Wi-Fi利用者向け簡易マニュアル

～安全なWi-Fiの利用に向けて～

令和2年5月版

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、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、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。

セキュリティ対策の３つのポイント

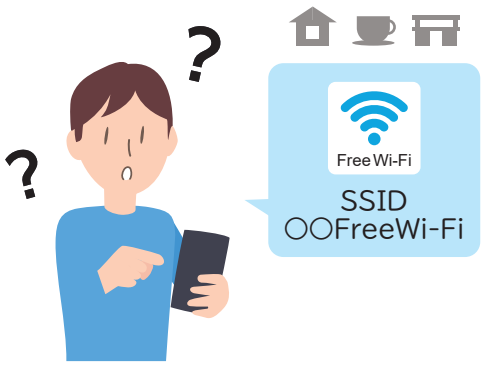
Wi-Fiを安全に利用するためには、どうすれば良いのでしょうか？ここでは、Wi-Fiのセキュリティ対策で欠かせない３つのポイントを紹介します。しっかり守れているかをチェックしてみましょう。

ポイント１ 接続するアクセスポイントをよく確認しよう （詳細は５ページを参照）

外出先で誰でも使えるWi-Fiを利用するときは、接続先をよく確認しましょう。近くに掲示されているステッカー等で、誰が提供しているどのようなサービスなのか、また、接続先の名前（SSID）やセキュリティ対策はどうなっているのかを確認してから利用しましょう。

Wi-Fiを利用する際に、メールアドレスやID・パスワードの入力を求められた場合は、正しい入力画面か確認しましょう。最近では偽のアクセスポイントが報告されています。いつも使っている名前（SSID）のWi-Fiでも、利用時の入力画面ではその都度、URLや鍵マークを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、利用をあきらめる決断も必要です。



ポイント２ 正しいURLでHTTPS通信をしているか確認しよう （詳細は７ページを参照）

Wi-Fiに限らず、インターネットでの通信内容は、いつどこで盗み見られているか分かりません。URLが「https://」から始まるHTTPS通信を使えば、手元の端末から通信先のWebサイトまでが暗号化されるため、通信内容は保護されます。

特にパスワードや個人情報を入力する場合は、URLや鍵マークを見てHTTPS通信を利用しているか確認するようにしましょう。

また、巧妙に似せた偽サイト（偽URL）による被害も報告されていますので、URL自体も正規の事業者のものか必ず確認し、少しでも不審な点があれば、アクセスしないようにしましょう。

ポイント３ 自宅に設置している機器の設定を確認しよう （詳細は９ページを参照）

自宅に設置しているWi-Fiルーター等の機器について、購入時に設定されている機種共通のパスワードをそのまま使い続けると、第三者に勝手に使われたり、機器を乗っ取られたりする可能性があり危険です。

Wi-Fiの暗号化のためのパスワード※1だけでなく、機器を設定するための管理用パスワードについても、第三者に推測されにくいものが設定されているか確認しましょう。

また、機器のファームウェアも最新の状態にしておきましょう。

※1　Wi-Fiを暗号化するための鍵は「暗号化キー」や「パスフレーズ」等と様々に呼ばれますが、本マニュアルでは「パスワード」と呼びます。

1 Wi-Fiの概要を知っておこう

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Wi-Fiとは、どのようなものなのか？詳しくはわからないという方向けにその概要を説明します。

1-1. Wi-Fi ってなんだろう?

Wi-Fiは、ケーブルを使わず無線通信（ワイヤレス）でデータをやり取りする仕組みのひとつです。

当初は職場や家庭のパソコン等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ましたが、スマートフォンやタブレット等の普及により利用が拡大しました。それに伴い、職場や家庭に限らず、空港、駅、ホテル、学校、図書館といった、さまざまな場所で利用できる環境が増えてきています。

1-2. Wi-Fiを使うと、どんな良いことがあるの?

