<2024/04/01 バージョン>

学認対応IdPサービス調達仕様案3 [松] (IDaaS)

### 本仕様の特徴と他の仕様の比較

　学認対応IdPサービス・システム調達仕様案は4つのパターンがあり、下記の表はそれを大まかに分類したものとなる。それぞれの機関において適宜選択の上、活用いただきたい。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | IDaaS1 梅 | IDaaS2 竹 | IDaaS3 松(当仕様) | オンプレミス(IaaS等含む) |
| 学認SP対応 | ⚪️ | ⚪️ | ⚪️ | ⚪️ |
| 学認以外のSP対応(1) | × | ⚪️ | ⚪️ | ⚪️ |
| IDM(2) 構築 | × | × | ⚪️ | × |
| サーバ保護(3) | ⚪️ | ⚪️ | ⚪️ | – (4) |
| 多要素認証(5) | ⚪️ | ⚪️ | ⚪️ | ⚪️ |
| 運用支援 | ⚪️ | ⚪️ | ⚪️ | ⚪️ |

1. 機関が運用している SP のうち SAML による認証連携ができる学認SP 以外の SP に対する対応(学内 SP など)
2. ID Manager (IDM による統合的な ID 管理)
3. FIreWall, WAF(Web Application Firewall), IPS/IDS によるサーバ保護
4. プライベートクラウドや IA サーバの場合、機関に既設のネットワークセキュリティ機器を想定。IaaS などのパブリッククラウドの場合は当該パブリッククラウドの提供するセキュリティ機能による保護を想定
5. 通常の ID・PW 認証に加え TOTP(Time-based One-time Password), メールOTP, FIDO2 に対応した認証機能

本調達仕様における注意

本文中青字の記載は「学認対応IdPサービス調達仕様案1 [梅] (IDaaS)」との差分を示している。また、＜赤字＞に記載されている内容は各項目の意図などを説明している文章であり、調達仕様作成時に各組織にて確認の後に削除のこと。

学認を学内へ展開する場合の資料

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

本調達で導入するシステムは次の事項を想定している(資料1.)。

調達対象システムの特徴：

1. SaaS ベースの学認対応 IdP サービス
2. 学認 SP 以外の学内SPおよび学外SPにも対応した統合的な認証システム
3. 学内 ID 情報の統合的な管理システム(IDM システム)
4. 1. 2. 3.に係る構築と運用管理
5. TOTP、メールOTP、 FIDO2 に対応した認証機能
6. 人事・学務システムとの ID 情報連携機能(IDM がある場合は IDM との連携機能)
7. WAF など IdP システムに対するセキュリティ対策

構築にあたっての前提条件(機関で準備しておく事柄)：

1. 人事・学務システムにおいて大学規定の手続きにより適切に教職員・学生が登録・管理されていることを想定している(Trusted DB は IAL2 相当で運用されていると想定)
2. 人事・学務システムから本調達に含む ID管理システム連携するための仕組みがある

＜2. の仕組みがない場合は、別途開発・調達する(本調達仕様では記述していない)＞

費用に関する条件：

1. 初期導入における設計・設定・構築費用
2. ライセンス費用(月・ユーザ単位で毎年必要)
3. 運用支援が必要な場合は、運用支援を含む保守契約(毎年必要)

### 本調達仕様における調達範囲



＜以上までは、調達にあたっての前提条件などであり、以下より調達仕様本文となる＞

### 調達システムの概要

　国内においては、学術雑誌のオープンアクセス化が進められており、日本学術振興会(JSPS)等の下での研究においても RDM やオープンアクセスが求められつつある。また、国外においては欧州連合(EU)の政策として、例えば Horizon Europe などの研究プログラムにおいて、研究成果のオープンアクセス化が義務付けられるようになった。さらにアメリカ国立衛生研究所(NIH)や国立科学財団(NSF)などが、公的資金による研究成果のオープンアクセス化を推進している。このような背景から、本学においても、研究データ管理(RDM)および研究データ管理計画(DMP)に対応するとともにし、研究論文や研究データのオープンアクセス(OA)に対応することで、研究力の質的な向上を目指している。

