



AN AIRMAGNET TECHNICAL WHITE PAPER

## 802.11 における 7 つのセキュリティ問題

株式会社東陽テクニカ  
IT ビジネス営業部 ワイヤレス LAN ソリューション  
TEL : 03-3245-1250  
E-Mail : [wlan@toyo.co.jp](mailto:wlan@toyo.co.jp)  
URL : <http://www.toyo.co.jp/wlan/>



## AirMagnet 無線 LAN アナライザ

# 7つのセキュリティ問題: セキュリティの脆弱性に対処するために 無線 LAN アナライザを用いる

著者 : Matthew Gast  
2002 年 8 月

2002 年 5 月 O'Reilly Network に私は 802.11 無線における “7つのセキュリティ問題”<sup>1</sup> という記事を掲載しました。その記事は無線 LAN においてネットワーク技術者がどう安全な無線ネットワークを構築するかという点で考えられる最重要な 7つの無線 LAN セキュリティ問題点について議論したものです。その記事について私が受けた数々の質問はネットワーク管理者が使いこなせるツールについてです。どのようなインターフェイスのネットワークと同様に、無線ネットワークにおいて、アナライザは管理者が最初に購入すべき物の 1つです。従来のプロトコル解析・診断機能に加えて、無線ネットワークアナライザは無線ネットワークに潜むセキュリティに関する情報を収集することができます。この記事は “7つのセキュリティ問題” からそれぞれを再考察し、そして無線 LAN のセキュリティを守るために、なぜどのように無線 LAN アナライザが必要なのか述べるものです。

### 問題 1 : 容易なアクセス

無線 LAN を見つけ出すことは容易です。クライアントが無線 LAN を見つけ出すためにネットワークはネットワークパラメータを含む Beacon フレームを送らなければなりません。もちろんその情報は、ネットワークに接続するために必要な情報であり、またネットワークに攻撃を開始するために必要な情報でもあります。Beacon フレームはなにも機密的な機能によって処理されてなく、そのことは無線 LAN カードを持つ誰もが 802.11 ネットワークを利用できることを意味します。高感度アンテナを持つ攻撃者は、近くの路上やビル等から物理的な接触無しにあなたのネットワークに攻撃し始めるでしょう。

<sup>1</sup> 本記事の英文のコピーは次の URL に掲載されています。  
<http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html>



## AirMagnet 無線 LAN アナライザ

### ソリューション1：アクセス制御を強化する

容易にアクセスできることは、必ずしも攻撃されやすいということではありません。無線ネットワークは接続性を考慮した設計となっていますが、もしセキュリティポリシーとして必要ならば接続制限を設けることもできます。極端な方法として無線ネットワークは電磁シールドルームに制限し、外部に感知できるようなRF信号漏れを無くすことができます。しかしほとんどの場合にそこまでの必要性はありません。しっかりとアクセス制御を行うことで、無線ネットワーク運用のリスクを軽減することができます。

無線ネットワークでのセキュリティ管理は、ある程度設計の問題に関係します。ネットワークにおいてアクセスポイントは、ファイアウォール等のセキュリティ管理デバイスの外側に置くべきであり、管理者は企業ネットワークにおいてVPNアクセスを行うようにすべきです。しっかりとユーザ認証を行うべきで、IEEE802.1x規格をもとにした新しい製品などが推奨されます。802.1xは、新たなフレームタイプを使ったユーザベースの認証を定義し、RADIUS等の企業ユーザデータベースと連携付ける手段となります。フロントエンド（無線）側での802.1xを使った認証交換は、バックエンド（有線）側でのRADIUS要求に変換されます。有線側ではアナライザを用いて、認証過程に対する分析をRADIUSの要求・応答を見ることにより判断できます。しかし、フロントエンド（無線）側で同様なレベルの分析のできる製品がほとんどありません。AirMagnetのエキスパート分析機能は、802.11認証を含む、無線LAN解析のための独自解析機能です。認証トラフィックモニタや、ネットワーク管理者に役立つ解析診断機能（骨の折れるようなパケット解析は必要としない）をご提供します。中央のスクリーンから802.1x認証メッセージ及びキー配布メッセージを追跡するエキスパート解析システムは、Interop Labの無線LANセキュリティプロジェクト<sup>2</sup>などの様な802.1xを使った無線LAN配備において、非常に有益であることが証明されています。

