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～

令和2年5月版

顧客や来訪者に対するサービス・利便性の向上を目的として、Wi-Fiを提供する施設等が増えてきています。一方で、セキュリティ対策が十分とられていないものもあり、そのような場合には、利用者のプライバシーが守られなかったり、不十分な設定や管理によって通信内容の漏えい等のセキュリティ被害を受けたりするおそれがあります。

本手引きは、Wi-Fiの提供者に対し、安全なWi-Fiの提供のために必要なセキュリティ対策等に関する理解を深めてもらうことを目的としています。

※Wi-Fi（ワイファイ）とは、無線LANの普及促進を行う業界団体であるWi-Fi Allianceから認証を受けた機器のことです。現在は認証を受けた機器が増えたことから、無線LAN全般を指してWi-Fiということもあり、本手引きでもその意味で使用しています。また、本手引きでは、「Wi-Fiによるインターネット接続サービス」も「Wi-Fi」と表記しています。

1 本手引きをお読みになる方へ

1-1. Wi-Fi提供の現状と本手引き作成の背景

顧客や来訪者に対するサービス・利便性の向上のためにWi-Fiを提供する施設等が増えており、災害時における通信手段の確保方法※1としてもWi-Fiは注目されています。

一方で、十分なセキュリティ対策がとられていないと、ネットワークへの不正アクセスやコンピュータウイルス配布の「踏み台」等に悪用される危険性があり、利用者にまで被害を及ぼす可能性もあります。

また、利用者の約３分の２がWi-Fiの利用に不安を感じているという調査結果もあり、安心してWi-Fiを利用してもらうためには、提供者側における適切なセキュリティ対策が必要となります。

1-2. 本手引きの対象者

本手引きは、Wi-Fiの提供を検討している、または、既にWi-Fiを提供している施設等の運営者やシステム担当者等を対象としています。また、いわゆる「公衆Wi-Fi」はもちろんのこと、施設等の利用者限定でWi-Fiを提供する場合も、本手引きの対象としています。

飲食店や小売店等をはじめ、地域の活性化に取り組む地方公共団体や商業組合、利用者にサービスを提供する宿泊施設や医療機関、そしてICTの利活用が進む教育機関等といった、Wi-Fiを提供する幅広い方々が、本手引きを通じて「Wi-Fi提供にはどのようなリスクがあるのか」「具体的にどのような対策をすればいいのか」といったことを確認するとともに、実際の環境に応じたセキュリティ対策をとるための参考として本手引きが活用されることを期待します。

※1　2011年の東日本大震災の際に、通信事業者がWi-Fiを無料開放して被災地の通信手段確保に貢献しました。これをきっかけに、「00000JAPAN（ファイブゼロ・ジャパン）」という取組が進められ、近年では地震や風水害等の災害発生時にWi-Fiサービスの無料開放が行われています。開放されると、ネットワーク名（SSID）が「00000JAPAN」でサービスが提供され、利便性を最優先して一切の認証なし・暗号化なしで提供されます。

2 利用者を守るための対策

施設等の運営者にとって、来訪者へのサービスとして提供したつもりのWi-Fiが、利用者に対してセキュリティ被害を及ぼすことは避けたいところです。適切なセキュリティ対策について確認しておきましょう。

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～

2-1. 利用者への周知啓発

Wi-Fiの利用にセキュリティ上の不安を覚える利用者が多い中、その解消には、提供者側で十分なセキュリティ対策をとることはもちろん、利用者に対してセキュリティの周知啓発を行うことが重要となります。

提供するWi-Fiにおいて実施しているセキュリティ対策を利用者に情報提供するとともに（詳細は10ページの4-1を参照）、総務省がWi-Fiの利用者に対して必要なセキュリティ対策等に関する理解を深めてもらうために作成した「Wi-Fi利用者向け簡易マニュアル」を周知していくといった対応が有効です。

2-2. 暗号化の実施とパスフレーズの伝達方法

Wi-Fiの暗号化を設定することで、無線区間において通信を覗き見られるリスクを下げることができるため、暗号化を行う場合はWPA2※2による暗号化を設定しましょう。

ただし、暗号の利用に必要なパスフレーズ（パスワード）を利用者にどう伝えるかが問題になります。例えば、パスフレーズを掲示して誰もが知りうる状態においてしまうと、通信を覗き見られるリスクを下げるという暗号化の目的を十分に達することができなくなるため注意が必要です。（詳細は次ページのコラムを参照）

