（公衆無線ＬＡＮ）

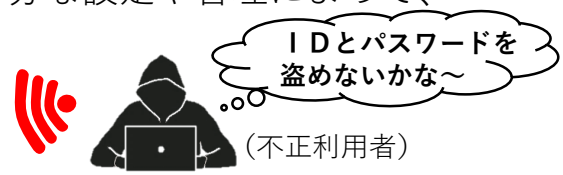
安全なFree Wi-Fiの提供に向けて

事業者の皆様へ

Free Wi-Fiは大変便利ですが、不十分な設定や管理によって、

通信内容の漏えい等の
セキュリティ被害を受ける

おそれがあります。



利用者を守るために

暗号化の実施

Wi-Fiの暗号化を設定することで、無線区間において通信を覗き見られるリスクを下げることができるため、暗号化を行う場合はWPA2による暗号化を設定しましょう。

利用者の端末を保護するための端末同士の通信禁止

一般的なアクセスポイントには、相互通信を禁止する機能が搭載されていますので、利用目的に応じて適切に設定しましょう。

Wi-Fiを安全に提供するために

Wi-Fi機器の適切な運用と業務用ネットワークとの分離

ネットワーク機器の管理用パスワードを複雑なものに設定し、厳重に管理するとともに、ファームウェアについても最新版にアップデートしましょう。また、自社・自組織で業務用に利用しているネットワークを使ってWi-Fiを提供することは避けましょう。

利用者情報の適切な確認とアクセスログの記録・保存

利用者情報の確認や認証の仕組みを導入していれば、誰がWi-Fiを利用していたか調査できるようになり不正利用防止につながります。また、アクセスポイントやルータ等のネットワーク機器は、アクセスログを記録することが可能です。同ログの記録はネットワーク機器にトラブルが発生したときの通信状況の把握等、目的に照らして必要最小限の範囲内での記録にとどめましょう。

利用者に安心を提供するために

Wi-Fi利用者が安心して使うための適切な情報の提供

どのようなセキュリティ対策を実施しているか、利用者に対してわかりやすい方法・内容で提供しましょう。

青少年有害情報のフィルタリング

青少年有害情報の閲覧を制限するフィルタリングの実施や、フィルタリングを提供・販売するサイトの紹介等を行い、青少年が有害情報の閲覧をする機会が少なくなるようにしましょう。

法令に準拠した個人情報保護・通信の秘密保護

利用者情報を登録させる場合は、登録させた個人情報等を適切に管理しなければなりません。また、アクセスログは業務上必要な場合のみに記録・保存が認められ、利用者の意に反する使い方はできません。

【総務省】Wi-Fi提供者向けセキュリティ対策の手引き　より作成

更に詳しく 神奈川県警察　サイバー関連ポータルサイト のホームページへ