コンピュータセキュリティ 11－6
（２０００．９．８）

カオス・ニューラルネットワークを用いた暗号系の基本的特性

川村 暁*，池田直弥*，吉田等明**，三浦 守*

*岩手大学大学院工学研究科
**岩手大学情報処理センター

あらまし
筆者らの提案によるカオス・ニューラルネットワーク (CNN) を用いた共通鍵暗号系 (CNN Cipher) に関して，その安全性と評価法などの基本的特性について述べる．本稿では初めに，CNN の出力するカオスの特異性を，他のカオス系との比較により明らかにする．次に，CNN Cipher の計算量的安全性について，CNN の性質を考察することにより評価する．

Basic Characteristics of Cryptosystem Using Chaos Neural Network

Satoshi KAWAMURA*, Naoya IKEDA*, Hitoaki YOSHIDA** and Mamoru MIURA*

*Graduate School of Engineering, Iwate University
**Computer Center, Iwate University

Abstract
This paper deals with basic characteristics of cryptosystem using chaos neural network (CNN Cipher), already proposed. At first, a distinctive feature of chaos in the CNN is described. Next, computational-time complexity of the CNN Cipher is considered with characteristics of chaos in the CNN.

1. はじめに

インターネットに代表されるオープンなネットワークの利用が，急速な広がりを見せている．この場合，情報に対する不正防止の必要性，すなわち，情報セキュリティ技術の必要性が増大する．中でもデータ秘匿の手段としての暗号とその応用は重要な基本的技術となる[1)~3)]．

これまで提案されてきた暗号系は，基礎理論として換字や転字と整数論の問題（素因数分解や離散対数問題）を用いている[1)~3)]．これに対し筆者らは，特異なカオス力学系であるカオス・ニューラルネットワーク（以下，CNN）[4)~12)] を暗号化関数に用いた共通鍵暗号の一方式を提案し，その特性について議論している[13)~14)]．この暗号系は，CNN の構成のみではなく，その実行環境（計算機や OS の種類）にも依存する特異なものであることを明らかにしている．

本稿では，CNN を用いた暗号系（以下，CNN Cipher）の構成について述べた後，CNN Cipher の基礎をなす CNN の出力するカオスの特性について考察する．次に，本暗号系の安全性の評価を試みる．

暗号の安全性評価には，その暗号が用いている基礎理論の計算量的困難さによる評価がなされる．よって本稿では，CNN Cipherの計算量的安全性について，CNN の特性を用いて，評価する．

2．CNNを用いた暗号系

CNN Cipher は，カオス応答する人工ニューラルネットワークを暗号化関数として用いている．本節では，CNN について概説する．

2.1 ニューラルネットワーク (NN)

NN とは，生物の神経系を模擬した情報処理様式である．神経細胞の動作を模擬するモデル（ニューロンモデル）を考え，これを複数個結合することにより NN が構築される．

式 (2.1) ～式 (2.3) と図 2.1 に，本稿で用いるニューロンモデルを示す．このモデルは，Hopfield Network や多層パーセプトロンなどにおいて一般的に用いられるモデルである．非線形出力関数として用いた sigmoid 関数を式 (2.2) に示す．

$$y_m(t) = f(u_m) \cdots\cdots\cdots\cdots\cdots\cdots \quad (2.1)$$

$$f(u_m) = 1/\{1+\exp(u_m/\lambda)\} \cdots\cdots\cdots \quad (2.2)$$

$$u_m = \sum_{i=1}^{n} w_{im}x_i(t) + \theta_m + I_m \cdots\cdots\cdots \quad (2.3)$$

ここで，各変数を以下のように定義する．

$y_m(t)$：ニューロン m の時刻 t の出力．
u_m：ニューロン m の内部状態．
λ：非線形出力関数 f の傾き係数
$x_i(t)$：時刻 t におけるニューロン i からの入力．
w_{ij}：ニューロン i からニューロン j への重み係数．
I_m：ニューロン m への外部入力値．
θ_m：ニューロン m の閾値．

2.2 カオス・ニューラルネットワーク (CNN)

