

はじめての学認 ～学認参加への第一歩～

2025.6.18 NII学術情報基盤オープンフォーラム2025
国立情報学研究所 中川 潤紀

学術認証フェデレーション「学認」とは

- 日本における
 - 【学術】 サービスについて
 - 【認証】 連携を行うために構成された
 - 【フェデレーション】 (=連合体)
- 組織を超えた安全・安定的な**シングルサインオン**を実現するための連合体
- 学認に参加することで、学認に参加している学術サービスをシングルサインオンで使える

シングルサインオンに至るユーザ認証の変遷

1. サービスの個別運用

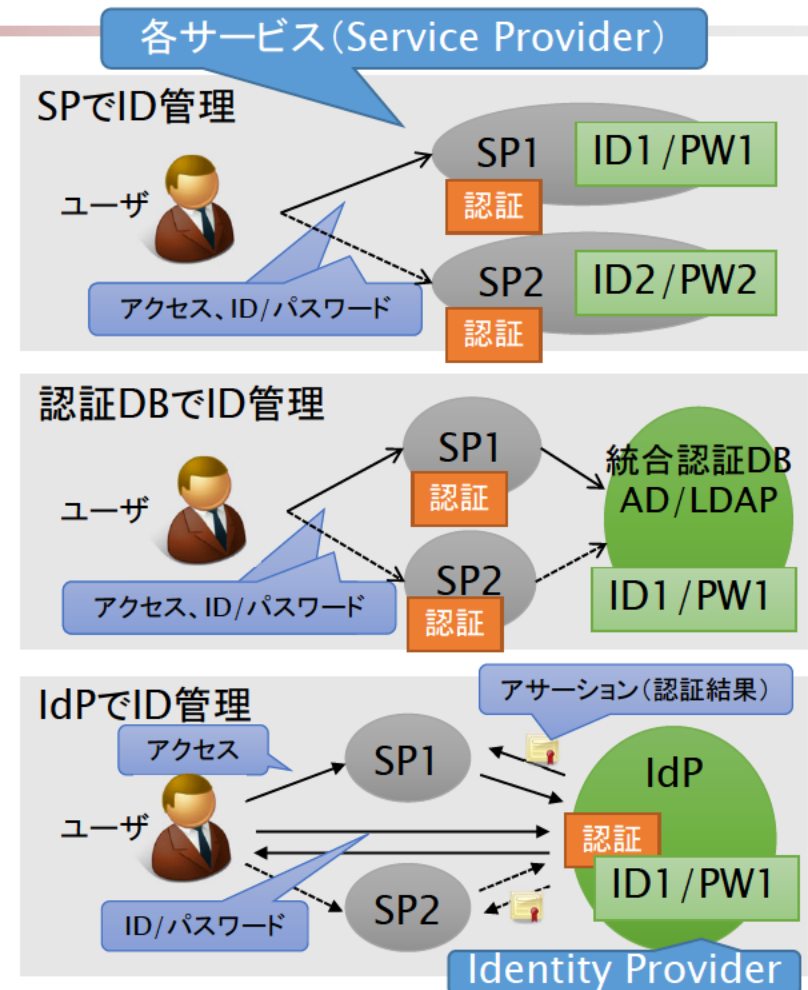
- ×ID・パスワードを覚えにくい
- ×SPごとの個別管理（コスト高）

2. ID統合

- ✓パスワード共通化
- ×SPごとに認証（コスト中）
- ×パスワード漏洩の危険性（高）

3. Single Sign-On(SSO)

- ✓認証処理の集約(IdP)
- ✓パスワードはSPに渡らない（安全）
- ✓認証処理の高度化も容易



フェデレーションとは

- 参加機関の相互信頼の枠組み（トラストフレームワーク）を実現するための連合体が「フェデレーション」
 - 学術サービスを利用する高等教育機関（Identity Provider : IdP）
 - 学術サービスを提供する事業者（Service Provider : SP）
 - 電子ジャーナル, e-learningサービス, ファイル転送サービス, 研究データ管理サービスなど…
 - フェデレーション管理者
- 各国・地域で同様の取り組み
- 日本における学術リソースの利用を目的とするフェデレーションが学術認証フェデレーション「学認」

相互信頼：トラストフレームワークと認証連携

- フェデレーション管理者が定めた規程の遵守と相互の信頼で認証連携が成立
 - 実施要領：<https://www.gakunin.jp/document/74>
 - 技術運用基準：<https://www.gakunin.jp/document/80>
- ⇒各参加機関がフェデレーションが定めた規程と技術基準を遵守していることを前提に
- SPはIdPから送られた認証情報や、属性情報（ユーザー情報）を信頼
 - IdPはSPが、渡した情報を適切に取り扱ってくれると信頼

