システム利用マナー教育のためのアクセス管理

久保美和子　大塚秀治　牧野　晋　林　英輔
麗澤大学　国際経済学部
麗澤大学情報システムセンター

概要

Windows システムでは１つのアカウントで複数の PC にログオン（多重ログオン）が可能である。麗澤大学では多重ログオン機能を利用した利用権限の他者への貸与問題や、そこから派生する利用資格自体（アカウント）の開示を伴う問題が顕在化してきた。学生ユーザの日常的な情報システムの利用において情報倫理教育の視点から多重ログオンアクセスを管理する必要性がある。本研究では、システム利用のマナー教育の側面から多重ログオンを抑制するアクセス管理システムを構築した。システムは多重ログオンを検知すると警告メッセージをユーザにフィードバックし注意喚起する。UNIX のファイルサーバシステムを利用したため安価で比較的簡便に構築可能である。アクセス管理システムを運用した結果、利用マナーの向上に一定の効果が得られた。

Access Control for Training Information System Users on Usage Etiquette

Miwako KUBO, Hideharu OHTSUKA, Susumu MAKINO, Eisuke HAYASHI
The International School of Economics and Business Administration

Reitaku University
Reitaku University Information System Center

Abstract

In a Windows system, a single account can be used to log on to multiple PCs(multi-logon). At Reitaku University, problems because of duplicated logon have become evident: the multi-logon facility was used for lending usage authorization to others, which led to disclosing user authorization information (the account) itself. For everyday use of the information system by students, accesses by multi-logon must be controlled in order to educate users in information ethics. In this study, we constructed an access control system to suppress multi-logon for the purpose of training on the proper etiquette to follow when using the system. Upon detection of a multi-logon, the system sends a warning message to the logon user as an alert. A UNIX file server system was used for this system and therefore it was possible to build the system comparatively easily and at low cost. Running the access control system resulted in definite improvements in the etiquette followed when the system was used.

1. はじめに

麗澤大学[1]では、1997 年より Windows ベースの教育システムを運用している。情報リテラシー科目を全学生必修としているため、コンピュータ室の利用率は高い。しかしコンピュータ設置台数は、学生約７名あたり１台と比較的余裕があるので、利用の待ち行列ができることはほとんどない。

[1] 千葉県柏市。学生数約 3,000 人の小規模な大学。情報システムセンターが管理する PC は約 600 台（Macintosh を含む）である。http://www.reitaku-u.ac.jp/

しかし、このような環境下で、利用規則に違反する学生も目立ってきた。とりわけ1つのアカウントで複数のPCにログオンする機能（多重ログオン）を利用した利用権の貸与の問題や、それらから派生する利用資格自体の開示を伴う貸与の問題が顕在化してきた。必修となっている情報リテラシー科目でコンピュータやネットワークの利用マナーを含む利用規則の教育を行っているのにもかかわらず、利用権限の不正貸与を行ったユーザのほとんどは、その行為がシステム利用マナーに反する行為であることを正しく理解していなかった。

このことは、机上のマナー教育だけでは利用資格の重要性を理解させることは難しく、技術的な対策を行うことが必要であることを示唆する。本研究では、利用資格の安易な貸借につながる多重ログオン機能を抑制する方策を検討・実装し、利用権を限定することで、利用マナーの向上を期待するものである。以下に多重ログオンを抑止するための、アクセス管理システムの構成と、運用結果から効果および問題点について報告する。

2. 情報教育の現状

2.1 コンピュータ環境

教育用PCのOSはWindows2000ProおよびMacOS9である。学生用のコンピュータ室で提供しているサービスは以下の通りである。

- Windowsおよび Macintoshの利用
- 電子メールの利用
- 共有プリンタの利用
- インターネットへの接続
- UNIXサーバへの接続
- UNIXベースのファイル共有サーバの利用

設置数はWindowsおよびMacintoshあわせて約450台である。うち150台は夜間（午後9時まで）も利用可能である。他に構内自営PHS網と教室に設置されている情報コンセントが利用できる。コンピュータ教室は、授業がない時間帯は常時自習利用できる（午前9時から午後6時）。自習室は空席があれば常に利用することができる。また、利用時間の制限はない。いずれも、ユーザ認証を受けなければ利用を開始することができず、利用資格を有するユーザのみが利用を許可されている[1]。

