=== ch00.docx

※ 「=== ch\*\*\*\*」で章ごとに区切られています。◆はタブの意味です。

=== ch00a\_tobira.docx

★★★P.i

実践 パケット解析 第2版 ―― Wiresharkを使ったトラブルシューティング

Chris Sanders　著

高橋 基信、宮本 久仁男　監訳

岡 真由美　訳

★★★P.ii

本書で使用するシステム名、製品名は、それぞれ各社の商標、または登録商標です。

なお、本文中では【TM】、【○R】、【○c】マークは省略している場合もあります。

★★★P.iii

※原書扉入る

★★★P.iv

Copyright 【○c】2011 by Chris Sanders.

Title of English-language original:

PRACTICAL PACKET ANALYSIS, 2ND EDITION, ISBN978-1-59327-266-1, published by No Starch Press.

Japanese-language edition copyright 【○c】2012 by O'Reilly Japan, Inc. All rights reserved.

本書は、株式会社オライリー・ジャパンがNo Starch Press, Inc.の許諾に基づき翻訳したものです。日本語版についての権利は、株式会社オライリー・ジャパンが保有します。

-----------------------------------------------------------------------

日本語版の内容について、株式会社オライリー・ジャパンは、最大限の努力をもって正確を期していますが、本書の内容に基づく運用結果については責任を負いかねますので、ご了承ください。

=== ch00b\_kenji.docx

本書、私の人生、そして私が行うであろうすべてのことは、与えられた信仰と受け取った信仰から生まれた結果である。本書は神、両親、そして私に対して信仰を示してくれたすべての人々に捧げる。

「もしあなたがたに、からしの種ほどの信仰があったら、この山に向かって『動け』と言えば、そのとおり山は動くのです。 何でもできないことはありません。」――マタイの福音書17:20

（http://www.biblica.com/uploads/pdf-files/bibles/japanese/nt/matthew.pdfから引用）

=== ch00c\_JP-KANYAKU.docx

[chap]監訳者まえがき

★★★後送　□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■

　□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■

　□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■

　□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■

[\_Author\_]2012年10月●日

[\_Author\_]高橋 基信、宮本 久仁男

=== ch00d\_Praise.docx

[chap]賞賛の声

「あらゆるレベルのネットワーク管理責任者に必須の本」

――LINUX PRO MAGAZINE

「すばらしく、使いやすく、わかりやすい」

――ARSGEEK.COM

「パケット分析の基本を完璧に理解する必要があるなら、この本は最適の出発点だ」

――STATEOFSECURITY.COM

「非常に有益であり、『実践』というタイトルがまさにふさわしい。パケット分析の実行のために知るべきことを読者に与えるという点ですばらしい仕事をしており、Wiresharkで何をするかという現実世界の生き生きとした例を即座に提供している」

――LINUXSECURITY.COM

「互いにコミュニケーションしている未知のホストがあるだろうか。私のマシンは他人と話しているだろうか。これらの質問の答えを見つけるには、パケットスニッファが必要だ。Wiresharkはこの仕事に最適なツールのひとつであり、このツールについて学ぶのに本書は最良の方法のひとつである」

――FREE SOFTWAE MAGAZINE

「初心者から中級者には最適」

――DAEMON NEWS

=== ch00e\_Intro.docx

[chap]まえがき

　実践パケット分析の第2版は、初版発行から約4年後の、2009年後半から2011年中盤に1年半かけて執筆されました。内容はほぼ一新され、キャプチャファイルやシナリオも完全に新しいものとなっています。初版を気に入っていただけたなら、本書も好きになって下さるでしょう。本書は初版と同じ調子で執筆され、シンプルでわかりやすい説明がつけられています。初版がお気に召さなくても、本書には新しいシナリオがあり、内容も拡大されているので、気に入っていただけるかもしれません。

[sec] なぜこの本なのか？

　なぜ、パケット解析を解説しているほかの本ではなく、本書を買うべきなのかと疑問に思うでしょう。答えはタイトルにあります。「実践パケット解析」（原著名は“Practical Packet Analysis”）。つまり、本書では現実世界で対面する問題とよく似たシナリオを通して、実践的なパケット解析を学ぶことができるのです。本書の前半では、パケット解析とWiresharkを理解するための前提知識が得られます。後半では、日々のネットワーク管理で遭遇する問題を実践的なシナリオに沿って解決していきます。

