

分冊 4

無線 LAN 利用環境のための運用上の セキュリティ対策

目次

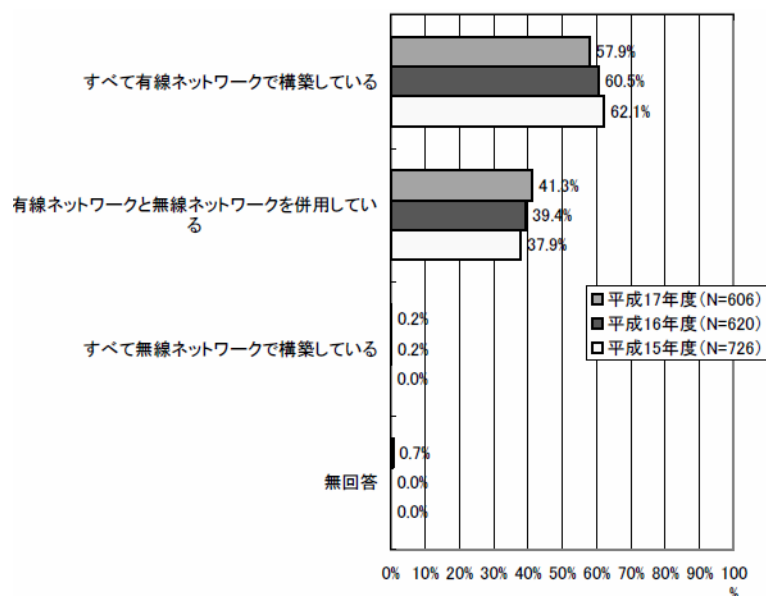
1	無線 LAN の利用とリスク	1
1.1	企業における現状と動向	1
1.2	システム概要	3
1.3	無線 LAN の規格	5
1.4	保護すべき情報資産	7
1.5	脅威とリスク	8
1.5.1	無線 LAN 通信の盗聴	8
1.5.2	無線 LAN への不正アクセス	9
2	無線 LAN におけるセキュリティ対策	11
2.1	技術的な対策	12
2.1.1	WEP 暗号の設定 ネットワーク	13
2.1.2	MAC アドレスフィルタリング ネットワーク	14
2.1.3	ESSID の ANY 接続拒否 ネットワーク	14
2.1.4	ESSID のステルス化 ネットワーク	14
2.1.5	IEEE802.1x 認証の導入 ネットワーク	15
2.1.6	IEEE802.11i (WPA2) の導入 ネットワーク	20
2.2	物理的対策	22
2.2.1	電波遮蔽シートの利用	22
2.3	運用面での対策	23
2.3.1	無線 LAN アクセスポイントの定期的なパスワード変更	23
2.3.2	無線 LAN アクセスポイントのログ収集	23
2.3.3	無線 LAN アクセスポイントの配置	23
3	用語	25

1 無線 LAN の利用とリスク

1.1 企業における現状と動向

無線 LAN とは、有線 LAN ケーブルを使わずに電波や赤外線を利用したネットワークのことである。最近では、無線 LAN 通信方式の標準化に伴い、無線 LAN 機器の低価格化や無線 LAN 機能を標準装備しているハードウェアが多く発売されている。これまで一部の教育機関などにしか使われていなかった無線 LAN が、最近では大企業や一般家庭においても広く利用されるようになってきている。警察庁「不正アクセス行為対策等の実態調査」によると、無線 LAN を導入している事業体は平成 17 年度で 4 割を超えており、増えつつあることがわかる（図表 1）。

図表 1 事業体内における無線 LAN の利用状況



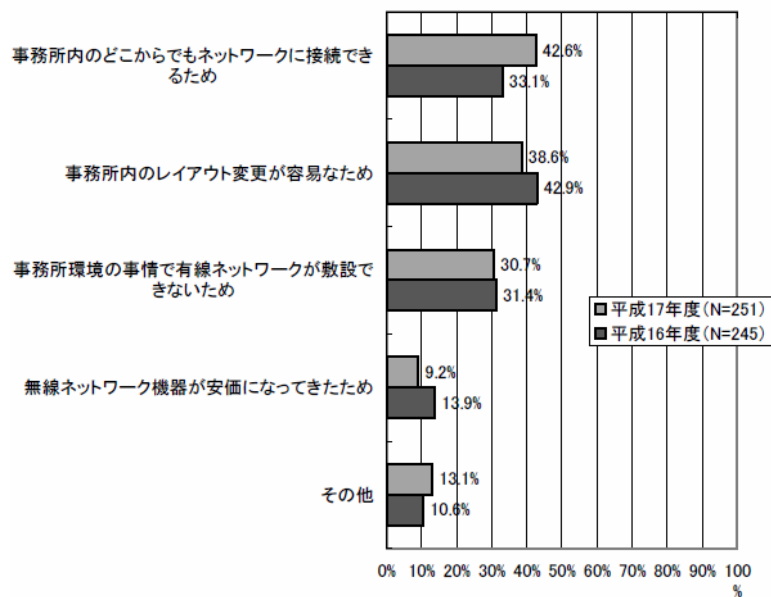
(出所) 警察庁「不正アクセス行為対策等の実態調査」(警察庁、平成 18 年 1 月)

無線 LAN 導入の理由は、どこからでもネットワークに接続できることによる物理的な制約からの解放が多いことがわかる（図表 2）。有線 LAN ケーブルの敷設や保守からも解放されることから、管理者としてのメリットも大きい。しかしながら、有線 LAN と異なり、無線 LAN では電波を用いていることから、有線 LAN とは異なる脅威が存在する。また、その対策が不完全である場合に起こりうる被害は、社内ネ

