カオスからの擬似乱数生成とその応用に関する研究

石巻専修大学 理工学部 情報電子工学科
川村　暁

1　はじめに

擬似乱数は，コンピュータシミュレーションや情報セキュリティ分野（暗号鍵の生成，番号の生成，one-time pad 暗号における使い捨て乱数等）における重要な要素技術である．計算機用擬似乱数生成法としては，簡単な数論に基づく，漸化式を用いた方法（線形合同法が有名）が用いられている．この手法から生成された擬似乱数は，比較的簡単な漸化式より擬似乱数を生成するため計算機実装には向く方法であるが，乱数性がよくないこと，乱数列の予測が可能なことが知られている [1, 2, 3, 4]．特に情報セキュリティ分野で用いる擬似乱数については，乱数列の性質がよいことと乱数列の予測困難性が重要であると指摘されている [3, 5, 6, 7]．

本稿では，新規な乱数生成法として，乱数性・予測不可能性に優れたカオスを用いた手法について述べる．カオスからの擬似乱数生成法はこれまでにも幾つか提案されているが，何れも乱数性が十分ではない [8, 9, 10, 11]．これに対し，特定の構造を持った，カオス応答する人工ニューラルネットワークを用いることにより，乱数性および予測不可能性に優れた擬似乱数を生成できることを明らかとした．この研究を通じて，カオスが良質な擬似乱数生成源として適応する場合があることを明らかにした．また本乱数生成器から生成された良質な乱数の応用として，one-time pad 暗号へ適応した例を示す．

2　カオス

カオスとは，微分または差分方程式で記述される系で，解の振る舞いが予測不可能な，複雑・不規則なふるまいを示す現象である．ある系がカオスである場合，以下の性質を示すことが知られている [12, 13, 14]．

- 単純な数式から生成された数列が，ランダムに見える複雑な振る舞いを示す．
- 初期値のごくわずかな差が，時間発展に甚大な差を生み出す，初期値鋭敏性がある．
- 過去の観測データから，時系列の短期予測は可能であるが，長期予測が困難である．
- カオス特有のアトラクタはストレンジアトラクタと呼ばれる特異なものであり，自己相似構造を含む場合が多い．

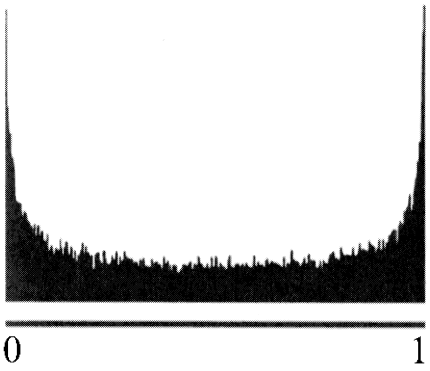

図 1: ロジスティック写像の出力値の頻度分布．

カオス時系列信号は，カオス特有のエルゴード性および軌道の稠密性により，同一の値を取らないことが知られている．また，カオス特有のストレンジアトラクタを持つことから，出力時系列の出力頻度の分布は，特徴的な分布を示す [12, 13, 14]，このため，カオス時系列信号をそのまま乱数とした場合，得られた乱数列にカオス特有の偏りが生じることが知られている [8, 6, 12]．

例として，ロジスティック写像の出力値の頻度分布を 1 に示す．

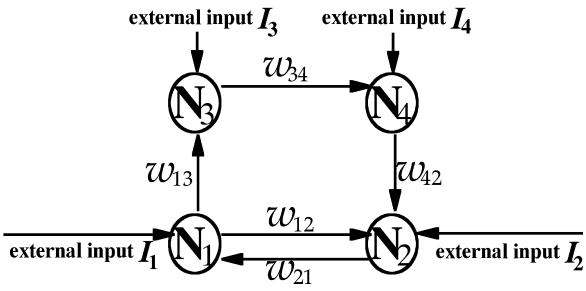

図 2: 4 つのニューロンからなるニューラルネットワーク．この構造のネットワークでカオス応答する系が存在し，CNN と定義している [17]

