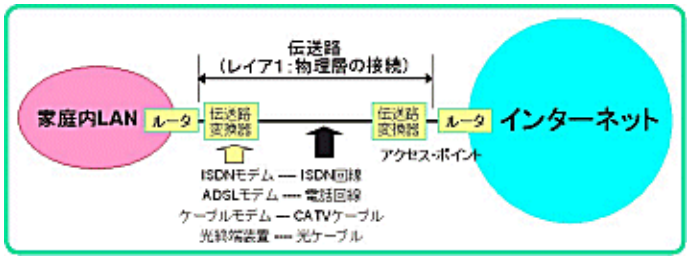
講座第２回目にようこそ。今回は課題②「ルータ、ハブなどのネットワーク機器の機能は？」 に応えて、関係する技術の要を学びましょう。

## 第２回：ルータ、ハブなどのネットワーク機器の機能

### １．ネットワーク機器

家庭内ネットワークをインターネットに接続するために、電話回線を使う場合はISDNモデムやADSLモデムを、CATVを使う場合は ケーブル･モデム、光ケーブルを使う場合は光回線終端装置を設置します。

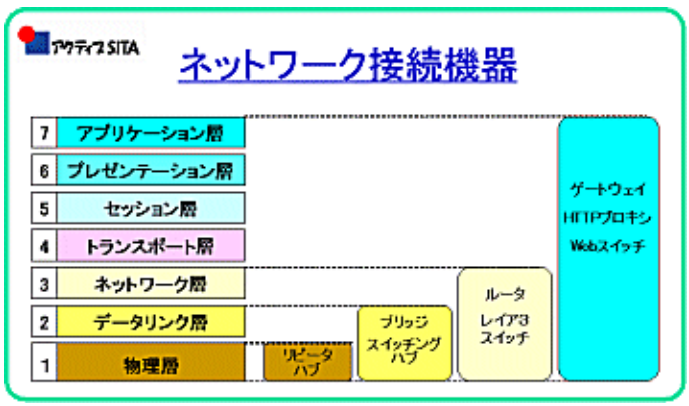



最寄りのアクセス･ポイントとの間で信号をやりとりするために、これら装置が家庭内LANの信号を伝送路 の信号に変換する役割をするもので、前回に説明したOSI参

照モデルのレイア１（物理層）を担っています。 ちょうど家の前から公道 が延びていて、そこへ出るには、「素足でなく靴を履く」ように、伝送路により信号の変換が必要です。

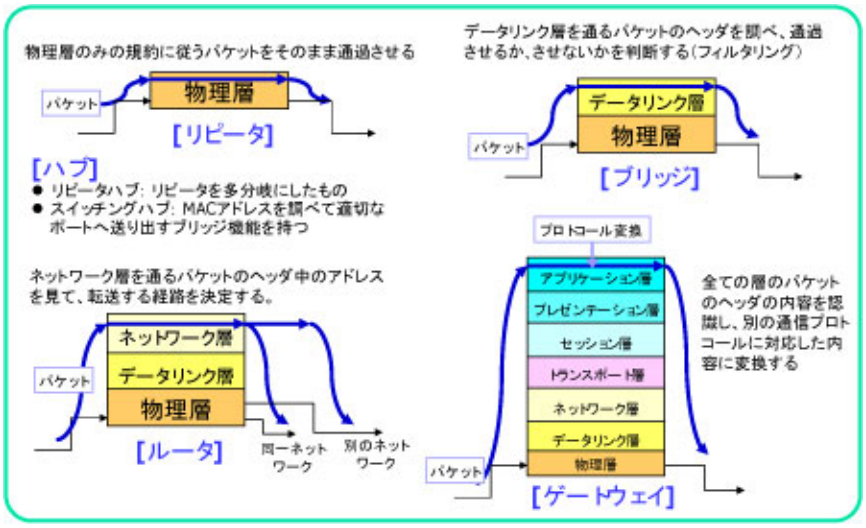
また家の廊下から道まで開けっ広げにしている家はなく、玄関や門扉を設けていますね。ネットワークにおける「玄関や門扉」の役割が「ルータ」の１つの機能です。「ハブ」や「ブリッジ」を介してインターネットに つなげる場合もありますが、それらはルータに比べ「簡易な門扉」と言えます。

（「簡易な門扉」では泥棒が入りやすい？--- 理由は後で）



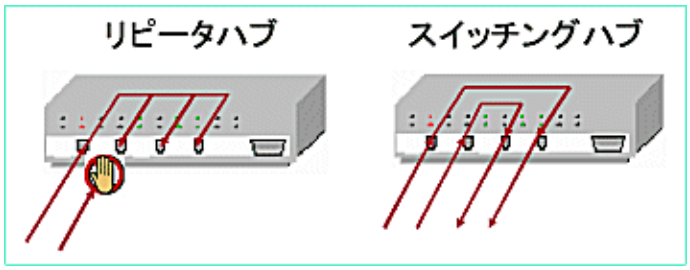

今、説明したようなモデムやルータやハブやブリッジなどをネットワーク機器と言います。それらの機能を 理解するためにも、前回説明したOSI参照モデルは大変役立ちます。例えば、モデムやハブやリピータという機器は「物理層」で動作する装置であると認識すると、およそどんな機能をもっているか解ります。つまり、「物理層」はLANケーブルやLANカードの規定をするものと理解しているので、それらと同等のレベルの役割ではないかと言う風に。

