KOSMOS―keio.jp 認証連携と認証サービスの今後

田邊　稔（たなべ　みのる）
（メディアセンター本部課長代理）

1　keio.jp 認証サービスと My Library

これまで，図書館が提供する keio.jp 認証サービスとしては，『図書利用状況照会』と『EJ/DB リモートアクセス』の２つがあった。今回の『KOSMOS My Library』は，第３のサービスというよりも，“図書利用状況照会の機能拡張版サービス”という位置づけに近い。図書利用状況照会では，自分の貸出・予約・未収金の状況を照会するだけのサービスだったが，My Library では，利用者自らがリアルタイムで予約・更新（貸出期限延長）できる機能が加わった。KOSMOS を開始した４月以降，My Library 経由での予約・更新の利用数が急速に伸びたことから考えても，利用者が長年待ち望んでいた機能であったことが分かる（図 1）。さらに，認証さえ受けていれば，タグやレビューなども登録できる。もう一つ大きな違いは，従来の２つのサービスと異なり，慶應 ID を持っていなくとも，図書館に利用者登録を行い，ID/Password を取得すれば，サービスを利用できるという点である。

2　PDS の機能とセキュリティの確保

Ex Libris（以下。E 社）の Primo パッケージに標準装備されている『PDS（Patron Directory Service）』には，Aleph パッケージの利用者データ（Patron）と直接連携できる独自の認証機能の他に，「Remote-LOGIN」や「Remote-SSO」と呼ばれる機能があり，外部の認証サービスと連携することができる。但し，セキュリティの観点から，KOSMOS（PDS）と keio.jp が直接連携する形ではなく，先行事例として実績のある EJ/DB リモートアクセス（以下。KRAS）のサーバが仲介する方式を採用した。おかげで，インフォメーションテクノロジーセンター（以下。ITC）・メディアセンターとも効率よく開発することができた。なお，PDS⇔KRAS⇔keio.jp 間はすべて SSL 通信とし，経路上セキュアな通信を確保することとした。

3　PDS と keio.jp との連携ポイント

まず，KOSMOS の認証サービスへ入る基本導線を以下の４つと想定した。

（1）KOSMOS トップの「ログイン」ボタンから
（2）KEIO-OPAC 書誌一覧の「リクエスト」リンクから
（3）図書館 HP やお気に入り（ダイレクトリンク）から
（4）keio.jp のアプリケーションメニューから

今回の実装に際し，最大のポイントだったのは，「慶應 ID 保持者と慶應 ID 非保持者へのシームレスな対応」である。つまり，慶應 ID を持っている人にも，持っていない人にも，同じ認証画面，同じ画面遷移でサービスを提供することを我々の最重要課題と捉えた。そのため，E 社への基本要件として，以下の２つを提示した。

