

Wi-Fi提供者向け セキュリティ対策の手引き

～ 安全なWi-Fiの提供に向けて～

平成26年4月1日版



スマートフォンが普及し、Wi-Fiを利用する人が増えています。そのため、来訪者向けのサービスとしてWi-Fiを提供する飲食店や宿泊施設なども多くなってきました。

本手引きは、Wi-Fiの提供に関する基本的な知識やメリット、必要なセキュリティ対策について理解を深めてもらうことを目的としています。

なお、本手引きでは特に断りのない限り、「Wi-Fiによるインターネット接続サービス」のことを「Wi-Fi」と表記しております。

本手引きの目的

Wi-Fiはインターネットへの接続環境を簡単に用意することができて、しかも利用者にとっても便利なサービスです。その反面、Wi-Fiはネットワークへの侵入や、掲示板への悪質な書き込み、コンピュータウィルス配布の「踏み台」として利用される等、悪用の対象として狙われ易いものでもあります。

本手引きは、Wi-Fiの提供者に「安心・安全なWi-Fiの提供に向けて、必要なセキュリティ対策について理解していただくこと」を目的に作成しています。

Wi-Fiを提供している方や、今後提供しようと考えている方は本手引きをご一読の上、セキュリティ確保に向けた取り組みをお願いいたします。

本手引きの対象者

本手引きは、来訪者へのサービスとして、「Wi-Fiを提供している」又は「Wi-Fiの提供を検討している」店舗や施設、地方自治体等を対象としています。



1 Wi-Fiの概要

本章では、Wi-Fi（“ワイファイ”と読みます）という言葉は初めて聞く方や、聞いたことはあるけど詳しくはわからないという方向けに、Wi-Fiの概要を説明します。

1-1. Wi-Fiの定義

Wi-Fiは、ケーブルを使わず無線通信を利用してデータをやり取りする仕組みです。一般的に「Wi-Fi」※1は「無線LAN」とも呼ばれています。本手引きでは、一般的によく利用されている「Wi-Fi」に統一して説明をしています。



1-2. Wi-Fiが使える機器

スマートフォン、タブレット端末、パソコンのほか、携帯ゲーム機、音楽プレーヤー、テレビ、プリンター等に搭載されており、わたしたちの生活圏内に広く普及しています。

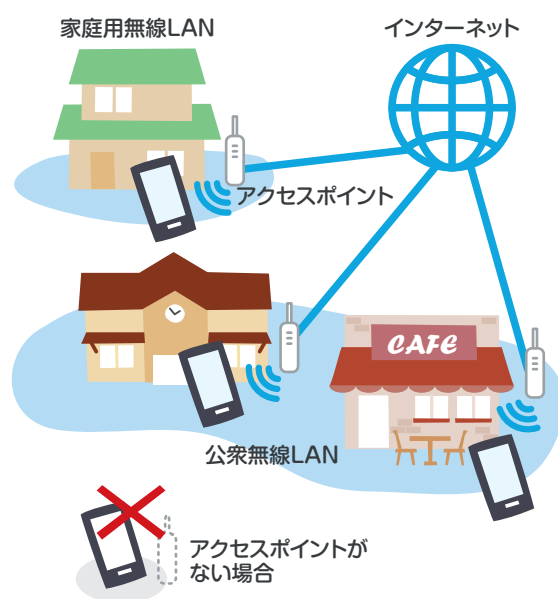


1-3. Wi-Fiが使える場所

Wi-Fiは、アクセスポイントと呼ばれるWi-Fiの機器が設置された環境において、そのWi-Fiの電波が届く範囲※2で利用できます。

家庭内はもとより、外出先でも利用できるように店舗や地下街などにアクセスポイントが設置され、利用できる場所が増えてきました。

また最近では、海外等から来た観光客が日本国内で携帯電話等の回線の契約をしていなくても、空港や観光地等で利用できるようWi-Fiのエリアを、自治体等が設置するケースも増えてきています。



