無線LANセキュリティの基礎

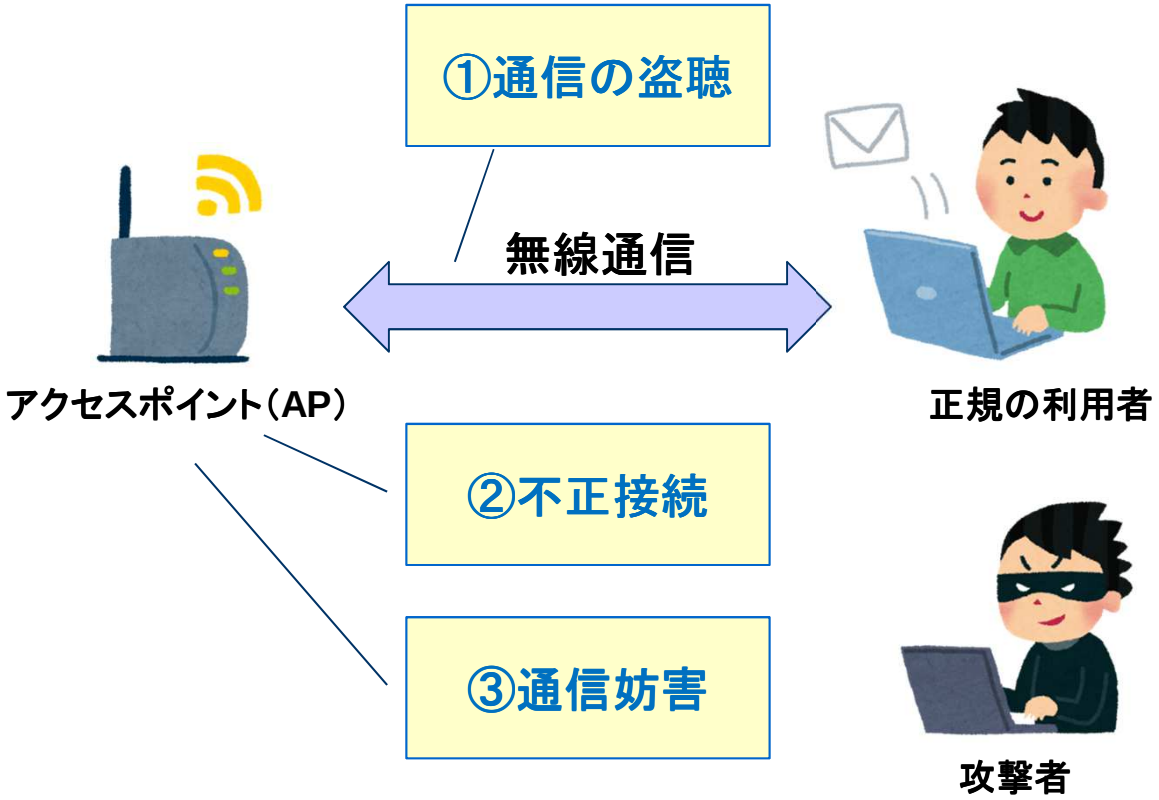
2015年4月19日

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

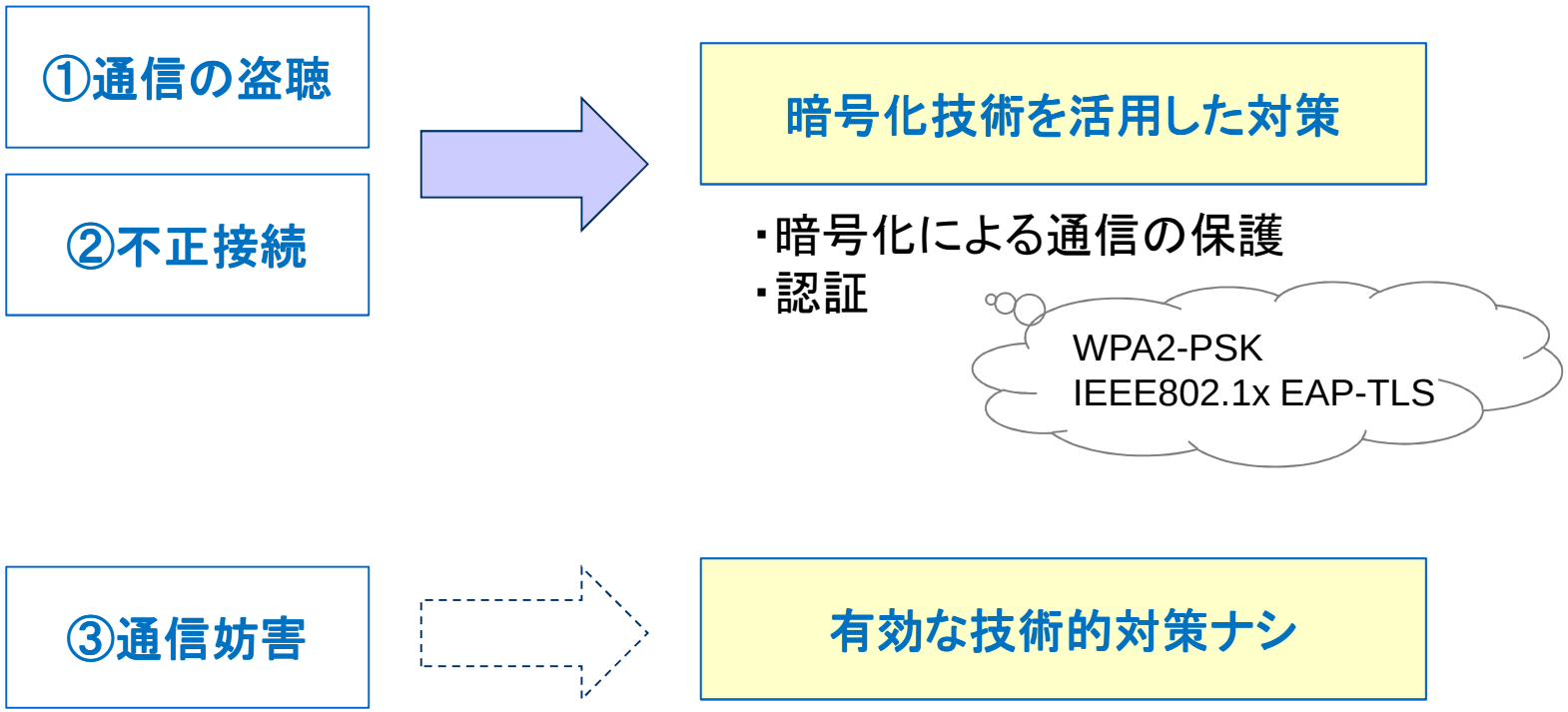
- ネットワークセキュリティの視点で見ると，無線LANの利用には，大きく分けて3種類の脅威があります。



