

「無線 LAN のセキュリティに関するガイドライン 改訂版」を改訂し
「無線 LAN のセキュリティに関する注意事項 第 1 版」に名称変更したものである

無線 LAN のセキュリティに 関する注意事項 第 1 版

2010 年 3 月

社団法人電子情報技術産業協会
パーソナルコンピュータ事業委員会
ホームデジタル専門委員会
無線 LAN 関連ガイドライン見直し WG

目次

1.	はじめに.....	1
2.	無線LANセキュリティの問題	2
3.	基本認識.....	3
4.	取り組み	4
4. 1.	ユーザの啓発について.....	4
4. 2.	無線LAN機器のセキュリティ機能設定について	6
4. 3.	無線LAN機器の用語について	7

付録

付-1.	お客様向けQ&A.....	8
付-2.	安全に使うためのチェックポイント.....	10
付-3.	用語解説	11
付-3.1	解説	11
付-3.2	用語説明一覧.....	18

1. はじめに

本書は、無線 LAN セキュリティの設定に関してとりまとめたものです。各位が速やかな対応を図られることを希望します。

*: 本書に掲載している用語については、使用者の責任において登録商標の確認および許諾を行うこと

2. 無線LANセキュリティの問題

何故、無線LANにセキュリティ機能が必要なのか？

セキュリティ機能の設定をしないと、無線 LAN の電波が届く範囲内であれば誰でも特別なツールを使わずに、通信内容を傍受、あるいはネットワークに侵入できる可能性があります。これを防止するためにもセキュリティ機能の設定が必要となります。

3. 基本認識

無線 LAN セキュリティの問題に関する基本認識は次の通りです。

① 無線LANセキュリティの重要性をユーザに認識してもらい正しく使っていただけるように啓発する。

無線 LAN 機器の低価格化と設定の容易化により中小企業や一般家庭、大企業の一部門など、専門知識がないユーザでも簡単に無線 LAN 環境を構築できるようになっています。これらユーザの多くがまったくセキュリティ機能を設定せずに使用したため、通信の内容を盗み見られたり、自分のパソコンに侵入されたりした事例が発生しています。このような専門知識をもたないユーザに対して技術的内容を出来る限りわかりやすく解説して、少なくとも最低限の無線 LAN セキュリティ機能を必ず設定して正しく使っていただけるように啓発し続けることが必要です。

② メーカーだけではユーザへの啓発は難しく、関連事業者からの多面的協力が必要である。

メーカー以外にも、無線 LAN 機器／パソコンの販売店や、無線 LAN の設定サービスを提供する業者などの協力を得る必要があります。これら無線 LAN 関連事業者にも働きかけ、この問題の重要性を認識していただき啓発活動に協力いただくことが重要です。

③ 啓発活動と並行して、専門知識のないユーザでも簡単・確実に無線LANセキュリティの設定が行えるようメーカーとして、改善努力を続ける必要がある。

無線 LAN の知識が全くないユーザにとってセキュリティ機能を理解し正しく設定することは必ずしも容易ではありません。

そのため、マニュアル／設定方法の改善、セキュリティ機能のかけ忘れ防止策、セキュリティ機能の容易な設定化など更なる改善を続けることが必要です。

④ 最後に。

無線 LAN に必要なセキュリティ機能は通信内容、用途、業種によって千差万別です。例えば、一部の公衆無線 LAN サービスではまったくセキュリティをかけていない場合もありますが、このような場合はセキュリティの無いサービスであることを認識した上で、個人情報等を扱わない範囲で利用するようにユーザに意識していただくことが必要です。どのようなセキュリティ機能を使用するかは一律に決められないため、ユーザまたはユーザのネットワーク管理部門が責任を持ってセキュリティ機能を選択し、管理していただく必要があります。

4. 取り組み

上記、認識に基づき、以下の指針を策定しました。

- ・ ユーザの啓発について
 - ・ 無線 LAN 機器のセキュリティ機能設定について
 - ・ 無線 LAN 機器の用語について

4. 1. ユーザの啓発について

ユーザ啓発のため以下の手段を通じて情報提供・啓発活動を行っていくことを推奨します。無線 LAN 機器メーカーおよびパソコンメーカーの対応事項は以下の通りです。

JEITA 非加盟の関連メーカーに対してもこの情報を公開し、同様の対応を呼びかけるものです。

① 設計部門(マニュアル作成部門)

「ユーザマニュアル」を通じて、ユーザに対して無線 LAN セキュリティについての注意喚起を行う。但し、メーカー毎に表現が異なっている場合は、ユーザの誤解を生む可能性もあるので、業界統一の表現を採用する。

② 販売促進部門(ユーザ対応窓口部門など)


「ホームページ」、「カタログ」など、ユーザの目に触れる可能性の高い媒体を使い、無線 LAN セキュリティについての注意喚起をユーザに対して行う。但し、これも、「ユーザマニュアル」同様、メーカー毎に表現が異なっている場合は、ユーザの誤解を生む可能性もあるので、業界統一の表現を採用する。

