令和７年２月版

公衆「Wi-Fi利用者」向け・簡易マニュアル・

公衆Wi-Fiの安全な利用に向けて

スマートフォンが普及し、公衆Wi-Fi環境の整備も進んできたことで、自宅だけではなく、外出先においても有料・無料を問わず多くの公衆Wi-Fiが利用可能となっています。
通信料金を気にせず、高速な通信を利用する手段として、公衆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。

本マニュアルは、公衆Wi-Fiの利用者に対し、安全なWi-Fiの利用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、本マニュアルでもその意味で使用しています。

総務省

［目次］

公衆Wi-Fi利用者向け簡易マニュアル

公衆Wi-Fiの安全な利用に向けて

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。本マニュアルでの呼び方をご紹介します。

本マニュアルにおける呼び方	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。

Chapter 1

[公衆Wi-Fiとは]

街中で「Wi-Fi（ワイファイ）」という言葉を見かける機会が増えてきました。そもそも公衆Wi-Fiとは、どのようなものでしょうか。詳しく知りたい人向けに、その概要を説明します。

1-1 公衆Wi-Fi って何だろう

Wi-Fiは、ケーブルを使わず無線（ワイヤレス）通信でデータをやりとりする仕組みの一つであり、その中でも外出先で誰もが使えるWi-Fiを公衆Wi-Fiと呼びます。Wi-Fiは職場や自宅のパソコンなどをワイヤレスでインターネットに接続する手段として普及し、スマートフォンやタブレットなどの普及により利用がさらに拡大しました。それに伴い、職場や自宅に限らず、空港、駅、ホテル、学校、図書館といった、さまざまな場所で使えるWi-Fiとして公衆Wi-Fiの提供が増えています。

公衆Wi-FiにはSSID（ネットワーク名）と暗号化キーを用いることで接続可能なものや、通信事業者などが提供するSIM認証※1により接続可能なもの、OpenRoaming※2に対応したものなどいくつか種類があります。本マニュアルではその中でもSSIDと暗号化キーを用いることで接続可能な公衆Wi-Fiを利用する際のセキュリティ対策などをご説明します。

1-2 公衆Wi-Fiを使うと、どんないいことがあるの？

公衆Wi-Fiが使われている主な理由は次のとおりです。

- 設定が簡単で、外出先で手軽にインターネットに接続できる※3。
- 携帯電話回線の通信料金（パケット通信量）を削減できる。
- 通信速度が速く※4、動画再生やアプリダウンロードに便利。

1-3 災害時にも活躍するWi-Fi

公衆Wi-Fiは災害時の通信手段としても活用されています。2011年の東日本大震災の際に、通信事業者が公衆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2024年の能登半島地震などの地震や風水害といった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公衆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、誰でも、暗号化キーを入力することなく接続して、安否確認などの情報の共有や入手に利用することができます※5。

※1　SIM認証はスマートフォンなどの端末に挿入されたSIMの情報をもとに行われる認証です。
※2　OpenRoamingは国際的な無線LANローミング基盤であり、一度設定するだけでOpenRoaming対応のアクセスポイントに接続可能になります。
※3　携帯電話会社が販売するスマートフォンでは、自社のWi-Fiサービスに接続できる設定があらかじめ行われている機種も多くなっています。
※4　Wi-Fiの通信速度は利用する規格や電波の状態、回線状況によって大きく変わります。
※5　ただし、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。そのため、情報入手のための利用にとどめるなど、利用にあたっては十分ご留意ください。災害時に限られた通信手段を譲り合って利用する観点からも、必要最小限の利用にとどめるようにしましょう。

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利用すると、通信内容が盗み見られたり（傍受）、ID・パスワードを盗用されて使われる（なりすまし）などの被害にあう危険性があります。

・脅威シナリオの例・

❶ 見知らぬ公衆Wi-Fiの利用

旅行中のAさんは、旅先で利用可能だった公衆Wi-Fiを利用しました。それまで利用したことのないSSID（ネットワーク名）でしたが、暗号化キー不要で接続できたので利用することにしました。

