- パスワードリセット

岡大ID変更


岡大ID・物品ID登録
ログインユーザ：[redacted] (keita) ロール：教員用ロール 前回ログイン日時：2
岡大ID・物品ID管理
配信処理
ロール切替
パスワード変更
属性入力
よくあるお問い合わせ
最終更新日
システムID
岡大ID
keita
個人番号
統合認証・所属コード①
研究所・センター等
統合認証・所属コード②
情報統括センター
統合認証・所属コード③
利用者種別
教員

メールエイリアス設定


岡大ID・物品ID登録
ログインユーザ：[redacted] (keita) ロール：大学メール用ロール(教員用) 前回ログイン日時：2011/07/28 20:12:(
変更
岡大ID・物品ID管理
サービス申請処理
配信処理
ロール切替
属性入力
よくあるお問い合わせ
最終更新日：2011/04/05 最終更
システムID
[redacted]
岡大ID
keita
漢字氏名(姓名)
河野 圭太
大学付与メールアドレス設定(アカウント/パスワードは、岡大ID/パスワードと同じです。)
大学付与メールアドレス
[redacted]@cc.okayama-u.ac.jp
・大学正式メールアドレス
・エイリアス設定
→
keita
削除
↑
↓
・メール転送設定
→

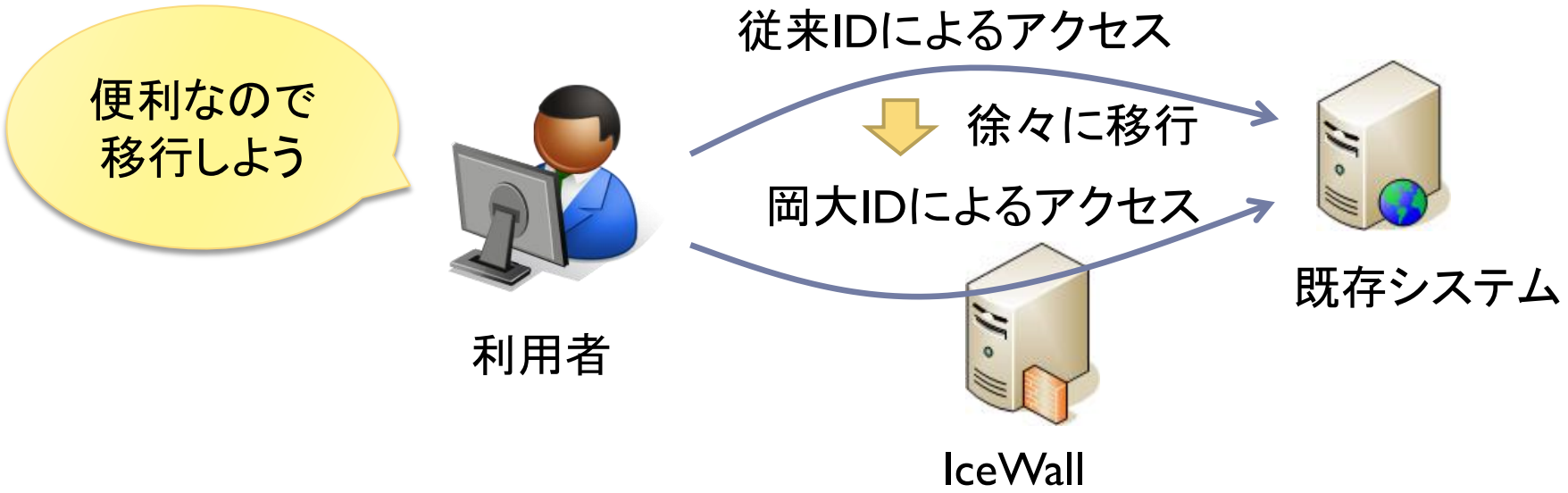
追加メールアドレスの申請

シングルサインオンシステム

- シングルサインオンの実現
  - ID・パスワード入力回数の削減
- 認証機構の統合
  - セキュリティ対策箇所の一本化
- 個人別認証ポータルの提供
  - 学内（外）システムへの入り口

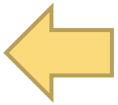
既存システムとの認証連携

- リバースプロキシ型製品（IceWall）によるソフトな連携
  - 利用者によっては岡大IDこそが新しく管理が必要なID



- Shibbolethによる連携
  - 対応できるものはShibbolethで

新規システムとの認証連携

- Shibbolethによる連携  こちらを推奨中
  - 以下の場合、連携は容易
    - 認証機構がカスタマイズ可能な場合
    - モジュールが提供されている場合
  - 認証プロキシを構築する方法も
- リバースプロキシ型製品（IceWall）による連携
  - 中にはShibboleth対応できないものも
    - 既製システム
    - 契約上？

いずれにしても運用担当者との事前の意思疎通は重要

システム連携に伴う課題

- 共用IDへの対応
  - 1つのIDを複数人で共用
  - パスワードを知っている人＝アクセスしてよい人という想定
  - 人事異動などに対応しなくてよい（？？）ため管理が楽

