社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－ＤＳＭ－41（16）
2006／5／12

教育用Windows端末の利用者認証システム

佐藤 貴彦[†,††] 久保田真一郎[†††] 升屋 正人[†††]

†鹿児島大学工学部 〒890-0065 鹿児島市郡元 1-21-40
††奈良先端科学技術大学院大学情報科学研究科 〒630-0192 生駒市高山町 8916-5
†††鹿児島大学学術情報基盤センター 〒890-0065 鹿児島市郡元 1-21-35
E-mail: ††takahiko-s@is.naist.jp, †††{kubota,masatom}@cc.kagoshima-u.ac.jp

あらまし オペレーティングシステムとしてWindowsを使用する教育用Windows端末においては，Active Directoryを用いて認証を行うのが一般的である．また，運用管理の省力化のため環境復元ソフトウェアを導入することが多い．ところがこうした環境下では，学会開催時などに部外者に対して発行する臨時のアカウント管理が煩雑である．また，環境復元ソフトウェアにより再起動時にユーザープロファイルが削除されてしまい，その作成のためログオン処理に時間がかかるという問題も生じる．これらの問題を解決するため，Windowsの標準のログオン機構に替えて，ワンタイムパスワードとCIFSサーバを用いる独自の利用者認証機構を開発した．

キーワード Active Directory，環境復元ソフトソフトウェア，ワンタイムパスワード，CIFS，GINA

Development of Authentication System for Classroom Windows PCs

Takahiko SATO[†,††], Shinichiro KUBOTA[†††], and Masato MASUYA[†††]

† Faculty of Engineering, Kagoshima University 1-21-40, Korimoto, Kagoshima, 890-0065 Japan
†† Graduate School of Information Science, Nara Institute of Science and Technology 8916-5, Takayama-cho, Ikoma-City, Nara, 630-0192 Japan
††† Computing and Communications Center, Kagoshima University 1-21-35, Korimoto, Kagoshima, 890-0065 Japan
E-mail: ††takahiko-s@is.naist.jp, †††{kubota,masatom}@cc.kagoshima-u.ac.jp

Abstract Active Directory is generally used for the authentication system of classroom Windows PCs. And in many case, some recovery software is installed on classroom PCs. In this situation, Active Directory server maintenance and temporary account registrations are complicated, and user logon process is very time consuming because user profiles are deleted in each start-up process. In order to avoid these problems, we have developed our own authentication system for classroom Windows PCs using one-time password and CIFS authentication.

Key words Active Directory, recovery software, one-time password, CIFS, GINA

1. まえがき

大学をはじめとした教育機関の端末室やパソコン教室では，複数のパーソナルコンピュータを設置し，Windows XP Professionalをオペレーティングシステムとして動作させる場合が多い．簡単のため，本論文ではこうした機器を教育用Windows端末と呼ぶ．一般に教育用Windows端末では，ソフトウェアライセンスの適正な使用やネットワーク利用者の把握のため，認証の仕組みを用いて受講生や学生・教職員に利用者を制限する必要がある．多数の教育用Windows端末それぞれにユーザーアカウントを用意するのは難しいが，Windows Server 2003が標準で搭載しているディレクトリサービスであるActiveDirectoryを用いたユーザーアカウントの一元的な管理を行うのが一般的である．

一方，教育用Windows端末には，授業利用時の環境の統一や許可のないソフトウェアのインストールを防ぐ目的で環境復元ソフトウェア（[1]～[3]など）を導入することが多い．環境復元ソフトウェアは，再起動時にハードディスクの内容をあらかじめ設定した状態に初期化する機能を持ったソフトウェアで，書き込まれたデータが保存されないため個人情報の保護やセキュリティ対策にも有効である．

ところが，Active Directoryと環境復元ソフトウェアを組み合わせた教育用Windows端末の運用に際しては，２つの問題がある．一つは，一時的な利用者に対するアカウント発行処理

