鹿児島大学の現状

学認CAMP2016 資料
2016/10/17

鹿児島大学 学術情報基盤センター
下園幸一
simozono@cc.kagoshima-u.ac.jp

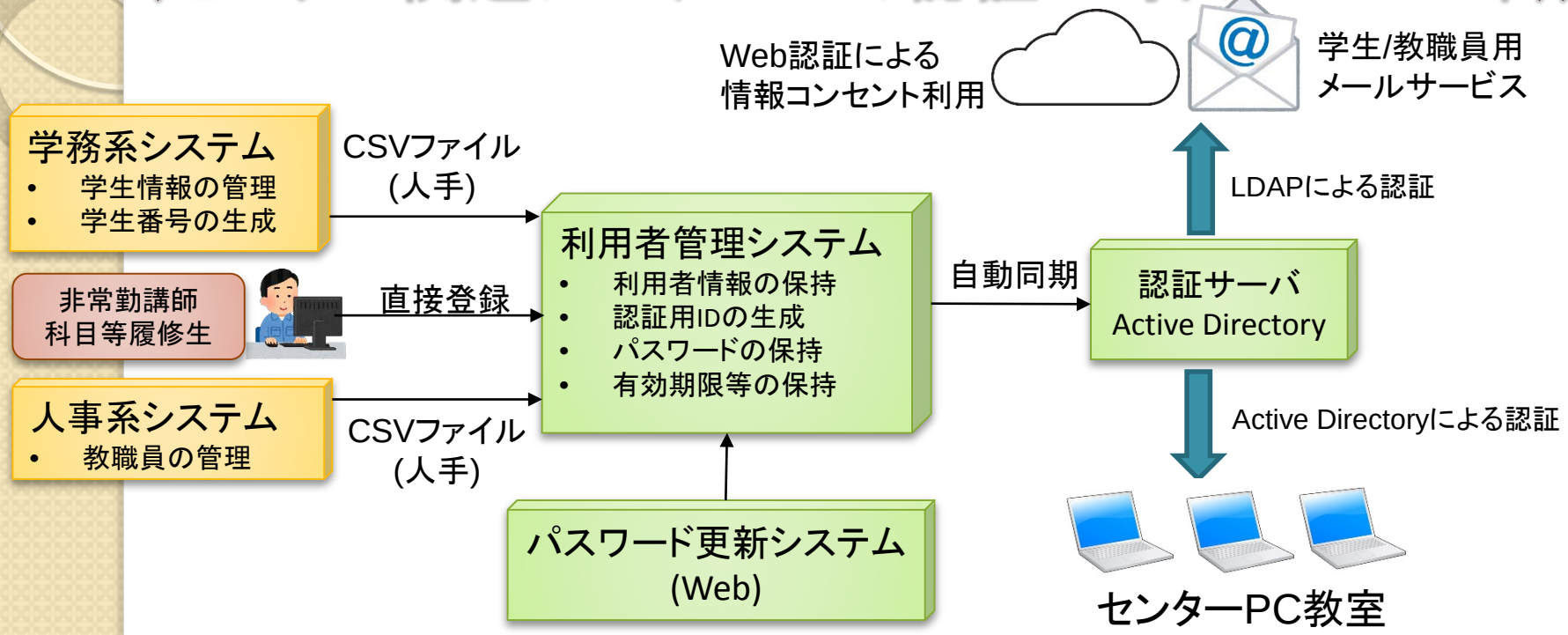
学認への参加？（本発表の内容）

- 「学認」に参加したい
  - 「まずは学内統一認証からでしょう」
    - まぁ、そうですね。
    - 鹿児島大学での認証IDの歴史を振り返ってみる
  - 鹿児島大学が「学認」に参加すると何がよくなるの？
    - eduroam は使えるようになります。その他は… よくわかりません。
    - うち（センター）がだけでなく、図書館もいろいろやってただかなければ、おそらく便利になりません。

