2.3 TCP/IP

2.3.1 TCP/IP の構成要素

TCP/IP は、パソコンのネットワークで標準的に利用されているプロトコルです。

TCP/IP の実体は、多数のプロトコルの集合体です。そのため「TCP/IP プロトコル群」や「TCP/IP プロトコルスイート」と呼ばれることもあります。これらの名称は、TCP/IP が単独のプロトコルではなく、複数のプロトコルの集合体であることを明示的に示す場合に使われます。そのような必要性がなければ、単に「TCP/IP」と呼んでも問題はありません。

表 2.3-1 TCP/IP プロトコル群

OSI での階層	プロトコル		
アプリケーション層	HTTP	POP	SMTP
	FTP	RTP	SIP
プレゼンテーション層	DNS	DHCP	
セッション層			
トランスポート層	TCP	UDP	
ネットワーク層	IP	IPsec	
	ARP	ICMP	
データリンク層	PPP	PPPoE	
物理層			

■ 上位層（セッション層以上）のプロトコル

個々のサービスを実装するためのプロトコルです。Web ページの転送であれば HTTP、メールならば POP と SMTP など、用途によって利用するプロトコルが異なります。

■ トランスポート層のプロトコル

通信を行うプログラム間での通信を管理するプロトコルです。トランスポート層では、ネットワーク上で動作するアプリケーションを識別するために、ポート番号を使います。

トランスポート層には、TCP と UDP の 2 つのプロトコルがあります。TCP は信頼性を重視する場合に使われ、UDP は負荷の軽さや性能を重視する場合に使われます。上位層のプロトコルは、通信が要求する信頼性のレベルによって、TCP と UDP を使い分けます。たとえば、Web ページの転送やメールやファイル共有を利用する場合は、信頼性が高い TCP が使われま

す。動画や音声を利用する場合は、性能の高い UDP が使われます。また、管理用のプロトコルなどネットワークの負荷を小さくしたい場合も UDP が使われます。

■ ネットワーク層のプロトコル

通信を行うコンピュータ間での通信を管理するプロトコルです。コンピュータを識別するために、IP アドレスが使われます。

TCP/IP で中心的な役割を果たす IP は、ネットワークのプロトコルです。IP の他に、補助プロトコルとして、ARP や ICMP が使われます。ARP は、IP アドレスと MAC アドレスの対応付けを行うプロトコルです。また、ICMP は、接続確認を行うためのプロトコルです。

■ データリンク層のプロトコル

TCP/IP のプロトコルのほとんどは、ネットワーク層以上で動作します。少数ですが、データリンク層で動作するプロトコルもあります。ダイアルアップ接続で使われる PPP や、ブロードバンド接続で利用される PPPoE などが該当します。

2.3.2　IP アドレスとサブネットマスク

■ IP アドレスとネットワーク機器の関係

IP アドレスは、ネットワークインターフェイスを識別するための番号です。ネットワーク層のプロトコルである IP プロトコルで使われます。

IP アドレスは、ネットワーク機器を識別する番号のように説明されることもありますが、正確にはネットワーク機器を識別するための番号ではなく、ネットワークインターフェイスを識別するための番号です。この違いは、1 つのネットワーク機器が、複数の IP アドレスを持つ場合に現れます。たとえば、有線 LAN と無線 LAN が使えるパソコンでは、それぞれのインターフェイスが異なる IP アドレスを持ちます。そのため、1 つのパソコンが 2 つの IP アドレスを持つことになります。このように、ネットワーク機器と IP アドレスの関係は、1 対 1 でないこともあります。

このように、IP アドレスからネットワーク機器を識別することはできますが、ネットワーク機器の IP アドレスは 1 つには決まりません。

■ IP アドレスのクラス

よく見かける IP アドレスは、「192.168.0.1」のような形式をしています。ドット“.”で区切られた数値は、0 ～ 255 の値をとります。0 ～ 255 は、2 進数で示せば 8 桁分の範囲です。言い換えれば、8 ビットの数値です。IP の実体は、8 ビットの数値が 4 組セットになった、32 ビットの数値です。

