

ワークグループによる 小規模LANの構築

< 理論編 >

岩手県立総合教育センター

目 次

I 解説編

1	ネットワークの概要	1
2	有線LANの構築に必要な機器	1
3	無線LANの構築に必要な機器	2
4	インターネット接続に必要な機器	3
5	LANの基礎知識	3
6	職員室LANの有用性	7
7	職員室LANの構築手順	8
8	職員室LAN構築の留意点ーセキュリティー	13

I 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利用できます。

LAN（ラン、「Local Area Network（ローカルエリアネットワーク）」の略称）とは、学校内や家庭内等物理的に限定された場所のネットワークのことをいいます。LANは、Ethernet（イーサネット）と呼ばれる方式によって構築されることがほとんどです。Ethernetは、コンピュータを接続するケーブルの形状や特性、通信における電気信号の形式、通信方法などが定められています。

LANは、物理的にどのように接続するかで有線LANと無線LANに分類されます。無線LANは、ケーブルを配線する必要がないので、配置換えが多い場所やケーブル配線が煩雑な場所では便利ですが、通信速度が距離や障害物など周囲の環境に左右されるほか、通信内容の盗聴の危険性によるセキュリティ対策をしっかりとる必要があります。

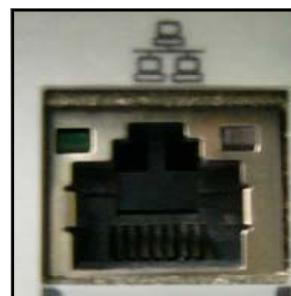
2 有線LANの構築に必要な機器

(略)

(1) NIC

NIC（ニック）とは、「Network Interface Card（ネットワークインターフェースカード）」の略称です。ネットワークカード、LANアダプタ、LANカード、LANボードと呼ぶ場合もありますが、全て同じ意味です。NICはネットワークケーブルを介してコンピュータをLANに接続する機器で、コンピュータに直接取り付けて利用します。

市販されているコンピュータのほとんどはNICを内蔵していますが、内蔵されているかどうかを調べるためには、コンピュータの側面あるいは背面に右図のようなマークやポートがあるかどうか確かめます。コンピュータにNICが内蔵されていない場合は、新たにNICを購入してコンピュータに取り付けます。デスクトップコンピュータ用、ノートコンピュータ用、USB接続型が市販されています。



NICの種類	価格帯
デスクトップPC用	800円～3,980円
ノートPC用	1,200円～5,040円
USB接続型	1,980円～5,750円

(2) ネットワークケーブル（LANケーブル）

現在、県内の学校で主流となっているネットワークケーブルは、通信速度が10Mbpsの10BASE-T、100Mbpsの100BASE-TXのタイプです。bps（ビーピーエス、「bit per second（ビットパーセカンド）」の略称）はデータの転送速度で、1秒で転送できるデータ量を表しています。10Mbpsとは、1秒で10M（メガ）ビット＝10,000,000ビットの情報を伝送できることを意味しますが、実際にはこの速度で通信することはできず、あくまで理論値です。ネットワークケーブルのことをLANケーブルともいいます。最近では1G（ギガ）bpsで通信できる



ギガビットイーサも普及してきました。ケーブルには、**ストレートケーブル**と**クロスケーブル**がありますが、**ハブやルーターを経由させる場合はストレートケーブル**を使い、2台のコンピュータを直接接続する場合はクロスケーブルを使います。

	1 m	2 m	3 m	5 m	10m
ストレートケーブル価格	約100円～	約200円～	約300円～	約500円～	約700円～

※100円ショップでも売っています

(3) ハブ

ハブとは、コンピュータに接続したネットワークケーブルを集線する（とりまとめる）装置です。

学校では、**リピータハブ**と**スイッチングハブ**が使われていますが、最近の主流はスイッチングハブです。スイッチングハブは効率よく通信するように工夫されており、ポート数（ネットワークケーブルを差し込む穴の数）には、5、8、12、16、24ポート等があります。リピータハブは、10BASE-Tでは4台までつなげて使用できますが、100BASE-TXでは2台までです。また、リピータハブとコンピュータの距離は100m以内にならなければならない制限があります。しかし、スイッチングハブは、基本的に何台つなげてでも大丈夫です。また、ハブとコンピュータの距離については特に制限はありません。

職員室にLANを構築する際には、「教職員数分+プリンタ台数分+α」のポート数が必要となります。先生方の机が並んでいる各しに8ポートもしくは16ポートスイッチングハブを1台（もしくは5ポートのスイッチングハブを数台）設置し、それらのハブをさらに集線するスイッチングハブを1台用意するのが一般的です。

