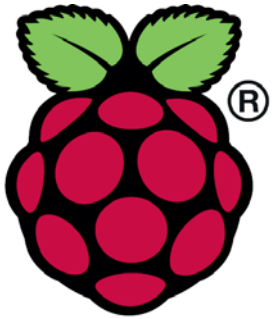
Spectrum Technology

Ver1.0 2017/1/3

WiFi Pen Test
手順書（aircrack-ng）

Raspberry Piを使ったIoT時代の必需品

スペクトラム・テクノロジー株式会社



Raspberry Pi

目次

抜粋情報

抜粋情報

Raspberry PiはRaspberry Pi foundationの登録商標です。

WiFi Pen Test手順書

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 Pen Test（侵入試験）
   - Ibeacon（BLE)のビーコン送信、受信
   - Pythonを使ったプログラム作成。今回wiresharkのデータ取得時に簡単なプログラムを紹介します。
   - 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：キーボードのCTLとjを同時に押します（コントロール：左下とj）

WiFi Pen Test手順書

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

root@raspberrypi:~# cd /home/pi/Documents　ディレクトリの切り替え
root@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ペして操作します
root@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
root@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
root@raspberrypi:~# rm ファイル名　ファイルの削除
便利な機能　rm –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る。すべてのコマンド共通(マイナスを2個とhelp)

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
root@raspberrypi:~# ps a　現状の動いているプロセスを表示
root@raspberrypi:~# kill　特定のプロセスを強制終了
root@raspberrypi:~# apt-get install pkg　パッケージのインストールなどに使用
root@raspberrypi:~# date　日付、時間の設定を行います。
root@raspberrypi:~# leafpad /etc/network/interfaces　インタフェースに記述してい内容を変更します。Viよりも使いやすいです。

④ モジュール、usb、メモリ、HDDなどの表示

root@raspberrypi:~# lsmod　linuxのモジュールリスト表示
root@raspberrypi:~# lsusb　usbのデバイス表示
root@raspberrypi:~# free –mt　メモリ使用状態表示
root@raspberrypi:~# df　HDD（マイクロSD）の使用状態表示

WiFi Pen Test手順書

3. プロトコル・アナライザ関係コマンド

① ネットワーク関係（wifi,LAN)

root@raspberrypi:~# ifconfig　　ネットワークインターフェースの状態表示

root@raspberrypi:~# ip l set wlan1 up　　wlan1のインタフェースのup(LANの場合はeth0)

root@raspberrypi:~# ip l set wlan1 down　　wlan1のインタフェースのdown

root@raspberrypi:~# iwconfig wlan1 mode monitor　　wlan1のインタフェースをmonitoモードに切り替えます。

root@raspberrypi:~# iwconfig wlan1 channel 11　　wlan1のチャンネルを11(2462MHz)に切り替えます。

root@raspberrypi:~# wireshark　　wiresharkを起動します。

root@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。

root@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。

② BLE関係

root@raspberrypi:~# hciconfig　　BLEのインタフェース状態を表示

root@raspberrypi:~# hciconfig hci0 up　　hci0のインタフェースをup

root@raspberrypi:~# hcitool lescan　　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と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。