本稿で用いたニューロンモデルでは，単一のニューロンでは出力は振動しない．出力が振動する最も基本的なネットワークを図 2.2 に示す．

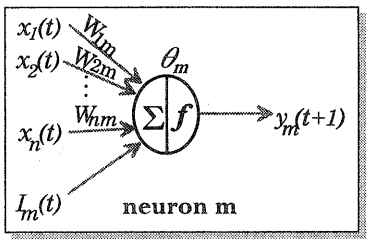

図 2.1 ニューロンモデル

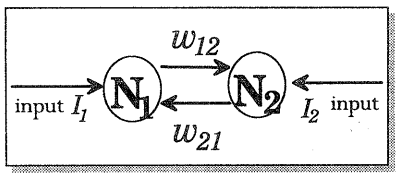

図 2.2 基本振動 NN

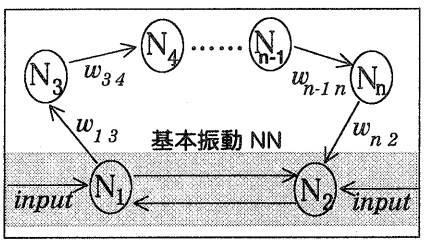

図 2.3 ネットワークモデル

我々はこれを基本振動ネットワーク（以下，基本振動 NN）と定義している[11),12)]．

基本振動 NN を含む，ニューロン数 n 個の NN へ拡張した構成を図 2.3 に示す．このネットワークは，以下の要素により特徴づけられる．

- 基本振動 NN の種類
- ニューロン数
- ニューロン間の重み係数

我々は，この構成のネットワークにおいてカオス応答する NN が存在することを明らかにしており，そのようなネットワークを CNN と定義している[11),12)]．例として，3個のニューロンからなる CNN の，分岐図を図 2.4，リアプノフ指数を図 2.5 に示す．分岐図とは，横軸に外部入力値 I，縦軸に出力をとったグラフであり，リアプノフ指数では横軸に外部入力値 I，縦軸にリアプノフ指数を表わす． 分岐図で点の密度が高くなっている部分で，リアプノフ指数が正の値の領域では，カオス応答していると示唆される．

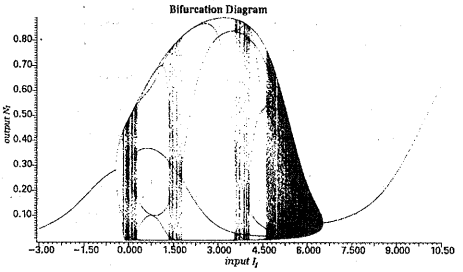

図 2.4　分岐図

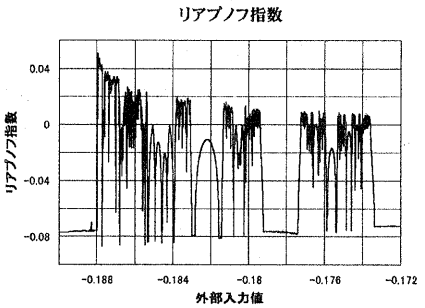

図 2.5　リアプノフ指数

2.3　CNN Cipher

本節では，CNN Cipher の構成法を示す．CNN Cipher は，暗号化鍵と復号鍵が同一で，平文メッセージユニットを一文字ずつ暗号化する逐次型慣用暗号系である[13),14)]．

本暗号系の概要を図 2.6 と式 (2.4), 式 (2.5) に示す．ここで，平文集合を **P**，暗号文集合を **C**，鍵集合を **K**，CNN のニューロン m の出力時系列を $\mathbf{Y}_m$ とする．

$$\text{暗号化}：\mathbf{C}=\mathbf{P}\diamond\mathbf{Y}_m \cdots\cdots (2.4)$$

$$\text{復　号}：\mathbf{P}=\mathbf{C}\diamond\mathbf{Y}_m \cdots\cdots (2.5)$$

ここで ◇ は演算子であり，論理演算や算術演算等の操作を表わす．

CNN cipher の特徴を図 2.7 に示す[13),14)]．本暗号系の安全性は，暗号化関数として用いた CNN の性質による．よって，CNN の出力するカオスの性質について次節で議論する．

