滋賀県警察からのお知らせ

Wi-Fiサービスについて

現在、訪日外国人対応や顧客サービス向上のため、フリーWi-Fiを提供する施設が増加しています。

近年ではフリーWi-Fiは、多くの宿泊・商業施設で必要不可欠なサービスとなりつつありますが、その重要性・利便性の一方で、セキュリティ対策を怠ると、重大なリスクにもなります。

Wi-Fiサービスで注意したいポイント

通信量制限	通信量制限がかけられていないと、短時間で大量の情報が漏えいする可能性があります。
ポート制限	通信可能なポートが制限されていないと、多様なサイバー犯罪ツールの利用が可能となります。
ネットワーク分離	ネットワークが分離されていないと、Wi-Fi利用者間でのウイルス感染や情報漏えいが起こる可能性があります。
通信の暗号化	通信が暗号化されていないと、Wi-Fiで通信した内容（個人情報やID・パスワード等）が漏えいする可能性があります。
コンテンツフィルタリング	コンテンツフィルタリングが設定されていないと、ウイルスサイトのような不適切なサイトに接続する可能性があります。
利用者認証	認証が不要・不十分なWi-Fiは、宿泊者・施設利用者以外が、無断で、不正利用する可能性があります。

ログの保存	Wi-Fi接続ログが保存されていないと、トラブル（故障・事件・事故）が起きた際に原因特定、事後の調査が困難になります。
利用規約の確認	Wi-Fi利用時に注意事項や禁止事項を表示することで、トラブル（故障・事件・事故）の未然防止につながります。
異常通信の監視	平時の通信状態を把握しておくと、事件・事故の発生を迅速に把握できます。
システム構成の把握	Wi-Fiのシステム構成を把握しておくと、トラブル（故障・事件・事故）対応がスムーズになります。

Wi-Fiが関係する事件

海外のセキュリティ企業が発表した、「**Darkhotel（ダークホテル）**」と名付けられた事件は、**ホテルを舞台としたウイルス感染・情報漏えい事案**で、**日本でも被害が発生**したと言われています。

Darkhotel事件では、まず犯人が、ホテルのWi-Fiシステムにウイルスを感染させ、次に、そのWi-Fiに接続した宿泊客のパソコンにウイルスが感染し、感染したパソコンから重要情報が漏えいしました。

このような事件を防止するためには、

Wi-Fiサービス構成機器のソフトウェアを最新状態に保つ

Wi-Fiサービス構成機器にウイルス対策ソフトを導入する

といった、Wi-Fiサービスを提供する施設側のセキュリティ対策も重要となります。

安全なWi-Fiサービスのために

Wi-Fiサービスを安全に提供するためには、

・**Wi-Fi提供者向けセキュリティ対策の手引き**（総務省）
（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_AP.pdf）

・**公衆無線LAN利用に係る脅威と対策**（情報処理推進機構）
（https://www.ipa.go.jp/files/000051453.pdf）

といった資料も役立ちます。

お問い合わせ先
滋賀県警察本部　サイバー犯罪対策室（077）522-1231