鹿児島大学の概要

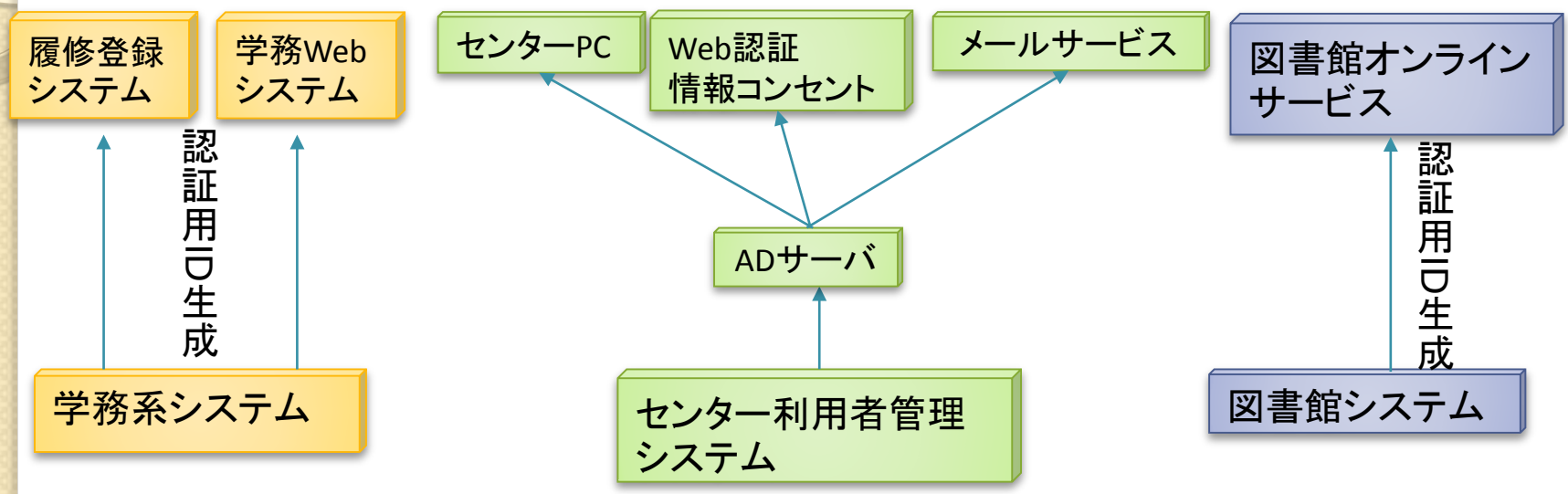
- 学生数(11,000名程度)
- 常勤職員数(2,600名程度(うち1,000名近くは大学病院)
- 9学部、9大学院
- 医学部・歯学部附属病院(病床数: 715床)
- 学内共同教育研究施設等(15施設)
  - 教育学部附属学校もある

学術情報基盤センターの認証システム（センター関連システムのみ認証の時代(～2008年)）



- 学生系、人事系ともに半年に1度程度、CSVファイルでデータをもらう
- 学部学生に対しては、全員にID発行および配布。大学院生は申請者のみ配布（IDは作成しておく）
- 教職員は申請者のみにID配布(IDは作成しておく)
- 科目等履修生や非常勤講師に関しては、申請ベースで情報入力、ID発行/配布

利用者から見た認証ID(2008年当時)



- 学務系、センター系、図書館系でそれぞれIDを作成/配布
  - 学務系は口頭でのみ公表
  - センター系は「学術情報基盤センター利用証」
  - 図書館系は「図書館利用証」
- それぞれは連携していない

学内認証IDの連携のはじまり(2008/2009年～)（1）

- 生涯メールサービス開始を機にセンター発行のID体系の変更
  - 生涯メールサービス(Live@Edu:現 Office 365)
  - 以前は、身分(学生/教職員)、学部/大学院別、所属学部、学生番号をベースにしたID体系
    - 学部移動等があると、IDを再発行
      - メールサービスでメールアドレスの変更が必要となる
- 変更点
  - 身分等によらず**‘K’ + ランダムな番号**
    - 身分が変わっても同じIDを使えるように
      - 実質的にこの運用は破綻した(後述)
    - 将来的な「全学統一認証ID」を目指して設計した物ではなかった。
      - できたらいいな程度

