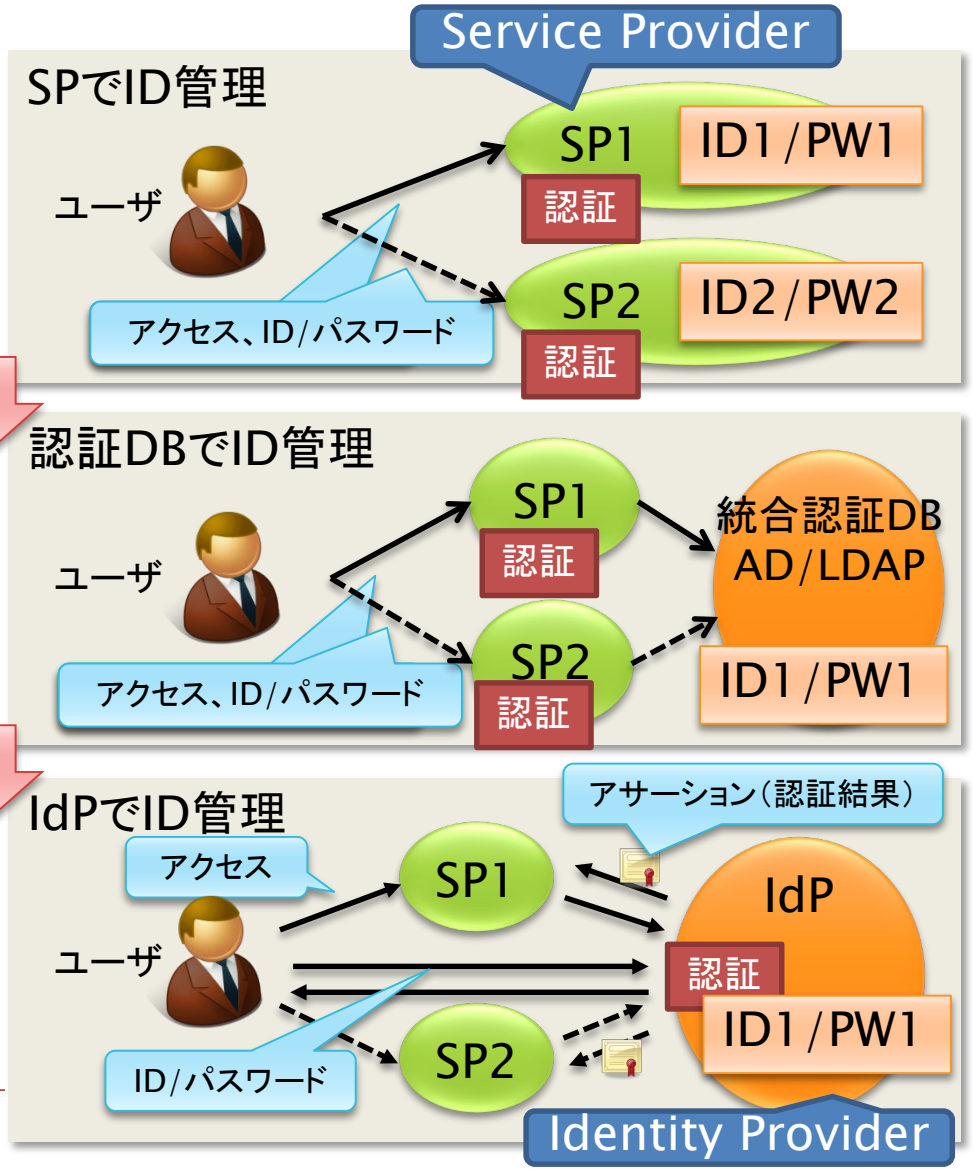
学認による本人認証の仕組みとLMSでの活用事例

国立情報学研究所
学術認証推進室　特任研究員　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）

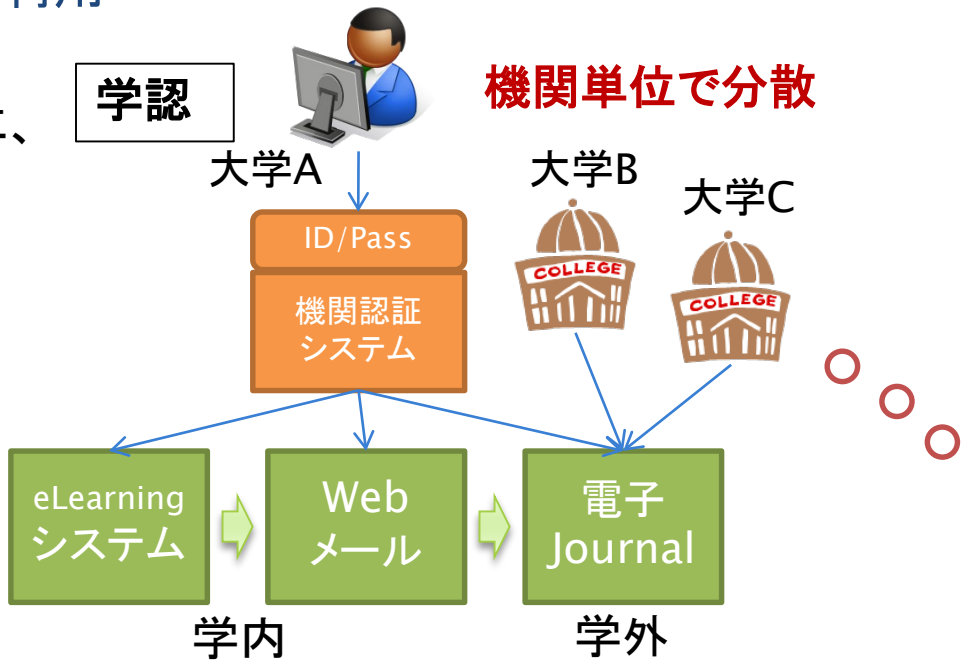
日本の学術認証フェデレーション「学認」

- 日本の学術系フェデレーションが「学認」

www.gakunin.jp

学術認証フェデレーション「学認」ってなに？

- WebアプリケーションへのSingle Sign-On(SSO)技術を、組織を越えて活用する分散型認証基盤
  - Single Sign-On：一度の認証で複数のサービスを再認証なく利用できる技術
    - 実現方法はいくつかあるが、フェデレーション内で技術の統一が必要
  - 安全・簡単・便利な統合認証を利用
    - 使用するID/PASSは一つだけ
    - 学認参加サービスの認証以外に、学内システムにも使える
    - その一方でセキュリティ水準を一定に保つ必要がある



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

「学認」参加よるサービス提供者のメリット

- 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
    - 認証は各機関のIdPで実施
    - サービス利用を組織単位で認可できる
  - ライセンス条件にそった適正な利用
  - コンプライアンス関連の負担を軽減
    - 個人情報の保存・処理を軽減

「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
    - 申請書の郵送が必要です
  - 参加申請は機関の長の名前でお願い致します(社長など)
  - 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！

SP構築の留意点

学認対応の属性について

- SPで受け取る属性について
  - どれだけの属性が必要か
    - 学認では21属性を利用
    - 全属性を出しているIdPはごく少ない
    - サービスに必要な属性を過不足なく要求する
  - 要求属性値の決定
    - ある機能を提供するにはどの属性値が必要か
    - SPが値を指定できるものもある

