

別添

～ 安心して無線 LAN を使用するために ～

参 考 資 料

平成 1 6 年 4 月 2 6 日

総 務 省

目 次

1 LANの基礎	3
(1) LANとは	3
(2) LANの伝送媒体～無線LANと有線LAN～	3
(3) LANの規格	3
2 無線LANについて	4
(1) 無線LANとは	4
(2) 無線LANの周波数	5
(3) 無線LANの特徴	6
ア 構成要素	6
イ 形態	7
ウ 通信状態	9
エ 電波干渉の影響	9
(4) 無線LANのメリットとデメリット	9
ア メリット	9
イ デメリット	9
(5) 無線LANの種類	10
ア IEEE 802.11 a	10
イ IEEE 802.11 b	10
ウ IEEE 802.11 g	10
(6) 無線LANのチャンネル間隔	12

(7) メーカー同士の相互接続の推進～Wi-Fi Allianceの誕生～	13
(8) 無線LANの利用形態～家庭、オフィス、公衆エリア～	14
ア 家庭における無線LANの利用形態	14
イ 企業における無線LANの利用形態	15
ウ 公衆エリアにおける無線LANの利用形態	16
3 無線LANのセキュリティ技術動向	17
(1) 無線LANのセキュリティ技術	17
ア WEP	17
イ SSID	21
ウ MACアドレスフィルタリング	22
エ まとめ	24
(2) 無線LANのこれからのセキュリティ技術	24
ア IEEE 802.1x	24
イ WPA (Wi-Fi Protected Access)	33
ウ IEEE 802.11i	39
(3) その他のセキュリティ	39
ア SSL (Secure Sockets Layer)	39
イ VPN (Virtual Private Network)	40
ウ SSL-VPN	45

1 LAN の基礎

(1) LANとは

オフィスや家庭などで、複数台のパソコンでインターネットを利用したり、ハードディスクを共有したりする時に必要なのがLANである。LANとは、英語の Local Area Network の略であり、文字通り、限られた範囲内、例えばオフィスや研究室、建物などに張られたネットワークのことを指す。一般的にLANを構築することで以下のようなメリットが挙げられると考えられる。

パソコン同士でデータの共有ができる。

アプリケーションソフトの共有ができる。

プリンタなどの周辺機器の共有ができる。

分散処理が可能になる。

高速にデータを送受信できる。

(2) LANの伝送媒体 ～有線LANと無線LAN～

LANの伝送媒体は有線と無線に分類される。有線としては、より対線（ツイストペアケーブル）、同軸ケーブル及び光ファイバケーブルの3種類があげられる。同軸ケーブルは高価であるが電気特性が良く、信頼性も高い。光ファイバは高速・大容量の伝送ができ、電氣的雑音に強い特長を持っている。一方、敷設や接続がより対線や同軸ケーブルに比べて容易ではないなどの欠点を持っているが、今後の高速・大容量の伝送のため、更に普及する可能性がある。

無線LANには、ケーブル敷設の煩雑さがなくことや移動可能という機動性に特長がある。一般に無線LANは電波を用いるものを指すが、赤外線等を利用するものもある。最近では、パーソナルコンピュータに2.4GHz帯の無線LANが標準装備されているものも多い。

(3) LANの規格

現在利用されているLANには多くの規格があり、その多くがIEEE802委員会によって標準化されている。IEEE802委員会とは、175か国36万人以上が参加する世界最大の学会IEEE（米国電気電子技術者協会）が1980年2月にLAN及びMAN（Metropolitan Area Network）の標準化を目的に設けた委員会である。委員会は約20のグループに分かれ、上位インターフェイス、論理リンク制御、音声/データ統合

などについて討議するグループの他にアクセス制御方式別にグループが存在する。表 1 に代表的なグループを示す。

表 1 IEEE802 委員会の代表的なグループ

グループ名	活動概要
802.1	上位層プロトコル
802.3	Ethernet (CSMA/CD)
802.11	無線 LAN
802.15	パーソナルエリア無線ネットワーク (WPAN: Wireless Personal Area Network)
802.16	広帯域無線アクセス (BWA: Broadband Wireless Access)
802.17	障害回復機能を持つパケットリング技術 (RPR: Resilient Packet Ring)
802.18	電波に関する規定技術諮問グループ
802.19	共存技術諮問グループ
802.20	モバイル広帯域無線アクセス網 (MBWA: Mobile Broadband Wireless Access)

Ethernet: 有線 LAN の一般的な通信方式。CSMA/CD は、通信が行われていない時を見計らってデータを送信する方式

2 無線 LAN について

(1) 無線 LAN とは

無線 LAN とは、有線ケーブルの代わりに、電波を利用することでパソコン同士を接続し、LAN を構築しようとするものである。最近のノートパソコンは、無線 LAN 機能が標準装備されているものが多く、無線 LAN の普及は急速に拡大している。現在では、企業や学校のみならず、一般家庭においても広く利用されるようになっており、喫茶店やファーストフード店、空港、駅、ホテルなどの公衆エリアにアクセスポイントを設置して無線 LAN 環境を提供する公衆無線 LAN サービスも行われている。

(2) 無線 LAN の周波数

1987年に米国の FCC (Federal Communications Commission : 米国連邦通信委員会) の規則改定により、それまで軍用にしか認められていなかった「スペクトラム拡散」方式による通信が開放され、民間でも ISM バンド (Industry Science Medical band 米国では 900MHz 帯、2.4GHz 帯、5.7GHz 帯) を利用してスペクトラム拡散通信を行うことが可能になった。この周波数帯では、無線局免許を不要としており、多くのベンダーが競って製品を作るようになった。また、当初は数 100kbps 程度と低速であったが、高速化の需要と共に、製品の本格的普及のため標準化の重要性が認識されるようになり、1990 年から IEEE802 委員会の IEEE802.11 グループにおいて 2.4GHz 帯と赤外線 (Ir : Infrared) の無線 LAN に関する標準化が正式にスタートした。

日本における無線 LAN に適用される周波数帯は、2.4GHz 帯、5GHz 帯であり、その他に準ミリ波帯 (19GHz 帯、25GHz 帯及び 27GHz 帯) を利用するものなどがある。また、赤外線やレーザーを用いるものもある。

日本における無線 LAN (2.4GHz 帯及び 5GHz 帯) の周波数割当状況について図 1 及び図 2 に示す。

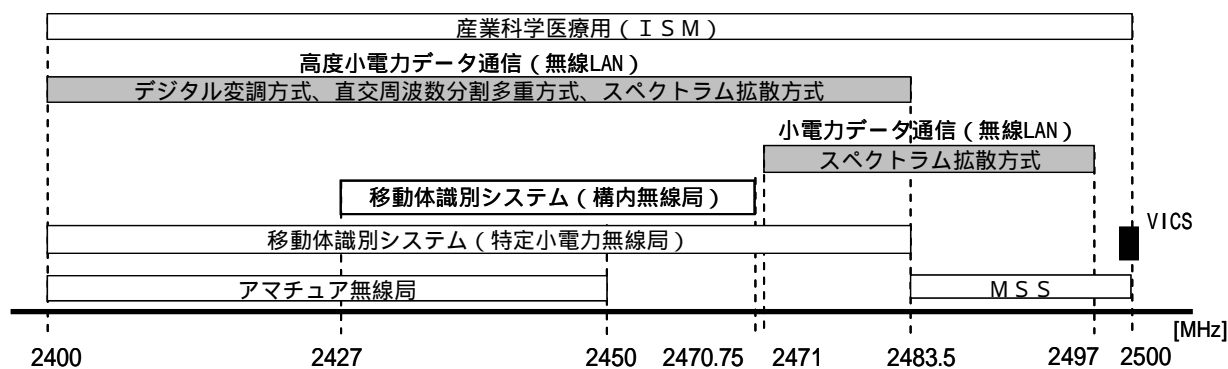


図 1 日本における無線 LAN の周波数 (2.4GHz 帯)

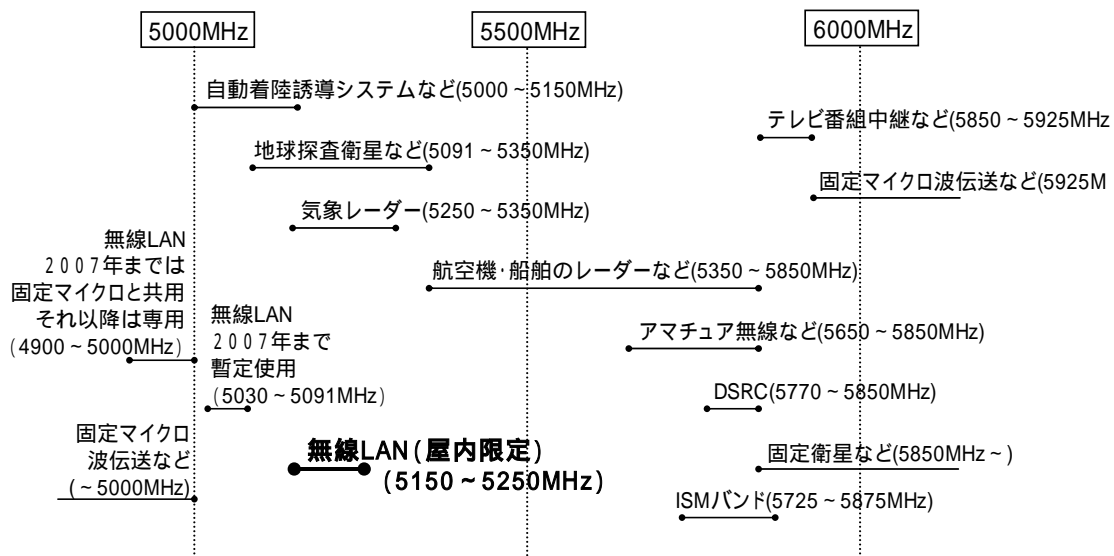


図2 日本における無線LANの周波数(5GHz帯)

(3) 無線LANの特徴

ここで、無線LANに関するいくつかの特徴を取り上げる。

ア 構成要素

有線LANと無線LANの根本的な違いは伝送媒体である。有線LANではLANケーブルを用いて伝送するのに対し、無線LANでは電波を用いて伝送する。そのため、無線LANではその電波を中継する無線LANアクセスポイントと無線LANアダプタが必要になる。

(ア) 無線LANアクセスポイントとは

無線LANで電波の送受信をするための基地局となる機器である。機器の中には、有線LANとのインターフェイスを持ち、有線LANと無線LANとの中継機器にもなるものや、ルーティングの機能などルータの機能を兼ねそろえたものもある。

(イ) 無線LANアダプタとは

無線LANカードとも呼ばれ、無線LANを利用するための拡張機能を提供するものである。無線LANアダプタの中には、ノートパソコン向けのPCカード型やUSBポート型などさまざまなものが存在する。また最近では、すでに無線LANアダプタが内蔵されている製品も多くなってきている。

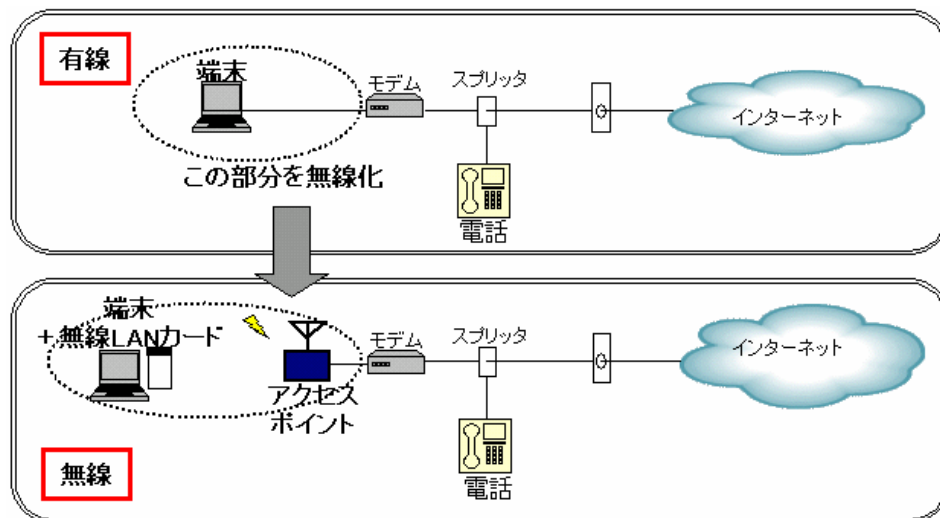


図3 有線と無線の構成の違い

イ 形態

無線LANのネットワーク構成には、インフラストラクチャモードとアドホックモードの2種類がある。

(ア) インフラストラクチャモード

このモードは、アクセスポイントと、その電波到達範囲（無線セル）内に存在する無線LAN端末（無線LAN端末とは、無線LANアダプタを取り付けた端末及びすでに無線LANアダプタが内蔵されているものはそのものを指し、無線LANを利用することができる端末を示している。）で構成されるものである。基本となる一つのアクセスポイントと、その配下の複数の無線LAN端末の構成をBSS（Basic Service Set、基本サービス・セット）と呼ぶ。無線LAN端末は、特定の一つのアクセスポイントと論理的な接続（Association）を確立する。アクセスポイントは、Ethernetなどのバックボーン・ネットワークに接続されており、無線LAN端末とバックボーン・ネットワーク間のパケットの中継を行う。また、配下の無線LAN端末同士が通信する際のパケットの中継も同時に行う。これにより、ユーザは無線を通じてネットワーク上の各種サーバと無線環境で通信できるようになる。図4にインフラストラクチャモードのネットワーク構成を示す。同じネットワークにつながるアクセスポイントをグループ化し、移動により以前のアクセスポイントと通信できなくなった場合、他のアクセスポイントへ接続関係を切り替えるハンドオフ機能を備えている場合があり、無線環境での移動が確

