ネットワーク/トランジット

ITマネジメント（内部統制）

意外と無防備!? な無線LAN。セキュリティの“抜け穴”を塞ぐには？

Point

- セキュリティ上の“抜け道”となり得る無線LAN
- 無線LANで使われる2つの認証方式の違いを理解する
- 負担を抑えて導入できるクラウド型無線LANソリューション

場所を問わずにネットワークに接続できる無線LANは便利な技術ですが、セキュリティ面での注意も必要です。家庭利用とは異なる、企業における無線LANセキュリティのポイントを解説していきます。

退職者が無線LANを通じてシステムに不正アクセス！

ある流通業で従業員が退職した後、なぜか競合会社が同じ商品を自社よりも安く販売するようになり、顧客が競合会社に流れるようになった。よくよく調べて見たところ、実は退職した従業員の転職先がその競合会社で、元の職場の無線LANを勝手に利用し、販売管理システムに不正にアクセスしていた……。

このようなトラブルは、決して絵空事ではありません。実際、在職中に使っていたアカウントを利用し、元の企業のシステムに不正アクセスして機密情報を盗むといった事件は発生しています。このような観点で先の事例を見た場合、ポイントとなるのは無線LANです。

オフィスのフリーアドレス化や場所を問わずにインターネットが利用できるメリット、あるいはスマートフォンやタブレット端末といったモバイルデバイスのビジネス利用が進んだことから、多くのオフィスで無線LANは積極的に導入されています。有線LANと異なり、無防備な無線LANは、電波が届く範囲であれば第三者に不正接続されてしまい、社内LANにも簡単に侵入されてしまいます。

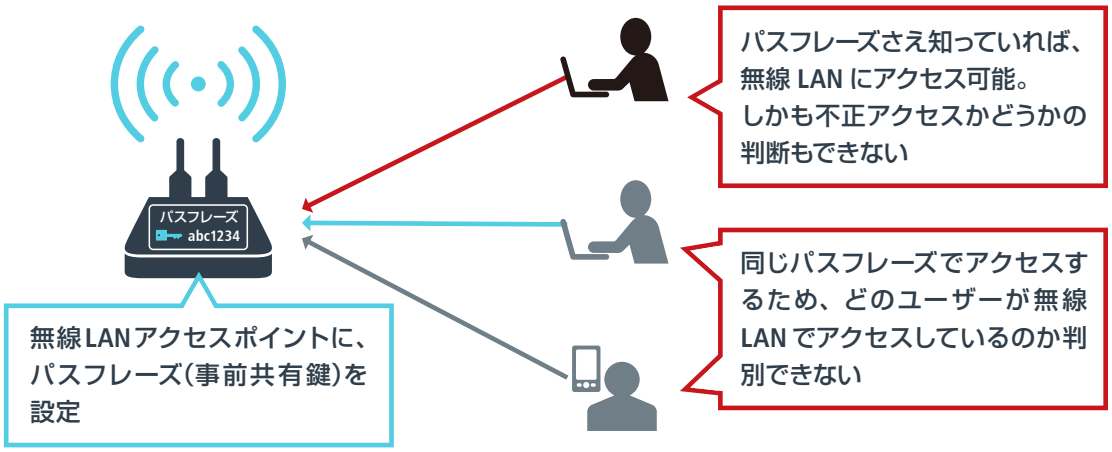
パソコンや各種モバイルデバイスを無線LANに接続する際に利用される無線LANアクセスポイントには、通信内容の暗号化や認証によるアクセス制限を実施するための機能が組み込まれています。これらを利用することで、通信内容の傍受や不正利用、アクセスポイントのなりすましなどの危険性を軽減します。ただ、ここで注意しなければならないのは、ユーザーのアクセス制限機能です。

無線LANにおける2つの認証方式の違いを正しく理解する

無線LANにおけるユーザー制限のための機能は、大きくわけて2つの方法が存在します。PSK(Pre-Shared Key、事前共有鍵)と呼ばれる共通のパスフレーズで認証する方式で、アクセスを許可する方法、そしてユーザーやデバイスごとに個別に認証する方法です。

手軽なのは前者で、パスフレーズを事前に設定し、利用者にそれを通知するだけで済みます。設定が容易であることから、個人や家庭向けの小規模な無線LANで広く普及しています。ただ、この方式ではパスフレーズさえ知っていれば、誰でもアクセスできるほか、すべてのユーザーが同じパスフレーズを使うため、誰がアクセスしているのかを把握することもできません。冒頭の事例に沿って言えば、退職者がパスフレーズを覚えていれば、簡単に以前の職場のネットワークにアクセスできてしまいます。

