

**企業等が安心して
無線LANを導入・運用するために**

**総務省
平成25年1月30日**

目次

はじめに	1
第1章 企業等の組織における無線LANの運用及び脅威	2
1.1 本手引書が対象とする範囲	2
(1) 無線LANの運用形態	2
(2) 無線LANの規格	2
1.2 情報セキュリティ上の脅威	3
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	4
2.1 技術面の対策	5
(1) 接続に関する認証及び通信内容の暗号化	5
(2) 管理フレームの暗号化・改ざん検知	8
(3) 利用者の属性等に応じた無線LANのネットワーク分割	9
(4) 無線IDS/IIPS（侵入検知/防止システム）	9
2.2 管理面の対策	9
(1) 電波の伝搬範囲の適切な設定	9
(2) アクセスポイントの管理者パスワードの適切な設定	9
(3) ログの収集・保存・分析	10
(4) 電波状況の監視	10
(5) アドホックモードの利用の制限	10
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	11
3.1 準備段階において実施すべき事項	11
(1) 無線LANからの利用を許可する資産の設定	11
(2) 無線LANの情報セキュリティ対策の検討	12
(3) 無線LANの利用を許可する端末の登録	12
(4) 電波の伝搬範囲の設定	12
(5) 無線LANの運用ルールの策定	12
3.2 構築段階において実施すべき事項	13
(1) パスワード等の適切な設定	13
(2) アクセスポイントの情報セキュリティの設定	13
(3) 設置したアクセスポイントの管理	13
(4) ログの収集・保存設備の構築	13
3.3 運用段階において実施すべき事項	14
(1) パスワード等の定期的な更新	14
(2) アクセスポイント情報の更新	14
(3) 許可されていない又は不正なアクセスポイント等の設置状況の監視	14
(4) ログの収集・保存・分析	14
3.4 廃棄段階において実施すべき事項	14
(1) 無線LANの設定情報の消去	14
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	15
4.1 無線LAN区間における通信内容の窃取及び改ざん	15
4.2 内部ネットワークへの侵入	15
4.3 利用者へのなりすまし	15
4.4 不正なアクセスポイントによる通信内容の窃取	16

はじめに

無線LANは、スマートフォン等の対応機器の増加、公衆無線LANの整備、携帯電話網の逼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、実施すべき事項についても示した。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紹介した。

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 企業等の組織における無線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を企業等の組織の構成員のみが利用する形態を対象とする¹。

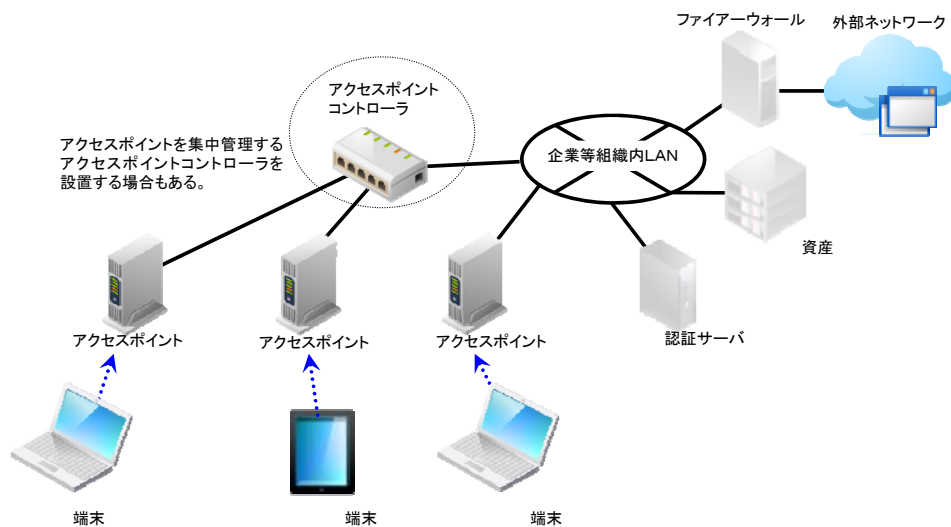


図1 企業等の組織における無線LANの構成例

(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LAN²を対象とし、無線LANと組織内の有線LANと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。また、IEEE802.11においては、表1に示す規格の情報セキュリティ対策として、IEEE802.11i及びIEEE802.11wが規格化されている。

なお、本手引書においては、有線LAN及び無線LANに共通するマルウェア感染対策等については取り扱わないこととするが、一般的な情報セキュリティ対策を実施することは、有線LANのみを運用する場合と同様に重要である。

