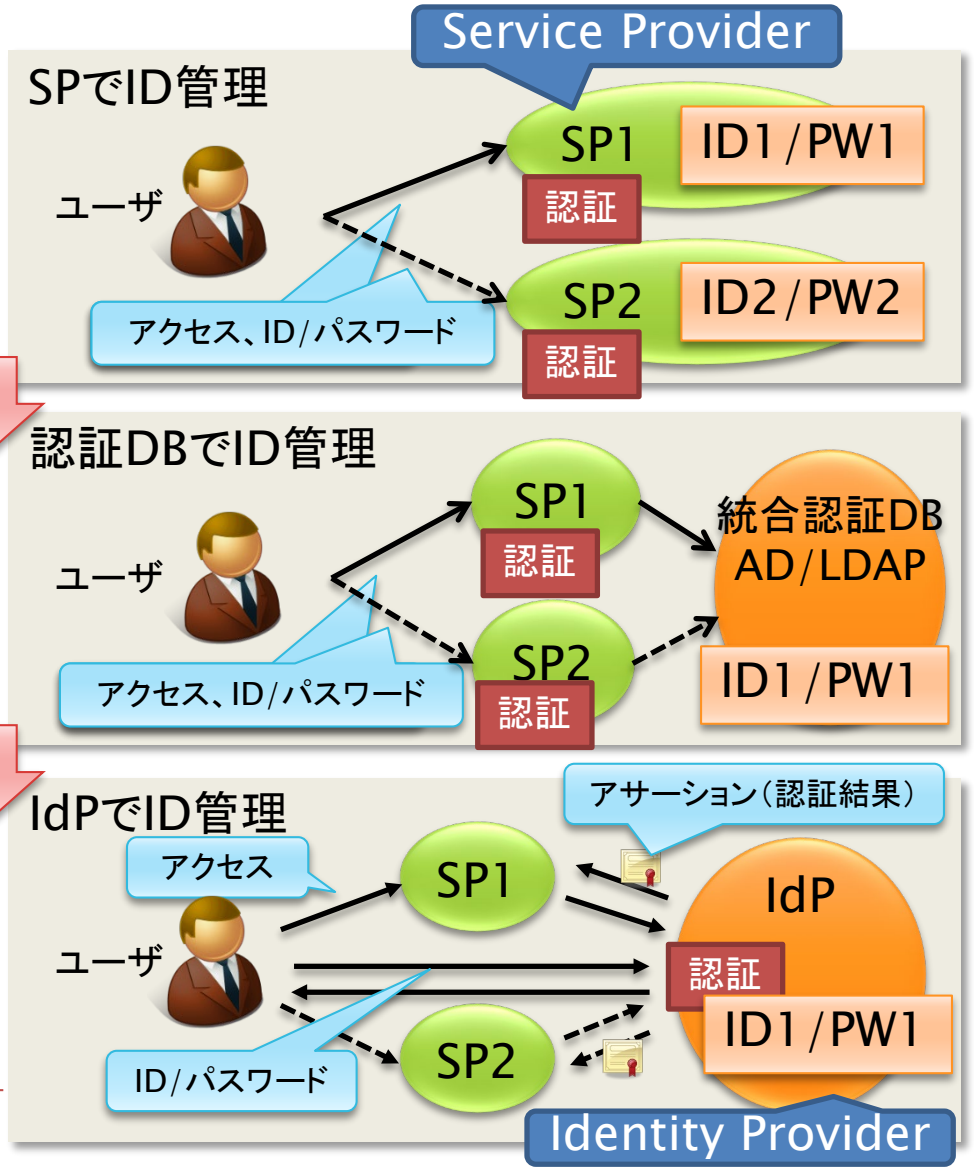
はじめての学認
～学認参加への第一歩～ 2019バージョン

2019.5.29　NII学術情報基盤オープンフォーラム2019
国立情報学研究所　西村　健

学認について

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

- 参加機関の相互信頼の枠組み（トラストフレームワーク）
  - IdP，SPから構成された連合体が「フェデレーション」
    - 国や地域単位の，学術リソースの利用を目的とするフェデレーションが各国で活動中
  - フェデレーション参加機関はそれぞれ以下を運用・管理
    - 大学等：認証基盤およびIdP（Identity Provider）
    - サービス提供側：サービスを提供するSP（Service Provider）
    - フェデレーション：IdPのリストであるDS（Discovery Service）

