GakuNin RDMを使うには？学認のしくみと始め方をやさしく解説

NII オープンフォーラム2025

2025.6.18

国立情報学研究所
トラスト・デジタルID基盤研究開発センター
学術基盤推進部 学術基盤課 学術認証推進室
鈴木 彦文

アウトライン

1. そもそも認証ってなに？　統合認証って？
2. 学認ってなに？
3. RDM で認証がないとどうなるの？
   - 信頼性の高い認証システムがないと・・・
   - 認証基盤の整備と RDM, OA
4. システム的にはどんな感じ？
5. 導入しろと言われても仕様書書くの面倒なんだけど・・・、
   いくらかかるか分からんし・・・
   - 学認対応IdP 標準仕様書
   - 価格表

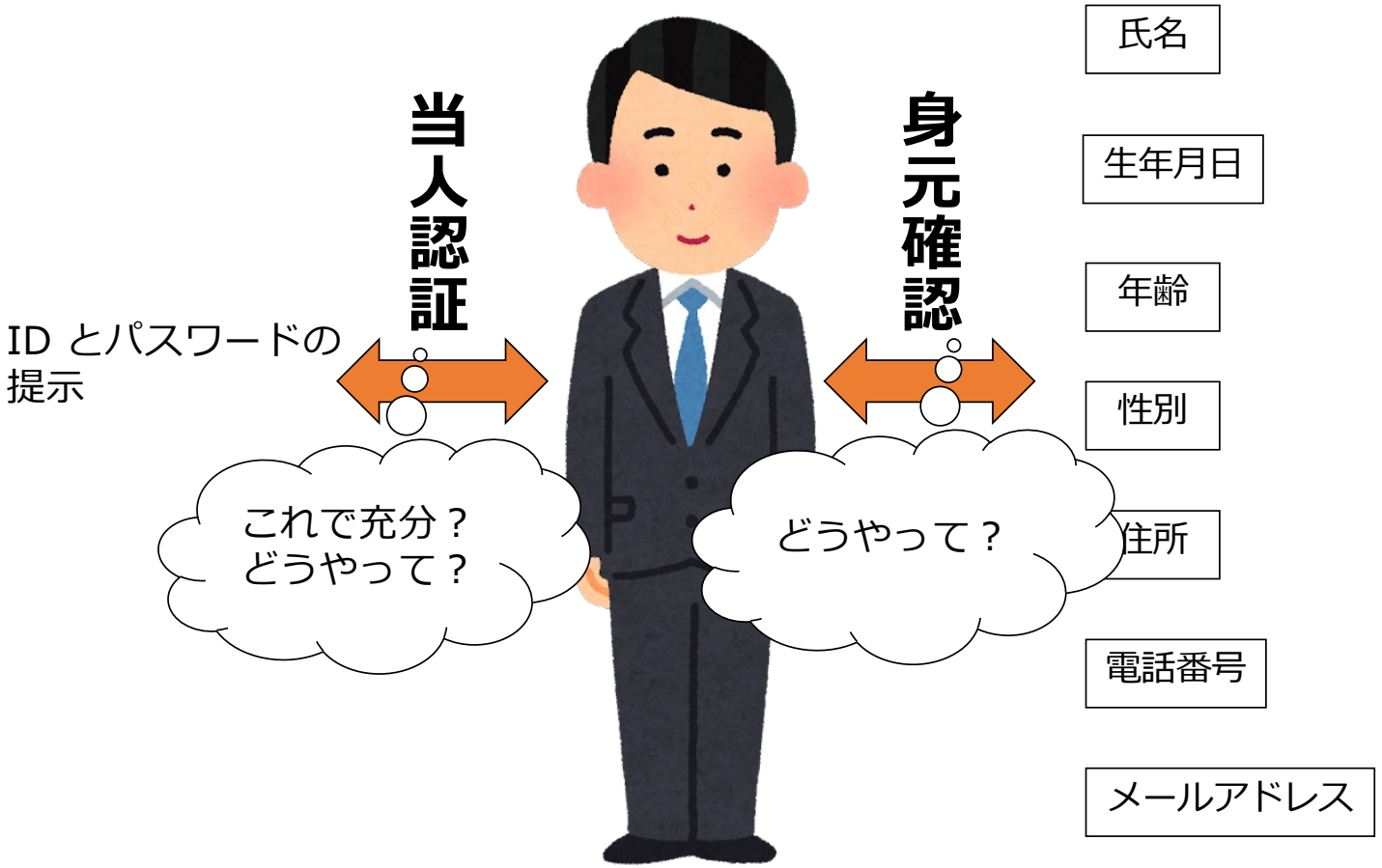
身元確認と当人認証

- 身元確認とは、利用者当人の実在性を確認すること
  - 登録するデータ（氏名・住所・生年月日等）が正しいことを証明／確認すること
- 当人認証とは、利用者の行為を確認すること
  - 例：IDとパスワードの提示