3．CNN の出力するカオスの性質

3.1　実験で用いた概念

カオスを用いた暗号系はすでにいくつか提案されている[15)~17)]．これらは CNN Cipher と同様，

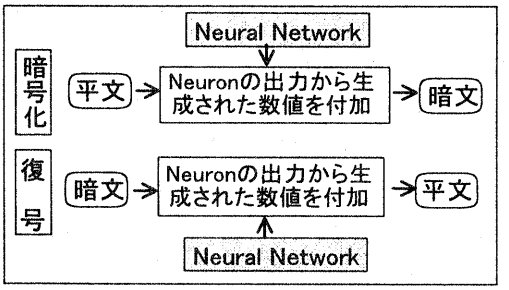

図 2.6　CNN Cipher の概念図

CNN Cipher の性質
- 特異なカオスを用いている
- 一方向性関数とハッシュ関数を構築できる
- 計算機環境に依存する

（ここで計算機環境とは，CPU の種類, OS, 計算精度, プログラムの実装方法 を指す）

図 2.7　CNN Cipher の特徴

暗号化関数にカオス写像を利用するものである．しかし，文献 15), 16) は区分線形性を持つカオス写像（テント写像など）をそのまま用いており，差分解読法などで容易に解読される．また，非線形写像を用いた場合の安全性は明らかにされていない．

本節では，暗号化関数として用いている CNN の出力するカオスの特性を明らかにするために，表 3.1 にあげるカオス系との比較実験を，表 3.2 に示す項目に対して行った．

はじめに，比較対象として用いたカオス系について述べる（表 3.1 参照）．

・ロジスティック写像 (Logistic)

一次元カオスの古典的モデルである May の

表 3.1　比較したカオス系

記号	名称
Logistic	ロジスティック写像
ChaoticNN	カオスニューロン
CNN	CNN

表 3.2　比較項目

記号	検討項目
exp-1	エントロピー型カオス尺度
exp-2	出力値の一致頻度

モデル[18),19)]を用いた．これは，次式で示すようなロジスティック写像によって表わされる．

$$f_a(x(t)) = ax(t-1)(1-x(t-1)) \cdots (3.1)$$
$$x(t) \in [0,1], 0 \le a \le 4$$

・カオスニューロン (ChaoticNN)

不応性を有するような生物のニューロンを模擬したモデルであり．合原らによって提案された[20),21)]．本稿で用いたモデルを次式に示す（南雲－佐藤のモデル）．ある時刻 t の出力 $x(t)$ は，式 (3.2) で表される．非線形関数 f は sigmoid 関数であり，$y(t)$ は内部状態を表わす．

$$y(t+1) = ky(t) - \alpha x(t) + a \cdots\cdots (3.2)$$
$$x(t+1) = f(y(t+1)) \cdots\cdots\cdots\cdots (3.3)$$

なお本稿では，α=1.0, k=0.5, λ=0.01 とした．a は外部入力値である．

・カオス・ニューラルネットワーク（CNN）

用いた CNN を式 (3.4), (3.5) に示す．

実験では，ニューロン 1 の出力値を対象とした．

・CNN-1: 3 個のニューロンより成る NN

$$W = \begin{bmatrix} 0 & 10 & 30 \\ -10 & 0 & 0 \\ 0 & -6 & 0 \end{bmatrix}, \quad \theta = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix} \cdots (3.4)$$

・CNN-2: 3 個のニューロンより成る NN

$$W = \begin{bmatrix} 0 & 10 & 25 \\ -10 & 0 & 0 \\ 0 & -7 & 0 \end{bmatrix}, \quad \theta = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix} \cdots (3.5)$$

次に，比較実験で用いた概念について述べる（表 3.2 参照）．

・エントロピー型カオス尺度（exp-1）

一般的に，系がカオス的であるかどうかを判断する指標としてはリアプノフ指数が用いられる．しかし，2次元以上の系の場合や実験による測定結果だけしか存在しない場合，リアプノフ指数を求めるのは困難である[21)~24)]．

そこで，リアプノフ指数と同様に系の状態を量的に計る指標として，エントロピー型カオス尺度 (以下，CD) を用いた．これは，大矢らが情報力学の視点から新たに導入した指標であり，状態の複雑さを表わし，カオスの強さを統一的な尺度で計ることができる[22)~24)]．本稿で用いたカオス尺度の計算条件を表 3.3 に示す．制御変数を変えながら計算を行い，その最大値で比較を行った．

