無線LANのセキュリティ管理手法

鴨志田昭輝

CONTENTS

要約

1 無線LAN（ローカルエリア・ネットワーク）のセキュリティが注目されている。無線LANはその性質上セキュリティリスクが高く、高度なセキュリティ対策が必要である。そのために多くのセキュリティ規格が策定され、多くの製品が各ベンダーから提供されている。しかし、技術的な対策には限界があるため、管理的な対策も必要である。

2 無線LANにおいても、セキュリティ管理を考えるうえではPDCAサイクルが基本となる。必要なセキュリティ対策を実施・運用する（Do）ことに目がいきがちであるが、それ以前にきちんと計画を策定し（Plan）、定期的に評価・監査を行い（Check）、問題点があれば是正措置を実施する（Act）ことが肝要である。

3 無線LANのセキュリティには特有の問題がある。なかでも特に、無線LANを設置する場所によりセキュリティリスクが変わってくることや、脆弱な無線LAN機器が企業内ネットワークに接続されることを防がなければならないことには注意が必要である。このため、無線LAN機器が発する電波の状態の調査（サイトサーベイ）を実施することが望まれる。

Ⅰ　無線LANのセキュリティの現状

1　無線LANの急速な普及

個人、企業を問わず、パソコンのネットワーク接続のために無線LAN（ローカルエリア・ネットワーク）が急速に普及している。

無線LANは、ケーブルを引き回す必要がないため、単純に便利というだけでなく、設置やレイアウト変更にかかる手間や経費をも節減できる。また、会議室や応接室でも自由にネットワーク接続ができ、それが生産性の向上にもつながる。特に、ノートパソコンの場合、こうしたメリットは大きい。

こうしたメリットだけでなく、無線LAN機器の価格の大幅な低下、無線周波数の利用に関する規制の緩和、規格化による互換性の確保などが、普及に弾みをつけている。

2　脆弱なセキュリティ

無線LANが従来利用されてきた有線LANと最も違う点は、電波を利用して通信することである。これは、そのままセキュリティ上のリスクに結びつく。なぜなら、無線LAN機器から発生する電波は、窓や壁から企業外に漏洩してしまうので、この電波を部外者が拾うことができれば、情報漏洩や不正アクセスの原因となりやすいからである。

3　セキュリティ対策

潜在的なリスクがある無線LANを安全に使うために、通信を暗号化するWEP（Wired Equivalent Privacy）という名称のセキュリティ規格が標準的に利用されている。しかし、この規格に致命的な問題が発見されており、暗号化したデータであっても解読することが可能である。WEPによる暗号通信を解読するためのソフトウェアも広く出回っており、ある程度の知識があれば、暗号化した通信を傍受・解読するのはそれほど難しくない。

このため、新しいセキュリティ規格が次々と策定され、各メーカーは競って新製品を投入してきている。それに伴って、多くの雑誌で特集が組まれるようになり、無線LANのセキュリティが大きな話題となっている。

4　普及しないセキュリティ対策

無線LANのセキュリティが大きな話題となっているのは、近年の無線LANの急速な普及に比べ、そのセキュリティ対策の普及が遅れていることが原因である。これはまるで、インターネットブームが到来し、その普及が一段落したあたりで、インターネットのセキュリティが大きな注目を集めるようになった経緯とよく似ている。

最新の技術を導入し、それを企業内すべての無線LANに正しく適用するには、大変な労力が必要である。しかし現実には、こうしたコストや労力の問題よりも、むしろセキュリティに関する情報や認識が不足しているため、十分なセキュリティ対策を行わずに無線LANを利用している企業が多いようである。なかには、セキュリティ対策を一切せずに無線LANを利用している企業も存在する。

5　報告された問題事例

こうした無線LANのセキュリティへの関心の高まりに伴って、問題のある事例も報道されるようになってきている。

最近、大手百貨店のPOS（販売時点情報

管理）システムで利用している無線LANが、通信を一切暗号化していなかった事実が外部の専門家の指摘により発覚し、大きく報道された。この事例では、顧客が買い物のために利用したクレジットカード番号も暗号化せずに無線LANで送信していたという。その他にも、官公庁で利用していた無線LANシステムが、外部から利用できるような状態であったことも報じられている。

それ以外にも、無線LAN機器（無線LANカード）を搭載したノートパソコンを携帯して市街地を移動し、拾うことのできる無線LANの電波を調査することも行われている。このような行為はウォードライビング（War Driving）と呼ばれており、その成果がウェブ上で公開されていることもある。それを見ると、多くの無線LANでセキュリティ対策が行われていないことがよくわかる。

また、都内で実施されたある調査によると、半数近くの無線LAN機器がWEPによるセキュリティ対策を施されていなかったという。

II　無線LANの利用における脅威

無線LANの利用における代表的な脅威として、以下の５点があげられる（図１）。

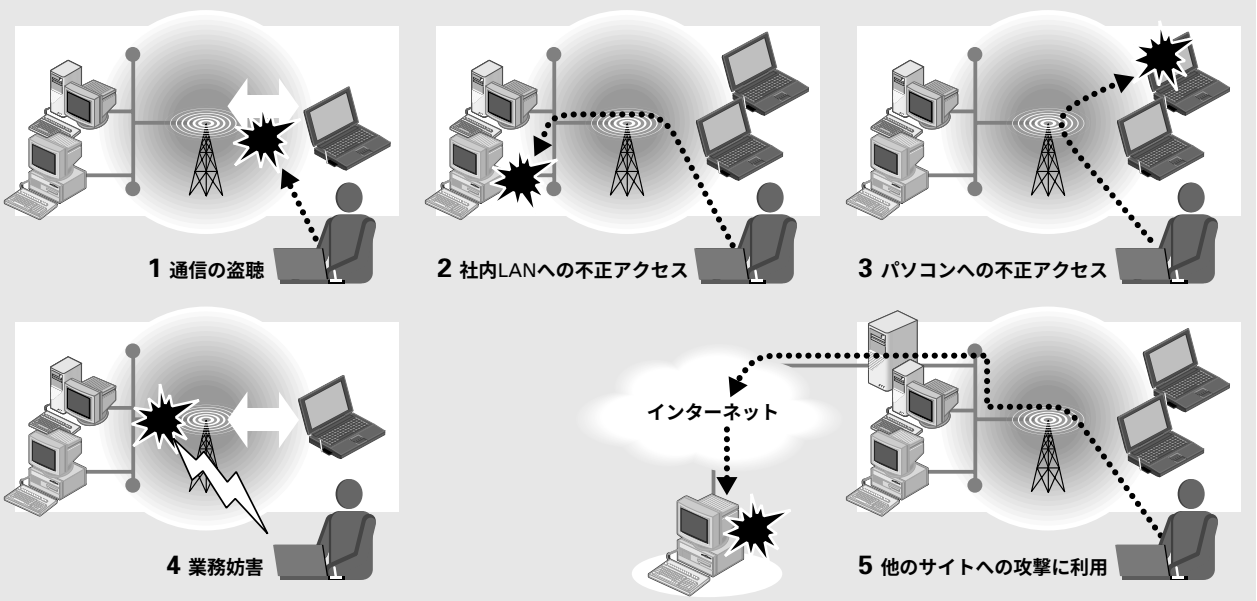
1　通信の盗聴

ネットワーク通信に利用している電波を部外者に拾われ、通信の内容を盗聴されるリスクが存在する。特に、建物の外で電波を拾うことができるようなケースでは、企業側が盗聴されている事実に気づきにくいため、事件が発覚しにくい。

2　企業内LANへの不正アクセス

企業内LANに接続されている無線LAN機器（アクセスポイント）を経由して、企業内LAN上にあるサーバーなどに不正にアクセスされるリスクも存在する。インターネットからの不正アクセスは、ファイアウォールなどのセキュリティ対策により防がれてしまう場合が多いが、企業内LANに接続された無

図1　無線LANのセキュリティリスク



出所）LAN：ローカルエリア･ネットワーク

線LAN機器からの不正アクセスについては、対策が十分でないことも多いようである。

3　パソコンへの不正アクセス

無線LAN機器（無線LANカード）が搭載されたパソコンに不正にアクセスされるリスクも存在する。最近のノートパソコンには無線LAN機能が内蔵されているものも少なくないが、工場出荷時の設定のままでは、外部からの不正アクセスに対して非常に弱い製品がほとんどである。しかも、各社員が利用しているパソコンは、企業内の管理者が管理しているサーバーに比べると、セキュリティが十分でないことも多く、こうした不正アクセスを受ける可能性が高いため危険である。

4　業務妨害

無線LANが利用する周波帯の電波が発信され、無線LANの利用を妨害されるリスクも存在する。専用の妨害電波発生装置がなくても、安価な無線LAN機器（アクセスポイント）を置いておくだけで、無線LANの性能（通信速度）を低下させることができる。

5　他のサイトへの攻撃に利用

企業内LANに不正にアクセスされた後、企業内LAN経由でインターネットに接続されることにより、他のサイトへの攻撃に利用されるリスクも存在する。最終的に被害を受けたサイトからは、企業内LANから攻撃が行われたように見えるため、攻撃に利用された企業が損害賠償を請求される恐れがある。このようなケースでは、真の攻撃者を特定することが困難である。

このように、いわば踏み台として利用するために、企業内の無線LANを狙うケースも今後増えてくると思われる。このような踏み台として利用可能な無線LANは、前述のウォードライビングなどによって発見され、その結果がウェブサイトで公開されていることもある。それほど重要な情報を扱っていないため、不正アクセスを受けたところで被害は少ないと思っていても、踏み台として利用されると、損害の賠償や社会的信用の失墜など、大きな被害を受けてしまうこともあるので、セキュリティ対策を怠ってはならない。

III　無線LANで利用されているセキュリティ技術

1　暗号化

無線LANのセキュリティを考えるうえで非常に重要なのは、電波を利用して通信するデータを暗号化することである。無線LANで利用している電波を、特定のエリアだけに押し込めることは困難であり、コストもかかる。このため、電波を利用する通信をすべて暗号化することによって、データの盗聴を防ぐのが現実的な対策だといえる。

現在、標準的に利用されている暗号化方式は前述のWEPである。だが、この方式には致命的な欠点があるため、この欠点を修正したTKIP（Temporal Key Integrity Protocol）などの方式も利用されるようになっている。

2　認証

認証も、無線LANのセキュリティを考えるうえで重要な技術である。これは、無線LANに接続できるユーザーを特定するための技術であり、無線LANに限らず、以前か

らセキュリティ対策として広く採用されてきた。IDとパスワードの組によって認証を行う場合が依然として多いようである。

現在、標準的に利用されている認証方式は、WEPキーや、無線LANカードのMACアドレス（各ネットワーク機器に固有のID番号）を利用した方式である。これらの方式は認証方式としては不十分なものであるため、より高度なセキュリティ機能を有するIEEE802.1x規格に準拠した認証方式が利用されるようになってきている。

3　技術的対策の限界

前述のような最新の暗号化・認証技術を導入すれば、安全に無線LANを利用することができるのは確かである。ただし、それは、こうした技術が適切に導入され、間違いなく運用されることが前提である。

例えば、いくら高度なセキュリティ機能を備えた無線LAN機器を導入したとしても、それらの機器が適切に設定されていなければ、通信が全く暗号化されていなかったという事態にもなりかねない。また、無線LANの導入を外部のベンダーに任せっきりにしたら、導入後はベンダーが全く面倒を見てくれなかったというケースもあるという。

さらに、たとえ導入時にセキュリティがしっかり設定されていたとしても、いつまでも安全に利用できるとは限らない。以下のようなケースは比較的起こりやすいので、注意が必要である。

- 日々進歩するセキュリティ侵害の技術に対抗できなくなる。
- 構成変更やネットワーク増強の際に、設定が変更される。
- 社員用にユーザーアカウントを作成したが、異動・退職時に削除されない。
- 利便性を向上するために、社員がセキュリティ機能をオフにしてしまう。

その他のリスクとしては、利便性を高めるため、社員が無線LAN機器（アクセスポイント）を勝手に企業内ネットワークに接続してしまうことがあげられる。このような無線LAN機器に十分なセキュリティ対策が施されていないと、情報漏洩や不正アクセスの原因になりうるので、特に注意が必要である。

このように、いくらセキュリティ技術が進歩したところで、それを利用する企業側のセキュリティ管理がしっかりしていなければ、依然として無線LANは危険なままである。

Ⅳ　PDCAサイクルによるセキュリティ管理

1　セキュリティ管理の必要性

無線LANの場合に限らず、企業がセキュリティ対策に取り組む際には、対策の漏れを減らすだけでなく、これが一過性のものに終わることがないようにしなければならない。これは、新しいセキュリティ侵害手法が開発されたり、業務内容の変化により扱う情報資産が変化したりするといった種々の要因によって状況が変化しても、企業が保有するリスクレベルを一定以下に抑えるよう、必要なセキュリティ対策をつねに見直す活動を継続的に実施するということである。

このためには、個別の脅威に対抗するセキュリティ対策を実施するだけでなく、これを継続・維持するためのセキュリティ管理が必要となる。

2　PDCAサイクルの確立

セキュリティ管理を実施するに当たっては、PDCAサイクルを確立することが非常に重要である。PDCAサイクルは、Plan（計画策定）、Do（実施・運用）、Check（評価・監査）、Act（改善・是正）の４つのステップから構成されるモデルであり、セキュリティ技術を導入するだけでなく、それを適切に運用し、問題点が発見されたらそれを是正して、よりセキュリティを強固にしていくことを目的としている（表１）。

①Plan（計画策定）

ポリシーやルールの策定などを実施する。電波の漏洩範囲を特定し、その結果に基づいてリスク分析を行うことも重要である。

②Do（実施・運用）

必要なセキュリティ技術を導入する。多くのセキュリティ関連の雑誌や書籍では、もっぱらこのステップが重視されている。これは、ベンダーやシステムインテグレーターの利益に直接結びつくといった商業的な側面があり、また多くのエンジニアにとって興味深いテーマであるからだと思われる。だからといって、その他のプロセスをおろそかにしてよいというわけではない。

③Check（評価・監査）

このステップでは、現在のセキュリティの見直しを行う。システム監査やセキュリティアセスメントといった監査・評価が定期的に行われるのが望ましい。

④Act（改善・是正）

評価・監査で問題点が発見されたり、セキュリティ侵害の事件が発生したりした場合、セキュリティ管理を改善・是正するための措置をとらなくてはならない。

表１　無線LANのセキュリティ管理におけるPDCAサイクル

ステップ	実施事項
Plan（計画策定）	●サイトサーベイ（電波の漏洩範囲の確認） ●リスク分析 ●ルールの策定 ●アセスメント（構成レビュー）
Do（実施・運用）	●セキュリティ機能の導入・設定 ●アセスメント（設定チェック）
Check（評価・監査）	●サイトサーベイ（不正な無線LAN機器の発見） ●アセスメント（設定チェック） ●アセスメント（侵入チェック） ●ログの監査 ●不要なユーザーアカウントの発見
Act（改善・是正）	●改善・是正計画の立案 ●改善・是正計画の実施

V　無線LANにおけるセキュリティ管理対策

無線LANにおけるセキュリティ管理対策で特徴的なリスク分析とサイトサーベイについて、具体例を述べる。

1　リスク分析

潜在的にリスクの高い無線LANを利用するに当たっては、セキュリティ対策を徹底する必要がある。一般的なセキュリティ対策にもいえることだが、対策を万全にするには多くのコストや労力がかかるため、リスク分析を実施し、必要とされるセキュリティレベルに基づいて最適なセキュリティ対策を実施することが重要である。

無線LANの場合、設置する場所によってセキュリティリスクが大きく異なるので、注意が必要である。例えば、大通りに面した建物、ガラス張りの建物、ビルの低層階、テナントビルなどは電波が漏洩する範囲に部外者がいてもおかしくないため、セキュリティ上

のリスクは高い。こうした場所で無線LANを利用する場合には、認証にハードウェアトークンを併用するなどの、より高度なセキュリティ対策を実施することが必要となる。

その他、扱っている情報資産などの要因によってもセキュリティリスクは大きく変化する。これらについては、一般的なセキュリティ対策でのリスク分析と同様に考えてよい。

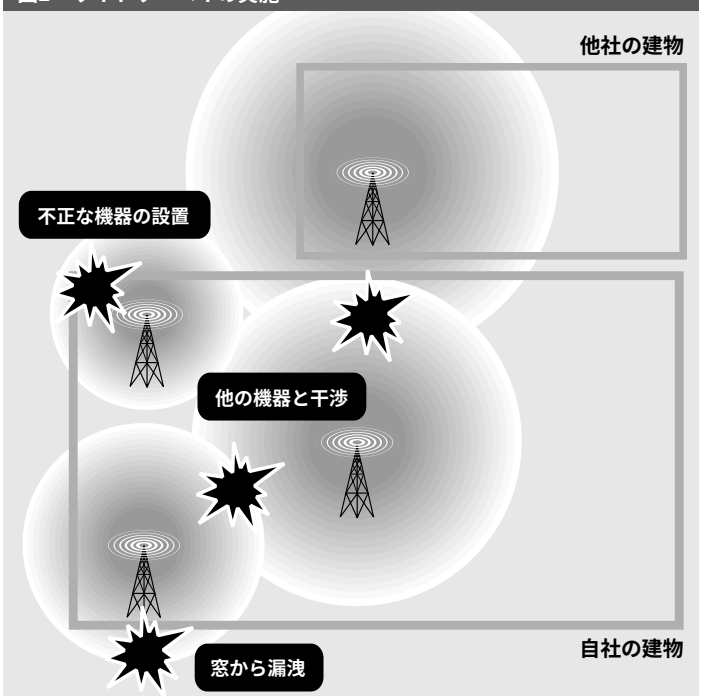
2　ルールの策定

セキュリティ管理を行ううえで、ルールの作成は必要不可欠である。特に、セキュリティ対策の行われていない無線LAN機器が企業内に設置されないように、注意しなくてはならない。このルールには、以下のような項目を盛り込むとよい。

①セキュリティ技術の導入

無線LANを利用する場合には、適切なセキュリティ技術の導入を義務づける。前述の暗号化と認証は、どちらも必須である。

図2　サイトサーベイの実施



②無線LAN機器の適切な設定

無線LAN機器を導入する際には、それらの機器を適切に設定するよう義務づける。また、これらの設定が適切に行われているか、定期的にチェックすることが望まれる。

③許可のない無線LAN機器の設置の禁止

無線LAN機器を、許可なく企業内LANに接続することを禁止する。アクセスポイントだけでなく、ノートパソコンに内蔵されている無線LAN機能についても、不要な場合はそれを使用不可にすることが望まれる。

3　サイトサーベイの実施

設置場所におけるセキュリティリスクの存在を知るために、無線LAN機器が発する電波の状態の調査が必要になる。このような調査のことを、筆者らはサイトサーベイと呼んでいる。サイトサーベイでは、無線LANを利用しているオフィスとその周辺で、以下の点について調査を行う（図2）。

①電波の漏洩範囲の確認

建物外を含め、電波が届く範囲を調査する。電波が届く範囲に、社外の人物がいてもおかしくないような場所があれば、セキュリティリスクは高くなるため、より高度なセキュリティが必要となる。また、このような場所に不審な人物が長時間いないか、日頃から気を付けることも重要である。

②不正な無線LAN機器（アクセスポイント）の発見

無線LAN機器が発している電波を調査し、企業内で管理されていない無線LAN機器がないかどうかを調査する。主に、社員が企業の許可なく設置した無線LAN機器を発見することが目的である。

③電波の干渉の調査

無線LAN機器（アクセスポイント）が発する同じ周波数帯の電波が重なる場所では、電波の干渉が起こり、無線LANの性能（通信速度）が低下する。セキュリティとは直接関係ないが、こうした無線LAN機器同士の干渉がないかどうかも調査しておく必要がある。このとき、社外の無線LAN機器が発する電波が窓などから入っていると、自企業内の無線LAN機器が発する電波と干渉してしまうことがあるので、注意が必要である。

4　アセスメントの実施

前述のようなルールを策定したとしても、守られなければ意味がない。特にセキュリティ関連のルールは、社員の利便性を損ねることが多いため、なかなか守られない傾向にある。このため、ルールが守られているかどうか監査を実施することが必要になる。さらに、実際のシステムにおいてセキュリティ対策に漏れはないか、セキュリティ機能が正しく動作しているか確認することも必要である。

これらは総じてアセスメント（評価）と呼ばれている。アセスメントを自社内で実施することは、セキュリティに関する専門性の観点からも困難であると思われる。公平性の観点からも、外部のセキュリティ専門家に委託して実施するのが望ましい。

無線LANのアセスメントとしては、以下のようなメニューが考えられる。

①無線LANの構成のレビュー

セキュリティを考慮してネットワークが構成されているかをレビューする。Planのステップとして、ネットワーク構築前に実施しておくのが望ましい。

②無線LAN機器の設定のチェック

無線LAN機器が適切に設定されているかをチェックする。Doのステップとして導入時に実施するだけでなく、Checkのステップとして定期的に実施するのが望ましい。

③侵入テスト

企業内無線LANに対して、擬似的に不正アクセスを試み、セキュリティホールが存在しないかをテストするもので、Checkのステップとして実施する。

④サイトサーベイ

前述のサイトサーベイも、アセスメントのメニューの1つとして考えられる。特に、不正な無線LAN機器の発見については、Checkのステップとして定期的に実施するのが望ましい。また、電波の漏洩範囲の確認については、Planのステップとしてネットワーク構築前に実施しておくのが望ましい。

Ⅵ　求められる総合的対策

無線LANのセキュリティ対策を行う場合、まずは技術的対策だけでは不十分なことを認識することが必要である。そのうえで、通常のセキュリティ対策と同様に、PDCAサイクルによるセキュリティ管理の仕組みを確立する必要がある。とはいえ、無線LAN特有のリスクも存在するため、サイトサーベイによるセキュリティ評価も行う必要がある。

著者

鴨志田昭輝（かもしだあきてる）
NRIセキュアテクノロジーズ情報セキュリティ調査室セキュリティコンサルタント
専門は情報セキュリティにかかわる調査、評価、コンサルテーション、教育