東京大学における認証基盤の取り組み

東京大学 情報システム本部
中村 誠

NII Open Forum 2023, 2023-05-30

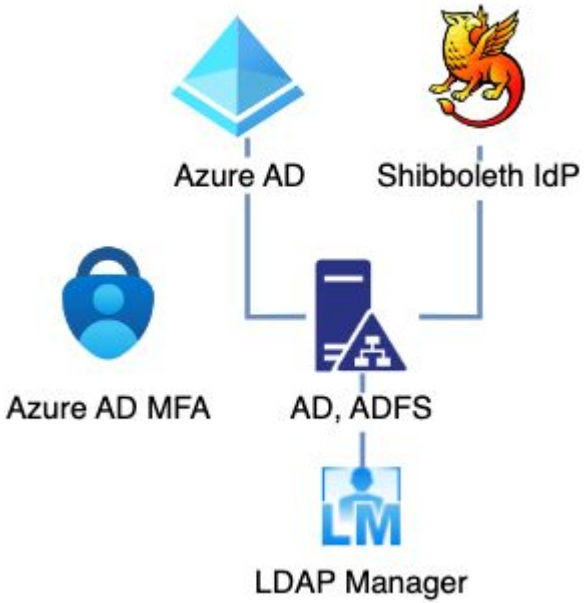
もくじ

- UTokyo Accountのしくみ
- 最近のできごと
- 最近のなやみ

UTokyo Accountのしくみ

- フェデレーションは Shibboleth IdP と Azure AD
- パスワード認証は ADFS、
  多要素認証(MFA)は Azure AD
- ID管理は LDAP Manager
  - ディレクトリは Active Directory (AD) と OpenLDAP

- 2015-2016年頃に構築
  - クラウドなど外部サービスとの連携
  - MFAへの対応



最近のできごと

1. MFAの普及促進
   - MFA有効なユーザのみ
     新しいサービスを利用可能に
     VPN, Slack

2. パスワードポリシーの調整
   - MFA有効なら”有効期限”を廃止
   - 文字数を**12-64**に（従来は8-16

3. セッション期間の調整（試行錯誤）
   - AAL2再認証規程への対応 - AAL2では12時間を要求
   - … Azure ADは14日（短縮、デフォルト「 90 日のローリング ウィンドウ」）
   - … Shibboleth IdPは1日（延長、デフォルト1時間）

最近のなやみ

- セッション期間短縮 → 再認証頻度上がる
  - SSOといってもブラウザとデスクトップアプリ（それぞれ複数）で独立して動作
  - 何度もサインインしろと言われるよね
    → 最近、Azure ADはデフォルトに戻した
- “MFA疲労攻撃”対策
  - スマホへのプッシュ通知を多数送り操作ミスを誘発するらしい
  - 2桁の数字 “99” を入力しなくちゃいけなくなった
- OS・IdP・IdMのバージョンアップ
  - サポート終了期限が迫ってきた
  - パスワードレス認証など新しい技術への対応
  - 次世代学認への対応
    - AAL2 & IAL2
- 多様なユーザへの対応
  - オフキャンパスなユーザ（海外や他機関所属
  - 連携サービスが増えるほどにユーザ数が増加

サインイン画面

Microsoft Authenticator の MFA 承認画面

https://jpazureid.github.io/blog/azure-active-directory/defend-your-users-from-mfa-fatigue-attacks/

おわり

補足

- NIST SP 800-63B ref

Requirement	AAL1	AAL2	AAL3
Reauthentication	30 days	12 hours or 30 minutes inactivity; MAY use one authentication factor	12 hours or 15 minutes inactivity; SHALL use both authentication factors

- 「REFEDS Multi-Factor Authentication Profile V2.0 - working draft」ref
  - https://refeds.org/profile/mfa
  - https://refeds.org/profile/mfa/recent ← 12時間
  - https://refeds.org/profile/mfa/immediate