まえがき

乱数については統計学の分野において，古くからよく論じられてきており，大学での統計学に関連した講義の中でも取り上げられてきている（例えば教科書としては [7]，[5]，[22] 等）．本書ではこの乱数についての一般論を論じようとするものではない．本書で取り上げようとしているのは，統計学の世界において今まであまり馴染みの深くない一つの分野での乱数の使用とそれから発生する統計学上の問題の紹介である．

本書で議論の対象となる応用の分野は「暗号」の世界である．近年通信システムにおいてセキュリティの問題は注目を集めている（[21]，[15] 等）．ある秘匿の必要があるメッセージ等を送信しようとするとき，第三者がそれを手に入れて判読しようとしても不可能なようにし，送信の相手がそれを受け取ったとき，もとの文章が得られるようにするために，種々の方策が考案されている．この方策には数学的な表現を用いれば大まかにいって代数的な方策と乱数を用いる方策がよく議論されているようである．本書ではこのうち乱数を用いる方策を取り上げ，ここで用いる乱数に関する統計学上の問題を議論する．我が国においても情報セキュリティの研究や業務等に携わっておられる方々は多くおられ，その方々の間ではこの方面の問題についても熱い議論が交わされている（[23]，[6] 等）．本書では，用いる乱数に関する統計学上の問題についてそれを統計学の観点から紹介を行い，その一部について筆者らが行ってきている解決法を述べることにする．

本文中，「**統計理論 Note**」と記して，本書を読み進んでいただく上で必要となる統計学の概念や用語を説明した部分がある．統計学における概念や用語の一般的な説明ではなく，本書の内容に即した形で説明したつもりである．統計学にあまり馴染みのない方にそのあとに続く内容をよりよくご理解いただきたいと願ってつけたものである．したがって統計学の知

統計学One Point【7】巻　暗号と乱数―乱数の統計的検定―
藤井 光昭著
http://www.kyoritsu-pub.co.jp/bookdetail/9784320112582

識をお持ちの方は，その部分を読み飛ばしていただきたい．なお統計学における概念や用語について，本文において最初に出てきた箇所に統計理論 Note をつけることはしないで，関連する概念や用語をまとめて後ほどつけたところがある．もし必要になった場合には索引を利用していただくなどしてご利用いただきたいと願っている．さらに詳しい知識等が必要の場合においては [20] 等を参考にしていただきたい．

本書の内容は 2002 年度から 2006 年度において中央大学が研究拠点となって行われた文部科学省 21 世紀 COE プログラム「電子社会の信頼性向上と情報セキュリティ」（拠点リーダー 辻井重男教授）において推進された研究が基となっている．中央大学において統計学の研究に携わっている教授（当時）もこのプログラムの事業推進担当者として加わった．この推進担当者を中心に統計グループとして活動を行った．このグループには杉山高一，鎌倉稔成，渡辺則生の各教授（当時）と筆者および竹田裕一 21 世紀 COE プログラム研究員（当時）や若い研究者・大学院学生が加わり，定期的に研究会を開催した．そしてこの 21 世紀 COE プログラム終了後も研究を進めてきた．統計グループの皆様といろいろご指導いただいた拠点リーダーの辻井重男教授には心から感謝申し上げたい．

アメリカ国立標準技術研究所 (National Institute of Standards and Technology(NIST)) の統計工学部門 (Statistical Engineering Department) の Andrew Leo Rukhin 博士（メリーランド大学名誉教授）は上記 COE プログラムでお招きし講演していただいたが，それ以来，筆者は同博士と種々の研究交流を続けてきている．今回本書の原稿作成にあたって主として 3.2 節「NIST による一組みの乱数性の統計的検定方法」を執筆の際に，筆者の疑問点に親切にご回答いただいたり種々の面でご支援をいただいた．厚く感謝申し上げたい．

グループとして研究活動を進めてきているが，皆様のご了解を得て，主として関連したテーマの研究を進めてきた一人の藤井光昭が本書の執筆を担当することになった．しかし，本書の内容等は統計グループの皆様の多大なご協力なしにはでき得なかったものである．特に竹田裕一氏（神奈川工科大学准教授）とはこの 21 世紀 COE プログラムの当初から共同で研

統計学One Point【7】巻 暗号と乱数―乱数の統計的検定―
藤井 光昭著
http://www.kyoritsu-pub.co.jp/bookdetail/9784320112582

究を進めてきている．本書で学会誌より引用するシミュレーションとその結果は竹田裕一准教授によるものである．竹田裕一准教授と統計グループの皆様に深い感謝の意を表したい．

原稿の段階で本書をお読みくださり，辻井重男教授（中央大学 研究開発機構．東京工業大学名誉教授．元 情報セキュリティ大学院大学学長）とその研究グループのお一人である五太子政史氏（中央大学 研究開発機構 客員研究員）からは大変貴重なご意見をいただき，原稿の改善に大いに役立てさせていただき，誠にありがたかった．辻井重男教授はわざわざ私のために研究会を開催してくださり，ご出席の皆様からは私にいろいろご質問等をいただいた．これらのご質問等は執筆の上で大変参考になった．皆様に心より御礼申し上げたい．

本書の刊行にあたり，このシリーズの編集委員長の中央大学の鎌倉稔成教授と共立出版編集部にはいろいろの面で大変お世話になった．厚く御礼申し上げたい．

2018 年 2 月

藤井光昭