大学における情報基盤整備の中核となる統合認証システム

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

学内の情報基盤が整備された現在、学内の組織による各種情報システムが増えつつある。これらの情報システムの多くは認証を受けて利用するシステムであり、情報システムごとの利用者管理では、利便性及び安全性の両面で不都合がある。そこで、大学における情報システムの認証の統合を行うシステムを提案する。また、統合認証システムのための、技術的人的基盤について議論する。このような統合認証システムの構築は、情報処理センターの業務において、コンピュータやネットワークなどの物理的基盤の整備に代わる、一つの新しい中心になる機能となると考える。

Integrated Authentication System as a Base of Campus Information Infrastructure

Hirofumi ETO† , Kenzi WATANABE‡ , Shin-ichi TADAKI† and Yoshiaki WATANABE‡
†*Computer and Network Center, Saga University*
‡*Department of Information Science, Saga University*

The number of information systems is increasing according to the improvement of campus network infrastructure. Some of these information systems require user authentication. It will contains various problems in convenience and security, if those systems have their own independent authentication mechanisms. We propose an integrated authentication scheme for information systems in an university. We will discuss the technical and organization bases of the integrated authentication systems. The integrated authentication system will be a more important service of university computer center than improving physical information infrastructure.

1 はじめに

情報処理技術は、大学における全ての研究教育分野で、基盤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。様々な研究教育情報もオンラインで提供されている。そのため、大学の全構成員が個人用の利用者 ID を持ち、各種情報システムを、認証を受けて利用する環境が整備されつつある。

現在のところ、上記のような情報システムは、OS や設置者の違いにより、各システムごとに利用者情報を収集し、個別の認証システムを実装する場合が多い。一つの大学内において複数の認証機構を有すると、利用者が複数の利用者 ID とパスワードの組を管理する一方で、各情報システムの管理者が個々に利用者情報の収集及び管理を行うことになる。このような環境は、情報基盤として様々な問題を有している。

大学の利用者は、情報処理技術にはじめて触れる新入生から、大規模計算の利用者まで多様である。このような多様な利用者に複数の利用者 ID とパスワードの管理を求めると、一部の利用者によるパスワード忘れや簡単なパスワードの設定、という問題を誘発する。また、複数のシステムでの個人情報収集と管理のコストが必要なだけでなく、複数のシステムで利用者情報のセキュリティー管理が必要となる。

今日、情報システムの利用資格は、単にコンピュータを使う権限ではなく、大学構成員の基本要件として、大学の基本情報へアクセスする権限となっている。従って、大学内における利用者 ID と認証機構を統一することが、情報基盤の一層の利用促進と安定運用に不可欠である。

統合認証は、全学的に共通の認証機能を提供することを目的とするものである。従って、大学の全構成員の情報を保持していることが必要である。また、認証を行うシステムの多様性に対応して、多様な認証方法を提供する必要がある。特に、情報システムの設置や更新が非同期的に行われることから、できるだけ既存の汎用的手法を組み合わせて用いることが重要である。

本稿では、こうした統合認証を可能にする枠組を提案するとともに、それを支える技術的・人的要素を検討し、佐賀大学における実装及び運用状況を報告する。

2 統合認証システム

2.1 統合認証システムの機能

統合認証システムは、全学に分散する多様な情報システムに認証情報を提供することを目的としたシステムである。情報システムには、大まかに二つのタイプのものがあり、これら両方に認証情報を提供できなければならない。第一は、端末利用などの情報システムに直接ログインするものである。第二は、Web 情報システムのように、情報アクセスに認証を必要とするものである。

統合認証システムは、利用者情報を集中登録するデータベースシステムを中心に、上述の二種類の情報システムへ認証情報を提供する。

システムに直接ログインが必要な情報システムとして、情報教育用システムや、研究用計算機システムがある。これらのシステムは、通常、UNIX 系 OS と Windows 系 OS が併存していることが多い。この二つの OS を有するシステムに共通の利用者管理を行う方法についてはさまざまな研究が行われてきた [1]-[6]。しかし、現在利用できるもっとも安定した方式は、両者を独立して管理し、パスワード同期などの仕組みを別途組み込む方式である。

