（情シ８）
令和２年６月１１日

都道府県医師会
情報システム担当理事　　殿

日本医師会
常任理事　石川　広己
（公印省略）

無線 LAN のセキュリティに関するガイドラインの周知について

拝啓　時下ますますご清祥のこととお慶び申し上げます。新型コロナウイルス感染症対応におきましてお力添えを賜り深く感謝申し上げます。

さて、今般、総務省において、策定・改定を行っている、「無線 LAN セキュリティに関するガイドライン（「Wi-Fi 利用者向け簡易マニュアル」及び「Wi-Fi 提供者向けセキュリティ対策の手引き」）につきまして、令和 2 年度 5 月版が公表されました。
本件について、医療機関においても ICT の利活用が進みつつあることから、厚生労働省が医療機関の対策の要点をまとめた資料が作成されましたので、ご連絡申し上げます。

内容としては、医療機関内において、業務での無線 LAN 利用や来訪者向けに無線 LAN を利用可能としている場合に、「医療機関で特に重要と考えられる対策」として、「来訪者向け Wi-Fi と業務用無線 LAN の分離」「機器管理用パスワードの複雑化」「電波漏れ等が起きないような電波出力の調整」「電波の解読リスクの認識」「業務用 Wi-Fi や患者持込の回線との干渉リスク把握」などについて注意を呼び掛けるものとなっております。

別添の資料につきましては、
厚生労働省「医療分野のサイバーセキュリティ対策について」
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/index.html#h2_free7
こちらにも掲載されておりますので、併せてご参照いただければ幸いです。

都道府県医師会におかれましては、別添の資料をご確認いただくとともに、郡市区等医師会、並びに会員の先生方にご周知いただきますようよいただきますようお願いいたします。

敬具

事　務　連　絡
令和２年６月４日

公益社団法人日本医師会　御中

厚生労働省医政局研究開発振興課

無線 LAN のセキュリティに関するガイドラインの周知について

日頃より医療分野の情報化に関し、格別のご配慮を賜り、厚く御礼申し上げます。

今般、総務省より別添１のとおり、無線 LAN のセキュリティに関するガイドラインについて、ICT の利活用が進みつつあることを鑑みて、病院等に対して幅広く周知するよう依頼がございましたので、周知いたします。

なお、当該ガイドラインの内容のうち、医療機関で重要となる対策のポイントを別添２のとおり整理しましたので、あわせてご活用ください。

貴会におかれましては、本ガイドラインを貴会会員の医療機関等に対してご周知いただきますようご協力方よろしくお願いいたします。

なお、本周知は別途自治体宛にも送付しておりますので申し添えます。

別添１

総サ統第１０６号
令和２年５月29日

厚生労働省医政局長
吉田　学　殿

総務省サイバーセキュリティ統括官
竹内　芳明

無線LANのセキュリティに関するガイドラインの周知について（依頼）

日頃より当省の業務に御理解と御協力をいただき誠にありがとうございます。

当省では、無線LANの利用者及び提供者において、無線LANを安全に利用又は提供するために必要となるセキュリティ対策等に関する理解を深めていただくことを目的として、無線LANのセキュリティに関するガイドライン（「Wi-Fi利用者向け 簡易マニュアル」及び「Wi-Fi提供者向け セキュリティ対策の手引き」）を策定しているところです。

今般、新技術や最新のセキュリティ動向に対応するため、当該ガイドラインの見直しを行い、令和２年５月版として改定の上、次のURLにて公表しています。

https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

つきましては、安全・安心に無線LANを利用できる環境の整備に向けて、利用者及び提供者の双方に対してのセキュリティ対策に関する周知啓発を図っていく必要があることから、ICTの利活用が進みつつあることに鑑みて、病院等に対して幅広く、当該改定後のガイドラインの内容を周知していただきますようお願いいたします。

別添２

総務省「無線 LAN のセキュリティに関するガイドライン」における医療機関で重要となる対策のポイント

今般、総務省が見直しを行った「無線 LAN のセキュリティに関するガイドライン」について、医療機関で特に重要と考えられる対策は、以下のとおり。

- 来訪者向け Wi-Fi と業務用無線 LAN は分離すること
- 機器管理用パスワードはして推測されにくいものを設定すること
- 無線 LAN の暗号化パスワードを掲示等する場合は解読リスクを認識すること
- 混雑を避けるために周波数やチャネルをよく検討すること（業務用 Wi-Fi や患者持込の回線との干渉リスク）
- 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、電波の出力等について適切に調整すること（電波漏れ等のリスク）

