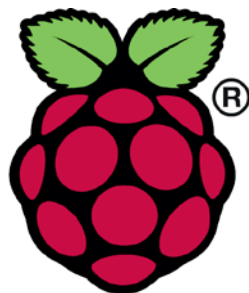


抜粋版

WiFiプロトコル・アナライザ V2

～Raspberry Piを使いwifi6e対応～
運用編



Raspberry Pi



WIRESHARK

スペクトラム・テクノロジー株式会社

<https://spectrum-tech.co.jp>

sales1@spectrum-tech.co.jp

目次

ページ

1.	Raspberry Piでできること	<u>3</u>
2.	Linux基本的なコマンド	<u>3</u>
3.	プロトコル・アナライザ関係コマンド	<u>5</u>
4.	Raspberry Pi基本操作	<u>6</u>
5.	日常運用	
	• セキュリティ対策(アンチウイルス更新、スキャン)	<u>8</u>
	• パッケージの更新	<u>9</u>
6.	Wifiプロトコル・データの取得	
①	WiFi6e 6GHzチャンネル モニタ	<u>10</u>
②	2.4G/5G チャンネル モニタ 20MHz	<u>15</u>
③	2.4G/5GHzチャンネル モニタ 40MHz	<u>20</u>
④	2.4G/5GHzチャンネル モニタ 80MHz	<u>21</u>
⑤	airodumpを使ってスキャン 2.4G/5G	<u>22</u>
⑥	airodumpを使ってスキャン 6G	<u>23</u>
⑦	tsharkによるデータ取得	<u>24</u>
7.	LANプロトコル・データの取得	<u>25</u>
8.	BLEプロトコル・データの取得	<u>27</u>

参考

2.4GHz チャンネル配置

5GHz チャンネル配置

6GHz チャンネル配置

抜粋版のためページと本文は一致しません

プロトコル・アナライザ運用マニュアル

1. Raspberry Piでできること

- WiFi, LAN, BLE (一部) のwiresharkを使ったプロトコル・アナライザ
- Wifiのスキャン: airodumpのみ解説します
- Ibeacon (BLE)のビーコン送信、受信
- 他にweb,メール、センサ制御など無限大の利用価値がありますが説明は割愛します。

2. Linux基本的なコマンド

① システム関係

- 起動: 電源を入れると自動で起動します。
- 再起動: # reboot
又は、menu>shutdown>reboot; 左上のメニューから
- 終了: # shutdown
又は、menu>shutdown>shutdown; 左上のメニューから
- ログアウト # exit
又は、menu>shutdown>logout; 左上のメニューから
- 日本語／英語の入力切替: 半角/全角のキー、切り替わらない場合は、上のiconのキーボードでmozc選択

プロトコル・アナライザ運用マニュアル

2. Linux基本的なコマンド

② ディレクトリ操作、コピー、移動、削除

masa@raspberrypi:~\$ **cd** /home/pi/Documents

ディレクトリの切り替え

masa@raspberrypi:/home/pi/Documents# **ls** ファイルとディレクトリの表示(表示したら操作したいファイルを右クリックでコピーして操作します)

masa@raspberrypi:~\$ **cp** ファイル名 ディレクトリ

配下のディレクトリのファイルを別のディレクトリへコピー

masa@raspberrypi:~\$ **mv** ファイル名 ディレクトリ

配下のディレクトリのファイルを別のディレクトリへ移動

masa@raspberrypi:~\$ **rm** ファイル名

ファイルの削除

便利な機能
rm --help
せる。すべてのコマンド共通(マイナスを2個とhelp)

コマンドのオプションが分からない場合は、ヘルプで問い合わせ

③ ユーザ権限、プロセス他

pi@raspberrypi:~\$ **su** -

スーパーユーザ(root)に切り替え、パスワードを入力

masa@raspberrypi:~\$ **ps** a

現状の動いているプロセスを表示

masa@raspberrypi:~\$ **kill**

特定のプロセスを強制終了

masa@raspberrypi:~\$ **apt-get** install pkg

パッケージのインストールなどに使用

masa@raspberrypi:~\$ **date**

日付、時間の設定を行います。

masa@raspberrypi:~\$ **mousepad** /etc/network/interfaces
りも使いやすいです。

インタフェースに記述して内容を変更します。Viよ

④ モジュール、usb、メモリ、HDDなどの表示

masa@raspberrypi:~\$ **lsmod**

linuxのモジュールリスト表示

masa@raspberrypi:~\$ **lsusb**

usbのデバイス表示

masa@raspberrypi:~\$ **free -mt**

メモリ使用状態表示

masa@raspberrypi:~\$ **df**

HDD(マイクロSD)の使用状態表示

プロトコル・アナライザ運用マニュアル

3. プロトコル・アナライザ関係コマンド

パーミッションエラーが出た場合は、sudoをつけて

① ネットワーク関係 (wifi, LAN)

```
masa@raspberrypi:~$ ifconfig
```

```
masa@raspberrypi:~$ ip l set wlan1 up
```

```
masa@raspberrypi:~$ ip l set wlan1 down
```

```
masa@raspberrypi:~$ iwconfig wlan1 mode monitor
```

```
masa@raspberrypi:~$ iwconfig wlan1 channel 11
```

```
masa@raspberrypi:~$ sudo wireshark
```

