



無線LANセキュリティの基礎

2015年4月19日
セクタンラボ



1.無線LANセキュリティの基礎

無線LANネットワークに対する脅威

- ネットワークセキュリティの視点で見ると、無線LANの利用には、大きく分けて3種類の脅威があります。

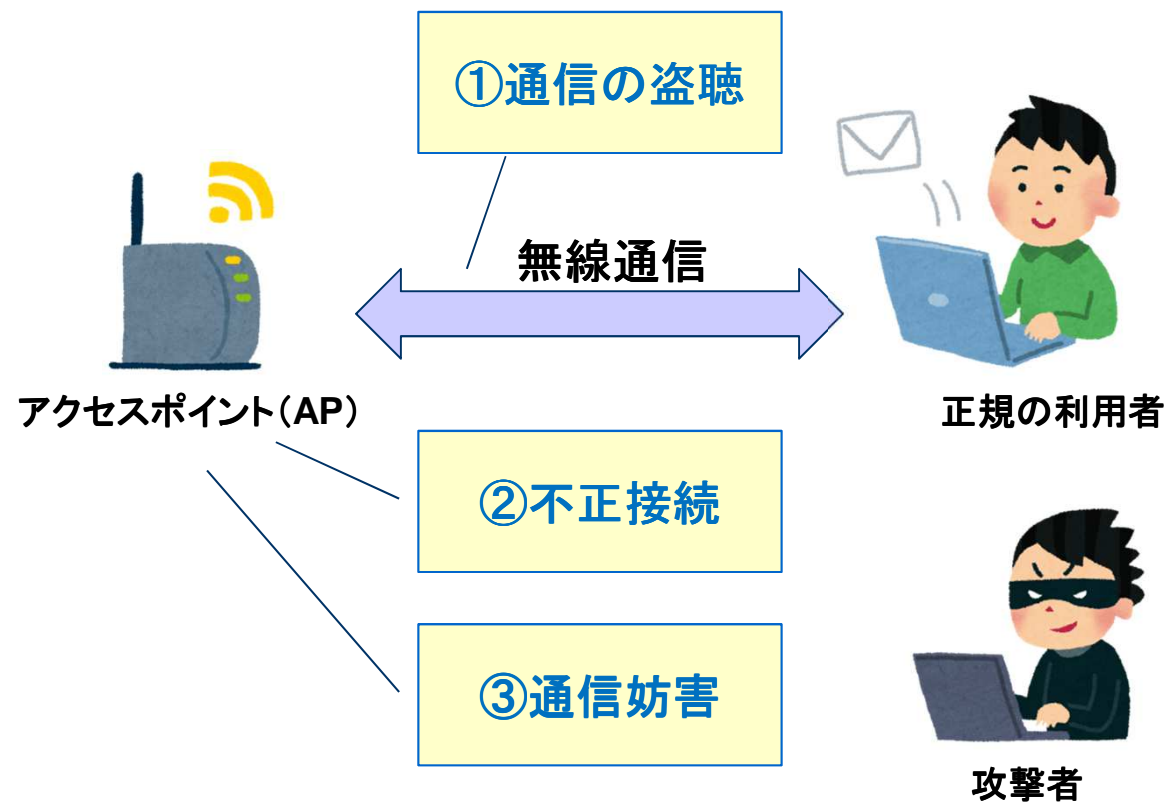
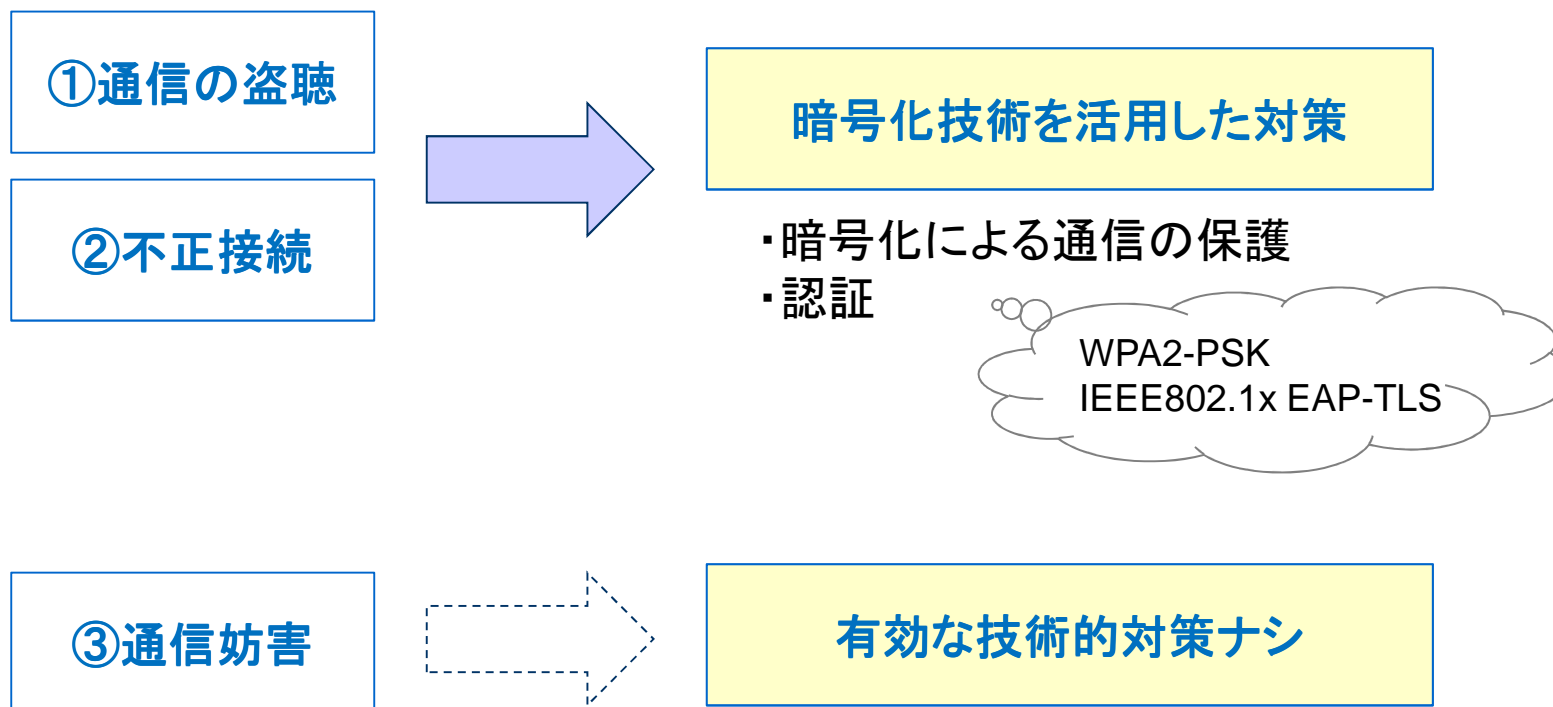


