

目

次

第1章	電子メールに潜む危険と その対処	1
1.1	電子メールがメッセージ伝達の中心となりつつある	2
1.2	電子メールがコンピュータウイルスの感染経路 ナンバーワンとなっている	5
1.3	マクロウイルスは簡単に作り出される	8
1.4	HTMLメールからの感染もある	10
1.5	電子メール悪用ウイルスはなぜ急増したのか	11
1.6	コンピュータウイルスは 誰が何のために作り出しているのか	14
1.7	コンピュータウイルスに対抗する	15
	■クライアント用ウイルス対策ソフト	17
	■サーバ用ウイルス対策ソフト	17
	■ゲートウェイ用ウイルス対策ソフト	17
1.8	ウイルス対策ソフトは更新が必要	18
1.9	未知のコンピュータウイルスにも 対抗する必要がある	22
	■スタティックヒューリスティック法	23
	■ダイナミックヒューリスティック法	24
1.10	最悪の場合に備えてバックアップをとっておく	30
1.11	不要なメールが送りつけられる	31
1.12	メールが不正に使われる	35

1.13	電子メールを使った攻撃に対抗する	37
------	------------------------	----

第2章 インターネットで やり取りする情報を守る 41

2.1	インターネットを流れる情報は狙われている	42
2.2	インターネット上の情報はこうして盗聴、 改ざんされる	43
2.3	盗聴、改ざんを防止するには暗号メールを使用する ..	46
2.4	暗号化のしくみ	50
	■暗号化とはどのようなものか	50
	■共通鍵暗号化方式	53
	■公開鍵暗号化方式	56
2.5	電子署名のしくみ	58
2.6	認証機関とは	60
2.7	暗号メールの詳細	63
	■PGP	64
	■S/MIME	65
	■S/MIMEとPGPの違い	66
2.8	暗号メールの現実	66
2.9	進化する暗号化	68
	■強力な公開鍵暗号化方式	68
	■次世代の共通鍵暗号化方式	69

第3章	オンラインショッピングを安全に進める	71
3.1	インターネットを普及させたホームページ	72
3.2	オンラインショッピングの情報が盗み出される危険がある	79
3.3	そのホームページは本物か	82
3.4	ホームページと安全にやり取りする	84
3.5	インターネットでの情報のやり取りはSSLが標準となっている	87
3.6	SSLはWWWサーバを認証する	88
3.7	SSLは利用者を認証することもできる	90
3.8	利用者はまだまだ安全性を信頼していない	91
3.9	オンラインショッピングで扱う情報に対する本質的な危険	93
3.10	より安全なクレジットカード決済を実現するSET	94
	■SETを使用するには	96
	■SETのしくみ	98
	■SETの現状	102
3.11	セキュリティ確保のためのインフラ	105

第4章 インターネットからの侵入攻撃を防ぐ 111

- 4.1 インターネットに接続するとどうなるか 112
- 4.2 増加するホームページへの攻撃 114
- 4.3 誰が不正アクセスをしているのか 116
- 4.4 コンピュータ自身にも不正利用防止機能はある 119
- 4.5 境界点に警備員を置いてインターネットからの不正アクセスを防止する 124
- 4.6 パケットフィルタリングで最低限のセキュリティは守れる 128
 - パケット通信 128
 - パケットフィルタリング 131
- 4.7 パケットフィルタリングの弱点をつく攻撃 134
- 4.8 ステートフル・インスペクション方式のファイアウォール 137
- 4.9 高いセキュリティを確保できるアプリケーションレベルゲートウェイ方式ファイアウォール 138
 - プロキシサーバ 138
 - アプリケーションレベルゲートウェイ 139
 - アプリケーションレベルゲートウェイ方式の欠点 142
- 4.10 ファイアウォールを構築するにはファイアウォール製品を使用するか、構築サービスを利用する 143
- 4.11 パーソナル・ファイアウォールの使用 146

- 4.12 インターネットからアクセス可能なサーバは
どう設置するか 147
- 4.13 プライベートアドレスを使って安全性を高める 151
- 4.14 ファイアウォールは万能ではない、
それをカバーする必要がある 153
- 4.15 セキュリティの欠陥がないか検査することが
必要である 157

第5章 **モバイルコンピューティングと リモートアクセスを安全に行う** 161

- 5.1 コンピュータの小型軽量化と携帯電話／PHSの普及に
よりモバイルコンピューティングがさかんになる ... 162
- 5.2 モバイルコンピューティングではファイアウォールに
頼れない 166
- 5.3 リモートアクセスには危険がある 167
- 5.4 不正アクセスの簡単な防止策 169
- 5.5 規模の大きいネットワークでは
認証サーバを設置する 170
- 5.6 ワンタイムパスワードを使った認証でセキュリティを
強固にする 173
- トークンを使用してワンタイムパスワードを
生成する方法 173

- トークンを使わないワンタイムパスワード認証システム ... 175
- 安全なモバイルコンピューティングの実現 177

第6章 ネットワーク同士を安全に接続する 179

- 6.1 企業内ネットワークを拡張する
拠点間ネットワーク 180
- 6.2 LAN間接続の手段 183
- 6.3 プロバイダが提供するIP-VPNサービスを利用すれば
安全、高速な拠点間通信が行える 185
- 6.4 インターネットをプライベートネットワークとして
利用する 188
- 6.5 トンネリングと暗号化によりインターネットを
安全な拠点間ネットワークにする 189
- 6.6 安全なインターネットVPNを実現するための
標準技術 192
- 6.7 IPSecのしくみ 194
- 6.8 インターネットVPNの弱点 197
- 6.9 IP-VPNを使うのかインターネットVPNを
使うのか 198

第7章 セキュリティ対策システム 構築の考え方 201

7.1	セキュリティ対策システム構築の計画	202
■	全組織的な体制の策定	203
■	セキュリティ対策の基本方針の策定	203
■	予算計画の策定	206
■	セキュリティ対策製品／サービスの購入計画の策定	206
■	緊急時対応計画の策定	207
7.2	セキュリティ対策システムの導入	208
■	セキュリティ対策システムを構成する製品、サービスの導入	208
■	試験運用	209
7.3	セキュリティ対策システムの運用	210
■	監 査	210
■	監 視	210
■	保 守	211
■	セキュリティ教育	211
■	回 復	212
■	補 償	212

第8章 ネットワークセキュリティを 取り巻く環境

213

8.1	ネットワークセキュリティに関連する法整備	214
	■不正アクセス防止法	214
	■電子署名法	215
	■暗号技術輸出規制	216
8.2	個人情報保護法とネットワークセキュリティ	217
8.3	保険による被害の補償	220
8.4	セキュリティの国際標準基準	221
8.5	ネットワーク犯罪の世俗化	222

コラム

Webから侵入する不正なプログラム ～コンピュータウイルス、スパイウェア、インターネットバンダル～	26
増加する有害なホームページに対抗する	75
電子商取引とは	103
サービスを停止させる攻撃	116

索引	223
----------	-----

