



# CONTENTS

はじめに 3

<b>第1章</b>	<b>ネットワークセキュリティ入門</b> .....	1
<b>1.1</b>	<b>TCP/IPの概要</b> .....	2
<b>1.1.1</b>	<b>TCP/IP</b> .....	2
<b>1.1.2</b>	<b>OSI参照モデル</b> .....	3
	■OSI参照モデルの階層 .....	3
	●アプリケーション層 .....	4
	●プレゼンテーション層 .....	4
	●セッション層 .....	4
	●トランスポート層 .....	4
	●ネットワーク層 .....	5
	●データリンク層 .....	5
	●物理層 .....	5
<b>1.1.3</b>	<b>TCP/IPプロトコルアーキテクチャ</b> .....	5
	■ネットワークアクセス層 .....	6
	■ネットワーク層 .....	7
	●データグラム .....	8
	●データのフラグメント化 .....	8
	●ネットワークアクセス層とトランスポート層の間のデータの受け渡し .....	8
	●ICMP .....	8
	■トランスポート層 .....	9
	●UDP .....	9
	●TCP .....	10
	■アプリケーション層 .....	11
<b>1.1.4</b>	<b>アドレッシング、ルーティング、マルチプレクシング</b> ...	12
	●アドレッシング .....	12
	●ルーティング(経路制御) .....	12
	●マルチプレクシング .....	12
<b>1.1.5</b>	<b>IPアドレス</b> .....	12
	■IPアドレスの構造 .....	12
	●アドレスの表記 .....	13
	●グローバルアドレスとプライベートアドレス .....	13
	●クラスの問題 .....	14
	■IPアドレスの枯渇とその対策 .....	14
	●IPアドレスの枯渇と短期的解決策(CIDR) .....	14
	●IPアドレスの枯渇と長期的解決策(IPv6) .....	16
	●IPアドレス枯渇に対するその他の対応策 .....	16
<b>1.1.6</b>	<b>ルーティングアーキテクチャ</b> .....	17
<b>1.1.7</b>	<b>ルーティングテーブル</b> .....	17

	■ルーティングテーブルの管理	19
	●ダイナミックルーティング(dynamic routing)	19
	●スタティックルーティング(static routing)	20
1.1.8	■プロトコル、ポート、ソケット	20
	■プロトコル番号	20
	■ポート番号	20
	■ソケット	21
1.1.9	■ソケット接続	22
	■デーモンプロセス	23
	●スーパーサーバ	24
	●親プロセス/子プロセス	24
	●TCP_Wrapper	26
1.2	■ネットワークセキュリティの概要	27
1.2.1	■守るべきものは何か	27
	■情報	27
	■企業/個人の評判	28
	■システム	29
	■ネットワーク	29
1.2.2	■どの程度守るべきか	29
	■情報価値の見積もり	30
	■ブロック化して設定	30
1.2.3	■誰から守るのか	30
	■外部利用者/内部利用者	31
	■確信犯と愉快犯	31
	■踏み台	32
1.2.4	■いかにして守るか	33
	■内部ネットワークをいかにして守るか	33
	●ファイアウォールによるセキュリティ	33
	●IPSec	34
	●SSH	34
	■ホストをいかにして守るか	34
	●TCP_Wrapper	34
	●サーバ自身がアクセス制御する	35
	■ファイルを守る	35
	■ユーザ認証	36
	■データの暗号化	36
	■システムログ	36
	■セキュアネットワーク	37

1.3	代表的な攻撃 .....	38
1.3.1	パスワード攻撃 .....	38
1.3.2	トロイの木馬 .....	38
	■トロイの木馬対策 .....	39
1.3.3	バックドア .....	39
	■バックドアの種類 .....	40
	●ユーザアカウント .....	40
	●ネットワークデバイス .....	41
	●スタートアップファイル .....	41
	●自動メカニズム .....	44
	●共有ライブラリ .....	48
	■バックドア対策 .....	48
	●バックドアをインストールしない .....	48
	●適切なファイルパーミッション .....	49
	●開発環境以外からソースコードを削除 .....	49
	●セキュリティツールの削除 .....	49
	●バックドアの発見 .....	50
1.3.4	ウィルス .....	50
	■広義と狭義のウィルス .....	50
	■バクテリア/ラビット .....	51
1.3.5	スプーフィング .....	51
	■IP(アドレス)スプーフィング .....	51
	■ARPスプーフィング .....	52
	●ARPスプーフィング対策 .....	52
	■ICMPスプーフィング .....	53
	●ICMPスプーフィング対策 .....	53
	■経路スプーフィング .....	53
	■DNSスプーフィング .....	54
	●ゾントランスファとスプーフィング .....	55
	●DNSキャッシュとスプーフィング .....	55
	●DNSスプーフィングの対策 .....	55
	■TCPコネクションスプーフィング .....	56
	●TCPセグメントの認証 .....	56
	●初期シーケンス番号の重要性 .....	56
	●TCPコネクションのハイジャック .....	57
	●TCPコネクションハイジャックの防止 .....	57
	■電子メールスプーフィング .....	58
	●電子メールスプーフィング対策 .....	59
1.3.6	スニффィング .....	59
	■スニフアの原理 .....	60

