無線LANの危うさと、今日からできるセキュリティ対策

無線LANはケーブルを使用せず、電波で端末（パソコン等）を接続する方式のネットワークです。端末の設置場所が固定されないため、現在では多くの場所で活用されています。しかしその利便さの一方で、セキュリティ面に不安なところがあり、適切な設定をして利用しないと盗聴やパソコンの乗っ取りにあう可能性もあります。そこで今回は無線LAN利用の基礎知識と、今日からできるセキュリティ対策についてご紹介します。

1 無線LANの長所と短所

長所

- ケーブルを施設する必要がないため、端末の設置場所を固定しなくて良い。
- 駅やホテルのラウンジなどのアクセスポイントを利用すれば、出先でも手軽にインターネットを利用できる。

短所

- 電波の伝送範囲を制限できないため、盗聴の危険がある。
- 電波の状態により通信速度が低下したり不安定になることがある。

2 無線LANにとっての脅威とその対策

無線LAN環境は、電波による通信のためセキュリティに対する脅威が有線LANよりも増すことを忘れてはいけません。無線LANにおける一般的な脅威は以下のとおりです。(図1)

- 盗聴
  不正に端末の電波を傍受し、内容を盗み読むこと
- 不正アクセス
  許可されていない端末がアクセスポイントに接続し、その先のネットワークに侵入すること

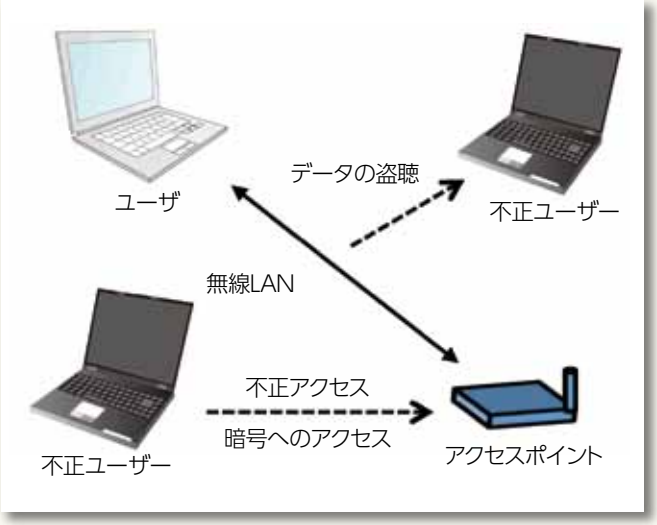

図1 盗聴と不正アクセス

盗聴に対する対策としては、設置者のはっきりしないアクセスポイントに接続しないこと、また不正アクセスを防ぐには、ユーザー認証や接続の制限を行うことです。

そして不正アクセスを察知するには、通信監視ソフト等を使っての通信ログ（履歴）の定期的なチェック等が有効です。

3 今日からできるセキュリティ対策

今や様々なセキュリティ対策ソフトや対策手法が存在しますが、比較的簡単にできるセキュリティ対策を2つご紹介します。

1つ目は、インターネットを利用しない時には無線LANを切断することです。「そんなことで?」とお思いになるかもしれませんが、実は不正アクセス対策としては有効な手段です。

不正ユーザーが標的とするパソコンに侵入するには、まずそのパソコンの動作状況を観察し、長時間使われていない時を狙って対象のパソコンを操作することが多いのです。これを防ぐためには、インターネットを使わないときは、ネットへの接続を一時的にでも切断すること（図2）が、セキュリティ対策として有効になります。

図2
インターネットを利用しないときは、無線LANをこまめに切断する癖を付ける。
切断するには、通知領域の無線LANアイコンをクリック①。
切断ボタンをクリック②

2つ目は、インターネットに接続する端末は、中身を見られる可能性があるという認識を持ち、企業情報や個人情報など重要なデータの入ったパソコンをインターネットに接続しないことです。

公衆無線LANを利用する場合、パソコンやタブレット等の端末は、同じネットワークに同居することになります。その状況で、ご自身のパソコンのファイル共有などを許可していると、第三者にファイルの中身を見られてしまいます。

これを防ぐためには、公衆無線LAN等に接続するパソコンやタブレットには絶対に重要なデータを入れておかないことです。理想をいえばインターネット用とデータ保存用のパソコンを別々に使い分けることですが、1台しか使えない場合は重要なデータは外付けハードディスクに保存して、こまめに抜き差しすることで同様の効果を得られます（外付けハードディスクを紛失したりすると本末転倒ですが）。

セキュリティ対策としてこれをしたから大丈夫というものはありません。そのため、会社など複数人でLANを利用する環境では、利用者一人ひとりがセキュリティ意識を高くもつことが必要となっています。

お問い合わせ先
京都府中小企業技術センター 企画連携課 企画・情報担当　TEL：075-315-8635　FAX：075-315-9497　E-mail：kikaku@mtc.pref.kyoto.lg.jp