第1章 Wi-Fiフレームや TCP/IP パケットの中身をのぞき見る 開発ボード選びから環境構築まで

ダウンロード・データあります

# ESP32で自作する! パケット・アナライザの全体像と準備



足立 英治

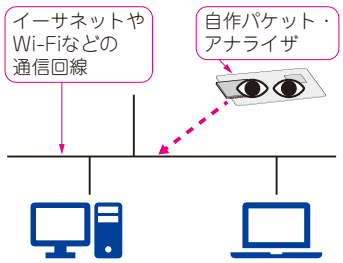
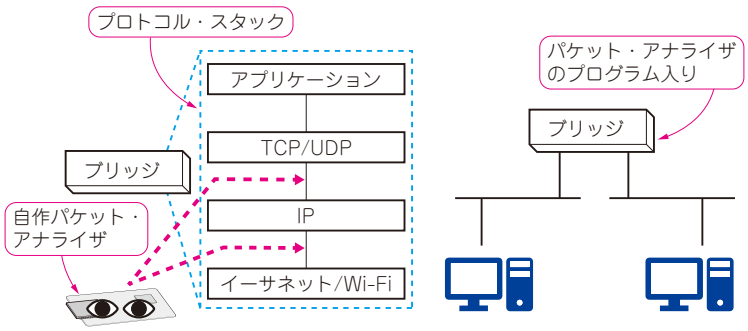



**図1　自作するパケット・アナライザの方式①…通信回線上でのぞき見る**
Wi-Fiやイーサネットの通信回線上に流れるプロトコルを読み取る方法．第3章で，この方法によるパケット・アナライザの作成方法を紹介する




（a）プロトコル・スタックのプログラム上でのぞき込む　（b）パケット・アナライザの配置場所…通信経路の途中

**図2　自作するパケット・アナライザの方式②…プロトコル・スタック上でのぞき見る**
ルータやハブ，ブリッジ上で動作するプロトコル・スタックの途中にフックをかけて読み取る方法．第4章で，この方法によるパケット・アナライザの作成方法を紹介する

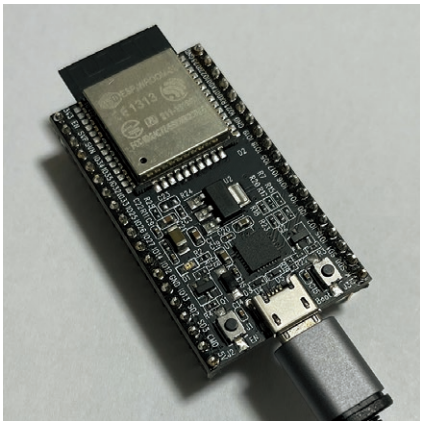


**写真1　第1部で紹介する自作パケット・アナライザのプログラムは ESP32-DevKitC（Espressif Systems）で動作する**

第1部では，ネットワークと通信プロトコルの基礎知識を学びながら，ESP32で動作するパケット・アナライザ（通称スニファ）のプログラムを開発し，実際に動かして通信実験を行います（**図1**，**図2**）．

ここで紹介するパケット・アナライザは，**写真1**のESP32-DevKitC（Espressif Systems）などで実際に動かしながら試せます．

第1部で紹介するプログラムは，次のURLから入手できます．

```
https://interface.cqpub.co.jp/202402t/
```

## ● パケット・アナライザはネットワークをのぞき込んで解析する装置

ネットワークを使っていると，なぜか期待通りに動かなかったり，不安定になったりすることがあります．アプリケーションやサーバの動作ログだけではその原因が分からず，通信内容の確認が必要なときもあります．

そのようなときに，ネットワークをのぞき込むことをスニッフィングと呼び，それを行うものをスニファと呼びます．スニッフィングするには，通信回線上で流れる通信プロトコルをキャプチャ（記録）して，そのプロトコルを解析（アナライズ）する必要があります．そのため，スニファにはパケット・アナライザとしての機能も含む場合があります．前者の記録する機能がPCAP（Packet Capture）であり，専用のハードウェアを用いたり，PC上でPCAPソフトウェアやライブラリを用いたりします．後者の解析するソフト