サイエンティフィック・システム研究会
システム技術分科会 2022年度会合

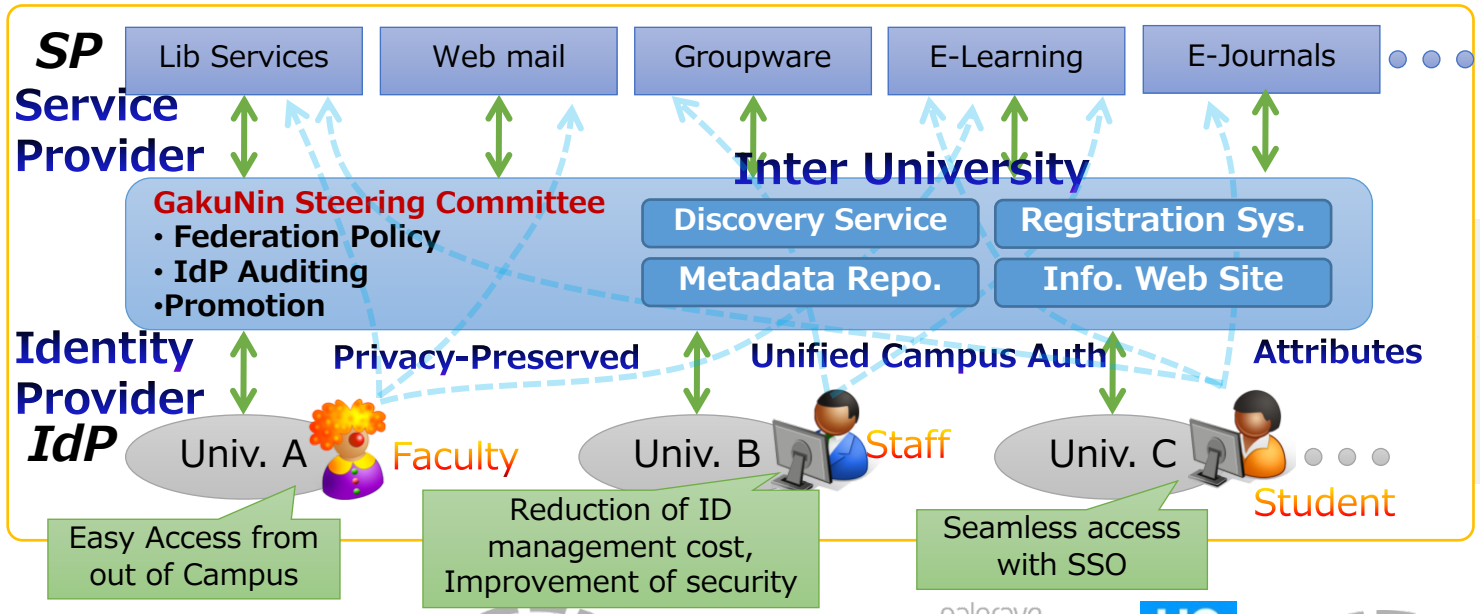
学認が目指す次世代認証連携

坂根 栄作

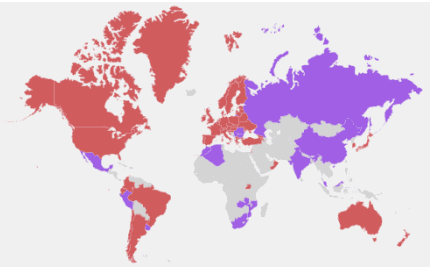
国立情報学研究所

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



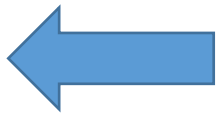
Academic Federations have been established per country basis



研究・教育DXを推進するために

- 研究・教育データ流通の加速が必須
  - 融合領域研究におけるコミュニティ間
  - 産学連携
  - 国際連携
- データ流通の加速には、全学的なサービスだけでなく、多種多様なサービスの円滑な利活用が必要

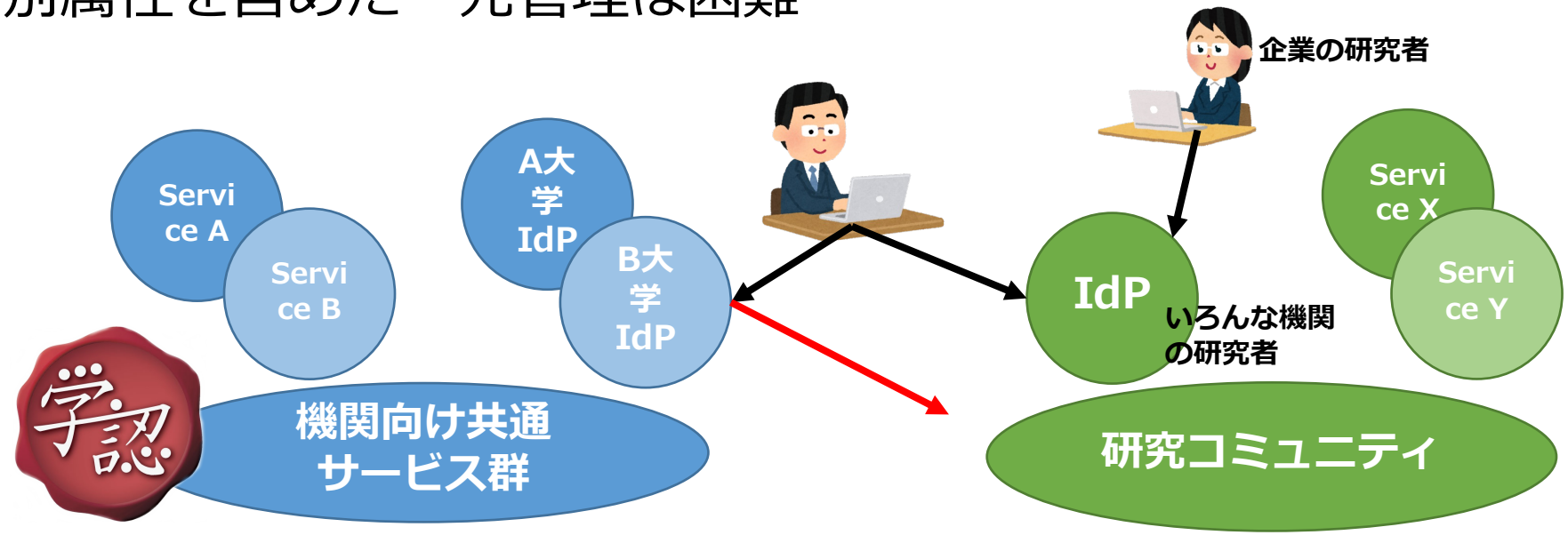
- データ流通において、認証認可は極めて重要
  - データを、誰が提供するのか
  - データに、誰が参照するのか



複雑化

多様なサービスの円滑な利活用

- 機関共通サービスからより多様なサービスへ
  - 研究者は、機関共通サービスだけではなく、研究固有のサービスを利用
  - 研究固有サービスの認証認可における要件も多種多様：
    - 利用者と ID データとの紐付け度合い
    - 利用属性
  - 大学(ID管理者)は、多種多様な研究者が存在するため、共通属性以外の個別属性を含めた一元管理は困難



研究・教育DXを推進するために（続き）

- 研究・教育データ流通の加速が必須
- データ流通において、認証認可は極めて重要
  - データを、誰が提供するのか
  - データに、誰が参照するのか

- コミュニティ単体で対応することの限界
  - 独自のトラストフレームワークに基づいた基盤運用は持続可能か？
  - コミュニティ間でデータをどのように流通させるのか？

- 研究・教育DXを推進する新しいトラストフレームワーク
  - 認証ポリシの相互運用性
    - Identity Assurance Level (IAL), Authenticator Assurance Level (AAL)
  - 認証認可技術の高度化

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
    - e.g., 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し、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

