

抜粋版

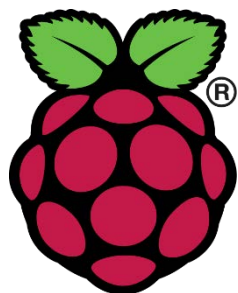
遠隔モニタ設定・運用マニュアル

スペクトラム・テクノロジー株式会社

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

sales@spectrum-tech.co.jp

筑波大学大学院研究プロジェクト



目次

ページ

1. 設定編	4
① 全体構成	5
② ソフトインストール	
• VPNサーバ	7
• 管理マネジャ	7
• VPNクライアント	11
③ 管理マネジャ設定	15
1. クイック設定	16
2. VPNサーバ接続設定	22
① 新規接続	22
② サーバ／ブリッジ選択	23
③ 接続詳細	24
④ Hub設定／DDNS確認	25
⑤ L2TP／IPsec設定	26
⑥ VPN Azure設定	27
⑦ ユーザ作成	28
⑧ ローカルブリッジ設定	30
④ VPNクライアント設定	31
⑤ Spyserver設定	34
⑥ ルータ設定	36

抜粋版になります。ページと内容が一致しません。

目次

ページ

2. 運用編	<u>37</u>
① Spy server運用	<u>38</u>
② VPNクライアントからの運用	<u>39</u>
③ Spy server network利用	<u>41</u>
④ ログ管理	<u>42</u>
⑤ セッション管理	<u>44</u>
3. 困ったとき	
① 故障かな	<u>46</u>
② FAQ	<u>47</u>
③ 免責事項	<u>49</u>
④ 問い合わせ先	<u>50</u>

抜粋版になります。ページと内容が一致しません。

参考

ルータ設定(スマホ用)

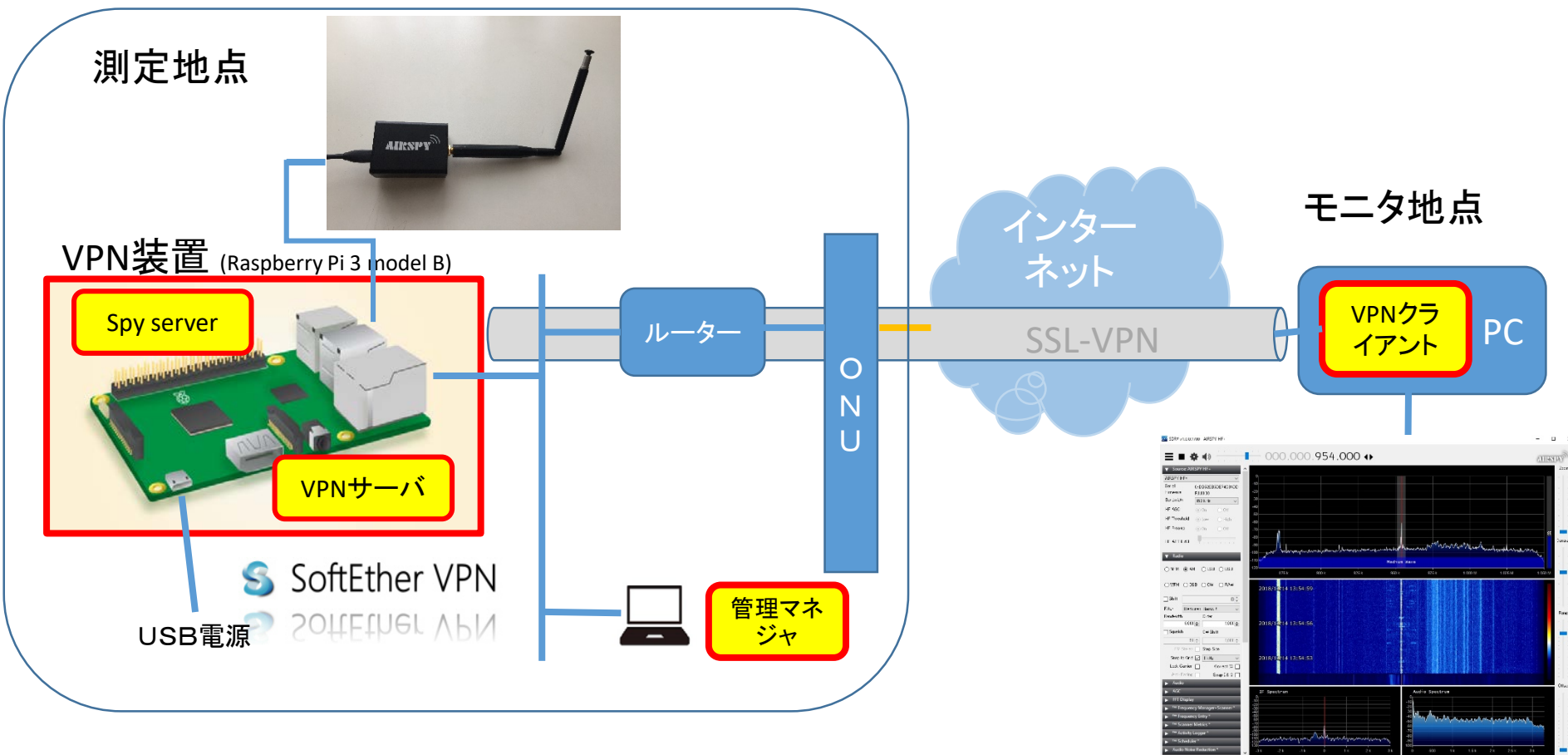
スマホ設定(ios, android)

