=== ch11.docx

[chap]11章　無線LANのパケット解析

無線LANの世界は、伝統的な有線LANとは少々違うものです。TCPやICPといった一般的な通信プロトコルは使いますが、OSI参照モデルの下層レベルへ行くと話が少々変わってきます。無線LANの性質と物理層によって、データリンク層が特に重要になってくるのです。この層によってアクセスできるデータとキャプチャする方法が変わってきます。

そう考えると、まるまる1章を無線LANでのパケットキャプチャと解析にあてても不思議ではないでしょう。この章では、パケット解析を考えたときに、なぜ無線LANが特別なのか、またこの課題をどう乗り越えるかについて説明します。もちろん無線LANキャプチャの実際の例も見ていきます。

物理学的考察

無線LANで転送されたデータをキャプチャし、解析するときにまず考えなければいけないのは、物理的な転送媒体です。これまではケーブル上で通信してきたため、物理層については考えてきませんでした。しかし今度は目に見えない電波で通信し、パケットが空中を飛び交うことになります。

1つのチャンネルをスニッフィング

無線LAN（WLAN）のトラフィックのキャプチャでもっとも特徴的なのは、無線周波数が共有されている媒体だということです。各クライアントが独自のネットワークケーブルでスイッチに接続している有線ネットワークとは異なり、無線通信媒体はクライアントが共有する空域で、容量に限りがあります。ひとつのWLANが802.11周波数に占める割合はほんのわずかです。このため複数のシステムが、周波数の異なる部分を使い、同じ物理的空間において動作できるのです。

注　無線LANは、米電気電子技術者協会（IEEE）が開発した802.11規格に基づいています。この章に登場する無線LAN用語は802.11規格に準拠しています。

空間の分割は、周波数をチャンネルに分割することで実現しています。米国には11のチャンネルがあります。WLANは一度に1つのチャンネルでしか通信しないので、同時に1つのチャンネルだけをスニッフィングします（図11-1）。そのためチャンネル6のWLANをトラブルシューティングするときには、チャンネル6でのトラフィックをキャプチャするようにシステム設定する必要があります。

図11-1　同時に1つのチャンネルしかスニッフィングできないので、退屈になるかもしれない

無線LANクライアント　アクセスポイント

周波数帯（11チャンネル）

注　伝統的な無線LANスニッフィングは同時に1つのチャンネルでしか行えませんが、例外がひとつだけあります。一部の無線スキャニングアプリケーションは、データを収集するためにすばやくチャンネルを切り替える「チャンネルホッピング」というテクニックを採用しています。なかでももっとも有名なツールがKismet (<http://www.kismetwireless.net/>)で、1秒間に最高10チャンネルまで切り替えられるため、複数のチャンネルを同時にスニッフィングすることができます。

無線LANのインターフェース

データが空気を通って送られるため、無線LANではいつでも信用できる通信が行われているわけではありません。何かが信号を妨げることがあります。無線LANには干渉を制御する機能が備わっていますが、それがうまく動作しないときもあります。したがって無線LANでパケットをキャプチャするときには、電波を反射するもの、硬くて大きなもの、電子レンジ、2.4GHzのコードレス電話、厚い壁、高密度のものなどが近くにないことを確認しましょう。これらはパケット消失や重複パケット、不正な形式のパケットの原因になります。

チャンネル間の干渉も考慮しましょう。同時にひとつのチャンネルしかスニッフィングできないとはいえ、注意が必要です。無線周波数では複数の異なるチャンネルが利用可能ですが、容量が限られているため、図11-2のようにチャンネル同士でややかぶっている部分があります。つまりチャンネル4とチャンネル5にトラフィックがあって、どちらかのチャンネルをスニッフィングしているとすると、もう一方のチャンネルのパケットをキャプチャしてしまう場合があるのです。一般には、同じ領域に共存するネットワークは、互いにかぶらないチャンネル1、6、11を使うよう設計されているため、このような問題は起こりにくいのですが、万一の場合に備え、なぜこうした事態が生じるかを理解しておきましょう。

