

A Study of Authentication Proxy Service for Various Research Communities

Eisaku Sakane*, Motonori Nakamura**, Yuusuke Komiyama*,
Takaaki Komura**, Takeshi Nishimura*, Sayako Shimizu*

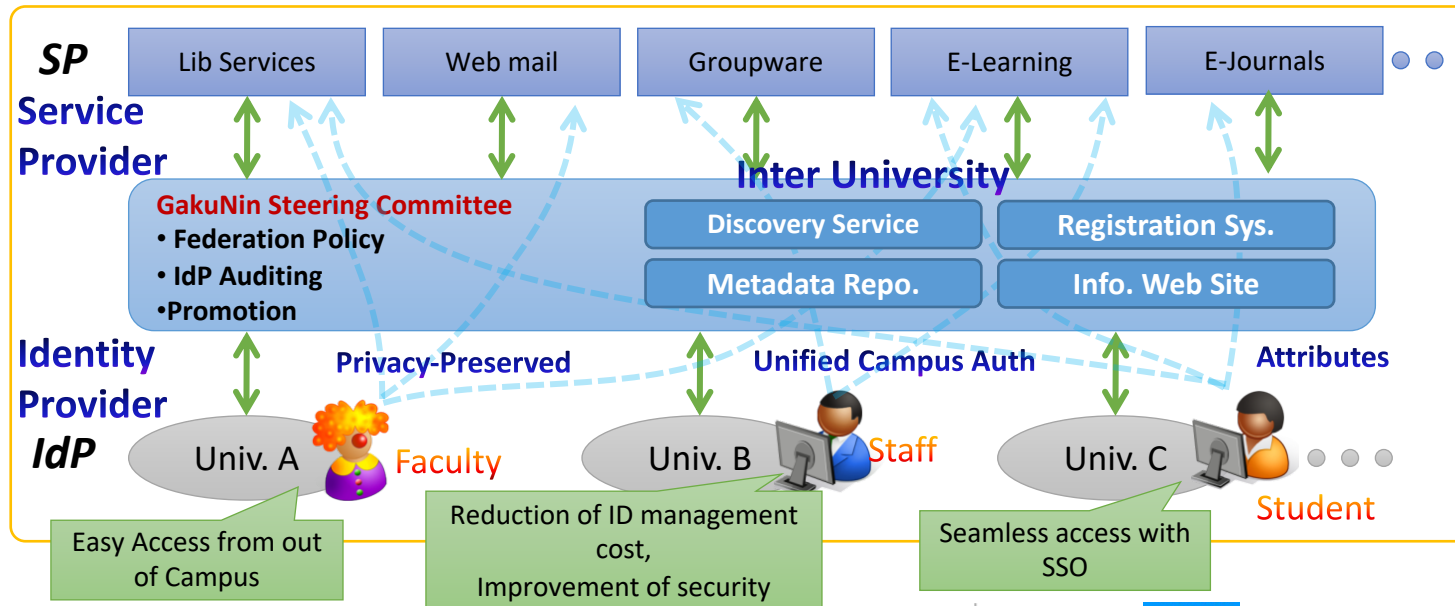
*National Institute of Informatics

**Kyoto University

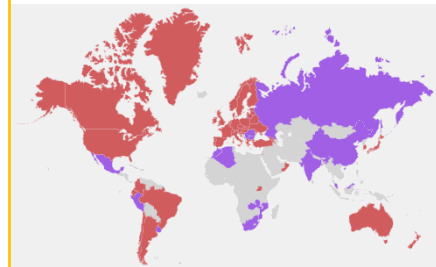




- Build up new ICT infrastructure to support R&E based on SSO technologies
- Provides trust framework (technologies, policies and assessment)
- Offers value added services (academic discount, etc.) by collaboration with commercial
- Improves usability and security with continuous R&D (including multifactor/cert. auth.)



Academic Federations have been established per country basis



Background

- Necessity for a new trust framework in Japan
 - GakuNin has provided a stable trust framework to academia in Japan.
 - There are many research communities in Japan, but they don't always rely on IdPs in GakuNin because all GakuNin IdP do not satisfy the requirement of the communities.
 - As a result, a trust framework has been formed in each research community.
 - Many of users in the research communities are also constituent members of IdPs that join GakuNin.
 - It is natural for users to demand to use home organization account for services in the research communities. In other words, users shouldn't want to manage several accounts.

