別紙３

一般利用者が安心して無線ＬＡＮを利用するために

平成 24 年 11 月２日

総 務 省

無線ＬＡＮ[1]は、電波を使って情報をやり取りするため、ケーブルを気にすることなくインターネットが利用できます。最近では、パソコンからだけではなくスマートフォンから無線ＬＡＮが利用されることも増えています。しかし便利さの反面、適切な情報セキュリティ対策を取らずにいると、電波の届くところから気がつかないうちに通信内容が盗み見られたり、無断で無線ＬＡＮのアクセスポイント（親機）が悪用されてウイルスの配布等に使われたりすることがあります。

本書では、無線ＬＡＮの情報セキュリティ上の脅威や、一般利用者が安心して無線ＬＡＮを利用するための方策について述べます。

本書の読み進め方

まず、Ⅰ.の「無線ＬＡＮ情報セキュリティ３つの約束」では、一般利用者が最低限取るべき情報セキュリティ対策を提示します。

Ⅱ.の「一般利用者が安心・安全に利用するためのガイドライン」では、利用者のリテラシーや重要度に応じた段階別の対策を、Ⅰ.の「無線ＬＡＮ情報セキュリティの３つの約束」を含め総合的に示します。

Ⅲ.の「無線ＬＡＮを適切に利用しないと生じる危険性の具体的事例と解決策」では、Ⅰ.及びⅡ.で示した情報セキュリティ対策を適切に取らずに無線ＬＡＮを利用すると生じる危険性について、具体的な事例を交えて解説し、それぞれの事例における問題点をどのようにすれば解決できるのかについて説明します。

本書により、一般利用者による無線ＬＡＮの情報セキュリティに関する理解が深まり、無線ＬＡＮが便利に安心して活用されることを期待します。

また、スマートフォンの利用者は、スマートフォンを利用するに当たって最低限取るべき対策を提示した「スマートフォン情報セキュリティ３か条」[2]もあわせてご覧ください。

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/ippan20.htm

1：無線 LAN とは、電波でデータの送受信を行う構内通信網（LAN：Local Area Network）のことです。Wi-Fi（ワイファイ、Wireless Fidelity）とも呼ばれることがありますが、これは、正式には無線 LAN の普及促進を行う業界団体である Wi-Fi Alliance から、相互接続性等の認証を受けた機器のことです。

2：「1. OS（基本ソフト）を更新」、「2. ウイルス対策ソフトの利用を確認」、「3. アプリケーションの入手に注意」

I.無線ＬＡＮ 情報セキュリティ ３つの約束

パソコンやスマートフォンから、ケーブルを気にすることなく利用できて便利な無線ＬＡＮは、電波を使って情報をやりとりするため、利用者自身が適切な情報セキュリティ対策を取ることが必要です。

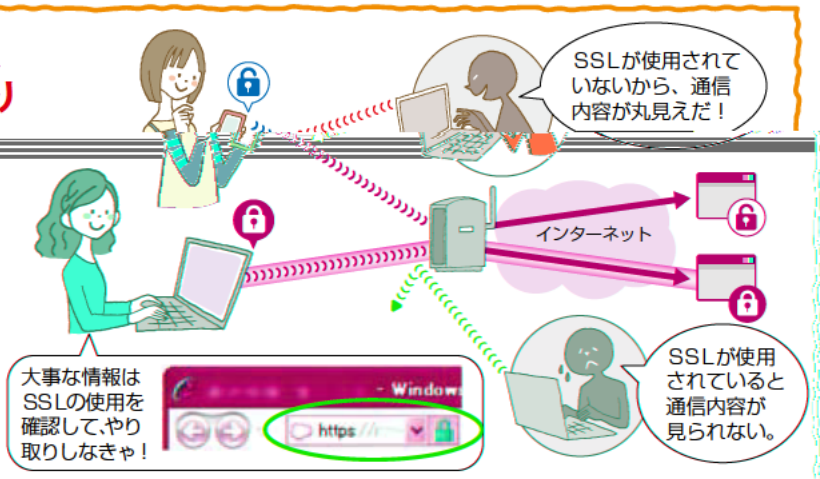
また、スマートフォンは、設定によっては利用者が無意識のうちに無線ＬＡＮに接続されている場合がありますので、スマートフォン利用者は、そのことを認識するべきです。

無線ＬＡＮを便利に安心して利用するために、一般利用者が最低限取るべき情報セキュリティ対策である「３つの約束」を守りましょう。

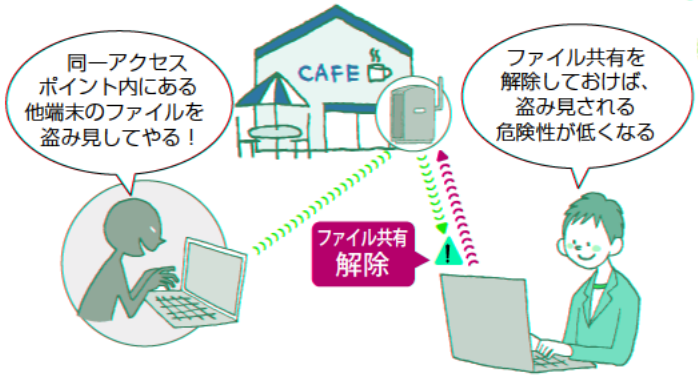
約束 1 無線ＬＡＮを利用するときは、大事な情報はＳＳＬでやりとり

インターネットは、一般に通信内容を盗み見られる危険性があるものですが、無線 LAN 利用時には、ケーブルの代わりに電波を使っているため、その危険性が高まります。

そのため、ID・パスワード等のログイン情報、クレジットカード番号やセキュリティコード、暗証番号といった決済に関する情報のほか、プライバシー性の高い情報など大事な情報を無線 LAN でやりとりする場合には、SSL[3]により暗号化がされていることを確認しましょう。



約束 2 無線ＬＡＮを公共の場で利用するときは、ファイル共有機能を解除



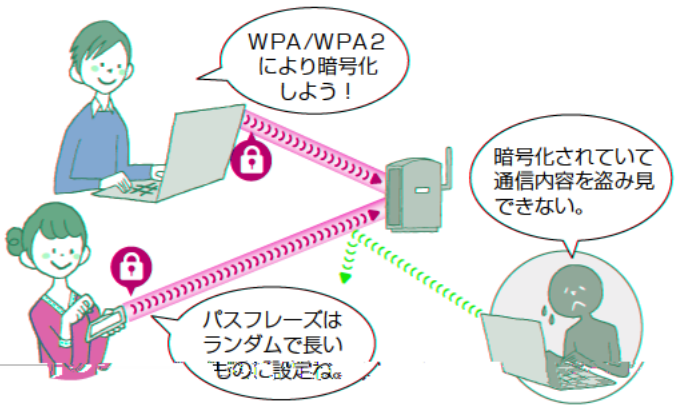
公共の場で無線 LAN を利用する際に、ファイルの共有機能[4]が有効になっていると、他人からパソコンやスマートフォン内のファイルが読み取られたり、ウイルスなどの不正なファイルを送り込まれたりすることがあります。

