

# 校内サーバの構築と活用 (小中学校)

岩手県立総合教育センター

# 目 次

## 解説編

1	ネットワークの概要	1
2	ネットワークに関する用語知識	1
3	サーバー構築の手順	8
4	基本的なネットワーク関係コマンド	9
5	サーバー関係のトラブル	10
6	校内ネットワーク関係のトラブル	13
7	クライアント側で行うセキュリティ対策	14

## 操作編

A	基本的なネットワークの構築	18
1	ワークグループ管理されているピアツーピアネットワークの構築	18
2	ローカルユーザーアカウントの登録	18
3	ファイルサーバーの構築	19
4	ネットワーク接続ストレージ (NAS) の利用	23
5	Macintosh向けのファイル共有	24
6	ルーターの設置	34
B	ActiveDirectoryドメインネットワークの構築	35
1	ドメインコントローラ (ActiveDirectory) のインストール	35
2	ドメインユーザーの登録方法	39
3	グループへの登録方法	40
4	コンピュータの登録方法	41
C	DNSサーバーの役割と構築	44
1	DNSサービスのインストール	44
2	DNSサービスの設定確認	47
3	DNSサービスの役割確認	49
D	WINSサーバーの役割と構築	51
1	WINSサービスのインストール	51
2	DNSサービスからの参照設定	52
E	Webサーバーの構築	53
	別冊「情報サイト8 利用マニュアル」	
F	FTPサーバーの構築	54
1	FTPサーバーの設置	54
2	DNSサービスからの参照設定	55
G	メールサーバーの構築	57
1	校内メールシステム及びメールアカウントの作成	57
2	DNSサーバーへのメールサーバー登録	58
3	クライアント側のメールソフトの設定	59
4	校内メールシステムで外部とメールを交換する方法	60
5	中継許可	62
H	プロキシサーバーの構築	64
1	HTTP用プロキシの設定	64
2	フィルタリングの設定 (セキュリティ)	65
3	DNSサーバーへのプロキシサーバー登録	66
4	ブラウザの設定 (Microsoft Internet Explorer)	66
I	セキュリティを高める	67
1	ブラウザでセキュリティを高める (インターネットエクスプローラーの設定)	67
2	ルーターでセキュリティを高める	69
3	マルウェア対策	70

# 解説編

## 1 ネットワークの概要

ネットワークとは、複数台のコンピュータを接続することを言います。コンピュータを単独で動作させる（スタンドアロン）よりも、効果的にコンピュータを活用できるようになります。

LAN（ラン、「Local Area Network（ローカルエリアネットワーク）」の略称）とは、学校内や家庭内等限定された場所のネットワークのことをいいます。したがって、学校内のネットワークを、校内ネットワーク、または、校内LANと呼びます。県内各学校の校内LANは、全て、Ethernet（イーサネット）と呼ばれる方式によって構築されています。

本講座は、校内LANにおける各種サービスを提供するために最低限必要と思われる技能の習得を目指して研修を進めていきます。したがって、どの学校でもすぐ活用できる内容に絞り込んでいます。

## 2 ネットワークに関する用語知識

### (1) ネットワークの管理方法 - ワークグループとドメイン -

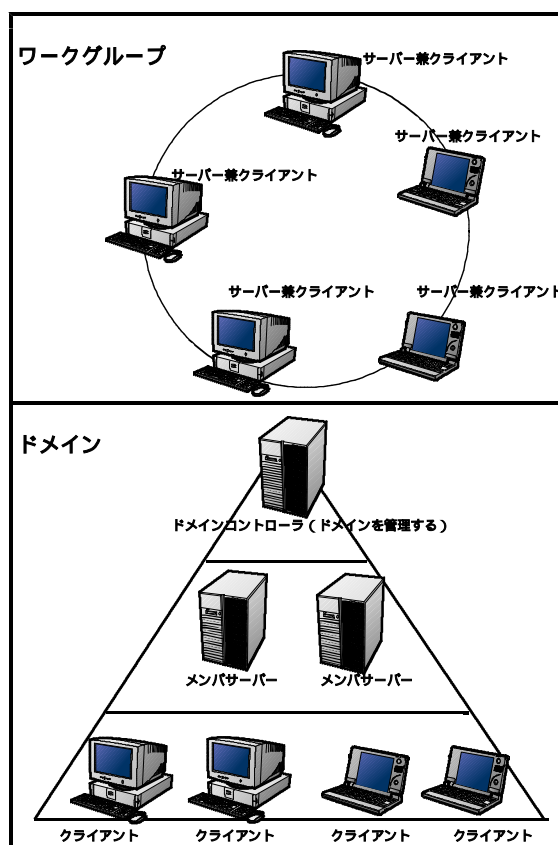
コンピュータの台数が増えるほど、それぞれのコンピュータの管理がたいへんです。ここでは、ネットワークの管理方法であるワークグループとドメインの違いについて説明します。

コンピュータをグループという単位でまとめて管理する方法を、Windowsでは「ワークグループ」と呼んでいます。教師が使うコンピュータのグループ、児童生徒が使うコンピュータのグループといったようにまとめます。管理するときにはワークグループ毎に行います。ワークグループで管理されているコンピュータを利用する際には、各コンピュータにユーザー名とパスワードを設定します。例えば、ネットワークに接続している2台のコンピュータをみんなで使いたい場合には、2台のコンピュータ双方に利用する人のユーザー名とパスワードを全員分登録します。ワークグループは、専門的知識を必要としない簡易なネットワークであり、構築しやすいことが何よりの特徴です。

しかし、このワークグループの数が増えてくるともはやそれぞれのワークグループに所属するコンピュータを管理すること自体がたいへんになってきます。学校で言えば、例えば、3月から4月にかけては人事異動や卒業入学の時期でもあり、それぞれのワークグループに所属する全台のコンピュータに全員分のユーザー登録をしなければなりません。

そこで、全てのコンピュータやユーザ情報全体を一つにまとめて集中管理する必要が出てきました。その役割を担うのが「ドメイン」です。「ドメイン」は、全てのコンピュータやユーザ情報を一元管理するドメインコントローラが頂点となって構成されているネットワークです。したがって、ユーザー名やパスワードはドメインコントローラに登録するだけでよく、他のサーバー（メンバサーバーと呼ばれる）やクライアントはドメインの一員と見なされドメインコントローラのみで管理することができます。ドメインは、大規模なネットワークで管理しやすいことが何よりの特徴です。

ワークグループの共有リソースを利用するためには、各コンピュータにユーザー名とパスワードをあらかじめ登録し、アクセスするたびに入力しなければなりません。ドメインの共有リソースを利用するためには、ドメインコントローラのみユーザー名とパスワード登録するだけでよいのです。



## (2) コンピュータの接続形態

LANに接続したコンピュータの役割毎に、名前がつけます。サーバーは、種々のサービス（ファイル提供サービス、プリンタ提供サービスなど）を行います。一方、クライアントは、サービスを受けるコンピュータのことです。

コンピュータの接続形態には大きく2種類あります。あるときはサーバーとして機能しているコンピュータが、こんどは他のコンピュータのサービスを利用するクライアントとなるように、それぞれのコンピュータがサーバーとクライアントの両方の機能を持てる接続形態をピア・ツー・ピア型といいます。ピア・ツー・ピア型の接続形態はワークグループ管理しかできません。これに対して、サーバー専用のコンピュータが設置され、クライアントとサーバーが明確に区別される接続形態をサーバークライアント型といいます。最近の学校では、専用のサーバーOS（オペレーティングシステム）を用いたサーバークライアント型が増えてきました。サーバーは常時電源がオフになることはなく、日常のメンテナンスも必要なため、特定の管理者によって管理されます。



## (3) 対応するOS

### ア ワークグループ管理

Windows95、98、98SE、Me、NT4.0WS、2000、XP、Vistaは、クライアントとサーバーのどちらでも利用できます。サーバー専用OSである「WindowsServer2003」「Windows2000Server」「WindowsNT4.0server」は、サーバーとして利用することが可能です。

MacはOSXであれば、Windowsネットワークに比較的容易にクライアントとしてもサーバーとしても接続することができます。OS9以下をWindowsを中心とするネットワークに接続したいのであれば、「DAVE」(右図)と呼ばれる専用ソフトウェアを勧めます。



### イ ドメイン管理

ドメイン管理できるOSは、サーバー専用のOSです。Windowsには「WindowsServer2003」「Windows2000Server」「WindowsNT4.0server」、Macintoshには「MacOSXserver」があります。

ドメイン管理される側（クライアント側）のOSは、Windows95、98、98SE、Me、NT4.0WS、2000、XPPro、Vista(Business、Enterprise、Ultimate)になります。ただし、Windows95、98、98SE、Meをドメイン管理するには、特別な方法が必要でMicrosoft社では一般向けには推奨していません。ネットワーク上の共有リソース（共有フォルダや共有プリンタ、共有スキャナ）を利用するだけであれば、Windows95、98、98SE、Me、MacOSXでも比較的容易に設定可能です。注意してほしいことは、**ドメイン管理されているネットワークにWindowsXPHome、VistaHome(Basic、Premire)で動作しているコンピュータを接続することは不可能**ということです。

### ウ NTドメイン（Windowsドメイン）

NTドメインとは、「WindowsNT4.0server」で実装していた管理方法です。NTドメインは、全てのユーザーを一元管理することができますが、コンピュータの一元管理はできません。

### エ ActiveDirectory（アクティブディレクトリー）ドメイン

ActiveDirectoryドメインとは、「WindowsServer2003」「Windows2000Server」で実装している管理方法です。ActiveDirectoryドメインは、全てのユーザーだけでなく、コンピュータ等までを一元管理することができます。ActiveDirectoryをインストールしなければ、ワークグループで管理することになります。

## (4) プロトコル（TCP/IP）

プロトコルとは、ネットワーク上でコンピュータ同士が正しく通信を行うための手順や方法を定めた規約です。インターネット標準は、TCP/IP(Transmission Control Protocol/Internet Protocol)というプロトコル群です。校内ネットワークのプロトコル群もこのTCP/IPが主流です。

TCP/IPプロトコル群には、HTTP(Webページ等)、FTP(ファイル転送等)、SMTP(メール送信用)、POP3(メール受信用)等があります。このプロトコルが異なると、情報のやりとりができなくなります。



## (5) MACアドレス

MACアドレスとは、メディアアクセスコントロールアドレス(Media Access Control address)の略で、NICには全てMACアドレスが割り振られています。MACアドレスは、世界に一つしかありません。言い換えれば、私たちヒトのDNAや指紋のようなものと考えてください。LANやインターネットでは、NICに割り振られたMACアドレスをたよりにデータの送受信が行われます。私たちは、このMACアドレスを変更することはできませんが、無線LANアダプタやプリンタサーバー等の機器をネットワークに接続する際に必要となることがしばしばあります。NICのMACアドレスは機器本体に記されていますが、見つけれない場合には、NICのプロパティで確認します。

## (6) コンピュータ名

ネットワークの世界では、本来ホスト名と呼ばれます。コンピュータ名という言い方は、Windowsに限られたものであることに注意が必要です。

LANに接続されたコンピュータは、コンピュータ名(ホスト名)で識別されます。コンピュータ名(ホスト名)は、コンピュータの持ち主やネットワーク管理者が設定できます。言い換えれば、私たち一人一人につけられている氏名のようなものと考えてください。同姓同名の人がいた場合、氏名だけでは区別できないのと同じように、同じコンピュータ名が存在すると他のコンピュータから区別できなくなります。

## (7) IPアドレス

ネットワークではコンピュータ同士が情報のやりとりを行います。そのとき、相手のコンピュータを探す際に必要になるのがIPアドレスです。言い換えれば、住所と考えてください。TCP/IPプロトコルによる通信では、IPアドレスを用いてネットワーク上のコンピュータを特定しています。

私たち人間社会では、別々の場所に同じ住所が2つ存在することはありません。これと同じように、ネットワークの世界でも、同じネットワークに存在するIPアドレスは一つのみです。同じネットワークに二つのIPアドレスは存在できないのです。

### ア グローバルIPアドレス

インターネット上でIPアドレスに重複があってはならないため、割り当てなどの管理は各国の「Network Information Center」が行っています。このような、世界に唯一のIPアドレスをグローバルIPアドレスといいます。現在のIPアドレスでは約42億台までしかインターネットに接続することができず、IPアドレスが足りなくなることが懸念されています。このため、128ビットのIPv6の標準化が進行しています。

### イ プライベートIPアドレス

LANの内部にあるような、直接インターネットに接続しないコンピュータには、ネットワーク内部だけで利用できるIPアドレスを割り振ります。このIPアドレスをプライベートIPアドレス(ローカルアドレス)といいます。このIPアドレスはネットワーク管理者やネットワークを構築する人が割り振ることができます。プライベートIPアドレスとして利用できるアドレスは、次のように決められています。本講座の実習では、クラスCのプライベートIPアドレスを用います。

クラス	IPアドレス範囲	サブネットマスク	接続可能台数
A	10. 0. 0. 0 ~ 10.255.255.255	255. 0. 0. 0	16,777,216台
B	172. 16. 0. 0 ~ 172. 31.255.255	255.255. 0. 0	65,536台
C	192.168. 0. 0 ~ 192.168.255.255	255.255.255. 0	256台

クラスは、Aにいくほど上位に位置付けられる

## (8) IPマスカレード

グローバルIPアドレスが一つしかない場合に、それを複数個のプライベートIPアドレスに変換してくれる機能のことを言います。また、クラス上位のプライベートIPアドレスが1個あった場合、それより下位であれば、複数個のプライベートIPアドレスに変換してくれます。つまり、学校でインターネットに接続できるIPアドレスが一つしかない場合でもIPマスカレードを導入することにより、コンピュータ全台をインターネットに接続することができるようになります。

### (9) NAT (ナット)

ネットワークアドレストランスレーション (Network Address Translation) の略語です。ネットワークを他のネットワークに接続したい場合、IPアドレスが異なるためにそのままでは接続できません。そこで、IPアドレスを他のIPアドレスに変換してくれる機能のことを言います。

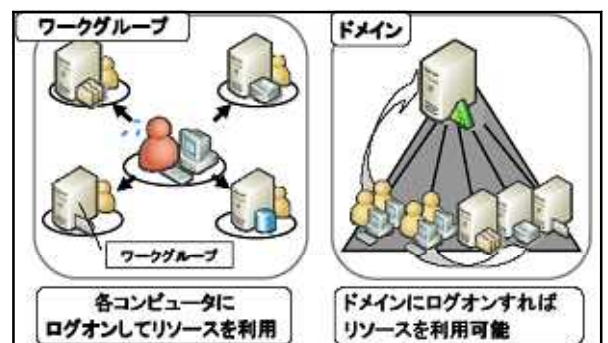
最近、IPマスカレードの機能を含めてNATというようになりました。これらの機能は、ルータやサーバーOSについてくることが多くなってきたことから、セキュリティ対策としても用いられています。この方法を用いると、外部からネットワーク内部のコンピュータが見えなくなるため、不正な侵入や攻撃の防止ができ、セキュリティの向上につながるわけです。

### (10) セグメント (segment)

「全体をいくつかに分割したうちの一つ」の意図をあらわします。ネットワークでは、大規模なネットワークを構成している個々のネットワークのことを言います。教師用ネットワークと児童生徒用ネットワークを分けるといったセキュリティ対策として現在導入されることが多くなっています。セグメントを分ける方法としては、IPアドレスを変える、例えば、教師用は「192.168.1.」を使って、児童生徒用は「192.168.2.」を用いるといった方法をとります。また、物理的に、ルータやVLAN対応のハブを設置することによりセグメントを分けることができます。

### (11) ユーザーIDとパスワード

ネットワークに接続されたコンピュータは「誰が使ってもいいのかわからない」という許可を与える必要があります。ユーザーID (ユーザ名、単にIDとも言う) は、コンピュータを使うことを許された人に与えられるもので、パスワードはそのことを証明する暗号です。これらのものをユーザーアカウント、または、ユーザー情報と言い、ユーザーアカウントを管理することをユーザー管理と言います。



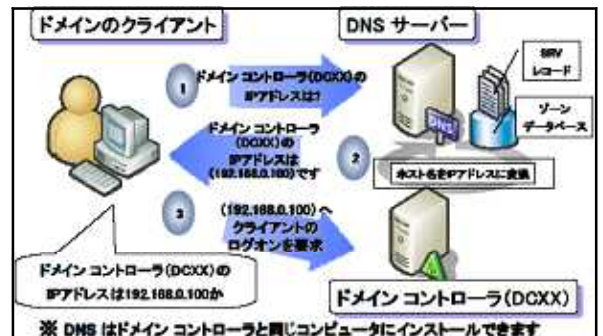
ローカルユーザーアカウント：コンピュータにログオンするために設定するユーザーIDとパスワードのこと。ワークグループ管理されたネットワークでは、各コンピュータにログオンする必要がある。サーバーとなるコンピュータには、全てのローカルユーザーアカウントを登録する必要がある。

ドメインユーザーアカウント：ドメインにログオンするために設定するユーザーIDとパスワードのこと。ドメイン管理されたネットワークでは、ネットワークにログオンするだけでよいため、ユーザーIDとパスワードをドメインコントローラだけに設定する(各コンピュータに設定する必要はない)。

### (12) DNSサーバー

ネームサーバーや名前解決サーバーとも呼ばれています。DNS (Domain Name System) は、インターネット上にあるコンピュータの名前を識別して対応するIPアドレスに変換する役目をもちます。

本来、インターネット上では、IPアドレスで各コンピュータを識別しています。しかし、私たちが、数字のみで構成されているIPアドレスを利用してインターネット上のコンピュータにアクセスすることは非常に困難ですし、IPアドレスを公開することはセキュリティ上問題があります。そこで、IPアドレスの代わりに完全修飾ドメイン名を使用してインターネット上のコンピュータにアクセスできるようにしています。私たちはWebページを閲覧するとき、ブラウザアドレス欄に「http://www1.iwate-ed.jp/」のように入力します。DNSがあるとIPアドレスを入力することなく、覚えやすい名前を入力するだけでWebページを閲覧できるのです。DNSサーバーは、このDNSサービスを提供しています。逆に、DNSサーバーソフトがなければ、IPアドレスをい



ちいち入力しなければなりません（インターネットが普及し始めた頃のWebページのほとんどは、DNSサーバーがとても高価で導入されていなかった。そこで、IPアドレスを入力して閲覧させていた）。

ActiveDirectoryドメインのクライアントコンピュータは、ネットワークにログオンするときにドメインコントローラを探します。このとき、DNSサーバーを参照してドメインコントローラを見つけ出す仕組みになっています。「Windows2000Server」と「WindowsServer2003」のActiveDirectoryではDNSサーバーが必須ですし、サーバークライアント型のイントラネットやインターネットを構築する際には必須のサービスです。

### (13) WINSサーバー

WINS (Windows Internet Naming Service) サーバーは、NetBIOSに対応したネームサーバーです。Windows95、98、98SE、Meまでの製品は、通信アプリケーションの規格としてNetBIOSが用いられてきました。NetBIOSは、MS-Networks、LANManager、WindowsForWorkgroups、WindowsNT、Windows95、98、98SE、Meを用いたネットワーク上で「ファイル共有」「プリンタ共有」「ポップアップメッセージ受信」「ブラウジング」等を行うときに用いられています。これらを動作させるネットワークアプリケーションの中にはNetBIOSしか対応していないものがあります。

ワークグループで構成しているネットワークで以下のような経験をした先生はいませんか？「古い98SEマシンをファイルサーバにしたとき、あるXPマシンからはブラウジングもできるしファイル共有もできるのに、別のXPマシンからはブラウジングもファイル共有もできない。」これは、同じWindows XPでも、製品版とOEM版では使っているネットワークアプリケーションの仕様が異なっていたり、同じOEM版だとしても仕様が異なっていたりするためです。こういった場合には、「XPマシン側プロトコルにNetBIOS互換プロトコルをインストールする(CDからインストールする必要があるマシンもある)」「98SEマシン側が使用するネットワークにWindowsネットワークを選択する」「98SEマシン側プロトコルにNetBEUI (NetBIOS Extended User Interface) をインストールする」のも対応策の一つです。

また、「XPマシンをファイルサーバにしたとき、2000/XPマシンからはブラウジングもできるしファイル共有もできるのに、Windows95/98/98SE/Meマシンからはブラウジングもファイル共有もできない。」といった現象の場合には、XPマシン側に「NetBIOS互換プロトコルをインストールしてみる」とよいでしょう。ActiveDirectoryで構成しているネットワークの場合は、ネットワークに接続するクライアントのOSにWindows95、98、98SE、Meがあるとすれば、WINSサーバーの構築は必須となります。

### (14) ファイルサーバー

ハードディスク等の記憶装置をネットワーク上の他のコンピュータと共有し、外部から利用できるようにするサービスをファイル共有サービスといいます。このサービスを提供する役目を担うのがファイルサーバーです。ファイルサーバ上にあるファイルは、許可されていれば誰でも他のコンピュータから読みこんだり書きこんだりできるため、データの一括管理が容易になります。

ファイルサーバの導入によりコンピュータ間でのファイルをやりとりする際の煩雑さが解消され、個々のコンピュータに保存されているファイルの整合をとる必要がなくなります。他人が途中まで編集したデータにその場で手を加えて完成させることも可能になります。

現在、校内LANの最も基本的なサービスとして利用されています。最近では、ファイルサーバ機能だけを持った専用コンピュータや専用ハードディスクも市販されており、それらを「NAS」(Network Attached Storage)と呼んでいます。

ただし、本来、ネットワークの世界では、ファイル共有は同一セグメント内で有効であり、セグメントの異なるネットワークでファイル共有はできません。

### (15) プリントサーバー

プリンタを他のコンピュータと共有し、外部から利用できるようにするサービスをプリンタ共有サービスといいます。このサービスを提供する役目を担うのがプリントサーバーです。

印刷したいコンピュータは、プリントサーバに印刷データを送信した時点で印刷作業から解放され、後はプリントサーバがスプールしたデータに従って処理します。このため、直にプリンタを接続している場合に比べ、各コンピュータにかかる負担を軽減することができます。プリントサーバ機能だけを持った小型専用プリントサーバーも市販されています。

## (16) Webサーバー

http(HyperText Transfer Protocol)を利用して、インターネット上でWebページを公開するサービスをWebサービスといいます。このサービスを提供する役目を担うのがWebサーバーです。Webサーバーは、HTML文書や画像などの情報を蓄積しておき、ブラウザなどのクライアントソフトウェアの要求に応じて、インターネットなどのネットワークをとおして情報を送信する役割を果たします。

初期のWebサーバは、あらかじめ用意しておいたデータを送出する機能しか持ちませんでした。しかし、最近では機能が増え、要求に応じてプログラムを実行し、結果をクライアントに送信する動的ページ生成の機能や、データベースと連携した処理機能などを持つものも登場してきました。中でもCGIやSSIなどの拡張機能は歴史が古く、最も一般的に利用されています。Java言語を利用したJavaサーブレットやJSP、Microsoft社独自の技術であるASPなどを利用したWebサイトも増えてきています。これらの技術を利用したものが、Webアプリケーションとサーバーサイドアプリケーションの一部です。Webアプリケーションには、グループウェアや掲示板、チャット、ブログ、アクセスカウンタ等があります。Webアプリケーションを動作させるためには、WebサーバーソフトウェアとWebアプリケーション、それと拡張機能を用いるためのモジュールが必要です。今回の研修で使用する当総合教育センターの「情報サイト8」は、ASP(ActiveServerPages)を用いて開発しており、拡張機能を用いるためのモジュールとして「BASP21」を用いています。

Webサービスの提供には、Webサーバー用のソフトウェアがまず必要になります。Webサーバーソフトウェアとしては、フリーソフトの「Apache」「BlackJumboDog」「ANHTTPServer」やMicrosoft社の「IIS(Internet Information Services)」等があります。本講座では、「IIS」を用います。

## (17) FTPサーバー

ftp(File Transfer Protocol)を利用して、インターネットやイントラネットのネットワークでファイルを転送するサービスをFTPサービスといいます。このサービスを提供する役目を担うのがFTPサーバーです。セグメントの異なるネットワークでも、ファイル共有ができるのでたいへん便利です。FTPサーバーは、ファイルを蓄積しておき、ftpクライアントソフトやブラウザの要求に応じて、インターネットなどのネットワークをとおしてファイルを送受信する役割を果たしています。

学校における利用方法は、作成したWebページのデータをWebサーバに転送する際に用いることが一般的ですが、セキュリティ性が高いことから校内LANにおいても利用されるようになってきました。(昨今、セキュリティを高めるために、NAT機能を持つルータやコンピュータが設置されていますが、設置することによりネットワークのセグメントが異なってしまう、ファイル共有ができなくなる等の問題も生じています。具体的には、職員室で作成したデータをコンピュータ室のサーバーに保存できない等です。ftpサーバーはネットワークのセグメントに左右されずにファイルの転送が可能です。)

ftpサービスを提供するためには、ftpサーバーソフトウェアが必須です。Webサーバーソフトウェアとしては、フリーソフトウェアの「BlackJumboDog」やMicrosoft社の「IIS(Internet Information Services)」等があります。本講座では、手軽に導入できる「BlackJumboDog」を用いて実習を進めます。

## (18) メールサーバー

ユーザーの電子メールの送受信を行なうサービスをメールサービスといいます。このサービスを提供する役目を担うのがメールサーバーです。実際には、SMTP(Simple Mail Transfer Protocol)を利用して電子メールを送信するサービスと、POP3(Post Office Protocol version 3)を利用して電子メールを保管してユーザからの受信要求に対応するサービスの2つからなります。同じコンピュータがSMTPサービスの提供とPOP3サービスの提供を兼ねていることが多いため、それら2つをあわせてメールサーバーと呼ぶようになりました。(コンピュータの負荷を減らすために、2つのサービスを別々のコンピュータで稼働することもある。)

メールサービスを提供するためには、メールサーバーソフトウェアが必須です。メールサーバーソフトには市販品、フリーソフトウェアとも数多くあります。県立学校で利用されている「I-mail」やフリーソフトウェアである「BlackJumboDog」もその中の一つです。本講座では、「BlackJumboDog」を用いて実習を進めます。

## (19) プロキシサーバー

代理サーバーとも呼ばれます。外部との回線の負荷を軽減するために、一度読みこんだデータをしばらく保存しておき（キャッシュ機能）、クライアントからの要求に応じて読み込んだデータを提供するサービスのことをプロキシサービスといいます。このサービスを提供する役目を担うのがプロキシサーバーです。例えば、クライアントがブラウザにどこかのWebページを表示させようとしています。すると、まず、クライアントはプロキシサーバーにアクセスします。キャッシュした中に、クライアントが要求したWebページのデータがあるときには、プロキシサーバーはそのデータをクライアントに提供します。データがないときには、プロキシサーバーがクライアントに代わってWebページにアクセスして、そのデータをキャッシュします。つまり、私たちが利用しているコンピュータからWebページを閲覧しに行くときには、実際にはプロキシサーバーにキャッシュされているデータを見ているのであって、直接インターネットの世界にあるWebページを見ているわけではありません。

調査したところ、県内の学校は、インターネットに接続する際に必ずプロキシサーバーを経由しています。このことにより、外部のネットワークに接続する際に発生する負荷が軽減され、「インターネットに繋がらない」という現象をできるだけ軽減しています。

プロキシサーバーは、（設定にもよるが）数日～数ヶ月データをキャッシュしています。クライアントから更新の指示があると（ブラウザで更新ボタンを押すと）、再度新しいWebページのデータを取りに行きます。したがって、しばらくぶりに閲覧するWebページやたびたび閲覧するWebページをブラウザに表示させる際には、「更新ボタン」を押しましょう。そうしないと、場合によっては古いWebページを閲覧しているおそれがあります。しかし、それでも見かけ上は更新されていますが、実際にはプロキシサーバーが見に行っています。更新ボタンをクリックすることは言い換えれば、「プロキシサーバーさん、新しい情報をとってきて！」と命令するボタンなのです。このプロキシサーバーを用いずに直接自分のコンピュータで見に行き、更新されていたときだけプロキシサーバーにキャッシュさせる方法があります。それは、キーボードの「Ctrl」キーを押しながら更新ボタンをクリックするのです。これは言い換えれば、「プロキシサーバーさん、見に行くのはちょっと待って！自分で見に行くから・・・もし更新されていたらその情報を君にあげるね。」というところでしょうか。

プロキシサービスには、Webページをキャッシュするhttpプロキシだけでなく、ftpによるファイル転送ルートをキャッシュするftpプロキシ、メール送受信ルートをキャッシュするメールプロキシ等があります。

また、プロキシサーバーは、httpやftpのようなTCP/IPプロトコル群を利用した外部からの侵入を防ぐことができます（自分のコンピュータは見に行っていない訳なので・・・）。このことから、最近では、プロキシサーバーにNICを2枚装着してLANとインターネットの境界に設置し、外部からの侵入を食い止める役割を持たせたり（ファイアウォール機能）、IPアドレスを変換させたり（NAT/IPマスカレード機能）する傾向があります。

プロキシサービスを提供するためには、プロキシサーバーソフトウェアが必須です。プロキシサーバーソフトには市販品、フリーソフトウェアとも数多くあります。本講座では、「BlackJumboDog」を用いて実習を進めます。

## (20) ログ

ログとは、コンピュータの利用状況やデータ通信の記録を取ることや記録そのものをいいます。操作やデータの送受信が行われた日時と、行われた操作の内容や送受信されたデータの中身などが記録されます。Webサーバー・FTPサーバー・メールサーバー・プロキシサーバー等はログを取ることができます。つまり、「いつ、どのコンピュータが（場合によってはどのユーザーが）、どのIPアドレスで、どのWebページの、どのファイルを閲覧した」「いつ、どのIPアドレスを持つコンピュータが、誰に、どのメールを送ったか」「いつ、どのコンピュータが、どのWebページから、どのファイルをダウンロードした」等の記録が全て細かく残ります。

## (21) DHCPサーバー

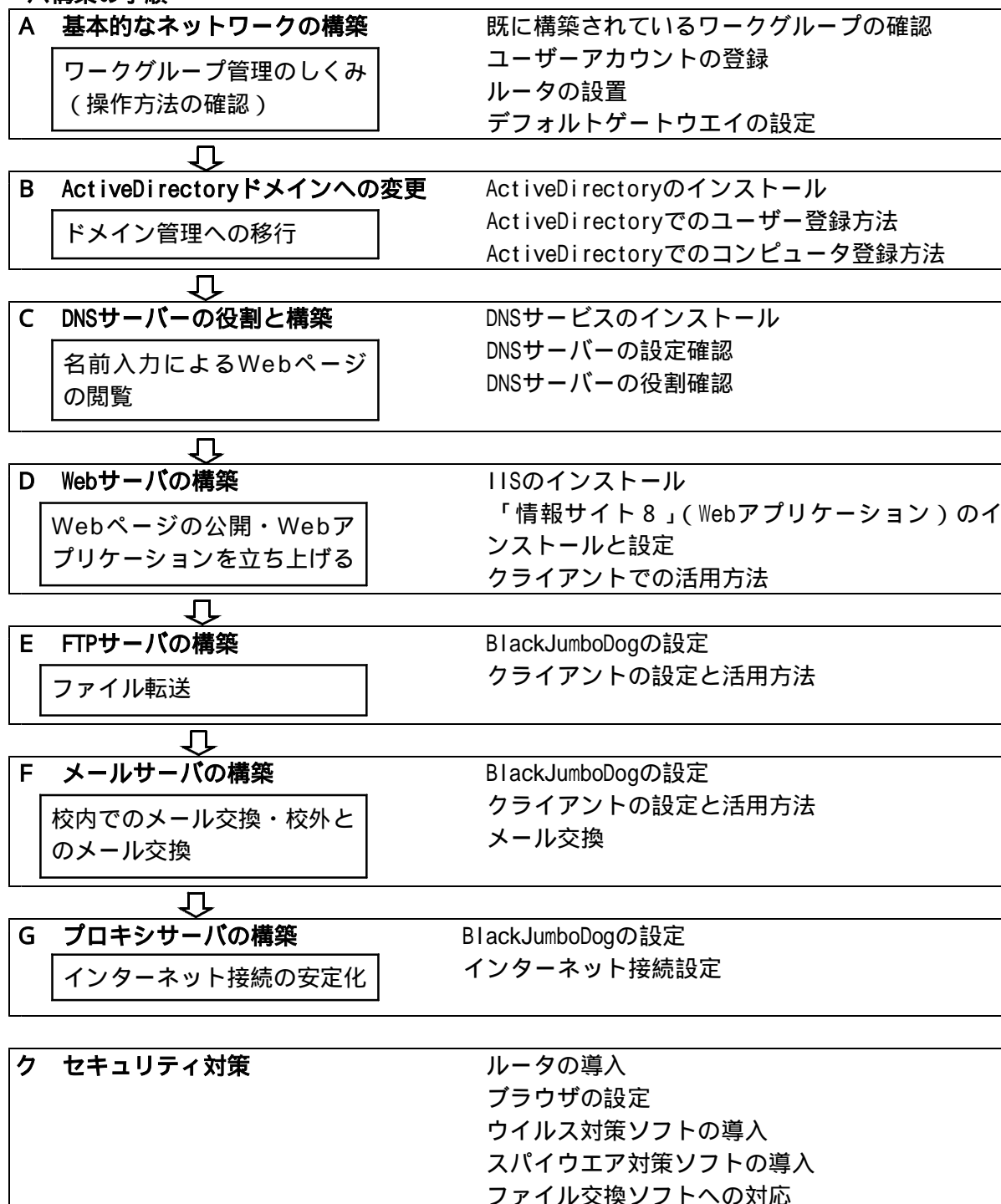
DHCP（Dynamic Host Configuration Protocol）を利用して、IPアドレスをコンピュータに自動的に割り振るサービスをDHCPサービスといいます。このサービスを提供する役目を担うのがDHCPサーバーです。

