第 2 章 校内 LAN(Local Area Network)再構築

学校において校内LAN※1構築を行うにあたり、特に注意するべきことは外部からのセキュリティ対策及び先生方と生徒の間のネットワークを隔離する内部のセキュリティ対策である。また、ネットワークを構築する際にハブ※2などの中継機器の接続方法にも注意すべきことがある。そのため、安全で動作環境のよいネットワークを構築するには、現在利用している学校のネットワークがどのような状態にあり、どこを改善する必要があるのかを理解しなければならない。そのためには、まず学校のネットワーク構成を知る必要がある。学校におけるネットワーク構築は、ただハブからネットワークケーブルを引いて接続すればいいというようなものでない。誤った接続をしてしまうと、外部から攻撃を受けるだけでなく、学校の情報が流出したり生徒から先生の情報が見えてしまうなど非常に危険な状態になってしまう恐れがある。構築しようとしているネットワークがどのようなネットワークに属しているのかなど理解して接続しないと、非常に危険な状態でネットワークを利用することになる。

再構築を行なう場合の作業手順として、

現状の校内ネットワーク構成調査
↓
現状のネットワーク構成の検討
↓
ネットワーク改良・整備

となる。

1「現状の校内ネットワーク構成調査」現状のネットワーク構成図作成

2「現状のネットワーク構成の検討」構成図からの現状のネットワークにおける検討（教員・生徒間のネットワーク隔離、ネットワーク中継機器の接続見直し、新しい接続場所への配線方法など）

3「ネットワーク改良・整備」校内ネットワークの再構築（現状のネットワークに問題があった場合の改善）および新しくインターネット利用環境を整備したい場合は、インターネット利用を可能にする教室への配線等の整備を行う。

新しくネットワーク環境を整備したい場合は、常に現状のネットワーク構成からネットワークの安全性を検討し、安心して利用できるネットワーク環境を構築するようにしなければならない。

※1「LAN(Local Area Network)」
近くのコンピュータで構成されたネットワーク。学校の LAN はスター型 LAN（ハブなどの集線装置を中心にコンピュータを接続する方式）という接続形態をとっている。（引用文献 1 より）

※2「ハブ(HUB)」
LAN ケーブルの集線装置のこと。10BASE-T などのツイストペアケーブル（絶縁体で覆われた 2 本の銅線をねじり合わせたものを束ねたケーブル。）を集線する装置のことでネットワークの中継点としての役割を果たす。（引用文献 1 より）

2-1 学校のネットワーク構成

学校のネットワーク構成を調べるには、インターネットがどこからつながっているのかを調べ、モデム※3もしくはターミナルアダプタ（TA）※4のような信号変換装置からルータ※5やハブによって校内ネットワークがどのように形成されコンピュータ室などのインターネットを利用する教室に接続されているというネットワーク接続経路をしらべる。調べるときは、どのポートがどのネットワークグループに属しているのかを調べることが重要になる。学校のネットワーク構成を調べ、ネットワーク構築を行うときに生徒が利用するネットワークと先生方が利用するネットワークが隔離できているように構築しなければならない。また、ネットワークを有効に活用するためにハブの接続方法など注意する点やケーブル配線における点など注意する点がある。

ネットワーク構築を行なう前に、実際に校内 LAN における構成図を作成し改善しなければならないネットワーク構成を検討する。

※3「モデム(modem)」
電話回線などのアナログ回線を経由して、遠隔地のコンピュータ間で通信を行なうための機器。アナログ回線を利用したコンピュータ間の通信はモデムによって信号を変換する必要がある。（引用文献 1 より）

※4「ターミナルアダプタ(terminal adapter)」
アナログ回線やモデムなどの通信機器を ISDN 回線に接続する際に必要な信号変換機のこと。（引用文献 1 より）

※5「ルータ(router)」
LAN と LAN、LAN と WAN を接続するネットワーク機器。ネットワーク層で接続するため、ネットワークアドレスやノードをもとにしてパケットの通過に最適な経路を決定したり、適切なパケットのみを送信するなどの制御を行う。（引用文献 1 より）

2-1.1 主なネットワーク構成について

学校における構成として注意するのは、先生・生徒間のネットワーク隔離である。そして、ネットワーク隔離を行なっているネットワークの中でも、VLAN※6を使用しているかVLANを使用せずルータのみでネットワーク構築を行なっているかなどネットワーク構成に違いが出てくる。

※6「VLAN(virtual LAN)」LAN(Local Area Network)において、LANケーブルやコンピュータなどの接続形態に関わらず、LAN上の端末を仮想的にグループ化する機能のこと。VLANでは、物理的に離れた場所にあるコンピュータどうしを、同一のLANに接続されているように扱うことが可能となる。(引用文献1より)

・ルータによるネットワーク構成

「ネットワーク隔離が行なわれていないネットワーク構成」

このネットワーク状態は、外部ネットワークとの隔離は行われているが、生徒のネットワークと先生のネットワーク環境がつながっている状態であり、非常に危険である。コンピュータ室のPCで近くのネットワークを調べたら職員室の環境が見えてしまうという環境の学校は、このような先生・生徒間のネットワーク隔離が出来ていないネットワーク環境である。早急に改善対策が必要であると考えられる。

