リモートアクセスサービス実現までの経緯と今後の課題

田邊 稔（たなべ みのる）
（メディアセンター本部課長代理）
平吹佳世子（ひらぶき かよこ）
（同　課長代理）

1　はじめに

慶應義塾大学メディアセンター（以下 MC）では，2006 年 11 月 1 日より試行版として，オフキャンパスから電子ジャーナル/データベース（以下 EJ/DB）を利用するためのリモートアクセスサービス（以下 KRAS）を開始した。開始後，約 8 ヶ月が経過したが，利用件数は着実に伸びている（図 1）。

しかし，当サービス実現までの道のりは決して平坦なものではなく，いくつもの「壁」があり，これらを突破するのに多くの人手と約 3 年もの歳月を費やした。本稿では，この 3 年間の経緯を振り返るとともに，運用に至るまでの設計思想や実装方法を概説し，コンテンツ提供元とのライセンス許諾の現状についてまとめ，次世代図書館サービスを支える共通認証基盤としての課題について言及したい。

なお，残念ながら，実装技術の詳細については，セキュリティ上記述することができないことをあらかじめ断っておく。

2　実現までの経緯

MC では，教員や大学院生を始めとして，誰もがこのサービスを切望していることはわかっていた。ネットワーク環境がこれだけ充実している昨今，レポート作成や論文執筆時に自宅や外出先でも情報収集したいと思うのは利用者行動として当然の欲求である。ただ，その需要がどれだけ一般的か，一部のヘビーユーザによるものではないか，など疑問だった。つまり，一般的なユーザにとって「あれば便利（nice-to-have）」なサービスか，「なくてはならない（must-have）」かの判別が付かなかった。また，慶應義塾の統合認証基盤（以下 keio.jp）が立ち上がることがわかっていたため，あえて MC 独自の認証システムを構築することを避けた。

事の起こりは，今から約 3 年前に遡る。法科大学院の創設を控えた 2004 年 2 月に担当教員から「自宅から法学系のデータベースにアクセスできないか？」との要望があがった。それまでも，医学部の一部の教員などからは要望が出ていたが，この時ほど強く切望されたのは初めてだった。

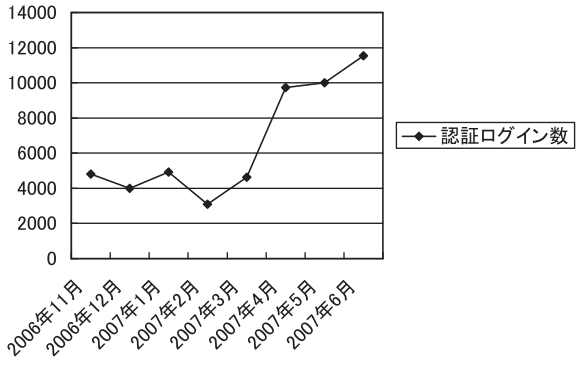

図 1.　認証ログイン数

結局，このときは MC としては協力には至らなかったが，そこから約 1 年半経過後の 2005 年 9〜11 月の 2 ヶ月間に SSL-VPN[注1] 使った EJ/DB リモートアクセス実証実験を行った。といっても，MC が勝手に実施した訳ではなく，事前に ITC 本部に相談した上で，実験レベルでの keio.jp 連携としては最も簡易でセキュアな方式を採用した。

実験では，keio.jp 認証に Radius[注2] 方式，SSL-VPN 通信に Aventail 社の EX-1500 というアプライアンス（特定用途向けの専用装置）をそれぞれ採用した。EX-1500 で利用できる SSL-VPN には 2 種類の方式があった。1 つは「WebProxy」で，EX-1500 側の URL の後ろにコンテンツの URL を埋め込んでアクセスする方式で，もう 1 つは「OnDemand」で，端末側のブラウザにエージェント（ネットワーク機器の管理/監視を行なうために，管理対象機器にインストールするプログラム）を設定することにより，あたかもキャンパス内のネットワークからアクセスしてい