DHCPサーバーは、クライアントがネットワークに接続しようとする空いているIPアドレスを自動で割り振ってネットワークに接続させます。また、クライアントが通信を終えると割り振ったIPアドレスを自動で回収し、他のコンピュータに割り当てます。DHCPを使うとネットワークの設定に詳しくない管理者やユーザーでも比較的容易にインターネットに接続することができます。

しかし、DHCPサーバーを安易に導入することは避けましょう。ある程度ネットワークの知識を持ったユーザーであれば不正侵入することが容易になりますし、ログに残されたIPアドレスは、コンピュータやユーザーを特定する材料にはなりません。県立学校では、セキュリティ上の観点と管理者責任という立場からDHCPサーバは導入していません。

既に、業者によってDHCPサーバーが導入されているのであれば、今述べてきたことを理解したうえで、人的セキュリティを充分強化する必要があります。

### 3 サーバ構築の手順



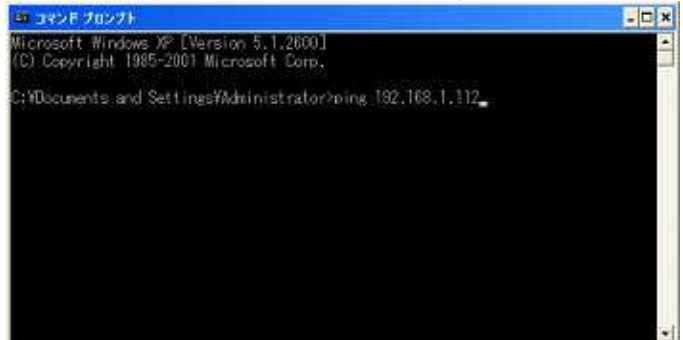


#### 4 基本的なネットワーク関係コマンド -

##### ping

ネットワークの障害検出用のパケットを特定のコンピュータに送信して、応答が返るかどうかによって、そのコンピュータが実際に稼働しているか、その間のネットワーク上に障害があるかを調べるコマンドです。正常であれば、パケットを送信してから応答が返るまでの往復時間が表示されます。1秒間待っても応答がない場合は、「Requested timed out」と表示され、相手先のコンピュータが稼働していないか、ネットワーク上に何らかの障害が起きていることが推測できます。

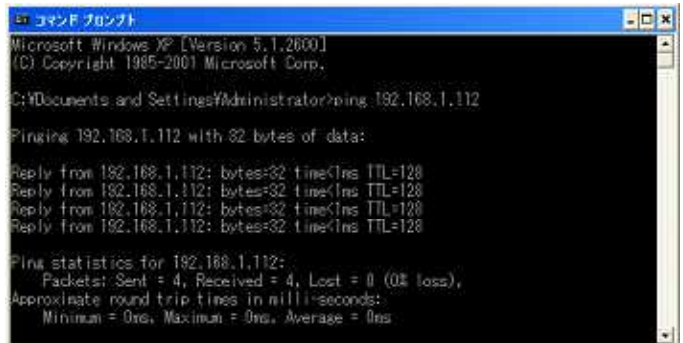
- ・デスクトップ左下の「スタート」ボタン「すべてのプログラム」「アクセサリ」「コマンドプロンプト」の順にクリックします。
- ・右図のように、「ping 192.168.1.112 (相手先のIPアドレス)」と入力した後、「Enter」キーを押します。  
は半角スペース空白



```
コマンドプロンプト
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.1.112
```

- ・pingが自動的に4回実行されて、右図のような結果が表示されます。



```
コマンドプロンプト
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

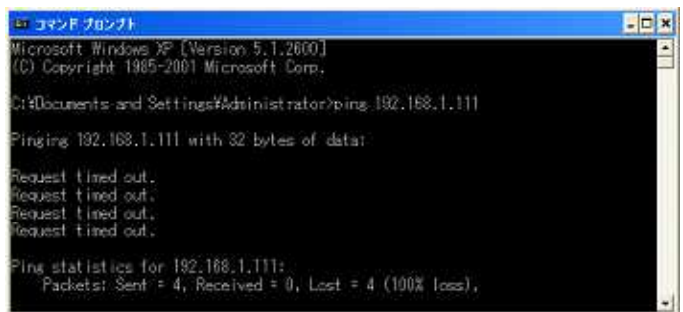
C:\Documents and Settings\Administrator>ping 192.168.1.112

Pinging 192.168.1.112 with 32 bytes of data:

Reply from 192.168.1.112: bytes=32 time<ms TTL=128
Reply from 192.168.1.112: bytes=32 time<ms TTL=128
Reply from 192.168.1.112: bytes=32 time<ms TTL=128
Reply from 192.168.1.112: bytes=32 time<ms TTL=128

Ping statistics for 192.168.1.112:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- ・LANに接続していない場合には、右図のように表示されます。



```
コマンドプロンプト
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.1.111

Pinging 192.168.1.111 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

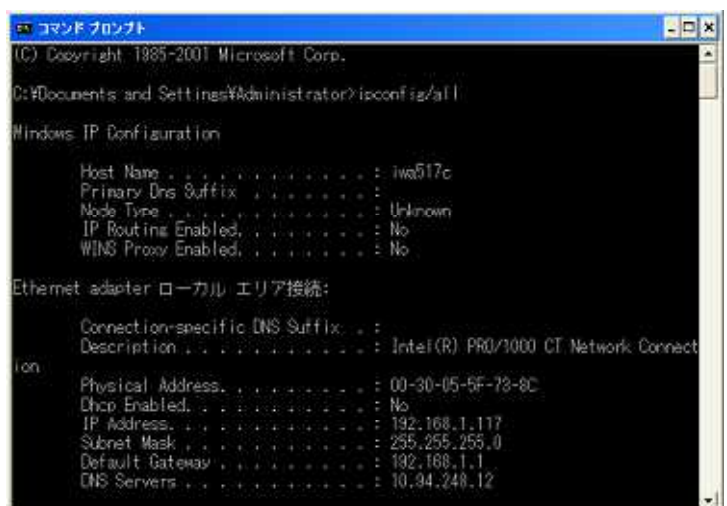
Ping statistics for 192.168.1.111:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

##### ipconfig

自分が使っているコンピュータのIPアドレスなど、NICに関する詳細な情報を表示します。なお、Windows95/98/Meは「winipcfg」というコマンドを使います。

##### 【Windows2000/XP】

- ・デスクトップ左下の「スタート」ボタン「すべてのプログラム」「アクセサリ」「コマンドプロンプト」の順にクリックします。
- ・「ipconfig/all」と入力し「Enter]キーを押すと、右図のように表示されます。



```
コマンドプロンプト
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig/all

Windows IP Configuration

Host Name . . . . . : iwa517c
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter ローカル エリア接続:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 CT Network Connect
ion
Physical Address. . . . . : 00-30-05-5F-78-8C
Dhcp Enabled. . . . . : No
IP Address. . . . . : 192.168.1.117
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DNS Servers . . . . . : 10.94.248.12
```

##### 【Windows95/98/Me】

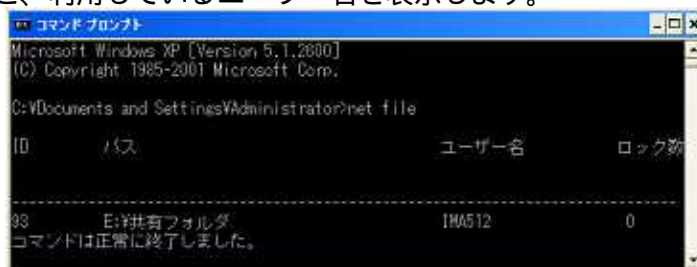
- ・デスクトップ左下の「スタート」ボタン「ファイル名を指定して実行」の順にクリックします。
- ・「winipcfg」と入力し「Enter]キーを押します。



## net file

共有フォルダを使って公開しているファイルへのアクセス状況を知ることができます。他のユーザーによって開かれている共有ファイルの一覧と、利用しているユーザー名を表示します。

- ・デスクトップ左下の「スタート」ボタン  
「すべてのプログラム」 「アクセサリ」 「コマンドプロンプト」の順にクリックします。
- ・「net file」と入力し「Enter」キーを押すと、右図のように表示されます



## 5 サーバー関係のトラブル

サーバー関係のトラブル原因は数多くあり、それら全てを網羅することは不可能です。また、校内サーバの場合、それぞれの校内ネットワークの特性に応じた設定になっていますから、トラブルが起こりやすい部分は学校によって異なります。しかし、サーバー関係のトラブルのほとんどは、クライアントがネットワークやサーバーに「つながらない」「何かの機能が使えなくなった」といったクレームから発覚します。ここでは、サーバーに起因するものに限定してトラブルの内容を説明します。

### (1) ドメインコントローラ関係

ドメインで構成されているネットワークのトラブルシューティングは専門的な知識が必要で、私たち教員では対処不可能のトラブルが数多くあります。また、ドメインコントローラのトラブルは、校内ネットワークの全てに関わることになるので、変な設定をしてしまうと2度と復旧不可能になってしまいます。

ここでは、私たち教員がある程度まで対処できるトラブルの内容を示しますが、無理をせず、メンテナンス業者に問い合わせることがよいでしょう。メンテナンス業者が契約されていない場合には、サーバを導入した市町村教育委員会に連絡してみましょう。その他、ネットワークに関するご相談に教育センター情報教育室では可能な限り対応していきますので、気軽にお問い合わせください。

#### ア ドメインに一部のユーザーがログオンできない

ユーザーアカウントが登録されていない

ユーザーアカウントを登録します

ユーザー名が違う

「Active Directoryユーザーとコンピュータ」でユーザーログオン名を確認します

パスワードが違う

パスワードは、大文字と小文字を区別します。パスワードを再設定します。

ログオン先のドメインが違う

ユーザーアカウントが登録されているドメインを選択し、再度ログオンします

アカウントがロックアウトされている

「アカウントがロックアウトされているため、ログオンできません。管理者に相談してください。」というメッセージが表示されます。「Active Directoryユーザーとコンピュータ」を起動後、対象ユーザーをダブルクリックし、「アカウントのロックアウト」のチェックをはずします。

ユーザーアカウントに制限が設定されている場合があります。以下のメッセージが表示される場合です。

アカウントの無効：「ユーザーのアカウントは使用不可能になっています。システム管理者に相談してください。」のメッセージが表示されます。

ログオン時間：「ユーザーのアカウントにはログオン時間の制限が設けられており、現在はログオンできません。ログオン可能時間にログオンしてください。」のメッセージが表示されます。

ログオン先：「ユーザーはこのワークステーションにはログオンできません。別のワークステーションでログオンしてください」のメッセージが表示されます。

アカウントの有効期限：「アカウントの有効期限が切れています。システム管理者に相談してください」のメッセージが表示されます。

「Active Directoryユーザーとコンピュータ」を使用し、対象ユーザーをダブルクリックして、制限項目の設定を確認し、必要に応じて制限をはずします。

#### イ ドメインに全てのユーザーがログオンできない

ドメインコントローラがダウンしている

ドメインコントローラが稼働しているかを確認し、再起動します

DNSサーバーがダウンしている

「ドメインが見つかりません」のメッセージが表示されます。DNSサーバーが稼働しているか確認します。DNSサーバーが稼働しているときには、名前解決ができていません。ドメインコントローラのアドレスとドメイン名がDNSサーバー側で一致しているか確認します。

ドメインコントローラもしくはDNSサーバーがクラッシュしている

業者に連絡して、Windows Server 2003及びActive Directory、DNSサーバー等を再インストール・再設定してもらいます

### (2) Webサーバー関係

グループウェアや掲示板等のブラウザで利用しているアプリケーションはほとんどがWebアプリケーションです。それらのソフトウェアが正常に動かない場合には、WebサーバーのトラブルかWebアプリケーションのトラブルかどちらかが原因であることがほとんどです。

#### ア Webサーバーソフトウェアが稼働していない

IISやApache、BlackJumboDog等のWebサーバーが稼働しているか確認します。一部のWebアプリケーションは、専用のWebサーバーを持っています。具体的には、スズキ教育ソフト社の「ハイパーキューブNet」「ハイパーキューブねっとJr」やJustsystem社の「つたわるねっと@フレンド」「つたわるねっとTeen's@フレンド」が該当します。これらのソフトは、セットアップする際に自動的にWebサーバーソフトをインストールする仕組みになっています。

稼働していないときには、Webサーバーソフトを起動することにより、トラブルは解決します。

#### イ Webサーバーソフトウェアが2つ以上稼働している

Webサーバーソフトは同一のコンピュータに2つ以上インストールされていると不具合を起こします。例えば、IISとBlackJumboDogの両方が稼働している場合がこれに該当します。

小学校や中学校で特に多いトラブルは、スズキ教育ソフト社の「ハイパーキューブNet」「ハイパーキューブねっとJr」やJustsystem社の「つたわるねっと@フレンド」「つたわるねっとTeen's@フレンド」がサーバーにインストールされている場合です。具体的には、スズキ教育ソフト社の「ハイパーキューブねっとJr」とJustsystem社の「つたわるねっと@フレンド」の両方がサーバーで稼働している場合やこれらどちらかのソフトが稼働しているにもかかわらずWindows標準のIISも稼働している場合です。

このようなときには、どちらか使っていない方のWebサーバーソフトを一つ終了させるとトラブルは解決します。

#### ウ Webアプリケーションに一部のユーザーがログオンできない

Webアプリケーション側にユーザーアカウントが登録されていないか、登録していたものが削除されているか、パスワードまたはユーザー名の登録ミスです。Webアプリケーションのマニュアルにしたがって再登録します。

#### エ Webアプリケーションに全てのユーザーがログオンできない

Webアプリケーションがダウンしている可能性が高いと思われます。Webアプリケーションを正しく稼働させます。

### (3) FTPサーバー関係

90%以上のトラブルは、FTPサーバーに登録されたユーザーアカウントが原因です。ユーザーアカウント（利用者）が正しく登録されているか確認し、場合によっては設定し直します。

次に多いのは、FTPサーバーが起動していないことによるものです。起動させればトラブルは解決します。

もう一つは、FTPサーバーで登録しているフォルダが何らかの原因でなくなってしまったことです。フォルダを作成し直します。

#### (4) メールサーバー関係

##### ア 全てのユーザーがメールを送信できない

SMTPサーバーのトラブルです。各種設定が正しくなされているか確認します。

##### イ 全てのユーザーがメールを受信できない

POP3サーバーのトラブルです。各種設定が正しくなされているか確認します。

##### ウ 全てのユーザーがメールを送受信できない

メールサーバーに登録しているユーザーアカウントが何らかの原因で削除されています。登録し直します。

メールサーバーがダウンしています。再起動をかけるか、メールサーバーソフトを再インストールし、設定し直します。

##### エ 一部のユーザーがメールを送信できない

そのユーザーが使っているメールソフトのSMTPサーバーが正しく設定されていません。SMTPサーバーのアドレスをきちんと設定します。

##### オ 一部のユーザーがメールを受信できない

そのユーザーが使っているメールソフトのPOP3サーバーが正しく設定されていません。SMTPサーバーのアドレスをきちんと設定します。

##### カ 一部のユーザーがメールを送受信できない

メールサーバーに登録しているユーザーアカウントが何らかの原因で削除されています。登録し直します。

メールサーバー側とメールソフト側のユーザー名もしくはパスワードが一致していません。正しく登録し直します。

メールソフト側の原因がほとんどですので、ユーザーが使っているメールソフトをまず調べてください。

#### (5) プロキシサーバー関係

プロキシサービスを提供する最大の目的は、クライアントのWebアクセスを快適にすることです。その他の目的は、ほとんどが付随して出てきたものと言っても過言ではありません。例えば、NICを2枚さしてNAT/IPマスカレード機能もつけようとか、フィルタリングをしようとか、ファイヤーウォールにしようといった事柄です。ですから、様々な要素を同じレベルで考えるのではなく、プロキシの本来の意味である「代理」ということをきちんとわきまえた上でトラブル対処に当たることが大切です。

##### ア 全てのユーザーがWebにつながらない

Webサービスに原因がないことがわかった場合、次に考えられる原因としてあげられることがプロキシサービスです。

プロキシサーバーが何らかの原因で稼働していない

プロキシサーバーを起動します

上位のプロキシが設定されていない

学校関係のプロキシサーバーは階層構造になって初めて、全世界のWebにアクセスできることを知りましょう。したがって、上位のプロキシをきちんと設定しましょう。設定されていなければ、構築したプロキシサーバーそのものがWebにアクセスできないこととなります。

設定しているセッション数が少なすぎる

学校で結構多いトラブルがこれです。プロキシをたてたのに、Webページの表示が遅いとか更新ボタンを押すとなかなか更新されずタイムアウトになってしまうといった現象です。プロキシサーバーに設定しているセッション数が少ないために、Webを見に行ったプロキシが膨大な時間をかけてキャッシュすることになってしまいます。「Black Jumbo Doc」の場合には、「キャッシュ」タブにある「サイズ(ディスク)」「サイズ(メモリ)」「最大サイズ」の数値を大きくとりましょう(プロキシサービスを稼働させているコンピュータの搭載メモリ容量や搭載ハードディスク容量にもよりますが・・・)。

## イ 一部のユーザーがWebにつながらない

クライアントのブラウザにプロキシサーバーのアドレスが設定されていない、間違っている  
正しく設定します。I Eの場合には、インターネットオプションの「接続」にある「詳細設定」  
で正しいプロキシサーバーのアドレスを入力します。

プロキシサーバーで利用許可を与えていない

「Black Jumbo Doc」の場合には、「利用許可」タブで利用するクライアントのアドレスを入力  
します。

## 6 校内ネットワーク関係のトラブル

LANに関するトラブルは、ケーブルや機器といった物理的な問題からソフトウェアの設定など、広い  
範囲で考えられます。原因を特定するには、トラブルの可能性がある場所を切り分けていく必要があり  
ますが、実は構築と同様の手順で確認していけば比較的容易に特定できます。考えられる原因を消去法  
で対処していくのです。その経験が多ければ多いほど、トラブルを解決するスキルも高まります。

トラブル原因の多くは意外に単純な場合が多く、深い知識が必要な深刻なトラブルは、むしろ少ない  
というのが経験からきた結論です。以下に、比較的単純なトラブルの原因をいくつかあげてみます。8  
0%以上はこれで対処できるはずです。

### ネットワークケーブルの接続

ネットワークケーブルがNICやハブにしっかり接続されていないことがあります。一度抜いてか  
らカチッと音がするまで接続して、ハブのランプが点灯しているか確認します。

### ネットワーク機器の電源

ハブ等の電源ケーブルがコンセントから抜けていないか確認します。

### ネットワークケーブルの取り回し

ネットワークケーブルは、曲げに弱い重いものがのるとすぐに断線してしまいます。別のネッ  
トワークケーブルで接続し直すことで繋がるようなときには間違いなく断線です。新しいケーブルと  
取り替えましょう。ネットワークケーブルの被膜が破れている場合も、すぐに新しいケーブルに取り  
替えます。

### ハブ等の初期不良

最近のネットワーク機器は、以前に比較して価格が下がっている反面、初期不良が多くなったと  
言われます。このような場合、予備の機器があれば、障害時にネットワークが使えないというトラブ  
ルを避けることができます。また、ハブは正常でも、ポートの一つが故障している可能性があります。  
そのときは、別のポートに差し込み接続確認を行うことで確認できます。

### ハブのカスケードポートの不理解

カスケードとは、ハブとハブをネットワークケーブルでつなぎあわせることいいます。ハブには、  
コンピュータ用ポートのほかに、ハブ用のカスケードポートがある場合があります。これには、カス  
ケードポートが独立してあるタイプと、スイッチによってカスケード用とコンピュータ用を切り替え  
るタイプがあります。ハブのタイプによって接続方法が違うので、接続方法をよく確認します。

### コンピュータ名の重複または消失

Windowsネットワークでは、コンピュータ名でコンピュータを識別するので、一つのLAN上にコ  
ンピュータ名は一つしか許されません。たとえ違うワークグループに所属していても、コンピュータ  
名の重複は許されません。もし重複すると、ネットワークに後から参加しようとしたコンピュータの  
ユーザーがネットワーク接続を拒否されます。

また、何らかの原因でコンピュータ名が消えている場合があります。正しいコンピュータ名が入力  
されているか確認しましょう。

### IPアドレスの重複または消失

何らかの原因でIPアドレスやサブネットマスクが消えている場合や入力ミスで同じIPアドレス  
が2台のコンピュータに割り振られている場合があります。正しいIPアドレスが入力されているか  
確認しましょう。

IPアドレスの重複はコンピュータ名の重複より深刻で、最悪の場合、重複するコンピュータば  
かりでなくネットワーク全体に影響が出て他のコンピュータ全てが接続できない結果を招く場合  
があります。

## **N I C の非認識**

コンピュータに取り付けている N I C が、何らかの原因で認識されなくなる場合です。きちんと差し込まれていない場合が最も多いので、一度抜いてからカチッと音がするまで接続します。それでも接続されない場合には、ドライバが壊れた可能性があるので、一度ドライバをアンインストールした後、再インストールして設定し直します。ドライバは最新のものを使いましょう。N I C のメーカー Web サイトからダウンロードすることができます。

### **中古パソコンの流用**

以前に使用したパソコンをそのままネットワーク上で再利用する際、以前の設定がそのまま残っているケースです。中古パソコンを転用するときの基本は、O S の再インストールです。

### **ユーザ名の消失または登録忘れ**

サーバーに作成した共有フォルダにアクセスできない原因で最も多いのがこれです。サーバー側のコンピュータに登録していたユーザ I D が消失しているのです。共有フォルダのアクセス権をグループで設定している場合には、特にも見つけにくい原因です。

### **パスワードの間違い**

サーバーに作成した共有フォルダにアクセスできない原因で次に多いのがこれです。サーバー側にユーザ登録をする際、うっかり間違えて入力を間違えてしまったというものです。クライアント側でいくら正しいパスワードを入力してもアクセスはできません。

年度末や年度初めのメンテナンスの際に、本人も無意識のうちに入力し直してしまう例が多いようです。

### **家庭内 L A N との共用コンピュータ**

小中学校の先生方のほとんどは、仕事用のコンピュータと家庭用のコンピュータが同一です。つまり、家で使っているコンピュータを学校に持ってきてネットワークに繋ぐ方が多いのです。家庭でのインターネット接続回線も A D S L や光ケーブルといったブロードバンド回線が主流になってきているため、家庭内 L A N を構築していたり、プロバイダから I P アドレスが割り振られていたりする環境が増えてきました。基本的に、1 台のコンピュータは一つのネットワークにのみ接続できる仕組みになっています。それは、情報漏洩やプライバシー保護といった様々な観点からそのような仕様になっています。

職員室 L A N に接続できる設定にしたのに、家に帰れば別の設定になってしまう訳ですから、当然、次に学校に持ってきたときには繋がりません。

昨今、別のネットワークにも接続できるようにするソフト（ I P アドレスやコンピュータ名を切り替えるソフト等）が出回ってきましたが、教育機関に勤務する私たち教員としてはあまり好ましい姿勢とは言えません。1 台のコンピュータを別のネットワークに接続すると言うことは、ネットワーク内にあるデータを別のネットワークに持ち込むことになります。情報漏洩につながった例が数多くあります。

どうしても、双方のネットワークに繋ぐ必要があるときには、きちんとルールを作成してください。繋ぐ方法はソフトで行うよりも、N I C を 2 枚装着して、2 つの I P アドレスを使い分けることをお勧めします。

## **7 クライアント側で行うセキュリティ対策**

### **(1) 個人情報保護**

教職員、児童生徒の個人情報が漏洩することのないようにしましょう。個人情報を簡単に説明すれば、個人が特定できる情報、個人の秘密に関わる情報です。住所やメールアドレス、成績等も該当します。成績は共有フォルダではなく、メディアに保存するなどして金庫に保管する必要があります。

県立学校ではコンピュータが 1 人 1 台利用できる環境にあり、学校外への持ち出しも許可されています。県内小中学校のほとんどでは、コンピュータは個人持ちのものを学校で利用しています。教職員や児童生徒の個人情報が、教職員のコンピュータやメディアに保存され、学校外に持ち出されることのないようにしなければなりません。これは、L A N が構築されているされていないの問題ではなく、一人一人がしっかりと心に刻み込み、すぐにでも実行する必要があります。

## (2) ウイルス対策

今やインターネット上にウイルスが存在することは当たり前となってしまいました。ウイルスに感染して恐いのは、被害者になることではなく加害者になることです。今のウイルスは、どんどん感染していきます。自分のコンピュータが感染したことがわからない場合、自分のコンピュータからどんどん他のコンピュータにウイルスが感染していきます。

家から持ち込んだデータを学校のコンピュータで利用しようとしてウイルスに感染させてしまった例もあります。その際、ネットワーク管理者は、全てのコンピュータからウイルスを駆除するのに結局3ヶ月もかかったそうです。その間、仕事で使うコンピュータはネットワークに接続できませんでした。最近では、データを壊し、ネットワークさえも破壊してしまうウイルスがいます。

今や、ウイルス対策ソフトをインストールして毎日最新のパターンファイルに更新することはコンピュータを利用する人の常識です。注意してほしいことは、コンピュータを購入した際に付属してきたウイルス対策ソフトが初期状態のままインストールされていることです。コンピュータに付属してきたウイルス対策ソフトは、体験版や試用期間が決められているものがほとんどです。必ず、ユーザ登録を行い（正規版を購入し）、毎年1回、お金を支払って更新手続きをしましょう。インストールした後も、最新のパターンファイルを常にダウンロードする必要があります。最近のものは、自動でパターンファイルをダウンロードしてくれるものがほとんどなので、自動アップデート欄を有効にしておきましょう。ウイルス対策ソフトはパターンファイルが命です。動作が遅くなるからと言って、アンインストールしたり、常駐機能を無効にすることはもってのほかです。

ウイルス対策用フリーソフトがいくつかあります。また、学校に対して無償提供している企業もあります。本講座の実習でも取り上げますが、「Kingsoft Internet Security 2007 Free」の入手先を以下に記載しておきます。

KINGSOFT Webページ (<http://www.kingsoft.jp/>)

大手企業や公的機関から機密情報や個人情報の流出する事件が激増しています。警察の捜査情報や被害者個人情報、自衛隊の機密情報、役所の個人情報等がインターネット上に流出した事件が有名です。教員のコンピュータが原因で「公立小学校の児童と教職員の名簿が流出した」事件もあります。これらの事件は、Winnyをとおして感染するウイルス「Antinny（アンチニー）」とWinnyに関係なく感染する「山田オルタナティブ」が原因となって引き起こされたものです。

「Antinny」は、ファイル交換ソフトWinny（ウイニー）を用いて入手したファイルから感染します。つまり、Winnyユーザーが感染の対象です。「Antinny」に感染すると、自分のコンピュータ内にあるファイルやデスクトップの画面がWinnyユーザーに流出します。さらに、自己増殖機能を持っているので、感染したコンピュータの中のファイルに自分自身をくっつけてばらまきます。流出したファイルは事実上回収不可能です。

「山田オルタナティブ」は、Winnyに関係なく感染するウイルスで、メールの添付ファイルやWebサイトからのダウンロードで感染します。つまり、Winnyユーザーでなくても感染します。「山田オルタナティブ」に感染すると、自分のコンピュータのファイルのみならず、自分自身のコンピュータの中身全てがインターネット上にWebページとして公開されます。また、「山田オルタナティブ」に感染したコンピュータ同士のリンク集も自動作成して、インターネット上に公開します。さらに、感染しているコンピュータに誘導するためのURLをインターネット上の掲示板やチャットに勝手に書き込みます。これらのページにアクセスし、特定のファイルを実行すると、「山田オルタナティブ」に感染します。「山田オルタナティブ」には自己増殖する機能はないものの、作成されたページは巧みなつくりになっており、人間の興味本位をくすぐりながらじわじわと感染を広げています。

これらのウイルスによる情報漏洩を防ぐためには以下のことを必ず実行しましょう。

### ア Winnyを使わない

Winnyがインストールしてあるパソコンに感染するAntinnyはWinnyとともに行動します。今年3月15日に、内閣官房長官が「確実な対策はWinnyを使わないこと」と国民に呼びかけました。

### イ ウイルス対策ソフトを利用する

既に利用している人（最新版パターンファイルがインストールしてあり、常駐機能が有効になっていることが条件）は安心です。利用していない人は、すぐに購入してインストールしてください。



Microsoft Windows セキュリティセンターのウイルス対策パートナー

<http://www.microsoft.com/athome/security/viruses/wsc/ja/default.aspx>

#### ウ 「Microsoft Update」を有効にする

Windowsを利用する人は「Microsoft Update(旧Windows Update)」の自動更新を有効にしましょう。「Microsoft Update」は、「Antinny」「山田オルタナティブ」が動作していると駆除してくれます。(ウイルス対策ソフトの場合は、これらのウイルスが動作していなくても駆除してくれます)

### (3) スパイウェア対策

本来、スパイウェアの定義は、「マイクロプロセッサの空き時間を借用して演算処理や通信を行うアプリケーションソフト」のことでした。スパイウェアは単独でインストールされることはなく、何かのソフトやツールと一緒にインストールされます。従来、スパイウェアで入手した情報が悪用されることはなく、むしろ、業務の自動化や企業の業務改善、製品の開発に用いられてきました。「自動化」の例として代表的なものは「Windows Update」ですから、これは必要なものと言えます。

しかし、昨今、個人のパソコンからユーザIDとパスワード、メールアドレス、IPアドレス等を盗むスパイウェアが増えてきています。さらに、ブラウザを開いただけでスパイウェアがインストールされることもあります。スパイウェアと聞くと、何かとても悪いことをするソフトウェアといった印象が当たり前になってしまいました。スパイウェアの定義は「パソコンを使うユーザの行動や個人情報などを収集すること」のみに変化してきたといっても過言ではありません。得られたデータはスパイウェアの作成元に送られます。「行動を収集」の例では「国際電話を勝手にかける」、「個人情報を収集」の例では「スパムメール」「ワンクリック詐欺」が挙げられます。

こういった現状から、校内のネットワークに接続するコンピュータには、ウイルス対策と併せてスパイウェア対策を施す必要がでてきています。

スパイウェア対策のフリーソフトがあります。ここでは、「Windows Defender」「Ad Aware SE」「Spybot」の入手先を以下に記載しておきます。

「Ad Aware SE」: LavaSoft (<http://www.lavasoftusa.com/japanese/>)

(家庭内個人のみ使用可。学校に持ち込むコンピュータで使用するためには製品版を購入する。)

「Spybot-Search & Destroy」: Spybot (<http://www.spybot.info/>)

(Windows全てのバージョンのOSに対応。Microsoftでも推奨しているソフトウェア。)

### (4) その他

「Google」では「Googleパック」として、ウイルス対策ソフトとスパイウェア対策ソフトを無償で提供しています。

予算的に、市販されている製品を校内のPC(持ち込みPCも含む)にインストールすることが難しい場合には、Googleパックを利用することも一つの方法です。

Googleパック

(<http://pack.google.com/>)