	■よく使用されるスニファ	60
	■スニッフィング対策	61
	●スイッチドネットワークトポロジー	61
	●スニファの検出	61
1.3.7	ポーツキャン	62
	■何を調べるのか	62
	■ポーツキャンの種類	63
	●TCP (接続)スキャン	63
	●TCP SYNスキャン	64
	●ステルススキャン	64
	●UDPスキャン	66
	■ポーツキャンツール	66
	●ポーツキャンツール	67
	●ポーツキャンの検出ツール	67
	■ポーツキャン対策	68
	●不要なポーツは閉じておく	68
	●WindowsNT環境での対策	68
1.3.8	サービス不能 (DoS) 攻撃	68
	■DoS攻撃の種類	69
	●帯域幅の消費	69
	●リソースの枯渇	69
	●プログラミングの欠陥	69
	●ルーティングDoS攻撃	70
	●DNS DoS攻撃	70
	●DDoS攻撃 (分散型DoS攻撃)	70
	■SYN flood攻撃	70
	●ハーフオープン用のバッファを溢れさせる	71
	●SYN flood攻撃対策	72
	■smurf攻撃	73
	●fraggle攻撃	74
	■ARP攻撃	74
	■フラグメントパケット攻撃	75
	■Out of Band攻撃	75
1.3.9	バッファオーバーフロー	75
	■スタック領域	76
	■バッファオーバーフローの仕組み	77
	■バッファオーバーフローを引き起こす関数	78
	■関数ポインタを破壊する方法	79
	■プログラムの実行権限	80
	■バッファオーバーフローを防ぐ	81
	●Stack Guard	82

	●カーネルの書き換え	82
	●ライブラリの変更	82
1.3.10	ファイル名攻撃	84
	■ファイル名攻撃の仕組み	84
	■ファイル名攻撃への対策	85
1.4	安全性に欠けるプロトコル	86
1.4.1	finger	86
	■fingerサーバ(fingerd)	86
	■finger対策	87
1.4.2	RPCプログラム	88
	■RPCプログラムの危険性	88
	■セキュリティ対策	89
1.4.3	telnet	89
	■セキュリティ対策	89
1.4.4	FTP	90
	■セキュリティ対策	90
1.4.5	TFTP	91
	■セキュリティ対策	92
1.4.6	“r” コマンド	92
1.4.7	X.11	92
	■クライアントサーバ方式	93
	■X11サーバの危険性	93
	■X Window Systemのセキュリティ	94
	●/etc/Xn.hostsによる認証	94
	●xhostによる認証	94
	●トークンベース認証	95
	■X11パケットのフィルタリング	98
第2章	セキュリティポリシー	99
2.1	セキュリティ対策の基本的な考え方	100
2.1.1	セキュリティのポイント	100
	■機密性	100
	■正確性	101
	■可用性	101
	■本人確認	101
	■否認の防止	102
2.1.2	システム構築要件の明確化	102

	●システム構築の目的は何か	102
	●セキュリティポリシーの適用範囲	102
	●システムを構成するハードウェア、ソフトウェア	103
	●保護対象の資産	103
	●準拠すべき法律、規則、標準	103
	●運用体制と保守体制	103
	●セキュリティ事件への対策	103
	●処罰規定	103
	●システム拡張計画	103
<b>2.1.3</b>	<b>リスクの分析と対策</b>	<b>104</b>
	■一般的な脅威とその対策	104
	●物理的な脅威とその対策	104
	●ソフトウェアとデータへの脅威とその対策	105
	●システムへの脅威とその対策	105
	●ネットワークへの脅威とその対策	105
	●ソーシャルエンジニアリングとその対策	106
	■リスクの分析	106
	●リスク分析のステップ	107
	●資産・資源の調査と評価	107
	●リスクの調査と分析	107
	●セキュリティ対策の選択	108
	■実施計画の決め方	108
<b>2.2</b>	<b>セキュリティポリシーの構造と策定手順</b>	<b>109</b>
<b>2.2.1</b>	<b>セキュリティポリシーとは何か</b>	<b>109</b>
	■セキュリティポリシー策定時に考慮すべき事柄	109
	■セキュリティポリシーの記述内容	109
	■セキュリティポリシーの適用範囲	110
	■改訂/更新基準	100
	●改訂の必要な場合	100
	●更新すべき場合	100
<b>2.2.2</b>	<b>ドキュメントの作成手順</b>	<b>111</b>
	■作成チームの結成	111
	■適用範囲の決定	111
	■現状のポリシーを収集	112
	■ドキュメントの作成	112
	■承認	112
	■ドキュメントの配布	112
	■レビューと改訂	112
<b>2.2.3</b>	<b>セキュリティポリシーの例</b>	<b>113</b>
	■総則	113

	■情報資産の把握	113
	■リスクの把握	113
	■情報セキュリティ	113
	■ネットワークセキュリティ	114
	■セキュリティ管理体制	114
	■その他に規定すること	114
2.2.4	セキュリティポリシーの運用基準	115
	■セキュリティ基準	116
	●システム利用者基準	116
	●アクセス承認	116
	●パスワード規約	116
	●正当利用の範囲	117
	●システム管理者の権利と責任	117
	●グループアカウント	117
	●バックアップオペレーション	117
	●追加・変更・廃棄	118
	●ログ監視オペレーション	118
	●障害発生時オペレーション	118
	●倫理規定	118
第3章	暗号技術	119
3.1	暗号技術の概要	120
3.1.1	慣用暗号と公開鍵暗号	120
	■暗号技術の使い分け	120
3.1.2	用語の説明	121
3.2	慣用暗号	122
	■ブロック暗号とストリーム暗号	122
	■拡散と攪乱	122
3.2.1	代表的な慣用暗号	123
	■DES、3DES	123
	●処理モード	123
	●DESの問題点	126
	●3DES (Triple DES)	127
	■AES	128
	■IDEA	128
	■RC2、RC4、RC5、RC6	129
	●RC2	129
	●RC4	129
	●RC5	129
	●RC6	129

	■Blowfish、Twofish .....	130
	●Blowfish .....	130
	●Twofish .....	130
	■CAST-128、CAST-256 .....	130
	●CAST-128 .....	130
	●CAST-256 .....	130
	■慣用暗号アルゴリズムの選択 .....	130
<b>3.3</b>	<b>公開鍵暗号</b> .....	131
<b>3.3.1</b>	<b>公開鍵暗号とは</b> .....	131
	■公開鍵暗号の提供する機能 .....	131
	●暗号化と復号化 .....	131
	●電子署名 .....	132
	●鍵の交換 .....	132
	■代表的な公開鍵暗号方式 .....	133
	■公開鍵暗号の選択 .....	133
<b>3.3.2</b>	<b>RSA</b> .....	133
	■RSAアルゴリズム .....	134
	■RSAはなぜ強固なのか .....	134
<b>3.3.3</b>	<b>Diffie-Hellman法</b> .....	135
	■Diffie-Hellman法のアルゴリズム .....	135
	■Diffie-Hellman法の問題点 .....	136
<b>3.4</b>	<b>ハッシュ関数とメッセージ認証</b> .....	137
<b>3.4.1</b>	<b>一方向性ハッシュ関数</b> .....	137
	■代表的な一方向性ハッシュ関数 .....	138
	●MD2、MD4、MD5 .....	138
	●SHA-1、SHA-256、SHA-384、SHA-512 .....	138
	●RIPEMD-160、RIPEMD-128 .....	138
	■一方向性ハッシュ関数の選択 .....	139
<b>3.4.2</b>	<b>メッセージ認証コード(MAC)</b> .....	139
	■メッセージ認証コード(MAC)の種類 .....	140
	●DES-MAC、AES-MAC .....	140
	●HMAC-MD5、HMAC-SHA-1、HMAC-RIPEMD-160 .....	140
	■メッセージ認証コード(MAC)の選択 .....	140
<b>3.5</b>	<b>電子署名</b> .....	141
<b>3.5.1</b>	<b>電子署名とは</b> .....	141
	■電子署名の基本的な仕組み .....	141
<b>3.5.2</b>	<b>DSA</b> .....	142

	■ DSAの概要	142
	■ DSAのアルゴリズム	143
	● 公開鍵の要素	143
	● 利用者の非公開鍵	143
	● 利用者の公開鍵	143
	● 利用者のメッセージごとの秘密鍵	144
	● メッセージごとの検証鍵(公開鍵)	144
	● メッセージダイジェストの計算	144
	● 署名	144
	● メッセージの送信	144
	● 署名の検証	145
	● 署名の検証がなぜ正しいのか	145
	● DSAの安全性	146
	● DSAの問題点	146
3.5.3	代表的な電子署名のアルゴリズム	147
	● RSA署名	147
	● EL Gamel署名	147
	● DSA (DSS) 署名	147
	● ECDSA署名	147
	■ 電子署名アルゴリズムの選択	148
<b>第4章</b>	<b>システムセキュリティ</b>	149
<b>4.1</b>	<b>アカウントのセキュリティ</b>	150
4.1.1	アカウントの必要性	150
4.1.2	パスワード	150
	■ よいパスワード、悪いパスワード	150
	● よくないパスワードの例	151
	● 解読されにくいパスワードを選択するために	151
4.1.3	セルフパスワードクラッキング	153
	■ クラッキングツール	153
	● Crack	154
	● John the Ripper	154
4.1.4	パスワードの定期変更	155
4.1.5	シャドウパスワードシステム	155
	■ パスワードシステムの切り換え	156
4.1.6	パスワードのないアカウント	157
	■ パスワードのないアカウントの検索	157
4.1.7	休止アカウント	159
	■ 休止アカウントの検索	159
4.1.8	スーパーユーザ	161

	■スーパーユーザのアカウントルール .....	162
	●検索パス .....	162
	●suコマンドを使用する場合は絶対パス指定 .....	162
	●他人のプログラムを実行しない .....	162
	●端末やワークステーションを離れる前にスーパーユーザのシェルから抜ける .....	162
	●rootのパスワードは頻繁に変える .....	162
	●rootのパスワードは他人には教えない .....	163
	●rootではログインしない .....	163
4.1.9	グループアカウントとグループ .....	163
4.1.10	アカウントの使用制限 .....	163
	■アカウントのロック .....	163
	■ログインシェルの変更 .....	164
	■管理者以外のログイン禁止 .....	165
4.1.11	アカウントの保護 .....	165
	■検索パス .....	165
	■初期化ファイル .....	167
	■ファイルとディレクトリのパーミッション .....	167
4.1.12	ユーザの行動の追跡 .....	168
	■lastlog .....	168
	■utmp .....	170
	■wtmp .....	170
	●whoコマンド .....	171
	●lastコマンド .....	171
	●lastbコマンド .....	172
4.2	システムの起動とシャットダウン .....	173
4.2.1	システムのスタートアップ .....	173
	■起動スクリプトの注意点 .....	173
	■システムの起動とシャットダウンの監査 .....	174
	●COPS .....	174
	●Tripwire .....	174
4.3	ジョブスケジューリング .....	175
4.3.1	cronの概要 .....	175
	■crondの起動と停止 .....	175
	■crontabファイルの構成 .....	175
	■crontabファイルの編集 .....	176
	●crontabの使用許可 .....	176
	■cronを利用したバックアップ .....	177
	■cron使用上の一般的な注意事項 .....	178

	●スクリプトファイル、プログラムのパーミッションに注意	178
	●一般のユーザには特別の理由のないかぎりcronを使用させない	178
	●PATHの指定に注意	178
	■cronの監査	178
	●COPSによる監査	179
	●Tripwireによる監査	179
<b>4.4</b>	<b>ログ</b>	180
<b>4.4.1</b>	<b>UNIXシステムログ (syslogd)</b>	180
	■/etc/syslog.conf	180
	●selectorの指定	181
	●ログの保存場所 (actionの指定)	182
	●設定例	183
	●ログの保存に関する注意事項	183
	●xferlog	184
	●cron	184
	●syslogdの再起動	185
	■リモートホストからのログ情報	185
	●ログホストの/etc/syslog.conf	185
	●syslogd起動用のスクリプトファイルの修正	186
	■syslogd自身の対策	186
	●DoS攻撃への対策	187
<b>4.4.2</b>	<b>syslogdの置き換え</b>	188
<b>4.4.3</b>	<b>プログラム固有のログファイル : httpd</b>	188
	■access_log、error_log	189
	■suexec_logファイル	189
	■CustomLogディレクティブ	189
	■LogFormatディレクティブ	190
	●CustomLog、LogFormatの使用例	190
<b>4.4.4</b>	<b>ログファイルの管理</b>	190
	■logrotate	190
	■swatch	191
	●swatchの設定	192
	●swatchの起動	195
	●swatchの自動起動	195
	■logcheck	197
	■logsurf	197
<b>4.5</b>	<b>ファイルシステムのセキュリティ</b>	198
<b>4.5.1</b>	<b>UNIXファイルシステムの概要</b>	198
	■ファイル名	198

	■ディレクトリ名	198
	■ディレクトリの階層構造	199
	■ファイルの種類	199
	●普通のファイル	199
	●ディレクトリファイル	199
	●デバイスファイル	199
	■ファイルの論理構造	200
4.5.2	■ファイルの保護	200
	■ファイルパーミッション	200
	●ファイル属性	201
	■モード	201
	●ファイルの型	202
	●許可されたアクセス方法	202
	■SetuidとSetgid	204
	●set-user-ID (SUID)ビット	204
	●set-group-ID (SGID)ビット	206
	●SUIDとプロセス	206
	●SUID/SGIDビットのセットされたファイルの検索	207
	■stickyビット	209
	■時刻	209
	●最終更新時刻と最終変更時刻の変更	210
	●タイムスタンプの変更	210
	■マスク	211
	●マスクの確認	211
	●マスクの設定	212
	■ディレクトリのパーミッション	212
	■ホームディレクトリ	213
	■デバイスファイル	213
4.5.3	■Tripwireによるファイル改竄チェック	214
	■Tripwire	214
	●Tripwireのパッケージ	215
	●Tripwireの動作	215
	■Tripwireのインストール	216
	●tripwireのプログラム/ファイル	216
	■インストール後の一連の流れ	216
	●ステップ①：ポリシーファイルの作成	216
	●ステップ②：ベースラインデータベースの作成	218
	●ステップ③：整合性のチェック	218
	●ステップ④：Tripwireレポートファイルの確認	218
	●ステップ⑤：データベースのアップデート	219
	●ステップ⑥：ポリシーのアップデート	220
	●ステップ⑦：チェック	223

	●ステップ⑧：設定ファイルの変更	223
	■ポリシーファイルの作成	224
	●プロパティの設定例	227
	●プロパティ設定のポイント	228
	●オブジェクト	229
	●コメント	229
	●ルール属性	229
	●ストップポイント	231
	●命令	231
	■設定ファイルの作成	233
	●設定ファイルに必須の変数	234
	●オプション変数	234
	●電子メールレポートの変数	236
	■レポートの送信	236
	●レポートをメール送信するための設定項目	236
	●設定例	237
	●整合性チェックでのオプション指定	238
	■cronへの登録	238
	■syslogへの出力	238
	■tripwire、twadmin、twprint	239
	●tripwire	239
	●twadmin	239
	●twprint	240
4.5.4	COPSによるローカルシステムのチェック	241
	■COPSを使用するうえでの注意	242
	■システムの必要条件	243
	■インストール	243
	●ソースの入手	243
	●ドキュメント	243
	●コマンドパスの指定	243
	●make	244
	■ファイルの編集	245
	●COPS本体の修正	246
	●is_able.lst	247
	●crc_list	248
	■COPSの実行	249
	●実行例	250
	●実行結果をメールで送信する場合	252
	●自動化スケジューリング	252
第5章	ネットワークサービスのセキュリティ	253
5.1	スーパーサーバinetd	254

5.1.1	inetdの概要	254
5.1.2	inetdの役割	254
5.1.3	inetd.conf	255
	■標準の設定	257
	■telnetサービスの呼び出し例	258
5.1.4	inetdの再起動	259
5.2	TCP_Wrapper	260
5.2.1	TCP_Wrapperとは何か	260
5.2.2	TCP_Wrapperの設定	260
	■hosts.allow	261
	■hosts.deny	263
	■ルール作成の基本的な考え方	263
5.2.3	TCP_Wrapperの使用例	264
	■tcpdchkコマンドによるチェック	264
	■tcpdmatchコマンドによる設定の確認	265
5.3	xinetd	266
5.3.1	xinetdとは何か	266
	■xinetdの機能	266
	●アクセス元のIPアドレスによる制御	266
	●アクセス元のドメイン名による制御	266
	●TCP、UDP、RPCに対する制御	266
	●サービス提供時間の制限	266
	●フルロギングのサポート	267
	●DoS攻撃の抑制	267
	●サービスを特定のインターフェースに限定	267
	●proxyとして利用可能	267
5.3.2	xinetdの入手	267
5.3.3	コンパイル	268
	●pathの指定	268
	●TCP_Wrapperのライブラリの利用	269
	●max_loadのチェック	269
	●IPv6の使用	269
5.3.4	xinetdの設定	269
	■xinetdの起動設定	269
	●スクリプトに実行権を与える	273
	●シンボリックリンク	273
	■設定ファイルの書式	274

■ アクセス制御	275
■ アクセス可能時間の設定	276
■ 接続数の制限	277
● instances	278
● per_source	278
● cps	278
● max_load	278
■ ログの出力	279
● log_type	279
● log_on_success	280
● log_on_failure	281
■ デフォルトセクションの設定	282
● disabledを利用する	282
● 原則拒否の設定	283
■ サービスの設定	284
■ INTERNALサービス	286
● 設定時の注意点	286
■ PORT binding	287
■ 他のホストへのサービスリダイレクション	288
■ chroot	290
● ファイル位置に注意する	291
● chrootディレクトリへのファイルの配置	292
■ TCP_Wrapperのサポート	293
■ IPv6のサポート	294
■ inetd.confファイルの変換	294
■ 属性 (attribute) 一覧	295
● disabled	295
● id	295
● type	295
● flags	295
● disable	297
● socket_type	297
● protocol	297
● wait	297
● user	298
● group	298
● instances	298
● nice	298
● server	298
● server_args	298
● only_from	298
● no_access	298
● access_times	299

- log\_type .....299
- log\_on\_success .....299
- log\_on\_failure .....299
- rpc\_version .....300
- rpc\_number .....300
- env .....300
- passenv .....300
- port .....300
- redirect .....300
- bind .....301
- interface .....301
- banner .....301
- banner\_success .....301
- banner\_fail .....301
- per\_source .....301
- cps .....301
- max\_load .....302
- groups .....302
- enabled .....302
- include .....302
- includedir .....303
- rlimit\_as .....303
- rlimit\_cpu .....303
- rlimit\_data .....303
- rlimit\_rss .....304
- rlimit\_stack .....304

- 第6章 SSH .....307**
- 6.1 なぜSSHが必要なのか .....308**
- 6.1.1 Berkeley “r” コマンド .....308**
- telnetとrlogin .....308
  - NVT .....309
  - rlogin .....309
- FTPとrcp .....310
- rsh .....310
- 6.1.2 “r” コマンドの危険性 .....311**
- /etc/hosts.equivファイル .....311
- ~/rhostsファイル .....313
- トラステッドユーザ .....313
  - トラステッドユーザの危険性 .....313
- トラステッドホストの問題 .....315
- IPスプーフィングの問題 .....315

6.1.3	<b>SSHの概要</b> .....	316
	■SSH実装のバージョン .....	316
	■SSHプロトコルのバージョン .....	316
	●本書の記述について .....	317
6.2	<b>SSH1</b> .....	318
	■ssh1.5パケットヘッダ .....	318
6.2.1	<b>通信の暗号化</b> .....	318
	■sshdのポート番号 .....	319
	■親プロセス .....	319
	■子プロセス .....	319
	■SSH接続シーケンス .....	320
	●SSHバージョン識別名の交換 .....	320
	●サーバはホストとサーバの公開鍵を送信 .....	320
	●共有鍵を生成し、公開鍵で暗号化して送信 .....	320
	●暗号化方式の選択 .....	320
	●暗号化チャネルの確立 .....	321
	●暗号化チャネル上で、ユーザのパスワードを認証 .....	321
	●セッションの接続 .....	321
	●接続の終了 .....	321
	■鍵の交換とセッションの暗号化 .....	321
6.2.2	<b>ユーザ認証</b> .....	325
	■RSAユーザ鍵認証 .....	325
	■Rhosts RSA認証 .....	327
	■Trusted HOST認証(Rhosts認証) .....	328
	■パスワード認証 .....	328
6.2.3	<b>SSH1クライアントの仕組み</b> .....	329
	■クライアントの動作手順 .....	329
6.3	<b>SSH2</b> .....	330
6.3.1	<b>SSH2の標準化</b> .....	330
6.3.2	<b>SSH1.5とSSH2.0の違い</b> .....	330
6.3.3	<b>SSH2プロトコルの概要</b> .....	331
	■SSHセキュリティレイア .....	331
	●トランスポート層 .....	331
	●認証層 .....	333
	●接続層 .....	333
	■バージョンと公開鍵暗号 .....	334
6.4	<b>OpenSSH</b> .....	335

6.4.1	<b>OpenSSHのインストール</b> .....	335
	■OpenSSHのインストールに必要なもの .....	335
	■OpenSSLのインストール .....	336
	●OpenSSLの入手先 .....	336
	●コンパイルの準備 .....	336
	■OpenSSHのインストール .....	337
	●OpenSSHの入手 .....	337
	●コンパイルの準備 .....	338
	●コンパイル .....	338
	●インストール .....	338
6.4.2	<b>SSHサーバの設定</b> .....	338
	■sshd_config .....	339
	■sshd設定ファイルのオプション .....	340
	●通信と暗号化のオプション .....	341
	●認証のオプション .....	344
	●X11フォワーディング、TCPポートフォワーディングのオプション .....	348
	●その他のオプション .....	349
	■sshdの起動 .....	350
	●sshdの自動起動 .....	351
	■sshdコマンドラインオプション .....	351
	●基本的な動作に関するオプション .....	351
	●認証に関するオプション .....	352
	●通信と暗号化に関するオプション .....	353
	●その他のオプション .....	353
6.4.3	<b>SSHクライアントの設定</b> .....	354
	■設定ファイルの書式 .....	354
	●Hostキーワード .....	355
	●特殊な項目 .....	356
	●通信/暗号化に関する項目 .....	357
	●ポート転送に関する項目 .....	360
	●認証に関する項目 .....	363
	●その他の項目 .....	365
	■コマンドラインオプション .....	366
	●基本的な動作に関するオプション .....	366
	●通信と暗号化に関するオプション .....	366
	●X11フォワーディング、TCPポートフォワーディングに関するオプション .....	367
	●端末の制御に関するオプション .....	368
	●ログに関するオプション .....	370
	●認証に関するオプション .....	370
	●その他のオプション .....	371
	■sshコマンドの使い方 .....	371
	●アクセスアカウントの変更 .....	372
	●コマンドのリモート実行 .....	373

	■scpコマンド .....	373
	●scpコマンドのオプション .....	374
	■sftpコマンド .....	376
	●sftpコマンドのオプション .....	377
	●インタラクティブコマンド .....	377
<b>6.5</b>	<b>鍵の管理と公開鍵認証 .....</b>	<b>378</b>
	■ssh-keygenコマンドのパラメータ .....	378
<b>6.5.1</b>	<b>SSH1用の公開鍵認証の鍵ペアの生成 .....</b>	<b>379</b>
	■バージョン1.3と1.5対応のRSA鍵ペアの生成 .....	379
	●鍵ファイルの確認 .....	380
	●公開鍵を接続マシンに転送 .....	381
<b>6.5.2</b>	<b>SSH2用の公開鍵認証の鍵ペアの生成 .....</b>	<b>382</b>
	■DSA鍵ペアの生成 .....	382
	●鍵ファイルの確認 .....	382
	●公開鍵を接続マシンに転送 .....	383
	■バージョン2対応のRSA鍵ペアの生成 .....	383
	●鍵ペアの確認 .....	384
	●公開鍵を接続マシンに転送 .....	384
<b>6.6</b>	<b>認証エージェント .....</b>	<b>385</b>
<b>6.6.1</b>	<b>ssh-agentの設定 .....</b>	<b>385</b>
	■ssh-agentの起動 .....	386
	■ユーザキーの登録 .....	387
	■GNOMEを使用している場合 .....	387
<b>6.7</b>	<b>SSHによるトラフィック転送 .....</b>	<b>389</b>
<b>6.7.1</b>	<b>X11フォワーディング .....</b>	<b>389</b>
	■magic cookie .....	389
	■コマンドの使い方 .....	391
<b>6.7.2</b>	<b>ポートフォワーディング .....</b>	<b>391</b>
	■ローカルポートフォワーディング .....	392
	●ローカルポートフォワーディングの実例 .....	393
	●SSHサーバとアプリケーションサーバが異なる場合 .....	395
	●telnet以外での使用 .....	396
	■リモートポートフォワーディング .....	396
	●リモートポートフォワーディングの実例 .....	396
	●リモートポートフォワーディングの問題点 .....	397
<b>6.8</b>	<b>SSHポートフォワーディングとセキュリティ .....</b>	<b>399</b>
	■ファイアウォールとポートフォワーディング .....	399

	■SSHのアクセス制御機能 .....	400
	■SSHシステム以外のアクセス制御機能の利用 .....	400
<b>第7章</b>	<b>ファイアウォール</b> .....	401
<b>7.1</b>	<b>ファイアウォールの概要</b> .....	402
<b>7.1.1</b>	<b>ファイアウォールとは何か</b> .....	402
	■境界線上で求められるもの .....	402
	■ファイアウォールにできること .....	403
	●セキュリティ管理の効率化 .....	403
	●ログの管理 .....	403
	●被害の最小化 .....	403
	■ファイアウォールにできないこと .....	403
<b>7.1.2</b>	<b>ファイアウォールに関する用語の定義</b> .....	404
<b>7.1.3</b>	<b>ファイアウォールのタイプ</b> .....	406
	■ファイアウォールの基本型 .....	406
	●パケットフィルタリングファイアウォール .....	406
	●プロキシゲートウェイファイアウォール .....	406
	●パケットフィルタとプロキシゲートウェイの違い .....	406
	■パケットフィルタリングファイアウォール .....	407
	●フィルタリングルールの適用 .....	407
	●パケットフィルタリングの長所 .....	408
	●パケットフィルタリングの短所 .....	408
	■プロキシゲートウェイファイアウォール .....	408
	●アプリケーションレベルゲートウェイ .....	409
	●サーキットレベルゲートウェイ .....	411
	●プロキシゲートウェイファイアウォールのコネクション確立 .....	412
	■その他のファイアウォール .....	413
	●ハイブリッドファイアウォール .....	414
	●セッションフィルタリング(コネクションフィルタリング)ファイアウォール .....	414
	●コンテンツフィルタリング .....	416
<b>7.2</b>	<b>パケットフィルタリング</b> .....	417
<b>7.2.1</b>	<b>パケットフィルタリングとは何か</b> .....	417
	■パケットの持つ情報 .....	417
	●IPヘッダ .....	417
	●TCPヘッダ .....	422
	●UDPヘッダ .....	424
	■パケットフィルタリングの判断基準 .....	426
	■パケットフィルタリングとプロキシ .....	426
	■パケットフィルタリングルールの設計指針 .....	427
	●原則拒否のルール .....	427

	●外部からの接続要求を認めない	428
	●入力UDPトラフィックをブロック	428
	●ファイアウォールの外からのX11サーバへの接続を認めない	429
	●内部サーバのポートをチェック	429
	■パケットフィルタリングのバージョン	429
	●ipfwadm	430
	●ipchains	430
	●iptables	430
	■IPフィルタのためのカーネルの再構築	430
	●Linuxでネットワーク機能を使用するための設定項目	431
	●IPフィルタリング機能のための設定項目：カーネル2.2.x	431
	●IPフィルタリング機能のための設定項目：カーネル2.4.x	431
	■パケットフィルタリング利用のための準備	432
	■パケットフィルタリングの処理手順	433
	●どこでフィルタリングを行うか	433
7.2.2	<b>ipchains</b>	434
	■ipchainsの構文	434
	●ipchainsのコマンド	434
	●ルール指定パラメータ	436
	●オプション	438
	■ipchainsの使い方	439
	●基本的なチェーン	439
	●ipchainsの使用例	440
	■ルールの設定	441
	●ipchainsのポリシー	442
	●ポリシーの設定	442
	●電子メールの設定	443
	●telnetの設定	444
	●アクティブオープンとパッシブオープン	446
	●FTPの設定	445
	●DNSの設定	445
	■チェーンの効果的な使用法	447
	●ユーザ定義チェーンの追加	447
	■IPスプーフィングのブロック	449
	■ICMPのフィルタリング	450
	●ブロックすべきICMPメッセージ	451
	●ICMPに関する設定の例	451
	■ipchainsサポートスクリプト	452
	●起動スクリプトの書き方①	453
	●起動スクリプトの書き方②	453
	●RedHat Linuxのブートの仕組み	456
7.2.3	<b>netfilter</b>	461

	■ipchainsの問題点 .....	461
	■netfilterによる改善 .....	461
	●iptables .....	462
	■ipfwadmとipchainsに対する下位互換性 .....	462
	■iptablesの使用法 .....	462
	●iptablesコマンドの書式 .....	463
	●filterテーブルの操作で使用するコマンド .....	463
	●ルール指定パラメータ .....	465
	●オプション .....	466
	●拡張機能 .....	467
	■iptablesの設定例 .....	469
7.2.4	IPマスカレード .....	471
	■IPマスカレードの動作原理 .....	472
	●変換テーブル .....	473
	■IPマスカレードのメリットと副作用 .....	474
	●NATの後ろの内部ネットワークは外から見えない .....	474
	●処理効率の問題 .....	474
	●NATと整合性に欠けるプロトコル .....	474
	■カーネルの再構築 .....	475
	●カーネル2.2.xの場合 .....	475
	●カーネル2.4.xの場合 .....	476
	■iptablesコマンドの書式 .....	476
	●テーブルの選択 .....	476
	●コマンド/パラメータ/オプション/拡張機能 .....	477
	●ターゲット .....	477
	■IPマスカレードの設定 .....	479
	●ipchainsによるIPマスカレード .....	479
	●iptablesによるIPマスカレード .....	480
	■特殊なプロトコル .....	483
	●カーネル2.2.xの場合 .....	483
	●カーネル2.4.xの場合 .....	483
7.3	SOCKS .....	484
7.3.1	SOCKSの概要 .....	484
	■SOCKS server .....	484
	■SOCKS client .....	485
	■SOCKS5の特徴 .....	485
7.3.2	SOCKS5の仕組み .....	486
	■コネクションの要求 .....	486
	■ソケットの利用 .....	487
7.3.3	SOCKS5のインストール .....	488

	●ダウンロード	488
	●ファイルの展開	488
	●Configure	488
	●make	489
	●インストール	489
	●まとめ	489
7.3.4	<b>Configureスクリプトの実行</b>	490
	●再ビルド	492
7.3.5	<b>SOCKS5の設定</b>	492
	■環境設定	492
	■SOCKS5サーバ設定ファイル	493
	●access controlエントリ	493
	●routingエントリ	495
	●authenticationエントリ	496
	●proxyエントリ	497
	■SOCKS5クライアント設定ファイル	498
7.3.6	<b>ユーザ認証</b>	499
	■環境設定ファイル	499
	●ユーザ認証の設定例	500
	●設定時の注意	501
7.3.7	<b>SOCKS5の使用例</b>	501
	■SOCKS5デーモン	501
	■SOCKS5ファイアウォールのアーキテクチャ	502
	●ケース①: Single-homed socks5 server	503
	●ケース②-1: Multi-homed socks5 server	505
	●ケース②-2: Multi-homed socks5 server	506
	●ケース③: Server to Server chaining	507
	■SOCKS5でVPNを作る	509
	●SSLの実装	510
7.3.8	<b>SOCKS5サーバの起動</b>	511
	●RedHat Linuxでのプログラムの自動起動	511
	●/etc/rc.d/init.d/配下のスクリプトファイルの書き方	512
7.3.9	<b>SOCKS5の動作実験</b>	514
7.3.10	<b>アプリケーションのSOCKS対応</b>	515
	■再コンパイル	516
	●makefileの修正	516
	●ソースプログラムの修正	516
	■OpenSSHのSOCKS対応	517
	●OpenSSHバージョン1.xの場合	517
	●OpenSSHバージョン2.xの場合	517
	●connectコマンドの書式	518

	●connectコマンドの使い方 .....	519
	■runsocksの使用 .....	519
	■アプリケーションをSOCKS化するDLL .....	519
7.4	セキュアネットワークデザイン .....	521
7.4.1	ファイアウォールのトポロジ .....	521
7.4.2	セグメンテーション .....	522
7.4.3	VLANの導入 .....	523
第8章	IPSec .....	525
8.1	IPSecとは何か .....	526
8.1.1	TCP/IPのセキュリティ確保 .....	526
	■IPSecのアプローチ .....	526
	■IPSecによるVPNの実現 .....	527
	●イントラネットVPN .....	527
	●エクストラネットVPN .....	527
	●リモートアクセスVPN .....	528
8.2	IPSecの概要 .....	529
8.2.1	IPSecが保証するもの .....	529
	■IPSecの利点 .....	529
	●ホストに負担をかけないサイトセキュリティ向上 .....	529
	●アプリケーションに対して透過的 .....	530
	●端末ユーザに対して透過的 .....	530
	●個人ユーザに対するセキュリティ .....	530
	●ルータの経路制御の保護 .....	530
8.2.2	IPSecの構造 .....	530
	■IPSecのプロトコル .....	531
	■用語の説明 .....	531
	●ピア .....	531
	●トランスフォームセット .....	531
8.2.3	セキュリティアソシエーション .....	532
	■SAの識別 .....	532
	●SPI (Security Parameters Index) .....	532
	●宛先IPアドレス .....	532
	●セキュリティプロトコルの識別子 .....	532
	■SAD .....	533
	●シーケンス番号カウンタ .....	533
	●シーケンス番号の範囲超過 .....	533
	●リプレイ攻撃防止ウィンドウ .....	533

	●AH情報	533
	●ESP情報	533
	●パケットが属しているSAの有効期間	533
	●IPSecプロトコルモード	534
	●経路MTU	534
	■SAセレクト	534
8.2.4	IPSecトンネルモードとトランスポートモード	535
	■トランスポートモード	535
	■トンネルモード	536
	●トンネルモードで保護されるもの	539
8.2.5	パケット認証ヘッダ	539
	■MACを利用する	539
	●MAC計算に使用される項目	540
	■AHヘッダフォーマット	541
	●トランスポートモードとAH	542
	●トンネルモードAH	542
8.2.6	カプセル化セキュリティペイロード(ESP)	542
	■ESPフォーマット	543
	●トランスポートモード	544
	●トンネルモード	545
	■暗号化と認証アルゴリズム	546
8.2.7	SAの組み合わせ	546
	■AHとESPの違い	546
	■SAバンドル	547
	●トランスポート隣接(transport adjacency)	547
	●繰り返しトンネリング(iterated tunneling)	548
	●トランスポート隣接と繰り返しトンネリングの組み合わせ	548
8.2.8	自動鍵交換：IKE	552
	■IKEでSAを動的に作成する	552
	●フェーズ1	552
	●フェーズ2	553
	■IKEの特徴	554
	●双方向性	554
	●SAの動的確立	554
	●動的な鍵の再生成	554
	●デジタル証明書とCAサーバによる認証	555
	●PFS (Perfect Forward Secrecy)	555
	■IKEのプロトコル	555
	●ISAKMP	555
	●Oakley、SKEME	556
	■アンチリプレイ攻撃	556

	●スライディング受信ウィンドウ .....	556
	●その他のリプレイ攻撃 .....	558
<b>8.3</b>	<b>PKI</b> .....	559
8.3.1	公開鍵の保証 .....	559
	■公開鍵の信頼性を保証する第三者 .....	559
8.3.2	標準PKI : X.509 .....	560
	■CAの公開鍵は信用できるのか .....	561
<b>8.4</b>	<b>IPSecと他のテクノロジーとの比較</b> .....	562
8.4.1	データリンク層レベルの技術との対比 .....	562
8.4.2	アプリケーション層レベルの技術との対比 .....	563
	■攻撃に対する防御力 .....	563
<b>8.5</b>	<b>FreeS/WAN - IPSecの実装</b> .....	564
8.5.1	FreeS/WANの概要 .....	564
	■対応カーネル .....	564
8.5.2	FreeS/WANのインストールに必要なもの .....	565
8.5.3	カーネルの設定 .....	565
	■カーネル設定の手順 .....	566
	●initrdイメージの作成 .....	567
	■FreeS/WAN IPSecゲートウェイのためのカーネルオプション .....	568
	●Code maturity and level options .....	568
	●Processor type and futures .....	569
	●Loadable module support .....	569
	●General setup .....	570
	●Plug and Play support .....	570
	●Blockデバイス .....	570
	●Networkingオプション .....	570
	●Telephony support .....	577
	●SCSI support .....	577
	●I2O device support .....	577
	●Network device support .....	577
	●Amateur radio support .....	577
	●IrDA (infrared) support .....	577
	●ISDN subsystem .....	577
	●Old CDROM drivers .....	577
	●Character devices .....	577
	●Filesystems .....	577
	●Network filesystems .....	578
	●Console drivers .....	578
	●Sound .....	578

	●Kernel hacking .....	578
<b>8.5.4</b>	<b>FreeS/WANの入手</b> .....	578
	■ソースの展開 .....	578
<b>8.5.5</b>	<b>FreeS/WANのインストール</b> .....	579
	■インストールステップ .....	580
	■新しいカーネルのインストール .....	581
	●メッセージを確認する .....	581
<b>8.5.6</b>	<b>FreeS/WANの設定ファイル</b> .....	583
	■ipsec.conf .....	583
	●共通パラメータ .....	585
	●CONNセクションのパラメータ .....	585
	●CONFIGセクションのパラメータ .....	591
	■ipsec.secrets .....	595
	●index .....	596
	●エントリ .....	596
	■FreeS/WANの設定例 .....	597
	●ipsec.confファイルの修正 .....	598
	●ipsec.secretsファイルの修正 .....	600
	●設定ファイルを反映させる .....	601
<b>8.5.7</b>	<b>IPSec接続のテスト</b> .....	601
	■インターフェースの確認 .....	602
	■接続のスタート .....	604
	■確認と接続のクローズ .....	605
	●クローズ .....	606
	●その他のテスト .....	606
<b>8.5.8</b>	<b>IPSecによる内部ネットワークの保護</b> .....	606
	■サブネットワークのセット .....	607
<b>8.6</b>	<b>IPSec導入への今後の課題</b> .....	609
<b>8.6.1</b>	<b>処理能力の問題</b> .....	609
<b>8.6.2</b>	<b>実行順序の矛盾</b> .....	609
<b>8.6.3</b>	<b>帯域幅の最適化</b> .....	610
	■リンク層の圧縮 .....	610
	●IPcomp .....	611
	■QoS .....	612
	●QoSとは何か .....	612
	●QoSとキュー管理 .....	612
	●QoSとIPプレシデンス(優先度) .....	612
	●IPプレシデンスを再定義するDiffserv .....	613
	●IPSecとRSVP .....	613

	●SAとQoS .....	614
8.6.4	マルチキャスト .....	615
	■マルチキャストにIPSecを利用する場合の問題点 .....	615
	●IKEの鍵管理との関係 .....	615
	●送信元の認証の問題 .....	615
	●SPIとアルゴリズムの選択 .....	615
	●リプレイ攻撃との関係 .....	615
	■マルチキャストセキュリティフレームワーク .....	616
	■マルチキャスト通信の保護 .....	616
	●MESP .....	616
	●AMESP .....	616
	■グループ鍵管理 .....	617
8.6.5	パケットの分類 .....	617
	■パケットフィルタ .....	617
	■プロキシファイアウォール .....	618
	■コンテンツフィルタ .....	618
	■NAT(ネットワークアドレス変換) .....	619
	●NATを使うためには .....	620
8.6.6	ネットワークインフラストラクチャ .....	620
	■IPルーティングプロトコル .....	620
	●認証 .....	620
	●ルートのアップデート情報の暗号化 .....	621
	■ドメインネームシステム(DNS) .....	621
	●DNSクライアントからの問い合わせにDNSサーバが回答できない場合 .....	621
	●ゾーン転送 .....	622
8.6.7	ネットワーク監視 .....	622
8.6.8	ネットワーク管理 .....	623
	■SNMP .....	623
	■RMON .....	624
8.6.9	音声と映像 .....	624

索引 .....	625
----------	-----

