=== ch03.docx

[chap]3章　Wireshark概要

1章で触れたように、パケット解析に使うスニッファにはさまざまな種類がありますが、本書ではWiresharkを取り上げています。この章ではWiresharkの概要を説明します。

Wiresharkの歴史

Wiresharkには長い歴史があります。Wiresharkはカンザスシティにあるミズーリ大学でコンピュータサイエンスを学んだジェラルド・コームズ（Gerald Combs）が作ったものです。1988年にGPL（GNU Public License）により公開されました（当時の名前はEthereal）。

Etherealが公開された8年後、コームズは新たなキャリアを求めてそれまで勤めていた企業を退職しました。残念ながら退職した企業がEtherealの著作権を持っていたため、コームズはEtherealをそれ以上開発することができなくなってしまいました。かわりに、コームズとEtherealの開発チームは、2006年半ばにWiresharkという新たな商標を取得しました。

Wiresharkは非常に人気があり、劇的に成長してきました。開発には500人もの人がかかわっています。Etherealという名のプログラムはもう開発されていません。

Wiresharkの利点

Wiresharkには、日々パケット解析を行う人にとって便利なさまざまな特徴があります。1章で述べたスニッファの評価項目に従ってWiresharkを評価してみましょう。

サポートされているプロトコル

現在WiresharkはIPやDHCPのような一般的なものから、AppleTalkやBitTorrentのような特定のメーカーやソフトウェアでしか使われないものまで、850以上のプロトコルをサポートしています。Wiresharkはオープンソースモデルとして開発されており、Wiresharkのアップデートごとに新しいプロトコルが追加されています。

注　めったにないことですが、Wiresharkがサポートしていないプロトコルがあれば、自分でそのプロトコルをサポートするコードを書いてWiresharkの開発者に提供することもできます（もちろんそのコードが承認されればですが）。

ユーザーフレンドリかどうか

Wiresharkには他のスニッファに比べ非常に分かりやすいインターフェースが備わっています。メニューはわかりやすく、見やすいレイアウトのGUIベースのアプリケーションです。たとえばデータはプロトコルごとに色分けされているなど、高いユーザビリティを持つ設計になっています。tcpdumpのような難解なコマンドラインインターフェースのアプリケーションと違い、Wiresharkはパケット解析を始めようという人にとって使いやすいツールといえます。

コスト

Wiresharkはオープンソースで、GPLライセンスのもと無償で入手することができます。個人利用でも商用利用でも、誰でもWiresharkをダウンロードして使うことができます。

注　Wiresharkはたしかに無償ですが、間違ってお金を払っている人もいます。eBayでスニッファを検索すると、Wiresharkの「プロフェッショナル企業ライセンス」を、最低価格でも39.95ドルで売りつけようとしている人々がたくさんいることに驚くでしょう。もちろんこれは茶番ですが、本当に買いたいなら、私に電話をください。ケンタッキーIで売りに出ているビーチ沿いの物件について話しましょう。

スニッファのサポート体制

ソフトウェアの善し悪しはそのサポートによって決まるといっても過言ではありません。Wiresharkのようなフリーで公開されているソフトウェアには、公式サポートというものが存在しません。オープンソースのソフトウェアのサポートは、ユーザーに頼っている部分があります。幸運なことに、Wiresharkのユーザーコミュニティはオープンソースプロジェクトの中でも非常に活発です。WiresharkのWebページには、オンラインドキュメント、開発者のためのWiki、FAQ、開発者も参加しているメーリングリストに登録するための方法が載っています。CACE TechnologiesのSharkNetプログラムを利用すれば、有償サポートを受けることもできます。

OSのサポート

WiresharkはWindows、Mac OS X、Linuxなど、現代の主要なOSのほとんどをサポートしています。WiresharkのWebページで、サポートしているOSの一覧を見ることができます。

Wiresharkのインストール

Wiresharkのインストールは驚くほど簡単です。ただしインストールする前に、以下のシステム要件を満たしているかどうかを確認する必要があります。

CPU 400MHz以上

128MBのRAM

75MB以上の空き容量

プロミスキャスモードをサポートしているNIC

WinPcapパケットドライバ（Windowsのみ）

WinPcapパケットドライバは、PcapパケットドライバのWidows APIです。このドライバによって生のパケットデータをキャプチャしたり、それをフィルタリングしたり、NICをプロミスキャスモードに切り替えたりできるようになります。