　ネットワーク技術者、ネットワーク管理者、CIO、コンピュータの技術者、デスクワークする人、あるいはネットワークセキュリティアナリストであっても、本書から多くの知識を得、本書で説明されているパケット解析テクニックを活用することができるでしょう。

[sec] コンセプトとアプローチ

　筆者はのんびりした人間なので、コンセプトを語るときもやっぱりのんびり語ることになるでしょう。それは本書の口調にも現れています。技術的なコンセプトを語るときはどうしても技術用語が多くなり、のんびりした口調にはなりませんが、それでもできる限りカジュアルな説明になるよう努力したつもりです。明確で要領を得て、過不足なく記述しています。つまり、私は偉大なるケンタッキー州出身なので、難しい言葉の使用は最小限に抑えています（本書全体にみられるド田舎風の言い回しはお許しください）。

　本当にパケット解析を学びたいと思っているのなら、本書の前半で紹介されているコンセプトを理解する必要があります。後半部分を理解するために不可欠だからです。本書の後半部分は完全に実践的です。あなたの職場で起こる問題とまったく同じシナリオを読むことはできませんが、本書でコンセプトを学んでおかなければ実際の問題に遭遇したときに解決することは難しいでしょう。

　以下は本書の各章の内容の簡単な説明です。

[term1]1章 パケット解析とネットワークの基礎

[term2]◆パケット解析とはなんでしょう？ どのように機能するのでしょう？ どうやってやるのでしょう？この章ではネットワークの通信とパケット解析の非常に基礎的な部分を学びます。

[term1]2章 ケーブルにもぐりこむ

[term2]◆この章では、ネットワーク上にどうスニッファを配置するのかについて述べています。

[term1]3章 Wireshark概要

[term2]◆Wiresharkはどこで入手可能か、どうやって使うのか、何ができるのか、なぜすぐれているのかなどWiresharkの基本について述べています。

[term1]4章 Wiresharkでのパケットキャプチャのテクニック

[term2]◆Wiresharkを設定、実行したら、キャプチャしたパケットとやりとりする方法について知りたくなるでしょう。ここではその基礎を学びます。

[term1]5章 Wiresharkの高度な機能

[term2]◆基本を身につけたら、実際に使ってみましょう。この章では高度なWireshark機能を掘り下げ、普段は目立たない機能に焦点を当てます。

[term1]6章 一般的な下層プロトコル

[term2]◆この章では、もっともよく使われる下層プロトコル――TCP、UDP、IPなど――が、パケットレベルではどう見えるかを紹介します。各プロトコルで起こる問題を理解するために、それらがどう機能するかをここで学んでおきましょう。

[term1]7章 一般的な上層プロトコル

[term2]◆プロトコルの続きです。この章では、もっともよく使われる3つの上層プロトコル――HTTP、DNS、DHCP――が、パケットレベルではどう見えるかを紹介します。

[term1]8章 基本的な現実世界のシナリオ

[term2]◆この章には、一般的なトラフィックの分析と、現実世界で起こる問題をもとにしたシナリオが出てきます。各シナリオは読み進めやすい形式で書いてあり、そのシナリオの問題、問題の解析、そして解決策が盛り込まれています。これらの基本的なシナリオには数台のコンピュータで構成されたネットワークのみが登場するので、パケット解析を始めるのにちょうどよい難易度になっています。

[term1]9章 ネットワークの遅延と戦う

[term2]◆ネットワークの問題でもっとも多いのは、ネットワークの遅延です。この章ではネットワークの遅延に関する問題に焦点を当てます。

[term1]10章 セキュリティのためのパケット解析

[term2]◆情報技術分野において、ネットワークセキュリティはもっとも関心の高い話題でしょう。10章では、パケット解析によってセキュリティ関連問題解決に結びつくいくつかのシナリオを示します。

[term1]11章 無線LANのパケット解析

[term2]◆本章は無線パケット解析の入門です。この章では、有線LANと無線LANのパケット解析の違いについて、無線ネットワークトラフィックの例を通じて説明します。

[term1]付録A ★★★★★★★★★

[term2]◆付録Aは監訳者による日本語版オリジナルの記事です。□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■

