全学的な共通情報アクセス環境のための統合認証システム

江藤博文、渡辺健次†、只木進一、渡辺義明†
佐賀大学学術情報処理センター
†佐賀大学理工学部

概要

情報処理技術が一般化・多様化し、コンピュータとネットワークが情報流通の基盤となりつつある。それにともない、様々な情報がオンラインで提供されるようになった。また、大学の全構成員が大学の研究教育用コンピュータシステムの利用資格を有するようになった。さらに、演習室利用だけでなくネットワーク利用や情報システム利用にあたって認証が必要となっている。従来のように、それぞれの情報システムが個別に認証機能を有したのでは、利用者が複数の利用資格を管理する一方で、管理者が個々に認証情報を収集登録しなくてはならない。認証情報を一括管理し、異なる情報システムへ認証情報を提供するための統合認証システムを提案し、その運用状況について報告する。併せて、情報処理センターの役割変化について議論する。

Integrated Authentication for Campus-wide Information Systems

Hirofumi Eto, Kenzi Watanabe‡, Shin-ichi Tadaki and Yoshiaki Watanabe‡
Computer and Network Center, Saga University
‡Department of Information Science, Saga University

Abstract

Utilization of information and communication technologies becomes common with diversity. Computers and networks become an infrastructure for information and communication. We are required to construct various types of online information systems. And currently all members of an university have their own user IDs for the university computer system. The university computer system and other information systems require user authentication. If those information systems require their own authentication mechanisms as before, users have to manage various user IDs and administrators are required to collect and maintain user information for each information system separately. We propose an integrated authentication mechanism to maintain user information and provide authentication information to systems in campus. We also report the current status of our integrated authentication system. We discuss the new role of information center in university.

1　はじめに

情報処理技術の利用は、大学における全ての研究教育分野において必要なものの一つとなりつつある。情報リテラシ教育は、大学における基礎教育に位置づけられ、それに対応した教育用情報システムが整備されている。こうしたシステムは、ネットワークに接続され、利用者認証が必要となっている。また、これらのシステムでは、複数の OS が併存したり、学部学科の独自システムが併設される場合がある。

一方、コンピュータとネットワークは、情報通信の基盤の一つとなりつつある。大学内においても、様々な情報がオンラインで提供されている。オンラインで提供される情報の中には、利用者認証を必要とするものも含まれている。

このように、現在の大学には、認証を要する複数の情報システムが共存している。これらは、OS の差に基づいて認証メカニズムが異なる場合や、設置主体が異なるために元となる利用者情報が異なる場合など、異なる認証体系となっている場合が多い。そのため、情報サービスの増加は、利用者に多数の利用者名を持たせることになり、利用者の負担が増えてしまう。管理者側でも、情報サービスごとに利用者情報を収集・管理する必要があり、管理コスト面からサービス増大を躊躇させる。

本稿では、認証情報を統合し、様々な情報システムへ提供する枠組について提案をする。また、佐賀大学において実装した統合認証システムの概要を述べ、運用状況について報告する。統合認証情報を情報処理センターが提供することによって、情報処理機器が一般化した状況下での情報処理センターの新しい役割について議論する。

2　統合認証システム

2.1　統合認証はなぜ必要か

情報処理技術が一般化したことにより、大学内において様々な情報システムが利用されている。これらでは利用者を制限したり特定したりするために、必要に応じて利用者認証が行われている。これらの認証機構を大学内で統合する必要性について、はじめに論じる。

現在、情報リテラシ教育及び情報処理技術を前提とした専門教育が広く行われている。それに対応するための、研究教育用コンピュータ及びネットワークシステムの整備も各大学において行われている。このようなシステムにおいては、従来からあるプログラミング教育を中心に据えた UNIX 系システムと、ビジネスアプリケーションを中心に据えた Windows 系システムがしばしば併存する。

UNIX 系システムと Windows 系システムの利用者情報の統合については、様々な試みが行われている [1–6]。しかし、基本的には、別々に利用者登録を行ない、パスワード管理を行う必要がある。一定以上の規模を有する大学においては、全学共通の演習システムの他に、学部や学科が設置する専門教育用演習システムを別に有している場合もある。