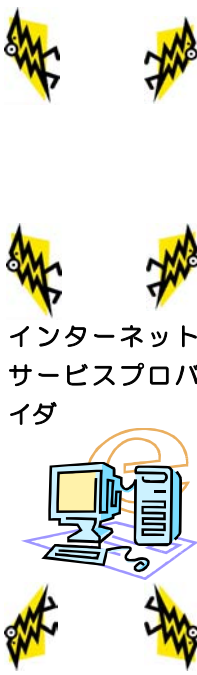
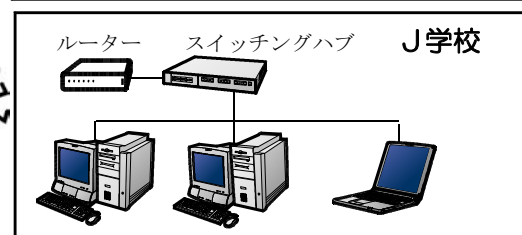
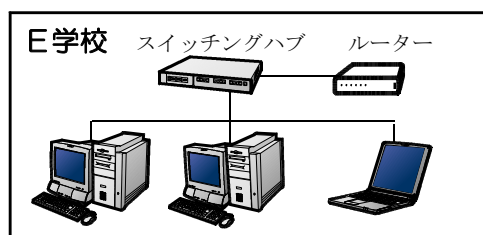
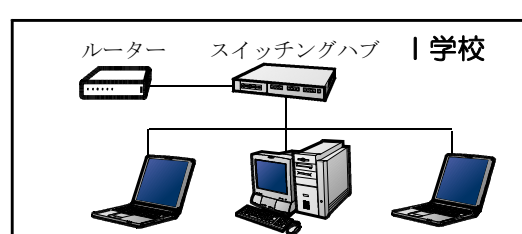
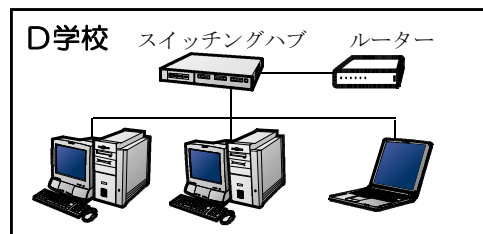
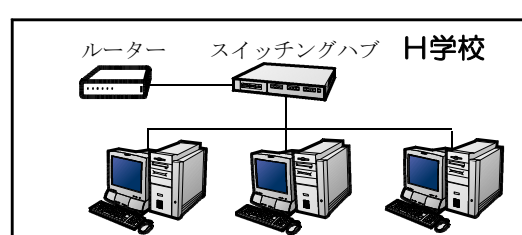
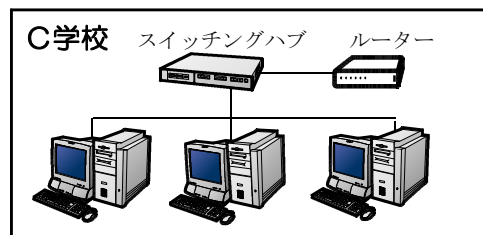
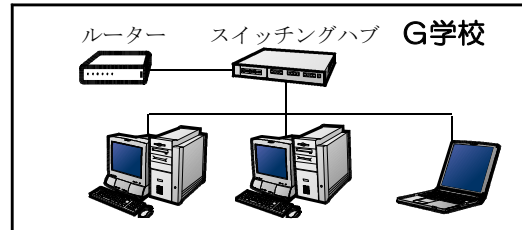
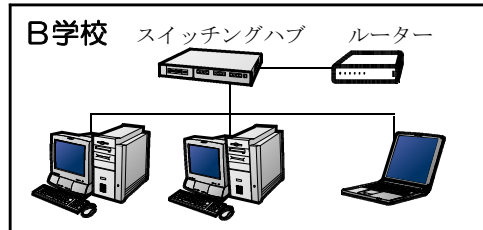
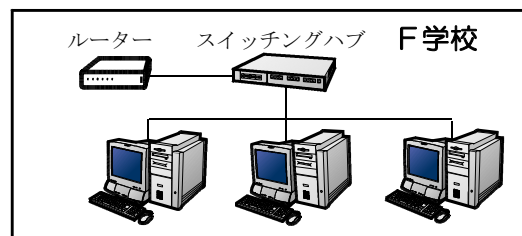
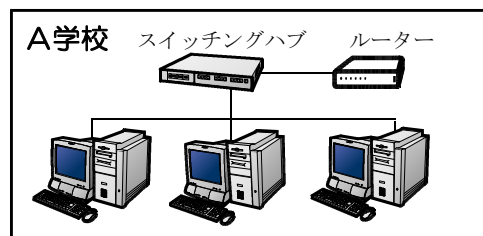
## II 操作編

サーバーを構築するに当たって大切なことは、「目的を明確にし、仕組みを理解し、必要なスキル（技能：知識と技術）を身に付け、わかりやすく構築し、サービスをユーザーに提供する」ことです。したがって、「サーバー＝コンピュータ」ではなく「サーバー＝サービス」といった考え方をしっかり持つ必要があります。つまり、「サーバーをマシンとしてのみとらえるのではなく、人への心がけとしてとらえる」気持ちが大切であると考えます。

コンピュータの設定やソフトウェアの操作方法を理解するというよりは、各サービスのしくみとはたらきや設定手順を理解していただければと思います。そのことにより、OSが変わってもサーバーソフトウェアが変わっても手順は共通ですから、ソフトウェアのマニュアルを見れば操作できるようになります。

本講座で構築するドメインネットワークの概要は以下のとおりです。




- 一人あたり一つの学校を担当することとします
- 最終的に、ActiveDirectoryドメインによるネットワークを構築します
- コンピュータは1校あたり3台用います
- 1台はドメインコントローラ兼各サーバ（DNS、Web、FTP、メール、プロキシ）です
- 2台はクライアントで、1台が教師用、1台が児童生徒用とします
- 各校のネットワークにルータを設けて、それを介してインターネットサービスプロバイダ（県または市町村または民間）に接続するものとみなします



## A 基本的なネットワークの構築（復習）

### 1 ワークグループ管理されているピアツーピアネットワークの構築

- ① コンピュータを起動してください。コンピュータの管理者でログインします。Server2003の場合、ユーザー名は「Administrator」パスワードは「root」です。Vistaの場合は、ユーザー名は「root」パスワードは「root」です。XPの場合は、ユーザー名は「Administrator」パスワードは空欄です。
- ② 下図中◎にご自分のgroup番号を朱書きしてください
- ③ 2台のクライアントのコンピュータ名を下図中○に朱書きしてください
- ④ 3台のコンピュータとスイッチングハブの有線接続を確認してください
- ⑤ 3台のコンピュータのコンピュータ名とワークグループ名を設定してください
- ⑥ 3台のコンピュータのIPアドレスとサブネットマスクを設定してください
- ⑦ 2台のクライアントからサーバーに接続できるかpingコマンドで確認してください

ワークグループ名 : grp◎	スイッチングハブ		
			
持たせたい役割	サーバー	教師用クライアント	生徒用クライアント
コンピュータ名	grp◎sv	iwa5○○c	iwa5○○c
サブネットマスク	255. 255. 255. 0	255. 255. 255. 0	255. 255. 255. 0
IPアドレス	<grp1> 192. 168. 1. 2	192. 168. 1. 51	192. 168. 1. 101
	<grp2> 192. 168. 2. 2	192. 168. 2. 51	192. 168. 2. 101
	<grp3> 192. 168. 3. 2	192. 168. 3. 51	192. 168. 3. 101
	<grp4> 192. 168. 4. 2	192. 168. 4. 51	192. 168. 4. 101
	<grp5> 192. 168. 5. 2	192. 168. 5. 51	192. 168. 5. 101
	<grp6> 192. 168. 6. 2	192. 168. 6. 51	192. 168. 6. 101
	<grp7> 192. 168. 7. 2	192. 168. 7. 51	192. 168. 7. 101
	<grp8> 192. 168. 8. 2	192. 168. 8. 51	192. 168. 8. 101
	<grp9> 192. 168. 9. 2	192. 168. 9. 51	192. 168. 9. 101
	<grp10> 192. 168. 10. 2	192. 168. 10. 51	192. 168. 10. 101

### 2 ローカルユーザーアカウントの登録

- ① サーバーに教師用と児童生徒用のローカルユーザーアカウントを下表の通りに登録してください。
- ② 教師用クライアントにユーザーアカウントを登録してください。
- ③ 児童生徒用クライアントにユーザーアカウントを登録してください。

	サーバー	教師用クライアント	児童生徒用クライアント
grp1	管理者 : Administrator パスワード : root	ユーザー名 : iwa502 パスワード : grp1iwa502	ユーザー名 : iwa503 パスワード : grp1iwa503
grp2	管理者 : Administrator パスワード : root	ユーザー名 : iwa508 パスワード : grp2iwa508	ユーザー名 : iwa509 パスワード : grp2iwa509
grp3	管理者 : Administrator パスワード : root	ユーザー名 : iwa514 パスワード : grp3iwa514	ユーザー名 : iwa515 パスワード : grp3iwa515
grp4	管理者 : Administrator パスワード : root	ユーザー名 : iwa520 パスワード : grp4iwa520	ユーザー名 : iwa521 パスワード : grp4iwa521
grp5	管理者 : Administrator パスワード : root	ユーザー名 : iwa505 パスワード : grp5iwa505	ユーザー名 : iwa506 パスワード : grp5iwa506
grp6	管理者 : Administrator パスワード : root	ユーザー名 : iwa511 パスワード : grp6iwa511	ユーザー名 : iwa512 パスワード : grp6iwa512
grp7	管理者 : Administrator パスワード : root	ユーザー名 : iwa517 パスワード : grp7iwa517	ユーザー名 : iwa518 パスワード : grp7iwa518

grp8	管理者: Administrator パスワード: root	ユーザー名: iwa523 パスワード: grp8iwa523	ユーザー名: iwa524 パスワード: grp8iwa524
grp9	管理者: Administrator パスワード: root	ユーザー名: iwa526 パスワード: grp9iwa526	ユーザー名: iwa527 パスワード: grp9iwa527
grp10	管理者: Administrator パスワード: root	ユーザー名: iwa529 パスワード: grp10iwa529	ユーザー名: iwa530 パスワード: grp10iwa530

### 3 ファイルサーバの構築

ファイルサービスのしくみやはたらきは既にご存じのことと思います。WindowsServer2003を用いているといっても、構築の方法も設定画面もWindowsXP等と同様です。

ここでは、教職員用フォルダ（フルアクセス）「teacher」と児童生徒用フォルダ（フルアクセス）「student」のフォルダをつくります。

注意することは、必ず、データドライブに作成することです。決して、OSがインストールされているシステムドライブ（たいていはCドライブ）に作成することは避けます。サーバが不安定になる原因となります。

操作方法は下記の通りですが、「(サ) はサーバーでの操作」を示し、「(ク) はクライアントでの操作」を示しています。（本実習では特に扱いません。学校に戻ったときの参考にしてください。）

#### (1) 共有するフォルダの作成

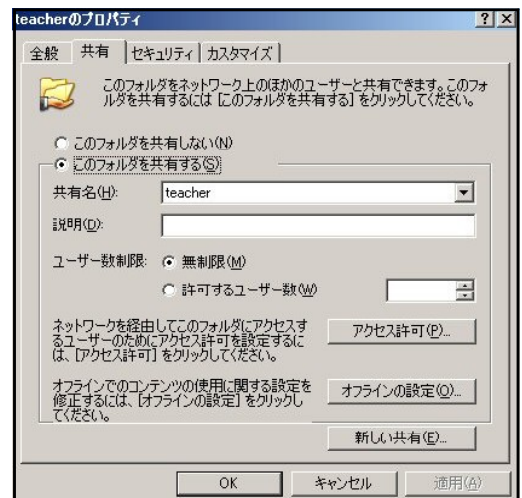
(サ) データドライブに「Netdrv」フォルダを作り、その配下に「teacher」と「student」の2つのフォルダを作成してください

#### (2) アクセス権の設定

①(サ) 「teacher」を右クリックして、表示されたメニューから「共有とセキュリティ」をクリックします。

②(サ) 「teacherのプロパティ」ダイアログが表示されるので、「共有」タブをクリックします。

③(サ) 右図のように、「このフォルダを共有にする」にチェックをいれると、右図のように、「共有名」にフォルダ名が自動入力されます。

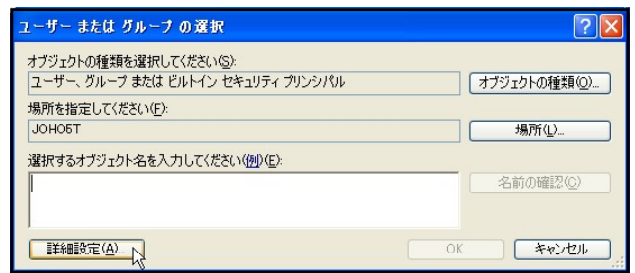


④(サ) 「アクセス許可」ボタンをクリックします。

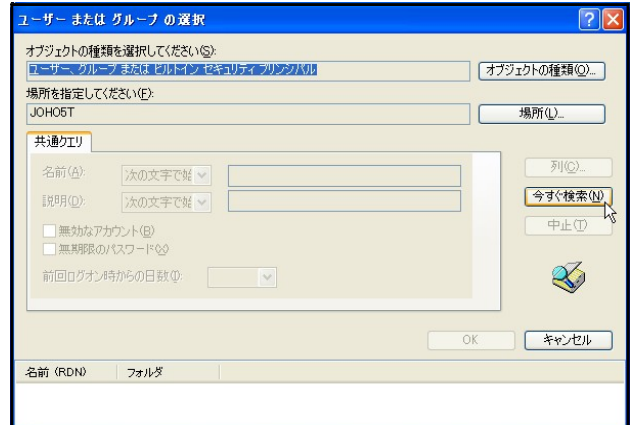
⑤(サ) 「teacherのアクセス許可」ダイアログが開くので、「追加」ボタンをクリックします。



- ⑥(サ)「ユーザーまたはグループの選択」ダイアログが表示されるので、「詳細設定」ボタンをクリックします。

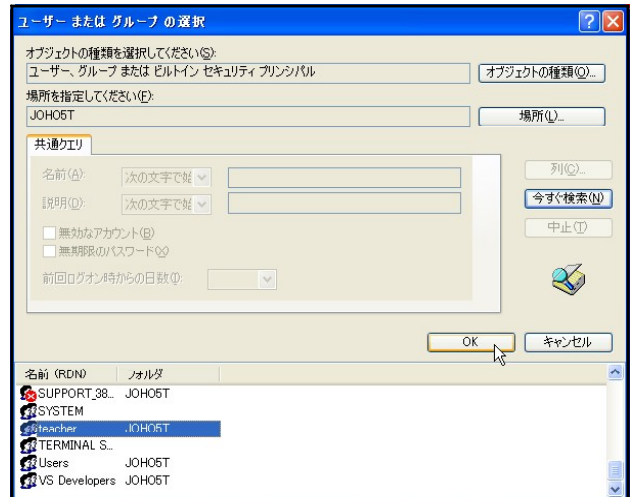


- ⑦(サ)右図の画面が表示されるので、「今すぐ検索」ボタンをクリックします。

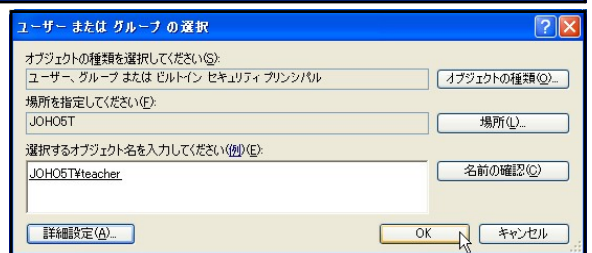


- ⑧(サ)教職員だけにアクセス許可を与えるので、下に表示された中から「teacher」グループをクリックし、「OK」ボタンをクリックします。

※教職員一人一人のユーザーを選択していてもいいのですが、その場合、人数が多い場合や転入出があった場合に作業がたいへんです。

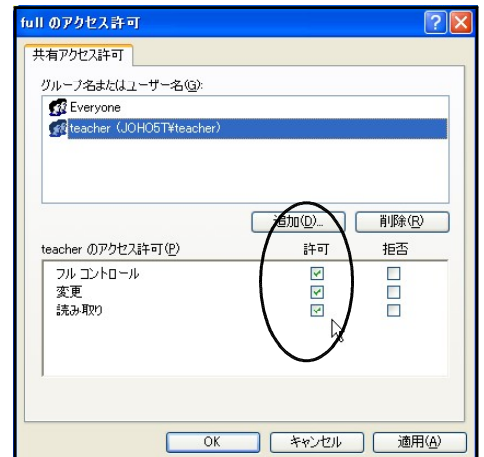


- ⑨(サ)右図のように表示されますので、「OK」ボタンをクリックします。



- ⑩(サ)右図の画面が表示されるので、共有アクセス許可に追加された「teacher」グループをクリックします。「teacher」グループ、つまり、教職員全てに読み書き可能なアクセス許可を与えたいので、「teacherのアクセス許可」欄の「フルコントロール」の「許可」にチェックを入れ、「適用」をクリックします。

※「読み取り」の「許可」にチェックを入れると、ファイルを上書き保存したり、編集したり、消去したりできなくなります。編集されたくないファイル、例えば、様式などを保存しておくフォルダは「読み取り」のみにします。





⑪(サ) unnecessary グループやユーザーを削除します。「グループ名またはユーザー名」の「Everyone」をクリックし、「削除」ボタンをクリックします。

⑫(サ) 「適用」をクリック後、「OK」ボタンをクリックします。

### —演習—

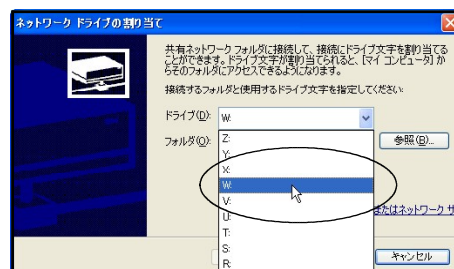
フォルダ「student」に、教職員と児童生徒がフルアクセスできるように設定しましょう。

### (3) 共有フォルダの利用

サーバーの「teacher」フォルダを各クライアントではZドライブとして利用できるようにします。

① (ク) 「コンピュータ」を開き、メニューバー「ツール」－「ネットワークドライブの割り当て」の順にクリックします。

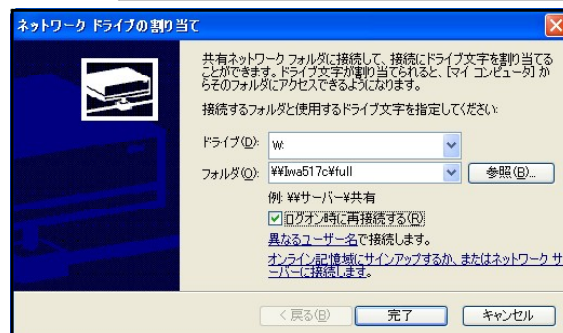
② (ク) 右図「ネットワークドライブの割り当て」ダイアログが開くので、Zドライブを選択して「参照」ボタンをクリックします。



④ (ク) 右図「フォルダの参照」ダイアログが開くので、自分のgrpをダブルクリック、各グループのサーバをダブルクリックして、「teacher」フォルダをクリックした後、「OK」ボタンをクリックします。



⑤(ク) 右図のような画面が表示されるので、「ログオン時に再接続する」にチェックを入れ、「完了」ボタンをクリックします。



⑥(ク) 「マイコンピュータ」を開くと、Wドライブが追加されています。

※このフォルダには、登録した教職員全ての人を読み書き自由な設定になっています。しかし、「teacher」グループに属さない、例えば児童生徒等はこのフォルダをみることはできても、フォルダにアクセスすることはできません。

### —演習—

フォルダ「student」をクライアントのYドライブに割り当ててください。

※この「student」フォルダには、教職員も児童生徒も読み書きできるようにしてください。

#### (4) セキュリティを高めるための方法

作成した共有フォルダのセキュリティを高める2つの方法を紹介します。一つは、アクセス権を細かく設定する方法です。もう一つは、クライアントがブラウジングしても表示されない隠しフォルダを作成する方法です。このことにより、フォルダ自体が見えなくなってしまうので、つまり、どんなフォルダがあるかさえ、クライアントからはわからなくなってしまうのです。

##### ア より細かなアクセス権の設定

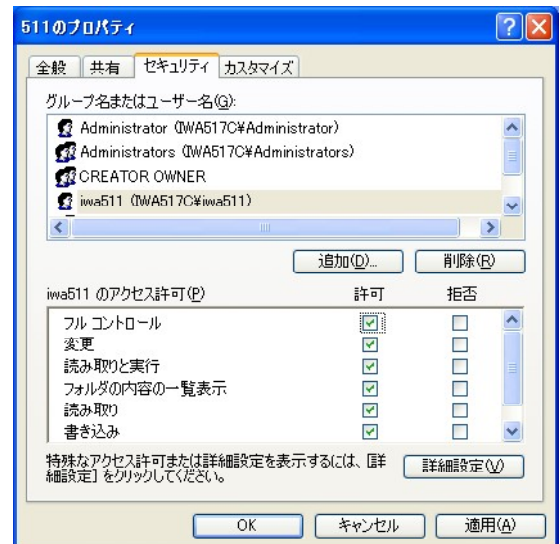
①(サ)「マイコンピュータ」を開き、設定したいフォルダで右クリックし、出てきたメニューの「共有とセキュリティ」をクリックします。

②(サ)表示された画面の「セキュリティ」タブをクリックします。

③(サ)「共有」タブをクリックしたときと同じ手順でユーザーまたはグループを設定します。

④(サ)設定したいユーザーまたはグループを選択し、アクセス許可を与えます。「共有」タブをクリックしたときに表示されるアクセス許可よりも細かな選択ができます。

⑤(サ)必要な許可を与えたら「適用」ボタンクリック後、「OK」ボタンをクリックします。

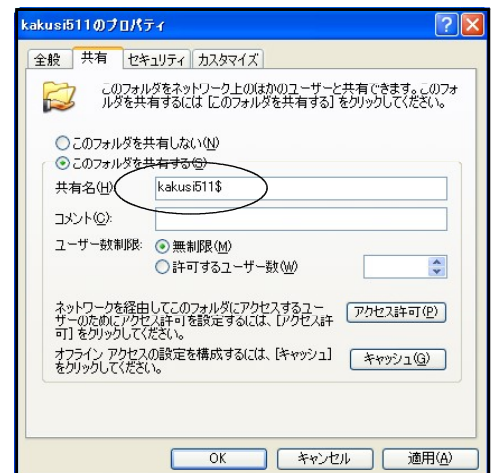


##### イ 隠しフォルダの作成

アクセス権があるユーザーだけがサーバーの共有フォルダを見えるようにします。具体的には、「teacher」フォルダ自体を児童生徒から見えなくする方法です。

①(サ)「teacher」フォルダを右クリックして、表示されたメニューから「共有とセキュリティ」をクリックします。

②(サ)「共有」タブをクリックし、「共有名」の末尾に半角で\$を入力します。(teacher\$)



③(ク) ネットワークドライブとして割り当てなおします。その際、「参照」ボタンをクリックしてもこのフォルダはブラウジングできません。「フォルダ」欄は手入力します。

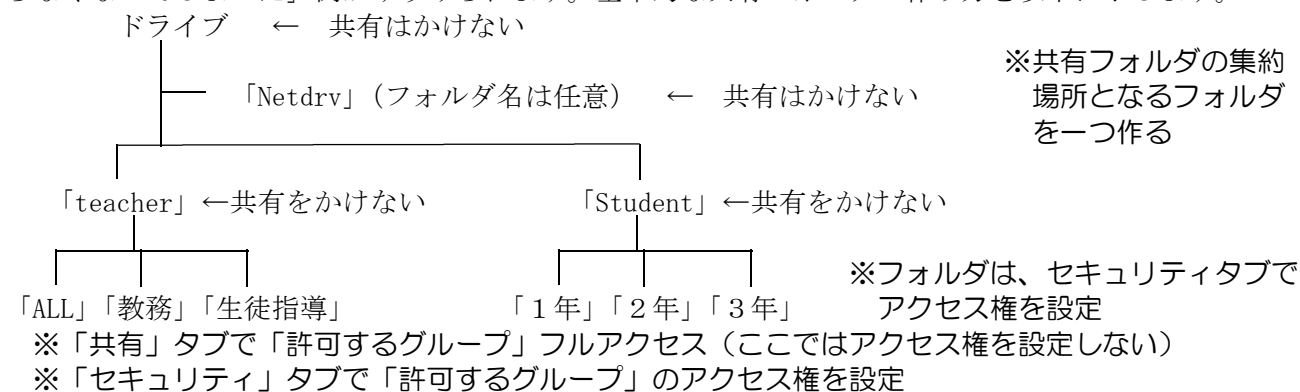
手入力する内容

「¥¥サーバーのコンピュータ名¥共有フォルダ名」

②(ク)ブラウジングしてもそのフォルダは見えませんが、きちんとネットワークドライブに割り当てられています。

## 共有フォルダの作り方

ファイル共有設定を行っているうちに、「フォルダやファイルが乱立し、制限やセキュリティもわからなくなってしまった」例がみうけられます。基本的な共有フォルダの作り方を以下に示します。



## 4 ネットワーク接続ストレージ (NAS) の利用

NAS (ナス) はNetwork Attached Storage (ネットワークアタッチドストレージ) の略で、急速に普及してきている周辺機器です。簡単に言うと、ネットワークに直接接続して使用するファイルサーバ専用機です。ハードディスクとNIC、OS、管理用ユーティリティなどを一体化した単機能サーバで、記憶装置をネットワークに直に接続したように (ブラウジングすると1台のコンピュータとして表示) 見えることからこのように呼ばれます。ネットワークに接続した他のコンピュータからは、通常のファイルサーバと同様に利用することができます。ファイルシステムやネットワーク通信機能は最初から内蔵されており、ファイルサーバ用のコンピュータを用意する必要もないことから、導入が容易で安価に済みます。新しくファイルサーバを導入しようとしている学校には最もお勧めしたい製品です。

### (1) ネットワーク対応外付けハードディスク

ハードディスクに付属するネットワークケーブルの他端をハブに接続するだけで、ファイルサーバになってしまう優れたものです。無線LAN対応も市販されていますので、校内のネットワークにあわせて選択できます。(本講座でも用意しています)



市販例) BUFFALO社「LinkStation」シリーズ 23,100円 (250GB) ~178,900円 (2TB)  
IOデータ社「LANDISK」シリーズ 25,300円 (250GB) ~168,200円 (2TB)

### (2) ネットワーク対応外付けUSBポート

最近はとても便利なUSBポートが市販されています。「USB-LANコンバーター」と呼ばれる製品で、コンバーターに付属するネットワークケーブルの他端をハブに接続するだけで、様々なUSB接続機器が共有できるようになる優れたものです。USB接続型ハードディスクやUSBメモリを接続すればファイルサーバ、プリンタを接続すればプリンタサーバになります。学校に既にある資産を有効に活用することができる製品です。(本講座でも用意してあります)



市販例) IOデータ社「USB-LANコンバーター」 15,800円

## MEMO



## 5 Macintosh向けのファイル共有

県内小中学校及び私立学校には、Macintoshを利用している先生がいらっしゃいます。従来、管理面やセキュリティ面で課題が残るという理由で、WindowsネットワークにMacintoshをクライアントとして接続させてもらえない例がみうけられました。しかし、セキュリティ面での問題はWindowsよりも少ないというのが事実です。実際には、管理者がMacintoshを接続するノウハウを持ちあわせていないために繋がってもらえなかったというのが実情です。特にも、ファイル共有のしくみがWindowsとMacintoshでは異なっています。Windowsでは、TCP/IPやNetBEUI上でファイル共有を実現しています。NetBEUI上ではSMB(Servier Message Block)を利用しており、TCP/IP上ではCIFS(Common Internet File System)を利用しています。一方、Macintoshでは、AppleTalk上でAppleShareを利用してファイル共有を実現しています。したがって、このままではファイルを相互に利用することはできません。

WindowsServer2003には、Macintoshに対してWindowsマシン同様にファイルサービスやプリントサービスを提供する機能があります。以下に解説しますので、学校での参考にしてください。

### (1) MacOSXの場合

MacOSXにはSMBクライアントとCIFSクライアントの機能が実装されています。したがって、クライアントとなるMacOSX側に、コンピュータ名、ユーザー名、パスワード、ドメイン名またはワークグループ名、IPアドレス、サブネットマスク、デフォルトゲートウェイアドレス、DNSサーバーアドレス、プロキシサーバー等、適切な設定を行うだけでWindowsネットワーク(ActiveDirectoryドメインネットワークでもワークグループネットワークでも)のクライアントとして動作します。本講座では、10.4.1(Tiger)の画面で解説します。

#### ア アカウムの設定

Windowsネットワークに接続するユーザの登録を行います。

- ①(ク)「アップルメニュー」－「システム環境設定」の順にダブルクリックします。すると、右図のように、「システム環境設定」ダイアログが開きます。この中にある「アカウント」アイコンをダブルクリックします。



- ②(ク)右図の「アカウント」ダイアログが開きます。ネットワークに接続するためのアカウントを新規に作成します。左下にある「+」マークをクリックします。次に、Windowsネットワークで割り当てられているユーザ名を「名前」欄と「ユーザ名」欄に入力します。また、パスワードを「パスワード」欄と「確認」欄に入力します。さらに、「ログインオプション」をクリックして、「自動ログイン」のチェックをはずします。(MacOSXでは、初期状態では自動ログインの設定になっており、そのままではネットワークに接続することはできません。右図では、ユーザー名を「iwa527」、パスワードを「pas527」として設定しています)設定が終わったら、左上の赤いボタン(閉じるボタン)をクリックします。



#### イ コンピュータ名の設定

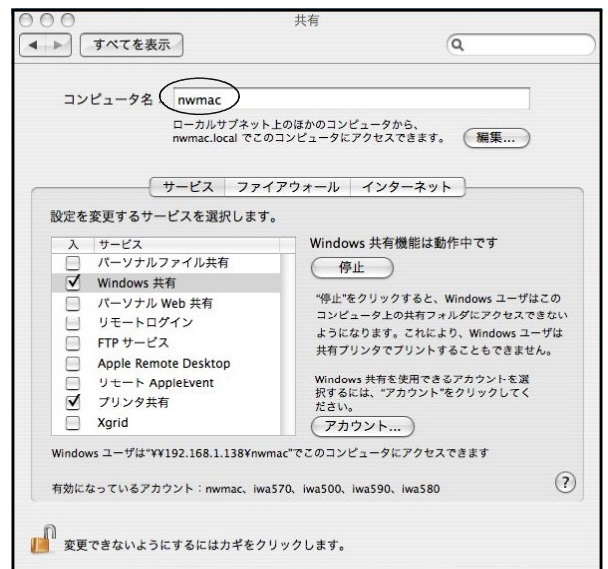
Windowsネットワークに接続するコンピュータ名の設定を行います。

- ①(ク)「アップルメニュー」－「システム環境設定」の順にダブルクリックします。すると、右図のように「システム環境設定」ダイアログが開きます。この中にある「共有」アイコンをクリックします。



②(ク)右図のように「共有」ダイアログが開くので、「コンピュータ名」欄にネットワーク上でブラウズしたときに表示されるコンピュータ名を入力します。この画面では、「nwmac」と入力しています。設定が終わったら、左上の赤いボタン（閉じるボタン）をクリックしてください。

（サービス欄にある「Windows共有」と「プリンタ共有」にチェックを入れると、WindowsマシンがこのMACマシンに接続できるようになり、Mac側のファイルやプリンタを共有することができます）



## ウ ワークグループ名 (ActiveDirectoryドメイン名) の設定

ネットワークで使用しているワークグループ名かActiveDirectoryドメイン名を入力します。Windowsネットワークをワークグループで構成している場合、MacOSXは、初期状態のワークグループ名が「空欄」または「WORKGROUP」になっているため、どんなにIPアドレスを設定してもそのままではつながりません。また、ActiveDirectoryでドメインネットワークを構成している場合、MacOSXは、初期状態のドメイン名が「空欄」または「WORKGROUP」になっているため、どんなにIPアドレスを設定してもそのままではつながりません。

①(ク)「MacintoshHD」を開き、「アプリケーション」アイコンをダブルクリックします。



②(ク)続けて、「ユーティリティ」アイコンをダブルクリックします。



③(ク)さらに「ディレクトリアクセス」アイコンをダブルクリックします。



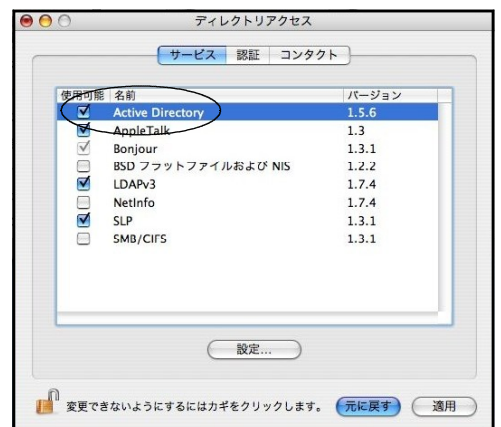
- ④(ク)「ディレクトリアクセス」ダイアログが開きます。ワークグループに接続するときには「SMB/CIFS」にチェックを入れ、「設定」ボタンをクリックします(パスワードの入力画面が表示されたときには、Macの管理者用パスワードを入力します)  
ドメインに接続する時には、⑥に進んでください



- ⑤(ク)右図の画面が表示されるので、「ワークグループ」欄に、接続したいWindowsネットワークのワークグループ名を入力します。(右図では「server」と入力しています。「WINSサーバ」欄にはWINSサーバーをたてているときだけWINSサーバーのIPアドレス、またはコンピュータ名を入力します。)  
設定が終わったら、「OK」ボタンをクリックし、「適用」ボタンをクリックの後、左上の赤いボタン(閉じるボタン)をクリックします。



- ⑥(ク)ActiveDirectoryによるドメインネットワークに接続するときには、右図のように「ActiveDirectory」にチェックを入れ、「設定」ボタンをクリックします(パスワードの入力画面が表示されたときには、Macの管理者用パスワードを入力します)



- ⑦(ク)右図の画面で、「ActiveDirectoryのドメイン」欄に、接続したいドメイン名を入力します。(右図では「grp4.local」と入力しています)  
設定が終わったら、「OK」ボタンをクリックし、「適用」ボタンをクリックの後、左上の赤いボタン(閉じるボタン)をクリックします。



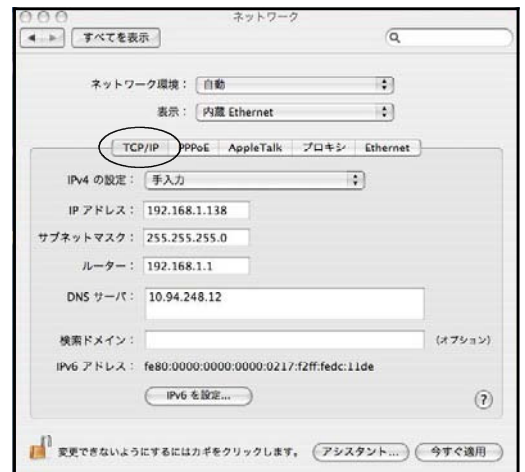
## エ IPアドレスとプロキシサーバの設定

- ①(ク)「アップルメニュー」－「システム環境設定」の順にダブルクリックします。すると、右図の「システム環境設定」ダイアログが開きます。この中にある「ネットワーク」アイコンをダブルクリックします。