ファイル共有機能の利用は、家庭内や職場の LAN に接続したときに限るようにして、公共の場での無線 LAN 接続時には解除しましょう。

約束 3 自分でアクセスポイントを設置する場合には、適切な暗号化方式を設定

自分で設置したアクセスポイント（親機）でも、電波の届くところから気がつかないうちに通信内容が盗み見られたり、ウイルスの配布等に悪用されたりする危険性があります。

そのため、家庭の無線 LAN の親機やモバイル Wi-Fi ルータ、スマートフォンのテザリング機能[5]を設定する場合には、WPA や WPA２[6]により暗号化しましょう。その際、アクセスポイントと端末との間に設定する共通のパスフレーズ[7]は、ランダムで長いものにしましょう。



3：SSL（Secure Socket Layer）とは、信頼できるウェブサイトやサーバとの間で、インターネット上でデータを暗号化して送受信する方法です。ＳＳＬが使われていることは、ＵＲＬが「https」からはじまっていることや、パソコンやスマートフォンの主なブラウザに「鍵マーク」が表示されることで確認できます。

4：ファイル共有機能とは、ネットワークを通じて、ひとつのファイルを複数の端末から利用できるようにする機能です。スマートフォンは、ＯＳによるファイル共有機能を有しませんが、アプリケーションによりファイルを共有することが可能です。

5：テザリング機能とは、スマートフォンを無線ＬＡＮのアクセスポイントとして利用し、携帯電話事業者のネットワーク等を使って、無線ＬＡＮ対応のパソコンやゲーム機器等をインターネットに接続させる機能です。

6：WPA（Wi-Fi Protected Access）や WPA2 は、従来の無線ＬＡＮの情報セキュリティの仕様である WEP（Wired Equivalent Privacy）の弱点を補強し、解読が難しいとされている暗号化方式を採用した仕様のことです。

7：アクセスポイントと端末との接続に必要となる鍵で、事前に共有しておきます。なお、パスフレーズのほか、暗号化キー、暗号キー、共有キー、事前共有キー、ネットワークキー、パスワード、Pre Shared Key 等と呼ばれています。

Ⅱ　一般利用者が安心・安全に利用するためのガイドライン

一般利用者が「無線ＬＡＮを利用するとき」及び「自分で無線ＬＡＮのアクセスポイントを設置するとき」それぞれにおいて、情報セキュリティ対策をまとめました。

１．無線ＬＡＮを利用するときの情報セキュリティ対策

レベル１に示す情報セキュリティ対策は、無線ＬＡＮを利用するすべての一般利用者が最低限取るべき対策です。

レベル２に示す情報セキュリティ対策は、レベル１の対策に加えて一般利用者が取ることが望まれる対策です。

表１　無線ＬＡＮを利用するときの情報セキュリティ対策

	対策	危険性と効果
レベル１（必須対策）	(1)大事な情報はＳＳＬでやりとり	無線ＬＡＮ利用時には、通信内容が盗み見られる危険性が高まります。(1)の対策により、大事な情報が盗み見られることを防ぐことができます。
	(2)公共の場では、ファイル共有機能を解除	ファイル共有の機能が有効になっていると、同じアクセスポイントに接続する他人から、パソコンやスマートフォンにアクセスされる危険性があります。(2)の対策により、アクセスされる危険性が低くなります。
レベル２（追加で実施が望まれる対策）	(3)知らないアクセスポイントには接続しない	悪意を持って設置されたアクセスポイントに接続すると、通信内容を盗み見られる危険性があります。(3)から(5)の対策により、悪意を持って設置されたアクセスポイントに接続するのを防ぐことできます。
	(4)公衆無線ＬＡＮサービスのログイン画面に電子証明書エラーが表示されたら接続しない	
	(5)接続しているアクセスポイントを確認	
	(6)アクセスポイントが暗号化に対応していることを確認	暗号化に対応していない無線ＬＡＮでは、通信内容が盗み見られる危険性があります。(6)の対策により、通信内容が盗み見られる危険性の高いアクセスポイントを利用することを防ぐことができます。

(1) 大事な情報は、ＳＳＬでやりとり

インターネットは一般に通信内容を盗み見られる危険性があるものですが、無線ＬＡＮ利用時には、その危険性が高まります。

そのため、ＩＤ･パスワードなどのログイン情報、クレジットカード番号やセキュリティコード、暗証番号といった決済に関する情報のほか、プライバシー性の高い情報など大事な情報を無線ＬＡＮでやりとりする場合には、ＳＳＬによる暗号化がされていることを確認しましょう。ＳＳＬが利用されていることは、ＵＲＬが「https」で始まっていること、パソコンやスマートフォンの主なブラウザに「鍵マーク」が表示されることなどによって確認できます。

特に、公共の場で無線ＬＡＮを利用するときには、他人に通信を傍受されたり、偽のアクセスポイントに接続させられたりする危険性が高まります。公共の場で無線ＬＡＮを利用するときには、大事な情報はなるべくやりとりしないようにしましょう。どうしても大事な情報を公共の場でやりとりしたい場合には、ＳＳＬによる暗号化がされていることを確認してから行いましょう。

ＳＳＬが利用されていないときには、通信内容が盗み見られる危険性を理解した上で、大事な情報をやりとりするかどうか判断してください。

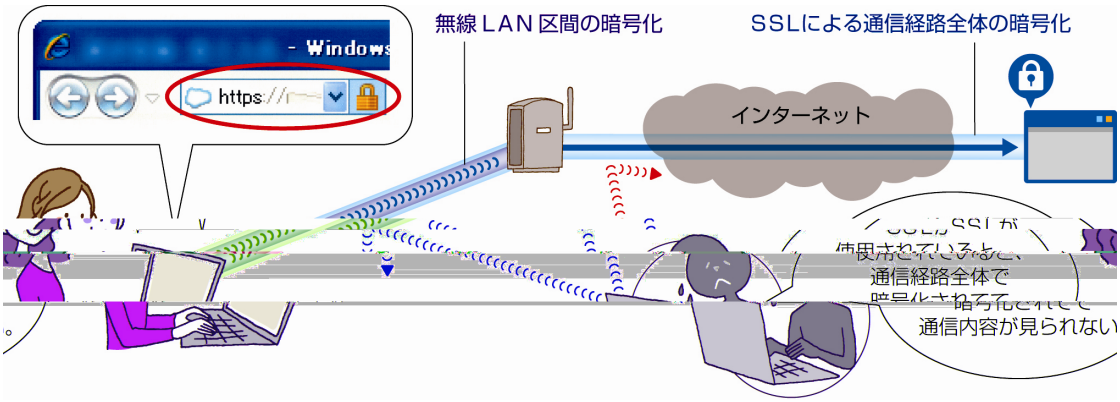


図１．ＳＳＬによる暗号化

＜ＳＳＬについて詳しく知りたい方へ＞

ＳＳＬ（Secure Socket Layer）[8]とは、インターネット上でデータを暗号化して送受信する方法です。無線ＬＡＮを通じてインターネットを利用するときには、無線ＬＡＮの暗号化機能を利用することにより、端末とアクセスポイントとの間の通信は暗号化されますが、アクセスポイントとウェブサイトやサーバとの間は暗号化されずにデータが送信されます。そのため、通信の途中でその内容が盗み見られる危険性があります。

