淑徳短期大学研究紀要第44号（2005.2）

情報実習室のトラブル対策Ⅰ

小　杉　誠　司

（2004年9月23日受理）

要　約

情報実習室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論じた。次にWindowsの起動ドライブを専用のツールを用いてイメージ・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の紹介と、たくさんある瞬間復元ツールのなかから適切なものを選択する際のポイントについて論じた。情報実習室の課題はここで論じたトラブル対策だけではなく、ウィルス対策などもある。これらの問題を総合的に捉えたときに、本稿で考察した手法をどのように組み合わせて導入したらよいかについて考察した。

キーワード　クライアント管理　障害復旧　システム・ポリシー　イメージ・バックアップ　瞬間復元ツール

はじめに

情報教育の必要性が叫ばれ、パーソナル・コンピュータ（PC）を使った授業が増えると、それに伴い情報実習室のトラブルも増える。日常的に実習室で起こるトラブルにはいろいろなものがある。ウィルスに感染したり、DLL[1)]ファイルやレジストリが壊れたためにWindowsが起動しない。ハードディスクのセクターが破損したために、起動しても動作が不安定である。学生が設定を誤って変えてしまったために、アプリケーション・ソフトが起動しないなどのトラブルの原因の多くは、ソフトウェアの異常によるものである。

本論文ではこれらのトラブルの対処法について考察する。まず最初に紹介する方法は、学生が誤った操作をしてトラブルを起こさないように、システム・ポリシーを利用して、学生が使用できるPCの機能を制限することである。具体的にはPCのコントロールパネルを利用できなくしたり、ネットワークを経由したサーバー上のファイルへのアクセスを禁止したり、システムの環境設定ファイルが存在するCドライブを

学生から見えなくすることなどがある。

しかし、このようにシステム・ポリシーを使って学生が使える機能を制限しても、トラブルの頻度は減っても、全くなくなるわけではない。どうしてもWindowsの起動ドライブであるCドライブのバックアップをとっておいて、トラブルが生じたときにリストアすることが必要になる。Cドライブのバックアップをとる方法として二つ紹介する。一つは、DドライブにもOSをインストールする方法である。Dドライブから起動すれば、専用のツールを使わなくてもCドライブのバックアップをとることができる。しかしこの方法にはライセンスの問題やWindowsが起動できなくなったときに使えないという欠点がある。

このようなときには専用のバックアップ・ソフトウェアを利用するしかない。ここではこのようなツールの一つである「Symantec Ghost [2)]」を紹介し、クライアントPCでフロッピーから起動し、ネットワークを経由してサーバーにハードディスクの内容を、バックアップ／リストアする方法について述べる。このツールは障害復旧のためだけでなく、情報実習室にPCを新規導入する際に、標準的なPC環境を一括してセットアップするのに使うこともできる。モデルPCのハードディスクのイメージを他のPCにコピーすると、二つのコンピュータ名やSID [3)]などが同じになってしまい、そのままではネットワーク上で共存することができない。この問題を解決するユーティリティであるGhost Walkerについても紹介する。

ユーザーの誤操作でWindowsのシステム環境を破壊したり、さらにハードディスクをフォーマットしても、ハードディスクの内容を簡単に復元できるツールがある。このような瞬間復元ツールをPCにインストールしておくと、再起動するだけで完全に元の状態に戻すことができる。このようなツールの一つであり、本学で導入している「瞬快 [4)]」について紹介する。

「瞬快」の他にも多くの瞬間復元ツールがある。次にそれらのツールを選択する際の要点について考察する。ネットワークを経由してクライアントPCをリモートで管理する機能は必須である。またこれらのツールの選択の際には、どうしても瞬間復元の機能に目がいきがちであるが、実際にはサービスパックの適用やアプリケーションの追加など、環境を変更しなければならない必要がたびたび生じるので、これらの作業が簡単にできるツールを選択することが大切である。その他にも、余分な作業がちょっとしたものであっても、操作するPCの台数が多いと案外面倒になるので、選択の際にはよく吟味する必要がある。またGhostのようなイメージング・ツールを併せて導入するときには、そのツールとの相性も検討しなければならない。

情報実習室の管理者がやらなければならないことは、不調に陥ったPCの復旧作業などのトラブル対策だけでない。サービスパックの適用や、ソフトウェアの追加やバージョンアップといった作業、さらにはウィルス対策もある。最後に、これらの問題を総合的に捉えて対処法を考えたとき、本稿で紹介したシステム・ポリシーやGhostのようなイメージング・ツールさらに瞬間復元ツールなどを、実際にどのように組み

合わせて情報実習室へ導入したらよいかについて考察する。

システムポリシーを用いた機能の制限

学生が勝手にディスプレイの設定を変更してしまう。エクスプローラの操作中に誤ってシステムに必要なファイルを削除してしまう。またネットワークを通してアクセスして欲しくないデータにアクセスする。これらの行為はトラブルを引き起こし、システム管理者を困らせる。しかしこれらの操作をシステム・ポリシーで制限することができる。

システム・ポリシーを使うと、ネットワーク上のクライアント・コンピュータのシステム環境を一斉に変更することができる。例えばユーザーがデスクトップから実行できる操作や、コントロールパネルを使って設定できる対象を制限できる。ここで言うポリシーとは、ユーザーがログオンしたコンピュータのシステム環境を規定しているレジストリ設定のことである。

本学の情報実習室では、Windows NT サーバーをプライマリ・ドメインコントローラ[5]として設定しているので、システム・ポリシーを利用することができる。クライアント PC の OS は Windows XP である。クライアント PC をドメインに参加させるように設定すると、「リモート更新」がオンになり、自動的に標準のパス（¥¥プライマリ・ドメインコントローラのサーバー名¥netlogon）からシステム・ポリシーがロードされる。またシステム・ポリシーをダウンロードするパスを、手動で指定することもできる。

