学認対応IdP標準仕様書と活用

2024.6.12

学術基盤推進部 学術基盤課 学術認証推進室

学認対応 IdP 標準仕様書とは？

学認に参加するにあたり構築が必要となる学認対応 IdP を構築・運用するための仕様書

- 2023年度 学認対応IdPホスティング実験実証の結果を受けて作成
- IDaaS版(松竹梅)・オンプレミス版を用意
- 信頼性の高いデータベースから ID を生成
- 学内外 IdP を統合しているバージョンとしていないバージョン
- ID 管理サービス・システムを意識している(無くても問題ない)

学認をとりまく状況

- RDM(DMP)対応：GakuNinRDM
- Green OA(論文・データのオープンアクセス)対応：JAIRO Cloud
  OA 加速化事業(論文・データのセルフアーカイブの促進 -> 信頼度の高い研究者 ID が必要となる)

学認をとりまく状況・OAに関連する閣議決定など

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

学認対応 IdP 標準仕様書の種類

お知らせ ->[図書館職員向け即時OA（オープンアクセス）を支える認証に関するページの公開について](https://www.gakunin.jp/news/20240405)
https://www.gakunin.jp/news/20240405

- 2024年度
- 2023年度
- 2022年度
- 2021年度
- 2020年度
- 2019年度
- 2018年度
- 2017年度
- 2016年度
- 2015年度
- 2014年度
- 2013年度
- 2012年度
- 2011年度

図書館職員向け即時OA（オープンアクセス）を支える認証に関するページの公開について

2024-04-05 11:27 by 中川

平素より本サービスの運営にご協力頂きありがとうございます。学認事務局です。

このたび、オープンアクセスを担当される図書館の皆さま向けに、【即時OA（オープンアクセス）を支える認証について】
として，即時OAの実現と，それを支える「学認」に関して解説するページを作成しましたので，お知らせいたします。
公開ページ：（図書館職員向け）即時OA（オープンアクセス）を支える認証について

なぜ学認が即時OAを支えると言えるのか，学認参加を実現するための学内説明資料のひな形，学認対応に必要なIdPと呼ばれるサーバを構築するための仕様書案などを公開しておりますので，ぜひご活用いただけますと幸いです。

本件に関する連絡先：
==========
国立情報学研究所　学術基盤課　認証基盤・クラウド推進チーム（認証担当）
お問い合わせフォーム：https://www.gakunin.jp/contact
==========

学認対応 IdP 標準仕様書の種類

- 概要
  - 外部との連携と利便性の向上に向けて
  - 広報・普及活動
  - （図書館職員向け）即時OA（オープンアクセス）を支える認証について
- 運営体制
- Shibbolethによる学術認証フェデレーションへの参加メリット

（図書館職員向け）即時OA（オープンアクセス）を支える認証について

このページは、オープンアクセスを担当される図書館の皆さまに向け、即時OAを支える認証について情報をまとめたものです。

学術認証フェデレーション「学認」に参加いただくことで、大学等における即時OAの効果的な実現が期待されます。
資料1は、なぜそのように言えるか説明します。
資料2は、学認参加について学内で合意を得るための説明資料雛形です。
資料3は、学認参加に必要となる学認対応IdPを調達するための仕様案で、4つのパターンを示しています。
（※学認対応IdP自体は調達せず、独自に構築することも可能です。）

資料2及び3は、各大学等の事情に合わせカスタマイズして利用いただくことを想定しています。
また、皆さまからのご意見や各種動向等を踏まえ、このページ及び資料は随時改訂等することを想定しています。

1. 図書館員のみなさまへ
「なぜオープンアクセスの話に学認が出てくるんだろう？」と疑問を持っているみなさまに聞いていただきたい即時OAを支える認証のおはなし

2. 学認参加のための学内説明用資料雛形(令和6年度版)

