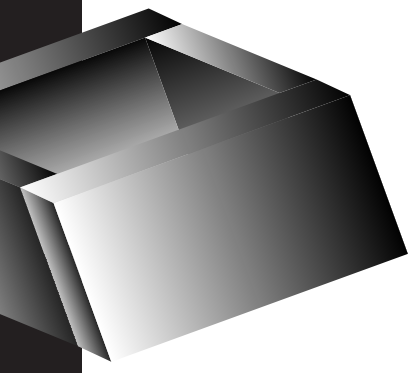
INTERNET

インターネット最新テクノロジー：第２回

IPアドレスの枯渇をくいとめる！
NAT（Network Address Transrator）

最近、ダイアルアップルーターのカタログに「NAT」という文字をみかけるようになった。ダイアルアップルーターは本来、LANにつながった複数のコンピュータから同時にインターネットにアクセスするために使う機器であり、多くのユーザーが使っている「端末型ダイアルアップ接続」ではつなぐことができない。しかし、「NAT」に対応しているダイアルアップルーターは、端末型接続ができる。一体「NAT」とはどのような機能なのか、また何のために使うものなのだろうか。本稿では「NAT」のしくみと今後の動向について説明したい。

鈴木淳一郎
suzuki jyunichiro



NATとはアドレス変換機能のこと

NAT（ネットワーク・アドレス・トランスレーター）とは、IPアドレス空間において、グローバルアドレス空間とプライベートアドレス空間を接続するための技術である。グローバルアドレス空間とはすなわちインターネットのことであり、これに対してプライベートアドレス空間はスタブエリアと呼ばれる（RFC1631で規定されている）。

グローバルアドレス空間とプライベートアドレス空間の間に立ち、NATの動作を行うユニットは、一般には「NAT box」あるいは「NAT箱」と呼ばれている（図1）。

NAT箱がIPアドレスを付け替える

NAT箱はお互いの空間から見れば、まさにルーターとして見える。しかしながら、NAT箱は単なるルーターとは異なり、IPアドレスの付け替えを行う。

たとえば、インターネットにスタブA、Bの2つが接続されているとしよう（図2）。スタブA、BはそれぞれNAT箱A、Bでインターネットに接続されており、スタブ内部ではともに「10.0.0.0/8」というプライベートアドレスを用いているとする。また、スタブAではインターネットに接続するためのグローバルアドレスとして「aaa.bbb.ccc.ddd」を、スタブBでは「eee.fff.ggg.hhh」を利用しているとする。このとき、スタブA内のホストA（10.33.96.5）から、スタブB内のホストB（10.81.13.22）にパケットを投げようとすると、以下のような動作となる。

（1）ホストAは始点IPアドレスを10.33.96.5に、終点IPアドレスをeee.fff.ggg.hhhに設定したパケットをNAT箱Aに投げる
（2）NAT箱Aはパケットの始点IPアドレスをaaa.bbb.ccc.dddに変換してインターネットへ送り込む
（3）インターネットからパケットを受け取ったNAT箱Bは、終点IPアドレスを10.81.13.22に変換する
（4）ホストBがパケットを受け取る

すなわち、NAT箱は、プライベートからグローバルの方向に対しては始点IPアドレスを、逆にグローバルからプライベートの方向に対しては終点IPアドレスを変換する。このIPアドレス変換こそがNATの基本である。

NATの動作に関して、NAT箱以外のホストAとBやインターネット内のルーターなどは特別なことは何もいらないのに注目してほしい。面倒なことはすべてNAT箱が引き受け、その他のユニットにはソフトやハードを含めて何の変更もいらないところは、NATの大きな利点の1つだ。

NAT箱はさまざまな働きをする

NAT箱は単にIPヘッダー内の始点や終点のIPアドレスを書き換えていればよいだけではない。IP/UDP/TCPのチェックサムの再計算やFTPのPORTコマンドの引数および「PASV」コマンドの戻り値の変換、エラー通知のための「ICMP」パケットに含まれるIP

