Q フリーWi-Fiを安全に使うには？

出かけた先で、パスワードが設定されていないフリーWi-Fiを使ってパソコンをインターネットにつなげたいと思うことがあります。フリーWi-Fiを安全に使うコツなどはありますか。

A フリーWi-Fiを利用するなら、いくつか注意したい点があります。まずは一般的なWebサイトの表示などにとどめること。個人的な情報を扱う際にはサーバーとの通信が暗号化されている状態か確認すること（図1）。通信が暗号化されない電子メールの送受信は避けること――といった点です。

一般的なフリーWi-Fiでは無線の通信が暗号化されていないため、ほかのパソコンで同じ電波を受信し、分析用のソフトで通信内容を読み取ることが可能です。利用するソフトやサービスが通信を暗号化するように作られていないと、送受信した電子メールの内容や、入力したパスワードなどがそのまま読み取られてしまう危険があるのです。

個人向けのVPNソフトを使うのが一つの対策です（図2）。専用サーバー経由で通信することでパソコンからの通信全体を暗号化するため、セキュリティ対策になります。

フリーWi-Fiでなく、単に通信が暗号化されていないだけの個人や企業のWi-Fiに接続しないよう注意することも大切です。周囲にサービスについて掲示がないか探す、スマートフォンで地域や施設、店舗の情報を検索するなどして、今いる場所で使えるフリーWi-Fiの名前を調べるとよいでしょう。

Windows 10の設定によっては、接続先の一覧に「Wi-Fiセンサー」という表示が出ることがあります（図3）。これは、ほかのユーザーも同じ名前の接続先を利用していて、「フリーWi-Fiのサービスである可能性が高い」とマイクロソフトが判断した接続先に表示されます。ただ、「Wi-Fiセンサー」の表示が有効だと、マイクロソフトの推奨するフリーWi-Fiに自動で接続されてしまうことがあります。不安なら設定を無効にしておきましょう（図4）。

（斎藤 幾郎＝ライター）

フリーWi-Fiのセキュリティを高めるには

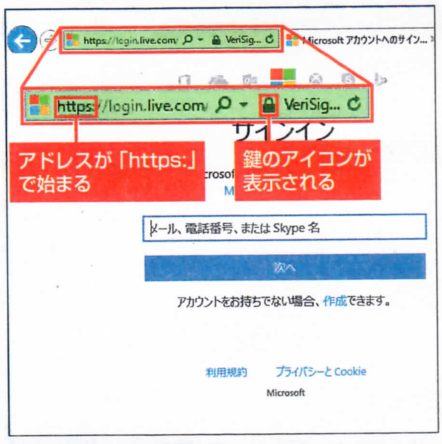

図1 Internet ExplorerなどのWebブラウザーでは、アドレスが「https:」で始まり、鍵マークが付くなどすれば、通信が暗号化されている

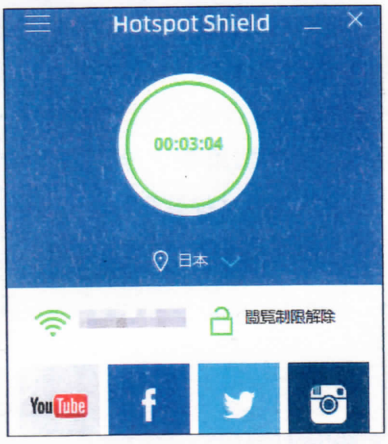

図2 VPNソフトの「Hotspot Shield」。ソースネクストが「Wi-Fiセキュリティ」の商品名で1年版を販売。機能制限のある無料版もある

図3 Wi-Fiの接続先選択で、暗号化されていないことを示す盾のマークや「オープン」の語句に加え、「Wi-Fiセンサー」の表示もあると、フリーWi-Fiである可能性が高い

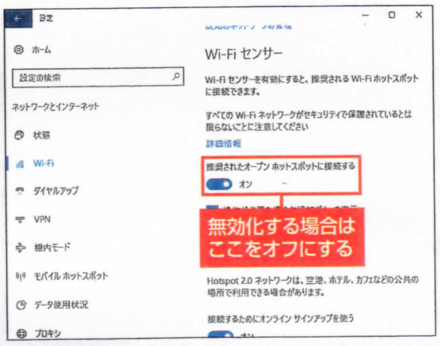

図4 「設定」アプリの「ネットワークとインターネット」を開いて「Wi-Fi」を選び、「推奨されたオープンホットスポットに接続する」のスイッチで機能のオン／オフを切り替える