システム・ポリシーは、システム・ポリシー・エディタを使って作成する。システム・ポリシーを設定するには、まず最初に、「オプション」メニューの「ポリシー・テンプレート」を使って、ADM テンプレートを読み込む必要がある。設定することができるポリシー・オプションは、ポリシーの一覧であるこのテンプレートによって決まる。システム・ポリシーは次の二つのプロファイルで構成されている。「既定のコンピュータ」プロファイルは HKEY_LOCAL_MACHINE レジストリに、「既定のユーザー」プロファイルは、HKEY_CURRENT_USER レジストリに関連付けられたポリシーを制御する。これら二つのプロファイルの他に、ドメインの任意のコンピュータあるいは任意のユーザーやグループを追加して、そのシステム・ポリシーを設定することができる。例えば既定のユーザーの他に、教員のグループである「Teachers」を追加して、それぞれのポリシーを設定すれば、二つのグループに対するポリシーを区別して適用することができる。例えば教員に対しては利用できる機能の制限をしないでコンピュータを使用させるが、既定のユーザーである学生には機能を制限したポリシーを適用するといった使い方ができる。

特定のポリシーを有効にするには、制限をかけたい項目のチェック・ボックスをオンにする。特定のポリシーを無効にするには、対応する項目のチェック・ボックスを

オフにする。灰色表示になっている項目は、システム・ポリシー・エディタによって無視されるので、前回のログオン時の設定が有効になる。

ポリシー・ファイルは、Windows 95/98ではConfig.polという名前で、Windows 2000やWindows XPなどのWindows NTベースのOSでは、NTConfig.polという名前でnetlogonフォルダに保存する。ポリシー・ファイルがnetlogonフォルダに格納されると、ドメイン・コントローラは自動的にそのポリシー設定を有効にして、ユーザーがドメインにログオンすると、ユーザーのコンピュータはシステム・ポリシー・ファイルを読み取り、対応するポリシーを適用する。管理者が既存のポリシーを変更すると、ユーザーが次回ドメインにログオンしたときに、その変更内容が自動的に反映される。

重要なシステムファイルやフォルダなどを自由に操作できないようにしたり、システムに致命的なダメージを与える可能性がある危険なコマンドを使えないようにするなど、学生が使用する機能に制限をかけたいときによく使われる、ポリシー・プロファイルの「ユーザー」の設定項目について挙げると、次のものがある。

・コントロールパネルの「画面」を制限する
・「ファイル名を指定して実行」コマンドを削除する
・「スタート」メニューの「設定」からフォルダを削除する
・「スタート」メニューの「設定」から「タスクバー」を削除する
・「検索」コマンドを削除
・「ネットワークコンピュータ」から「ネットワーク全体」を削除する
・エクスプローラの標準のコンテキスト・メニューを使用不可にする

この項目を有効にすると、右クリックしてもエクスプローラの標準のコンテキスト・メニューが出現しない。

・選択されたドライブだけを表示する

この項目を有効にすると、マイコンピュータに選択されたドライブだけを表示するように設定することができる。例えばA:とZ:（ユーザのホームディレクトリ）だけを表示し、システムファイルがあるC:などを表示しないように設定できる。

学生が使用する機能に制限をかけることだけが、システム・ポリシーの利用法ではない。システム・ポリシーを使うとネットワークにつながったクライアントPCのシステム設定を一斉に変更できるので、非常に便利である。このように使用すると便利なポリシー・プロファイルの設定項目について挙げると、次のものがある。

