東京大学の
共通IDとID管理の実態

東京大学 情報システム本部
中村 誠

AXIES認証基盤部会 勉強会, 2024-09-17

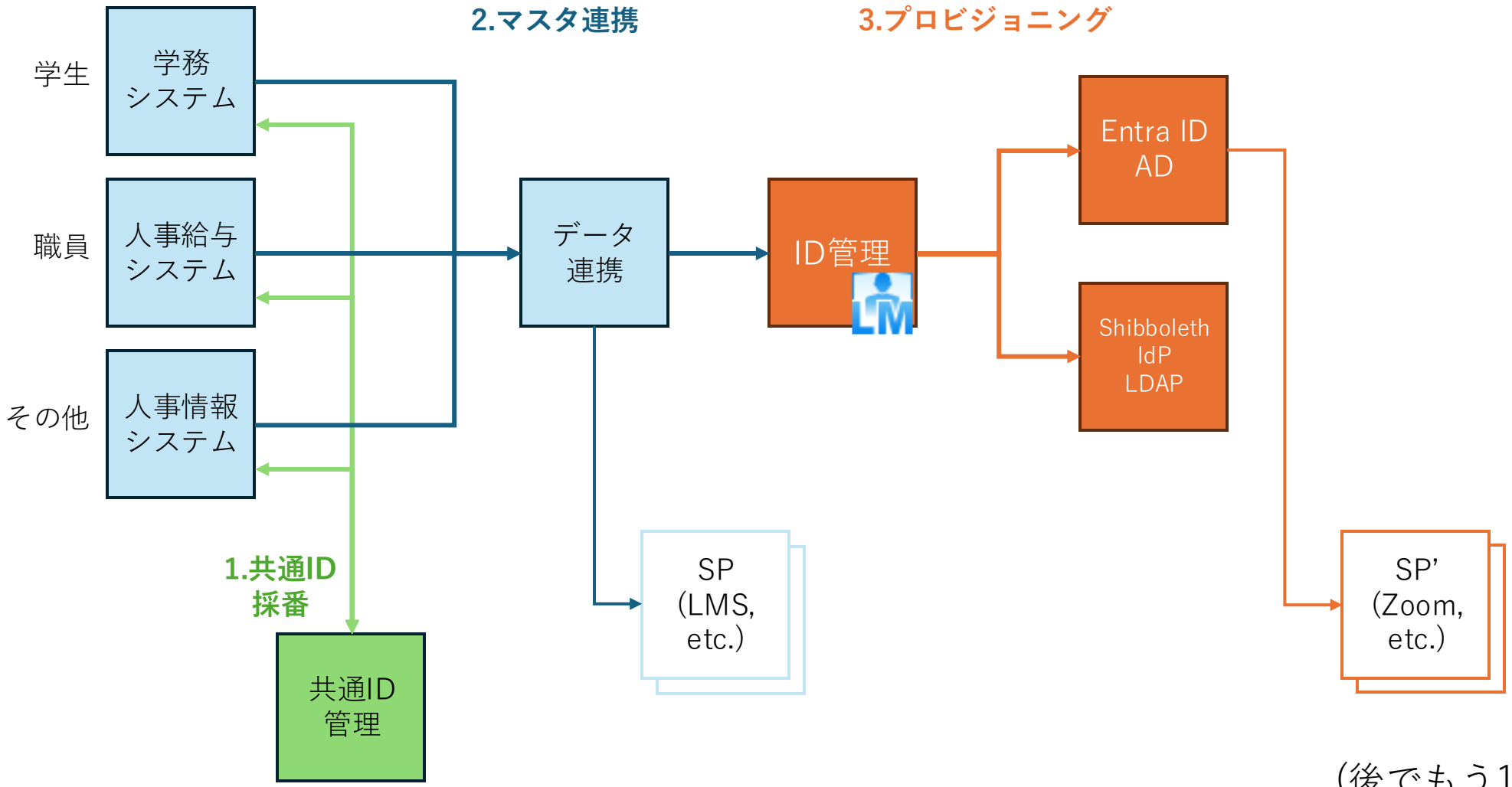
あらすじ

- “ID”?
- “共通ID”
  - 一元化
- ID管理
  - UTokyo Account
- 皆さんと考えたいこと
  - 名寄せ問題
  - アカウントの対象とライフサイクル問題
  - ちょっとした“離籍”問題

“ID”?