ハブはLANケーブルを何本かに分ける機能を持ち、複数のパソコンをまとめて接続することができるという訳です。ブリッジやスイッチング･ハブは「データリンク層」で、ルータやレイア3･スイッチは「ネットワーク層」で、ゲー




トウェイ と言われる物は「全層」をカバーする機能があります。

もう少し詳しくは、上図を見て下さい。 リピータは「物理層」でパケット信号の全てのフレームを中継し、 ブリッジは「データリンク層」を見てパケットをとうすかどうか判断する機能を持っています。ルータは「ネットワーク層」を見て判断します。「ゲートウェイ」という装置は全ての層のパケット内容を認識し、 別の通信プロトコールに対応できるように内容を変換します。




ところで、初期のハブはリピータハブで、リピータ機能をもった多数のポート（ここでは物理的な端子と理解 して下さい）を有する装置で、任意のポートにきた信号を他の全てのポートに流します。その時には、他のポートへは信号を送る ことはできません。

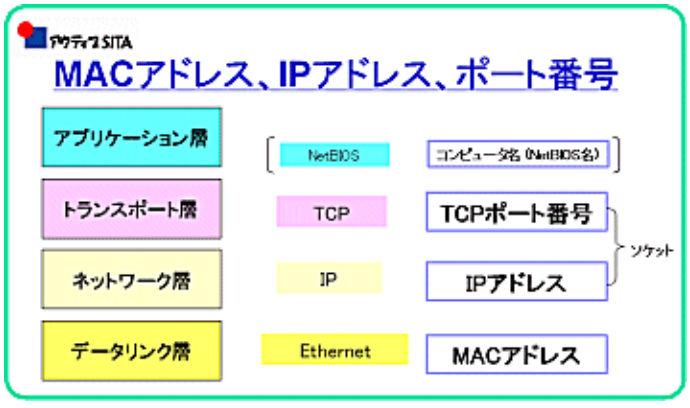
一方、スイッチングハブは、２つのネットワークを橋渡しする「ブリッジ」から派生した装置です。ブリッジは 「データリンク層」で動作し、MACアドレスをもとにEthernetフレームの転送先を決めるものです。スイッチングハブも同様にMACア ドレスを調べ、必要なポートにのみフレームを流す装置です。

▲先頭へ

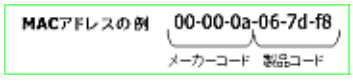
## 2．ネットワーク内のアドレス

ブリッジやルータが各層で主に「見る」ものとは、各層で付与される「アドレス」です。各層の「アドレス」 には、MACアドレス、IPアドレス、ポート番号およびコンピュータ名（これは次回に説明）があり、ネットワーク上で 大変重要です。なぜなら、郵便物の「宛先住所」や「宛名」と同じで、それらがないと、先方に届かないのですから。