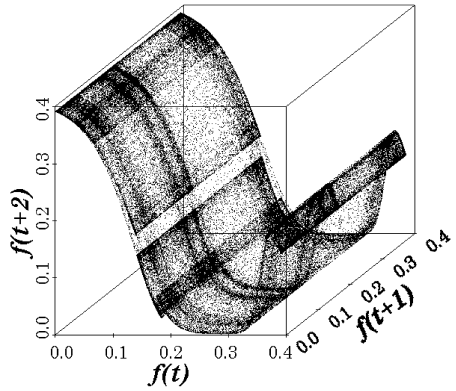

図 3: CNN のアトラクタの例．時間遅れ座標系に再構成して得られた．自己再帰（フラクタル）的な構造があることがわかる．

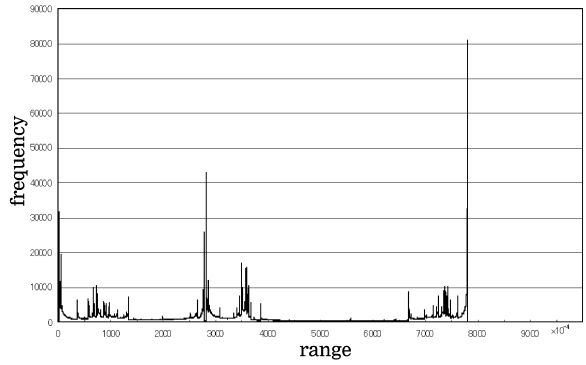

図 4: CNN の出力値の頻度分布．y 軸は出力頻度の対数表示である．カオス特有の複雑な頻度分布となっている．

3　カオス・ニューラルネットワーク（CNN）

（人工）ニューラルネットワークとは，生物の神経回路網を計算機上に模した情報処理手法のことである．生物は，外部の情報にあわせて学習を行うことができる．生物の学習機構にヒントを得て，計算機上で学習を行う手法として考えられた．通常のアルゴリズムでは記述が難しい問題や，因果関係が陽に記述できない問題などに適応される．

生物の神経回路網において，複数のニューロン群で振動現象が観測されている [15, 16]．たとえば，心臓の拍動，大脳における種々のパルス応答（脳波）などである．生物でみられる振動現象は，周期運動だけではなく，非周期的なものや，カオス的な応答をすることが知られている [15, 16]．

生物の神経回路網をモデル化した（人工）ニューラルネットワークに基本的な性質を研究した結果，周期運動，準周期運動，カオス応答をする場合があることを明らかにしている [17, 18, 19, 20, 21, 22]．とくに文献 [17] において，(人工）ニューラルネットワークにおいて一般的に用いられるモデルを用いた場合，ニューロン数 3 個でカオス応答する場合があり，これが，カオス応答する最小構成であることを明らかにしている [17]．一般的なニューロンモデルから成るニューラルネットワークがカオス応答するものを，カオス・ニューラルネットワーク（CNN）と定義している [17, 18, 19, 20, 21, 22]．

図 2[18] に，4 個のニューロンから成る CNN を示す．以後 CNN とは，この構成のことを指す．

4　カオスからの乱数生成

カオスを乱数源として用いる研究がいくつか行われている．しかし，これまでの研究では，乱数性・高速性に優れた乱数生成器の実現例は報告されていない．

そこで本稿では，カオス写像の出力値のうち微小桁部分に着目し，これを取り出し乱数とする方法を用いる 5．カオス時系列信号の微小桁部分は，カオス軌道がストレンジアトラクタ上を遍歴しながらも同一の値を取らない [12, 13, 14] ことから，異なった値が得られると考えられるためである．

乱数の初期値としては，カオス写像の初期値を用い

た．カオス写像は，特有の特有のストレンジアトラクタを持つことからもわかるとおり，ある特定の範囲内の運動である [12, 13, 14]．しかし，カオス特有のエルゴード性および軌道の稠密性により，同一の値を取らないことから，カオス写像の初期値を乱数の種（seed）として用いる事ができると考えた．すなわち，異なる初期値から発展した時系列は他の時系列とは異なっていると考えられる．