るかのように見せる方式である。どちらも一長一短あって，データベースによっては，うまくハンドリングできずに，接続に至らないケースもあった。他に，本番運用までにクリアしなくてはならない大きな課題が二つあった。「利用者の属性情報によるアクセス制御（以降３章）」と「コンテンツ提供元への利用許諾確認（以降５章）」である。

それから半年ほど何も動きがなかったが，2006年３月に急展開が起き，ITC 本部より「リモートアクセスサービスの実装を急ぎたい」との連絡が入り，いよいよ本腰を入れることとなった。MC としては，これまでの経緯を説明するとともに，SSL-VPN ではなく，“EZproxy”という EJ/DB に特化したプロキシサービス（大学構内からインターネットへのアクセスを代行するサーバーで，欧米の大学では既にデファクトとなっている）を利用したい旨を ITC 本部に申し入れた。

３　設計思想と実装における工夫

先に述べた実験結果より，本番運用に向けて，技術面・コスト面・契約面などの様々な課題をクリアしなくてはならないことがわかった。技術的な協力・支援を依頼する ITC 本部にも EZproxy の特性や挙動を十分理解してもらった上で，開発を進める必然性があった。そこで，まず実装方法を含め全体の運用（想定される導線）イメージを数パターン書いてみた。パターン１は最も理想とする形で「既存の DB/EJ リストより特定のコンテンツを選択したときに必要に応じて keio.jp 認証画面が表示されるパターン」，パターン２は「keio.jp ログイン後のアプリ選択メニューから入るパターン」，パターン３は「リモートアクセス専用のエントリ画面を用意して，利用可能なコンテンツのみ表示し，コンテンツ選択後必要に応じて keio.jp 認証画面を表示するパターン」である。結局，現実的な実装方法として，パターン３が採用された。ここに「全塾利用のコンテンツで提供元に許諾の取れたもの」から順次掲載することとした。

技術的には，EZproxy の挙動の把握と keio.jp とのセキュアな連携がキーポイントだった。そこで，ITC 本部でも EZproxy をテスト導入し，セキュリティ面を中心に動作検証を行った。その結果，「少し工夫すれば問題なく使えそうだ」との回答を得た。まずは第一関門をクリアした。次に，利用者の属性情報のハンドリングについて検証した。フルタイム雇用契約（以下 FTE）では，教職員であれば「常勤」であること，学生であれば「正規生」であることがそれぞれ前提となる。そのためには，keio.jp から引き渡される属性情報を見て判別できることが必要となる。幸い，EZproxy ではこれが可能であった。

約１ヶ月弱で keio.jp と EZproxy を連携するアプリケーションのプロトタイプを作成し，MC 内で評価したところ，自宅から認証を経て提供元 URL への接続に関しては概ね問題ないが，KRAS トップページのデザインや掲載する文言に関しては，数多くの意見が出され改訂を重ねた。まずは文言優先ということで，デザインに関しては先送りした。もう１つ大きい指摘は，「図書館の専用メニューからではなく，keio.jp ログイン後のアプリケーションメニューに“EJ/DB リモートアクセス”がないのは不自然」というものであった。これについては，先に書いたパターン２の通り想定はしていたが，後送りにする予定だった。しかし，この基本導線は譲れないとのことで，ITC 本部と協議の上，11 月のスタートまでに実装することとなった。これが間に合ったことはまさに奇跡だった。これにより，keio.jp 認証とのフロントエンド連携とバックエンド連携という２種類の“ハイブリッド型連携”が実現され，サービスの幅が格段に広がった。

コンテンツと EZproxy との連携で特に工夫した点は，慶應義塾の電子ジャーナル検索システム（EJ-OPAC）での実装方法にある。EJ-OPAC には，利用されるキャンパスによってコンテンツを変化させるしくみがあり，これを利用し「リモートアクセス」という仮想的なキャンパスを作り出し，EZproxy 経由でアクセスされた場合にリモートアクセス用のコンテンツのみを表示することに成功した。