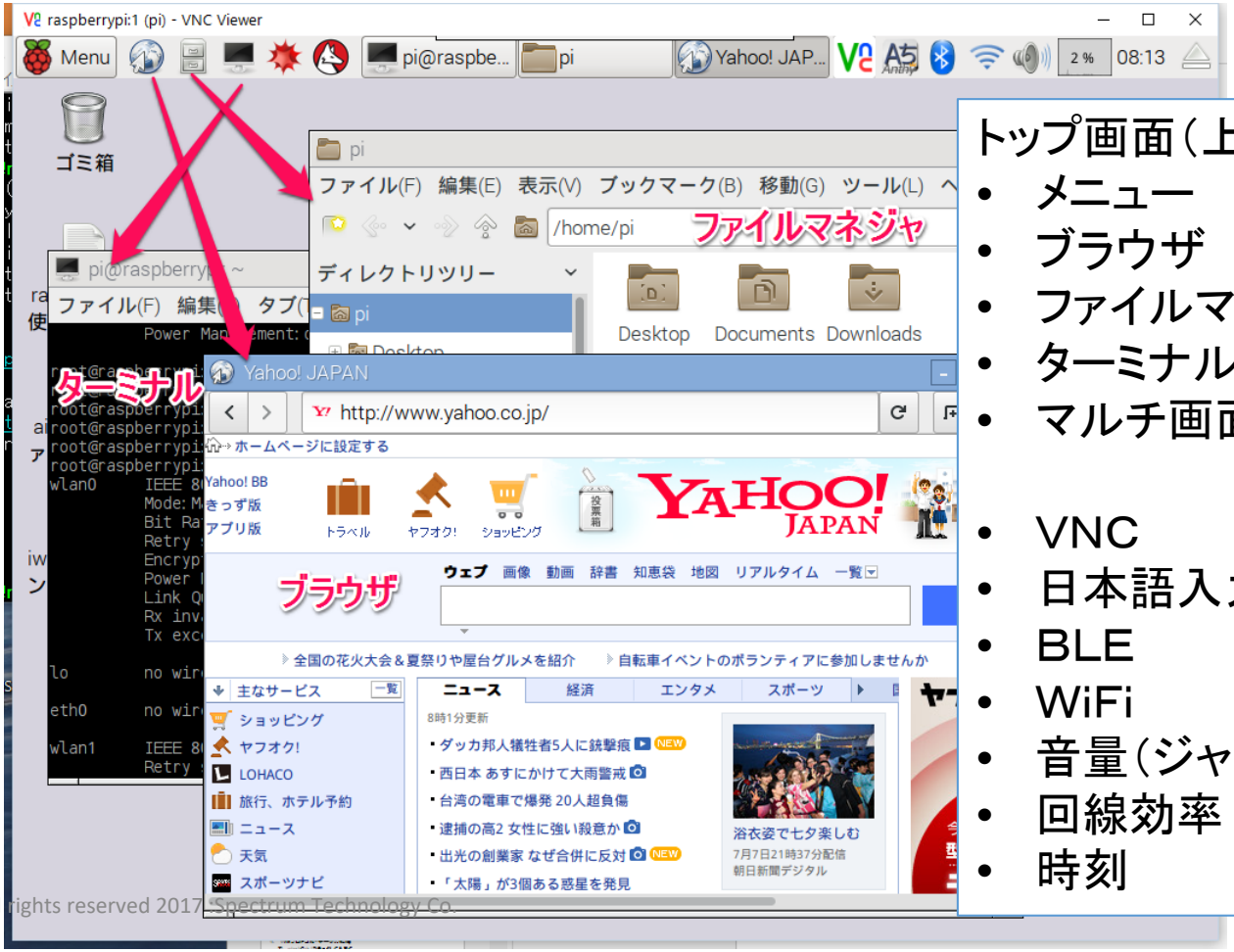
root@raspberrypi:~# hcidump –a　　BLEの接続状態をダンプします。