5　生成された乱数の性質

前章で記した手法を用いて，複数のカオス写像を用いて乱数生成器を構成した．表**??**に，構成した乱数生成器を示す．

これらの乱数生成器の乱数性を明らかにするために，統計的な検定により乱数性の検定を行った．統計的な検定を用いる場合，どの検定に合格すれば乱数性が十分かという基準は存在しない．しかし，文献 [1, 2, 3, 4, 27, 28] では，できるだけ検定に合格した方がよいと指摘されている．本稿でもこの立場を取り研究を進めた結果，CNN から乱数を生成した場合，もっとも乱数性に優れた乱数を生成できることを明らかとしている [18, 19, 20, 21, 22]．

本稿ではこのうち，最も基本的な一様性の検定を行った結果を，図 6 および図 7 に示す．実験結果は，カオス写像の初期値 $(0, 1)$ の空間を一万等分して乱数の種（seed）として乱数を生成し，それぞれの乱数列が一様性の仮定を満足するか検定を行っている．一養成の検定には，統計パッケージ R[26] を用いた．図では，検定により，一様乱数ではないと棄却された乱数列の割合で示している．実験結果より，CNN から生成された乱数は，ほかの系列に比べ，乱数性に優れていることが示唆された．

なお，一様性の検定結果からは，従来法である rand, random，mrand48 の乱数性も良好であるように見えるが，より詳細な diehard 検定 [27, 28] を用いた場合，CNN PRNG よりも乱数性が劣ることを明らかとしている．

このように，カオスを用いた擬似乱数生成器において，仮数部の下位ビット側を乱数にするという比較的簡単な方法で乱数を生成しても，用いた写像によっては，乱数性に優れた擬似乱数列が生成できることを明

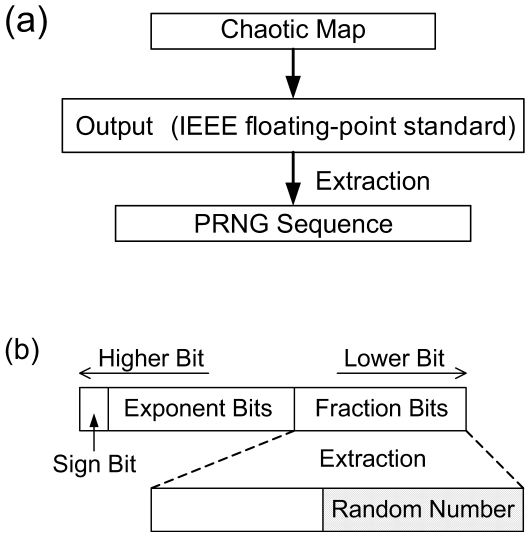

図 5: カオス写像からの乱数生成方法．
(a) カオス時系列信号は IEEE 754 準拠の浮動小数点数で表現されている．この数から乱数を取り出す．
(b) カオス出力からの擬似乱数の取り出し方法．仮数部下位ビット側を乱数として取り出す．

乱数生成器	概要
CNN PRNG	4 つのニューロンから成るカオス・ニューラルネットワークを用いた擬似乱数生成器（提案法）
LM PRNG	ロジスティック写像を用いた擬似乱数生成器
Henon PRNG	ヘノン写像を用いた擬似乱数生成器
2-map PRNG	二次写像を用いた擬似乱数生成器
rand	C 言語 rand 関数
mrand48	C 言語 mrand48 関数
random	C 言語 random 関数

