学術情報システムの整備と統合認証システム

只木進一*

1　はじめに

佐賀大学における情報基礎科目の教育は、すっかり定着した感があります。専門科目においても情報処理技術を利用する機会が増えているようです。学術情報処理センターの演習室においても、学生の皆さんがレポートを作成したり、インターネットから情報収集を行なうために自習する姿が非常に多くなりました。特に学期末には、ほぼ全ての端末が自習に利用されることがあります。コンピュータ演習環境の絶対的な不足が明瞭です。

一方で、学生の皆さんが自身のパーソナルコンピュータ (PC) を持つようになってきました。自宅にデスクトップ型 PC を持って、インターネットに接続するばかりでなく、ノート型 PC を持って大学で利用する姿を見る機会が増えました。平成 15 年度からは、一部の学科で個人のノート型 PC 保有を前提に演習を計画しているようです。

情報処理技術の一般化や情報機器の普及は、様々な情報のオンライン化と一体で進んで来ました。オンライン化された情報には、誰でもが匿名で利用できるものばかりでなく、利用者を制限したり、利用を記録するものも含まれています。利用者の制限や利用記録のためには、パスワードを使った本人同定の認証機能を持つことになります。

佐賀大学においても、学術情報処理センターの研究教育用システムの他、電子図書館システムなどで認証が必要なシステムがあります。まだ、学生用の認証が必要な Web 型情報システムはあまり多くありませんが、成績、各種証明書、就職活動などに関連したシステムが近い将来に構築されるでしょう。このように、学内においてさへ、認証を必要とする情報システムが増えていくでしょう。

認証が必要な情報システムの数が単純に増えると、一人の利用者が多数の利用者名とパスワードの組を保持しなければならなくなります。このような状況では、利用者が異なる利用資格に同じ簡単なパスワードを設定したり、あるいは利用者名とパスワードを他人の目に容易に触れる場所に置いたりする可能性が高くなります。

管理者側から見ると、各情報システムごとに利用者情報を収集するコストがかかります。更に、利用者がどの利用者名とパスワードの組を使うべきなのかの問い合わせへの対応というコストも増大します。このように認証を各システムごとに行っていたのでは、認証システム導入が情報サービス構築のブレーキになってしまいかねません。

利用者が多数の利用者名とパスワードの組を使うのを、少なくとも学内では一つに統一しようというのが、統合認証システムです。大学の全構成員の情報を持ったデータベースシステムを中心に、コンピュータやネットワーク利用と Web 情報システムへのアクセスの認証機能を提供するシステムです [1]。

2　学術情報システムの整備

情報処理技術が一般化するのに伴って、学術情報システムの整備が大学の基盤整備として重要になってきました。学術情報処理センターでは、教育用コンピュータシステムと基幹ネットワークの他に学術情報システムの整備に努めてきました。

- 学術情報処理センターが提供する基幹コンピュータシステムは、2002 年春に更新されました。その中心として、Windows 環境と UNIX 環境をデュアルブートで利用できる演習用端末 215 台を整備しました (図 1)。この端末はハードディスクを持たず、サーバから起動するものです。ハードディスクの破損や利用者による変更が不能であるとともに、Windows Update やウィルスパターンファイルの更新などもサーバ側の変更だけで行うことが可能となり、保守コストを大幅に削減することが可能となりました。このシステムは全国の情報処理センターから注目を浴び、多くの見学者が来ています [2]。

  この演習システム導入と併行して、後述する統合認証システムを構築し、Windows と UNIX 系 OS

*学術情報処理センター

図 1: 学術情報処理センター演習室

の間で利用者名とパスワードの統合を行いました。Web を介して、パスワードを同期的に変更したり、自分のファイル利用容量を調べるシステムのサービスも構築しました。

- 学術情報処理センターへの改組にあたって、電子図書館システムの構築が新たな業務として追加され、2001 年春から電子図書館システム「とんぼの眼」を運用開始しました。附属図書館との協力の下、蔵書検索だけでなく、オンラインシラバス、教官総覧、研究業績リストなどの情報システムが提供されています。電子図書館機能は、全国の国立大学で数校しかないもので、注目されています。