　この RDM や DMP、および研究論文や研究データのオープンアクセスに適切に対応するためには、研究に関わる全ての論文やデータを、それぞれの研究に携わる研究者の下で適切に管理する必要があり、このためには研究に携わる研究者個人の所属や本人性を組織が保証する形で認証し認可する必要がある。しかしながら、従来からのアドホックな利用者管理や脆弱なパスワードのみに基づく認証システムを用いた場合、特にオープンアクセスにおいて、信頼性や追跡性などの問題が生じる。これに対し、学術認証フェデレーション「学認」は、世界基準での一定の運用基準を定めており、この基準に基づいた認証システムを運用することで信頼性や追跡性が確保されるとともに、「学認」に対応している GakuNin RDM および JAIRO Cloud (OA)を活用することにより、コストを抑えつつ研究データ管理・公開基盤システムを導入することができる。

　この学認は、大学の認証基盤を学内サービスのみならず、連携する他大学や商用サービスにも活用するための仕組みである。インターネット上の学術サービスを、大学による契約の下で、個人やその所属機関を保証する形で安心・安全に提供および利用することができる。さらに、シングルサインオンの機能も提供されることにより、利用者は一度ログインするだけで、学内・学外の複数のサービスにシームレスにログインができる。一方大学にとっても、学認に対応した認証基盤を構築することで、アカウント管理やセキュリティ対策を集約することができるため、ID管理工数の軽減やセキュリティ対策レベルの底上げを実現できる。

　本調達は、本学がこの「学認」に参加し学認対応 IdP を構築・運用することで、適切な研究データ管理やオープンアクセスを実現するとともに、学内における認証基盤の整備を実現するものである。

### 学認対応IdPの提供方法

学認参加時に必要となる IdPサーバを IDaaS（Identity as a Service）として提供すること。IDaaSの提供においては、以下のユーザ数を実現すること。

 ・ 総ユーザ数：10,000

 ・ 対応な SP 数：50

＜各大学にて必要な人数、SP数に修正する必要がある。年度変わりなどに不足しないように考慮すること。＞

### 用語

* Trusted DB : 本学における人事・給与に関するシステムが有する人事・給与 DB と学務に関するシステムが有する学生 DB
* 管理者 : 本学のID情報に関する管理業務担当者
* 利用者 : 教職員及び学生

### 機能要件

1. 学認対応IdPサービス

1.1 SAML 2.0 の認証連携機能を有し、利用者が学認 SP を含む複数の SAML に対応した複数の学認 SP に対してシングルサインオンする機能を有すること。

＜学認IdPにて学認SP以外のSPも対応するように記述している。資料 1., 3.＞

1.2 送信属性同意画面

1. 利用者の認証時、学認 SP への送信属性同意画面が表示機能を有すること。

 2. 2度目以降の認証時における送信属性同意画面の表示または非表示は、利用者による選択機能を有すること。

1.3 認証フローにおける暗号署名処理に利用するデジタルサーバ証明書管理

 1. 学認対応 IdP で利用するデジタルサーバ証明書の管理機能を有すること。

 2. 学認対応 IdP で利用するデジタルサーバ証明書発行のための CSR(Certificate Signing Request : 署名リクエスト) の作成機能を有すること。

1.4 学認SP管理について管理者が、学認SPの追加、変更、削除の設定をすることができること。

1.5 新規参加 SP、SP の更新 (必須属性や証明書の変更など)、SP の学認からの解約に対応するため、定期的に SP メタデータを取得できること。

1.6 学認SPとの連携実績として、学認対応機能を有する IDaaS として、学認 SP との連携実績があること。

1.7 利用者の利用場所(IP アドレス)により、以下の認証方式の選択、またはアクセス禁止の設定を組み合わせて設定できること。

 1. パスワード認証

 2. 多要素認証

 3. 多段階認証

1.8 多要素認証として以下の多要素認証機能を有すること。

 1. TOTP(Time-based One-time Password : タイムベースドワンタイムパスワード)による認証機能を有すること。

 2. 事前に登録された利用者のメールアドレスに対して送信した確認コードによる認証機能を有すること。

 3. パスワードレス認証方式として、FIDO Alliance によって規格化された FIDO2 (Fast IDentity Online 2) の認証機能を有すること。

