サイバーセキュリティの置き薬

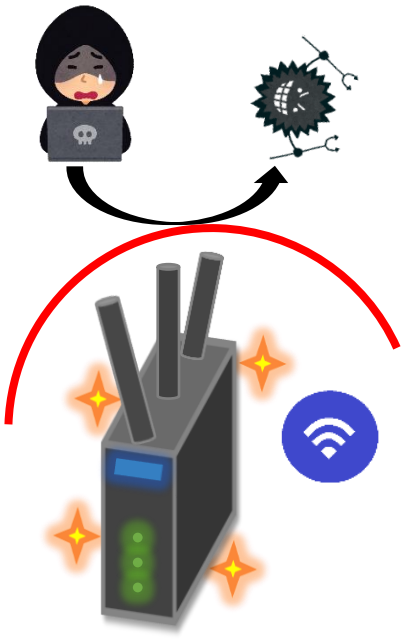
2023年
第6号

Wi-Fiルータの定期的なアップデート、設定確認を！

自宅や会社で使用するWi-Fiルータには「ファームウェア」という機器制御プログラムが搭載されており、そのプログラムに脆弱性が含まれる場合があります。

ファームウェアの脆弱性は、アップデートにより修正できますが、アップデートが提供されなくなると脆弱性が修正できなくなり、その脆弱性が原因でWi-Fiルータが乗っ取られ、**サイバー攻撃の「踏み台」に悪用される恐れ**があります。

Wi-Fiルータの機能や設定を定期的に確認し、適切な管理を行いましょう。



最新ファームウェアを登載したWi-Fiルータ

被害に遭わないための対策

○　ファームウェアを常に最新の状態にする

ファームウェアをアップデートし、常に最新の状態にしましょう。

○　管理画面の初期パスワードを変更する

管理画面にログインするための初期パスワードは、メーカーの取扱説明書等に記載されており、第三者に不正アクセスされる危険性があるため、変更しましょう。

○　管理画面のパスワードは英数字記号を使い、長くて複雑なものにする

単語や生年月日を使ったり、短くて単純なパスワードは、簡単に推測されてしまいます。英数字記号を組み合わせた推測されにくいものを設定しましょう。

○　ファームウェアのアップデートが提供されなくなったWi-Fiルータは買換えを検討する

メーカーのホームページを参照して、ファームウェアのアップデート提供状況を確認し、アップデートが提供されなくなった場合は、買換えを検討しましょう。

○　Wi-Fiルータの機能や設定の状況を定期的に点検する

管理画面にログインした際に、「身に覚えのない機能や設定が有効になっていた」「身に覚えのないアカウントが追加されていた」等、不審な状況を認めた場合はWi-Fiルータを初期化する等、適切な被害防止対策を行いましょう。

被害を受けた場合は、警察への通報をお願いします！

【参考】
NISC：家庭用無線LANルーターの設定・利用
https://security-portal.nisc.go.jp/cybersecurity/month/2022/basics/router/index.html
NISC：インターネットの安心・安全ハンドブックVer. 5.00
https://security-portal.nisc.go.jp/guidance/pdf/handbook/handbook-all.pdf
警視庁：家庭用ルーターの不正利用に関する注意喚起について
https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/router.html