増えるシステム、認証管理をどう軽減するか？
-福岡大学における統合認証-

福岡大学　総合情報処理センター
奥村　勝

2009年1月29日　SS研究会システム技術分科会

福岡大学

発表内容

- 1. 福岡大学の概要
- 2. 統合認証システムの現状
  - 実現できたこと、実現できていないこと
  - システム構成
  - 運用状況
- 3. 連携システム事例
  - 教務系Webシステム
  - ICカード向け共通基盤
- 4. 組織と認証
- 5. まとめ

福岡大学

1. 福岡大学の概要紹介

- 9学部、31学科、10大学院研究科、
  2つの大学病院からなる私立総合大学

- 大学規模
  - 学生数
    - 約21，000人
  - 教職員（病院含む）
    - 約3，000人
  - キャンパス内のPC数
    - 約5，000台弱

福岡大学

2. 福岡大学における統合認証の現状

- 平成17年（2005年）4月より稼働開始
  - 4年弱の運用期間が経過
  - 導入の経緯 → 予稿集をご参照ください

- 学内の情報システム利用時のIDとパスワードを
  一組に整理し、一元的に管理

- 連携済みシステム
  - 全学規模 13サービス（システム） 5部門
  - 小・中規模 6サービス（システム）

- 登録者数 約24，000名

2．1　実現できたこと

- 大学の情報基盤として全学サービス用のアカウントを一元管理する仕組みを提供
  - アカウント管理（発行・削除）
  - 連携する情報システムへのアカウント配信
  - 連携する情報システムへの認証機構の提供
  - パスワード変更の一元化
  - ICカードの発行情報の一元管理
- 導入効果
  - 利用者の利便性向上
  - 管理者/運用部門の負担軽減

連携済みシステム一覧

連携システム名	運用部門	学生	教職員
教育研究システム	総合情報処理センター	○	○
情報コンセント（有線・無線）		○	○
PPP		○	○
SSL-VPN			○
ウィルス対策配布			○
E-learning		○	○
ポータルシステム	教務部	○	○
自動証明書発行機		○	
図書システム	図書部	○	○
グループウェア	総務部		○
旅費申請システム			○
電子文書ライブラリ			○
研究者情報システム	研究推進部		○
その他の小規模システム（6）	学部等	○	○

利用者の立場から

- 学内情報システム利用時のID/パスワードの共通化

- 導入前
  - 利用システム毎にID/パスワードを個別に管理、使い分けが必要
  - トラブル時の問い合わせ先が分かりにくい

- 導入後
  - 1組のID/パスワードでさまざまなシステムを利用できる
  - トラブル時の問い合わせが分かり易くなった

部門システムの管理者の立場から

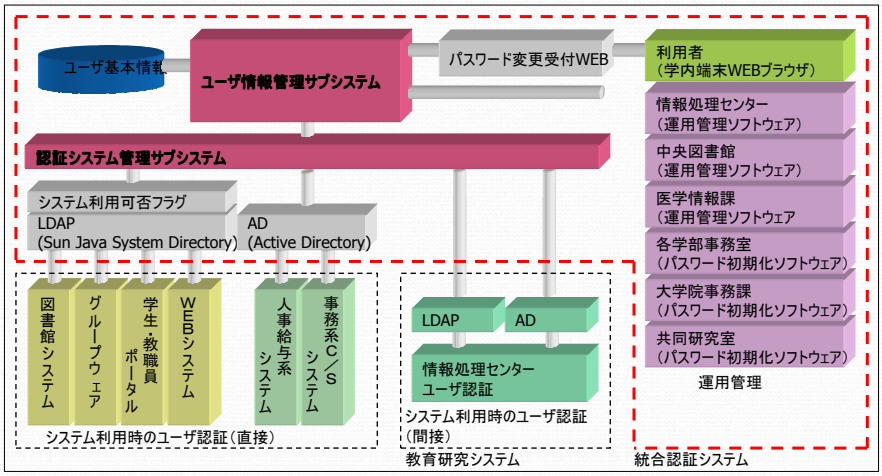
- アカウント(IDとパスワード)の一元管理
  - アカウント発行・削除、連携システムへの配信
  - パスワード変更

