福山大学工学部紀要
第24巻 2000年10月

電子・電気工学科コンピュータ教室におけるネットワーク構築

田中　聡

A System Design of the Networks for the Computer Classroom.

Satoshi TANAKA*

ABSTRACT

We have integrated the computer education classroom for teaching both the core computing skills and the expetise in the Electric and Electronic Enginnering. The classroom system is incomposed with the windows 2000 computers by looking ahead into the future.

This papaer shows the concepts and the feature of this system. The network configuration is the crux for the high performance, useablity and enhanced security of this system. To enhance the network throughput, the client PC's are formed five groups under each server computer. The multi-master replication feature on DNS , DFS with the windows are increased the system fault tolerance and usablility.

キーワード：コンピュータ教室，ネットワーク, LAN, ウインドウズ
Keywords: Computer Classroom, Education, Network, LAN, Windws 2000

1．まえがき

IT(Infomation Technology)技術の展開により社会の根底から変革してしまう可能性が指摘され、コンピュータ、通信技術の開発とそれらのインフラの整備そしてITに関する教育は、今後の日本を支えていく上で最重要な課題となった。電子・電気工学科では平成12年度4月に特色のある教育を行うことを目的として、学科の計算機実習室を新設した。この教室では1年次生のコンピュータリテラシの基礎教育から、2，3年次生の電子・電気工学専門科目の教育、そして、4年次生および大学院生の研究室における研究まで幅広い利用が可能となるように機器・設備およびソフトウエアの導入において考慮されている。また、数年前から学生の就職活動においては電子メールやホームページなどのインターネットの利用が必須となってきたことから、インターネット教育を行い、利用者が自由に使用できるオープンな環境を目指していることも特徴のひとつである。

本システムは教室の学習システムであるとともに電子・電気工学科の情報システムの中核とも位置づけられている。学科ホームページの公開や学生用のメールシステム、学科内情報の発信・共有などの目的でも利用されている。

本稿では本学科の計算機実習室についてその設計概要について述べる。特に教室のセキュリティのあり方および負荷分散のためのネットワーク構成を中心に検討したシステム設計について述べる。

学校におけるコンピュータ教室には一般企業のコンピュータシステムとは異なり、次のようなシステム要件が課せられる。

（1）年次毎に利用目的が変化するが、基本的な利用方法については学年進行によらない連続性

*電子・電気工学科

が求められる。

（２）多数の学生が同時に同じリソースをアクセスしても障害が発生しない。

（３）ファイアーウォールなしでもある程度のセキュリティが求められる。

（４）スキルやモラルに大きな違いのある利用者が多数存在する中で、教育上の効果が求められると同時に、保全性を確保する必要がある。

以下、これらの要件を柱として教室のシステム設計を各節に分けて解説する。

２．機種選定

（１）の要件はコンピュータをリプレースする場合には過去の資産との連続性を維持しなければならないというよく知られた点とともに、低学年次における教室での利用形態と卒業研究などの研究室での利用形態および個人データの利用方法にできるだけ連続性が欲しいというものである。

マイクロソフト社は平成１２年２月１７日に新しいビジネス用 OS として Windows 2000 を発売した。世界のパーソナルコンピュータ市場において Windows 系を OS とするコンピュータの出荷台数は９割以上といわれている。アプリケーションソフトも豊富で汎用性も高い。最初に普及した Windows 3.1 が出荷されてから１０年以上にわたって常に OS の主流を占めている点など安心感も高い。また、本学でも多くの計算機実習室や研究室に導入されており、学生も使い慣れているという点は重要である。

しかしながら実際に導入するに際して不安材料もある。Windows 2000 は最初のビジネス OS として実績を積んだ windows NT の後継として登場してはいるものの、発売から間もないこともありバグの対処や使い方に関するノウハウが十分蓄積されていないという点である。ただ、平成１２年８月１８日にサービスパック１（SP1）としてバグフィックスがリリースされたことによりとりあえず運用に踏み切る環境が整ったと判断される。

