IT化スモールスタート解説（第1回）

Wi-Fiの仕組み＆社内にWi-Fiを導入する方法

2020.03.18

今や誰もが当たり前のように利用するWi-Fiですが、その仕組みや安全に使うためのセキュリティ対策はご存じでしょうか。Wi-Fiは手軽に利用できるため、あまり気にしない方も多いかもしれませんが、普段使うものだからこそしっかりと身に付けておきたい知識であるといえます。

今回は、Wi-Fiの概要から、導入するメリット、セキュリティ対策、導入方法について解説します。

Wi-Fiとは何か

はじめに、Wi-Fiの概要についておさらいしましょう。

Wi-Fiは、パソコンやスマホなどを、LANケーブルを使用せず、ネットワークに接続する技術です。より厳密にいえば、ネットワークへの無線接続の規格となります。

ネットワークへの無線接続が登場した頃は、製品ごとに共通した規格が定まっておらず、異なる製品間では通信が行えませんでした。それを解決するために定められた規格がIEEE802.11であり、その規格に準拠したものがWi-Fiです。現在では、市販されるほとんどの製品がWi-Fiに対応しています。

Wi-Fiによる無線接続は、親機となるルーターと、パソコンやスマホなどの子機の間で電波を飛ばして接続する仕組みです。Wi-Fiを使うことでネットワークへの無線接続が可能となるため、複数台の端末を接続したり、距離があって物理的に接続が難しかったりしても、接続が可能となりました。

社内にWi-Fiを導入するメリット

Wi-Fiを社内に導入する最大のメリットは、物理配線が不要になることでしょう。物理配線が不要になる利点は、単に煩わしいコード類がなくなるだけではありません。

以下の2つのようなメリットを社内にもたらします。

1.社内のレイアウト変更がしやすくなる
　物理配線が不要となれば、たとえパソコンが数百台あったとしても、配線を考慮したり変更したりする必要がないため、社内のレイアウト変更が行いやすくなります。

2.端末をネットワークにつなげたまま移動ができる
　物理配線がないので、端末をネットワークにつなげたまま移動ができます。例えば、作業をするオフィスから会議室へ端末を持って移動する際、有線接続の場合は一度ネットワークから切断しなければなりません。Wi-Fiを用いれば、ネットワークへの再接続の手間を減らせ、ネットワークのシームレスな環境が構築できます。

上記のほか、スマホなどのモバイルデバイスを社内ネットワークに接続できるようになるのも、Wi-Fiを社内に導入するメリットです。

社内のWi-Fiを安全に使うためのセキュリティ対策

ここまでWi-Fiのメリットを紹介しましたが、一方でリスクを抱えていることも理解する必要があります。

＜Wi-Fi導入のリスクとは＞
Wi-Fiを導入することで新たに発生するリスクは、有線接続とは異なるセキュリティ対策が必要になる点です。

Wi-Fiは、接続時にSSIDとパスワードを利用します。このSSIDとパスワードは、知っていれば誰でも簡単にネットワークへ接続できます。つまり有線LANよりも、外部から侵入されやすいといえます。外部から社内ネットワークに侵入されると、機密情報や個人情報などの漏えいにつながる可能性があるため、Wi-Fiのセキュリティ対策は常に万全にしておく必要があります。

＜Wi-Fiのセキュリティ対策方法＞
Wi-Fiを利用する際のセキュリティ対策方法について見ていきましょう。

1.セキュリティが強固な「WPA-AES」「WPA2-AES」を利用する
Wi-Fi接続時は、外部からの盗聴を防ぐ目的で暗号化を行います。その際に利用する暗号方式が「WPA-AES」や「WPA2-AES」です。Wi-Fiは電波通信のため、内容が暗号化されていないと簡単に盗聴できます。セキュリティが強固な暗号方式を利用することが大切です。

2.SSIDステルス機能を使う
ルーターのセキュリティ機能の1つである「SSIDステルス機能」の利用も有効です。通常ルーターは、周囲に自身のネットワーク名（SSID）を知らせるための電波を飛ばしていますが、この機能を使えば、その電波を停止できます。SSIDを隠し、第三者からは分かりづらくすることで、外部から社内ネットワークへの不正アクセスが困難になります。

