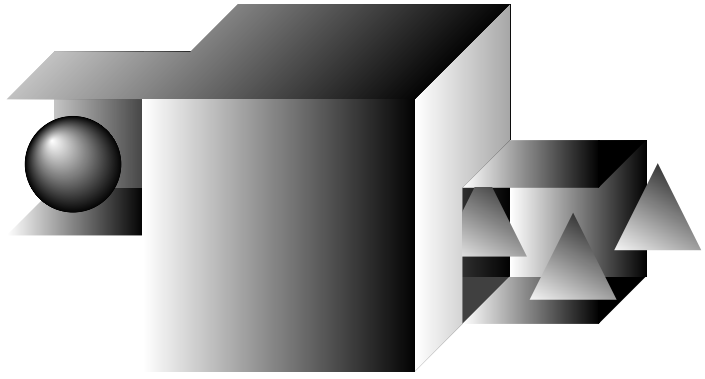
インターネット最新テクノロジー：第17回

プライベートアドレスで透過的にインターネットと通信できる

アドレス変換

数少ないIPアドレスを使ってインターネットにたくさんのホストを接続させたい。SOHO環境ではこういった問題に突き当たることが多い。これを解決する方法の1つがNATやIPマスカレードといった技術である。これらはプライベートIPアドレスをグローバルIPアドレスに変換する仕組みを実現することによって、IPアドレスの無駄使いを防ぐことができる。今回はアドレス変換技術を実装したNATとIPマスカレードについて解説し、さらにNATやIPマスカレードの拡張部についても触れてみたい。

恒成 英一（mgicho@fsi.co.jp）
富士ソフトABC株式会社技術調査室
テクニカル・アナリスト



枯渇するIPアドレス

現在使用されているIPアドレスはIPv4（Internet Protocol Ver.4）で定義されているものである。32ビットのIPアドレスでは約40億のIPアドレス空間が確保できる。定義された当時は32ビットのアドレスにより世界中のどのコンピュータとも通信できると考えられていた。実際、この頃のコンピュータは非常に高価であり、どこにでも存在するものではなかったうえ、個人で所有するケースは希であった。また、この頃のネットワークの接続形態はUUCPである場合が多かったため、IPアドレスを使用する局面はそう多くなかった。

ところがWWWの普及により爆発的にインターネットに接続されるコンピュータが増加するようになると、サービスを提供するために多くのホストが追加されていった。おそらくIPv4を設計した人の想像をはるかに超える増加数であろう。

IPアドレスを必要とするホストの増加により深刻な問題が浮上してきた。IPアドレス枯渇の問題である。実際にはまだすべてを使いきっているわけではないが、枯渇は時間の問題となっている。

透過的な通信を可能にする

IPアドレス枯渇の問題を解決するためにIPv6への移行が計画されている。しかし突然移行できるものではないので、現状ではIPv4の範囲内でいろいろな策が打たれている。

まずNICはクラスBのIPアドレスの発行を停止した。そしてRFC1519によるCIDR割り当てを開始した。

急成長し、不幸にもクラスBのIPアドレスを必要とする企業があったとする。しかし、今ではクラスBの割り当ては行われていない。この企業内で使用するIPアドレスの道は1つしかない。RFC1597によるプライベートIPアドレスを使うことである。ところが、プライベートIPアドレスはあくまでも閉じたネットワークでの使用を目的としており、インターネットでは使えない。さらに、異なるネットワークからも接続できないのである。

この問題の解決方法としてプライベートIPアドレスを持つホストからプロキシーを経由してインターネット上のホストと通信することが考えられる。ただし、プロキシーを経由すると透過的に通信できないことが多い。そこで、プライベートIPアドレス空間をグローバルIPアドレス空間に対して透過的に接続させようという方法が考えられた。RFC1631によるNAT、そして今回取り上げるIPマスカレードがそれである。

外部からアクセスできるNAT

NATとは、IPアドレス空間においてパブリックIPアドレス空間とプライベートIPアドレス空間を接続するための技術である（1997年1月号参照）。このNATの機能が持つ通信機

TECHNOLOGY

器を「NAT BOX」と呼ぶ。

プライベートIPアドレス空間からグローバルIPアドレス空間へパケットを投げた場合を考えてみよう。

このパケットの始点アドレスは構内ネットワークのプライベートIPアドレスであるが、このパケットをそのままグローバルIPアドレス空間であるインターネットには流せない。そこでNAT BOXにルーターとしての機能を持たせ、NAT BOXの変換テーブルに従ってグローバルIPアドレスに変換した後、インターネットに流す。返信パケットも同様に、NAT BOXがグローバルIPアドレスをプライベートIPアドレスに変換して構内ネットワークに流す（図1）。