表1 IEEE802.11における代表的な伝送規格

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ご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）

² IEEE Std802.11™-2012

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。企業等の組織による無線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。

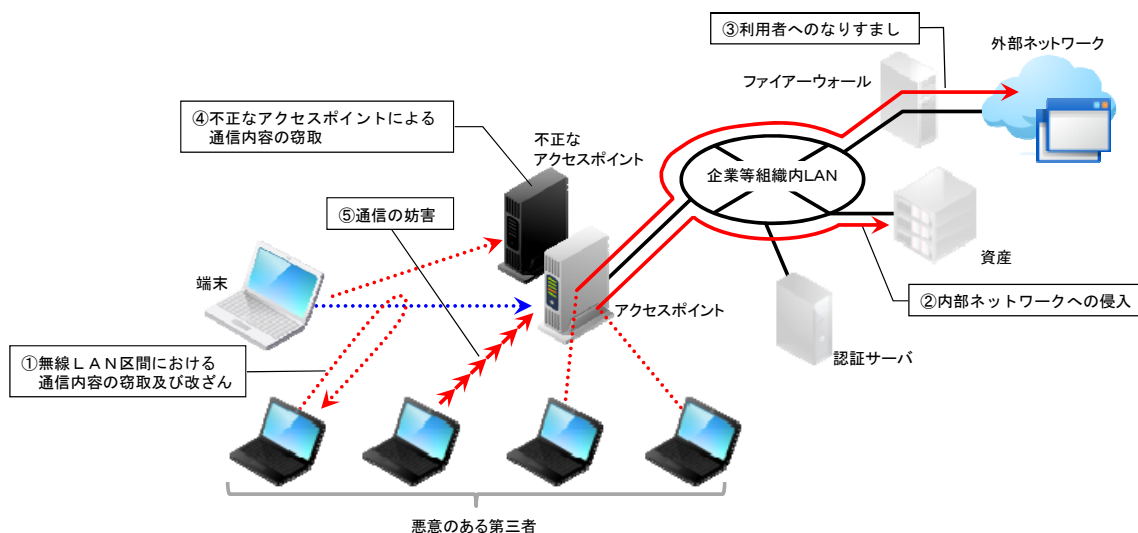


図2 情報セキュリティ上の主な脅威

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、内部の資産³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D o S (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、通信速度が低下する又は通信が不可能となるおそれがある。

³ 組織にとって価値をもつもの。物理的財産（例：コンピュータ ハードウェア、通信設備、建物）、情報・データ（例：文書、データベース）、ソフトウェア、製品又はサービスを提供する能力等を指す（JIS Q 13335-1-2006、ISO/IEC 13335-1-2004）。

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、暗号化等の技術面の対策及び機能制限等の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 無線LANの情報セキュリティ対策

想定される脅威	脅威への情報セキュリティ対策	
①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
②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ワードの設定、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・分析
	△	無線IDS/IPSの導入
③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ワードの設定、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・分析
	△	無線IDS/IPSの導入
④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
⑤通信の妨害	○	ログの収集・保存・分析
	△	管理フレームの暗号化・改ざん検知 (IEEE 802.11w)
	△	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 Alliance⁴により規格化されているWPA (Wi-Fi Protected Access) 及びWPA 2⁵がある。

WPA及びWPA 2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等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、適宜組み合わせで使用する。

なお、WPA 2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、WPA 2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、IEEE 802.11により規格化されている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IEEE 802.1X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・共有されているパスワードから、それぞれPSKと称される鍵を生成し、端末及びアクセスポイントを相互に認証する方式⁶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、パスワード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。認証用の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、共通のパスワードを設定する必要があることから、パスワードが外部に漏れいする危険性がある。また、総当たり攻撃 (Brute Force Attack)⁷等により、パスワード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、定期的なパスワードの更新が必須となる。万一、パスワードが漏れいした場合、パスワード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ワードを更新する必要がある。

⁴ 無線LANの普及促進を目的として設立された業界団体。

⁵ 無線LANの情報セキュリティの規格は、IEEE 802.11i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、IEEE 802.11i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。WPA 2は、2004年に正式に標準化されたIEEE 802.11i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。

⁶ 端末、アクセスポイントの設定項目等では、「WPA/WPA 2-PSK」、「WPA/WPA 2-Personal」等と表記される。

⁷ 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。

PSK認証は、パスフレーズそのものを用いて認証を行うのではなく、パスフレーズからPMKを、さらにPMKを用いてPTKを生成し、PTKにより端末とアクセスポイントそれぞれの認証を行う。この仕組みにより、認証ごとに異なる鍵を利用することになり、情報セキュリティ強度を高めている。

