



ざっくりわかる  
Tracerouteの作り方

# インターネット プログラミング

ダイヤモンドブリコット電話研究所

山崎 はるか

YAMAZAKI, Haruka

<http://www.nda.co.jp/>

第12回

Pingを使ったツール  
~Tracerouteの作り方

.NET Framework 2.0では、System.Net.NetworkInformation名前空間が新設された。この名前空間のメンバのうちの一つ“Pingクラス”は、Pingに特化して作られたクラスである。もちろんメソッド一発で使えるほど甘くはないが、作法さえ守れば誰でも使いこなせる便利な存在である。今回はPingクラスとICMP.DLLを比較しながら、それぞれでPingクライアントとTracerouteを作り、基本動作をマスターしておこう。

## TTLってなに？

カンタンなPingについては、本誌2005年12月号で述べているので、今回は少し詳細な部分を中心に解説させてもらうことにしよう。

RAW (ナマ) パケットを射出するとき、IPアドレス/メッセージタイプなどと共に必ず指定するのがTimeOutとTTL。

TimeOutはmsecで指定するので、「相手の応答を待つ時間」というのはすぐにわかる。しかしTTLってなんだろうか。

TTLとはTime To Liveの略。「有効回数」(生存期間)のことである。ここでいうTimeは時間のことではなく「回数」と解釈したほうがよい。

じゃあ、その回数とはなにか。

インターネットでは、送出されたパケットがいつまでもネットワークに滞留しないように、RFC791にてIPパケットに寿命カウンタを設けている。これがTTLである(図1)。

図2のように、ゲートウェイ/ルータを通過(ホップ)するたびにTTLは削られ、「0」になると消失したことを差し出し元に通知する(Time Exceededメッセージ)。

Pingでは、TTLの値を「255」(最大値)にして送る。目的のホストの途中で破棄されては困るからである。

しかしTracerouteは、これを逆手に取る。つまりわざとTTLを小さい値にして、途中のノード(ルータなど)にTime Exceededを送らせるのである。返信パケットにはTime Exceededを発信したノードのIPが入っているので、

レベル >>> Level

1 2 3 4 5

言語 >>> Language

▪ Visual Basic  
▪ C/C++

ツール >>> Tool

▪ Visual Studio .NET 2003  
▪ Visual Studio 2005

サンプル >>> Sample

この記事で取り上げたソースコード  
およびサンプルプログラムは、  
<http://www.shoeisha.com/mag/windev/>  
からダウンロード可能です。

