

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

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

{t_myst,yamai,oosumi,haya}@cc.okayama-u.ac.jp

概 要

教育用計算機システムの運用において、利用者認証はシステムの不正利用を防止するために、またトラブル等が判明した場合に利用者を特定できるようにするために必須である。ところが、システムの構成や運用方針により、必ずしも他機関の利用者認証方法が適用できるとは限らず、実際に我々は独自の工夫をしている。本稿では、岡山大学総合情報処理センターの教育用計算機システムにおける利用者認証方法について述べる。また、その応用として、電子メールにおける発信者詐称防止機能や WWW における利用者単位のアクセス制御機能などについても紹介する。

User Authentication and Its Application in Computer Center, Okayama University

Takuya Miyashita, Nariyoshi Yamai, Yoshihiro Oosumi and Nobuhiko Hayashi

Computer Center, Okayama University

{t_myst,yamai,oosumi,haya}@cc.okayama-u.ac.jp

Abstract

User authentication is one of the most important function of educational computer systems in order to prevent users from unauthorized access and to identify users when some trouble occurs. Since an applicable authentication mechanism for a system depends on the configuration or the operation policy of the system, we have developed a tailored authentication system. In this paper, we show how to build our authentication system. We also mention some other application functions based on the authentication system, such as protection function against e-mail sender address spoofing, a user-basis access control function of WWW clients, and so on.

1 はじめに

岡山大学は学生数約 13,500 人、教職員数約 2,800 人で 11 学部を擁する、地方大学としては比較的大規模の総合大学である。このような多数の学生に対する情報処理教育や計算機を用いた専門教育に供するため、本学総合情報処理センター（以下、センター）では教育用計算機システムを整備し、また日常業務

として本システムの管理・運用を行っている。現在利用されている教育用計算機システムは 2001 年 1 月に更新されたもので、約 610 台の教育用 PC と各種サーバ計算機群、およびこれらを相互接続するネットワークシステムなどから構成されている。

この教育用計算機システムは、公開講座等で利用する場合を除き、原則的には本学の学生・教職員（利用有資格者）に対して教育用の用途に限って利用が

認められる。したがって、利用有資格者のみに本システムの利用を限定するため、また目的外利用やトラブルが判明した場合に利用者を特定できるようにするために利用者認証は必須である。特に 2000 年 2 月 13 日に施行された不正アクセス防止法 [1] ではアクセス管理者による防御措置義務（努力義務）が規定されており、同法施行以降ますます利用者認証は重要になっている。

教育用計算機システムにおける利用者認証は、たとえば文献 [2], [3] に示されるように多くの教育機関において様々な方法で行われている。しかし、システムの構成や運用方針により、必ずしも他機関の利用者認証方法が適用できるとは限らず、実際にセンターでは独自の工夫をしている。

本稿では、岡山大学総合情報処理センターの教育用計算機システムにおける利用者認証方法とともに、その応用について紹介する。

2 教育用計算機システムの概要

まず、本学における教育用計算機システムの配置状況について述べる。岡山大学には 9 学部を擁する津島キャンパスと 2 学部を擁する鹿田キャンパスの 2 つの主要なキャンパスがあり、津島キャンパスには約 11,500 人、鹿田キャンパスには約 2,000 人の学生が在籍している。津島キャンパスには総合情報処理センターの他、殆どの学部情報処理実習室が設けられ、合計で 10 教室に 532 台の教育用 PC が設置されている。また、鹿田キャンパスには 2 つの情報処理実習室があり、合計で 80 台の教育用 PC が設置されている。両キャンパスの間は地域ネットワークである岡山情報ハイウェイを経由して 155Mbps で接続されている。

このような配置状況を考慮して、我々は教育用計算機システムを以下のように構成した。

- 教育用 PC (津島: 532 台, 鹿田: 80 台)
 - 名称: NEC Mate NX MA80T/C
 - CPU: PentiumIII 800MHz
 - OS: Windows 2000 Professional
- ファイルサーバ (津島: 1 台, 鹿田: 1 台)
 - 名称: Sun Enterprise450
 - CPU: UltraSparcII 400MHz
(津島: 4 基, 鹿田: 1 基)
 - OS: Solaris 2.6
 - HD: 470GB(津島), 180GB(鹿田)
- 認証サーバ (津島: 3 台, 鹿田: 1 台)