表 3.3　カオス尺度の計算条件

区間 [0,1] の分割数	1,000
アイドリング回数	100,000
写像ステップ回数	1,000,000

表 3.4　出力値の一致の比較条件

アイドリング回数	100,000
保持した出力値の回数	10,000
比較回数	1,000,000,000

・出力値の一致頻度（exp-2）

決定論的カオスでは，ある時刻の出力値 $\xi(t_1)$ と，別の時刻の値 $\xi(t_2)$ が，

$$\xi(t_1) \neq \xi(t_2) \cdots\cdots\cdots\cdots (3.6)$$

となることが知られている[19)~21)]．

計算機でカオス力学系を計算した場合，計算機の計算精度（演算に用いるビット数や丸め誤差）等による影響を受ける．そのため，観測される性質は実システムとは大きく異なると考えられる．計算機の数値表現は有限ビット長であるため真のカオスとはいえず，表現ビット数を最大周期とする非常に長い周期をもっていると考えられる[21),25)]．

出力値の一致が生じるか，表 3.4 にしめす条件で実験を行った．アイドリング回数後，出力値をサンプリングし(保持した出力値の回数)，それらの値を比較回数分の出力と比較した．一致回数が 10,000 回を越えた時点で計算をうち切った．外部入力値は，エントロピー型カオス尺度が最大となる値を用いた．これを CD_{max} と表記する．

なお，CNN では，ニューロン N_1 の出力とネットワーク全体の出力をベクトルと見なした場合で実験を行った．

計算機実験で用いた計算機環境を，次頁表 3.5 に示す．

表 3.5　実験に用いた計算機環境 ※

計算機	VT-600 (CPU:Alpha 21164A)
OS	Red Hat Linux 5.2
C コンパイラ	Compaq C Compiler (ccc)
変数の型	double 型 (64bit浮動小数点型)

※: RSP10(補)岩手-58,RSP10(補)岩手-59「ネットワーク暗号化・復号装置」で購入した機器を用いた.

表 3.6　exp-1 : エントロピー型カオス尺度

	Logistic	Chaotic NN	CNN CNN-1	CNN-2
e.inp	4.000	0.738	2.004	1.424
CD_{max}	1.504	3.621	3.916	4.032

CD_{max} : エントロピー型カオス尺度の最大値,
e.inp : CD_{max} のときの外部入力値

表 3.7　exp-2 :出力値の一致頻度
尚, CNN は単一ニューロンの出力値で比較した.

	Logistic	Chaotic NN	CNN CNN-1	CNN-2
一致回数	0	10000*	2	0

*: 繰返し回数が 10810762 回で一致が10000 回(上限)に達した.

3.2　実験結果と考察

exp-1の結果を表 3.6 , exp-2 の結果を表 3.7 に示す.

exp-1 より, 比較に用いた系のカオスの強さと, 情報量的な複雑さが読みとれる. CD 値が Logistic で 1.5, ChaoticNN で 3.6 であるのに対し, CNN は 4.0 程度であり, いずれの系よりも情報量的に複雑であるといえる.

exp-2 の結果より, CNN-1 は 2 回一致が観測され, ChaoticNN は非常に一致が発生しやすいことが分かる. これに対し, CNN-2 と Logistic は一致する場合は全く観測されなかった. さらに, CNN-1 について, 単一ニューロンではなく, NN を構成する全てのニューロンの出力値をベクトルと見なして比較した場合, ベクトルが一致する場合は見られなかった. ゆえに, 単一ニューロンの出力値は 一対多写像であるといえる.

これらより, CNN の出力するカオスは, CD 値が他のカオス系に比べて非常に大きく, 情報量的に強いカオスであると示唆される. 更に, 出力値の一致も 0 回と 2 回であり, 出力ベクトル単位では一致が発生しないことから, 比較したカオス系よりも状態の表現空間が広い特異なカオスであると考えられる.

4. CNN Cipher の安全性評価

本節では, CNN Cipher の安全性評価を試みる. はじめに, CNN Cipher で基礎理論として用いている CNN の性質を, 暗号学的側面から検討する. 次に, CNN を疑似乱数と見なした場合の, CNN Cipher の計算量的安全性について考察する.

