

第4回統合認証シンポジウム報告

只木進一*

1 はじめに

総合情報基盤センターは、その名の通り、大学の教育、研究、診療、組織業務を支える「情報基盤」を整備し、運用すること、及びそのための調査・研究・企画を第一の任務とする組織です。「情報基盤」は、様々な情報システムを運用するために必要となるネットワークなどの基盤のハードウェア、認証情報などのソフトウェア、それらを運用するための組織体制などを指しています。電気やガスのような生活基盤とその整備運用と同じものと考えて頂いて間違いありません。

情報化は、紙媒体であった書類などを電子化することではありません。データの共有・連携によって、従来の情報から新しい情報を生み出すことが情報化の意義であり、目標です。データ連携のもっとも基本的な部分が利用者情報の連携です。

利用者情報の一元管理と連携は、利用者にとって一つの認証情報で様々なシステムへログインすることを可能とします。また、管理者には、一度の利用者情報取得で、多数のシステムの利用者管理を可能すると同時に、セキュリティ強化を可能とします。さらに、人の情報に紐づいたデータベース構築が可能となります。

このような考えのもと、本センターでは、1990年代末から、附属図書館との協力を手始めに、「統合認証システム」の構築を進めてきました。利用者の情報を教務や人事といった情報の発生源から直接取得して管理するとともに、必要とする情報システム間で共有することで、情報の重複を防ぎ、迅速で精度の高い利用者情報提供を可能とするシステムのことで、昨年3月のシステム更新では、統合認証システムは、新しい機能として、シングルサインオン (SSO) 機能を提供するようになりました。

統合認証あるいは認証基盤の整備は、技術的問題と

ともに組織的問題も並行して解決していかなければなりません。大学の場合には、学生と教職員という、管理部署が異なる情報を統合し、教学用システムから事務用システムまで利用者情報を提供しなければなりません。このような、大学全体にわたる情報の管理・運用をする部署はどこなのか、というところから解決していく必要があります。そのため、システムの必要性は認識できても、実装や運用の困難さのために、整備できていない大学が多く残っています。認証基盤の整備は、着実に進んでいますが、2009年度の調査では、3割以上の大学で、認証基盤の整備が出来ていません [1]。

本センターでは、統合認証に関わる技術的問題、組織的問題、活用事例などを共有するために、2007年度より、「統合認証シンポジウム」を開催してきました。2010年には、シングルサインオンに焦点を絞り、4回目を開催しました。大学だけでなく情報関連企業からも多数の方の参加を頂きました。ありがとうございました。



図 1: シンポジウムの様子

*総合情報基盤センター

表 1: 第 4 回統合認証シンポジウムプログラム

あいさつ 中島 晃 (佐賀大学 CIO)
はじめに 只木 進一 (佐賀大学)
学術認証フェデレーションによる地の循環基盤の創成 曽根原 登 (国立情報学研究所)
Shibboleth を含んだ統合認証システムの導入 梶田 秀夫 (京都工芸繊維大学)
佐賀大学における Shibboleth への対応とシステムの開発 渡辺 健次 (佐賀大学)
Shibboleth による金沢大学統合認証基盤の構築と今後の展開 松平 拓也 (金沢大学)
徳島大学における SSO の実現と課題 松浦 健二 (徳島大学)



図 2: カッチーくんもお出迎え

2 概要

2010年12月22日に、教養教育運営機構大講義室にて、「第4回統合認証シンポジウム」を開催しました。今回の主なテーマは、Shibbolethによるシングルサインオンとその利活用としました。

最初に、只木から、認証基盤整備におけるシングルサインオンの位置づけについて、概要を整理しました。利用者情報を統合し、認証基盤を整備する技術的方法については着実に成熟しています。次の問題としては、利活用の範囲・方法をどのように広げていくかが課題となっています。

近年、組織の情報システムはクライアント・サーバ型から、急速に Web 型に変化してきています。Web

型情報システムでは、OS などシステム基盤へのログイン権限と独立して Web 型情報システムへの利用権限を設定できること、クライアント側に標準的な Web ブラウザ以外のソフトウェアを要求しないことが理由です。このような Web 型情報システムの間で認証済という情報を共有することで、情報システム間をシームレス(境目なく)に移動することを可能にするのがシングルサインオンという仕組みです。

