安心して無線LANを利用するために

総　　務　　省

今日、無線ＬＡＮは、ブロードバンド・アクセスの手段として大きく期待され、その利便性から急速に普及しています。

無線ＬＡＮは無線を利用することから、無線に対応した適切なセキュリティ設定を行わないままで使用すると、盗聴、情報の改ざん、漏洩及び破壊などの重大な被害を受けかねません。しかしながら、現在のところ、このような危険性に対するユーザの認識は低く、セキュリティ対策が十分に行われていない状況にあります。

総務省では、こうした状況を踏まえ、無線ＬＡＮの健全な利用を促進するため、平成15年９月から、社団法人電波産業会への委託により、「無線LANセキュリティ調査研究会」（座長：吉田 進 京都大学教授）を開催し、無線ＬＡＮの技術動向、課題、セキュリティ対策等について調査研究を行ってきました。本書「安心して無線ＬＡＮを利用するために」は、この調査研究の結果等を受けて作成したものです。

本書は、無線ＬＡＮのセキュリティについて理解を深め、適切な対応をとることにより、無線ＬＡＮを安全に利用する方策を示しています。

本書によって無線LANの利用者がセキュリティに対する理解を深めることにより、無線LANを安全に利用し、無線LANによるブロードバンド・アクセスが促進されることを期待します。

なお、本書の理解に供するための参考資料も同時に作成し、総務省のホームページにおいて公開しておりますので、ご利用ください。

【　http://www.soumu.go.jp/joho_tsusin/lan/index.html　】

安心して無線ＬＡＮを利用するために

1　無線ＬＡＮを安全に使うためには

(1) 無線ＬＡＮの利用にあたって

近年、無線ＬＡＮは製品の低価格化と手軽さを背景に益々普及しており、家庭やオフィスにとどまらずあらゆるシーンで利用されることが期待されています。一方で、無線ＬＡＮを正しく利用しないことに起因する問題も数多く報道されています。

本書では、無線ＬＡＮのセキュリティの問題点について理解を深め、適切な対応をとることにより、無線ＬＡＮの特性を最大限に活用し、便利に安全に利用するための方策等について述べます。

(2) 無線ＬＡＮを適切に利用しないと生じる脅威

無線ＬＡＮの代表的なセキュリティ脅威として、「通信内容の傍受（盗聴）」、「無線ＬＡＮの不正利用」、「アクセスポイントのなりすまし」があります。以下、それぞれの脅威について事例を交えて解説します。

ア　通信内容の傍受

無線ＬＡＮでやりとりされるデータは、電波を利用して送受信されます。そのため無線ＬＡＮのセキュリティ技術を適切に利用しないと正規の利用者の目の届かない所で容易にデータを傍受することが可能となってしまいます。通信内容が傍受されることにより、

・ＩＤ、パスワードなどの個人情報

・メールの内容

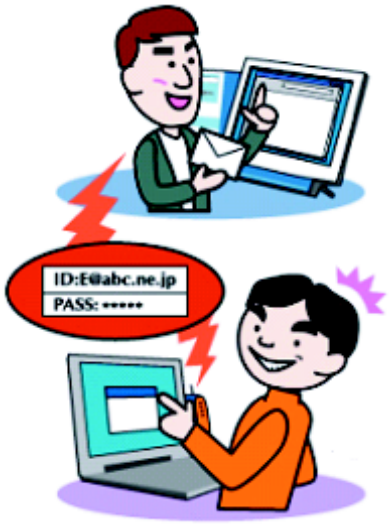
等の通信が盗み見られる可能性があります。

事例　通信内容の傍受１

Ｓさんが仕事の続きをするために自宅でノートパソコンを起動させたところ、他の人の無線ＬＡＮの電波を受信していることを発見。最近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、近所のＥさんの

メールアカウントとそのパスワードを偶然傍受することができた。Ｓさんは自分のパソコンのメールソフトをＥさんの設定にしてＥさんのメールを受信し、先週Ｅさんが最近温泉に行ったことを知った。

翌日、Ｓさんと雑談している中で、Ｅさんは近所では誰にも話していない温泉の話をＳさんが何気なく話題に出したので驚き、メールが覗かれていると思った。Ｅさんは、温泉のことだったので驚いただけで済んだが、他の人には知られてはいけない重要な秘密だったとしたら、と身も凍る思いをした。



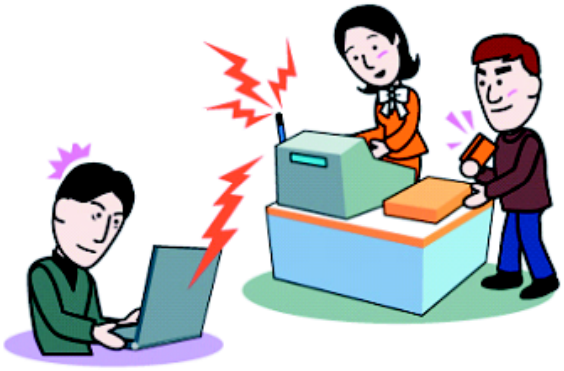
問題点

Ｅさんが適切に無線ＬＡＮのセキュリティ設定を行っていなかったため、Ｓさんが容易にＥさんのメールを見ることができた。

事例　通信内容の傍受２

商店Ａでは、顧客が商品を購入した際に利用する*ＰＯＳシステムに無線ＬＡＮを利用することで、作業性の向上と季節毎に行われるレイアウト変更時の作業量の減少を実現。無線ＬＡＮの導入により当初目的として掲げていたオペレーションコストの削減を実現した。