統合認証システムは、基本のデータベースに全利用者情報を保持し、そこから UNIX 系 OS の認証サーバー (NIS や NIS+など) へ認証データを提供するとともに、Windodws 系 OS の認証サーバ (PDC) への認証データの提供を行う。パスワード同期に関しては、両システムのパスワードを一度に変更する機能を別途導入することで実現する。

学内には Web を介して利用できる様々な情報システムが構築されつつある。これらのシステムでは、管理者以外の利用者 ID をシステム内に保持しない場合が多い。多くの Web サーバでは、リモートの利用者情報を使って認証を行う機能を容

易に構築できる。統合認証システムは、これらの情報システムに対して認証情報を提供する必要がある。

利用者が直接ログインするような情報システムの場合、利用者権限の制御はグループ ID のような機能を使って行うことができる。従って、統合認証システムが利用者身分に応じたグループ ID 管理を行うことで、利用者権限の制御を行うことができる。

一方、Web 利用などの場合、認証によって行うことは本人同定だけである。利用者権限の制御が必要な場合、Web 情報システム自体が利用者ごとの権限データベースを持つか、統合認証システムのデータベースと交信することで権限区分を取得する必要がある。

2.2 統合認証システムの構成

統合認証システムは、全利用者情報を管理するデータベース部分と、各情報システムへ認証データを提供する部分から構成される (図 1)。

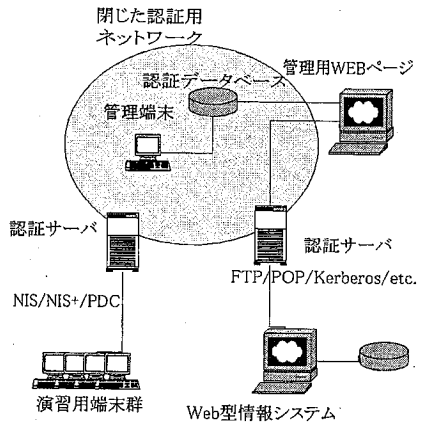

図 1: システム構成

認証データベースに保持されるのは、個人情報であるため、孤立したネットワーク構成とするなどに、安全性に対する十分な配慮が必要である。認証サーバへのデータ転送なども、できる限りこの孤立したネットワーク内に留めることが必要である。

認証データベースには、一般的な関係データベースを用いる。基本となる利用者テーブルには、氏名、読み、ローマ字表記、所属、身分、状態などを収める。利用者 ID と初期パスワード、有効期限や状態などを有するシステム利用情報テーブルを別にすることで、所属や身分変更と利用者 ID とを切り離して管理することができる。初期パスワードは、利用者がパスワードを忘れた場合に利用する。佐賀大学の場合、図書館の利用者管理用テーブルが用意され、所属及び身分管理を共用している。

利用者によるログイン時の認証のためには、NIS や NIS+ といった UNIX 認証サーバ及び Windows 用に PDC を用意する。こららの UNIX 系 OS や Windows 系 OS の認証サーバへの情報提供は、認証データベースからそれぞれの認証サーバのデータ形式に合わせた出力を生成することで行う。つまり、データベース内容の更新は、管理端末から行うのみで、認証サーバ側からは行わない。このことによって、システム障害や誤操作による基本データベースの障害を防ぐ。

Web 型情報システムへの認証情報提供は、汎用的な認証サーバを設置することで行う。この認証サーバは、上述の UNIX 系 OS の認証サーバの NIS ドメインなどの管理下に置く。Web 型情報システムは、FTP、POP あるいは IMAP など、及びそれらの SSL 化されたプロトコルを使って認証サーバへの接続を確かめる方法や、Radius や Kerberos などによって認証サーバから認証を受けることで利用者の同定を行う。