上記のような場合、利用者は複数の利用者 ID を持ち、パスワードの管理などを行わなければならない。管理者は、各システムごとに利用者情報を集め、登録管理作業を行うことになる。

オンラインで情報を収集及び提供する情報システムの整備も各大学において進んでいる。オンラインシラバスや教員情報のオンライン化など教育研究情報の登録、オンラインによる講義登録や履修者一覧提供など教務情報のオンライン化、更に物品請求などの事務情報のオンライン化も進められている。このようなシステムにおいても、利用者の身分や所属を含めた認証が必要である。

現状では、各情報システムの OS などの違い、及び設置主体の違いから、各情報システムが個別に認証情報を管理している。このような状況は、以下のような理由で、利用者側と管理者側の双方から不都合である。

利用者は、各情報システムごとに利用者 ID とパスワードを管理しなければならない。学生を含む情報処理技術レベルの多様な利用者に、複数 ID の管理を求めることは、非常に危険である。平易な共通パスワードを設定したり、他人の目に容易にふれる場所にパスワードを書くなど、という状況を誘発するからである。

管理者側から見ると、利用者情報の収集管理を各システムで行う必要が発生する。また、利用者からどの ID を使うべきかの問い合わせが増大することも、大きな管理コストとなる。

大学の構成員は、原則として 1 年単位で変更される。また学生と教職員の情報は学生部や任用係で管理され、かつこれらでほぼ全ての構成員情報を尽くしている。

この情報に基づいて、全学で共通的な認証システムを構築することが出来れば、利用者及び管理者の双方に大きな利点となる。

2.2 統合認証に必要な機能

情報システムの認証には、大きく分けて二つのタイプがある。第一は、通常の OS が行うような機器利用のための認証である。第二は、Web からの情報アクセスのような特定の機能を使うための認証である。

機器の利用に際した認証では、各 OS ごとの認証サーバに利用者情報の登録が必要である。利用者の権限の制御は、利用者のグループなどに対応した ID によって制御されている。これら、OS ごとに異なる認証サーバのデータ生成、管理、パスワード変更に、統合認証システムは対応しなければならない。

情報アクセスに際した認証においては、二つの情報の確認が必要である。一つは、当該利用者が、情報にアクセスする権限を有しているかの確認である。つまり、利用者名だけでなく、身分、所属などを判別する必要がある。本稿では、これらの情報を汎用的データベースで管理することを前提として論を進める。

第二の確認事項は、利用者 ID とパスワードから本人であることを確認することである。情報システムごとに、通常の機器利用と同様に利用者情報を登録しないためには、この認証はネットワークを介して、中央の認証サーバに行う方式が必要となる。この場合、できるだけ汎用的で多様な認証方式の提供が必要である。

上述のように、統合認証システムは、複数の OS に対して認証データを提供するとともに、利用者権限管理の基となる所属や身分に関する情報を提供しなければならない。構成員の大規模な移動が 1 年ごとに行われることと、組織改変なども時々起こること、更に一時的な転出転入も起こることから、汎用的データベースシステム上で利用者管理を行うことが効率的である。

認証情報の基本となるのは、個人情報であり、高度のセキュリティーレベルを保持しなければならない。従って、認証の基本データを保管するデータベースシステムなどの中心システムは、ネットワーク的に隔離した構成を取るべきである。また、認証を必要とする情報システムから、認証情報へのアクセスは適切な暗号化通信路を確保すべきである。

2.3 統合認証システムの基本構成

統合認証システムは、基本となるデータベースシステム、各 OS に対応した認証サーバ、多様な認証プロトコルに対応した認証サーバ、及びそれらの基盤となるネットワークシステムから構成される (図 1)。

