学認への参加と運用について(1/3)

- **参加について**
  - ✓ 学認への参加は無料です。参加にあたっては、SINETへの加入の有無は不問です。詳細は、学認実施要領を参照してください。病院等の参加も受け付けています。
  - ✓ 学認では、テストフェデレーションと運用フェデレーションの2種類のフェデレーションを提供しています。テストフェデレーションは、構築したシステムの技術的な動作検証を行うための環境です。運用フェデレーションでは、実アカウントを利用して実サービスが利用できます。
  - ✓ いずれのフェデレーションも、参加手続きは、「学認申請システム」（http://office.gakunin.nii.ac.jp/）から申請してください。テストフェデレーションは誰でも参加できます。運用フェデレーションの場合は、印刷し機関として責任を持つ者が押印した申請書の郵送が必要となります。
  - ✓ 申請は、認証サーバ（IdP）、サービス提供サーバ（SP）一台ごとにお願いします。
  - ✓ 学認に参加することで、何らかの有料サービスが無料で利用できるようになるわけではありません。必要に応じてSP毎に別途契約をお願いします。既に契約がある場合は、一般に、学認によるアクセス開始の申請がSP毎に必要です。詳しくは、学認WebのSP一覧を参照してください（https://www.gakunin.jp/participants/）。
  - ✓ 学認に参加することで、学内のコンテンツが自動的に学外から参照されるようになるわけではありません。
- **利用者の範囲について**
  - ✓ 学認において認証できる利用者の範囲は、原則として、教職員（名誉教授を含む）および学生です。電子ジャーナル等、有償サービスの契約条項で定められた利用者の範囲とは異なることがあります。各サービスとの契約が優先されますので、これに反することのないよう注意をお願いします。
  - ✓ SPによっては、利用が許可された利用者であることを後述の属性情報（eduPersonEntitlement等）で提示することにより区別できるものがあります。
  - ✓ SPが必要とする属性情報をIdPから送出しないことにより、特定の利用者に対してサービスの利用を制限することも技術的には可能です。詳細は学認WebのFPSP (Filter Per SP)プラグインの説明を参照してください。
  - ✓ 利用者に関する情報を、学生と教職員で異なるLDAPに分けて管理しているような場合や、キャンパス毎に異なるLDAPで管理しているような場合でも、一つのIdPからそれらを参照して認証させることが可能です。但し、IDが重複しないようにする必要があります。
- **セキュリティについて**
  - ✓ 利用者は、認証の際にIDとパスワードをIdPに対して入力しますが、それらはIdPでの本人確認にのみ利用され、SPには送られません。パスワードはIdPのみに閉じて扱われるため、連携するSPが不正アクセス等で侵入されてもパスワードが漏洩することはありません。
  - ✓ 認証情報を含む利用者情報は、LDAPやActive Directory (AD)（学内統合認証データベースの類）で管理し、IdPからこれらを参照するのが一般的です。基本的に、IdP上で利用者情報を管理する必要はありません。
  - ✓ IdPおよびSPでは、通信の暗号化と、成りすまし防止のためのデジタル署名用に、サーバ証明書を利用します。学認の参加の際に必要となるサーバ証明書として、UPKIサーバ証明書が利用できますが、商用のパブリックなサーバ証明書も利用可能です。
  - ✓ IdPでは、様々な認証方式に対応できる仕組みを持っています。クライアント証明書認証や多要素認証等の高度な認証方式にも対応可能です（Login Handlerの設定）。
  - ✓ システム構築時には、脆弱性のある古いバージョンを利用しないよう注意してください。また、運用に当たっても、セキュリティ情報に注意し、ソフトウェアのバージョンアップ等への迅速な対応をお願いします。

（続く）

情報・システム研究機構 国立情報学研究所 National Institute of Informatics
学術基盤推進部 学術基盤課 総括・連携基盤チーム
TEL:03-4212-2218　FAX:03-4212-2230　e-mail: gakunin-office@nii.ac.jp