1. Ios設定
2. Ios接続
3. Android設定
4. Android接続

1. 設定編

1-① 全体構成

- VPN装置とクライアントなどの全体構成を示します。



1- ② ソフト・インストール

• 管理マネージャ

- ダウンロードしたexeファイルをダブルクリックして、インストールします。

a. ようこそ

b. 管理マネージャを選択

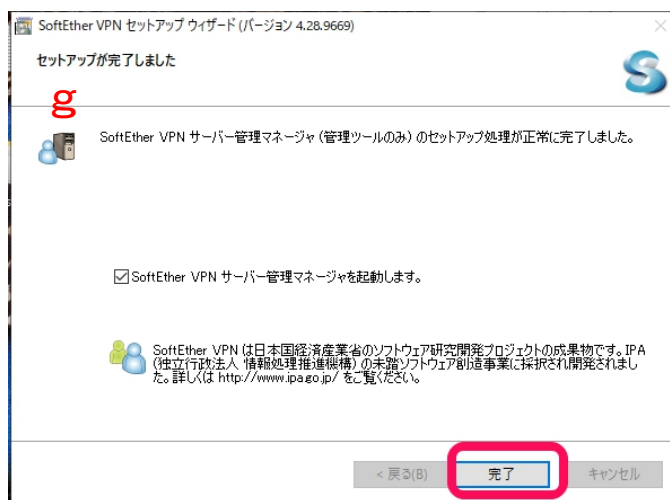
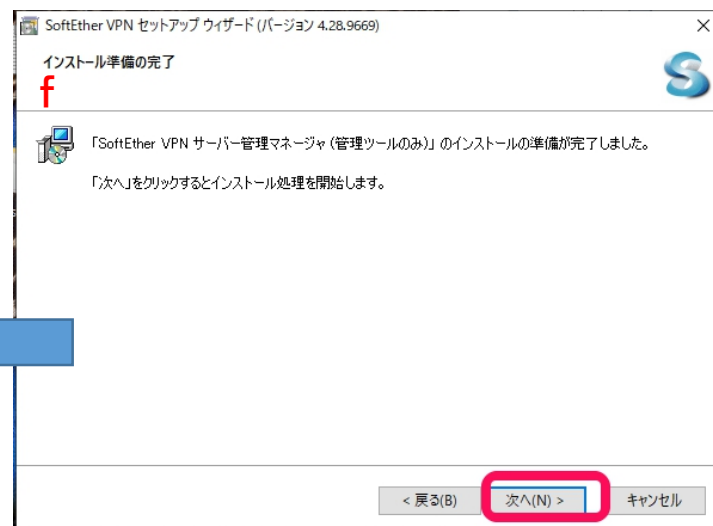


