

AXIES 年次大会 2022
認証基盤部会 企画セッション

認証プロキシサービス Orthros



坂根 栄作

国立情報学研究所

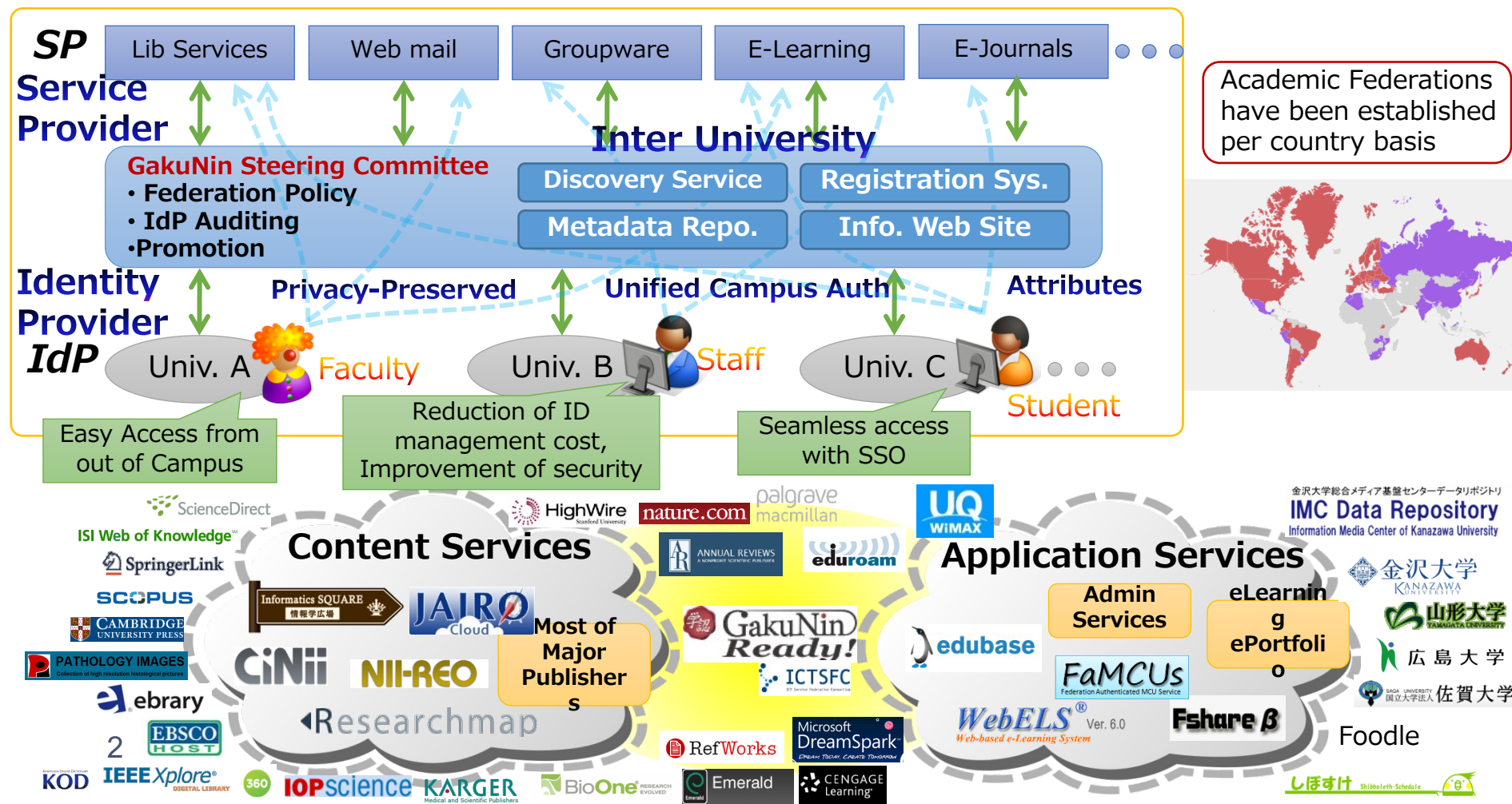
学術認証フェデレーション



GakuNin



- 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



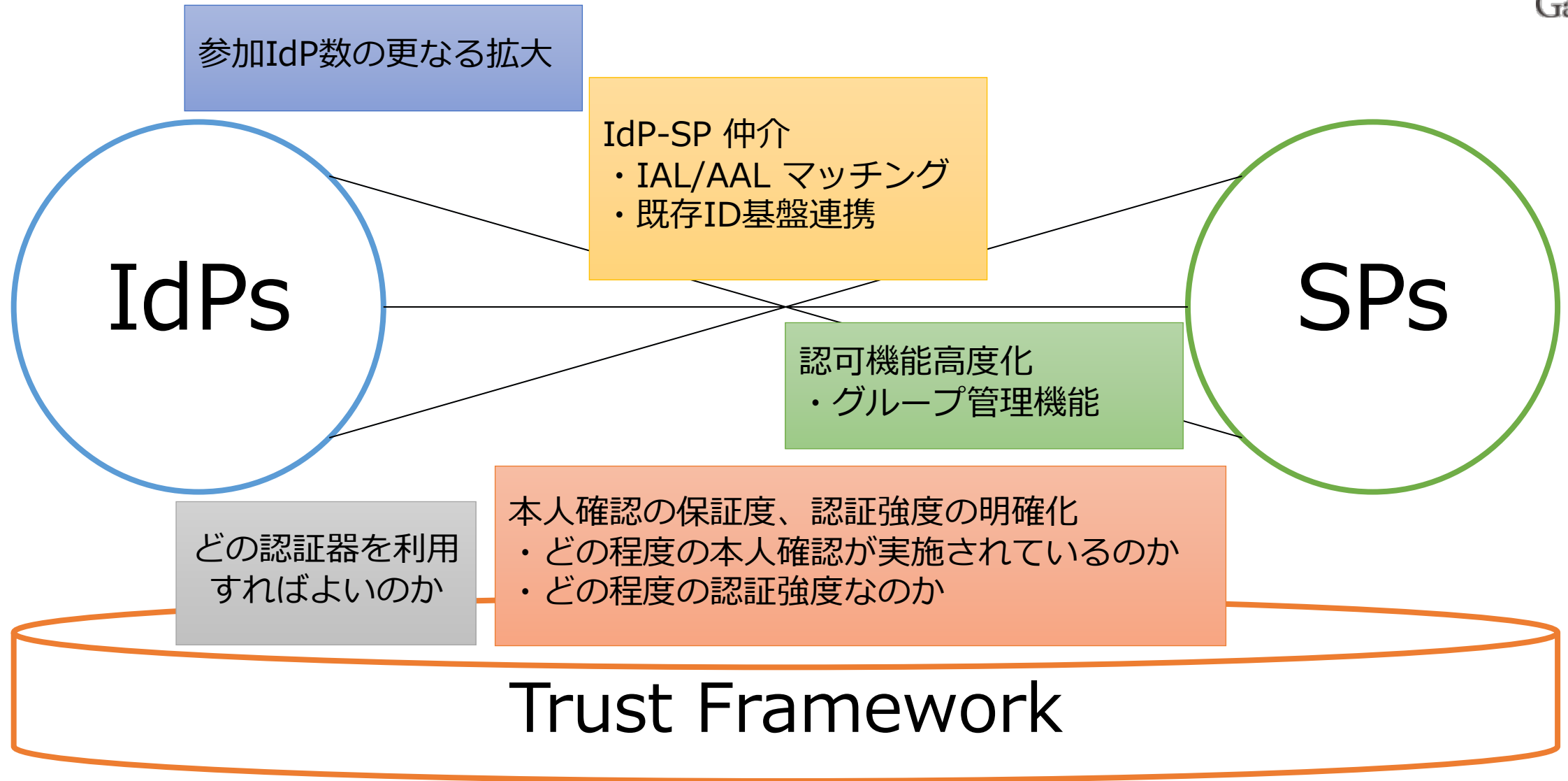
研究・教育DXを推進するために

- 研究・教育データ流通の加速が必須
- 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
 - 認証ポリシーの相互運用性
 - 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上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）