WinPcapは個別でダウンロードすることもできますが（<http://www.winpcap.org>から）、WiresharkにはWinPcapが同梱されているのでその必要はありません。同梱されているWinPcapは動作が確認されたバージョンですので、個別にインストールせず、Wiresharkのパッケージからインストールすることをお勧めします。

Windowsでのインストール

まず、WiresharkのWebページ（<http://www.wireshark.org/>）から、最新版のWiresharkをダウンロードしてください。Webサイトのダウンロードセクションへと進み、ミラーサイトを選択してください。パッケージをダウンロードしたら、以下の手順でインストールしてください。

1．.exeファイルをダブルクリックし、表示されたダイアログ上で[Next]ボタンをクリックします。

2．使用承諾書を読み、同意するなら[I Agree]ボタンをクリックします。

3．インストールするコンポーネントを図3-1のように選択します。ここでは何も変更せず[Next]をクリックします。

図3-1　インストールするコンポーネントを選択

4．[Additional Tasks]ウィンドウで[Next]をクリックします。

5．Wiresharkのインストール先を入力し、[Next]ボタンをクリックします。

6．WinPcapをインストールするかどうかのダイアログが表示されるので、[Install WinPcap]チェックボックスが図3-2のようにオンになっていることを確認し、[Install]ボタンをクリックします。インストールが始まります。

図3-2　WinPcapパケットドライバをインストールする

7．Wiresharkのインストールの途中で、WinPcapパケットドライバのインストールが始まります。ダイアログが表示されるので[Next]ボタンをクリックし、使用承諾書を読んでから[I Agree]ボタンをクリックしてください。

8．WinPcapパケットドライバがインストールされます。終了したら[Finish]ボタンをクリックします。

9．Wiresharkのインストールが続きます。終了したら[Next]ボタンをクリックします。

10．インストールの終了を確認するウィンドウで、[Finish]ボタンをクリックします。

Linuxでのインストール

まず、インストールパッケージを入手します。ただし、すべてのLinuxディストリビューションがパッケージを提供しているわけではありません。

一般にシステムワイドベースのソフトウェアの場合、ルートアクセスが必要となります。しかしソースからコンパイルしたローカルソフトウェアインストールは、通常ルートアクセスなしでインストール可能です。

RPMベースのシステム

Red Hat LinuxのようなRPMベースのディストリビューションにWiresharkをインストールする場合は、適切なインストレーションパッケージをWiresharkのWebサイトからダウンロードしてください。コンソールを開き、次のように入力します（ファイル名はダウンロードしたパッケージのものに変えてください）

rpm –ivh wireshark-0.99.3.i386.rpm

依存するパッケージがインストールされていない場合は、それらをインストールし再度Wiresharkをインストールしてください。

DEBベースのシステム

DebianやUbuntuのようなDEBベースのディストリビューションの場合は、システムリポジトリからWiresharkをインストールすることができます。コンソールを開き、次のように入力してください。

apt-get install wireshark

ソースからコンパイルする

手持ちのLinuxディストリビューションが自動化パッケージ管理ソフトウェアを使っていない場合、Wiresharkをインストールする最適な方法はソースからのコンパイルです。このためには次のように実行します。

1．WiresharkのWebページからソースパッケージをダウンロードします。

2．次のように入力してアーカイブを解凍します（ファイル名はダウンロードしたパッケージのものに変えてください）。

tar –jxvf wireshark-1.2.2.tar.bz2

3．ファイルの解凍先となる新規に作成したディレクトリに変えます。

4．ルートレベルのユーザーの場合、ソースを設定し、コマンド./configureを使ってLinuxディストリビューションを正しく構築できるようにします。デフォルトのインストレーションオプション以外のものが使いたい場合は、この時点でそのオプションを指定します。依存するパッケージが見つからない場合、エラーの可能性が高くなります。インストールが成功すれば、図3-3のようなメッセージが表示されるはずです。

図3-3　./configureコマンドで成功した場合のアウトプット

5．[make]コマンドを入力し、ソースをバイナリにします。

6．[make install]で最終インストールを起動します。

Mac OS Xシステムでのインストール

Mac OS X Snow LeopardにWiresharkをインストールするには若干の注意が必要ですが、インストールそのものは難しい内容ではありません。インストールの手順を示します。

