IT化スモールスタート解説（第5回）

社内に無線LANを導入する前に確認しておきたいこと

2020.03.26

ネットワークへの接続方法として、LANケーブルを使わない無線LANは、非常に便利な接続方法です。しかし、導入する際は何点か注意しなければならないポイントがあります。

今回は、無線LANの仕組みと合わせて、メリット・デメリット、選ぶときのポイント、セキュリティ対策方法について解説します。

無線LANの仕組み

無線LANは、LANケーブルを使わずにネットワークに接続するLANシステムであり、ワイヤレスLANとも呼ばれます。無線LANの通信方法はさまざまで、代表的なものがWi-Fiです。これは普及している無線LANの一規格、「IEEE802.11」を使用します。

無線LANは電波を使って通信を行うため、受信できるデバイスがあれば簡単に通信内容を盗聴されてしまいます。そのため、SSID（サービスセット識別子）と呼ばれる識別子と暗号化方式を組み合わせ、セキュリティ対策を取ります。

SSIDは、無線LAN接続のグループ分けに利用するIDです。混信を避けるために付ける名前で、ルーターごとに最大32文字の英数字で設定が可能です。パソコンやスマホなどの端末は子機となり、SSIDによって無線LANの接続先を選択しています。

無線LANで利用される暗号化方式には、WEPやWPA、WPA2などがありますが、現在ではWPA2以降の暗号化方式の利用が推奨されています。WEPやWPAはセキュリティの脆弱（ぜいじゃく）性が見つかっており、暗号化していても簡単に盗聴されてしまうからです。特にWEPは、無線LAN初期の暗号化方式で、10秒程度で解読される恐れがあり、注意が必要です。

無線LANで使用する電波は、規格ごとに通信速度や周波数帯が異なります。詳しくは後ほど解説しますが、周波数帯は2.4

GHzや5GHzなどを利用します。

社内に無線LANを導入するメリット・デメリット

社内に無線LANを導入する際は、メリットと合わせてデメリットも理解しておかなければなりません。1つずつ見ていきましょう。

＜メリット＞
社内に無線LANを導入する最大のメリットは、配線がなくなりスッキリするところでしょう。配線がなくなれば、従業員が個々の席を持たず自由なスペースで働く「フリーアドレス」制の導入が可能です。固定したデスクにとらわれないため、業務の効率化が期待できます。

基本的にルーターは、有線接続できる数が限られます。そのため、スイッチやハブを使って接続台数を増やしますが、無線LANであれば、ルーターだけで多くのデバイスに接続可能です。

また、最近はデバイスの小型化が進み、LANケーブルを接続できないデバイスも少なくありません。パソコンだけでなく、スマホやタブレットも簡単にネットワークに接続できるのは、無線LANのメリットといえるでしょう。

＜デメリット＞
デメリットとしては、通信速度が有線LANに劣ること、さらにセキュリティ面の注意が必要という点です。

無線LANの通信速度は非常に高速化しています。有線LANのほうが速いケースが多く、接続の安定性も有線LANには劣りますが、無線LANの規格の中には、通信速度が最大6.9Gbpsのものもあります。

セキュリティ面も有線LANと比べた際、より意識しなければならない点です。無線LANは電波を使って通信を行うため、盗聴を防ぐ暗号化が欠かせません。また、有線LANであれば物理的に接続しなければならないため、誰がどんなデバイスで接続しているかを確認できますが、無線LANは接続デバイスの確認が難しいといえます。無線LANに対応したデバイスであれば、どんなデバイスでも接続可能であり、セキュリティ的には不安要素です。

とはいえ、無線LANが登場して久しい現在では、さまざまなセキュリティ対策が施され、通常利用する上でのセキュリティ上の不安は少なくなっています。次からは、このセキュリティ対策についてご紹介します。

社内に無線LANを導入するときのセキュリティ対策

無線LANを導入する際には、セキュリティ対策が必須です。ここでは、セキュリティ対策をしないことによって生じるリスクと、セキュリティ対策方法について解説します。

＜セキュリティ対策をしないリスク＞
無線LANでセキュリティ対策をしない場合、次の3つのリスクがあります。

1.通信内容を盗聴される
無線LANは電波によって通信を行います。電波を受信できるデバイスがあれば、暗号化されていない通信内容は、簡単に盗聴されます。

2.不正アクセスされ、情報漏えいにつながる
通信内容の中には、デバイスやWebサービスなどのログイン情報（ログインIDやパスワード）も含まれます。不正アクセスのリスクと併せて、情報漏えいのリスクも高まります。

3.通信回線を第三者に勝手に利用される
契約している通信回線を、第三者に勝手に利用される可能性もあります。同時接続可能台数や、処理できる通信量にも上限があるため、勝手に利用されるとネットワークに接続できなくなったり、通信速度が遅くなったりするリスクもあります。

