国立大学法人岩手大学　情報処理センター研究紀要　第 2 号 2014 年　Online edition: ISSN 2188-4811
Bulletin of Iwate University Super Computing and Information Sciences Center, No.2, 2014

小さな領域中の雲を用いたカオス・ダイナミクスの研究

吉田等明[†1]　平　寛人[†2]　小毛利　徹[†2]　中西貴裕[†1]

小さな領域中にとったカオス力学系の複数個の初期状態から生じる複数のカオス軌道の時間変化を同時に追うことによって，カオスの過渡状態を研究した．ある時刻に限定すると，複数の軌道は点の集合として表現できる．この集合を雲と呼ぶ．雲の過渡状態として，拡散の様な散らばり広がる運動（通常の拡散と区別して擬拡散と呼ぶ）と形状の変形を別々に観測した．最初，小さな 4 次元立方体の中に均一に分布していた雲は，一旦，直線状に変化するが，カオス特有の引き延ばしと折り畳みによる変化を繰り返しながら，カオス・アトラクタ（定常状態）へと近づいていく．雲の形状の変化及び擬拡散は，初期状態の 4 次元立方体の大きさδ に依存しており，実験から求めた関係式によって，フラクタル次元が約 1 に保たれる期間の長さを見積もることができた．このようなシステムを暗号に応用する場合には，安全性の面から直線のなどの規則的な形状にある期間を考慮に入れることは重要と思われる．

Study on Chaos Dynamics by Using a Cloud in a Small Region

Hitoaki YOSHIDA, [†1] Hiroto TAIRA, [†2] Touru KOMORI, [†2] and Takahiro NAKANISHI[†1]

Transient state of a chaos has been studied with the time course of chaos orbits which start from different initial conditions within a small region. A chaos orbit is represented as a point in a phase space at a single instant. A set of the points is called a cloud. The transition of the cloud involves diffusional motion (called pseudo-diffusional motion) and transformation of the shape of the cloud. At first a uniformly distributed cloud in 4D-cube, the shape once has been transformed into a line shape and then continuously transformed until reach a chaos attractor (steady state). The transformation of the cloud shape and the pseudo-diffusional motion depend on the size of the initial 4D-cube (δ). The period that keeps D=1 has been estimated experimentally. The result is useful for evaluating the safety of such chaotic cipher.

1. はじめに

通常，カオス力学系 F の軌道$\{F^t(y_0)\}$を調べる際には，位相空間内の 1 点を初期点 y_0 として，その時間発展（iteration）を追っていく．

$$y_{t+1} = F(y_t) \qquad (1)$$

ここで，t は整数とする．

Romeiras, Grebogi, と Ott は別の実験方法を提案している．それは，定義全体に一様に分布した初期点の集合（雲）から始めて，時間発展に伴って変化する雲のスナップショット・パターン（点の空間分布）を観測する方法である．ここで雲とは，ある時刻における，位相空間内の複数の軌道が作る点の集合とする．2 つの異なった方法で観測し続けた場合においても，長時間経過後（$t\to\infty$）アトラクタの形は非常に似通ったものとなる．言い換えると，充分な時間の経過後に，その雲は定常状態に到達する．[1], [2]

我々は，Hopfield ネットワークや BP 法で用いられる通常の人工ニューロンからなるカオス・ニューラルネットワーク(CNN)を用いたカオスの生成について研究を行ってきている．[3], [4]　最近，CNN をストリーム暗号に応用し，情報セキュリティ・システムとして商品化している．[5] 本研究では，小さな領域内の雲を初期値の集合として用いることにより，CNN 出力の過渡状態を研究した．過渡状態において観測された，拡散に類似した現象（擬拡散）はカオスの初期値鋭敏性の研究の観点から興味深い結果を与えるものであり，暗号への応用の際には，雲の形状の変化と共に安全性を考察する重要な知見を与えるものであるので報告する．