保されている。このBSSの集合で構成されるグループをESS(Extended Service Set、拡張サービス・セット)と呼ぶ。

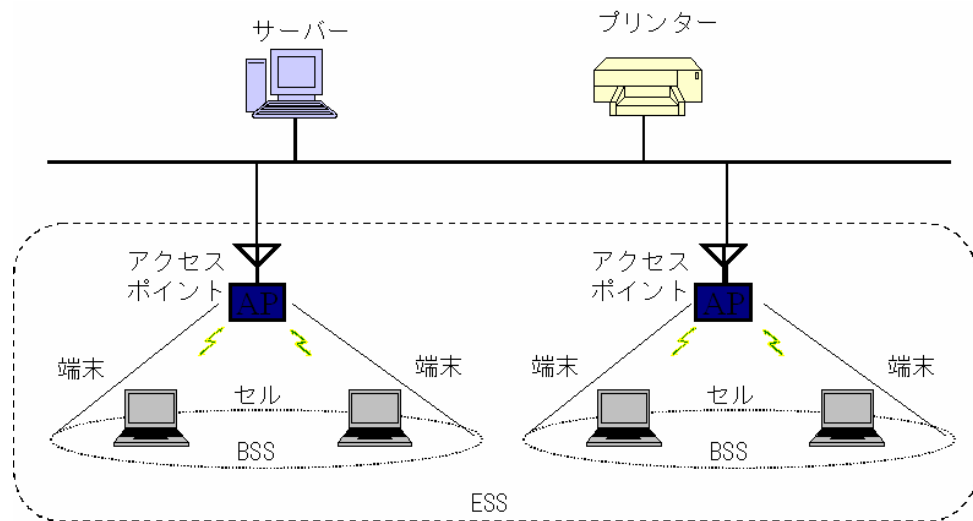


図4 インフラストラクチャモード

(1) アドホックモードのネットワーク

アドホックモードではアクセスポイントを必要とせず、無線LAN端末のみで構成するため、インフラ・モードのBSSと区別してIBSS(Independent BSS、独立したBSS)と呼ぶ。

無線LAN端末は、無線パケットを中継する機能を持たず、直接お互いに無線パケットをやり取りして通信を行う。

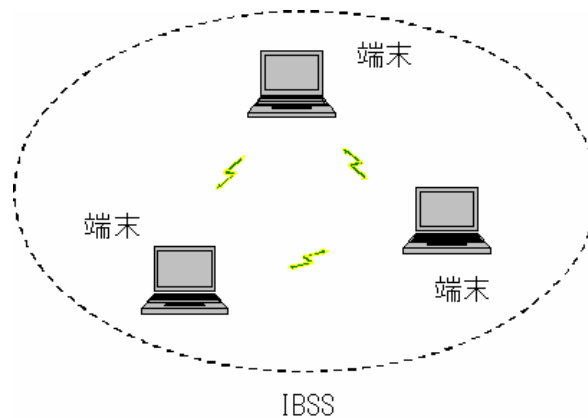


図5 アドホックモード

ウ 通信状態

無線 LAN では、無線の特質上、通信状態が常に一定であるとは言いがたい。携帯電話に表示される電波の状況と同じように、場所や周囲の環境によって大きく電波環境が変わる。無線 LAN の規格を決めている IEEE802.11 グループでは電波環境に対応してその通信速度が変化するように規定をしている。例えば、環境が良ければ 11Mbps で、悪ければ 1Mbps など、無線 LAN の通信速度は変化する。

エ 電波干渉の影響

現在、無線 LAN で用いられている 2.4GHz 帯では、無線局免許を不要としている。この周波数帯は、工業用や医療用の高周波機器や家庭用の電子レンジなどにも利用されており、同じ場所で同時に利用すれば干渉が起こる。また、アクセスポイント同士及び無線 LAN 端末同士でも干渉が起こる。

(4) 無線 LAN のメリットとデメリット

ア メリット

(ア) モビリティ

無線 LAN は見通しの良い場所であれば 100m 近く電波が飛ぶので、離れた所を自由に移動しながらデータ通信を行うことができる。

(イ) ケーブル配線の煩雑さの解消

無線 LAN には有線特有の配線のトラブル、例えば、ケーブルの断線、アダプタからの脱落、接続先の誤りなどは発生しない。

(ウ) スムーズなネットワーク構築

家庭内や SOHO の事務所など、大掛かりな配線工事を避けて、比較的簡単にネットワークを構築でき、有線よりも低コストでできることもある。

イ デメリット

(ア) 通信の不安定さ

無線 LAN はその性質上周りの環境にかなり影響を受ける。電波の届きにくいところでは通信速度は安定しない可能性がある。

(イ) セキュリティ対策が必要

無線 LAN は見通しが良いところであれば、100m 近く電波が飛ぶので、無線 LAN に関して高度な知識を持つ悪意のある第三者によって盗聴されるだけでなく、個人情報盗まれるなど思わぬ犯罪に巻き込まれたりする危険性がある。このよ

うな事態から身を守るには、WEP や MAC アドレスフィルタリング、SSID などを用いてデータの暗号化や認証などの点でセキュリティ対策を十分に行わなくてはならない。

(5) 無線 LAN の種類

無線 LAN では、IEEE802.11a/b/g の 3 種類が主に用いられている。

ア IEEE802.11a

新たに無線 LAN 用に割り当てられた 5GHz 帯を利用し、最大 54Mbps の伝送速度を実現する物理層の規格。変調方式として OFDM を利用し、高速化された。通信速度としては、6/12/24Mbps の伝送速度に準拠するように要求されており、他に 9/18/36/48/54Mbps の伝送速度もオプションで用意されている。5.15~5.25GHz は衛星通信に利用されているため、屋外での利用は禁じられている。

イ IEEE802.11b

2.4GHz 帯を利用し、最大 11Mbps の伝送速度を実現する物理層の規格。無線 LAN の最初の規格であった IEEE802.11 は、2.4GHz 帯を用いて通常 1 チャンネル 2Mbps の伝送速度しか得られなかったため、有線 LAN と比べ見劣りのするスペックとなっていた。そこで、その物理層（電波の周波数帯、データの変調方式、物理層ヘッダなど）を改良することでデータ通信の高速化が図られてきた。

ウ IEEE802.11g

2.4GHz 帯を利用して最大 54Mbps の伝送速度を実現する物理層の規格。変調方式として IEEE802.11a と同じ OFDM を利用することで、2.4GHz 帯での高速化を実現している。IEEE802.11b に対して上位互換性も考えられているため、IEEE802.11a と比較して既存の無線 LAN 端末と共存しやすいメリットがある。

2.4GHz 帯の周波数を利用する IEEE802.11b と IEEE802.11g は、同じ物理ヘッダを使用しており、変調方式も高速な IEEE802.11g が IEEE802.11b の方式である CCK（Complementary Code Keying）変調方式をサポートしているため、互換性がある。例えば、IEEE802.11g のアクセスポイントに IEEE802.11b と IEEE802.11g の無線 LAN 端末が同時に接続しても通信が可能である。ただし、IEEE802.11g は速度の遅い IEEE802.11b との互換性を保つために、制御系の情報を運ぶ物理ヘッダを 1Mbps で送信する必要がある（無線 LAN 規格には前述のとおり、その電波環境などによる、いくつかの伝送速度をサポートしている。例えば、IEEE802.11b では、1、2、5.5、11Mbps

と4種類の速度モードがある。速度のモードは、電波の状況に応じてフレーム毎に変えられるが、どういう変調方式でどの速度モードにしたいのかを相手に確実に伝えなければならない。そこで、こうした情報を伝える物理層ヘッダは、最も低速の1Mbpsで送ることにしている。)ので、IEEE802.11aに比べると速度が落ちる。IEEE802.11aとIEEE802.11gはともにOFDM方式を適用しているが、IEEE802.11aは5GHz帯、IEEE802.11gは2.4GHz帯なので互換性はない。

表2 IEEE802.11a/b/gの違い

無線LAN規格	IEEE802.11a	IEEE802.11g	IEEE802.11b
使用周波数帯	5.2GHz帯屋内限定 (5.15~5.25GHz)	2.4GHz帯 (2.400~2.4835GHz)	2.4GHz帯 (2.400~2.497GHz)
伝送方法	直交周波数分割多重方式(OFDM)	直交周波数分割多重方式(OFDM) 直接拡散スペクトラム拡散方式(DSSS)	直接拡散スペクトラム拡散方式(DSSS)
伝送速度	54,48,36,24,18,12,9,6(Mbps)	54,48,36,24,18,12,11,9,6,5.5,2,1(Mbps)	11,5.5,2,1(Mbps)
チャンネル	34,38,42,46ch(20MHz毎)	1~13ch(14ch利用不可)	1~14ch(5MHz毎、14chは日本独自)
伝送距離(目安)	屋内約100m	屋外:約300m 屋内:約100m	屋外:約300m 屋内:約100m
最大データ転送速度	54Mbps (無線区間、それ以外の部分の影響により実効速度は、20Mbps程度)	54Mbps (無線区間、それ以外の部分の影響により実効速度は、20Mbps程度。さらに、IEEE802.11bと共存時は低下する)	11Mbps (無線区間、それ以外の部分の影響により実効速度は、3~5Mbps程度)
長所	・伝送速度が速い ・電波干渉の可能性が低い	・伝送速度が速い ・IEEE802.11bとの互換性がある	・現在の無線規格の主流であり、種類が豊富、値段が安い
短所	・対応製品がまだ少ない ・電波の届く範囲が短い	・対応製品がまだ少ない ・干渉が起こりやすい	・伝送速度が遅い ・干渉が起こりやすい

(6) 無線 LAN のチャンネル間隔

無線 LAN のチャンネル間隔は、IEEE802.11b/g には 5MHz 間隔で 13 チャンネル、IEEE802.11a では 20MHz 間隔で 4 チャンネル定義されている。IEEE802.11b/g のメインロープの幅は、約 22MHz であるため、チャンネルが近いと使用周波数が重なってしまい、通信が上手く行えない場合がある。このため、周波数の重なりを避けるには、5 チャンネル以上離す必要がある。例えば、チャンネル 1 を利用する場合、チャンネルが重ならないようにするには 6 チャンネルを利用するといった具合である。一方、IEEE802.11a を利用する場合には、チャンネル間隔を 1 以上離すと互いに帯域が重なり合わない。

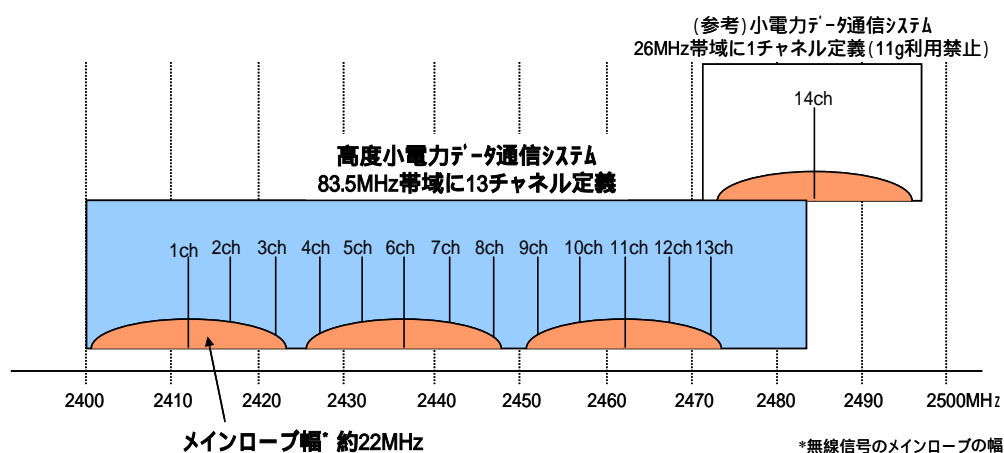


図 6 2.4GHz 帯のチャンネル

日本では IEEE802.11b の場合、1～14 チャンネルを利用することができるが、米国では 1～11 チャンネルまで、ヨーロッパではほとんどの国で 1～13 チャンネルまでを利用することができる。ちなみに、フランスでは 2.457G～2.472GHz の 4 チャンネル、スペインに至っては 2.457GHz と 2.462GHz の 2 チャンネルに制限されている。グローバル対応の IEEE802.11b 及び IEEE802.11g 製品（ノートパソコン内蔵製品などの一部）は 1～11 チャンネルにのみ対応している。このため、日本でも 1～11 チャンネルがよく用いられている。表 3 に 2.4GHz 帯のチャンネル周波数を示す。

5GHz 帯については日本では、5.150～5.250GHz が利用可能である。また、5.03～5.091GHz 及び 4.9～5.0GHz が屋外利用可能な帯域として開放されている。5.03～5.091GHz は 2007 年までの時限開放である。

表3 2.4GHz 帯のチャンネル周波数

チャンネル	中心周波数	日本	米国	ヨーロッパ
1	2.412GHz			
2	2.417GHz			
3	2.422GHz			
4	2.427GHz			
5	2.432GHz			
6	2.437GHz			
7	2.442GHz			
8	2.447GHz			
9	2.452GHz			
10	2.457GHz			
11	2.462GHz			
12	2.467GHz			
13	2.472GHz			
14	2.484GHz			

