ビジネスWi-Fiで会社改造（第10回）

安心して使ってもらうーセキュリティ強化作戦

2022.07.20

柔軟なオフィスレイアウトを可能にし、テレワークではシームレスな働き方を実現、お客さまにも利便性を提供できるビジネスWi-Fi。しかし、ワイヤレス接続であるためセキュリティ上のリスクも存在する。ビジネスWi-Fiだからこそ留意しなければならないセキュリティリスクはどこにあり、どんな対策が必要なのか。今回は、ビジネスWi-Fiのメリットを安全・安心に享受するために、Wi-Fiにおけるセキュリティ上の脅威とその回避策を解説する。

セキュリティ強化の第一歩は最新の「WPA3」の導入

本連載でこれまで取り上げてきたように多くのメリットがあるビジネスWi-Fiだが、ワイヤレスであるがゆえに、有線LANに比べてセキュリティ面での脆弱性があるのも事実だ。ビジネスWi-Fiだからこそ考えられるセキュリティリスクは大きく2つある。データを盗聴されるリスクと、外部から侵入される不正アクセスのリスクだ。

盗聴されるリスクへの対策の第一歩は暗号化だ。連載の第3回でも解説したように、Wi-Fi環境におけるセキュリティは「認証方式」と「暗号化方式」の組み合わせによって確保される。

一定時間ごとに暗号鍵が自動変更される認証方式「WPA」の最新の暗号化規格が2018年6月に発表された「WPA3」だ。パスワードが漏えいしても通信内容を暗号化して解読を防ぐ機能や、誤ったパスワードでのログインが繰り返されるとログインをブロックする機能を備える。

Wi-Fi6からこのWPA3に対応しており、最新機器の多くで採用され、最も高いレベルのセキュリティ強度を実現する。それ以前のWi-Fiが対応している「WPA2」もそれなりの強度を有しているものの、脆弱性も指摘されている。より安心を手に入れたいならWPA3に対応した機器の導入をお勧めする。

もう1つのセキュリティリスクである不正アクセスへの対策は、ユーザー認証の強化が有効だ。通常、Wi-Fiにアクセスする際には、接続したいアクセスポイントのSSIDを指定して、Wi-Fiルーターのパスワードを入力する。このパスワードはSSIDごとに共通であり、多くの人が同じパスワードでビジネスWi-Fiを利用している。

この状態でパスワードが漏えいすると誰でもアクセス可能になり、ビジネスWi-Fiのセキュリティ対策としては十分とはいえない。そこで検討したいのが、社員ごとにIDとパスワードを発行して個別に認証を行うID/パスワード認証の導入だ。

万が一社員の誰かのパスワードが流出した場合には、該当するアカウントだけを利用停止にすれば被害を最小限に抑えられる。ただし、この方法ではIDとパスワードさえ分かれば、誰でもアクセスできることに変わりはない。例えば端末を紛失したり、盗難にあったりすれば、その端末から不正にアクセスされる可能性がある。

セキュリティ向上に社員教育は欠かせない… 続きを読む