目　次

はじめに　iii

第 1 章
ネットワークセキュリティ序説　1

1.1 インターネットの発展と潜在する脅威　**1**

1.2 具体的な脅威　**9**

第 2 章
古典的な暗号　22

2.1 準備　**22**

2.2 転置暗号　**24**

2.3 換字暗号　**25**

第 3 章
共通鍵暗号　41

3.1 はじめに：古典暗号から現代暗号へ　**41**

3.2 DES　**42**

3.3 DES に対する解読法　**49**

3.4 トリプル DES　**55**

3.5 AES　**57**

3.6 暗号アルゴリズムの適用　**61**

第 4 章
公開鍵暗号 (1) — 基本的な考え方　68

4.1 はじめに：共通鍵の問題　**68**

4.2 公開鍵暗号のアルゴリズム (RSA) 69

4.3 ハイブリッド暗号 82

第 5 章 公開鍵暗号 (2) — デジタル署名と公開鍵の配送 85

5.1 デジタル署名 85

5.2 公開鍵の配送について 95

第 6 章 ユーザ認証 103

6.1 ユーザ認証とは 103

6.2 ユーザ認証の仕組み 104

6.3 認証情報 105

6.4 ユーザ認証に対する脅威 109

6.5 ユーザ認証の強化 114

6.6 CAPTCHA 117

第 7 章 組織内ネットワークのセキュリティ 123

7.1 組織内ネットワーク 123

7.2 ネットワーク機器におけるセキュリティ対策 125

7.3 ファイアウォールと侵入検知システム 129

7.4 無線 LAN のセキュリティ 136

第 8 章 インターネットのセキュリティ 142

8.1 インターネットにおけるセキュリティ 142
8.2 Web におけるセキュリティ 143
8.3 電子メールにおけるセキュリティ 145
8.4 リモート接続におけるセキュリティ 150
8.5 仮想プライベートネットワーク 152

第 9 章 情報セキュリティマネジメント 161

9.1 情報セキュリティマネジメントとは 161
9.2 情報セキュリティマネジメントの考え方 162
9.3 情報セキュリティマネジメント体制の構築 164
9.4 情報セキュリティポリシーの策定 168
9.5 技術的な情報セキュリティ対策の基本 175
9.6 情報セキュリティ対策の導入と運用 185
9.7 情報セキュリティ状況の監視と侵入検知 190
9.8 情報セキュリティ対策の評価 192

9.9 情報セキュリティ対策の見直しと改善 195

9.10 情報セキュリティマネジメントのまとめ 197

第 10 章 プライバシーの保護と情報セキュリティの確保 201

10.1 プライバシーの保護と情報セキュリティの確保とは 201

10.2 プライバシー権の起源と発達 202

10.3 プライバシーを保護するための国際的な取り組み 206

10.4 日本におけるプライバシー権の法制度上の根拠と法的救済 208

10.5 情報セキュリティの確保 210

第 11 章 日本の情報セキュリティ法 224

11.1 日本の情報セキュリティ法とは 225

11.2 電子署名及び認証業務に関する法律 228

11.3 情報セキュリティを確保する個別の法律 228

11.4 著作権法 233

11.5 個人情報の保護に関する法律 236

11.6 自主規制でセキュリティを向上させる場合の基準 242

11.7
セキュリティ侵害に対する損害賠償責任 243

11.8
展望 246

索 引 248