令和６年３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

Chapter 1

[自宅Wi-Fiとは]

一般家庭で「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通信（ワイヤレス）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、スマートフォンやタブレット等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、家庭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が便利。

※1　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。

Chapter 2

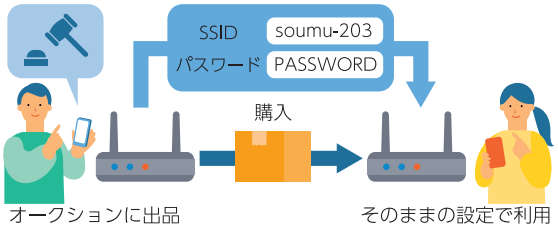
［自宅Wi-Fiに潜む脅威・リスク］

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（盗聴）、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・

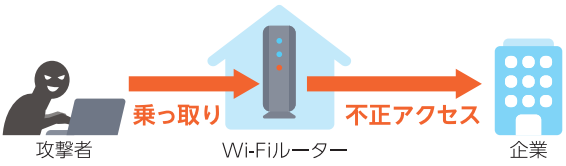
❶Wi-Fiルーターをそのままの設定で利用

Aさんは、Wi-Fiルーターをインターネットのオークションサイトで購入し、自宅で利用することにしました。自宅のLANポートに接続し、機器の裏面に記載のパスワードを入力すると接続できたので、そのままの設定で利用しました。



❷悪意の第三者により自宅Wi-Fiが犯罪行為に悪用される

数日後、Aさんの利用するWi-Fiルーターから、とある企業への攻撃が行われたとの連絡が警察からありました。調査した結果、AさんのWi-Fiルーターが悪意の第三者に乗っ取られて攻撃に利用されたことが分かりました。



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、Wi-Fiルーターの設定を確認せずに、そのままの状態で利用してしまったことです。そのため、悪意の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、

・安全なセキュリティ方式を選択する
・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
・ファームウェアを最新のものに更新する

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。

コラム　SSIDから身元を特定されることも

Wi-Fiに接続する際にマンションの隣の部屋で使っているWi-Fiが表示され、そのアクセスポイント名（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アクセスポイント名（SSID）は誰でも見ることができるため、アクセスポイント名（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※2機能を用いてパソコン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アクセスポイント名（SSID）として設定される場合があります。氏名や電話番号等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。

※2　スマートフォンなどの端末をアクセスポイントとして設定し、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。

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ルーター等の機器の設定を確認しましょう。

3-1 セキュリティ方式※3は「WPA2またはWPA3」を選択しよう

Wi-Fiのセキュリティ方式（詳細は下記のコラムを参照）は、「WPA2」または「WPA3」にしましょう※4。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方式。今後対応製品の普及が期待される。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で強化されており、WPA2で報告されていた脆弱性も解消されている。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、登録されたパスワード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。
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	セキュリティなし（暗号化なし）	通信が暗号化されず、誰でも接続可能。

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のセキュリティ対策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のですが、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。

※3　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。
※4　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。

3-3 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ことも多いため、自動更新設定を有効にしておくことを推奨します。

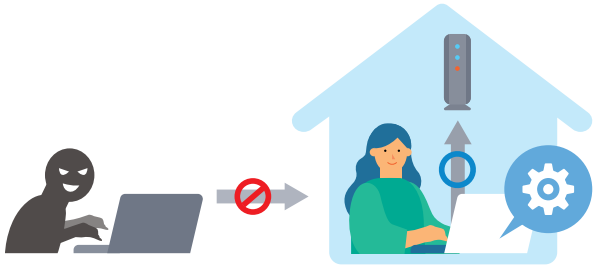
機器が古い場合はメーカーのサポートが終了しており、ファームウェアの更新が行われなくなっていることがあります。その場合、新たな脆弱性が発見されても対策されないため、サイバー攻撃を受けるリスクが高まります。

利用している機器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機器の買い替えを検討しましょう。

コラム 機器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もあります。利用しない機能は無効に設定するようにしましょう。

また、第三者に外部から機器に不正に侵入されてしまった場合、これらの設定が変更されてしまうことがあります。下記をはじめとする機能の設定が不正に変更されていないか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が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ルータ（管理画面）への接続機能**※5
  外出先等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。

