滋賀県警察サイバーセキュリティ情報
R５年度 No.１７

サイバーコネクトSHIG@

今、注目のサイバーセキュリティに関する情報をお届けします。

御社のWiFi設定大丈夫ですか！？

十分なセキュリティ対策がとられていないと・・・

一年の始まりを機に、各システムや機器の点検をおすすめしていますが、今回は、いつの間にか乗っ取られていて、影響が広がりやすい点検項目を御紹介します。

みなさまが、社内外で設置されて運用管理されているルータなどの通信機器の設定はいかがですか？IDやパスワードが初期設定のままではないですか？

いつの間にか乗っ取られていたということになると、やはり、設置者・管理者の運用責任が問われることになります。WiFi利用者のセキュリティを確保するためにも、通信機器の定期的な点検をお願いします。

利用者を守るための４つのポイント！

ポイント①:ぜい弱性対策

ファームウェアの自動更新機能をONにしましょう。自動更新機能がない場合は、最新のファームウェアがリリースされたらすぐに更新しましょう。

ポイント②:アクセスポイントやルータの管理画面の設定

機器管理用のパスワードは、第三者に推測されにくい複雑なパスワードに設定し、厳重に管理しましょう。また、機器の管理画面へのアクセスは、インターネットからアクセスできないなどの制限をかけましょう。

ポイント③:偽アクセスポイント対策

https化した認証用URLの案内や、接続用アプリを提供することで、利用者が確実に正規のアクセスポイントに接続できるようにしましょう。

ポイント④:利用者の確認・認証

メールアドレスの登録やSNSアカウントにログインを求めるなどして、利用者情報の確認ができる認証方式を導入しましょう。

参考（総務省Wi-Fiガイドライン） https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/