ネットワークインターフェースの状態表示

wlan1のインタフェースのup(LANの場合はeth0)

wlan1のインタフェースのdown

wlan1のインタフェースをmonitoモードに切り替えます。

wlan1のチャンネルを11(2462MHz)に切り替えます。

wiresharkを起動します。必ずsudoをつけること。Rootに切替て実施するとではエラー

```
masa@raspberrypi:~$ airodump-ng -band abg wlan1
```

wlan1のインタフェースで2.4G,5Gの全チャンネルのデータを取得できます。Wiresharkの個別チャンネルに比べて、データが欠落します。確認程度でお使いください。

```
masa@raspberrypi:~$ tshark -i wlan1 -w test0707.pcap
```

wiresharkを起動する代わりにコマンドでデータを取得し保存します。

wiresharkを起動する代わりにコマンドでデータを取得

② BLE関係

```
masa@raspberrypi:~$ hciconfig
```

```
masa@raspberrypi:~$ hciconfig hci0 up
```

```
masa@raspberrypi:~$ hcitool lescan
```

タフェースを選択しておくでプロトコルが取得できます。RF帯ではありません。限られたプロトコルになります。

```
masa@raspberrypi:~$ hcidump -a
```

BLEのインタフェース状態を表示

hci0のインタフェースをup

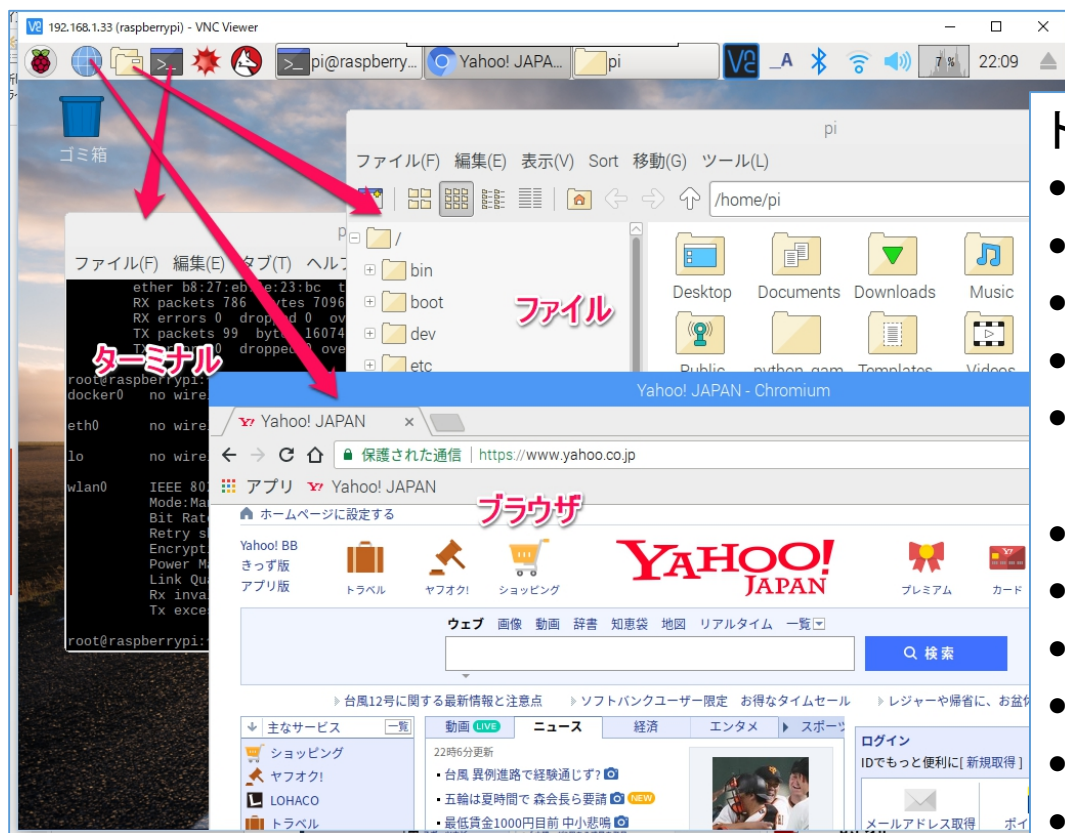
BLEのデバイスを検索します。wiresharkを立ち上げてBLEのインタフェースを選択しておくでプロトコルが取得できます。RF帯ではありません。限られたプロトコルになります。