フェデレーション参加機関の役割

- サービス利用機関
 - 認証基盤とIdPサーバの適切な管理・運用
 - セキュリティ水準の維持
 - 運用状況の点検・確認（運用状況調査への回答）
<https://www.gakunin.jp/join/316>
- サービス提供機関
 - サービスを提供するSPサーバを運用
 - サービスの利用に必要な属性を提示
 - セキュリティ水準の維持
- 参考資料
 - 学認参加のための学内説明用資料
<https://www.gakunin.jp/document/730>

フェデレーション参加機関の「適切な管理・運用」

- 認証基盤の管理・運用に関する「決まり」を作ってください

参考資料

- 高等教育機関の情報セキュリティ対策のためのサンプル規程集
全学認証基盤運用に関わるサンプル規程（D2601～2603）
<https://www.nii.ac.jp/service/sp/>
- 個人情報保護にご注意ください
 - 学認ではサービス提供機関に、属性情報として利用者の個人情報を含む情報が送信されることになる
 - 「学認参加のための学内説明用資料」雛形
 - 送信される情報が個人情報に該当するかの見分け表
<https://www.gakunin.jp/document/730>
 - 個々人が認証する際に同意を取る機能(オプトイン機能)も実装されている

フェデレーション管理者の役割

- 運用規程（ポリシー）の策定
 - 学認実施要領や学認技術運用基準
- 参加機関の承認
 - 学認申請システムから申請受付と承認
- DSの運用
 - 参加機関のIdPリスト
- IdPからSPへ送信される属性情報の規定
 - 学認は全21種
- フェデレーションメタデータの配布
 - フェデレーション参加機関のサーバ情報をまとめたデータ

メタデータ

- IdPとSPの認証連携に必要な情報をまとめたもの
 - 「entityID」と呼ばれる各IdP固有のIDや「サーバ証明書」など
 - 「そのIdPやSPがなにものであるか」を示す相互信頼の根拠
- 各参加機関はフェデレーションにメタデータを提出
 - 提出されたメタデータは、認証基盤やサービス提供者の「身元証明」となる
 - このメタデータを照合して信頼できるか判断

メタデータ

- フェデレーションはフェデレーションメタデータを配布
 - 各参加機関の提出したメタデータを公開
 - IdP・SPはダウンロードしたフェデレーションメタデータの電子署名を検証した上で利用
 - 偽物を信頼しないように
- メタデータに含まれるサーバ証明書の役割
 - IdPが証明書により電子署名すれば、それが真正であることをSPが確認できる
 - IdPがデータを暗号化して送れば真正なSPのみ復号できる
 - 「正しい証明書」はメタデータを見れば分かる

おさらい：日本の学術認証フェデレーション「学認」

- 日本における
【学術】サービスについて
【認証】連携を行うために構成された
【フェデレーション】（＝連合体）が
- 「学認」



GakuNin

学認に参加すると何ができるの？

- 学認に参加している学術サービス（SP）がSSOで使える
 - 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
 - 研究データ管理サービス
 - ファイル転送サービス
 - 学割サービス

⇒利用できるサービス一覧はWebで公開中

- 2025/6時点で147SPが掲載（＝147のサービスが利用可能）

IdP・SP一覧：<https://www.gakunin.jp/participants>

※有料サービス等、個別に契約が必要な場合も
必ずしも無条件・無料で利用できるようになるという事ではない

「学認」に参加するメリット

- サービス利用機関（IdP）側メリット
 - シームレス（学内外）なアクセス管理システム統合
 - ID/PW送受信時の（サービスに依存しない）セキュリティ水準の向上
 - ID管理、ユーザサポート業務、セキュリティ教育の集約によるコスト削減
 - 大学など情報セキュリティ準拠、個人情報保護などへの対応
- サービス利用者メリット
 - 多数のID/パスワード管理からの解放
 - IPアドレスに依存しないアクセス（自宅や出張先からもアクセスできる）
 - 個人情報の送信制御、匿名アクセス（所属機関として認証）
 - SSOによる利便性向上、より多様なサービス連携への期待
- サービス提供機関側（SP）メリット
 - 学術機関に対してサービスがを見つけやすくなる
 - 素早いスタートアップ
 - ID管理からの解放、ユーザサポート業務の軽減
 - ライセンス条件にそった適正な利用

「学認」 参加手続き

「学認」への参加

- 参加申請は【学認申請システム】から
- まずは**テストフェデレーション**へ参加
<https://www.gakunin.jp/join/test>
 - 構築した学認対応システムの動作確認や接続試験，利用試験等を行う事が出来る環境
 - 学認参加対象機関“以外”でも参加可能
申請情報登録（およびアカウント作成）
 1. 事務局での参加承認
 2. フェデレーションメタデータの自動更新