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

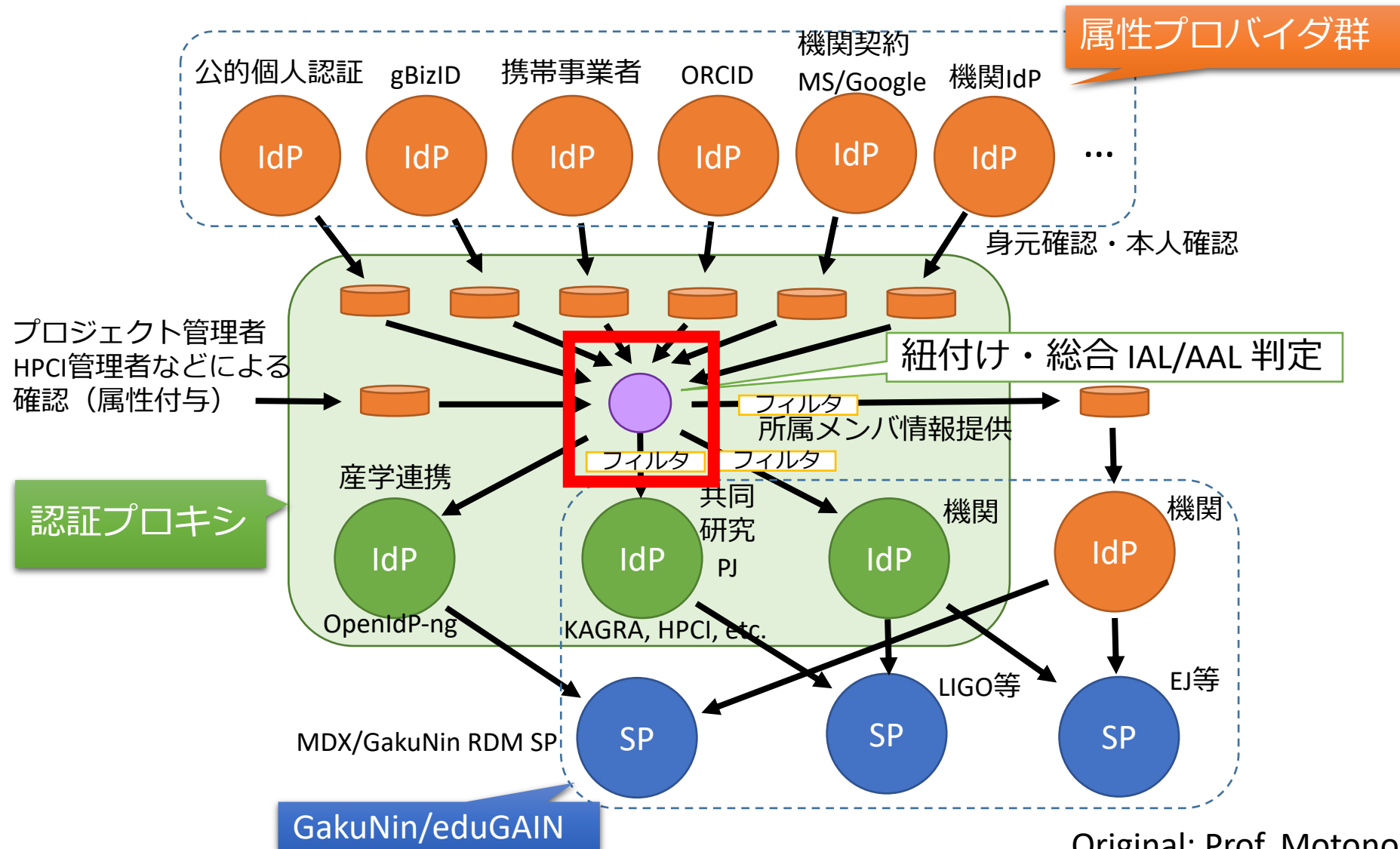
グループ管理機能の高度化

- 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

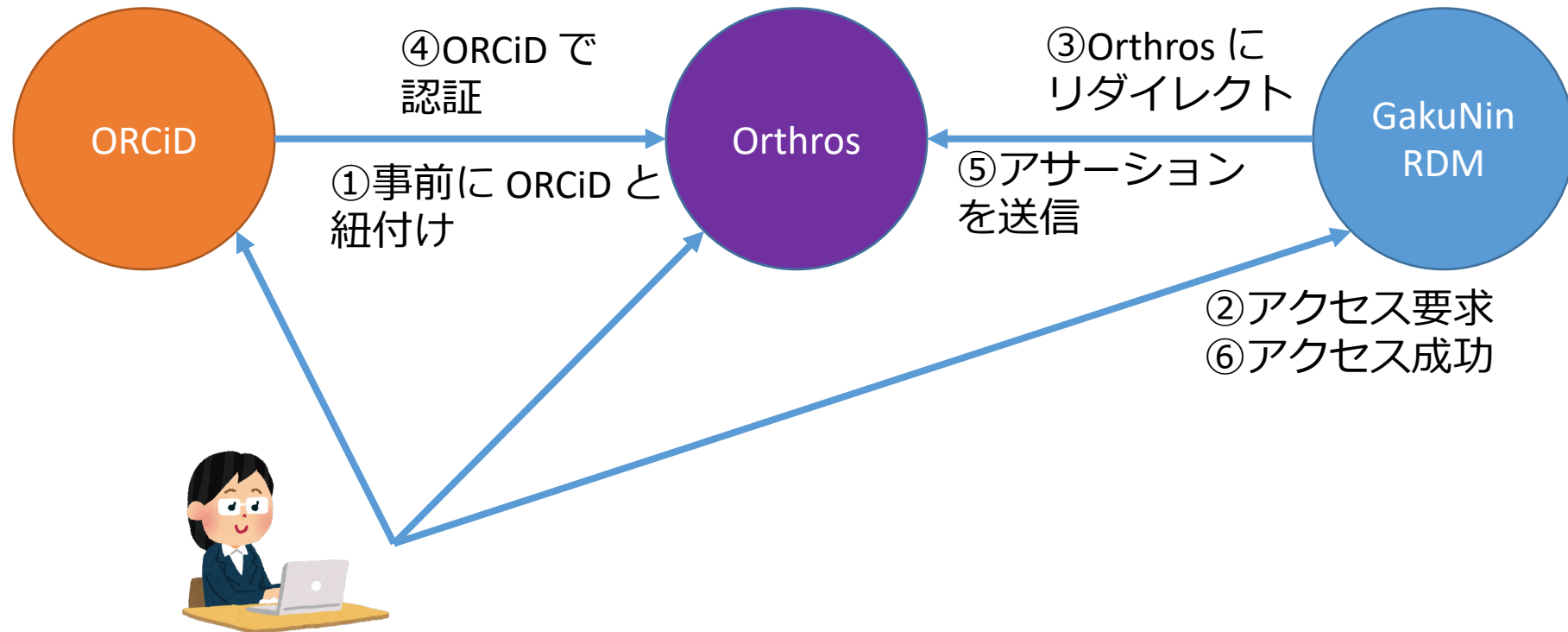
- 産学連携を含む多種多様な研究を支援する SP への Id 連携時に、必要な Id 保証を柔軟に担保するなどの機能を提供する
 - IAL, AAL matching, AL enhancement
 - credential bridging (e.g., OAuth access token -> SAML assertion)
- 既存の研究コミュニティのもつトラストフレームワークにおいて、Id 基盤部分を外だしできるようにする
 - 本人確認手続きを外部に依頼できる