なお、Wi-Fiの提供状況によっては、パスフレーズを利用者に伝えることが困難な場合もあり、状況とリスクを総合的に判断し、暗号化を実施しないことも現状ではやむを得ない場合があります。この場合には、利用者に対する周知を適切に行う必要があります。（詳細は10ページの4-1を参照）

※2　WPA3に対応している場合は、WPA3も有効にしましょう。なお、WEP方式は短時間で解読する方法が知られており、使用は控えましょう。

コラム　Wi-Fiのセキュリティ方式

Wi-Fiには複数のセキュリティ方式があり、WEPからWPA、WPA2、WPA3と時代を経るごとに強化されています。現在では一般的にWPA2が使われています。

セキュリティ強度	セキュリティ方式	特　　徴
強	WPA3	2018年に発表された最新のセキュリティ技術を用いた次世代の方式。今後対応製品の普及が期待される。
	WPA2	WPAより堅牢な現在主流のセキュリティ方式。
弱	WPA	WEPの弱点を補強した方式だが、一部脆弱性があり、現在では推奨されない。
	WEP	暗号を短時間で解読する方法が知られており、現在では容易に解読されてしまう方式となってしまっている。
無	セキュリティなし（暗号化なし）	通信が暗号化されず、だれでも接続可能。

コラム　パスフレーズ公開のリスク

WPA2によるWi-Fiの暗号化は複数の詳細方式がありますが、費用をかけずに手軽に利用できる「WPA2パーソナル（WPA2-PSK）」方式が多く利用されています。

この方式では、アクセスポイントに接続する人全員が同じパスフレーズを共有しており、このパスフレーズが第三者にわからない状態であれば、通信内容を解読される心配はなく安全に利用可能です。

一方で、パスフレーズが知られてしまっている場合、アクセスポイントの通信内容は、条件が整えば比較的容易に解読できてしまいます。加えて、パスフレーズが分かっていれば、同じ名前（SSID）とパスフレーズを設定することで、偽のアクセスポイントを設置して、容易に通信内容を盗むことも可能となります。

WPA2パーソナル方式はこうした特徴があるため、パスフレーズを掲示して誰もが知りうる状態においてしまうことは望ましくありません。例えば、Wi-Fiを必要とする利用者にパスフレーズを記した用紙を個別に配付したり、定期的にパスフレーズを変更してパスフレーズを知りうる人を少ない状態にしたりといった対応が望まれます。

コラム　新しいセキュリティ方式

2018年にWPA3（Wi-Fi Protected Access 3）及びWi-Fi CERTIFIED Enhanced Openが発表されました。

WPA3パーソナル（WPA3-SAE）では、弱いパスフレーズを使われた場合のセキュリティが強化されており、WPA2パーソナルより改良されています。

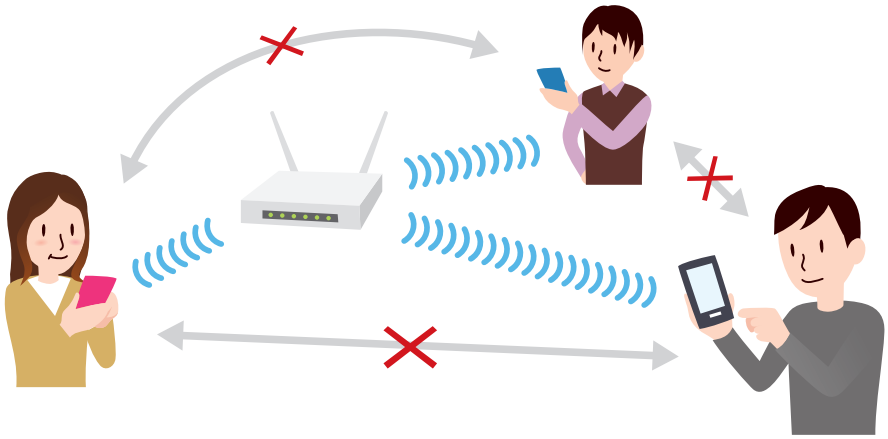
Wi-Fi CERTIFIED Enhanced Openは、パスフレーズなしで接続でき、暗号鍵は個別に設定され通信内容は秘匿されます。不特定多数に提供するWi-Fiサービスのセキュリティ強化策として期待されています。

