美作女子大学・美作女子大学短期大学部紀要
2001, Vol. 46, 57～70

論　文

Windows 95 / 98におけるシステムポリシーについての一考察 I
－ZAKの活用－
A Study of System Policy on Windows 95 / 98 (I) : The Application of Zero Administration Kit

長谷川　勝　一

はじめに

先行研究[1) 2)]において，本学の学内LANを例にあげ，電子メール環境の構築に関連した特有のノウハウについて検討を試みた。

パーソナル・コンピュータ（以下PC）用OS（Operating System）として普及したMicrosoft Windows 95とその後継OSであるWindows 98[3)]の移動プロファイルを利用することで，個々の電子メール環境の設定を管理し，不特定多数のユーザーが同じく不特定多数のネットワーク端末としてのＰＣを共有して利用することができる。

本論では，先行研究において取り上げた，Windows NT Serverをサーバー，Windows 95 / 98をクライアントとしたC/S（Client－Server）環境における移動プロファイル利用時の問題点[4)]について，より安全な構築のための検討を行うことを目的とする。

Zero Administration Kit

Windows 95 / 98はローカルディスクに保存した情報に対するセキュリティが基本的に欠けているため，標準設定のままでは問題が発生する可能性が高い。システム設定の変更やアプリケーションの勝手なインストールあるいはアンインストール，ローカルディスク中のディレクトリやファイルへの変更や削除に対する有効な対策手段はOSの機能として用意されていない。

不特定多数のユーザーがPCを共同利用する環境では，一人が設定を変更したことにより他の多くのユーザーが迷惑を被るということは十分考えられる。

また，情報処理教室のように多数のPCを一括して，かつ同一条件に管理・維持しなければならない環境では，そのメンテナンスに必要な労力と時間は膨大なものとなる。

さらに，Windows 95 / 98のユーザーインターフェースは必ずしも初心者にとって優しいというものではない。多彩なプログラムメニューは，どのアプリケーションを選択すべきかという時点ですでに余計な判断をユーザーに要求することになる。デスクトップには様々なアイコンが並び，それらをすべて把握しなければならないような強迫観念を覚えるユーザーもいる。初心者にとってはシンプルな操作性が一番重要なことであるのに，Windows OSはユーザーを惑わすように様々な機能を盛り込もうとする。

この問題により発生するコストは規模が大きくなるにつれ膨大なものとなる。企業であれば業務に対する，教育機関であれば教育に対する効率が低下する。この問題に対する懸念はＯＳの開発・発売元であるMicrosoft社でも十分に認知しており，この問題を改善するためのツールがいくつか用意されている。

本論では，そうしたツールの代表的なものである，Zero Administration Kit（以下ZAK）の導入を中心に検討を加えることにしよう。

ZAKはMicrosoft社から無償で提供されているツールであり，現在，Windows NT用とWindows 95用が公開されている。希望者はMicrosoft社のWWWからのダウンロードもしくはCD-ROMの購入によってツールを入手することができる。今回検討を加えたのはZero Administration Kit for Microsoft Windows 95 Version 1.0である。

ZAKのセットアップに際しWindows 95のCD-ROMが必要となるが，ZAKのシステム自体はWindows 98にも対応している。本論では紛らわしいので論考に際しては基本的にWindows 95での環境構築に関する記載とし，ZAKの導入によるWindows 95とWindows 98での相違点についてはまとめて後述する。

ZAKの検討を行うために，テスト用のWindowsドメインを立ち上げた。ZAKに含まれるマニュアル（以下管理者ガイド）[5]にインストールに関する詳細な情報が掲載されているので，運用にあたっては熟読することが必要である。管理者ガイドによると，ZAKシステムの評価に必要なリソースは以下の通りである。[6]

必要なネットワーク構成

- Windows NT Server Version 4.0を実行する1台のコンピュータ。
- Windows 95を実行できる2台のコンピュータ。
- すべてのコンピュータがTCP/IPを実行していなければならない。

必要なサーバー環境

- プライマリドメインコントローラ（PDC）。
- 1GB以上の空き領域のあるハードディスク。
- 32MB以上のRAM（Microsoft Exchangeを使う場合は64MB）。
- CD-ROMドライブ。
- Windows NT Server Version 4.0とService Pack 3。
- ファイルシステムはNTFSであること。

必要なワークステーション構成

- 可能な限りハードウェア構成が似ていること。
- 486以上のプロセッサ。
- 16MB以上のRAM。
- 500MB以上の空き領域のあるハードディスク。
- MS-DOSのネットワーク起動ディスク。

その他の要件

- Zero Administration Kit for Windows 95 CD-ROM。
- Windows 95（完全な製品バージョン）。
- Windows 95 Service Pack 1。
- インターネットエクスプローラ管理者キット（IEAK）。
- Office 97。
- 『Microsoft Windows 95 リソースキット』。
- 『Microsoft Office 97 リソースキット』。
- Exchange Server 4.5（Outlookクライアントを Exchangeでテストする場合）。

なお，ZAKには以下の4点の機能がある。

- システムポリシーによるユーザーインターフェースの統一
- システムポリシーによるプロファイル情報の統一
- ZAKクライアントでのWindows 95およびOffice 97の自動セットアップ[7]
- ZAKクライアントでのOffice 97ネットワーク共有[8]

このうち，本論ではシステムポリシーによるユーザーインターフェースの統一およびプロファイル情報の統一に限って検討を加える。

上記の内容を評価するためのテスト環境として，以下のコンピュータを用意した。なお，すべてのコンピュータはネットワークに接続されている。

- Windows NT Server Version 4.0 （Service Pack 6a）を実行する1台のコンピュータ。
- Windows 95 OEM Service Relese 2（OSR2）[9]を実行する1台のコンピュータ。
- Windows 98 Second Edition（SE）[10]を実行する1台のコンピュータ。