主にスマートフォンでWi-Fiが使われている理由は次のとおりです。

- 設定が簡単で、家庭でも外出先でも手軽に接続できる。※2
- 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※3、動画再生やアプリダウンロードが便利。

1-3. 災害時にも活躍するWi-Fi

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Wi-Fiサービス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、誰でも、パスワードを入力することなく接続して、安否確認等の情報の共有や入手に利用することができます。※4

※2　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。

※3　Wi-Fiの通信速度は利用する規格や電波の状態、混雑状況によって大きく変わります。

※4　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、情報入手等のための利用にとどめるなど、利用に当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。

2 Wi-Fiセキュリティに関する危険事例

Wi-Fiのセキュリティ対策を行わずに利用した場合、通信内容が盗み見られたり（盗聴）、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。

事　例

(1) 見知らぬアクセスポイントの利用

旅行中のＡさんは、旅先でたまたま利用可能であったWi-Fiを利用しました。利用したことのないアクセスポイント名（SSID）でしたが、パスワード入力不要で簡単に接続できたので、利用することにしました。

(2) ID・パスワードの安易な入力

接続したところ、利用に当たってはSNSでの認証が必要であると求められたため、SNSのID・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。

(3) 悪意の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無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・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わかりました。

今回のＡさんが受けた被害の原因は何でしょうか。

それは、悪意で設置されたアクセスポイントに接続してしまい、入力したSNSのID・パスワードが盗まれてしまったのです。入力画面が偽物だったのです。

このような被害を防ぐためには、

・接続するアクセスポイントをよく確認する

・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。外出先だけではなく自宅でのWi-Fi利用の場合も含めて、こうした危険を回避するために気を付けていくべき具体的な内容について、次のページから詳しく説明します。

3 接続するアクセスポイントをよく確認しよう（外出先でのWi-Fi利用開始時の注意点）

外出先でWi-Fiの利用を開始しようとするときは、接続先をよく確認するようにしましょう。

ポイント 接続しようとしているWi-Fiサービスを確認しよう。

近くに掲示されているステッカー等で、誰が提供しているどのようなサービスなのか確認してから接続しましょう。パスワードなしで接続可能なアクセスポイントがあっても、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。

ポイント 接続先の名前（SSID）を確認しよう。（偽アクセスポイントに注意しましょう。）

＜自分の端末から確認する場合＞

接続しようとするアクセスポイントの名前（SSID）が、提供者が案内しているものと同じか確認しましょう。（右図の❶部分）

悪意のあるアクセスポイントが、偽の入力画面に誘導して、ID・パスワード等の入力情報をだまし取る例が多く報告されています。よく知っている（使ったことがある）名前（SSID）でも、偽のアクセスポイントが設置されていることもあります。アクセスポイントに接続して、ID・パスワードやメールアドレス等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。

▶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）

Wi-Fi事業者のID等を入力する場合は事業者のURL、SNSのID等を入力する場合はSNSサイトのURLとなります。https（鍵マーク）でも、本物のURLに巧妙に似せた偽URLの場合があるため、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」等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※5ので、ID等の入力は大変危険です。この事象は、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、そのアクセスポイントを利用しない決断も必要です。

なお、Wi-Fi事業者が公式に提供する接続アプリでは、偽のアクセスポイントへ接続されないような対策がなされているものもありますので、これを使うのもひとつの方法です。ただし、公式ではない接続アプリには信頼性の低いものがあるため、利用は控えましょう。

そして、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してしまうと、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。

※5　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。

ポイント　接続先のセキュリティ対策を確認しよう。

Wi-Fiサービスの多くは最初の利用時に、サービス利用に係る同意画面や認証画面等が出てきます。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９ページのコラムを参照）が「セキュリティ（暗号化）なし」や「WEP」と表示されている場合には、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、パスワードが知られていると傍受される可能性があります。（詳しくは下のコラムを参照）

コラム　WPA2でも安心できない

外出先で誰でも使えるWi-Fi（公衆Wi-Fi）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、家庭や個人での利用に限れば十分な安全性を持った方式です。

しかしながら、この方式の特徴として、アクセスポイントに接続する人全員が同じパスワード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、利用者全員がパスワードを知っている状態にあります。パスワード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、パスワードが分かっていれば、同じ名前（SSID）とパスワードを設定することで、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。

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、以下に挙げた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留意してください。