図. 無線LANネットワークに対する脅威

根本的な対策

- 通信の盗聴, 不正接続に対しては, 暗号化技術による対策を講じる必要があります。
 - 暗号化技術を使っていない対策は, 根本的な対策にはなりませんので注意してください。
- 通信妨害に対しては, 残念ながら有効な技術的対策はありません。(たぶん)



暗号化技術の適用範囲(1) 無線LANの接続手順

- 暗号化技術を使っても、クライアントが、APに接続する際、ESSID確認の通信は暗号化されません。

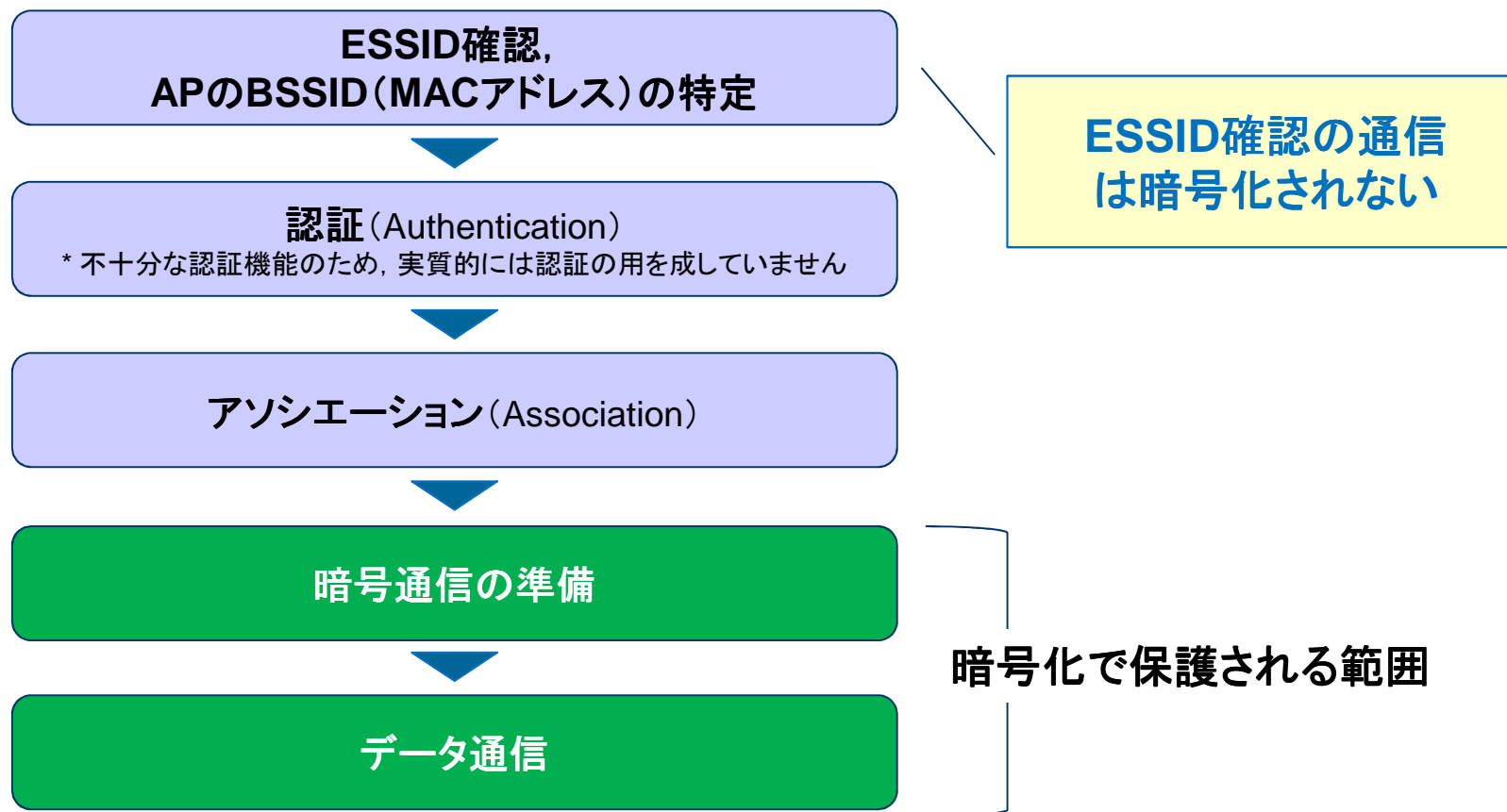


図. 無線LANの接続手順

暗号化技術の適用範囲(2) 無線LANフレーム

- 無線LANフレームは、ざっくり言うと、「IEEE802.11ヘッダー」と「データ」で構成されています。
- このうち、暗号化されるのは、「データ」部分のみです。
(どの暗号化方式を採用しても同じです)
- IEEE802.11ヘッダーに含まれるMACアドレス等は暗号化されません。