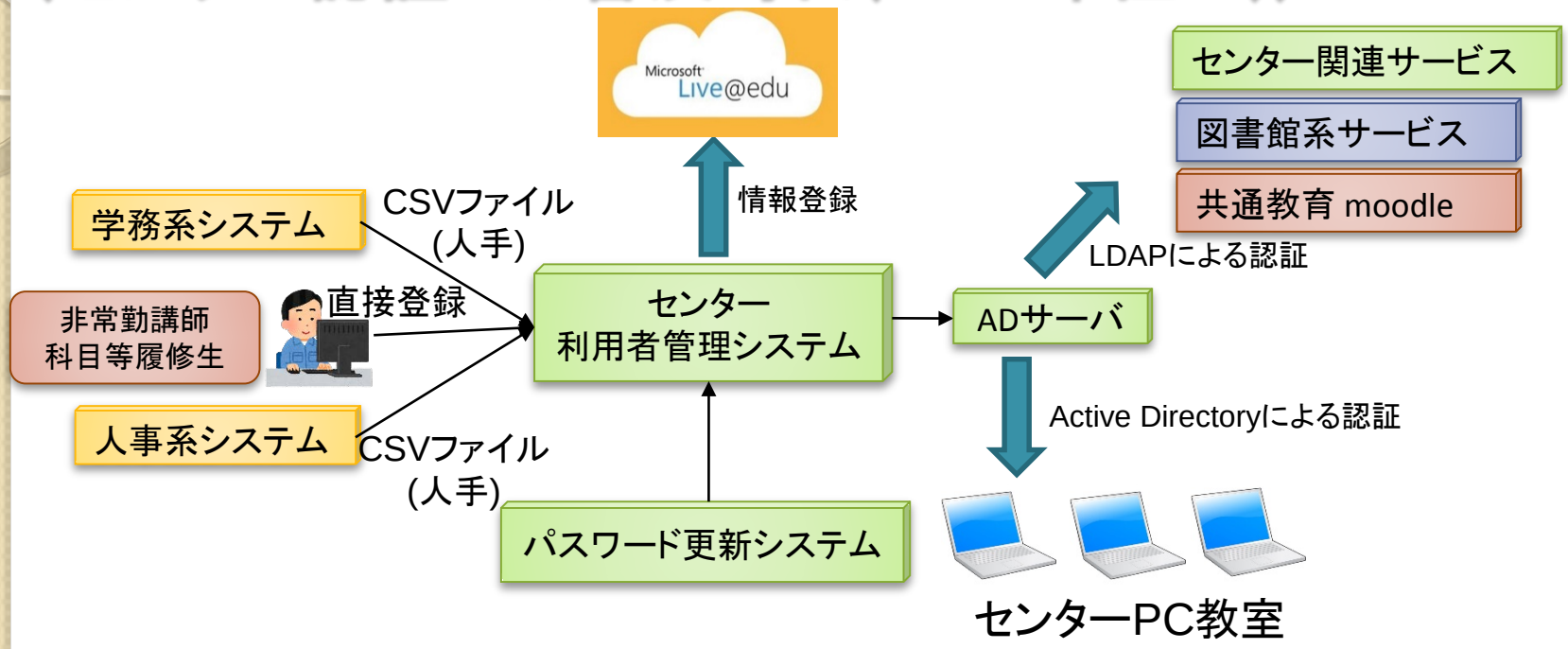
センターの認証IDの運用

- 入学時に「学術情報基盤センター利用証」を配布
  - 認証用IDと初期パスワードを記載
  - 一ヶ月以内に初期パスワードを変更しないとロックされる
  - パスワードを忘れた場合
    - 事前に「秘密の質問とその答え」を登録していれば、Web上で自身で変更可能（2009年～の新機能）
    - その他の場合は、センター受付にて「利用証記載の初期パスワード」に初期化
  - 利用証を紛失した場合
    - 初期パスワードを変更して再発行

学内認証IDの連携のはじまり(2008/2009年～)（2）

1. 図書館システムの更新時にセンター認証サーバと連携
   - センター認証サーバ(Active Directoryサーバ)をLDAPサーバとして連携
   - 提供する属性情報は口頭でのみ公表
   - 連携に至った理由（図書館側理由）
     - 新図書館システムではオンラインサービス範囲が増加、そのため、図書館システム側で認証を独自実装するのは効率が悪いと思われた。
     - オンラインサービス利用者が増え、なおかつ2008年度から運用開始された鹿児島大学教職員証への対応を検討する中で、図書館独自での全教職員のオンラインサービスのパスワード管理に限界が生じてきたこと。
   - 連携に至ったわけ（センター側）
     - 図書館システムの調達にセンター職員が参加→人的連携が容易
2. 共通教育(教養教育)で利用されている moodle の認証連携
   - moodle 運用開始当初は連携していなかった。しかし、すぐ(運用開始1年程度？)連携
     - パスワードの運用管理の負荷大（moodle 側理由）
     - moodle の運用Working Group にセンター職員が参加→人的連携が容易

