

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28年8月版



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、コンピュータウイルス配布の「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）という言葉を知って聞く方や、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。

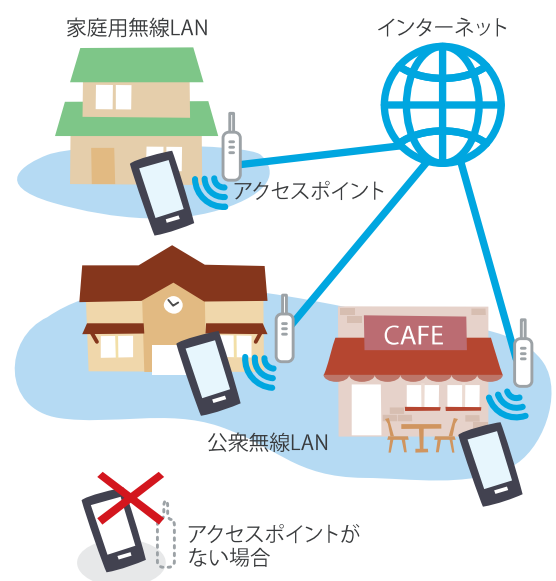


1-3. Wi-Fiが使える場所

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な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発信を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。



3

Wi-Fiを安全に提供するために

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、

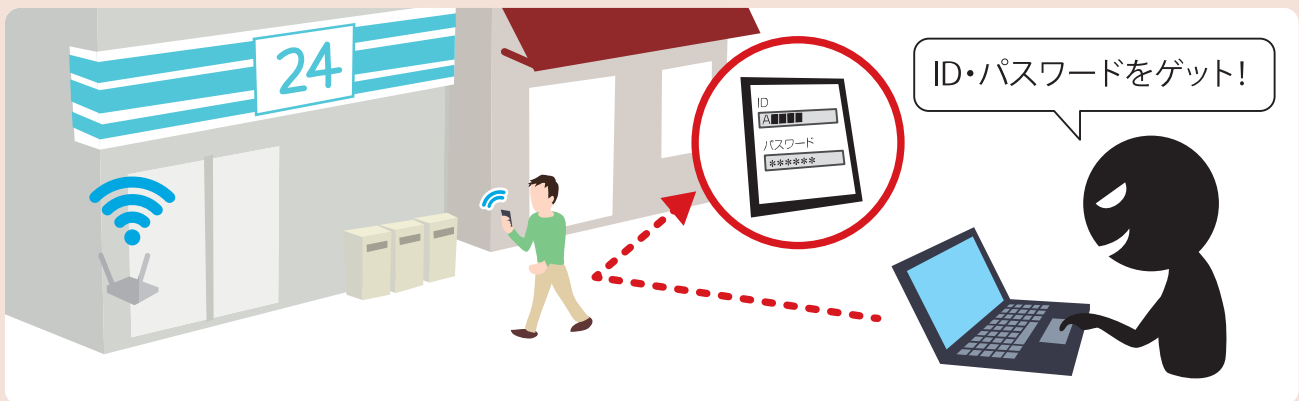
- 他のWi-Fi利用者の通信内容が盗聴されてIDやパスワードが盗まれる
- 迷惑メールの送信や掲示板への悪意ある書き込みに悪用される
- 第三者への攻撃等に悪用される

