別紙２

企業等が安心して
無線LANを導入・運用するために
（案）

総　　務　　省

平成２４年１２月

目　次

はじめに

無線ＬＡＮは、スマートフォン等対応機器の増加、公衆無線ＬＡＮの整備、携帯電話網のひっ迫緩和を目的とした携帯電話事業者による利用促進を背景として、一般における利用が拡大している。これに対して、企業等の組織においては、ネットワークの構築及び変更が容易であるなどの利点から、従来の有線ＬＡＮを置き換える形で、無線ＬＡＮの導入が進展している。他方、無線ＬＡＮは、マルウェア感染等インターネットの利用における情報セキュリティ上の脅威一般に加え、電波を利用するために有線と比較して傍受等が容易であることに起因する脅威にもさらされており、無線ＬＡＮの利用に当たって、適切な情報セキュリティ対策が取られていない場合には、通信内容の窃取等の行為を惹起するおそれがある。

そのため、サイバー攻撃等の脅威が増大している昨今、機微な情報を取り扱う企業等の組織においては、一般の利用者と比して、より入念な情報セキュリティ対策を積極的に取ることが求められている。

本手引書では、企業等の組織が当該組織の構成員にのみ無線ＬＡＮ利用を許可する形態において、想定される情報セキュリティ上の脅威、及びそれらの脅威に対して当該組織のＬＡＮ管理者が取るべき情報セキュリティ対策を示した。また、無線ＬＡＮの導入・運用の各段階において、取るべき情報セキュリティ対策や方式の検討等、実施すべき事項を示した。さらに、情報セキュリティ対策を適切に取らずに運用すると生じる危険性について、具体的な事例を交えて解説し、それぞれの事例の原因と解決策を示した。

なお、本手引書は、読み手の一定の技術的知見を前提とするものであり、組織内にそのような知見を持つ人材がいない場合には、無理に組織内で対処するのではなく、適宜、外部の専門業者等の協力を求めることが適当である。ただし、その場合であっても、組織が保有する情報資産に関する責任は、当該組織が負うことに留意する必要がある。

企業等の組織が、本手引書を参考にすることにより、無線ＬＡＮを安心して導入・運用することが望まれる。

第１章　企業等における無線ＬＡＮの運用及び脅威

1.1 本手引書が対象とする範囲

(1) 無線ＬＡＮの運用形態

無線ＬＡＮは、ネットワークの構築及び変更が容易であるなどの利点から、企業等の組織において、従来の有線ＬＡＮを置き換える形で導入が進展している。

企業等の組織における無線ＬＡＮの運用形態は、当該無線ＬＡＮの利用を許可する者の範囲（例えば、組織の構成員に限定、組織の構成員に加え第三者にも開放等）により様々な形態を取るが、本手引書においては、最も基本的かつ一般的な運用形態、即ち図１に示すように無線ＬＡＮを、組織の構成員のみが利用する形態を対象とする[1]。

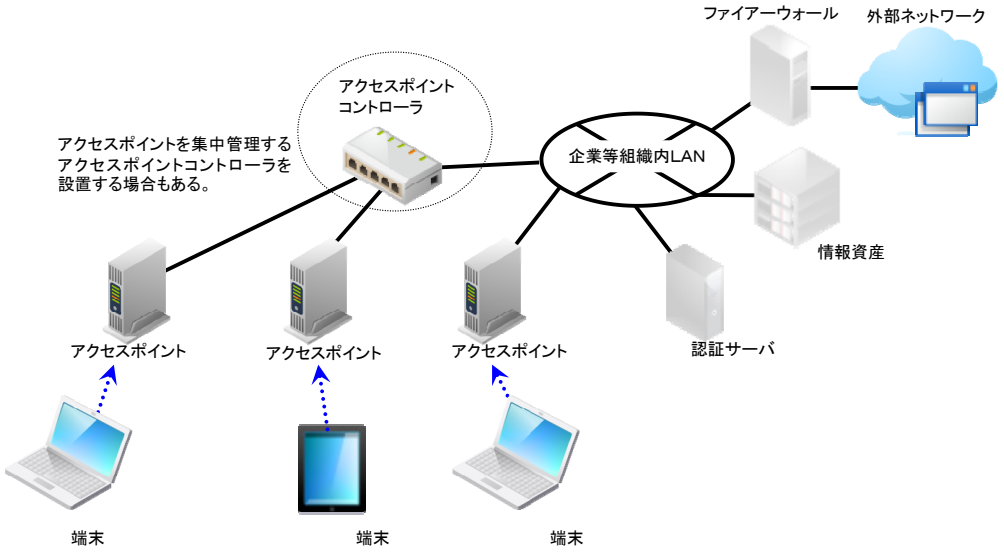

図１　企業等の組織における無線ＬＡＮの構成例

(2) 無線ＬＡＮの規格

一般に企業等の組織における無線ＬＡＮは、表１に示すＩＥＥＥ（米国電気電子学会）802 委員会のＩＥＥＥ802.11 グループで定められている規格に対応した無線通信機器により構成される。よって、本手引書においては、ＩＥＥＥ802.11 で規格化されている無線ＬＡＮを対象とし、無線ＬＡＮと端末の接続点であるアクセスポイントにおける情報セキュリティ対策を中心に述べる。

なお、有線ＬＡＮ及び無線ＬＡＮに共通するマルウェア感染対策等一般的な情報セキュリティ対策については、取り扱わないこととする。

表１　ＩＥＥＥ802.11 の代表的な規格

規格名	使用する周波数帯	最大通信速度	屋外使用の可否
IEEE802.11b	2.4GHz 帯	11Mbps	可
IEEE802.11g	2.4GHz 帯	54Mbps	可
IEEE802.11a	５GHz 帯	54Mbps	５GHz 帯の一部で不可
IEEE802.11n	2.4GHz 帯及び５GHz 帯	600Mbps	５GHz 帯の一部で不可

[1] 第三者に対する無線ＬＡＮの使用許可については、各府省情報化統括責任者（ＣＩＯ）補佐官等連絡会議 情報セキュリティワーキンググループ（ＷＧ４） 無線ＬＡＮセキュリティ要件ＳＷＧが 2011 年３月に取りまとめた「無線ＬＡＮセキュリティ要件の検討」において、組織の構成員と来訪者とにそれぞれ別のアクセスポイントを設置する形態が、ユースケースとして示されている。（http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/dai65/65lan_kentou.pdf）

1.2 情報セキュリティ上の脅威

無線ＬＡＮは、インターネットの利用における情報セキュリティ上の脅威一般に加え、電波を利用するために、有線と比較して傍受等が容易であることに起因する脅威にもさらされている。企業等による無線ＬＡＮの運用における情報セキュリティ上の主な脅威を以下に示す。

