公衆Ｗｉ－Ｆｉ、狙われていますよ！（提供者向け）

“覗き見”、“踏み台”、対策不足のＷｉ－Ｆｉに潜む危険！

公衆Ｗｉ－Ｆｉの悪用事例（イメージ）

設置された正規のアクセスポイントの機器のぜい弱性の放置や機器管理設定の不備等のセキュリティ対策の不備をつき、公衆Ｗｉ－Ｆｉ利用者の通信内容の覗き見やアクセスポイントを踏み台にした他の企業等へのサイバー攻撃を行う

また、偽のアクセスポイントを設置し、騙されて接続した利用者の通信内容を覗き見る

セキュリティ対策の不備は自社だけでなく、利用者や他の企業等の被害も招きます！

利用者を守る為の４つのポイント！

ポイント１：ぜい弱性対策

ぜい弱性にはアップデートで確実に対処！

・ファームウエアの自動更新機能をＯＮにする！

・自動更新機能が無い場合は、新しいファームウエアがリリースされたらすぐに更新する！

・サポート期限切れの場合は買い換えを検討する！

ポイント２：機器の管理画面の設定

機器の乗っ取りを防ぐために適切な設定を！

・機器管理用のパスワードは、推測されにくい複雑なパスワードに設定し、厳重に管理する！

・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させない等、制限をかける！

ポイント３：偽アクセスポイント対策

利用者を守る為、偽ポイントへの誘導を防止！

・https化した認証画面用ＵＲＬの案内や接続用アプリの提供により、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する！

ポイント４：利用者の確認・認証

利用者情報の確認・登録で不正利用防止！

・利用者情報が確認できるように、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の認証方式を導入する！

ご参考（総務省Ｗｉ－Ｆｉガイドライン）

https://www.soumu.go.jp/main\_sosiki/cybersecurity/wi-fi/

その他サイバー犯罪対策に関する事は、大阪府警ホームページをご確認ください。

企業・組織等に向けたサイバーセキュリティ講演も実施中！

https://www.soumu.go.jp/main\_sosiki/cybersecurity/telework/