4.1　CNN の性質

筆者らは文献 13), 14) で, CNN Cipher の満たす性質について議論している. その中から重要なものをi), ii) にあげる.

i). 一方向性関数

CNN への外部入力値 I を x, あるニューロンの出力値を y とし, x と y の関係式 $y=f(x)$ を考える. このとき, f は一方向性関数である.

ii). ハッシュ関数

CNN の遷移回数を x, そのときのあるニューロンの出力値を y とし, x と y の関係式 $y=f(x)$ を考える. このとき, f はハッシュ関数 h である.

i), ii) より, CNN は一方向性ハッシュ関数を構成できる[13].

4.2　CNN Cipher の計算量的安全性

暗号系の計算量的安全性は, 暗号化関数が元としている数学的問題の困難性に依存している[3)~5)]. この場合, 数学的問題が以下の特徴を持てば安全であろうといわれている[1)~3)].

a. 系はある数学的問題を解かなければ破られない.

b. ある条件を満たす場合, この数学的問題を比較的短い時間で解くアルゴリズムが存在しない.

CNN Cipher について考えてみると,

・暗号化に使用した CNN と同様の系を用い

ない限り，暗号を解読できない．

・カオスの予測の困難性および計算機能力の現状から，適切に選択されたCNNの出力するカオスを再現する事は非常に困難である．

といえる．適切に選択されたCNNと同様のカオスを取り出すことは非常に困難であり，また，カオスの長期間予測は非常に困難であることから，CNNを共有するもの以外，本暗号系を破ることはできないと考えられる．(付録参照)

他方，一方向性関数から暗号学的に安全な疑似乱数が構築できることが示されている[1)~3)]．CNNを用いて一方向性関数が構築できることから，CNNは疑似乱数生成器と見なせる．よってCNN Cipherは，暗号化に乱数列を付加させる暗号であると考えられ，計算量的にワンタイムパッド暗号と同程度の安全性があると考えられる．

5. まとめ

カオス・ニューラルネットワークを用いた暗号系について，CNN Cipherの基礎原理であるCNNの性質を，他のカオス系との比較により明らかにした．この結果，CNNは，情報量的に複雑なカオスであることを明らかにした．

