

## 無線 LAN ～導入編

一般家庭でも企業のように PC を複数台持つことが当たり前になったこの時代。家庭内ネットワークを築くのもはや常識となりつつあります。

無線 LAN は文字通り、無線で接続する LAN (Local Area Network) です。

有線 LAN ケーブルを使わず、フレキシブルにネットワークを構築できます。

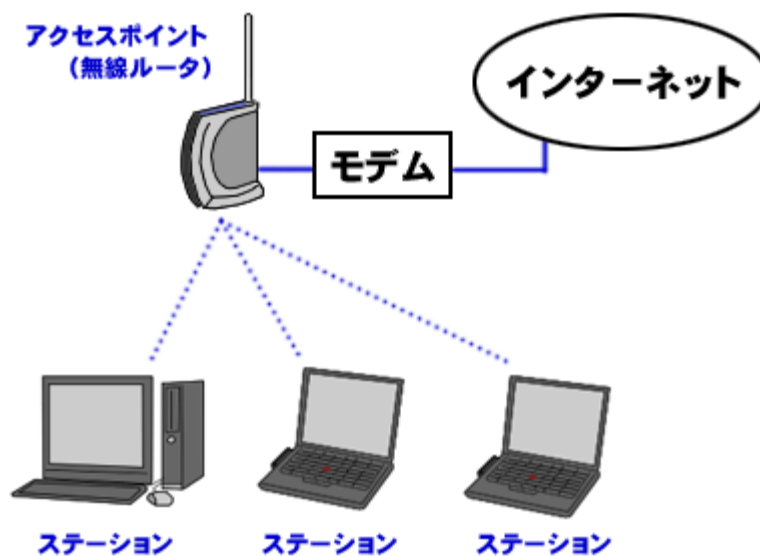
### 無線 LAN 機器を購入する

無線 LAN 機器は、大きく分けて次の 2 種類があります。

1. アクセスポイント(親局)
2. ステーション(子局)

アクセスポイントは、子局を収容する基地局となる無線 LAN 機器です。コードレス電話の親機のようなものです。ステーションは、親局に接続する無線 LAN 端末です。先の例えでいうと、コードレス電話の子機になります。

アクセスポイントの下にステーションが 1 台、あるいは複数台がぶら下がる形になります。



## **アクセスポイント(親機)**

アクセスポイントには、ブリッジタイプとルータタイプがあります。

ブリッジとは、無線 LAN 機器同士を単純に接続するもので、有線 LAN でいう HUB のような役割です。ルータとは、インターネットに複数台の PC が接続する LAN を構築する際に必要な機器です。

ブリッジタイプのアクセスポイントは、基本的に 1 台の PC しかインターネットに接続できないと考えてください。同時に複数台の PC でインターネットに接続する場合は、ルータタイプのアクセスポイントが必要になります。通常は、ルータタイプを買えばまず問題ありません。ADSL モデムなどにルータ機能が備わっていても、どちらかのルータ機能を OFF にすればいいだけだからです。

今は 1 台しか PC がないという人も、とりあえずルータタイプを買えば、今はもちろん、将来的に PC を買い足すようなことがあっても問題ありません。

## **ステーション【子機】**

子機のステーションの方ですが、ステーションには様々なタイプのものがあります。

CardBus タイプ、USB タイプ、Ethernet メディアコンバータなどです。

CardBus はノート PC で使用します。最近のノート PC ならば殆どの機種に CardBus スロットが搭載されているはずです。

Ethernet メディアコンバータは、デスクトップ PC で使用するのにお勧めです。他のステーションよりやや高価だったり、電源が必要だったりという欠点もありますが、文字通り Ethernet (有線 LAN) を無線 LAN に変換してくれる機器ですので、デスクトップ PC に有線 LAN ポートが備わっていれば、デスクトップ PC の OS に依存することなく使用できます。つまり、ドライバなどをインストールしなくても、機器の設定だけで使用できます。