- 本人確認とは、両方の組み合わせを通じて行うもののこと

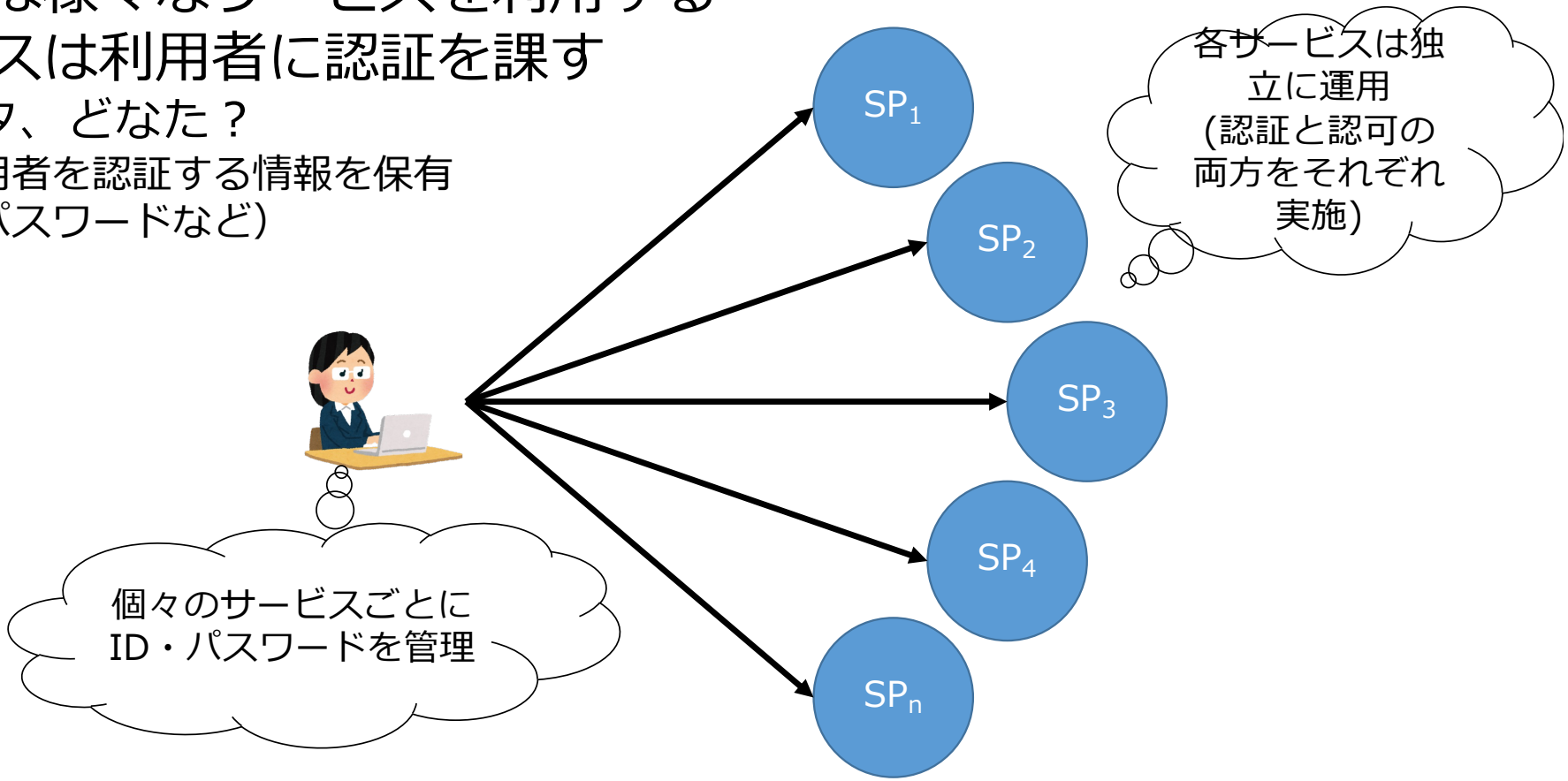
経済産業省, NEDO, PwC「オンラインサービスにおける身元確認手法の整理に関する検討報告書（概要版）」（https://www.meti.go.jp/press/2020/04/20200417002/20200417002-1.pdf）（検索日：2023年10月1日）

本人確認：身元確認、当人認証



認証認可分離以前

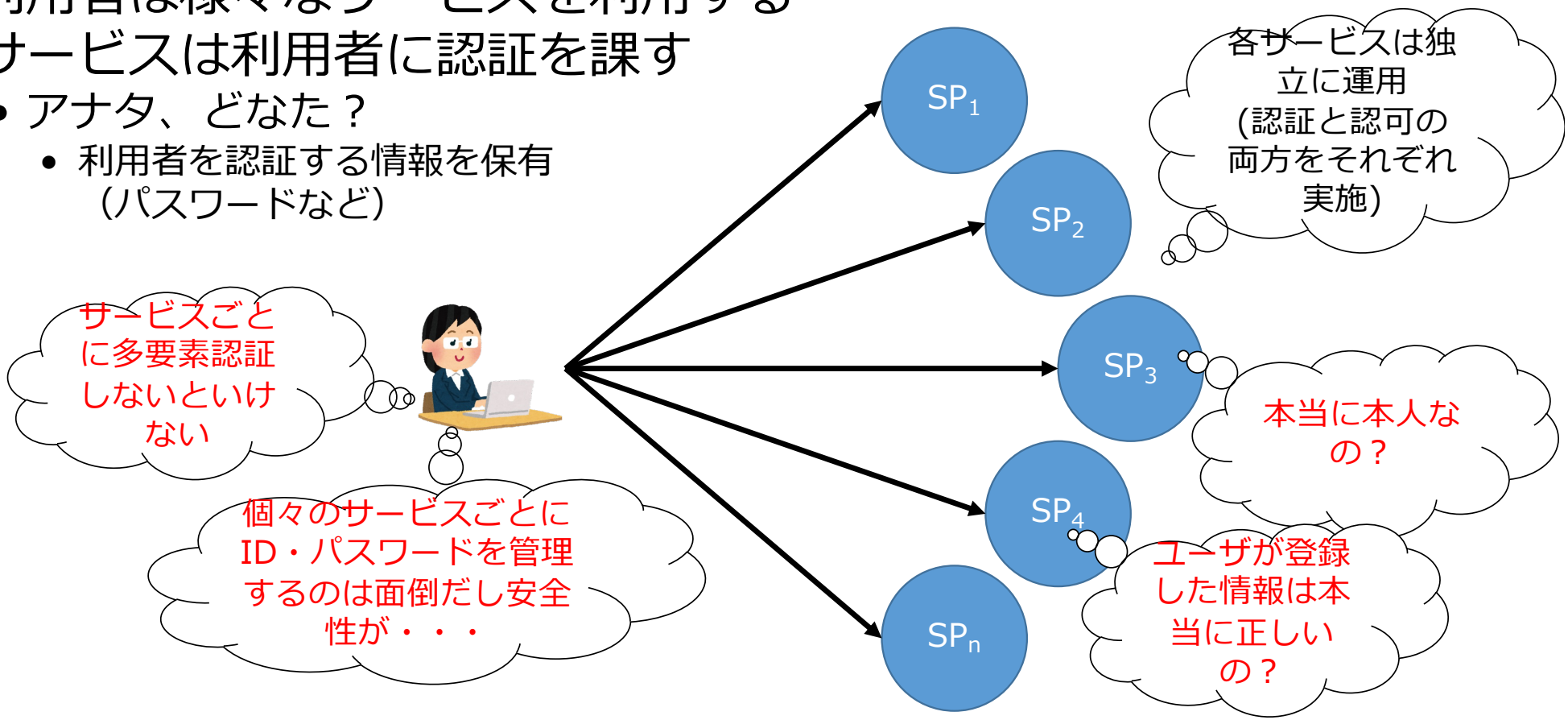
- 利用者は様々なサービスを利用する
- サービスは利用者に認証を課す
  - アナタ、どなた？
    - 利用者を認証する情報を保有
      （パスワードなど）



