NII 学術情報基盤オープンフォーラム 2022
認証トラック３

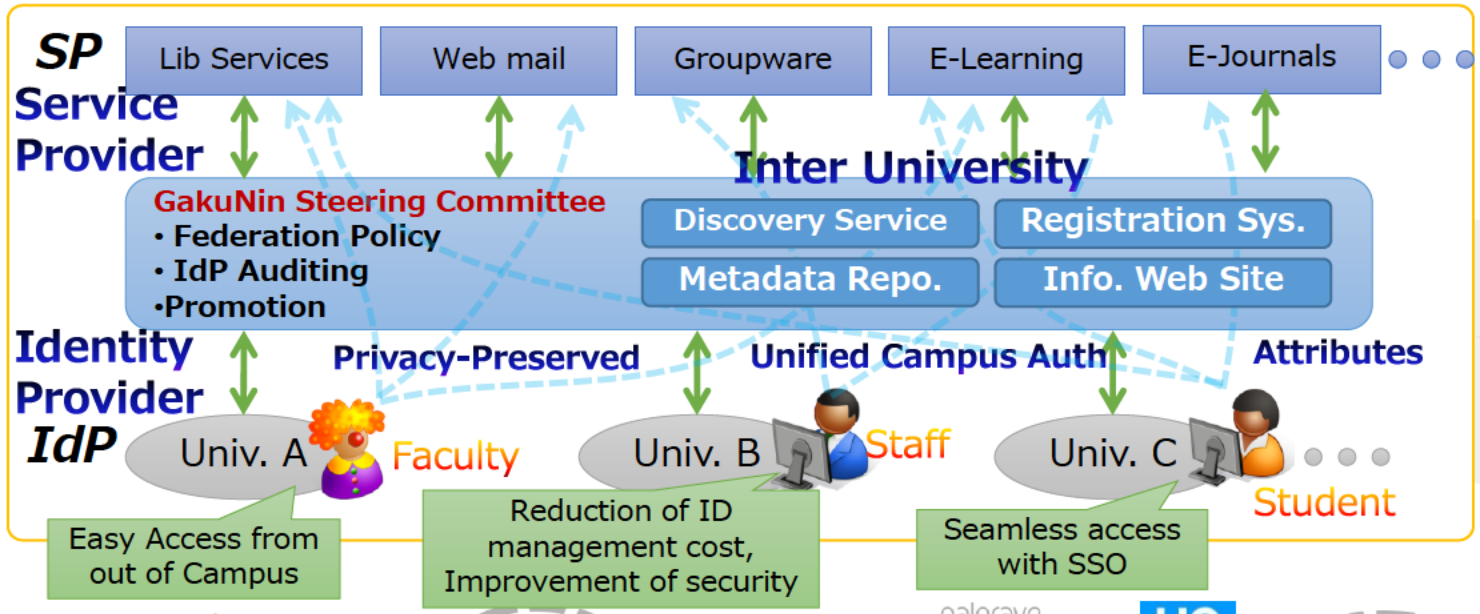
認証プロキシサービス Orthros の概要

坂根 栄作

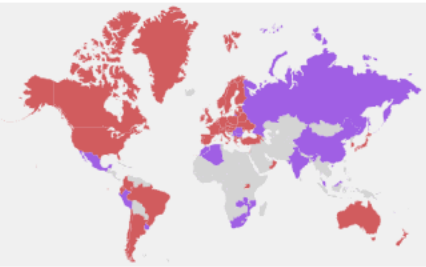
国立情報学研究所

学術認証フェデレーション

- 学認は、サイバー空間における円滑な学術活動を支援すべくトラストフレームワーク（ポリシ、技術、評価）を提供
  - 全学的なサービスに対してうまく機能



Academic Federations have been established per country basis



次世代認証連携への要望（SP視点）

- IdP を持たない利用者の認証
  - 利用者は、必ずしも学認に参加するIdPのアカウントを所有しているわけではない
  - 信頼に足る本人確認を行っている IdP に依拠したい
- 認証レベルの把握
  - Id&Password か 多要素か
  - 多要素認証を経た利用者のみにサービスを提供する、のようなフィルタリング

- 複数組織に所属する利用者の同定
- 組織異動における利用者の同一性の担保
  - 組織間異動があっても情報資産利活用の継続性を担保したい
    - GakuNin RDM 上の資産を継続的に利用したい

- 用途に応じた属性の提供
  - 例：居住者か非居住者かを把握したい（輸出管理）

IdP 拡大の取り組み

- 適切な IdP がない利用者をどのように認証するか
  - 学術機関の利用者
    - 所属機関の学認参加を支援
  - 企業の利用者

- 一方で、一般社会には様々な Id 基盤が存在する
  - gBizID, ORCID, Google/Microsoft, SNS, 公的個人認証, 携帯事業者, …
  - これらのプロバイダと連携することで、SP に認証情報を送信

- 利用者は、適切な IdP を選択して SP の認証に利用できるようになる

IdP 強化の取り組み

- より強い認証に向けて
  - 本人確認の保証度（Identity Assurance Level: IAL）
  - 認証強度（Authenticator Assurance Level: AAL）

- 本人確認の保証度
  - IdP の IAL 評価基準と認定手続きの確立
  - 単一の IdP で IAL 要件を満たさない場合に、複数 IdP の組み合わせにより IAL を上げる仕組みの検討
- 認証強度
  - 多要素認証の技術支援（導入・運用）
  - 単一の IdP で AAL 要件を満たさない場合に、AAL を上げる仕組みの検討

