シングルサインオン実証実験
経過報告～広島大学～

総務室情報化推進グループ
情報メディア教育研究センター

広島大学

シングルサインオン実証実験

広島大学

- 本学の目的
  - 広島大学の全学認証基盤を利用し，電子ジャーナルやその他の学術リソースを共有できるかどうか実証する
  - IdPサーバの構築 (認証連携サーバ)
  - 広島大学認証サーバとの連携
  - SP (学外サーバ) へのアクセス

IdPサーバ構築

広島大学

- 広島大学IdP
  - idp.hiroshima-u.ac.jp
  - IdP_Manual_1.2.pdf にしたがって導入
    - VMwareイメージを利用
      - ホストOS：CentOS5.3　VMware-server-1.0.7-108231.i386.rpm
      - ゲストOS：VMware　upkishibIdPv1.0.tar.gz
  - Username/Passwordによる利用者認証設定
    - https://spaces.internet2.edu/display/SHIB2/IdPAuthUserPass
  - 既設の全学電子認証システムと連携
  - NIIサーバへアクセスを確認

IdPサーバ構築時の問題など

広島大学

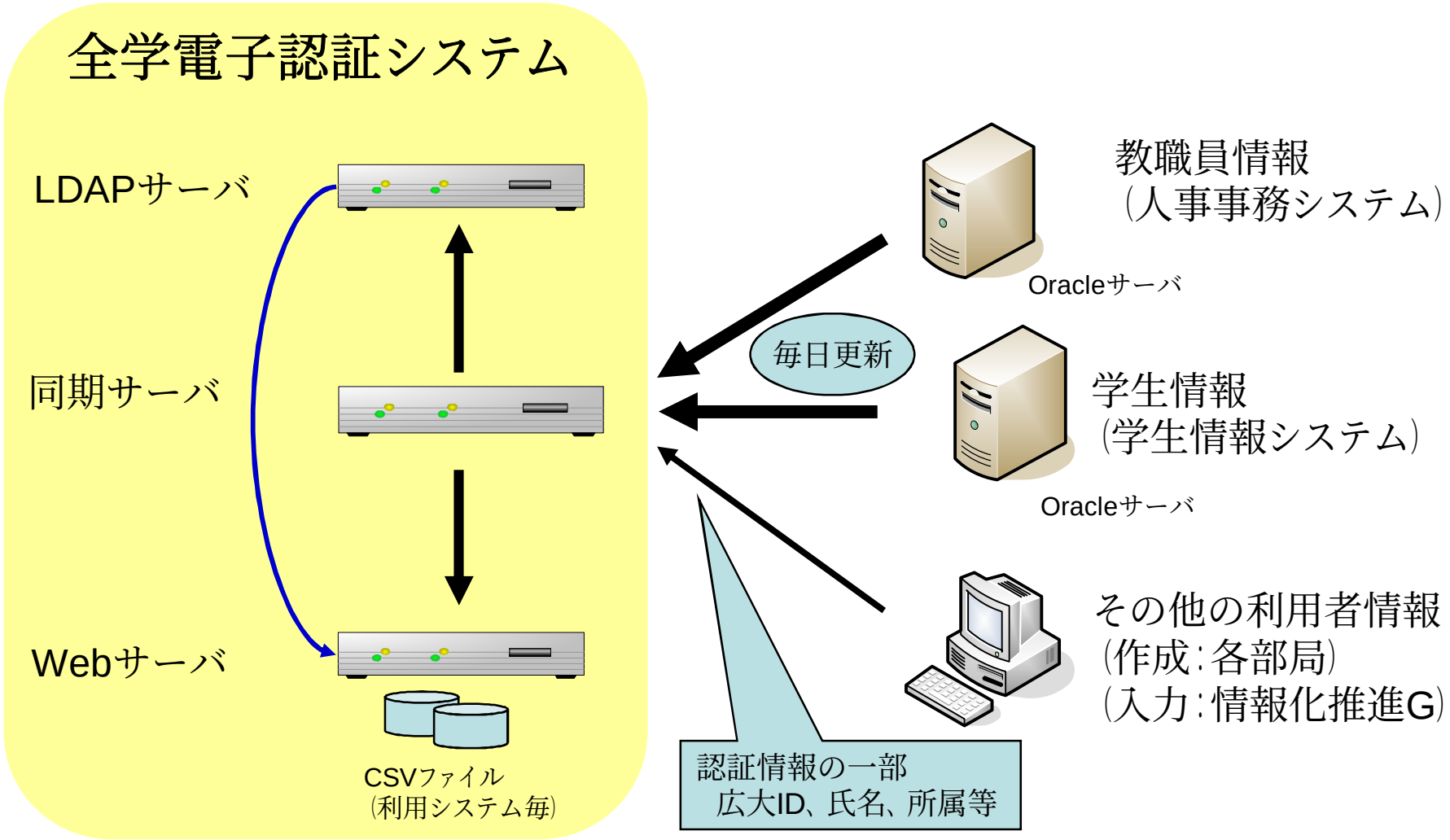
- 設定上の問題
  - eduPersonPrincipalName
    - 大学固有のIDを晒したくない
      - 公開用メールアドレスであっても慎重であるべき
    - IDをハッシュした値を利用（script attribute definition）
      - UPKI-Fed 実証実験通信 Vol.14 で紹介
      - しかし、“71b5762ba6e3f7a03fdc651b6e1c0f5b@hiroshima-u.ac.jp さん、いらっしゃい”と表示されるのは気持ち悪い
  - eduPersonAffiliation
    - 大学の認証システム上では、身分と職種の組み合わせで表現されている
      - “faculty”（教員）に相当する人は複雑な組み合わせ条件
    - 複数属性からマッピングを利用（maped attribute definition）
- 設定の確からしさの確認
  - SPに何が渡されているか？を簡単に調べる手段が必要