Ver1.0 2017/1/3

WiFi Pen Test手順書

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）

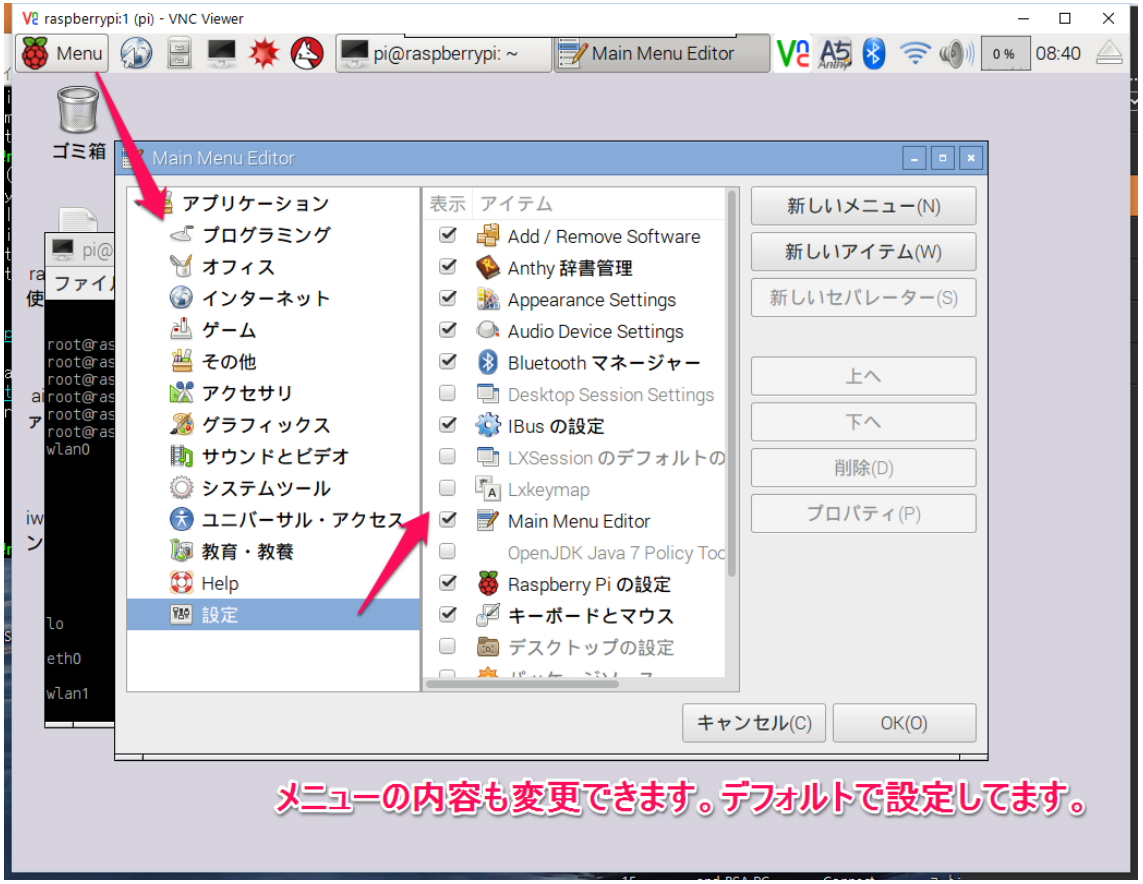
- メニュー
- ブラウザ
- ファイルマネジャ
- ターミナル
- マルチ画面選択

