動かしながら分かる！

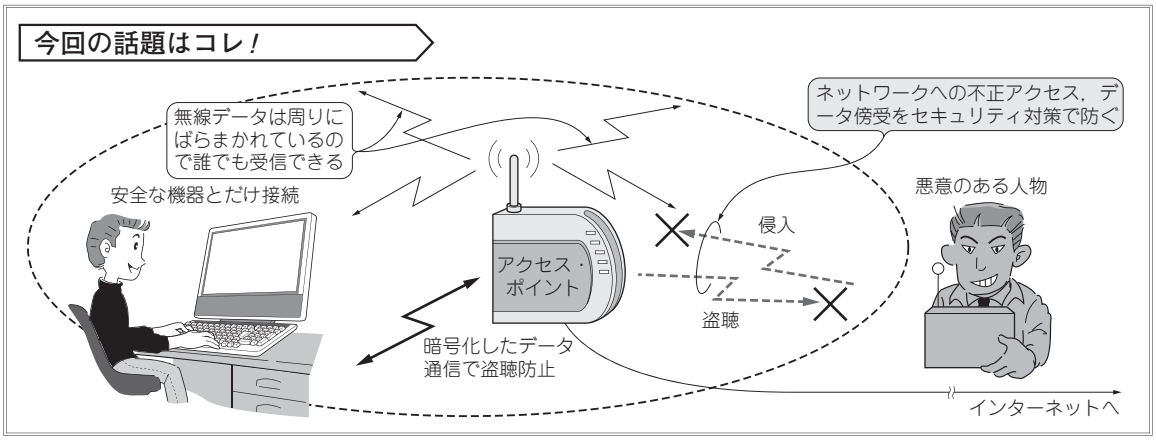
いつでもどこでも世界と簡単接続

今どきモジュールで Wi-Fi/無線 LAN 超入門

第3回 データの盗聴や侵入を防ぐセキュリティのしくみ

安全な接続先であることを見定めて暗号で通信する

西山 高浩
Takahiro Nishiyama



無線LANは電波でデータをやり取りするので，通信データは電波の届く範囲にばらまかれています．この電波は誰でも受信できるので，放っておくと「侵入（ネットワークへの不正アクセス）」と「盗聴（データ傍受）」という脅威にさらされることになります．よって「侵入」を防ぐ「認証」，「盗聴」を防ぐ「暗号化」というセキュリティ対策が規格で定められています．

定められているセキュリティ対策の規格の組み合わせは複数ありますが，既に破られているものもあります．それぞれのセキュリティ対策についてよく知っておく必要があります．

セキュリティがかかるまで

無線LANのネットワークを構築するアクセス・ポイント（以降，AP）と，無線LANに接続する装置ステーション（以降，STA）が，接続を確立し，データのやり取りを始めるまでの流れを見てみます．

図3-1に示すように，大きく四つのステップに分類でき，それぞれを人が家を訪ねるようすに例えると次のようになります．

①スキャン
訪問相手の家を探します．

②認証
訪問相手の家のインターホンを押して，お互いを認識します．

③アソシエーション
玄関から入ります．

④データ・フレーム送受信
会話を始めます．お互いにしかわからない暗号を使って会話します．

②認証のステップで，侵入を防ぐ仕組みが使われています．④データ・フレーム送受信のステップで，盗聴を防ぐ仕組みが使われています．

それぞれのステップについて，詳細に見ていきましょう．無線LANモジュールを使うときに，セキュリティで設定すべき暗号化の項目の意味がわかります．

① スキャン～ネットワークの検出～

無線LANネットワークに接続しようとするSTAは，まず接続可能なAPを探します．探索方法には2通りあります．接続までの時間と，STAの消費電力とのトレードオフにより探索方法を選択することになります．

▶アクティブ・スキャン…ステーションから積極的にアクセス・ポイントに呼び掛ける

STAはチャネル（使用する周波数）を変えながらプローブ要求フレーム（Probe request）を出力し，APは

● 連載予定
第1回：無線LAN装置がインターネットと結ばれるまで
第2回：接続に必要なハードウェアとその役割