しかしながら、ある日商店Ａのお得意様の個人情報が流出していることが発覚した。更に調査を進めたところ、○月△日×時ごろ商店Ａでクレジットカードを利用して買い物をした複数の顧客にクレジットカードでの心当たりのない高額物品の購入などのトラブルが頻発していることも発覚した。



その後の調査で、商店Ａで利用していた無線ＬＡＮはセキュリティを未設定のまま利用しており、そこからＰＯＳ情報が流出したことが明らかとなった。

問題点

商店Ａが適切に無線ＬＡＮのセキュリティ設定を行っていなかったため、個人情報が流出しこのような事件が起こった。顧客に大きな損害を与えてしまうと同時に、商店Ａにとっても信頼の低下につながった。

＊　POS システム（Point Of Sales システム）
店舗等で商品を販売する毎に商品の販売情報を記録し、集計結果を在庫管理やマーケティングの材料として利用するためのシステム

イ　無線ＬＡＮの不正利用

セキュリティ設定を行わないアクセスポイントは、利用可能範囲にあるどんなパソコンからの接続も許可します。このことは、無線ＬＡＮを用いて他の人が通信を行うことも可能であることを意味します。

無線ＬＡＮを不正利用されることにより、

・　メール等を他人に送受信される　（なりすまし）
・　ホームページの内容を書き換えられる　（改ざん）
・　パソコン・サーバ上の個人情報の流出　（情報漏洩）
・　コンピュータウィルスの感染によるシステム破壊　（破壊）
・　ウィルスの配布や＊ＤｏＳ攻撃の踏み台にされる　（踏み台）

の可能性があります。

＊　DoS 攻撃（Denial of Services 攻撃）
ネットワークを通じて攻撃する手法。攻撃の対象物に大量のパケットデータを送りつけるなどして、使用不能に陥らせたりする。

事例　無線ＬＡＮの不正利用

Ｋさんが営業の合間にコーヒーショップでいつも持ち歩いているノートパソコンを開き午後の予定を確認していたところ、ノートパソコンに内蔵している無線ＬＡＮがネットワークに接続していることに気づいた。ネットワークの詳細を確認するとコーヒーシップの向かいにある、Ｔ社のネットワークであることがわかった。

その数日後、Ｔ社のホームページが改ざんされるとともに、Ｔ社から顧客に対して無数のウィルスメールが送信される事件があった。Ｋさんはこのことをニュースで知り、きっとＴ社の無線ＬＡＮの運用が適切でないからこのような事が起ったと思った。

問題点

Ｔ社が適切に無線ＬＡＮのセキュリティ設定を行っていなかったため、何者かに無線ＬＡＮを不正利用され簡単に社内ネットワークに侵入された。今回の事例では、ホームページの改ざんとウィルスメールの送付という被害だったが、社内の機密情報など重要データが流出し、更に被害が拡大する可能性があった。

ウ　アクセスポイントのなりすまし

従来の無線ＬＡＮ端末は、接続先のアクセスポイントが本来接続すべき正当なアクセスポイントであるか否かを確認することができません。このため、近隣に同一の設定を施した不正アクセスポイントが設置され、気づかずに重要な情報を不正なアクセスポイントのネットワークに流してしまい、その情報を搾取されてしまう可能性があります。

事例　アクセスポイントのなりすまし

Ｓさんは無線ＬＡＮを購入後、電源を入れたら何も設定せずに使えたのでそのまま使っていた。最近、無線ＬＡＮの接続が不安定になることがあったが、無線だから仕方がないと思いそのまま利用していた。

ところがある日からＳさんのメールには多くの広告メールが届くようになり、自宅にいたずら電話もかかってくるようになった。どうやらＳさんの個人情報が流出したらしい。Ｓさんは原因が良くわからず、インターネットに詳しい友人に相談することにした。

いろいろ調べてもらった結果、無線ＬＡＮを経由してＳさんの個人情報が流出したことが明らかになった。無線ＬＡＮが不安定だった理由は近隣のＸさんがＳさんのアクセスポイントと全く同じ設定にしてＳさんのアクセスポイントになりすましていたのである。Ｘさんが不正にＳさんの個人情報を流出させたらしい。ＳさんはＸさんのなりすましたアクセスポイントへ個人情報を送信していたのである。

問題点

Ｓさんが適切に無線ＬＡＮのセキュリティ設定を行っていなかったため、Ｘさんが、アクセスポイントのなりすましによりＳさんの個人情報を取得し、それを悪用した。

このように「通信内容の傍受（盗聴）」、「無線ＬＡＮの不正利用」、「アクセスポイントのなりすまし」は、無線ＬＡＮの設置者が被害を受けることは勿論、多くの人に被害が及ぶ可能性もあり、厳重な注意を払って無線ＬＡＮを利用する必要があります。

なお、無線通信を傍受して、その秘密を漏らし又は窃用すること、*暗号化された無線通信を傍受して、それを秘密漏洩・窃用目的で復元すること（復元の未遂を含みます。）のほか、他人のＩＤ・パスワードを無断で使用することは、電波法や不正アクセス行為の禁止等に関する法律により禁止されており、いずれも１年以下の懲役又は５０万円以下の罰金に処せられることがあります。

＊「暗号化された無線通信を傍受して、それを秘密漏洩・窃用目的で復元すること（復元の未遂を含みます。）」に対する罰則は、平成１６年６月８日から新たに施行されました。

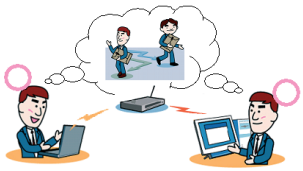
２　無線ＬＡＮを安全に利用するためのチェック項目

(1) 無線ＬＡＮ機器のセキュリティ機能

市販されている多くの無線ＬＡＮ製品は、利便性の観点から機種が異なっても接続が可能となるように作られています。これは、利用者が無線ＬＡＮ製品のセキュリティ設定を施さないと、他人が勝手に自分の通信を盗み見たり、自分のアクセスポイントに接続したりすることができることを意味しています。

現在の無線ＬＡＮ製品には、セキュリティ機能として表２－１の設定項目があります。

表２－１　無線ＬＡＮ製品のセキュリティ機能

セキュリティ機能	説　　明	
WEP	きちんと暗号化されていますね。 	無線LAN通信を暗号化するための規格です。（ただし、現在の WEP には脆弱性が指摘されています。）
MAC アドレス フィルタリング	アクセスポイントに端末のMACアドレスを登録した人は通信できて、登録していない人は通信できませんね。 	通信機器固有の識別子である MAC アドレスを用いてアクセスポイントに接続可能な無線 LAN 端末を制限する方式です。 （ただし、MAC アドレスは、容易に割り出し、詐称することができます。）
SSID	アクセスポイントの SSID を知っている人だけが通信でき、知らない人は通信できませんね。 	無線 LAN のネットワークの識別子として利用されており、アクセスポイントと同一のSSIDを設定した無線LAN端末が通信可能となります。 （ただし、現在では、Windows XPや一部の無線 LAN カードのユーティリティソフトを使うと SSID は容易に見ることができ、セキュリティ機能として用いるには問題があります。このため、一部のアクセスポイントには SSID を隠蔽する機能(ステルス機能)が用意されており、これを用いることで SSID を容易に見ることができなくなります。）
IEEE802.1x認証	暗号化されたものを信頼する人たちが一人ひとりに届けてくれれば、安心して通信を行う事ができますよね。 	IEEE802.1xに対応した無線 LAN 端末（ノートパソコン等）とアクセスポイント、認証サーバを用いた、ユーザ認証と個別暗号の鍵配布を行う方式です。
WPA		WEP の脆弱性を補強するために Wi-Fi Allianceによって策定されたセキュリティ規格です。WPA はひとつの技術によるセキュリティ機能ではなく、ユーザ認証を行う「IEEE802.1x」、新しい暗号化方式である「TKIP」などを組み合わせて高セキュリティを実現しています。 WPAにはアクセスポイントと無線LAN端末にPre-Sharedキーを設定するWPA-PSK方式とIEEE802.1x認証と組み合わせて動作するWPA-EAP方式があります。

