＜実践報告・資料＞

ネットワークシステム運用管理の実践報告

中国職業能力開発大学校
附属福山職業能力開発短期大学校　日浦悦正
甲田大樹
中谷久哉

A practical report in operative administration of network system

Etsumasa HIURA, Taiki KOUDA and Hisaya NAKATANI

要約　IT 化の進展に伴い当校でもネットワークシステムの整備拡充を行ってきた。特に５年に１回の電算機システム及び３次元 CAD/CAM システムの新規整備時にはネットワークシステムを見直し、時代に合ったシステムに変更してきた。2000年４月には導入ベンダーとの話し合いを重ね、既存のネットワークシステムの資産を活かし、可能な限り最新のネットワークシステムを導入し、その後も様々な変更改良を加え現在に至っている。導入から現在までの運用管理の経過及び課題について報告する。

Ⅰ　はじめに

当校では2000年４月に電算機システム及び３次元 CAD/CAM システムのリース換えが行われた。基幹ネットワーク部分は、それまでの電算機システムのベンダーであった日本 IBM 株式会社が担当し、電算機システムのある B 実験実習棟を中心に各棟（事務棟、研修棟、教室棟、A 実験実習棟）へ敷設されていた。そして新日本製鐵が新たなベンダーとなり、既に敷設された基幹ネットワークに組み込む形で今の電算機システムが導入された。それから３年半経過したが、その中でネットワーク管理は当校のネットワーク委員会（現 IT 部会）を中心に、主に情報系の指導員が行ってきた。WAN も含めたネットワーク環境の見直しや整備、電算機システムのセキュリティ面の対策やユーザ数増加によるサーバ面での見直し拡充が行われてきた。これまでの運用管理と、現在のネットワークシステムでの課題を述べることで、ネットワークシステムがより整備され、情報教育訓練を充実させ、外部へ有効な情報発信もできるものと考える。

Ⅱ　ネットワークシステムの構成

１　導入時（2000年４月）のシステム

導入時の電算機システムは図１に示すようにバックボーンに Gigabit Ether の Core Switch（以下 SW）を用いている。このバックボーン SW に３つの UplinkSW を光ファイバにより接続し、その SW から各部屋（端末室１、端末室２、WS 室）の PC に100BASE-T で接続されている。また、外部とは OCN エコノミーにより接続されており、この接続形態は従来の資産を引き継いだものである。基幹ネットワークのサーバは４台で構成されており、その機能と仕様を表１に示す。B 実験実習棟から各棟へのネットワークは既設の10BASE-５と10BASE-２のケーブルを使用したため、B 実験実習棟以外の棟ではスループットが十分に得られないネットワークシステムとなっている。

