

目 次

① インターネットの仕組み.....	1
1.1 電話とインターネット.....	2
1.2 プロトコル.....	8
1.3 OSI 参照モデルと階層化.....	10
1.4 第1層（物理層）.....	13
1.5 第2層（データリンク層）.....	16
1.6 第3層（ネットワーク層）.....	21
1.7 第4層（トランスポート層）.....	32
1.8 第7層（アプリケーション層）.....	39
1.9 DNS（ドメイン名とIPアドレス）.....	39
1.10 HTTP（ホームページとブラウザ）.....	41
1.11 SMTP（電子メール）.....	43
1.12 POPとIMAP（郵便局と郵便ポスト）.....	48
② 暗号の世界へ飛び込もう.....	51
2.1 コンピュータにおける3つの脅威.....	51
2.2 情報セキュリティ3大要素 CIA.....	54
2.3 古代暗号を見てみよう.....	55
2.4 共通鍵暗号.....	61
2.5 暗号モード.....	66
2.6 優れたアイデア D-H鍵共有.....	67
2.7 modの世界へようこそ.....	72
2.8 公開鍵暗号.....	76

2.9 橋円曲線暗号	82
2.10 暗号危険化を知ろう	85
(3) インターネットとセキュリティ	95
3.1 トンネリング	95
3.2 電子署名を知ろう	97
3.3 公開鍵認証基盤 (PKI)	102
3.4 インターネットと PKI の関わり	108
3.5 SSL/TLS	111
3.6 電子証明書を見てみよう	120
3.7 私たちの生活と PKI	128
(4) インターネットにおけるサイバー攻撃	133
4.1 解析ツールを使ってみよう	134
4.2 マルウェア	136
4.3 DDoS を知ろう	143
4.4 アンプ (增幅) 攻撃	146
4.5 フラッディング攻撃	147
4.6 なりすまし	150
4.7 標的型攻撃の脅威	150
4.8 ドライブバイダウンロード	154
4.9 ソフトウェアアップデート機能の悪用	155
4.10 クロスサイトスクリプティング (XSS)	156
4.11 SQL インジェクション	159
4.12 WAF を知ろう	171
4.13 セッション ID とクッキーの関係	172
4.14 セッションハイジャック	175
4.15 DNS キャッシュポイズニング	176
4.16 クロスサイトリクエストフォージェリ (CSRF)	180
4.17 匿名化と Tor	187

4.18 ゼロデイ脅威に気づこう	192
4.19 トラヒックと可視化	193
(5) ハードウェアとソフトウェア	197
5.1 暗号ハードウェア	198
5.2 サイドチャネル攻撃を知ろう	199
(6) 私たちを取り巻くセキュリティ	203
6.1 脆弱性に関わる情報源	204
6.2 情報セキュリティと法律を見てみよう	205
6.3 セキュリティ人材育成の取り組み	214
サイバーセキュリティへの確かな道標に寄せて (コーディネーター 井上克郎)	221
索 引	226