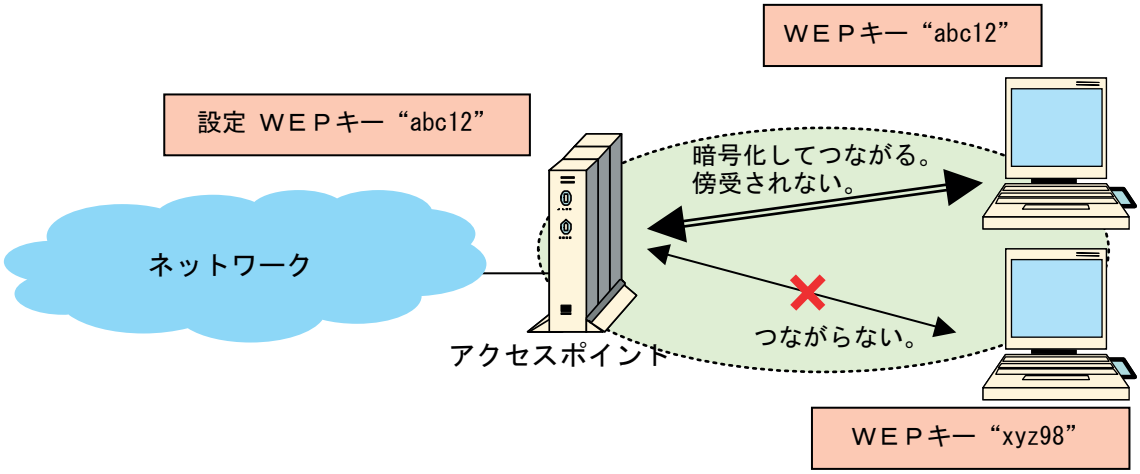
(2)　無線ＬＡＮのセキュリティ機能の詳細

ア　ＷＥＰの仕組み

・アクセスポイントと端末間をＷＥＰキーを使い暗号化して通信

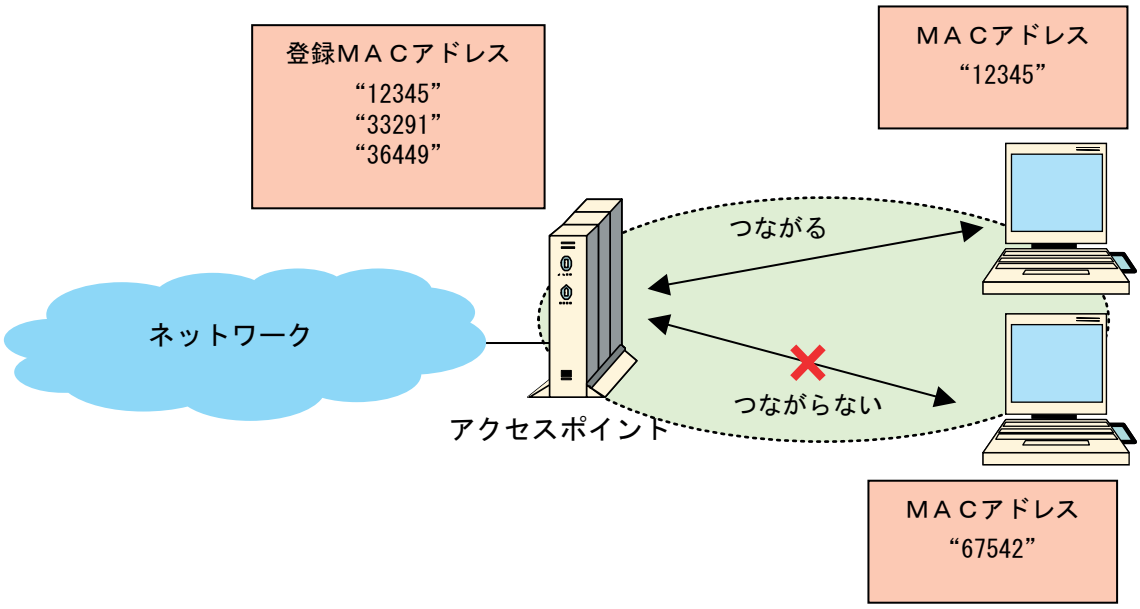
・ＷＥＰキーが一致した場合、傍受されずに通信ができます。

・ＷＥＰキーをかけない場合や、ＷＥＰキーが解読された場合、通信を傍受される可能性があります。



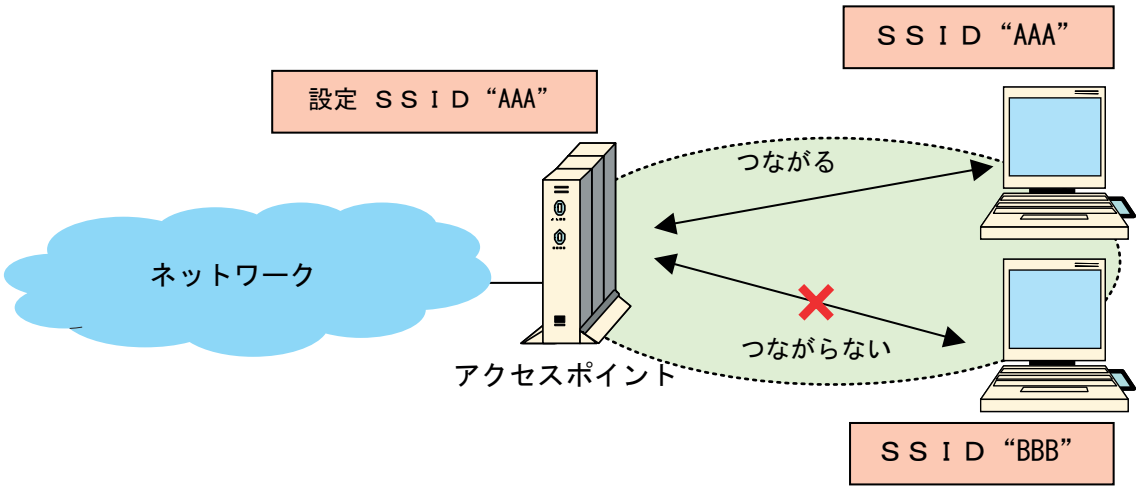
イ　ＭＡＣアドレスフィルタリングの仕組み

接続する端末のＭＡＣアドレスをアクセスポイントに登録。それ以外の端末は接続させません。



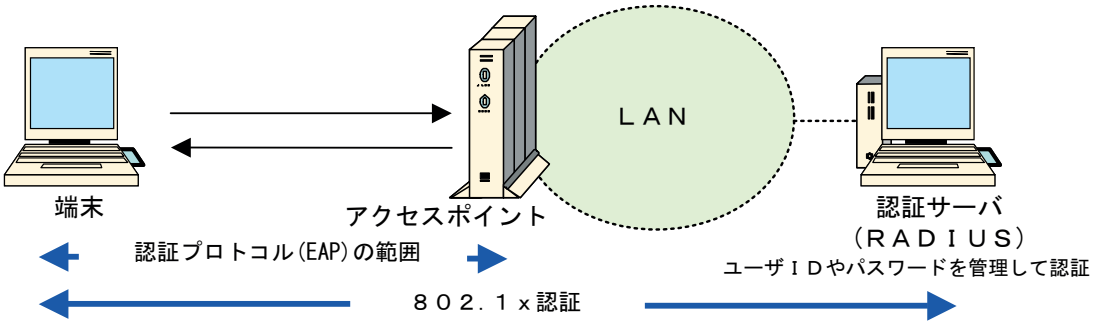
ウ　ＳＳＩＤ設定の仕組み

ＳＳＩＤは、無線ＬＡＮのネットワークの識別子であり、アクセスポイントと同一のＳＳＩＤを設定した無線ＬＡＮ端末のみが通信可能となります。



エ　ＩＥＥＥ802.1x認証の仕組み

認証サーバを用いて、ユーザ認証を行うとともに、ユーザ毎の個別暗号鍵の配布を行います。



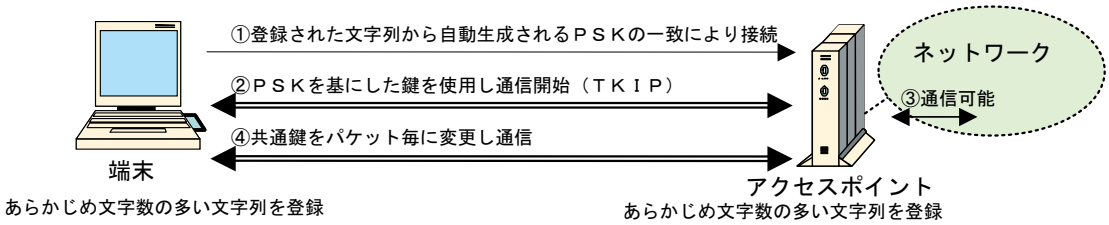
オ　ＷＰＡ－ＰＳＫ方式（小規模事業所や一般家庭向け）の仕組み

ＰＳＫ：事前共有鍵（Pre-Shared Key）

・アクセスポイントと、これと通信を行うすべての端末に共通の文字数の多い文字列を登録しておき、その文字から生成される128bitのＰＳＫにより端末を認証

・ＷＥＰと比べ強固な暗号方式を採用（ＴＫＩＰ）

・認証サーバ等を必要としない。



【ＴＫＩＰ】ＷＥＰを拡張した暗号方式　ＷＥＰとの主な違いは以下のとおりです。

・共有鍵を端末毎、接続毎に異なるよう、１パケット毎に変更

・暗号方式の複雑化のため、パケット毎に使われる鍵の不規則性を高める。

・暗号解読のヒントとなるＩＶ（Initialization Vector ：平文で通信する内部鍵）を避けて使用

カ　ＷＰＡ－ＥＡＰ方式（企業ユーザや公衆無線ＬＡＮ事業者向け）の仕組み

ユーザ認証「ＩＥＥＥ 802.1x」と新しい暗号化方式「ＴＫＩＰ」等を組み合わせて実現します(認証サーバ等の設置が必要です。)。

・認証サーバにより、端末を個別に認証

・認証サーバによる端末毎に異なる鍵の安全な配信