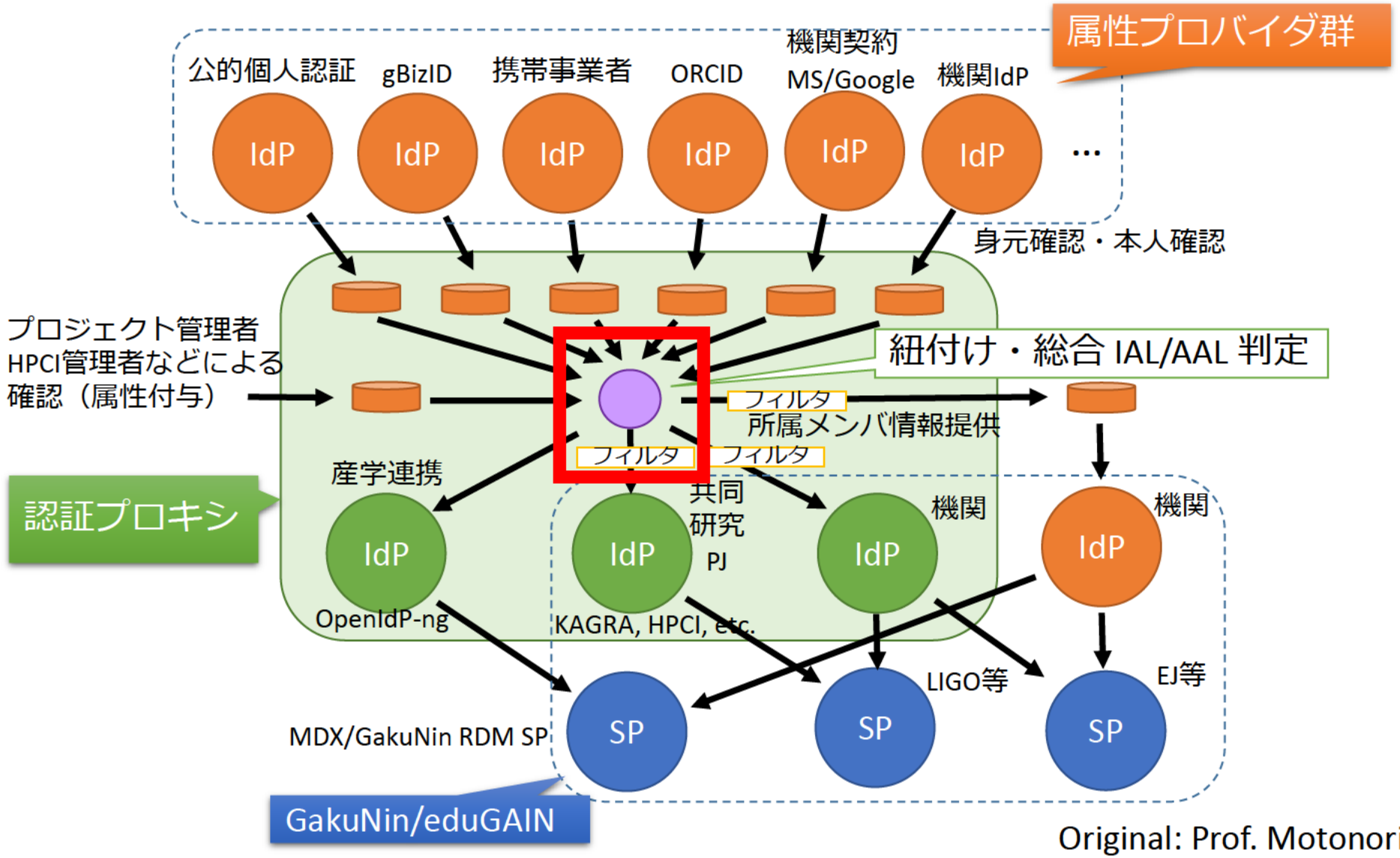
- 利用者は、適切な保証度の認証で SP を利用できるようになる

認証プロキシサービスの研究開発

- 産学連携を念頭においた SP への Id 連携時に必要な Id 保証の担保などに柔軟に対応する
  - IAL, AAL matching, AL enhancement
  - credential bridging (e.g., OAuth access token -> SAML assertion)

- 既存の研究コミュニティのもつトラストフレームワークにおいて、Id 基盤部分を外だしできるようにする
  - 本人確認手続きを外部に依拠できる

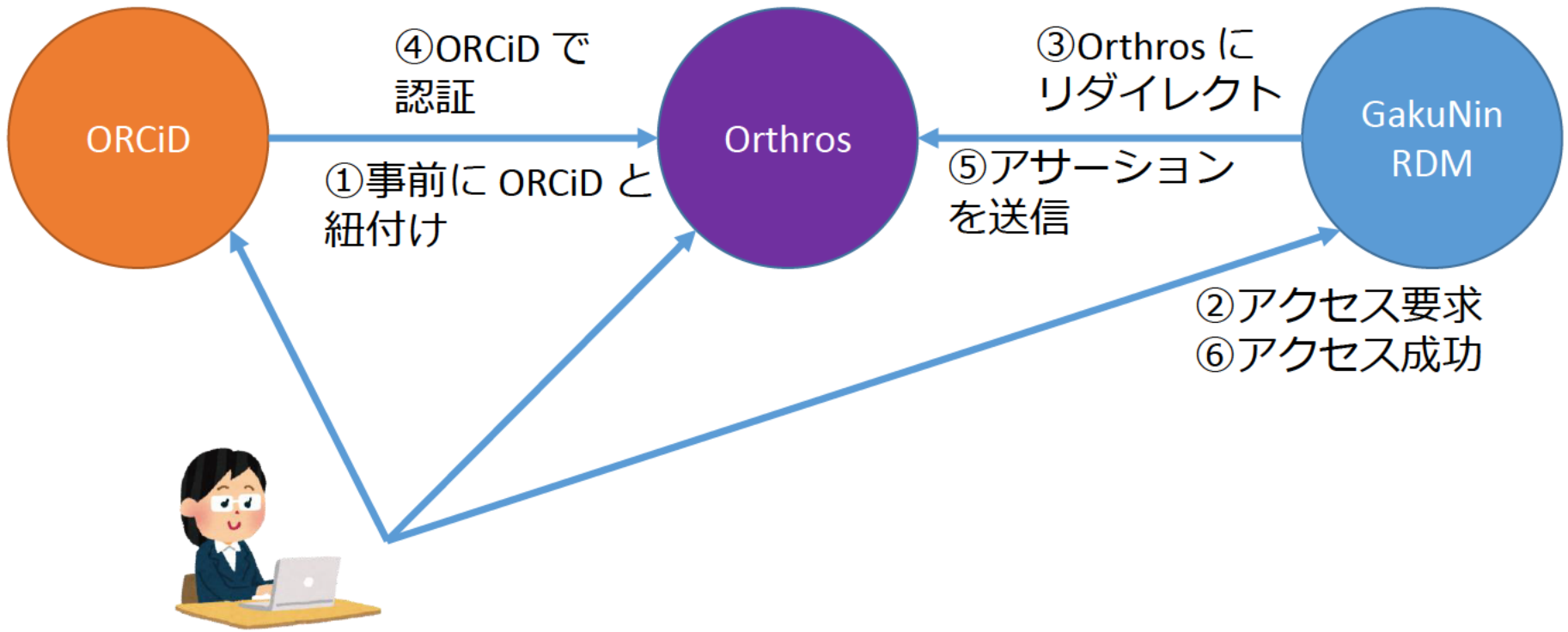
認証プロキシのデザイン



Original: Prof. Motonori Nakamura

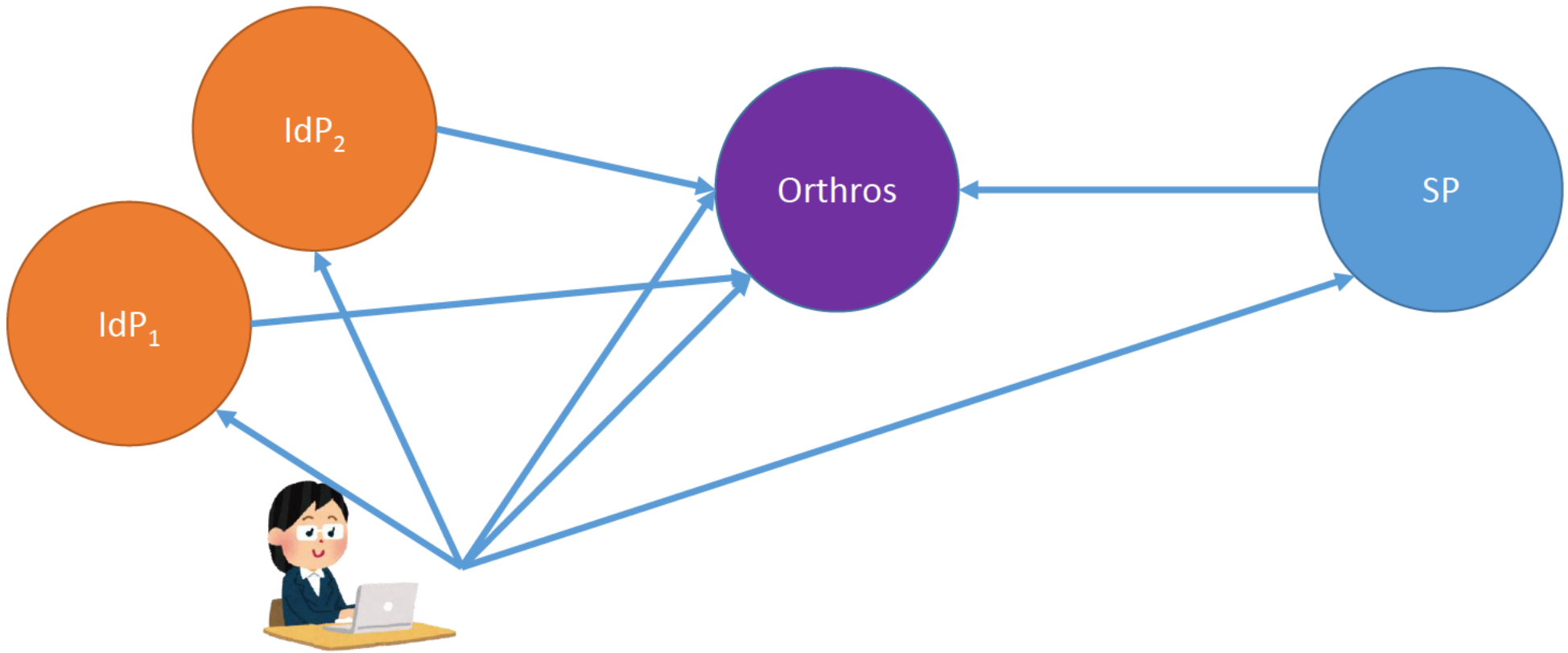
ユースケース１ – credential bridging

- 企業の研究者が GakuNin RDM を利用する



ユースケース2 – IAL enhancement

- 複数の Id を紐づけることにより、SP の要求 IAL, AAL に対応する



認証プロキシサービス Orthros の設計・実装

- 認証プロキシコア部 (IDaaS) – **SELMID** https://ctc-insight.com/selmid
- 各種機能設定インターフェイス部 (マイページ機能) – 内製

