

## はじめに

私たちは誰でも、秘密 他人に知られたくない情報 を持っています。たとえば、銀行口座の暗証番号は他人に知られたくありません。クレジットカードの番号、ローンの額、異性関係、犯罪歴、病歴、メールのパスワード……このような情報を他人に知られて平気な人はいません。年齢、身長や体重も知られたくない人がいるでしょうし、相手によっては自分の名前すら知られたくないという場合もあるでしょう。

現代社会では、多くの情報がコンピュータ上にあります。コンピュータ上にある情報はとても便利です。コピーは一瞬でとれますし、誤りの修正も簡単です。世界中どこにいる相手にもメールで送ることができますし、Web ページとして公開すれば世界中の誰でも読むことができます。

けれど、まさにこのために、現代社会では自分が秘密にしたい情報を守ることがとても難しくなっていました。

あなたの秘密の情報を誰かがコピーしても、あなたはそれに気づかないでしょう。情報がなくなるわけではないからです。修正が簡単にできてしまうので、誰かがあなたの重要なファイルを書き換える危険性があります。誰かが、あなたの秘密をメールで第三者に送ったり、Web ページに公開したら大変です。

このような状況を改善するために、さまざまな暗号技術が開発されています。たとえば、盗聴されたメッセージを読めなくするための「暗号」、メッセージが書き換えられたことを検出するための「一方方向ハッシュ関数」、正しい相手からのメッセージであることを確かめるための「デジタル署名」などです。本書で紹介するさまざまな暗号技術は、コンピュータを使って生活やビジネスを行っている私たちの秘密を守り、情報の正しさを確かめるために存在します。

しかし、どんなに高度な暗号技術にも大きな弱点があります。それは「人間」という弱点です。ユーザが暗号技術を正しく運用しなければ、セキュリティをきちんと維持することはできません。どんなに強力な暗号でファイルが守られていても、ユーザが使っているパスワードが弱ければ、何の意味もありません。暗号技術を正しく運用するためには、個々の暗号技術についてきちんと理解しておく必要があります。「自分はいま何をしているのか」「この技術はどんな意味を持っているのか」をよく理解しなければならないのです。

本書は、暗号技術をわかりやすく紹介した入門書です。ややこしい数学の話は極力少なくした上で、個々の暗号技術の役割と意味をきちんと理解できるようにしました。

暗号は、もはや専門家だけのものではありません。暗号は、現代に生きる私たちにとって必須の技術なのです。本書を通して、暗号技術とセキュリティの基礎知識を身につけてください。

## 本書の特徴

本書には次のような特徴があります。

### ■ ■ ■ 暗号技術をわかりやすく解説

暗号技術には、非常にたくさんの種類がありますが、どれも複雑で難解です。本書では、そのなかから特に重要なものをピックアップし、たくさんの図を使ってわかりやすく解説します。

### ■ ■ ■ 暗号技術の相互関係を解説

個々の暗号技術は単独で存在するわけではありません。相互に関連し合い、補い合って大きなフレームワークを形作っています。本書では、大きなジグソーパズルを組み立てるように暗号技術の相互関係を解き明かします。

### ■ ■ ■ 「暗号の常識」を解説

一般常識と暗号における常識との間には、ずれがあります。たとえば、普通の人には「暗号アルゴリズムを秘密にすれば安全だろう」と考えてしまいがちです。しかし、暗号の世界では「秘密になっている暗号アルゴリズムは使わない」というのが常識になっています。本書では、一般常識と暗号の常識とが異なっている部分に注目して、読者が誤った判断をしないように注意をうながします。

### ■ ■ ■ 対象読者

本書は、以下の読者を主な対象としています。

- ・暗号全般に興味がある人
- ・公開鍵暗号やデジタル署名など、暗号技術の仕組みを理解したいと思っている人
- ・セキュリティに興味がある人

### ■ ■ ■ 数学が苦手な人にもわかりやすく

暗号技術は数学を基礎として成り立っているため、どうしても複雑な数式が登場します。本書では、数式の羅列はできるだけ避け、図解を多くし、数学が苦手な人でも理解できるように注意を払いました。