③ 保守及びサービス業務部門

保守に関する案内・受付のホームページ等で、無線 LAN セキュリティの重要性・必要性の注意喚起を行う。

上記、啓発活動でユーザマニュアル、ホームページ、カタログ等で業界統一の表現を行うため、下記の注意喚起文を使用するものとします。

なお、これは、今後の技術の進歩などと共に、変更の可能性があります。また、メーカー毎に情報の追加もできるものとします。



無線 LAN 製品ご使用時におけるセキュリティに関するご注意

無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコン等と無線 LAN アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。

その反面、電波はある範囲内であれば障害物(壁等)を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

- ・ 通信内容を盗み見られる
悪意ある第三者が、電波を故意に傍受し、
ID やパスワード又はクレジットカード番号等の個人情報
メールの内容
等の通信内容を盗み見られる可能性があります。
- ・ 不正に侵入される
悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、
個人情報や機密情報を取り出す(情報漏洩)
特定の人物になりすまして通信し、不正な情報を流す(なりすまし)
傍受した通信内容を書き換えて発信する(改ざん)
コンピュータウイルスなどを流しデータやシステムを破壊する(破壊)
などの行為をされてしまう可能性があります。

本来、無線 LAN 製品は、セキュリティに関する仕組みを持っていますので、その設定を行って製品を使用することで、上記問題が発生する可能性は少なくなります。

セキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。

4. 2. 無線LAN機器のセキュリティ機能設定について

無線 LAN の専門知識がないユーザでも簡単・確実にセキュリティ機能の設定が行えるよう、無線 LAN アクセスポイントならびに無線 LAN 端末(無線 LAN 内蔵 PC、無線 LAN 内蔵電気機器、無線 LAN PCカード、無線 LAN USB ドングル等)に関して、下記の対応を取ることを推奨します

[適用対象製品]

無線 LAN アクセスポイント、無線 LAN 端末の製品で PC やその他電気機器に内蔵もしくは接続されるもの。

[適用対象外製品]

下記のもの本ガイドラインの適用対象外とします。

- ・ 2005 年 4 月 1 日以前から出荷されている無線 LAN アクセスポイントならびに無線 LAN 端末
- ・ ネットワーク管理者のいる事業所や、ネットワークオペレータが運用するネットワーク向けに出荷される無線 LAN アクセスポイントならびに無線 LAN 端末

[適用内容]

① 無線 LAN アクセスポイント

下記のいずれか、もしくは全ての対応を取ることを推奨します。

- ・ 初期セットアップの流れでセキュリティ機能設定画面を必ず通過し、暗号化機能の設定を促す。
- ・ 暗号化機能を有効にせずに初期セットアップを終了した場合、ユーザに対して警告を行う。
例) 「無線 LAN の暗号化機能が設定されていません。安全に御使用するために設定する事を強くお勧めします」。
- ・ 初期セットアップでユーザが意図してオフに設定しない限り、ユーザ使用時には機器毎にユニークな暗号化キーを使った暗号化機能がオンの状態となる。

② 無線 LAN 端末

下記、対応を取ることを推奨します。

- ・ 暗号化機能が有効になっていない無線 LAN アクセスポイントと接続する場合、ユーザに対して警告を行う。
例) 「セキュリティ設定が行われていない無線 LAN アクセスポイントに接続しようとしています。データ盗聴などの危険がありますので御注意ください」。

4.3. 無線LAN機器の用語について

通常、ユーザは無線 LAN 機器のマニュアルを見ながらセキュリティ機能の設定を行いますが、ここに使用される専門用語がメーカー毎に統一していないとユーザが混乱し、正しく設定されない可能性があります。

マニュアル等で使用する専門用語は、下表を参考に使用することを推奨します。

<用語一覧表>

推奨	別名(現在、各社で使用されている名称)
AES	
ANY プローブ応答禁止	ANY SSID に対する応答禁止, SSID ステルス
ANY 接続拒否	
IEEE802.1X	IEEE802.1x
MAC アドレスフィルタリング	MAC アドレスによる制限
PSK	事前共有キー
SSID	ESS-ID, ESSID, ネットワーク名, サービスセット識別子
SSID の隠蔽	SSID を見せない設定, SSID 非通知, SSID マスクビーコン, SSID ステルス
TKIP	
WEP キー	WEP 暗号化キー, 暗号化キー
WPA-PSK	
WPA2-PSK	
アドホック通信	無線 LAN パソコン間通信, コンピュータ相互通信, ピアツーピア通信
インフラストラクチャ通信	アクセスポイント通信, アクセスポイント経由通信
オープンシステム認証	
キーインデックス	WEP キー番号, キー番号
キー更新間隔	暗号化更新時間
共有キー認証	シェアードキー認証
無線 LAN	ワイヤレス LAN
無線 LAN アクセスポイント	ワイヤレス LAN ステーション, アクセスポイント, 親機, 各社の製品名称
無線 LAN 端末	子機, ワイヤレスステーション

