# 大学における認証インフラの整備

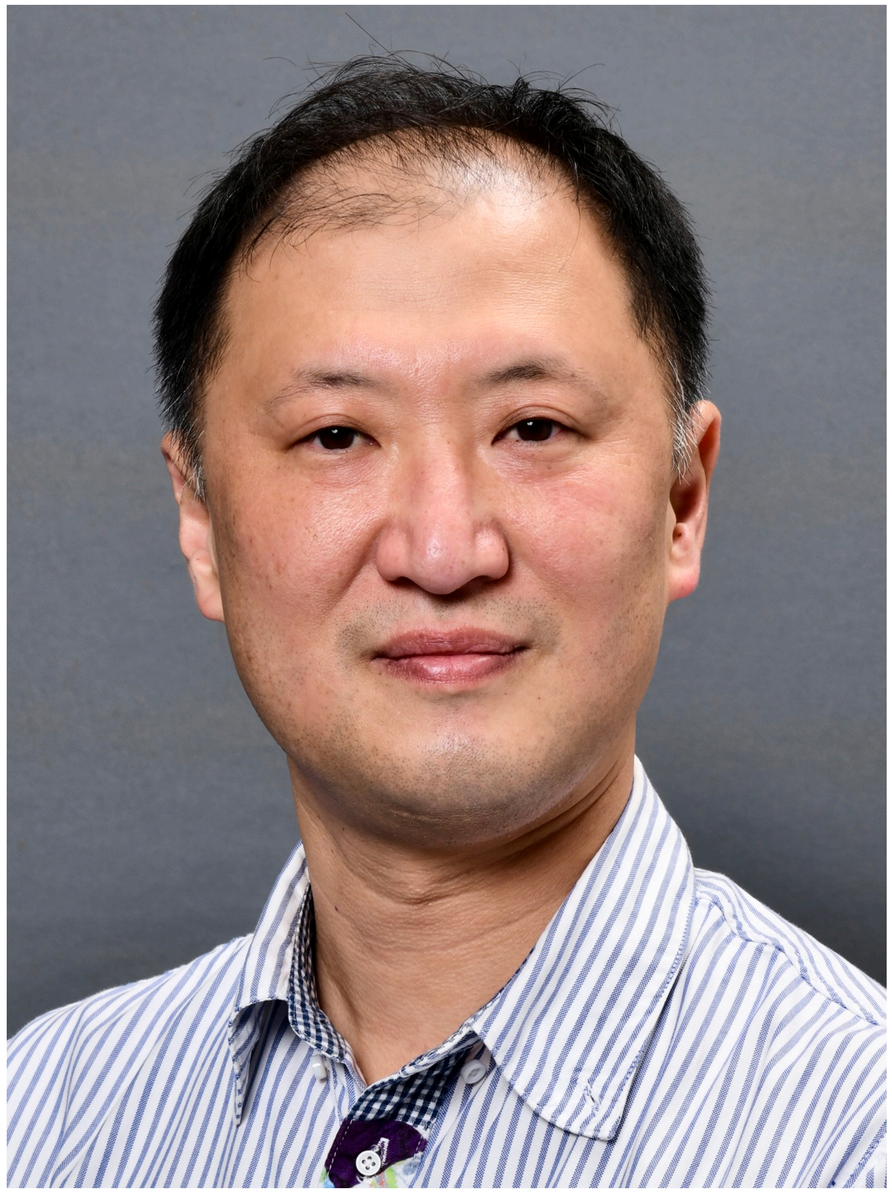
## ～JAISTでの二要素認証導入などを通して～

北陸先端科学技術大学院大学 (JAIST)
遠隔教育研究イノベーションセンター / 情報社会基盤研究センター
宇多 仁 (UDA Satoshi)

# 宇多 仁 (UDA Satoshi)

**北陸先端科学技術大学院大学 (JAIST)**
**遠隔教育研究イノベーションセンター / 情報社会基盤研究センター 准教授**

- 2004 年より JAIST にて全学情報インフラの企画導入運用に従事。
- 専門はインターネットアーキテクチャ、キャンパス情報基盤、データセンタ、サイバーセキュリティ。
- Interop Tokyo の ShowNet に NOC メンバーとして長年にわたり貢献。



