

# 目次

はじめに

## Chapter1

### 狙われているあなたのデータ

#### 誰もが利用しているインターネット

個人から企業まですでにインターネットはインフラになった..... 10

#### 居ながらにしてさまざまなサービスを受けることができる

急速にさまざまなサービスが増加しているインターネット..... 12

#### インターネットに流れる重要情報

個人情報から企業機密まで重要な情報が24時間流れている..... 14

#### 危ない人が多いインターネット

誰でも被害者になり加害者になれるインターネット..... 16

#### ハッキングはカンタン!

誰でもハッカーになれる..... 18

#### 勝手に入り込んだり、盗んだり

多様化するハッキングの手口..... 20

#### なぜ狙われるのか?

情報自体を利用する場合とそれ以外の場合がある..... 22

#### 盗んだり壊さずに利用する

侵入して利用するというのが最近のトレンド..... 24

#### セキュリティを確保する

侵入の防御と運用面での管理がポイント..... 26

#### セキュリティ意識を高めることがポイント

ファイアウォールだけではセキュリティは確保できない..... 28

Column ハッキングされて何を失うのか?..... 30

## Chapter2

### ハッキングの手口

#### ハッキングの種類

主なハッキングの手口には7種類ある..... 32

#### 密かに入り込む「侵入」

最も基本となるのがネットワークへの侵入だ..... 34

#### プライバシーを覗かれてしまう「盗聴」

データを拾い集め再構築して盗聴する..... 36

#### 勝手にデータを変えてしまう「改ざん」

電子データは簡単に改ざん/消去が可能..... 38

<b>他人にすり替わる「なりすまし」</b> 知らない間に膨大な請求が来るなりすましの脅威	40
<b>データやシステムを壊してしまう「破壊」</b> ソフト的に壊すことは簡単にできる	42
<b>他の人の活動を阻害する「妨害」</b> ネットワークコミュニティならではの問題	44
<b>知らないうちに感染するウイルス</b> 謎の病原体として繁殖するウイルス	46
<b>ハッキングテクニックを知っておく</b> 基本的にはシステムの弱点を攻撃するのがハッキングの基礎	48
<b>オープンネットワークのメリット/デメリット</b> 開かれたネットワークだからこそハッキングはなくなる	50
Column 常に調査や攻撃を受けているサーバー	52

## Chapter3

### インターネットの基礎知識

<b>インターネットの歴史</b> インターネットについて知っておこう	54
<b>インターネットのしくみ</b> プロバイダによって構成されているインターネット	56
<b>サーバーとクライアント</b> ネットワークを構築するサーバーとクライアントとは?	58
<b>データを中継する中継機器</b> データを通信回線に乗せるためには変復調装置が必要	60
<b>パケット通信とは?</b> 通信ネットワークではデータをそのまま送らない	62
<b>通信プロトコルとは?</b> データの送受信にはルールが必要だ	64
<b>インターネットは通信プロトコルのかたまり</b> さまざまな通信プロトコルによってデータを伝送する	66
<b>階層構造を持つ通信プロトコル</b> 通信プロトコルは7つの種類に分類することができる	68
<b>TCP/IPのしくみ</b> TCPとIPが合体したTCP/IPはパケット通信の基本だ	70
<b>データを伝送するIP</b> 相手先を見つけ、最短経路を探り、エラーを確認するIP	72
<b>データの中身をチェックし通信をコントロールするTCP</b> TCPのおかげでデータの中身が保証され、通信が円滑に行われる	74
<b>上位通信プロトコルへパケットを引き渡すTCP</b> ポート番号で上位通信プロトコルとパケットのやり取りを行う	76

<b>IPアドレスとは?</b> 相手先のコンピュータを特定するにはIPアドレスを使う	78
<b>IPアドレスのしくみ</b> IPアドレスはグローバルアドレスとプライベートアドレスがある	80
<b>ドメイン名とIPアドレス</b> DNSによってIPアドレスとドメイン名を変換する	82
<b>最短経路を探し出すルーティング</b> ルーターは2つのIPアドレスを持っている	84
<b>通信プロトコルとパケットの流れ</b> パケット通信では各階層同士の通信プロトコルでやり取りを行う	86
Column 通信プロトコルとハッカー	88