「Wi-Fi 提供者向け セキュリティ対策の手引き」に記載されている主な対策（例）

頁数	題　名	対　策　内　容
P.3	2-1. 利用者への周知啓発	・提供者側での十分なセキュリティ対策 ・利用者に対する周知啓発（「Wi-Fi 利用者向け簡易マニュアル」の周知等）
	2-2. 暗号化の実施とパスフレーズの伝達方法	・WPA2 による暗号化（パスフレーズを掲示等して誰もが知りうる状態にした際のリスクに注意） ・提供状況とリスクを総合的に判断し暗号化を実施しない場合は、利用者への適切な周知
P.5	2-3. 利用者の端末を保護するための端末同士の通信禁止	・同じアクセスポイントに接続した端末同士の相互通信の禁止（状況に応じて検討）
	2-4. 偽アクセスポイント対策	・利用者が正しいアクセスポイントであるかが分かるよう、認証画面の https 化や URL の周知
P.6	3-1. Wi-Fi 機器の適切な運用	・管理者パスワードを第三者に推測されにくいものに変更 ・機器のファームウェアの更新（運用時の定期的な確認）
	3-2. 業務用ネットワークとの分離	・Wi-Fi 提供用ネットワークと業務用ネットワークの分離
P.7	3-3. 利用者情報の適切な確認	※不特定かつ多数の利用者が利用する場合における、メールアドレスや SNS アカウント等を使っ

頁数	題　名	対　策　内　容
		た利用者識別が紹介されているが、患者や来訪者向けに Wi-Fi を提供するのであれば、取得する個人情報は最小限とすること、必要以上に取り過ぎないことに注意。
P.9	3-4. アクセスログの記録・保存	・アクセスログはプライバシー性が高く、業務目的に照らして必要最小限で記録 ・利用者への同意なく外部へ提供できないが、礼状に従う場合は警察等に提供することが可能 ・Wi-Fi の運用を他の事業者に委託している場合は記録内容や保存期間等を把握し、問い合わせがあった際の対応方法を委託先と確認しておく
	3-5. その他の対策	・接続 1 回当たりの利用時間制限 ・メール送信制限　等
P.10	4-1. Wi-Fi 利用者が安心して使うための適切な情報の提供	・利用者に対し、提供者・利用条件（料金・利用時間等)、セキュリティ対策の有無と内容（暗号化方式等)、Wi-Fi の危険性と安全な使い方（偽アクセスポイントの注意喚起等）を周知
	4-2. 青少年有害情報のフィルタリング	・フィルタリングを提供・販売するサイトの紹介等
	4-3. 法令に準拠した個人情報保護・通信の秘密保護	・アクセスログも含む利用者の情報を厳格に管理する法的な責任
P.11	5 より使いやすい Wi-Fi の提供に向けて	・混雑を避けるために周波数やチャネルをよく検討（業務用 Wi-Fi や患者持込の回線と干渉するリスク） ・施設内にのみ電波が届くように電波出力の調整

※　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。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。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」も「Wi-Fi」と表記。

「Wi-Fi提供者向けセキュリティ対策の手引き」で医療機関で特に重要と考えられる対策

来訪者向けWi-Fiと業務用無線LANは分離しましょう
また、機器管理用PWは推測されにくいものを設定しましょう

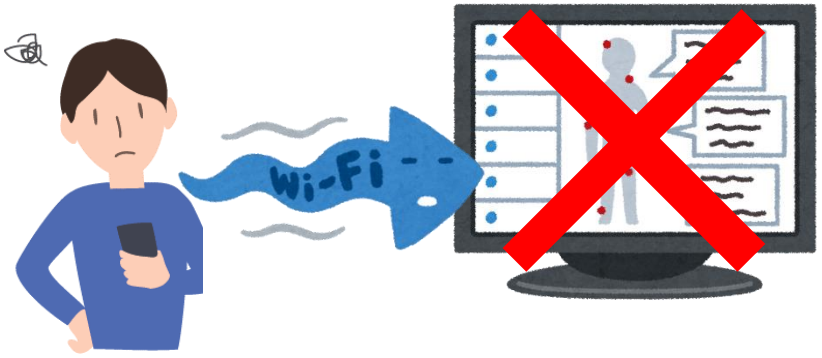
無線LANの暗号化パスワードを掲示等する場合は
解読リスクがあることを認識しましょう

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、電波の出力等について適切に調整しましょう（電波漏れ等のリスク）