が簡単でないことである．学生や教職員などの在籍者に対しては名簿データなどに基づいたアカウント発行処理を年に一度程度行えばよい．しかし，大学においては講習会や学会・研究会などの在籍者ではない参加者に対して臨時のアカウントを発行する必要が多く発生する．複数の臨時アカウントをあらかじめ準備しておくことも考えられるが，利用可能な期限を講習会や学会ごとに設定しなければならず，アカウントの新規発行と手間は変わらない．このため，一人のユーザーアカウントを複数の教育用 Windows 端末で共有するという不適切な利用が行われてしまう場合もある．

もう一つは，環境復元ソフトウェアによりユーザープロファイルが削除されるため，ログオン処理に時間がかかることである．ユーザープロファイルとは Windows においてユーザーごとに用意されるフォルダで，辞書，ドキュメント，ソフトウェアの環境設定データなど，ユーザーごとに異なるデータを保持している．インストールしているソフトウェアの数や種類により異なるが，最低でも数十 MB の容量となることが多い．Active Directory による認証と組み合わせることで，どの端末でも同じ環境で作業できる．しかし，ユーザープロファイルをサーバに保持する“移動プロファイル”や“固定プロファイル”は，導入ソフトウェアが異なる環境に対応できないことや，ファイル転送に時間がかかりすぎログオン処理に長時間を要するため数十台から数百台規模の教育用 Windows 端末を設置する環境で用いることは適切でない．一方，ファイル転送を伴わない“ローカルユーザープロファイル”であっても，ログオンの度にあらかじめ準備されたデフォルトユーザープロファイルをコピーしてユーザープロファイルを作成する必要があるためログオン処理に時間がかかることになる．環境復元ソフトウェアが導入されていなければ，初回のログオン以外は Windows XP Professional を導入したパーソナルコンピュータを個人で使用している場合とログオン処理に要する時間は同等で問題とはならない．しかし，毎回同じ機器を使用するとは限らず，特に環境復元ソフトウェアを導入している場合はすべての端末でログオンの度にユーザープロファイルのコピーが発生し，ログオン処理に時間がかかることになる．

一元的なユーザー管理と授業利用時の利便性，セキュリティなどを考えれば Active Directory と環境復元ソフトウェアの組み合わせは教育用 Windows 端末にとって不可欠なもので，Windows のログオン認証の仕組みに起因するこれら２つの問題は避けがたい．もちろん，教育用端末に Mac OS X や Linux，Solaris など Windows 以外のオペレーティングシステムを導入し，ターミナルサービスの仕組みを用いてリモートデスクトップ接続により Windows Server 2003 を共用すればこれらの問題は発生しない．教育用端末をシンクライアントとする方法である．しかし，多数のユーザーの同時使用に耐えうる性能の高いサーバ機器が別途必要になり，各端末の CPU 資源を有効に活用できないほか，ソフトウェアによってはターミナルサービスでの動作を保証していないものも存在している．運用管理の手間やコストまで考えれば，Active Directory と環境復元ソフトウェアを用いて教育用端末群を構築するのが多くの教育機関にとって妥当であると思う．

教育用 Windows 端末の認証システムに必要なのは，使用が許可されていない者の使用を許さないことである．環境復元ソフトウェア存在下での個々のユーザーの環境やデータの保持はログオン認証とは独立に Common Internet File System (CIFS) プロトコルを用いたファイル共有（Windows ファイル共有）により実現でき，ユーザープロファイルのコピーを伴う Active Directory を使ったユーザー環境の保持は必須ではない．もちろん，Windows に標準で搭載されているログオン認証の仕組みを用いる限り，ローカルアカウントに対する認証以外は Active Directory を使用せざるを得ないが，Windows のログオン認証機構は独自のものに入れ替えることができるようになっている．たとえば，スマートカードなどハードウェアをキーとした認証はログオン認証機構を入れ替えることで実現されている．そこで本研究では，ワンタイムパスワード認証の仕組みと CIFS プロトコルを用いた認証の仕組みをあわせ持つ独自の認証機構を Windows に組み込むことで，Active Directory を用いずユーザープロファイルの作成を伴わないログオンを実現することにした．これにより，Active Directory と環境復元ソフトウェアに起因する２つの問題の回避が可能となる．

2. Windows のログオン機構

Windows XP Professional の認証機構は実行ファイルである `Winlogon`（ファイル名は `winlogon.exe`）と `Winlogon` から呼び出される DLL (Dynamic Link Library) である `GINA` (Graphical Identification and Authentication，ファイル名は `msgina.dll`）によって実現されている．Windows NT，Windows 2000 についても同様である．`Winlogon` と `GINA` は相互に呼び出しを行って認証処理を行う．手順は以下の通りである [4], [5].