ットワークおよびイントラネットに対するものとなりうるため、甚大となることが多い。

無線 LAN を安全に安心して利用するために、適切なセキュリティ対策を実施することが重要である。

図表 2 無線 LAN を利用する理由

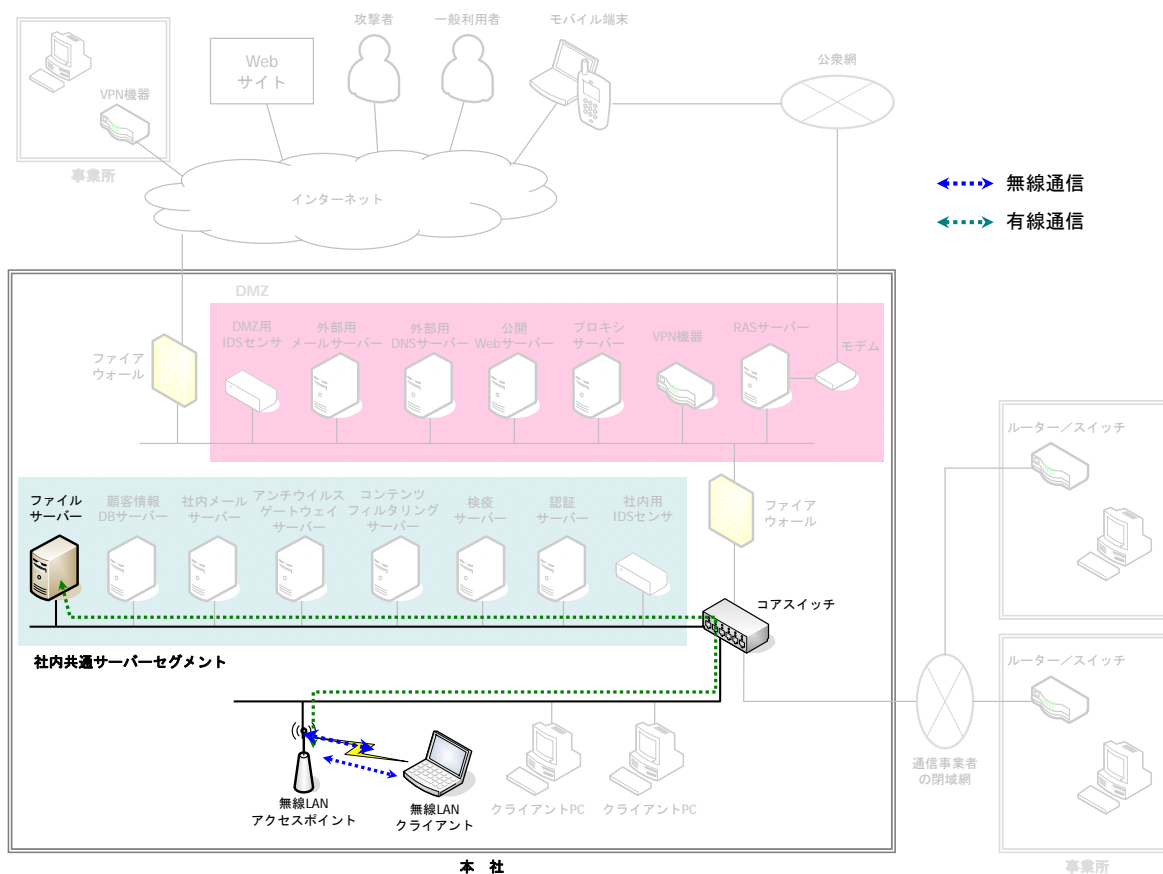


(出所) 警察庁「不正アクセス行為対策等の実態調査」(警察庁、平成18年1月)

1.2 システム概要

無線 LAN 環境の基本的なシステム構成を図表 3 に示す。

図表 3 無線 LAN 環境のシステム構成



※ファイルサーバーは便宜上示しているが、必ずしも無線 LAN システムに必要ではない。

(1) 無線 LAN アクセスポイント

無線 LAN アクセスポイントとは、無線電波によりデータを送受信し、無線 LAN クライアントと社内ネットワークを接続する中継器である。現在は有線 LAN との接続機能も持っている機器が主流である。

(2) 無線 LAN クライアント (無線 LAN 端末)

無線 LAN クライアントとは、無線電波によりデータを送受信する機能を持った PC 端末等をいう。企業における無線 LAN クライアントの接続形態は、無線 LAN アクセスポイントを経由してネットワークに接続するインフラストラクチャモード (Infrastructure Mode) が一般的であるが、無線 LAN クライアント同士が直接通信することもできる (アドホックモード (Adhoc Mode))。

現在では様々なタイプの製品があり、PC カードや USB ポートに差し込んで使用するタイプや、最近では端末自体に無線 LAN 機能が内蔵されているノート PC もある。

1.3 無線 LAN の規格

無線 LAN にはいくつかの規格があり、それらは IEEE（米国電気電子学会）の 802 委員会で定められている。2007 年現在の市場に見られる無線 LAN の通信規格には、以下の 4 つがある。

- IEEE802. 11a
- IEEE802. 11b
- IEEE802. 11g
- IEEE802. 11n

以下、それぞれについて説明する。

(1) IEEE802. 11a

5. 2GHz 帯の無線で最大 54Mbps の通信を行なうことができる。転送速度で見ると IEEE 802. 11b から大幅に高速化されているが、障害物があると繋がりにくいなどの欠点がある。また、移動体衛星通信システムにも利用されていることから、電波法によって屋外での利用が禁止されている。

(2) IEEE802. 11b

2. 4GHz 帯の無線で最大 11Mbps の通信を行なうことができる。無線免許なしで自由に使え、11Mbps の速度で 50m～100m の距離にある端末間で通信を行なうことができる。同じ 2. 4GHz 帯の電波を使う医療用機器や電子レンジ、Bluetooth 対応製品などが近くにあると電波干渉が発生し、通信速度が低下することがある。

(3) IEEE802. 11g

IEEE802. 11b の上位規格として策定され、IEEE802. 11b と同じ 2. 4GHz 帯 を利用しているが、最大通信速度は 11Mbps から 54Mbps に高速化されている。IEEE802. 11b と同様、他の電波を発する機器からの電波干渉を受ける可能性がある。

また、IEEE802. 11b に対する上位互換性を持っており、従来の IEEE802. 11b 規格の機器と接続する場合は、IEEE802. 11b モードで動作するため、最大 11Mbps での通信が可能である。

(4) IEEE802.11n (2007年策定予定)