本学は比較的自由に学外者の立ち入りが可能である。このため、夜間の利用ができる教室・建物は入退出管理を行っている。また、防犯カメラ・Webカメラによる監視体制を整備している。認証に際しては、利用資格を確認すると同時に利用履歴を認証サーバ内に保存している。

2.2 利用マナー教育

ユーザ認証に利用するアカウントは、全学生に配布される。利用規則で、アカウントは配布された本人以外の利用を禁止している。配布は、全1年生必須の情報リテラシー科目内にて行なわれる。入学後の最初の授業でコンピュータ利用上での規則および公式に定められたガイドラインに準拠して情報倫理・利用マナーについて詳細な説明が行われる[2]。その後、諸規則を遵守することを誓約する書類（誓約書）に自筆でのサインの記入を求める。この誓約書と交換でアカウントが記載された用紙が配布される。利用マナーに関する講義は初回の授業に限定されるものではなく、情報リテラシー科目内で繰り返し説明が行われる[3]。

利用規則に違反した全ての学生は、個別に情報システムセンター長から口頭で教育的指導を受けた上で、利用規則違反の内容により一定期間コンピュータシステムの利用権が停止[4]される。また、個人情報を伏せた形で違反内容と利用の停止期間が教室入口に告示される。

2.3 利用状況と規則違反

教育用コンピュータの利用率を設置場所別にまとめたものが図1である。1号棟はコンピュータ教室、2号棟・図書館は自習専用コンピュータ室である。2000年度は、コンピュータシステムの更新が行われたため、実際に授業でコンピュー

[2] 複数の教員が担当することになるため、詳細なマニュアルが用意されている。このため、クラス間の理解度の差は最小限に押さえられている。

[3] 2001年度より情報倫理のWBT教材も導入された。

[4] 単にPCの利用が停止されるだけでなく、リモートアクセス権限や情報コンセントの利用権も停止される。

タ教室が使われ始めたのは５月はじめとなっている。また、長期休暇期間は図書館の自習室以外を閉室している。

授業の合間にしか利用できない１号棟の利用率は30%程度とあまり高くない。しかし、実習専用コンピュータ室である図書館・２号棟については全体の利用率が80%を超える月がある。

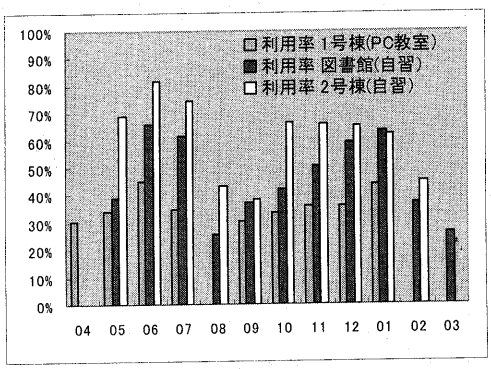

図 1 コンピュータ利用状況（2000/4~2001/3）

WindowsPC への全ログオン回数は約 25 万 7 千回で、総利用時間は約 4 万 2 千時間となる。1 回あたりの平均接続時間は 56 分、学生ひとりあたり年間 85 回以上 WindowsPC[5]を利用している計算となり、コンピュータの利用度の高さが示される。

一方、2000 年度中、利用規則違反をして利用停止のペナルティを受けた学生数は総数 76 名であった。違反者の重複は無いので、全ユーザの3.7%が規則違反を行ったことになる。規則違反の内訳を示したものが図２である。もっとも多い内容がアカウント貸借に関わるもので 42%を占める。アカウント貸借のほとんどが多重ログオンに起因したものだった。

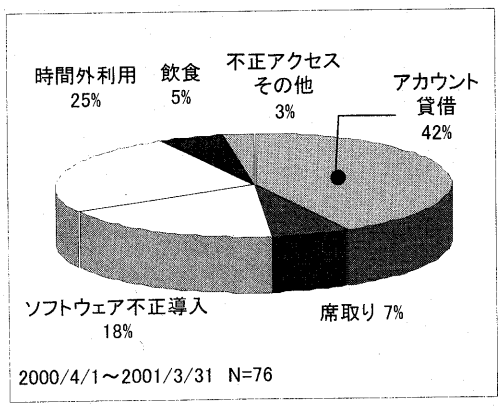

図 2 利用規則違反者(2000/4~2001/3)