（1） Windows が起動すると `Winlogon` が `GINA` の `WlxNegotiate` 関数を呼び出し，`GINA` に `Winlogon` のバージョンを通知する．

（2） `Winlogon` が `GINA` の `WlxInitialize` 関数を呼び出し，`Winlogon` の関数のアドレスや `Winlogon` のハンドルを通知するとともに，`GINA` の `WlxDisplaySASNotice` 関数を呼び出して CTRL+ALT+DEL キーを押すよう求める画面を表示する．このとき，`GINA` は SAS (Secure Attention Sequence) イベントの待ち受け状態に入る．SAS イベントは標準では CTRL+ALT+DEL キーの同時押下により発生する．

（3） CTRL+ALT+DEL キーを同時に押すことにより，SAS イベントが発生すると `GINA` は `Winlogon` の `WlxSasNotify` 関数を呼び出す．すると `Winlogon` は `GINA` 中で認証を直接担当している `WlxLoggedOutSAS` 関数を呼び出し，`GINA` の認証機構を起動する．ユーザー名とパスワードの入力を求める対話的なログオン認証画面（図 1）はここで `GINA` により表示される．ドメインのメンバとなり Active Directory を使用する場合は，ドメイン名を指定するため「ログオン先」を選択するリストボックスが図 1 のダイアログに追加される．認証の結果は `WlxLoggedOutSAS` 関数の戻り値として `Winlogon` に戻される．

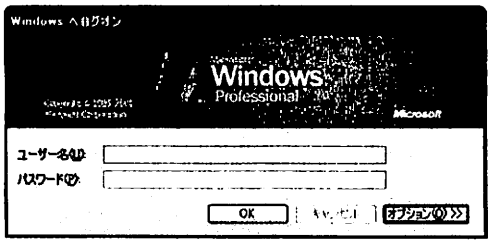

図1 GINA による対話的なログオン認証ダイアログ
Fig. 1 Interactive authentication dialog displayed by GINA.

ログオンに成功した場合は WLX_SAS_ACTION_LOGON，失敗したりログオンをキャンセルした場合は WLX_SAS_ACTION_NONE，シャットダウンを要求した場合は WLX_SAS_ACTION_SHUTDOWN が戻されることになる．

(4) ログオンに成功し，WLX_SAS_ACTION_LOGON が戻された場合は GINA の WlxActivateUserShell 関数が呼び出され，認証後の処理が開始される．このとき，ユーザープロファイルが存在しないユーザーである場合には，そのコピーが行われることになる．

以上の手順の中で，実際のログオン認証は WlxLoggedOutSAS 関数の内部で行われる．したがって，Winlogon と GINA により実現されている Windows の認証機構を独自のものに変更するには，GINA の関数である WlxLoggedOutSAS 関数を独自のものに変更すればよいことになる．

3. 本システムのログオン機構

本研究では，GINA の WlxLoggedOutSAS 関数の変更により，Active Directory と環境復元ソフトウェアを組み合わせて教育用 Windows 端末を運用管理する場合に生じる２つの問題の解決を図った．一時的な利用者に対するアカウント発行処理の困難さの問題は，Active Directory とは独立したワンタイムパスワード認証機構を WlxLoggedOutSAS 関数に追加することで解決した．プロファイルのコピーが原因のログオン処理に時間がかかる問題は，Active Directory を使った認証ではなく，CIFS サーバに対するファイル共有要求の成否による独自の認証機構を WlxLoggedOutSAS 関数に追加することで解決した．