また、学術情報の流通形式も急速に電子化が進んでいます。世界的に流通する学術雑誌の電子化が急速に進み、研究者は図書館で学術雑誌を調べるのではなく、研究室で Web ブラウザを使って学術雑誌を検索し、読むようになりました。もちろん、辞書、事典、各種のデータなども Web ブラウザ経由で提供されつつあります。教育においても、Web を用いたオンデマンド授業、講義資料配布が広く用いられています。

サービス提供を行う情報システムへ渡す利用者情報を上手に制御することができれば、シングルサインオンは、組織の枠をこえて、組織間での認証連携を可能とします。国立情報学研究所は2009年から、Shibboleth というシングルサインオン方式を使って大学間連携を推進しています。大学の認証基盤を、相互に緩く連携させることにより、電子ジャーナルや教材などの学術情報など認証が必要なサービスを大学間で共有しようとする試みです。欧米では、既に定着・拡大しつつあ

る取組です。このプロジェクトの一層の拡大へ向けて、国立情報学研究所の曾根原先生から、「学術認証フェデレーション・学認」(図3[2])の拡大による新しい知の循環基盤の創成についてお話いただきました。

Shibboleth 認証で利用可能なサービスは、着実に増え続けています。「学認」に対応したサービスとしては、電子ジャーナル、ソフトウェアダウンロード、ファイル宅配サービスなどが提供されています。「学認」に参加している大学・学術研究機関も2011年9月現在で、26機関となっています。参加機関の増大は、そこに保管されている利用者ID数の増大を意味し、サービス提供側から見て、魅力的な対象となるでしょう。逆に、サービスが増えれば、「学認」参加のメリットが大きくなります。この認証連携が、更に拡大し、有料のコンテンツサービスへと拡大する可能性もあります。

更に、曾根原先生は、巨大な認証連携基盤が可能とする新しい型の学術研究の可能性についても紹介されました。認証基盤の整備は、匿名化されてはいても、個々の利用者の軌跡の追跡を可能とします。ネットワーク上に分散した、人からの情報収集、人への情報提供によって、新しい型の科学、あるいは新しい型のサービスが可能となるでしょう。

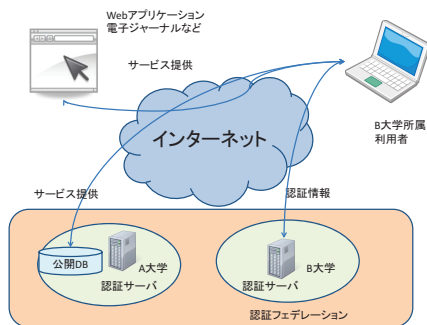


図3: 学術認証フェデレーション

シングルサインオンの導入事例として、京都工芸繊維大学の事例を榎田先生に紹介いただきました[3]。京都工芸繊維大学では、佐賀大学と同様に2010年3月にシステム更新を行い、シングルサインオン機構を導入しています。

佐賀大学のシングルサインオンサービスとの違いの一つに、電子メールのシングルサインオン化があります。電子メールは、インターネットサービスのもっとも古くからあるサービスの一つであり、利用者が最も

多いサービスです。古くからあるサービスであるため、メールサーバの認証機構と強く結びついています。京都工芸繊維大学では、シングルサインオンに対応したWeb型のメールサービスのソリューションを導入しています。本学でも、独自方式をテストしているところです。

本学も2010年度末から、国立情報学研究所が進める「学認」に参加いたしました。いくつかの電子ジャーナルに、シングルサインオンによってアクセスが可能です。詳しくは、附属図書館に問い合わせてください。本学のシングルサインオンサービスへの取組を渡辺先生から紹介していただきました。

本学でのシングルサインオンの特色の一つとして、Web型の情報システムへのログインだけでなく、本学が10年あまりサービスしてきた利用者用認証ネットワーク opengate にも利用をしている点があります。利用者は、持ち込みPC等をネットワーク接続する際に、Webでシングルサインオン認証を受けます。この認証を受けることで、教務システム等の情報システム群へシームレスに入ることが可能となっています[4]。また、学外からの利用者には、一時利用IDを提供する方式と、「学認」を通じてそれぞれの大学の認証を使う方式を提供しています。

