福岡大學

学認参加事例紹介
学認との連携を考慮したハイブリッド型SSO環境の構築

福岡大学総合情報処理センター
准教授　中國　真教
e-mail: nak@fukuoka-u.ac.jp

もくじ

- 福岡大学のご紹介
- 福岡大学における認証基盤の歩み
- 福岡大学が認証基盤に求める要件
- 認証基盤の刷新
- 2つのSSOの導入
- 現況
- 今後の計画

福岡大学のご紹介

福岡大学の紹介

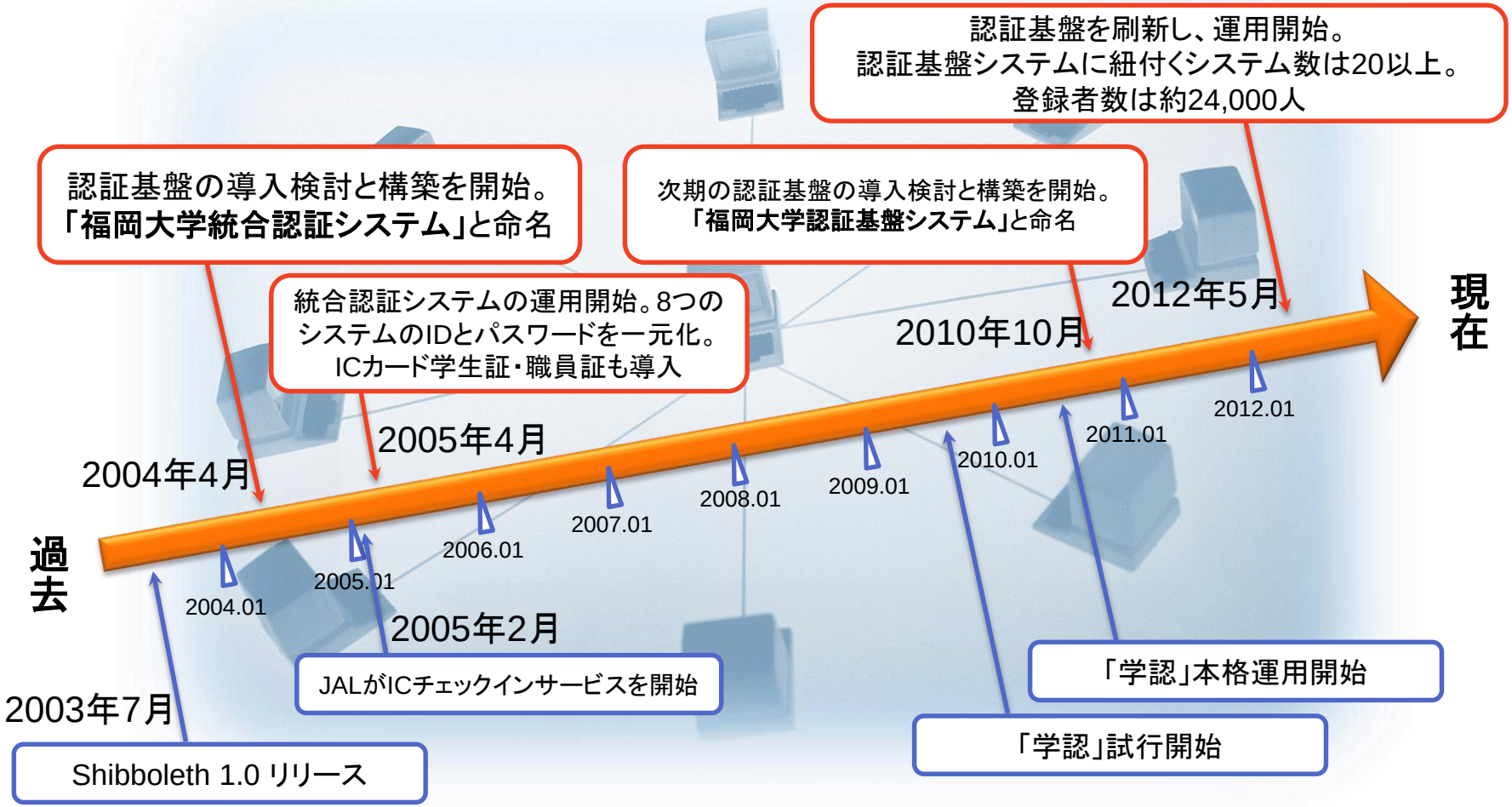
- 本部所在地
  - 福岡市城南区七隈
- キャンパス
  - 七隈
  - 北九州学術研究都市
- 組織
  - 9学部、31学科、10研究科、7付置研究所、15センター
  - 2つの大学病院、2つの附属学校
- 規模
  - 学生数　　約21,000人（卒業生数 約23万人）
  - 教職員数　　約 3,000人

福岡大学公式ホームページ　http://www.fukuoka-u.ac.jp/

福岡大学における認証基盤の歩み

福岡大学における認証基盤の歩み（1/5）

■ 福岡大学における認証基盤の歴史



福岡大学における認証基盤の歩み(2/5)