Request from Research Communities

- Authenticating users that don't have suitable IdP accounts.
 - Users that RC offers services not always possess the account of an IdP joining GakuNin.
 - RC want to rely on IdP that provides sufficient identity assurance.
- Grasping authenticator level
 - Password only or multi-factor authentication
 - For certain services RC want users to impose MFA.
- Identification user that belongs to several organization.
- Ensuring user identity moving between different organizations.
 - SP want to provide continuously and efficiently services to users moving between different organizations.
- Support for suitable attributes for purpose
 - e.g., grasping whether resident or not (export control)

Key Components in New GakuNin Trust Framework

GakuNin IAL/AAL

- Stipulation of IAL and AAL

Authenticator Registry

- Evaluation of authenticators based on GakuNin AAL

Authentication Proxy Service "Orthros"

- AL matching, credential bridging, attribute coordination

IdP Hosting Service

- Addressing issues of IdP building and operation

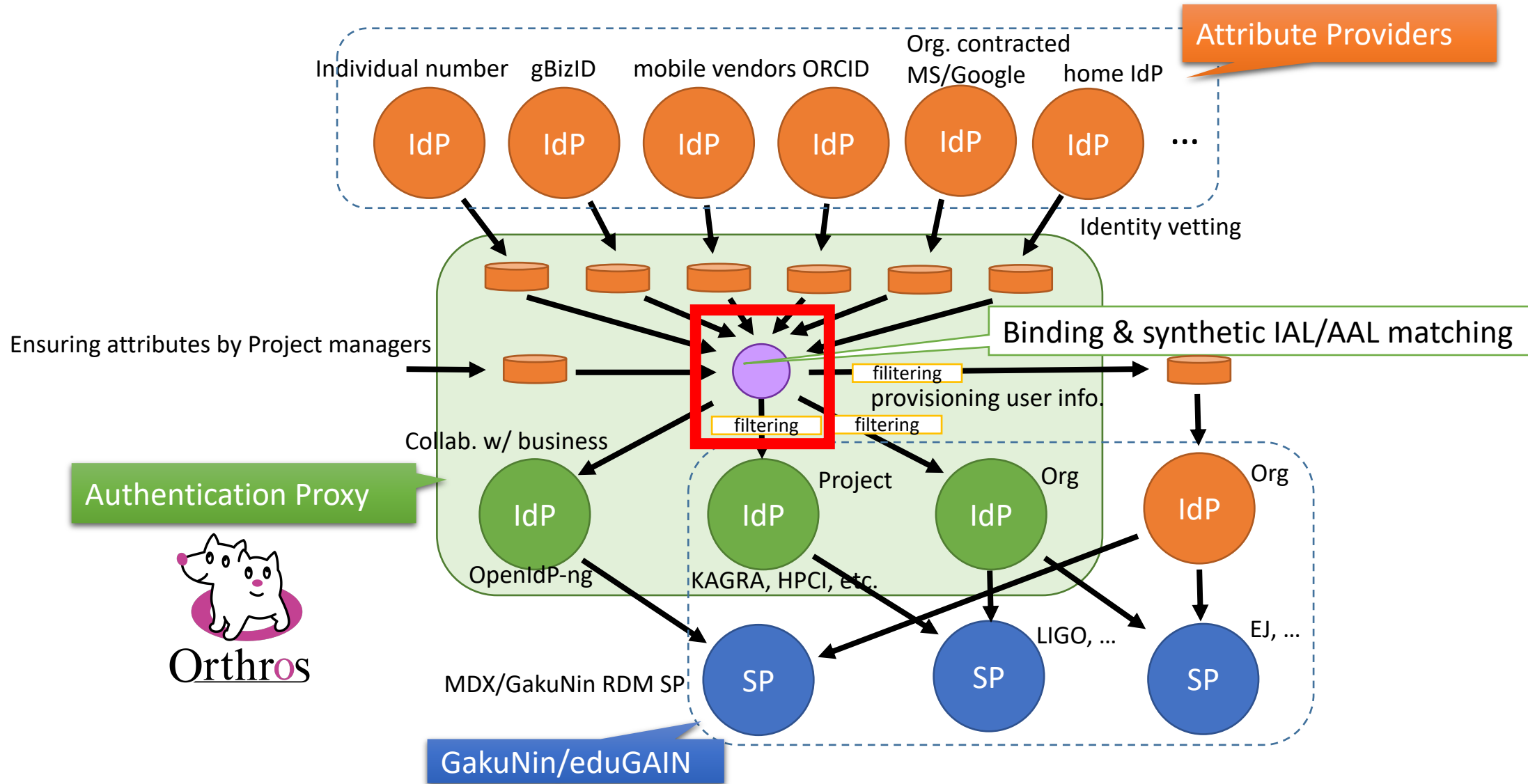
Advanced Group Management

- Support for high and complex authorization control

Development of Authentication Proxy Service

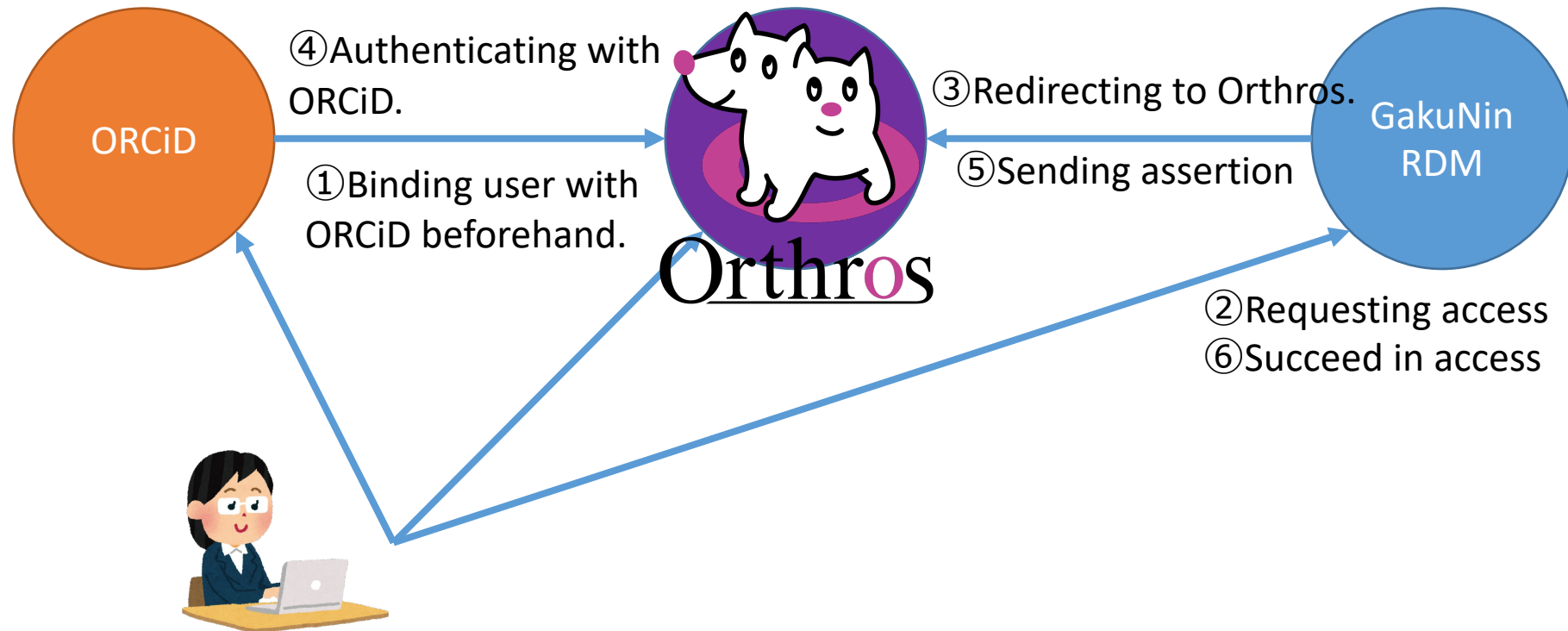
- Support for the new GakuNin trust framework.
- Bridging between IdPs and SPs, and enabling IAL/AAL management and attribute assurance.
- Enabling research communities to delegate identity vetting to user's IdP.

Design of Authentication Proxy Service, "Orthros"