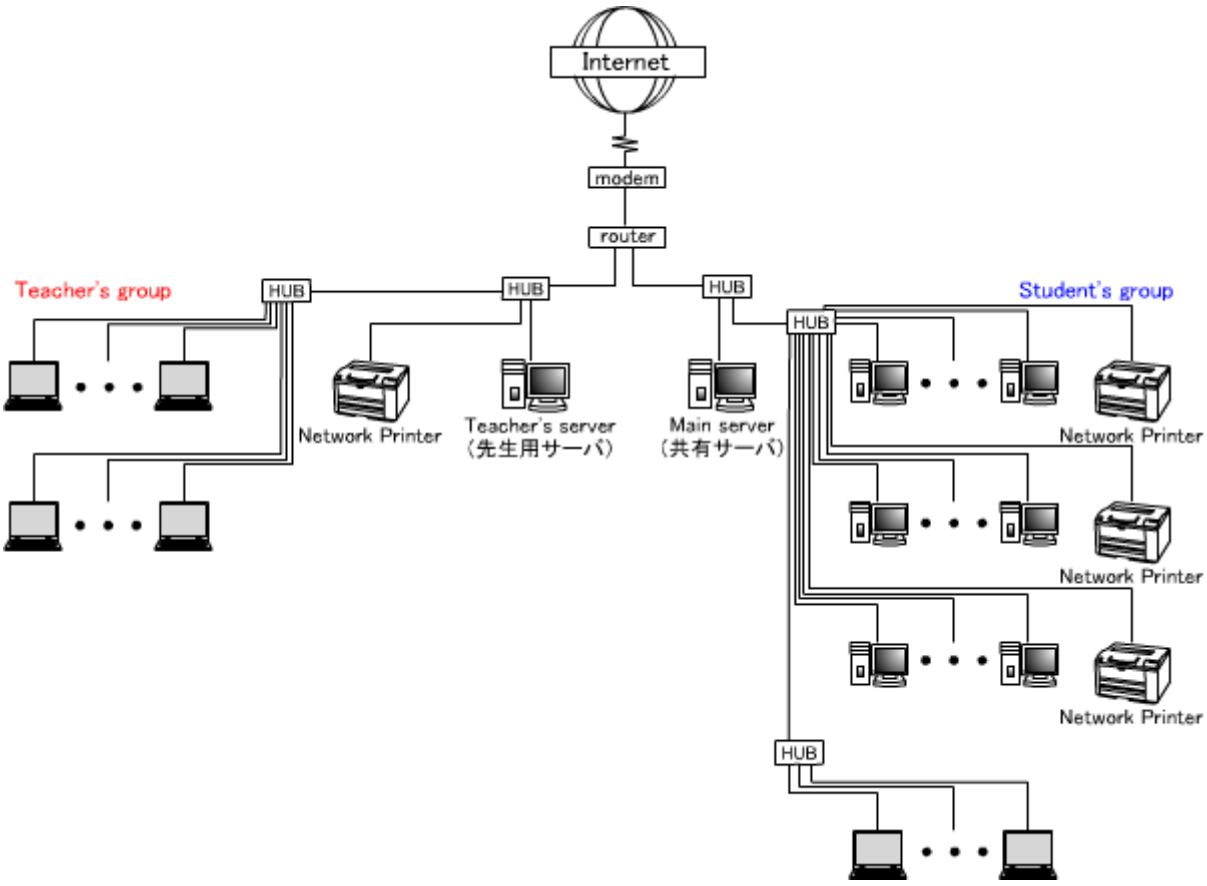

図 2.1 ネットワーク隔離が行なわれていない構成図

図 2.1 のようなネットワークでは生徒と先生のネットワーク環境がつながった状態であり、職員室PCでうかつにファイル共有※7などをかけてしまうと生徒側のPCから見えてしまうため、学校において生徒の個人情報や成績などが流出してしまう恐れがあり、PCによる情報管理が出来ない状態である。

「ネットワーク隔離が行なわれているネットワーク構成」

学校において独自にネットワーク構築を行う場合、ルータを複数台用いて先生側と生徒側のネットワークを隔離することが可能である。下図 2.2 のようにルータを複数代用いることでネットワークを隔離することが可能になる。

※7「ファイル共有(file sharing)」
LAN などを利用して、複数のコンピュータで 1 つのファイルを共有すること。ネットワーク上のコンピュータどうしでファイルの共有設定を行うことで、そのファイルを LAN 経由で共有できる。（引用文献 1 より）

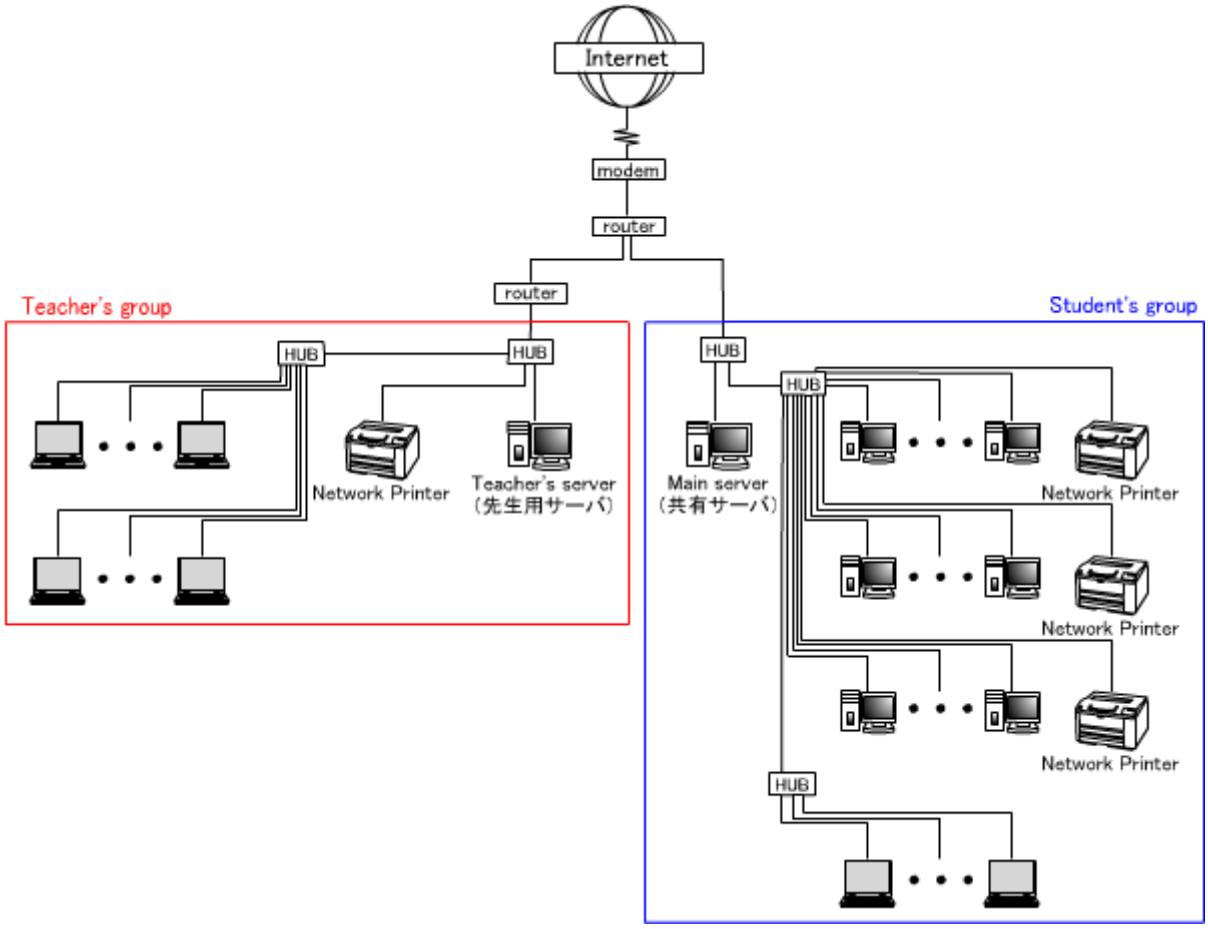

図 2.2 ルータによりネットワーク隔離された構成図

図 2.2 のようにネットワークを形成することによって先生・生徒間におけるネットワーク環境の隔離が可能になる。これによって先生・生徒間のネットワークが隔離されているため、先生たちはある程度安心してファイル共有などを行なうことが出来る。このネットワークでは、生徒→先生のネットワークはファイアーウォール※8により通信できないようになっているが、先生→生徒への通信は出来るようになっているため、生徒が授業で作ったファイルを職員室の先生のPCからコンピュータ室にとってくることは可能である。また、コンピュータ室で授業のときに使用したい教材を授業のときに取れるようにするには共有サーバもしくは共有サーバがない場合は生徒PCにファイル共有を一時的に利用するとよい。学校でネットワークを構築する上で先生と生徒のネットワーク環境を隔離することは必須であるためこのようにルータによるネットワーク隔離は必要であると思われる。

・VLAN によるネットワーク構成

現在、学校に導入が進んでいる高度なネットワーク構築としてレイヤ 2 スイッチ※9・レイヤ 3 スイッチ※10を利用したVLANによるネットワーク構築が考えられる。