- Identity, Identification, Identifier?
- Identifier 識別子
  → “共通ID”
- Identity アカウント
  → “UTokyo Account”

ID管理:共通IDとUTokyo Account



(後でもう1回出てきます

共通IDとは

- 2005年からICカード身分証とともに運用を開始
  - 従来は学生は学生証番号、職員は個人番号 (not マイナンバー)
- 立場や身分によらず“一人一ID”
  - 実際には学生と職員で異なるID
  - 学生でもある職員(後述)には学生証と職員証を発行

- ICカードのID番号として書き込み
- システムレコードのID項目として登録
- 2010年頃からアカウントのID、ユーザ名としても使用

共通IDは

- 10桁の数字な文字列（正式?には18桁、ただし上8桁は“0”）
  - “0123456789”, “3141592653”, …

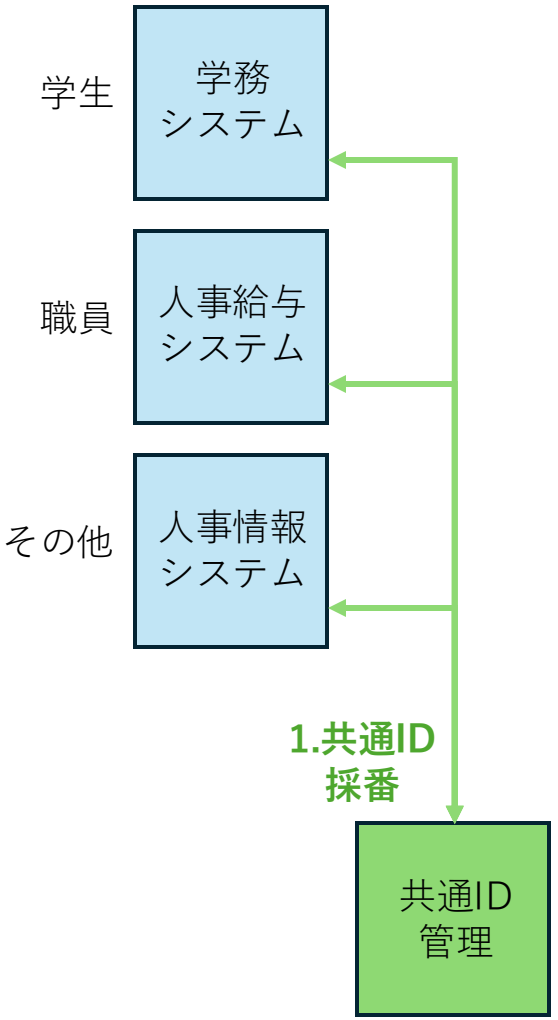
- とある素数冪な数列をもとに生成
  - $a_k = p^k \pmod q$

- “0”で始まる数字も使っています…
  - CSV取り込みで0落ちします！

共通IDを“採番”