BLEの接続状態をダンプします。

プロトコル・アナライザ運用マニュアル

4. Raspberry Piの基本操作

① 表示画面と内容



トップ画面（上段のタスクバーで選択）

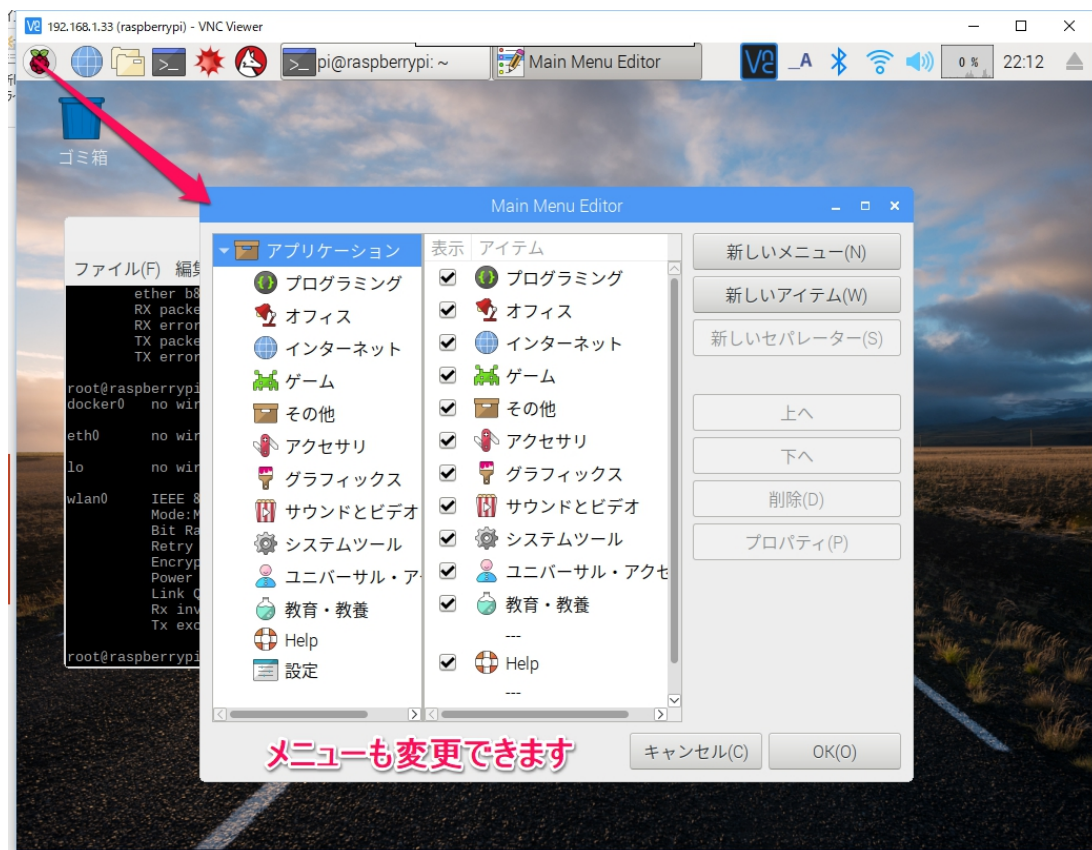
- メニュー
- ブラウザ
- ファイルマネージャ
- ターミナル
- マルチ画面選択

- VNC
- 日本語入力
- BLE
- WiFi
- 音量（ジャックで聴けます）
- 回線効率
- 時刻

プロトコル・アナライザ運用マニュアル

4. Raspberry Piの基本操作

② メニュー内容



メニュー内容

- プログラミング
- オフィス
- インターネット

カスタマイズ可能です。

プロトコル・アナライザ運用マニュアル

5. 日常運用

① セキュリティ対策(アンチウイルス更新、スキャン)

- アンチウイルス対策として無料のclamAVをインストールしてます。
- 手動での運用を基本としています。

パターンファイル更新

自動で更新されます。# freshclamはエラーになります。

手動でスキャン

\$ sudo clamscan --infected --remove --recursive
約5分かかります。

```
pi@raspberrypi: ~  
ファイル(F) 編集(E) タブ(T) ヘルプ(H)  
ERROR: /var/log/clamav/freshclam.log is locked by another  
ERROR: Problem with internal logger (UpdateLogFile = /var/  
og).  
root@raspberrypi: ~# leafpad /etc/clamav/freshclam.conf  
root@raspberrypi: ~# freshclam  
ClamAV update process started at Fri J  
main.cvd is up to date (version: 57, sigs: 4218790, f-level: 60, builder: mishh  
ammer)  
daily.cvd is up to date (version: 21862, sigs: 394456, f-level: 63, builder: neo  
)  
bytecode.cvd is up to date (version: 283, sigs: 53, f-level: 63, builder: neo)  
root@raspberrypi: ~# clamscan --infected --remove --recursive  
SCAN SUMMARY  
Known viruses: 4607906  
Engine version: 0.99.2  
Scanned directories: 264  
Scanned files: 2063  
Infected files: 0  
Data scanned: 61.31 MB  
Data read: 49.02 MB (ratio 1.25:1)  
Time: 71.844 sec (1 m 11 s)  
root@raspberrypi: ~#
```