3.安易なパスワードを使用しない
セキュリティ強度を高めるためには、SSIDと一緒に利用するパスワードも安易なものを使用しないようにしましょう。パスワードは数字・大文字・小文字・記号などを織り交ぜ、8文字以上で意味のない文字列の設定をお勧めします。

4.ルーターのバージョンを常に最新にする
ルーターのバージョンを常に最新にすることもセキュリティ対策になります。古いバージョンを使用していると、ソフトウエアの脆弱性を狙った攻撃を受ける可能性があるからです。定期的なアップデートで、常に最新状態にすることを意識しましょう。

社内へWi-Fiを導入する方法

次に、社内へWi-Fiを導入する場合の具体的な手順やポイントを解説します。

＜Wi-Fiの導入手順＞
導入手順は、次の通りです。

1.社内環境を調査し、必要な環境要件を出す
1つのルーターに何台の端末を接続するのか、オフィスの広さから何台のルーターが必要になるか、といった情報を調査してまとめます。

2.利用方針を決め、システムを設計する
Wi-Fiの導入は、1つのネットワークシステムを導入することと同義です。そのため、社内のみにするのか、訪問者も許可するのかなど、接続許可の範囲や利用方針を定めて設計します。

3.運用管理方法をマニュアル化する
導入前に運用管理方法をマニュアル化することも大切です。パスワードの管理方法やルーターのバージョンアップ方法など、Wi-Fi環境を継続利用するための運用管理方法をまとめておきます。事前にマニュアル化しておくと、Wi-Fi導入後もスムーズに運用・管理ができるでしょう。

4.Wi-Fiルーターの設置、アクセスポイントの調整
ここまでの手順が完了したら、親機となるWi-Fiルーターを用意し、設置しましょう。現在ではほとんどのルーターがWi-Fiに対応していますが、中には有線接続のみに対応したルーターもあるため注意が必要です。実際に設置した際、パーテーションなどの影響で電波が弱まる可能性もあるため、アクセスポイントとなるWi-Fiルーターを調整します。

＜Wi-Fi導入時のポイント＞
Wi-Fi導入時は、Wi-Fiルーターの選定がポイントです。Wi-Fiルーターと一言でいっても、その種類は非常に多く、オフィスの環境によって最適なものは異なります。

Wi-Fiルーターは、家庭向けと法人向け（業務用）に分けられます。大きな違いは「同時接続数」です。同時接続数は、一度に接続できる端末数のことで、家庭向けのものは接続数が多くありません。オフィスの規模によっても変わりますが、基本的には法人向けのWi-Fiルーターをお勧めします。

また、Wi-Fiには複数の規格があり、規格によって通信速度や周波数帯が異なります。それぞれの規格について、以下の表にまとめました。

規格	通信速度（最大）	周波数帯
IEEE802.11b	11Mbps	2.4GHz
IEEE802.11g	54Mbps	2.4GHz
IEEE802.11a	54Mbps	5GHz
IEEE802.11n	600Mbps	2.4GHz/5GHz
IEEE802.11ac	6.9Gbps	5GHz
IEEE802.11ad	6.7Gbps	60GHz

下に行くほど新しい規格で、通信速度に大きな違いがあります。古いWi-Fiルーターは新しい規格に対応していません。ルーター選びの際は気を付けてください。

社内ネットワークにWi-Fiを導入しよう

今やWi-Fiによるネットワーク接続は広く浸透しています。公共の場のみならず、一般家庭でも日常的にWi-Fiを利用する機会は多いでしょう。

便利で効率も良いWi-Fiを、社内に導入するメリットは非常に大きいものがあります。それと同時に、導入時のリスクも理解しなければなりません。Wi-Fi導入時には、セキュリティ対策が必ず必要となります。

NTT西日本では、ラクラク設置でカンタン導入ができるWi-Fi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」が特長のWi-Fiで、充実のセキュリティ対策機能を搭載。社内にWi-Fiを導入したいとお考えであれば、ぜひお問い合わせください。

※掲載している情報は、記事執筆時点のものです