第７章 無線 LAN

7.1 無線 LAN の概要

無線 LAN は煩わしいケーブリングを必要とせず，物理的に配線が不可能な環境であっても使用できるなど利便性の高い通信形態であるが，一方ではセキュリティの維持が難しく，使い方を誤ると思わぬトラブルに巻き込まれる恐れもあり，注意が必要である。

近年では，屋外におけるホットスポット（無線 LAN が使用可能なエリア）の数も急増し，将来的には全ての携帯電話が無線 LAN を通してインターネットに直接接続する計画になっているなど，一般社会にも広く浸透し始めている。

技術革新の速度も速く，新たな機能の追加や，セキュリティホールの発見なども短期間に起こる可能性もあり，注意を怠ってはいけない分野であると言える。

なお，ここでの解説は IEEE802.11 シリーズの無線 LAN 規格について行う。無線通信規格である Bluetooth（ブルーツゥース）や赤外線通信についてはここでは取り扱わない。

7.2 無線 LAN 規格（IEEE802.11 シリーズ）

主な無線 LAN の規格（IEEE802.11 シリーズ）を以下に挙げる。

・IEEE802.11b

802.11b で使用される 2.4GHz 帯は **ISM**（Industry Science Medical band）**バンド**と呼ばれ，免許不要で様々な目的で利用可な周波数帯である。そのため 802.11b は同じ周波数帯を使用している電子レンジや Bluetooth などと電波干渉を起こしやすい。

5MHz ごとの間隔で 13 個のチャンネルと 802.11b 専用の 1 チャンネルを持つが，チャンネルの幅は約 22MHz であるため，チャンネル同士は重なり合って配置されていることになる。従って，隣り合わせのチャンネルは干渉を起こし易く，干渉を完全に防ぐには 4 つ以上のチャンネル間隔を空ける必要がある（図 7.1 チャンネルの区分は国によって異なる）。

速度レートも最大 11Mbps と低速であり，現在では殆ど使用される事はない。

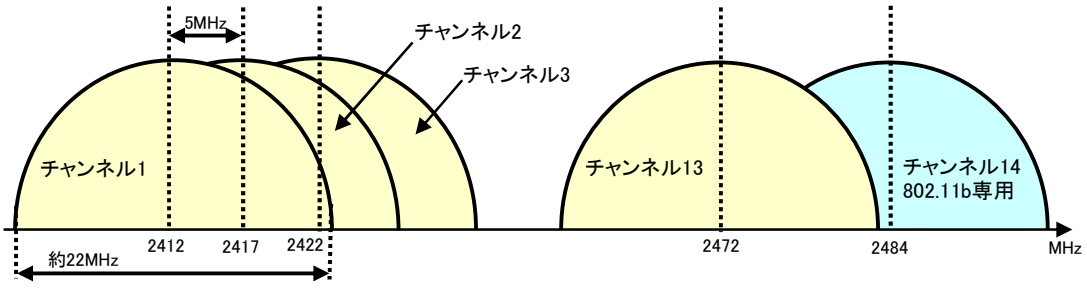


図 7.1 IEEE802.11b/g のチャンネル帯域

・IEEE802.11g

802.11b の上位互換規格であり，802.11b と同じ周波数帯域とチャンネルを使用する（図 7.1 ただしチャンネル 14 は使用しない)。従って，802.11b と混在させることも可能だが，802.11b と同様に電子レンジや Bluetooth などと電波干渉を起こし易い。最大通信レートは 54Mbps である。

・IEEE802.11a

802.11b/g とは互換性のない規格である。5GHz の周波数帯を使用し，802.11g と同じ最大 54Mbps の通信レートを実現する。

5GHz 帯の周波数帯には W52(5.2GHz 帯)，W53(5.3GHz 帯)，W56(5.6GHz 帯)，W58(5.8GHz 帯)のチャンネルグループが存在する（日本では現行 W58 は使用不可)。使用するチャンネルは完全に分離しており，チャンネル間の干渉は発生しない。電子レンジや Bluetooth などとの電波干渉も少ない。ただし，W53,W56 は気象レーダーと干渉する恐れがある。また W52,W53 のチャンネルグループの屋外使用は，基本的に日本では禁止されている（W52 は条件付きで可)。