TECHNOLOGY

図1：NATはプライベートアドレスをグローバルアドレスに変換する機能

アドレスの変換などをする。このほかにIPアドレス情報を含むプロトコルがあれば、そのIPアドレス情報も変換する。

以上のうち、チェックサムの再計算は必須である。しかし、ICMPに関しては事実上、処理は不要である。厳密なチェックを行うホストはほとんどない。

FTPの場合は面倒な調整が行われる

FTPの場合、「PORT」コマンドの引数に、あるいは「PASV」コマンドの戻り値にIPアドレスが文字列として書かれている。このIPアドレスがもしプライベートアドレス空間のものであれば、NAT箱はそれをグローバルアドレス空間のものに変換しなくてはいけない。文字列であるIPアドレスを変換すると、パケット長が変化することが問題となる。たとえば、先の例のホストAでは、スタブA内でのプライベートアドレスは10.33.96.5で10オクテット、グローバルアドレスはaaa.bbb.ccc.dddで15オクテットとなり、変換後のパケット長は5オクテット長くなる。FTPはTCP上で実現されているため、パケット長が変化すると、TCPのシーケンス番号に調整が必要となる。これ以上はTCPについての予備知識がないと理解できない話になってしまうので深入りするのはよすが、とにかく、NATでFTPを扱うのは面倒だということだけは理解して欲しい。

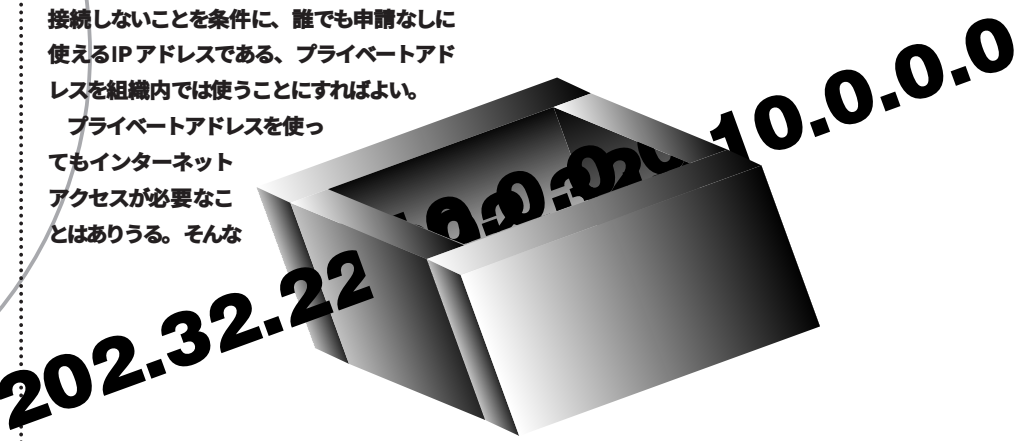
NATはIPアドレス枯渇とセキュリティーのために必要

それでは、なぜNATが必要になるのだろうか。1つにはIPアドレスの枯渇問題がある。

現在、インターネットで使われているIPはバージョン4であるために、「IPv4」と呼ばれる。IPv4は1970年代に設計され、当時は、IPアドレスとして32ビット、4億台が識別できるというスペックは十分なものに思われた。

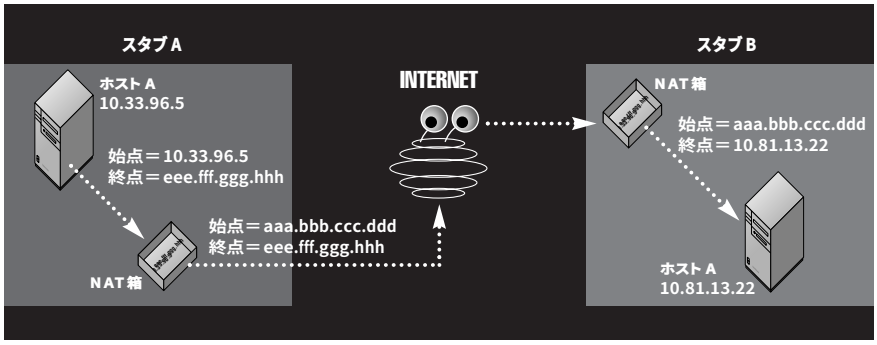
しかし、インターネットの急成長とそれに引き続くイントラネットブームはIPアドレスの枯渇という深刻な問題を引き起こした。組織内のホストのうち、本当にインターネットとの間で通信が必要なものは限られている。特にイントラネットとしての利用であれば、多くのホストは組織内のサーバーと通信できればそれで十分だ。そこで、インターネットと接続しないことを条件に、誰でも申請なしに使えるIPアドレスである、プライベートアドレスを組織内では使うことにすればよい。

プライベートアドレスを使ってもインターネットアクセスが必要なことはありうる。そんなときに、NATを使えるようセットアップしておけば、他のソフトやハードを変更することなく、かなり自由にインターネットにアクセスできる。

