Red Hat® Linux® Firewalls

Bill McCarty 著
ヴァインカーブ 監訳
中川和夫 訳

Red Hat Linux Firewalls
by Bill McCarty

Japanese language edition publishing by Softbank Publishing Inc.

Original Cover design by Michael J. Freeland
Cover photo © Hulton/Getty

謝 辞

まずこの謝辞に目を通してくれた読者に感謝したい。教師としての筆者の経験からすると，「誰がこの本の出版にかかわっているか」にまで興味を示す読者はめったにいない。役に立ったと感じた本についても同様だ。本書をつくりあげたチームに関心を持たれたことにまず感謝したい。

Debra Williams Cauley氏は企画編集者として，筆者とともに本書のコンセプトをみがきあげ，本書の企画を出版にまでつないでくれた。彼女は各章の初稿を注意深くチェックし，そのつど貴重なコメントを送ってくれた。

プロジェクト担当編集者のEric Newman氏は本書の進行を見守り，執筆の道筋をつけてくれた。彼は筆者が気づかなかった問題を指摘し，ときにはその解決策も示してくれた。彼のおかげで，本書の品質は大きく改善され，恥ずかしいミスを避けることができた。

Red Hat, Inc.のエンジニアリング担当上級ディレクタでありApache Weekの編集者でもあるMark Cox氏は，原稿に目を通し，技術的な正確さ，完全さ，妥当性などをチェックしてくれた。Markの厳密なチェックのおかげで，数多くの間違いを訂正することができた。まだ間違いが残っているとしたら，それはひとえに筆者の責任である。

Rebecca Whitney氏はコピー担当編集者として，筆者の書いた英語を平明で簡潔なものへと改善してくれた。筆者の学生がよく知っているように，この面では筆者には大いに改良の余地がある。

Waterside Productions, Inc.のMargot Maley-Hutchinson氏は筆者の代理人として，このプロジェクトを紹介してくれ，プロジェクトのビジネス面を取り仕切ってくれた。

筆者の家族（Jennifer，Patrick，Sara）は，筆者が新しい技術書の執筆にとりかかることを許し，さまざまな面で協力してくれた。

最後に，良きことすべての創造主であるイエス・キリストに対し，その犠牲と救済の約束に感謝しなければならない。

発刊によせて

ファイアウォールなしではにっちもさっちもいかない。

Information Assurance and SecurityのCenter for Education and Researchを統括するGene Spafford氏が言うように，「システムをほんとうにセキュアにするには，電源をオフにして，コンクリートのブロックで囲み，鉛で裏張りした部屋に入れ，ガードマンに見張りさせる必要がある。それでも一抹の不安は残る」。コンピュータをコンクリートのケースに入れるのが現実的でないとすれば，ファイアウォールこそが防御の最前線になる。適切に設定されたファイアウォールはネットワークのセキュリティを大幅に強化する。といっても，ファイアウォールはセキュリティの不安を一瞬のうちに取り除いてくれる魔法の杖ではない。

ファイアウォールはシステムを攻撃から守ってくれる（より正確には，一部の攻撃から守ってくれる）。

インターネットはシステムを外部の世界につなぐドアのようなものだ。ドアが無防備なら，誰もが自由に出入りする。Code Red，Ramen，Nimdaなどのワームは既知のセキュリティホールを利用して，ご存じのような大きな被害をもたらした。ネットワークを通じて外部につながっている限り，セキュリティの問題はなくならない。ソフトウェアのセキュリティホールは毎日のように発見され，すべてにすばやく対処するのはますます難しくなっている。新しいセキュリティホールを解析するには時間がかかる。新しいセキュリティホールは自分のシステムに影響するだろうか。セキュリティホールを利用した攻撃はすでに発生していないだろうか。回避策はあるだろうか。パッチはリリースされているだろうか。パッチには副作用がないだろうか。

私のホームネットワークでは，ファイアウォールを通じてたった1つのポートだけが開いている。開いているのはポート80であり，Webトラフィックの着信を受け入れる。私は自分のファイアウォールを信頼しており，注意を要するのはリモートからの攻撃だけだ。lpd（印刷サービス）やOpenSSHなどのソフトウェアのセキュリティホールに気をつかう必要はない。ファイアウォールコード，TCP/IP，Apacheなどのセキュリティホールには注意しなければならないが，幸い危ない事態はそう頻繁には発生しない。

