無線 LAN の規格とセキュリティー ～ 802.11b･a･g･n ～

無線を利用して LAN を構成し、ネットワークを共有したりインターネットの利用を共有したりする「無線 LAN」が急速に普及してきました。

無線を利用することで、ケーブルが乱雑する煩わしさから解放され、見た目がすっきりする上、何より無線の届く範囲内での移動が可能となります。

各デバイスの無線接続については、Bluetooth とは で解説しましたが、本項では、無線 LAN の規格とセキュリティーについて解説したいと思います。

さて、まず無線による接続はどうするかというと、大きく分けて 2 つの接続方法がありますが、基本的な接続方法は、親機に子機を接続して、親機を介して子機同士が通信するという形態が一般的です。

つまり、無線 LAN を構築する場合、親機となる機器に子機となるパソコンが接続する形態となります。このように、その無線 LAN のグループがアクセスする親機のことを、

無線 LAN アクセスポイント

と言います。無線アクセスポイントは、ルータが兼ねる場合が一般的で、無線 LAN 機能を有したルータをアクセスポイントとして無線 LAN を構築します。(ルータについては、データ伝送 を参照してください)

つまり、例えば家庭内とした場合、ルータがインターネット接続のゲートウェイとなり、さらに家庭内を無線でネットワークした LAN に IP アドレスを与え、通信を仲介する親機ともなるわけです。

したがって、ルータ(それぞれの機能を有しているルータ)が一台あれば、インターネットとの接続、ファイアフォールやパケットフィルタリングによるセキュリティ機能、無線 LAN のアクセスポイント、DHCP や NAT 機能による各端末への IP アドレスの割り当て、ハブとしての機能など様々な役割を担ってくれるのです。(DHCP については、IP アドレスとは(1) を参照してください)

対して子機の側は、

無線 LAN アダプタ(LAN カード)

と呼ばれる拡張カードを子機に接続して、アクセスポイントと通信します。無線 LAN アダプタは、PC カードタイプのものや USB タイプのもの、すでにアダプタを搭載しているパソコンもあります。

このように、アクセスポイントを介して接続する形態を「*インフラストラクチャモード*」、そして、アクセスポイントを介さずに機器同士で直性通信し合う形態を「*アドホックモード*」と言います。アドホックモードで代表的なのは、携帯用ゲーム機同士の通信などです。

では、実際に LAN を構築するとして、無線接続形態が決まったら次に「通信規格」を決めなければなりません。前項で解説した有線接続のイーサネット規格のように、無線 LAN にも規格がいくつかあり、それに従って通信を行います。

無線 LAN の規格は、インターフェースとは で解説のとおり、IEEE の 802.11(アイトリプルイー ハチマルニテンイチイチ)によって定められています。「802」というのは、IEEE という電子技術者協会の 802 委員会(1980 年 2 月に活動開始から由来)が定めたという意味で、「11」はワーキンググループ 11 の意味で、無線 LAN にかかる項目を指します。

※ 有線 LAN は、IEEE802.3 委員会、Bluetooth などの PAN は、IEEE802.15 委員会で規格が策定されています。

IEEE802.11b

もっとも初期に普及した無線 LAN の規格で、Bluetooth と同じ免許不要の 2.4GHz 帯の電波を使用する規格です。通信距離、安定性にも優れており、多くの機器が対応している無線 LAN の代表的な規格になります。
ただし通信速度は、最大 11Mbps（実質速度は 5Mbps 程度）と若干遅く、光ファイバーなどの大容量回線を利用してインターネットを利用している場合には、ルータまでは 100Mbps 程度の速度があっても、ルータから子機端末までは 11Mbps となり、力不足となります。
また、2.4GHz 帯は他の機器も使っており、*Bluetooth 機器と混信する* というデメリットがあります。混信を避けるために、3 チャンネル程度の間隔を空けて利用します。

IEEE802.11a

11b のデメリットである、他の機器との混信を解消するため、アメリカ連邦通信委員会が 5GHz 帯の一部を免許不要な無線アクセス用に開放したことを受け、5GHz 帯を使用し、最大 54Mbps（実質速度は 20Mbps 程度）の通信速度を実現した規格です。
ただし、5GHz 帯の利用制限として、*屋外での使用が認められていない*、*11b 機器と通信できない* というデメリットがあります。

IEEE802.11g

11b、11a 双方のデメリットを解消するため、11b の帯域（2.4GHz）に 11a の技術を適用することで、最大 54Mbps の高速通信速度を実現した規格です。
11g は 11b の上位規格であり、11b 機器と 11g 機器の通信が可能となります。11b 機器との通信は 11Mbps で行われます。ただし、11a 機器と通信することはできません。（現在では、同時接続が可能なルータが販売されています）
デメリットとしては、2.4GHz 帯の混信問題は完全に解消されない、11b 機器を混在させると実効速度が落ちるといったデメリットがあります。

IEEE802.11n

2009 年に正式に製品化された次世代規格で、複数のアンテナでの送受信、複数のチャンネルの結合などを行う技術を用いて、高速大容量化を実現した規格です。この技術を、