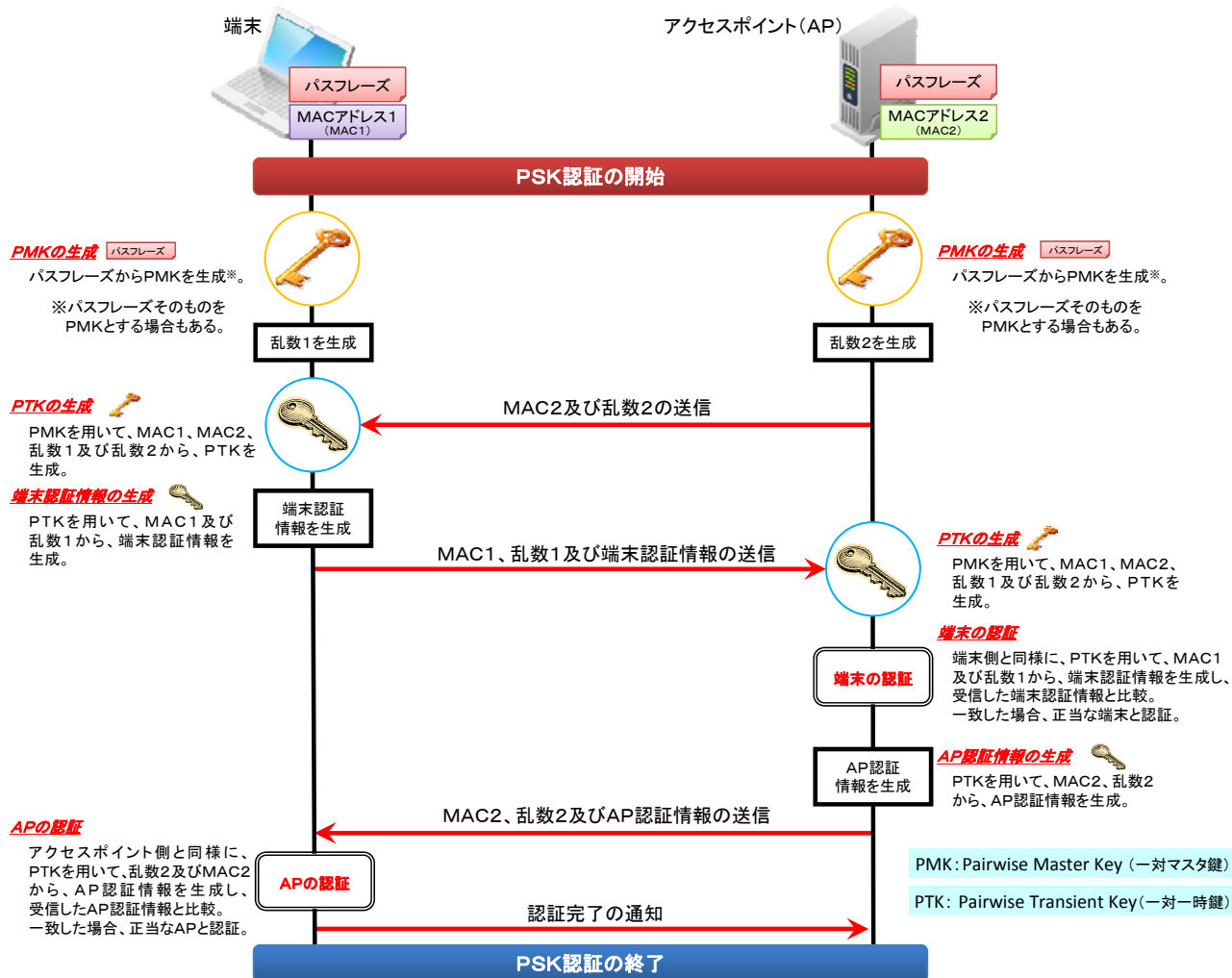


図3 PSK認証の仕組み

◇ IEEE 802.1X認証

IEEE 802.1X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 (Extensible Authentication Protocol)⁸を採用しており、パスワード、電子証明書⁹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¹⁰である。

IEEE 802.1X認証は、一般に、端末に搭載された認証用ソフトウェア、IEEE 802.1X認証に対応したアクセスポイント、RADIUS (Remote Authentication Dial-In User Service) と呼称される認証サーバの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る認証方式である。

