計測自動制御学会東北支部 第 187 回研究集会(2000,6,2)
資料番号 187-1

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 ~相手認証への適用~

A Novel Authentication Method Based on Chaos Neural Network Cryptosystem

川村暁*，○池田直弥*，吉田等明**，三浦守*

Satoshi Kawamura*, ○Naoya Ikeda*, Hitoaki Yoshida**and Mamoru Miura*

*岩手大学工学部情報システム工学科
**岩手大学情報処理センター

*Department of Computer and Information Science, Faculty of Engineering, Iwate University
**Iwate University Computer Center

キーワード：カオス(chaos)，ニューラルネットワーク(neural network)
共通鍵暗号(conventional encryption)

連絡先：〒020-8551 盛岡市上田 4-3-5 岩手大学 工学部 情報システム工学科 三浦研究室
川村 暁，E-mail:kawamura@cis.iwate-u.ac.jp

1. はじめに

ネットワークシステムのオープン化・汎用化が，社会活動のあらゆる局面において中心的役割を担うようになった現在，機密情報転送や電子商取引（Electronic Commerce）のような分野では特に，セキュリティ確保が緊急の課題となっている．セキュリティ上の脅威としては，盗聴，なりすまし，改ざん・偽造，事実の否認など様々なものが考えられる．特に，情報通信において通信相手やメッセージが正当なものであるかを確認する技術，いわゆる認証技術が非常に重要である．

相手認証には利用者の秘密情報に基づくパスワード方式が主に用いられているが，この方法は容易に第三者がなりすましを行うことが可能であるため，相手認証法の，暗号技術を用いたプロトコルとしての研究が行われている [1〜3].

本論文では，認証の手順には従来法を使用し，パスワードを生成する関数に，我々が提案した新しい暗号系である，カオス・ニューラルネットワーク（CNN） [4]を用いることで，従来の認証方式より強固な認証方式を提案する．

本論文の構成を示す．第 2 章では，従来から用いられている認証法について考察し，第 3 章で, 提案法の基本原理である CNN とこれを用いた暗号系について解説する．第 4 章では，CNN を用いた認証法を提案する．第 5 章で，提案法の計算機実験結果を示す．第 6 章はむすびである．

2. 従来の暗号方式と認証法

2.1 従来の暗号方式

従来の暗号方式として，共通鍵暗号方式と公開鍵暗号方式，また従来法のパスワード生成関数として用いられてきた DES（Data Encryption Standard）をあげ，その特徴を記す．

2.1.1 共通鍵暗号方式

暗号化と複合に同一の鍵を用いる方式．計算量が少ない（高速である）という長所がある反面，通信経路毎に鍵が必要になるため，複数の相手と暗号通信を行う場合には膨大な数の鍵とその管理が必要になる．この代表例として DES（Data Encryption Standard）がある．

・DES（Data Encryption Standard）[1]

従来法のパスワード生成関数として用いられてきた DES は米国政府が公式に認定したブロック暗号化の基準で，対称型の共通鍵暗号方式をとり，アルゴリズムは公開されている．鍵長は 56bit（＋parity 8bit = 64bit）．

表 2.1　共通鍵暗号と公開鍵暗号の比較

	共通鍵暗号	公開鍵暗号
アルゴリズム	組合わせ論	整数論
鍵の秘密配送	×必要	○不要
秘密に保持すべき鍵	×通信相手毎に必要	○自分の秘密鍵のみ
電子署名	×困難	○可能
処理速度	○高速	×低速
公開鍵の管理	○不要	×必要
暗号通信による認証	○可能	×困難

2.1.2 公開鍵暗号方式

暗号化と複合に異なる鍵を用いる暗号である．いずれか一方の鍵から他方の鍵が容易に計算できないため，一方の鍵を公開することができるという特徴がある．他方は秘密に保持する．鍵の秘密配送が不要（相手の公開鍵を入手するだけでよい）という長所があるが，共通鍵暗号方式に比べて処理が低速という欠点もある．公開鍵暗号方式の安全性（公開鍵から秘密鍵を計算することの難しさ）は，素因数分解問題や離散対数問題といった数論に基づいている．

2.2 従来の認証法

従来の認証法として，使い捨てパスワード方式とチャレンジレスポンス方式を示す．これらを説明する前に，重要な基本的概念である，一方向性関数とハッシュ関数について，その特徴を記す．

2.2.1 一方向性関数

ある関数 $y=f(x)$が一方向性関数であるとは，x より $y=f(x)$を計算するのは容易であるが, 逆に y より x を求めるのが困難な関数のことをいう．

