AXIES 2023 認証基盤部会 企画セッション
「多様なサービスの活用に向けた
ID連携におけるID管理に求められるもの」

大学としての ID管理の実情(京都大学の場合)

京都大学 情報環境機構 情報環境支援センター

センター長・准教授

森村吉貴

京都大学

KYOTO UNIVERSITY

京都大学におけるID管理の概要

- 全学的な情報システム・サービス利用のIDとして「全学アカウント」があり「統合認証システム」が100を超えるSPに認証機能を提供
  - Shibboleth/SAML または LDAP
  - 主要SP：Microsoft 365, Google Workspace, 教職員グループウェア, 学内Wi-fi, **電子ジャーナル・データベース**, LMS, 財務会計システム…
- アカウント種別は教員用／学生用／その他に大別
  - 教員用は人事給与システム、学生用は教務情報システムをTrusted DBとみなして情報取り込み
  - その他として、名誉教授等の雇用に基づかない称号付与対象者等にも利用可能SPが限定されたアカウントを付与

情報環境機構／情報環境支援センターの役割

- 情報環境機構
  - 全学のITサービスに係る企画・設計・運用を行う
  - 全学アカウント・統合認証システムを管理する
- 情報環境支援センター（以降、センターとする）**※発表者の所属先**
  - 情報環境機構のITサービス全般のヘルプデスクを担当
  - 全学アカウントの発行・運用を担当

➡ アカウント関係のサポート・トラブル対応は全面的に担当

Know Your Customer (※直訳の意味で)

- そもそも、センターは“顧客”をどの程度知っているのか？
  - 学生は教務情報システム／教職員は人事給与システムを
    Trusted DBとみなす → センターは身元検証の手段を持たない
  - では、教務／人事はTrusted DBを構築している意識はあるか？

    →身元情報を管理するためのDBではなく、あくまで業務用DB
    　本人確認は「業務の必要に応じて」行う
  - ならば、アカウントリカバリは？

    本人から直接センターに問い合わせが来るが、本人確認をどうするのか？
    名前や職員（学生）番号・生年月日を聞く？
    内線番号・学内便で折り返す？　部局の教務・人事に照会する？

    アカウント種別やリカバリ対象に応じて
    上記を組み合わるが、どの方法が最適か確信が持てない

Know Your Customer (※直訳の意味で)

- そもそも、センターは“顧客”をどの程度知っているのか？
  - 雇用・学籍がない関係者には「その他」のアカウントを発行するが、Trusted DBがないため発行時にセンターが直接身元確認を行う
  - センターにできる「身元確認」とは？
    1. 名誉教授証など大学側が発行する身元証明書を確認
    2. 本人の公的身分証＋大学側との関係を示す書類を確認
    3. 各部局の事務担当者からの依頼に基づき発行し、
       アカウント有効化書類を送り返す(Trusted DB取込に準ずる手続き)

  場合に応じて上記を使い分けるが、ポストコロナでは3.の比重が増加

全学情報システム利用規則の一例（全学アカウントの発行根拠）

- 【学生等】 学部学生及び大学院学生、外国学生、委託生、科目等履修生、聴講生、特別聴講学生、特別研究学生、特別交流学生等(京都大学通則（昭和２８年達示第３号)第５章に定めるもの）、研究生、研修員等（京都大学研修規程（昭和２４年達示第３号）に定めるもの）その他本学規程に基づき受け入れる研究者等をいう。
- 【利用者】教職員等及び学生等で、全学情報システム又は特定部局情報システムを利用する者をいう。

→その他本学規程・・・？

職名・称号の多様性

- 当学で確認された教授一覧
  - 教授・特定教授・特定拠点教授・特定外国語担当教授・特任教授・特命教授特別教授・名誉教授・客員教授・招へい教授・特別招へい教授・招聘特別教授・病院教授・臨床教授・法科大学院特別教授・専門職大学院特別教授
- 雇用はあったり（職名）なかったり（称号）する
  - 利用者対応時の切り分けが直感的にできない
- 概ね規定に「教育研究に携わる」的な文言がある
  - 何らかの情報サービスを利用する必然性がある

全学情報システム利用規則

- 第６条 情報環境機構長は、教職員等及び学生等以外の者について、次の各号のいずれかに該当し必要があると認めるときは、全学情報システム臨時利用者として、全学情報システムの利用の許可を与えるものとする。