本研究では，4 個の人工ニューロンから構成した離散力学系のカオス・ニューラルネットワーク（B-4nn）をカオス発生器として用いる．（図 1）

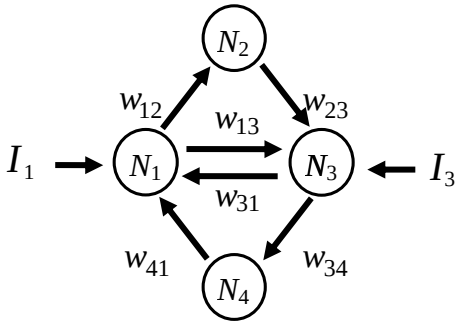


図 1　２つの環構造を持つ CNN（B-4nn）
Figure 1　CNN having bicyclic structure (B-4nn).

j 番目のニューロンの時刻 t+1 における内部状態 $f(u_j(t))$は式(2)の関係を用いて式(3)で定義される．ここで，w_{ij} は i 番目のニューロンと j 番目のニューロンのシナプス重み，θ_j は

†1 岩手大学情報メディアセンター
Super Computing and Information Sciences Center, Iwate University
†2 岩手大学大学院工学研究科
Graduate School of Computer and Information Sciences, Iwate University

j 番目のニューロンの閾値，I_j は j 番目のニューロンの外部入力値である．

$$u_j(t) = \sum_{i=1}^{n} w_{ij} x_i(t-1) - \theta_j + I_j \qquad (2)$$

ここで代表的なパラメータ値を示すと，

$w_{12} = 4.4$，$w_{13} = 5.3$，$w_{23} = -5.0$，$w_{31} = 6.5$，$w_{34} = 20.3$，$w_{41} = 4.6$
$\theta_1 = 0.0$, $\theta_2 = 2.0$，$\theta_3 = 0.0$，$\theta_4 = 3.0$，　$I_1 = I_3 = -2.45$
である．パラメータ値は経験的に決めたものであり，カオス出力を得るためには，正と負のシナプス重みを設定する必要がある．外部入力値は分岐図を作成してカオス状態を調べ, 周期窓を避けてカオス出力が得られる値を設定する．

カオスの性質として，小さな誤差が指数関数的に増加する初期値鋭敏性が知られている. このような系においては，演算誤差が計算結果に大きな影響を及ぼす．特に，桁落ち誤差によって，変数の有効桁数が減少すると表現できる数値の範囲が減少するため，桁落ち誤算発生はできるだけ避けなければならない．

通常用いられるシグモイド関数（式(3)）の代わりに，本研究では桁落ち誤差を避けるために，式(4)に示す関数を用いた．これは，式(2)を式(3)に代入し，加減算を避ける形に変形したものである．

$$f(u_j(t)) = \frac{1}{1+\exp\{-u_j(t)\}} \qquad (3)$$

$$f(u_j(t)) = \frac{1}{1+\exp(\theta_j)\exp(-I_j)\prod_{i=1}^{4}\exp\{-w_{ij}x_i(t-1)\}} \qquad (4)$$

この値は，時刻 t+1 におけるニューロン j の出力であり，ニューロン j の内部状態と呼ぶことにする．

時刻 t におけるニューラルネットワーク B-4nn を構成する 4 つのニューロンの内部状態（$x_1(t)$, $x_2(t)$, $x_3(t)$, $x_4(t)$）を用いると，4 次元相空間内で B-4nn の状態を一意に表現する点 $X(t)$を定義することができる．

$$X(t) = (x_1(t), x_2(t), x_3(t), x_4(t)) \qquad (5)$$

B-4nn はカオス力学系 G に従うとして式(6)のように，その時間発展（iteration）を表現することができる．

$$X(t+1) = G(X(t)) \qquad (6)$$

2. 小さな領域の雲

本研究では，初期点の分布を定義域全体に取るのではなく，小さな矩形領域の中に取る方法を提案する．この結果の一部は，既に国際会議で報告しているが[7]，ここではその方法の詳細を議論していく．