図11-2　周波数帯域が限られているためにチャンネル同士がかぶっている

チャンネル周波数（GHz）

信号干渉を検出、解析する

無線信号干渉のトラブルシューティングは、Wiresharkでパケットを見るだけでできるようなものではありません。無線LANのトラブルシューティングでキャリアを積みたいなら、定期的に信号干渉をチェックする必要があります。周波数におけるデータや干渉を表示するツール、周波数アナライザを使えば可能です。

商業用の周波数アナライザは数千ドルはしますが、日常的に使えるソリューションもあります。MetaGeekのWi-Spyという製品は、802.11周波数全体の干渉を監視するUSB機器です。MetaGeekのChanalyzerソフトウェアと組み合わせると、Wi-Spyは周波数を出力しグラフ化してくれます。そのサンプルを図11-3に示しました。

図11-3　Chanalyzerの出力によって同じ領域で複数の無線LANが動作しているのがわかる

無線LANカードのモード

無線LANのパケットをキャプチャする前に、無線LANカードのモードについて学んでおきましょう。

無線NICモードは4種類あります。

マネージドモード

マネージドモードでは、クライアントはアクセスポイント（WAP：Wireless Access Point）に直接接続します。このモードでは、クライアントはアクセスポイントに通信の制御を任せます。

アドホックモード

アドホックモードは、クライアント同士が直接無線を介して通信するときに使います。このモードでは通信を行う2つのクライアントが、アクセスポイントの代わりに通信を制御します。

マスターモード

ハイエンドな無線LANカードは、マスターモードもサポートしています。このモードでは、特別なドライバソフトウェアにより、クライアントがアクセスポイントのような役割を担うことができます。

モニターモード

これがもっとも重要なモードです。モニターモードの無線LANカードは、データの送受信を行わず、飛び交うパケットを監視します。Wiresharkで無線LANのパケットをキャプチャする場合は、キャプチャするコンピュータの無線LANカードがモニターモードをサポートしている必要があります。パケットキャプチャするために無線LANカードを買うときは、モニターモード（RFMONモードとも呼ばれます）をサポートしていることを確認してください。

無線LANカードのほとんどはマネージドモードかアドホックモードになっています。各モードの動作を図11-14に示します。

図11-4　無線LANカードのモード

クライアント　マネージドモード　アクセスポイント　クライアント

クライアント　アドホックモード　クライアント

クライアント　マスターモード　クライアント（マスター）　クライアント

クライアント　モニターモード　クライアント（マスター）　クライアント

注　無線パケット解析にはどの無線LANカードがいいかとよく聞かれます。私自身が使っていて、一番お勧めしたいのが「ALFA 1000mW USB」無線アダプタです。どのパケットでも確実にキャプチャできる、もっともすぐれた製品として高く評価されています。ほとんどのオンラインのコンピュータハードウェアサイトで入手可能です。

Windows上での無線LANのスニッフィング

モニターモードをサポートしている無線LANカードを使っていても、Windowsではそのモードを使うことができません（WinPcapもサポートしていません）。ほかのドライバが必要です。

AirPcapの設定

AirPcap（CACE Technologies、現在はRiverbed傘下：<http://www.cacetech.com/>）は、Windows上で無線LANのパケット解析を行うために設計されたものです。AirPcapは無線LANでのパケットキャプチャのために設計されたUSBフラッシュドライブです（図11-5）。AirCapは3章で説明したWinPcapドライバを使っており、専用の設定画面があります。

図11-5　AirPcapはノートPCと一緒に簡単に持ち運べるくらいコンパクト

AirPcapの設定はオプションが少ないので非常に簡単です。[AirPcap Control Panel]から以下のオプションが設定可能です（図11-6）。

[Interface]

キャプチャに使うデバイスを選択できます。解析するときに、複数のAirPcapを使って複数のチャンネルを同時にスニッフィングする場合があります。

[Blink Led]

AirPcapのLEDを点滅させます。複数のAirPcapを使っているときに、どれを使っているかを示すためのものです。

[Channel]