SP: Service Provider

認証認可分離以前

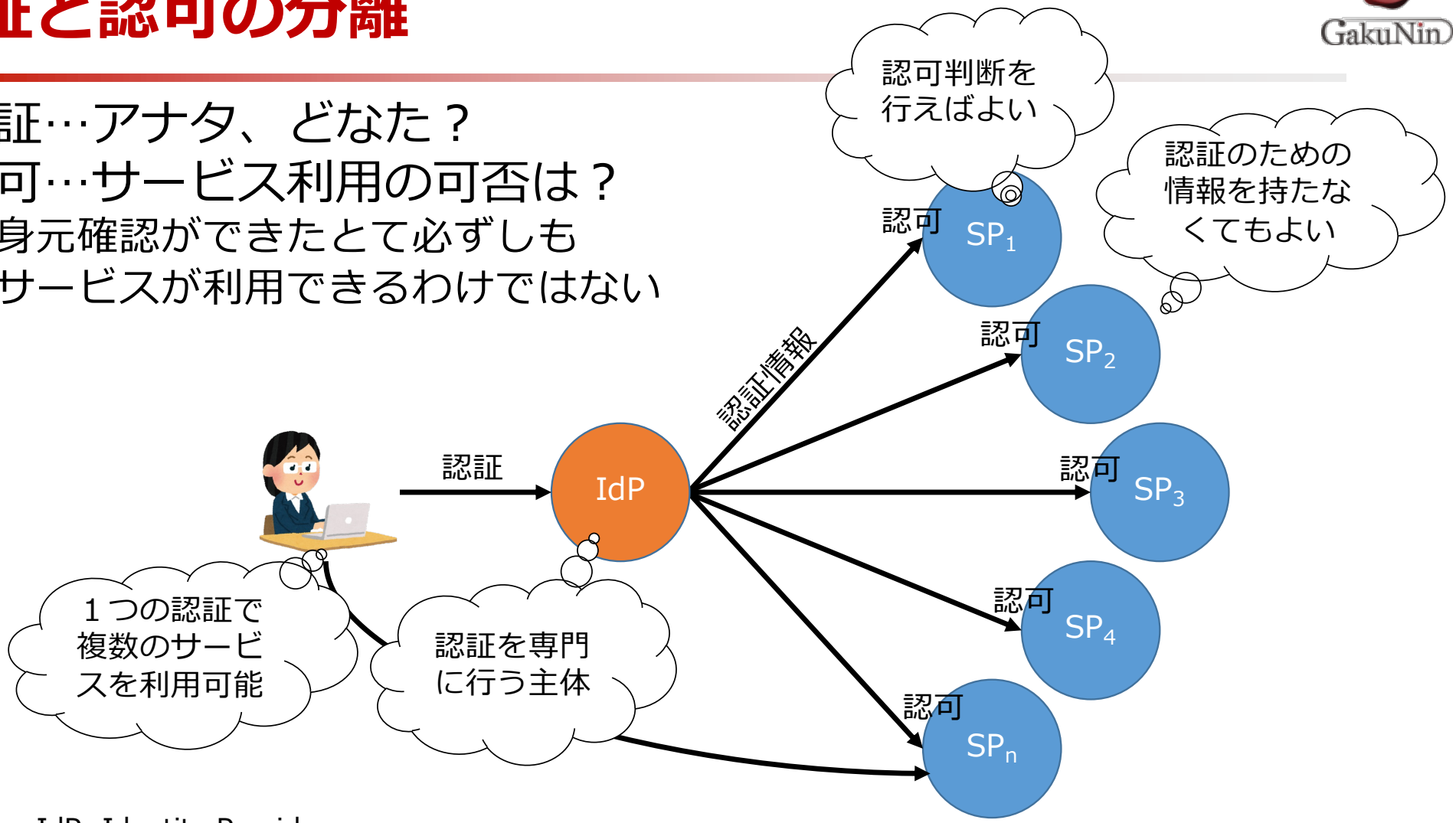
- 利用者は様々なサービスを利用する
- サービスは利用者に認証を課す
  - アナタ、どなた？
    - 利用者を認証する情報を保有（パスワードなど）