では、なぜ IP アドレスは、32 ビットの数値をわざわざ 4 組に分けているのでしょうか。これは、IP アドレスを 2 つのパートに分けて使うためです。2 つのパートは、例えるならば人間の名前の姓と名です。IP アドレスの前半のパートは、企業や団体などのコンピュータやネットワーク機器の集団を識別します。これを「ネットワーク部」と呼びます。IP アドレスの後半のパートは、企業や団体などの中で個々のコンピュータやネットワーク機器を識別します。これを「ホスト部」と呼びます。「ホスト」という言葉は、TCP/IP の世界では「コンピュータやネットワーク機器」と同義語と考えてください。

これからは、IP アドレスのネットワーク部が同じであるコンピュータやネットワーク機器の集団を「ネットワーク」と呼びます。ネットワークは、人間で言うならば同姓の家族と考えてください。

ところで、IP アドレスを 2 つに分けるだけならば、ドット“.”は 1 つでもよいはずです。ドット“.”が 3 つあるのは、ネットワークの大きさ、言い換えれば企業や団体の規模によって、IP アドレスの境目を使い分けようという目的があるためです。

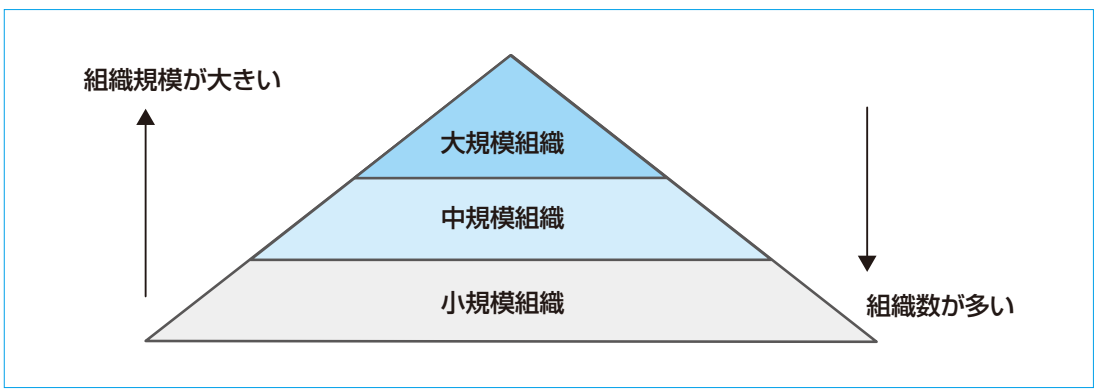

図 2.3-1 IP アドレスのネットワーク部の考え方

大規模組織では必要とされる IP アドレス数は多くなりますが、大規模な組織は小規模な組織にくらべて数は多くありません。大企業の事業者数は中小企業の事業者数より、はるかに少ないのです。逆に、小規模組織では必要とされる IP アドレスは少なくて済みますが、