エリア外で勝手に利用され、悪意ある利用がされることも

混雑を避けるために周波数やチャネルをよく検討しましょう
（業務用Wi-Fiや患者持込の回線との干渉リスク）

混雑により、データ入力中に切断して入力し直し



セキュリティ対策を徹底し、大切な情報を守りましょう！

ひと、くらし、みらいのために
厚生労働省
Ministry of Health, Labour and Welfare

Wi-Fi提供者向け
セキュリティ対策の手引き

～安全なWi-Fiの提供に向けて～

令和2年5月版

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、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、Wi-Fiの提供者に対し、安全な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」も「Wi-Fi」と表記しています。

1 本手引きをお読みになる方へ

1-1. Wi-Fi提供の現状と本手引き作成の背景

顧客や来訪者に対するサービス・利便性の向上のためにWi-Fiを提供する施設等が増えており、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」等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、利用者の約３分の２がWi-Fiの利用に不安を感じているという調査結果もあり、安心して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。

1-2. 本手引きの対象者

本手引きは、Wi-Fiの提供を検討している、または、既にWi-Fiを提供している施設等の運営者やシステム担当者等を対象としています。また、いわゆる「公衆Wi-Fi」はもちろんのこと、施設等の利用者限定でWi-Fiを提供する場合も、本手引きの対象としています。

飲食店や小売店等をはじめ、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等といった、Wi-Fiを提供する幅広い方々が、本手引きを通じて「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、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 利用者を守るための対策

施設等の運営者にとって、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。

Wi-Fi利用者の安全を確保するために
～Wi-Fi利用者がさらされる危険～

2-1. 利用者への周知啓発

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となります。

提供するWi-Fiにおいて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10ページの4-1を参照）、総務省がWi-Fiの利用者に対して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ために作成した「Wi-Fi利用者向け簡易マニュアル」を周知していくといった対応が有効です。

2-2. 暗号化の実施とパスフレーズの伝達方法

Wi-Fiの暗号化を設定することで、無線区間において通信を覗き見られるリスクを下げることができるため、暗号化を行う場合はWPA2※2による暗号化を設定しましょう。

ただし、暗号の利用に必要なパスフレーズ（パスワード）を利用者にどう伝えるかが問題になります。例えば、パスフレーズ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くなるため注意が必要です。（詳細は次ページのコラムを参照）

なお、Wi-Fiの提供状況によっては、パスフレーズ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、利用者に対する周知を適切に行う必要があります。（詳細は10ページの4-1を参照）

※2　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おり、使用は控えましょう。

コラム　Wi-Fiのセキュリティ方式

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。

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。
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方式となってしまっている。
無	セキュリティなし（暗号化なし）	通信が暗号化されず、だれでも接続可能。

コラム　パスフレーズ公開のリスク

WPA2によるWi-Fiの暗号化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、アクセスポイントに接続する人全員が同じパスフレーズを共有しており、このパスフレーズが第三者にわからない状態であれば、通信内容を解読される心配はなく安全に利用可能です。

一方で、パスフレーズ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、パスフレーズが分かっていれば、同じ名前（SSID）とパスフレーズを設定することで、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。

WPA2パーソナル方式はこうした特徴があるため、パスフレーズ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パスフレーズを記した用紙を個別に配付したり、定期的にパスフレーズを変更してパスフレーズを知りうる人を少ない状態にしたりといった対応が望まれます。

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-SAE）では、弱いパスフレーズを使われた場合のセキュリティが強化されており、WPA2パーソナルより改良されています。

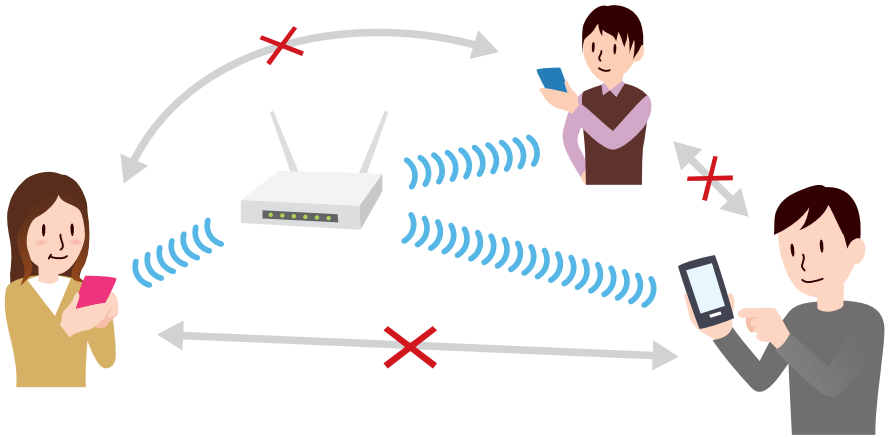
Wi-Fi CERTIFIED Enhanced Openは、パスフレーズなしで接続でき、暗号鍵は個別に設定され通信内容は秘匿されます。不特定多数に提供するWi-Fiサービスのセキュリティ強化策として期待されています。