SP: Service Provider

認証と認可の分離

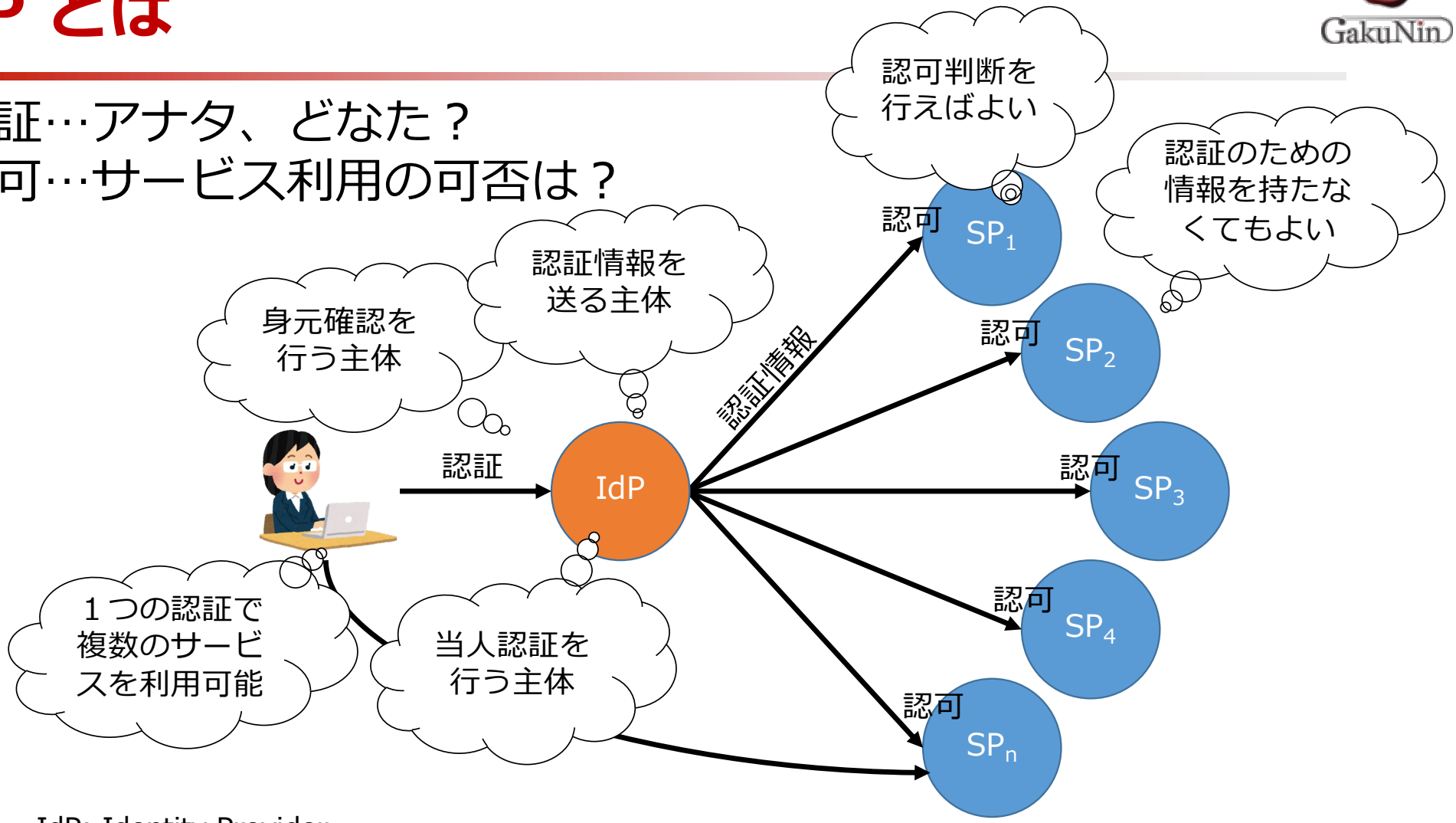
- 認証…アナタ、どなた？
- 認可…サービス利用の可否は？
  - 身元確認ができたとて必ずしも
    サービスが利用できるわけではない



IdP: Identity Provider

IdP とは

- 認証…アナタ、どなた？
- 認可…サービス利用の可否は？



IdP: Identity Provider

認証認可分離後

- 利用者視点
  - サービスごとのID・パスワード管理からの解放
- SP 視点
  - 利用者を認証するための照合データ管理からの解放
  - 認可判断だけを行えばよい
    - 判断基準によって、認可条件の簡素化が可能
- IdPでの認証結果を複数のSPに対してうまく連携することにより、１回の認証で複数のサービスを利用可能（シングル・サインオン）