組織数が多くなります。そこで、組織規模によってネットワーク部とホスト部の境目を変えて利用するために、ドット “.” が３つもあるのです。

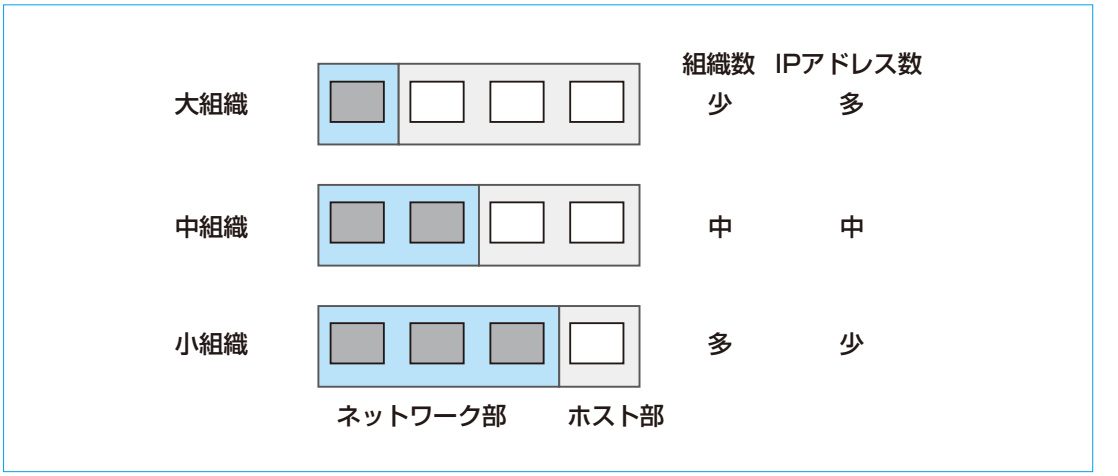

図 2.3-2 IP アドレスの構成

この IP アドレスが想定している３つの組織規模は、クラスと呼ばれます。

	ネットワーク部	ホスト部
クラス A	8 ビット	24 ビット
クラス B	16 ビット	16 ビット
クラス C	24 ビット	8 ビット

高度な IP アドレスの設計を行う場合は、クラスの３分類では不足するため、さらに細かい分割方法をとることもあります。この手法は、**CIDR** と呼ばれます。また、クラスを使わないことを意味する「クラスレス」という言葉で、呼ばれることもあります。これに対して、クラスを利用する方法を「クラスフル」と呼びます。

クラスレスの IP アドレスは、小規模のネットワークではあまり利用されません。そのため、パソコン整備士２級では、クラスフルの IP アドレスのみを扱います。

NOTE

CIDR：Classless Inter-Domain Routing、「サイダ」と読みます。

コラム：IPv6

IP アドレスは、32 ビットのデータです。では 32 ビットで識別できる数は、どれくらいあるのでしょうか。答えは、2 の 32 乗= 4,294,967,296 で、約 43 億になります。実は、地球人類が IP アドレスを 1 個ずつ使うと、IP アドレスは足りなくなってしまうのです。現在、TCP/IP ネットワークが活用されていない国や地域があるので 43 億個の IP アドレスで足りていますが、今後インターネットがますます普及すれば、いずれは使い切ってしまうのは必至です。これは、IP アドレスの枯渇問題と呼ばれます。

そこで、次世代の IP プロトコルとして登場したのが、IPv6 です。現在の IP プロトコルはバージョン 4 で、IPv4 になります。バージョン 5 は特別な用途に使われるプロトコルなので、IPv4 の次は IPv6 になりました。

IPv6 の最大の特徴は、IP アドレスが 32 ビットから 128 ビットに拡張された点です。128 ビットで識別できる数は、次のような膨大な数になります。

340,282,366,920,938,463,463,374,607,431,768,211,456

この IPv6 によって、アドレスの枯渇問題は根本的に解決される見通しになっています。

IPv6 の特長は、アドレス数だけではありません。セキュリティの向上や、通信性能や通信品質の向上、また情報家電を想定したアドレスの自動付与機能の実装など、さまざまな改良が図られています。

そして、すでにさまざまなネットワーク機器が IPv6 に対応しています。Windows でも IPv6 を利用できます。IPv6 は、使おうと思えばいつでも使える技術的環境は整備されています。しかし、IPv6 は広く普及しているとは言えない状況です。

なぜ、IPv6 の利用は広がらないのでしょうか。IP アドレスの枯渇問題への対応も、セキュリティの向上も、その他の IPv6 のメリットも、ほとんどがネットワーク設計者やネットワーク管理者に対するメリットなのです。ウェブサイトの運営者にとっては、IPv4 でアクセスされることを前提にしているアプリケーションの変更が必要になる場合があり、IPv6 に移行する影響が大きいためです。そのため、大企業で利用されることはあっても、個人や小企業レベルまでは広がっていません。