今後、Wi-Fiの新規設置や、機器更改の際には、是非採用を検討しましょう。なお、これらの方式を利用するためには、スマートフォン等の接続機器も対応している必要がありますが、対応機器は今後増えていくと考えられます。

2-3. 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では、同じアクセスポイントに接続した端末同士が情報共有等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。

一般的なアクセスポイントには、相互通信を禁止する機能※3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Wi-Fiを提供しましょう。



2-4. 偽アクセスポイント対策

悪意のある者が、実在するWi-Fiのアクセスポイントと同じ名前（SSID）を設定した偽アクセスポイントを設置し、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。詐取された情報を悪用され、利用者が被害を受けてしまいます。

しかし、提供者で取れる対策は限られており※4、利用者側での対策が必須です。利用者が正しいアクセスポイントであるかが分かるよう、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となります。

また、正しいアクセスポイントか否かを確認できる接続アプリの提供もひとつの方法です。これも、偽アプリの問題がありますので、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、利用者が安心できる環境を整える必要があります。

※3　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」等の名称で呼ばれています。
※4　エンタープライズ認証では、電子証明書を利用して、正しいアクセスポイントではなかった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Wi-Fiには向いていません。

3 Wi-Fiを安全に提供するための対策

提供しているWi-Fiが不正アクセスに悪用されるなどすると、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機器が乗っ取られると、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。

3-1. Wi-Fi機器の適切な運用

Wi-Fi環境を提供するには、アクセスポイントやルーター等のネットワーク機器を施設に設置し、それを適切に管理する必要があります。

ネットワーク機器の管理には、管理者IDとパスワードの入力が必要ですが、パスワードが設定されていなかったり、簡単な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。複雑なパスワード※5を設定し、厳重に管理しましょう。なお、初期設定されているパスワードを使用している場合は、同じ機種で共通であったり、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ましょう。

また、ネットワーク機器のファームウェアについても、脆弱性対応等でセキュリティが強化された更新版が提供されることもあるため、最新のファームウェアにアップデートしましょう。なお、ネットワーク構築時だけではなく運用時においても、更新版が提供されていないか定期的に確認するようにしましょう。

3-2. 業務用ネットワークとの分離

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Wi-Fiを提供することは避けましょう。業務用のPC等にWi-Fiからアクセスされるなどにより、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技術等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。

また、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等の対策により業務用のネットワークとWi-Fi提供用のネットワークの分離を確実に行うようにしましょう。

※5　単語等により容易に推測できず、アルファベット・数字・記号等の種別を組み合わせた、できるだけ長い文字列を設定しましょう。また、パスワードを複数のサービスで使いまわさないようにしましょう。

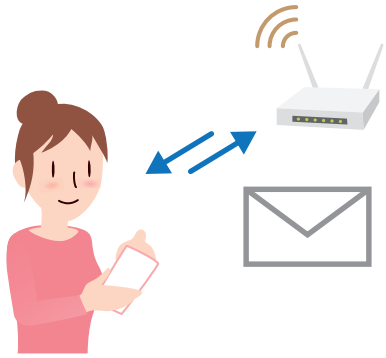
3-3. 利用者情報の適切な確認

Wi-Fiの提供に当たっては、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Wi-Fiを使用していたのかを調査できるようになり不正利用防止につながります。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。

なお、屋内施設や塀等により区切られた敷地内（空港や駅構内等）でWi-Fiが提供される場合や、目視や監視カメラ等により、利用者の出入りを十分把握できるような場合、利用者情報の確認や認証の仕組みは必ずしも必要ではありません。

① 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等で利用可能



② 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

③ SMS連携方式

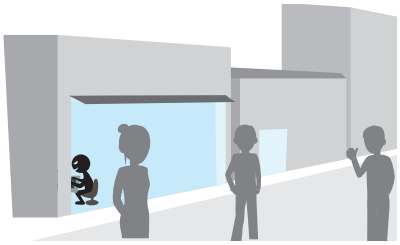
- 利用開始時に電話番号を入力（電話番号は利用者特定の観点から重要な情報となりえます）
- システムから利用コードがSMSで発行され、利用コードを入力することで利用可能
- 格安プラン等でSMS利用不可の人がいることに留意

