第5章 プライベート・アドレスとグローバル・アドレスを変換して世界中のホストとパケットを送受信する

ステップ④…IPアドレスを変換するNAT

柚山 大哉

表1　特定のアドレス範囲はプライベート・ネットワーク用のアドレスとして割り当てられている
このプライベート・アドレスとグローバル・アドレスの変換にNATの技術が使われる

アドレス・ブロック	個　数
10.0.0.0/8	16777216
172.16.0.0/12	1048576
192.168.0.0/16	65536

本章では，NAT（Network Address Translation）というIPアドレスを変換する技術をルータ・プログラムに実装します．

NATはIPアドレスを変換する技術の総称で，多くの種類があります．

- 送信元IPアドレスを変換するSNAT（Source NAT）
- 送信先IPアドレスを変換するDNAT（Destination NAT）
- IPアドレスだけでなく，ポート番号も書き換えNAPT（Network Address Port Translation）
- IPv6とIPv4を変換するNAT64

本章では，家庭用ルータなどでよく使用されている，送信元IPアドレスと送信元ポートを書き換える変換技術「NAPT」を実装します．また，ここから「NAT」は「NAPT」のことを表すことします．

IPアドレスやポート番号を変換する「NAT」

■ 基礎知識

● NATはグローバル・アドレスの共有に使える

現在，インターネットで使用されているIPv4で用いられるIPアドレスは，32ビットで表されるので，2^{32}個，約40億台ほどのホストしか表せません．これだと世界の人口よりも少ないので，1人当たり1つの世界でユニークなIPアドレスを使うと足りなくなります．実際に，IPアドレスの管理を行う団体であるIANAのIPアドレスの在庫は枯渇し，新たなアドレスを払い出せない事態となっています．

▶特定のアドレス範囲はプライベート用として割り当てられている

組織に割り当てられない特定のアドレス範囲をプライベート・アドレスとして割り当て，その範囲を全世界のプライベート・ネットワークで使用すれば，グローバルなアドレスを消費しないようにできます（**表1**）．しかし，プライベート・アドレスのままではインターネットの通信には利用できません．なぜなら，インターネットでは一意なアドレスでないと通信できないからです．

ここで，インターネットに出ていくときにNATが活躍します．複数のプライベート・アドレスと1つのグローバル・アドレスを変換するのにNATを使用しています．

▶インターネットに出るときに送信元IPアドレスとポート番号を一意に変換

プライベート・ネットワークからインターネットにパケットを送るとき，IPアドレスと送信元ポート番号を変換して送出します．このとき，送信元ポート番号は重複しないように書き換えられます．

ただIPアドレスを書き換えるだけだと，通信相手からのパケットが返ってきたときに困ります．コンピュータの通信は基本的に双方向で行われるので，相手からインターネットを経由して入ってくる通信も考慮しなければなりません．そこで，TCPやUDPパケットの送信元ポートをステートフルに記録して，戻ってきたパケットを適切にローカル・ネットワークに転送します．

● ICMPパケットをNATで変換する方法

ICMPは，IPパケットをカプセル化して送受信するプロトコルですが，ポート番号を持っていません．ICMPのクエリ・パケット（Echo Request/Reply）は，idという数字も持っていて，これをポート番号の代わりに使えます．

ICMPのエラー・パケットは，エラーとなったパケットのIPヘッダと先頭8バイトを含んでいます．これを解釈するとエラー・パケットをNATで扱えるようになりますが，処理が煩雑になるので，今回は実装しませんでした．