淑徳短期大学研究紀要第45号（2006.2）

情報実習室のトラブル対策Ⅱ

小　杉　誠　司

（2005年9月17日受理）

要　約

情報実習室のサーバーで起こるトラブルの対処法について考察した。最初にサーバーのハードウェアの故障対策について、次にサーバーのデータのバックアップについて論じた。本学の情報実習室ではWindows NTサーバーを二つ稼動させて、ドメインを構築している。一台をプライマリ・ドメインコントローラ（PDC）として、ファイル・サーバー、プリンタ・サーバー、DHCPサーバー、WINSサーバーとして利用している。さらに他の一台をバックアップ・ドメインコントローラ（BDC）として稼動させている。PDCが故障すると、そこに学生の移動プロファイルやホームディレクトリが保存されているので、授業ができなくなってしまう。そのときにはBDCをPDCに昇格させる。また故障したPDCの修理が終わりドメインに復帰させるときには、以前のようにPDCとして稼動させる必要がある。これらの具体的な処方箋について詳しく考察した。

キーワード　Windows NT Server、プライマリ・ドメインコントローラ、
バックアップ・ドメインコントローラ、昇格、障害復旧

はじめに

前論文[1)]では情報実習室で起こるトラブルのうち、学生機で起こるトラブルの対処法について考察した。最初にシステム・ポリシーを用いて学生が利用できる機能を制限する手法について、次にWindowsの起動ドライブのイメージ・バックアップを取り、トラブルが生じたときにリストアする手法を紹介した。最後に、再起動するだけで学生機のハードディスクの内容を完全に元の状態にもどすことができる瞬間復元ツールを紹介した。本論文ではサーバーで起こるトラブルの対処法について考察する。

まず本学の情報実習室のシステム環境について簡単に説明する。本学ではWindows NTサーバーを二つ稼動させて、ドメインを構築している。1台のNTサーバーをプライマリ・ドメインコントローラ（PDC）[注1)]としてログオン認証に利用し、そのPDCをファイル・サーバー、プリンタ・サーバー、DHCPサーバー、WINSサー

バーとして利用している。さらにバックアップ・ドメインコントローラ（BDC）[注2]を1台導入している。BDCはPDCのセキュリティ・アカウント・マネージャー（SAM）[注3]データベースのバックアップを所有しているので、PDCに代わってユーザー認証を行なうことができる。メール・サーバーやWebサーバーなどのインターネット・サーバーは、ホスティングサービスを利用しているので、本学の情報実習室にはない。

100台近くあるクライアントPCのOSはWindows XP Professionalである。それらをドメインに参加させ、またログオン時にPDCの¥Netlogon共有ディレクトリにあるポリシー・ファイルを読み込むように設定して、ログオンしたユーザーのシステム環境にシステム・ポリシーを適用している。

Windowsではユーザーごとのシステム環境を、ローカルマシンまたは、サーバー上にユーザープロファイルとして保存している。サーバー上にプロファイルを保存しておけば、ユーザーがドメイン内のどのWindows PCからログオンしても、同じ操作環境を使用できるので非常に便利である。本学の情報実習室ではこの移動プロファイルを使用しており、このプロファイルをPDCに保存している。またPDCに個々の学生のホームディレクトリを作成し、学生が授業中にOffice等で作成したファイルを、フロッピやローカルPCのハードディスクではなく、このホームディレクトリに保存している。

本論文では、最初にPCサーバーのハードウェアの故障対策について考察する。上で述べたように授業ではPDCをいろいろなサーバーとして利用しているので、PDCが停止すると授業に大きな支障が出てしまう。最悪の場合には授業を休講にしなければならない。そうならないようにするためには、ハードウェアの故障対策を万全にする必要がある。その対策としてハードディスクのRAID構成、無停電電源装置の利用、また電源ユニットや冷却ファンの二重化について述べる。

次にサーバーのデータのバックアップについて考察する。サーバーのハードディスクをRAID構成にしてハードディスクの故障に備えたとしても、操作ミスによってデータを損失することもある。またサービスパックやパッチを当てたあとに不具合が生じてしまい、元の状態に戻したいこともあるので、サーバーのデータのバックアップは必要である。サーバーのバックアップといえば、一昔前ではテープにとるのが定番であったが、ハードディスクが大容量化し、テープ装置に比較してはるかに低価格になった現在では、ハードディスクにとるのがよいと思う。

次にブート・パーティションのバックアップをとる方法をいくつか紹介する。そのなかでDドライブにNT Workstationをインストールする方法が最も推薦できる。ライセンスの問題はあるが、他の方法に比べて安価で、簡単である。

サーバーの故障対策をいろいろ講じていても、どうしても予期しない故障は起きてしまう。PDCが故障すると授業ができなくなってしまうので、稼動しているサーバーが一台だけというのは不安である。そこで、既に述べたように、本学ではもう一台

NT サーバーを稼動させ、それを BDC としている。

通常の稼動時には PDC の ¥Home を BDC の ¥Home にミラーリング[注4)]をおこない、バックアップをとっている。PDC のその他のディレクトリも必要があるものは BDC にバックアップをとっている。そして PDC が故障したときには、BDC を PDC に昇格し、授業に支障が生じないようにしている。

故障した PDC の修理が終わり戻ってきたときには、以前のように PDC として稼動させる必要がある。また故障中に学生が授業で作成したファイルなどを、PDC にコピーする必要がある。これらの手法について具体的に詳しく考察する。

PC サーバーのハードウェアの故障対策

多くの企業においては、サーバー停止がビジネスの機会損失や損害発生のリスクに直接つながるので、サーバーのシステム・ダウンは許されない。学校の情報実習室においても、程度の違いはあるが、事情は同じである。そこで、サーバーが深刻な状態に陥らないようにするための対策が必要になる。

PC サーバーのハードウェアの故障対策としては、次のことが考えられる。

①ハードディスクの故障を回避するために RAID 構成にする。RAID は複数のディスク・ドライブを組み合わせて、性能や耐障害性を高める技術である。よく使われる RAID 5 というレベルは、3 台以上のディスク・ドライブを組み合わせて構成し、データをディスクに記録する際、そのデータのパリティ情報を生成して、残りのデータとともに複数のディスクに分散して書き込む。こうしておくと 1 台のドライブが壊れたときに、残りのドライブの情報から壊れたドライブのデータを復旧することができる。さらにホットスワップという機能があれば、サーバーを稼動したままの状態で故障したディスクを入れ替える作業をできので、サーバーを止めずに済む。[注5)]

②無停電電源装置（UPS）を利用する。UPS は Uninterruptible Power Systems の略であり、停電や電源変動などの電源トラブルが発生したとき、内部バッテリーを電源としてコンピュータや周辺機器等に電源を供給する装置である。その間に PC を安全にシャットダウンする。しかし電源トラブルが発生した際、必ずしもシステム管理者がサーバーの側にいて手動でシャットダウンできるとは限らない。PC をシャットダウンせずに放置すると、内部のバッテリーが完全放電して UPS は停止してしまうため、ファイルが破壊しデータが消失してしまうことがある。このようなときのためにシステム管理者が不在でも自動的に安全かつ確実にサーバーをシャットダウンする機能がある。