図．無線LANネットワークに対する脅威

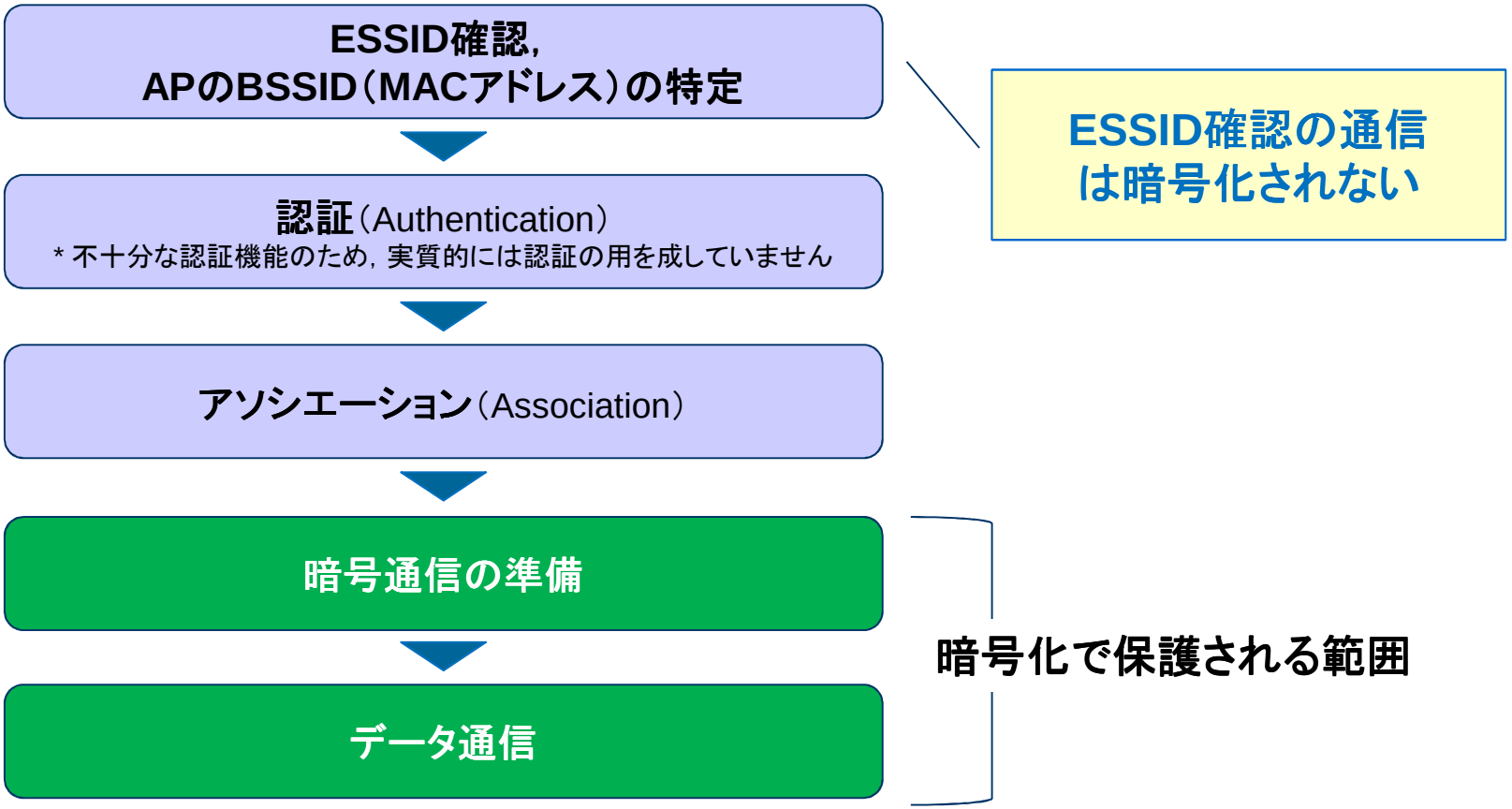
根本的な対策

- 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