ウェブサイトやサーバにＳＳＬが利用されているときには、ウェブサイトやサーバと端末との間の通信が暗号化されるため、途中で盗み見られることなく、大事な情報をやり取りできます。また、万一、アクセスポイントとの間の通信が傍受されても、通信内容が知られることを防ぐことができます。

ＳＳＬを使うウェブサイトでは「電子証明書」[9]が使われます。信頼できる第三者機関が発行した証明書が使われていれば問題ありませんが、利用者をだますために偽造した証明書が使われている場合があります。主なブラウザでは、偽造した証明書が使われているときには「証明書エラー」という画面が表示されますので注意しましょう。

ご利用の電子メールサービスがＳＳＬ[10]に対応している場合には、メールソフトを設定することで、メールソフトとメールサーバとの通信を暗号化できます。ＳＳＬにより暗号化することにより、万一、無線ＬＡＮでの通信が傍受されても、電子メールの内容やパスワードなどが知られることを防ぐことができますので、積極的に利用しましょう。

---

[8] ＳＳＬを基に標準化されたＴＬＳ（Transport Layer Security）という規格もあります。ＳＳＬという名称がよく知られているため、ＴＬＳを含めてＳＳＬと呼ばれることが多くなっています。

[9] 電子証明書が信頼のおける認証局から発行されている場合に、当該電子証明書に記載のあるウェブサイトやサーバが、偽造されたものではなく、その管理者によるものであることを保証する仕組みです。

[10] メールソフトとメールサーバとの間の通信をＳＳＬにより暗号化するには、POP3s（POP3 over SSL）、IMAP4s(IMAP4 over SSL)、SMTPs(SMTP over SSL)を利用します。POP3s、IMAP4s、SMTPs を利用するための設定は、契約しているプロバイダーのマニュアルをよく読むなどしてください。

(2) 公共の場では、ファイル共有機能を解除

公共の場で無線ＬＡＮを利用する際に、ファイルの共有機能が有効になっていると、パソコンのファイルが読み取られたり、ウイルスなどの不正なファイルを送り込まれたりすることがあります。

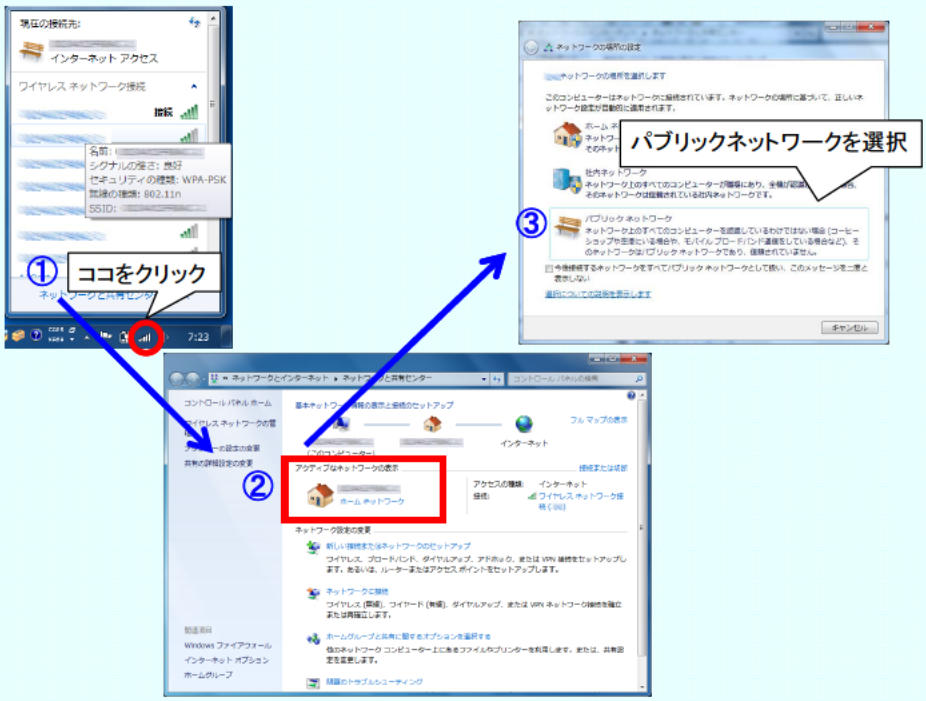
そのため、ファイル共有機能の利用は、家庭内や職場のＬＡＮに接続したときに限るようにして、公共の場での無線ＬＡＮ接続時には解除しましょう。

なお、スマートフォンは、ＯＳによるファイル共有機能を有していませんが、アプリケーションによるファイル共有が可能です。公共の場での無線ＬＡＮ接続時には、ファイル共有アプリケーションを終了しましょう。

＜ファイル共有機能の解除の手順＞

ここでは Windows 7 を例にファイル共有機能の解除手順を説明します[11]。

無線ＬＡＮに接続した上で画面右下のタスクバーに表示されている  をクリックし、「ネットワークと共有センターを開く」を選択します。「アクティブなネットワークの表示」に「パブリックネットワーク」が表示されている場合には、ファイル共有機能は解除されています。「ホームネットワーク」又は「社内ネットワーク」と表示されている場合には、これを選択し「ネットワークの場所の設定」から「パブリックネットワーク」を選ぶとファイル共有機能が解除されます。



なお、スマートフォンは、ＯＳによるファイル共有機能を有していませんが、アプリケーションによるファイル共有が可能です。アプリケーションによるファイル共有の機能を解除については、お使いアプリケーションのマニュアルをよく読むなどしてください。

[11] 他のＯＳでのファイル共有機能の解除手順はお使いの端末やＯＳのマニュアルをよく読むなどしてください。

(3) 知らないアクセスポイントには接続しない

無線ＬＡＮのアクセスポイントには、情報セキュリティ対策が取られておらず、誰でも利用できる状態になっているものがあります。これらのアクセスポイントの中には、通信内容を盗み見ることなどを目的に悪意を持って設置されたものが含まれている可能性があります。

そのため、誰でも利用できる状態になっているからといって、知らないアクセスポイントには接続しないことが大切です。

(4) 公衆無線ＬＡＮサービスのログイン画面に電子証明書エラーが表示されたら接続しない

ＳＳＬが使われていない場合や、ＳＳＬが使われていても電子証明書のエラーが表示される場合には、偽のアクセスポイントに接続している危険性があります。

公衆無線ＬＡＮサービス[12]にログイン画面が表示されるときには、ＳＳＬという通信方法が使われていることを確認しましょう。

電子証明書のエラーが表示される場合には、ＩＤとパスワードは入力せずに、契約している公衆無線ＬＡＮサービス事業者等に問い合わせましょう。

なお、アクセスポイントの暗号化対応については、２．(1)で詳しく説明します。

(5) 接続しているアクセスポイントを確認

無線ＬＡＮでは、アクセスポイントに自動的に接続するよう設定することができるため、暗号化等の十分な情報セキュリティ対策が取られていないアクセスポイントや悪意を持って設置されたアクセスポイントなど、望まないアクセスポイントに意図せず接続してしまい、通信内容が盗み見られるなどの危険性があります。