表 1: 構成した擬似乱数生成器（PRNG）．

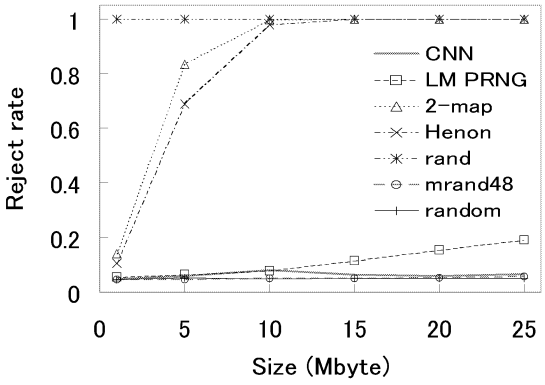

図 6: 一様性の検定結果．検定は 4 bit 単位で行った．CNN PRNG だけが，乱数性がよい（棄却された系列の数が少ない）ことがわかる．

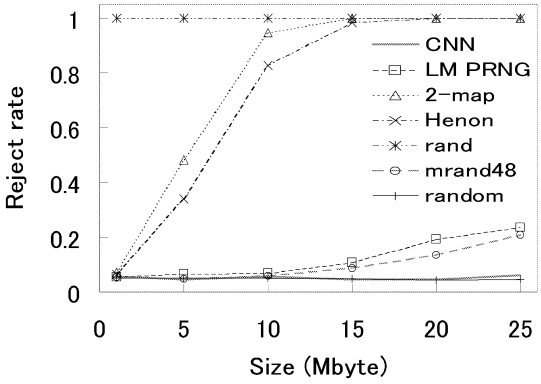

図 7: 一様性の検定結果．検定は 8 bit 単位で行った．CNN PRNG だけが，乱数性がよい（棄却された系列の数が少ない）ことがわかる．

らかとした．

6　暗号系への応用

暗号は，大きく 2 種類に分類される [5, 6, 7]．暗号化と復号を同一の鍵（共通鍵）で行う共通鍵暗号と，暗号化と復号に異なる鍵を用いる公開鍵暗号である．共通鍵暗号は，暗号強度が高く処理速度も高速であるという特徴を持つが，通信者間で鍵配信の問題を解決しなければならない．これに対し公開鍵暗号では，暗号化鍵と復号鍵は別のものを用いるため，鍵配送を行う

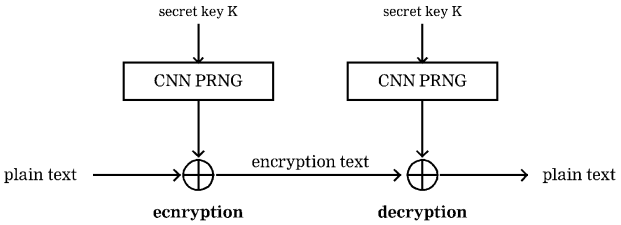

図 8: CNN から生成された乱数を用いた暗号系の例．CNN より乱数を生成し，乱数は使い捨てにする．暗号鍵は，CNN の設定をあてる．

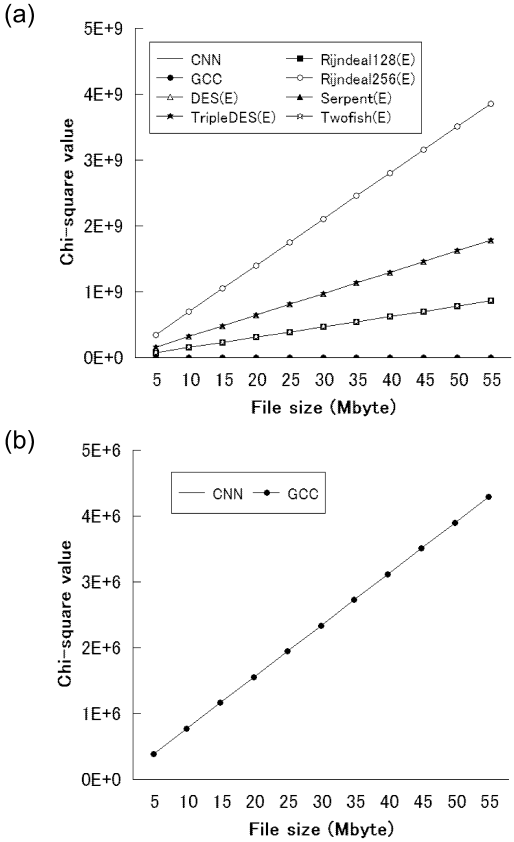

図 9: 暗号強度評価の例．x 軸は暗号化対象のファイルサイズ，y 軸は χ 二乗値を示した．ファイルはすべて 0 から成る．

(a) いろいろな暗号系の χ 二乗検定の結果．CNN Cipher 以外は，χ 二乗値が単調に増加している．(b) CNN Cipher と GCC カオス暗号の χ 二乗値の比較，GCC カオス暗号も，χ 二乗値が単調に増加している．