VLAN によるネットワーク構築によって先生側ネットワークと生徒側ネットワークをそれぞれグループ化することによりネットワークを隔離することが可能になる。グループの設定はスイッチの各ポートごとに設定が可能であるため、下図のように同じスイッチからケーブルを引いても接続するポートによってグループが違うという利用用途ごとの自由度が高い。その反面ポートを間違えやすく、間違えて違うポートに接続してしまうと非常に危険な状態でネットワークを利用することになってしまう。

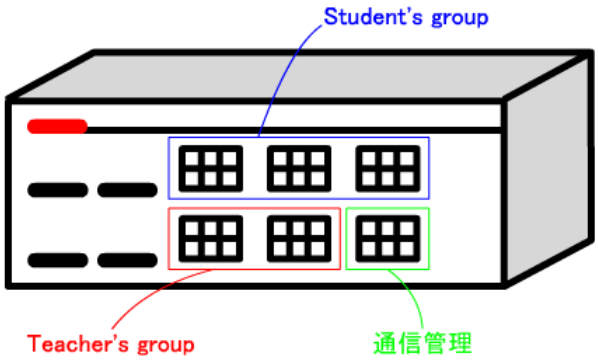

図 2.3 レイヤ 2・3 スイッチにおけるポートごとのネットワークグループ設定図

さらに、レイヤ 3 スイッチにおいて設定したグループをタグ VLAN

※8「ファイアーウォール(fire wall)」
IP 接続された LAN などのネットワーク上に設置し、ハッカーやクラッカーからの侵入や破壊を未然に防ぐためのしくみ。主に Proxy サーバーやゲートウェイを用いてシステム構築する。（引用文献 1 より）

※9「レイヤ 2 スイッチ(layer2 switch)」
ネットワーク中継機器の一つ。データリンク層のデータによりパケットの行き先を判断することによって転送を行なう。（R2.1 IT用語辞典 e-wordsより）

※10「レイヤー3 スイッチング(layer3 switching)」
スイッチングハブの機能のひとつで、送信されてきたデータからネットワークアドレスを検出して振り分ける機能。ソフト側で行う作業をハード側で受け持つことで、処理の高速化を実現できる。（引用文献 1 より）

によって他のレイヤ 3 スイッチやレイヤ 2 スイッチにおいても設定が有効となるため同じ教室にないネットワークもグループの隔離を行なうことが出来る。

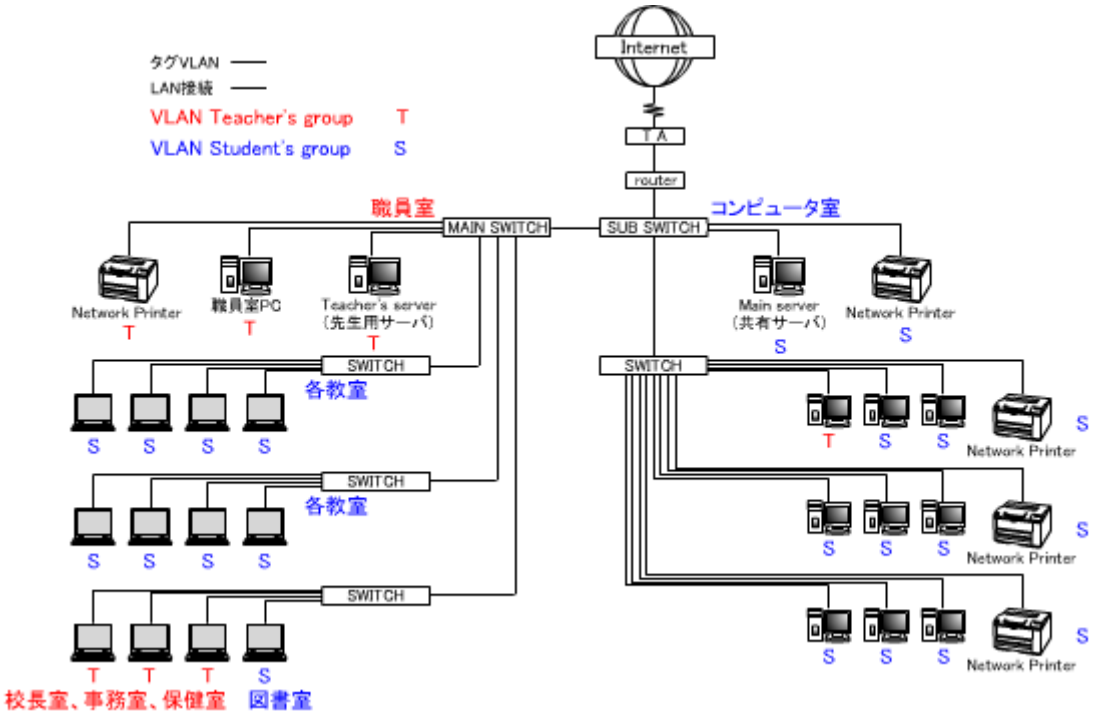

図 2.4 VLAN によるネットワーク隔離された構成図

上の図 2.4 は、「平成 15 年度 仙台市小学校ネットワーク構成図」を参考にしたVLANによるネットワーク構成図である。ここでは、MAIN SWITCHとSUB SWITCHにレイヤ 3 スイッチを利用し、その他のSWITCHはレイヤ 2 スイッチを利用している。MAIN SWITCHによりVLANの設定を行い、タグVLAN※11によってその他のSWITCHにもVLANの設定を適応している。

VLANによるネットワークでは、先生・生徒間のネットワーク隔離が出来ている。さらに、レイヤ 3 スイッチの機能によっては、先生からの通信は可能だが生徒からの通信は不可能にすることも出来る。現在の学校のネットワークではこの機能が用いられている。このようにネットワーク形成上はルータの組み合わせと同じパフォーマンスが得られている。だが、通信速度やトラフィック※12のパフォーマンスなどさまざまな性能の点を考えるとVLANの方が勝っている点が多い。また、レイヤ 3 スイッチが多機能なほど自由なネットワーク設計が出来るようになっている。

※11タグVLAN
通信させるデータにグループの識別ができる「タグ」を付けて、所属するVLANをデータごとに識別させる方法。(R2.2 Allied Telesis「学校のネットワーク(文教市場)校内LANに必要なセキュリティ」より)

※11補足
タグとは、マークアップ言語（独自に定義された書式に沿って文章を記述していく言語のこと。）で用いられる制御情報のこと。

※12「トラフィック(traffic)」
通信回線上で一定時間内に転送されるデータ量のこと。通信回線の利用状況を調査する目安となる。(引用文献 1 より)

2-1.2 教室におけるネットワークの現状について

学校における主なネットワーク利用場所は「コンピュータ室」「職員室」「その他職員が利用する教室（校長室や保健室など）」「各教室」だと考えられる。この場合、先生方が利用するネットワークは「職員室」「その他職員が利用する教室（校長室や保健室など）」で、生徒たちが利用するネットワークは「コンピュータ室」「各教室」というように分かれる。

「コンピュータ室におけるネットワーク」

現在、ほぼすべての学校に生徒がコンピュータを授業で利用する場所としてコンピュータ室が導入されている。コンピュータ室はSWITCH によって隔離されている場合もある。
コンピュータ室の PC の配置などは学校の方針によって異なる。コンピュータ室で利用される PC は主にデスクトップコンピュータが多いと思われるが、学校によっては PC の移動の自由が利くことなどからノート PC を利用している学校もある。

「職員室・その他職員が利用する教室におけるネットワーク」

職員室のネットワークはネットワーク整備してある学校は先生一人一人にインターネットの利用環境があるが、整備されていない学校は職員室にインターネットを利用できるPCが 1 台でプリンタもそのPCでしか利用できず、自分のPCで作成したファイルをプリントアウトや教材化をしたい場合は、その 1 台の職員室PCにフロッピーディスク※13やCD-R※14などのメディア※15を利用してファイル移動し作成する必要がある。また、先生一人一人にインターネット環境があっても、先生・生徒間のネットワーク隔離が出来ておらずファイル管理など満足に利用できない状況の学校もある。そして、学校によってはネットワーク整備された学校も職員室内での職員室内のハブから各先生のPCまでのケーブル配線は先生たち自身で行なわなければならないようになっている。

「各教室におけるネットワーク」

各教室へのネットワーク整備は平成 17 年度までに行なわれるよていである。現在はまだ行われていない学校がほとんどだと聞いている。各教室までのネットワーク整備が出来ても設置されるコンピュータは 1～2 台だけというような状況である。

※13「フロッピーディスク (floppy disk)」
プラスチック製の円盤に磁性体を塗布し、それをジャケットに収めた記憶媒体。（引用文献 1 より）

※14「CD-R (CD-recordable)」
太陽誘電が開発した書き込み可能な CD の規格。Orange Book と呼ばれる規格書で定義されている。（引用文献 1 より）

※15「メディア（media)」
ここでのメディアは、記憶媒体のこと。ハードディスクやフロッピーディスク、MO ディスク(光磁気ディスク)などの他に、メモリーカードなども含まれる。新聞やテレビのようなメディアは情報媒体という。（引用文献 1 より）

2-2 校内 LAN に利用されるネットワーク構成機器

学校におけるネットワークを形成するネットワーク構成機器学校での利用について解説する。

・校内 LAN におけるサーバの利用

学校においてサーバとして利用されているのはWindows※16サーバが多い。Unix※17やMac※18サーバもあるがWindowsサーバが学校において導入されていることが多い。低コストに抑えたい場合はUnix系のVine Linux※19やFedora※20のようなOSを利用した独自のサーバを構築するとよい。

サーバが主に提供するサービスは、Webサーバ※21・ファイル共有・DNSサーバ※22・プロキシサーバ※23・DHCPサーバ※24・メールサーバ※25等である。学校において実際に利用されているサービスはファイル共有、DHCP、プロキシ、DNSなどである。特に利用されているサービスはファイル共有である。しかし、ネットワーク構成がしっかりしていないとファイル共有は危険となる場合がある。Webサーバは市町村が管理するサーバに学校用のWebページ用のフォルダがあり、そこにアップしていくという形式で、学校のサーバ自体はWebサーバとして働いていない。DHCPやプロキシ、DNSはインターネット接続上のサービスだが、DHCPは職員室などにおいて先生方がインターネット接続を行なう際に使用される。また、サーバによってルータを独自に構築することも可能である。

・ルータ（router）

ルータはLANとLAN、LANとWAN※26を接続するネットワーク機器である。学校では主に外部ネットワークから学校内LANへの不正アクセス※27を防ぐなど、校内ネットワークセキュリティの強化に利用されている。ルータの中でも、個人向け製品でルーティング※28できるプロトコル※29はIP※30だけだが、企業向け製品は、IPに加えてAppleTalk※31やIPX※32なども扱えることやセキュリティ機能、特に不正侵入検知が高機能な点のような違いがある。しかし、個人向け製品のルータでもファイアーウォール機能やパケットフィルタリング※33機能があり、ネットワークのセキュリティ向上や隔離などを行なう場合にも利用することが出来る。また、コスト的にも学校に導入しやすいと思われる。

※16「Windows」
マイクロソフトが販売しているパソコン用 OS。（引用文献 1 より）

※17「UNIX」
マルチユーザーに対応した OS。企業などの基幹サーバーとして利用されている。独自の機能を持つ UNIX が開発され、多くのプラットフォームに移植された。（引用文献 1 より）

※18「Mac(Macintosh)」
米 Apple 社が製造・販売しているパーソナルコンピュータ、「Macintosh」シリーズの略称。Apple 社が販売するパーソナルコンピュータを総称して「Macintosh」と呼ぶ。(引用文献 1 より）

※19「Vine Linux」
Project Vine が Red Hat Linux をベースに開発した、Linux ディストリビューション(Linux などのカーネルとアプリケーションのパッケージをまとめてインストールできるようにしたもの)。アプリケーションやインストーラ、ヘルプなどさまざまな点で日本語に対応していることから、主に日本で普及している。（引用文献 1 より）

※20「Fedora Core」
Fedora Project が提供している Linux ディストリビューション。「Red Hat Linux」(RHL)の後継。(IT 用語辞典 e-words より）

・LAN ケーブル

LAN ケーブルには 10BASE-T、100BASE-TX、1000BASE-T のように通信速度などによっていくつかの種類がある。ただ速ければいいというものではなく、現段階において学校でネットワーク整備に利用する LAN ケーブルとしては 100BASE-TX/1000BASE-T 対応のものでよいと思われる。LAN ケーブルはパソコンに接続して利用するだけの状態で市販されているが、300m などの長い LAN ケーブルやコネクタ、工具を購入すると必要に応じて、必要な長さのケーブルをつくることが簡単に出来るので便利である。また、ケーブルが破損した場合すぐに LAN ケーブルを作成し交換することが可能になる。

写真 2.1 LAN ケーブルの作成に必要な用具

※21 「wwwサーバー(world wide web server)」
Web ブラウザからの要求に応じて HTML ファイルや動画などを送信するサーバー。(引用文献 1 より)

※22「DNSサーバー(domain name system server)」
クライアントの問い合わせたドメイン名に対応する IP アドレスを通知するサーバーのこと。(引用文献 1 より)

※23「Proxyサーバー」
代理サーバーの意味。イントラネット上のユーザー端末に代わって外部サーバーとのやりとりを行う。ファイアーウォールを構築するために設置し、セキュリティ強化や Web ページのドメイン名をキャッシュすることが出来る。(引用文献 1 より)

※24「DHCP(dynamic host configuration protocol)」
IP アドレスをクライアントに一定の時間だけ割り当て、期限の切れた IP アドレスを回収するしくみ。また、ゲートウェイアドレスやサブネットマスクなども通知できる。(引用文献 1 より)

・共有プリンタ（shared printer）

プリンタは、プリントサーバ※34もしくはプリンタ内部にプリントサーバの機能がある場合はネットワークプリンタ※35として利用する。しかし、プリントサーバがない場合でも学校のプリンタに接続しているPCからプリンタに共有をかけることでネットワークプリンタとして利用することが可能である。プリンタ共有を利用するとプリントサーバを必要としないのでプリントサーバを利用したネットワークプリンタに比べて低コストに抑えることが出来る。ただし、同時に印刷命令が出たときなど先に出た印刷命令をプリンタが処理してからしか次の印刷命令を受け付けないことやプリンタに接続しているPCのアプリケーションを利用してプリンタ共有を行うことから、各コンピュータへの負担が大きくなってしまう。