- 基本機能
  - ID 管理、ログイン、ID 紐付け、ID 紐付け管理、属性更新
- SP管理機能（管理者向け機能）
  - SP毎に要求するIALおよびAALを設定する機能
- SP単位の同意管理機能
  - 利用者がSPに初回ログインする際に同意を取得する機能
  - 利用者が自身の同意状態の確認・取り消しが出来る機能
  - 管理者が機関内のユーザの同意状態を確認する機能
- 属性保証（旧機関管理）
  - 管理者が管理対象ユーザの属性を保証する機能
  - 例）自機関に所属するユーザの所属属性を保証する（招待による確認～属性付与）

Orthros の設計・実装（続き）

- 更なる機能強化
  - メールアドレス変更時の通知機能
  - アカウント停止機能
  - マイページ上に連携済みIdPの情報を表示する機能
  - パスワードの強制リセット機能

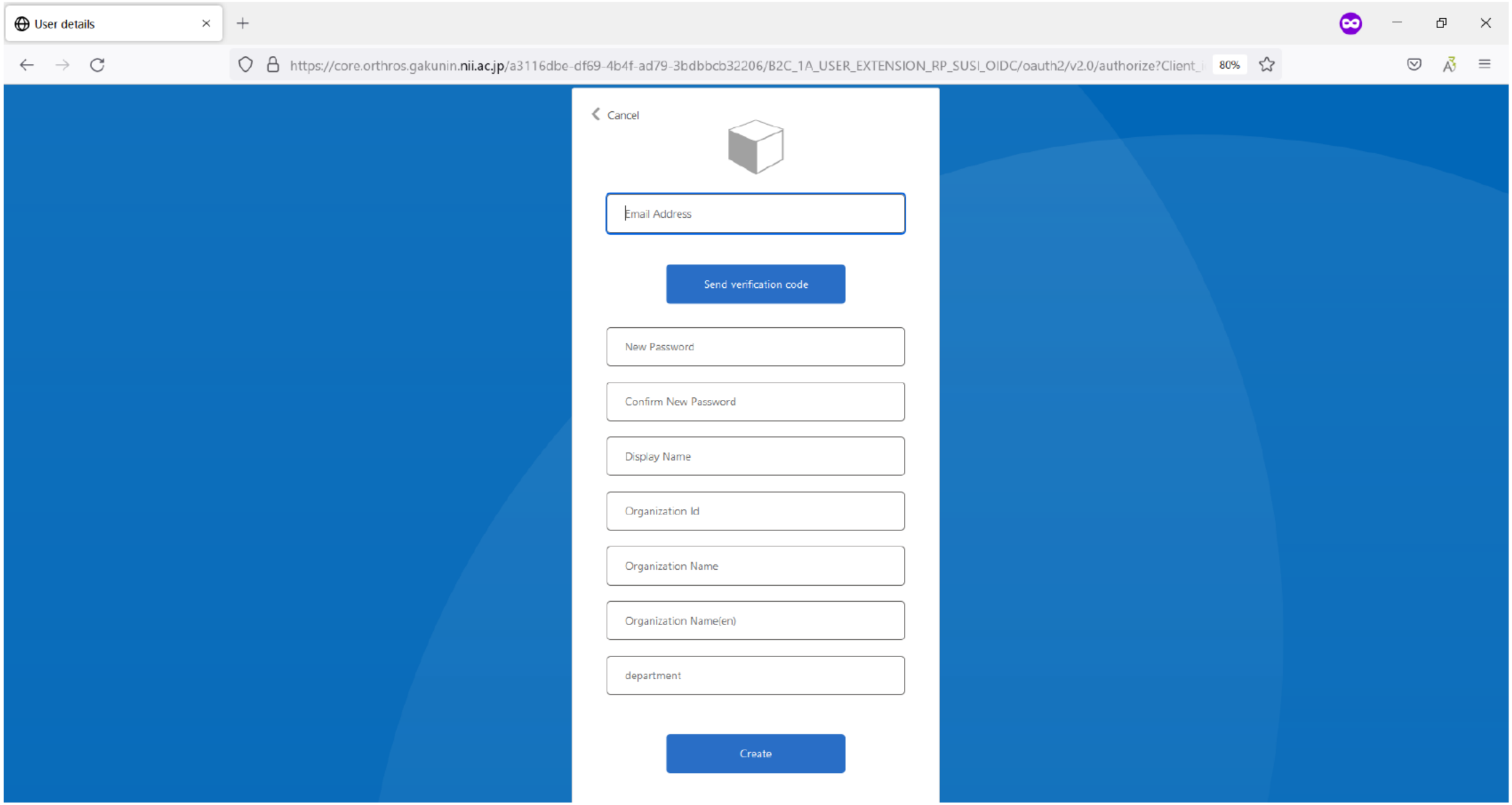
- 外部IdPの追加
  - 接続済み：LINE, Google, Yahoo! JAPAN, Facebook, Twitter
  - 調整中：gBizID, ORCiD

- SP の追加
  - meatwiki, GakuNin RDMステージング環境

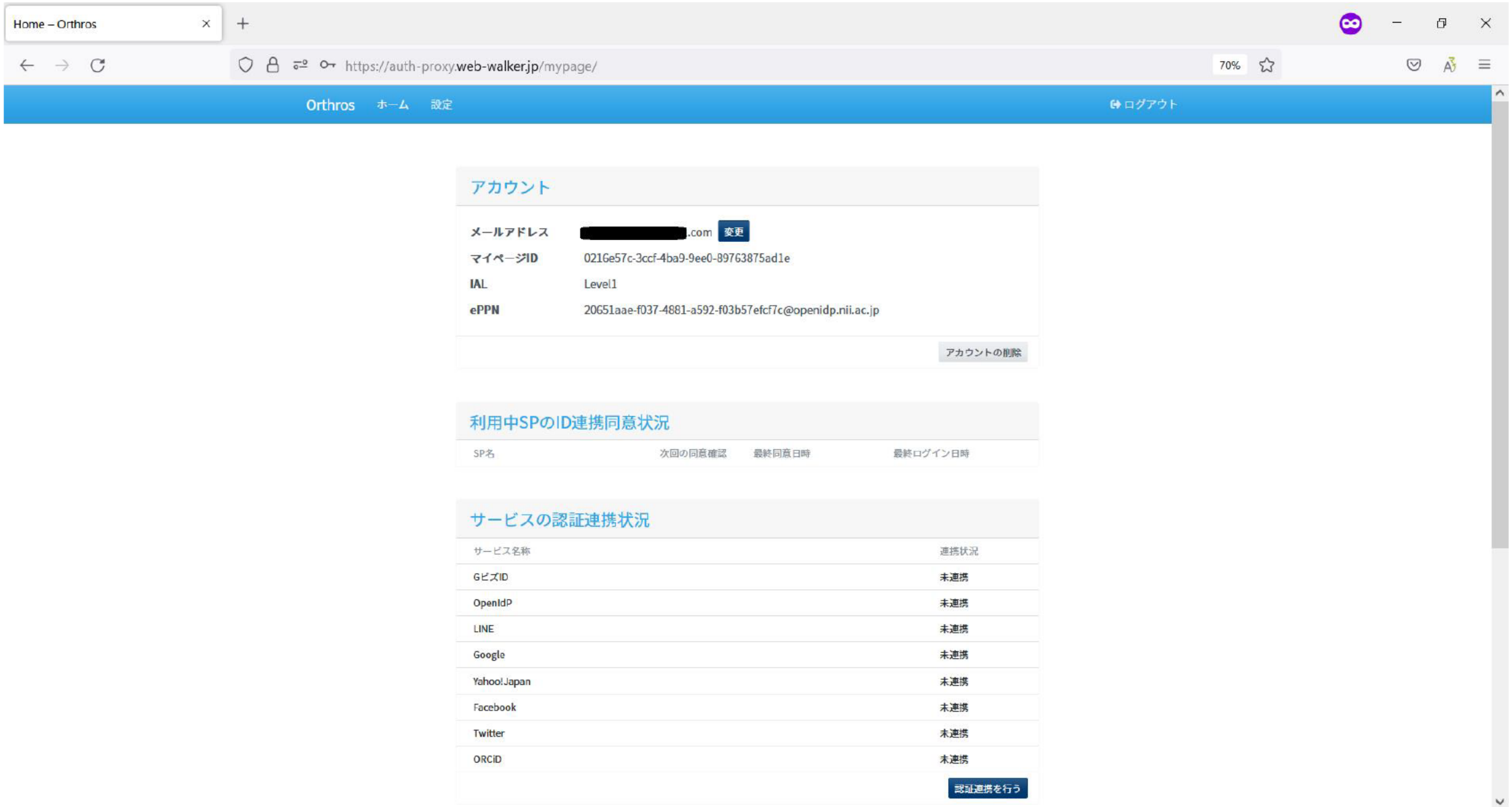
新規登録 (1/4)