IEEE が 2007 年後半策定予定の無線 LAN 規格の一つであり、実効速度 100Mbps 以上、IEEE802.11a や IEEE802.11g との上位互換性を持つことが特徴である。高速化に、MIMO (Multiple-Input Multiple-Output) と呼ばれる、多重化したデータを複数の送信アンテナと受信アンテナによって送受信する技術を用いている。2006 年 3 月、Draft Ver1.0 が策定された。

図表 4 に、各無線 LAN 通信規格の特徴を示す。

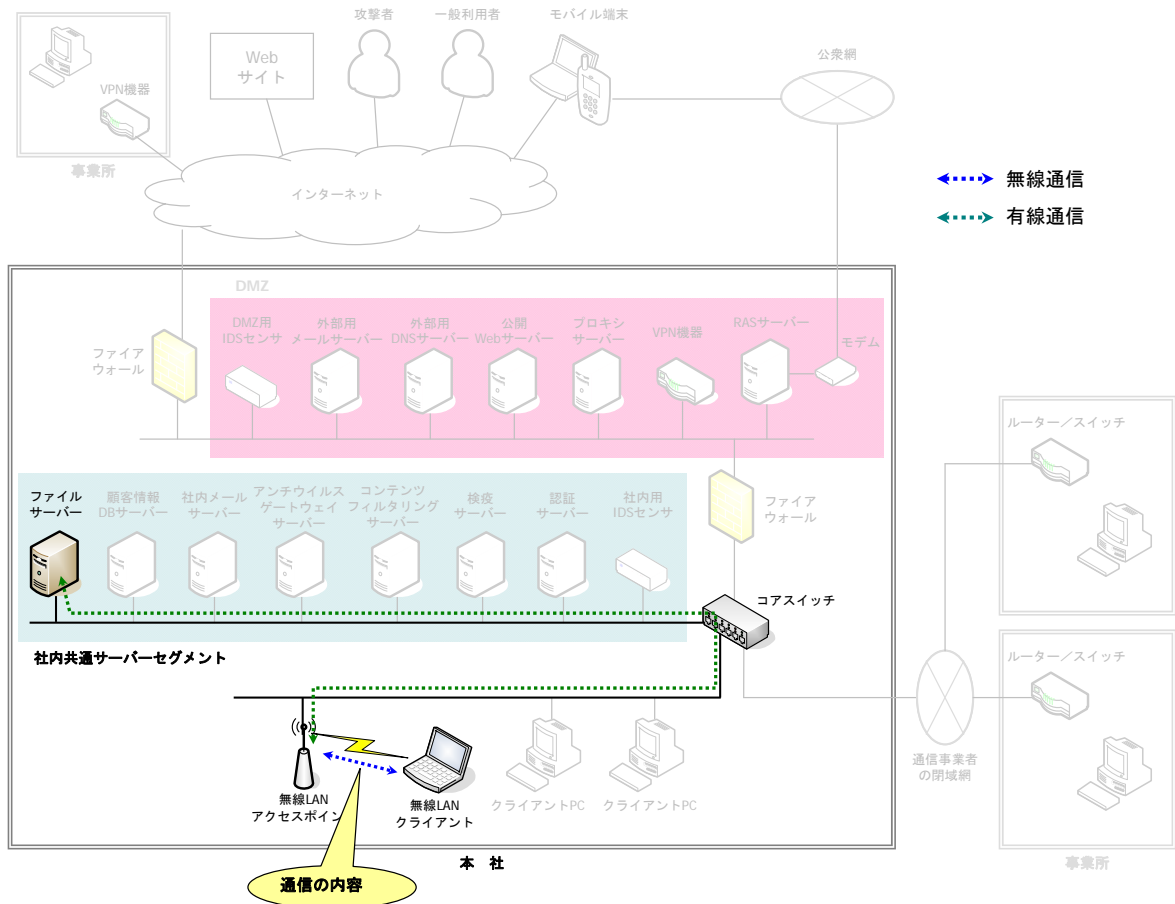
図表 4 無線 LAN 通信規格の特徴

	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
使用周波数帯	5.15～5.25GHz	2.4～2.472GHz	2.4～2.472GHz	20 また 40MHz 帯
伝送速度 (Mbps)	54/48/36/24 /18/12/9/6	11/5.5/2/1	54/48/36/24 /18/12/9/6	約 100Mbps
チャンネル数 (同時)	4 (4)	14 (4)	13 (3)	未定
最大伝送距離	約 90m	約 180m	約 180m	未定
屋外利用	不可	可	可	未定
特徴	電波干渉に強く、伝送速度も速いが、屋外使用が不可。	導入コストが安い が伝送速度が遅く、電波干渉を受けやすい。	伝送速度が速く、11b との上位互換も可能。11b と比べてコストが割高。 電波干渉を受けやすい。	高速通信が可能。 具体的な詳細は未定。

1.4 保護すべき情報資産

保護すべき情報資産として、想定されるものを例示する（図表 5, 6）。

図表 5 保護すべき情報資産



図表 6 保護すべき情報資産

箇所	情報資産
無線通信	通信の内容*

※ 機密情報や個人情報など、企業における情報資産を含んだものを対象としている。

1.5 脅威とリスク

1.5.1 無線 LAN 通信の盗聴

概要

無線 LAN における通信の盗聴とは、悪意のある第三者が無線電波を故意に傍受し、その通信内容を盗み見る行為を指す。無線電波の傍受そのものは、パケットキャプチャツールを使用すれば簡単に行うことができる。無線 LAN の電波は、使用している規格にもよるが、約 100 メートル程度まで届く場合がある。また、市販されているアンテナ等を利用することで、300 から 400 メートル離れた無線 LAN の通信内容を盗聴することも可能となる。

リスク

通信を暗号化していない場合は、機密情報を通信した場合に外部に漏洩してしまうおそれがある。

この脅威への有効なセキュリティ対策

- 2.1.1 WEB 暗号の設定 ネットワーク
- 2.1.6 IEEE802.11i (WPA2) の導入 ネットワーク
- 2.2.1 電波遮蔽シートの利用

1.5.2 無線 LAN への不正アクセス

概要

不正アクセス行為については、「不正アクセス行為の禁止等に関する法律」に定義された不正アクセス行為および不正アクセスを助長する行為のことをいい、具体的には、以下に示す行為を指す。