シングルサインオン対応サービスの拡大支援の方法として、簡単にシングルサインオン対応ページを作成するためのサービスも行っています。Shibboleth対応のWebサーバを一旦構築すると、認証の仕組みを個別に作成する必要はなくなります。しかし、そのサーバの構築は、あまり簡単ではありません。そこで、シングルサインオン認証が必要な部局等に、対応したフォルダをレンタルするサービスを行っています。

金沢大学は、認証基盤整備において先進的取組をしている大学です。金沢大学のシングルサインオンへの取組を松平先生に紹介していただきました[5]。「認証」は本人であることの確認であって、その人が対象となる情報システムを使う権限があるかを確認する「認可」とは異なるものです。認可情報を効率的に流通させるために、金沢大学では利用者情報に「ロール」という情報を付加し、サービス側での基本的な認可に活用しています。

また、シングルサインオンが学内の多数の情報サービスで活用されるに伴って、その冗長性の確保も必要となっています。金沢大学では、認証サーバ及びサー

ビスプロバイダの多重化が実施されています。大変、参考になりました。

最後に、徳島大学の松浦先生に、徳島大学でのシングルサインオンの環境と活用について紹介いただきました [6]。徳島大学では、認証基盤整備が非常に戦略的に進められています。法人化以降、センターだけでなく法人との議論の積み重ねがありました。大変参考になりました。



図 4: 懇親会でも活発な情報交換が続きました。

3 今後の展望

本学において、「学認」に対応した Shibboleth を活用したシングルサインオンが稼働を始めて 1 年半以上が経過しました。教務システムや図書館ポータル、教職員のグループウェアなど、基幹的サービスがシングルサインオン配下となり、個別の認証画面を表示さず移動が可能となっています。2011 年度に稼働したポートフォリオシステムも、シングルサインオン配下で稼働しています。利用者の方々は気が付いているでしょうか。気が付かないうちに利便性が向上しているようにするのも、情報基盤整備の一部です。

本学が契約している電子ジャーナルも Shibboleth 対応が進んでいます。これまでは、学内からのアクセスしか可能ではありませんでしたが、現在では学外から認証を通じてアクセスすることが可能です。ライセンスの拡大とともにサービスが増えていくことが期待できます。

情報システムを保有せずに、アウトソーシングしたり、クラウドサービスを受ける場合、利用者とその認証情報をどのように扱うかがセキュリティ確保の観点

から問題となります。Shibboleth を使ったシングルサインオンを用いると、認証そのものの情報を情報サービス側に渡さずに、そのサービスを受けることが可能となります。アウトソーシングの可能性が、大きく広がるでしょう。本学でも、検討を進めたいと考えています。

「学認」には、現在、26 組織が参加し、約十萬の ID が管理されています。参加組織が増え、保有する ID が増えることで、巨大な利用者グループが発生することを意味します。それによる、サービスの充実が期待されています。また、多様なサービスが参加することで、利用者側が管理しなければならない、ID とパスワードの組が減ることにもなります。本センターでは、大谷准教授を国立情報学研究所に派遣するなど、「学認」の運用や企画に積極的に関わり、推進に寄与しています。

統合認証シンポジウムは 4 回目になりました。認証は、情報基盤整備の核となる部分であり、まだまだ話題は尽きません。本年度も 12 月 22 日に第 5 回統合認証シンポジウムを予定しています。サービス提供者だけでなく、利用者側からも多数の参加をお待ちしています。

参考文献

- [1] 文部科学省研究振興局情報課「平成 21 年度学術情報基盤実態調査報告書」(2010/6).
- [2] <https://upki-portal.nii.ac.jp/docs/fed/>
- [3] 京都工芸繊維大学情報科学センター
<http://www.cis.kit.ac.jp/>
- [4] 大谷誠, 江藤博文, 渡辺健次, 只木進一, 渡辺義明, 「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 51 (2010) 1031.
- [5] 金沢大学アキャンサスポータル
<https://acanthus.cis.kanazawa-u.ac.jp/Portal/>
- [6] 徳島大学情報化推進センター
<http://www.ait.tokushima-u.ac.jp/>