図1：ICMPデータグラム

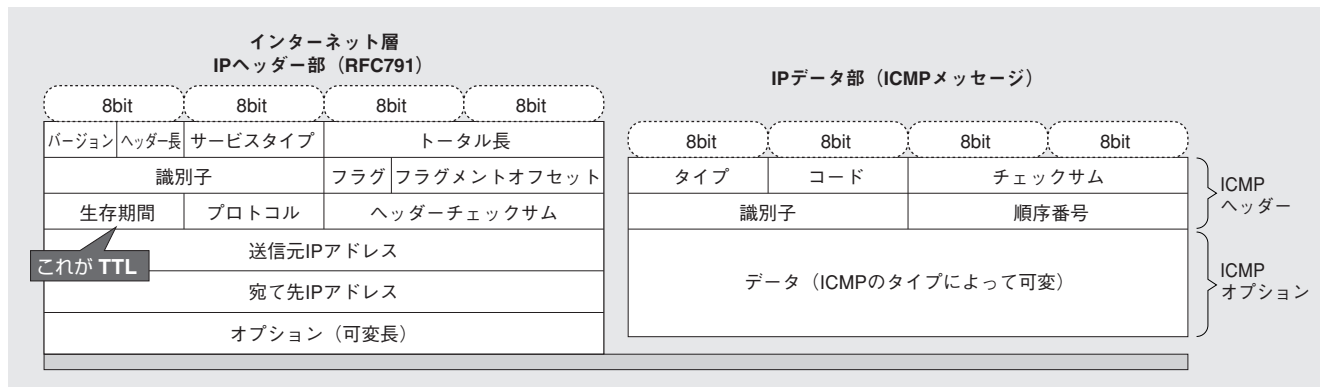
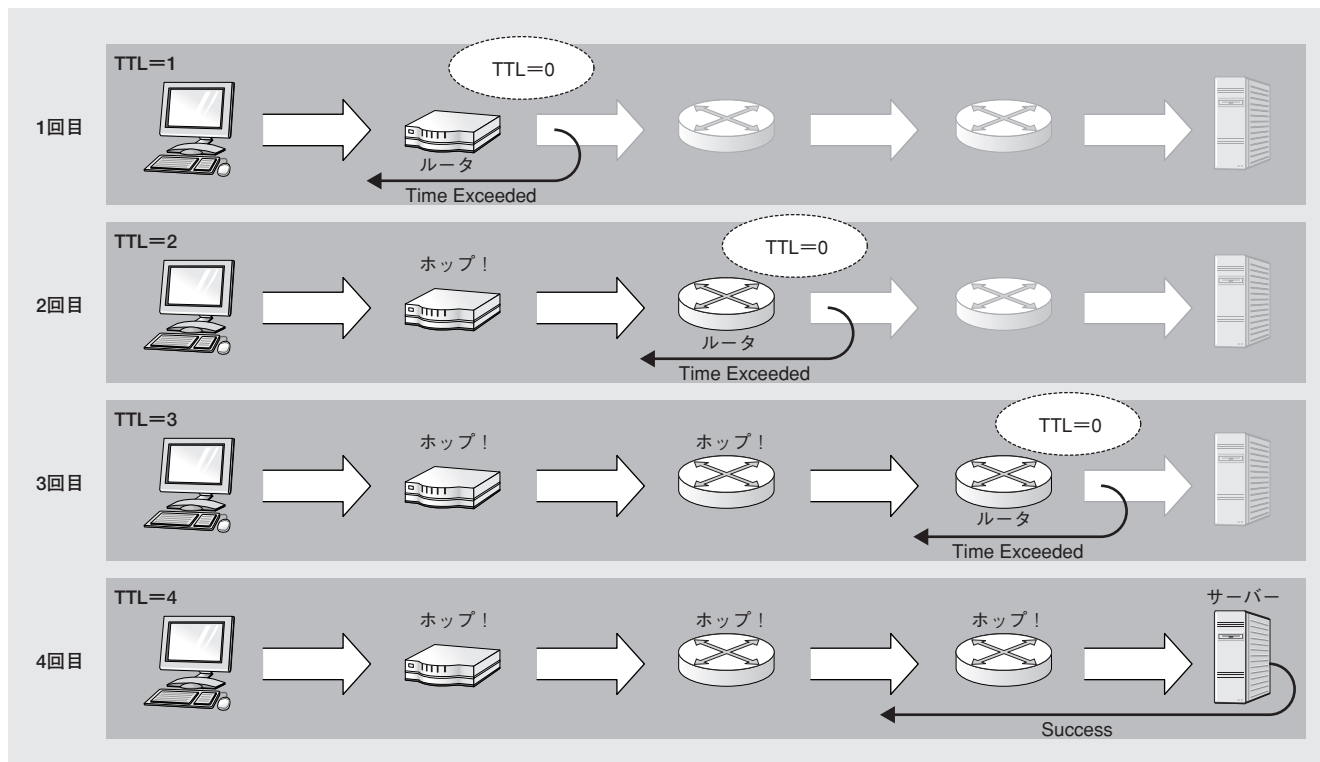


図2：Tracerouteの原理



中継点がわかる。

Tracerouteの原理は、TTL値を「1」にしてパケットを送出することからはじめ、次にTTL=2、TTL=3と増やしてパケットを送出することにより、目的のノードまでのルート情報を調べられるのである。

つまり、

- TTLを最大値「255」にして打ち出すのがPing
- TTLを「1」から順番に増やしてゴールまで打ち続けるのがTraceroute

と考えればよいだろう。



最初にPingクライアントを作ってみよう。