Orthros
https://auth-proxy.web-walker.jp
Orthros
Orthrosへようこそ。
ログイン
新規登録

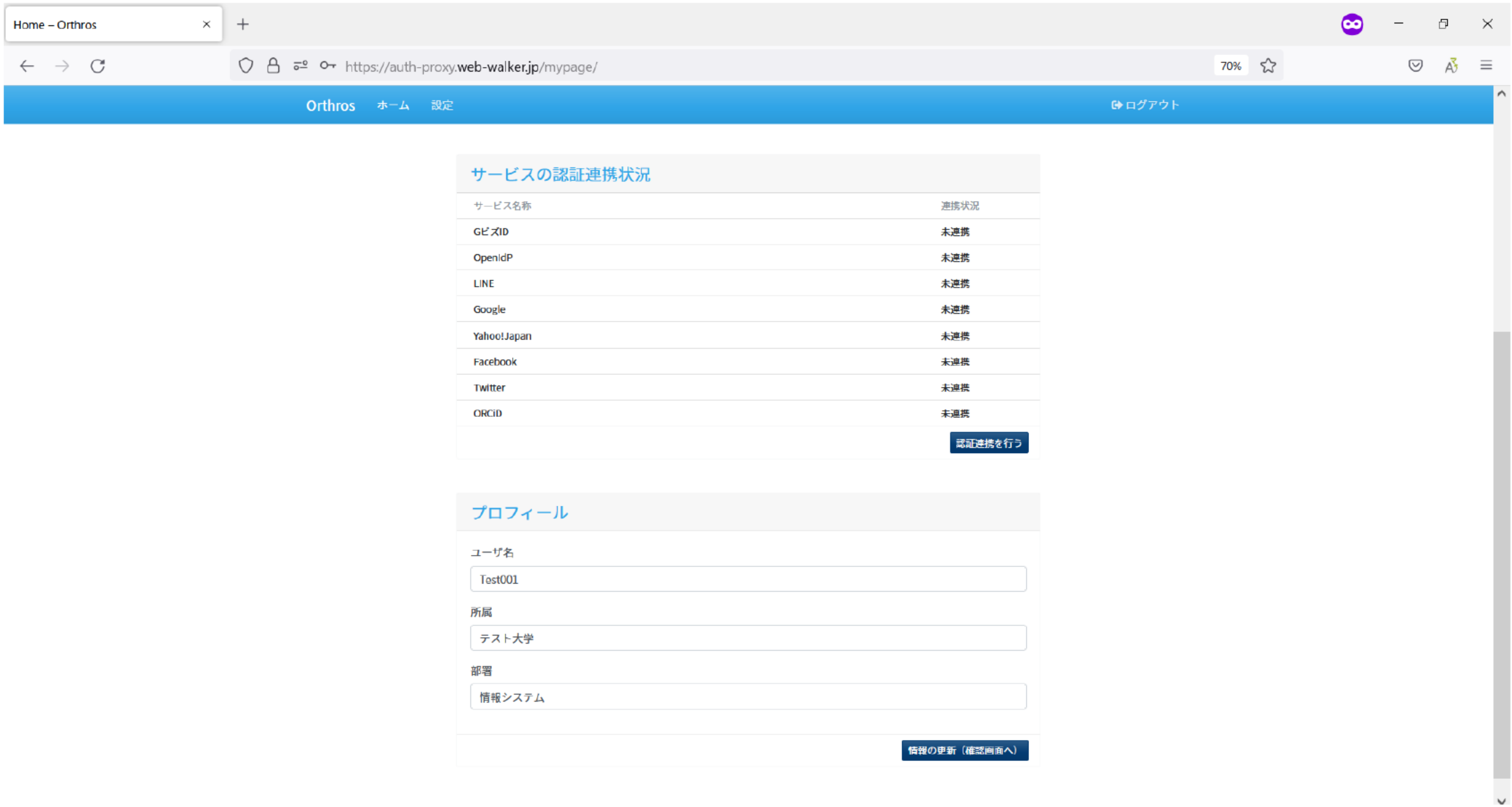
新規登録 (2/4)


User details
https://core.orthros.gakunin.nii.ac.jp/a3116dbe-df69-4b4f-ad79-3bdbbcb32206/B2C_1A_USER_EXTENSION_RP_SUSI_OIDC/oauth2/v2.0/authorize?Client_
80%
Cancel
Email Address
Send verification code
New Password
Confirm New Password
Display Name
Organization Id
Organization Name
Organization Name(en)
department
Create