今後、IPv6 の普及のために、IPv6 の特長を生かしたアプリケーション（「キラーアプリケーション」と呼ばれます）の登場が期待されています。

■ サブネットマスク

サブネットマスクは、ネットワーク部とホスト部の境目を示す数値です。IP アドレスと同じような形式で、255.255.255.0 などの数値が使われます。

では、なぜサブネットマスクが必要になるのでしょうか。ここまでに、IP アドレスがネットワーク部とホスト部の 2 つに分かれること、そして IP アドレスを利用する組織の規模によってク

ラスを使い分けることを説明しました。ここで必要になるのは、3 つのドット“.”のどれを境目としているか、言い換えれば IP アドレスがどのクラスに属するかを判別する方法です。IP アドレスの説明では、ネットワーク部とホスト部を名前の姓と名に例えました。人間の名前ならば、姓と名の間に空白を入れて区別できます。そのため同じ漢字の並びでも、正しく区切ることができます。たとえば「金田一正」という名前は、空白を入れることによって、「カネダ カズマサ」なのか「キンダイチ タダシ」なのか区別がつくのです。しかし、IP アドレスではすべて同じドット“.”で区切っているために、区別がつきません。そこで、サブネットマスクが必要になるのです。

クラスフルの IP アドレスの場合、サブネットマスクのルールは単純です。ネットワーク部に相当する部分は 255、ホスト部に相当する部分は 0 とするだけです。

例 1　IP アドレス　192.168.0.1　　サブネットマスク 255.255.255.0
ネットワーク部は“192.168.0”で、ホスト部は“1”

例 2　IP アドレス　10.128.0.1　　サブネットマスク 255.0.0.0
ネットワーク部は“10”で、ホスト部は“128.0.1”

IP アドレスとサブネットマスクを併記する場合には、区切りとしてスラッシュ“/”を使うのが一般的です。したがって、上の例 1 の IP アドレスとサブネットマスクは、
192.168.0.1/255.255.255.0 のように記述します。

サブネットマスクには、もう 1 つの書き方があります。

クラス A	10.0.0.1/255.0.0.0	10.0.0.1/8
クラス B	172.16.0.1/255.255.0.0	172.16.0.1/16
クラス C	192.168.0.1/255.255.255.0	192.168.0.1/24

新しい書き方のスラッシュ“/”の後ろは、ネットワーク部のビット数を示しています。たとえば、クラス C ではネットワーク部が 8 ビットを 3 組使っているので、24 ビットです。スラッシュ“/”の後ろは、正確には「プレフィクス値」と言います。単に「マスク」と呼ばれることもあります。この場合は、「マスクが 24 ビット」などと表現されます。

当初、サブネットマスクは、サブネットワークにおけるネットワーク部とホスト部を示すために使われていました。サブネットワークとは、ネットワークの中に作られた、さらに小さいネットワークです。たとえば、会社全体のネットワークの中に、部門ごとのネットワークを作ったも

のがサブネットワークです。しかし、ネットワークの中のパソコンから見れば、自分の属するネットワークがサブネットワークであっても全体的なネットワークであっても、大きな違いはありません。そのため、サブネットマスクはネットワーク部とホスト部の境目を示すために一般的に使われるようになりました。同時に、「サブネットマスク」は「サブ」を付けずに「ネットマスク」と呼ばれることもあります。

■ 特別な IP アドレス

パソコンに割り当てる IP アドレスを設計する場合には、IP アドレスの特別ルールに注意する必要があります。これから紹介する IP アドレスは、個々のコンピュータやネットワーク機器に割り当てることはできません。