*ヨーロッパはフランス・スペインを除く。

(7) メーカー同士の相互接続の推進 ~Wi-Fi Allianceの誕生~

無線LAN技術はEthernetなどと比べるとまだ歴史が浅いため、当初は規格の解釈の違いや実装されている機能などに差異があり、すべての製品間で相互に問題なく接続できるわけではなかった。特定の機種同士では接続することができても、別の機種同士では通信できなかつたり、使用する場所や状態によってはうまく通信できなかつたりした。このような状況は、無線LAN業界としても問題であるばかりでなく、ユーザにとってもどの製品を選ぶべきか選択が困難になり、ひいては無線LAN製品全体に対する信頼が揺らぐことにもなりかねない。

そこで無線LAN技術の推進団体Wi-Fi Alliance(旧称WECA:Wireless Ethernet Compatibility Alliance)では、無線LAN規格に対応した製品同士が確実に相互運用できるかどうかを検証し、無線LAN技術を普及促進することを目的とした、Wi-Fi認定試験を行っており、最低限サポートすべきSSIDの仕様やペイロード(*)の暗号化サポートの有無、パワーセーブ・モードの有無、WEPのサポート仕様、応答時間や転送レートの要求仕様、ローミング時の扱いなどのほか、規格上であいまいになっている部分やオプションとなっている部分などに対しても具体的な取り扱い方法などを決

め、標準的な環境を用意して相互運用性をテストしている。この Wi-Fi 認定テスト (Wi-Fi System Interoperability Test Plan) に合格した製品には図 7 に示す Wi-Fi 認定ロゴが与えられ、ある一定レベルの相互運用性が保証される。ユーザはこのロゴを製品選択の参考にすることができる。

*ペイロード： 通信パケットのうち行き先などの付加情報であるヘッダ部分を除いた、本来転送したいデータ本体を指す。送られるパケットは、「ヘッダ+ペイロード」という構成になっている。



図 7 Wi-Fi ロゴマーク

(8) 無線 LAN の利用形態 ~ 家庭、オフィス、公衆エリア ~

さまざまな場面で利用されている無線 LAN であるが、以下に具体的な無線 LAN 利用形態について示す。

ア 家庭における無線 LAN の利用形態

自宅における無線 LAN の利用は以下の点でメリットがあると考えられる。

インターネットの共用

ケーブルの配線が不要で美観を損ねない

ADSL、光を用いた高速インターネット利用が家庭にも浸透し始め、パソコンをブロードバンドに複数接続して、家族全員がインターネットを楽しむことができる。無線 LAN を利用することで、いつでもどの部屋でも利用することができるメリッ

トがある。例えば、キッチンでレシピを見る、リビングでインターネットを利用するなど、無線LANの強みを生かした柔軟な活用が可能になる。

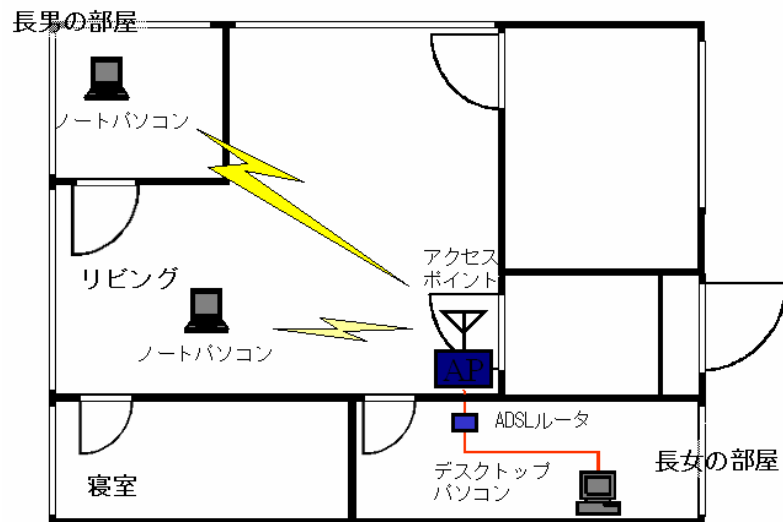


図8 家庭における無線LANの利用形態

イ 企業における無線LANの利用形態

企業における利用としては、以下のようなメリットが考えられる。

配線の簡略化

端末の移動、増設、レイアウト変更が容易

床上げをしていない、配線できない場所でも、ネットワーク接続が可能

ランニングコストの削減

特に、企業などでは人事異動によるネットワーク環境の変更や、会議を行う際にノートパソコンを会議室へ持ち込んで行う場面が多々ある。このような状況において、無線LANのメリットが生かせる。

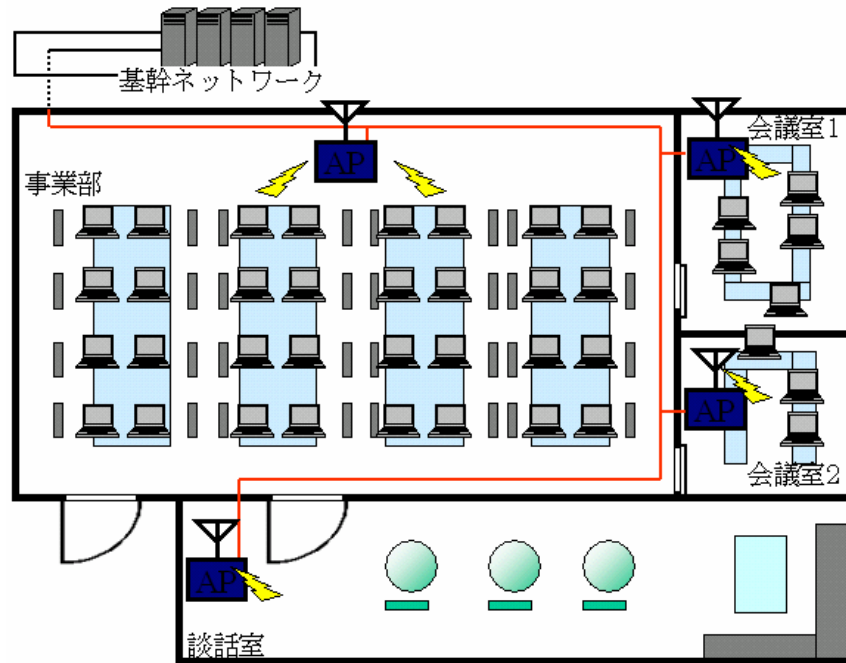


図9 企業における無線LANの利用形態

ウ 公衆エリアにおける無線LAN利用形態

一般家庭や企業に普及しているような無線LANブロードバンド環境を、外出先の飲食店・駅・ホテル等のサービスエリアから利用できるのが公衆無線LANである。公衆無線LANとしては、電気通信事業者が契約者に対してインターネット接続環境を提供するサービス（本資料では「公衆無線LANサービス」と呼ぶ。）、個人・団体などがアクセスポイントを設置し、無料で使用できるようにしたもの（本資料では「店舗開放型無線LANサービス」と呼ぶ。）がある。

3 無線 LAN のセキュリティ技術動向

(1) 無線 LAN のセキュリティ技術

これまでの無線 LAN では、WEP、SSID、MAC アドレスフィルタリングという三つの技術をセキュリティ技術として用いることが可能である。

ア WEP

WEP (Wired Equivalent Privacy) とは、IEEE により標準化された無線 LAN 通信を暗号化するための規格で、IEEE802.11b 等で使用される暗号化仕様の総称である。無線 LAN は、電波の届く範囲であれば、誰でも通信内容を傍受することができ、重要なデータが盗まれる可能性がある。そこで、通信を暗号化し、第三者に通信内容を容易に知られないようにするために使用する。実際にデータを暗号化する際に用いられるアルゴリズムは「RC4」、鍵方式は共通鍵方式であり、鍵生成方法などを含めて WEP が構成されている。

しかし、WEP による暗号化は、仕組み上いくつかの問題点が存在するため、WEP を用いて暗号化することがセキュリティとして万全であるとは言い難い。

(ア) 鍵の問題

WEP の暗号化で使われる鍵 (キー) は、事前にアクセスポイントと無線 LAN 端末間で任意の文字列を共有しておく必要がある (ユーザが設定する必要がある。ここでは、設定キーと呼ぶ。)。この設定キーと IV を基にデータを暗号化 / 復号化するための鍵 (ここでは、WEP キーと呼ぶ。) が自動生成される。この WEP キーは長さが 64bit の場合と 128bit の場合が選択でき、後者は鍵長が長いことから秘匿性が向上する。

アクセスポイントには複数の無線 LAN 端末がアクセスするが、WEP ではどの無線 LAN 端末も同じ WEP キーを使う。したがって、第三者による総当たり攻撃 (可能な暗号の組合せをすべて試みる攻撃手法) などにより、これを突き止められた場合、同じアクセスポイント配下に接続された他の無線 LAN 端末のデータも簡単に解読されてしまう。

(イ) IV (Initialization Vector)

WEP では、送信側の無線 LAN 端末が送信フレーム毎にランダムに IV という 24 ビットの情報を生成し、設定キーと組み合わせて暗号化アルゴリズムの WEP キー

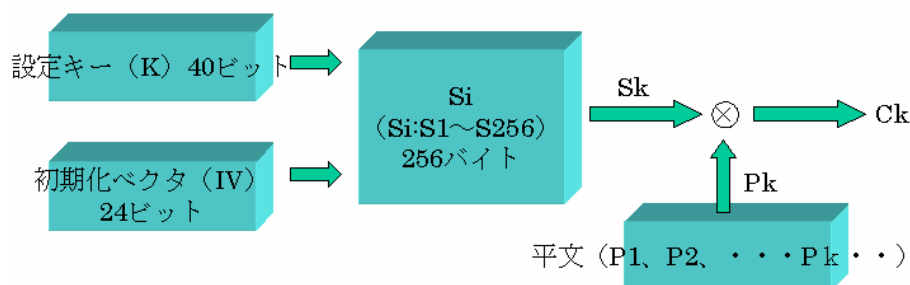
として使用する。これにより、平文（暗号化されていない生の文章）と暗号文のペアを知られてしまうと次に送られてきた暗号文から平文が判明してしまうという問題を防ぐ。

なお、IV 自体は、フレーム・フォーマットに組み込んで暗号化させずにそのまま送信する。これは、受信側が復号化する際に、どのような IV で暗号化したかという情報が必要という理由からである。

(ウ) RC4 (Rivest Cipher 4)

暗号化アルゴリズムには、RC4 というアルゴリズムを使用している。これは共通鍵暗号方式の一種で、1987 年に米 RSA DATA Security 社により開発された。共通鍵暗号方式にはストリーム暗号方式とブロック暗号方式の二種類があり、RC4 は前者である。ストリーム暗号とは、暗号鍵から鍵系列と呼ばれる疑似乱数を生成し、平文を 1 ビットあるいは数ビット毎に排他的論理和による演算を用いて逐次暗号化するアルゴリズムである。

しかしながら、WEP キー自体の長さは、64bit 又は 128bit など限られた長さしかないので、第三者が暗号文と平文（の一部）を入手した場合、暗号文と平文との排他的論理和を算出することによって鍵系列（の一部）が分かってしまう。これによって、さらに総当り攻撃（パスワードの割り出しや暗号の解読に使われる攻撃手法の一つで辞書にある単語を片端から入力して試すというもの。）等を用いることで WEP キー候補から正しい WEP キーを絞り込むことができ、結果としてすべての暗号文を解読されてしまう。WEP の RC4 暗号化アルゴリズム処理の流れを図 10 に示す。図は WEP キーを 64bit に設定した場合である。



出典：松江英明、守倉正博監修「802.11高速無線LAN教科書」(IDGジャパン、2003年)

図 10 WEP の暗号化アルゴリズム RC4 の処理の流れ

(イ) WEPで暗号化される範囲

WEPで暗号化される範囲は、データ部分とICV(Integrity Check Value:完全性検査値)部分である(図11参照)。ICVは、送信されるデータの整合性をチェックするために送信時にIA(Integrity Algorithm)により計算されたCRC32[32ビットのCRC(Cyclic Redundancy Check:巡回冗長検査)]の値を指す。この値は、暗号化されたデータとともに送信され、受信側でエラー検出に利用されている。

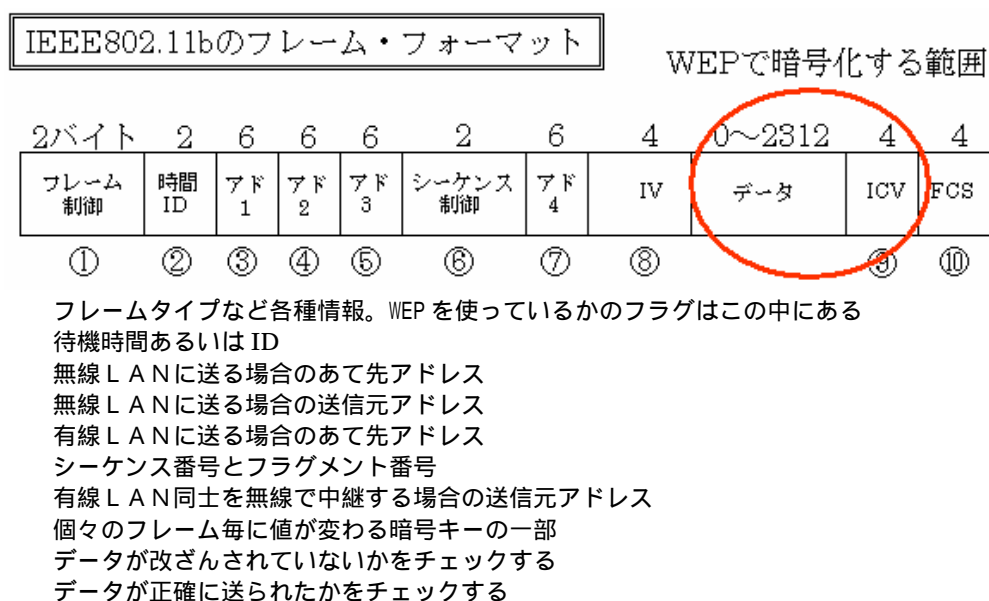


図11 WEPの暗号範囲

(オ) WEPの脆弱性

WEPは、コア部分であるRC4自体の安全性及び設定キーが40bitと短いことから、当初から安全性が懸念されていた。2001年夏には、WEPを解読したことが、RSA暗号の開発者のひとりであるShamir氏により発表された。

