MATHEMATICAL
SCIENCES
September 2006 Number 519

特集／ランダムネス

ランダムネスのおもしろさ

渡辺 治

1. はじめに

「ランダム」は，数理科学の用語の中では，一般にも馴染みのある言葉である．普通の大人であれば，たぶん，ランダムという言葉を，誰もが一度や二度は使った経験があるのではないだろうか？

ただ，それだけにランダムについては，いろいろな解釈や先入観があるように思う．ランダムというのは，「でたらめ」とか「乱雑」というイメージもあるし，「偏りがなく公平」と思う人もいれば，「予測不可能」で扱いにくい，と思っている方もいるだろう．

それらはすべて，ランダムネス*1)の各側面を表している．けれども，少々誤解されている面もある．ここでは，皆さんに，ランダムネスを少し見直して頂くために，ランダムネスのあまり知られていない側面を 3 つほど紹介する．

本特集では，ランダムネスの不思議さ，おもしろさを，各分野の第一線の研究者に紹介して頂いているが，それらの前座として，各紹介記事の導入になれば幸いである．

*1) 本特集を通して，ランダムネスは，「ランダムであること」，あるいは「ランダム性」という意味で用いる．

2. ランダムが役に立つ!?

ランダムには「予測できない」という側面がある．一般には予期できないことには，不測の事態，とか，不慮の出来事，などのように負のイメージがある．けれども，その予測不可能性が，役に立つ場合もあるのだ．

最も身近な例は，テレビゲーム，コンピュータゲームだろう．ロールプレイングゲームなどで，障害物や敵が出てくるタイミングや種類などが，プレーヤーに完全に予測できてしまっては，つまらない．ゲームにはランダムネスは必要不可欠である．

このテレビゲームの応用例は，実は，とても示唆的である．予測不可能性が役立つ場面は，テレビゲームのように，人との，あるいは人同士のコミュニケーションに現れることが多い．その最たるものは暗号通信である．古くから，乱数表などが暗号通信に欠かせない道具として使われてきた．これも予測不可能性を保証するための手段だったのである．現代では，暗号も含め，情報セキュリティのためのランダムネスの研究が飛躍的に進歩している．これについては本特集の小柴氏の記事をご覧頂きたい．

ここでは，情報セキュリティ技術の研究の副産