なお、用語の説明については、付-4.1 を参照して下さい。



ユーザ啓発の一助として、お客さま向け Q&A(付-1)、安全に使うためのチェックポイント(付-2)、用語解説(付-3)を次頁以降に添付しますのでご利用ください。

付一1. お客様向け Q&A

- Q-01. なぜ無線 LAN ではセキュリティが重要なのですか？
どうして無線 LAN だけとりわけセキュリティの問題が取り上げられるのですか？
- A-01. 有線 LAN 環境では、通信はネットワークケーブルを流れるため、通信の内容を盗み見たり不正に侵入するためにはケーブルに物理的に近づく必要があります。これに対し、無線は電波の届く範囲であれば、目の届かないところで第三者が電波を傍受しても知ることが出来ません。無線 LAN を搭載したパソコン・無線アクセスポイントは特別な設定なしに全ての装置が相互に通信ができるように設計されています。セキュリティの設定を行わず無線通信を行うことは、鍵を掛けずに出かけるようなものであり、とても無用心な状態となります。
-
- Q-02. 無線 LAN 機器にはセキュリティ機能の設定は必要ですか？
- A-02. セキュリティ機能の設定は無線 LAN 通信を行うための必須の設定ではありません。しかしセキュリティ機能の設定を行っていない場合には、第三者が勝手に盗聴・侵入することが可能となりますので、セキュリティ機能の設定を行うことを強く推奨いたします。また電波法の改正により、セキュリティ機能の設定で暗号化された無線 LAN のデータを第三者が悪用を目的に解読した場合には、犯罪行為として罰則の対象となります。しかし暗号化されていないデータの場合には罰則の対象とはなりませんので、セキュリティ機能設定による無線 LAN データの暗号化を強く推奨致します。
-
- Q-03. セキュリティ機能の設定を行っていない場合にはどのようなことがおきますか？
- A-03. セキュリティ機能を設定しなかった場合、盗聴による情報漏洩、侵入によるなりすまし・改ざん・破壊などさまざまな被害にあう可能性があります。具体的には以下のような事例です。
- ①電波を故意に傍受し、ID やパスワード又はクレジットカード番号等の個人情報、メールの内容などを盗み見る。
 - ②無断で個人や会社内のネットワークへ侵入し、個人情報や機密情報を取り出したり、不正な情報を流す。さらに通信内容を書き換えて発信したり、コンピュータウイルスなどを流しデータやシステムを破壊する。
-
- Q-04. パーソナルファイアウォールを既に設定して使っています。どうして無線 LAN 機器のセキュリティ機能設定がさらに必要なのでしょうか？
- A-04. パーソナルファイアウォールもネットワークのセキュリティ確保に有効な手段ですが、保護する対象と目的が異なります。パーソナルファイアウォールはインターネット(WAN 側)からパソコンへの不正進入に対する防御壁の役目を果たします。一方無線 LAN のセキュリティ機能設定は、ネットワークの内側(LAN 側の無線区間)のデータの盗聴/漏洩やネットワークへの不正進入を防止する役目をします。そのため、それぞれ両者を同時に使用することを推奨致します。
-
- Q-05. セキュリティ機能にはどんな種類がありますか？
- A-05. 簡単に設定できるセキュリティ機能としては SSID で行うこと、MAC アドレスフィルタリングで行うこと、WEP や WPA/WPA2(無線 LAN の業界団体である Wi-Fi Alliance で制定したセキュリティ方式)で行うこと、などがあります。

無線 LAN のセキュリティに関する注意事項 第1版

- Q-06. SSID とはどんな機能で、どのように使用すればよいのでしょうか？
- A-06. ネットワークの識別名(SSID)をアクセスポイントに設定する事で、同じ SSID を設定した無線 LAN 機器のグループだけが接続可能になる機能です。設定した SSID は、第三者が簡単に見ることが出来るので、SSID に自分の苗字や組織名など利用者を特定できる名前は避けて、出来るだけ意味を持たない名前を設定するようにします。さらに一部の無線 LAN 機器には SSID が簡単に見られないようにする機能もあります。こちらを活用するのも有効です。
-
- Q-07. WEP とはどんな機能で、どのように使用すればよいのでしょうか？
- A-07. WEP キーと呼ばれる暗号化キーで無線 LAN 機器間のデータを暗号化する機能です。WEP キーとして 128 ビットまたは 64 ビットの設定が可能です。WEP には脆弱性が指摘されているため、より強固なセキュリティ方式である WPA や WPA2 の使用を推奨します。
-
- Q-08. WPA や WPA2 とはどのようなセキュリティ方式でしょうか？
- A-08. 無線 LAN の業界団体である Wi-Fi Alliance で制定されたセキュリティ強化のための規格です。WPA では WEP の脆弱性を回避するために TKIP (Temporal Key Integrity Protocol)による強力な暗号化をサポートします。WPA2 では TKIP よりもさらに強力な AES という暗号アルゴリズムをサポートします。
-
- Q-09. MAC アドレスフィルタリングとはどんな機能で、どのように使用すればよいのでしょうか？
- A-09. 個々の無線 LAN 機器が持つ機器固有番号 (MAC アドレス) をアクセスポイントにあらかじめ登録しておき、登録されている無線 LAN 端末(パソコン等)だけを接続可能または接続拒否にする機能です。ネットワークへの侵入防止に効果がありますが、盗聴防止には効果がありません。
-
- Q-10. 個々の機器が備えるセキュリティ機能を適切に使用すれば万全ですか？
- A-10. セキュリティ機能を適切に使用すれば、出かけるときに鍵を掛けたことに相当し、一般にはより安全な状態になります。ただし、ピッキングの例に見られるように、これだけで 100%の安心は出来ず、泥棒は手を換え品を換えてやって来ます。できるだけ高度な暗号化機能を利用し、WEP を利用する場合には SSID や WEP キーの変更を定期的に行うなど、セキュリティの維持に配慮した無線 LAN 機器の使用をお奨めします。
-
- Q-11. 偶然、電波を傍受し通信内容を知った場合になにか注意することはありますか？
- A-11. 電波法では電波を傍受して得た通信内容を第三者に漏洩することは違法となりますのでご注意ください。さらに暗号化された無線 LAN データの場合には、第三者に漏洩しなくても暗号を解読しようとする行為自体が、解読に成功しない未遂の場合も含めて、違法行為となりますので十分にご注意下さい。
-