学術情報基盤センターの認証システム（センター認証IDの普及時代(2009年位～)）

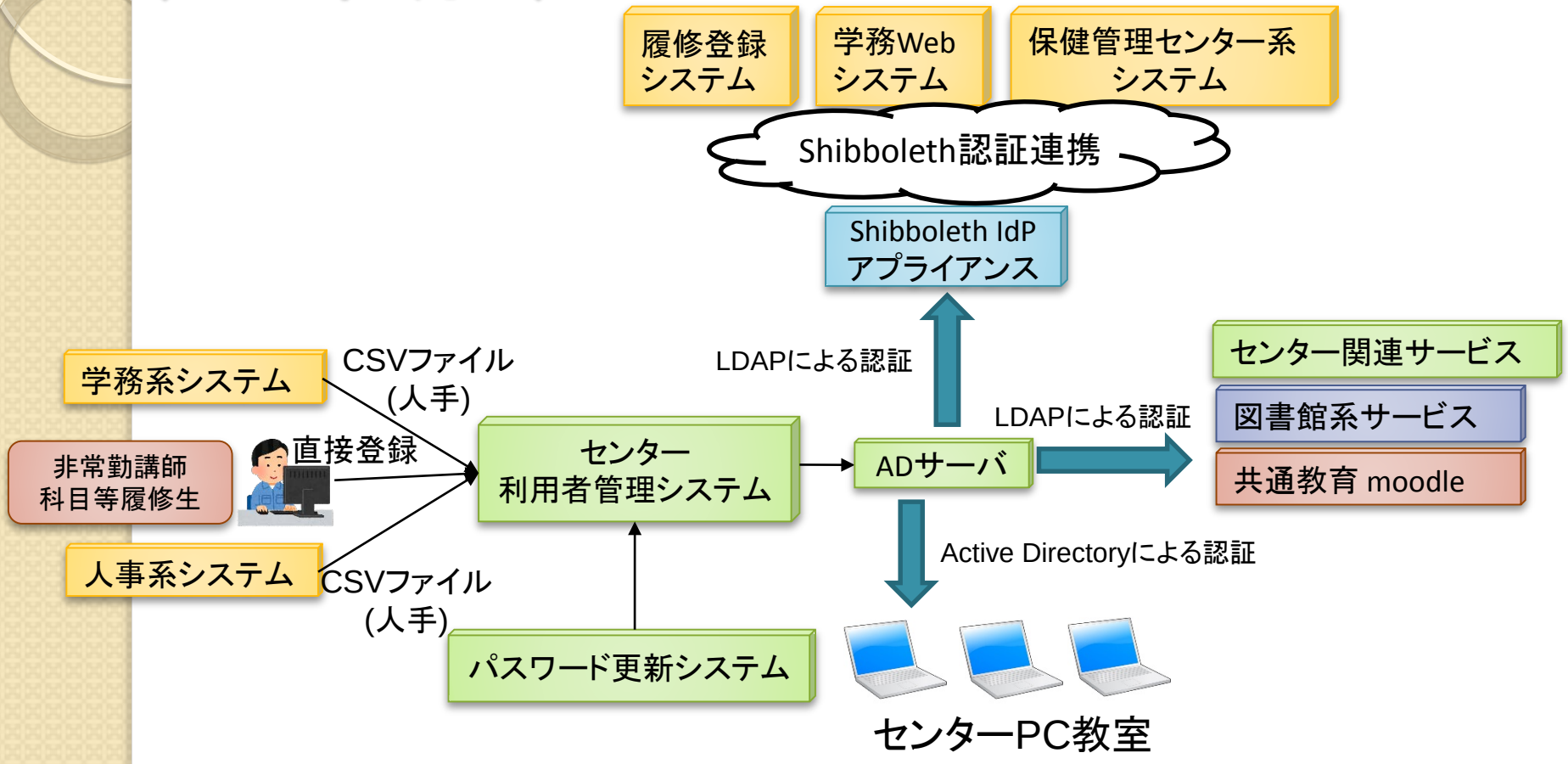


- 2009年にセンター利用者管理システムの更新：構成は以前とほぼ同じ
  - 大規模に変更する時間的/費用的余裕がなかった
- 学生系：2011年頃？より1ヶ月に一度程度、CSVファイルでデータをもらう
  - 学務システムを扱っている部署が基盤センターに近くなったため（情報企画課）
- 人事系：半年に1度程度？、CSVファイルでデータをもらう
- 科目等履修生や非常勤講師に関しては、申請ベースで情報入力、ID発行/配布

学内統一認証の動き(2012年頃～2014年頃)

- 学務系システム改修の動きに合わせて、学内統一認証システムへの要望が高まる(2012年後半)
- 学内統一認証システムの学内予算確保(2013年後半)
  - センター発行の認証IDで行うことを確認
  - Shibboleth認証で行うことも決定
    - 個人的に「Shibboleth、Shibboleth」と連呼してみた
  - 2013末に導入し、動作検証/運用方法の検討
    - 既存システムのSP化のドキュメント等の整備
- 学内統一認証システムの本格運用開始(2014年6月)
  - 学務Webシステム、保健管理センター(定期健康診断システム等)が最初に連携
  - 2014年9月より履修登録システムも連携
- 提供属性
  - 口頭でのみ公表

センターの認証システムと統一認証システム (2014年6月～)



