特集にあたって

東京大学工学部　伏見　正則

「12月号の特集を何とかしてください」編集委員会から電話をいただいたのは，7月の半ばであった．原稿の締切りは8月の末とのこと．そんな無茶な，と思ったが，事情を聞けば，編集委員会の交代のために穴があいてしまって苦慮しているという．私自身も以前編集委員をしたことがあるので，当時の自転車操業もどきの編集作業を思い起こし，何とかご協力申し上げることにした．そういうわけで，短期間に原稿を書いていただけそうな方に頼み込むのが第一だったので，全体のバランスは必ずしも良くはないかもしれないが，ご容赦を願いたい．また，ご多忙中（あるいは夏季休暇を削って）執筆をしてくださった皆さんにお礼を申し上げたい．

乱数に関する研究の歴史はきわめて長く，これにたずさわった著名人も数多いが，なかでもJ. von Neumannは特筆に値するであろう．彼は，世界初の電子計算機ENIAC上で，四則演算によって乱数を作り出そうという“神に背く”大胆な試みを実行するとともに，円周率πや自然対数の底eを2000桁以上計算し，これらが（十進1桁の数字の列と見た場合に）乱数列と見なせるかどうかを統計的に検討をしている．最近では，スーパーコンピュータの発展と数値計算法の進歩により，πの値も10億桁以上計算されるようになった．そこで，その統計的検定にかかわる話を三好氏に書いていただいた．

他方，四則演算によって乱数らしきもの（擬似乱数）を作り出そうとするvon Neumannの試みは失敗に終わったが，その後まもなくLehmerによって線形合同法が提案され，長いあいだ実用に供されてきた．しかし，その欠点も次第に明らかになり，これに代わる種々の方法も提案され，研究されてきた．高橋氏は，これらの中で，特に組合せ論的な乱数列の定義と，その意味で良い乱数列であるM系列について解説してくださった．また，手塚氏には，M系列にもとづく一様乱数の発生方法のひとつであるGFSR法について，その理論的側面の一端を最近の研究から紹介していただいた．

最近のスーパーコンピュータの進歩や並列計算の普及といった計算環境の変化に伴い，古典的な線形合同法では不十分であるという状況もしばしば生ずるようになってきたので，そのような環境条件のもとで有効な乱数発生法として最近研究されている方法のうち，セル・オートマトンによる方法，および線形合同法の行列版であるmatrix generatorについても手塚氏に解説していただいた．

乱数を使って，解きたい問題に対する近似解を求める方法はモンテカルロ法と呼ばれる．この場合，誤差の標準偏差は，計算の反復回数Nの平方根に反比例することはよく知られている．しかし，問題が特殊で，多重積分の形に書き表わされるならば，乱数ではなくて，準乱数と呼ばれるものを使う方が，誤差を(オーダの意味で)小さくできる．この方法を準モンテカルロ法という．高橋氏と伏見は，これについて解説している．前者では被積分関数の解析性が大変に良い場合の理論，後者では微分可能性や連続性といった条件が成り立たなくても適用できる方法が紹介されている．誤差のオーダは，ほぼ$1/N$であり，モンテカルロ法に比べると，いちじるしく改善される．

一般に，一様乱数列といえば，文字どおり“一様性”と“乱数性（ランダムネス）”という2つの性質を満たす数列をさすものと考えられる．このうちで，一様性をとことん追求して，乱数性を排除したものが準乱数であると見ることもできよう．一方，通信の安全をはかるための暗号用乱数列にとっては，ランダムネスこそが命であるといえよう．M系列は，一様性とともに，乱数性のひとつである無相関性も備えているが，暗号用乱数列にとって重要な“予測不可能性”は弱いといわざるを得ない．そこで，M系列をもとにして暗号用の乱数列を作る方法や，もっと一般的に，暗号学的に安全な乱数列とは何か，といった問題が最近研究されているが，これらの話題のごく一部を中村・田中の両氏に解説していただいた．