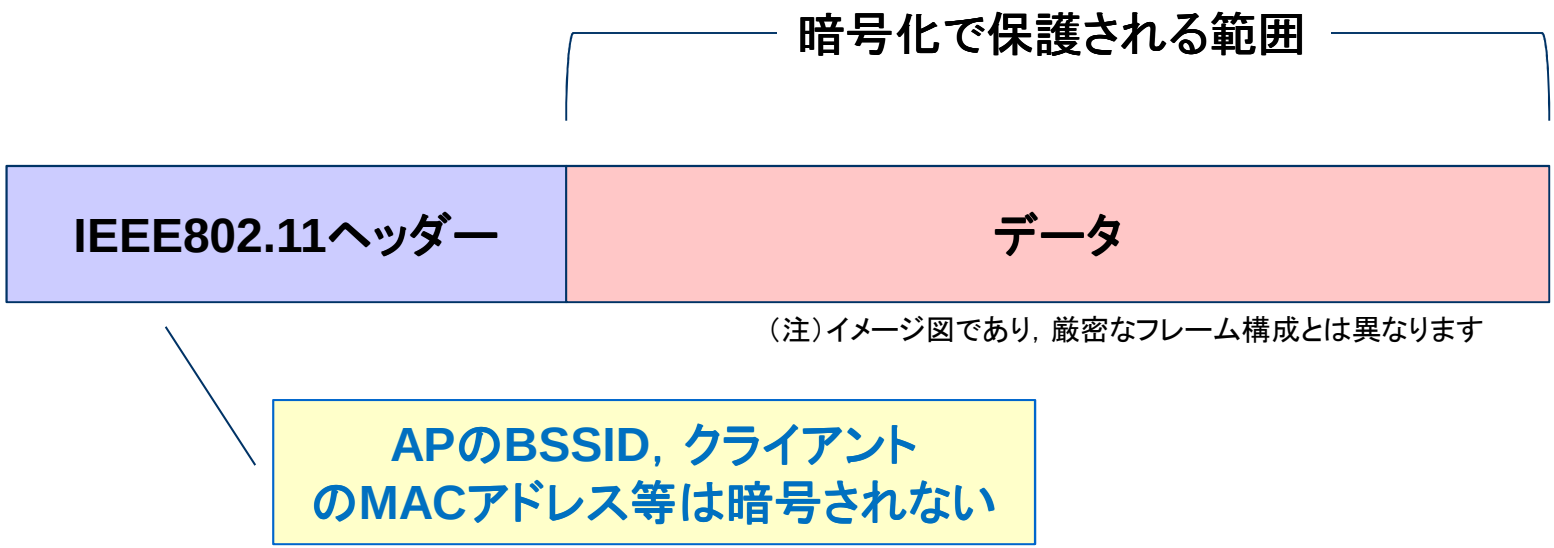
- 暗号化技術を使っていても，クライアントが，APに接続する際，ESSID確認の通信は暗号化されません。