手動でスキャン

プロトコル・アナライザ運用マニュアル

5. 日常運用

② インストール済パッケージの更新情報収集、アップグレード

- Linuxの場合は、頻繁に更新が発生します。アップデートとアップグレードを定期的実施してください。
- 更新前には、バックアップを取ることをお勧めします。特にアップグレードはまれに動作不良、戻せない状態が発生します。

```
pi@raspberrypi: ~  
ファイル(F) 編集(E) タブ(T) ヘルプ(H)  
Mem: 925 596 329 9 28 381  
-/+ buffers/cache: 186 739  
Swap: 99 0 99  
root@raspberrypi: ~# apt-get update  
ヒット http://archive.raspberrypi.org jessie/  
ヒット http://mirrordirector.raspbian.org jessie/contrib Translation-ja_JP  
ヒット http://archive.raspberrypi.org jessie/contrib Translation-ja  
ヒット http://mirrordirector.raspbian.org jessie/contrib Translation-en  
ヒット http://archive.raspberrypi.org jessie/main Translation-ja_JP  
ヒット http://mirrordirector.raspbian.org jessie/main Translation-ja  
ヒット http://mirrordirector.raspbian.org jessie/main Translation-en  
ヒット http://mirrordirector.raspbian.org jessie/non-free Translation-ja_JP  
無視 http://archive.raspberrypi.org jessie/non-free Translation-ja  
無視 http://archive.raspberrypi.org jessie/non-free Translation-en  
無視 http://archive.raspberrypi.org jessie/rpi Translation-en  
root@raspberrypi: ~# apt-get upgrade  
パッケージリストを読み込んでいます... 完了  
状態情報を読み取っています... 完了  
アップグレードパッケージを検出しています... 以下のパッケージが自動でインストー  
ルされましたが、もう必要とされていません:  
libwebrtc 0 rtkit  
これを削除するには 'apt-get autoremove' を利用してください。  
完了  
アップグレード: 0 個、新規インストール: 0 個、削除: 0 個、保留: 0 個。  
root@raspberrypi: ~#
```

更新情報収集

\$ sudo apt-get update

更新の実施

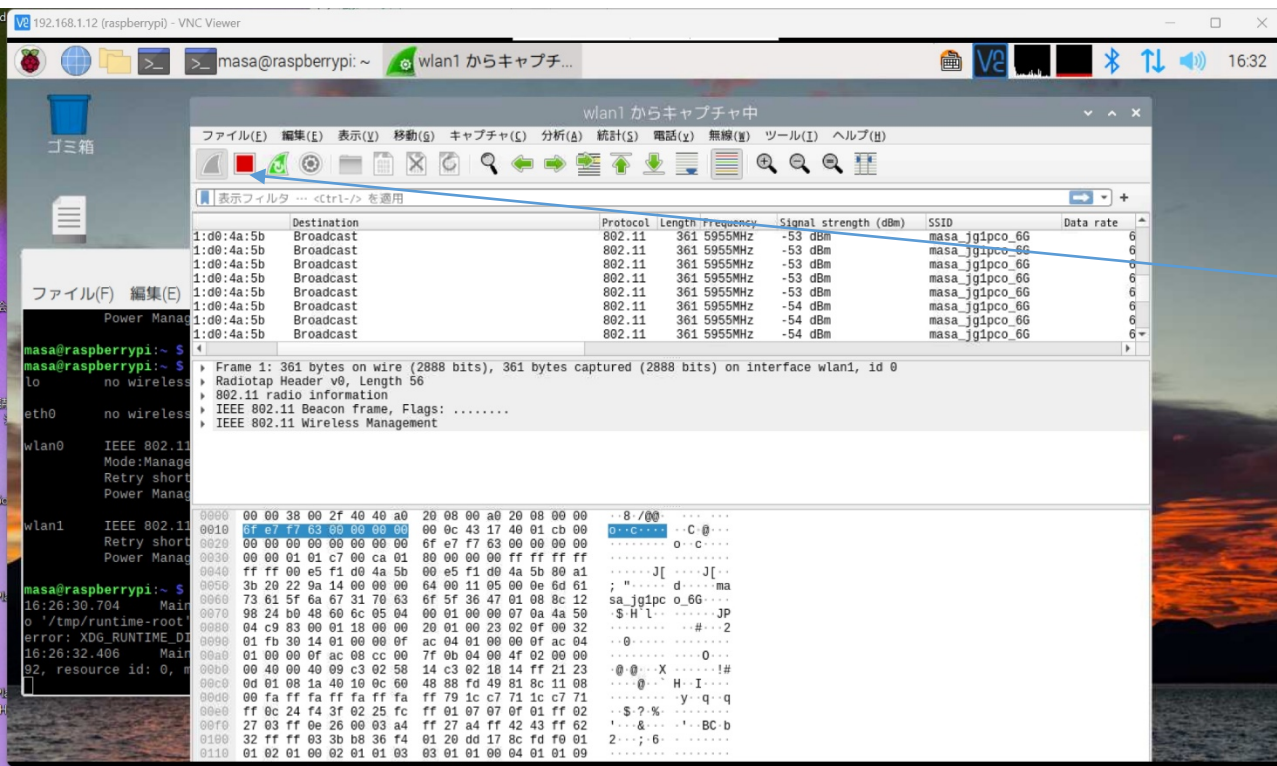
\$ sudo apt-get upgrade

必ず実施前にバックアップ

プロトコル・アナライザ運用マニュアル

6. Wifiプロトコル・データの取得

① WiFi6e 6GHzチャンネル モニタ Wiresharkによるパケット取得



\$ sudo wireshark
wireshark起動
オプション> wlan1選択し、開始
取得終了したら、赤ボタンで停止
ファイル>として保存。以下のフォルダ
/home/masa/Documents/wifi
ファイルをsamba経由で取り出す場合は、
権限を変更のこと。wifiフォルダ全部変
更の場合
\$ sudo chmod a=rwx -R wifi