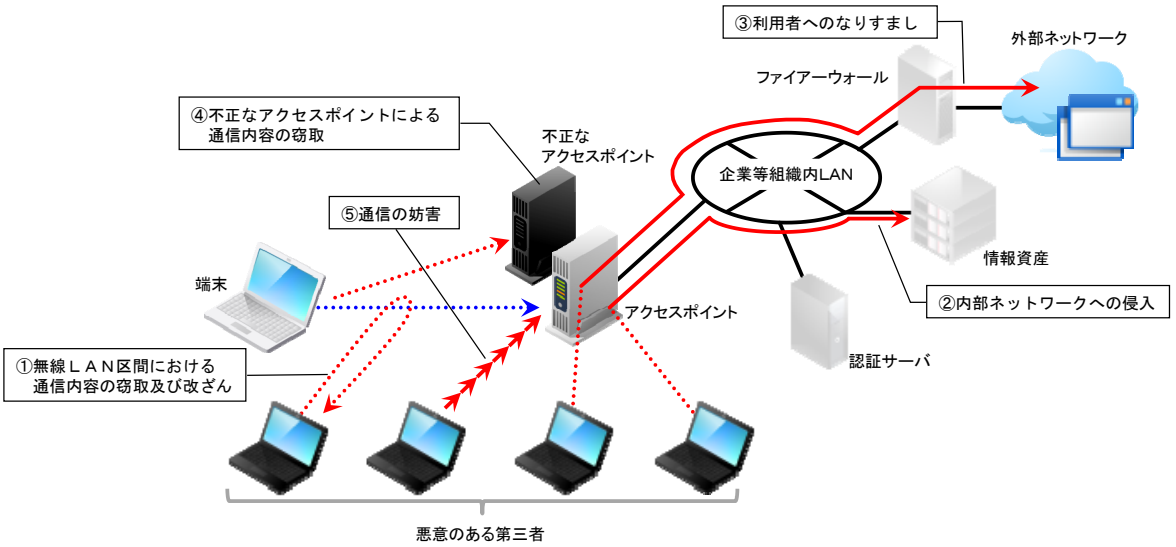

図２　情報セキュリティ上の主な脅威

① 無線ＬＡＮ区間における通信内容の窃取及び改ざん

悪意のある第三者により無線ＬＡＮ区間の通信を傍受され、通信内容が窃取及び改ざんされるおそれがある。

② 内部ネットワークへの侵入

悪意のある第三者に無線ＬＡＮに不正に接続されることによって、内部の情報資産が窃取、改ざん及び破壊されるおそれがある。

③ 利用者へのなりすまし

悪意のある第三者に無線ＬＡＮのアクセスポイントに不正に接続されることによって、当該無線ＬＡＮの正当な利用者になりすましてインターネット等外部のネットワークに接続されるおそれがある。

④ 不正なアクセスポイントによる通信内容の窃取

悪意のある第三者により不正なアクセスポイントが設置され、当該アクセスポイントを正規のアクセスポイントと誤認させられた利用者の端末が接続することで、通信内容が窃取されるおそれがある。

⑤ 通信の妨害

悪意のある第三者によって、大量のパケット等が送信されることによるＤｏＳ（Denial of Service）攻撃、不正な電波発生源が設置されることによる電波干渉等により、通信速度が低下し又は通信が不可能となるおそれがある。

第２章　無線ＬＡＮの技術面及び管理面における情報セキュリティ対策

無線ＬＡＮの情報セキュリティ対策としては、大別して、暗号化等技術面の対策及び機能制限等管理面の対策がある。これらの対策を重層的に取ることにより、無線ＬＡＮの運用において必要な情報セキュリティを確保することが可能となる。

表２ 技術面及び管理面における対策

想定される脅威	脅威への情報セキュリティ対策	
無線ＬＡＮ区間における通信内容の窃取及び改ざん	◎	ＷＰＡ／ＷＰＡ２（ＣＣＭＰ）の採用と適切な設定 ※ ＴＫＩＰにのみ対応している機器を運用中の場合は、当面の間ＴＫＩＰを使用することに差し支えはないと考えられる。
	◎	アクセスポイントの管理者パスワードの適切な設定
内部ネットワークへの侵入	◎	ＷＰＡ／ＷＰＡ２－ＥＡＰの採用と適切な設定 ※ ＰＳＫ認証を選択する場合は、ＰＳＫ認証のぜい弱性のほか、無線ＬＡＮに接続する端末の数が増えるとパスフレーズの設定、更新等の管理・運用が煩雑になることを認識する必要がある。
	◎	アクセスポイントの管理者パスワードの適切な設定
	○	電波の伝搬範囲の適切な設定 ※ 情報セキュリティ上の脅威に対する直接的な対策ではないが、電波の伝搬範囲を必要最低限とすることで、アクセスポイントの存在を悪意ある第三者に知らしめる危険性等を低減する効果が期待される。なお、電波の伝搬範囲は、アクセスポイントの設置箇所周辺の状況等の影響を受けるため、一定ではないことを注意する必要がある。
	○	ログの収集・保存
	△	無線ＩＤＳ／ＩＰＳの導入
利用者へのなりすまし	◎	ＷＰＡ／ＷＰＡ２－ＥＡＰの採用と適切な設定 ※ ＰＳＫ認証を選択する場合は、ＰＳＫ認証のぜい弱性のほか、無線ＬＡＮに接続する端末の数が増えるとパスフレーズの設定、更新等の管理・運用が煩雑になることを認識する必要がある。
	◎	アクセスポイントの管理者パスワードの適切な設定
	○	電波の伝搬範囲の適切な設定 ※ 情報セキュリティ上の脅威に対する直接的な対策ではないが、電波の伝搬範囲を必要最低限とすることで、アクセスポイントの存在を悪意ある第三者に知らしめる危険性等を低減する効果が期待される。なお、電波の伝搬範囲は、アクセスポイントの設置箇所周辺の状況等の影響を受けるため、一定ではないことを注意する必要がある。
	○	ログの収集・保存
	△	無線ＩＤＳ／ＩＰＳの導入
不正なアクセスポイントの設置による通信内容の窃取	◎	ＷＰＡ／ＷＰＡ２－ＥＡＰの採用及び適切な設定
	△	電波状況の監視
	△	無線ＩＤＳ／ＩＰＳの導入
通信の妨害	○	ログの収集・保存
	△	管理フレームの暗号化・改ざん検知（ＩＥＥＥ802.11w）
	△	電波状況の監視
	△	無線ＩＤＳ／ＩＰＳの導入