3. 多重ログオンの問題

アカウントの貸借は、当然のことながら利用規則上で禁止している。利用権限のあるユーザがPC にログオンして他者に利用させる場合（パスワードを教えない場合）も禁止している。これは、不正使用や間違った利用を避けるためである。誤操作でネットワークドライブ内のファイルを消してしまうことも考えられる。学外者に利用させてしまう場合もある。さらに、悪意のある相手であれば本学のユーザになりすまして他の組織のユーザを中傷したり、内外のネットワークを攻撃する危険性もある。

利用者が２台の PC にログオンして、その１台を学外の友人に利用させる場合、実際には利用権限を貸与しているのだが、ユーザには規則違反の意識はほとんどない。他者がログオンして利用していても、自分も問題なく利用できるし、多重ログオンによって自己が有するリソースが減少しないためである。ファイルサーバ上の自分のファイルの削除、改変を伴うアクセスが行なわれる危険があるにも関わらず、CPU 時間や接続時間での課金や制限時間[6]の消費を伴わないため、安易にアカウントの貸借が行われる傾向にある。

多重ログオン自体は便利な機能でもある。通信プログラムやクライアントサーバのプログラムを作成する場合には複数のコンピュータを同時に利用しなければならない[7]。複数台のコンピュータを利用して負荷分散して作業を行う場合にも便利である。また、授業中に利用していたコンピュータがハングアップした場合、別のコンピュータでログオンして授業を続けたいというケースも考えられる。

---

[5] Macintosh の利用状況は本稿では割愛した。

[6] 本学では課金や利用時間の制限は行っていない。

[7] 研究室で利用する PC については、そのような利用が可能である。

しかし、コンピュータ教室や自習室といった環境では、利用者のいないログオン中のPCが存在することは好ましいことではない。さらに、すでに述べたように、多重ログオン機能の利用方法によっては、利用者のアカウントに関する管理責任の意識低下を招くことになり、それによるリスクも大きい。ユーザが自身の利用資格を守ることの重要性を教育するためにも、多重ログオンの機能を柔軟[8]に抑止することが望ましい。

4. 多重ログオンアクセス管理システム

4.1 システムの目的

本システムは、多重ログオン機能を検知しその行為をユーザに警告することにより、利用権限の貸与目的でのログオンを抑制することを目的としている。多重ログオンの状態をユーザにフィードバックしユーザが自発的にログオフするよう促している。多重ログオンを検知した場合に強制的にログオフすることも技術的には容易に可能であるが、マナー教育の観点からあえて採用していない。

なお、本システムで検知できる範囲を、表1に示した。①アカウントを他者に譲渡してしまい、自身は利用しない②アカウントが破られ悪意の他者に利用されている③自身がログオンして、他者に利用させ、自身は利用しない　というケースでは検知不能である。また、何らかの状態遷移の異常により、多重ログオンとして検知してしまう誤検知の可能性を有する。同一の利用資格が指定された利用空間で利用を開始した場合にのみ検知が可能となる。

表1　検知できる範囲

利用状況 / 状態	利用権限 不正	利用権限 正
多重ログオンあり	検知	誤検知
多重ログオンなし	検知不可能	通常利用

4.2 システムの概要

本システムはWindowsベースのネットワーククライアントはログオン時に自動的にファイル共有の設定が可能であることに着目し、ユーザのログオン状況をファイル共有サーバとなるUNIXサーバ上で確認する方式を採用した。全学生約3,000人を管理対象とし、教室・自習室・研究室設置PC（約400台）にログオンした際に稼動するよう設定した。多重ログオンを検出すると、該当ユーザのログオン画面に警告メッセージが表示される（図4）。

ファイルシステムの機器構成は以下の通りである。

サーバ
Sun Microsystems社Ultra Enterprise 5500
(8CPU, 4GBMem, 380GBHD, Solaris2.6)

ファイル共有システム
Totalnet社　TAS4.0
Samba　2.0.7-ja-2.2

クライアントPC
Compaq社製　　DESKPRO
OS　　Windows2000 Pro

本学のファイルサーバシステムは2001年3月までTotalnet社のTAS4.0、2001年4月よりフリーソフトsambaを利用している。本システムは、2000年11月にTotalnet社のTAS4.0用に開発し、その後samba用に移行した[9]。

なお、ユーザがログオンしている間は、ファイルサーバのセッションが接続されている状態であることが必須となる。このため、ファイルサーバの設定のうち、セッションタイムアウト時間