今後、Wi-Fiの新規設置や、機器更改の際には、是非採用を検討しましょう。なお、これらの方式を利用するためには、スマートフォン等の接続機器も対応している必要がありますが、対応機器は今後増えていくと考えられます。

2-3. 利用者の端末を保護するための端末同士の通信禁止

オフィスや家庭用のWi-Fiでは、同じアクセスポイントに接続した端末同士が情報共有等のために相互に通信可能となっていることがあります。しかし、不特定多数の人が接続するWi-Fiでは、こうした相互通信がセキュリティ上の問題になりかねません。

一般的なアクセスポイントには、相互通信を禁止する機能※3が搭載されていますので、利用目的に応じて適切に設定した上でWi-Fiを提供しましょう。



2-4. 偽アクセスポイント対策

悪意のある者が、実在するWi-Fiのアクセスポイントと同じ名前（SSID）を設定した偽アクセスポイントを設置し、接続してきた利用者を偽の認証画面に誘導して、入力されたID・パスワードやメールアドレスを詐取する事例が報告されています。詐取された情報を悪用され、利用者が被害を受けてしまいます。

しかし、提供者で取れる対策は限られており※4、利用者側での対策が必須です。利用者が正しいアクセスポイントであるかが分かるよう、認証画面をhttps化し、そのURLを周知するなど、継続した周知啓発活動が不可欠となります。

また、正しいアクセスポイントか否かを確認できる接続アプリの提供もひとつの方法です。これも、偽アプリの問題がありますので、アプリの提供は公式ストアから、提供者を明確に判別できる形で行うなど、利用者が安心できる環境を整える必要があります。

※3　一般的には「プライバシーセパレータ」、「クライアントアイソレーション」、「ピアツーピアブロッキング」等の名称で呼ばれています。
※4　エンタープライズ認証では、電子証明書を利用して、正しいアクセスポイントではなかった場合は接続させない機能がありますが、不特定多数に提供するWi-Fiには向いていません。

3 Wi-Fiを安全に提供するための対策

提供しているWi-Fiが不正アクセスに悪用されるなどすると、提供者のネットワークも被害に巻き込まれる可能性があります。また、Wi-Fi機器が乗っ取られると、多くの利用者が被害に巻き込まれるおそれもあります。このような不正利用を防止するため、適切な対策を講じる必要があります。

3-1. Wi-Fi機器の適切な運用

Wi-Fi環境を提供するには、アクセスポイントやルーター等のネットワーク機器を施設に設置し、それを適切に管理する必要があります。

ネットワーク機器の管理には、管理者IDとパスワードの入力が必要ですが、パスワードが設定されていなかったり、簡単なパスワードが設定されていたりすると、第三者に侵入され設定を書き換えられたり、アクセスログを盗まれたりする危険性があります。複雑なパスワード※5を設定し、厳重に管理しましょう。なお、初期設定されているパスワードを使用している場合は、同じ機種で共通であったり、規則性があり容易に推測できたりする場合があるため、第三者に推測されにくいものに速やかに変更しましょう。

また、ネットワーク機器のファームウェアについても、脆弱性対応等でセキュリティが強化された更新版が提供されることもあるため、最新のファームウェアにアップデートしましょう。なお、ネットワーク構築時だけではなく運用時においても、更新版が提供されていないか定期的に確認するようにしましょう。

3-2. 業務用ネットワークとの分離

自社・自組織で業務用に利用しているネットワークを使ってWi-Fiを提供することは避けましょう。業務用のPC等にWi-Fiからアクセスされるなどにより、不正アクセスの被害を受けるおそれがあります。

物理的に異なるネットワークを構築（物理分離）するか、VLAN技術等を用いて論理的に別のネットワークを構築（論理分離）して、業務用のネットワークとWi-Fi提供用のネットワークは分離しましょう。

また、インターネット接続回線を共用する場合には、パケットフィルタやファイアウォール等の対策により業務用のネットワークとWi-Fi提供用のネットワークの分離を確実に行うようにしましょう。

※5　単語等により容易に推測できず、アルファベット・数字・記号等の種別を組み合わせた、できるだけ長い文字列を設定しましょう。また、パスワードを複数のサービスで使いまわさないようにしましょう。

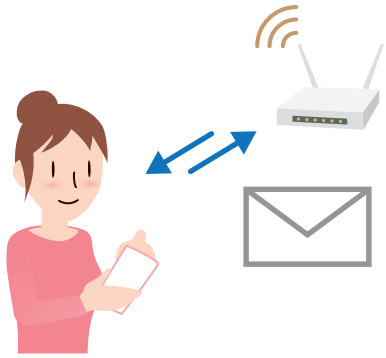
3-3. 利用者情報の適切な確認

Wi-Fiの提供に当たっては、事件や事故が発生したときに、利用者情報の確認や認証の仕組みを導入していれば、誰がWi-Fiを使用していたのかを調査できるようになり不正利用防止につながります。具体的な仕組みとして代表的なものは以下の①～③のとおりです。利用者の利便性確保の観点からは、①と②を利用者が選べるなど多くの認証方式が利用可能であることが望まれます。

なお、屋内施設や塀等により区切られた敷地内（空港や駅構内等）でWi-Fiが提供される場合や、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、利用者情報の確認や認証の仕組みは必ずしも必要ではありません。

① 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 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
- SNSを利用していない人がいることに留意

③ SMS連携方式

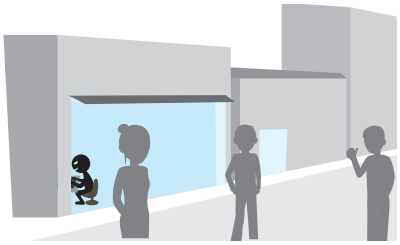
- 利用開始時に電話番号を入力（電話番号は利用者特定の観点から重要な情報となりえます）
- システムから利用コードがSMSで発行され、利用コードを入力することで利用可能
- 格安プラン等でSMS利用不可の人がいることに留意

また、最近では、利用者情報を一度登録すれば、複数のWi-Fiを利用する場合でも認証を自動的に行ってくれる接続アプリもあります。こうした認証連携に参加することもひとつの方法です。

利用者情報の確認や認証が有効な例

不特定かつ多数の利用者がWi-Fiを利用する場所では、誰がいつWi-Fiを使っているのかを目視や監視カメラ等で把握することが困難です。こうした環境では、利用者情報の確認や認証によって利用者を把握できるようにすると良いでしょう。

路上に設置された
アクセスポイント



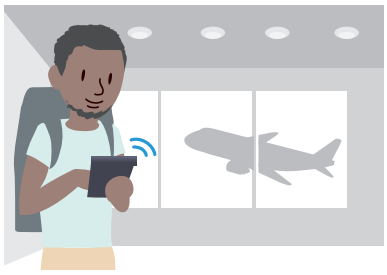
ショッピング街等、屋外で多くの
利用者が利用するアクセスポイント

屋外イベント等、開かれた空間で
多くの利用者が自由に出入りし、
利用するアクセスポイント

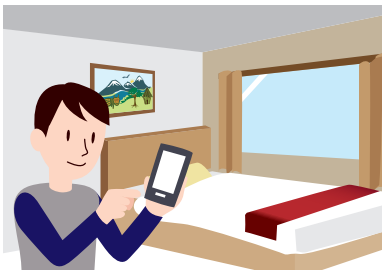
利用者情報の確認や認証が必ずしも必要ではない例

目視や監視カメラ等で利用者の出入りを十分に把握できる環境や、帳簿やシステム記録等で利用者の出入りを十分把握できる場合は、必ずしもWi-Fiシステム側で利用者情報の確認や認証を行う必要はありません。ただし、これらの場合でも、サービス環境や利用者の状況に応じて、利用者情報の確認や認証を行うことが適切な場合もあります。

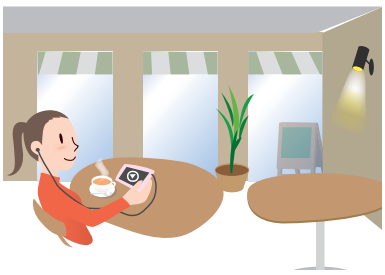
また、意図したエリア内に限ってサービスが提供されるように、電波の出力等について適切に調整することも大切です。