ここでは、AirPcapを使ってキャプチャするチャンネルを選択します。

[Indlude 802.11 FCS in Frames]

OSによっては、デフォルトで無線LANのパケットのチェックサムの最後の4ビットを取り除いてしまうことがあります。このチェックサムはFCS（Frame Check Sequences）と呼ばれており、転送している間にデータが破損していないことを保証するために使われています。特に理由がなければ、チェックボックスをオンにしてFCSチェックサムを削除しないようにしましょう。

[Capture Type]

[802.11 Only]と[802.11 + Radio]という2つのオプションがあります。[802.11 Only]というオプションは、標準的な802.11のパケットのヘッダもキャプチャするということです。[802.11 + Radio]は、レート、周波数、信号レベルやノイズレベルを含むラジオタップヘッダもキャプチャします。入手可能なすべての情報を見られるようにするため、[802.11 + Radio]を選択しましょう。

[FCS Filter]

[Include 802.11 FCS in Frames]のチェックボックスをオンにしていなくても、このオプションを有効にしておけばFCSのチェックによりデータが破損していると判断されればパケットはフィルタされます。[Valid Frames]オプションをオンにすれば、FCSのチェックによりデータが正しく受信されたと判断されたものだけが表示されます。

[WEP Configuration]

ここでは、スニッフィングしたいネットワークのWEPキーを入力し、WEPによって暗号化されたデータを解釈できるようにします。WEPキーについては？？？ページの「ワイヤレスセキュリティ」の項で説明します。

図11-6　AirPcapの設定用プログラム

AirPcapを使ったパケットキャプチャ

AirPcapをインストールして設定したら、Wiresharkを立ち上げて[Capture]から[Options]を選択します。次に[Interface]からAirPcapを選択します①（図11-7）。

図11-7　キャプチャするインターフェースとして、AirPcapのデバイスを選択する

[Wireless Settings]というボタン以外は見慣れた画面だと思います。[Wireless Settings]　ボタンをクリックするとAirPcapと同じオプションが表示されます（図11-8）。WiresharkはAirPcapと完全に一体化しているため、AirPcatで設定できることはWiresharkでも設定できます。

図11-8　[Advanced Wireless Settings]ダイアログではWiresharkからAirPcapの設定ができる

設定がすべて終わったら、[Start]ボタンを押してパケットキャプチャを開始してください。

Linux上での無線LANスニッフィング

Linuxでのスニッフィングに必要なのは、無線LANカードをモニターモードにすることだけです。残念ながらモニターモードに変更する手順は無線LANカードごとに異なるため、ここでそのやりかたを説明することはできません。無線LANカードによっては変更が不要なものもあります。ご自分の無線LANカードについて、Googleで検索してみてください。

Linux上で無線LANカードをモニターモードに変更するもっとも一般的な方法は、Linuxにビルトインされている機能を使うことです。iwconfigコマンドを使えば、無線LANカードを設定できます。コンソール上でiwconfigを実行すると、以下のような結果になります。

$ iwconfig

Eth0 no wireless extensions

Lo0 no wireless extensions

Eth1 IEEE 802.11gESSID: "Tesla Wireless Network"

Mode: Managed Frequency: 2.462 GHz Access Point: 00:02:2D:8B:70:2E

Bit Rate: 54 Mb/s Tx-Power-20 dBm Sensitivity=8/0

Retry Limit: 7 RTS thr: off Fragment thr: off

Power Management: off

Link Quality=75/100 Signal level=-71 dBm Noise level=-86 dBm

Rx invalid nwid: 0 Rx invalid crypt: 0 Rx invalid frag: 0

Tx excessive retries: 0 Invalid misc: 0 Missed beacon: 2

iwconfigコマンドの結果から、802.11gという無線LANのプロトコルについての情報が表示されているEth1が無線LANのインターフェースであることが分かります。Eth0とLo0では無線LANは使えません。

Eth1と表示されている行の下の行を見てください。iwconfigコマンドを実行して得られる無線LANカードのESSID（Extended Service Set ID）や周波数などの情報とともに、モードがManagedであると表示されています。これを変更する必要があります。