### ① MAC (Media Access Control) アドレス

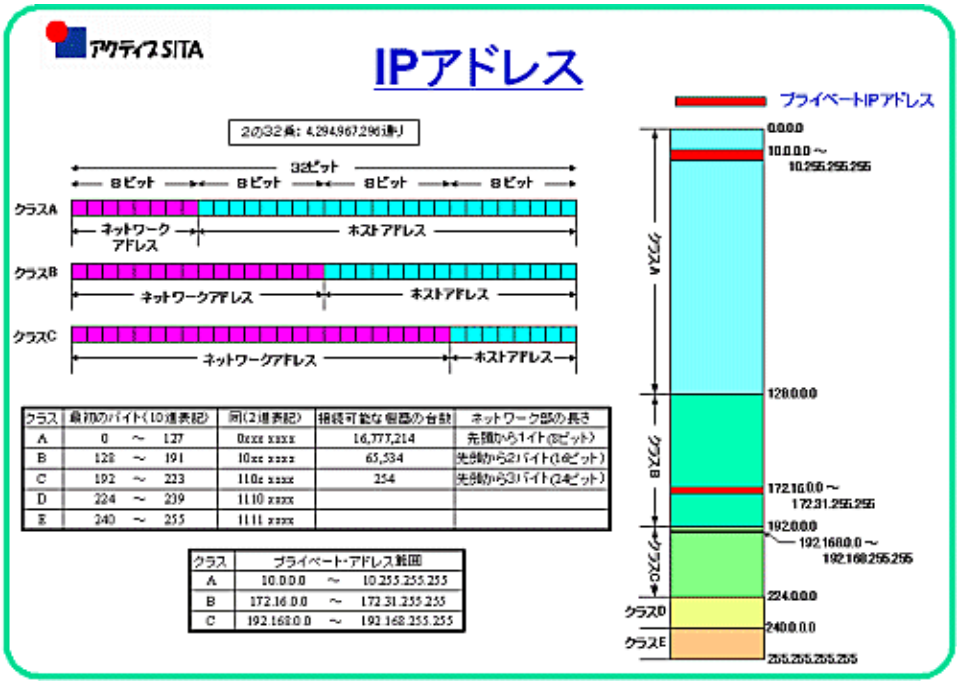



データリンク層で使用する物理的なアドレス情報です。 MACアドレスは48ビット値で、8ビット毎に16進で表記され、各機器を特定する固有のものです。




次に述べる論理的なIPアドレスだけでは通信を行うことはできず、LAN内では、機器固有のMACアドレスで宛先を確定しています。

### ② IPアドレス




| クラス | 最初のバイト(10進表記) | | 同(2進表記) | 接続可能な機器の台数 | ネットワーク部の長さ |
|---|---|---|---|---|---|
| A | 0 | ～ 127 | 0xxx xxxx | 16,777,214 | 先頭から1バイト(8ビット) |
| B | 128 | ～ 191 | 10xx xxxx | 65,534 | 先頭から2バイト(16ビット) |
| C | 192 | ～ 223 | 110x xxxx | 254 | 先頭から3バイト(24ビット) |
| D | 224 | ～ 239 | 1110 xxxx | | |
| E | 240 | ～ 255 | 1111 xxxx | | |

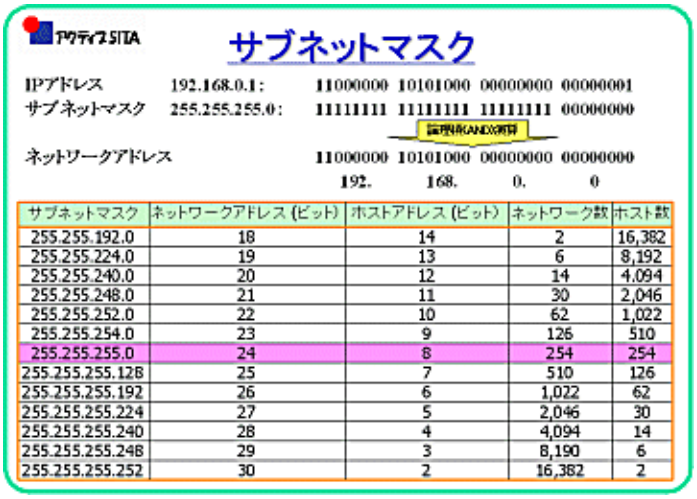
| クラス | プライベート・アドレス範囲 | | |
|---|---|---|---|
| A | 10.0.0.0 | ～ | 10.255.255.255 |
| B | 172.16.0.0 | ～ | 172.31.255.255 |
| C | 192.168.0.0 | ～ | 192.168.255.255 |

インターネットの代表的なアドレス（住所）です。世界中で通用し、その割当は管理されています。管理されているIPアドレスを「**グローバルIPアドレス**」と言います。

それとは別に、家庭

内LANでもIPアドレスを使うと便利なので、LAN内だけで自由に使える「**プライベートIPアドレス**」と言うのも決められています。32ビット構成で、8ビットの4区切りで表現します。

IPアドレスは、「ネットワークアドレス」と「ホストアドレス」に区切られています。IPアドレスとしては、全て1とか、最後のビットが0のものは除かれます。



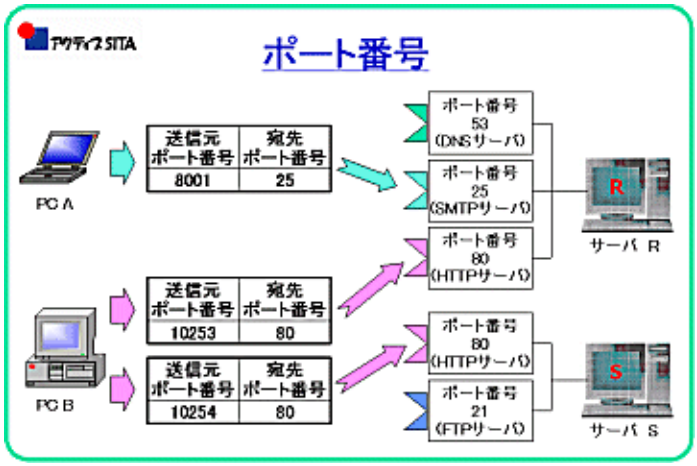

| サブネットマスク | ネットワークアドレス (ビット) | ホストアドレス (ビット) | ネットワーク数 | ホスト数 |
|---|---|---|---|---|
| 255.255.192.0 | 18 | 14 | 2 | 16,382 |
| 255.255.224.0 | 19 | 13 | 6 | 8,192 |
| 255.255.240.0 | 20 | 12 | 14 | 4,094 |
| 255.255.248.0 | 21 | 11 | 30 | 2,046 |
| 255.255.252.0 | 22 | 10 | 62 | 1,022 |
| 255.255.254.0 | 23 | 9 | 126 | 510 |
| 255.255.255.0 | 24 | 8 | 254 | 254 |
| 255.255.255.128 | 25 | 7 | 510 | 126 |
| 255.255.255.192 | 26 | 6 | 1,022 | 62 |
| 255.255.255.224 | 27 | 5 | 2,046 | 30 |
| 255.255.255.240 | 28 | 4 | 4,094 | 14 |
| 255.255.255.248 | 29 | 3 | 8,190 | 6 |
| 255.255.255.252 | 30 | 2 | 16,382 | 2 |