どんなに完全な設計であっても、現時点の構成が設計のセキュリティ目的と一致しているかどうか定期的な検査をしなければなりません。AirMagnetのエキスパート分析機能は、フレームについて詳細な解析をおこない、802.11に共通する色々なセキュリティ問題を見つけだすことができます。昨年は、多数のWEPアタックが報告されましたが、ベンダのパッチによりWEPの良く知られた弱点に

<sup>2</sup> Interop Labの無線LANセキュリティプロジェクトの詳細については次のURLを参照ください。  
[http://www.ilabs.interop.net/details?topic=WLAN\\_Sec](http://www.ilabs.interop.net/details?topic=WLAN_Sec)



## AirMagnet 無線 LAN アナライザ

対処することが可能です。AirMagnet のエキスパート解析では、予想できる IV (Initial Vector) パターンを使った IV の再利用、AirSnort のような WEP 解読プログラムなどを使うことを可能とするような、弱い WEP の実装を管理者に警報することができます。実装上の弱点の確認により、管理者はネットワークセキュリティを維持するための適切なファームウェアアップグレードを適用することができます。

不適切な設定は、セキュリティの弱点の主要原因となるかもしれません。特に、もしセキュリティ技術者が監督すること無しに無線 LAN が構築された場合などです。AirMagnet のエキスパート機能は、製造時のデフォルト設定の状態で作られているアクセスポイントを検出することができます。これにより管理者はなにもセキュリティ機能が設定されていないアクセスポイントを探知することができます。セキュリティ検査のために、AirMagnet1.5 では VPN や 802.1x のような強固なセキュリティを使っていないデバイスを見つけ、アラームとして記録します。

### 問題 2 : “不正な” アクセスポイント

アクセスが容易な無線 LAN は、配備が容易です。これら 2 つの性質はネットワーク管理者やセキュリティ管理者にとって頭痛のたねです。誰でも近所のコンピュータショップに行き、アクセスポイントを買い、許可無く企業ネットワークに接続する可能性があります。現在であれば、多くのアクセスポイントは課長決済などの価格帯で手軽にアクセスポイントを手に入れることができます。そして各部門において IT 統括部門の許可無しに独自の無線 LAN を構築してしまう場合があります。エンドユーザによって配置された、いわゆる “不正な” アクセスポイントは、重大なセキュリティリスクを引きおこします。エンドユーザがセキュリティに詳しくなく、無線 LAN により引きおこされるリスクに気づかないかもしれません。“war drivers”により記録され場所を報告された多くの無線 LAN の配置は、セキュリティ機能が有効になっておらず、重要な機能がデフォルト設定のままでした。

### ソリューション 2 : 定期的なサイト調査

他のネットワーク技術と同様に、無線ネットワークにおいてもセキュリティ管理者は警戒する必要があります。ネットワークアクセスの為にこれらの様々な技術



## AirMagnet 無線 LAN アナライザ

が簡単に利用できると、不正にネットワークが設置された際に学習が非常に重要な仕事となります。

無許可のネットワークを見つける明確な方法は、攻撃者と同じことをする、すなわちアンテナを使ってそれらを捜索し、攻撃者につけ込まれるより早く無許可ネットワークを発見することです。このようなサイト検査は、出来るだけ頻繁に行うべきです。トレードオフとして、より頻繁な検査をすれば、より無許可ネットワークをキャッチできますが、従業員の高い時間コストのため歩き回っての検出は電波感度の良い環境を除いてはどうにもなりません。一つの妥協案としては小型でハンドヘルドなツールを選択すること（例えば Compaq iPAQ のような）、そしてヘルプデスク技術者はハンドヘルドスキャナーを用いてユーザサポートの電話に応えながらキャンパスの中から無許可のネットワークを検出することです。

