

ルータ&パケットフィルタリング 目次.....

はじめに.....3

本書の読み方.....5

---

**◆1章◆ セキュリティ.....13**

**1-1 セキュリティはなぜ必要なのか.....14**

**1-2 クラッカーがサイトを狙う目的.....19**

**1-3 セキュリティ確保の方法.....22**

**1-4 セキュリティポリシーの考え方.....25**

# Router & Packet Filtering

## CONTENTS

## ◆2章◆ TCP/IPとルータの役割.....27

### 2-1 TCP/IPの基礎知識.....28

- 2-1-1 OSI参照モデル.....28
  - OSI各層の働き.....32
- 2-1-2 TCP/IP.....33
  - ネットワークアドレスとホストアドレス.....33
  - クラスとCIDR.....34
- 2-1-3 パケット.....37
  - アプリケーションとポート番号.....38
  - UDPとは.....39
  - TCPとは.....40
  - ICMPとは.....42
  - IPとは.....44
  - イーサネットとMACアドレス.....47
  - プロトコルヘッダ.....48

### 2-2 ルータの役割とその動作.....49

- 2-2-1 ARP.....49
- 2-2-2 ルータが別セグメントにパケットを転送するとき.....51
- 2-2-3 ルーティング情報.....54

---

## ◆3章◆ セキュリティポリシー.....57

### 3-1 セキュリティポリシーの実装に関して.....58

### 3-2 セキュリティポリシーの基本.....59

- 3-2-1 クラッカーの手口と対策.....59
- 3-2-2 プライベートアドレス空間と  
ループバックアドレスを使ったアクセス.....64
- 3-2-3 こちらのIPアドレス空間を使ったアクセス.....65
- 3-2-4 ルーティングを指定しているパケット.....65
- 3-2-5 ルーティング情報を受け付けない.....66
- 3-2-6 ホスト別に不要なポートを閉じる.....66
- 3-2-7 稼働していないホストへのアクセスを記録する.....67
- 3-2-8 クラッカーから姿をくらます.....68
- 3-2-9 万一乗っ取られた場合でも他のサイトに  
影響を及ぼさない方法.....69

# Router & Packet Filtering

## CONTENTS

<b>3-3</b>	<b>危険なポートを閉じる</b> .....	71
3-3-1	一般的に危険と言われているポート.....	71
3-3-2	Proxyの悪用.....	73
3-3-3	メーカー製品が使用しているポート.....	73
	●各メーカーが使用している代表的なポート.....	74
3-3-4	アタックとアタック以外を明確にするテクニック.....	77
3-3-5	フィルタリングフローチャート.....	79
3-3-6	ポートを閉じる場合のセキュリティポリシー.....	80
<b>3-4</b>	<b>必要なポートのみを開く</b> .....	81
3-4-1	外部からサイトへのアクセス.....	82
3-4-2	サイトから外部へのアクセス.....	83
3-4-3	フィルタリングフローチャート.....	86
3-4-4	必要なポートのみを開く場合のセキュリティポリシー.....	87
<b>3-5</b>	<b>ポートを閉鎖しつつ 確立したパケットは通過させる</b> .....	88
3-5-1	フィルタリングフローチャート.....	88
3-5-2	ポートを閉鎖しつつ確立したパケットは 通過させる場合のセキュリティポリシー.....	90

---

## ◆4章◆ 日々の監視作業.....93

### 4-1 アタックの発見方法と対処.....94

- 4-1-1 日々の監視.....94
- 4-1-2 セキュリティ情報の入手.....96
- 4-1-3 アタック元を調べる.....96
- 4-1-4 アタック元に連絡する.....101
- 4-1-5 アタックが続く場合.....103
- 4-1-6 公的機関に報告する.....103

### 4-2 SYSLOG受信ツールとNTPのセットアップ.....104

- 4-2-1 ルータ側の設定.....106
- 4-2-2 Windows 95/98、NT4.0.....107
- 4-2-3 Macintosh.....117
- 4-2-4 UNIX (FreeBSDの場合) .....119

## ◆5章◆ ルータ設定例.....125

### 5-1 想定ネットワーク.....126

### 5-2 YAMAHA RT シリーズ.....128

5-2-1 ポートを閉じる方法.....129

5-2-2 ポートを開く方法.....132

5-2-3 ポートを閉じつつ確立したパケットを  
通過させる方法.....135

### 5-3 MN128SOHO/SL10.....138

5-3-1 ポートを開く方法.....139

# Router & Packet Filtering

.....CONTENTS

## ◆付録◆

147

付録1	トップレベルドメイン	148
付録2	TCP・UDPポート一覧	152
	●よく使用されるポート	152
	●Reserved【予約済み】ポート	166
付録3	参考文献/資料/サイト	194

---

おわりに 195

索引 198

## Column

- |                        |     |
|------------------------|-----|
| 1. 執筆中に検出した不正アクセス      | 56  |
| 2. 絨毯爆撃の傾向             | 92  |
| 3. Port 137がフィルタに引っかかる | 124 |
| 4. サポートに疑問あり           | 146 |