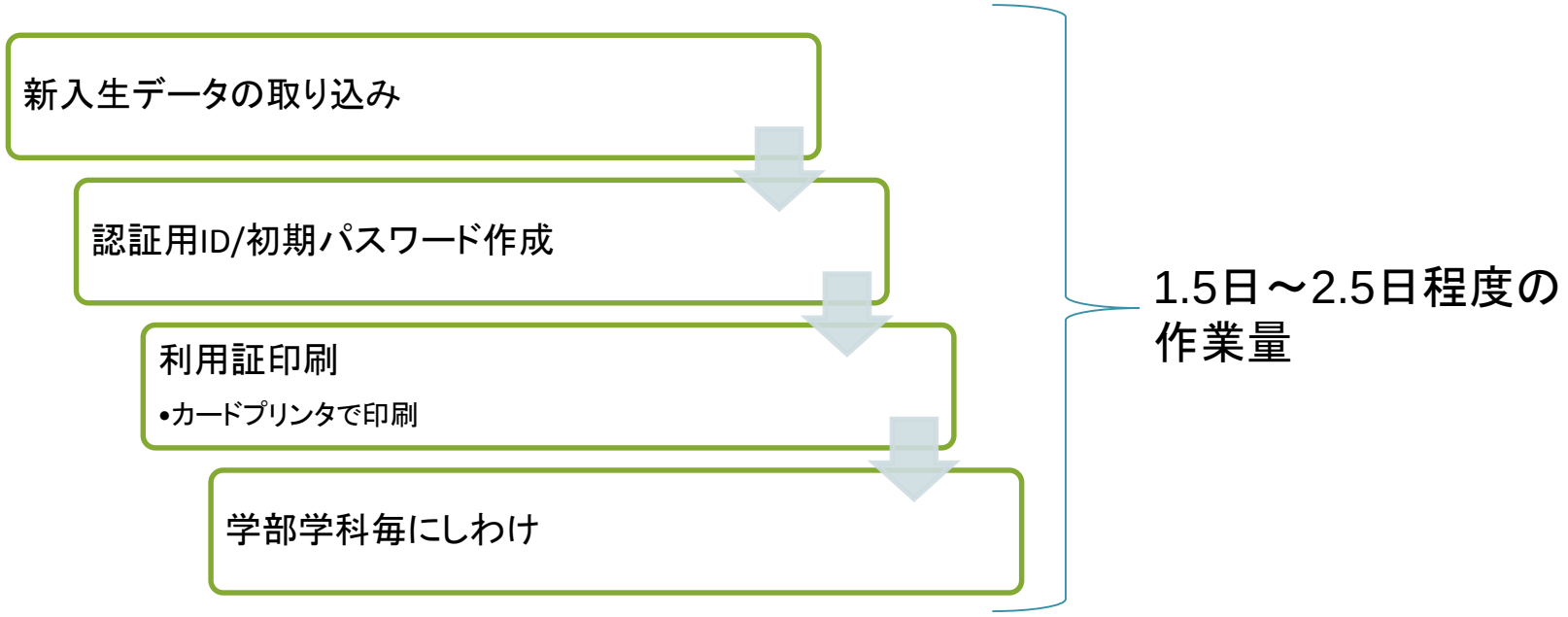
- 統一認証システムは、既存センター認証システム上にかぶせただけ
- 新規連携システムのみ Shibboleth 対応となった
  - 他システムの改修予算なしのため

センター利用者管理システムの更新(2015/09)

- 6年毎の更新(前回は2009年)
  - センター利用者管理システムは「ネットワークシステム」調達の一部
- 2014/06～運用の統一認証IDの運用および連携システム運用上の問題が見えてきていた
  - センター認証IDの名称を「鹿児島大学ID」へ
  - IDの新入生への配布問題
  - IDおよびパスワードに関する問い合わせ問題
  - 「身分が変わっても同じIDが使えるように」の破綻
  - IdPの更新/保守継続性

新入生用センター利用証の作成

- 学務系システムより新入生のデータをいただけるのは xxxx/3/31 17:00 以降
  - 学生番号が定まらないため



利用証の配布問題

- 新入生履修登録は4月4日に全員を1カ所に集めて行う(前日に学部新入生オリエンテーション)
  - 履修登録システムが連携する前の時代
    - 履修登録後、センターに全員来ていただいて利用証配布、初期パスワードからの変更、「秘密の質問とその答え」の登録
      - 初期パスワードを変更させる理由:5月になってから「利用できません」ユーザが殺到
  - 履修登録システムが連携した2015年4月
    - 4月3日早朝までに利用証作成、学部オリエンテーションで配布
      - 利用証作成がさらにタイトなスケジュール
    - 4月4日:初期パスワードで履修登録、その後、センターにてパスワード変更、「秘密の質問とその答え」登録
      - 利用証を忘れてくるユーザ
      - 初期パスワードをなかなか入力できないユーザ(履修登録に時間がかかる)→担当課から文句