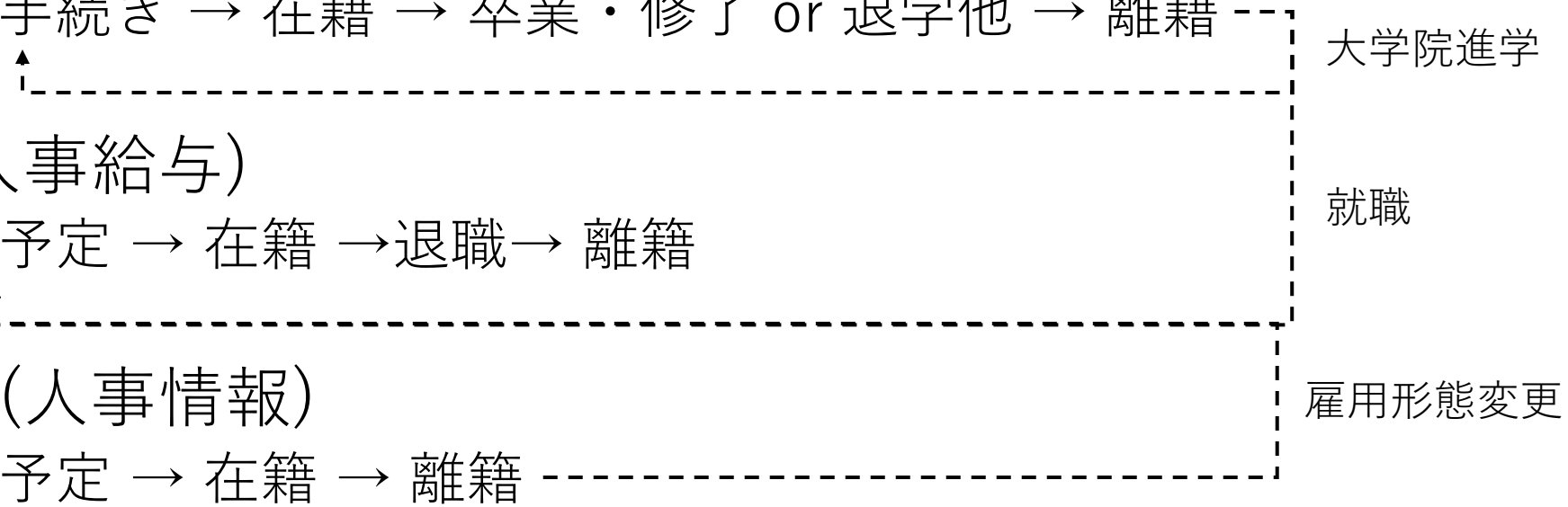
- 学務/人事で管理対象者を登録したら
  共通ID管理に採番依頼し結果を取り込み
  - 学生は手動、職員その他は自動・日次で

- いつ採番を依頼？
  - 学生：入学手続き(学務)
    - 学部、大学院-修士、大学院-博士、研究生他
  - 職員：採用手続き(人事給与)
    - 教職員、有期/短時間職員、非常勤講師、TA/RA、など
  - その他：構成員登録手続き(人事情報(後述))
    - 派遣職員、名誉教授、客員教員、研究生、などなど



繰り返し採番するの？
ライフサイクルを見てみる

- 学生(学務)
  - 入学手続き → 在籍 → 卒業・修了 or 退学他 → 離籍
- 職員(人事給与)
  - 採用予定 → 在籍 →退職→ 離籍
- その他(人事情報)
  - 在籍予定 → 在籍 → 離籍



同一人物とは？名寄せ問題

- 氏名と生年月日
  - 「東大太郎」「1877年4月12日」
  - 比較：マイナンバーカード基本4情報は氏名、生年月日、住所、性別＋「東京都文京区本郷7-3-1」「男/女」

- 氏名
  - 氏名、カナ氏名、英字氏名
  - 異体字、“難しい”漢字、“□”、母国語表記
  - 日本語な読みカナ、母国語な読みカナ
- 生年月日
  - 表記方法が国・地域により異なる。もし“4/1/12”と入力されたら
- 住所
  - そもそも聞いていないが、扱い切れない？

