Virtual PC による Windows Server 2003，Exchange Server 2003 と ISA Server 2000 の統合運用

富　岡　恒　雄

（受付　2005 年 5 月 10 日）

1. は　じ　め　に

情報科学を学ぶ学生にとって，プログラミングに関する学習は重要な項目の 1 つである。それ故，筆者はゼミナールでの基礎教育として，アルゴリズムとデータ構造の理解を目的としたプログラミング演習を行ってきた。そこでは，抽象的なデータ構造の概念を理解し，それを基にして適切なアルゴリズムを選択し組み合わせ，プログラム言語で記述する一連の過程を体験させている。そのために，教材資料を使用して，講義と課題作成演習を組み合わせた形態での授業を行っている。

ところで，本学でもパソコン教室と学内外ネットワーク環境の整備が進められたことにより，プログラミングの授業において，学生が 1 台ずつコンピュータを使用し，プログラムを作成しなから演習を行うことが可能な体制になっている。また，ネットワーク上での教育環境の開発が個人や研究室のレベルで可能な状況である。

そこで，独自の教育目的と方針に沿った情報教育を側面から支援する環境として，まず，Windows NT Server と Exchange Server 5.5 でシステムを構成し，運用した。その後，Windows 2000 Server と Exchange 2000 Server でシステムを更新し，新たに Windows 2000 Server のターミナルサービスを導入して，操作方法や環境設定の統一を実現した[1]。現行のシステムは，Windows Server 2003 と Exchange Server 2003 に更新してあり，サーバーを保護するために ISA Server 2000 を導入している。

現在，コンピュータ上に仮想マシンを作成して稼動させるソフトウェア Virtual PC 2004 がリリースされている。このソフトを本システムに導入し，新たな活用を試みた。それは，一般には専用のコンピュータを用意し独立して稼動させる ISA Server 2000 を，Virtual PC 2004 で生成した仮想マシン上で稼動させることにより，同一のコンピュータ上で他のサーバーと共に統合運用することである。その概要について，ISA Server 2000 によるシステムの保護と合わせて報告する。

2. ISA Server 2000 によるシステムの保護

本システムのサーバーは自研究室内に設置してあり，Windows Server 2003 のターミナルサービスと Exchange Server 2003 のメールサービスをクライアントに提供している。このサーバーを学内 LAN に直結すると，不正アクセスの対象となりかねない。この危険を防止し，回避するためには，外部ネットワークと内部ネットワークを分離し，両者の間に流れる情報を制御する必要がある。

そこで，学内ネットワークから自研究室内への引き込みケーブル上，サーバーの直前にゲートウェイを置いて，サーバー側を内部ネットワーク，研究室外を外部ネットワークとして分離している。一般には，ゲートウェイの働きにより内側のネットワーク上のサーバーやクライアント群を保護するが，このシステムでは研究室内に設置してあるサーバーのみ保護するのが目的である。

本システムのゲートウェイには，ルーティング，ファイアウォール，サーバー公開の機能が必要である。そのために，サーバーに ISA Server 2000 Standard Edition をインストールして，これらの機能を実現している。以下，インストールおよび運用上の設定について述べる。

ISA Server をコンパクトに仕上げるため，以下の設定でインストールした。

(1) ISA Server 本体と一般的なオプションを組み込む「標準インストール」を指定して，必要な最小限のコンポーネントを組み込んである。
(2) ファイアウォールモードを選択して，ファイアウォール機能のみを組み込み，必要のない「キャッシュ」と「Web 公開」の機能は省略している。
(3) Windows Server 2003 のドメインに参加させず，スタンドアローンサーバーにしてある。

ISA Server のファイアウォール機能の内で，

パケットフィルタリング
警告，ログ，レポート
ポリシーベースのアクセス制御
サーバーコンピュータの保護

について設定を行っている。以下，その詳細を述べる。

パケットフィルタの設定には，既定で利用可能な

DHCP クライアント

DNS フィルタ
ICMP ping 要求
ICMP ping 応答
ICMP ソースの制御
ICMP タイムアウト
ICMP 未到達
ICMP 送信

をそのまま使用している。他に，独自のパケットフィルタの定義も可能であるが，必要ないので特に追加はしていない。

ISA Server に対する不正なアクセスを検出するため，パケットフィルターレベルの侵入検出を

Windows out-of-band
Land
Ping of Death
IP Half scan
UDP bomb
Port Scan

について行う設定をしてある。

アクセス制御に関するポリシー要素として，内部ネットワークと外部ネットワークの間で通信に使用するために独自に定義したプロトコルを以下の通り作成してある。

（1）「外部ネットワークにあるリモートコンピュータ」から「内部ネットワークにあるサーバー」へのターミナルサービス接続に対応するプロトコルとして，

プロトコルの定義名　RDP in
ポート番号　3389
プロトコルの種類　TCP
方向　着信

（2）内部ネットワークにあるサーバーのターミナルサービスセッションで実行中のプログラムからの出力を，外部ネットワークにあるリモートコンピュータの TCP/IP 接続ローカルプリンタで印刷させるためのプロトコルとして，

