サイバーセキュリティだより

発行：愛媛県警察本部生活安全部サイバー犯罪対策課

令和2年
8月24日
Vol.48

Wi-Fi提供者向け「セキュリティ対策」

今回は、Wi-Fiを提供する側のセキュリティ対策ポイントの一部を掲載しますので、Wi-Fiを安全に提供するため、理解を深めましょう！詳細→総務省HP『Wi-Fi提供者向けセキュリティ対策の手引き(https://www.soumu.go.jp/main_content/000690267.pdf)』

Wi-Fi提供がもたらす脅威の例と対策

「Wi-Fiが暗号化されていない」「通信するためのパスワードが誰でも知り得る環境にある」

→第三者にWi-Fiを不正に利用されたり、通信内容を傍受されたりする可能性あり！！！

～ 対 策 ～

○ セキュリティ強度が高い方法（WPA2以上の設定）でWi-Fiを暗号化
○ 状況やリスクを総合的に判断し、適切な方法でWi-Fi利用者にパスワードを伝達
○ 同じアクセスポイントに接続した端末同士の通信を禁止

「ネットワーク機器の管理用パスワードの設定がない、またはパスワードが簡単又は初期値」

→第三者に設定の書き換え、アクセスログの窃取、通信内容の覗き見等をされる可能性あり！！！

～ 対 策 ～

○ ネットワーク機器の管理には、複雑なパスワードを設定
○ ネットワーク機器のファームウエアは、常時最新版に更新

「悪意のある者が、実在するWi-Fiのアクセスポイントと同じ名前（SSID）でポイントを設置」

→本物のアクセスポイントと思い接続した利用者の重要情報等が窃取される可能性あり！！！

～ 対 策 ～

○ 接続アプリの提供や認証画面のhttps化を行った上でそのURL等を周知啓発

「業務に利用しているネットワークを使って訪問者等にWi-Fiを提供」

→Wi-Fiを利用して、提供者側の業務用PC等へ不正にアクセスされる可能性あり！！！

～ 対 策 ～

○ 物理的又はVLAN等を用いて論理的に異なるネットワークを構築するなど、業務用とWi-Fi提供用のネットワークを分離

その他のセキュリティ対策

○ 「サービスの提供者と利用条件（料金や利用時間等）」、「セキュリティ対策の有無と内容（暗号化方式や認証方法等）」、「Wi-Fiの危険性と安全な使い方（偽アクセスポイントの注意喚起と見分け方の周知等）」等を利用者にわかりやすく情報提供
○ 利用者情報の確認や認証の仕組みを導入
○ 利用ルールを設定（接続１回あたりの利用時間やメールの送信などに制限を設ける等）
○ 青少年が有害情報を閲覧できないよう制限するフィルタリングを設定
○ 法令に準拠した個人情報（利用者の登録情報等）や通信記録の保存

『Wi-Fi利用者向け簡易マニュアル』https://www.soumu.go.jp/main_content/000690266.pdf
も合わせて確認し、提供者だけでなく、利用者自身のセキュリティ対策も図りましょう！

相談窓口
愛媛県警察本部サイバー犯罪対策課　TEL089-934-0110(代)