②(ク)右図のダイアログが開くので、「TCP/IP」ボタンをクリックします。固定したIPアドレスにするため、「IPv4を設定」欄は、三角スピンをクリックして「手入力」を選択します。「IPアドレス」欄、「サブネットマスク」欄、「ルータ」欄、「DNSサーバ」欄に必要な事項を手入力します。ここでいうルータとは、Windowsでのデフォルトゲートウェイのことです。ネットワークがドメイン管理されているときには、「検索ドメイン」欄にドメイン名を入力します。



③(ク)次に、プロキシサーバを設定します。インターネットに接続するために必要な設定です。「プロキシ」ボタンをクリックすると右図の画面になります。「Webプロキシ(HTTP)」にチェックを入れ、右側にある「Webプロキシサーバ」欄にプロキシサーバの名前かIPアドレスを入力します。併せて、ポート番号も入力します。設定が終わったら、「今すぐ適用」ボタンをクリックの後、左上の赤いボタン（閉じるボタン）をクリックします。



## オ Windowsネットワークへの接続確認（ブラウジング）

①(ク)右図のように「ファインダ (Finder)」 - 「移動」 - 「サーバへ接続」の順にクリックします。



②(ク)右図のように「サーバへ接続」ダイアログが開くので、「ブラウザ」ボタンをクリックします。



③(ク)ネットワークにうまく接続できていると、右図のように、同一セグメントにあるネットワークがフォルダのようなアイコンで表示されます。接続したいネットワークのアイコンをダブルクリックします



④(ク)ネットワークに接続しているコンピュータが表示されます。

## カ フォルダの共有

Windowsマシンにある共有フォルダにアクセスします。ここでは、ファイルサーバ「iwa500c」にある「full」という共有フォルダにアクセスすることとして解説します。

①(ク) 前述したオ④で見えているコンピュータアイコンをダブルクリックすると、右図のような認証画面が表示されます。「ワークグループ/ドメイン」欄に表示されているワークグループ名またはドメイン名を確認して、正しいときにはそのままにしておき、間違っているときには正しいワークグループ名またはドメイン名を入力します。「ユーザ名」欄にユーザ名を入力し、さらに「パスワード」欄にパスワードを入力して「OK」ボタンをクリックします。



②(ク)すると、右図のように「SMB/CIFSマウント」の画面が表示されます。三角スピンをクリックして、共有フォルダを選び、「OK」ボタンをクリックします。ここでは、共有フォルダである「full」を選択しています。



③(ク)すると、デスクトップ上にファイルサーバの共有フォルダである「full」がデスクトップにマウントされます。右図は、マウントされた共有フォルダをダブルクリックして開いたようすです。



## (2) Mac OS9の場合

Mac OS Xでは、Windowsネットワークに接続できる機能を持っていたのでWindows Server 2003側で設定しなくてもクライアントとして接続できたのですが、Mac OS 9やMac OS 8にはAppleTalkの通信機能しかないので、Windows Server 2003側で必要なサービスを提供する必要があります。Windows Server 2003には、Mac OS 9やMac OS 8をクライアントにするためのAppleTalkプロトコルとAppleShareサーバー機能が用意されています。そこで、Macをクライアントにするために、Windows Server 2003に「AppleTalkプロトコル」「Macintosh用ファイルサービス」「Macintosh用印刷サービス」の3つのコンポーネントを追加し、これらのサービスを提供できるようにします。

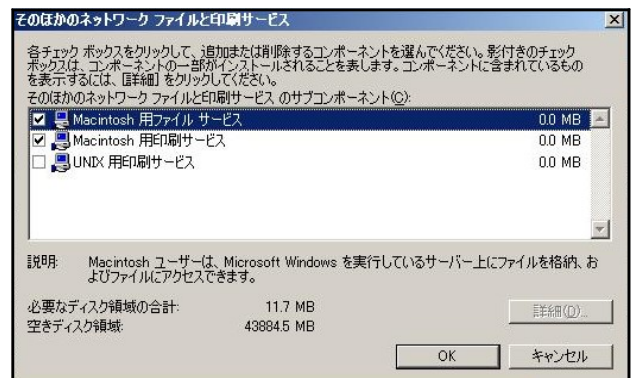
### ア コンポーネントのインストール

①(サ) 「AppleTalkプロトコル」「Macintosh用ファイルサービス」「Macintosh用印刷サービス」の3つのコンポーネントは、「プログラムの追加と削除」からインストールする必要があります。そこで、「コントロールパネル」→「プログラムの追加と削除」→「Windowsコンポーネントの追加と削除」の順にクリックします。

②(サ) 右図のダイアログが開くので、「そのほかのネットワークファイルと印刷サービス」にチェックを入れ、「詳細」ボタンをクリックします。



③(サ)右図のダイアログが開くので、「Macintosh用ファイルサービス」と「Macintosh用印刷サービス」の2つにチェックを入れ、「OK」ボタンをクリックします。



④(サ)「Windowsコンポーネントウィザード」ダイアログに戻るので、「次へ」ボタンをクリックします。

⑤(サ)完了画面が表示されるので、「完了」ボタンをクリックします。これで、3つのコンポーネントのインストールは完了です。

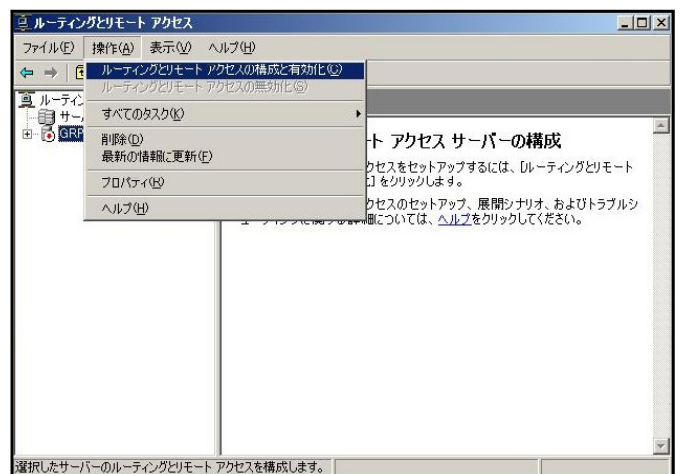
## イ AppleTalkネットワークの設定

### (7) ルーティングの設定

AppleTalkとWindowsネットワークのルーティングをします。ルーティングとは、ネットワークの境界で最適な経路を選択記憶し、外部からのパケットを自分のネットワークにあるホスト（コンピュータ）へ転送したり、自分のネットワークからのパケットを別のネットワークへ転送したりすることをいいます。WindowsServer2003に、WindowsネットワークとAppleTalkネットワークを同時に二つつくることになるのですが、それぞれのネットワークが別々ではファイル共有はできないので、WindowsServer2003自身に繋ぎ合わせる役目を持たせるわけです。

①(サ)「スタート」－「管理ツール」－「ルーティングとリモートアクセス」の順にクリックします。

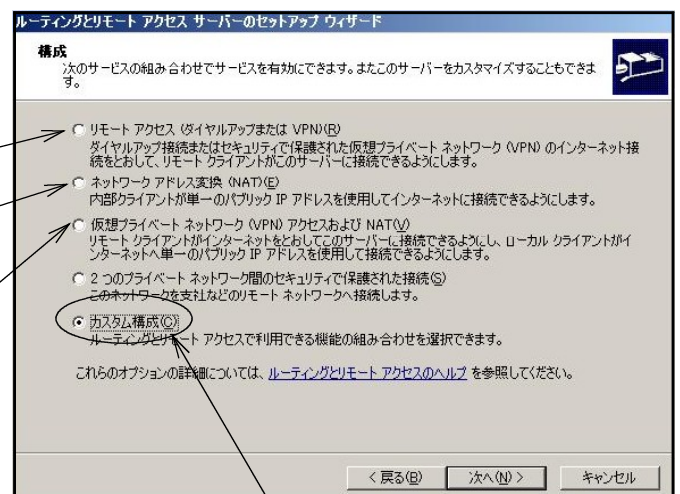
②(サ)右図の画面が開くので、サーバー名（右図の画面では「GRP4SV」）を選択します。



③(サ)メニューバー「操作」－「ルーティングとリモートアクセスの構成と有効化」の順にクリックします。ここを選択することで「RRAS(Routing and Remote Access Service)管理ツール」のインストールがはじまります。

③(サ)「ルーティングとリモート アクセスサーバーのセットアップウィザードの開始」ダイアログが表示されるので、「次へ」ボタンをクリックします。

④(サ)右図の画面が表示されるので、「カスタム構成」にチェックを入れ、「次へ」ボタンをクリックします。



VPNからのリモートアクセス

NAT(正確にはIPマスカレード)

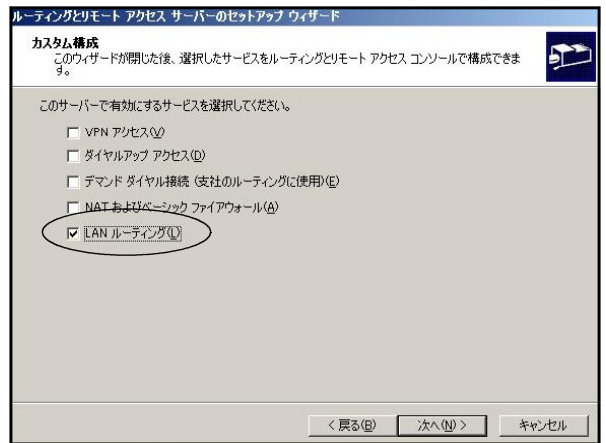
リモートアクセス及びNAT  
(前述した2つのことをできるようにする)

ルーティング

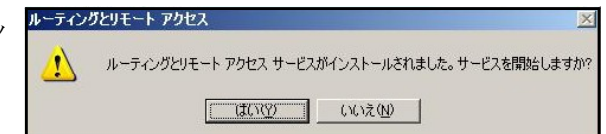
(正確にはNATつまり2つの異なるネットワークを接続する)



⑤(サ)右図の画面が表示されるので、「LANルーティング」にチェックを入れ、「次へ」ボタンをクリックします。

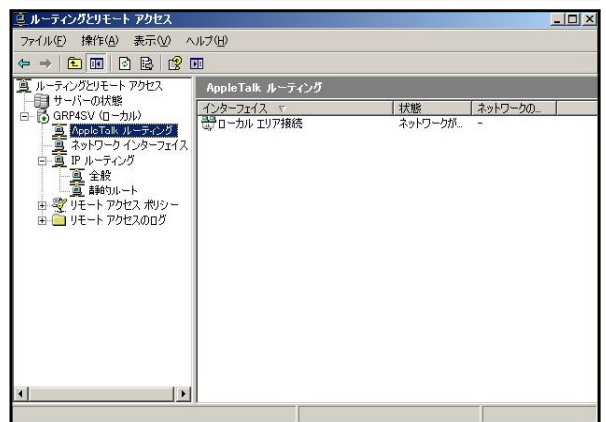


⑥(サ)セットアップウィザード完了の画面が表示されるので「完了」ボタンをクリックします。

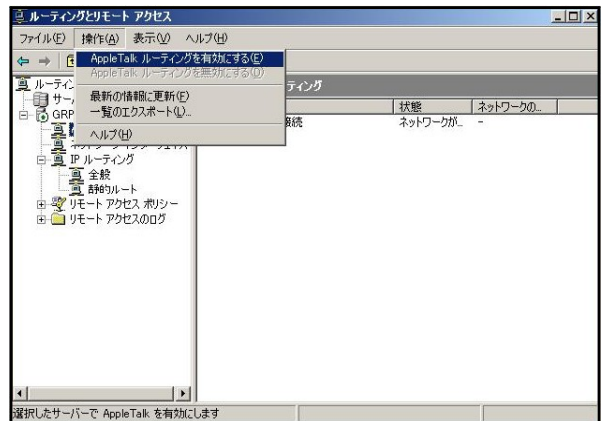


⑦(サ)右図の画面が表示されるので、「はい」をクリックします。

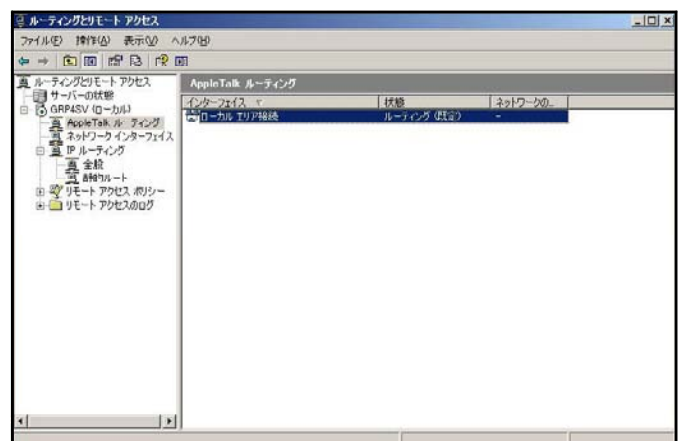
⑧(サ)「ルーティングとリモートアクセス」ダイアログに戻りますので、左側ツリー画面に「AppleTalkルーティング」が追加されていることを確認します。(追加されていない場合は、インストールは失敗しています。そのときには、再起動後もう一度①から操作をやり直します。)



⑨(サ)⑧で追加された「AppleTalkルーティング」をクリックしたうえで、メニューバー「操作」→「AppleTalkルーティングを有効にする」の順にクリックします。



⑩(サ)しばらくすると、右図のように、右側のインターフェース欄にある「ローカルエリア接続」の状態が「ルーティング (既定)」に設定されます(「ローカルエリア接続」という名称はネットワーク接続設定の名前が使われています。設定されているネットワークにより表示される名称は異なります。)。これでWindowsネットワーク側とAppleTalkネットワークのルーティングの設定が完了しました。

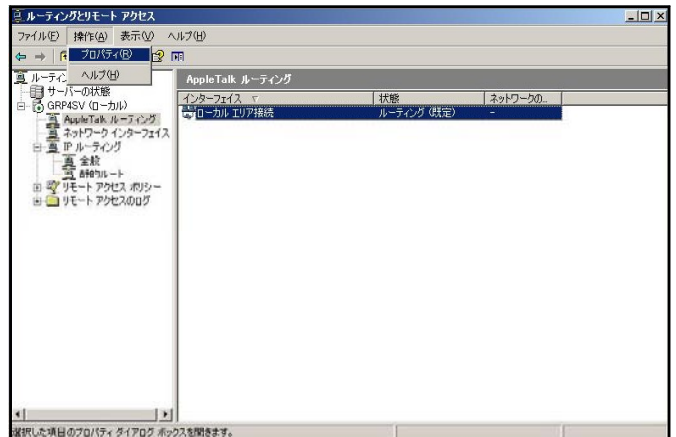




#### (イ) AppleTalkゾーンとAppleTalkネットワークアドレスの設定

Macintoshを新たに接続するには、AppleTalkゾーンとネットワークアドレスを用意する必要があります。AppleTalkネットワークの「ゾーン」は、Windowsネットワークの「ワークグループ」のようなものと考えてください。また、AppleTalkネットワークアドレスは、TCP/IPネットワークのIPアドレスのようなものと考えてください。ここでは、WindowsServer2003でAppleTalkゾーンとAppleTalkネットワークアドレスの作成方法を解説します。

①(サ)まず、AppleTalkネットワークアドレスを作成します。「ルーティングとリモートアクセス」ダイアログで左側「AppleTalkルーティング」を選択、右側でインターフェイス欄にある「ローカルエリア接続 (名称は任意)」を選択します。



②(サ)右図のようにメニューバー「操作」－「プロパティ」の順にクリックします。

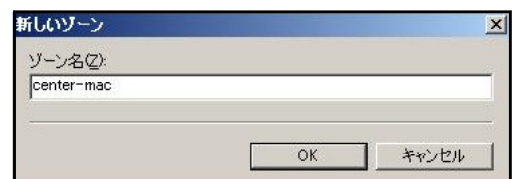
③(サ)右図の画面が開くので、「このネットワークでシードルーティングを有効にする」にチェックを入れます。



④(サ)「ネットワークの範囲」の「開始」アドレスを「1」、「終了」アドレスを256と入力します。AppleTalkネットワークのアドレス範囲で指定できる値は、1～65279間の整数で他のAppleTalkゾーンで使用されているネットワークアドレスと重複しなければOKです。ここでは、とりあえず256台分（実質24台分）設定しています。

⑤(サ)次に、AppleTalkゾーンを作成します。Windowsネットワークで言うところのワークグループ名を設定することとほぼ同義です。「ゾーン」欄にある「新規」ボタンをクリックします。

⑥(サ)右図のダイアログが開くので、「ゾーン名」欄に任意の名前（半角英数字にすること）を入力します。ここでは、「center-mac」と入力しています。「OK」ボタンをクリックします。



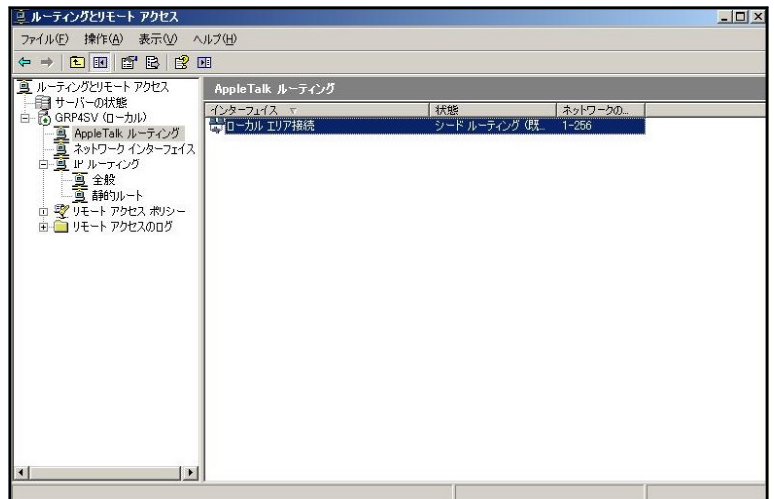
⑦(サ)右図のように、「利用可能なゾーン」に⑥で入力したゾーン名が追加されているはずですが。



⑧(サ)右図の「ゾーン」欄にある「既定のゾーン」に新規に作成したゾーン名（ここでは「center-mac」）が表示されていることを確認してください。もし、表示されていなければ、「規定値に設定」ボタンをクリックしてください。

⑨(サ)「適用」ボタン－「OK」ボタンの順にクリックします。

- ⑩(サ) 設定完了していると、右図のように「状態」のところに「シードルーティング」、「ネットワーク」のところに指定したネットワークアドレスが表示されています。もし、表示されていない場合には、途中の操作を誤っていますので再度設定し直します。



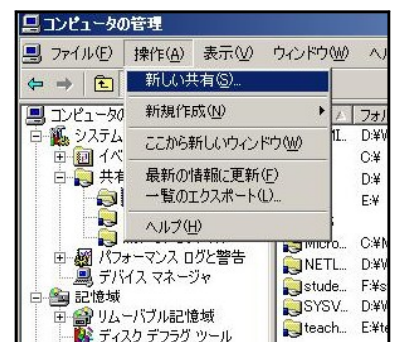
#### (ウ) Macintosh用共有フォルダの指定

Macintosh用に共有フォルダ（Macintoshからみた場合には共有ボリュームという）を設定する際に留意することがあります。それは、①NTFSフォーマットであること、②フォルダのプロパティ画面ではなく、「コンピュータの管理」画面で設定することです。したがって、共有したフォルダのあるドライブがFATフォーマットやFAT32フォーマットの場合にはMacintoshに対して公開することができません。また、Windows共有の時のように、フォルダを右クリックしてそのプロパティから共有を設定しただけではMacintosh側に公開したことにはならないのです。

以下に解説するのは、Macintosh用共有フォルダ（共有ボリューム）の設定手順です。この操作によって、WindowsとMacintoshの両方からアクセスできるようになり、ファイルの共有が可能になります。

- ①(サ) スタートボタン－「管理ツール」－「コンピュータの管理」の順にクリックします。

- ②(サ) 「コンピュータの管理」ダイアログが開くので、左側ツリーにある「共有」を選択した後、右図のように、メニューバー「操作」－「新しい共有」をクリックします。



- ③(サ) 「フォルダの共有ウィザードの開始」画面が表示されるので、「次へ」ボタンをクリックします。

- ④(サ) 右図の画面が表示されるので、共有させたいフォルダの場所を手入力するか、「参照」ボタンをクリックして該当するフォルダを選択します。

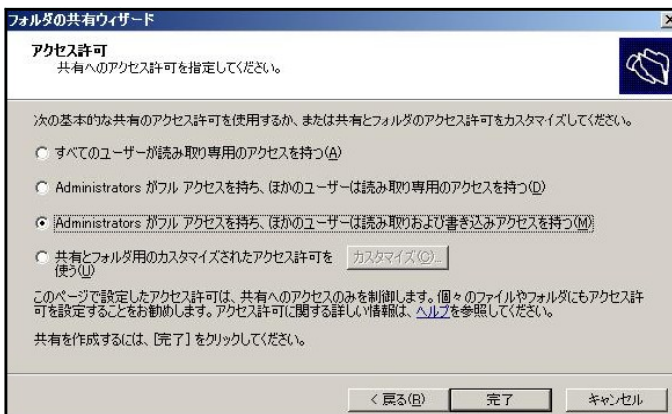


- ⑤(サ) 「次へ」ボタンをクリックします。

⑥(サ) 右図で、WindowsとMacintoshの両方のユーザーに対する共有設定を行います。「Microsoft Windowsユーザー」にチェックを入れ、「共有名」をキーボードから手入力します。さらに、「Apple Macintoshユーザー」にもチェックを入れ、共有名をキーボードから手入力します。両方のユーザーにチェックを入れることで、両方のユーザーに共有させることができます。共有名はわかりやすいように同じ名前にします。「次へ」ボタンをクリックします。

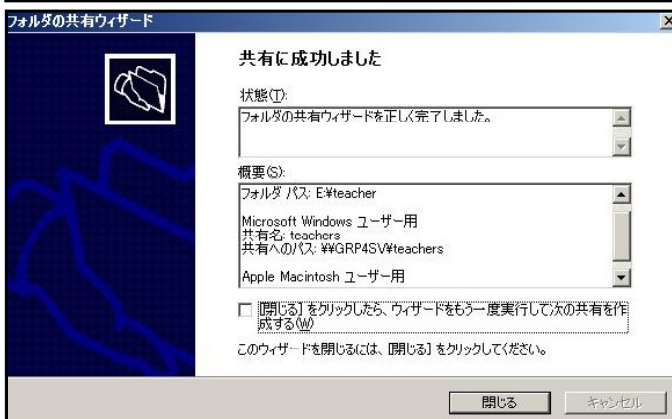


⑦(サ) 右図画面が開くので、「Administratorがフルアクセスを持ち、他のユーザーは読み取りおよび書き込みアクセスを持つ」にチェックを入れ、「完了」ボタンをクリックします。**細かなアクセス権は、OSごとに設定するのではなく、フォルダのプロパティにあるセキュリティタブでユーザー毎に設定します。**



⑧(サ) 右図の画面が表示されるので、「閉じる」ボタンをクリックします。

これで、設定は完了です。



## MEMO

## 6 ルーターの設置

別々のネットワークを相互に接続する場合に用いる機器がルーターです。ここでは、ネットワークにルーターを繋いで、別のネットワークに接続する方法を研修します。



ルーターを用いると、インターネットに接続できるIPアドレスが学校に一つしかなくても、NAT/IPマスカレード機能を用いて、全台のコンピュータが接続できるようになることから、県内の学校では、校内ネットワークの出口にルーターが設置されています（トップルータと呼ぶことが多い）。

校内ネットワークを県や市町村のネットワーク、民間のプロバイダ等のWAN（広域通信網）に接続することを想定して研修します。

### (1) ルーターの接続

- ① スwitchingハブのカスケードポートとルーターのLAN側ポートをネットワークケーブルで接続します。
- ② ルーターのWAN側ポートに外部からきているネットワークケーブルを接続します。

### (2) ルーターの設定

本講座ではBUFFALO社有線ブロードバンドルーター「BBR-4MG」、または、BUFFALO社無線LANブロードバンドルーター「WHR-HP-AMPG」、または、corega社有線ブロードバンドルーター「BAR SD」のうち、どれか一つを用いますが、各自でマニュアルを見ながら設定していくこととします。

このルーターの設定で、特に大切なことを以下に示しておきます。

#### ア LAN側のIPアドレスを設定すること

ルーターのLAN側IPアドレスはLAN内のコンピュータの「デフォルトゲートウェイ」になります。したがって、ルーター用にIPアドレスを一つ確保します。

#### イ WAN側の各種アドレスを設定すること

学校が県もしくは市町村のネットワークに接続しているのであれば、県もしくは市町村から与えられているIPアドレス、サブネットマスク、デフォルトゲートウェイ、DNSサーバーを設定します。民間プロバイダを利用しているのであれば、民間プロバイダからもらったアドレスを設定します。

#### ウ NAT/IPマスカレード機能を有効にすること

このことにより、インターネットに接続できるIPアドレスが学校に一つしかなくても、全台のコンピュータがインターネットに接続できるようになります。

#### 本講座で用いるルーターの各種アドレス及び設定

<grp1>	LAN側IPアドレス	192.168.1.1	WAN側IPアドレス	10.94.250.31
<grp2>	LAN側IPアドレス	192.168.2.1	WAN側IPアドレス	10.94.250.32
<grp3>	LAN側IPアドレス	192.168.3.1	WAN側IPアドレス	10.94.250.33
<grp4>	LAN側IPアドレス	192.168.4.1	WAN側IPアドレス	10.94.250.34
<grp5>	LAN側IPアドレス	192.168.5.1	WAN側IPアドレス	10.94.250.35
<grp6>	LAN側IPアドレス	192.168.6.1	WAN側IPアドレス	10.94.250.36
<grp7>	LAN側IPアドレス	192.168.7.1	WAN側IPアドレス	10.94.250.37
<grp8>	LAN側IPアドレス	192.168.8.1	WAN側IPアドレス	10.94.250.38
<grp9>	LAN側IPアドレス	192.168.9.1	WAN側IPアドレス	10.94.250.39
<grp10>	LAN側IPアドレス	192.168.10.1	WAN側IPアドレス	10.94.250.40
	WAN側サブネットマスク<共通>		255.255.255.192	
	WAN側デフォルトゲートウェイ<共通>		10.94.250.62	
	WAN側DNSサーバー<共通>		10.94.248.12	

※NAT機能を必ず有効にすること      ※DHCPサーバー機能を無効にすること

※ルーターのシステムを更新（または再起動）すること

### (3) クライアントコンピュータのデフォルトゲートウェイ設定

各クライアントコンピュータに「デフォルトゲートウェイ」のアドレスを設定してください。デフォルトゲートウェイのアドレスは、ルーターのLAN側アドレスです。



## B ActiveDirectoryドメインの構築

ここからはActiveDirectoryドメインによるネットワークを構築していきます。ドメインネットワークを構築するためには、最初にドメインコントローラを設置する必要があります。今まで用いてきたサーバーをドメインコントローラにしましょう。

### 1 ドメインコントローラ (ActiveDirectory) のインストール

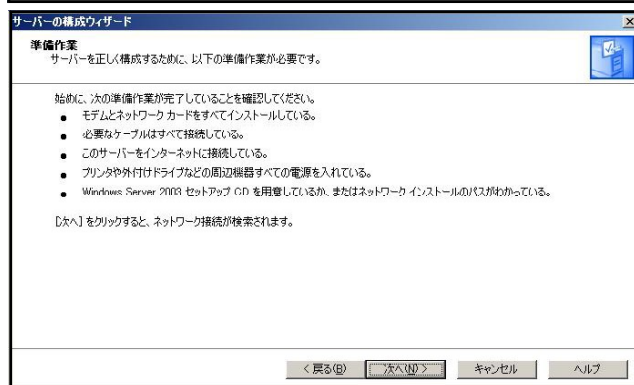
ドメインコントローラをインストールすることにより、ActiveDirectoryもインストールされます。

- ①(サ)「スタート」ボタン→「管理ツール」→「サーバーの構成ウィザード」の順にクリックします。Windows Server 2003でサービスをインストールするときには、この「サーバーの構成ウィザード」を使うと便利なので覚えておきましょう。(サービスのインストールの方法は、「サーバーの構成ウィザード」を使う以外にも、他のWindowsと同じように、「コントロールパネル」→「プログラムの追加と削除」→「Windows コンポーネントの追加と削除」→「ネットワークサービス」でも行うことができます)

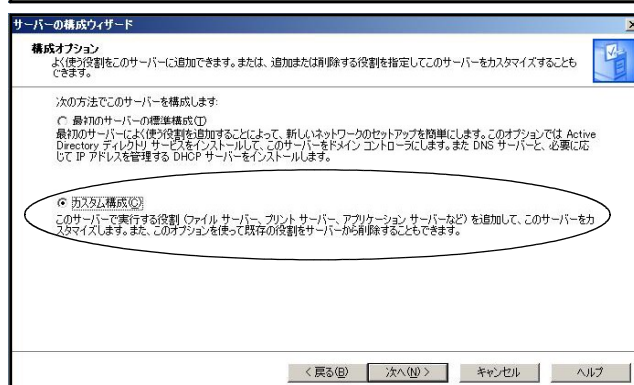
- ②(サ)右図の「サーバーの構成ウィザード」ダイアログが表示されますので、「次へ」ボタンをクリックします。



- ③(サ)右図の画面が表示されるので、そのまま「次へ」ボタンをクリックします。

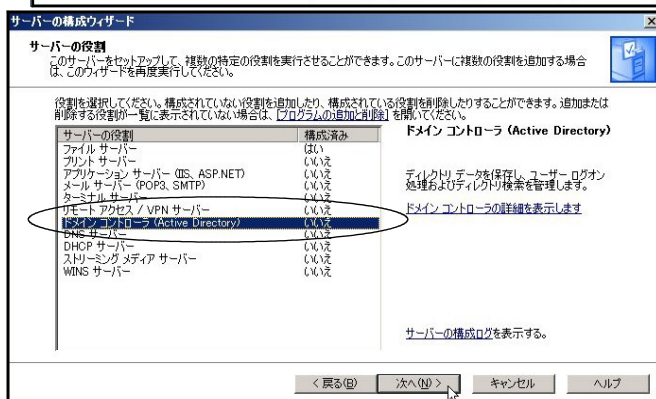


- ④(サ)右図の画面が表示されるので、「カスタム構成」を選択します。「最初のサーバーの標準構成」は絶対に選択しないでください。初級者向けをうたったメニューですが、自由がきかないのです。



- ⑤(サ)「次へ」ボタンをクリックします。

- ⑥(サ)右図の画面が表示されるので、「ドメインコントローラ (ActiveDirectory)」を選択し、「次へ」ボタンをクリックします。



⑦(サ)右図の画面が表示されるので、そのまま「次へ」ボタンをクリックします。



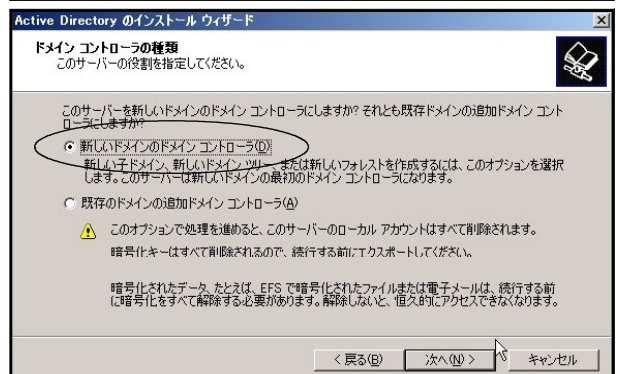
⑧(サ)右図の画面が表示されるので、そのまま「次へ」ボタンをクリックします。



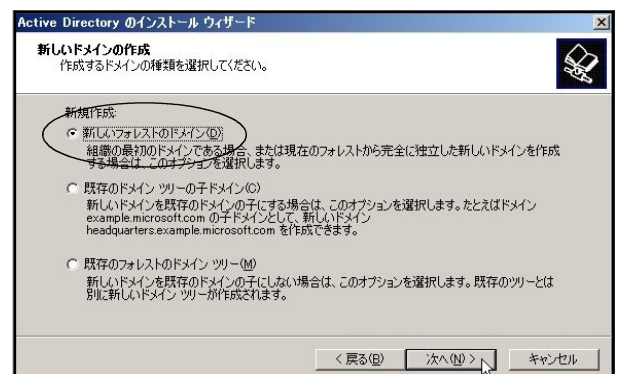
⑨(サ)右図の画面が表示されるので、そのまま「次へ」ボタンをクリックします。



⑩(サ)右図の画面が表示されるので、「新しいドメインのドメインコントローラ」を選択し、「次へ」ボタンをクリックします。

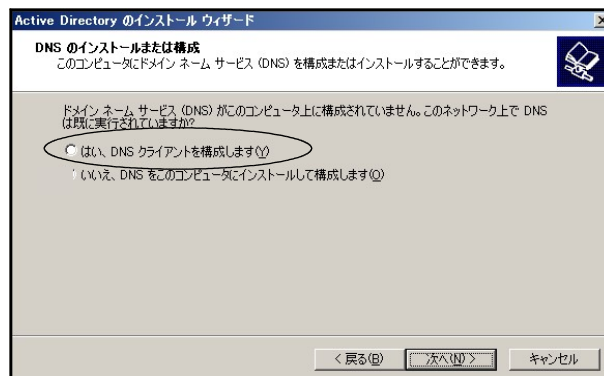


⑪(サ)右図の画面が表示されるので、「新しいフォレストのドメイン」を選択し、「次へ」ボタンをクリックします。





- ⑫(サ)もし、右図のような画面が表示されたら、「はい、DNSクライアントを構成します」のチェックを外し、「次へ」ボタンをクリックします。右図が表示されない場合には、⑬に進んでください。