●WPA2エンタープライズ（WPA2-EAP）

共通のパスワードを利用するWPA2パーソナル（WPA2-PSK）方式とは異なり、利用者ごとにID等を設定し、接続の際に利用者側とアクセスポイント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。利用者からアクセスポイントに対する認証も行うため、偽アクセスポイントへ接続する心配もありません。しかしながら、個別にID等を配付し設定する必要があるため、不特定多数が利用するWi-Fiサービスでは利用が難しい状況です。

●SIM認証（WPA2-AKA）

携帯電話事業者が提供している方式です。WPA2エンタープライズ（WPA2-EAP）の一種ですが、ID等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では、自動でWi-Fiに接続できるため、安全性と共に利便性も高くなっています。

●Wi-Fi CERTIFIED Enhanced Open

2018年に発表された新しい方式です。パスワードなしで接続でき、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、対応した製品が増えていくと考えられます。

4 正しいURLでHTTPS通信をしているか確認しよう（外出先でのWi-Fi利用時の注意点）

Wi-Fiの利用時に限らず、インターネットの通信は、海外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※6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。アクセスポイント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全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、悪意の第三者から通信内容を保護することが可能です。（詳細は次ページのコラムを参照）

Wi-Fiを使わない場合でも共通の注意事項となりますが、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 ブラウザのURL入力欄を確認しよう。

ブラウザを開いてWebサイトの閲覧をしようとするときは、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。

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」と表示されたりするときは、Webサイトとの間の通信が安全に暗号化されていません。盗聴の危険があるため、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。

近年では、Webメールやショッピングサイトといった重要な情報を扱うWebサイトはほぼHTTPS通信に対応しています。Webサイトを利用するときは、Webサイトとの通信が暗号化されているかどうかを確認する習慣をつけましょう。

また、本物のURLに巧妙に似せた偽URLの可能性があるため、URL（特にドメイン部分）を併せて確認して、偽のWebサイトに騙されないようにしましょう。

ポイント ブラウザ以外での通信でも暗号化されているか確認しよう。

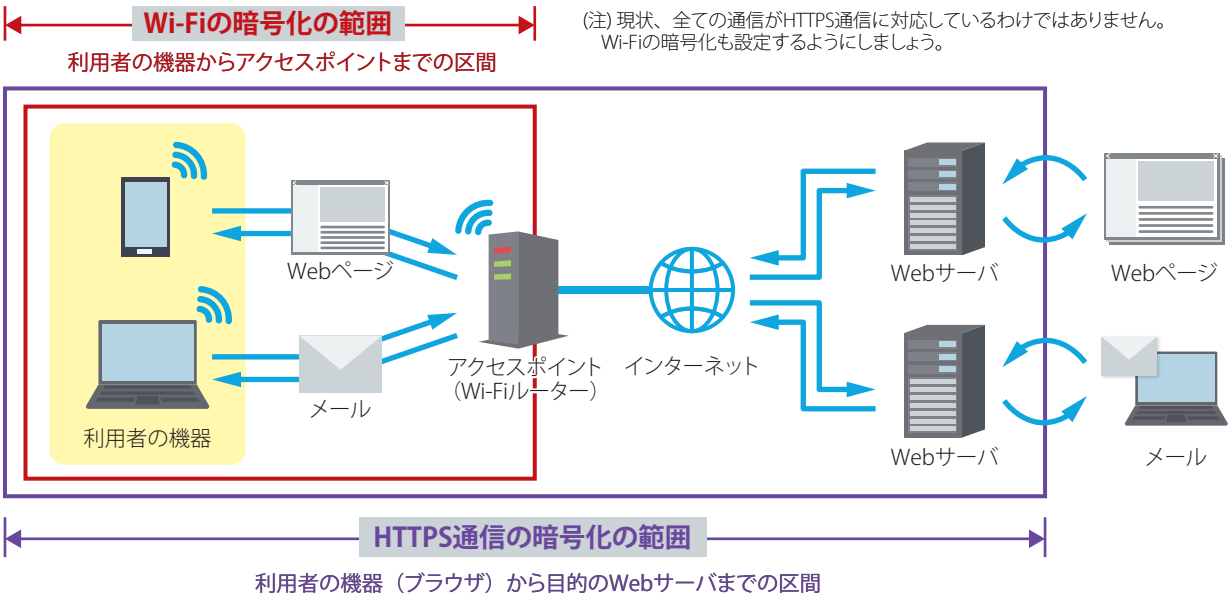
パソコン等で、メールソフトでのメール送受信（SMTP・POP・IMAP）やファイル転送（FTP）を利用する場合は、暗号化のための設定変更（SMTPであればSMTPsに変更するなど）を行うようにしましょう。よく分からない場合は、外出先ではブラウザからWebメールを使うなど、利用をブラウザのみに限定することもひとつの方法です。

また、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ひとつの方法です。

※6　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。

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、赤枠で囲んだ、利用者の機器からアクセスポイント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、紫枠で囲んだ、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。

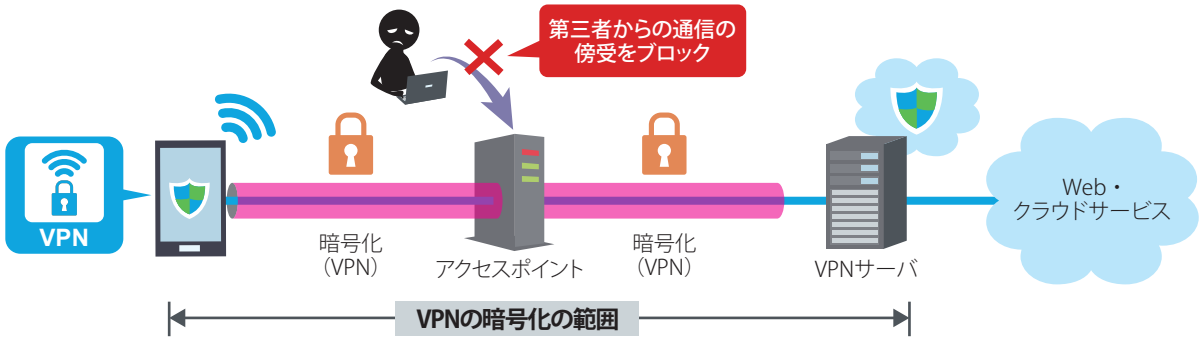


コラム　通信をまるごと暗号化するVPN

外出先のWi-Fiを安全に利用するのであれば、VPNを活用するのもひとつの方法です。信頼できる接続先や接続後の認証手続きを簡略化したり、より高度なセキュリティ機能を使って接続したりできます。

● VPNとは

VPNを利用すると、スマートフォンやパソコン等の機器とVPNサーバとの間の通信がまるごと暗号化されます。このため、ブラウザによるWebページの閲覧に限らず、全ての情報が安全にやりとりできます。



● VPNを使うには

職場や自宅のルーターにVPN機能があれば、設定することでVPNサーバとなります。また、通信事業者やセキュリティ対策ベンダー等が提供するVPNアプリを使うと、事業者が設置するVPNサーバが利用できます。いずれも、設定はやや難しく、中上級者向けとなります。なお、VPNサーバから先は暗号化されないため、VPNアプリを使う場合は信頼できる事業者を選ぶことが重要です。※7

※7　悪意のある者が提供するVPNアプリによって、VPNサーバで通信内容が盗まれるといった事例も報告されています。

5 自宅に設置している機器の設定を確認しよう（自宅でのWi-Fi利用の注意点）

自宅でWi-Fiを利用する場合は、設置しているWi-Fiルーター等の機器の設定を確認しましょう。

ポイント セキュリティ方式※8は「WPA2」を選択しよう。

Wi-Fiのセキュリティ方式（詳細は下のコラムを参照）は、「WPA2」にしましょう※9。

WPA2が複数方式ある場合は、「WPA2パーソナル（WPA2-PSK）」を設定しましょう。また、「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。）

ポイント パスワードは第三者に推測されにくいものにしよう。

Wi-Fiの暗号化のためのパスワードは、初期設定として一台ごとに固有のものが割り振られている場合が多いですが、簡単なものが設定されている場合は、第三者に推測されにくいものに変更しましょう。

