中小企業の

セキュリティー対策

―20―

無線LANに潜むリスク

第三者が不正利用

ノートパソコンやタブレット、スマートフォンなどのモバイル端末の普及に伴い、中小企業でも無線LANの導入が進んでいる。無線LANを導入することで、会議室や工場などに端末を持ち込んでの業務実施や従業員の異動に伴う配線工事が不要になるなどメリットがある半面、無線LANならではのリスクもあり、注意が必要だ。

例えば、無線LANは電波が届く範囲であれば壁や障害物を越えて通信が可能なため、第三者に接続されて悪用されてしまう可能性がある。無線LANのパスワードは推測されにくく、ブルートフォース攻撃（パスワード総当たり攻撃）の対策として20文字以上の長さに設定することなどが必要となる。また、接続を認めた端末以外が接続できないようにMACアドレス（端末固有のアドレス）による フィルタリングを行うことも有効だ。しかし、MACアドレスは偽装することができるため、可能であれば「IEEE 802・1X」などのより強固な認証を導入したい。

また、通信内容を読み取られないために通信の暗号化設定を行なう。WEPは短時間で読解される方法が発見されているため、現時点ではWPA2が推奨される。しかし、昨年10月にWPA2の脆弱（ぜいじゃく）性が報告されており、今年6月にセキュリティー機能を改善したWPA3の規格が公表されている。今後、WPA3に対応したルーターやアクセスポイント、端末が各メーカーから提供されるため、新たに無線LANを導入したり、入れ替えたりする場合は、改めて動向を確認してほしい。

通信内容を盗聴

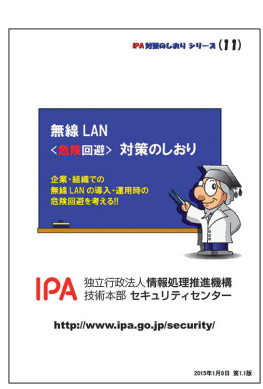
外出先での無線LANの利用にも注意が必要である。空港や公共施設、カフェ、ホテルなどさまざまな場所で公衆向け無線LANの提供が増えているが、パスワードを設定していないアクセスポイントの中には悪意ある第三者が設置して利用者の通信内容を盗聴している場合がある。信頼がおけるアクセスポイントだけ接続するようにしたい。また、公衆向け無線LANの利用に当たっては通信内容を読み取られないように暗号化機能の利用が必須だ。

しかし、信頼のおけるアクセスポイントであっても、通信の暗号化機能を利用していても、SSID（アクセスポイントの識別名）とパスワードが公開されている場合、盗聴される可能性がある。外出先での業務が多いのであれば、VPN（仮想専用線）やモバイルルーターなどを利用するようにしたい。加えて、不特定多数の利用者が同一のネットワーク上に接続する場合、設定の不備により、不正アクセスを受ける可能性がある。ネットワークを通じたファイルやフォルダの共有設定は解除しておく必要があるだろう。

これら無線LANの利用に当たっての危険性や社内ルールは、従業員教育を行なうことが望まれる。また、万が一の場合に迅速に対応できるようにするため、ルーターなどのログを取得しておくことが望まれる。

独立行政法人情報処理推進機構（IPA）では企業での無線LANの導入・運用時の危険回避を考えるための資料として「無線LAN〈危険回避〉対策のしおり」を公開している。詳しくはウェブサイト（https://www.ipa.go.jp/security/antivirus/shiori.html）を確認してほしい。

（独立行政法人情報処理推進機構・江島将和）



無線LAN〈危険回避〉対策のしおり