第15回統合認証シンポジウム

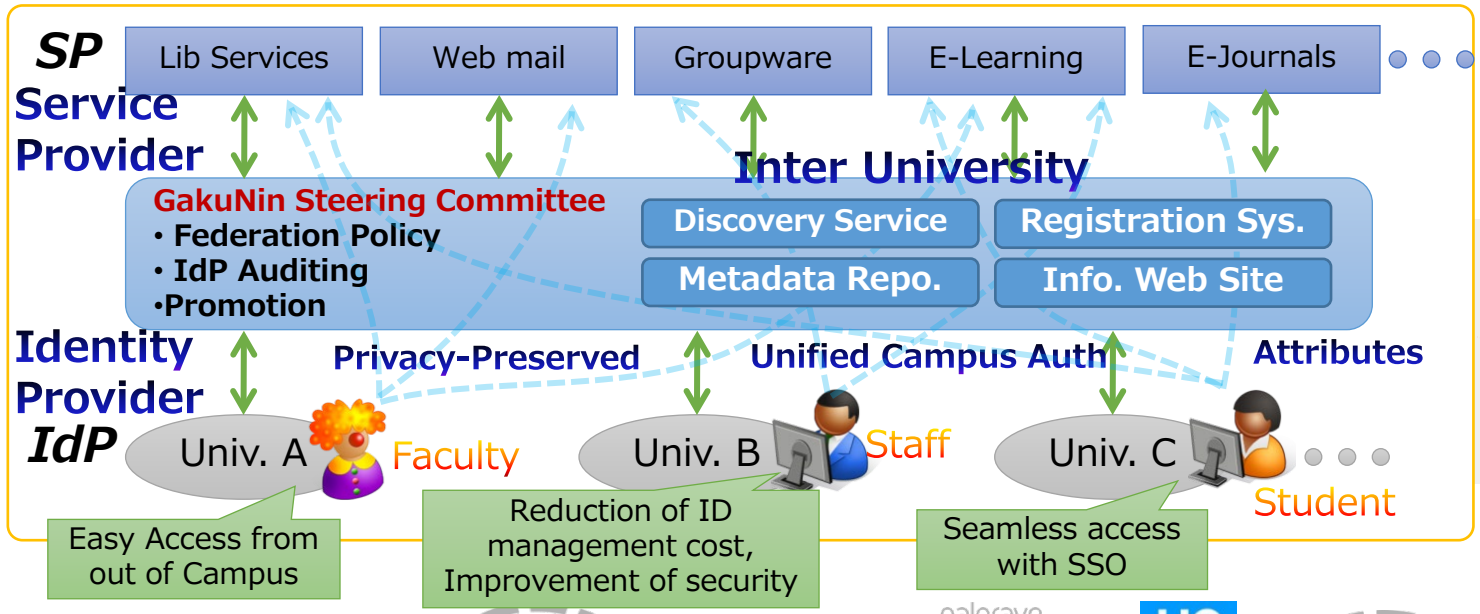
新学認におけるNIIの取り組み：Orthros × mAP Core

西村健

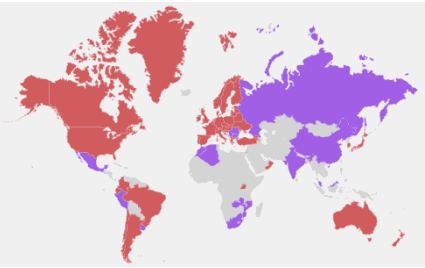
国立情報学研究所

学術認証フェデレーション「学認」

- 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



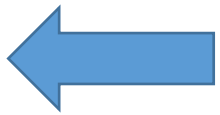
Academic Federations have been established per country basis



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

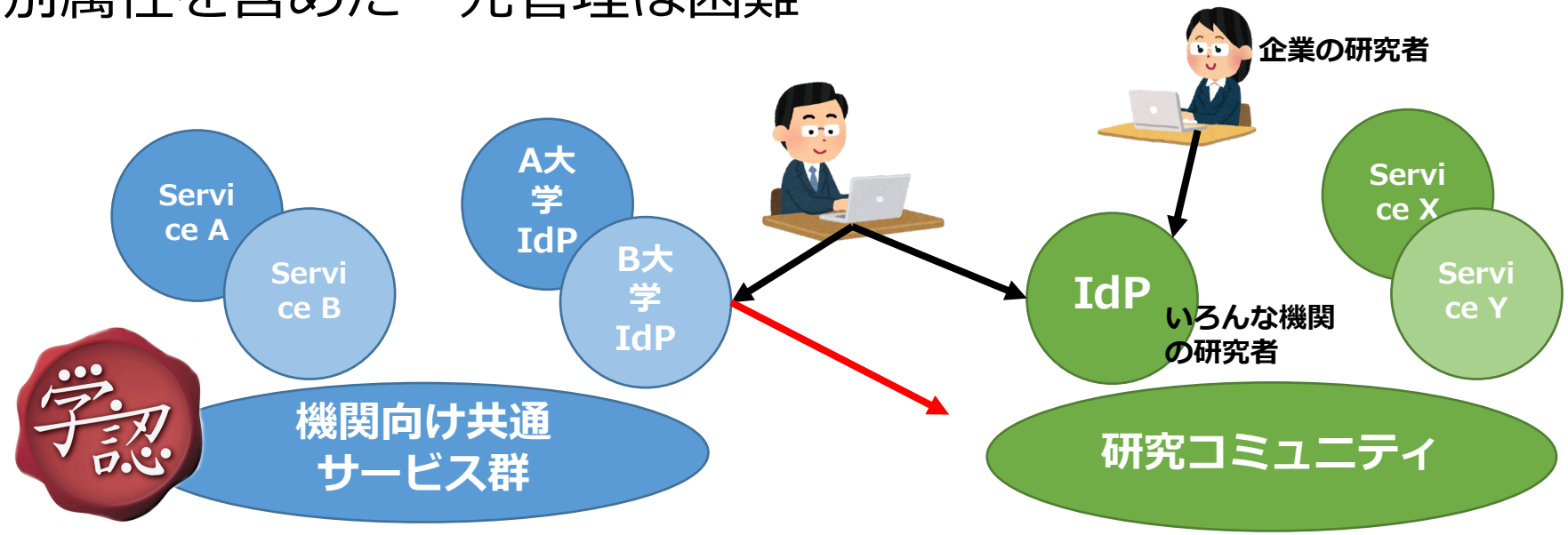
- データ流通において、認証認可は極めて重要
  - データを、誰が提供するのか
  - データに、誰が参照するのか



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

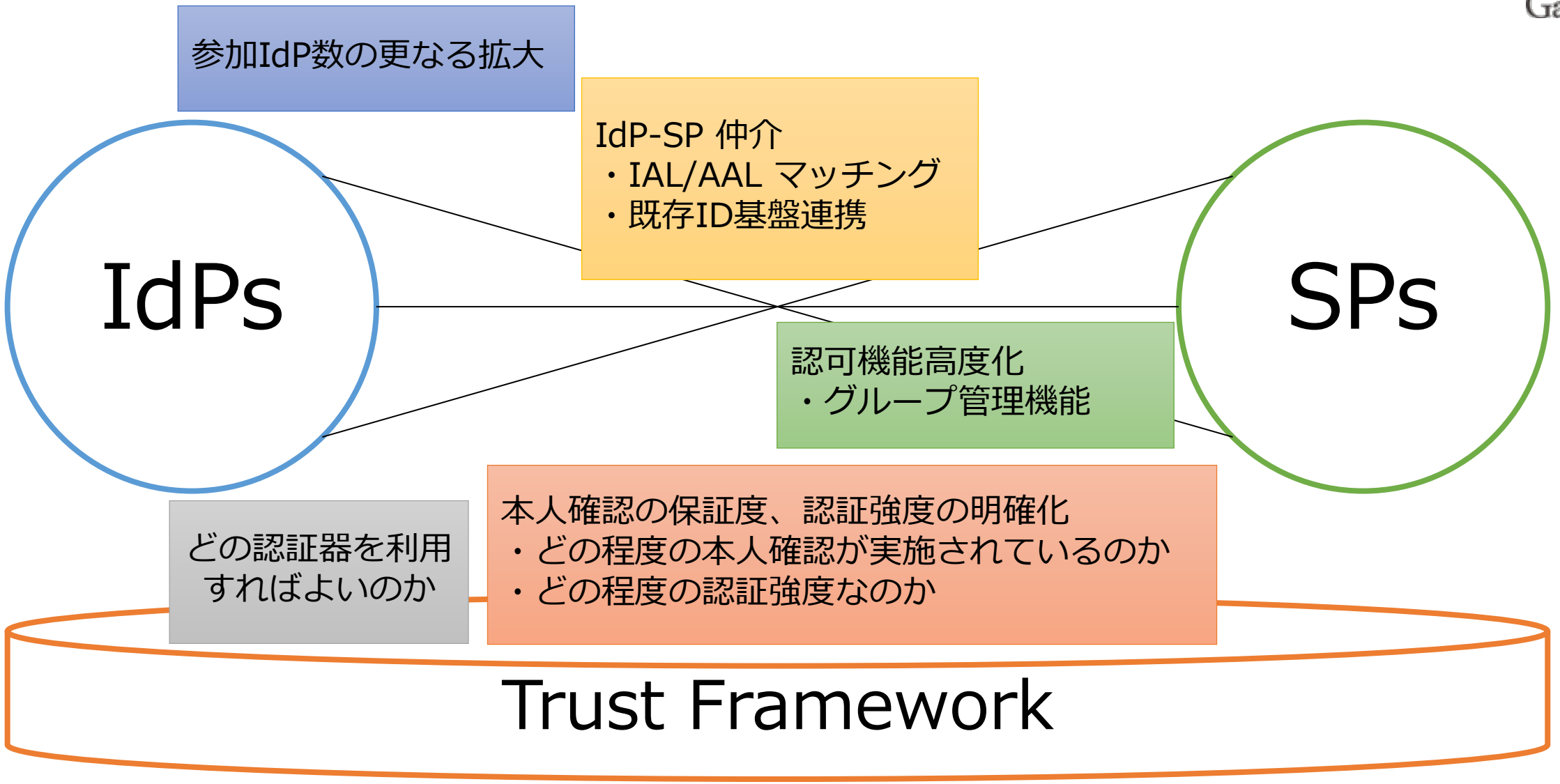
IdP 強化の取り組み

- 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

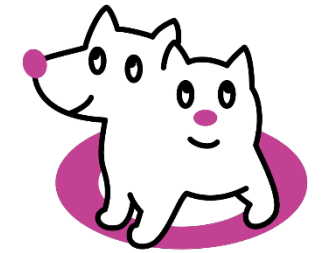
- より高度な認可要求に対応

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)

