

本文章は筆者が執筆しコンピュータサイエンス誌Bit. 1996年3月号に掲載した「BOOKガイド 暗号セキュリティ編」を原稿をベースに作成したものです。

本の紹介

1997年10月バージョン

すずきひろのぶ

hironobu@h2np.suginami.tokyo.jp

書名 **情報セキュリティの科学～マジック・プロトコルへの招待**

ブルーボックス

著者 **太田和夫 黒澤馨 渡辺治**

出版社 **講談社**

発行年 **1995年**

ISBN-4-06-257055-6 全232ページ 760円

暗号というのはネットワーク社会を支える安全な情報伝達技術であるという今日的ポジションから暗号を紹介している入門書です。この本の著者は、暗号に対しマジック・プロトコルという名前を与えています。このマジック・プロトコルというのは、この本の著者が作った新たな造語なのですが、すばらしい命名だと私は思います。この本の中で述べられているように、「電話で公平なジャンケンをする」とか「自分の秘密を明かさずに、相手に自分が秘密を知っていることを判らせる」ということができる暗号という技は、まさにマジックです。そしてプロトコルという言葉は、相手とコミュニケーションをするため道具であるということを強く表現しています。「こうした不思議なプロトコルがマジック・プロトコルである。．．．マジック・プロトコルには『良質のパズル』のようなおもしろさがある」と書いている部分こそがこの本の本質だと思います。

一方向性ハッシュ関数、公開鍵暗号方式、デジタル署名、ゼロ知識証明といった内容を最新の情報を使って解説しており、しかも、まったくの初心者であるような読者でも、やさしく解かりやすい解説になっています。初心者にとって次のステップに進むための大切な役割を果たす参考文献紹介も、最新で、定評があり、手に入りやすい書籍がリストアップされている点も見逃せません。

書名 暗号のおはなし～情報セキュリティの新しい鍵

著者 今井秀樹

出版社 日本規格協会

発行年 1992年

ISBN4-542-90159-9 全209ページ 1400円

現代暗号に関する基本的知識として身に付けようとする人にとって格好の入門書です。内容は体系だっており、教養として暗号を学ぼうとする人が教科書として利用するには格好の本だと思います。技術に関してと、その技術に関連する議論、暗号やその安全性に関する考え方といった、著者のエッセンスがピシッと詰まっています。200ページ程度の本にも関わらず、教養レベルとして、今日の暗号に関する知識に関する必要不可欠な部分はすべて得られることができると言っても過言ではありません。

私が、この本を読んでいて、特に印象の強い部分が2つあります。それは、NTTの開発したFEALに対する批判の部分と、著者がヒューマンクリプトと呼ぶ、人間と暗号技術との共存関係に関する部分です。

前者に対する批判は、かなり厳しいものがあります。その上で、暗号の作る側、使う側の安全性に関するスタンスをこう述べています。「．．．．頻繁に鍵を取り替えるなら、目標の安全性を達成できるかもしれません。しかし、その場合には、ユーザにその暗号の安全性の程度を十分に認識してもらう必要があります。そうでなければ、誤った使い方をするかもしれないからです。」

後者のヒューマンクリプトに関して著者は、暗号技術の認証は、管理センターなどによって認証されたことを根拠とするが、人は人を認証する場合、形式的ではなく、もっと人間的な要素が入ると指摘しています。

書名 **公開鍵暗号系**
著者 **アルト・サロマー（著） 足立暁生（訳）**
出版社 **東京電気大学出版局**
発行年 **1992年**
ISBN4-501-51840-5 全344ページ 4500円

公開鍵暗号に関して、基礎から応用まで、懇切丁寧に解説してくれる本です。基本的な概念部分から丁寧に説明しているので独学で学ぼうとする人には心強い味方になってくれる本です。公開鍵暗号に関する予備知識がない人でも、この本で公開鍵暗号を学ぶことができるでしょう。ただし、入門ではなく、教科書の部類に入る作りなので、ざっと目を通すというための本ではありません。体系的で、かつ、考えを導いてくれるような書き方がされているため非常に読みやすく感じます。本書のはしがきによると、著者が1983年以来、複数の大学で行っていた暗号学の講義では本書の原稿を使ってきたということが書いてあります。残念なことに楢円暗号は、残念ながら解説されていません。

書名 暗号・ゼロ知識証明・数論

著者 岡本龍明 太田和夫(編)

出版社 共立出版

発行年 1995年

ISBN4-320-02740-X 全248ページ 4429円

ゼロ知識証明に関して、現代暗号の理論を理解する上で必要な数論に関してカバーしている教科書的な本です。通信セキュリティとして必要な暗号についてのトピックスは、最新の研究成果を網羅し、体系的にまとめられています。ただし内容的には、大量の新しい内容をサラッと書いていたりしますので、詳しく内容を追っかけようとする、参照されている大量の文献に当たる必要があります。

この本の特徴は、本の半分を数論アルゴリズムのパートに割り当てていることです。今までで、暗号に使われている数論をここまで体系的にまとめたものはあまり見かけないので、その点で重要な本と言えます。暗号研究、理論の方は、この本は必読でしょう。ただし、実際計算機の上に載せた時の話題があまり出てこない、システムやプログラミングに興味のある人は、少々物足りない感じるでしょう。

書名 APPLIED CRYPTOGRAPHY (2ndED)

著者 BROUCE SCHNEIER

出版社 JohnWiley & Sons, Inc.

