Shibboleth認証で変わる学術情報アクセス

野田, 英明
千葉大学附属図書館

吉田, 幸苗
東京大学情報基盤センター

井上, 敏宏
京都大学附属図書館

片岡, 真
九州大学情報システム部

他

出版情報：カレントアウェアネス. (307), pp.4-7, 2011-03-20. 国立国会図書館 関西館 図書館協力課
バージョン：
権利関係：

CA1736 Shibboleth認証で変わる学術情報アクセス

1. はじめに

現在、大学を始めとする教育・研究機関で提供される電子コンテンツの大半は、出版社などのベンダーと各機関との間でライセンス契約を結んでいるもので、その認証は、IPアドレスによって行われることが多い。しかし、米国情報標準化機構（NISO）のワーキンググループであるSERU（Shared Electronic Resource Understanding）[1]がガイドラインとして示したように、一般的に教育機関に所属する学生、教職員等のユーザは、キャンパス外からでもこうしたライセンスリソースへのアクセスが認められるようになってきている。これを技術的に実現するために、VPN[2]や、リバースプロキシ[3]などが用いられてきた。なかでもEZproxy[4]は、ユーザ側が特別なソフトウェアをインストールすることなく、ユーザID／パスワードによりアクセスできること、また電子コンテンツへのアクセスに特化しており、利用者コミュニティが充実していることなどから、図書館で広く使われてきた。

このような状況のなか、最近、IPアドレス認証に代わり、機関が個人認証を行う技術としてShibboleth（シボレス）[5]が注目を集めている。IPアドレスによる認証が、キャンパスという「物理的な場所」に基づいて認可を行うのに対し、Shibbolethによる認証は、アクセスする利用者の「属性」（所属部局、教員／学生など）に基づいた認可を実現している。また、キャンパスの内外を意識することなく各サービスへアクセスできること、シングルサインオン（SSO）、パーソナル機能との連携、ユーザ管理の利便性向上などのメリットもある。さらに、ライセンスリソースへのアクセス認証管理を一元化するため、英米を始めとする世界各国で、国レベルのShibbolethフェデレーションを運用する動きが広がりを見せており、日本でも国立情報学研究所（NII）を中心とした「学術認証フェデレーション」（学認：GakuNin）が立ち上がっている[6]。また、GakuNinの運用を行うため、NIIと大学関係者により、「学認タスクフォース」が立ち上がっており、筆者らは図書館関係者としてこのタスクフォースに参加している。本稿では、Shibbolethについて国内外の動向をまとめるとともに、GakuNinの取り組みを紹介する。

2. Internet2のShibbolethプロジェクトと各国のフェデレーション

Internet2[7]は、1996年に米国34大学の代表によって設立された、ネットワーク技術の発展を目的とした組織である。現在は、研究者へのツールやサポートの提供、サイバーインフラによる協力活動といった4つの目標を掲げて活動しており、Shibbolethは、その中で、SSOを前提としたアクセスコントロールを行うためのオープンソースのミドルウェアとして開発された。2003年にバージョン1.0、2008年にはバージョン2.0がリリースされ、現在に至っている。

Shibbolethでは（広義の）認証プロセスにおける、本人確認を行う「認証（authentication）」とサービス利用の権限を付与する「認可（authorization）」を分離し、ユーザ認証はサービス利用機関が設置するIdP（Identity Provider）側で、認可はサービス提供元（ベンダー）が設置するSP（Service Provider）側で行う[8]。SPは独自に認証を行わず、IdPから送信される「属性（attribute）」情報を信頼して利用認可を行う。利用機関とベンダーの相互信頼に依存する認証方式であることから、双方が国や地域を単位としたフェデレーションと呼ばれる連合組織を結成し、利用ポリシーの策定や連携に必要なメタデータの集中管理を行うのが一般的である。Internet2自身もプロジェクトの一環としてInCommonというフェデレーションを組織しており[9]、また英国情報システム合同委員会（Joint Information Systems Committee：JISC）も2008年にShibbolethを採用し、UK-Fedを組織している[10]。