利用証の廃止(2015/9～)

- 「一部学生のみがセンターを利用」時代の名残り
- 「鹿児島大学ID通知書」に変更
  - 鹿児島大学IDとパスワードを登録するためのパスコード(数字のみX桁)をA4で通知
    - パスワードを登録するとパスコードは無効
    - 新入生用ID作成、通知作業が大幅に短縮
  - パスコードの有効期限は従来の「初期パスワード」より短く
- パスワードを忘れた場合の手段
  - 事前に「秘密の質問とその答え」の登録
  - 事前に「パスコード通知用メールアドレス」の登録(新機能)
  - センター窓口および各学部学生係窓口にて新規パスコードの通知
- 2016/04/04 の履修登録
  - 04/03までに「鹿児島大学ID通知書」配布
  - 履修登録前にパスワード設定、その後履修登録
  - 「秘密の質問とその答え」「パスコード通知用メールアドレス登録」は全員受講の教養科目「情報活用」の第1回授業で設定するよう依頼

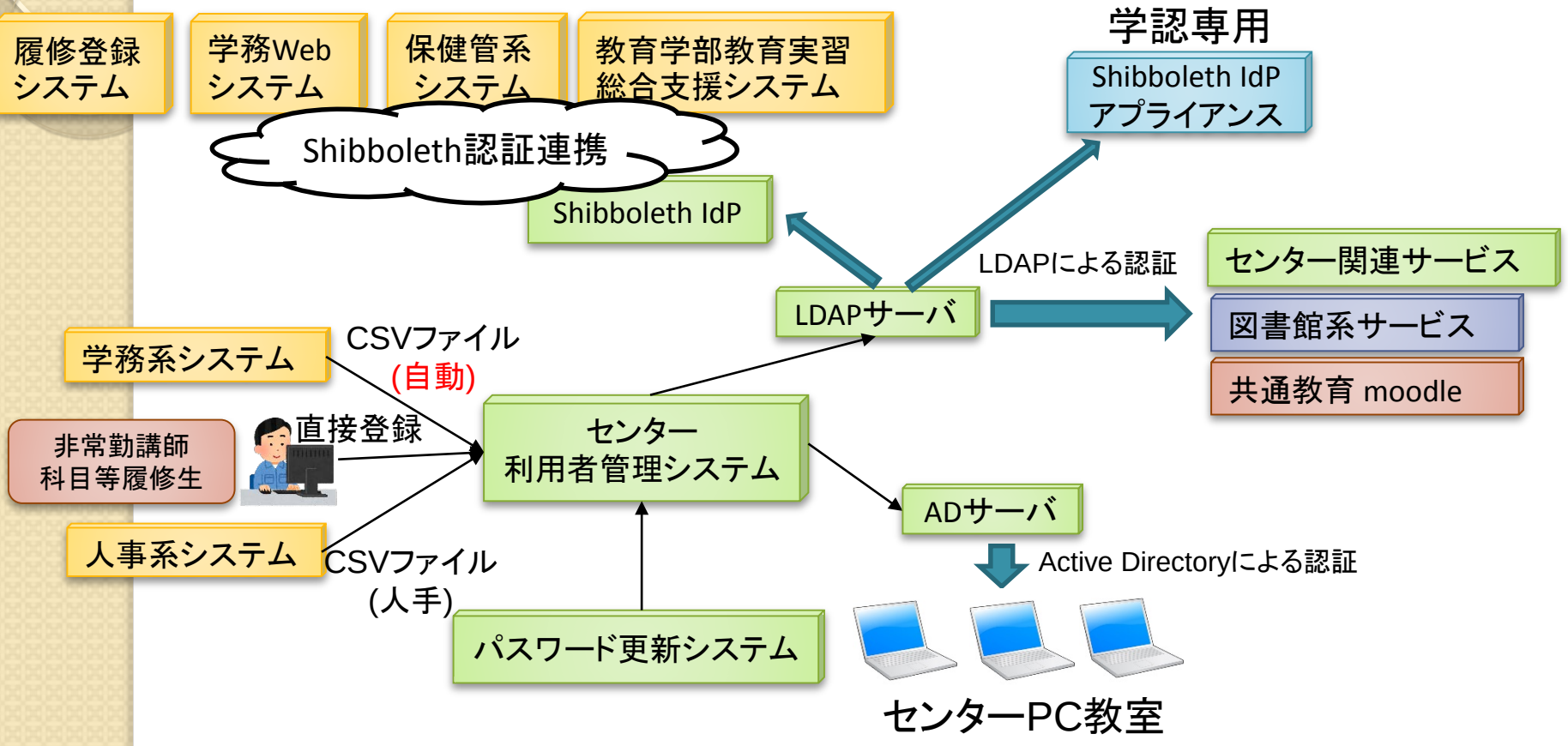
「身分が変わっても同じIDが使えるように」の破綻

- 生涯メールを開始するにあたって、「学部時代の認証IDで身分が変わってもメール＆センター利用ができるように」
  - 実際に運用してみると…
    - 学部時代の情報と大学院の情報がリンクしていない(学務系システムに存在しない)
  - 利用者の申請でIDに紐付く情報を付け替え
    - 「付け替えるユーザ」と「付け替えずIDを2つ持つユーザ」
      - センター利用の場合は、学部時代のIDは卒業時に無効となるが、生涯メールでは有効
- 大学院生の履修登録(Web)も 4月4日
  - 結局、大学院生全員に認証ID配布
  - 付け替える時間余裕無く、IDを利用し、履修登録
    - 事実上、付け替えるユーザは、ほぼいなくなる
- 2015/09 より、付け替えを廃止

IdPの更新/保守継続性

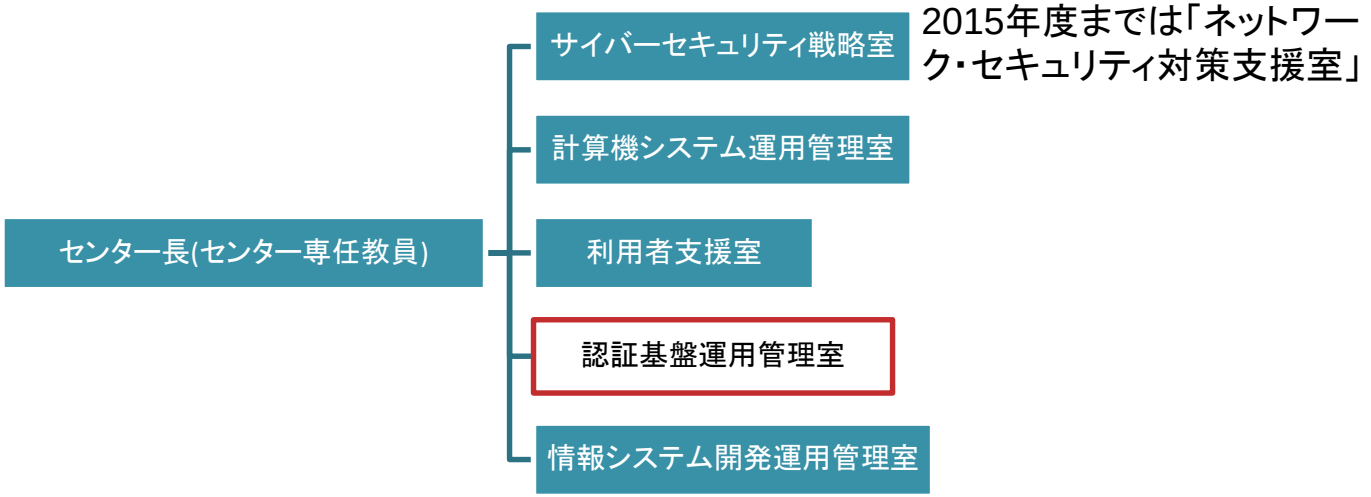
