

学術情報基盤オープンフォーラム2023

認証トラック3

# 学認対応 IdP ホスティングサービスについて 国立研究機関の事例

上野悟, 星佳芳

国立保健医療科学院 保健医療情報政策研究センター

学術情報基盤オープンフォーラム2023 COI開示

認証トラック3

# 学認対応 IdP ホスティングサービスについて 国立研究機関の事例

上野悟, 星佳芳

**演題発表に関連し、発表者らに開示すべき  
COI関係にある企業などはありません。**

## 国立保健医療科学院の使命

国立保健医療科学院ホームページから御参照ください。

<https://www.niph.go.jp/information/pamphlet2021.pdf>

## 国立保健医療科学院の沿革

国立保健医療科学院ホームページから御参照ください。

<https://www.niph.go.jp/information/pamphlet2021.pdf>

## 科学院のご紹介 -組織図-

国立保健医療科学院ホームページから御参照ください。

<https://www.niph.go.jp/soshiki/soshikizu/>

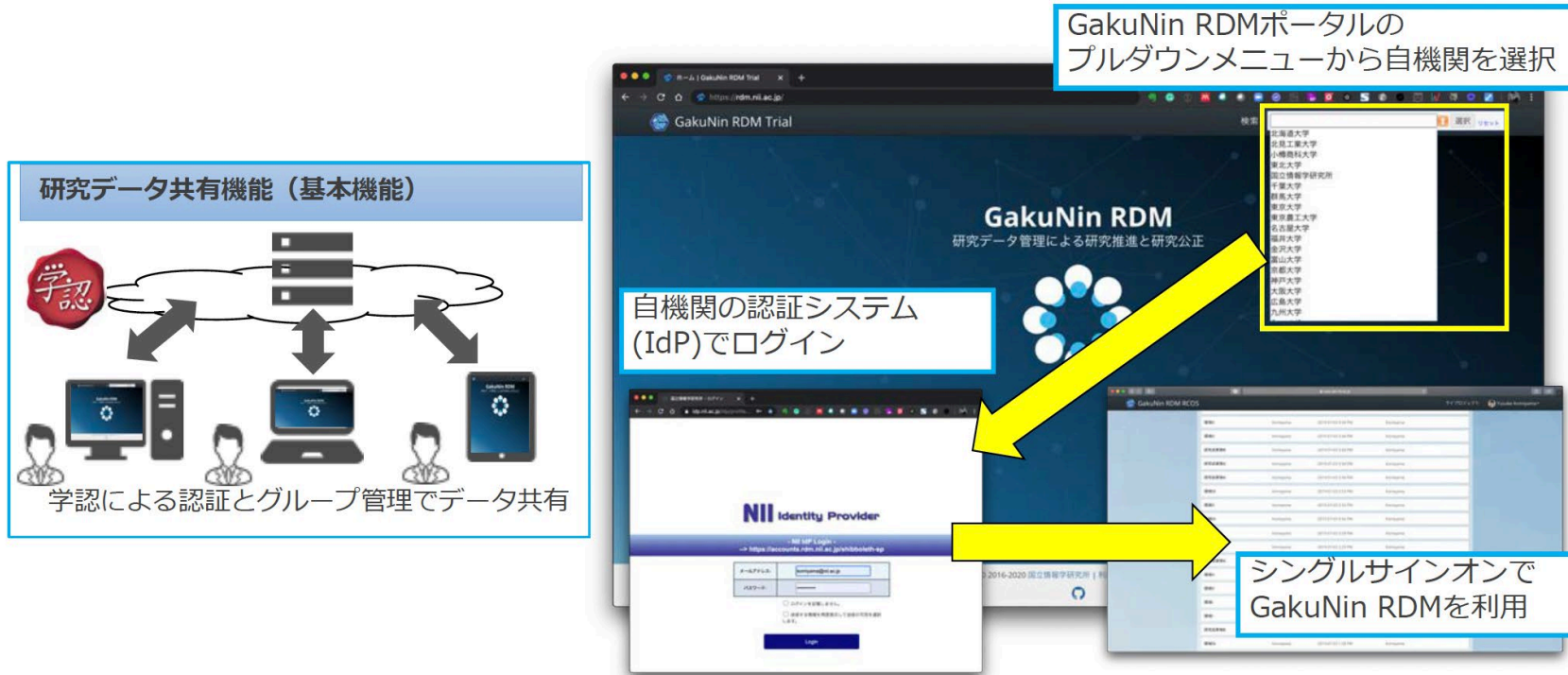
人材育成プログラム

調査研究

国立保健医療科学院ホームページから御参照ください。

<https://www.niph.go.jp/information/pamphlet2021.pdf>

# 背景 | 研究データ管理サービス 学認フェデレーション参加のIdPが必要

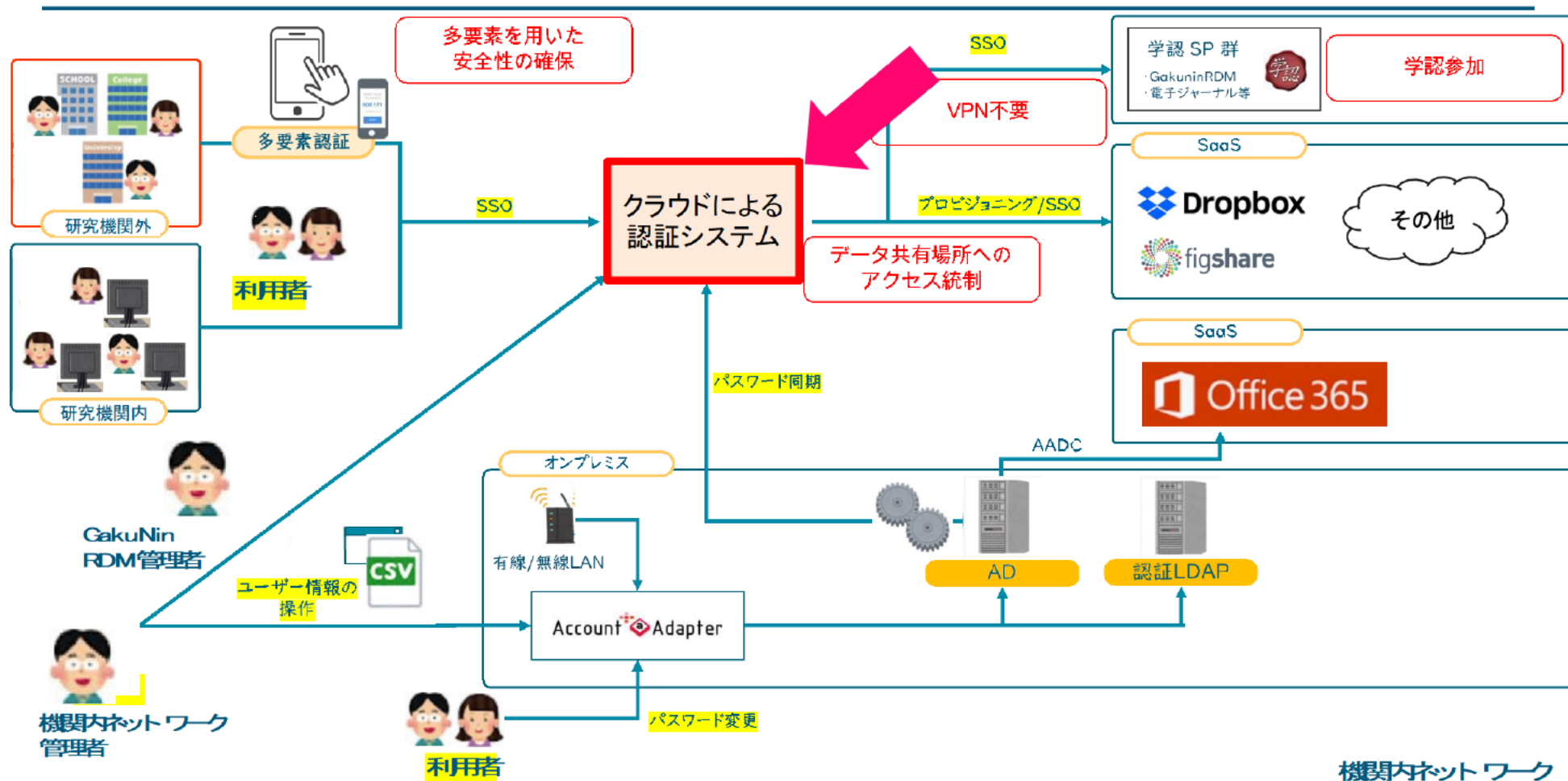


GRDMでは、学術認証（学認）フェデレーションにサービスプロバイダ（SP）として登録済みのため、学認に参加していればアイデンティティプロバイダ（IdP）連携のみで導入が可能

# 構想 |

# GakuNin RDMサービス利用にあたり必要となる環境

## 1. 学認フェデレーション参加のIdPの導入





### 学認フェデレーション参加のIdPの導入

#### 学認連携可能なIdPとの連携方法

- 自施設にて学認連携可能なIdPサーバ（オンプレミス）を設置、維持、管理