◎：必須対策

○：追加的に実施することが有効な対策

△：情報セキュリティ対策をより強固にしたい場合に検討する対策

本章において、これらの対策を以下で解説する。

2.1 技術面の対策

(1) 接続に関する認証及び通信内容の暗号化

無線ＬＡＮの有効な情報セキュリティの方式として、Wi-Fi Alliance[2]により規格化されているＷＰＡ（Wi-Fi Protected Access）及びＷＰＡ２[3]がある。

ＷＰＡ及びＷＰＡ２は、端末とアクセスポイントとの接続に関する認証方式及び通信内容の暗号化方式を包含した規格であり、認証により利用権限のない端末の接続を防止するとともに、暗号化により通信内容の窃取及び改ざんを防止する。認証方式及び暗号化方式には、それぞれ複数の方式が存在しており、適宜組み合わせて使用する。

なお、ＷＰＡ２は、アクセスポイントから別のアクセスポイントへのローミングを迅速に行うことが可能など高度な機能を有しているが、同一の暗号化方式を採用していた場合、情報セキュリティの観点からはＷＰＡと同等である。ただし、ＷＰＡ２は、より強力な暗号化方式を標準としている。

その他の情報セキュリティ規格として、ＩＥＥＥ802.11により規格化されたＷＥＰ（Wired Equivalent Privacy）があるが、現在では様々なぜい弱性が明らかになっており、容易に暗号が解読されるおそれがあるなど情報セキュリティ対策としての有効性を既に失っていることから、本手引書では有効な情報セキュリティ対策として取り扱わないこととする。

ア 接続に関する認証

端末及びアクセスポイント双方、又は一方を認証する方式として、ＰＳＫ（Pre-Shared Key）認証及びＩＥＥＥ802.1X認証の２つの規格がある。

ただし、いずれの認証も端末及びアクセスポイントの機器の認証であり、利用者の本人性を認証するものではないことを十分に認識すべきである。本人性の確認については、別途、ＩＤ及びパスワード等による認証が必要となるが、無線ＬＡＮ特有の問題ではないことから、本手引書では取り扱わないこととする。

◇ ＰＳＫ認証

ＰＳＫ認証は、端末及びアクセスポイントにおいて事前に設定・共有される共通の鍵であるＰＳＫ（パスフレーズ）により、端末及びアクセスポイントを相互に認証する方式[4]である。具体的には、図３に示すとおり、端末及びアクセスポイント双方において、パスフレーズから暗号化鍵を生成し、その一致をもって端末及びアクセスポイントが正当であると認証する。認証サーバが不要なため採用が比較的容易であることから、小規模な組織で利用されている認証方式である。

ＰＳＫ認証は、同一のアクセスポイントに接続する端末では、共通のパスフレーズを設定する必要があることから、パスフレーズが外部に漏えいする危険性がある。また、総当たり攻撃（Brute Force Attack）[5]等により、パスフレーズを窃取される危険性もある。

そのため、ＰＳＫ認証の利用の際には、定期的なパスフレーズの更新が必須となる。万一、パスフレーズが漏えいした場合、パスフレーズを保存した端末を紛失したことが明らかになった場合等には、速やかに全ての端末及びアクセスポイントのパスフレーズを更新する必要がある。

---

[2] 無線ＬＡＮの普及促進を目的として設立された業界団体。

[3] 無線ＬＡＮの情報セキュリティの規格は、ＩＥＥＥ802.11iにおいて標準化されている。ＷＰＡは、無線ＬＡＮのぜい弱性に早急に対処するため、ＩＥＥＥ802.11iにおける標準化を待たずに、採用が予定されている一部の機能がWi-Fi Allianceにおいて規格化されたものである。ＷＰＡ２は、2004年に正式に標準化されたＩＥＥＥ802.11iに準拠する形で、Wi-Fi Allianceにおいて規格化されたものである。

[4] 端末、アクセスポイントの設定項目等では、「ＷＰＡ／ＷＰＡ２－ＰＳＫ」、「ＷＰＡ／ＷＰＡ２－Personal」等と表記される。

[5] 考えられる全ての組合せを入力して試す攻撃手法。また、全ての組合せではなく、識別符号として使用される頻度の高い文字列（これを集約したものを比喩的に「辞書」と呼ぶ。）を入力して認証を試行する「辞書攻撃」も存在する。

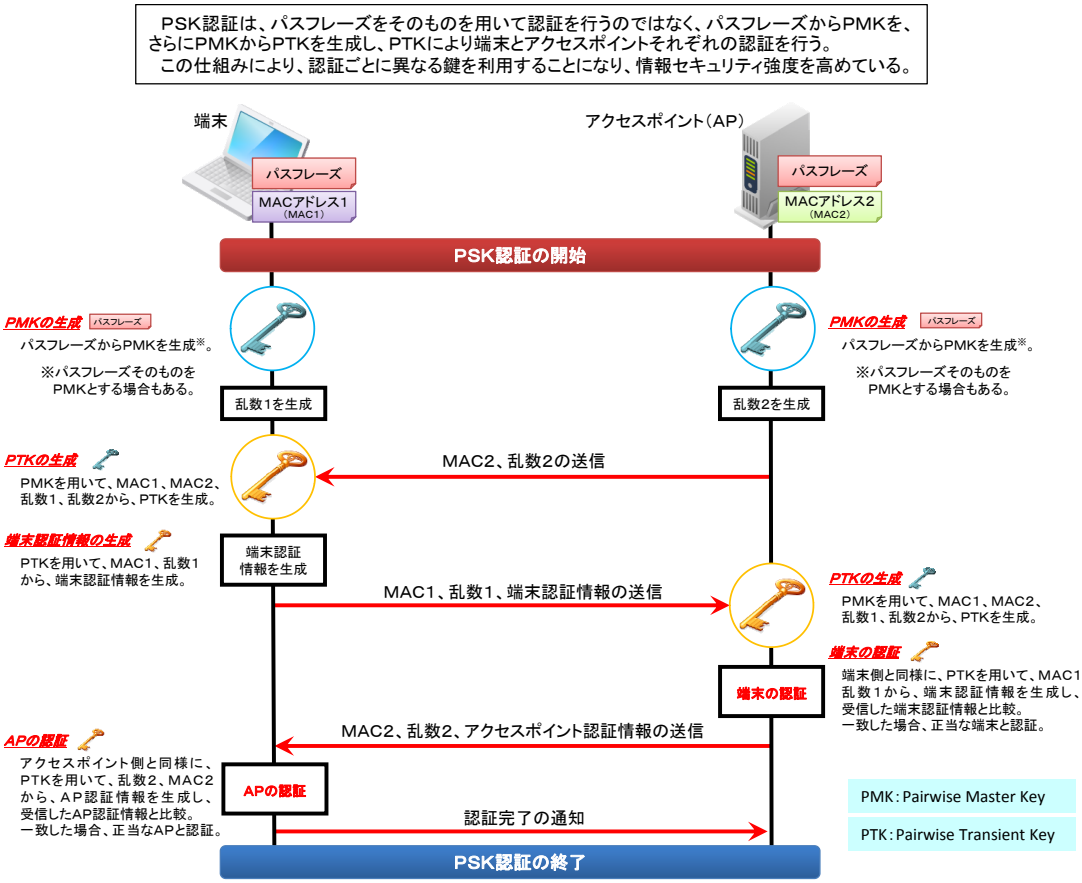

図３　ＰＳＫ認証の仕組み

◇　ＩＥＥＥ802.1X 認証

ＩＥＥＥ802.1X 認証は、有線でも用いられるネットワーク認証の規格であるＰＰＰ（Point to Point Protocol）を拡張したプロトコルであるＥＡＰ（イーエーピー）（Extensible Authentication Protocol）[6]を採用しており、パスワード、電子証明書[7]等により端末及びアクセスポイント双方、又は端末を認証する方式[8]である。