- 導入前
  - システム毎にアカウントを管理(追加・削除)
    - 学生情報や人事情報を運用部門毎に入手して個別対応
- 導入後
  - 統合認証システムと連携することでアカウント管理の負担が大幅に軽減
    - アカウント管理は、統合認証システムの運用部門が実施
    - 問い合わせ対応も、統合認証システムの運用部門が窓口に

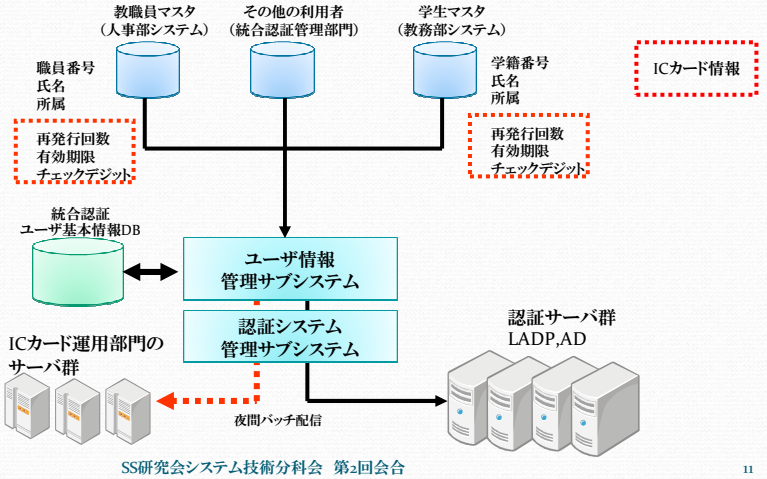
2．2　まだ実現できてないこと

- SSO（シングル・サイン・オン）の標準的な仕組みの提供
  - 現状、アプリレベルで可能なところは「見かけ」上認証をスキップしているが、SSOの仕組み自体は提供していない
- 生涯ID対応
  - 教職員：　職員番号は人事部で継続割り当て
  - 卒業生：　卒業生への生涯メールアドレス配布の話題もチラホラ
- ユーザ情報リポジトリとしての活用
  - 認証DB以外の情報DBとしてのデータの収集、活用
  - 権限管理等に活用
- 学外組織との認証連携（UPKI）
- PKI対応

2．3 統合認証システムの構成



アカウント情報の流れ



ユーザ基本情報として管理する項目

- 学生情報
  - 教務システムより
- 教職員情報
  - 人事システムより
- 黄色部分の情報は、後述の権限管理に利用

項目	学生	教職員
氏名	○	○
アカウント名/パスワード	○	○
職員番号（学籍番号）	○	○
職種		○
雇用区分		○
発令資格		○
職務役職		○
所属部/所属学部	○	○
所属課/所属学科	○	○
現状区分	○	○
採用年月日/入学年月日	○	○
退職年月日/入学年月日	○	○
ICカード再発行回数	○	○
ICカード有効期限	○	
チェックデジット	○	○

2．4　運用状況

- パスワードの有効期限（1年間）
  - 一組のID/パスワードが盗用されると多数のシステムが利用されてしまう恐れ
  - Web履修等の混乱を考慮した期限措置
    - 春先は5月末に自動延長
  - 2008年年12月末での期限切れ者数
    - 教職員　有効 2，170人　期限切れ　510人
    - 学生　　有効20，295人　期限切れ　562人

パスワードの初期化対応

- 有効期限切れ、パスワード忘れへの窓口対応
- 1日のみ初期パスワードへ戻し、即日変更
- 当日変更しないと、翌日からは利用不可
- 2008年1月~12月の初期化件数
  - 教職員　709件、学生　7，236件
  - ピークは6月　1，700件

3. 連携システム事例

- 教務系Webサービス
- ICカード情報共通基盤

3. 1 教務系Webサービス

- 学生向けサービス
  - 履修登録
  - 時間割確認
  - 成績確認
  - 出席状況確認
- 教員向けサービス
  - シラバス登録
  - 出席簿ダウンロード
  - 成績登録
  - 出席状況確認・修正
  - 講義支援
- 原則、すべてインターネットからも利用可能