学術 IdP の役割

- 組織の構成員の身元確認
- 組織の構成員に対する当人認証
- 組織の構成員の認証情報を連携 SP に送信

学術サイバー空間では

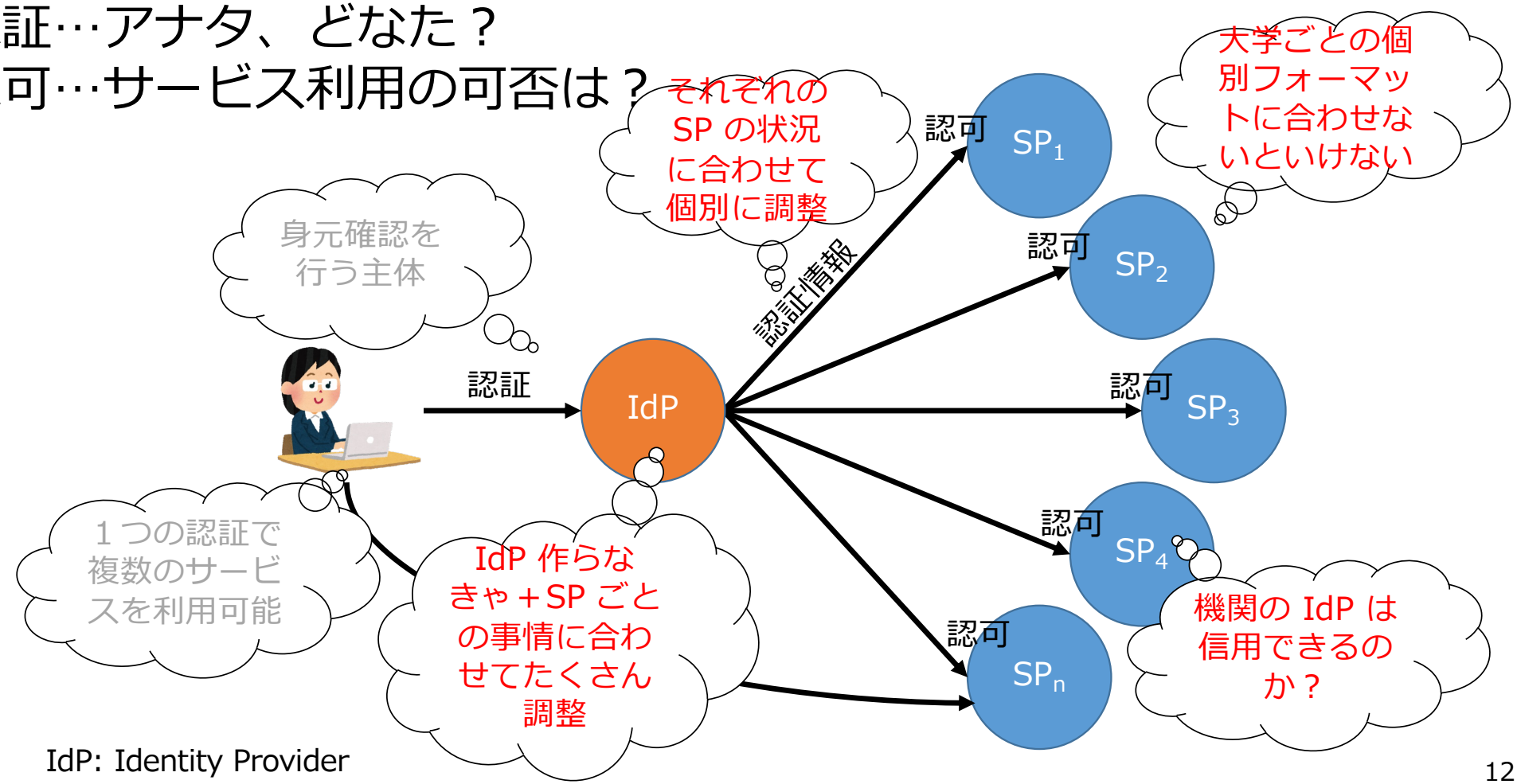
- 利用者：研究者、教師、学生、職員…

- IdPを担う主体：大学や研究機関
  - 構成員（学生、教職員）の認証を行い、
  - その結果をSPに送る

- SPの例
  - 電子ジャーナル
    - 認可判断：大学に所属していること（が保証されていればよい）
  - 学生割引サービス
    - 認可判断：学生であること
  - その他