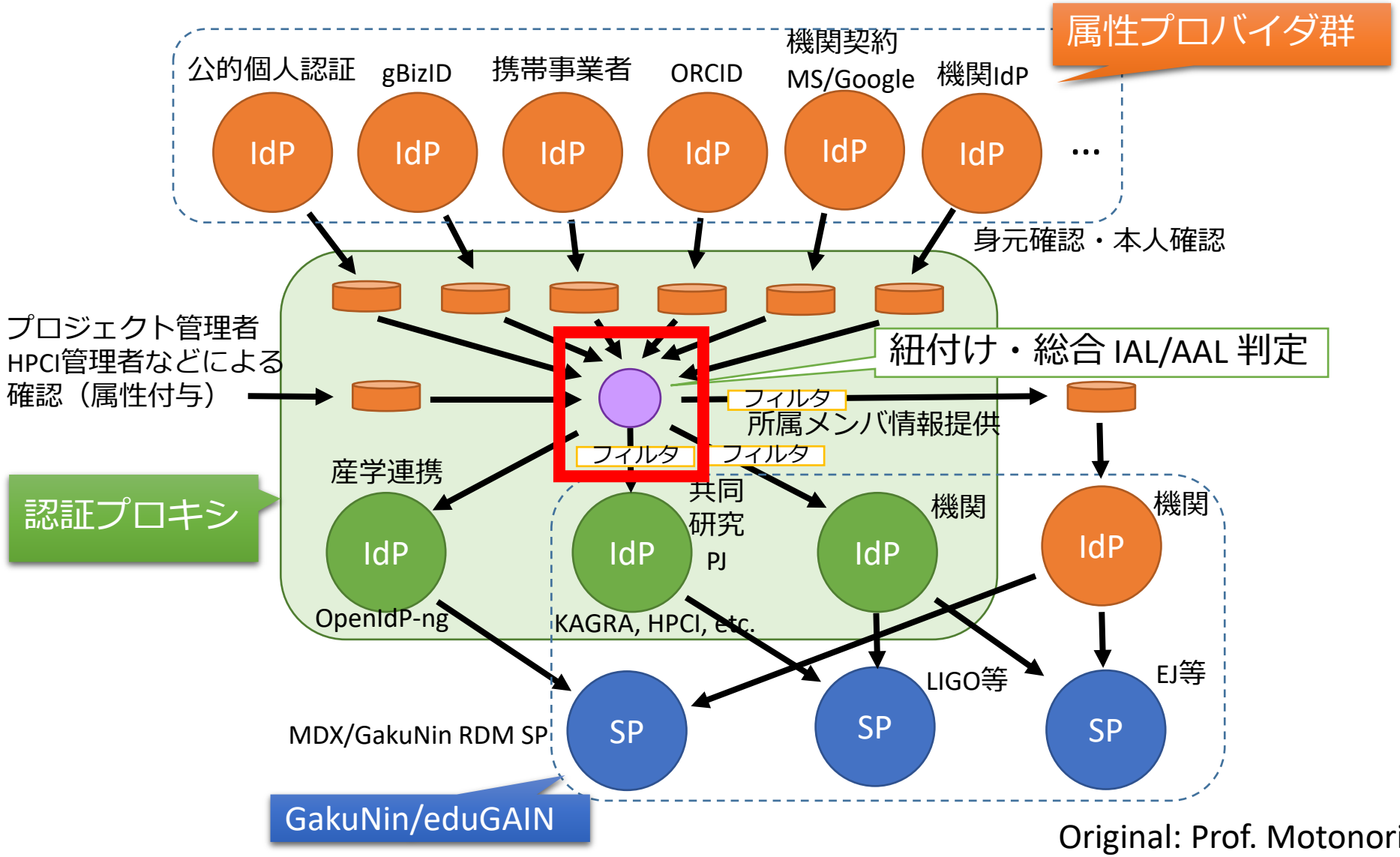
- 既存の研究コミュニティのもつトラストフレームワークにおいて、Id 基盤部分を外だしできるようにする
  - 本人確認手続きを外部に依拠できる

- 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

認証プロキシサービス Orthros の設計・実装

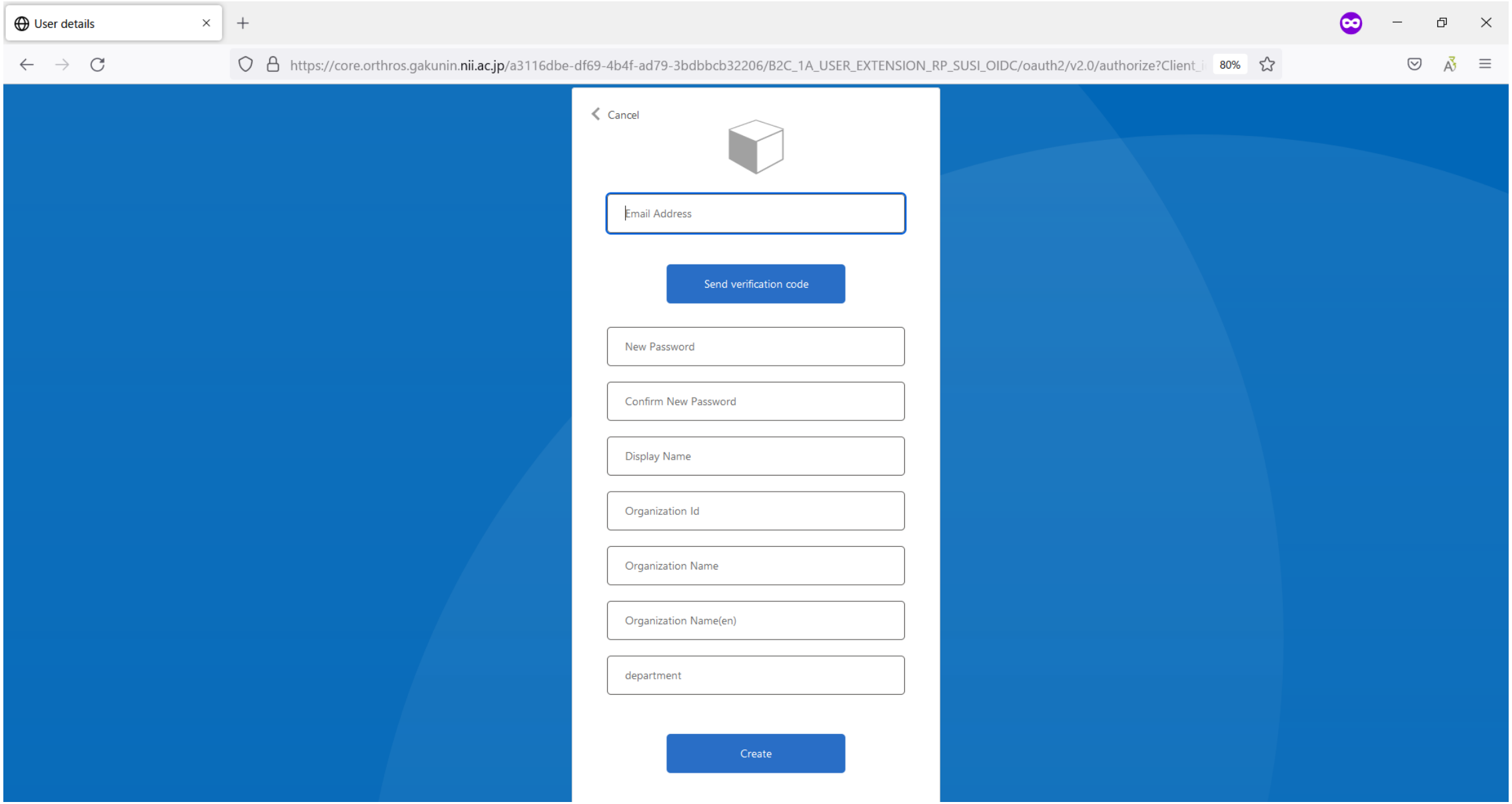
- 認証プロキシコア部 (IDaaS) – **SELMID** https://ctc-insight.com/selmid
- 各種機能設定インターフェイス部 (マイページ機能) – 内製

- 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
- その他
  - 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