3.1 GINA を入れ替える方法

独自の GINA を作成する場合には，オリジナルの GINA が持つすべての関数を用意する必要がある．しかし，本研究では WlxLoggedOutSAS 関数の変更を行うだけでよく，他の関数については標準のものをそのまま利用したい．そこで，Platform SDK for Windows XP SP2 [6] に含まれているサンプルコード，GinaStub を基に WlxLoggedOutSAS 関数の変更を行った独自の GINA を作成した．作成に当たっては，同じく Platform SDK for Windows XP SP2 [6] に含まれている GinaHook と文献 [5] に紹介されているサンプルコードも参照した．作成した独自の GINA を GinaStub.dll とすると，このファイルを%SystemRoot%\System32 ディレクトリにコピーし，レジストリ HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon に名前が GinaDLL，種類が REG_SZ，データが GinaStub.dll のキーを追加して Windows を再起動すれば，独自の GINA を有効にできる．

3.2 教育用 Windows 端末に用意するアカウント

本システムでは，個々の教育用 Windows 端末のアカウントと認証に用いるユーザーアカウントが独立しているため，その関係を独自に定義することができる．この特徴を利用して教育用 Windows 端末には以下の２つのユーザーアカウントのみを用意した．

(1) **Administrator**

教育用 Windows 端末の管理者権限を持ち，すべてのファイルの読み書きとすべてのアプリケーションの実行が可能なアカウント

(2) **Guest**

システムファイル等へのアクセスが制限され，部外者でも使用できるライセンス形態のアプリケーションのみ実行可能なアカウント

どちらのアカウントも Windows XP Professional に標準で用意されているが，**Guest** アカウントについては無効となっている．このため **Guest** アカウントを有効化するとともに，パスワードの設定，起動可能なアプリケーションの設定を事前に行った．独自の認証機構を用いるため，これら２つのアカウントとそれぞれに対するパスワードは独自の WlxLoggedOutSAS 関数のソースコード内に直接記述する．これらのパスワードが漏れたとしても，本システムではそれを用いてログオンすることはできないためセキュリティ上の脅威とはならないが，Windows XP Professional で使用可能な最大長のパスワードを設定し，パスワードの総当たり攻撃に対する耐性を最大とした．アカウント名も **Administrator**，**Guest** 以外のものに変更するのが適切で，実際に変更したが，簡単のため本論文では変更前の名称を用いる．

環境復元ソフトウェアにおける復元ポイント設定に先立って，**Administrator**，**Guest** でのログオンを一旦行っておくことで，両アカウントに対するユーザープロファイルが作成される．その後復元ポイントを設定すれば，**Administrator**，**Guest**，どちらかのアカウントでログオンする限り，ユーザープロファイルのコピーは発生せず，ログオン処理を短時間で終えることが可能となる．

3.2.1 Administrator アカウントでのログオン

あらかじめアカウントが用意されている学生や教職員などが本システムの認証機構において CIFS サーバを用いたユーザー認証に成功した場合，教育用 Windows 端末に対しては **Administrator** アカウントでログオンさせる．これにより，使用者は常に教育用 Windows 端末の管理者権限を持つことになる．

環境復元ソフトウェアが導入されている環境では，すべてのユーザーがオペレーティングシステムの管理者権限を持っていても，環境復元ソフトウェアの管理パスワードや BIOS パスワードを知られない限りシステム破壊の危険性は無い．Windows 用のソフトウェアの中には一般ユーザーの権限では動作しない

ソフトウェアもあるほか，システム領域への書き込みが必要なWebブラウザのプラグイン等も多い．授業に必要なソフトウェアを臨時に導入したい場合もある．すべてのユーザーが管理者権限を持つことで，ファイルやフォルダのアクセス権に関わるこれらの問題を完全に解消できることになる．

また，Windowsでは一般ユーザーが管理者権限でプログラムを動作できるセキュリティ上の欠陥が時折発見されるが，管理者権限を持つユーザーに関して言えばこれは欠陥ではない．このため，緊急レベルとされるセキュリティ修正プログラムであっても適用する必要がない場合が多く，運用管理コストの削減もできることになる．