ファイアウォールは私自身のエラーからも私を守ってくれる（ファイアウォールなしではひどい目に遭っているはずだ）。

私はRed Hat社でセキュリティ対応チームの運営にかかわっている。このため，Red Hat LinuxやApacheの最新のリリースを絶えず試すことができ，さまざまなネットワークやセキュリティアプリケーションに触れる機会もある。新しいアプリケーションをテストすれば，いずれかのネットワークサービスが開くかもしれない。こうしたことをいちいち気にしながらテストするのはたまったものではない。ネットワーク上にセットアップしたすべてを強いパスワードで保護するのもたいへんだ。ファイアウォールは私のちょっとした間違いや見逃しがセキュリティのリスクにつながることを防止してくれる。

私のホームネットワークには私のガールフレンドのWindowsシステムがつながっているが，これもそう脅威ではない。ファイアウォールが守ってくれるからだ。新しいNetBIOSプロトコルに重大なセキュリティホールが見つかったとしても，脆弱なNetBIOSポートへのパケットははじめからファイアウォールによってブロックされている。ホームネットワークにTiVoをつないだときも，セキュリティについて心配する必要はなかった。セキュリティのルールがリモートからの攻撃を防いでくれる。せっかく保存した「Cops」の番組がリモート攻撃によってすべて削除されるといった最悪のシナリオは発生しない。

ファイアウォールが効果を発揮するには，適切な設定と管理が欠かせない。いったん内側に侵入されれば，ファイアウォールのパワーはゼロになる。不適切な設定のファイアウォールは誤った安心感を生み出す。ファイアウォールを構築するときには，その仕組みと機能，そして限界を理解しなければならない。何よりも重要なのは，正しい設定方法を知ることだ。本書の役割はここにある。

市販のファイアウォールソリューションも数多くリリースされているが，ファイアウォールの仕組みと機能を理解しなければならないことに変わりはない。最新のLinuxディストリビューションでは，自前のファイアウォールを構築するのに必要なテクノロジがすべて用意されている。このため，本書はオープンソースのソフトウェアを使ってファイアウォールを構築する方法に照準を定めている。本書を理解すれば，ごくわずかなコストで市販のソリューションに匹敵するファイアウォールをセットアップできる。

ファイアウォールの設計，構築，管理については，数多くの解説書があり，インターネット上の情報にも事欠かない。しかし，本書の利点は必要なことがすべて一箇所に集められ，一貫したやり方で説明されていることだ。本書は背景情報を説明し，個々のテクノロジの目的と使用法を明らかにし，すぐに使えるコードと設定例を示す。しかもうれしいことに，本書の例はすべてRed Hat Linuxにあわせてカスタマイズされている。

では，コーヒーでもかたわらにリラックスして，Red Hat Linuxやそのほかのオープンソースのソフトウェアを使ってどのようにファイアウォールを構築するか，Bill McCarty氏とともに見ていこう。外部からの攻撃だけでなく，自らのエラーからもネットワークを守る方法を習得できるはずだ。

Mark J. Cox
Senior Director of Engineering, Red Hat

はじめに

Red Hat LinuxはほかのOSに比べればセキュアなシステムだ。適切にインストールし設定したRed Hat Linuxシステムは，そう簡単には攻撃に屈しない。しかし，インターネットを介した攻撃のレベルは上がる一方だ。外部ネットワークにつないだRed Hat Linuxシステムはファイアウォールでしっかりと守る必要がある。本書は，Red Hat Linuxファイアウォールを使ってコンピュータとネットワークを守る方法を説明する。

●本書が対象とする読者

本書では，Red Hat Linuxシステムとネットワーク管理に関する一般的な知識を前提とする。したがって，本書が対象としている読者は，ファイアウォールの導入を計画しているRed Hat Linuxシステム管理者やネットワーク管理者ということになる。しかし，Red Hat Linux以外のLinuxディストリビューションやLinux以外のUNIXライクなシステムを使っている場合も，本書を利用してファイアウォールを構築するのはそう難しくないだろう。

