

電子ジャーナル認証代行(SSO)実証実験

CiNii認証代行プロジェクト(SSO実証実験)への参加の呼びかけ

佐藤周行, 西村健
東京大学情報基盤センターPKIプロジェクト
2008年9月1日

NII(国立情報学研究所)がサービスする文献サービスCiNiiの利用に当たっては一部認証を必要とするものがあります。従来はCiNiiが独自に利用者管理を行なってきました。このプロジェクトは、SSO(Single Sign On)の枠組を提供し、東大内部での認証によってCiNiiの認証を代行する実証実験です。実験に当たり、参加者を募集します。

参加者はCiNiiを含む各種サービスの提供が受けられます。また、将来的には現在総合図書館が行なっている電子ジャーナルとの連携も視野に入れます。

目次

- [はじめに](#)
- [実験の概要 -- 利用可能サービス](#)
 - [実験にあたっての留意事項](#)
- [実験の概要 -- ID編](#)
 - 一般の利用者
 - UT-CA実証実験参加者
- [参加申し込み](#)
- [将来の展望](#)
 - 期間
 - 技術的なこと

はじめに

ネットワークを利用してサービス提供を受けるのが一般的になってきました。サービスには、文献検索などの研究に必須なものや、サイボウズなどのグループウェア、予算管理、成績管理など、教育研究事務に係わるものまでが広く含まれます。

それとともに問題になってきたのが認証に関するコストです。「認証」は一般的な言葉になってきたのでしょうか。従来は計算機システムへの「ログイン」とよばれてきたプロセスがこれに一番近いものになります。サービスを受けるに当たって、ネットワークの向こうからやってきたデータ(を持っているプロセス)の持ち主が、サービスを受ける資格があるかどうかをチェックする手続きです。ネットワークを利用したサービスが一般的になるということは、個人情報と言うに及ばず、予算状況などいわゆる「あぶない」データを普通に扱うということですから、認証はある意味で必須です。誰にでもデータを見せてよい牧歌的な次代は過ぎ去りました。

認証を考えるにあたり、コストが問題になりました。サービスが巨大化するにあたり、ユーザ情報の管理は一般に大変になります。特に全国、全学に対してサービスを行なうときに、ユーザの登録、消滅、変更に関する管理コストは莫大なものになります。東大においても、教育用計算機システムのID体系の維持に関するコストは大変なものがあります。年に一回のパスワード強制変更は、IDの質(なりすまし、幽霊ユーザの整理)を維持するのに必須なものとはいえ、大変だと感じる人も多いと思います。

管理する側のコストだけを言い募るわけには行きません。個人が情報サービスを利用するに当たりサーバに提供する、またはせざるを得ない情報が正しく利用されているかどうかについては、疑心暗鬼が生じています。自分のIDに関する情報が、知らない間に他で使いまわされているというのは、気持ち悪いものです。知らないところから自分のメールアドレスに直接ダイレクトメールがくるのは、気持ち悪さを超えて明らかな研究の邪魔になっています。

そこでわれわれは、認証を信頼できる輪(学内なら学内、部局なら部局)に限り、そこではある程度のコストをかけてきちんと管理する枠組を作ることになりました。信頼できる輪の中では認証情報は使い回しができます。情報サーバごとに認証のプロセスを抱え込む枠組と比較して、この枠組は情報サーバの管理コストを格段に節約できます。それだけでなく、一度どこかで認証すればサービス間で認証情報を使いまわしてくれるのですから利用者の側からしても、これにはメリットがあります。認証情報をその輪を超えて利用する場合は、開示する情報を管理できる枠組を作りました。この枠組は一般にSSO(Single Sign On)と呼ばれています。

NII(国立情報学研究所)がサービスする文献サービスCiNiiの利用に当たっては一部認証を必要とするものがあります。従来はCiNiiが独自に利用者管理を行なってきました。IPアドレスによる認証も行なってきました。PKIプロジェクトでは、NIIと協力し、[SSO\(Single Sign On\)の枠組を提供し、東大内部での認証によってCiNiiの認証を代行する実証実験を行なうことになりました](#)。ここではIPアドレスの認証は必要ありません。つまり、学外からCiNiiのサービスが利用可能になります。東大では、すでに教育用計算機システムのID体系とSSLVPNを利用した学外からの文献サービスを行なってきました。今回の実験はCiNiiに対する同種の試みです。

実験に当たり、参加者を募集します。参加者はCiNiiを含む各種サービスの提供が受けられます。

実験の概要 -- 利用可能サービス

CiNiiは以下でアクセスできます。 [CiNii \(実験のためのサイト\)](#)

ログインを求めるところで「Shibboleth Login」を選択してください。なお、利用にあたっては通常のCiNiiの利用と同じ [規約](#) が適用されます。御一読ください。

さらに、[実験にあたっての留意事項](#) を確認してください。

実験の概要 -- ID編

文献サービスですから、ICカードを利用するなど強固過ぎる認証は必要ありません。 [IDとパスワードによる認証を行ないます](#)。

一般の利用者

われわれは認証情報として、以下を利用します。

1. 共通ID(総長発行の職員証にふられているID)
2. 所属部局

共通IDは、現在でも予算管理システムなどに利用されている全学共通のIDシステムです。現状では、ICカード化された職員証・学生証を持つ東大の構成員にふられています。

この実験では、共通IDを持つ東大の教職員・学生を対象とします。認証データベースには、上の2つの情報を格納します。それ以外の情報の記載を任意で求められるかもしれませんが、拒否しても実験参加を拒むわけではありません。

なお、東大内部での認証では共通IDを用いますが、CiNii利用に関しては、共通IDの情報は使いません。学外に共通ID情報はわかりません。また、個人名などの情報もわたらないようにします。

UT-CA実証実験参加者

情報基盤センターでは2006年度から全学PKIの立ち上げのための実証実験を行なっています（[UT-CA実証実験](#)）。この実験に参加している利用者に対してはパスワード登録サービスを提供します(10月を予定)。一般の利用者は本人確認とパスワード登録が必要ですが、UT-CA実証実験参加者については、本人確認はICカードを利用、パスワード登録はオンラインでできます。

参加申し込み

まずは、情報基盤センターPKIプロジェクトにコンタクトを取ってください。schuko@cc.u-tokyo.ac.jp(○を適宜変更)

実験参加に当たっては共通IDのデータベースへの登録が必要となりますので、その同意、また本人と共通IDの「ひも付け」を行ない、その後パスワードを配布します。UT-CA実証実験参加者については、共通IDの登録同意だけで利用可能になります。

将来の展望

期間

この実験は、今年(2008年度)中に終了することになっています。これ以上のことは公式には何も言えません。ただ、終了するといっても好評ならば拡充にむけた動きが出てくると思います。

技術的なこと

この実験の技術的な核は以下の二つです。

1. ShibbolethによるSSO
2. 共通IDを格納したLDAPサーバ

SSOについては、今回はいきなり全国レベルのサービスを提供しますが、学内限定のサービスについてもShibbolethの傘下に入ることで、認証代行が可能になります。学内にサービスを行なってきた、認証に関係する仕事(ユーザ管理その他)が負担になってきているところはぜひご相談ください。

LDAPサーバについては、現在学内で有名なものに教育用計算機システムのID体系のものがああります。われわれは、共通IDのLDAPサーバを構築するテストを行ない、教育用計算機システムのID体系を利用したサービスの一部(一番有用なものの一つはSSLVPNを利用した図書館電子ジャーナルの学外からの利用)と連携する交渉を機を見てははじめようと思います。