第4章 Androidスマートフォンの通信をプロトコル・スタック上でのぞき見る

ステップ②…TCP/UDPパケットのキャプチャと解析

足立 英治

IPパケットやTCP/TDPパケットをWi-Fiフレームのパケット・アナライザで解析しようとする場合，暗号化されたパケットの復号が必要になります．

ESP32は，アクセス・ポイント・モード(Soft-APモード)とステーション・モード(Stationモード)を同時に起動した上で，NAPT(Network Address Port Translation)を有効にすると，ESP32をNAT(Network Address Translation)ルータとして動作させることができます．

図1は，NATルータとして動作するESP32のプロトコル・スタック上の通信の流れです．この途中でパケットをキャプチャすることで，IPパケットやTCP/UDPパケットをのぞき見ることができます．ここではその実装について説明します(**図2**)．

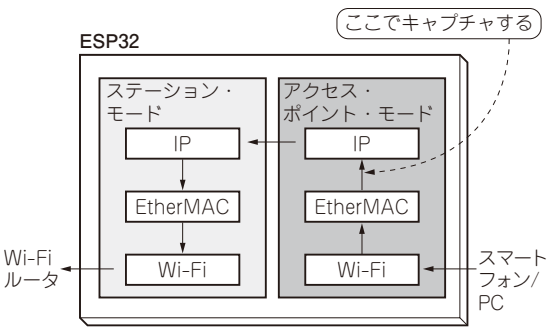

図1　本章でやること…TCP/UDPパケット・アナライザのプログラムを実装する
NATルータとして動作するESP32のソフトウェア構成．このソフトウェアに変更を加えて，プロトコル・スタック上でIPパケットやTCP/UDPパケットをのぞき見ることができるようにする

ステップ①…ESP32でNATルータを実装する

● モードの初期化とWi-Fi起動

ESP32でアクセス・ポイント・モードとステーション・モードを同時に起動するには，モードにWIFI_MODE_APSTAを指定した上で，2つのモードをそれぞれ初期化します(**リスト1**)．

初めにNATルータが正しく動くことを確認する必要があるので，公式サンプルを参考にそれぞれモードのネットワーク・インターフェースの初期化を実装します．

アクセス・ポイント・モード側は，スマートフォンやPCなどからの接続を受け付けるためのSSIDやパスワードなどを設定します．

ステーション・モード側は，中継先として接続するWi-FiルータのSSIDとパスワードなどを指定します．このとき，ESP32が接続できるWi-Fiルータを指定する必要があります．

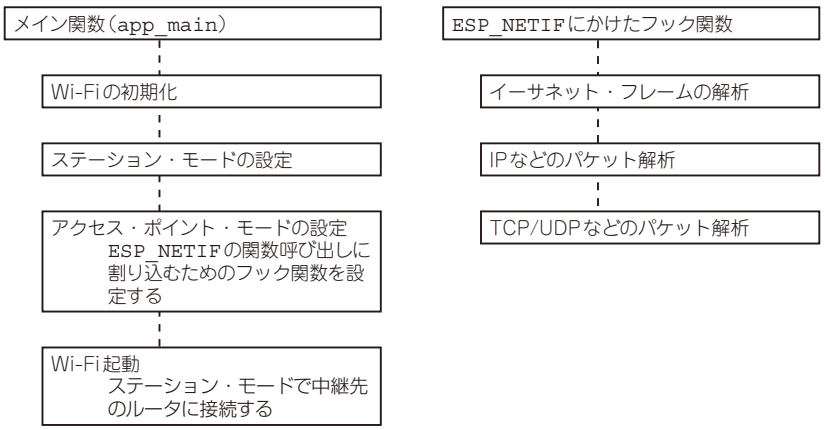

図2　TCP/UDPパケットをキャプチャ・解析するプログラムの全体像