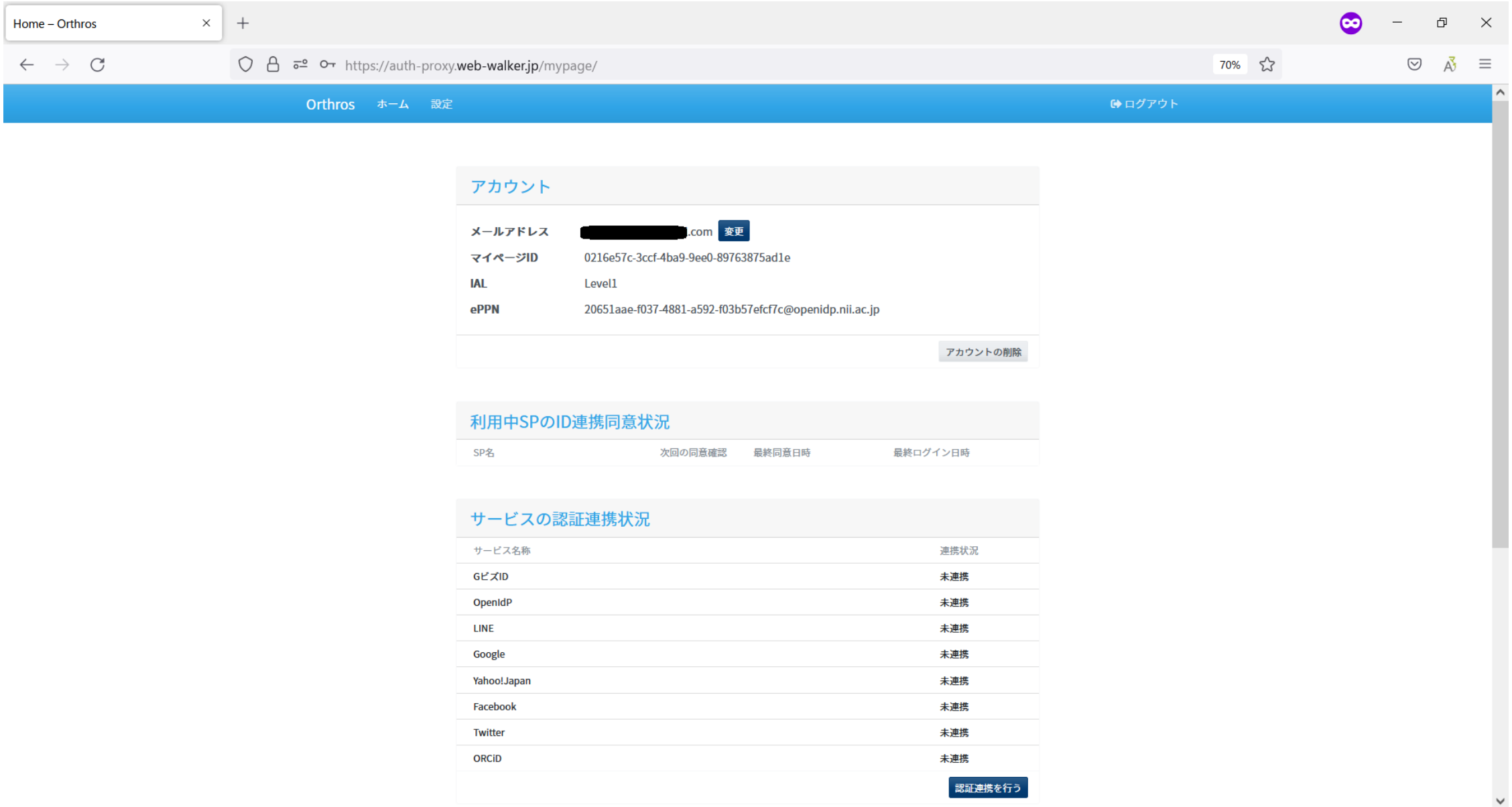
新規登録 (1/4)


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

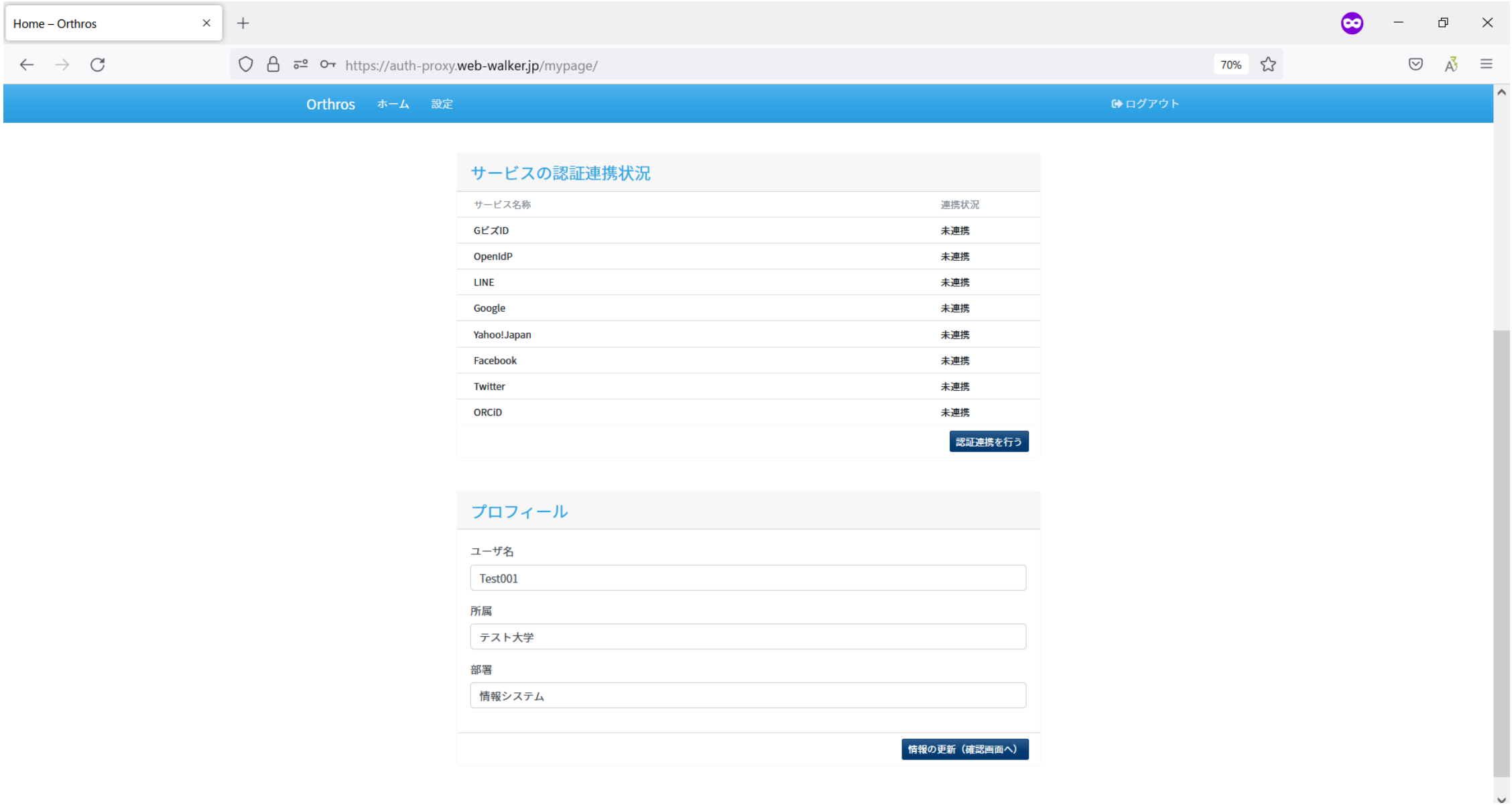
新規登録 (2/4)


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

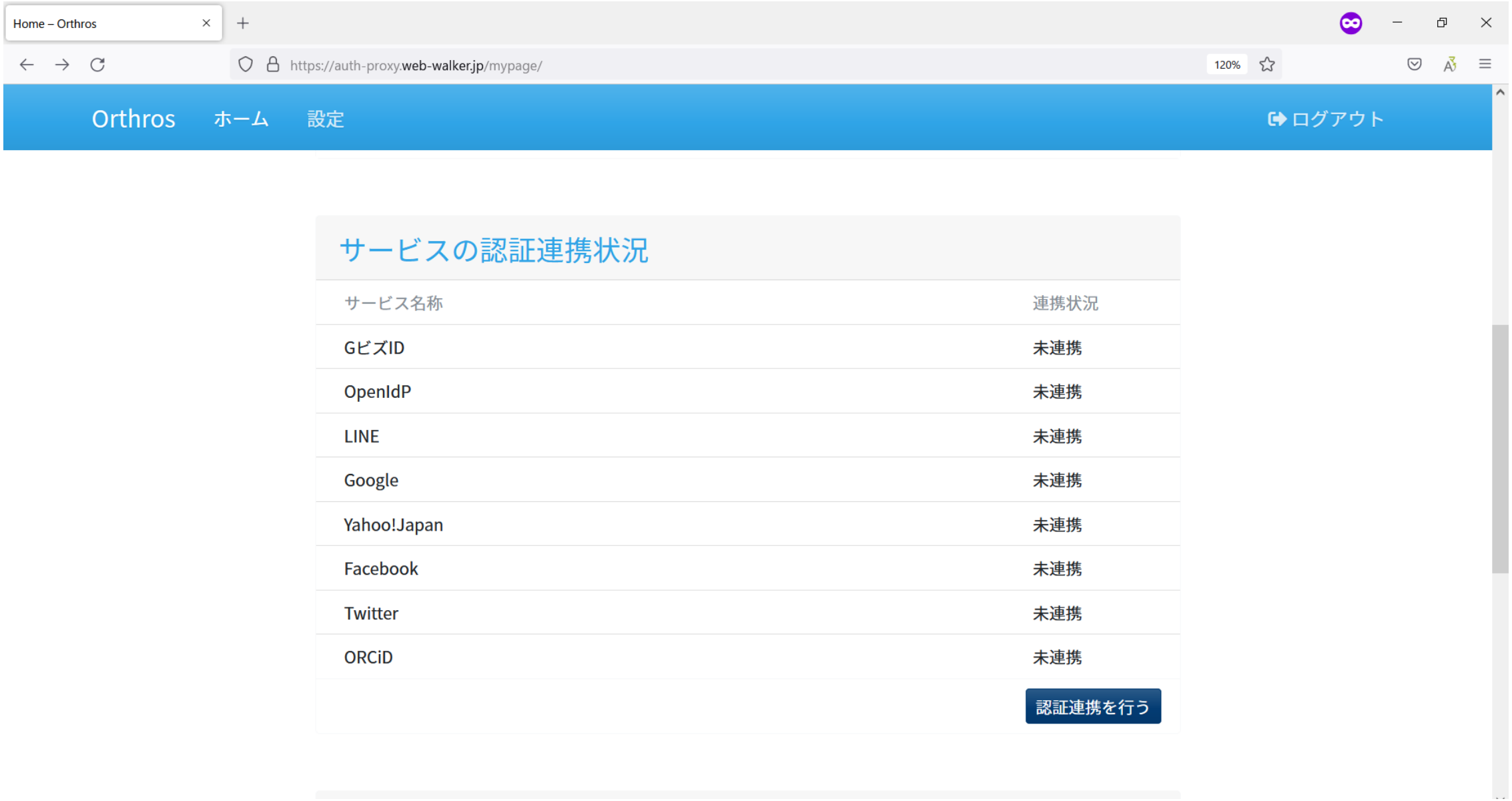
新規登録 (3/4)