トラストフレームワークと認証連携

- 規程の遵守と相互の信頼で認証連携が成立
  - サービス利用機関は認証基盤とIdPの適切な管理・運用
  - サービス提供側はIdPから渡される情報を信頼
  - 各参加機関はフェデレーションが定めた規程と技術基準を遵守
    - IdPやSPのセキュリティ水準を一定レベルに維持
      - セキュリティ水準の維持により互いに信頼して連携可能
  - 規程を遵守することが信頼への第一歩

フェデレーションの役割

- 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

フェデレーション参加機関の役割

- 認証基盤運用機関
  - 認証基盤とIdPの適切な管理・運用
  - 運用状況の点検・確認（運用状況調査への回答）
- サービス提供機関
  - サービスを提供するSPを運用
  - サービスの利用に必要な属性を提示
- 参考資料
  - 「学認参加のための学内説明用資料」雛形
    - URL：https://www.gakunin.jp/document/260 （学内関係者用）
    - URL：https://www.gakunin.jp/document/259 （会議用）

認証基盤運用機関の役割

- 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
      - URL：https://www.nii.ac.jp/service/sp/
      - 全学認証基盤運用に関わるサンプル規程（C2601～2603）
  - 個人情報保護にご注意ください
    - 関連資料
      - 学術認証フェデレーションと個人情報
        ー学認と個人情報保護法とを理解し、法を遵守した運用を行うためにー
      - URL： https://www.gakunin.jp/document/83

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が「学認」

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
  - テレビ会議システム

※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

「学認」に参加するとこんなメリットが

- ID管理側（IdP）メリット
  - 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
  - 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
  - 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
  - シームレス（学内外）なアクセス管理システム統合
- サービス側（SP）メリット
  - 学術機関に対するサービスのビジビリティの向上
  - 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
- 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，マッシュアップによるサービス連携への期待

「学認」への参加

- 参加申請は学認申請システムから
  - URL: https://office.gakunin.nii.ac.jp/
- まずはきちんと動作することを確認するため
  テストフェデレーションへ参加
  1. 申請情報登録（およびアカウント作成）
  2. 事務局での参加承認
  3. 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

「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
  - オフラインによる確認が1ステップ増えるだけ
  - 参加申請は機関の長の名前でお願い致します(学長など)
  - 参考：GakuNin道しるべ
    URL：https://www.gakunin.jp/document/98

- 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)
  - 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)
  - 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)
  - IdPを検索するシステム
    - フェデレーションが運用
    - 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

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」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

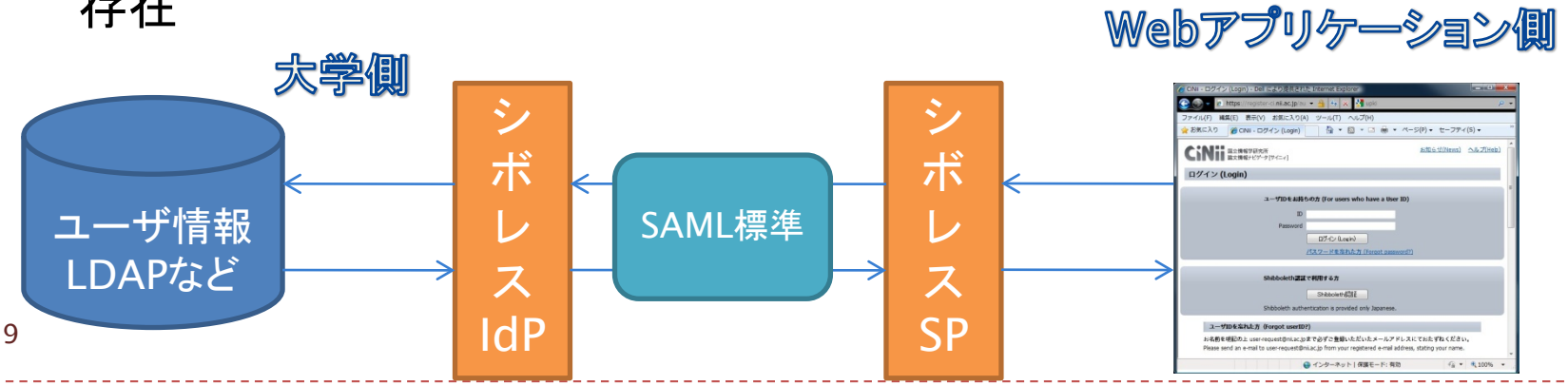
メタデータ

- 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結合して公開
  - 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

「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、学術界では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