共通IDにまつわる課題

- 異なる「氏名と生年月日」の同一人物問題
  - データが誤登録されていることも
- 同一「氏名と生年月日」の別人問題

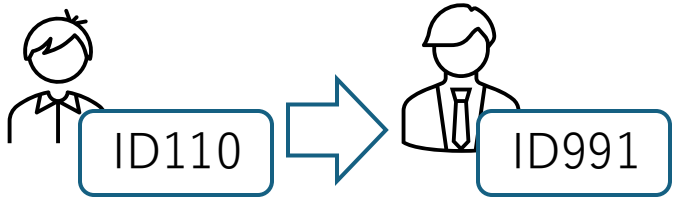
(条件)
- 入学採用手続き時のバーストな処理負荷時に実施な方法

(現状)
- 完全一致するデータが1件→確定、2件以上→確認
- 部分一致するデータのみ→確認

共通IDを一元化 Why?

a. 学生が職員に
   - 学生が卒業修了し教員/研究員、職員として就職

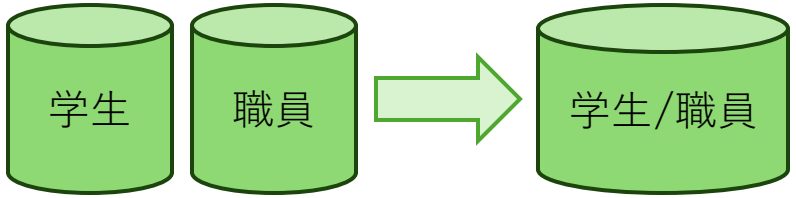
b. 学生かつ職員に
   - 学生が大学職員として勤務
   - 大学院学生が病院に医師として勤務
   - 職員が社会人学生として入学



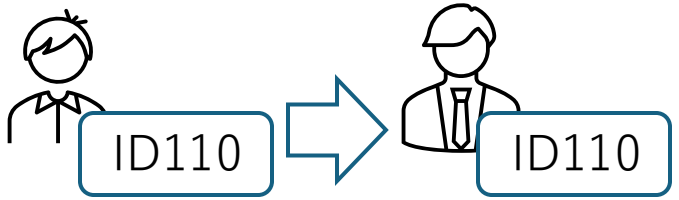
- 学生と職員でIDが違うと“不便”
  a. 学生から職員になると昨日まであったファイルが見えなくなる
  b. 1)どちらのIDでサインインしたブラウザを使うかで、できることが違う、できないことがある
     2)情報セキュリティ教育、多要素認証で二度手間をかける
     3)オンキャンパスジョブの事務手続きで大量に煩雑な作業が発生

共通IDを一元化

- **立場や身分によらず“一人一ID”** → “一元化”
  - 「氏名と生年月日」で名寄せ



- 学生かつ職員は学生のIDに統合
  - 職員のIDを廃止し、学生のIDを職員としても使用



- 人事データを修正
  - 関連システムも修正
- データの移行/コピー、権限の修正
  - 共有の再設定、グループメンバの更新なども
    - ウェブページで案内 https://utelecon.adm.u-tokyo.ac.jp/notice/2024/utokyo-account-consolidation

※共通ID誤採番と同じ対応

共通IDが一元化されると(システム視点)

- 複数の身分（学生と職員）で1つのID
- 学生なら使える機能、職員なら使える機能が混在
  - LMSで授業を学生として履修、TAとして管理のような複雑なケースも

（対応策）

1. サインイン時に選択
2. “学生かつ職員”グループの権限を設定
3. 身分属性を複数値で連携 → サービス側に委ねる
   - eduPersonAffiliation {‘student’, ’staff’}
   - 例えば職員のみ eduroamビジター用アカウント発行可能

if ‘student’ in ePA then **deny** #想定外
elseif ‘staff’ in ePA then allow

UTokyo Accountとは

- 東京大学の情報システムを利用する際に必要となる全学的なアカウント
  - 東京大学の構成員（学生および教職員）が各種情報システムを利用する際はこのアカウントでサインイン

- ユーザ名は10桁の数字“共通ID”
  - レルム付きの *0123456789*@utac.u-tokyo.ac.jp のことも
  - なおePPNは *0123456789*@u-tokyo.ac.jp （スコープ）