ZAKのインストール

ZAKは管理者ガイドの指示にしたがって作業を行うことでインストールができるように配慮されている。インストーラーは残念ながら英語表記であるが，管理者ガイドは日本語化されている。Windows NT Serverの管理経験がある人間であれば，注意深く管理者ガイドを読みながら作業を進めることで問題なくセットアップは終了すると思われる。しかしながら，管理者ガイドの記述はZAKのフルセットアップを想定したものであり，ZAKクライアントへのWindows 95およびOffice 97の自動セットアップに関する情報も含まれている。また，一部明らかなミスや改善すべき点があるため，以下に簡単にセットアップ手順を説明し，修正すべき点については詳しく記述することとする。

PDCとなるサーバーの構成としては，先行研究[11]と同様に，コンピュータ名としてNtsrv1，Microsoftネットワークにおけるドメイン名としてsakuraを使用した。C:¥にシステムをインストールしており，D:¥にはあらかじめUsersとHomeというディレクトリを作成，それぞれUSERS$とHOMEという名称で共有（共有権はEveryoneに対してフルコントロール）している。なお，いずれのディレクトリもアクセス権はEveryoneに対して読み取り，Administratorに対してフルコントロールを設定しているものとする。サーバー上での作業はすべてAdministratorのユーザー権限で行った。

1. Zero Administration Kit for Windows 95 CD-ROMをPDCにセットし，CD-ROMのルートディレクトリにあるZAKSETUP.EXEをダブルクリックする。
2. ZAKの配付ポイントを指定する。デフォルト設定のC:¥ZAK95のままでよい。確認後［次へ］をクリックする。
3. ZAKに必要なディレクトリの作成を指定する。ここもデフォルト設定のC:¥ZAK95¥Setupのままでよい。確認後［次へ］をクリックする。
4. Office 97をネットワーク上で配付，共有するための設定について選択する。共有する場合は“Yes, create a Microsoft Office 97 share”を選択する。今回はこの機能についての検討はしないので，“No, do not create a Microsoft Office 97 share”を選択した。確認後［次へ］をクリックする。
5. ZAKクライアント用のネットワーク起動ディスクの作成について確認がある。ネットワーク起動ディスクはZAKクライアントへのWindows 95の自動セットアップに利用するものであるが，今回はこの機能について検討しないために“No, do not create a boot disk.”を選択する。確認後［次へ］をクリックする。
6. ネットワークのドメイン名，ワークグループ名，パススルー認証エージェント名[12]を順次確認されるので，この例ではそれぞれsakuraを入力する。実際の入力にあたっては例示を各自の環境で使用するドメイン名等に読み替えること。確認後［次へ］をクリックする。なお，これらの項目はZAKクライアントへのWindows 95自動セットアップに利用するものであるため，今回の検討内容とは直接関係がない。
7. ZAKで使用するポリシーファイルおよびログオンスクリプトファイルの配付ポイントを指定する。この例では¥¥Ntsrv1¥NETLOGONとなる。Windows NT Serverを構築すればNETLOGONという共有名で共有ディレクトリが自動的に作成されており，これを利用する。確認後［次へ］をクリックする。
8. ZAKクライアントが使用するネットワークプリンタ名を指定する。各自の環境で使用するネットワークプリンタ名を入力し，確認後［次へ］をクリックする。なお，この項目もZAKクライアントへのWindows 95自動セットアップに利用するものであるため，今回の検討内容とは直接関係がない。
9. Exchangeをインストールしたサーバーを確認されるので，この例ではなにも加えず空欄のまま

［次へ］をクリックする。

10. ZAKクライアントに自動セットアップするWindows 95をインストールするディレクトリ名を指定するよう指示される。とくに変更する必要がなければデフォルト設定のC:¥Windowsのままでよい。確認後［次へ］をクリックする。なお，この項目もZAKクライアントへのWindows 95自動セットアップに利用するものであるため，今回の検討内容とは直接関係がない。
11. Windows 95のCD-ROMをPDCにセットし，［次へ］をクリックする。[13]
12. インターネットエクスプローラのMSIE*.EXEを指定するよう指示されるので，MSIE*.EXEがある場所を指定する。[14]
13. ZAKのセットアップが成功したことが告げられたら［完了］ボタンをクリックする。

以上でZAKのセットアップは終了である。この時点では，ZAKの運用に必要なポリシーファイルやログオンスクリプトファイルはPDCにコピーされていないので，最終的には必要なファイルをZero Administration Kit for Windows 95 CD-ROMからコピーする必要がある。コピーが必要なファイルについては後述する。

ZAKユーザーアカウントの作成

次いでPDCにZAKを利用するユーザーのアカウントを作成する。この手順についてもマニュアルに詳細な記述がある。[15]

1．ZAK用グローバルグループの追加

まずZAKユーザーが所属するグローバルグループを作成する。ZAK用として作成する必要があるものはAppUserとTaskUserである。ユーザーが複数のアプリケーションソフトウェアを使用する環境が必要なのであれば前者を，単独のアプリケーションソフトウェアのみを使用する環境でよければ後者を選択する。

ちなみに，AppUserが実現する環境をアプリケーションステーションモードと呼び，TaskUserが実現する環境をタスクステーションモードと呼ぶ。後者の場合はWindowsデスクトップインターフェースがユーザーから隠される。本論ではアプリケーションステーションモードでの使用を想定してユーザーを作成する。

1. PDCでドメインユーザーマネージャを起動し，［ユーザー］メニューの［新しいグローバルグループ］を選択する。
2. ［新しいグローバルグループ］ダイアログが表示されるので，［グループ名］のボックスにAppUserを入力する。［所属するメンバー］ボックスに既にユーザーまたはローカルグループが表示されている場合はそのアイコンをクリックし，［削除］ボタンをクリックする。すなわち，AppUserのグループにはこの段階ではユーザーもしくはローカルグループは一切含まれない。AppUserの設定が終了した後［OK］ボタンをクリックし，グループを追加する。
3. 同じ手順でTaskUserグループを作成する。