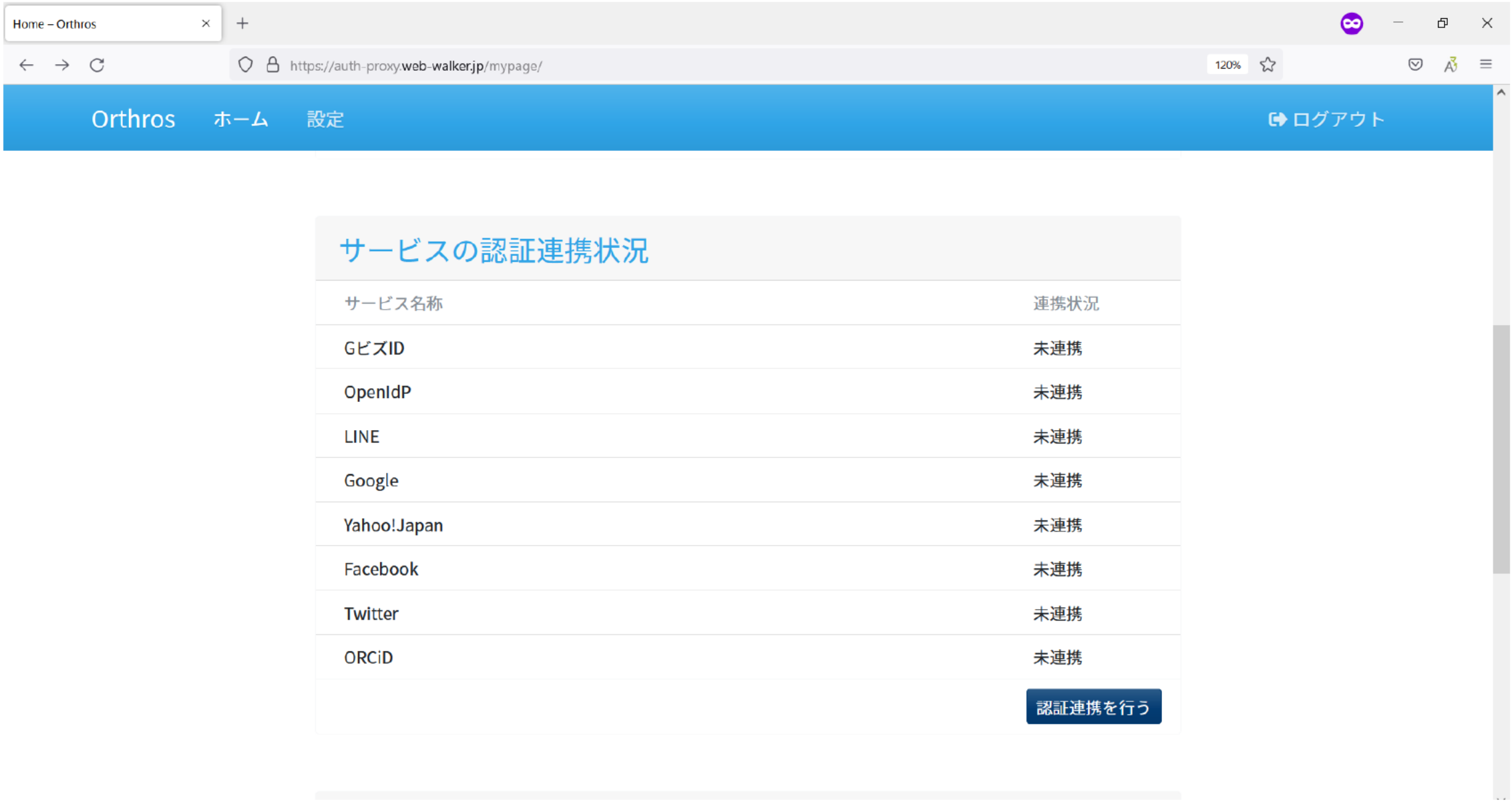
新規登録 (3/4)


Home – Orthros
https://auth-proxy.web-walker.jp/mypage/
70%
Orthros
ホーム
設定
ログアウト
アカウント
メールアドレス
[redacted].com
変更
マイページID
0216e57c-3ccf-4ba9-9ee0-89763875ad1e
IAL
Level1
ePPN
20651aae-f037-4881-a592-f03b57efcf7c@openidp.nii.ac.jp
アカウントの削除
利用中SPのID連携同意状況
SP名
次回の同意確認
最終同意日時
最終ログイン日時
サービスの認証連携状況
サービス名称
連携状況
GビズID
未連携
OpenIdP
未連携
LINE
未連携
Google
未連携
Yahoo!Japan
未連携
Facebook
未連携
Twitter
未連携
ORCiD
未連携
認証連携を行う

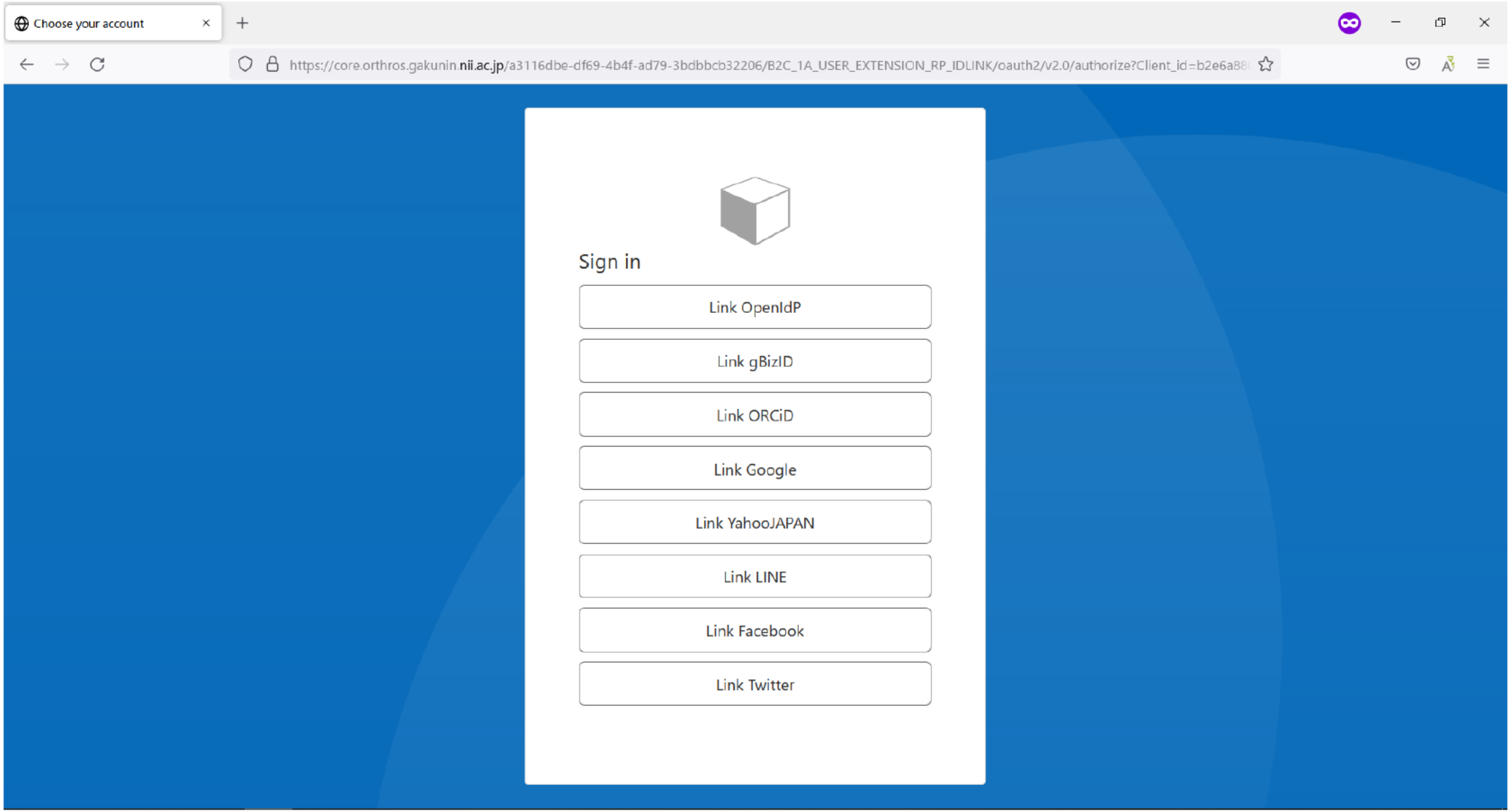
新規登録 (4/4)


Home – Orthros
https://auth-proxy.web-walker.jp/mypage/
70%
Orthros
ホーム
設定
ログアウト
サービスの認証連携状況
サービス名称
連携状況
GビズID
未連携
OpenIdP
未連携
LINE
未連携
Google
未連携
Yahoo!Japan
未連携
Facebook
未連携
Twitter
未連携
ORCiD
未連携
認証連携を行う
プロフィール
ユーザ名
Test001
所属
テスト大学
部署
情報システム
情報の更新（確認画面へ）