学認への参加と運用について(2/3)

- **属性情報について**
  - ✓ 学認では18種類の利用者に関する属性情報を定めていますが、属性情報を全て準備する必要はありません。広く利用されているものはごく一部に限られます。最低限準備が必要なものはO、jaO、eduPersonPrincipalName、eduPersonTargetedID、eduPersonAffiliation/eduPersonScopedAffiliationです。
  - ✓ SPごとに要求する属性情報が決まっています。大学として利用したいSPを選定し、SPごとの情報（SP一覧に掲載）を参照して必要となる属性情報のみ送出するようにIdPを設定してください。
  - ✓ IdPの設定は学認申請システムと連携した設定が可能です。学認申請システム上で、利用するSPにチェックを入れると、そのSPを利用するための属性情報送出の定義が自動生成されIdPに読み込ませることができます。詳細は「attribute-filterの自動生成機能を使う」を参照してください。
  - ✓ SPが要求する属性情報には、必須(mandatory)と任意(optional)の区別があります。任意の属性情報は必ずしも送出する必要はありません。SPによっては、任意の属性情報を送信することで、利用可能な機能が増えることがあるので、SPごとの属性情報利用に関する説明を確認してください。
- **プライバシー保護について**
  - ✓ 学認では個人を特定するための識別子をIdPからSPに送出することになりますが、これについて3通りの形態が提供されています。
    1. Autonym/実名 (eduPersonPrincipalName) ― 全てのSPに対して共通となる識別子です。
    2. Anonym/匿名 ― SPに対して識別子を送信しません。電子ジャーナル等のサイト契約など、利用者を特定する必要のない場合のアクセス方法です。セッション毎の識別子はやりとりされるため、不正アクセスを追跡することは可能です。
    3. Pseudonym/仮名 (eduPersonTargetedID) ― SPごとに異なる識別子です。SPをまたがった利用者行動履歴に対する名寄せを防止します。
       なお、eduPersonTargetedIDの管理方法には、computed IDとstored IDの2通りありますが、ハッシュ衝突等の考慮がなされたstored IDを推奨します。
  - ✓ 属性情報の中には氏名やメールアドレスなどの個人情報に該当するものも含まれます。IdP用のプラグインuApprove-ipを利用すると、IdPから送出される属性情報を利用者が確認でき、さらに送出する属性情報を選択することが可能です。これを利用することで、国立大学等に求められる個人情報の第三者提供時のオプトインに対応することが可能です。
- **運用フェデレーションでの動作確認**
  - ✓ IdPから送信される属性情報の確認には、以下のSPによる属性情報表示サービスが利用できます。テスト時には、不必要に個人情報が送出されないようにご注意ください。
    - https://attrviewer20.gakunin.nii.ac.jp/ (SAML 2.0用)
    - https://attrviewer13.gakunin.nii.ac.jp/ (SAML 1.3用)
- **DS（ディスカバリーサービス）**
  - ✓ IdPの申請が承認されると、学認が提供するDS上の機関一覧に掲載されます。
  - ✓ DS上で機関名が選択できても、全てのSPが利用できるわけではないことに注意してください。別途、SPへの利用申請が必要かどうかは、SPごとの説明を参照してください。（一般に、SPが独自にDS機能を有している場合は、SPに利用申請を行う必要があります。）
  - ✓ SP側において、利用を許可している機関のみをDSの一覧で表示させたい場合は、SP独自でDS機能を実装する他に、学認で提供しているEmbedded DSをSPに組み込む方法があります。この場合、アクセスを許可するIdPのリストは、JSON形式（DiscoFeed形式）で用意します。また、Embedded DSを用いると、学認に参加していないIdPをリストに表示させることも容易です（Shibboleth環境構築セミナー：活用編：Embedded DSの導入を参照）。

