連載　新シリーズ❶

科学するこころ

暗号解読

荘銀総合研究所　顧問（山形大学名誉教授）
成　澤　郁　夫

前回までは、「科学する目」というシリーズで、日常身辺に見られるさまざまな現象を科学的な目で眺めてきた。目ということばを特別に意識したわけではないが、光や色で織りなす自然や人工的な形や模様など、実際に目で見る美しさや楽しさが直接感じられる現象を取り上げる機会が多かった。科学への関心というのは、人間の感覚を通じて取り入れた情報を美しいと思ったり、不思議と思ったりするところから引き起こされるものであり、しかも、人間の五感のなかではまずなによりも見るということがもっとも基本になっていると考えたことにもよる。これから連載する「科学するこころ」というシリーズでもこの本質はあまり変わらないけれども、科学の歴史のなかではもともと人間の遊び心が実は科学するこころであり、科学の進歩を支えて来たことについて触れてみたい。

情報社会と暗号

プロ野球新球団が仙台にできることになった。昨年は球団の新設や買収をめぐる話題が茶の間を賑わしたが、名乗りをあげたのはいずれも近年急激に成長した情報関連企業である。これらの企業が成功したのは、なんといってもインターネットの普及が大きい。ショッピングや旅行予約などはもちろんのこと、今ではあらゆるサービスがインターネットを通じて簡単にできる時代になって来ている。このようなサービスシステムをいち早く作り上げたところにこれらの企業の勝因がある。インターネットサービスを利用したときに、私たちが気になるのは、個人データやクレジットカードなどの情報が他に漏洩（ろうえい）しないかということである。信頼できるサイトでは、暗号化して送るから安全というメッセージが示されるのでこれを信頼するほかはないのであるが。

たとえば、暗証番号のような４桁程度の数字の組み合わせであれば、１万回の数字をしらみ潰（つぶ）しで組み合わせればよいから、コンピューターを使えば秒単位で解答がでてしまう。桁（けた）数がもっと増えてもほとんど同じである。しらみ潰しで調べる方法は総当り攻撃といって暗号解読の初歩とされるが、何回でも繰り返し試行が許されるならば、コンピューターがこれだけ発達した現在では、解読できない暗号は存在しないと思った方が良いかも知れない。現在インターネットで使われている暗号化の技法は、巨大な整数を素因数分解しなければならないために、現存する最大処理速度をもつコンピューターといえども計算には途方もない長い時間がかかるので、実際上は解読が不可能であるということを安全の根拠にしている。もっとも原理的には解ける問題であるから、コンピューターの性能がさらに向上し、ネットワークを使って多数のコンピューターを用いた分散処理などをすれば力ずくで解読できるので、永久に安心というわけにはいかない。絶対に破られない暗号としては量子暗号の研究が行われている。読み取ることで情報が変化するので、ただ１回しか解読できないことが特徴になっている。

ことば遊びと文字遊び

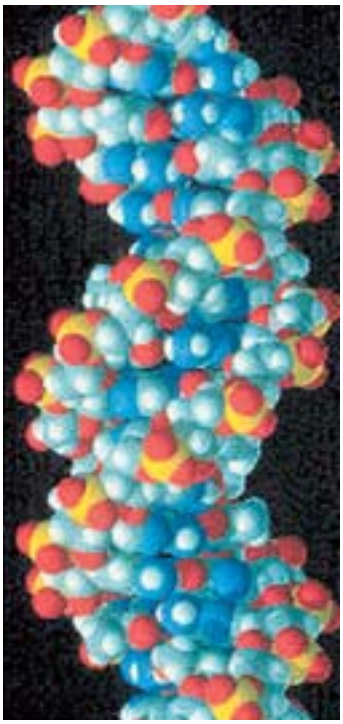
暗号通信を使い始めた歴史は古く、人間がことばをもち始めた時代にまで遡るとされる。メッセージの内容を第３者に秘めて特定の人にだけ伝えたいという要求は、恋の思いを打ち明けたいと

か、財宝のありかを仲間に伝えたいとかの理由で、人間が社会生活を始めるとともに出てくるようである。現人類が進化の幹から分離して文明や文化を築き上げることができたのは、多様な音声を発することができて、ことばや文字を持つことができたからといわれている。しかも、人間にとってことばや文字を使って遊ぶことが楽しみにさえなっていることは、どんな言語や文字を使っていても駄洒落やギャグが好きな人が結構いることを見てもよくわかる。また、文字遊びについても同様で、昔からどこの国でも絵混じり文というのがあったが、今はメールにまで無理やりに笑い顔や怒り顔を入れないと気がすまない人もいる。

暗号通信はこのことばや文字の遊びに起源をもっている。アクロスティックといわれる文字遊びがあるが、一見してなんでもない文章のなかの定められた文字を拾って繋げると、あるメッセージが浮かび上がるという遊びである。どの文字を選ぶかということが暗号解読のキーとなる。米国のエドガー・アラン・ポーが「黄金虫」という暗号小説のなかでこれを使ったが、この方法はすでに日本の古い和歌にも見られる遊びである。兼好法師が友人に宛てた、「夜も涼し寝覚めの刈穂手枕も真袖の秋に隔てなき風」という歌の各フレーズの頭と末尾の字を拾って繋げて見ると、秘かに頼みごとの暗号通信を試みていることが分かる。ぜひ読者が解読してみて欲しい。

自然界の暗号通信

なによりも自然そのものが暗号であるといった暗号解読者もいる。ひとりの人間をつくり、生命活動を維持させていく遺伝子情報はヒトゲノムといわれる。この情報はすべてDNAといわれる、らせん状にねじれて連結している２本の長い分子の紐のなかに含まれている。この繋がりのなかには塩基といわれる４種類の化学物質が整然と配列されており、この物質が文字となってその並び方によって情報を保存している。ヒトゲノム解析というのはこの４つの文字の配列を調べることで遺伝情報を読み取るという試みであるが、なにしろヒトのDNAに記された全遺伝情報は30億文字の並びに相当し、しかも４種類だけの単純な文字の羅列ということで、上手に読まないと読んでいる場所さえわからなくなってくる。1991年にこの配列を解読するヒトゲノム計画が始まったが、当初は15年かかるといわれたものが、今ではすでに解読が済んでいる。しかし、解読して分かったことはDNAの機能はもっと複雑であり、生命の維持に必要な各種のタンパク質を生み出すことに関わっているのは、多くの遊んでいる配列の一部だけらしく、その部分がどこかと探すのはまさしく暗号解読と同じである。しかも文字の欠落や挿入、置き換えなどがあることも暗号通信と同様である。暗号を解読する作業が要求されるのは、なにもこればかりではないようで、考古学では発掘した一部の破片をつなぎ合せて古代の文明を推定する。天文学では宇宙の規模から見ればごく僅かの観測データによってその進化を推測するなど、学問すべてが暗号解読といえるのかも知れない。



らせん構造のDNA模型

（答：米たまへ、ぜにもほし）