3. 学認対応IdPサービス調達仕様案
・IDaaS編
　[梅]　※比較的コンパクトに調達する場合
　[竹]　※中庸的に調達する場合
　[松]　※多くの機能を盛り込んで調達する場合
・オンプレミス編

https://www.gakunin.jp/fed/732

学認対応 IdP 標準仕様書の種類

	IDaaS1 梅	IDaaS2 竹	IDaaS3 松	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

学認対応 IdP 仕様書の読み方 (共通)

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**
＜赤字＞の記載は各項目の意図などを説明しており、**調達仕様作成時に各組織にて確認の後に削除**

例：IDaaS (松) からの抜粋：

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

赤字：各機関で注意することを記述している

青字：IDaaS (梅)との差分があることを示している

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

学認対応 IdP 仕様書の読み方 (梅)

調達対象システムの特徴：

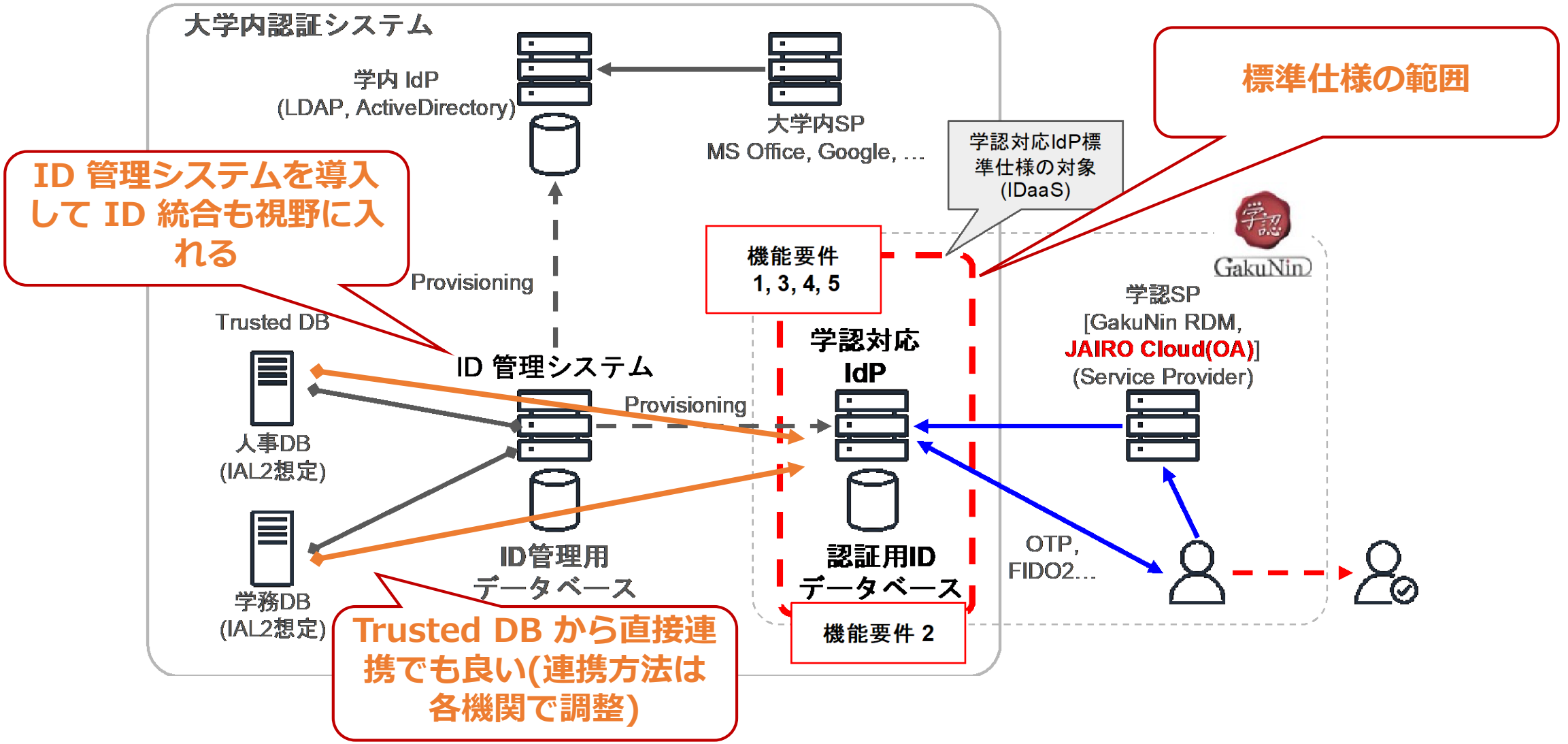
1.SaaS ベースの学認対応 IdP サービス
2.1. に係る構築と運用管理
3. TOTP、メールOTP、 FIDO2 に対応した認証機能
4.人事・学務システムとの ID 情報連携機能(IDM がある場合は IDM との連携機能)
5.WAF など IdP システムに対するセキュリティ対策