- 統合認証システム(旧認証基盤)と紐付いていたシステム(Webサービス)の代表例
  - 大学ポータルサイト
  - 教育研究システム(e-Learningシステム、Microsoft Live@edu、その他)
  - ネットワーク認証・検疫システム
  - 図書館利用者向けサービス(Myポータル)
  - SSL-VPNサービス
  - ウィルス対策システム(インストール時の認証)
  - グループウェアサービス
  - シラバス関連システム
  - 出張申請システム
  - 研究者情報システム

※下線のあるシステムは旧認証基盤でSSO機能実装済み

福岡大学における認証基盤の歩み(3/5)

- 旧システムの課題(利用者から見た側面)
  - パスワード変更時のリアルタイムな反映ができない
    - パスワード変更が反映されるのは次の日
  - パスワード忘れに対する対応窓口のトラブル
    - パスワード初期化の依頼者の行列ができることも！
  - 学外からパスワード変更をさせないポリシー
    - 利用者の意見としては、パスワード変更のために大学に来るのは面倒！諸事情により来られない場合もある！とのこと

福岡大学における認証基盤の歩み(4/5)

- 旧システムの課題(管理者から見た側面)
  - システムの機能拡張が困難
    - ソフトウェアは機能拡張を意識した造りになっておらず、機能拡張のたびに大きな改修が必要
  - システムがブラックボックス化していた
    - 仕様がわかりにくく、保守性に問題があった
  - パスワードとして使用できる文字種が少ない
    - 旧システムと連携していたシステムでは、アルファベットと数字しか使えず、記号が使えなかった

福岡大学における認証基盤の歩み(5/5)

- 旧システムから新システムへの移行についての課題
  - 現行の(疑似)SSOを今後どのように取り扱うのか？
    - 選択肢: 「今後も使う」 or 「今すぐ捨てる」
    - 検討結果: もう暫く使ってから捨てる