（1）認証ログイン画面は慶應側が提供するものとし，慶應 ID 保持者用と非保持者用を共通のものとする。

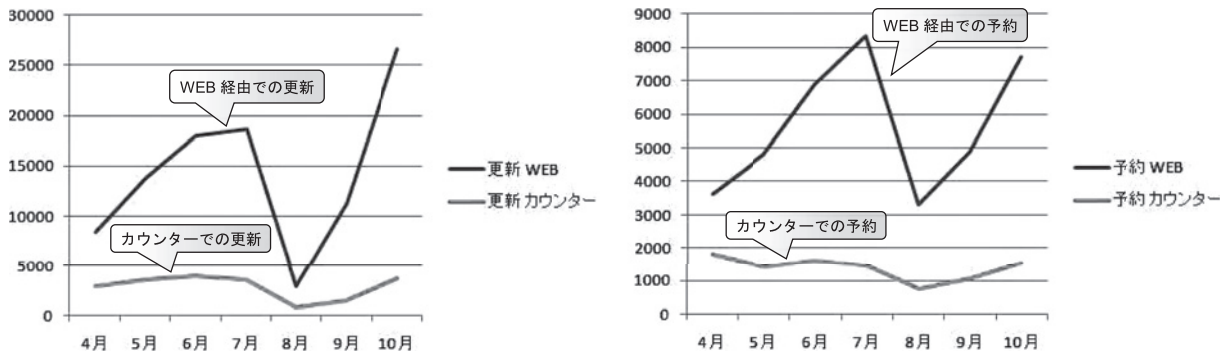

図 1.　更新/予約［カウンター vs Web（My Library）経由］統計の推移

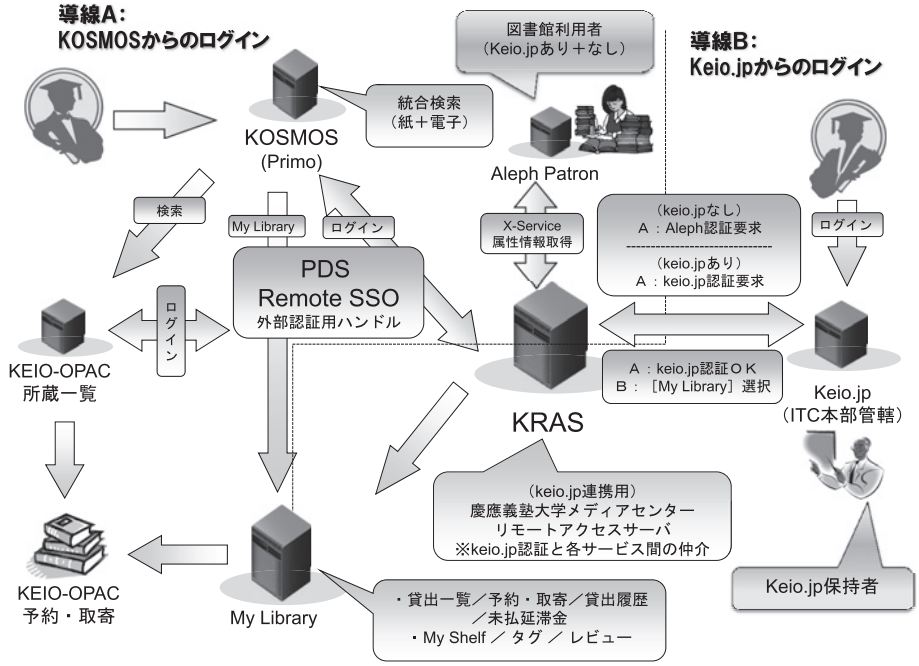

図 2.　My Libary の認証フロー

(2) 図書館システム側では慶應 ID を保管しないこと。

慶應 ID は ITC が管理する ID であるため，入力された ID/Password を一時的にせよ，図書館システム上を通過することも，保管することも許されるものではない。そのため，ITC が用意した keio.jp ログイン画面を使うことを必須要件とした。但し，ログイン画面は共通でも，慶應 ID でログインされた場合と非慶應 ID（図書館利用者 ID）でログインされた場合では，裏側の仕組みは大きく異なる。この実装にはかなり手を焼いたが，具体的な実装方法としては，大きく下記の通りとなる。(図 2)

(1) 入力された ID 体系で判別する。
(2) 慶應ID体系の場合は，keio.jpに認証を要求する。
(3) それ以外（図書館利用者 ID）の場合は，X-Service の認証 API を使って，Aleph 利用者情報に直接認証を要求する。
(4) 認証エラー処理は，(2)と(3)それぞれで行う。
(5) 認証通過後の動きは，(2)と(3)で共通とする。

4　KOSMOS ログイン端末の誕生

今回の keio.jp 連携でもう一つ大きな進展があったのは，従来の OPAC 端末が「蔵書検索に特化した専用端末」という位置づけだったものが，館や設置ゾーンによっては，ログイン認証して予約・更新ができる端末「KOSMOS ログイン端末」を用意できたことだ。そもそも，OPAC 端末は強固にフィルターされており，蔵書検索以外何もできない（させない）“極端に自由度の低い端末”である。そこに，認証サービスを載せることは，当然ながら“御法度”だと思い込んでいた。しかし，ITC に相談したところ，ITC 端末でも ITC アカウントで認証利用させていることもあり，きちんと利用指導を行い，システム面・運用面でリスクをカバーできるのであれば，問題なかろうとの見解だった。

OPAC 端末で認証サービスを提供するにあたり，最大の問題となったのが，「サービス利用後，いかにログアウトしてもらうか」と「ログアウトされなかった場合のリスクをどこまで最小化できるか」ということだった。そこで工夫したこととして，運用面ではログアウトを促すために，端末そのものに大きく「利用後は必ずログアウトしてください。ログアウトしない場合，誤って次の利用者があなたの ID を使ってしまう恐れがあります。」といった注意喚起のシールを張ることにした。システム面では，3 分間未操作状態の場合に端末を自動ログアウトする仕掛けを作った。もちろん，未ログイン状態で 3 分間の間に次の利用者が飛び込んだ場合のリスクはあるが，それは一種の“事故”と割り切ることとし，運用を開始するに至った。