RC4では、同じ暗号鍵を使用したデータをいくつか収集して解析すると、暗号化される前のデータを推測しやすくなるという特徴があるため、暗号鍵を毎回変化させる必要がある。しかし、WEPでは暗号鍵(WEPキー)が常に同じ設定キーと送受信フレーム毎に異なるIVの組合せで作られており、暗号鍵を毎回変更させる役割はIVが担っている。IVの長さは24ビットしかなく、例えば、スループットが5Mbpsのアクセスポイントでは、24ビットで組合せ可能なパケットが12時間程度で全部通過することを考慮すると、明らかに短いと言える。

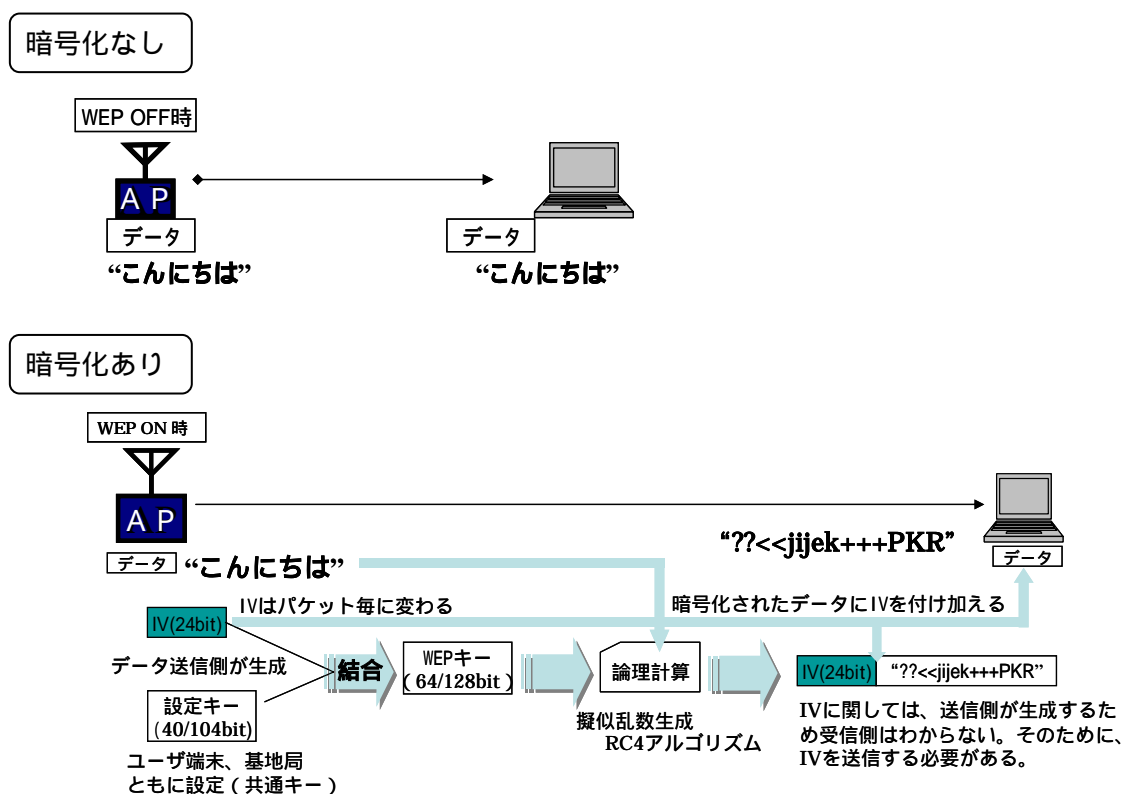


図 1 2 W E P の仕組み (設定キーが 40bit の場合)

(カ) W E P の設定方法

図 1 3 に W E P のアクセスポイントにおける設定例を示す (各社毎に設定画面は異なる。)。設定は、アクセスポイントと無線 L A N 端末両方に同じキーを設定する (設定キー)。図では、W E P キーの長さ 128bit 16 進数が選択されている。この場合、W E P キー (設定キーに相当) の部分には、104bit (*) = 26 バイト = 26 文字を入力する必要がある。また、図は W E P キーを 4 つ設定できるものであるが、実際に使用するのは一つであり、ユーザがどれを用いるかを指定することができる。もちろん、アクセスポイントと端末側はともに同じキーを設定する必要がある。

(*) ユーザが実際に設定するのは、IV の 24bit 部分を除いた部分になる。つまり、64bit の W E P キーを用いる場合は 40bit (5 文字)、128bit の W E P キーを用いる場合は 104bit (26 文字) を設定することとなる。

ステルス機能の利用	<input checked="" type="radio"/> 利用する <input type="radio"/> 利用しない
WEP暗号化設定	
WEPを利用する	<input checked="" type="radio"/>
WEPキー長	<input type="text" value="128bit 16進数"/> <div style="border: 1px solid black; padding: 2px; display: inline-block; margin-left: 10px;"> 128bit 16進数 64bit 16進数 128bit 16進数 64bit ASCII 128bit ASCII </div>
WEPキー1	<input type="text" value="1234567890abcdefghijklmnop"/> <div style="text-align: right; margin-top: -15px;">26文字</div>
WEPキー2	<input type="text"/>
WEPキー3	<input type="text"/>
WEPキー4	<input type="text"/>

図 1 3 アクセスポイントにおける設定例

イ SSID

IEEE802.11 では、無線 LAN におけるネットワーク識別子の一つとして SSID を利用している。SSID はいわゆるネットワーク名としての役割を果たす。

インフラストラクチャモードのネットワーク構成の場合、基本となる一つのアクセスポイントと、その配下の複数の無線 LAN 端末で構成されるネットワークを BSS (Basic Service Set) と呼ぶが、その際に使用する識別子を BSSID と呼ぶ。また、複数の BSS で構成されるネットワークのことを ESS と呼び、その際に使用される識別子を ESSID と呼ぶ (本資料では、特に記述がない場合、SSID はこの ESSID を指しているものとする。)。

SSID の設定は、意図しないネットワークに繋がらないようにするため、又は繋ぐものを識別するためのものである。つまり、アクセスポイントと無線 LAN 端末は同じ SSID を設定しないと接続が不可能になる。この機能を使ってある程度使用者を制限することができるが、アクセスポイントは Beacon と呼ばれるパケットデータを周期的に配信している。この Beacon パケットの中には、無線 LAN 端末が接続に必要なアクセスポイントの SSID 名が含まれているので、この電波が届く範囲の無線 LAN 端末にアクセスポイントの存在を知らせている。また、Windows XP や一部の設定ユーティリティソフトを使用することで、SSID 名を知ることができるので、第三者が無断で SSID を設定し使用してしまう可能性がある。さらに、ど

のアクセスポイントにも接続できる「ANY」接続という SSID を指定しない接続方法もある。無線 LAN 端末側が、SSID の設定欄を「ANY」や空欄にしておくと、すべての SSID で通信可能にするということになる。これは、公衆無線 LAN サービスを意識した仕様であると考えられるが、逆にいえば SSID を知らなくても「ANY」や空欄にしていればネットワークに接続できるということになる。これらの対策として、最近販売されているアクセスポイントの中には、SSID を隠蔽する機能(ステルス機能)を用いることができるものが出てきている。この機能は各社によって多少仕様が異なるが、基本的には SSID を表示しないようにするとともに、「ANY」や空欄で接続を行おうとする端末を拒否することができるようになっている。しかし、これらの手法を用いても、無線区間を飛び交うデータには必ず SSID が含まれているので、無線区間を飛び交うパケットをキャプチャすることで SSID を知ることはできる。このようなことから、SSID はアクセスポイントと無線 LAN 端末の集合を区分け(グループ化)するための単なる「文字列」でしかなく、不正なアクセスを確実に防ぐセキュリティ機能ではないという点は認識しておくべきである。

図 1 4 に SSID のアクセスポイントにおける設定例を示す。

SSID名	Wireless
使用チャンネル	6 ▼
データ転送速度 (Mbit/s)	自動 ▼

図 1 4 S S I D の設定例

ウ MAC アドレスフィルタリング

MAC アドレスとは、各通信機器の固有の ID 番号のことである。世界中の通信機器にはそれぞれ固有の番号が割り当てられており、この ID を元に各通信機器のデータの送受信が行われている。MAC アドレスは 16 進数で表された 12 桁の値で、上 6 桁(24 ビット)は IEEE 委員会で管理する固有の ID で、下 6 桁が各通信機器の連番となり、世界中で同じアドレスを持つ通信機器は存在しない。MAC アドレス認証とは、同じアドレスを持つ通信機器が存在しないという特徴を生かした認証方式である。MAC アドレスフィルタリングを有効にすると、アクセスポイントは無線 LAN

N端末の MAC アドレスとアクセスポイントの「MAC アドレスフィルタ設定」(ベンダーによって表示は異なる。)に登録されている MAC アドレスとを比較し、一致する MAC アドレスを持つ無線 LAN 端末のみ通信を行う。世界に唯一の ID 番号であるから、セキュリティ設定は一見万全のようにも見える。しかし、一部のユーティリティソフトを使用すると、通信している無線 LAN 端末の MAC アドレスを知ることができてしまう。そして、MAC アドレスを偽造するソフトもインターネットなどから無償で手に入られるため、SSID 同様、第三者が無断で設定し使用する可能性があるため堅牢なセキュリティ対策とは言えない。

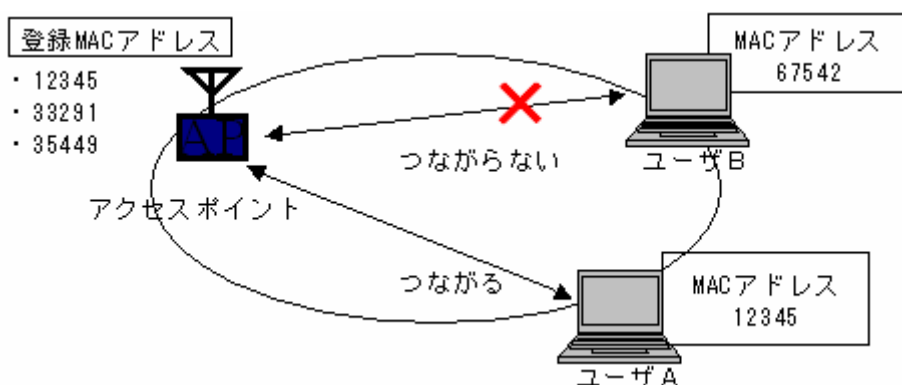


図 1 5 MAC アドレスフィルタリングの仕組み

図 1 6 に MAC アドレスフィルタリングにおける設定例を示す。設定はアクセスポイント側で行う。

MACアドレスフィルタを有効にする	はい <input checked="" type="checkbox"/> いいえ <input type="checkbox"/>
MACアドレス1	012345678900
MACアドレス2	345344478900
MACアドレス3	
MACアドレス4	
MACアドレス5	

図 1 6 MAC アドレスフィルタリングにおける設定例

エ まとめ

以上、無線 LAN における三つのセキュリティ技術を紹介した。家庭などで、無線 LAN を利用する場合、WEP を有効にし、MAC アドレスフィルタリングを行うことで、ある程度のセキュリティは確保できる。

(2) 無線 LAN のこれからのセキュリティ技術

無線 LAN の危険性として挙げられるものは主に二つある。ひとつは、勝手にアクセスポイントに繋がれてしまうこと、もうひとつは、通信中の電波を傍受され内容を読まれてしまうことである。こうした危険を防ぐために「IEEE802.1x」や「WPA」というセキュリティ規格が作られた。WPA は、WEP の弱点を補強した無線 LAN の暗号化方式の規格である。

ア IEEE802.1x

IEEE802.1x は、LAN スイッチなどネットワーク機器のポート単位でユーザ認証する手順を定めたものである。認証サーバを使ってユーザ認証を行う。WPA が登場する以前は、無線 LAN 製品のベンダーが独自に IEEE802.1x を認証の仕組みとして製品に実装させていたが、WPA では IEEE802.1x を標準機能として盛り込んだ。有線の場合は物理的な LAN ポートが、無線の場合はユーザが接続してきた時点で生成される論理的なポートが管理対象となる。また、IEEE802.1x にはさまざまな種類が存在している。

IEEE802.1x を使うためには、

IEEE802.1x 対応のユーザ端末 (Supplicant)

アクセスポイント (Authenticator)

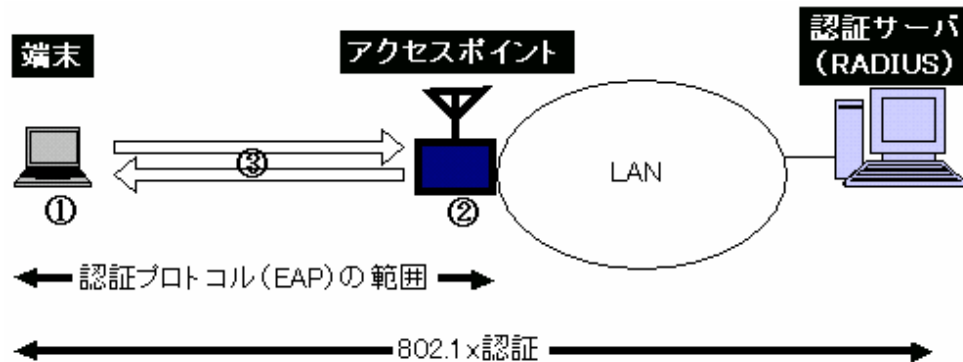
ユーザ ID やパスワードを管理する IEEE802.1x 対応の認証サーバ (RADIUS)