計算機実習室は Windows 2000 Professional 版をインストールした４４台のクライアントＰＣと５台の Windows 2000 Server を導入している。クライアント機パーソナルコンピュータは複数年にわたる導入をおこなったため Intel 社 Celeron プロセッサ 433MHz から Peitium Ⅲ 500MHz の機種まで３種類が混在している。一方、サーバ機は NEC 製 Express5800/120Mc (Pentium Ⅲ Xeon プロセッサ 733MHz)を導入してサービス性能向上を図っている。システムでは Windows 2000 Server により提供される以下の機能を

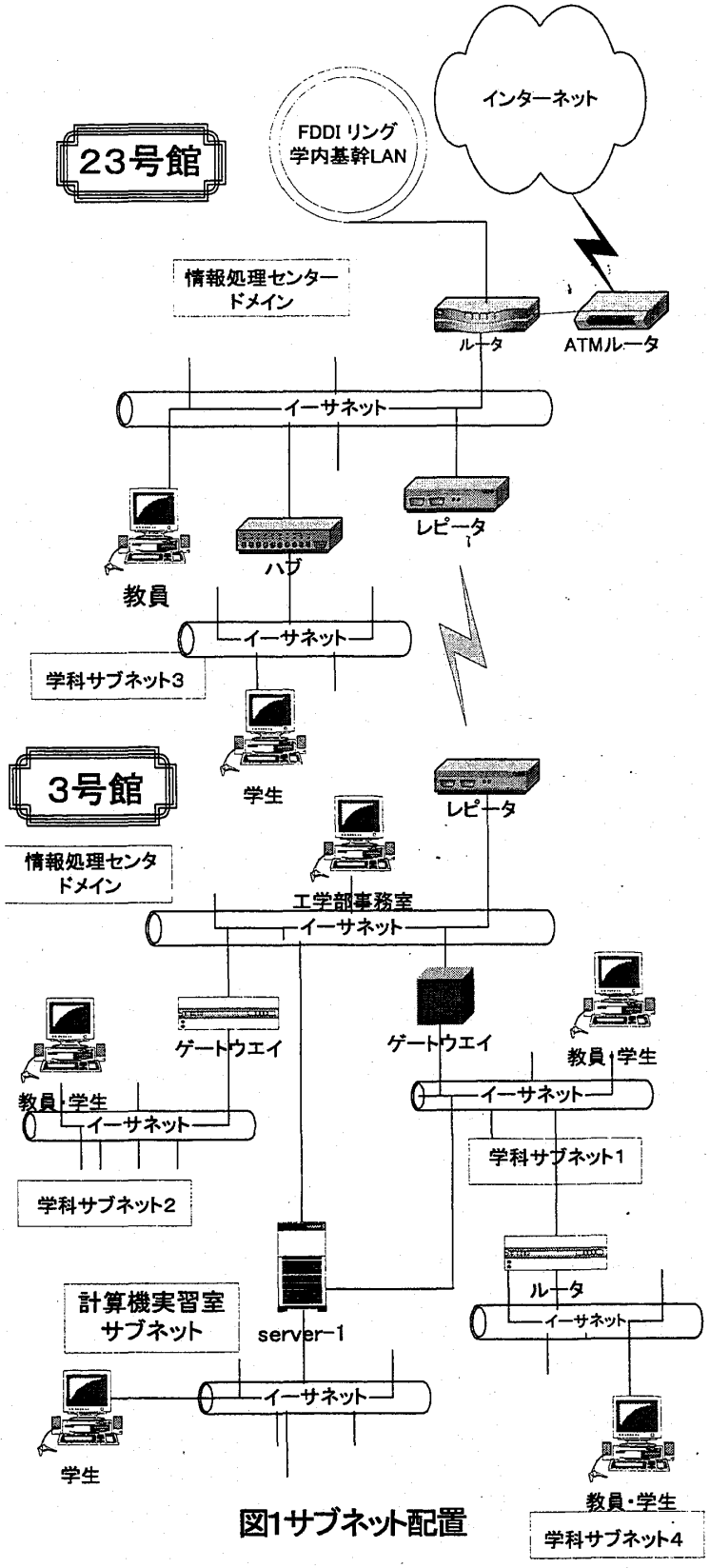


図1サブネット配置

利用する[2]。

（ａ）ドメインコントローラ(DC)
（ｂ）動的 DNS(Dynamic Domain Name Service)
（ｃ）DHCP(Dynamic Host Configuration Service)
（ｄ）Wins(Windows Name Service)
（ｅ）分散ファイルシステム(Distributed File System)
（ｆ）共有ファイル
（ｇ）移動プロファイル
（ｈ）Windows Media Service