※25「電子メールサーバー(electronic mail server)」
電子メールの送受信作業を行うサーバー。送受信を担当する SMTP サーバーと、届いた電子メールをユーザーPC に受信する POP3 サーバーに分かれる。（引用文献 1 より）

※26「WAN(wide area network)」
広域情報通信網。企業の本社と支社のように、離れた場所にある LAN どうしを結んだネットワークのこと。（引用文献 1 より）

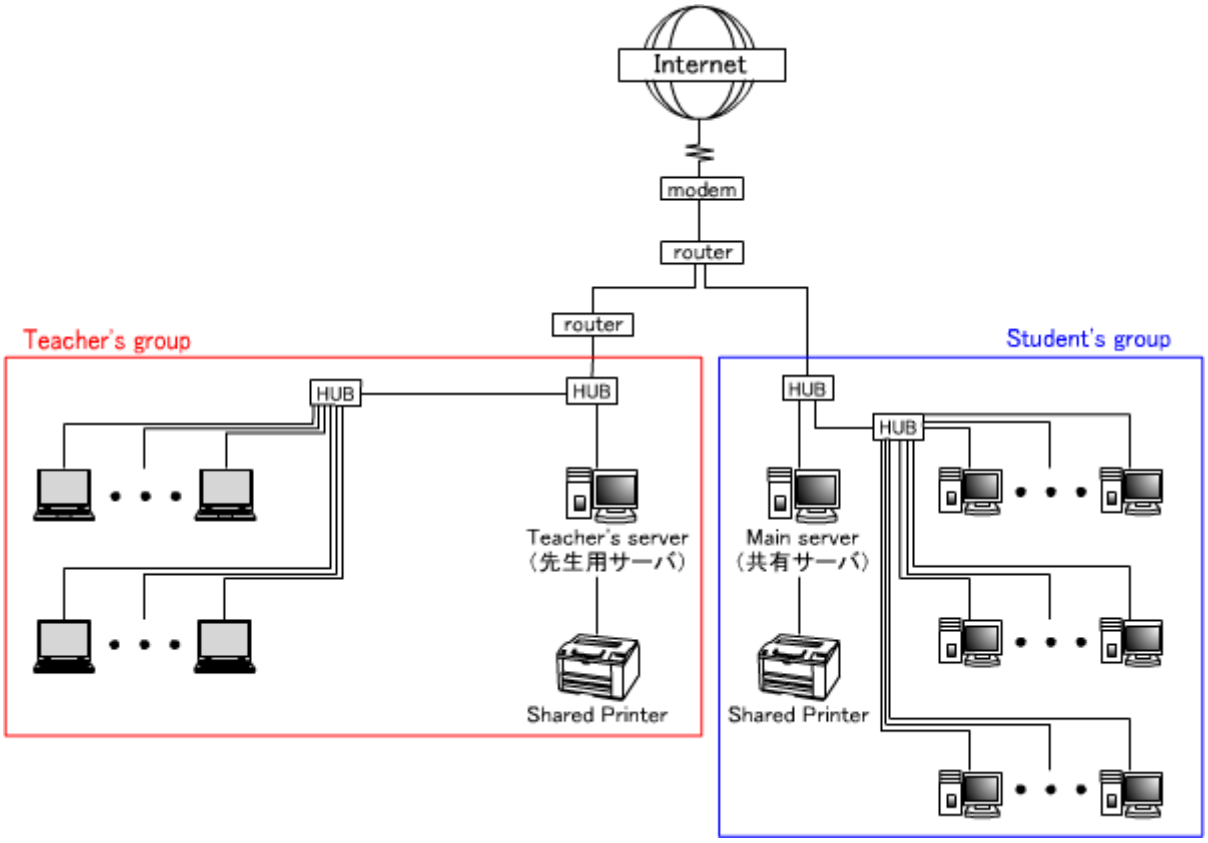

図 2.5 共有プリンタにおけるネットワーク構成図

・ハブ(HUB)について

学校で利用されるハブとしてリピータハブ(repeater hub) ※36とスイッチングハブ(switching hub) ※37がある。リピータハブにおいて10BASE-Tハブはカスケード接続※38台数が 4 台(4 段)まで、及び各機器の接続距離が 100mにより最大約 500mの接続が可能である。しかし、一般的な 100BASE-TXクラスIIリピータハブは、カスケード接続台数=2 台(2 段)まで、ケーブルの最大延長距離=100mまで及び、ノード※39間距離（機器←→ハブ←→ハブ←→機器の合計接続距離）が 205mの制限がある。それに対し、スイッチングハブは基本的にカスケード接続台数に制限がない（7 段くらいまでが理想）。（R2.3 PLANEX COMMUNICAATIONS「スイッチングハブ」より）VLAN(Virtual LAN)というネットワーク構築を行う際に利用するレイヤ 2 スイッチやレイヤ 3 スイッチはスイッチングハブに含まれる。また、ネットワーク構築時にハブ同士を接続させる場合はループするような接続はしてはならない。

※27「不正アクセス禁止法(act against unauthorized access)」
不正アクセスとは、ハッキングを行って他人の ID やパスワードを盗用して不正にアクセスする行為。（引用文献 1 より）

※28「ルーティング(rooting)」
ネットワーク上でデータを送信先へ届ける経路の中で、最適な経路を見つけ出すこと。またはその制御技術。（引用文献 1 より）

※29「プロトコル(protocol)」
コンピュータ間でデータ通信を行うために必要な規約。（引用文献 1 より）

データリンク層※40で動作する「リピータハブ」と「スイッチングハブ」の違い

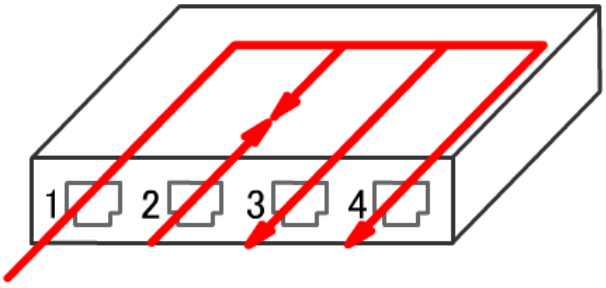

図 2.6 リピータハブのデータ通信

リピータハブの場合は、すべてのポートにデータを流すため、1 台しか同時に通信できずコリジョン※41が起こりやすい。

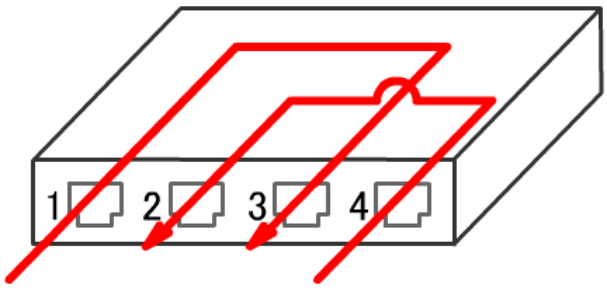

図 2.7 スイッチングハブのデータ通信

スイッチは、ポート 1 から 3 へ送信されたフレームは 3 へ、ポート 4 から 2 へ送信されたフレームは 2 へ送られ、同時に通信が可能でありコリジョンが起こりにくい。