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。



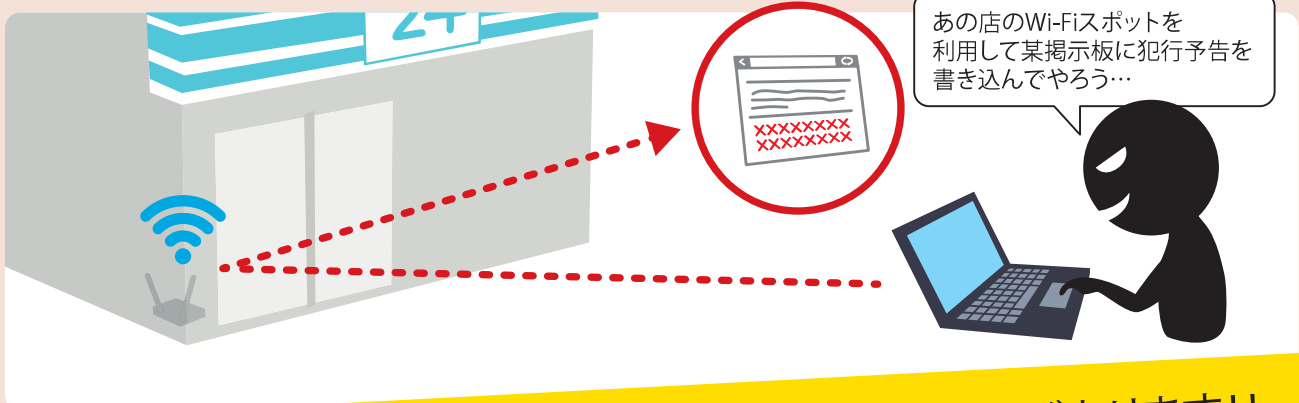
Wi-Fi利用者の安全を確保するために

～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

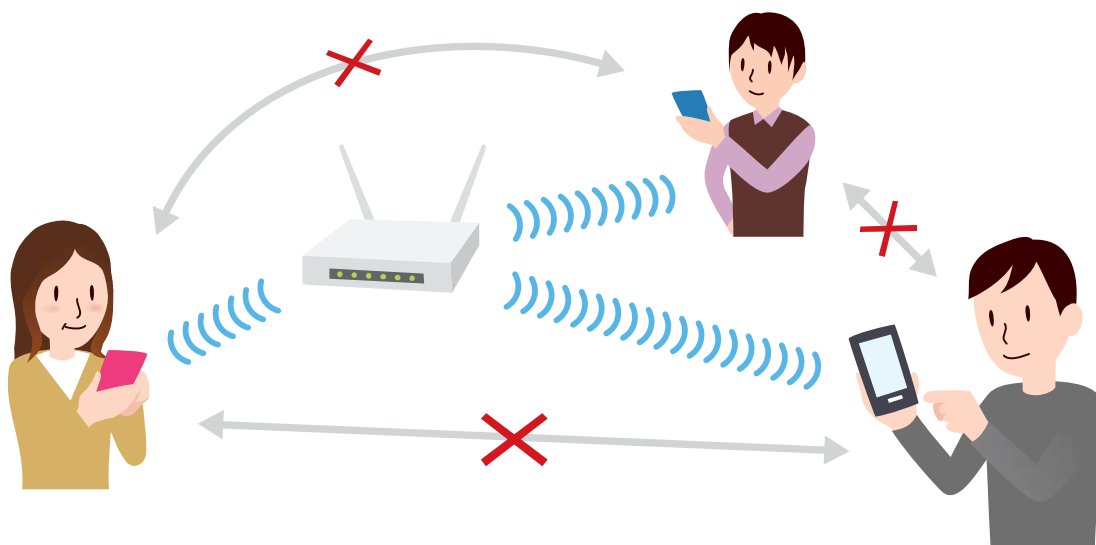
強固な暗号化を設定



○暗号化を行う場合はWPA/WPA2による暗号化を設定しましょう。

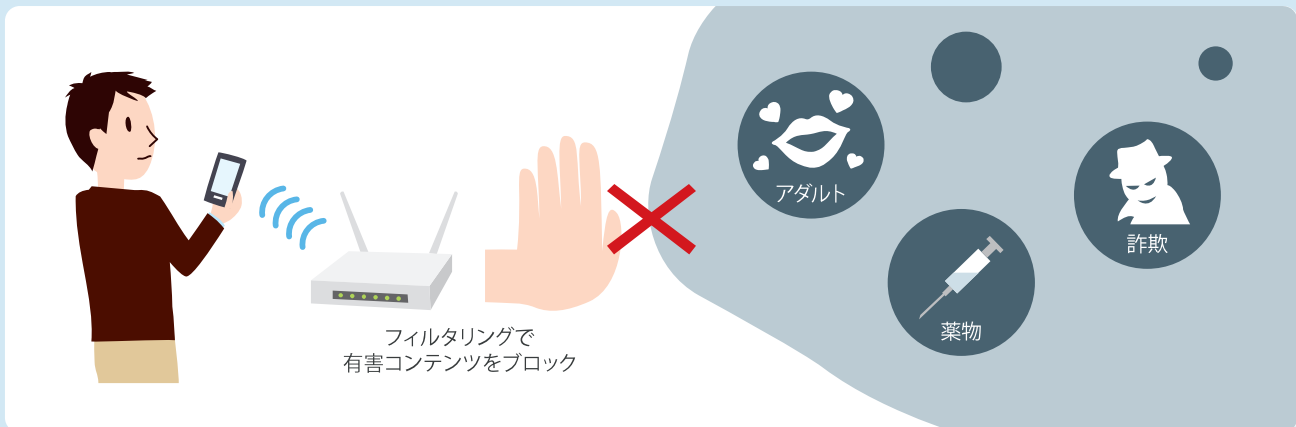
○WEPによる暗号化は脆弱性が明らかになっており危険です。使用は控えましょう。

Wi-Fiで接続している端末同士の通信をできなくする



○「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ができないようにしましょう。

違法・有害情報のフィルタリング等



- 青少年による利用が予想される場所では、違法・有害情報に対するフィルタリングの実施又はフィルタリングを提供・販売するサイト等の紹介を行い、青少年が有害情報の閲覧をする機会をできるだけ少なくするようにしましょう。