## Chapter4

### データを守るための基礎知識

<b>守るべき情報には何があるか?</b> 企業情報、個人情報それぞれに守るべき情報がある	90
<b>物理的に情報を守る、ソフト的に情報を守る</b> 物理的なセキュリティとソフト的なセキュリティを組み合わせる	92
<b>IDとパスワードによる認証</b> IDとパスワードは唯一の本人認証手段	94
<b>認証のしくみ</b> 認証にはレベルがある	96
<b>利用者の利用範囲を限定するアクセス権</b> 重要なデータを利用できる人を制限するアクセス権	98
<b>パケットレベルのセキュリティ</b> パケット単位でセキュリティを確保する	100
<b>ファイアウォールとは?</b> ハッキングからの守護神がファイアウォールサーバーだ	102
<b>暗号化によって安全にデータを送る</b> 積極的にセキュリティを確保する暗号化	104
<b>秘密鍵方式での暗号化</b> 同じ鍵を使って暗号化と復号を行うのが秘密鍵方式	106
<b>公開鍵方式での暗号化</b> 2つの鍵で暗号化する公開鍵方式	108
<b>電子署名とは?</b> 公開鍵方式の暗号化を利用したのが電子署名	110
<b>電子証明書とは?</b> インターネット時代の必須アイテムが電子証明書だ	112
<b>SETとSSLのしくみ</b> オンラインショッピングの安全性を高める技術	114
Column 電子証明書が普及しないワケ	116

## Chapter5 身近なセキュリティ対策

<b>すぐそこにある危険</b> 日常的なことから注意しよう .....	118
<b>オフィス内での危険性</b> 一番危ないオフィスでのパソコン利用 .....	120
<b>IDとパスワードを守るには？</b> もっとも基本となるIDとパスワードのセキュリティ .....	122
<b>他人にコンピュータを覗かれないために</b> パソコンを他人が利用できなくすることがポイント .....	124
<b>常時接続時代の落とし穴</b> 常時接続は企業内のLANのパソコンと同じと考えよう .....	126
<b>常時接続時代のパーソナルセキュリティ</b> 自分の情報やコンピュータは自分で守るセキュリティ意識が必要 .....	128
<b>無線LANも危ない</b> 無線LANもセキュリティ対策を検討する .....	130
<b>捨てるとき、貸すときのセキュリティ対策</b> コンピュータにはデータが記録されていることを忘れずに！ .....	132
<b>悪徳商法もハッキングの一種だ</b> 意味のない電子メールや悪徳商法からのセキュリティ .....	134
<b>ブラウザクラッキングに注意</b> ホームページを見ただけでコンピュータが動作しなくなるブラウザ .....	136
Column 個人でもできるアクセス権設定 .....	138

## Chapter6 ハッキングあれこれ

<b>ウイルスとは？</b> 伝染→発症→伝染を繰り返すウイルス .....	140
<b>ウイルスの種類</b> ウイルスにはさまざまな種類があり、次々に新種が登場している .....	142
<b>ますます巧妙化するウイルス</b> 知らない間にハッカーの手先になってしまうこともあるのだ .....	144
<b>ウイルス対策</b> ウイルスには検知ソフトと駆除ソフトで対応する .....	146
<b>侵入の手口</b> 絶対に侵入できないということはない .....	148
<b>パスワードを盗む</b> パスワードは意外に簡単に盗むことができる .....	150
<b>通信プロトコルの機能を悪用する</b> 便利な機能を逆手にとって悪用する .....	152