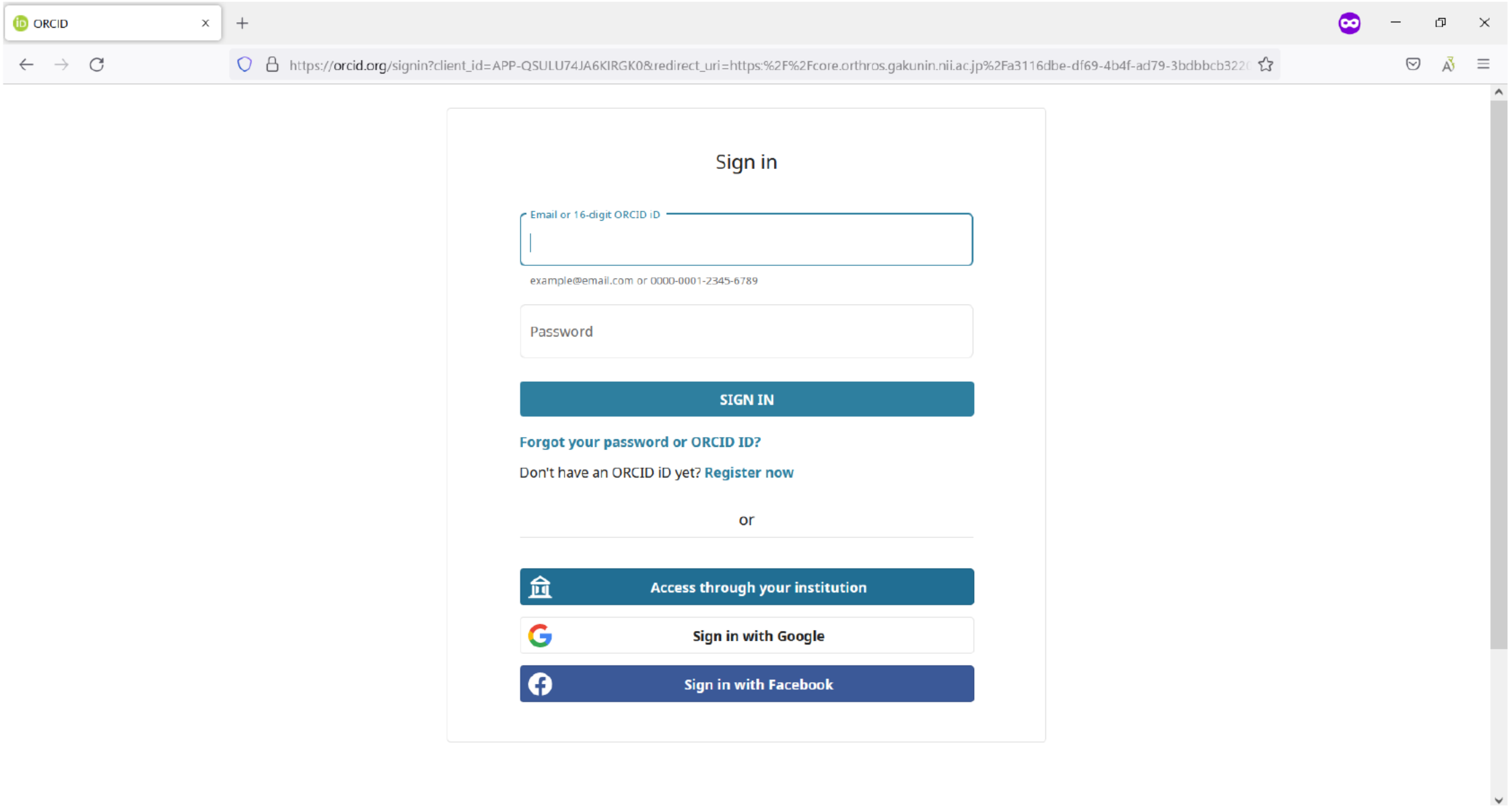
外部ID連携 (1/4)


Home – Orthros
https://auth-proxy.web-walker.jp/mypage/
120%
Orthros
ホーム
設定
ログアウト
サービスの認証連携状況
サービス名称
連携状況
GビズID
未連携
OpenIdP
未連携
LINE
未連携
Google
未連携
Yahoo!Japan
未連携
Facebook
未連携
Twitter
未連携
ORCiD
未連携
認証連携を行う

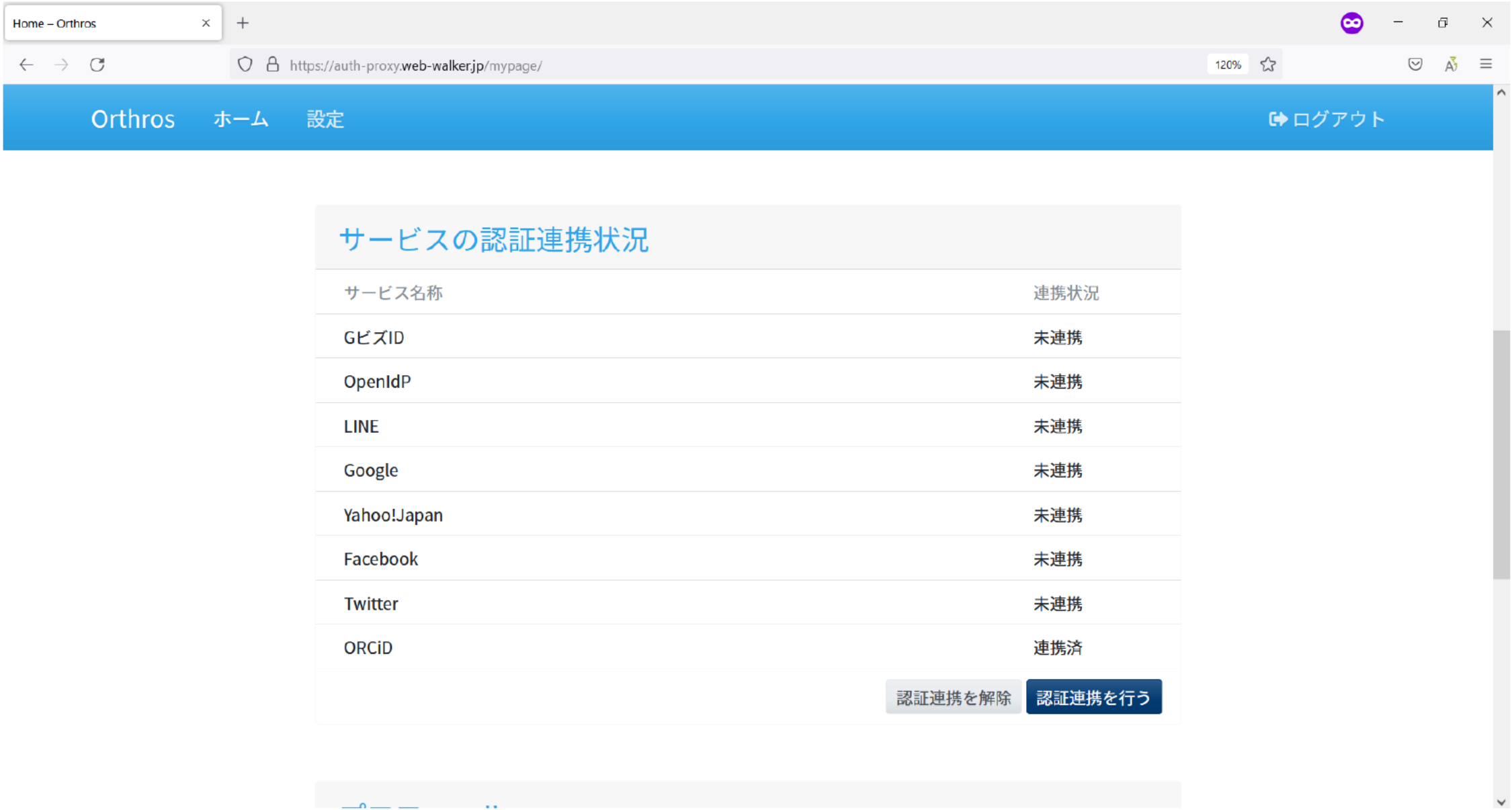
外部ID連携 (2/4)