図２．接続しているアクセスポイントの確認

そのため、無線ＬＡＮを利用しているときには、どのアクセスポイントに接続しているか確認しましょう。思ってもいないアクセスポイントに接続していないか、確認することが大切です。

これまで利用したことがないアクセスポイントには、自動的に接続しないよう設定できる端末もあります。アクセスポイントに自動的に接続するよう設定するときには、マニュアルをよく読むなどして、十分注意して使うようにしましょう。

公衆無線ＬＡＮサービスを利用するときには、偽のアクセスポイントでないか、サービス事業者のアクセスポイント検索やステッカーなどで、その場所で本当にサービスが提供

[12] 屋外や店舗、公共施設等に設置されたアクセスポイントを通じて、設置者以外にインターネット接続環境等を提供するものです。

されているのか確認することも有効です。
　また、スマートフォンでは、設定によっては利用者が無意識のうちに、携帯電話回線から無線ＬＡＮに接続が切り替わっている場合があります。携帯電話回線と無線ＬＡＮのどちらで通信しているのか、確認するようにしましょう[13]。携帯電話回線とは異なり、無線ＬＡＮでは適切な情報セキュリティ対策を取らずにいると、通信内容が盗み見られるなどの危険性があります。

＜接続しているアクセスポイントの確認手順＞

　Windows 7 では、画面右下のタスクバーに表示されている をクリックすることで、現在接続しているアクセスポイントが確認できます。

　Android 4.1 搭載のスマートフォンでは「設定」、「Wi-Fi」を順に選ぶと現在接続しているアクセスポイントが確認できます。

　iPhone (iOS6.0)では、「設定」、「Wi-Fi」を順に選ぶと「Wi-Fi ネットワーク」で現在接続しているアクセスポイントを確認できます。

(6) アクセスポイントが暗号化に対応していることを確認

暗号化に対応していない無線ＬＡＮでは、通信内容を盗み見られる危険性があります。

そのため、アクセスポイントが暗号化に対応していることを確認しましょう。

、ウェブサイトやサーバと端末との間の通信が暗号なくなりますが、すべてのインターネットサービスません。暗号化に対応していない無線ＬＡＮで、Ｓサービスを利用する場合には、通信内容が盗み見らりとりするかどうか判断してください。

なお、ＳＳＬを利用することにより化され、途中で盗み見られる危険性はがＳＳＬに対応しているわけではありＳＳＬに対応していないインターネットれる危険性を理解した上で、情報をや

たことに気がつかないと、高額な通信料金が請求されることもあ

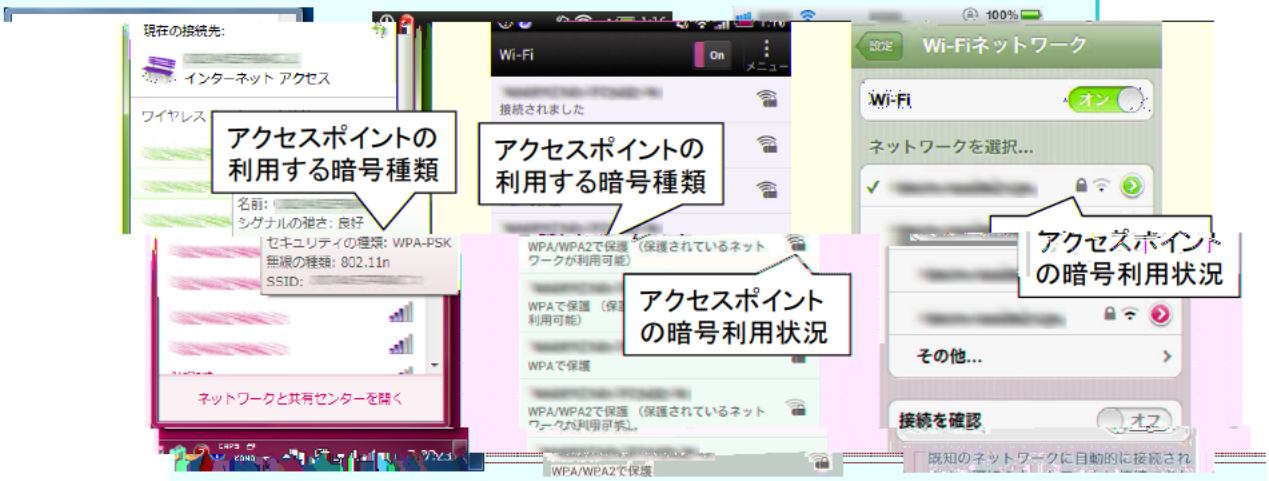
[13] 海外で、無線ＬＡＮから携帯電話回線に切り替わっります。

＜公衆無線ＬＡＮサービスに暗号が利用されていることの確認方法＞

Windows 7 では、画面右下のタスクバーに表示される をクリックすると、利用できるアクセスポイントの一覧が表示されます。アクセスポイントにカーソルを合わせると吹き出しが表示されます。「セキュリティの種類」が「保護なし」と表示されているときには暗号が利用されていません。「WEP」や「WPA-PSK」等と表示されているときには暗号が利用されています。

Android 4.1 搭載のスマートフォンでは、「設定」、「Wi-Fi」を順に選ぶと利用できるアクセスポイントの一覧が表示されます。暗号化が利用されている場合には、アクセスポイントの名前の右側に鍵のマークが付いたアイコンが表示され、名前の下に「WEP で保護」「WPA／WPA2 PSK で保護」などと表示されます。鍵のマークが付いていないときには、暗号化はされていません。

iPhone (iOS6.0)では、「設定」、「Wi-Fi」を順に選ぶと「Wi-Fi ネットワーク」に利用できるアクセスポイントの一覧が表示されます。アクセスポイントの名前の横に鍵のマークが表示されているときには暗号が利用されています。鍵のマークが付いていないときには、暗号化はされていません。



２．自分でアクセスポイントを設置するときの情報セキュリティ対策

家庭の無線ＬＡＮの親機やモバイル Wi-Fi ルータ、スマートフォンのテザリング機能を設定するときの情報セキュリティ対策には以下のようなものがあります[14,15]。

レベル１に示す情報セキュリティ対策は、自分でアクセスポイントを設置するすべての一般利用者が最低限取るべき対策です。

レベル２に示す情報セキュリティ対策は、レベル１の対策に加えて一般利用者が取ることが望まれる対策です。

レベル３に示す情報セキュリティ対策は、追加的に実施することで、無線ＬＡＮを安心して利用することにつながりますが、対策を実施するには知識が必要になるなど上級者[16]向けのものです。

＜スマートフォンのテザリング機能での注意点＞

スマートフォンのテザリング機能を利用するときには、家庭の無線ＬＡＮの親機やモバイル Wi-Fi ルータと比較して、以下のように利用できる情報セキュリティ機能に違いがあることに注意してください。