Eth1をモニターモードに変更するにはroot権限が必要なので、suコマンドでユーザーを変更します。

$ **su**

Password: <rootのパスワードを入力>

rootになれば、無線LANカードのオプションを設定するコマンドを実行することができます。Eth1をモニターモードにするには、以下のコマンドを実行してください。

# **iwconfig eth1 mode monitor**

モニターモードに変更したら、iwconfigをもう一度実行して変更を有効にします。以下のコマンドを実行してください。

# iwconfig eth1 up

iwconfigコマンドでチャンネルを切り替えることもできます。Eth1のチャンネルを3に切り替えるには、以下のコマンドを実行してください。

# iwconfig eth1 channel 3

注　パケットキャプチャをしている間にもチャンネルを切り替えることができるので、遠慮なく変更してください。スクリプトを作ってしまえばより簡単に実行することができます。

設定が終わったらWiresharkを起動し、パケットキャプチャを開始してください。

802.11のパケット構造

無線LANと有線LANのパケットの違いは、802.11ヘッダがあるかないかです。このレイヤ2ヘッダにはデータ転送に使う媒体の情報が含まれています。802.11パケットには3つのタイプがあります。

マネージメント

レイヤ2でホスト間の接続を確立するために使われるパケットです。マネージメントパケットのサブタイプには、認証、アソシエーション、ビーコンパケットがあります。

コントロール

マネージメントパケットとデータパケットを配送、またパケットが込み合わないようにします。一般的なサブタイプとしてRTS（Request-to-send）とCTS（Clear-to-send）パケットがあります。

データ

実際にデータを含んだパケットで、また無線LANから有線ネットワークへと転送が可能な唯一のパケットタイプです。

無線LANの構造はパケットのタイプとサブタイプによって決まるので、構造には相当な数があります。ファイル*80211beacon.pcap*のパケットを見て、構造のひとつを見てみましょう。このファイルには図11-9に示したように、ビーコンというマネージメントパケットの例が含まれています。

図11-9　802.11ビーコンパケット

ビーコンは無線LANでの通信においてもっとも有益なパケットの1つです。ビーコンはアクセスポイントからブロードキャスト宛に送信されるパケットで、そのアクセスポイントに接続可能なクライアントに対して、接続に必要なパラメータを教えるために送信されます。例では、このパケットは802.11ヘッダのタイプ／サブタイプフィールドでビーコンと定義されています①。

802.11マネージメントフレームヘッダには、次の情報を含むたくさんの追加情報が含まれています。

Timestmp　パケットが転送された時間です。

Beacon Interval　ビーコンパケットが再送されるまでの間隔です。

Capability Information　アクセスポイントのハードウェアの性能についての情報です。

SSID Parameter Set　アクセスポイントがブロードキャストしている無線LANセグメントのSSIDです。

Supported Rates　アクセスポイントがサポートしているデータの転送レートです。

DS Parameter　アクセスポイントがブロードキャストしているチャンネルです。

ヘッダにはまた、送信元と宛先のアドレスと、ベンダ特有の情報が含まれています。

これらの知識をもとに、ビーコンを送信しているアクセスポイントについてかなりの情報が得られます。これは802.11b規格（B）③によるD-Linkデバイス②で、チャンネル11④を使っているのは明らかです。

802.11マネージメントパケットの中身や目的は変わりますが、一般的な構造はこの例と同じです。

無線LAN特有の情報をパケット一覧のペインに追加

Wiresharkのパケット一覧のペインには通常6つのカラムがあります。無線LANの解析を先へ進める前に、パケット一覧のペインに新たに3つのカラムを追加しておきましょう。

・RSSI（Received Signal Strength Indication：受信信号強度）カラム。キャプチャパケットの無線周波数（RF）信号の強さを示します。

・TX Rate（Transmission Rate）カラム。キャプチャしたパケットのデータ転送レートを示します。

・Frequency/Channelカラム。パケットが収集された周波数とチャンネルを示します。

これらの指標は無線LANでのトラブルシューティングにおいて大きな助けになるでしょう。たとえば無線LANのクライアントが信号が強いということを示しているとき、これらのカラムがあればそれが本当なのかどうかを確かめることができます。