フェデレーション間の連携を推進することを目的として結成されたREFEDs（Research and Education Federations）[11]の調査によると、2010年10月現在、学術情報へのアクセスを主目的とするフェデレーションは世界中に27団体存在している[12]。これらのフェデレーションへ参加している利用機関数を合計すると、およそ1,800にもなる[13]。

各フェデレーションにおけるサービスの力点は様々であるが、GakuNinでは後述のように各機関がサイトライセンスで購入している電子ジャーナル等を含む教育・研究用のサービスを充実させようとしている。

3. 日本におけるShibbolethの利用

日本においてShibboleth認証を学術情報へのアクセスに利用する動きは、2008年3月、NIIにおいて開催された懇談会に始まる。NIIの「全国大学共同電子認証基盤（UPKI）構築事業」の一環としてShibbolethを利用した認証連携基盤の設立が協議され、2008年度に27機関が参画して「UPKI認証連携基盤によるシングルサインオン実証実験」が実施された[14]。実証実験でフェデレーションとしての運用

開始に見通しがついたことから、2009年度に試行的なフェデレーションとして「学術認証フェデレーション（UPKI-Fed）」がスタートした。2010年度からは愛称を「学認（GakuNin）」に改め、本格運用に移行している。また情報部門や図書館のスタッフなど、フェデレーションを構成する機関の実務担当者としての立場からGakuNinの運用に参画する、学認タスクフォースが発足している。

国内における取り組みの中で、タスクフォースに関わり、先行して実際にサービス運用に入るなどした、いくつかの事例を紹介する。

千葉大学においては、Shibbolethを電子ジャーナルへのリモートアクセスを実現するツールと位置付け、附属図書館が主体となって利用環境を構築した。研究者の文献利用行動を「図書館目線」で体系化し、中核となる「電子ジャーナルを読む」ことを中心に、文献を「検索する」「読む」「管理する」という一連のプロセスをSSOで実現することを目標としてサービスを行っている。システム面では、情報部門である総合メディア基盤センターとの連携により、全学ネットワークやメールシステムを利用するための利用者情報を格納したLDAPサーバのデータを参照させて認証を行っている。また、IdPのハードウェア周りの管理にも総合メディア基盤センターの協力を得ている。図書館と情報部門の緊密な連携が重要であることは先行フェデレーションである英国などでも強調されているが、これは日本においても同様であろう。

九州大学では、情報部門である情報統括本部と附属図書館の連携によって、IdPの立ち上げを行い、図書館のマイアカウントサービス（きゅうとMyLibrary）及び電子コンテンツへの自宅・出張先からのアクセスサービス（どこでもきゅうと）でのShibboleth認証を実現した[15]。GakuNinへも正式参加しており、大学独自のサービスと商用サービスの双方で、ShibbolethによるSSOの実現を目指している。

京都大学においては従来から、図書館として提供している電子リソースへのアクセスの際、ユーザがWebサイトに直接アクセスするのではなく、間にプロキシサーバを立て、サーバ上で稼働しているSquidというフリーソフトウェアにより認証をかけてきた。利用統計の取得と、大量ダウンロード等を理由とするアクセス遮断措置を受けた場合の調査対応の迅速化のためである。また、学内の電子リソースアクセスを図書館にあるプロキシサーバに集約している。このため、ユーザ、IdP、SP間で通信が成り立つShibboleth認証を採用することができず、現時点において、Shibboleth認証に対応しているのは、プロキシを経由させていないCiNii、RefWorksと、図書館の提供ではないMicrosoft DreamSparkのみである。今後、この認証プロキシをShibboleth対応させる事が課題である。

4. 対応サービス拡大への取り組み

Shibboleth認証が有する利点の一つとして、サービス側に送信する利用者の属性情報をIdPの管理者がコントロールできる点が挙げられる。どのような属性情報をサービス側に送信するかは、サービス利用機関とベンダーの合意によってフェデレーションごとに定められており、例えばスイスのSWITCHaai[16]やデンマークのWAYF[17]では、利用者を特定できる情報を含んだ属性をSPに送信させることにより、eラーニングコンテンツを多機関で共同利用するサービスが活発に展開されている。一方、英国のUK-Fedやフランスの Éducation-Recherche[18]では、認証に必要な属性情報が比較的少ない、電子ジャーナルをはじめとする商用の学術コンテンツでの利用が先行している。