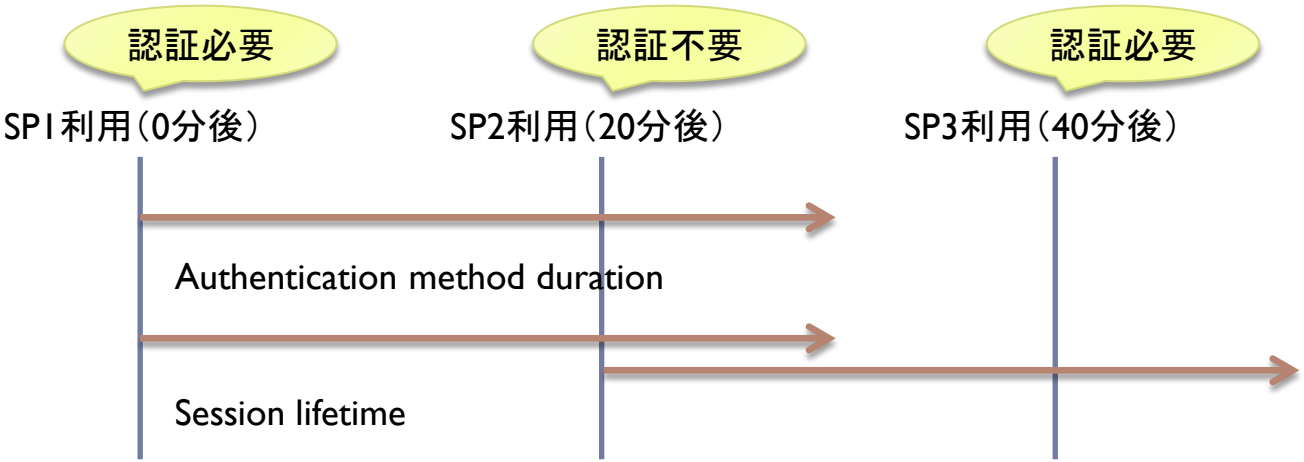
セキュリティポリシー上は問題

個人認証が必要だが理解が得られにくい。

運用負担を増やさない移行方法の検討が必要

ShibbolethによるSSOの課題

- IdPタイムアウト時間の調整
  - Authentication method duration：認証後30分
  - Session lifetime：（IdPと）無通信30分



- SPログアウトの実装
  - ログアウトしたのにログインしている？（SSOで再ログイン）

学内システム接続状況

20システム以上

- 教育・研究支援情報システム
  - 教育用PC、学生Gmail、教（職）員メール　他
- ネットワークシステム
  - ネットワーク認証（有線、無線LAN）
- e-Learningシステム
  - WebClass、ALC NetAcademy 2　他
- 業務システム
  - 教員活動評価、財務会計システム　他
- 学務システム
  - 学生履修登録・成績確認（予定）、教員成績入力　他
- その他システム
  - 情報共有システム、部局独自システム　他

（下線はShibboleth接続のシステム）

学認SP接続状況

17SP

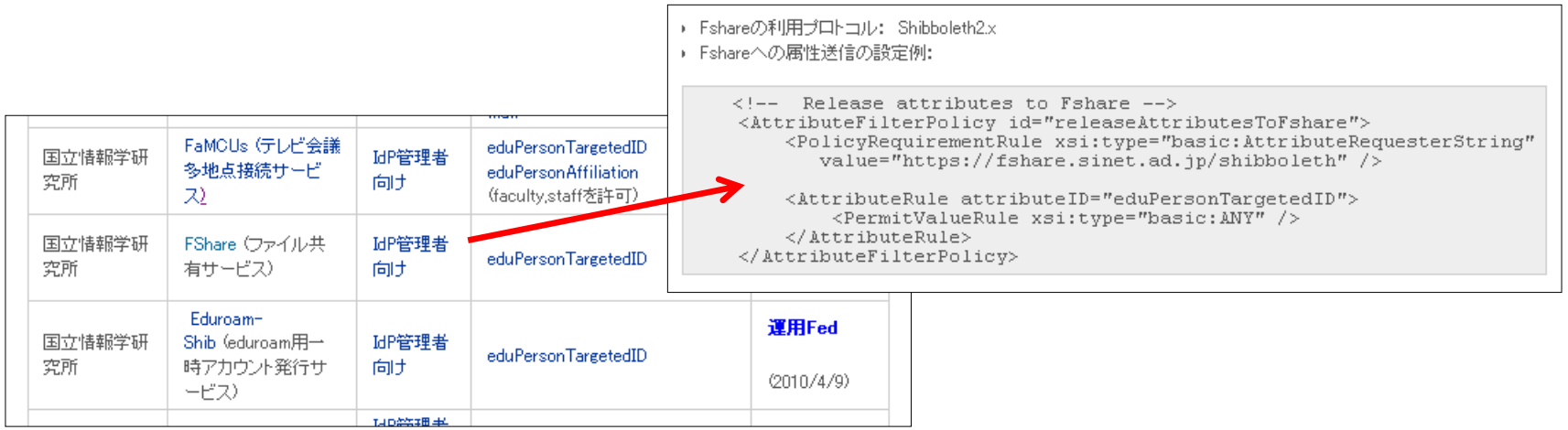
- Elsevier　Science Direct
- Springer　SpringerLink
- Thomson Reuters　Web of Knowledge
- CUP　Cambridge Journals Online
- EBSCO　EBSCO host
- 国立情報学研究所　CiNii
- 国立情報学研究所　FaMCUs/FShare/
  Eduroam-Shib/WebELS/
  edubase Cloud/学認申請システム
- 金沢大学　File Transfer Service/
  Opens non-Bibliographic
  Contents Service
- 山形大学　科学技術の学術情報共有のための
  双方向コミュニケーションサービス
- 広島大学　HINETの無線LANゲスト利用サービス
- 佐賀大学　無線LANゲスト利用サービス