- 既存のサービスを導入して、学認連携可能なIdPを利用

#### 問題

- 設置：専門的な知識、経験が必要  
維持管理：継続的なメンテナンスが必要
- 費用確保し続けられるか  
→システム専門部署がなく、人材確保困難  
→費用の面からも、オンプレミスは難しい

### 課題、検討事項

#### 認証システムに対する要望

- 既存のネットワークや認証システム（LDAP等）と連携したい
- しかし、既存のネットワークが止まることは避けたい

#### 課題

- 機関内の認証サーバーとの連携ができないと、ID/PWが異なるので管理が大変
- 普及するには現状以上の利便性と使いやすさが必要  
→既存のサービスを導入  
→既存のネットワークを考慮し、スモールスタートを目指す

# 事例紹介 | 学認対応IdPホスティングサービス実証実験 スケジュール

- **2023/01/30** 学認対応IdPホスティングサービス実証実験 参加機関募集のご案内
- 2023/01/31 学認対応IdPホスティングサービス実証実験 参加希望連絡
- 2023/02/01 お問合せフォームを受領の返信
  
- **2023/02/15** **お申込み期限：2023年2月28日 ⇒ 2023年2月17日**  
(お申込み多数のため、早期に締め切らせていただきます。 2月15日更新)
  
- 2023/02 学認対応IdPホスティングサービス実証実験 打合せ
  
- 2023/03/07 学認対応IdPホスティングサービス実証実験 選考結果のご連絡
  
- 2023/03/08 学認対応IdPホスティングサービス実証実験 事務局と連絡開始
  - 関連サービスの申し込み手続き
  - SP接続先の検討
    - GakuNin RDMの利用申請
    - 機関ストレージの設定
  - SP接続先の設定確認 など

# 事例紹介 | 学認対応IdPホスティングサービス ログイン画面のイメージ



# 事例紹介 | 学認対応IdPホスティングサービス IdP設定

The screenshot shows the '学認 IdP 設定' (IdP Settings) page in the GakuNin management console. The page is divided into several sections:

