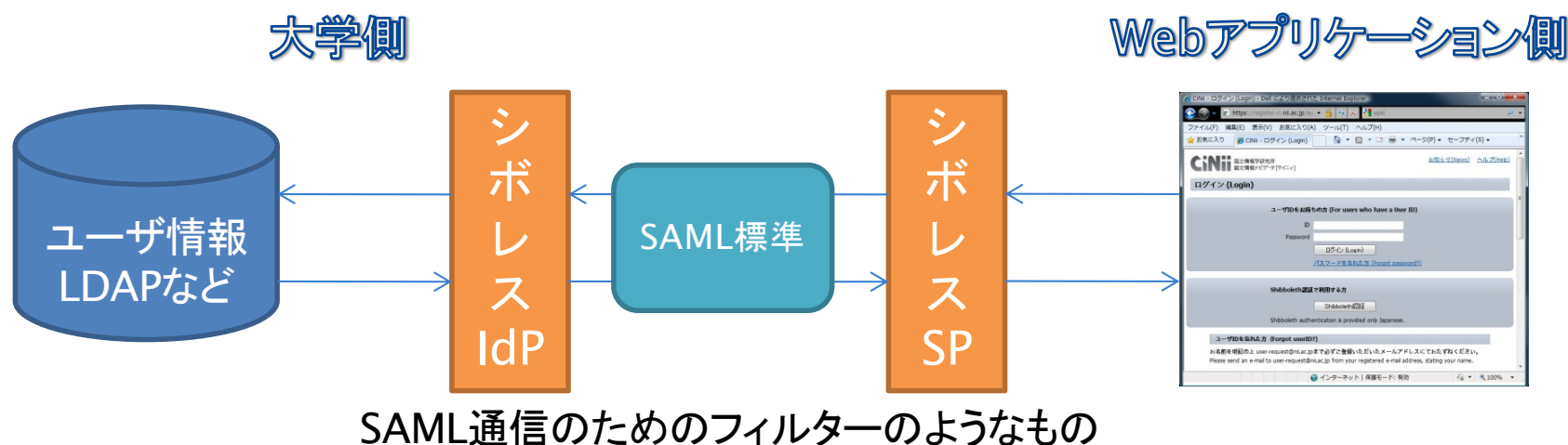




学認について

2021.1.19 NIIサービス説明会
国立情報学研究所 西村 健

- ▶ 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

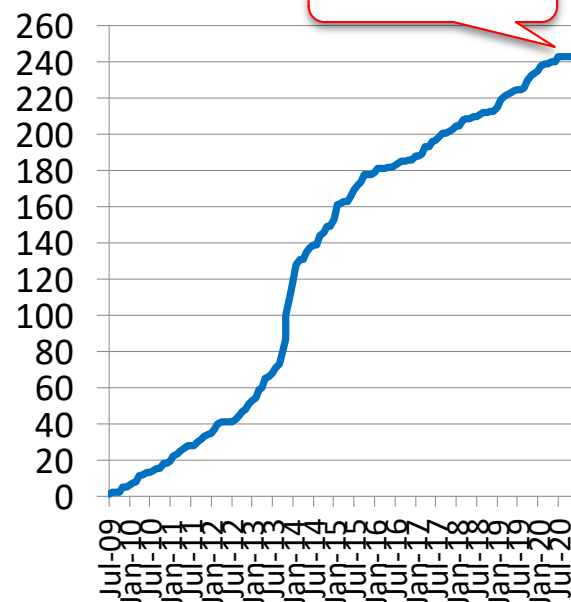


- ▶ 詳細は2019年NIIオープンフォーラム「はじめての学認」をご参照ください
 - ▶ https://www.nii.ac.jp/openforum/2019/day1_4.html
 - ▶ <https://www.youtube.com/watch?v=pMCw7oJablo&feature=youtu.be>

IdP/SPの推移(2020/12末現在)

