

認証と連携の強化の取り組み

東京大学 情報システム本部

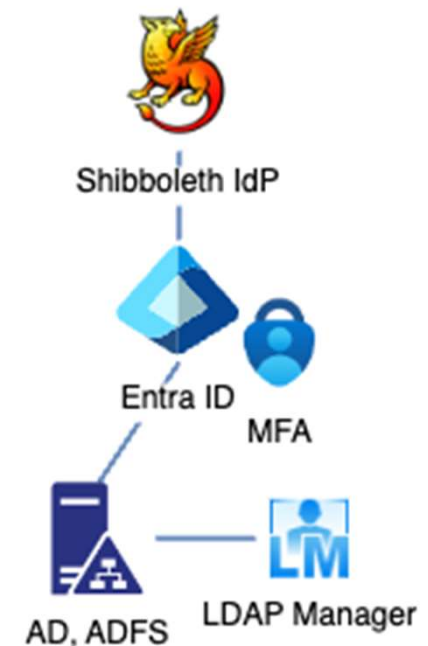
中村 誠

あらすじ

- 東京大学の認証基盤 最近のできごと
 - Shibboleth IdP V5にバージョンアップ
 - 多要素認証MFA 100%
 - 共通ID一元化
- 学認 短期取組検討サブWG・中規模実証実験
 - AAL2普及過渡期のIdP-SPの橋渡し
 - mdxを事例に

Shibboleth IdP V5にバージョンアップ

- **学認AAL2**に対応 (AuthnContextClassRef)
 - SAML Proxy構成
 - 認証コアはEntra ID
- **パスワードレス認証** (所持+生体/知識)
 - スマホアプリ、FIDOキー、パスキー*
Windows Hello for Business, macOS platform SSO*も



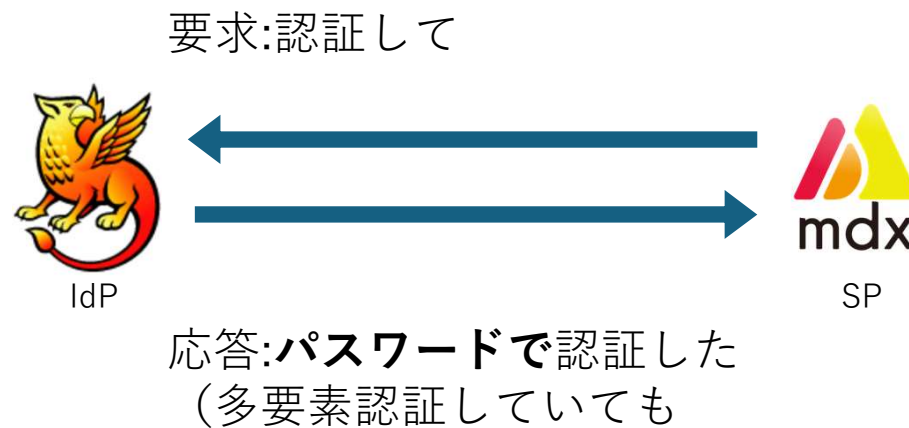
*プレビュー



- データ科学・データ駆動科学・データ活用応用にフォーカス
高性能仮想化環境
 - 9大学2研究所が共同運営し全国共同利用
 - @東京大学 柏2キャンパスに設置
- “学認”でログイン → 機関IdPでの認証 + **メールtoken認証**
 - **機関IdPで多要素認証済みなら独自/追加の認証は省略？**
- 民間企業等向け**mdx独自アカウント**(パスワード+TOTP認証)
 - NII認証プロキシ  **Orthros**に期待

機関IdPで多要素認証済みなら独自/追加の認証は省略？

- IdPとSPのやりとりを見てみると
普通のIdPと普通のSP



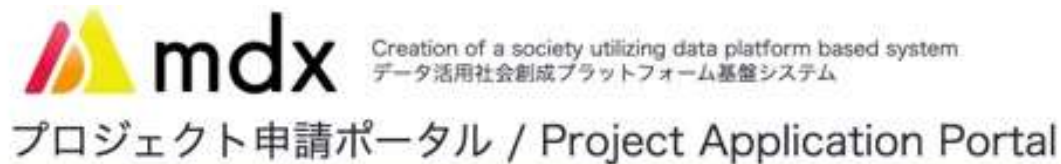
機関IdPで多要素認証済みなら独自/追加の認証は省略？

- IdPとSPのやりとりを見てみると
 - 通常「希望する認証」を送らない
 - 通常「どう認証したか」は「パスワード認証」と返ってくる（実際には多要素認証していても）
 - いきなり「学認AAL2で認証した」とは返してくれない
 - いきなり「学認AAL2を希望」しても「知らない」と言われる

AAL2普及過渡期のIdP-SPの橋渡し

- 「学認AAL2」 ボタン
- Step-down シーケンス
- Federation-assisted シーケンス

「学認AAL2」 ボタン



学術認証フェデレーション「学認 (GakuNin)」でログイン
Login with Academic Access Management Federation in Japan (GakuNin)

下記のリストに所属組織がある場合、所属組織選択後「選択」ボタンを押してログイン画面にお進みください。
if you find your institution, select it and click the "Login" button.