電子ジャーナルが中心

2011年11月～
（講演を機に
急遽設定）

学認SP接続手順～つないでみた～

- メタデータの交換　→　自動更新設定済
- 属性管理
  - 利用属性の定義　→　学認利用属性は定義済
  - 送信属性の設定　→　学認HPに設定例



国立情報学研究所	FaMCUs（テレビ会議多地点接続サービス）	IdP管理者向け	eduPersonTargetedID eduPersonAffiliation (faculty,staffを許可)	
国立情報学研究所	FShare（ファイル共有サービス）	IdP管理者向け	eduPersonTargetedID	
国立情報学研究所	Eduroam-Shib（eduroam用一時アカウント発行サービス）	IdP管理者向け	eduPersonTargetedID	運用Fed (2010/4/9)

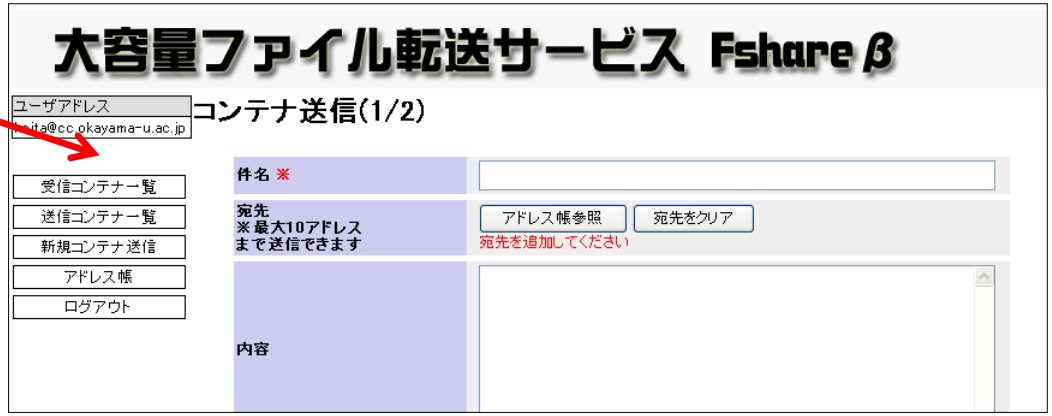
- Fshareの利用プロトコル：Shibboleth2.x
- Fshareへの属性送信の設定例：

```
<!--  Release attributes to Fshare -->
<AttributeFilterPolicy id="releaseAttributesToFshare">
    <PolicyRequirementRule xsi:type="basic:AttributeRequesterString"
       value="https://fshare.sinet.ad.jp/shibboleth" />

    <AttributeRule attributeID="eduPersonTargetedID">
        <PermitValueRule xsi:type="basic:ANY" />
    </AttributeRule>
</AttributeFilterPolicy>
```

数（十）分程度の作業時間で11SPを接続

学認SP利用手順～使ってみた～



学認SP利用手順～会場で使ってみた～

学認との連携に伴う課題

- Shibbolethの認可制御
  - IdPの送信属性に基づきSP側で実施
    - IdPの利用者範囲≠SPの利用者範囲の場合、対応はSP次第
    - SPによっては認可制御をしないものも

⇩ 現在は自組織の利用者のみを登録しているが・・・

柔軟かつ厳格な運用にはIdPによる認可制御が必要

（今年度中に対応予定）

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）

> 3.2） 属性情報の信頼性
>
> IdP は，自組織に所属する利用者の属性を保証すべきである。また，自組織に所属しない利用者の属性を保証すべきではない。例えば，A 大学の IdP が B 大学の学生の属性を保証すべきではない。ただし，自組織に所属しない利用者を自組織が管理する場合，SP に対する不正なアクセスが発生しないよう特に属性管理に注意することで，そのような利用者の属性を保証してもよい。

まとめ

- 統合認証の取り組み
  - 岡大IDによる学内（外）システムの統合利用
  - 全構成員に対する統一的なID付与
  - Shibbolethを中心とした認証連携を推進中
- 学認との連携
  - 2011年12月現在　17SPと接続