# JAIST 情報環境の認証インフラの変遷

- 1990年代 (開学当初から)
  - NIS(YP) による集中的な利用者管理
- 2000 年代〜
  - NIS から LDAP への移行
  - Windows 環境への対応: LDAP <-> AD ユーザ/パスワード同期
- 2010 年代後半〜
  - Web SSO 向け SAML IdP / Shibboleth IdP の導入
  - 二要素認証の導入

# LDAP (NIS) による利用者管理時代

- 全学の利用者ならびに認証情報を集中管理
- 各システムは LDAP を参照して認証・認可
  - 全学のどのサービスも同じ ID / Password で利用できる
  - 当初は UNIX 系システムが中心であったが、Web ベースのサービスからも参照し、また AD との同期により Windows へも対応。

➡ 非常にうまく機能していた

  - あまりにうまく機能していたが為に(?) Web SSO 導入が遅れた

# 統合認証基盤の導入整備 (2017〜)

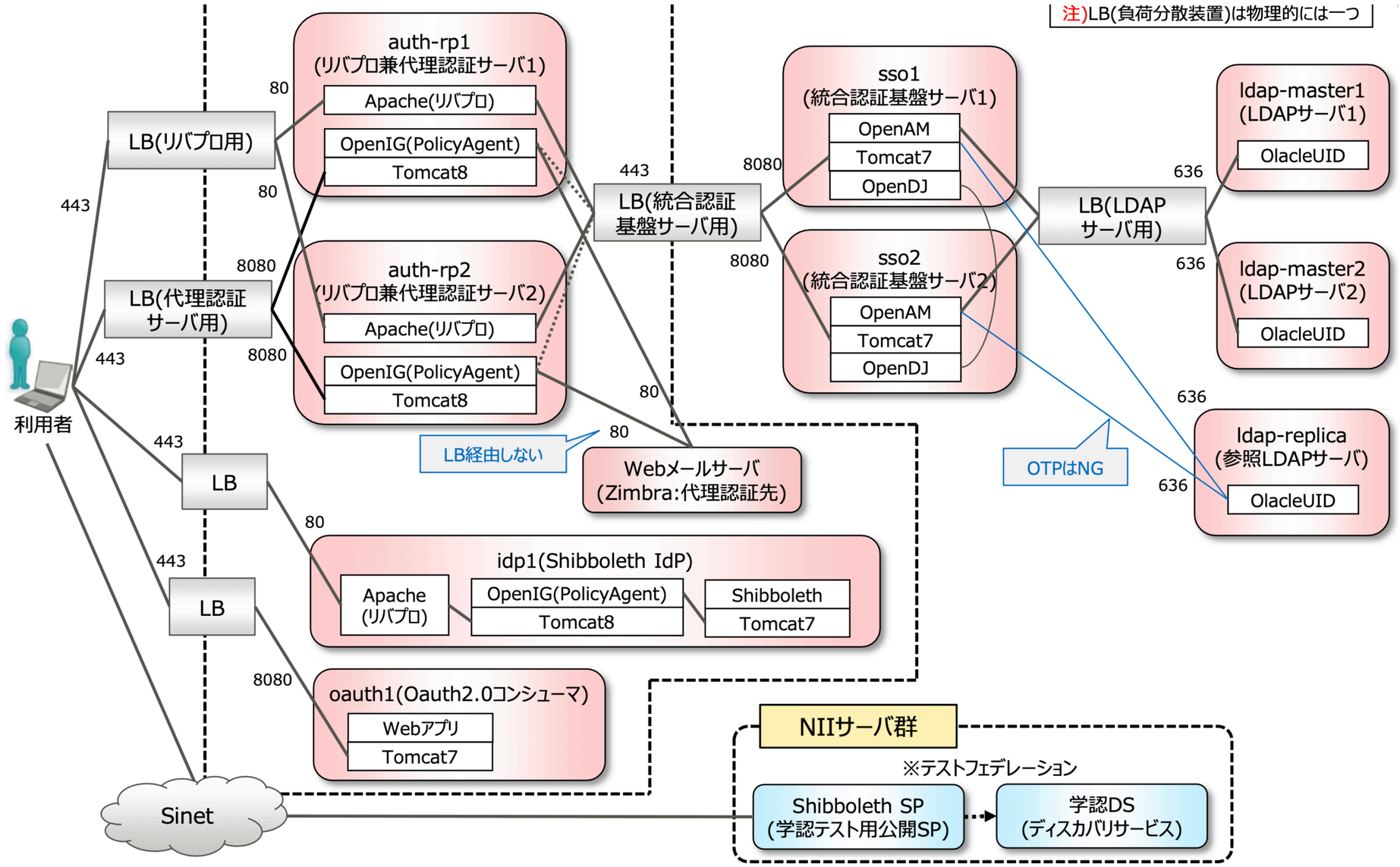
- 背景
  - Web ベースのサービスの増加
  - 認証ポリシ/システムの分散への懸念 (管理コストも含む)
    - システム毎での 2 要素認証など
  - Shibboleth をはじめとした外部認証連携への期待
- 課題
  - (当時) 必ずしも普及が進んでいない SAML / Shibboleth
    - 認証 (SAML) を優先するか、その他の核心的な機能を優先するか…
  - 数多の既存システムの認証をいかに認証基盤に集約していくか

