パケットづくりではじめる ネットワーク入門

第23回 BSDでもLinuxでも使える 標準的パケット送受信ライブラリ libpcap

坂井 弘亮

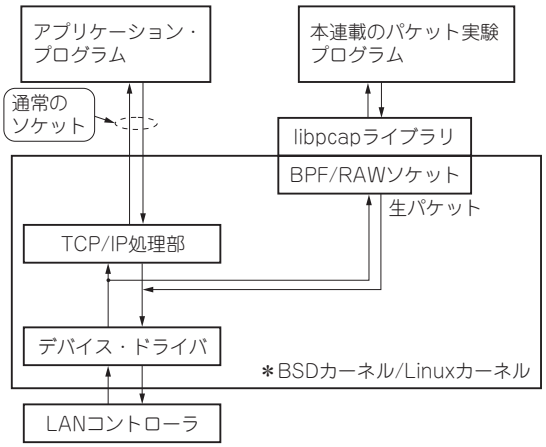

図1 「libpcap」ライブラリを用いればBPF（NetBSDやFreeBSDなど）やRAWソケット（Linux）といったインターフェースの違いを気にせずにパケットの送受信を行える

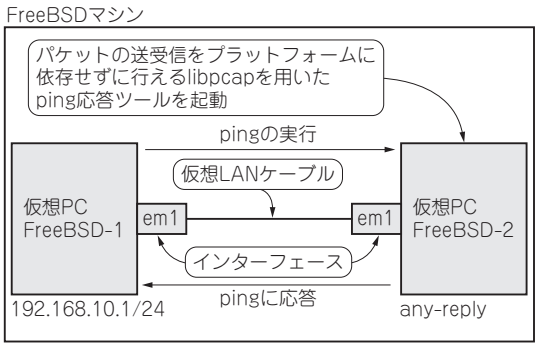

図2 動作確認に用いた実行環境

● 今回すること…BSDでもLinuxでも同じプログラムでパケット送受信

本連載ではここまで，動作プラットフォームとして，主にFreeBSDとLinuxを想定していました．例えばパケット・ライブラリによるパケットの送受信には，＊BSD（NetBSDやFreeBSDなど）のBPF（Berkeley Packet Filter）か，LinuxのRAWソケットが利用されています．

しかし，＊BSDのBPFやLinuxのRAWソケットを直接使う代わりに，libpcapというライブラリを利用すれば，パケットの送受信をプラットフォームとなるOSに依存せずに行うことができます（**図1**）．

今回はlibpcapの使い方について説明し，パケット・ライブラリをlibpcapに対応させます．またlibpcapを利用したパケット・ライブラリを用いて，（第5回に作成したものを再ビルド）「ping応答ツール」の動作を確認します（**図2**）．

これは，Windows環境をサポートする際の準備になります．WindowsではlibpcapのWindows版ともいえる，WinPcapというライブラリが利用できます．

BSDでもLinuxでも（Windowsでも）使える標準的パケット送受信ライブラリ libpcap

定番のパケット解析ソフトウェアWiresharkをインストールする際に，libpcapやWinPcapというライブラリが追加でインストールされます．

libpcapはテキスト・ベースの代表的なパケット・アナライザであるtcpdumpの，キャプチャ部分を扱う低層のライブラリとして，tcpdumpから分離・独立したものです．キャプチャだけでなくpcapフォーマットでの出力や入力なども可能です．

またWindows版としてWinPcapというライブラリがあり，Windowsへの移植も（libpcapの利用部分については）少ない変更で可能になっています．

つまりlibpcapを使えば，パケットをキャプチャしてpcapフォーマットで保存するようなツールを簡単に，移植性高く作成できます．

libpcapを使うための準備

● インストール

libpcapはWiresharkなどをインストールすることで，依存するライブラリとしてパッケージ・インストールされていることも多いかと思います．しかしlibpcapを使ったプログラムを作成するためには，開発

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/