

無線LANを安心して利用するために

～ 無線LANを利用するときの情報セキュリティ対策 ～

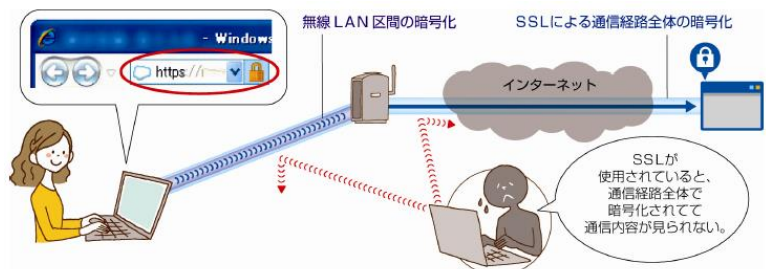
1 大事な情報は、SSL¹でやりとり

インターネットは一般に通信内容を盗み見られる危険性があるものですが、無線LAN利用時には、その危険性が高まります。

特に、公共の場で無線LANを利用するときには、他人に通信を傍受されたり、偽のアクセスポイントに接続させられたりする危険性が高まります。

公共の場で無線LANを利用するときには、大事な情報はなるべくやりとりしないようにしましょう。どうしても大事な情報を公共の場でやりとりしたい場合には、SSLによる暗号化がされていることを確認してから行いましょう。

SSLが利用されていないときには、通信内容が盗み見られる危険性を理解した上で、大事な情報をやりとりするかどうか判断してください。



2 公共の場では、ファイル共有機能²を解除

公共の場で無線LANを利用する際に、ファイルの共有機能が有効になっていると、パソコンのファイルが読み取られたり、ウイルスなどの不正なファイルを送り込まれたりすることがあります。

そのため、ファイル共有機能の利用は、家庭内や職場のLANに接続したときに限るようにして、公共の場での無線LAN接続時には解除しましょう。

なお、スマートフォンは、OSによるファイル共有機能を有していませんが、アプリケーションによるファイル共有が可能です。公共の場での無線LAN接続時には、ファイル共有アプリケーションを終了しましょう。

3 知らないアクセスポイントには接続しない

無線LANのアクセスポイントには、情報セキュリティ対策が取られておらず、誰でも利用できる状態になっているものがあります。これらのアクセスポイントの中には、通信内容を盗み見ることなどを目的に悪意を持って設置されたものが含まれている可能性があります。

そのため、誰でも利用できる状態になっているからといって、知らないアクセスポイントには接続しないことが大切です。

4 公衆無線LANサービスのログイン画面に電子証明書エラーが表示されたら接続しない

SSLが使われていない場合や、SSLが使われていても電子証明書のエラーが表示される場合には、偽のアクセスポイントに接続している危険性があります。

公衆無線LANサービスにログイン画面が表示されるときには、SSLという通信方法が使われていることを確認しましょう。

電子証明書のエラーが表示される場合には、IDとパスワードは入力せずに、契約している公衆無線LANサービス事業者等に問い合わせましょう。

5 接続しているアクセスポイントを確認

無線LANでは、アクセスポイントに自動的に接続できるよう設定することができるため、暗号化等の十分な情報セキュリティ対策が取られていないアクセスポイントや悪意を持って設置されたアクセスポイントなど、望まないアクセスポイントに意図せず接続してしまい、通信内容が盗み見られるなどの危険性があります。

そのため、無線LANを利用しているときには、どのアクセスポイントに接続しているか確認しましょう。思ってもいないアクセスポイントに接続していないか、確認することが大切です。

これまで利用したことがないアクセスポイントには、自動的に接続しないよう設定できる端末もあります。アクセスポイントに自動的に接続するよう設定するときには、マニュアルをよく読むなどして、十分注意して使うようにしましょう。

公衆無線LANサービスを利用するときには、偽のアクセスポイントでないか、サービス事業者のアクセスポイント検索やステッカーなどで、その場所で本当にサービスが提供されているのか確認することも有効です。

また、スマートフォンでは、設定によっては利用者が無意識のうちに、携帯電話回線から無線LANに接続が切り替わっている場合があります。携帯電話回線と無線LANのどちらで通信しているのか、確認するようにしましょう。携帯電話回線とは異なり、無線LANでは適切な情報セキュリティ対策を取らずにいと、通信内容が盗み見られるなどの危険性があります。



6 アクセスポイントが暗号化に対応していることを確認

暗号化に対応していない無線LANでは、通信内容を盗み見られる危険性があります。そのため、アクセスポイントが暗号化に対応していることを確認しましょう。

なお、SSLを利用することにより、ウェブサイトやサーバと端末との間の通信が暗号化され、途中で盗み見られる危険性はなくなりますが、すべてのインターネットサービスがSSLに対応しているわけではありません。暗号化に対応していない無線LANで、SSLに対応していないインターネットサービスを利用する場合には、通信内容が盗み見られる危険性を理解した上で、情報をやりとりするかどうか判断してください。

【用語】

- 1: SSL(Secure Socket Layer)とは、信頼できるウェブサイトやサーバとの間で、インターネット上でデータを暗号化して送受信する方法です。SSLが使われていることは、URLが「https」からはじまっていることや、パソコンやスマートフォンの主なブラウザに「鍵マーク」が表示されることで確認できます。
- 2: ファイル共有機能とは、ネットワークを通じて、ひとつのファイルを複数の端末から利用できるようにする機能です。スマートフォンは、OSによるファイル共有機能を有しませんが、アプリケーションによりファイルを共有することが可能です。

《出典：総務省『国民のための情報セキュリティサイト』》

※総務省『国民のための情報セキュリティサイト』を加工して作成
(http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/wi-fi.html)

本メールに関して御質問、お問い合わせがある場合は下記まで御連絡ください。

【担当】 福井県安全環境部県民安全課 鈴木

電話：0776-20-0745（直通） メール：kenan@pref.fukui.lg.jp

「家庭の日」推進テーマ 12月「一年をかえりみ、幸せな家庭を喜ぼう」

「青少年育成の日」推進テーマ 12月「一年を振り返り、感謝の気持ちを持とう」