※1 正式には「Wi-Fi」は、無線LAN機器を普及し易くするために、米国の団体が定めた無線LANの規格の一つのことを指します。

※2 Wi-Fiの電波が届く範囲は、アクセスポイント機器、設置条件により異なりますが、周囲の見通しがよければ半径約50～100メートル程度の範囲で利用可能です。

2 Wi-Fiを提供するメリット

近年、Wi-Fiを提供する交通機関や商業施設、公共施設が増加しています。Wi-Fiの提供には、次のようなメリットがあります。

1 来訪者サービスの向上

SNSの人気もあり、いつでも・どこでもインターネットを利用したい人が多くなっています。また、最近ではスマートフォンで動画を見る人も増えており、無料で高速な通信を実現するWi-Fiの導入は、来訪者サービスの向上に繋がります。



2 外国人観光客の誘客

海外では無料のWi-Fiが普及していることもあり、日本でもWi-Fiを利用したいと考える外国人観光客が多くなっています。誰でも利用できる無料Wi-Fiを設置することは、海外からの観光誘客にも繋がります。



3 店舗・施設情報の発信

Wi-Fiと組み合わせて店舗や施設の情報を発信することができるので、来訪者に対するPRにつなげることも可能です。さらに、Wi-Fiを利用してスタンプラリーやクーポンの配信といった活用に取り組む事例もあります。



4 災害時の活用

災害時には携帯電話回線が利用しにくくなることがあります。Wi-Fiは災害時でも比較的つながりやすいため、代替の通信手段として活用することができます。



Wi-Fiは便利で来訪者にも喜んでもらえるサービスとなりますが、悪意のある者からは格好の標的にもなります。

3-1. Wi-Fi提供時に注意していただきたいこと

セキュリティ対策を行わずにWi-Fiを提供した場合、

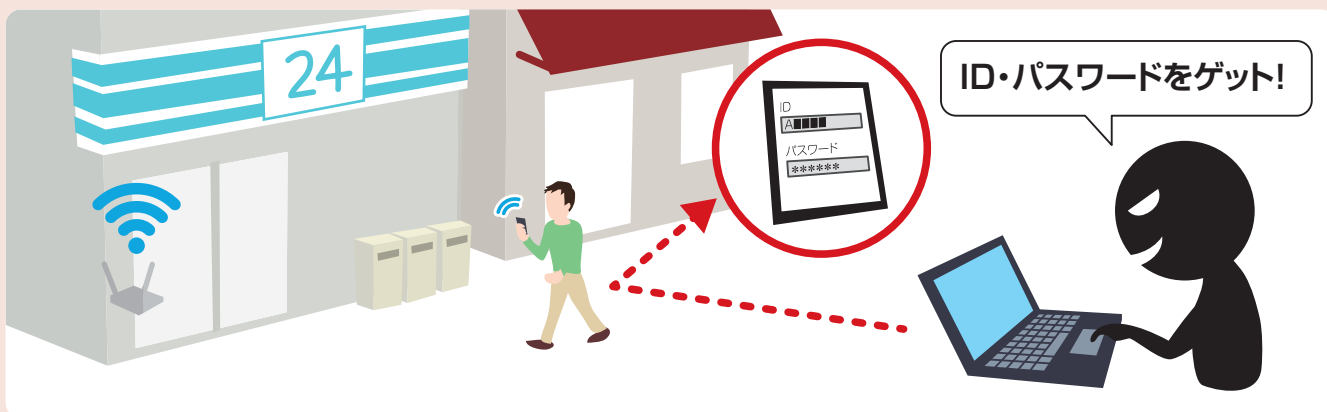
- 他のWi-Fi利用者の通信内容が盗聴されてIDやパスワードが盗まれる
- 迷惑メールの送信や掲示板への悪意ある書き込みに悪用される
- 第三者への攻撃等に悪用される