２　外部との接続

システムの導入時インターネット接続は「OCN エコノミー」を契約していた。これは NTT がサービスしている最大128kbps のデータ転送が行える専用線接

論文受付日　H15.11.4

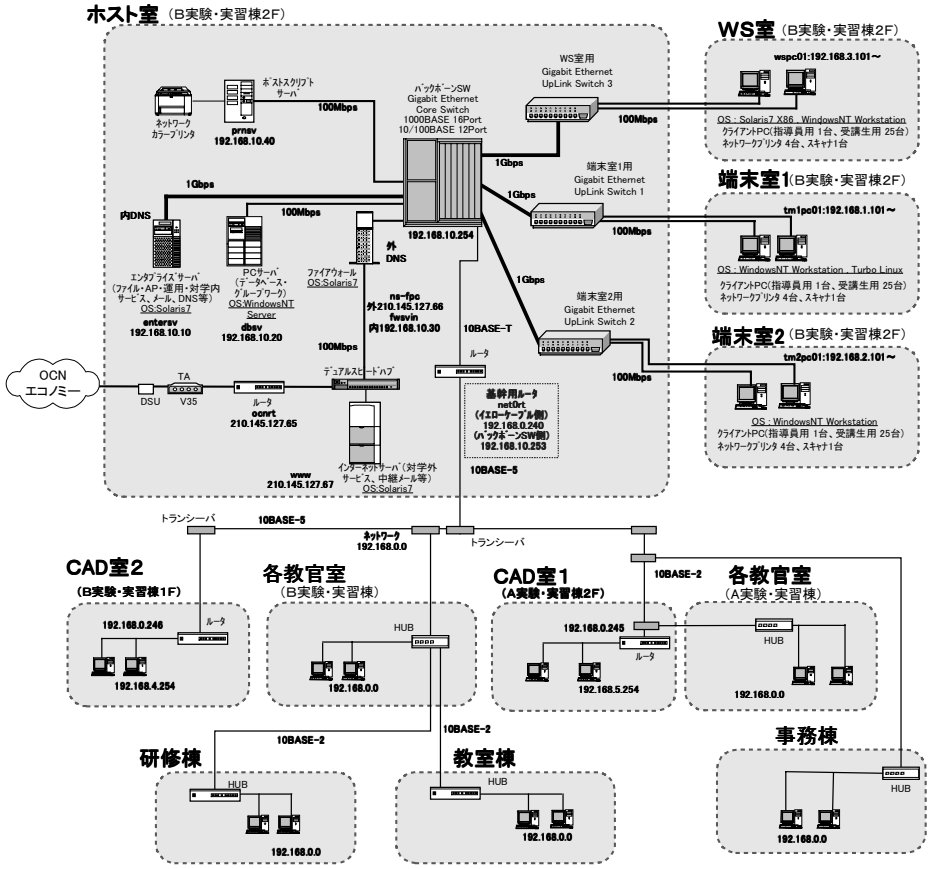

図１　ネットワークシステム構成（2000年４月時点）

表１　サーバ構成

マシン名	機　能	仕様（OS, アプリケーション）
entersv	ファイル管理 メール DNS プロキシー	Solaris 7 Tivoli SecurID ACE Netscape Suite Spot3. 5 Plus Netscape Proxy Server3. 5
fwsvin	ファイアー ウォール	Solaris 7 FireWall－１ Virus Wall
www	インターネット トサーバ	Solaris 7 Netscape Suite Spot3. 5 Plus
dbsv	データベース	Windows NT Back Office Server4. 5 Tivoli

表２　プロキシサーバの構成

マシン名	機　能	仕様（OS, アプリケーション）
proxysv	プロキシー	CPU : PentiumIII　１GHz メモリ：２GB SDRAM HDD：108GB OS, アプリケーション： Windows2000Server ISA Server2000

続サービスである。しかし当校の PC の台数が増大しインターネット接続もレスポンスが悪くなったことから2001年４月に「スーパー OCN」へと変更した。「OCN エコノミー」は帯域の保証がないベストエフォート型であり、最大24ユーザで１本の128kbps 回線を共有する。もしこのうちの１ユーザが128kbps の帯域を使い切っていると、他の23ユーザはまったくサービスを受けられないことになる。それに比べ「スーパー OCN」では IP バックボーンに直接接続するため、各ユーザに128kbps のスループットが保証されており、他のユーザのトラフィックの影響を受けることはない。また、より高速な接続形態として ADSL や光ファイバによる接続も考えられたが、ADSL は当校が NTT の交換局から4. 7km と離れていることで期待される速度が得られなかった。光ファイバ接続は2004年１月に予定している。