・通信中、パケット毎に暗号鍵を変更（ＴＫＩＰ）

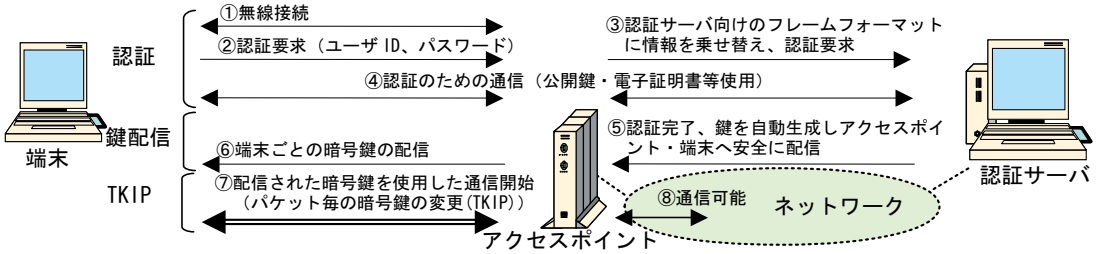


表２－２　各種セキュリティ機能と効果

セキュリティ機能	セキュリティ			単体効果
	不正アクセスの防止 無線LANのアクセスポイントの電波をつかめないようにするとともに、アクセスポイントのなりすましを防止	暗号化 他人に傍受されても通信内容が解読されないための技術	認証 正規利用者であるかの確認	
WEP	－	○	－	○
MACアドレスフィルタリング	－	－	△	△
SSID	△*	－	－	× （△*）
IEEE802.1x認証	－	－	○	○
WPA		◎	○	◎

◎：効果抜群　　○：効果あり　　△：ある程度効果あり　　×：効果薄

＊：ＳＳＩＤを容易に推測できない文字列にするとともに、ＳＳＩＤを隠蔽する機能(ステルス機能)を利用することにより、一定の効果があります。

(3) その他

無線ＬＡＮのセキュリティ機能はあくまでもアクセスポイントと無線ＬＡＮ端末間のセキュリティを確保するものであり、個人情報等の重要な情報の送信の場合には、無線ＬＡＮ端末から通信相手先までのエンドーエンドでセキュリティを確保するＳＳＬや、ＶＰＮ等を用いることが望まれます（表２－３参照）。

また、最近ではインターネットに接続していると、ウィルスメールを送られたりパソコンをスキャンされたりといった攻撃を受けることがあり、自己防衛のためにファイアウォールの設定やウィルス対策ソフトをインストールしておく必要があります（表２－４参照）。

このように無線ＬＡＮの利用時にも通常のインターネット利用時等と同等のセキュリティの確保に注意を払うことが重要です。

表２－３　ＶＰＮやＳＳＬの利用

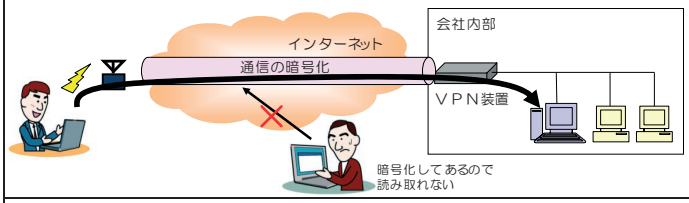
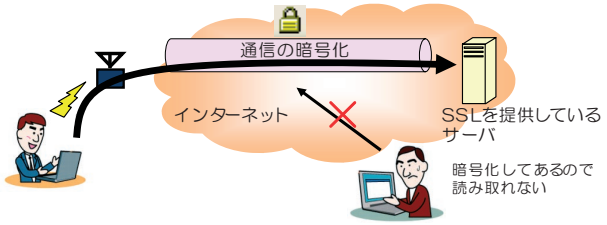
対策	説明
VPNの利用 	インターネットや IP ネットワークを仮想的に専用線のように利用するための技術です。専用線のような役割を果たしますので、社外から社内にあるサーバへセキュリティを確保しながら安全にアクセスを行うことができます。
SSLの利用 	データを暗号化してやり取りする方法です。 SSLを使用すると、送信するデータが暗号化されるので、 プライバシーに関わる情報を第三者に見られずにやり取りすることができます。