職員室にLANを構築する際には、「教職員数分+プリンタ台数分+α」のポート数が必要となります。先生方の机が並んでいる各しに8ポートもしくは16ポートスイッチングハブを1台（もしくは5ポートのスイッチングハブを数台）設置し、それらのハブをさらに集線するスイッチングハブを1台用意するのが一般的です。



	5ポート	8ポート	16ポート	24ポート
スイッチングハブ	約950～7,000円	約1,500～11,000円	約4,500～50,000円	約13,000～90,000円

3 無線LANの構築に必要な機器

(略)

(1) 無線LANアダプタ

無線LANアダプタもNICの1種ですが、ここではわかりやすく区別するために「無線LANアダプタ」と呼ぶことにします。無線LANアダプタにも、デスクトップコンピュータ用、ノートコンピュータ用、USB接続型があります。無線LANアダプタは、NICの1種ですからコンピュータに直接取り付けて利用します。無線LANアダプタ内蔵のコンピュータも市販されています。Vista対応パソコンに内蔵してある無線LANアダプタは安定しておりお勧めです。規格には、「IEEE802.11a」、「IEEE802.11g」、「IEEE802.11b」の3種類があります（略して11a、11g、11bと呼ぶ）。市販されているものは、11a・11g・11bの3規格対応か、11g・11bの2規格対応かの2タイプが多いようです。11a・11gは54Mbpsで通信できるので高速です。規格が異なるとLANに接続することができないので、無線LANアダプタを購入する際には、使用するアクセスポイント（後述）の規格と合わせる必要があります。

デスクトップPC用 ノートPC用 USB接続型



	価格帯
デスクトップPC用	3,500円～9,500円
ノートPC用	2,800円～15,000円
USB接続型	3,700円～18,000円

(2) アクセスポイント

アクセスポイントとは、コンピュータを無線LANで接続するための中継機のことです。無線LANアダプタから送信された電波をアクセスポイントが受信することでネットワークにつながる仕組みになっています。無線LANではコンピュータ同士が直接通信するアドホックモードと、アクセスポイントの中継して通信するインフラストラクチャモードがあります。アドホックモードは無線LANアダプタだけあればいいので便利なのですが、同時に3台以上のコンピュータと通信できないなどの制限があることから、学校現場で使われることは滅多にありません。アクセスポイントを用意して快適に通信できる環境を整えます。

アクセスポイントにはブリッジタイプとルータタイプの2種類があります。ブリッジタイプは単純にデータの中継を行なう機器なので、有線LANのハブに近いものと考えてください。ルータタイプはインターネットと職員室LANといった異なるネットワークの仲立ちに使います。職員室だけでLANを組むといっても、校内LANやインターネットといった他のネットワークと接続することがほとんどなので、ルータタイプのアクセスポイントを購入するか、ブリッジタイプのアクセスポイントとルータ（後述）の二つを購入してネットワークに接続します。（本実習では、ルータタイプアクセスポイントを使います）

学校において無線LANを構築するための機器を購入する際には、いくつか注意が必要です。無線LANアダプタと同様に、「11a」、「11b」、「11g」の通信方式の違いによる対応・非対応があります。お勧めは11a、11g、11b全てに対応したルータタイプアクセスポイントの購入です。

アクセスポイント (BBR含む)



価格帯	約7,000～80,000円
-----	----------------

4 インターネット接続に必要な機器

1台のコンピュータをインターネットに接続する場合には、モデムやターミナルアダプタ (TA) といった機器が必要ですが、さらに、LANでは複数台のコンピュータをインターネットに接続する必要があります。その場合、学校においては**ルーター**という機器を用いると便利です。ルーターは、異なるネットワーク間を接続するための機器です。ルーターには、通信経路が記されており、目的のネットワークに正しく中継する機能を持っています。また、インターネット接続用に配布されている一つのIPアドレスを、学校にあるコンピュータ台数分のIPアドレスに置き換える機能を持っています。職員室のLAN程度であれば、安価なルータで充分です。

ルーターは、インターネット接続以外にも、LAN内のコンピュータの台数がとても多くなり、通信が遅くなるときに、ネットワークの混雑を解消する目的で導入することがあります。

また、セキュリティを高める目的で導入されることがあります。外部のネットワークから、ルーターを設置しているLANの中のコンピュータを見ることができないしくみになっています。職員室にLANを構築する際、このルーターを設置することにより、児童生徒用コンピュータから教員のコンピュータやデータを見ることを防ぐことができるようになります（DNZ機能、静的マスカレード設定、ポートフォワーディング設定等オフの場合）。さらに、フィルタリングといった機能も併せ持っていますので、学校のネットワークには必需品と言えましょう。