外部の認証局サーバ (CA : Certificate Authority)

などが必要である。

IEEE802.1x での基本構成を図 17 に示す。基本的に、IEEE802.1x では、アクセスポイントで認証プロトコルを終端し、アクセスポイントと認証サーバが別プロトコルで認証に必要な情報を送受信する。これで、ユーザから見れば、アクセスポイントがあたかも認証サーバとして働いているかのように見える。このように、認証プロトコルをアクセスポイントで終端しておけば、未認証のユーザがネットワーク側 (アクセスポイントより上流) にパケットを送出してしまうことを容易に防止す

ることが可能となる。



無線LAN端末は、認証が完了するまでパケットをLANに送出できない。
 アクセスポイントは、認証サーバ向けのフレーム・フォーマットに情報を載せてマルチプロトコルをサポートする。
 認証情報をEAPフレームでやり取りする。アクセスポイントでEAPプロトコルが終了するので、無線LAN端末からのパケットはLAN側に流れない。

図17 IEEE 802.1xのネットワーク構成

CAとは、申請者の公開鍵が申請者自身のものであることを証明し、その証明書を発行する機関のことである。CAを用いると、パスワードが不要なため安全だが、CAの設定と証明書の発行・管理が必要となる。図18には、クライアント及び認証サーバ両方に証明書が必要であるEAP-TTLの構成を示す。

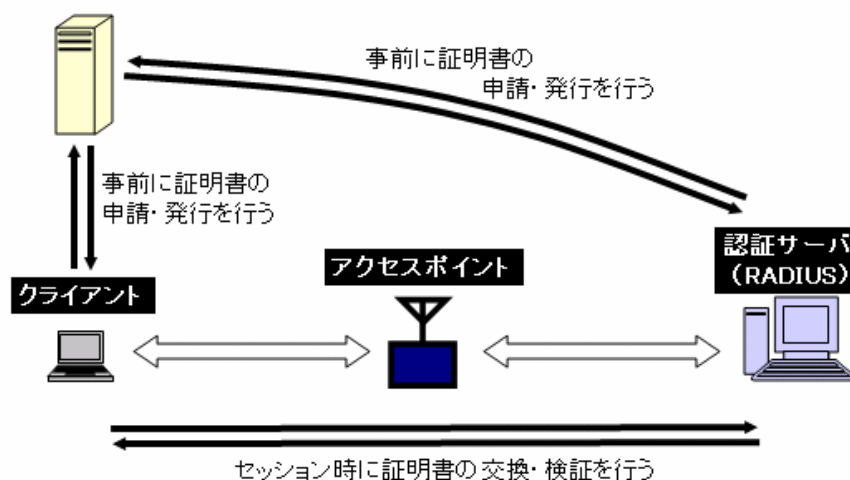


図18 CA(認証局)の役割

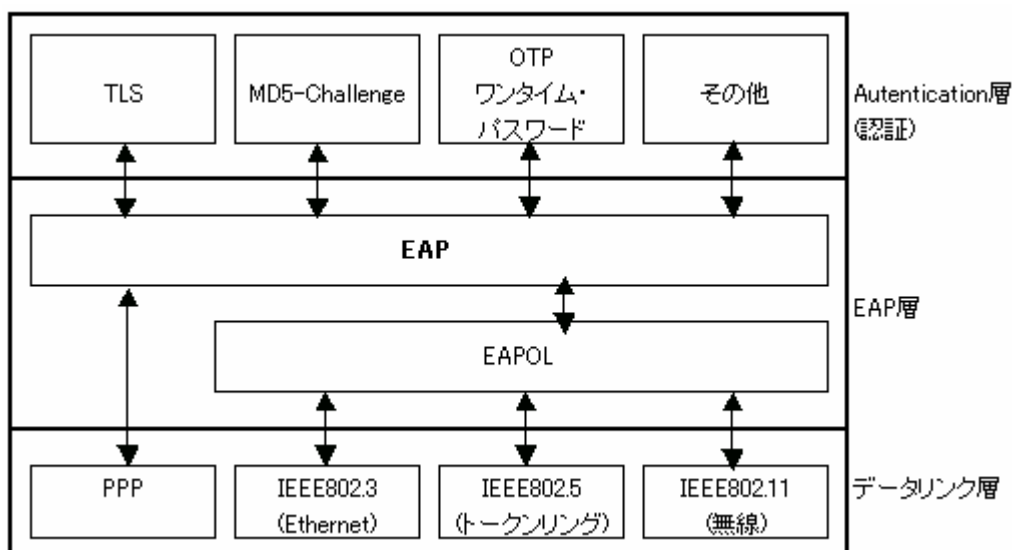
IEEE802.1x のプロトコルは、

「データリンク層」

「EAP (PPP Extensible Authentication Protocol) 層」

「Authentication 層」

という三つの階層に分けることができる。



* EAPOL (Extensible Authentication Protocol over LAN) :
LAN上に動作する拡張可能な認証プロトコル。IEEE802.1x に規定されている認証に使用する仕組みである。

図19 IEEE802.1xプロトコルスタック

EAP 層の役割は、Authentication 層で使用する認証プロトコルを選択できるようにすることである。認証プロトコルには、「TLS (Transport Layer Security)」、「MD5-Challenge」、「OTP (ワンタイムパスワード)」、「TTLS (Tunneled TLS)」、「PEAP (Protected EAP)」など様々な認証方式がある。IEEE802.1x の EAP 自体に認証機能はなく、具体的な認証手順や鍵の配送手順はすべて自由となっている。実際の認証手順、鍵の配送手順としては、「EAP-TLS」、「EAP-TTLS」、「PEAP」が有力である。

* MAC 層 (Media Access Control layer) :
OSI 参照モデルの第 2 層 (データリンク層) は、MAC 層と LLC 層に分かれており、MAC 層では各 LAN に特有な問題を扱い、LLC 層では複数の上位プロトコルがデータリンクを共有するためのフィールドを定義している。

表4 IEEE 802.1xの認証の種類

方式	認証方式	相互認証	WEPキー	対応端末 OS	端末設定	サーバ設定
EAP-TLS	証明書	あり	生成可	Windows XP、2000 SP4	証明書のインストール	証明書のインストール
EAP-TTLS	ID/パスワード	あり	生成可	主要各 OS (ファンクのスプリカントが必要)	容易	証明書のインストール
PEAP	ID/パスワード	あり	生成可	Windows XP、2000 SP4	容易	証明書のインストール
EAP-MD5	ID/パスワード	なし	固定	Windows XP (ただし SP1 では未対応)	容易	容易
LEAP	ID/パスワード	あり	生成可	主要各 OS (シスコシステムズのドライバが必要)	容易	容易

(7) EAP-TLS

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) は、証明書ベースの認証方式である。無線 LAN 端末と認証サーバの間で証明書の交換による双方向認証、暗号化アルゴリズムの選択、暗号鍵を安全に共有するための階層的な鍵の生成を行う。この方式で使われる認証サーバは CA (認証局) ではないため、認証サーバも CA から証明書の発行を受け、相互認証の片側として動作し、無線 LAN 端末と暗号化のための鍵を共有する。その後で、アクセスポイントに無線 LAN 端末と共有した鍵を配送する。

以下に EAP-TLS のシーケンスを示す。

最初にアクセスポイントを介して、RADIUS サーバに認証の要求信号が届くと、まず一往復 (無線 LAN 端末 - RADIUS サーバ間) があり、認証開始の信号を認証サーバと無線 LAN 端末が交換する。

Server Hello、Client Hello という情報要素の中で、random1、random2 という乱数を交換する。

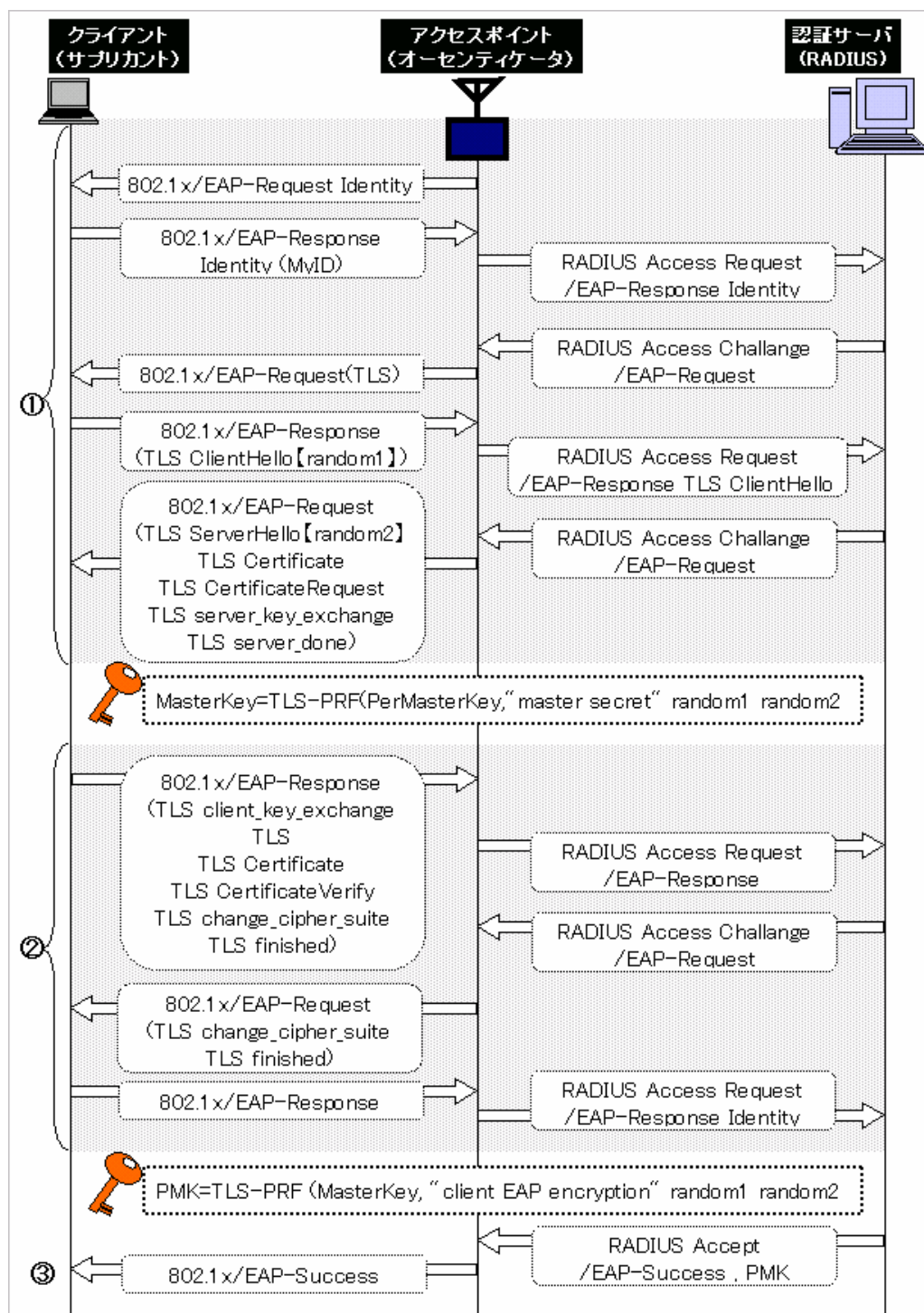
認証サーバから、証明書 (Server Certificate) と乱数 (Server Key Exchange に含まれる。random1、random2 とは別のもの) を送る。

無線 LAN 端末は、これを受信した後、乱数を発生し、client_key_exchange に含めてサーバへ送る。client_key_exchange と、server_key_exchange に含まれている乱数から Pre Master Key を算出し、TLS - PRF という関数で Pre Master Key と random1、random2 から、Master Key を算出する。認証サーバは自分の秘

密鍵でPre Master Keyを復号し、Pre Master Keyとrandom1、random2からMaster Keyを算出する。

認証が終わった後、両者はMASTER KEYをそのまま使わず、さらに情報交換を行いMASTER KEYを元にPair Wise Master Keyを作成し、これをアクセスポイントと無線LAN端末が共用する秘密鍵にする。以上で、アクセスポイントと無線LAN端末の鍵共有は完了する。

この方法はパスワードを用いない点で安全である。しかし、CAを設置する必要があるため、その分の追加費用が発生する上、各無線LAN端末側にも証明書が必要なため、手間がかかるなどの欠点もある。



図の見方

どの EAP 認証方式を用いるか決定する (ここでは EAP-TLS)。
 TLS ネゴシエーション
 暗号鍵が発行されて、暗号化セッションが開始される。

出典: 松江英明、守倉正博監修「802.11高速無線LAN教科書」(IDGジャパン、2003年)