SP を同一 ID で使えると便利だけど独自IdPだと・・・

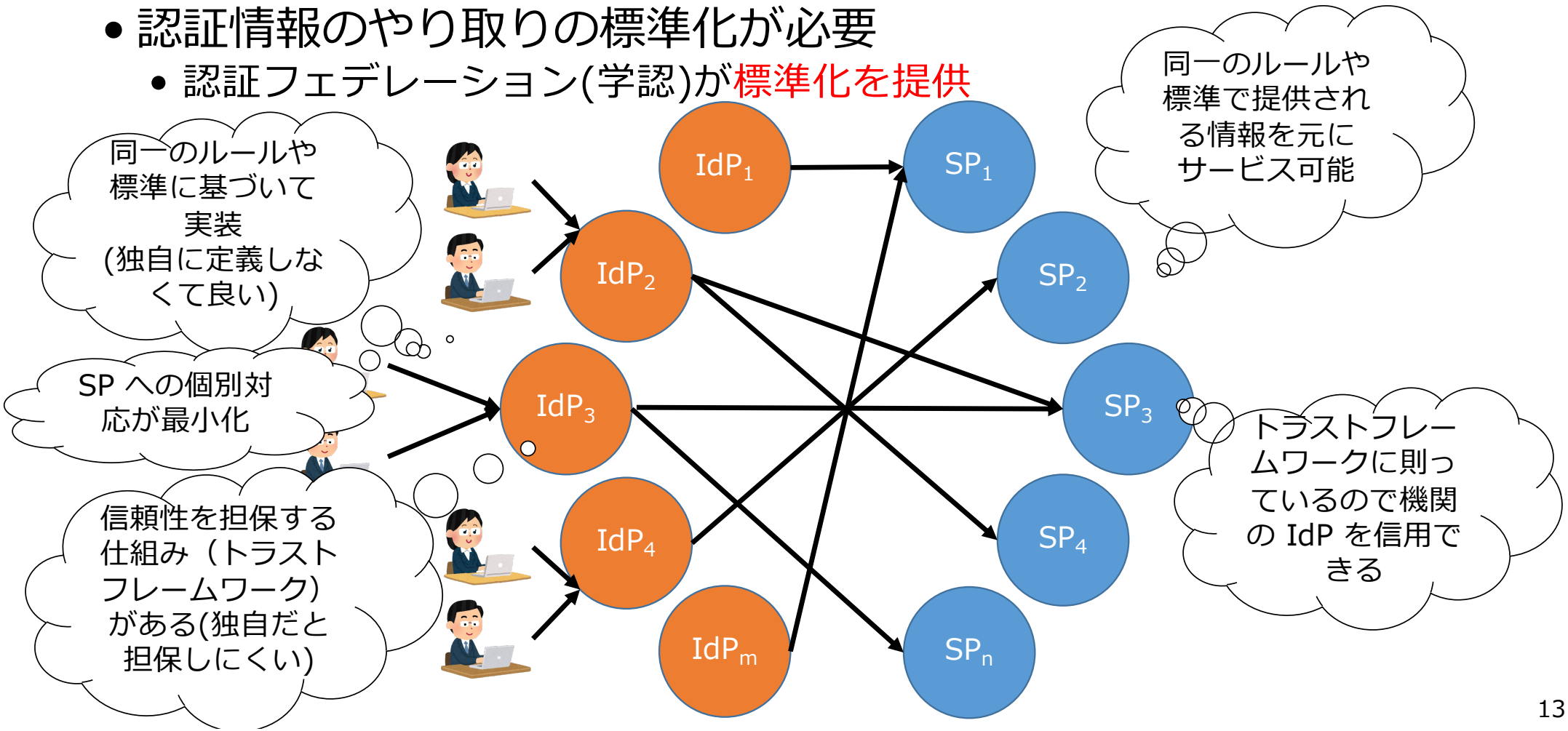
- 認証…アナタ、どなた？
- 認可…サービス利用の可否は？



IdP: Identity Provider

学術フェデレーション(学認)の必要性

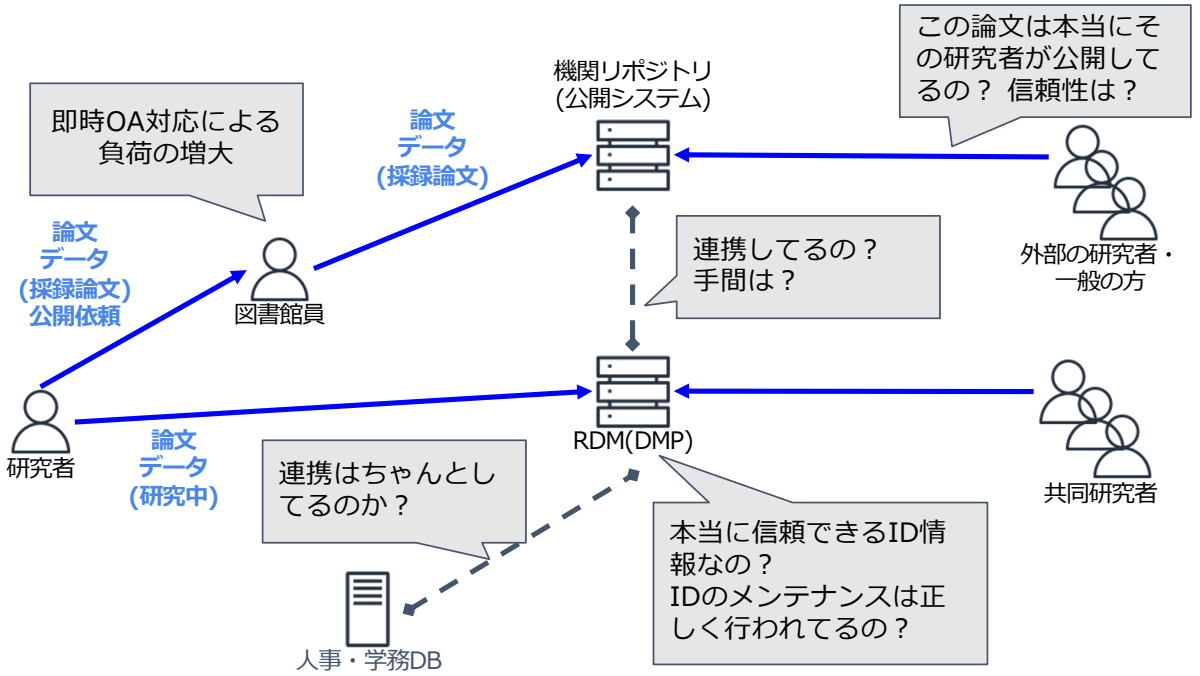
- 認証情報のやり取りの標準化が必要
  - 認証フェデレーション(学認)が標準化を提供



本人確認の保証度によく出てくる用語の説明

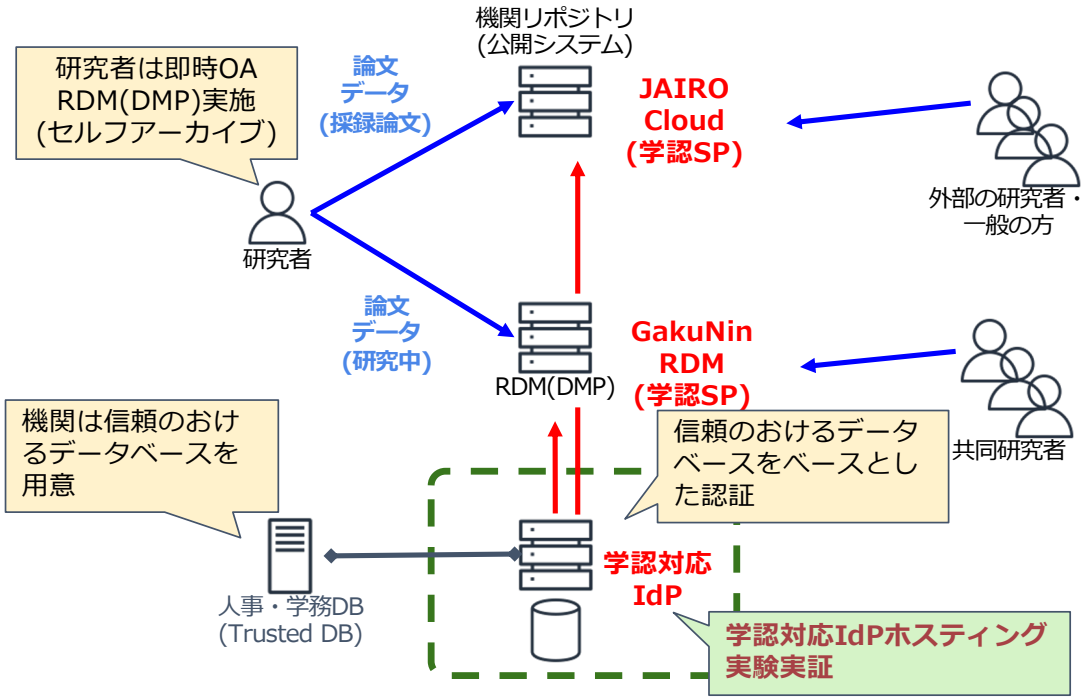
- 身元確認や当人認証は、それらのやり方次第で保証度に違いがある
- 身元確認：**Identity Assurance Level (IAL)**
  - 例：氏名と住所と生年月日を確認する方法は…
  - 自己申告のみ（何も確認しない）
  - 公的身分証（の写し）を活用して確認する
  - 対面で、かつ、公的身分証を活用して確認する
  - IAL1(低) → IAL2 → IAL3(高)
- 当人認証：**Authenticator Assurance Level (AAL)**
  - ID・パスワードの提示以外の別の手段はあるのか？
  - 認証要素（知識、所持、生体）の整理から多要素認証へ
  - AAL1(低) → AAL2 → AAL3(高)
  - 単要素 → 多要素

信頼性の高い認証基盤(学認)がないと...