Windows NT/2000/2003 サーバーは、デフォルトで UPS 管理ツールを持っており、自動シャットダウン機能やログ機能[注6)]といったごく基本的な機能は備えている。しかし UPS ベンダーが提供している管理ツールには、電源トラブルが回復

しUPSのバッテリが充電された時点でサーバーを再起動させる自動リブート機能、システムを使用しない夜間や週末に自動的にサーバーをシャットダウンし、授業が始まる前にリブートするように設定するスケジュール機能、サーバーをシャットダウンする前に、シャットダウンについてLAN上のユーザーに通知する機能等を備えている。

③PCサーバーのなかで壊れやすいものは、回転するものと熱を発生するものである。その意味では、電源ユニットや冷却ファンも壊れやすいので、二重化したほうがよい。しかし、実際にはこれらを二重化したPCは高価で、設置するのは難しい。しかし少なくとも予備を用意しておくことは必要である。

RAID構成にしたりUPSを使用して、ハード面で耐障害機能を備えるだけでは信頼性を獲得できない。障害が起きる前に、あるいは起きたときに出す警告を管理者が確実に受け取ることが重要である。そのためにはOS標準のツールである「イベントビューア」や「パフォーマンス・モニター」等を利用することに加えて、サーバー付属のシステム管理ツールをインストールしておくことも必要である。

サーバーのデータのバックアップ

サーバーのデータが消失する原因として以下のものが考えられる。

①ハードウェアの故障
②操作ミス
③地震、火災などの災害
④コンピュータ・ウィルス
⑤サービスパックやパッチを当てたあとの不具合

少し前には、RAIDがすなわちバックアップと考えられたこともあった。しかしRAIDはバックアップではない。上の②～⑤の原因でデータを失ったときには、RAIDでは元に戻せないので、データのバックアップは必要である。

従来はサーバー内のディスクにRAIDを使い、サーバーのバックアップといえばテープにとるのが定番であった。テープはバックアップメディアとして最も普及し、低コストであった。またリムーバブルで可搬性のあるメディアなので、災害時対策のために遠隔地にバックアップを保管することができる。また他のリムーバブルメディアに比べ、高速である。

テープへバックアップをとるには、まず最初にすべてのデータを保存するフル・バックアップをおこなう。その後はそのデータを基準に、当日のデータとの差分をバックアップする差分バックアップをとるか、直前のバックアップとの相違部分をバックアッ

プする増分バックアップをとる。これらの保存先が複数のテープになることも多い。このときにはこれらのテープのうち一本でも不具合があるとリストアできない。

その他に、テープでバックアップをとる場合の欠点として次のことが考えられる。

①テープ装置は週に１回程度の定期的なクリーニングが必須である。これを怠ったために装置が故障したこともあった。

②テープの数が多いとテープの管理が大変である。紛失することもある。また大量のデータをバックアップするときには、テープの劣化を遅らせるために、使用回数が同じになるようにメディアを使用する順番を規則的に決めておく必要があり、管理が面倒である。

③ディスクに比べると低速である。特にデータがテープの最後の方にあると、読み出すのに時間がかかる。

④リストアに時間がかかる。バックアップ時の速度に対して10分の１程度しかパフォーマンスが出ないことが少なくない。

そこでテープは個人や小規模の事業所などで利用される機会がほとんどなくなってしまった。しかし依然として、企業などのサーバーのバックアップでは中心的な役割を担っているが、その企業でもバックアップをとらなければならないデータが爆発的に増大しているのに、大容量のデータを高速に処理できるテープ装置がないので、どうバックアップをとるか悩んでいるのが現状である。

そこで企業ではハードディスクを使ったバックアップが注目されている。その背景には、ハードディスクの大容量化と低価格化、RAIDによりハードディスク装置の信頼性が向上したこと、ネットワーク装置の高速化と低価格化などがある。ハードディスクではテープに比べて10倍もの高速バックアップが可能である。またテープで起こりがちな劣化がなく、クリーニングも不要でメンテナンスコストが少ない。

学校の情報実習室においても、企業の場合とは事情が違うが、学生数がそれほど多くなければ、バックアップはハードディスクにとるのがよいと思う。ベンダーはサーバーには必ずといってよいほどテープ装置を付属して提供したがるが、現在ではテープ装置はハードディスクに比較して非常に高価である。バックアップ先は、ファイル・サーバーやNAS[注7)]等も考えられるが、本学のようにバックアップをとるサーバーが1、2台のときには、サーバーのローカルのハードディスクにとるのが一般的である。ハードディスクがRAID構成ならばディスクの故障対策はできているので、容量に余裕があれば、新たにバックアップ用のディレクトリを作成して、そこにバックアップを保存してもよい。RAID構成になっていないときには、別のハードディスクにバックアップをとる。

ではどのようにしてハードディスクにバックアップをとったらよいのか。バックアップをとるべきサーバーのデータには、大別して二つある。一つはデータファイル、もう一つはシステムファイルである。データファイルのバックアップは簡単で、例えば

エクスプローラを使えばよい。もっともバックアップに掛かる時間を短縮するにはミラーリング・ソフトなどを使うのがよいが、ネット上にはこの種の無料のソフトがたくさんあるので、容易に探し出すことができる。

しかしブート・パーティションのバックアップは、システムファイルが使用中であるためロックされていて、エクスプローラ等によるファイルのコピーではバックアップできない。ブート・パーティションのバックアップとして、まず最初に思いつくのは、サード・パーティ製のバックアップ・ソフトを使う方法である。これらのソフトは本来テープ装置用のものであるが、最近ではハードディスクへのバックアップにも対応している。しかしサーバー用の製品は価格が高く10万円以上はするので、わざわざそのためだけに、それを購入する気にはなれない。[注8)]

次にクライアントPCでよく利用されているGhostなどのイメージング・ツールを利用することが考えられる。これらのツールはDOS上で動くので、Windowsをシャットダウンしなけらばならないが、学校のサーバーの場合には、インターネット・サーバーは別にしても、ファイル・サーバー等をシャットダウンする時間を見出すことは比較的容易である。しかしハードディスクがRAID構成のときには使えないツールがほとんどである。[注9)]

ここで、クライアントPCのバックアップをとる方法の一つとして、以前に紹介した方法[1)]が利用できる。それはDドライブにもOSをインストールする方法である。本学では、CドライブにNTサーバーがインストールされているので、DドライブにNT Workstationをインストールする。やり方は簡単で、NT WorkstationのCDを入れて、¥i386¥autorun.exeをダブルクリックすれば、インストールを始める。Dドライブに既にデータが存在していても、インストールによってそのデータは削除されないし、必要なスペースも200MB程度と少ない。Cドライブにあるシステムファイルをバックアップするときには、Dドライブから起動してCドライブの内容をバックアップする。このときサーバーの機能を停止しなければならないが、学校の場合にはサーバーを停止する時間があることと、それほど頻繁にCドライブのバックアップをとる必要はないので、特に困ることはない。本学には二つサーバーがあるが、そのうちの一つのサーバーにはテープ装置がないので、この方法でバックアップをとっている。