ことができる（暗号化鍵から復号鍵は推測できない）．

共通鍵暗号は，さらにいくつかに分類できる．暗号の処理をある決まったブロックごとに行うブロック暗号，乱数などを付加することにより実現されるストリーム暗号，特殊な辞書を用いて暗号化を行う方式（辞書により，文字例の置換などを行う方式）である．このうちストリーム暗号は，暗号化処理を逐次的に行うことができる利点があるが，乱数の性質が安全性（暗号強度）を左右する．特にこの方式では，乱数を使い捨てにし，その乱数が自然乱数であれば，絶対に解読されない，one time-pad 暗号が構成できることが知られている [6, 7]．すなわち，予測が困難な乱数を用いた場合，非常に暗号強度の高いストリーム暗号が生成できると考えられる [18, 21, 23, 24, 25]．

カオスは，比較的簡単な漸化式が複雑な振る舞いを示す現象である．カオスの重要な性質として，初期値鋭敏性と長期予測不可能性がある [12, 13, 14]．これらの性質から，生成された乱数列の乱数性が良質であれば，ストリーム暗号が構成できると考えられる．

そこで，カオスを用いた擬似乱数生成器の中でもっとも乱数性に優れた CNN を用いた乱数生成器を，ストリーム暗号に適応することを考えた．図 8 に，CNN によりストリーム暗号を構成した構成を示す．秘密鍵としては，CNN の構成と初期条件をあて，乱数列は使い捨てにする．この暗号系を CNN Cipher とする [18, 21, 23, 24, 25]．

CNN Cipher の安全性は，乱数生成源である CNN PRNG の，乱数性が良質であるかどうかにかかっている．すなわち，乱数性が良質でない場合，乱数系列や CNN の構造を推定される危険性が増大するためである．

CNN Cipher と一般的に用いられているいくつかの暗号系の，暗号文に基づいた強度比較結果を，図 5[18] に示す．強度比較法として，暗号文の偏りに基づく，累加 χ 二乗の法則に基づいた手法を用いた [23, 24, 29]．暗号文の偏りが大きいとは，暗号系に関する情報をより得やすいことを表しており，暗号系としてはふさわしくない．これに対して本法則が成立せず，χ 二乗値が増加しない場合，その暗号系の強度は高いと示唆される [23, 29]．

実験結果より，CNN Cipher は，累加 χ 二乗の法則が成立しておらず，暗号文から情報が得にくい暗号系であると示唆される．これに対してほかの暗号系では，暗号文の偏りがそれぞれの方式により特定の値をとるため，暗号文に関する統計処理を用いて暗号系を解読される可能性が示唆される．

なお，これらの乱数生成器および暗号システムについては，研究だけではなく，権利化についても JST 等の支援を得ながら進めている [24, 25]．また，実用化については，JST・岩手県などの支援を得ながら，企業 ((株) アドテックシステムサイエンス，(株) 大井電気) と共同で製品開発について検討している，

7　まとめと今後の課題

カオスを擬似乱数生成に用いる手法について検討した．特異なカオス系であるカオス・ニューラルネットワーク（CNN）を用いた場合に，乱数性および予測不可能性に優れた乱数を生成できることを明らかとした．また，この乱数生成器の応用例として，乱数性および予測不可能性に優れた乱数が必要である，one-time pad 暗号へ適応した場合を示した．本暗号系については，実用化についての検討例を示した．

今後も，岩手大学および複数の企業と共同で研究開発を通じて，実用化の進展等を推進する予定である．

参考文献

[1] 伏見政則, 乱数, 東京大学出版会, 1989.

[2] 宮武修, 脇本和昌 , 乱数とモンテカルロ法, 森北出版, 1978.

[3] D. E. Knuth 著, 渋谷政昭 訳, 準数値算法／乱数, サイエンス社, 1981.

[4] P. L'Ecuyer, Uniform Random Number Generator, Annals. of Operations Research, Vol.53, pp.77-120, 1994.