縦置きタイプ



横置きタイプ



価格帯	約3,000～50,000円
-----	----------------

5 LANの基礎知識

(1) 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、コンピュータには名前がつけます。よく聞く名前はサーバとかクライアントと言った名前です。サーバとは、LANなどのネットワークを通じて、特定のサービス（ファイル提供サービス、プリンタ提供サービスなど）を行うコンピュータのことです。また、クライアントとは、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。あるときはサーバとして機能しているコンピ

ユーザが、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とクライアントの両方の機能を持つような、対等に接続される形態を**ピア・ツー・ピア型**といいます。これに対して、サーバ専用のコンピュータが設置され、クライアントとサーバが明確に区別される接続形態を**サーバクライアント型**といいます。



最近の学校でもサーバクライアント型による接続形態が増えてきており、専用サーバが設置されることが多くなってきました。サーバ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。サーバには、プリンタの機能を提供するプリントサーバ、共有ファイルを提供するファイルサーバ、データベースシステムによるデータベースサーバ等があります。サーバには専用のサーバOS（オペレーティングシステム）を導入します（後述）。

サーバクライアント型ネットワークを構築・管理・運用するためには、ネットワークに関する高度な知識が必要です。そして、ピア・ツー・ピア型ネットワークの考え方や構築方法が全てのネットワークの基礎となります。本講座では、ピア・ツー・ピア型ネットワークを取り入れ、基礎的な構築方法をマスターできるよう計画しています。

(2) 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れば増えるほど、それぞれのコンピュータやネットワークの管理がたいへんになってきます。そこで、コンピュータをある単位でまとめて、グループにして管理します。これを、Windowsでは「ワークグループ」と呼んでいます。「ワークグループ」は、ピア・ツー・ピア型ネットワークでよく利用される考え方です。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（例えばコンピュータ室のコンピュータ）のグループといったようにまとめます。そうすることにより、管理するときにはワークグループ毎に行えばよいことになります。

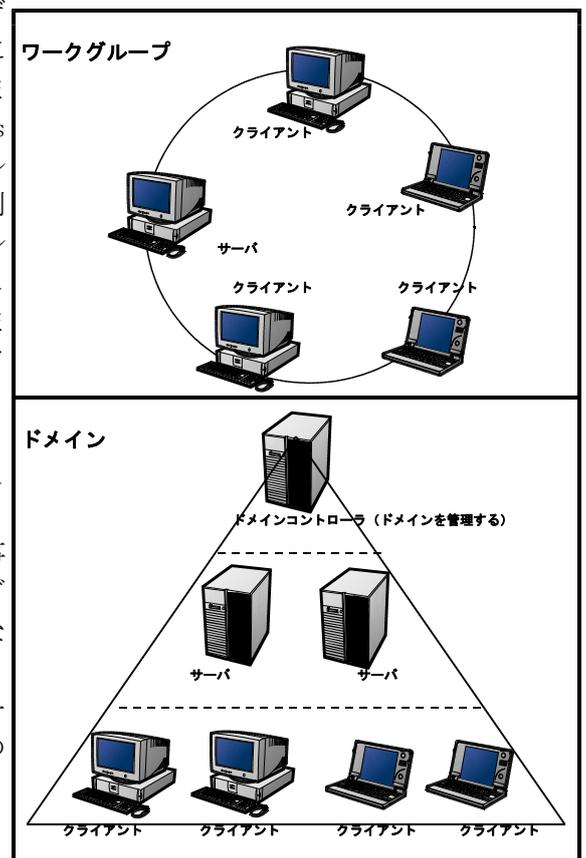
しかし、このワークグループの数が増えてくると、もはやそれぞれのワークグループに所属するコンピュータを管理すること自体がたいへんになってきます。学校で言えば、例えば、3月から4月にかけては人事異動や卒業入学の時期でもあり、それぞれのワークグループに所属する全てのコンピュータの設定を変えなければなりません。

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」とは、ドメインコントローラを頂点としてサブドメインを階層化して管理するといった構造的な特徴があります。

こうした大規模なネットワークでも管理できるようにしたものが「ドメイン」なのです。

各サーバやクライアントは、ドメインに参加することでドメインの一員と見なされ管理されることになります。逆にドメイン管理できれば、サーバ1台でほとんど全てのコンピュータやユーザの設定管理運用ができることになります。

ワークグループはネットワークに関する高度な知識や技術がなくても構築でき、ネットワークに関する全てのスキルが網羅されている管理方法です。一方、ドメインはまとめて集中管理できるものの高度な知識と技術が必要となります。本講座の実習では、ワークグループの考え方を取り入れ、基礎的な構築方法を完全にマスターできるよう計画しています。