図 2(a)のように，4 次元相空間内に一辺がδの小さな4次元立方体を定義し，その中に10^4個の初期点を一様に配置する．ここで時刻 t における雲を集合 $U(t)$として式(7)のように定義する．4 次元の雲を観察するために，図 2 では，4 次元目の座標軸を色で表現している．

$$U(t) = \{X_k(t) \mid k = 1, 2, \ldots, 10^4\} \qquad (7)$$

この方法の長所は，繰り返し毎に（各時刻での）雲のスナップショット･パターンを観測できることである. 集合 $U(t)$ に対しても, カオス力学系 G の時間発展を式(8)のように書くこととする．これは，式(7)で表される $U(t)$の要素の一つ一つについて，式(6)の操作を繰り返し行うことで時刻 t+1 の集合 $U(t+1)$を得ることを表している．

$$U(t+1) = G(U(t)) \qquad (8)$$

(i) $\delta = 10^{-4}$-10^{-10} の場合

本研究では，$\delta = 10^{-4}$-10^{-10} の範囲の小さな 4 次元立方体の中に初期点を配置して，その後の時間発展を調べた．興味深いことに比較的長い過渡状態を持ち，その間にδの値に依存した様々な特徴を持つ変化が観察された.（図 2）

(ii) $\delta = 1$ の場合

比較のため$\delta = 1$ の場合も実験した. 定義域全体に一様に初期点を配置することになるので，文献[1], [2]の初期点の配置に準ずるものとなる．この場合には(i)の場合とは全く異なり，スナップショット・パターンは，t =19 で速やかにカオス・アトラクタに収束した．（図 3）

3. 時間発展に伴う雲の形状の変化

時刻毎に，雲 $U(t)$のスナップショット・パターンを観測した結果の一部を図 2 に示した．ここでは，小さな雲の形状を観察するために最大値を 1 に規格化して，値の変化を[0,1]の範囲で表現してある．長い過渡状態(t = 1-133)の間に様々な形状の変化が観察される．時刻 t = 12 では面が連なったような形状に変化し，時刻 t = 27 では直線状に変化していくのが観察される．そして，直線は折れ曲がり，折りたたまれて（図 2(d)，図 2(e)）次第にカオス・アトラクタに近づいていく（t = 133，図 2(f)）．

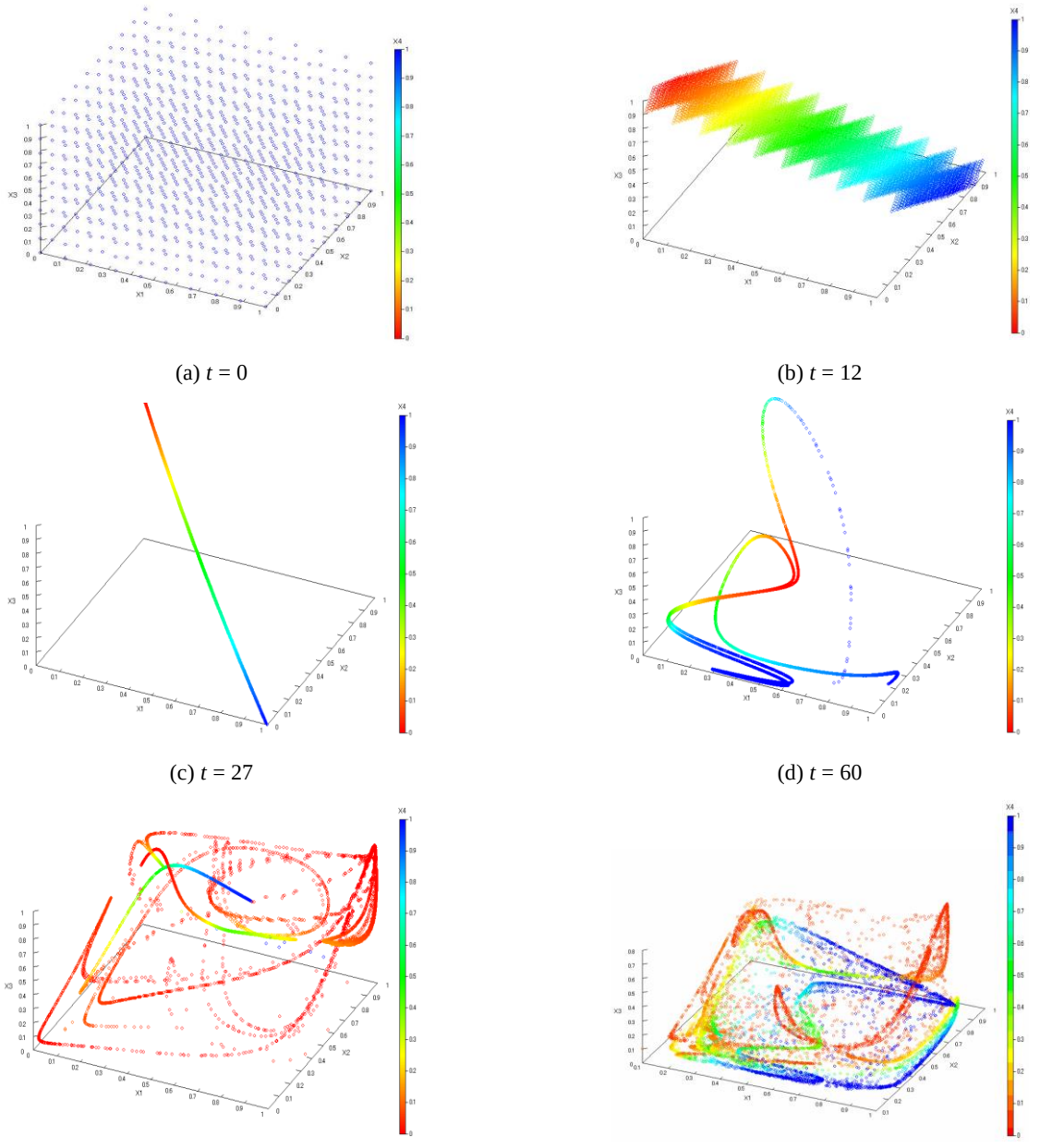
この形状の変化を様々なケースで調べると，異なる力学系（例えば異なる構造やパラメータで定義されるカオス・ニューラルネットワーク）では異なる変化を示したが，本研究では，B-4nn についての結果についてのみ述べる．