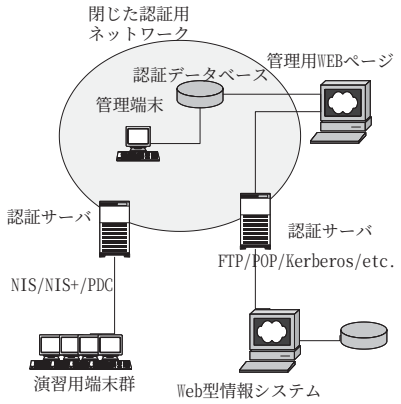

図 1: 統合認証システムの概要

認証データベースは、全利用者の氏名や所属などの基本情報を保存する基本テーブル、情報システムで使われる利用者名とパスワードなどを保存する情報システム専用テーブル、管理者名と管理者権限を保存する管理者テーブル、及び所属、身分、状態などを表すコードテーブルから構成される。個別の情報システムで独自情報が必要な場合には、別に個別情報システム専用テーブルを設ける。

大学の全構成員の利用者情報の集約のため、学生部や任用係などの利用者情報の発生元での、情報入力及び管理を可能にする必要がある。そのために、管理者テーブルを介して、変更可能な情報の範囲を制御する。

機器利用に際した認証では、それぞれの OS に応じた認証サーバを構築する必要がある。例えば、UNIX 系システムに対しては NIS や NIS+サーバを、Windows 系システムに対しては PDC を設置する。UNIX 系システムと Windows 系システムが共存する場合には、パスワード同期のための仕組みを別途用意する。

情報アクセス時の認証については、利用者 ID とパスワードを使った本人同定と、利用権限の確認が必要である。前者については、ftp などの一般的通信プロトコルや Kerberos などの汎用的認証プロトコルを用いて NIS 等と同期したサーバへ問い合わせ、後者については認証データベースへの問い合わせを行う。

認証基本データを有するデータベースは、外部からのアクセスが出来ない閉じたネットワークとして構成する。

2.4 統合認証を支える人的体制

統合認証システムは、全学の構成員全員が登録されて、はじめてその価値が発揮出来るシステムである。大学の構成員は、学生、教職員、その他の構成員に分類することができる。学生は学生部などの事務組織が、教職員は任用係などの事務組織が全員のデータを保持している。これらの事務組織が有するデータを円滑に登録することが、統合認証システムの運用には不可欠である。

学生部や任用係などの人の動きを管理する事務組織からの直接的な入力が行えることが望ましい。次善の策としては、統合認証システムを管理する部門との間のデータ交換フォーマットや、定期的な情報交換などの仕組みが必要である。

大学では、学生と教職員以外の身分の人を受け入れることがある。これらの利用者の登録は、利用申込に基づいた個別入力によって対応する。

3 佐賀大学における統合認証システム

3.1 システム基本構成

佐賀大学は、4 学部と旧教養部に対応する全学教育センターから構成され、学部及び大学員生の総数約 7000 人、教職員約 500 人を要する小規模総合大学である。全学部が、本庄キャンパス一箇所に設置されている。

学術情報処理センターでは、2002 年 2 月のシステム更新において統合認証システムを構築し、運用を行っている。統合認証システム導入の契機は三つある。第一は、学術情報処理センター内の研究教育用システムの利用者管理において、UNIX システムと Windows システムの利用者情報の統合を図ることである。第二は、附属図書館び電子図書館システムの利用者管理を学術情報処理センターの利用者管理と統合することである。第三は、全学に設置した教育用情報基盤ネットワークへの認証機能の提供である。

統合認証システムは、前節で述べたように、認証データベース、NIS 及び NIS+ サーバ、PDC 及び BDC から構成されている。情報システムからの認証は ftp や pop などの汎用的プロトコル、及びそれらの暗号化された汎用的なプロトコルによって行われている。

認証データベースは、個人情報の基礎となるメインテーブルの他、学術情報処理センターの利用者 ID を管理するセンター用メインテーブル、附属図書館利用者 ID を管理する図書館メインテーブルを中心に、所属テーブル、身分テーブル、状態テーブルなどの付属テーブルから構成されている。

テーブルへの登録・変更は、専用の管理端末の他、アクセス制限と利用者認証機能を持った専用の Web ページから行う。専用 Web ページを使って、センター及び附属図書館では利用申込を扱う事務担当者が登録を行っている。また、専用 Web ページからは、センター側担当者はセンター関連情報のみを、附属図書館側担当者は図書館関連情報のみを入力・編集する。