広大全学電子認証システム経緯

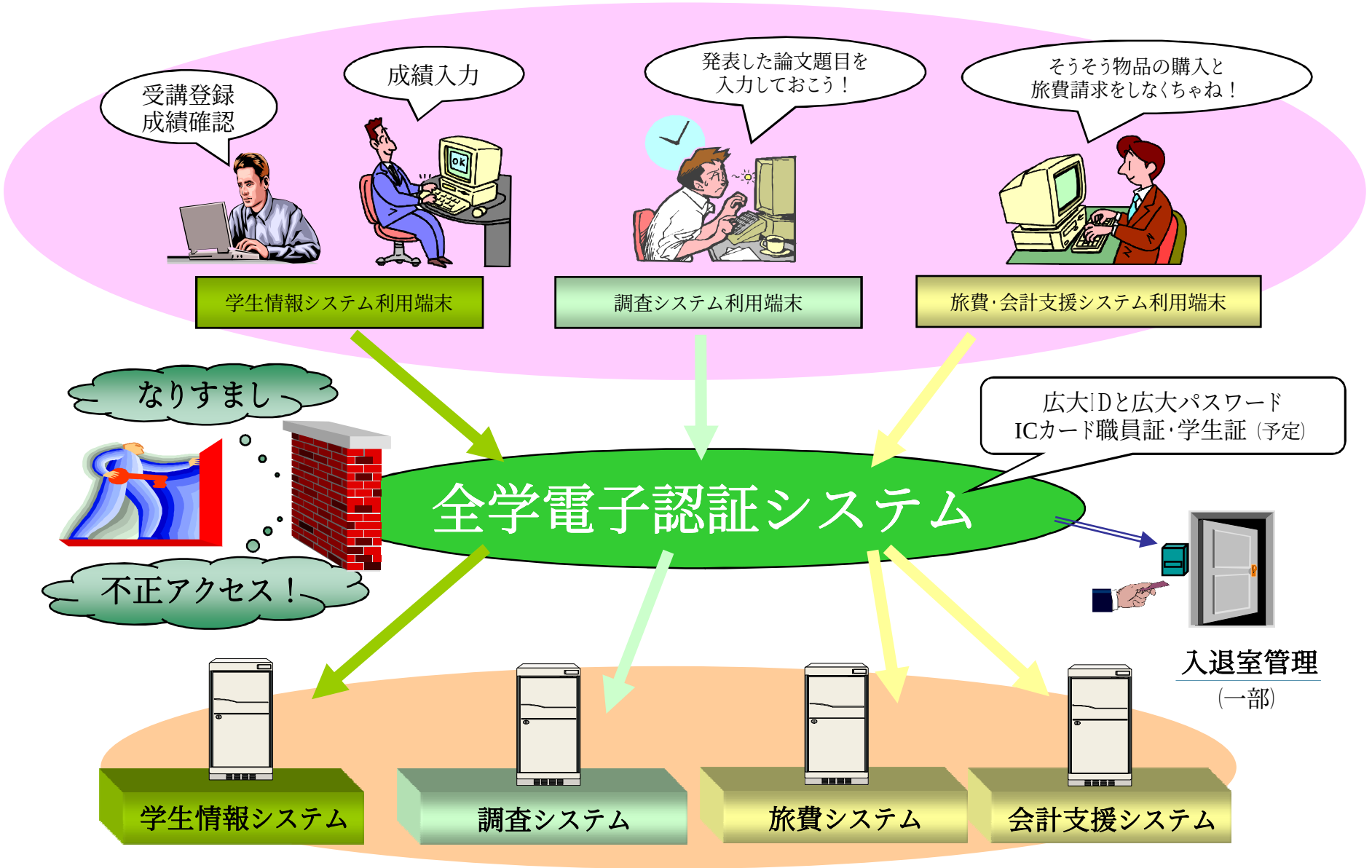
広島大学

- 導入の経緯
  - 情報通信･メディア委員会（全学委員会）
    - 平成10年頃
      - 磁気カード型学生証･職員証の見直しと認証システムの検討
    - 平成12年度
      - 全構成員に対する電子認証システムの導入およびICカード導入の検討
    - 平成13年度
      - 全学電子認証システムのみ導入決定
  - 全学電子認証システム（第1期：平成14年度～）
    - 全学統合個人認証（教職員＋学生＋その他）、パスワード認証
  - 全学電子認証システム（第2期：平成19年度～）
    - 第1期とほぼ同様の機能
- 利用状況
  - リアルタイム連携（LDAP）
    - 学生情報、電子事務局（会計支援、旅費）、学内無線LANアクセス、キャンパスネットワーク（HINET2007）
  - 非リアルタイム連携（CSV）
    - 図書館、保健管理センター、入退室管理