既存の疑似SSOの仕組みを今後も踏襲するべきではないことは理解できるが、過去の遺物を今すぐには捨てられない。

新たに構築する SSO と 疑似SSO を平行して利用することに決定

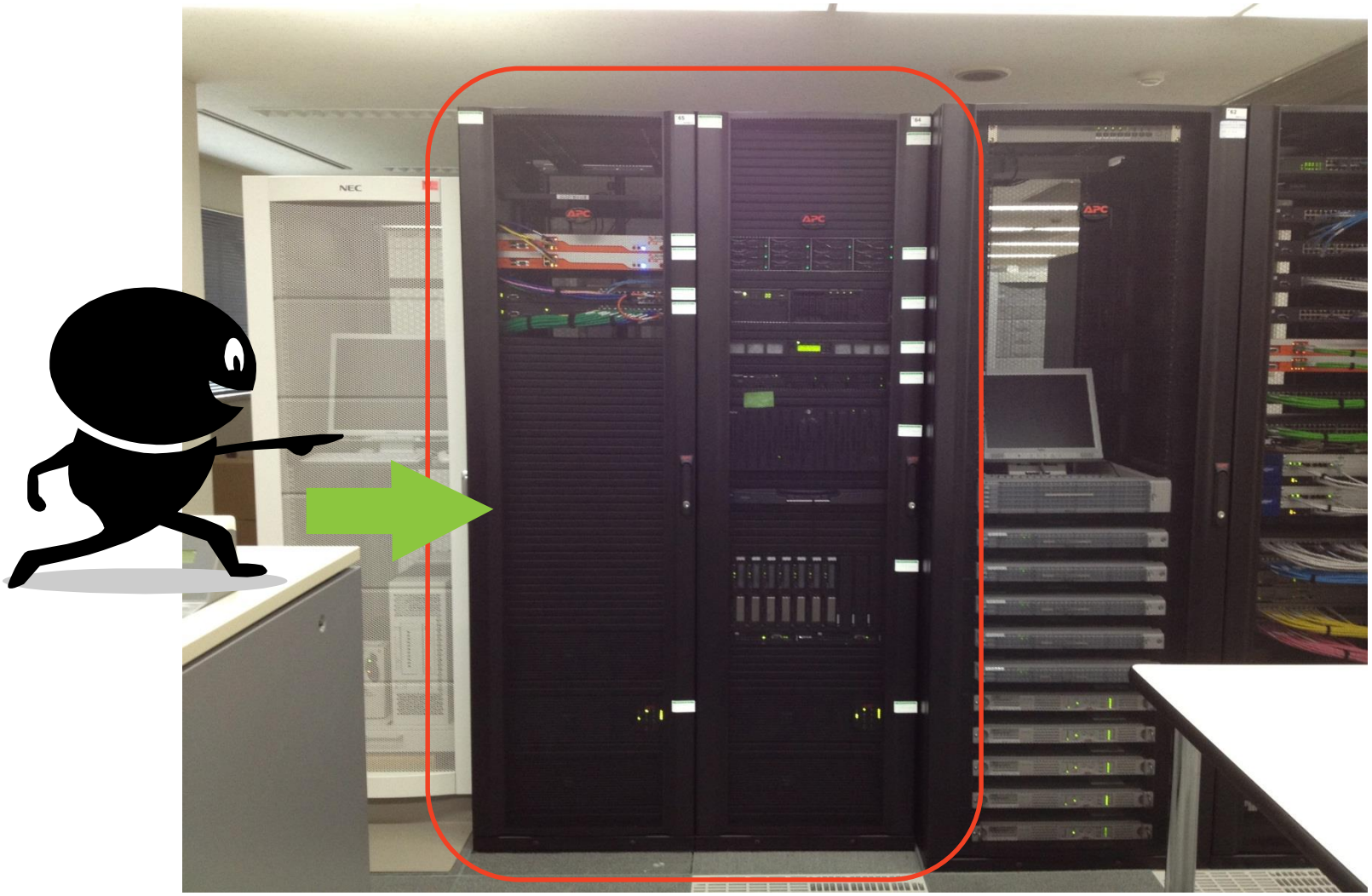
福岡大学が認証基盤に求める要件

福岡大学が認証基盤に求める要件

- 利用者への負担の軽減
  - ID申請の電子化（常勤の教員・職員の申請）
  - パスワード管理に関する負担軽減
  - パスワード変更時の全システムへの即時反映
  - SSOへの対応
- 連携するシステムとの親和性
  - 標準的な技術を用いた汎用性の高いシステムとする
  - 上位システム（利用者情報を保持する人事給与システムや教務システム）から受け取る利用者情報の適切な処理
- 高い拡張性
  - ベースとなる部分は、2012年から10年間利用する予定。必要に応じて機能拡張を実施する予定

