令和７年２月版

自宅「Wi-Fi利用者」向け・簡易マニュアル・

自宅Wi-Fiの安全な利用に向けて

当初Wi-Fi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。
通信速度が速く、携帯電話回線の通信料金（パケット通信量）を削減できる手段としてWi-Fiは大変便利ですが、自宅に設置している機器の設定が適切でないと、第三者に勝手に利用さ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。

本マニュアルは、自宅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］

自宅Wi-Fi利用者向け簡易マニュアル

自宅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。
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

[自宅Wi-Fiとは]

自宅で「Wi-Fi（ワイファイ）」を利用する機会が増えてきました。そもそも自宅Wi-Fiとは、どのようなものなのでしょうか。詳しく分からないという人向けに、その概要を説明します。

1-1 自宅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す。

当初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。

本マニュアルは、自宅で用いるWi-Fiを対象にしています。

1-2 自宅Wi-Fiを使うと、どんないいことがあるの？

自宅でWi-Fiが使われる主な理由は次のとおりです。

- 設定が簡単で、自宅で手軽にインターネットに接続できる。
- 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※1、動画再生やアプリダウンロードに便利。

※1　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。

Chapter 2

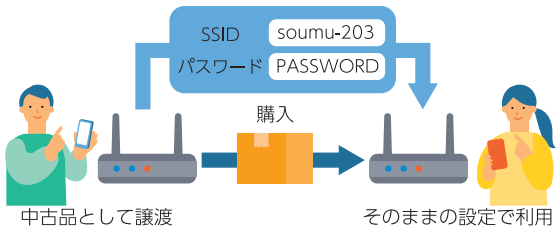
［自宅Wi-Fiに潜む脅威・リスク］

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）、第三者に不正利用されたりす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・

❶ Wi-Fiルーターをそのままの設定で利用

Aさんは、自宅用としてWi-Fiルーターを中古で購入しました。利用にあたって特にWi-Fiルーターの設定変更などは行わず、自宅のLANポートに接続し、Wi-Fiルーターに記載の暗号化キーを入力することで利用を始めました。

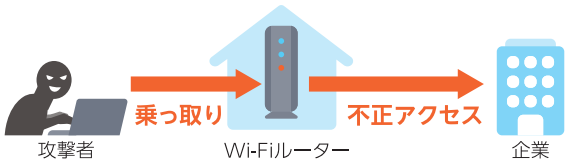


❷ ○×社へのサイバー攻撃を行ったと疑われる

数日後、○×社へのサイバー攻撃について警察から連絡がありました。サイバー攻撃の容疑者としてAさんが疑われているとのことです。

❸ 悪意をもった第三者により自宅Wi-Fiが犯罪行為に悪用されていた

調査した結果、AさんのWi-Fiルーターが悪意をもった第三者に乗っ取られて犯罪行為に利用されたことが分かりました。Aさんの疑いは晴れましたが、Aさんは調査への協力で多くの時間と労力を割く結果となりました。



このような事態となった原因は何でしょうか。

それは、Wi-Fiルーターを中古で購入したのに初期化をせずに、そのままの設定で利用してしまったことです。そのため、悪意をもった第三者に不正利用されたのです。

このような被害を防ぐためには、

・中古でWi-Fiルーターを入手した場合には利用前に初期化を行う
・ファームウェアを最新のものに更新する
・安全なセキュリティ方式※2を選択する
・パスワード（暗号化キー・管理用パスワード）を第三者から推測されにくいものに変更する

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。

※2　セキュリティ方式は、利用するWi-Fiルーターにより“暗号化Protocol” “暗号化” “セキュリティ”等、表記が異なります。

Chapter 3

［自宅Wi-Fiを使うときに気を付けるべきポイント］

自宅でWi-Fiを利用するときは、設置しているWi-Fiルーターの設定を確認しましょう。

3-1 セキュリティ方式は「WPA2またはWPA3」を選択しよう

Wi-Fiのセキュリティ方式（詳細は以下のコラムを参照）は、「WPA2」または「WPA3」にしましょう※3。

複数の方式がある場合は、「WPA2パーソナル（WPA2-PSK）」または「WPA3パーソナル（WPA3-personal）」を設定しましょう。また、「WPA2」を利用する際に「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※4が発見されています）。

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や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のものに更新することで安全に利用することが可能。
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。
無	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。

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。そのうちの一部は古いゲーム機などのためのものであり、古い暗号化方式が設定されている場合があります。それぞれの必要性を確認し不要な場合は停止し、必要な場合は適切な設定に変更するようにしましょう。

3-2 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暗号化のための暗号化キー（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のですが、簡単なものが設定されている場合は、安全なもの※5に変更しましょう。

また、Wi-Fiルーターを設定するための管理用パスワードについても、同様に安全なものに変更しましょう。

※3　Wi-Fiルーター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。
※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。
※5　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/end_user/general/01/）