（ａ）（ｂ）（ｃ）は計算機実習室のドメインに関する基本的な機能の実現のためであるが、不特定多数のユーザが出入りするコンピュータ室ではセキュリティ管理のためにユーザ認証やユーザ利用記録（ログ）の監視も重要な要件である。

Windows 2000 server ではマルチマスタによるドメイン制御が可能であるため、万一１台のサーバに障害が発生しても残りのサーバによるユーザ認証が可能である。DNS においても同様であるが、従来の BIND を用いた DNS の下位のドメインから BIND に動的変更を要求すると DNS にエラーが発生するため、静的な動作にとどめている。この制約のため DHCP により動的に接続されるクライアントは自動的にはドメインに登録されない。

個々のユーザの環境を好みに合わせてカスタマイズするための移動プロファイルを導入している。移動プロファイルはユーザ環境をサーバ機上のユーザの固有フォルダに保存することにより、ログインするコンピュータに依らず同じ環境を使うことができる機能である。

３．外部ネットワーク構成

電子・電気工学科は３号館と２３号館の２つの建物に学生、教員が分散して所属している。３号館と２３号館の間は平成２年度に設置された１０M bps の光リピータで接続されており、両方に情報処理センターのドメインが作られている。また、各建物内にはドメインの異なる複数のサブネットが存在する（図１）。本学の学内基幹 LAN は今日のような大容量の通信を想定したネットワークではないため CSMA/CD によるコリジョンドメインがほとんど全学にわたる。３号館のネットワークにも学内のあらゆるコンピュータからのパケットが流入し混雑している。今回計算機実習室が設置されたのは３号館であり、インターネットや学内基幹 LAN へ接続するゲートウエイが２３号館であるため、このリピータ接続がネットワークのボトルネックになる可能性がある。特に Windows Media サーバによる、動画像の配信では１つの通信に４～９ Mbps の帯域を必要とするが、３号館から２３号館に向けての帯域が確保できない状況である。今後基幹系のネットワークの高速化を進めていかなければならない。

本システムには学生や教員が３号館と２３号館のどちらからでもサーバにアクセスしフォルダ共有ができるような構成が求められている。さらに windows 系の OS のコンピュータブラウジングによりコンピュータが発見可能であることが望ましい。そこで、Server-1 には３つのネットワークインターフェースを取り付け、教室内と３号館および２３号館の３つの方向への接続を行い（図２）、サブネット１および情報処理センタドメインからはブラウジングを可能とした。また、WINS サーバを設けて他のサブネットからの検索も可能とした。この接続の効果として、教室から発生するインターネットへのアクセスを３号館のサブネットを経由することなく２３号館へ送り出すことができた。

他のサーバ機は教室内と３号館の２方向にインターフェースを設けた。Windows 2000 ではインターフェースを複数もつマルチホーム型の構成において、それぞれのインターフェースに異なるサブネット名を付けることができるようになった。教室外向けのインターフェースは HUB-1 を介して５台のサーバを接続するとともに３号館の１つのサブネットにつながれている。使用した HUB はスイッチングタイプであるため不要なパケットを３号館のネットワーク１に流すことなく、サーバ間を結ぶバックラインとして利用することができる。

また、Windows 2000 Server の新しい機能である分散ファイルシステム（ｆ）を用いると、別々のサーバにある共有フォルダを一つのリンクに接続して、どのサーバからでもそのリンクをたどってファイルに到達することができる。また、DNS のラウンドロビン機能により接続するサーバをアクセス毎に順次切り替えることができるため負荷を分散できる。ただし、NetBIOS 名を用いた接続の転送となるらしく WINS サーバもしくは LMhosts ファイルにより IP アドレスに変換を設定しておかなければリンク先にたどり着けない。

４．内部ネットワーク構成

教室内のネットワーク（図２）は、４４台のクライアントＰＣを５つのグループに分け、それぞれのグループに１台ずつのサーバを割りあてて 100BASE-TX の LAN により接続した。一般に用いら