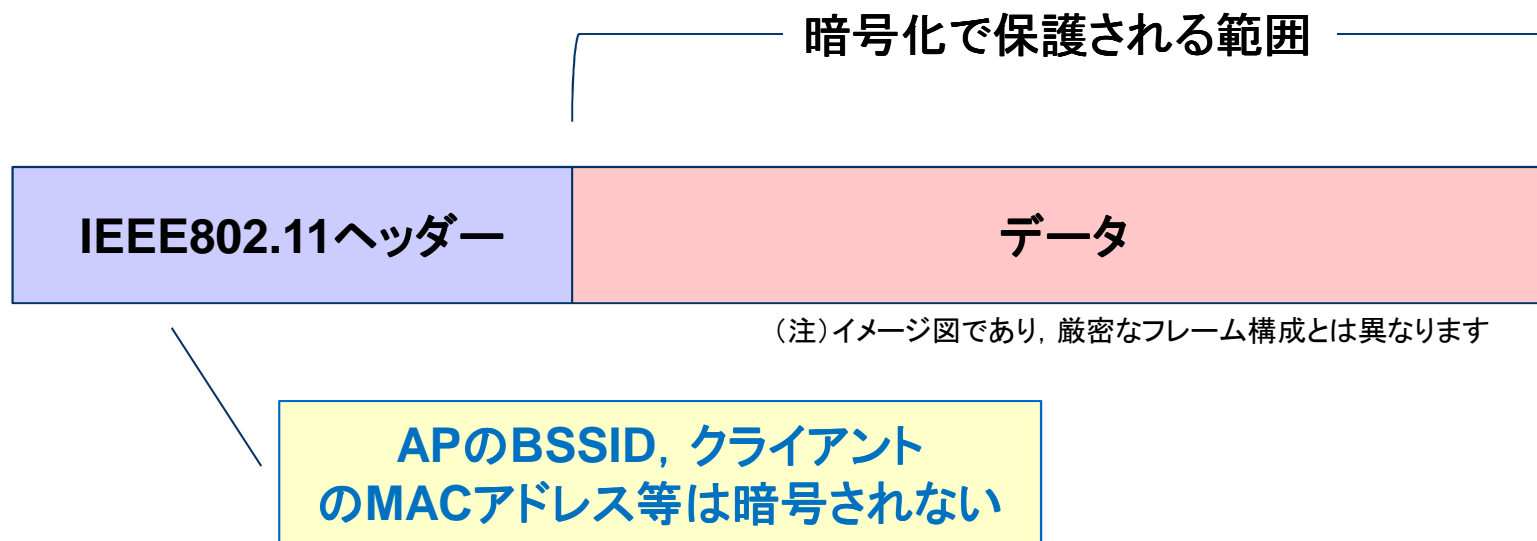


図. 無線LANフレームのイメージ

対策(?) ステルスSSID

- APをステルスSSIDに設定にすると、APはビーコンによるSSIDの発信を停止します。
- ステルスSSIDのAPに接続したいクライアントは、接続したいSSIDを埋め込んだ「Probe Request」発信します。
- APは、自身のSSIDと一致した場合、「Probe Response」で応答し、接続手順に進みます。

①SSIDが〇〇のAPいますかー？
いませんか！？(Probe Request)



クライアント

②ハイ！僕です！
(Probe Response)



アクセスポイント(AP)

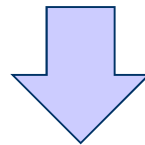
**SSID確認の通信は暗号化されないため、
ステルスSSIDにしても、SSIDはすぐバレる**
(それに、クライアントが社外でProbe Requestを発信するのは気持ち悪い?)