・初期設定が暗号化を利用しない設定となっている場合があります。
・ＷＰＳ[17]やメーカ独自の自動設定機能が利用できない場合があります。
・SSID[18]のステルス機能[19]に対応していない場合があります。
・ＭＡＣアドレス[20]フィルタリング機能に対応していない場合があります。

---

[14] その他、これらの機器のぜい弱性に関するアップデートが提供されている場合があります。その場合には、アップデートを適用し最新のものにするようにしましょう。アップデートの方法は、機器のマニュアルをよく読むなどしてください。

[15] 無線ＬＡＮには、アクセスポイントを使わずに端末同士が直接通信するアドホック・モードがあります。ただし、適用できる情報セキュリティ対策が限られるため、利用する場合には十分注意しましょう。

[16] 本ガイドラインにおける「上級者」とは、無線ＬＡＮのアクセスポイントの暗号化方式等を、メーカが用意している自動設定機能を使わずに、自分で設定したり変更したりできる人を想定しています。

[17] ＷＰＳ(Wi-Fi Protected Setup)は、無線ＬＡＮ機器の情報セキュリティに関する設定を自動で行う機能のことです。スマートフォンでは、携帯電話事業者がアプリケーションとしてこの機能を提供しています。

[18] SSID（Service Set Identifier）は、無線ＬＡＮのアクセスポイントを識別する名称です。

[19] 無線 LAN のアクセスポイントは自身の存在を端末側に知らせるために、SSID を周囲に発信しています。ステルス機能とは、この SSID の発信を停止し、無線 LAN のアクセスポイントの存在を隠ぺいする機能です。

[20] ＭＡＣ(Media Access Control)アドレスは、端末に一意に割り振られた番号のことです。正規のＭＡＣアドレスに同じ番号は存在しません。

表２　自分でアクセスポイントを設置するときの情報セキュリティ対策

		設定内容	危険性と効果	備考
レベル１（必須対策）	(1)アクセスポイントに適切な暗号化方式を設定	ＷＰＡやＷＰＡ２による暗号化を設定します。 パスフレーズはランダムで長いもの[21]にします。	電波の届くところから気がつかないうちに通信内容が盗み見られたり、無断で悪用されたりする危険性があります。 端末とアクセスポイントの間の通信を強固に暗号化し、通信内容が盗み見られることを防ぎます。 複雑なパスフレーズにより無断で無線ＬＡＮが利用されることを防ぎます。	
レベル２（追加で実施が望まれる対策）	(2)SSIDの設定	SSID を推測困難なものに設定し、ステルス機能を活用します。	メーカ名が推測できる SSID にしていると、そのメーカのアクセスポイントにぜい弱性が発見された場合等に、攻撃を受ける危険性が高くなります。 また、SSID として自分の名前などを設定すると、他人の興味を不用意に惹く危険性があります。 SSID を簡単には推測又は検出されないようにすることで、他人から無断で利用されるなどの危険性を低くすることができます。	SSID を完全に隠すことはできません。
	(3)使わない時にはモバイルWi-Fiルータやテザリングの機能をオフに	使用時以外には機能をオフにします。	自分は利用していないつもりでも、無断で悪用されるなどの危険性があります。 使わないときに機能をオフにすることで、使用していないときに他人に無線ＬＡＮを利用されることなどを防ぎます。	
レベル３（上級者向け追加対策）	(4)ＭＡＣアドレスフィルタリングの利用	アクセスポイントに接続できる端末のＭＡＣアドレスを登録します。	アクセスポイントは他人に無断で悪用される危険性があります。 アクセスポイントに接続できる端末を登録することで、登録した端末以外からアクセスポイントが利用される危険性を低くすることができます。	ＭＡＣアドレスを偽装した端末からの接続は、この対策では防止できません。
	(5)無線端末同士の通信の遮断設定	同一のアクセスポイントに無線で接続する機器同士の通信を禁止します。	同じアクセスポイントを利用する他の人から、無断で端末にアクセスされてしまう危険性があります。 同じアクセスポイントに電波で接続する端末同士の通信を禁止することで、他の端末からアクセスされることを防ぎます。	アクセスポイントにケーブルで接続している機器へのアクセスについては、防止できない場合があります。

[21] 推奨されるパスフレーズの長さについては、文献により異なりますが、無線ＬＡＮの規格書（IEEE Std 802.11™–2012）には、「A key generated from a passphrase of less than about 20 characters is unlikely to deter attacks.」と記載されており、おおよそ 20 文字以上を推奨しています。

(1) アクセスポイントに適切な暗号化方式を設定

自分で設置したアクセスポイントでも、電波の届くところから気がつかないうちに通信内容が盗み見られたり、ウイルスの配布等に悪用されたりする危険性があります。

そのため、家庭の無線ＬＡＮの親機やモバイル Wi-Fi ルータ、スマートフォンのテザリング機能を設定する場合には、ＷＰＡやＷＰＡ２により暗号化しましょう。その際、アクセスポイントと端末との間に設定する共通のパスフレーズはなるべくランダムで長いものにしましょう。

これらの暗号化方式や暗号のパスフレーズの設定は、アクセスポイントやアクセスポイントに接続する機器のマニュアルに従って適切に行いましょう。

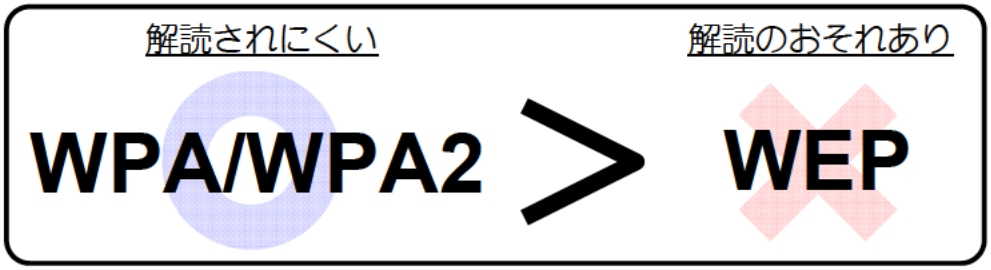


図３．情報セキュリティ強度

＜暗号化について、より詳しく知りたい方への情報＞

暗号化とは、大事な情報を他人には知られないようにするため、データを見てもその内容がわからないように、定められた規則に従い、鍵（パスフレーズ）でデータを変えてしまうことです。暗号化されたデータは元に戻すことができますが、その規則や鍵（パスフレーズ）を知らなければ元の内容を知ることはできません。

①暗号化方式

無線ＬＡＮには、ＷＥＰ、ＷＰＡ、ＷＰＡ２の３種類の情報セキュリティ方式があります。

ＷＥＰは最も古い方式で容易に解読されるおそれがあり、現在では安全ではありません。ＷＰＡやＷＰＡ２は、ＷＥＰの弱点を補強し、解読が難しいとされている暗号化方式を採用しています。