GakuNinでも学術コンテンツへのアクセスをサービスの柱として位置づけている。利用者がShibbolethの利便性を享受するには対応サービスの拡大が必須であるが、GakuNinを通じて利用できるサービスは、2011年1月現在で19に留まる。海外のフェデレーションでもコンテンツの増加を図ることがフェデレーションの利便性を向上させる鍵であることが指摘されており[19]、例えばInCommonでは、対応する学術コンテンツを拡大するため、InCommonに参画する個々の機関がInCommon Library Subgroups[20]を組織し、フェデレーションの利益を代表してベンダー各社と交渉を行っている。GakuNinでもInCommonに範をとり、学認タスクフォースに参加している図書館関係者によってGakuNinライブラリーチームを結成し、学術コンテンツのベンダー各社とShibboleth対応の交渉を行っている。

対応サービスを増加させることはGakuNinの利便性を向上させる上で重要であり、それにより参加する学術機関の増加も期待できる。しかし、ベンダーにとっては、提供するサービスをGakuNinに対応させるために、金銭的・人的なコストがかかるため、逆にGakuNin参加機関の増加等による、メリットが必要である。このような状況のなか、GakuNinの利用に関するベストプラクティスを見出し、参加する学術機関、対応するサービスの双方の増加を促していくことが、GakuNinライブラリーチームの使命の一つであると考えている。

このように、GakuNin ライブラリーチームは、現在 Shibboleth に対応する学術コンテンツの拡大に力点を置いているが、実際に Shibboleth 認証が適用できるサービスの可能性は、これに留まらない。金沢大学や佐賀大学などでは、大学ポータルや教務システムなどの学内サービス、ネットワーク利用者認証システム等での実装が実現されており[21][22]、四国地区の 8 大学で構成される e-Knowledge コンソーシアム四国[23]では、e ラーニング教材を参加大学が共同で利用する試みがなされている。Shibboleth が有する可能性を最大限に発揮し、利用者の利便性を向上させる取り組みとして、これらの方向からのアプローチにも期待したい。

5. 国際連携の取り組み

Shibboleth の SP は、1 台のサーバで複数のフェデレーションに対応できるが、そのためにはフェデレーションごとの設定を追加していく必要がある。このため、既に海外のフェデレーションに参加しているサービスであっても、ただちに GakuNin で利用できるとは限らない。そのため、複数のフェデレーションが SP を相互に提供し合う、Inter-Federation の取り組みも欧州では始まっている[24]が、個人情報保護をはじめ運用ポリシー面での調整に課題を抱えているなど、拡大にもう少し時間を要すると思われる。

こうした運用ポリシーやユーザインターフェースなど、各国のフェデレーションに共通する問題点については、各国フェデレーションのメンバーによって構成される REFEDs において調査・議論がなされている。例えば Shibboleth の利用に直結する問題として、ユーザインターフェースの問題が挙げられよう。Shibboleth 認証へのリンクは各コンテンツのトップページに用意されることが一般的であるが、現在のところ、その位置や表記方法はサービスごとに大きく異なっている。より利用しやすいインターフェースとなるように、一定のガイドラインを設けてベンダーに推奨していくことが検討されている。複数のフェデレーションが共通して利用するものであることから、どのような配置であれば利便性が高まるか、また、どのように各ベンダーへ働きかけていくか、REFEDs において議論されているところである。

6. おわりに

IP アドレス認証はユーザが特段の操作を要さず、簡便にリソースを利用できることが最大の特長である。しかしその認可判断の基準は「アクセス発生源が特定のネットワークである」という、いわば「物理的な場所に基づいた」判断に限られる。VPN やリバースプロキシを使った場合でも、ベンダー側で認可を判断する基準が IP アドレスになる点は同じである。これに対して Shibboleth は、アクセスする利用者の「属性に基づいた」認可判断が可能であり、誰が、どのコンテンツにアクセスが可能なのか、細かなアクセス管理を可能とするものである。また、ベンダーに利用者データを登録してユーザ ID ／パスワードを発行する形式の認証とは異なり、利用者データとその属性を機関側で管理できることから、個人情報の保護にも資する。