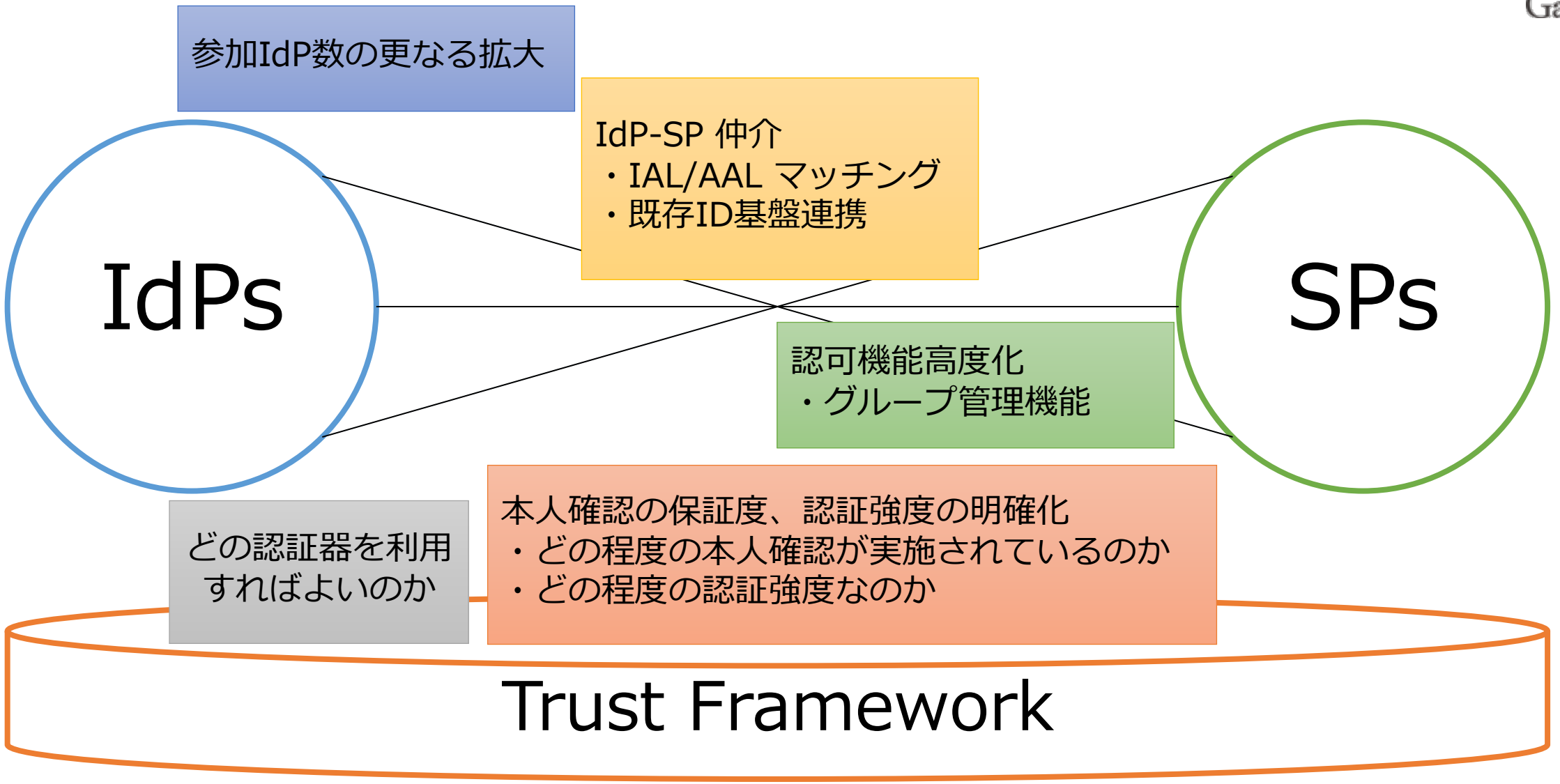
IdP 強化の取り組み

- 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

新しいトラストフレームワーク



次世代認証連携における主要構成要素

学認IAL/AAL

- 本人確認の保証度、認証強度について規定

認証器レジストリ

- 学認AALに基づく認証器の評価

認証プロキシサービス

- IAL/AAL matching, Credential bridging, Attribute coordination

IdPホスティングサービス

- 大学、研究機関のIdP構築運用の課題を議論

グループ管理機能の高度化

- より高度な認可要求に対応

作業部会およびサブWGにおける活動

- 学術認証運営委員会にて、以下の作業部会を設置
  - 次世代認証連携検討作業部会
    - 短期取組検討サブワーキンググループ

- 次世代認証連携検討作業部会
  - IAL/AAL 評価基準および認定手続きの検討
  - AAL 技術支援の検討
  - persistent ID の検討

- 短期取組検討サブWG
  - IAL2/AAL2 の認証試行開始に向けて
    - まずは試験的 IdP/SP で実証実験を実施予定
    - 各大学の実運用 IdP への展開に向けた課題整理
    - 実証実験参加機関を募集

規準策定の取り組み

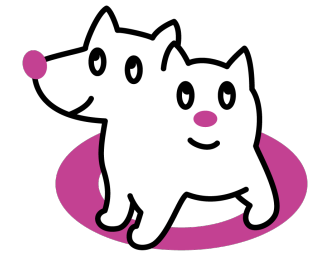
- 身元確認：IAL2 規準の策定
  - “IAL2の新学認での運用に当たって（案） Version 2”
  - 多くの大学等で達成が可能 -- Trusted DBの運用を前提
  - 組織外の研究者を受け入れる研究機関でも対応可能
    - eKYC 対応
- 当人確認：AAL2 規準の策定
  - “AAL2の新学認での運用に当たって（案）”
- https://meatwiki.nii.ac.jp/confluence/x/OZhyBQ

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)

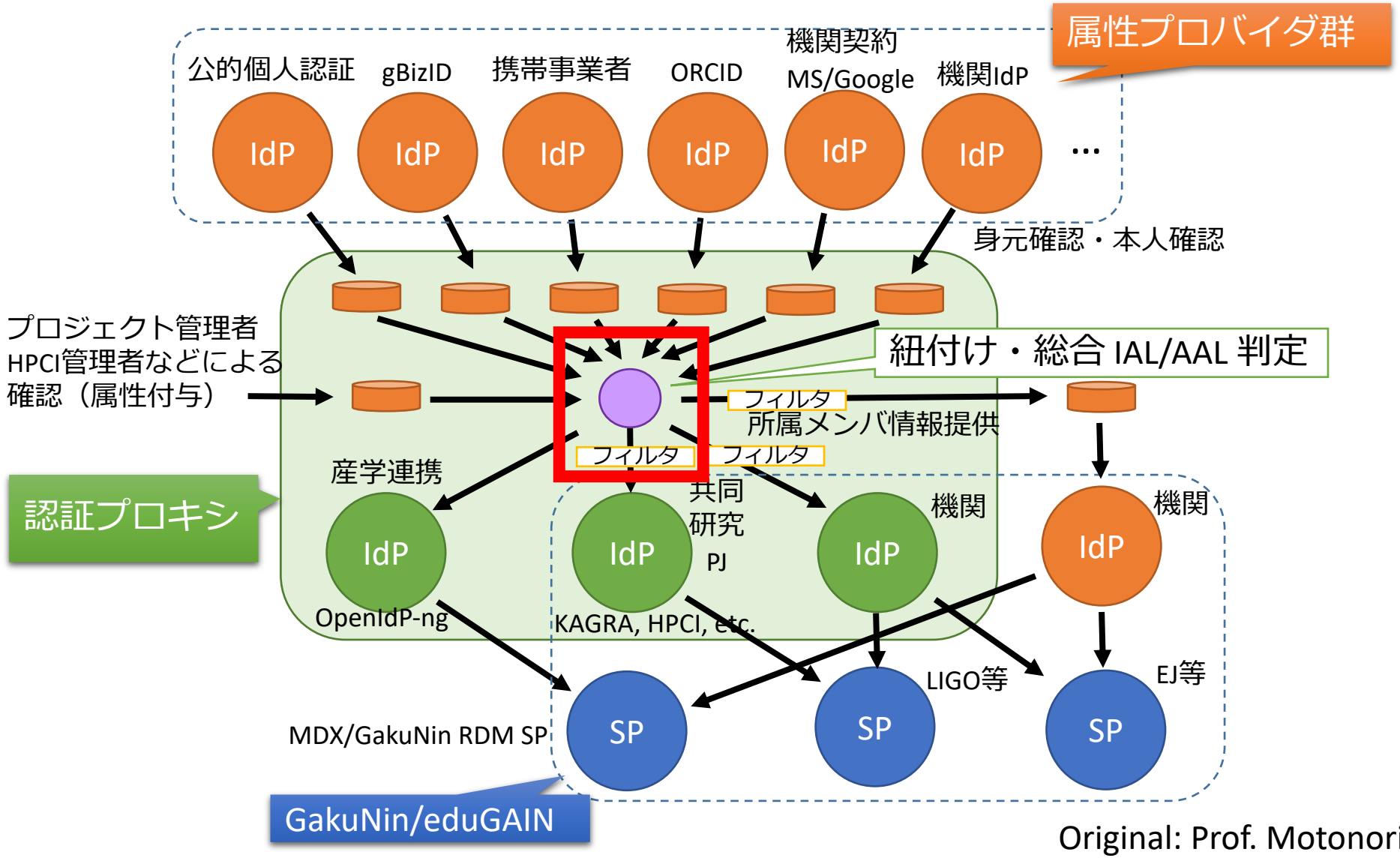
- 既存の研究コミュニティのもつトラストフレームワークにおいて、Id 基盤部分を外だしできるようにする
  - 本人確認手続きを外部に依拠できる