＜必要に応じて具体的な認証方式、例えば生体認証などの認証方式を記述しても良い。＞

1.9 管理者が以下の設定及び確認機能を有すること。また管理者が行う初期設定として、利用者に対して以下の設定に基づく認証方式を指定可能なこと。認証方式は 1.8 に示すものとする。

 1. 利用者ごとの多要素認証の強制設定機能を有すること。

 2. 利用者が多要素認証を設定済みであるかの確認機能を有すること。

 3. 利用者の多要素認証設定の解除機能を有すること。

＜利用者の認証フローを想定・確認して具体的に記述しても良い。＞

1.10 外部 IdP 連携機能(認証プロキシ)として他の IdP に対して SAML を利用し認証機能を委譲できること。

＜本項目は機関がすでに IdP を運用しており、その IdP を利用することを想定している。利用可能な IdP がない場合は本記載は削除してよい。＞

1.11 認証用IdPサーバは冗長化されていること。

＜Active-Active や Active-Standby 方式、DC・リージョンを変えるなど様々な方式があるため各機関で最適なものを記述すること。＞

2. 学認対応IdPサービス用認証IDデータベース

2.1 学認対応IdPサービス用データベースについて、学認SPの認証用のID情報を保持するデータベース(以下「認証用データベース」)を有すること。また、学認SP以外の SAML に対応している SP に対応した認証用データベースも有すること。なお、当該認証用データベースは同一でもよい。ID情報は、本学の構成員である利用者の識別子、および、属性情報で構成される。

＜学認IdPにて学認SP以外のSPも対応するように記述している。資料 1., 3.＞

2.2 属性情報の管理と拡張性を確保するため、学認SPの認証用データベースの属性情報について、本学のID情報に関する管理業務担当者(「管理者」)が任意に拡張し、管理することができること。

2.3 ID情報を格納するデータベースは冗長化されていること。

＜Active-Active や Active-Standby 方式、DC・リージョンを変えるなど様々な方式があるため各機関で最適なものを追記すること。＞

3. ID 管理サービス

＜ID 情報を統合的に管理するシステムやサービスを想定している。＞

3.1 プロビジョニング機能

3.1.1 ID 情報は、Trusted DB における追加、変更、削除、および、管理者、利用者がメンテナンスを行った際、以下のデータベースに対して連携(プロビジョニング)することができること。

 1. 「2. 学認対応IdPサービス用認証IDデータベース」

 2. 本学の既設のディレクトリサービス

＜ActiveDirectory や LDAP による認証システムを想定している＞

 3. 学内、および、学外の SP

＜2. 3. は資料を作成して具体的にどのシステムやサービスに対して連携したいのかリストを作成すること。＞

3.1.2 管理者は、「4. ID 管理サービス ID 管理用データベース」の情報と、3.1.1 に記載した対象の ID 情報にかかる属性情報の連携について、管理面でのマッピングによる設定ができること。

3.1.3 プロビジョニングの結果はログ情報として記録されること。

3.2アクセス権限の設定として、 ID 管理ポリシーに応じて、管理者と利用者で権限を分けることができること。また、必要に応じて権限の見直しが可能な機能を有すること。

＜管理者と利用者の細かな権限設定の内容は、各大学にて検討の上決定すること。＞

3.3 Trusted DB との連携

3.3.1 本学における人事・給与に関するシステムが有する人事・給与 DB、および、学務に関するシステムが有する学生 DB (「Trusted DB」) に登録されたアカウント情報と連携し、管理者は利用者の ID 情報を追加、変更、削除する機能を有すること

＜利用者ID情報の追加、変更、削除する機能については、原則的には本調達サービスシステムで行うのではなく、源泉となるTrusted DBで行うように連携することが望ましい。＞