Shibboleth 認証は幅広い可能性と高い利便性を有する認証方式であるが、そのポテンシャルを最大限に享受するためには、対応サービスの増加が何よりも重要である。その一方で、多くのベンダーを GakuNin に呼び込むためには、利用機関の増加も必須である。より多くの利用者に Shibboleth の利便性を体感していただけるように、GakuNin の更なる充実にご協力を賜れれば幸いである。

（千葉大学附属図書館：野田英明（のだひであき））
（東京大学情報基盤センター：吉田幸苗（よしだゆきなえ））
（京都大学附属図書館：井上敏宏（いのうえとしひろ））
（九州大学情報システム部：片岡　真（かたおかしん））
（国立情報学研究所学術基盤推進部：阿蘇品治夫（あそしなはるお））

（1）NISO SERU Working Group. “SERU: A Shared Electronic Resource Understanding”. National Information Standards Organization. http://www.niso.org/publications/rp/RP-7-2008.pdf, (accessed 2011-01-21).
（2）PC にインストールしたソフトウェアを使って拠点の LAN に接続し、ネットワーク通信を仮想的にキャンパス内の環境にするもの。
（3）キャンパス内に設置したサーバが PC からのアクセス要求を中継することによって、キャンパス内からのアクセスであるかのように装うことができるようにするもの。
（4）“EZproxy”. OCLC. http://www.oclc.org/ezproxy/, (accessed 2011-01-21).
（5）“Shibboleth”. Internet2. http://shibboleth.internet2.edu/, (accessed 2011-01-21).
（6）学術認証フェデレーション . http://www.gakunin.jp/, (参照 2011-01-21).
（7）Internet2. http://www.internet2.edu/, (accessed 2011-01-21).
（8）「IdP」「SP」はサーバを意味する場合もあれば、それらのサーバを設置している主体を意味する場合もある。本稿では特に明記のない限りは、サーバを示すものとする。
（9）InCommon Identity and Access Management. http://www.incommonfederation.org/, (accessed 2011-01-21].
(10) UK Access Management Federation for Research and Education. http://www.ukfederation.org.uk/, (accessed 2011-01-21).
(11) “REFEDs: Research and Education Federations”. Trans-European Research and Education Networking Association. http://www.terena.org/activities/refeds/, (accessed 2011-01-21).
(12) “Federations”. REFEDs. 2010-10-22. https://refeds.terena.org/index.php/Federations, (accessed 2011-01-21).
(13) 原則として IdP 数なので一つの団体で複数の IdP を立ち上げているところはそれらもカウントしている。また、一部 SP 数やテスト段階も含む。
(14) “ 平成 20 年シングルサインオン実証実験報告書 ”. 国立情報

学研究所 . 2009-04-20.
https://www.gakunin.jp/docs/open/fed/6,（accessed 2010-02-10）.
⑮ 伊東栄典ほか . Shibboleth 認証基盤構築と学術認証フェデレーションへの参加：今後のｅリソースサービス基盤にむけて . 九州大学附属図書館研究開発室年報 . 2010, 2009/2010, p. 11-15.
⑯ “SWITCHaai”. SWITCH.
http://www.switch.ch/aai/index.html,（accessed 2011-01-21）.
⑰ WAYF.
https://www.wayf.dk/wayfweb/frontpage.html,（accessed 2011-01-21）.
⑱ “The federation Éducation-Recherche”. GIP RENATER.
https://federation.renater.fr/en/index,（accessed 2011-01-21）.
⑲ Marsh, Sara et al. “Identity and Access as a UK Priority”.
https://sites.google.com/site/jiscfam/documents/IdentityandAccessasaUKPriorityv5.pptx?attredirects=0,（accessed 2011-02-07）.
⑳ “InC-Library”. Internet2.
https://spaces.internet2.edu/display/inclibrary/InC-Library,（accessed 2011-01-21）.
㉑ 松平拓也ほか . 特集 , 多様な価値を創出する情報システム：大学における Shibboleth を利用した統合認証基盤の構築 . 情報処理学会論文誌 . 2011, 52(2), p. 703-713.
㉒ 大谷誠ほか . シングルサインオンに対応したネットワーク利用者認証システムの開発 . 情報処理学会論文誌 . 2010, 51(3), p. 1031-1039.
㉓ e-Knowledge コンソーシアム四国 .
http://www-ek4.cc.kagawa-u.ac.jp/,（参照 2011-01-21）.
㉔ eduGAIN. http://www.edugain.org/,（accessed 2011-01-21）.