表 2.3-2 特別な IP アドレス

名称	意味	192.168.0.0/255.255.255.0 のネットワークでの例
ネットワークアドレス	ネットワーク全体	192.168.0.0
(ディレクテッド) ブロードキャストアドレス	ネットワーク内の全ホスト	192.168.0.255
(リミテッド) ブロードキャストアドレス	全ホスト	255.255.255.255
ループバックアドレス	自ホスト	127.0.0.1

ネットワークアドレスは、ネットワーク全体を示す IP アドレスです。個々のホストに割り当てることはできません。ネットワークアドレスは、ネットワーク構成図を書いたり、パケットの転送先を指定したりする場合などに使われます。

ブロードキャストアドレスには、2 種類あります。範囲を特定のネットワークに限定したディレクテッド ブロードキャストアドレスと、範囲を特定のネットワークに限定していないリミテッド ブロードキャストアドレスです。ブロードキャストとは「放送」を意味します。どちらも複数のホストを一度に指定する点が共通しています。通常、この 2 つはどちらも「ブロードキャストアドレス」と呼ばれます。明示的には区別されないことが多いので注意が必要です。

ディレクテッド ブロードキャストアドレスは、ネットワーク内のすべてのコンピュータやネットワーク機器を示す IP アドレスです。ネットワーク内のすべてに対して問い合わせを行う場合などに使われます。たとえば、ARP というプロトコルはディレクテッド ブロードキャストアドレスを使います。**ARP** は、IP アドレスに対応する MAC アドレスを調べるプロトコルです。

NOTE

ARP：Address Resolution Protocol

ARP はネットワーク内の全ホストに対して MAC アドレスを一度に問いかけるために、ディレクテッド ブロードキャストを使います。

リミテッド ブロードキャストアドレスは、特定のネットワークに限定されないブロードキャストアドレスです。IP アドレスを持つすべてのホストが対象になります。たとえば、**DHCP** は、リミテッド ブロードキャストアドレスを使います。DHCP は、IP アドレスなどのネットワーク設定を自動的に行うためのプロトコルです。DHCP によってネットワーク設定を行うパソコンは、自分の IP アドレスを持っていないため、ネットワークが限定されるディレクテッド ブロードキャストは使えません。そのため、リミテッド ブロードキャストによって全ホストに対して、ネットワーク設定値を要求するパケットを送信します。

どちらのブロードキャストも、特別な処理をしない限り、ルータを越えて他のネットワークに送られることはありません。そのため、ネットワークを分割することにより、ブロードキャストによるネットワークの負荷を減らすことができます。

ループバックアドレスは、いつでも自分自身を示す IP アドレスです。人間で言えば、一人称と考えてください。「私」は誰が使っても自分を示します。これと同じように、127.0.0.1 は、192.168.0.1 のパソコンでも、10.0.0.1 のパソコンでも、自分のパソコンを示します。自分自身のサービスが動作しているか確認したり、自分自身のサービスに接続する場合に利用したりできます。127.0.0.1 という IP アドレスはよく利用されるため、通常は「localhost」というホスト名でアクセスできるようになっています。ループバックアドレスで重要なのは、IP プロトコル内だけで処理される点にあります。ハードウェアには一切関係しないのです。そのため、ループバックアドレスはハードウェアがどのような状況でも、IP プロトコルが正常である限りは使えます。ケーブルが切断されていても、LAN カードが装着されていない場合でも、127.0.0.1 だけは利用できます。もし、127.0.0.1 が利用できない状況であったら、それは IP プロトコルの異常です。

■ グローバルアドレスとプライベートアドレス

IP アドレスは、ネットワークインターフェイスを識別するための番号です。そのため、重複があってはなりません。外部とは独立したネットワークであれば、ネットワーク内で重複しないように IP アドレスを設定すれば問題は起きません。しかし、インターネットでは簡単にはいき

NOTE

DHCP：Dynamic Host Configuration Protocol
NIC：Network Information Center
「ニック」と読みます。なお、LAN カードを意味する Network Interface Card も NIC と略されますので、注意してください。