現時点では、ＷＰＡやＷＰＡ２による暗号化を推奨します。

ＷＥＰにしか対応していない端末を接続するためにアクセスポイントの設定をＷＥＰに変えることは避けましょう。どうしてもＷＥＰにしか対応していない端末を接続したいときには、複数の暗号化方式を使い分けられる機能（マルチ SSID）を備えたアクセスポイントを使いましょう。マルチ SSID 機能を備えたアクセスポイントは、複数の SSID を設定し、SSID ごとに別の暗号化方式を設定することができます。例えば、ＷＥＰにしか対応していないゲーム機を無線ＬＡＮにつなぐ場合には、ＷＥＰに設定した SSID で接続し、解読が難しいＷＰＡやＷＰＡ２に設定した別の SSID で、他のパソコンやスマートフォン等を接続することができます。

②パスフレーズの設定

ＷＰＡやＷＰＡ２による暗号化では、無線ＬＡＮのアクセスポイントと端末に共通の鍵（パスフレーズ）を事前に設定する必要があります[22]。パスフレーズは、他人が推測できないよう、記号や英数字を使った、なるべくランダムで文字数の長いパスフレーズにする必要があります。ＷＰＳやメーカ独自の自動設定機能を使うと、パスフレーズの設定等を自動で適切に行うことができます。

万一、無線ＬＡＮのパスフレーズの設定を行っている端末をなくしたり、盗まれたりしたときには、アクセスポイントや他の端末のパスフレーズを変更するようにしましょう。

なお、マルチＳＳＩＤの機能を利用する際は、暗号化方式ごとに異なるパスフレーズを設定しましょう。同じパスフレーズを使用していた場合、ＷＥＰが解読されることにより、ＷＰＡ／ＷＰＡ２も安全でなくなります。

(2) SSID の設定

SSID は、無線ＬＡＮのアクセスポイントを識別する名称です。アクセスポイントと同一の SSID を端末に設定しないと、無線ＬＡＮへは接続できませんが、アクセスポイントの SSID は、誰でも端末から確認することができます。簡単には見えなくする機能（ステルス機能）もありますが、SSID を完全に隠すことはできません。そのため、情報セキュリティ対策としての効果は限られています。

他人の興味を不用意に惹かないよう、SSID に自分の名前などを設定することは避けましょう。

また、SSID の初期設定がメーカ名、ＯＳ名等になっている場合には、SSID を変更しましょう。初期設定のままにしていると、他人が同じメーカのアクセスポイントを利用していた場合に、自分のアクセスポイントと区別することができなくなります。また、メーカ名が推測できる SSID にしていると、そのメーカのアクセスポイントにぜい弱性が発見された場合等に、攻撃を受けやすくなるおそれがあります。

(3) 使わない時にはモバイル Wi-Fi ルータやテザリングの機能をオフに

無線ＬＡＮへの接続は、インターネット上の脅威一般にさらされることになるため、自分は利用していないつもりでも、ウイルスに感染したり、無断で悪用されたりする可能性があります。

そのため、モバイル Wi-Fi ルータやスマートフォンのテザリング機能は、使わないときにはこまめに切るようにしましょう。

[22] 企業等では、本人確認のためのサーバを設置し、暗号鍵を自動的に生成・配布する方式が利用されることもあります。

(4) MAC アドレスフィルタリングの利用

無線ＬＡＮを他人に無断で利用されないために、アクセスポイントのＭＡＣアドレスフィルタリング機能を利用することができます。

ＭＡＣアドレスフィルタリングは、無線ＬＡＮのアクセスポイントに接続できる端末を登録しておき、登録されていない端末の接続を禁止する機能です。接続を禁止する端末を登録する方式のアクセスポイントもあります。

登録には端末に一意に割り振られたＭＡＣアドレスを使います。ＭＡＣアドレスに同じ番号は存在しません。

ただし、他人がＭＡＣアドレスを知ったり、ＭＡＣアドレスを偽装したりできるため、他の情報セキュリティ対策と組み合わせて使うようにしましょう。

スマートフォンのテザリング機能では、ＭＡＣアドレスフィルタリング機能に対応していない場合があります。

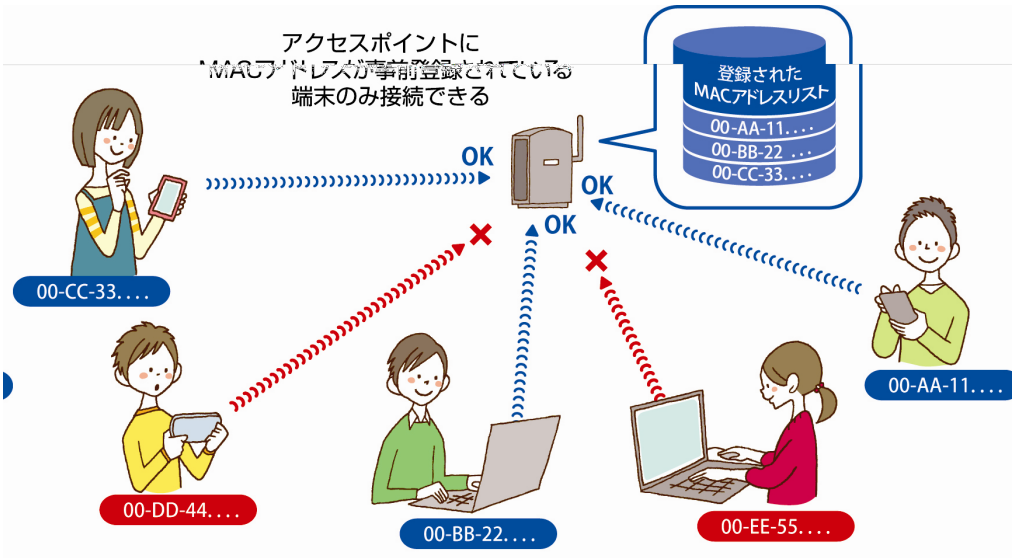


図４．ＭＡＣアドレスフィルタリングの利用

(5) 無線端末同士の通信の遮断設定

無線ＬＡＮを利用する他の人から、無断で端末にアクセスされてしまうことを防ぐために無線端末同士の通信の遮断設定を利用することができます。

ネットワーク分離機能やポートセパレート機能、プライバシーセパレータ機能などと呼ばれ、本機能を備えたアクセスポイントでは、無線端末同士の通信の遮断設定を行うことにより、アクセスポイントに電波で接続している端末同士の通信を禁止できます。

ただし、電波ではなく、ケーブルで接続している端末との通信は可能な場合もありますので、ケーブルで接続している端末がある場合には、他人に無線ＬＡＮが利用されないよう注意する必要があります。

