



# Wi-Fi(無線LAN)を利用する方へ セキュリティ対策のお願い

通信料金を気にせず、高速な通信を利用する手段として、Wi-Fiは大変便利ですが、その反面、適切なセキュリティ対策をとらずにいると、気づかない間に通信内容が盗み見られたり、不正アクセスを受けたりするおそれがあります。



## 接続する**アクセスポイント**をよく**確認**しよう

外出先でのWi-Fi利用は、接続先をよく確認しましょう。

Wi-Fi利用時、メールアドレスやID・パスワードの入力を求められた場合、正しい入力画面かどうか確認しましょう。偽のアクセスポイントの可能性もあるので、利用時の入力画面ではその都度、URLや鍵マーク等確かめる習慣をつけましょう。

### 【利用時の注意点】

#### ▶ 接続するWi-Fiサービスを確認



【偽アクセスポイントのしくみ】

#### ▶ 接続先の名前(SSID)を確認 (偽アクセスポイントに注意)



【SSIDを端末から確認する場合】

※ 総務省「Wi-Fi提供者向けセキュリティ対策の手引き」引用

## 正しい**URL**で**HTTPS**通信をしているか**確認**しよう

インターネットでの通信内容は、いつどこで盗み見られているか分かりません。

URLが「https://」から始まるHTTPS通信を使えば、通信先のWebサイトまで暗号化されるため、通信内容は保護されます。

特にパスワードや個人情報を入力する場合は、URLや鍵マークを見てHTTPS通信を利用しているか確認するようにしましょう。

### 【利用時の注意点】

- ▶ ブラウザのURL入力欄を確認
- ▶ ブラウザ以外での暗号化通信も確認



【HTTPS通信のURL】

## 自宅に設置している**機器(ルーター)**の**設定**を確認しよう



詳しくは「**Wi-Fi提供者向けセキュリティ対策の手引き**」(総務省)をご覧ください  
[https://www.soumu.go.jp/main\\_sosiki/cybersecurity/wi-fi/](https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/)