2.2.2 ハッシュ関数

一般的にハッシュ関数とは，ある大きな領域Dから小さな領域Rへの多対一のマッピングを行う関数hのことであり，

$$h：D \rightarrow R \text{ かつ } |D|>|R| \qquad (1)$$

となる場合を考える．このとき，関数hとその定義域のある値xが与えられて，$h(x)=h(y)$となるようなyを求めることが難しいような関数hのことである．

2.2.3 使い捨てパスワード方式

通信経路で転送されるパスワードが盗まれても安全である方式．パスワードは一度の使用しか認められない．この方法は以下の手順をとる．

一方向性関数をfとして，パスワードPW_iは次式で表される．

$$\begin{aligned} PW_1 &= f(r) \\ PW_2 &= f(PW_1) \\ PW_3 &= f(PW_2) \\ &\vdots \\ PW_{n-1} &= f(PW_{n-2}) \\ PW_n &= f(PW_{n-1}) \end{aligned} \qquad (2)$$

STEP 1 クライアントは，予め一方向性関数fよりn個の使い捨てパスワードを生成しておく．

STEP 2 クライアントは生成してあったパスワードのうち，未使用のパスワードをサーバに送る．

STEP 3 サーバは登録してあるrとパスワードの使用履歴より，パスワードが未使用で且つパスワード生成関数を満たすことを検証する．

2.2.4 チャレンジレスポンス方式

サーバとクライアントの間で，サーバがチャレンジコードを提示し，クライアントがこのコードに対応した応答を返すことでサーバがクライアントの検証を行う方式．この方法の手順を以下に示す．

STEP 1 サーバはチャレンジコードrを生成して，クライアントに通知する．

STEP 2 クライアントはrをハッシュ関数Hを用いて，ハッシュ化した結果$X = H(r)$をサーバに送る．

STEP 3 サーバはXが成り立つことを検査する．

この手順を繰り返すことにより，本人であるかどうか認証する．

3. カオス・ニューラルネットワーク

当研究室において，通常用いられている一般的なニューロンから構成されたネットワークがカオス応答をすることが観察されている[4,5]．

本研究で用いたニューロンモデルとカオス・ニューラルネットワークモデルを以下に示す[4,5]．

なお，カオスとは，決定論的システムが複雑な振る舞いをする現象である．

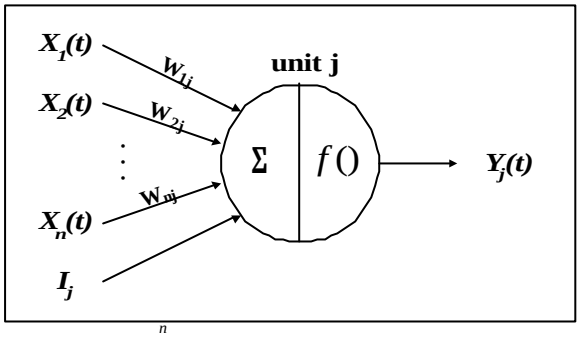
3.1 ニューロンモデル

CNNで用いるニューロンモデルは,通常用いられている一般的なニューロンを使用している．このモデルではニューロンの自己回帰結合がなく，非線形関数にはシグモイド関数を使用している．図3.1にそのニューロンモデルを示す．