また、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ひとつの方法です。

利用者情報の確認や認証が有効な例

不特定かつ多数の利用者がWi-Fiを利用する場所では、誰がいつWi-Fiを使っているのかを目視や監視カメラ等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
アクセスポイント



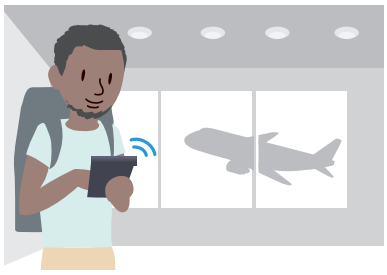
ショッピング街等、屋外で多くの
利用者が利用するアクセスポイント

屋外イベント等、開かれた空間で
多くの利用者が自由に出入りし、
利用するアクセスポイント

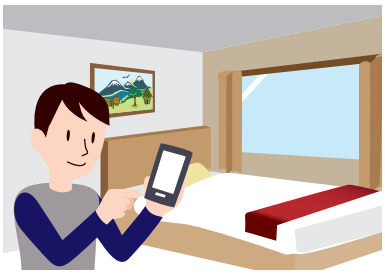
利用者情報の確認や認証が必ずしも必要ではない例

目視や監視カメラ等で利用者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等で利用者の出入りを十分把握できる場合は、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。

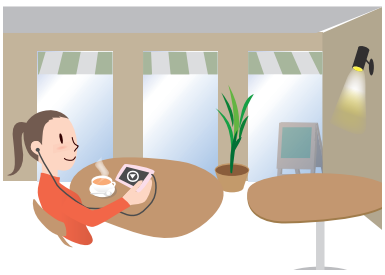
また、意図したエリア内に限ってサービスが提供されるように、電波の出力等について適切に調整することも大切です。



空港等が提供する
アクセスポイント
（空港は不特定多数の利用者がいる環境ですが、監視カメラ等で利用者の状況を把握しやすい）



ホテル客室等で提供される
アクセスポイント
（客室ごとにWi-Fiが提供されるホテル等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等の店舗内に
設置されるアクセスポイント
（店員の目視や監視カメラ等で利用者を特定しやすい）

3-4. アクセスログの記録・保存

アクセスポイントやルーター等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わ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等、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等の目的に使うことや、第三者に提供すること等のないよう、十分に注意して扱いましょう。

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、警察等に提供することができます。例えば、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等が挙げられます。

なお、Wi-Fiの運用を他の事業者に委託している場合は、アクセスログもその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等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。

3-5. その他の対策

上記のほか、Wi-Fiの不正利用を防止する観点から、接続１回当たりの利用時間を制限することや、メールの送信について制限を設けること等も有効です。

4 利用者に安心を提供するための対策

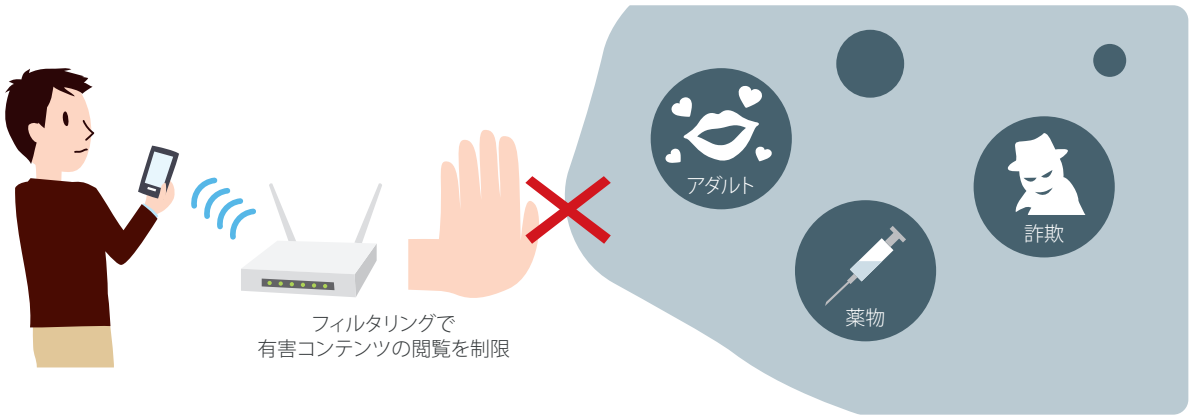
4-1. Wi-Fi利用者が安心して使うための適切な情報の提供

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Wi-Fiを使ってもら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、利用者に対してわかりやすい方法・内容で提供※6しましょう。