❷ ID・パスワードの安易な入力

公衆Wi-Fiの利用にあたりSNSでの認証が求められたため、SNSのIDとパスワードを入力しました。入力画面のURLはよく確認していませんでしたが、インターネット接続は問題なく利用できたため気にしませんでした。

❸ 悪意をもった第三者によるなりすまし被害

数日後、SNSに自分の名前で覚えのない誹謗中傷の投稿がされているのを見つけました。調査した結果、SNSのIDとパスワードが盗用されて、第三者のなりすましによる不正アクセスをされたことが分かりました。

Aさんが被害を受けた原因は何でしょうか。

それは、悪意をもって設置された偽の公衆Wi-Fiに接続してしまったことです。そのため、入力したSNSのIDとパスワードが盗まれてしまったのです。

このような被害を防ぐためには、

・接続する公衆Wi-Fiをよく確認する

・インターネットを利用する場合、正しいURLでHTTPS通信をしているか確認する

といったセキュリティ対策が重要です。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

[公衆Wi-Fiを使うときに気を付けるべきポイント]

3-1 接続する公衆Wi-Fiをよく確認しよう

誰もが使える公衆Wi-Fiを利用するときは、どのようなサービスなのか接続先をよく確認しましょう。

また、最近では偽の公衆Wi-Fiの存在が報告されています。いつも使っているSSID（ネットワーク名）の公衆Wi-Fiでも、不審な点がないか確かめる習慣をつけましょう。

少しでも不審な点があれば、利用を控える判断も必要です。

ポイント1 接続しようとしている公衆Wi-Fiを確認しよう

近くに掲示されているステッカーなどで、誰が提供しているどのようなサービスなのか、セキュリティ対策はどうなっているのかなどを確認してから接続しましょう。暗号化キーなしで接続可能な公衆Wi-Fiがあっても、提供者が不明のものや不審だと感じるものには接続しないようにしましょう。

また、利用するスマートフォンによっては無線LANへの自動接続機能がある場合があります。意図せず不審な公衆Wi-Fiへ接続してしまう可能性があるため、自宅や職場のWi-Fiなど日常的に利用するSSID以外は自動接続する設定を無効化しましょう。

ポイント2 接続先の名前（SSID）を確認しよう（偽の公衆Wi-Fiに注意しましょう）

接続しようとする公衆Wi-FiのSSID（ネットワーク名）が、提供者の案内しているものと同じか確認しましょう。

偽の公衆Wi-Fiが、SNSのログイン画面を模した偽の入力画面に誘導して、ID・パスワードなどの入力情報をだまし取る例が報告されています。よく知っている（使ったことがある）SSID（ネットワーク名）であっても、偽の公衆Wi-Fiが設置されていることがあります。

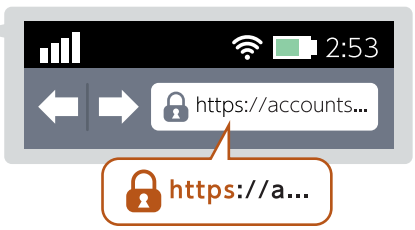
公衆Wi-Fiに接続して、ID・パスワードやメールアドレスなどの入力画面になった場合は、次の点を必ずチェックしましょう。

自分の端末から確認する場合

❶接続中のアクセスポイント名（SSID）
❷アクセスポイントの暗号利用状況

Android13搭載スマートフォン　iPhone（iOS16.6.1）

- **URLが「https://」で始まっているか、または、ブラウザに鍵マークが表示されているか。**
  （HTTPS通信については7ページを参照）



- **URLが正しいか（いつもと変わらないか）。**
  公衆Wi-Fi事業者のIDなどを入力する場合は事業者のURL、SNSのIDなどを入力する場合はSNSサイトのURLとなります。HTTPS通信をしていても、本物のURLに巧妙に似せた偽URLの場合があるため、URL全体を確認するようにしましょう。スマートフォンの場合、デフォルトではURL全体が表示されないことがあるため注意が必要です。