ません。インターネットは、多数のネットワークが相互に接続しているためです。そこで、インターネット上で重複のない IP アドレスを利用するために、**NIC** という機関が IP アドレスの管理および割当てを行っています。インターネットにコンピュータやネットワーク機器を直接接続する際には、NIC に申請して IP アドレスの割当てを受ける必要があります。この NIC から割当てを受けたインターネット上で利用できる IP アドレスを、「グローバルアドレス」と呼びます。

なお、日本国内における IP アドレスの割当ては、NIC の下部組織である JPNIC が行っています。利用者からは大手 ISP が IP アドレスの割当てをやっているように見えます。これは、利用者の利便性を向上させるため、大手 ISP では IP アドレスをあらかじめ割り当ててもらい、その中から契約者に IP アドレスを付与しているからです。どのような形態で IP アドレスが付与されても、インターネットに直接つなげられる IP アドレスは、グローバルアドレスだけであることには変わりありません。

このグローバルアドレスに対して、「プライベートアドレス」があります。これは、インターネットに直接つなげない限り、自由に使ってよい IP アドレスです。

クラス A	10.0.0.0	～	10.255.255.255
クラス B	172.16.0.0	～	172.31.255.255
クラス C	192.168.0.0	～	192.168.255.255

では、なぜプライベートアドレスが必要なのでしょうか。

インターネットと接続されていないネットワークを考えてください。このようなネットワークは外部のネットワークと、IP アドレスの重複を心配する必要はありません。そのような場合でも NIC に申請して IP アドレスの割当てを受けることは、非常に非効率的です。また、申請を受ける側の NIC も非効率的です。そこで、インターネットに直接つなげないことを条件に、自由に利用できる IP アドレスが定められています。これがプライベートアドレスです。

インターネットにつなげないならば、どの IP アドレスを使っても問題なさそうです。しかし、実際にはプライベートアドレスの範囲が定められています。これは、なぜでしょうか。

これは、「アドレス変換」という技術を使えば、プライベートアドレスでも間接的にインターネットとつなげられるからです（アドレス変換については後述）。もしプライベートアドレスの範囲を定めずに自由に使えるルールにすると、アドレス変換の機能に不具合が生じたときに問題が起きます。内部ネットワークに設定した IP アドレスが、世界のどこかの IP アドレスと重複してしまう可能性があります。このように、アドレス変換に不具合が起きたときでも問題にならないように、プライベートアドレスの範囲が定められているのです。

また、外部とつないでいないネットワークであっても、いつネットワークの利用形態が変化して、インターネットにつなぐことになるかもしれません。したがって、たとえ外部と隔離されているネットワークであっても、プライベートアドレスを使うルールになっているのです。

■ アドレス変換

インターネットに接続するためには、NIC に申請が必要なグローバルアドレスが必要です。しかし、私たちが使っているパソコンに、グローバルアドレスが割り当てられていることは、めったにありません。プライベートアドレスが割り当てられていることがほとんどです。これは、アドレス変換と呼ばれる技術によって、プライベートアドレスでもインターネットに接続できるようにしているからです。アドレス変換技術は、家庭向けのブロードバンドルータでも実装されており、日常的に利用されています。

では、アドレス変換のしくみについて説明する前に、アドレス変換の必要性について説明します。まず、アドレス変換を使わずに、すべてのパソコンにグローバルアドレスを割り当てることを考えます。この場合は、さまざまな問題が発生します。