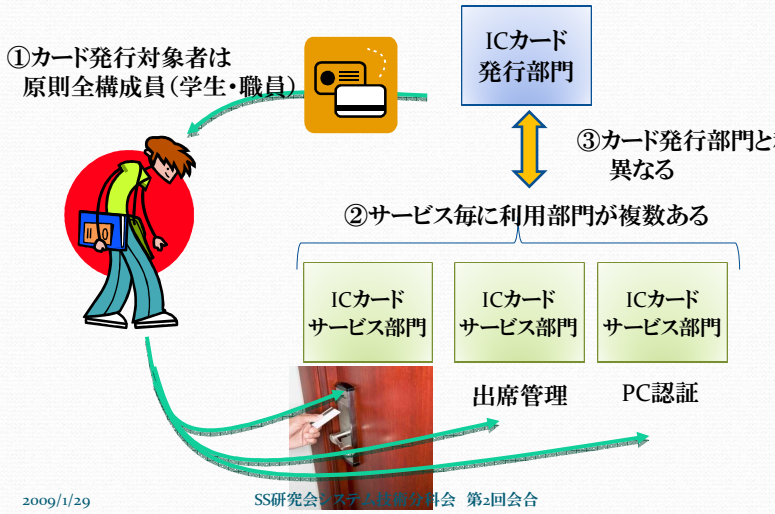
教員によるWeb成績登録

- 担当講義の成績のWeb提出
  - Web画面からの成績入力、CSVによる一括登録
    - 最終的には紙に印刷し、目視チェック後提出
- 非常勤の利用も考慮し、インターネットからも可能
  - アクセス期間限定
  - 統合認証＋別キーワードによる認証の二重化

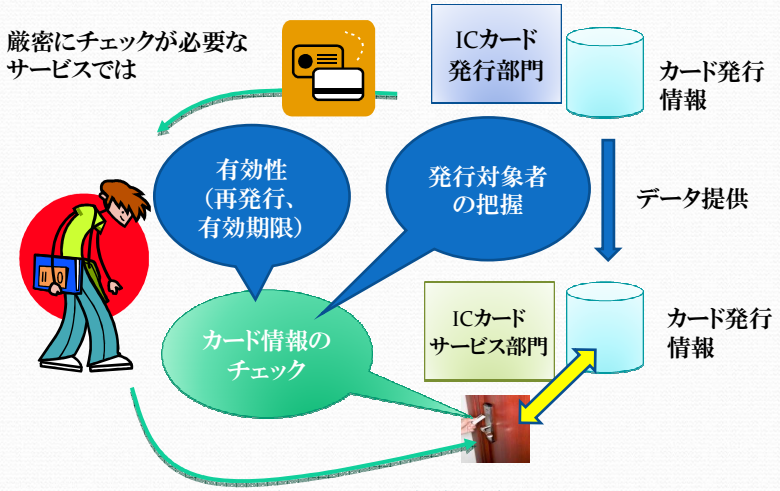
3．2 ICカードの学内利用

- Felica FCFによるICカード学生証/職員証
- キャンパスでの利用サービス
  - 出席調査
  - 図書貸し出し
  - 証明書発行
  - 入館・入室管理
  - PCログイン認証