3.3.2 「5. 学認対応IdPサーバログ管理機能」において、Trusted DBとの連携処理のログ情報が取得されること。

3.3.3 Trusted DB との連携は以下の方法で連携すること。

 ＜ID の連携が、自動連携であるのか手動連携なのかによって選択が必要となる。本仕様書は自動連携と手動連携が可能なように記述している。1. が手動連携、2. が自動連携となる＞

 1. CSV ファイル

 2. SCIM API

 なお、本学の ID 基盤は「別紙1 想定するシステム構成(概要)」に示す構成となる。

＜1. CSV ファイルについて、他の形式(TSV, XML, JSON 形式など)の場合は導入を予定する IDaaS の対応状況を調査の上決定すること。＞

3.4 ID 情報検索機能において、管理者は、利用者の ID 情報および、属性情報をフィルタ条件として、検索を行う機能を有すること。

3.5 ID 情報エクスポート機能として、管理者は、利用者の ID 情報を CSV ファイル形式でエクスポートする機能を有すること。

3.6 ID のライフサイクル管理機能として、指定日に自動的に有効化、無効化、削除する機能を有すること。

3.7 利用者属性情報管理機能として、利用者は、自身の ID 情報をメンテナンスする機能を有すること。なお、利用者が管理可能な ID 情報については、本学担当者と協議の上決定すること。

＜利用者自身が管理可能な ID 情報となるので、変更可能な ID 情報を適切に選定すること。＞

3.8 パスワードポリシー設定機能として、以下のパスワードポリシーを設定可能な機能を有すること。

 1. パスワードの長さにおける最小文字数と最長文字数

 2. 入力必須文字タイプ

 3. 入力許可文字

 4. 入力禁止属性(属性情報として格納されている文字列を禁止する)

 5. 認証の失敗回数が指定回数に達した場合のアカウントロック設定

 6. アカウントをロックする期間

 7. パスワード有効期限切れ前に通知する機能

 8. パスワード有効期限

 9. 過去に設定したパスワードの再利用を禁止する設定(5世代以上)

 10. 管理者がアカウントロック状態を確認でき、ロック状態を解除できること

3.9 パスワードリセット機能

 利用者がパスワードを忘れた場合、以下のいずれかの方法でパスワードをリセットできる機能を有すること。

 1. 管理者によるパスワードの再設定

 2. 利用者自身によるパスワードの再設定

＜再設定フローを想定・確認して具体的に記述しても良い。＞

4. ID 管理サービス ID 管理用データベース

＜ID 管理サービスのデータベースを想定している。＞

4.1 ID 管理用のデータベースとして、本学の ID 情報に関する管理者や利用者がメンテナンスを行うことができるデータベースを有すること。ID 管理サービス ID 管理用 データベースの ID 情報は、「3.3 Trusted DB 」との連携を源泉とし、「2. 学認対応IdPサービス用認証IDデータベース」および 3.1.1 に記載したサービスやシステムに対してプロビジョニング連携を行うこと。

4.2 属性情報の管理と拡張性を確保するため、ID 管理サービス ID 管理用データベースの属性情報について、本学のID情報に関する管理者が任意に拡張し、管理することができること。