(3) 対応するOS

ア ワークグループ管理

Windows95、98、98SE、Me、NT4.0WS、2000、XPHome、XPPro、Vista(全バージョン)は、クライアントとしてもサーバとしても利用することが可能です。サーバ専用OSである「WindowsServer2008」「WindowsServer2003」「Windows2000Server」「WindowsNT4.0server」はサーバとして利用できます。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としても接続することができます。OS9以下をWindowsネットワークに容易に接続するためには、「DAVE」(右図)と呼ばれる専用ソフトウェアを購入する必要があります。



イ ドメイン管理

ドメイン管理できるOSは、サーバ専用のOS(サーバOS)です。Windowsには「Server2008」「Server2003」「2000Server」「NT4.0server」、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)OSは、Windows95、98、98SE、Me、NT4.0WS、2000、XPPro、VistaBusiness、VistaEnterprise、VistaUltimateがあります。ただし、Windows95、98、98SE、Meをドメイン管理するには、高度なネットワーク技術が必要です。ドメイン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、高度な知識がなくても95、98、98SE、Me、MacOSXで可能です。**XPHome、VistaHomeをドメイン管理することはできません。逆に言えば、ドメイン管理されているネットワークに接続することは不可能です。**

(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。現在学校で構築されるネットワーク(職員室LANを含む)のプロトコル群もこのTCP/IPが主流です。(他にはNetBEUI等が用いられています。)

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)、POP(メール受信用)、TELNET(電話回線との通信用)等があります。コンピュータが物理的にLANにつながっているように見えても、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、ネットワークに接続するNICには全てこのMACアドレスが割り振られています。NICに割り振られる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、様々な機器(例えば、無線LANアダプタやプリンタサーバ等)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。最近では、セキュリティ上の観点からNIC本体に記載しないことが多くなってきています。

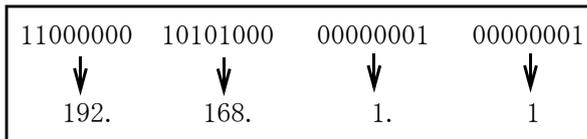
(6) コンピュータ名(ホスト名)

LANに接続されたコンピュータは、コンピュータ名で識別されます。コンピュータ名は、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。一般的にネットワークの世界では、「ホスト名」の言い方をします。「コンピュータ名」はWindows独特の言い方で、「ホスト名」と同じ意味です。

(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。この情報のやりとりのことを通信と言います。通信するとき、相手のコンピュータを探す際に必要なものがIPアドレスです。言い換えれば、私たち人間社会の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。これは、8ビットずつ区切った32ビットの数値で形成されていますが、実際に表記する場合は、人間にわかりやすいようにそれぞれの8ビットを0～255までの10進数に変換して、ピリオドで区切って表記しています。



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」が行っており、ここに申請を行い使用します。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ビットのアドレスが使われる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**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ります。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。これは、ローカルアドレスともいわれるもので、校内のネットワーク管理者が自由に利用できるアドレスです。

※クラスは、Aにいくほど上位に位置付けられる

	プライベートIPアドレス	アドレス数
クラスA	10. 0. 0. 0～10. 255. 255. 255	16, 777, 216
クラスB	172. 16. 0. 0～172. 31. 255. 255	65, 536
クラスC	192. 168. 0. 0～192. 168. 255. 255	256

職員室LANをインターネットに接続するときはルーターを用いると良いことを説明しました。ルーターは1個のグローバルIPアドレスを複数のプライベートIPアドレスに変換してくれるため、どのコンピュータからでも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。これをNAT機能といいます。

例えば、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、複数のプライベートIPアドレスに変換してくれるのです。この方法を用いることにより、IPアドレスが有効利用でき、ルーターを境に外部からLAN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。

(8) サブネットマスク

IPアドレスに対応させて4つの数字で接続できるコンピュータ数を決めるものです。具体的には、「255. 255. 255. 0」と設定した場合です。「0」と指定すると理論上254台接続できるようになります。「255」と指定すると1台も接続できません。つまり、「255」と指定してやると、その部分は「マスク」がかかり、ネットワークに接続させないようにできるのです。「255. 255. 0. 0」と設定すれば254×254=64516台接続できます。「255. 255. 255. 200」と設定すれば54台まで接続できます。IPアドレス「192. 168. 1. 0～192. 168. 1. 255」(254台分)と考えても、サブネットマスクを「255. 255. 255. 200」としてしまえば、「192. 168. 1. 0～192. 168. 1. 255」のIPアドレス範囲内で54台までしか接続できません。このことにより、空いているIPアドレスの不正使用を防ぎます。

