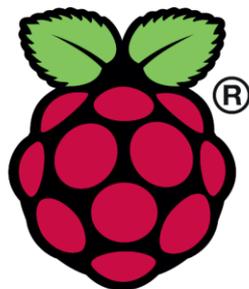


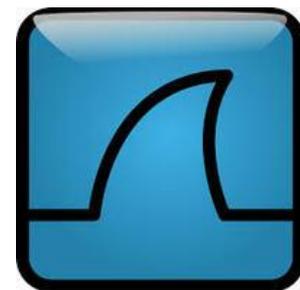
抜粋版

WiFiプロトコル・アナライザ V3

～Raspberry Pi5を使いwifi7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	3
2.	Linux基本的なコマンド	3
3.	プロトコル・アナライザ関係コマンド	4
4.	Raspberry Pi基本操作	6
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)	7
	• パッケージの更新	8
	WiFiプロトコルアナライザ V3 接続構成	9
1.	ハード概要	10
2.	ソフト概要	11
3.	Wifiツールの使い方	12
4.	Wifiプロトコル・データの取得	
	① 6GHzチャンネル モニタ 20MHz-160MHz、MLO	14
	② 2.4G/5G チャンネル モニタ 20MHz-160MHz	20
	③ airodumpを使ってスキャン 2.4G/5G	27
	④ tsharkによるデータ取得	28
	⑤ kismetによるデータ取得	29
	⑥ wavemonによるデータ取得	36
	⑦ horstlによるデータ取得	37
5.	LANプロトコル・データの取得	38
6.	BLEプロトコル・データの取得	40

参考

2.4GHz チャンネル配置

5GHz チャンネル配置

2.4G/5G チャンネル番号: 中心周波数

6GHz チャンネル配置

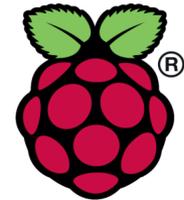
チャンネル番号: 中心周波数

Wifi7 6GHz 分析例

抜粋版のため、ページと一致しません

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のスキヤン: 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

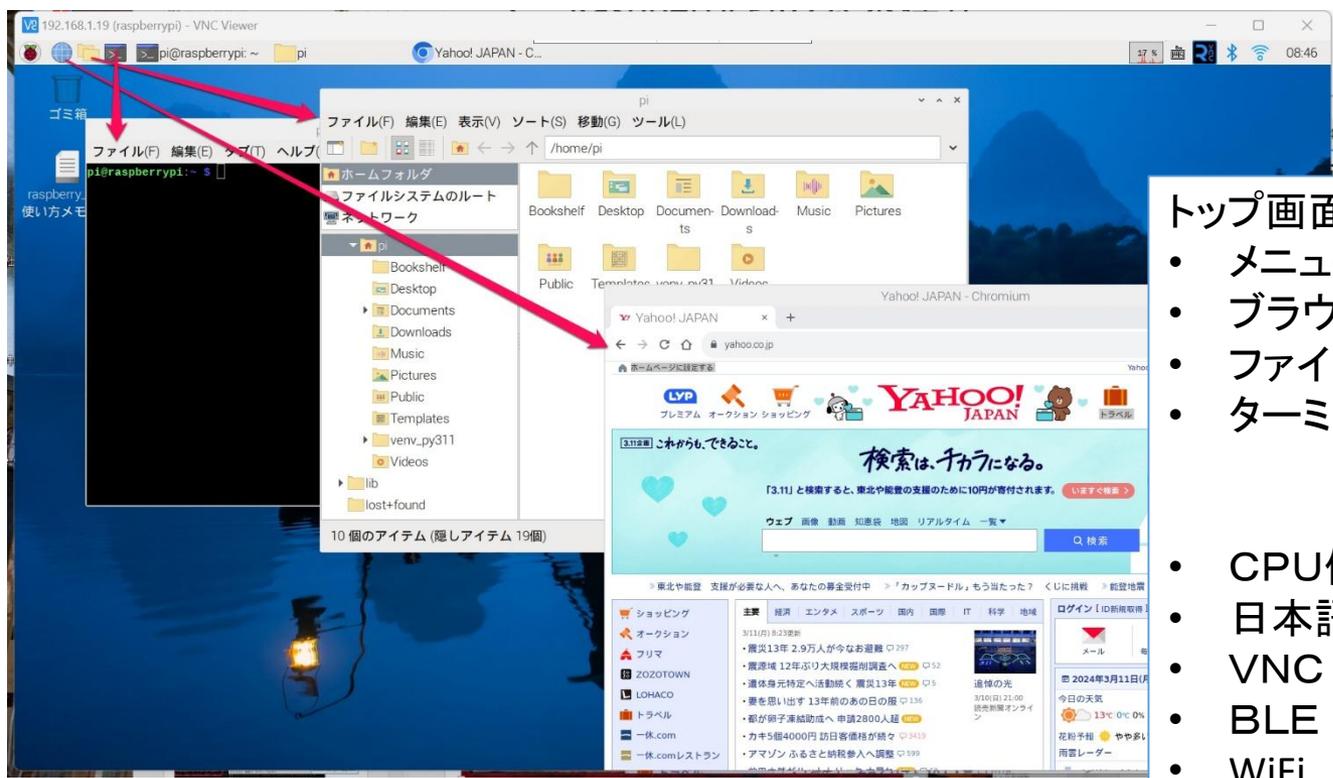


Raspberry Pi

RaspberryPi運用マニュアル

4. Raspberry Piの基本操作

① 表示画面と内容

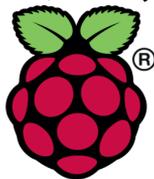


トップ画面(上段のタスクバーで選択)