6 BDCのPDCへの昇格

サーバーのハードウェアの故障対策やデータのバックアップをとることは重要であるが、故障対策に万全ということはなく、どうしても予期していない故障は起きてしまうので、稼動しているサーバーが一台だけというのは、非常に不安である。確かに対策を講じておけば復旧作業が順調に進み、その結果速く復旧することができるが、その間に授業があればどうしても支障が出てしまう。

そこで本学の情報実習室ではWindows NTサーバーを二つ稼動させて、ドメインを構築している。一台のNTサーバーをPDCとしてログオン認証に利用し、そのPDCをファイル・サーバー、プリンタ・サーバー、DHCPサーバー、WINSサーバーとして利用している。さらにBDCを一台導入している。BDCは通常の稼動時には、PDCに代わってユーザー認証をおこなっている。BDCが故障してもPDCが正常ならば、なんの支障もなく授業をおこなうことができるが、PDCが故障するとそこに学生の移動プロファイルやホームディレクトリが保存されているので、通常の授業ができなくなってしまう。そこでこのときには、BDCをPDCに昇格させ、PDCの役割を果たさせようとしているわけである。以下にPDCが故障したときの処方箋について解説する。

Ⅰ．故障が起きる前におこなっておくこと

（1） 本学ではPDCにディレクトリ￥Homeを作成し、更にその下に各学生のホームディレクトリを作成して、学生が授業で作成したファイルやユーザープロファイルなどを保存している。授業をおこなうとこのディレクトリの内容が変更されるので、日常的にこの￥HomeをBDCの￥Homeにミラーリングをおこなっている。PDCが故障したときにはBDCをPDCに昇格するので、PDCに保存してあって授業で使用しているファイルはすべてBDCにも保存しておく必要がある。その他のディレクトリも、必要があればミラーリングをおこなっている。例えば、本学では、￥Network（学生が送った出席票やレポートファイルを保存したり、教員が授業のときに学生に送るファイルを保存してあるディレクトリ）、￥User（学生のデスクトップ構成等を保存してあるディレクトリ）、￥Scm（ScreenCamで作成した教材ファイルを保存してあるディレクトリ）、￥Netlogonなどもミラーリングをおこなっている。具体的にはバッチファイルを作成し、次のようなATコマンドを使って、夜間におこなっている。[注10)]

EXEC AT.EXE 23:00 /every:M,T,W,Th,F,Su "D:￥Winbat￥Winbat32.exe" D:￥Winbat￥MirrHome.btw

ミラーリングをとるタイミングをどうするか、迷うところである。間をおかずにリアルタイムにとるのがいいとは、一概にいえない。例えば新しいファイルがウィルスに感染していれば、感染したファイルが直ぐにコピーされてしまう。あるいは間違ってファイルを保存してしまったために、古いファイルが必要になることもあるからである。本学では、夜間にまとめてミラーリングをおこなっている。

ここで、ミラーリングでおこなっている通常のコピーでは、BDCのディレクトリに対する共有の設定とセキュリティの設定は、コピーされないので注意する必要

がある。当然のことであるが、PDC だけでなく BDC においてもまた、これらのディレクトリやファイルに対する共有とセキュリティの設定をおこなう必要がある。特に PDC の ¥Home にある学生のホームディレクトリは、学生がアカウント登録をしたときに作成されるので、[注11] そのあと BDC でも同じ名前のディレクトリを作成し、BDC で共有とセキュリティの設定をおこなう次のバッチジョブを夜間に実行している。

```
MD D:¥Home¥%User%
CACLS D:¥Home¥%User% /T /E /C /G Administrators:F
CACLS D:¥Home¥%User% /T /E /C /G %User%:F
CACLS D:¥Home¥%User% /T /E /C /R Everyone
NET SHARE %User%=D:¥Home¥%User%
```

ここで、学生のディレクトリ %User% に対するセキュリティの設定では、そのユーザーと Administrators に対してフルコントロールにしているが、それ以外のユーザーにはアクセス権を与えていない。¥Home のセキュリティの設定は、Everyone に対してフルコントロールにしてある。

（2） PDC をプリンタ・サーバーとして利用しているので、当然 PDC にはクライアントの OS である Windows XP のプリンタ・ドライバーがインストールされている。BDC にも XP のプリンタ・ドライバーを前もってインストールしておく必要がある。

しかしここで問題がある。最近発売されたプリンタの XP のドラーバーは、プリンタのマニュアルに従って簡単に Windows NT サーバーにインストールできるが、古いプリンタ（例えば EPSON LP9200SX）の場合には、XP のドライバーを直接 NT サーバーにインストールしようとしてもできない。次のようにして、クライアント PC から NT サーバーにインストールしなければならない。

①サーバーにプリンタの Windows NT 用のドライバーをインストールする。

②次の方法で NT サーバー（ここでサーバー名を BackupX とする）においてプリンタを追加しておく。スタートメニューから、設定→プリンタ→プリンタの追加→このコンピュータ→ポートの追加→LPR Port→プリンタのIPアドレスを入力→サーバーのプリンタ名（例えば PrinterX1）を入力→閉じる→次へ→EPSON LP9200SX→次へ→「現在のドライバーを使う」にチェックを入れる→プリンタ名（例えば PrinterX1）を入力→「共有する」にチェックを入れる→「次へ」をクリック。しかしこの段階ではまだ XP のドライバーはインストールされていない。

8

③クライアントPCでWindows XPのドライバーをインストールする→検索の中止をする→エクスプローラー等で￥￥BackupX￥PrinterX1を右クリック→共有のタブをクリック→「追加ドライバー」をクリック→「Intel Windows 2000またはXP」にチェックを入れる。こうしてBackupXにXPのドライバーがインストールされる。