●**HTTPS通信のエラーが発生していないか。**

ブラウザの鍵マークの代わりに「！」マークが表示されたり、「接続が安全ではありません」などのエラーメッセージが表示されたりする場合は、正しいサイトではない可能性が高い※6ため、IDなどの入力は大変危険です。この現象は、通信が中断した場合にも発生することがあるので、ブラウザの再読み込みをする、ブラウザを再起動する、Wi-Fiを一旦OFFにして再びONにするなどしてやり直してみましょう。それでも同じ状況であれば、その公衆Wi-Fiを利用しない判断も必要です。

なお、公衆Wi-Fi事業者が提供する接続アプリの中には、偽の公衆Wi-Fiへ接続しないための対策がなされているものもあるため、これを使うことも一つの方法です。

インターネット利用時の一般的な注意事項ですが、ID・パスワードの使い回しをすると、万一だまし取られてしまった場合に被害が拡大してしまいます。使い回しは避けるようにしましょう。また、生体認証と組み合わせるなどの二要素認証が設定可能な場合は積極的に利用しましょう。

ポイント3 接続先のセキュリティ対策を確認しよう

公衆Wi-Fiの多くは最初の利用時に、サービス利用についての同意画面や認証画面などが出てきます。その中でWi-Fiのセキュリティについて説明されていますので、理解した上で利用することが重要です。

また、セキュリティ方式（詳細は以下のコラムを参照）は一般に「WPA3」または「WPA2※7」が望ましいとされています。「セキュリティ（暗号化）なし」や「WEP」と表示されている場合は、個人情報やオンラインサービスのログイン情報の入力などの周囲に見られてはいけない情報を扱うような利用は避け、通信内容が周囲に見られても構わない場合に限って利用しましょう。「WPA」や「WPA2」でも、暗号化キーが知られていると傍受される可能性があります（詳細は6ページ上のコラムを参照）。

コラム Wi-Fiセキュリティ方式※8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、なるべく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
	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。対応機器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※9も解消されている。
	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。
	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。

※6　Wi-Fi事業者の一部では、未認証状態で通信を行った場合に、正規の通信応答に代わって認証用ログイン画面を強制表示させる機能（キャプティブポータル）を利用しています。この場合に、ブラウザの「ホームページ」（起動時に最初にアクセスするページ）の設定が「https://」から始まるページになっていると、強制表示させる機能をブラウザがエラーと判断してしまうことがあります。

※7　「TKIP」と「AES」が選択できる場合は「AES」を選択しましょう（「TKIP」には脆弱性が発見されています）。

※8　セキュリティ方式は、利用する機器により“暗号化Protocol” “暗号化” “セキュリティ”など、表記が異なります。

※9　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 WPA2でも安心できない

誰もが使える公衆Wi-Fiには、WPA2で暗号化されているものも多くあります。WPA2にはその詳細方式が複数あり、費用をかけずに手軽に利用できるものが「WPA2パーソナル（WPA2-PSK）」という方式です。この方式は、自宅や個人での利用に限れば十分な安全性を持っています。

しかしながら、この方式の特徴として、接続する人全員が同じ暗号化キーを共有する必要があるため、不特定多数が利用する公衆Wi-Fiでは、利用者全員が暗号化キーを知っている状態にあります。そのため、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。このため、WPA2パーソナル（WPA2-PSK）方式の公衆Wi-Fiについては、暗号化されていない場合と同様に留意して利用する必要があります。

コラム 安全なWi-Fiセキュリティ方式

上のコラムで、公衆Wi-Fiにおいては、WPA2パーソナル（WPA2-PSK）方式は必ずしも安心できないとお伝えしましたが、以下に挙げるものは安全性が高い方式です。これらの方式が利用可能な場合は積極的に利用しましょう。なお、いずれもWi-Fiの無線区間のみの暗号化方式であることには留意してください。

- **携帯電話事業者が提供する公衆Wi-Fiのセキュリティ方式**

  携帯電話事業者が提供している公衆Wi-Fiの中には、SIM認証（EAP-SIM/EAP-AKA）というセキュリティ方式を用いているものがあります。IDなどを個別に配付する代わりに、SIMの情報を鍵として利用し、認証や暗号化を行います。対応しているスマートフォンは自動的に公衆Wi-Fiに接続するため、安全性と共に利便性も高くなっています。