「コンピュータ」の設定項目では

・リモート更新の更新モードを設定
・最後のログオンしたユーザ名を表示しない

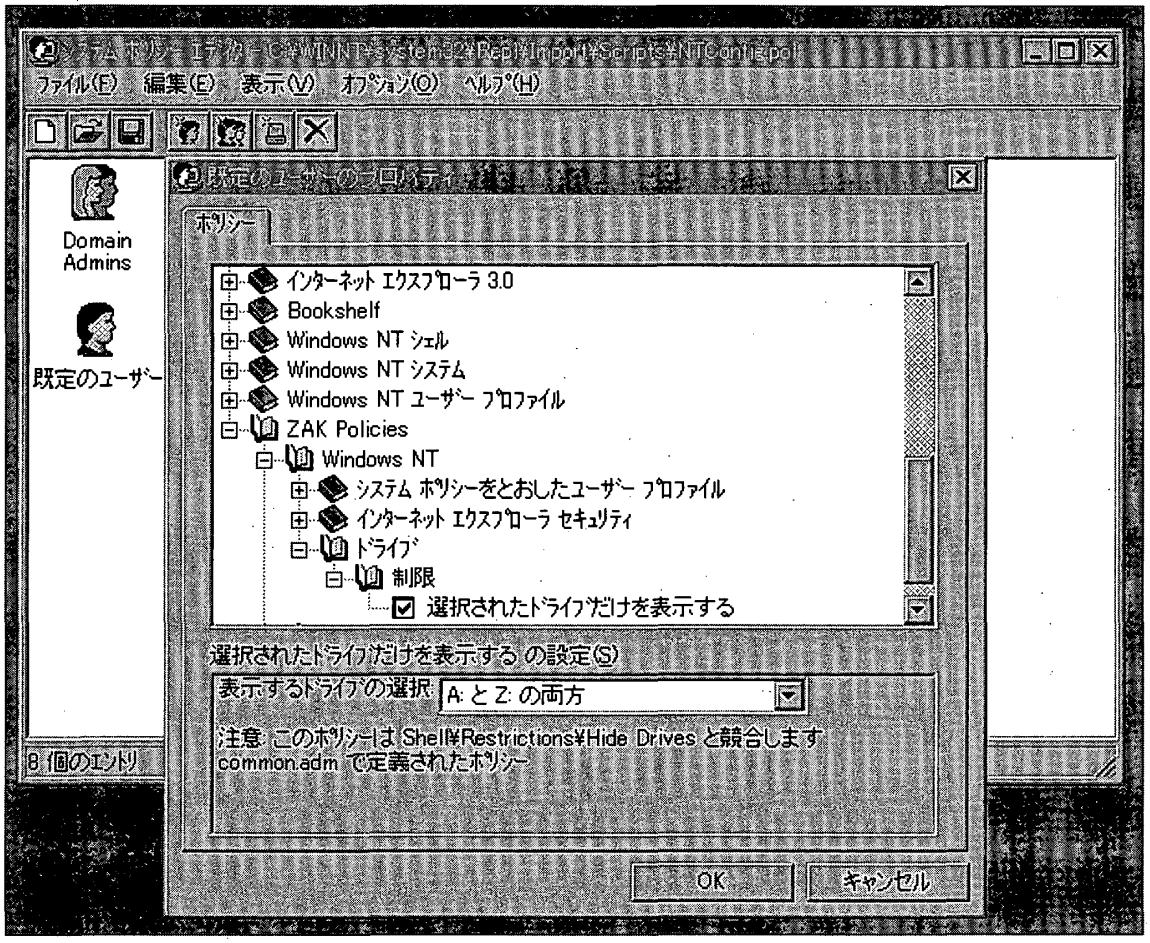

図1　ポリシー・プロファイルの設定項目「選択されたドライブだけを表示する」

・一時記憶された移動プロファイルのコピーを削除する

「ユーザー」の設定項目では

・ログオン時に numlock をオンにする

・longon サウンド消去

・longoff サウンド消去

・タスクバーの音量表示のオフ

・プロキシを使用可能にする

これをオンにし、プロキシ・サーバーのアドレスとポート番号を入力すると、クライアントのプロキシ・サーバーを一斉に設定することができる。このアドレスにわざと間違ったアドレスを入力すると、プロキシ・サーバーが見つからないので、当然インターネットが利用できなくなる。試験のときにインターネットの利用を制限したい場合に、この設定を使うと便利である。

・フォルダのカスタム設定

ここでは、

①デスクトップにおくアイコンを取得するパス

②プログラム・フォルダの項目を取得するパス
③「スタートアップ」フォルダの項目を取得するパス
を指定することができる。これらのパスをサーバー上におけば、一斉にこれらの項目を変更することができる。

・移動プロファイルでディレクトリを除外する

移動プロファイルを使用している場合、ログオフしたときにユーザープロファイルをサーバーに戻す。このときプロファイルのなかで戻す必要のないディレクトリ（例えばTemporary Internet Filesなど）を指定することができる。

Office10.admテンプレートを読み込むと、Office XPに共通するシステム・ポリシーの設定をおこなうことができる。例えばOffice XPのファイル・メニューにある「ツール」の「オプション」設定にある項目を設定することができる。

このようにシステムポリシーを使用して、学生が操作できる機能を制限しても、トラブル発生の頻度は減少するが、トラブル対策として万全ではない。このようにしてもハードディスクに書かれている重要なファイルが壊れることがある。

Cドライブのバックアップとリストア

OSやアプリケーション・ソフトにトラブルが生じた場合の対策としてまず考えられるのは、Cドライブの内容をバックアップしておき、異常が生じたときにリストアする方法である。しかしシステムの起動をおこなうブート・パーティションのバックアップやリストアは、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処理できない。

本学では学生機のOSがWindows NT Workstationのとき、Cドライブのバックアップをドライブに取ったことがあった。OSをDドライブにもインストールし、Dドライブから起動できるようにすると、Cドライブのデータを簡単にバックアップすることができる。[6] ただしDドライブにもOSをインストールするには、別にソフトウェアのライセンスが必要になる場合があるので注意が必要である[7]。

本学の情報実習室では移動プロファイルを使用しているので、学生がOffice等で作成したファイルやプロファイルはサーバーに保存されている。従って、スタンドアロンでPCを使用している場合と違い、これらのファイルをCドライブから他のドライブに移動させておく必要はない。もし移動プロファイルを利用していない場合で、学生が作成したファイルやアプリケーション・ソフトの設定ファイルがある場所が、Cドライブのままであるときには、他のドライブに移動させておかないと、Cドライブをリストアしたときに、ユーザのデータが上書きされてしまうので、注意が必要である。

通常の使用ではCドライブからOSを起動する。トラブルが生じたらDドライブか

ら起動し、Dドライブに保存してあるCドライブのバックアップを、Cドライブにリストアする。こうすることによって、間違って変更してしまったCドライブの内容を、ミラーリング・ソフトウェアを使って簡単に、時間をかけずに元に戻すことができる。

この方法の欠点は、すべてのクライアントPCのDドライブにOSをインストールしなければならないことと、設定を変更したり新しいソフトウェアをインストールして、Cドライブの内容を変更する度に、この新しい内容をDドライブのバックアップに反映しなければならないことである。もっともすべてのクライアントPCでバックアップをとる必要はないかもしれない。一つの情報実習室に導入されているPCは通常は同じ機種なので、一つか二つのPCに対してのみバックアップをとれば十分である。バックアップをとらなかったPCにトラブルが発生したときには、Dドライブから起動し、ネットワークを経由してバックアップをとったPCからリストアをすればよい。[8)]

上で紹介した方法は、PCを購入したときに付属品としてついてくるリカバリーCDを利用する方法とは少し違う。リカバリーCDを使えばOSとOfficeの再インストールまではリストアできるが、できるのはそこまでであって、その後にユーザーがおこなった他のソフトウェアのインストールや様々な設定作業は、またもう一度おこなわなければならない。このことに多くの時間がかかってしまう。しかし上で述べた方法では、すべての設定が終わった後にCドライブの内容をバックアップしているので、リストアすればそのまま使えるから、所要時間は少なくてすむ。

突然のトラブルでPCが起動しなくなってしまうことはよくある。信頼性が増しているとはいえ、ハードディスクはまだ壊れやすいデバイスである。ハードディスクが壊れれば、当然Windowsは起動しない。ハードディスクが正常であっても、OSのトラブルでWindowsが起動しないこともある。上で述べた方法では、このようなとき、どうしようもない。Windows XPにはバックアップ・ソフトウェアが添付されているが、PCが起動しない場合には、やはり使えない。

このようなときのために専用のバックアップ・ソフトウェアがある。これらのツールは、ハードディスクをディスク単位、あるいはパーティション単位で丸ごとイメージ・ファイルとしてバックアップし、リストアすることができる。現在、イメージング・ツールは、基本的な機能を持った個人のクライアントPC向けと、法人向けの2種類が存在する。法人向けには、多数のPCで利用するためのソフトウェア・ライセンス体系や、サーバーから多数のクライアントPCに同時にイメージを転送できるネットワーク機能がある。さらにネットワーク経由でサーバー側からクライアントPCを管理する機能などもある。