AppUserおよびTaskUserの名称はZAKのシステムから参照されることになるので，必ずAppUserおよびTaskUserという名称に設定する。

なお，管理者ガイドにはこの次の作業としてUsersディレクトリの共有について記載があるが，すでにPDC上にUsersという名称で作成している（共有名はUSERS$）ものとする。ただし管理者ガイドでは，Usersディレクトリに対しEveryoneグローバルグループにフルコントロールのアクセス権を設定する旨の指示があるが，これは危険であるので，本論では読み取りのアクセス権に変更する。

2．ZAKユーザーアカウントの作成

ユーザーアカウントの作成手順は以下の通りである。

1. PDCのドメインユーザーマネージャで［ユーザー］メニューの［新しいユーザー］を選択する。［新しいユーザー］ダイアログが表示される。
2. 新規アカウントのための情報を入力する。仮に，

   ユーザー名　z120001
   フルネーム　Mimasaka Hanako
   説明　ZAK AppUser
   パスワード　**仮パスワード**

   とする。
3. ［グループ］アイコンをクリックし，AppUserをユーザーが所属するグループに加える。タスクステーションモードのユーザーの場合はTaskUserを加える。設定後［OK］ボタンをクリックする。
4. ［新しいユーザー］ダイアログに戻るので，［プロファイル］アイコンをクリックし，必要な情報を入力する。仮に，

   ログオンスクリプト　APPLOGON.BAT
   ホームディレクトリ
   ドライブ　U:
   パス　¥¥Ntsrv1¥USERS$¥%username%

   とする。タスクステーションモードのユーザーの場合はログオンスクリプト名のボックスを空白のままにする。なお，ホームディレクトリボックスのNtsrv1の指定は各自の環境におけるPDCのサーバー名もしくは移動プロファイル情報を保存するサーバー名に読み替える必要がある。%username%はそのままの入力であるが，アカウント追加後，自動的にユーザー名が変数として代入される。設定後［OK］ボタンをクリックする。
5. ［新しいユーザー］ダイアログに戻るので，［追加］ボタンをクリックしてドメインにユーザーを追加する。以後，必要なユーザーを上記手順で繰り返し作成する。［ユーザー］メニューの［コピー］を利用すると，グループやプロファイルの情報がコピーされる。

管理者ガイドではこの後，ZAKクライアントの自動セットアップのためのZAKSETUPユーザーを作成する手順が記載されているが，本論では割愛する。

テスト環境の評価をするためにはいくつかのテストアカウントを作成しておいた方がよいので，同様の手順でz120002およびz120003も作成しておく。また，このユーザーのホームディレクトリとして，共有ディレクトリUSERS$内にそれぞれアカウント名のディレクトリが作成されていることを確認する。手作業でアカウントを作成した場合，このディレクトリのアクセス権はそのアカウントのユーザーに対してのみフルコントロールの設定になっているので，Administratorであってもディレクトリ内部を参照することはできない。管理上問題があるならば各ディレクトリ以下に対しAdministratorへの所有権およびアクセス権の取得を設定しておく。

共有名USERS$内の各ディレクトリは各ユーザーのホームディレクトリとしての扱いであるが，先行研究[16]でも指摘したように，実際にはWindows NTにおけるユーザープロファイル用ディレクトリとしての扱いを受けている。この領域にWindows 95の移動プロファイルデータが保存されるが，移動プロファイルデータにはユーザー用レジストリデータであるUSER.DATが含まれる。上記の先行研究では各ユーザーが作成，修正するファイルやディレクトリを保存する領域と，移動プロファイルデータを保存する領域を同じディレクトリとする設定を紹介したが，重要なファイルであるUSER.DATがユーザーの目に直接触れることは管理上好ましくない。[17] したがって，Windows NTのように移動プロファイルデータと各ユーザーの管理するデータを保存する領域は分けておいた方がより安全である。

そこであらかじめ用意しておいたPDC上のHOMEという共有ディレクトリ内に各ユーザーのディレクトリ名で新規にディレクトリを作成し，そちらを各ユーザーのホームディレクトリとする。手作業で作業する場合，このディレクトリはアクセス権としてAdministratorにフルコントロールが設定されている

が，各ユーザーのアクセス権もフルコントロールで追加することが必要である。

クライアントPCでの設定

次いでZAKを利用することになるPC側の設定について説明する。基本的には先行研究における設定[18]を踏襲することになる。すなわち，TCP/IPによる通信が可能で，Windowsドメインにネットワークログオンできることが前提である。また，移動プロファイルに対応するように設定する。

1．グループポリシー機能のインストール

ZAKのために新たに追加する設定としては，グループポリシーと呼ばれる機能をクライアント側に追加するため，GROUPPOL.DLLをインストールすることである。これはWindows 95のインストールCD-ROMを使用してインストールを行う。以下，作業手順を『Microsoft Windows 95 リソースキット』の「第15章 ユーザープロファイルとシステムポリシー」に沿って説明する。[19]

1. コントロールパネルの［アプリケーションの追加と削除］を選択し，［Windowsファイル］シートをクリックした後，［ディスク使用］ボタンをクリックする。
2. ［フロッピィディスクからインストール］ダイアログボックス内で［参照］ボタンをクリックし，Windows 95 CD-ROMの*%CD-ROM_Root%*¥ADMIN¥APPTOOLS¥POLEDIT指定し，［OK］ボタンを2回クリックする。
3. ［ディスクを使ったインストール］ダイアログボックス内で［グループポリシー］にチェックが入っていることを確認して［インストール］をクリックする。

以上の手順でGROUPPOL.DLLがクライアントPCの*%SystemRoot%*¥WINDOWS¥SYSTEMにインストールされ，レジストリに必要な変更が加えられる。グループポリシー機能のインストールはZAKを利用するすべてのクライアントPCで行う必要がある。