などの恐れがあります。このような事態に巻き込まれないようにするためにも、Wi-Fiのセキュリティ対策を実施しましょう。



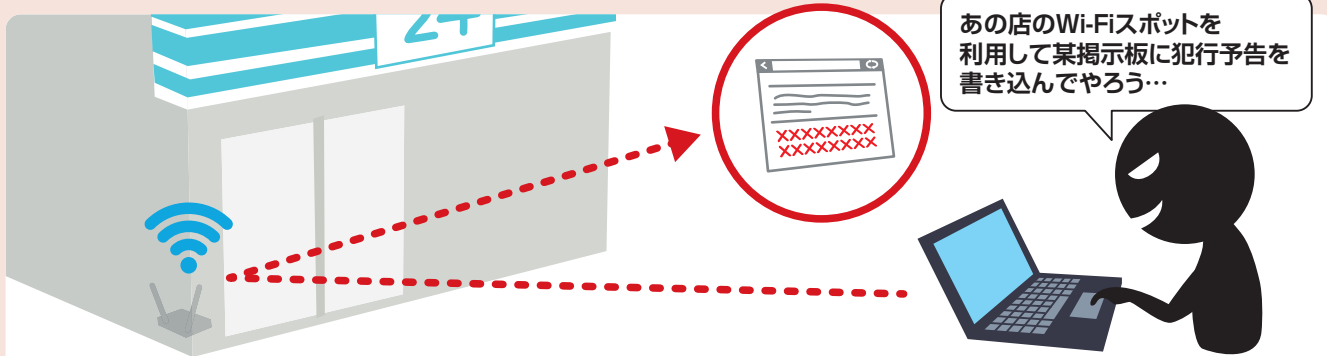
Wi-Fi利用者の安全を確保するために

～Wi-Fi利用者がさらされる危険～



提供するWi-Fiの悪用を防ぐために

～提供するWi-Fiが悪用される危険～



あなたが提供するWi-Fiが、悪用される危険があります!!

3-2. Wi-Fiの安心・安全な利用を確保するためのセキュリティ対策

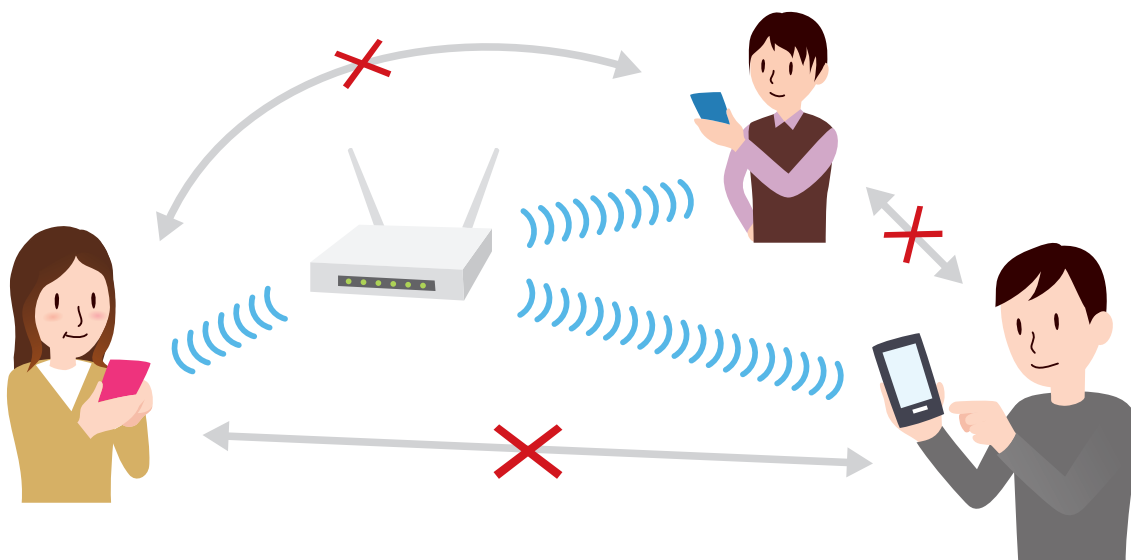
●Wi-Fi利用者の安全を確保するために

⋮ 強固な暗号化を設定



- WPA/WPA2による暗号化を設定しましょう
- WEPによる暗号化は脆弱性が明らかになっており危険です

⋮ Wi-Fiで接続している端末同士の通信遮断



- 「ネットワーク分離機能」や「プライバシーセパレータ機能」と呼ばれる設定によって、Wi-Fiで接続されている端末同士の通信を遮断しましょう

Wi-Fi利用者への適切な情報の開示



24
Wi-Fi

24Wi-Fiへようこそ!