- メニュー
- ブラウザ
- ファイルマネージャ
- ターミナル

- CPU使用率
- 日本語入力
- VNC
- BLE
- WiFi
- 時刻

WiFiプロトコルアナライザ V3 接続構成



Raspberry Pi5

Raspberry Pi



Wifi7 USB

インターネット接続用

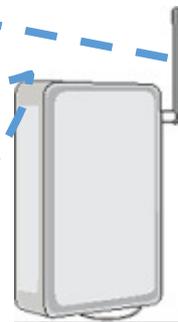
microHDMI

初回設定時のみ
モニター接続し設定

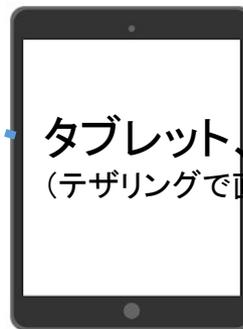
マイクロUSB
電源 (TypeC)



VNC接続



インター
ネット



タブレット、スマホ、PCなど
(テザリングで直接接続も可能)

1. ハード概要

本体

品名	項目	内容	備考
Raspberry Pi5	CPU	2.4GHz 4コア Cortex-A76 (ARMv8、64bit)	
	GPU	VideoCore VII®	
	メモリ	4GB RAM	
	OS	Raspbian bookworm(Debianベース)	
	インターフェース	2.4/5GHz WiFi(802.11 bgnac), Bluetooth 5.0, BLE, 1G ether, USB 2.0x2, USB 3.0x2, micro HDMIx2, microSDカード, 40 GPIO pin	
	電源／消費電力	Micro USB Type C 3.0A	
	サイズ	85x56x18mm	
Wifi7 usb	Tp-link Archer TBE400UH	IEEE 802.11a/b/g/n/ac/ax/be 6GHz : 2,882Mbps + 5GHz : 2,882Mbps + 2.4GHz : 688Mbps	MLO実施の場合、2個以上のUSBが必要
付属品		内容	備考
ケース		赤白、FAN付。	
microSD 64GB		Raspbian OS, 必要なモジュールをインストールして提供します。お客様が設定するものは必要最低限のパスワード設定、WiFi設定になります。	
プログラム		Wireshark, kismet, airodump-ngなど インストール済	
マニュアル		設定編、運用編	

USB電源ケーブル、HDMIケーブルは付属していません。
別途オプション品を購入ください

2. ソフト概要

提供するソフトウェアの概要です。

区分	ソフト名	バージョン	備考
OS	Raspbian	Bookworm 64bit	Kernel:6.12.62
ネットワーク関係	iw	5.19	
	nwcli	1.42.4	
プログラム言語	python3	3.11.2	
アプリ	airodump-ng	1.7	
	wireshark	4.0.17	tshark
	kismet	2026.02	
	Wavemon	0.9.7	
	horst	5.1	

3. wifiツールの使い方

お勧め

① 各ツールの特徴と使い方

ツール名	主な用途	モニターモード 対応	帯域幅の扱い	6GHz対応	強み	弱み	弊社からのお勧め
Wireshark/tshark	パケット・プロ トコル解析	対応	チャンネル構造 (20+20など)を 表示、実際の NIC帯域幅は不 可	対応	詳細解析、 HE/EHT情報	実帯域幅は分 からない	故障、製品開発な どのパケット解 析、MLO対応
Kismet	スキャン、 AP/STA一覧、 ログ	対応	帯域幅は不可	対応	広域スキャン、 6GHzホッピング グ	帯域幅/RSSI時 系列が弱い	使用チャンネル把 握、利用アクセスポ イント把握
airodump-ng	チャンネルス キャン、AP/STA 一覧	対応	帯域幅は不可	部分対応	軽量スキャン	6GHz制限多い、 帯域幅なし	同上、6GHz未対応
horst	軽量リアルタ イムモニタ	対応	帯域幅は不可	部分対応	軽量、リアルタ イム	6GHz情報が少 ない	kismetの軽量版
wavemon	接続状態監視	部分対応	接続時のみ帯 域幅が見える、 モニターモード 不可	部分対応	RSSI/SNR可視 化	モニターモード では帯域幅なし	信号強度のグラフ
iw	ドライバ状態、 周波数/帯域 幅設定	対応	実際のNIC帯域 幅 (20/40/80/160 MHz)を表示	対応	正確な帯域幅 情報	パケット解析不 可	インターフェースの 把握

プロトコル・アナライザ運用マニュアル

4. Wifiプロトコル・データの取得

- ① 6GHzチャンネル モニタ 20MHz-160MHz
wlan1のモニタチャンネル設定

```

pi@raspberrypi: ~
ファイル(F) 編集(E) タブ(T) ヘルプ(H)
ifindex 4
wdev 0x200000001
addr e0:d3:62:5f:1f:4b
type monitor
wiphy 2
channel 1 (2412 MHz), width: 20 MHz (no HT), center1: 2412 MHz
multicast TXQ:
      qsz-byt qsz-pkt flows  drops  marks  overlmt hashcol tx-bytes
tx-packets
      0      0      0      0      0      0      0      0
pi@raspberrypi:~ $ sudo iw dev wlan1 set freq 6295 160MHz
pi@raspberrypi:~ $ iw wlan1 info
Interface wlan1
  ifindex 4
  wdev 0x200000001
  addr e0:d3:62:5f:1f:4b
  type monitor
  wiphy 2
  channel 69 (6295 MHz), width: 160 MHz, center1: 6345 MHz
  multicast TXQ:
        qsz-byt qsz-pkt flows  drops  marks  overlmt hashcol tx-bytes
tx-packets
        0      0      0      0      0      0      0      0
pi@raspberrypi:~ $

