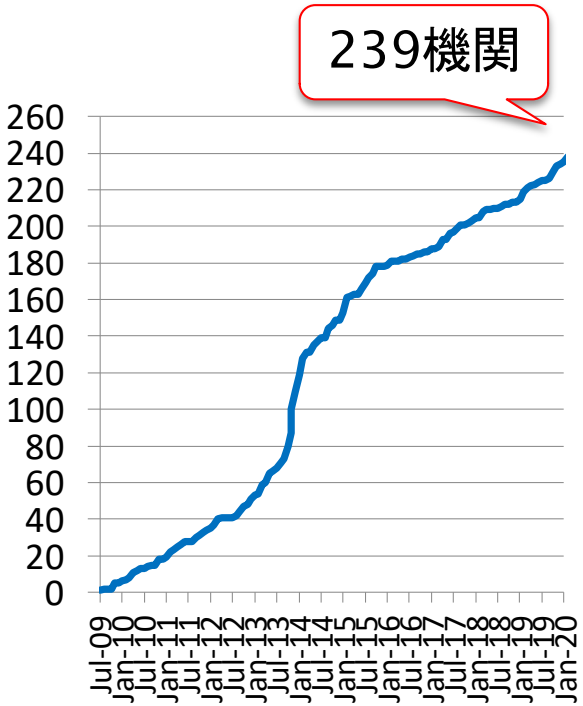
学認アップデート

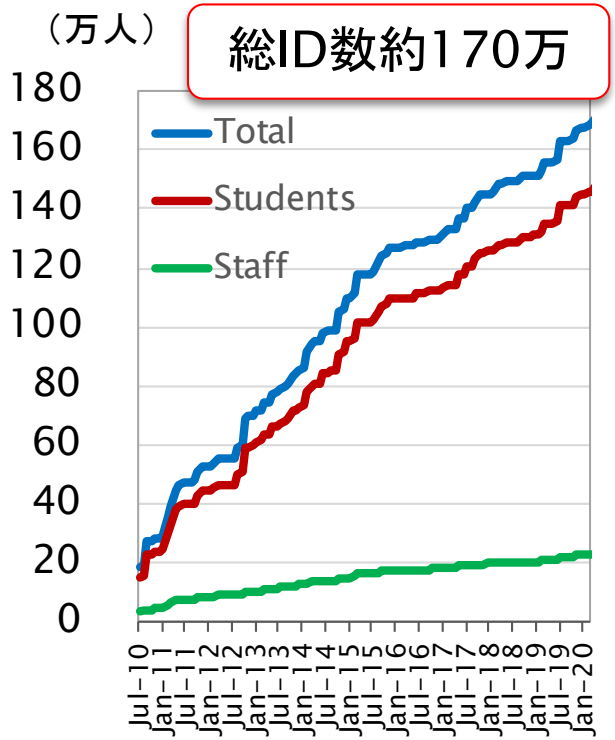
2020.6.10　NII学術情報基盤オープンフォーラム2020
国立情報学研究所　西村　健

IdP/SPの推移（2020/5末現在）

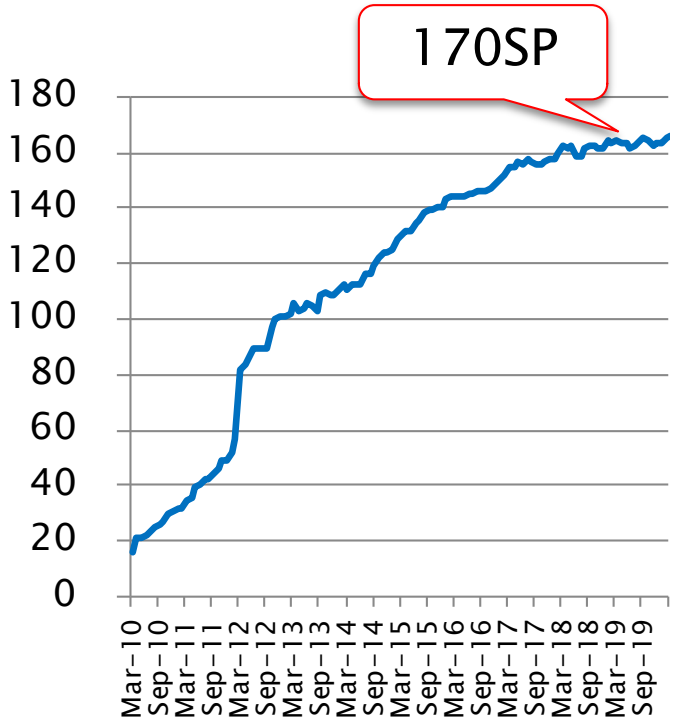
IdP機関数



IdPユーザ数



SP数



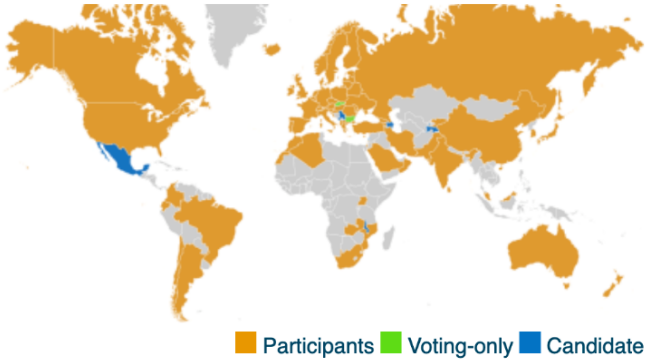
	国立大学	公立大学	私立大学	短期大学	高等専門学校	共同利用機関	その他	合計
学認参加数	77	24	74	0	51	3	10	239
カバー率	89%	26%	12%	0%	89%			
総機関数	86	91	604	333	57			

学認の近況について

- 学認実施要領および学認技術運用基準改定（2/28）
- Shibboleth IdPバージョン4リリース（3/11）
- eduGAIN
  - 学認からの参加数(2020年6月現在)
    - IdP:44 （この2か月ほどで+8機関！）
    - SP:4

eduGAIN

- 世界各国の学術IDフェデレーションを相互接続(inter-federation)し、グローバルな研究・教育コミュニティのためのコンテンツ、サービスなどの資源へのアクセスを容易にすることを目指しています
  - https://edugain.org/
- eduGAINには、60以上の国と地域が参加しています
  - 3000以上のIdPと、2000以上のSP
  - ORCID, SheerID, Dropbox, FileSender, MATLAB, 一部の電子ジャーナル など



https://technical.edugain.org/status

- 学認からはオプトインで参加できるようになっています
  - 参加するには、学認申請システムで「eduGAINに参加する」にチェック
    - 注意:連絡先種別は「support」または「technical」としてください
  - 残りの設定手順は学認ウェブサイトの「eduGAINに参加する」参照のこと
    - ⇒https://www.gakunin.jp/join/eduGAIN/

- ※最初期にeduGAINに参加した方へ:メタデータダウンロードにCDNを使うように設定手順が変更されておりますので設定を今一度ご確認ください

学認実施要領および学認技術運用基準改定

- 大規模国際連携プロジェクトの推進のため、条件付きで「機関の設置した組織」からのIdPの参加を認めるための改定を行いました
- SP参加の場合についても、同様に条件付きでサービス提供担当部署からの申請を認めることとしました
- 詳細は事務局までお問い合わせください

- 学認実施要領
  - https://www.gakunin.jp/document/74
- 学認技術運用基準（最新はv2.5）
  - https://www.gakunin.jp/document/80

以前の id.nii.ac.jp のURLではアクセスできなくなっておりますのでご注意ください!

Shibboleth IdPバージョン4リリース（3/11）

- Shibboleth IdP v3.xのEOLについて、2020年12月末と公表されました
- Shibboleth IdP v4への移行の準備をお願いします
  - https://meatwiki.nii.ac.jp/confluence/x/FCbxAg
  - v2からv3へのアップデートほどの混乱は起きないと思われる
  - 旧書式(DEPRECATED)の設定がv4ではエラーとなります
  - v3.4ではDEPRECATEDのwarningとしてログに出力
    - v3.4系の最新版でチェックしてください
  - 最も影響の大きいフラット化については別ページがありますのでご注意を
  - 次に影響が大きいものとしては、<Dependency>要素は内容によって<InputAttributeDefinition>と<InputDataConnector>に変更が必要
  - 詳細は本家参照：https://wiki.shibboleth.net/confluence/x/PgLKAg
    - 変更のある要素の置き換え方法へのリンク等含めて記載
  - v4.0準備としてwarningが出なくなるまで設定ファイルを修正することを推奨

フラット化およびDEPRECATED対応の学認テンプレート配布中

Shibboleth IdPバージョン4についてその他

- Java 11以上が必須となり、またv3で使われていたTomcat 7はv4では非対応となります
- LDAP連携のためのライブラリがJNDIからUnboundIDに変更になり、凝ったことをしている場合は若干の設定変更が必要です
- NIIが提供しているIdPプラグインは順次対応版を提供予定です
  - uApproveJP
  - TiqrShib
  - TOTP（手順書）
- また技術ガイドもv4向けに更新してまいります
- v4からの目玉の新機能については後日解説予定
  - authn/SAMLログインフロー（アサーションのプロキシ）
  - OIDC対応本格化（IdPプラグインとして）
  - 属性レジストリ（conf/attributes/default-rules.xml）

Shibboleth IdPバージョン4についてピックアップ

- IdPv3の環境を引き継ぎたい場合は、別ホストで引き継ぐ場合もIdPv4の環境を新規に構築するのではなく、一旦IdPv3の環境を構築（ディレクトリコピー）し上書きインストールしてください。（in place upgrade）