・IEEE802.11n

802.11a/g に続く高速無線 LAN 規格であり，2009 年 9 月に策定された。複数アンテナで送受信を多重化する **MIMO**（マイモ：Multiple Input Multiple Output）技術を利用し，802.11a/b/g との互換性を保ちながら 100Mbps 超の通信速度を実現する規格である。

・IEEE802.11ac

高速無線 LAN 規格. 2014 年 1 月に策定。 5 GHz 帯を使用し，最大通信レートの理論値 6.9Gbps と高速である。ただし最大理論値は 8 ストリームを使用時の値である。日本では殆どの場合，AP は 4 ストリーム（2167Mbps)，クライアントでは 2 ストリーム（867Mbps）が使用される。

・IEEE802.11ad

11ac より約 1 年早く策定された（2012 年 12 月)。60GHz 帯を使用し，最大通信レートの理論値は 6.8Gbps。 ただし現状ではそれほど普及していない。

・IEEE802.11ax

2.4/5/6GHz 帯を使用し，最大の通信レートの理論値は 9.6Gbps である。通常は下りと上りの両方の通信が多重化されるが，混雑時の多重化は下りのみである。屋外使用も想定し，高い伝送効率を目指した。策定途中で 6GHz 帯の使用も追加され，2021 年 2 月に正式策定された。

Wi-Fi Alliance（IEEE802.11 無線 LAN 規格製品の相互接続を保証するための業界団体）は 2019 年よりこの（策定途中の 6GHz を除いた）規格を **Wi-Fi CERTIFIED 6**（または単に **Wi-Fi 6**）と呼称し普及を図った。なおこの呼称開始により， 802.11n は **Wi-Fi 4**, 802.11ac は **Wi-Fi 5** とも呼ばれるようになった。また 6GHz を追加した完全な 802.11ax 規格は **Wi-Fi 6E** とも呼ばれる。ただし 2021 年 2 月現在，日本では 6GHz 帯の使用は許可されていない（従って Wi-Fi 6E は現状日本では使用できない）。（2022 7/27，今後日本でも 6GHz 帯の一部が解放される予定）

・IEEE802.11ay（ドラフト）

802.11ad の後継であるが，策定は大幅に遅れている（2021 年 2 月現在でまだ策定中の模様）。60GHz 帯を使用し，最大理論値は 100Gbps を見込む。利用周波数が高いため屋内・近距離利用を想定している。

・IEEE802.11be

802.11ax の後継候補で Wi-Fi 7 候補と目されている（正式な決定ではない）。周波数帯は 802.11ax と同様に 2.4/5/6GHz 帯で，最大通信レートの理論値は 46Gbps を目指している。ドラフトが 2021 年 3 月にリリースされる予定である。日本では今後 6GHz の使用が許可されるかどうかが，普及の鍵になると思われる。

・IEEE802.11i

無線 LAN でのセキュリティ規格である。ただし，策定途中で **WEP** の脆弱性が問題となったため，2002 年 10 月に 802.11i の一部分を前倒しで **WPA** として標準化した。その後，802.11i は 2004 年 6 月に正式に標準化され，**WPA2** の基本規格となった。

・IEEE802.11e

無線 LAN で **QoS**（Quality of Service）を実現するための追加規格である。優先度の高い通信フレームに対して，先行転送を行う **EDCA**（enhanced distributed channel access）機能と専用帯域を割り当てる **HCCA**（hybrid coordination function controlled channel access）機能により QoS を実現する。