3.2.2 Guestアカウントでのログオン

本システムの認証機構においてワンタイムパスワードによる認証に成功した一時的な利用者はGuestアカウントでログオンさせる．これは学会や研究会などの開催に際して，教育用Windows端末をインターネット端末として利用させる場合や，アカウントを準備する期間のない臨時利用を想定している．

学会や研究会の多数の不特定の参加者に対して事前に個別のアカウントを発行するのは不可能である．学会・研究会当日に申請・発行するとなると業務の煩雑さは計り知れない．利用者を特定しない多数の期日指定のアカウントを事前に発行して学会事務局に事前に渡すなどして対応するのが現実的であるが，利用者を特定しないのであればアカウントを複数準備することに意味はない．運用ポリシーに反するかもしれないが，一つのアカウントを共用させる場合が多いように思う．アカウントの準備が間に合わない場合も同様にあらかじめ準備してあるアカウントで対応する場合が多い．

しかし，部外者に使用させることができないソフトウェアが導入されている場合に学内の利用者と同じ権限を与えるのは適切ではない．また，学内の情報システムのシングルサインオン化が進展している場合には，一つのアカウントでログオンできるシステムが多岐にわたり，部外者に利用させるのが適切でないシステムが存在する可能性がある．これらのような場合には，使用可能なアプリケーションやログオン可能なシステムを限定するなどの措置も必要となり，臨時のアカウントの運用管理に高いコストがかかることになる．

臨時利用させる場合にワンタイムパスワードによる認証を行ってGuestアカウントでログオンさせる本システムであればアカウント管理のコストはかからず，利用者ごとのアクセス制御も必要ない．Guestアカウントは各教育用Windows端末ごとに用意するので，ソフトウェア構成が異なる複数の教育用Windows端末を有する場合にも対応できる．また，CIFSサーバを用いたユーザー認証に成功したユーザーであっても，ユーザーIDに特定の文字を含む場合にGuestアカウントでログオンさせるような制御を行うことが容易である．教育用Windows端末の使用は制限するが同じユーザーアカウントを用いる他のサービスは利用させる，といった運用ポリシーの適用も可能である．

3.3 Active Directoryを使用しない利点

Active Directoryを使用しないことで，個々の教育用Windows端末をドメインに参加させる操作が不要となる．複数の教育用Windows端末に同じソフトウェアを導入する場合，もっとも単純で確実な作業方法は一台の端末のハードディスクをコピーすることである．ところがこの場合，各端末が独立して持つべきセキュリティ識別子（SID）も同じになってしまい，2台目以降がドメインに参加できない．このため，コピーした後にSIDを1台ずつ変更する作業が必要となる．環境復元ソフトウェアや環境を複製するソフトウェアの中にはこの機能を持つものもあるが，別途導入するとなると追加の費用が必要となる．ドメインに参加させる操作が不要であればSIDの変更作業が不要となり，教育用Windows端末の運用管理コストを削減できることになる．

3.4 ワンタイムパスワードによる認証機構

ワンタイムパスワードは一回または一定時間だけ有効なパスワードで，実装する方法には，チャレンジレスポンス方式や時刻同期方式などがある．チャレンジレスポンス方式の実装には，S/Key [7] が使われることが多い．一方，時刻同期方式のワンタイムパスワード認証の応用例としてはSecureID [8] が代表的で，インターネットバンキングでも活用されている．

本システムでは，臨時利用に対してワンタイムパスワードを用いるため，一定時間経過後はパスワードが無効になる時刻同期式が最適である．すでにSecureID [8] などで時刻同期式ワンタイムパスワードをWindowsログオンに用いる仕組みは実現されているが，導入には費用がかかり，本システムのように環境復元ソフトウェアの存在を意識したものではないため，必ずしも教育用Windows端末で利用できるものではない．そこで本研究では独自の時刻同期式ワンタイムパスワードの仕組みを開発して用いることにした．

