愛媛大学教育学部紀要　教育科学　第45巻　第1号　143～148　1998

WindowsNT Serverによる研究室内LANの構築

（第2報：プライベートネットワークの管理とセキュリティ）

村尾卓爾
（技術教育講座）

（平成10年4月30日受理）

A laboratory LAN constructed of *WindowsNT Server* for the network operating system

～ Security of the private network ～

Takuji MURAO

1．まえがき

Windows NT Serverをネットワーク・オペレーティングシステム（以後，NOSと呼ぶ。）とするクライアント／サーバ方式の研究室内LANを構築した。そのうち，研究室内のネットワークであるプライベートネットワークと研究室外のネットワークである愛媛大学学内LANやインターネットを結び，情報の送受信を行うために必要な三つのサーバ，WWWサーバ，DNSサーバ，及びメールサーバの構築については前報[1]で報告した。今回は，プライベートネットワークの利用者（以後，ユーザと呼ぶ。）の管理及びファイルやデータなどの情報資源の管理と安全性（以後，セキュリティと呼ぶ。）の確保について報告する。プライベートネットワークを整備し，管理機能を強化するため，ファイル管理とアクセス権の設定に有効なProxyサーバを導入した。さらに，情報資源の一つであるIPアドレスの有効利用を目指して，DHCP（Dynamic Host Configuration Protocol）サーバを構築した。それらサーバの有用性を検討する。

また，前報と同様に，このLANとして用いた情報処理システムを学校教育現場に適用することの可能性について検討する。

なお，前報で詳述した用語については，今回は略称で示す。

2．プライベートネットワークの構成

2．1　ネットワークの方式

コンピュータ・ネットワークを構成するには，次のような方法がある。これらについては，研究室規模あるいは学校規模の LAN を念頭において，得失を検討する。

ホスト－端末型　メインフレームなどの大きなコンピュータであるホストを中心にして，通信機能に特化したコンピュータである端末が放射状に接続されたネットワークで，データの蓄積やプログラムの実行はホストでのみ行われる方式のネットワークである。学校規模でのネットワーク（以後，校内 LAN と呼ぶ。）として情報教育実習用だけに限れば，この方式でもある程度の教育効果を上げることはできる。

LAN 及び WAN　それぞれ独立して情報の蓄積やプログラムの実行をするコンピュータ（ネットワーク上に接続されたコンピュータは，ホスト，ローカルコンピュータ，あるいはマシンと呼ばれるが，上記のホストとの混乱を避けるため，ここではマシンと呼ぶ。）が何らかの方法で接続され，相互に情報や資源の交換を行うことが出来る方式のネットワークである。これには，インターネットの技術を応用した LAN で，外部との境界にファイアウォールを設置してセキュリティを強化したイントラネットや，外部から公衆電話回線などを利用してイントラネットに参加できるエクストラネットが含まれる。

学校外部とは接続していないが，類似の方式のネットワークが小中学校規模でも使用されて来た。従来の学校の情報処理実習室のネットワークでは，LAN 型と端末型の折衷的なシステムが多く使われて来たが，それらは，マシンに相当する個々のコンピュータ相互の情報交換機能が十分でない。今後，学校内の情報ネットワークが情報実習室にとどまらないで，全校規模のものとなることを予想すれば，LAN 型のシステムの方が適したものになるであろう。校内 LAN には，分散型のクライアント／サーバ方式（C/S 方式）よりも共有型のサーバ／クライアント方式（S/C 方式）の方がデータの一括管理が容易で，適している面も有るとも考えられるが，現在のところ S/C 方式の取り扱い容易で適当な NOS がない。

インターネット　ネットワーク同士を接続したネットワーク。

その他　今後の校内 LAN は地域のネットワーク，さらにはインターネットに接続されると予想される。その場合に学校単位のネットワークで外部と接続するか，あるいは地域の教育機関のネットワークを構築し，そこを通してインターネットに接続するか，ネットワークの教育面での利用方法の発達と関連させて考慮されねばならない。経費と管理維持の煩雑さ及び前報[1]でも述べた教師の負担軽減を考慮すれば後者の方が現実的である。