空港等が提供する
アクセスポイント
（空港は不特定多数の利用者がいる環境ですが、監視カメラ等で利用者の状況を把握しやすい）



ホテル客室等で提供される
アクセスポイント
（客室ごとにWi-Fiが提供されるホテル等ではチェックイン時に利用者を確認できる）



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
（店員の目視や監視カメラ等で利用者を特定しやすい）

3-4. アクセスログの記録・保存

アクセスポイントやルーター等のネットワーク機器は、アクセスログを記録することが可能ですが、アクセスログは、どの端末が、いつ、どこにアクセスしたのかがわかる点で高いプライバシー性を有するものです。このため、アクセスログを記録する際は、ネットワーク機器にトラブルが発生したときの通信状況の把握等、目的に照らして必要最小限の範囲内での記録にとどめましょう。また、利用者からの問い合わせに答えるような場合にもアクセスログが必要になることがあります。ただし、このように業務上の必要性から保存したアクセスログであっても、利用者の同意なくマーケティング等の目的に使うことや、第三者に提供すること等のないよう、十分に注意して扱いましょう。

アクセスログを利用者の同意なく外部へ提供することはできません。ただし、業務上の必要性から保存しているアクセスログについて、裁判官の発付する令状に従う場合は、警察等に提供することができます。例えば、Wi-Fiから外部サイトへの不正アクセス行為がなされた場合は、アクセスログを含めた犯人を特定するための情報の提供を警察から求められる場合等が挙げられます。

なお、Wi-Fiの運用を他の事業者に委託している場合は、アクセスログもその委託先の事業者において記録・保存されますが、その記録内容や保存期間等を把握するようにしましょう。また、問い合わせがあった場合の対応方法も、委託先事業者と確認しておく必要があります。

3-5. その他の対策

上記のほか、Wi-Fiの不正利用を防止する観点から、接続１回当たりの利用時間を制限することや、メールの送信について制限を設けること等も有効です。

4 利用者に安心を提供するための対策

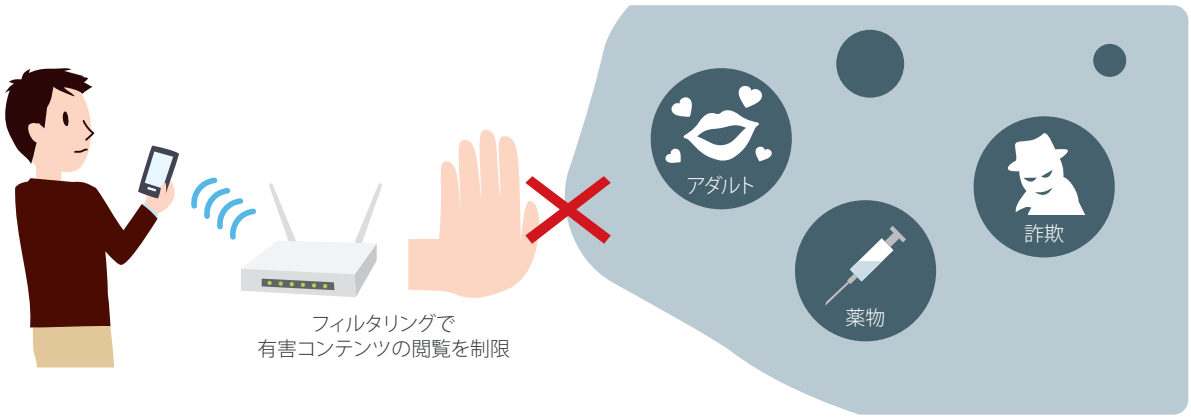
4-1. Wi-Fi利用者が安心して使うための適切な情報の提供

提供条件が明らかでないWi-Fiは、利用者に不安を与える可能性があります。利用者がWi-Fiのセキュリティについて理解した上で、安心してWi-Fiを使ってもらえるようにするために、次の情報をはじめとしてどのようなセキュリティ対策を実施しているか、利用者に対してわかりやすい方法・内容で提供※6しましょう。

- サービスの提供者と利用条件（料金や利用時間等）
- セキュリティ対策の有無と内容（暗号化方式や認証方法等）
- Wi-Fiの危険性と安全な使い方（偽アクセスポイントの注意喚起と見分け方の周知等）

4-2. 青少年有害情報のフィルタリング

青少年による利用（家族や子供の利用）が想定される場所では、例えば青少年有害情報の閲覧を制限するフィルタリング※7の実施（実施には利用者の事前同意が必要）や、フィルタリングを提供・販売するサイトの紹介等を行い、青少年が有害情報の閲覧をする機会が少なくなるようにしましょう。