付一2. 安全に使うためのチェックポイント

無線 LAN を安全に使うためには、次の3点をすべてカバーするように無線 LAN 機器を設定しましょう。

① SSIDは以下のように設定していますか？

無線 LAN アクセスポイントには工場出荷時に SSID が設定してありますが、製品名や個人名を第三者に類推されないようにできるだけ意味を持たない名前に変更しましょう。

また、「ANY 接続拒否」や「SSID の隠蔽」の機能を ON に設定しておくことで SSID を第三者に見られる危険性が少なくなります。

② MACアドレスフィルタリング(固有機器以外接続拒否)を設定していますか？

アクセスポイントの MAC アドレスフィルタリング機能を ON にして、無線 LAN 端末の MAC アドレスをアクセスポイントに登録しましょう。未登録の端末からの侵入防止に役立ちます。

③ 暗号化機能を設定していますか？

暗号化機能は WEP, TKIP, AES の3種類がありますが、WEP より TKIP、TKIP より AES の方が暗号の解読が難しいといわれています。そこで、無線 LAN アクセスポイントと無線 LAN 端末の暗号化機能が同じときは最も解読の難しい暗号化機能に設定しましょう。無線 LAN アクセスポイントと無線 LAN 端末の暗号化機能は同じでなければ通信できません。例えば、アクセスポイントが AES、TKIP、WEP に対応していても端末が WEP しか持たない場合は、アクセスポイントも WEP に設定します。

1) WEP(共通鍵暗号方式)に設定する場合

暗号化キー(WEP キー)のビット長を最大に設定しましょう。たとえば、64ビット、128ビットの2種類に対応していれば、128ビットで設定します。

もし、無線 LAN アクセスポイントも端末も 152 ビットをサポートしている場合は 152 ビットを設定しましょう。また、WEP キーは最低でも月に1回程度は変更することを推奨します。

- ・ なるべく辞書に載っている単語を使わない
- ・ 無意味な英数字と記号を適宜組み合わせる

2) WPA-PSK(TKIP)/WPA2-PSK(AES)に設定する場合

安全のために、PSK(プリシェアードキー)を文字入力する場合は次の設定を推奨します。

- ・ なるべく辞書に載っている単語を使わない
- ・ 無意味な英数字と記号を適宜組み合わせる
- ・ 文字数を少なくとも 13 文字以上、できれば 20 文字以上とする

付一3. 用語解説

付一3.1 解説

■ LAN

LAN(ラン:Local Area Network)とは、複数台のパソコン等を、相互に接続して作られた状態(これをネットワークといいます)を表す言葉です。

有線 LAN

LAN 構築時、複数台のパソコンを接続する方法として、“イーサネット”と呼ばれる LAN 接続規格を用いるのが一般的です。イーサネットでの LAN 接続には、“LAN カード”と呼ばれるパソコン機器と、LAN ケーブルが必要になります。

このような方式を、後述する“無線 LAN”と対比して、この技術解説では“有線 LAN”と呼びます。

無線 LAN

無線 LAN とは、上記有線 LAN の LAN ケーブル部を無線に置き換えたものです。

無線 LAN での LAN 接続には、各パソコン等に取り付けられる“無線 LAN カード”と送受信される無線電波の相手側となる“無線 LAN アクセスポイント(Access Point)”から構成されています。無線 LAN アクセスポイントは、イーサネットにて利用されるハブ(Hub)の機能も有しています。

■ セキュリティ

LAN や無線 LAN では、LAN 接続されたパソコンが相互に通信できるように、決められた手順(プロトコル:Protocol)で通信することになっています。これは、決められた手順を守れば第三者のパソコンであっても、相互に通信することができ、これにより、第三者に、他のパソコン中のファイルや周辺機器が利用される可能性のあることを意味しています。

第三者に、パソコンのファイルや周辺機器を利用されたり、通信内容を盗聴されることを防ぐために、LAN では安全保護を行うことが強く推奨されています。この安全保護のことを“セキュリティ(Security)”といいます。

ただし、セキュリティ方式は常に万全ではありません。そのため、多重にセキュリティを施すことが、LAN 全体のセキュリティを向上させることになります。

有線 LAN と無線 LAN の差異

近年普及をみせる無線 LAN においては、従来以上のセキュリティが要求されています。有線 LAN での LAN 接続と、無線 LAN を用いての LAN 接続の違いから、セキュリティの対応内容にどのような違いがあるかを以下に説明します。