  電子図書館機能の一環として、学内に所蔵されている学術情報の電子化の支援も行っています。現在は、農学部が所蔵する植物資源遺伝情報のデータベース化作業中で、2003 年春の公開に向けて作業しています。

- 全ての教育場面で文書作成、情報交換、情報収集、データ処理のためにコンピュータとネットワークが必要になっています。それに対応するために、利用者が持ち歩くノート型 PC に対応したネットワーク構築を 2001 年末から行っています。

  インターネット利用時には、学術情報処理センターで利用している利用者名とパスワードによる認証が必要です。現在のところ、全ての教室を含む公開空間で有線及び無線を使ったインターネット利用が可能となっています [3, 4]。

- 全ての利用者が学内に公開された Web ページを持つことができるようになっています。この機能を使って、講義資料の配布やレポート提出などが行われています。また、2003 年からは、教職員に限って、申請により学外公開 Web ページを持つことが可能となりました。

3 統合認証とは

学術情報処理センターでは、研究教育用のコンピュータシステムのサービスをしています。佐賀大学の全学生と全教職員が、センターに設置されている演習用端末で Windows2000 と Linux を利用し、またセンター内の UNIX システムを利用することができます (図 1)。この時のログインに使う利用者名とパスワードは共通になっています。このように、統合認証の一つの機能は、異なるオペレーティングシステム (OS) で共通の利用者名とパスワードの組が使えるようにするもので

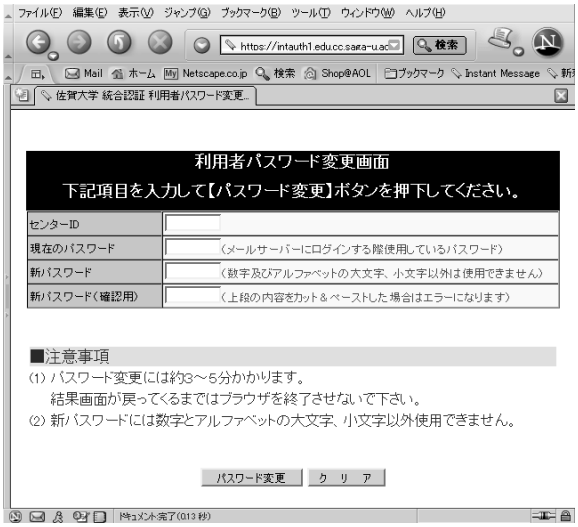

図 2: パスワード変更画面:Windows200 と UNIX のパスワードを同時に変更することができる。

す (図 2)。

佐賀大学の教員は、電子図書館「とんぼの眼」の中のオンラインシラバス、教員基礎情報データベース、研究業績データベースに、自らの情報を登録することができます。この際に、本人確認のために認証が必要です。ここでも、センターのコンピュータシステムを利用する際と同じ利用者名とパスワードを使うことができます (図 3)。このような Web を介した情報システムの利用の際の認証は、そのコンピュータへログインを許可するものとは異なり、単に本人を同定し情報へのアクセスを許可するものです。

佐賀大学の各教室では、有線または無線を使って、利用者は自分のノート型 PC をネットワークに接続することができます。これらの利用者が持ち込むノート型 PC と附属図書館や就職相談室などの公開端末がインターネットへ接続する際に、利用者認証が行われ、利用が記録されます。その際の認証にも、センターの利用者名とパスワードが使われています [3, 4]。

このように、統合認証システムを導入することによって、利用者にとっては、一つの利用者名とパスワードの組を覚えるだけで、学内の様々な情報システムを利用することが可能となります。情報システム管理者は、利用者が大学の構成員となった最初に一回だけ、利用者登録を行えばよく、複数のシステムに対応して利用者情報を集める必要がなくなります。