周回による検査は、NetStumbler によってよく行われます。NetStumbler は、大量のアクセスポイントを見つけ、それらを地図アプリケーション上で物理的位置と関連付けする便利なツールですが、それは専門ネットワーク管理者のため限定のツールです。NetStumbler の現行バージョンは、アクセスポイントを見つけ出すためにアクティブなプロービングに頼ります、しかし多くのアクセスポイントは、そのような要求を無視する設定をすることができます。AirMagnet は空中の AP による伝送の発見にパッシブ分析を行っており、アンテナの範囲内のすべてのアクセスポイントを発見することが可能です。

ネットワーク管理者はいつも時間に追われており、許可されたアクセスポイントを無視して“不正な”アクセスポイントを見つける便利な方法が必要です。AirMagnet のエキスパートエンジンにより、管理者が管理（許可）アクセスポイントリストを登録設定することが可能です。なにか無許可のアクセスポイントがあればアラームをあげ、アラームへの対応としてネットワーク管理者は AirMagnet の検出ツールを使い、リアルタイム電波（シグナル・ノイズ）強度メータに基づいて、そのアクセスポイントやステーションにたどり着くことができます。検索ツールは非常に正確とまではいきませんが、探索エリアを一つまたはいくつかのキュービクルまで絞り込むには十分です。

### 問題 3：許可されていないサービスの使用

数人の“war drivers”が、大半のアクセスポイントは、デフォルト設定を若干変更しただけで運用されているとした結果を公表しています。デフォルト設定で運



## AirMagnet 無線 LAN アナライザ

用されているアクセスポイントのほとんど全ては WEP が使われていないか、あるいはベンダ毎の出荷時のデフォルトキーが設定されています。WEP 無しでは、いつでもネットワークアクセスされてしまう状況にあります。二つの問題がそのようなオープンアクセスに起因すると言えます。無許可使用のための帯域負担に加えて、法的問題も生じるかもしれません。無許可ユーザは、サービスプロバイダーのサービス規約に従う必要はないかもしれませんが、結果として不正使用者は ISP から接続されてしまうくらいでしょう。

### ソリューション 3 : 強固な認証の為の設計と検査

無許可ユーザに対する明白な防御は、ネットワークにアクセスさせないことです。アクセス権限はユーザ確認によるため、強固な暗号化によって保護された認証が前提条件となります。無線リンク上に転送されるトラフィックを保護するために導入される VPN ソリューションは、強固な認証を提供します。802.1x が十分な技術対策であるとしてリスク評価を行っている企業は、さらに暗号化による安全な認証方法、例えば Transport Layer Security ( TLS ) や Protected EAP ( PEAP ) または Tunneled TLS ( TTLS ) などが選択されているかどうかを確認すべきです。802.1x のモニタリングの部分として、AirMagnet はユーザ名と EAP タイプのような重要な 802.1x 特性を検出することができます。

一旦ネットワークが稼動しだすと、認証と許可方針が順守されていることを確認することが不可欠です。不正アクセスポイント問題では、解決策は配備された無線ネットワーク機器の定期的な調査を実行し、強固な認証が使用されているか、そしてネットワーク機器が正しく構成されているかを確認することです。もし無許可ステーションのネットワーク接続が発見されたならば、AirMagnet ハンドヘルドを、その物理的な位置をつきとめるために使用することができます。

### 問題 4 : サービスとパフォーマンスの制約

無線 LAN は伝送量に限界があります。802.11b においては 11Mbps、802.11a においては 54Mbps となります。MAC レイヤーのオーバーヘッドにより、純粋なデータスループットは規定の約半分となってしまう、キャパシティはアクセスポイントにアソシエイトする全てのユーザで共有しなければなりません。ローカルエリアアプリケーションが、そのような限られたキャパシティを圧倒したらどうなる