3.2 ネットワークモデル

カオス・ニューラルネットワークの一例としてニューロンが3個の場合を示す．

図3.2にネットワークモデルを，図3.3に入出力特性図を，図3.4にリアプノフ指数を，示す．



$$u_j = \sum_{i=1}^{n} w_{ij} x_j(t) + q_j$$

$$f(u_j) = \frac{1}{1+\exp(-u_j / l)}$$

$Y_j(t)$：時刻 t におけるニューロン j の出力

$\mathbb{W}_{ij}$：ニューロン i から j への結合荷重

I_j：ニューロン j への外部入力値

λ：シグモイド関数の傾き係数

θ：ニューロン j のしきい値

図 3.1　ニューロンモデル

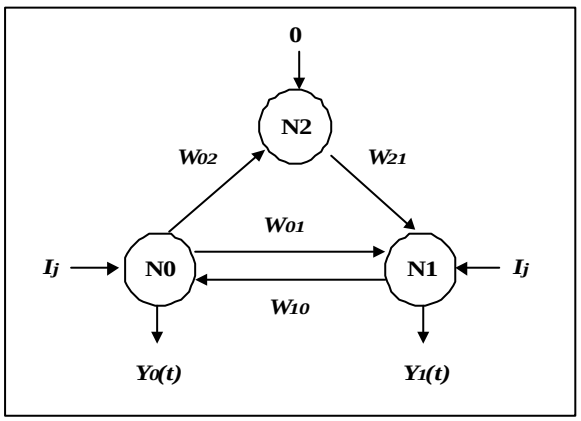


図 3.2　ネットワークモデル

入出力特性図で，点の密度が高い部分が見られる．この部分について考えてみると，図 3.4 より，リアプノフ指数の最大値は約 0.06582（外部入力値：1.24 近傍）である．ここでのポアンカレ切断面は折り畳み構造が見られ，自己相似（フラクタル）的な構造であることが示されており[4]，このネットワークはカオス応答をしている．

本提案では，このカオス・ニューラルネットワークを用いる．

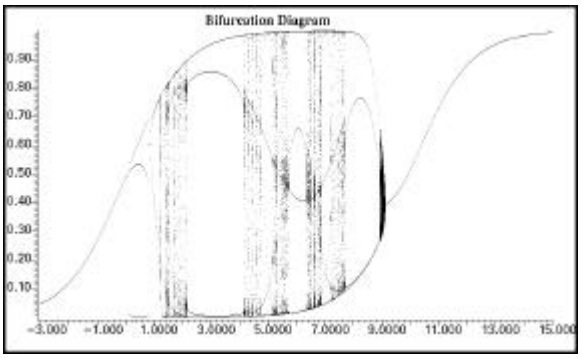


図 3.3　入出力特性図

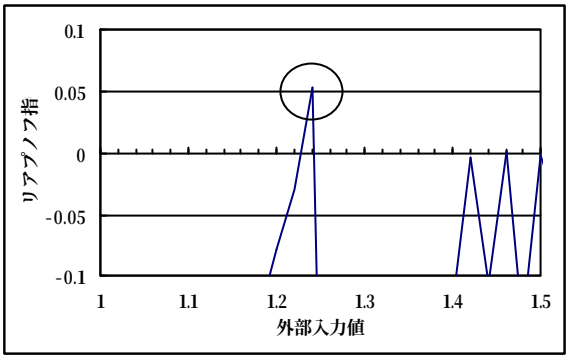


図 3.4　リアプノフ指数

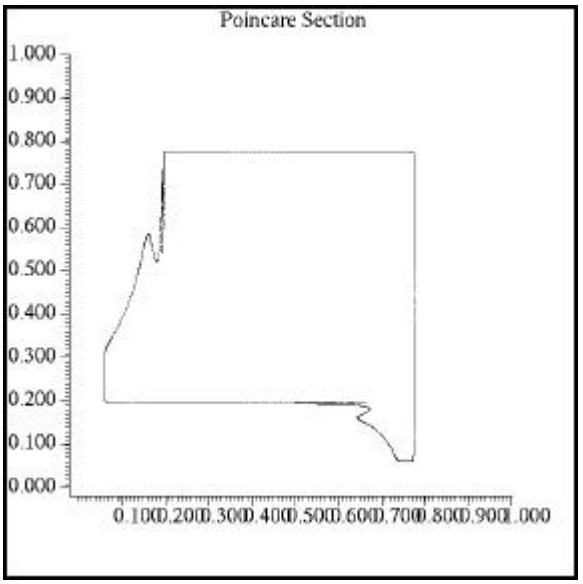


図 3.5　ポアンカレ切断面

4.　CNN を用いた暗号と相手認証

4.1　CNN を用いた暗号

前節では，CNN の信号特性について考察を加えた．本節では，この系の出力信号を暗号に用いる事を考える[4].

4.1.1　暗号方式

これまで公開されている暗号は，暗号の組立方法や鍵を公開するか否かにより，共通鍵暗号系と公開鍵暗号系に分類される．

共通鍵暗号系は，暗号化の基本構成単位をどのようなものにするかにより，サイファ方式とコード方式に分けられる．とくにサイファ方式とは，データの成分を原字単位または綴り字を基本単位として暗号化する方式であり，このときデータの文字列を一文字ずつ組み立てるものを逐次型暗号，数文字をまとめて暗号化するものをブロック暗号という．