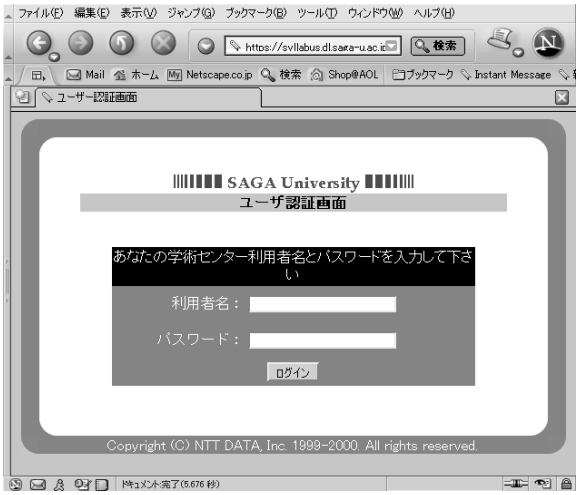

図 3: オンラインシラバスの認証画面

4 情報システムの利用権の変質

ここで、コンピュータの利用の形態が急速に変質していることに注目しましょう。佐賀大学がインターネットに接続したのは、国立大学の中では非常に早く、1990 年でした。そこ頃、コンピュータやネットワークを利用する人は非常に少なく、それらの人々は数値計算やシミュレーションなど特殊な目的のためにコンピュータを使っていました。つまり、その頃のコンピュータの利用者資格は、特殊な研究や教育を目的としていました。

現在はどうでしょう。コンピュータとネットワークの利用は、文書作成、資料収集、資料整理、様々な連絡など、日常的な研究教育活動に不可欠なものとなりました。コンピュータとネットワークを利用することは、大学で研究をしたり、教育を受けたりするための、基本的な権利・資格となっています。

従って、大学の全ての教職員と学生が大学の基本的な情報システムを利用できるように、情報システムが対応できるとともに、全員が確実に利用者として登録される事務的体制が不可欠になります。

5 統合認証の基本要素

統合認証システムは、情報処理センターなどの基幹コンピュータシステムの認証だけでなく、大学内に設置される多様な情報システムの認証を単一利用者名で

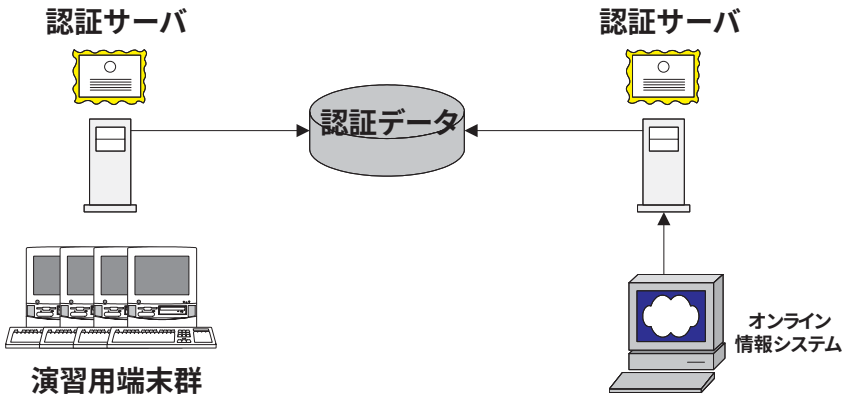

図 4: 統合認証システムの概要

行うためのシステムです。従って、全利用者の情報情報を保持したデータベースから、認証サーバへの認証情報の提供を柔軟に行える仕組みが必要です。更に、全利用者情報を円滑に登録・変更するための技術的仕組みと事務的仕組みが必要です。

統合認証システムは、基本情報を保持する認証データベース、コンピュータシステムへのログイン時に利用する認証サーバ、Web 情報システムからの認証に利用される汎用認証サーバ、及びこれらを支えるネットワークと管理端末から構成されます。

学内の様々な情報システムに認証情報を提供するために、基本となる利用者データベースには、利用者の氏名、よみ、ローマ字表記の他、所属や身分などを保持する必要があります。これは、特定の所属や身分の利用者の認証情報を提供することを可能とするためです。このデータベースを中心に、コンピュータシステムの利用者情報などの必要な個別システムごとの情報を保持することも可能です。