### ■ ■ ■ クイズで理解を確認する

本文中には、理解を確認するためのクイズがあります。本を読みながら短い時間で答えられるやさしいものがほとんどです。クイズの解答は各章の最後のページにあるので、自分の理解度を確かめつつ本書を読み進めることができます。

## 本書の構成

### ■ ■ ■ 第 部 暗号

第1章「暗号の世界ひとめぐり」では、暗号技術の全体像を解説します。

第2章「歴史上の暗号」では、歴史上重要な役割を果たした暗号について解説し、暗号解読について考えます。

第3章「対称暗号（共通鍵暗号）」では、暗号化を行う基本的な技術である対称暗号（共通鍵暗号）について解説します。長い間標準として使われてきたDESから、最新のAESまでを解説します。

第4章「ブロック暗号のモード」では、対称暗号での暗号化の手順を表す「モード」を解説します。ECB、CBC、CFB、OFB、CTRの各モード、およびブロック暗号とストリーム暗号についてお話します。

第5章「公開鍵暗号」では、現代の暗号技術において最も重要といえる公開鍵暗号について解説します。鍵配送問題について解説した後、公開鍵暗号RSAの計算を実際に行います。

第6章「ハイブリッド暗号システム」では、対称暗号と公開鍵暗号を組み合わせることで高速で安全な暗号化・復号化を行う方法についてお話します。

### ■ ■ ■ 第 部 認証

第7章「一方向ハッシュ関数」では、メッセージの指紋と呼ばれるデータを作り出す一方向ハッシュ関数について解説します。一方向ハッシュ関数を持つべき性質を解説してから、MD5、SHA-1、RIPEMDなどの具体的な一方向ハッシュ関数を紹介します。

第8章「メッセージ認証コード」では、対称暗号と一方向ハッシュ関数を組み合わせてメッセージが正しく伝達されたかどうかを確認するための技術を解説します。

第9章「デジタル署名」では、公開鍵暗号技術を使って認証を行う技術を解説します。これらの技術は「なりすまし」や「改竄<sup>かいざん</sup>」の防止に役立ちます。

第10章「証明書」では、公開鍵の正しさを示すための証明書と、証明書を発行する認証局について解説します。また公開鍵基盤(PKI)の仕組みも解説します。

### ■ ■ ■ 第 部 鍵・乱数・応用技術

第11章「鍵」では、暗号で使われている鍵の管理について解説し、私たちが日ごろ入力しているパスワードについて考えます。

第12章「乱数」では、コンピュータ上で乱数を生成する擬似乱数生成器について解説します。擬似乱数生成器は、暗号の鍵を作る際に重要な役割を果たします。暗号で使われる乱数の持つ性質についてお話してから、対称暗号や一方向ハッシュ関数を使った擬似乱数生成器についてお話します。線形合同法を暗号で使うのは危険であるという話もします。

第13章「PGP」では、広く使われている暗号ソフトウェア、Pretty Good Privacy (PGP) について解説します。PGPには対称暗号、公開鍵暗号、一方方向ハッシュ関数、デジタル署名、鍵の管理、乱数生成など、多くの重要な暗号技術が見事に集約されています。PGPの構成を学ぶことで、暗号技術を組み合わせる方法を理解することができるでしょう。

第14章「SSL/TLS」では、Secure Socket Layer (SSL) および Transport Layer Security (TLS) について解説します。SSL/TLSは、Webでのオンラインショッピングなどでセキュリティを保つために使われている技術です。

第15章「暗号技術と現実社会」では、これまでの章で解説した暗号技術を整理し、現実社会のセキュリティにおける暗号技術の役割について考えます。

正枝、松岡正恭、まつしまひでき、松戸正春、松本悠希、松森久也、丸下博宣、御簾納一、美馬孝行、三宅喜義、宮成敏裕、宮本信二、村上佳久、持尾聡史、盛尋樹、森川浩司、森田大輔、矢野正謹、倭聡、山本耕司、山本哲也