  (1) 部局情報セキュリティ責任者（＝本学においては部局長指定）より臨時利用の目的・範囲・期間等を明示して申請があったとき。

全学アカウントの利用資格について考える

- 規定に基づく研究員であったり、部局長の申請であれば、
  雇用や学籍の有無に関わらずアカウントを発行可能な
  制度である
- もちろん個別に必要性を判断することは担保されているが、
  必要性の事前の定義はない
  制度運用開始時には敢えて踏み込まなかったと考えられるが
  学内のあらゆるリソースの利用が情報システム・サービスに
  基づくようになるとその判断の意味が非常に重くなる
  - 情報技術の枠内での「認証・認可」だったつもりが、
    大学の構成員としての資格そのものの「認証・認可」を意味しかねない

→情報系のセンター単体では判断しづらい・してはいけない状況が顕在化

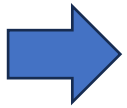
ID発行手続きのケーススタディ：新入生へのアカウント発行の電子化

- 京都大学では入学手続きの電子化推進、履修登録の迅速化のため2016年より学生アカウントの入学前発行を実施
- ３月末までに以下の手続きを実施

［当該図表は資料共有時に割愛］

ID発行手続きのケーススタディ：新入生へのアカウント発行の電子化

- 業務効率化／紙ベース配布物の削減のため
  本人へのアカウント情報の提供を電子化
- 本人確認に利用可能な情報を慎重に検討・再整理
  → 入試・入学業務全体の流れの把握が必要だった



新構成員の
KYCはさらなる
検討が必要

［当該図表は資料共有時に割愛］

認証に付随するアカウント属性情報

- 統合認証システムは認証成功時にアカウント属性情報を
  SPに提供可能
  - 姓名、職種、ID、仮名化ID、大学メールアドレス…
- **別途、部局担当者向けの一括ダウンロード提供システムを準備**
  - SP側のユーザープロビジョニング等に活用可能
  - 源泉DBである人事・教務情報の取り出し手段として汎用に用いられるように
    （100件弱の利用者）

    → 人に関する全学DB的な性質を帯びて来たが、完全・無矛盾ではない
- 属性情報の信頼性
  - 海外姓名表記への対応、改姓対応、などで一貫したポリシーが敷けていない
  - 「その他」アカウントの属性情報は自己申告でセンターで正確性を検証できていない

統合認証DBを人に関する全学DBとして用いる場合の問題

- 教務情報と人事情報に由来する非整合性の問題
  - 利用目的が異なるため、部局の単位やコードなどが一致しない
  - TAやRAなどで学生・教職員の身分の二重化が発生するが
    完全な解決はされない（全学アカウント自体は学生側に片寄せ）
    - 必要に応じてSP側で運用による解決
  - 短時間雇用教職員は財源単位の雇用となり、複数財源雇用者は
    人事給与システム上は複数エントリが存在する

→センターが属性入力する「その他」アカウントと合わせ、
名寄・紐づけを行わないと「人」ベースの情報とならない

多要素認証の導入時の課題

- パスワードのみの単要素認証を行う場合に比べ、
  利用者の習熟が必要なケースが多い
- 教育的な情報提供から問題発生時のリカバリまでが
  必要になるが、利用者・センターともに高負担
  - 教職員側のコアサービスでの多要素必須化は完了、学生・その他アカウントのスケジューリング中
- オンライン授業等で緊急対応が必要！等の危急の要請は
  個別SPや所属部局の都合によって生じるが、
  どこまでサポートするか？の程度について全学的に合意があるとは言えない
  →しかし、この程度は確実に体制的コストに直結
- 宣伝：明日「午前２」のユーザーコミュニケーション部会
  企画セッション【多要素認証を「使ってもらう」ためのユーザーコミュニケーションとは】でも関連の議論を行います！

今後の展望

- 諸課題は情報環境機構／情報環境支援センターが
  単体では解決できないフェイズに入っている→**全学的な対応が必要**
- 今月、**情報担当理事直下に「認証次世代化・ID体系化タスクフォース」発足**
  - 部局長級教員および事務本部の人事・教務・情報の部長級職員を委員に
  - 部局との対話の場を設定
  - 事務本部のDXプロジェクトと併走し、相互協力することを明記
- 大学全体として以下の目標を検討することに
  - 本人確認方法の基準の提示
  - ID情報の体系化（当面は ≠ 一元化 ）を推進
  - 上記を活用したID情報や高度認証の積極的活用