認証プロキシのデザイン



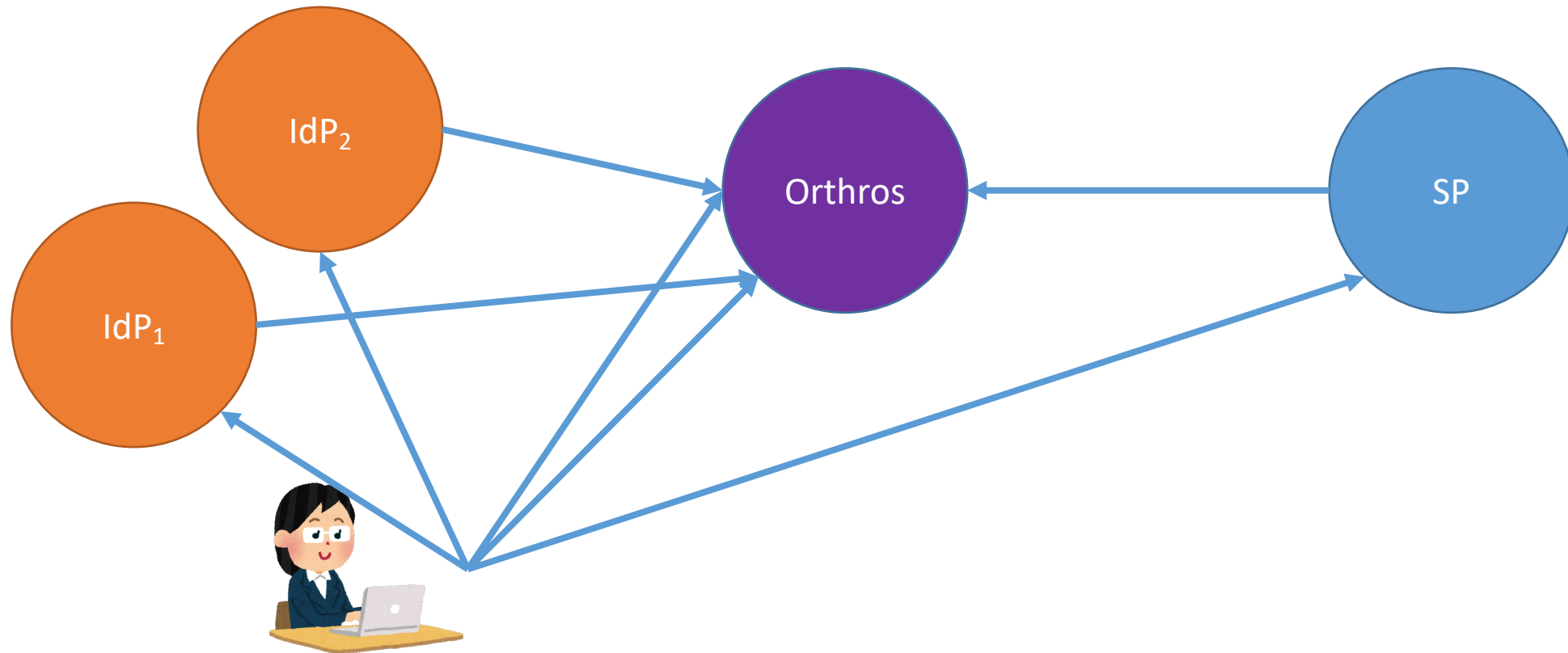
ユースケース 1 – credential bridging

- 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)



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

Send verification code

Create



16

外部ID連携 (1/4)