ポリシーファイルおよびログオンスクリプトファイルの作成

ここではZAKを運用するにあたって必要不可欠なポリシーファイルおよびログオンスクリプトファイルの作成について説明する。ポリシーテンプレートと呼ばれる，制限事項についてのレジストリキーや規定値についての情報を定められた方法により記述した[20]テキストファイル（*.ADM）をシステムポリシーエディタ（POLEDIT.EXE）上に読み込み，GUI環境上で適切な設定を加えることでポリシーファイル（*.POL）を作成する。ポリシーファイルはユーザーの操作環境や設定内容に一定のルールを強制することができる。

システムポリシーエディタでの作業は，編集できるキーがあらかじめ規定されているため，適切に作成されたポリシーテンプレートを使用する限りレジストリエディタ（REGEDIT.EXE）よりも自由度はないが安全性は高い。[21]

1．ポリシーファイルの作成

Windows 95 CD-ROMにはシステムポリシーエディタが付属しており，PCにインストールすることが可能であるが，Windows 95 CD-ROMに付属のシステムポリシーエディタを用いてはいけない。ZAKに付属のシステムポリシーエディタ[22]を使用する必要がある。ZAKでは複数のポリシーテンプレートファイルを読み込んで使用するが，この機能はZAKに付属のシステムポリシーエディタで実現されたものである。

また，Windows 95用のポリシーファイルを作成するためには，システムポリシーエディタをWindows 95で実行する必要がある。Windows NT環境で実行すると，Windows NT用のポリシーファイルが作成される。

ZAKに付属のシステムポリシーエディタはインストール作業を行う必要はなく，直接起動することで利用できる。[23]

ポリシーファイルの作成はクライアントPC上で作業する必要がある。したがって，ポリシーファイル作成用のPCを確保しておくことが望ましい。システムポリシーエディタはレジストリエディタよりも安全性が高いとはいえ，やはり無知なユーザーが利用するのは危険であるため，一般ユーザーが使用するPCにはインストールしない方がよい。

Windows 95 CD-ROMからシステムポリシーエディタのインストールを行っていないPCでは，最初にシステムポリシーエディタを起動した際に*%SystemRoot%*¥INFにポリシーテンプレートCOMMON.ADMがない旨警告されるが，これは無視してよい。[OK]をクリックするとポリシーテンプレートを指定するためのダイアログが表示されるので［キャンセル］をクリックする。

次いでZAK用に用意されたポリシーテンプレートをシステムポリシーエディタに読み込む必要がある。これはZero Administration Kit for Windows 95 CD-ROMの*%CD-ROM_Root%*¥POLICIESにあるファイルを使用する。これらのファイルは一般的に用いられるADMIN.ADMと，ZAK用に作成されたZAK95.ADM，インターネットエクスプローラ用のIEAK.ADM，Office 97用のOFF97W95.ADM，Access 97用のACCESS97.ADMからなっている。また，この他にも，各種リソースキットに含まれているポリシーテンプレート（*.ADM）ファイルを利用することができる。

Zero Administration Kit for Windows 95は，Windows 95というOSにOffice 97およびインターネットエクスプローラ3.0をインストールして使用する環境を前提に提供されているので，それ以後に提供されたポリシーテンプレートは含まれないが，使用することはできる。それぞれの環境に合わせてポリシーテンプレートを追加することで，より強固な環境を提供することができる。

本論ではZAK自体の評価を行うことを目的とするため，基本的なポリシーテンプレートであるADMIN.ADMとZAK95.ADMを用いるのみとしたが，実際の運用では各種応用アプリケーションソフトウェアを使用するのが一般的であるので，各自の環境で使用するソフトウェアにあわせ，必要なポリシーテンプレートを追加しておく。

ポリシーテンプレートの追加は以下の通りである。

1. システムポリシーエディタの［オプション］メニューから［ポリシーテンプレート］を選択する。
2. ［ポリシーテンプレートのオプション］ダイアログが表示されるので，［追加］をクリックしてZero Administration Kit for Windows 95 CD-ROMの*%CD-ROM_Root%*¥POLICIESにあるADMIN.ADMとZAK95.ADMをそれぞれ追加する。
3. ［ポリシーテンプレートのオプション］ダイアログの［OK］をクリックする。

次いで追加したポリシーテンプレートを利用してポリシーファイルを作成する。システムポリシーエディタの［ファイル］メニューから［新規作成］を選ぶことで新規のポリシーファイルを用意することができるが，これを使用してはいけない。［ポリシーを開く］を選択し，Zero Administration Kit for Windows 95 CD-ROMの*%CD-ROM_Root%*SCRIPTS¥CONFIG.POLを指定して，それを利用する。このファイルにはすでにZAK環境用にカスタマイズされた様々な設定が施されているので，一部分を修正し利用する。

システムポリシーエディタによりZAKのCONFIG.POLを開くと以下の項目のアイコンが表示される。それぞれのアイコンには基本的なポリシーがすでに設定してある。

- AppUser：AppUserに所属するユーザーが強制されるポリシー。
- Domain Admins：Domain Adminsに所属するユーザーが強制されるポリシー。管理者用である。

- TaskUser：TaskUserに所属するユーザーが強制されるポリシー。
- **既定のコンピュータ**：クライアントPCに強制されるポリシー。
- **既定のユーザー**：クライアントPCを利用するユーザーに強制されるポリシー。

「既定のコンピュータ」「既定のユーザー」という概念が難しいかもしれない。Microsoftネットワークログオンを用いてかつユーザープロファイルが使用可能になっている場合，クライアントであるWindows 95は所属するドメインのWindows NT Server上のNETLOGONディレクトリからCONFIG.POLという名称のポリシーファイルを自動的にダウンロードしようとする。[24] いずれかのユーザーがドメインにログオンした時点で，ポリシーファイルに指定された設定はレジストリのUSER.DATおよびSYSTEM.DATにコピーされ，以後その設定が有効となる。「既定のコンピュータ」のポリシーはクライアントPCのSYSTEM.DATに対するポリシー設定である。[25]