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

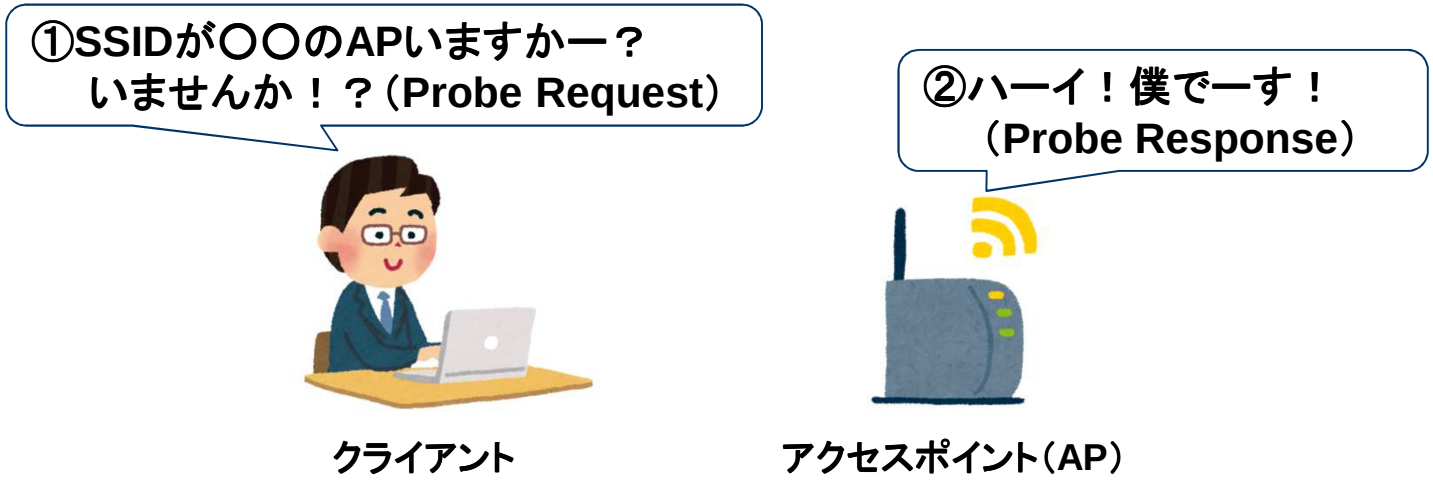
- 無線LANフレームは，ざっくり言うと，「IEEE802.11ヘッダー」と「データ」で構成されています。
- このうち，暗号化されるのは，「データ」部分のみです。
（どの暗号化方式を採用しても同じです）
- IEEE802.11ヘッダーに含まれるMACアドレス等は暗号化されません。



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。



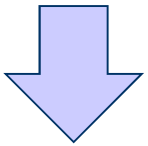
SSID確認の通信は暗号化されないため，
ステルスSSIDにしても，SSIDはすぐバレる
（それに，クライアントが社外でProbe Requestを発信するのは気持ち悪い？）

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

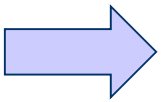
（APのパスワードを知っている正規利用者の私的な利用抑制など）

2.WPA2-PSK

いきなり結論

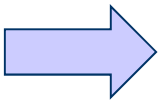
- **WPA2-PSK（暗号アルゴリズム：AES）を利用すれば，とりあえず安全です。**
- **ただし，いくつか注意点があります。**