## AirMagnet 無線 LAN アナライザ

か、あるいは攻撃者が限られた帯域に DOS 攻撃を始めたらどうなるか想像することは難しくありません。

無線キャパシティは、いくつかの方法で溢れさせることができます。たとえば、有線ネットワーク側から無線チャンネルが処理できる以上の率のトラフィックを流すことで溢れを起こさせることができます。もし攻撃者が Fast Ethernet セグメントから ping flood を始めると、簡単にアクセスポイントのキャパシティを溢れさせることができます。ブロードキャストアドレスを使うことにより、いくつかの直接接続されたアクセスポイントを溢れさせることが可能です。攻撃者は、トラフィックを、無線アクセスポイントを取り付けることなしに無線ネットワークに注入することができます。802.11MAC は、多数のネットワークが同じ場所と無線チャンネルを共有できるように設計されています。無線ネットワークを持ち出したいと願う攻撃者は、同じ無線チャンネル上に自身のトラフィックを送ることができ、そして標的ネットワークは標準の CSMA/CA メカニズムにより、できる限り新たなトラフィックを収容しようとしします。

大きなトラフィック負荷は悪意的でなくとも発生する、と多くのネットワーク技術者がとなえることでしょう。大きなファイルの転送、あるいは複雑なクライアント/サーバシステムは、ユーザの作業を補助するためにネットワーク上に大量データを転送します。もし十分なユーザが、同じアクセスポイント経由でデータを引っ張り出したならば、ネットワークアクセスは、高速ブロードバンドサービスの提供者によって使用される、不十分なダイヤルアップアクセスと同じような振る舞いを始めます。

### ソリューション4：ネットワークのモニタ

パフォーマンス問題を扱うことは、それらのモニタリングと検出から始まります。多くのアクセスポイントは、SNMP 経由で統計情報を報告するでしょう。しかし、それらはエンドユーザが感じるパフォーマンス不満を解決できるような詳細なレベルではありません。無線ネットワークアナライザは、現在地における信号品質とネットワーク診断を報告することができます。AirMagnet アナライザは、受信したトラフィックを伝送速度あるいはフレームタイプに分けて分析することができます。大量の低速伝送が起こる原因は外部電波干渉、厳しいマルチパスフェージング、単純に端末側のアクセスポイントまでの距離が遠すぎるということが考えられます。チャンネルごとの瞬時の伝送速度を表示することにより、チャンネル上の使用可能な容量を視覚的な描写であらわし、容易にチャンネルが混雑しているかどうか



## AirMagnet 無線 LAN アナライザ

見ることができます。アクセスポイントへの過度のトラフィックは、アクセスポイントのカバー範囲をより小さく分割すること、あるいはバックボーンと無線ネットワークの合流点でトラフィックシェーピングソリューションを用いることで処理することができます。AirMagnet のエキスパート解析エンジンはまた、アクセスポイントに対してアタックを始める悪意のあるクライアントを特定することができます。

### 問題 5 : MAC なりすましとセッション乗っ取り

802.11 ネットワークは、フレームの認証を行いません。どんなフレームも送信元アドレスを持つが、空中にあるフレームが、実際にそのステーションが送ったフレームである保障がありません。従来の Ethernet ネットワーク上と同様に、フレーム送信元アドレスの偽造に対する保護がありません。攻撃者は“なりすまし”フレームを使ってトラフィック変え、ARP テーブルを間違っただけのものに書き換えることができます。ずっと簡単なレベルでは、攻撃者はネットワークで使われている MAC アドレスを見て、これらのアドレスを悪意のある送信に使用します。この種の攻撃を防止するために、802.11 ネットワークのユーザ認証方法が開発されました。ユーザの認証を行うことにより、無許可ユーザをネットワークにアクセスさせないことができます。ユーザ認証の基準は、802.1x 規格として 2001 年 6 月に批准されました。802.1x は、ネットワークにアクセスする前にユーザ認証が必要とすることができますが、無線ネットワークに必要とされる鍵管理機能のすべてを供給するための追加的な機能が必要です。その追加的な機能は 802.11i として最終批准にむけ目下調整されています。

攻撃者は、アクティブなアタックにもなりすましフレームを使うことができます。セッションの乗っ取りの他に、攻撃者はアクセスポイントの認証の欠如を利用することができます。アクセスポイントは Beacon フレームのブロードキャストにより認識されます。アクセスポイントであることを主張し、正しい SSID (Service Set Identifier : ネットワークネームともいう) を送るどんなステーションも、許可されたネットワークの一部として見えるでしょう。しかしながら攻撃者は、802.11 においてアクセスポイントが本当にアクセスポイントであると証明するものが無いので、簡単にアクセスポイントのふりをすることができます。その点において、攻撃者はクライアントの証明書を盗み、MITM (Man In The Middle) アタックを通じてそれらを使いネットワークにアクセスします。幸運にも、相互認証をサポートするプロトコルが 802.1x において存在します。TLS (Transport Layer Security) に基づいた方法を使えば、クライアントが認証証明



## AirMagnet 無線 LAN アナライザ

書をだす前にアクセスポイントがそれらの身分を証明する必要があるでしょう。そして証明書は、無線環境において強固な暗号化により保護されます。セッションの乗っ取りは、802.11MAC が 802.11i の一部であるフレーム毎の認証に対応するまで完全には解決されないでしょう。

### ソリューション 5：強固なプロトコルの採用とそれらの使用

802.11i の批准まで、MAC なりすましは脅威でしょう。ネットワーク技術者は、より攻撃されやすいコアなネットワークから無線ネットワークを切り離すことにより MAC なりすましによる被害を食い止めるよう集力しなければなりません。AirMagnet は、なりすましアクセスポイントを検出でき、さらなる調査をするように管理者に警告するアラームをあげることができる様、デフォルトで構成されています。同時にセッションの乗っ取りは、IPSec のような強固な暗号化プロトコルを使うことによつてのみ防ぐことができます。キャプチャフレーム分析の一部として、AirMagnet アナライザは、どのセキュリティレベルが使われているのか、希望通りのセキュリティプロトコルが使われているのかどうかをネットワーク管理者が一目で判断することを可能とします。

強固な VPN プロトコルを使うことに加えて、802.1x におけるユーザ認証を使う必要があるかもしれません。試験的な段階では、AirMagnet の 802.1x 認証ステータス詳細解析は 802.1x 認証交換の無線コンポーネントでの重要な確認を可能にします。設置後に行う現場検査の場合、AirMagnet アナライザは認証タイプをデコードし、強固な暗号法によりパスワードが守られていることをネットワーク管理者が確認することができます。

### 問題 6：トラフィック解析と盗聴

802.11 は、パッシブなトラフィック観察をおこなう攻撃者に対しては防御できません。主要なリスクは、802.11 には盗聴に対して安全にデータ伝送する方法がないことです。フレームヘッダは、無線ネットワークアナライザで常にはっきりと、そして誰でも目で見ることができます。盗聴に対するセキュリティは厳しい非難をあげた WEP 仕様によって提供されるはずでした。WEP の弱点についてかなりの量の文献が書かれています。それはネットワークアソシエーションの最初とユーザデータフレームのみを保護します。管理・制御フレームは WEP によって暗号化あるいは認証されず、攻撃者に広い範囲でなりすましフレームによる伝送の



## AirMagnet 無線 LAN アナライザ

混乱を許してしまいます。初期の WEP の実装は、AirSnort や WEPcrack などのツールで攻撃されやすいものでした。しかしほとんどのベンダの最新のファームウェアリリースでは、知られているアタックのすべてが除去されています。さらなる予防策として、最新製品はもう一歩進み、WEP キーを 15 分毎に変更する鍵管理プロトコルを使っています。非常に混み合った無線 LAN でさえ、既知の攻撃を行うために、15 分で鍵を解読するのに十分なデータは発生しません。

### ソリューション 6 : リスク解析の実行

盗聴の恐れを扱う場合、キーとなる決断は、WEP のみを使うことの脅威と、より実証されたソリューションを配備する複雑さを対照することです。現在のファームウェアでは知られた弱点のすべてを処理するにもかかわらず、同じことが 2001 年 8 月の深刻な解読以前にも述べられていました。