- サービスの提供者と利用条件（料金や利用時間等）
- セキュリティ対策の有無と内容（暗号化方式や認証方法等）
- Wi-Fiの危険性と安全な使い方（偽アクセスポイントの注意喚起と見分け方の周知等）

4-2. 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※7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等を行い、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。



4-3. 法令に準拠した個人情報保護・通信の秘密保護

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、Wi-Fiの提供に当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等を適切に管理※8しなければなりません。また、Wi-Fi提供者は、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。

※6　利用者に対しても、「Wi-Fi利用者向け簡易マニュアル」の６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。
※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。
※8　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。

5 より使いやすいWi-Fiの提供に向けて

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。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、多数のアクセスポイントが密集する場所では、それぞれのアクセスポイント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Wi-Fi を提供するためにも、周囲の環境との干渉も考慮した取組が必要です。

◉使いやすい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

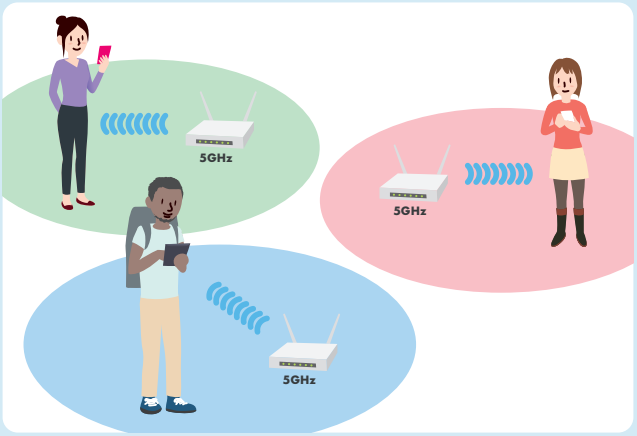
Wi-Fiでは、主に2.4GHz帯と5GHz帯の２種類の周波数帯を利用できます。2.4GHz帯は、家電製品や産業機械をはじめ様々な通信機器でも利用されている混雑しやすい周波数帯です。そのため、比較的混雑しておらず、2.4GHz帯よりも広い帯域が利用可能な5GHz帯※9も提供していきましょう。

●干渉を避けられるチャネルを選択する

アクセスポイントを設置するときは、周囲に設置されている既存のアクセスポイントとの干渉を避ける工夫が必要です。同じチャネル※10を使うと干渉してしまうことから、重複しないように調整しながらアクセスポイント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

アクセスポイント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、近隣の施設等と干渉する可能性も高くなります。施設等内で提供する場合は、施設等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。



●共有型のアクセスポイントを設置する

観光地や商店街等、人が多く集まるところでは、それぞれの施設が個別にWi-Fiを提供すると、干渉等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アクセスポイントの設置を検討しましょう。

※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。5GHz帯も気象用レーダー等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。

※10　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。

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。

電気通信事業法に基づく登録や届出

Wi-Fiサービス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第９条の登録又は同法第16条第１項の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登録や届出は不要です。

○ 本来の業務（電気通信役務以外）に付随してWi-Fiサービスを提供する場合
（例）ホテル事業者が宿泊サービスの一環として宿泊者にWi-Fiを提供するケース

○ 対価を得ずにWi-Fiサービスを提供する場合
（例）商店街において活性化や集客のために無料でWi-Fiを提供するケース

なお、地方公共団体によるWi-Fiサービスの提供は、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」等を参照ください。

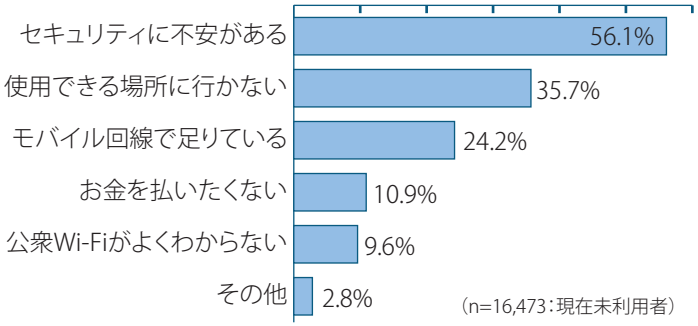
青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律

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等が規定されています。青少年が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等に努めましょう。