USB タイプは最もお勧めできないタイプのステーションです。OS にドライバのインストールが必要であったり、変な位置に設置する必要があったり、内蔵アンテナが質がさほど良くない傾向があるからです。

ステーションの長所、短所を種類ごとにまとめると、次のようになります。

種類	長所	短所
Ethernet メディアコンバータ	ドライバ不要、OS 不問	別途電源が必要
CardBus	ノート PC 用に最適 電源不要	要ドライバ、OS 依存 ノート PC から出っ張る
USB	電源不要	要ドライバ、OS 依存 電波の飛びがあまり良くない

また、最近のノート PC のハイエンドモデルの場合は、無線 LAN が内蔵されている場合があります。無線 LAN 内蔵のノート PC を持っている場合は、そのノート PC のためにステーションを用意する必要はありません。

ステーションを購入するのに問題になるのは、何を買えばいいのかということです。PC 等の種類別に見ると、一般的に次のようになります。

使用機器	条件	お勧めステーション
デスクトップ PC	有線 LAN 使用可	Ethernet メディアコンバータ
ノート PC	無線 LAN 内蔵	不要
	内蔵無線 LAN なし	CardBus
プレイステーション 2	—	Ethernet メディアコンバータ
PSP Nintendo DS	無線 LAN 内蔵につき不要	

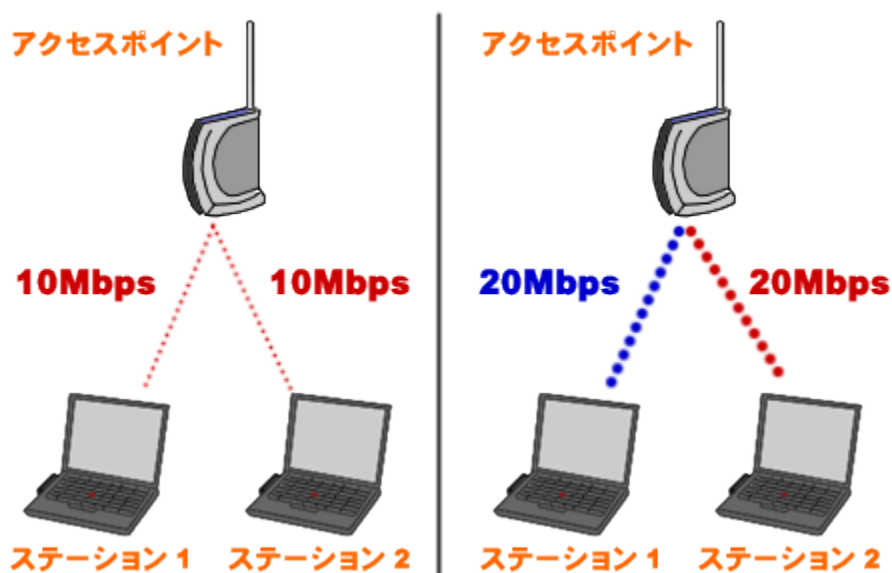
### アクセスポイントのタイプ

アクセスポイント(無線ルータ)だけは入手時、気を付ける必要があります。

アクセスポイントには、IEEE802.11a(5GHz 帯)と IEEE802.11g(2.4GHz 帯)を切り替え

で使えるタイプと、両規格を同時に使えるタイプがあります。どちらか一方ができればいいような気がする人もいるかと思いますが、そうではありません。無線 LAN は、5GHz と 2.4GHz の帯域で、それぞれどちらも普通にやれば 20Mbps 程度の通信速度になります。ここで、例えば、11g だけの無線ルータ(親機)に 2 台のステーション(子機)が接続したとすると、それぞれのステーションは 20Mbps の速度を分け合うことになり、単純にいうと 10Mbps ずつの通信速度になります。