(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。)

Wi-Fi利用者への適切な情報の開示

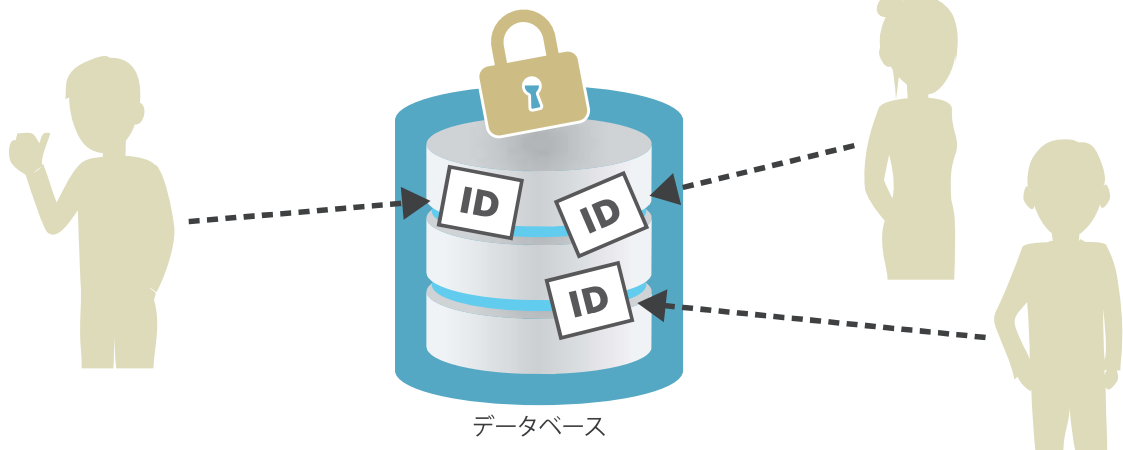
<p>24 Wi-Fi</p> <p>24Wi-Fiへようこそ! 24Wi-Fiは24ストアをご利用のお客さまが無料でご利用いただけるインターネット接続サービスです。</p> <p>料金 サービスのご利用料金は無料です。</p> <p>ご利用条件 →ご利用条件詳細</p> <p>サービスの紹介ページ例</p>	<p>WPA/WPA2認証で接続</p> <p>24Wi-FiではWPA/WPA2認証で保護された安全な接続をご提供しております。セキュリティ上の脆弱性が明らかになっているWEP認証についてはサポートしておりません。</p> <p>クライアント同士の通信遮断</p> <p>24Wi-Fi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。</p> <p>セキュリティ確認ページ例</p>
--	---