３　プロキシサーバの導入

インターネット接続の切り替えと同時にプロキシサーバ用として１台サーバを増設した。それまで entersv でメール、DNS と共用で動作させていたのを

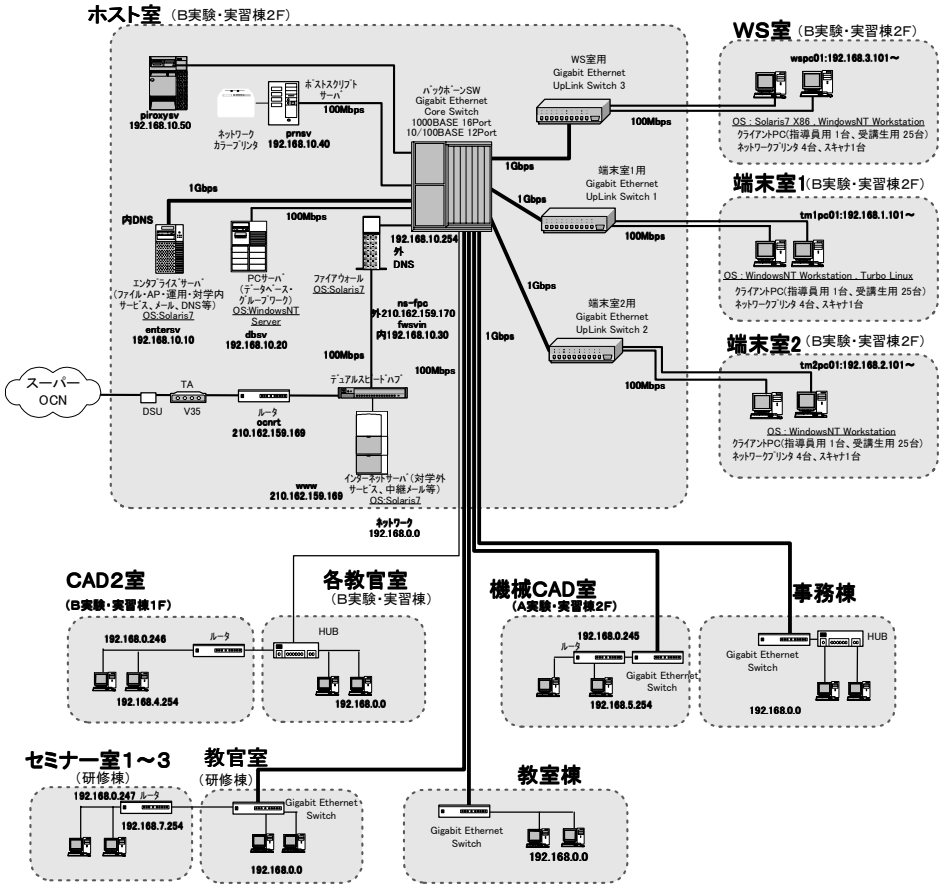

図２　ネットワークシステム構成（2003年10月時点）

Proxy のみ独立させることで、サーバ負荷の分散を実現した。特に内部サーバの中でもプロキシサーバはトラフィックが集中するため、より高いハードウェアスペックが必要となる。導入したサーバのスペックは表２のとおりである。また実習などでインターネットを利用する場合は特にキャッシュの設定が有効である。キャッシュの設定をすることによって、繰り返してアクセスするホームページの情報を一時的にメモリやハードディスクに保存しておくことから、インターネットへのアクセスを効率よく行え、トラフィックの減少、レスポンスの短縮が期待できる。

４　ネットワークの高速化

システムの導入時、校内を結んでいる基幹 LAN は 10BASE-２の媒体が中心であった。しかしケーブルの老朽化によるネットワークの断線対策、またネットワークの高速化を図るため2001年５月基幹 LAN の Giga Bit 化を行った。各棟に Giga Bit の SW を入れ、ホスト室のCore SWに光ファイバで接続する形とした。

５　現在（2003年11月）のシステム

以上の、改良を加えた結果の現在のネットワーク構成を図２に示す。現在、150台近い PC がネットワークに接続された環境になっている。

III　利用形態に基づく運用管理

１　実習教室での運用管理

各教室におけるクライアント PC の構成であるが、それぞれに２台の外付け HDD（SCSI）を接続している。これは複数の OS を切り替えて実習を行うことを前提としており、メリットとしては外付け HDD の電源の ON/OFF により簡単に OS の切り替えが行えることである。また内蔵の HDD は実習では使用しておらず、主にシステムのバックアップ用としてのみ使用している。デメリットとしてはトラブルの確率が高い。ディスク自体の故障はもちろんであるが、接続している SCSI ケーブル、SCSI カードなどに問題が発生し PC が起動できない状態が発生した。

プリンタに関しては４台のネットワークプリンタを

設置している。クライアントPCからはTCP/IP接続により、直接プリンタへ印刷する設定もできるが、各教室の４台のPCに共有プリンタの設定を行い、他のPCからはその４台を経由して印刷する構成にしている。これは複数の受講生が同時に印刷を実行すると、ネットワークプリンタのバッファだけではメモリ不足で印刷に問題が発生することを防ぐためである。