(9) 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。

(10) 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。

最近では、IPマスカレードの機能を含めてNATと呼ぶ場合があります。これらの機能は、ルータやプロキシサーバーソフトウェア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。

(11) 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「192.168.1.〇」を使って、児童生徒用は「192.168.2.〇」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。

(12) ユーザIDとパスワード

ネットワークの構築ではコンピュータ等機械ばかりではなく、人のことも考える必要があります。ネットワークに接続されたコンピュータは「誰が使ってよいのか」という許可です。ユーザ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情報と言い、ユーザ情報を管理することをユーザ管理と言います。

コンピュータにユーザIDとパスワードが設定されることにより、ネットワークが使えるばかりでなく、コンピュータそのものを使うことができるようになります。コンピュータにユーザIDやパスワードが設定されていないと、ネットワークも使えない、コンピュータも使えないこととなります。

6 職員室LANの有用性

平成17年7月に文部科学省より「校内ネットワーク活用ガイドブック2005」が発行されました。

■校内ネットワークを活用しよう

http://www.mext.go.jp/a_menu/shotou/zyouhou/kounai/index.html

■校内ネットワーク活用ガイドブック

<http://www.japet.or.jp/handlers/getfile.cfm/4,158,116,32,pdf>

① 校務文書の共有化により校務の効率化を図る

定型の校務文書、例えば、復命書や動静表、各種申請書の様式を共有フォルダに保存しておくことにより、LANに接続できる先生はいつでも取り出して作成することができます。作成し終えた文書も専用の共有フォルダをつくり、そこに保存するようになれば、管理職が一度に閲覧することが可能になります。具体的な例としては、長期休業前に教頭先生が動静表の枠を共有フォルダに保存し、各先生がそこに入力、教頭先生は印刷して配布する等です。

② 学習教材の共有化により授業準備の効率化を図る

授業のために作成した評価規準表や学習指導案、学習プリント、問題プリント等を共有フォルダに保存しておくことにより、LANに接続できる先生はいつでも取り出して利用することができます。授業で用いた有効なコンピュータ教材を保存しておき、みんなで利用している学校もあります。

コンピュータ室等で見せたい教材も、職員室から保存できるようになります。いちいち、コンピュータ室まで行く必要がなくなることは大きな魅力です。

③ 教育情報の入手が容易になる

職員室LANをインターネットに接続できる環境を整えれば、先生型の机上にあるコンピュータからインターネットに常に接続できるようになります。

文部科学省や県教育委員会、教育事務所、教育センターから最新の情報を入手することが可能になります。授業に必要な学習指導案や児童生徒に見せたい写真や映像もインターネットで検索して入手することが可能になります。

④ 省資源・省エネルギーにつながる

大きな効果はペーパーレスとしてあらわれます。紙に印刷して配布していたものが一気に少なくなるからです。また、共有プリンタを準備するだけでも、先生方が単独で多くのプリンタを用意しているときと比べて15%以上の電気代節約になった例もあります。

7 職員室LANの構築手順

(1) 構築前の準備

ア 接続形態や管理方法

まず、職員室にLANを構築することについて上司と必ず相談しましょう。

さて、構築の言葉には、何もないところから作り始めるといった意味があります。初めて構築するので、高度な知識や技術を必要としない形態や管理方法をできるだけ選択すべきです。そして、身に付けていったスキルに応じて、ネットワークを使いやすいものにつくりかえていくことです。初めから高度なネットワークを形成してしまうと、その後の維持ができなかったり、トラブルに対処できなかったり、次に引き継いだ先生が管理できなかったりします。「小さく産んで大きく育てる」がネットワーク構築の基本です。

初めての構築であれば、**ワークグループで管理できるピア・ツー・ピア型ネットワーク**にすることをお勧めします。作成した文書等を共有できるようにコンピュータを接続して専用のファイルサーバとします。そのコンピュータにさらにプリンタを接続して、プリンタサーバとしても機能させます。ピア・ツー・ピア型ネットワークなので、用意するコンピュータは新しいコンピュータである必要はありませんし、高価なサーバOSを用意する必要もありません。既に職員室にあるコンピュータやハードディスクに容量があればWindows95等のコンピュータでも充分です。

ピア・ツー・ピア型ネットワークやワークグループ管理はネットワーク構築の基本中の基本です。これが理解できなければ、とうていサーバクライアント型のネットワークは構築できませんし、ドメイン管理も理解できないばかりか、無線LANの考え方も理解できません。ネットワークトラブル解決の基本手順も、全てこの中に含まれています。