では「既定のユーザー」とはなにか。これはAppUser，TaskUser，Domain Adminsのいずれでもないユーザーに対して強制されるポリシーである。このポリシーはADMIN.ADMとZAK95.ADMのテンプレートを使用するため，AppUserやTaskUserのユーザーに対するポリシー項目と同じ項目がポリシーの対象としてあがっているが，初期設定では［Zero-Administration設定］の［安全なタスクマネージャーを使用］項目が［No］になっていることを除けば原則として制限を受けていない。修正を加えることで制限を強制することが可能である。

「Domain Admins」はDomain Adminsに所属するユーザーに対して強制されるポリシーである。このグループはWindows NT Serverのデフォルトグローバルグループとして作成されているので，ZAKの運用にあたって新たに作成する必要はない。このポリシーも「既定のユーザー」同様，［Zero-Administration設定］の［安全なタスクマネージャーを使用］項目が［No］になっていることを除けば制限を受けていない。ただし，「既定のユーザー」が［コントロールパネル］［デスクトップ］［ネットワーク］に関連するポリシー項目がすべてオフになっているのに対し，「Domain Admins」はこれらのポリシー項目を無視（淡色表示）するよう設定されている。

システムポリシーによるグループポリシーは，最も優先順位の低いグループから優先順位の高いグループへと順番にダウンロードされ，優先順位の低いグループよりも優先順位の高いグループの設定が優先される。グループの優先順位はシステムポリシーエディタの［オプション］メニューにある［グループの優先順位］で確認できる。ZAKが用意しているポリシーファイルでは，TaskUser，AppUser，Domain Adminsの順で優先順位が高くなっている。グループによって相反するポリシーを設定している場合でかつユーザーが複数のグループに所属している場合は，相反する部分にはより優先順位の高いポリシーが適用される。

ZAKが用意しているグループは上記3つのみであるが，この設定をひな形にして，管理者がさらに複数のグループを作成することは可能である。たとえば，大学であれば学部・学科・学年によって細かくグループを作成し，それぞれのグループの利用に見合ったポリシーを強制することが可能である。グループ毎に［スタート］メニューの内容を制御することができるので，それぞれの教育内容に応じた環境を提供することが可能である。

以上，ZAKに付属するCONFIG.POLについて簡単に述べたが，このままでは使用にあたって一部不都合があるので，修正が必要となる。修正すべき点は「既定のコンピュータ」ポリシーの以下の項目である。

1. ［ネットワーク］→［アクセス制御］→［ユーザーレベルアクセス制御］
   認証名：DomainName　→　各自のWindows NTドメイン名へ変更
2. ［Microsoftネットワーククライアント］→

[WindowsNTへログオン]
ドメイン名：DomainName → 各自のWindows NTドメイン名へ変更

3. [Microsoftネットワーククライアント] → [ワークグループ]
ワークグループ名：WorkGroupName → クライアントPCが所属するワークグループ名へ変更

なお，ZAKに付属するCONFIG.POLの設定ではクライアントPCのキャンセルログオンが認められない。したがって，一度ZAKユーザーがネットワークログオンした時点でそのクライアントPCはキャンセルログオンが不可能になる。不特定多数のユーザーが使用する環境ではキャンセルログオンができない方がセキュリティ的には望ましいが，これを解除するには，一旦Windows NT Server上で共有されているCONFIG.POLに修正をかけ，再度クライアントPCからネットワークログオンする必要がある。この時点で変更されたポリシーがクライアントPC側にコピーされる。Windows 95の場合はローカルディスクに対しアクセス権が設定されていないため，Domain Adminsに所属している管理用アカウントを作成し，それを用いて管理するようにしておけば，日常のメンテナンスにおいてとくにキャンセルログオンの必要はないだろう。

ただし，Windows NT Serverが稼動するドメインコントローラに障害が発生した場合は，キャンセルログオンができない状態ではクライアントPCはどうすることもできない。この危険を避けるためには，PDC以外にBDCを用意する[26]しかない。

キャンセルログオンのオンオフは「既定のコンピュータ」ポリシーの［ネットワーク］→［ログオン］→［ネットワークからのWindowsへのアクセスに認証を要求する］のチェックと連動している。

2．ログオンスクリプトファイルの作成

ZAKのアプリケーションステーションモードはMicrosoftネットワークでのログオン時にログオンスクリプトを利用する。ひな形がすでに用意されている[27]ので，それをコピーし，編集して利用する。

なお，APPLOGON.BATというファイル名はZAKユーザーアカウント作成時のプロファイルで用いたログオンスクリプト名と対応している必要がある。言い換えれば，APPLOGON.BAT以外の名称であっても対応に間違いがなければ問題はない。すなわち，複数のユーザー環境に合わせてログオンスクリプトを用意し，それぞれの内容を使い分けることも可能である。ZAKに用意されたAppUserやTaskuser以外のグループを作成することも可能だと前述したが，各グループに応じたログオンスクリプトを用意することで，より柔軟な環境を提供することが可能である。

ZAKに付属のAPPLOGON.BATからAppUser環境に必要な部分を抽出したリストは以下の通りである。

```
net use o:¥¥<dist-server>¥<netapps share>
net use u:¥¥<dist-server>¥<user share>
```

上記2行の内容を各自のネットワーク環境にあわせて修正する必要がある。本論の例の場合，

```
net use o:¥¥Ntsrv1¥NETAPPS
net use u:¥¥Ntsrv1¥HOME
```

とする。管理者ガイドでは<user share>の部分をUSERSにするよう指示がある[28]が，移動プロファイルに使用するディレクトリをユーザーから隠すために本論ではHOMEを指定することにする。

この他，ログオンスクリプトファイル中に

```
net time ¥¥Ntsrv1 /set /yes
deltree /y C:¥Windows¥Profiles
```

と記載しておくことで，クライアントPCは毎回のログオン時にPDCと時刻合わせを自動的に行い，*%SystemRoot%*¥WINDOWS¥PROFILES中にあるユーザーの移動プロファイルディレクトリを削除する。[29]