利用者アンケート結果

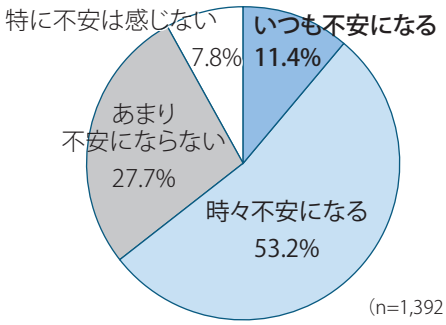
令和元年度「公衆無線LANのセキュリティ対策に係る周知啓発事業（現状等調査）」より作成
（対象地域：全国　期間：2020年2月13日～17日　調査数：31,112（公衆Wi-Fi利用者1,392をスクリーニング調査））

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）

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

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

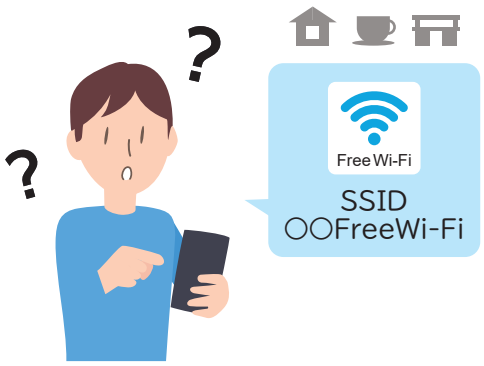
Wi-Fiを安全に利用するためには、どうすれば良いのでしょうか？ここでは、Wi-Fiのセキュリティ対策で欠かせない３つのポイントを紹介します。しっかり守れているかをチェックしてみましょう。

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。

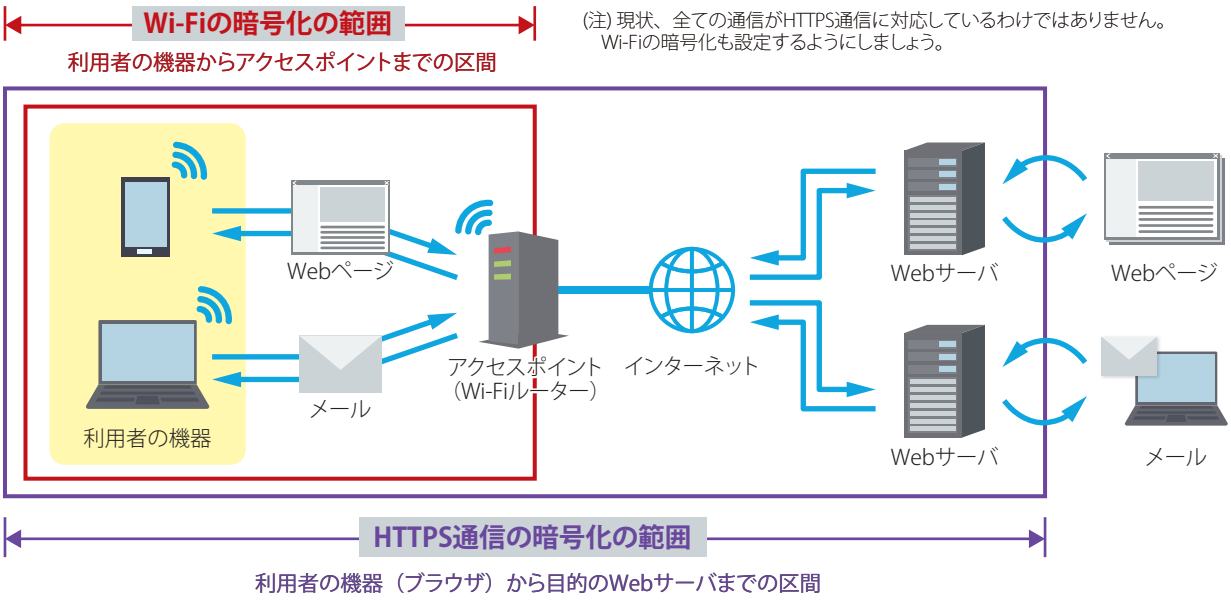
パソコン等で、メールソフトでのメール送受信（SMTP・POP・IMAP）やファイル転送（FTP）を利用する場合は、暗号化のための設定変更（SMTPであればSMTPsに変更するなど）を行うようにしましょう。よく分からない場合は、外出先ではブラウザからWebメールを使うなど、利用をブラウザのみに限定することもひとつの方法です。