従来の有線 LAN 接続では、第三者は直接 LAN ケーブルに、LAN アダプターを介して接続しなければなりません。これはオフィスや家庭内の LAN に接続するためには、そのオフィス内や家庭内に侵入しないと LAN 接続出来ないことになります。よって、LAN でのセキュリティ以外に、オフィスや家庭の戸締りや不審者の立入りを禁止することも LAN 接続のセキュリティと考えることができます。

一方、無線 LAN では、無線電波の届く範囲であればオフィスや家庭内に侵入しなくても、PC に接続された無線 LAN カードで無線電波を受信し、LAN 接続をおこなうことができます。

無線 LAN の場合、戸締りや不審者の立入りを禁止しても LAN 接続のセキュリティとすることができません。有線 LAN に比べて、第三者の侵入を許す可能性が高いことになります。有線 LAN 接続以上にセキュリティの配慮が求められるのは、上記理由によります。

■ LAN のセキュリティ

有線 LAN および無線 LAN ともに、セキュリティ方式は大きく2つ(接続制限・暗号化)に分けられます。それぞれの方式は、独立して動作する場合や、協調して動作する場合があります。

接続制限

LAN 接続を行うユーザ/機器が LAN 接続を許可されているユーザ/機器であるかを確認し、承認されることで LAN 接続をおこなう方式です。これら確認作業を“認証(authentication)”と呼びます。認証にて、認証対象が利用者(ユーザ)である場合は、“ユーザ認証(User Authentication)、機器である場合は”機器認証“と呼び、メールやファイルなどの場合は、“デジタル認証“と呼ばれます。

- ・ **ユーザ認証**

ユーザ認証では、“ユーザ名”と“パスワード”を用いてログインや保護されたリソースへのアクセス許可を行います。銀行の ATM での暗証番号入力も、一種のユーザ認証であるといえます。また、ID カードや指紋・網膜を利用した方式もあります。

- ・ **機器認証**

機器認証では、利用機器固有の値を用いて、その機器が“なりすまし等”のない正しい機器であるかどうかを確認します。

・ **デジタル認証**

デジタル認証 (digital authentication) とは、電子メールやオンライン取引などにおいて、そのメッセージが正当な発信者から発信され、途中で改ざんなどが行なわれていないことを確認する方式です。認証作業には、添付された“デジタル署名”を用います。

暗号化 (encryption)

暗号とは、決められた規則に基づいて変換させたデータのことです。このデータを生成する手順を“暗号化”、暗号化されたデータを元に戻す手順を“復号”と呼びます。

暗号化されたデータは、決められた規則を知らなければ元のデータに戻せないため、規則を知らない第三者は、たとえ暗号化されたデータを入手しても、その中身を判読することができません。

暗号化する規則が公開されている場合などでは、規則を知る全員が内容を判読できます。これを避けるには、暗号化するごとに規則を変化させる必要があります。このときに用いられるのが、“暗号鍵”です。暗号鍵を知らなければ、データの暗号化・復号をすることができません。

暗号鍵を用いた暗号化には、“共有鍵暗号方式”と“公開鍵暗号方式”の2つがあります。

■ ■ ■ **メモ** ■ ■ ■

LAN 接続を行うには、接続する LAN 毎に指定されたパラメータを設定する必要があります。有線 LAN・無線 LAN とともに、“IP アドレス”等関連の値を知らない場合は、物理的に LAN 接続を行っても、LAN を利用できません。

しかしながら、不正な LAN 接続を試みるユーザは、これらのパラメータを LAN 上を流れるデータから簡単に割り出すことができるため、あまりセキュリティには使えないものとなります。

■ **無線 LAN のセキュリティ**

無線 LAN のセキュリティにおいても、前記“接続制限”および“暗号化”が一般的です。

以下の方式が一般的です。

接続制限方式: SSID、MAC アドレスフィルタリング

暗号化方式: WEP、WPA/WPA2

下記に、それぞれの詳細を説明します。

SSID

接続先のネットワークを識別するための ID で、英数文字 32 文字までの範囲で設定可能です。無線 LAN アクセスポイントに SSID を設定しておき、その無線 LAN アクセスポイントと接続するパソコン等にも同じ SSID を設定する事で、通信が可能になります。このように、SSID で、接続する無線 LAN アクセスポイントを指定する事が出来ます。SSID は、セキュリティ機能の一つに分類される場合もありますが、あくまでも接続先の識別機能ですので、SSID を設定しただけでセキュリティを設定したつもりにはなりません。

無線 LAN のセキュリティに関する注意事項 第1版

IEEE802.11 の仕様により、無線 LAN アクセスポイントの SSID を知らなくても、参照する事は可能です。従って、ネットワークを所有する個人や会社名が推測可能な SSID にすると、たまたま SSID を参照した人の興味を引く事になり望ましくありません。また、パソコン等の SSID 設定を空白や“ANY”という文字列にする事は避けるべきです。

製品により、SSID 以外に、ESSID、ネットワーク名、Network Name と表記してある場合があります。

MAC アドレスフィルタリング

無線 LAN カードには、有線 LAN とおなじく、一つひとつに MAC アドレスが設定されています。

MAC アドレスとはすべてのネットワークカードに付与される番号で 12 桁の 16 進数(48 ビット)で表します。前半 24 ビットがメーカー固有の ID で、後半 24 ビットが各メーカー内の連番となっています。すべてのネットカードに異なる値が設定されおり、世界中に一つしかないユニークな番号になっています。

