特設　超定番プロトコル解析ツールWiresharkリファレンス・ガイド

第1章　オープンソースの定番
ネットワーク・プロトコル・アナライザ

パケットを見える化！ Wiresharkの基礎知識

ご購入はこちら

竹下 恵

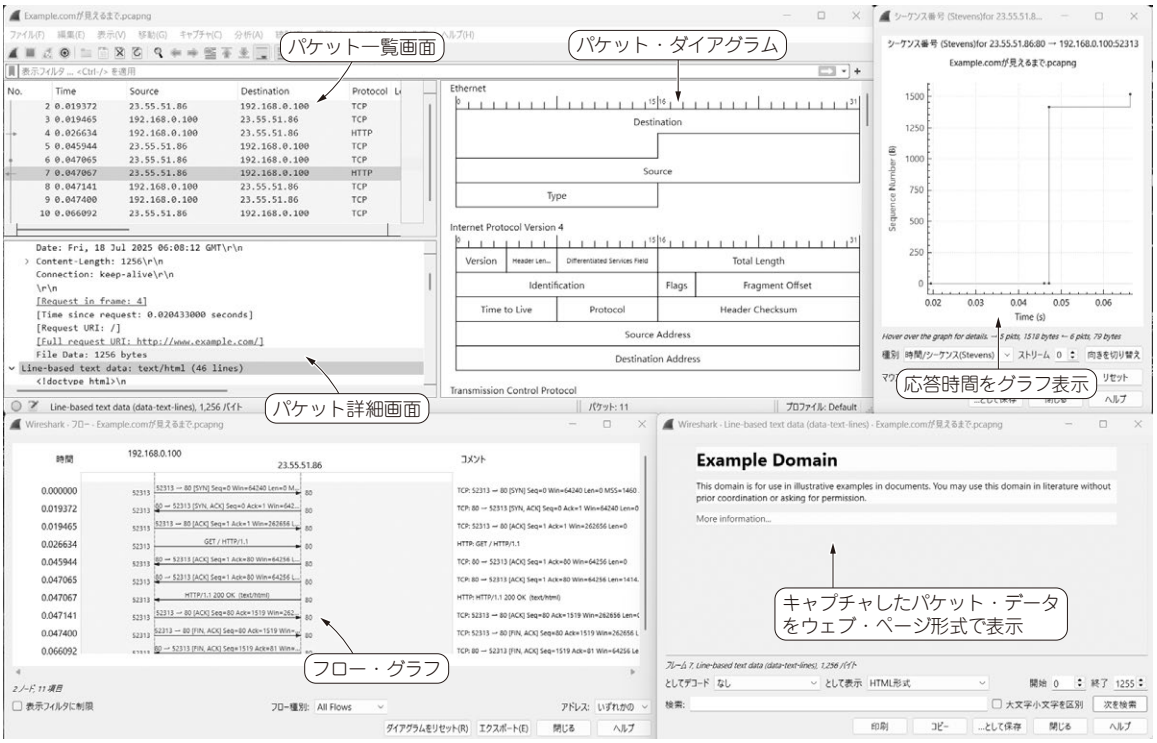

図1　オープンソースの力で現在も進化中！定番ネットワーク・プロトコル・アナライザ「Wireshark」
本稿執筆時点で最新のWireshark 4.4系では，3000以上のプロトコルに対応し，総フィールド数は26万5000以上，ソースコードは360万行（周辺を含めて660万行）の大きなプロジェクトとなっている

特集の第1部～第2部では，Pythonのコマンドやコードを使った通信実験を行うことで，ネットワークの仕組みについて説明しました．作成したプログラムが正しく通信を行っていることを確かめるには，ネットワークを流れるパケットを見える化する手段が必要です．そのためのツールとして，ネットワーク・プロトコル・アナライザと呼ばれる機器やソフトウェアがあります．

特設記事では，無料で使える定番ネットワーク・プロトコル・アナライザWireshark（ワイヤーシャーク）（**図1**）について紹介します．Wiresharkは，本誌でも何度か登場した定番ネットワーク・プロトコル・アナライザです．進化を繰り返し，USBなどネットワーク以外のインターフェースでも使える汎用性があります．本特設では，Wiresharkの基本的な使い方から，実践的なパケットの解析手法，独自プロトコルの解析方法までを紹介します．（編集部）

ネットワーク・プロトコル・アナライザ「Wireshark」の概要

電流，電圧など人間の目に見えないものの挙動を理解するために，オシロスコープなどの測定機器で可視化するように，有線LANや無線LANを流れるパケットを見える化するツールが，ネットワーク・プロトコ