初期設定が機種共通の管理用パスワード※6で、そのまま使用している場合は、第三者に乗っ取られる可能性があります。速やかに変更しましょう。

3-3 サポート期限内のWi-Fiルーターを利用しよう

世の中のWi-Fiルーターにはサポート期限が設定されているものがあります。この期限を過ぎるとそのWi-Fiルーターに関する問い合わせやファームウェアの更新などの対応がされなくなってしまいます。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、サイバー攻撃を受けるリスクが高まります。

Wi-Fiルーターのサポート期限はWi-Fiルーターのメーカーのホームページなどで確認可能※7です。利用しているWi-Fiルーターのサポート期限を把握し、サポート期限が切れている場合はWi-Fiルーターの買い替えを検討しましょう。

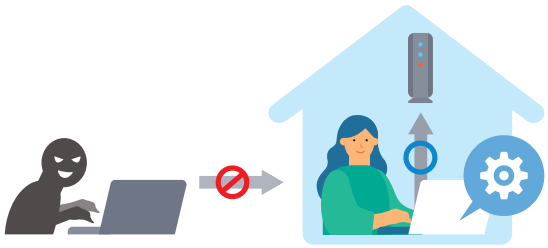
3-4 ファームウェアを最新の状態にしよう

Wi-Fiルーターのファームウェア（ソフトウェア）に脆弱性が生じたときは、メーカーから更新版が提供されます。ファームウェアを最新のものに更新（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ことも多いため、自動更新設定※6を有効にしておくことを推奨します。

3-5 Wi-Fiルーターの設定を定期的に確認しよう

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※8。

また、第三者にWi-Fiルーターを乗っ取られてしまった場合、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か、定期的に確認しましょう。



※6　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。

※7　「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。

※8　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/）

- **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自宅の外からWi-Fiルーターを経由してインターネットに接続できるようになるため、第三者によるWi-Fiルーターを踏み台とした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、インターネットからのアクセスが容易になり、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**※9

  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。

- **自動設定機能**※10

  対象のボタンを押すことで、無線接続やSSID（ネットワーク名）、暗号化キーなどの設定を自動で行うことができ、簡単に端末をWi-Fiルーターに接続できる機能です。暗号化キーを変更していたとしても本機能を用いることで接続が可能となるため家に人を招く場合などは注意が必要となります。

- **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。

- **DMZ機能**

  外部からの通信を特定の機器に転送する機能です。外部にWebサーバを公開する際などに利用することがあります。DMZ設定をした機器はインターネット側から見えるため、適切な対策を取らないと攻撃を受ける危険性が高まります。

これらの使わない機能が有効になっていた場合や、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のものに更新する（5ページ参照）
・パスワードを変更する（4ページ参照）

といった対策を行いましょう。

コラム　SSID（ネットワーク名）から身元を特定されることも

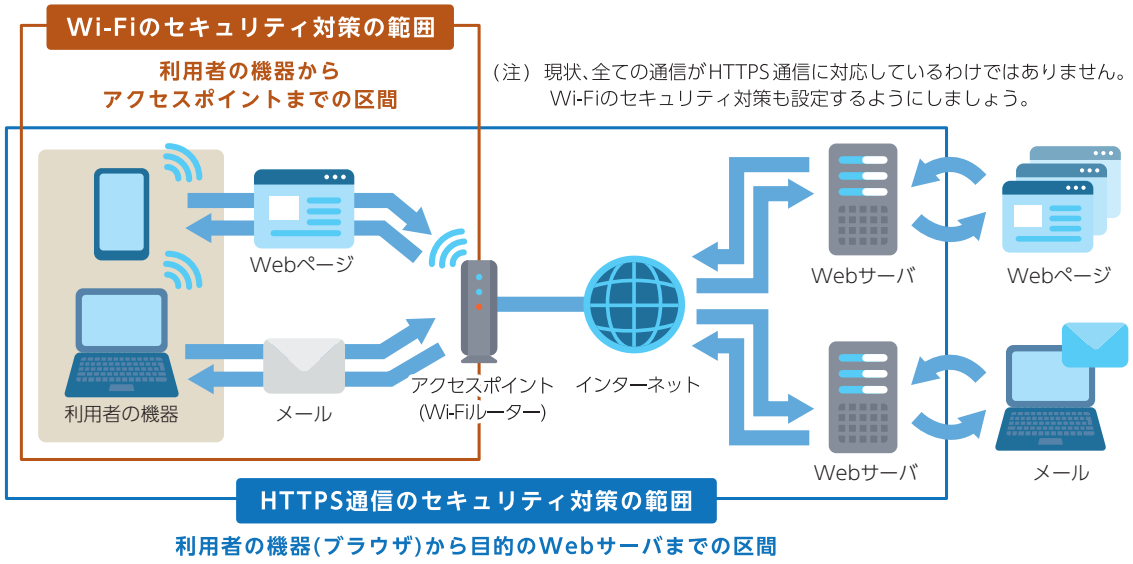
自宅で利用するWi-Fiが、自宅の外でも表示され、そのSSIDから身元が特定される事例もあります。電波の届く範囲にいればSSIDは誰でも見ることができるため、SSIDを変更する場合は、名前やマンションの部屋番号など身元の特定につながるような名称にしないよう注意しましょう。