発行年 1996年

ISBN 0-471-11709-9 全758ページ \$49.95

たぶん、現在もっとも有名な暗号の解説書といえば、この本でしょう。この本は、現代暗号のほぼすべて網羅している、といっても過言ではない内容とボリュームを持った本です。

ソースコードが書かれた章を差し引いても621ページにわたって、びっしりと暗号の解説が書かれています。内容は、本当に初心者から、エキスパートまで利用できる、本当にすごい本になっています。

初心者にとっての謎、誰もが知っていて、誰も教えてくれないような事まで丁寧に教えてくれています。一方、エキスパートですら中々手に入らない情報も満載しています。たぶん、RC5 (RSA社が出している最新のBlock Cipher) やGOST(旧ソ連が開発したBlock Cipherで旧ソ連政府が使っていた。西側に内容が公開されたのは、ほんの最近のこと)まで解説を収めている本は、現在この本だけでしょう。しかも、RC5もGOSTのソースコード・リストは本に収められています。

本書の位置づけを考えた場合、教科書というよりも辞書に近い位置づけになるでしょう。ある程度、暗号が解ってきてからでないと、本書を読んでも、その知識を有効に活かすことはできないのではないかと思います。暗号の本で一冊だけ選べと言われたら、迷わずこの本の名前を上げます。

書名 PGP 暗号メールと電子書名
著者 Simon Grfinkel (著) 山本和彦 (監訳)
出版社 オーム社 (国内) O'Reilly ' Associates, Inc (原書)
発行年 1995年 (原書)
ISBN 1-56592-098-8 全393ページ \$24.95 (原書)

書名 The official PGP user's guide
著者 Philip Zimmermann
出版局 MIT Press
発行年 1995年
ISBN0-262-74017-6 全127ページ \$14.95

前者は、PGPに関する本です。PGPの技術や使い方だけではなく、PGPを取り巻く問題や状況(当時)を詳しく説明しています。PGPに関しては、筆者も雑誌記事(Software Design, 1995年4月号及び5月号, 技術評論社)を書いていますので、そちらも参考になるでしょう。

後者は、PGPの著者であるPhilip Zimmermannの著書であるThe Official User's Guideは著者直伝の使い方と、PGPユーザへのメッセージです。

書名 **暗号とデータセキュリティ**

著者 D.E.R **デニング** (著) **上園忠弘 小嶋格 奥島晶子** (訳)

出版社 培風館

発行年 1988

ISBN4-563-00792-7 全408ページ 5800円

この本の特徴は半分が暗号に関して、あと半分はデータ・セキュリティに関しての教科書だという点です。ここでのデータ・セキュリティとしてのというのは、コンピュータ・サイエンスとしてのデータ・セキュリティです。アクセス制御、情報フロー制御に関しての章では、データ・セキュリティとは本質的にオペレーティング・システムのデータ管理に必要な制御と同等だということを教えてくれます。この本を読めば、次から次へと現れるパソコン・ウイルスの問題の本質は、オペレーティング・システムの致命的な欠陥にあると気づくはずです。

書名 **暗号理論入門**

著者 **岡本栄司**

出版社 **共立出版**

発行年 1993年

ISBN4-320-02633-0 全190ページ 2390円

入門という名前がついていますが、初心者向きではなく、授業用の教科書といった内容です。一通り通して読めば、きちんと必要な部分は押さえて学べるので、入門書では少々足りない、でも、まだ専門書は重すぎるといった人にとって役に立つ本でしょう。

書名 HANDBOOK OF APPLIED CRYPTOGRAPHY
著者 Alfred J Menezes, Paul C. van Oorschot, Scott A.
Vanstore
出版社 CRC Press, Inc.
発行年 1996年
ISBN 0-8493-8523-7 全780ページ \$79.95

今日の暗号技術のすべてを解説している暗号専門家のための暗号技術百科事典です。
かなりの数に登る協力者の一覧を見ると、今日の世界の最前線で研究している世界中の
一流暗号学者が作成に協力しているのがわかります。

書名 **現代暗号**

著者 **岡本龍明、山本博資**

出版社 **産業図書**

発行年 1997年

ISBN 4-7828-5353 全350ページ 3800円

基礎から応用まで今日的視点から暗号を解説した本です。1997年時点における最新の成果と動向を踏まえて書かれている本です。専門課程に進んだ学部生、あるいは大学院生にとって良い本であると同時に、技術者や研究者が最新の暗号に関する知識を得るにはもってこいの本です。暗号の基本的知識は必ずしも必要ありませんが、計算機科学の基礎知識と数学の基礎知識は必要です。