- Header:** 国立保健医療科学院 (National Institute of Public Health), 上野 悟 (Ueno Hiroshi), and 管理コンソール (Management Console).
- Navigation:** ユーザー (Users), グループ (Groups), アプリケーション (Applications), ログ (Logs), ダウンロード (Downloads), 設定 (Settings).
- Section 1:** 学認 IdP 設定 (IdP Settings) and 学認 SP 設定 (IdP SP Settings).
- Section 2:** 学認 IdP 基本情報 (Basic Information) with a button for 学認属性マッピング設定 (IdP Attribute Mapping Settings).
- Entity Information:**
  - entityID: [Redacted]
  - スコープ / schacHomeOrganization: [Redacted]
  - 機関名称(日本語): 国立保健医療科学院
  - 機関名称(英字): National Institute of Public Health
  - SAML2 シングルサインオンエンドポイント: [Redacted]
- Section 3:** 学認 IdP 証明書 (IdP Certificate) with a button for + 新しい証明書を追加する (Add New Certificate).
- Table:** A table listing certificates with columns for 表示名 (Display Name), 有効期限 (Validity Period), 状態 (Status), and 編集/削除 (Edit/Delete). One certificate is listed: 学認対応IdP証明書2023, with a status of 運用中 (In Use).
- Footer:** © 2016 EXGEN NETWORKS Co., Ltd.