1- ② ソフト・インストール

• 管理マネージャ

- ダウンロードしたexeファイルをダブルクリックして、インストールします。

- ようこそ
- 管理マネージャを選択
- 使用許諾
- 重要事項説明
- インストール先
- インストール準備
- 完了



1- ③ 管理マネージャ設定

管理マネージャで設定する手順と内容

1. クイック設定

事前に設定している内容で、簡単に利用できます

2. VPNサーバ接続設定

VPNサーバを搭載したRaspberry Piとの接続設定

① 新規接続

管理マネージャとVPNサーバの新規接続を選択

② サーバ／ブリッジ選択

リモートアクセス、拠点間接続などの方式を選択します

③ 接続詳細

管理マネージャとVPNサーバの新規接続の詳細を設定します。

④ Hub設定／DDNS確認

仮想Hub名、DDNSホスト名の確認を行います。DNSキーは一度設定されると使いまわしができません。コンピュータが壊れた場合にそなえて保存しておいてください。

⑤ L2TP／IPsec設定（スマホ用）

スマホを接続する時のプロトコルのための設定です。

⑥ VPN Azure設定

DDNS機能、クラウドのIPアドレスをAzureが提供してくれます。無料です。有効ボタンを押すのみ。

⑦ ユーザ作成

仮想Hub配下で使用するユーザ名、パスワードを設定します。

⑧ ローカルブリッジ設定

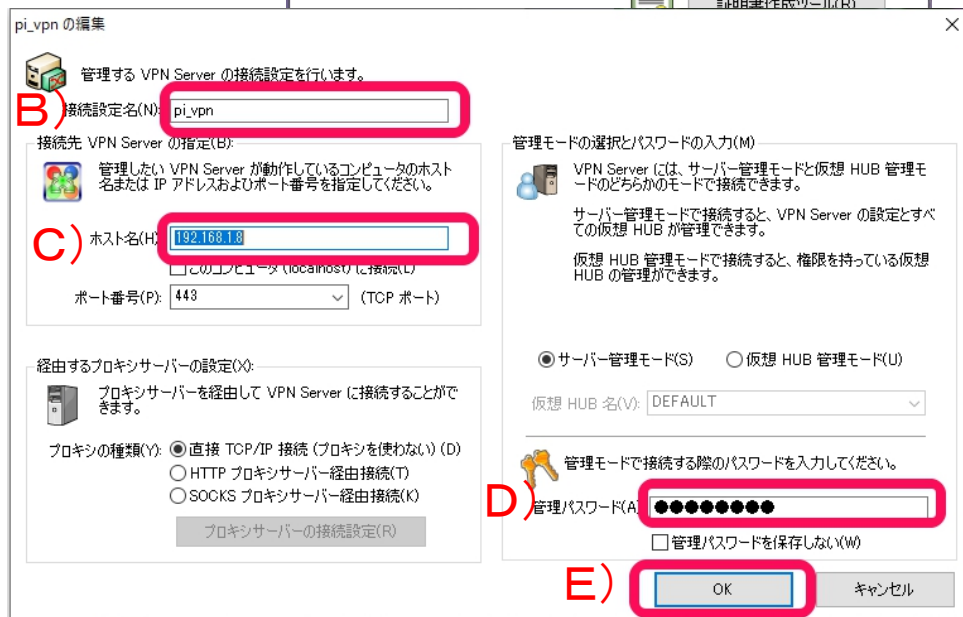
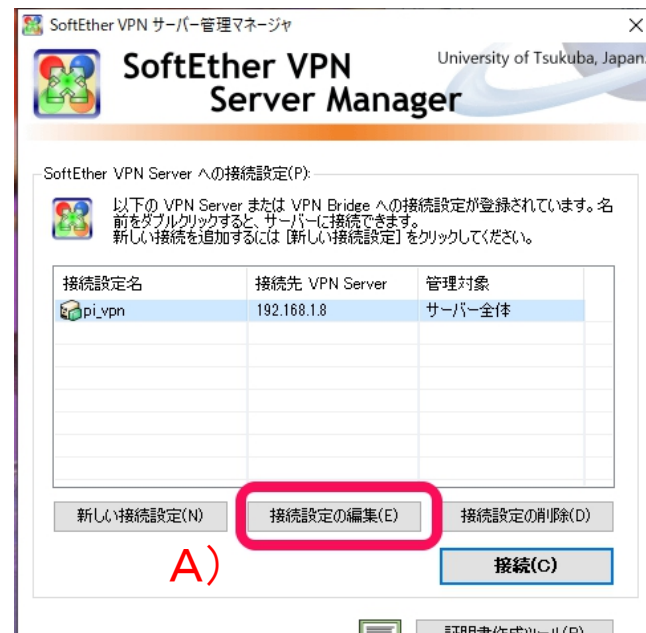
VPNサーバの仮想hubと実際のLANインターフェース(eth0; raspberry Piのetherインターフェース)をブリッジ接続します。Wlan0との接続も可能です。

1- ③ 管理マネージャ設定

1. クイック設定: 接続設定

- A) 接続設定の編集
- B) 接続設定名を入力: **pi_vpn**(変更可能)
- C) IPアドレスの変更 (Raspberry Piで調べたIPアドレスに変更)
- D) 管理パスワード: **pi**(変更可能)
- E) OK