しかし、2 台のステーション(子機)を 11a と 11g で別々に接続すると、それぞれで 20Mbps の通信速度を期待できるのです。



ですので、ステーションが 2 台以上になる場合は、**11a/g 同時利用タイプ**のアクセスポイント(無線ルータ)を導入した方が、帯域を有意義に使え、かつ同時接続時の通信速度の低下も防ぐことができます。

ただし、IEEE802.11a (5GHz 帯)の電波の飛びは、IEEE802.11g のそれと比べるとあまり期待できませんので、11a に期待して導入しても、結局電波が届かず、利用できないというリスクがあることも考慮しておく必要があります。

## 無線 LAN のセキュリティ対策

### 狙われる無線 LAN

最近では、ノート PC だけでなく、さまざまな機器が無線 LAN を使い、通信を行っている。最近大流行しているタブレット型端末やスマートフォン、さらにはゲーム機なども無線 LAN を使えるようになっている。

また、家庭内では、ブロードバンドルーターにアクセスポイントの機能を付加することで、LAN 配線が不要になり、無線電波の届く範囲であれば、自由に LAN を使用することができるようになるなど、一見するととても便利な機能であるが、この点を突いた攻撃が行われているのである。

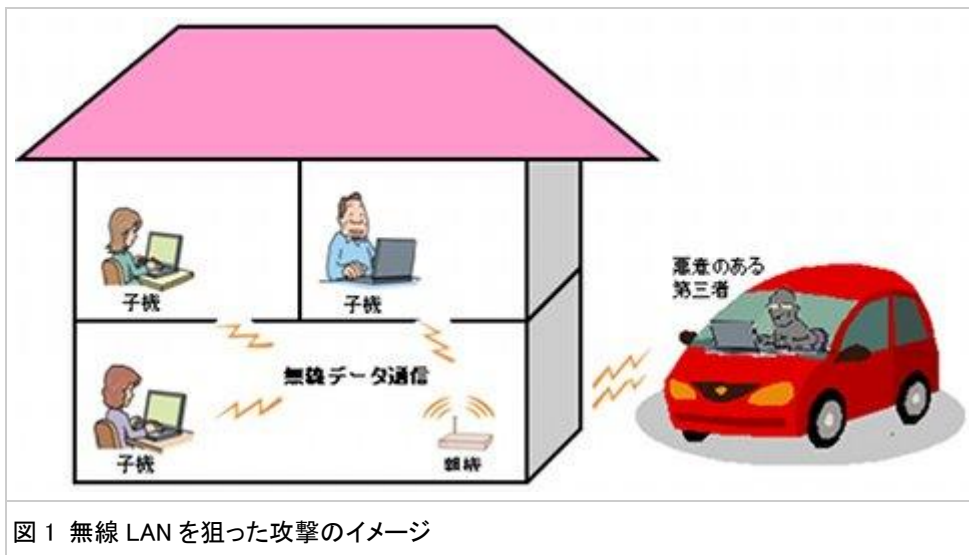


図 1 無線 LAN を狙った攻撃のイメージ

図 1 を見ていただきたい。無線 LAN を使った一般的な利用例である。無線 LAN アクセスポイント (親機) から、ノート PC などの子機と通信を行っているものだ。しかし、電波は、目に見えるものではない。また、多少の遮蔽物あっても、電波ならば透過してしまう可能性もある。最近では、通信速度の高速化と同時に無線 LAN の到達範囲も拡大されている。つまりは、屋外でも状況によっては、無線 LAN の電波を傍受することが可能となっているのである。これを、悪意を持った犯罪者が狙うのである。