- 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

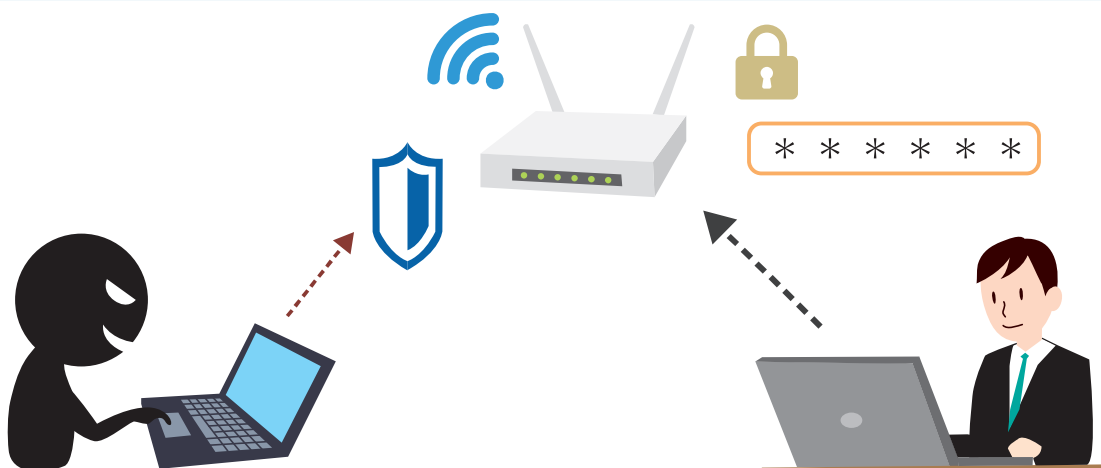


○Wi-Fiの利用IDを発行するため、利用者の氏名や住所、メールアドレス等を取得する場合は、個人情報の適切な取り扱いが必要です。

○利用者のアクセスログを記録・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の悪用をふせぐために

Wi-Fi管理機器の適切な運用



○悪意のある者にWi-Fi機器の悪用をされないためには、Wi-Fi機器の管理IDやパスワードを強固なものにすることが必要です。

○機器の初期パスワードはそのまま利用せず、他の機器等で使用していない複数の文字種や十分な長さのパスワードを設定しましょう。

利用者情報の適切な確認

不特定かつ多数の者の利用を目的として提供される無料Wi-Fiサービスについては、サービスの円滑な提供や不正利用防止のため、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や塀等により区切られた敷地内で提供される場合や、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ような場合は除きます。

①SMS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



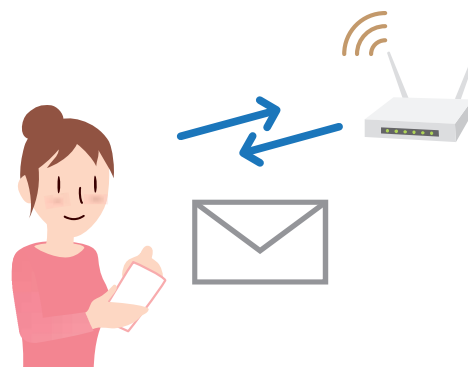
②SNSアカウントを利用した認証方式

- ・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



②、③を選択可能にすることで利用者の利便性を確保することができます。

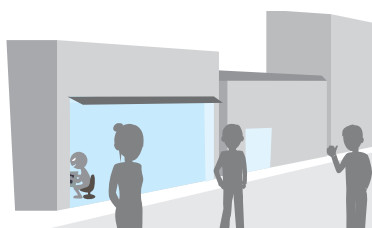
認証による利用者情報の確認が必要な場合／必ずしも必要でない場合の具体例は次のとおり。