これらのカラムをパケット一覧のペインに表示させるには、以下の手順に従ってください。

1．メインメニューの[Edit]から[Preference]をクリックします。

2．[Columns]を選択して[New]ボタンをクリックします。

3．[Title]のテキストボックスにRSSIと入力し、[Field type]ドロップダウンリストで[IEEE 802.11 RSSI]を選択します。

4．TX RateとFrequency/Channelカラムについても同じ手順を繰り返し、[Field type]ドロップダウンリストでそれぞれ[IEEE 802.11 TX Rate]と[Channel/ Frequency]を選択します。図11-10は以上の手順を終えた後の[Preferences]ウィンドウです。

5．[OK]をクリックして変更を保存します。

6．Wiresharkを再起動して新しいカラムを表示します。

図11-10　無線LAN特有の情報を表示するカラムをパケット一覧のペインに追加する

無線LAN特有のフィルタ

フィルタの有用性については4章で議論しました。有線LANでは各通信機器にケーブルが存在するため、キャプチャしたいパケットのみをキャプチャするフィルタは簡単に作ることができました。しかしながら、無線LANでは各クライアントによって発生するすべてのトラフィックがチャンネル上に共存しており、1つのチャンネルをキャプチャするとさまざまなクライアントのトラフィックが混在したものが記録されます。ここでは、自分が求めるパケットのみをキャプチャできるようなフィルタの作り方を学びます。

特定のBSSIDでフィルタリング

各アクセスポイントには、BSSID（Basic Service Set Identifier）と呼ばれるユニークな名前が割り振られています。アクセスポイントが発信する、無線LANのマネージメントパケットとデータパケットの中には、この名前が含まれています。

あなたが解析しようとしている無線LANのBSSIDが分かれば、あとは特定のアクセスポイントから送信されるパケットを見つけるだけです。Wiresharkでは、パケット一覧のペインのInfoカラムでパケットを転送しているアクセスポイントを表示してくれますので、目的のパケットを見つけ出すのは簡単でしょう。

解析したい無線LANのアクセスポイントから送信されているパケットを見つけたら、802.11ヘッダからBSSIDを見つけ出しましょう。これがフィルタの基本となるアドレスです。BSSIDのMACアドレスを見つけたら、次のようなフィルタが使えます。

wlan.bssid.eq 00:11:22:33:44:55:66

これでこのアクセスポイントを通過するトラフィックのみがキャプチャされるようになります。

無線LANのパケットタイプでフィルタリング

この章の最初で、無線LANのパケットにはいくつかのタイプがあるということを述べました。時折、これらのタイプやサブタイプによってパケットをフィルタリングする必要があります。タイプ別であればwlan.fc.type、タイプとサブタイプを組み合わせる場合は*wc.fc.type\_subtype*のフィルタを使うことができます。たとえばNULLデータパケット（16進数ではタイプ2サブタイプ4のパケット）をフィルタリングしたい場合、フィルタwlan.fc.type\_subtype eq 0x24が使えます。無線LANパケットをタイプとサブタイプでフィルタリングする際の一般的なフィルタの参照として、表11-1を利用してください。

