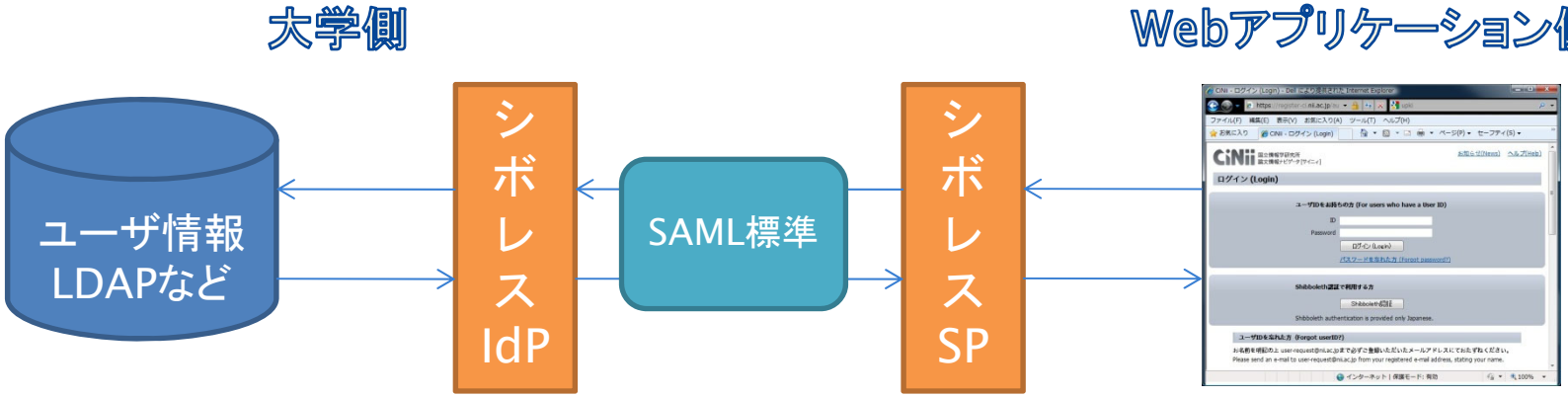
学認について

2021.11.17　NIIサービス説明会
国立情報学研究所　西村　健

学認の基礎

- 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



SAML通信のためのフィルターのようなもの

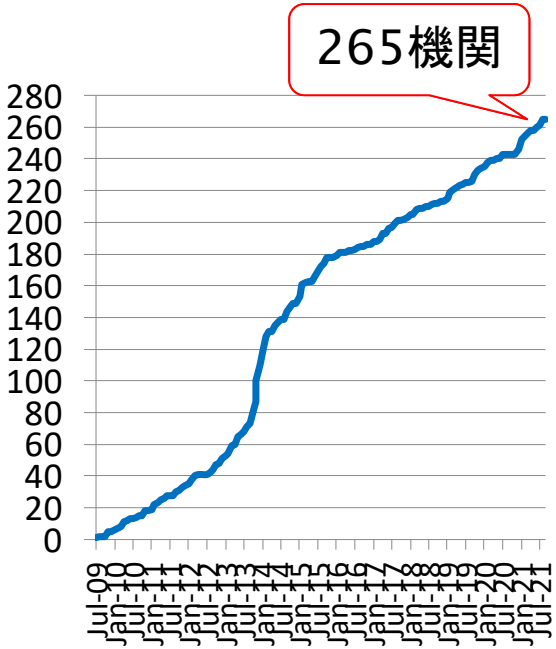
- 詳細は2019年NIIオープンフォーラム「はじめての学認」をご参照ください
  - https://www.nii.ac.jp/openforum/2019/day1_4.html
  - https://www.youtube.com/watch?v=pMCw7oJablo&feature=youtu.be

参考:「はじめての学認」の章立ておよび内容

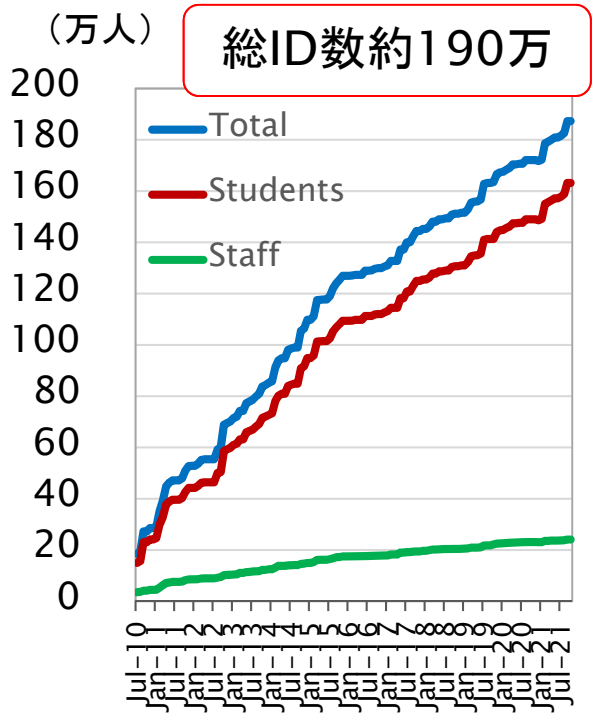
- 学認について
  - シングルサインオン・フェデレーションとは
  - フェデレーションの役割
  - フェデレーション参加機関の役割
  - 学認とは
  - 学認に参加するメリット
  - 学認への参加手順
- 「学認」に必要な技術
  - フェデレーションに必要なサーバ
  - メタデータとは
  - Shibbolethについて
  - IdPの調達と構築
  - 属性について
  - SPの学認連携／学内連携
- 「学認」参加後の運用について
  - 証明書の更新、責任者・担当者引継ぎなど