パスフレーズによる無線LAN利用制限



一方、ユーザーおよびデバイスごとに個別に認証を行う方法は、誰が(あるいはどのデバイスが)無線LANを利用しているのかを把握できます。アカウントの制御も個別に行えるため、退職者のアカウントを削除して、以降のアクセスを遮断することも可能です。しかしこの方法で無線LANを利用するには認証用のサーバーを構築しなければなりません。この負担を避けるために、企業での無線LAN利用であっても、パスフレーズによるアクセス制御で運用しているケースが少なくないようです。しかしそこには大きなリスクが伴うことを認識しなければなりません。

認証サーバーでユーザーやデバイスごとに無線LANを利用制限

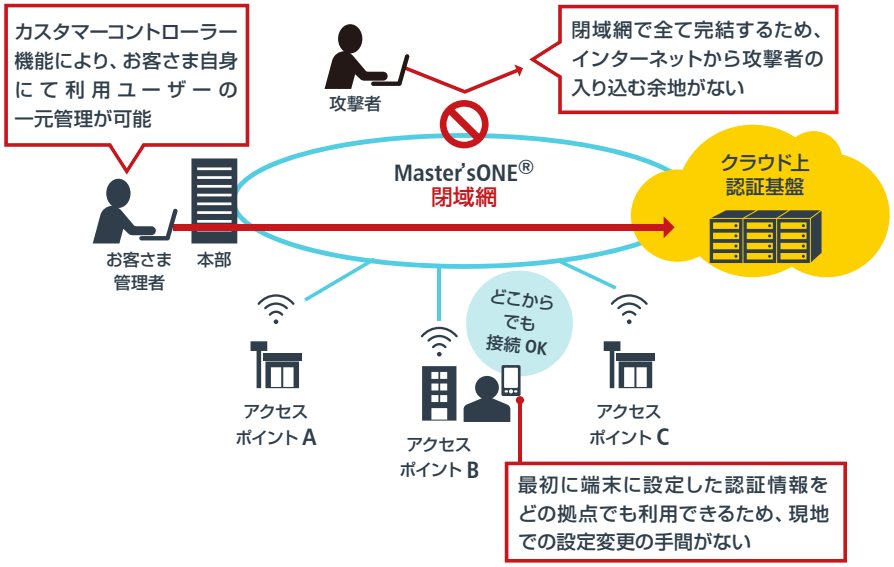
クラウド型無線LANソリューションが広まるワケ

このような課題を解決するために、昨今広まりつつあるのがクラウド型の無線LANソリューションで、具体的なサービスとしては、NTTコミュニケーションズの「Arcstar Universal One クラウドWi-Fi」やNTTPCコミュニケーションズの「Master'sONE® 無線LANサービス」です。

両サービスとも、複数拠点の無線LANアクセスポイントと、クラウド上の認証サーバーをVPNサービスで接続することが可能です。各拠点にアクセスポイントを設置していますが、その認証基盤はクラウド上で提供されているため、拠点ごとに認証サーバーを構築することなく、ユーザーごとに認証を設定することが可能になります。これにより、誰がいつ無線LANを利用しているのかを詳細に把握できるようになります。

また、どの拠点でも同じように無線LANが使えることも利点で、たとえば従業員が別の拠点に行って作業するといったケースでも、無線LANの設定を切り替えることなく、いつもと同じように無線LANにつなげて仕事ができるため、ユーザーの利便性も向上します。

閉域網で利用可能な無線LANサービスイメージ



拠点の多い企業では、無線LAN環境の構築を拠点ごとに任せているケースがまだまだ多いようです。その際、家電量販店などで販売されている、個人利用を想定した無線LANアクセスポイントを購入し、簡単なパスフレーズによる運用をしていた場合、冒頭のシナリオのような、情報漏えいなどのリスクが十分に考えられます。さらに、誰が無線LANを使っているのかを把握できなければ、情報漏えい時の原因究明すら困難になります。

このような事態が発生する前に、あらためて自社における無線LANの利用状況を把握し、企業での利用に適した環境に移行することをぜひご検討ください。

関連サービス

Arcstar Universal One クラウドWi-Fi

Arcstar Universal Oneでは、アクセスポイントのレンタルから認証基盤まで、セキュアなWi-Fi環境に必要なすべてをNTTコミュニケーションズが一元的に提供します。さらにアクセスポイント設置やLAN配線工事などを行い、ネットワークと合わせて24時間365日保守対応するプランも提供することで、お客さまの負担を軽減し最適なWi-Fi環境の構築を実現します。

Master'sONE® 無線LANサービス

Master'sONE®の『無線LANサービス』は、認証基盤をクラウド型で提供するため、VPN網に接続された全国のオフィスや店舗に、高セキュリティな無線LAN環境を1台の無線LANアクセスポイントから簡単に導入する事を可能にします。管理コンソールにて端末や証明書の管理が可能なため、運用負担も軽減されます。また、弊社にてVPNやリモートアクセス、クラウドを始めとする弊社各種サービスと一元的に運用・保守いたしますので、安心してご利用になれます。