

サイバーだより

栃木県警察本部
サイバー犯罪対策課
令和3年8月

安全なFree Wi-Fiの提供に向けて

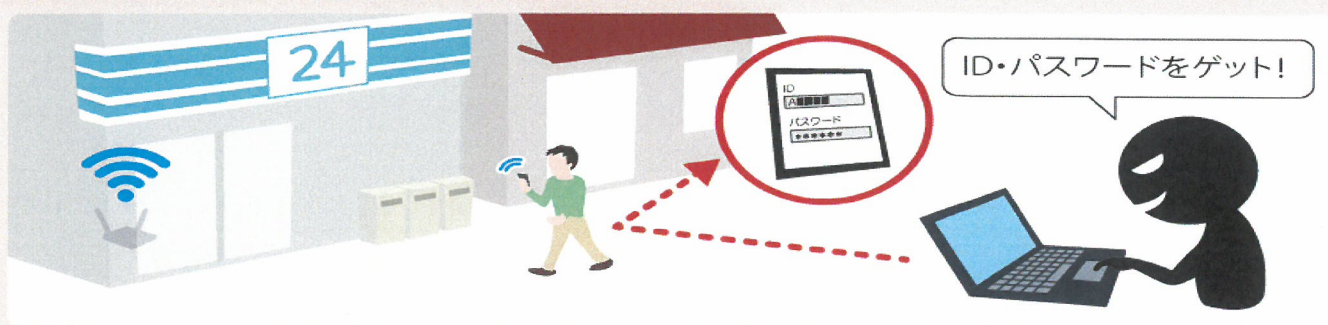
事業者向け

Free Wi-Fiはとても便利で、提供する施設は次々と増えてきています。しかし、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。

どのようなリスクがあるか理解して対策できていますか？



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～



場合によっては、クレジットカード情報が盗まれるなどして、利用者に金銭的な被害が発生することもあります！！

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のの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。

どのような対策が必要？

～ 利用者を守るための対策 ～

① 暗号化設定の実施

暗号化設定をすることで、通信を覗き見られるリスクを下げるすることができます。

こういった被害を避けるためにも、**Wi-Fi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。

Wi-Fiには、複数のセキュリティ方式があり、WEPからWPA,WPA2,WPA3の順に強化されています。

暗号化は、現在では一般的にWPA2,WPA3が使われており、**WEP,WPAは推奨されません**。

② パスワードは個別に配布、定期的な変更を

パスワードを誰もが知り得る状態にせず、必要とする人に用紙を個別に配布したり、定期的に変更して、パスワードを知る人が少ない状態にしましょう。

③ 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が相互に通信可能となることがあります。

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が搭載されているので、利用目的に応じて適切に設定しましょう。

～Wi-Fiを安全に提供するための対策～

① 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。

② 利用者情報の適切な確認

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。

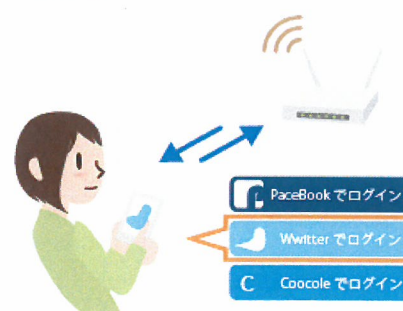
②-1 利用していることの確認を含めたメール認証方式

- ・ 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



②-2 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



②-3 SMS連携方式

- ・ 利用開始時に携帯電話番号を入力
- ・ 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



～利用者に安心を提供するための対策～

① Wi-Fi利用者が安心して使うための適切な情報の提供

サービスの提供者と利用条件、セキュリティ対策の有無と内容、Wi-Fiの危険性と安全な使い方等について、利用者にわかりやすい方法・内容で提供しましょう。

② 青少年有害情報のフィルタリング

青少年による利用が想定される場所では、閲覧を制限するフィルタリングの実施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、青少年が有害情報を閲覧する機会が少なくなるようにしましょう。



③ 法令に準拠した個人情報保護・通信の秘密保護

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しなければなりません。また、利用者のアクセスログは、業務上必要な場合のみ記録・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。

サイバーだより

栃木県警察本部
サイバー犯罪対策課
令和3年8月

Free Wi-Fiを安全に利用するために

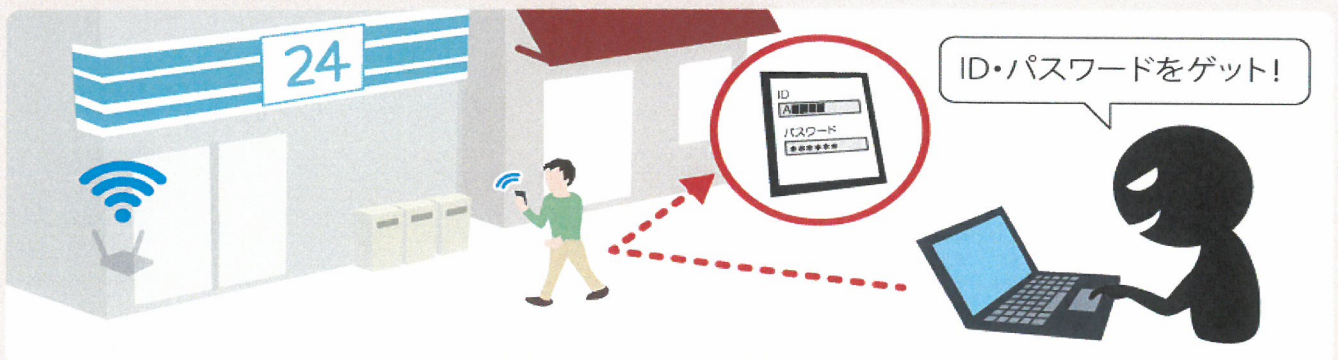
利用者向け

通信料金を気にせず利用できるFree Wi-Fiはとても便利ですが、その反面、適切なセキュリティ対策を取らずにしていると、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。

どのようなリスクがあるか理解して利用できていますか？



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～



場合によっては、クレジットカード情報が盗まれるなどして、利用者に金銭的な被害が発生することもある！！
セキュリティ対策を取らずに利用すると、たくさんの危険が待ち受けています！

安全に利用するためにはどうすれば良いの？

～ セキュリティ対策のポイント ～

① 接続するアクセスポイントをよく確認しよう

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、通信の暗号化などのセキュリティ対策はどうなっているのかをよく確認してから利用しましょう。



①-1 提供者や暗号化について確認しよう

＜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どうか確認しましょう。（右図の①部分）
- ・ 利用しようとしているWi-Fiサービスは暗号化されているかどうか確認しましょう。
鍵マークが付いているWi-Fiサービスは、通信が暗号化されています。
- ・ 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、提供者が不明なものや不審に感じるものには接続しないようにしましょう。
- ・ 少しでも不審な点があれば、利用を諦める決断も必要です。



② 正しいURLでHTTPS通信をしているか確認しよう

通信先のWebサイトのURLが「https://」から始まるHTTPS通信を使っていれば、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Webサイトを確認するようにしましょう。

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。



③ 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。

セキュリティ方式が、「セキュリティなし」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。

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。
	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いる。
	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。

※〔総務省〕 「Wi-Fi提供者向け セキュリティ対策の手引き(令和2年5月版)」

「Wi-Fi利用者向け 簡易マニュアル(令和2年5月版)」

より作成