第2章 画面の表示内容からパケット解析のコツまで

Wiresharkの使い方&パケットの見かた

竹下 恵

本章では，Wiresharkの基本的な使い方について説明します．具体的には，画面の表示内容からパケットのキャプチャ方法，キャプチャ・データの閲覧方法まで説明します．（編集部）

1 基本的な使い方

● 起動方法とスタートアップ画面の表示内容

Windows 11 Pro 64ビット版の日本語環境において，Windows版のWireshark 4.4.7（カスタマイズしていないデフォルト設定）を使用します．

Wiresharkのインストーラを実行してインストールした後，Wiresharkを起動すると，**図1**に示すスタートアップ画面が表示されます．

▶表示/キャプチャ・フィルタ

この画面では，日本語化されたメニューやボタンの下に表示フィルタ・バーが表示されます．表示フィルタは，Wiresharkが取得したパケットを絞り込むために利用するもので，次に示すWiresharkのダイセクタの書式で入力します．

プロトコル．フィールド．サブフィールド

メインの画面の「キャプチャ」セクションに，「…このフィルタを利用」というキャプチャ・フィルタ入力部があります．

キャプチャ・フィルタはdumpcapがキャプチャ・ライブラリを呼び出す際の引数としてインターフェースごとに利用されるものです．libpcapのフィルタ式（pcap-filter）で入力することで，取得するパケット自体を絞り込むことができます．そして，この下にはWiresharkが認識したキャプチャ・インターフェースが並びます．

▶キャプチャ・インターフェース

図1のように，キャプチャ・インターフェースは，パケットが到着したアクティブなインターフェースから順番に並んでおり，その右側の折れ線グラフで到着したパケットを視覚的に確認できます．また，任意のインターフェースにマウスを載せることでポップアップされた画面よりIPアドレスやIPv6アドレス，キャプチャ・フィルタを確認できます．

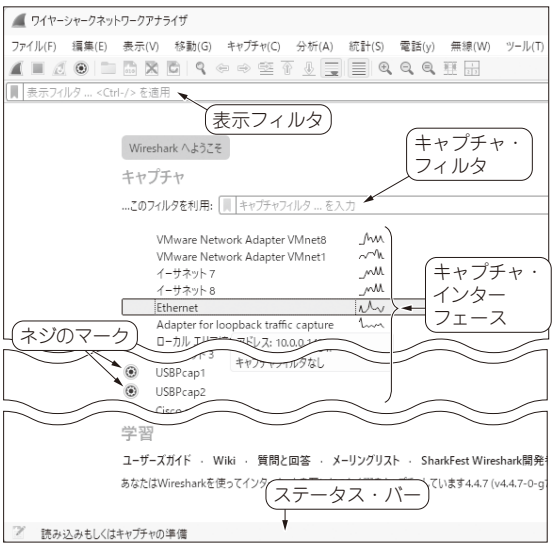

図1　Wiresharkのスタートアップ画面
インターフェースを選択し，マウス・ポインタを載せることでポップアップされた画面よりIPアドレスやIPv6アドレス，キャプチャ・フィルタを確認できる

また，キャプチャ・インターフェースを見ると，ネジのマークが付いたインターフェースを確認できます．これは外部（拡張）インターフェースで，インストール時に追加して選択したり，ユーザで独自に追加したりすることで，キャプチャ元として外部の入力を利用できます．

例えば**図1**では，ネジのアイコンの付いた外部（拡張）インターフェースの先頭にUSBPcap1，USBPcap2があります．これはWiresharkにUSBPcapのドライバを導入することで，PCに接続されたUSBインターフェースを流れるUSBフレームを取得することができる外部（拡張）インターフェースです．USB機器を開発やデバッグする際に，ベンダIDやプロダクトIDなどの情報を確認できます．

▶ステータス・バー

一番下にはステータス・バーがあり，キャプチャ・