大文字小文字同一視(ignoreCase)問題

- 規定はされている、が、読んでない人がいる
- eduPersonTargetedIDにおけるBASE32推奨(3.3.2から)
  - 仕様上caseExactMatchなのだがignoreなSPが多いためShibbolethが折れた
  - saml-nameid.properties:
    idp.persistentId.encoding=BASE32
  - 現行の学認テンプレートはこれを参照していない=BASE64（デフォルト）

運用中のsaml-nameid.propertiesのBASE〇〇を確認してください！
詳しくは技術ガイドの学認テンプレートv3.4.0の注意書きをご参照ください!
https://meatwiki.nii.ac.jp/confluence/x/34S5

- データベースにストアされるユーザーID、大文字小文字同一視していますか？
- LDAPにおけるユーザーIDについてはどうでしょうか？
  - 全角半角同一視問題も…
- 今一度チェックしてみてください

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
今年度の基礎編・活用編はオンラインで実施します！

- 教育・研究機関等のシステム運用担当の教職員を対象としています
- 基礎編
  - 7月16~17日
  - テーマ：Shibboleth環境の構築
- 活用編
  - 9月3~4日
  - テーマ：Shibboleth IdPバージョン4移行を含めた構築されたShibboleth環境に対してアドバンストな機能の実現
- IDaaS編
  - 11月5~6日
  - テーマ：IDaaS環境の構築・テスト・カスタマイズ
- 詳細は下記にて：
  https://hrd.nii.ac.jp/joho-karuizawa/2020

研究奨学環境のスムーズな連携のために

- 大学・研究機関等の様々な活動がオンライン化を余儀なくされている昨今、研究者がすぐに研究環境にアクセスできるよう取り組みを進めています
  - eduGAIN経由の国際連携が目下のターゲットです
- SIRTFI (Security Incident Response Trust Framework for Federated Identity)
- REFEDS R&S (Research and Scholarship)（近日提供予定）

研究奨学環境のスムーズな連携のために – SIRTFI (Security Incident Response Trust Framework for Federated Identity)

- SIRTFI (Security Incident Response Trust Framework for Federated Identity)
  - 認証連携におけるセキュリティ対策・インシデント対応を求められたときにその体制が整っていることを宣言するための枠組み
  - eduGAIN SPの中にはこの宣言を要求するものがあります（CERN, CILogonなど）ので、そのSPを利用しようとするIdPはSIRTFIを宣言する必要があります。
    - 端的には、インシデント対応に責任を持つ連絡先（メールアドレス）の登録とメタデータでの公開が必要
  - 詳細は: https://refeds.org/sirtfi

研究奨学環境のスムーズな連携のために –
REFEDS R&S (Research and Scholarship) （近日提供予定）

- REFEDS R&S (Research and Scholarship)（近日提供予定）
  - Wikiやプロジェクト管理などコラボレーションツールを対象としたスムーズな利用のための枠組み
  - R&Sとして審査を受けたSPに対してIdPは以下の属性情報をまとめて提供
    - Personal identifiers: email address, person name, eduPersonPrincipalName
    - Pseudonymous identifier: eduPersonTargetedID
    - Affiliation: eduPersonScopedAffiliation（オプショナル）
  - IdPにおいて個別SPに対する作業なく対象SPが利用できるようにすることでeduGAINの活用を促進
  - 詳細は: https://refeds.org/research-and-scholarship

学認における多要素認証について(1/2)

- 参加機関が導入しやすいように統一的な基準を制定
  - 学認多要素認証プロファイル
    - アサーションに含める値を定義するプロファイル
      - 当該ユーザが多要素で認証されたことを明示し、保証
    - REFEDSのプロファイルをベースに作成
      - 学認のプロファイルとイコールではないが、条件を満たそうとしたときに、余分な処理が必要ないよう配慮
      - 将来的にeduGAINのSPとの連携も容易になる
  - UPKIクライアント証明書を多要素認証の1要素とする基準とガイドを作成
    - 体制やルールの構築・整備を高速化・容易化
    - 学認MFAクライアント証明書運用基準
      - この基準に従うことで、学認多要素認証プロファイルに定める、IdPから送出するSAMLアサーションの基準に適合する
    - 学認MFAクライアント証明書運用ガイド
      - 本ガイドラインにそってクライアント証明書を運用すると、「学認多要素認証プロファイル」に定めるSAMLアサーションをIdPから送出する資格を満たす

学認における多要素認証について(2/2)

- クライアント証明書以外の要素を用いる場合は、その要素に対応した運用基準・運用ガイドの策定が必要
  - FIDOなど
  - これらについては順次策定を検討する

- 以下のプラグイン開発・設定手順書の提供
  - FIDO2
    - 以下のサーバー実装を利用したIdPプラグインを近日提供予定
      https://github.com/duo-labs/webauthn.io
  - 証明書認証
  - TiqrShib
  - TOTP
  - Shibboleth MFA
    - 各種認証を要素(ログインフロー)として取り扱う
    - 組み合わせ自由自在

NII FileSender

- ストレージ増設しました！

SPにおけるAES-GCM暗号対応状況 情報収集のお願い

- 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)/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

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

- 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。