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しまいました。

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うな」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ので、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Ⅰ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て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Ⅱ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が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（かいざん）」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Ⅲ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。

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くださっ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編集部の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（シェア）してくれることに感謝しつつ。

2003年8月　横浜にて

結城　浩

CONTENTS

第III部　鍵・乱数・応用技術