Home - Orthros

+

← → ↺

https://auth-proxy.web-walker.jp/mypage/

120% ☆

🔍 🌐 ☰

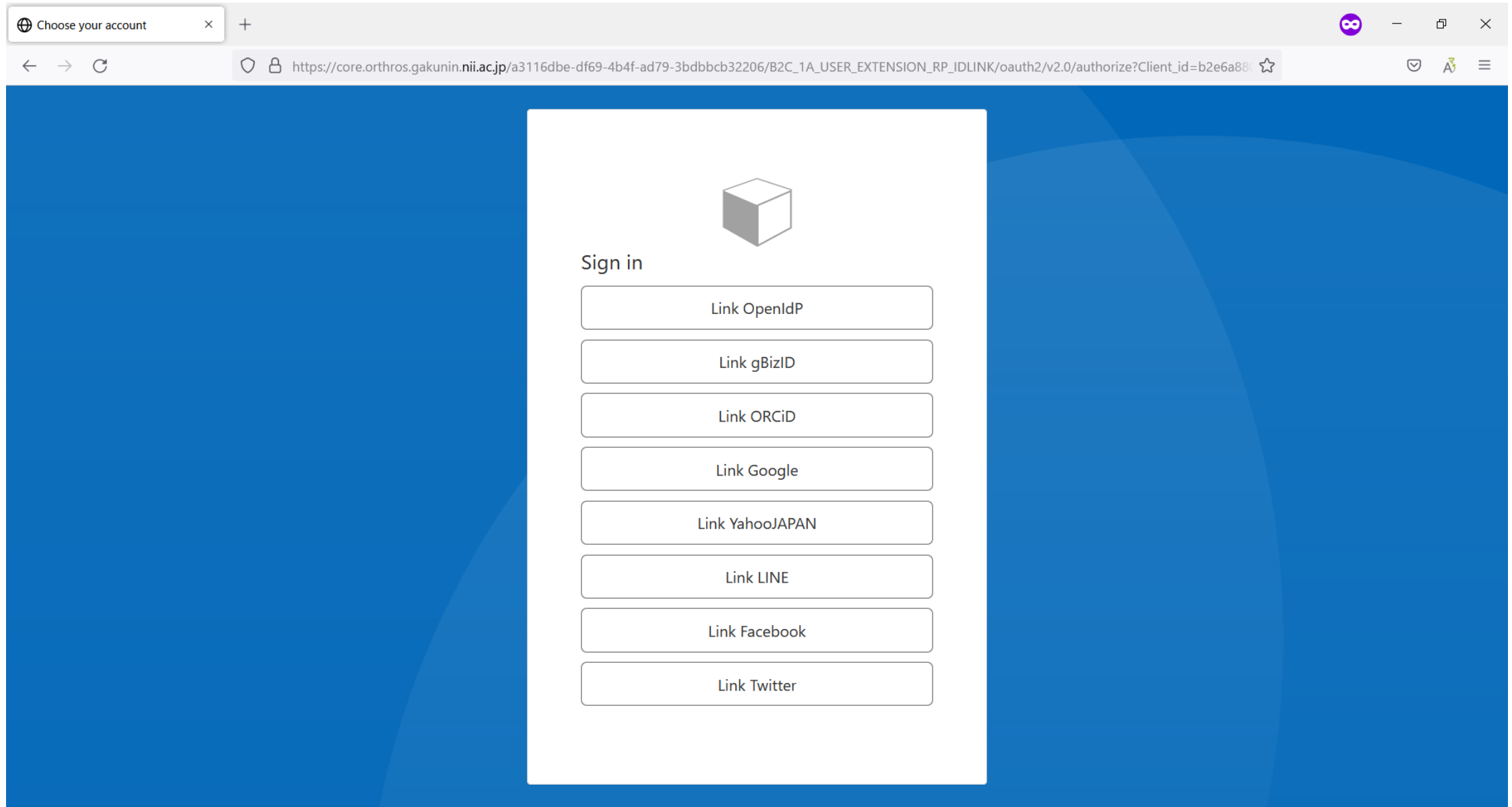
⌵

Orthros ホーム 設定 ログアウト

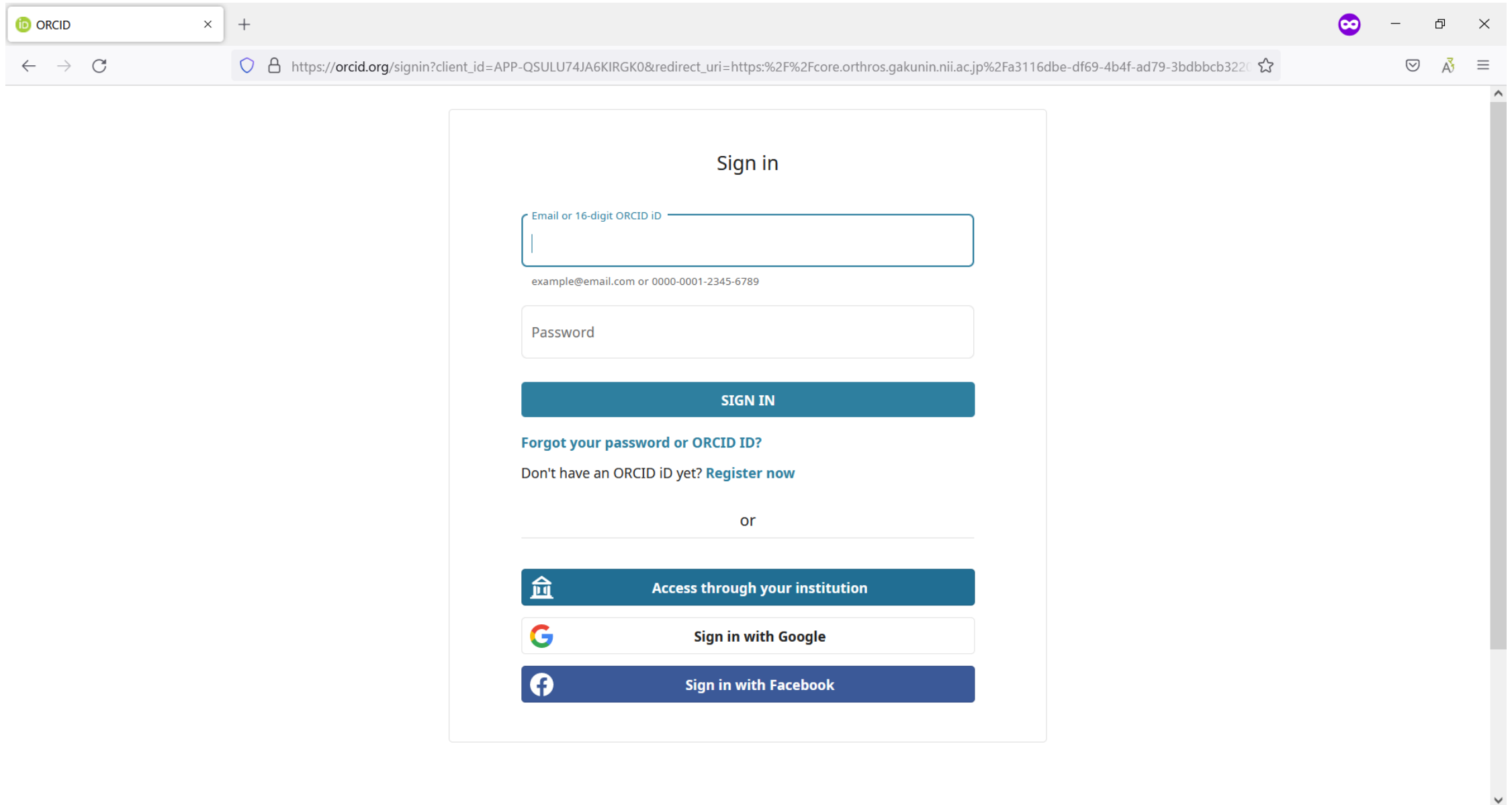
サービスの認証連携状況

サービス名称	連携状況
G.bizID	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)



外部ID連携 (3/4)



id ORCID

https://orcid.org/signin?client_id=APP-QSULU74JA6KIRGK0&redirect_uri=https:%2F%2Fcore.orthros.gakunin.nii.ac.jp%2Fa3116dbe-df69-4b4f-ad79-3bdbbcb3220

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

+

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.bizID	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)



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

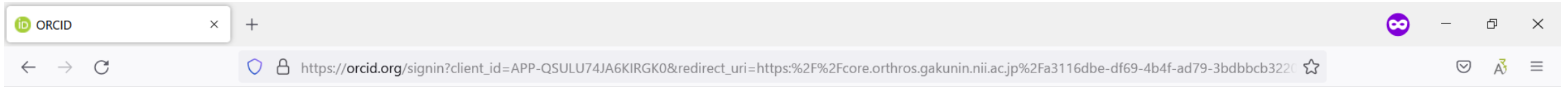
 Twitter

Yahoo! Japan

 Google

ORCID

ログイン (3/4)



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

+

70%

☆

🔒

🔍

☰

Orthros ホーム 設定 ログアウト

アカウント

メールアドレス

●●●●●●.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.bizID	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

まとめ



GakuNin

Orthros

- 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