本システムでは，時刻同期式ワンタイムパスワードの生成を以下の手順で行う．

（1） 日付と時刻にPINコードを付加した文字列をシード文字列とする

たとえば，2006年5月11日の場合は，"06/05/11" にPINコードを付加した文字列をシード文字列，同日14時の場合には "06/05/11 14" にPINコードを付加した文字列をシード文字列とする．

（2） シード文字列の128bit MD5ハッシュ [9] を求める

（3） MD5ハッシュをあらかじめ用意する16進-ASCII変換テーブル (表1) により16文字のASCII文字列に置換する

キーボードで直接入力可能なASCII文字列の数は限られているため，変換テーブルではすべての文字が2回以上出現する．これによりパスワードの強度が低下するが，使用可能な期間が限定されていることと教育用Windows端末のログオン認証にしか用いられないことを考えれば強度は十分であると考える．PINコードとこの変換テーブルを同時に知らない限り，MD5ハッシュによりパスワードを生成していることを知ってもパスワードの再現は極めて困難である．

PINコードと変換テーブルはパスワードを生成する側と解読する側で共通に持つ必要がある．本システムでは，パスワード生成器をPDA上に実装した（図2）．使用したPDAはWindows

表1 16進-ASCII変換テーブルの例
Table 1 Example of hex-ascii conversion table.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
2	w	x	y	z	A	B	C	D	E	F	G	H	I	J	K	L
3	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	!	"
4	#	$	%	&	'	(	)	=	~	|	-	^	\	@	[	'
5	{	;	:	]	+	*	}	,	.	/	<	>	?	_	a	b
6	c	d	e	f	0	1	2	3	4	5	6	7	8	9	a	b
7	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
8	s	t	u	v	w	x	y	z	A	B	C	D	E	F	G	H
9	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
A	Y	Z	!	"	#	$	%	&	'	(	)	=	~	|	-	^
B	\	@	[	'	|	;	:	]	+	*	}	,	.	/	<	>
C	?	_	a	b	c	d	e	f	0	1	2	3	4	5	6	7
D	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n
E	o	p	q	r	s	t	u	v	w	x	y	z	A	B	C	D
F	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

Mobile 5.0を搭載したシャープ社製W-ZERO3である．

パスワード生成器をソフトウェアとして公開すると暗号解読の危険性が高まるが，実装したPDAを貸し出すことによってのみパスワード生成を行わせれば秘匿性は高まる．また，本システムではパスワード生成に際しても，管理パスワードを要求するようにすることでさらに秘匿性を高めている．パスワード生成を多く行う必要がある場合には，認証機能付きWebアプリケーションとしてパスワード生成器を実装し，Webブラウザや携帯電話からの利用を実現することもできる．

3.5 CIFSを用いた認証機構

本システムでは，ワンタイムパスワードによる臨時利用以外は，CIFSサーバに対するファイル共有要求の成否によりログオン認証を行う．CIFSサーバとしては，Windows Server 2003はもちろん，CIFSプロトコルに対応した大容量ストレージシステムやLinuxなどで実現可能なSambaサーバを利用できる．これらのCIFSサーバは，自身がユーザーアカウントを持つことができるほか，外部のActive Directoryサーバ，NISサーバ，RADIUSサーバ，LDAPサーバなどと連携できることが多い．本システムでは間接的にこれらの認証サービスを利用できることになる．これらの認証サービスを直接利用するよう独自の認証システムを構築することも不可能ではないが，教育用Windows端末では，各ユーザーのファイル保存領域としてCIFSサーバのディレクトリをマウントすることが多い．ログオン認証時にCIFSサーバのディレクトリをマウントしても，ユーザーの権限が異なるためログオン後の利用はできないが，CIFSサーバに対するファイル共有アクセスの可否の確認のみを行うことで利用者認証を実現することが可能である．

図2 PDA上でのワンタイムパスワード発行．
Fig. 2 One-time password generation on PDA.