通常一日で
承認
テスト開始可能



学認が提供するテストSPやIDPを利用して接続確認

※既に学認参加実績がある場合などはスキップ可能

「学認」への参加

- 一通り確認が済んだら**運用フェデレーション**へ参加
<https://www.gakunin.jp/join/production>
- いわゆる本番環境
- テストフェデレーションより厳密な手続きが必要
- 参加機関に制限がある（学認実施要領第5条）
 - 以下の役職者の選出が必要
 - 運用責任者（IdP/SPの管理・運用を担う部門の長など責任を負う者）
 - 運用担当者（IdP または SP の管理・運用に関する業務を担当する者）
- 申請書の郵送が必要
 - 機関の長(学長など)の記名・公印の押印
- 申請書提出から承認まで数週間～1か月程度
 - SPの場合, サービス内容等について精査させて頂く場合もあり
- 申請が承認されたら「学認」の仲間入り！

「学認」に必要な技術

フェデレーションに必要なサーバ

- IdP (Identity Provider)
 - 利用機関が用意するサーバ
 - フェデレーション内に構成員の情報を流すサーバ
 - それ自身では情報を持たない
 - LDAPなどの認証基盤を参照
 - 必要な情報のみ外部へ送信するフィルタのようなもの
 - 認証したユーザの「属性」を保証



フェデレーションに必要なサーバ

- SP (Service Provider)
 - サービス提供機関側が用意するサーバ
 - 認証を受けた人に対してサービスを提供するサーバ
 - 電子ジャーナル、e-Learningなどのサービスを提供
- DS (Discovery Service)
 - フェデレーション管理者 (NII) が用意するサーバ
 - IdPを検索するシステム
 - DSにIdPが掲載されることにより「フェデレーションに参加」となる
- 「SAML」 (サムル) 形式の通信が可能なこと
 - 学認ではShibboleth IdP/SPというソフトウェアを推奨

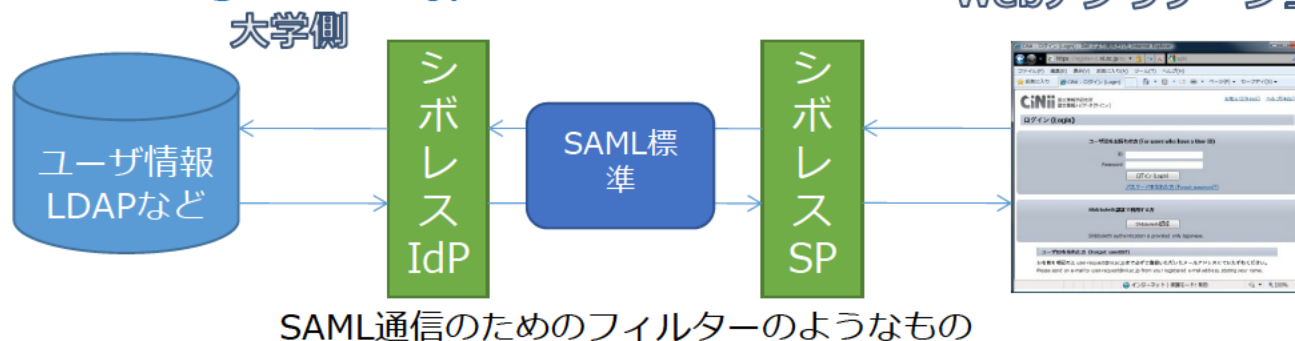
学認推奨のミドルウェア

Shibboleth (シボレス) : 統合認証対応ミドルウェア

- 個人情報やセキュリティに配慮したオープンソースのミドルウェア
- 安全な認証・認可を行う「SAML」(サムル)形式の通信を実装
- Windows, Linux等対応
- SAMLによる認証連携方法として、学术界でのデファクトスタンダード
- 認証を行うIdP、サービスを提供するSP、IdPのリストを表示するDSが存在
- 技術ガイドにて標準的なShibbolethの構築について公開中

<https://www.gakunin.jp/technical/325>

Webアプリケーション側



IdPの調達と構築

①学内に構築して運用する

- 教職員が構築して運用
 - スキルに自信がある場合、お安くすみませす
- 業者に委託して学内やクラウド上に構築・運用
 - サポートしてもらう範囲を決めましょう