さらに、IPアドレスと共に「サブネットマスク」という情報も必要です。それは、 IPアドレス内の「ネットワークアドレス」を検出するためです。左図のようにIPアドレスとサブネットマスクから、論理積（AND）の演算によりネットワークアドレスが求められます。

サブネットマスクは、必ず１から始まり１が続き、０となると０が連続します。最初から１が幾つ続くかで表現することができ、 サブネットマスク 255.255.255.0 は１が24個続くので、192.168.0.1/24 と表記するとサブネットマスクがわかります。

**③ ポート番号**

MACアドレスとIPアドレスに比べ、ポート番号はわかり難いです。レイア４「トランスポート層」で、 その上位の「アプリケーション」とを関係付けるために必要な割当番号です。（「ポート」というと物理的な「端子」 と混同されますが、ここでいう「ポート番号」は、ソフト上での番号付けと理解してください。）



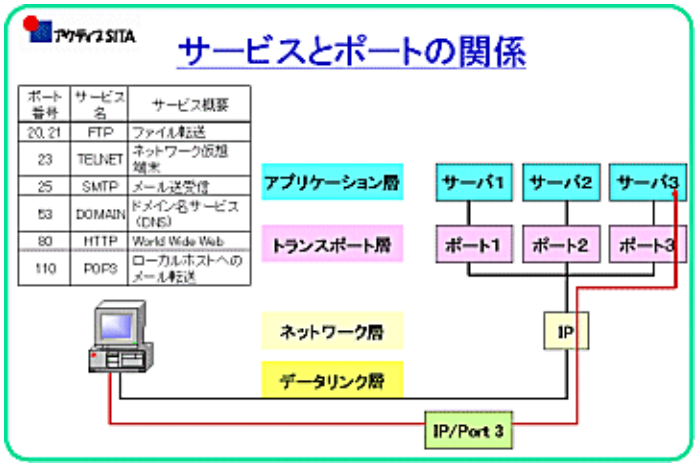

なぜ、ポート番号が必要かを解説します。左図のように、サーバにアクセスする時に、サーバに何を要求 するか、何の「サービス」を受けたいのかをポート番号で指示します。

喩えれば、「町田市役所」の住所は1つなので、そこへは行けますが、行っても「窓口」がわからないと必要な情報がとれず、 用事も足せません。 （「案内係がいるから大丈夫よ」と声が聞こえますが、でも事前にわかっている「窓口」は知って行った方がスムースに事 が運びますよね。）

もう1つ、ポート番号が必要な説明は、上図の下側です。今あなたがブラウザで http://rrrrr としてサーバRのサイトを見ていて、同時に http://sssss としてサーバSのサイトも参照したい時がありますね。 自分のIPアドレスやMACアドレスは１つしかないのに、なぜ、２つ以上も見えるのかというと、自分のＰＣで別の窓口 （送信元ポート番号）を開いているからです。 サーバRのウェブ情報はポート「10253」に戻り、サーバSのウェブ情報はポート「10254」に戻るので、２つが混同されること はなく受信され、表示されるのです。

先ほど、市役所の「サービス」と「窓口」の関係が事前にわかっていたらスムースだと言いましたが、インターネットでは 「よく知られた（well known）ポート」と言われています。次図の中に代表的な「サービス」と「ポート番号」 を示しています。（住民がよく使う役所の「窓口」くらい知らなくてはというのと同程度に、インターネット人は 「Well Known Port」くらいは知らなくてはということになりますかね。 でも、パソコン・ネットワークで

は当人が知らなくてもパソコンが「よく知っています」から大丈夫ですが。）




ポートと関連して、ソケットという言葉もネットワークやパソコンで使われます。少々細かいことなので、下枠に記します。

**ソケット（Ｓｏｃｋｅｔ）**

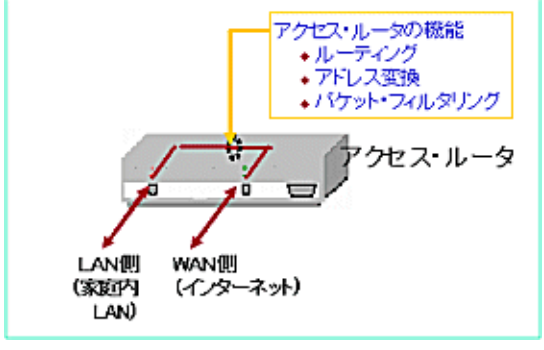
IPアドレスとポート番号を組み合わせたネットワークアドレスのこと。

ソケットには、通信を行うアプリケーションソフトがTCP/IPを扱うための仮想的なインターフェースという意味もある。WindowsでTCP/IPの機能を利用したソフトウェアを開発するためのAPIをWinsock (Windows Socket))という。