名称: NEC Express5800 Model 120Mc
CPU: PentiumIII Xeon 600MHz
OS: Windows 2000 Server

- 1 次 WWW プロキシ (各情報実習室に 1 台)
 - 名称: NEC Mate NX MA80T/C
 - CPU: PentiumIII 800MHz
 - OS: FreeBSD 4.5R(2002 年 6 月現在)
- 2 次 WWW プロキシ (センター内に 6 台)
 - 名称: (組立て PC)
 - CPU: PentiumIII 800MHz
 - OS: FreeBSD 4.5R(2002 年 6 月現在)

このうち、教育用 PC には利用者や外部からの不正アクセス者による設定変更を防止するため、ハードウェア的にディスク内容を保護する装置 (ComGuard[4]) を導入している。この装置には鍵が取り付けられており、鍵が開かれている状態では通常通りディスクを読み書きできるが、鍵が閉じられた状態では保護領域に対する書き込みは実際にはディスク上の別の領域に書き込まれ、電源再投入時には消去されるようになっている。これにより、シャットダウンするまでの間はあたかも書き込みが実際に行われたかのように見えるが、電源再投入時には初期状態に戻るようになっている。

ファイルサーバには利用者単位でディスク使用量を制限できるように UNIX ベースのシステムを採用して quota 機能を有効にし、同システム上で samba[5] を動作させている。利用者当たりの標準の上限利用量は 250MB となっている。津島、鹿田の各ファイルサーバには、各キャンパスに所属する利用者用のホームフォルダが格納され、ログオン時には Z ドライブとして利用できるようになっている。また、個人用プロファイルもホームフォルダ内に格納され、移動プロファイル機能を用いてログオン時にはファイルサーバからローカルディスクに読み込まれ、ログオフ時には逆にローカルディスクからファイルサーバに書き戻されるようにしている。なお、My Documents フォルダもホームフォルダ内に格納されるが、移動の対象とはしておらず、常にネットワーク経由でアクセスされるように設定している。

教育用計算機システムが接続される教育系ネットワークはセキュリティの面からプライベートアドレス (172.25.0.0/16) を割り当てている。このアドレスに関する経路情報は学内の研究系ネットワーク (150.46.0.0/16) に対してはアナウンスされているため、教育用 PC から研究系ネットワークへの通信

は自由に行えるが、学外への通信は直接は行えない。そこで、センター内に教育系ネットワークと研究系ネットワークの双方に接続される(2次)WWWプロキシを6台設置して教育用PCから学外へのアクセスを中継するようにし、さらに後述するように利用者単位のWWWアクセス制限機能を実現するため各情報実習室に1台ずつ(1次)WWWプロキシを配置した。

この他にメールサーバ、WWWサーバ等の役割を兼ねているスカラ計算サーバ(Sun Enterprise 3500)や大規模科学技術計算を行うためのベクトル計算サーバ(NEC SX-5S/2)など、多くの計算機が研究用計算機システムとして存在し、一部の機能が教育にも用いられている。

現在稼動している教育・研究用計算機システムの全体の構成を図1に示す。

3 利用者認証方法

3.1 UNIX と Windows との利用者情報の共有

本システムの導入当初は、更新前のシステムにおけるUNIX用利用者情報(特にパスワード)をそのまま流用する方針を立てていた。これを実現するため当時検討したのは、(1)Services for UNIX (SFU)[6]を用いる方法、(2)sambaのPrimary Domain Controller (PDC)機能を用いる方法、(3)Kerberosを用いる方法などである。

