=== ch14\_appC.docx

[chap]付録C　推薦文献

本書で使用したツールはWiresharkですが、パケット解析を実行する場合、それが一般的なトラブルシューティング、ネットワーク遅延、セキュリティ問題、あるいは無線LANであっても、他のツールが大いに役立つでしょう。この章では便利なパケット解析ツールと、パケット解析の学習に役立つリソースをご紹介します。

パケット解析ツール

Wiresharkに加え、パケット解析に便利なツールがいくつかあります。ここでは実際に使ってみて一番役に立ったものをいくつか紹介します。

tcpdumpとWindump

Wiresharkは非常に人気がありますが、tcpdumpほどは普及していないでしょう。完全にテキストベースのtcpdumpは、多くの人々の間でパケットキャプチャおよび解析ツールの業界標準とみなされています。

tcpdumpにはグラフィック機能はありませんが、たとえばLinuxのsedやawkといった他のコマンドで出力をパイプする場合など、大量のデータを動かすには非常に便利です。パケット解析をさらに掘り下げたければ、Wiresharkとtcpdumpの両方を使うことになるでしょう。tcpdump は<http://www.tcpdump.org/>でダウンロードできます。

WindumpはtcpdumpのWindows版で、<http://www.winpcap.org/windump/>でダウンロード可能です。

Cain & Abel

2章で説明したように、Cain & AbelはARPキャッシュポイゾニングを実行するためのWindows用ツールです。Cain & Abelは非常に堅牢なスイートなので、ほかの用途でも利用できるでしょう。<http://www.oxid.it/cain.html>で入手できます。

Scapy

ScapyはPythonライブラリで、コマンドラインスクリプトを使ってパケットを作成、操作することができます。言ってみればScapyは、もっとも強力かつ柔軟性のあるパケット作成アプリケーションです。<http://www.secdev.org/projects/scapy/>でScapyの詳細やスクリプトのサンプル、またScapyそのものをダウンロードできます。

Netdude

Scapyほど高機能なものが必要でなければ、Netdudeが便利です（Linux向け）。Netdudeの機能は限られていますが、リサーチ目的のパケットを作成、変更するのに、非常に使いやすいGUIを備えています。図A-1はNetdudeの使用例です。Netdudeは<http://netdude.sourceforge.net/>でダウンロード可能です。

図A-1　Nedtudeでパケットを変更

Colasoft Packet Builder

WindowsユーザーでNetdude同様のGUIが欲しければ、Colasoft Packet Builderがいいかも知れません。Colasoftでも使いやすいGUIでパケットの作成や変更が可能です。Colasoftは無料ソフトで、<http://www.colasoft.com/packet_builder/>から入手可能です。

CloudShark

QA Cafe開発のCloudSharkは、パケットキャプチャをオンラインで共有できるサイトです。Wireshark風に、ブラウザ内にキャプチャファイルを表示することができます（図A-2）。キャプチャファイルをアップロード、共有したい相手にリンクを送ることで、解析が共有できます。

図A-2　CloudSharkで見たキャプチャファイルのサンプル

CloudSharkがお気に入りなのは、登録が不要で、URLから直接リンクできるからです。つまり自分のブログにPCAPファイルへのリンクを投稿すると、誰かがそれをクリックするだけで、パケットを見られるからです。ファイルのダウンロードやWiresharkで開く手間が省けます。

CloudSharkのサイトは<http://www.cloudshark.org/>です。

pcapr

pcaprはMu Dynamicsが開発した、PCAPファイル共有のための非常に堅牢なWeb 2.0プラットフォームです。本書執筆時点で、pcaprには約3000のPCAPファイルがあり、400以上の異なるプロトコルの例が含まれています。図A-3はpcaprでのDHCPトラフィックキャプチャの例です。

図A-3　pcaprでDHCPトラフィックのキャプチャを見る

通信の例を探すとき、まずはpcaprで探します。たくさんのキャプチャファイルを持っているなら、<http://www.pcapr.net/>にアップロードして共有しましょう。

NetworkMiner

NetworkMinerは、おもにネットワークフォレンジックに使われるツールですが、ほかのさまざまな場面でも役に立ちます。パケットキャプチャにも使えますが、PCAPファイルの解析に本領発揮します。NetworkMinerはPCAPファイルを取り出し、OSごと、またホスト間のセッションごとに分割します。キャプチャから直接ファイルを抽出することもできます。NetworkMinerは無料ソフトで、<http://networkminer.sourceforge.net/>で入手できます。