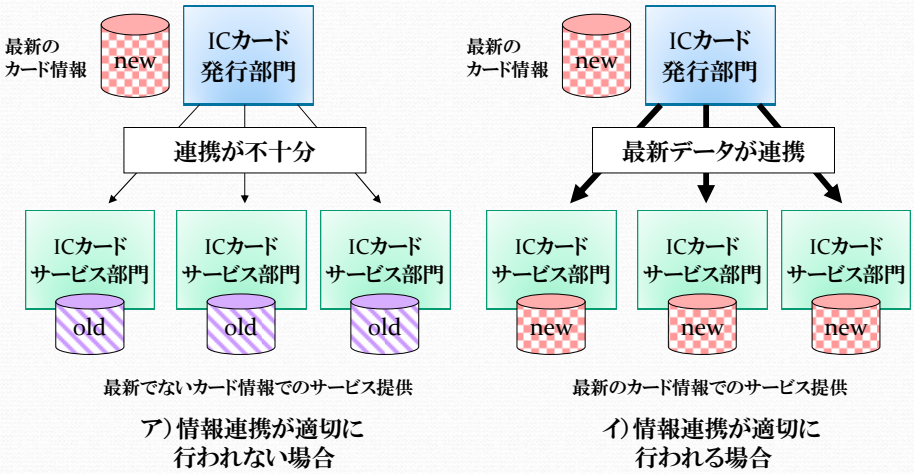
キャンパスにおけるカードの発行と利用



カード利用時のチェック



ICカード発行情報の連携



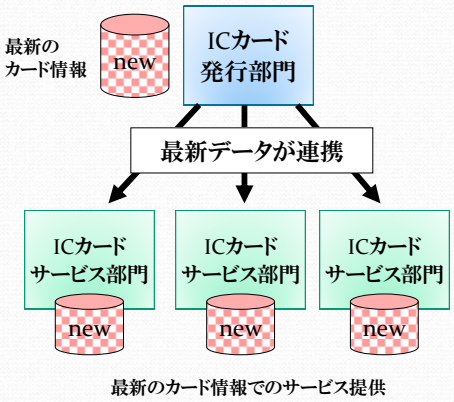
ICカードサービス運用時の課題

- ICカード情報を管理する全学的な仕組みが必要
  - 有効性のチェック
  - 発行管理（新規発行、再発行、廃止）
- 情報システムのアカウント管理と同様の問題が、ICカードサービス運用部門に生じる
  - 幸いにして「人」に紐づく問題である

福岡大学

ICカード向け共通情報基盤の整備

- カード発行の最新情報を利用部門に情報連携させる仕組み
- 情報連携は夜間バッチにて最新情報をファイルで提供
- 既存の統合認証システムの追加機能として実装



福岡大学

4. 福岡大学における組織と認証

- 組織構成員に対するアカウント発行方針
- 認証と権限の分離

福岡大学

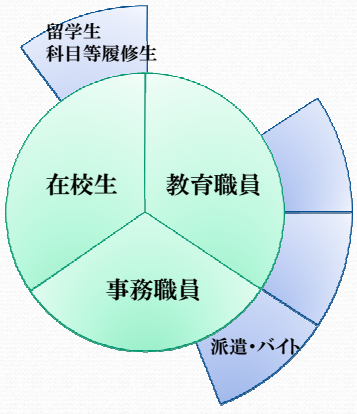
4．1　福岡大学でのID発行方針

- 統合認証アカウント（ID/パスワード）
  - 全学的なシステム利用が必要な人
    - 学生　→　無条件発行
    - 教職員　→　申請制/部署申請
  - 全学的なシステム利用が不要な人
    - なくても不自由しないので申請しない人が大半
  - 利用者からの申請がベースの考え方
- ICカード（学生証/職員証）
  - 身分証として必ず発行される

福岡大学

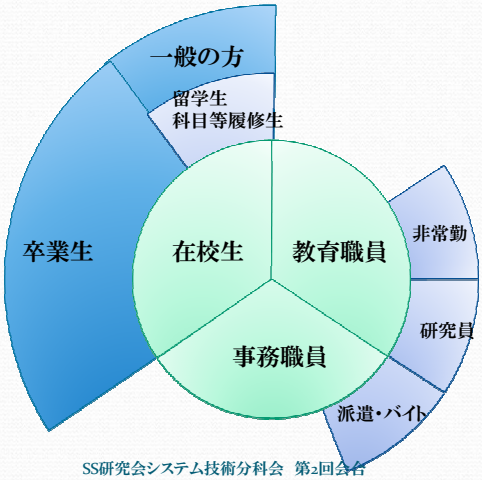
大学の組織構成員

- 固定メンバー（常勤）と流動メンバー（非常勤・派遣等）



サービス対象者

- 構成メンバーと必ずしもイコールではない



統合認証ID発行状況（学生編）

	在籍	統合認証ID	ICカード	ポータル	教研	図書
学部学生	○	◎自動発行	◎	◎	◎	◎
大学院生	○	◎自動発行	◎	◎	◎	◎
交換留学生		◎自動発行	◎	×	◎	◎
科目等履修生		◎自動発行	◎	◎	◎	◎
研究生	○	◎自動発行	◎	◎	◎	◎
一般市民		○	×	×	×	○

統合認証ID発行状況（職員編）

	常勤	統合認証ID	ICカード	ポータル	教研	図書
専任教員	○	○申請	◎	◎	○	◎
非常勤		○申請	○	◎	○	○
研究員		○申請	×	×	○	○
専任事務職員	○	○申請	◎	◎	×	◎
派遣職員		○部署申請	△部署	○部署申請	×	○
アルバイト		○部署申請	△部署	○部署申請	×	○
看護職員	○	○申請	◎	×	×	◎
研修医	○	○申請	◎	×	○	◎
名誉教授		×	×	×	×	○