この無線 LAN カードの MAC アドレスを無線 LAN アクセスポイントに登録することによって、許可されたパソコン等以外は無線 LAN アクセスポイントに接続することが不可能になります。この機能を MAC アドレスフィルタリングといいます。無線 LAN アクセスポイントへの設定方法は機種によって異なりますが、接続可能な MAC アドレスを登録する方式や、接続を排除する MAC アドレスを登録する方式があります。

WEP (Wired Equivalent Privacy)

無線 LAN 規格(IEEE802.11)にて規格化されている“暗号化”方式の一つです。

直訳は、“有線 LAN と同等のプライバシー機能”となり、無線 LAN に対するセキュリティの有効な手段とされています。

WEP を設定することで、無線電波が第三者に傍受されても、暗号を解読しないとデータの中身を判読することができなくなり、また無線 LAN に侵入することもできません。

WEP 機能は、パソコン等および無線 LAN アクセスポイント側の両方に『WEP キー(WEP 暗号化鍵)』を設定する必要があります。市販の無線 LAN 製品は、64ビットおよび128ビット長の WEP キーをサポートしています。各ビット長の内、ユーザが設定できる WEP キー長は、それぞれ「40-bit (5-byte)」、「104-bit (13-byte)」となります。残りの 24 ビットは IV (Initialization Vector) と言われる自動的にパソコンや無線 LAN アクセスポイントにより付加されるデータとなります。WEP には脆弱性が指摘されているため、より強固なセキュリティ方式である WPA や WPA2 の使用を推奨します。

WPA (Wi-Fi Protected Access) / WPA2

無線 LAN の業界団体である Wi-Fi Alliance(*1)で制定された、無線 LAN のセキュリティ強化のための規格です。WPA/WPA2 では以下の点が強化されています。

1. IEEE 802.1X による認証をサポートします。IEEE 802.1X は認証のためのサーバを必要とし

無線 LAN のセキュリティに関する注意事項 第1版

ますが、WPA/WPA2 では認証サーバを必要とするエンタープライズモードと認証サーバを利用しないホームモードがあります。ホームモードでは仮共有キーによる WPA-PSK を利用します。

2. WPA では TKIP (Temporal Key Integrity Protocol) による強力な暗号化をサポートします。WEP では 24 ビットの IV (Initialization Vector) をユーザの設定した WEP キーと単純に組み合わせることで暗号キーを生成していました。TKIP では新しいキー生成アルゴリズムを用い、ユーザにより設定された仮共有キーである WPA-PSK もしくは IEEE 802.1X により生成されたキーと IV および MAC アドレスからキーを生成します。IV のビット長も 48 ビットに拡張され、キーは定期的に更新されます。キーが定期的に更新される事により、無線 LAN の通信が盗聴され、キーが解読されたとしても、すぐにキーが更新されるので、WEP と比較して高いセキュリティを実現しています。
3. WPA2 では TKIP よりさらに強固な暗号アルゴリズムとして AES (Advanced Encryption Standard) というアメリカ国務省標準技術局 (NIST) が定めた新しい暗号アルゴリズムを採用しています。

(*1) Wi-Fi Alliance

無線 LAN の推進・相互運用性を保証するための業界団体。

Wi-Fi Alliance のテストラボでの認定テストにパスした製品には Wi-Fi CERTIFIED の認定が与えられます。

IEEE802.1X

ユーザ認証の方式として、IEEE802.1X があります。

IEEE802.1X では通信を開始する前にユーザ名、パスワードや電子証明書を使って認証をおこない、認証されたユーザのみが通信を許可されます。これにより、不正なユーザのアクセスを禁止することが出来ます。

IEEE802.1X の実現のためには、無線 LAN カード、無線 LAN アクセスポイントがともに、IEEE802.1X に対応している必要があり、認証サーバも必要となります。このため、家庭の個人が使用するというよりは、オフィス等の大勢の人数での使用時に集中的に管理するのに適した方法といえます。

有線 LAN の仕様として規格されたものですが、一般に無線 LAN での認証の仕様として使用されています。認証動作には、EAP (RFC2284) を使用します。EAP を実現するためには、外部サーバ (RADIUS サーバ) を用いるのが一般的です。

- RADIUS (Remote Authentication Dial-in User Service)
VPN や無線 LAN 等様々なネットワークサービスでの認証プロトコルに利用されています。本プロトコルを実行するサーバを RADIUS サーバと呼びます。
また、認証 (Authentication) 以外に承認 (Authorization)、課金 (Accounting) も実装されています。

- EAP (Extensible Authentication Protocol)
PPP(Point To Point Protocol ダイアルアップで接続のときに必要なプロトコル)における認証方式を拡張したプロトコルで、無線 LAN や有線 LAN の接続制限のために利用されています。RFC2284 にて規定されており、IEEE802.1X で採用されています。EAP には多くの方式があります。

■ 更に強固なセキュリティ方式

セキュリティ方式は常に万全ではないため、多様なセキュリティ方式を多重に実施することが、更なるセキュリティ強化につながります。

以下に、無線 LAN 関連以外のセキュリティ方式について説明します。一部のセキュリティ方式では、“接続制限方式”と“暗号化方式”を同時に利用しています。

VPN (Virtual Private Network)