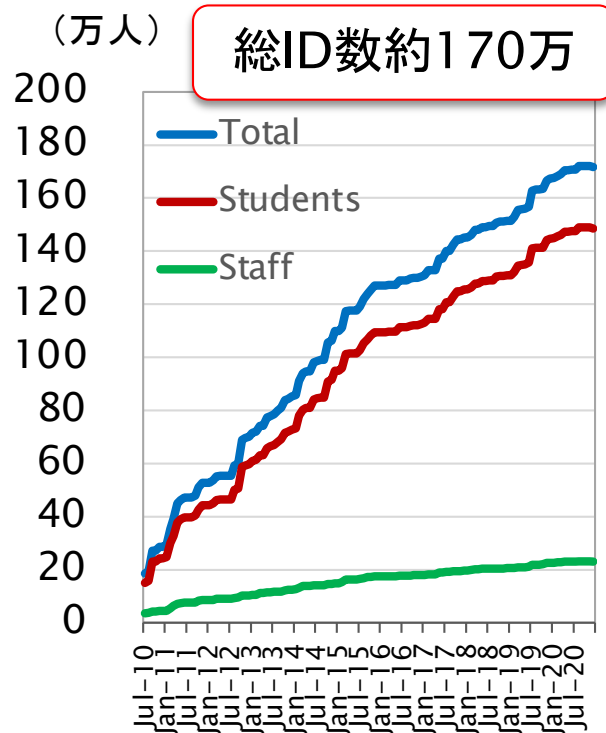
IdP機関数

243機関



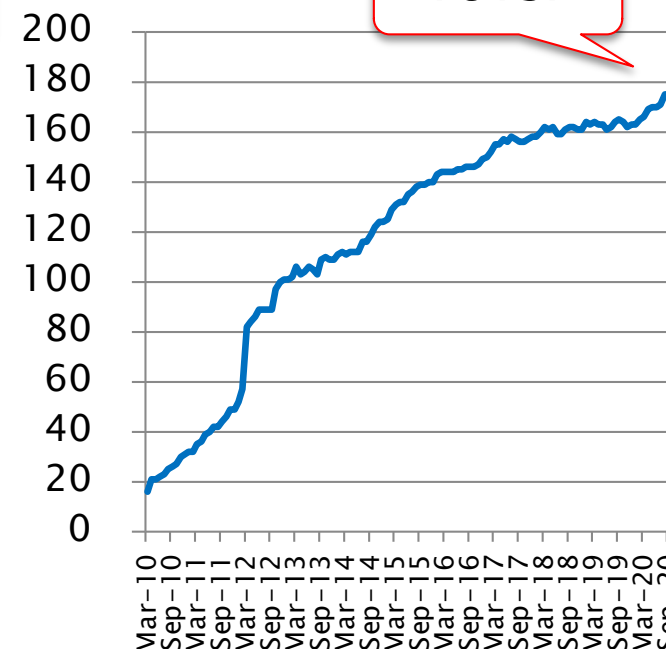
IdPユーザ数

総ID数約170万



SP数

181SP



	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	77	25	76	0	51	4	10	243
カバー率	89%	27%	13%	0%	89%			
総機関数	86	91	604	333	57			



Shibboleth IdPバージョン4に関して IdP管理者・SP管理者がやらなければならないこと(1 / 2)

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>





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

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
- ▶ 今後提供するV4対応情報
 - ▶ TigrShibプラグイン(必要な方は個別に事務局までご連絡ください)
- ▶ ちなみに、最新版は2020年6月3日リリースの4.0.1
3系の最終版は3.4.8





GakuNin

テストフェデレーション署名鍵更新(2020年12月実施)

- ▶ テストフェデレーションの署名鍵を10年周期で更新しており、去年12月に新鍵・証明書に切り替えました
 - ▶ 学認情報交換MLにてアナウンス済み
 - ▶ 11月以前に構築したテストフェデレーションのIdPもしくはSPをお持ちの場合は、今一度設定をご確認ください
- ▶ 新証明書の情報は以下の通り
 - ▶ 公開URL: <https://metadata.gakunin.nii.ac.jp/gakunin-test-signer-2020.cer>
 - ▶ SHA256 Fingerprint=
FA:11:11:5B:EC:13:4D:55:85:AF:60:32:E1:6C:01:01:EF:9C:A0:6B:17:8C:8B:9C:7F:2B:69:
41:EB:68:30:1E
- ▶ Shibboleth IdP/SPにおける設定変更方法を下記ページでご案内しました
 - ▶ 一時的に新旧2つの証明書を併記することで、切り替えXデーに関わらずいつでも問題なく設定変更いただくことが可能
- ▶ IdP設定変更手順: <https://meatwiki.nii.ac.jp/confluence/x/WZcHB>
- ▶ SP設定変更手順: <https://meatwiki.nii.ac.jp/confluence/x/W5cHB>

▶ 更新を実行された方は、古い証明書を削除するのを忘れずに



NIIが提供するSPのご紹介その1: FaMCUs

- ▶ テレビ会議用MCUサービスの予約・制御機能です
- ▶ FaMCUs終了のお知らせ
 - ▶ 新型コロナウイルス感染拡大に伴うZoom等のオンライン会議サービスの認知度向上・普及の影響もあってか、FaMCUsサービスのご利用数が減少しております。
 - ▶ このような状況から、維持コストとご利用率の観点から、令和2年度末(2021年3月31日)をもちましてFaMCUsサービスの運用を終了することとさせていただきます。
 - ▶ 学認の黎明期に提供を開始したFaMCUsを長きに渡りご利用いただきました皆様のご愛顧に感謝申し上げます。
 - ▶ 終了までのスケジュールなど近日中に学認情報交換MLにてアナウンスいたします。





NIIが提供するSPのご紹介その2: NII FileSender

- ▶ 学認にIDをお持ちの方が安全にファイル交換できるサービスです

- ▶ NII FileSenderバージョン2
 - ▶ 目玉はEnd-to-End暗号化！
 - ▶ ただしグループメンバー全通知機能などV1でのNII独自カスタマイズは削除
 - ▶ 同等機能について検討中
 - ▶ 今年度中に移行を実施予定です。
 - ▶ V2での変更点や移行スケジュールなど近日中に案内予定です。学認情報交換MLでのアナウンスにご注目ください。
 - ▶ 連携するIdPではeduPersonTargetedIDを送信するように設定変更をお願いします！（V1では任意）



参考: SPにおけるAES-GCM暗号対応状況 情報収集のお願い (NIIオープンフォーラム2020資料より)

- ▶ 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。
- ▶ 非Shibbolethの大部分のSPや、一部の古いShibbolethや古いOS (RHEL/CentOS 5等)ならびに古いソフトウェアを用いているSPはGCMをサポートしておらず、GCMに変更した場合はこれらのSPと連携が取れなくなるとの情報がございますので、IdPv4を新規インストールされる際はご注意ください。
- ▶ 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。
- ▶ 詳細はShibboleth Wikiの下記ページをご参照ください。
 - ▶ <https://wiki.shibboleth.net/confluence/display/IDP4/GCMEncryption>



GakuNin

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。