認証が必要となるWi-Fiアクセスポイントの設置例

目視等で利用者の出入りを十分把握することが困難な場合



路上に設置されたアクセスポイント



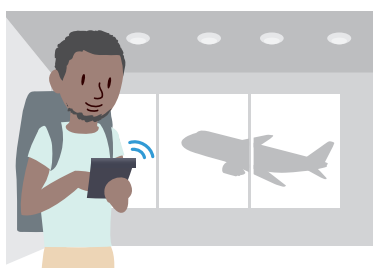
ショッピング街等、屋外で多くの利用者が利用するアクセスポイント



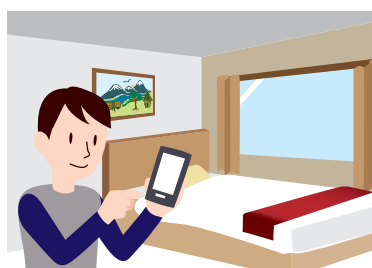
屋外イベント等、開かれた空間で多くの利用者が自由に入出し、利用するアクセスポイント

認証を必ずしも必要としないWi-Fiアクセスポイントの設置例

目視等で利用者の出入りを十分把握できるような場合



空港等が提供するアクセスポイント



ホテル客室等で提供されるアクセスポイント



レストランやカフェ等の店舗内に設置されるアクセスポイント

※上記は、目視、監視カメラや利用者の帳簿等から利用者の出入りを十分把握することが可能であり、認証を必ずしも必要としないWi-Fiアクセスポイントの設置方法を例示したものです。上記の例の場合でも、サービス環境や利用者の状況に応じ、認証を行うことが適切な場合もあります。