ID管理:構成員とは？

- 「(共通ID)いつ採番を依頼？」を振り返ると
  - 学生：入学手続き(学務)
  - 職員：採用手続き(人事給与)
  - **その他：構成員登録手続き(人事情報)**
    - **派遣職員、名誉教授、客員教員、研究生、などなど**
- 規則によると

(1)　役員とは、東京大学基本組織規則(平成１６年４月１日東大規則第１号。以下「基本組織規則」という。)第２章第１節に掲げる役員をいう。

(2)　教職員等とは、基本組織規則第２章第２節に掲げる教職員及び派遣職員をいう。

(3)　学生とは、本学の規則に基づき、入学、聴講又は履修を許可された者をいう。

(4)　本学の構成員とは、役員、教職員等及び学生をいう。

(5)　本学の構成員に準ずる者とは、本学の構成員以外の者であって、本学の経営及び教育研究活動に参画又は従事するものをいう。

(6)　本学の構成員等とは、本学の構成員及び本学の構成員に準ずる者をいう。

“人事情報システム”とは

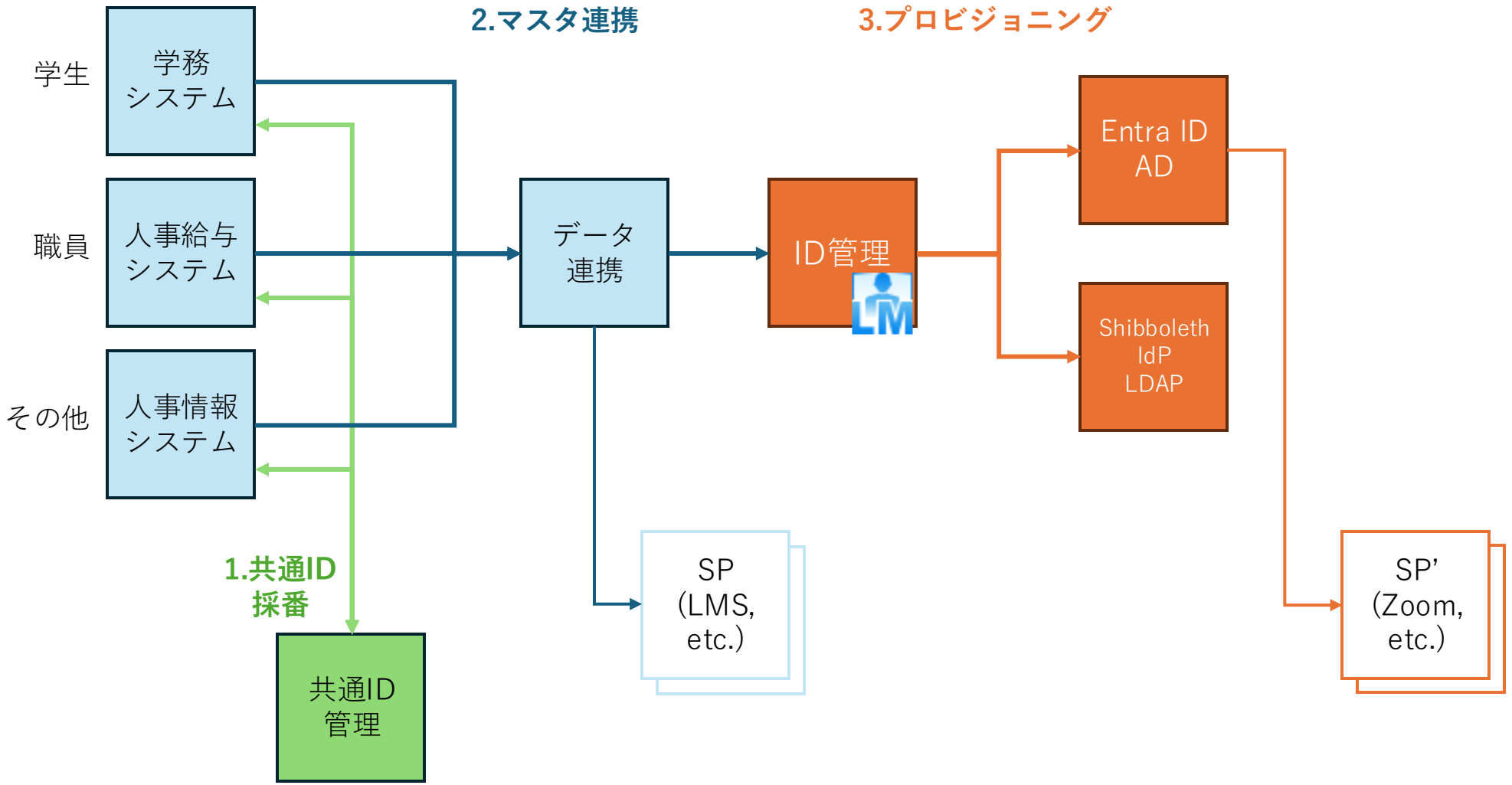
「東京大学として、学内の危機管理及び安全衛生管理を行うと共に、法人としての経営判断を行うために、**本学に定常的に在籍する者の情報を収集する**こととした。併せてこの情報資源の有効活用を図り、各システムとデータ連携を行うことにより、**業務の効率化を推進する**ことを目的に、人事情報システムを導入する。
　本システムでは、本学に定常的に在籍する人の情報をデータベース化し、各業務システムのログインIDとして使用する共通IDの発行機能、職員名簿機能および他の業務システムとのデータ連携機能を実装する。データ登録については、**基礎情報は対象者が所属する本部及び部局担当者が実施**し、予備情報は必要に応じて本人もしくは担当者が登録する。」