```

```

$ sudo iw dev wlan1 set freq 6295 160MHz
$ iw wlan1 info
設定チャンネルを確認
6GHzはチャンネルでの設定はできません。
先頭チャンネルの周波数から設定する場合は、以下
sudo iw dev wlan1 set freq 5955 HT20
sudo iw dev wlan1 set freq 5955 HT40+
sudo iw dev wlan1 set freq 5955 80MHz
sudo iw dev wlan1 set freq 5955 160MHz
センタ周波数を設定する場合
sudo iw dev wlan1 set freq 5955 40 5965
sudo iw dev wlan1 set freq 5955 160 6025

```

```

iw [options] dev <devname> set freq <freq>
[NOHT|HT20|HT40+|HT40-|5MHz|10MHz|80MHz|160MHz]

Iw dev <devname> set freq <control freq>
[5|10|20|40|80|80+80|160] [<center1_freq> [<center2_freq>]]

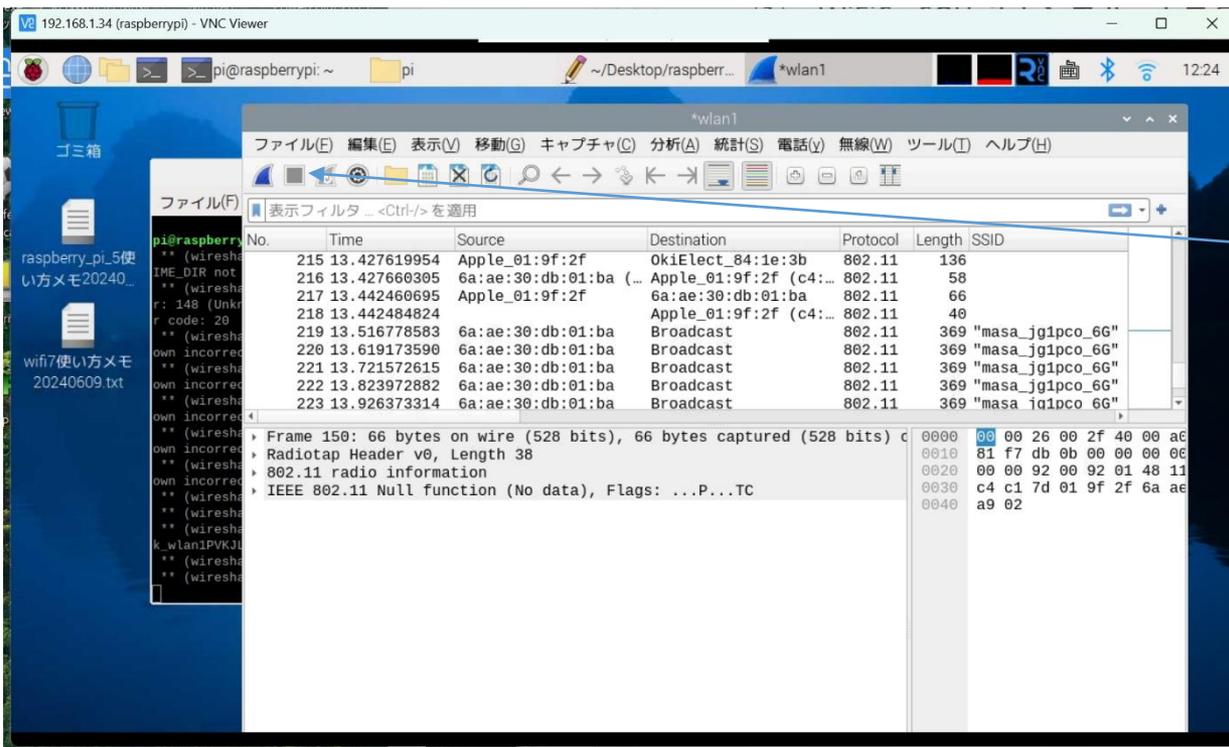
```