各教室のPCには移動プロファイル方式を採用している。Windows NT／2000Serverで設定ができ、ユーザのプロファイルがサーバに保存されるため各受講生が作った環境をどの教室、どのPCからでも同じように継続的に利用することができる。

２　ユーザアカウント管理

サーバには事前にユーザアカウントを登録し、各PC利用者はそのユーザアカウント、パスワードを使ってログオンする形式を取っている。各教室は専門課程、能力開発セミナー、IT習得コース、アビリティコースなど多数の者が使用するため、ユーザ管理に苦慮するところである。専門課程では学生ごとに１人１アカウントを発行する。アカウントは学籍番号と同一とし入学時に登録、卒業時に削除する形で２年間有効とする。またパスワードも定期的に変更するよう指導する。アビリティコースでは訓練生ごとに１人１アカウントを発行する。アカウントは「ability99」などの識別子＋連番とする。修了した時点でフォルダ、プロファイルの削除を行い再度、初期状態から使用できるようにする。IT習得コース等の飛込みのコースにおいては基礎的な内容が中心で、あまりOSの環境を変更する必要がないため１コース１アカウントを発行する。パスワードの設定は担当する講師が行い、受講者に使用させる。コース終了後はアカウントを無効にするか、担当講師でパスワード変更などをして不正アクセスできないようにしている。プロファイルの変更を不可にしておくと、常時初期状態で使用できるため運用が容易である。能力開発セミナーにおいては後々の保守を考えるとIT習得コースと同じく１コース１アカウントにするのが望ましい。しかし個別に環境を保持する必要がある場合は、人数分のアカウント登録が必要となる。その場合においてもコース終了後はアカウントを無効にするなど、不正アクセスできないようにしている。

ワンタイムパスワードに関して述べる。当校ではシステムの導入時、米国RSA Security Inc．社のワンタイムパスワードシステム（SecurID）を使用していた。このシステムにおいてはPIN番号と呼ばれる４桁の固定番号と事前に渡されたSecurIDに表示される６桁のTokencodeを入力することによりユーザ認証を行うものである。Tokencodeは60秒ごとに変化するので、たとえパスワードを盗まれても不正アクセスはできなくなるというメリットがある。しかしデメリットとしてはSecurIDを事前に使用者に配布しておかねばならないことや、SecurIDは壊れやすく、破損、紛失した場合、再度購入しなければならない。またワンタイムパスワードを入力した場合に、ログオンできないなどのトラブルが発生した時に管理者の対応が必要となること等が挙げられる。そのため2000年12月に廃止し、現在はユーザアカウント、パスワードでのみユーザ認証を行っている。

３　ユーザファイル管理

サーバの共有フォルダとアクセス権に関して述べる。１ユーザアカウントに対応し１共有フォルダを作成すると、実習で作成したファイルをサーバに保存することができる。但し他のユーザの誤操作などを防ぐためアクセス権を正確に設定しておく必要がある。特に「フルコントロール」の権限を与えてしまうとアクセス権の変更まで出来るため、利用者に対しては「変更」の権限までにとどめておく必要がある。すべてのフォルダに対してAdministratorが「フルコントロール」権限を持っていると後々保守がやり易くなる。また専門課程ごと、アビリティコースごとに共通で使用できる共有フォルダを作成しておくと、各学生および訓練生へファイルを配布する時などに使用できる。

IV　障害発生時や保守時における運用管理

2000年３月の導入時から３年半の間に148件を越える障害が報告されておりその代表的なものに関して述べる。

１　プロキシサーバの障害

かなりの頻度でプロキシサーバがダウンする障害が生じた。主な原因はトラフィックが集中し処理ができなかったことである。これはシステム構成で述べたプロキシサーバの増設により問題は解決した。