24Wi-Fiは24ストアをご利用のお客さまが無料でご利用いただけるインターネット接続サービスです。

料金

サービスのご利用料金は無料です。

ご利用条件

[→ご利用条件詳細](#)

サービスの紹介ページ例

WPA/WPA2認証で接続

24Wi-FiではWPA/WPA2認証で保護された安全な接続をご提供しております。セキュリティ上の脆弱性が明らかになっているWEP認証についてはサポートしておりません。

クライアント同士の通信遮断

24Wi-Fiに接続したクライアント（パソコン・スマートフォン・タブレットなど）同士の通信を遮断することにより、利用者間でのセキュリティを確保しております。

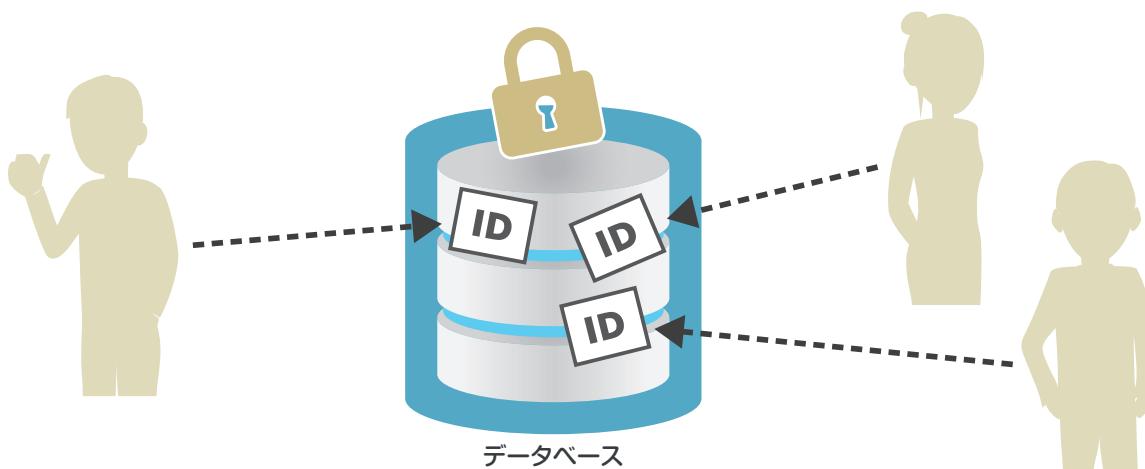
セキュリティ確認ページ例

○利用者が安心してWi-Fiを利用できるように、以下の情報を提供しましょう

- サービスの提供者と利用条件（料金や利用時間）
- セキュリティ対策の有無と内容（暗号化方式）
- Wi-Fiの危険性と安全な使い方

総務省では、安全なWi-Fi利用に向けた「Wi-Fi利用者向け簡易マニュアル」を作成しています。そちらもご利用ください。

個人情報保護・通信の秘密保護



○Wi-Fiの利用IDを発行するため、利用者の氏名や住所、メールアドレス等を取得する場合は、個人情報の適切な取り扱いが必要です

○利用者の通信履歴を記録・保存することは、業務上必要な場合にのみ認められます

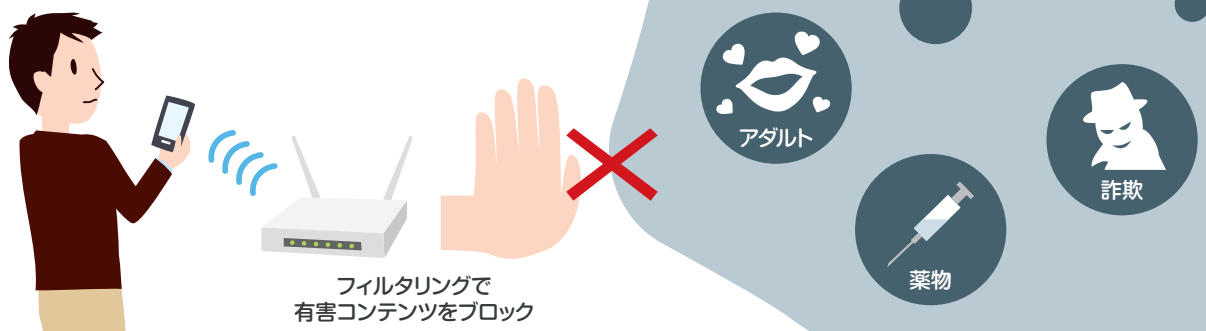
●提供するWi-Fiの悪用を防ぐために

： アクセスログの保管



○接続した端末の情報やエラー情報等の**アクセスログを一定期間保管**し（目安として数か月程度）、悪意ある利用が明らかになった場合にその状況を確認できるようにしましょう