同じ種類のプリンタをBackupXに追加する場合には、上の②の操作でプリンタの追加をおこなう必要があるが、③の操作は必要ない。

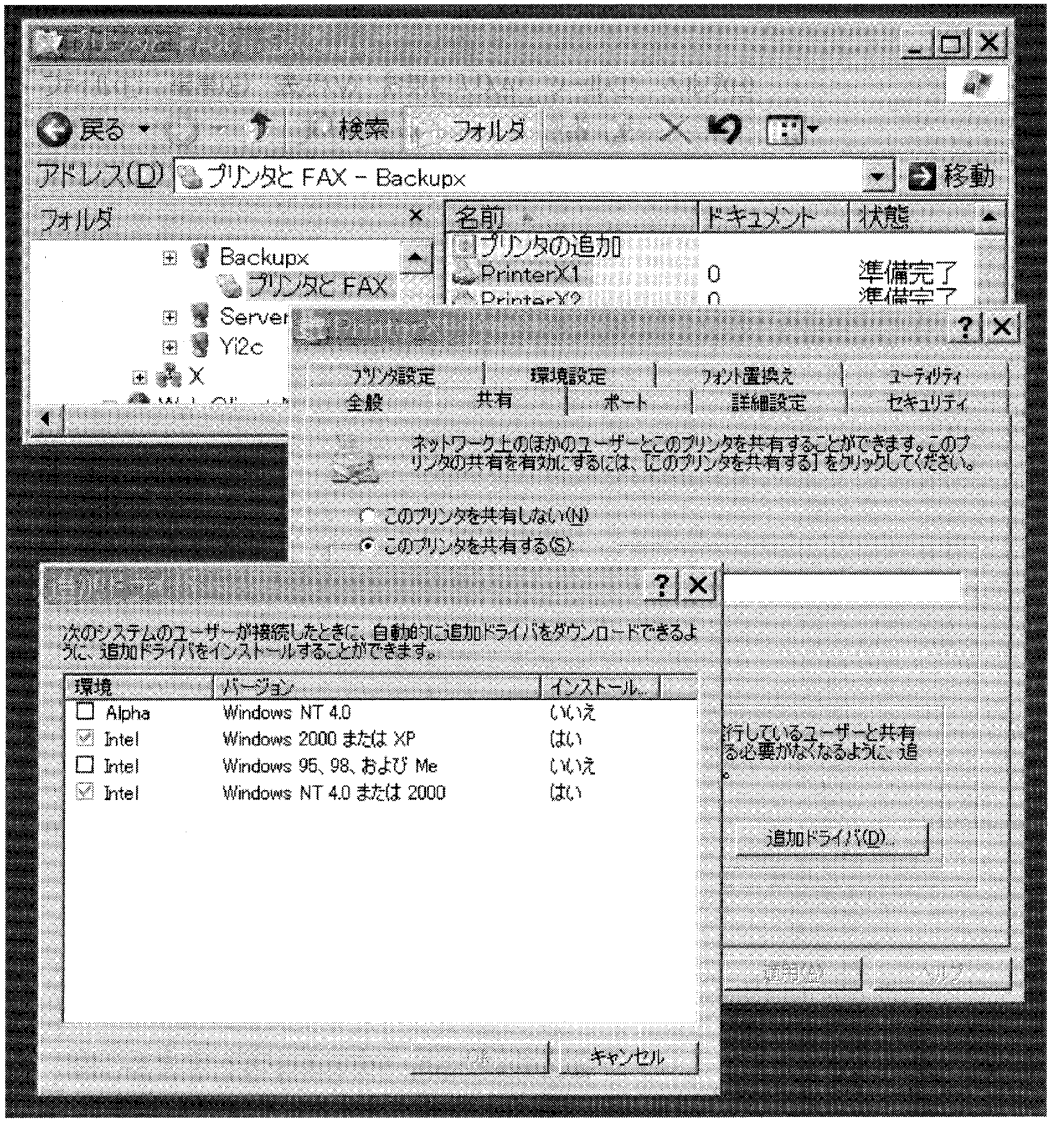

図1　Windows XPのドライバーのインストール

（3） WINSの設定

WINS（Windows Internet Name Service）はWindowsネットワーク環境において、NetBIOS[注12)]で使われているマシン名とIPアドレスを対応させるためのサービスである。WINSが使われる以前は、LMHOSTSファイルという、NetBIOS名とIPアドレスの対応を静的に記述したデータベース・ファイルが利用されていた。しかしDHCPサービスなどの導入により、各マシンが必ずしも固定的なIPアドレスを持たなくなってきたので、新たにWINSというシステムが開発された。

PDCだけでなくBDCでも日常的にWINSのサービスを開始している。そしてDHCPの設定で、PDCをプライマリWINSサーバーに、BDCをセカンダリのWINSサーバーにしている。複数のWINSサーバーを構成すると、サーバー間の負荷のバランスを取ることができる。プライマリWINSサーバー上のデータベースとセカンダリWINSサーバー上のデータベースの整合性を保つために、双方のサーバーが互いにプッシュ・パートナーとプル・パートナーになっているようにする。ここでプル・パートナーとは、パートナーからデータベースのデータを引き出すWINSサーバー、プッシュ・パートナーとは、パートナーへデータを送り出すWINSサーバーのことである。

WINSサーバーの設定をおこなうには、「管理ツール(共通)」の「WINSマネージャー」を起動する。複製パートナーを追加するには、「サーバー」メニューの「複製パートナー」をクリックする。次に「追加」をクリックし、一覧に追加するWINSサーバーの名前またはIPアドレスを入力する。

複製パートナーをプッシュ・パートナーとプル・パートナーの両方になっているように構成するには、

①「サーバー」 メニューの「複製パートナー」をクリックし、「複製パートナー」ダイアログ ボックスの「WINSサーバー」一覧で、構成するサーバーをクリックする。

②図2に示すように、「複製オプション」で「プッシュ・パートナー」と「プル・パートナー」チェック ボックスをオンにする。

データベースの複製をどのようなタイミングでおこなうかを指定するには、「サーバー」メニューの「構成」をクリックし、「WINSサーバーの構成」ダイアログ・ボックスでおこなう。

①「プル・パラメータ」の「初期化時に複製」チェック・ボックスをオンにすると、システムの初期化時や複製に関連するパラメータの変更時に、必ずこのWINSサーバーが既知のパートナーから複製物を引き出す。

②次に、「プッシュ・パラメータ」の「初期化時に複製」チェック・ボックスと「アドレス変更時に複製」チェック・ボックスをオンにする。こうすると、このサーバーがシステムを初期化したときにデータベースの状態をプル・パートナー

図2 「複製パートナー」の「複製オプション」の設定

に通知する。またマッピング・レコード内のアドレスが変更されたときにデータベースの状態をプル・パートナーに通知する。

③それ以外の設定はデフォールトのままとした。

（4） DHCPの設定

DHCP（Dynamic Host Configuration Protocol）は、各クライアントの起動時に動的にIPアドレスなどを割り当て、終了時にIPアドレスを回収するためのプロトコルである。DHCPサーバーには、クライアントPCに割り当てるIPアドレスの範囲や利用可能期間（リース期間）、更にゲートウェイやDNSサーバーのIPアドレスやサブネットマスクなどが設定されており、アクセスしてきたPCにこれらの情報を提供する。DHCPサーバーにこれらの値を設定しておけば、あとはクライアントがサーバーから自動的に値を読み取り、設定するので、いちいちすべてのクライアントに対して、手動でIPアドレスを割り振る必要がなくなる。

もちろんクライアントPCの設定で、DHCPサーバーからIPアドレスを取得するようにする必要がある。例えば、Windows XPがDHCPクライアントになるに

は、「TCP/IP のプロパティー」の設定で「IP アドレスを自動的に取得する」にチェックを入れる必要がある。

クライアントはサブネット全体へのブロードキャストによって DHCP サーバーを発見するので、一つのサブネットに一つの DHCP サーバーを立てる必要がある。一つのサブネットに複数の DHCP サーバーを配置することも理論上は問題ないが、DHCP サーバーは相互に情報を交換しないので、DHCP サーバーは二つ立てないほうがよい。もし立てるときには利用可能な IP アドレスの範囲が重複しないように注意する。また利用可能な IP アドレス以外の設定は、二つの DHCP サーバーで同じにする