⁸ 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。

⁹ 通信先の本人性を確認する電子的な証明書のこと。

¹⁰ 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。

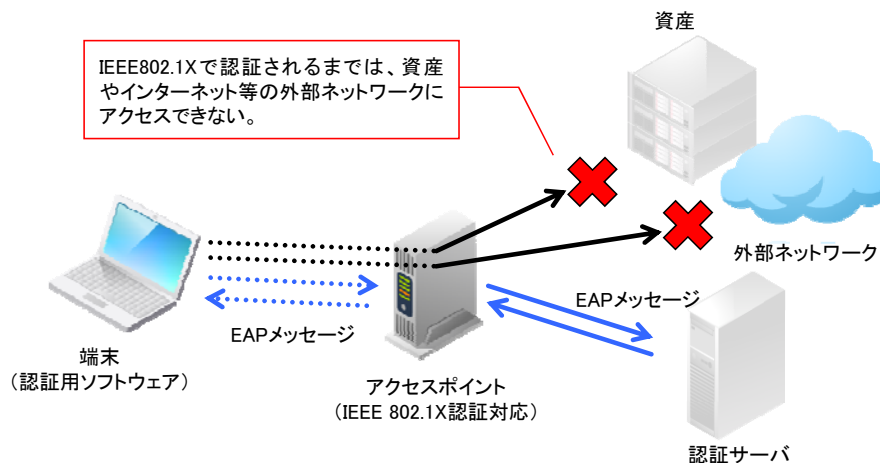


図4 IEEE 802.1X認証の仕組み

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¹¹。

現時点において、適切な情報セキュリティの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¹²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、情報セキュリティの強度は高くなる。

¹¹ 例えば、LEAP (Lightweight Extensible Authentication Protocol) 及びEAP-MD5 (Message Digest algorithm 5) 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。

¹² 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
情報セキュリティの強度	◎	○	○	◎	×	×
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	ID・パスワード	×
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)¹³の2つの規格¹⁴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¹⁵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¹⁶。

(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¹⁷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¹⁸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。

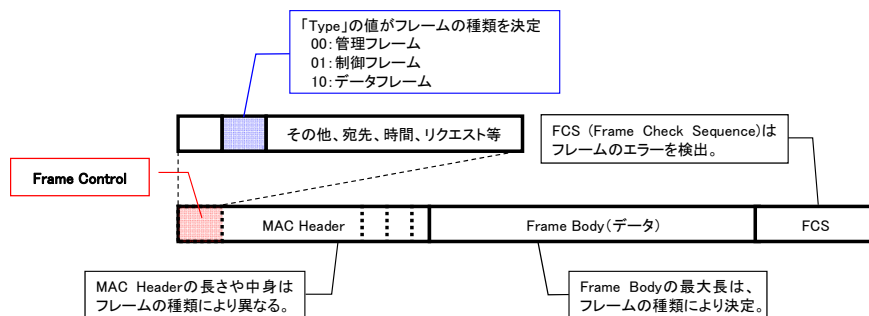


図5 無線LANのフレームの構造

¹³ 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。
¹⁴ 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。
¹⁵ Martin Beck, Erik Tews, "Practical attacks against WEP and WPA", 2008. T. Ohigashi, M. Morii, "A Practical Message Falsification Attack on WPA", Joint Workshop on Information Security (JWIS 2009), 2009.
¹⁶ 独立行政法人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、TKIPによる暗号化の際は、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。なお、更新間隔の短縮は、情報セキュリティの観点からは一般に望ましいといえるが、極端な短縮は無線LAN機器へ過度な負荷を与え、通信速度の低下を引き起こすおそれがあることに留意する必要がある。
¹⁷ 無線LANのアクセスポイントの通知及び検出、無線LANへの接続及び切断、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。
¹⁸ 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との接続及び切断は、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切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、D o S 攻撃が可能となる。

そこで、IEEE 802.11w 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 D o S 攻撃によって無線 LAN への接続が遮断されることを防止することができる¹⁹。

(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、システムへのフルアクセスを許可されている社員、一般社員等、資産の利用権限ごとに異なる SSID (Service Set Identifier)²⁰ を設定し、マルチ SSID 機能²¹ を備えたアクセスポイントを利用して 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 のトラフィックを監視し、D o S 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、許可なく設置又は接続されたアクセスポイント及び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 を経由した内部ネットワークへの侵入、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、一定ではないことに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