MIMO（マイモ）

と言います。MIMO は「Multiple Input Multiple Output」の略で、複数のアンテナで同時に異なるデータを送信し、受信時に合成する技術です。したがって、理論上はアンテナが増えるほど広帯域を使用できることになり、11n では、MIMO によって最大 600Mbps（実質速度 100Mbps 以上）の超高速な伝送速度を実現します。
ただし、600Mbps というのは、アンテナ 4 本という最も高速な組み合わせによる理論上の速度であり、現在では法律上の制限などで、最高速度は 300Mbps の製品が販売されています。
さらに、11n は 11a をベースに、複数のアンテナを使うため、2.4GHz／5GHz の 2 つの周波数帯域を同時に使用することでき、それによって、11b、11a、11g との相互接続が可能となります。
また、複数のアンテナから複数の経路を通って電波が届くことで、安定したデータ伝送が可能になるという効果もあります。

無線 LAN の規格

項目	IEEE802.11b	IEEE802.11a	IEEE802.11g	IEEE802.11n
周波数帯域	2.4GHz	5GHz	2.4GHz	2.4GHz／5GHz
通信速度	最大 11Mbps	最大 54Mbps	最大 54Mbps	最大 600Mbps
メリット	ほとんどの製品が対応してい	混信がない	11b と互換性がある	速度が速い

無線 LAN の規格

項目	IEEE802.11b	IEEE802.11a	IEEE802.11g	IEEE802.11n
	る			他規格と互換性がある
デメリット	速度が遅い 混信がある	屋外では使用不可 11b と互換性がない	混信が解消されたわけではない 11b を混在させると速度が落ちる	現在のところ特になし

現在では、次世代規格である 11n の普及が進んでいます。また、MIMO 技術によって、従来の 11g 製品でも 2 倍以上の通信速度を実現した製品も登場しています。

このように、現在ますます無線化の流れが進んでいますが、無線 LAN の普及を進めるために、WECA という業界団体が無線 LAN 製品に与えるブランドを創設しました。そのブランド名を、

Wi-Fi（ワイファイ）

と言います。Wi-Fi は「Wireless Fidelity」の略で、Wi-Fi ブランドは、他社製品との互換性が検証された無線 LAN 製品に与えられます。認定製品は、Wi-Fi のロゴを使用することができます。

では次に、セキュリティ対策について解説して行きましょう。

無線によってデータをやり取りするということは、電波に乗ってデータがそのまま空中を飛んでいるということです。したがって、有線とは異なった特有のセキュリティ対策が必要になってきます。

無線 LAN による危険性は、電子メールのセキュリティ編 で解説した、盗聴・改ざん・なりすまし・否認やマルウェア、踏み台などの有線の接続と同様の危険性があり、さらに無線特有の危険性があります。そのため、無線 LAN では機器に適切なセキュリティ設定を行わないままで使用すると、重大な被害を受けかねません。

無線 LAN 特有の危険性には、

電波の傍受とネットワークへの不正接続

が挙げられます。電波の傍受は、無線で空中を飛び交うデータを盗聴されるということで、無防備なデータは簡単に盗聴されてしまいます。

不正接続は、電波の届く範囲内であれば、セキュリティ対策をしていないネットワークの場合、誰でもそのアクセスポイントに接続することができ、なりすましによるインターネットの利用、ひいてはそのネットワーク内に進入できてしまうことになります。

ネットワークに侵入出来てしまうということは、電子メールを盗聴・改ざんされるのとはわけが違い、パソコン内に保存している情報をすべて見られてしまうということになりかねません。

こうした脅威に対抗するためには、様々な対策を講じる必要があります。基本的なセキュリティ対策の概要としては、

ネットワークに接続する機器を制限する

通信を暗号化する

という 2 本柱になります。ネットワークに接続する機器を限定することで、外部の第三者による不正接続を防止することができ、通信を暗号化することでデータを盗聴されても、内容を解読される恐れがなくなります。

まず、ネットワークに接続する機器を限定するための方法は、

MAC アドレスフィルタリング

MAC アドレスとは、プロトコルとは で解説のとおり、LAN アダプタなどのイーサネットカード（NIC）に与えられる固有の番号です。

無線 LAN のアクセスポイントに、利用するパソコンの MAC アドレスを登録して、登録されていない MAC アドレスはアクセスポイントを利用できないようにフィルタリングすることを、MAC アドレスフィルタリングと言います。
MAC アドレスフィルタリングにより、第三者が電波を不正利用するのを防ぐことができます。

ESSID の変更・ステルス化

ESSID（イーエスエスアイディー）とは「Extended Service Set IDentifier」の略で、無線 LAN における LAN をグループ分けするための識別名を指します。（SSID とも呼ばれます）
同じ ESSID が設定されているアクセスポイントとパソコン間でのみ通信を行うことができるため、逆に言えば、ESSID を知っていればその無線 LAN を利用することができます。
そのため、極力推察されにくい名称に変更しておくことも重要な対策です。多くの製品では、初期設定がメーカー特有のものだったりして推測されやすい名称が設定してあるためです。
また、第三者からの ESSID 検索に応答しないために、ESSID の通信信号をステルス化（隠ぺい）することも有効な対策になります。
アクセスポイントは、定期的に ESSID を通知する信号（ビーコン信号という）を発信しており、このビーコン信号を停止することで、ネットワークの存在を検知されにくくすることができます。