6.3 無線 LAN における通信制御と通信モード

6.3.1 衝突検出

イーサネットでは信号の衝突検出方式（メディアアクセス方式）として，**CSMA/CD** を採用していた。しかしながら無線 LAN において，送信ノード側は空中における電波の衝突（干渉）を検知することは不可能なので，CSMA/CD を利用することはできない。

無線 LAN では **CSMA/CA**（Carrier Sense Multiple Access with Collision Avoidance）

と呼ばれる手法で衝突回避を行う。CSMA/CA では，各ノードは使用周波数における電波の強度をチェックすることによりキャリアのセンス（Carrier Sense）を行う。他のノードが通信を行っている場合にはランダムな時間だけ待機した後，さらにランダムな時間電波強度をチェックし，通信中の他ノードが存在しなければ信号の再送を行う。また，受信側では信号を受信した場合，信号が衝突（干渉）無しに受信側に確実に到達したことを知らせるために，送信側へ確認応答用の ACK フレームを送信する（**CSMA/CA with ACK**）。送信側で ACK を受信できない場合は，データの再送信を行う。

ただし，例えば図 7.2 のような場合，受信ノードである AP（アクセスポイント）では，ノードＡとノードＢからの電波を検知できるが，ノードＡとＢはお互いの電波が届かないため，相手の送信を電波強度のチェックからでは検知することができない（隠れ端末問題）。

このような状況で電波の衝突（干渉）を回避するために **RTS**（Request To Send）フレームと CTS（Clear To Send）フレームが使用される場合がある。送信を行おうとするノードは AP に対して RTS フレームを送信し，AP は受信可能であれば CTS フレームを返信する。もし自分が RTS フレームを送信していないにもかかわらず，CTS フレームを受信した場合には，他のノードが AP と通信を行っていることになるので，一定時間通信を停止する（**CSMA/CA with RTS/CTS**）。これにより，隠れ端末が存在している状況でも，電波の衝突（干渉）を回避することが可能となる。

以上のように無線 LAN のメディアアクセス制御は有線に比べ非常に複雑であり，これらの処理のオーバヘッドだけで無線 LAN の通信効率は公称値の 70%～60%程度になるとさえ言われている（ノードとアクセスポイント間の電波の強度や輻輳の有無，TCP/IP の使用によるオーバヘッドなどにより実際の通信効率は更に下がる）。

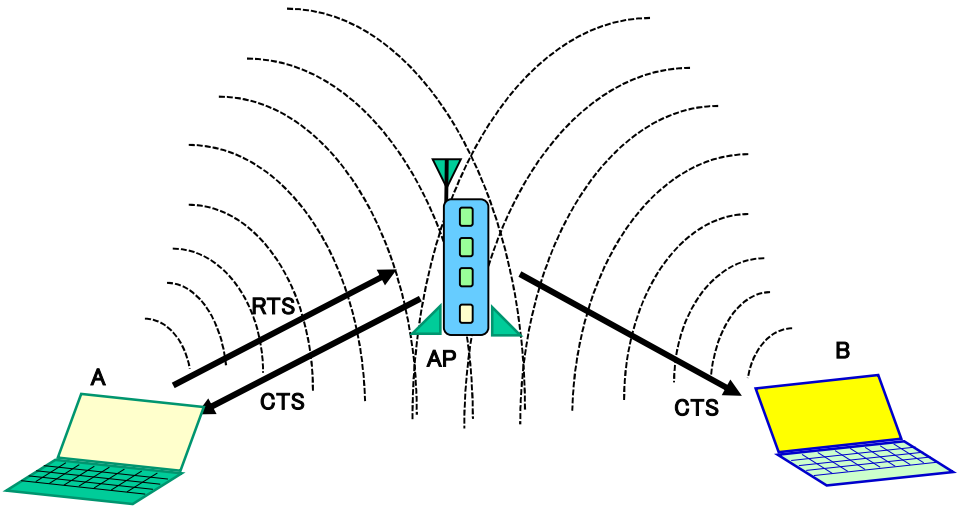


図 7.2 隠れ端末問題

7.3.2 ESS-ID（SS-ID）

無線 LAN では複数の通信チャンネルを持つことにより混線を防止しているが，チャンネル数も有限であるため，多数の AP が存在するような環境ではどうしても通信チャンネルが被ってしまう。