れる多ポートの HUB を用いたスター状の集線方式では HUB に全てのパケットが集中してしまい、通過するための待ち時間が大きくなってしまう。これを避けトラフィックを分散させること、そして、HUB故障時の迂回路を設定しやすくすることが目的である。さらにグループのサーバが故障の場合は別のサーバへサービスを要求できるように、各グループのHUB －２～６間も HUB －７で相互接続している。

各クライアントＰＣはユーザ用に２種類の共有フォルダをサーバから取得する。一つは各ユーザの固有のデータを保存するためのユーザフォルダであり、もう一つは共有のアプリケーションをサーバ上からクライアントに配布するためのアプリケーションフォルダである。

システムの要件（２）に提起したように、講義という形態をとる場合には教師の操作を学生がまねるため、一つのリソースに同時にアクセスすることが多く、ピーク時のサーバやネットワークの負荷が極めて高くなる。特にアプリケーションフォルダから同時にクライアント台数分のアプリケーションを起動しようとする場合はサーバの負荷分散を考えなければならない。例えば、５台のサーバにファイルを複製し、それぞれのサーバにに８台～１０台のクライアントを１００M bps の LAN で接続したとき、通信のオーバーヘッドや衝突によるパケットロスが全く無い場合に各クライアントが取得できるデータ量は１．２Mバイト／秒程度である。実際はこれより２０～５０%は低い値となる。一方学生がこの共有アプリケーションの起動のため、アイコンをクリックして応答を待つ場合、無応答だと誤認して再度クリックするまでの待ち時間は約５秒程度でしかない。この時間内に転送できるデータ量は多く見積もっても６Mバイト、実際は３Mバイト程度であろう。共有アプリケーションフォルダに配置するアプリケーションの構成には読み込まなければならないファイルサイズを３Mバイト以下とし、二重起動を防止できるような仕組みを持つアプリケーションが望ましい。

５台のサーバ上に同じアプリケーションをコピーするために Windows 2000 の分散ファイルシステム（DFS）が持つ File Replication Service を利用する。この機能もマルチマスタであり、１つのサーバのファイルを書き換えると残りのサーバに順次反映されるが、全てが更新完了するまで１０分から１時間程度待たなければならない。更新を急がなければならない場合に備えて、ミラーリング用のソフトを導入して強制的に更新することもできるようにした。

各サーバ機に導入した複数のネットワークインターフェース間は IP 転送を行わない。その代わり、インターネットと接続するために Server-1 に proxy サーバを設定する。Server-1 では３方向のパケットトラフィックを教室内とリピータ側のみに限定するため Deerfield 社の WinGate を採用した。クライアントのプロキシの設定をこのサーバに向けることによりインターネットとの接続が可能になる。だが、Server-1 の故障時の接続確保のために Server-2,Server-3 に予備のプロキシを導入した。なお、プロキシの切り替えは DNS の変更による。

５．セキュリティ管理

セキュリティには機密性、保全性、可用性の３側面があり、可用性と他の２者は二律背反の関係にある。全くの初心者が自由に練習を積みスキルアップを図れる「初心者にやさしい」環境を整える必要がある反面、高度の知識を悪用しようとする者が現れることを想定しておかなければならないという教育システム独自の課題もある。

機密性を確保するためほとんどの企業のネットワークではファイアーウォールが設けられているが、大学のネットワークでは設置されないところが多い。本学でも現時点では設けられていない。これは、大学のコンピュータネットワークは教育研究用であり、無知もしくは故意によるコンピュータの不正な操作や毀損は教育現場において容易に発生しうること、また、コンピュータネットワークの可用性を最重視し、実験的利用による障害の発生をもある程度容認しなければならないとの立場があることがあげられる。さらに、企業ネットワークと比較し蓄積されるデータ重要性の高いものが少ない環境にあることも大きな理由である。とはいえ、セキュリティの甘いコンピュータネットワークが外部から踏み台として利用され、他組織のコンピュータの攻撃に使用されるなどの事件が発生し、社会的な信用の低下や実質的損害を発生させている。また、法的にも平成１２年２月に制定された「不正アクセス行為の禁止などに関する法律（略称：不正アクセス禁止法）」に「第５条　アクセス管理者による防御措置」に努力目標が規定されており、速やかな実効が期待されている。