- **公衆Wi-Fi向けの新しいセキュリティ方式**

  2018年に公衆Wi-Fi向けの新しいセキュリティ方式としてWi-Fi CERTIFIED Enhanced Openが発表されました。暗号化キーなしで接続でき、暗号鍵は個別に設定されるため、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、対応した機器が増えていくと考えられます。

- **企業向けのWi-Fiセキュリティ方式**

  一般利用者向けであるWPA2パーソナル（WPA2-PSK）やWPA3パーソナル（WPA3-personal）に対して、企業向けのWi-Fiセキュリティ方式としてWPA2エンタープライズ（WPA2-EAP）・WPA3エンタープライズ（WPA3-enterprise）があります。共通の暗号化キーを利用するWPA2パーソナル（WPA2-PSK）やWPA3パーソナル（WPA3-personal）と異なり、利用者ごとにIDなどを設定し、接続の際に利用者側とWi-Fiルーター側で相互に認証する方式です。認証の際に暗号鍵も個別に設定されます。利用者からWi-Fiルーターに対する認証も行うため、偽の公衆Wi-Fiへ接続する心配もありません。個別にIDなどを配付し設定する必要があるため、これらの企業向けのWi-Fiセキュリティ方式は不特定多数が利用する公衆Wi-Fiサービスではあまり利用されていません。

コラム 一度の登録でシームレスに接続可能なOpenRoaming

OpenRoaming※10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。また一度OpenRoamingの利用登録をすることで、全世界のOpenRoaming対応の公衆Wi-Fiを設定なしで利用可能となります。国内では東京や大阪をはじめとした都市圏で導入が進んでおり、対応する公衆Wi-Fiも順次拡大される予定となっています。

※10　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/)

3-2 正しいURLでHTTPS通信しているか確認しよう

Wi-Fiの利用時に限らず、インターネットの通信はさまざまな事業者を経由することもあり、通信内容が必ずしも保護されるとは限りません。通信内容をどこかで盗み見られたり、改ざんされたりする可能性があります。

そこで、通信内容を守るために利用されるのがHTTPS通信※11です。

Wi-Fiの暗号化も重要ですが、守られるのは無線区間だけです。Wi-Fiルーターから先は守られません。HTTPS通信ならアクセス先のサーバまですべて暗号化されるので、仮にWi-Fiが暗号化されていない場合でも、悪意をもった第三者から通信内容を保護することが可能です（詳細は8ページのコラムを参照）。

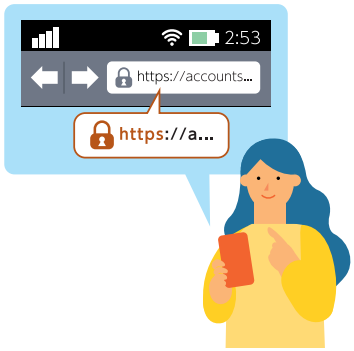
上記はWi-Fiを使わない場合も含め、インターネット利用時の一般的な注意事項ですが、Wi-Fiは電波を利用している以上、周囲の第三者が容易に受信できる状況となるためリスクが高く、HTTPS通信は必須と考えましょう。

ポイント1 ブラウザのURL入力欄を確認しよう

ブラウザを開いてWebサイトを閲覧するときは、ブラウザのURL入力欄（アドレスバー）に注目しましょう。

「https://」から始まるWebサイトにアクセスすると、HTTPS通信が開始され、ブラウザに鍵のアイコンが表示されます。ブラウザによっては、アドレス欄をクリックすることで鍵マークやURL全体が表示されるものもあります。多少手間がかかっても、確認を怠らないようにしましょう。

アドレスが「http://」で始まっていたり、ブラウザに「！」アイコンや「保護されていない通信」、「安全ではありません」などと表示されたりするときは、Webサイトとの間の通信が適切に暗号化されていません。傍受の危険があるため、こうしたWebサイトでパスワードや個人情報を入力するのは危険です。



