Wi-Fi提供時のセキュリティ対策について

秋田県警察本部　警務課サイバーセキュリティ対策係

お客様向けのサービスとしてWi-Fiを提供する際に、セキュリティ対策が不十分だとサイバー攻撃に利用され、加害者となる恐れがあります。

加害者とならないために、機器を設置した業者様とセキュリティ対策について相談してください。

世界規模で発生しているサイバー攻撃や、2020年開催の東京オリンピック・パラリンピック大会に対するサイバー攻撃に利用されないように十分なセキュリティ対策をお願いします。

◇　利用者情報の適切な確認

Wi-Fiサービスの円滑な提供や不正利用防止のため、次の①～③のいずれかの認証方式により利用者情報を確認しましょう。

なお、空港や駅構内等の屋内施設で、目視や監視カメラ等により利用者の出入りを十分把握できる場合は除きます。

① SMS連携方式
- ◎利用開始時に電話番号を入力
- ◎システムから利用コードがSMSで発行され、利用コードを入力することで利用可能

② SNSアカウントを利用した認証方式
- ◎利用開始時に自身が利用しているSNSサービスにログインすることで利用可能

③ 利用していることの確認を含めたメール認証方式
- ◎利用開始時にメールアドレスを登録
- ◎登録したアドレスに返信される利用コードの入力や認証URL等で利用可能

◆ 安全・安心なWi-Fiを提供するためのチェックリスト

次の点について確認しましょう！

- □ **WPA/WPA2による暗号化を設定していますか？**
- □ **Wi-Fiで接続している端末同士の通信をできないようにしていますか？**
- □ **Wi-Fiの提供条件やセキュリティ対策を提示していますか？**
- □ **不必要な個人情報を取得していませんか？**
- □ **業務上必要な限度でアクセスログを保管していますか？**
- □ **違法・有害情報のフィルタリング等をしていますか？**

詳細は、総務省発行「Wi-Fi提供者向けセキュリティ対策の手引き」平成28年8月版」をご覧ください。
URL:http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_AP.pdf