The screenshot shows the '属性マッピング設定' (Attribute Mapping Settings) page in the GakuNin management console. The page is divided into several sections:

- Header:** 国立保健医療科学院 (National Institute of Public Health), 上野 悟 (Ueno Hiroshi), and 管理コンソール (Management Console).
- Navigation:** ユーザー (Users), グループ (Groups), アプリケーション (Applications), ログ (Logs), ダウンロード (Downloads), 設定 (Settings).
- Section 1:** 学認属性マッピング設定 (IdP Attribute Mapping Settings).
- Section 2:** Mapping settings for 'extic' to 'GakuNin'. The table below shows the mappings:
- Table:** A table showing attribute mappings from 'extic' to 'GakuNin'. Each row has a dropdown menu for the source attribute, a '必須' (Required) checkbox, and a dropdown for the target attribute.
- Buttons:** 保存 (Save) and キャンセル (Cancel).
- Footer:** © 2016 EXGEN NETWORKS Co., Ltd.

Source Attribute	Required	Target Attribute
niph.go.jp	必須	スコープ / schacHomeOrganization
国立保健医療科学院	必須	jaOrganizationName
National Institute of Public Health	必須	organizationName
機関内所属名称(日本語)		jaOrganizationalUnitName
機関内所属名称(英字)		organizationalUnitName
姓(日本語)		jaSurname
姓(英字)		surname
名(日本語)		jaGivenName
名(英字)		givenName
表示名		jaDisplayName
表示名(英字)		displayName / commonName
学認用メールアドレス		mail
職種, 職種2, 職種3, 職種4, 職種5		eduPersonAffiliation
マッピングしない		isMemberOf
マッピングしない		gakuNinPersonalUniqueCode

# 事例紹介 | 学認対応IdPホスティングサービス SP設定



学認 IdP 設定 学認 SP 設定

学認 SP 設定 + 新しい学認 SP 設定を追加する

表示名	エンティティ ID	編集/削除
APRIN e-learning program ( eAPRIN )	https://edu.aprin.or.jp/shibboleth-sp	<input checked="" type="checkbox"/> 学認ユーザー情報の照合 <span>編集</span> <span>削除</span>
CINii Research	https://auth.cir.nii.ac.jp/shibboleth-sp	<input checked="" type="checkbox"/> 学認ユーザー情報の照合 <span>編集</span> <span>削除</span>
GakuNin RDM 基本機能 ( アカウント管理 )	https://accounts.rdm.nii.ac.jp/shibboleth-sp	<input checked="" type="checkbox"/> 学認ユーザー情報の照合 <span>編集</span> <span>削除</span>
GakuNin RDM 管理機能 ( GakuNin RDM Admin )	https://admin.rdm.nii.ac.jp/shibboleth-sp	<input checked="" type="checkbox"/> 学認ユーザー情報の照合 <span>編集</span> <span>削除</span>
GakuNin RDM データ解析機能 ( データ解析 )	https://jupyter.cs.rcos.nii.ac.jp/shibboleth-sp	<input checked="" type="checkbox"/> 学認ユーザー情報の照合 <span>編集</span> <span>削除</span>
JAIRO Cloudから学認へのログインロキサービス	https://idp.repo.nii.ac.jp/shibboleth-sp	<input checked="" type="checkbox"/> 学認ユーザー情報の照合 <span>編集</span> <span>削除</span>
NII FileSender	https://filesender.nii.ac.jp/shibboleth-sp	<input checked="" type="checkbox"/> 学認ユーザー情報の照合 <span>編集</span> <span>削除</span>
eduroam JP 認証連携 ID サービス	https://federated-id.eduroam.jp/shibboleth-sp	<input checked="" type="checkbox"/> 学認ユーザー情報の照合 <span>編集</span> <span>削除</span>
eduroam JP 申請システム	https://office.eduroam.jp/shibboleth-sp	<input checked="" type="checkbox"/> 学認ユーザー情報の照合 <span>編集</span> <span>削除</span>
meatmail ( GakuNin mAP対応メールリストサービス )	https://meatmail.nii.ac.jp/shibboleth-sp	<input checked="" type="checkbox"/> 学認ユーザー情報の照合 <span>編集</span> <span>削除</span>
researchmap	https://researchmap.jp/shibboleth-sp	<input checked="" type="checkbox"/> 学認ユーザー情報の照合 <span>編集</span> <span>削除</span>
学認LMS	https://lms.nii.ac.jp/shibboleth-sp	<input checked="" type="checkbox"/> 学認ユーザー情報の照合 <span>編集</span> <span>削除</span>
学認クラウドゲートウェイサービス ( 学認LMSのユーザ管理 )	https://cg.gakunin.jp/shibboleth-sp	<input checked="" type="checkbox"/> 学認ユーザー情報の照合 <span>編集</span> <span>削除</span>
府省共通研究開発システム ( e-Rad )	https://www.e-rad.go.jp/shibboleth-sp	<input checked="" type="checkbox"/> 学認ユーザー情報の照合 <span>編集</span> <span>削除</span>