- 2013年末に学内予算で購入した「Shibboleth IdP アプライアンス」
  - 毎年毎年、保守経費(ハード/ソフト)がかかる
  - 将来、機種耐用年数時の機種更新の際、予算確保はできるのか？
- 2015/09の「ネットワークシステム-利用者管理システム」調達にShibboleth IdP も含める
  - 仮想マシンとなった
  - 大きな変更以外は、調達の範囲内で保守
- 「Shibboleth IdP アプライアンス」は学外認証連携用(学認専用)
  - 調達に含めた IdP は「学内 Shibboleth 認証連携専用」とする
  - 設定変更がある場合、学内用と学外用を分けた方がよいと判断
    - しくじった時、「学認だけが利用できません」で済む

鹿児島大学ID認証システム (2015年9月～)



- 認証サーバとして、ADサーバとLDAPサーバを分離
- 学生情報は学務系システムより毎日取り込める状態
  - 毎日取り込んで登録しているわけではない

センター内組織構成の変更



- 専任教員6名、業務系常勤職員3名、業務系非常勤職員3名
- 各室に室長1名(教員)、室員は全教員＋職員
- 認証基盤運用管理室の新設(2016/04～)
  - 業務内容
    - 鹿児島大学IDの運用、学内認証基盤(学内IdP)の運用、学認用IdP運用、UPKI
  - 昨年度までは
    - 利用者管理システム/UPKI →現「サイバーセキュリティ戦略室」
    - IDの運用→利用者支援室
    - 学内IdPの運用→情報システム開発支援室

学認への参加 – IdPの用意

- 2013年末に導入した「Shibboleth IdPアプライアンス」で学内統一認証をShibboleth へ
  - IdP や SPの構築/運用技術をつけた
  - 2015/09「ネットワークシステム-利用者管理システム」調達でのIdP移行も問題なし
- 2015/09 以後、アプライアンスは実運用に利用していないため、自由にいじれる
  - 技術的課題はほとんどない。

学認への参加 – どのSP?