ＩＥＥＥ802.1X 認証は、一般に、端末に搭載された認証用ソフトウェア、ＩＥＥＥ802.1X 認証に対応したアクセスポイント、ＲＡＤＩＵＳ（Remote Authentication Dial-In User Service）サーバ等の３つの要素により構成される。ＲＡＤＩＵＳサーバにおいて一元的に認証が行われるため、端末及びアクセスポイントの増加に対応可能であることから、大規模な組織における運用にも耐えうる認証方式である。

[6] ＥＡＰの仕様は、インターネットの技術仕様を策定するＩＥＴＦ(Internet Engineering Task Force)において、ＲＦＣ(Request for Comments) 3748 として規格化されている。
[7] 通信先の本人性を確認する電子的な証明書のこと。
[8] 端末、アクセスポイントの設定項目等では、「ＷＰＡ／ＷＰＡ２－ＥＡＰ」、「ＷＰＡ／ＷＰＡ２－Enterprise」等と表記される。

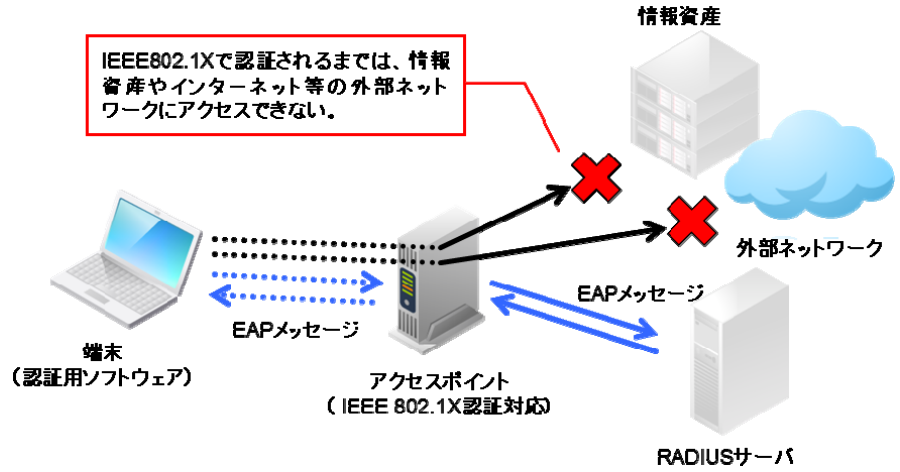

図４　ＩＥＥＥ802.1X 認証の仕組み

ＥＡＰの規格には、認証に用いる識別符号（ＩＤ及びパスワード、電子証明書等）、認証の方向（双方向・一方向）等の違いにより様々なものが存在しているおり、規格によって情報セキュリティの強度は一様でない。これらの規格の中には、ぜい弱性が明らかとなっているために、情報セキュリティ対策としての有効性を既に失っているものも存在する[9]。

現時点において、適切な情報セキュリティ強度を保つことができる代表的なＥＡＰの規格は次のとおりである。

▷ ＥＡＰ－ＴＬＳ（Transport Layer Security）

本規格は、端末及びサーバの相互認証であり、電子証明書により双方の認証を行う規格である。電子証明書を利用した相互認証であるため、情報セキュリティの強度が高い。

▷ ＰＥＡＰ（Protected ＥＡＰ）

本規格は、端末及びサーバの相互認証であり、ＩＤ及びパスワードにより端末の認証、電子証明書によりサーバの認証を行う規格である。

端末の認証は、ＩＤ及びパスワードにより行うが、各端末で一定時間ごとにパスワードから生成する認証情報を更新するため、情報セキュリティが強化されている。また、本規格では端末側に電子証明書が不要であるため、ＥＡＰ－ＴＬＳよりも、管理・運用は容易である。

▷ ＥＡＰ－ＦＡＳＴ（Flexible Authentication via Secure Tunneling）

本規格は、端末及びサーバの双方の相互認証であり、ＩＤ及びパスワードにより双方の認証を行う規格である。

ＰＡＣ（Protected Authentication Credential）と呼ばれる鍵を用いて、認証のための専用の通信経路を確立し、安全な当該経路でＩＤ・パスワードにより認証を行う。

▷ ＥＡＰ－ＳＩＭ（Subscriber Identity Module）／ＥＡＰ－ＡＫＡ（UMTS Authentication and Key Agreement）

本規格は、端末及びサーバの相互認証であり、ＥＡＰ－ＳＩＭとＥＡＰ－ＡＫＡとでは一部手順が異なるが、ともに携帯電話のＳＩＭカード[10]により双方の認証を行う規格である。

ＳＩＭカードに格納されている携帯電話事業者のみ知り得る情報から認証情報を生成するため、情報セキュリティ強度は高くなる。

[9] 例えば、ＥＡＰ－ＭＤ５及びＬＥＡＰが有名であるが、これらの方式はぜい弱性が明らかとなっており、使用することは適当ではない。

[10] ＳＩＭ（Subscriber Identity Module）カードとは、携帯電話事業者が発行する携帯電話向け利用者識別用のＩＣカードであり、利用者の電話番号、識別番号等の情報が記録されている。

表３　ＥＡＰの規格の比較

	EAP-TLS	PEAP	EAP-FAST	EAP-SIM EAP-AKA	LEAP	EAP-MD5
情報セキュリティ強度	◎	○	○	◎	×	×
端末の認証	電子 証明書	ID・ パスワード	PAC、ID・ パスワード	SIM	ID・ パスワード	ID・ パスワード
サーバの認証	電子 証明書	電子 証明書	PAC	SIM	－	×
相互認証	○	○	○	○	○	×

以上のように、ＰＳＫ認証及びＩＥＥＥ802.1X 認証は、それぞれ特徴を有しており、構築する無線ＬＡＮの規模、採用や運用に必要なコスト等を勘案して認証方式を決定することが適当である。