２　クライアントのログイン時の障害

クライアントPCからログオン／ログオフに時間がかかったり、dbsvの共有フォルダへ接続するのにレ

スポンスが悪くなるといった障害が発生した。ユーザ認証も dbsv で行っているため dbsv 自体か、もしくはクライアント PC を繋ぐネットワークに問題がある可能性が高いことに注目し原因を調査し、移動プロファイル方式が原因であることが分かった。これはユーザがログオン／ログオフするたびにサーバ上にあるプロファイルがローカルへ、あるいはローカルからサーバ上のプロファイルにコピーされるため、dbsv とネットワーク両方に負荷がかかることが分かった。そのためユーザが作成したファイルはローカルのプロファイル環境の「デスクトップ」や「My Documents」などではなく、サーバの「共有フォルダ」に保存するようなルール作りを行った。

3　ルーティング障害

当校の LAN はいくつかのセグメントに分割しているが、教官ネットワークからサーバやインターネット接続できない現象が発生した。各ネットワークを繋いでいるルータや SW にはすべて RIP を使用し動的にルーティングを行っているが、停電や機器障害などによってルーティングテーブルが消えてしまうことが原因であった。対策としてはサーバなど主要な機器については静的なルーティングテーブルの作成を行うことで対処した。

4　SPAM メールによる障害

近年、SPAM メールあるいはそれを大量送信するためにメールの第三者中継が問題になってきている。導入時に使用していた「Netscape Mail」ではこのような第三者からの中継メールを拒絶することができず、一時的に中継サーバとして使用されたことがあった。この対策としてはメールサーバを SPAM 防止に対応したものに入れ替えるのが一番早いと考え、2001 年 6 月にメールサーバを SPAM 対策がされている「PostOffice」に切り替えた。ウィルスに関してはサーバにおいて侵入検知ツールやセキュリティ検査ツールは導入していないが、ウィルス等の標的となる新しいセキュリティホール対策のアナウンス等はメールで行っている。

5　その他の障害

PC が立ち上がらない、プリンタに出力できない、サーバに繋がらないなど細かなトラブルが発生した。これらのトラブルが発生した場合はハードウェアに問題があるのか、ソフトウェアに問題があるか原因追求を行い、それに対する対策を考える必要がある。トラブルの対処時に履歴を残しておくと次回同じ現象が発生した場合に参考になるが、すべて管理者が対応するとは限らないため難しい面がある。

V　今後の課題

1　セキュリティポリシーの策定に関して

現在、ネットワーク利用について、専門課程学生に対しては学生便覧にあるネットワーク利用規定を遵守して使用させるようにしている。本年度、規定違反者の罰則について、利用停止から処分という形の見直しを行った。ここには学生外のネットワーク利用者にも準用するよう明記されているが、学生便覧の中だけで終わっており、受講生に対してはアナウンス等が行われていない。特にアビリティコース増加による受講生の著しい増加とインターネットへの接続の増加が予想されるため、受講生が知らない間に加害者となるケースなども十分考えられ、指導を含めた対策は急務である。また、職員に対しては、各系、課の IT 委員が管理者となり運用、管理を行っているが、共通の認識を持って情報に対するリスクを十分に考慮した管理ができているとはいえない。

現状をみると、構成員の内部のセキュリティに対する意識の低さと対策の不十分さは否めない。このような状況を改めるため、当校のネットワークシステム運用においては、当校内部で行われる学術研究・教育活動・機構業務の質を高めるためにも、情報基盤の整備や内外からの不正アクセス等に対する、情報資産のセキュリティを確保するための体制作りが必要不可欠である。

そこで、さまざまな脅威から情報資産を守るための第一歩として「セキュリティポリシーの策定」がある。セキュリティポリシーとは、「組織における情報セキュリティに対する基本的な考えから具体的な対策までを示すもの」と定義できる。これを明文化することで、組織のセキュリティに対する対応を内外に示すことができる。また、新しく構成員となる人への教育も一定レベルが確保できると考える。

このような状況のもとで当校では、次の 6 つの点を内容とするセキュリティポリシー（基本方針・対策基準）を早急に策定しなければならないと考える。

第 1 に組織と体制を確立である。当校に最高ネットワーク責任者をおき、IT 部会の委員長となり情報セキュリティ対策を推進する。その果たすべき役割、責

任および権限を明確にしておかねばならない。さらに、日常的な業務、例えば学外からの様々な攻撃および学内からの加害行為に対する遮断等の措置を、どの組織で、どのような手順で、どのような体制で行うかを明確にしておかねばならない。

