CIAJ セキュリティ Information

ルーターセキュリティの現状と対策
～ルーターを安全に使うための基礎～

2017 年 6 月 27 日

CIAJ 通信ネットワーク機器セキュリティ分科会

インターネットが普及して約 20 年、今では企業、一般家庭の多くでインターネットを利用できる環境ができてきています。今後、IoT の普及に伴い、さらにインターネットの利用機会、範囲が広がることが予想されます。

その、インターネットに接続するために必須な装置、その 1 つがルーターとなります。ルーターは、企業ではインターネットと社内網（イントラネット）をつなぐ役割を担い、また、一般家庭でもインターネットと宅内 LAN をつなぐ役割を担っています。

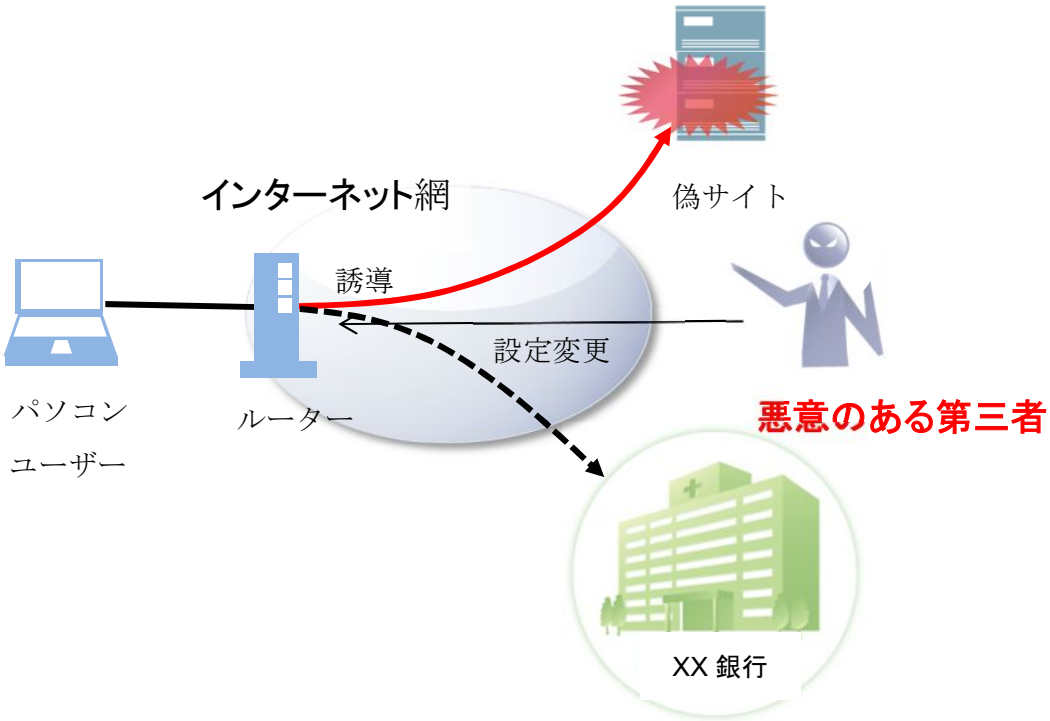
そのルーターですが、インターネットからの不正利用が 2010 年ごろから確認され、総務省、警視庁、JEITA さらにルーターベンダー各社からも注意喚起、基本的な対策が発信され、再発防止に向けた活動が行われています。しかし、未だに不正利用の検出が後を絶たず、問題が収束していないのが現状です。