3．ポリシーファイルおよびログオンスクリプトの共有

ポリシーファイルの作成およびログオンスクリプトの編集が終了したら，この2つのファイルをMicrosoftネットワーク上で共有しなければならない。ポリシーファイルであるCONFIG.POLの作成は必ずWindows 95上で作業を行う必要があるため，このファイルはフロッピィディスクなどの移動メディアかネットワークを通じてドメインコントローラに移動させる。2つのファイルの移動先はドメインコントローラのNETLOGON共有ディレクトリである*%SystemRoot%*¥SYSTEM32¥REPL¥IMPORTS¥SCRIPTSである。

ただし，複数のドメインコントローラが稼動しているネットワークでは，ユーザーがドメインにネットワークログオンする際にどのドメインコントローラのNETLOGONディレクトリを参照するか分からないので，すべてのドメインコントローラ上で上記ファイルの内容を同一に保つ必要がある。意外にこの更新作業は忘れやすいので，Windows NT Serverの機能であるディレクトリ複製機能を利用して，特定のサーバーの*%SystemRoot%*¥SYSTEM32¥REPL¥EXPORT¥SCRIPTSディレクトリの内容を自動的にすべてのNETLOGON共有ディレクトリにコピーするようにしておく方がよいだろう。

4．スタートメニューの共有

ZAKユーザーが使用する［スタート］メニューはサーバーで一括管理することができる。ZAKサーバーの*%SystemRoot%*¥Zak95¥NetApps¥StartMenu¥Programsが対象ディレクトリとなる。このディレクトリにZAKユーザーが使用してもよいショートカット（*.LNK）を保存する。[30]

ショートカットはクライアントPCのアプリケーションソフトウェアに対するものでなければならない。したがって，ポリシーファイルと同様，クライアントPCで使われているショートカットをサーバーにコピーする。

また，このディレクトリはWindows NT Serverのアクセス権を反映するので，ショートカットに対して個別のアクセス権を設定したり，サブディレクトリを作成し，サブディレクトリに対するアクセス権を設定することができる。利用方法としては，例えば特定のグループ（教員や特定の授業を受講しているユーザー）に対してのみ特定のショートカットのアクセス権を認めることで，アプリケーションの利用方法を学習していないユーザーが誤ってソフトウェアを起動し，混乱することを避けることができる。

さらに，ポリシーファイル上で複数のグループを作成している場合は，それぞれのグループ毎に［スタート］メニューの共有位置を指定することができるので，この指定を利用することでグループ別のスタートメニューを管理することができる。対象となるグループポリシーの［シェル］→［［プログラム］フォルダのカスタム設定］で対象となるディレクトリのパスを指定する。共有ポイントの問題があるので，*%SystemRoot%*¥Zak95¥NetApps中に*Groupname*¥StartMenu¥Programsなどの名称でディレクトリを作成する方がよいだろう。[31]

ZAKの問題点

ここまでの作業を実行することでZAKを利用できるようになるはずである。AppUserグループとして登録されたユーザーであれば，図1のような画面でWindowsシステムを利用できるようになる。

それではZAKの問題点について，いくつか気付いたことを指摘しておこう。

1．ユーザー主体のパスワード管理ができない

ZAKのポリシーでは原則としてパスワードキャッシュ機能が無効になっているため，クライアントPCの*%SystemRoot%*内にユーザー毎のパスワードファイル（*.pwl）を作成することがない。これはパスワードの一元管理という点で好ましい。また，パスワードに対し英数字の組み合わせや最小文字数の指定を強制することができる。これもセキュリティの向上のた

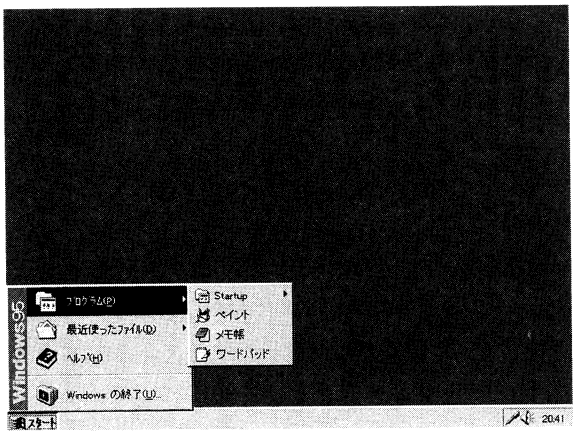

図1　ZAKユーザーのデスクトップ画面（アプリケーションステーションモード）

めには重要なことである。しかしながら，ZAKのポリシーはコントロールパネルをユーザー側に提示しない。したがって，Microsoftネットワークパスワードの変更に際し，ユーザーは管理者に依頼して，次回ログオン時にパスワード変更のためのダイアログを出してもらうようにする必要がある。

考え方によっては，定期的にパスワード変更をするよう管理者側で一括に作業を行う方法をとることもできるが，ユーザーによってはいきなりパスワードの変更を求められて困惑するケースも想定できる。

ZAKのポリシーを緩め，コントロールパネルのパスワードのみを提示するようにできればよいのであるが，残念ながらZAKに用意されたポリシーではコントロールパネルを提示するかしないかの選択ができるだけである。提示することを許可するとコントロールパネル内のすべてのアプレットが表示されてしまう。管理者ガイドには「Windows 95 Zero Administration Kitでは、コントロールパネルのすべてのコンポーネントについてアクセスが制限されます」[32] とあるが，ZAKのポリシーでアクセスが制限できるのは［画面］，［ネットワーク］，［パスワード］，［システム］のアプレットと［プリンタ］だけであり，その他の項目はフルコントロール状態となる。

この問題はTweak UI[33] というツールを利用することで一応解決する。Tweak UIはコントロールパネルのアプレットの表示／非表示を設定することができる。したがって，Tweak UIとパスワード以外のアプレットを非表示にしておく[34] ことで，システム設定に関してセキュリティを確保することができる。