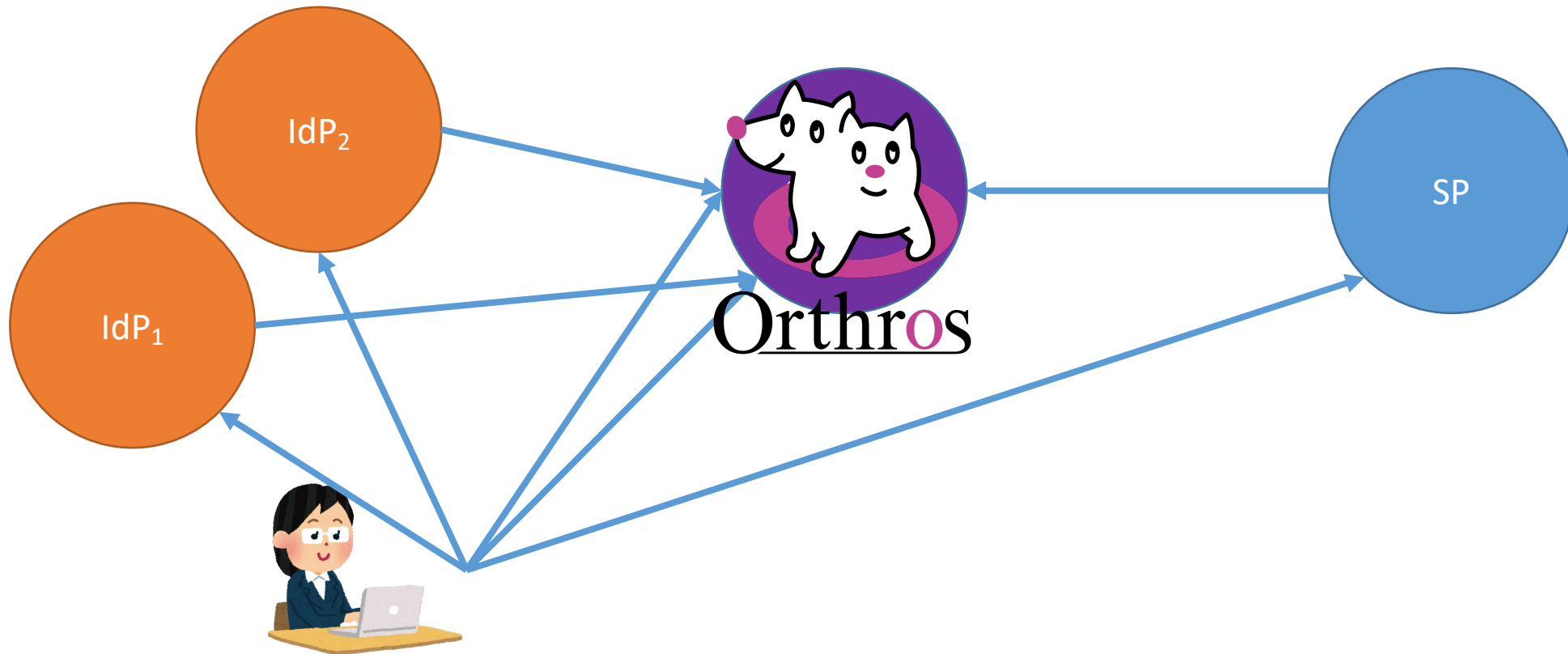
Use case 1 – credential bridging

- Researchers of companies use GakuNin RDM with ORCID credential.



Use case 2 – IAL enhancement

- By binding several ID, IAL required by SP is satisfied.



Design and Implementation of Orthros

- Core part of authentication proxy (IDaaS)
 - **SELMID** – <https://ctc-insight.com/selmid>
- User interface part
 - developed in-house
- Fundamental functions
 - ID management, login, ID binding, management of ID binding, attribute management
- SP management (for SP administrator)
 - handling IAL/AAL imposed by each SP
- Agreement management for each SP
 - Getting user agreement when user initially login to SP
 - Enabling user to confirm or cancel the current status of agreement.
 - Enabling administrator to check the status of agreement of user.
- Attribute assurance
 - Enabling administrator to ensure attributes of user whom the administrator manage.
 - e.g. ensuring user affiliation attribute

Design and Implementation of Orthros (Cont'd)

- More functions implemented
 - Notification at changing mail address.
 - Termination of account.
 - Management of IdP linkage.
 - Forcible password resetting.
- Linking external IdPs
 - Linked : LINE, Google, Yahoo! JAPAN, Facebook, Twitter
 - Now in progress : gBizID, ORCiD
- Linking more SPs

Sign-up (1/4)




Sign-up (2/4)

User details x +

← → ↻ https://core.orthros.gakunin.nii.ac.jp/a3116dbe-df69-4b4f-ad79-3bdbbcb32206/B2C_1A_USER_EXTENSION_RP_SUSI_OIDC/oauth2/v2.0/authorize?Client_id 80% ☆

< Cancel



Email Address

Send verification code

New Password

Confirm New Password

Display Name

Organization Id

Organization Name

Organization Name(en)

department

Create

Sign-up (3/4)



GakuNin

Home - Orthros × + 8 - □ ×

← → ↻ 🔒 📄 🔍 📄 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.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](#)

Sign-up (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.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