表２－４　その他の対策

対策	説明
ファイアウォールの設定	一般に、企業内LANなどを外部からの不正アクセスから保護する、あるいは企業内からインターネットへアクセスする場合に特定のサービスだけ使えるようにするシステムです。 また、インターネットからの不正アクセスや攻撃から個々のパソコンを守るための、パーソナルファイアウォールもあります。
ウィルス対策ソフトのインストール	コンピュータウィルスの侵入を検知し、駆除するためのソフトです。 ※セキュリティ対策ソフトの中に、ウィルス対策機能があるものとないものがあるので、購入の際に注意が必要です。

以上のような脅威並びにセキュリティ技術があることを十分認識して、現在利用している無線ＬＡＮ製品又は購入予定の無線ＬＡＮ製品の機能を確認し、本書に示す確認及び設定項目に従い適切な設定を行うことが必要です。

３　無線ＬＡＮを安全に利用するためのガイドライン

無線ＬＡＮを利用する代表的な場面として、「家庭」、「オフィス」、「公衆無線ＬＡＮサービス」及び「店舗開放型無線ＬＡＮサービス」を取り上げ、それぞれの環境による無線ＬＡＮのセキュリティレベル毎に、確認・設定すべき項目を以下のようにまとめました。

自身の利用シーンを確認して適切なレベルで無線ＬＡＮを利用することが重要です。

＊「公衆無線LANサービス」は通信事業者が提供する無線LANサービスと、「店舗開放型無線LANサービス」は店舗経営者等が顧客に無線LAN利用環境を開放提供するサービスと定義します。

(1) 家庭で利用する際の無線ＬＡＮセキュリティ設定

無線ＬＡＮはその利便性から一般家庭で広く使われるようになっていますが、セキュリティ対策を施さない無線ＬＡＮは自分だけでなく、設置したアクセスポイントが不正利用されることにより、インターネットを利用する多くの人に被害を与える可能性があります。このことを十分に留意して、表３－１の項目を確認し適切な対策を実施することが必要です。

表３－１　家庭で利用する際の無線ＬＡＮセキュリティの確認・設定項目

レベル	アナロジー（比喩）	セキュリティレベルの説明	設定項目	設定内容	効果	留意点
家庭 レベル０	内緒話を大声で行っている状況。誰にでも聞こえてしまいますね。 	無線 LAN のセキュリティ対策を全く施さない極めて危険なレベル。家の外から他人が勝手に接続できるレベルです。すぐに現在の利用環境を見直してください。	なにもしていません。			市販品及び事業者が配布するものの初期状態はこのレベルのものが多いです。
家庭 レベル１	内緒話はしないで封書にした状況。ただし透かしてみたら、字が読めてしまうことがあるかもしれませんね。 	これまでに多数市販されてきている無線 LAN 製品でも実現可能なセキュリティ対策。 まず初めに暗号化を行ってください（WEP の設定）。	WEP	アクセスポイントと無線 LAN 端末に同一の WEP キーを設定します。64bit と 128bit の WEP キーを選択できる場合は 128bit で設定します。なお WEP キーは容易に推測できない文字列を設定します。 また、アクセスポイントの WEP キーを定期的に交換します。 更新期間目安 *WEP キーの更新間隔は一般的な情報量のホームページを１日約 100ページ見ると仮定して算出。利用頻度の高い場合はこれより短い間隔で定期的に変更します。 64bit の場合：約 20日程度 128bit の場合：約 40日程度	通信内容の暗号化の実現。	WEP キーは、16 進設定と ASCII 設定がありますが、できるだけ 16 進設定をしてください。 WEP キーの 64bit を 40bit と表記している製品もあります。 128bit より長い WEP キーを設定可能な製品もありますが、異なるメーカー間での相互接続は保障されておりませんのでご注意ください。
			MAC アドレスフィルタリング	アクセスポイントに使用する無線 LAN 端末の MAC アドレスを設定します。	アクセスポイントに接続可能な無線 LAN 端末を制限することが可能。	特になし。
			SSID	SSID の内容から誰のアクセスポイントかを容易に推測できない文字列に設定します。SSID を隠蔽する機能（ステルス機能）の設定を行います。	個人を特定しにくくすることで、攻撃先にならないようにします。アクセスポイントの存在の秘匿。	SSID を隠蔽する機能（ステルス機能）を有しない製品もあるので確認してください。
家庭 レベル２	封書にして文書も暗号化した状況。これなら安心ですね。 	家庭で利用するにあたり高いセキュリティレベル。ただし WPA は比較的新しい製品のみで対応しています。今後購入を予定している場合にはセキュリティの観点から WPA 搭載を一つの基準に入れて選択してください。	WPA-PSK	アクセスポイントと無線 LAN 端末に Pre-Shared キーの設定を行います。なお、13 文字以上の文字列を設定することが望まれます（「%」、「&」などの記号を用いると更に効果的です。一部製品では使用できない場合があります）。	強固な暗号方式を実現。	Pre-Shared キーはパスフレーズで 63 文字まで設定可能です。

(2) オフィスで利用する際の無線ＬＡＮセキュリティ設定

無線ＬＡＮシステムの危険性は新聞等で数多く報道されていますが、そのほとんどのものは適切な無線ＬＡＮ設定を行わないために生じています。オフィスではシステム管理者のみならずその利用者も無線ＬＡＮを正しく理解し、適切に利用することが必要です。このことを十分に留意して、表３－２の項目を確認し適切な対策を実施することが求められます。

