用語解説

電子マネー (Electronic Money)

電子マネーとは，デジタル化された情報によって実現された貨幣のことである．電子マネーが通常の貨幣と同じような利便性を実現するためには，(1) 貨幣が完全に情報のみで自立して実現されている，(2) コピーや偽造などの不正ができない，(3) 利用者の購買に関する情報が小売店や銀行など取引に介在する者に露見しない，(4) 小売店での支払い処理が銀行へのオンライン・チェックなしに行える，(5) 他人への譲渡ができる，(6) 任意に分割利用できる，という6つの条件が必要である．

これらの条件を満たす電子マネーは，ブラインド署名ならびにcut and choose法を利用して構成できる．まず、貨幣価値を示す情報とIDをK個のメッセージに分解し，それぞれに乱数を付加して銀行に電子署名を依頼する．乱数の付加によって銀行にメッセージの内容を知られることなく署名を得ることができる（ブラインド署名）．銀行はこのK個のメッセージのうちの半分を任意に選び，このメッセージに対応する乱数を開示要求して依頼者の正当性を確かめる（cut and choose法）．こうして得られた残りK/2個の銀行の署名付きメッセージを電子マネーとして用いる．不正利用があっても，銀行にK/2個のメッセージが記録されているので，不正利用者が銀行の審査を免れる確率はわずかに2のk/2乗分の1でしかない．このようにして条件(1)-(4)を満たす電子マネーが構築できる．さらに条件(5)(6)を満たす理想的電子現金方式も提案されている．

文献：[1]D.Chaum, Security without identification: transaction systems to make big brother obsolete, Comm. of the ACM 28, pp.1030-1044, 1985
[2]情報理論とその応用学会，暗号と認証，培風館，1996

(埼玉大学　経済学部　川越敏司)

フラクタル次元 (Fractal dimension)

時系列データを多次元空間に埋め込んだときにできる軌道の複雑さを測るための手法の一つにフラクタル次元(fractal dimension)がある。これは、1975年にB.Mandelbrotによって命名されたものである。一般に非整数次元を与える次元には、容量次元(capacity dimension)、情報次元(information dimension)、相関次元(correlation dimension)などがある。フラクタル次元を求めるために最も良く用いられているのが、他の方法と比べて計算機処理上有利な相関次元である。この概念は次のようなものである。いま、d次元空間に再構成されて得られる集合(たとえばアトラクタ(attractor))を考える。このd次元空間を一辺がεの超立方体で分割したときの超立方体の総数を$n(\varepsilon)$とする。アトラクタを構成する軌道(trajectory)がi番目の超立方体を通過する確率p_iを式(1)で求める。

$$p_i = \lim_{N \to \infty} \frac{N_i}{N} \tag{1}$$

ここで、Nはアトラクタを構成するベクトル数、N_iはi番目の超立方体を通過するベクトルの数である。これを用いて(2)式により求める。

$$D = \lim_{\varepsilon \to 0} \left\{ \frac{\log\left(\sum_{i=1}^{n(\varepsilon)} p_i^2\right)}{\log \varepsilon} \right\} \tag{2}$$

具体的で便利な計算方法は参考文献に詳しく解説されているので、そちらを参照されたい。

代表的なカオスにおけるフラクタル次元は、カントール集合（約0.63)、エノンマップ(約1.21)、ローレンツ系（約2.05)である。

なお、フラクタル次元を用いて時系列データの位相構造の違いを把握し、システムのダイナミクスの変化をとらえ異常診断への応用が研究されている。

文献：長島弘幸、馬場良和共著、カオス入門、培風館、1992

(明電舎　システム技術部　五百旗頭 正)