- **NTP機能**
  時刻情報の同期に利用する機能です。Wi-FiルーターのNTPサーバ機能が外部へ公開する設定となっている場合、攻撃者によってNTPリフレクション攻撃※6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状態になっていた場合や、機器を中古で購入した場合などは、

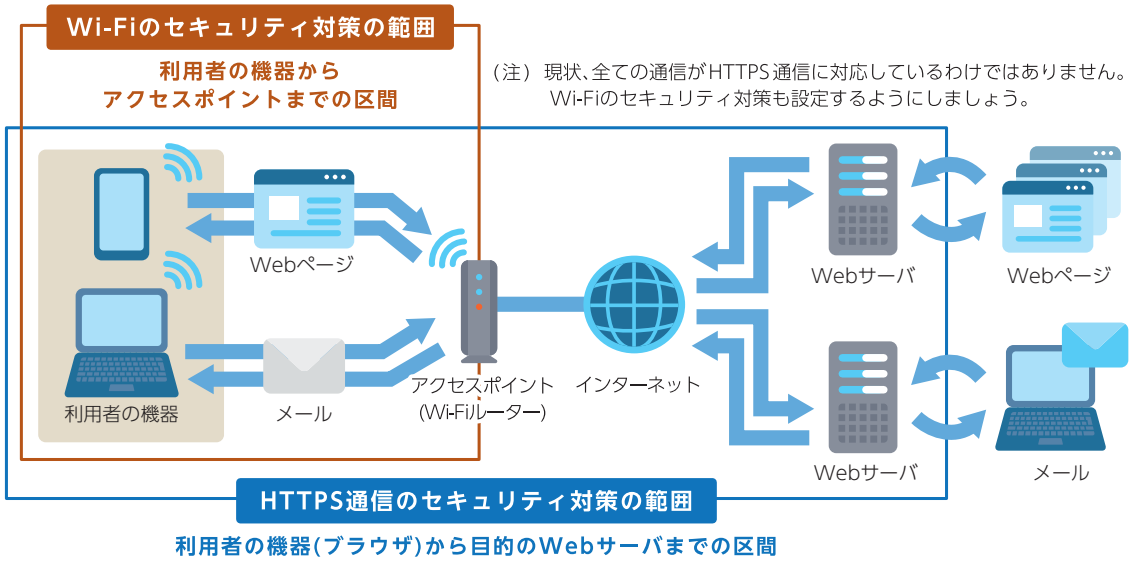
- Wi-Fiルーターを初期化し、その後不要な設定を無効とする。
- ファームウェアの最新化（上記の3-3を参照）
- パスワードの変更（4ページの3-2を参照）

といった対策を行いましょう。

※5　メーカーによって機能名が異なる場合があります。
※6　NTP機能を悪用し攻撃対象に大量のデータを送信することで正常なサービス提供を妨げる攻撃方法です。

コラム HTTPSのセキュリティ対策の範囲とは

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のセキュリティ対策範囲は、茶枠で囲んだ、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通信のセキュリティ対策範囲は、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。

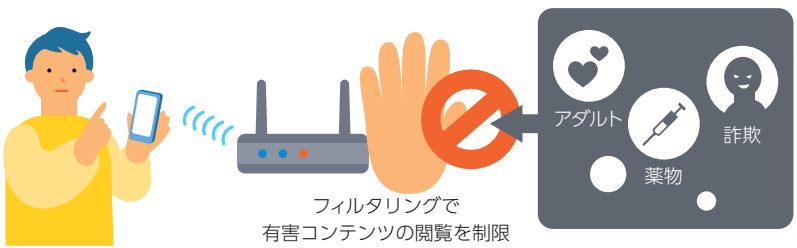


コラム 電波の出力調整

アクセスポイント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。

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※7を実施し、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。



※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。

[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 ※8	使用する周波数帯 ※9	最大伝送速度 ※10
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	6GHz帯	9.6Gbps