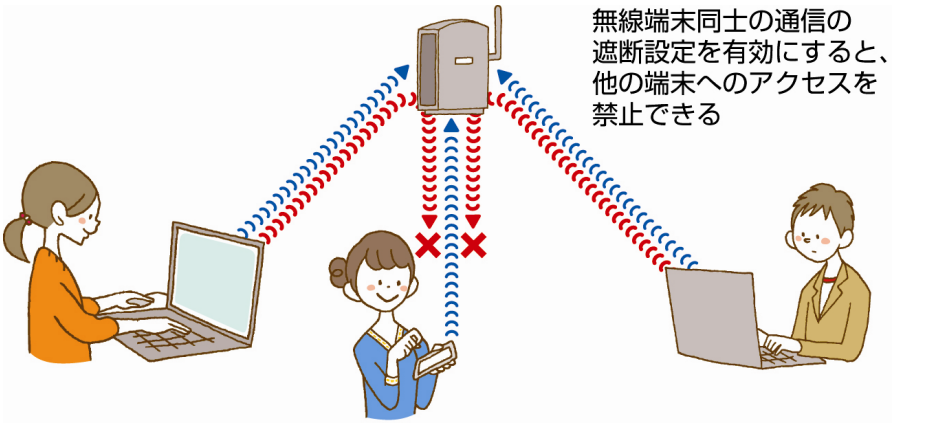


図５．無線端末同士の通信の遮断

（ご参考）

情報セキュリティ全般に関する情報をお知りになりたい場合は、以下の総務省サイトをご覧ください。

総務省「国民のための情報セキュリティサイト」

（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm）

Ⅲ　無線ＬＡＮを適切に利用しないと生じる危険性の具体例と解決策

無線ＬＡＮを、情報セキュリティ対策を取らず利用すると、通信内容が盗み見られたり、無断で無線ＬＡＮのアクセスポイントが悪用されたりする危険性があります。こうした危険性について事例を交えて解説します。また、それぞれの事例における問題点とその解決策について説明します。

(1) 通信内容が盗み見られる

無線ＬＡＮでは電波を使って情報を送受信します。そのため、適切な情報セキュリティ対策が取られていないと、電波が届くところから気がつかないうちに通信内容が盗み見られることがあります。家の中で使っているからと思っていても、家の外まで電波が届いて盗み見られてしまうこともあります。どのようなウェブサイトを閲覧したのかということに加え、ＩＤやパスワード、電子メールの内容等が知られてしまう危険性があります。

＜事例＞

Ａさんの無線ＬＡＮのアクセスポイントに友人Ｂが持ってきたゲーム機を繋げようとしたところ、うまくいかなかった。友人Ｂに「暗号を外して」と言われたＡさんは、アクセスポイントの暗号化機能を解除した。Ａさんは、その後も元に戻さないまま、無線ＬＡＮを使っていた。

近所のＣさんは、他の人の無線ＬＡＮの電波を受信していることを発見した。パソコン雑誌に載っていたＬＡＮ上の通信内容を確認するソフトをインストールして起動したところ、Ａさんのメールを見ることができた。ＣさんはＡさんの内容から、先週Ａさんが温泉に行ったことを知った。

翌日、ＡさんとＣさんが雑談していると、Ａさんは近所では誰にも話していない温泉の話をＣさんが話題に出したので驚き、メールが覗かれていると思った。

＜問題点＞

Ａさんは友人Ｂさんのゲーム機を接続するために暗号化機能を解除したため、アクセスポイントの情報セキュリティ設定が適切ではなくなり、Ｃさんが容易にＡさんのメールを見ることができた。

※　この事例では、「一般利用者が安心・安全に利用するためのガイドライン」の「１．(1) 大事な情報は、ＳＳＬでやりとり」及び「２．(1) アクセスポイントに適切な暗号化方式を設定」を守ることが大切です。

(2) 無線ＬＡＮが他人に利用されてしまう

情報セキュリティに関する設定をしていないアクセスポイントは誰でも利用できるため、あなたの無線ＬＡＮのアクセスポイントが他人に無断で使われてしまう危険性があります。

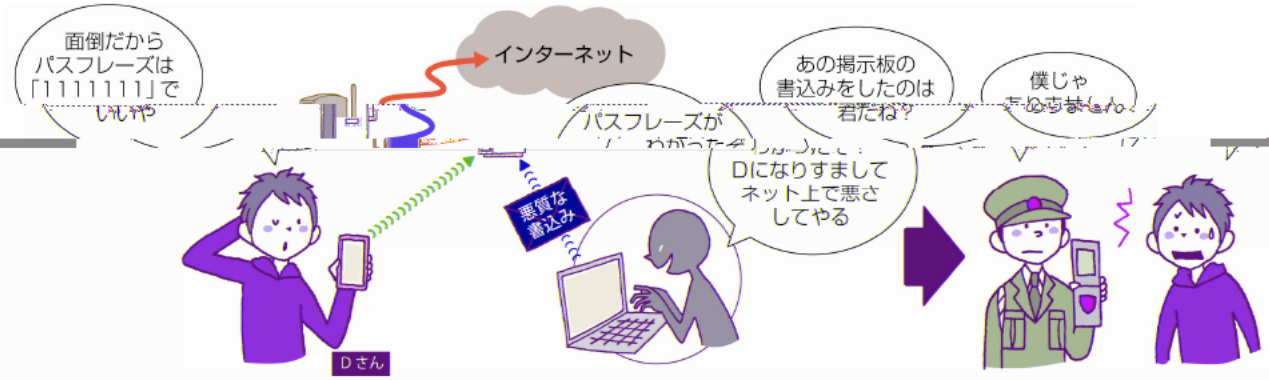
さらに、無断であなたの無線ＬＡＮが利用された上で、犯罪予告の書込みやウイルスの配布などが行われると、あなたが犯人として疑われる可能性もあります。

＜事例＞

スマートフォンを利用するようになったＤさんは、スマートフォンを自宅の無線ＬＡＮに繋げようと考えた。スマートフォンに複雑なパスフレーズを入力するのが面倒だと考えたＤさんは、無線ＬＡＮのパスフレーズを「11111111」に変更してしまった。

後日、インターネット掲示板に犯罪を予告する書込みを行ったのではないかと警察から事情を聞かれた。

その後の調査で、Ｄさんの無線ＬＡＮのパスフレーズが推測され、無断で無線ＬＡＮのアクセスポイントが利用され、掲示板への書込みが行われていたことがわかった。



＜問題点＞

Ｄさんは適切に無線ＬＡＮの情報セキュリティ設定を行っていなかったため、容易に無線ＬＡＮのパスフレーズが推測され、何者かに無線ＬＡＮのアクセスポイントを不正利用されてしまった。