ラズベリパイ設定編の
8ページ参照
HDMIケーブルとキー
ボードをつないで
\$ ifconfig



1- ③ 管理マネージャ設定

2. VPNサーバ接続設定

① 新規接続

- A) 管理マネージャのアイコンをダブルクリックして立ち上げ
- B) 新しい接続設定:vpnサーバに接続するために



1- ③ 管理マネージャ設定

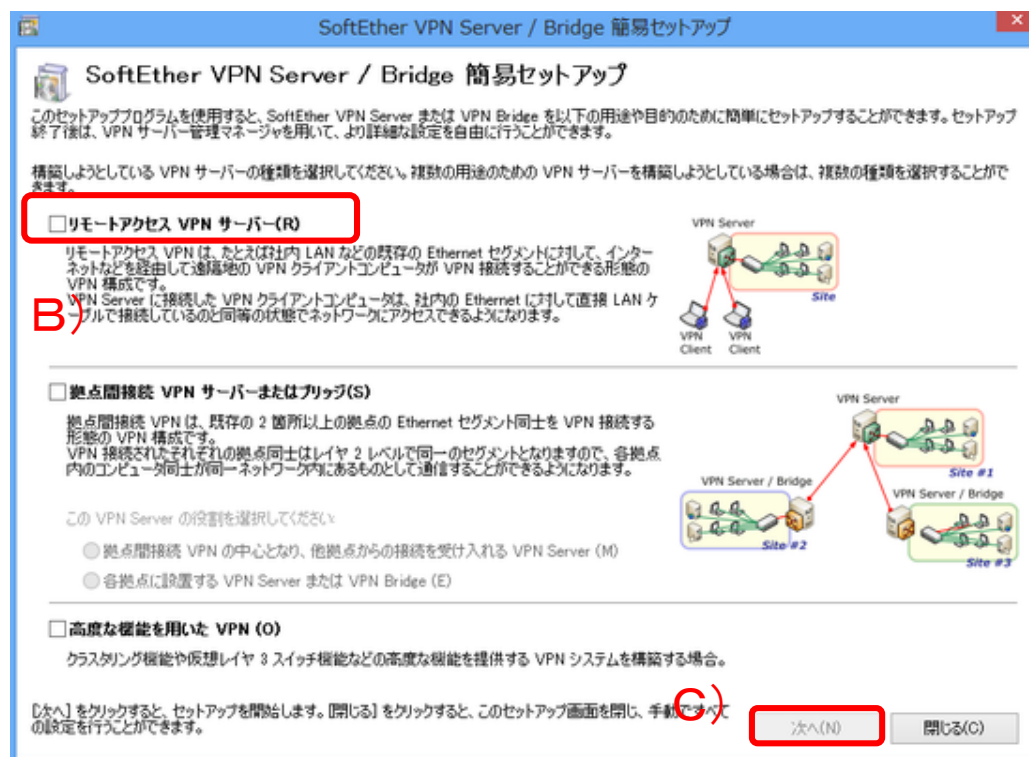
2. VPNサーバ接続設定

② サーバ／ブリッジ選択

A) VPN Server／Bridge簡易セットアップ

B) リモートアクセスVPN選択

C) 次へ



1- ③ 管理マネージャ設定

2. VPNサーバ接続設定

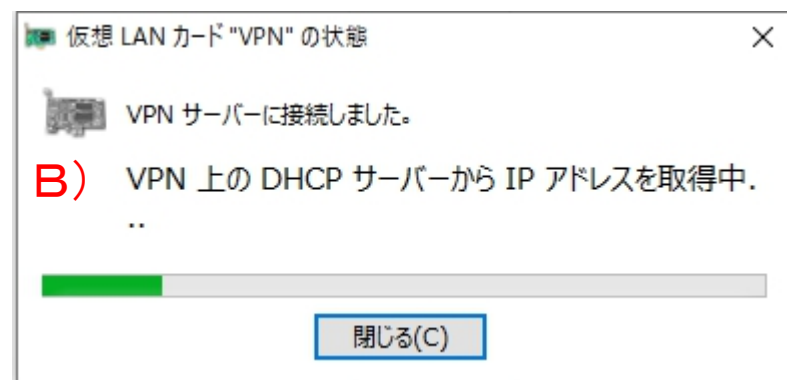
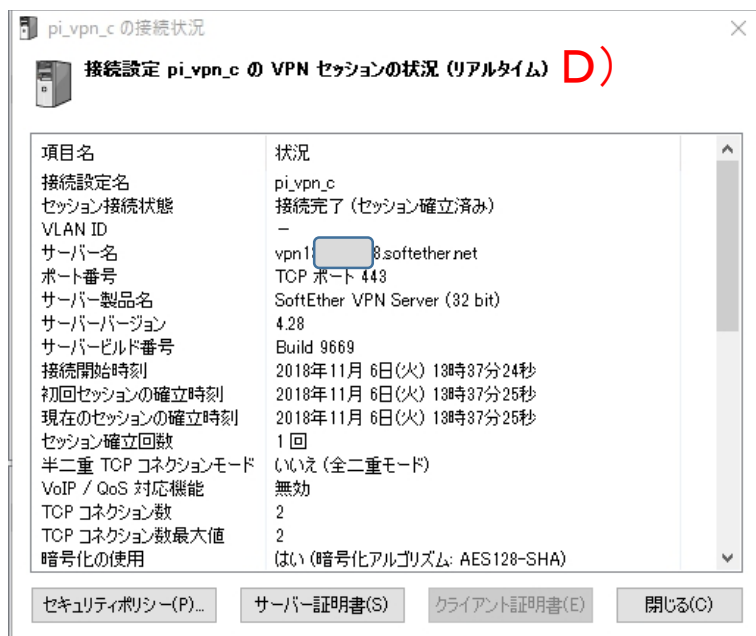
③ 接続詳細

- A) 新しい接続設定:vpnサーバに接続するために
- B) 接続設定名:入力
- C) ホスト名:IPアドレス
- D) OK
- E) 管理パスワード入力
- F) OK