このうち、(1)については、UNIX側のNIS(Network Information Service)機能をWindowsでも利用できるのではないかと期待していたが、実際には逆にWindows側で提供したNIS機能をUNIX側で利用するものであったため、断念した。(2)については、sambaはWindows NTによるドメイン(NTドメイン)としてのPDC機能を有しており、またsambaではUNIX用利用者情報を用いて認証することが可能であったが、当時利用可能であったsamba 2.0.xはWindows 2000クライアントに対してはPDCとなることができず、これによる利用者認証を断念した¹。また、(3)についてもWindows 2000ではKerberosがサポートされるという情報を入手したため検討を始めたが、これもWindows 2000独自の仕様によるものであることが判明し、結局断念した。

以上のように、当時検討した方法はすべてUNIX用利用者情報の流用は無理であったため、結局利用

¹現在利用できるsamba 2.2.xではWindows 2000クライアントに対してもNTドメインのPDCとなることが可能になっている。

者情報の管理は利用者管理データベースシステムであるDeviasを用いて集約し、利用者の登録・削除あるいはパスワードの変更はDeviasが認証サーバ、ファイルサーバ、スカラ計算サーバ等に対して個別に行うようにした。なお、これによりパスワードの再登録が必要になったが、教育系利用者に対してはセンター側で新たにパスワードを作成して通知し、また研究系利用者に対しては旧パスワードの更新依頼を通知した²。

3.2 アクセスログの記録

利用者認証は、単に利用有資格者のみに教育用計算機システムの利用を限定するためだけでなく、目的外利用やトラブルが判明した場合に利用者を特定できるようにするためにも用いられる。これを行うには、いつ、誰が、どの計算機を利用したかを示す情報(アクセスログ)を取り、これを記録する必要がある。

本システムの導入当初は、認証サーバにおいてイベントログを収集し、この中からログオン、ログオフの情報のみを抜き出して利用しようと考えていた。しかし、このイベントログには認証の成功・失敗の記録しかなく、またイベント情報の解析が難解で、どの計算機を利用したかを判明できなかった。

そこで、次にファイルサーバにおけるsambaへのアクセス情報をもとにログオン、ログオフの情報を構成する方法について検討した。本システムの運用形態では、ログオン時の処理の流れは以下のようになる。

- (1) 利用者は教育用PCに利用者名とパスワードを入力してログオンしようとする。
- (2) 教育用PCは入力された利用者名とパスワードを認証サーバに送り、利用者の認証を求める。
- (3) 認証サーバは認証結果を教育用PCに送り返す。
- (4) 教育用PCは認証結果に基づき、利用者のログオンを許可する。
- (5) 教育用PCは利用者のアカウント情報に基づき、ファイルサーバの利用者用領域をマウントしようとする。
- (6) ファイルサーバは認証サーバに利用者認証を求め、その結果を受け取る。

²初回変更時に旧システムのパスワードが入力可能で、変更後は教育系システムを含む全システムのパスワードが連動して変更される。

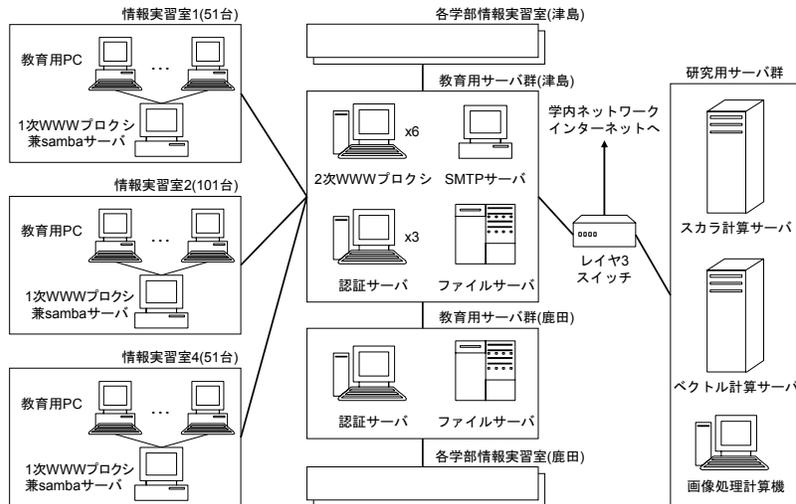


図 1: 教育・研究用計算機システムの構成

- (7) ファイルサーバは受け取った認証結果に基づき、利用者用領域のマウントを許可する。このとき、samba のログファイルに誰がどの計算機からどの領域をマウントしたかが記録される。