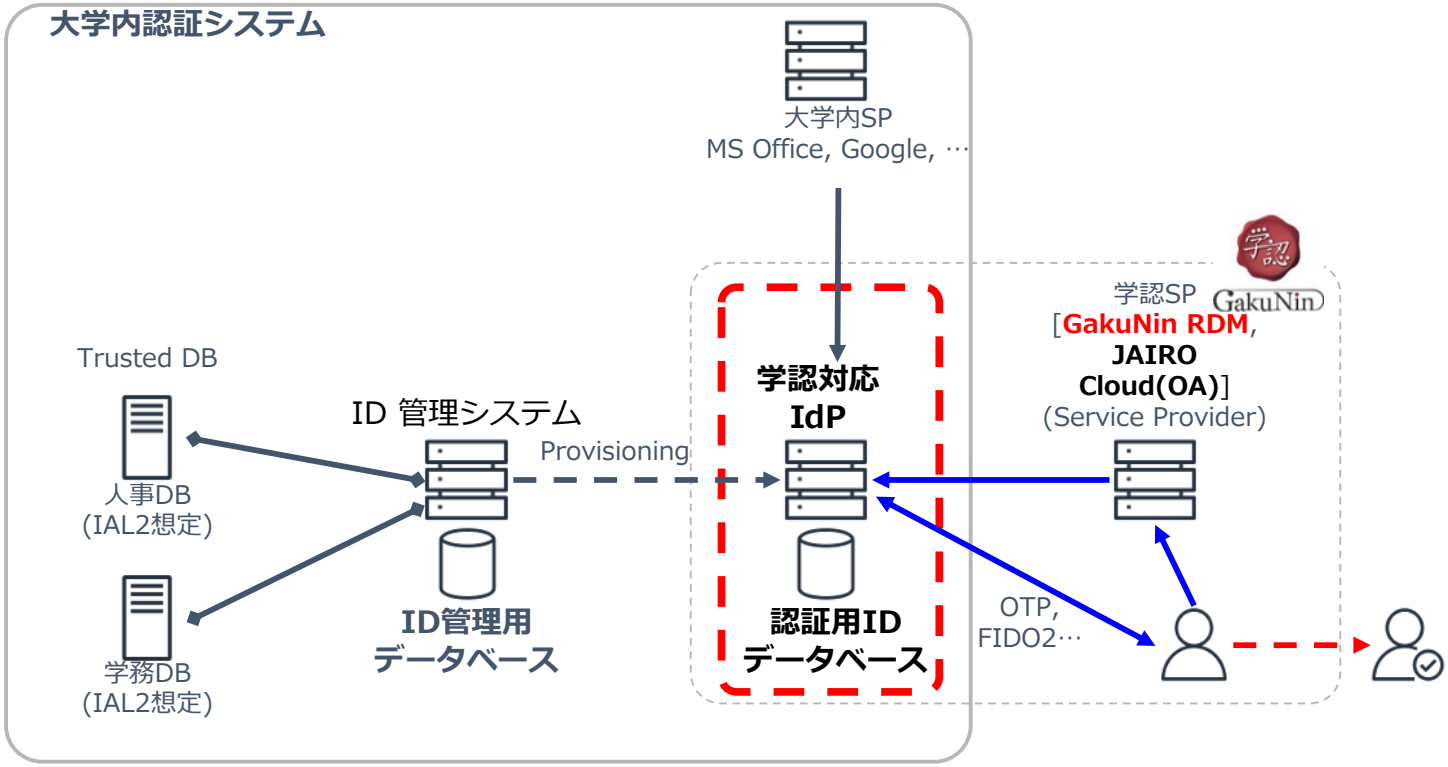
学認に対応した基盤を用いていない場合、信頼性の低い ID でデータ管理・公開するため、信頼性が低い OA 対応となってしまう。例えば、研究データの共有時に、存在確認が取れていない ID (内部の人が使っているか外部の人が使っているかわからないIDなど)によって OA 対応しなければならない。学認は運用状況調査を毎年実施することで高い信頼性を担保している。

即時OAを支える認証基盤(学認IdP)の整備



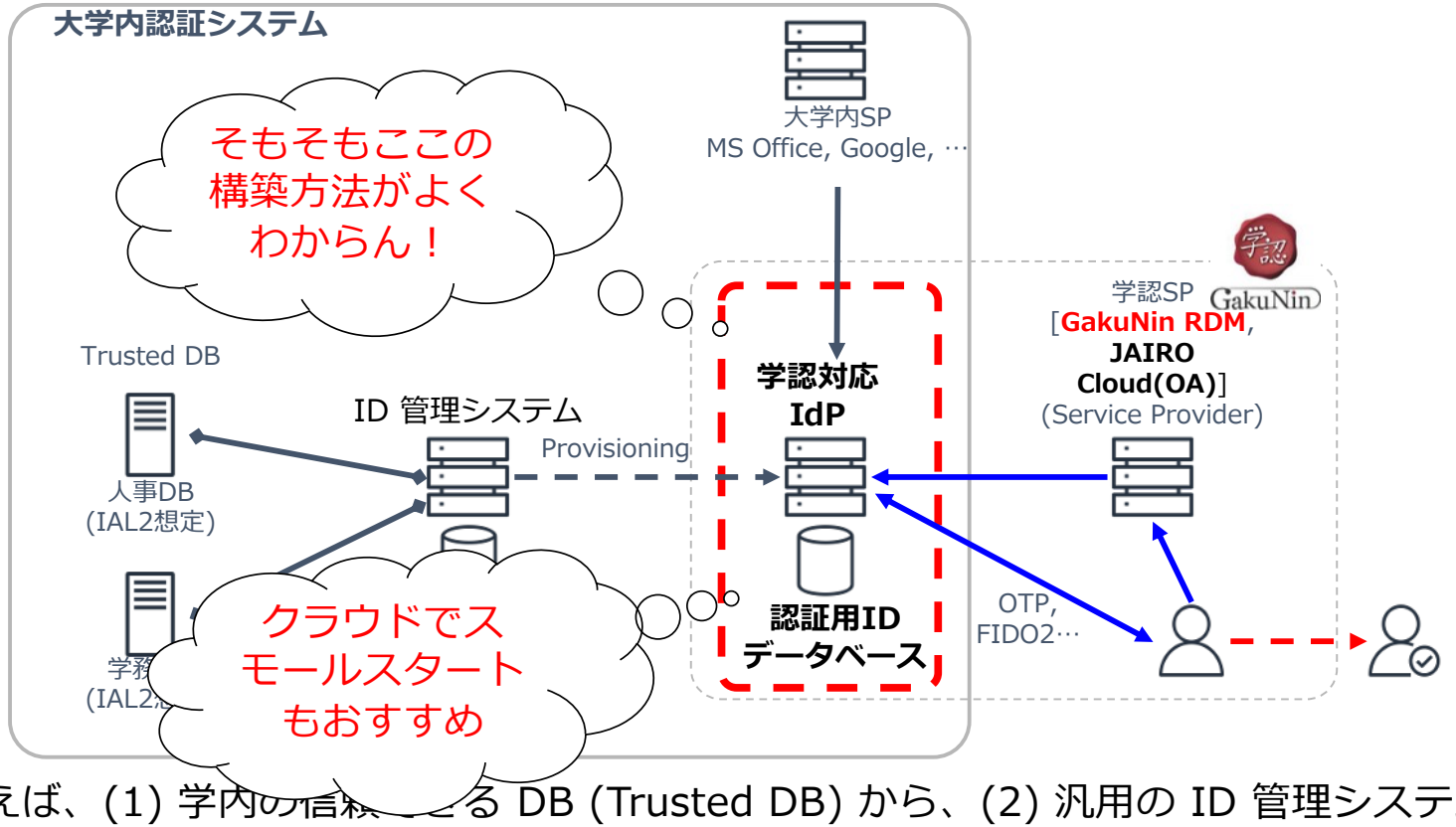
研究者は JAIRO Cloud(OA) や GakuNin RDM にて論文・データの公開や管理が可能となる。その基盤として学認があり、学認は Trusted DB (教職員学生の存在が保証がされている DB) をベースとする機関保証のある信頼性の高い ID 情報とそれに基づく認証機能を提供することで、相互運用性を高めることができる。