ポイント2 ブラウザ以外での通信も暗号化されているか確認しよう

パソコンなどで、メールソフトでのメール送受信（SMTP・POP・IMAP）やファイル転送（FTP）を利用する場合は、暗号化のための設定変更（SMTPであればSMTPsに変更するなど）を行うようにしましょう。よく分からない場合や設定を変更することで利用に差し支える場合は、外出先ではブラウザからWebメールを使うなど、利用をブラウザのみに限定することも一つの方法です。

スマートフォンで、ブラウザ以外のアプリから通信を行う場合は、アプリが行う通信がHTTPS 通信かどうかを利用者が判断することは困難ですが、公式ストアからインストール可能なアプリにHTTPS通信を義務付ける動きもあるため、大半のアプリはHTTPS通信を行っています。心配な場合は、外出先のWi-Fiではブラウザの利用だけにとどめることも一つの方法です。

※11　Webページのアクセスに用いられる暗号化されていないHTTP通信を、TLS（SSL）というセキュリティ技術により暗号化したもの。

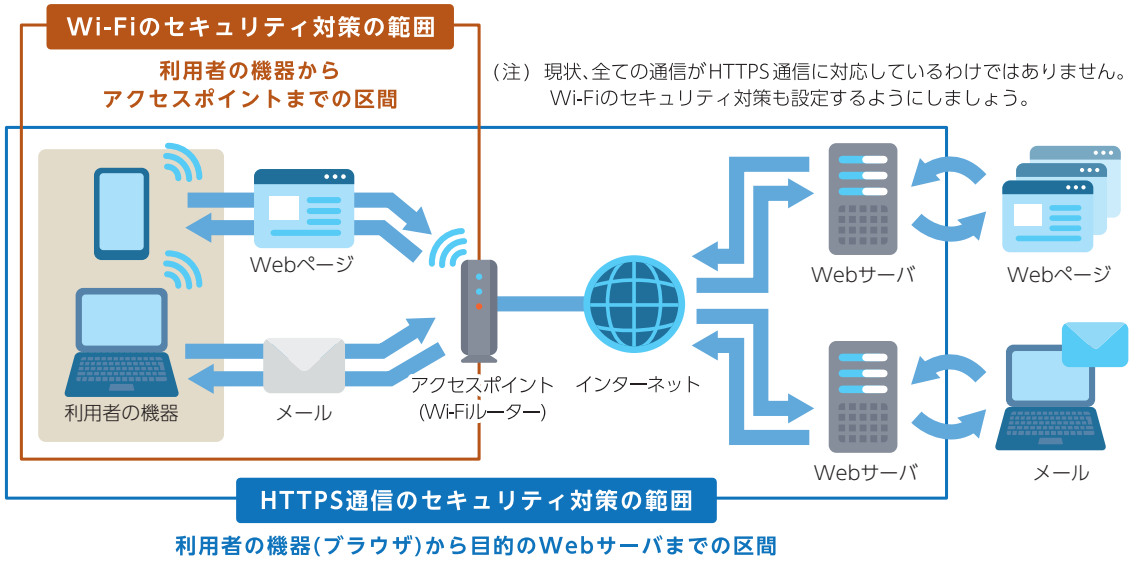
3-3 パソコンの共有設定に注意しよう

オフィスや自宅用のWi-Fiでは、同じWi-Fiルーター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ないため、公衆Wi-Fi提供者には端末同士の通信を禁止することが推奨されています。

すべての公衆Wi-Fiが端末同士の通信を禁止しているとは限らないため、利用者としてもパソコンを公衆Wi-Fiに接続して利用する際には共有フォルダの無効化や認証機能の有効化などの対策を行いましょう。

コラム HTTPS通信の暗号化の範囲とは

下の図は、Webページ閲覧時の通信のやりとりを表しています。Wi-Fiによる暗号化範囲は、茶枠で囲んだ、利用者の機器からWi-Fiルーターまでの区間に限られます。一方、HTTPS通信による暗号化範囲は、青枠で囲んだ、利用者の機器（ブラウザ）から目的のWebサーバまでの区間です。HTTPS通信を使うことで、Wi-Fi利用区間を含め、インターネット上の第三者が通信内容を見ることができなくなります。