＜無線LANのセキュリティ対策＞
無線LANのセキュリティを万全にするため、「WPA2（AES）の暗号化方式を使用する」「IEEE802.1x認証（EAP）などの認証を付加する」対策を取りましょう。

WPA2（AES）の暗号化方式は、無線LANの通信内容を暗号化するもので、現在最も強固な暗号化方式ともいわれています。AESは2000年に米国政府標準の暗号方式として採用されるほど強固な暗号規格となっています。

無線LANに接続するためのユーザー認証を付加することも、セキュリティ対策として有効です。IEEE802.1x認証は、無線LANを利用するクライアントがアクセスポイントに接続する際、ユーザー認証を付加する方式であり、認証プロトコルとしてEAPが利用されます。

EAPには複数の種類があり、電子証明書を使うEAP-TLSやID/パスワードで認証するEAP-FASTなどがあります。IEEE802.1x認証を行うには、認証サーバーを用意したり、認証コントローラが必要になったりしますが、強固なセキュリティを築けるため、企業の規模や運用方法に合わせて選択しましょう。

社内の無線LANを選ぶときのポイント

社内で無線LANを導入する際、どんな点に注意して選べばよいでしょうか。ここでは、選ぶときの3つのポイントを紹介します。

＜1：無線LANの通信規格＞
無線LANには複数の通信規格があり、規格ごとに特徴があります。

規格	通信速度（最大）	周波数帯	特徴
IEEE802.11b	11Mbps	2.4GHz	古い規格。現在ではほとんど利用されない
IEEE802.11g	54Mbps	2.4GHz	家庭用で利用されることが多い
IEEE802.11a	54Mbps	5GHz	家庭用で利用されることが多い
IEEE802.11n	600Mbps	2.4GHz/5GHz	現在主流の通信規格
IEEE802.11ac	6.9Gbps	5GHz	対応機器が増え、主流になりつつある規格
IEEE802.11ad	6.7Gbps	60GHz	高周波数帯を利用することで高速通信を実現する 次世代無線通信規格の1つ
IEEE802.11ax	9.6Gbps	2.4GHz/5GHz	11acを高速化させた規格であり、Wi-Fi6とも呼ばれる 高速次世代無線通信規格の1つ

無線LANの通信規格だけでもこれだけの種類があり、規格ごとに通信速度は大きく異なります。なお、記載速度は、あくまでも理論上の最大通信速度で、実効速度は理論通りではないのでご注意ください。

また、周波数帯による違いもあります。2.4GHz帯は対応機器が多く、障害物に強い特徴がありますが、電波干渉によって通信速度が遅くなる場合があります。5GHz帯は電波干渉が少なく、安定した通信を実現できますが、障害物に弱い特徴を持っています。

無線LANを選ぶ際には、通信速度や周波数帯の違いによる特徴を理解した上で、通信規格に対応するルーターやデバイスを選択しましょう。通信規格としては、11n以降に対応したものを推奨します。

＜2:同時接続台数＞

無線LANを実現するためのルーターを選ぶ際に、忘れてはならないポイントが「同時接続台数」です。ルーターごとに、一度に接続できる台数の上限が決まっています。社内で利用するデバイスの数に合わせて選択しましょう。

同時接続台数は、家庭用と法人用のルーターで、最も差が出る部分でもあるため、しっかりと確認する必要があります。

＜3:メッシュネットワークへの対応＞

最近の無線LANには、メッシュネットワークに対応したものがあり、環境によっては選ぶ際のポイントにするとよいでしょう。

メッシュネットワークとは、通信ネットワークの構成の1つです。通信機能のある端末が相互に接続する、網目状に張り巡らされたネットワークのことです。無線LANでは、メッシュ型無線LANやメッシュWi-Fiと呼ばれます。

従来の無線LANシステムと異なり、ルーターに集中するネットワーク負荷を分散でき、安定したネットワーク接続が実現可能です。広い部屋などでも、網目状にネットワークが張り巡らされ、電波がつながりづらい場所をなくせます。

無線LANの接続範囲の拡張も簡単に行えるため、オフィスへの導入に向いています。無線LANを導入する際に、メッシュネットワークの対応有無もポイントとして確認してみてください。

通信規格やセキュリティ対策を意識して、無線LANを導入しよう

社内に無線LANを導入すれば多くのメリットがあります。導入する際は、通信規格や接続台数と併せて、しっかりセキュリティ対策を行わなければなりません。

とはいえ、無線LANには専門用語も多く、セキュリティ対策が難しいと感じる方もいるでしょう。そこで、NTT西日本では、ラクラク設置でカンタン導入ができる無線LANサービスを提供しています。「スマート光ビジネスWi-Fi」は、「簡単」「高速」「安心」がキーワードで、充実のセキュリティ対策機能を搭載します。

IEEE802.11ac
に対応し、同時接続台数は50台まで対応するため、社内に導入する無線LANとして適したサービスです。導入をお考えの際は、ぜひご相談ください。

※掲載している情報は、記事執筆時点のものです