学認参加後のIdP運用道しるべ

2021.12.17 AXIES2021

国立情報学研究所 西村 健

GakuNin道しるべ

- https://www.gakunin.jp/document/98
- 学認参加後（もしくはIdP/SP構築後）の指針となるべく用意したドキュメントです
- 内容が多岐にわたるため、今回はIdPに限定し、また内容を最新に更新してお送りします

日本の学術認証フェデレーション「学認」

- 日本の学術系フェデレーション「学認」

に参加したはいいけどそのあとどうしよう／何が待っているのだろう

学認に参加すると何ができるの？

- 学認に参加しているサービス（SP）が使えます
  - 各出版社の電子ジャーナル
  - e-Learningサービス
  - アカデミック向けソフトウェアパッケージ配布
  - 無線LANゲスト利用サービス
  - researchmap
  - 学割サービス
  - ファイル転送サービス

※有料サービスは個別に契約が必要です。学認に参加しただけでは使えません

各SPに対して属性送出設定を行わなければならない

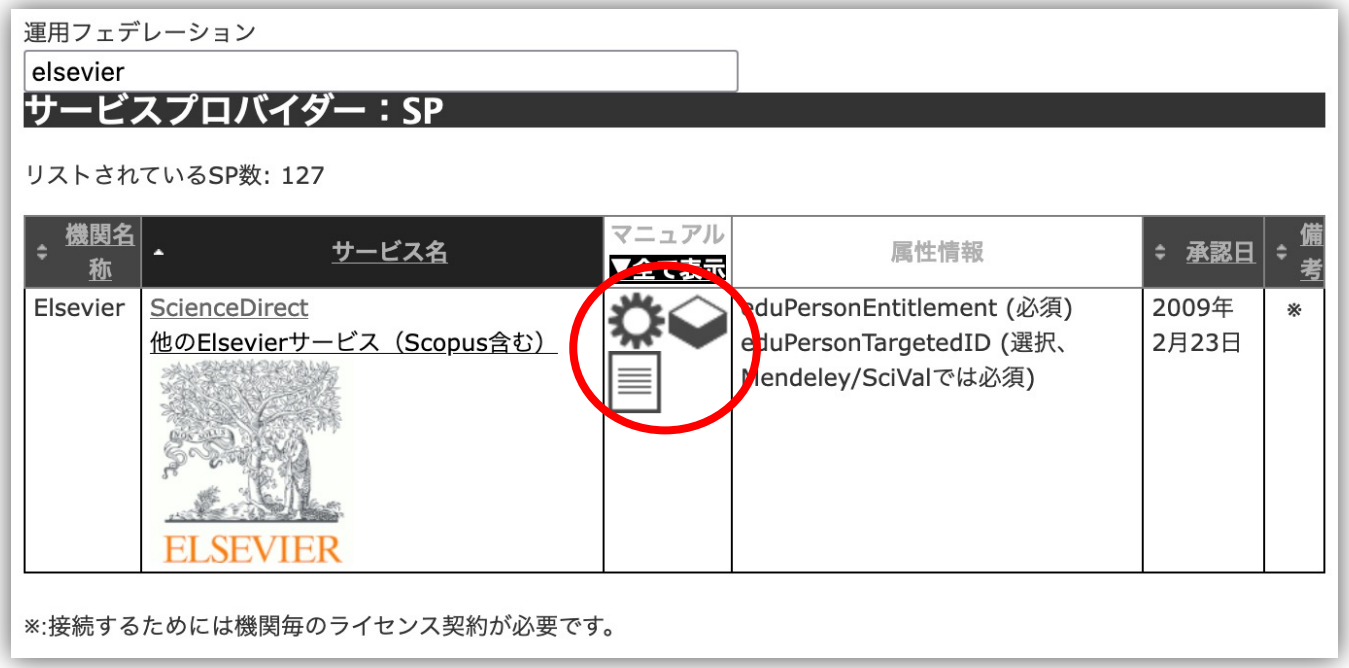
- IdPの初期状態ではどのSPにも何の属性も送出しない
  - 少なくとも学認技術ガイドに沿った構築では
- 利用する各SPに対して属性送出設定を行う
  - Shibbolethでいうとattribute-filter.xml
  - 学認ウェブサイトのSP一覧を参照のこと

- 属性送出設定追加のタイミング
  - 新しいSP
  - 利用者からの利用要望を受けて

- 属性の必須／選択（任意）とは？
  - https://meatwiki.nii.ac.jp/confluence/x/YAf6

SPの利用契約について

- 学認に参加することで、何らかの有料サービスが無料で利用できるようになるわけではありません。必要に応じてSP毎に別途契約をお願いします。既に契約がある場合は、一般に、学認によるアクセス開始の申請がSP毎に必要です。詳しくは、学認WebのSP一覧を参照してください
  ⇒ https://www.gakunin.jp/participants


運用フェデレーション

elsevier

サービスプロバイダー：SP

リストされているSP数: 127

機関名称	サービス名	マニュアル	属性情報	承認日	備考
Elsevier	ScienceDirect 他のElsevierサービス（Scopus含む） ELSEVIER		eduPersonEntitlement (必須) eduPersonTargetedID (選択、Mendeley/SciValでは必須)	2009年2月23日	※

※:接続するためには機関毎のライセンス契約が必要です。

学認対応の属性について

- IdPから送出する属性について
  - どれだけの属性を設定・送出するか
    - 学認では21属性を利用
    - 全属性を設定する必要なし
      - 氏名などはほぼ使われません
    - 利用したいサービスに必要な属性を過不足なく送出できるか
  - 属性の値の決定・生成
    - 各属性にはどんな値を設定するか
    - 認証基盤から導出（変換）可能か

属性	内容
organizationName	機関名称
jaOrganizationName	機関名称（日本語）
organizationalUnitName	機関内所属名称
jaOrganizationalUnitName	機関内所属名称（日本語）
eduPersonPrincipalName (eppn)	フェデレーション内の共通識別子
eduPersonTargetedID	フェデレーション内の仮名識別子
eduPersonAffiliation	職種(faculty, staff, student, member)
eduPersonScopedAffiliation	職種（@ドメイン名が付いた形式）
eduPersonEntitlement	資格
surname	氏名（姓）
jaSurname	氏名（姓）（日本語）
givenName	氏名（名）
jaGivenName	氏名（名）（日本語）
displayName	氏名（表示名）
jaDisplayName	氏名（表示名）（日本語）
mail	メールアドレス
gakuninScopedPersonalUniqueCode	教職員番号・学籍番号
isMemberOf	所属グループ名
eduPersonAssurance	IDの保証レベル
eduPersonUniqueId	共通識別子(opaque)
eudPersonOrcid	ORCID識別子

利用者の流れ

- 学認の想定する利用者の基本的な流れ
  - SP → DS → IdP → SPに戻る
- あるいは、機関が用意した「ポータル」
  - IdPから利用可能なSPをリストしたもの
  - IdP → SP
- あるいは、学認クラウドゲートウェイサービス
  - https://cloud.gakunin.jp/cgw/