ActiveDirectoryのドメインコントローラを動かすためにはDNSサービスが必要なので、ここでインストールしてもよいのですが、インストールすると、それぞれのはたらきが見えにくくなってしまうために、本講座では、あえて別々にインストールします。

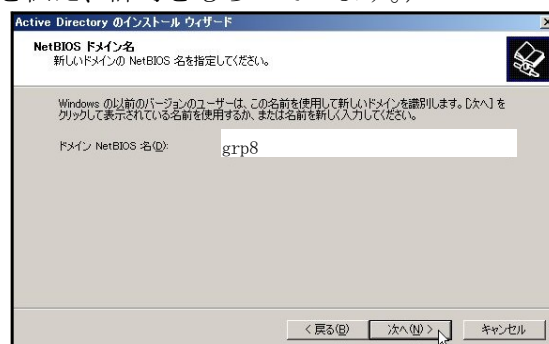
- ⑬(サ)右図の画面が表示されるので、「新しいドメインの完全なDNS名」に「grp○.local」と入力し「次へ」ボタンをクリックします。(○の部分には、各grpの数字を入れることとします)



ドメイン名は、ルールにしたがって名前を付けることが大切です。例えば、プロバイダもしくは市町村から「ginga.hanamaki.iwate.jp」のような「ginga」というサブドメイン名（この場合、「hanamaki.iwate.jp」がドメイン名）をもらっていればその名前を入力します。このような場合にはすでにドメインコントローラとDNSサーバーが構築されている可能性が大きいので（学校になくても市町村やプロバイダにある）、勝手なドメイン名を用いると大きなネットワークトラブルがおき、セキュリティを脅かし、大変な結果を招きます。

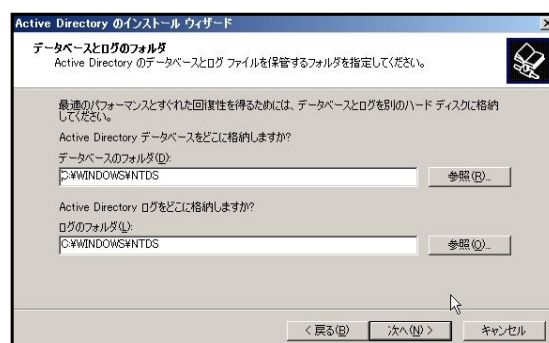
どんな名前をつけたらよいかわからない場合には、付けた名前の後に「.local」と入力します。このことにより、上位ネットワークの管理者は、ローカルでドメインを作ったことが一目瞭然となります。あなたが学校のネットワーク管理者なら、自分が管理する範囲内にとどめておくことが大切です。あなたが学校のネットワーク管理者でないならば、学校にドメインを構築することはもってのほかということになりますので、必ず、学校のネットワーク管理者に相談することです。（学校のネットワーク管理者は、教員とは限りません。市町村で行っていたり、民間に委託されていたりと様々です。必ず、確認することが、ネットワークセキュリティ上重要です。ちなみに、本講座においては教育センターのネットワーク管理者に「grp1.local」～「grp10.local」までの10ドメインを構築することを伝え、許可をもらっています。）

- ⑭(サ)右図の画面が表示され、「grp○」というように先ほど入力した「.local」の文字がない状態が表示されるので、そのまま「次へ」ボタンをクリックします。

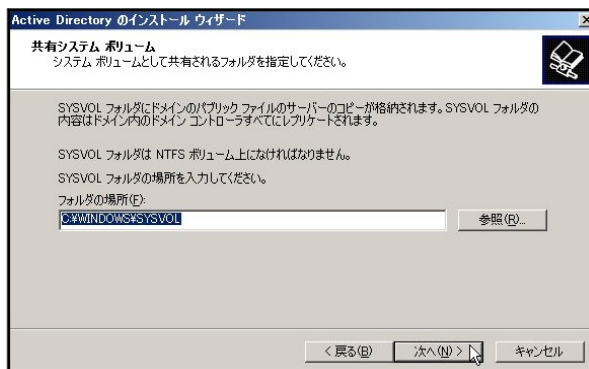


WindowsServer2003以前のWindowsは、この「NetBIOS」をつかってドメインにログオンすることになります。（この名前を変えると、後々わかりにくくなるので、このまますすめた方が無難です）

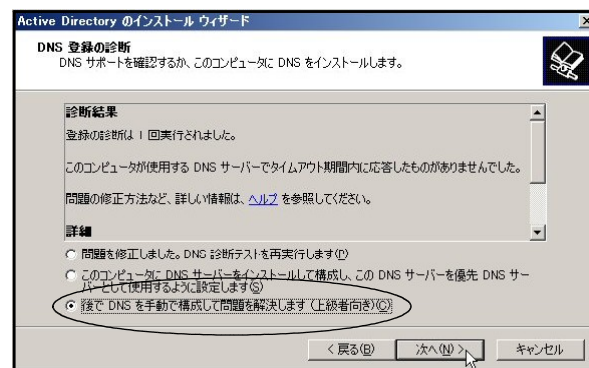
- ⑮(サ)右図の画面が表示されるので、そのまま「次へ」ボタンをクリックします。



- ⑩(サ)右図の画面が表示されるので、そのまま「次へ」ボタンをクリックします。

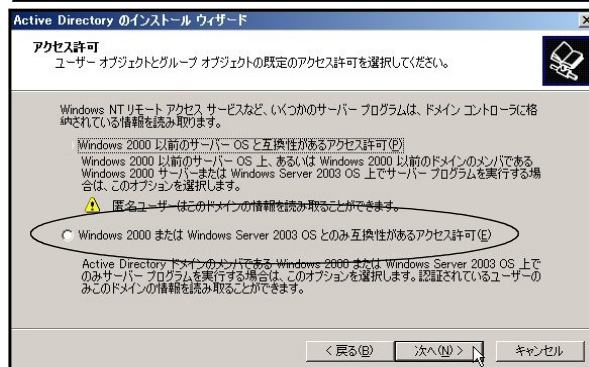


- ⑪(サ)右図の画面が表示されたら、「後でDNSを手動で構成して問題を解決します」を選択し、「次へ」ボタンをクリックします。右図が表示されない場合には、⑫に進んでください。



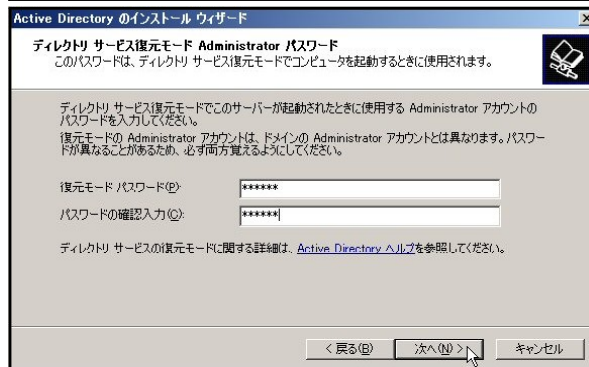
ActiveDirectoryのドメインコントローラを動かすためにはDNSサービスが必要なもので、ここでインストールしてもよいのですが、インストールすると、それぞれのはたらきが見えにくくなってしまったために、本講座では、あえて別々にインストールすることとします。

- ⑬(サ)右図の画面が表示されるので、「Windows2000またはWindowsServer2003とのみ互換性があるアクセス許可」を選択し、「次へ」ボタンをクリックします。

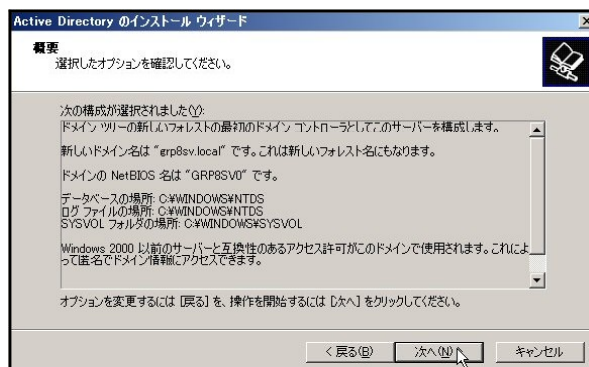


本講座では、WindowsServer2003のみ用いるのでこちらを選択しています。学校で別サーバーとしてNT4.0Serverを構築するときは、他方を選択します。クライアントが用いるOSではないので勘違いしないように注意してください。

- ⑭(サ)右図の画面で、「復元モードパスワード」と「パスワードの確認入力」に「Grp0sv」と入力し、「次へ」ボタンをクリックします。(○の部分には、各grpの数字を入れることとします。また、今回は、わかりやすいようにコンピュータ名をそのままパスワードとして使うこととします。)



- ⑮(サ)右図の画面が表示されるので、そのまま「次へ」ボタンをクリックします。画面が切り替わりますが、数分～数十分間設定にかかります(予想以上に時間がかかります。「キャンセル」ボタンを押すことのないようにじっと我慢してください。)



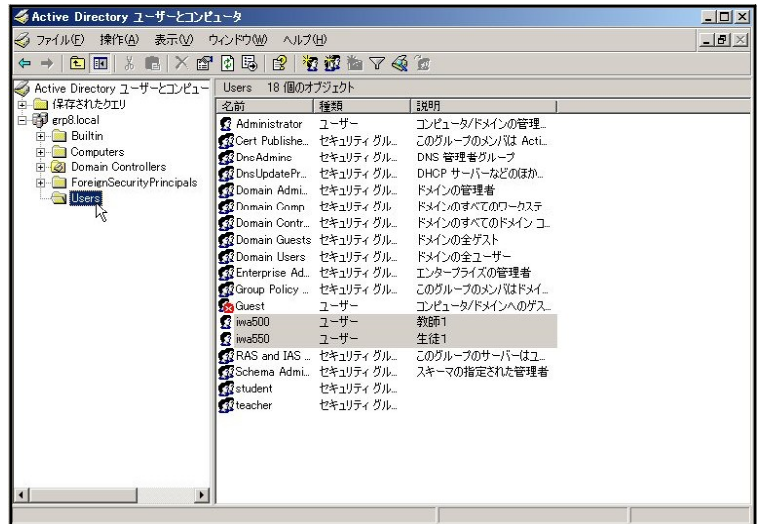
しばらくすると、ウィザード完了画面になりますから、「完了」ボタンをクリックしてインストールは終了です。

## 2 ドメインユーザーの登録方法

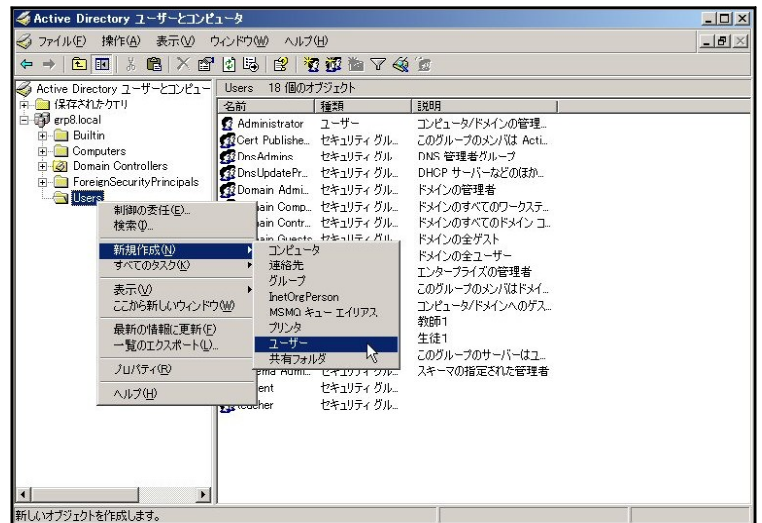
このコンピュータをドメインコントローラにしたことから、ドメインネットワークを管理するコンピュータになりました。ワークグループのときには、それぞれのコンピュータにログオンさせるため、ローカルユーザーアカウントを登録してきました。ドメインコントローラはドメインにログオンするユーザーやコンピュータの管理をしますので、ドメインユーザーアカウントを登録します（ローカルユーザーアカウントは登録する必要がありません（つまり、ネットワークに接続するためのユーザー名を各クライアントに設定する必要はないということです）。それでは、新規にドメインユーザーアカウントを作成し、既存のグループに登録します。

- ① (サ) 「スタート」 - 「管理ツール」 - 「ActiveDirectoryユーザーとコンピュータ」の順にクリックします。

- ② (サ) 右図の画面が表示されるので、ドメイン名「grp〇.local」をダブルクリックして開き、「User」をダブルクリックして右欄に表示されたドメインユーザーを確認してください。  
ここには、以前ワークグループの時に作成した「iwa5〇〇」と「iwa5〇〇」のユーザーが見えます。ドメインコントローラをインストールすると、ワークグループの時に作成したローカルユーザーアカウントは、このようにドメインユーザーアカウントに自動的に格上げされます。



- ③ (サ) 右図のように、「User」で右クリックし、「新規作成」 - 「ユーザー」の順にクリックします。

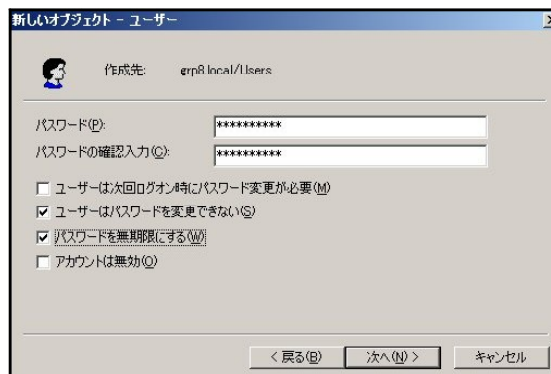


- ④ (サ) 右図の画面が開きますので、「姓」「名」に自分の氏名をそれぞれ入力します（フルネームには自動入力されます）。「ユーザーログオン名」欄に（今回は研修として）「iwa600」と入力し、「次へ」ボタンをクリックします。





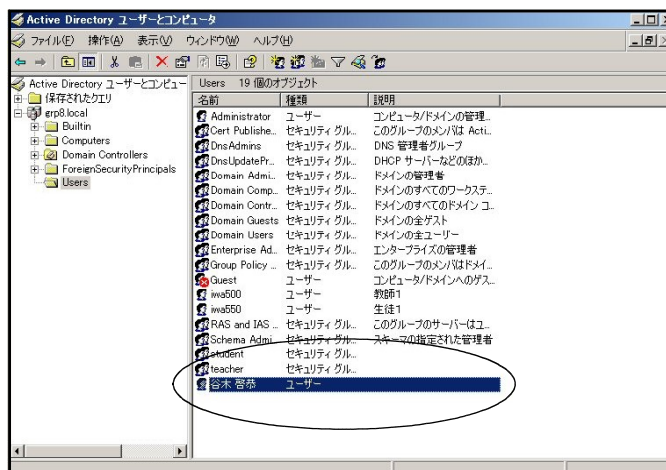
⑤(サ)右図の画面が表示されるので、「パスワード」欄にパスワードを入力します。ここでは、「GrpOpas600」と入力します。○の部分には、各grpの数字を入ることとします。「パスワードの確認入力」欄にもう一度同じパスワードを入力します。ActiveDirectoryでドメインコントローラを構築した場合、デフォルトでパスワードの入力に制限があります。①7文字以上にすること、②半角アルファベット大文字と半角アルファベット小文字と半角数字を用いること、③ユーザー名と同じ文字数字を使わないことです。



⑥(サ)右図が表示されるので、そのまま「完了ボタン」をクリックして作業は終了です。

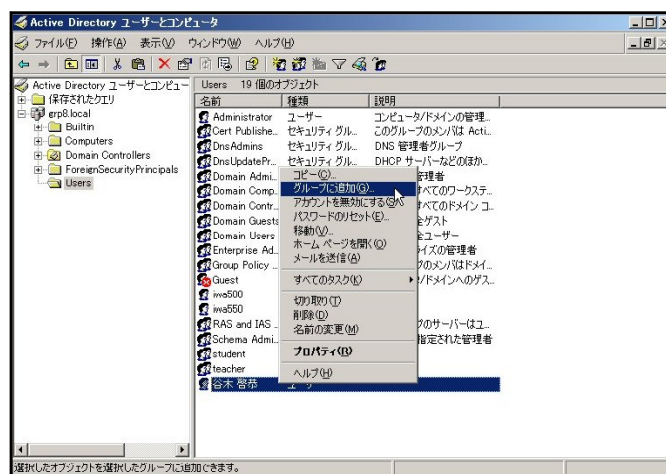


⑦(サ)右図のように、新しいドメインユーザーアカウントが登録されます。

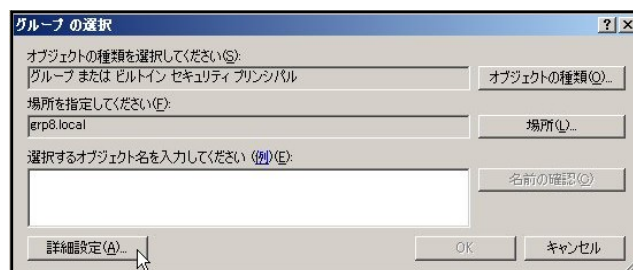


### 3 グループへの登録方法

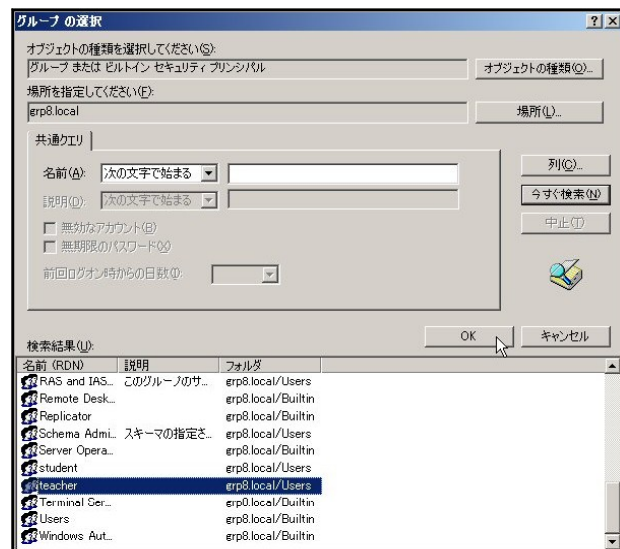
①(サ)右図のように、新しいドメインユーザーを右クリックし、「グループに追加」をクリックします。



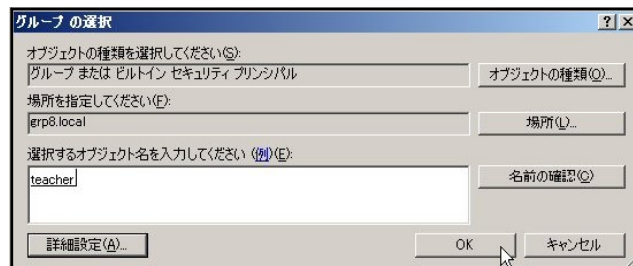
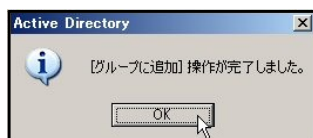
②(サ)右図の画面が表示されるので、「詳細設定」をクリックします。



③(サ)右図の画面が表示されるので、「今すぐ検索」ボタンをクリックして、「検索結果」欄から「teacher」を選択し、「OK」ボタンをクリックします。



④(サ)右図の画面のように、「teacher」が追加されるので、「OK」ボタンをクリックすると、数が表示され作業が終了します。



#### 4 コンピュータの登録方法

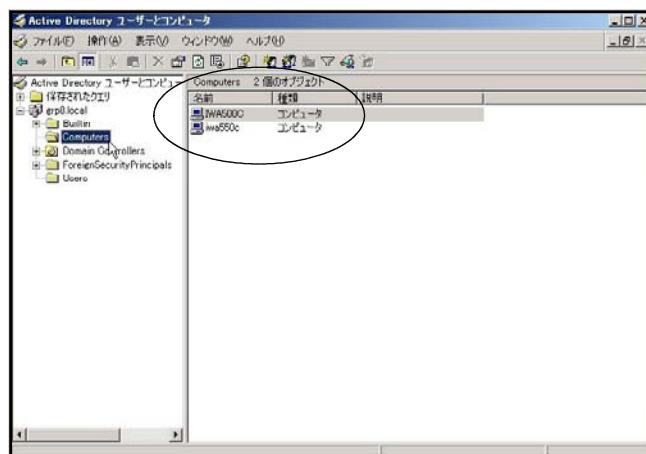
NTドメイン (Windowsドメイン) では一元管理といってもコンピュータ等のリソースの管理はたいへんでした。しかし、ActiveDirectoryドメインでは、コンピュータも含めて一元管理できるようになりました。このことにより、コンピュータやソフトウェアにアクセス権を設定することが可能になりました。通常、ドメインユーザーアカウントでドメインにログオンできれば、ドメインコントローラには自動的にコンピュータアカウントが作成される仕組みになっています。

コンピュータアカウントがドメインコントローラにないドメインにはログオンできないので、コンピュータアカウントを作成する方法を述べておきます。(トラブル対処の時は、**一注意一参照**)

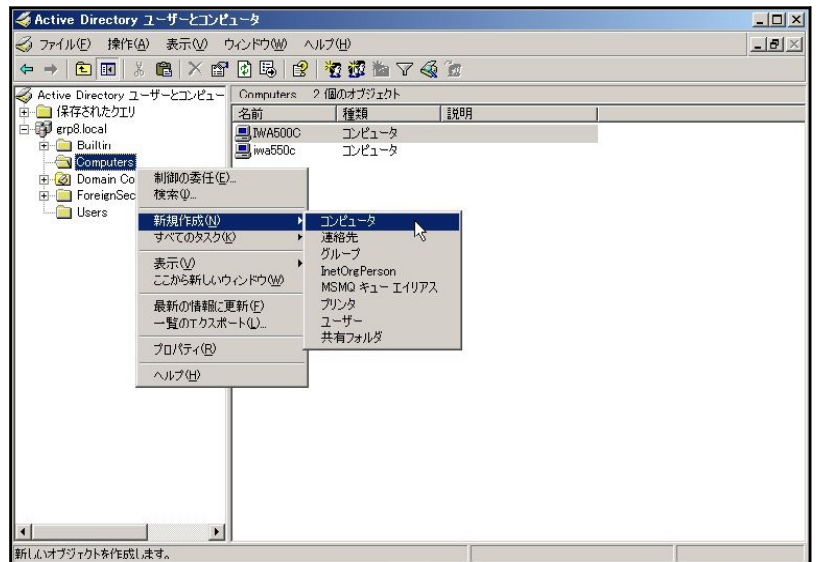
① (サ)「スタート」－「管理ツール」－「ActiveDirectoryユーザーとコンピュータ」の順にクリックします。

② (サ) 右図のように「Computers」をクリックします。

すると、右側に2台のコンピュータがコンピュータ名として表示されています。本来、ActiveDirectoryはドメインで使用するコンピュータを管理者が登録します。しかし、ドメインユーザーがどこかのコンピュータからドメインにアクセスすると、そのコンピュータはドメイン管理されるコンピュータとして自動的に登録されるようになっています。



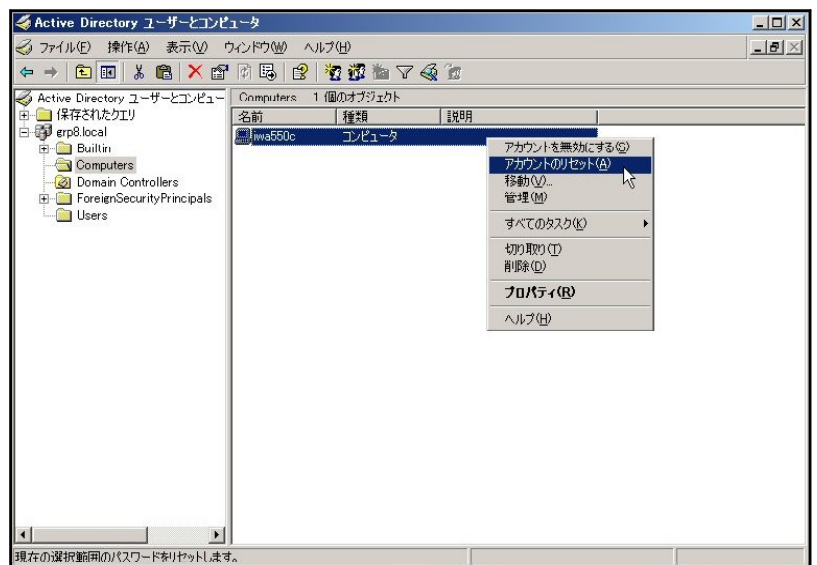
- ③(サ) コンピュータをドメインに登録するためには (コンピュータアカウントと呼ぶ)、右図のように、「Computers」で右クリックし、「新規作成」→「コンピュータ」の順にクリックします。



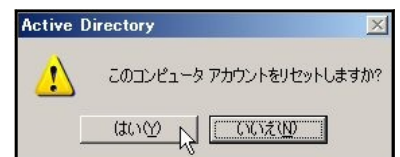
- ④(サ) 右図の画面が表示されるので、ドメインに登録する「コンピュータ名」を入力して、「次へ」ボタンをクリックします。



- ⑤(サ) コンピュータアカウントを登録したときや設定を変更したときは、必ず、「アカウントのリセット」を行います。右図の画面が表示されるので、リセットをかけるコンピュータを選択して右クリックし、「アカウントのリセット」をクリックします。



- ⑥(サ) 右図のメッセージが表示されるので、「はい」をクリックして作業完了です。





－注意－

見た目には、正しいユーザーアカウントとコンピュータアカウントが登録されているのに、クライアントからログオンしようとするときのようなエラーメッセージが表示されることがあります。

「・・・コンピュータアカウントが登録されていません・・・」

- 対処方法：クライアントで「このコンピュータ」の管理者でログオンします  
クライアント側でワークグループを適当に作成して「OK」ボタンを押します  
(一時ワークグループに待避します)  
IDとパスワードを求めてきたら、ドメイン管理者のIDとパスワードを入力します  
クライアントを再起動します  
ドメインコントローラの該当するコンピュータアカウントを削除します  
クライアントで「このコンピュータ」のAdministratorでログオンします  
クライアント側でドメイン名を入力し、「OK」ボタンを押します  
(ドメインにログオンします)  
IDとパスワードを求めてきたら、ドメイン管理者のIDとパスワードを入力します  
クライアントを再起動します  
ドメインユーザーアカウントでドメインにログオンします  
ドメインコントローラーにコンピュータアカウントが自動的に作成されます

「ユーザーアカウントパスワードの文字の長さが足りないか、複雑な要件を満たしていません・・・」

- 対処方法：ドメインコントローラーでユーザーのパスワードを作成し直します  
大文字英字と小文字英字と数字で7文字以上のパスワードを作成し直します  
(決してユーザーアカウントを削除してはいけません。)  
新しいドメインユーザーアカウントのパスワードでログオンします

「ドメインコントローラーが見つかりません」

- 対処方法：ドメインコントローラーとして稼働しているコンピュータを再起動します

以上は、ドメインユーザーアカウントを作成し直したり、コンピュータアカウントをリセットした際に最も現れやすいメッセージです。ワークグループでのローカルユーザーアカウントのときのように、「変な動きをするユーザーアカウントがあればすぐ削除、動作がおかしければすぐに削除、そして作り直せばいい」といった方法は、ドメインコントローラーでは決してやってはいけないことです。一度削除した後、同じ名前のドメインユーザーアカウントを作成しても、うまく動作しないことがほとんどです。それは、見た目には再登録できていてもドメインコントローラー内部にはその情報が残っており、私たち教員では解決不可能な事態になる可能性が大了。

ワークグループ管理されていたユーザーアカウントが自動的にドメインユーザーアカウントに格上げされるのは大変便利なのですが、ドメインユーザーアカウントのパスワードにはデフォルトで規定があり、そのためにログオンできない場合があります。

こういった場合に多いかということ、ワークグループでのローカルユーザーのパスワードを①7文字以上にすること、②半角アルファベット大文字と半角アルファベット小文字と半角数字を用いること、③ユーザー名と全く同じ文字や数字を取り入れないこと、のうち一つでも守れていないときに、ドメインユーザーアカウントに格上げされると不具合が起きやすいのです。

これを防ぐためには、ワークグループ管理の段階で、サーバのローカルユーザーアカウントをいったん削除し、その後、ドメインコントローラーをインストールするのがよいでしょう。そして、ドメインコントローラーで新規にドメインユーザーアカウントを登録してやります。

ユーザーのパスワードを①7文字以上にすること、②半角アルファベット大文字と半角アルファベット小文字と半角数字を用いること、③ユーザー名と全く同じ文字や数字を取り入れないことを3つとも守っている場合には何の問題もありません。

また、インストール後、ドメインユーザーの「アカウントポリシー」の「パスワードのポリシー」を変更してもかまいません。これは、「スタート」－「管理ツール」－「規定のドメインコントローラーセキュリティの設定」の順にクリックし、「セキュリティの設定」－「アカウントポリシー」－「パスワードのポリシー」の順にクリックすることにより設定画面が表示されます。

## C DNSサーバーの役割と構築

DNSサービスは名前解決を行うために必要です。特に、クライアントコンピュータがインターネットに接続するためには必須です。小中学校は、県もしくは市町村のネットワーク、または、民間のプロバイダを経由してインターネットに接続しています。DNSサーバーはドメイン毎に必ず必要なので、学校にドメイン管理されているネットワークやドメインコントローラがあれば、DNSサーバーもあります。仮に学校側にドメインコントローラやDNSサーバーがないとしても、学校の接続先である県もしくは市町村または民間プロバイダに必ず設置されています。実は、このこと以外にも、学校独自にDNSサーバーをたてると、IPアドレスを覚える必要がなくなり、わかりやすい名前でもpingをとばせる等ネットワーク管理が容易になるといった長所があります。DNSサービスは一度提供すれば、特にメンテナンスも必要としないため、安定稼働するコンピュータであれば、ServerOSでなくても機能します。

ここでは、DNSサービスの機能を理解するためにDNSサーバーを構築し、その役割を確かめていきます。

### DNSサービスの役割

- ・前方参照ゾーン：名前（コンピュータ名や完全修飾ドメイン名）をIPアドレスに変換する  
<必ず必要。これがないと各コンピュータはWebページを閲覧できない、メールが送れない等の問題が起こる。また、アクティブディレクトリには必ず必要な機能。>
- ・逆引き参照ゾーン：IPアドレスを名前（コンピュータ名や完全修飾ドメイン名等）に変換する  
<学校規模程度であれば必要なし>
- ・フォワーダ：ドメイン内の名前解決はドメイン内のDNSサーバーが行う。それ以外の名前解決は上位にあるドメインのDNSサーバーを利用する。そのため、フォワーダに一つ上位のDNSサーバーを（問い合わせ先として）登録する。

## 1 DNSサービスのインストール

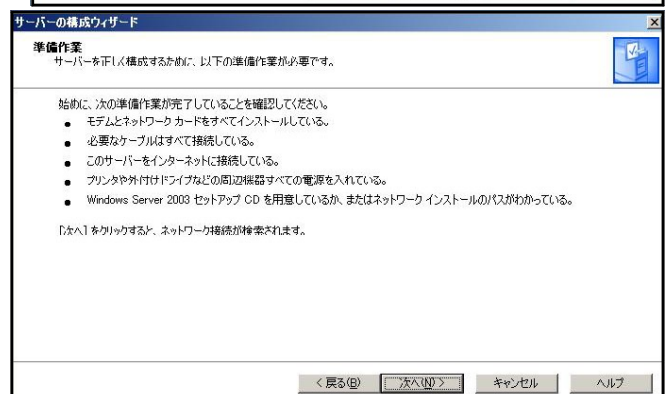
この実習では、WindowsServer2003が標準装備しているDNSサービスを用います。

- ①(サ)「スタート」ボタン→「すべてのプログラム」→「管理ツール」→「サーバーの構成ウィザード」の順にクリックします。WindowsServer2003で何かサービスをインストールするときには、この「サーバーの構成ウィザード」を使うと便利なので覚えておきましょう。（サービスのインストールの方法は、「サーバーの構成ウィザード」を使う以外にも、他のWindowsと同じように、「コントロールパネル」→「プログラムの追加と削除」→「Windowsコンポーネントの追加と削除」→「ネットワークサービス」でも行うことができます）