「レイヤ 2 スイッチ」と「レイヤ 3 スイッチ」の違い

VLAN はレイヤ 2 スイッチ・レイヤ 3 スイッチ単体でも構築可能である。機能の違いとして、レイヤ 2 スイッチでは VLAN グループの設定により通信不可能なグループは完全に通信できなくなってしまう。

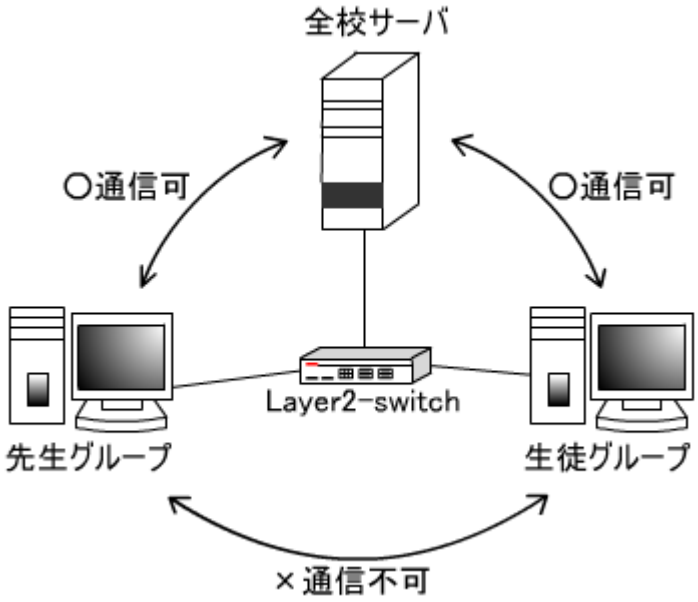

図 2.8 Layer2-switch の VLAN 間通信

※30「IP(Internet protocol)」
ネットワークに参加している機器の住所付けや、ゲートウェイとホストの間の通信経路を定義するプロトコル。OSI 参照モデルのネットワーク層に位置している。(引用文献 1 より)

※31「Apple Talk」
米 Apple 社が開発したネットワークプロトコル。MacOS に標準で搭載されていて、Macintosh を中心としたネットワークで広く利用されている。(引用文献 1 より)

※32「IPX/SPX (internetwork packet exchange/sequenced packet exchange)」
米 Novell 社が開発した、NetWare で使用するプロトコルのこと。IPX は OSI 参照モデルのネットワーク層に当たる。(引用文献 1 より)

それに対してレイヤ 3 スイッチでは、レイヤ 2 スイッチのデータリンク層(第 2 層)でパケットの行き先を判断して転送を行なう機能に加え、ネットワーク層(第 3 層)※42のルーティングなどの機能を持たせることにより自由なネットワーク設計が出来るようになっている。

図 2.9 レイヤ 3 スイッチの機能（R2.4 NETWORK MAGAZINEより）

レイヤ 2 スイッチでは VLAN グループの設定により通信不可能なグループは完全に通信できなくなってしまったのに対して、レイヤ 3 スイッチでは VLAN グループ間の通信を自由に設定することが可能となる。よって、レイヤ 3 スイッチを用いた学校における VLAN では、生徒グループから先生グループへの通信は不可能だが先生グルー

※33「フィルタリング(filtering)」
インターネットにおいて、ユーザーが受信する情報を規制すること。(引用文献 1 より)

プから生徒グループへの通信は可能という設定ができるようになるため、生徒の PC 管理が可能となることなどが考えられる。また、レイヤ 3 スイッチが多機能なほど自由なネットワーク設計が出来るようになっている。

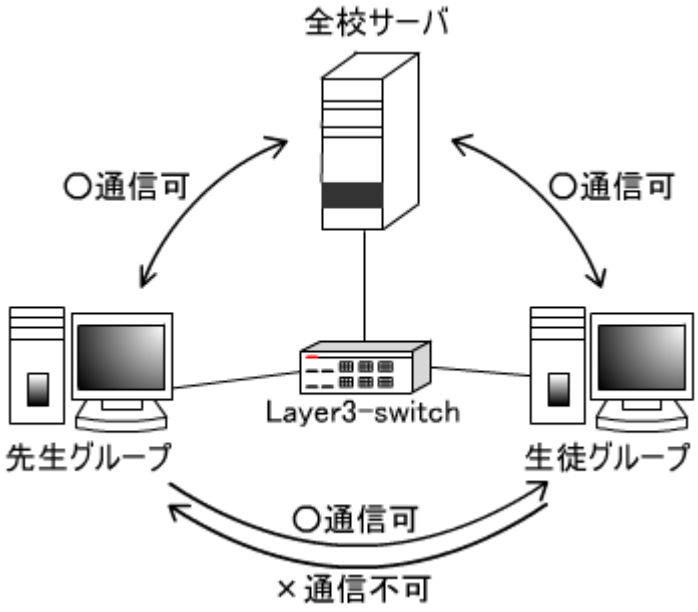

図 2.10 Layer3-switch の VLAN 間通信

現在、学校に導入が進んでいる VLAN によるネットワークは、レイヤ 2 スイッチとレイヤ 3 スイッチ両方を利用したネットワークである。レイヤ 3 スイッチにおいて設定した VLAN グループや VLAN 間の通信制御がタグ VLAN によって他のレイヤ 3 スイッチやレイヤ 2 スイッチにおいても有効となるため、柔軟なネットワーク設計を行なうことが可能となる。

※34「プリントサーバ（print server）」
プリントサーバに接続されたプリンタ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コンピュータ。各コンピュータにかかる負担を軽減することができる。(IT 用語辞典 e-Words より)

※35「ネットワークプリンタ(network printer)」
LAN などのネットワーク上で共有して使用できるプリンタのこと。(引用文献 1 より)

※36「リピータハブ（repeater hub）」
ホストから受信したデータを他の端末すべてに送信するハブ。シンプルなハブで、データの送り先を限定せず、送信先以外のホストは関係ないデータを受け取ることになる。機密性の高いデータを送受信したり、大量のデータが行き交う環境には適さない。(IT用語辞典 e-Wordsより)

※37「スイッチングハブ(switching hub)」
送信されてきたデータから宛先を検出しその送信先にのみデータを送るスイッチング機能を搭載したハブ。効率よく複数のポートにデータを転送でき、データ信号の衝突も起きない。(引用文献 1 より)

2-3 ネットワーク整備

実際にネットワーク整備を行う場合は、ネットワーク構成から、改善すべき点・新しく増築するネットワーク・配線方法などを検討してから行なう。

まず､改善すべき点としては先生と生徒におけるネットワークの隔離や中継機器の接続状況などである｡次に新しく増築するネットワークとしては、職員室・コンピュータ室・職員が利用する教室・各教室など、どこにネットワークの増築を行ないたいのかを明確にし、その教室までの配線方法などについて検討する必要がある。そして、実際に教室内への配線においてどのような手法を用いるか利用用途における配線方法や配線経路について検討してからネットワーク構築を行なう。