Choose your account
https://core.orthros.gakunin.nii.ac.jp/a3116dbe-df69-4b4f-ad79-3bdbbcb32206/B2C_1A_USER_EXTENSION_RP_IDLINK/oauth2/v2.0/authorize?Client_id=b2e6a88
Sign in
Link OpenIdP
Link gBizID
Link ORCiD
Link Google
Link YahooJAPAN
Link LINE
Link Facebook
Link Twitter

外部ID連携 (3/4)


ORCID
https://orcid.org/signin?client_id=APP-QSULU74JA6KIRGK0&redirect_uri=https:%2F%2Fcore.orthros.gakunin.nii.ac.jp%2Fa3116dbe-df69-4b4f-ad79-3bdbbcb322
Sign in
Email or 16-digit ORCID iD
example@email.com or 0000-0001-2345-6789
Password
SIGN IN
Forgot your password or ORCID ID?
Don't have an ORCID iD yet? Register now
or
Access through your institution
Sign in with Google
Sign in with Facebook

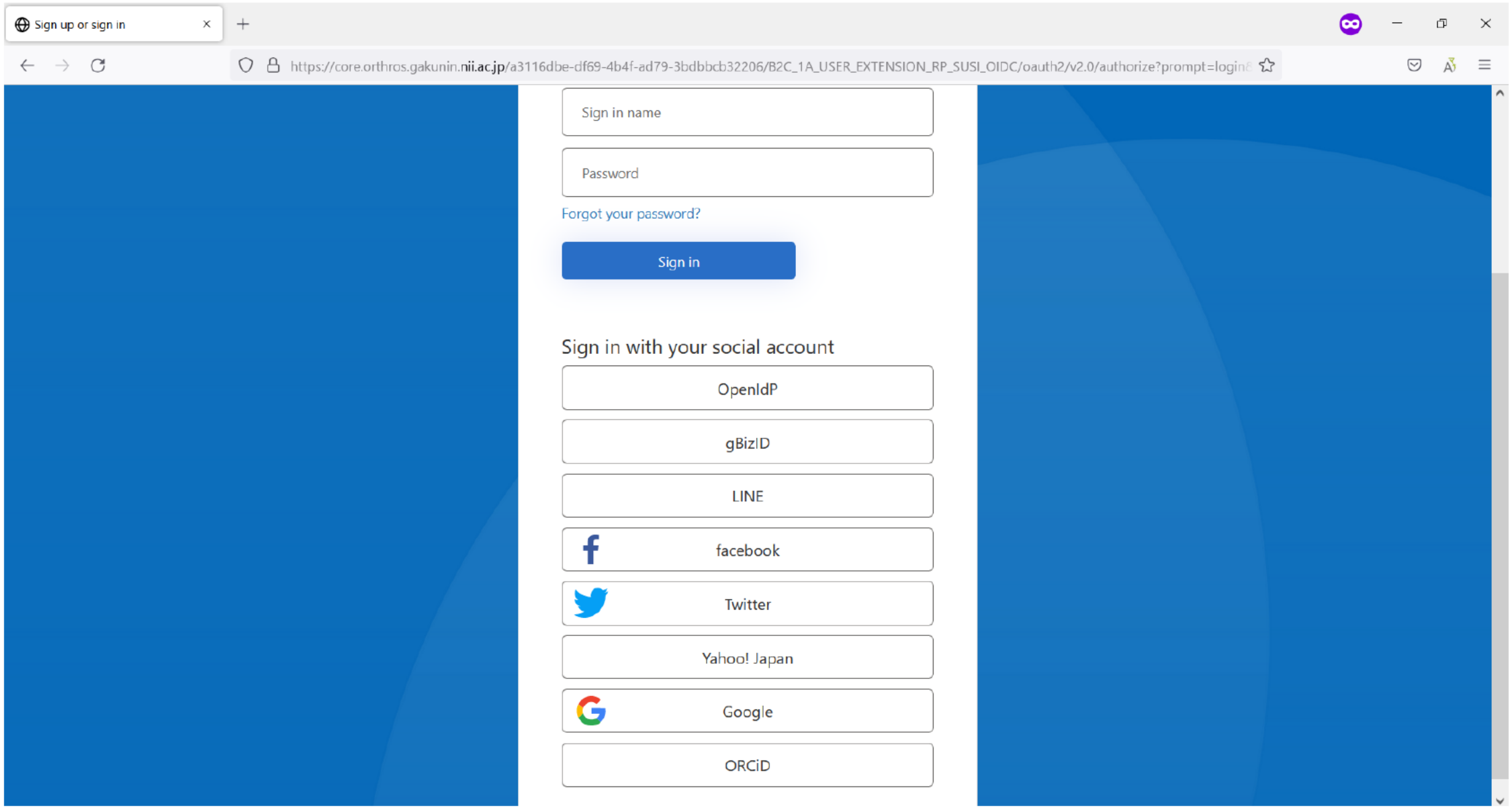
外部ID連携 (4/4)


Home – Orthros
https://auth-proxy.web-walker.jp/mypage/
120%
Orthros
ホーム
設定
ログアウト
サービスの認証連携状況
サービス名称
連携状況
GビズID
未連携
OpenIdP
未連携
LINE
未連携
Google
未連携
Yahoo!Japan
未連携
Facebook
未連携
Twitter
未連携
ORCiD
連携済
認証連携を解除
認証連携を行う

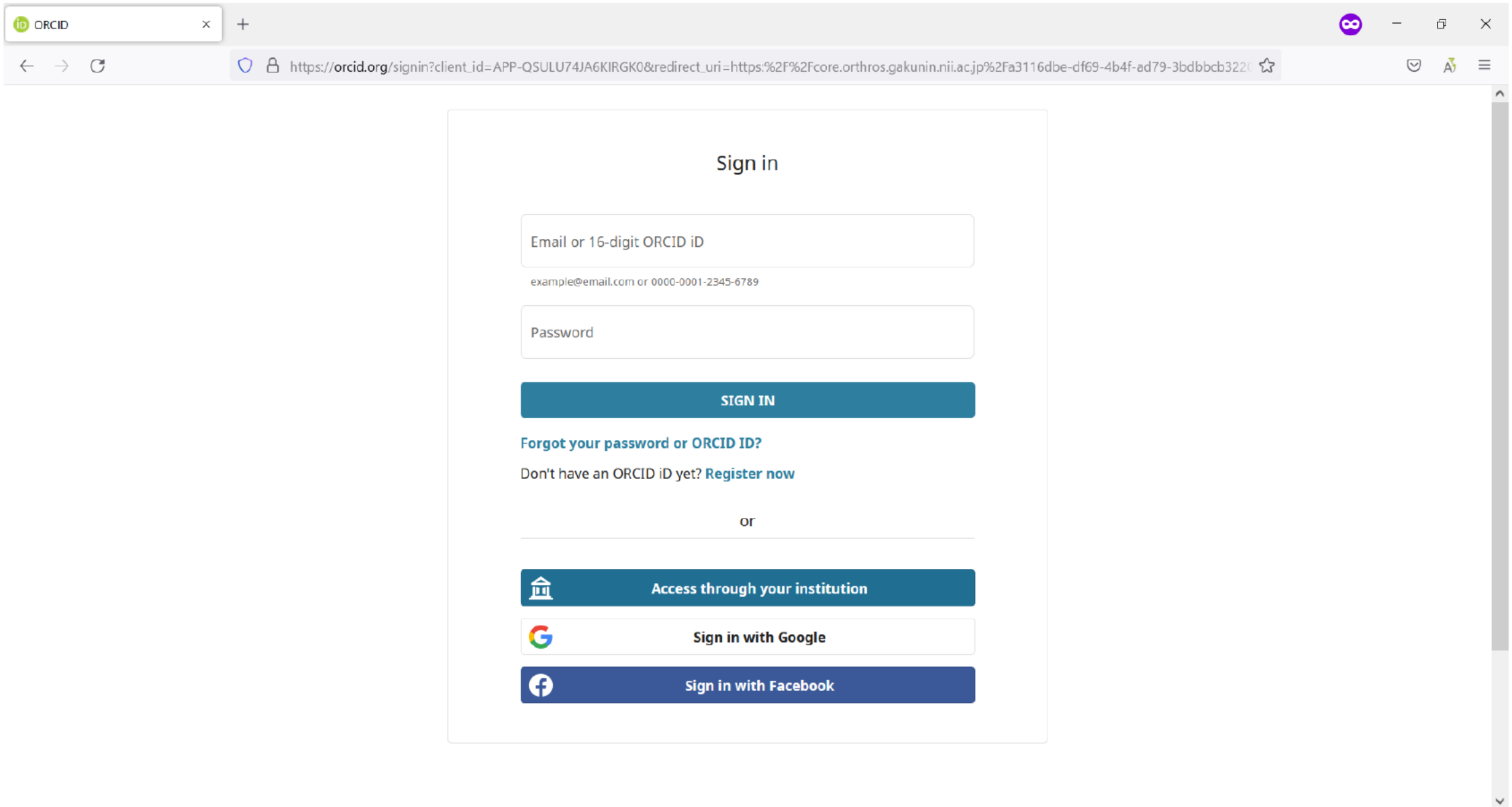
ログイン (1/4)