ここでは，LAN についてのみ，特にパソコンを主体とする LAN を主として検討する。現在，一般に使われているパソコン LAN は，ピア・ツー・ピアと呼ばれる方式とクライアント／サーバ方式と呼ばれる二つの方法が主である。前者は，主として個人レベルでの情報資源の管理を念頭に置いたパーソナルユースを目的としたもので，Windows 95や AppleTalk を NOS とする場合によく使われる。後者は，NetWare や Windows NT（以後，NT と略称する。）を NOS とするもので，基本的にビジネスユースを目的としたものであり，動作の安定性やセキュリティの確保に重点を置いている。従って，NT は管理機能を強化するために，様々な管理機能を備えたパソコン用 NOS と捉えられ，ここでもこれを活用する。

クライアント／サーバ方式のネットワークでは，ネットワークを統括するドメインコントローラと呼ばれる管理用サーバが設置される。さらに，ネットワークの中に，ファイルサーバ，プリンタサーバ，データベース用サーバなどが含まれる。これらのサーバは，基本的には独立した（スタンドアローンと呼ばれる。）コンピュータとしてでも機能するものである。最近では，負荷をかけないドメインコントローラにパソコンを用い，大きな容量を必要とするデータサーバなどにはワークステーションを用いることが多い。大規模校の情報システムとしては，或る程度のワークステーションを含めたデータベースを設置する必要があるかもしれない。

2．2　Windows NT によるネットワーク

ピア・ツー・ピア型の LAN は，基本的にマシンを管理の単位とし，さらにマシンをワークグループ単位で管理するのが通常である。従って，マシンにさえアクセスできれば，ユーザは誰でもほぼ自由に LAN にアクセスできることになる。これに対し，NT などの C/S 方式 LAN では，ユーザを管理の対象とし，それをドメイン単位で管理する。従って，マシンにアクセスできたとしても，それだけではネットワークにアクセスできない。ネットワークへのアクセスは別途登録されたユーザにだけ許される。ユーザは個人で登録するが，一般にはユーザは種別されたワークグループに所属する。さらに，NT では，ユーザのアクセス権はファイル単位及びディレクトリ単位で指定できるので，高信頼性，高安全性が確保される。これはマシンのハードディスクを NTFS というファイルシステムでフォーマットすることにより可能となる[2]。しかしながら，一般のパソコンで用いられている FAT システムでフォーマットされた他のシステムとの互換性がないことが欠点である。

この特徴は学校現場での情報システムを構築する場合には極めて有用とされている。すなわち，教師などの管理者グループのアクセス権と生徒とのアクセス権を明確に区分できること，授業中の生徒によるシステムの破壊，ファイルの誤った削除等の問題を未然に防ぐことができること，また，LAN 上の情報資源を校外からの不正なアクセスに対して防護することができることなどが効果的と考えられる。

なお，NT Server には Windows Messaging というメールシステムが含まれている。メールサーバの代用として作動するので，教育現場では電子メールの教育に役立つと考えられ，生徒相互の情報交換に有用と推察される。インターネットに接続するメールサーバについては，前報[1] で詳述した。

また，学校の内外を問わず情報発信をするための Web サーバについても前報で述べたシステムを利用することが適当である。

3．プライベートネットワークのセキュリティ

前章で述べたように，NT のネットワークはアクセス権の管理が多様に行われる。すなわち，NT のネットワーク上で作動するマシン（ローカルコンピュータ）の使用に対するアクセス権の管理が行われる。次いで，ユーザマネージャというユーティリティでユーザの登録，権限の割当，パスワードの登録，ログイン可能時間，ユーザグループの設定，グループの権限設定等きめ細かく設定できる。すなわち，ネットワーク上で共有される情報資源に対するアクセス権をディレクトリ単位で，あるいは，ファイル単位で一括管理することができる。本研究では，

クライアント側に開発したアプリケーションプログラムを置き，サーバ側からアクセスして十分稼働することを確認した。使用したプログラム言語は，Visual BASIC と Java である。

このことから，学校現場でも，個々の生徒あるいは教師が自作したアプリケーションソフトをネットワーク上で共有することの有効性が確認された。ユーザによりアクセス権を区分けし，生徒には読み取りの許可，教師には読み取り書き込みの両方を許可，重要なファイルには学校管理者のみアクセス可能などのように権限を必要に応じて設定することが必要である。