なお，Tweak UIの設定はコントロールパネルの制御を行うすべてのクライアントPC上で作業する必要がある。

2．ZAKのポリシー制限を受けないソフトウェアが存在する

残念ながら，ZAKのポリシー制限を受けないソフトウェアが存在する。例としてOSに付属のエクスプローラがある。ZAKのポリシーはエクスプローラのコントロールが十分でないために，たとえばユーザーに見せたくない*%SystemRoot%*の内容が見えてしまう。

このようなソフトウェアはセキュリティホールとなる可能性が高いため，ユーザーに使用させないようにする必要がある。ソフトウェアの供給に関しては事前の調査が必要である。

3．Windows 95とWindows 98での相違点

本論では今までクライアントPCのOSがWindows 95である場合のZAK環境の構築について検討してきたが，ZAKはWindows 98でも使用することができる。ただし，一部ポリシーの実行において差異がみられる。簡単にまとめると以下のようになろう。

- **ホームディレクトリの扱い**：筆者がテスト環境として使用したWindows 95 / 98では，ログオンスクリプトでホームディレクトリであるU:¥やスタートメニューのためのO:¥をマウントしているにもかかわらず，OSのインターフェース上でそれらのドライブを確認することができなかった。ただし，Windows 98ではファイルの参照や保存を行う際にデフォルトでマイドキュメントディレクトリを参照するが，このディレクトリが実はU:¥としてマウントしている¥¥Ntsrv1¥Homeである。

このため，Windows 98ではネットワークコンピュータをZAKユーザーに見せる必要はないが，Windows 95では見せる必要がある。ZAKのデフォルトポリシーファイルではネットワークコンピュータのワークグループの内容を削除することになっているので，Windows 95では一旦ネットワーク全体に移動し，目的のドメイン（例ではSakura）の中に入らないと目的のサーバーが見つからず，この作業は初心者には負担が重い。ホームディレクトリに関連する環境はWindows 98の方が優れている。

- **Windowsデスクトップアップデートコンポーネントへの対応：**これはWindows 95 / 98の差異というよりもOSにプリインストールされているインターネットエクスプローラの問題というべきであろう。Windows 95ではインターネットエクスプローラ3.0[35]が，Windows 98では4.0以降[36]が標準でインストールされている。インターネットエクスプローラ4.0からデスクトップアップデートコンポーネントの組み込みをオプションとすることができるが，ZAKはこれらの機能に一部対応していない。例えばアップデートにより［スタート］メニューに表示される［お気に入り］はZAKのポリシーでコントロールできないので，Tweak UIなどのツールで表示を制御する必要がある。Windows 95においてもインターネットエクスプローラ4.0以降をインストールすれば同様の現象が発生する。この他，GUI的に追加される機能としては，設定項目として「タスクバーと［スタート］メニュー」「フォルダオプション」「アクティブディスクトップ」が追加され，タスクバーには「クイック起動バー」が追加される。「アクティブディスクトップ」に関してはTweak UIの制限機能と組み合わせることで，無効にすることができる。
- **Windows Updateへの対応：**Windows 98からWindows Updateの機能が付加された。ZAKのポリシーはこの機能をコントロールすることができない。Windows Updateに関してはレジストリのキーが判明しているので，ポリシーテンプレートを作成してコントロールすることは可能である。

おわりに

Windows 95 / 98のレジストリはSYSTEM.DATとUSER.DATの2つのファイルに分割されており，移動プロファイル環境では前者はクライアントPCに，後者はユーザーのホームディレクトリに保持される。ホームディレクトリにUSER.DATが存在しない場合，クライアントPCが保持しているキャンセルログオン用のUSER.DATの設定をコピーして使用することはZAK環境であっても同じである。

あらかじめすべてのクライアントPCのレジストリを統一しておくか，デフォルトのレジストリを用意し，アカウント作成時に配付するかしておく必要があるのは通常のWindows 95 / 98と変わらない。

また，ZAKによるコントロールはポリシーファイルの中に規定されたレジストリキーにのみ効果がある。コントロールされないキーはレジストリのコピーが終了すると，各ユーザーのホームディレクトリの中に分散して配置されるため，後日ポリシーファイルにないキーの状態を統一しようとすると，あらたにそれ用のポリシーテンプレートを作成し，コントロールする必要がある。

このようなポリシーテンプレートは，システムポリシーを利用している企業や学校現場においては重宝されるべきものであり，ポリシーテンプレートファイルはもっと公開され共有されてもよいと思う。今回の検討ではWindows 95よりもWindows 98の方がZAKにおけるクライアントPCとしての適性があるように思われるが，後者ではOSの拡張部分のコントロールが不十分であるため，より安全な環境構築のためには他のツールの併用やWindows 98用のポリシーテンプレートの利用が必要である。今回は紙面の都合で紹介できないが，機会があればそれらのより具体的な方策の一例について紹介したい。

参考文献

Karanjit S.Siyan,Ph.D. （アクロバイト監訳）『Windows NT Server 4 ネットワークバイブル』 インプレス，1998年。

Kathy Ivens （舟木将彦訳）『Windows レジストリ最適化手法』 オーム社開発局，1998年。

Microsoft Corporation 『Microsoft Windows95リソースキット』 Vol.1－2 アスキー出版局，1995年。

Microsoft Corporation 『Microsoft WindowsNT 4.0 Server リソースキット』 アスキー出版局，1997年。

註

1) 拙論，「小規模校における電子メール環境の構築 I 」『美作女子大学・美作女子大学短期大学部紀要』44号（1999年）82-92頁。

2) 拙論，「小規模校における電子メール環境の構築 II」『美作女子大学・美作女子大学短期大学部紀要』45号（2000年）72-92頁。

3) 現在ではWindows 98の後継OSとしてWindows Meが発売されているが，筆者の環境でまだ評価を検討するまでに至っていない。したがって，以後の比較・検討ではWindows Meは含まない。また，以降のMicrosoft社の商標に関してはMicrosoftの表記を省略するものとする。