IDとICカード発行区分の整理

統合認証ID発行

		学内構成員	学外者
自動発行	無条件	○	本人管理
申請発行	本人希望	○	
部署申請発行	所属長の決裁		○ 部署管理

ICカード発行

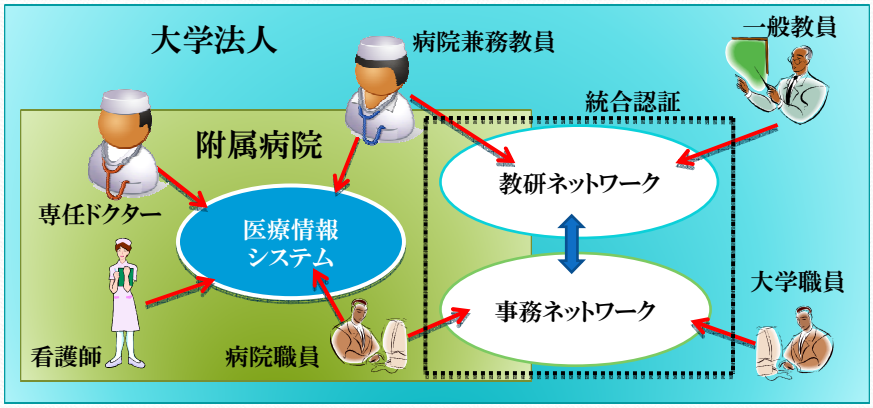
		学内構成員	学外者
自動発行	無条件	○	本人管理
申請発行	本人希望	○	
部署申請発行	所属長の決裁 部署用にカードを発行 部署内でカード管理		○ 部署管理

アカウント未発行問題

- 全構成員へのアカウント発行を前提としたいのだが・・・
  - 付属病院の看護職員、付属中・高校教員はID未取得
    - 医療業務以外の業務端末がない → アクセス手段が未整備
    - 医療業務以外の利用用途がない → キラーサービスが不在
    - 病院業務、付属学校という組織・業務的な独立性が高い
  - 将来的な全構成員対象サービス実施時に混乱が・・・

付属病院の事例

- 現状、医療情報システムのみのユーザは統合認証は未登録



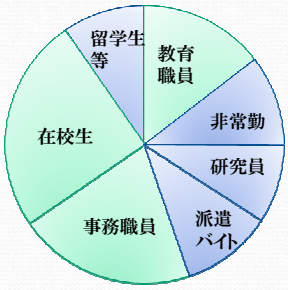
4．2　認証と権限（管理）

- 認証
  - 本人であることを確認する手段
- 権限（管理）
  - その利用者ができることの区別（を管理すること）

- 統合認証システムに求められる機能
  - 1．認証（データ）のための仕組み
  - 2．権限管理のための仕組み

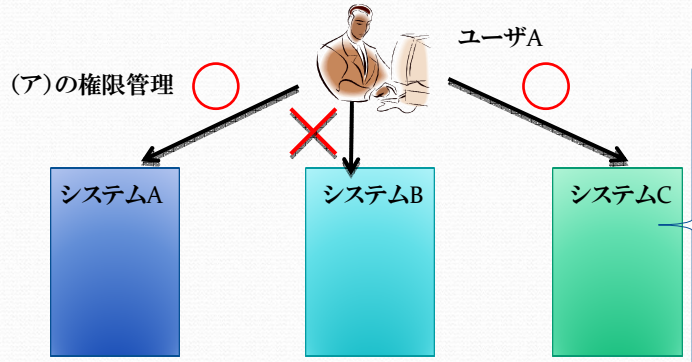
統合認証上のアカウント

- アカウント（ID/Password）情報
  - 認証のための情報
  - 固定・流動の区別なく、フラットに管理されている



権限管理の区分

- (ア)個別システムに対する利用権限管理
- (イ)特定システム内での各種権限管理



統合認証システムのユーザ基本情報の活用

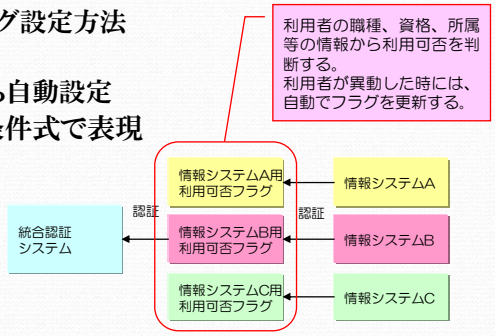
- (ア)の対応
  - システム利用可否フラグ
- (イ)の対応
  - ユーザ基本情報のエクスポート