ANY 接続の拒否

ANY 接続とは、アクセスポイントの ESSID を空欄に設定した場合に、クライアントから電波が届く範囲にあるアクセスポイントの中で最も電波状態が良いアクセスポイントに接続する方法のことです。
この方法を使うと、アクセスポイントの ESSID がわからなくても接続がすることができるので、フリースポット（ホテルや飲食店、駅などで無線 LAN のアクセスポイントを開放して、無料でインターネットにアクセスできるエリアサービス）を提供している場所などで利用されています。
しかし、 ANY 接続を許可していると、当然ネットワークに不正接続される危険性が高まります。ANY 接続は必ず拒否するように設定しましょう。
これらが、不正接続を防止する基本的な対策になります。この他にも、アクセスポイントの接続にパスワードを設定したり、ID を変更したりすることも有効な対策になります。
次に、通信を暗号化するための方法は、以下の 3 つの規格があります。

WEP（ウェップ）

WEP は「Wired Equivalent Privacy」の略で、主に 11b の通信を暗号化するために使われている技術です。
暗号化には 64 ビットもしくは 128 ビット（どちらかの指定が可能）の WEP キーと呼ばれる暗号鍵が使われますが、鍵の値の一部が固定されているため、コンピュータの処理速度の向上に伴い、解読が可能となっています。
したがって、古いルータなど、WEP しか対応していない製品は買い換えた方が無難です。

WPA（ダブリュ ピー エー）

WPA は「Wi-Fi Protected Access」の略で、Wi-Fi が策定した規格になります。企業向けと一般向けの2種類の規格がありますが、本項では個人用の一般向けについて解説します。
WPA は、WEP の脆弱性を補強した上位規格で、暗号化には、

TKIP（ティーキップ）

と呼ばれる暗号化プロトコルを採用しています。TKIP は「Temporal Key Integrity Protocol」の略で、WEP とは異なり、暗号鍵は一定の間隔で更新され、端末（通信パケット）ごとに異なる暗号鍵が使われます。つまり、その無線 LAN 内のパソコンごとに異なる暗号鍵が使われるということです。
また、WEP の強化版であるため、WEP との互換性も確保されており、旧機種でもファームフェア（詳しくは、プログラムとソフトウェアのまとめ を参照してください）のバージョンアップのみで WEP に対応できる製品もあります。

ただし、WPA においても TKIP の鍵を数秒から数十秒で算出する方法が、神戸大学と広島大学の教授らによって開発されており、脆弱性が懸念されています。

WPA2（ダブリュ ピー エー ツー）

WPA2 は、WPA のバージョンアップ版で、より強固な暗号化方式です。基本的にはそれほど WPA と変わりませんが、暗号方式は TKIP に代わり、

AES（エーイーエス）

と呼ばれる現在主流の共通鍵暗号化方式を採用しています。（AES については、電子メールのセキュリティ（1） を参照してください）

AES も TKIP と同様に、通信中でも暗号鍵を変更し続けることで鍵が解読されることを防ぐ方式ですが、暗号化処理の方法が TKIP がソフトウェアで行うのに対し、AES はハードウェアで行うため、より高度な処理が可能となっています。

そのため、アクセスポイントとアダプタ両方のハードウェアに機能として組み込まれている必要がありますが、改ざん検知の機能も備えた、現在において最もセキュリティの高い規格となています。

無線 LAN の暗号化方式

規格	WEP	TKIP	AES
WPA	○	◎	△
WPA2	○	△	◎

上表は、無線 LAN の暗号化方式と暗号化の規格の対応状況を表しています。WPA でも AES に対応している機種があります。（△の部分の対応はメーカーや機種によって異なります）

今後は、WEP は当然ですが、TKIP も脆弱性が発見されていますので、WPA2 規格による AES 暗号化通信が主流になると思われます。安全な通信を行うために、WPA2 に対応した製品を購入する、買い換えるといったことが必要だと思います。

さて、無線 LAN にはこのようにいくつかの規格があり、無線独特のセキュリティ対策が必要になります。ただ、こうした一つひとつの対策は、ある程度の知識が必要で初心者では難しい上に、かなり煩雑な作業になります。

そこで、ルータ等のデバイスの大手メーカーの BUFFALO（バッファロー）は、親機と子機のボタンを押すだけで、ワンタッチで無線接続とセキュリティ設定が完了してしまう機能システムを開発しました。このワンタッチ機能のことを、

AOSS（エーオーエスエス）

と言います。AOSS は「AirStation One-Touch Secure System」の略で、親機と子機の双方で同時に AOSS ボタンを押せば、無線 LAN のあらゆる設定を自動的に行うことができます。

AOSS システムは、プレステ 3 やニンテンドーDS、Wii などのゲーム機にも組み込まれています。