NATが有効な局面としては、ネットワークアドレス空間を分けているときに外部から内部へのアクセスも可能にする場合である。IPアドレスが一対一に割り当てられているため、接続を許可するかどうかのポリシーは別として、原理的に外部からの接続もできるのである。

SOHO環境に有効なIPマスカレード

IPマスカレードを説明する前に簡単にNATについて触れたのは、IPマスカレードとNATが非常に似ているからである。特に、IPマスカレードはIPアドレスの枯渇問題に対応するためのものであり、IPアドレスの付け替えを行うというただ一点において、NATとほぼ同じものを目指しているといえる。またNATがグローバルIPアドレスとプライベートIPアドレスとのアドレス変換を行う機能を提供していることに対し、IPマスカレードではUDPとTCPのポート番号の変換までも行っている。

IPマスカレードはUDPとTCPのポート番号の変換を行うことにより、1つのグローバルIPアドレスにプライベートIPアドレスを持つ複数のホストを割り当てることができる（図2）。これに対しNATではIPアドレスの対応はあくまでも一対一である（図3）。

IPマスカレードでは、プライベートIPアドレ

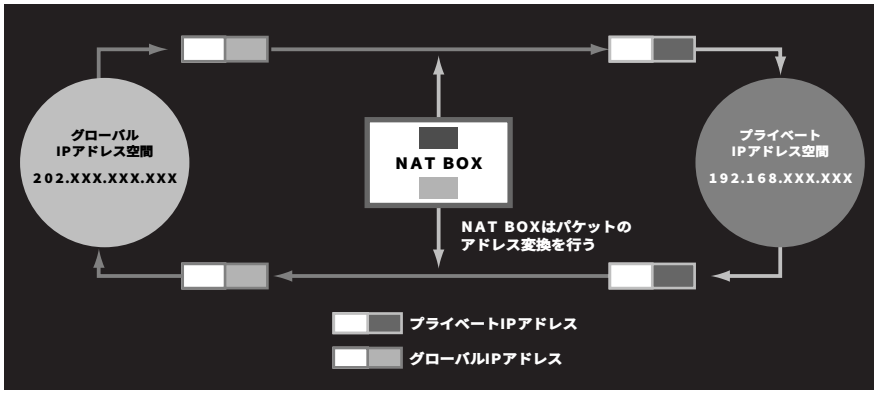


図1　アドレス変換の仕組み

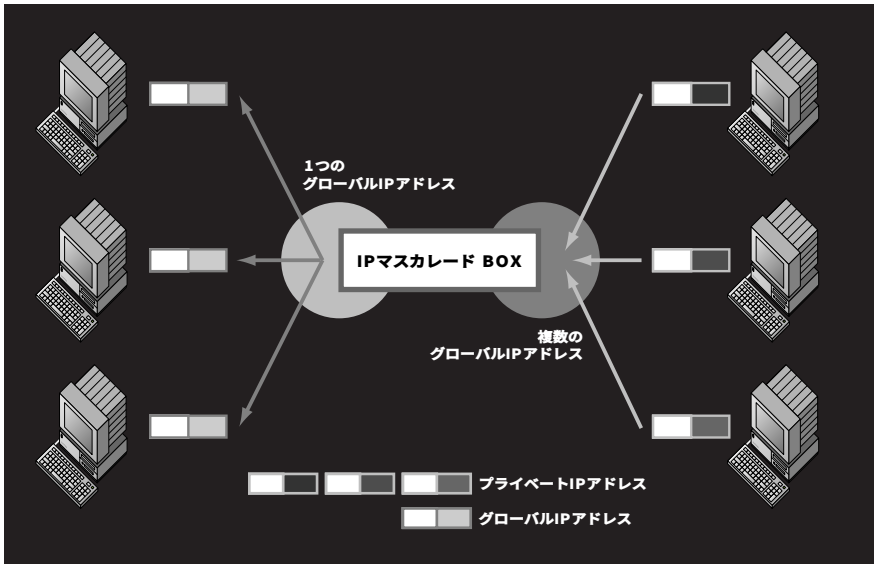


図2　IPマスカレードの仕組み

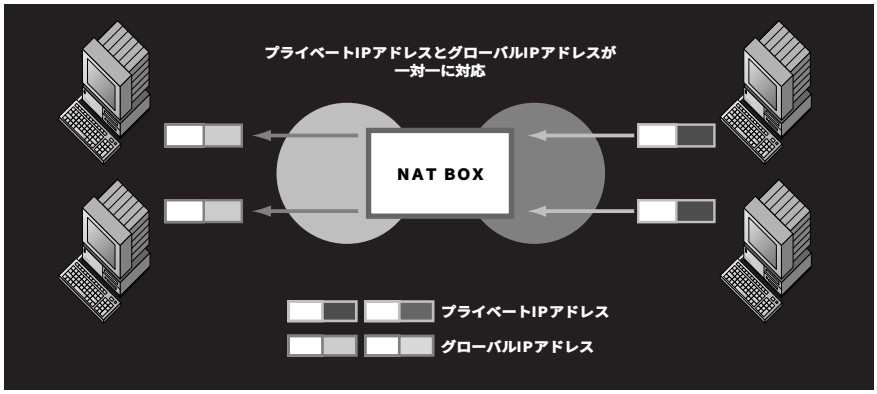


図3　NATの仕組み

スを持つ複数のホストが1つのグローバルIPアドレスでインターネットに出て行くことができる。しかし次に記述する問題点の項で挙げているように、その逆は容易でない。

家庭やSOHO環境などのように、外部から接続することが少なく、なおかつ限られたIPアドレスを使用して複数のホストがインターネットの世界に出て行く場合には、IPマスカレードが有効な局面となるのである。