<b>セキュリティホールを狙う</b> セキュリティホールはバグだけではない .....	154
<b>ハッカーは綿密な調査を行う</b> 闇雲にハッキングをするわけではない .....	156
<b>DOS攻撃</b> DOS攻撃にはさまざまなバリエーションがある .....	158
<b>犯人が特定できないDDOS攻撃</b> 一度にたくさんのクライアントから攻撃されるDDOS攻撃 .....	160
<b>バックドアで自由に侵入する</b> バックドアを作られたら、ハッカーの手中に落ちたも同然だ .....	162
<b>踏み台にされるコンピュータ</b> 痕跡を残さずに踏み台にされるとまったくわからない .....	164
<b>ホームページのハッキング</b> ホームページの改ざんやブラウザは簡単に効果のあるハッキング .....	166
Column ハッキングの手口もどんどん進化する .....	168

## Chapter7 LANとセキュリティ

<b>LANとは？</b> LANについてきちんと理解しておこう .....	170
<b>LANを構成する機器</b> ルーター、ゲートウェイサーバー、ハブが3種の神器 .....	172
<b>サーバーとセキュリティの関係</b> サーバーが停止するとネットワークも使えなくなる .....	174
<b>LANとインターネットの違いはどこにある？</b> グローバルアドレスとプライベートアドレスの違い .....	176
<b>通信プロトコルとLAN</b> LAN内ではどんな通信プロトコルを使ってもOK .....	178
<b>3種類のプロバイダLANへのアクセス方法</b> 常時接続環境がセキュリティ上注意しなければならないワケ .....	180
<b>LANでのセキュリティ</b> ソフト的なセキュリティと運用面でのセキュリティがポイント .....	182
<b>公開サーバーの配置</b> LAN内では公開サーバーの配置がセキュリティのポイントになる .....	184
Column ハッカーとクラッカー .....	186

## Chapter8 インターネットと法律

<b>インターネットと法律</b> .....	188
現実社会と同様に法律が適用されるインターネット .....	188

<b>知的所有権とは</b>	
サーバー内の情報は知的所有権として保護されている.....	190
<b>特許のハッキング</b>	
申請しなければ特許にならない.....	192
<b>著作権は自動的に発生する</b>	
知らないで権利を侵害してしまう著作権.....	194
<b>侵入を犯罪行為とみなす不正アクセス禁止法</b>	
ハッキングそのものを処罰の対象とした法律.....	196
<b>不正競争防止法</b>	
不正競争防止法で差し止め請求ができる.....	198
<b>オンラインショップを取り巻く法律</b>	
オンラインショップも現実の法律が適用される.....	200
<b>権利を侵害した場合はどうするか？</b>	
調査し、権利者を確定してから最終決定を行う.....	202
Column ウイルスは犯罪か？.....	204

## Chapter9

### セキュリティ対策の実際

<b>セキュリティ対策を考えよう</b>	
セキュリティ対策の流れを理解しておく.....	206
<b>セキュリティポリシーとは？</b>	
セキュリティの方針を決めてトップダウンで実行する.....	208
<b>ネットワークの構成を見直す</b>	
すでにLANが構築されている場合には見直しが必要.....	210
<b>サーバーの設置方法を考える</b>	
公開サーバーのセキュリティを確保する.....	212
<b>システム設定の重要性</b>	
設定がきちんと行われていれば90%のハッキングは防げる.....	214
<b>システムをバックアップしておく</b>	
ネットワークシステムにダウンはつきものだ.....	216
<b>ウイルスを防ぐ</b>	
ウイルス防御ソフトで対処する.....	218
<b>アクセス権によるセキュリティ対策</b>	
利用制限によってネットワーク内のデータを守る.....	220
<b>システム監査の実施</b>	
ネットワークは常にメンテナンスが必要.....	222
<b>セキュリティ教育と啓蒙</b>	
利用者のセキュリティ意識がないとセキュリティ対策は無意味.....	224
<b>セキュリティをアウトソーシングする</b>	
セキュリティ対策やサーバーを丸ごとアウトソーシングするケース.....	226
Column 企業とともに成長していくセキュリティ対策.....	228