表3－2　オフィスで利用する際の無線ＬＡＮセキュリティの確認・設定項目

レベル	アナロジー（比喩）	セキュリティレベルの説明	設定項目	設定内容	効果	留意点
オフィス レベル0	内緒話を大声で行っている状況。誰にでも聞こえてしまいますね。 	無線 LAN のセキュリティ対策を全く施さない極めて危険なレベル。オフィスの外から他人が勝手に接続できるレベルです。すぐに現在の利用環境を見直してください。	なにもしていません。			市販品及び事業者が配布するものの初期状態はこのレベルのものが多いです。
オフィス レベル1	内緒話はしないで封書にした状況。ただし透かしてみたら、字が読めてしまうことがあるかもしれませんよね。 	これまでに多数市販されてきている無線 LAN 製品でも実現可能なセキュリティ対策。 ただし、オフィスでは、多くの人が利用していることで、暗号解読される可能性もあるため、更にレベルを上げてください。 まず初めに暗号化を行ってください（WEP の設定）。	WEP	アクセスポイントと無線 LAN 端末に同一の WEP キーを設定します。64bit と128bitの WEP キーを選択できる場合は128bit で容易に推測できない文字列を使います。 1 つのアクセスポイントで10人が利用し、1人が 1 日、一般的な情報量のホームページ約100ページ分の情報を利用すると仮定して、64bitの場合約 2 日、128bitの場合約 4 日で WEP 暗号解読される可能性があります。そのため、日々の運用管理が重要です。	通信内容の暗号化の実現。	WEP キーは、16 進設定と ASCII 設定がありますが、できるだけ 16進設定をしてください。 WEP キーの64bitを 40bit と表記している製品もあります。 128bitより長いWEPキーを設定可能な製品もありますが、製品間の相互接続は保証されておりませんので注意してください。
			MAC アドレスフィルタリング	使用する無線 LAN 端末の MAC アドレスをアクセスポイントに設定します。	アクセスポイントに接続可能な無線 LAN 端末を制限することが可能。	無線LAN端末台数が増えると、無線 LAN 端末の管理が煩雑になるなどの問題が出ます。
			SSID	SSID の内容から誰のアクセスポイントかを容易に推測できない文字列に設定します。SSID を隠蔽する機能（ステルス機能）の設定を行います。	企業名や部署名を特定しにくくすることで、攻撃先にならないようにします。 アクセスポイントの存在の秘匿。	SSID を隠蔽する機能（ステルス機能）を有しない製品もあるので確認してください。
オフィス レベル2	封書にして文書も暗号をした状況。これなら安心ですね。 	オフィスで利用するにあたり高いセキュリティレベル。ただし WPA は比較的新しい製品のみで対応しています。今後購入を予定している場合にはセキュリティの観点から WPA 搭載を一つの基準に入れて選択してください。	WPA- PSK	アクセスポイントと無線 LAN 端末に Pre-Shared キーの設定を行います。なお、13文字以上の文字列を設定することが望まれます（「%」、「&」などの記号を用いると更に効果的です。一部製品では使用できない場合があります）。	強固な暗号方式を実現。	Pre-Sharedキーはパスフレーズで 63文字まで設定可能です。

オフィス レベル 3	暗号化した文書を封書に入れ信頼できる配達人に確実に相手先に届けてもらう状況。これならかなり安心ですね。 	オフィス利用にも耐えうる高いセキュリティレベル。サーバ設定・運用など高度なIT技術を要するレベル。暗号鍵の動的配布・更新が可能です。 （右の設定のいずれかを選んでください。）	IEEE 802.1X 認証	RADIUSサーバの設置・設定とパソコンへのIEEE802.1X クライアントソフトのインストール・設定。	ユーザ認証と動的鍵配布・更新を実現。	構築・運用するためには、高度なIT スキルが必要です。システム構築・運用におけるコストがかかります。
			WPA-EAP	RADIUSサーバの設置・設定とパソコンへのIEEE802.1X クライアントソフトのインストール・設定。 アクセスポイントのWPA設定。	ユーザ認証と動的鍵配布・更新を実現。 強固な暗号方式を実現。	

注意事項：レベル１から３であっても、WEP キーや Pre-Shared キー、ユーザ認証の情報、WPA キーなどが第三者に漏れることがないように管理をしっかりと行ってください。鍵情報やユーザ認証の情報が流出すると、レベル０と同等になります。

(3) 公衆無線ＬＡＮサービス利用時の無線ＬＡＮセキュリティ確認

公衆無線ＬＡＮサービスは、事業者により様々な無線ＬＡＮセキュリティの仕組みがなされています。公衆無線ＬＡＮサービスを利用する際には、公衆無線ＬＡＮサービス事業者のサービス仕様を十分に確認し、不明な点は事業者に問い合わせることが必要であり、利用者自身も自己防衛対策を講じることが必要です。

公衆無線ＬＡＮサービスのセキュリティレベル判断基準として表３－３を、利用者の自己防衛対策として表３－４を参照してください。基本的には、レベル２の無線ＬＡＮサービスを利用することが望まれます。

表３－３　公衆無線ＬＡＮサービスのセキュリティレベル判断基準

レベル	アナロジー（比喩）	セキュリティレベルの説明	確認項目	確認内容	効果	留意点
公衆無線ＬＡＮサービス レベル 1	アンケートに答えるときに、個人情報のところにシールを張って他の人に見えないようにする状況。 	公衆無線LANサービスとしての最低限のレベル。	ログインID/パスワードの秘匿	WEP暗号化に加え、ログイン時の ID/パスワードを秘匿する仕組みとしてSSL等を利用しているかどうか。	ログイン情報の秘匿が可能。	ID/パスワードを人目に触れないようにします。パスワードは定期的に交換するように心掛けます。
公衆無線ＬＡＮサービス レベル 2	アンケートそのものを暗号化して回答する状況。これでは他人が見ても内容がわかりませんね。 	公衆無線LANサービスとしては十分なレベル。	IEEE802.1X 認証、動的鍵交換の利用	RADIUSサーバを使用して ID/パスワードや証明書による認証を行っているかどうか。	ユーザ認証と同時に暗号鍵の動的利用が可能。	ID/パスワードを人目に触れないようにします。パスワードは定期的に交換するように心掛けます。