本学では、通常の稼動時には、PDC を DHCP サーバーにしている。しかし PDC が故障したときには BDC を DHCP サーバーにする必要があるので、そのときのために PDC と同じスコープやオプションの設定を、BDC においても前もっておこなっている。しかし通常の稼動時には、BDC においては DHCP サーバーのサービスは停止している。

DHCP サーバーのサービスを開始または停止するには、コントロール・パネルの「サービス」アイコンをダブルクリックし、「サービス」一覧のなかから「Microsoft DHCP Server」をクリックし、次に、「開始」、「停止」、「一時停止」、または「続行」をクリックする。

DHCP マネージャを起動するには、「管理ツール(共通)」をポイントし、「DHCP マネージャ」をクリックする。DHCP の設定では、まず一つ以上のスコープを作成する必要がある。ここでスコープとは、サーバーがクライアントに割り当てることができる IP アドレスの範囲のことである。新しいスコープを作成するには、まず「管理ツール(共通)」をポイントし、「DHCP マネージャ」をクリックして、DHCP マネージャを起動する。次に

①「DHCP マネージャ」ウィンドウの「DHCP サーバー」一覧で、スコープを作成するサーバーを選択する。

②「スコープ」メニューの「作成」をクリックする。

③「開始アドレス」ボックスと「終了アドレス」ボックスに、先頭の IP アドレスと末尾の IP アドレスを入力して、利用可能な IP アドレスの範囲を定義する。ここで注意しなければならないのは、ネットワーク内には静的 IP アドレスを与える必要があるサーバーがあるという点である。例えば、DHCP、DNS、および WINS サーバーは、すべて静的 IP アドレスを使用する必要があるので、PDC と BDC には、静的 IP アドレスを割り当てている。したがって、割り当て済みの IP アドレスのいくつかはスコープの範囲に入れないようにする。

12

④「サブネット・マスク」ボックスに、サブネット・マスクを入力する。

⑤IP アドレス・プールの範囲内で除外するアドレスを定義するには、「除外範囲」を使う。除外範囲の先頭の IP アドレスを「開始アドレス」ボックスに入力し、

除外範囲の末尾のIPアドレスを「終了アドレス」ボックスに入力する。次に、「追加」をクリックする。

⑥スコープ内のIPアドレスのリース期間を指定するには、「期間」をクリックし、次に、「日」、「時間」、および「分」の各ボックスで、アドレス・リースの長さを定義する値を入力する。通常、リース期間はデフォルト値で1週間程度となっている。利用できるIPアドレスに余裕がある場合には、「無期限」に設定する。しかし余裕がない場合には、リース期間を見直し、1日から数日にする。こうすることで、サーバーでプールに戻されるIPアドレスの割合が上がり、効率的な割り当てが可能になる。しかしあまり短すぎるとDHCPへのアクセスが頻繁に起こってしまう。スコープの作成を終了すると、作成したスコープがアクティブでないことを注意するメッセージが表示される。「はい」をクリックすると、作成したスコープは直ちにアクティブ化されるが、このスコープに対するDHCPオプションの定義を完了するまでは、新しく作成したスコープをアクティブにしないでおく[注13)]。

次に、IPアドレス情報に加えて、DHCPクライアントに渡すその他のDHCPオプションを割り当てる。オプションは、すべてのスコープに対してグローバルに定義することも、選択したスコープまたは個別のDHCPクライアントに対して定義することもできる。DHCP構成オプションを割り当てるには、

①「DHCPマネージャ」ウィンドウの「DHCPサーバー」一覧で、構成するスコープを選択する。

②現在選択しているサーバー上のすべてのスコープに対してオプション設定を定義する場合は、「DHCPオプション」メニューの「グローバル」をクリックする。「DHCPマネージャ」ウィンドウで現在選択しているスコープに対してオプション設定を定義する場合は、「スコープ」をクリックする。

③「使用しないオプション」一覧のなかから、適用するDHCPオプションの名前を選択し、「追加」をクリックすると、選択したオプション名が「使用するオプション」一覧に移動する。たとえば、ルーターを指定する場合には、「使用しないオプション」一覧の「003ルーター」をクリックし、次に「追加」をクリックする。よく指定するその他のオプションには、006 DNSサーバー、044 WINS/NBNSサーバー、046 WINS/NBTノードタイプ[注14)]などがある。

④オプションの値を定義するには、まず「使用するオプション」ボックスで値を定義するオプションの名前をクリックし、次に「値」をクリックしてオプションのデータ型に応じて値を入力する。