スナップショット・パターンの時間変化を，フラクタル次元を使って定量化した結果の模式図を図 4 に示す．ここ

Online edition: ISSN 2188-4811

でフラクタル次元解析には，ボックスカウント法を用いている．サンプルとなるスナップショット・パターンは，規格化したデータと，規格化しないデータの両方を区別して用いている．青色の線は規格化したデータを用いたフラクタル次元の時間変化を示す線であり，赤色の線は規格化しないデータを用いたフラクタル次元の変化である．ここでは，細かな値の変動を無視して滑らかな線の組み合わせで模式図として表現してある．

準安定状態 M1 は面が連なった構造のパターンを含む部分であり（図 2(b)），フラクタル次元は約 2.1 を保っている，そして準安定状態 M2 では直線状のパターンとなり（図 2(c), 図 5），フラクタル次元は約 1 を保っている．面に近いパターンであれば，フラクタル次元は 2 に近い値となり，線に近いパターンであればフラクタル次元は 1 に近い値となることは自然なことである．しかしこれは必要十分条件ではないことに注意されたい．即ち，フラクタル次元が 2 に近いからと言って必ず面状の構造を取る訳ではなく，フラクタル次元が 1 に近いからと言って必ず線状の構造を取る訳ではない．このようにフラクタル次元のみから雲の形状を



(a) t = 0　(b) t = 12

(c) t = 27　(d) t = 60

(e) t = 72　(f) t = 133

図 2　規格化した雲の形状変化($\delta = 10^{-5}$)

Figure 2　The shape change of the normalized cloud ($\delta = 10^{-5}$).

Online edition: ISSN 2188-4811

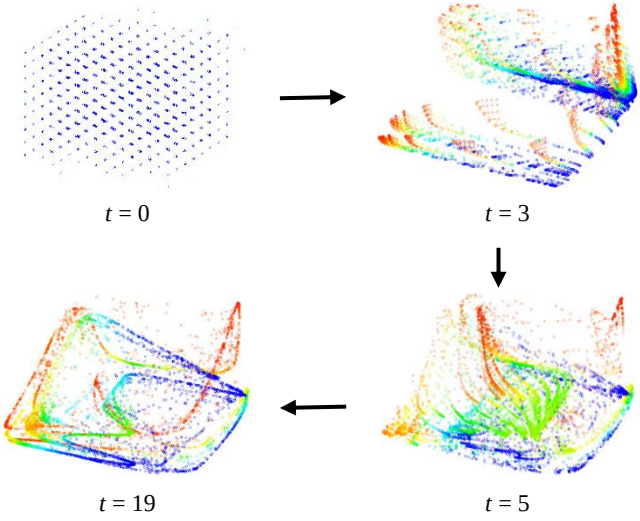


図 3　雲の形状変化($\delta = 1$)

Figure 3　The shape change of the cloud ($\delta = 1$).