¹⁹ 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 D o S 攻撃を防止することはできない。

²⁰ SSID を利用した情報セキュリティ対策として、SSID の存在を隠す SSID のステルス化があるが、ステルス化された SSID を検知するツールが公開されているため、企業等の組織が無線 LAN を運用する際の情報セキュリティ対策としての有効性は乏しい。

²¹ 一つのアクセスポイントに複数の 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。

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であるなど、よく知られていることがあるため、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パスワードに変更することが適当である。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・分析

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し、又は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・保存により、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

無線LANを構築・運用している場所及びその周辺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。

例えば、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(Media Access Control)アドレス²²、電波強度等の電波状況を確認する。また、多数のアクセスポイントを設置し、大規模な無線LANを構築・運用している場合には、専用の機器を利用し詳細に確認することが適当である。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に留意する必要がある。

なお、アクセスポイント以外の不正な電波発生源を検知するためには、スペクトルアナライザ等の専用の機器が必要となる。

(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²³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。

そのため、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、アドホックモードの利用を禁止することが適当である。

²² MACアドレスを利用した情報セキュリティ対策として、端末のアクセスポイントへの接続を端末のMACアドレスによって制限するMACアドレスフィルタリングがあるが、MACアドレスを偽装することは可能であるため、企業等の組織が無線LANを運用する際の情報セキュリティ対策としての有効性は乏しい。

²³ WPA及びWPA2の利用ができないことがあるIBSS(Independent Basic Service Set)の他に、Wi-Fi Allianceが策定した仕様であるWi-Fi Directがある。Wi-Fi Directは、WPA2が標準で利用できるなど、IBSSよりも情報セキュリティが高いがアクセスポイント及びサーバにログが残らない、LAN管理者が管理・監視することが困難であるなどの理由から、利用許可については慎重を期すべきである。

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、企業等の組織が定めた無線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継続的に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、企業等の組織が定める無線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。

表4 無線LANの導入・運用の各段階において実施すべき事項

段階	実施すべき事項	
a. 準備段階	◎	無線LANからの利用を許可する資産の設定
	◎	無線LANの情報セキュリティ対策の検討
	○	無線LANの利用を許可する端末の登録
	△	電波の伝搬範囲の設定
	◎	無線LANの運用ルールの策定
b. 構築段階	◎	パスワード等の適切な設定
	◎	アクセスポイントの情報セキュリティの設定
	◎	設置したアクセスポイントの管理
	○	ログの収集・保存設備の構築
c. 運用段階	◎	パスワード等の定期的な更新
	◎	アクセスポイント情報の更新
	△	許可されていない又は不正なアクセスポイント等の設置状況の監視
	○	ログの収集・保存・分析
d. 廃棄段階	◎	無線LANの設定情報の消去

◎：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

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²⁴。

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（組織の一部の構成員のみに限定するか、組織の全ての構成員に提供するかなど）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、外出用の端末の組織内の利用に関して、インターネット接続は許可するが組織内のデータベース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。

²⁴ 総務省「無線LANビジネス研究会報告書」（平成24年7月）

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資産の範囲の性質に応じて、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ワードを設定するため、パスワード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、パスワード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、パスワードの設定、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止することができる。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²⁵。

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を経由した内部ネットワークへの侵入、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、端末ごとに接続するアクセスポイント

²⁵ 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ワードの設定、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。

トを定めること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、組織の構成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、組織外の無線LANを利用して組織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、組織内システムに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組織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、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²⁶。

(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を検出するため、組織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・保存設備の構築

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・保存する設備を構築する。

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

²⁶ 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。

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²⁷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、IEEE 802.1X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が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。

(3) 許可されていない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²⁸となる許可されていないアクセスポイント、不正なアクセスポイント等の設置を防止するため、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) ログの収集・保存・分析

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止する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。

²⁷ 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。

²⁸ 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止するためには、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ファイルについて、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、顧客ファイルの情報を盗んだ上で、ファイル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を採用していた。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、攻撃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てしまった。これにより、当該攻撃者のみならず、複数の第三者が無線LANへアクセス可能となり、内部のネットワークに侵入された。

<解決策>

このような事例の発生を防止するためには、認証方式及び暗号化方式の設定等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。

なお、無線LANを利用する場合に限らず、ファイル等へのアクセスコントロールを設定することは、一般的な情報セキュリティ対策として重要である。

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ネットワークへ

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止するためには、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、特段の措置を講じなかった。

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止するためには、WPA/WPA2-EAPを採用することが有効である。また、電波状況の監視を行うことが望ましい。