# 統合認証基盤の導入整備 (2017〜)

- Fujitsu OpenAM + OpenIG + Shibboleth という構成を採用
  - 利用者情報の管理蓄積には引き続きLDAPサーバを利用
  - さまざまな認証プロトコルへの対応 (SAML, OAUTH, …)
  - 柔軟・多様な認証ポリシの適用が可能 (2要素認証, リスクベース認証, …)
  - 学認系サービスは Shibboleth IdP で連携
    - Shibboleth IdP の認証は OpenAM の SP として実装
  - 認証プロトコルにネイティブ対応していないサービスは OpenIG のリバースプロキシで認証しサービスへ接続
  - 既存サービス類は一気に全て対応することは現実的で無く、更改時に順次対応を進める

# OpenAM + OpenIG + Shibboleth (2017)

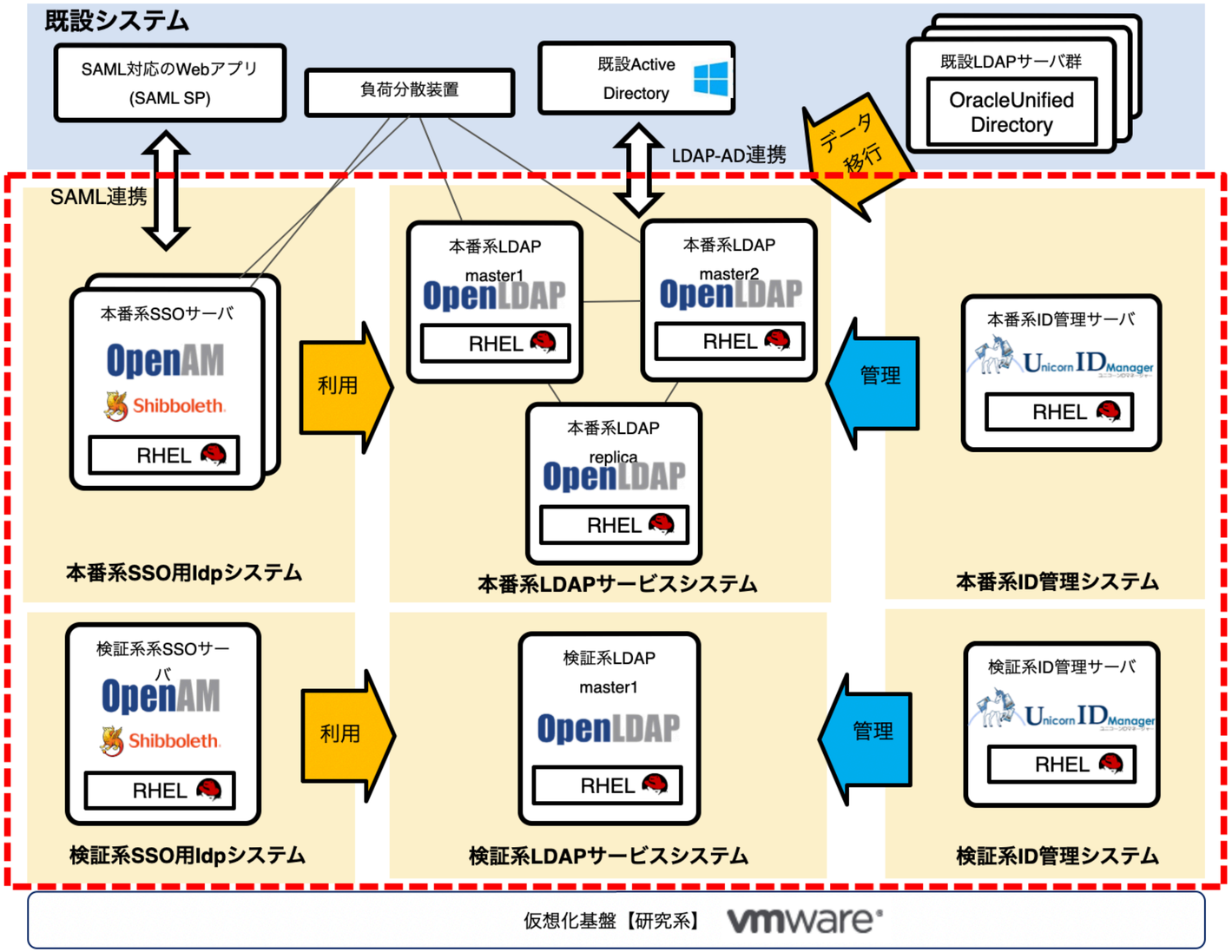
# OpenAM + OpenIG + Shibboleth (2017)



# 統合認証基盤の更改 (2021〜)

- さまざまな検討
  - クラウドサービス (IDaaS) なども含め
- 最終的に OSSTech OpenAM + OpenIG + Shibboleth という構成を採用
  - 主な更改点
    - OpenAM 側で認可処理が可能に
      - ユーザ属性に応じて SP の利用可否を集中管理できるようになった