CIFSサーバに対するファイル共有アクセスには，Windows XP Professionalに標準で付属しているnetコマンドを以下の構文で用いる．

net use \\コンピュータ名\共有名 パスワード /user:ユーザー名

コンピュータ名はCIFSサーバのホスト名，共有名はCIFSサーバで設定されている共有ディレクトリの名称，ユーザー名とパスワードには認証の対象となるユーザーアカウント名とそれに対するパスワードを指定する．

CIFSサーバに対するアクセスが成功した場合，netコマンドは「コマンドは正常に終了しました。」と表示し，環境変数%ERRORLEVEL%に「0」を戻す．パスワードを間違えた場合には，「システム エラー 1326 が発生しました。」と表示し，環境変数%ERRORLEVEL%に「2」を戻す．その他アクセスに失敗した場合にも環境変数%ERRORLEVEL%に「2」が戻されるため，この値が「0」かどうかでCIFSサーバに対するファイル要求の成否を判断できる．これを用いて認証を行うことで，Active Directoryの仕組みを使わない認証を実現できる．確認後はnet use \\コンピュータ名\共有名 /deleteとして，CIFSサーバへの接続を一旦遮断する．ログオン処理に当たってWlxLoggedOutSAS関数から入手したユーザーIDとパスワードの情報をあらためて使用することで，共有ディレクトリのマウントを実現することができる．

Active Directoryで管理されているWindows Server 2003でファイル共有が実現されている場合であっても，この方法を用いることで教育用Windows端末の認証をActive Directoryから分離させ，あらかじめ用意しているAdministratorアカウントでログオンさせることが可能となる．これにより，ユーザープロファイルのコピーによりログオン処理に時間がかかる問題は発生しない．

ファイル共有を行わない場合であっても，Sambaをサーバとすることで Linux 上のアカウントを利用し認証を実現でき，ユーザーアカウントの管理に必要なサーバの維持管理コストを低く抑えることができる．

3.6 本システムの認証ダイアログ

本システムの認証ダイアログを図3に示す．Active Directoryを使用しないため，「ログオン先」を選択するリストボックスは無い．CIFSサーバへの接続要求は独自に作成したGINAのWlxLoggedOutSAS関数の内部で行われる．Windows標準のログオンダイアログとは異なり「一時利用」ボタンを追加している．このボタンをクリックすると，入力したユーザー名とパスワードに対してワンタイムパスワード認証を実行する．ワンタ

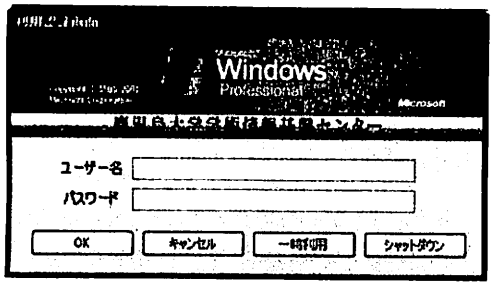

図3 本システムの対話的なログオン認証ダイアログ
Fig. 3 Our new interactive authentication dialog.

イムパスワードは3.4で述べた方法で生成するが，ユーザー名としては，日付のみをシード文字列としたパスワードに対しては"day"，時刻（時）までをシード文字列としたパスワードに対しては"hour"を用いることにした．

3.7 本システムのログオン認証の流れ

本システムのログオン認証の流れを図4に示す．ユーザーIDとパスワードを入力した後，「OK」ボタン，「一時利用」ボタンのどちらがクリックされたかによって処理が分岐する．「OK」ボタンがクリックされた場合は，CIFSサーバに対するファイル共有の成否を確認し，net useコマンドが成功した場合に，**Administrator**アカウントで教育用Windows端末にログオンする．CIFSサーバ自身がアカウントを持っていてもよいが，外部の認証サーバと連携可能なCIFSサーバであればActive Directoryサーバや RADIUSサーバをアカウントの一元管理に利用できる．「一時利用」ボタンがクリックされた場合は，MD5ハッシュと16進-ASCII変換テーブルにより生成したパスワードとの比較を行い，一致した場合には**Guest**アカウントで教育用Windows端末にログオンする．CIFSサーバを用いた認証の場合も，ユーザーIDによっては**Guest**アカウントでログオンさせることも可能である．