4．プロキシ（Proxy）サーバの導入

前章で述べた，アクセス権の管理をより堅固に，かつきめ細かく設定することができるとともに外部からのアクセスに対しても管理機能を持つ Proxy サーバを導入した。ゲートウェイサーバの一種である[3]。Microsoft 社の試供品 MS Proxy Server 2.0 を使用した。一般に，LAN には，外部からの不正なアクセスに対抗するためファイアウォールを設ける。MS Proxy サーバはファイアウォールの一部の効用に類似の機能を持つので，今回のネットワークに利用した。ファイアウォールの機能としては，①外部からの不正侵入の防止，②内部からインターネットへのアクセス制限，あるいは効率的運用などが挙げられる。しかし，新しく出現するインターネット上の情報に迅速に対応できないこと，さらには，クライアント側にもプロキシに対応した設定が必要なことなどの不便さも付随する。

ここで利用する MS Proxy には次の得失がある。まず，MS Proxy ではクライアント側の WinSOCK という API を Proxy サーバ対応に拡張しており，多くのインターネット上のアプリケーションが MS Proxy 上で稼働する。次いで，プロトコル変換機能がある。すなわち，プライベートネットワーク内で TCP/IP 以外のプロトコルを使用していても，インターネットにアクセスする時にはプロトコルを TCP/IP に変換する。また，この逆も可能である。また，今回は使用しなかったが，小規模のダイアルアップサーバとして使用できる。さらに，IP アドレスのマッピング機能を持っているので，プライベートアドレスを使用しているクライアントからでも MS Proxy サーバ経由でインターネットにアクセスできる。なお，インテリジェントアクセス機能を持っているので，インターネット上の WWW サイトへアクセスしてダウンロードしたファイルを Proxy サーバ上にキャッシュ（一時的に記憶）するので，繰り返しての同じサイトへのアクセスに対してこのキャッシュを利用できることから，プライベートネットの負荷が軽減される。

MS Proxy サーバは，Socks Proxy，WinSOCK Proxy，Web Proxy を統合したもので，これを，パソコンにインストールする際には，次の基本ソフトが必要である。①Windows NT Server 4.0，②Windows NT Service Pack 3，③Microsoft Internet Information Server 3.0

Proxy サーバとしては，ドメインフィルタで IP アドレスのアクセス制限を設定できること，ユーザとサイト（マシン，クライアント，ホスト）もサービス（WWW，FTP など）毎に指定できること，プロトコルも選択する事ができること，キャッシュの設定，及びキャッシュサイズの設定が可能である。なお，クライアント側の設定は LAN 上で行うことができる。

MS Proxy Server を導入し，研究室内のマシンとユーザのアクセス権の管理を行って，十分実用になることを確認した。前章で述べた，自作のアプリケーション・プログラムのアクセ

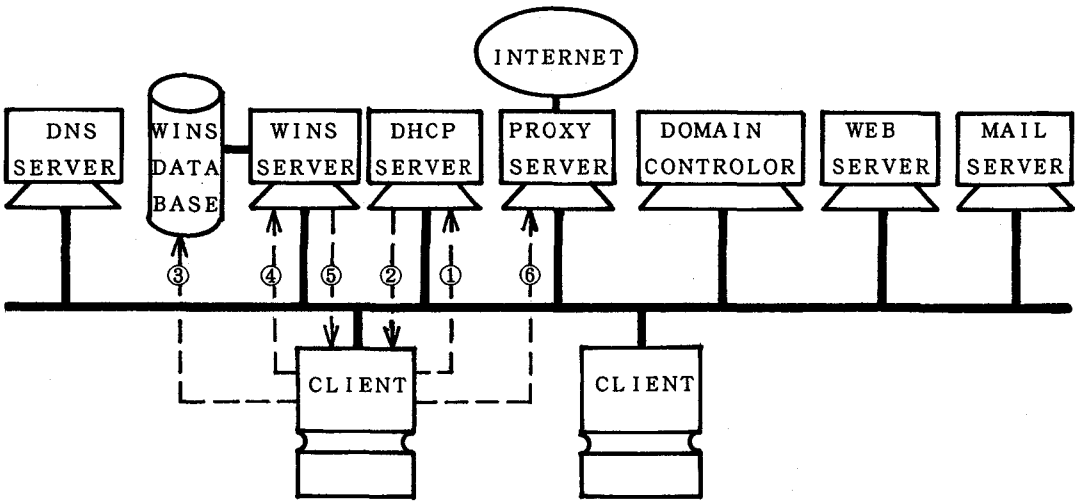
ス権をユーザに応じて設定すること，及び外部ネットワークであるバリアネットへのアクセス権をマシン毎に設定することで，緻密なセキュリティ対策が取れることを確認した。