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



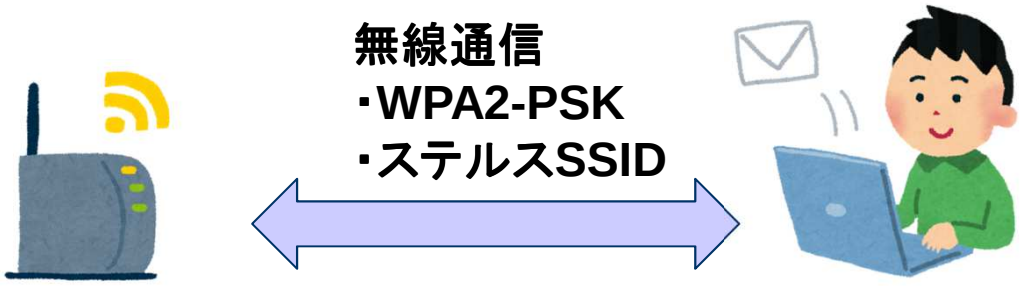
ビジネスホテル等の無料の公共無線LANを利用する際は，
盗聴される前提で利用しましょう（POP3はやめましょう）

（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ょう。



アクセスポイント(AP)

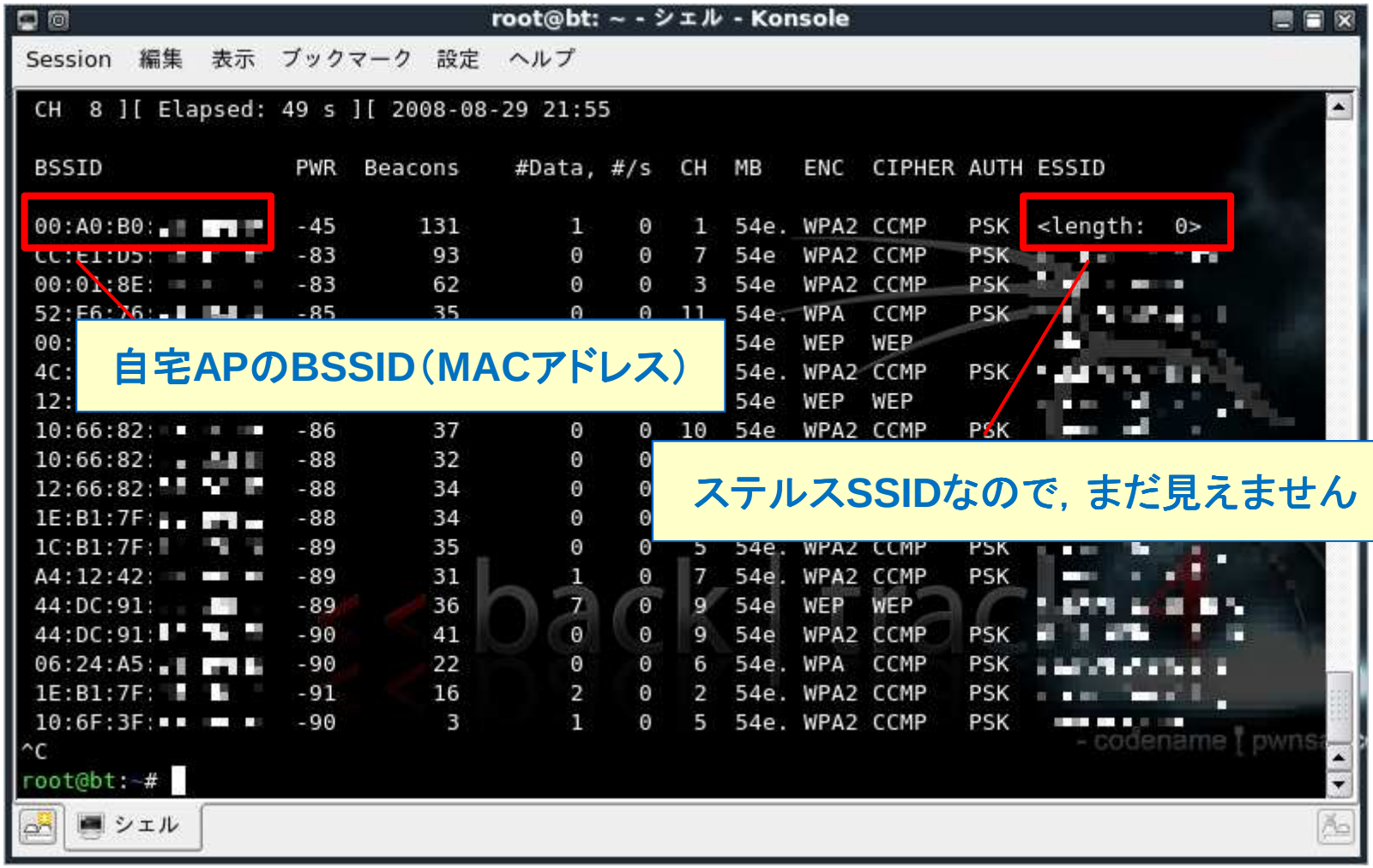