知ることはできないので，図による観察は重要である．また，$t = 0$ でフラクタル次元が 2 以下の値となるのは，点が全体に分散して疎になっているためである．

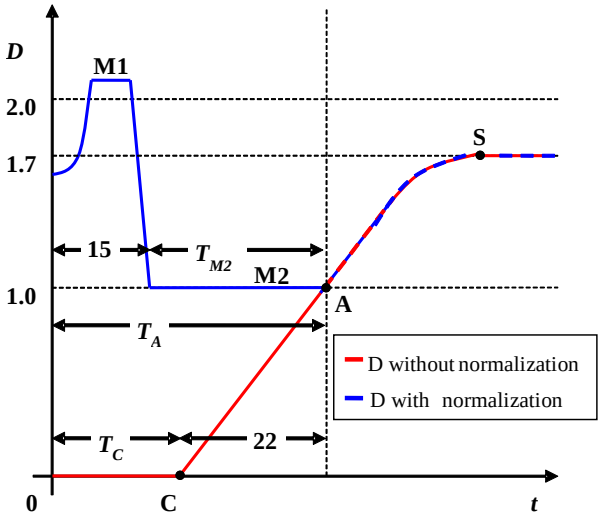


図 4　模式図で示したフラクタル次元の時間変化

Figure 4　Time course of the fractal dimension (D) in schematic diagram.

ここで，図 2(c)のような高度な対称性を持つスナップショット・パターンの場合，異なる初期値からスタートした軌道であっても，相互の関連性から予測できる可能性がある．即ち，フラクタル次元が約 1 に保たれる期間 T_{M2} の長さを見積もっておくことは，暗号系に応用する際には重要と考えられる．実際の暗号への攻撃方法は参考文献[8]で報告している．また，直線状の準安定状態は，Logistic map や Lorentz map を用いた著名なカオスの場合でも観測される一般的な現象であることを見出し報告している．[6]

図 4 において，規格化しない場合に（赤色の線）フラクタル次元がゼロでない値を持ち始めるまでの時間 T_c は，雲の初期サイズδに依存して異なる値となる．時間 T_A，時間 T_{M2} もその影響を受けて変化する．[7]　規格化しない場合，時間 T_c の間，雲のサイズは小さすぎてフラクタル次元を観測できない($D = 0$)．何故なら，ボックスカウント法で用いるボックスのサイズより雲のサイズが小さいからである．全体として雲は拡散過程のように点 A まで広がって行く．しかしながら，規格化した場合にはフラクタル次元が観測でき（青色の線），雲の形状変化とともに考察することができる．２つの異なる時間変化は，雲のサイズがダイナミックレンジに到達する点 A 以降はほぼ同じになる．

また点 S は，それ以降フラクタル次元はほぼ一定の値となる点である($D = 1.7$)．これはフラクタル次元を尺度とした観測では，定常状態に達したことを意味する．過渡状態と定常状態との境界についての詳細な議論は，今後の報告で述べることにしたい．