1-④ VPNクライアント設定

4. 接続

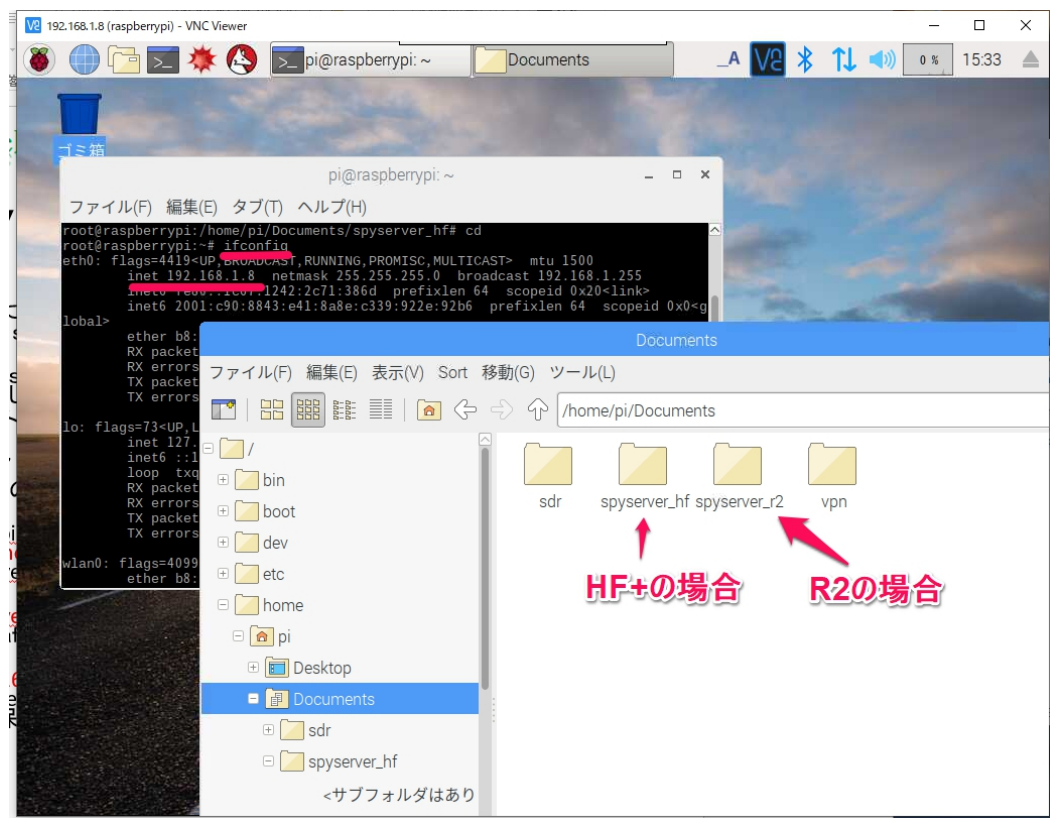
- A) 接続先をダブルクリック
- B) IPアドレス取得中
- C) 接続先の状態: 接続完了、再度ダブルクリック
- D) セッションの状態表示



1- ⑤ Spy server設定

• Spy server

- ① Raspberry Piのipアドレスを確認します。
- ② コマンドプロンプトを開き、`root`で入ります。
- ③ `pi@raspberrypi:~ $ su -`
- ④ パスワード:rootのパスワードを入力します
- ⑤ `root@raspberrypi:~ # ifconfig`
Inetの下にipアドレスが表示されます
- ⑥ Spy serverのフォルダは、`/home/pi/Documents`配下に二つあります。Airspyの種類によって使い分けてください。