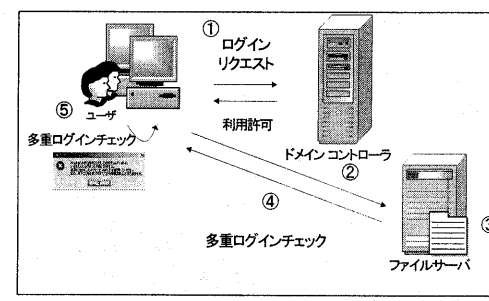

図 3 多重ログオンチェックの流れ

[8] 利用者や利用場所によって容易に設定を変更することができ、必要に応じて多重ログオンを可能にすることができる機能。

[9] ファイルサーバを商用版からフリーウェアに移行した主な理由は、クライアントPCがWindows2000の場合ログオン・ログオフを繰り返すうちにファイルサーバに接続が不能となるトラブルが頻発したためである。

(deadtime) を無制限とした。ソフトウェアは、ユーザ警告用システムおよび管理者監視用システムの2種類を開発した[2]。ユーザ警告用システムの基本的な動作は図3の流れとなる。

①WindowsPC 上では、ログオンが発生すると、認証後ログオンスクリプトが起動する。ログオン時のユーザ名は環境変数から得ることができる。

②ログオンスクリプト内では、ログオン時のユーザ名を利用し UNIX サーバ上のシェルスクリプトを rsh にてキックする。

③シェルスクリプトは、ファイル共有システムのステータスを参照し、現在接続中のユーザリストから許可できる接続かどうかを判断する。

④シェルスクリプトは結果をWinodwsPC側の標準出力へ書き込む形で送る。同時にログに記録する。

⑤WindowsPC 側では許容されない接続だった場合、警告のポップアップメッセージを表示し、ログアウトを促す。

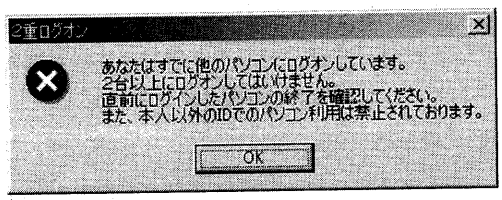

図 4 ポップアップ画面の例

サーバ側は、接続中のユーザを表示するためのファイルサーバ付属ツールを利用し、現在ログオンしたユーザが多重ログオンでないかチェックするスクリプトを perl とシェルスクリプトにて作成した。サーバ側プログラムはそれと同時に UNIX サーバ上に記録を残す。

WindowsPC 側は、Visual Basic Script を利用し、ログオン時に多重ログオンを検知した場合には、警告のポップアップメッセージ（図4）を表示する仕組みとなっている。

管理者用監視システムは、多重ログオンとなるセッションを検出すると管理者に電子メールで通知する。これは、UNIX サーバ上の cron により5分間隔で起動し多重ログオンセッションを検出している。多重ログオンを検知すると図5に示したような警告メールを管理者者向けに送信する仕様となっている。

ファイルサーバのセッションタイムアウト時間を無制限としているため、PC のハングアップで強制電源切断を行った場合、ファイルサーバシステム上でユーザセッションが正しく消去されない状態になる可能性がある。このため、管理用監視システムは、多重ログオンを検知した場合ログオン先それぞれの PC の稼動確認を行い、応答がないものは UNIX 上のファイルサーバの接続プロセスを強制終了させる機能を有している。

```
==============================
USER-ID: user1
PC-NAME: c37-x1 c37-x2
user1 NB N(c37-x1<00>/1/1)1105 Wed Jan 10 11:33:15 2001
user1 NB N(c37-x2<00>/1/1)1142 Wed Jan 10 11:29:55 2001
------------------------------
Login name: user1    In real life: user1_user1
Directory: /homexx/user1              Shell: /bin/csh
Never logged in.
No unread mail
------------------------------
DNS:
Name:     c37-x1.pc.reitaku-u.ac.jp
Address:  157.17.37.xx
Name:     c37-x2.pc.reitaku-u.ac.jp
Address:  157.17.37.yy
------------------------------
PING:
c37-x1.pc.reitaku-u.ac.jp is alive
c37-x2.pc.reitaku-u.ac.jp is alive
------------------------------
user1:x:xxx:1110:user1_user,D0xx:/homexx/user1:/bin/csh
```