[term1]付録B ★★★★★★★★★

[term2]◆付録Bは××の○○氏による日本語版オリジナルの記事です。□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■□□□□□□□□□■

[term1]付録C 推薦文献

[term2]◆付録として、本書で学んだパケット解析のテクニックを使い続けるために便利なツールやWebサイトを集めました。

[sec] 本書の使い方

　本書には2つの使い方があると筆者は思っています。

　1つは、1つ1つの章を読んでゆき、パケット解析の理解を深めるためのテキストとして使う方法。現実世界の問題に沿ったシナリオが掲載されている後半部分に特に重点を置きます。

　もう1つの使い道は、本書をリファレンスとして使う方法。頻繁に使用するわけではないWiresharkの機能をいちいち覚えておく必要はありません。そういった機能を使うときのリファレンスとして本書が本棚に置いてあれば役に立つことでしょう。またパケット解析を仕事に活用するときに便利なリファレンスとなるいくつかのユニークな図表、略図、手法も提供しています。

[sec] サンプルファイルについて

　本書で使われているキャプチャファイルはすべて、No Starch Pressのhttp://www.nostarch.com/packet2.htmから入手可能です。本書を最大限利用するために、これらのサンプルファイルをダウンロードしてそれと一緒に本書を読むことをお勧めします。

[sec] Rural Technology基金

　実践パケット解析から生まれた最良のことについて触れないわけにはいきません。本書の初版が発行されて間もなく、筆者は最大の夢のひとつの頂点となる501(c)(3)非営利団体を創設しました。

　地方の学生の場合、たとえ素晴らしい成績であったとしても、都市や郊外の学生と比べると技術に触れる機会がかなり少なくなります。Rural Technology Fund（RTF）は、地方のコミュニティと都会とのデジタル格差を埋める目的で、2008年に設立されました。奨学金プログラム、コミュニティの参加、宣伝活動、地方の技術支援運動を通じて活動しています。

　奨学金は、地方在住で、コンピュータ技術に情熱を持ち、この分野でさらに教育を受けたいと考える学生たちを対象としています。この奨学金資金とするため、本書の売り上げの100％がRural Technology基金に直接提供されることをここに謹んで発表いたします。Rural Technology基金についてもっと知りたい、あるいはどのように貢献できるかを知りたければ、http://www.ruraltechfund.org/を参照してください。

[sec] 筆者の連絡先

　私が執筆したものに対する読者からのフィードバックをいつも楽しみにしています。何らかの理由で筆者と連絡を取りたい、質問やコメントを送りたい、脅迫、プロポーズをしたい場合は、直接chris@chrissanders.orgへどうぞ。また頻繁にブログhttp://www.chrissanders.org/を書いているほか、Twitterの@chrissanders88でもフォローできます。

★★★オライリーの前付の「定型文書」入る

[sec] 本書の表記

　本書では、以下の表記を使用しています。

[term1]太字（[\_Fb\_]Bold[\_/Fb\_]）

[term2]◆新しい用語、強調やキーワードフレーズは太字で表記します。

[term1]等幅（[\_Fc\_]Constant Width[\_/Fc\_]）

[term2]◆プログラムのコード、コマンド、配列、要素、文、オプション、スイッチ、変数、属性、キー、関数、型、クラス、名前空間、メソッド、モジュール、プロパティ、パラメータ、値、オブジェクト、イベント、イベントハンドラ、XMLタグ、HTMLタグ、マクロ、ファイルの内容、コマンドからの出力は、等幅で表記します。

[term1]等幅の太字（[\_Fcb\_]Constant Width Bold[\_/Fcb\_]）

[term2]◆ユーザーが入力するコマンドやテキストは、等幅太字で表記します。重要な部分を強調するために使う場合もあります。

[\_TIP\_]

[\_note\_]このアイコンとともに記載されている内容は、ヒント、提案、または一般的な注意事項を表します。

[\_/TIP\_]

[\_WARNING\_]

[\_note\_]このアイコンは、警告や要注意事項を表します。

[\_/WARNING\_]

[sec]意見と質問

　本書（日本語翻訳版）の内容については、最大限の努力をもって検証および確認していますが、誤りや不正確な点、誤解や混乱を招くような表現、単純な誤植に気づかれることもあるでしょう。本書を読んで気づいたことは、今後の版で改善できるように知らせてください。将来の改訂に関する提案なども歓迎します。