そこで、ルーターセキュリティの現状と対策について、基礎的なポイントを解説します。

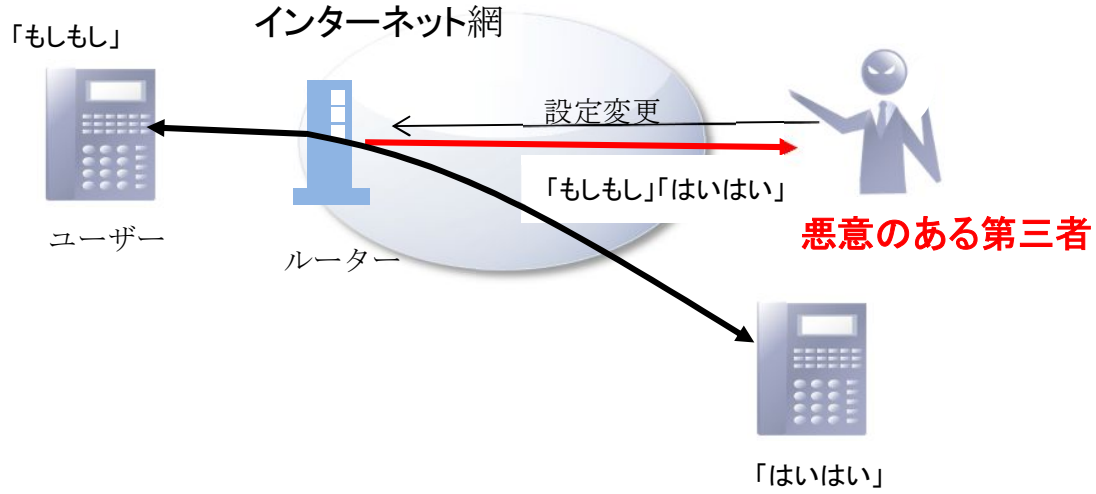
１．ルーターセキュリティ事故事例

現在までに確認されたルーターのセキュリティ事故事例のいくつかを紹介します。

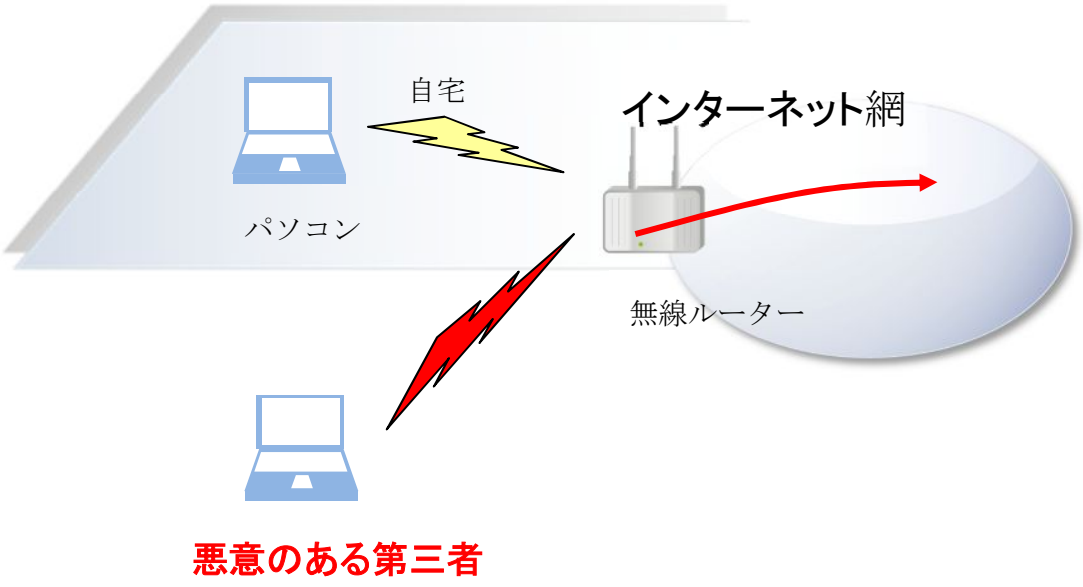
（例 1）悪意のある第三者が外部から不正アクセスをして、ユーザーが気付かないうちにルーターの設定を変更します。そうすると、ユーザーがあるウェブサイト（例えば銀行）にアクセスしようとすると、本物のウェブサイトに似せた偽ウェブサイトに誘導して、そこで、ID やパスワード、個人情報や重要な情報等を搾取します（DNS チェンジャー）。これにより、悪意ある第三者がその情報から、ユーザーになりすまして、不正送金等を行う被害にあってしまいます。