- 認証プロキシサービス “Orthros”



Orthros

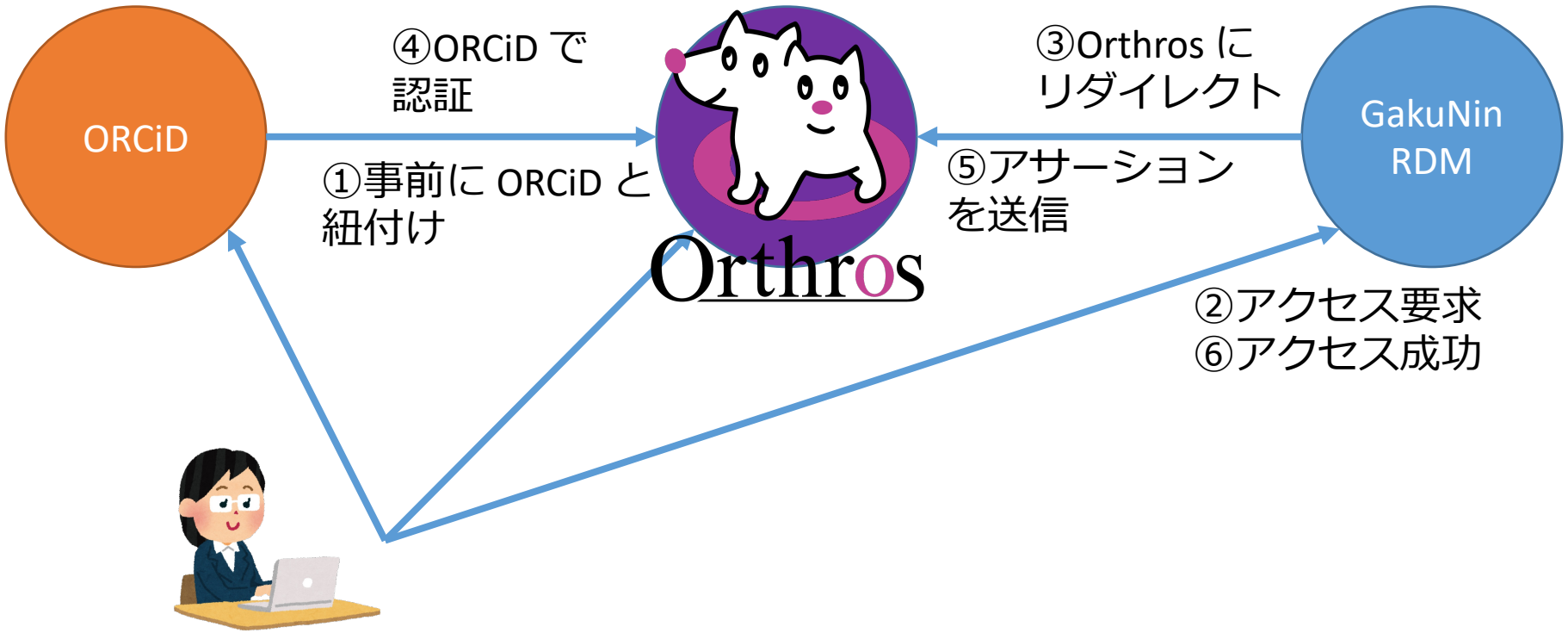
認証プロキシのデザイン



Original: Prof. Motonori Nakamura

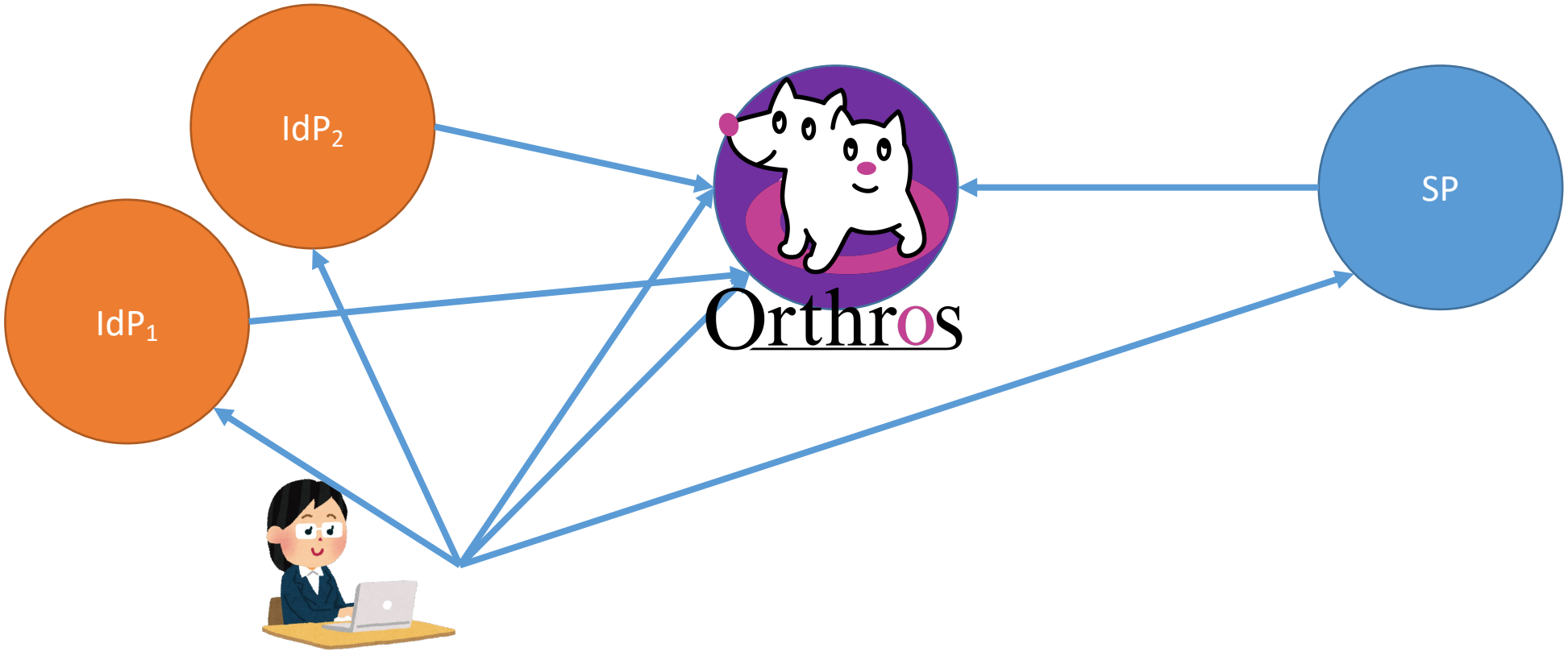
ユースケース１ – credential bridging

- 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