プロフィール

ユーザー名

Test001

所属

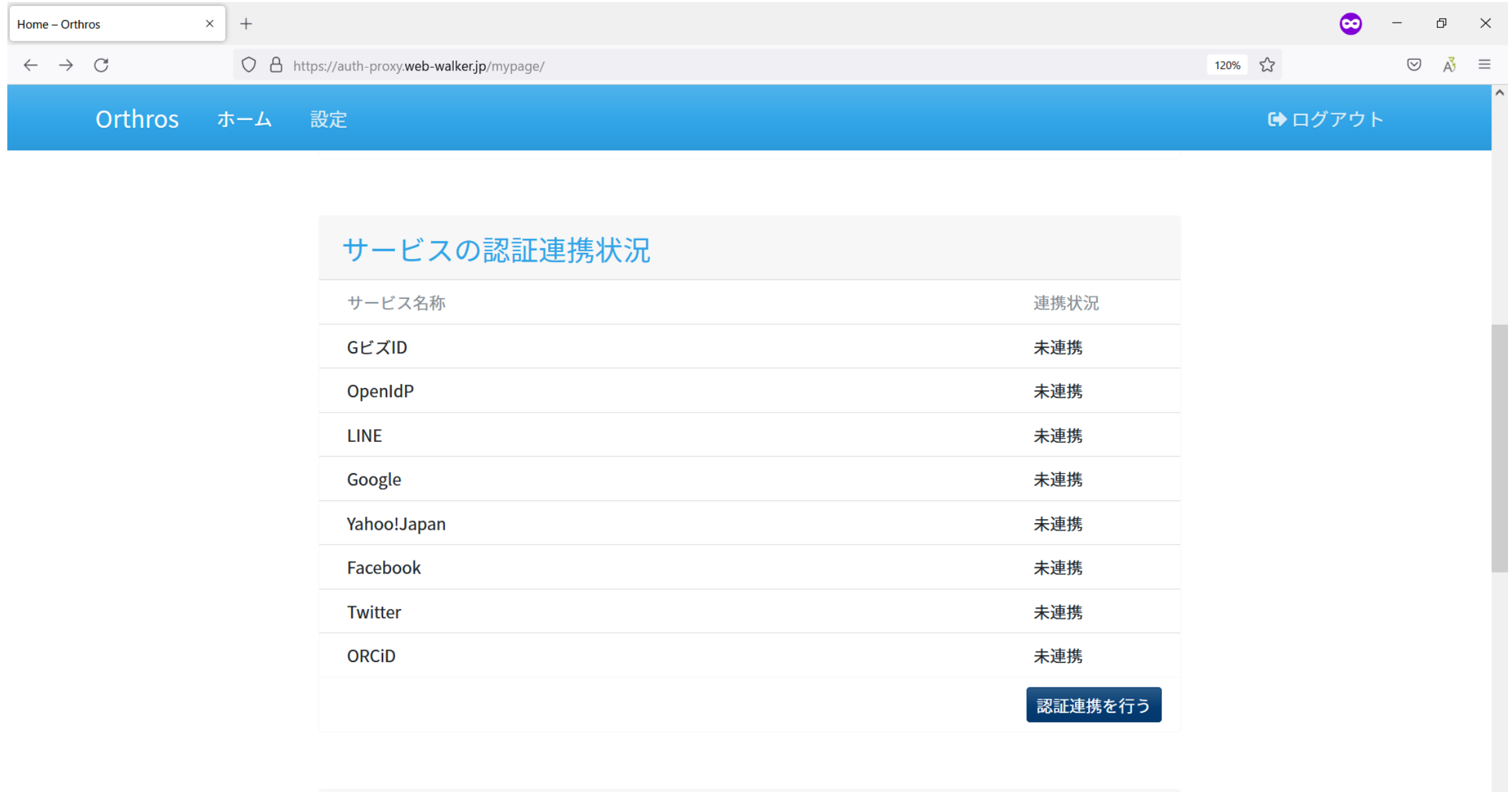
テスト大学

部署

情報システム

情報の更新 (確認画面へ)

Linking external ID (1/4)



