コンピュータセキュリティ 10−17
(2000. 7. 25)

「ブロック暗号ガイドブック」について

清水 秀夫† 関 春樹† 金子 泰祥† 宮野 浩‡ 金子 敏信*

†通信・放送機構 横浜リサーチセンター
〒221-0031 横浜市 神奈川区 新浦島町 1-1-32 ニューステージ横浜 1F
電話番号: 045-450-1245 E-mail: {shimizu hseki kaneko}@yokohama.tao.go.jp
‡NEC ソリューションズ インターネットソフトウエア開発本部
〒108-8557 東京都港区芝浦 2-11-5
電話番号: 03-5476-1284 E-mail: miyano@ab.jp.nec.com
* 東京理科大学 理工学部 電気工学科
〒278-8510 千葉県 野田市 山崎 2641
電話番号: 0471-24-1501 (内 3709) E-mail: kaneko@ee.noda.sut.ac.jp

あらまし 通信・放送機構 (TAO) の情報セキュリティ技術に関する研究開発プロジェクトが成果の一つとしてまとめた「共通鍵ブロック暗号の選択／設計／評価に関するドキュメント」(ブロック暗号ガイドブック) を紹介する。
キーワード 共通鍵ブロック暗号, ガイドブック, 通信・放送機構

On the Block Cipher Guidebook

Hideo Shimizu† Haruki Seki† Yoshiyasu Kaneko† Hiroshi Miyano‡
Toshinobu Kaneko*

†Yokohama Research Center, Telecommunications Advancement Organization of Japan
New Stage Yokohama, 1-1-32 Shin-urashima-cho, Kanagawa-ku, Yokohama, 221-0031 JAPAN
TEL: +81-45-450-1245 E-mail: {shimizu hseki kaneko}@yokohama.tao.go.jp
‡ NEC Corporation
2-11-5, Shibaura, Minato-ku, Tokyo 108-8557, JAPAN
TEL: +81-5476-1084 E-mail: miyano@ab.jp.nec.com
*Department of Electrical Engineering, Science University of Tokyo
2641 Yamazaki Noda, Chiba, Japan 278-8510
TEL: +81-471-24-1501(ex.3709) E-mail: kaneko@ee.noda.sut.ac.jp

Abstract We summarize the document "Technical Report on Design, Analysis and Use of Block Ciphers", which is a part of a result of Information Security Project of Telecommunications Advancement Organization of Japan.
Key Words Symmetric Block Encryption Algorithm, Guidebook, Telecommunications Advancement Organization of Japan

1 はじめに

通信・放送機構[1]が1995年10月に開始した直轄プロジェクトである「情報セキュリティ技術に関する研究開発プロジェクト」[2]は、2000年9月末日に5年間のプロジェクト期間を終える。本稿では、プロジェクトの成果の一環として作成した「共通鍵ブロック暗号の選択／設計／評価に関するドキュメント」の概要を紹介する。以下、ガイドブックと呼称することにする。

2 ガイドブックの概要

ガイドブックはタイトルの通り、共通鍵ブロック暗号に焦点を当てている。例えば公開鍵暗号と共通鍵暗号の違いといったような一般の教科書に書いてあるようなことは一切書かれておらず、まさに共通鍵ブロック暗号のことだけを掘り下げている。

研究員が第1稿を執筆し、サブリーダの先生方を交えた16回のレビューにより推敲を重ね、作成作業は約1年間に渡っている。

目的 ガイドブック作成の目的として以下を考えた。

- 蓄えられた知見や技術を集約して、より広く利用可能にする。
- 「研究者の皮膚感覚」を明文化する。

共通鍵ブロック暗号に関して深く掘り下げた教科書が日本語では見当たらないので、前者は意義があると考える。また後者は通常は論文等には記載されないような事由まで集積するということである。

編集方針 以上の目的を実現するために以下のような方針で編集を行った。

- 「利用者編」「設計者編」に分け、読者層を想定することで記事の視点に一貫性を持たせるようにした。
- 各記事について、その項目だけを読めば最低限の知識は得られるような構成になるべくするために、記事間の記述の重複は恐れないこととした。
- 各項目の記述をなるべく簡潔にするために、より深い知識を必要とする読者には、各自参考文献を読んでいただくことを前提とした構成になっている。そのために、参考文献は、各記事毎に記されている。

3 ガイドブックの構成

タイトルにある選択／設計／評価という3本の柱を軸に7つの章で構成した。この7つの章を対象となる読者を元に2つのパートに大別した。

Part I 共通鍵暗号の導入・選択 (利用者編) 対象となる読者は、共通鍵ブロック暗号をシステムに組み込もうとする技術者であり、組み込もうとする暗号アルゴリズムを選択する際に知っておくべきことを中心に記述している。即ち、3つの柱のうちの「選択」である。

Part Iは以下の3つの章で構成されている。

[1] http://www.shiba.tao.go.jp
[2] http://www.yokohama.tao.go.jp

第 1 章 導入・選択時の判断要素とその概要
共通鍵ブロック暗号をシステムに導入する際に、どのような判断要素があり、どのように考慮しなければならないかを取り上げた。

第 2 章 暗号解析学的な安全性と実用上の安全性との関連
まず安全性 (攻撃) について最低限知っていた方がよいと思われる事柄を述べた後、実際にシステムに対する脅威を判定するための方法について述べている。

第 3 章 標準化について
共通鍵ブロック暗号アルゴリズムの標準化動向、および様々な暗号利用技術の国際標準を取り上げた。

Part II 共通鍵暗号の設計・評価 (設計者編) 対象となる読者は、これから暗号アルゴリズムの設計を行おうとしている技術者、もしくは暗号研究を行おうとしている初学者である。様々な知見や情報を集約することで導入を容易にすることを目的としている。

Part II の前半の 4,5 章は「設計」に当てられ、後半の 6,7 章は「評価」に当てられている。

第 4 章 共通鍵ブロック概論
背景となる知識として、研究の流れを中心とした共通鍵ブロック暗号の歴史と、1 章で取り上げた判断要素と対をなす設計思想を取り上げた。

第 5 章 共通鍵ブロック暗号の設計
共通鍵ブロック暗号アルゴリズムを解剖し、各パーツについて解説した。

第 6 章 代表的な攻撃アルゴリズム
現在、代表的と考えられる差分攻撃や線形攻撃のような攻撃アルゴリズムを取り上げ、各々について解説した。設計者はあらゆる攻撃を熟知していなければならない。

第 7 章 設計事例の分析
既存の暗号アルゴリズムの様々な設計から欠点を抽出し分析することで、今後の設計への教訓 (反面教師) とすることを意図している。

4 まとめ

どのような目的、方針でガイドブックを作成したか、またガイドブックがどのような構成になっているのかについて述べた。

本稿で述べたガイドブックは共通鍵ブロック暗号だけを取り上げているということで言えば非常にユニークで他に類をみないドキュメントである。IT 文明の拡大に伴うセキュリティ技術の重要性が増している今日、本稿で取り上げたガイドブックが、特に急峻な進歩を遂げている共通鍵ブロック暗号技術を敷衍するための一助となることを期待したい。

正誤表

p.ii (誤) 日立制作所 → (正) 日立製作所

p.ii (誤) 大熊 健司 → (正) 大熊 建司

目 次