Information-technology
Promotion
Agency, Japan

第 13-38-305 号
2013 年 12 月 2 日
独立行政法人情報処理推進機構

今月の呼びかけ

一般利用者向け：「“ただ乗り”を するなさせるな 無線 LAN 」

最近では、外出時にパソコンやタブレット端末を常に持ち歩き、場所や時間を問わずインターネットを利用する人が増え、簡単にインターネット接続が行える、公衆の無線 LAN 環境も整ってきています。

また、インターネットに接続して利用する機器が増え、家庭内でも無線 LAN 環境を整備し、ゲーム機やスマートテレビなど、様々な機器をワイヤレスで接続して利用する家庭が増えています。

IPA では、2011 年 4 月に家庭内において適切なセキュリティ設定がされていない無線 LAN 環境が他人に使われてしまわないよう、注意喚起を行っています※1。しかし、**家庭内における無線 LAN のセキュリティ設定が適切でない例が未だ見受けられます**※2。また、インターネットに接続できる機器（ノートパソコン、携帯型ゲーム機、スマートフォン、タブレット端末、携帯音楽プレーヤー等）やそれを持ち歩く利用者が増え、知らないうちに家庭内の無線 LAN が “ただ乗り”をされてしまう可能性は 2 年半前に比べて高まっています。

2013 年 10 月には、タブレット端末から適切に設定されていない無線 LAN 環境を無断で利用してウェブサイトにアクセスする、いわゆる**“ただ乗り”**により、殺人予告等を書き込んだとして未成年者が逮捕されたとの報道がありました。

今月の呼びかけでは、無線 LAN 環境を“ただ乗りされた場合”と“ただ乗りした場合”における危険性について解説し、対策を示します。

※1 ：2011 年 4 月の呼びかけ「無線 LAN を他人に使われないようにしましょう！」
http://www.ipa.go.jp/security/txt/2011/04outline.html
※2 ：「2012 年度　情報セキュリティの脅威に対する意識調査」調査報告書　59 ページ
http://www.ipa.go.jp/security/fy24/reports/ishiki/

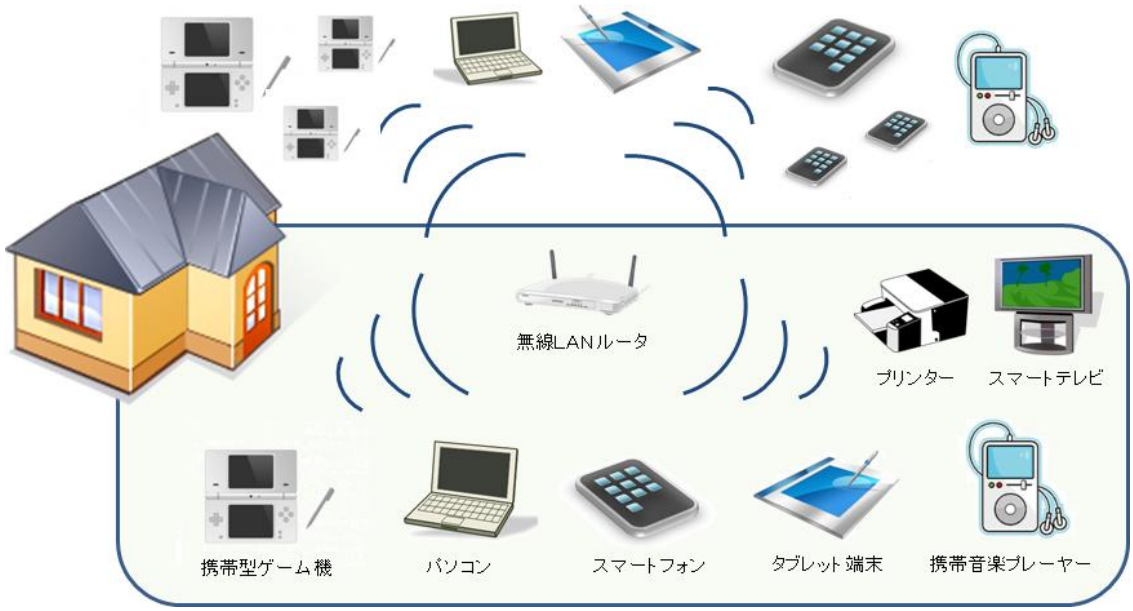

図 1：無線 LAN には様々な機器が屋外からでも接続が可能

(1) “ただ乗り”される危険性について

ここでは、無線 LAN について簡単な解説と、“ただ乗り”される危険性について示します。

【1】無線 LAN とは？

無線 LAN は、電波を使い無線 LAN のアクセスポイント（以下、「親機」）と無線 LAN 機能を持つパソコン、スマートフォン、携帯型ゲーム機など（以下、「子機」）との間で通信を行うネットワーク環境のことです。無線 LAN では親機と子機の双方に通信に必要な設定をすることで、**電波の届く範囲であれば、壁などの障害物を越えて通信が可能**となります。