▲先頭へ

## ３．複数のパソコンからインターネットに同時に接続できるのは？ -- ルータの役割

これまでの下準備で、いよいよ家庭内LANで最も重要な機能を発揮しているネットワーク接続機器であるルータの機能を説明します。

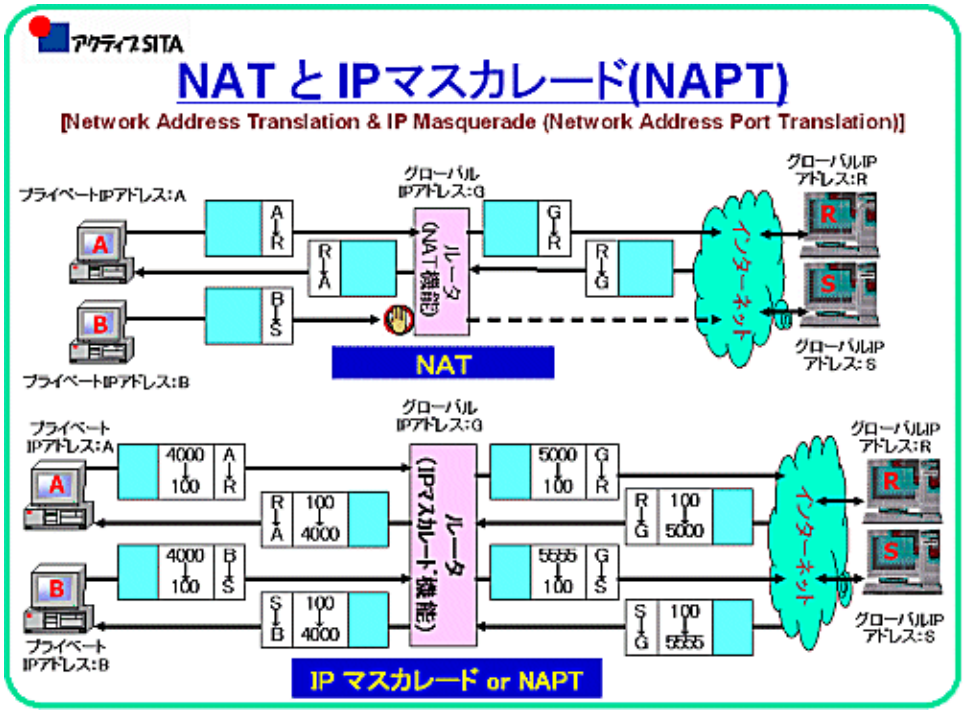



家庭内LANからインターネットへ接続するために使われるルータを「アクセス・ルータ」と称します。単にLANとLANをつなぐためのルータを「ローカル・ルータ」といい、若干機能が違います。

ルータ機能は主に図に示すように３つ有ります。 家庭内LANで複数のパソコンから同時にインターネットにアクセス できるようにしているのが、「アドレ

ス変換」（NAT：Network Address Translation）です。

インターネットの世界では、各PCがグローバルIPアドレスを持たないと宛先からの返信を受けることができません。 ところが、一般に家庭ではISPからはグローバルIPアドレスが１つだけしかルータに割当てられていません。




そこで、左図の上側の様にルータがNAT機能を発揮します。パソコンＡがサーバＲと通信する時に パケットのIPヘッダ内のIPアドレスが変換され、通信が可能となります。このように、NAT機能でプライベート IPアドレスとグローバルIPアドレスを一対一に対応させますが、これでは、同時に複数のパソコンからの要求があると対応できません。

そこで、アクセス・ルータにはIPマスカレードという機能があります。

これは、NAT機能をポート番号にまで拡張した機能で、NAPT(Network Address Port

Translation） と呼び、LAN内にある複数のPCが同時にインターネットに アクセスできるようにします。図の下側に描いているのが、その機能の説明です。masquerade とは 「仮面」、「仮装」という意味で、「仮面」をかぶって出かけても中味は間違われないとでも言うことでしょうか。 パソコンＡはＲにアクセスする場合、グローバルIPアドレスはＧしかないので、Ｇの「仮面」をかぶり、 同時にパソコンＢもＧの「仮面」で成りすまします。しかし、それらの背後で（パケットのヘッダー内で）ポート番号と結び付け られているので（図では、ポート番号5000と5555)、Ｒからの情報はＡへ、ＳからはＢへ、間違いなくつながります。秘密は「仮面」 の内側にあり･･･ですね。

ルータの他の機能、先に「家の玄関や門扉」相当と言った「パケット・フィルタリング」機能とは、「IPアドレス」と「ポート番号」 の組み合わせをみて、パケット信号を通過させるか非通過とするか、どこへ通過させるか等の機能のことです。