（続く）

情報・システム研究機構 国立情報学研究所 National Institute of Informatics
学術基盤推進部 学術基盤課 総括・連携基盤チーム
TEL:03-4212-2218　FAX:03-4212-2230　e-mail: gakunin-office@nii.ac.jp

学認への参加と運用について(3/3)

- **サーバ証明書の更新**
  - ✓ IdPおよびSPで使用するサーバ証明書の有効期限切れによる更新の際は、メタデータで古い証明書と新しい証明書を同時に使用する期間を設けることで、サービス利用の中断が発生しないようにします。通常、この期間には2週間を要します。詳しくは学認WebのIdP Key Rollover/SP Key Rolloverのページを参照してください。
- **IdP冗長化について**
  - ✓ IdPの可用性を高めるために冗長構成をとることが可能です。冗長化の方法はいくつかあります。詳細は技術情報のIdP Clusteringのページを参照してください。
- **Webアプリの学認対応（SP化）について**
  - ✓ 「学認対応学内システム情報」のページで情報を提供しています。情報をお寄せください。
  - ✓ IdPでの認証が成功し処理がSPに戻ってくると、IdPから送られてきた属性情報は、環境変数を介して参照することができます。
  - ✓ Webアプリケーションの学認対応（SP化）には大まかに以下の4つの方法があります。
    1. Webアプリの手前にShibboleth認証と従来認証を橋渡しするリバースプロキシを設置（Webアプリの改変なし）
    2. Apacheの認証機能からShibbolethの認証処理を呼び出す（Webアプリの改変なし）
       （詳細については技術ガイドの「Webアプリケーションのシボレス化」を参照）
    3. 既存のローカルアカウントに紐づける（全てのユーザは、既にローカルアカウントを発行されている）
       （アカウントの紐付けを行う手順を用意すれば、対応作業はほぼ完了）
    4. Webアプリ側で独自のアカウント管理を行わない（新規にShibboleth対応のWebアプリを開発）
       （メールサービスなど、利用者がログインする前からサービス提供が始まる場合は、別途、プロビジョニング作業が必要となる）
- **LoA 1認定プログラムについて**
  - ✓ 米国国立衛生研究所(NIH)が提供する生物医学系文献検索等約90のサービスに機関のIdPを用いてアクセスする場合には、US FICAMのLoA 1要件を満たしていることの認定を受ける必要があります。学認では、この認定を米国OIX (Open Identity eXchange)の元で行っています。認定を受けるための費用は無料です。詳細については「OIX LoA 1 認定プログラム開始のお知らせ」を参照してください。
- **海外フェデレーションとの連携**
  - ✓ eduGainと呼ばれるインターフェデレーションの仕組みが、欧州TERENAにより提供されています。学認はeduGainに参加していますので、別途手続きを行うことでeduGainに参加しているSPを利用することが可能です。学認申請システムにおいて、IdPの情報をeduGainに提供する設定を行うことで、IdPのメタデータがeduGainに提供されます。
- **学認ロゴのデータおよびその利用について**
  - ✓ 学認ブランド使用ガイドラインのページをご確認ください。学術関係者は、事前にNIIに許諾を得る必要はありません。
    https://www.gakunin.jp/info/logo/
- **学認に関する情報源**
  - ✓ 大学における学認活用事例のケーススタディを公開しています。学認Webの「関連情報」のページを参照して下さい。
  - ✓ 学術認証環境の構築や利用に関する公開メーリングリストを開設しています。自由に情報交換・意見交換ができる場としてご活用ください。また、本メーリングリストの過去ログもWebにて公開しております。登録方法などについては、学認Webの「情報交換メーリングリスト」を参照して下さい。
    https://www.gakunin.jp/ml/

情報・システム研究機構 国立情報学研究所 National Institute of Informatics
学術基盤推進部 学術基盤課 総括・連携基盤チーム
TEL:03-4212-2218　FAX:03-4212-2230　e-mail: gakunin-office@nii.ac.jp
Ver. 1.0　2014.8.20