[term2]◆株式会社オライリー・ジャパン

[term2]◆〒160-0002◆東京都新宿区坂町26番地27 インテリジェントプラザビル1F

[term2]◆電話◆03-3356-5227

[term2]◆FAX◆03-3356-5261

[term2]◆電子メール◆japan@oreilly.co.jp

　本書に関する技術的な質問や意見については、次のあて先に電子メール（英文）を送ってください。

[term2]◆info@nostarch.com

　本書に関連するファイルは本書のWebページからダウンロードできます。

[term2]◆http://www.oreilly.co.jp/books/9784873115696/★★★

[term2]◆http://oreilly.com/catalog/9781593272661/（原書）

[term2]◆http://nostarch.com/packet2.htm（原書）

　監訳者のWebページには、正誤表や追加情報が掲載されています。以下のアドレスでアクセスできます。

[term2]◆http://★★★★★★★★★★★★/

　オライリーに関するその他の情報については、次のオライリーのWebサイトを参照してください。

[term2]◆http://www.oreilly.co.jp/

[term2]◆http://www.oreilly.com/

[sec]謝辞

　本書は非常に多くの人々による、直接的そして間接的な貢献によって実現しました。

　何よりもまず、すべての賞賛は神のものです。本書の執筆では、かなりのポジティブそしてネガティブな感情が生み出されました。ストレスを感じると、神が気持ちを落ち着かせてくれます。いらいらすれば、安心感を与えてくれます。混乱すると、解決方法を示してくれます。疲れれば、休息を与えてくれます。うぬぼれると、冷静にさせてくれます。本書、そして私のキャリアと存在は、神と神の息子であるイエス・キリストのおかげでしかありません。

　お父さん。多くのものから刺激を受けましたが、私を誇りに思うというあなたの言葉ほど、私を幸せにしてくれるものはありません。それを伝えてくれることに、感謝してもしきれません。

　お母さん。本書の第2版は、あなたがこの世を去ってちょうど2年目となる日の直前に発行されました。お母さんが私を見守っていて、誇りに思ってくれているのはわかっています。これからもっと誇りに思ってくれればと思います。

　DebiおばさんとRandyおじさん。あなた方は最初から、私の最大の支援者です。私の家族は大きくはないですが、自分の家族、特におじさんとおばさんのことを大切に思っています。思うようには会えませんが、第2の両親のようにいてくれることに感謝のしようもありません。

　Tina Nance。以前ほどは話ができなくなってしまったけれど、いつも2人目の母のように思っています。あなたがサポートし、私を信じてくれていなければ、現在していることを成し遂げられなかったでしょう。

　Jason Smith。誰よりも頻繁に愚痴を聞き、気持ちを落ち着かせてくれたね。すばらしい友人そして同僚でいてくれて、そしてさまざまなプロジェクトでインプットを与えてくれ、一度は6カ月間も車庫を使わせてくれてありがとう。

　過去そして現在の同僚についていえば、周囲によい人々がいる人は、よい人になれると常に信じてきました。私はこの仕事でもっとも優秀な、素晴らしい人々と仕事ができるという幸運に恵まれています。君たちは家族です。

　Mike Poor。あなたは疑いなく、私のパケット分析の崇拝者です。あなたの仕事と手法は、私にひらめきを与え、行動を助けてくれています。

　Tyler Reguly。本書の技術編集をしてくれたことに本当に感謝します。楽しいプロセスではなかったでしょうが、必要だったのは間違いなく、心より感謝しています。

　そしてGerald CombsとWireshark開発チームにも感謝しています。Geraldと、Wiresharkをすばらしい分析プラットフォームにしたその他大勢の開発者の貢献のおかげです。彼らの努力がなかったら、本書は存在していません。存在したとしても、単なるtcpdumpであり、まったくつまらないものだったでしょう。

　BillとNo Starch Pressのスタッフは、このケンタッキー出身のガキに、一度ばかりか二度もチャンスを与えてくれました。チャンスをくれて、辛抱してくれて、そして私の夢の実現を支援してくれて、ありがとう。

=== ch00f\_toc.docx

[chap]目次

★★★DTPで抽出