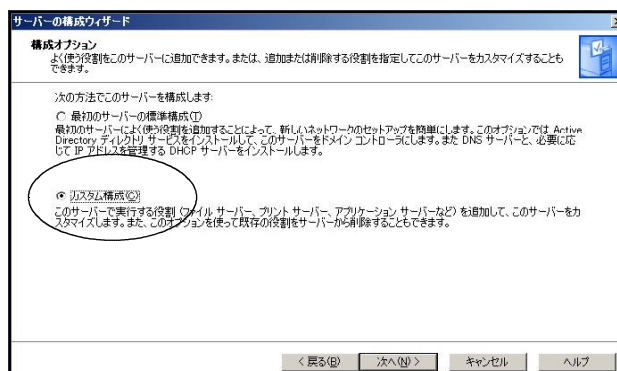
- ②(サ)右図の「サーバーの構成ウィザード」ダイアログが表示されるので、「次へ」ボタンをクリックします。



- ③(サ)右図の画面が表示されるので、そのまま「次へ」ボタンをクリックします。

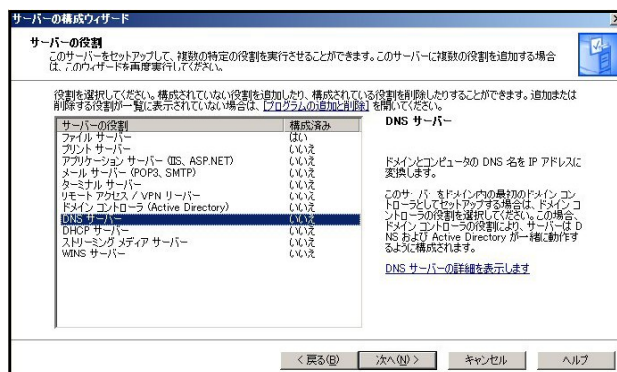


④(サ)右図の画面が表示されるので、「カスタム構成」を選択します。「最初のサーバーの標準構成」は選択しないでください。初級者向けをうたったメニューですが、自由がきかないのです。



⑤(サ)「次へ」ボタンをクリックします。

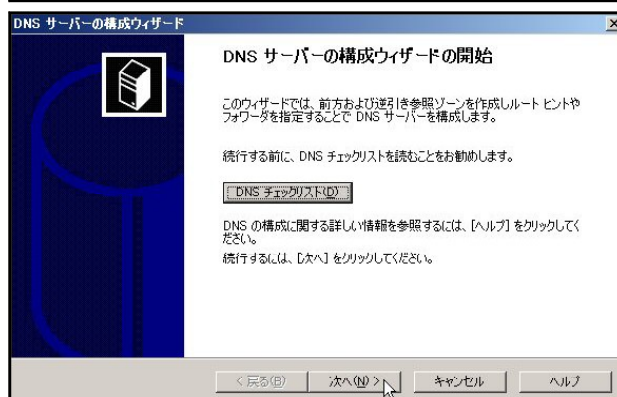
⑥(サ)右図の画面が表示されるので、「DNSサーバー」を選択して「次へ」ボタンをクリックします。



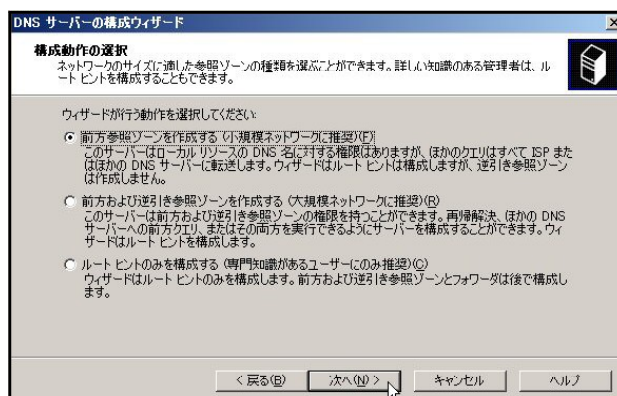
⑦(サ)右図の画面が表示されるので、そのまま「次へ」ボタンをクリックします。



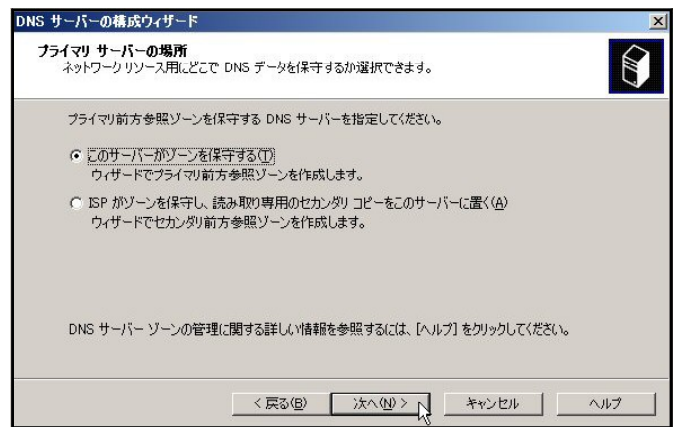
⑧(サ)右図の画面が表示されるので、そのまま「次へ」ボタンをクリックします。



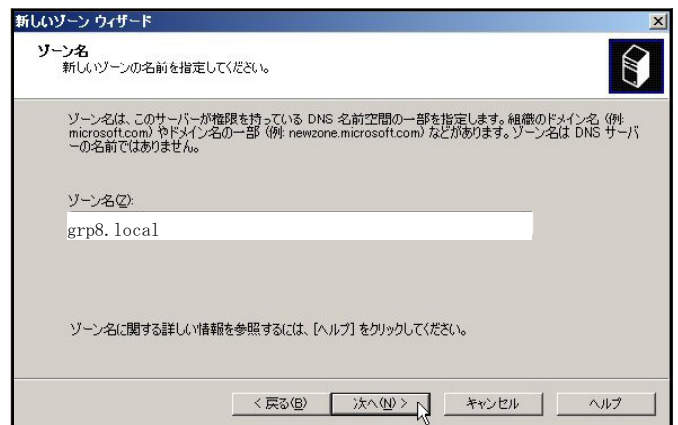
⑨(サ)右図の画面が表示されるので、「前方参照ゾーンを作成する (小規模ネットワークに推奨)」を選択し、「次へ」ボタンをクリックします。



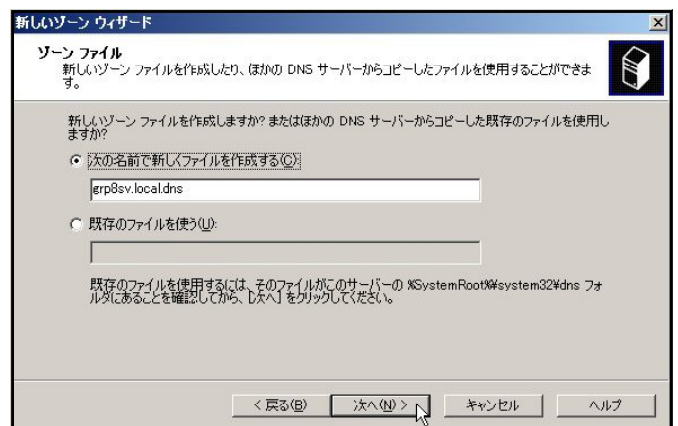
- ⑩(サ) 右図の画面が表示されるので、「このサーバがゾーンを保守する」を選択し、「次へ」ボタンをクリックします。



- ⑪(サ) 右図のような画面が表示されるので、「ゾーン名」欄に、ドメインコントローラを構築するときに入力したドメイン名と同じもの (grp0.local) を入力します。  
この名前を間違えると、ドメインコントローラもDNSサーバーも動かなくなりますので注意してください。  
入力が完了したら「次へ」ボタンをクリックします。



- ⑫(サ) 右図のような画面が表示されるので、「次の名前でも新しくファイルを作成する」にチェックが入っていることを確かめ、「次へ」ボタンをクリックします。  
自動的に入力されているものでOKです。

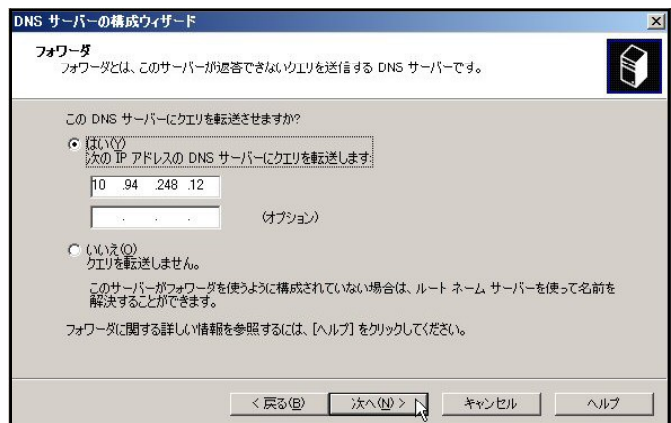


- ⑬(サ) 右図の画面が表示されるので、「セキュリティで保護された動的更新のみを許可する」にチェックを入れます。これにチェックを入れることができない場合には、右図のように「非セキュリティ保護およびセキュリティ保護の両方による動的更新を許可する」にチェックを入れ、「次へ」ボタンをクリックします。



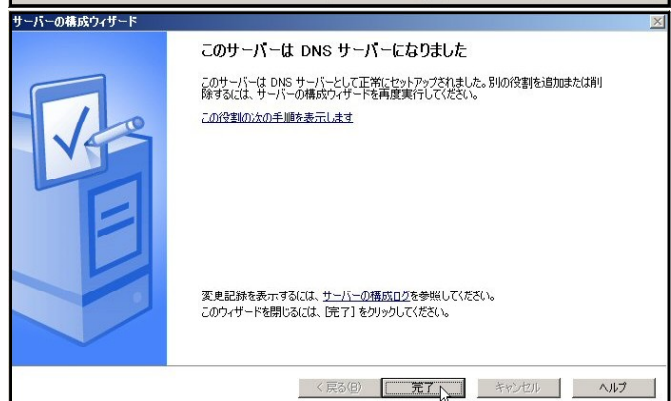


⑭(サ)フォワーダの設定を行います。右図の画面が表示されるので、「はい」を選択し、「次へ」ボタンをクリックします。(本実習では、「10.94.248.12」と入力。上位あるDNSサーバーのアドレスです。)



⑮(サ)「既に設定されている」「同じフォワーダが設定されている」旨のウィンドウが開いたときには、「はい」または「OK」ボタンをクリックします。

⑯(サ)右図の画面が表示されるので、「完了」ボタンをクリックします。

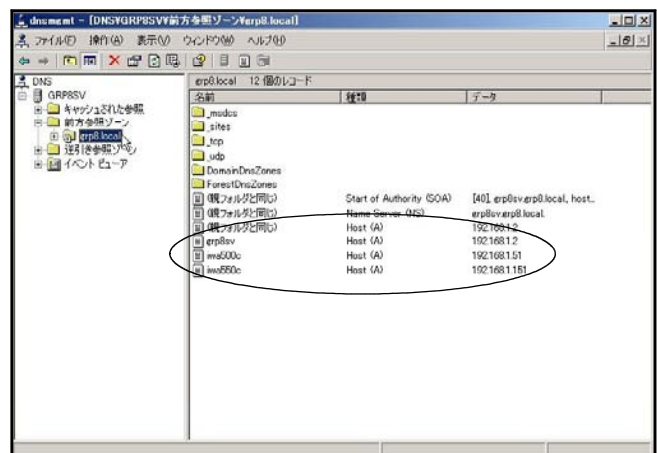


## 2 DNSサービスの設定確認

### ア 前方参照ゾーンの設定

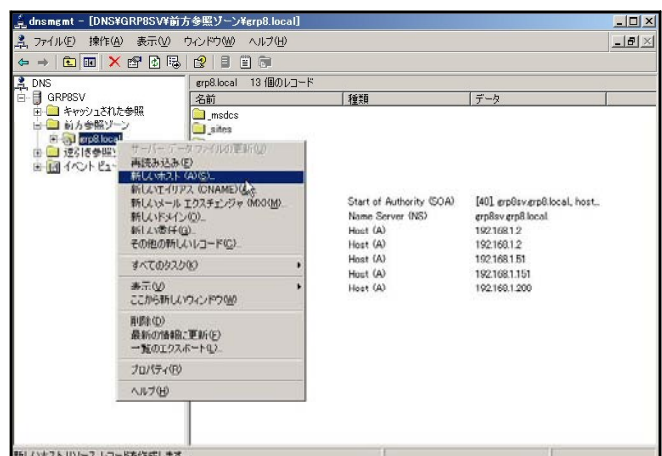
①(サ)DNSの設定を確認します。「スタート」－「管理ツール」－「DNS」の順にクリックします。

②(サ)右図の画面が表示されます。該当するDNSサーバー名 (GRP○SV) をダブルクリックし、さらに「前方参照ゾーン」をダブルクリックした後、「ドメイン名」の「grp○.local」をクリックします。

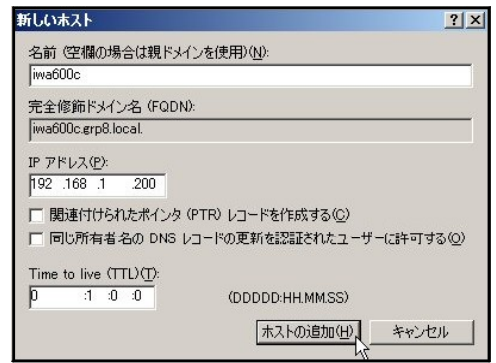


③(サ)自分のコンピュータとドメイン上のコンピュータが、右図のように登録されていることを確認できます。例えば、右図の場合、grp8svに対応したIPアドレスが192.168.1.2というように記述されています。

④(サ)登録されていない場合には、右図のように、ドメイン名である「grp8.local」で右クリックして、「新しいホスト」をクリックします。「ホスト」とは「コンピュータ名」のことと覚えましょう)



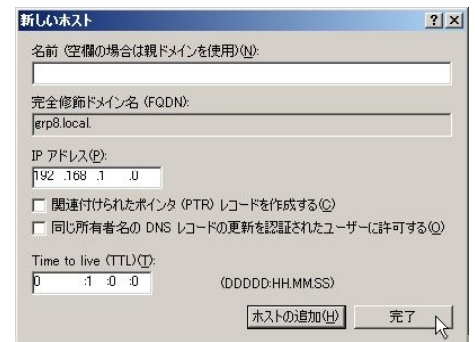
- ⑤(サ)右図の画面が表示されますので、「名前」欄にコンピュータ名を入力し、さらに「IPアドレス」欄にそのコンピュータに割り当てたIPアドレスを入力して「ホストの追加」ボタンをクリックします。



- ⑥(サ)右図のような画面が表示されますので、「OK」ボタンをクリックします。



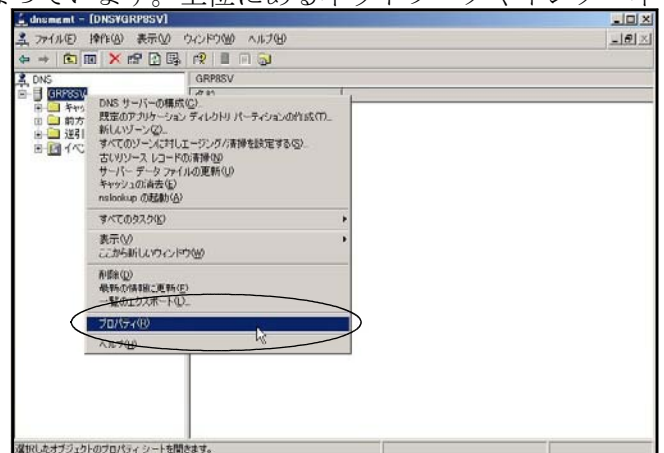
- ⑦(サ)右図のような画面が表示されますので、「完了」ボタンをクリックします。



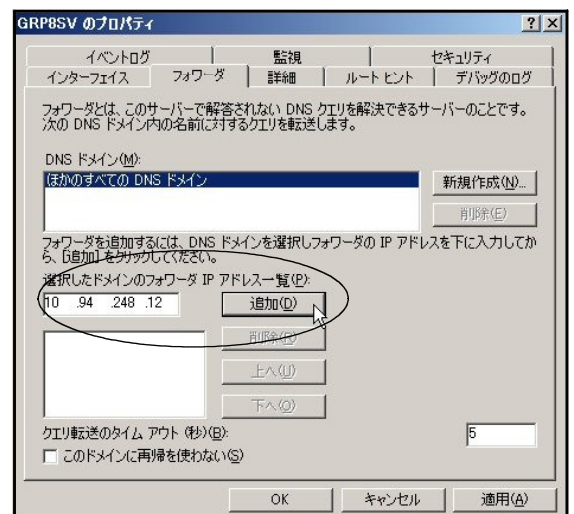
## イ フォワーダの設定

現在、ドメイン内の名前解決ができる設定になっています。上位にあるネットワークやインターネットの名前解決もできるように、DNSサービスの設定をします。具体的には、構築したDNSサーバーの一つ上位に当たるネットワークのDNSサーバーをフォワーダに登録します。このことにより、今立ち上げているDNSサーバーで名前解決できない場合には、フォワーダに登録されているDNSサーバーに問い合わせをして名前解決を図ることができるようになります。

- ①(サ)「スタート」－「管理ツール」－「DNS」の順にクリックします。右図の画面が表示されるので、DNSサーバー名「GRP8SV」で右クリックし、「プロパティ」をクリックします。

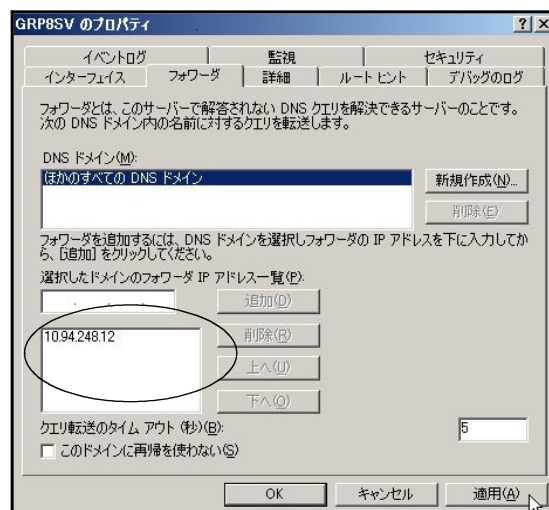


- ②(サ)右図のようなプロパティが表示されるので、「フォワーダ」タブをクリックし、「選択したドメインのフォワーダIPアドレス一覧」に「10.94.248.12」と入力します。このIPアドレスは、教育センターで設置しているDNSサーバーです。この研修室に構築したそれぞれのドメインは、実際には教育センターのネットワークを介してインターネットに接続されますので、一つ上位のネットワークは、教育センターのネットワークになります。「追加ボタン」をクリックします。既に入力されているときには、この操作は必要ないので、③に進みます。



- ③(サ)「OK」ボタンをクリックします。

④(サ)右図のように、一覧に追加されます。



### 3 DNSサービスの役割確認

DNSサービスは、入力したドメイン名からIPアドレスを調べて変換（前方参照）してくれたり、入力したIPアドレスからドメイン名を調べて変換（逆引き参照）してくれたりします。

ここでは、最初に、適当な名前をIPアドレスに割り当て、その名前でもコンピュータを検索できるようにすることで、DNSサービスの役割を確認したいと思います。次に、構築したドメインネットワークにクライアントコンピュータを接続します。さらに、インターネットへの接続設定を行って、DNSサービスのはたらきを振り返りたいと思います。

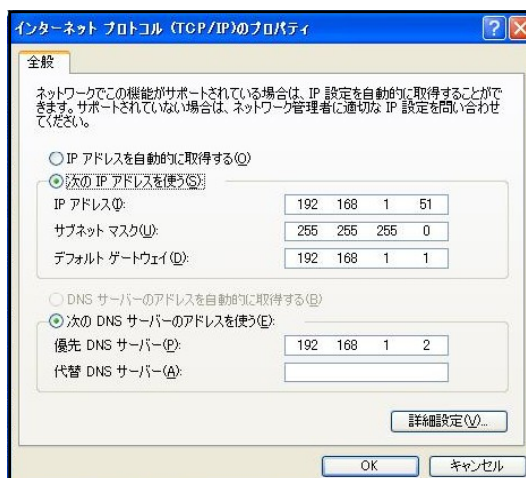
#### ア pingによる接続確認

- ①(サ)DNSに「henoheno」等適当な名前を登録し、IPアドレスを割り当て、pingをとばして、検索できるかどうか確かめます。「スタート」－「管理ツール」－「DNS」の順にクリックします。
- ②(サ)「前方参照ゾーン」の「grp○.local」に新しいホストとして「henoheno」等適当な名前を半角英字で入力します。
- ③(サ)「henoheno」等の名前を付けたホストにクライアントのIPアドレス「192.168.○.51」を割り当てます。
- ④(サ)「ホストの追加」ボタンをクリック、「OK」ボタンをクリック、「完了」ボタンをクリックして作業を完了します。
- ⑤(サ)「スタート」－「すべてのプログラム」－「アクセサリ」－「コマンドプロンプト」の順にクリックします。
- ⑥(サ)表示されているコマンドプロンプトに「ping 192.168.○.51」と入力して「Enter」キーをクリックします。
- ⑦(サ)「192.168.○.51」のコンピュータに接続できる旨、表示されます。
- ⑧(サ)今度は、「ping henoheno」（先ほど適当に付けた名前）を入力して「Enter」キーを押します。
- ⑨(サ)「henoheno」のコンピュータに接続できる旨、表示されます。そのコンピュータのIPアドレスが「192.168.○.51」であることも表示されます。これが、DNSサービスのしくみです。

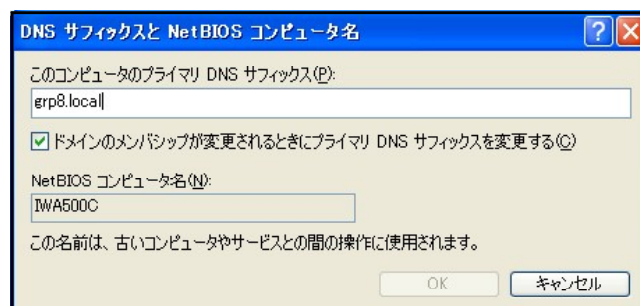
## イ ドメインネットワークへの接続設定

すべてのクライアントコンピュータの「IPアドレス」欄にDNSサーバーのアドレスを入力します。

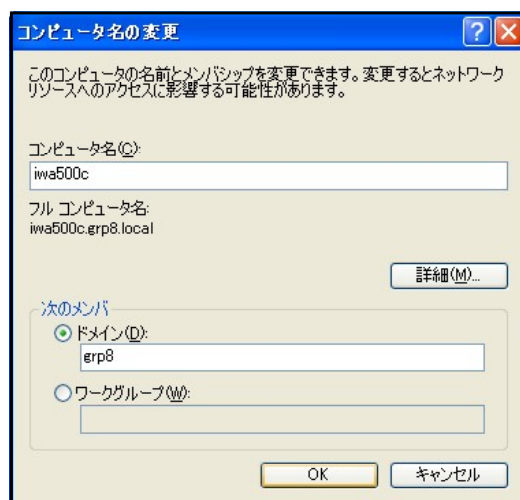
- ①(ク)「コントロールパネル」－「ネットワーク接続」の順にクリックします。
- ②(ク)「ローカルエリア接続」アイコンを右クリックして、「プロパティ」をクリックして開きます。
- ③(ク)「次のDNSサーバーのアドレスを使う」にチェックを入れ、「優先DNSサーバー」欄に「192.168.0.2」と入力し、「OK」ボタンをクリックします。  
「192.168.0.2」は、自分で構築したDNSサービスが稼働しているコンピュータのIPアドレスです。各グループ番号に相当します。



- ④(ク)次に、「マイコンピュータ」を右クリックして「プロパティ」を表示し、「詳細」ボタンをクリックします。
- ⑤(ク)「DNSサフィックスとNetBIOSコンピュータ名」ダイアログが表示されるので、「このコンピュータのプライマリDNSサフィックス」欄に、構築したドメイン名「grp0.local」を入力します。  
入力が終わったら、「OK」ボタンをクリックして、再起動をかけます。



- ⑥(ク)「次のメンバ」欄の「ドメイン」にチェックを入れ、構築したドメイン名「grp0」を入力します。
- ⑦(ク)「OK」ボタンをクリックします。うまく接続できれば、「grp0へようこそ」のメッセージボックスが表示されますが、接続できない場合にはエラーメッセージが表示されます。(エラーメッセージに対処するいくつかの方法を、この章末に記載しておきました。参考にしてください。Server2003のヘルプで検索すると、説明やトラブルシュートを読むことができます。)



## ウ インターネットへの接続設定

インターネットに接続するために、ブラウザにプロキシサーバのアドレスを入力します。

- ①(ク)アドレスは「proxy.center.iwate-ed.jp」、ポート番号は「8080」です。もうおわかりですね。教育センターのネットワークにはDNSサーバーがたっているので、アドレス欄にコンピュータ名(ホスト名)やドメイン名のような名前をいれてもよいわけです。DNSサーバーがたっていない場合には、IPアドレスを入力することになります。
- ②(ク)ブラウザを開いて、Webページをブラウジングしましょう。



## D WINSサーバーの構築

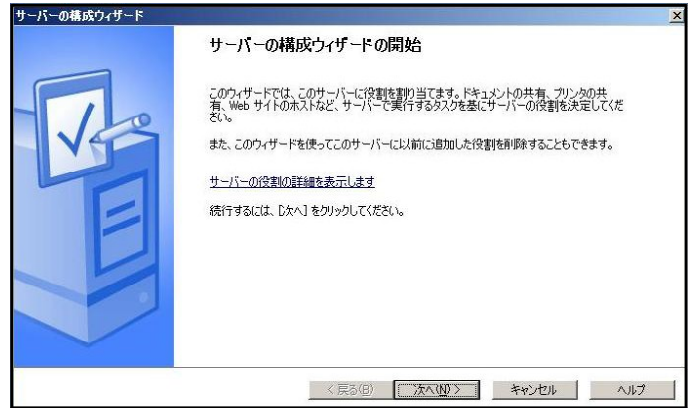
ActiveDirectoryドメインを構築する際、Windows95/98/98SE/Meマシンをクライアントとして接続するためにはWINSサービスが必須となります。逆に、クライアントがWindows2000、XP、Vistaのみであれば、WINSサーバーは必要ありません。

### 1 WINSサービスのインストール

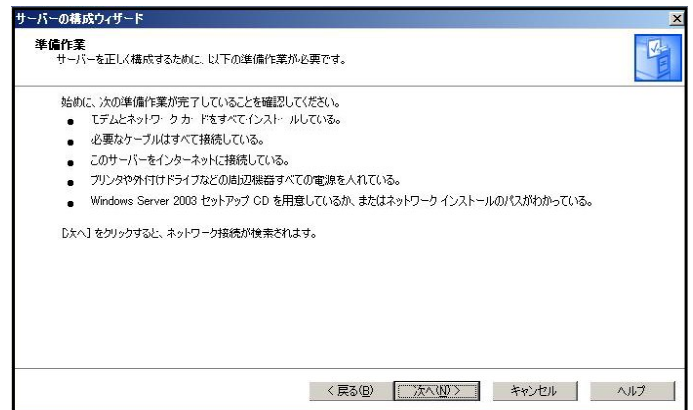
この実習では、WindowsServer2003が標準装備しているWINSサービスを用います。

①(サ)「スタート」ボタン→「すべてのプログラム」→「管理ツール」→「サーバーの構成ウィザード」の順にクリックします。

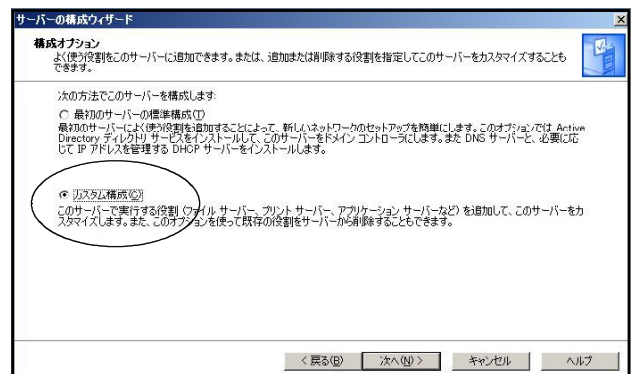
②(サ)右図の「サーバーの構成ウィザード」ダイアログが表示されるので、「次へ」ボタンをクリックします。



③(サ)右図の画面が表示されるので、そのまま「次へ」ボタンをクリックします。

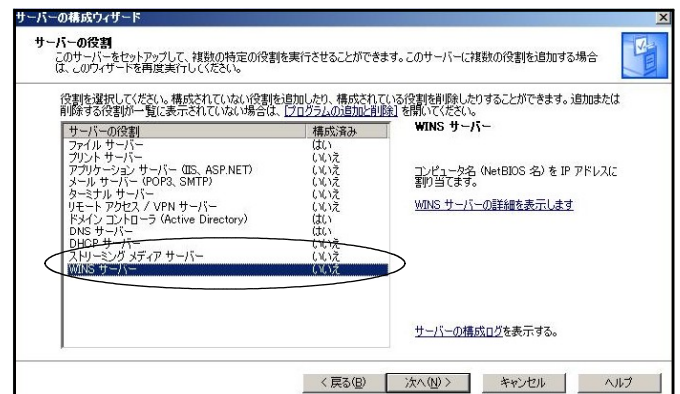


④(サ)右図の画面が表示されるので、「カスタム構成」を選択します。「最初のサーバーの標準構成」は絶対に選択しないでください。初級者向けをうたったメニューですが、自由がきかないのです。



⑤(サ)「次へ」ボタンをクリックします。

⑥(サ)右図の画面が表示されるので、「WINSサーバー」を選択して「次へ」ボタンをクリックします。



⑦(サ)右図の画面が表示されたら、「次へ」ボタンをクリックします。



⑧(サ)しばらく待つと、右図の画面が表示されるので、「完了」ボタンをクリックします。これで、WINSサーバーの導入は終了です。



## 2 DNSサーバーからの参照設定

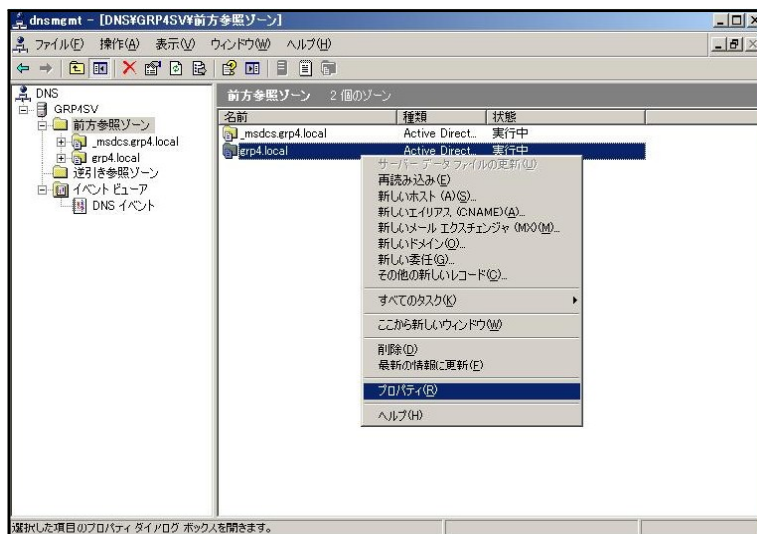
ネットワーク上でWindows95、98、98SE、Me、NTが共存しており、NetBIOSを通じて稼働するファイル共有やプリンタ共有がある場合（これらのOSマシンがサーバーとなっている場合等）には、WINSサーバーが必要であることを前述しました。

Windows95、98、98SE、Me、NT各クライアントマシンが名前解決を行う手順は、①DNSサーバーに問い合わせを行う、②DNSで解決されない場合だけ、WINSサーバーを参照するように各クライアントに回答を返す、③各クライアントはWINSサーバーに問い合わせを行う、というしくみになっています。したがって、DNSサーバーの前方参照ゾーンにWINSサーバーが動作しているコンピュータの「コンピュータ名とIPアドレス」の設定を行う必要があります。