2-3.1 ネットワークの隔離

学校における主なネットワーク利用場所として「コンピュータ室」「職員室」「その他職員が利用する教室（校長室や保健室など)」「各教室」などがあげられる。この場合、大きく分けると先生方が利用するネットワークは「職員室」「その他職員が利用する教室（校長室や保健室など)」で、生徒たちが利用するネットワークは「コンピュータ室」「各教室」というように分けられる。

※38「カスケード接続(cascade connection)」
LANなどのネットワーク接続で用いられる、ケーブル接続方法のひとつ。複数個のハブを設置して大きなネットワークを構築していく。(引用文献 1 より)

※39「ノード (node)」
ネットワークを構成するコンピュータや端末、通信装置、ルータなどの機器の総称。(引用文献 1 より)

※40「データリンク層(data link layer)」
OSI 参照モデルの第 2 層に位置する。接続した機器どうしで送受信するパケットの構成や識別方法を定義している。(引用文献 1 より)

※41「コリジョン(collision)」
LAN などのネットワークにおいて発生する、データどうしの衝突のこと。衝突を起こしたデータはそのまま破棄されるため、通信エラーが発生する。(引用文献 1 より)

※42「ネットワーク層」
ネットワークに接続されたコンピュータのアドレス管理と通信経路を定義している。(引用文献 1 より)

「ルータによるネットワークの隔離」

ルータにおけるネットワークの隔離においては、先生方が利用するネットワークグループを形成するには、学校 LAN のルータとは別にもう一台先生ネットワーク用のルータを準備し、学校 LAN のルータと先生ネットワーク用のルータを下図のように接続し、先生ネットワーク用のルータから先生用 LAN の構築を行なう。

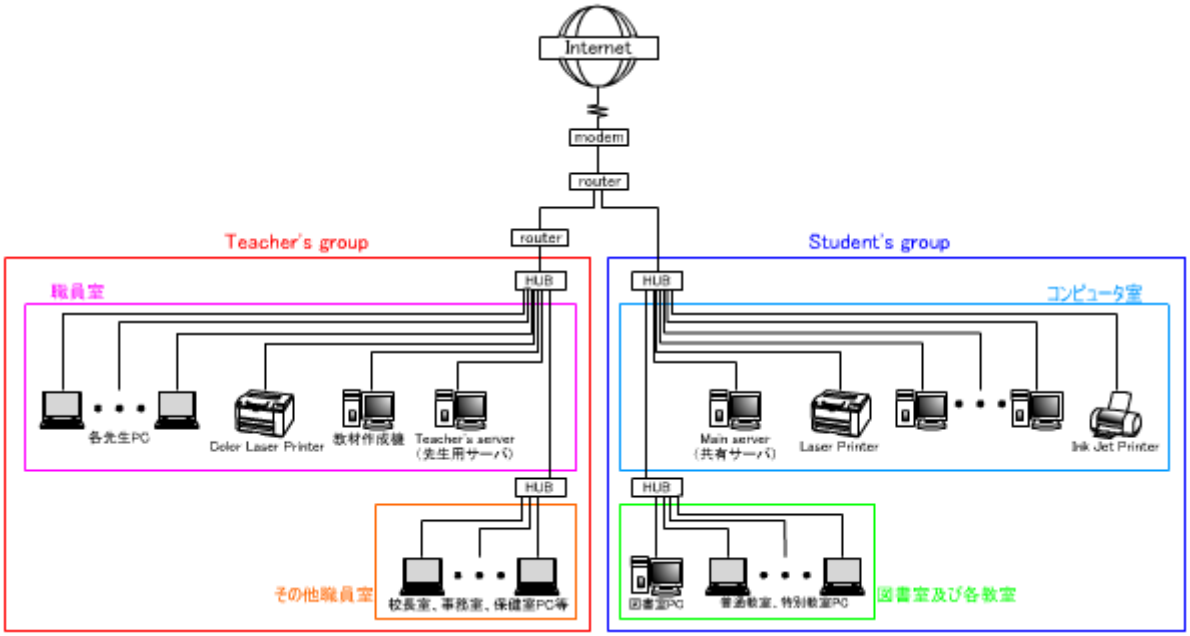

図 2.11 ルータにおけるネットワーク隔離図

ルータによりネットワーク隔離を行なった場合は、ルータによって先生グループのネットワークと生徒グループのネットワークがはっきり分かれるため間違って先生が利用する PC を生徒のネットワークに接続してしまうということはあまり起きないと思うが、間違わないようにしなければならない。校内 LAN を形成しているルータからハブなどを経由したネットワークは生徒のネットワーク環境（Student's group）であり、校内 LAN の内部で先生用 LAN を構築しているルータから接続したネットワークは先生のネットワーク環境（Teacher's group）となる。

「VLAN によるネットワークの隔離」

VLAN においては、先にも書いたがレイヤ 2 スイッチ・レイヤ 3 スイッチの設定により各ポートごとにネットワーク隔離が可能である。その反面ポートを間違えやすく、間違えて違うポートに接続してしまうと非常に危険な状態でネットワークを利用することになってしまうので、十分に調査してネットワーク接続を行なう。

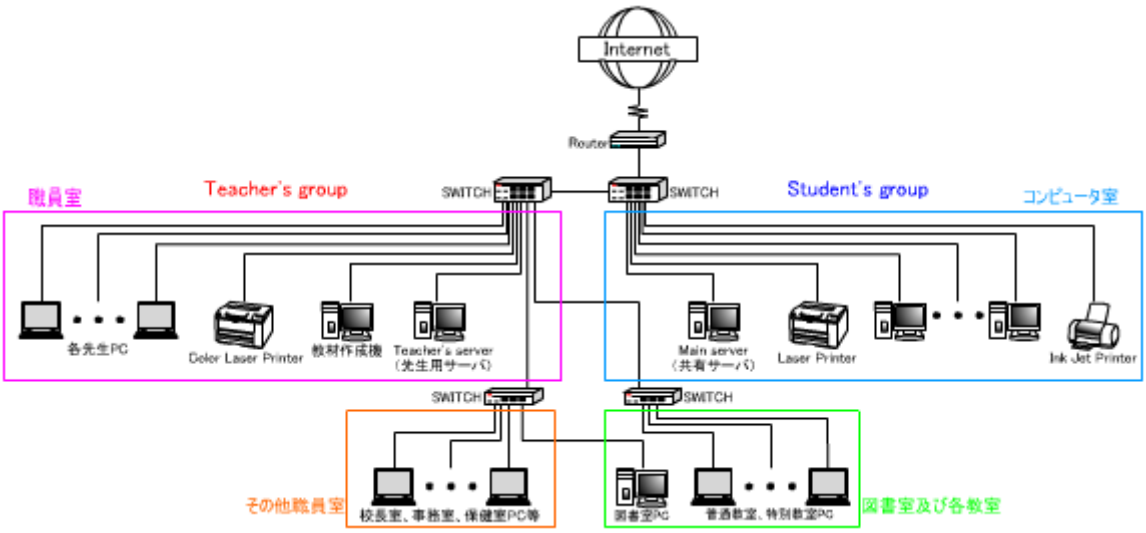

図 2.12 VLAN によるネットワーク隔離図

VLAN によるネットワーク構築では、ポートごとにグループ分け出来るためレイヤ 2 スイッチ・レイヤ 3 スイッチからであればどのスイッチからでも先生のネットワーク･生徒のネットワークどちらのネットワークにも接続が可能となる。そのため、インターネット環境を構築したい教室に一番配線しやすいスイッチからケーブル配線を行なえばよい。