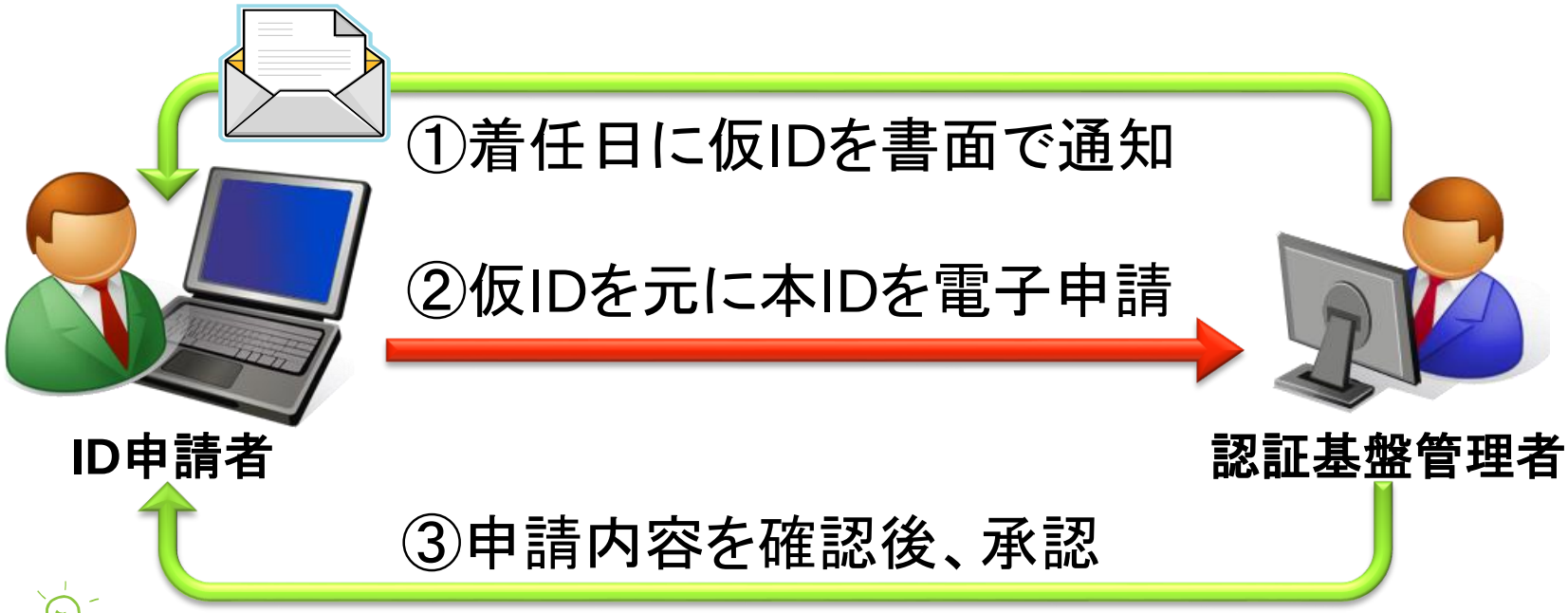
認証基盤の刷新

認証基盤の刷新（ハードウェアの外観）



認証基盤の刷新（ID/パスワード編）（1/4）

- 利用者への負担の軽減
  - ID申請の電子化（常勤の教員・職員の申請）



従来行われていた、申請者による申請書作成や提出、認証基盤管理者による申請書の煩雑な処理が不要になった。

認証基盤の刷新（ID/パスワード編）（2/4）

- 利用者への負担の軽減
  - パスワード管理に関する負担軽減（1）

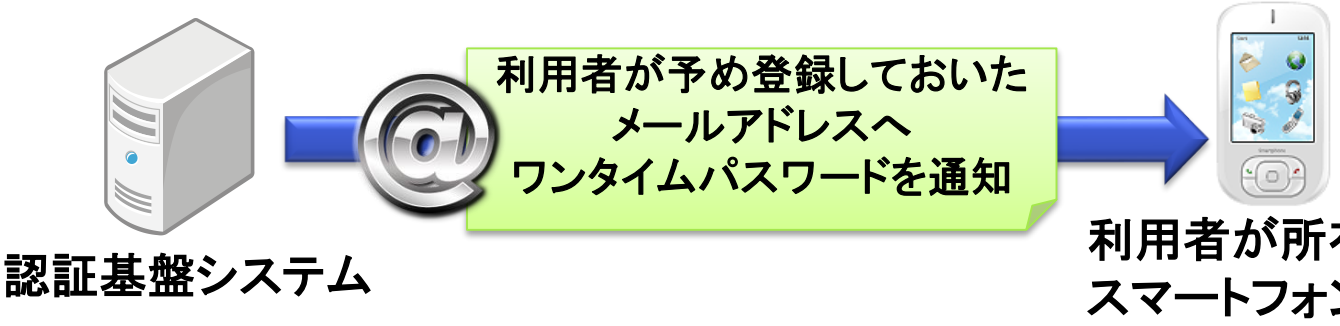
パスワード初期化端末の導入による、初期化手続きの高速化

依頼者が所有するICカード学生証をかざすことで、初期化対象者を容易に検索でき、利用者からの依頼へ迅速に対応できるようになった（1人あたりの対応時間は2分から1分へ短縮）。

認証基盤の刷新（ID/パスワード編）（3/4）

- 利用者への負担の軽減
  - パスワード管理に関する負担軽減（2）

学外からパスワードを変更する際には、ワンタイムパスワードを併用し、2要素認証によって利用者を認証する仕組みを導入

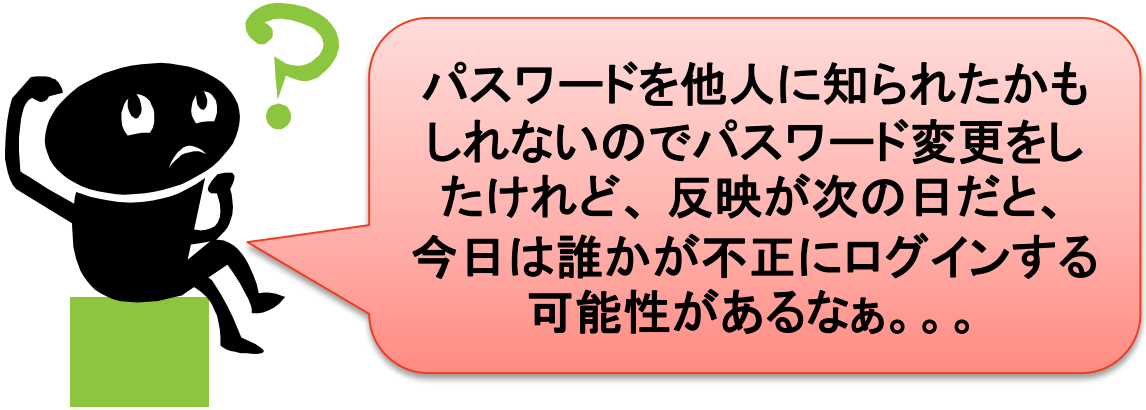


パスワードの有効期限を迎える日に、海外への長期出張（在外研究など）、留学、長期休暇などのため大学から離れた場所に居た場合でも、パスワードが失効することなく、IDを継続して利用できるようになった。

認証基盤の刷新（ID/パスワード編）（4/4）

- 利用者への負担の軽減
  - パスワード変更時の全システムへの即時反映

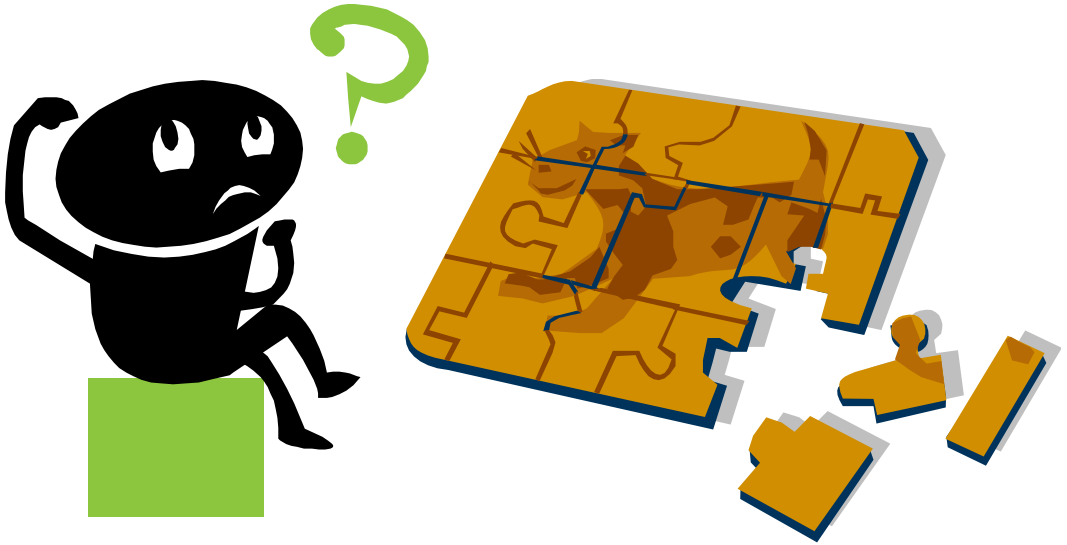
旧認証基盤では、パスワード変更を行っても、新しいパスワードが有効になるのは次の日以降であり、何かと不都合が生じたため、即時反映を可能にする仕組みを導入した。