CA1737

米国の図書館就職事情

はじめに

米国図書館界では 1990 年代の終わりころから、2010 年以降に起こるベビー・ブーマーの大量退職で、図書館界が人材不足に陥るのではないかと危惧されてきた（CA1583 参照）。米国のベビー・ブーマーとは 1946 年から 1964 年に生まれた約 7,800 万人の人たちを指し[1]、彼らの多くは今後 20 年内に退職すると言われていたためである[2]。ところが、ベビー・ブーマーの最年長が 65 歳を迎えた 2011 年現在のところ、米国で図書館員が不足するとの「噂」は神話にとどまっているように思われる。

ベビー・ブーマー大量退職による図書館員不足の懸念

米国図書館協会（ALA）の会員を対象とした図書館員人口調査には 2010 年 5 月までに約 5 万 4 千人が回答し、その内 46.2%がベビー・ブーマー世代であった[3]。業界人口の約半数が今後 20 年以内の内に次々と 65 歳を迎える図書館界で、退職者の穴埋めをどうするか懸念するのは自然な事である。

ベビー・ブーマー大量退職による図書館員不足の懸念を示した例を時系列に幾つか紹介する。

1995 年には、学術図書館員の人口統計学的研究で著名なワイルダー（Stanley J. Wilder）が、1995 年時点での北米研究図書館協会（ARL）加盟館の図書館員がいつ退職時期を迎えるかを調査し、退職者の割合が年々増えていくことを予想した[4]（表参照）。

表　1995 年時点で在職している学術図書館員の予想される退職時期

予想される退職時期	割　合
1995 年から 2000 年	16%
2000 年から 2005 年	16%
2005 年から 2010 年	24%
2010 年から 2020 年	27%

出典：(4) を基に筆者が作成

時間は少し進んで 2002 年には American Libraries 誌でも、1990 年の人口調査で職業を「ライブラリアン」と申告した者が 65 歳に達する時期をまとめ、2010 年–2014 年がピークで申告者の 20％強が退職すると予想した[5]。2004 年になると ALA は 2000 年度の人口調査の結果を受け、図のとおり、2010 年から 2019 年の間に 65 歳を迎える図書館員が増える事で大量退職の波が来る事を提示し、再度図書館員不足の懸念を

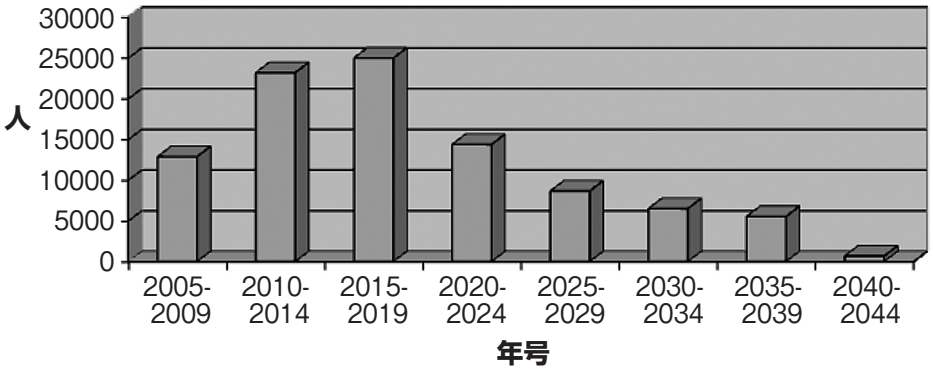

図　2000年度の人口調査結果に基づくライブラリアンの65歳人口の推移予想

出典：(6) を基に筆者が作成