ダウンロード・データあります

パケットづくりではじめるネットワーク入門

第7回　パケット操作用基本ツール群pkttoolsの機能

坂井 弘亮

本連載はネットワーク上を流れるパケットを直接扱うようなツールを自作しつつ，ネットワークの仕組みを勉強していきます．テーマは「自作」「現物ベース」「動く感動」の三つです．ネットワークにはイーサネットとIPを想定しています．

● 今回行うこと

連載の第6回（2016年1月号）までは，ARPのやりとりを行うライブラリを実装し，自作のping送信と応答ツールを作成しました．また，確認にはpkttoolsというツールを使ってきました．

pkttoolsは筆者が開発しているパケット送受信用のツール群です．パケットを操作するためのさまざまな機能を持っており，連載中で作成するツールの動作確認のために引き続き利用していきます．

今後のためにpkttoolsの使い方について説明します．pkttoolsは本誌2014年8月号の特集で説明しましたが，対象バージョンが1.1と少し古くなっています．現在はさまざまな機能が追加されているため，ここで詳細に説明します．

最新版パケット操作ツールpkttools

pkttoolsはネットワーク・パケットを操作するためのフリー・ソフトウェアです．以下の特徴があります．

- テキスト・ベースのツールであり，CUIで操作する
- 単体のツールではなく，さまざまな操作を行うツール群になっている
- それぞれのツールをUNIXパイプで接続し，組み合わせて使用する
- スクリプトなどと組み合わせて処理がしやすい作りになっている

pkttoolsは下記のウェブ・ページからダウンロードできます．

```
http://kozos.jp/software/
```

執筆時点の最新版は，pkttools-1.9です．従来はFreeBSD/Linux用でしたが，最新版のpkttools-1.9からはWindows版も同時に配布されており，Windows環境でも利用できます．

なおパケットを直接扱うため，ネットワーク上で不用意に利用するとさまざまな影響を与えたり，問題となったりする可能性があります．勉強や検証を目的として，ローカル・ネットワーク上で利用するか，ネットワーク管理者の許可を得た上で，動作を正しく理解した上で利用してください．

● ビルドする

FreeBSD/Linux環境ではpkttools-1.9.zipを取得して，以下のようにしてビルドすることができます．

```
% wget␣http://kozos.jp/software/pkttools-1.9.zip↵
% unzip␣pkttools-1.9.zip↵
% cd␣pkttools-1.9↵
% make↵
```

Windows環境では配布サイトからpkttools-1.9-win.zipを取得してください．解凍すると，ビルド済みの実行ファイルがあります．実行ファイルの一覧を**表1**に示します．また，ツールのオプションの一覧を**表2**に示します．

アーカイブを解凍するとREADMEというファイルがあり，ツールに関する詳細な説明があります．疑問点があれば，そちらも参照してください．

パケット送受信機能

パケットの送受信はpkt-send/pkt-recvによって行いますが，利用前にいくつかの準備があります．

● FreeBSDでのみ必要な準備

FreeBSD環境ではパケットの送受信にBPF（Berkeley Packet Filter）を利用するため，次のように，/dev/bpfを読み書き可能にしておきます．Linux/Windows環境では不要です．

```
# chmod␣666␣/dev/bpf↵
```