プロトコル・アナライザ運用マニュアル

6. Wifiプロトコル・データの取得

② 2.4G/5GHzチャンネル モニタ 20MHz wlan1のモニタチャンネル設定

- 現在、netgearは、160MHzは未対応。
- 40MHz, 80MHzの設定は[こちら](#)へ

```
masa@raspberrypi: ~  
ファイル(F) 編集(E) タブ(T) ヘルプ(H)  
masa@raspberrypi:~ $ sudo iwconfig wlan1 freq 5180M  
masa@raspberrypi:~ $ iwconfig  
lo          no wireless extensions.  
  
eth0        no wireless extensions.  
  
wlan0       IEEE 802.11  ESSID:off/any  
            Mode:Managed  Access Point: Not-Associated  Tx-Power=31 dBm  
            Retry short limit:7  RTS thr:off  Fragment thr:off  
            Power Management:on  
  
wlan1       IEEE 802.11  Mode:Monitor  Frequency:5.18 GHz  Tx-Power=3 dBm  
            Retry short limit:7  RTS thr:off  Fragment thr:off  
            Power Management:on  
  
masa@raspberrypi:~ $ sudo iwconfig wlan1 channel 36  
masa@raspberrypi:~ $ iwconfig  
lo          no wireless extensions.  
  
eth0        no wireless extensions.  
  
wlan0       IEEE 802.11  ESSID:off/any  
            Mode:Managed  Access Point: Not-Associated  Tx-Power=31 dBm  
            Retry short limit:7  RTS thr:off  Fragment thr:off  
            Power Management:on  
  
wlan1       IEEE 802.11  Mode:Monitor  Frequency:5.18 GHz  Tx-Power=3 dBm  
            Retry short limit:7  RTS thr:off  Fragment thr:off
```

\$ sudo iwconfig wlan1 freq 5180M
又は
\$ sudo iwconfig wlan1 channel 36
\$ iwconfig
設定チャンネルを確認

別紙の[2.4GHz](#), [5GHz](#)チャンネル
配置を参照

プロトコル・アナライザ運用マニュアル

6. Wifiプロトコル・データの取得

⑤ airodumpを使ってスキャン 2.4G/5G

```

masa@raspberrypi: ~
ファイル(F) 編集(E) タブ(T) ヘルプ(H)

CH 1 ][ Elapsed: 6 s ][ 2023-03-22 14:03

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH ESSID
00:E5:F1:D0:4A:4E -43      4         0    0  11  360  WPA2 CCMP  SAE <length: 0>
18:EC:E7:24:AC:39 -69      2         0    0  11  130  WPA2 CCMP  PSK Extender-G-ACF0
00:E5:F1:D0:4A:49 -35      3         0    0  11  360  WPA2 CCMP  PSK masa_jg1pco_2G
0A:10:86:34:59:2B -64      4         0    0  11  54e. WEP WEP      aterm-c8108d-gw
08:10:86:34:59:2B -66      8         0    0  11  195  WPA2 CCMP  PSK aterm-c8108d-g
7E:3A:EF:E3:2E:92 -68      5         0    0  11  260  WPA2 CCMP  PSK KAONM-32E8D
74:3A:EF:E3:2E:91 -68      4         0    0  11  260  WPA2 CCMP  PSK KAONM-32E8D-G
D6:2C:46:86:B4:B3 -68      2         5    2  4  130  WPA3 CCMP  SAE Buffalo-G-B4B0-WPA
D6:2C:46:86:B4:B2 -70      3         2    0  4  130  WPA2 CCMP  PSK Buffalo-G-B4B0
A4:12:42:3E:BF:E2 -1       0         0    0  7   -1
74:03:BD:76:98:36 -88      3         0    0  1  130  WPA2 CCMP  PSK elecom-1269cf-5GHz
00:1C:7B:FB:4A:95 -69      6         0    0  1  130  WPA2 CCMP  PSK BCW710J-C93EE-G
DC:FB:02:D5:81:F1 -86      2         0    0  1  130  WPA2 CCMP  PSK Buffalo-G-81F0
50:29:4D:10:3B:2A -37      7         5    0  1  130  WPA2 CCMP  PSK Gw_103B2B
9E:77:E7:71:AD:AC -62      5         0    0  1  260  WPA2 CCMP  PSK KAONM-1ADA7
98:77:E7:71:AD:AB -62      5         0    0  1  260  WPA2 CCMP  PSK KAONM-1ADA7-G
90:F3:05:E1:BE:BA -93      2         0    0  1  130  WPA2 CCMP  PSK HUMAX-1BEAD
00:E5:F1:D0:4A:57 -34      2         0    0 100  866  WPA3 CCMP  SAE <length: 0>
00:E5:F1:D0:4A:52 -35      2         0    0 100  866  WPA2 CCMP  PSK masa_jg1pco_5G

BSSID          STATION          PWR   Rate   Lost  Frames  Notes  Probes
00:E5:F1:D0:4A:49 7C:D5:66:92:75:91 -42   24e-24e    0    16
00:E5:F1:D0:4A:49 40:B4:CD:62:7F:D6 -49   24e-24e    0    24
  