## IdP・SP一覧

### ■SP一覧のマニュアルおよび属性情報について

SP一覧のマニュアルおよび属性情報は、SPからの申請に基づいたものとなります。

変更があった場合には変更申請をいただくようお願いしておりますが、情報が古い場合がございます。もしそういったことがありましたら、お問い合わせフォームより学認事務局にお知らせください。SP側に確認を行い、正しいものに修正いたします。

### 運用フェデレーション

機関名称もしくはサービス名で絞り込み

### サービスプロバイダー: SP

リストされているSP数: 130

機関名称	サービス名	マニュアル ▼全て表示	属性情報	登録日	備考
Serials Solutions	360 Search, 360 Link, Electronic Journal Portal		eduPersonTargetedID (必須)	2011年3月30日	*
株式会社 エル・インターフェース	Academic Express3  The English Language Materials Bank		eduPersonPrincipalName (必須)	2018年8月17日	*
American Chemical Society	ACS Publications 		eduPersonTargetedID (選択)	2020年8月19日	*
Publishing Technology	AIP Scitation		eduPersonTargetedID eduPersonPrincipalName (上記どちらか必須)	2014年9月9日	*
Annual Reviews	Annual Reviews		不要 (IdPのentityIDをチェック)	2012年6月15日	*
一般財団法人公正研究推進協会	APRIN e-learning program (eAPRIN)		eduPersonPrincipalName (必須)	2022年2月28日	
asknet AG	asknet AG		eduPersonScopedAffiliation (必須) eduPersonAffiliation (選択)	2016年6月28日	
Masaryk University	Atlases - Pathology Images		eduPersonTargetedID (必須) mail (選択、ユーザ登録時利用)	2009年10月10日	
Atypon Systems	Atypon Service Provider		サービスごとに必要な送信属性が異なる可能性がありますので、各サービスの提供元パブリッシャーもしくは代理店にお問い合わせください。	2015年9月15日	*
一般社団法人大	AXIES Website		eduPersonPrincipalName (必須)	2020	*