図 5 多重ログオン検知メール

4.3 システム運用結果

不正利用とみなされた多重ログオンについては、システム導入前の1ヶ月間は13件であった

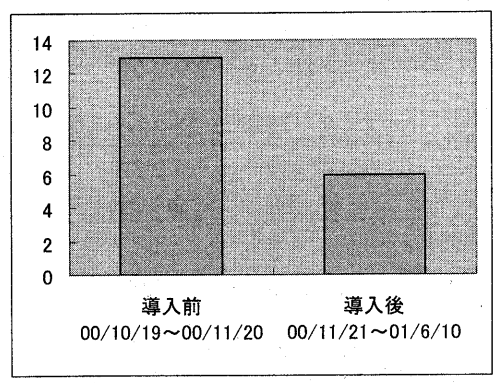

図 6 不正な多重ログオンの検出件数

のに対し、システム稼動後は約半年で6件と減少した。このことから、警告メッセージが有効に作用していることが示された（図6）。

4.4 実装上の問題点と対応

すでにのべたように、UNIXシステム側のプロセス異常終了により、シェルスクリプトが正常に動作しないことが考えられる。このため、UNIXシステムに残る異常なプロセスを削除する機能を有している。この機能は通常の ping を用いICMPの応答が無い状態をもってプロセス異常と判断するため、PC の電源が入っていれば多重ログオンと誤検出を行う。この点については、改善の余地を残している。

上記のようなケースは、ユーザからのサポート窓口への問い合わせや管理者宛て多重ログオン通知メールを分析することで発見される。管理者が該当PCの稼動状態を目視で確認を行い、必要に応じてファイルサーバ上のプロセスを手動で削除している。表2は、2001年4月1日から6月10日までの多重ログオン検知数である。

表2 多重ログオン検知件数

稼働日（2001/4/1～6/10）	54日
検知数	32件
有効検知	2件

サーバ上で接続中のユーザを順次照合するため、応答時間が長くなる可能性がある。表3は315台アクセス時のログオン完了時間の比較である。この結果では、ユーザが意識できるような増大は認められなかった。なお、これまでの実運用での最大同時アクセス数は364台である。

表3 ログオン完了時間の比較（315台稼動時）[10]

	スクリプトなし（秒）	スクリプトあり（秒）
ログオン完了時間	18	18.8

[10] 315台接続中の同一クライアントでの10回の測定の平均値。ただし、ファイルサーバは他の処理サービスも行うため、負荷状況によって、測定値は大きく異なる。

本システムではログオン時のチェックにはリモートシェルを利用している。リモートシェルの許可はセキュリティ上の問題も多い。現在は、学外からのリモートシェルは禁止している。しかし、学内からは利用可能であるため悪用される危険性があり、検討が必要な部分となっている。

また、システムを運用した結果、警告メッセージの効果により利用規則違反者の数は減少したものの依然として違反がある。これは、本システムが多重ログオンを検知し、警告メッセージのみ表示する仕組みであることが原因であると考えられる。ログオフするかどうかはユーザの自主性に任せているため、メッセージを無視することも可能である。メッセージがでてもよく読まないまま閉じる不注意な行動を行うユーザも目立つ。また、全学生の約15%が外国人留学生であるため、日本語の読解能力次第ではメッセージの意味が読み取れないケースもある。

これらの問題点を考えると、メッセージを多言語で表示する工夫や多重ログオンを検知後、自動的にログオフする仕組みが有効である可能性も考えられ、今後の検討課題となっている。

5. まとめ

多重ログオンの抑制を低コストで実現可能な方法を提案し、実装評価を行なった。多重ログオンシステムの導入によって、利用マナーの改善を得ることができた。本研究では、その結果一定の効果を得ることができることを示し、アカウントの貸借に起因する不正な利用が減少することが示された。

参考文献

[1] 石橋勇,坂本晃,山井良,安倍広多,大西克実,松浦敏雄,情報コンセントにおける認証とアドレス偽造防止を VLAN 機能により実現するシステム, 分散システム/インターネット運用技術研報告, 99-DSM-14, 情報処理学会, pp.137-142(1999).

[2] 久保美和子, Windows ネットワークのセキュリティ対策 (1) - 多重ログオン抑止の一方策 -, 第13回KIUインターネット教育研究フォーラム・第2回TRAIN協会講演会,pp1-4(2001).