ゲスト用 Wi-Fi 設定の勧め

ゲスト用 Wi-Fi とは何か、セットアップ方法や家庭用ゲーム機などの IoT デバイスとの関連性について学習します。

現代社会はインターネットに大きく依存しています。そのうち、家に遊びに来た人が「こんにちは、元気だった？」の次に「Wi-Fi のパスワードを教えてもらっていい？」と言うようになるでしょう。しかし、その情報を教えると自宅ネットワークのセキュリティが危険に晒されることに、客を迎える側は気付いているでしょうか？

たとえば、来客が誤って悪意あるプログラムをダウンロードするかもしれませんし、すでに感染しているスマートフォンやラップトップをネットワークに接続するかもしれません。ローカルネットワーク上で増殖するタイプのマルウェアも多いため、マルウェアに感染しているデバイスがあなたの家の Wi-Fi に接続すると、ネットワーク内にあるすべてのデバイスが感染してしまう恐れがあります。

ゲスト用 Wi-Fi をセットアップする理由

客をもてなしつつ、セキュリティを確保することは可能です。ゲスト用 Wi-Fi をセットアップすればいいのです。ゲスト用 Wi-Fi とは、自宅のルーター上の、基本的に独立したアクセスポイントです。自宅内のデバイスは、すべて 1 つのアクセスポイントに接続されてネットワークを構成しています。ゲスト用ネットワークはそれとは別のアクセスポイントで、インターネットにはアクセスできますが、ホームネットワークには接続できません。名前が示す通り、これは自宅を訪れるゲストのためのネットワークです。

ゲスト用ネットワークは双方にとって有益です。友人知人は外界との接触を保てますし、もてなす側も自分のデータに不正アクセスをされずに済みます。ゲストのスマートフォンが何らかの理由でマルウェアに感染していたとしても、ホストの家族写真のアーカイブやその他重要なファイルが影響を受けることはありません。

ゲスト用 Wi-Fi のセットアップ方法

ゲスト用ネットワークを構成するのは、それほど難しくありません。ケーブルをもう 1 本敷設したり ISP に追加料金を支払ったりする必要はなく、Wi-Fi ルーターの設定画面を開いてゲスト用ネットワークを有効にすればいいだけです。以下に標準的な手順をご紹介しますが、メニュー名などはルーターによって異なりますので、詳しくはルーターの取扱説明書をご確認ください。

Buffalo製ルーターで実際にゲスト用WiFiを作成して見ましょう。

1. Wi-Fi ルーターの設定画面を表示します。
2. 「ゲストポート」をオンに切り替えます。

IoT デバイスをゲスト用ネットワークに接続するのが望ましい理由

ところで、ゲスト用 Wi-Fi ネットワークが役に立つのは、友達が大勢いる場合だけに限りません。家の中にスマートデバイスがたくさんある場合にも有効です。スマートテレビや家庭用ゲーム機などもインターネットに接続する必要がありますが、そうしたデバイスの多くは、最新のアップデートがインストールされたコンピューターに比べると非常に脆弱です。つまり、スマートデバイスがメインのネットワークに接続されている場合、そのデバイスがハッキングされてしまうと、他のデバイスにも侵入されてしまう可能性があります。

スマートデバイスについては、多くのエキスパートが「ハッキングされる可能性がある」ではなく「間違いなくハッキングされる」と述べています。ボットネットの一部に変えられてしまったスマート電球を何とかするのは比較的簡単かもしれませんが、ゾンビ化してしまったコンピューターについてはそうはいきません。何よりも、ボットネットはさまざまなマルウェアの拡散に使われます。また、感染したマルウェアは基本的に、ゾンビ化したコンピューターのメモリに自由にアクセス可能です。

メインのネットワークではなく、正しく設定されたゲスト用ネットワークにすべての IoT デバイスを接続すれば、そうした攻撃に対する防御を強化できます。IoT デバイスの1つがサイバー犯罪者にハッキングされても、メインのネットワークに侵入されることはなく、メインのネットワーク内のコンピューターやスマートフォンに不正アクセスされることもありません。

もちろん、ゲスト用ネットワークに接続されたスマート洗濯機がボットネットのメンバーと化し、DDoS 攻撃や仮想通貨マイニングの一端を担う可能性はあります（スマートデバイスを手に入れれば、必ずと言っていいほどこうしたリスクを抱えることになります）。しかしその場合でも、あなたが銀行情報などの重要なデータを保存したコンピューターには影響が及ばずに済みます。

最後にもう 1 つ。ボットネットを作成する者にとって、ルーターは格好の標的です。ですから、自宅のルーターのファームウェアを定期的に更新することを忘れないでください。多くの場合、ハッキングに悪用されかねない脆弱性が最新バージョンで修正されています。