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.学内 ID 情報の統合的な管理システム(ID 管理システム)、または人事・学務システムから、学認対応IdPサービスに教職員や学生の ID 情報を連携またはプロビジョニングする仕組みがある

＜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)＞

学認対応 IdP の基本構成(梅)



学認対応 IdP 仕様書の読み方 (竹)

調達対象システムの特徴：

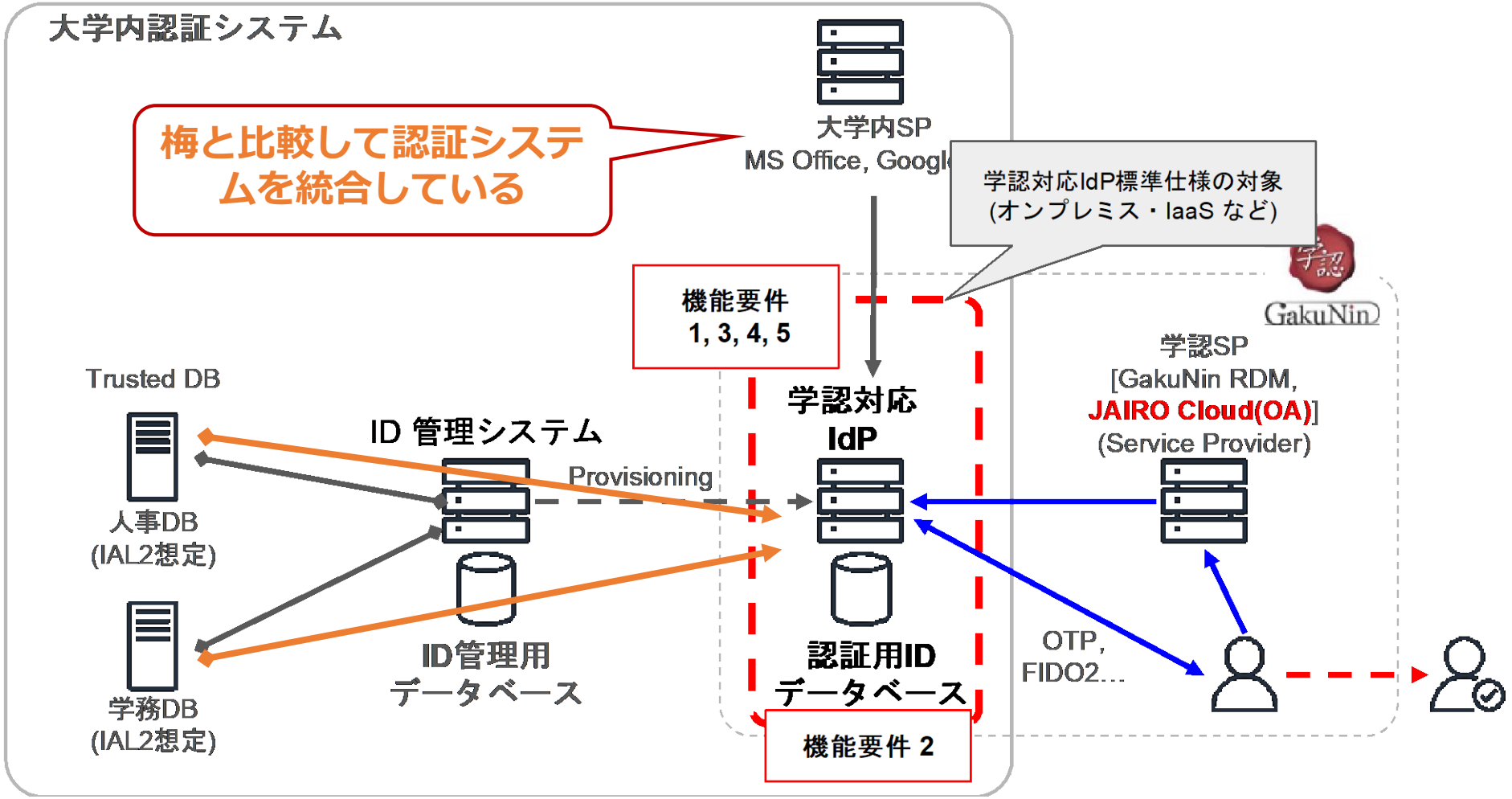
1.SaaS ベースの学認対応 IdP サービス
2.学認 SP 以外の学内SPおよび学外SPにも対応した統合的な認証システム
3.1. 2.に係る構築と運用管理
4. TOTP、メールOTP、 FIDO2 に対応した認証機能
5.学内人事・学務システムとの ID 情報連携機能(IDM がある場合は IDM との連携機能)
6.WAF など IdP システムに対するセキュリティ対策