プロトコルの定義名　LPR in
ポート番号　515
プロトコルの種類　TCP

方向	着信
プロトコルの定義名	LPR out
ポート番号	515
プロトコルの種類	TCP
方向	発信

インターネットへのアクセスを許可する（ISA Server を通過できる）プロトコルを設定するために，既定の「インターネットアクセス用プロトコル・ルールの作成」でプロトコル・ルールの構成を行った。その際，標準設定の FTP，FTP Download only，HTTP，HTTPS はそのまま残し，Gopher は使用することがないので解除してある。さらに，標準のプロトコルおよびユーザ定義のプロトコルから選んだ

DSN Query
Exchange RPC Server
NetBios Datagram
NetBios Name Service
NetBios Session
RDP（Terminal Service）
RDP in
Telnet

を追加してある。

また，クライアントの TCP ポート接続してあるプリンタによる印刷出力を行うために，下記の標準のプロトコルおよびユーザ定義のプロトコル

LPR in
LPR out
SNMP
SNMP Trap

も追加してある。

ISA Server は Windows Server 2003 上で動作している。この土台となる Windows Server に対する保護は ISA Server の機能を使って行うが，ISA Server がファイアウォール専用として機能するので，「専用レベルのセキュリティー」で行っている。

ISA Server のパブリッシング（公開）機能は，内部ネットワークに存在するサーバーを安全に公開するための機能で，標準には Web 公開とサーバー公開の 2 種類をサポートしている。このシステムでは，Web 公開は必要がないので使用せず，ターミナルサービスを提供するためにサーバー公開のみ使用している。このために，サーバー公開ルールを以下のように作成してある。

ルールを適用するプロトコルにはユーザ定義の「RDP in」を指定し，適用するクライアントの種類には特定のコンピュータのクライアントアドレスセットを指定している。このアドレスセットには，ゼミナールの授業で使用するパソコン教室のコンピュータに割り振られた IP アドレスだけが登録してある。これにより他のコンピュータからのアクセスを拒否できる。

さらに，ISA Server の「メールサーバーの保護」機能を使って，サーバーに組み込まれている Exchange Server 2003 の公開と保護を行っている。これにも，不正なアクセスを制限するために，上記のクライアントアドレスセットを指定してある。

3. 仮想マシンによるサーバーの運用

小規模なネットワークを構成する際，何台ものサーバー用コンピュータを用意することは限られた予算や運用管理の面から困難なので，1 ～ 2 台で賄うことになる。一般にはゲートウェイは単独のコンピュータで運用するのが望しいが，1 台のサーバーにファイアウォール，メールサーバーなどの機能を集約することもできる。

このようにすることで，システムの導入や管理の費用を抑えることができる。しかし，サーバーに対する負荷が高くなるので，CPU やハードディスクでのボトルネックの発生と障害に対する影響の大きさが懸念される。よって，安全性を求めるならば，少なくともファイアウォールは分離した方が望ましいと言える。この相互に矛盾する問題・要求を解決するには，1 台の物理コンピュータ上に 1 台以上の仮想マシンを実現できればよい。

1 台の物理コンピュータ上に複数の仮想マシンを作成して，それらが同時に動いているようにみせかける PC エミュレータと呼ばれるソフトウェアがある。これを使えば，1 台のサーバーをホストコンピュータとして，その上に複数の仮想サーバーを作ることが可能になる。もちろん，欠点として仮想マシンの動作は遅くなる。

本システムでは，サーバーに Windows Server 2003 をインストールして，Active Directory を備えたドメインコントローラと，ターミナルサービスを提供するターミナルサーバーを組み込んである。そして，メールサーバーとして Exchange Server 2003 を，PC エミュレータとして Virtual PC 2004 をインストールしてある。これらのサーバーは，次に述べる ISA Server と異なり，物理コンピュータの Windows Server 2003 上で稼動する通常の運用形態である。

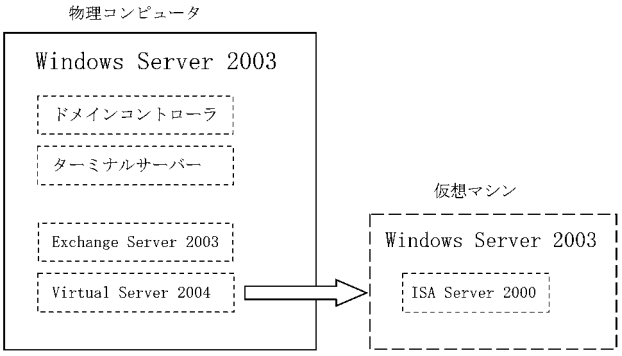

図1　物理コンピュータと仮想マシンの関係

ファイアウォールを他のサーバーから分離するために，Virtual PC を使って，192MB のメモリー，2GB のハードディスク，2 枚の LAN カードを持つ構成で仮想マシンを 1 台作成した。この仮想マシンにはゲスト OS として Windows Server 2003 がインストールしてあり，ISA Server を前節で述べた設定でインストールして，稼動させている。一般に，仮想マシンでは画面表示の遅さが問題となるが，ISA Server を稼動させる上でその点は重要ではないので，問題とならない。

