第3章 ESP32の初期化から受信部と解析部の実装まで

ステップ①…Wi-Fiフレームのキャプチャと解析

足立 英治

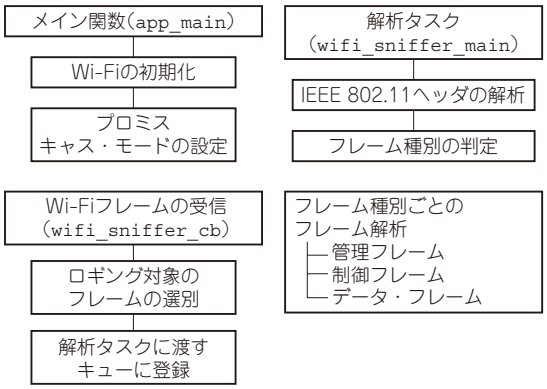

図1 Wi-Fiフレームをキャプチャ・解析するプログラムの全体像

本章では，Wi-Fiがどのように通信を確立して，どのようにデータを交換しているのかを理解するために，Wi-Fiのパケットをキャプチャする実装を説明します(**図1**)．

ただし，Wi-Fiは何度も規格が拡張されていて，完全に動作するパケット・アナライザはかなり複雑なので，基本的な部分に注目する形で説明を進めていきます．

1 ESP32の初期化の実装

● パケットをキャプチャするための初期化設定

Wi-Fiのフレームをキャプチャするには，受信した全てのデータを読み込むプロミスキャス・モード(Promiscuous Mode)を用いるので，通信の記録をストレージに残さず，メモリ上に記録するように設定し，通信モードも無指定にしておきます(**リスト1**)．

● プロミスキャス・モードで起動

ESP32をプロミスキャス・モードで起動すると，通常のモードとは異なり，アンテナに届くフレームをすべて傍受することが可能になります．このモードで起動しないと，通信対象以外のフレームを見ることができません．

リスト1 ESP32の初期化の実装①…パケットをキャプチャするための初期化設定

通信の記録をストレージに残さず，通信モードも無指定にしておく

```
wifi_init_config_t cfg = WIFI_INIT_CONFIG_DEFAULT();
esp_wifi_init(&cfg);
esp_wifi_set_storage(WIFI_STORAGE_RAM);   ← メモリ上に記録
esp_wifi_set_mode(WIFI_MODE_NULL);
                                          ← 通信モード未指定
```

リスト2 ESP32の初期化の実装②…プロミスキャス・モードを有効に設定する

フレームの種類や，コールバック関数の設定などを行う

```
uint8_t channel = 11;
wifi_promiscuous_filter_t wifi_filter =
                    { WIFI_PROMIS_FILTER_MASK_ALL };   ← フィルタ設定
esp_wifi_set_promiscuous_filter(&wifi_filter);
esp_wifi_set_promiscuous_rx_cb(wifi_sniffer_cb);       ← コールバック関数を設定
esp_wifi_set_promiscuous(true);
esp_wifi_set_channel(channel, WIFI_SECOND_CHAN_NONE);
                                                       ← プロミスキャス・モード有効
```

プロミスキャス・モードで起動するときは，どの種類のフレームを傍受するかのフィルタと，傍受したフレームを通知するコールバック関数の設定を行い，プロミスキャス・モードを有効に設定します(**リスト2**)．

この状態ではチャネル11をスニッフィングするので，傍受したいBSS(Basic Seavice Set)が通信を行っているチャネルに書き換えます．このとき，傍受するチャネルだけでなく，帯域幅が20MHzなのか40MHzなのかも確認して合わせます．

ESP32がサポートしているのは，2.4GHz帯のIEEE 802.11 b/g/nです．5GHz帯や，IEEE 802.11 acのような広い帯域幅(80MHzや160MHz)の電波は受信できません．

2 フレームの受信

● フレームの受け渡しを行うキューの用意

傍受したフレームを通知するコールバック上で，フレーム処理(ストレージへの保存やログの出力)を行うと，プロトコル動作が追いつかなくなります．