イ 通信内容の暗号化

端末とアクセスポイントとの間の通信を暗号化するとともに改ざんを検知する方式として、ＴＫＩＰ（Temporal Key Integrity Protocol）及びＣＣＭＰ（Counter Mode with Cipher Block Chaining MAC Protocol）[11]の２つの規格[12]がある。

ＴＫＩＰについては、特殊な条件下において通信の改ざんが可能であることが報告[13]されているため、ＣＣＭＰを利用することが適当である。ただし、現にＴＫＩＰにのみ対応している機器を運用中の場合に、直ちにＣＣＭＰ対応の機器に改修する必要があるほどの脅威がＴＫＩＰに確認されているわけではないことから、他の対策を重層的に取ることにより、当面の間ＴＫＩＰを使用することに差し支えはないと考えられる[14]。

(2) 管理フレームの暗号化・改ざん検知

無線ＬＡＮの管理フレーム[15]を暗号化し、改ざんを検知する規格として、ＩＥＥＥ802.11w がある。ＴＫＩＰ又はＣＣＭＰによる暗号化はいずれもデータフレーム[16]のみに関するものであり、管理フレームを暗号化・改ざん検知するためにはＩＥＥＥ802.11w を適用する必要がある。

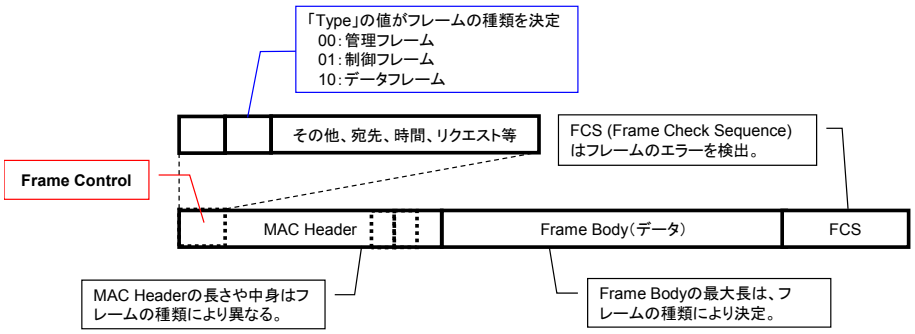

図５ 無線ＬＡＮのフレームの構造

[11] ＣＣＭＰは、暗号アルゴリズムとして米国政府標準暗号であるＡＥＳ（Advanced Encryption Standard）を採用しているため、端末、アクセスポイントの設定項目等では「ＡＥＳ」と表記されることもある。

[12] ＷＰＡでは、ＴＫＩＰを標準、ＣＣＭＰをオプションの規格としている。また、ＷＰＡ２ではＣＣＭＰを標準、ＴＫＩＰをオプションの規格としている。一部の機種では標準の規格のみの対応となっている場合がある。

[13] Martin Beck, Erik Tews, "Practical attacks against WEP and WPA", 2008. 等

[14] 産業技術総合研究所「無線ＬＡＮのセキュリティに係わる脆弱性の報告に関する解説」（http://www.rcis.aist.go.jp/TR/2009-01/）においては、暗号化の鍵の更新間隔を 120 秒程度の値に設定することなどが推奨されている。

[15] 無線ＬＡＮのアクセスポイントの検出、無線ＬＡＮへの接続及び離脱、認証及び認証の解除等を行うための情報が格納されている。

[16] 通信の相手先に送付する情報が格納されている。

端末とアクセスポイントの接続及び遮断は、管理フレームにより実現されている。そのため、悪意のある第三者によって、利用者の端末の接続を遮断する管理フレームが送信されたとしても、端末側では当該管理フレームが偽装されたものであると判断することができずに正当なものとして扱うため、アクセスポイントとの接続を切断することになる。このような偽装した管理フレームを繰り返し送信することにより、ＤｏＳ攻撃が可能となる。

そこで、ＩＥＥＥ802.11w を活用することにより、管理フレームの正当性を判断できるようになり、この種のDoS攻撃によって無線ＬＡＮの接続が遮断されることを防ぐことができる[17]。

(3) 利用者の属性等に応じた無線ＬＡＮのネットワーク分割

利用者の属性ごとに無線ＬＡＮから利用できる情報資産を制限するため、ＶＬＡＮ(Virtual Local Area Network)等の機能を用いて、ネットワークを仮想的に分割する。

例えば、マルチＳＳＩＤ機能[18]を備えたアクセスポイントを利用し、システムへのフルアクセスを許可されている社員用のＳＳＩＤ、一般社員用のＳＳＩＤ等、情報資産の利用権限ごとに異なるＳＳＩＤを設定し、ＳＳＩＤごとにＶＬＡＮを設定することでネットワークを分割する。

なお、無線ＬＡＮと有線ＬＡＮとの境界にファイアウォールを設置するなどして両者を分離し、無線ＬＡＮから有線ＬＡＮ内のシステムへのアクセスを制御することも考えられる。

(4) 無線ＩＤＳ／ＩＰＳ（侵入検知／防止システム）

無線ＩＤＳ（Intrusion Detection System）の設置により無線ＬＡＮのトラヒックを監視し、ＤｏＳ攻撃等の不審な通信を検知する。

無線ＩＤＳは、一般に端末及びアクセスポイントの情報を収集しリスト化する機能、許可なく設置及び接続されたアクセスポイント並びに許可されていない端末を検知する機能、攻撃が疑われる活動を検知して警告を出す機能等を備えている。複数のＩＤＳセンサで受信した電波強度をもとに三角測量の原理で、これらの端末及びアクセスポイントの位置を特定する機能を有する場合もある。

検知だけではなく、通信の遮断等により攻撃を防止する機能を有する機器は、ＩＰＳ（Intrusion Prevention System）と呼ばれる。

2.2 管理面の対策

(1) 電波の伝搬範囲の適切な設定

情報セキュリティ上の脅威に対する直接的な対策ではないが、通信の傍受、無線ＬＡＮへの侵入、電波干渉による通信速度低下等の危険性を低減するため、アクセスポイントの電波の伝搬範囲を制限する。具体的には、次のような対策が考えられる。

－ 窓、外壁付近等にアクセスポイントを設置しない。
－ アクセスポイントの電波出力を調整する。
－ アクセスポイントのアンテナとして指向性を有するものを使用する。
－ 無線ＬＡＮの利用区画と非利用区画の間に電波遮蔽シート等を使用する。

なお、電波の伝搬範囲は、アクセスポイントの設置箇所周辺の状況等の影響を受けるため、一定ではないことを注意する必要がある。

(2) アクセスポイントの管理者パスワードの適切な設定

無線ＬＡＮの情報セキュリティ対策において重要な役割を担うアクセスポイントの情報セキュリティ設定について、設定権限のない者により変更されることを避けるために、アクセス