ISA Server 用仮想マシンの 1 つの LAN カードには内部アドレスを，もう 1 つには外部アドレスを割り当ててある。一方，奇妙な印象を与えるが，ホスト OS が稼動しているサーバーの LAN カードには内部アドレスを割り当ててある。即ち，内部ネットワークに接続したサーバーの扱いとなっている。

ISA Server 用仮想マシンの「外部ネットワークに接続する LAN カード」に対して，そのプロパティーで

（1） Microsoft ネットワーク用クライアントを無効にする

（2） Microsoft ネットワーク用ファイルとプリンタ共有を無効にする

（3）「この接続のアドレスを DNS に登録する」を無効にする

（4） NetBIOS over TCP/IP を無効にする

設定を行った[3]。これにより外部からの接続を制限することで，セキュリティーを高めている。

なお，運用の便宜を図るために，以下のことを行った。

通常，仮想マシンは Virtual PC コンソールを起動して，そこに表示される仮想マシンを選択することで起動される。しかし，特定の仮想マシンに対してこれを毎回行うのは手間である。そこで，起動用コマンド“Virtual PC.exe”にコマンドライン引数「-singlepc -pc“仮想マシン名”-launch」を指定したショートカットをデスクトップに作った。これをダブルクリッ

クすることで，コンソールを介さずに直接仮想マシンを起動できる。

仮想マシン自身の起動は短い時間で済むが，そのマシン上でゲスト OS を毎回最初から起動していては時間がかかり，効率がよくない。そこで，仮想マシンを終了させる際にゲスト OS をシャットダウンせず，終了オプションで「状態を保存する」を選択する。こうすれば，次回の起動時には短時間で前回保存した時点の状態へ復帰するので，手間が省け，起動の所要時間を短縮できる。

4. お わ り に

長期間にわたり整備してきた教育支援システムを保護するために，ファイアウォールを導入した。そのために，ISA Server 2000 を選択したが，運用管理の手間と費用節減を考慮して，専用のコンピュータは設置しなかった。その代わりに Virtual PC 2004 により生成した仮想マシン上で ISA Server を稼動させることで，物理的には 1 台のコンピュータでありながら，ISA Server を仮想的に独立して運用できることを確認した。全体としてのパーフォーマンスの向上に向けて，ハードウェアの強化と各種システムパラメータの調整が必要である。そのための調査と試行を今後の課題としたい。

その他に，教職課程の情報免許に関わる科目などでの実践的な教育の一環として，Virtual PC を活用できる可能性として以下のことが考えられる。

OS のインストール作業を経験させることは望ましい。しかし，誤操作によるシステムの破壊や機器の故障などを引き起こして支障をきたす危険を考えると，通常の業務に使っているコンピュータに直接インストールすることは避けなければならない。その点，仮想マシンであれば，インストールによる不具合が物理コンピュータのホスト OS の環境まで及ぶことはない。また，費用を投じて，新たにテスト用コンピュータを準備する必要もない。

サーバー関連の技術を学習しようとすれば，サーバー用とクライアント用の 2 台のコンピュータを用意して LAN で接続することになる。しかし，新たにテスト用コンピュータを準備するには費用がかかる。その点，仮想マシンを使うならば，それと物理コンピュータを共に LAN に接続し，必要な OS とアプリケーションソフトを組み込むだけで，容易に通信試験を行える環境が作成できる。

以上の点について，ターミナルサービスを使って開いたセッションの中で，仮想マシンを生成してテストすることを構想している。今後教育の場で実践し，サーバーに対する負荷の大きさを調べるなど，運用上の問題点を把握するとともに，教育効果も検証していく予定である。

参 考 文 献

［1］ 富岡恒雄，情報教育支援システムへの Winodws 2000 Server ターミナルサービスの導入，日本生産管理学会論文誌 Vol.9 No.1，2002年
［2］ 斗光佳輝，ISA Server 2000 インターネット接続ガイド，リックテレコム，2001年
［3］ 岡崎俊彦，ISA Server 導入と運用の基本，毎日コミュニケーションズ，2003年
［4］ 藤本　壱，Virtual PC 2004 活用ガイド，技術評論社，2005年
［5］ 岡崎俊彦，Windows 活用ステップアップ No. 251～255，Data Communication 誌，831～835号，電波新聞社，2004年
［6］ http://support.microsoft.com，文書番号825289，2003年