セキュリティ面の課題が解決しただけでなく、パスワード変更直後に新しいパスワードが有効になっているかを即座に確認できるようになったため、利便性が向上した。

認証基盤の刷新（SSO編）（1/4）

- SSOへの対応
  - 過去の遺物（疑似SSO）との連携（共存）方法は？
  - SSOで連携するWebサービスの選定は？
  - SSOを実現するためにどの製品を使うのか？



認証基盤の刷新（SSO編）（2/4）

- SSOで連携するWebサービスの選定
  - どのような視点で選定する？
    - 利用者数が多いシステムを優先
  - 候補となったシステム
    - 大学ポータルサイト（FUポータル）
    - Microsoft Live@edu （Outlook Live）
    - e-Learningシステム（HIPLUS、Moodle）
    - ネットワーク認証・検疫システム
    - 図書館利用者向けシステム（Myポータル）

ログイン時にメールアドレス（長い文字列）の入力が必要であるため、利用者から不評だった。

認証基盤の刷新（SSO編）（3/4）

- SSO製品の選定
  - Shibbolethを選択
    - 理由：国立情報学研究所や他大学から提供されているサービスを活用しやすくするため。
  - しかし、Shibbolethでは不安な点も。。。
    - 運用実績がそれほど多くない（只今、増加の最中）
    - 今後、市場に出回るシステムはShibboleth（SAML SP）への対応をどのように考えているのか不明

認証基盤の刷新（SSO編）（4/4）

- Shibboleth導入についての懸念
  - SAML非対応のシステム（アプリケーション）は改修が必要だが、開発者が改修に応じてくれるとは限らない（自力で改修できれば良いが。。。）
  - SAML対応への改修にはコストがかかるかも？
  - Shibbolethの標準機能では、認証方式がID/Password方式であるため、将来的にDesktop SSOやクライアント証明書によるSSOの機能の導入が必要になった場合は、Shibbolethでは実現がやや難しいかも？
  - 改修できたとしても、Shibbolethがバージョンアップした際には、その対応のために再度改修が必要となり、コストが増大する可能性がある

2つのSSOの導入

2つのSSOの導入(1/9)