- コンピューターの OS やアプリケーションあるいはハードウェアに存在する脆弱性（セキュリティホール）を利用して、コンピューターのアクセス制御機能を迂回し、コンピューター内に侵入する行為（侵入行為）
- 他の人に与えられた、利用者 ID およびパスワードをその持ち主の許可を得ずに利用して、持ち主に提供されるべきサービスを受ける行為（なりすまし行為）
- 持ち主の許可を得ずに、その持ち主の利用者 ID およびパスワードを第三者に提供する行為

無線 LAN を設置した際には、そのアクセスを従業員等の特定者に限定する意図であったにもかかわらず、攻撃者が無線 LAN アクセスポイントを通じてネットワークにアクセスする可能性がある。この行為は、通常は、不正アクセス禁止法に規定された不正アクセスに該当しないが、ここでは、それも含めて広義の「不正アクセス」と呼ぶ。

無線 LAN アクセスポイントと無線 LAN クライアントは、基本的に同じ ESSID¹ と呼ばれる識別子が設定されていなければ接続できない仕組みになっている。ここで、無線 LAN クライアント側で ESSID を「ANY」あるいは空欄に設定した場合、すべての無線 LAN アクセスポイントと通信することが可能になる。これは、無線 LAN アクセスポイントから、Beacon（ビーコン）と呼ばれるパケットデータを周囲に配信しているためである。この Beacon の中には ESSID が含まれており、攻撃者はこの Beacon から ESSID の値を読み取ることで不正アクセスを行うことが可能となる。

リスク

不正アクセスを許し社内の無線 LAN に侵入されてしまった場合、攻撃者の PC は社内ネットワークに接続されたクライアント PC と全く同じ存在となる。したがって、社内クライアント PC がアクセスできる範囲のネットワークに対し、攻撃者も同じくアクセスできることになるため、共有サーバー等へのセキュリティ対策が脆弱である場合は、機密情報を盗まれるなど被害が拡大するおそれがある。

この脅威への有効なセキュリティ対策

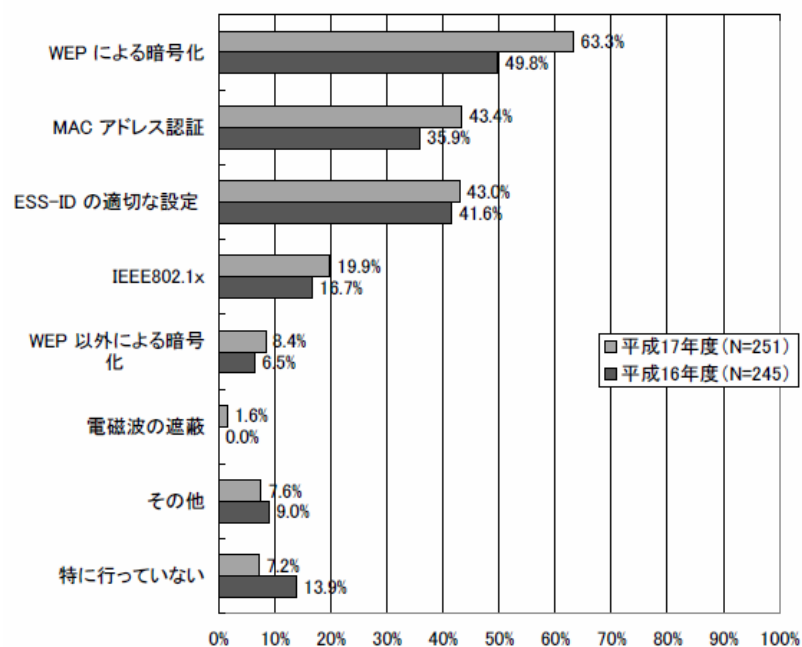
- 2.1.2 MACアドレスフィルタリング ネットワーク
- 2.1.3 ESSIDのANY接続拒否 ネットワーク
- 2.1.4 ESSIDのステルス化 ネットワーク
- 2.1.5 IEEE802.1x認証の導入 ネットワーク
- 2.2.1 電波遮蔽シートの利用

2 無線 LAN におけるセキュリティ対策

無線 LAN を利用する場合において適切なセキュリティ設定を行わないまま使用することは、通信の盗聴や不正な利用による重大なリスクを招くことになる。

ここでは無線 LAN に対して施すべきセキュリティ対策を示す。なお、警察庁「不正アクセス行為対策等の実態調査」の報告によると、何らかのセキュリティ対策を講じている企業が増えつつあることがわかる(図表 7)。

図表 7 事業体内無線 LAN へのセキュリティ対策

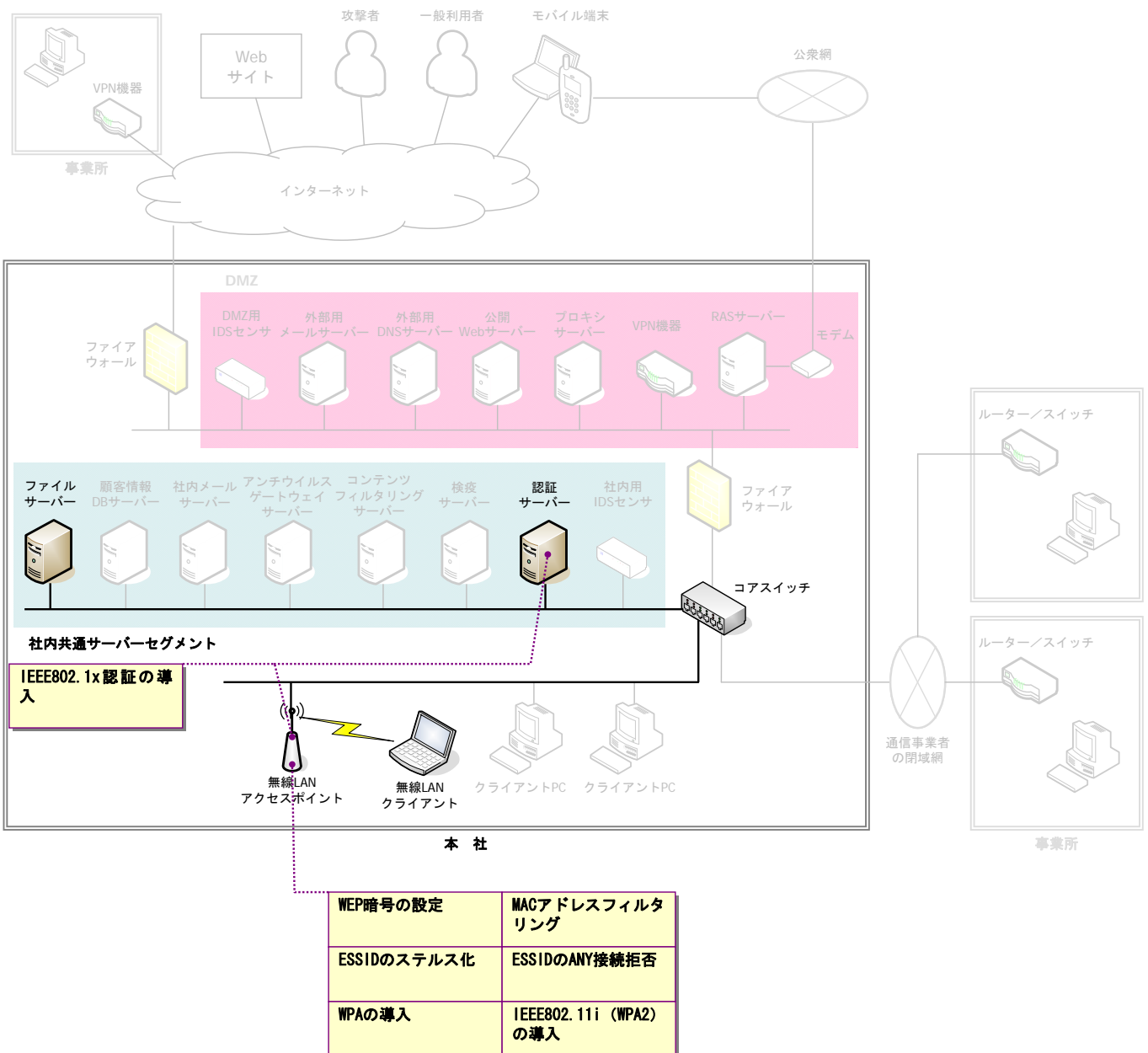


(出所) 警察庁「不正アクセス行為対策等の実態調査」(警察庁、平成 18 年 1 月)

2.1 技術的な対策

ここでは、無線 LAN 環境を運用する上での脅威に対する技術的なセキュリティ対策を説明する（図表 8）。ここに登場するセキュリティ対策は、リスクに応じて導入することが望ましい。

図表 8 無線 LAN 環境における技術的なセキュリティ対策



2.1.1 WEP 暗号の設定 ネットワーク

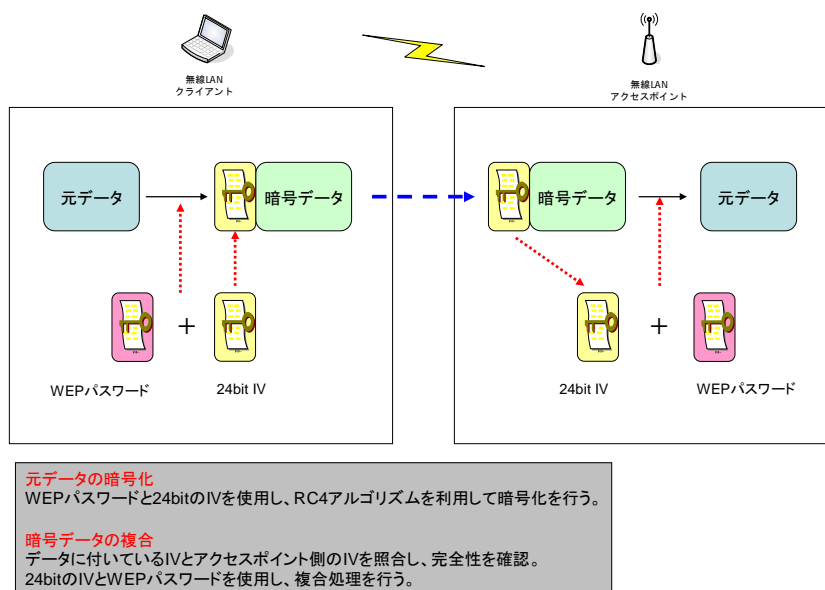
この対策により防ぐことができる脅威

1.5.1 無線 LAN 通信の盗聴

WEP (Wired Equivalent Privacy) とは無線通信における暗号化技術である。無線通信は交信が可能な範囲内であれば屋外からでも容易にアクセスできるため、送信されるパケットを暗号化して内容を知られないようにする必要がある。ユーザーが設定する秘密鍵と、製品内部で決める IV (Initialization Vector、初期化ベクタ) とをあわせた数字を基に、RC4 と呼ばれる暗号化アルゴリズムを用いて擬似的な乱数列を作り、データをフレームごとに暗号化する (図表 9)。

WEP を使用するには、ユーザーが設定した秘密鍵を、無線 LAN クライアントと無線 LAN アクセスポイントの双方に設定する必要がある。秘密鍵の長さは 64bit と 128bit を設定することができるが、128bit の方が設定できる文字列が長くなることから、64bit に比べ秘匿性が向上する。しかし、同じ秘密鍵と同じ IV (初期化ベクタ) を使った複数のパケットを集めると容易に暗号が解読されてしまうぜい弱性が見つかり、現在では必ずしも WEP を使用してさえいけば 128bit 鍵長であっても安全だとは言えなくなっているため、運用の際には定期的に秘密鍵の変更を行う必要がある。

図表 9 WEP 暗号化の流れ



2.1.2 MAC アドレスフィルタリング ネットワーク

この対策により防ぐことができる脅威

1.5.2 無線 LAN への不正アクセス

MAC アドレスフィルタリングとは、無線 LAN クライアントのネットワークインタフェースが持つ MAC アドレスによってアクセスを制御する認証方式である。無線 LAN アクセスポイント側で登録された MAC アドレスを持つ機器が、無線 LAN アクセスポイントへ通信を行った場合のみ接続することができる。仮に、登録されていない MAC アドレスを持つ無線 LAN クライアントからアクセスがあった場合は、アクセス拒否を行う。

2.1.3 ESSID の ANY 接続拒否 ネットワーク

この対策により防ぐことができる脅威

1.5.2 無線 LAN への不正アクセス

ESSID の ANY 接続拒否とは、無線 LAN アクセスポイントの設定において ESSID が「ANY」や空欄の設定になっている無線 LAN クライアントを拒否する対策のことをいう。この対策により、不特定多数の無線 LAN 端末からの接続を防ぐことが可能となる。

2.1.4 ESSID のステルス化 ネットワーク

この対策により防ぐことができる脅威

1.5.2 無線 LAN への不正アクセス

ESSID のステルス化とは、無線 LAN アクセスポイントから定期的には送信している Beacon 信号を停止する対策をいう。正規のユーザーは ESSID を無線 LAN アクセスポイントからの配信以外の手段で入手し、無線 LAN クライアントに設定する必要がある。

2.1.5 IEEE802.1x 認証の導入 ネットワーク

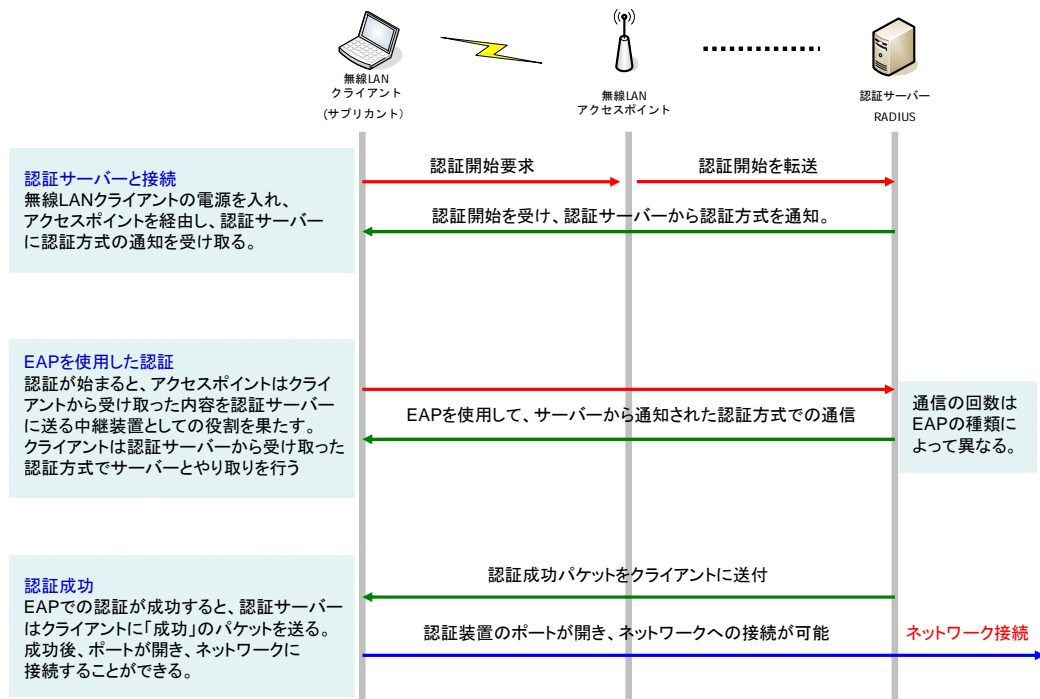
この対策により防ぐことができる脅威

1.5.2 無線 LAN への不正アクセス

IEEE802.1x 認証とは、ユーザーを認証してから、ネットワークへの接続を許可するための認証技術であり、有線 LAN と無線 LAN のどちらでも使用することができる。

図表 10 に IEEE802.1x 認証の概要を示す。必要な機器としては、IEEE802.1x に対応した無線 LAN アクセスポイントと、これとは別に認証を行うための認証サーバーが必要となる。認証サーバーには RADIUS² サーバーが利用されることが多い。無線 LAN クライアント側には「サブリカント」と呼ばれる専用のソフトウェアが必要となるが、Windows 2000 SP4 以降もしくは Windows XP や Windows Vista であれば、標準でインストールされている。IEEE802.1x 認証では、EAP (Extensible Authentication Protocol) が用いられる。EAP とはダイヤルアップ接続等に利用されている認証プロトコルである PPP (Point to Point Protocol) を拡張したもので、MD5 や証明書を用いた TLS などの認証方式をサポートしている。

図表 10 IEEE802.1x 認証の概要



以下、EAPとして広く使われているEAP-TLS、PEAP、EAP-TTLSについて説明する。

(1) EAP-TLS (Extensible Authentication Protocol-Transport Layer Security)

EAP-TLSでは認証サーバー(RADIUSサーバー)と無線LANクライアントの両方に、CAサーバーが発行したサーバー証明書とクライアント証明書が必要になる。ユーザー名とパスワードを用いる認証方式と比較して、ユーザーだけでなく利用端末まで特定できるのが特徴である。

証明書には、ユーザー名、有効期限などの属性情報と、CAサーバーの電子署名が含まれる。この証明書をRADIUSサーバーと無線LANクライアントとの間で交換し、電子署名が正しいものであると検証された後に、相互を信頼する公開鍵認証方式を用いているため、セキュリティレベルが高いという特徴がある。

(2) PEAP (Protected Extensible Authentication Protocol)

PEAPとは、認証サーバー側で証明書を発行し、またクライアント側ではIDとパスワードを用いることによって、サーバーとクライアントで相互認証を行う認証方

式である。暗号化技術には WEP が用いられており、定期的に WEP 暗号文の生成・配布が行われることによって WEP 暗号のセキュリティの向上が図られている。

EAP-TLS と比較するとセキュリティレベルは若干落ちるが、クライアント側で証明書管理の必要がないため、管理が容易になる。

(3) EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security)

EAP-TTLS とは、暗号化によって保護された ID とパスワードを用いた認証方式である。EAP-TLS が、クライアントとサーバーの間で相互に証明書を交換することで相互認証を行う認証方式であるのに対し、EAP-TTLS では、クライアント側は証明書を発行せず、その代わりにユーザー名とパスワードを用いて認証を行う。その際、鍵暗号を用いて通信を暗号化することによって盗聴による情報漏洩の危険性を抑えている。EAP-TTLS は、EAP-TLS に劣らないセキュリティ性を保ちながら、個々のコンピュータに依存せずどこからでもユーザー認証を行うことができるというメリットがあるが、専用のサブリカントをクライアント側に入れる必要がある。

前ページまでに、一般的な認証方法として、EAP-TLS、PEAP、EAP-TTLS を挙げたが、それ以外には、EAP-MD5、LEAP などの認証方式がある。図表 11 にそれらを含めた認証方式の特徴をまとめた。

図表 11 認証方式の特徴

認証方式	証明書		サブリカント	相互認証	特徴
	サーバー	クライアント			
EAP-TLS	○	○	Windows2000SP4以降	証明書	セキュリティレベル：高 証明書の管理がクライアント側でも必要となる。証明書は USBメモリや IC カードでの管理が推奨される。
PEAP	○	×	Windows2000SP4以降	証明書および ID/パスワード	セキュリティレベル：中 EAP-TLS と比較するとセキュリティレベルは若干落ちるが、クライアント側で証明書を管理する必要がないため、管理が容易。
EAP-TTLS	○	×	要インストール	証明書および ID/パスワード	セキュリティレベル：中 EAP-TLS と比較するとセキュリティレベルは若干落ちるが、クライアント PC 側に証明書を導入する必要がなく管理は容易。ただし、EAP-TTLS に対応している OS がないため、専用サブリカントをインストールする必要がある。
EAP-MD5	×	×	Windows2000SP4以降	CHAP による チャレンジ/レスポンス	CHAP を使うため、サーバ側からクライアントへの一方向の認証であり、他の EAP の認証方式と比べるとセキュリティ強度が劣る
LEAP	×	×	Cisco 製品に添付	ID/パスワード	証明書を使用しないため管理は容易。Cisco 製品のみで使用するため、機器をそろえる必要がある。

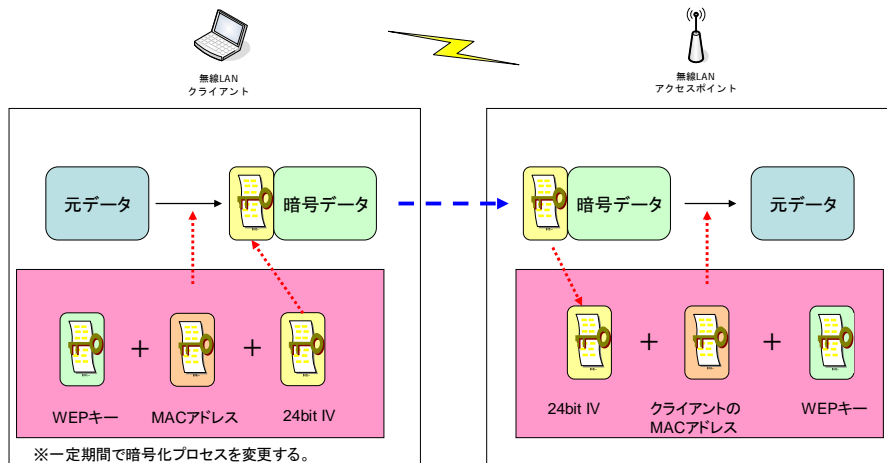
2.1.6 WPA の導入 ネットワーク

この対策により防ぐことができる脅威

1.5.1 無線 LAN 通信の盗聴

2.1.1 で述べた WEP は、いくつかのセキュリティ面での脆弱性が懸念されていたおり、WEP に代わる規格として登場したのが WPA (Wi-Fi Protected Access) である。WEP では、無線 LAN クライアントと無線 LAN アクセスポイントが共通の暗号鍵を長期間にわたって用いていたため、暗号鍵が解読される可能性があった。一方、WPA では TKIP (Temporal Key Integrity Protocol) と呼ばれる、暗号鍵を一定の時間ごとに自動的に変更するという技術を用いるなどの改良がなされている (図表 12)。

図表 12 WPA 暗号化の流れ



元データの暗号化

WEPパスワード、24bitのIV、MACアドレスのハッシュ値を使用し、暗号化を行う。また、暗号化のために必要な鍵は、定期的(一定期間または一定パケットの送受信)に変更される。

2.1.7 IEEE802.11i (WPA2) の導入 ネットワーク

この対策により防ぐことができる脅威

1.5.1 無線 LAN 通信の盗聴

IEEE802.11i は、2004 年 7 月に制定された無線 LAN におけるセキュリティ標準を定める規格である。先に挙げた WPA は IEEE802.11i に採用される予定であった暗号化規格の一部である。IEEE802.11i 制定後、Wi-Fi Alliance はさらにセキュリティを高めた WPA2 という WPA の改良規格を発表した。WPA2 では AES³ が暗号化アルゴリズムとして用いられている。今後導入する場合は、WPA2 に対応した無線 LAN アクセスポイントを購入し、WPA2 を利用することが望ましい。WPA との違いを以下に示す。

(1) 暗号化方式

WPA が採用している RC4 方式は 1bit ごとに暗号化を行うストリーム方式であるのに対して、WPA2 が採用している AES は 128/192/256bit の鍵長をサポートするブロック暗号方式である。

(2) 改ざん検出機構

データの完全性を確保するために従来使用していた ICV, MIC 方式ではなく AES を用いた CCM 方式を用いている。これにより、順番が誤って送信されたパケットは無線 LAN アクセスポイント側で破棄される。

図表 13 に、WEP、WPA、WPA2 の比較を示す。

図表 13 無線 LAN で用いられる暗号の比較

	WEP	WPA	WPA2
暗号鍵の長さ	64/128	128	128/192/256
IV の長さ	24	48	48
暗号化アルゴリズム	RC4	RC4	AES
改ざん検出	ICV	MIC	CCM
セキュリティレベル	低い	やや高い	高い