4.3 ID 情報を格納するデータベースは冗長化されていること。

＜Active-Active や Active-Standby 方式、DC・リージョンを変えるなど様々な方式があるため各機関で最適なものを追記すること。＞

5. ID 管理サービスログ管理機能

5.1 ID 情報操作ログ機能として、以下の機能を実現できること。

＜ログの保存期間については各大学のポリシー等に照らし合わせて指示すること。＞

 1. 管理者が実施した利用者の ID 情報の追加、変更、削除処理に対するログや、利用者による ID 情報操作処理に対するログを記録する機能を有すること。

 2. 1. の記録について、 管理者は全ての記録について、利用者は自身の記録について、検索、参照する機能を有すること。

 3. 管理者は 1.の情報を CSV ファイル形式でエクスポートする機能を有すること。

5.2 認証ログ機能として、以下の機能を実現できること。

＜認証操作における認証ログとは、利用者の行ったログインやログインの結果などを記録したログのことを指す。＞

 1. 管理者は利用者の認証操作に関するログを取得し、検索、参照することができること。

 2. 管理者は 1.の情報を CSV ファイル形式でエクスポートする機能を有すること。

6. 利用者画面機能

6.1 管理者はログイン画面のロゴが変更できること。

6.2 ログイン画面は日本語と英語表記に対応すること。

6.3 ログイン前において、管理者がメッセージを表示設定可能な機能を有すること。

6.4 RFC 8446 に準拠した TLS 1.3 以上に対応したログイン画面であること。

＜TLS 1.2 以上とする場合は RFC 5246となる。＞

7. システム監視サービスとネットワークセキュリティサービス

7.1 システム監視サービスとして、「1.学認対応 IdP サービス」における認証機能、「2. 学認対応IdPサービス用認証IDデータベース」、「3. ID 管理サービス」、「4. ID 管理サービス ID 管理用データベース」、「5. ID 管理サービスログ管理機能」に対して、以下のシステム監視サービスを 24時間365日で実施できること。

7.1.1 死活監視

 1. IP アドレス、ポート、URL に対する死活監視を行うこと。

 2. サーバレスプラットフォームの場合は、1.に相当する監視の結果を確認できること。

7.1.2 リソース使用率監視

 1. CPU 使用率、メモリー使用率、ディスク使用率等について閾値を設けた監視を行うこと。

 2. サーバレスプラットフォームの場合は、1.に相当する監視の結果を確認できること。

7.1.3 サービス、プロセス監視

 1. ログ機能や監視ツールによりサービス、プロセスの監視を行うこと。

 2. サーバレスプラットフォームの場合は、1.に相当する監視の結果を確認できること。

7.2 ネットワークセキュリティサービスとして、「1.学認対応 IdP サービス」における認証機能、「2. 学認対応IdPサービス用認証IDデータベース」、「3. ID 管理サービス」、「4. ID 管理サービス ID 管理用データベース」、「5. ID 管理サービスログ管理機能」に対して、以下のネットワークセキュリティサービスを 24時間365日で実施できること。

 1. ファイアウォール機能

 2. WAF 機能

 3. IDS/IPS 機能

＜ファイアウォール機能やIPS/IDS については UTM にまとめても良い。また各セキュリティ機能についてはポリシーを協議の上決定することが望ましい。＞

### 非機能要件

8. IDaaS の設計・設定作業と接続テスト

8.1 以下に示す設計・設定作業を実施すること。

 1. 属性情報の設計と設定

 2. パスワードポリシーの設計と設定

 3. ポリシーに応じた認証方法の設計と設定

 4. 学認SP (資料2.) への送信属性の設計と設定

 5. サーバ証明書の設計と設定

 6. 本学の既設のディレクトリサービスへの接続設定

 7. 本学の既設のディレクトリサービスへの ID 情報のプロビジョニング設計と設定

 8. 学内・学外SP (資料3.) への接続設定

 9. 学内・学外SP (資料3.) への送信属性の設計と設定

 10. 学内・学外SP (資料3.) への ID 情報のプロビジョニング設計と設定

＜学認IdPにて学認SP以外のSPも対応するように記述している。資料 1., 3.＞

8.2 認証における接続テストにおいて、本学が利用する学認SP (資料2.)、および、学内・学外SP(資料3.)との接続テストを実施すること。

＜学認IdPにて学認SP以外のSPも対応するように記述している。資料 1., 3.＞

8.3 プロビジョニングにおける ID 情報連携テストにおいて、本学が利用する学内・学内SP、および、ディレクトリサービスとのプロビジョニングテストを実施すること。