インターネットなどの第三者が存在する公衆回線等を経由しながらも、安全な通信を可能にするセキュリティ技術のこと。企業等においては、専用線の代替インフラとして、普及を見せています。VPN にて LAN 通信を行う場合は、パソコン側に専用の VPN アプリケーションと、相手側に VPN 機能を備えた専用装置(以下、VPN 装置)が必要となります。最近では LAN 機器であるルータやファイアウォールにその機能が含まれています。

VPN 機能の実装は VPN 装置に依存するため、基本的には同じ(ベンダーの)装置でなければ通信はできません。しかし、インターネット技術の標準化を進める IETF により、IPSec (Internet Protocol Security) というパケットの暗号化と認証技術が標準化されているため、IPSec をサポートした VPN 装置であれば、互いに通信が可能とされています。

IPsec(IP Security)

TCP/IP 環境で IP パケットの暗号化と認証を行うセキュリティ技術です。

L2TP (Layer2 Tunneling Protocol) などのデータリンク層でのトンネリングプロトコルと異なり、ネットワーク層で動作します。

■ LAN に関する用語補足

インフラストラクチャモード

無線 LAN アクセスポイントを利用して通信を行うモードです。通常、パソコン等をインターネットに接続して使う場合は、このモードに設定します。このモードで、無線 LAN アクセスポイントとパソコン等で通信を行うには、まず無線 LAN アクセスポイントに SSID を設定します。パソコン等は、接続したい無線 LAN アクセスポイントと同じ SSID に設定すれば接続できます。

WEP や MAC アドレスフィルタリング等のセキュリティを設定してください。

アドホックモード

無線 LAN アクセスポイントが不要で、直接無線 LAN 対応のパソコン同士での通信を行うモードです。無線 LAN アクセスポイントの無い場所で、無線 LAN 対応のパソコン同士でデータを転送したり、共有するのに便利です。このモードを利用する場合、セキュリティに関する設定が出来ない場合があります。

ファイル共有

ネットワークに接続されたパソコン同士で、自分のコンピュータにあるファイルを他人がアクセスできる状態にし、複数人でファイルを共有すること。単一のファイルでなく、ファイルを格納しているフォルダ単位等で共有できるように指定出来ます。

この機能により、自分のコンピュータに保存されているデータを簡単にネットワークに接続された他のパソコン等から参照することができるようになります。ファイルへの書き込み、読み出しなど、他人にどのような操作を許可するかを設定することが出来ますが、他人から不正にデータを参照・改ざんされる危険性も増すため、十分なセキュリティを施す必要があります。

無線 LAN スポット

喫茶店・ホテルなどの店舗や駅・空港などの公共の場所で無線 LAN によるインターネット接続サービスを提供するものです。無線 LAN スポットにはレストランなどの店舗が顧客サービスの為に提供するものや公共エリアや屋外の利用等を前提とした商用サービス等いろいろな形態があります。

無線 LAN のセキュリティに関する注意事項 第1版

付-3.2 用語説明一覧

用語	説明
AES	Advanced Encryption Standard の略。米国政府内での情報処理用に採用された“次世代標準暗号化方式”のこと。規定の基準(暗号強度、処理速度等)を満足しており、その仕様も公開されていることから、広い分野での利用が行われている。IEEE802.11i/WPA/WPA2 の暗号化方式の一つに採用されている。
ANY プロンプト応答禁止	SSID の問い合わせを拒否する設定。
ANY 接続拒否	SSID を「ANY」にセットした無線 LAN 端末もしくは SSID に任意の文字列を入れた端末からの接続を拒否する設定。
EAP	Extensible Authentication Protocol の略。任意の認証機能を用いるための仕様。ダイヤルアップで用いられる PPP (Point-to-Point Protocol)の拡張として開発された。ユーザ名・パスワード以外にもスマートカード(IC カード)やデジタル証明書などさまざまな認証方式をサポートできる。EAP-TLS、EAP-TTLS などがある。
EAP-TLS	TLS(Transport Layer Security)を用いた EAP 方式の認証プロトコル。利用にはクライアント証明書およびサーバ証明書が必要となる。
EAP-TTLS	TLS(Transport Layer Security)を用いた EAP 方式の認証プロトコル。EAP-TLS とは異なり、クライアント証明書は必要とせず、かわりにユーザ名・パスワードが用いられる。
IEEE802.11i	IEEE が標準化した”無線 LAN 用セキュリティ規格“認証方式や暗号化方式、暗号化キーの取り扱い等について規定している。
IEEE802.1X	無線 LAN 上で認証と動的なキーの生成および配送を行う仕組み。IEEE 標準。有線 LAN でポートアクセス管理を行うためにも用いられる。EAP および RADIUS を用いる。
MAC アドレスフィルタリング	無線 LAN 端末固有の MAC アドレスを無線 LAN アクセスポイントに設定する事で、無線 LAN 端末を無線 LAN アクセスポイントに接続するか否かを制御するセキュリティ方式。
PSK	Pre-Shared Key の略。 TKIP 暗号プロトコルにて、暗号化キーを生成するために用いられる共有(秘密)鍵のこと。この鍵を用いて直接暗号化を行うものではなく、暗号鍵を生成するためのものであることから“事前共有鍵”と呼ばれる。PSK とは、事前共有鍵を用いる認証方式を表す場合がある。
RADIUS	Remote Authentication Dial-in User Service の略。ネットワークアクセス全般に対する認証、アクセス承認、課金管理を行うプロトコル。
SSID	Service Set Identifier の略。 無線 LAN を構成する無線 LAN アクセスポイントと端末につけられた識別子のこと。無線 LAN をグループ化するために用いられる。無線 LAN アクセスポイントと端末で同じ SSID を設定されていないと