したがって、samba のログファイルを監視すれば、いつ、誰が、どの計算機を利用したかを特定できることになる。ただし、ファイルサーバは津島、鹿田キャンパスに1台ずつしかなく、特に講義開始・終了時には移動プロファイルのアクセスのためにかなりの負荷がかかることが予想された。そこで、最終的には負荷を分散させるために各情報実習室に設置されている1次WWWプロキシにsambaを導入し、そこでアクセスログを取ることにした。この場合、上記の手順に加えて以下の手順が実行される。

- (8) ログオンスクリプトにおいて、情報実習室内の1次WWWプロキシ兼sambaサーバ(計算機名をSSとする)上の特定の共有リソース(\\SS\pub)をマウントしてアクセスするようにする。
- (9) 1次WWWプロキシ兼sambaサーバはこの共有リソースへのアクセスを許可する。このとき、sambaのログファイルを監視し、どの計算機から誰がログオンしたかを記録する。

同様に、ログオフするときにも以下のような処理を行い、明示的にアクセスログを残すようにした。

- (10) ログオフスクリプトにおいて、SS上の特定の共有リソース(\\SS\end)をマウントしてアクセスするようにする。
- (11) 1次WWWプロキシ兼sambaサーバはこの共有リソースへのアクセスを許可する。このとき、sambaのログファイルを監視し、どの計算機から誰がログオフしたかを記録する。

ここで、ログオン、ログオフの記録は、後で他のプログラムから参照しやすいように工夫している。具体的には、utmp形式に従って端末名、利用者名、計算機名、ログオン時刻の4つ組から構成されるレコードを作成し、/var/log/wtmp及び/var/run/wintmp(/var/run/utmpの代わり)に記録するようにした。その際、端末名としては8文字以内に制限されていることから教育用PCのIPアドレスを16進表記したもの(たとえばac190c0b)とし、計算機名の部分についてはIPアドレスをドット付き10進表記したもの(たとえば172.25.12.11)を格納するようにした。

さらに、/var/run/wintmpに記録する際の位置³については、IPアドレスの下位2オクテットを用いて

³/var/run/wtmp では tty slot() を用いて位置を決定する。

決定する (たとえば 172.25.12.11 の場合には 0x0c0b = 3083 番目のエントリを参照する) ようにし、IP アドレスが与えられた場合にファイルを探ることなく直ちにエントリを参照することができるようにした。

以上のような工夫により、last や who などの UNIX 標準コマンドを利用して各教育用 PC の利用状況を管理することが可能となり、また後述するように種々の用途に認証情報を利用することが可能となった。

4 利用者認証機能の応用

これまでに述べた利用者認証機能を利用して、本センターでは種々のセキュリティ強化策や情報提供サービスを実施している。本節ではそのうちのいくつかについて紹介する。なお、これらの機能は更新以前の教育・研究用計算機システムでも運用していたが、システム更新時に運用を一時中断し、2002年4月より運用を再開している。

4.1 電子メールにおける発信者詐称防止機能

現在の電子メールでは端末側のソフトウェアの設定で発信者を容易に変更することができるなど、セキュリティ上の問題が多い。そこで本センターでは文献 [7] に示すように種々の対策を行っているが、そのうちの1つとして利用者認証機能を応用した発信者詐称防止機能 [8] を開発し、運用している。

この機能では、教育用 SMTP サーバは教育用 PC から電子メールの配送要求を受けると、当該教育用 PC の現在の利用者名を 1 次 WWW プロキシ兼 samba サーバに問い合わせ、その結果から生成した正しいメールアドレスと実際の発信者アドレスとを比較するようになっている。このとき、もし両者が一致しなければ、教育用 SMTP サーバは強制的に発信者アドレスを正しいメールアドレスに書き換え、今までの発信者アドレスを X-Original-From ヘッダとして残すようにする。また、強制的にアドレスを書き換えたことを syslog を用いて記録する。