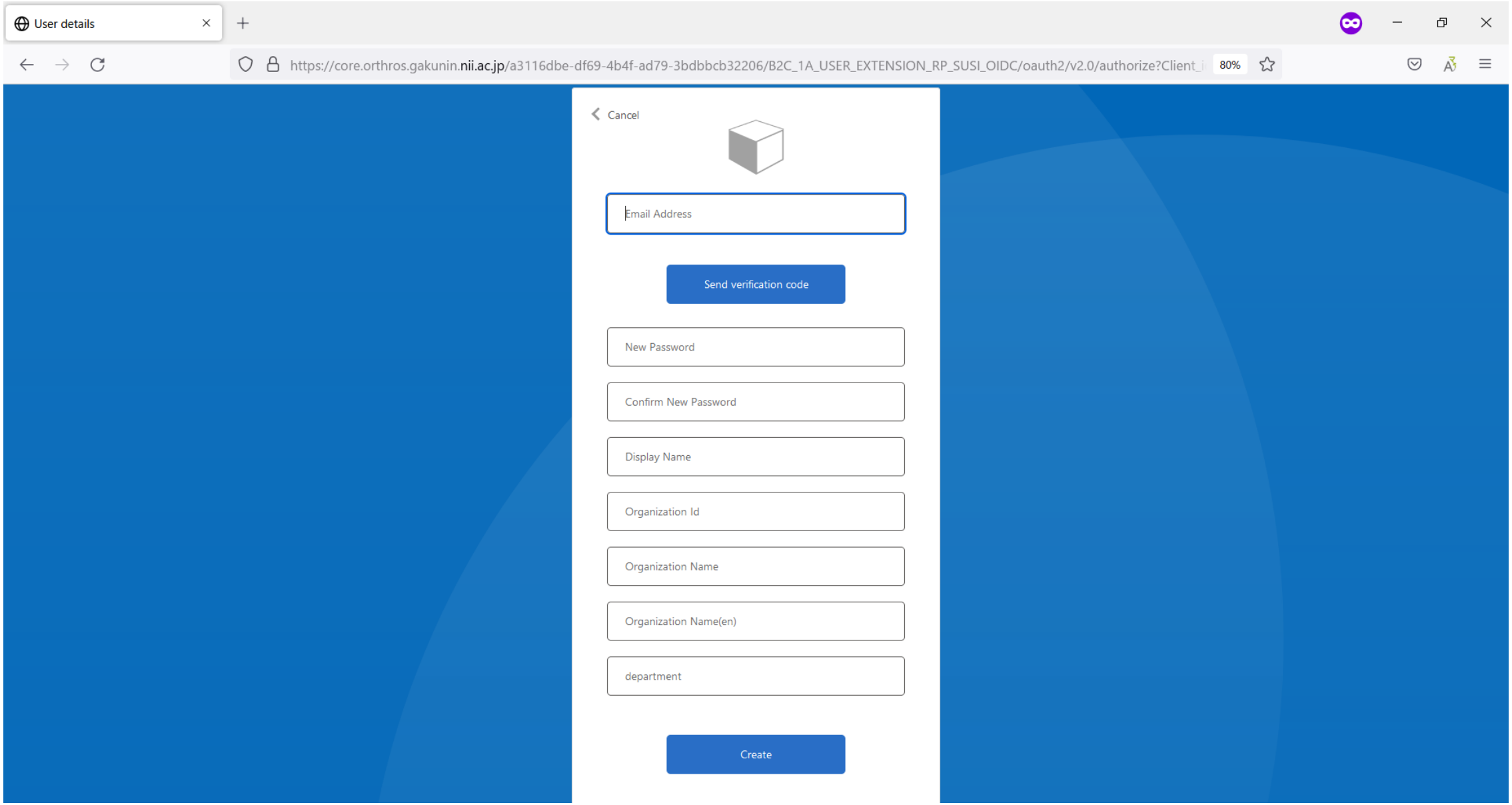
- 外部IdPの追加
  - 接続済み：LINE, Google, Yahoo! JAPAN, Facebook, Twitter
  - 調整中：gBizID, ORCiD

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

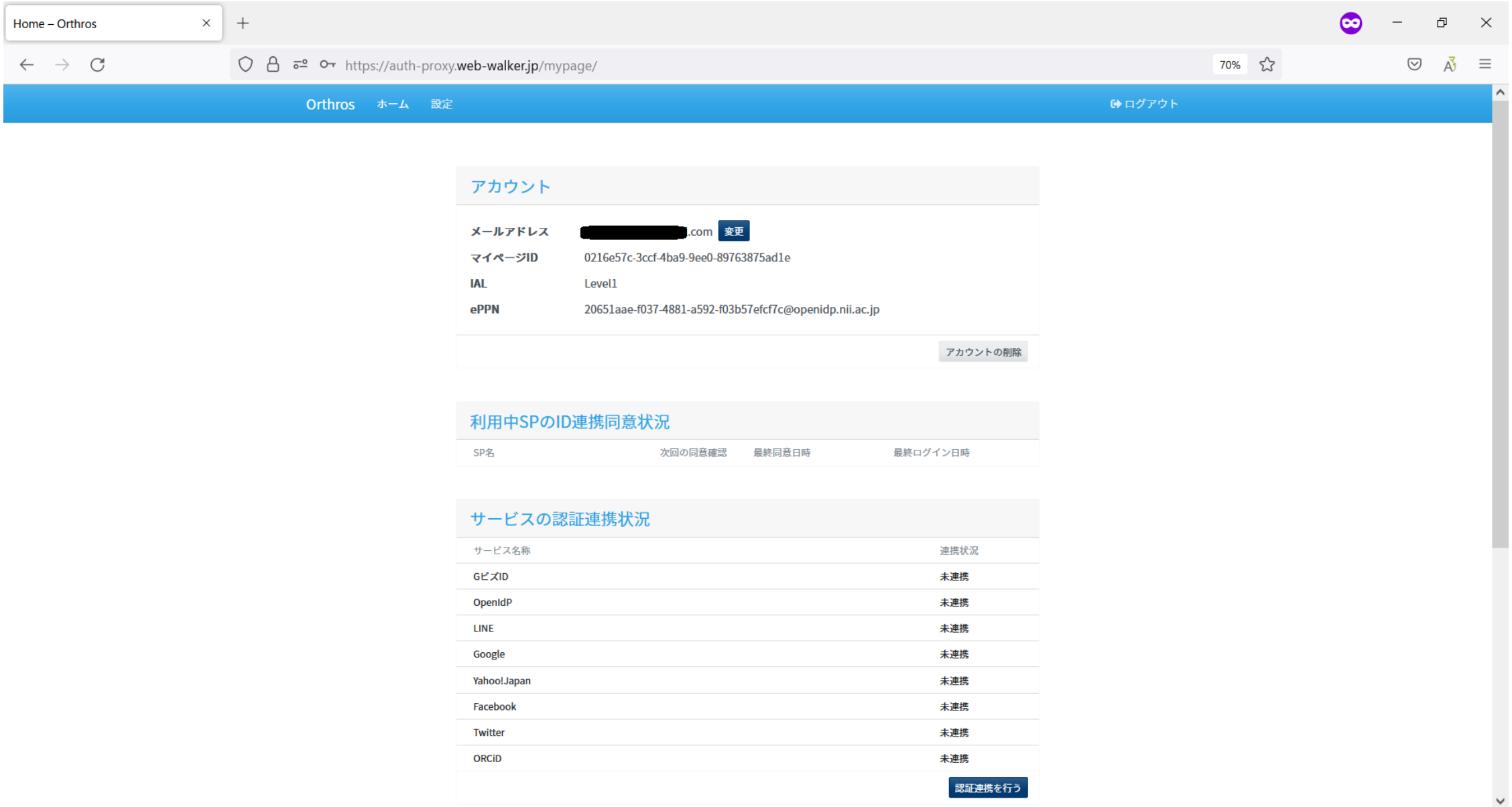
新規登録 (1/4)


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

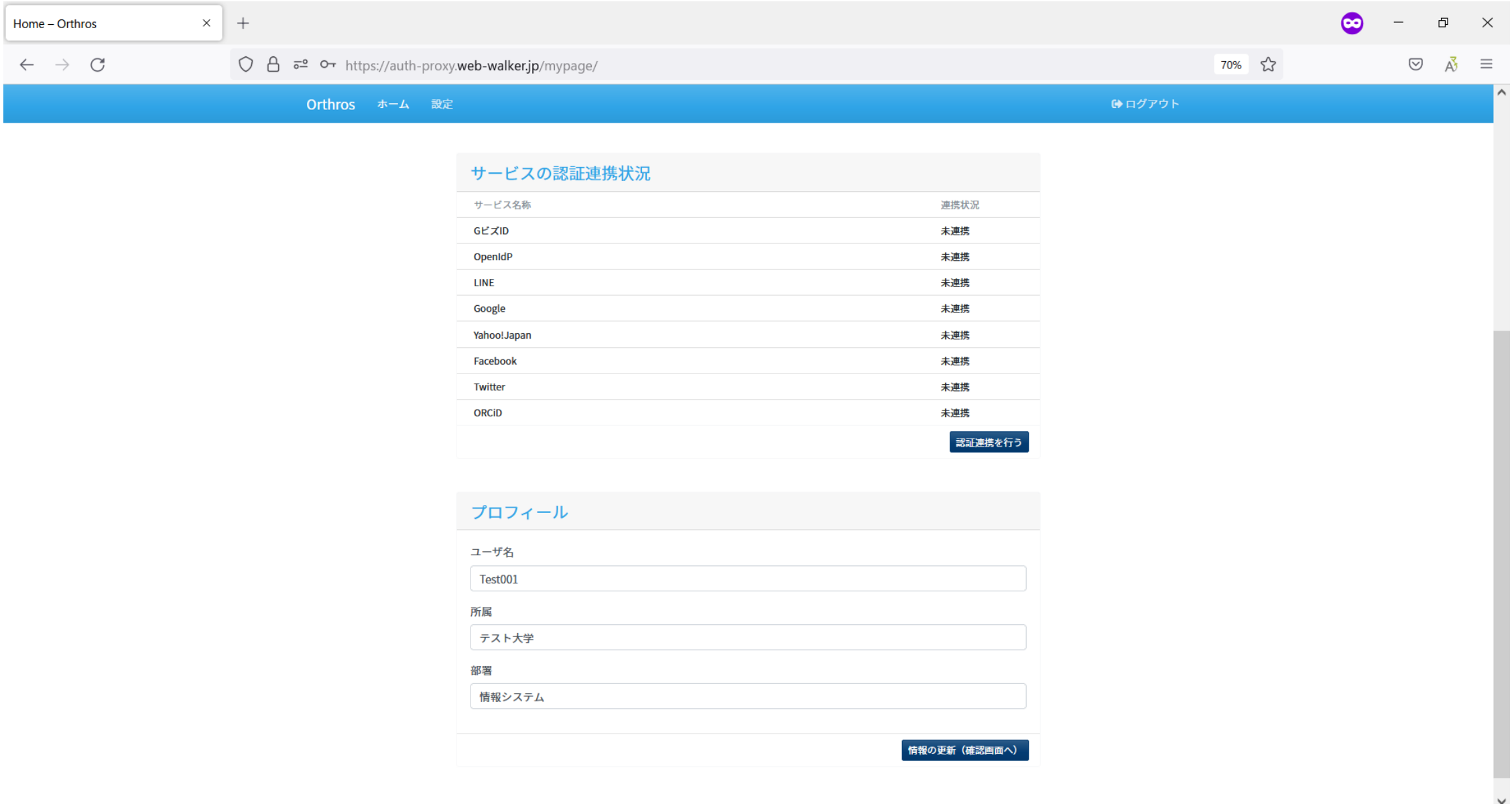
新規登録 (2/4)


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

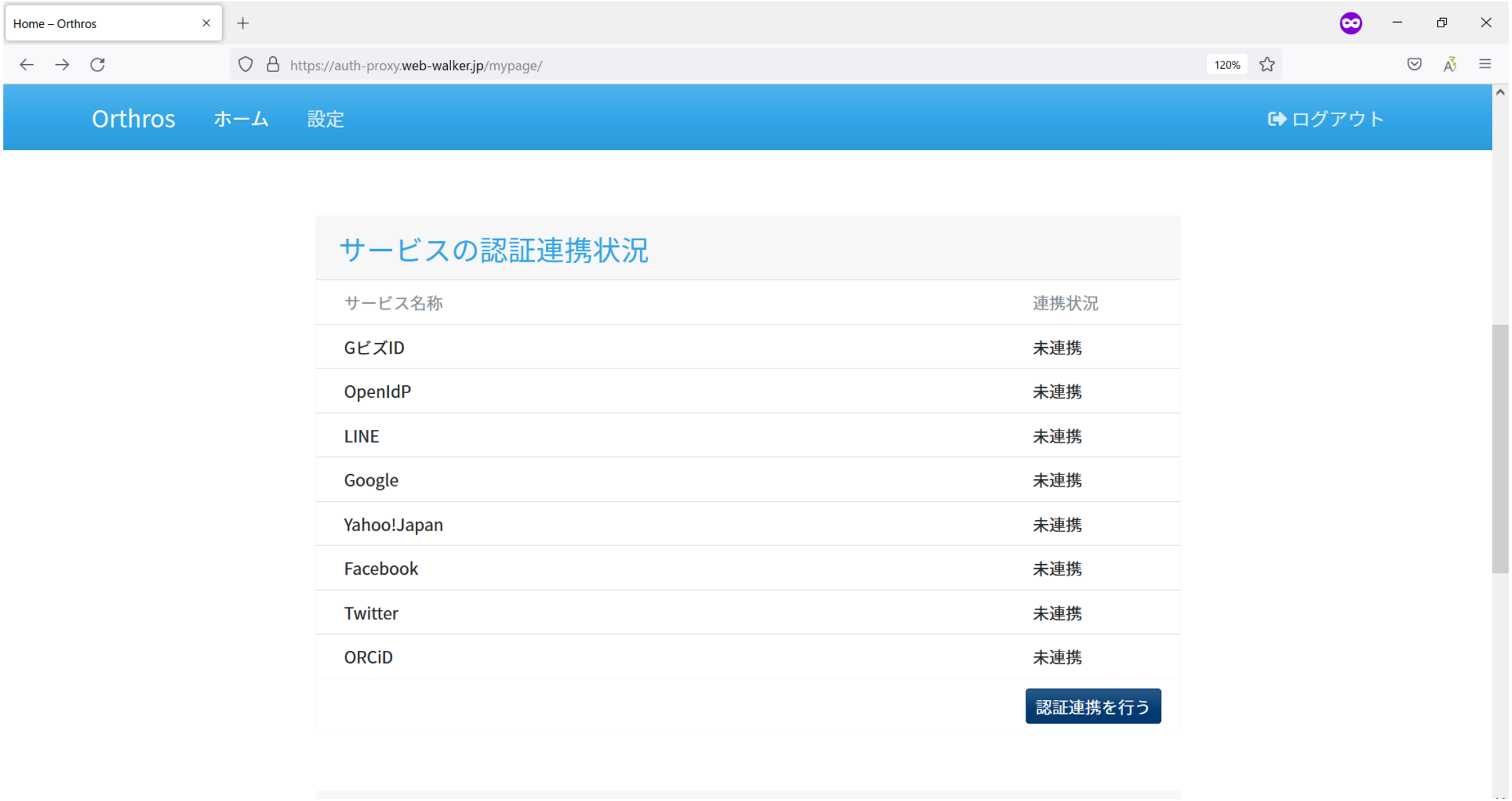
新規登録 (3/4)


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

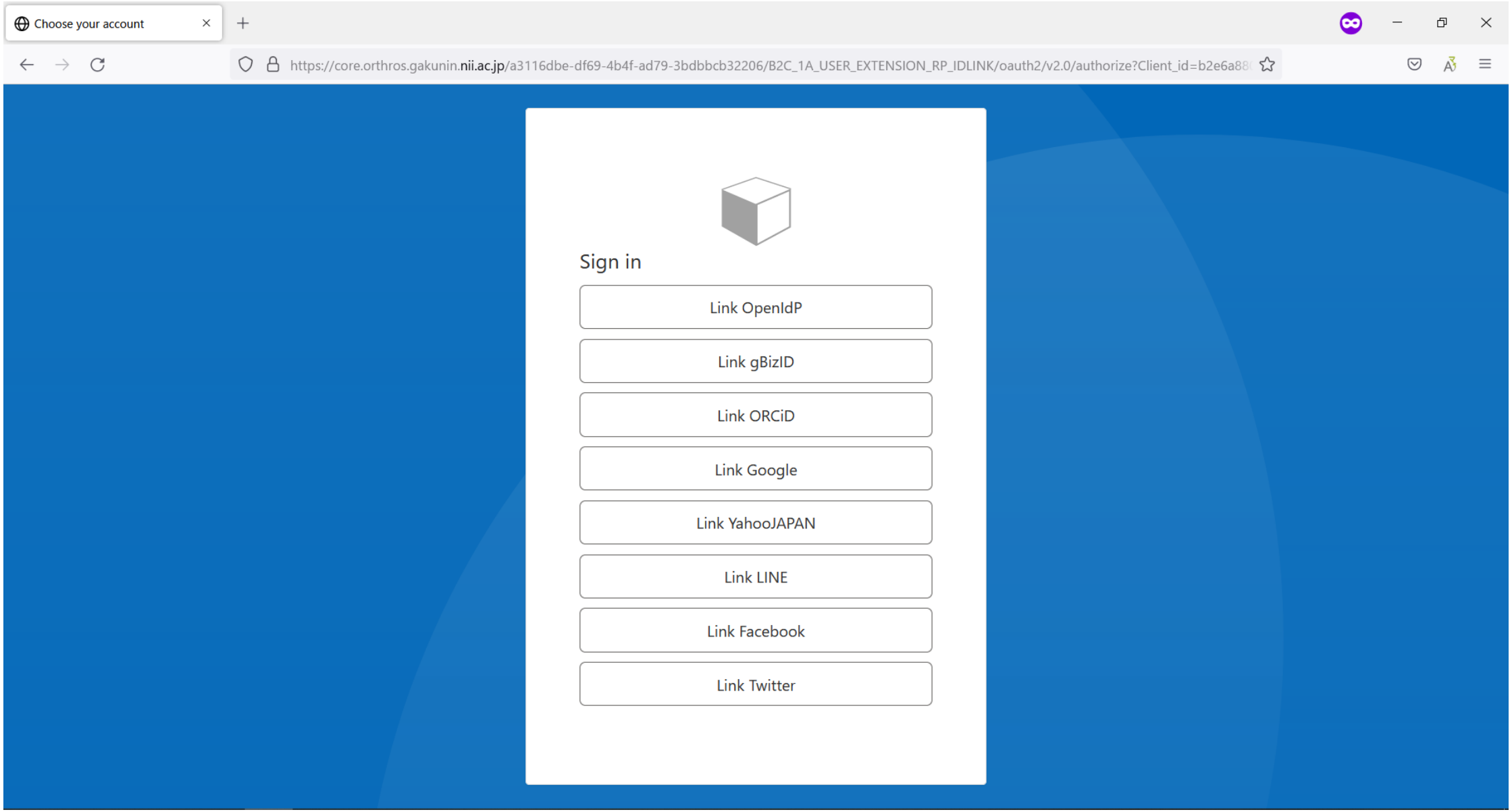
新規登録 (4/4)


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）

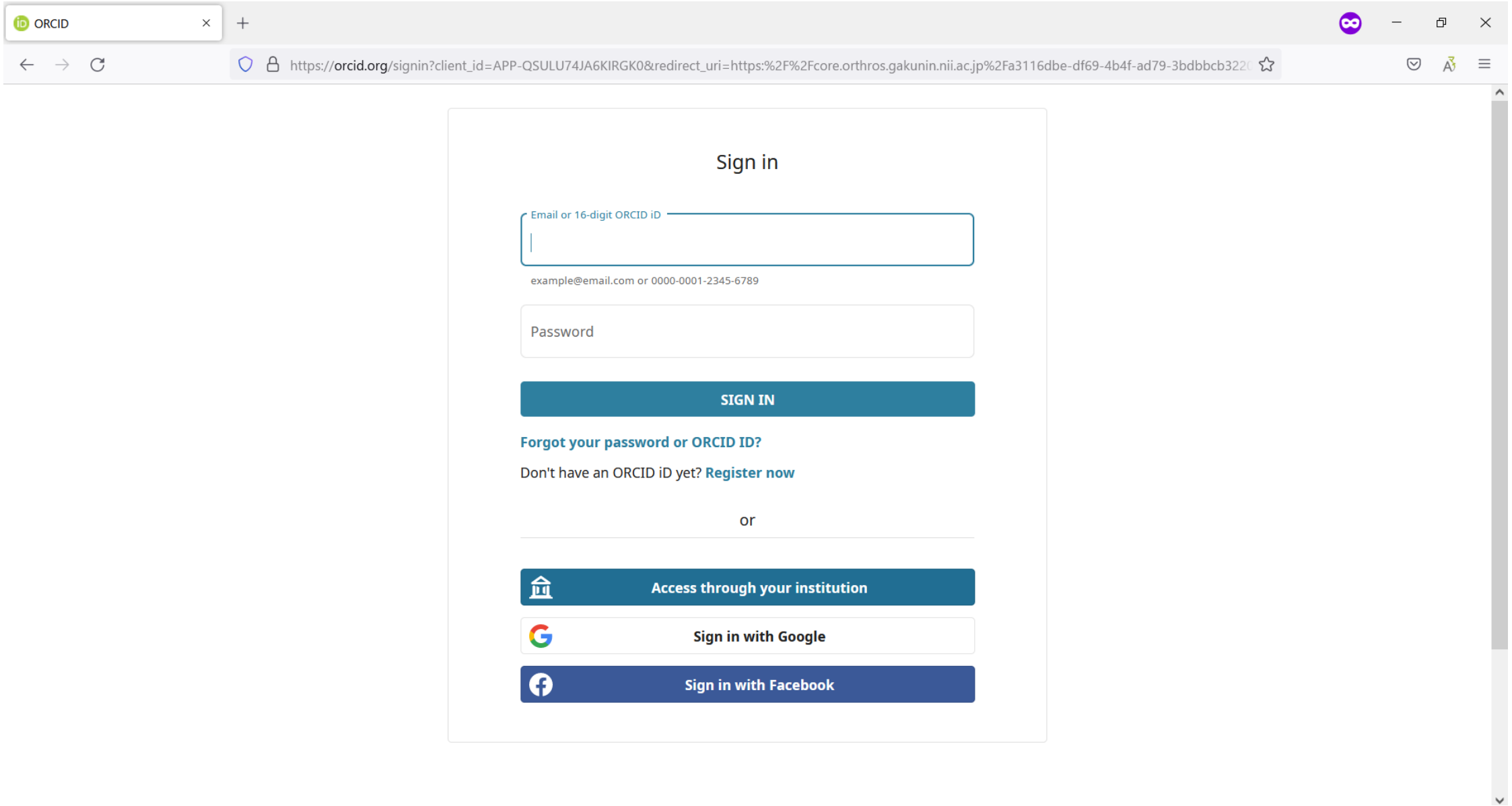
外部ID連携 (1/4)


