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17回 定番pcapフォーマットで ネットワーク・パケットを取り込む

坂井 弘亮

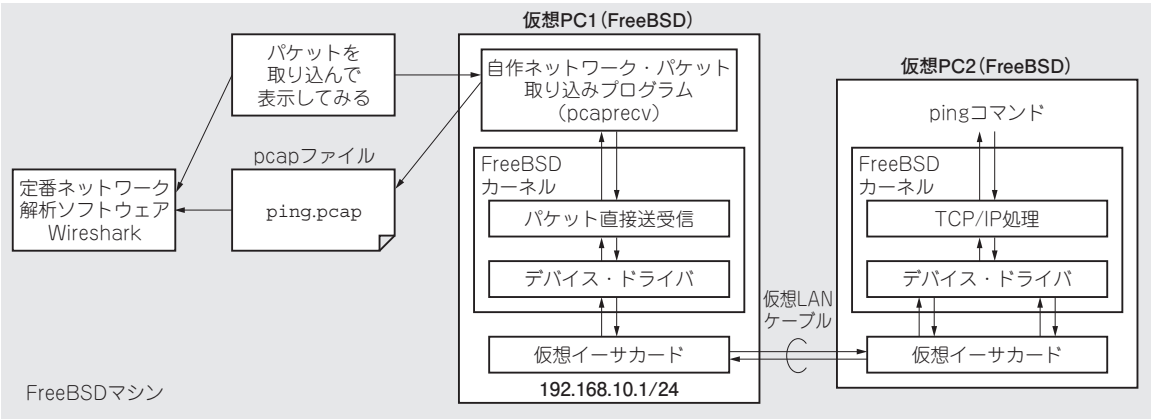

図1　実験すること…定番pcapフォーマットでネットワーク・パケットを取り込んでみる
定番解析ソフトウェアWiresharkに入力して表示もさせてみる

前回（第16回，2016年11月号）は，L2ネットワークの種別を調べ，さらに種別に応じて受信バッファの先頭オフセットを調整することで，バッファのアドレスのアラインメントを考慮せずに済むようにする方法を説明しました．

今回は，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す[注1]．

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」を作成してみます（**図1**）．なおpcapフォーマットからの入力は，次回に扱います．

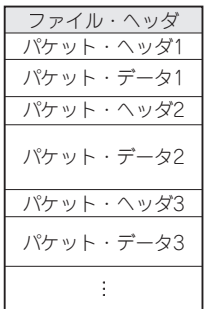

図2　ネットワーク・パケットの定番pcapフォーマットの構造

ネットワーク・パケットの定番 pcapフォーマットを知る

● フォーマットの全体像

pcapフォーマットの全体像は，**図2**のようになっています．

ファイルの先頭にはファイル・ヘッダがあります．ファイル・ヘッダの後には，パケット・ヘッダとパケット・データが対となって連続しています．

ファイル・ヘッダにはフォーマットのバージョンや時刻情報のタイムゾーンなど，ファイル全体に関わる情報が格納されています．対してパケット・ヘッダには，パケットごとの情報が格納されます．

図2では3つのパケット・データが示されています

注1：pcapフォーマットについては，本誌2014年8月号の特集中（pp.54-56）でも説明されている．しかしここで説明されているのはフォーマットの概略と簡単なサンプル・プログラムのみなので，今回はpcapフォーマットの解析結果や情報の調べ方など，実践的な内容を紹介する．

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/