[17] 端末とアクセスポイントの接続が確立する前に、送受信される管理フレームを暗号化することはできないため、接続及び認証を要求する管理フレームを数多く送信するＤｏＳ攻撃を防ぐことはできない。
[18] 複数のＳＳＩＤを設定する機能。認証方式及び暗号化方式は、SSID ごとに設定可能である。

ポイントの管理者用パスワードを適切に設定する。
　初期設定のパスワードは、当該機器のベンダにより共通などよく知られていることがあるため、パスワードには大文字、小文字、数字及び記号を組み合わせ、なるべくランダムで文字数の長いものに設定する必要がある。また、管理者用パスワードは定期的に更新することが適当である。
　なお、複数のアクセスポイントの管理を可能とするアクセスポイントコントローラを利用することにより、管理者パスワードの設定等の管理を容易に行うことが可能である。

(3) ログの収集・保存

　一般にアクセスポイント及び認証サーバは、ログを収集・保存する機能を有している。本機能を利用して、アクセスポイント及び認証サーバに接続及び接続を試みた端末の情報、エラー情報等をログとして収集・保存する。取得したログを定常的に分析することにより、不正な通信、攻撃等が疑われる通信等を早期に検知し、情報漏えい等の被害を防止することが可能となる。また、攻撃等を受けた場合の追跡、攻撃手法の解析等も期待できる。
　なお、取得したログを他のサーバ等に転送する機能を備えている場合には、複数のアクセスポイント及び認証サーバのログの集中的な管理及び長期間にわたる収集・保存が可能となる、横断的かつ時系列の分析が可能である。

(4) 電波状況の監視

　アクセスポイントの電波状況を定期的に監視し、許可なく設置されたアクセスポイント及び不正なアクセスポイントを検知する。
　無線ＬＡＮの通信機能を備えたパソコンに、無線ＬＡＮの電波状況を確認するソフトウェアをインストールすることにより、周囲のアクセスポイントのＳＳＩＤ、ＭＡＣアドレス、電波強度等の電波状況を確認する。ただし、ＳＳＩＤ及びＭＡＣアドレスは偽装することが可能であることを留意する必要がある。

(5) アドホックモードの利用の制限

　アクセスポイントを介すことなく端末同士が直接通信するアドホックモード[19]の利用を制限する。
　アドホックモードによる通信においては、無線ＬＡＮの情報セキュリティ対策に重要な役割を担うアクセスポイントが介在せず、適用できる情報セキュリティ対策が限定されることから、通信内容の窃取等の情報セキュリティ上の脅威が増大する。
　業務上アドホックモードを利用する特別な理由がない場合には、適切な情報セキュリティを確保するために、アドホックモードの利用を禁止することが適当である。

[19] ここでのアドホックモードはＩＢＳＳ(Independent Basic Service Set)と呼ばれ、端末同士がアクセスポイントを介さずに、直接通信する形態をいう。端末同士を直接する形態として、アドホックモードの他に、Wi-Fi Alliance が策定した仕様 Wi-Fi Direct に基づくものがある。Wi-Fi Direct ではＷＰＡ２が利用できるなどアドホックモードよりも情報セキュリティが高い。アクセスポイントを介さずに直接通信する場合には、Wi-Fi Direct を利用することが望ましい。

第３章　無線ＬＡＮの導入・運用の各段階において実施すべき事項

企業等の組織において無線ＬＡＮを導入・運用するに当たっては、情報セキュリティ上の脅威に備え、「準備」、「構築」、「運用」及び「廃棄」の各段階において、それぞれ第２章で解説した情報セキュリティ対策や方式の検討等を実施する必要がある。

また、企業等の組織において、無線ＬＡＮの情報セキュリティ対策を有効に機能させるためには、技術面や管理面の対策を取ることに加え、企業等が定めた無線ＬＡＮ利用に関する方針を、当該組織の利用者に遵守させる必要がある。そのために、利用者に対する教育を実施することが適当である。利用者への教育においては、無線ＬＡＮを利用する上で想定される情報セキュリティ上の脅威、情報セキュリティ対策の必要性、企業等が定める無線ＬＡＮの運用ルール等について説明を行うことが考えられる。

本章では以下において、無線ＬＡＮの導入に向けた準備や構築、無線ＬＡＮの運用及び廃棄の各段階における対策をそれぞれ示す。

3.1 準備段階において実施すべき事項

① 無線ＬＡＮからの利用を許可する情報資産の設定

無線ＬＡＮは、ネットワークの構築及び変更が容易、端末の自由な移動が可能、有線の接続口がないタブレット等の端末が接続可能等の利点がある。一方、利用に際して適切な情報セキュリティ対策がなされていない場合、有線と比較して情報セキュリティ上の脅威が増大するなどの欠点もある[20]。

無線ＬＡＮを利用するに当たっては、利点及び欠点を比較衡量した上で、無線ＬＡＮの利用を許可する者の範囲（一部の利用者のみに限定するか、全利用者に提供するかなど）を設定する。

また、利用者の属性（利用者グループ）ごとに、どこまでの情報資産の利用を許可するか定める必要がある。例えば、外出用の端末に対してインターネット接続は許可するが社内のデータベース等へのアクセスは許可しないなどの方針を定めた上で、これを実現するための情報セキュリティ対策を検討する必要がある。

あわせて、利用者グループ等に応じて、無線ＬＡＮの利用を許可する場所について検討する必要がある。

② 無線ＬＡＮの情報セキュリティ対策の検討

利用者グループ及び利用する情報資産の範囲の特性に応じて、無線ＬＡＮに採用する認証方法、暗号化方式等を含めた情報セキュリティ対策を検討する。

一般に、情報セキュリティ対策と利用者の利便性とは相反する要素と捉えられることがあるが、二者択一の発想ではなく、利便性を維持しながら、無線ＬＡＮを利用する業務の特性に応じて、どのような情報セキュリティ対策を講ずべきかという視点で検討することが重要である。

暗号化方式には、ＷＥＰ、ＴＫＩＰ及びＣＣＭＰの３つの規格がある。ＷＥＰは様々なぜい弱性を有しており、採用するべきではない。また、ＴＫＩＰも特殊な条件下においてはぜい弱性が報告されていることから、新たに無線ＬＡＮを導入する際には、ＣＣＭＰを利用することが適当である。