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.学内 ID 情報の統合的な管理システム(ID 管理システム)、または人事・学務システムから、学認対応IdPサービスに教職員や学生の ID 情報を連携またはプロビジョニングする仕組みがある

<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)>

学認対応 IdP の基本構成(竹)



学認対応 IdP 仕様書の読み方 (松)

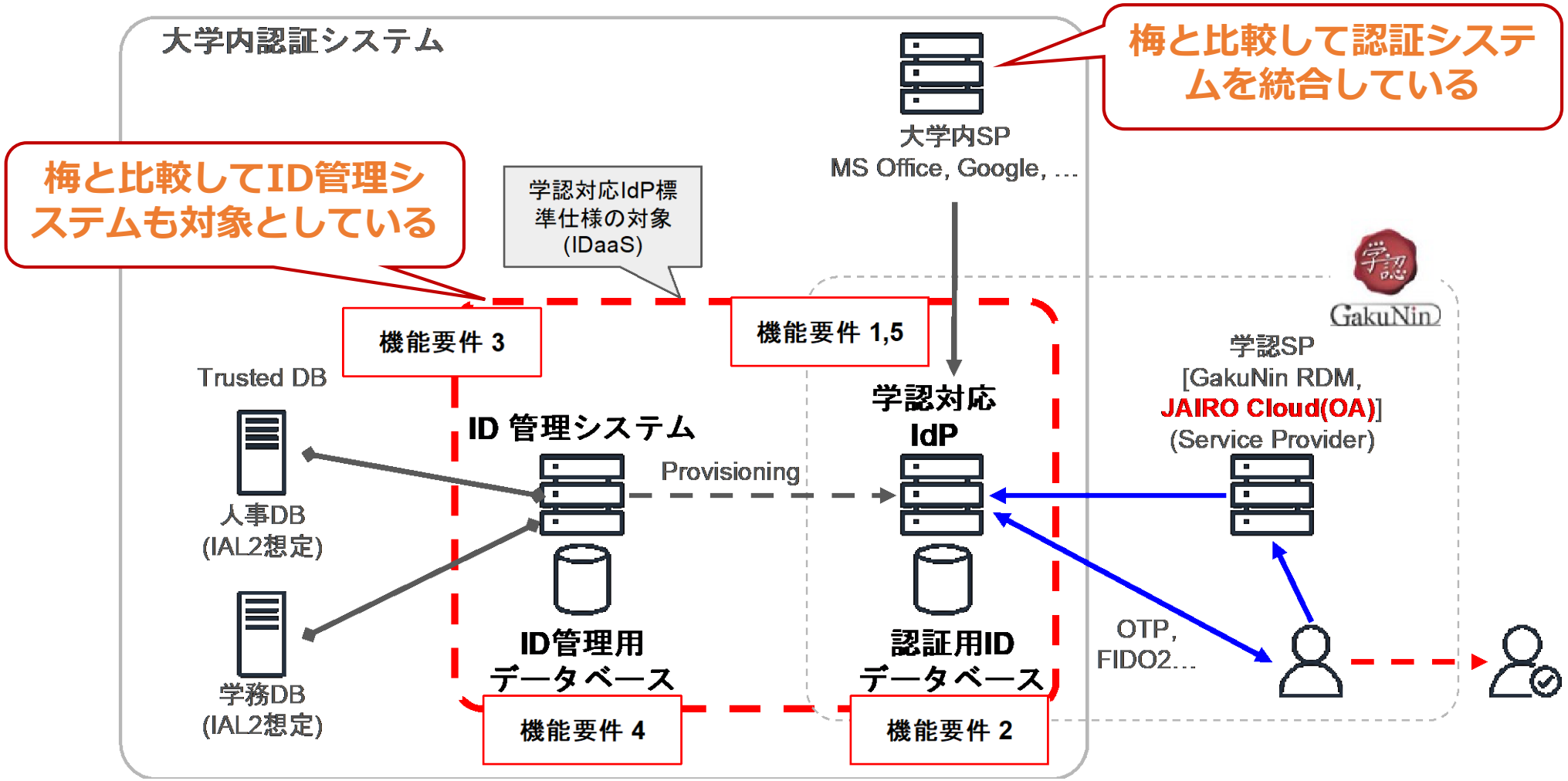
調達対象システムの特徴：

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)＞

学認対応 IdP の基本構成(松)



学認対応 IdP 仕様書の読み方 (オンプレミス・IaaS版)