Web 型情報システムにおいて利用者権限の制限を行うために、利用者の所属や身分を確認するには、認証データベースからそれらの情報を得なければならない。認証データベースへ SQL リクエストを送ることは、システムの可搬性を低下させるとともに、安全性の問題を引き起こす可能性がある。後述する LDAP などによる実装が必要であろう。

2.3 統合認証システムのための組織体制

統合認証システムは、学内の全構成員の登録が必要不可欠である。大学には学生、教職員、その他の構成員が存在し、学生部及び任用係などの事務組織がほぼ全員のデータを保持している。これらの事務組織と密接な連絡体制を整え、構成員が移動した場合に円滑に対応することが必要である。

構成員の移動を管理する事務組織が基礎となるデータの直接的な入力を行なうことが最も望ましい。情報システムの利用が、大学の活動の基盤である以上、利用者情報管理の大学としての組織的取り組みを行うべきである。現状では、データ交換フォーマットの統一や、定期的な情報交換などで対応することが現実的である。

3 佐賀大学における運用状況

3.1 システム構成

佐賀大学では、2002 年春のシステム更新において、学術情報処理センターの利用者管理と附属図書館の利用者管理を一元化することを目的として統合認証システムの構築を行った。統合認証システムの構築によって、従来は学術情報処理センターと附属図書館で個別に行っていた利用者登録作業を一括して行うことを可能とした。学術情報処理センターが提供する研究教育用コンピュータシステム、特に Wiindows と Linux 環境を提供する演習用システム、電子図書館システム、利用者のノート型パーソナルコンピュータが接続できるネットワークでの認証、附属図書館の利用者管理、附属図書館内の検索端末の認証を統合的に行うことが可能となった。

基本となる認証情報データベースに対する登録・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。この際の利用者認証も統合認証システムを利用し、学術情報処理センター及び附属図書館の利用申込を扱う事務担当者が登録作業を行っている。その際、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・編集するように制限をかけている。

3.2 センターシステム

2002 年春から稼動している佐賀大学学術情報処理センターの演習用システムは、Windows と Linux のダブルブートをディスクレスで実現するシステムである [7, 8]。このシステムには、佐賀大学の全学生及び全教職員の利用者 ID が登録されている。この利用者 ID は、演習システムだけでなく、メールサーバ、研究用 UNIX システム、後述するネットワーク利用にも共通するものである。

利用者は専用の Web ページからパスワードを変更することで、UNIX 系 OS と Windows 系 OS を同期的に変更することができる (図 2)。

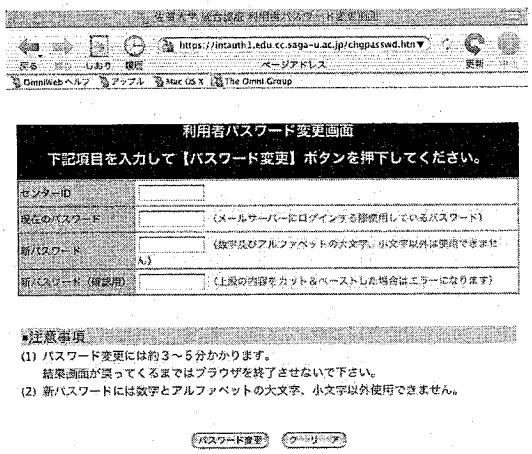

図 2: パスワード変更画面

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用いて本の貸し出しなどの業務を行っている。更に、教員ならば図書の購入を行うことが可能であることなどの、身分に応じた処理にも、統合認証システムを用いた処理を行っている。