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

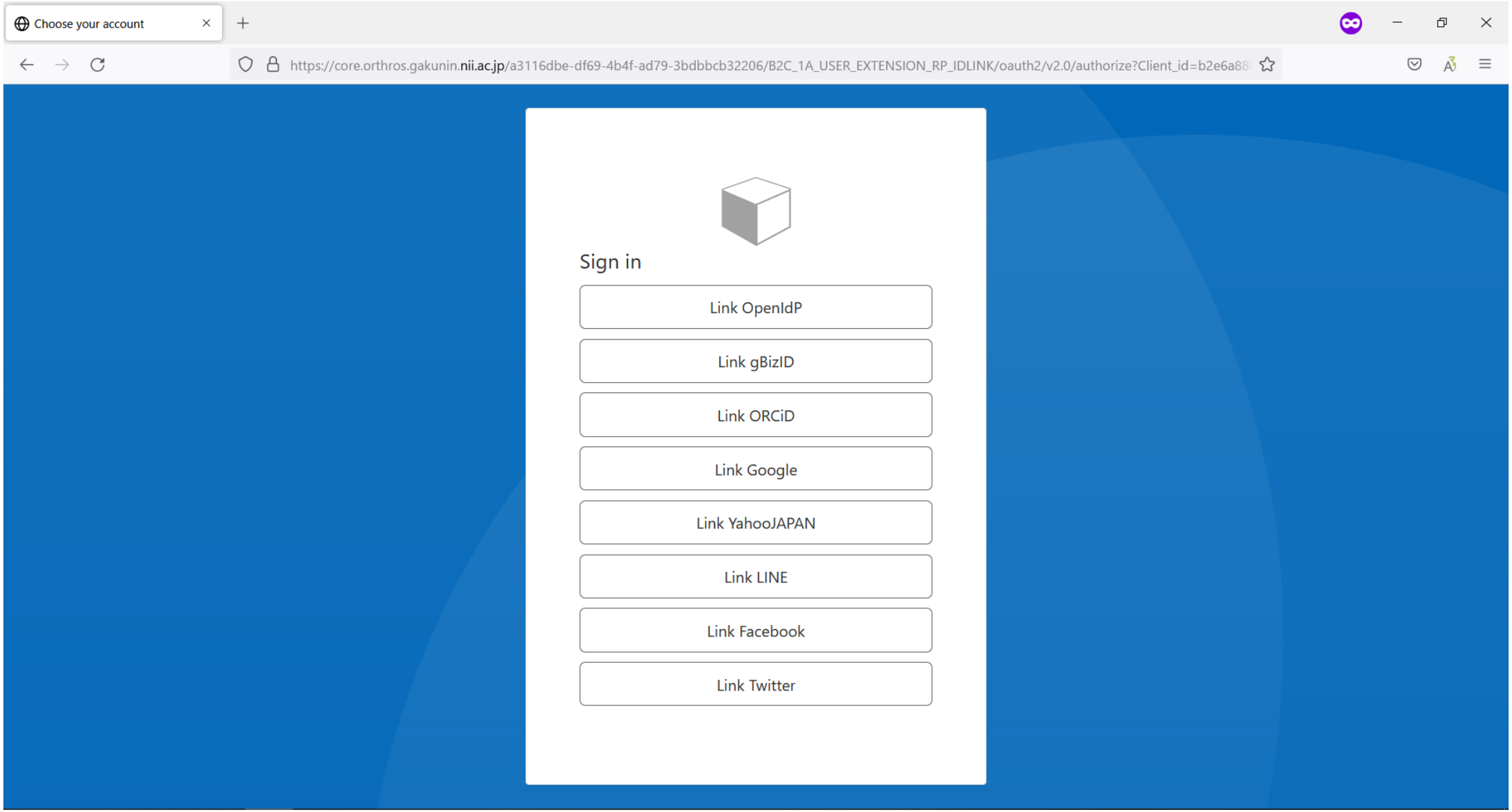
新規登録 (4/4)


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）

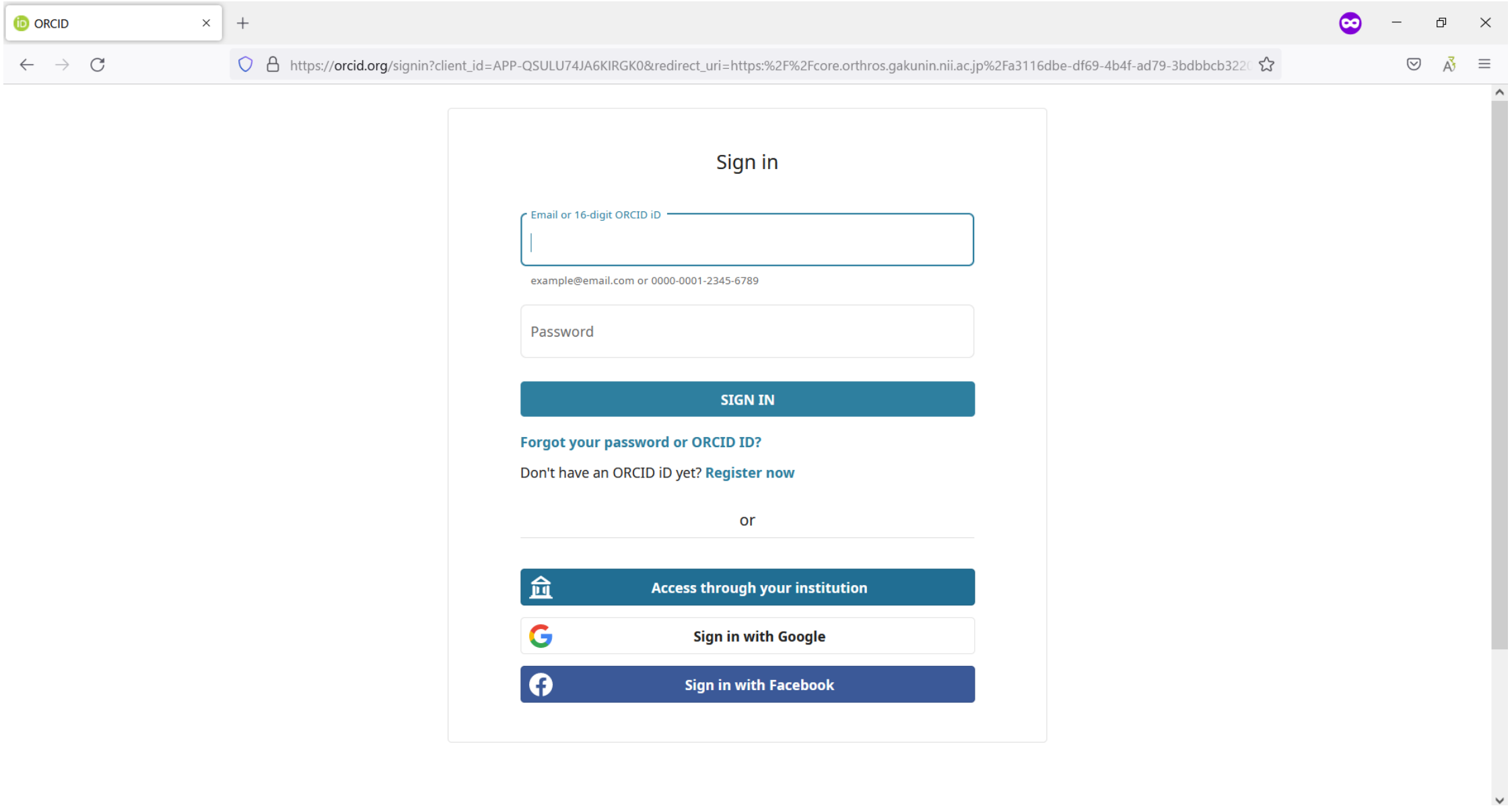
外部ID連携 (1/4)


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

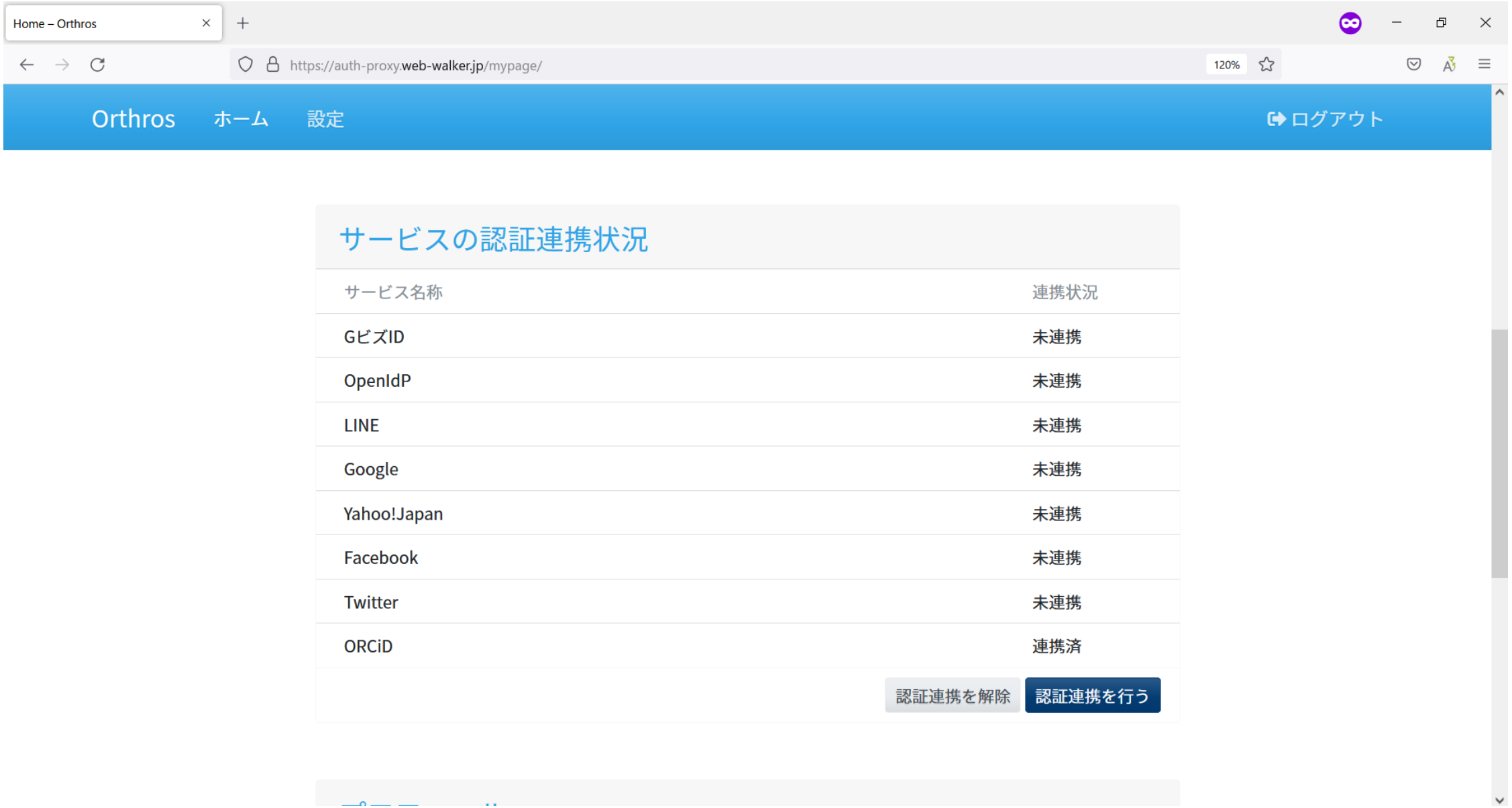
外部ID連携 (2/4)