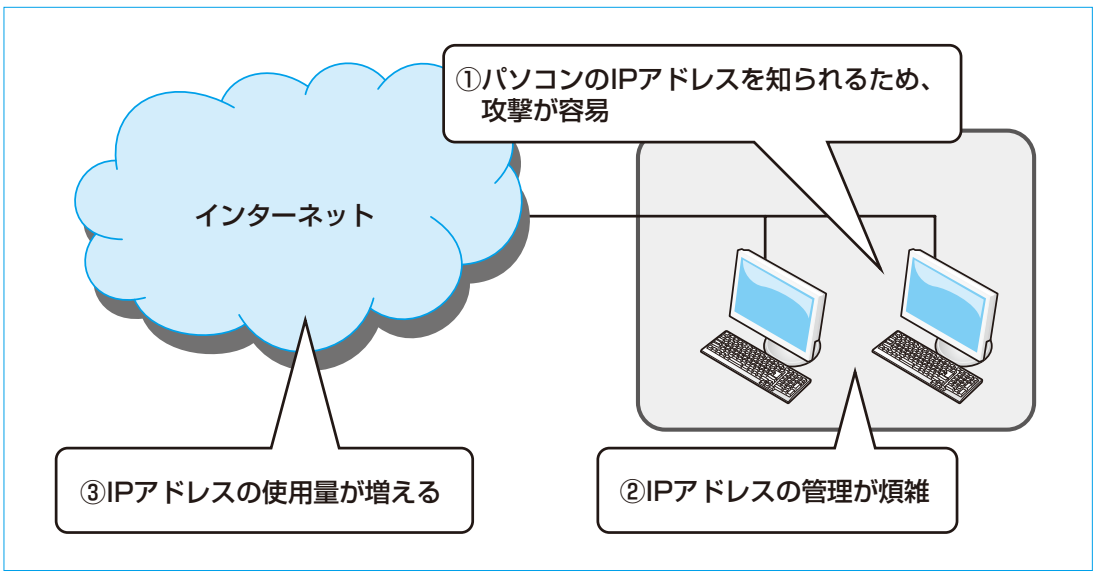

図 2.3-3 グローバルアドレス割当で発生する問題

まず、第一はセキュリティの問題です。グローバルアドレスを使えば、インターネット上にパソコンの IP アドレスが知られることになります。そのため、攻撃者にとっては目標を特定しやすくなり、攻撃しやすくなるのです。

第二は、IP アドレス管理の問題です。グローバルアドレスを利用するためには、NIC に申請しなければなりません。IPv6 が普及しておらず IPv4 のアドレス枯渇問題があるので、IP アドレスは必要最小限の分が付与されます。もし、ネットワークが拡張されパソコンが増えた場合、新たに IP アドレスを付与するための申請が必要になります。また、新たに付与された IP アドレスは今までと同じ範囲とは限りませんので、場合によってはすべての IP アドレスを変更しなくてはなりません。

第三は、IP アドレスの使用量の問題です。これは、上の 2 つと異なり、ネットワークを利用する側には直接関係しない社会的問題です。IPv4 の IP アドレスは現在、世界的に不足しています。この状況下で、大企業が社内のパソコンにグローバルアドレスを割り当てると、大量にグローバルアドレスを消費することになります。内部ネットワークでグローバルアドレスを利用することは、アドレス枯渇問題にますます拍車をかけてしまうのです。

これらの問題を解決するのが、アドレス変換技術です。アドレス変換は、外部ネットワークへの通信を行う際に、送信元のプライベートアドレスをグローバルアドレスに変換します。このグローバルアドレスは、外部のネットワークとの境界に置かれるルータの、外側のインターフェイスに割り当てられた IP アドレスです。