- 職名「派遣職員、業務協力者、名誉教授、客員教員、客員研究員、研究生、受託研究員、東京大学特別研究員、その他研究員、その他職員、ゲスト」

- 現在は？ ※発表者個人の見解です

「**UTokyo Accountでサインインする情報システム(*)を使用して業務を行う者**（ただし学生および職員を除く）を登録・管理し、業務の効率化を推進することを目的に、人事情報システムを運用する。」(*)コミュニケーション・コラボレーションツールMicrosoft 365, Google workspace, Zoom, Slackや、情報インフラWi-Fiや、教育系システムUTAS, UTOL, ECCSや、業務系システム 財務会計、人事、研究支援など多岐にわたる

ID管理：共通IDとUTokyo Account

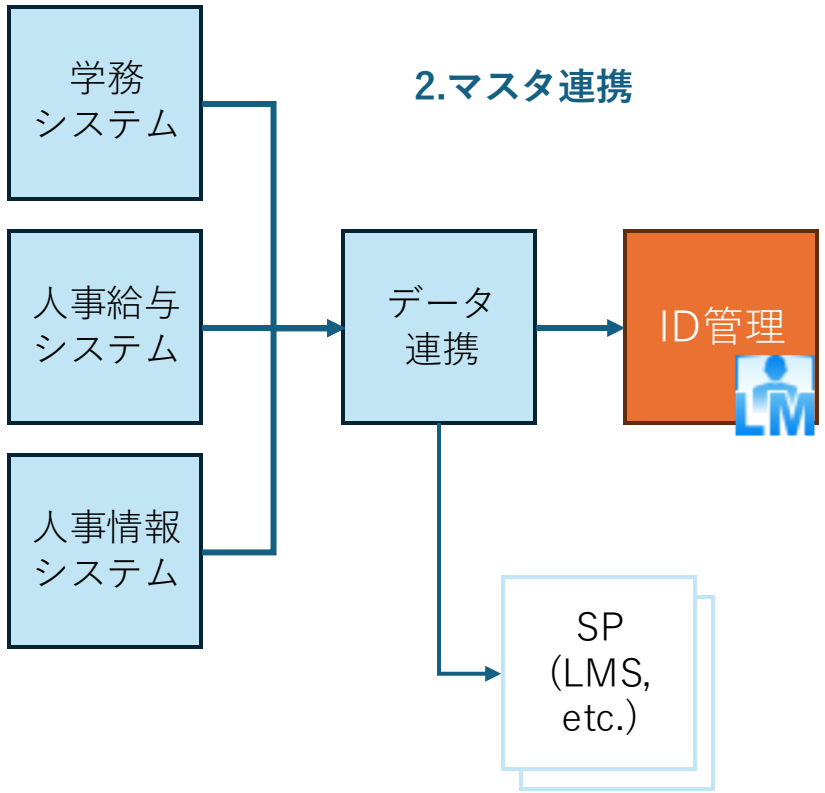


ID管理: マスタ連携