Home - Orthros

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

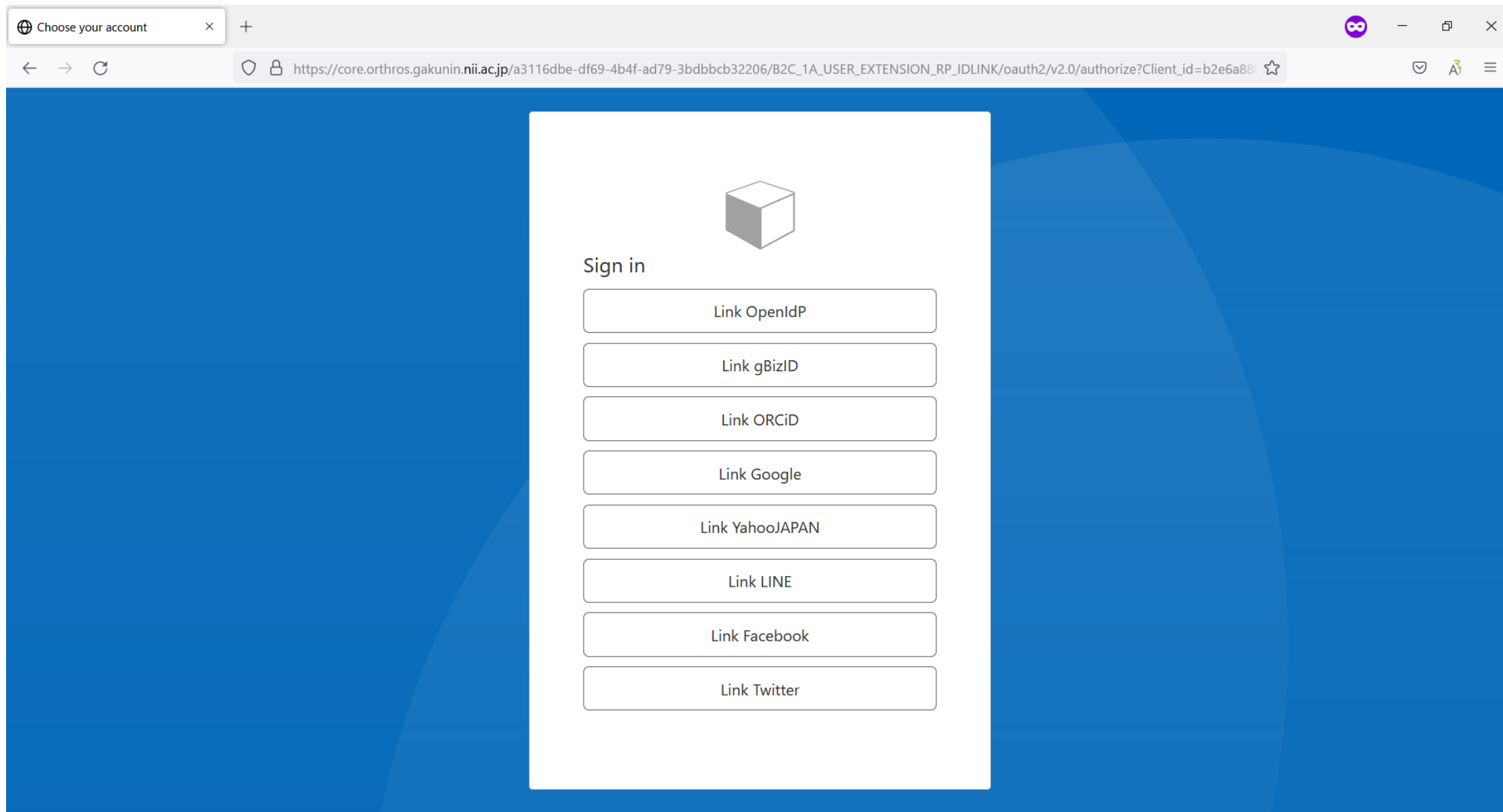
Orthros ホーム 設定 ログアウト

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

Linking external ID (2/4)



Choose your account

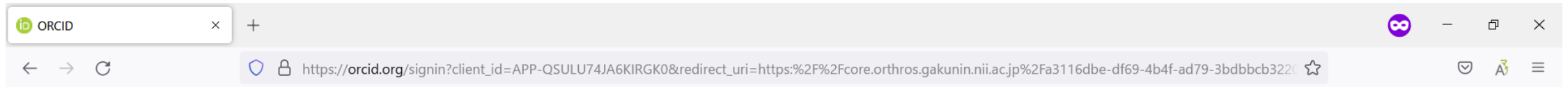
https://core.orthros.gakunin.nii.ac.jp/a3116dbe-df69-4b4f-ad79-3bdbbcb32206/B2C_1A_USER_EXTENSION_RP_IDLINK/oauth2/v2.0/authorize?Client_id=b2e6a88f...



Sign in

- Link OpenIdP
- Link gBizID
- Link ORCID
- Link Google
- Link YahooJAPAN
- Link LINE
- Link Facebook
- Link Twitter

Linking external ID (3/4)



Sign in

Email or 16-digit ORCID ID


example@email.com or 0000-0001-2345-6789


SIGN IN


[Forgot your password or ORCID ID?](#)

Don't have an ORCID ID yet? [Register now](#)