本書の主要なターゲットは何台ものサーバを使って各種のネットワークサービスを提供しているシステムの管理者だが，本書で説明するツールやテクニックはパーソナルネットワークでも十分活用できる。

本書はハードウェアやソフトウェアをベースとした市販のファイアウォール製品には立ち入らない。本書で取り上げるのは，Red Hat Linuxに標準で装備されているIPTables機能だ。IPTablesは柔軟で高度なステートフルファイアウォール機能であり，その機能とパフォーマンスは市販のファイアウォール製品に優に匹敵する。予算の限られた組織にとって，IPTablesファイアウォールには低コストという大きな魅力もある。また，今では古くなったIPChainsファイアウォール機能についてもふれる。IPChainsを使ってステートフルファイアウォールを構築することはできないが，旧システムとの互換性やなじみやすさからIPChainsのほうを好む管理者もいる。

Red Hat Linuxファイアウォールを構築するには，TCP/IPプロトコルファミリに関する知識が必要になる。しかし，市販のファイアウォールソリューションを利用する場合も事情は変わらない。たとえ市販の製品であれ，TCP/IPを理解することなくファイアウォールを設定し運用することはできない。本書は，Red Hat Linuxファイアウォールの設定と運用に必要なTCP/IPネットワーキングの基礎とIPTables/IPChainsの詳細を説明する。

●本書の構成

本書は4つのPartから構成されている。

Part I ：ネットワークセキュリティを巡る背景

Part Iでは，ネットワークセキュリティが重要な理由を明らかにし，ネットワークを守るうえでファイアウォールが果たす役割を説明する。さらに，ファイアウォールの設計にとって重要なTCP/IPプロトコルファミリーを詳しく説明する。

Part II ：ファイアウォールの設計と実装

Part IIでは，IPChainsファイアウォールとIPTablesファイアウォールの設計と実装を説明する。まずファイアウォールの基本アーキテクチャを明らかにし，ファイアウォールポリシー設計の各要素を示したうえで，IPChainsとIPTablesの詳細を説明する。

Part III：ファイアウォールの運用

Part IIIではファイアウォールの運用と管理に焦点をあわせる。各章では，攻撃に対してホストを強化する方法，ファイアウォールのテストとトラブルシューティング，ファイアウォールの状態の監視方法を説明する。

Part IV：Appendix

本書はいくつかのAppendixで締めくくられる。記載されているのは，VPN（Virtual Private Network）の概要，役に立つWebサイト，よく使われるポート，プロトコル番号，ICMPメッセージなどのリスト，用語集である。

●本書の利用法

コンピュータセキュリティやTCP/IPプロトコルファミリに詳しくない場合は，Part Iを読んでからPart IIとIIIに進む。Part Iは，コンピュータセキュリティがなぜ重要なのかを明らかにし，他の防御策と併せてどのようにしてファイアウォールを使うべきか，また，Red Hat Linuxファイアウォールの実装に必要なTCP/IPプロトコルファミリーの詳細を説明している。すでにこれらのトピックに精通しているなら，Part Iを飛ばしてPart IIに進もう。

Part IIとIIIはどちらから読みはじめてもよい。Red Hat Linuxファイアウォールの構築をすでに経験しているなら，Part IIに先立ってPart IIIを読むのもよい。IPChainsファイアウォールを導入する場合，第7章「IPChainsファイアウォール」は必須になる。IPTablesファイアウォールのみを計画しているなら第7章はスキップできる。第7章を除き，Part IIの各章は順に読む必要がある（どの章も先行の章を前提としている）。

Part IIIの各章はどの順に読んでもよい（Part IIより先でもよい）が，ファイアウォールをはじめて構築する場合は，第11章「要塞ホストの実装」を読んでからほかの章に進むことをお勧めする。第11章はRed Hat Linuxのセキュアなインストールと設定を説明している。