また、Wi-Fi機器を設定するためのパスワード（管理用パスワード）についても、同様に第三者に推測されにくいものにしましょう。

初期設定が機種共通のパスワードで、そのまま使用している場合は、第三者に侵入される可能性もあります。速やかに変更しましょう。

ポイント ファームウェアを最新の状態にしよう。

機器のファームウェア（ソフトウェア）に脆弱性が生じた場合は、メーカーから更新版が提供されます。最新のファームウェアに更新（アップデート）してセキュリティを保ちましょう。新しい機種では自動更新が可能となっている機種も多いため、自動更新設定を有効にしておくことも推奨されます。

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が使われています。WEP等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
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。
	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。
弱	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 (暗号化)なし	通信が暗号化されず、だれでも接続可能。

※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 " 等、表記が異なります。
※9　アクセスポイントと接続機器がどちらもWPA3に対応している場合は、WPA3に設定しましょう。

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。

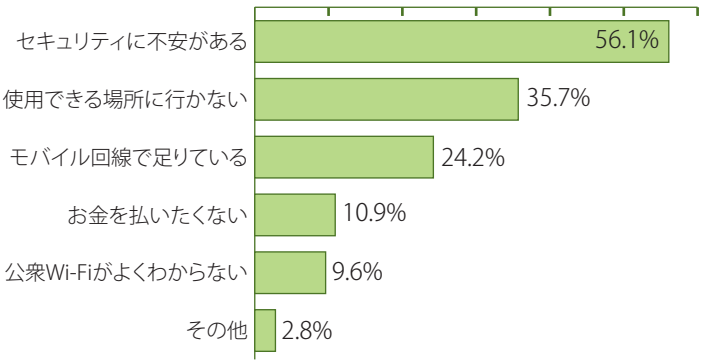
利用者アンケート結果

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））

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。

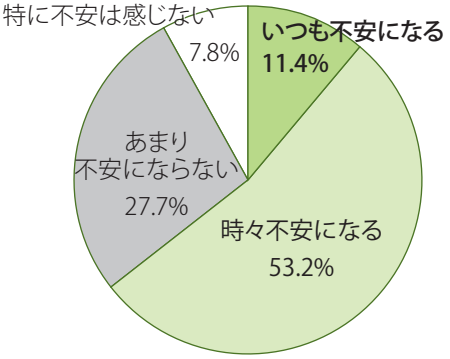
公衆Wi-Fiを利用しなかった理由

（n=16,473：現在未利用者）



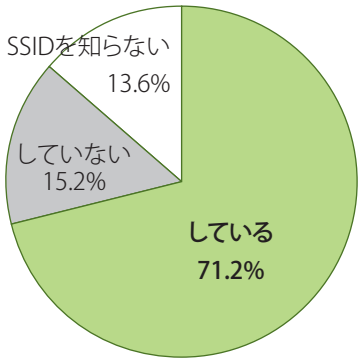
公衆Wi-Fiで不安を感じるか

（n=1,392：公衆Wi-Fi利用者）



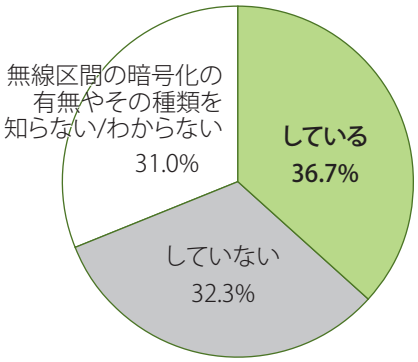
公衆Wi-Fi利用時のSSID確認

（n=1,392：公衆Wi-Fi利用者）



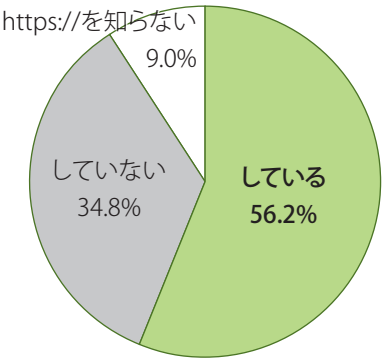
公衆Wi-Fi利用時の暗号化確認

（n=1,392：公衆Wi-Fi利用者）



公衆Wi-Fi利用時のhttps確認

（n=1,392：公衆Wi-Fi利用者）



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