```

アクセスポイント側

端末側

airodumpで全チャンネルスキャンします。
 周辺のアクセスポイントの状況確認に使用
 2.4G/5G(ch140まで)の場合
 \$ sudo airodump-ng --band abg wlan1

スキャンを停止する場合は**CTL**と**c**を同時に押してください。

6GHzの全チャンネルの場合

\$ sudo airodump-ng -C 5955-6415 wlan1

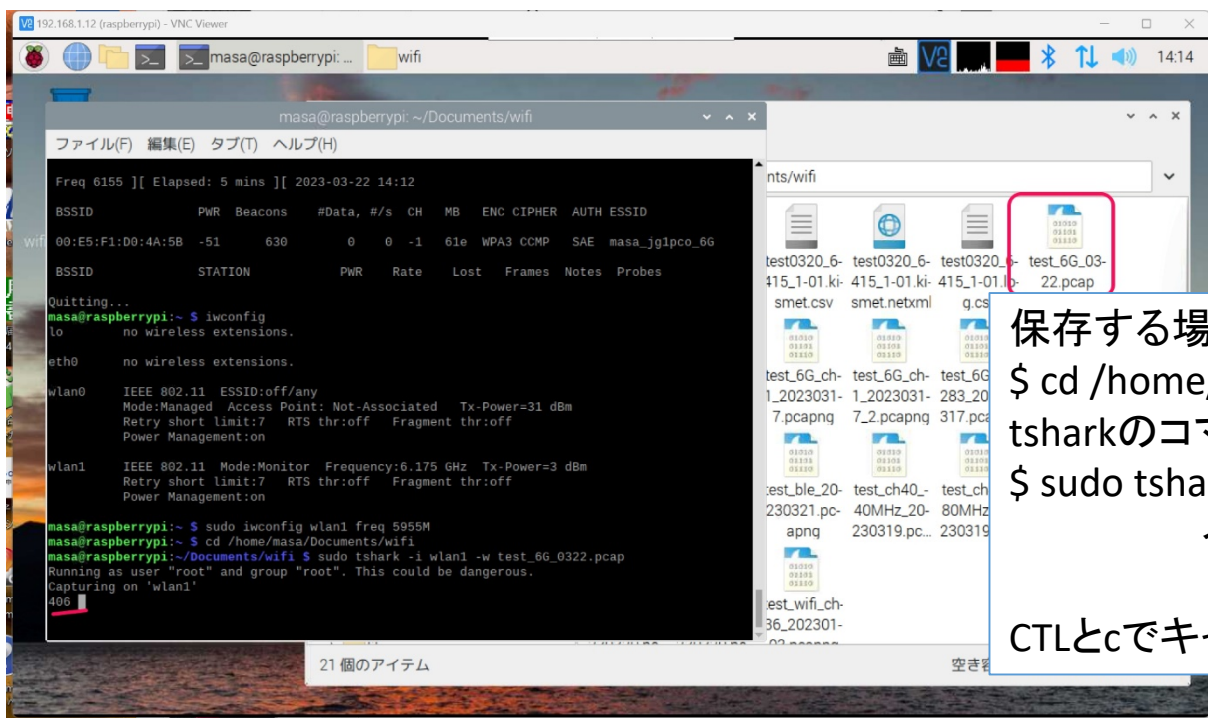
- 個別に複数のチャンネルを指定することもできます。
- 使用チャンネル、暗号化方式などがわかります。
- Macアドレスなどが含まれてますので、個人情報保護法に基づいて使用してください。

プロトコル・アナライザ運用マニュアル

6. Wifiプロトコル・データの取得

⑦ tsharkによるデータ取得

wiresharkのGUIの場合途中止まるとデータがなくなるおそれがあるので、ファイルに都度書き込むtsharkを使います。



保存する場所に切り替えます。

```
$ cd /home/masa/Documents/wifi
```

tsharkのコマンド

```
$ sudo tshark -i wlan1 -w test_6G_0322.pcap
```

インタフェース ファイル名

CTLとcでキャプチャを停止します。

プロトコル・アナライザ運用マニュアル

7. LANプロトコル・データの取得

- ① LAN上のプロトコル・データの取得してみます。Wifiと同じです。

```
masa@raspberrypi: ~/Documents
ファイル(F) 編集(E) タブ(T) ヘルプ(H)
masa@raspberrypi:~/Documents/wifi $ cd ..]
bash: cd: ..]: そのようなファイルやディレクトリはありません
masa@raspberrypi:~/Documents/wifi $ cd ..
masa@raspberrypi:~/Documents $ sudo chmod a=rwx -R wifi
masa@raspberrypi:~/Documents $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.12  netmask 255.255.255.0  broadcast 192.168.1.255
    inet6 fe80::37e5:f04f:ac1f:f57b  prefixlen 64  scopeid 0x20<link>
    inet6 2405:6582:2ea0:4900:fd36:fd5:9558:ee82  prefixlen 64  scopeid 0x0<global>
    ether dc:a6:32:70:ea:34  txqueuelen 1000  (イーサネット)
    RX packets 119583  bytes 11382760 (10.8 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 78755  bytes 46469232 (44.3 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (ローカルループバック)
    RX packets 222  bytes 15909 (15.5 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 222  bytes 15909 (15.5 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
    ether dc:a6:32:70:ea:35  txqueuelen 1000  (イーサネット)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

wlan1: flags=803<UP,BROADCAST,NOTRAILERS,PROMISC,ALLMULTI>  mtu 1500
```