筆者の活動をいつも支援してくださるソフトバンク パブリッシング株式会社書籍局 第6編集部野沢喜美男編集長に感謝します。

最愛の妻に本書を捧げます。無数の秘密を私と共有してくれることに感謝しつつ。

2003年8月 横浜にて

結城 浩

## 謝辞

『暗号技術大全』の著者ブルース・シュナイアー、およびPGPの生みの親フィリップ・ジマーマンに感謝します。

本書執筆中に貴重な情報と励ましを送ってくださった、山形浩生さんに感謝します。

筆者の書籍・雑誌連載・メールマガジンの読者の方々に感謝します。筆者のWebページに集う友人たちや、いつも筆者のために祈ってくれているクリスチャンの友人たちに感謝します。

本書の原稿は、執筆と並行してインターネット上でレビューが行われました。レビューを行う方々は年齢・国籍・性別・住所・職業の区別なくインターネットで公募され、すべてのやりとりは電子メールとWebを使って行われました。本書のレビューに参加していただいた方々に感謝します。貴重な意見、改善案、励ましの言葉を送ってくださった、以下の各氏に感謝します(五十音順、敬称略)

青木久雄、新真千恵、天野勝、ANDO Yoko、池田大、石井勝、石川昭彦、石野幸夫、伊藤浩一、稲毛一行、井村ゆき乃、岩沢正樹、上原隆平、植松喜孝、植村光秀、江口加奈子、榎本直紀、大澤日出男、大竹宏志、大谷晋平、大谷祐史、奥田佳樹、尾関善行、織田京子、小原剛、小柳津靖志、katokt、角田直行、加藤近之、角征典、金子統浩、上山誉晃、彼谷哲志、川合元洋、川崎昌博、川島光博、川村正安、北川敦史、木村岳文、久保山哲二、久米川昌弘、小山毅、近藤晋也、後藤英雄、榊原知香子、貞池克己、佐藤正明、佐藤康二、佐藤勇紀、佐山秀晃、澤義和、重信和行、しばむらしのぶ、末石淳一郎、鈴木隆介、平良公一、高島修、高橋英一郎、高橋健、高橋立明、滝口幸子、竹内康二、武智儀明、竹中明夫、辰巳晋作、田中篤博士、津田昌樹、富長裕久、鳥海喜代江、土居俊彦、中島能和、中村圭輔、中森博久、野田知哉、野々垣一義、林孝彰、春岡徳久、比嘉一朋、比嘉陽一、檜垣健太郎、平澤俊継、廣中利光、古屋智久、細川賢太郎、細野英朋、保戸塚貴博、堀正人、volo、米田重治、前原正英、松浦

# CONTENTS

はじめに	iii
本書の特徴	iv
本書の構成	v
謝辞	vi

## 第 部 暗号

<b>第 1 章</b>	<b>暗号の世界ひとめぐり</b>	
	この章で学ぶこと	4
	暗号	4
	アリスとボブ	4
	送信者・受信者・盗聴者	4
	暗号化と復号化	6
	暗号は機密性を守る	7
	解読	7
	対称暗号と公開鍵暗号	8
	暗号アルゴリズム	8
	鍵	8
	対称暗号と公開鍵暗号	9
	ハイブリッド暗号システム	10
	そのほかの暗号技術	11
	一方向ハッシュ関数	11
	メッセージ認証コード	11
	デジタル署名	12
	擬似乱数生成器	12
	暗号学者の道具箱	13
	ステガノグラフィと電子透かし	14
	暗号とセキュリティの常識	15
	秘密の暗号アルゴリズムを使うな	15
	弱い暗号は暗号化しないよりも危険である	16
	どんな暗号もいつかは解読される	16

暗号はセキュリティのほんの一部である	17
この章のまとめ	18
クイズの解答	19

## 第2章 歴史上の暗号

### 他人が読めない文章を作る

この章で学ぶこと	22
シーザー暗号	22
シーザー暗号とは何か	22
シーザー暗号の暗号化	23
シーザー暗号の復号化	24
ブルート・フォース・アタックによる解読	25
単一換字暗号	26
単一換字暗号とは何か	26
単一換字暗号の暗号化	27
単一換字暗号の復号化	28
単一換字暗号の鍵空間	28
頻度分析による解読	29
エニグマ	34
エニグマとは何か	34
エニグマによる暗号通信	34
エニグマの構造	34
エニグマの暗号化	36
「日替わり鍵」と「通信鍵」	38
通信エラーの回避	39
エニグマの復号化	39
エニグマの弱点	40
エニグマの解読	41
考えてみよう	42
なぜ暗号アルゴリズムと鍵とを分けるのか	42
この章のまとめ	44
クイズの解答	45

## 第3章 対称暗号（共通鍵暗号）

### 1つの鍵で暗号化し、同じ鍵で復号化する

スクランブルエッグと対称暗号	48
----------------	----

この章で学ぶこと	48
文字の暗号からビット列の暗号へ	49
符号化	49
XOR	50
使い捨てパッド 絶対に解読できない暗号	52
使い捨てパッドとは	52
使い捨てパッドの暗号化	53
使い捨てパッドの復号化	53
使い捨てパッドは解読できない	54
使い捨てパッドはなぜ使われないのか	54
DES	56
DESとは何か	56
暗号化・復号化	57
DESの構造（フィステルネットワーク）	58
トリプルDES	64
トリプルDESとは何か	64
トリプルDESの暗号化	64
トリプルDESの復号化	67
トリプルDESの現状	67
AESの選定プロセス	68
AESとは何か	68
AESの選定プロセス	68
AES最終候補の絞り込みとAESの決定	69
Rijndael	70
Rijndaelとは何か	70
Rijndaelの暗号化と復号化	70
Rijndaelの解読	71
どの対称暗号を使えばよいのか	72
この章のまとめ	74
クイズの解答	75

## 第4章 ブロック暗号のモード

### ブロック暗号をどのように繰り返すか

この章で学ぶこと	78
ブロック暗号のモード	79
ブロック暗号とストリーム暗号	79
モードとは何か	79

平文ブロックと暗号文ブロック	80
能動的な攻撃者マロリー	81
ECBモード	81
ECBモードとは何か	81
ECBモードの特徴	81
ECBモードへの攻撃	83
CBCモード	85
CBCモードとは何か	85
初期化ベクトル	85
CBCモードの特徴	87
CBCモードへの攻撃	88
CBCモードの利用例	90
CFBモード	91
CFBモードとは何か	91
初期化ベクトル	92
CFBモードとストリーム暗号	93
CFBモードの復号化	93
CFBモードへの攻撃	93
OFBモード	95
OFBモードとは何か	95
初期化ベクトル	95
CFBモードとOFBモードの比較	95
CTRモード	97
カウンタの作り方	97
OFBモードとCTRモードの比較	99
CTRモードの特徴	99
エラーと機密性	100
どのモードを使うべきか	100
この章のまとめ	102
クイズの解答	103

## 第5章

### 公開鍵暗号

公開鍵で暗号化し、プライベート鍵で復号化する	
コインロッカーの使い方	106
この章で学ぶこと	106
鍵配送問題	106
鍵配送問題とは	106

鍵の事前共有による鍵配送問題の解決	107
鍵配布センターによる鍵配送問題の解決	109
Diffie-Hellman 鍵交換による鍵配送問題の解決	110
公開鍵暗号による鍵配送問題の解決	111
公開鍵暗号	111
公開鍵暗号とは	111
公開鍵暗号の歴史	112
公開鍵を使った通信の流れ	113
さまざまな用語	114
公開鍵暗号でも解決できない問題	114
時計演算	116
加算	116
減算	118
乗算	119
除算	120
累乗	123
対数	124
時計の針からRSAへ	125
RSA	125
RSAとは何か	125
RSAによる暗号化	126
RSAによる復号化	126
鍵ペアを作る	127
具体的にやってみよう	131
RSAへの攻撃	134
暗号文から平文を求める	134
ブルート・フォース・アタックでDを見つける	135
EとNからDを求める	135
man-in-the-middle 攻撃	136
他の公開鍵暗号	139
ElGamal方式	139
Rabin方式	139
楕円曲線暗号	139
公開鍵暗号に関するQ&A	140
公開鍵暗号の機密性	140
公開鍵暗号と対称暗号の鍵長	140
対称暗号の未来	141
RSAと素数	141

RSA と素因数分解	142
RSA のビット長	142
この章のまとめ	143
クイズの解答	144

## 第 6 章 ハイブリッド暗号システム

対称暗号でスピードアップし、公開鍵暗号でセッション鍵を守る	
ハイブリッド車	148
この章で学ぶこと	148
ハイブリッド暗号システム	148
対称暗号と公開鍵暗号	148
ハイブリッド暗号システム	149
暗号化	150
復号化	152
ハイブリッド暗号システムの具体例	154
強いハイブリッド暗号システムとは	154
擬似乱数生成器	154
対称暗号	154
公開鍵暗号	155
鍵長のバランス	155
暗号技術の組み合わせ	155
この章のまとめ	156
クイズの解答	157

# 第 部 認証

## 第 7 章 一方向ハッシュ関数

メッセージの「指紋」をとる	
この章で学ぶこと	162
一方向ハッシュ関数とは何か	162
このファイルは本物かしら	162
一方向ハッシュ関数とは	166
一方向ハッシュ関数の性質	168
用語について	172

一方向ハッシュ関数の応用例	172
ソフトウェアの改竄検出	172
パスワードを元にした暗号化	174
メッセージ認証コード	174
デジタル署名	174
擬似乱数生成器	175
ワンタイムパスワード	175
一方向ハッシュ関数の具体例	175
MD4, MD5	175
SHA-1, SHA-256, SHA-384, SHA-512	175
RIPEMD-160	176
一方向ハッシュ関数SHA-1	176
全体の流れ	176
(1) SHA-1 : パディング	177
(2) SHA-1 : $W_0 \sim W_{79}$ の計算	179
(3) SHA-1 : ブロックの処理	180
(4) SHA-1 : 1ステップの処理	183
一方向ハッシュ関数への攻撃	184
ブルート・フォース・アタック (攻撃のストーリー1)	184
誕生日攻撃 (攻撃のストーリー2)	186
一方向ハッシュ関数で解決できない問題	189
この章のまとめ	189
クイズの解答	190

## 第 8 章 メッセージ認証コード

メッセージは正しく送られてきたか	
この章で学ぶこと	194
メッセージ認証コード	194
これは正しい送金依頼か	194
メッセージ認証コードとは何か	195
メッセージ認証コードの利用手順	195
メッセージ認証コードの鍵配送問題	197
メッセージ認証コードの利用例	198
SWIFT	198
IPsec	198
SSL/TLS	198
メッセージ認証コードの実現方法	198

一方向ハッシュ関数を使って実現	198
ブロック暗号を使って実現	199
その他の方法で実現	199
HMAC の詳細	199
HMAC とは何か	199
HMAC の手順	199
メッセージ認証コードに対する攻撃	202
再生攻撃	202
鍵の推測による攻撃	204
メッセージ認証コードで解決できない問題	204
第三者に対する証明	205
否認防止	205
この章のまとめ	206
クイズの解答	207

## 第 9 章

### デジタル署名

#### このメッセージを書いたのは誰か

おかあさんヤギの認証	210
この章で学ぶこと	210
デジタル署名	210
アリスの借用書	210
メッセージ認証コードからデジタル署名へ	211
署名の作成と署名の検証	212
公開鍵暗号とデジタル署名	213
デジタル署名の方法	216
メッセージに直接署名する方法	216
メッセージのハッシュ値に署名する方法	218
デジタル署名に対する疑問	221
暗号文がなぜ署名として使えるのか	221
機密性が保てないのではないか	221
コピーが作れるのではないか	222
書き換えができるのではないか	222
署名だけ再利用できてしまうのではないか	223
署名を削除しても「契約破棄」できないのではないか	224
どうして否認防止になるのか	224
デジタル署名は本当に署名の代わりになるのか	225
デジタル署名の利用例	226

セキュリティ情報のアナウンス	226
ソフトウェアのダウンロード	227
公開鍵の証明書	227
SSL/TLS	227
RSA によるデジタル署名	228
RSA による署名の作成	228
RSA による署名の検証	228
具体的にやってみよう	229
他のデジタル署名	230
ElGamal 方式	230
DSA	230
Rabin 方式	230
デジタル署名に対する攻撃	231
man-in-the-middle 攻撃	231
一方向ハッシュ関数に対する攻撃	232
デジタル署名を使って公開鍵暗号を攻撃	232
その他の攻撃	233
比較してみよう	234
メッセージ認証コードとデジタル署名	234
ハイブリッド暗号システムとハッシュ値へのデジタル署名	234
デジタル署名で解決できない問題	235
この章のまとめ	236
クイズの解答	236

## 第 10 章

### 証明書

#### 公開鍵へのデジタル署名

この章で学ぶこと	238
証明書	238
証明書とは何か	238
証明書を扱うシナリオ	238
証明書を作ってみよう	241
ペリサインの無料お試しサービス	241
証明書の作成	241
証明書を Web ブラウザからエクスポートする	244
証明書の内容	244
証明書の標準規格 X.509	244
公開鍵基盤 (PKI)	247



公開鍵基盤 (PKI) とは何か	248
PKI の構成要素	248
認証局の仕事	250
階層になった証明書	251
さまざまなPKI	253
証明書に対する攻撃	255
公開鍵の登録前を攻撃	255
似た人間を登録する攻撃	255
認証局のプライベート鍵を盗み出す攻撃	256
攻撃者自身が認証局になる攻撃	256
CRL の隙を突く攻撃 (1)	257
CRL の隙を突く攻撃 (2)	258
証明書に対するQ&A	259
証明書がなぜ必要なのか	259
独自の認証方法を使ったほうが安全ではないか	260
認証局はどうやって信頼するか	261
この章のまとめ	263
クイズの解答	264

## 第 部 鍵・乱数・応用技術

### 第11章 鍵

秘密のエッセンス	
この章で学ぶこと	268
鍵とは何か	268
鍵はとても大きな数	268
鍵は平文と同じ価値を持つ	270
暗号アルゴリズムと鍵	270
さまざまな鍵	270
対称暗号の鍵と公開鍵暗号の鍵	270
メッセージ認証コードの鍵とデジタル署名の鍵	272
機密性のための鍵と認証のための鍵	272
セッション鍵とマスター鍵	273
コンテンツを暗号化する鍵と、鍵を暗号化する鍵	274
鍵を管理する	275

鍵を作る	275
鍵を配送する	276
鍵を更新する	276
鍵を保存する	276
鍵を捨てる	279
Diffie-Hellman 鍵交換	280
Diffie-Hellman 鍵交換とは何か	280
Diffie-Hellman 鍵交換の手順	280
イブは鍵を計算できないのか	282
生成元の意味	282
具体的にやってみよう	284
パスワードを元にした暗号 (PBE)	285
パスワードを元にした暗号とは何か	285
PBE の暗号化	286
PBE の復号化	288
ソルトの役割	290
パスワードの役割	290
PBE の改良	292
安全なパスワードを作るには	292
自分だけが知り得る情報を使うこと	293
複数のパスワードを使い分けること	293
メモを有効に使うこと	294
パスワードの限界を知ること	294
この章のまとめ	295
クイズの解答	296