※　この事例では、「一般利用者が安心・安全に利用するためのガイドライン」の「２．(1) アクセスポイントに適切な暗号化方式を設定」を守ることが大切です。

(3) 無線ＬＡＮを利用する他の人から、無断で端末にアクセスされてしまう

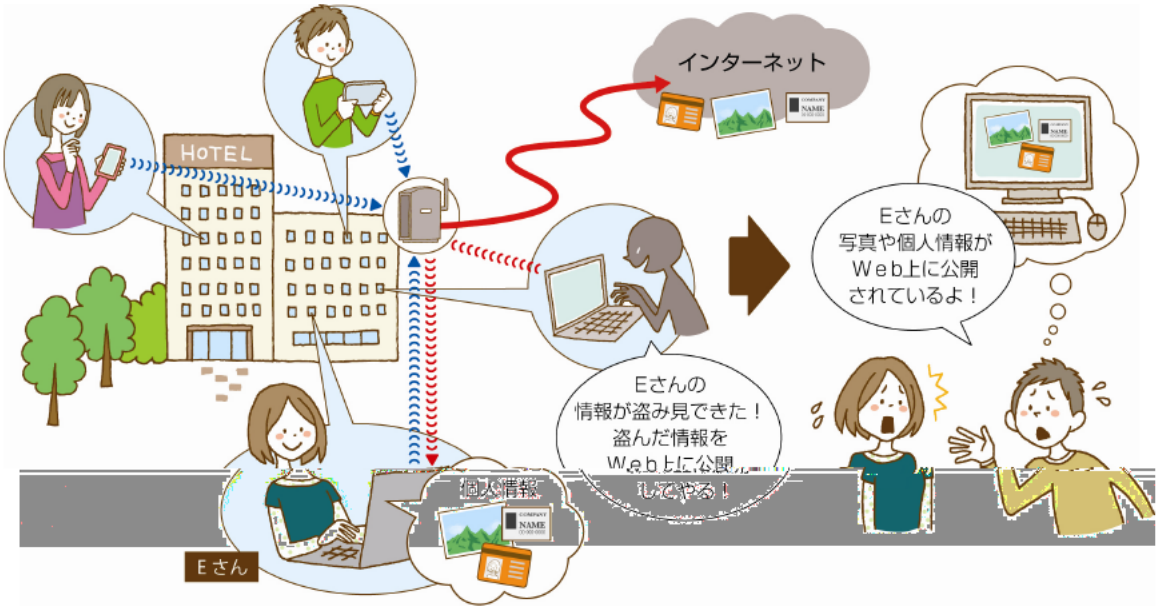
無線ＬＡＮの設定によっては、同じアクセスポイントを利用する他の人が、無線ＬＡＮを通じてあなたの端末にアクセスできる場合があります。その場合、あなたの端末に保存している写真やビデオ、電子メール等のプライバシー性の高い大事な情報が、他人に盗まれたり書き換えられたりする危険性があります。

＜事例＞

旅行に出かけたＥさんは、宿泊先で無線ＬＡＮが使えると聞き、持参したノートパソコンを無線ＬＡＮに接続してインターネットを利用した。

その後しばらくして、いたずら電話がかかってくるようになった。また、友人からインターネット上にＥさんの写真と名前、電話番号等が書かれていることを教えられた。

Ｅさんのノートパソコンはファイル共有機能が有効になっており、ノートパソコンに保存していた写真等が、宿泊先の無線ＬＡＮを利用していた他の人に盗まれてしまったのである。



＜問題点＞

Ｅさんはファイル共有機能を有効にしたまま、宿泊先の無線ＬＡＮサービスを利用したため、無線ＬＡＮを利用する他の人が、Ｅさんのパソコンに保存されている情報を見ることができる状態になっていた。その結果、パソコンに保存していた写真や個人情報が盗まれてしまった。

※　この事例では、「一般利用者が安心・安全に利用するためのガイドライン」の「１．(2) 公共の場では、ファイル共有機能を解除」を守ることが大切です。

(4) なりすました無線ＬＡＮのアクセスポイントに情報を盗み取られる

無線ＬＡＮのアクセスポイントに、同一の名称（SSID）、暗号化方式、パスフレーズが設定されると、それが本来接続するべき正しいアクセスポイントなのか、正しいアクセスポイントになりすました不正なアクセスポイントなのか判別できないことがあります。

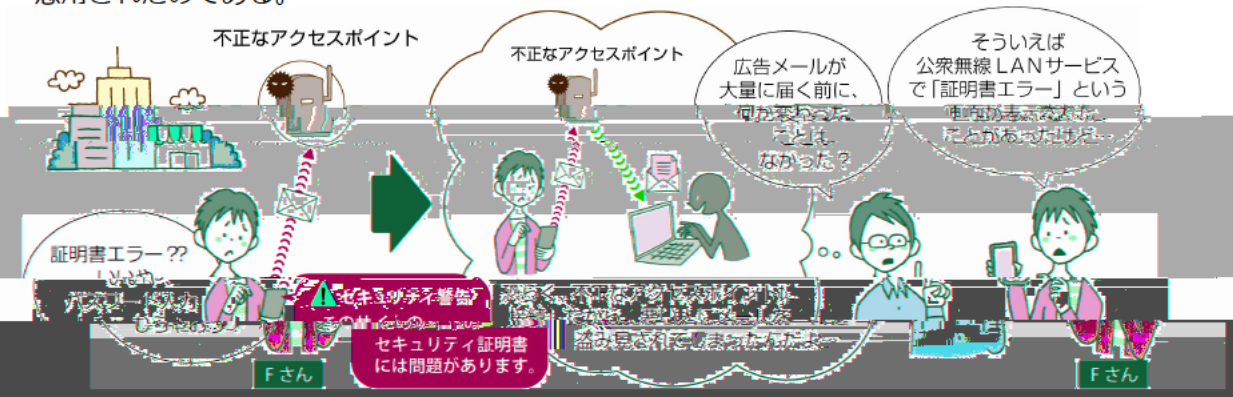
不正なアクセスポイントに気がつかずに接続すると、あなたのＩＤやパスワード、電子メールの内容等が盗み見られたり、ウイルスに感染させられたりする危険性があります[23]。

＜事例＞

Ｆさんは外出先でインターネットを利用しようと思った。利用できるアクセスポイントの一覧に、契約している公衆無線ＬＡＮサービスと同じ名前のアクセスポイントがあったので接続した。「証明書エラー」という画面が表示されたがよく分からなかったので、ＩＤとパスワードを入力した。いつも通りインターネットが使えたため気にせずメールを使ったり、ブログを更新したりした。

その後、Ｆさんのメールには多くの広告メールが届くようになった。どうやらＦさんの個人情報が流出したらしい。Ｆさんは原因がよくわからず、インターネットに詳しい友人に相談することにした。

いろいろ相談している内に、公衆無線ＬＡＮサービスで「証明書エラー」という画面が表示されたことを思い出した。どうやらＦさんは、公衆無線ＬＡＮサービスのアクセスポイントと全く同じ設定をした不正なアクセスポイントに気がつかずに接続してしまったようである。ブログの更新にはＳＳＬを使っていたため、ブログのＩＤやパスワード等は盗まれなかったが、電子メールにはＳＳＬを使っていなかったためメールアドレスが知られ、悪用されたのである。



＜問題点＞

公衆無線ＬＡＮサービスに接続する時に、証明書エラーが表示されるなど、いつもと違う様子に気がつかないまま、不正なアクセスポイントに接続したため、Ｆさんの個人情報は盗まれて悪用された。不正なアクセスポイントに接続していてもＳＳＬを使っていたブログの情報は盗まれなかった。

※ この事例では、「一般利用者が安心・安全に利用するためのガイドライン」の「1. (1) 大事な情報はＳＳＬでやりとり、(4) 公衆無線ＬＡＮサービスのログイン画面に電子証明書エラーが表示されたら接続しない及び(5) 接続しているアクセスポイントを確認」を守ることが大切です。

[23] ウイルス感染対策として、ウイルス対策ソフトの導入が有効です。

＜連絡先＞
総務省情報セキュリティ対策室
TEL： 03-5253-5749
FAX： 03-5253-5752
E-mail：wlan-security@ml.soumu.go.jp