本学では、法人向けのツールである「Symantec Ghost」を利用している。実は、このツールはいま論じている障害復旧のためではなく、PCの新規導入の際に、標準的なPC環境を一括してセットアップするツールとして導入したのであるが、個別のPC環境のバックアップやリストアに利用することもできる。

Ghostによるイメージ・ファイルの作成は、いくつかの方法で行うことができるが、ここではサーバー上でGhost Castを使い、ネットワーク経由でイメージ・ファイルをモデルPCからサーバーへダンプする手順と、サーバーからクライアントPCにイメージ・ファイルをロードする手順について説明する。まず適当なPCをサーバーにして、そのPCにGhost標準ツールをインストールする必要がある。次にそのサーバー上でGhostブートウィザードを起動し、「ネットワークブートディスク」を選択して、ネットワークサポート付きのブートディスクを作成する。手順の詳細は省くが、簡単に作成できる。ただクライアントPCにインストールされているネットワークカードのドライバーを、選択することが若干難しい。

Ⅰ．イメージ・ファイルをクライアントPCからダンプする手順

イメージを取る前にモデルPCがドメインに参加しているときには、ドメインからから抜けておく。

①Ghost Castサーバーのスタート・メニューで、「プログラム」→「Symantec Ghost」→「Ghost Castサーバー」の順に選択して、Ghost Castセッションを開始する。
②セッション名を入力する。例　room1。
ここで記入するセッション名と、クライアントPCで記入するセッション名を合わせることで、イメージをダンプ／ロードするクライアントPCを特定している。複数台のPCにイメージをロードする場合には、各PCで同じセッション名を入力することになる。
③「クライアントからダンプ」を選択する。
④イメージ・ファイル名と保存する場所の絶対パスを入力する。
⑤パーティションのイメージを取る場合は、「パーティション」を選択する。
ディスク全体のイメージを取る場合は、「ディスク」を選択する。
⑥「クライアントを受け入れる」をクリックし待機する。
⑦モデルPCで「ネットワークブートディスク」挿入し、フロッピから起動し、Ghost.exeを実行する。
⑧Ghostメニューで「Ghost Cast」を選択する。
⑨Unicastを選択する。
⑩セッション名を入力し「OK」をクリックする。②で入力した名前と同じ名前にする。
⑪ダンプするディスクを選択して「OK」をクリックする。
⑫必要に応じてダンプするパーティションを選択して「OK」をクリックする。
⑬圧縮率を選択する。（Fastを選択した。）

⑭「Yes」をクリックする。
　このあとダンプが開始する。

Ⅱ．サーバーからクライアントPCへイメージ・ファイルをロードする手順

上で述べたイメージ・ファイルをクライアントPCからダンプする手順とほとんど同じである。相違点を以下に述べる。

③で「クライアントにロード」を選択する。
④ではロードするイメージ・ファイルを選択する。
⑨ではコピー先のPCが一台の場合は「Unicast」を選択し、複数台のときには「Multicast」を選択する。
⑬の圧縮率は選択する必要がない。

トラブルが生じた1台のPCに対してのみ、イメージをロードするときにはこれでよいが、PCの新規導入のときのように、複数台のPCへロードするときには、⑦から⑭までの操作をコピー先のすべてのPC上でおこなう必要がある。このあとGhost Castサーバーで「送信」をクリックするとファイルのロードを始める。転送が完了

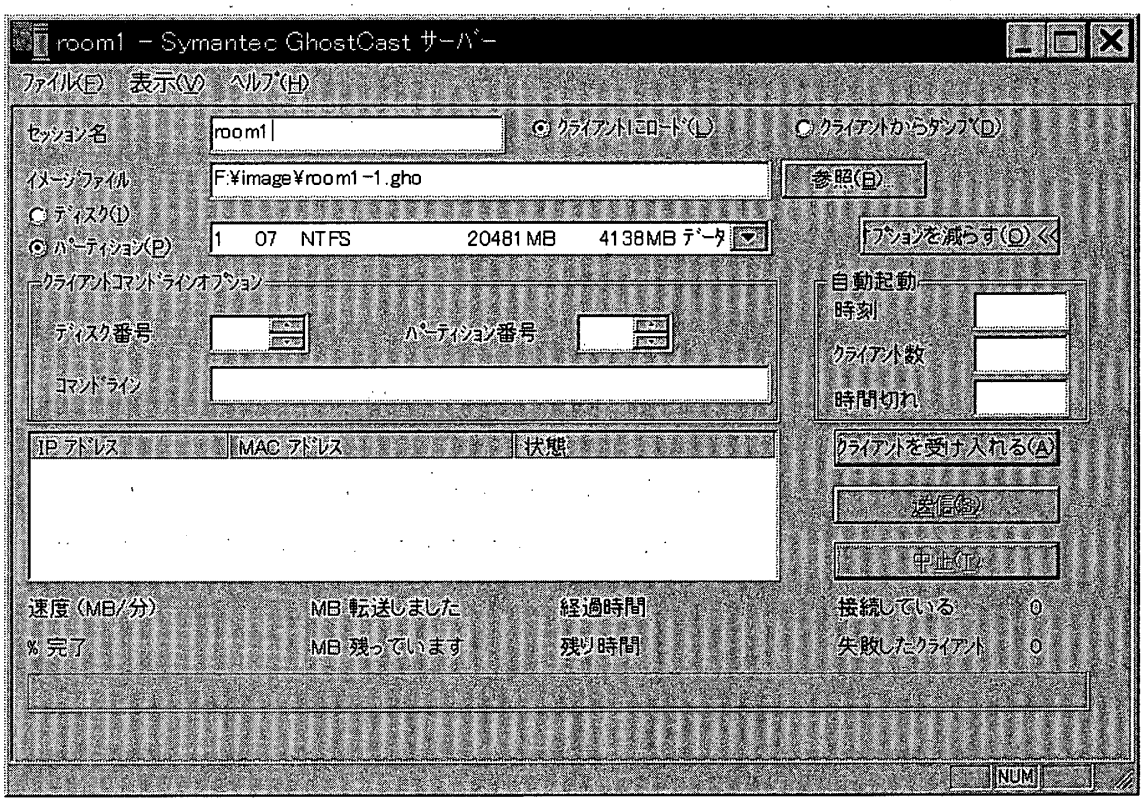

図2　Ghost Cast のサーバーの設定画面

したらサーバー上で「OK」をクリックし、Ghost Cast セッションを終了させる。

モデル PC のハードディスクのイメージを他の PC にコピーすると、当然のことながら、二つのコンピュータ名やSIDなどが同じになってしまい、そのままではこれらの値が競合して、ネットワーク上で共存することはできない。この問題を解決するために「Symantec Ghost」では二つの方法を提供している。一つはマイクロソフトが提供する SysPrep ユーティリティを用いる方法、もう一つは Ghost Walker とよばれるユーティリティを用いる方法である。