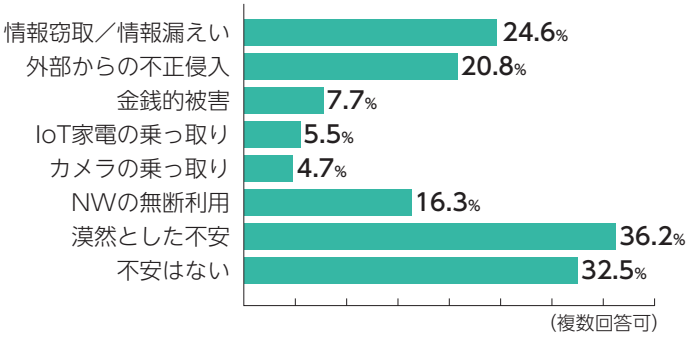
※8　規格名をわかりやすくするため、業界団体（Wi-Fi Alliance）が「Wi-Fi 6E」といった呼称を規定しています。
※9　5GHz帯にはW52（5.2GHz帯；制限付き屋外利用可）・W53（5.3GHz帯；屋外利用不可）・W56（5.6GHz帯；屋外利用可）があります。屋外利用については、総務省電波利用ホームページ（https://www.tele.soumu.go.jp/j/sys/others/wlan_outdoor/）をご覧ください。
※10　規格上の速度であり、実際のデータ伝送速度はこれよりも遅くなります。

利用者アンケート結果

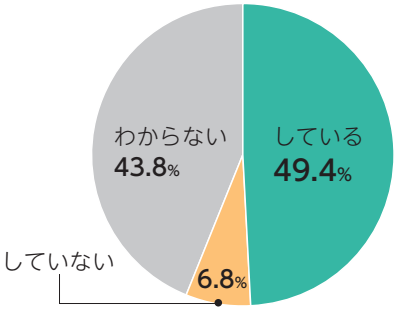
本マニュアルが自宅Wi-Fiの利用に不安を感じている方々の参考となり、各種セキュリティ対策事項の実施率が向上していくことを期待しています。

令和４年度「無線LANのセキュリティ確保に関するガイドラインの策定検討等に関する調査研究の請負」事業より作成。
（期間：2022年10月27日～ 2022年11月15日　調査数：30,000（うち無線LAN利用者1,000をスクリーニング）

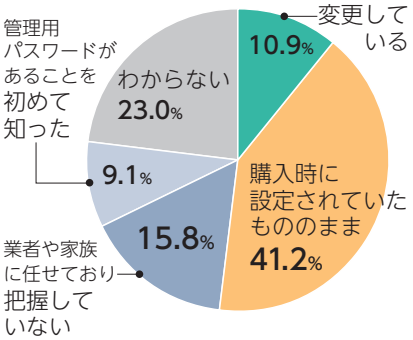
自宅無線LANでのセキュリティ上の不安
（n=956：自宅無線LANの利用者）



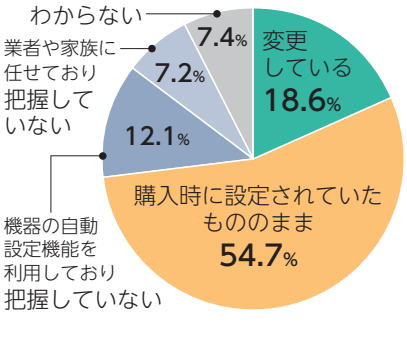
自宅無線LANの暗号化
（n=956：自宅無線LANの利用者）



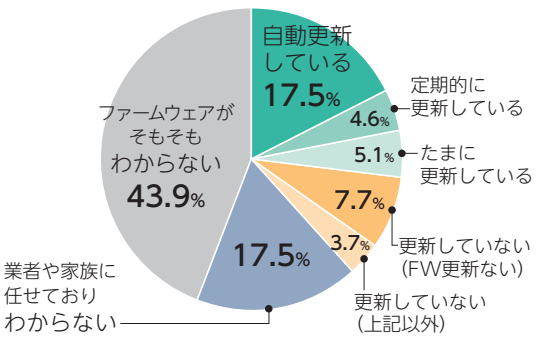
自宅無線LANの管理用パスワード
（n=956：自宅での無線LAN利用者）



自宅無線LANの暗号化パスワード
（n=472：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=956：自宅無線LANの利用者）



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