附属図書館と学術情報処理センターが共同で運用する電子図書館では、オンラインシラバス [9]、

教員基礎情報、及び研究業績データベース [10] が稼働している。これらは担当教員及び教員本人がオンラインで入力、編集を行うことを基本としている (図 3)。

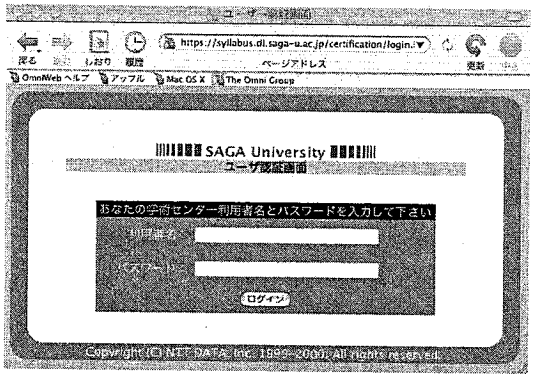

図 3: オンラインシラバス認証画面

このシステムは、統合認証システムに先行して構築されたため、統合認証システムとの連携は部分的である。

3.4 ネットワーク利用

佐賀大学では、全教室及び附属図書館や学生会館などの学生が利用する公共スペースなどを中心に、新しいタイプのネットワーク構築を進めている [11]。このネットワークは、学術情報処理センターの利用者 ID を有する者はだれでも、個人のパーソナルコンピュータなどの情報機器を接続することができる。また、このネットワーク下に設置された端末を利用して、インターネットに接続することができる。従来のネットワークとは異なり、機器接続を登録するのではなく、利用者資格を得ることで利用できるシステムである。

このシステムを通じてインターネットに接続する際に認証するシステム Opengate を開発整備した [12]。この際の認証にも、統合認証システムが利用されている。

3.5 汎用プロトコル対応認証サーバ

佐賀大学にはいくつかの組織が独自に設置している情報システムが存在する。これらのシステムは、様々な OS や認証機構で構成されているため汎用的な認証が可能なサーバが必要である。

我々はこれらのシステムの認証のため、汎用的なプロトコルに対応した認証サーバを設置した。これらのプロトコルの一部は通信経路が暗号化されていないため、盗聴などによるセキュリティ上の問題がある。これらのプロトコルについては、SSL に対応した認証サーバを設置した。

対応認証プロトコルを表 1 に示す。

表 1: 対応認証プロトコル

POP3(Post Office Protocol Version3)
POP3S(POP3 over SSL/TLS)
IMAP(Internet Mail Access Protocol)
IMAPS(IMAP4 over SSL/TLS)
FTP(File Transfer Protocol)
FTPS(FTP over SSL/TLS)
TELNET
TELNETS(TELNET over SSL/TLS)
RADIUS
SSH(Secure SHell)

4 まとめと議論

大学内には複数の情報システムとその認証を行う複数の認証システムが存在する。我々はこれらの認証システムを単一のユーザ ID とパスワードで認証を行う統合認証システムを構築した。

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とその認証サーバから構成される。認証サーバは OS ごとの認証を行うサーバと情報システムの認証を行うサーバに分けられる。情報システムの認証を行う認証サーバには汎用的な認証プロトコルを用いているが、そのままではネットワーク上を平文のパスワードが通るためセキュリティ上問題である。このため我々は汎用的な認

証プロトコルを SSL に対応させるとともに、他のセキュアなプロトコルによる認証サーバを設置し、よりセキュリティの高い認証システムの構築を行った。

今回実装した認証サーバ以外にも Kerberos などのセキュアなプロトコルが存在する。今後これらのプロトコルでの認証サーバも検討する。

ネットワーク上の軽量なディレクトリサービスである LDAP が、認証サービス機能として注目を集め始めている。Solaris などの UNIX 系 OS や Windows XP においても、認証として利用可能になりつつある。特に、異なる OS 間での利用者管理の統合が期待されている。現行の統合認証システムへ、LDAP を導入し、特に Windows 系 OS と UNIX 系 OS の利用者管理のより円滑な連携を図るための準備を行っている。

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] 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.19-23(2002).

[8] 佐賀大学学術情報処理センター「センターシステムの紹介」http://www.cc.saga-u.ac.jp/system/CenterSystem/index.html

[9] 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).

[10] 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).

[11] 江藤博文、渡辺健次、只木進一、渡辺義明「新しい教育用情報基盤の実現へ向けて〜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, pp. 13 (2002).

[12] 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.15-20(2001).