- 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

WiFi Pen Test手順書

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

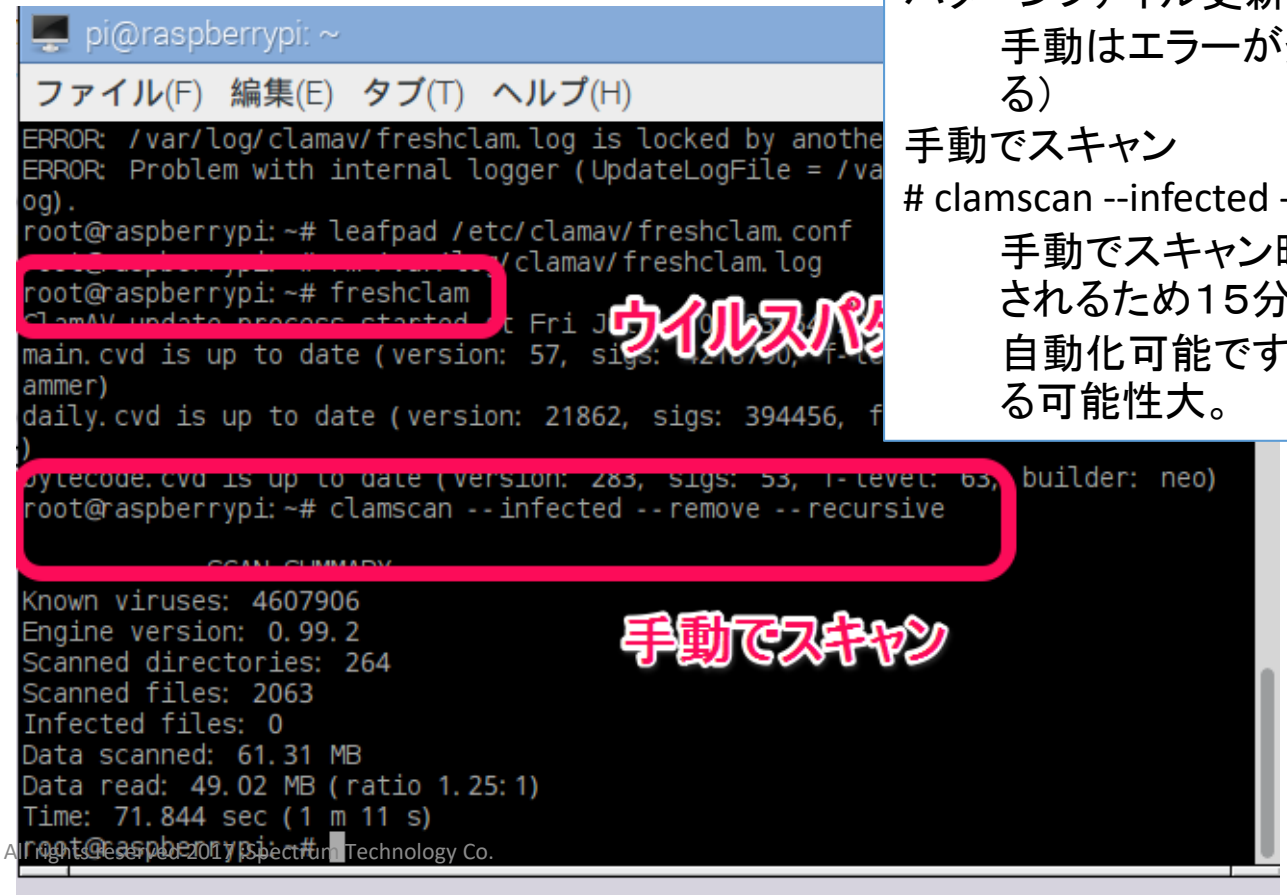
カスタマイズ可能です。

WiFi Pen Test手順書

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ます。



パターンファイル更新

手動はエラーが発生します。（バグと思われる）

手動でスキャン

clamscan --infected --remove --recursive

手動でスキャン時にパターンファイルが更新されるため15分要します。

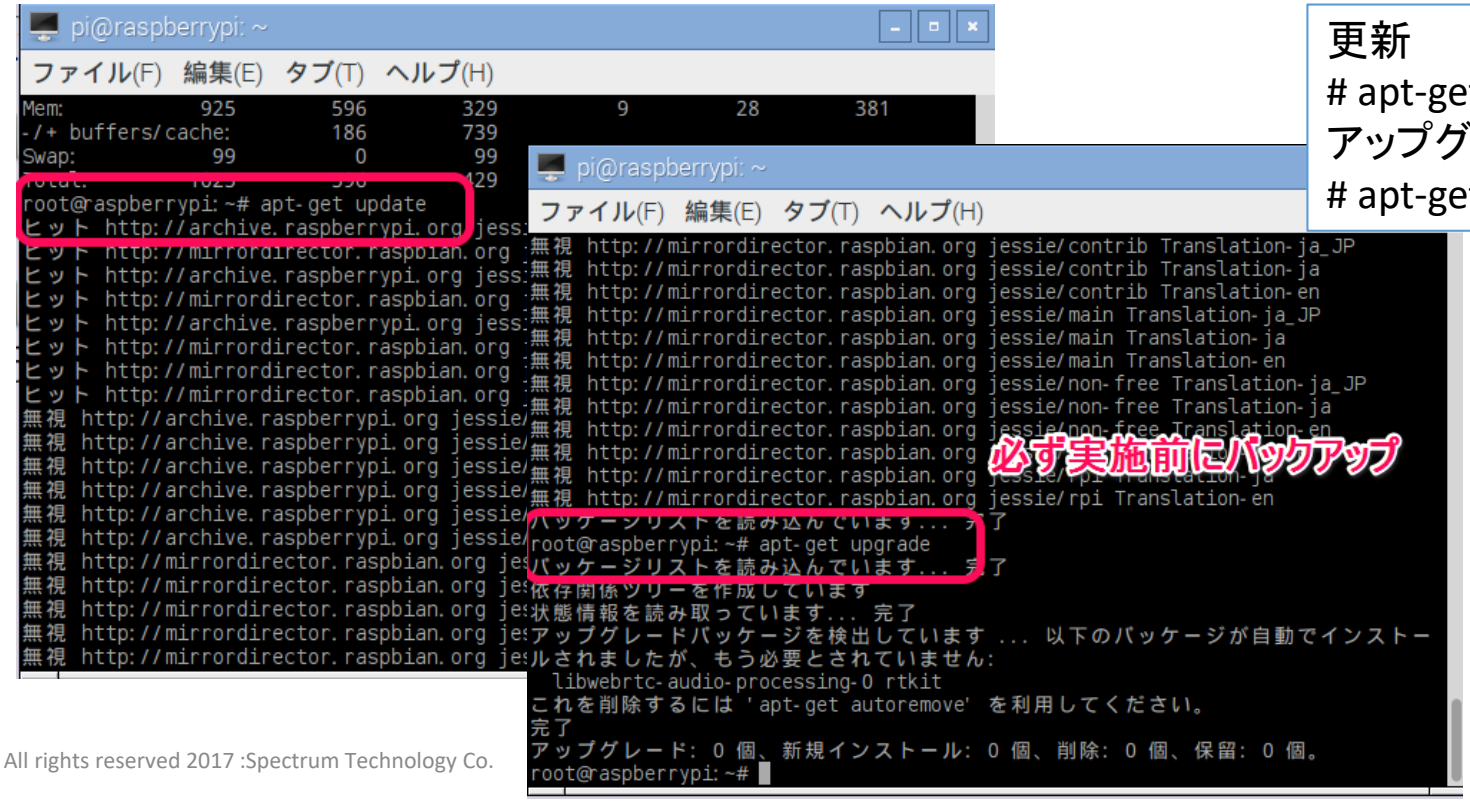
自動化可能ですが、バックグランドで重くなる可能性大。

WiFi Pen Test手順書

5. 日常運用

② インストール済パッケージの更新、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に実施してください。
- 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。



更新
apt-get update
アップグレード手動
apt-get upgrade

WiFi Pen Test手順書

6. Aircrack－ngの体系：http://www.aircrack-ng.org/doku.php?id=Main
数多くの機能が準備されてますが、一部のよく使われる機能を解説します。
6.1 airbase-ng：ハニーポット用基地局
6.2 aircrack-ng：wep パスワード解析
- airdecap-ng
- airdecloak-ng
- airdrop-ng

6.3 aireplay-ng：アソシエーション、ARPリクエストなどIVを送信して、wep解析を加速する
- airgraph-ng

6.4 airmon-ng：プロトコルモニター
6.5 airodump-ng：プロトコル取得、複数チャンネル実施するとデータが欠落します
- airolib-ng
- airserv-ng
- airtun-ng
- besside-ng
- easside-ng
- packetforge-ng
- tkiptun-ng
- wesside-ng

