最終改定日：2024/01/17

Nexmon環境構築ガイド

静岡大学 情報学部 情報科学科4年

峰野研究室

学籍番号:70010065　氏名:原田海斗

Nexmon official「 https://github.com/seemoo-lab/nexmon 」
Nexmon Setup Page Home「 https://github.com/nexmonster/nexmon_csi 」
Nexmon Setup Page (for RasPi)「 https://github.com/nexmonster/nexmon_csi/tree/pi-5.10.92 」

RasPi4Bのセットアップ

初期起動設定 (for Windows10/11)

○ **RaspberryPi4Bの起動**

— Nexmon対応のイメージを，RasPi Imager で microSD に書き込む

— microSDをRasPi4に差し込み，起動 (HDMIを電源より先に挿入)

※1 起動後，sudo raspi-configコマンドで，[System Options] > [Boot/Auto Login] > [Yes] をしておくと便利

○ **Wi-Fi接続設定**

— 設定(etc)フォルダ下の，WPA認証ファイルをエディタで開く (以下，nanoで開く例)

— 右の文を，末尾に追記・保存して閉じる (「“ ”」は必要)

```
$ sudo nano /etc/wpa_supplicant/wpa_supplicant.conf
$ rfkill unblock wifi                # Wi-Fiの内部ロックを外す
$ sudo ifconfig wlan0 up             # 無線LAN有効化
$ sudo reboot                        # 再起動
```

```
network={
ssid="任意のSSID"
psk="パスワード"
key_mgmt=WPA-PSK
}
```

追記する文

— ifconfigコマンドでwlan0項目にIPアドレスが表示されていれば完了

RasPi4Bのセットアップ

初期起動設定 (for Windows10/11)

○ **SSH接続設定**

— RasPi4BでSSH接続を有効にする

```
$ sudo raspi-config
```

▶ [Interfacing Options] > [SSH] > [Yes]を選択

— RasPi4BのIPアドレスを確認する

```
$ ifconfig
```

▶ wlan0の項目に記載のIPアドレスを確認(記録)する

— SSH接続を行うデバイスで，PowerShellを管理者として起動

```
$ ssh pi@XXX.XXX.XXX.XXX     # 先ほど確認したIPアドレスを入力
```

※2 警告「WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!」が出た場合

原因：過去にSSH接続を行った際の認証キーが「.ssh」フォルダの「known_hosts」ファイルに残っている

解決方法：「known_hosts」を削除して、再度SSH接続を実行

RasPi4Bのセットアップ

RasPi4BでCSIを有効にする

図1：Wi-Fi Analyzer画面

○ **Nexmonのインストール**

— Nexmon_csiのバイナリファイルからインストールスクリプトを実行 (目安:2分)

```
$ sudo curl -fsSL https://raw.githubusercontent.com/nexmonster/nexmon_csi_bin/main/install.sh | sudo bash
```

※3 sudo rebootで再起動すればNexmonのインストールは完了
※4 無線SSH接続ができなくなるため，有線SSH接続に切り替える

○ **CSI収集テスト**

— Wi-Fiアナライザ(図1)などで観測したい無線通信のチャネルと帯域幅などを確認する

— mcpコマンドで，base64でエンコードされたパラメータ文字列を作成

```
$ sudo mcp –C 1 –N 1 –c 36/80
```

例) 帯域幅80[MHz]のチャネル36でCSIを観測する

— ここで出力された文字列を記録しておく (あとで引数として使用する)

RasPi4Bのセットアップ

RasPi4BでCSIを有効にする

○ **CSI収集テスト(続き)**

― 観測パラメータ文字列を設定し，モニターモード(mon0)インターフェースを追加

```
$ sudo ifconfig wlan0 up
$ sudo nexutil –Iwlan0 –Iwlan0 –s500 –b –l34 –v(mcpで生成したパラメータ文字列)
$ sudo iw dev wlan0 interface add mon0 type monitor
$ sudo ip link set mon0 up
```

― tcpdumpコマンドで，CSIデータを収集開始

```
$ sudo tcp dump –i wlan0 dst port 5500 –vv –w output.pcap –c 1000
```

※5 output.pcapファイルに書き込む
※6 1000[Packet]分収集したら終了(設定しない場合は終了するまで無限に収集する)

▶ **Pingなどで，観測したい通信を発生させて適切に動作しているか確認する**

RasPi4Bのセットアップ

RasPi4BでCSIを有効にする

○ **CSIデータ(.pcap)をCSVファイルに復号**

— WinSCPなどを使用して，RasPi4Bからpcapファイルをダウンロードする

— csi_changerフォルダ内のpcapfilesフォルダに復号したいpcapファイルを置く

— csi_changer.pyを起動する

```
$ python csi_changer.py
```

— 「pcapファイル名(拡張子なし)」と「帯域幅」を入力

```
Pcap File Name: XXX
Band Width: XXX
```

— resultフォルダ内に「XXX_CSI_Amp」と「XXX_CSI_Pha」が出力されていれば完了

▶ **以上でCSI収集環境構築～CSIデータ復号までの一連の流れが完了**