図. ステルスSSIDのイメージ

対策(?) MACアドレス制限

- 正規クライアントが通信する際、IEEE802.11ヘッダーにMACアドレスを平文で埋め込んだフレームを発信しています。

「正規クライアントのMACアドレス」はすぐバレる



「認証」として頼るべきではなく、補助的に使うべき
(APのパスワードを知っている正規利用者の私的な利用抑制など)

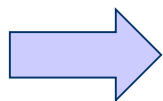


2.WPA2-PSK

いきなり結論

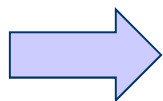
- WPA2-PSK(暗号アルゴリズム:AES)を利用すれば, とりあえず安全です。
- ただし, いくつか注意点があります。

正規クライアントの暗号通信の準備パケットをキャプチャすれば,
オフラインで総当たり攻撃が可能



とことん長いパスワードを設定しましょう
(IPAでは最低でも20文字を推奨)

同じAPに接続しているクライアント(=同じパスワードを利用)であれば,
通信の盗聴が可能



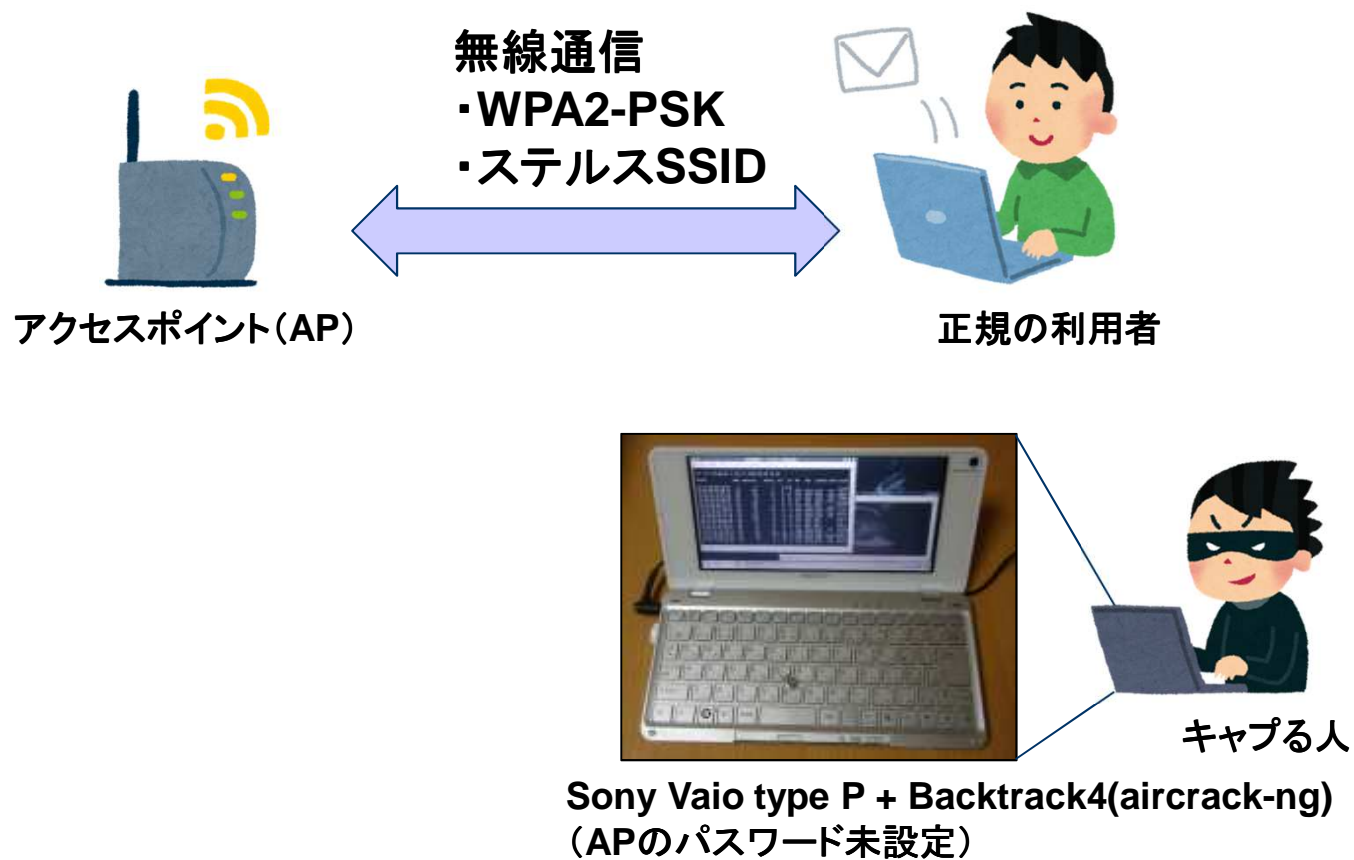
ビジネスホテル等の無料の公共無線LANを利用する際は,
盗聴される前提で利用しましょう(POP3はやめましょう)
(企業で使う場合は, IEEE802.1x EAP-TLSを使いましょう…)