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

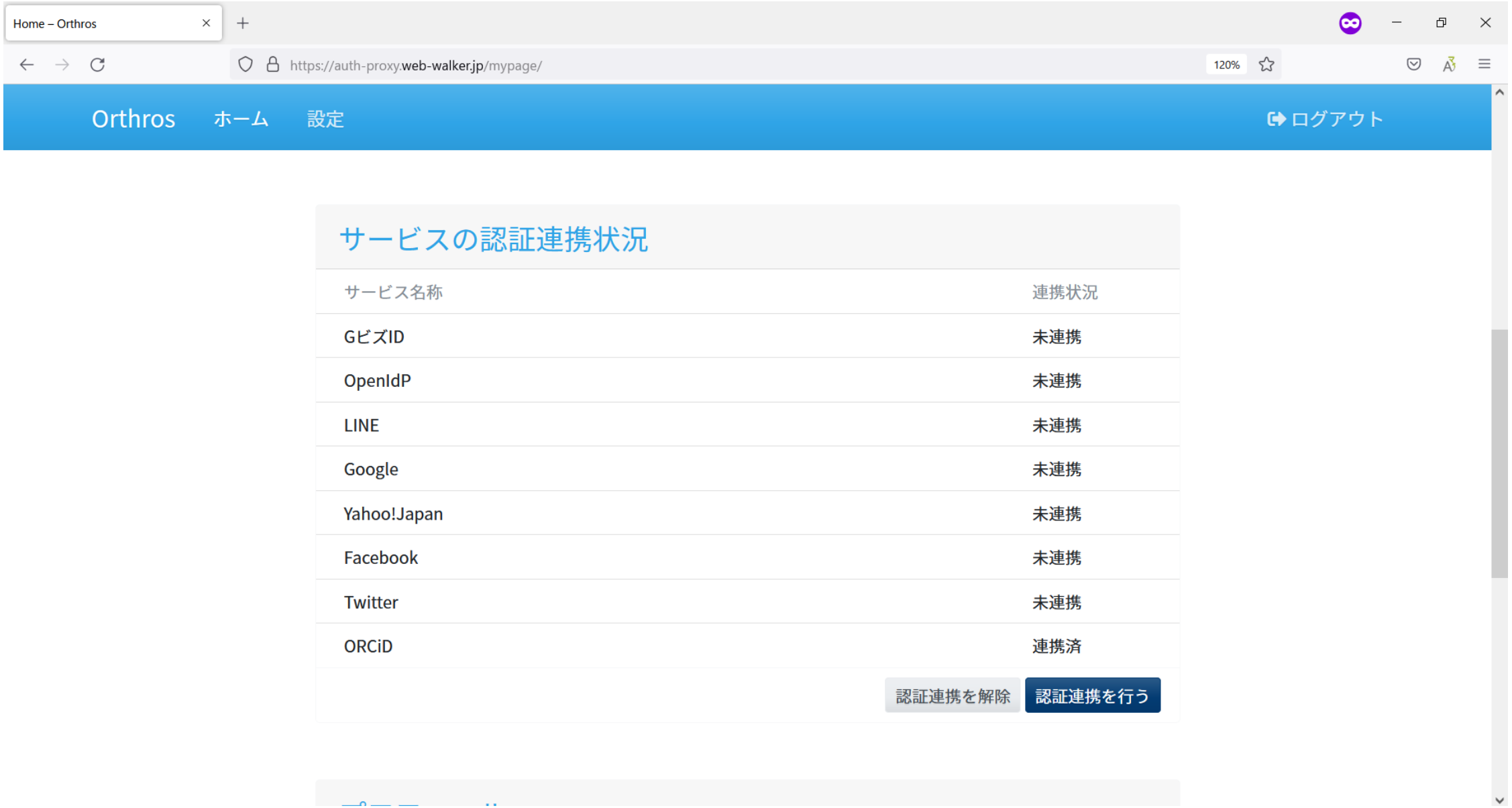
外部ID連携 (2/4)


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

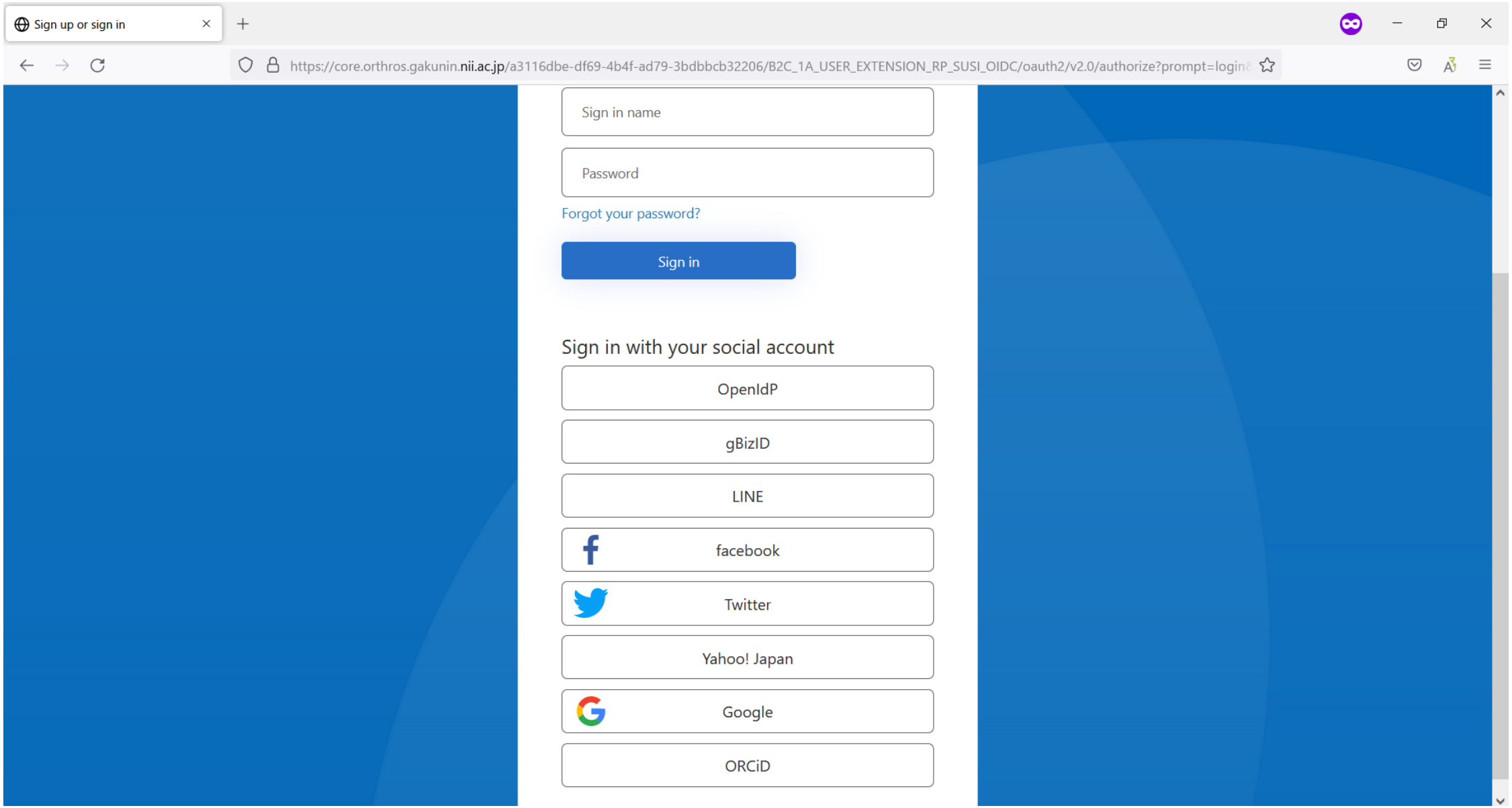
外部ID連携 (4/4)