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

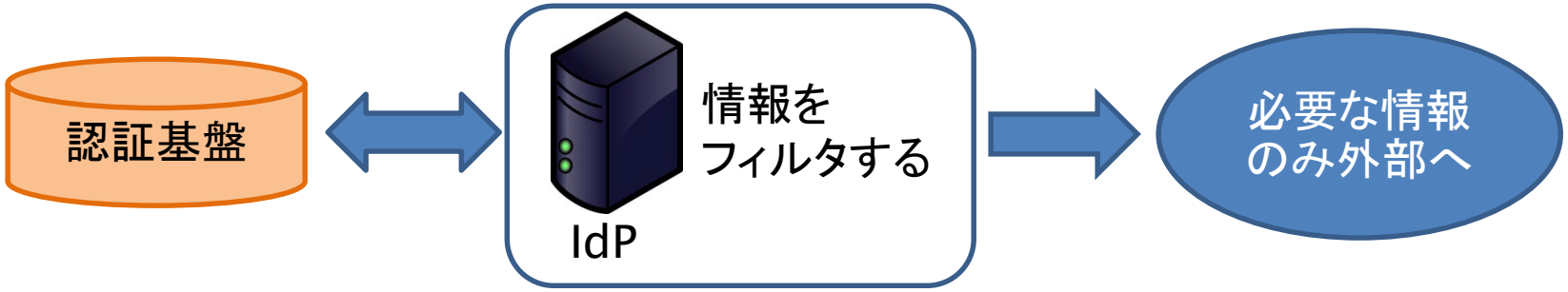
SP運用の注意点

- 契約機関への情報周知
  - サービス利用を契約した大学等に以下をお知らせください
    - サービスのentityID
    - サービスの利用に必要な属性
- IdPから送られた属性情報の取り扱い
  - サービス内部での利用にとどめてください
  - サービスの提供に必要な属性以外を取得しないようにしてください
- 脆弱性への対応
  - SPに使用されているソフトウェアのアップデート情報の収集
    - Shibbolethに関するものであれば学認情報交換MLでお知らせします
    - それ以外については独自収集が必要です
- 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」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

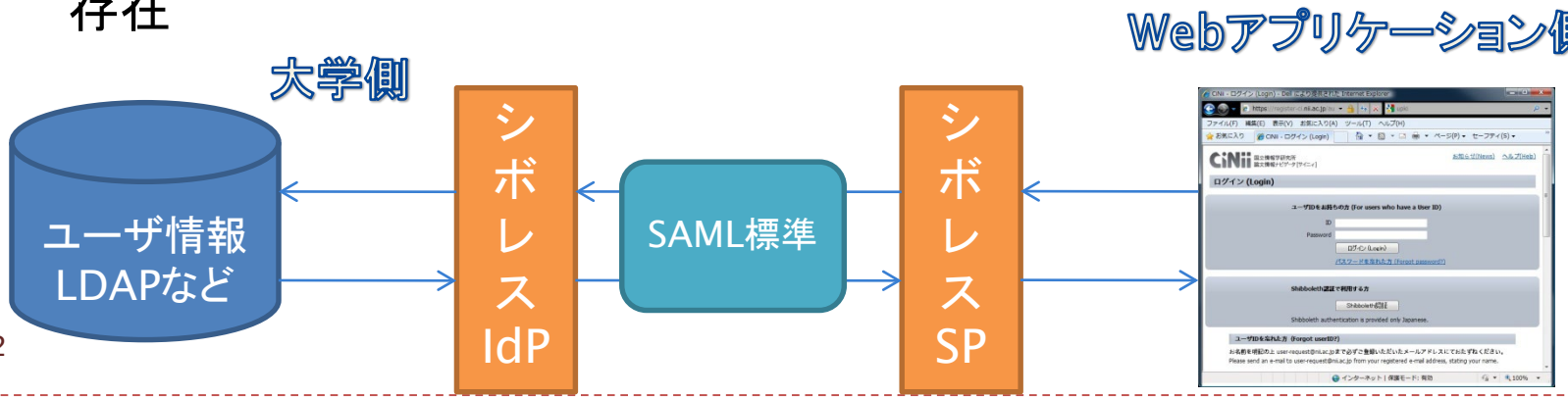
メタデータ

- 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

SP構築の注意点

- SAML2.0対応のミドルウェア利用が必要
  - 学認標準ではShibbolethの利用をおすすめしています
  - Shibboleth以外のミドルウェア(simpleSAMLphp等)も可
    - ただし学認のサポートはCentOS + Shibbolethの場合のみ
    - Windows ServerやShibboleth以外のミドルウェアの知見がありません