<https://www.gakunin.jp/participants>

# 事例紹介 | 学認対応IdPホスティングサービス 操作ガイド (管理者編)



## 学認対応 IdP ホスティングサービス 操作ガイド

管理者編

2023 年 3 月 28 日版

学認対応 IdP ホスティングサービス事務局

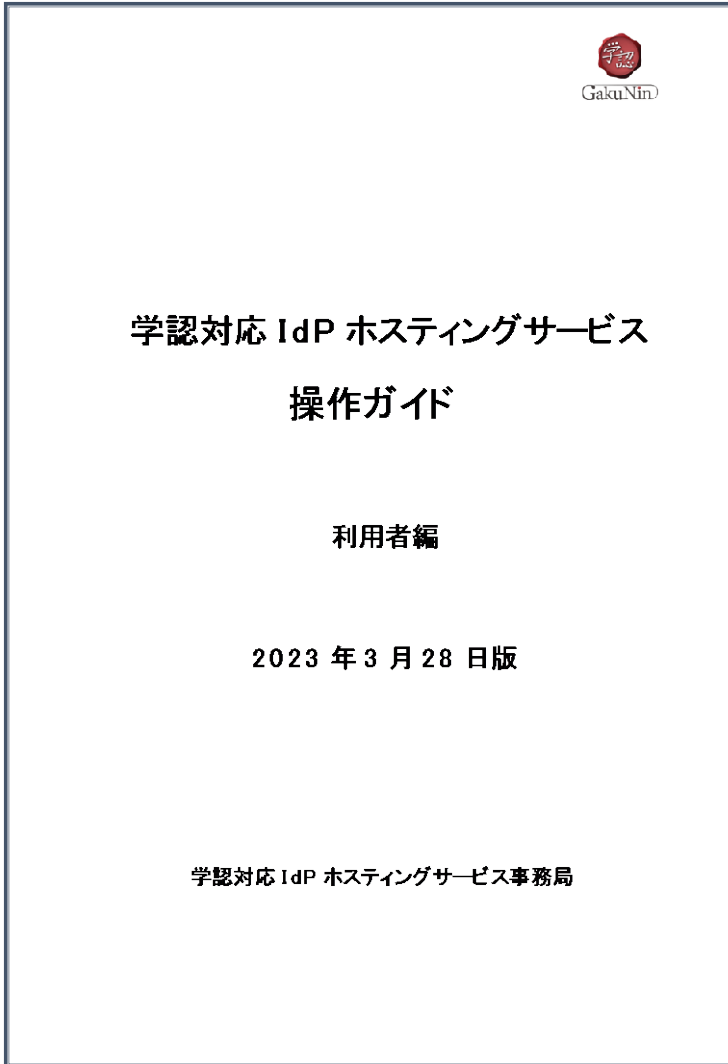


1 はじめに	1
1.1 本ガイドについて	1
1.2 管理者ユーザーの種別	1
2 基本操作	2
2.1 管理コンソールの操作	2
2.1.1 管理コンソールの表示方法	2
2.1.2 管理コンソールのメニューについて	2
2.2 契約情報の確認	3
3 基本設定	4
3.1 パスワードポリシーの設定	4
3.2 認証ルールの設定	5
3.3 表示文章の設定	6
4 ユーザーのメンテナンス	7
4.1 ユーザーの個別メンテナンス	7
4.1.1 ユーザーの追加	7
4.1.2 ユーザーの編集	9
4.1.3 ユーザーの削除	9
4.2 ユーザーの一括メンテナンス	10
4.2.1 一括メンテナンスの流れ	10
4.2.2 CSV ファイルの作成	11
4.2.3 CSV ファイルのインポート	14
4.3 ユーザーメンテナンス結果の確認	15
5 グループのメンテナンス	16
5.1 グループの概要	16
5.2 グループの個別メンテナンス	16
5.2.1 グループの追加	16
5.2.2 グループの編集	17
5.2.3 グループの削除	17
5.3 グループの一括メンテナンス	18
5.3.1 一括メンテナンスの流れ	18
5.3.2 CSV ファイルの作成	18
5.3.3 CSV ファイルのインポート	18
5.4 グループメンテナンス結果の確認	19
6 学認連携機能のメンテナンス	20
6.1 基本情報の確認	20
6.2 学認属性マッピングの設定	20