UNIX システムでの UID や初期パスワードなどは、別途生成して、システム管理者によって、データベースへの登録と NIS+サーバ及び PDC への登録が行われている。ここで登録されるパスワードは、初期パスワードを暗号化したものであって、利用者によるパスワード変更には同期しない。パスワード忘れの際に、登録された初期パスワードに戻すために保持している。認証サーバへの登録まで含めた一連の登録作業の自動化は、今後の検討課題である。

3.2 研究教育用システム

学術情報処理センターでは、2002 年 2 月にシステム更新を行い、研究教育用 UNIX サーバの他、約 200 台からなる演習用端末群を導入した [4]。演習用端末はディスクレスで、Linux と Windows2000 をブートできる。UNIX サーバ群と演習用端末の Linux は NIS+ による認証を行っている。Windows 系 OS に対しては PDC による認証を行っている。

全ての利用者は UNIX 系 OS と Windows 系 OS に利用 ID を有し、初期パスワードは同じものが設定されている。パスワード変更を、専用の Web ページから行うことで、パスワードの同期を行っている。専用 Web ページでのパスワード変更に際しては、NIS+側の現在のパスワードで認証して、新たなパスワードを

NIS+側及び PDC 側に設定している (図 2)。

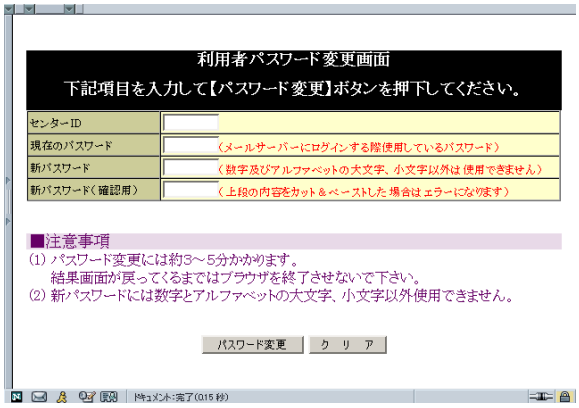

図 2: パスワード変更画面

3.3 附属図書館及び電子図書館

附属図書館では、統合認証システムの個人情報を使って、貸し出しなど図書館業務固有のデータベースなどの整備を行っている。

佐賀大学の電子図書館システムは、2001 年度より整備が始まったものである [7,8]。電子図書館システムには、オンラインシラバス、教員基礎情報、及び研究業績データベースが含まれている。これらのデータベースへの入力は、教員本人が Web を介して入力することを基本としている。そのため、入力フォームへのアクセス時に、認証データベースと連動した教員 ID データベースへ接続し、教員 ID を得た後に、NIS+を使って認証を行っている (図 3)。

図 3: オンラインシラバスの認証画面

3.4 ネットワーク利用

全学の構成員がキャンパス全域で柔軟にネットワーク利用可能なように、新しいタイプのネットワーク整備を 2001 年度に行った。全学の全ての普通教室やオープンスペースに、情報コンセントと無線 LAN 局を設置し、公開端末や利用者の持ち込む移動端末を申請などを行わずに接続することができるシステムである。

ネットワーク利用を開始する際に認証を受ける仕組み Opengate が導入されている [9,10]。利用者が Web ブラウザを起動すると、自動的に認証画面が表示されるものである。この認証には、学術情報処理センターの認証サーバが使われ、利用者はセンターシステムの利用者 ID とパスワードでネットワーク利用を開始することができる。

3.5 その他情報システム

Web を使った情報システムが様々な形で実現されている。これらの情報システムの中には、認証が必要なものも多い。前述の電子図書館システムも、Web を使った情報システムであるが、システム構成の際に NIS+の認証を採用した。ネットワーク的に NIS+ドメインから離れている場合等には、別の認証方法を採用する。

例えば、学術情報処理センターでは、システム管理者間で各サーバ類のネットワーク関係ソフトウェアのバージョン管理情報を共有するシステムを運用している。このシステムでは、アクセス可能な管理者テーブルを有し、アクセス権限の制御とともに、認証サーバに対して利用者の同定を行っている。