企業内のネットワークにおいて、そのホストに対する社外からの接続がなく、社外に出るのみであれば、少なくとも1つのグローバルIPアドレスを使用するだけで済む。外部に対して公開する必要があるメールやWWWなどのサーバー以外のホストにグローバルIPアドレスを割り当てるなどという無駄なことは少なくなるのである。

もちろん、予算の関係やISPのようにプライベートIPアドレスを割り振ることが難しい場合もあるだろう。必要なところに必要に応じて割り振るということが重要なのである。

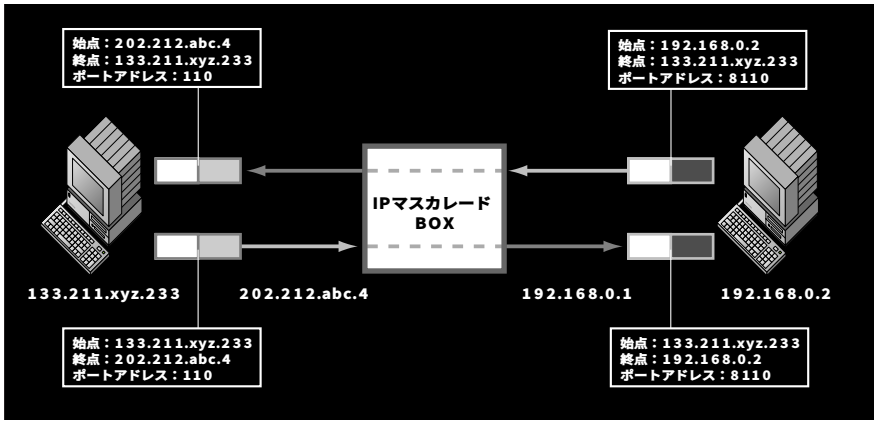


図4　IPマスカレードの動作

	NAT	IPマスカレード
ネットワークの変更	○	△
LAN環境での端末型IP接続	×	○
外部からの接続	○	×
IPアドレスの節約	△	○

○：適している
△：やや適している
×：適していない

図5 NATとIPマスカレードの機能比較

IPマスカレードの動作原理

IPマスカレードの動作原理に関して、誌面の都合上詳細にわたって説明することができないため、詳細に関しては、たとえばLinuxのカーネルソースなどを追いかけていただきたい。ここでは、簡単な考え方のみ解説する。

IPマスカレードの動作を一言で書くならば、IPパケットの始点アドレスと終点アドレスを書き換えているということである。

通常はこの始点アドレスと終点アドレスにより、IPパケットを受け取ったホストは送信元の始点アドレスを参照して応答パケットを送出する。グローバルIPアドレスを持つホストからプライベートIPアドレス側にあるホストに対して応答パケットを送出する段階になって、初めて送出元のIPアドレスが見えなくなる。IPマスカレードではグローバルIPアドレス側のホストにIPパケットを送る際、始点アドレスをIPマスカレードが動いているホストのグローバルIPアドレス側のネットワークインターフェイスに割り当てているIPアドレスに書き換える。これにより、相手側のホストからもIPパケットが戻ってくることになる（図4）。これに加えて、UDPとTCPのポート番号の変換を行うのである。