IdPの管理・運用について

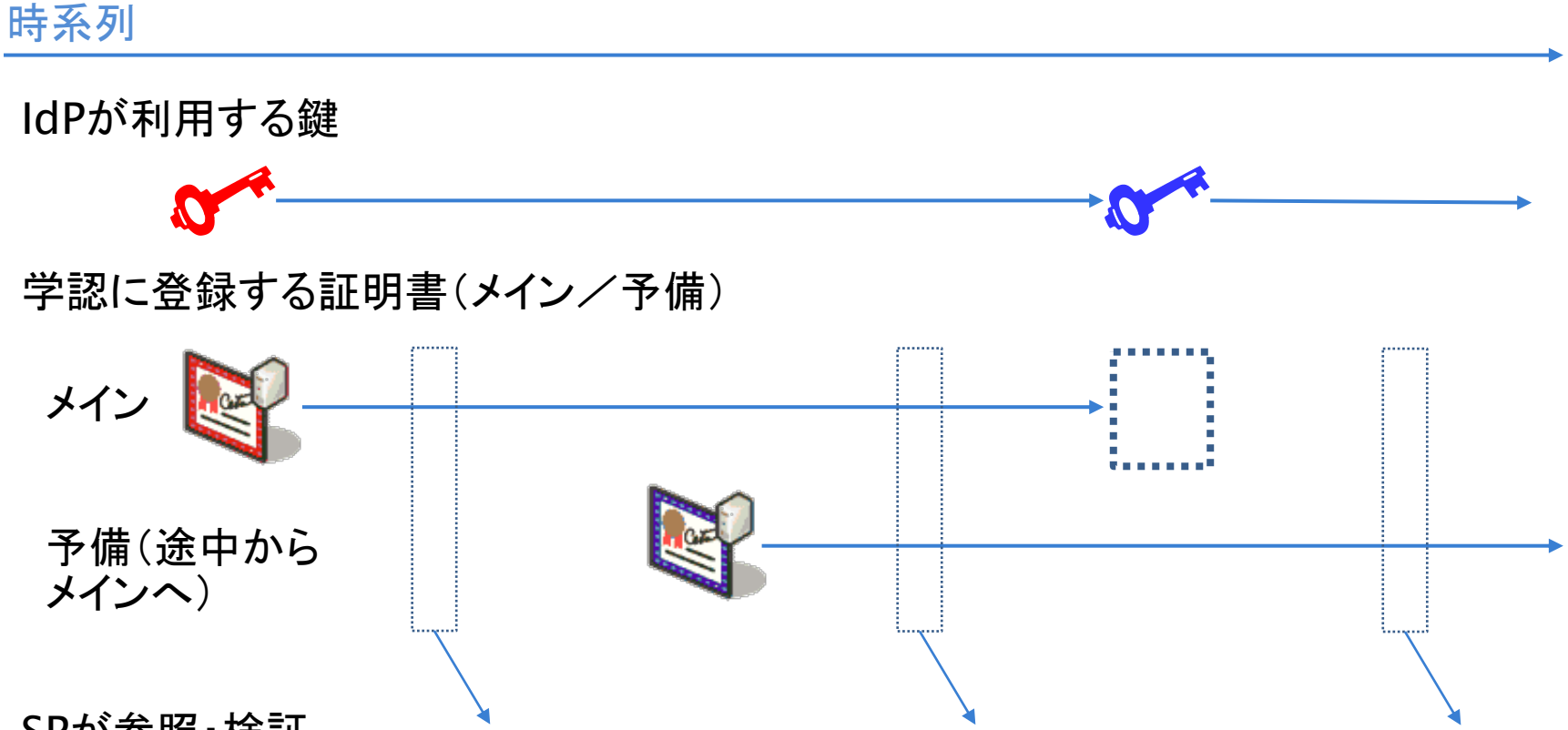
- ユーザIDのライフサイクル管理
  - 離職や卒業等によるユーザIDの失効等を確実に実施してください
- 脆弱性への対応
  - 必要に応じてShibbolethおよび関連ソフトウェアのバージョンアップ等を行ってください
    - 情報源：学認情報交換ML、その他
- サーバ証明書の更新とメタデータの更新
  - サーバ証明書の期限切れに伴う更新時にはメタデータの証明書も更新してください
    - 運用中IdP/SPでエラーが発生しないよう手順が決まっています
    - 詳細：IdP Key Rollover：メタデータ記載の証明書更新手順 https://meatwiki.nii.ac.jp/confluence/x/44W5

IdPの管理・運用について（続）

- 運用責任者・運用担当者の交代・引継ぎ
  - 人事異動等による交代時には変更申請をしてください
- 学認参加IdP運用状況調査への回答
  - 年に一回実施
    - 規程に定められているとおりに運用されているか確認
      - □必ずご回答ください
      - □フェデレーション全体の信頼性にも係わる調査です
- システム更新→ホスト名同一を推奨
  - https://meatwiki.nii.ac.jp/confluence/x/mYMoAQ

IdP証明書更新の際はご注意を

- https://meatwiki.nii.ac.jp/confluence/x/44W5
- 流れ：証明書発行→予備登録→利用する鍵切り替え→旧証明書登録削除



eduGAINについて

- 世界各国の学術IDフェデレーションを相互接続(inter-federation)し、グローバルな研究・教育コミュニティのためのコンテンツ、サービスなどの資源へのアクセスを容易にすることを目指しています
  - https://edugain.org/
- eduGAINには、60以上の国と地域が参加しています
  - 3000以上のIdPと、2000以上のSP
  - ORCID, SheerID, Dropbox, FileSender, MATLAB, 一部の電子ジャーナル など

https://technical.edugain.org/status

- 学認からはオプトインで参加できるようになっています
  - 参加するには、学認申請システムで「eduGAINに参加する」にチェック
    - 注意:連絡先種別は「support」または「technical」としてください
  - IdP/SPの設定手順は学認ウェブサイトの「eduGAINに参加する」参照のこと
    - ⇒ https://www.gakunin.jp/join/eduGAIN

- eduGAIN
  - 学認からの参加数(2021年12月現在)
    - IdP: 60
    - SP: 6

学認に関するお問合せは・・・

国立情報学研究所　学術基盤推進部

学術基盤課　総括・連携基盤チーム（認証担当）

Web: https://www.gakunin.jp/contact
もしくは
mail: gakunin-office@nii.ac.jp

まで，お気軽にどうぞ。