この部分の情報

項目	学生	教職員
氏名	○	○
アカウント名/パスワード	○	○
職員番号（学籍番号）	○	○
職種		○
雇用区分		○
発令資格		○
職務役職		○
所属部/所属学部	○	○
所属課/所属学科	○	○
現状区分	○	○
採用年月日/入学年月日	○	○
退職年月日/入学年月日	○	○
ICカード再発行回数	○	○
ICカード有効期限	○	
チェックデジット	○	○

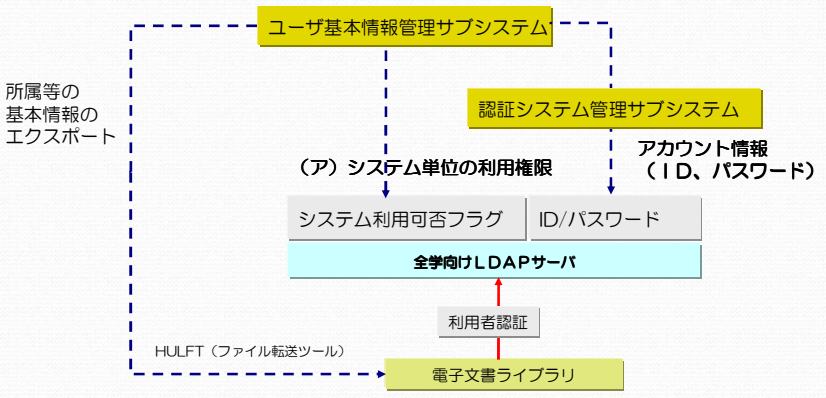
システム利用可否フラグ

- 統合認証システムが管理するシステム利用可否フラグの状態を判断して、システム毎のユーザ認証の成否を行う機能
- 2種類のシステム利用可否フラグ設定方法
  - 職種、資格、所属等情報から自動設定
    - システムの利用資格を条件式で表現
  - 個々のアカウントに対して、ON/OFFを手動設定



ユーザ基本情報のエクスポート

- 例：電子文書ライブラリの権限設定



福岡大学

権限の管理

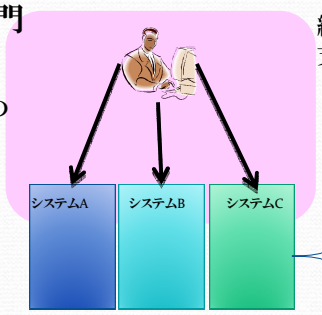
- 現状の統合認証システム
  - 連携システムの権限管理を支援する機能を提供
- 権限ポリシー、アクセスポリシーの管理
  - 各システムの運用部門

誰に利用を
許可するのか？

システム単位の
利用権限管理

誰にどこまで
許可するのか？

システム内の
利用権限管理



統合認証は
支援機能を提供

どこからのアクセスを
許可するのか？

福岡大学

5. まとめ（1）

- 福岡大学における統合認証システムの紹介
  - 主な機能
  - システム構成
  - 連携システム
- 統合認証システムの効果
  - 利用者の利便性の向上（今どきは、当たり前のようですが）
    - システムやサービスを意識しなくてよい
  - システム管理者の負担軽減
    - 統合認証システムの管理部門は、それなりに大変

5. まとめ(2)

- 統合認証導入のポイント
  - 導入に先立っては
    - 組織内で認証システム基盤の必要性を理解してもらう
      - 必要性、予算、導入への協力体制
  - 運用後は
    - 部署を超えた情報・業務連携の重要性
      - マスター情報の提供・更新、部署を跨ぐシステム連携
    - うまく回るかは事務方業務の円滑さ次第
      - 日常の運用に、教員が直接的にタッチすることは少ない