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

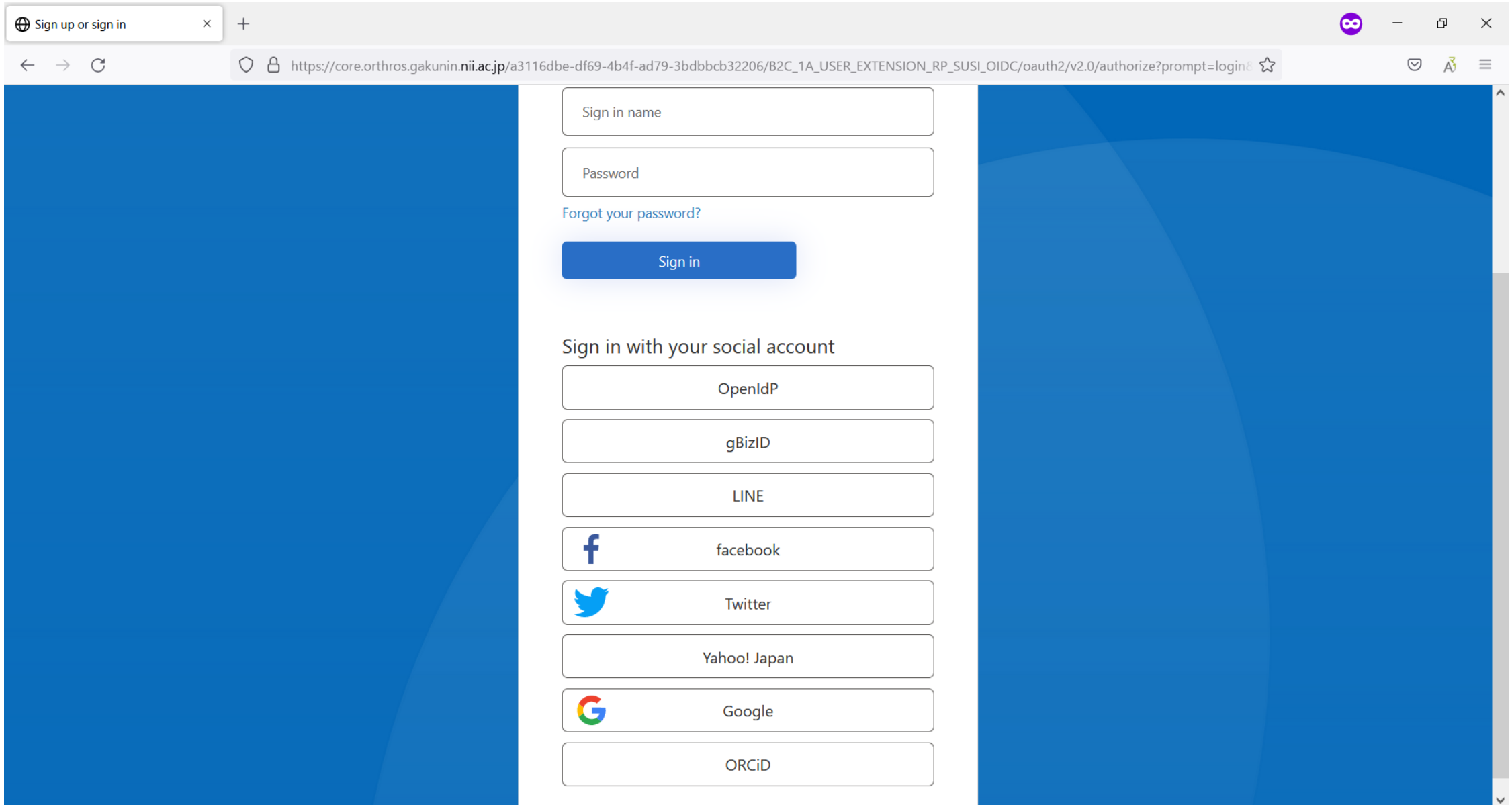
外部ID連携 (4/4)


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

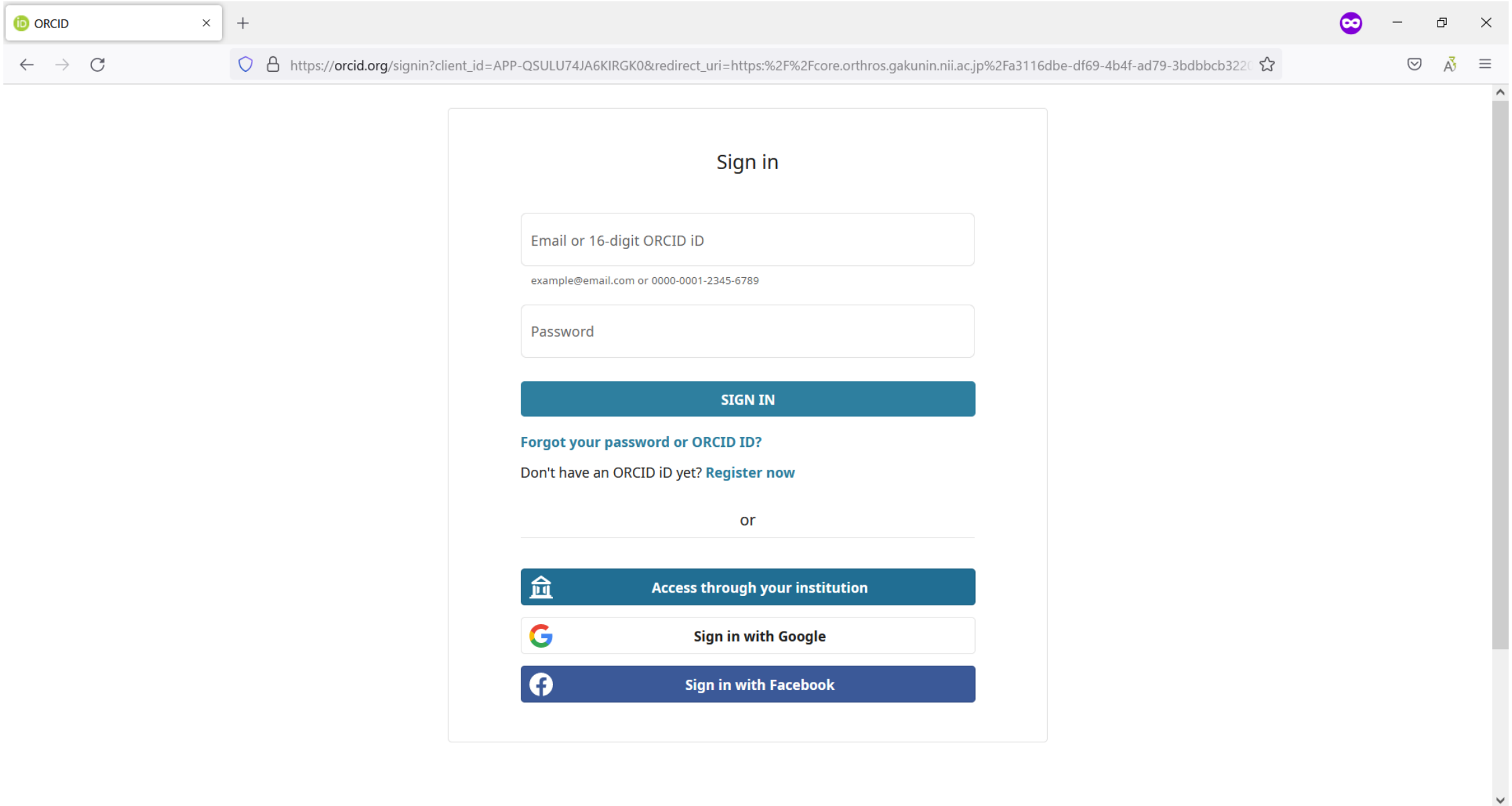
ログイン (1/4)