1．WiresharkのWebページからDMGパッケージをダウンロードします。

2．Wireshark.appをアプリケーションフォルダにコピーします。

3．Wirehsark.appのユーティリティフォルダを開きます。

4．ファインダで[Go]をクリックし、[Go To Folder]を選択します。/user/local/bin/と入力し、ディレクトリを開きます。

5．コマンドラインフォルダの中身を/user/local/bin/にコピーします。これにはパスワードの入力が必要です。

6．ユーティリティフォルダで、ChmodBPFフォルダをStartupItemsフォルダにコピーします。これを実行しインストールを完了するには、再度パスワードの入力が求められます。

Wiresharkの基本

Wiresharkを首尾よくインストールできれば、すぐにそれを使うことができます。ついにあなたはスニッファを手にしたのです。しかし…何も表示されません！

Wiresharkは起動しただけでは特に興味を引くものは表示されません。面白いものを見るには何かデータが必要です。

最初のパケットキャプチャ

Wiresharkでパケットを解析するには、まずパケットをキャプチャしなければいけません。「ネットワークに障害がないのにどうやってパケットをキャプチャするのだろう？」と疑問に思うかもしれません。

まずネットワークには、常に障害が存在しています。疑うならネットワークユーザー全員にメールを送信して、すべてが完璧に届くかどうか確認してごらんなさい。

第2にパケット解析は、障害があるときだけやるものではありません。実際のところ、ネットワーク管理者はトラブルシューティングより障害のないネットワークの解析に時間を割いています。ネットワークのトラブルシューティングを効果的に行うためには、ネットワークが正常な状態にあるときの情報が必要なのです。たとえばDHCPの障害を解決しようとする場合、DHCPのトラフィックがどういうものなのかを理解しておく必要があります。

つまりネットワークの異常を見つけるためには、正常な状態も知っておかなければならないということです。ネットワークが順調に動いているときを基準にすれば、正常なときのトラフィックの状態がわかります。

それではさっそくパケットをキャプチャしてみましょう！

1．Wiresharkを起動します。

2．メインメニューの[Capture]を選択し、[Interfaces]をクリックします。パケットをキャプチャできるNICの一覧が、IPアドレスとともにダイアログ上に表示されます。

3．図3-4のように、使いたいNICを選択し、[Start]をクリック、またはウェルカムページのインターフェースリスト一覧の下にあるNICをクリックします。ウィンドウがデータで埋まるはずです。

図3-4　パケットをキャプチャするNICを選択する。

4．数分待って十分にパケットをキャプチャできたら、キャプチャのドロップダウンメニューで[Stop]ボタンをクリックします。

以上の手順でパケットキャプチャを終了すると、Wiresharkのメインウィンドウにデータが表示されます。大量のデータに圧倒されるかもしれませんが、メインウィンドウの機能を理解すれば、それほど難しいことはありません。

Wiresharkのメインウィンドウ

パケット解析中に一番よく見るのが、このメインウィンドウでしょう。ここにはキャプチャされたすべてのパケットが、見やすい形にフォーマットされて表示されています。たった今キャプチャしたパケットを使って、図3-5に示したようなWiresharkのメインウィンドウを見てみましょう。

図3-5　 3つのペインのメインウィンドウ

メインウィンドウの3つのペインの表示はお互いに依存しています。パケット一覧のペイン（上段）からパケットをクリックすると、パケット詳細のペイン（中段）にそのパケットの詳細が表示されます。また、バイナリのペイン（下段）でそのパケットのバイナリデータを見ることができます。

注　図3-5で、パケット一覧のペインに少し違ったプロトコルを表示されているのがわかります。レイヤが違っても、プロトコルの見た目に違いはありません。ネットワーク上で受け取られたすべてのパケットが表示されます。

各ペインに含まれるものは次の通りです。

パケット一覧のペイン

上段のペインには、キャプチャファイルに存在するパケットの一覧が、パケット番号、キャプチャされた時間、パケットの送信元と宛先、パケットのプロトコル、その他パケットに含まれる情報とともに表示されています。

注　本書中でのトラフィックという単語は、パケット一覧のペインに表示されているすべてのパケットのことだと思ってください。たとえばDNSのトラフィックと言ったときには、パケット一覧のペインに表示されているすべてのDNSのパケットのことです。

パケット詳細のペイン

中段のペインには、パケットの詳細がツリー状に表示されています。ツリーは最初折りたたまれていますが、展開することですべての情報を見ることができます。

バイナリのペイン

下段のペインには、フォーマットされる前の生のパケットが表示されています。つまり、ケーブルを通るパケットの本来の形です。このままでは解析が非常に困難だということが分かると思います。