IdP/SPの推移（2021年10月末現在）

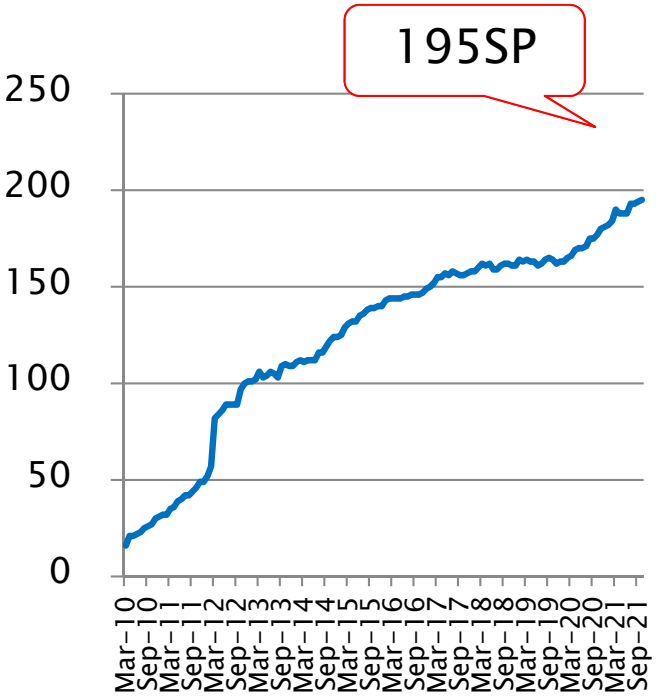
IdP機関数



IdPユーザ数



SP数



	国立大学	公立大学	私立大学	短期大学	高等専門学校	共同利用機関	その他	合計
学認参加数	78	28	92	1	51	4	11	265
カバー率	91%	31%	15%	0%	89%			
総機関数	86	91	604	333	57			

Shibboleth IdPバージョン4リリース（去年3月）

- 旧バージョンをお使いの方はすでにEOLを迎えておりますので移行をお願いします！
- 最新版は4.1.4 （3系の最終版は3.4.8）
- V4情報: https://meatwiki.nii.ac.jp/confluence/x/FCbxAg

- 注: パスワード等が credentials/secrets.properties に移動
- 新規インストール時のみに影響する項目（in-place upgrade時はV3時の挙動を受け継ぐ）
  - SAML1無効化
  - Attribute Query無効化
  - PKIX証明書検証無効化
  - AES-GCMがデフォルト 後述
  - CSRF protection
  - Attribute Registry 後述

Shibboleth IdPバージョン4に関して IdP管理者がやらなければならないこと

IdP管理者の方は

- お使いのShibboleth IdPバージョン3（or 2）を4にバージョンアップしてください
  - V3は今後脆弱性が発見されても更新されません！
  - ただし yum update のように簡単にバージョンアップできません。設定ファイル要修正
  - アップデート手順: https://meatwiki.nii.ac.jp/confluence/x/FCbxAg
  - ※V4に合わせて技術ガイドで使用するサーブレットコンテナをTomcatから Jetty に変更しました
    - 今後検証を重ねつつ乗り換えを案内していきます

- 今後SP追加（attribute-filter.xml追加）の際はV4向けの書式になっているか確認・必要なら修正の上適用ください
  - 世の中の情報はV3向けのまま更新されていない場合があります
  - 詳細: https://meatwiki.nii.ac.jp/confluence/x/P60HB

属性レジストリ(Attribute Registry)について

- V4新規インストールのみ影響
- 従来attribute-resolver.xmlに記述していたSAML2エンコード情報(<AttributeEncoder>)を別途管理する仕組み
  - 「id(attributeId)が所定の属性値と一致する場合、所定のOIDを付与して送信」
  - attribute-resolver.xmlはスッキリ
  - Simple AttributeDefinitionが不要になる場合も
- 学認からテンプレートとして配布している gakunin-rules.tar.gz を適用してください！
  https://meatwiki.nii.ac.jp/confluence/x/34S5
  - 学認で規定している、かつ、Shibboleth配布物には含まれない属性を属性レジストリに登録します
- 便利機能: exportAttributes
  - LDAP DataConnector等で生成された属性を直接出力するための仕組み
  - 属性名をスペース区切りで列挙する
  - 属性名を1つも指定していないとエラーになりますのでご注意を
    - 最近の学認テンプレートではダミーの属性名を指定してエラーを回避しています
  - 注:ここで列挙した属性名が属性レジストリに登録されているものと一致しなければならない(jaou とか)