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。

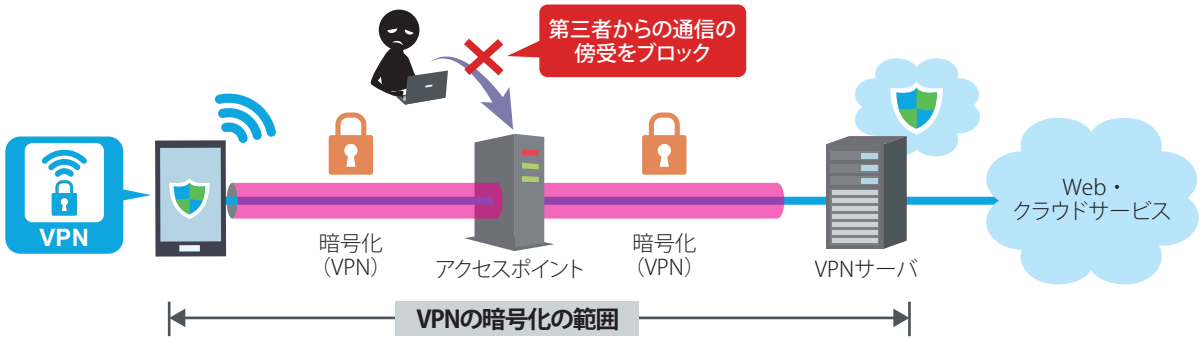


コラム　通信をまるごと暗号化するVPN

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。

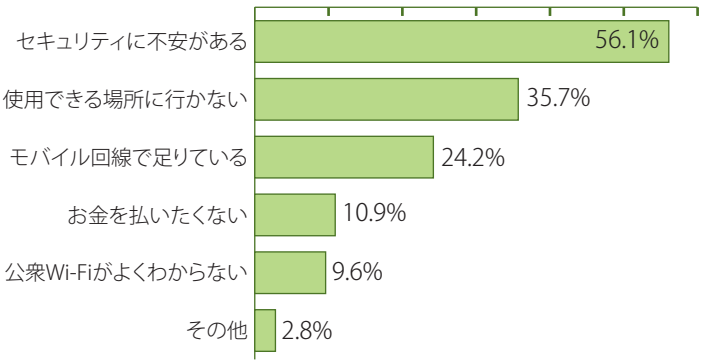
利用者アンケート結果

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。

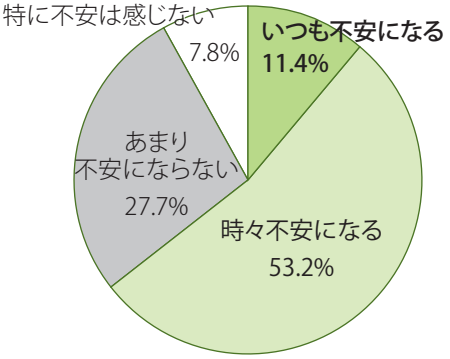
公衆Wi-Fiを利用しなかった理由

（n=16,473：現在未利用者）



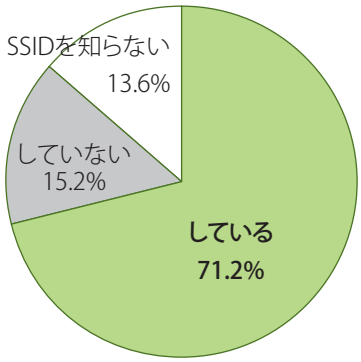
公衆Wi-Fiで不安を感じるか

（n=1,392：公衆Wi-Fi利用者）



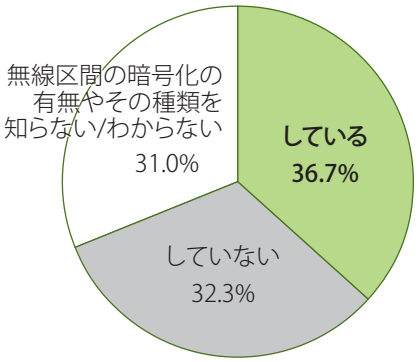
公衆Wi-Fi利用時のSSID確認

（n=1,392：公衆Wi-Fi利用者）



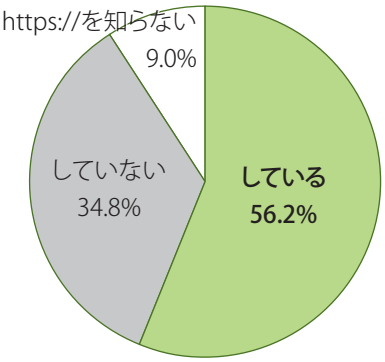
公衆Wi-Fi利用時の暗号化確認

（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/**