校内 LAN にとどまらず，地域の学校を結んで LAN を構築する必要が予想される。すなわち，公衆回線を経由して LAN を設定しなければならず，いわゆる仮想プライベートネットワーク（Virtual Private Network）の構築が必要になるであろう。この場合には，IPSec の使用とともにファイアウォールを設置してセキュリティの確保を図ることが必要である。

5．DHCP サーバの構築

IP アドレスはインターネットに接続されたすべてのコンピュータに付けられた識別番号であり，8 ビット 4 桁の数字の羅列である。この IP アドレスは，ネットワーク ID とホスト ID の組み合わせからできている。一方，プライベートネットワークでは，ある範囲のアドレスを勝手に使用することが認められている。これをプライベートアドレスといい，プライベートネットワーク内部でマシンを効率的に管理することが可能である。一方，プライベートネットワークに割り当てられた IP アドレスが少ない場合には，これを効率的に運用することが望まれる。これを行うのが DHCP サーバ[4] である。

ネットワーク上の IP アドレス識別には静的に IP アドレスの名前を検索する（名前解決サービスと呼ぶ。）DNS（Domain Name System）と動的に解決する WINS（Windows Internet Name System）がある。すなわち，WINS は WINS クライアントが起動したときに WINS サーバに自分の名前を登録するので，接続時にだけ内容が反映されるという利点がある。WINS を使わなくても DNS を利用して外部に解決を依存するブロードキャストという方法も



① IP アドレスの貸し出し請求
② IP アドレスの割り当て
③登録
④名前解決要求
⑤コンピュータ名に対応する IP アドレスの提供
⑥インターネットへのアクセス

図 1　研究室プライベートネットワークの概念図

行われるが，解決できない場合やネットワーク・トラフィック（交通量）が増大するという問題も考えられるため，WINS の使用が望ましい。WINS サーバ，DHCP サーバの概念上の構成を図1に示す。この図に示す諸サーバは，完全修飾名が melab. edsystem. ed. ehime-u. ac. jp である1台のマシンにすべて搭載されている。

DHCP サーバは Windows NT Server に附属しているので，追加機能として導入する。クライアントの登録，使用する IP アドレスの範囲の設定，リース期間の設定を DHCP マネージャで行う。本研究では，133.71.34.110～113の IP アドレスを使って2台の DHCP クライアントを動かし，DHCP サーバが順調に稼働していることを確認した。

現在インターネットで使われている現行の8ビットでの IP アドレス資源の枯渇が予想されており，IP アドレスの32ビット化が検討されているものの，現段階では，ネットワーク上の全てのホストに IP アドレスを供給することは難しいとみられ，特に校内 LAN をインターネットに接続する場合には，DHCP システムの利用は不可欠と予想される。

6．ま と め

Windows NT を NOS とする研究室内 LAN を構築し，プライベートネットワークの効率的な運用を目標にするとともにセキュリティの確保が可能なシステムの構築を試みた。そのため，Proxy サーバと DHCP サーバを導入して，その有効性を検討した。

(1) 研究室規模の LAN の NOS として，Windows NT は有効である。

(2) ユーザ管理，ファイル管理を適切に行うことができた。プライベートネットワーク上で，言語 Java と Visual BASIC を用いて開発したアプリケーションプログラムが有効に作動していることを確認した。

(3) Proxy サーバを導入し，ユーザ及びマシンのアクセス管理が厳密に行われていることを確認した。

(4) DHCP サーバを構築し，IP アドレスの有効利用が可能であることを確認した。

(5) 学校規模のネットワークである校内 LAN に NT が有用であること，DHCP サーバが不可欠であることを示した。

謝　　辞

終わりに，本研究の遂行に当たり有益な助言を賜った岩手大学 田中稔教授及び松山南中学校 星川良紀教諭に厚くお礼申し上げます。また，ネットワーク構築作業に際して多大の貢献をされた，当時の愛媛大学生 岡田文恵君，渋谷昌子君，中川聡子君，松岡佳子君に感謝します。

参 考 文 献

1）村尾卓爾：Windows NT Server による研究室内 LAN の構築，愛媛大学教育学部紀要第 I 部教育科学，第44巻第1号，135，(1997)．

2）Windows NT 4.0 リソースキット，アスキー出版局，(1997)．

3）SOHO 構築入門キット，海上忍，秀和システム，(1997)．

4）Windows NT World，97. 7，IDG コミュニケーションズ，(1997)．