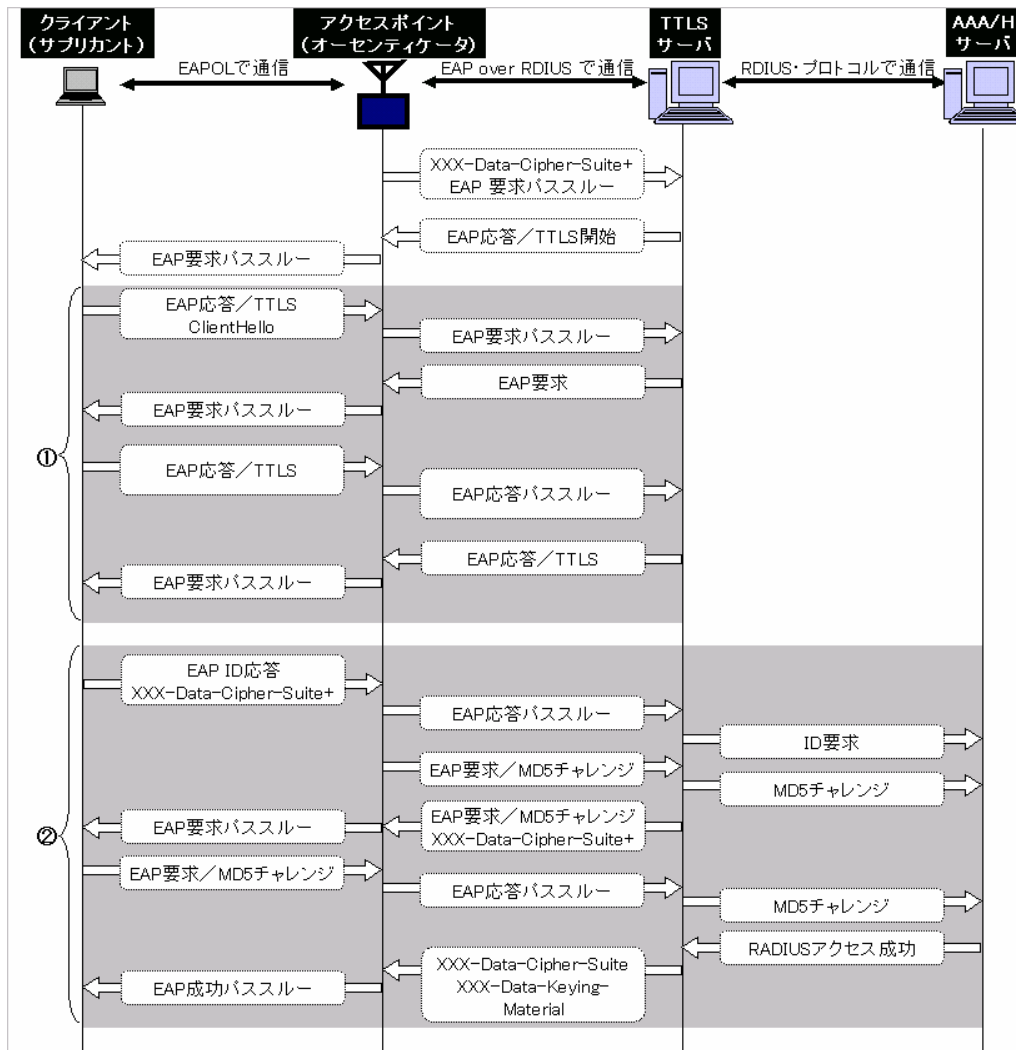
図 2 0 E A P - T L S のシーケンス

(1) EAP-TTLS及びPEAP

EAP-TTLS (Tunneled-TLS) と PEAP (Protected EAP) はほぼ同様の認証手順である。EAP-TTLS は、証明書運用がネックの EAP-TLS を改良し、無線 LAN 端末側の証明書の発行を不要とした認証方式である。さらに、そのアーキテクチャをベースとし、より軽い認証方式にしたものが PEAP である。

パスワードの認証は、EAP-TTLS、PEAP の両方とも、TTLS サーバ又は EAP サーバ (このサーバは PEAP の動作をするものではなく、単に EAP の処理をしているだけである。) から Certificate (証明書) を送り、無線 LAN 端末側から Client Key Exchange (無線 LAN 端末と TTLS サーバや EAP サーバとの通信の暗号化に用いられる鍵) を送り返してできた暗号化のトンネルで行われる (図 2 1 に描かれている「MD5 チャレンジ」などはそのための信号要素である。図 2 2 では、「EAP-Type = X」というメッセージでパスワードを送受信している。)。こうすることで、パスワードの受け渡しが暗号で保護される。認証を行った後の鍵の配送は EAP-TLS の場合と同じである。このように、サーバ側のみ証明書があればよいため、各無線 LAN 端末に証明書を発行する煩雑さを省略することができる。

なお、TTLS では、AAA/H (ユーザの認証が行われる「ホームドメイン」にある AAA (Authentication Authorization and Accounting) サーバ) までトンネル化されるが、PEAP では EAP サーバまでしかトンネル化されないため、TTLS サーバから AAA/H まで無線 LAN 端末と共有した鍵が配送されなければならない。これらのことから、PEAP は、AAA/H が送出した鍵が別の無線 LAN 端末から割り込まれて盗まれる危険性があることが指摘されている。



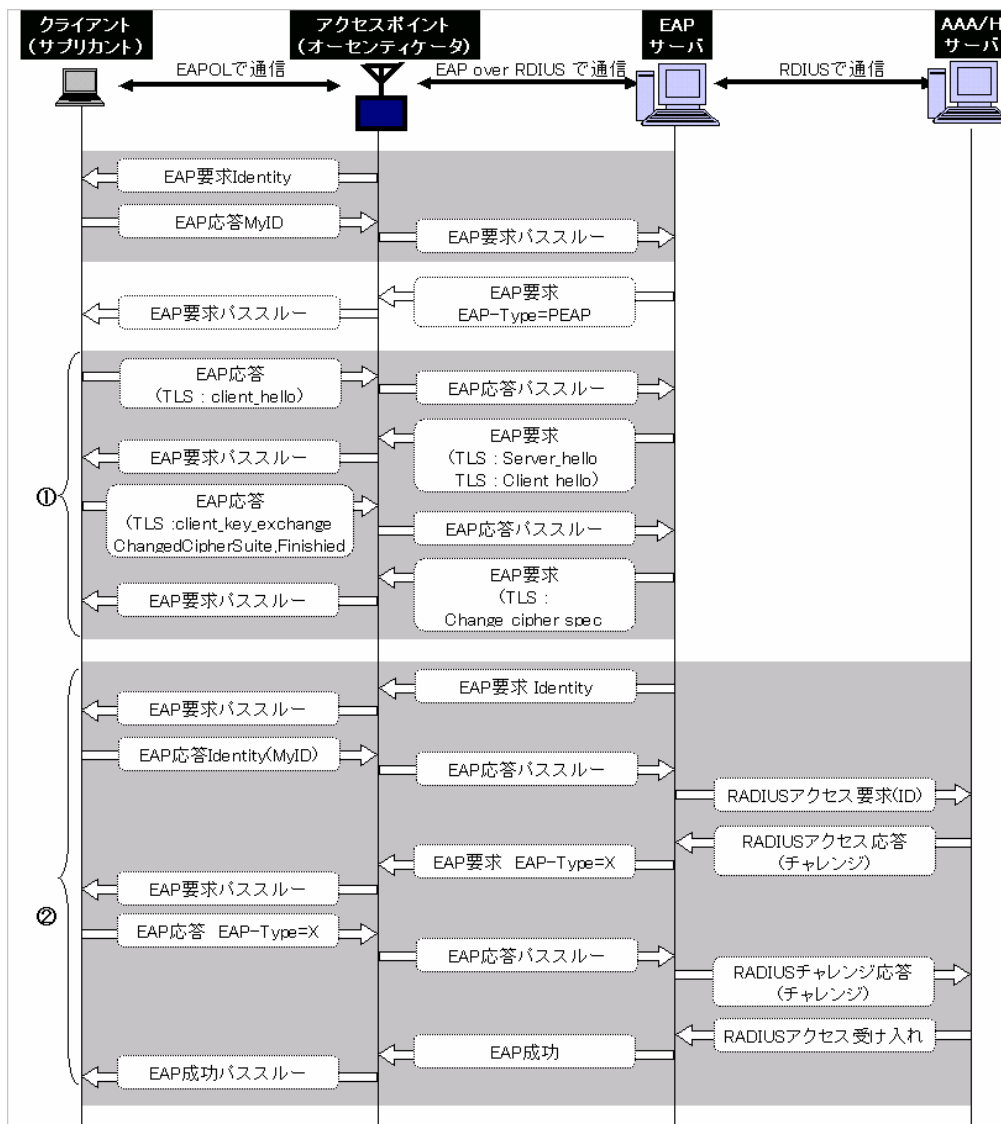
図の見方

TLS ネゴシエーション (サーバ証明書発行)

TLS トンネル (端末認証)

出典: 松江英明、守倉正博監修「802.11高速無線LAN教科書」(IDGジャパン、2003年)

図 2 1 EAP-TTLSのシーケンス



図の見方

TLS ネゴシエーション (サーバ証明書発行)

TLS トンネル (端末認証)

出典: 松江英明、守倉正博監修「802.11高速無線LAN教科書」(IDGジャパン、2003年)

図 2 2 P E A P のシーケンス

(ウ) E A P - M D 5 (EAP-Message Digest 5)

ユーザ ID とパスワードによる接続認証方式で、認証には MD5 によるハッシュを使用する。MD5 は、どんな文字列でもメッセージを 16 バイト単位のビット列(これをハッシュ符号と言う。)の演算結果になるようなアルゴリズムである。

MD5 は、無線 LAN 端末及び認証サーバの両方に電子証明を必要としないため

実装が容易になり管理しやすい。しかし、無線 LAN 端末のみを認証する片方向認証であり、WEP キーの自動生成を行うことができないため、暗号解読によるデータ漏洩には脆弱な面がある。

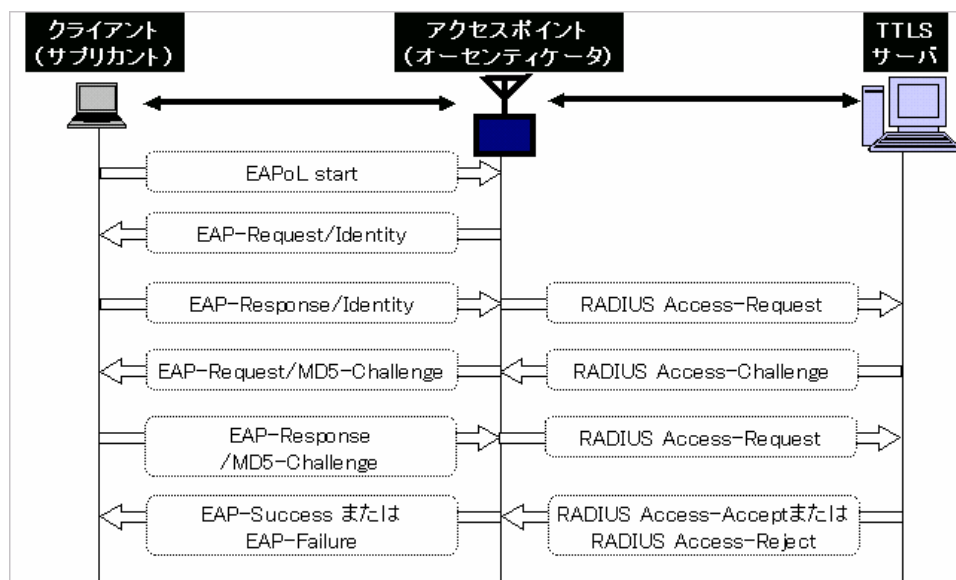


図 2 3 E A P - M D 5 のシーケンス

(I) L E A P (Lightweight EAP)

米シスコシステムズ社独自の認証プロトコル。ユーザ ID、パスワードによる、サーバと端末の双方向認証方式である。使用する際は、Cisco クライアントソフトあるいは Cisco Compatible eXtensions プログラムにて認定された内蔵無線 LAN パソコン及び対応クライアントソフトが必要である。なお、総当たり攻撃等に弱いという脆弱性があるとの報告がされている。

イ W P A (Wi-Fi Protected Access)

WEPの弱点を補強する新たな規格としてWi-Fi AllianceによりWPAが規定された。WPA は、ひとつの技術によるセキュリティ機能ではなく、複数のセキュリティ規格の総称である。無線 LAN でユーザ認証を行う「IEEE802.1x」、新しい暗号化方式である「TKIP」が規定されている。この方式は、WEP に比べて高いセキュリティ機能を持ち、WEP と同じ技術で実現可能である。

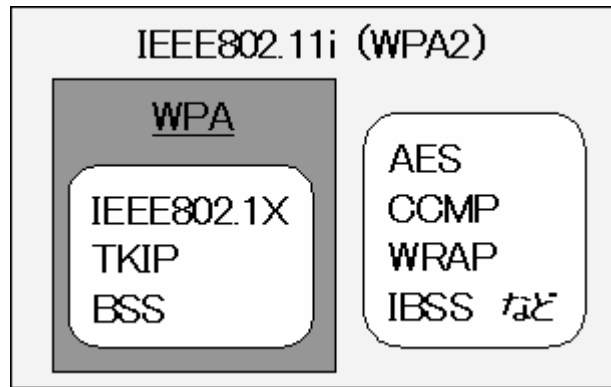


図24 WPAとIEEE802.1xの関係

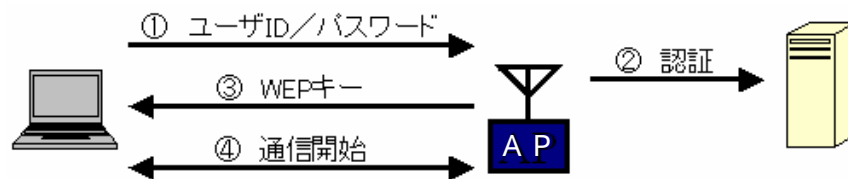
この WPA には大きく分けて、企業又は公衆無線 LAN 事業者向けの「EAP (Extensible Authentication Protocol) モード」と、SOHO (小規模事業所) 及び一般家庭向けの「PSK (Pre-Shared Key) モード」の 2 種類がある。