SAML通信のためのフィルターのようなもの

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

IdPの調達と構築

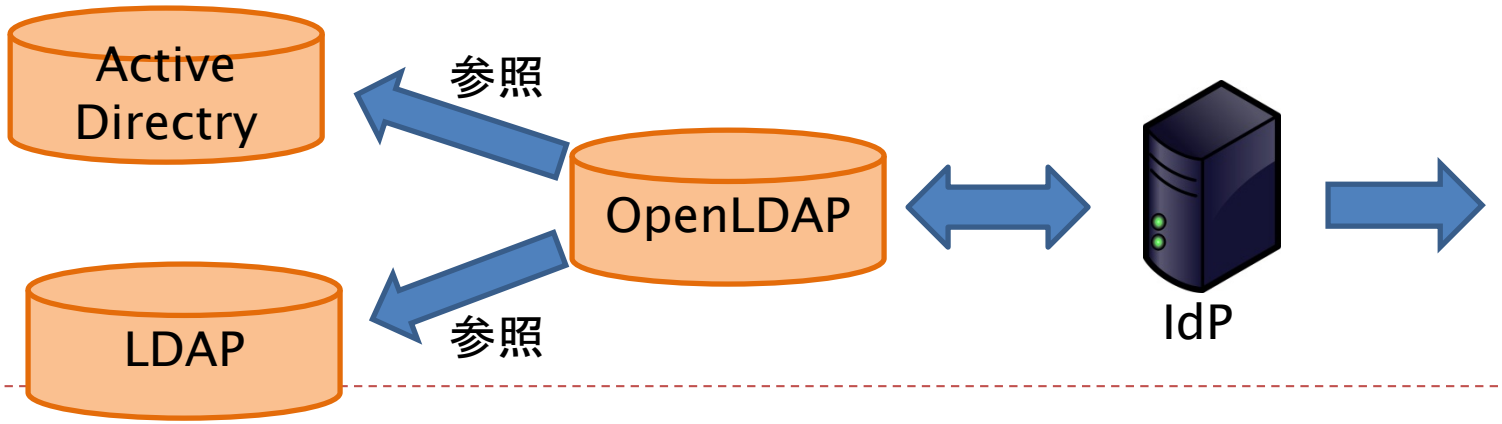
- ③クラウドサービスの利用
  - クラウド型IdPサービス(IDaaS)
    - IdPホスティングだけ？　ID管理も含める？
- 仕様書をどう書くか
  - 学認提供資料「学認参加のための学内説明用資料」に仕様・見積の例示あり
- 認証基盤を共存するADなどと共有できるか
  - 大元の認証基盤を、ShibbolethのOpenLDAPから参照するなど

IdP調達の仕様書等について

- IdPの冗長化構成をどうするか
  - 学認でIdP最新版対応の冗長化手順書公開
    - https://meatwiki.nii.ac.jp/confluence/x/25sxAQ
  - この手順書を提示して「これに従って冗長化すること」と盛り込む
  - バックエンドの冗長化は別途
- 学内システムをどこまでShibboleth SP化するか
  - SP化できないシステムがある場合、どうするか
    - 一部はADFS連携する、リバースプロキシでやるなど

認証基盤の調査

- 認証基盤はどうなっているか
  - 全学統一の認証基盤がある
    - LDAPやADをIdPと連携させる
  - 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工夫してください



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

SPの学認連携と学内連携について

- 学認連携(SPを学認に登録する)
  - 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
    - 利用できるIdPを制限可能

- 学内連携（SPを学認に登録しない）
  - 教務システムなど、各大学で独自に持っているシステムに適する
    - 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

「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)
  - 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・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

お知らせ：情報処理技術セミナー

NIIの教育研修事業として例年2日間コースでShibboleth等の実習を行っております

- 対象者：教育・研究機関等(大学、短期大学、高等専門学校、大学共同利用機関法人、大学校、独立行政法人、施設等機関、国立国会図書館等)の情報処理関連部署に勤務し、機関内のシステム運用・管理に係る業務を担当、もしくは6か月以内の担当を予定している教職員
- 基礎編
  - 日時：2019年7月18日(木)～19日(金)
  - テーマ：Shibboleth環境の構築
  - 申込締切：2019年5月31日(金)
- 活用編
  - 日時：2019年8月29日(木)～30日(金)
  - テーマ：構築されたShibboleth環境に対してアドバンストな機能の実現
- IDaaS編
  - 日時：2019年11月7日(木)～8日(金)
  - テーマ：IDaaS環境の構築・テスト・カスタマイズ
- 詳細：https://www.nii.ac.jp/hrd/ja/joho-karuizawa/

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）

mail: gakunin-office@nii.ac.jp

まで，お気軽にどうぞ。