基本となるデータベースシステムは、全利用者の基本的な情報を含んでいます。従って、このシステムの安全性を保持するために、認証情報のための閉じたネットワークを構築することが望ましいでしょう。

認証データベースから、認証サーバへデータが提供されます。コンピュータへのログイン時の認証は、オペレーティングシステムごとに異なる方式が使われています。特に、Windows 系 OS と UNIX 系 OS の認証は、非常に異なり、その共通化は情報処理センターを長い間悩ませて来ました [2]。認証データベースから、これらの二つの認証データを生成する仕組みを組み込みます。

Web を介して情報にアクセスする型の情報システムが認証を必要とする場合を考えます。この場合の認証は、ログイン認証とは異なり、その情報システムが稼働しているコンピュータの利用者情報とは異なる利用者管理が必要です。ネットワークを介したアクセスなどを利用することで認証を行うことが可能です。これに対応して、汎用的なネットワーク認証を可能とする認証サーバも設置します。

もっとも構築の難しい要素は、大学の全利用者を確実に登録する仕組みです。従来は、コンピュータシステムの利用者登録は、システム管理者 (root 権限者) の重要な仕事でした。しかし、利用者が大学の全構成員というように数千人、数万人となるとシステム管理者だけではその作業を賄いきれません。入学、退学、転入、転出といった人の動きを確実に追うことは、コンピュータシステム管理者の守備範囲を大きく越えています。学生の移動は学生部、教職員の動きは事務局が一番把握しています。こうした事務組織から人の移動の基本情報を認証データベースへ登録してもらえるのが望ましいと考えています。

6 統合認証システムの今後

2003 年 10 月に、佐賀大学は佐賀医科大学と統合されて新しい大学となります。その際に両方の情報システムの統合が必要となり、統合へ向けた作業が始まっています。その際に問題となるのが、両大学の基幹コンピュータシステムが既に動いている状態であり、重複した利用者名があることです。

住所録や名簿のような木構造のある情報を保持するLDAP (Lightweight Directory Access Protocol) が新しい認証機構として注目されています。例えば、ネットワークサーバ類として多用されるオペレーティングシステムであるSolarisやWindowsドメイン内の利用者管理を行うActive DirectoryがLDAPへ認証機能を移行させつつあります[5]。学術情報処理センターでは、認証機構をLDAPへ移行することで、佐賀医科大学との統合時に認証機構を更新しようと考えています。LDAPを認証の中心に据えることで、WindowsとUNIX系OSとの認証統合も一層円滑に可能となりそうです。

LDAPは多様な情報を保持することが可能です。例えば、情報処理センター以外の部局が設置するコンピュータシステムに対して認証を提供したり、分散したメールサーバへの配信を行う機能を提供できるでしょう。更に、適切にアクセス制御を行う必要はありますが、学内に対して電話番号簿や教員のメールアドレス帖として提供することも可能です。

参考文献

[1] 江藤博文、渡辺健次、只木進一、渡辺義明「全学的な共通情報アクセスのための統合認証システム」情報処理学会研究会報告 2002-DSM-27 (2002) pp.31.

[2] 江藤博文、只木進一「UNIX環境とWindows環境を提供可能な教育用ディスクレス端末システム」情報処理学会研究会報告 2001-DSM-24 (2001) pp.25.

[3] 渡辺義明、渡辺健次、江藤博文、只木進一「利用と管理が容易で適用範囲の広い利用者認証ゲートウェイシステムの開発」、情報処理学会論文誌 Vol.**42**, No.12 (2001) pp.2802.

[4] 江藤博文、只木進一、渡辺健次、渡辺義明「新しい教育用情報基盤の実現に向けて〜認証システムをベースとしたキャンパス規模のオープンネットワーク〜」、学術情報処理研究 No. 6 (2002) pp.13.

[5] Tom Bialaski and Michael Haines, *Solaris and Ldap Naming Services: Deploying Ldap in the Enterprise* (Prentice Hall, 2001).