通信チャンネルが被って（干渉ではなく）混線した場合に，通信エリアを特定するための識別 ID が ESS-ID である。ESS-ID はデフォルトでは，無線 LAN カードの MAC アドレスを元に自動生成される。通常は，AP とノード間で ESS-ID を一致させないと AP に接続できないが，AP を **ANY 接続**のモードに設定した場合は ESS-ID が違っていても接続可能である。

7.3.3 通信モード

無線 LAN における通信モード（端末ノードのモード）には**アドホックモード**と**インフラストラクチャモード**がある。

アドホックモードは端末ノード同士の通信であり，携帯ゲーム機同士の通信などもこれに該当する。**インフラストラクチャモード**は AP（アクセスポイント）を通して通信を行う通常のモードである。

アドホックモードではノード（PC）からノード（PC）に直接コンピュータウィルスが感染する可能性もあり，注意が必要である。また，インフラストラクチャモードにおいても，同じ AP に接続しているノード同士は直接接続できないような設定を行い，ノード間でのウィルス感染を防止する場合もある。

7.4 無線 LAN のセキュリティ

無線 LAN は非常に便利である一方，一般ユーザのそのセキュリティに関する意識は総じて低く，今日一般家庭などでは，無線 LAN のセキュリティ対策は緊急を要するレベルにある。つまり，それらの環境の大半は何時トラブルに巻き込まれても不思議ではない状況にあると言える。

無線 LAN においてセキュリティを考慮しない場合，悪意ある第三者による通信内容の傍受やネットワーク内の PC の不正利用，他の組織への攻撃の踏み台にされるなどの被害を受ける可能性が十分にある。無線 LAN を使用する場合は，その利便性とセキュリティ機能を十分に把握し，慎重に利用しないと思わぬ落とし穴に嵌る危険性がある。

7.4.1 ESS-ID による接続制限

通常では AP（アクセスポイント）の ESS-ID が分らなければ，無線ノードは AP にアクセスすることはできない。その機能を利用して ESS-ID を隠すことにより，アクセスを制限しようと試みる場合がある。しかしながら，ESS-ID は元々セキュリティのための機能ではなく，ESS-ID のビーコン信号を受信すれば，簡単に ESS-ID を割り出すことができる。

また ESS-ID のビーコン信号を止める **ESS-ID ステルス**と呼ばれる機能もあるが，この場

合でも無線ノードと AP の通信内容を傍受して解析すれば，簡単に ESS-ID を割り出すことが可能である。ESS-ID ステルスの使用は，ESS-ID を設定せずに ANY 接続を許可するなどと言った状況よりは幾分ましであるが，それでセキュリティが確保される訳ではない。

7.4.2 MAC アドレスによるフィルタリング

MAC アドレスは NIC の ROM に焼き付けられていることから，偽装が不可能であると思い込んでいるユーザも多い。しかしながら，MAC アドレスを読み出すプログラム（システムコール）の改変や，メモリ上の MAC アドレスのキャッシュ情報の改変などにより，MAC アドレスは簡単に偽装することが可能である。従って，MAC アドレスによる無線ノードのアクセス制限を行っていたとしても，通信の傍受により使用中の MAC アドレスを検出し，攻撃者のノードの MAC アドレスを検出した MAC アドレスで偽装すれば，簡単にアクセスフィルタを突破することができる。

つまり,MAC アドレスによるフィルタリングも決定的なセキュリティ対策とはならず。「できるならば行った方が良い」程度の意味しか持たない。

7.4.3 暗号化：WEP（Wired Equivalent Privacy）

無線 LAN の暗号化方式の一つである **WEP（ウエップ**：Wired Equivalent Privacy）は，現在では暗号の体を成していないと言える。つまり WEP にはその実装方法による欠陥が存在し（暗号化アルゴリズムは **RC4**），そのため解読する方法が既に幾通りも知られており，簡単に解読することが可能だからである。