別紙の[6GHz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

4. Wifiプロトコル・データの取得

- ① 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/pi/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
```

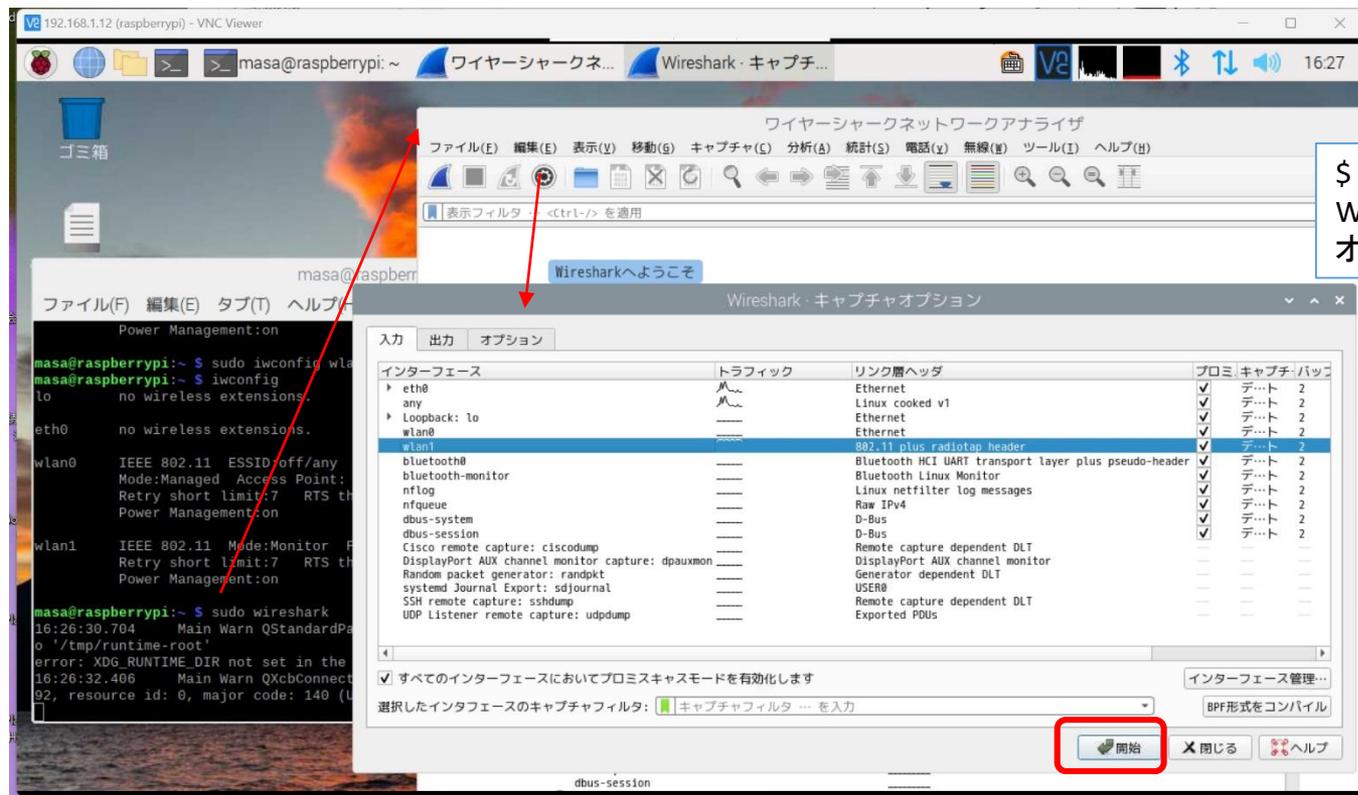
powerBIを使った分析例: オプションで提供可能

プロトコル・アナライザ運用マニュアル

4. 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

Wiresharkによるパケット取得

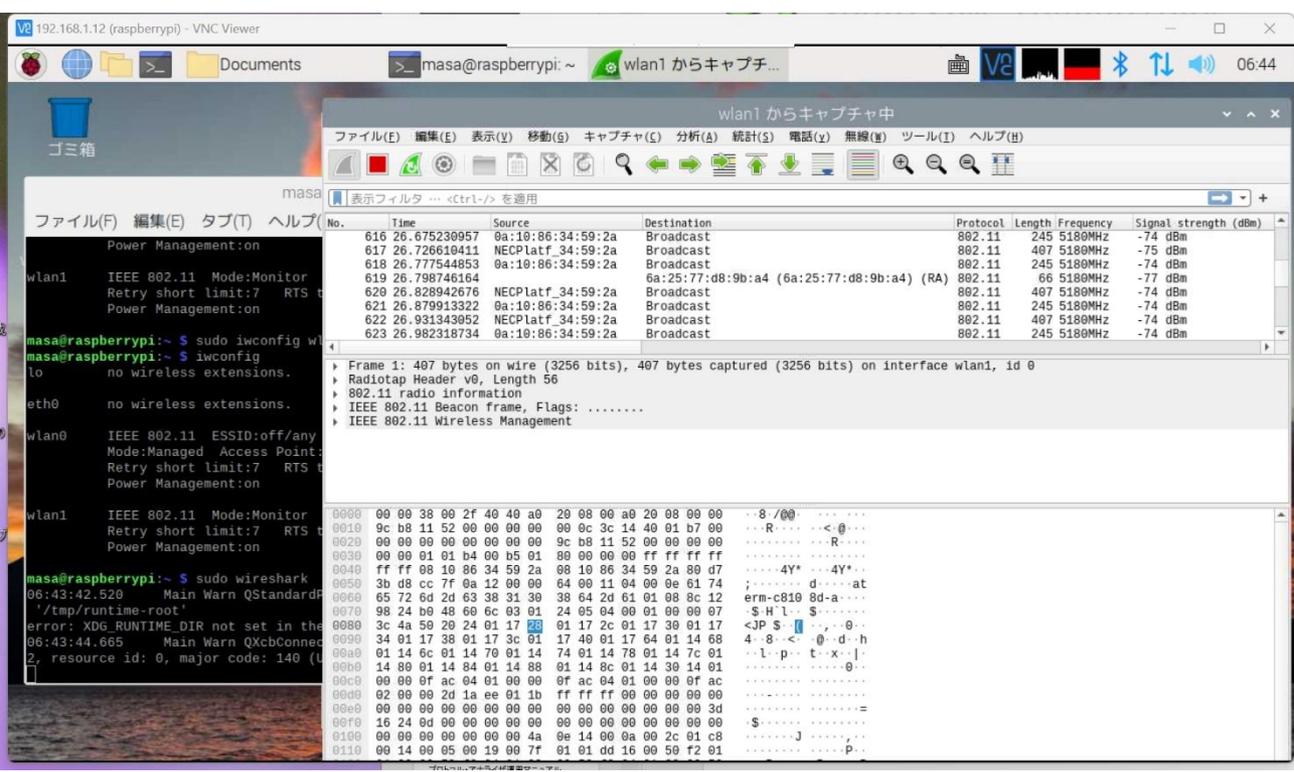


\$ sudo wireshark
Wireshark起動
オプション> wlan1選択し、開始

プロトコル・アナライザ運用マニュアル

4. 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
- 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/pi/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

4. Wifiプロトコル・データの取得

③ airodumpを使ってスキャン 2.4G/5G

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、モニターモードで。
 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**を同時に押しください。

6GHzの全チャンネルの場合
 \$ sudo airodump-ng -C 5955-6415 wlan1 **動作しません**
 Kismetを使用のこと

- 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。

```

pi@raspberrypi: ~
ファイル(F) 編集(E) タブ(T) ヘルプ(H)
pi@raspberrypi:~$ sudo ip link set wlan1 up
pi@raspberrypi:~$ sudo airodump-ng --band abg wlan1