ここでは Ghost Walker を用いる方法について述べる。[9] Ghost Walker はクライアント PC にイメージをロードした後、再起動しないで SID を変更できる。またコンピュータ名やコンピュータ SID だけでなく、クライアント PC のすべてのユーザー SID を変更することができる。

①クライアント PC で D OS を起動し、コマンドラインに ghstwalk と入力する。
②Enter を押すと、PC 上にあるすべてのボリュームを表示する。
③ PC 上に複数の OS がある場合は、System ID を入力する。また「Change Additional Vols」を選択し、SID を更新する必要があるブート不能ボリュームを追加する。
④Nと入力し Enter を押し、新しいコンピュータ名（以前のコンピュータ名と同じ長さにする必要がある）を入力する。
⑤Enter を押すと、しばらくして新しいコンピュータ名と新しいSIDが表示される。

Ghost Walker を終了したあと、Windows を起動し、ドメインへコンピュータ・アカウントを追加する必要がある。

瞬間復元ツールによる環境の維持・復旧

ユーザの操作ミスで、ハードディスクをフォーマットしたりファイルを削除したりすると、OS が起動できなくなり他の利用者に影響を及ぼす。またユーザが雑誌の付録 CD-ROM に入っているソフトウェアの試作版をインストールして、PC が不安定になったりすることもある。またデスクトップのアイコンがなくなっていたり、操作ミスで環境を破壊することもよくある。このような場合には、OS やアプリケーション・ソフトの再インストールをしなければならないケースも稀ではない。これらの復旧作業やバックアップ作業をシステム管理者自身でおこなわなければならず、システム管理者の大きな負担となっている。保守契約を結ぶことも可能であるが、次の授業に支障をきたすような急を要する場合には、システム管理者自身が対応せざるを得ない。また保守料金の予算を獲得するのもなかなか難しい。

このようなときに環境の瞬間復元ツールを導入すれば、ハードディスクに誤ってデー

タを追加したりあるいは削除しても、また利用者が勝手にPCの環境を変えても、再起動するだけで完全に元の状態に戻すことができる。

瞬間復元ツールにはいろいろな種類があるが、ここでは本学で導入している「瞬快」について最初に説明する。「瞬快」には、「特上」と「上」と「並」の3種類の製品があるが、本学で導入しているのは「並」である。

「並」では、保護したいハードディスクの内容を自動復旧することができる。設定できる修復対象は、ドライブ単位あるいはファイル/フォルダ単位で指定する。「保護モード」にしておけば、ハードディスクに変更が加えられても、自動的に環境を復旧することができる。ハードディスクの状態を元に戻したくない場合には、「更新モード」にすればよい。「更新モード」にした後の環境は維持される。また各クライアントPCに対する動作モードの変更などを、リモートで一斉におこなうことができる。

「瞬快」のインストールの前にしておくべきことは、すべてのハードウェアとソフトウェアをインストールし、システム環境の設定作業を完了しておくことである。そのあと保護するハードディスクの領域に不良セクタがないかどうかチェックし、更に断片化したファイルがないようにディスクの最適化をおこなう必要がある。インストールは非常に簡単で、環境設定画面を表示するために必要となるパスワードの設定、図3に示した環境設定画面での設定、それに修復実行のタイミングの選択だけである。例えば図4に示したように「毎回起動時」を選択すれば、起動時にハードディスクの状態が修復される。

クライアントPCに「瞬快」の「並」をインストールした後、アプリケーションの追加や削除、システムの設定の変更など、ハードディスクの内容を変更したい場合には、「個別環境の変更」のモードを使う。その手順を以下に簡単に説明する。

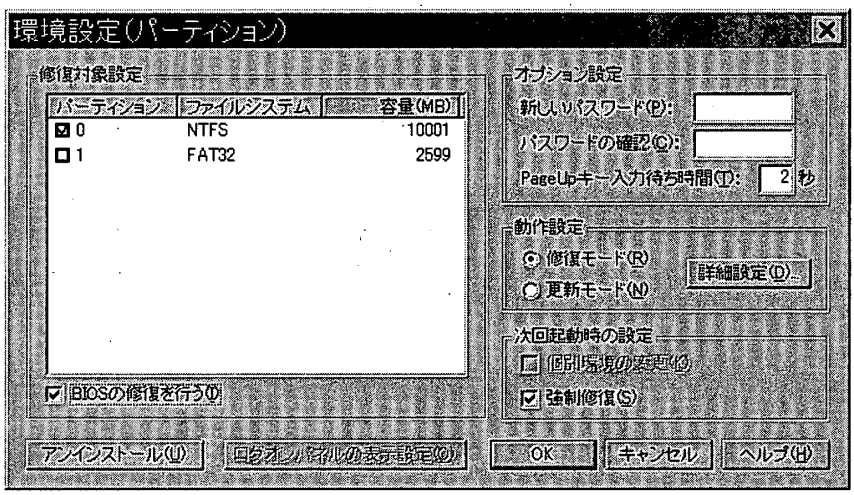

図3 「瞬快」のパーティション単位の環境設定画面

①図3の環境設定画面で、「瞬快」の動作設定を「更新モード」に変更すると、コンピュータが再起動する。
②アプリケーションのインストールやシステムの設定の変更などをおこなう。
③変更した内容が正常に動作することを確認した後、再起動する。
（この段階で不具合が生じた場合には、元の状態に戻すことができる。）
④環境設定画面で、「個別環境の変更」にチェックを入れ、「OK」をクリックし再起動をおこなうと、個別環境が変更される。このとき以後の動作を修復モードにしたいときには、「修復モード」を選択しておく。このすぐ後で説明するように、クライアントに対する①、③、④の操作は、リモートで一斉に操作することができる。