②アプライアンス製品を導入する

- 製品の選定
- 保守・管理の範囲を決めましょう

③クラウドサービスの利用

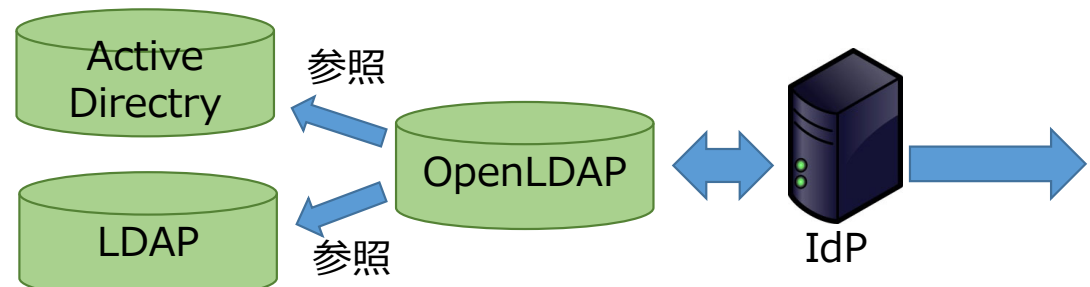
- クラウド型IdPサービス(IDaaS)
 - IdPホスティングだけ？ ID管理も含める？

IdPの調達と構築

- どの様に対応業者を見つけるか
 - 学認情報交換メーリングリスト等で情報収集
 - IdP, SP, Sierなど様々な立場の方が参加中
<https://www.gakunin.jp/ml>
- 仕様書をどう書くか
 - 技術ガイド : <https://www.gakunin.jp/technical/325>
 - 学認対応IdPサービス調達仕様案
<https://www.gakunin.jp/document/731>

認証基盤の調査

- 現状の認証基盤はどうなっているか
 - 既に全学統一の認証基盤がある
 - LDAPやADを利用している
 - GoogleやMicrosoftの認証基盤を利用している
 - ⇒ IdPと連携することにより学認連携可能
- 教員・職員・学生で異なる認証基盤を使っている
 - Ex) 教職員用はLDAPだが、学生用はActive Directory
 - このような場合、Shibbolethと連携させるには工夫が必要
 - 各機関のご事情に合わせて様々な構築が可能
 - 学認サービスデスクでNIIに相談
 - 学認情報交換メーリングリスト等で情報収集
 - 利用製品が決まっている場合は提供業者に相談



学認対応の属性について

- 認証した人に関わる「情報」
 - 学認では21種類の属性を規定・利用
 - 全属性を設定する必要なし
 - 氏名などはほぼ使われない
 - 利用したいサービス側で求められる属性を送出できるか
 - SP一覧で必要な属性が公開されている
<https://www.gakunin.jp/participants>
- 必要な属性が決まったら、値の決定・生成
 - 各属性の値の設定（機関名称など）
 - 認証基盤から導出可能か（氏名など）

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)
eduPersonOrcid	ORCID識別子

SPの学認連携と学内連携について

- 既に学内で運用しているサービスもShibbolethSP化することでSSO可能に
 - ただし、必ずしも「学認にSPとして参加する必要はない」
- 自機関のみで利用する場合 ⇒ 学内連携（学認に登録しない）
 - 各大学で独自に持っているシステムなど
 - 既存のシステムをShibboleth SP化して連携させる
 - IdPとSPを1対1で連携させる
 - 各SPのメタデータをIdPに個別に設定する
 - IdPのメタデータは個別に設定するかフェデレーションメタデータから取ってきて利用できるIdPを制限する
- 他機関でも利用する場合 ⇒ 学認連携(学認に登録する)
 - 一つのサービスを複数の大学等が利用するSPに適する
 - ex) 大学コンソーシアム共通システムなど
 - この場合でも利用できるIdPは制限可能

「学認」参加後の運用について

IdP・SPの管理・運用について

- ユーザIDのライフサイクル管理（IdPのみ）
 - 離職や卒業等によるユーザIDの失効等を確実に実施
- 脆弱性への対応（IdP・SPともに）
 - 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う
 - 主要な脆弱性情報は学認事務局より通知（Shibboleth IdP/SPに係る脆弱性など）
 - IDaaS製品を使う場合は製品側で対応される場合も
- サーバ証明書の更新とメタデータの更新（IdP・SPともに）
 - 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
 - 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
 - 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・SPの管理・運用について

- 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（IdPのみ）
 - 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アンケートです

学認関連サービス状況報告

- NII学術認証推進室の提供するサービスのメンテナンス情報を公開中
 - Orthros, NII FileSender, meatwiki, meatmailなど…
<https://meatwiki.nii.ac.jp/confluence/x/KICT>
- meatwiki運用終了について
 - 今年度12月までに移行予定
 - 詳細は学認情報交換メーリングリスト等で案内しております
<https://groups.google.com/a/nii.ac.jp/g/upki-fed-archives/c/BEkG--ItfzQ>
- 即時OAに向けた学認の整備
 - 即時OAと学認の関係の説明, 学内説明資料ひな形, 標準仕様書 等
<https://www.gakunin.jp/fed/732>
- 情報処理技術セミナー認証編について
 - 今年度は基礎編・活用編共に開催いたしません

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 認証基盤・クラウド推進チーム（認証担当）

問合せフォーム：<https://www.gakunin.jp/contact>

まで、お気軽にどうぞ。

