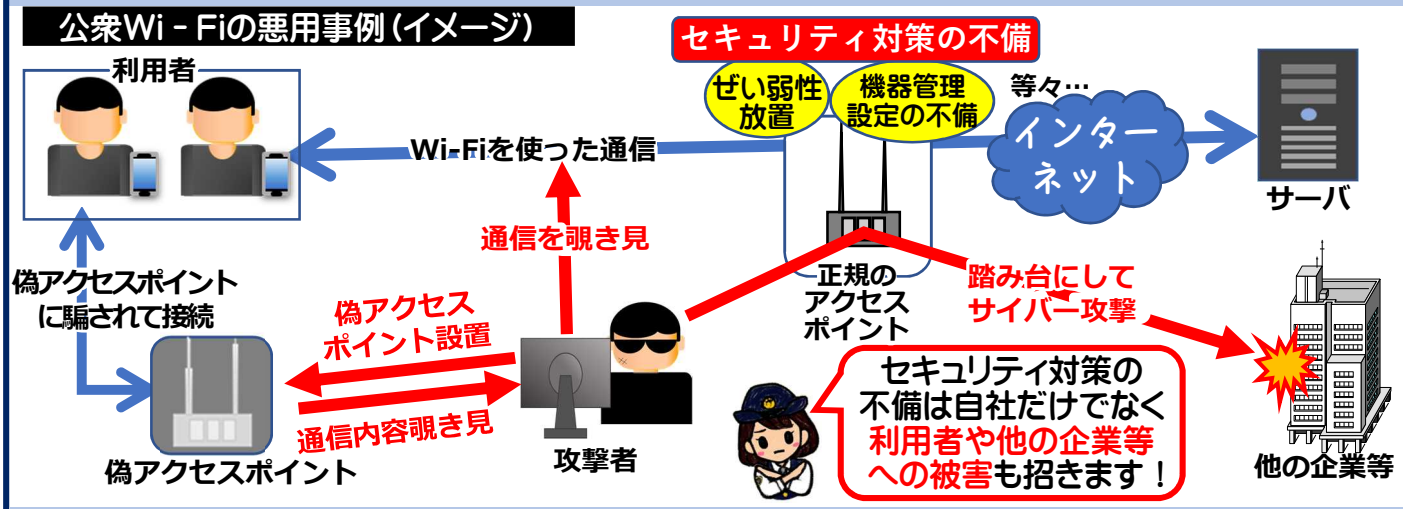
サイバーセキュリティ対策通信

大阪府警察本部サイバーセキュリティ対策課

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！



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にする！
- 自動更新機能が無い場合は、新しいファームウェ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！

ぜい弱性にはアップデートで確実に対処！

ポイント②：機器の管理画面の設定

- 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をさせない等、制限をかける！

機器の乗っ取りを防ぐために適切な設定を！

ポイント③：偽アクセスポイント対策

- 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！

利用者を守る為偽ポイントへの誘導を防止！

ポイント④：利用者の確認・認証

- 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等の認証方式を導入する！

利用者情報の確認・登録で不正利用防止！

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・組織に向けたサイバーセキュリティ講演も実施中！

警察庁 National Police Agency