「瞬快」では、リモートで複数のクライアントPCを一斉に操作して、電源のON／OFF／再起動、動作モードの変更ができる。ネットワークに接続されていないPCに対しては、リモート操作を使わずに各クライアントPCで、これらの操作を個別におこなうこともできる。ネットワークに接続されていても、一台だけクライアントPCの動作モードを変更したいときもあるので、個別に動作モーを変更できるのは便利である。リモート管理機能を利用するには、リモート操作をおこなうPC（これがサーバーになる）にリモート管理機能をインストールする。さらにグループを作成し、そこに管理されるクライアントのコンピュータを登録しておく必要がある。

リモート管理機能を利用したクライアントの操作手順について、以下に簡単に説明する。

①リモート管理機能を起動する。
②リモート操作するクライアントを選択する。
③動作モードを変更すると、各クライアントが再起動し、動作モードが変更される。

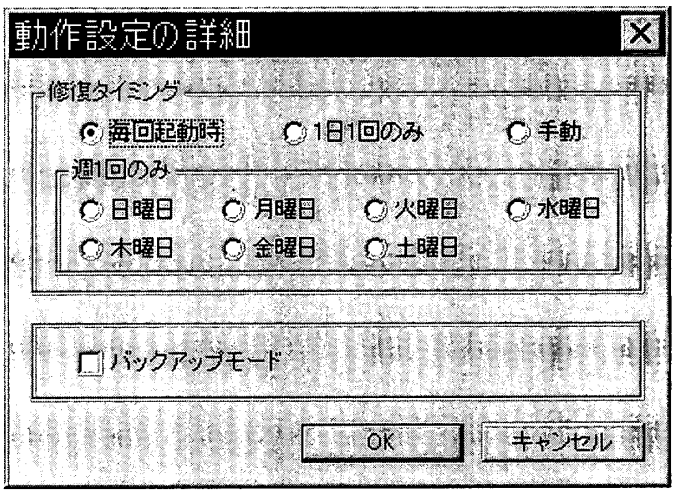

図4 「瞬快」の動作モードの詳細設定画面

「瞬快」では、Ghostのようなイメージング・ツールを用いて、「瞬快」がインストールされたハードディスクの状態を、ディスク・イメージとしてクライアントPCに展開することができるので、それぞれのクライアントに個別に一台づつ「瞬快」をインストールする必要がない。ただし、このときの動作モードを「バックアップモード」にしたものを、ディスクイメージにとる必要がある。

「瞬快」に限ったことではないが、瞬間復元ツールを使用していれば、もしウィルスに感染したとしても、再起動すれば保護しているハードディスのドライブはウィルス感染前の状態に戻るから、瞬間復元ツールはウィルス対策にもなる。但しMelissaなどのWindowsが動作中に発症するウィルスに対しては、復元する前にウィルスが活動するのを止めることはできないので、その対策は万全とはいえない。ワクチンソフトを導入すると、ウィルスのパターンファイルを絶えず更新しなければならないが、瞬間復元ツールを利用しているとファイルを元に戻してしまうので、この更新操作に手間がかかる。しかし「瞬快」では、リモート操作コマンドをスケジューリングすることで、決められた時間にウィルスのパターンファイルの自動更新処理が行うことができる。

その他に「瞬快」では、BIOSに変更があった場合も自動的に元の状態に復元することができる。またWindowsとLinuxのマルチブート環境を構築することもできる。しかしLinuxがインストールされた領域を復元することはできない。またフロッピーディスクからPCを起動した場合には、ハードディスクの復元はできない。

「瞬快」の「上」では、「並」の機能の他に、OSの環境設定やアプリケーションを

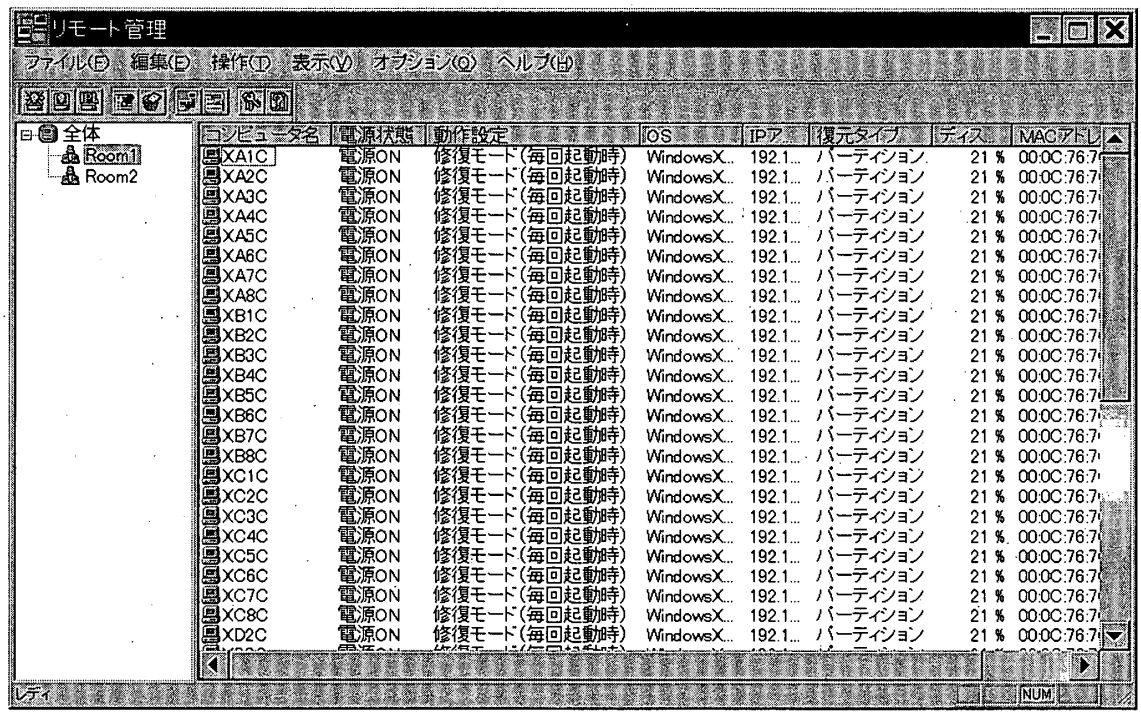

図5 「瞬快」のリモート管理機能の設定画面

各クライアントに配付できる。またファイル配付や配付後のバッチファイルを実行したり、OSやOffice等のセキュリティパッチを各クライアントへ配付適用することができる。しかし、OSのサービスパックを「瞬快」をインストールした後に適用する場合は、上で述べた「アプリケーションの登録／配付」機能を利用することができない。「個別環境の変更」機能などを使用してクライアントにサービスパックを適用する必要がある。Internet Explorerを後からバージョンアップする場合も同様である。