3.[オマケ]やってみよう！

やってみよう(1) 検証環境

- 論より実践！ご家庭の無線LAN通信をキャプチャしてみましよう。



やってみよう(2) キャプチャ直後の状況

- キャプチャ始めた直後の画面です。電波がたくさん飛んでいるのが分かります。

```
root@bt: ~ - シェル - Konsole
Session 編集 表示 ブックマーク 設定 ヘルプ
CH 8 ][ Elapsed: 49 s ][ 2008-08-29 21:55

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:A0:B0:      -45   131      1  0   1  54e. WPA2  CCMP  PSK  <length: 0>
CC:E1:D5:      -83    93      0  0   7  54e. WPA2  CCMP  PSK
00:01:8E:      -83    62      0  0   3  54e. WPA2  CCMP  PSK
52:F6:76:      -85    35      0  0  11  54e. WPA  CCMP  PSK
00:          54e. WEP  WEP
4C:          54e. WPA2  CCMP  PSK
12:          54e. WEP  WEP
10:66:82:      -86    37      0  0  10  54e. WPA2  CCMP  PSK
10:66:82:      -88    32      0  0
12:66:82:      -88    34      0  0
1E:B1:7F:      -88    34      0  0
1C:B1:7F:      -89    35      0  0  5  54e. WPA2  CCMP  PSK
A4:12:42:      -89    31      1  0  7  54e. WPA2  CCMP  PSK
44:DC:91:      -89    36      7  0  9  54e. WEP  WEP
44:DC:91:      -90    41      0  0  9  54e. WPA2  CCMP  PSK
06:24:A5:      -90    22      0  0  6  54e. WPA  CCMP  PSK
1E:B1:7F:      -91    16      2  0  2  54e. WPA2  CCMP  PSK
10:6F:3F:      -90     3      1  0  5  54e. WPA2  CCMP  PSK
^C
root@bt:~#
```

自宅APのBSSID (MACアドレス)

ステルスSSIDなので、まだ見えません

やってみよう(3) 特定APの詳細情報

- 自宅APのBSSIDの詳細情報を見ると、クライアントのMACアドレスが見えます。

```
root@bt: ~ - シェル - Konsole
Session 編集 表示 ブックマーク 設定 ヘルプ

CH 1 ][ Elapsed: 1 min ][ 2008-08-29 22:02

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:A0:B0:00:00:00 -34 100    618    247  0   1  54e. WPA2 CCMP  PSK <length: 0>

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
00:A0:B0:00:00:00 64:80:99:00:00:00 -14   0 - 6e   0      314

back | track 4
- codename [ pwnsa
```


やってみよう(5) キャプチャしたパケットの確認

The image shows a Wireshark interface with a packet capture of a Probe Response. The packet list pane shows a list of packets, with packet 108 highlighted. The packet details pane shows the structure of the IEEE 802.11 wireless LAN management frame, with the SSID parameter set tag expanded to show the SSID in plaintext. The packet bytes pane shows the raw data of the packet, with the SSID bytes highlighted.