CH 159 ][ Elapsed: 1 min ][ 2026-03-01 06:54

BSSID          PWR  Beacons  #Data,  /s  CH  ENC  CIPHER  AUTH  ESSID
-----
B6:12:42      -91      2          0  0  7  54e.  WEP  WEP      <len
74:03:BD      -94     11          0  0 116 866  WPA2  CCMP   PSK  elec
0E:34:AF      -97      4          0  0 108 1733 WPA2  CCMP   PSK  <len
9A:77:E7      -85     12          0  0 108 1733 WPA2  CCMP   PSK  KAONI
98:77:E7      -85     12          0  0 108 1733 WPA2  CCMP   PSK  KAONI
7C:13:1D      -75     11          0  0 100 1733 WPA2  CCMP   PSK  7C13
94:09:37      -81     12          0  0 100 1170 WPA2  CCMP   PSK  HUMA
02:24:6B      -97      7          0  0  44 866  WPA2  CCMP   PSK  5Gssi
02:24:6B      -96     10          0  0  44 54e.  WEP  WEP      5Gsg
DC:FB:02      -95      9          0  0  44 270  WPA2  CCMP   PSK  Buffi
00:00:00      -1       0          0  0 -1 -1
40:AE:30      -35     10          2  0  36 866  WPA2  CCMP   PSK  masa
34:3D:C4      -80     11          0  0  36 390  WPA2  CCMP   PSK  HUMA
EE:5A:31      -69     12          0  0  36 866  WPA2  CCMP   PSK  Buffi
D4:2C:46      -69     12          0  0  36 1733 WPA3  CCMP   SAE  Buffi
D4:2C:46      -69     12          0  0  36 1733 WPA2  CCMP   PSK  Buffi
    
```

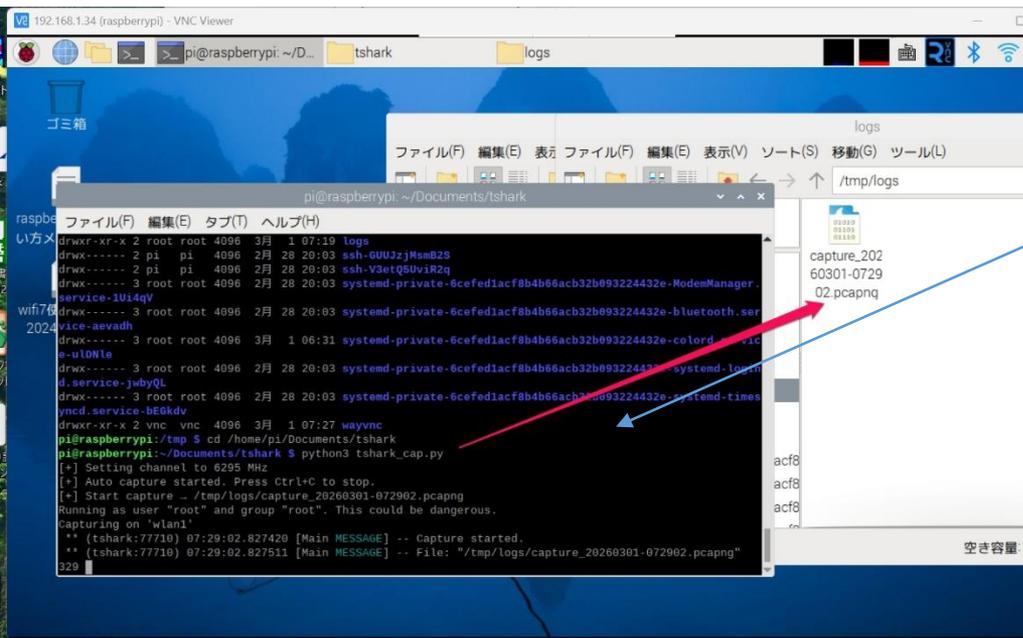
アクセスポイント側

プロトコル・アナライザ運用マニュアル

4. Wifiプロトコル・データの取得

④ 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。



自動プログラム

```

$ cd /home/pi/Documents/tshark
設定: tshark_cap.py
$ sudo mousepad tshark_cap.py
/tmp/logsのroot配下でないと保存できません
$ python3 tshark_cap.py
    
```

又は

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。

ファイルをsamba経由で取り出す場合は、権限を変更のこと。logsフォルダ全部変更の場合