LANポートにケーブルを接続します。
インタフェースの状態を確認します。
ifconfig
eth0がインターフェース名になります。
IPアドレスが確認できます。

プロトコル・アナライザ運用マニュアル

8. BLEのプロトコル・データの取得

① hci0のプロトコル・データの取得

```
masa@raspberrypi: ~  
ファイル(F) 編集(E) タブ(T) ヘルプ(H)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
ether dc:a6:32:70:ea:35 txqueuelen 1000 (イーサネット)  
RX packets 0 bytes 0 (0.0 B)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 0 bytes 0 (0.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
wlan1: flags=803<UP,BROADCAST,NOTRAILERS,PROMISC,ALLMULTI> mtu 1500  
unspec 94-18-65-3D-72-2C-18-0C-00-00-00-00-00-00-00-00 txqueuelen 1000  
RX packets 714053 bytes 188506503 (179.7 MiB)  
RX errors 0 dropped 1 overruns 0 frame 0  
TX packets 34 bytes 4531 (4.4 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
masa@raspberrypi:~/Documents $ sudo wireshark  
14:21:26.084 Main Warn QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-masa@raspberrypi'  
error: XDG_RUNTIME_DIR not set in the environment.  
14:21:27.737 Main Warn QXcbConnection: XCB error: 148 (Unknown), sequence: 192, resource id: 0, major code: 140 (Unknown), minor code: 20  
masa@raspberrypi:~/Documents $ cd  
masa@raspberrypi:~ $ hciconfig  
hci0: Type: Primary Bus: UART  
BD Address: B8:27:EB:55:26:88 ACL MTU: 1021:8 SCO MTU: 64:1  
UP RUNNING  
RX bytes:2203 acl:0 sco:0 events:130 errors:0  
TX bytes:3968 acl:0 sco:0 commands:130 errors:0  
masa@raspberrypi:~ $
```