調達対象システムの特徴：

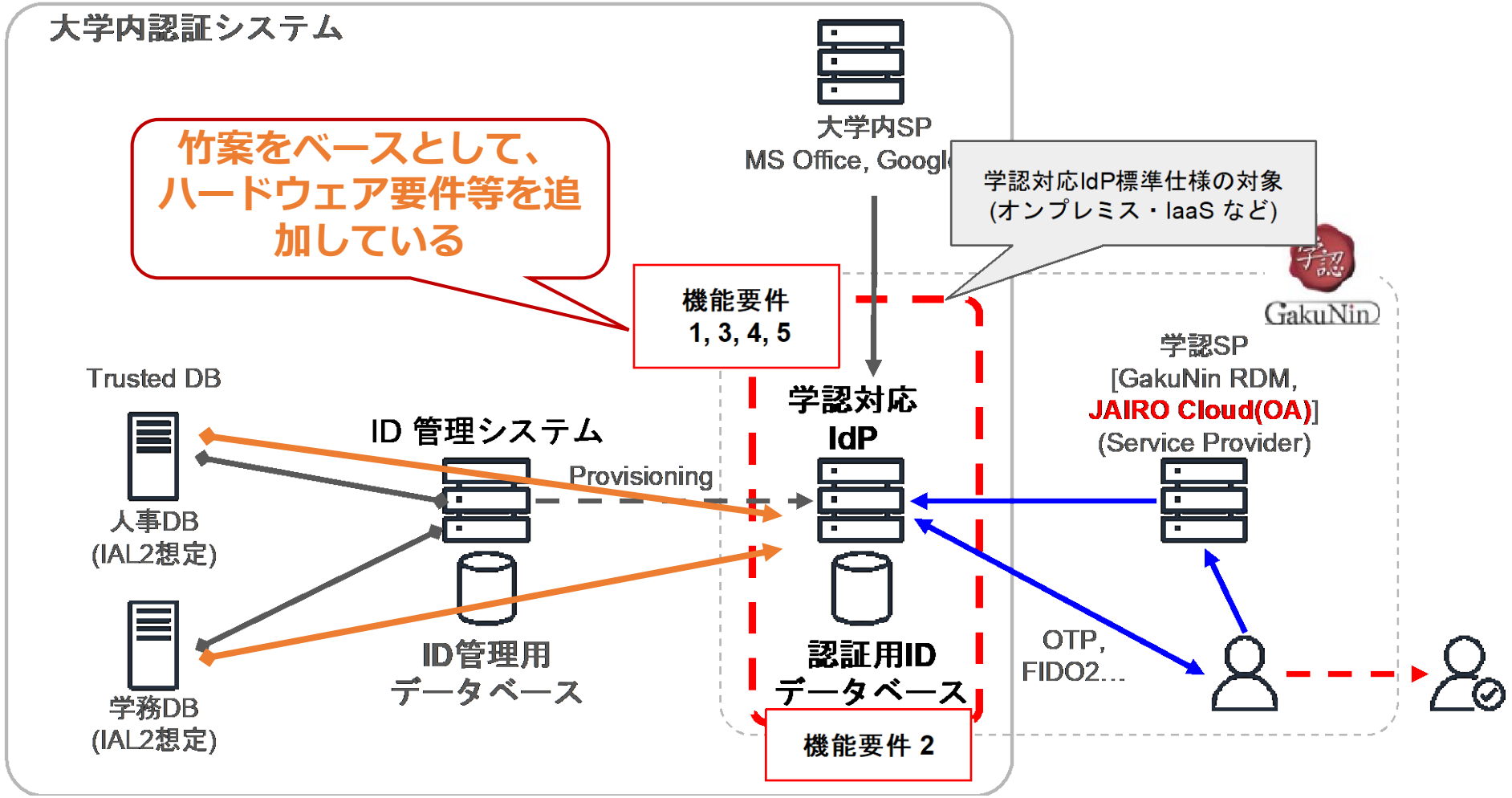
1.オンプレミス、IaaS、PaaS ベースの学認対応 IdP システム
2.学認 SP 以外の SAML 対応の Web サービスにも対応した統合的な認証システム
3.1. 2.に係る構築と運用管理
4. TOTP、メールOTP、 FIDO2 に対応した認証機能
5.人事・学務システムとの ID 情報連携機能(IDM がある場合は IDM との連携機能)
6.syslog 形式で syslog サーバにログを転送できるので、SIEM 等で解析を実施可能

構築にあたっての前提条件(機関で準備しておく事柄など)：

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.学内 ID 情報の統合的な管理システム(ID 管理システム)、または人事・学務システムから、学認対応IdPサービスサーバに教職員や学生の ID 情報を連携またはプロビジョニングする仕組みがある
3.仮想基盤(パブリッククラウド(IaaS, PaaS)、プライベートクラウド)または、学内の IA サーバ基盤があり、その上で本システムを構築可能である
4.UTM・WAF など IdP システムに対するセキュリティ対策装置は既設の装置を利用
5.導入においては1つの機能を複数のサーバで分散処理することで実現してもよい

＜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)＞

学認対応 IdP の基本構成(オンプレミス・IaaS)



学認対応 IdP 標準仕様と関連情報

（図書館職員向け）即時OA（オープンアクセス）を支える認証について

https://www.gakunin.jp/fed/732

- 1. 図書館員のみなさまへ
  「なぜオープンアクセスの話に学認が出てくるんだろう？」と疑問を持っているみなさまに聞いていただきたい即時OAを支える認証のおはなし
- 2. 学認参加のための学内説明用資料雛形(令和6年度版)
- 3. 学認対応IdPサービス調達仕様案
  - IDaaS編
    [梅]　※比較的コンパクトに調達する場合
    [竹]　※中庸的に調達する場合
    [松]　※多くの機能を盛り込んで調達する場合
  - オンプレミス編

- [お問合せもこのページに掲載]

まとめ

- 学認対応IdP標準仕様書を公開しました
- 各機関で利用する場合、適宜修正や改造等行って大丈夫です

- 論文の OA 化に伴いセルフアーカイビングが重要になります
- OAは各大学で対応が必要となりますが、信頼性の高い研究者IDでの公開が重要となりますので、学認をご活用ください