- 「学認」に参加してどのようなSPを利用する/したいのか？
  - センターはIdP提供側であり、どのようなSPを利用したいのか、わからない
  - (私が思う)有用なSPは、ほぼ「別途契約」
- 図書館の人に聞いてみる
  - 機関契約しているサービスのオプションで「学認でも認証可能」
    - 機関契約(大学のIPアドレスで判定)しているため、学内からは、ほぼほぼ利用可能
    - 学外からは「基盤センターVPSサービス」を利用すると学内扱いで利用可能(ライセンス的に大丈夫かは未確認)
  - 「学認に参加してないと利用不可」という状態でない
    - 図書館側から:「現在機関契約しているサービスで、無料でShibboleth 対応している所とは、連携したい」

学認への参加 – どの属性？

「GakuNin道しるべ」より

- 属性情報について
  - 学認では18種類の利用者に関する属性情報を定めていますが、属性情報を全て準備する必要はありません。広く利用されているものはごく一部に限られます。最低限準備が必要なものはO、jaO、eduPersonPrincipalName、eduPersonTargetedID、eduPersonAffiliation / eduPersonScopedAffiliationです。
  - SPごとに要求する属性情報が決まっています。大学として利用したいSPを選定し、SPごとの情報（SP一覧に掲載）を参照して必要となる属性情報のみ送出するようにIdPを設定してください。

- 連携したいSP毎に必要な属性を一つ一つ調べろって事ね。
  - 結局は最低限でよさそうだ。

- 利用者の範囲について
  - 学認において認証できる利用者の範囲は、原則として、教職員（名誉教授を含む）および学生です。電子ジャーナル等、有償サービスの契約条項で定められた利用者の範囲とは異なることがあります。各サービスとの契約が優先されますので、これに反することのないよう注意をお願いします。

- IdP担当者(センター)とSPとの契約者(図書館)とで利用者の範囲の確認を行えって事ね。
  - あるSPと、あるSPで eduPersonAffiliation = member の解釈が違ったらどうするんだ？

学認への参加 - eduroam

「学長と学部卒業予定者との懇談会」

〔要望〕
本学では学術情報基盤センターに利用登録して学内のシステムを利用しているが、他大学では、どこの大学の学生であっても、その学生の所属大学の認証IDを使って、大学のネットワークを利用できるエデュローム（eduroam）というシステムが導入されている。本学も学術認証フェデレーション（学認）に参加してシステムを導入してほしい。
〔回答〕
現在、前向きに検討中である。

- 心の声

  口頭でのみ公表

- eduroam を利用できるように
  - 学認への参加
  - (RADIUS Proxy も準備中)

学認への参加 – 現在の状況

- 2016/06月末
  - テストフェデレーションに参加済み(自構築 IdP v2 と IdP v3)
  - 「Shibboleth IdP アプライアンス」のv3対応を待つ
- 2016/11月上旬
  - 「Shibboleth IdP アプライアンス」のv3へのバージョンアップ & テストフェデレーションに参加して動作確認
  - 一気に本番系へ移行？
    - とりあえず、契約なしのSPから利用できるようにするか？
- その後
  - 図書館と調整して、機関契約しているサービスで学認が利用できるSPと追加契約

学認への参加が遅れた理由(本発表の総括)

- 「利用者管理システム- 認証システム」は、センター「ネットワークシステム」調達の一部
  - 6年更新(2009/09, 2015/09)のため、抜本的な修正は、そこでしかできない
  - 2013年末の「学内統一認証システムの学内予算確保」は、内部的な強い要求
    - 「学認参加」のみの理由だと、予算は確保できなかったと思う
- 学認対応サービスの一部とは包括契約しているので、不便ではない
  - 「イチオシSP」ってありますか？
    - 要件:
      - 学認に参加していないと利用手段はない
      - 「他の大学では利用できるのに本学が学認に参加していないので利用できない」と学生から声が上がるくらい
      - (できれば無償):有償だと「お金がないから」で、学生の声を却下できる可能性
  - IdP担当者はSPのことをよく知らない
    - 私はよく知らない。知らなきゃダメ？

IdP担当として

- 一度は言ってみたいセリフ

ヤマト 工作班長：真田志郎

「こんなこともあろうかと、
既に 

参加済みです」