TomcatからJettyへの移行

- 技術ガイドはV4からJettyで構築する記述となっています
- V3からの流れでTomcat 8/9をご使用の方々はJetty 9.4への移行をご検討ください
  - Tomcatで凝った設定をしている場合に移行問題があれば、お知らせください
  - （体感で）軽量です!

次に来た4.1の波

- 4.1.0が3月にリリースされました（最新版は4.1.4）

- プラグイン/モジュールを容易に扱える仕組みが導入されました
  - 組み込みの機能は多数モジュール化されております
  - 4.0.xからのアップデートの場合は自動的に有効化されますが、新規インストールの場合は最小限のモジュールが有効化された状態です
    - 新規インストールでオプション機能を利用する場合はモジュール有効化が必要な場合があります
      例：属性送信同意機能：https://meatwiki.nii.ac.jp/confluence/x/BixsB
  - 従来の形式のサードパーティープラグインもそのまま利用可能です

- /opt/shibboleth-idp/system/ 配下のファイルがJARファイル内に移動しているのでご注意を
  - uApproreJPインストール方法は修正済み
    https://meatwiki.nii.ac.jp/confluence/x/flADAQ

SPにおけるAES-GCM暗号対応状況について

- V4新規インストールのみ影響
- Shibboleth IdPv4より、新規インストール時のデフォルトのXML暗号化アルゴリズムの設定が従来のAES-CBCからAES-GCMに変更され、AES-GCMに非対応の一部のSPにて問題が発生しています。
  - IdPv3からのアップグレード時には従来通りのAES-CBCが維持されます。
- 現時点で問題があると情報が寄せられたSPは以下の5件です：
  - HeinOnline
  - Emerald Insight
  - Clarivate社のWeb of Science
  - HighWire
- 最新情報、IdPでの対処方法など以下でまとめます：
  https://meatwiki.nii.ac.jp/confluence/x/IShsB
- また、SP運用ご担当の方におかれましては、SPがGCMをサポートしているかをご確認いただき、サポートしていないことが判明しましたら、その旨を学認事務局までご一報いただけますと幸いです。
  - テストフェデレーションでGCMをテストいただけるテスト用IdPを提供しております。ぜひご利用ください。
    利用方法: https://meatwiki.nii.ac.jp/confluence/x/OoHDB

Shibboleth IdPバージョン4に関して
SP管理者がやらなければならないことその2

SP管理者の方は

- IdP管理者向けに出している情報がV4対応になっているかご確認ください
  - 書式および一部属性の表記が異なります
  - 参照: https://meatwiki.nii.ac.jp/confluence/x/k64HB
  - 個別にSP運用担当者にご案内差し上げる予定です

参考: ブラウザにおけるSameSiteなしcookieハンドリング挙動変更によるIdP/SPへの影響について（NIIオープンフォーラム2020資料より）

- 最新情報・詳細は: https://meatwiki.nii.ac.jp/confluence/x/AhEwAw
- Google Chromeにて、cookieの取り扱いに関する挙動が変更になり、この影響で特定の設定のIdP/SPにおいて期待するSSOの挙動を示さない、などの問題が発生する可能性があります。

- Shibboleth IdPについて:

  下記の影響が見られますのでHTML Local Storageの有効化（idp.storage.htmlLocalStorage=true）が推奨されています。
  - （学認の技術ガイドに沿って構築したIdPについて）特定のSPからの認証要求でSSOが期待される場面でもログイン画面が表示されID/パスワードを要求される
- Shibboleth SPについて:

  学認技術ガイドに沿った構築でかつWebアプリケーションの構成が単純な場合、影響を受けない模様です。
  - RelayStateにcookieを使うよう設定変更をしている場合、認証に時間がかかると本来の遷移先を忘れ認証後にサイトトップ等に遷移する
  - Webアプリケーションが独自にセッションを管理しておらずShibbolethセッションに依存している場合、クロスサイトのPOSTを伴う場合にログイン状態が維持されない
  - Form Recovery機能を有効にしている場合、認証に時間がかかるとこれが機能しない

- これはSAMLの仕様に起因するものであるため、Shibboleth以外（simpleSAMLphp,ADFS等）のIdP/SPも影響を受ける可能性がございます。またSP側のWebアプリケーション自体に、クロスサイトでデータを受け渡すことに依存する部分があれば今回の挙動変更の影響を受ける可能性があります。

運用されている各IdP/SPでサービスの挙動に問題がないかご確認をお願いいたします

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。