もちろん実際の動作はこのように単純ではないが、まずは単純なイメージで理解し、各種資料やソースコードを参照するといいだろう。

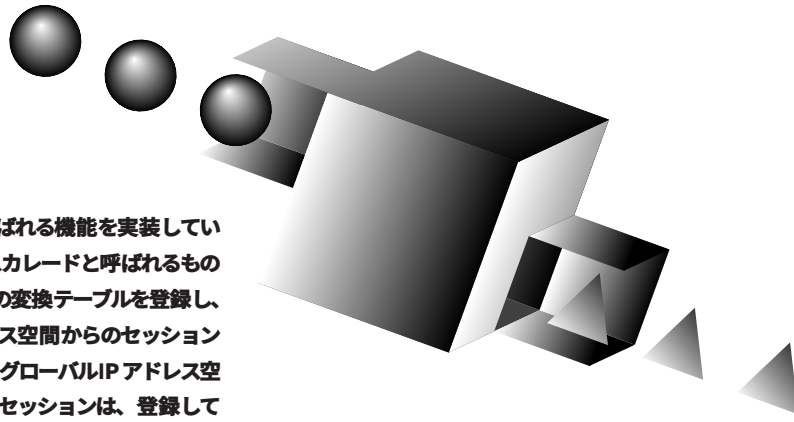
ポート番号変換における問題

IPマスカレードはポート番号を変換する点において、NATでは問題とならなかった部分が主に問題となる。

▶ICMP

ICMPはポート番号の概念がないので取り扱えない。たとえばpingが通らないといった問題が発生する。

NATの場合ではグローバルIPアドレスとプライベートIPアドレスは一対一になっている



ため、ICMPエコーなどのグローバルIPアドレス空間から到達するパケットの配送先の識別を行うことは可能である。しかしIPマスカレードではIPアドレスが一対一ではないため、どのホストにリレーすべきパケットであるのかが判断できない。なおこの問題に対して、機能の拡張を行うことによりICMPを通すように実装しているものもある。

▶ マイクロソフトネットミーティング

複数のポート番号を動的に使用しているため、基本的には利用できない。

▶ r コマンド

rshやrloginなどのrコマンドで使われるプロトコルは、クライアント側のポート番号がウェルノウンポート（プロトコルによって割り当てが決められているポート）の範囲内である必要がある。そのため、ポート番号を変換してしまうIPマスカレードでは利用できない。

▶ FTP

通常、データコネクションはftpd側から張り、なおかつセッションごとにポート番号を変更するため、原則としては利用できない。ただし、実装によっては可能となる。

▶ 外部からの接続

グローバルIPアドレスからのアクセスができない。これはある意味においては「軽いセキュリティー」であるともいえる。ファイアーウォールといえるかどうかは意見の分かれるところである。

NATの拡張とIPマスカレード

最近のISDNルーターに実装されている「NAT+」では、今までできないことも少しずつ可能になってきているので、そのうちにRFCに反映されるときが来るであろう。

たとえばヤマハのISDNルーターでは、NATとIPマスカレードをうまく組み合わせて静的IPマスカレードと呼ばれる機能を実装している。この静的IPマスカレードと呼ばれるものは、IPマスカレードの変換テーブルを登録し、グローバルIPアドレス空間からのセッション開始も可能になる。グローバルIPアドレス空間側から開始されたセッションは、登録しておいた変換テーブルを参照し、一緒に登録しておいたプライベートIPアドレスを持つホストへIPパケットを振るという処理を行う。

図5にNATとIPマスカレードについて目的に応じた主な機能の比較をまとめてみる。

大規模サイトでの用途は未知数

IPマスカレードによって、内部ネットワークにあるホストは透過的に外部と接続できる。これまで、SocksやRemote Windows Socketsのように透過型プロキシーと呼ばれる仕組みがあったが、アプリケーションの対応やSocksCapのように工夫が必要である場合が多かった。IPマスカレードは、この面倒な部分を省いてしまう。

現在のところ、大企業などでIPマスカレードを導入しているところは多くないであろう。しかし、「部」単位で導入しているケースは少なくない。全体で導入されることが多くない理由は、数十万ホストを抱えるサイトで運用に堪えられるかどうかの実績を持っていないという点が挙げられる。IPマスカレードの実装によってこの上限は変わってくるが、パフォーマンスチューニングにも関係してくる。ただし、IPマスカレードではポート番号の変換を行うため、最大数は4096となる。

現在では主に小規模なサイト、特に家庭やSOHO環境では多くの実績を持ち、絶大な効果を上げている。だからといって小規模サイト向けのものであると早合点しないでいただきたい。あくまでも大規模サイトにおける用途は未知数なのである。

●

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp