令和７年２月版

公衆「Wi-Fi提供者」向け
・セキュリティ対策の手引き・

安全な公衆Wi-Fiの提供に向けて

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、公衆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、公衆Wi-Fiの提供者に対し、安全な公衆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」を「公衆Wi-Fi」と表記しています。

総務省

［目次］

公衆Wi-Fi提供者向け セキュリティ対策の手引き

安全な公衆Wi-Fiの提供に向けて

Chapter 1 本手引きをお読みになる方へ

公衆Wi-Fi提供の現状と本手引きの背景……02

Chapter 2 公衆Wi-Fiに潜む脅威・リスク

脅威シナリオの例①、②……03

Chapter 3 利用者のための対策

利用者への周知啓発……04
暗号化の実施と暗号化キーの伝達方法……04
コラム「Wi-Fiセキュリティ方式の種類を知ろう」……05
コラム「暗号化キー公開のリスク」……05
コラム「新しいセキュリティ方式」……06
利用者の端末を保護するための端末同士の通信禁止……06
偽の公衆Wi-Fi対策……06
利用者が安心して使うための適切な情報の提供……07
青少年有害情報のフィルタリング……07
法令に準拠した個人情報保護・通信の秘密保護……07
より使いやすい公衆Wi-Fiの提供に向けて……07
コラム「一度の登録でシームレスに接続可能なOpenRoaming」……08

Chapter 4 提供者（自身）のための対策

Wi-Fiルーター（アクセスポイント）の適切な運用……09
コラム「宿泊施設の利用者を狙った攻撃」……10
Wi-Fiルーター（アクセスポイント）の設定の定期的な確認……10
業務用ネットワークの分離……11
コラム「Wi-Fiルーター（アクセスポイント）の設置場所にも注意が必要」……11
利用者情報の適切な確認……12
アクセスログの記録・保存……14
そのほかの対策……14

●参考資料……15

コラム Wi-Fiに関する用語について

Wi-Fiに関連する用語の中には、複数の呼び方をされるものもあります。本手引きでの呼び方をご紹介します。

本手引きにおける呼び方	別の呼び方の例
Wi-Fiルーター ※パソコンやスマートフォンなどの端末をWi-Fiに接続するための機器	**アクセスポイント**
暗号化キー ※Wi-Fi暗号化のためのパスワード	**ネットワークキー　セキュリティキー　パスワード** ※スマートフォンでは単にパスワードと記載される場合が多いです。
管理用パスワード ※Wi-Fiルーターを設定するためのパスワード	**管理者パスワード　管理パスワード**

Chapter 1

[本手引きをお読みになる方へ]

顧客や来訪者に対するサービス・利便性の向上のために公衆Wi-Fiを提供する施設などが増えており、災害時における通信手段の確保方法※1としても公衆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」など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9割弱がWi-Fiの利用に不安を感じているという調査結果※2もあり、安心して公衆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。

1-1 公衆Wi-Fi提供の現状と本手引きの背景

本手引きは、公衆Wi-Fiの提供を検討している、または、すでに公衆Wi-Fiを提供している施設などの運営者やシステム担当者などを対象としています。また、施設などの利用者限定でWi-Fiを提供する場合も、本手引きの対象としています。

飲食店や小売店などをはじめ、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などといった、公衆Wi-Fiを提供する幅広い方々が、本手引きを通じて「公衆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などの災害発生時やモバイル通信事業者の大規模な障害の発生時に避難所などで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、SSID（ネットワーク名）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　総務省「令和5年度無線LAN利用者実態調査」より（https://www.soumu.go.jp/main_content/000957254.pdf）

Chapter 2

［公衆Wi-Fiに潜む脅威・リスク］

Wi-Fiのセキュリティ対策を行わずに提供した場合、利用者の通信内容が盗み見られたり（傍受）、提供する公衆Wi-Fiを第三者に不正利用されるなどの被害にあう危険性があります。

脅威シナリオの例①

❶ Wi-Fiルーター（アクセスポイント）の設定を確認せずに公衆Wi-Fiを提供

Aさんは自身が営むカフェで、利用者の利便性向上のために公衆Wi-Fiを提供することにしました。
SSID（ネットワーク名）をAさんのカフェが提供する公衆Wi-Fiであると分かるような名前に変更し、そのほかの設定については特に確認せずに提供を開始しました。

❷ 公衆Wi-Fi利用者の端末内の情報が第三者に覗き見られる

後日、カフェで公衆Wi-Fiに繋いでブログを書いているBさんが自分のパソコンの中にあるファイルを開こうとしたところ、ほかの人がそのファイルを開いていると表示されました。知らない人からパソコンの中のファイルを覗かれてしまっていたのです。調査の結果、同じ公衆Wi-Fiに接続した端末同士の通信が可能な状態になっているなど、機器の設定が不適切であったことが分かりました。

脅威シナリオの例②

❶ 業務用ネットワークを用いての公衆Wi-Fiの提供

あるホテルで利用者に向けた公衆Wi-Fiを提供することになりました。経費を抑えるためにホテルの業務用に使っているネットワークを用いて公衆Wi-Fiの提供を開始しました。

❷ 業務用機器への不正アクセスが可能な状態に

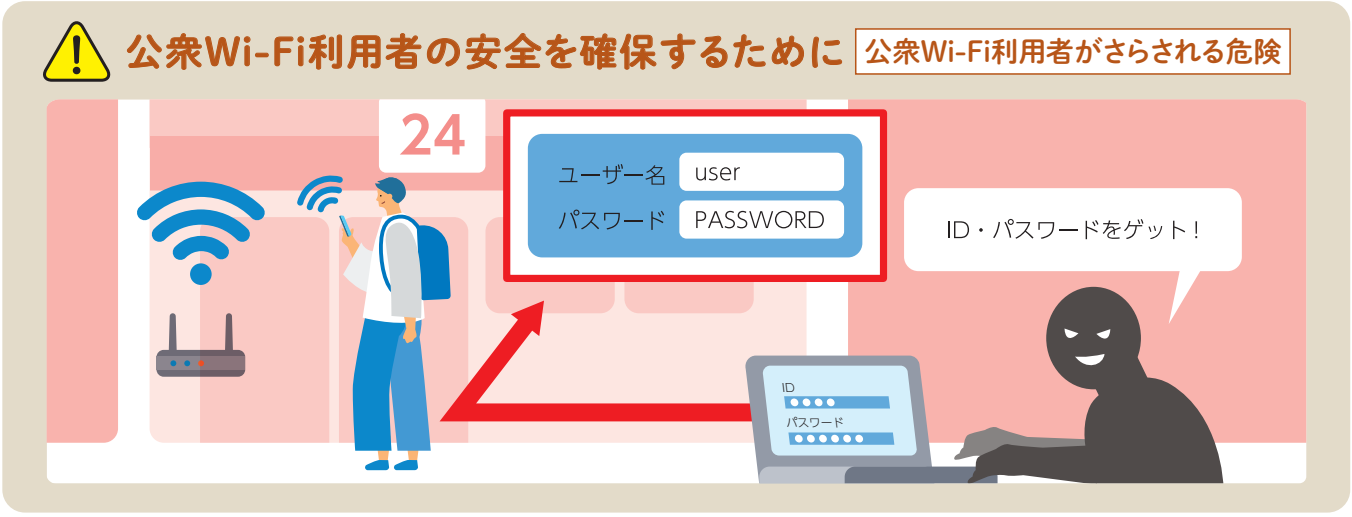
数日後、宿泊者からホテル事務室のコピー機に保存されているファイルが、宿泊者のパソコンから見える状態になっている、との報告を受けました。調査の結果、業務用のネットワークと宿泊者に提供しているネットワークの分離が適切にできていなかったことが分かりました。

これらの事例のようにセキュリティ対策を適切に行わないと、公衆Wi-Fiの利用者・提供者（自身）共に情報漏えいなどの被害を受けるリスクが高まります。こうした危険を回避するために気を付けるべき具体的な内容について、次章から詳しく説明します。

Chapter 3

［利用者のための対策］

施設などの運営者にとって、来訪者へのサービスとして提供したつもりの公衆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。



3-1 利用者への周知啓発

公衆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です。

提供する公衆Wi-Fiで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7ページの3-5を参照）、公衆Wi-Fiの利用者に対して必要なセキュリティ対策などに関する理解を深めてもらうために総務省が作成した「公衆Wi-Fi利用者向け 簡易マニュアル」を周知する対応が有効です。

3-2 暗号化の実施と暗号化キーの伝達方法

Wi-Fiの暗号化を設定しないと、無線区間において通信を傍受されるリスクが高まります。また、暗号化キーを設定せず誰でも利用可能な状態にすると悪意をもった第三者により公衆Wi-Fiを犯罪行為に悪用される可能性もあります。暗号化を行う場合は、WPA2またはWPA3[※3]による暗号化を設定しましょう。

ただし、接続に必要な暗号化キーを利用者にどう伝えるかが問題になります。例えば、WPA2を利用している場合に暗号化キー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いため注意が必要です（詳細は5ページ上のコラムを参照）。

Wi-Fiの提供状況によっては、暗号化キー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、利用者に対するリスクの周知を適切に行う必要があります（詳細は7ページの3-5を参照）。

※3　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いるため、使用は控えましょう。

コラム Wi-Fiセキュリティ方式の種類を知ろう

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以降が使われています。WEPなどの古いセキュリティ方式は、暗号の解読方法が知られているため、WPA2またはWPA3などの新しいセキュリティ方式を選ぶようにしましょう。

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方式。対応するWi-Fiルーター（アクセスポイント）の普及が進んでいる。新しい暗号鍵の交換ロジックや管理フレームの暗号化などセキュリティ面が強化されており、WPA2で報告されていた脆弱性※4も解消されている。 SAEハンドシェイク（Simultaneous Authentication of Equals）という仕組みにより通信に鍵情報を流すことなく暗号鍵交換ができるようになっており、登録された暗号化キーの強度が低い場合や通信が盗聴されている場合においても鍵を盗まれるリスクが低減されている。
	WPA2	WPAより堅牢な現在主流のセキュリティ方式。KRACKsという脆弱性が発見されたが、KRACKsに対処するファームウェアを各ベンダーが配布しているため、ファームウェアを最新化することで安全に利用することが可能。
	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。
弱	セキュリティ（暗号化）なし	通信が暗号化されず、誰でも接続可能。
無		

Wi-Fiルーターの中には2つ以上のSSID（ネットワーク名）を持つものがあります。そのうちの一部に古い暗号化方式が設定されている場合があるため、利用しない場合は停止するようにしましょう。

コラム 暗号化キー公開のリスク

WPA2によるWi-Fiの暗号化に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、公衆Wi-Fiに接続する人全員が同じ暗号化キーを共有しており、この暗号化キーが第三者に知られない状態であれば、通信内容を解読される心配はありません。

一方で、暗号化キーが知られている場合、公衆Wi-Fiの通信内容は、条件が整えば比較的容易に解読されてしまいます。加えて、暗号化キーが分かっていれば、同じSSID（ネットワーク名）と暗号化キーを設定することで、偽の公衆Wi-Fi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パーソナル方式にはこうした特徴があるため、暗号化キー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暗号化キーを記した用紙を個別に配付する、定期的に暗号化キーを変更して暗号化キーを知りうる人を少ない状態にする、といった対応が望まれます。

※4　脆弱性（ぜいじゃくせい）とは、プログラムの不具合や設計上のミスが原因となって発生するサイバーセキュリティ上の欠陥のことです。脆弱性が残された状態でコンピュータを利用していると、不正にアクセスされたり、ウイルスに感染したりする危険性があります。

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-Personal）では、暗号化キーが漏えいした場合においても直ちに通信内容が盗まれることはなく、弱い暗号化キーを使われた場合のセキュリティがWPA2パーソナル（WPA2-PSK）より改良されています。

Wi-Fi CERTIFIED Enhanced Openは、暗号化キーなしで接続でき、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。

Wi-Fiの新規設置や、Wi-Fiルーター（アクセスポイント）更改の際には、ぜひ採用を検討しましょう。

3-3 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ルーター（アクセスポイント）では、同じネットワークに接続した端末同士が情報共有など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公衆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Wi-Fiルーターには、相互通信を禁止する機能※5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公衆Wi-Fiを提供しましょう。

3-4 偽の公衆Wi-Fi対策

悪意のある者が、実在する公衆Wi-Fiと同じSSID（ネットワーク名）を設定した偽の公衆Wi-Fi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。詐取された情報が悪用され、利用者が被害を受けてしまいます。

しかし、公衆Wi-Fiの提供者が取れる対策は限られており※6、利用者側での対策が必須です。利用者に適切な対策を行ってもらえるように、正しい公衆Wi-Fiであるかどうかを判断できるように認証画面を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です。

また、正しい公衆Wi-Fiか否かを確認できる接続アプリの提供も一つの方法です。これも偽アプリの問題があるため、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、利用者が安心して利用できる環境を整える必要があります。

※5　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」などの名称で呼ばれています。
※6　エンタープライズ認証には、電子証明書を利用して、正しいアクセスポイントでない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公衆Wi-Fiには向いていません。

3-5 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、安心して使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、利用者に対して分かりやすい方法・内容で提供[※7]しましょう。

- サービスの提供者と利用条件（料金や利用時間など）
- セキュリティ対策の有無と内容（暗号化方式や認証方法など）
- Wi-Fiの危険性と安全な使い方（偽の公衆Wi-Fiの注意喚起と、正しいSSID（ネットワーク名）やキャプティブポータル[※8]の画面・URLの周知など）

3-6 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[※9]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などを行い、青少年が有害情報を閲覧する機会が少なくなるようにしましょう。

3-7 法令に準拠した個人情報保護・通信の秘密保護

公衆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、公衆Wi-Fiの提供にあ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などを適切に管理[※10]しなければなりません。また、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。

3-8 より使いやすい公衆Wi-Fiの提供に向けて

公衆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。公衆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、多数の公衆Wi-Fiが密集する場所では、それぞれの公衆Wi-Fi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公衆Wi-Fiを提供するために、周囲の環境との干渉も考慮した取組が必要です。

※7　利用者に対しても、「公衆Wi-Fi利用者向け 簡易マニュアル」の5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。
※8　インターネットを利用する前に特定の画面の表示を強制する技術です。Wi-Fiに接続したユーザーに対し、利用規約の確認を要求するのに用いる場合もあります。
※9　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。
※10　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。

使いやすい公衆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、6GHz帯の3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さまざま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。6GHz帯は2022年から日本国内で使用可能※11になった新しい帯域であり、使用できる帯域幅が広いのがメリットです。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6GHz帯や5GHz帯※12の提供も検討しましょう。

●干渉を避けられるチャネルを選択する

公衆Wi-Fiを設置するときは、周囲に設置されている既存の公衆Wi-Fiとの干渉を避ける工夫が必要です。同じチャネル※13を使うと干渉してしまうため、重複しないように調整しながら公衆Wi-Fi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

公衆Wi-Fi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、近隣の施設などと干渉する可能性も高くなります。また、サービス提供範囲外から意図しない利用をされる危険性も高まります。施設内などで提供する場合は、施設内などにのみ電波が届くように出力を調整する工夫が必要です※14。電波の出力を自動調整してくれるWi-Fiルーター（アクセスポイント）もあります。

●共有型の公衆Wi-Fiを設置する

観光地や商店街など、人が多く集まるところでは、それぞれの施設が個別に公衆Wi-Fiを提供すると、干渉など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Wi-Fiルーターの設置を検討しましょう。

コラム　一度の登録でシームレスに接続可能なOpenRoaming

OpenRoaming※15は、最新のWi-Fi技術やサービスの導入・推進を実施するグローバル組織であるWireless Broadband Allianceが支援している国際的なWi-Fi Roaming基盤です。OpenRoamingに対応した公衆Wi-Fiでは、通信の暗号化や偽の公衆Wi-Fiへの接続を防止する技術が使われており、ユーザーは安全に公衆Wi-Fiを利用することができます。導入※16を検討している場合には、Wi-Fiルーター（アクセスポイント）の導入を委託しているベンダーなどに相談してみましょう。

※11　6GHz帯はEIRP25mW以下のVery Low Power(VLP)に限り屋外利用が認められています。無線LANの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。
※12　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など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。
※13　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。
※14　Wi-Fiの電波が施設の外まで届いていないか確認する手軽な方法として、スマートフォンを持って家の周囲を歩いて確かめる方法があります。
※15　Wireless Broadband AllianceにてOpenRoamingの提供スポットが確認できるマップが公開されているため参考にしましょう。（https://wballiance.com/openroamingmaps/）
※16　Wireless Broadband AllianceにてOpenRoamingの提供事例などが紹介されているため参考にしましょう。（https://wballiance.com/openroaming/resources/）

Chapter 4

[提供者(自身)のための対策]

提供している公衆Wi-Fiが不正アクセスに悪用されると、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ルーター(アクセスポイント)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。

4-1 Wi-Fiルーター(アクセスポイント)の適切な運用

Wi-Fi環境を提供するには、Wi-Fiルーターやアクセスポイントを施設に設置し、それを適切に管理する必要があります。

- **安全な管理用パスワードを設定する**

  ネットワーク機器の管理には、管理用IDと管理用パスワードの入力が必要ですが、管理用パスワードが設定されていなかったり、簡単な管理用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。安全な管理用パスワード※17を設定し、厳重に管理しましょう。初期設定されている管理用パスワードをそのまま使用すると、同じ機種で共通※18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てください。

- **管理画面へのアクセスを制限する**

  第三者によって不正に設定変更がされないよう、有線接続でのみ管理画面へアクセス可能なように設定を変更することも対策として有効です※19。

- **ファームウェアを最新な状態に保つ**

  ネットワーク機器のファームウェアは、脆弱性対応などでセキュリティが強化された更新版が提供されるため、最新のファームウェアにアップデートしましょう。ネットワーク構築時だけでなく運用時においても、新しいファームウェアが提供されていないか定期的に確認してください。新しい機種では自動更新が可能となっていることも多いため、自動更新設定※18を有効にしておくことを推奨します。

- **サポート期限内のWi-Fiルーターを利用する**

  Wi-Fiルーターが古い場合はメーカーのサポートが終了しており、ファームウェアの更新が行われません。その場合、新たな脆弱性が発見されても対策されないため、提供者自身はもちろんのこと、公衆Wi-Fiの利用者もサイバー攻撃を受けるリスクが高まります。
  公衆Wi-Fi提供者としての責任をもって、利用しているWi-Fiルーターのサポート期限を把握※20し、サポート期限が切れている場合はWi-Fiルーターを買い替えるようにしましょう。

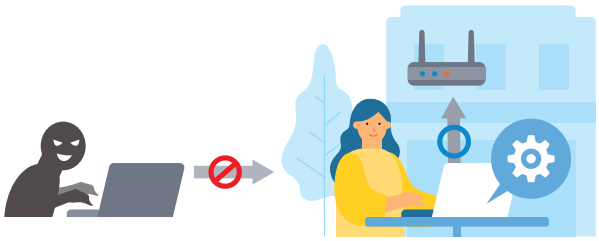
※17　国民のためのサイバーセキュリティサイトにて安全なパスワードの設定について解説されているため参考にしましょう。
(https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/staff/06/)
※18　現在はファームウェアの自動更新機能や管理画面へのログインIDもしくはパスワードの固有化といったセキュリティ対策機能が出荷時から搭載されているDLPA推奨Wi-Fiルーターといったものもあります。
※19　やむを得ず、第三者が物理的にアクセス可能な箇所にWi-Fiルーターを設置する際にはこの限りではありません。
※20　「メーカー名 + Wi-Fiルーターの型番 + サポート期限」などのキーワードでインターネット検索すると機器のサポート期限を確認できることが多いです。

コラム **宿泊施設の利用者を狙った攻撃**

宿泊施設を狙った攻撃事例も存在します。宿泊施設で提供される公衆Wi-Fiにおいて、利用時の挙動がおかしく、不審に思った利用者が通信元を確認したところ、通信経路が不正に変更されていることが分かりました。この事例では、管理画面へのアクセスコントロールが不十分であったことにより、悪意の第三者が意図的に通信経路を切り替えたものと考えられています。

こういった危険を回避するためにも、Wi-Fiのセキュリティ対策はしっかりと行いましょう。

4-2 Wi-Fiルーター（アクセスポイント）の設定の定期的な確認



Wi-Fiルーターにはさまざまな機能があります。どの機能も適切に利用すれば便利なものですが、誤った設定をしてしまうと攻撃に悪用される危険があります。利用しない機能は無効に設定するようにしましょう※21。

また、第三者に外部からWi-Fiルーターに不正に侵入されてしまった場合、継続的に攻撃ができるように一部の設定を変更されてしまうことがあります。不要な機能を無効に設定するのみでなく、機能の設定が不正に変更されていないことを定期的に確認しましょう。

- **VPN機能**
  通信の暗号化に利用する機能です。本機能が有効になっていると遠隔からWi-Fiルーターに接続できるようになるため、攻撃に悪用される可能性があります。設定が無効になっているかだけでなく、見覚えのないVPNアカウントが増えていないかも確認するようにしましょう。
- **DDNS機能**
  動的に変動するグローバルIPアドレスが割り当てられている場合でも、Wi-Fiルーターに固定のドメイン名で接続できるようにする機能です。この機能が有効になっていると、永続的に同じドメイン名で接続できるようになるため、攻撃者に悪用される可能性があります。
- **インターネットからWi-Fiルーター（管理画面）への接続機能**※22
  外出先などからインターネット経由でWi-Fiルーターの管理画面へ接続できるようにする機能です。攻撃者によって外部からWi-Fiルーターの設定を変更するために悪用される可能性があります。
- **UPnP（ユニバーサルプラグアンドプレイ）**
  ネットワークに接続された機器同士が相互に認識しあえるようにする機能です。UPnPはネットワークに接続している機器は信頼できるものという前提に機能しており、認証を行っていないため、攻撃者に悪用される可能性があります。

これらの機能の設定が見覚えのないものとなっていた場合や、Wi-Fiルーターを中古で購入した場合などは、

・Wi-Fiルーターを初期化し、その後に不要な設定を無効とする。
・ファームウェアを最新化する（9ページ参照）。
・パスワード（暗号化キー・管理用パスワード）を変更する（9ページ参照）。

といった対策を行いましょう。

※21　Wi-Fiルーターをはじめとするlot機器はセキュリティ対策が十分に行われていないとマルウェアに感染し、サイバー攻撃に加担してしまう危険性があります。総務省・国立研究開発法人情報通信研究機構（NICT）・インターネットサービスプロバイダ（ISP）が連携し、サイバー攻撃の予防や、被害の最小化を目的としたNOTICEという取り組みを行っています。（https://notice.go.jp/）
※22　メーカーによって機能名が異なります。

4-3 業務用ネットワークの分離

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公衆Wi-Fiを提供することは避けましょう。業務用のパソコンなどに公衆Wi-Fiからアクセスされるなど、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技術など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。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などの対策により、業務用のネットワークと公衆Wi-Fi提供用のネットワークの分離を確実に行いましょう。

コラム **Wi-Fiルーター（アクセスポイント）の設置場所にも注意が必要**

無線接続だけでなく、有線接続によって公衆Wi-Fiに不正な操作をされたり、利用者の通信内容が窃取されたりする可能性があります。LANケーブルを抜かれたり、電源を落とされたり、サービス提供を妨害される可能性もあります。そのため、公衆Wi-Fiは第三者が物理的にアクセスできない場所に設置しましょう。ホテルの客室内の公衆Wi-Fiなど、監視カメラや従業員の目が届かない場所に設置する際は注意が必要です。

4-4 利用者情報の適切な確認

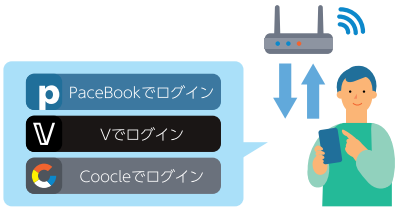
事件や事故が発生したときに、利用者情報の確認や認証の仕組みを導入していれば、誰が公衆Wi-Fiを使用していたのかを調査でき、不正利用防止につながります。すべての公衆Wi-Fiに必須となる対策ではありませんが、提供する公衆Wi-Fiを守るために導入を検討してみてください。具体的な仕組みとして代表的なものは、以下の①～③のとおりです。利用者の利便性確保の観点からは、①と②を利用者が選べるなど多くの認証方式が利用可能であることが望まれます。

❶ 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などで利用可能

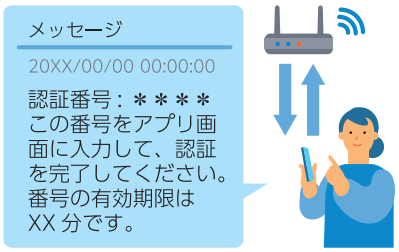
❷ SNSアカウントを利用した認証方式

- 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



❸ 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
- 格安プランなどでSMS利用不可の人がいることに留意



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一つの方法です。

■ 利用者情報の確認や認証が有効な例

不特定かつ多数の人が公衆Wi-Fiを利用する場所では、誰がいつ公衆Wi-Fiを使っているのかを目視や監視カメラなど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。

路上に設置された公衆Wi-Fi

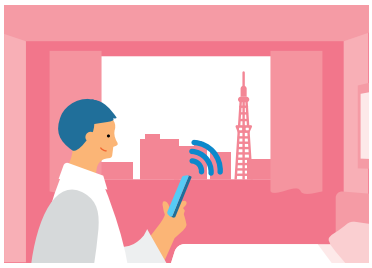
ショッピング街など、屋外で多くの人が利用する公衆Wi-Fi

屋外イベントなど、開かれた空間で多くの人が自由に出入りし、利用する公衆Wi-Fi

■ 利用者情報の確認や認証が必ずしも必要ではない例

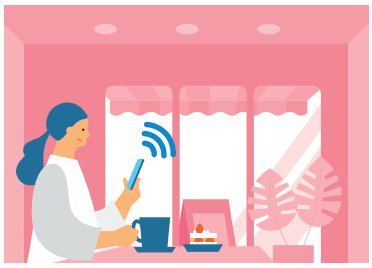
目視や監視カメラなどで人の出入りを十分に把握できる環境や、帳簿やシステム記録などで利用者を十分に把握できる場合は、必ずしもWi-Fiシステム側で利用者情報の確認や認証を行う必要はありません。ただし、これらの場合でも、サービス環境や利用者の状況に応じて、利用者情報の確認や認証を行うことが適切な場合もあります。

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、電波の出力などについて適切に調整することも大切です。



ホテル客室棟で提供される公衆Wi-Fi

客室ごとに公衆Wi-Fiが提供されるホテルなど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などの店舗内に設置される公衆Wi-Fi

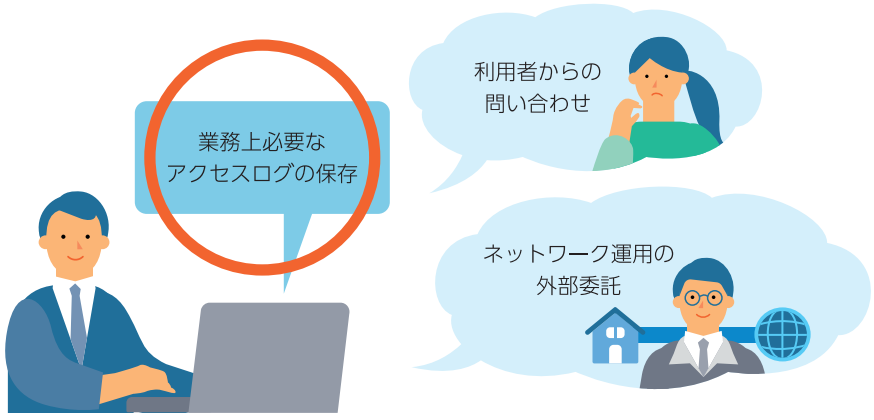
店員の目視や監視カメラなどで利用者を特定しやすい

4-5 アクセスログの記録・保存

Wi-Fiルーター（アクセスポイント）など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分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など、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などの目的に使うことや、第三者に提供することなどのないよう、十分に注意して取り扱いましょう。

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、警察などに提供することができます。例えば、公衆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などが挙げられます。特に利用者がWi-Fiルーターを用いて外部通信を行う際のIPアドレスが、業務用ネットワークと同一のものである場合には、不正アクセスが業務用ネットワークから行われていないことを証明する大切な証拠になります。

なお、公衆Wi-Fiの運用をほかの事業者に委託している場合は、アクセスログも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など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。



4-6 そのほかの対策

上記のほか、公衆Wi-Fiの不正利用を防止する観点から、接続１回あたりの利用時間を制限することも有効です。

迷惑メールの発信元として悪用されることが心配される場合には、Wi-Fiルーター（アクセスポイント）のIPフィルタ機能を用いて、LANからインターネットへのPOP3やSMTPのプロトコルを用いた通信を禁止設定することも有効です。ただし、正規のメールも送ることができなくなることにご注意ください。

[参考資料]

Wi-Fiの伝送規格

Wi-Fiには、「WPA2」や「WPA3」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です。

規格名	呼称 ※23	使用する周波数帯 ※24	最大伝送速度 ※25
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
IEEE 802.11ax	Wi-Fi 6E	2.4GHz帯 & 5GHz帯 & 6GHz帯	9.6Gbps
IEEE 802.11be	Wi-Fi 7	2.4GHz帯 & 5GHz帯 & 6GHz帯	46Gbps

無線LANの屋外利用について

無線LANは大きく分けて2.4GHz帯、5GHz帯及び6GHz帯の周波数帯を使用し、5GHz帯はさらに5.2GHz、5.3GHz、5.6GHz帯に分けられます。

また、令和４年９月から利用可能となった6GHz帯では、EIRP25mW以下のVery Low Power（VLP）に限り、屋外での利用が可能になりました。

屋外利用にあたっては条件があるため、規則の詳細については総務省ホームページにおいて公開している「無線LANの屋外利用について」などを参照ください。

電気通信事業法に基づく届け出

公衆Wi-Fi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に基づいた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）に付随して公衆Wi-Fi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公衆Wi-Fiを提供するケース
- 対価を得ずに公衆Wi-Fi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公衆Wi-Fiを提供するケース

なお、地方公共団体による公衆Wi-Fi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」などを参照ください。

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などに関する法律

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などが規定されています。青少年が公衆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などに努めましょう。

※23　規格名を分かりやすくするため、業界団体（Wi-Fi Alliance）が「Wi-Fi 6E」といった呼称を規定しています。
※24　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。
※25　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。

［参考資料］

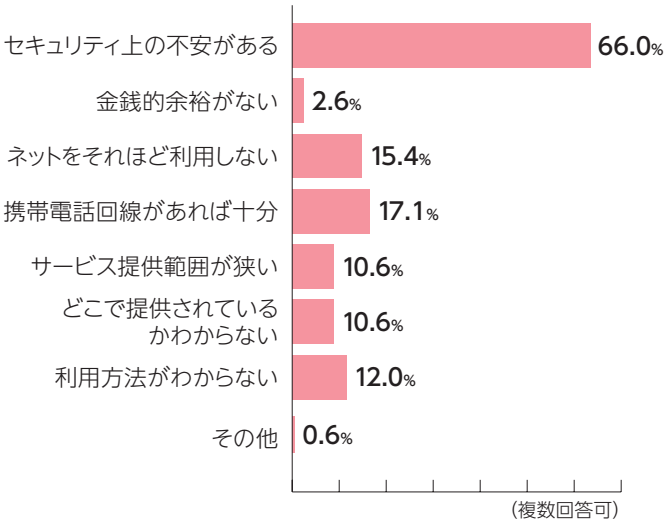
利用者・サービス提供者アンケート結果

本マニュアルが公衆Wi-Fiの提供に不安を感じている方々の参考となり、各種セキュリティ対策事項の実施率が向上していくことを期待しています。

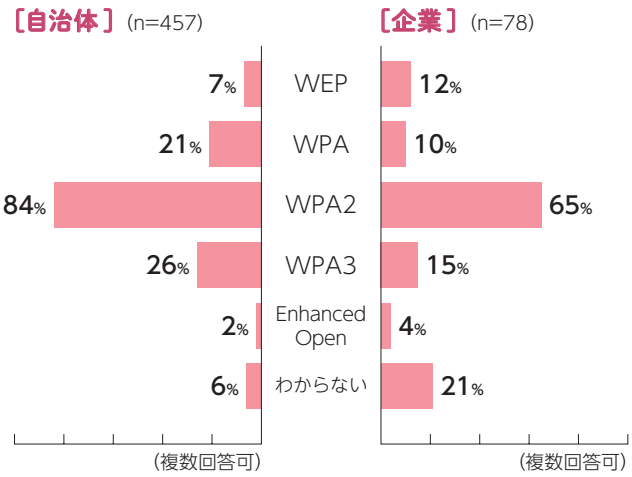
「令和5年度無線LANのセキュリティに関わる実態調査の請負業務」事業より作成。
無線LAN利用者実態調査期間：2024年3月5日～ 2024年3月8日調査数：1,422 (うち無線LAN利用者1,000をスクリーニング)
無線LAN提供者実態調査期間：2024年2月26日～ 2024年3月14日調査対象：地方自治体1,726団体および企業等714社に依頼

公衆無線LANを利用していない理由

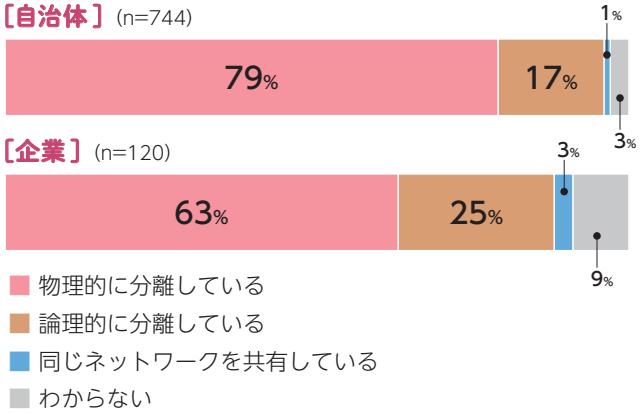
(n=12,235：未利用者)



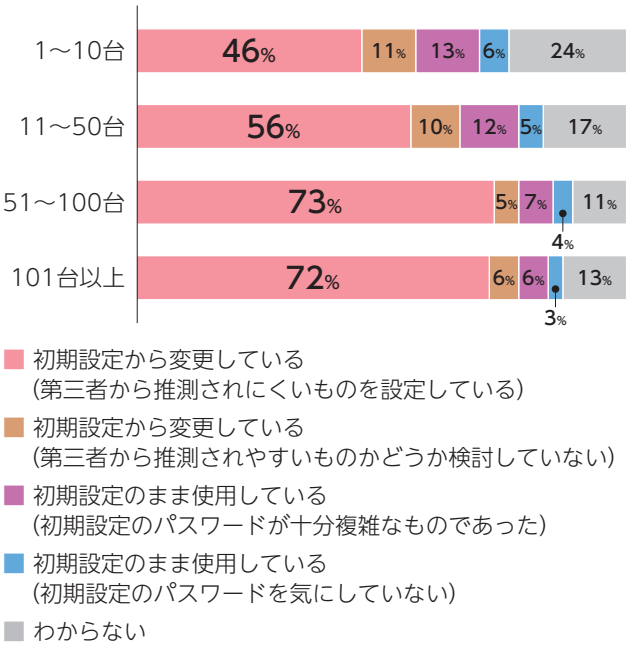
無線LANサービスの暗号化方式



業務用ネットワークとの分離



管理者パスワードの管理（導入規模ベース）



memo

総務省

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 wlan-security@ml.soumu.go.jp
ＵＲＬ https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/