4-3. 法令に準拠した個人情報保護・通信の秘密保護

Wi-Fi提供者には、利用者の情報を厳格に管理する法的な責任が課せられます。例えば、Wi-Fiの提供に当たって利用者情報を登録させる場合は、登録させた個人情報等を適切に管理※8しなければなりません。また、Wi-Fi提供者は、利用者がいつ、どこにアクセスしたかというアクセスログは、業務上必要な場合のみに記録・保存が認められ、利用者の意に反する使い方はできません。

※6　利用者に対しても、「Wi-Fi利用者向け簡易マニュアル」の６ページにおいて、接続先のセキュリティ対策を確認し、理解した上で利用することが重要であると案内しています。
※7　フィルタリング機能により、あらかじめ登録された分類のWebサイトや特定のWebサイトの閲覧を制限することが可能となります。
※8　利用目的を提示した上で収集し、外部に漏えいしないように管理することや、提示した目的以外で利用者の同意なく利用することは認められないことに注意が必要です。

5 より使いやすいWi-Fiの提供に向けて

Wi-Fiが使える場所が増えることは、利用者にとって歓迎すべきことですが、それによって新たな問題が発生することがあります。Wi-Fiで利用できる電波の帯域（周波数帯）には限りがあるため、多数のアクセスポイントが密集する場所では、それぞれのアクセスポイントが発する電波同士が干渉し、つながりにくい状況になったり、通信速度が低下したりすることがあります。

安定した通信速度でWi-Fi を提供するためにも、周囲の環境との干渉も考慮した取組が必要です。

◉使いやすいWi-Fiを実現するための取組

●混雑を避けるために複数の周波数帯を提供する

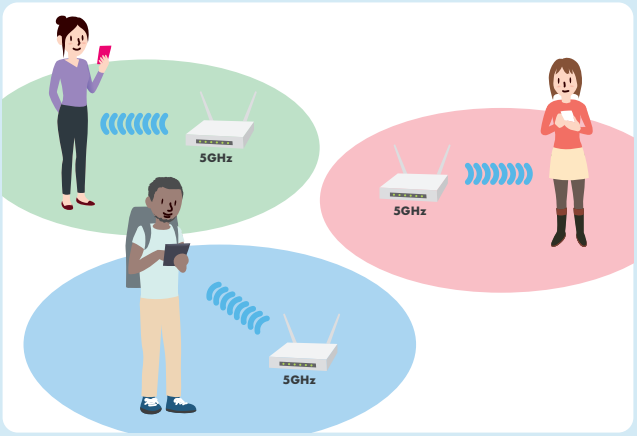
Wi-Fiでは、主に2.4GHz帯と5GHz帯の２種類の周波数帯を利用できます。2.4GHz帯は、家電製品や産業機械をはじめ様々な通信機器でも利用されている混雑しやすい周波数帯です。そのため、比較的混雑しておらず、2.4GHz帯よりも広い帯域が利用可能な5GHz帯※9も提供していきましょう。

●干渉を避けられるチャネルを選択する

アクセスポイントを設置するときは、周囲に設置されている既存のアクセスポイントとの干渉を避ける工夫が必要です。同じチャネル※10を使うと干渉してしまうことから、重複しないように調整しながらアクセスポイントのチャネルを設定しましょう。自動チャネル設定機能があれば、それを設定することが有効です。

●電波の出力を調整する

アクセスポイントが発する電波の出力を上げると、遠くまで電波が届きますが、その分、近隣の施設等と干渉する可能性も高くなります。施設等内で提供する場合は、施設等内にのみ電波が届くように出力を調整するといった工夫が必要です。電波の出力を自動調整してくれるアクセスポイントもあります。



●共有型のアクセスポイントを設置する

観光地や商店街等、人が多く集まるところでは、それぞれの施設が個別にWi-Fiを提供すると、干渉等の問題が発生しやすくなる上に、設備の効率も悪くなります。

複数の設備が、別々の通信事業者を使っている場合でも設備を共有できる共有型のアクセスポイントの設置を検討しましょう。

※9　5GHz帯には、W52（5.2GHz帯；制限付き屋外利用可）、W53（5.3GHz帯；屋外利用不可）、W56（5.6GHz帯；屋外利用可）があります。5GHz帯も気象用レーダー等と干渉することがあるため、安定した通信環境の提供には2.4GHz帯と複数の5GHz帯の組合せ（トライバンド）が有効です。なお、屋外利用については、総務省電波利用ホームページ（https://www.tele.soumu.go.jp/j/sys/others/wlan_outdoor/）をご覧ください。