また、ルータの本来の機能の「ルーティング」とは、家庭内LANに留まる通信か外部のインターネットで出て行く通信かを見分ける ことです。また、インターネット内でのルータの機能は、従来の電話回線交換網における「電話交換機」に相当し、インターネット 網内での要の装置です。

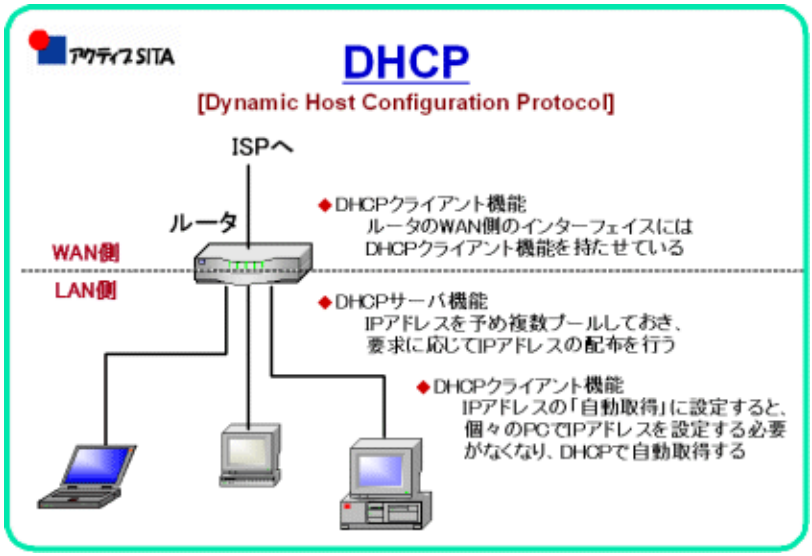
▲先頭へ

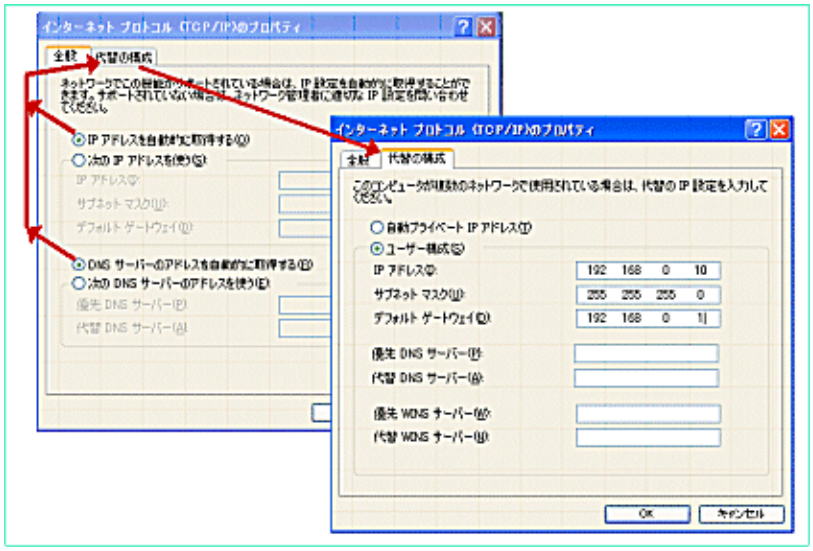
## ４．DHCPとかDNSとかはどう言うもの？

少し脇道にそれますが、インターネットの「重要」機能の中で、感覚的にもやもやしていて解り難い、頭に’ Ｄ’ の付く、DHCPとDNS（これらは互いに関係はないのですが）に関して、すっきりさせておきましょう。

### （１）DHCP

先に述べたIPアドレスをパソコンやネットワーク機器に設定するには、パソコンの設定画面を開いて手動で簡単に設定 できますが、他のパソコンやネットワー



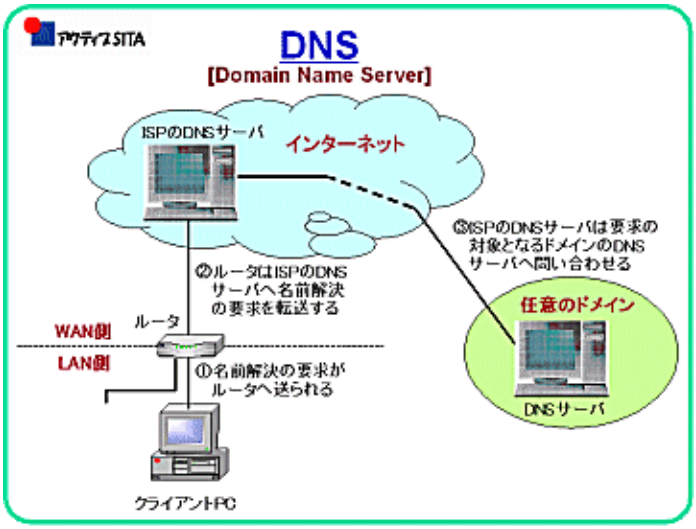
ク機器と重複なく、間違わずにIPアドレスを設定しなければならないので、 気をつかいます。そこで、 自動的に設定される方法としてDHCPという機能があるのです。