EAP モード

EAP モードでは、IEEE802.1x と RADIUS サーバを利用してユーザの個別認証を実現している。認証プロトコルとしては EAP が採用されている。

WPA では無線 LAN 端末がアクセスポイントに接続するとき、最初の段階では認証プロトコル以外のトラフィックが遮断されている。このため、無線 LAN 端末は EAP を使って自分の ID とパスワードなどをアクセスポイントに送信して認証を試みる。アクセスポイントはこの通信を受け取ると、これを RADIUS サーバへ転送し、そこで認証を行う。そして、認証成功の場合は、暗号に用いるマスター鍵など接続に必要な情報が無線 LAN 端末に渡される。これにより、WEP ではできなかったユーザの個別認証やユーザ毎の異なる鍵の安全な配信が可能になる。

企業ユーザや公衆無線 LAN サービス事業者は、RADIUS サーバを使った IEEE802.1x により EAP による認証を行い、秘密鍵を共有することが推奨されている。



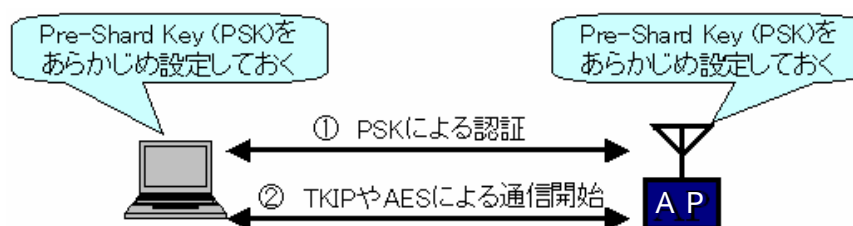
IEEE802.1x によるユーザ認証と、WEP キーの配送が可能

図25 EAPモード

PSK モード

一般的に RADIUS 認証などの大掛かりな手段を家庭で用いることは難しく、SOHO ユーザが用いることを想定して作られたものが PSK モードである。PSK モードは、RADIUS サーバを必要としない、PSK と呼ばれる共通鍵によって無線 LAN 端末を認証する機能である。アクセスポイントと、これと通信を行うすべての無線 LAN 端末に共通の文字列(パスフレーズ(*))を登録しておき、パスフレーズより生成される PSK が認証時に利用される。即ち、アクセスポイントと端末の PSK が同一ならば認証され、異なれば認証されないということである。

(*)パスフレーズ： WPA では、パスフレーズは最小 8 文字、最大 63 文字の ASCII 文字列と定義されている。WPA で定められたアルゴリズムに基づき、パスフレーズから自動的に 128bit の PSK が生成される(一般に文字数が多い場合、パスワードと区別してパスフレーズと呼ぶ。)



無線 LAN 端末とアクセスポイントに PSK を設定することにより認証が可能

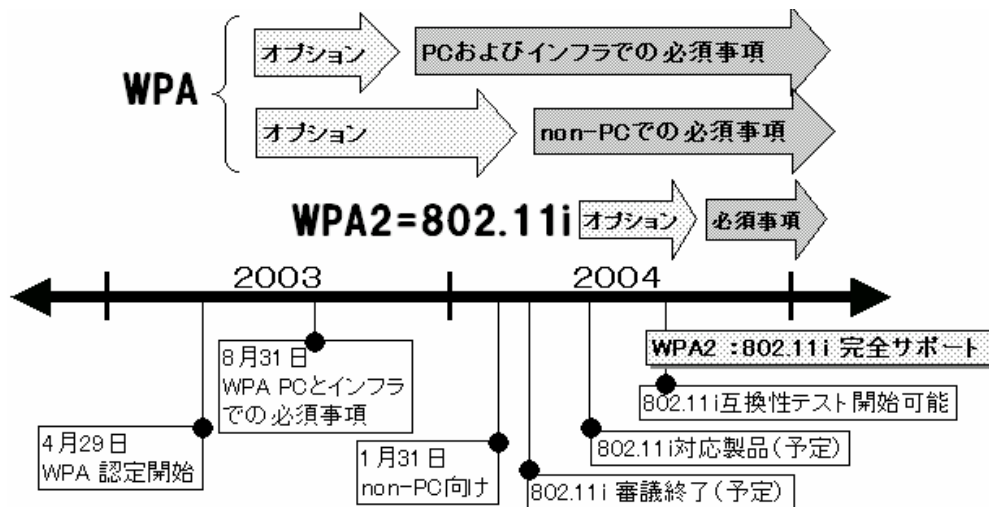
図 2 6 P S K モード

表 5 E A P モードと P S K モードの比較

	EAP モード	PSK モード
対象	企業又は 公衆無線 LAN 事業者向け	SOHO 及び一般家庭向け
RADIUS サーバ	必要	不要
暗号鍵生成	TKIP (アルゴリズムは RC4)	TKIP (アルゴリズムは RC4)
暗号鍵生成 (オプション扱い)	AES (アルゴリズムは Rijndael)	AES (アルゴリズムは Rijndael)
認証	IEEE802.1x	Pre-Shared キー

WPAは、IEEE802.11i Draft3.0の一部をWi-Fi Allianceが標準化した規格である。これは、IEEE802.11i の策定に時間を要する中、WEP の脆弱性を克服する新しいセキュリティ規格の早期導入ニーズを踏まえ策定されたものである。

将来的には、IEEE802.11i をフルサポートした「WPA2」も予定されている。WPA から WPA2 への移行は容易に行えるようになっている上、WPA2 は、WPA と WPA2 の両方をサポートする「ミックスモード」も提供する。



Wi-Fi is everywhere! Wi-Fi アライアンスのご紹介 (Wi-Fi Alliance) より

図 2 7 セキュリティのロードマップ

(ア) T K I P (Temporal Key Integrity Protocol)

WPA は、WEP の問題点である、

鍵を交換できない

IV の中には解読に利用されやすいものがある

という脆弱性を新しい暗号化プロトコルである「TKIP」を利用することにより補っている。

TKIP では、既存の WEP 製品がドライバやファームウェアを更新するだけで対応できるよう、暗号化アルゴリズム自体は WEP と同じ「RC4」が使われている。ただし、暗号化アルゴリズムを変えずに暗号強度を強化するために、暗号鍵として使われるシードの作り方に特徴を持たせた。シードは、

「IV (Initialization Vector) 」

「一時鍵 (TK: Temporal Key) 」

「無線LANカードのMACアドレス」

の三つのデータを基に生成される。TKIPの暗号鍵(シード)生成方法を図28に示す。

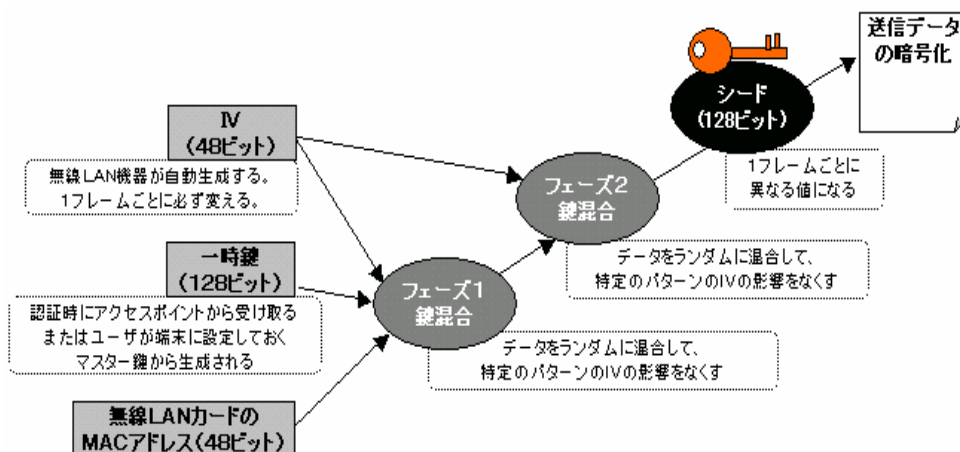


図28 TKIPの暗号鍵(シード)生成方法

TKIPで用いられるIVは、WEPが24bitであったのに対し、2倍の48bitに拡張された。これにより、同じIVのフレームが現れるタイミングは、WEPの場合と比べると約1700万倍にもなり、事実上同じフレームが送信されるという心配はない。その上、フレーム毎にIVの値が必ず変わるように、その値がインクリメント(値を1ずつ増加)され、同一のIVで暗号化されることはない。一時鍵は、WEPでユーザが設定する暗号鍵に相当するものである。TKIPが使用するシーズは、無線LAN端末とアクセスポイントで共通な128ビットの一時鍵(EAPモードでは鍵配送されたマスター鍵、PSKモードではPSK)を基にして生成される。一時鍵と従来のIVを混合して鍵を作成(フェーズ1)した後、その鍵にさらにIVの拡張された部分を混合して鍵を作成(フェーズ2)し、この鍵で平文を暗号化するという二重の鍵混合プロセスを採用することにより、パケット毎に異なる鍵で暗号化でき、パケット毎に使われる鍵の不規則性を高めて暗号解読のヒントになるようなIVが登場しないようにも工夫されている。TKIPでは、暗号化アルゴリズムではなく、暗号化のプロセスを強化することによって、より高い安全性が実現されている。シーズの生成には、ユーザのMACアドレスが使用されるため、すべてのユーザで異なるシードが使われるようになる。

(イ) MIC (Message Integrity Check)

MICはWPAで採用された、データの改ざんを検出するためのハッシュ値である。このハッシュ値を求めるために「ハッシュ関数」が用いられる。元データにハッシュ関数を用いて計算すると固定長のビット列ができる。元データが1ビットでも変わると、このハッシュ値も変わってしまう。ハッシュ関数には、不可逆な一方方向関数が含まれるため、ハッシュ値から元のデータを再現することはできない。また、異なるデータ(意味のあるデータ)が同じハッシュ値になることはまずない。このことにより、データの完全性をチェックすることができる。

(ウ) AES (Advanced Encryption Standard : 高度暗号標準)

WPA のオプションである AES は米国政府が使用する暗号方式として、NIST (National Institute of Standards and Technology : 米標準技術局) で標準化された暗号化方式であり、「Rijndael」という秘密鍵暗号化アルゴリズムが使われている。この方式は、ハードウェア処理を行わないと、54Mbps という IEEE802.11a の通信速度に対応できない。

AES で使われている「Rijndael」は、高い安全性と速度、プラットフォームに依存しない性能、消費電力などの面で、非常にバランスの取れたアルゴリズムである。

CCMP (Counter mode with CBC-MAC [Cipher-Block Chaining-Message Authentication Code]) は、AES で改ざんを検出するプロトコルである。IEEE802.11i では、AES を採用した通信方式として、CCMP が必須とされている(TKIP はオプション扱いである。)。

CCMP では、暗号化に使われるのと同じ鍵が用いられ、データの暗号化(Counter mode と呼ばれる方法での暗号化)と並行して CBC-MAC という方式で改ざん検出符号化を行い(アルゴリズムは AES)、MIC フィールドに出力する。

表6 CCMP、TKIPの比較

	CCMP	TKIP
暗号方式	AES	RC4
鍵長	104bit 暗号化 64bit 認証	128bit
IV	48bit	48bit

ウ IEEE802.11i

現在、標準化に向けて策定中の無線 LAN セキュリティ規格。認証に IEEE802.1x を、暗号化には TKIP に加えて米国商務省標準技術局によって次世代標準暗号化方式にも選ばれている AES を採用することが決まっている。IEEE802.1x のうち、どの方式を標準とするかまでは規定しない。

(3) その他のセキュリティ

無線 LAN 用に策定されたセキュリティ規格以外に、有線 LAN におけるセキュリティを確保する方法も広く使われている。

ア SSL (Secure Sockets Layer)

SSL は、通信データの暗号化と認証を行うことにより、通信の盗聴や改ざん、なりすましを防止するためのプロトコルである。

SSL では、暗号化と復号化に同じ鍵を使う共通鍵暗号方式が使われている。通信を行うサーバ間で同じ種類の鍵を共有して暗号化と復号化を行う。暗号化通信を始めるときに互いに相手を認証する（片方のみ認証する場合もある。）と同時に、そのセッションで使う共通鍵を受け渡す。このセッションを盗聴しても共通鍵がわからないように、共通鍵は公開鍵暗号方式という別の方法で暗号化されて受け渡される。公開鍵暗号方式は、秘密鍵と公開鍵という対になった二種類の鍵を使う。これらは全く違う符号列でできた鍵である。

SSL のデータ通信で使われる共通鍵は、公開鍵で暗号化される。公開鍵で暗号化したデータは、公開鍵と対となっている秘密鍵でしか復号化できない。しかし、秘密鍵はサーバそれぞれが各自持っているものなので、ネットワーク上を流れることはない。そのため、この秘密鍵を奪われない限り、データを解読することはできない。さらに、共通鍵はセッション毎の使い捨てなので、通信が終わると同時に無効となる。

現在、クレジットカード番号や個人情報を扱うホームページの多くは、通信途中での傍受やなりすましを防ぐ目的で SSL を利用している。IE (Internet Explorer) や Netscape などの SSL に対応した Web ブラウザを利用して SSL で保護されたサイトに接続すると、通信相手の認証が行われ、通信データが自動的に暗号化される。このとき、Web ブラウザのステータス欄には鍵のマークが表示される。

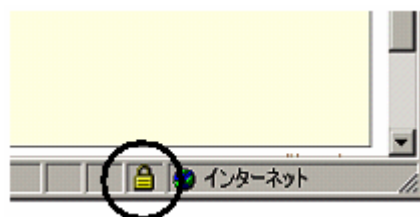


図 2 9 Internet Explorer のステータス欄の鍵マーク

イ VPN (Virtual Private Network)