2-3.2 各教室におけるネットワーク構築

校内 LAN 構築を行なう主な場所として「コンピュータ室」「職員室」「その他職員が利用する教室（校長室や保健室など）」「各教室」が考えられる。

「コンピュータ室におけるネットワーク構築」

コンピュータ室におけるネットワークは各学校の利用方針に合わせて構築する。コンピュータ室の PC はデスクトップが多かったが、近年ではノート PC をメインにコンピュータ室に取り入れるなどコンピュータ室も利用方法に応じてコンピュータ室の形態も変わるようになってきた。学校に合ったコンピュータ室の導入を行なうことにより授業に対してコンピュータを有効的に利用できる環境を整備するとよい。

「職員室におけるネットワーク構築」

職員室にネットワーク利用環境を構築する場合、利用するのは先生方が中心となるので生徒や外部に漏れてはいけない情報を取り扱う。よって、職員室のネットワークを隔離しセキュリティを高くしなければならない。先にも書いたが、VLAN（Virtual LAN）を利用している学校は生徒が利用するグループのポートと先生方が利用するグループのポートがあるが、どのポートがどちらのグループに属しているかはっきり理解して、絶対に間違わないように先生方が利用するグループのポートからネットワークケーブルを引き、ネットワーク構築を行う。また、VLAN を使用せずに、ルータを利用してネットワークを隔離しそこから先生方用のネットワークケーブルを引きネットワーク構築を行う。

「その他職員が利用する教室（校長室や保健室など）」

その他職員が利用する教室にネットワーク環境を構築する場合は、先生方用のネットワークケーブルは職員室の先生ネットワークグループから引いてきてくると思われる。先生方用のポートからケーブルを引き先生グループのネットワークに入っていれば職員室からでなくてもとくに問題はない。ただこの場合、構築する教室の場所によっては学校の配管などを通して利用教室へケーブルを引かなければならないなど大掛かりになることもあると考えられる。

「各教室」

各教室にネットワーク構築を行う場合は、生徒が利用することが考えられるので生徒用のポートからケーブルを引き配線を行う。教室までネットワークケーブルを引いたら、生徒用の設定でインターネット接続を行なう。教室において複数代のネットワークコンピュータを利用したい場合は、ハブによってさらに各教室の PC までケーブルを引く必要がある。常時接続可能な状態にするためには教室内においてさらに配線作業を行なう必要がある。

最近では、各教室でネットワークを利用する場合は無線LAN※43を利用することも行なわれている。教室で 1 台だけ利用する場合は教室まで引いたケーブルだけでよいが、複数台利用する場合は教室内にケーブルを引かなければならない。しかし、無線LANを利用するとアクセスポイント※44を設置するだけで教室内での複数台のネットワークコンピュータ利用が可能になる。また、必要に応じて無線LAN環境を教室に作り出すことも可能であるので常時接続できる状態にしなくても利用できる。ただし、無線LANの利用では利用台数やセキュリティに不安を抱えることが考えられるが、最近では同時に接続できる台数が最大 50 台のものやTKIP※45やAES※46など暗号化※47通信機能も強固になってきている。

「ケーブル配線について」

ケーブル配線において注意しなければならないことは、学校における環境は、人の出入りが激しく子供たちが多くいることから、ケーブルが危険となるような配線をしてはならない。ケーブル配線を行う場合は壁沿いや屋根上、床下というような歩行などに邪魔にならなく目に付かない場所を通すとよい。また、配線を行う場合は必ずモールなどのケーブルカバーを用いなければならない。これは、ケーブルの損傷や切断などからケーブルを保護するための事でもある。

また、「各教室」の中でも紹介しているが、無線 LAN を学校に導入するということも行われてきている。無線で電波を飛ばしインターネットを利用できるようにするため、配線工事がいらなくなる。また、離れた校舎や体育館などへのインターネット利用環境の提供も容易に行えるようになる。という利点があげられる。無線 LAN のセキュリティにおいては、「各教室」でも述べたが暗号化や特定の PC で利用するような環境では利用できる PC を特定の PC に制限するということも行うことができる。

※43「無線LAN(wireless LAN)」
有線ケーブルではなく、電波や赤外線を使って行う LAN。数メートルから数百メートルの範囲で利用できる。(引用文献 1 より)

※44「無線LANアクセスポイント(wireless LAN access point)」
無線LANで端末間を接続する電波中継機。無線LANでは各端末間が直接通信を行なう「アドホックモード」と、アクセスポイントを中継して通信する「インフラストラクチャモード」がある。(IT用語辞典 e-Wordsより)

※45「TKIP(Temporary Key Integrity Protocol)」
WEPの後継にあたる暗号化の規格。WEPが暗号化キーを固定で使用していたのに対し、TKIPでは一定時間ごと、もしくは一定パケット量ごとに自動的に暗号化キーを変更する。さらに、TKIPはWEPとの互換性があり、ファームウェアのバージョンアップで対応できる機器が多い。しかし、通信速度がWEPに比べ遅くなってしまう。学校などのように大量の無線LAN機器を利用する環境には適さない。(R2.5 jmc 株式会社ジェイエムシーより)

※46「AES(Advanced Encryption Standard)」
NIST(米国商務省標準技術局)によって策定された次世代暗号方式。ベルギーの開発者が考案した「Rijndael(ラインダール)」という暗号方式が用いられる。(引用文献 1 より)

2-3.3 ネットワーク構築する際の注意点

教室までの配線の際、ハブから離れた教室までケーブル配線を行なう場合はむやみにケーブルを引っ張ればいいというものではない。接続するまでのネットワークケーブルが長すぎると接続できなくなってしまう。また、だからといってハブを何台も経由して接続するのもだめである。

先の「2-2 校内LANに利用されるネットワーク構成機器および構築道具」の中のハブについてでも書いてあるが、リピータハブにおいて10BASE-Tハブはカスケード接続台数が 4 台(4 段)まで、及び各機器の接続距離が 100mにより最大約 500mの接続が可能である。しかし、一般的な 100BASE-TXクラスIIリピータハブは、カスケード接続台数=2 台(2 段)まで、ケーブルの最大延長距離=100mまで及び、ノード間距離（機器←→ハブ←→ハブ←→機器の合計接続距離）が 205mの制限がある。それに対しスイッチングハブは基本的にカスケード接続台数に制限がない（7 段くらいまでが理想）。（R2.3 PLANEX COMMUNICAATIONS「スイッチングハブ」より）とある。

VLAN(Virtual LAN)というネットワーク構築を行う際に利用するSWITCH（レイヤ 2 スイッチやレイヤ 3 スイッチ）はスイッチングハブに含まれる。

配線の際はこのようなネットワークケーブルの接続方法にも注意して行なわなければならない。

※47「暗号化(encryption)」データを一定の規則に従って変換し、元の内容がわからないようにすること。特に、インターネット上でデータをやり取りする場合、暗号化は重要な技術である。暗号化したデータを元に戻すことを、復号化と呼ぶ。（引用文献 1 より）