今回、WINSサーバーはDNSサーバーと同一コンピュータに導入していることから、以下に示す手順で設定していきます。

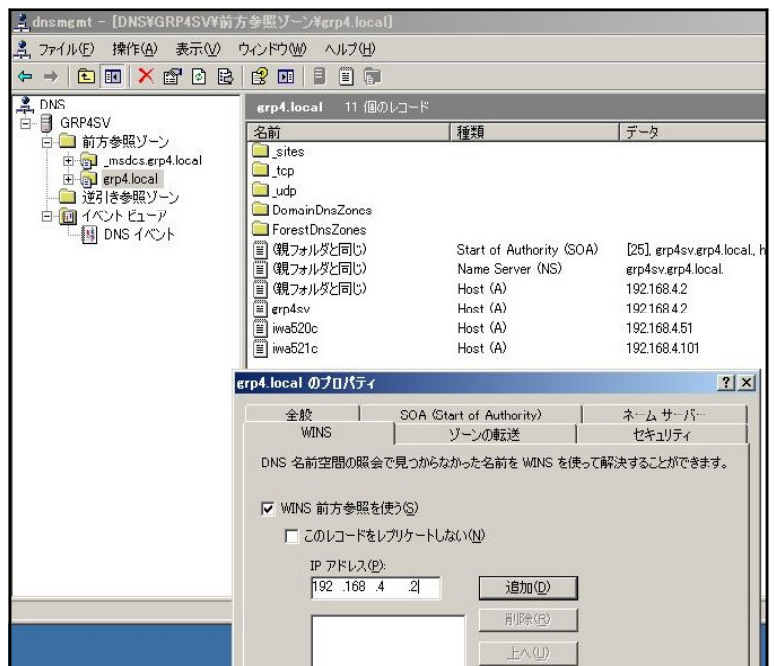
①(サ)「スタート」ボタン－「管理ツール」－「DNS」の順にクリックします。

②(サ)右図の画面が開くので、画面左側のDNSサーバー名（ここでは「GRP4SV」）の下にある「前方参照ゾーン」をクリックします。



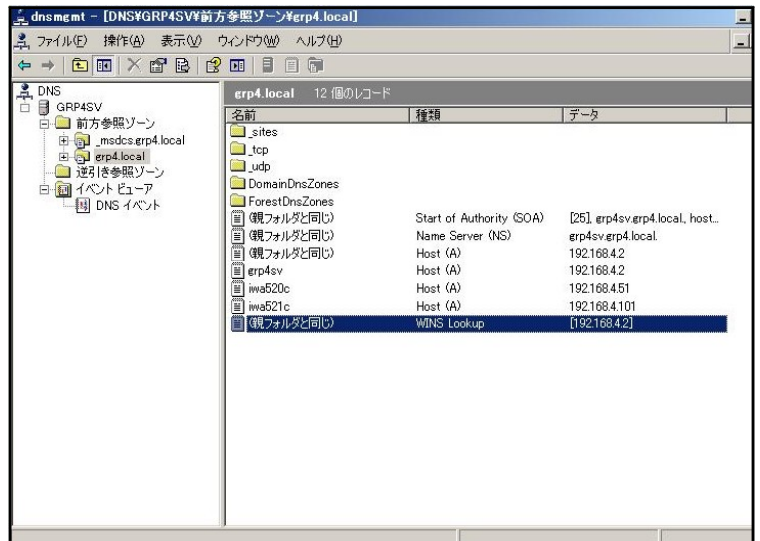
③(サ)右図の画面が開くので、ドメイン名「grp○.local」で右クリックし、表示されたメニューにある「プロパティ」をクリックします。

④(サ)右図のように、ダイアログが開くので「WINS」タブをクリックし、「WINS前方参照を行う」にチェックを入れた後、「IPアドレス」欄に「WINSサーバー」のIPアドレスを入力します。(本実習ではDNSサービスもWINSサービスも同一のコンピュータに導入しているので、同じIPアドレスを入力しています。これらのサービスはネットワークに負荷をあまりかけないことから、学校においても、DNSサービスとWINSサービスを導入するコンピュータを分ける必要はありません)



⑤(サ)IPアドレスの入力が終わったら、「追加」ボタンをクリックした後、「適用」ボタン→「OK」ボタンの順にクリックし、設定を完了させます。

⑥(サ)右図のように、DNSサーバーの前方参照ゾーンに「WINS Lookup」が追加されました。



## E Webサーバーの役割と構築

※別冊「情報サイト8 (Webアプリケーション)利用マニュアル」を参照してください。

## MEMO

## F FTPサーバーの構築

FTPは、インターネットで広く使われているファイル転送用プロトコルです。不特定多数の相手にファイルをダウンロードさせたり、Webサーバーへコンテンツをアップロードさせたりするのに利用されています。Windowsファイル共有との大きな違いはセキュリティ面です。Windowsファイル共有の場合は、フォルダやドライブにユーザー毎のアクセス権を設定するので、設定が煩雑になるだけでなく、フォルダやドライブは丸見えになります。「ファイル共有をかけていたら児童生徒からフォルダが丸見え」「機密性の高いファイルを他の人に見られる」「住所氏名の入ったファイルが勝手にコピーされる」といったこともなくなります（FTPの場合、共有しているフォルダさえ見ることはできません）。また、ルータを利用している場合（例えば、職員室はワークグループ管理で校内ネットワークに接続するためにルータを設置している等）は、職員室のクライアントから校内サーバの共有フォルダにアクセスすることができませんが、FTPであれば、アクセスすることが可能になります。

今後は、設定が容易なWindowsファイル共有とセキュリティが高いFTPサーバを用途によって使い分けていくことが大切です。

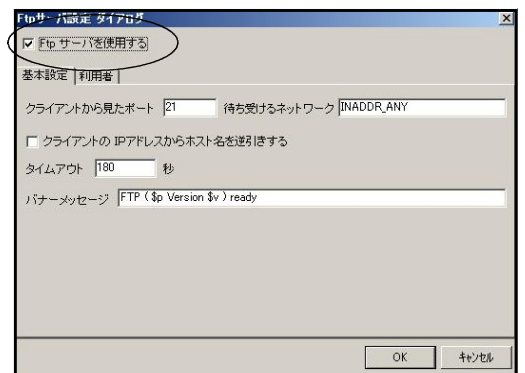
本実習では、フリーソフトウェアである「Black Jumbo Dog」を利用してFTPサーバーを構築し、FTPサービスを運用できるようにします。（IISにもFTPサービスの機能があります。設定や管理や楽なのですが、トラブルに対処する際、他のサービスとの連携部分が多く、原因を特定するのに時間がかかることから、本実習では扱いません。）

### 1 FTPサーバーの設置

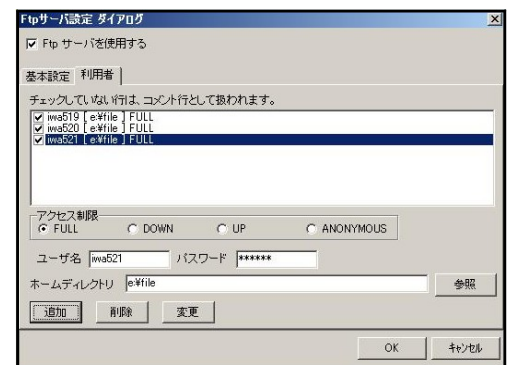
- ①(サ)「Black Jumbo Dog」を起動し、右図のように「設定」 - 「FTPサーバ」の順にクリックします。



- ②(サ)右図のように「FTPサーバを使用する」にチェックを入れます。



- ③(サ)「利用者」タブをクリックし、右図画面を表示させます。「ユーザー名」欄に利用を許可するユーザーIDを入力します。さらに「パスワード」欄にも入力します。



- ④(サ)ホームディレクトリ欄の「参照」ボタンをクリックし、FTPで共有するフォルダを指定します（本実習ではEドライブに「file」フォルダを作成して共有させることとします）。

- ⑤(サ)「アクセス制限」欄でアクセス権限を設定します。

「full」：フルアクセス。読み書き可能。

「DOWN」：ダウンロードのみ可能。つまり、読み込みのみ可能。

「UP」：アップロードのみ可能。つまり、書き込みのみ可能。

「ANONYMOUS」：ゲスト接続。つまり、閲覧のみ可能で、読み込みも書き込みも不可能。

- ⑥(サ)「OK」ボタンをクリックして設置及び設定完了です。



## 2 クライアントからの利用

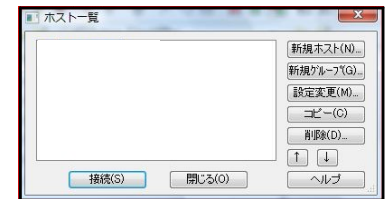
FTPサービスを利用する一つは、FTPクライアントソフトウェアを用いる方法です。クライアントソフトとしては、Windows標準添付のエクスプローラやWebページ作成ソフトの付属ソフトがあります。また、フリーソフトも数多く出回っており、その中には、安定動作することで有名な「ffftp」があります。

### (1) フリーソフト (FFFTP) による利用

①(ク)「Sota's Web Page(<http://www2.biglobe.ne.jp/~sota/>)」からffftpを任意の場所にダウンロードします。(ffftpは、曾田純氏が開発したフリーソフトで、Vistaにも対応しています。)

②(ク)任意の場所に保存した「ffftp-1.95.exe」をダブルクリック等して、コンピュータにインストールします。(提示された画面に従ってインストール作業を行います)

③(ク)ffftpを起動すると、右図の画面が表示されるので、「新規ホスト」ボタンをクリックします。



④(ク)右図の画面が表示されるので各種設定を行います。

#### ホストの設定名

任意です。わかりやすい名前をつけましょう。

#### ホスト名(アドレス)

校内ネットワーク内のFTPサーバーのコンピュータ名を入力します。インターネット上のFTPサーバーであれば、そのサーバーのIPアドレスかドメイン名を入力します。

(例)「ftp://www1.iwate-ed.jp」であれば、「www1.iwate-ed.jp」と入力する

ユーザー名：アクセス許可されたユーザー名を入力します

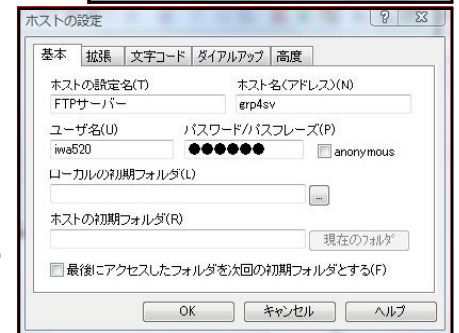
パスワード：該当するパスワードを入力します

#### ローカルの初期フォルダ

ffftpが起動したとき、最初に表示させるクライアント側フォルダを指定します

#### ホストの初期フォルダ

ffftpが起動したとき、最初に表示させるFTPサーバー側のフォルダを指定します



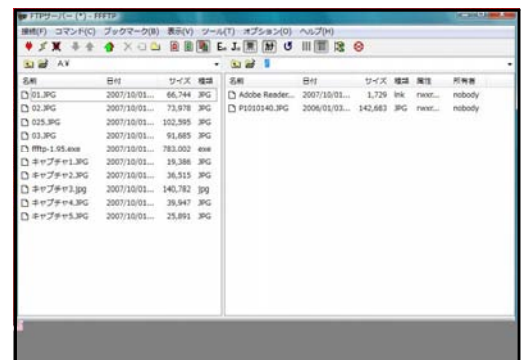
⑤(ク)「OK」ボタンをクリックして設定を完了します。

⑥(ク)右図の画面が表示されるので、「ホスト一覧」にある先ほど設定した「ホスト名」を選択し(ここでは「FTPサーバー」)、「接続」ボタンをクリックします。



⑦(ク)接続に成功すると、右図のような画面が表示されます。左側に表示されているのがクライアント側、右側に表示されているのがサーバー側です。

必要なファイルをドラッグアンドドロップすることにより、アップロードやダウンロードの作業を行います。



## (2) エクスプローラによる利用

①(ク)「スタート」－「コンピュータ」の順にクリックするなどしてエクスプローラを起動します。



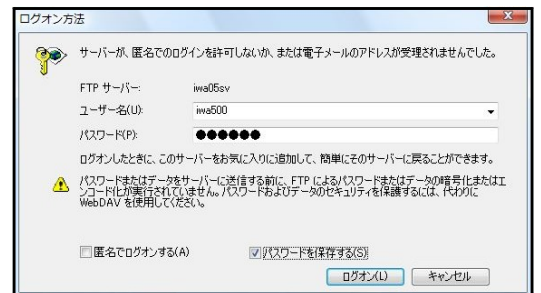
②(ク)右図のように起動したら、アドレスバーにあるコンピュータアイコンをクリックします。

③アドレスを青色反転させ、「Delete」キーを押してアドレスを消去します。

④(ク)右図のように、アドレスバーに「ftp://〇〇〇〇/」(〇〇〇〇はサーバーのコンピュータ名またはIPアドレス)を入力し、「Enter」キーを押します。



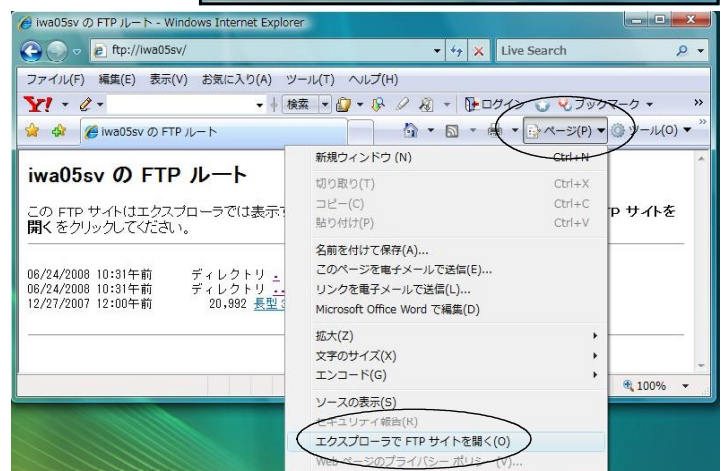
⑤(ク)右図のログオン画面が表示されたら、ユーザー名とパスワードを入力して、「パスワードを保存する」にチェックをいれ、「ログオン」ボタンをクリックします。



⑥(ク)右図のように、FTPサーバーにログオンでき、保存されているファイルが表示されます。



⑦(ク)右図の画面が表示されたときには、ツールバーにある「ページ」ボタンをクリックし、表示されたプルダウンメニューの「エクスプローラでFTPサイトを開く」をクリックします。



⑧(ク)ユーザー名とパスワードの入力を求められる画面が表示されるので、任意のユーザー名とパスワードを入力します。

## G メールサーバーの構築

フリーソフトウェアである「Black Jumbo Dog」を利用して、校内で電子メールを交換できるようにします。また、学校に一つしかない代表メールアドレスを、教職員全員で使えるようにする設定方法を紹介します。

### 1 校内メールシステム及びメールアカウントの作成

①(サ)「Black Jumbo Dog」を起動し、「設定」－「メールサーバ」の順にクリックします。

②(サ)「メールサーバを使用する」にチェックを入れます。

メールサーバ 設定ダイアログ

メールサーバを使用する

基本設定 | 追加ドメイン名 | ヘッダ制御 | サーバ配信 | インターネット転送 | 中継許可 | 別名指定 | 利用

ドメイン名 bjd.ne.jp

メール送信(SMTP)  
クライアントから見たポート 25 待ち受けるネットワーク INADDR\_ANY

メール受信(POP3)  
クライアントから見たポート 110 待ち受けるネットワーク INADDR\_ANY

POP3サーバ認証方式  
 両対応  APOPのみ  USER/PASSのみ

メールを保存するディレクトリ  
C:\PROGRAMS\BLACKJ\MAILBOX 参照

ユーザごとに保存可能なメールの数 200 通

ユーザごとに保存可能なメールの容量 0 KByte

メールアドレス一覧のURL mailaddress.html

OK キャンセル

③(サ)「基本設定」タブをクリックし、「ドメイン名」欄に「grp○.ed.jp」と入力します。このドメイン名は、校内メールアカウントの@（アットマーク）以降に表記されます。

メールサーバ 設定ダイアログ

メールサーバを使用する

基本設定 | 追加ドメイン名 | ヘッダ制御 | サーバ配信 | インターネット転送 | 中継許可 | 別名指定 | 利用

ドメイン名 grp○.ed.jp

メール送信(SMTP)  
クライアントから見たポート 25 待ち受けるネットワーク INADDR\_ANY

メール受信(POP3)  
クライアントから見たポート 110 待ち受けるネットワーク INADDR\_ANY

POP3サーバ認証方式  
 両対応  APOPのみ  USER/PASSのみ

メールを保存するディレクトリ  
C:\PROGRAMS\BLACKJ\MAILBOX 参照

ユーザごとに保存可能なメールの数 200 通

ユーザごとに保存可能なメールの容量 0 KByte

メールアドレス一覧のURL mailaddress.html

OK キャンセル

④(サ)「利用者」タブをクリックし、メールを利用する人のメールアカウントを登録します。

「アカウント」「パスワード」は、ドメインユーザーと同じものを用います。「コメント」欄には氏名等を入力しておくとうわかりやすいと思います。管理者のアカウントは消去しないようにします。

一人分の入力が終わったら「追加」ボタンをクリックします。

メールサーバ 設定ダイアログ

メールサーバを使用する

追加ドメイン名 | ヘッダ制御 | サーバ配信 | インターネット転送 | 中継許可 | 別名指定 | 利用者 | パスワード

チェックしていない行は、コメント行として扱われます。

master【管理者】

アカウント jwa511

パスワード \*\*\*\*\*

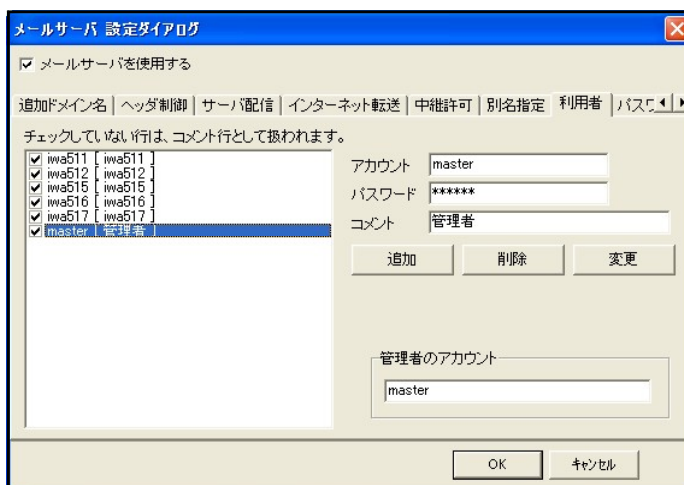
コメント jwa511

追加 削除 変更

管理者のアカウント  
master

OK キャンセル

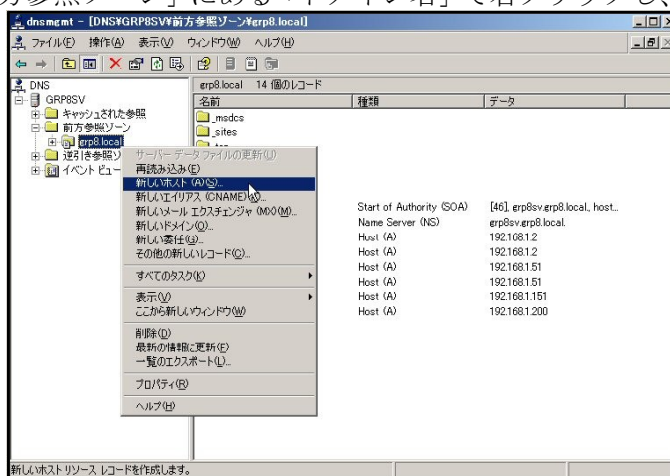
- ⑤(サ) ドメインユーザー全員分のメールアドレスを入力します



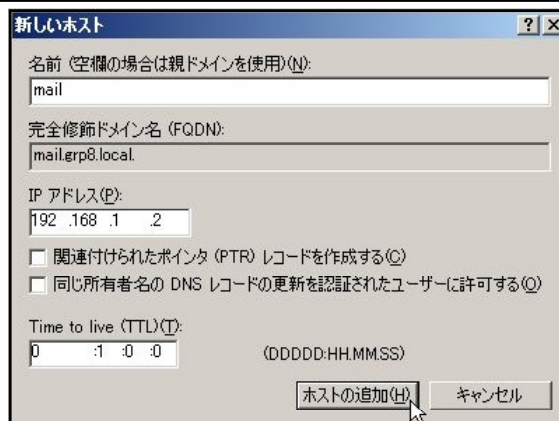
## 2 DNSサーバーへのメールサーバー登録

クライアントのメールソフトにメールサーバー（SMTP（送信用）サーバーとPOP3（受信用）サーバー）の登録を容易にするため、メールサーバーに名前を付け、DNSサーバーに登録します。

- ①(サ) DNSサービスを開き、DNSサーバーの「前方参照ゾーン」にある「ドメイン名」で右クリックし、「新しいホスト」をクリックします。



- ②(サ) 右図のような画面が表示されるので、「名前」欄に「mail」、「IPアドレス」欄に「192.168.0.2」と入力します。  
このことにより、メールソフトにメールサーバーを登録する際、IPアドレスを入力することなく「mail.grp0.local」または「mail」と入力すればよいこととなります。



- ③(サ) 入力し終わったら、「ホストの追加」ボタンをクリックします。

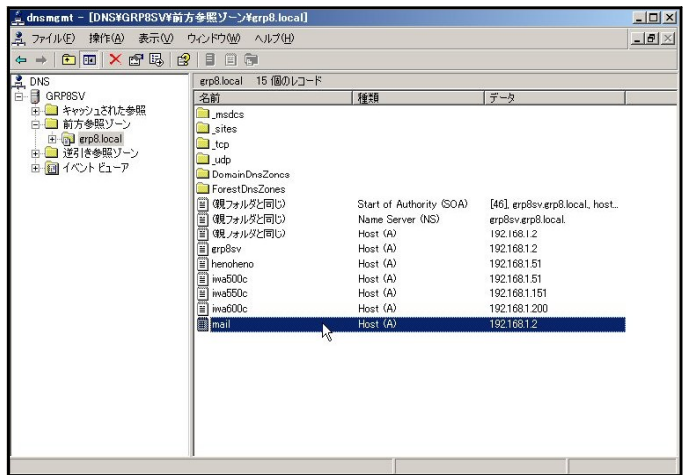
- ④(サ) 右図の画面が表示されるので、「OK」ボタンをクリックします。



- ⑤(サ) 次に表示される画面で「完了」ボタンをクリックします。

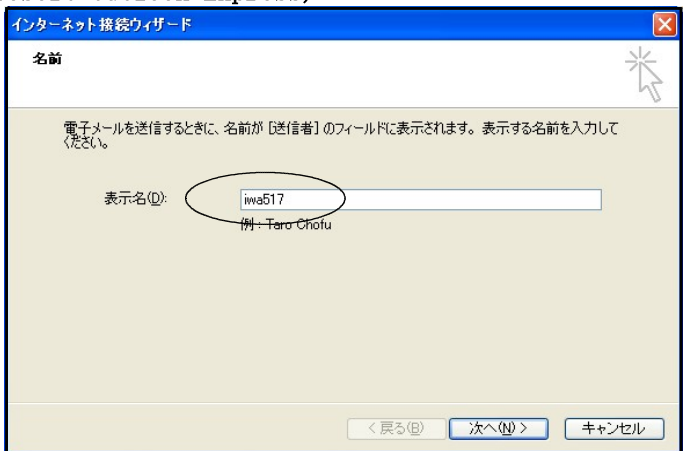


- ⑥(サ)「名前」欄に「mail」が追加されました。

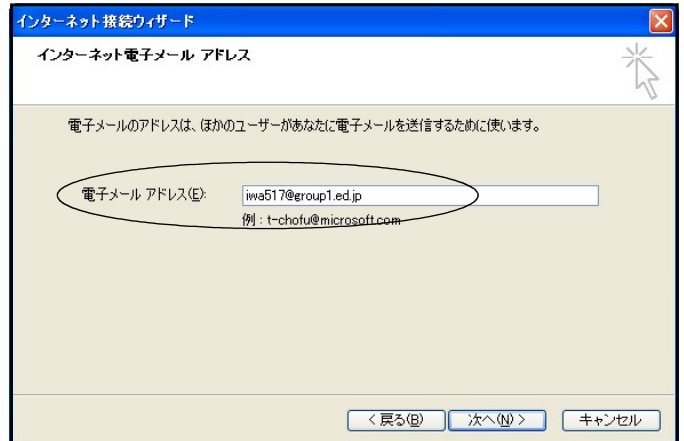


### 3 クライアント側のメールソフトの設定 (Microsoft Outlook Express)

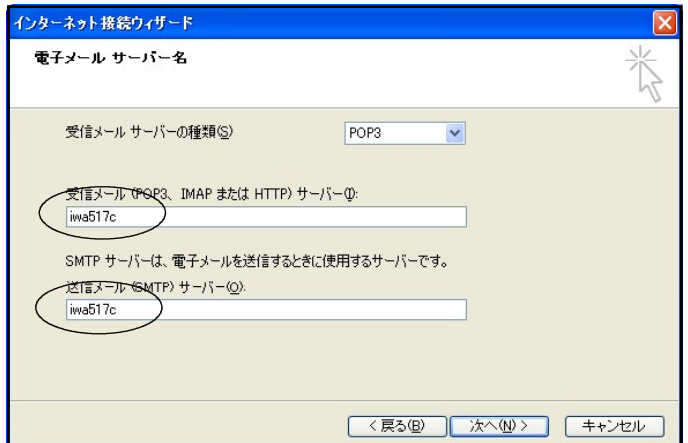
- ①(ク)「インターネット接続ウィザード」で表示名を入力します。



- ②(ク) 電子メールアドレスを入力します。(ドメイン名を「grp4.ed.jp」、アカウントを「iwa520」とあらかじめ設定したならば、ここには、「iwa520@grp4.ed.jp」と入力します)

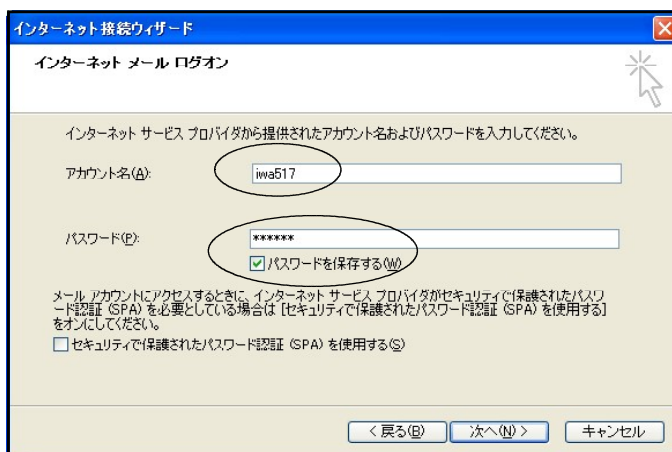


- ③(ク) 受信 (POP3) メールサーバー欄、送信 (SMTP) メールサーバー欄のそれぞれにメールサーバーのIPアドレス (192.168.0.2) か、コンピュータ名 (grp○sv) か、DNSサーバーに登録した「mail.grp8.local」あるいは「mail」と入力します。(本実習では、メールサーバーはドメインコントローラと同じコンピュータです)



④(ク)メールサーバーへ登録したものと同じメールアドレスとパスワードを入力します

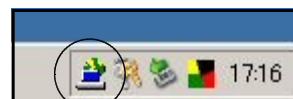
⑤(ク)「パスワードを保存する」にチェックを入れます。



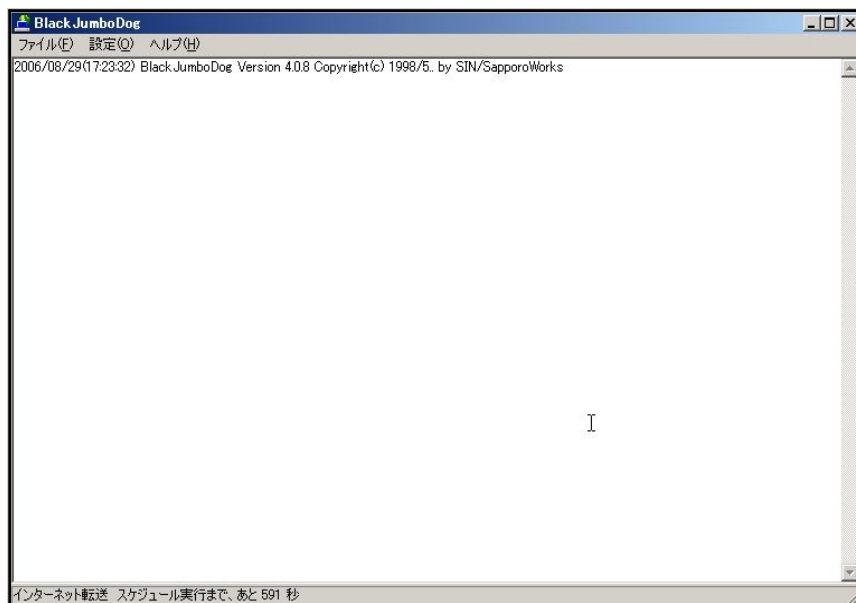
#### 4 校内メールシステムで外部とメールを交換する方法

県内の小中学校には、メールアドレスが学校代表として一つだけ割り当てられていることが多いようです。その一つだけしかないメールアドレスを教職員全員で用いる方法を紹介します。この方法は、「Black Jumbo Dog」で校内メールシステムを構築していることを前提にしています。

①(サ)「Black Jumbo Dog」が起動していることを確認します。起動していれば、右図のように、システムトレイに「Black Jumbo Dog」のアイコンが表示されています。もし、表示されていなければ、「スタート」－「すべてのプログラム」－「Black Jumbo Dog」－「Black Jumbo Dog」の順にクリックしてください。



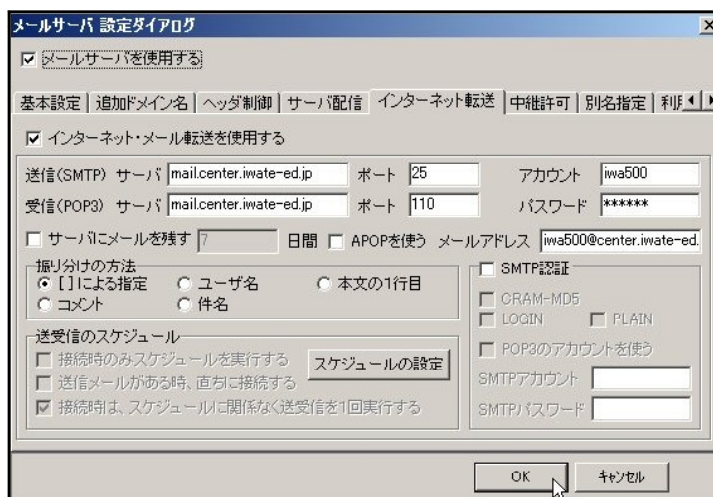
②(サ)①のアイコンをダブルクリックします。すると、右図の画面が起動します。



③(サ)メニューバー「設定」－「メールサーバー」の順にクリックします。



④(サ)「インターネット転送」タブをクリックし、「インターネット・メール転送を使用する」にチェックを入れると、右図の画面が表示されます。



⑤(サ)「送信(SMTP)サーバ」欄に、市町村あるいはプロパイダから割り当てられている送信メールサーバのアドレスを入力します。本講座では、「mail.center.iwate-ed.jp」と入力します。

⑥(サ)「送信(SMTP)サーバ」の「ポート」欄に25を入力します。この数値は決まっているものなので変更してはいけません。

⑦(サ)「受信(POP3)サーバ」欄に、市町村あるいはプロパイダから割り当てられているプロパイダの受信メールサーバのアドレスを入力します。本講座では、「mail.center.iwate-ed.jp」と入力します。

⑧(サ)「受信(POP3)サーバ」の「ポート」に110を入力します。この数値は決まっているものなので変更してはいけません。

⑨(サ)「アカウント」欄、「パスワード」欄、「メールアドレス」欄に市町村あるいはプロパイダから指定されたものを入力します。本講座では、以下のように入力してください。

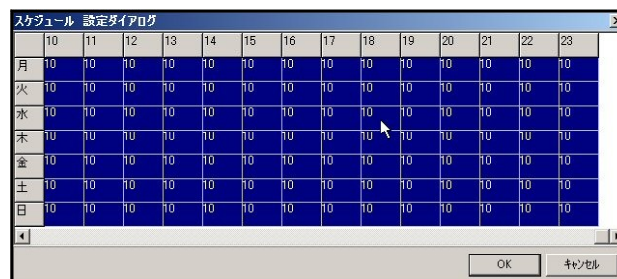
	アカウント	パスワード	メールアドレス
grp2	iwa501	pas501	iwa501@center.iwate-ed.jp
grp3	iwa507	pas507	iwa507@center.iwate-ed.jp
grp4	iwa513	pas513	iwa513@center.iwate-ed.jp
grp5	iwa519	pas519	iwa519@center.iwate-ed.jp
grp6	iwa504	pas504	iwa504@center.iwate-ed.jp
grp7	iwa510	pas510	iwa510@center.iwate-ed.jp
grp8	iwa516	pas516	iwa516@center.iwate-ed.jp
grp9	iwa522	pas522	iwa522@center.iwate-ed.jp
grp10	iwa525	pas525	iwa525@center.iwate-ed.jp

⑩(サ)「サーバにメールを残す」のチェックをはずします。ここにチェックを入れておくと、メールサーバーのディスクが一杯になり、送受信できなくなります。

⑪(サ)「振り分けの方法」欄にある「[]による振り分け」にチェックを入れます。

⑫(サ)専用線や光ケーブル、ケーブルテレビ、ADSL等によるブロードバンド接続の学校の場合は、以下のようにします。

「送受信のスケジュール」欄にある「スケジュールの設定」ボタンをクリックすると、右図の画面が表示されるので、メールサービスを行う曜日及び時間帯をドラッグで指定します。本講座では、すべての曜日及び時間帯をドラッグにより指定してください。



⑬(サ)青色反転しているところで右クリックします。

⑭(サ)右図の画面が表示されるので、「30分間」または「1時間毎」にチェックを入れます。これは、市町村あるいはプロバイダのメールサーバーにアクセスする時間間隔を設定するものです。ブロードバンドの場合は何時間つないでも定額なので、比較的短い間隔でサーバーへ接続した方がよいでしょう。逆に、ダイヤルアップやISDNで接続している学校の場合は、接続するたびに料金が課金されますから、このスケジュール方法では設定しません。