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

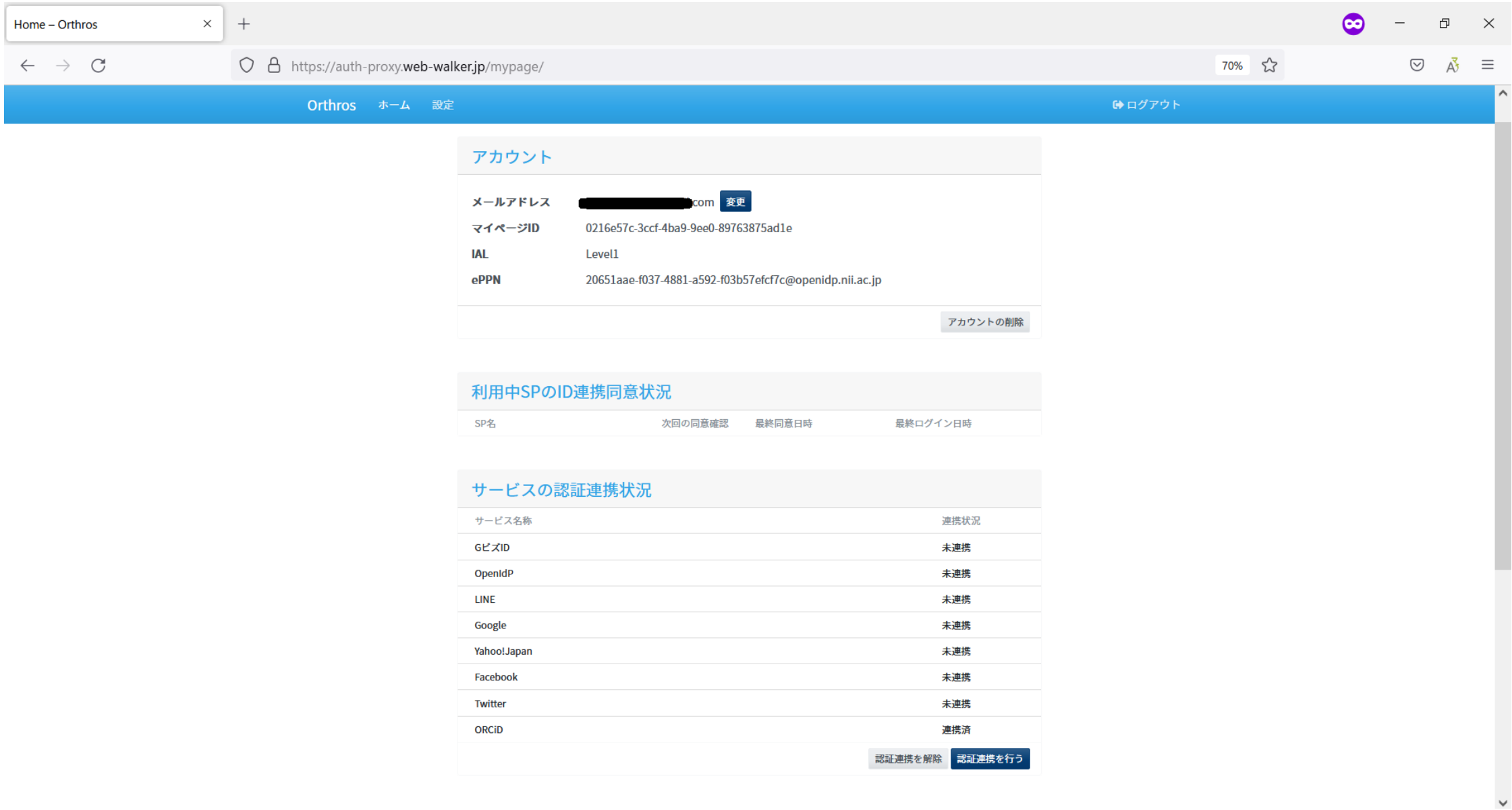
ログイン (2/4)


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

OpenIdPのOrthrosへの移行について

OpenIdP移行

- OpenIdPが提供している機能をOrthrosでも提供して、現行OpenIdPは提供終了としたい
- OpenIdP経由でログインして利用している学認申請システム等のSPに対して、Orthros経由でもログインできるようにする
- 現在、必要な機能の実装、移行手順の詳細を詰めている

移行準備

- Orthrosと現行OpenIdPを連携（認証プロキシ）させ、OpenIdPのID/PWでログインできるようにする
- OpenIdPのIDと紐づいたOrthrosアカウントについて、OpenIdPが送出するePPNをOrthros側で記憶し、Orthrosも同じePPNを送出するようにする
- 現在OpenIdPで連携しているSPと、Orthrosも連携する（同じ属性を当該SPに送出できるように設定しておく）

移行手順

- （利用者による完全手作業）

- 1. OpenIdPを利用していた利用者は、Orthros上にアカウントを作成する
- 2. 作成したアカウントとOpenIdPのIDを紐づけする

- これで、従来OpenIdP経由で利用していたSPがOrthros経由で利用できるようになる

おおまかなスケジュール

	2022Q4	2023Q1	2023Q2	2023Q3	2023Q4
Orthros構築	→				
移行期間		→	→	- - -	- - -

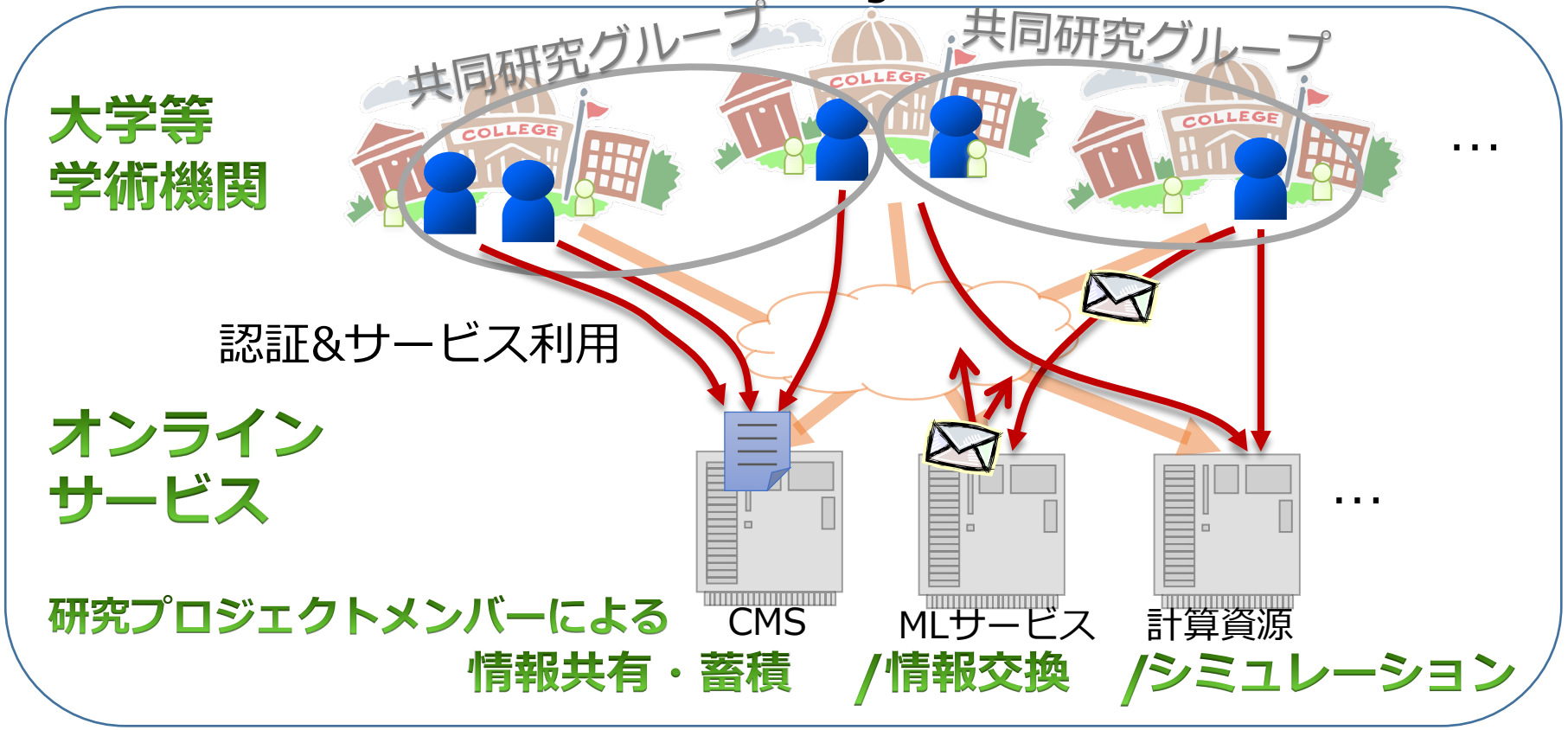
移行期間後はOpenIdPが利用できなくなるため、その後「使えないんだけど」という問い合わせが来たらOrthros新規アカウントで利用できるようにする必要がある（必要ならSP側で従来のIDとして扱われるようにする）

