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18回 ネットワーク・パケットの定番pcapフォーマットを解読する

坂井 弘亮

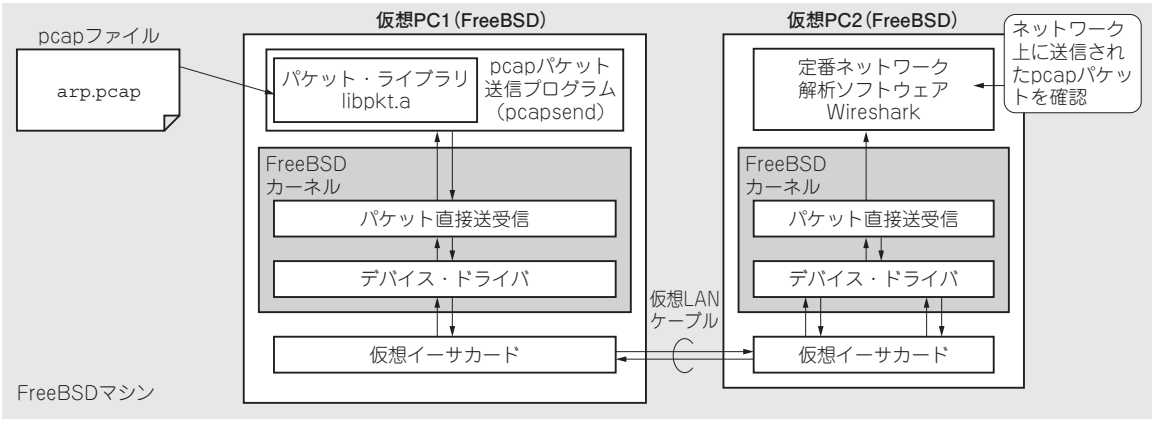

図1　今回すること…ネットワーク・パケットの定番pcapフォーマットを解読する
解読したパケットをネットワークに再送信して解析ソフトウェアWiresharkで確認してみる

前回（2016年12月号）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，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」を作成しました．

今回はpcapフォーマットからの入力について説明します．また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す（**図1**）．

pcapフォーマット解読の注意点

pcapフォーマットは，ファイルの先頭にファイル・ヘッダがあり，その後にパケット・ヘッダとパケット・データの対が連続している構造になっています（**図2**，詳細は前回，第17回参照）．pcapフォーマットからパケットを読み出す際には，以下の注意点があります．

● その1：エンディアンの考慮

pcapフォーマットのヘッダ中のフィールドのエンディアンは，そのフォーマットを生成した環境に依存します．

例えばリトル・エンディアンの環境で作成したpcapファイルのヘッダ情報はリトル・エンディアンで格納されますが，ビッグ・エンディアンの環境ならばビッグ・エンディアンで格納されます．

そしてエンディアンはファイル・ヘッダの先頭のマ

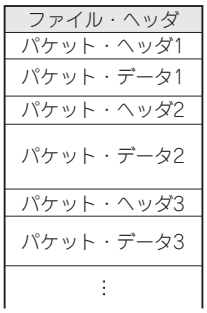

図2　ネットワーク・パケットの定番pcapフォーマットの構造
定番解析ソフトウェアWiresharkの入力にも使われる．前回（第17回）図2再掲

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/