認証方式には、ＰＳＫ認証及びＩＥＥＥ802.1X 認証がある。ＰＳＫ認証では認証サーバが必要ないなど採用は容易であるが、同一のアクセスポイントに接続する端末では共通のパスフレーズを設定するため、パスフレーズが漏えいした場合には、なりすまして接続される危険性がある。また、パスフレーズを個々の端末に自動的に配布する仕組みがないため、接続する端末の数が増えると、パスフレーズの設定、更新等の管理及び運用が煩雑になる。ＩＥＥＥ802.1X 認証では認証サーバが必要となるが、端末を認証してからネットワークへの接続を許可するた

[21] ＰＳＫ認証を選択する場合は、ＰＳＫ認証のぜい弱性のほか、無線ＬＡＮに接続する端末の数が増えるとパスフレーズの設定、更新等の管理・運用が煩雑になることを認識する必要がある。

め、許可されていない端末が無線ＬＡＮに接続されることを防ぐことができる。無線ＬＡＮを利用する端末の数、業務の特性等に応じて認証方式を検討する必要があるが、基本的には、端末認証が行えるＩＥＥＥ802.1X 認証を利用することが適当である[21]。

その他、業務の特性等に応じて、ＶＬＡＮ等による無線ＬＡＮのネットワーク分割、パケットフィルタリングによるアクセス制御、無線ＩＤＳ／ＩＰＳシステムの導入等の必要性について、利用者の利便性、導入・運用コスト等も考慮しながら検討する必要がある。

③ 無線ＬＡＮの利用を許可する端末の登録

無線ＬＡＮの利用を許可されていない端末の検出を容易にするために、無線ＬＡＮの利用を許可する端末をリストに登録する。

④ 電波の伝搬範囲の設定

情報セキュリティ上の脅威に関する直接的な対策ではないが、通信の傍受、無線ＬＡＮへの侵入、電波干渉による通信速度低下等の危険性を低減するため、無線ＬＡＮを利用できる場所として設定した範囲を超えて電波が漏出しないよう、電波の伝搬範囲を限定する。

電波の伝搬範囲を限定するためには、窓側及び外壁付近を避け、なるべく中央にアクセスポイントを設置するなどの工夫を行うことが考えられる。また、より積極的な対策として、指向性のあるアンテナの利用、アンテナの向きの調整、電波出力の調整、電波遮蔽シートの使用等も有効である。

⑤ 無線ＬＡＮの運用ルールの策定

無線ＬＡＮを安全に利用するために必要な運用ルールを設定する。例えば、情報セキュリティ対策が適切に行われていないアクセスポイントが、利用者によって設置されると、当該アクセスポイントを通じて内部ネットワークへ侵入される危険性が高まるため、許可なくアクセスポイントを設置してはならないなどのルールを定めることが考えられる。

また、複数の通信インタフェースを備える端末に対し、無線ＬＡＮと有線ＬＡＮの同時接続を許可すると、無線ＬＡＮ側から端末を経由して有線ＬＡＮ内のシステムに接続される危険性がある。そのため、無線ＬＡＮと有線ＬＡＮとの同時接続を禁止することが適当である。

さらに、業務上利用する特別な理由がない場合には、適用できる情報セキュリティ対策が限られているアドホックモードの利用を禁止することが適当である。

その他、アクセスポイントの管理者パスワード、ＰＳＫ認証におけるパスフレーズ、ＩＥＥＥ802.1X 認証におけるＰＥＡＰのパスワードの更新ルール等、必要に応じて無線ＬＡＮの運用ルールを定め、社員に対して周知する必要がある。

なお、本手引書の対象外ではあるが、社外の無線ＬＡＮを利用して社内システムにリモートアクセスする時には、ＶＰＮを利用するなどのルールを定めることが考えられる。その際、社内システムにＶＰＮ接続している端末においてテザリング機能が利用可能な場合には、テザリング機能を通じて許可されていない端末が社内システムにアクセスできる可能性があるため、特別な理由がない場合には、ＶＰＮ接続時にはテザリング機能の利用を禁止するなどのルールを定めることが適当である。

3.2 構築段階において実施すべき事項

① パスワード等の適切な設定

アクセスポイントの管理者パスワード、ＰＳＫ認証におけるパスフレーズ、ＩＥＥＥ802.1X 認証におけるＰＥＡＰのパスワード等を適切に設定する。

総当たり攻撃等により、パスワード等が容易に推測されることのないよう、パスワード等は

[21] ＰＳＫ認証を選択する場合は、ＰＳＫ認証のぜい弱性のほか、無線ＬＡＮに接続する端末の数が増えるとパスフレーズの設定、更新等の管理・運用が煩雑になることを認識する必要がある。

大文字、小文字、数字及び記号を組み合わせ、なるべくランダムで文字数の長いものにする必要がある[22]。

② アクセスポイントの情報セキュリティの設定

無線ＬＡＮの情報セキュリティ対策において重要な役割を担うアクセスポイントについて、導入段階の検討及びその後の見直し状況に基づき、認証方式、暗号化方式等を適切に設定する。

認証方式として、ＩＥＥＥ802.1X 認証を採用した場合には、アクセスポイントだけではなく認証サーバを構築・設定する必要がある。

複数のＳＳＩＤを設定する機能を備えたアクセスポイントでは、ＳＳＩＤごとの認証方式、暗号化方式等の設定、ＶＬＡＮの設定による論理的なネットワークの分割も可能である。

無線ＬＡＮを通じて利用できる情報資産が異なる利用者グループ等を設定する場合は、利用者グループに応じたＳＳＩＤ、認証方式、暗号化方式、ＶＬＡＮ、パケットフィルタリング等の設定を行うことが必要となる。

③ 設置したアクセスポイントの管理

許可なく設置されたアクセスポイントや不正なアクセスポイントの検出するため、社内への設置を許可したアクセスポイントをリストに登録する。

④ ログの収集・保存

情報セキュリティ上の脅威の早期の検出及び迅速な対応を可能とするため、アクセスポイント及び認証サーバのログを収集・保存する。

ログの収集・保存に当たっては、情報セキュリティ上の脅威の発生した際に横断的かつ時系列的に詳細に分析するために、複数のアクセスポイント、認証サーバ等のログを集中して管理することが適当である。なお、ログを正確に分析するためには、アクセスポイント、認証サーバ、その他ルータ等のネットワーク機器について時刻を同期[23]しておく必要がある。

3.3 運用段階において実施すべき事項

① パスワード等の定期的な更新

アクセスポイントの管理パスワード、ＰＳＫ認証におけるパスフレーズ、ＩＥＥＥ802.1X 認証におけるＰＥＡＰのパスワード等を定期的に更新する。

ＰＳＫ認証の利用において、パスフレーズ等を保存した端末の紛失及び盗難があった場合、パスフレーズが漏えいした可能性がある場合等には、速やかにパスフレーズを変更する必要がある。