mAP Core

mAP Coreの目指すところ：研究教育活動を支援するサイバースペースの提供

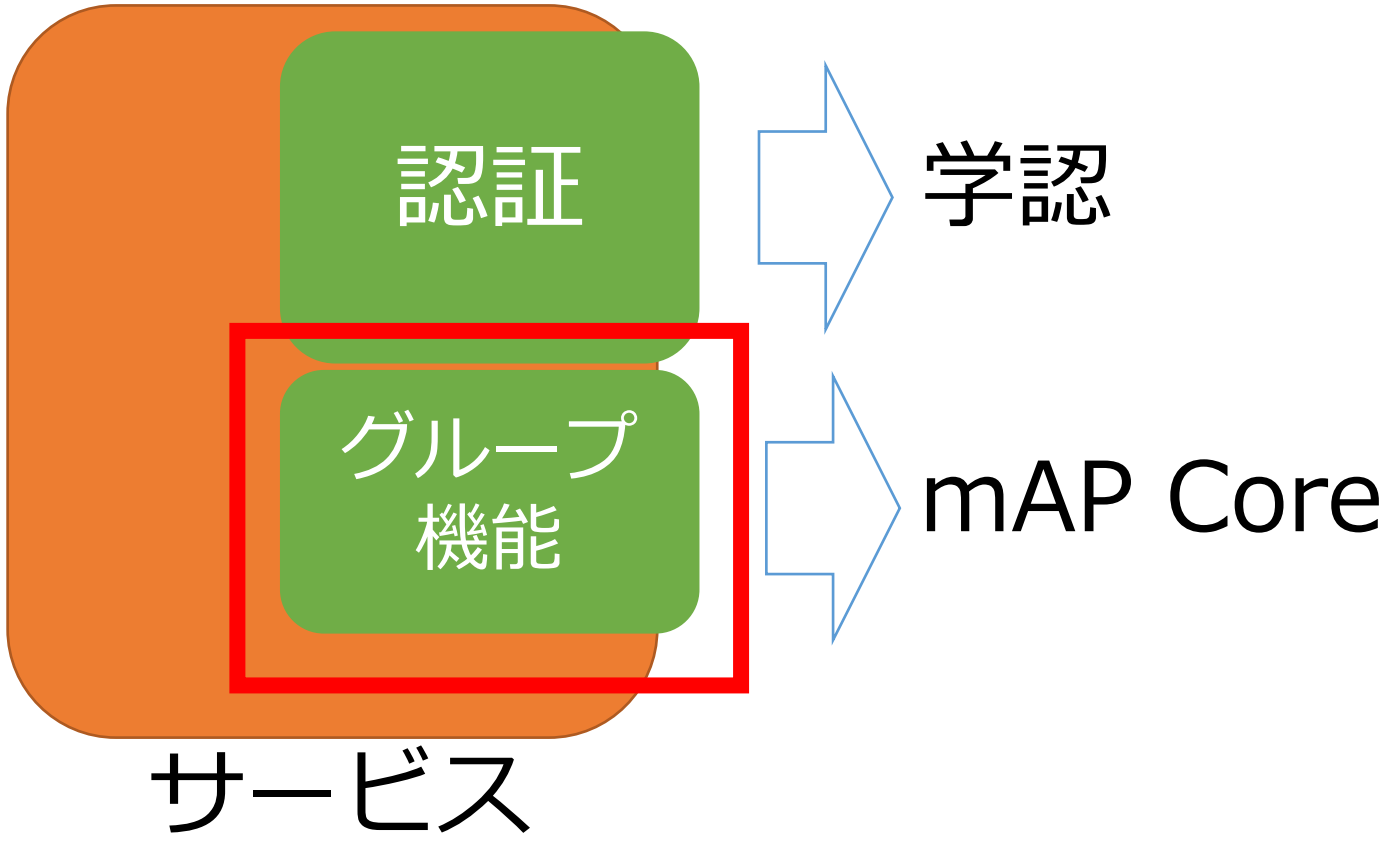
研究教育活動支援の各種オンラインサービスが簡単に利用できる場

- 研究活動/教育活動 - 例えば
  - 研究プロジェクトの推進（情報共有、情報交換、スケジューリング、計算資源利用）
  - 論文作成（文献検索、文献閲覧、収集・蓄積）
  - 講義の実施（履修登録、資料提供、e-Learning）



mAP Coreのイメージ

- 従来サービスの中にあった機能の一部を外出し・サービス間で共有

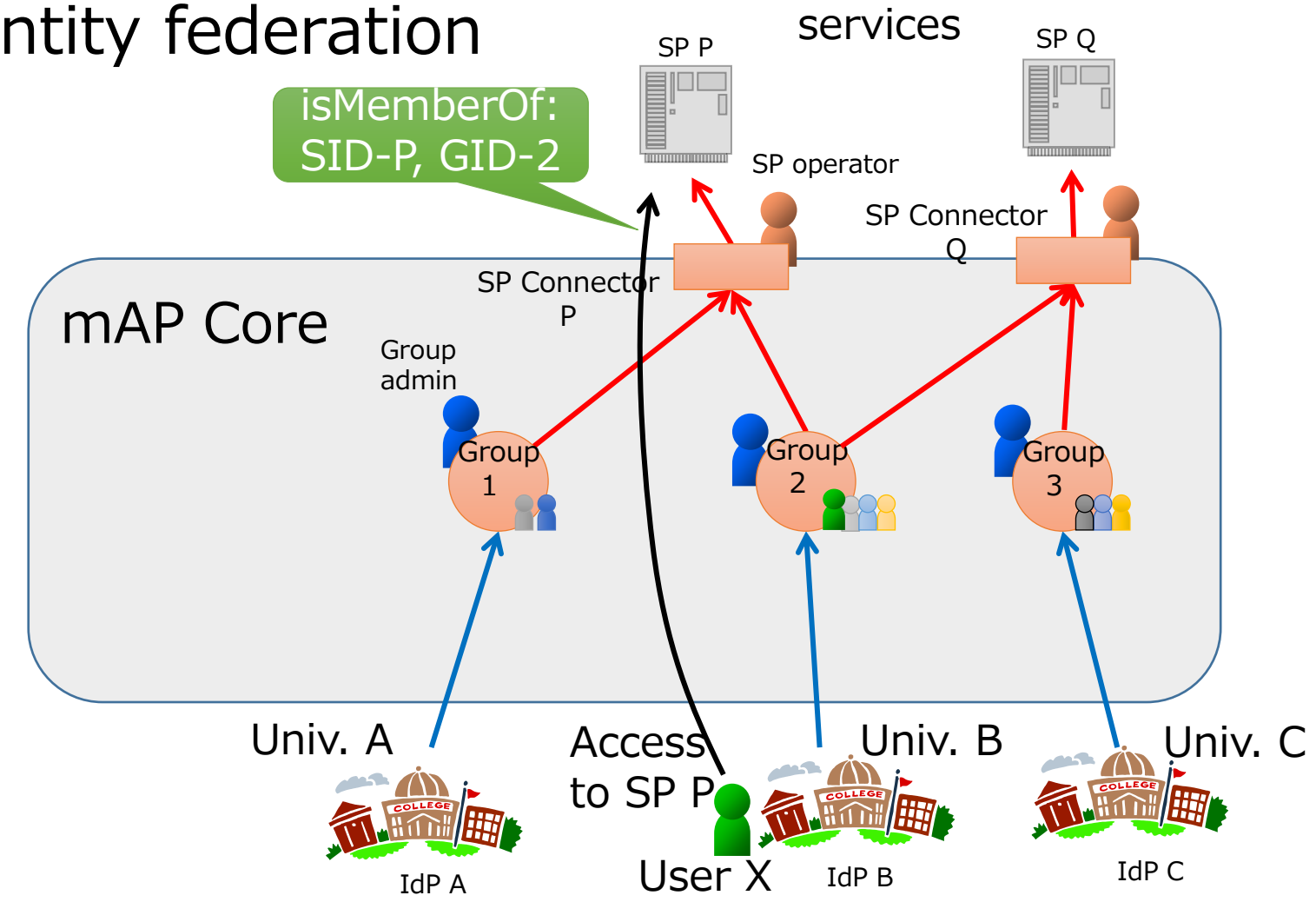


mAP Core概要と経緯

- 今回の内容は以下を包含します
  - GakuNin mAP
  - 学認クラウドゲートウェイサービスのグループ機能
- 改めて学認のグループ機能を「mAP Core」と命名。
- グループ機能：共同研究グループなど学認のIDの任意の集合を「グループ」として扱い学認参加SPに対してグループ情報・メンバー情報を提供する
  - 利用例：
    - グループ機能対応Wiki
    - グループ機能対応メーリングリストサービス
    - 実習システム
    - GakuNin RDM
  - 全てのSPが全ての情報を取得できるわけではなく、グループが利用するSPを選択しそのSPに限って情報提供する（情報の保護）

mAP Core overview

- provides membership information of groups to services within an identity federation



mAP Coreの外部とのインターフェース

mAP Coreが提供するグループ管理のインターフェース・API（ユーザに対するUIを除く）：

① SAML 2.0 Attribute Query
- ePPN（もしくはメールアドレス）をキーに、所属するグループIDを取得できる
- 属性交換仕様として国際標準
- meatwiki、しぼすけ他多くのグループ機能対応SPで利用
- 大学にサーバーを立ててmAP Coreがプロキシして学内情報との連携を実施した実績あり

② 情報取得API（Groups API / People API）
- グループ情報・メンバー情報取得のためのAPI
- `https://meatwiki.nii.ac.jp/confluence/x/lwic`
- VOOTベースだが認証は独自
- MLサービスで利用

③ mAP Core API V1
- グループ作成、メンバー管理を含めたREST API

④ mAP Core API V2
- SCIMに準拠した汎用的なAPI

グループ機能が装備しておくべき機能

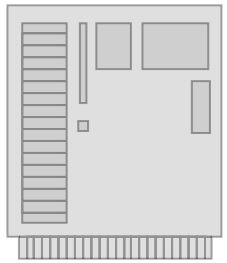
- 利用者がグループを作成、メンバーを設定できること
- サービスが利用者の所属グループを把握できること(①)
  - 個人のIDを知っていることが前提。
  - SAML Attribute Query他
- サービスが接続されたグループ情報メンバー情報を取得できること(②)
  - 利用者がログインしたタイミングでなくとも把握できる
  - 例：MLサービス
- サービスが利用者に成り代わってグループ作成・メンバー管理できること(③,④)
  - サービスが持つグループ情報を同期するなど

従来

Web UIによる操作

NEW

③/④によるグループ
作成・メンバー管理



サービス

mAP Core

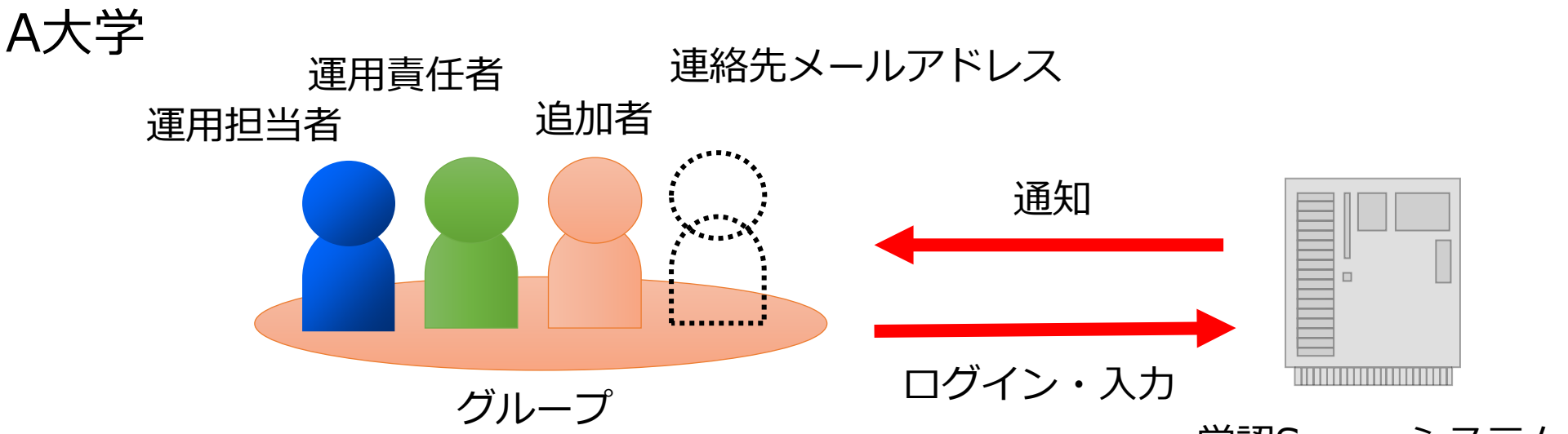
APIにおけるプライバシー・権限管理

- そもそも接続していないサービスにはグループ・メンバーの情報が流れない
- サービス利用開始にあたって各利用者から属性送信の同意を取得する
- REST APIでもこれを反映するよう各データと権限者のマトリクスを作成

attribute name	修正不可	未使用	必須	ユーザ本人	招待主	グループ管理者(所属グループ)	サービス管理者(利用中サービス)	組織(Id
.				rw	rwd	r	r	r
schemas[]	1			-	-	-	-	
id	1			r	r	r	r	
externalId	1		1	rw	rw	r	r	r
userName			1	rw	r	r	r	
displayName				rwd	rwd	r	r	rw
nickName				rwd	rwd	r	r	rw
profileUrl				rwd	rwd	r	r	rw
title		1		rwd	rwd	r	r	rw
userType		1		rwd	rwd	r	r	rw
preferredLanguage				rwd	rwd	r	r	rw
locale		1		rwd	rwd	r	r	rw
timezone		1		rwd	rwd	r	r	rw
password		1		-	-	-	-	
meta.resourceType				r	r	r	r	
meta.created	1			r	r	r	r	
meta.lastModified	1			r	r	r	r	
meta.location				r	r	r	r	
meta.createdBy	1			r	r	r	r	
name.familyName		1		rwd	r	r	r	rw
name.givenName		1		rwd	r	r	r	rw
name.middleName		1		rwd	r	r	r	rw