通常，WEP の解読は多数の通信パケットを収集し，その解析により行われる。有名な **KoreK’s アタック**では数十万～百万のパケットの IV を収集すれば，128bit の暗号化キー（WEP キー）であっても容易に割り出すことができる。数十万～百万のパケットと言うと，非常に大量のパケットのように思われがちだが，現在の高速無線 LAN では，20 分から 1 時間ほど盗聴すれば収集することが可能である。またアクティブでない AP に対しても，攻撃側から信号を送り，その信号に反応させることによってアクティブ状態にすることも可能である。

さらに，2008 年には **TeAM-OK**（TeramuraAsakuraMorii-OhigashiKuwakado）攻撃と呼ばれる攻撃方法が発表され，この攻撃方法では 3 万程度のパケットの解析で WEP キーを割り出すことが可能であるとされている。

以上より，現在では無線 LAN の暗号化方式として WEP を選択することは，殆ど意味のないこととなっている。

以上より，現在では無線 LAN の暗号化方式として WEP を選択することは，殆ど意味のないこととなっている。大量のパケットによる WEP キー解析の危険性は，既に 2001 年頃から認識されている。それにも関わらず,現在でも WEP により暗号化されている AP は存在する。このことは無線 LAN のセキュリティに関するユーザの意識の低さを表していると言える。

7.4.4 暗号化：WPA (Wi-Fi Protected Access)

WPA (Wi-Fi Protected Access) は，無線 LAN のセキュリティ規格である **IEEE802.11i** の先行規格である。2002 年に WEP の脆弱性が広く認識されるに至り，当時策定中であった IEEE802.11i の一部分を急遽，前倒しで規格・標準化したものが **WPA** である。暗号化には **TKIP** (Temporal Key Integrity Protocol) を使用する (鍵長 104Bit)。

TKIP では暗号アルゴリズムは WEP と同じ **RC4** を用いるが，WEP に存在した実装の際の問題点を解決している。 また **IEEE802.1X** によるユーザ認証を組み合わせることも可能であるが，一般家庭などで IEEE802.1X を使用しない場合は，最初の**事前共有 (PSK) キー** (つまり初期 WEP キー) の入力を必要とする (**WPA-PSK**)。

WPA はソフトウェアで実現できるため，古い機器でもファームウェアの更新により対応可能である。後にオプションで **CCMP**(**AES**, 鍵長 104Bit)も使用できるようになった。

7.4.5 暗号化：WPA2

WPA2 (Wi-Fi Protected Access 2) は IEEE802.11i の実装規格である。暗号化には **CCMP** (Counter with CBC-MAC) を使用している。暗号化アルゴリズムは米国の標準暗号である **AES** (Advanced Encryption Standard) を使用し (鍵長 128Bit)，IEEE802.1X によるユーザ認証機能も備えている。また，後にオプションで **TKIP**(**RC4**, 鍵長 128Bit)も使用できるようになった。

WPA と同様に IEEE802.1X を使用しない場合には,事前共有キーを必要とする(**WPA2-PSK**)。しかしながら，このキーが短いものであったり，または単純であったり，辞書に載っている単語である場合には，最初のセッション開始時のネゴシエーション用のパケット (4Way Handshake) (図 7.3) を盗聴するだけで，オフラインの**ブルートフォース (総当り) 攻撃**や**辞書攻撃**が可能であることが知られている (この問題は WPA でも発生する)。

セッション開始時のパケットを傍受するために，わざと接続中のセッションを妨害して通信を切断させ，再セッションを行わせる手法もある (**DEAUTH ATTACK**)。従って，事前共有キーが短い，単純である，または辞書に載っている単語であるような場合には，WEP よりさらに危険性が大きいと言える。

