パケットづくりではじめる ネットワーク入門

第22回　さすがPcapNG②… 複数インターフェースを1ファイルにまとめる

坂井 弘亮

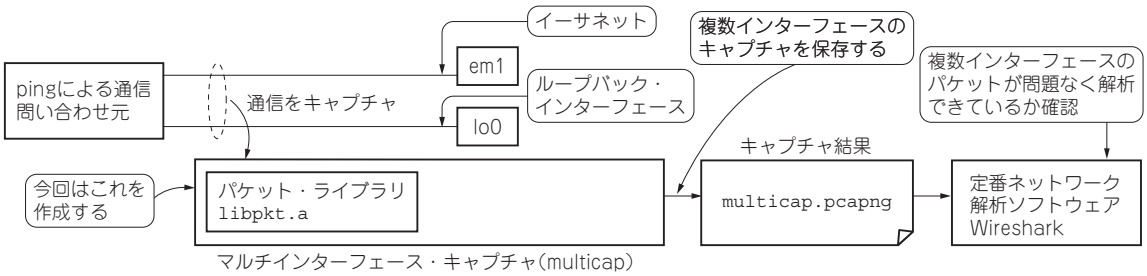

図1　今回すること…複数インターフェースのキャプチャ結果を1ファイルに保存する
保存した複数インターフェースのキャプチャ結果を定番解析ソフトウェアWiresharkで確認してみる

● 今回すること…できたら便利! 複数インターフェースのキャプチャ・データを1ファイルにまとめる

前回までは，ネットワーク・パケットを保存するための次世代PcapNGフォーマットについて説明し，コメントを付加できる機能などを紹介してきました．

今回はPcapNGで可能となった機能として，特にルータなどで便利な，複数のインターフェースを1つのファイルにまとめる機能について説明し，複数インターフェースのキャプチャ情報を保存できる「マルチインターフェース・キャプチャ」を作成してみます(**図1**)．

PcapNGの新機能…複数インターフェースのキャプチャを1ファイルに保存

pcapフォーマットでは不可能だったが，PcapNGフォーマットで可能となった機能は多くあります．前回はその中の1つとして，パケットへのコメントの追加について説明しました．

他の有用な機能としては，複数のインターフェースを1つのファイルにまとめる機能があります．

● 従来のpcapフォーマットだと難しい

複数のインターフェースでのキャプチャ・データを1つのファイルにまとめることは，pcapフォーマットでは原理的にできません．これはpcapフォーマットがファイル・ヘッダにインターフェース情報を持っており，1ファイルに1つのインターフェース情報しか持てない構造になっているためです．

複数のインターフェースが同じリンク種別(例えば全てイーサネットなど)ならば，キャプチャ・データを1つのファイルに混ぜてしまうことは不可能ではありませんが，異なるリンク種別のインターフェース(例えば片方はイーサネットでもう片方はPPPなど)では，パケットごとにリンク種別を判断することが不可能となってしまいます．つまり，パケット・データは格納できても，先頭のヘッダが何のプロトコルのものなのかが判断できないわけです．

これは例えばルータなど複数のインターフェースに対応している機器でキャプチャを行う際に，不便な場合があります．pcapフォーマットではインターフェースごとにファイルを分割して保存するしかありませんが，ファイルを分割してしまっては，パケットを時系列で参照したりなど，複数のインターフェースをまたがっての解析をするときに不都合があります．

● PcapNGならできる

これに対してPcapNGでは，インターフェース情報はIDBという独立したブロックに格納されており，複数保持できます．このため複数のインターフェースを持つキャプチャ・データを持つことが可能です．

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/