4.2 WWW における利用者単位のアクセス制御機能

WWW はインターネットにおいて最もよく利用されるサービスの1つである。しかし、十分に教育を受けていない利用者が WWW を利用した場合、た

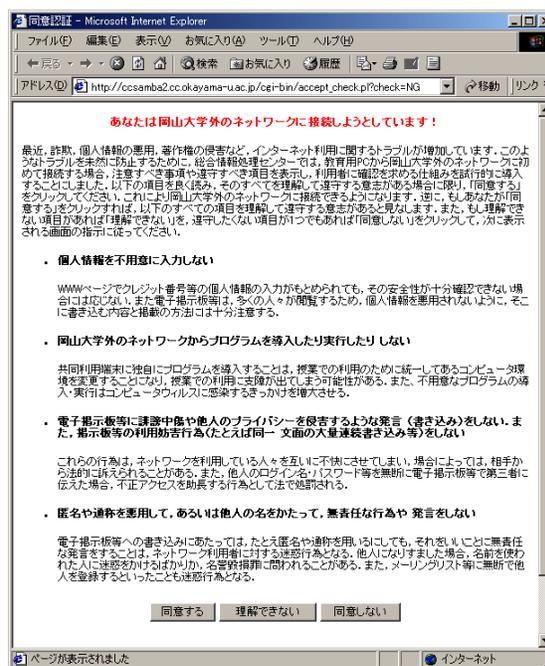


図 2: WWW 利用時の注意事項表示

たとえばクレジットカード番号などの個人情報の盗用やコンピュータウィルスの感染などのトラブルが発生する危険性がある。そこで本センターでは WWW でアクセスするときに利用者単位でアクセス制御を行う機能 [9] を開発し、運用している。

この機能では、教育用 PC においてブラウザが 1 次 WWW プロキシを経由して HTTP サーバにアクセスするように設定し、1 次 WWW プロキシでは教育用 PC から HTTP 要求メッセージを受け取ると当該教育用 PC の利用者を特定してその利用者とアクセス先 URL の組に基づいてアクセス制御を行うようになっている。このアクセス制御の動作には、(1) 無条件に許可する、(2) 無条件に禁止する、の 2 種類の動作に加えて、(3) 特定の条件が満たされた場合のみ許可する動作を設けている。これによりたとえば講義中のみアクセスを許可する、最初のアクセス時に注意事項を表示するなどの動作が可能となり、WWW 利用に関する様々なトラブルを軽減させる効果が期待できる。

本センターでは現在のところ各情報実習室から初めて学外の WWW サーバにアクセスするとき図 2 に示す注意事項を表示し、その遵守に同意した場合のみアクセスを許可するように本機能を設定している。この場合、条件付きアクセス制御機能を用いることにより、既に注意事項の遵守に同意している場合には注意事項が表示されないようになっている。

情報実習室の利用者一覧																								
最新更新: 2013年 05月 06日 木曜日 14時 13分 22秒																								
学部: <input type="text" value="日本語"/> <input type="button" value="更新"/>																								
000 en14238					001 en14238					002 en14238					003 en14238					004 en14238				
005		006		007		008		009		010		011		012		013		014		015		016		
en14238		en14227		en14218		en14242		en14286		002		003		004		005		006		007		008		
en14548		en14235		en14205		en14253		en14253		en14205		en14239		en14249		en14287		en14222		en14222		en14222		
029		030		031		032		033		034		040		041		042		043		044		045		
en14284		en14284		en14205		en14225		en14205		en14225		en14263		en14259		en14235		en14211		en14228		en14177		
041		042		043		044		045		046		047		048		049		050		051		052		
en14242		en14229		en14229		en14234		en14234		en14234		en14239		en14258		en14258		en14258		en14258		ec10465		
050		054		055		056		057		058		059		060		061		062		063		064		
en14233		en14250		en14216		en14217		en14232		en14232		en14244		en14251		en14213		en14204		en14206		en14203		
065		066		067		068		069		070		071		072		073		074		075		076		
ec11823		en14242		en14231		en14215		en14228		en14228		en14223		en14281		en14207		en14256		en14262		en14234		
en14214		en14221		en14241		en14236		en14239		en14239		083		084		085		086		087		088		
en14214		en14221		en14241		en14236		en14239		en14239		en14260		en14212		en14253		en14230		en14239		en14252		
089		090		091		092		093		094		095		096		097		098		099		100		
ec13808		en14249		en14245		ec13947		ec13928		ec13950		en14249		en14245		ec13947		ec13928		ec13950		ec13950		