さらに，CNNの性質から，CNN Cipherの計算量的安全性について，予備的考察を行った．

今後の課題は，CNNの出力値の統計的解析と，CNN Cipherのより詳細な安全性評価を行うことである．

謝辞 本研究は，RSP10(補)岩手-58,RSP10(補)岩手-59「ネットワーク暗号化・復号装置」を用いた．

参考文献

1). 岡本龍明, 山本博資, 現代暗号, 産業図書, 1997.
2). N. コブリッツ著, 林彬訳, 暗号の代数理論, シュプリンガーフェアラーク東京, 1999.
3). 岡本栄司, 暗号理論入門, 共立出版, 1993.
4). 吉田等明, 三浦守, "多様な周期で振動するニューラル・ネットワーク", 計測自動制御学会東北支部30周年記念学術講演会, pp.53--58, 1994.
5). H. Yoshida and M. Miura, "Chirality in Neural Network System", Proc. of APCCAS '94, 4A.1, pp3-7, 1994.
6). 吉田等明, 三浦守, "ニューラルネットワークにおけるキラリティ 振動周期の教師無し学習", 平6東北連大, 2F1, 1994.
7). 米城健二, 吉田等明, 三浦守, "人工ニューラルネットワークにおける振動発生機構", 計測自動制御学会東北支部第153回研究集会, 153, pp.1/3-7/3, 1995.
8). 米城健二, 吉田等明, 三浦守, "人工ニューロンの組み合わせによるカオスの発生", 平7東北連大, 1E15, pp.181, 1995.
9). 米城健二, 吉田等明, 恒川佳隆, 三浦守, "ニューラルネットワークにおける振動, 準周期振動, カオス", 第18回情報理論とその応用シンポジウム E-7-3, pp.735-738, 1995.
10). Hitoaki Yoshida, Kenji Yoneki, Yoshitaka Tsunekawa and Mamoru Miura, "Chaos Neural Network", Proc. of ISPACS'96, vol.1of3, pp.16.1.1-16.1.5, 1996.
11). 吉田等明, 川村暁, 恒川佳隆, 三浦守, "ニューロン3個から成るネットワークの振動現象", 計測自動制御学会東北支部 第174回研究集会 174-9, pp1/9-9/9, 1998.
12). 川村暁, 吉田等明, 恒川佳隆, 三浦守,"カオス・ニューラルネットワークの最小構成", 信学技報 NC98-107, pp.67-74, 1999.
13). 川村暁, 吉田等明, 高橋友樹, 恒川佳隆, 三浦守,"カオス・ニューラルネットワークを用いた暗号化の一方式", 計測自動制御学会東北支部第181回研究集会 181-2, pp1/10-10/10, 1999.
14). 川村暁, 池田直弥, 吉田等明, 三浦守, "カオス・ニューラルネットワークを用いた暗号プロトコル ー相手認証への適用ー", 計測自動制御学会東北支部 第187回研究集会, pp1/7-7/7, 2000.
15). T. Habutsu, Y. Nishio, I. Sasase and S. Mori, "A Secret key cryptosystem by iterating chaotic map", Proc. Eurocrypt '91, pp.127-140, 1991.
16). 枝池雅文,上田哲史, 西尾芳文, "カオス的二次元写像を用いた暗号系の電子メイルへの応用", 信学技報, NLP96-19, 1996.
17). 増田直紀, 合原一幸, "有限状態パイコネ変換を用いたカオス暗号",信学論(A), vol.J82-A, no.7, pp.1038-1046,1999
18). R. R. May,"Simple mathematical models with very complicated dynamics", Nature, vol.261, pp.459-467, 1976.
19). Robert. L. Devaney, 上江洲達也ら著, カオス力学系の基礎, アジソン・ウェスレイ, 1997.
20). K. Aihara et al., "Chaotic Neural Networks", phyics letters A, vol.144, number 6,7, 1990.
21). 合原一幸 著, "カオスの数理と技術ーカオス, フラクタル, 複雑系への序章ー", 放送大学, 1997.
22). Masanori OHYA, "Information Dynamics and Its Applications to Optical Communication Processes", Lecture Notes in Physics, vol.378, pp.81-92, Springer, 1991.
23). 大矢雅則, 小坂稔, "情報力学によるカオス現象の考察", 信学論 (A), vol.J80-A, no.152, pp.2138-2144, 1997.
24). 田仲康匡, 井上啓, 大矢雅則, "池田写像のエントロピー型カオス尺度を用いた特徴づけ", 信学技報, IT99-24, pp.55-60, 1999.
25). 合原幸一編, "カオスセミナー", 海文堂, 1994.
26). 鈴木正信, ケビン ジュッド, 合原一幸, 小谷誠, "x動径基底関数ネットワークを用いたロジスティック写像の近似", 信学論 (A), vol.J76-A, no.8, pp.1177-1184, 1993.
27). 増田直紀, 合原一幸, "ウェーブレット係数列を用いたカオス時系列の予測", 信学論 (A) , vol.J82-A, pp.1710-1718, 1999.
28). 吉田和子, 石井信, 佐藤雍昭, "オンライン EM アルゴリズムによるカオス力学系の学習と耐ノイズ性", 信学論 (A), vol.J83-A, no.1, pp.28-37, 2000.
29). 村尾健次, 大洲紀道, 秋田大介, "動径基底関数モデルを用いたカオスの時系列解析", 信学技報, CAS96-11, pp.69-76, 1996.
30). 湊谷敏之, 大洞喜正, "カオスニューラルネットワークの統計的性質",信学技報, NC97-39, pp.31-36, 1997.

付録：カオス時系列の予測（近似）

カオス時系列信号の予測は，非線形関数近似の応用問題としてとらえられる．すなわち，現象が決定論的カオスである場合，カオス時系列を生成している非線形力学系を近似することにより，その系の将来の予測が可能となるためである．このような短期予測手法としては，区分線形近似による方法[21)]，動径基底関数を用いる方法[26)]，ウェーブレット変換を用いる方法[27)]や正規化ガウス関数ネットワークを用いる方法[28)]などが提案されている．しかし，十分長期の予測はできず，最長でも30タイムステップ程度までの短期予測にとどまっている．他方，時系列そのものではなく，カオス写像の統計量や確率分布を近似するという研究[29),30)]が行われている．この場合，時系列を直接予測するのではなく，その構造を近似する．

このようにカオス時系列の予測は，ごく短いオーダーでは可能であるが，長期予測は難しいといえる．□