- ID情報の源泉となる学務/人事から
  マスタデータを日次で取り込み
  - 在籍者と在籍予定者のデータを
  - データ連携システム経由で

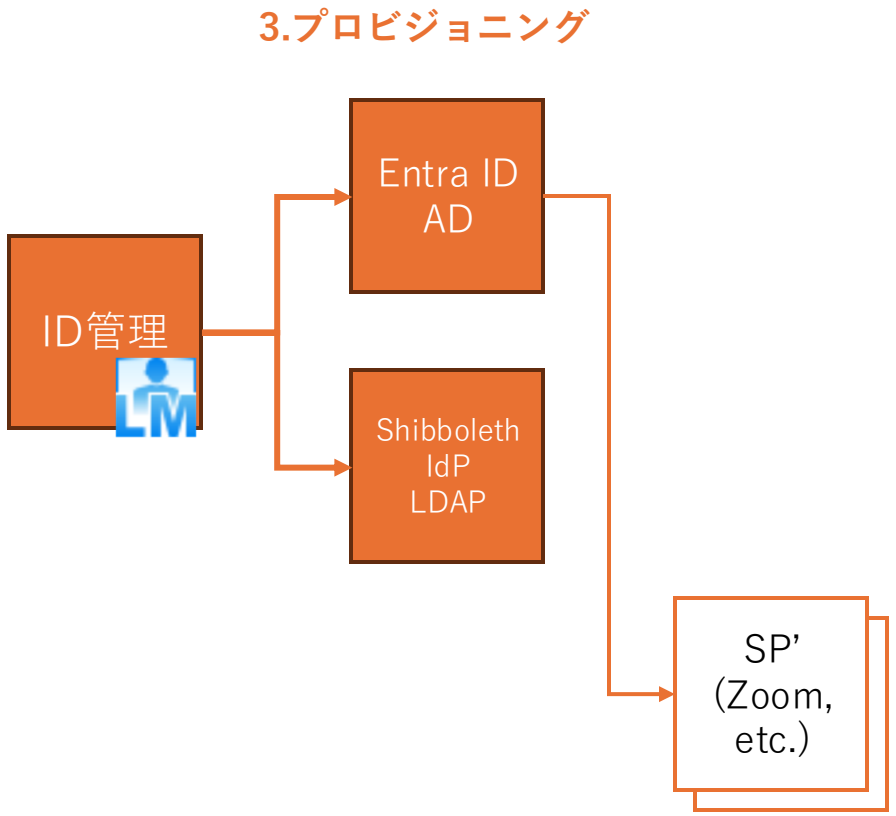
- データ連携システムとは
  - システム間の橋渡し役
  - WebDAVでファイル共有
    - CSV, XML, etc.
  - 学務、人事、財務、LMSなど

  ※ID管理システムは認証システムに注力



ID管理: プロビジョニング

- 源泉から取り込んだID情報を IdPにプロビジョニング
  - Entra ID/AD
  - Shibboleth IdP/LDAP
- Zoom, Slackなど一部のSPはIdPとの認証連携時に動的にJITプロビジョニング
- IdP認証サービスは SAML, OpenID ConnectでSPと連携