学認対応 IdP システムの構成例



理想を言えば、(1) 学内の信頼できる DB (Trusted DB) から、(2) 汎用の ID 管理システムで ID を管理し、(3) さまざまなシステムに ID 情報を流通させる仕組みを作った上で、(4) 学認対応 IdP を作ることだが、それをしなくても学認対応 IdP を構築・運用は可能(CSV ファイルで登録でも OK)

学認対応 IdP システムの構成例



理想を言えば、(1) 学内の信頼できる DB (Trusted DB) から、(2) 汎用の ID 管理システムで ID を管理し、(3) さまざまなシステムに ID 情報を流通させる仕組みを作った上で、(4) 学認対応 IdP を作ることだが、それをしなくても学認対応 IdP を構築・運用は可能(CSV ファイルで登録でも OK)

学認対応 IdP を作る時の参考(標準仕様書)

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

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

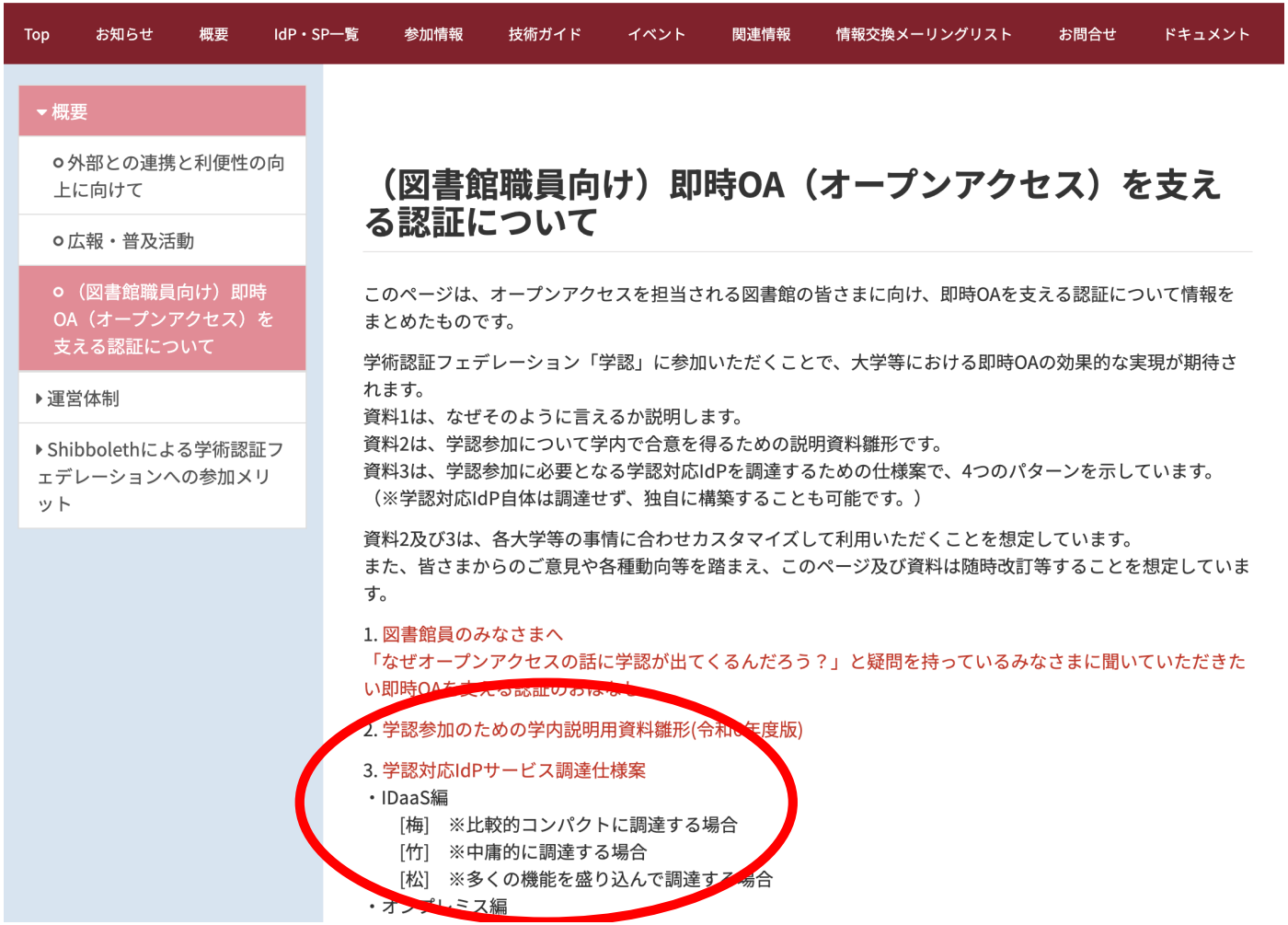
平素より本サービスの運営にご協力頂きありがとうございます。学認事務局です。

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 を作る時の参考(標準仕様書)



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

標準仕様書読んだけどごちゃごちゃしてわからん

不明な点についてなにかありましたら、サービス説明会(個別質問)、問い合わせ窓口から適宜ご相談ください。

[泥臭い話でも入門的な質問でも大丈夫です！]

RDM や OA のためにも
是非学認にご参加ください！！