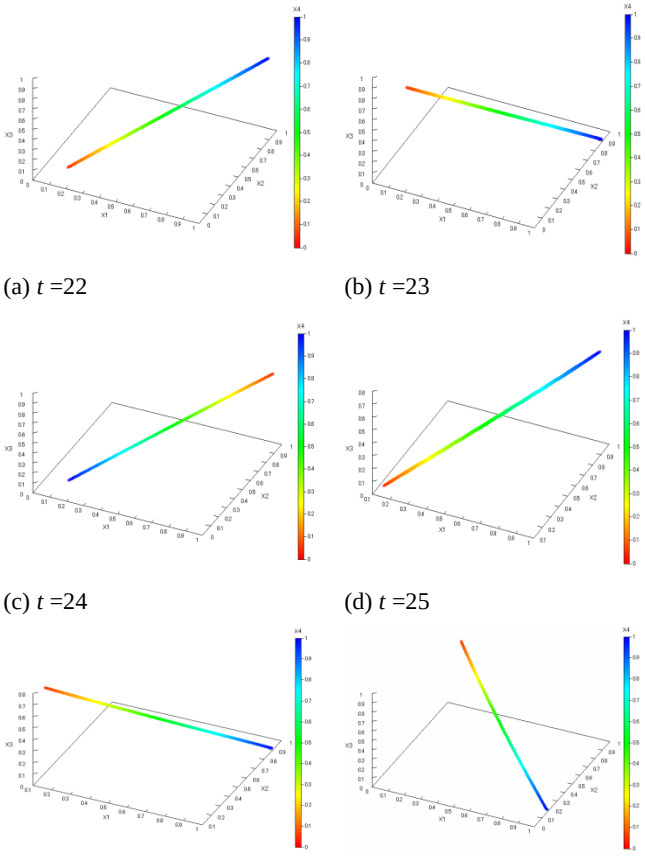


図 5　4 次元相空間内における規格化した直線状の雲の回転運動

Figure 5　Rotational motion of normalized line shaped clouds in 4D-phase space.

雲の初期サイズδによる違いは，規格化しない場合には時間 T_c の変化として現れ，規格化した場合にはフラクタル次元が約 1 に保たれる時間 T_{M2} の変化として観測される．準安定状態 M2 の間，雲の形状はほぼ直線状を保ったまま，主に伸びと回転運動（図 5）が起きている．[8]　フラクタル次元解析では変化を捉えにくいため，次のセクションでは雲のサイズを定義してその変化を調べることで，この時間帯に何が起きているかを検討して行く．
この雲が散らばり広がる現象は，拡散過程からの類推で擬拡散（pseudo-diffusional motion）と呼ぶことにする．

4.　擬拡散

フラクタル次元解析では，雲の変化は時間 T_c の間観測することができなかった．そこで，その間の雲の動きを観測するために別の方法を用いる．ここで雲のサイズ L を以下のように定義する．

$$S_n = \max(x_n) - \min(x_n) \tag{9}$$

$$L = \frac{1}{2}\sqrt{S_1^{\,2} + S_2^{\,2} + S_3^{\,2} + S_4^{\,2}} \tag{10}$$

ここで x_n は n 番目の座標の値，$\max(x_n)$ は x_n の最大値，そして $\min(x_n)$ は x_n の最小値である(n = 1, 2, 3, 4)．ある一つの座標値で表した雲のサイズ S_n は時間に依存して大きく変化し，単純な結果を与えなかった．この原因は図 5 に示す回転運動や，カオス特有の引き延ばしと折り畳みのプロセスの結果と考えられる．即ち，雲の形状は 4 つの次元それぞれの方向において，等しく広がって行くわけではなくいびつであるため，回転によって個々の S_n は大きく変化しているものと考えられる．

そこで式(10)のように，4 次元のそれぞれの成分についての二乗平均 L を雲の長さとして定義する．これであれば，回転運動による値の変動を比較的小さく抑えて表すことができると考えられる．L の時間変化の観測値を図 6 に示す．縦軸は log L であり，横軸は時間 t である．実験値は×印で示してあり，回帰直線及び直線の方程式も合わせて示してある．相関係数は 0.995 であり，雲のサイズの対数値 log$L$ は時間と強い相関を示している．時間経過とともに最大値である L=1 まで広がって行く様子が観察できる．

初期点を含む 4 次元立方体の 1 辺がδ= 10^{-10} であり，1 辺には 10 個の点が一様に配置してあるため，2 つの初期点の間隔はδの 1/10 である 10^{-11} となる．この微小な初期値の違いが，カオスに特有の初期値鋭敏性によって指数関数的に広がって行く．それが，図 6 に示す擬拡散の原因と考えられる．