運用開始にあたっては，利用者からの問い合わせ体制を確立する必要があった。そこで，まず「問い合わせ対応フロー」を作成し，連絡体制と責任分担の明確化を行った。次に「問い合わせ専用フォーム」を準備した。問い合わせフォームを置く場所については，本部システム担当内でも異論反論があったが，当面はどのような種類の問い合わせがどのくらいの頻度で来るのかなどを把握したいという私個人の強い意向で，ログイン前の KRAS トップページに

フォームのリンクとメールアドレスを置いた。

本部システム担当として一番恐れたのが，大量の問い合わせが来た場合の稼働負荷であった。本部システム担当は，いわゆる「サポートセンター」ではないので，その体制がないまま受けるのは本意でないからだ。しかし，いざ蓋を開けてみると，2006年11月1日から開始して現在（2007年6月29日時点）までの問い合わせ総数は「17件」で，稼働に影響するレベルには至っていない。問い合わせ内容の内訳は，内5件が慶應ID（keio.jpサービス用のID）取得に関する案件（ITC本部マター）で，残りの12件がコンテンツの接続エラーや新規掲載希望であった（MC本部マター）。

また，運用後まもなく，コンテンツの新規掲載ルールについてMC内で以下の通り取り決めを行った。

（1）各地区から掲載希望がある場合，「本部電子資源担当（2007年4月より新設）」に申請を行う。
（2）本部システム担当で技術的な動作検証を行った上で，掲載可否を判定する。
（3）掲載可と判定されたものについて，契約主管地区にて提供元の契約内容を確認し，必要に応じて，提供元と覚書などを交わす。
（4）掲載時期の調整を行って，KRASへアップする。

4　EZproxyとの出会いとコミュニティの力

EZproxyとの出会いは，約4年前に遡る。当時の上司から「北米に電子ジャーナルのアクセスに特化したクールなProxyがあるので，レビューしてほしい」との要請があったため，テスト用のLinuxサーバに入れて遊んでみたのがきっかけである。しかし，最初はとっつきにくく，どこまで手を入れられるのかまったくわからなかった。標準テンプレートにコンテンツをいくつか追加していくレベルであれば問題なかったが，ログイン画面を含めてデザインの変更ができるのか，他の認証システムとどのように連携させればよいのかなど具体的なことは一切不明だった。当時，国内には前例がほとんどなく，他大学でも動通レベルの検証にとどまっていた。しかし，何といっても，ライセンスは1サーバあたり$495（約5万円）と安価で，海外の大手データベースとの親和性が高いことが採用の決め手となった。唯一，セキュリティ面だけが気になっていた。

本格的に導入が決定してから，いろいろ疑問点が湧いてきて，EZproxy開発メーカーの問い合わせ窓口（info@UsefulUtilities.com）に英語で問い合わせを行っていた。その都度，担当のChris Zager氏（以下Chris）から的確かつ丁寧な回答をいただいて技術的な壁を突破してきた。そのうち，EZproxyユーザコミュニティのメーリングリスト（以下ML）「ezproxy@ls.suny.edu」が公開されていたことに気づき，そこに参加することにより，欧米を中心とした世界各国のEZproxyユーザの動向が手に取るようにわかるようになった。そこでは，自由闊達でカジュアルな意見交換が繰り広げられていて，Chrisに問い合わせを行うまでもなく，そこである程度解決してしまう問題も多い。もちろん，そのMLの中でもChrisはカリスマというか，もはや「神」的な存在で，数限りない難題に立ち向かい，解決に導いている。Chrisとのメールのやりとりは実に淡白で問題解決のための伝達以外，ほとんど記述しないタイプで，文面からは職人気質を想像させるが，そんなChrisにもプライベートな一面を覗かせるエピソードがあるので紹介しよう。

今年の5月24日から6月6日までUseful Utilities社が休暇を取る際に，Chrisから次のメールがML宛てに流れた。

“Useful Utilities will be closed from May 24 to June 6. Details appear at :（省略）

I had alternate plans for coverage during this time, but they did not come together. Although it might be more appropriate to cancel this break, life is short and kids grow quickly. ”