表11-1　無線LANのタイプ／サブタイプ別フィルタ一覧

タイプ／サブタイプ　フィルタ構文

マネジメントフレーム

コントロールフレーム

データフレーム

アソシエーションリクエスト（Association request）

アソシエーションレスポンス（Association response）

リアソシエーションリクエスト（Reassociation request）

リアソシエーションレスポンス（Reassociation response）

プローブリクエスト（Probe request）

プローブレスポンス（Probe response）

ビーコン

ディスアソシエート（Disassociate）

オーセンティケーション（Authentication）

デオーセンティケーション（Deauthentication）

アクションフレーム（Action frames）

ブロックACK リクエスト（Block ACK requests）

ブロックACK（Block ACK）

PS-Poll（Power save poll）

RTS（Request to send）

CTS（Clear to send）

ACK

CF-End（Contention free period end）

NULL データ（NULL data）

QoS データ（QoS data）

Null QoS データ（Null QoS data）

周波数でフィルタリング

複数のチャンネルからのパケットを含むトラフィックを調べるなら、チャンネル別フィルタが非常に役に立ちます。たとえばチャンネル1と6にしかトラフィックがないと分かっていれば、11チャンネルすべてのトラフィックを表示するようフィルタリングします。もしこの2つのチャンネル以外でトラフィックが見つかれば、設定ミスか通信機器に障害があるなど、何か問題があることになります。周波数別にフィルタリングするには、次のような構文を使います。

radiotap.channel.freq == 2412

これでチャンネル1のすべてのトラフィックが表示されます。2422の値を別の周波数に変えれば、他のチャンネルをフィルタリングできます。表11-2は各チャンネルのその周波数の一覧です。

表11-2　無線チャンネルと周波数

チャンネル　周波数

無線LANのためにフィルタを作成する方法は何百とあります。キャプチャフィルタのサンプルは<http://wiki.wireshark.org/>のWireshark Wikiを参照してください。

無線LANのセキュリティ

無線LANを展開、管理するときの最大の懸念が、転送するデータのセキュリティです。データは空中を飛んでいくため、やり方さえわかれば誰でもタダで横取りできるので、データの暗号化が重要です。いいかえれば、WiresharkとAirPcapカードさえあれば、誰でもデータが見られるのです。

注　SSLやSSHなどの別の層の暗号化を使うと、トラフィックはその層では暗号化されるため、ユーザーの通信をパケットスニッファで読むことはできません。

無線LANで安全にデータを転送するために当初好まれていたのが、WEP（Wired Equivalent Privacy）規格でした。WEPはその暗号キー管理方法にいくつかの弱点が発見されるまで、数年にわたってある程度の広がりを見せていましたが、セキュリティ向上のために、現在は新たな規格が策定されています。それがWPA（Wi-Fi Protected Access）とWPA2規格です。WPA、そして改良版であるWPA2にも欠点はありますが、WEPよりははるかに安全だと考えられています。

この項ではWEPおよびWPAのトラフィック、また認証失敗の例を見ていきます。

WEP認証の成功

ファイル80211-WEPauth.pcapには、無線LANへの接続の成功例が含まれています。このネットワークのセキュリティは、WEPキーで設定されています。認証に成功し、データを暗号化して送信するために、アクセスポイントに渡す必要があるのがこのWEPキーです。無線LANのパスワードと考えればいいでしょう。

図11-11に示したように、キャプチャファイルはアクセスポイント(00:11:88:6b:68:30) からクライアント（00:14:a5:30:b0:af）に、4番目のパケットでチャレンジが送信されるところから始まっています①。クライアントのWEPキーが正しいかどうかを確認するのがチャレンジの目的です。802.11ヘッダを広げ、タグ付されたパラメータを見れば確認できます。

図11-11　アクセスポイントからクライアントにチャレンジが送信されている

チャレンジは5番目のパケットで確認されます。クライアントはWEPキーを使って、暗号化されたチャレンジのテキストを復号し、図11-12のようにアクセスポイントに返します①。

図11-12　クライアントは復号したチャレンジをアクセスポイントに返す

パケットは再び7番目のパケットで確認され、アクセスポイントは図11-13のように8番目のパケットでクライアントに応答します。応答には認証プロセスが成功したという通知が含まれています①。

図11-13　アクセスポイントがクライアントに認証が成功したことを伝えている

認証が成功すると、クライアントは接続要求を送信し、応答確認を受信して、ついに無線LANに接続します（図11-14）。

図11-14　認証の処理はシンプルな接続要求と接続許可によって行われる

WEP認証の失敗

次の例では、ユーザーがアクセスポイントに接続するためにWEPキーを入力したものの、数秒後にクライアントのユーティリティが接続できなかったと報告しています。その結果のファイルが80211-WEPauthfail.pcapです。