なお、意図したエリア内に限ってサービスが行われるように、電波の強度等については適切に調整する必要があります。

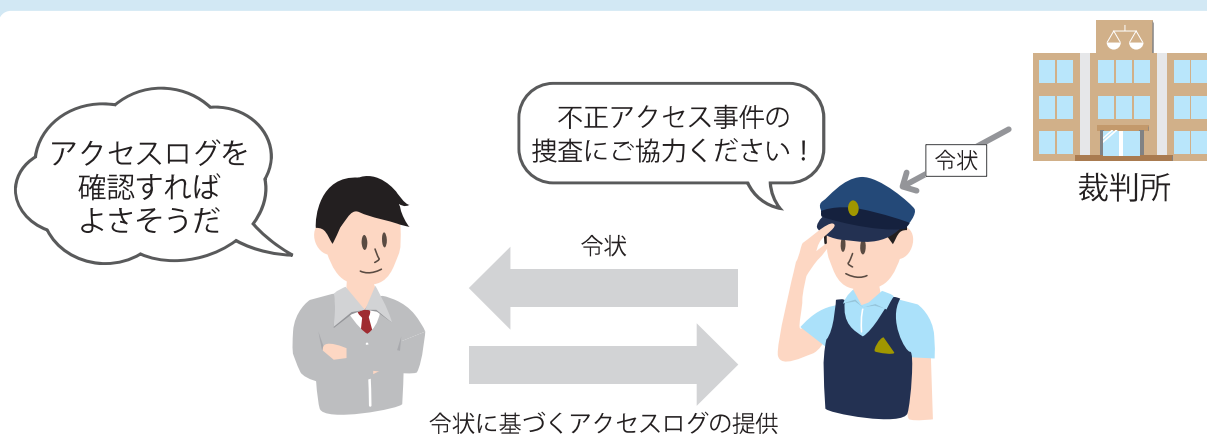
◎提供Wi-Fiが悪用されたときの対応

● アクセスログの保管



○利用者からの問合せ対応やネットワークの保守・管理などの業務のために必要な範囲・期間で、アクセスログを保管し、その業務に役立てることができます。

● 令状に基づくアクセスログの提供



○業務上の必要性から保管しているアクセスログについては、裁判所の発付する令状に従うなどの場合には外部(警察等)に提供することができます。

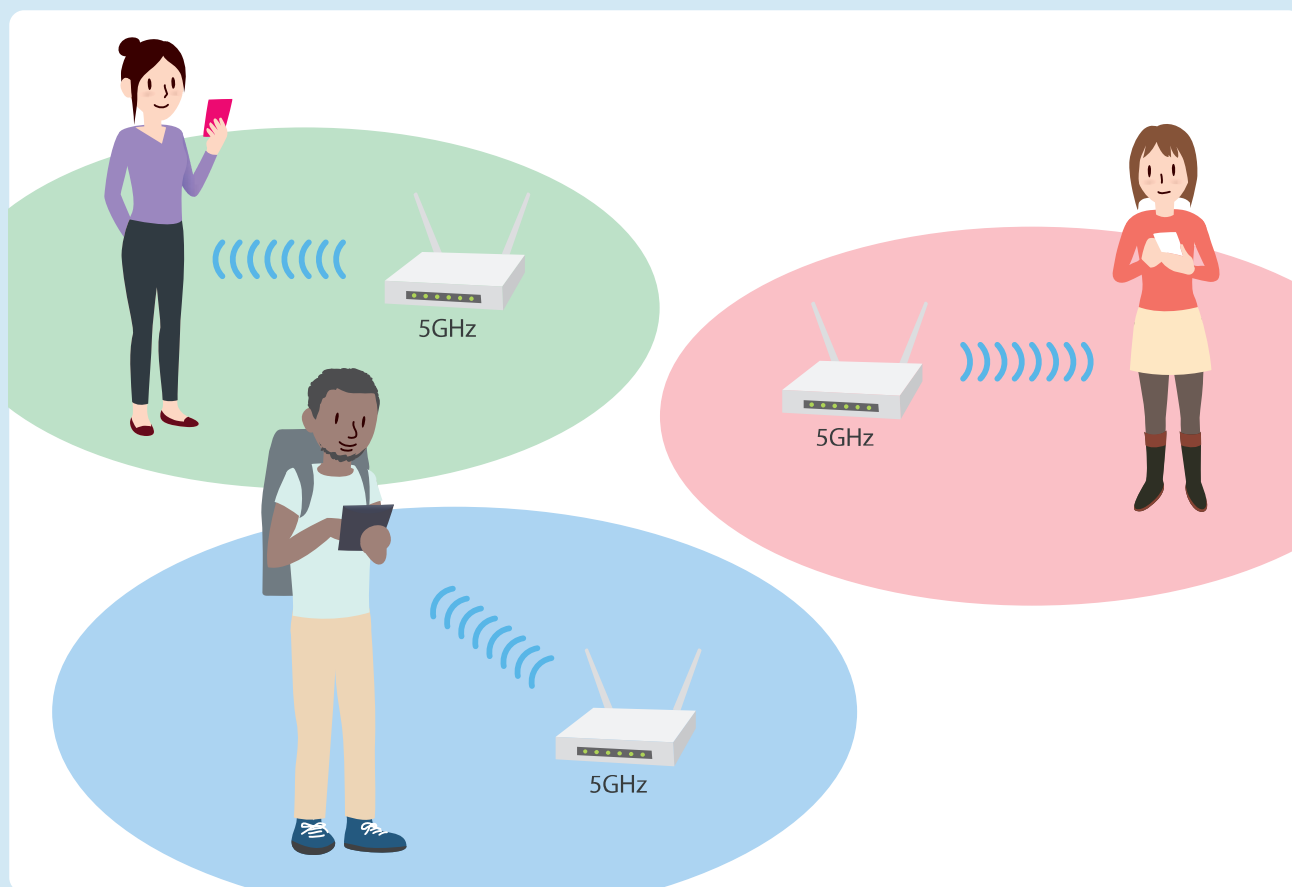
その他、次のようなセキュリティ対策を行う例があります。

- 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！

安全・安心なWi-Fiを提供するために

- ✔ 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？



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サービス提供は、営利を目的としない場合であっても、「不特定かつ多数の者」が利用する場合は、同法第165条第1項の届出が必要となります。

青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律

青少年のインターネットの利用に係る事業を行う者が、青少年がインターネットを利用して青少年有害情報の閲覧をする機会をできるだけ少なくするための措置を講ずることを、努力義務として規定しています。

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