正規の利用者

キャプる人

Sony Vaio type P + Backtrack4(aircrack-ng)
（APのパスワード未設定）

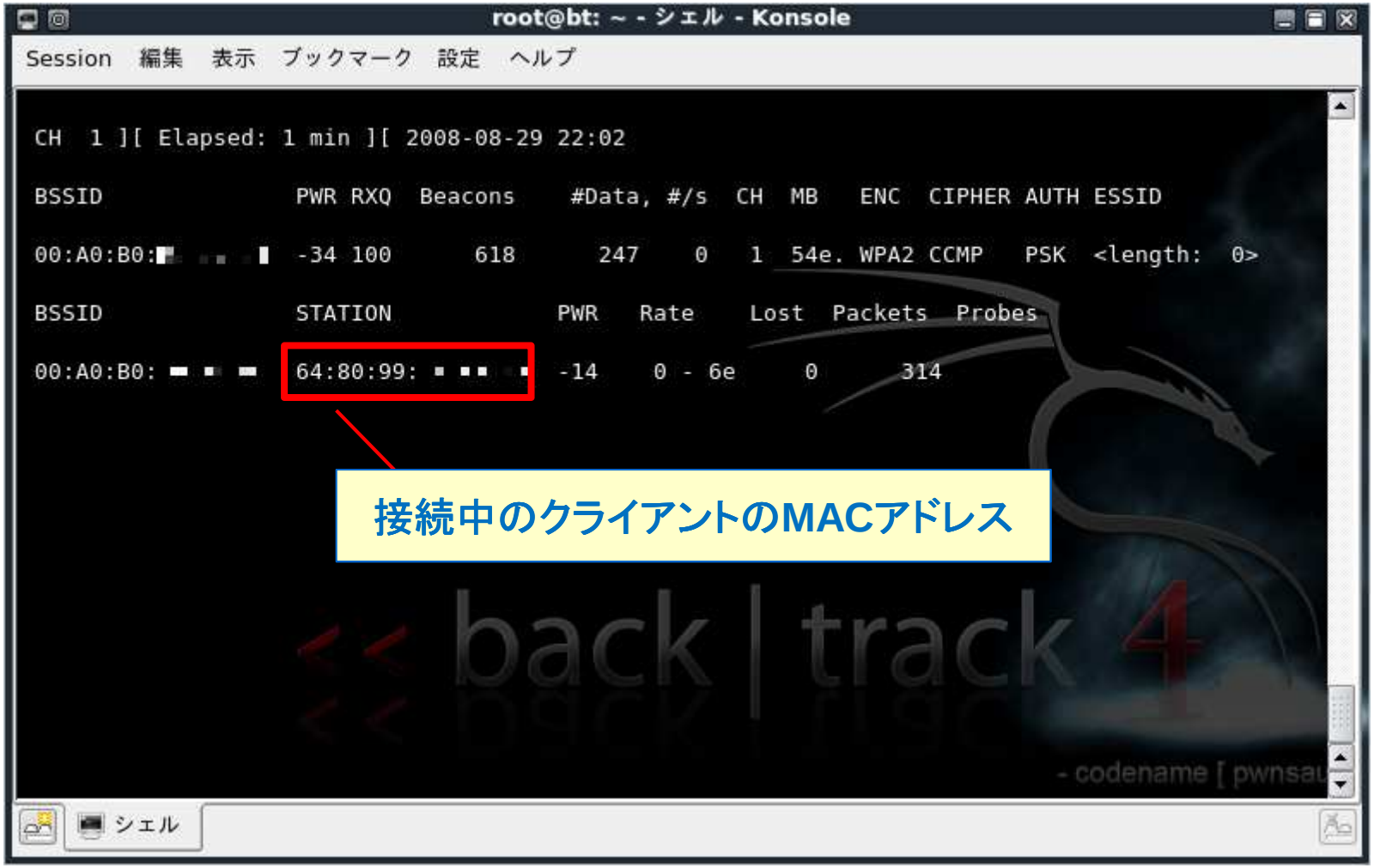
やってみよう(2) キャプチャ直後の状況

- キャプり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。



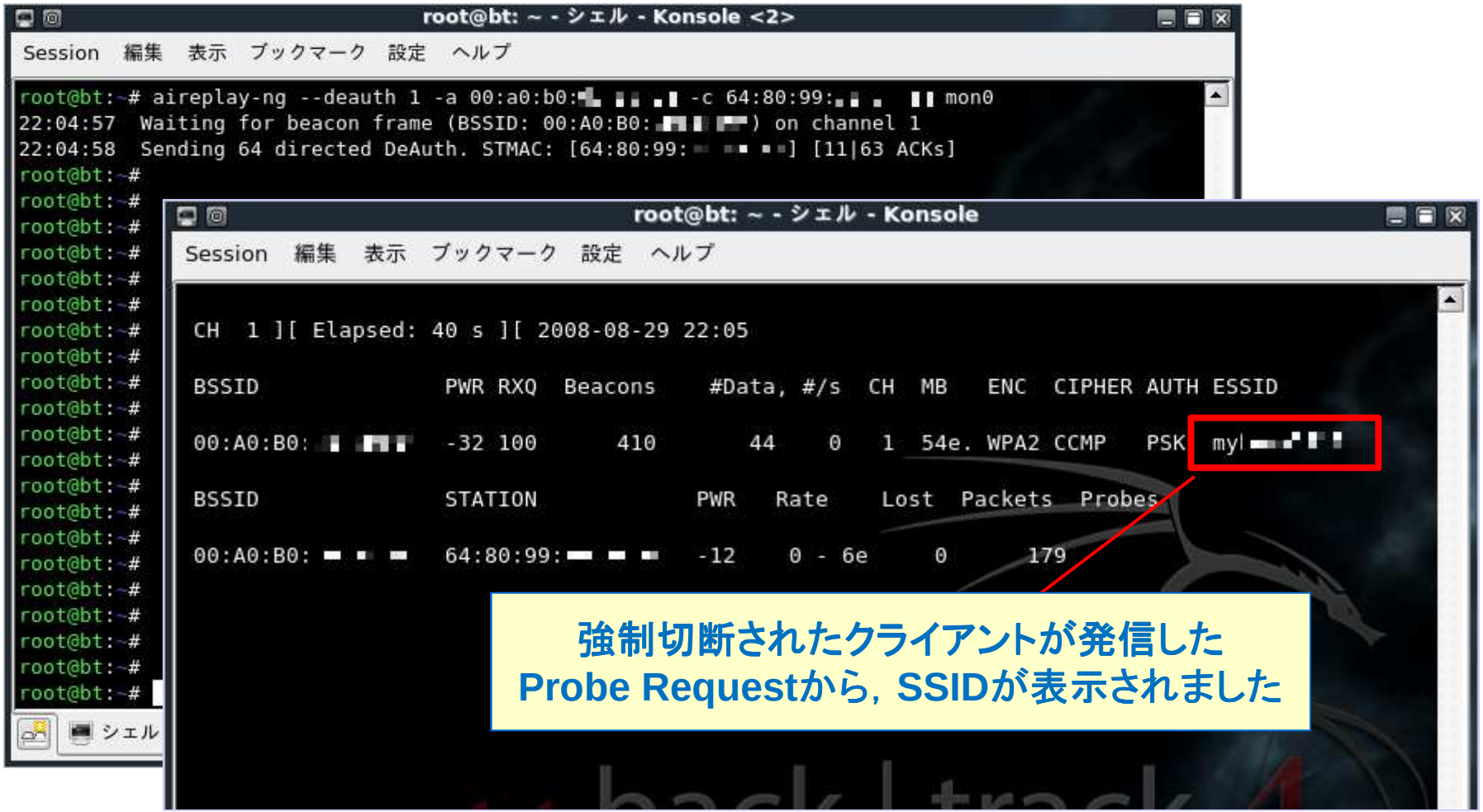
やってみよう(3) 特定APの詳細情報