なお，WPA2 の暗号化方式である AES は処理の負荷が高く，AES を使用すると AP への同時アクセス数が大幅に制限される場合がある。

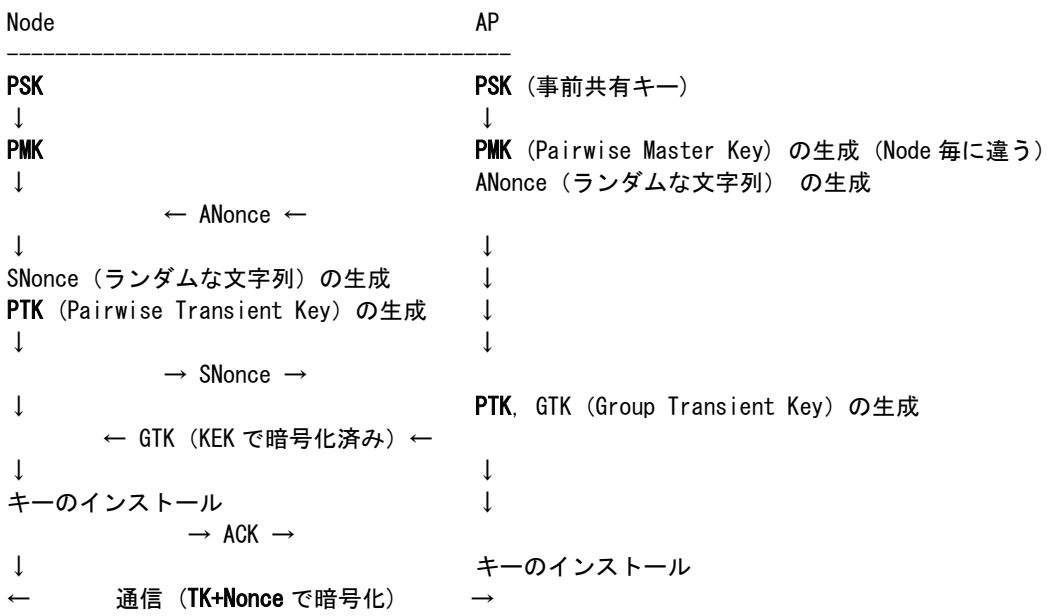
2017 年には，WPA,WPA2 に対して一定の条件下で，中間者攻撃が可能であることが発見されている (**KRACKs**)。

7.4.6 暗号化：WPA3

WPA2 策定からかなりの年月が経過していることもあり，次世代のセキュリティ規格として 2018 年 6 月に策定された。暗号化には **CCMP**(**AES/CNSA** 128bit/192bit)が使用されてい

る［**CNSA**（Commercial National Security Algorithm）は 米 NSA（National Security Agency：国家安全保障局）が定めた暗号スイート］。

WPA, WPA2 へのオフラインアタック対策として，SAE（Simultaneous Authentication of Equals）を使用した **Dragonfly** というハンドシェイクプロトコルを実装しており，これにより単純な PSK であってもオフラインによる解析が困難となっている。しかしながら，2019 年 4 月には早くもハンドシェイクのダウングレード攻撃などの脆弱性が指摘されている。



・**PTK**（Pairwise Transient Key）= **KCK + KEK + TK**： PMK, SNonce, ANonce, お互いの MAC から生成.
・GTK（Group Transient Key）はマルチキャスト・ブロードキャスト用の共通暗号鍵.
・KEK（Key Encryption Key） 4Way Handshake 中にのみ使用される.
・KCK（Key Confirmation Key）4Way Handshake 中にのみ使用される. 確認用.
・TK（Temporary Key） ユニキャスト用の共通暗号鍵.
・Nonce（number used once: パケット番号).