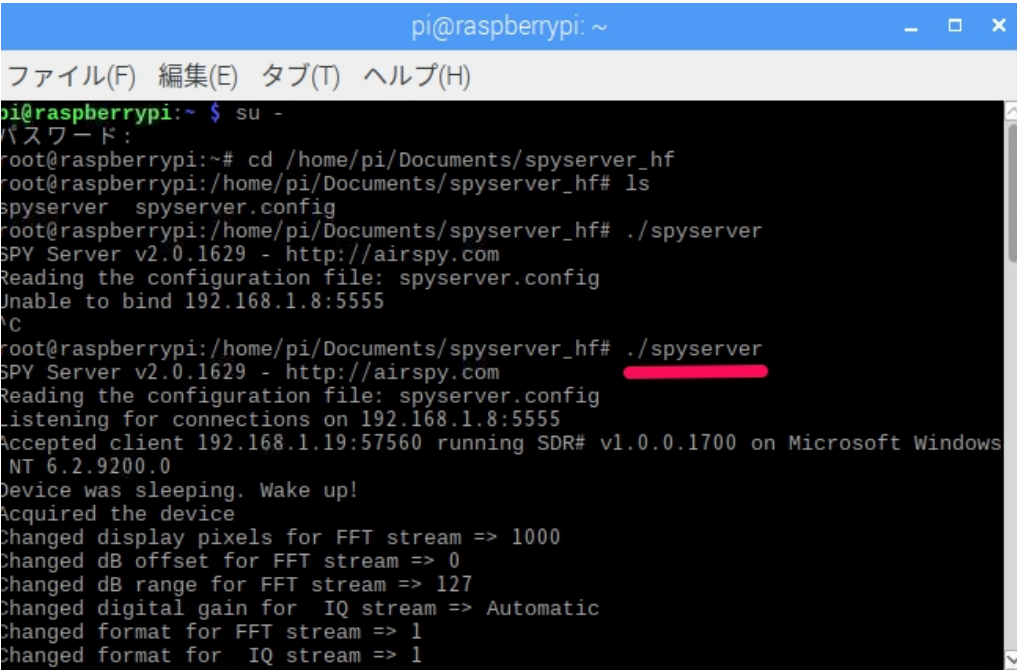
2. 運用編

2- ① Spy server運用

- Spy server

Raspberry Piのターミナル画面から

- ① `root@raspberrypi:~ # cd /home/pi/Documents/spyserver_hf` フォルダに移動
- ② `# ./spyserver`
- ③ リスニング状態になります。
- ④ VPNクライアント側が接続されるとAcquired deviceと表示されます。



```
pi@raspberrypi: ~  
ファイル(F) 編集(E) タブ(T) ヘルプ(H)  
pi@raspberrypi:~$ su -  
パスワード:  
root@raspberrypi:~# cd /home/pi/Documents/spyserver_hf  
root@raspberrypi:/home/pi/Documents/spyserver_hf# ls  
spyserver  spyserver.config  
root@raspberrypi:/home/pi/Documents/spyserver_hf# ./spyserver  
SPY Server v2.0.1629 - http://airspy.com  
Reading the configuration file: spyserver.config  
Unable to bind 192.168.1.8:5555  
^C  
root@raspberrypi:/home/pi/Documents/spyserver_hf# ./spyserver  
SPY Server v2.0.1629 - http://airspy.com  
Reading the configuration file: spyserver.config  
Listening for connections on 192.168.1.8:5555  
Accepted client 192.168.1.19:57560 running SDR# v1.0.0.1700 on Microsoft Windows  
NT 6.2.9200.0  
Device was sleeping. Wake up!  
Acquired the device  
Changed display pixels for FFT stream => 1000  
Changed dB offset for FFT stream => 0  
Changed dB range for FFT stream => 127  
Changed digital gain for IQ stream => Automatic  
Changed format for FFT stream => 1  
Changed format for IQ stream => 1
```