先生方の中ですでに職員室LANが構築されている学校に勤務されているのであれば、ぜひこの機会にピア・ツー・ピア型ネットワークのしくみやワークグループ管理といったネットワークの基本をマスターしてください。

イ 配置図の作成

職員室の配置図をつくりましょう。机、コンピュータ、ハブ、プリンタの配置図と考えてください。本講座で使用しているネットワーク研修室の図が一例です。

このような簡単な図を作成するだけでも、何ポートのハブが何個必要か、ネットワークケーブルは何mのものが何本必要かといった必要となる物品をリストアップすることができます。

各GROUPに6台のコンピュータがありますので、とりあえず8ポートハブが1個となります。室全体を考えると6個ということになります。

ネットワークケーブルは、各コンピュータに1本必要です。コンピュータは全部で26台ありますから26本。各機のハブから一つに集線するために4本、集線したハブからインターネットにつなげるためにさらに1本。合計31本になります。

ウ 必要物品の入手

配置図を作成しながらリストアップした物品を一覧表に書き表すことにより、予算等のおおよその目安を付けます。下記に例を示します。ただし、NIC及びウイルス対策等のソフトはコンピュータに内蔵されているか、教職員個人で購入するものと仮定しています。

必要物品	単価	個数	総額	備考
8ポートスイッチングハブ	3,000	6	18,000	
1mネットワークケーブル	105	24	2,520	各GROUPコンピュータ用

3 mネットワークケーブル	315	2	630	サーバ用
10mネットワークケーブル	735	6	4,410	各机集線用等
			25,560	

ネットワークケーブルを天井からぶら下げたり、床に這わせたりと言ったことを考えれば、ケーブルカバーといった物品も必要になってくるかと思いますが、それらを見積もらなければ、3万円位で構築できます。安価になるのは、工事費等一切かかっていないことも要因です。構築開始までに必要物品を入手します。無線LANで構築する場合にはケーブルやハブは必要ないのでもっと安価になります。

エ ユーザIDとパスワードの作成

アクセスできるユーザは、所属校の教職員に限定されます。先生1人に対して、ユーザIDとそれに対応したパスワードを決めて配布します。構築者が決めても結構ですし、一人一人に申請してもらっても結構です。作成したら一覧表にして金庫等に保管します。個人へは紙に書き、封筒に入れて、直接本人に手渡します。管理者と本人以外は絶対にわからないようにすることが重要です。

ーユーザIDー

小文字半角英数字を使います。最初の一字は必ずアルファベットにします。文字数は4文字以上とし、あまり多い文字数はユーザから嫌われます。既に決められているものがあればそれと同じものを利用しましょう。初めてならば、ユーザにとってわかりやすい（忘れにくい）IDにしましょう。県立学校は氏名を利用したIDになっています。小中学校の場合には、先生方の転勤等もあることから「teacher01～teacher50」といった連番にすると便利です。新しく赴任した先生には、転出した先生のIDを割り振るという方法です。サーバに新たなユーザ登録をする必要がなくなります。

ーパスワードー

大文字小文字をとりまぜた半角英数字の組み合わせです。8文字以上がベストです。

例)「Jb03ty67」「az3067KL」・・・

オ コンピュータ名及びIPアドレスの作成

アクセスできるコンピュータを限定します。コンピュータ名とIPアドレスを決めて設定します

ーコンピュータ名ー

管理する人にわかりやすい名前が結構です。例) 銀河中学校:「gintyu01」「gintyu02」・・・

ーIPアドレスー

「職員室に既にLANが組まれている」場合には、使えるIPアドレスは既に決まっていますので、ネットワーク管理者（小中学校の場合は情報教育担当等）に聞きましょう。わからない場合には、業者が設定したネットワークで市町村が管理しています。勝手にIPアドレスを割り振ると不正アクセスと見なされ罰せられる対象となりますので、市町村に相談する必要があります。

「職員室LANを初めて構築する」場合にはクラスCのプライベートIPアドレスを使います。ただし、コンピュータ室にLANが組まれている場合には、クラスCのプライベートIPアドレスを既に使っている可能性がありますので、IPアドレスが重複しないように設定します。

例) 192.168.1.0～192.168.1.255

静的（固定）IPアドレスで管理することをお勧めします。高度なスキルがないのに動的IPアドレスを導入することはセキュリティ上危険ですし、許可していない市町村も多いのです。

(2) 構築の実際

構築の手順を以下に示します。（詳しくは操作編で・・・本講座の実習はこの手順に従って進めていきます。）



ここまでがLANの構築になります(本講座1日目)

