

公衆無線LANを安全に 利用するために確認すべきこと

事業所内で無線LANを使うときと公衆無線LANを使うときと
では注意点が異なります！！

家庭内や事業所内など、特定の人しか利用しない環境であれば、無線LANの暗号方式に「WPA2-PSK」を利用しても危険性はほとんどありません。
しかし、不特定多数の人が利用する公衆無線LANの暗号方式が、「WPA2-PSK」であるときは盗聴などの危険性があります。



どうして同じ暗号方式なのに 危険性が変わるのか？

暗号方式にある「PSK」とは「Pre-Shared Key」の略であり、事前に暗号キーを共有するということを示しています。そしてこの暗号キーは、固定されたものであるため、全員で同じ暗号キーを利用しているのです。

そのため、家庭内や事業所内など内部の人しか利用しない環境であれば危険性はほとんどなかったのですが、

公衆無線LANなど不特定多数の者が利用する環境

だと、その中に悪意を持った者がいる可能性もあり、通信を盗聴される危険性ができます。

公衆無線LANを安全に利用するための確認事項

公衆無線LANを安全に利用するためには、他人と同じ暗号キーを利用しない（暗号キーを他人と共有しない）ことです。

具体的には、無線LANの接続を行うときの設定のセキュリティ項目などに

「WPA2-EAP」、「WPA2-エンタープライズ」、
「IEEE802.1x」、「SIM認証」

などの用語が含まれたものを利用するという事です。

これらは、利用者一人ひとり個別の暗号キーを用いて通信しているため、他人に暗号キーを知られることはありません。

右図の無線LANに接続した場合、利用者個別の情報が入っているSIMカードを認証に用い、個別の暗号キーで無線LAN通信を行います。