表３－４　公衆無線ＬＡＮサービス利用者の自己防衛対策

	アナロジー（比喩）	セキュリティレベルの説明	設定項目	設定内容	効果	留意点
対策１ 全ユーザ向け	戸を閉めて、他人が勝手に入ってこられない状況。 	公衆無線LANサービスを利用する際に最低限注意を払うレベル。	共有フォルダの設定解除	公衆無線 LAN サービスを利用する際は無線 LAN 共有フォルダの設定を解除します。	共有フォルダ内のファイルを容易に搾取･改ざんされる可能性を低減することが可能。	公衆無線 LAN を利用する際に共有フォルダ設定が解除されていることを確認するようにしてください。
	部屋の中でも大事なものは引き出しにしまっておく状況。 		送信情報内容に関する注意	個人情報を送るときは、SSL 等の暗号化が行われていることを確認します。	個人情報等重要な情報の流出を防ぐことが可能。	
対策２ 全ユーザ向け	鍵を閉めて、更に防犯センサを取り付けている状況。これなら誰かが侵入しようとしたらわかりますね。 	公衆無線LANサービスを利用するにあたって標準的なレベル。	ウィルス対策ソフト･ファイアウォールソフトの活用	利用するパソコン等にウィルス対策ソフトやファイアウォールソフトをインストールしマニュアルに従い適切に設定します。	ネットワーク経由での脅威を低減することが可能。	ウィルス対策ソフトやファイアウォールソフトは、最新のものになっていることを確認するようにしてください。
対策３ ビジネスユーザ向け	大事なものを、信頼できる人に託して届けてもらう状況。 これならもう安心ですね。 	公衆無線LANサービスを利用するにあたって十分に安心できるレベル。	VPN の利用	無線LAN利用時にIPsec等の VPN 技術を併用します。	上位層での高セキュリティを実現。	クライアントソフトをインストールするのにある程度のスキルが必要です。 ある特定の通信相手との通信時のみ有効です。利用したいVPN技術がサポートされていることを確認してください。

(4) 店舗開放型無線ＬＡＮサービス利用者の無線ＬＡＮセキュリティ確認

街中の店舗等において顧客に対して独自に無線ＬＡＮ環境を開放提供しているような環境では、一般的に店舗を利用する顧客に自由に使ってもらうことを目的としているため、無線ＬＡＮのセキュリティの観点では対策を行っていないことが多くあります。

店舗開放型無線ＬＡＮサービスを運用する側においては、表３－５のような点に注意を払うとともに、利用者においては表３－６のような自己防衛対策を講じることが重要です。

表３－５　店舗開放型無線ＬＡＮサービスを運用する側の注意事項

導入時	無線 LAN の利用可能エリアを把握し、アクセスポイントの発射する電波の出力の調整や設置場所の工夫によって、利用想定外のエリアで利用できないように適正化を図ること。
運用時	なりすましや不正アクセスに用いられるおそれがあるため、ネットワークを自衛する観点から、適切な措置を講じるとともに、必要最小限の範囲で「誰が」、「いつ」、「どこで」利用したかを確認できるようにしておくことが望まれる。

表３－６　店舗開放型無線ＬＡＮサービス利用者の自己防衛対策

	アナロジー（比喩）	セキュリティレベルの説明	対策	対策内容	効果	留意点
対策１ 全ユーザ向け	戸を閉めて、他人が勝手に入ってこられない状況。 	店舗開放型無線 LAN サービスを利用する際に最低限注意を払うレベル。	共有フォルダの設定解除	店舗開放型無線 LAN サービスを利用する際は無線 LAN 共有フォルダの設定を解除します。	共有フォルダ内のファイルを容易に搾取・改ざんされる可能性を低減することが可能。	店舗開放型無線LANサービスを利用する際に共有フォルダ設定が解除されていることを確認するようにしてください。
	部屋の中でも大事なものは引き出しにしまっておく状況。 		送信情報内容に関する注意	個人情報を送るときは、SSL 等の暗号化が行われていることを確認します。	個人情報等重要な情報の流出を防ぐことが可能。	
対策２ 全ユーザ向け	鍵を閉めて、更に防犯センサを取り付けている状況。これなら誰かが侵入しようとしたらわかりますね。 	店舗開放型無線 LAN サービスを利用するにあたって標準的なレベル。	ウィルス対策ソフト・ファイアウォールソフトの活用	利用するパソコン等にウィルス対策ソフトやファイアウォールソフトをインストールしマニュアルに従い適切に設定します。	ネットワーク経由での脅威を低減することが可能。	ウィルス対策ソフトやファイアウォールソフトは、最新のものになっていることを確認するようにしてください。
対策３ ビジネスユーザ向け	大事なものを、信頼できる人に託して届けてもらう状況。 これならもう安心ですね。 	店舗開放型無線 LAN サービスを利用するにあたって十分に安心できるレベル。	VPN の利用	無線 LAN 利用時に IPsec 等の VPN 技術と併用します。	上位層での高セキュリティを実現。	クライアントソフトをインストールするのにある程度のスキルが必要です。 ある特定の通信相手との通信時のみ有効です。利用したい VPN 技術がサポートされていることを確認してください。

■連絡先■

総務省　総合通信基盤局電波部　移動通信課推進係

電話：(代表) 03-5253-5111　(内線) 5894　(直通) 03-5253-5894　FAX：03-5253-5946

H16.5