エ ファイルの共有	①共有フォルダの作成・隠しフォルダの作成 ②ユーザの作成・アクセス権の設定
-----------	--

オ プリンタの共有	①ローカルプリンタの共有 ②プリンタサーバを利用した共有 ③ネットワークプリンタの共有
-----------	---



ここまでがサーバの構築になります(本講座1日目)

カ ネットワークを発展させる	①インターネットへの接続 ②無線LANで接続
----------------	---------------------------



ここまでがLANの応用になります(本講座2日目)

キ セキュリティ対策	①ルータの導入 ②ブラウザの設定 ③ウイルス対策ソフトの導入 ④スパイウェア対策ソフトの導入 ⑤ファイル交換ソフトへの対応
------------	---

(3) 構築後の管理運用

ネットワークの構成は運用方法や構築した人によって異なります。ただ機械や配線を見ただけでは、そこに構築されているネットワークの仕組みを理解することはできません。そこで、ネットワークを構築する際には、記録をとっておくことが大切です。私たちは教員ですので、専門的な設計図等は必要ありませんが、転勤や機種更新が考えられますので、**自分で構築したLANに関する情報を整理して残すことが大切**なのです。具体的には、①コンピュータ名とIPアドレス、②ユーザIDとパスワード、程度の記録は必ず残すようにしましょう。

ア 動作試験

職員室LAN構築後は必ず動作試験を行います。特に、ネットワーク内のコンピュータがブラウジングできるか、ファイルサーバへのアクセスは可能か、プリンタサーバでの印刷は可能かといった試験は、全てのコンピュータできちんと行います。

イ 管理運用

ネットワークを構築した人にとって、最も大切なことは「構築すること」ではなく、構築したネットワークを「管理運用」することです。これはネットワーク管理者にとっても重要です。「管理運用」を一言で言えば、「構築した当初の動作を維持すること」です。そのためには、「コンピュータやネットワーク機器のメンテナンス」と「ネットワークトラブルへの対処」を確実に行う必要があります。

(7) コンピュータやネットワーク機器のメンテナンス

毎日何かをしなければならぬと言うことはありません。先生方に不具合があったら報告してもらえようにすることです。ネットワークに接続できることを確認するコマンド等がありますので知っているとたいへん便利です。機械的な故障は「買い換え」または「修理」になります。

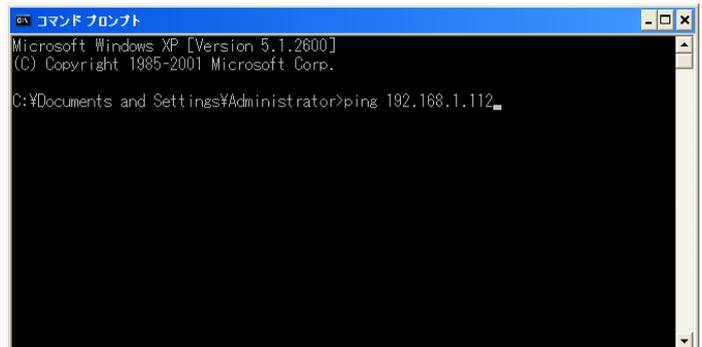
ー基本的なネットワーク関係コマンドー

① 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

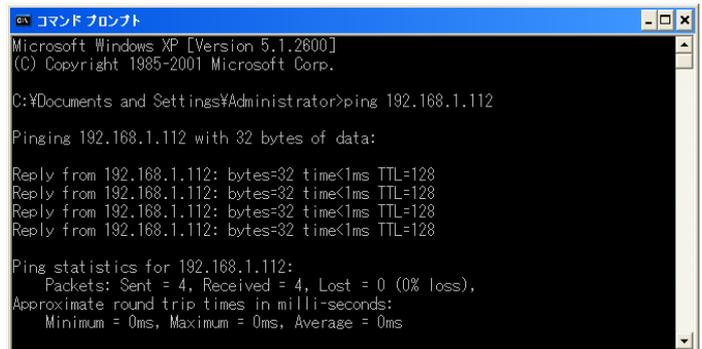
が推測できます。

- 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
- 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
```



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

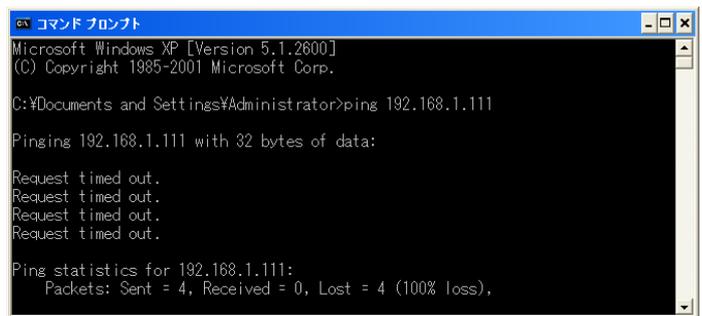
C:\Documents and Settings\Administrator>ping 192.168.1.112

Pinging 192.168.1.112 with 32 bytes of data:

Reply from 192.168.1.112: bytes=32 time<1ms 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),
```