13

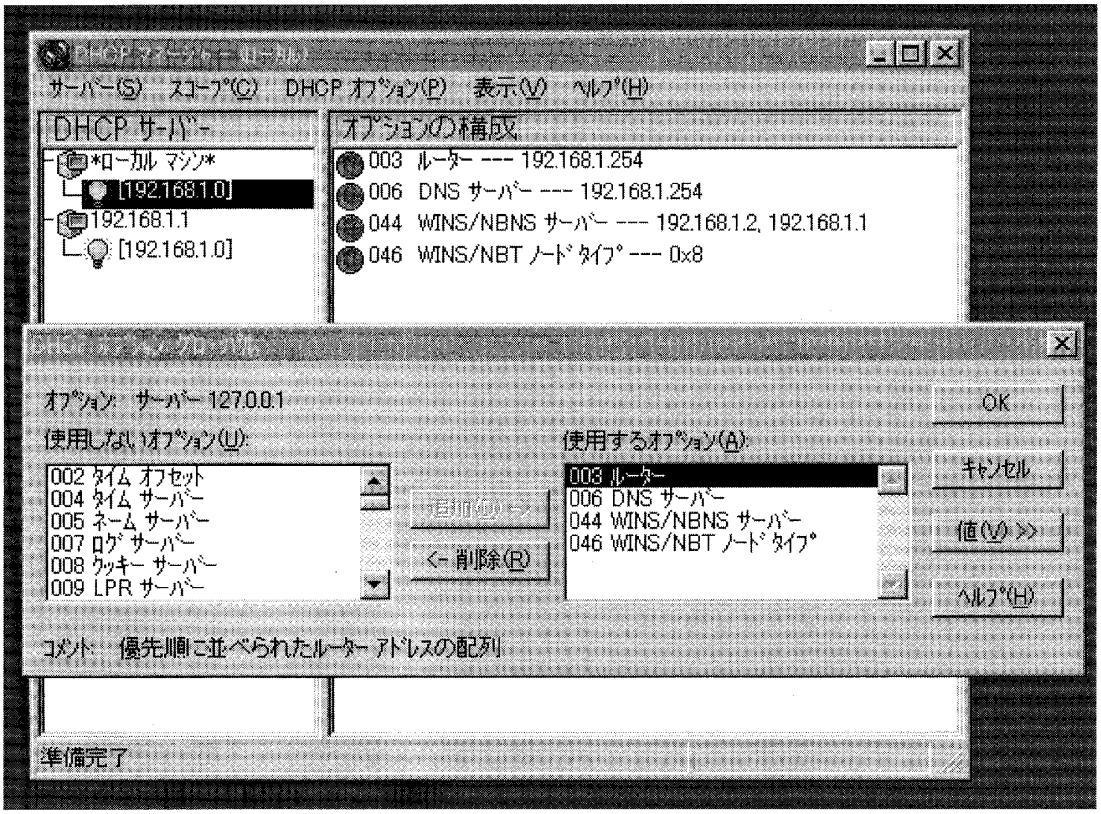

図3　スコープのオプション設定

Ⅱ．PDCが故障したときの対処法

ここで、通常の稼動時のPDCとBDCのコンピュータ名をそれぞれServerX、BackupXとして説明する。

PDCが故障したときでも、BDCが起動しているので学生機からログインはできる。しかし、ユーザープロファイルのパスやホームディレクトリのパスがServerXにあり、それが故障のためネットワーク上にないので、移動プロファイルやホームディレクトリにあるファイルを利用できない。そこで、BDCをPDCに昇格し、BDCのコンピュータ名をBackupXからServerXに変更する必要がある。BDCをPDCに昇格しないで、コンピュータ名だけを変更することもできるが、BDCではユーザーの追加や削除あるいはパスワードの変更といった管理作業ができないので、困る場合がある。そこで、ここではBDCをPDCに昇格する処方を考察する。

14

①BDCのサーバー・マネージャーでBDCをPDCに昇格する。このとき故障したPDCがドメインにないので、「PDCが見つかりません。昇格を実行すると、“ドメイン”の以前のプライマリ・ドメインコントローラーがオンライン状態にもどったときにエラーが発生する可能性があります。昇格を実行しますか？」ときいてくるが、「OK」をクリックする。

②ユーザープロファイルのホームディレクトリは￥￥ServerX￥Homeに設定さ

れているので、コンピュータ名をBackupXからServerXに変更する必要がある。従って昇格したばかりのPDCのコンピュータ名をServerXに変更し再起動する。このときWINSのデータを削除しないと名前の変更ができない場合もあるので注意する。

③WINSマネージャーを起動し、WINSのデータの削除をおこなう。方法はマッピング→データベースの表示→「所有者の削除」をクリックする。ここでBDCのコンピュータ名をServerXに変更したことによって、データベースに矛盾が生じるのでデータの削除をおこなっている。矛盾が生じる可能性があるのは、コンピュータ名がServerXとBackupXのデータだけであるが、一応すべてを削除している。このあとコマンドプロンプトで>nbtstat -RRと打つ。ここでWINSサーバーに登録されたこのコンピュータのNetBIOS名を更新している。

④コントロールパネルの「サービス」で「Microsoft DHCP Server」のサービスを開始する。

⑤通常稼動時に、BDCの学生のホームディレクトリに対して、共有とアクセス権の設定をしていない時には、ここで、学生のホームディレクトリに対して共有の設定とセキュリティの設定をおこなう必要がある。このときそのホームディレクトリにあるすべてのファイルに対してアクセス権の設定をおこなうので、学生数が多いと非常に時間がかかる。本学では1,000名程度の学生がいるが、その場合5

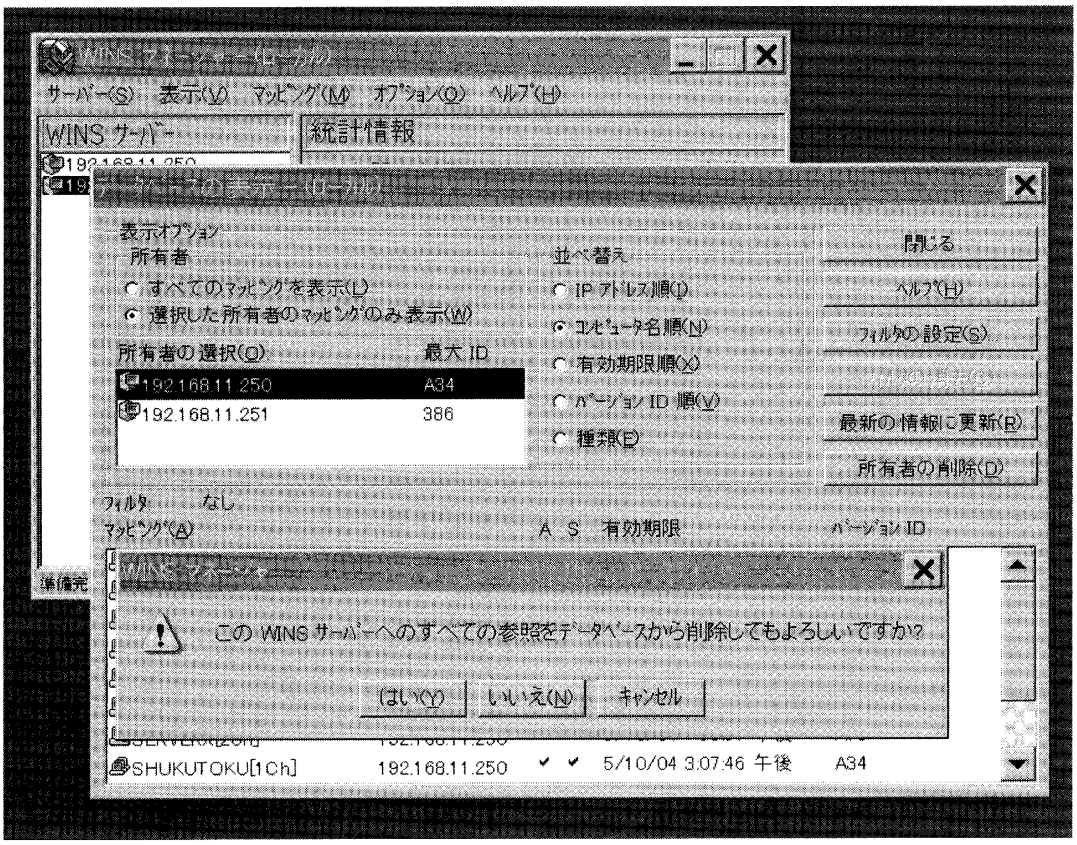

図4　WINSのデータの削除

時間程度かかった。（この時間は当然コンピュータの性能による。）従って通常の稼動時に共有とアクセス権の設定をおこなっておかないと、5時間以上サーバーを利用できないことになる。

Ⅲ．以前のServerXの修理が終わり復帰してきたときの対処法

BackupXはあくまでServerXが故障したときの予備であり、PCとしての性能はSeverXより劣るので、ServerXの修理が終わり稼動できるようになれば、これをまたPDCに戻す必要がある。そのためには、クライアント機がログオンしないようにしてから、以下の作業をおこなう。

①PDCのコンピュータ名をBackupXに戻して再起動する。
②BackupXで「Microsoft DHCP Server」のサービスを停止する。
③戻ってきたPDC（ServerX）を起動させる。このとき二つのPDCが存在しているので、「プライマリ・ドメインコントローラはこのドメインで既に実行されています。」というエラーメッセージがでる。このときServerXではNet Logonサービスが開始していない。
④図5に示すように、ServerXをPDCに昇格させる。昇格できないときにはBackupXでServerXをドメインから削除し、BDCとして追加したあと、ServerXをPDCに昇格させる。