Time	Source	Destination	Protocol	Length	Info
105	22:04:57.749492	IntelCor_...	I-ODataD_...	802.11	38 Deauthentication, SN=15, FN=0, Flags=.....
106	22:04:57.749575	IntelCor_...	I-ODataD_...	802.11	39 Deauthentication, SN=15, FN=0, Flags=.....
107	22:04:57.754495	I-ODataD_...	IntelCor_...	802.11	38 Deauthentication, SN=16, FN=0, Flags=.....
111	22:04:57.754533	I-ODataD_...	IntelCor_...	802.11	39 Deauthentication, SN=16, FN=0, Flags=.....
108	22:04:57.755546	I-ODataD_...	IntelCor_...	802.11	289 Probe Response, SN=257, FN=0, Flags=.....C, BI=100, SSID=my...
109	22:04:57.756858	IntelCor_...	I-ODataD_...	802.11	38 Deauthentication, SN=17, FN=0, Flags=.....
116	22:04:57.756903	IntelCor_...	I-ODataD_...	802.11	39 Deauthentication, SN=17, FN=0, Flags=.....
110	22:04:57.758302	I-ODataD_...	IntelCor_...	802.11	289 Probe Response, SN=257, FN=0, Flags=....R...C, BI=100, SSID=my...
112	22:04:57.760716	I-ODataD_...	IntelCor_...	802.11	38 Deauthentication, SN=18, FN=0, Flags=.....

Packet 108 details:

- .000 0001 0011 0000 = Duration: 304 microseconds
- Receiver address: IntelCor_...
- Destination address: IntelCor_...
- Transmitter address: I-ODataD_...
- Source address: I-ODataD_...
- BSS Id: I-ODataD_...
- Fragment number: 0
- Sequence number: 257
- Frame check sequence: 0xe45afc15 [correct]
- IEEE 802.11 wireless LAN management frame
 - Fixed parameters (12 bytes)
 - Tagged parameters (217 bytes)
 - Tag: SSID parameter set: my...
 - Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
 - Tag: DS Parameter set: Current channel: 1
 - Tag: FRP Information

Packet bytes:

Offset	Bytes	ASCII
0040	00 0a 6d 79	d.1. my
0050	01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10
0060	11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20	2...0..
0070	21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30
0080	31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40
0090	41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50>.0..
00a0	51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60P.
00b0	61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70BC^ .b2/...
00c0	71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80

パケットキャプチャすると、SSIDが平文で発信されていることが確認できます

やってみよう(6) PSKの解読(辞書攻撃)

```
root@bt:~# aircrack-ng hoge-01.cap -w dic.txt
```

```
Opening hoge-01.cap  
Read 533 packets.
```

```
# BSSID          ESSID          Encryption  
1 00:A0:B0:XX:XX:XX MyAP-WPA      WPA
```

```
Choosing first network as target.
```

```
Opening hoge-01.cap  
Reading packets, please wait...
```

```
Aircrack-ng 1.0 r10
```

```
[00:00:00] 4 keys tested (35.47 k/s)
```

```
KEY FOUND! [ 1a2s3d4f5g6h7j8k9 ]
```

```
Master Key   : 01 C5 42 7B 15 77 B2 8B E1 9D 16 7D A8 8D F5 D2  
              AE 19 EF 1E AF C0 8F 9F 92 AB 5F 14 63 3E 2D FF
```

```
Transient Key : 6C DA 3A B7 B0 08 F3 71 8F 11 B0 07 4F 16 8A AF  
              FE 7C 8C 3C 3E 0C 3E D0 CA 06 A2 CC 57 44 A0 6B  
              C1 01 53 BD B8 90 96 20 23 CA 05 64 32 61 4B 7A  
              B6 31 37 56 36 B4 54 71 27 8C 77 DD 53 46 94 22
```

```
EAPOL HMAC   : 95 F4 48 36 50 3B BA 41 35 94 5D AC 49 54 69 19
```

```
root@bt:~#
```

キャプチャしたデータを解析します。
今回は辞書に載っているパスワード
だったので、瞬殺でした
(type Pでは、総当たりでこの文字数は厳しい)

まとめ

無線LANのセキュリティ対策は、適切な暗号化技術で実施

WPA2-PSK(AES)はとりあえず安全。でも、いろいろ注意が必要
(大企業であれば、IEEE802.1x EAP-TLSを使うべき。現時点では最強)

ステルスSSID, MACアドレス制限は、補助的に利用