⑯以降の方法で設定してください。

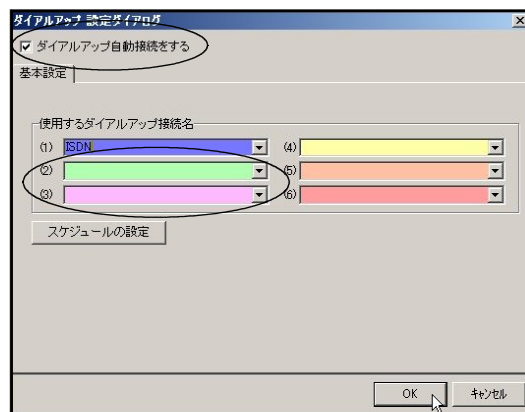
「OK」ボタンをクリックします。

⑮(サ)⑬の画面に戻るので、「OK」ボタンをクリックします。これで、ブロードバンド接続の場合は終了です。

⑯(サ) ISDN等ダイヤルアップを用いて接続している学校の場合には、以下のように設定します。一度、「OK」ボタンをクリックして、「メールサーバ設定ダイアログ」を閉じます。次に、右図のように、メニュー「設定」→「ダイヤルアップ」の順にクリックします。



⑰(サ)右図の画面が表示されますので、「ダイヤルアップ自動接続をする」にチェックを入れ（ブロードバンド環境では必ずこのチェックは外すこと）、「使用するダイヤルアップ接続名」の三角スピンをチェックして、コンピュータに登録されている「ダイヤルアップ設定名」と同じ名前を選択します。つまり、ダイヤルアップ接続の場合には、ダイヤルアップ設定がなされているコンピュータに、このメールサーバーをたてることとなります。「OK」ボタンをクリックして、この画面を閉じます。



⑱(サ)再度、メニュー「設定」→「メールサーバー」の順にクリックし、「インターネット転送」タブをクリックします。そして、「接続時のみスケジュールを実行する」のチェックを外します。このチェックを入れると、別の理由でダイヤルアップ接続が接続されているときに、スケジュールのタイミングが来ると転送を実施します。比較的、接続する機会が多い環境では、このスイッチを入れることで、経済的な運用が可能になります。

⑲(サ)「送信メールがある時、直ちに接続する」のチェックを外します。このチェックを入れると、外部（インターネット）向けのメールがあるとき、スケジュールに関係なく直ちに接続を開始するようになります。

⑳(サ)「接続時は、スケジュールに関係なく送受信を1回実施する」にチェックを入れます。これで、ダイヤルアップ接続の場合は終了です。

## 5 中継許可（セキュリティ）

4で構築した校内メールシステムには、外部とメール交換を行うしくみがありません。そこで、外部と交換できる一つのメールアドレスを中継して外部とやりとりしようとするものです。この方法は、外部の人がメールアドレスをみただけで、メールが中継されていることを容易に理解できます。



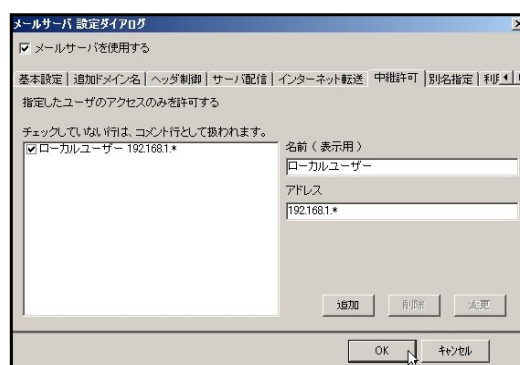
ただし、悪意のある人物は、そのようにして構築されたメールアドレスから容易に校内メールシステムの情報を知り悪用しようとし、第三者中継といって、自分の所在を隠すために他のメールアドレスやメールサーバーを用いるのです。具体的には、設置したメールサーバーが踏み台にされ、他者にウイルスやスパイウェア、スパムメール等をばらまきます。

「Black Jumbo Dog」はそういった踏み台にされないように「中継許可を与える」方法でセキュリティを確保しています。「中継許可」とは、メールの送受信に用いるコンピュータを限定し、そのコンピュータのみ許可を与えるものです。（本来、電子メールはユーザーアカウントだけで制御しており、コンピュータの制限はありません。つまり、どのコンピュータからでも、自分のメールアドレスでメール交換ができるしくみになっているのです。）

ここでは、校内のコンピュータにだけ中継許可を与え、セキュリティを保つ方法を研修します。

①(サ)「Black Jumbo Dog」を起動し、メニューバー「設定」－「メールサーバー」の順にクリックします。

②(サ)「メールサーバ設定ダイアログ」が表示されるので、「中継許可」タブをクリックして、右図の画面を表示させます。



③(サ)「名前 (表示用)」欄に、「ローカルユーザー」または「校内教職員」と記述します。

④(サ)「アドレス」欄に、校内のコンピュータに割り振られているIPアドレスを入力して「追加」ボタンをクリックします。すると、上図のように、「指定したユーザのアクセスのみを許可する」欄に追加されます。本講座では、「192.168.〇.\*」と記入します。\*はアスタリスクで、「ここに入るのは何でもいよいよ」という意味になります。IPアドレスですから、具体的には「0～255の数字の何がきても、そのIPアドレスを持っているコンピュータは許可するよ」の意味になります。

⑤(サ)設定が終了したら、「OK」ボタンをクリックします。

#### －注意－

校内～校内へのメールの宛先の書き方は、特に意識する必要はありません。通常通りアカウント@ドメイン名のように記述します（本講座の場合は、「〇〇@grp〇.ed.jp」）。校内～外部へのメールの宛先の書き方も特に意識する必要はありません。通常通りアカウント@ドメイン名のように記述します（本講座の場合は、「〇〇@grp〇.ed.jp」）。

外部～校内へのメールの宛先の書き方には決まりがあります。最初に校内メールシステムのユーザ名を[]でくくって記述し、次にインターネット転送の為に使用した（市町村やプロバイダからもらっている）メールアドレスを<>でくくって記述します。具体的には、iwa550@grp.ed.jpのメールアドレスをお持ちの先生が送信するときには、[iwa550]<iwa500@center.iwate-ed.jp>のように記述します。

先生方に使い方等を説明するとき、「<>でくくられた部分は学校代表メールアドレスです。送り先の人に対して、学校代表メールアドレスを用いている公的なものであることを明確に示すことができます。」と説明します。その上で、「私的な使用は控えてください」と話すことにより、人的セキュリティが高まります。さらに、管理職に、きちんとメール交換の履歴がサーバーに残ることも伝えておきましょう。

#### －演習－

学校（grp）単位でメール交換ができることを確かめてください（校内メールシステムの動作確認）  
学校（grp）をこえて、他の学校（grp）の人とメール交換をしてください（外部とのメール交換）  
携帯電話をお持ちの先生は、ご自分の携帯電話へメールを送信してみてください（外部とのメール交換）

## H プロキシサーバーの構築

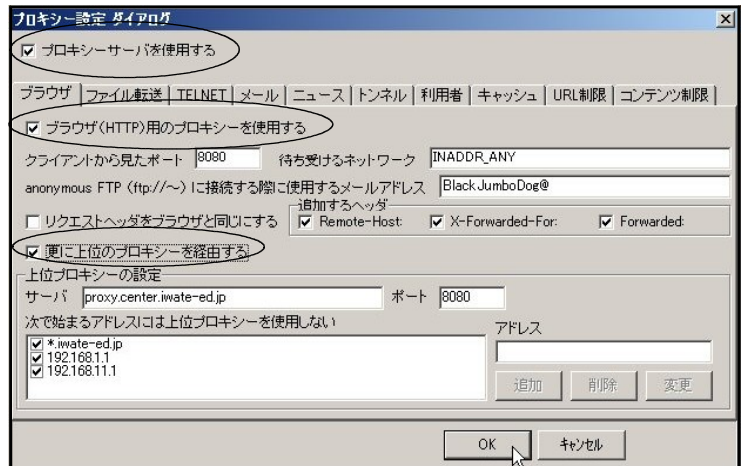
フリーソフトウェアである「Black Jumbo Dog」を利用して、プロキシサーバーを構築します。プロキシサーバーを構築すると、Webページにつながりにくい現象が改善されたり、Webページの表示も早くなったりすることがあります。また、プロキシの特性を生かして、フィルタリング機能を付加することも容易です。

### 1 HTTP用プロキシの設定

httpは、ブラウザでWebページをみるときになどに用いられているプロトコルです。つまり、Webページを閲覧するための代理サーバーにします。

①(サ)「Black Jumbo Dog」を起動し、「設定」－「プロキシサーバ」の順にクリックします。

②(サ)右図のように、「プロキシサーバを使用する」にチェックを入れ、「ブラウザ」タブをクリックします。次に、「ブラウザ(HTTP)用のプロキシを使用する」にチェックを入れ、さらに、「さらに上位のプロキシを経由する」にチェックを入れます。



③(サ)「上位プロキシの設定」の「サーバ」欄に、今まで使ってきたプロキシサーバーのアドレスを入力します。わからないときには、Webページを閲覧できるブラウザを開き、メニューバー「ツール」－「インターネットオプション」－「接続」タブ－「LANの設定」ボタンの順にクリックし、表示された「プロキシサーバー」欄を確認します。本講座では、「proxy.center.iwate-ed.jp」と入力します。ここで入力したプロキシサーバーは、教育センター内で稼働しているプロキシサーバーです。

④(サ)「上位プロキシの設定」の「ポート」欄に半角で「8080」と入力します。教育センターでは、8080ポートを使っているのがこのように設定します。

⑤(サ)「次で始まるアドレスには上位プロキシを使用しない」の「アドレス」欄に、イントラネット内各サーバーのアドレスを入力します。

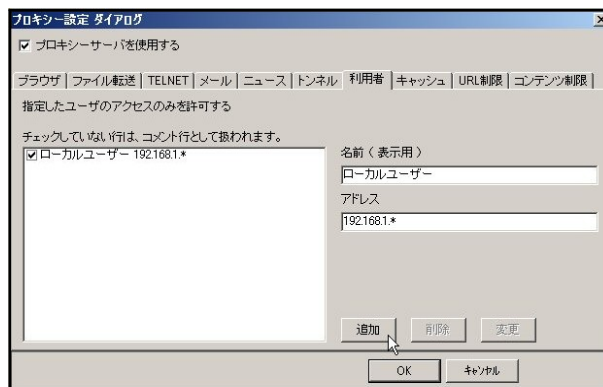
イントラネットで公開しているWebページは、イントラネット内から見に行けるので、このように設定するとWebページの表示が早くなります。この設定がされておらず、ルーターが設定されていると、イントラネット内で公開しているWebページ（グループウェアや掲示板などのWebアプリケーション）を閲覧できなくなります。

プロキシサーバーを設定すると、ブラウザを閲覧しなさいという命令は全てプロキシサーバーを経由します。その後、インターネットの世界に飛び出してから、再びイントラネット内の戻ってきます。したがって、ルーターがあると、全く表示されなくなってしまいます。

教育センターのネットワークは、「いわて教育情報ネットワーク」というイントラネット内にあります。したがって、この欄に「\*.iwate-ed.jp」を入力して、「追加」ボタンを押し、「次で始まるアドレスには上位プロキシを使用しない」に登録します。さらに、「192.168.0.1」を入力して、「次で始まるアドレスには上位プロキシを使用しない」に登録しておきます。この「192.168.0.1」は、先生方に構築していただいたドメインのルーターです。このアドレスを登録しておかないと、ブラウザアドレス欄に「192.168.0.1」と入力しても、ルーターを設定するユーティリティは起動しません。

- ⑥(サ)次に、このプロキシサーバーの利用を許可するコンピュータを設定します。「利用者」タブをクリックします。「名前 (表示用)」欄に利用を許可するユーザー名を記入します。さらに、「アドレス」欄に許可したユーザーが使用しているコンピュータのIPアドレスを入力し、「追加」ボタンをクリックします。

本講座では、右図のように、名前 (表示用) 欄に「ローカルユーザー」、「アドレス」欄に「192.168.0.\*」と入力します。



- ⑦(サ)キャッシュ関係の設定をします。「キャッシュ」タブをクリックし、「ブラウザ (HTTP) 用のキャッシュを使用する」にチェックを入れます。「サイズ (ディスク) (KByte)」の値を「50000」、「サイズ (メモリ) (KByte)」の値を「10000」、「最大サイズ (KByte)」の値を「3000」に変更します。「OK」ボタンをクリックして設定は終了です。

この値が小さいとキャッシュできる容量やデータを転送できる量が少なくなるので、数多くの人がWebページを同時に表示しようとする「遅くてつながらない」現象が発生します。プロキシサーバーを設置したことでWebページの表示が遅くなる理由は、この値が小さいことが原因です。



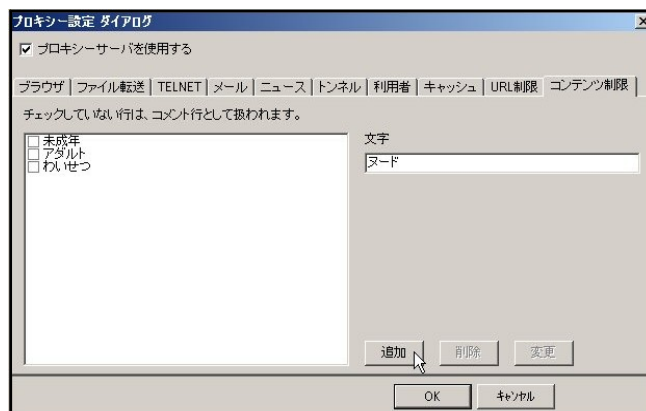
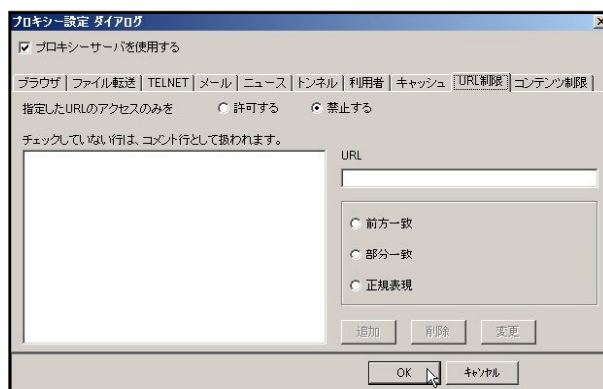
## 2 フィルタリングの設定 (セキュリティ)

プロキシサーバーのフィルタリング機能について「Black Jumbo Dog」で説明します。このフィルタリングは、2つの機能を持っています。一つはリストによるフィルタリングで、もう一つはレイティングによるフィルタリングです (I-1 参照)。

右上図は「URL制限」タブをクリックしたときのもので、リストによるフィルタリングの設定画面です。「指定したURLのアクセスのみを」の「許可する」にチェックを入れればホワイトリスト、「禁止する」にチェックを入れればブラックリストのフィルタリングとして機能します。

一方、右下図の画面は「コンテンツ制限」タブをクリックしたときのもので、レイティングによるフィルタリングの設定画面を表示したものです。「文字」欄に言葉を入力して、「追加」ボタンをクリックすると、その言葉から連想されるいっさいのWebページをRSACiの基準にあてはめて表示することを禁止します。

学校で見せたくないWebページを見つけたときには、とても有効な機能です。



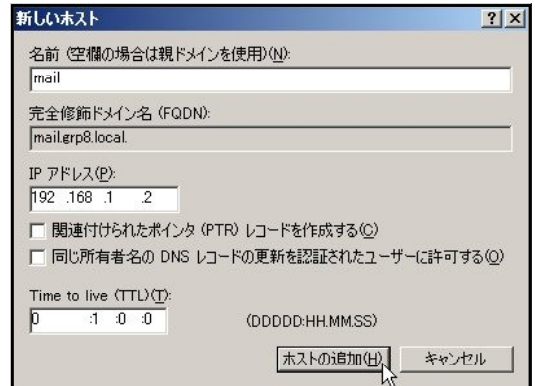
### 3 DNSサーバーへのプロキシサーバー登録

ブラウザにおけるプロキシサーバーの登録を容易にするため、プロキシに名前を付け、DNSサーバーに登録します。

- ①(サ)DNSサービスを開き、右図のように、DNSサーバーの「前方参照ゾーン」にある「ドメイン名」で右クリックし、「新しいホスト」をクリックします。



- ②(サ)右図のような画面が表示されるので、「名前」欄に「proxy」、「IPアドレス」欄に「192.168.0.2」と入力します。これにより、ブラウザにプロキシサーバーを登録する際、IPアドレスを入力することなく「コンピュータ名 (grp○sv)」または「proxy.grp○.local」、「proxy」と入力すればよいことになります。



- ③(サ)入力し終わったら、「ホストの追加」ボタンをクリックします。

- ④(サ)正しく作成された旨の画面が表示されるので、「OK」ボタンをクリックします。次に表示される画面で「完了」ボタンをクリックします。「名前」欄に「proxy」が追加されました。

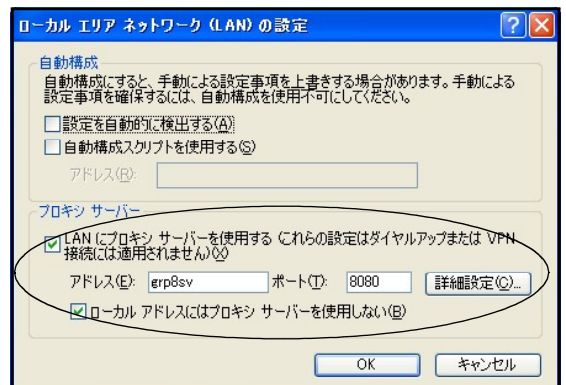
### 4 ブラウザの設定 (Microsoft Internet Explorer)

- ①(ク)ブラウザを起動します。

- ②(ク)メニューバー「ツール」－「インターネットオプション」－「接続」タブ－「LANの設定」ボタンの順にクリックします。

- ③(ク)「プロキシサーバー」欄の「LANにプロキシサーバーを使用する (これらの設定はダイアルアップまたはVPN接続には適用されません)」にチェックを入れます。

- ④(ク)「アドレス」に、プロキシサーバーのIPアドレス (192.168.0.2) か、コンピュータ名 (grp○sv) か、DNSサーバーに登録した「proxy.grp○.local」または「proxy」と入力します。さらに、「ポート」に「8080」と入力します。



- ⑤(ク)「ローカルアドレスにはプロキシサーバーを使用しない」にチェックを入れます。

- ⑥(ク)「詳細設定」ボタンをクリックすると、「プロキシの設定」ダイアログが表示されるので、「例外」欄に「\*.iwate-ed.jp;192.168.0.1」と入力します。「OK」ボタンをクリックして設定を完了します。

- ⑦(ク)ブラウザでWebページを表示させ、プロキシサーバーの動作を確認します。



## I セキュリティを高める

### 1 ブラウザでセキュリティを高める（インターネットエクスプローラーの設定）

インターネットには教育や学習に役立つ情報がたくさんある一方、子どもたちに見せるには、好ましくない情報もあります。インターネットは、現実社会のルールが適用される場ですから、違法な情報には、法律に基づいて情報発信を止めさせることができます。

しかし、インターネットにおける情報発信を子どもに適した情報だけに制限することは、言論の自由や表現の自由を侵害することになることから社会的には認められません。そこで、学校や家庭等の情報を受信する側において、情報を選択し閲覧する等の対応が求められます。

学校における「有害情報」とは、(社)日本教育工学会が「未成年の児童生徒がその情報を閲覧することで心身の健全な発達に影響を及ぼす情報、またはその可能性がある情報」と説明しています。一般的には、「性的なこと、暴力等反社会的なこと、生理的に不快感を与えること、法に触れることを載せたサイトが有害サイト」です。

学校において、不適切な情報の閲覧を防止するには、道徳的な指導をとって予防することが大切ですが、意図しない偶発的な閲覧を防止するには、フィルタリングが効果的です。フィルタリングは、あらかじめ設定した閲覧可能レベルに合った情報だけを選別する機能です。

#### (1) レイティングにより規制する方法

有害情報とは、「全ての人にとって有害なのではなく、ある年齢以下にとっては有害となる情報のこと」といった考え方があります。

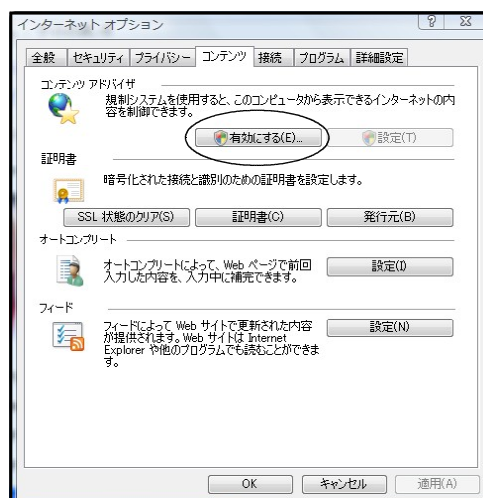
具体的には、性に関する情報は年齢の低い子供にとっては有害かもしれませんが、思春期の子供には正確な情報を与えるべき場合もあります。そこで、Webページの情報に対して児童・生徒の発達段階を考慮したレベル付け（レイティング）を行い、それを用いて有害情報を年齢に応じて段階的に排除しようというわけです。

インターネットエクスプローラー7のレイティングは、従来の4カテゴリから13カテゴリに増え、具体的に細かく設定できるようになり実用的になりました。

ここでは、ブラウザの設定でフィルタリングを行う方法を説明します。

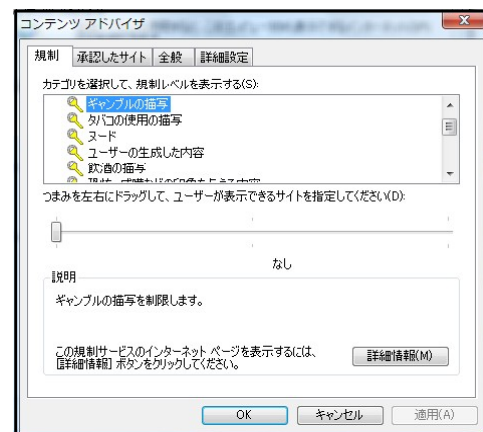
①(ク)インターネットエクスプローラーのメニューバーから「ツール」－「インターネット オプション」の順に選択します。表示される「インターネットオプション」のダイアログから「コンテンツ」のタブを選択します。

右図の画面が表示されるので、[コンテンツ アドバイザ]にある[有効にする]ボタンを選択します。



②(ク)右図の設定画面が表示されるので、アクセスを規制するカテゴリをクリックで選択し、中央のスライダーを動かして表示できるサイトのレベルを指定します。最後に「適用」ボタンを選択します。

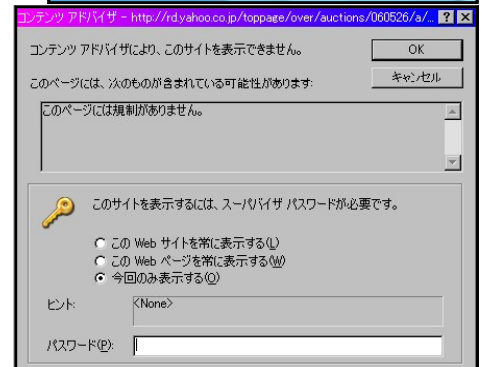
この設定によって、有害情報へアクセスする場合には、パスワードの入力が求められるようになります。



- ③(ク)「全般」のタブを選択すると右図画面が表示されるので、「スーパーバイザ パスワード」欄の「パスワードの作成」を選択して設定します。



- ④(ク)ページを表示させようとする時、左図のようにパスワードの入力ダイアログが表示されます。パスワードを入力しないとページが表示されません。

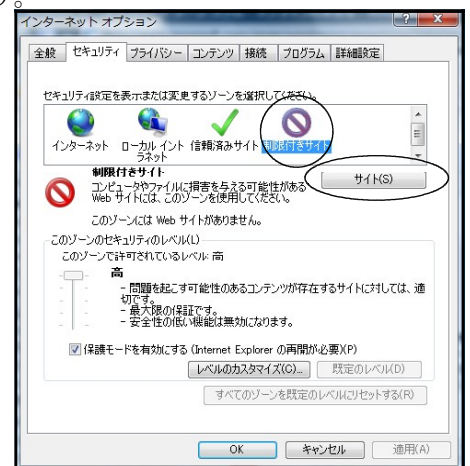


## (2) リストにより規制する方法

リストによる規制する方式には、「ブラックリスト方式」(制限付きサイト)と「ホワイトリスト方式」(信頼済みサイト)があります。「ブラックリスト方式」は、見せたくないページをあらかじめブラックリストとして登録しておき、リストに記載されたURLへのアクセスだけを禁止します。「ホワイトリスト方式」は、推奨するページをあらかじめ登録しておきリストに記載されたURLへのアクセスだけを許可するものです。これらの方式の場合、リストに記載された一つ一つのURLに制限をかけるため多くの労力が必要となります。

インターネットエクスプローラーには、ブラックリスト方式のフィルタリングが実装されています。それでは、実際にフィルタリングを有効にしてみましょう。

- ①(ク)インターネットエクスプローラーのメニューバーから「ツール」－「インターネットオプション」を選択します。「セキュリティ」タブを選択し、「制限付きサイト」－「サイト」を選択します。



- ② 制限付きサイトを登録するダイアログが表示されます。ここにURLを入力して「追加」ボタンを押すと、見せたくないページ登録がされます。



もっと厳密に、より確実に有害情報から守るためには、市販されている専用のソフトウェアを利用

するのがよいでしょう。あるフィルタリングソフトは、50台1年間利用で約30万円でした。このソフトは新しいサイトを毎日検索して有害サイトをリストにして契約者に配布します。ソフトで制限をかけるので更新が必要になりますがインターネットの速度は落ちません。また、全県立学校が加入している「いわて教育情報ネットワーク」に加入するとチャットを含めたフィルタリングが働きます（加入は市町村教育委員会単位なので学校独自に加入できません）。

フィルタリングソフトを購入することが困難である場合、フリーソフトとして財団法人インターネット協会のレイティング／フィルタリング連絡協議会 (<http://iajapan.org/rating/>) のサービスを利用することができます。利用するためには、協会に申し込みをする必要があります。無料で提供されているのはJava環境で作動するプロキシサーバタイプのフィルタリングソフトです。プロキシサーバとしてインストールしたあとに、ブラウザのプロキシ設定を変更する必要があります。構築のための手順が掲載されています。

フィルタリングの基準は、人によって判断が異なりますが、日本は「暴力」や「ヌード」を児童生徒に見せることについて欧米や韓国よりも寛容すぎるので、一度学校現場で話し合ってみることも良いでしょう。また、フィルタリング機能を使ったからといって、100%安全というわけではないので、児童生徒がどんなページを見ているのか常に注意をして見る必要があります。



※児童生徒がブラウザを使って調べ学習を行う際、子ども向けの検索エンジンを利用することも有害情報から守る方法の一つです。（ただし、検索数は少なくなります。）



「Yahoo!きっず」 (<http://kids.yahoo.co.jp/>)



「キッズgoo」 (<http://kids.goo.ne.jp/>)

## 2 ルーターでセキュリティを高める

ルーターは、別々のネットワークを相互に接続できる機器であり、他のネットワークとの接続窓口になっていると述べました。しかし、ルーターの機能は数多く、この機能を活かすことにより、セキュリティ面を強化することもできます。

### (1) 設置するだけでセキュリティ向上

ルーターには、WAN側のIPアドレスとLAN側のIPアドレスを設定する必要があります。LANの内側にあるコンピュータからは、インターネットのような広大なネットワークに接続することも可能ですし、WAN側にあるコンピュータの共有フォルダを利用することもできます。では、WAN側からLANの内側を見ることはできるのでしょうか？答えはNOです。ルーターの外側にあるコンピュータからはルーターしか見えません。LANの内側にあるコンピュータをブラウジングすることさえできないのです。極端に言うと、LANの内側に何台のコンピュータがあり、どんな共有フォルダがあるかといったことは全くわかりません。

このことを校内ネットワークや職員室LANに応用します。職員室LANを組むと、共有フォ

ルダに様々なファイルが保存されます。校内ネットワークが既に組まれている学校の中には、「教師がつくったファイルが児童生徒に丸見え」といった問題がおきているところがあります。こういった問題は、職員室LANの出口、つまり、校内ネットワークとの接続点にルーターを1台設置するだけで解決できます。

## (2) フィルタリング機能

最近のルーターには、フィルタリング機能が内蔵されてきました。特定の packets をフィルタリングしたり（右図）、特定のプロトコルをフィルタリングしたりする機能です。

例えば、Webページを閲覧するときに用いるプロトコルはHTTP、ファイル転送のときに用いるプロトコルはFTPというように決められていて、ルーターはプロトコルの種類で適切にデータをやりとりします。

児童生徒にWebページの閲覧はさせるがメールは使わせないとか、ファイル転送はダメといった場合にはそのプロトコルをブロックすることができます。

## (3) ファイアウォール機能

ファイアウォールとは、fireWall、つまり防火壁のことです。ネットワークへ外部から侵入されるのを防ぐシステムのことを言います。

インターネット等、外部のネットワークには、ハッキング等の悪意ある行動をとる人もいます。相手のパソコンやルータなどに不正なデータを送信して使用不能に陥らせたり、トラフィックを増大させて相手のネットワークを麻痺させようとするわけです。

こういった様々な外部からの攻撃からネットワークを守る機能です。

## 3 マルウェア対策

マルウェア対策は必須です。インターネットに接続するのであれば、マルウェア対策ソフトをインストールするのは常識です。県立学校や一部の市町村では、ネットワーク上でのウイルスやスパイウェアの感染及び蔓延を防ぐため、サーバクライアント型マルウェア対策ソフトがインストールされています。ネットワーク管理者や情報教育担当の指示に従い、パターンファイルを常にアップデートできるように設定しておくことが大切です。また、そのような処置がなされていない場合には、必ず、先生方のコンピュータ1台1台にインストールしてもらいます。ベストはやはり市販品で、パターンファイルのアップデートが頻繁に行われています。実習では、「Kingsoft InternetSecurity2007Free (Kingsoft社)」について紹介します。

### (1) ダウンロード

- ① アドレス<<http://download.kingsoft.jp/kisfree/>>を表示し、「今すぐダウンロードボタン」をクリックします。
- ② 表示された画面で「保存」ボタンをクリックし、デスクトップ等任意のフォルダに保存します。

### (2) インストール

- ① ダウンロードしたファイル「kisfree\_24.exe」をダブルクリックします。
- ② 右図の画面が開くので、「次へ」ボタンをクリックします。





③ 右図の画面が開くので、「無料版を使用する」にチェックを入れ、「次へ」ボタンをクリックします。



④ 「使用許諾契約」の画面が開くので、同意するときには「同意する」ボタンをクリックします。

⑤ 「情報収集ポリシー」の画面が開くので、同意するときには「同意する」ボタンをクリックします。

⑥ 右図の画面が開くので、「標準」にチェックを入れ、「次へ」ボタンをクリックします。

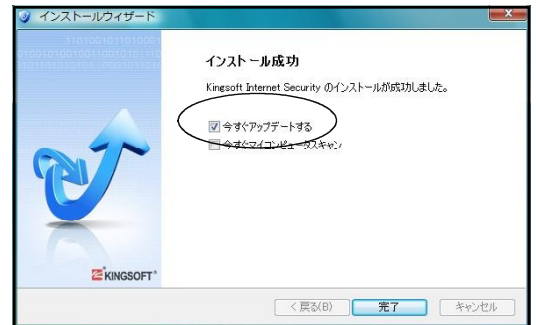


⑦ 「ファイルのコピー開始」画面が表示されるので、「次へ」ボタンをクリックします。

⑧ 「ファイルコピー完成」画面が表示され、インストールウィザードに入る旨表示されるので、「次へ」ボタンをクリックします。

⑨ 「ようこそKingsoft Internet Securityインストールウィザードへ」画面が開くので、「デフォルト設定」にチェックを入れ、「次へ」ボタンをクリックします。

⑩ しばらくすると、右図の画面が表示されるので「今すぐアップデートする」にチェックを入れ、「完了」ボタンをクリックします。



⑪ 右図の画面が表示されるので、「カスタムアップデート」にチェックを入れ、「次へ」ボタンをクリックします。



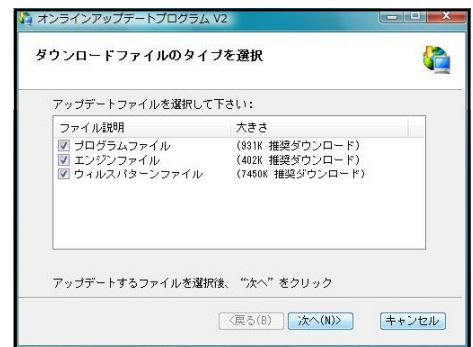
⑫ 右図の画面が表示されるので、「インターネット経由」にチェックを入れ、「プロキシ」ボタンをクリックします。



- ⑬ 右図の画面が表示されるので、「Internet Explorerのプロキシ設定を使用する」にチェックを入れ、「OK」ボタンをクリックします。



- ⑭ Kingsoftのサイトにアクセスできると、右図の画面が表示されるので、そのまま「次へ」ボタンをクリックします。



- ⑮ アップデートが完了すると、右図の画面が表示されるので、「完了」ボタンをクリックします。これで、インストールは完了しました。



### (3) 画面構成

ここを選択して、手動でアップデートを実行

ウイルス対策

スパイウェア対策

ファイヤーウォール

アンチスパム  
スパムメール駆除

セキュリティ分析  
脆弱性の発見

岩手県立総合教育センター  
情報教育担当

平成20年7月1日発行

このテキストを執筆するにあたり、多大なるご協力を  
いただいた（株）NTT東日本様に深く感謝申し上げます