Orthros
https://auth-proxy.web-walker.jp
Orthros
Orthrosへようこそ。
ログイン
新規登録

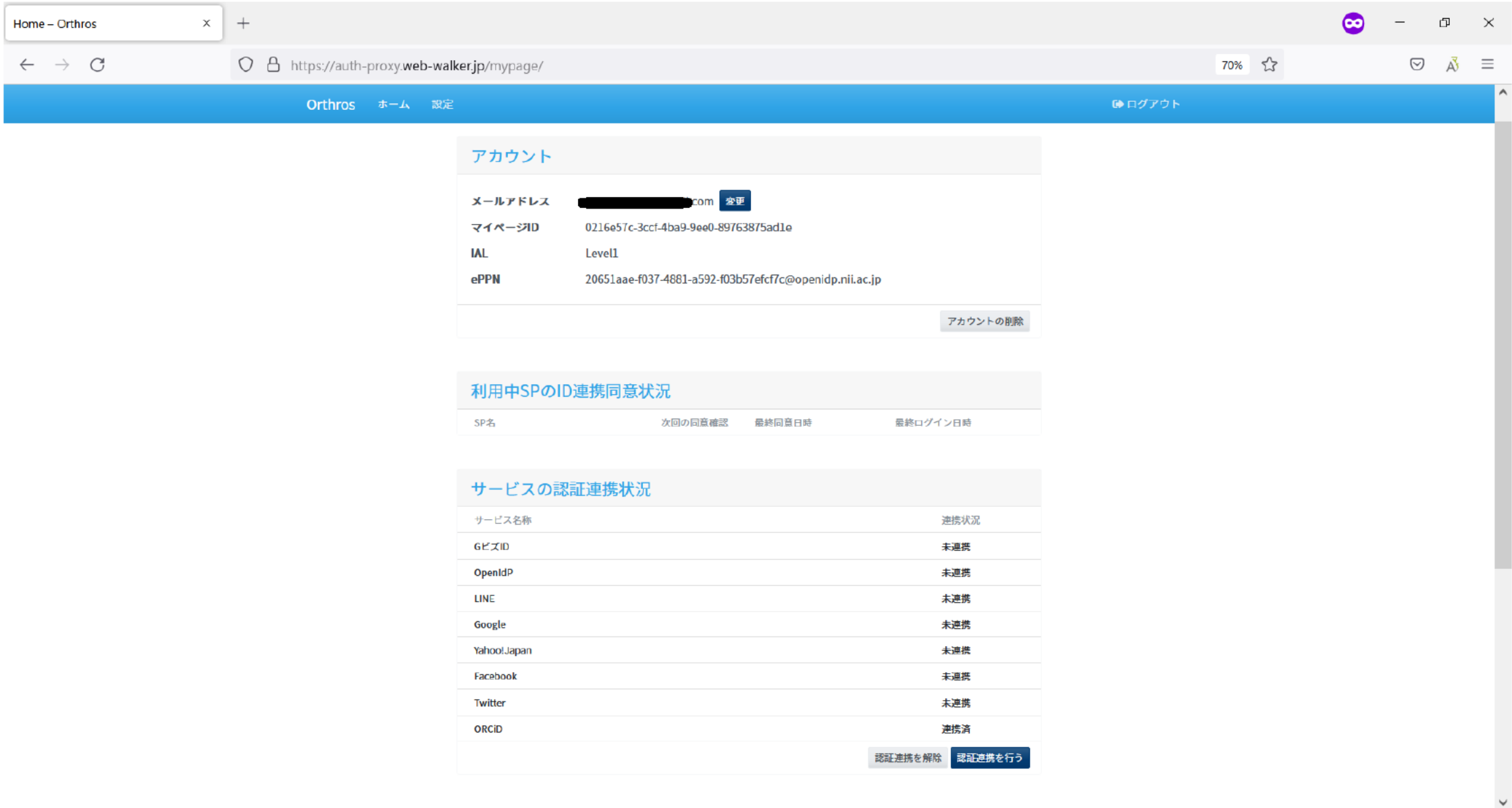
ログイン (2/4)


Sign up or sign in
https://core.orthros.gakunin.nii.ac.jp/a3116dbe-df69-4b4f-ad79-3bdbbcb32206/B2C_1A_USER_EXTENSION_RP_SUSI_OIDC/oauth2/v2.0/authorize?prompt=login
Sign in name
Password
Forgot your password?
Sign in
Sign in with your social account
OpenIdP
gBizID
LINE
facebook
Twitter
Yahoo! Japan
Google
ORCiD

ログイン (3/4)


ORCID
https://orcid.org/signin?client_id=APP-QSULU74JA6KIRGK0&redirect_uri=https:%2F%2Fcore.orthros.gakunin.nii.ac.jp%2Fa3116dbe-df69-4b4f-ad79-3bdbbcb322
Sign in
Email or 16-digit ORCID iD
example@email.com or 0000-0001-2345-6789
Password
SIGN IN
Forgot your password or ORCID ID?
Don't have an ORCID iD yet? Register now
or
Access through your institution
Sign in with Google
Sign in with Facebook

ログイン (4/4)


Home – Orthros
https://auth-proxy.web-walker.jp/mypage/
70%
Orthros
ホーム
設定
ログアウト
アカウント
メールアドレス
[redacted]com
変更
マイページID
0216e57c-3ccf-4ba9-9ee0-89763875ad1e
IAL
Level1
ePPN
20651aae-f037-4881-a592-f03b57efcf7c@openidp.nii.ac.jp
アカウントの削除
利用中SPのID連携同意状況
SP名
次回の同意確認
最終同意日時
最終ログイン日時
サービスの認証連携状況
サービス名称
連携状況
GビズID
未連携
OpenIdP
未連携
LINE
未連携
Google
未連携
Yahoo!Japan
未連携
Facebook
未連携
Twitter
未連携
ORCiD
連携済
認証連携を解除
認証連携を行う

FY2022 開発計画

- Orthros 機能強化
  - 一般利用者／管理者の利便性向上
  - 組織異動における利用者の同一性の担保
    - 異動前後の異なるIdPの認証情報の紐付け
    - Persistent ID の活用（異動の裏付け）
    - SP の認可条件更新支援（そのためのプロトコル策定）
  - 属性の整理（認可属性は mAP Core に委譲）

- Orthros パイロット運用開始
  - 環境構築
  - OpenIdP 移行
  - 属性保証機能の活用
    - IdP ホスティング
  - 運用ポリシ・運用規程策定
    - IAL/AAL 認定手続き

まとめ

- 認証プロキシサービス Orthros
  - 次世代認証連携作業部会で議論する課題を解決する提案手法の１つ
  - Credential bridging, IAL/AAL matching, AL enhancement
    - 複数ID紐付け

- IdP と SP とを仲介する Orthros