    - 対応する認証手段の多様化
      - 2要素認証の拡張
    - LDAP サーバの変更
      - SunJava DS から OpenLDAP へ
    - 簡易的なID管理機能を付与
      - パスワード変更、リカバリ…
    - 構成の簡素化を図り運用管理を容易に

# OpenAM + OpenIG + Shibboleth (2021)



# 2要素認証への取り組み

- あまりに脆弱なパスワード認証
  - パスワードの強度や、他サービスとの使い回し
  - 学外からの攻撃の増加 → 特に学外からのパスワード(のみ)認証の撲滅を目指して
- 変遷
  - 特に高リスクなサービスでの電子証明書認証の活用 (2008〜)
  - SAML IdP / Shibboleth IdP 導入と 2 要素認証の活用拡大
    - TOTP (2017〜)
    - 電子証明書, Windows SSO, FIDO2 (2021〜)

# 電子証明書の活用

- 利用者へのクライアント証明書のオンデマンド発行
  - Verisign Managed PKI (2008〜2012)
  - Globalsign + Carasuite (2012〜2016)
  - UPKI + J-UPKI (2016〜)
- 当初は北風戦略
  - 特定のサービス(VPN, Wifi等)の利用には電子証明書での認証が必須
  - 利用者にとって難しい設定、こなれていない UI