オンボーディングと認証方法

- 在籍予定の段階で通知書を印刷
- クラス発表/入学ガイダンス/着任時に通知書を配付
  - 学部学生は準備のため学生証配布/授業開始前に

- ユーザは認証方法を設定
  - パスワードを設定
  - スマホアプリ、電話、TOTPなどを設定
  - 多要素認証を有効化

※引き続き情報セキュリティ教育を受講

オフボーディングと失効/削除

- 離籍後にアカウントを失効（論理削除）
  - 離籍＝源泉データに含まれなくなる
  - 失効＝無効化（パスワード初期化＋フラグ変更）
    - 多要素認証の認証方法はそのまま
- 失効後一定期間後にデータを削除（物理削除）

アカウントリカバリー

- パスワード忘れ
  - 事前に登録したメールアドレスを利用したセルフサービス型での再設定が可能
  - 従来職員は大学アドレスに限定していたが、現在は任意
- 多要素認証の本人確認方法再登録
  - 専用申請サイトでパスワード認証＋ICカード身分証の写真アップロードによる本人確認

  ※あらかじめ2個以上の本人確認方法の登録を案内

- あるいは所属の学部・研究科等の窓口で対応

属性

- プロビジョンしている属性は？
  - Entra ID: ユーザ名、氏名、所属、メールアドレス
    - 所属は職員のみ、職員向けメールサービス アドレス帳用
    - メールアドレスはアカウントリカバリー用
  - Shibboleth IdP: ユーザ名、eduPersonAffiliation、メールアドレス
  - ユーザ識別、認証機能に必要な最小限の属性のみ

- 属性の扱いに関しては悩ましいことが多い
  - ディレクトリ機能でのユーザ検索やリスト表示の制御
  - プロフィールのユーザによる設定の制御
  - 所属など属性に基づくアクセス制御、グループ管理

ID管理にまつわる課題

- アカウントの対象とライフサイクル問題
  - 誰までアカウントを発行すればよいのか
  - {いつから,いつまで}アカウントが使えるのがよいのか
  - 事前準備の期間をどう扱えばよいか

- ちょっとした“離籍”問題
  - 厳密には制度上卒業式当日に離籍、翌年度に進学先で“再”在籍
  - 在籍者の登録作業漏れで一時的に“離籍”状態になることも
  - アカウントの無効化、削除は即時反映してよいのか
  - 認証方法の初期化は即時反映してよいのか

ユーザ名にまつわる課題

- ユーザ名勝手にメールアドレス扱い問題
  - アカウントのレルム付きユーザ名はメールアドレスではない
    - たしかに @utac.u-tokyo.ac.jp って形式だけどさぁ
  - しかしながらシステムからの通知メールが配信される場合があり仕方ないので転送されるようにした…
  - Mail属性は何のためなんでしょう？
- ユーザ名が扱いにくい、長い問題？
  - 共有相手、グループメンバを“共通ID”で指定するのは難しい？
  - レルムは省略したいこともある？
  - Hintパラメータを指定させてもらえたら…
    - ロゴのカスタマイズとかブランド設定が可能なら

皆さんと考えたいこと

参考)
2023年 年次大会
https://auth.axies.jp/sig/68/
2022年 年次大会
https://auth.axies.jp/sig/50/

- 名寄せ問題
  - 何を根拠に同一人物と判断すればよいのか
    - マイナンバー的な情報に依拠できないか
- アカウントの対象とライフサイクル問題
  - 誰に、{いつから,いつまで}、事前準備の期間
    - 参考) 学生証は事前作成、職員証は着任後に申請＆作成
      メールアドレスは在籍後に各自で設定
- ちょっとした“離籍”問題
  - アカウント無効化/削除、認証方法初期化は即時反映してよいのか