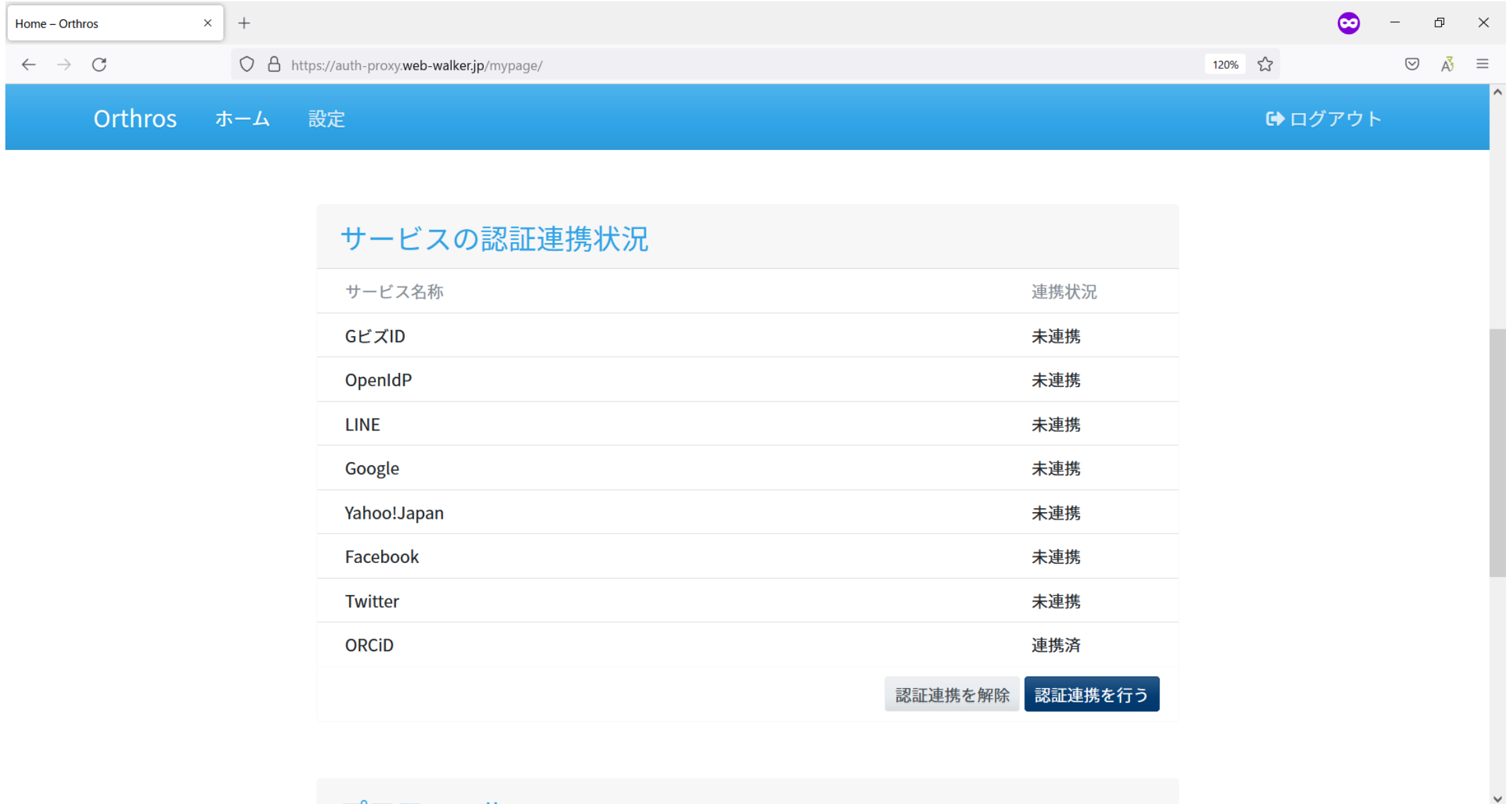
or

 **Access through your institution**

 **Sign in with Google**

 **Sign in with Facebook**

Linking external ID (4/4)



Home - Orthros

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

Orthros ホーム 設定 ログアウト

サービスの認証連携状況

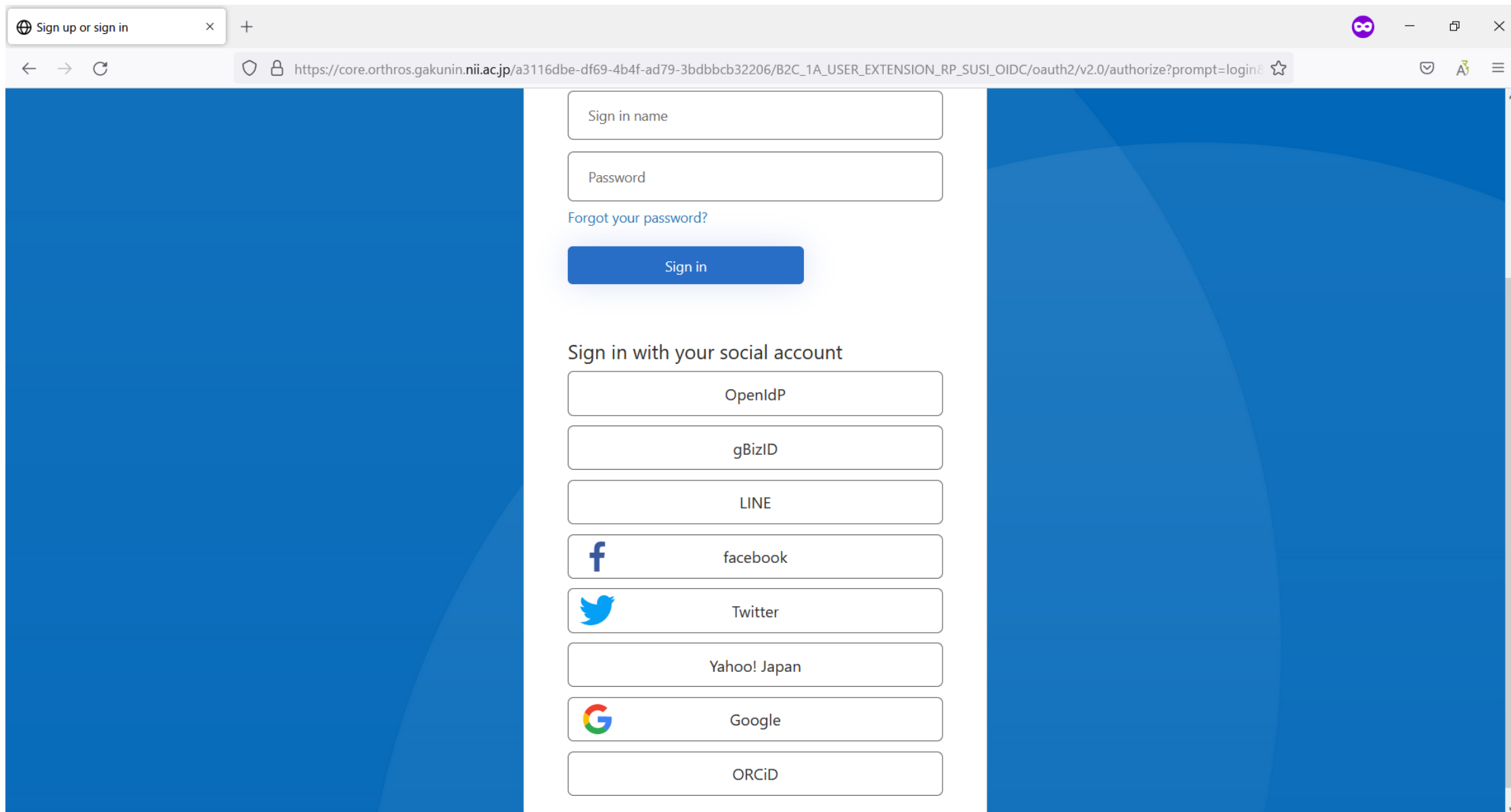
サービス名称	連携状況
GbizID	未連携
OpenIdP	未連携
LINE	未連携
Google	未連携
Yahoo!Japan	未連携
Facebook	未連携
Twitter	未連携
ORCID	連携済