成功した接続と同様、ここでもアクセスポイントが3番目のパケットでクライアントにチャレンジを送信するところから始まっています。これが確認され、クライアントは5番目のパケットで、WEPキーを使って応答しています。

本来はここで認証に成功したという通知を受け取るはずですが、図11-15に示したように、7番目のパケットには違う内容が見えます①。

図11-15　認証に失敗したというメッセージ

メッセージには、チャンレジに対するクライアントの応答が正しくないとあります。これはつまり、クライアントがチャレンジテキストの復号に使ったWEPキーが間違っていたことを意味します。そのために接続に失敗したのです。正しいWEPキーで再度接続を試みなければなりません。

WPA認証の成功

WPAはWEPとはまったく異なる認証メカニズムを用いていますが、接続にキー入力を求める点は一緒です。ファイル80211-WPAauth.pcapにWPA認証の成功例があります。

ファイルの最初のパケットは、アクセスポイントからのビーコンです。このパケットの802.11ヘッダを広げて、タグ付されたパラメータの下を見て、図11-16のように[Vendor Specific]ヘディングを広げてみましょう。アクセスポイントのWPA属性専用の項が見えるはずです①。これによってアクセスポイントがWPAをサポートしていること、またサポートされているバージョンと実装がわかります。

図11-16　ビーコンによってアクセスポイントがWPA認証をサポートしているのが分かる

ビーコンを受信すると、クライアント（00:14:6c:7e:40:80）はアクセスポイント（00:0f:b5:88:ac:82）にプローブリクエストを送信し、アクセスポイントが応答します。認証、接続リクエスト、レスポンスは、4番目から7番目のパケットで行われます。

8番目のパケットから大きく進みます。ここでWPAハンドシェイクが始まり、11番目のパケットまで続きます。図11-17でお分かりのように、WPAのチャレンジレスポンスが行われるのがこのハンドシェイクプロセスです。

図11-17　これらのパケットはWPAハンドシェイクの一部

ここには2つのチャレンジとレスポンスがあります。図11-18のように、802.1x認証ヘッダの下の[Replay Counter]フィールドによって、チャレンジとレスポンスが一組になっています。最初の2つのハンドシェイクパケットのReplay Counter値は１①、次の2つのハンドシェイクパケットの値は2②になっています。

図11-18　[Replay Counter]フィールドによってチャレンジとレスポンスを1組にできる

WPAハンドシェイクが終了し認証が成功すると、クライアントとアクセスポイント間でのデータの送受信が始まります。

WPA認証の失敗

WEP同様、ユーザーがWPAキーを入力し、クライアントのユーティリティが接続できないという報告をしたところから見ていきましょう。このファイルが80211-WPAauthfail.pcapです。

先ほどと同じく、キャプチャファイルはWPA認証に成功した場合と同じように始まっています。ファイルにはプローブ、認証、接続要求が含まれています。WPAハンドシェイクは8番目のパケットで始まっていますが、なぜか認証に成功した場合の4個ではなく、8個のハンドシェイクパケットが存在しています。

WPAハンドシェイクの最初の2つのパケットが、8番目と9番目のパケットです。しかしここでは、クライアントからアクセスポイントへ送信されたチャレンジテキストが間違っています。その結果同じプロセスが10番目と11番目、12番目と13番目、そして14番目と15番目で繰り返されているのです（図11-19）。[Replay Counter]値を使えば、リクエストとレスポンスを一組にすることができます。

図11-19　パケットの多さがWPA認証の失敗を示している

ハンドシェイクプロセスの試みが4回繰り返されると、通信が破棄されます。図11-20のように、16番目のパケットでアクセスポイントから認証の失敗を知らされました。

図11-20　WPAハンドシェイクが失敗、認証が失敗した

まとめ

無線LANは現在もあまり安全ではないと考えられていますが、さまざまな環境での普及がスローダウンしているわけではありません。無線LANへの移行とともに、有線LANと同様のデータキャプチャと解析が行えるようになるのが重要です。この章で学んだスキルと概念は完全なものではありませんが、パケット解析による無線LANのトラブルシューティングの難しさを理解するのに役立つはずです。