具体的に以下のような被害が報告されている。

- インターネットに接続可能な携帯ゲーム機を使用して他人の家の無線 LAN に無断で接続。さらに、インターネットの掲示板に無差別殺人をほのめかす書き込みをしたとして、男が逮捕された(2008 年 6 月)
- インターネットオークションで、児童ポルノの DVD を販売したとして逮捕された男が、他人の家の無線 LAN に無断で接続し、児童ポルノのファイルを入手していた(2008 年 10 月)
- 他人の家の無線 LAN に無断で接続し、あらかじめ不正に入手していた他人のクレジットカード情報を使用してインターネットで買い物をしたとして、詐欺グループのメンバー 2 人が逮捕された(2010 年 2 月)
- インターネットの掲示板に銀行口座を販売するなど書き込み、現金を騙し取ったとして逮捕された男が、身元が特定できないように他人の家の無線 LAN から無断でインターネットに接続していた(2010 年 6 月)

ここで注目したいのは、直接的に接続した無線 LAN 内の PC などから情報を奪取することが目的ではなく、自らの存在を隠すために隠れ蓑(このようなことを「踏み台」にするという)にしている事例が多いことである。

犯罪行為を実行するにあたり、まずは身元を隠そうとしているのである。このように実害は発生しなくても、犯罪行為に加担することになってしまう。

## 無線 LAN の対策は？

さて、このような無線 LAN の盗聴に対し、どのような対策が求められるのか？電波自体は見えないし、その到達範囲を設定することは不可能である。

### ●アクセス制限による不正侵入防止

MAC アドレスを無線 LAN(アクセスポイント)に登録し、登録されていない MAC アドレスからの接続を拒否することができる。

### ●無線 LAN の SSID を隠す

無線 LAN 接続するためには ESS-ID と呼ばれる無線 LAN におけるネットワークの識別 ID が必要になる。ただ ESS-ID はピーコン(周囲に送信されている情報)に含まれているため、ESS-ID を知らない人でも情報を取得して接続することができてしまう。

ESS-ID ステルス機能を使用すると、「ピーコン」に ESS-ID を含まないようにすることが出来る。

### ●データ暗号化

基本は親機と子機間の通信を暗号化することである。その方法に 2 つの重要なポイントがある。まずは、「適切な暗号化方式の選択」である。一般的な認証方式には、次の 3 つがある。

\* 無線の内容を暗号化し、データの盗聴を防ぐことができる。また、パスワードを知らないと接続することも出来なくなる。

暗号化規格	解説
WEP	初代の暗号化規格、暗号化解析ツールなどがインターネット上に出回っており、解読されてしまう可能性がある。
WPA	WEP の解析されてしまう脆弱性が改善されている。 現在、解析方法などは発見されておらず比較的安全とされている。
WPA2	WPA がさらに強化されている。

後者ほど安全性が高い。さらに、WPAとWPA2には、AESとTKIPという2つの暗号化方式があり、機器によってはこれらを組み合わせて設定できる。

IPA(独立行政法人情報処理推進機構)では、**暗号化方式に AES、認証方式に WPA2 の WPA2-PSK(AES)を使うようにすべき**としている(その理由は、TKIP による暗号が解読されたことによる)。WPA2 が使えない場合は WPA を選択するが、WPA の場合も同様に AES の暗号化を選択する(つまりいずれの認証方式でも、**暗号化は AES を使うべきである**)。暗号化をしないや WEP は決して選択すべきではない。



図 2 認証と暗号化方式の設定

なお、これらの設定は機器によって異なるので、マニュアルなどで確認してほしい。同時に子機の設定も忘れずに行う。正しく設定された状態では、図 3 のように設定状態が確認できる。



図 3 親機の設定状態の確認

そして、もう1つのポイントが「適切なパスワードの設定」となる。暗号化では暗号鍵を生成するために、パスワードが必要になる。いくら安全な暗号化を設定しても、パスワードが弱い(一般的には短く、辞書にあるような文字列)と意味がない。IPA では、以下の注意事項をあげている。

1. 英語の辞書に載っている単語を使用しない
2. 大文字、小文字、数字、記号のすべてを含む文字列とする
3. 文字数は最低でも 20 文字(半角英数字＋記号の場合。最大で 63 文字)とする