② ipconfig

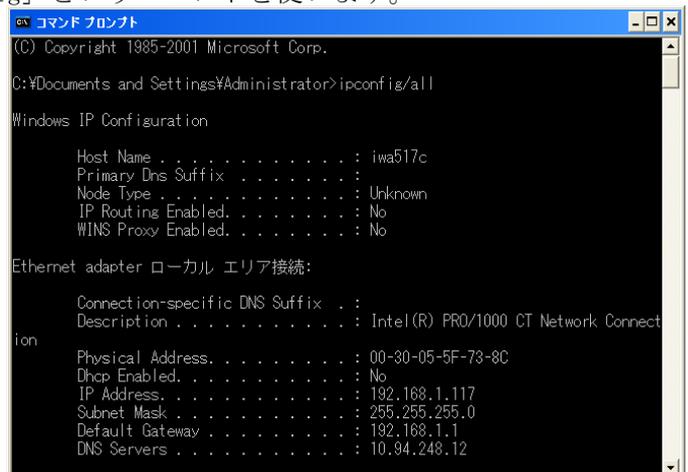
自分が使っているコンピュータのIPアドレスなど、NICに関する詳細な情報を表示します。なお、Windows95/98/Meは「winipcfg」というコマンドを使います。

【Windows2000/XP】

- 「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。
- 「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。

【Windows95/98/Me】

- 「スタート」→「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。



```
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-73-8C
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
```

③ 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

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>net file

ID          パス                                ユーザー名      ロック数
-----
03          E:\共有フォルダ                    IWA512          0
コマンドは正常に終了しました。
```

(イ) LANのトラブル

ネットワーク上のトラブルのほとんどは、「つながらない」「何かの機能が使えない」といった内容です。原因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、トラブルの可能性の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。80%以上はこれで対処できるはずです。

① 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。

② 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。

③ ネットワークケーブルの取り直し

ネットワークケーブルは、曲げに弱いいため重いもののがると断線する可能性があります。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。

④ 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。

⑤ 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をいいます。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。

⑥ 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。

⑦ 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。

⑧ NICの非認識

コンピュータに取り付けているNIC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。NIC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。

⑨ 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、OSの再インストールです。

⑩ ユーザ名の消失または登録忘れ

サーバ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。サーバ側のコンピュータに登録していたユーザID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。

⑪ パスワードの間違い

サーバ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。サーバ側にユーザ登録をする際、うっかり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。

⑫ 家庭内LANとの共用コンピュータ

小中学校の先生方のほとんどは、仕事用コンピュータと家庭用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と思います。家庭でのインターネット接続回線もADSL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LANを構築していたり、プロバイダからIPアドレスが割り振られていたりする環境が増えました。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LAN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（IP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いうことは、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となります。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、NICを2枚装着して、2種類のネットワーク設定（IPアドレス等）をそれぞれに行い、ネットワークを区別して使い分けることです。

8 職員室LAN構築の留意点ーセキュリティー

(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ますが、県内小中学校のほとんどは、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、LAN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附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。コンピュータに附属してきたウイルス対策ソフトは、体験版や試用期限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。

個人利用に限ってですが、フリーのウイルス対策ソフトがあります。ここでは「AVGAntiVirusFree Edition」の入手先を以下に記載しておきます。

■Grisoft Freeweb (<http://free.grisoft.com/>)

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をインストールしない

AntinnyはWinnyとともに行動します。絶対に、Winnyをコンピュータにインストールしてはいけません。プログラムをダウンロードしたり、コピーしたりすることも厳禁です。

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。
各社からウイルス体験版ソフトや専用駆除ツールが公開されていますので利用してください。

■MicrosoftWindows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.mspx>

ウ 「MicrosoftUpdate」を有効にする

Windowsを利用する人は「WindowsUpdate」または「MicrosoftUpdate」の自動更新を有効にしましょう。「Antinny」「山田オルタナティブ」が動作していると自動的に駆除してくれます。(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「WindowsUpdate」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、特にも、職員室LAN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。

フリーのスパイウェア対策ソフトがいくつかありますが、Vistaの場合は、標準で添付されている「WindowsDefender」の利用がお勧めです。他のWindowsOSの場合は、「Spybot-Search & Destroy」がよいでしょう。

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

MEMO

岩手県立総合教育センター
情報教育担当
平成21年7月6日発行