BLEの状態を表示します。

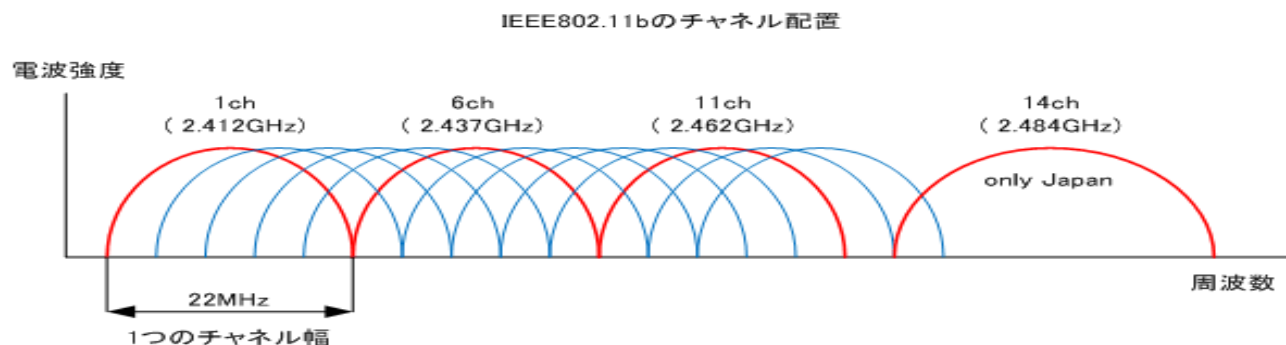
\$ hciconfig

Up runningになっていない場合は、インタフェースをupします。

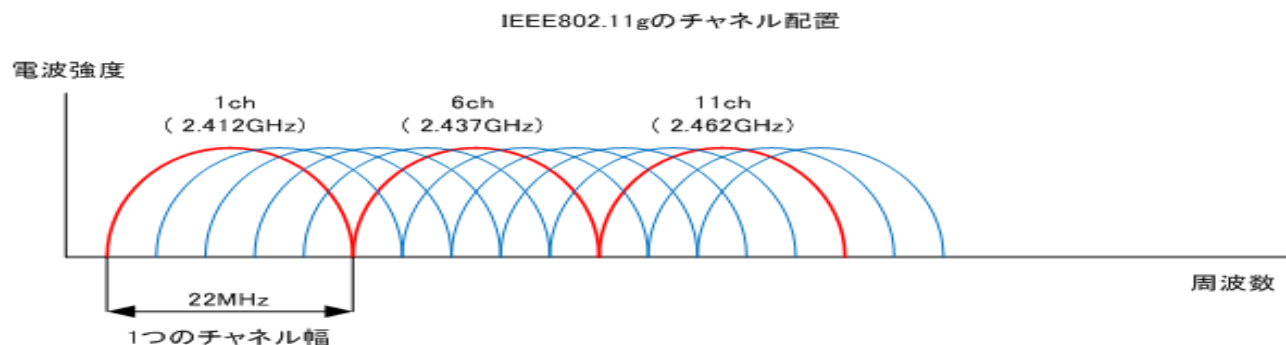
\$ sudo hciconfig hci0 up

参考

2.4GHzチャンネル配置

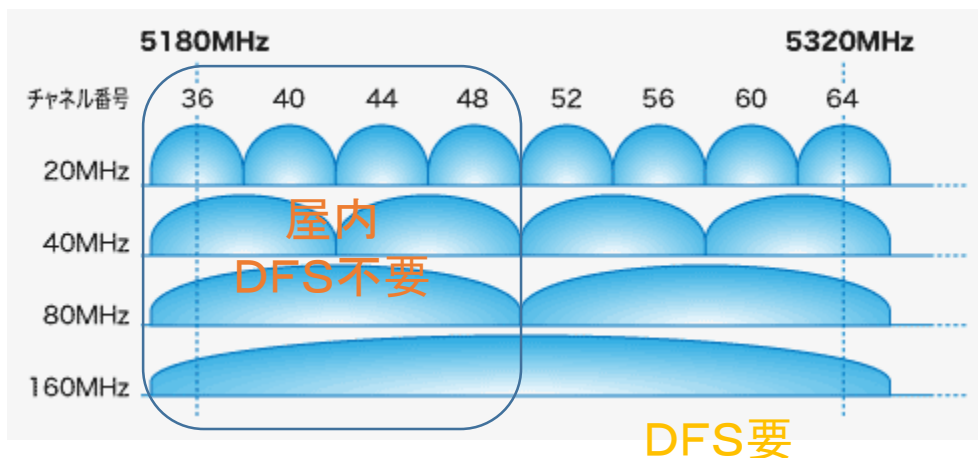


屋内外

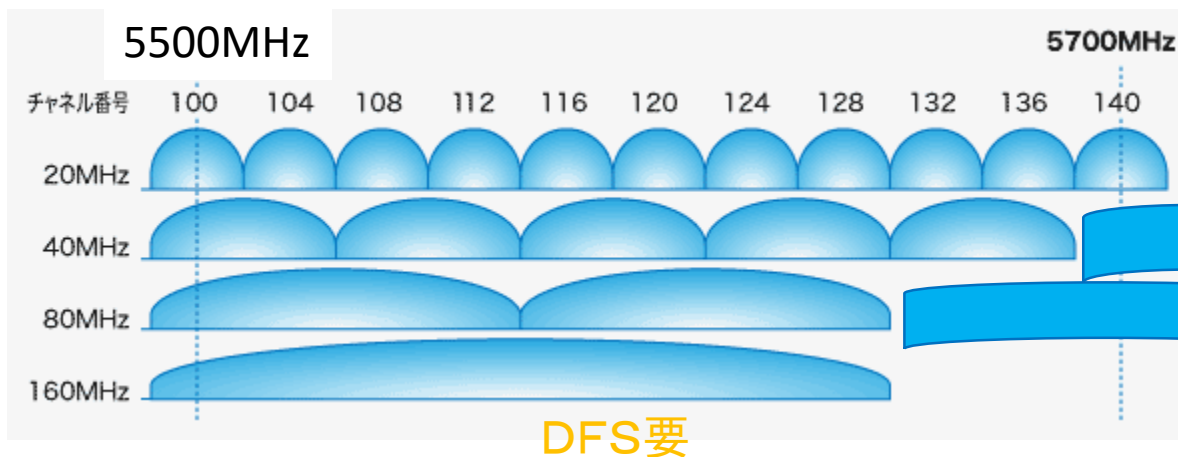


- 周波数帯: 2.4GHz-2.5GHzの100MHz
- チャンネル番号は、CH1-CH14。通常使っているのは3波(CH1, CH6, CH11)

5GHzチャンネル配置



屋内(固定衛星up、無線標定(気象レーダ)、地球探査衛星に割り当てられているため)



5720MHz

144(新規追加:201811)

屋内外

周波数帯: 5.15GHz-5.35GHz, 5.47GHz-5.73GHzの460MHz
CH番号: CH36-CH64までの8ch, CH100-CH144までの12CH

Wifi6e 6GHzチャンネル配置

ch	freq(MHz) 20M	40M	80M	160M
1	5955			
3		5965		
5	5975			
7			5985	
9	5995			
11		6005		
13	6015			
15				6025
17	6035			
19		6045		
21	6055			
23			6065	
25	6075			
27		6085		
29	6095			
31				
33	6115			
35		6125		
37	6135			
39			6145	
41	6155			
43		6165		
45	6175			
47				6185
49	6195			
51		6205		
53	6215			

ch	freq(MHz) 20M	40M	80M	160M
55			6225	
57	6235			
59		6245		
61	6255			
63				
65	6275			
67		6285		
69	6295			
71			6305	
73	6315			
75		6325		
77	6335			
79				6345
81	6355			
83		6365		
85	6375			
87			6385	
89	6395			
91		6405		
93	6415			

6GHzのチャンネル

- 20MHz帯域: 24ch
- 40MHz帯域: 12ch
- 80MHz帯域: 6ch
- 160MHz帯域: 3ch

表が各チャンネルと中心周波数