[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 ※12	使用する周波数帯 ※13	最大伝送速度 ※14
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

※12　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。
※13　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。
※14　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。

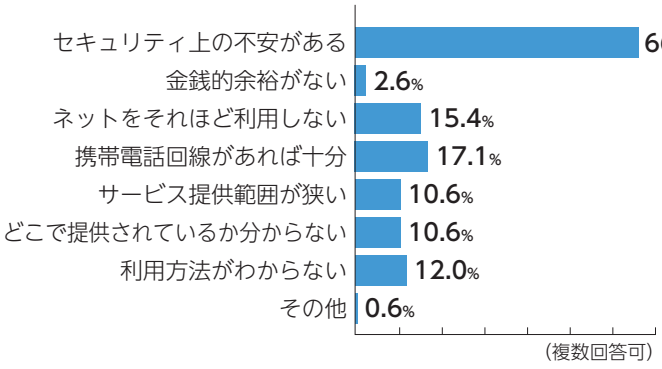
利用者アンケート結果

本マニュアルがWi-Fiの利用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。
（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）

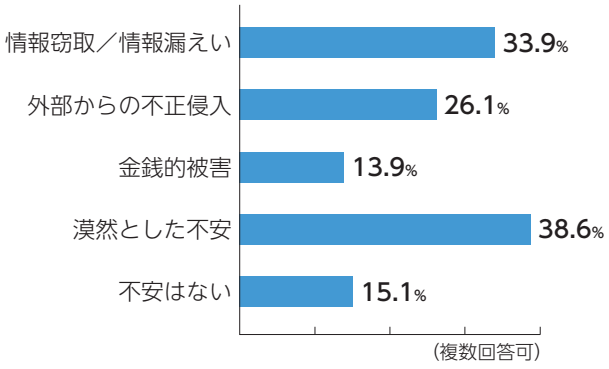
公衆無線LANを利用していない理由

（n=12,235：未利用者）



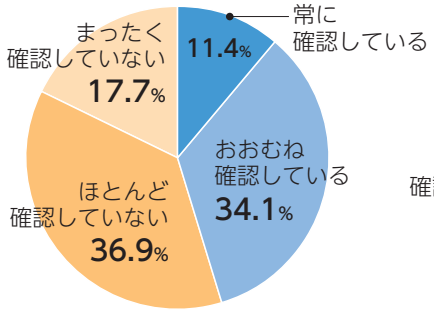
公衆無線LANでのセキュリティ上の不安

（n=514：公衆無線LANの利用者）



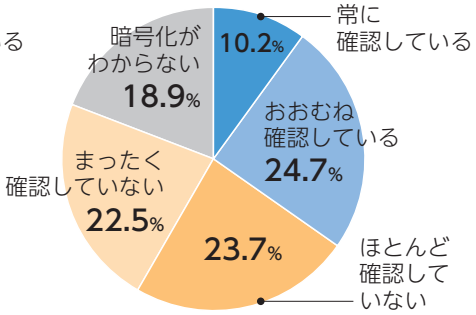
公衆無線LAN利用時のSSID確認

（n=502：公衆無線LANの利用者）



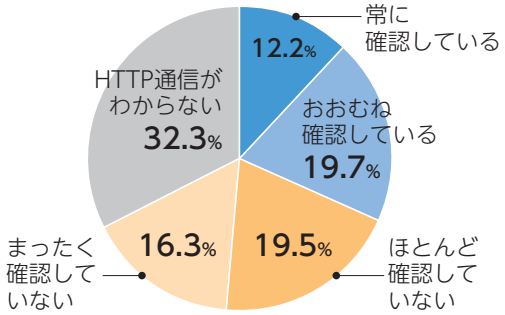
公衆無線LAN利用時の暗号化確認

（n=514：公衆無線LANの利用者）



公衆無線LAN利用時のHTTPS通信確認

（n=502：公衆無線LANの利用者）



memo

総務省

本マニュアル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/