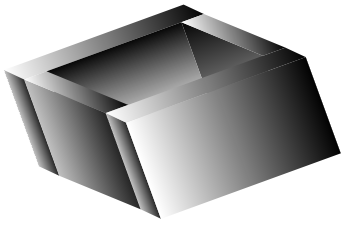


NATを使うもう1つの大きな理由として、セキュリティーの問題がある。インターネットに接続するということは世界中からのアクセスを受け入れるということである。そのため、不正にアクセスされる機会も増える。

図2：NATのしくみ



NATを用いて重要なホストはプライベートアドレスにしてしまえば、たとえ物理的につながっていたとしても、インターネットからはアクセスできない。仮にアクセスされたとしても、必ずNAT箱を通っているはずなので、そこでアクセスコントロールが可能となる（図3）。



NATではできないこともある

NATはアドレス変換という、IPではそもそも想定していないことを行う技術である。そのため、いくつか無理も生じる。NATで問題となるのは2点ある。1つはダイナミックルーティングができないことである。IPv4がインターネットになったことの理由の1つにダイナミックルーティングが基本であることがあげられる。しかし、NATを使う場合には、ダイナミックルーティングの恩恵にはあずかれない。手動設定が必要となる。

2点目は、少ないグローバルアドレスである。NATを用いる場合、利用できるグローバルアドレスの数はプライベートアドレス空間にあるホストの数よりは少ないのが普通だ。しかし、同時アクセス数はグローバルアドレスの数に制限される。

極端な例として、端末型ダイアルアップ接続にNATを適用することを考えてみる。端末型ダイアルアップ接続では、PPPのIPCPによりIPアドレスが1つだけ端末側に割り当てられる。しかし、これではインターネットにはホスト1台しか接続できない。せっかくNATを使っているのに、そうではないときと事態が変わらない。

図3：NATによるセキュリティー

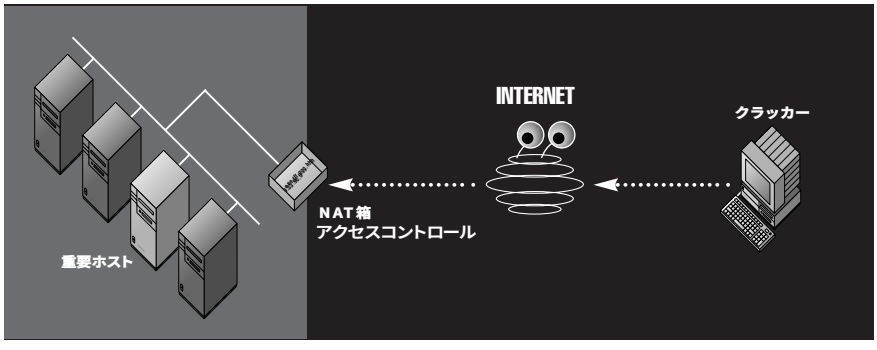
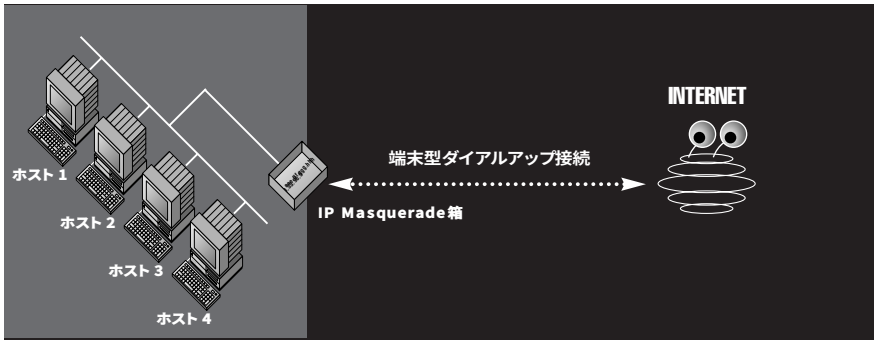