なお、本手引書の対象外ではあるが、組織の構成員以外のための無線ＬＡＮを設置し、利用の際にパスフレーズを発行している場合等においては、運用性等を含めて総合的に安全性を考慮した上で、パスワード等の更新を行うことが望ましい。

②アクセスポイント情報の更新

不正なアクセスポイントか識別できるようにするため、組織内への設置が許可されたアクセスポイントのリストを作成し、増設、更新、廃棄等にあわせてリストを更新する。

---

[22] 推奨されるパスフレーズの長さについては、文献により異なるが、無線ＬＡＮの企画書（IEEE Std 802.11 TM_2012 には、「A key generated from a passphrase of less than about 20 characters is unlikely to deter attacks.」と記載されており、おおよそ 20 文字以上を推奨している。

[23] 独立行政法人情報通信研究機構が提供する ntp.nict.jp 等の NTP（Network Time Protocol）サーバに接続することにより、時刻同期が可能となる。

③ 不許可又は不正なアクセスポイント等の設置状況の監視

通信内容の窃取等の行為を惹起するセキュリティホール[24]となる不許可のアクセスポイント、不正なアクセスポイント等の設置を防ぐため、電波状況を定常的に監視し、これらのアクセスポイントが設置されていないことを確認することが望ましい。

④ ログの確認

情報セキュリティ上の脅威を早期に検出し、迅速に対応するため、アクセスポイント及び認証サーバのログを確認する。

3.4 廃棄段階において実施すべき事項

① 無線ＬＡＮの設定情報の消去

ＰＳＫ認証方式でのパスフレーズ、アクセスポイントの管理パスワード等を窃取されることを防ぐためにこれらの情報セキュリティに関連する設定情報等を、設定の初期化、専用のソフトウェアの利用等により完全に消去する。

[24] 情報セキュリティ上の脅威の発生の端緒となるぜい弱性等のことを指す。

第４章　無線ＬＡＮを適切に運用しないと生じる危険性の具体例及び解決策

無線ＬＡＮを、情報セキュリティ対策を取らず利用すると、通信内容の窃取や無断で無線ＬＡＮのアクセスポイントが悪用されるなどの危険性がある。以下において、こうした危険性について想定される事例を交えて解説するとともに、それぞれの原因とその解決策について説明する。

4.1 無線ＬＡＮ区間における通信内容の窃取及び改ざん

＜事　例＞

無線ＬＡＮを早くから導入していたＡ社は、導入当時に暗号化方式として主流であったＷＥＰを採用して使っていた。

ある新商品を社内で極秘に開発していたところ、その写真がインターネット上に掲載されていることが判明した。社内サーバへの外部からのアクセスは確認されず、無線ＬＡＮ区間において通信内容が窃取されてしまったようである。

＜原　因＞

Ａ社では、ＷＥＰのぜい弱性が明らかになった後も、長年にわたり無線ＬＡＮの改修を行わずに使用し続けていたため、端末とアクセスポイントの間の通信を傍受され、その内容が窃取されてしまった。

＜解決策＞

このような事例の発生を防ぐためには、ＷＰＡ／ＷＰＡ２（ＣＣＭＰ）を利用して通信内容を暗号化する必要がある。

4.2 内部ネットワークへの侵入

＜事　例＞

ＷＥＰのぜい弱性を認識していたＢ社では、ＷＰＡ２（ＣＣＭＰ）対応機器を購入し、初期設定のまま無線ＬＡＮを運用していた。

その後、社内システムに保存してある顧客データベースについて、度重なるアクセスの後、破壊されていることが判明した。無線ＬＡＮ経由で社内システムに接続した第三者が、顧客データベースの情報を盗んだ上で、データベースを破壊したようである。

＜原　因＞

Ｂ社では、暗号化方式として、ＷＰＡ２（ＣＣＭＰ）を採用してはいたが、認証方式としてＷＰＡ２－ＰＳＫを採用し、ＰＳＫのパスフレーズ及びアクセスポイントの管理者用パスワードが初期設定のままであったため、第三者に当該パスフレーズ及びパスワードが推測され、誰でも接続できるようアクセスポイントの設定が変更された。これにより、当該の攻撃者のみならず、複数の第三者が無線ＬＡＮへアクセス可能となり、内部のデータベースに侵入された。

＜解決策＞

このような事例の発生を防ぐためには、認証方式及び暗号化方式の設定等の情報セキュリティ対策の要となるアクセスポイントについて、ＰＳＫのパスフレーズ及び管理者パスワードを適切に設定・更新することが必要である。

4.3 利用者へのなりすまし

＜事　例＞

Ｃ社では、アクセスポイントにＷＰＡ２（ＣＣＭＰ）を採用するなど内部システムへの侵入に様々な対策を取っていたが、アクセスポイントにおいてログを収集していなかった。また、社内のあらゆるところで無線ＬＡＮを利用できるように、アクセスポイントの電波出力を最大に設定していた。

ある日、社外のあるウェブサイトの管理者から、Ｃ社のＬＡＮ管理者宛に連絡があり、当該ウェブサイトに対してＣ社から大量のアクセスがあることが判明した。

＜原　因＞

社員の不注意によってＣ社のアクセスポイントの認証情報が流出したことにより、Ｃ社に隣接するオフィス付近からアクセスポイントが不正に利用され、そこから外部のウェブサイトへの大量アクセスが行われていた。

＜解決策＞

このような事例の発生を防ぐためには、アクセスポイント及び認証サーバにおいてログを収集・保存し、不審な通信が行われていないかを確認するとともに、アクセスポイントの電波の伝搬範囲を制限することが有効である。

4.4 不正なアクセスポイントによる通信内容の窃取

＜事　例＞

Ｄ社の社員が、ノートパソコンを紛失したが、ハードディスクには機密情報を保存しないように心がけていたため、特段の処置を取らなかった。

後日、ＬＡＮ管理者が社内の電波状況をチェックしたところ、社内の無線ＬＡＮのアクセスポイントと同じＳＳＩＤと情報セキュリティ方式が設定されている別のアクセスポイントが、社外に設置されていることが判明した。

＜原　因＞

社員が紛失したノートパソコンには、社内のアクセスポイントのＳＳＩＤやＰＳＫ認証のパスフレーズが保存されていた。このノートパソコンを拾得した第三者が、ＳＳＩＤやＰＳＫ認証のパスフレーズを入手し、これらの情報を設定したアクセスポイントを、Ｄ社が入居しているビルの別の階に設置した。

なお、Ｄ社の社員が当該アクセスポイントを正規のものと誤認してアクセスし、情報が窃取されていたおそれもある。

＜解決策＞

このような事例の発生を防ぐためには、ＷＰＡ／ＷＰＡ２－ＥＡＰを採用し、接続先のサーバの認証を行うことが必要である。また、電波状況の監視を行うことが望ましい。