2.2 物理的対策

2.2.1 電波遮蔽シートの利用

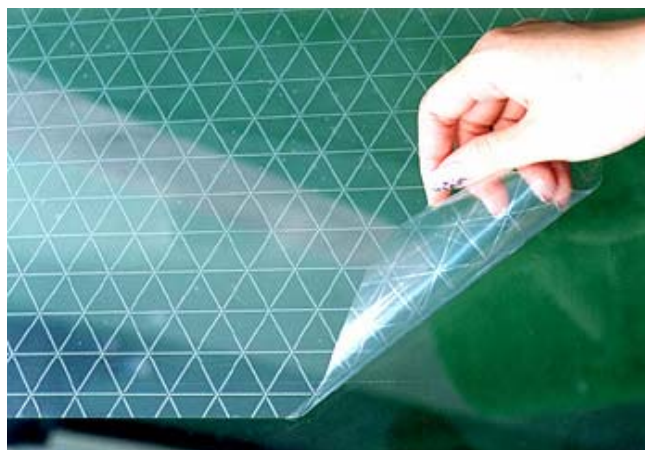
この対策により防ぐことができる脅威

- 1.5.1 無線 LAN 通信の盗聴
- 1.5.2 無線 LAN への不正アクセス

無線 LAN アクセスポイントや無線 LAN クライアントに対しセキュリティ対策を施したとしても、空間を行き交う電波そのものを制限することはできない。これは有線にはない無線特有のものであり、社外に漏れた電波を通じて盗聴、あるいは社内ネットワークに侵入されるおそれがある。そのため、導入を躊躇している企業も多い。

利用中の無線 LAN が使用している電波が社外に漏れることを防ぐための対策として、電波遮蔽シートがあげられる（図表 14）。電波遮蔽シートとは、アルミニウムや鉄などの導電体をシート状にしたもので、特に窓などの電波を遮蔽する能力に欠ける箇所に対して設置することが多い。電波遮蔽シートを利用することにより、手軽に窓や壁、天井などに対し電波の漏洩対策を実施することができる。また、遮蔽する周波数帯域を選定できるものもあり、無線 LAN に利用される周波数帯のみを遮蔽し、携帯電話や PHS などのモバイル端末の電波やテレビ電波を通すことができる製品もあるため、利用する環境における条件に応じて製品を選択することが重要である。

図表 14 窓に貼ることができる電波遮蔽シートの例



（出所） 鹿島建設株式会社資料

2.3 運用面での対策

無線 LAN アクセスポイントや、無線 LAN クライアントを安全に、かつ効率よく運用していくためには、技術的な対策だけでなく運用による対策も不可欠である。運用面での対策として代表的なものを紹介する。

2.3.1 無線 LAN アクセスポイントの定期的なパスワード変更

管理者は、無線 LAN アクセスポイントにログインした後、ユーザー管理や接続許可クライアントなどの様々な設定を行う。悪意のある第三者からの不正アクセスに備え、管理者のパスワードを推測されにくいパスワード（アルファベットの大文字 / 小文字、および数字の組み合わせ）に設定し、かつ、定期的にパスワード変更を行うことが望ましい。

2.3.2 無線 LAN アクセスポイントのログ収集

現在の無線 LAN アクセスポイントにはログを収集する機能を持つ製品も多く存在する。不正なアクセスを試みる無線 LAN クライアントの早期検知や、事故後の追跡のためにもアクセスログを取得することが望まれる。また、ログの転送機能を持った無線 LAN アクセスポイントの場合は、リアルタイムにログを転送するなどの設定を行うことが推奨される。

なお、承認されていない無線 LAN クライアントが無線 LAN アクセスポイントのそばを通過するだけで自動的に接続を試みるため、認証に失敗したアクセスの全てが不正とは限らない。

2.3.3 無線 LAN アクセスポイントの配置

同一スペース内に、複数の無線 LAN アクセスポイントを設置した場合、電波干渉を起こす可能性がある。電波状況は、設置されている机、キャビネット、パーティションの有無、天井の素材などによって変化するからである。

以下に紹介する機能やツールを利用することにより、電波干渉を防ぎ、効率よく無線 LAN アクセスポイントの設置または管理を行うことが可能である

(1) サイト・サーベイ・ツール

サイト・サーベイ・ツールとは、アクセスポイントを設置したいフロアの広さや、通信レートなどの基本的な情報を入力するだけで、設置イメージを表示するツールである。表示されたイメージに従って、アクセスポイントの設置を行えば良い。

(2) キャリブレーション機能

キャリブレーション機能とは、無線 LAN アクセスポイントが持つ機能で、複数設置されたアクセスポイント同士が、お互いに電波を送受信し、他の無線 LAN アクセスポイントとの位置関係や、距離を検知し、送信出力などを自動的に調整する機能である。

(3) 集中管理ソフトウェア

集中管理ソフトウェアとは、1 台のコンソール上で複数の無線 LAN アクセスポイントの使用状況、ファームウェアの更新、また、無線 LAN アクセスポイントに接続されている無線 LAN クライアントなどの表示を行うことができるソフトウェアである。

3 用語

1. **ESSID** Extended Service Set Identifier の略。無線 LAN におけるネットワーク識別子の一つ。混信を避けるために使用するネットワーク名としての役割を果たす。ESSID を用いることにより、正規のユーザーが、意図しないネットワークに接続しないようにすることと同時に、ある程度の使用者を制限することができる。SSID (Service Set Identifier) とも呼ばれる。
2. **RADIUS** Remote Authentication Dial-In User Service の略。ネットワーク利用者の認証と利用記録を、ネットワーク上の認証サーバーに一元化することを目的としたプロトコルである。認証サーバーに収容されたユーザー情報に基づいて接続の許可/不許可を判断し、接続の記録を取るのが主な役割である。元々は、名前にもあるように、ダイヤルアップネットワーク接続を、実現することを目的として開発されたが、無線 LAN サービスなどでも広く利用されている。
3. **AES** Advanced Encryption Standard の略。従来の標準暗号として 1977 年から使用されていた DES が、コンピュータの高性能化や、暗号理論の発展に伴い信頼性が低下してきたため、公募方式によって新たに選定された米国政府標準暗号であり、ISO/IEC 18033-3 ブロック暗号の一つとして採用されている。DES では暗号鍵が 56 ビットであることに対し、AES では 128、192、256 ビットの長さから選択する。