2- ② VPNクライアントから運用

• VPNクライアント

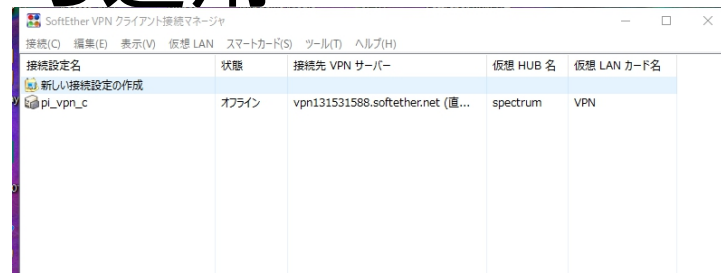
- ① 設定したVPNクライアントから接続。

• SDRソフト起動

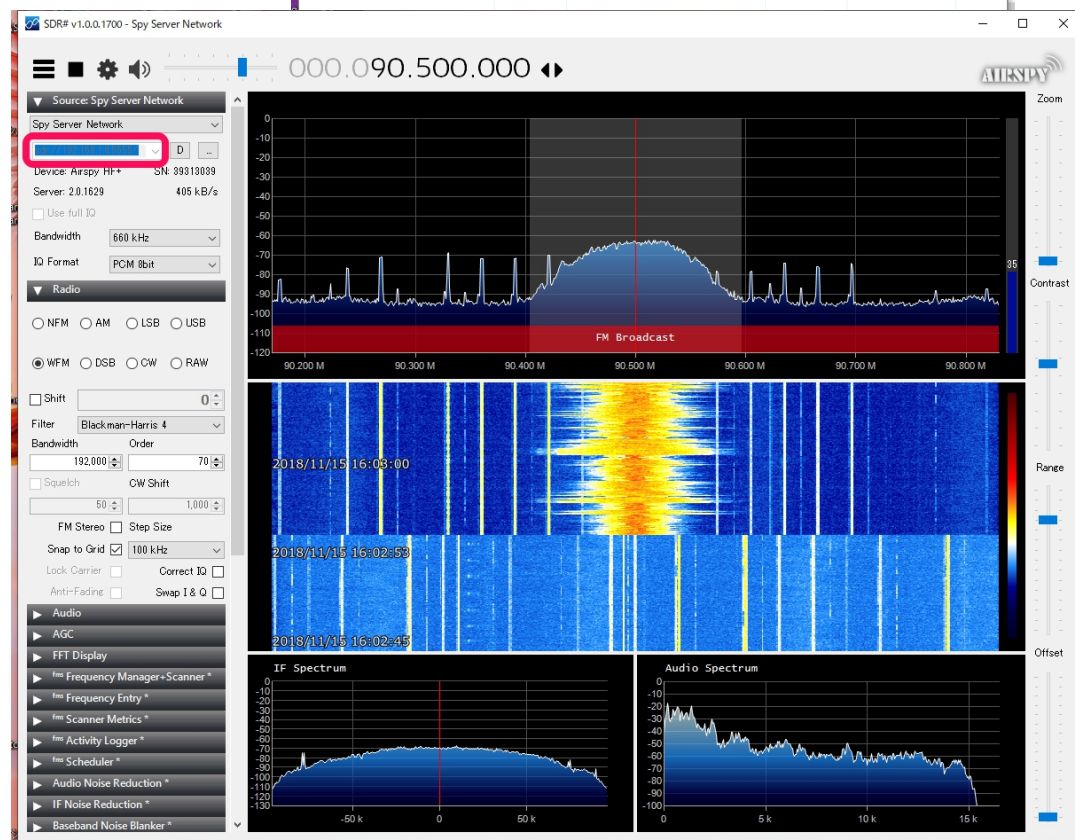
VPNクライアントのWindows PCにインストールしているSDR#から

- ① Source: **Spy server network** 選択
- ② **sdr://192.168.1.x:5555**と入力
- ③ 後の操作は通常どおり

5555ポートを使用する場合は、管理サーバで設定変更: 次ページ参照



接続設定名	状態	接続先 VPN サーバー	仮想 HUB 名	仮想 LAN カード名
新しい接続設定の作成				
pl_vpn_c	オンライン	vpn131531588.softether.net (直...	spectrum	VPN

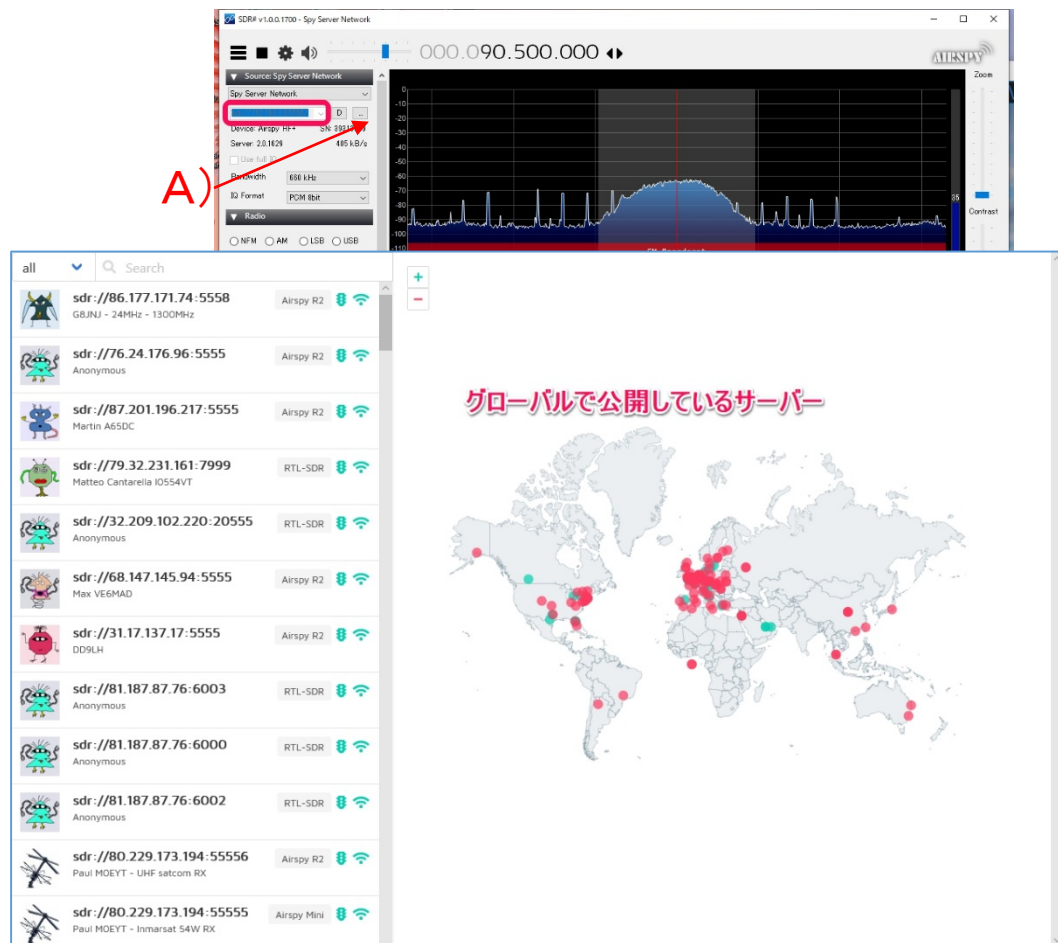


2- ③ Spy server network利用

- Webで公開されているサーバが確認できます。

<https://airspy.com/directory/>

- SDR#のこちらをクリック
- URLをクリックするとモニターできます。
- 公開する場合は、セキュリティがかかっていない、自宅などのIPアドレスはDDNSを利用していないと変更されるため、あまりお勧めしません。
- お友だちのグループ間で弊社の遠隔モニタ(VPNサーバ)を使って共有しましょう。