換言すると、ネットワーク内のある機器が動的に、アドレス情報（IPアドレス、ゲートウェイIPアドレスなど）を、要求するパソコン 等に配布するサービス（プロトコール）のことです。
図の様に、DHCPサーバ機能の付いているブロードバンド･ルータを利用する ケースが多いようです。

Windows XPのパソコンにIPアドレス自動取得（DHCP）を設定するには、「インターネット プロトコール （TCP/IP）プロパティ」で「IPアドレスを自動取得する」にチェックします。
さらに、右側に示すような「代

替の構成」というのがあり、DHCP機能が不具合になる場合に備え、固定割付もできるようになっています。

### （2）DNS




DNSとは、インターネット上で、IPアドレスとドメイン名（例えばactive-sita.com） を相互に結びつける役割をするサーバです。ブラウザのアドレスに、数字の羅列のIPアドレスを入力するのではなく、 ドメイン名で入れれば（http://active-sita.com の様に）、所望の宛先のIPアドレスに変換されるし、メールで xxxxxx@active-sita.com とすると所望のメールボックス宛に送信されるのも、DNS機能がインターネット の中にあるからです。

家庭内LANでは、「ワークグループ」や「ドメイン」として各パソコンには「コンピュータ名」を付けて ネットワーク化しており、DNSの一種のような「名前解決」を必要としています。これについては、次回の 「Windowsネットワーク」で説明します。

▲先頭へ

## 5．通信の仕組み--ＦＴＰ：ファイル転送プロトコルを例にとって

### ＦＴＰ（File Transfer Protocol）

今回の締めくくりとして、実際の通信において、ネットワーク機器の役割やIPアドレス、ポート番号等が どう係わっているのかを見てみましょう。私たちが日常的に使う通信は、メール

通信（SMTP/POP3）とウェブ閲覧通信（HTTP） ですが、ここではファイル転送通信（FTP：File Transfer Protocol）を取り上げます。

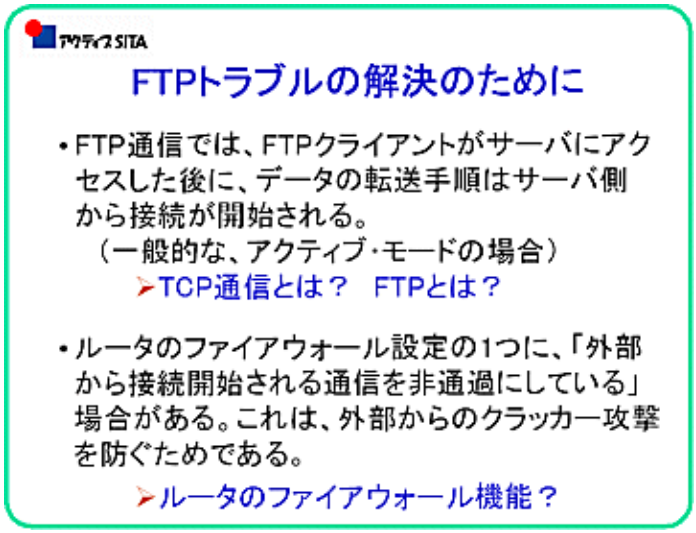
ISP（インターネット･サービス･プロバイダー）が提供するウェブ･サーバを用いて自分のホームページを公開している方は、 作成したホームページのファイルをアップロードする時などにFTPを使っているので、慣れていることと思います。我がアクティブＳＩＴＡでは効率的に活動を展開するため、サーバを介して様々なファイルを共有しており、会員はFTP通信でサーバにファイルのアップ／ダウンロードをしていますが、これまでに、うまくファイルのアップやダウンロードができないトラブルが幾つか発生しました。相当にエキスパート揃いのアクティブＳＩＴＡですが、FTPはHTTPやメールほど使い込まれていないためか、ちょっとした通信の仕組みを見逃していました。それらの問題を解決していく過程で、この通信の特徴とネットワーク機器の働きなどが良く理解されたので、その時のトラブル事例と問題解決は、通信とネットワーク機器の機能を説明するのに大いに役立つ教材だと思いました。

