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19回 次世代ネットワーク・パケット・フォーマット PcapNGを出力する

坂井 弘亮

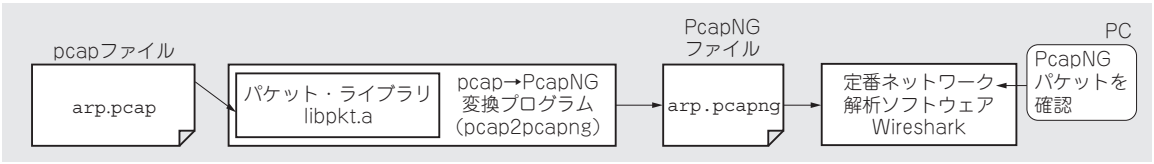

図1　今回すること…次世代ネットワーク・パケット・フォーマットPcapNGファイルを出力する
PcapNGフォーマットで出力したファイルを解析ソフトウェア(Wireshark)で解析してみる

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3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．

● 前回まで…ネットワーク・パケットの定番pcapフォーマットで入出力を行えるようになった

▶その1…pcapフォーマットの説明

前回(第18回，2017年1月号)までは，ネットワーク・パケットを保存するための一般的なフォーマットであるpcapフォーマットについて説明しました．

▶その2…pcapパケット送信ツールを作成

また受信したパケットをpcapフォーマットによって出力する「パケット・ロガー」と，pcapフォーマットのファイルからパケット・データを読み取りネットワーク上に送信するパケット送信ツールを作成しました．しかし，pcapフォーマットには幾つかの問題点もありました．

● 今回すること…次世代PcapNGフォーマットの出力にも対応

今回は次世代のパケット・フォーマットであるPcapNGについて説明します．またpcapフォーマットをPcapNGに変換するコンバータ(pcap2pcapng)を作成してみます(**図1**)．

次世代のネットワーク・パケット・フォーマットPcapNG

● 古くからある定番pcapの問題点

前回までに説明してきたpcapフォーマットは，もともとtcpdumpのパケット・キャプチャ部のライブラリとして開発されたlibpcapのパケット・ヘッダがベースになっています．

このためその設計は古く，例えば以下のような問題点があります．

- アラインメントの考慮がないため，mmap()して全体をランダム・アクセスするような処理に向いていない．
- 各フィールドのサイズが，プラットフォーム依存である(例えばパケット・ヘッダのタイム・スタンプには struct timevalが利用されているが，struct timevalのtv_secメンバの型はtime_tであり，環境によっては64ビットだったりする)．
- 複数のインターフェースを扱うことができない．
- パケットに対するコメントなどの付加情報を格納することができない．
- 拡張領域がないため，ユーザ拡張ができない．

これらの欠点は，次世代フォーマットであるPcapNG(PCAP Next Generation)フォーマットで解決されています．

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/