図 3: 利用者一覧の表示例

4.3 各情報実習室の利用者一覧機能

情報実習室で講義を行う場合、教員が各教育用 PC の利用者名を特定できたり、あるいは受講者、自習者を区別できたりすると便利である状況がしばしば発生する。また、学生にとっては、センター内の 3 つの情報実習室のうちどこが空いているかがわかると便利である。そこで本センターでは利用者認証機能を応用し、各情報実習室の利用者一覧を表示する機能を開発し、運用している。

本機能を用いて利用者一覧を表示した例を図 3 に示す。

現在のところ、各情報実習室内の教育用 PC から学生以外の利用者がこの機能を利用した場合には利用者名まで表示され、それ以外の場合には各教育用 PC が利用されているかどうかだけが表示されるようになっている。また、センターの学生用出入口付近にはセンター内の 3 つの情報実習室の利用状況が表示される計算機が設置されており、多数の学生利用者が利用している。

5 まとめ

本稿では、岡山大学総合情報処理センターの教育用計算機システムにおける利用者認証方法と、同方法を電子メールにおける発信者詐称防止や WWW における利用者単位のアクセス制御などに応用した例を紹介した。この他、学外からのアクセスに対する学生用 WWW サーバへのアクセス制御、POP サーバの運用などでも利用者認証に関する工夫を行っているが、詳細については割愛する。今後も利用者認証はますます広範囲で必要になり、また従来の認証技術だけでは対応できない状況が予想される

が、その都度様々な工夫を行って対処していきたい。

参考文献

- [1] 不正アクセス行為の禁止等に関する法律, http://www.meti.go.jp/policy/netsecurity/fusei_access_law.htm
- [2] 田中哲朗, 安東孝二, 吉岡顕: “複数 OS 環境におけるユーザ管理”, 情報処理学会分散システム/インターネット運用技術研究会研究報告, 1999-DSM-16-9, pp.49-54, 平成 11 年 11 月.
- [3] 倉前宏行, 島野顕継, 木村彰徳, 松本政秀, 亀島鉦二: “ディレクトリサービスを用いた教育用 PC クラスタシステムの学生ユーザアカウント管理”, 分散システム/インターネット運用技術シンポジウム 2001 論文集, 情報処理学会, pp.93-98, 平成 13 年 2 月.
- [4] “瞬間環境復元ツール コムガード HDG-01”, http://www.idk.co.jp/products/hdg/HDG-01_1/index.html.
- [5] “SAMBA Web Pages”, <http://www.samba.org/>.
- [6] “Microsoft Windows Services for Unix 2.0 日本語版”, <http://www.microsoft.com/japan/windows2000/sfu/>.
- [7] 山井成良, 大隅淑弘, 林伸彦, 宮下卓也, 岡本卓爾: “岡山大学における電子メールのセキュリティ対策”, 学術情報処理研究, No.4, pp.79-83, 平成 12 年 10 月.
- [8] 石橋勇人, 山井成良, 安倍広多, 大西克実, 松浦敏雄: “メールクライアントに修正を要しない発信者詐称防止方式”, 情報処理学会論文誌, Vol.41, No.11, pp.3133-3141, 平成 12 年 11 月.
- [9] 山井成良, 山外芳伸, 林伸彦, 宮下卓也, 松浦敏雄: “WWW における利用者単位のアクセス制御機構”, 分散システム/インターネット運用技術シンポジウム 2001 論文集, 情報処理学会, pp.51-56, 平成 13 年 2 月.