また、近年はスマートフォンなどのテザリング※11機能を用いて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機会も増えています。スマートフォンの機種によっては、登録しているスマートフォン名がそのままSSIDとして設定される場合があります。氏名や電話番号などを設定していると個人情報が周りに公開されることになるため、利用の際は注意しましょう。

※9　インターネットからルーター（管理画面）への接続機能はメーカーによって機能名が異なります。
※10　自動設定機能はメーカーによって機能名が異なります。
※11　スマートフォンなどの端末を持ち運び可能なWi-Fiルーターのように利用し、その端末と接続された機器をインターネットに接続できる機能です。テザリングのほかにインターネット共有と呼ばれることもあります。

コラム HTTPS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。



コラム 電波の出力調整

Wi-Fiルーターが発する電波の出力を上げると、遠くの部屋まで電波が届きますが、その分、家の外にも電波が届いてしまう可能性があります。自宅の外から不正に利用されないよう、自宅内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※12。電波の出力を自動調整してくれるWi-Fiルーターもあります。

コラム 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）がある場合は、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※13を実施し、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。

※12　Wi-Fiの電波が家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。

※13　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。

[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 ※14	使用する周波数帯 ※15	最大伝送速度 ※16
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

※14　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。
※15　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。
※16　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。

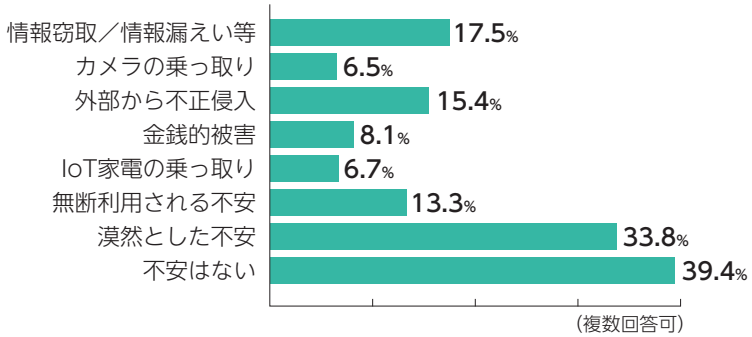
利用者アンケート結果

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）

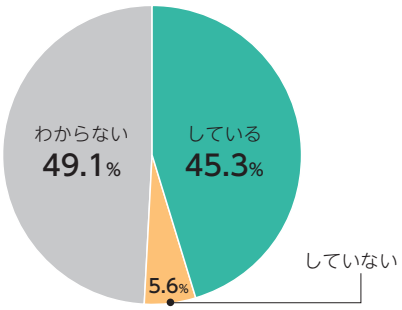
自宅無線LANでのセキュリティ上の不安

（n=961：自宅無線LANの利用者）



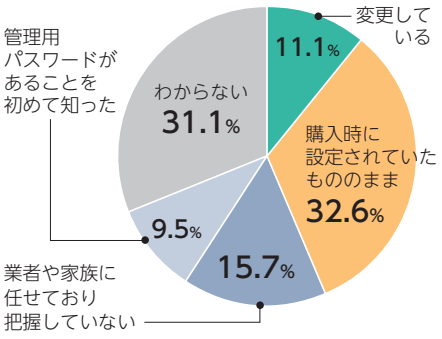
自宅無線LANの暗号化

（n=961：自宅無線LANの利用者）



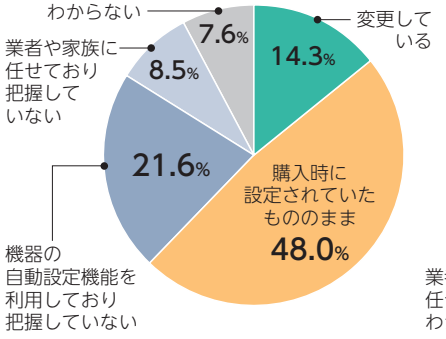
自宅無線LANの管理用パスワード

（n=961：自宅での無線LAN利用者）



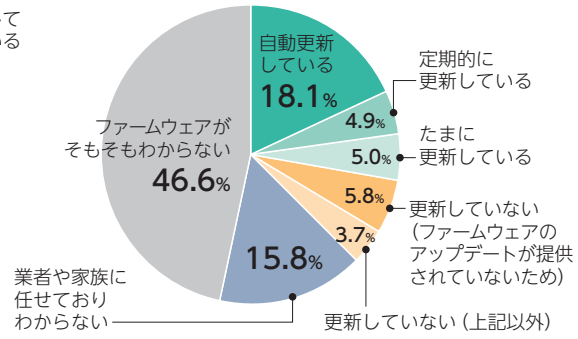
自宅無線LANの暗号化パスワード

（n=435：自宅無線LANを暗号化している利用者）



自宅無線LANのファームウェア更新

（n=961：自宅無線LANの利用者）



memo

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/