 GakuNin

所属機関:
東京大学

☐ ブラウザ起動中は自動ログイン

 選択

[リセット](#)

「サービス拒否」という主
ご所属組織での学認ご担当:
1. mdxを使用したいが
2. 説明が [学認ご担当者様へのページ](https://mdx.jp/guide/usage#to_gakunin_admin)(https://mdx.jp/guide/usage#to_gakunin_admin)にかかっている旨

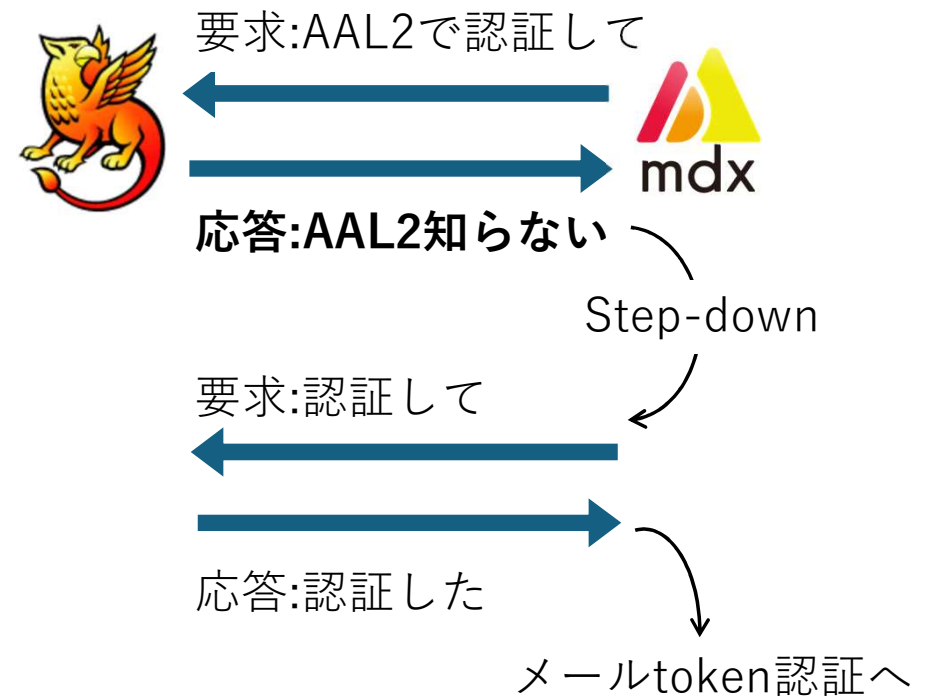
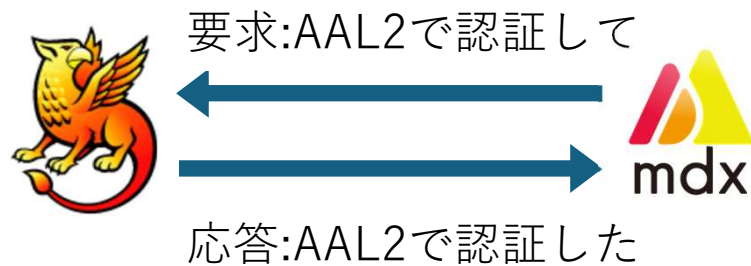
学認AAL2でログイン

学認アカウントをお持ちでない方 (mdxローカル認証でログイン)
For non-GakuNin user (Login with mdx account)

[mdxローカル認証 / mdx Local Login](#)