※10　2.4GHz帯ではチャネル同士の周波数が重複しており、干渉を起こさないようにするには5ch程度離れたチャネルを利用する必要があります。

参考資料

Wi-Fiの伝送規格

Wi-Fiには、「WPA2」といったセキュリティ方式とは別に、使用する電波（周波数帯）や最大伝送速度に関係する伝送規格が存在します。新しい規格ほど高速で安定した通信が可能となります。

規 格 名	呼称 *1)	使用する周波数帯 *2)	最大伝送速度 *3)
IEEE 802.11b	―	2.4GHz帯	11Mbps
IEEE 802.11a	―	5GHz帯	54Mbps
IEEE 802.11g	―	2.4GHz帯	54Mbps
IEEE 802.11n	Wi-Fi 4	2.4GHz帯 & 5GHz帯	600Mbps
IEEE 802.11ac	Wi-Fi 5	5GHz帯	6.9Gbps
IEEE 802.11ax	Wi-Fi 6	2.4GHz帯 & 5GHz帯	9.6Gbps

*1) 規格名をわかりやすくするため、業界団体（Wi-Fi Alliance）が「Wi-Fi 6」といった呼称を規定しています。
*2) 5GHz帯にはW52（5.2GHz帯；制限付き屋外利用可）・W53（5.3GHz帯；屋外利用不可）・W56（5.6GHz帯；屋外利用可）があります。
屋外利用については、総務省電波利用ホームページ（https://www.tele.soumu.go.jp/j/sys/others/wlan_outdoor/）をご覧ください。
*3) 規格上の速度であり、実際のデータ伝送速度はこれよりも遅くなります。

電気通信事業法に基づく登録や届出

Wi-Fiサービスを事業として提供する場合は、原則として電気通信事業法第９条の登録又は同法第16条第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電気通信事業法に基づく登録や届出は不要です。

○ 本来の業務（電気通信役務以外）に付随してWi-Fiサービスを提供する場合
（例）ホテル事業者が宿泊サービスの一環として宿泊者に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、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。

なお、手続や規律の詳細については、電気通信事業法令や、総務省ホームページにおいて公開している「電気通信事業参入マニュアル」、「無線LANビジネスガイドライン」等を参照ください。

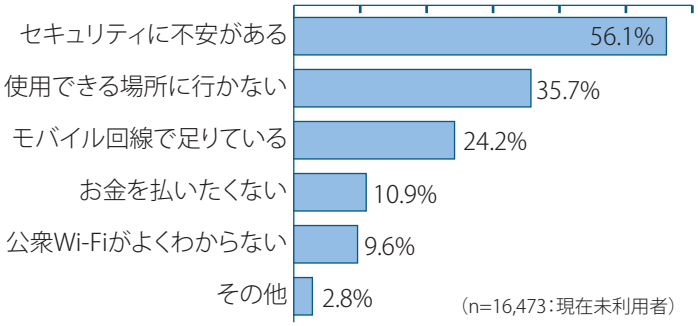
青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律

この法律では、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よう努めるなどの関係事業者の責務等が規定されています。青少年がWi-Fiを利用する可能性があるときは、必要に応じて、フィルタリングの案内等に努めましょう。

利用者アンケート結果

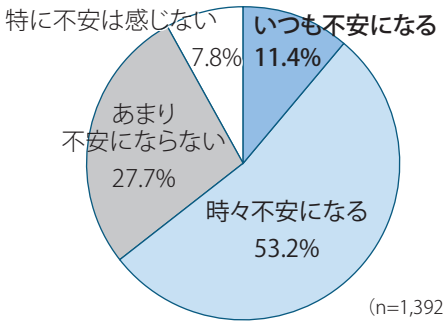
令和元年度「公衆無線LANのセキュリティ対策に係る周知啓発事業（現状等調査）」より作成
（対象地域：全国　期間：2020年2月13日～17日　調査数：31,112（公衆Wi-Fi利用者1,392をスクリーニング調査））

公衆Wi-Fiを利用しなかった理由



（n=16,473：現在未利用者）

公衆Wi-Fiで不安を感じるか



（n=1,392：公衆Wi-Fi利用者）

本手引きに関する問い合わせ先

総務省サイバーセキュリティ統括官室
Email　kokumin-security@ml.soumu.go.jp
ＵＲＬ　https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/