これに対し，以下のような反応が次々に入ってきた。いかに，多くのEZproxyユーザが日頃からChrisに恩恵を受けているかを表している。

“I hope you enjoy your well-deserved break!!”, “I concur ― enjoy your family. Have a great vacation. ”, “Please enjoy your vacation/break. Yes, life is very short esp. when we are getting matured. Many thing in our life have their own ‘requirements’, sometimes we are not able to fulfill all the ‘request’. When we have time, just do it. I love someone who take care their family. ”, “Enjoy the vacation Chris ; we can get by for a week or two

without you, as you have also provided us with a great support group. As long as nothing breaks Seriously, life IS short and they grow very quickly！”

5　コンテンツ提供元への許諾確認について

KRAS 実施にあたっては，コンテンツ提供元の許諾を受ける必要がある。海外版元が提供するコンテンツはほとんどがリモートアクセスを許可しており，契約書の記述内容で判断可能な場合もあったが，今回，EZproxy を使用してリモートアクセスを提供するということで，認証システム名も明確にして直接版元に許諾確認を取った。その結果，海外の版元からは全て許可するとの連絡を得た。しかし，国内コンテンツの場合，契約書のほかに認証システム名を記述した覚書を取り交わしたケースや，リモートアクセスするには，価格の上乗せが必要というケースがあった。いつでもどこでも利用できるという電子資源の利点を最大限に発揮するために，利用する人を正しく認証するシステムを使ってより多く使ってもらおうという海外版元と，リモートアクセスを許可した場合に無限に利用数が増えるのではないかという危惧のある国内版元の認識の違いがあるようだ。リモートアクセスによる利用の増加は予測できるが，必ずしも著しい増加につながるとは言い難い。もしかすると，“不正利用の温床”となることを危惧しているのかもしれない。しかし，不正利用を本気で危惧するのであれば，認証付きのリモートアクセスよりも，本人認証不要のオンキャンパス利用にも目を向けるべきだろう。その意味では，すべての EJ/DB 利用を認証付きとするのも一法かと思われる。

海外版元の契約書で主に確認した記述項目は，次の 3 項目である。

（1）Authorized users（機関における利用者の定義）
（2）Secure Network（ネットワークの安全性）
（3）Remote Access（リモートアクセス）

(3)の記述がある契約書は少なかったが，(2)の記述でリモートアクセスを含んだ解釈をするという回答が多かった。

一般的な記述例を以下に示す。

（1）Authorized users

Current members of the staff of the Licensee（whether on a permanent, temporary, contract or visiting basis）and individuals who are currently studying at the Licensee's institution, who are permitted to access the Secure Network from within the premises of the Licensee and from such other places where Authorized Users work of study, including without limitation halls of residence and lodgings and homes of Authorized Users, and who have been issued by the Licensee with a password or other authentication.

（2）Secure Network

A network（whether a standalone network or a virtual network within the Internet）which is only accessible to Authorized Users approved by the Licensee whose identity is authenticated at the time of log-in and periodically thereafter consistent with current, reasonable practice.

（3）Remote Access

Authorized Users may obtain remote access to the licensed materials through secure access procedures established by the Licensee.

また，契約書のガイドラインを定めようとしている NISO の SERU（Shared Electronic Resource Understanding）ワーキンググループでは，ドラフトの段階ではあるが電子資源における契約書の標準記述を発表している。この中の“The Subscribing Institution and Its Authorized users”の項目では，出版社は，高等教育機関が利用を許可すると判断した全ての利用者にコンテンツを提供しなければならず，この中にはリモートアクセスでの利用も含まれると書かれている。

今回は全塾で利用可能なコンテンツを対象に許諾確認を行ったが，地区毎の契約，複数地区での契約についても要望があるため，システム的な問題がクリアされた時点で，許諾確認を行う必要がある。理想としては，許諾確認を行わなくても，また価格の上乗せをすることなく全ての出版社がリモートアクセスを許可してくれることである。許可していない出版社と契約交渉する際には価格を上乗せすることなく契約条件に含めるよう努力したいと思っている。