```

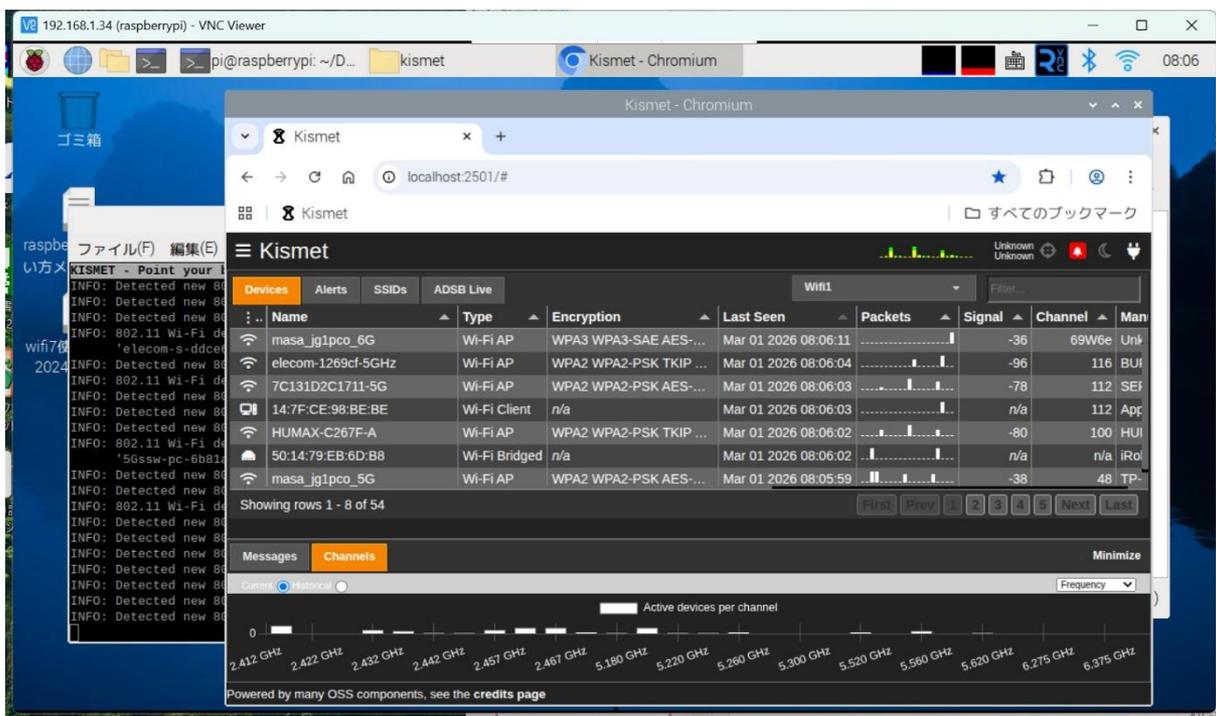
$ sudo chmod a=rwx -R logs
    
```

プロトコル・アナライザ運用マニュアル

4. Wifiプロトコル・データの取得

⑤ kismetによるデータ取得 全チャンネル

Wifiの可視化ツールになります。アクセスポイントのSSID,チャンネル、信号の強さがわかります。下にチャンネルの使用状況がわかります。6Gなどのチャンネルを調べるのに有効です。



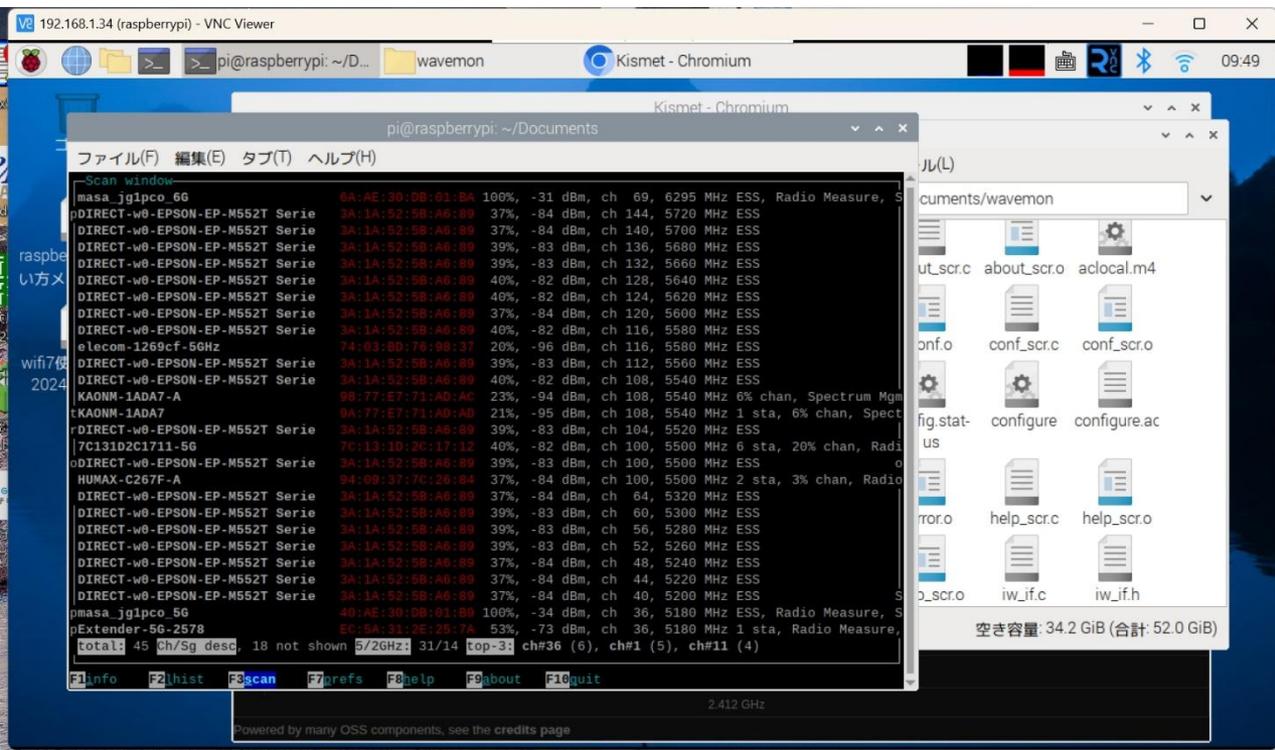
```
$ kismet -c wlan1:name=Wifi1 全チャンネル
```

ブラウザにアクセス
<http://localhost:2501>

プロトコル・アナライザ運用マニュアル

4. Wifiプロトコル・データの取得

- ⑥ wavemonによるデータ取得 6Gなどのチャンネル番号を高速に取得
Wifiの可視化ツールになります。



モニタモードにしなくてもOK
\$ sudo wavemon
F3でスキャン開始
F1はwlan1でAPに接続していると出力

プロトコル・アナライザ運用マニュアル

4. Wifiプロトコル・データの取得

⑦ horstによるデータ取得 信号強度のグラフ表示
Wifiの可視化ツールになります。2.4G/5Gのみ

モニタモードにしなくてもOK
\$ sudo horst -i wlan1
Sでグラフ表示、cで変更？動かない
hで信号強度履歴

The screenshot shows the horst tool running on a Raspberry Pi. The terminal output lists detected WiFi networks:

PK/ReX-Cha-Sig-RAT-TRANSMITTER	NODE-ST-MHz-TxR-ENCR-ESSID	INFO
14/0%	1 -79 6 3a:1a:52:5b:a6:89 AP	n 20 1x1 WPA2 DIRECT-w0-EPSON-EP-M552T Series
6/3%	1 -86 1 dc:fb:02:d5:81:f1 AP	n 20 0x2 WPA2 Buffalo-G-81F0
7/4%	1 -88 1 10:ef:3f:64:80:a2 AP	n 20 0x2 WPA12 106F3F6480A2
9/0%	1 -45 1 50:29:4d:10:3b:2a AP	n 20 0x2 WPA12 GW 103320
-10/2%	2 -36 1 40:ae:30:db:01:b8 AP	ac 80 2x2 WPA2 masa_jgipco_26
27/1%	1 -68 1 94:09:37:7c:26:8c AP	n 20 0x2 WPA12 HUMAX-C267F
6/27%	1 -83 6 ca:09:db:47:d3:a4 ST	bg 20 WPA12 HUMAX-C267F
1 -86 1 a8:c2:66:7e:a9:84 PR	n 40-0	
0/0%	2 -45 1 7c:d5:66:92:75:91 ST	bg 20
0/0%	2 -32 1 00:22:cf:fe:6d:b5 ST	bg 20
0/0%	1 -95 6 b6:16:4b:8c:69:7e	bg 20
0/0%	1 -41 1 b9:27:eb:a7:92:f2 PR	n 20 0
0/0%	1 -76 1 38:1a:52:5b:26:89 ST	bg 20
0/0%	2 -69 1 b8:27:eb:7e:88:86 PR	n 20 0

The bar chart shows signal strength (dBm) for channels 01 through 14 and 36 through 40. Channel 40 shows the highest signal strength at approximately -45 dBm.

The 'Signal/Rate History' graph shows a green signal trace over time, with a peak in signal strength around the 14th second.

プロトコル・アナライザ運用マニュアル

5. LANプロトコル・データの取得

- ① LAN上のプロトコル・データの取得して見ます。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:fd36:fd36:fd36  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

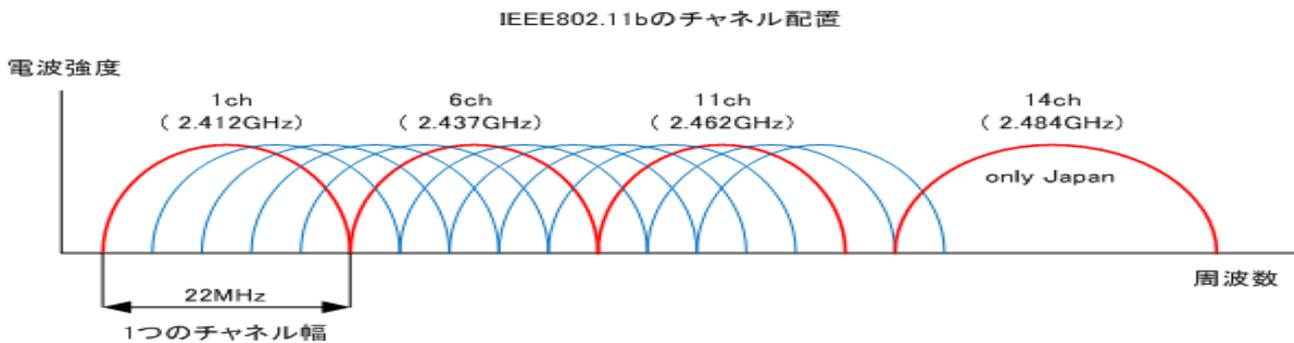
wlan1: flags=803<UP,BROADCAST,NOTRAILERS,PROMISC,ALLMULTI>  mtu 1500