： 公序良俗に反するコンテンツのフィルタリング



○可能であれば、**公序良俗に反するコンテンツのフィルタリング**を実施しましょう（フィルタリングを実施する際には、利用者の事前同意が必要です）

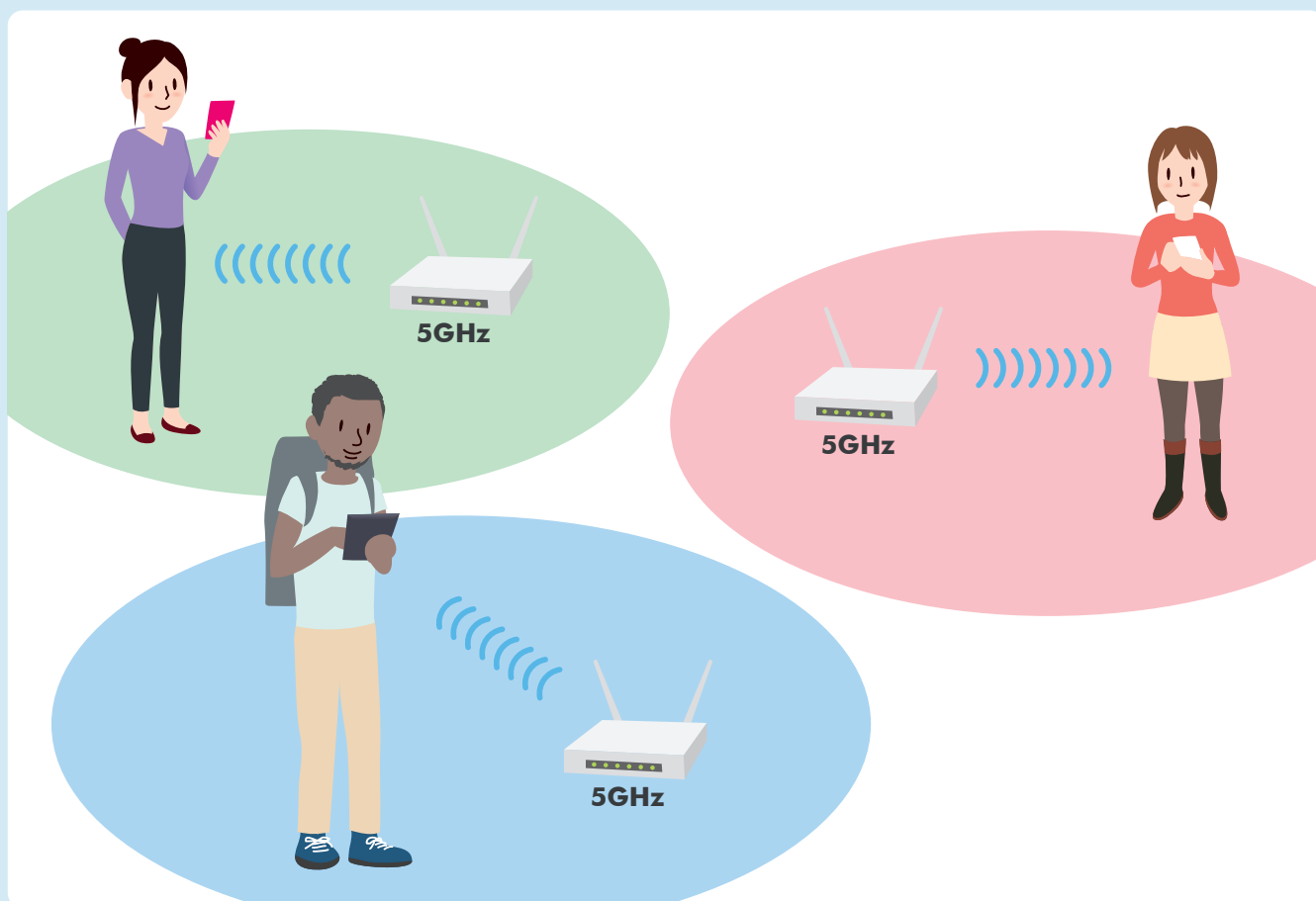
その他、次のようなセキュリティ対策を行う例があります

- 一回あたり利用時間の制限
- 利用者登録の実施
- メール送信の制限

3-3. より使いやすいWi-Fiの提供に向けて

Wi-Fi利用の増加に伴って、電波の混雑が生じています。利用者にとってより使いやすいWi-Fiとするためには、以下の取組みが有効です。

◎利用しやすいWi-Fiの提供



○より使いやすいWi-Fiとするため、以下の取組みを検討しましょう

- 5GHz帯に対応したアクセスポイントを設置する*
- アクセスポイントを複数設置する場合には、相互に影響が出ないように設置場所やチャンネル配置を選定する
- 来訪者が多く、アクセスポイントを設置する通信事業者の数も多い場合は、共用型アクセスポイントを設置する

* なお、5GHz帯の一部は屋外使用が出来ないものがあります。

チェックリスト

安全なWi-Fiを提供するために、特に以下の点について確認しましょう!

強固な暗号化を設定

- ✓ 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遮断していますか?
- ✓ 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?

設置したアクセスポイントの悪用を防ぐために

- ✓ アクセスログを保管していますか?
- ✓ 公序良俗に反するコンテンツをフィルタリングしていますか?



Wi-Fiのセキュリティ対策についてさらに知りたい方は…

総務省が作成する以下のガイドラインをご参照ください。

- ・「無線LANビジネスガイドライン」
http://www.soumu.go.jp/main_content/000233881.pdf
- ・「一般利用者が安心して無線LANを利用するために」