CNN を用いた暗号では，暗号化鍵と複号鍵が同一で，一文字ずつ暗号化する逐次型共通鍵暗号系を構築する．

4.1.2　暗号化方式

本節では，カオス・ニューラルネットワークを用いた逐次型共通鍵暗号系の構築例を示す．図 4.1 に暗号化と複号の概念図を示す．

暗文生成は，暗号化しようとする平文一文字単位で行う．カオス時系列発生源として用いるカオス・ニューラルネットワークのあるニューロンの出力値から 1～n の正整数を生成する．この生成された整数を平文に付加することによって暗号化する．一文字暗号化するごとに，ネットワーク遷移を行う．

複号は，暗号化時に用いたカオス・ニューラルネットワークと同一の構成・条件のものをカオス時系列発生源として用いる．暗文から，暗号化時に用いたカオス・ニューラルネットワークのあるニューロンの出力値より生成された正整数を作用させる（取り除く）ことによって，複号する．

これにより，カオス時系列信号の平文に作用させる暗号系が構成できる．

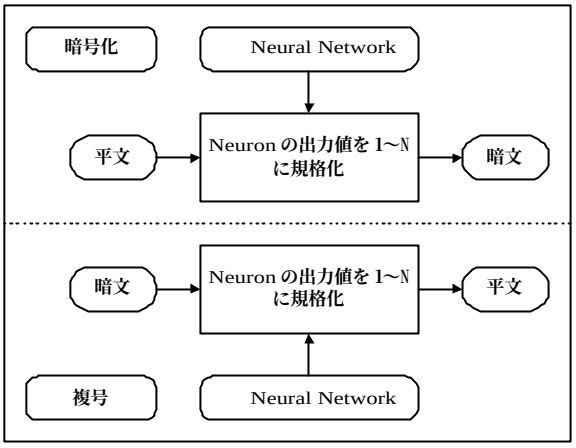


図 4.1　CNN を用いた暗号系

4.2　CNN を用いた相手認証

従来法や，UNIX などで利用者を認証する際にパスワード生成関数として DES 等が用いられているが，DES では各種攻撃（総当たり法，辞書攻撃など）に対して十分な強度を保つことができないことが確認されている[3]．