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

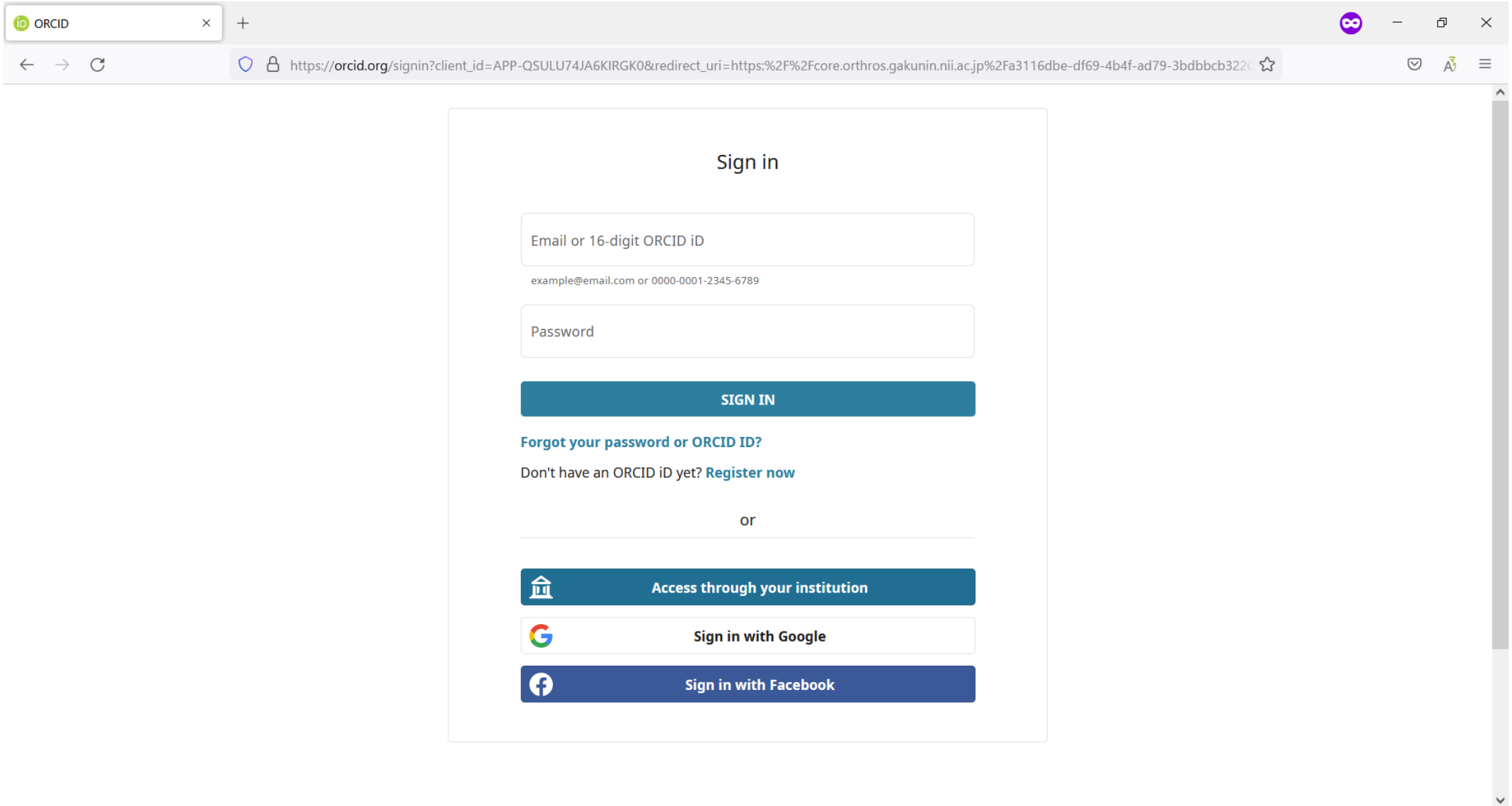
ログイン (1/4)


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

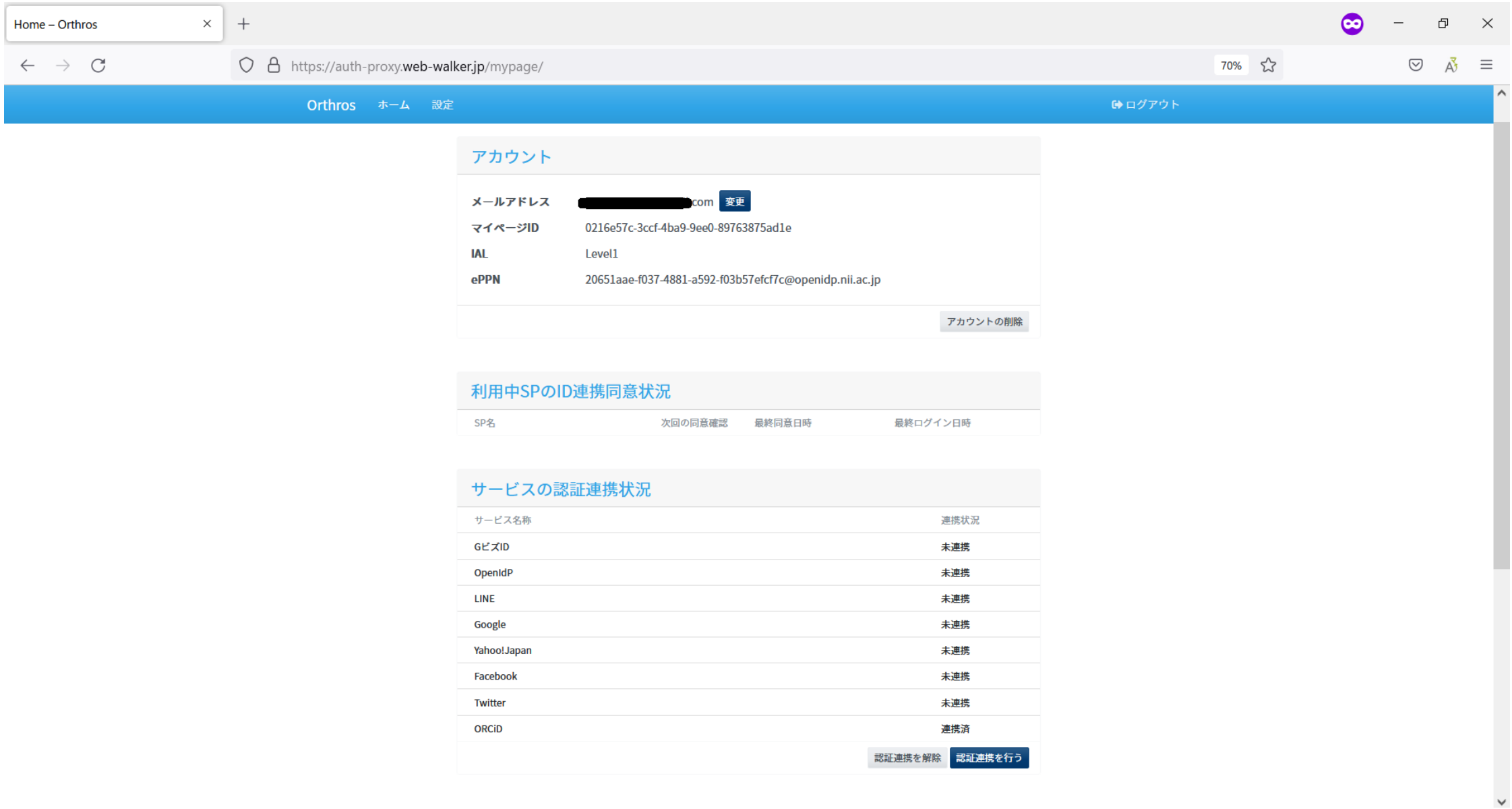
ログイン (2/4)


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：Q3-Q4

- Orthros 本格運用に向けて
  - OpenIdP 移行環境としての機能整理、基盤整備
  - OpenIdP からのユーザ移行準備・支援
  - 本格運用に向けた体制・手順整備
    - 運用ポリシ・運用規程策定

- FY2023 以降
- Orthros 拡張機能開発 – 次世代認証連携対応
  - 外部IdP（GビズID、ORCID）連携
  - SP単位の送出属性選択
  - 異動に伴うHome IdP Binding
  - 新学認IAL/AALポリシー対応
  - 認可属性の取り扱い強化

学認対応 IdP ホスティングサービス

- 学認の参加機関は **277** 機関（2022年10月末時点）
- 未参加機関の理由
  1. 人員的な問題（運用する人材、参加検討する人材の不足）（58件）
  2. 技術的な問題（サーバの構築や運用ができないなど）（23件）
  3. 金銭的な問題（20件）
  4. 必要かどうかわからない（11件）
  5. 委託業者が分からない（9件）
  6. 現在は不要である（5件）

- 学認が目指す将来像：全国の大学・研究機関のすべてが学認に参加すること
  - 研究者・学生の基本的な ID 基盤

- 運用形態の多様化に対応、運用効率化の研究開発
  - 学認対応 IdP ホスティングサービスを検討中

学認対応 IdP ホスティングサービス（続き）

- IdP サーバの構築・運用が困難な機関に対して、NII が IdP サーバを構築して貸出すサービス
  - 24時間365日監視、随時セキュリティパッチ更新、ハード/ソフトウェアのバージョンアップ対応、FIDO2の対応、導入支援（学認参加手続き、SP 連携など）などを想定

- 利用メリット
  - IdP サーバの構築が不要で、コスト削減に☆
    - ハード、ソフトウェアの購入および資産計上が不要に
  - 運用コストの削減に☆
    - IDaaS (認証基盤のSaaS) として 24/365 サービス監視、脆弱性対応
    - ソフトウェアのバージョンアップから解放
  - 高度な専門知識がなくても導入可能☆
    - 学認参加時の手続きや、SP連携などのサポートあり

- まもなく実証実験を開始（2023/3 から）

まとめ：次世代認証連携に向けて

- 学認 IAL/AAL 策定
- 認証器レジストリ
- 認証プロキシサービス Orthros
- 学認対応 IdP ホスティングサービス
- グループ管理機能の高度化