学認Surveyシステム

- 各参加機関の担当者（運用担当者・運用責任者）に対して調査
  - ・アンケートを行うシステム
  - 担当者をグループとして、認証した上で入力させる
  - 適格者を自分で追加・削除することが可能
  - 通知先メールアドレスを追加可能
  - 例年行っている学認参加IdP運用状況調査に利用

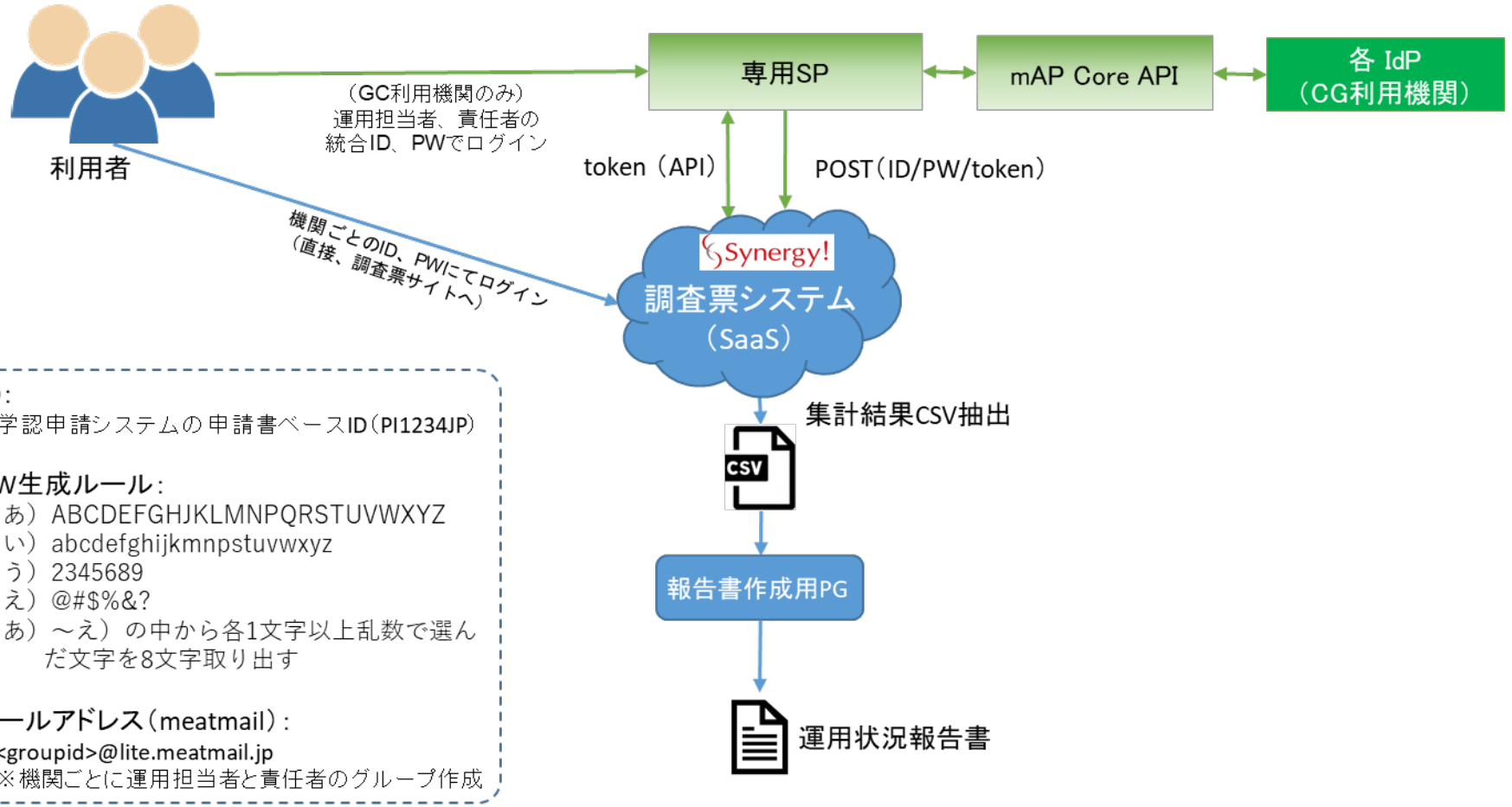


学認Surveyシステム（続き）

- mAP Core上に機関の数だけグループを作成する
- 通知には既存MLサービスであるmeatmailが利用できる
- 認可のためのグループ情報をmAP Core APIで取得する

APIを利用した学認Surveyシステムとの連携

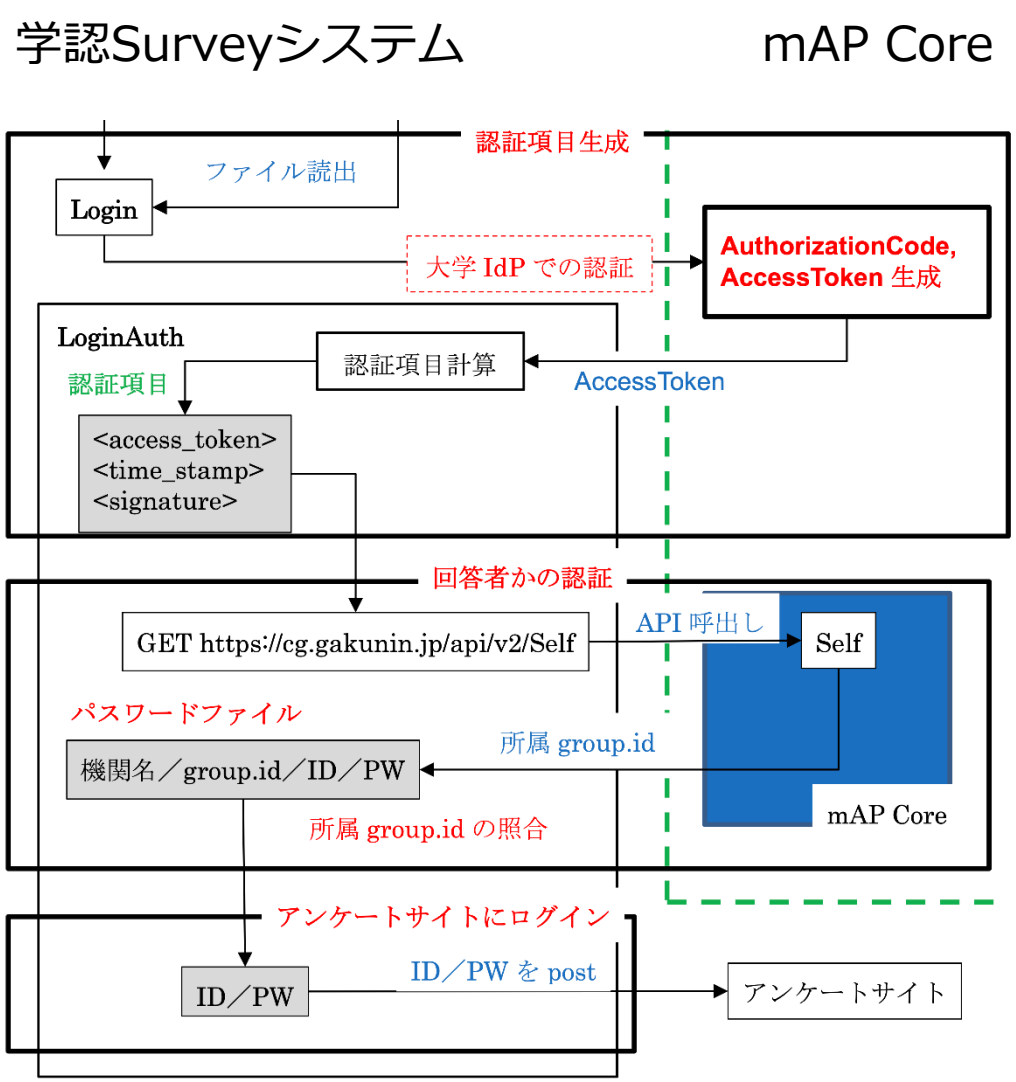
- 調査票システムはSaaS
- 専用SPが仲介となる



APIを利用した学認Surveyシステムとの連携（続き）

- 専用SP自身はIdPから属性をもらわない
  - mAP Coreで認証を行う
  - 専用SPはmAP Coreからグループ情報をもらうのみ

⇒新たな連携方法の可能性



参考：Shibboleth開発状況あれこれ（IdP）

Shibboleth IdPについてのあれこれ

- バージョン5（2023年Q3予定）にて行われる予定の仕様変更にあわせてご準備を
  - **JPA StorageServiceのプラグイン化**
    属性生成にデータベースを用いている場合、V5へのアップグレード時に代替プラグインの導入が必要になる予定です。V4.1以降で事前導入可能
    事前導入手順： https://meatwiki.nii.ac.jp/confluence/x/YpKfBQ
  - **eduPersonTargetedIDからpersistent-idへの移行？**
    eduPersonTargetedIDの生成機能がdeprecatedになっている
    ネタ元：https://shibboleth.atlassian.net/browse/IDP-2043