図4：IP Masqueradeのしくみ

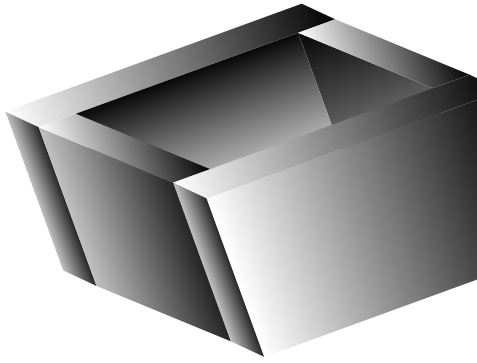


IPMasqueradeを使えば複数のマシンからアクセスできる

NATとよく似た技術として、IP Masquerade（アイ・ピー・マスカレード）がある。IP Masqueradeは、Linuxに実装されたのがおそらく最初で、IPアドレスに加えて、TCP/UDPのポート番号も変換してしまうことで、1つのグローバルアドレスで複数のホストをインターネットにアクセスできるようにする技術のことである。IP Masqueradeを用いると、NATではできなかった、端末型ダイアルアップ接続でLANをインターネットに接続することが可能となる（図4）。

IP Masqueradeの特徴は何といっても1つのグローバルアドレスで複数のホストが接続できることだ。その代わりに、TCP/UDPポート番号を変換するためにできないことも多くある。以下ではNATではできるが、IP Masqueradeでは不可能なことをあげてみよう。まずは「ICMP」。IP Masqueradeでは、ポート番号によりスタブ内のホストを識別する。そのため、ポート番号を持たない「ICMP」は利用できない。ICMPが使えないと、場合によってはネットワーク動作に重大な支障を

▼



きたすことがある。また、pingが使えないことを忘れているとテスト中に頭がパニックすることがある。

次に、インターネット側からのアクセスにも不具合が生じる場合があるという点だ。インターネット側からアクセスされる場合、最初のパケットはインターネット側からやって来る。グローバルアドレスとプライベートアドレスが1対1で対応するNATであれば、そのような場合でもパケットの配送先が分かるが、IP Masqueradeの場合は1対1対応ではないため、どのホストにパケットを送るべきかの判断がつかない。

3つめとして、rsh系（rsh、rlogin、rcp）のコマンドやlprが使えないことがあげられる。rsh系のコマンドで使われるプロトコルやlprで使われるLPRプロトコルでは、クライアント側のポート番号の値が1023以下のWELL KNOWNポートであること（本当はもっと範囲は狭い）が要求される。そのため、ポート番号を変換してしまうIP Masquerade越しにはこれらは利用できない。

NATやIP Masqueradeは便利な機能であるが、ある程度無理をする技術でもあるので、種々の制約が付きまとう。そのことをしっかり理解したうえで利用していきたいものである。

NATを実際に使うには・・・編集部

■機器はダイアルアップルーターが必要

NATを使用するにはまずNATに対応したダイアルアップルーターが必要である。NAT対応のダイアルアップルーターにはヤマハ株式会社の「RT100i」や株式会社メルコの「LBR-64」などがある。また、アセンド・コミュニケーションズ・ジャパンの「パイプライン25-Px」は独自のアドレス変換機能を備えているが、「NATを内包している」と同社では謳っている。また、セイコー電子工業株式会社の「NS-2480」もNATを拡張した独自のアドレス変換機能を持っており、FTPが確実に行える機能を持っている。また、RT100iと200iは次のファームウェアのバージョンアップで、今回解説した「IP Masquerade」という機能が使えるようになる。

■ISDNの契約と同期64Kbps接続が可能なプロバイダーに加入しよう

前述したダイアルアップルーターはどれもISDNの同期64Kbpsでの接続を前提にしているので、ISDNへの契約が必要だ。また、同期64Kbpsで接続できるプロバイダーにも入らなければならない。契約は端末型ダイアルアップ接続で構わない。

■ネットワークボードとイーサネットケーブルも必要

さらに、ダイアルアップルーターにはイーサネットで接続するので、ネットワークボードを装着し、イーサネットケーブルでつながなくてはならない。ネットワークボードは1万円台で購入できる。ケーブルも短いものなら1,000円程度だ。これらの機器については先月の特集でも紹介したので、今回は省略させていただく。

NAT機能を持つダイアルアップルーター

品名	発売元会社名	価格	問い合わせ先電話番号
RT100i	住商マシネックス中部株式会社	198,000円（キャンペーン価格）	052-963-2188
Pipeline25-Px	アセンド・コミュニケーションズ・ジャパン株式会社	オープンプライス（100,000円前後）	03-5325-7397
NS-2480	セイコー電子工業株式会社	98,000円	0120-234-288
LBR64	株式会社メルコ	98,000円	052-619-1825
ROUTE101	ビー・ユー・ジー株式会社	198,000円	03-3486-6710
AR-600	株式会社東芝	110,000円（DSU・アナログポート無しモデル）	03-3457-3301

●

［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