- OpenAMとShibbolethの導入
  - 学外サービス(SP)へのアクセスには

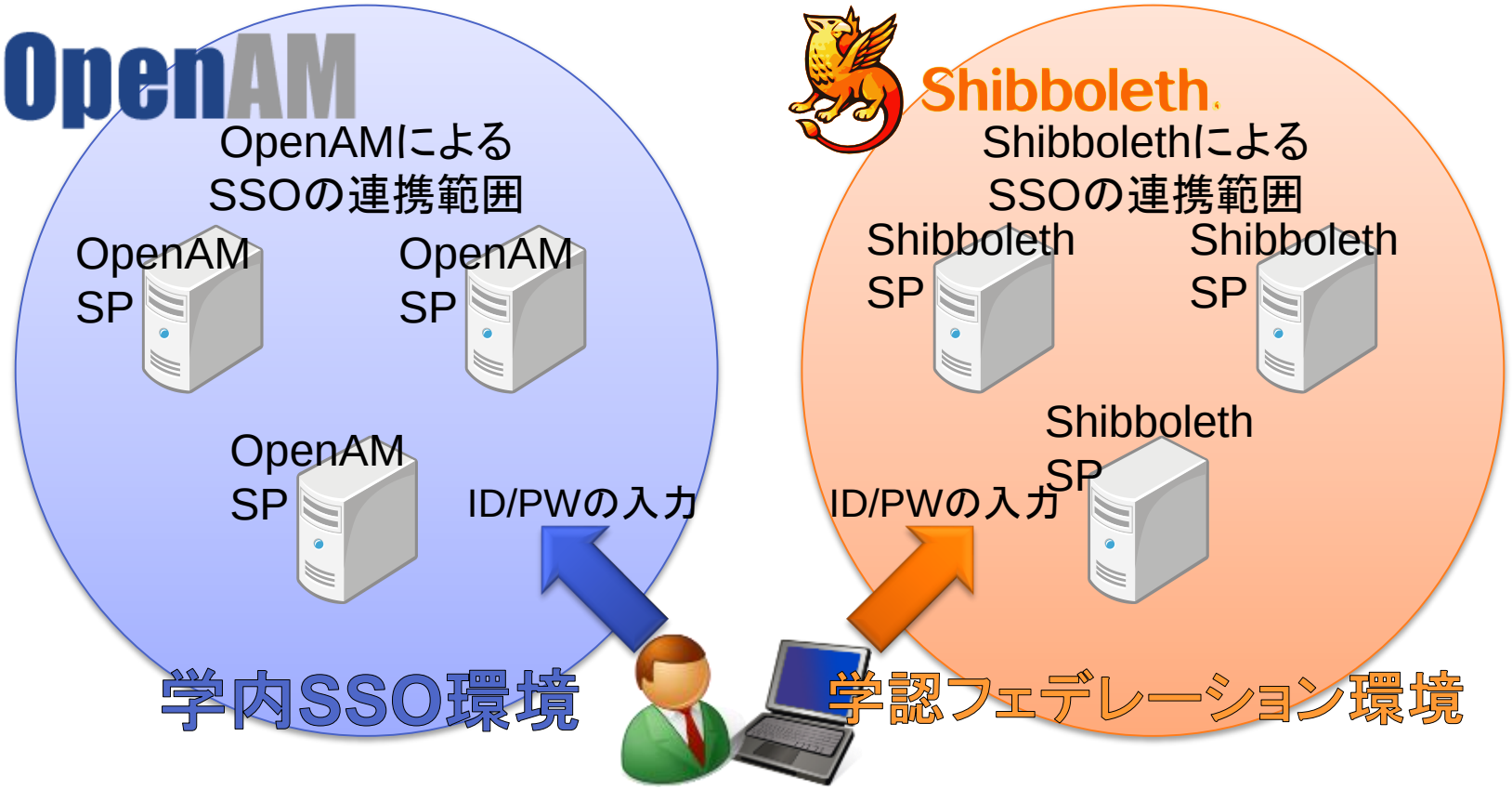
  - 学内サービス(SP)へのアクセスには

2つのSSOの導入(2/9)

- なぜ、OpenAMなのか？
  - OpenAMはシングルサインオンの方式を複数備えている(実は、SAMLにも対応)
    - SP側の改修費用は、Shibbolethと連携させる場合よりも安く抑えられる(多分。。。)
  - 多様な認証方式を用意
    - ID/パスワード認証以外にも認証方式を標準で備えており、システムのセキュリティや用途にあった認証方式の選択が可能

2つのSSOの導入(3/9)

- 2系統のSSO



SSOの系統が異なるため、それぞれのSSOの系統でのID/パスワードの入力が必要。

2つのSSOの導入(4/9)

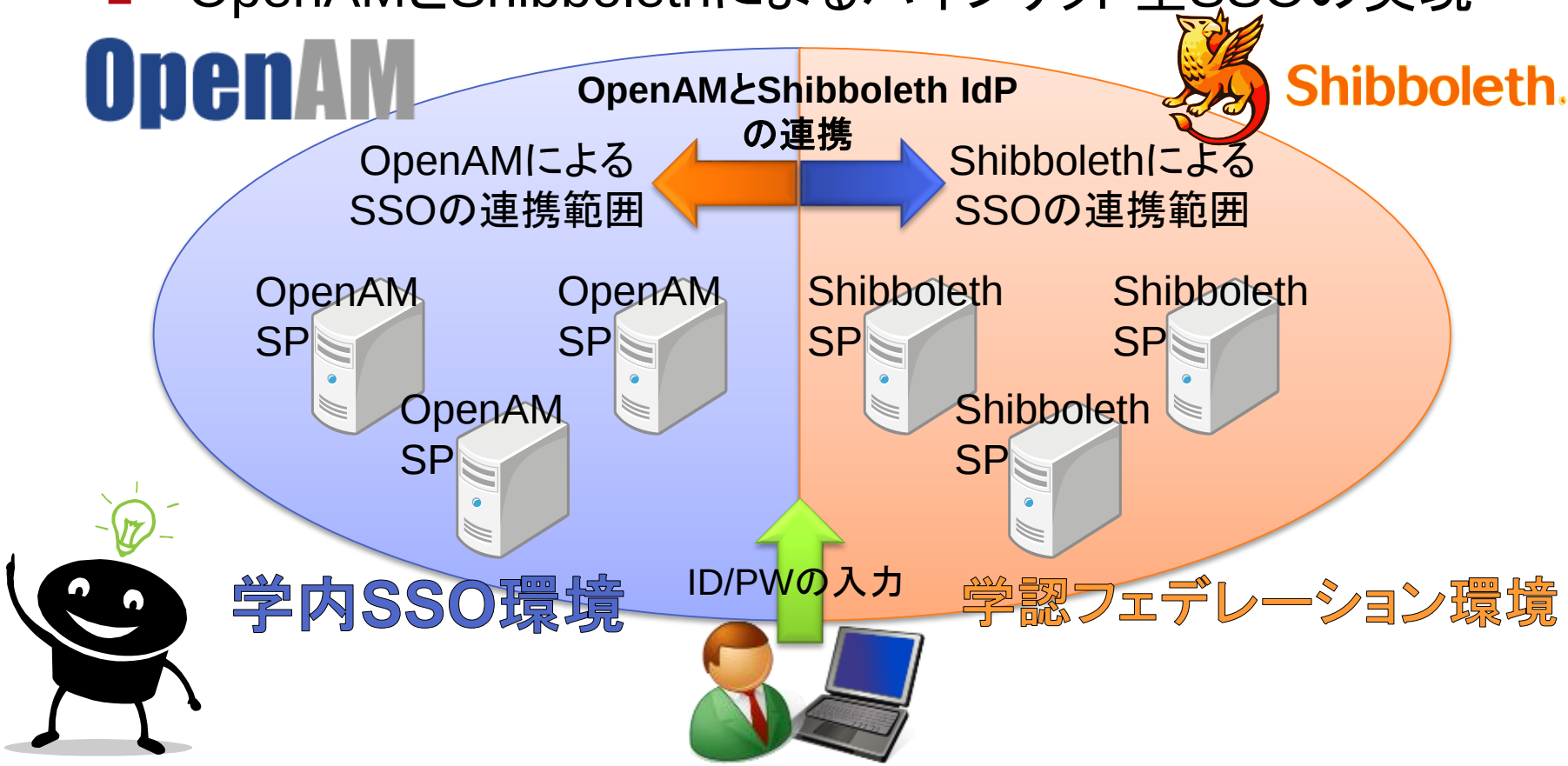
- SSOなのに2回も認証が必要なの？

この問題を解消するためにOpenAMとShibbolethの連携を検討

Rest APIによりShibbolethがOpenAMに認証済みかどうかの問い合わせを行うことで、Shibboleth IdPの認証をOpenAMで実現！

2つのSSOの導入(5/9)

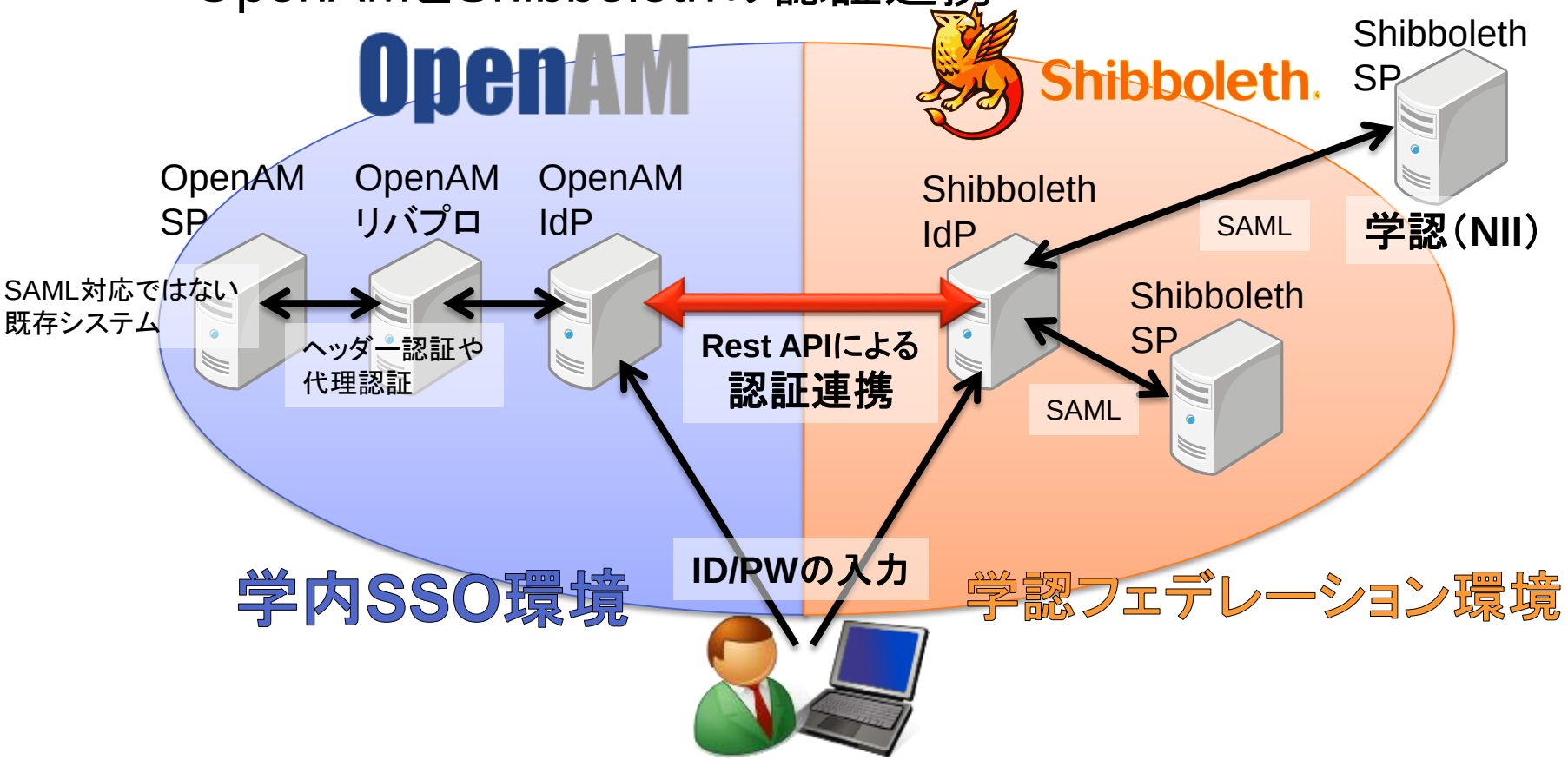
- OpenAMとShibbolethによるハイブリッド型SSOの実現



1度のID/パスワードの入力でOpenAMとShibbolethの両系統のリソースにアクセスできる。

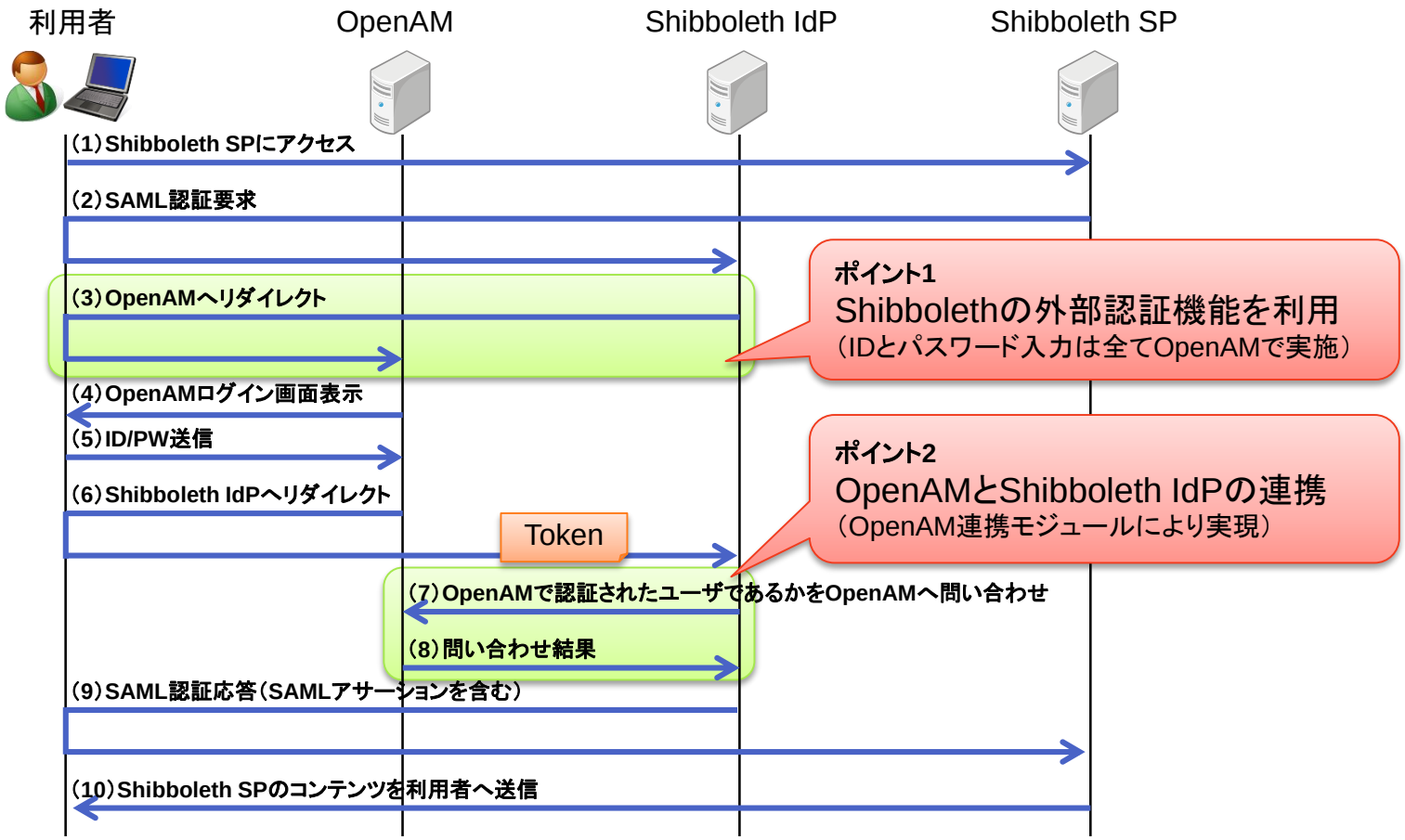
2つのSSOの導入(6/9)

- OpenAMとShibbolethの認証連携



2つのSSOの導入（7/9）

- ハイブリッド型SSOにおけるShibboleth SPへのログインシーケンス



2つのSSOの導入(8/9)

- 今回構築したハイブリッド型SSOの特長(まとめ)
  - OpenAMとShibbolethが認証連携
  - OpenAM側で利用者認証が完了すれば、Shibbolethと連携しているサービスにもSSOが可能(Shibbolethの外部認証機能を利用)
  - OpenAMの多様な認証方式(PKI認証、ワンタイムパスワード等)や柔軟な認可機能を利用して、サービスのセキュリティレベルに応じたアクセス制御が可能
  - Shibbolethに対応するための改修は不要
  - SSO基盤の構築は、オープンソースのみ※で実現

※LDAPサーバはOpenLDAP、リバースプロキシサーバはApache + OpenAM Policy Agent

2つのSSOの導入(9/9)

- ログイン画面

現　況

現況(1/2)

- 学認に参加し、現在はテストフェデレーションにて運用中(年内に運用フェデレーションへ移行予定)
- SSO連携するシステム
  - 図書館利用者向けサービス(Myポータル)
  - Microsoft Office365 for Education
  - e-Learningシステム(Moodle、HIPLUS)
  - 福岡大学ポータルサイト(ActiveCampus)

現況(2/2)

- 学外のクラウドサービスとのSSO連携の課題
  - Office365 for Education(Live@eduの後継)との認証連携における課題

Office365 for Educationのポリシーでは、
パスワード変更後のパスワード有効期限は90日！

福岡大学認証基盤システムとOffice365におけるパスワードポリシーの違いに困惑！

後に、Microsoft側のポリシーの緩和により無期限で設定できるようになったが、今後変更になる可能性は否定できない。
学外クラウドサービスと連携する際はこのような点にも注意が必要。

今後の計画

今後の計画

- 学内のPC教室の端末におけるデスクトップSSOの実現
  - 利用者認証における利便性の向上
- 二要素認証機能の提供
  - より高いセキュリティが求められる情報システムへの対応

ご清聴ありがとうございました

人をつくり、時代を拓く。

福岡大學