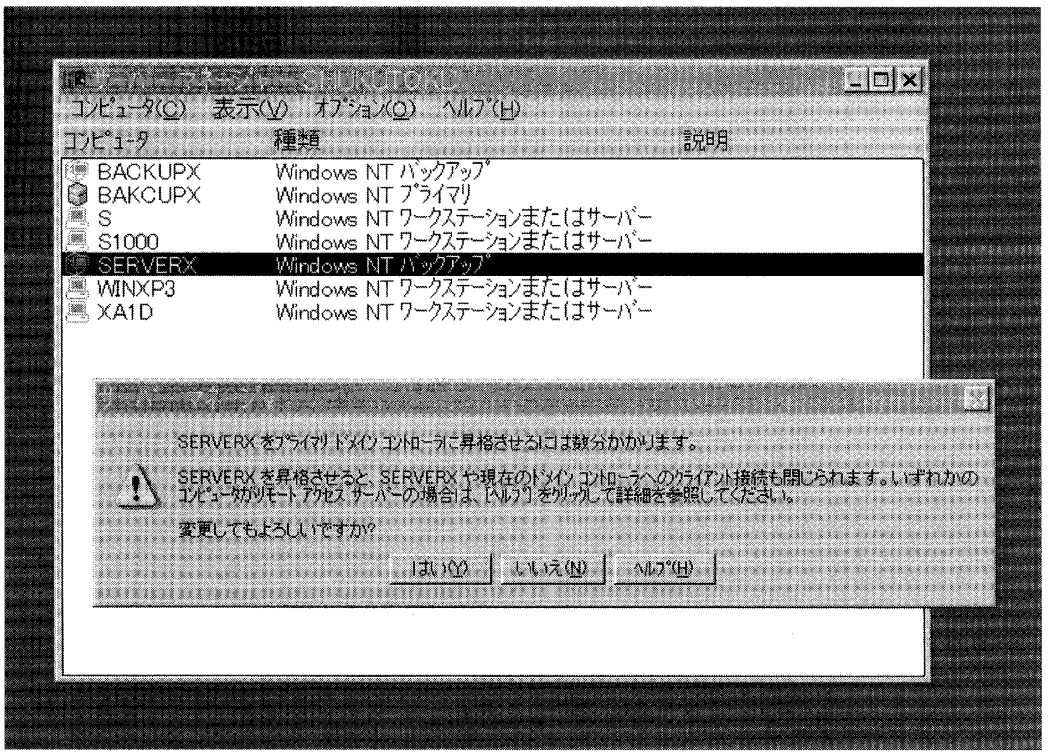

図5　BDCのPDCへの昇格

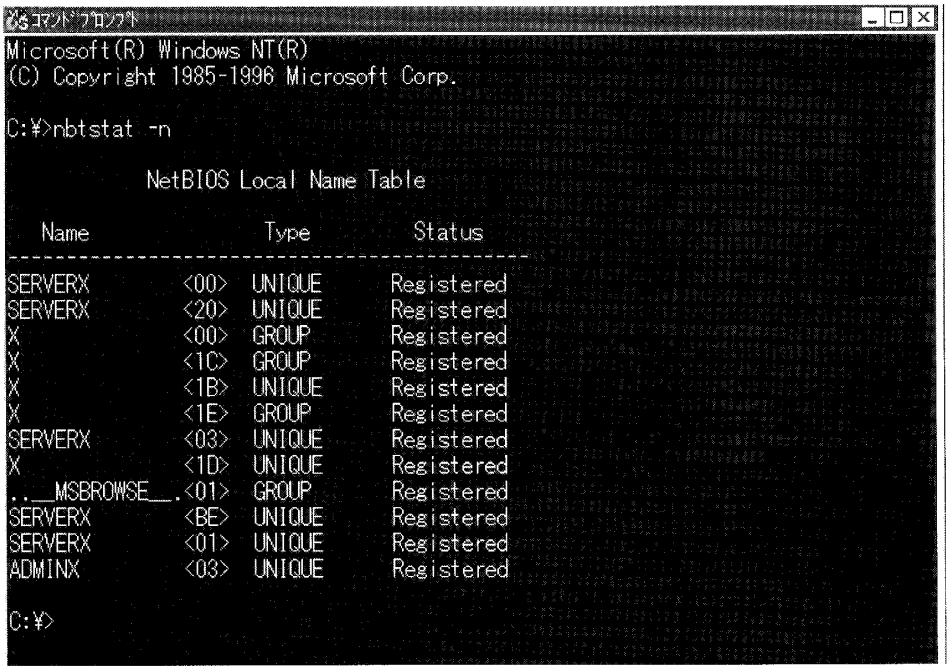

図6　コマンド nbtstat -n の出力

⑤ServerX で WINS マネージャーを起動して、WINS のデータをすべて削除し再起動する。このあと NetBIOS 名を更新させるために、コマンドプロンプトで >nbtstat -RR と打つ。

⑥BackupX で WINS マネージャーを起動して、WINS のデータをすべて削除し再起動する。このあとコマンドプロンプトで >nbtstat -RR と打つ。

⑦図6に示すように、>nbtstat -n を二つのドメイン・サーバーで実行し、WINS のデータベースに衝突、矛盾がないか確認する。

⑧予備のサーバー BackupX には、ServerX が故障している間に学生が作成したファイル等が保存されている。ServerX にはこれらのファイルは保存されていないので、これらを BackupX からコピーする必要がある。このために BackupX において次のコマンドを実行する。

>XCOPY D:¥Home J:¥ /D /S /E /C /K

ここで、ネットワークドライブ ¥¥ServerX¥Home を J: に割り当てている。また上のコマンドでは日付の指定をしていないので、送り側の日付が受け側の日付より新しいファイルだけをコピーする。

17

まとめと考察

本論文では、サーバーのいろいろな故障対策を考えた。ハードディスクをRAID構成にすることや UPS を使用することなどは常識であるが、壊れやすい電源ユニットや冷却ファンなどに対しては、予備を事前に用意しておくべきであろう。しかし本学

のようにもう一つサーバーを用意して、それをBDCとして稼動させれば、万が一PDCが故障してもすぐにBDCをPDCの代わりにすることができるので、サーバーの故障対策にそれほど神経を使わなくてもよい。なぜならPDCとBDCの両方が同時に故障する確率は非常に小さいと考えられるから。

サーバーのバックアップは非常に大事であるが、本学の場合、サーバーのデータファイルは、PDCのディレクトリからBDCのディレクトリへ夜間にミラーリングをおこなっている。従ってテープではなくハードディスクへバックアップしていることになる。ブート・パーティションのバックアップについては、PDCにはテープ装置がついているので、テープにバックアップをとっているが、BDCにはテープ装置がないのでDドライブにNT Workstationをインストールして、デュアルブートにしている。バックアップをとるときにはDドライブから起動する。このときCドライブのシステムファイルは単なるデータファイルとなるので、同じハードディスクにバックアップをとることができる。この方法はコストが安くて簡単なので、特に学校の情報実習室のように保守の時間を設定してサーバーを停止させることができる場合には、非常に有効である。