図 7.3 WPA2 における 4Way Handshake

7.4.5 暗号化：IEEE802.1X + EAP

WPA-802.1X, WPA2-802.1X は WPA, WPA2 において，**IEEE802.1X** でユーザの認証を行い，動的な WEP や CCMP キーを端末に配布（一定時間ごとに更新）する方式である。事前共有キー（PSK）を必要とせず，ホットスポットや大学などで使用する場合には，現時点でもっとも安全性の高い方式である。

IEEE802.1X（IEEE802.11X ではないので注意）は **Radius サーバ**（認証サーバの一種）などを利用したユーザ認証の規格であり，802.1X 自体には暗号化機能がなく，802.1X で暗号化された認証を行う場合には **EAP**（Extensible Authentication Protocol）と呼ばれる認証プロトコルを組み合わせなければならない。（なお IEEE802.1X の X は小文字で書いて良い

が，変数の x と混同されないように大文字書くことが多い）

EAP は PPP を拡張したプロトコルで，認証方式により，幾つかのモードに分類される。ただし EAP を使用する場合には，端末に「**サプリカント**」と呼ばれる認証ソフトをインストールすることが必要となる（MS Windows では，EAP のモードによってはデフォルトでサプリカントを内臓している）。

IEEE802.1X + EAP ではスイッチングハブなどの対応も必要で，ネットワーク内の全ての通信機器が，これらの機能をサポートしないとネットワークを形成することができない（図 7.4）。

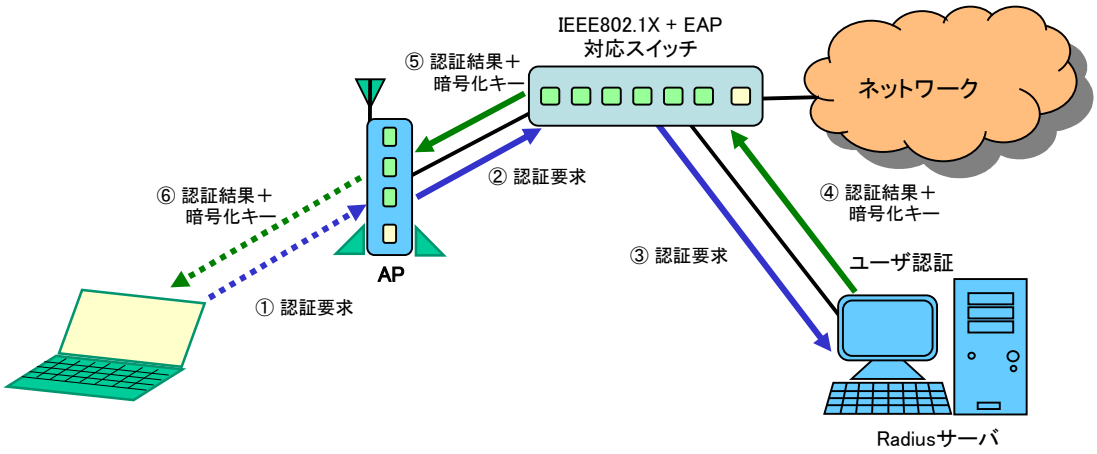


図 7.4 IEEE802.1X によるユーザ認証

7.5 偽の AP（双子の悪魔）

双子の悪魔（Evil Twins）とはホットスポットや大学などで，事前共有キーが公表または解析されている場合，盗聴者が偽の AP を立ててそこにユーザ端末を誘い込む手法である。AP が一個しかない環境では，端末から AP の状態を確認することにより発見可能であるが，多数の AP があるホットスポットや大学などでは，IEEE802.1X を用いて，サーバ側が端末を認証するだけでなく端末側からもサーバを認証する「相互認証」を行わないと，Evil Twins を発見することは難しい。

一方，盗聴者がわざと設定ミスを装ってオープンな AP を公開する恐れもある。もし一般ユーザがこのような AP に接続してしまった場合，HTTPS や SSL/TLS を用いて暗号化していない通信は全て盗聴されてしまう。