http://www.soumu.go.jp/main_content/000183224.pdf

セキュリティ技術についてより詳細に知りたい方は、次のガイドラインもご参照ください。

- ・「企業等が安心して無線LANを導入・運用するために」
http://www.soumu.go.jp/main_content/000199320.pdf

また、Wi-Fiを導入する通信事業者や機器メーカー等にもご相談ください。

Wi-Fiの規格

代表的なWi-Fiの規格は以下の通りです。

規格名	使用する周波数帯	最大伝送速度	日本における屋外使用の可否*
IEEE802.11b	2.4GHz帯	11Mbps	可
IEEE802.11g	2.4GHz帯	54Mbps	可
IEEE802.11a	5GHz帯	54Mbps	一部不可
IEEE802.11n	2.4GHz帯および5GHz帯	600Mbps	5GHz帯の一部不可
IEEE802.11ac	5GHz帯	6.9Gbps	一部不可

* 総務省の規定による

電気通信事業法に基づく登録または届出

Wi-Fiサービスを事業として提供する場合は、原則として事業法第9条の登録または同法第16条1項の届出が必要になります。ただし、以下に該当する場合は事業法に基づく登録または届出は不要です。

- 本来の業務に付随してWi-Fiサービスを提供する場合
(例) 喫茶店オーナーが来店者にWi-Fiを提供するケース
- 対価を得ずにWi-Fiサービスを提供する場合
(例) 商店街において活性化や集客のために無料でWi-Fiを提供するケース

なお、地方公共団体によるWi-Fiサービスの提供は、「不特定かつ多数の者」が利用する場合は届出の対象となります。

本手引きに関する問合せ先

総務省 情報流通行政局 情報流通振興課 情報セキュリティ対策室
『国民のための情報セキュリティサイト』

URL: http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/

Email: kokumin-security@ml.soumu.go.jp