3. 困ったとき

①. 故障かな

項番	機器、ソフト別	症状	対処方法
1	VPNサーバ(Raspberry Pi)	管理マネージャからつながらない	VPNサーバのIPアドレスが変更になっていませんか？ RaspberryPiにアクセスして# ifconfigで確認ください
2			Raspberry Piの電源、LANケーブル、回線はつながってますか？
3			Raspberry Piの赤ランプは点灯していますか？
4		VPNサーバのハードを交換したい	DDNSとDNSキーを前回使用していたものをコピーして移行してください。
5	管理マネージャ	VPNサーバにつながらない	VPNサーバのIPアドレスが変更になっていませんか？ RaspberryPiにアクセスして# ifconfigで確認ください
6	VPNクライアント (Windows PC)	接続できなくなった	VPNサーバの電源、LANケーブル、回線はつながってますか？
7			Windows PCはインターネットにつながっていますか？ (WiFi, LAN)
8	スマホ(ios, Android)	接続できなくなった	VPNサーバのIPアドレスが変更になっていませんか？ 変更になった場合は、ルータのポート変換、VPNパスルールのIPアドレスも合わせて変更してください。
9	ユーザ	特定のユーザだけつながらない	管理マネージャでユーザ名、パスワードの設定を確認してください。

3. 困ったとき

②.FAQ(ルータ、VPNサーバ編)

項番	機器、ソフト別	Q. 問い合わせ	A. 回答
1	ルータ	VPNパススルーについて教えてください	VPNをルータ配下で使用する時に、L2TP, IPsecなどの特定のポートを通過させる機能になります。今回のVPN装置はIPsecパススルーが必須となります。
2		使用中のルータには、IPsecパススルーの機能がありません。どのような影響がありますか	IPsecパススルーは、スマホの時に使用します。Windows PCは、VPNを使用できます。
3		ポート変換機能について教えてください。	NAPT(network address port translation)とも呼ばれて、IPアドレスの他にポートも変換します。ルータに入ってきた特定のポートを特定のIPアドレスとポートに変換します。本機能もスマホの時に使用します。 今回のVPN装置では必須です。使用ポートは、50,500,4500,1701になります。
4	スループット(回線効率)	VPNを使用した場合どれくらいパフォーマンスが落ちますか。	弊社の測定では、約15%伝送速度が低下しました。但し、10Mbps以上の回線では、体感上問題ありません。
5	VPNサーバのCPU使用率	VPNを使用した場合、CPU使用率はどれ位になりますか？	1ユーザがVPNを使用すると約10%のCPU使用率がUPします。家庭で使用する場合は特に問題ありません。
6	VPNサーバのセッション数	VPNサーバの最大セッション数は？	ソフトでは、4096です。実際の利用では、10セッション位が現実的です。

3. 困ったとき

②.FAQ(クライアント、スマホ編)

項番	機器、ソフト別	Q. 問い合わせ	A. 回答
1	スマホ	VPN接続時間はどれくらいですか？	一番最初のVPNの接続時間は、数秒で完了し、VPN又は鍵マークが表示されます
2		4G又はWiFiのどちらでもVPNは使用できますか？	利用できますが、4Gはセキュリティが高いためVPNは不要です。WiFi利用時に使用してください。またキャリアが提供しているWiFiもセキュリティが高いためVPNは不要です。
3		VPNを使った方がよい場所はどこ？	公衆無線LAN(空港、観光地で特にセキュリティのないもの)、ホテル、ホットスポット(カフェ)など共有で使用するWPA2の無線LAN(同じパスワードを使用し、LAN上は共有されている場合が多い) また海外でSNSなどにアクセス制御されている国の場合。
4	Windows PC	Windowsネットワークにも入れますか？	Windowsの端末などが共有設定になっていればネットワークのPCにも入れます。
5		Windows PCの場合、どの国でも利用できますか？	スマホの場合は、VPNを使用しても制限される場合がありますが、Windows PCで使用している方式は、どの国でも規制されません。
6	VPNアプリとの違い	アプリでVPNを利用できるものがありますが、VPN装置との違いは？	・VPN装置は、占有で利用しますので混雑の影響を受けません。そのため接続時間も短い。 ・ログを取られる心配がありません。 ・月額費用がかかりません。特に、家族でVPN装置を利用する場合は非常にお得です。

3. 困ったとき

③. 免責事項について

1. 本製品及びサービスの提供が困難となった場合は、当社の責めによらない場合は、当社は、損害賠償を負いません。
2. 本製品及びサービスは、メンテナンスのため、サービスの全部又は一部の利用を中止する措置をとることがあります。
3. 本製品及びサービスは、サービスを保証するものではありません。遅延、中断などが発生する場合があります。
4. 本製品は、輸出する時に許可がいる場合がありますので、日本国内での利用をお願いします。
5. 本製品の購入に当たっては、お客様が所有するルータの機能により、動作できない場合がありますので、注意事項等をよく読んで購入してください。購入後に、動作しないなどの苦情には、対応致しかねます。
6. 当社各マニュアルに反する利用に関して、当社は責任を負いません。