「瞬快」の「特上」では、上で述べた「上」の機能の他に、サーバーに登録した雛型のディスク・イメージをクライアントにマルチキャスト配信できる。またBIOSのアップデートプログラムや変更したBIOSの設定情報をクライアントに配布することができる。しかしサポートしているクライアントPCは富士通のFMVシリーズだけである。[10)]

瞬間復元ツール選択のポイント

「瞬快」以外にも多くの瞬間復元ツールがある。具体的に挙げると、「HDD Keeper」[11)]、「NetEasyRecovery」[12)]、「ウォッチドッグ」[13)]、「SAFETYPRO」[14)]、「DeepFreeze」[15)]、「コムガード」[16)]などがある。これらのツールを選択する際の要点について考察する。

学校の情報実習室のように20台以上のPCにツールを導入する場合には、ネットワークを利用した学生機のリモート管理機能は必須である。この機能があると一斉に動作モードを変更する際に、非常に便利である。しかしファイルの一斉送信やバッチジョブの実行などは、学生機がWindowsのドメインに参加している場合には、ログオンスクリプトにそれらのコマンドをかいておいて、実行させればよいので、必ずしも必要ないと思う。

瞬間復元ツールには大別してハードウェアタイプとソフトウェアタイプがある。ハードウェアタイプには、「HDD Keeper」、「ウォッチドッグ」、「SAFETYPRO」などがあり、これらのツールではPCIスロットにボードを差し込む。[17)]ハードウェアタイプでは、PCIボードがBIOSレベルからコンピュータの動作を監視しているので、フロッピーディスクから起動した場合でもハードディスクを保護することができる。しかしソフトウェアタイプのものは、ハードディスクから起動を開始した時点でツールのソフトウェアが動作するため、フロッピーディスクで起動した場合にはハードディスクを保護しない。[18)]ハードウェアタイプの方がよりセキュリティが高いと言える。

しかしBIOSの設定でハードディスクからの起動を第一順位にすれば、フロッピーからの起動はできなくなるので、この欠点を一応解決することができる。しかし管理者が学生機を管理する際に、フロッピーから起動しなければならないときもある。そのときにはBIOSの設定を変更しなければならず、面倒である。

ノートパソコンではPCIボードを差し込めないので、ソフトウェアタイプしか利

用できない。デスクトップパソコンにはハードウェアタイプを使用したほうがセキュリティが高くなるが、ハードウェアタイプの欠点は、すべての学生機にハードウェアを装着しなければならないことである。学生機が100台ある場合、管理者がすべてのPCの筐体を開けてハードウェアを装着するのは大変であろう。

瞬間復元ツールのインストールのあとも、アプリケーションの追加やサービスパックの導入など、環境を変更しなければならないときが度々生じるので、この作業が簡単なツールを選択することが重要である。このとき動作モードを変更してから追加・変更をおこなうが、そのあとツールによってはデフラグを実行しなければならないものがある。しかしデフラグには時間がかり、操作に手間取るので注意が必要である。

またWindowsのサービスパックの適用やInternet Explorerのバージョンアップの場合に、ツールを一旦アンインストールし、作業後にもう一度ツールのインストールを行うものがある。このようなツールの場合、リモート操作で一斉にツールのインストールとアンインストールができないと、学生機一台一台にこのような作業をしなければならず、非常に面倒である。

ちょっとした作業であっても、操作するPCの台数が多いと案外大変になるので、ツールの選択の際には操作の手順をよく吟味する必要がある。例えば、以前「HDD KEEPER」のソフトウェアタイプをデスクトップパソコンに利用したことがある。PCIスロットに機器を装着するのが手間だったので、ソフトウェアタイプを選択したのであるが、プリンタポートへロックコネクタを装着しなければならなかった。（PCIスロットに機器を装着するよりは、プリンタポートへロックコネクタを装着するほうがPCを開けなくてよいので、手間がかからないと判断したのである。）しかしこのコネクタを抜き差しするのが、ポートがPC本体の後面にあることと、生徒用のPCが50台近くあったために、案外大変であった。[19]面倒なのでずっと差したままにしていたら（差したままにしていても大丈夫であることを電話で確認していたが）、何台かのPCで、アンインストールのときにエラーメッセージがでた。

またこの「HDD KEEPER」をアンインストールするのが面倒であった。ハードウェアのアンインストールをまず最初にしてから、ソフトウェアのアンインストールをしなければならなかった。ソフトウェアタイプなので、これらのコネクタは本来必要ないはずである。どうも不正利用を防ぐために、ハードウェアのアンインストールの際に、ロックコネクタにツールのシリアル番号を戻しているようである。ハードウェアのアンインストールをしないでソフトウェアのアンインストールをすると、以後「HDD KEEPER」のインストールができなくなるので、面倒でもしなければならない。

瞬間復元ツールがインストールされているコンピュータ環境を、Ghostのようなコピーツールを使ってイメージ・ファイルを作り、それを雛型として残りのPCにコピーすることができないツールが多い。このようなツールの場合、インストールを学生機一台一台に個別におこなう必要があり面倒である。「瞬快」の場合には「バック