もし WEP を使うことを選択したならば、AirSnort アタックを受けやすすくないかを確認めるために、無線ネットワークを検査すべきです。AirMagnet 解析エンジンは、自動的に受信したトラフィック全てを分析し WEP 保護フレームにおいて知られた弱点を調査します。AirMagnet アナライザは、WEP が無効なアクセスポイントとステーション状況を通知するので、ネットワーク管理者がより詳しい調査を行うことが可能です。

もし無線 LAN で機密データを使っているならば、WEP は要求に対してかなり不足しているかもしれません。SSH, SSL, IPSec のような強固な暗号化ソリューションは、公共のチャンネル上に安全にデータを送信する様設計され、そして長年にわたりアタックに抵抗する手段として実証されており、間違いなくハイレベルなセキュリティを提供するでしょう。AirMagnet のアクセスポイント表示はアクセスポイントの間で WEP, 802.1x, VPN 技術のどれが使われているのか識別し、ネットワーク管理者が、ポリシーに従った強力な暗号化が行われているかを確認することができます。

### 問題 7 : より高いレベルの攻撃

一旦攻撃者が無線ネットワークへのアクセスを得ると、そこには他のシステムへのアタックの始点として働きます。多くのネットワークは慎重に構成され、詳細



## AirMagnet 無線 LAN アナライザ

にモニタを行う境界セキュリティ装置から成る硬い外殻を持っています。けれども殻の内側は弱く、攻撃の標的とされやすくなります。バックボーンに直接接続すれば無線 LAN はすぐに配置することができます。しかしネットワークを攻撃にさらすことになってしまいます。セキュリティの境界の場所次第で、他のネットワークを攻撃にさらすことになるかもしれず、あなたのネットワークが安息な世界を攻撃するための踏み台として使われて、あなたが不評となりかねない賭けをすることになります。

### ソリューション7: コアネットワークを無線 LAN から守る

無線 LAN のアタックに対する弱さは当然であるとして、信頼できないネットワークとして扱われるべきものです。多くの企業は、ゲストのためのアクセスポートをトレーニングルームやラボなどで提供しています。無線 LAN は概念的にゲストのためのアクセスポートと同等に扱うべきです。それは信頼できないユーザによるアクセスが高く見込まれる為です。無線 LAN をセキュリティ境界の外側に置き、無線 LAN とコアネットワークの間で Firewall のようなアクセス制御技術を使い、そして実証済みの VPN ソリューションを通じてコアネットワークへのアクセスを提供しましょう。

### 結論

このセキュリティ問題の話で終始共通したテーマは、認識された多くの欠点に対処するための技術的メカニズムは存在し、よく知られていますが、それらは保護を提供するために使用されなければなりません。合理的な警戒を行うことで、機動性と柔軟性による利益を上げたいと考える全ての企業にとって、無線ネットワークを安全にすることができます。多くの他のネットワーク技術と同様に、重要なことは、セキュリティを考えたネットワークを設計し、設計が配備のための実際上の基準として合致しているかを確認するために、定期的な検査を行うことです。トラブルシューティング分析から定期的な検査まで、無線ネットワークアナライザは無線ネットワーク技術者にとって必要不可欠なツールになります。



## AirMagnet 無線 LAN アナライザ

---

### **著者について**

Matthew Gast は 802.11 の著者である。 : The Definitive Guide は O'Reilly and Associates より 2002 年 4 月に出版されています。

### **AirMagnet 社について**

AirMagnet 社 2001 年設立。無線ネットワーク管理のための新世代の統合ソリューションをもって、ネットワーク及びセキュリティ技術者が無線ネットワークを配備し管理する際に対応する独自の挑戦に取り組んでいます。

VenGlobal キャピタルファンド及び個人投資家が投資しています。

Text copyright © 2002 Matthew Gast. All rights reserved. Used with permission. Portions © 2002 AirMagnet, Inc. All rights reserved. AirMagnet, AirWise and the AirMagnet logos are trademarks of AirMagnet, Inc. All other product names mentioned herein may be trademarks of their respective companies.