- 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。

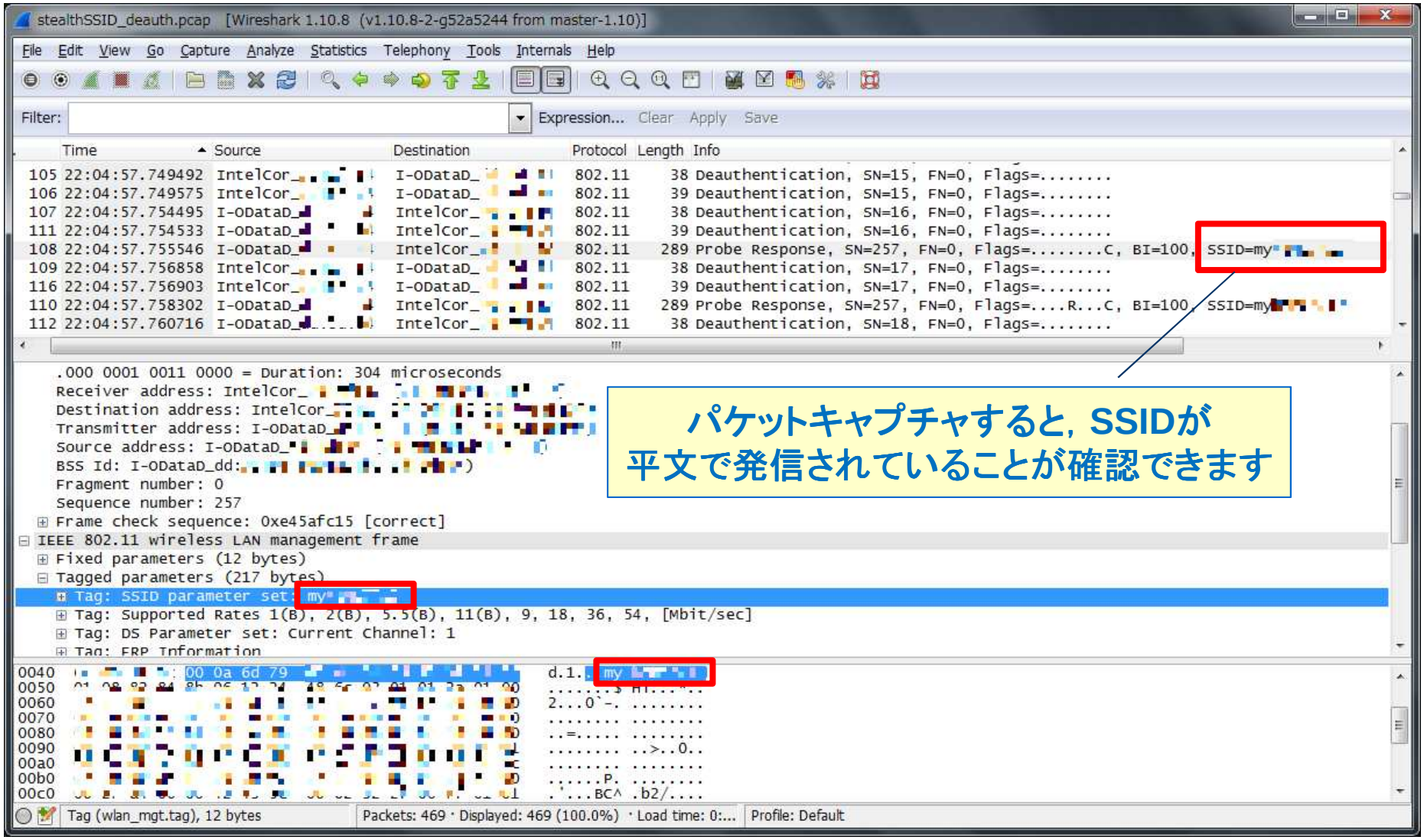


やってみよう(4) ステルスSSID回避

- ジっと待っていれば，いつかProbe Rquestが送信されますが，キャプる人は気が短いので，正規クライアントに認証解除フレーム(Deauthentication)を投げてみます。



やってみよう(5) キャプチャしたパケットの確認



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                  WP

      Choosing first network as target.

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

                                    Aircrack-ng 1.0 r1

                        [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