[5] 情報処理とその応用学会編, 暗号と認証, 培風館, 1996.

[6] 岡本 龍明, 山本 博資，現代暗号，産業図書，1997.

[7] Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, ohn Wiley & Sons Inc (Computers), 1995.

[8] 香田徹, 柿元厚志, 擬似乱数とカオス, 情報処理学会論文誌, Vol.27, No.3, pp289-296, 1986.

[9] 渡辺裕明, 金田康正, ロジスティック写像による擬似乱数生成法, 第 53 回情報処理学会全国大会論文集, Vol.1, pp.65-p66, 1996.

[10] 渡辺裕明, 金田康正, テント写像に基づいた擬似乱数生成法, 情報処理学会論文誌，Vol.40, No.7, pp.2843-2850, 1999.

[11] Haojiang Gao, Yisheng Zhang, Shuyun Liang, Dequn Li, A new chaotic algorithm for image encryption, Chaos, Solitons and Fractals, vol. 29, pp.393-399, 2006.

[12] 香田 徹，離散力学系のカオス，コロナ社，1998.

[13] 下條隆嗣，カオス力学入門, 近代科学社，1992.

[14] Mario Martelli, Discrete Dynamical Systems and Chaos, ongman Pub Group, 1993.

[15] R. Beale, T. Jackson, Neural Computing: An Introduction, Inst of Physics Inc, 1990.

[16] Judith E. Dayhoff , Neural Network Architectures: An Introduction, Van Nostrand Reinhold, 1989.

[17] 川村暁, 吉田等明, 三浦守 (2001) 通常のニューロンより成るカオス・ニューラルネットワークの最小構成, 信学論 (A), Vol.J84-A, No.5, pp.586-594

[18] Satoshi Kawamura at el., Implementation of Uniform Pseudo Random Number Generator and Application to Stream Cipher based on Chaos Neural Network, Proc. of the International Conference on Fundamentals of Electronics, Communications and Computer Sciences, R-18, pp.4-9, 2002.

[19] 川村　暁，吉田等明，三浦　守，カオス写像を用いた擬似乱数生成の試み，計測自動制御学会システム・情報部門学術講演会論文集，2C1-3，pp.343 -348，2003.

[20] 秋山真一，川村　暁，三浦　守，カオスに基づく擬似乱数生成器　～ リアプノフ指数と乱数性の関連について ～，電子情報通信学会技術研究報告, NLP2005-32, pp.23-26, 2005.

[21] 佐々木慶文，川村　暁，青木孝文，伊藤貴康，組込み機器を用いたコンパクトクラスタ計算機の開発と暗号処理への応用，情報処理学会研究報告，2004-DSM-35, pp.71-76, 2004.

[22] Satoshi Kawamura at el., Property of Random Series from Chaos Neural Network, Proc. of the 2006 Intl. Symposium on Nonlinear Theory and its Applications (NOLTA2006), pp.99-102, 2006.

[23] 川村　暁，吉田等明，三浦　守，カオスを用いた暗号系の暗号強度評価，石巻専修大学研究紀要 第１４号， pp.1-11, 2003.

[24] 吉田等明，川村　暁，西村聡，三浦　守，カオス・ニューラルネットワークを用いた乱数生成システム，特開 2003 － 76272, 2003.

[25] 吉田等明，川村　暁，三浦　守，カオス・ニューラルネットワークを用いた暗号化システム及び復号システム，特開 2006 － 259775，2006.

[26] Brian D. Ripley, The R project in statistical computing. MSOR Connections. The newsletter of the LTSN Maths, Stats and OR Network, 1(1), pp.23-25, 2001.

[27] G. Marsaglia and A. Zaman, Monkey tests for random number generators, Computers and Mathematics with Applications, Part A, Vol.26, No.9, pp.1?10, 1993.

[28] B. Narasimhan, JDiehard: An implementation of Diehard in Java, Proc. of the 2nd International Workshop on Distributed Statistical Computing, 2001.

[29] 加藤正隆，基礎暗号学 II －情報セキュリティのためにー，サイエンス社，1989.