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20回 次世代パケット・フォーマット PcapNGフォーマットを読み込む

坂井 弘亮

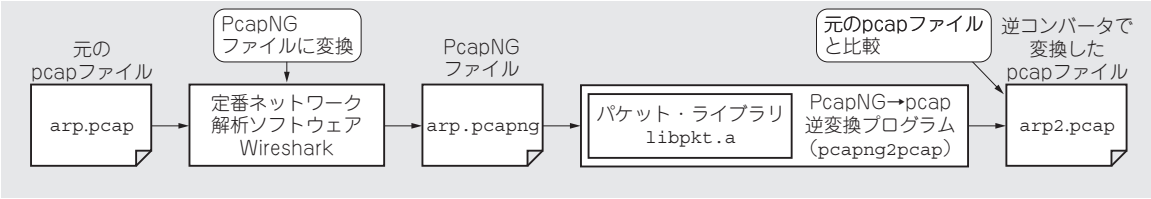

図1　今回すること…次世代パケット・フォーマットPcapNGを読み込む
pcapフォーマットに戻して正しいか確認する

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．

● 前回したこと…次世代パケット・フォーマットPcapNGの出力

前回（第19回，2017年2月号）は，ネットワーク・パケットを保存するための次世代フォーマットであるPcapNGフォーマットと，その出力方法の具体例について説明しました．従来のpcapフォーマットをPcapNGに変換するコンバータを作成しました．

● 今回すること…PcapNGの読み込み（入力）

今回は，PcapNGからの入力について説明し，PcapNGからpcapフォーマットに戻す逆コンバータを作成します（**図1**）

PcapNGフォーマット読み込み時の注意点

前回説明したPcapNGフォーマットのファイルを読む際には幾つかの注意点があります．

● その1…エンディアンを考慮しないといけない

PcapNGのブロック中のフィールド値は，生成した環境のネイティブなエンディアンで格納されます．つまりリトル・エンディアンとビッグ・エンディアンの両方があり得ます．

このためPcapNGを読み込む際は，本来ならば両エンディアンに対応する必要があります．エンディアンは，セクション先頭のSHB（Section Header Block）のマジック・ナンバを見て判断します．エンディアンの判断を行わない場合，自身の環境で生成したPcapNGファイルは読み込めても，エンディアンの異なる他環境で生成されたPcapNGファイルは正常に読み込めないといった問題が発生します．

なおエンディアン変換の処理は16/32ビットだけでなく，64ビットのものも必要です．これはSHBのセクション長が，64ビット値で格納されているためです．

● その2…不明なブロックをスキップするようにしておく

PcapNGはブロック単位で情報を保持しています．各ブロックの定義は以下にあります．

`http://pcapng.com/`

上記サイトの「Pcap-NG specification」がPcapNGの仕様です．各ブロックの定義は3章にあります．

現状では，7種類のブロックが定義されていますが，そのうちの1つ（Packet Block）は廃止となり，EPB（Enhanced Packet Block）を使うことが推奨されています．つまり，現状で主に利用されるブロックは6種類となります．しかし，今後，PcapNGフォーマットがバージョンアップした際には，ブロック種別が追加される可能性があります．

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/`