Wireshark設定

Wiresharkはさまざまなカスタマイズが可能です。Wiresharkの設定画面は、メインのドロップダウンメニューの[Edit]から[Preferences]をクリックすると表示されます。設定ダイアログには図3-6のように、いくつかのカスタマイズ可能なオプションが含まれています。

図3-6　設定画面のオプションでWiresharkをカスタマイズする

Wireshark設定画面は、6つの主なセクションに分かれています。

[User Interface]セクション

Wireshark上でのデータの表示方法を設定できます。ここでは、ウィンドウの場所を記憶するかどうか、ペインのレイアウト、スクロールバーの位置、パケット一覧のペインの位置、データを表示するときのフォント、ウィンドウのカラーなどが設定できます。

[Capture]セクション

デフォルトのNIC、プロミスキャスモードをデフォルトで使用するか、パケット一覧のペインにリアルタイムにキャプチャしたパケットを表示するかなど、キャプチャの方法について設定できます。

[Printing]セクション

データをプリントアウトする際のオプションを設定できます。

[Name Resolution]　セクション

MACアドレス、ネットワーク、ポート番号の名前解決をするかどうかを設定できます。また、名前解決のリクエストの最大数も設定できます。

[Statistics]セクション

Wiresharkの統計機能のいくつかのオプションが設定できます。

[Protocols]セクション

Wiresharkでデコードが可能なさまざまなパケットのキャプチャや表示に関連するオプションが設定できます。すべてのプロトコルを設定できるわけではありませんが、さまざまなオプションが変更可能なプロトコルもあります。しかしながら、これらのオプションは特に理由がなければ変更しないほうがよいでしょう。

パケットの色分け

Wiresharkでパケットをキャプチャすると、図3-7の例のように、パケット一覧のペイン上でパケットがさまざまな色に色分けされることに気づくでしょう（図はモノクロですが、意味はわかりますよね）。これらの色はランダムに決められているように見えますが、そうではありません。

図3-7　プロトコルごとに色分けされ、見やすくなっている

各パケットはプロトコルごとに色分けされています。たとえば、DNSのトラフィックは青、HTTPのトラフィックは緑といった具合です。色分けされているおかげで、パケット一覧のペインに表示されているすべてのパケットを1つ1つ確認する必要がありません。巨大なキャプチャファイルを扱うときに、この色分けの機能のおかげで解析が大幅にスピードアップするのを実感することでしょう。

図3-8のように、色分けのルールは、[Coloring Rules]ダイアログで設定が可能です。このダイアログを開くには、メインのドロップダウンメニューから[View]を選択し、[Coloring Rules]をクリックします。

図3-8　[Coloring Rules]ダイアログで、パケットの色分けルールを設定する

色分けのルールの一覧が表示されるので、好みの色に変更します。たとえば、HTTPのトラフィックの背景色をデフォルトの緑からラベンダーに変える手順は、以下のとおりです。

1．Wiresharkを起動し、[Coloring Rules]ウィンドウを表示します（[View]から[Coloring Rules]を選択）。

2．一覧からHTTPの色分けルールをクリックします。

3．[Edit]ボタンをクリックします。図3-9のように[Edit Color Filter]ダイアログが表示されます。

図3-9　[Colring Rules]ダイアログでは、文字色と背景色を設定できる

4．[Background Color]ボタンをクリックします。

5．色を選択し、[OK]ボタンをクリックします。

6．[OK]ボタンを2回押してメインウィンドウに戻ります。該当するパケットが、設定した色に変更されています。

Wiresharkを使ってパケット解析をしていると、あるプロトコルが他のプロトコルより多く表示されていることに気づくでしょう。色分けされていることでそれがより分かりやすくなるのです。たとえばDHCPサーバに障害が起こりIPアドレスの割り当てがうまくいかなくなった場合、DHCPのトラフィックを黄色に色分けしていれば、メインウィンドウが黄色に染まります。こうして、DHCPのトラフィックの選別が容易になり、より効率よくパケット解析ができるようになります。

自分だけのカスタムフィルター別に、色分けルールを利用することも可能です。

Wiresharkを起動し、実行したところで、パケット解析を行う準備が整いました。次章ではキャプチャしたパケットをどう扱うかについて説明します。