これに対して，提案法（使い捨てパスワード方式，チャレンジレスポンス方式）では，認証手順には従来法を使用し，パスワード生成関数に CNN を用いることを提案する．

4.2.1　使い捨てパスワード方式

使い捨てパスワードを生成する関数として CNN を用いる方法を提案し，概念図を図4.2に示す．

4.2.2　チャレンジレスポンス方式

チャレンジコードからパスワードを生成する関数として CNN を用いる方法を提案し，概念図を図 4.3 に示す．

5.　実験結果

前節で示した提案法の実験結果を示す．

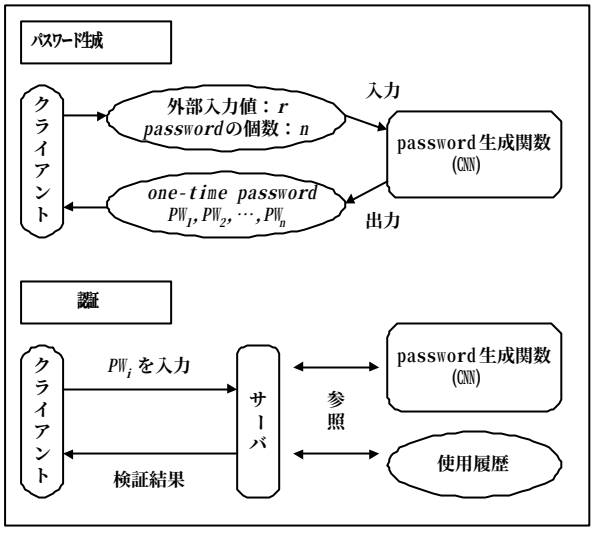


図4.2　使い捨てパスワード方式

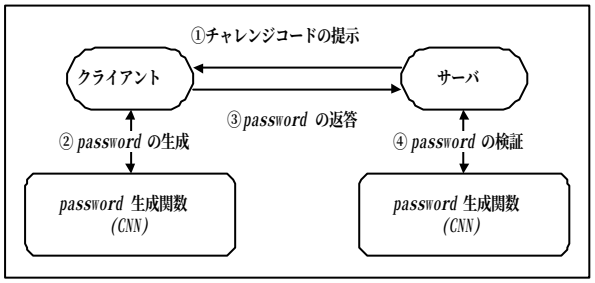


図4.3　チャレンジレスポンス方式

5.1　使い捨てパスワード方式

4.2.1 **より生成した使い捨てパスワードの一部を図** 5.1 **に示す.**

X0=0.30468586417778
X1=0.00278490588282
pwd = 3.088210938e-305

X0=0.50653736273740
X1=0.45232361776712
pwd = 1.600863404e-307

X0=0.01132630800908
X1=0.29318128344761
pwd = 4.882356640e-307

X0 : **ニューロン** 0 **の出力値**
X1 : **ニューロン** 1 **の出力値**
pwd : **パスワード**

図5.1　使い捨てパスワード方式

5.2　チャレンジレスポンス方式

4.2.2 **よりチャレンジレスポンス方式によって認証を行った結果を図** 5.2 **に示す.**

Transition Complete
code_c = 1000
pwd_c = 0.0051465447 0.1211394096
code_v = 1000
pwd_v = 0.0051465447 0.1211394096
Transition Complete
code_c = 2000
pwd_c = 0.1463193457 0.0027493881
code_v = 2000
pwd_v = 0.1463193457 0.0027493881
Transition Complete
code_c = 3000
pwd_c = 0.5065312770 0.0627490275
code_v = 3000
pwd_v = 0.5065312770 0.0627490275
OK!!

code_c：**クライアント側のチャレンジコード**
code_v：**サーバ側のチャレンジコード**
pwd_c：**クライアント側のパスワード**
pwd_v：**サーバ側のパスワード**

図5.2　チャレンジレスポンス方式

5.3　考察

5.1 **と** 5.2 **について，これらの方式は，毎回異なったパスワードを用いているため，総当たり法に耐えることが出来る．これは，**CNN **において，系の遷移回数** *x* **と出力値** *y* **の関数** *y=f(x)***は，ハッシュ関数であるから，毎回異なった値が得られるためである．**

次に，提案法の鍵長について検討してみる．提案法では，一つのニューロン毎に，double **型のパラメータが** 3 **個（閾値，シグモイド関数の傾き，外部入力値）あるため，**n **個のニューロンからなるニューラルネットワークの鍵長は，（**double **型：**64bit**）×（パラメータの個数：**3 **個）×（ニューロンの個数：**n

個）＝（192×n）bit となる．

これに対して，従来法の DES を例に考えてみると，複数の DES を使用することによって鍵長を増やすことができるが, DES を 1 段増やすことで鍵長は 56bit 増す．つまり従来法において DES を 1 段増やした場合と，提案法においてニューロンの個数を 1 個増やした場合では, CNN の方が DES の 3 倍以上鍵長を増やせることになる．

表 5.4　従来法と提案法の鍵長および計算時間

	鍵長（bit）	計算時間
DES（n 段）	56×n	O(n)
CNN Cipher（n ニューロン）	64×3×n =192×n	O(n)

6. むすび

従来法と提案法を比較すると，従来法のアルゴリズムが「組合せ論」や「数体上の問題」（整数論に基づくもの）を用いているのに対し，提案法で用いた特異なカオスを出力するカオス・ニューラルネットワーク（CNN）は, 一対多写像や一方向性関数，ハッシュ関数, さらに計算機環境（CPU の種類，OS，計算精度，プログラムの実装方法等）に依存する点が大きく異なる．

提案法では，パスワード生成に CNN の信号を用いているため以下のことがいえる．

(a) 一方向性が有り，第三者に今後のパスワードの予測は困難である．

(b) ハッシュ関数であるから，系として同じ値はとらない．

(c) それぞれの「今後使われるパスワード列」や，「パスワード生成関数とその条件」の予測は困難である

今後の方針としては，異なる計算機間においても認証が可能となるような改良と，ゼロ知識証明の手法を用いた認証法への拡張，また応用として認証局（CA）への利用が考えられる．

参 考 文 献

[1] 岡本龍明，太田和夫：暗号・ゼロ知識証明・数論，共立出版(1995)

[2] 山本格：暗号と認証，倍風館(1996)

[3] 岡本龍明，山本博資：現代暗号，産業図書(1997)

[4] 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，信学技法 NC98-107(1999-03)

[5] 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(1999)

[6] 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(1998)

[7] 新井朝雄：対称性の数理，日本評論社 (1993)

[8] 合原一幸 編：カオス -カオス理論の基礎と応用-，サイエンス社，(1992)

[9] 長島弘幸，馬場良和 共著：カオス入門 現象の解析と数理，倍風館，(1992)

[10] Denny Gulick 著，前田恵一ら 訳：カオスとの遭遇-力学系への数学的アプローチ-，産業図書，(1995)

[11] 芹沢治 著：カオスの現象学，東京図書, (1996)