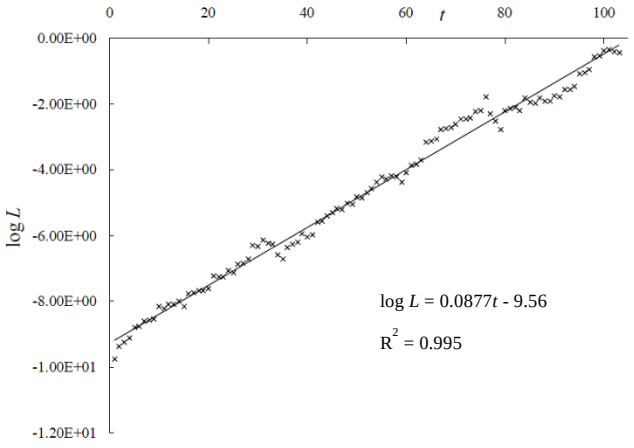


図 6　　雲のサイズ L の時間変化 ($\delta = 10^{-10}$)

Figure 6　The time course of L ($\delta = 10^{-10}$).

この実験をδ = 10^{-4}-10^{-9} で行った場合にも同様の結果が得られ，相関係数は 0.986-0.995 であった．しかしながら，図 3 のようにはじめから定義域全体に配置した場合(δ = 1)には，擬拡散に相当する現象は観測されない．

図 6 に示した回帰直線を一般式で表すと式(11)のようになり，変形すると式(12)の形になる．

$$\log L = at + b \tag{11}$$

$$L = 10^{at+b} \tag{12}$$

ここで a は回帰直線の傾き，　b は y 切片とする．

次に，10^{-4}-10^{-10} の範囲でδを変化させて同様の実験を行うと，y 切片 b はδ の値にかなり正確に比例した値となり（図 7），傾き a はδの値によらずほぼ一定値となる（図8）．その結果から，式(13)-(14)の関係式が得られる．

$$b = \log\delta + 0.406 \tag{13}$$

$$a \approx 0.089 \tag{14}$$

式(12)-(14)から，L が 1 に達するまでの時間 T_A を求めると，

$$T_A \approx -11.2 \times \log\delta - 4.56 \tag{15}$$

また，フラクタル次元が約 1 に保たれる時間 T_{M2} は，参考文献[7]での結果を用いると，近似的に以下のように表される．

$$T_{M2} \approx T_A - 15 \approx -11.2 \times \log\delta - 19.6 \tag{16}$$

Online edition: ISSN 2188-4811

もし，B-4nn からのカオス出力を暗号に応用する場合は，T_{M2} の時間内は攻撃の危険があることに注意しなければならない．攻撃方法の詳細については，参考文献[8]で報告しているので参照されたい．

このように拡散に類似した散らばり広がる現象（擬拡散）が観測されたことは，Namenson らの研究[1]や Romeiras らの研究[2]には現れてこなかったものであり，カオスの初期値鋭敏性の研究の観点からも興味深い．

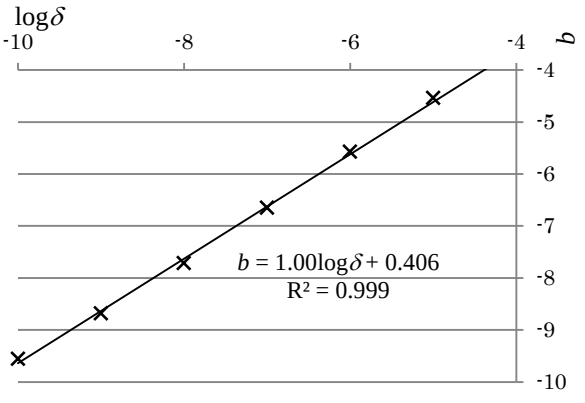


図 7　雲の初期サイズδによる回帰直線の y 切片 b の変化

Figure 7　The relation between the initial size of the cloud (δ) and the y-intercept of the regression line (b).