**・Ａさんからの連絡（問題発生時）**

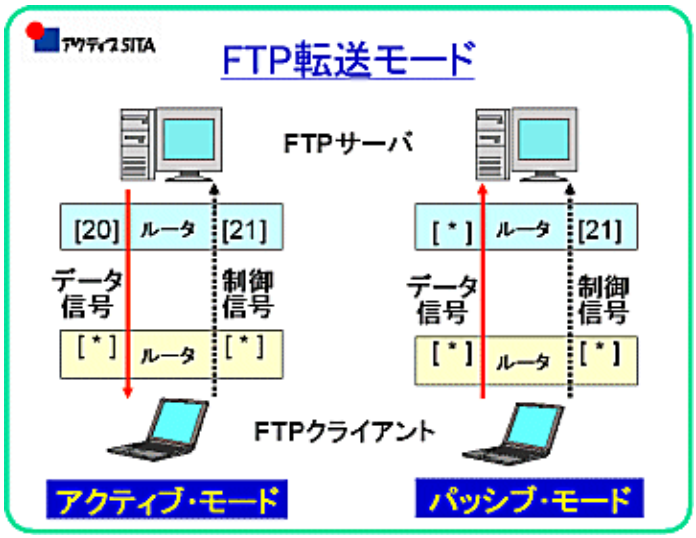
『今年になって１つのＩＳＰ経由でFTPサーバへ接続できなくなりました。ホームページビルダーのFTPツールでも、FFFTP（FTPクライアントソフト）でも駄目なのです。昨年は問題なかったのにどうしてでしょうか？ アクティブＳＩＴＡのメールもウェブへのアクセスも問題ないのですが。
また、他のISP経由でしたらビルダーのツールでもFFFTPも問題ありません。どうしてでしょう？』

**・Ｂさんからの連絡（問題解決時）**

『やっとFTPサーバにアクセスでき、問題が解決しました。 ADSLモデムのルータの「設定」オプションに、「IPフィルタ」という項目があり、そこに、フィルタする（通過／非通過）項目が登録されており、 その１つに「接続先から受信 0.0.0.0/0（送信元） 0.0.0.0/0（送信先）TCP-SYN（プロトコール）（ポート番号は＊） 非通過（アクション）」とあり、これが非通過に設定されていたので、FTPは受信できなかったようです。 これを「通過」に設定しろというプロバイダの指示でした。そこを変えただけでＯＫでした。 なぜそうなるかはよくわかりませーん!!! 』



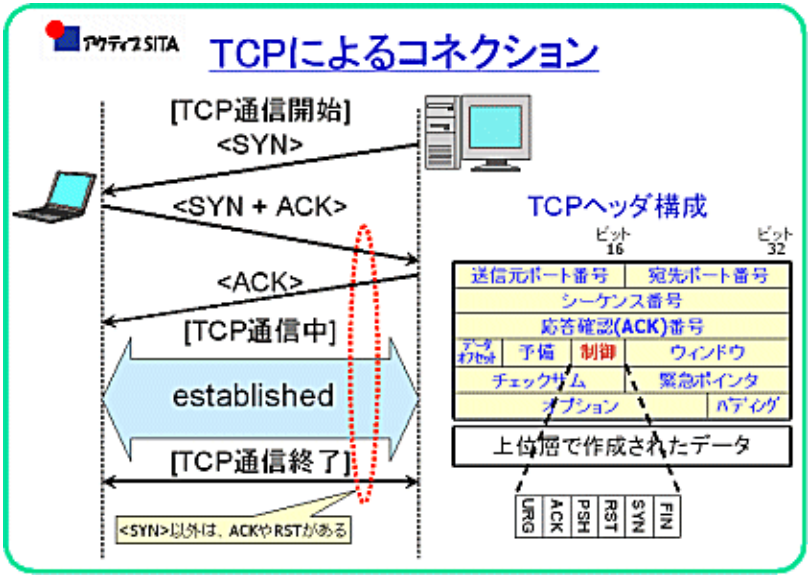

Ａさんは複数のISPに加入されており、それぞれにADSLモデムやケーブル（CATV）モデムでアクセスし、ルータも別々に設置しています。その内の一方がFTPを通すのに不具合となっている様です。しかも年を明けてから？そこで聞いてみると、昨年末にルータを置換したとのことでした。




ルータのメーカが設定している（あるいはISPの指示によるのか）、デフォルト設定で、FTP通信が不具合になるようなものがあります。FTPはクライアント側から起動しますが、次のステップのデータ伝送で、サーバ側から開始する方法をアクティブ･モード、クライアント側から開始する方法をパッシブ･モードといいます。Ａさんのルータは、アクティブモードのFTPを受付けない（ポート番号２１のFTP受信を拒否する）ように設定してあったのです。そこでパッシブモードに変えたら、うまくいきました。

Ｂさんの場合は、先に解決方法を記してしまいましたが、やはりルータでした。こちらのルータの設定は、もう少し特殊な厳しいもので、インターネット上の全てのところ（IPアドレス0.0.0.0/0の意味）からの、TCP-SYNというTCPヘッダー内の「TCP通信開始」信号（図参照）を拒否す

るように設定されていました。これは、外部からの「アタック」を警戒している設定で、一種のファイアウォールです。この場合、警戒をほどかなくても、やはりパッシブモードでFTPを開始すれば、ルータは通りました。




ルータは、「玄関や門扉」のようなもので、普段は出入りに便利な役割をしますが、一方で外部からの「侵入者」を警戒する役割もするため、必要な通信をも拒む場合もできてしまいます。ハブやブリッジでは、ファイア ウォール的な機能は設定できません。この辺りは大変重要で、もう一度、第5回の「ネットワーク･セキュリティ」の ところで述べましょう。

今回はネットワーク機器を中心に解説を試みましたが、如何でしたでしょうか？

では、次回にまたお会いしましょう。