第4章 受信/送信/解析/変換…組み合わせていろいろ使える!

フリーのパケット操作プログラム群pkttools

坂井 弘亮

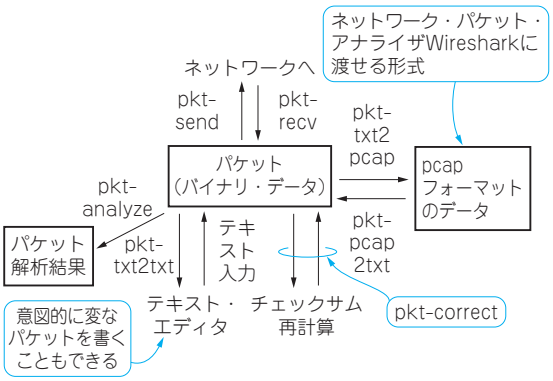

図1 筆者提供のパケット操作プログラム群「pkttools」のできること

表1 pkttoolsに含まれるプログラム

プログラム名	動 作
pkt-recv	パケット・キャプチャして，受信データをテキスト出力
pkt-send	テキスト入力されたパケットを送信
pkt-txt2txt	テキスト入力されたパケットをテキストで再出力(テキストの整形用)
pkt-txt2pcap	テキスト入力されたパケットをpcapフォーマットに変換
pkt-pcap2txt	pcapフォーマットを解読してテキスト出力する
pkt-analyze	テキスト入力されたパケットを解析
pkt-correct	テキスト入力されたパケットのチェックサムを再計算して再出力
pkt-pingrep	pingの応答を生成(後述)

筆者が作成しフリーソフトウェアとして公開しているパケット操作プログラム群pkttoolsがあります．

pkttoolsはパケットの送信や受信，解析，チェックサム計算やフォーマット変換などを行う各種プログラムの集合です．各プログラムの組み合わせの柔軟性が高く，**図1**のように連携させて，さまざまな処理を行うことができます．図中でpkt-*xxxx*となっているのが，pkttoolsが提供するコマンドです．

pkttoolsを組み合わせると各種解析や実験に使えます．pkttoolsの活用例として，pingを自動返信させる装置＆プログラムをAppendix4と第5章で紹介します．

なお，pkttoolsはBPFとRAWソケットの両方に対応しており，FreeBSDとLinuxの環境で利用可能です．

● pkttoolsの利用方法

pkttoolsは**表1**のツールを含んでいます．**リスト1**はLinuxでネットワーク・インターフェースのeth0上でパケットをキャプチャしたときの出力例です．なお，利用できるインターフェース一覧はifconfigというコマンドにより知ることができます．

このように出力はテキスト・ベースで行われます．さらに各プログラムをパイプで接続して，**図1**のように連係動作させることができます．

表2はプログラム群のさまざまな実行例です．**表3**は各プログラムを実行する時のコマンド・オプション一覧です．

リスト1 ネットワーク・インターフェースのeth0上でパケットをキャプチャしたときの出力例
出力はテキスト・ベースで行われる

```
% pkt-recv -i eth0
-- 1 --                    宛先MAC          送信元MAC        IPヘッダ
TIME: 1400296569.633895 Sat May 17 12:16:09 2014
SIZE: 98/98
000000: 00 11 22 33 44 55 00 66 77 88 99 AA 08 00 45 00 : .."3DU.f w.....E.
000010: 00 54 59 86 00 00 40 01 9D C4 C0 A8 01 0D C0 A8 : .TY...@. ........
000020: 01 01 08 00 D2 DA 66 11 00 00 53 76 D4 79 00 09 : ......f. ..Sv.y..
000030: AC 17 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 : ........ ........
000040: 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 : ........ .. !"#$%
000050: 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 : &'()*+,- ./012345
000060: 36 37                                           : 67
==
```