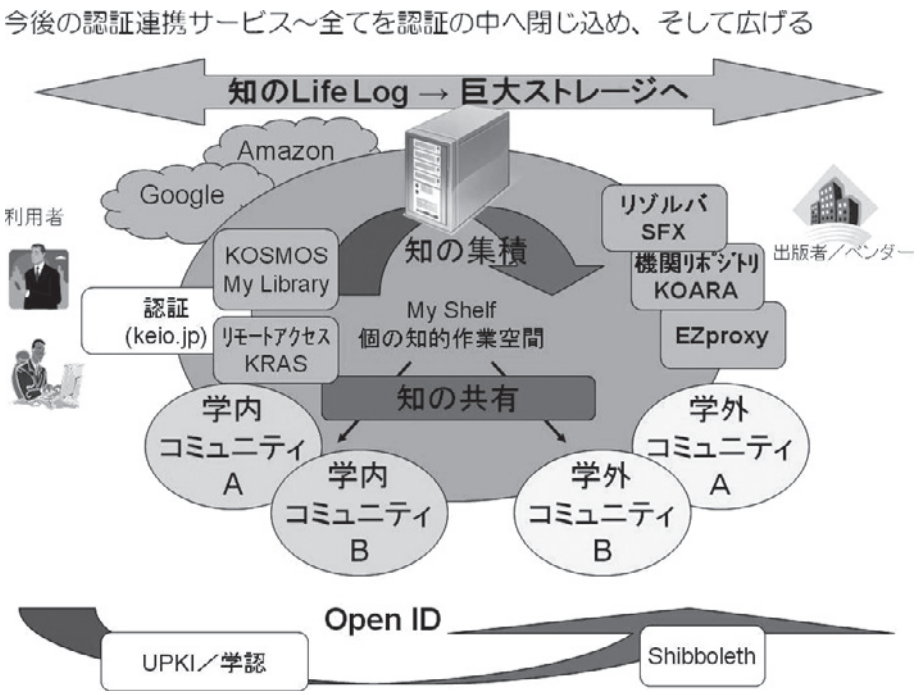

図 3.　今後の認証サービス

5　認証サービスにおける今後の課題

最後に，認証サービスとしての今後の課題を 5 点ほど掲載する。

1）中継サーバの信頼性向上

KOSMOS My Library と keio.jp と の 連 携 に KRAS を中継させることで，KRAS そのものの役割が重要となり，サーバの強化が急務となっている。具体的には，もう 1 台ミラーセットを用意し，最低限コールドスタンバイ構成を取り，万一の場合，最短のダウンタイムで切り替えられるよう，構築を急ぐ予定である。

2）keio.jp への図書館サービスの見せ方

現状，keio.jp ログイン後のアプリケーション一覧には「KOSMOS My Library」という 1 つのアプリとして実装しているが，今後，キラー的なアプリは「粒」で見せるなど工夫が必要だと思われる。

3）『学認（愛称：GakuNin）』[注1] との連携

Primo の PDS や KRAS の EZproxy [注2] は，Shibboleth [注3] 認証にも対応しているため，数年後には NII-UPKI が提供している GakuNin と連携したコミュニティサービスを実装することになろう。(図 3)

4）モバイル版 OPAC からの予約・更新

現在，携帯電話向けのモバイル版 KOSMOS(参照系のみ)は外部 ASP にて提供しているが，今後，認証付きサービスを載せるためには，ASP 版ではなく，慶應内のサーバにモジュールを置くモデルか，API 化して提供する必要がある。

5）電子学術書利用実験プロジェクトとの連携

現在進行中の「電子学術書利用実験プロジェクト」について，2010 年 12 月より利用実験を開始する予定である。利用範囲を慶應所属者に限定したり，コンテンツ利用ログを取得するなど，本人認証が必須となるため，KOSMOS⇔keio.jp⇔電子書籍アプリの連携を実装する必要がある。

注

1）「学術認証フェデレーション（愛称：GakuNin）」とは，学術 e-リソースを利用する大学，学術 e-リソースを提供する機関・出版社等から構成された連合体のこと．各機関はフェデレーションが定めた規程（ポリシー）を信頼しあうことで，相互に認証連携を実現することが可能となる．

2）「サイト契約の電子ジャーナルを遠隔地から利用させる」という目的に特化して開発されたソフト．現在は OCLC が販売，維持管理している．

3）米国 EDUCAUSE/Internet2 にて 2000 年に発足したプロジェクトで，SAML，eduPerson 等の標準仕様を利用した認証・認可のための標準仕様策定とオープンソース提供を行っている．