こうした観点から、学内のネットワークに関しては以下のような方針を掲げ、可用性とのバランスをとりながらセキュリティ対策を講じる。

（ｉ）システム防御は中継に使われやすいサーバ本体を中心に考える。

（ii）クライアント PC は速やかな復旧対策を中心

とし、できるだけ元のまま利用することによる教育効果を第一に考える。

（iii）重要度の高いデータの管理は各責任者の責任においてバックアップを行い、さらに重要度の高いデータはよりセキュリティの高いサブネットワークを構築するなどの対策をする。

（iv）不特定多数の利用する計算機実習室内では、利用できるネットワークサービスを限定し、障害の発生を最小限にとどめる。

（v）不正アクセスの監視をおこなうシステムの導入を図る。

（vi）パスワードの作成・管理技法について学生・教員に対して徹底を図る。

Windows 2000 ではファイルシステムが暗号化されていたり、Kerberos 認証を用いパスワードが暗号化されて送られるなど、ネットワーク上のセキュリティは強化されており、フォルダ共有であっても FTP などのファイル転送方式に比べて機密性が高い。しかし、Windows95 などの下位システムや Mac の混在する学科のコンピュータ環境ではこれらのセキュリティ機能も生かしにくいのも事実である。

不正アクセスだけではなく正当なアクセスにおいても、利用者の無知もしくは悪意によりシステムに障害を発生させることも考えられるが、教育用システムであるという本来の目的を重視して、迅速な回復を図ることのできる機能と体制を準備しておくこととした。すなわち、各クライアントにおいてはハードディスクの完全なバックアップイメージを常に準備して、障害発生時にはこのイメージのインストールにより回避する。

次に本システムにおいて不正アクセスが発生する経路による対策を考える。

①学外および他学科ネットワークから
②電子・電気工学科内のサブネットから
③コンピュータ教室内のクライアントＰＣから
④コンピュータ教室内のサーバ機へ直接

計算機実習室のネットワークは５台のサーバをファイアーウォールとして、教室内のクライアントコンピュータを他のネットワークから囲い込んだ構成としている。これは③の教室内からの不正アクセスの低減を狙ったものでる。大学内と学外の接続がほぼ透過的である現状では①②の不正アクセスの防御はサーバのセキュリティ機能に頼る以外にないと判断した。巷間 Windows サーバは Unix サーバに比べてセキュリティホールが多いと言われている。しかし、長年の運用経験により windows サーバのセキュリティチェックポイントが次第に明確になってきた。すなわち、

（ａ）IP パケットルーティング機能は極力用いず、他のソフトウエアを利用する。

（ｂ）Web サービスプログラム IIS を用いるときは認証や拡張機能を制限する。。

（ｃ）公開されるセキュリティパッチを的確に適用する。

等である。

④の物理的アクセスの防止には、部屋を分離するか、鍵つきのロッカーに収納する

６．まとめ

ネットワークセキュリティが求められている時代ではあるが、依然として従来のパスワードのようなクラッキング（解読による情報流失）されやすい方法でのアクセス管理が主流である。今後指紋認証などのバイオメディカルな認識法の導入が必要である。

コンピュータ技術やネットワーク技術の急激な発達により、コンピュータ機能の技術標準がまたたくまに向上し、最新のコンピュータも導入して３～５年で陳腐化してしまう。そして、次々と現れる新しいアプリケーションやネットワークコンテンツとサービスに対応するためには新しい技術導入を積極的に進めていかざるを得ない。こうしたなかで、教育の現場で求められる普遍性を語ることがたいへん困難な場面に直面しているように見える。やがて、技術トレンドを追いかけるコンピュータ教育の在り方を見直しをしなければならない時期がやってくるであろう。

同様にシステム設計や構築がソフトウエアやハードウエアメーカの考え方に常に引きずられている現状から見ると、急激な変化に耐えられるシステム構築技術の集大成が今ほど求められている時代は無いといえる。

謝辞

本稿を書くにあたりご協力いただいた電子・電気工学科川原講師に感謝する。また、教室システムの構築にご協力いただいた双葉工機　田村、村上の両氏、NEC フィールディング前島氏に感謝する。

参考文献

[1] Cowart R., Knittel B.:"Windows 2000 Professional ネットワークングバイブル",インプレス,2000.

[2] Microsoft Corporation:"Windows 2000 Server リソースキット",Vol.4-6,2000.

