第3部

第3章 TCPと比較しながら サーバ認証/相互認証/最新v1.3を試す

プログラム作りと実験で TLSで暗号化通信にトライ

古城 隆

TCPとTLSで通信内容を比較してみる

本章では，実際にプログラムを動かしながらTCPとTLSの通信内容を比較します．実験の構成を**図1**に示します．

● 通信実験の概要

クライアント役のPCとサーバ役のPCの2台の間で，サンプル・プログラムを使った1往復だけの通信を行ってみます．TCPとTLSの両方で通信して比較します．PCにはラズベリー・パイ4Bを使います．

今回はラズベリー・パイを使いましたが，ここで紹介するサンプル・プログラムやTLSライブラリ，パケット・キャプチャ・ツールなどは，一般的なLinux環境であれば動作します．自分の環境に応じて，UbuntuやmacOS，WindowsのWSL（Windows Subsystem for Linux）などでも試せます．パケット・キャプチャ・ツールには，Wiresharkを使います．

図1のように物理的に2台のPCを用意しなくても，例えば1台のラズベリー・パイ上でクライアント役とサーバ役の2つのプロセスで実験しても原理的には変わりません．その場合は，2つのターミナルを開いて実験します．

● 筆者の実験環境

記事の執筆に使用した実験環境は次の通りです．今回紹介した内容のほとんどはバージョンに依存しないので，さまざまな環境で同様に動作するはずです．

- サーバ役PC：ラズベリー・パイ4 Model B
- クライアント役PC：MacBook
- Wireshark：v3.4.10（ラズベリー・パイ上で動作）
- wolfSSL：v5.3.0-stable

実験の準備

実験に使うツール類をインストールしておきます．ネットワーク・プロトコル・アナライザのWiresharkは，2台のPCのうちどちらか一方で使います．wolfSSLライブラリとサンプル・プログラム一式は，2台両方に置いておきます．

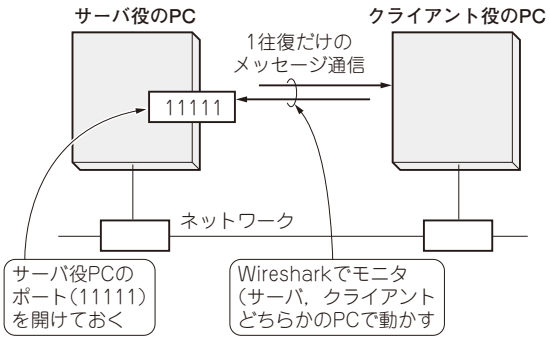

図1　TCPとTLSの通信内容を比較する実験の構成
ラズベリー・パイでも試せる．1台のマシンだけで試すことも可能である

● ステップ1…Wiresharkとポートの準備

▶手順1：Wiresharkのインストール

次のコマンドを実行してインストールします．サーバ役，クライアント役のどちらにインストールしても構いません．

```
$ sudo apt install wireshark↵
```

▶手順2：時系列表示にポート番号を追加する

Wiresharkの時系列表示には，パケットの送り元（Source）と送り先（Destination）のIPアドレスが表示されます．1台のPCで実験するときは，送り元，送り先のどちらもローカルのループ・バック・アドレス（127.0.0.1）になるので，メッセージの方向が分かりにくいです．1台のPCで実験する場合は，Wiresharkの時系列表示にポート番号を表示させるとサーバ，クライアントの区別がつきやすくなります．

図2にポート番号表示の追加手順を示します．

▶手順3：サーバ役PCのポートを解放する

クライアントからのTCP接続要求を受け付けるように，サーバ役PCのポートを解放しておきます．今回のサンプル・プログラムでは，他のアプリケーショ