```

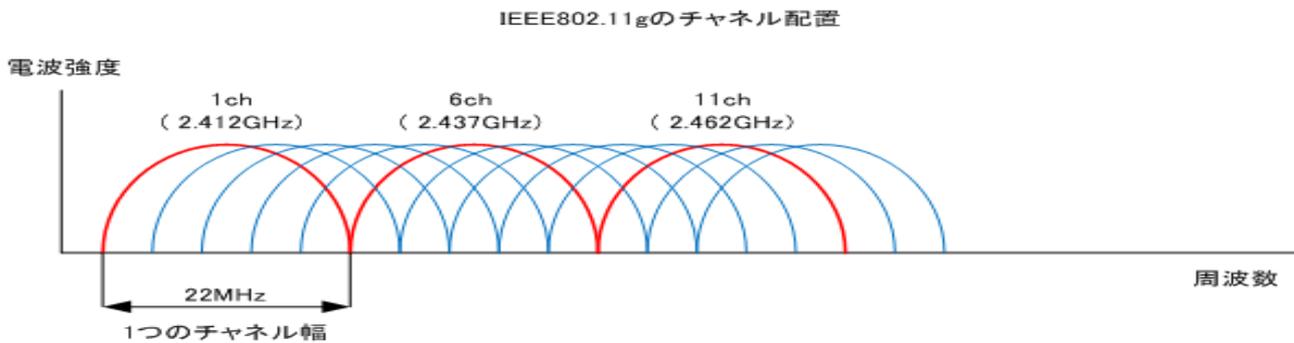
LANポートにケーブルを接続します。
 インタフェースの状態を確認します。
 # ifconfig
 eth0がインターフェース名になります。
 IPアドレスが確認できます。