無線 LAN のセキュリティに関する注意事項 第1版

用語	説明																
	通信できない。無線 LAN アクセスポイントを中心とした 1 つのグループである BSS(Basic Service Set)が 802.11 による無線 LAN のインフラストラクチャ通信の最小単位となるが、複数の無線 LAN アクセスポイントにまたがった際のローミングを考慮し、BSS を複数束ねた ESS(Extended Service Set)が定義されている。このため、SSID は ESSID と呼ばれることもある。																
SSID の隠蔽	SSID を無線 LAN アクセスポイントにより定期的送信されるビーコン中に含まないように設定すること。																
TKIP	Temporal Key Integrity Protocol の略。暗号化方式の一種で、WPA の暗号化方式として採用されている。PSK と呼ばれる“事前共有鍵”を元に暗号化キーを一定のデータ量また時間毎に生成し、暗号化を行う。																
WEP キー	WEP 暗号方式で用いられる“暗号化キー”のこと。種類は共有(秘密)鍵である。																
WPA/WPA2	<p>① Wi-Fi Protected Access の略。 Wi-Fi Alliance が規格化したセキュリティ規格のこと。WEP 方式よりセキュリティ強度が強化されている。暗号化方式と認証プロトコルにより、以下の4つに分類できる。</p> <table border="0" style="margin-left: auto; margin-right: auto;"> <tr> <td></td> <td></td> <td colspan="2" style="text-align: center;">認証</td> </tr> <tr> <td></td> <td></td> <td style="text-align: center;">PSK</td> <td style="text-align: center;">EAP</td> </tr> <tr> <td style="text-align: right;">暗号</td> <td style="text-align: center;">TKIP</td> <td style="text-align: center;">(1)</td> <td style="text-align: center;">(2)</td> </tr> <tr> <td></td> <td style="text-align: center;">AES</td> <td style="text-align: center;">(3)</td> <td style="text-align: center;">(4)</td> </tr> </table> <p>② WPA/WPA2 にて認証に外部サーバを用いる方式を表す。上記表内の(2)または(4)の方式</p>			認証				PSK	EAP	暗号	TKIP	(1)	(2)		AES	(3)	(4)
		認証															
		PSK	EAP														
暗号	TKIP	(1)	(2)														
	AES	(3)	(4)														
WPA-PSK	WPA にて認証に外部サーバも用いない方式を表す。上記表内の(1)または(3)の方式																
アドホック通信	無線 LAN アクセスポイントを使わず、無線 LAN 端末同士で通信を行うモードの通信。																
暗号化キー	暗号化を行う鍵のことで、暗号化方式により、公開鍵と 共有(秘密)鍵の 2 種類ある。																
インフラストラクチャ通信	無線 LAN 端末と無線 LAN アクセスポイントを利用した形態の通信。																
オープンシステム認証	無線 LAN の認証方式の 1 つ。無線 LAN 端末からは資格情報無しに無線 LAN アクセスポイントに認証依頼を行い、無線 LAN アクセスポイントは依頼された認証をそのまま受け入れる。そのため、基本的には認証は行われていない。																
キーインデックス	WEP 暗号方式では、仕様上 4 つの WEP キーを切り替えることができる。WEP 暗号方式では、無線 LAN アクセスポイントと無線 LAN 端末の両方のキーインデックスを同じにしなければいけない。製品によってはキーインデックスの値が“0~3”のもと“1~4”のものがあり、設定に注意しなければならない。																

無線 LAN のセキュリティに関する注意事項 第1版

用語	説明
キー更新間隔	暗号化方式 TKIP にて、暗号化キーを生成するデータ量間隔または時間間隔のこと。
共有キー認証	無線 LAN の認証方式の 1 つ。無線 LAN アクセスポイントと端末はネットワークキーを用いたチャンレジレスポンス認証を行う。
ネットワークキー	共有キー認証の「認証キー」、および暗号化機能の「暗号化キー」または「PSK」の両方に用いられる「キー」のこと。
無線 LAN アクセスポイント	ネットワークに無線 LAN 端末を接続する機器であり、一般的には有線 LAN の HUB に相当する機能を持つ。

無線 LAN のセキュリティに関する注意事項作成メンバー会社

パーソナルコンピュータ事業委員会
ホームデジタル専門委員会
無線 LAN 関連ガイドライン見直し WG

(五十音順)

エプソンダイレクト(株)

NECアクセステクニカ(株)

シャープ(株)

ソニー(株)

(株)東芝

日本電気(株)

パナソニック(株)

富士通(株)

計 8 社