第２に情報の分類と管理である。当校で扱われるすべての電磁的に記録された情報について、情報の重要度による分類と情報の管理方法及び管理責任を規定する。情報の種類として事務情報に加えて研究情報や教育情報がある。重要度の分類と改ざんや破壊によるリスク分析を、全校レベルおよび課・科レベルで検討する必要がある。

第３に物理的セキュリティの確保である。情報システムの設置場所について、安全性を保ち不正な立入りを阻止する対策を立てること。更に、パソコンまたは持ち運びを前提としたノートパソコン等の情報資産を保護するための対策にも十分配慮しなければならない。

第４に人的セキュリティである。全構成員に対し、セキュリティポリシーを周知徹底させるとともに、各人がどのような権限と責任を持っているかを明らかにし、情報セキュリティを確保するための啓発活動や教育を講じなければならない。

第５に技術セキュリティである。学外または学内からの不正なアクセスによる情報資産の破壊を阻止するため、情報ネットワークのアクセス制御・管理に必要な対策を講じるべきである。情報の分類によって物理的または論理的に異なるネットワークの導入を考慮すべきである。

第６に評価と見直しである。セキュリティポリシーは秒進分歩の情報技術の発展ならびに策定したポリシーの遵守度により、定期的に見直して改定を行い、セキュリティレベルを絶えず上げるよう努力しなければならない。更に、セキュリティ監査についても何らかの措置をとることが望ましい。

セキュリティポリシーの策定は、企業にとっては必要不可欠のものと受け止められている。これからの電子商取引などに関わる企業は、セキュリティポリシーがしっかりしている会社は信用するが、そうでない会社は取引にも応じてくれないといった事態にまで発展するといわれている。当校のセキュリティポリシーでは、本来の活動を妨げるような制約や制限を設けることは避けなければならない。しかし一方で、安易なセキュリティポリシーでは社会から切り離されるきらいのあることを忘れてはならない。従って、当校の実状にあったポリシーを早急に策定し、それを構成員全体が遵守し引き続いて短期間でセキュリティのレベルを上げていくことがキーポイントになると考える。このセキュリティポリシーの策定については、IT 部会の議題として検討する予定である。

２　ネットワークの二重化

当校のネットワークは各棟にネットワークは広がり、指導員の職員室なども各棟へ分散している。このような場合に講師・職員ネットワークと、専門課程学生ネットワーク・受講生（アビリティ、セミナー）ネットワークの切り分けを行うには VLAN によるネットワークの構築が効果的である。これにより、VLAN 間のセキュリティの確保が可能となり、各棟のレイヤー３SW 導入が急がれる。

VI　おわりに

秒進分歩のコンピュータの世界に追従していくには常に情報を収集しシステムにフィードバックさせていかねばならない。ネットワークは10Gigabit　Ether の時代に突入している。CPU 速度も３GHz を突破している。サーバも従来の複数台で行うのでなくコンピュータの性能の向上と、メインテナンスのしやすさから複数台の PC サーバを１つにまとめたサーバが提案されてきている。

現在、電算機システム及び３次元 CAD/CAM システムのリースが４年目に入っているが既に時代遅れになりつつある。今後は電算機システムと３次元 CAD/CAM システム含めたネットワークシステムをどのように運用管理してくかが本校を外部にアピールしていくための重要なメルクマールとなるであろう。

［参考文献］

⑴　白川浩・日浦悦正・平島隆洋・山下明博、情報通信ネットワークシステムの設計、職業能力開発報文誌、14号、1995年、P69−74

⑵　日浦悦正・甲田大樹・中谷久哉、ネットワークシステムの導入から現在までの運用管理、中国職業能力開発大学校　附属福山職業能力開発短期大学校　紀要、８号、2002年、P25−34

⑶　大学のセキュリティポリシーに関する研究会：大学におけるセキュリティポリシーの考え方、http : //www.kudpc.kyotou.ac.jp/Security/toshin2001. pdf、(2001)、P１－３