9. 学認参加及び学認 SP 利用申請手続きの支援業務

＜本作業は基本的には機関担当者が実施するものであるため、本業務はそのための支援となる。＞

9.1 学認参加申請手続きの支援業務として、本調達で手配した IDaaS を本学の IdP として、学認へ参加するための設置申請手続きを支援すること。

9.2 学認 SP 利用申請手続きの支援業務として、学認 SP を利用するための SP 利用申請方法の調査や申請の手続きを支援すること。

10. 設計・設定フェーズの技術支援

10.1 設計・設定に関する本学からの問い合わせに対応すること。

10.2 問い合わせは主にメール等の予め決定したコミュニケーションツール及び電話で対応すること。

＜コミュニケーションの方法については協議の上決定すること。＞

10.3 問い合わせ受付時間帯は平日 9:00～17:30 とすること。

10.4 問い合わせを受けた際には、1営業日以内に一次回答を行うこと。回答期限については、本学担当者と協議の上、期限を取り決めること。

10.5 問い合わせについては対応リストを作成し、指定の場所に保存し、情報共有を行うこと。

10.6 IDaaS、ID 管理、および、認証処理に関する操作説明会を実施すること。

11. 運用支援

11.1 サービス利用開始後、ID 管理、認証処理、システムセキュリティ、脆弱性等に関する本学からの技術的な問合せに対応すること。

11.2 問い合わせは主にメール等の予め決定したコミュニケーションツール及び電話で対応すること。

＜コミュニケーションの方法については協議の上決定すること。＞

11.3 問い合わせ受付時間帯は平日 9:00～17:30 とすること。

＜着手までの時間や、復旧対応までの時間制限が必要な場合は、関係者と協議の上、時間数などを追記すること。＞

11.4 IDaaS および IDaaS のプラットフォームサービスで障害が発生した場合は本学に告知し、復旧対応を行うこと。

＜通知までの時間や、復旧対応までの時間制限が必要な場合は、関係者と協議の上、時間数などを追記すること。＞

11.5 IDaaS および IDaaS のプラットフォームサービスでのバグフィックス、セキュリティアップデートに対応すること。本要件対応のためのメンテナンス作業は事前の告知を行い実施すること。

11.6 問い合わせについては対応リストを作成し、本学指定の場所に保存し、情報共有を行うこと。

＜問い合わせリストの形式については、運用開始までに協議し決定しておくこと。＞

＜本サービスの要不要については検討の上決定すること。＞

11.7 四半期毎に一回の定期連絡協議会を設けること。また、定期連絡協議会のために報告書を作成すること。

＜本協議会の要不要については検討の上決定すること。＞

11.8 認証サーバ証明書を更新すること。更新作業については本学担当者と協議の上、決定すること。

＜本件の要不要は、各大学において判断すること。＞

＜任意の学認 SP 登録・設定作業を運用支援で行う場合は次の項目を追加すること。

11.x 本サービス導入後において発生する本学が指定する学認 SP について、送信属性の設計と設定、および、接続テストを実施すること。

＞

12. ドキュメント作成

12.1 ID 情報メンテナンス手順書を作成すること。

12.2 学認 SP を追加する手順書を作成すること。

＜学認 SP 以外の SP を追加する場合の手順が必要な場合は追記すること。なお、学認 SP 以外の SP の設定手順は一般化されておらず手順書の作成は難しい。＞

13. ISMS

 ISO27001 および 27017 等の ISMS 基準を取得していること。なお、これらを部署単位で取得している場合は、本件の主な請負者が所属する部署で取得されていること。

## 資料1. 想定するシステム構成(概要)

****

## 資料2. 初期設定対応が必要となる学認SP

* JAIRO Cloud
* GakuNinRDM
* eduGAIN(フェデレーション)

## 資料3. 初期設定対応が必要となる学内・学外SP(学認SP以外のSP)

* Google WorkSpace
* Microsoft 365

### 関連する閣議決定・政府方針

内閣府、「公的資金による学術論文等のオープンアクセスの実現に向けた基本的な考え方（案）」を公表：公的資金を受けた学術論文等の即時オープンアクセス実現に向けた提言

<https://current.ndl.go.jp/car/194593>

第6期科学技術・イノベーション基本計画

<https://www8.cao.go.jp/cstp/kihonkeikaku/index6.html>

研究ＤＸ（デジタル・トランスフォーメーション）

<https://www8.cao.go.jp/cstp/kenkyudx.html>

「公的資金による研究データの管理・利活用」の項目参照