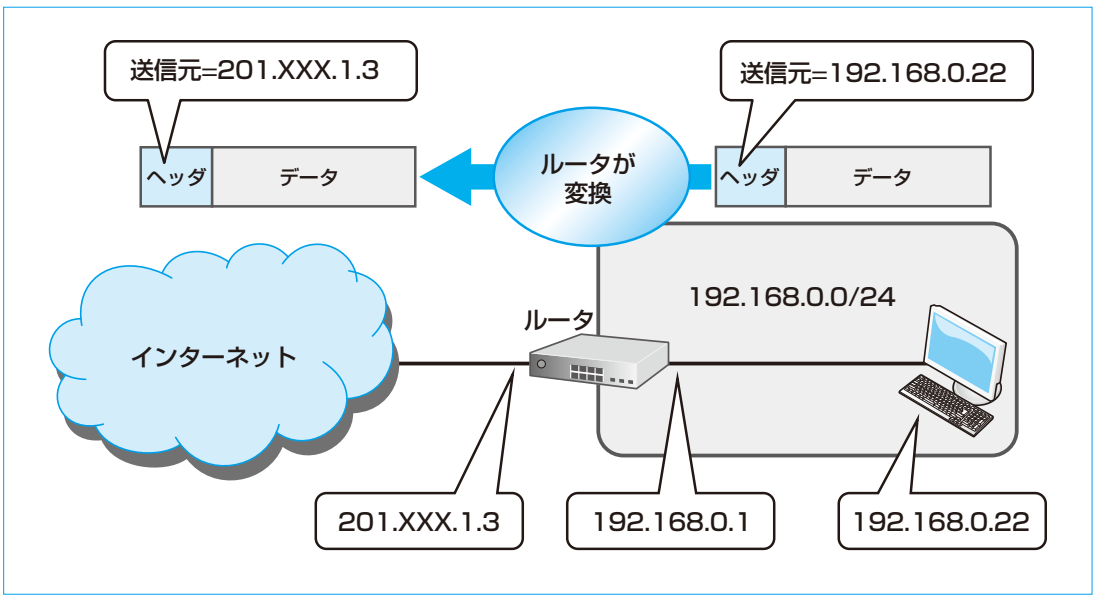

図 2.3-4 アドレス変換

アドレス変換を使うと、インターネット上のホストから見れば、送信元はすべてルータになり

ます。ネットワーク内部のパソコン等のIPアドレスは、インターネットから見えなくなります。これにより、第一の問題点であるセキュリティの問題が解決できます。なお、外部からIPアドレスを隠せることを「IPアドレスの隠蔽」と呼ぶこともあります。

また、ネットワーク内部はすべてプライベートアドレスを使っているので、アドレスは自由です。プライベートアドレスの範囲を使っている限り、NICへの申請は不要です。そのため、IPアドレスの管理の問題も解決できます。

そして、アドレス変換を使うと、ネットワーク内部のホストが複数であっても、利用する**グローバルアドレスは１個**です。そのため、IPアドレスの利用量も節約できます。

このように、アドレス変換を使えば、グローバルアドレスを使う場合の問題点が解決できます。アドレス変換は、「**NAT**」や「IPマスカレード」と呼ばれることもあります。以前は、グローバルアドレスとプライベートアドレスの対応が、1対1と1対多によって言葉を使い分けていました。1対1の場合はNAT、1対多の場合がIPマスカレードです。通常は、これらの言葉を厳密に区別して使うことはありません。1対1のアドレス変換は、あまり使われなくなっているからです。「アドレス変換」「NAT」「IPマスカレード」は、ほぼ同義語として使われています。なお、1対多のアドレス変換であることを明示する場合には、「**NAPT**」という言葉も使われます。厳密には、IPマスカレードはNAPTのひとつになります。しかし、IPマスカレードが最も著名なNAPT技術であるため、アドレス変換を示す一般用語として利用されています。

2.3.3　インターネット接続のための設定

ここでは、パソコンがインターネットに接続するために必要な、最低限の設定について説明します。パソコンがインターネットに接続するためには、次の4つの設定が必要になります。

IPアドレスとサブネットマスク
デフォルトゲートウェイ
DNSサーバのIPアドレス

NOTE

グローバルアドレスは１個：　大規模なネットワークでは、複数のルータを使ったり、１つのルータで複数のグローバルアドレスを使ったりすることもあります。本書では小規模のネットワークを扱っているので、グローバルアドレスは１個としています。
NAT：Network Address Translation、「ナット」と読みます。
NAPT：Network Address Port Translation、「ナップティー」または「ナプト」と読みます。
DNS：Domain Name Service