  ➡ 不評!?
- 現在は太陽となって好評
  - 電子証明書で面倒な TOTP を回避できる

# 2要素認証の活用 (TOTP)

- 時刻ベースのワンタイムパスワード
- 利用方法
  - 利用者側の操作でオンデマンド発行が基本
  - 各自のスマートフォンや PC にセットアップ
- 特徴
  - 配布が容易 → 紙に QR コードを印刷して配布するということも可能
  - 特別なデバイスが不要

# 2要素認証の活用 (FIDO2)

- PC やスマートフォンでの生体認証など
- 利用方法
  - 登録用 Web ページに対象デバイスで接続し登録する。
- 利便性
  - ワンタッチで認証することができ普段の利便性が高い

# 2要素認証の活用 (Windows SSO)

- Windows ドメインログオン情報を用いた認証
  - JAIST では認証チェーンの先頭で処理している
- アプリケーション起動に外部クラウド等へのサインインが必要な際に有効
  - Web-based Mail Service
  - Webex
  - Adobe Creative Cloud
  - etc.

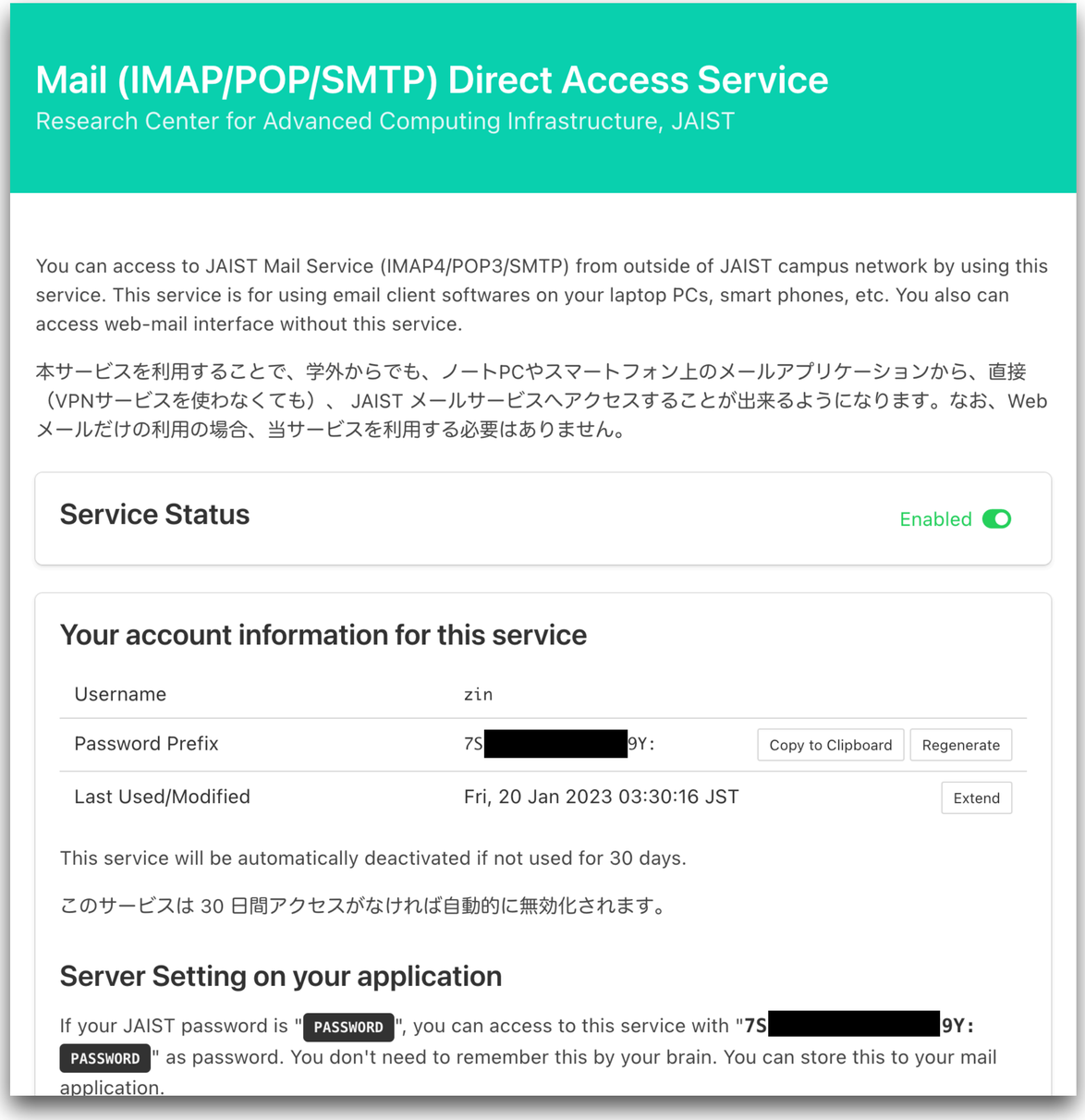
# Web 以外のプロトコルをどうするか…

- 電子メール (SMTP/IMAP/POP)
  - プロトコル的には SAML は無理だが OAUTH なら行けそう…

➡ 対応しているメールサーバが非常に限られ頓挫

  - でも通常のパスワード認証は撲滅したい

➡ 学外からのダイレクトアクセス用 Proxy + Password Prefix



# Web 以外のプロトコルをどうするか…

- 電子メール (SMTP/IMAP/POP)

# Web 以外のプロトコルをどうするか…

- Wifi 接続認証 (eduroamを含む)
  - radius サーバで認証
  - 電子証明書を用いた EAP-TLS 認証
    - パスワードは使わない
    - 例外) ゲスト利用者は専用の ID / Password を払い出して EAP-TTLS 認証
  - 懸念点
    - 学外利用時に、先方のネットワーク設定の不具合に起因して認証がうまく行かないことがある (パスワード認証に比べ認証時のパケット長が長くなる為)
    - 昨今は随分と改善している