Tcpreplay

ケーブルでパケットを再転送し、デバイスがどう反応するかを調べたいとき、いつもTcpreplayを使います。TcpreplayはPCAPファイルを取り出し、その中に含まれているパケットを再転送するために設計されています。<http://tcpreplay.synfin.net/>からダウンロード可能です。

ngrep

Linuxに慣れているなら、データ検索にはgrepを使うのが普通でしょう。ngrepはgrepとよく似ていて、PCAPデータで非常に的を絞った検索ができます。私はフィルタがうまく機能しない場合や、複雑になりすぎたときに使っています。<http://ngrep.sourceforge.net/>でngrepの詳細が載っています。

libpcap

高度なパケット解析、あるいはパケットを処理するアプリケーションを開発したいなら、libpcapに詳しくなるでしょう。簡単に言えば、libpcapはネットワークトラフィックキャプチャのための、ポータブルなC/C++ライブラリです。Wiresahrk、tcpdump、そしてそのほか多くのパケット解析アプリケーションが、libpcapライブラリを使っています。libpcapについては<http://www.tcpdump.org/>を参照してください。

hping

hpingは、多用途に使えるツールで、コマンドラインでパケットが作成、転送可能です。さまざまなプロトコルをサポートしており、簡単に使いこなすことができます。<http://www.hping.org/>でダウンロード可能です。

Domain Dossier

ドメインやIPアドレスの登録情報を検索する必要があるときに利用するのが、Domain Dossierです。<http://www.centralops.net/co/DomainDossier.aspx>でアクセスすることができます。

PerlとPython

PerlとPythonはツールではなく、スクリプト言語です。パケット解析に熟練してくると、ニーズを満たす自動化ツールが存在しないケースに出くわします。こうした場合のツールを作成できる言語が、PerlとPythonなのです。私はたいがいのアプリケーションにPythonを使っていますが、どちらを選ぶかは好みの問題です。

パケット解析に役立つリソース

Wiresharkのホームページ、学習コース、ブログに至るまで、パケット解析に役立つリソースは数多くあります。そのうちで私のお気に入りを紹介します。

Wiresharkホームページ

Wiresharkに関連するすべてが見つかるのがこのホームページ、<http://www.wireshark.org/>です。ここにはソフトウェアドキュメンテーション、キャプチャファイルのサンプルを含む非常に有益なwiki、Wiresharkメーリングリストの申し込み情報などがあります。

SANS Security Intrusion Detection In-Depth Course

SANSのメンターである私の意見は少々偏っているかも知れませんが、SANS SEC 503、Intrusion Detection In-Depthよりも優れたパケット解析のコースは存在しないと思います。セキュリティ専門でなくても、コースの最初の2日間を受けるだけで、パケット解析とtcpdumpのもっともよい入門編となるでしょう。

コースを指導しているのは、パケット解析のヒーロー的な存在であるMike PoorとJudy Novakの2人です。年に数回、ライブイベントの形式で行われています。旅行予算が限られているなら、オンラインやWebのオンデマンド形式でも受講が可能です。

SEC 503とその他のSANSコースについては、<http://www.sans.org/>を参照してください。

Chris Sandersのブログ

パケット解析に関する記事を、ときどき自分のブログ<http://www.chrissanders.org/>に投稿しています。私が執筆した他の記事や書籍のポータルとして役立つだけでなく、私と連絡を取る方法も載っています。

Packetstanブログ

パケット関連のブログで現在一番のお気に入りが、Mike PoorとJudy Novakのブログです。<http://www.packetstan.com/>には、興味深いトラフィックの分析が載っており、またここにあるコンテンツのすべてが特A級です。

Wireshark University

Laura Chappellはもっとも熱心なWireshark伝道者のひとりです。彼女のサイトにはWiresharkを使う際のヒントや、彼女が執筆した書籍「Wireshark Network Analysis」に関する情報、また指導するコースなどが掲載されています。<http://www.wiresharktraining.com/>を参照してください。

IANA

IANA（Internet Assigned Numbers Authority）<http://www.iana.org/>は、北米のIPアドレスとプロトコル番号を管理している組織です。Webサイトではポート番号の検索やトップレベルドメインに関する情報、RFCの検索や閲覧ができるサイトの一覧など、貴重な情報が掲載されています。

TCP/IP Illustrated（Addison-Wesley）

多くの人々にTCP/IPの聖書と考えられているのが、Richard Stevens博士によるこのシリーズ本で、パケットを専門とする人ならまず本棚にあるはずです。私の一番のお気に入りのTCP/IP関連書籍であり、本書執筆の参考にもしています。

The TCP/IP Guide（No Starch Press）

TCP/IP関連でもうひとつのお気に入りが、Charles Kozierokによるこの本です。1000ページ以上あり、非常に詳しく、たくさんの図表が載っています。