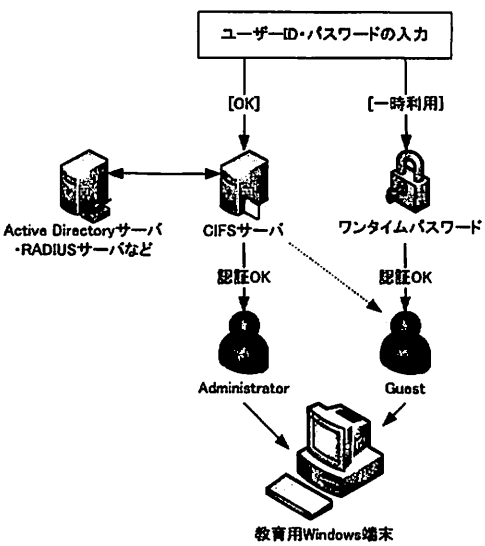

図4 本システムのログオン認証の流れ
Fig. 4 Flowchart of our authentication system.

3.8 ログオン処理に要する時間

鹿児島大学学術情報基盤センターの教育用Windows端末においては，Active Directoryを用いたログオン処理に1分30秒要している．この時間のほとんどはデフォルトユーザープロファイルをコピーする時間であると考えられる．本システムのログオン認証機構を同じ教育用Windows端末に導入し，ログオン処理に要する時間を測定したところ10秒で処理が終了した．本システムでは各教育用Windows端末に用意されているローカルアカウントにログオンすることになるため，ワンタイムパスワードを用いる場合とCIFSサーバに対するファイル共有の成否による認証でこの時間に違いはない．

4. まとめと考察

本研究では，Active Directoryと環境復元ソフトウェアを用いて教育用Windows端末を運用管理する上で問題となる，臨時アカウント発行と長いログオン処理の2つの問題を，独自の認証機構をWindowsに組み込むことで解決した．教育用Windows端末を対象とした類似の試みはこれまで行われたことがなく，本システムは多くの教育機関での運用管理の問題を解決できるものと思う．

本システムは特に，すべての教育用Windows端末が同一機種・同一構成ではない，大規模な教育用計算機システムの運用管理に有効である．たとえば鹿児島大学学術情報基盤センターが運用管理する教育用計算機システムは，361台のデスクトップ型教育用Windows端末と464台のノート型教育用Windows端末，さらに数十台の仕様の異なるデスクトップ型教育用Windows端末から構成されている．現在のところ，このうちデスクトップ型教育用Windows端末にのみ本システムを導入して実用可能性の検証を行っている段階であるが，近いうちにすべての教育用Windows端末に導入し，本格的に運用する予定である．

文　献

[1] 富士通四国システムズ，"瞬快，" http://jp.fujitsu.com/group/shikoku/services/packages/shunkai/
[2] トーエイ工業，"HDD KEEPER，" http://www.to-ei.co.jp/Av/sof/index.html
[3] アイ・ディ・ケイ，"ドライブシールド，" http://www.idk.co.jp/products/PCprotecttool/index.html
[4] K. Brown, "Security Briefs: Customizing GINA, Part1," MSDN Magazine, May, 2005. http://msdn.microsoft.com/msdnmag/issues/05/05/SecurityBriefs/
[5] K. Brown, "Security Briefs: Customizing GINA, Part2," MSDN Magazine, June, 2005. http://msdn.microsoft.com/msdnmag/issues/05/06/SecurityBriefs/
[6] Microsoft, "Platform SDK for Windows XP SP2," http://www.microsoft.com/msdownload/platformsdk/sdkupdate/XPSP2FULLInstall.htm
[7] N. Haller, "The S/Key One-Time Password System," RFC 1760, Feb, 1995.
[8] RSA セキュリティ，"SecureID", http://www.rsasecurity.co.jp/products/securid/index.html
[9] R. Rivest, "The MD5 Message-Digest Algorithm," RFC 1321, Apr, 1992.