WiFi Pen Test手順書

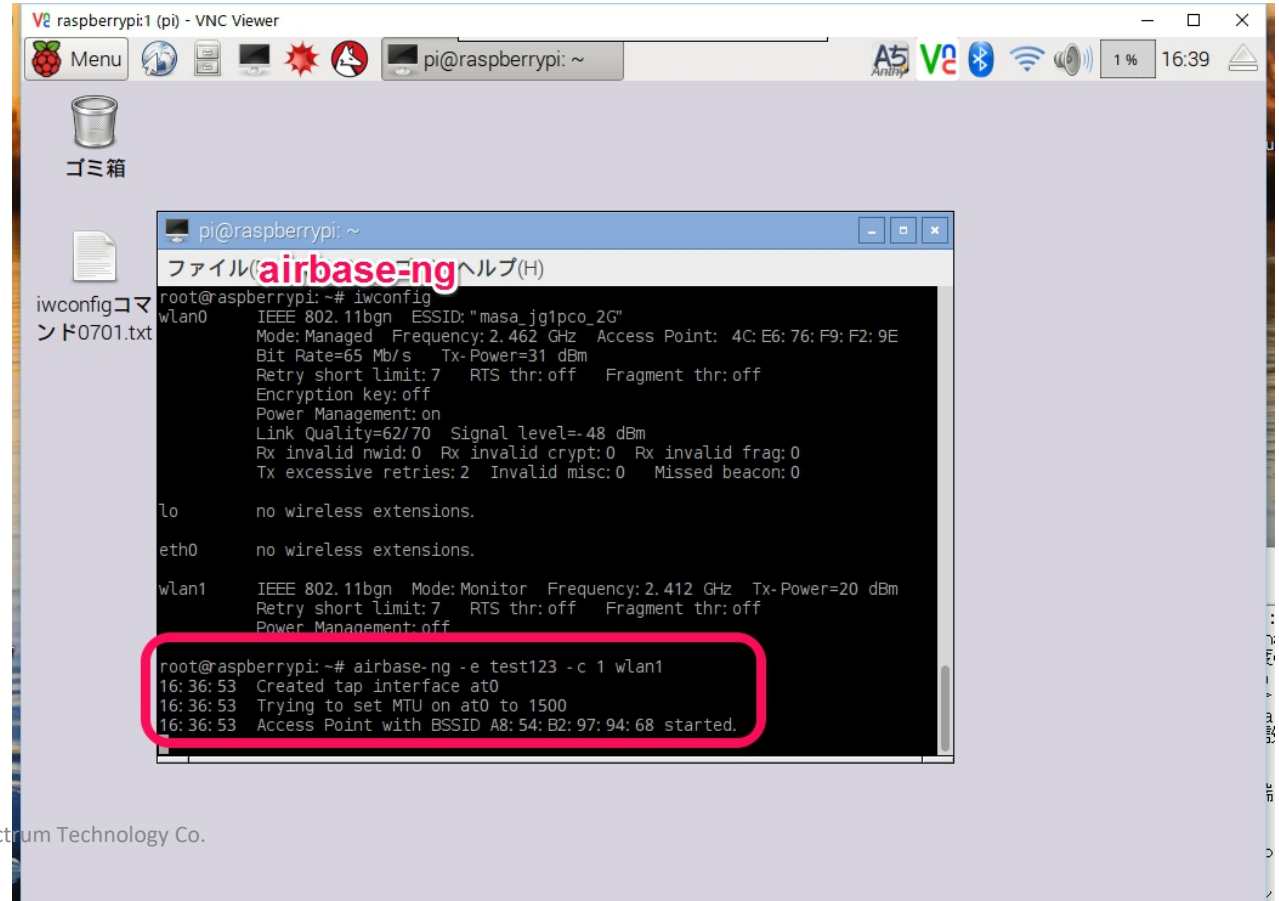
6．1 Airbase－ng

- WiFiのアクセスポイントを設定します。

airbase-ng -e ssid -c 1 wlan0

SSID名 チャンネル番号 インターフェース番号

- 送信停止は、CTLとcを同時に押します



WiFi Pen Test手順書

7. WEP解読手順

① モニターモード設定：iwconfig 又は airmon-ng(インターフェースがwlan1として）

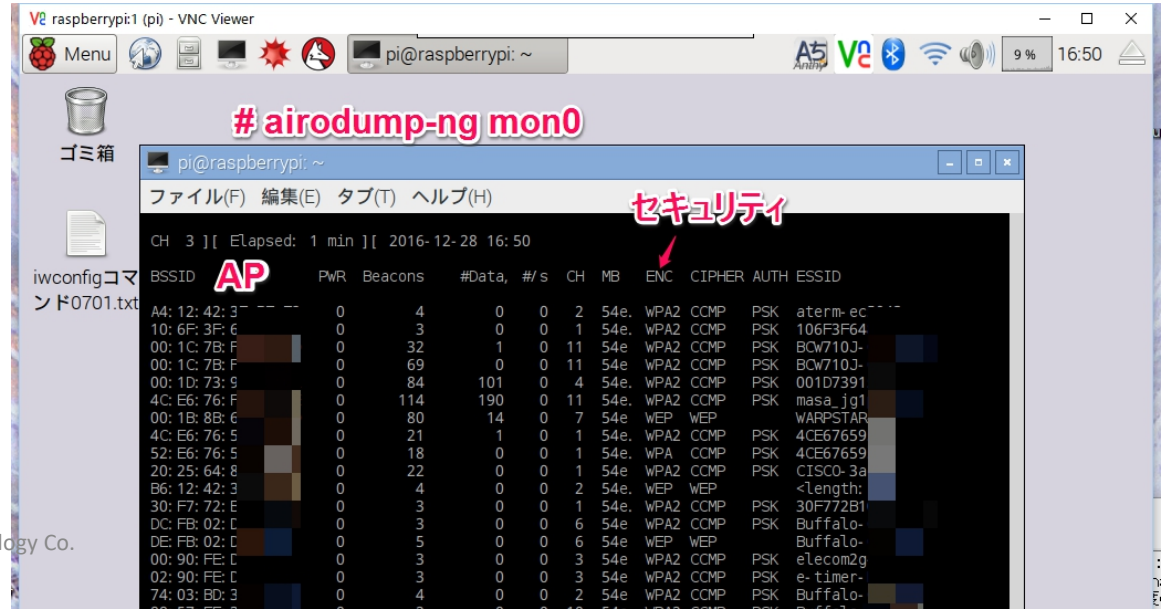
```
# ip l set wlan1 down
# iwconfig wlan1 mode monitor
# ip l set wlan1 up
```