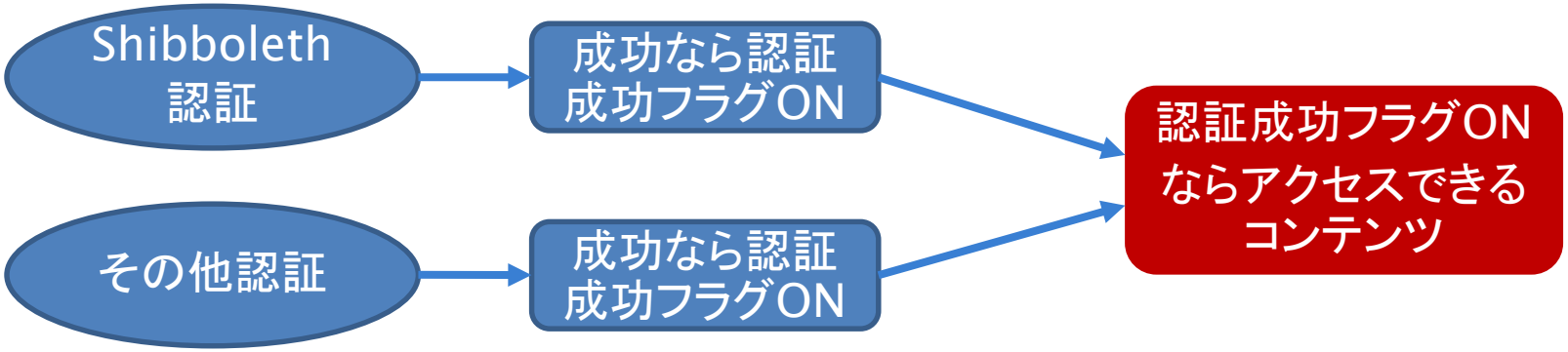
- 受け取った属性情報の取り扱いはWebアプリケーション側で実装
  - Shibboleth/その他SAML対応のミドルウェアは属性の受信まで
    - 受け取った情報をどう処理/取り扱うかはアプリケーション側で実装して処理しなければなりません
  - 属性情報はWebサーバの環境変数として格納
    - アプリケーションの実装言語で値を取り出してください
      - ex) phpの場合:$eppn = $_SERVER['eppn']
        - eppn:eduPersonPrincipalName属性

SP構築の注意点

- サービス利用の認証は学認だけか？
  - 学認経由の利用のみを想定？
  - 学認以外のユーザも受け入れる？
- ユーザの識別は必要か？
  - 契約した組織かどうかのみを確認できれば良い？
  - ユーザごとの識別も必要？
    - 識別に使う属性はどれにするか？
- 既存ユーザ情報と学認アカウントの紐づけ(ユーザを識別する場合)
  - 学認経由でない認証から学認経由の認証に切り替える際はどうするか
    - 別ユーザとして割り切る
    - なんらかの方法で紐づける
  - 紐づけを行う場合の方法の検討
    - 既存の認証方法でログイン→そのままログアウトせず学認で再ログインさせて既存プロファイルと学認アカウントを紐づける、など

SP構築の注意点

- Shibbolethで保護するアプリケーション領域の設定
  - Shibbolethでは%{DocumentRoot}/secure をデフォルトで保護
    - 保護された領域はアクセスにShibboleth(SAML)認証が必要
  - .htaccessでアクセスにShibboleth認証を必要とするディレクトリを指定可能
    - 保護ディレクトリの指定には注意が必要
    - アプリケーション全体を保護すると、Shibboleth認証以外での利用ができない
    - 特に、学認以外の認証方法を許容する場合は注意



学認についてのまとめ

- 学認における各役割
  - フェデレーション
    - フェデレーションメタデータの配布
    - IdPリスト(Discovery Service:DS)の提供
    - トラストフレームワークの運用(規程類、監査など)
  - IdP運用機関
    - 規程類の遵守
    - IDのライフサイクル管理・運用
    - IdP運用状況の点検・確認(監査)
  - SP運用機関
    - 規程類の遵守
    - サービスの提供
    - サービスの利用に必要な属性の周知

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。