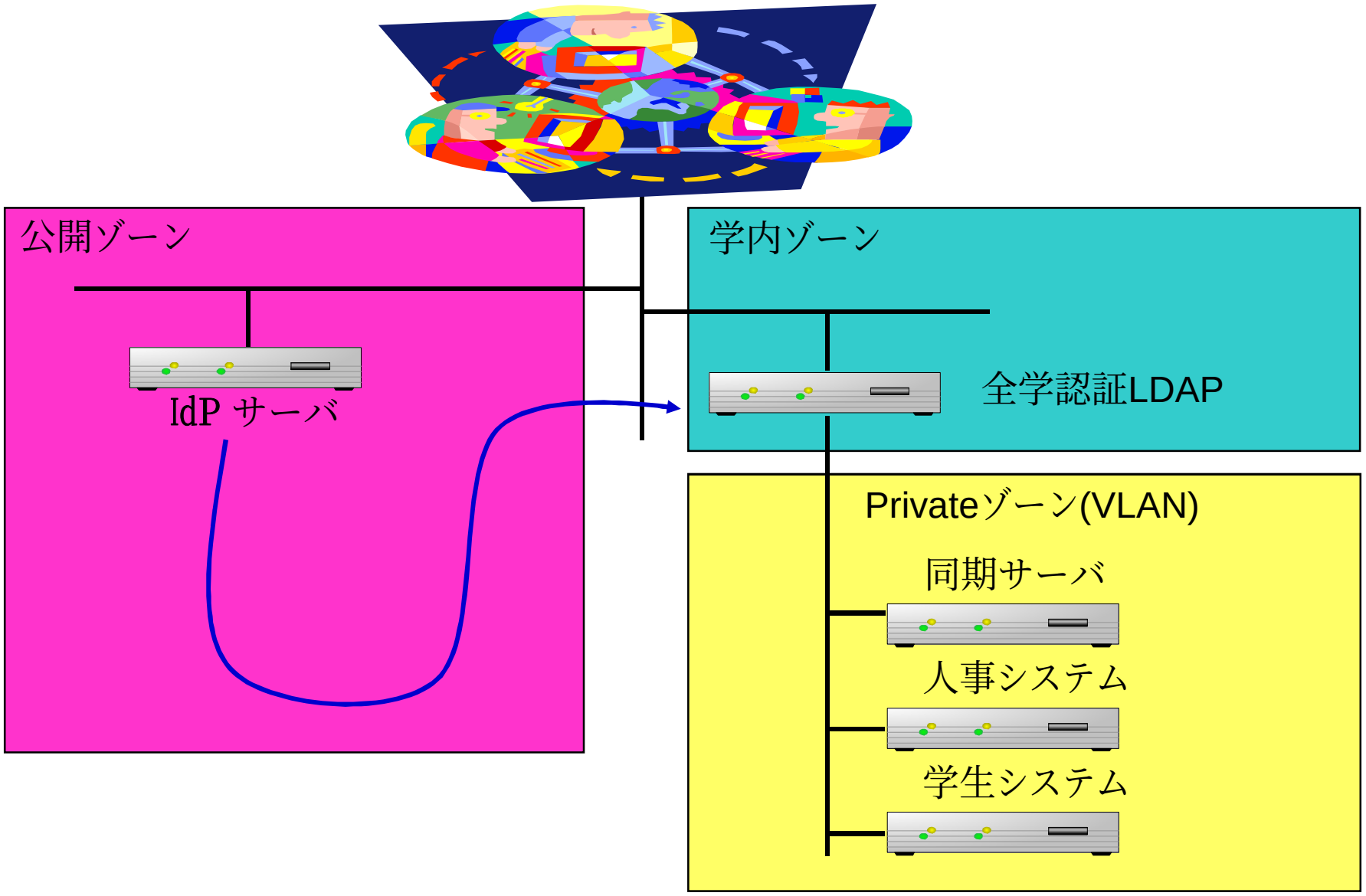
広大認証基本情報の統合処理



全学電子認証システム　利用イメージ



IdP構築状況(ネットワーク接続図)



課題と今後の予定

広島大学

- 課題
  - 属性情報の対応関係
  - 学内アナウンスや利用規定の制定
  - 利用者の限定方法（学生・教職員）
  - 学内SPの立ち上げ
- 予定
  - 学内アナウンス
  - 全学電子認証システム
    - LDAPによるリアルタイム連携
    - 属性情報の整理・追加
  - 学外（NII，他大学サービスの利用（SP)
  - 図書館との連携（電子ジャーナルなど）

UPKI認証実験処理概要（学内説明用）

広島大学