ダウンロード・データあります　ご購入はこちら

パケットづくりではじめる ネットワーク入門

第28回　汎用パケット操作ツールpkttoolsの新バージョン

坂井 弘亮

本連載ではパケットの操作のために「pkttools」という筆者自作のツールを利用しています．pkttoolsについては一度連載で説明していますが（第7回，2016年2月号），そこからバージョンも上がっており，新しい機能も追加されています．そこで今回は最新のpkttoolsについて，新たに追加されている機能などを紹介します．

パケット操作ライブラリ pkttools新バージョン

● 特徴＆入手方法

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，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で操作をする
- 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，組み合わせて使う
- スクリプトなどと組み合わせて処理がしやすいような作りになっている
- FreeBSD/Linux/Mac OS X/Windowsなど，さまざまな環境で利用できる

以下からダウンロードできます．

```
http://kozos.jp/software/
「簡易パケット操作ツール群（pkttools）」
```

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て，動作を正しく理解した上で利用してください．

● 新たに追加された機能

連載の第7回で紹介したときのバージョンはpkttools-1.9でしたが，本稿執筆時点での最新版はpkttools-1.16です．pkttools-1.9からpkttools-1.16までの間には，以下の機能が追加されています．

- pkt-recvに-soオプションを追加（送信パケットのみ受信する）
- 共通オプションとして-nb/-nmを追加（ブロードキャスト・マルチキャスト・パケットを無視）
- pkt-analyzeに-ll/-lh/-lvオプションを追加（解析する層やレベルの指定）
- pkt-analyzeでペイロードのダンプの表示を追加（解析レベル5で表示）
- PcapNGに対応（pkt-pcapng2txt/pkt-txt2pcapng）
- IPv4/IPv6フラグメント・パケットの分割・再構築に対応（pkt-fragment/pkt-defragment）
- TCP/UDP通信用のサンプル・プログラムを追加（toolsディレクトリ以下）
- データリンク層の指定を追加（LINKTYPE:の入出力と-ltオプション）
- イーサネット以外のインターフェースにも対応可能にする（ただし現状で対応しているのは，イーサネット以外はループバック・インターフェースのみ）
- Mac OS X，NetBSD，OpenBSDに対応
- 共通オプションとして-doを追加（データのみ出力）
- PCAP/PcapNGによる出力時のエンディアン指定を追加（-ne/-le/-beオプション）
- その他，細かいバグを多数修正

ビルドの方法

● FreeBSD/Linux でのビルド

FreeBSD/Linux環境ではpkttools-1.16.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 -nd http://kozos.jp/software/pkttools-1.16.zip↵
% unzip pkttools-1.16.zip↵
% cd pkttools-1.16↵
% make↵
```

本連載のプログラムのソースコードは以下の筆者のホームページからダウンロードすることができます．ライセンスはKL-01というもので，組込み機器などでも自由に利用することができます．
http://kozos.jp/books/interface/ethernet2/