そのため、電波が届けば、屋外からでもインターネット接続が可能で、とても便利です。しかし、**電波は目に見えず、不正にアクセスされても検知は難しく、またアクセスの痕跡も残らないことから、その便利さとは裏腹に悪意ある者から狙われ易いネット環境**とも言えます。

【2】無線 LAN の“ただ乗り”とは？

ここでは、適切なセキュリティ設定がされていない家庭用親機に無断で子機を接続して、インターネットを含むネットワーク環境を勝手に利用する行為を無線 LAN の“ただ乗り”と表現しています。

【3】“ただ乗り”をされてしまうと？

親機を“ただ乗り”されても、**それに気がつくことやアクセス者の特定が難しく**、先述した報道例のような犯行予告や下記のような**インターネット上の不正な行為や犯罪等に悪用され**、結果的に犯罪の手助けになりかねないばかりか、**無線 LAN 環境の持ち主自身に不正アクセスなどの嫌疑がかけられてしまう**ことも考えられます。

-あらかじめ窃取しておいたインターネットバンキングの ID／パスワードを使った不正送金
-あらかじめ窃取しておいたクレジットカード番号でオンラインショッピング
-親機経由でスマホ等の子機にもアクセスし、端末内の重要情報を窃取される
-親機経由でアクセスした子機の通信データの盗聴

図 2：悪意ある者に無線 LAN を“ただ乗り”されているイメージ図

(2) “ただ乗り”する危険性について

本来“ただ乗り”はモラル上、控えるべき行為です。この“ただ乗り”にはされる側だけでなく、する側にも落とし穴が存在し、**悪意ある者がわざと“ただ乗り”をさせて、接続してきた子機から情報を窃取したり、インターネット上の通信情報を盗聴したり、場合によってはウイルスを感染させたりする**可能性があります。安易な“ただ乗り”はモラルの面だけでなく、危険だということを理解することが必要です。

なお、公衆の無線 LAN 環境を使う場合、ID やパスワード、クレジットカード番号などの重要な情報を入力する際には暗号化通信（SSL※3 など）になっていることを確認する、パソコンの場合はファイル共有機能※4 を解除する、ことが重要です。

※3 ：インターネット上で情報を暗号化して送受信する通信上の約束ごと。
※4 ：ネットワーク上でファイルを複数の端末（この場合子機）で共有できる機能。

(3) 対策

“ただ乗り”されないための対策として、親機のセキュリティ設定が必須です。**そのポイントは「適切な暗号化方式の選択」と「適切なパスワードの設定」の 2 点です**。

「適切な暗号化方式の選択」には、主に「WEP」、「WPA」、「WPA2」の 3 種類があり、中でも「WPA2-PSK（AES）」は現時点で解読方法が確立されていない最もセキュリティ強度が高い方式です。設定ではこの方式を選択してください。

「適切なパスワードの設定」では、容易に推測されることを防ぐため、以下の注意事項に従って手動で行ってください。

- 英語の辞書に載っている単語を使用しない
- 大文字、小文字、数字、記号の全てを含む文字列とする
- 文字数は半角で最低でも 20 文字（最大は 63 文字）とする

上述した手動での設定が難しい場合は、WPS（Wi-Fi Protected Setup）などの**自動設定機能※5 の使用が便利です**。**これは、親機のボタンを 1 回押すだけで複雑なセキュリティ設定を簡単かつ安全に行い、親機と子機の無線 LAN 接続を行います**。

ただし、万が一に備え**普段は自動設定機能を無効にしておくと安心です**。この機能が常に有効になっていると、**勝手にボタンを押して、子機を親機に接続することができてしまいます**。また、場合によっては親機の設定内容がリセットされてしまい、それまでの設定もリセットされ、繋がらなくなる可能性もあります。**普段はこの機能を無効にしておきましょう**。

さらに、**無線接続端末からの親機設定を許可している場合は**、“ただ乗り”してきた子機がその設定を変えてしまうおそれがあるため、**親機の設定画面に強固なパスワードを設定するか、無線接続端末からの親機設定は許可しないようにしてください**。

※5 ：実際の機種では「AOSS」、「らくらく無線スタート」、「かんたん無線君」などと呼ばれるものがあります。

なお、親機の設定方法については、親機に付属の取扱説明書をお読みになるか、お使いの無線 LAN 機器メーカーにお問い合わせ下さい。

■お問い合わせ先
IPA 技術本部セキュリティセンター 加賀谷／田中
Tel:03-5978-7591 Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp