特設

ダウンロード・データあります

第3章 キャプチャ方法から名前解決/フロー・グラフ表示/応答時間確認/データ確認まで

実際にHTTPパケットを解析してみる

竹下 恵

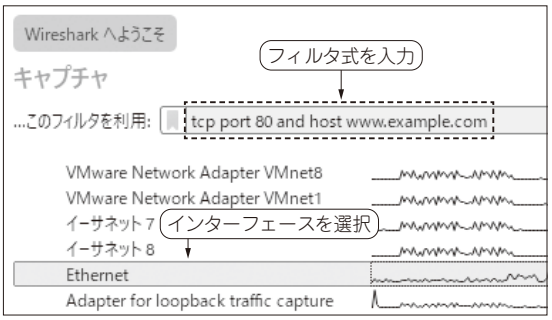

図1 有線LANインターフェースを選択してからキャプチャ・フィルタを設定

ここではEthernetという有線インターフェースを選択してから，キャプチャ・フィルタに「tcp port 80 and host www.example.com」を入力している

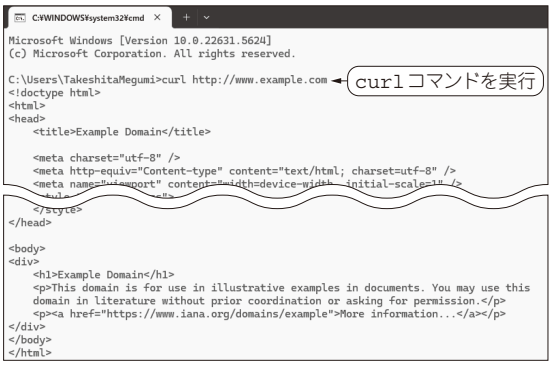

図2 curlコマンドを使ってHTTP通信を実行した様子

curl http://www.example.comを実行．コマンドを実行するとwww.example.comのホームページがHTMLで表示される

本章では，実際にパケットをキャプチャしてみます．平文HTTPのパケット・キャプチャを行います．

極力一般的なパケットが取得できるように行いますが，キャプチャしたPCのOSやアプリケーション，ネットワーク環境により，パケットとヘッダの構成やフィールドの値が異なるので，注意してください．筆者の環境でキャプチャしたサンプル・データは，次のウェブ・ページよりダウンロードできます．

```
https://www.cqpub.co.jp/interface/download/contents2025.htm
```

ステップ①…パケットをキャプチャする

キャプチャ・フィルタを適用してパケット・キャプチャを開始します．今回はhttp://www.example.comが見えるまでのパケットを取得します．そのため，TCP80番ポートとwww.example.comのパケットのみ取得します．

● 手順1…キャプチャ・フィルタの設定

Wiresharkを起動したら，メニュー・バーの[表示]-[名前解決]を選択し，「ネットワークアドレスを解決」にチェックが付いていることを確認します．チェックされていない場合は，選択してチェックします．

次に，有線LANのインターフェースとしてEthernetを選択し，キャプチャ・フィルタに次のようなフィルタ式を入力します(**図1**)．

```
tcp port 80 and host www.example.com
```

これはTCP80番ポートで，かつホスト名がwww.example.comのみパケットを取得するキャプチャ・フィルタです．フィルタ式が正しい場合，入力後に少し待つとキャプチャ・フィルタの背景色が緑になります．そして，選択した有線LANインターフェースをダブルクリックしてパケット・キャプチャを開始します．

● 手順2…HTTP通信の実行

コマンド・プロンプトを開いて，次のコマンドを入力します．

```
curl http://www.example.com
```

ここでhttpsと入力すると，TCP443番ポートのTLSのパケットとなり，暗号化されて内容をキャプチャできなくなるので，必ずhttp://と入力するよう注意します．

コマンドを入力して[Enter]キーを押すと，www.example.comにTCP80番ポートでTCP接続を行