VPN は、インターネットや IP ネットワークを仮想的にプライベートなネットワークとして利用するための、「認証」、「暗号化」及び「カプセル化」が組み合わされてできた技術である。

インターネットなどのパブリックなネットワークは、コスト面では非常に安いので容易に導入できる。しかし、パブリックであるがゆえに、経路途中での盗聴や改ざん、なりすましなどセキュリティ面での問題点が多いのも事実である。従来、遠隔地にある企業の本社、支社にそれぞれ施設されている LAN 同士を接続するには専用線などを利用していった。しかし、専用線は、帯域と遅延時間は保証されるが、二点間の距離と回線速度によりコストが上がり、一対一の接続のため複数の拠点と接続する場合かなりのコスト高となってしまう。そこで、インターネットなどのパブリックなネットワークを利用し、接続距離とは無関係に遠隔地の LAN 間接続を行う方法が考え出された。その一つが VPN である。

VPN では、大きく分けて、企業の本社 - 支社などを結ぶための「LAN 間接続 VPN」と、自宅や公衆無線 LAN などから社内 LAN などへアクセスするための「リモートアクセス VPN」がある。

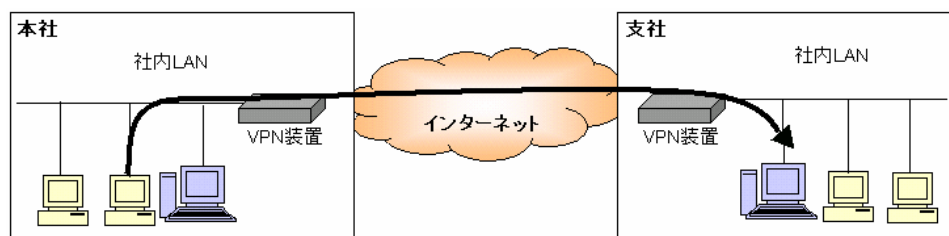


図 3 0 LAN 間接続 VPN

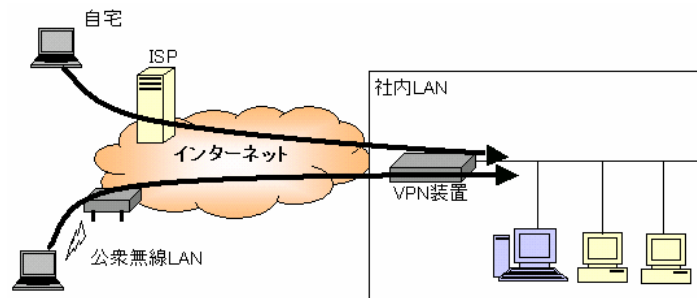


図 3 1 リモートアクセスVPN

現在、VPN を実現する際に利用される技術として、以下のような技術がある。

L2TP (Layer2 Tunneling Protocol)

PPTP (Point to Point Tunneling Protocol)

IPsec (Security Architecture for Internet Protocol)

SSL (Secure Sockets Layer)

* IP カプセル化： データパケットを IP ヘッダで包み込むこと。異なる通信プロトコルなどでも円滑に通信できるようにするための技術。

* トンネリング： 本来通信を行いたいプロトコルの環境の上に、異なる通信プロトコルを透過的に設定することにより通信を行う。

(ア) L 2 T P (Layer2 Tunneling Protocol)

データリンク層で PPP 通信をトンネリングするためのプロトコル。

L2TP は、PPTP (Point to Point Tunneling Protocol) と L2F (Layer 2 Forwarding) を統合して IETF により標準化されたレイヤ 2 トンネリング・プロトコルである。PPTP のトンネル制御部分と L2F のフレーム構造を組み合わせたような作りになっている。L2TP は、PPTP の PAC と PNS に相当する LAC (L2TP Access Concentrator) と LNS (L2TP Network Server) の間に仮想トンネルを構築する。制御チャンネルとトンネルは、L2F と同様に UDP (ポート 1701) を使う。PPTP は、IP ネットワーク上でのみ利用可能だが、L2TP は IP 以外の ATM やフレーム・リレー上での利用が可能である。また L2TP は、PPTP にはないトンネルを構築する際の認証手段を持つ。さらに、L2TP では一つの仮想トンネルで同時に複数のユーザとやりとりすることができる。L2TP は PPTP と同様にデータを暗号化する機能がないため、IPsec などの暗号化技術を組み合わせて利用されることが多い。

(イ) P P T P (Point to Point Tunneling Protocol)

米マイクロソフト社によって提案された暗号通信プロトコル。

データを IP カプセル化すると同時に、付加した IP ヘッダにユーザ認証用のデータを埋め込んでやり取りする。このため、インターネットを介して接続する場合でもエンドポイント間でユーザ認証を実現できる。Windows 環境でのみ利用可能である。

(ウ) I P s e c (Security Architecture for Internet Protocol)

ネットワーク層での暗号化と認証を行う、TCP/IP 環境で汎用的に用いることができる IETF により標準化されたセキュリティ技術である。IP パケット自体に認証用のヘッダと暗号化したデータを格納している。IPsec は、現在広く使われている IPv4 の後継として開発された次世代の IP プロトコルである IPv6 では標準でサポートされている。

IP を使った通信であれば、利用するアプリケーションは問われない。しかし、IPsec は、IP パケットに特化して設計されているため、IP パケット以外 (IPX、NetBIOS など) のパケットを転送することはできない。IPsec では、暗号化と認証の仕様に複数のプロトコルが使用されており、データが改ざんされていないことなども保証されている。

IPsec では、認証・暗号化・カプセル化の三つの機能を提供している。通信手順としては、

- 対向の VPN 装置が正しい相手かどうかを確認するための認証
- データを暗号化するための暗号鍵の決定
- データの暗号化 / カプセル化
- カプセル化したデータの送信

という順である。 、 は、実際のデータを送受信する前の準備にあたる。この段階では、通信としては VPN を使わないで情報のやりとりを行う。IPsec で鍵交換や暗号化に利用される代表的なプロトコルを表 7 に示す。

表 7 I P s e c に利用される代表的なプロトコル

プロトコル	説明
IKE (Internet Key Exchange)	暗号化に用いられる共通鍵を VPN 装置間で交換する
ESP (Encapsulating Security Payload)	データの認証と完全性、暗号化による機密性の機能を提供する
AH (Authentication Header)	データの認証と完全性の機能を提供する データの暗号化は行わない

IKE (Internet Key Exchange)

データを暗号化するための鍵交換の Protokol はいくつか存在するが、IPsec では「ISAKMP/Oakley」という鍵交換 Protokol を基にして作られた IKE を標準としている。これは、鍵交換を含めた SA (Security Association) の合意を自動的に行う一連の手順を決めたものである。SA とはセキュリティ Protokol で接続が保護された状態のことを指す。SA は手動で設定しておくことも可能であるが、暗号化通信の安全性をより向上させるために、暗号鍵を定期的に変えることが重要であるため、管理が容易に行えるよう、IKE で自動的に SA を変えるほうが望ましい。

IPsec は、鍵交換が完了して初めて暗号化が有効となるので、IKE 自体に IPsec を使うことはできない。IKE 自体の暗号化通信のためにさらに IKE 用の鍵交換手順が定められており、このため IKE はフェーズ 1、フェーズ 2 の 2 段階で鍵交換を行うことになる。

フェーズ 1 の目的は、IPsec 通信を行うための前段階として ISAKMP SA を確立させることである。フェーズ 2 で利用する暗号化アルゴリズムを決定し、暗号鍵を生成する。この暗号鍵の生成には、DH (Diffie-Hellman) というアルゴリズムを用いて通信相手同士で同じ鍵を作成する。DH では、鍵の素材となる乱数を双方が送りあうことによって、結果的に双方が同じ暗号鍵を生成することができ、通信内容を第三者に盗聴されても直ちに秘密鍵を知られることはなく、安全に鍵情報を交換することができる。このようにして SA を確立させることで安全性の高い通信環境が整う。

フェーズ 2 では、IPsec の SA を確立させるための情報を交換する。ここでの通信には、フェーズ 1 で共有された暗号鍵を使う。暗号化アルゴリズムの決定、暗号鍵の交換など、IPsec による通信に必要な情報がやり取りされた上でデータの暗号化通信が行えるようになる。

ESP (Encapsulating Security Payload)

ESP は、暗号化と認証の機能を持つ。ESP は、IP パケットのペイロード部分の暗号化を行い、暗号化されたペイロードを含む IP パケットの特定の部分をハッシュ値化して認証情報を加える。データ部分は暗号化されている上に、認証機能によってデータが改ざんされていないことが保証されている。

ESP には、トランスポートモードとトンネルモードという二つのモードがある。トランスポートモードでは、IP パケットのペイロード部を暗号化して相手に転送する。トンネルモードでは、IP ヘッダを含む IP パケット全体を暗号化し、ネットワーク層でカプセル化して相手側のネットワークに届ける。一般的に VPN ではトンネルモードが使われる。IPsec は、VPN のためだけに設計されたものではなく、あくまで IP パケットのセキュリティに関して作られたものであるため、二つのモードが存在している。



図 3 2 トランスポートモード

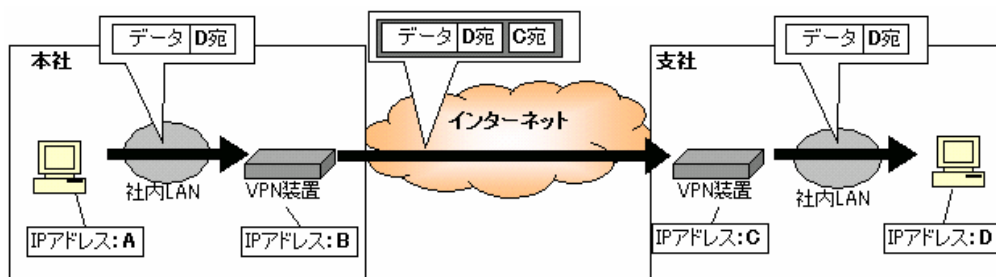


図 3 3 トンネルモード

AH (Authentication Header)

AH は、IP パケットの認証ヘッダ(オプション)である。1998 年 11 月に IPsec V2 (IPsec Version 2) が制定される以前は、ESP の送信元確認機能が弱かったため、ESP と AH の両者を組み合わせる場合もあったが、IPsec V2 で送信元確認機能が改善されたため、現在の実装では ESP を利用している。

AH は、安全性の保証と認証のための技術である。ESP のようなデータの暗号化機能は提供されない。パケットのほぼ全体を対象とする ICV (Integrity Check Vector : 完全性保証用認証値) を付加することで、IP ヘッダまで含めたパケットのほぼ全体の完全性を保証する。したがって、転送されたメッセージが改ざ

んされていないことだけでなく、IP ヘッダにある送信元アドレスやあて先アドレスが転送中に変更されていないことも受信側で確認できる。

表8 ESP、AHの提供するセキュリティ機能

	ESP	AH
秘密性	元のパケットの内容を暗号化して秘密にする	秘密性は提供されない パケットは暗号化されないため、盗聴者はパケットの中身を見ることができる
認証 (本人性確認)	そのパケットが本当にその送信元から届いたことを、限定的な範囲で保証できる	IP ヘッダまで含めて認証するため、そのパケットが本当にその送信元から届いたことを保証できる
認証 (完全性保証)	パケットが改ざんされていないことを保証できる	パケットが改ざんされていないことを保証できる
アクセス制御	設定に従ってパケットをフィルタリングすることができる	設定に従ってパケットをフィルタリングすることができる

ウ SSL-VPN

SSL-VPN とは、インターネットで広く使われている暗号化プロトコルである SSL を利用して、VPN を実現する技術である。

クライアントと SSL VPN ゲートウェイの間の通信を HTTPS プロトコルで暗号化し、リバースプロキシを使って内部のネットワークへ接続する。リバースプロキシとは、プロキシサーバ(この場合は SSL VPN ゲートウェイ)が社外にある PC の代理として社内の各アプリケーションにアクセスするものである。

SSL-VPN によって、社員が自宅から会社のネットワークに接続したり、関連企業のネットワークに接続したりして、安全に業務を遂行できる。

SSL は、前述のとおり、Web サーバとブラウザ間の通信を安全にするために作られたプロトコルである。SSL は、セッション層より上位のアプリケーション毎に暗号化を行う必要がある。HTTP や Telnet、POP3、SMTP などトランスポート層で TCP を使うアプリケーションが利用できる。

端末の環境としては、多くの Web ブラウザが始めから SSL に対応しているため安定した動作が期待できる。また、SSL-VPN はアクセスするサーバやアプリケーション、ユーザやグループ単位で容易に制限をかけることができる。こういったことから、運用管理面から見ても容易に SSL-VPN を実現することが可能である (SSL 未対

応のアプリケーションで SSL-VPN を実現させるには、Java アプレットや ActiveX コントロール、SOCKS などを利用する。)。

表9 IPsec と SSL の比較

	IPsec	SSL
OSI 参照モデル	ネットワーク層	セッション層
暗号化できるアプリケーション	IP で動作するアプリケーションすべて	TCP で通信するアプリケーション (制限あり)
端末環境	専用クライアントソフトが必要	Web ブラウザのみで通信可能
利用用途	L A N 間接続、リモートアクセス	リモートアクセス
アクセス制限	しにくい	しやすい

TCP/IP	OSI 参照モデル	
	アプリケーション層	
アプリケーション層	プレゼンテーション層	
	セッション層	SSL-VPN
トランスポート層	トランスポート層	
インターネット層	ネットワーク層	IPsec-VPN
ネットワーク インターフェイス層	データリンク層	
	物理層	