通常の稼動時には、PDCはプライマリWINSサーバーに、BDCはセカンダリWINSサーバーに設定し、PDCだけでなくBDCにおいてもWINSサービスを開始している。WINSサーバーが複数あると一つのサーバーにアクセスが集中しないのでサーバーの負荷を減らすことができる。

DHCPの設定は二つのサーバーでおこなっておくが、通常の稼動時にはPDCにおいてのみサービスを開始しておき、BDCではサービスを停止している。

PDCが故障したときには、PDCをドメインから切り離し、BDCをPDCへ昇格させて、授業をおこなう。故障したPDCが復帰してきたときには、これを以前のようにPDCに設定して、故障の間PDCの役目を果たしてきたBDCを元に戻し、この間に授業で学生が作成したファイル等を復帰したPDCにコピーする。これらのことについての詳しい具体的な処方箋については本文で述べた。

メール・サーバーやWebサーバーなどのインターネット・サーバーは、ホスティングサービスを利用しているので、本学の情報実習室にはない。これらのサーバーはファイアーウォールの外に置かなければならないので、クラッカーの攻撃に常に晒されており、運営・管理が非常に大変である。セキュリティホールがあるとたちまち攻撃され、最悪の場合にはサーバーが乗っ取られ、他のサイトの攻撃の踏み台にされてしまう。筆者の考えでは、学生数が非常に多い場合は別であるが、インターネット・サーバーはホスティングサービスやレンタルサーバー等を利用して、プロバイダー等の外部の事業者に運営・管理を委託した方がコストが掛からないと思う。

NT Server 4.0のマイクロソフトによるサポートが2004年末をもって終了した。これによって2005年からは深刻なセキュリティ・ホールが見つかっても、パッチの提供が受けられなくなった。パッチを適用しないと、悪意のあるプログラムを使った攻

撃からサーバーを守ることができないので、NT Server のユーザーは Windows Server 2003 への移行を進めようとしている。

Windows Server 2003 の Active Directory を使うと、ユーザー認証から共有リソースへのアクセス権、コンピュータやプリンタ、組織単位などが階層構造の中で一元管理することができる。また企業ではたくさんの NT ドメインが乱立していて、その管理が煩雑になっているが、これらをわかりやすく統合できるという。しかし学校の情報実習室のシステムはそれ程複雑ではない。またグループ・ポリシーによるクライアントの一元管理は魅力的であるが、NT でも同じ機能を持つシステム・ポリシーがあり、これで充分用途が足りていて大きな不満はない。他に IntelliMirror によるソフトウェアの自動配布なども、もっと簡単な他の方法を用いているので、情報実習室ではあまり魅力はない。

NT サーバーを使用していて特に困ることはない。唯一本文の中で述べたように、Windows XP 用のプリンタドライバーを NT サーバーにインストールできなくて困ったが、これも本文で既に紹介した方法を用いてインストールすることができた。このように現在の状況に大きな不満がないので、Windows Server 2003 に早急にアップデートする必要性を感じていない。

しかしセキュリティ面で不安がある。NT サーバーはファイアー・ウォールの中にいるので外部から直接攻撃を受けることはない。またサーバー上ではセキュリティ面で一番危険と思われる IIS（Internet Information Service）を無効にしている。NT サーバーから Web サイトを閲覧するときには、ウィルスに感染する恐れがあるので、信頼できる Web サイト以外にはいかないようにしている。これらのことから、サーバーが直接ウィルスに感染することは考えられないが、学生が使用するクライアント PC がインターネットへ出ていって、ウィルスに感染することはあり得る。クライアント PC には瞬間復元装置が導入されているので、リブートすればクライアント PC のウィルスは削除されるが、その前に、感染したクライアント機からサーバーが攻撃される可能性がある。それを防ぐために NT サーバーにはウィルス対策ソフトを導入しているが、サーバーとして常に稼動していなければならないサービス・プログラムにセキュリティ・ホールがあった場合に、ウィルス対策ソフトだけで防御できるか不安である。

注

1）Windows NT によって管理されるネットワーク（NT ドメイン）で、ユーザーやセキュリティに関する情報を管理し、ユーザー認証を行なうサーバー。

2）Windows NT ドメインで、PDC の持つユーザーやセキュリティに関する情報をコピーし、PDC に代わってユーザー認証を行なうサーバー。PDC はドメインに一台しか置くことはできないが、BDC はいくつでも置くことができる。また、BDC の一つを PDC に昇格させることができる。

3）Security Account Manager の略。ドメインコントローラが持っているユーザー、グループ、マシンのアクセス権限の情報等のユーザーアカウントに関するデータベースを管理する機能のこと。

4）ハードディスク等の指定したディレクトリ以下のディレクトリとファイルをバックアップ側で全く同じにすること。つまりマスター側で新しく作成したディレクトリとファイルをバックアップ側でも作成し、マスター側で消してしまったディレクトリ、ファイルをバックアップ側でも削除して、常に二つのディレクトリの内容を全く同じにしておくこと。

5）学校の情報システムでは、一時的にサーバーを停止してもあまり支障がないので、この機能の必要性は低い。

6）UPS の動作に関するイベントや電源状態（停電・電圧異常・自動シャットダウン・自動リブートなど）を時系列で表示する機能。

7）Network Attached Storage の略。ネットワークに直接接続する形式のストレージデバイス。いわゆる専用ファイルサーバーのこと。

8）Windows Server 2003 に標準搭載されている NTBackup は、ブート・パーティションのバックアップをディスク上にとることができる。また、「自動システム回復」という機能があり、C ドライブの内容をそのままバックアップし、システムを回復するときにはそれを自動的にリストアする。しかしこれらの機能は NT Server や Windows Server 2000 にはない。「修復セットアップ」という機能があるがバックアップの対象がレジストリやいくつかのシステム・ファイルだけであって、C ドライブのバックアップとは到底いえない。

9）RAID に対応し、Windows が稼動中であってもサーバーのイメージ・コピーができる製品がある。（株）ネットジャパンの「PowerQuest V2i Protector 2.0 Server Edition」である。しかしサーバー用のソフトウェアなので高価である。アカデミック 1ライセンスで￥192,000。

10）Winbat32.exe については、清水洋平氏のホームページ（http://hp.vector.co.jp/authors/VA000007/）を参照してください。MirrHome.btw のなかでディレクトリのミラーリングをおこなっている。

11）本学では、学生が情報実習室を利用する最初の授業で、学生のアカウントの登録をしている。

12）PC のネットワークサービス用 BIOS の API インターフェイスのこと。NetBIOS では、通信先の相手ノードは16バイトの名前（NetBIOS 名）によって識別されている。

13）DHCP スコープをアクティブにするには、「スコープ」メニューの「アクティブ化」をクリックする。

14）ノードタイプは NBT（NetBIOS over TCP/IP）環境における名前解決の方法を指定する。例えば、h（hybrid）ノードを指定したときには、まず NetBIOS ネーム・サーバー（WINS サーバー）を利用して名前の解決をおこない、それが失敗するとブロードキャストを利用する。

参考文献

1）小杉誠司「情報実習室のトラブル対策Ⅰ」『淑徳短期大学研究紀要』第44号，2005，p119-136.

21