認証連携を解除 認証連携を行う

Login (1/4)



Login (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

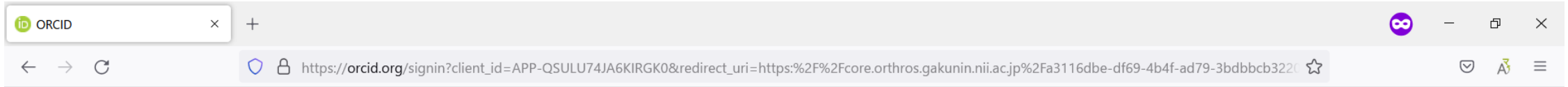
Twitter

Yahoo! Japan

Google

ORCID

Login (3/4)




Sign in


example@email.com or 0000-0001-2345-6789


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**

Login (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	██████████.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

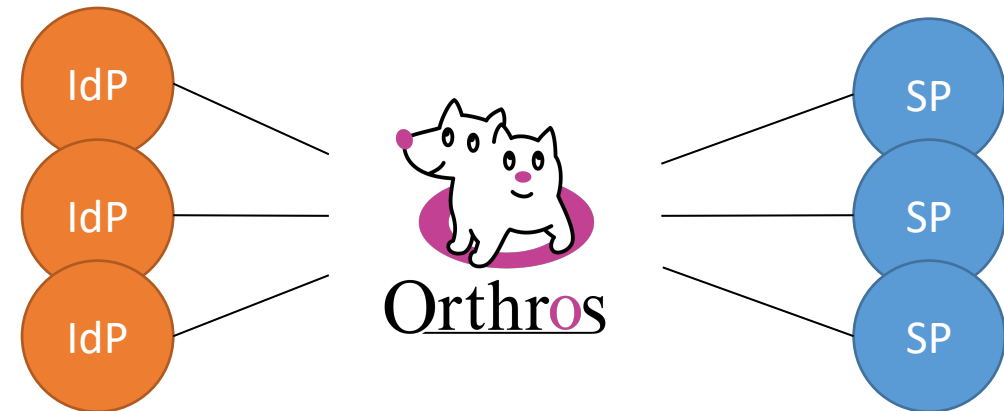
[認証連携を解除](#) [認証連携を行う](#)

Future Plan

- Toward Orthros in production operation
 - Migration OpenIdP to Orthros
 - OpenIdP supports users who do not possess an account of IdP that joins GakuNin.
 - Linkage external IdP (gBizID, ORCID) in production operation.
 - Enabling user to select attributes that user send to each SP.
 - Home IdP Binding at organization change.
 - Support for GakuNin IAL/AAL policy.
 - Enhancement of attribute handling for authorization.
- AL enhancement scheme.
- Operation policy and practice statement should be published.

Summary

- We developed an authentication proxy service, called “Orthros”, to solve the issues of current research situation in Japan.
- Orthros can
 - support new GakuNin trust framework,
 - match IAL/AAL required by SP or ensured by IdP,
 - enhance assurance level,
 - bridge different credentials,
 - coordinate attributes.



- We plan to proceed to trial operation in FY2023.