個人的には、airmon-ngの場合新しいmon0とかのインターフェースが出来、既存のwlan1とかの下一桁番号が違うため間違い防止のために使ってません。

② アクセスポイントの状況把握：airodump-ng

- APのMACアドレス、使用しているチャンネル、セキュリティ方式、SSID名

```
# airodump-ng wlan1
```



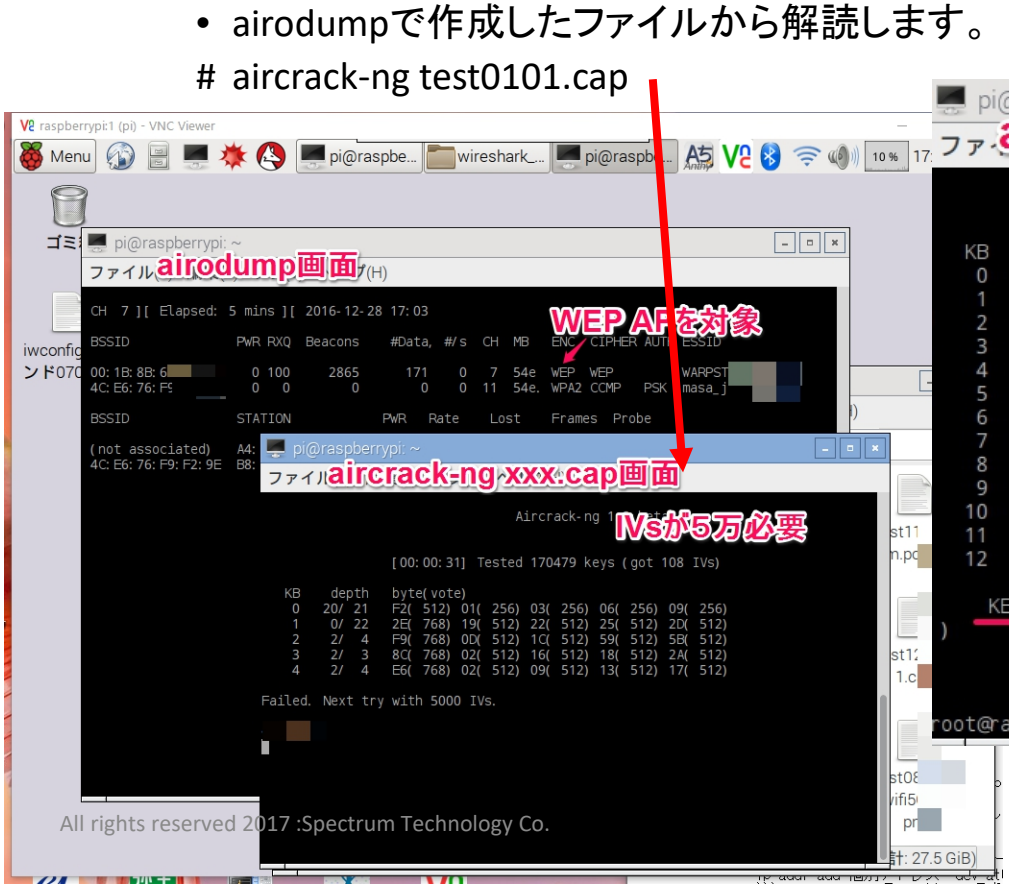
WiFi Pen Test手順書

7. WEP解読手順

⑦ WEP解読

- WEP解読を自動で実施します。約50000パケットで解読できます。ARPリクエストを行わなくてもデータが送受信されていれば解読可能ですが、長時間を要します。
- airodumpで作成したファイルから解読します。

aircrack-ng test0101.cap



解読が成功した例