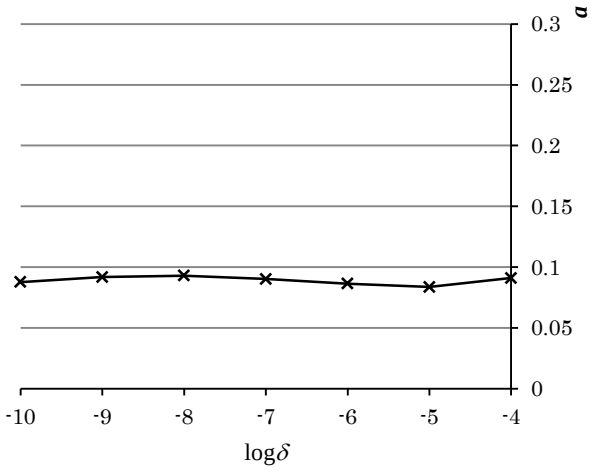


図 8　雲の初期サイズδによる回帰直線の傾き a の変化

Figure 8　The relation between the initial size of the cloud (δ) and the slope of the regression line (a).

5. 結論

小さな領域中（δ=10^{-4}-10^{-10}）にとった 10^4 個の初期状態の集合 $U(0)$（雲）の時間変化を追うことによってカオスの過渡状態を研究した．雲の過渡状態として，拡散の様な散らばり広がる運動(擬拡散)と形状の変形を別々に観測した．最初, 小さな 4 次元立方体の中に均一に分布していた雲は，一旦，直線状に変化する．これは，集合 $U(t)$は期間 T_{M2} の間，非常に強い相関を保っていることを意味する．その後カオス特有の引き延ばしと折り畳みによる変化を繰り返しながら，カオス・アトラクタ（定常状態）へと近づいていく．雲の形状の変化及び擬拡散は，初期状態の 4 次元立方体の大きさδ に依存していることを実験的に見出した．さらに実験から求めた関係式によって，フラクタル次元が約 1 に保たれる期間の長さ T_{M2} を見積もることができた．以前我々は，直線状の準安定状態が一般的に良く知られている Logistic map や Lorentz map を用いたカオスの場合にも同様に観測されることを示している．[6]　暗号に応用する場合には，安全性の面から直線などの規則的な形状にある期間を考慮に入れることは重要であるため，[8]　このような関係式が得られたことは非常に興味深い．

謝辞　本研究は，岩手大学情報処理センターの計算機を利用して行った研究である．運用及び維持管理に尽力しておられる情報処理センタースタッフ諸氏に深く感謝の意を表します．

参考文献

1) Namenson, A., Ott, E. and Antonsen, T. M.: Fractal dimension fluctuations for snapshot attractors of random maps, Phys. Rev. E 53, pp.2287-2291 (1996).
2) Romeiras, F. J., Grebogi, C. and Ott, E.: Multifractal properties of snapshot attractors of random maps, Phys. Rev. A 41, pp.784-799 (1990).
3) Yoshida, H., Yoneki, K., Tsunekawa, Y. and Miura, M.: Chaos Neural Network, Proceedings of Papers, ISPACS'96, vol.lof3, pp.16.1.1-5, (1996).
4) Kawamura, S., Yoshida, H. and Miura, M.: Minimum Constituents of Chaos Neural Network Composed of Conventional Neurons, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, Vol.J84-A, No.5, pp.586-594 (2001).
5) Kawamura, S., Yoshida, H., Miura, M. and Abe, M.: Implementation of Uniform Pseudo Random Number Generator and Application to Stream Cipher based on Chaos Neural Network, Proceedings of Papers, the International Conference on Fundamentals of Electronics, Communications and Computer Sciences, R-18 (2002).
6) Kakizaki, T. and Yoshida, H.: Study on Transition State of Chaos Time Series Using for Neighborhood Set, IEICE Technical Report, NLP2008-50, pp. 25-30 (2008).
7) Yoshida, H., Ohira, O., Taira, H. and Nakanishi, T.: Fractal Analysis of Chaos Neural Network Outputs in Transient State and Steady State, Proceedings of Papers, 2006 International Symposium on Nonlinear Theory and its Applications, pp.103-106 (2006).
8) 高橋直人，吉田等明: 近傍集合を用いた暗号攻撃手法の研究, 電子情報通信学会技術研究報告，NLP2008-49, pp. 19-24(2008).