（例２）悪意のある第三者が外部から不正アクセスをして、ユーザーが気付かないうちに、ルーターの設定を変更します。そうすると、インターネットとの通信内容を傍受、また改竄等を行えます。いわゆる「中間者攻撃」による被害が確認されています。これにより、入手した情報を悪用されることで、さらに被害が拡大することになります。



（例３）自宅で使用している無線 LAN ルーターを、他人が無断でアクセスして、インターネット接続する被害が確認されています。無線 LAN の電波は自宅外に漏れており、近所から無線 LAN にアクセスしていました。



２．ルーターセキュリティ事故対策

事故事例（例１）、（例２）にあるように、悪意のある第三者が外部から不正アクセスできてしまうことが最大の原因となります。そのためには、以下の対策を行うことが大切です。

（対策１）ルーターのファームウェアを最新にする。

外部からの不正アクセスをする手段として、ルーターのファームウェアの脆弱性をねらってアクセスする方法が過去事例として確認されています。ルーターメーカーではこのような事例が確認されると、対策をしたファームウェアをリリースしていますので、ホームページ等からダウンロードしてファームウェアの更新をしてください。

（対策２）パスワードを適宜変更する。

パスワードの値が、購入時の初期値のままだったため、外部から不正アクセスされる事例が過去確認されています。そこから不正アクセスされた事例も確認されています。パスワードを変更することで、外部からの不正アクセスを防ぐことが大事で、また、１回だけでなく、頻繁に、かつ不定期に変更することが望ましいです。

事故事例（例３）に対しては、以下の対策を行うことが大切です。

（対策３）MAC フィルタリング機能

MAC フィルタリング機能とは、無線 LAN ルーターにアクセスできる端末を制限する機能です。無線端末（PC 等）は１台１台個別の識別子として、MAC アドレスを持っています。無線 LAN ルーターの機能で、アクセスできる無線端末の MAC アドレスを登録することで、それ以外の無線端末のアクセスを規制することができます。

３．まとめ

インターネットの便利さは飛躍的に向上し、さらに、今後、さらにいろいろなサービスが増えていくことが予想されています。そのインターネットの要であるルーターにセキュリティの脆弱性があると、大変な被害をこうむる可能性があります。

特に、実際に被害にあってからでないと不正が行われているかわからないところが一番問題です。そのためにも、常日頃から被害にあった恐ろしさを認識し、常に対策をとるよう心がけることが大事です。ファームウェアの更新やパスワードの変更はそれほど大変ではありませんので、確実に実行してください。

最後に、ルーターのセキュリティ対策について、参考文献にあげたホームページで情報発信をしていますので、こちらの情報も定期的に確認することをお勧めします。

著者：佐々木　祥一（ささき　しょういち）　沖電気工業株式会社（OKI）
プロフィール
CIAJ 通信ネットワーク機器セキュリティ分科会委員、ユーザネットワークシステム委員会委員
TTC 企業ネットワーク専門委員会委員

参考文献

1) 一般社団法人電子情報技術産業協会（JEITA）「パソコンを安心して利用するために（セキュリティ対策）」
http://home.jeita.or.jp/cgi-bin/page/detail.cgi?n=786&ca=14
2) 総務省「国民のための情報セキュリティサイト」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
3) 警視庁「ロジテック社製の無線 LAN ルータをお使いの方へ」（2016 年 9 月）
http://www.keishicho.metro.tokyo.jp/kurashi/cyber/security/logitec_wirelesslan.html
4) 一般財団法人日本データ通信協会テレコム・アイザック推進会議「【注意喚起】ロジテック製ルータの脆弱性、および、利用者が行うべき必要対策（2012 年 09 月 24 日）
https://www.telecom-isac.jp/news/news20120730.html