### 第12章 乱数

予測不可能性の源	
ロバの錠前屋	298
この章で学ぶこと	298
乱数が使われる暗号技術	298
乱数は何に使われるか	298
乱数の性質	299
乱数の性質を分類する	299
無作為性	300
予測不可能性	301
再現不可能性	301

擬似乱数生成器	302
擬似乱数生成器の構造	302
具体的な擬似乱数生成器	303
でたらめな方法	304
線形合同法	305
一方向ハッシュ関数を使う方法	308
暗号を使う方法	310
ANSI X9.17	311
擬似乱数生成器に対する攻撃	314
種に対する攻撃	314
ランダムプールに対する攻撃	314
この章のまとめ	315
クイズの解答	316

## 第13章 PGP

暗号技術を組み合わせる職人芸	
この章で学ぶこと	318
PGPの概要	318
PGPとは何か	318
PGPの機能	319
鍵ペアの作成	321
暗号化と復号化	321
暗号化	321
復号化	325
デジタル署名の作成と検証	328
デジタル署名の作成	328
デジタル署名の検証	330
「デジタル署名の作成と暗号化」および「復号化とデジタル署名の検証」	333
デジタル署名の作成と暗号化	333
復号化とデジタル署名の検証	333
信頼の網	337
公開鍵の正当性	337
ケース1：自分自身のデジタル署名によって確認する	337
ケース2：自分が常に信頼している人のデジタル署名によって確認する	339
ケース3：自分が部分的に信頼している人たちのデジタル署名によって確認する	339
公開鍵の正当性と所有者信頼は別	340
所有者信頼の値は個人的なもの	340

この章のまとめ	343
クイズの解答	343

## 第14章 SSL/TLS

### セキュアな通信のために

この章で学ぶこと	346
SSL/TLSとは何か	346
アリスがボブ書店で本を買う	346
クライアントとサーバ	347
HTTPをSSL/TLSの上に乗せる	348
SSL/TLSの仕事	349
SSL/TLSは他のプロトコルも守ることができる	350
暗号スイート	350
SSLとTLSの違い	351
SSL/TLSを使った通信	351
階層化されたプロトコル	351
1 TLSレコードプロトコル	354
2-1 ハンドシェイクプロトコル	354
2-2 暗号仕様変更プロトコル	361
2-3 警告プロトコル	362
2-4 アプリケーションデータプロトコル	362
マスターシークレット	362
TLSで使われている暗号技術のまとめ	364
SSL/TLSへの攻撃	364
個々の暗号技術への攻撃	364
擬似乱数生成器に対する攻撃	365
証明書の隙を突く攻撃	365
SSL/TLSのユーザへの注意	365
証明書の意味を勘違いしないように	365
暗号通信前のデータは守られていない	366
暗号通信後のデータは守られていない	366
この章のまとめ	367
クイズの解答	368

<b>第15章</b>	<b>暗号技術と現実社会</b>	
	不完全なセキュリティの中で生きる私たち	
	この章で学ぶこと	370
	暗号技術のまとめ	370
	暗号学者の道具箱	370
	暗号と認証	371
	暗号技術のフレームワーク化	371
	暗号技術は圧縮技術	373
	完全な暗号技術を夢見て	375
	量子暗号	375
	量子コンピュータ	376
	どちらが先に誕生するか	376
	暗号技術が完全になっても、人間は不完全	377
	理論が完全でも、現実是不完全	377
	防御は完全でなければならないが、攻撃は一点を破ればよい	378
	攻撃例1：PGPで暗号化されたメールに対して	378
	攻撃例2：SSL/TLSで暗号化されたクレジットカード番号に対して	380
	この章のまとめ	381
	参考文献	382
	索引	385