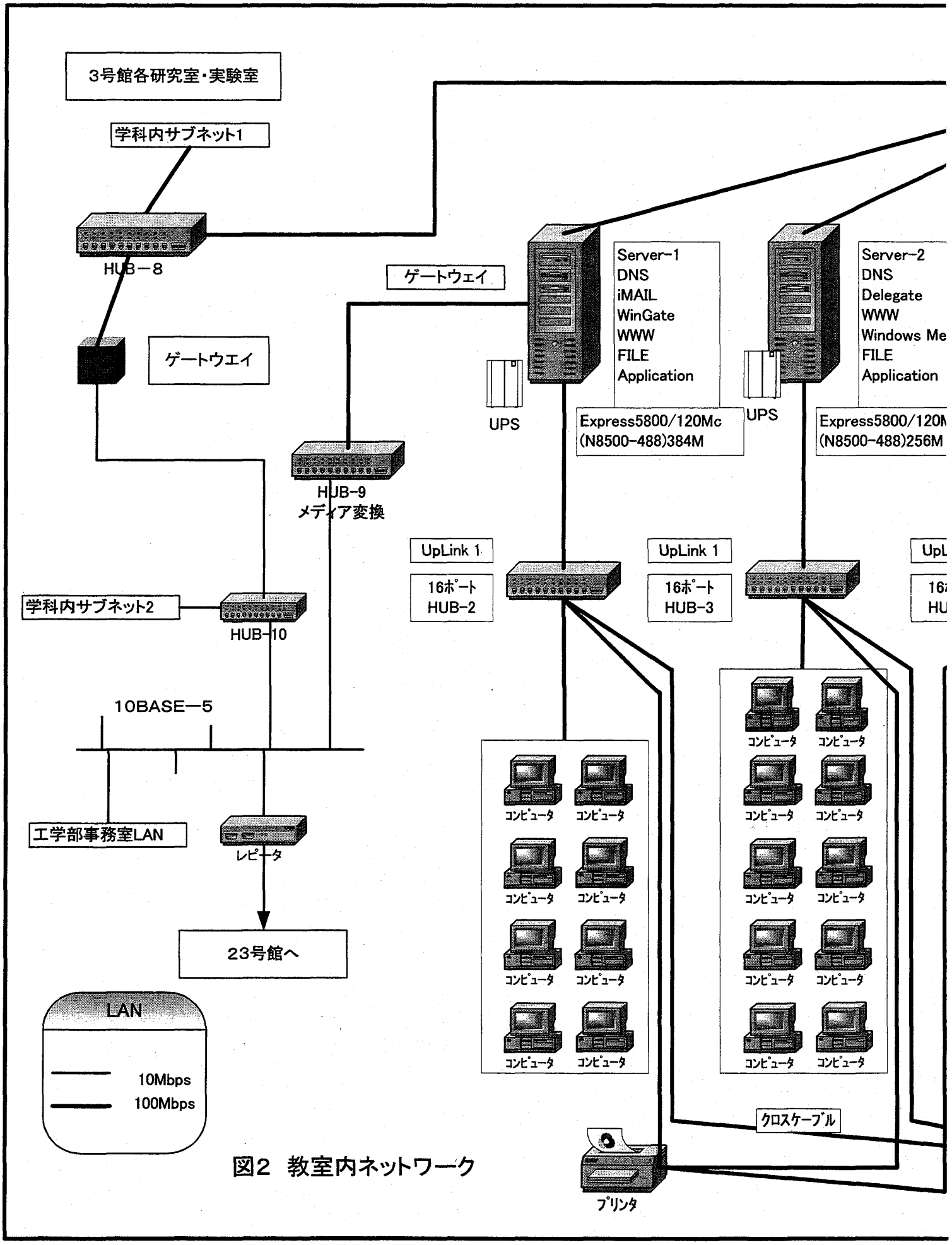
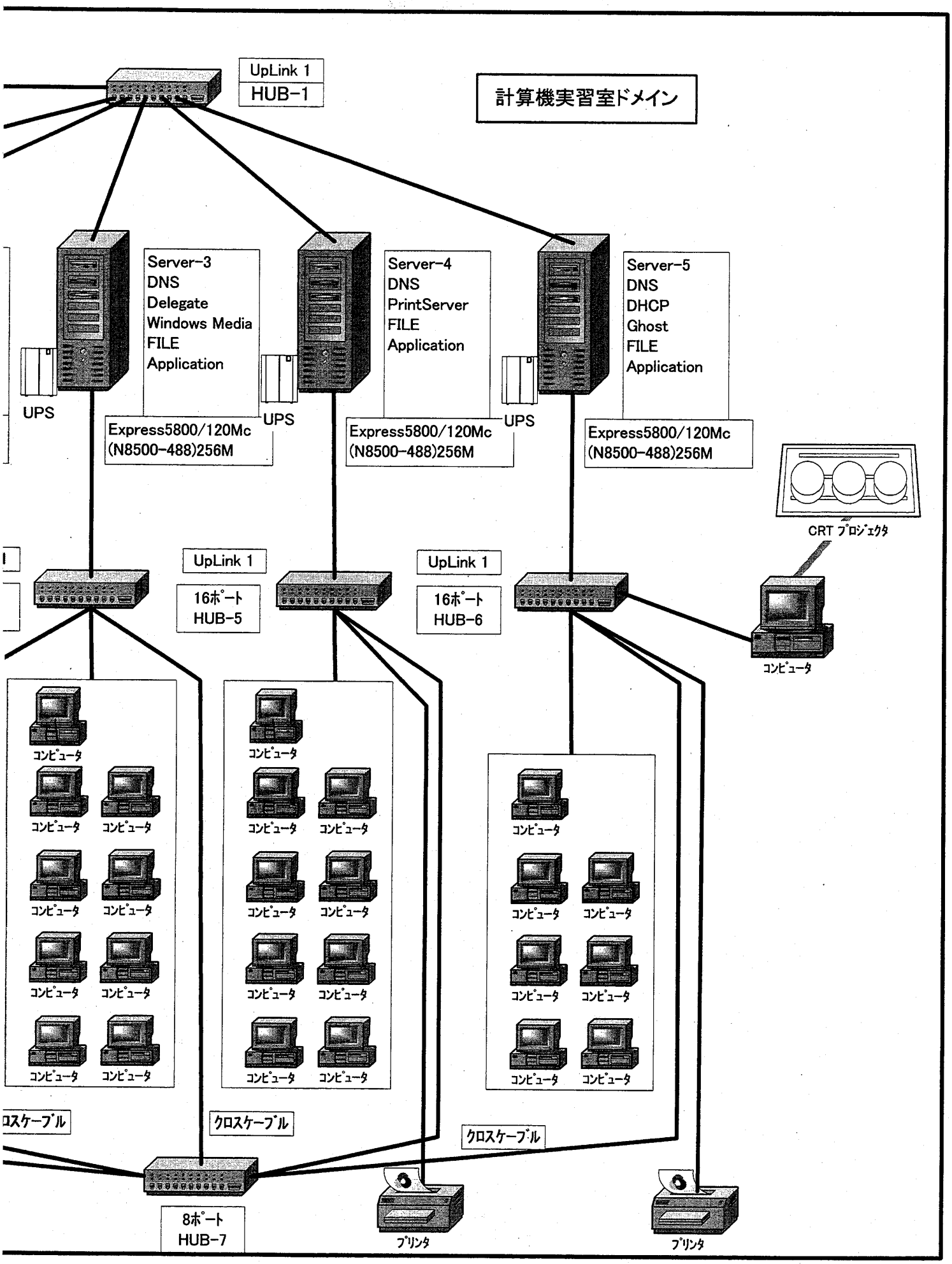


図2　教室内ネットワーク


UpLink 1
HUB-1
計算機実習室ドメイン
Server-3
DNS
Delegate
Windows Media
FILE
Application
Server-4
DNS
PrintServer
FILE
Application
Server-5
DNS
DHCP
Ghost
FILE
Application
UPS
UPS
UPS
Express5800/120Mc
(N8500-488)256M
Express5800/120Mc
(N8500-488)256M
Express5800/120Mc
(N8500-488)256M
CRT プロジェクタ
UpLink 1
16ポート
HUB-5
UpLink 1
16ポート
HUB-6
コンピュータ
クロスケーブル
クロスケーブル
クロスケーブル
8ポート
HUB-7
プリンタ
プリンタ