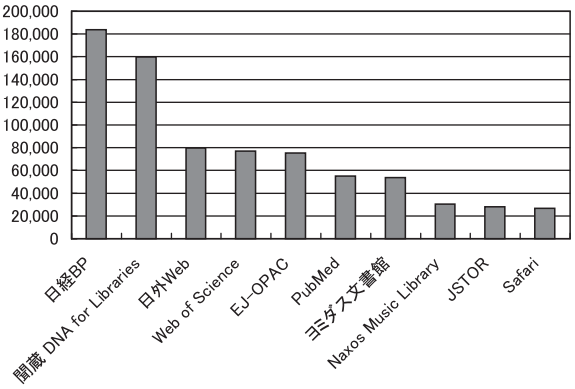

図2. 2007年6月コンテンツ別アクセス数（トップ10）

6 今後の課題

コンテンツによって利用件数に差異はあるものの(図2), KRASの利用は日々加速しており, 中にはアクセスが急増し，契約の見直しを余儀なくされるものも一部出てきている。また，学外からアクセスした時に，あたかもキャンパス内にいるかのようなアクセス環境を実現するには，いくつかの課題をクリアする必要がある。

課題の一つに，実際にいくつか問い合わせがあったケースとして「グレー身分」対応が挙げられる。現在契約中の提供元の大半がIP認証を採用しているため，オンキャンパス利用は比較的緩やかだが，オフキャンパス利用は厳しい制約があり，契約(FTE)上，教職員については「専任かつ常勤」であることが前提となるため，名誉教授や訪問研究員などは判断が難しい。大学としては，給与や社会保険などの雇用契約の関係から「常勤」にする訳にはいかないと思われるため,「非専任」や「非常勤」でも一部のケースで利用できるように，提供元との契約条件を見直す必要がある。これは，慶應義塾に限った懸案ではなく，他大学も同様であろう。その意味では，コンソーシアムなどへの期待が大きい。

その他の課題として,「キャンパス個別契約コンテンツへの対応」,「OPACやデータベース検索システムとの連携」,「リンクリゾルバ経由の認証」などがある。これらについては，具体的な実装方法の検討に着手したところである。また，将来的には「国際的な大学間・機関間連携認証システム(Shibboleth等)への対応」など大きなチャレンジがある。

7 おわりに

兎にも角にも，アプリケーションを“よりセキュアに”keio.jpと連携させるには，ITC本部との密なコミュニケーションが必要となる。なぜなら，アプリケーションの性質によって最適な連携方法も異なるからである。MCでは, 文献複写申込などのオンラインリクエストサービスを始め，keio.jpと連携させたいアプリケーションが次々に控えている。

折しも，この7月に慶應義塾図書館がアジアの図書館で初めてGoogleブック検索のLibrary Projectに参加することとなった。このこと自体，図書館界にとっては非常にインパクトのある動きだが，MCではこれに甘んじることなく，今後もITCや他部署と協力しながら，Googleに負けない“クールでセキュアなシステム”を次々とマッシュアップし，利用者へ迅速に提供していきたい。KRASが,「利用者に開かれた次世代図書館サービス」の先導者となることを切に願っている。

注

1) SSL-VPN（Secure Sockets Layer Virtual Private Network)とは，Webアクセスで広く使われている暗号通信プロトコルであるSSLを利用するリモート・アクセス技術。SSL-VPNを使うときには，アクセス先のネットワークとインターネットとの境界にSSL-VPNゲートウエイを置く。リモート・アクセスするパソコンは，Webブラウザを使ってSSL-VPNゲートウエイにアクセスする。パソコンにSSL-VPN用のソフトウエアをインストールしておく必要はない。パソコンとSSL-VPNゲートウエイの間は，SSLによって暗号化される。SSL-VPNゲートウエイは，リモートから送られてきた暗号データを復号し，学内ネットに中継する。

2) Radius（Remote Authentication Dial In User Service）とは，元来はダイアルアップによるリモート接続でのユーザ認証プロトコル。近年は，ダイアルアップだけでなく，ブロードバンド接続や, VPN，VLAN, 無線LANなどへの接続ユーザ認証にも利用されている。