●本書の表記法

各章の冒頭には，その章で学ぶトピックが羅列されている。また，本文中では随所に以下のようなアイコンを使用している。これらのアイコンは特別な情報や重要な情報を示す。

さまざまな問題（場合によってはデータの喪失）の原因となりうる操作を示す。この種の操作を実行するときには，特に注意が必要になる。

本文のトピックに関連して，本書のほかの箇所に記載されている追加情報を示す。

本文のトピックに関連して，興味深い情報や技術的な補完情報を示す。

役に立つヒントやアドバイスを示す。

上述のアイコンに加え，本書では以下の表記法を採用している。

- コードのサンプルは，グレーの背景に等幅フォントで表記する。
- データ構造体や変数名などのコード要素は等幅フォントで表記する。
- 重要な用語は太字で表記する。
- プレースホルダは*italic*で表記する。例えば，ICON *icon file name*という場合，*icon file name*は置き換えるビットマップファイルの名前を表す。
- コマンドは，例えば`boot: linux console=device`のように太字の等幅フォントで記載する。
- メニューは階層順にハイフンで区切って表記する。例えば，［ファイル］-［開く］は，メニューバーから［ファイル］をクリックし，表示されたサブメニューからさらに［開く］を選択することを意味する。
- キーボードのショートカットは，例えばCtrl＋Cキーのように表記する。
- 囲み記事は付加的な情報を提供する。本文で取り上げているトピックには関連していても，本文の理解にとって不可欠ではない情報は，囲み記事として提供している。

Contents

Part1　ネットワークセキュリティを巡る背景　1

Chapter1　ファイアウォールとは何か　3

ファイアウォールの必要性 . . . 3
- ネットワークはどのように脅威にさらされているか . . . 4
- アクセスが問題となるのはなぜか . . . 5

ファイアウォールは何をするか . . . 5

ファイアウォールの種類 . . . 8

ファイアウォールの問題点 . . . 8

そのほかのセキュリティ対策 . . . 10

Chapter2　TCP/IPの概要　11

TCP/IPの用語と概念 . . . 11
- プロトコル . . . 12
  - 層1 ― ネットワーク層 . . . 13
  - 層2 ― インターネット層 . . . 14
  - 層3 ― トランスポート層 . . . 14
  - 層4 ― アプリケーション層 . . . 17
- IPアドレッシング . . . 17
  - クラスAのアドレス . . . 17
  - クラスBのアドレス . . . 18
  - クラスCのアドレス . . . 18
  - 特別なIPアドレス . . . 19
- DNS . . . 21
- ルーティング . . . 21

TCP/IPデータグラムとセグメント . . . 22
- IPヘッダ . . . 23
- ICMPデータグラム . . . 25
- UDPデータグラム . . . 26
- TCPデータグラム . . . 27
  - TCP接続を確立する . . . 29
  - TCP接続を終了する . . . 30

TCP/IPのツール . . . 31
- ifconfig . . . 31
- ping . . . 33
- route . . . 33
- traceroute . . . 34

Contents

- host . . . 35
- dig . . . 35
- nslookup . . . 36
- netcat . . . 37
- tcpdump . . . 38
- tcpshow . . . 40
- iptraf . . . 41

TCP/IPの設定ファイル . . . 42
- /etc/sysconfig/network . . . 43
- /etc/sysconfig/static-routes . . . 43
- /etc/sysconfig/network-scripts/ifcfg-ethn . . . 43
- /etc/nsswitch.conf . . . 44
- /etc/hosts . . . 47
- /etc/resolv.conf . . . 47
- ネットワークの再ロード . . . 48

TCP/IPのトラブルシューティング . . . 48

Chapter3　攻撃と防衛の原則　51

ネットワークセキュリティへの脅威 . . . 51
- 攻撃のレベル . . . 51
- 攻撃者のタイプ . . . 52
- 攻撃の動機 . . . 53
  - 金銭または個人的な利益 . . . 53
  - コンピューティングリソースへのアクセス . . . 53
  - 遊びやいたずら . . . 54
  - 政治的動機 . . . 54
- 攻撃と法律 . . . 55
- 攻撃の被害 . . . 55
  - 保全性の喪失 . . . 56
  - 機密性の喪失 . . . 56
  - リソース可用性の喪失 . . . 57
- 攻撃の目標 . . . 57
  - システムを探る . . . 57
  - サービス拒否（DoS） . . . 58
  - システムに侵入する . . . 59

防衛の原則 . . . 60
- 原則1「敷居を高くする」 . . . 61
- 原則2「権限を最小にする」 . . . 61
- 原則3「制限と許可のポリシー」 . . . 61
- 原則4「最も弱い環」 . . . 62
- 原則5「深い防御」 . . . 63
- 原則6「幅広い防御」 . . . 63
- 原則7「単一のチェックポイント」 . . . 64
- 原則8「隠すことによるセキュリティ」 . . . 65
- 原則9「ソーシャルエンジニアリングに対する防御策」 . . . 65
- 原則10「シンプルであること」 . . . 66
- 警戒心 . . . 66

Chapter4　インターネットサービス　67

ネットワークトラフィック . . . 67

パケットフィルタリング型のファイアウォール . . . 69
- ファイアウォールのアクション . . . 70
- ファイアウォールのルール . . . 71
- ファイアウォールのステート . . . 71

パケットフィルタリングの例 . . . 72
- SSH . . . 72
  - AUTHサービス . . . 74
- FTP . . . 74
  - パッシブモードのFTP . . . 75
  - アクティブモードのFTP . . . 76
  - アクティブモードとパッシブモードの比較 . . . 78

よく使われるTCPアプリケーションプロトコル . . . 79
- AUTH . . . 80
- DNS . . . 80
- メールプロトコル . . . 81
  - IMAP . . . 81
  - POP . . . 81
  - SMTP . . . 82
- NNTP . . . 82
- マルチメディアプロトコル . . . 83
- RSYNC . . . 84
- Webプロトコル . . . 84
  - HTTP . . . 84
  - HTTPS . . . 85

Webプロクシ 85
WHOIS 86
よく使われるUDPアプリケーションプロトコル 86
DHCP 86
DNS 87
NTP 88
Traceroute 88
ICMPトラフィック 89
そのほかのTCP/UDPアプリケーションプロトコル 92
データベースサービス 92
LDAP 92
MySQL 93
PostgreSQL 94
ファイルとプリンタの共有サービス 94
LPD 94
NFS 95
Samba 96
メッセージングとユーザ情報のサービス 97
finger 97
IRC 97
ntalk/talk 98
リモートユーザサービス 99
Telnet 101
RPCベースのサービス 101
「小さい」サービス 103
chargen 103
daytime 104
discard 104
echo 105
quotd 106
time 106
システム/ネットワーク管理のサービス 107
RWHO 107
SNMP 107
システムログ 108
TFTP 108
Xウィンドウシステム 109
Xサーバ 109

XDM 110
XFS 110
サービスの管理とトラブルシューティングのためのツール 110
netstat 111
ps 112
init 113
chkconfig 114
サービス 116

Part2　ファイアウォールの設計と実装　117

Chapter5　ファイアウォールのアーキテクチャ　119

ファイアウォールのテクノロジ 119
パケット転送 120
パケットフィルタリング 123
プロクシ 124
NAT 126
VPN 127
よく使われるファイアウォールのアーキテクチャ 129
ルータファイアウォール 129
シングルホストのファイアウォール 131
マルチホストのファイアウォール 134

Chapter6　ファイアウォールの設計　139

ファイアウォール構築のライフサイクル 139
ファイアウォールの費用と便益 143
定量的アプローチ 143
定性的アプローチ 144
ファイアウォールのアーキテクチャ設計 144
ファイアウォール製品の選択 146
IPChains 146
IPTables 147
TIS Firewall Toolkit 148
CheckPoint Firewall-1 148
ハードウェアベースの製品 149
ファイアウォールのポリシー設計 150

Contents

Chapter7　IPChainsファイアウォール　153

IPChainsの機能 . . . 153
IPChainsのパケットパス . . . 154
ipchainsコマンド . . . 157
- IPChainsのルール . . . 157
  - インタフェース . . . 158
  - ソースのIPアドレス . . . 158
  - 宛先のIPアドレス . . . 159
  - プロトコル . . . 159
  - ポート . . . 160
  - ICMPメッセージのタイプ／コード . . . 160
  - IPとTCPのフラグ . . . 161
  - ターゲット . . . 161
  - ログ . . . 162
- ルールの操作 . . . 162
  - チェーンにルールを追加する . . . 162
  - チェーンにルールを挿入する . . . 162
  - ルールを削除する . . . 163
- チェーンの操作 . . . 163
  - チェーンのデフォルトのポリシーを設定する . . . 163
  - チェーンのルールを一覧表示する . . . 164
  - チェーンをフラッシュする . . . 165
- そのほかの操作 . . . 165
- シンプルなIPChainsファイアウォール . . . 166

IPChainsの管理 . . . 167
- sysctlコマンド . . . 167
- /etc/init.d/ipchainsスクリプト . . . 167
- chkconfigコマンド . . . 169

lokkitツール . . . 169
IPChainsファイアウォールのサンプル . . . 173

Chapter8　IPTablesの機能　183

IPTablesの仕組み . . . 183
IPTablesのパケットパス . . . 185
iptablesコマンド . . . 188
- IPTablesのルール . . . 188
  - プロトコル . . . 189
  - ソースのIPアドレス . . . 190
  - 宛先のIPアドレス . . . 190
  - INPUTインタフェース . . . 191
  - OUTPUTインタフェース . . . 191
  - フラグメントフラグ . . . 192
  - ソースポート . . . 192
  - 宛先ポート . . . 193
  - SYN . . . 193
  - TCPフラグ . . . 194
  - TCPオプション . . . 195
  - ICMPのタイプとコード . . . 195
- そのほかのパケット特性をテストする . . . 196
  - 接続状態 . . . 196
  - 頻度制限 . . . 196
  - MACソースアドレス . . . 197
  - 複数のポート . . . 198
  - マークしたパケットの削除 . . . 198
  - サービスタイプ . . . 198
  - TTL（有効期限） . . . 199
  - プロセス所有権 . . . 199
- IPTablesのターゲット . . . 199
  - 一般的なターゲット . . . 200
  - NAT用のターゲット . . . 202
  - めったに使われないターゲット . . . 202
- ルールの操作 . . . 203
  - チェーンの先頭にルールを追加する . . . 203
  - チェーンの末尾にルールを追加する . . . 204
  - ルールを削除する . . . 204
  - ルールを置き換える . . . 205
- チェーンの操作 . . . 205
  - チェーンのルールを一覧表示する . . . 205
  - チェーンをフラッシュする . . . 206
  - チェーンのデフォルトのポリシーを設定する . . . 207
  - チェーンのカウンタをゼロにする . . . 207
  - ユーザチェーンを作成する . . . 208
  - ユーザチェーンを削除する . . . 208
  - ユーザチェーンの名前を変更する . . . 208

IPTablesファイアウォールのサンプル . . . 209
IPChainsからIPTablesへの移行 . . . 209

Contents

Chapter9　IPTablesファイアウォールの実装　211

サンプルファイアウォールのポリシー 211
ファイアウォールの構造 212
- INPUTチェーン 213
- OUTPUTチェーン 214
- INチェーン 215
- OUTチェーン 218
- IN_ICMPチェーン 220
- OUT_ICMPチェーン 221
- BADIP，FLAGS，SHUNチェーン 223
  - 望ましくないIPアドレス 223
  - TCPフラグ 225
  - 敵対ホスト 226
- FLOODチェーン 227
- ロギングチェーン 228

チェーンのセットアップ 229
ファイアウォールのインストールと運用 230
- カーネルオプションを設定する 230
- IPTablesサービスを有効にする 231
- IPTablesサービスの開始と停止 231

ホストファイアウォールのサンプル 232

Chapter10　IPTablesファイアウォールの高度な実装　241

パケット転送 241
NAT 243
- 宛先NAT（DNAT） 243
  - 透過的プロクシ 244
  - ポート転送 244
  - 負荷分散 245
  - 一般的なケース 245
- リダイレクトNAT 245
  - ポート転送付きのリダイレクトNAT 246
- ソースNAT（SNAT） 247
  - マスカレード 248
  - ローカルネットワークからDNATホストにアクセスする 249

ファイアウォールのパフォーマンスを最適にする 250

スクリーンネットワークファイアウォールのサンプル 252
ファイアウォールを変更する 263
- バージョン管理 263
- ファイアウォールのバックアップ 265
- エラーリカバリ 265

Sysctlオプション 267
カーネルオプション 268
ブリッジファイアウォール 270

Part3　ファイアウォールの運用　273

Chapter11　要塞ホストの実装　275

配置を決める 275
ホストを強化する 276
- ハードウェアを設置する 276
- Red Hat Linuxをインストールする 277
- システムとカーネルのオプションを設定する 278
- ユーザアカウントを設定する 279
- サービスを設定する 280
- ログ機能を設定する 282
- ホストの時刻同期をとる 282
- サービスを保護する 284
- システムをアップデートする 285
- ファイル保全性のベースラインを確立する 287
- バージョン管理とバックアップの手順を確立する 289

Chapter12　ファイアウォールのテストとトラブルシューティング　291

ファイアウォールをテストするツール 291
- Nmap 291
- Firewall Tester 293
  - Firewall Testerをインストールする 293
  - Firewall Testerを設定する 295
  - Firewall Testerを実行する 296
  - Firewall Testerの結果を分析する 297
- Nessus 298
  - Nessusサーバをセットアップする 298
  - Nessusクライアントをセットアップする 300

Contents

スキャンを実行する 303
ポートのテスト 310
回帰テスト 310
トラブルシューティング 311

Chapter13　ファイアウォールの管理　313

リモートロギング 313
- リモートロギングを設定する 314
- リモートロギングをテストする 315

Logwatch 315
- Logwatchの主要な設定ファイル 315
- Logwatchの副次的設定ファイル 317
  - ログファイルグループ 318
  - サービス 319
  - カスタム解析 319

ログの検査と解析のためのそのほかのプログラム 320
- Fwlogwatch 320
  - Fwlogwatchのインストールと設定 321
  - Fwlogwatchのレポート 321
  - Fwlogwatchをカスタマイズする 322
- Port Scan Attack Detector 322
- Swatch 323
  - Swatchのインストール 323
  - Swatchサービスのセットアップ 324
  - Swatchの設定 326
  - Swatchの動作 327

ネットワークを監視する 328
- NetSaint 328
  - NetSaintのインストール 328
  - NetSaintの設定 329
  - NetSaintの機能 329
  - NetSaintの実行 332
- MRTG 332
  - MRTGの設定 333
  - MRTGの実行 333

不正侵入を検知する 334
- DShield 335
  - DShieldの入手 337
  - DShieldの設定 337
  - DShieldのインストール 338
  - DShieldのカスタマイズ 338
  - DShieldの実行 340
- Portsentry 340
  - Portsentryの設定 340
  - Portsentryの構築とインストール 342
  - Portsentryの実行 342
- Snort 343
  - 操作モード 343
  - Snortのインストール 345
  - Snortの設定 345
  - Snortの実行 347
  - Snortルールを作成する 349
  - Snortの高度なルール 351
- SnortSnarf 351
  - SnortSnarfのインストール 352
  - SnortSnarfの実行 352

インシデントに対応する 353

Part4　Appendix　355

Appendix A　VPN　357

VPNのテクノロジ 357
FreeS/WAN 358
- FreeS/WANのインストール 359
- FreeS/WANの設定 360
- VPNの開始と制御 362
  - VPNをテストする 363
- ファイアウォールとVPN 363

Appendix B　ファイアウォールとセキュリティのWebサイト　365

セキュリティ関連のWebサイト 365
メーリングリストとオンラインコミュニティ 366
セキュリティツールとソフトウェア 366
記事，FAQ，HOWTO，ホワイトペーパー 368

Contents

Appendix C　プロトコル番号　371

Appendix D　ポートとサービス　375

Appendix E　ICMPのタイプとコード　381

Appendix F　用語集　383

数字・アルファベット 383
あ行 385
か行 386
さ行 387
た行 390
な行 391
は行 392
ま行 395
や行 395
ら行 396
わ行 397

INDEX　398