# クラウドサービスと認証基盤 (SP)

- さまざまなサービス
  - 文献閲覧
  - Microsoft 365
  - Cisco Webex
  - Overleaf
  - Adobe Creative Cloud
  - etc.

➡ もはや大学の情報インフラにとっても無くてはならない

# クラウドサービスと認証基盤 (IDaaS)

- 認証基盤もクラウドサービスで運用できる時代
  - 比較的高機能なサービスが各種存在
    - 各種認証手段に対応、高度なセキュリティ機能、etc.
  - オンプレ運用に比べて低い管理運用コスト
- 検討ポイント
  - 提供ベンダーの信頼性
  - 耐障害性
    - 認証サービスの停止は全サービス利用不可に繋がる
  - オンプレ環境との連携
  - ベンダーロックイン

# 認証基盤の整備と集中管理

- 利点
  - セキュリティの確保・底上げ
    - 利用者情報の集中管理
      - アカウント棚卸し
    - 認証処理の集中提供
      - 脆弱性対応ポイントの集約
      - 認証機構の容易なアップグレード
  - クラウドサービス連携

# いかに認証基盤の利用を広げるか

- 鶏と卵!?
  - 認証基盤(IdP)が先か、使うシステム(SP)が先か…
  - まずは IdP 側が整わなければ何も始められない
- (国公立?)大学特有の課題
  - タテワリなシステム導入・運用
    - 強いリーダーシップをもって利用を広げる必要がある
  - 導入後のシステムを拡張することの難しさ
    - 現実的選択としては、各システムの更改にあわせて対応をすすめるなど
  - 進化の遅いクラシックなシステム類の多さ
    - SAML / Shibboleth ネイティブな認証に加え、認証プロキシなどさまざまなシステムに柔軟に対応出来る手段があると有効

# ゼロトラスト時代へ向けて

- クラウド利用により境界セキュリティが機能しなくなりつつある
- 出入りが激しく BYOD が横行する「大学」という組織では、そもそも境界セキュリティなんて機能していなかったのではないか!?

➡ セキュリティを高め、大学の資産を守りサービスを持続するためには、ゼロトラストの考え方にもとづいた設計・運用へ向かうことが必須

➡ 確固たる認証インフラの構築はその実現への重要な要素の一つ