アップモード」にしておけば、イメージ・ファイルにしたものをコピーすることができる。またその後リモート管理機能を使って、動作モードを一斉に変更できる。

ほとんどの瞬間復元ツールがWindowsのマルチブートに対応しているが、WindowsとLinuxのマルチブートには対応していないものもある。授業でLinuxを使用するときには確認する必要がある。またマルチブートに対応していても、Linuxがインストールされているパーティションの瞬間復元をおこなうものはない。しかし「SAFETYPRO」は、LinuxとBSDに対してバックアップ復旧をすることができる。また「ウォッチドッグ」もLinuxに対してコピー復元での復旧ができる。また「DeepFreeze」はMacintosh（OSX以上）に対応している版もある。

まとめと考察

学校の情報実習室の管理者にとって、多くのクライアントPCを管理することは大きな負担となっている。同じ仕様のPCを一括して導入することでサポートの負担が軽減されるとはいえ、何らかの理由で不調に陥ったPCの復旧作業などのトラブル対策は、管理者に大きな負担を強いている。しかも実際にやらなければならないことはトラブル対策だけではない。サービスパックの適用やパッチを当てたり、あるいはソフトウェアの追加やバージョンアップといった作業もある。さらにはウィルスなどのインターネット・セキュリティにどう対処するかという問題もある。これらの問題を総合的に捉えて対処法を考える必要がある。

システム・ポリシーの使い方は機能を制限することだけではないので、学生にPCを自由に使わせるポリシーを優先した場合でも、システム・ポリシーを全く利用しないということは考えられない。またGhostのようなイメージング・ツールはPCの初期導入の際にはどうしても必要なツールである。例えば100台近くのクライアントPCにソフトウェアをインストールして環境を設定するときに、クライアントPCのシステム環境を同じにすることは、このようなツールなしでは非常に大変な作業であり、業者に依頼するにしても、その費用は馬鹿にならない。

瞬間復元ツールを使わずに、システム・ポリシーで学生が利用できる機能を制限しながら授業をおこない、それでもトラブルが発生したときには、イメージング・ツールを使ってCドライブの状態を元に戻すという情報実習室の運営方法も十分可能である。しかしこのときにはウィルス対策が全くできていないので、ウィルス対策ソフトを導入する必要がある。このときにはパターンファイルの更新をどのような方法で行うかという新たな問題が発生する。パターンファイルの更新は毎日のようにあるので、非常に煩わしい作業である。

瞬間復元ツールを使えば、ウィルス対策は完全ではないが、ある程度はできている。特に本学のように移動プロファイルを利用しているときには、学生がOffice等で作成したファイルはサーバーに保存されるので、サーバーにだけウィルス対策ソフトを

導入して、ウィルスチェックをおこなえばよい。このときにはクライアントPCにウィルス対策ソフトを導入する必要がないので、100台近くあるクライアントPCで煩わしいパターンファイルの更新をする必要がない。

勿論、瞬間復元ツールも使うが、万全を期してウィルス対策ソフトをクライアントPCに導入する運営方法もある。実際にどのようにするかは、予算や実習室の管理者がどの程度の時間を情報実習室の管理に充てることができるかなどの状況によって違ってくると思われる。

システム・ポリシーのところで論じたように、一方で、トラブルが発生しないように、学生が操作できる機能やソフトウェアを制限するという管理のポリシーがある。管理のポリシーを優先させると、学生が使用できる機能が制限されてしまうので、その制限された箇所の学習ができないという欠点がある。他方で、学生がすべての機能を自由に使用できるような環境にして、たとえ管理者の手を煩わせるような失敗をすることがあっても、できるだけ多くの操作を体験させて学習させるという学習のポリシーがある。学習のポリシーを優先させることが、学生の学習は制限されないので、教育的には望ましい。しかし実際には、この学習のポリシーと管理のポリシーが相反的な場合が多い。そのときにはこれらをどう調和させるか、どこで妥協するかという問題を検討しなければならない。瞬間復元ツールを使って環境を復元する場合には、トラブルが生じても、すぐにトラブルが生じる前の状態に戻すことができるので、学習のポリシーを優先させることができる。

注

1）Dynamic Link Libraryの略。Windowsにおいて、複数のアプリケーション・ソフトが共通して利用する汎用性の高いプログラムの部品のこと。
2）http://www.symantec.com/region/jp/products/ghost_enterprise/
3）Windows NT系のOSでは、コンピュータ、ユーザー・アカウントやグループなどは、管理ツールに表示される「名前」ではなく、「SID（Security Identifier、セキュリティ識別子）」と呼ばれる一意のID番号列を使用して管理されている。
4）http://www.ftk.fujitsu.com/products/shunkai/
5）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、ユーザ認証を行なうサーバー。
6）一般にはCドライブから起動したときに、Cドライブの内容を完全にバックアップすることは、特殊なソフトウェアを使わないとできない。Windows XPの場合も、NTと同じようにDドライブにインストールすることができる。
7）パッケージで購入したライセンスやプリインストールされた形態で購入したライセンスを、デュアル・ブートで利用する場合には、それぞれのライセンスが必要になる。それに対してボリューム・ライセンス・プログラムで購入したライセンスでは、1つのライセンスで1台に2つまでのOSをインストールすることができる。
8）この場合でも後で論じるSIDの問題は残るが、コンピュータのSIDはコンピュータ名

17

を変えて新たにドメインに参加しなおせば、ほとんどの場合に問題はない。

9）Ghost Walker には、新しいコンピュータ名がコピー元のコンピュータ名と同じ文字数でなければならないという制約があるが、SysPrep に比べて簡便で分かりやすい。

10）「瞬快」の「上」と「特上」の資源配布機能は「Selfmaintenance」という以前からあるソフトウェアをベースに作られているので、動作が重く、比較的高機能のサーバーが必要ときいている。

11）http://www.to-ei.co.jp/Av/sof/index.html

12）http://www.kansai-elec.co.jp/classroom/soft/ner/

13）http://www.introhightech.co.jp/

14）http://www.santec-net.co.jp/products/saftypro.html

15）http://www.knj.co.jp/hdds/hdds02.html

16）http://www.idk.co.jp/products/hdg/HDG-01B.html

17）「HDD Keeper」、「SAFETYPRO」にはソフトウェアタイプもある。

18）ソフトウェアタイプでも「SAFETYPRO」は、フロッピーから起動した場合でもハードディスクを保護できる。

19）最近では USB タイプも発売されたので、これならばポートが前面にあるので比較的に扱いやすいと思われる。

18