6.3 学認 IdP 証明書の管理	20
6.3.1 学認 IdP 証明書の基本情報	20
6.3.2 CSR の作成	21
6.3.3 学認 IdP 証明書のインポート	21
6.4 学認 SP の設定	22
6.4.1 学認 SP の追加	22
6.4.2 学認 SP の編集	22
6.4.3 学認 SP の削除	23
7 認証結果の参照	24
7.1 認証ログの確認	24
8 データのエクスポート	25
8.1 ユーザーデータのエクスポ	25
8.2 グループデータのエクスポ	25
8.3 連携処理ログのエクスポ	25
8.4 認証ログのエクスポ	26
9 その他操作	27
9.1 通知の設定	27
9.1.1 パスワード変更時の連携エラー通知設定	27
9.1.2 アカウント管理バッチエラー通知設定	27
9.2 CSV インポート API の設定	27
9.3 CSV ファイル文字コードの設定	28
9.4 ログイン画面パスワード表示の設定	28
9.5 SCIM API の設定	28
9.5.1 Basic 認証の設定方法	28
9.5.2 Bearer トークンの設定方法	29
9.6 パスワード通知書印刷の操作	29
9.6.1 アプリケーションの検索設定	29
9.6.2 アプリケーションのインストール方法	30
9.6.3 パスワード通知書印刷用アプリケーションの設定	30
9.6.4 パスワードの変更とパスワード通知書の印刷	31

# 事例紹介 | 学認対応IdPホスティングサービス 操作ガイド (利用者編)



GakuNin

1 はじめに	1
1.1 本ガイドについて	1
2 学認対応 IdP に初めてアクセスする方へ	2
2.1 ログインの確認	2
2.2 パスワード再発行用メールアドレスの登録	4
2.3 初期パスワードの変更	6
3 学認対応サービスの利用方法	7
3.1 学認対応サービスのログイン方法	7
3.2 学認対応サービスのログアウト方法	7
4 パスワードの再発行方法	8
5 多要素認証 (FIDO2) の利用方法 (生体認証編)	10
5.1 FIDO2 認証書の登録	10
5.2 多要素認証 (FIDO2) を使ったログイン方法	12
5.3 FIDO2 認証書の登録削除	13
6 多要素認証 (OTP) の利用方法 (ワンタイムパスワード編)	14
6.1 アプリ認証の設定	14
6.2 メール認証の設定	17
6.3 ログイン方法 (アプリ認証の例)	19
6.4 設定解除方法 (アプリ認証の例)	20

# まとめ |

## 学認対応IdPホスティングサービス実証実験を利用した感想と今後の課題

### よかったところ

1. 情報システム分野の専門部署や人材の確保が十分でなくても、導入が可能である。
2. 維持管理のための設備、人材、費用が軽減できる。
3. IdP認証により利用したい学認対応SPのサービスが使える。
  - 研究データ管理を行うGakuNin RDMが利用可能となり、データの保存、共有がよりセキュアになる。
  - 学認SPの利用により、図書館関連サービスなどの利用が増える可能性がある。
  - 研究機関外からも認証が可能となるため、出張や外勤先、テレワーク時にも利用可能となる。

### よりよくなってほしいところ

1. 機関内の認証サーバーとの連携ができないと、IDとPWが異なるので管理が大変になる可能性あり。
2. SPごとに利用申請や変更申請が異なるため、より容易に手続きができると利便性が高まる。
3. SPごとに申請期限、利用開始時期、問合せ先などが異なるため、一覧があると情報検索に助かる。
4. 実証実験に参加した施設との情報交換、事例の公開があると、参考にして取り入れやすい。

### 今後の課題

- データの利活用や利用方法、研究データ管理ポリシーを共有し、段階的に実現可能内容を整理する。
- 実際に運用を行いながら最適化を進める。
- 既存の研究データ管理からの移行、普及、体制整備などの必要性がある。
- IdPに登録できない共同研究者（例：自治体、保健所、地方衛生研究所）などの登録は別途検討中



# 謝辞 |

国立情報学研究所 学術基盤推進部学術基盤課 学術認証推進室  
学認対応 IdP ホスティングサービス担当

ご担当者様

学認対応 IdP ホスティングサービス事務局

江川 淳一 様  
舟木 俊裕 様

エイチ・シー・ネットワークス株式会社

佐藤 弘行 様

国立情報学研究所 アーキテクチャ科学研究系

清水 さや子 先生

国立情報学研究所教育研修事業  
国立情報学研究所 学術基盤推進部 学術コンテンツ課  
教育研修事業担当

ご担当者様

ご清聴ありがとうございました