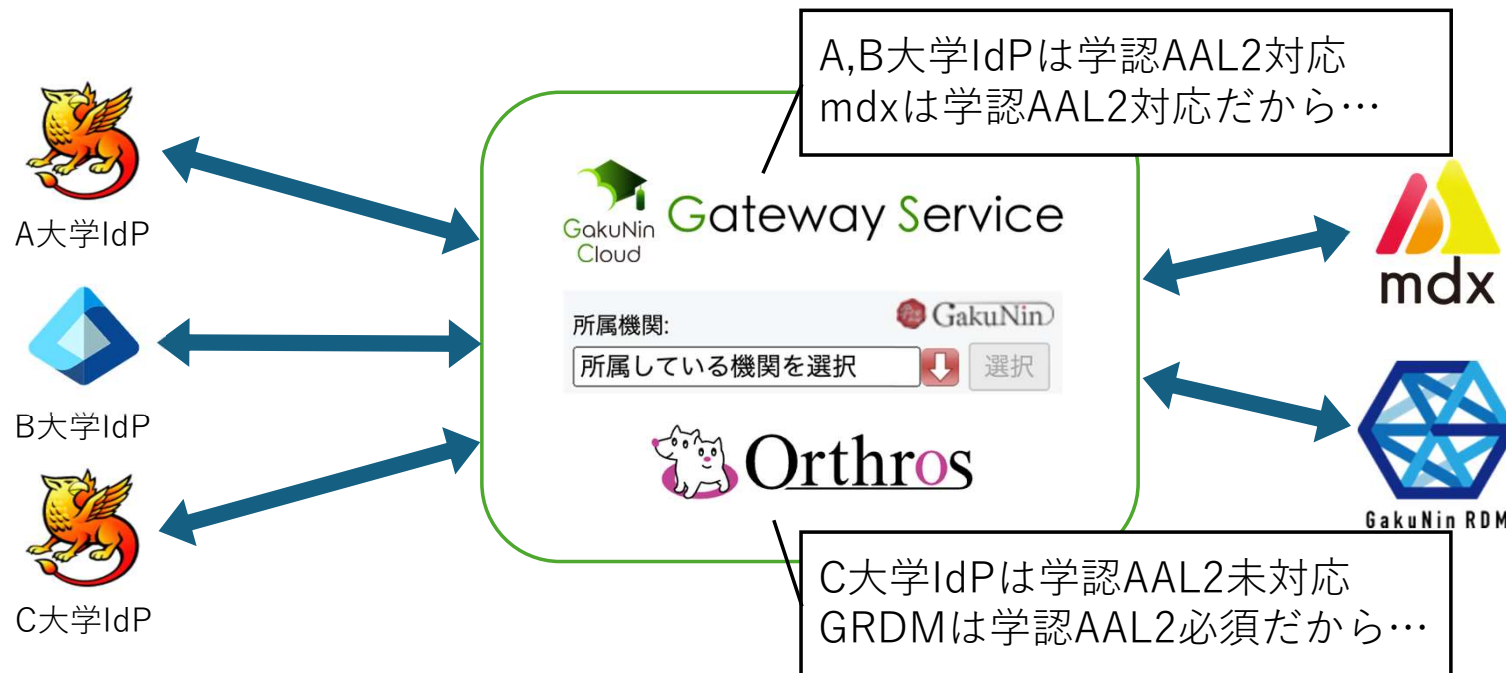
Step-down シーケンス

- AAL2認証要求に失敗したら従来の認証要求に戻す



Federation-assisted シーケンス

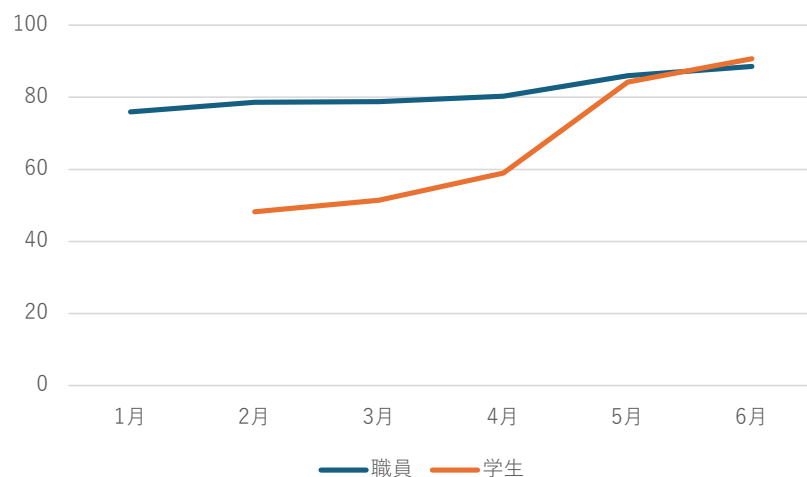
- 学認AAL2対応状況をメタデータに記載し
- Gateway, DS, Orthrosが仲介するとHappy？



おわり

付録)多要素認証 100% と 共通ID一元化

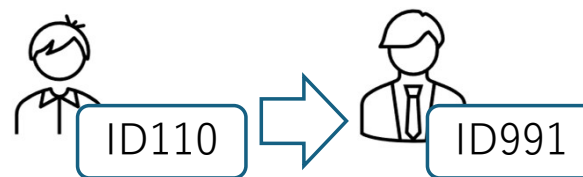
- 多要素認証 有効化率



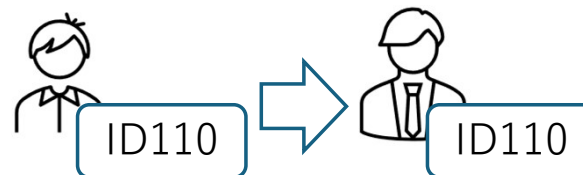
- UTokyo Wi-Fiアカウント発行に多要素認証を必要にした

- 学生→職員で共通ID不変に

従来:



現在:



- eduPersonAffiliation multi-valued
ePA = {'student', 'staff'}
if 'student' in ePA then **deny** #想定外
elseif 'staff' in ePA then allow

備考

- 東京大学における認証基盤の取り組み @NIIof2023認証1
- UTokyo Account & mdx AAL2&IAL2対応 @NIIof2022認証3