参考

2.4GHzチャンネル配置

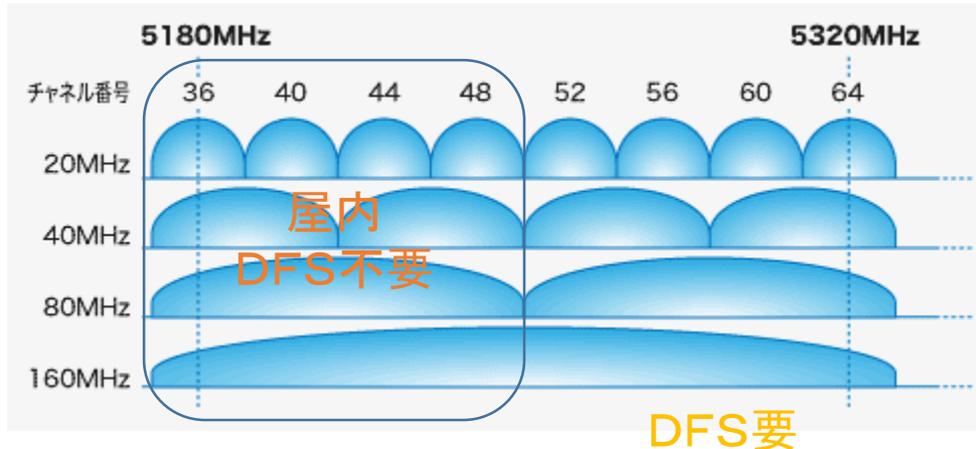


屋内外

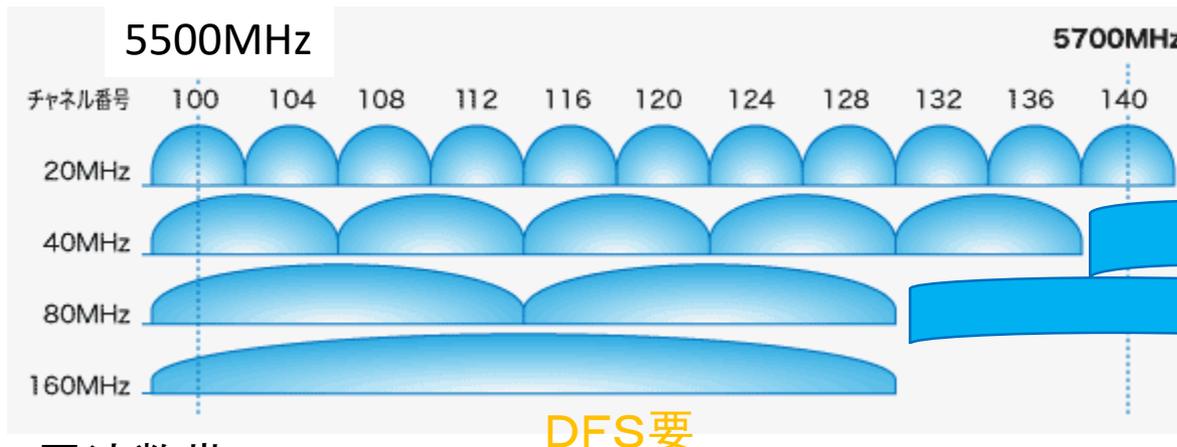


- 周波数帯: 2.4GHz-2.5GHzの100MHz
- チャンネル番号は、CH1-CH14。通常使っているのは3波(CH1, CH6, CH11)
- 詳細の周波数は、[こちら](#)

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)



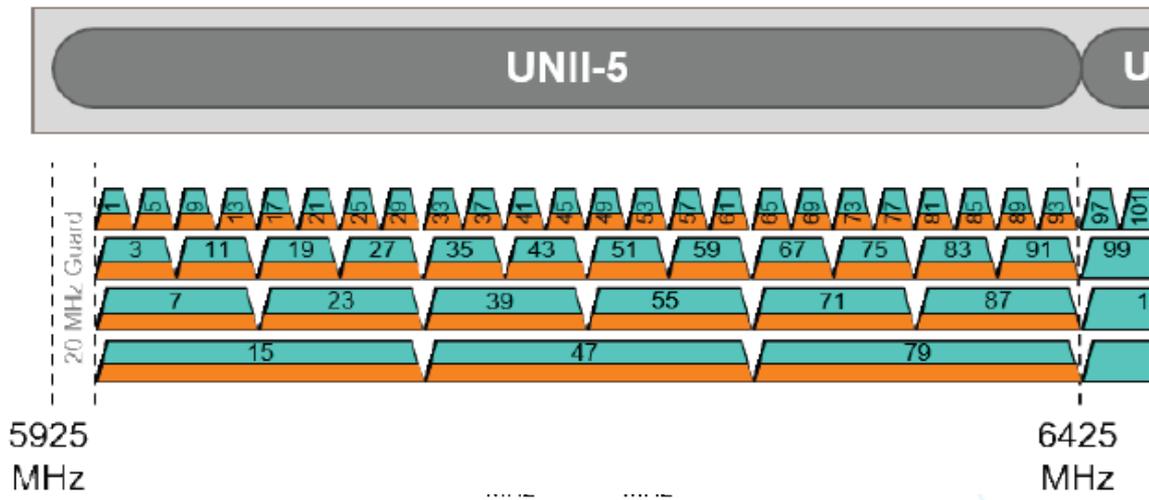
5720MHz
144(新規追加:201811)

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
 詳細の周波数は、[こちら](#)

周波数配置 (6GHz)

- 日本でのWiFi7/7は以下のチャンネル
- 5925MHz-6425MHz:480MHz帯域
- 20MHzx24ch、40MHzx12ch、80MHz x 6ch、160MHz x 3ch
- Ch1:5955MHz-ch93:6415MHz (20MHz帯域)
- PSC (Preferred Scanning Channel) : 37,53,69,85



= Low Power Indoor (LPI) Only
 = LPI & Automatic Frequency Coordination (AFC)

詳細の周波数は、[こちら](#)