4 まとめと議論

コンピュータとネットワークが情報通信基盤となることに対応して、学内において複数の情報処理システムが併存し、複数の認証システムが併存している。これらを統合し、利用者が一つの ID とパスワードの組を使って、様々な情報システムを利用するための、統合認証システムの提案を行った。

統合認証システムは、大学の全構成員の情報を持つデータベースシステムを中心に、情報端末利用のための OS ごとの認証サーバ、及び情報システムへのアクセスの際の認証サーバから構成される。情報システム

へのアクセスの際には、利用者 ID とパスワードを使った本人確認と同時に、認証データベースを使った利用者権限の制限を行うことができる。

佐賀大学では、2002 年 2 月のシステム更新時に、統合認証システムを導入した。電子図書館システムなど、先行するシステムについても、利用者情報や認証データの統合及び認証時の暗号化を進めている。

統合認証や情報管理については、Kerberos や LDAP などのプロトコルが提案され、実装されている。これらのシステムは、対応できるシステムや保持できるデータに制限がある。基本に統合認証データベースを持ち、汎用的な認証プロトコルに対して、認証データを提供することが有効であろう。

統合認証システムが有効であるためには、全構成員の情報を集約することが必要である。学生や教職員の移動を把握している事務組織との連携が不可欠である。学生や教職員の事務組織での登録時に、統合認証システムへの登録が行えるような仕組みの整備が必要である。

パーソナルコンピュータが高速化するとともに低価格になり、全学的なネットワーク整備が進んだ状況下で、情報処理センターの役割は大きく変化しつつある [11]。少なくとも地方大学の情報処理センターにおけるサービスの中で計算資源の提供はその重要性を大きく下げている。多くの教員と学生にとって、各研究室のパーソナルコンピュータなどの計算資源で十分であり、こく少数の大規模計算の必要な教員と学生にとっては情報処理センターが提供する計算資源では不足であるからである。

一方で、本稿で述べた統合認証、電子図書館などの情報システム、ネットワークセキュリティー対策などの需要が増大している。つまり、情報処理センターに求められている機能が、コンピュータやネットワークなどの物理的基盤の整備から、情報の収集、提供、及び管理へと移行している。統合認証システムは、情報処理センターの新しい役割の中心となるシステムになるであろう。

参考文献

[1] 江藤博文, 小野隆久、平良豊、只木進一、渡辺義明「UNIX と Windows の共存する教育用システムにおける利用者管理と端末管理」 学術情報処理研究 No. **2**, pp. 14 (1998).

[2] 佐野雅彦「教育用計算機システムにおけるユーザアカウント管理手法」 学術情報処理研究 No. **3**, pp. 13 (1999).

[3] 古瀬一隆、坂口瑛「UNIX と Windows を統合した情報処理教育環境の構築」 学術情報処理研究 No. **5**, pp. 21 (2001).

[4] 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 2002-DSM-25, pp. 19 (2002).

[5] 宮下卓也、山井成良、大隅淑弘、林伸彦「岡山大学総合情報処理センターにおける利用者認証とその応用」 情報処理学会研究会報告 2002-DSM-25, pp. 13 (2002).

[6] 丸山伸、北村俊明、藤井康雄「Virtual Machine を活用した大規模ファイルシステム」 情報処理学会研究会報告 2002-DSM-25, pp. 25 (2002).

[7] 安田伸一、木村伸子、福井市男、只木進一「オンライン・シラバス」学術情報処理研究 No. **4**, pp. 105 (2000).

[8] 安田伸一、木村伸子、福井市男、只木進一「佐賀大学電子図書館システム『とんぼの眼』」学術情報処理研究 No. **5**, pp. 81 (2001).

[9] 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 **42** (12), pp. 2802 (2001).

[10] 只木進一、江藤博文、渡辺健次、渡辺義明「公開端末及び利用者移動端末の認証システムとそのディスクレスマシンによる運用」学術情報処理研究 No. **5**, pp. 15 (2001).

[11] 津久間秀彦 他「大学情報サービス基盤整備における情報処理センターの役割」 学術情報処理研究 No. **4**, pp. 93 (2000).