4) 拙論，前掲「小規模校における電子メール環境の構築II」88頁において，Windows 95の移動プロファイル方式ではユーザーが勝手に設定を改変できることを指摘した。

5) Zero Administration Kit for Windows 95 CD-ROMの*%CD-ROM_Root%*¥DOC¥ZAKADMIN.DOC。

6) 管理者ガイド27-28頁。

7) ZAKの自動セットアップは，ネットワーク上に存在するクライアントPCが，サーバー上にあるWindows 95およびOffice 97のインストールデータを自動的にダウンロードしインストールする機能である。ZAKではインストール処理を行うセットアップスクリプトを用意しており，各自の使用環境にあわせて内容を修正することでこの機能を実現している。

8) ネットワークサーバー上にあるOffice 97のアプリケーションソフトウェアを，ネットワークを介してクライアントPCが起動し，利用する機能である。アップデートなどの修正が一括管理できる。

9) OSのビルド番号は4.00.950.Bを使用した。

10) OSのビルド番号は4.10.2222 Aを使用した。

11) 拙論，前掲「小規模校における電子メール環境の構築 II」80頁。

12) 異なるWindowsドメイン間で信頼関係を設定することにより，ユーザーは1つのドメインにユーザーアカウントを持つだけで信頼関係を結んだWindowsドメイン内のリソース（資源）にアクセスすることができる。信頼する側のドメインは，自分が管理するSAMと呼ばれるセキュリティデータベースにアカウントデータが存在していなくても，信頼されるドメインのデータベースを利用して認証を行うが，これをパススルー認証と呼ぶ。

13) 使用したメディアによっては，この後，Windows 95 Service Pack 1を要求されるかもしれない。

14) 今回はWindows 95 CD-ROMの*%CD-ROM_Root%*¥other¥ie30を使用した。

15) 管理者ガイド9-10頁。

16) 拙論，前掲「小規模校における電子メール環境の構築 II」91頁。

17) Usersディレクトリの共有名をUSERS$にした理由がこれによる。共有名に$を付けることで直接UNCパスを指定しない限りネットワーク上では不可視となる。ただし，アクセスできないということではない。

18) 拙論，前掲「小規模校における電子メール環境の構築 II」76-79頁。

19) Microsoft Corporation著，『Microsoft Windows 95 リソースキットVol.1』（アスキー出版局，1995年）511-512頁。

20) 表記方法については，Microsoft Corporation著，前掲「第15章　ユーザープロファイルとシステムポリシー」『Microsoft Windows 95 リソースキットVol.1』を参照していただきたい。

21) とはいってもむやみな変更によってクライアントが使用不可状態に陥ることもあるので，十分内容を検討した上で修正する必要がある。

22) Zero Administration Kit for Windows 95 CD-ROMの*%CD-ROM_Root%*¥TOOL¥POLEDIT.EXE。

23) ZAKに付属の管理者ガイドには詳しい作業手順についての記載がないので，詳細はMicrosoft Corporation著，前掲「第15章　ユーザープロファイルとシステムポリシー」『Microsoft Windows 95 リソースキットVol.1』を参照。

24) この設定は変更することが可能である。システムポリシーの手動ダウンロードと呼ばれる機能である。［既定のコンピュータ］ポリシーの［ネットワーク］→［更新］→［リモート更新］をオンにし，ダウンロードしたいポリシーファイルが存在するUNCパスとファイル名を指定することでシステムポリシーの手動ダウンロードが可能になる。

25)「既定のコンピュータ」のポリシーはそのPCに対しての

制御を担当するので，ユーザー固有の設定を保持するUSER.DATに対するポリシーは含まれない。

26）バックアップデータと同じことで，BDCはできれば違う場所（建物）に設置するのが望ましい。

27）Zero Administration Kit for Windows 95 CD-ROMの*%CD-ROM_Root%*¥SCRIPTS¥APPLOGON.BAT。

28）管理者ガイド44頁。

29）削除することで毎回のログオン時に「このコンピュータで初めてログオンされるユーザー名です。次回にログオンするときのために，ユーザー個別の設定をこのコンピュータに保存しますか？」というダイアログが表示されるようになる。移動プロファイルの一括管理という点ではクライアントの移動プロファイル情報は使用後に削除し，サーバーにのみ常に最新の情報がある方が好ましい。また，クライアントPCのシステムがインストールされたローカルディスクの空き容量が少ない場合もこの設定の方がよい。しかし，ネットワークやサーバーに負荷がかかる，上記ダイアログで「いいえ」を選択されるとローカルのプロファイル情報が使用されてしまうなどの問題もある。これはWindows 95 / 98のシステム上の欠陥である。

30）*%SystemRoot%*¥Zak95¥NetApps¥StartMenu¥Programs¥Startupはスタートアップソフトウェア用のフォルダである。

31）*Groupname*はZAK用グローバルグループの名称を代入する。

32）管理者ガイド22頁。

33）Tweak UIはMicrosoft社が提供していたPowerToysというユーティリティ群に含まれていたツールである。Microsoft社のWWWからダウンロードすることができ，2000年12月1日現在の最新版は1.33である。ただし，このツールはMicrosoft社が提供しているが動作の保障はしていない。したがって，自己責任においてツールを使用することになる。英語版のみの提供であるが，日本語版への移植ツールも有志によりWWWで公開されている。

34）Tweak UIのアプレットも非表示にすると，以後レジストリを直接修正しない限りTweak UIを実行できなくなるので，コントロールパネルの表示／非表示の制御もできなくなる。Tweak UIのアプレットは表示する設定にしておく方がよい。

35）筆者の環境では3.0（4.70.1158）がインストールされている。

36）筆者の環境ではWindows 98 SEであるため5（5.00.2614.3500）がインストールされている。

（2000年12月1日　受理）