Travel notes on bright future technology

雑学エンターテインメント

喜多が行く

明るい未来テクノロジー紀行

第8話

新種の混沌「デジタルカオス」のデタラメさ加減

コスモスと聞けば季節柄、野に咲くピンクの可憐な花弁を思い浮かべてしまうが、もともとは秩序とか調和、宇宙を意味する言葉である。そしてその反対概念の「カオス」は、辞書によれば「混沌。天地開闢(かいびゃく)のときの、混乱したさま」とか、「中国の故事に出てくる、体に穴のない化け物の住んでいた場所」とある。何が何だかわからない、無秩序な状態が「カオス」と名付けられたのである。

しかし、それが何だかわからないものであっても、いったん名前が付けられたからには誰かがその解明に挑戦しようとする。おかげで現在はカオスも数式で表現され、理論として体系だてて説明されるようになってきた。その核心は「自然界に多数存在する一見無秩序に見える事象の背後にも、かんたんな規則が潜んでいることがある」というもの。逆に言えば「かんたんな数式からでも、自然界に存在するような複雑な結果をもたらすことができる」ということだ。

かのアイザック・ニュートンは、なぜそんなに重要な発見をいくつもモノにできたのかと問われ、「巨人の肩の上に登ったからだ」と答えたそうである。先人たちの知的な成果の上に立って初めて、コスモス(宇宙)を統(す)べる万有引力の法則を見出し、歴史に新たな1ページを書き記すことができたのだと言っているわけだ。

「カオス」にも同じように、それを体系立てて理論化した巨人たちがいて、その肩の上を目指す者がいる。コードのハーケンとアルゴリズムのザイルで、巨人の背の絶壁を這い登りながら「カオス暗号」の実用化に取り組む研究者、梅野健氏を東京・小金井の通信総合研究所に訪ねた。

「理想の乱数」を求めて

「大学の卒業論文以来、カオス一筋なんです。カオス的なダイナミクスが脳の中での学習に寄与していると聞いて、これはおもしろいと思った。なんとかこれを万人にわかる形で説明してやろう、と」

残念ながら脳とカオスの話は理解を超えていたが、非常な意欲をもってカオスに取り組む人物であるということは、この一言だけからも伝わってくる。大学院から理化学研究所(理研)に進んだ梅野氏が次に取り組んだ「カオスモンテカルロ法」の説明あたりから、彼の現在の仕事を理解する糸口が少しつかめてきた。

モンテカルロ法とは計算機にサイコロを振らせることで近似値を求める計算手法だ。一回一回のサイコロの出る目はデタラメであっても、何回も何回もサイコロを投げれば、特定の目の出る確率は6分の1に近づいていく、というのがそのキモだ。

そのとき問題となるのはサイコロの出来である。そもそも「乱数」は、物理における質点(体積を持たない質量だけの存在)のような概念の世界の存在だ。だからモンテカルロ法などで現実に使われている乱数はみな「疑似乱数」、つまりある種の方法で作り出された「乱数みたいなもの」なのである。乱数発生器(サイコロ)にはさまざまあるので、出てくる疑似乱数にも質の違いがある。質の悪い乱数を使うと、答えが出なかったり、出るのに時間がかかったりすることになる。

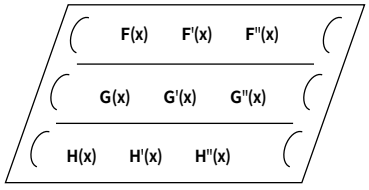
まず金融工学の現場にカオスでなぐり込み

現実世界のサイコロならば、面の直角と平行がきちんととれていて、重心の位置や重量バランスも優れ、角のエッジや丸み、面の滑らかさなども揃うように作られているもののほうがいいサイコロということになる。いっぽうで、また、無限にサイコロを振り続けるわけにはいかないので、可能ならばより速く6分の1という結果にたどり着いてほしい。そこに登場してきたのが、カオスサイコロだったのである。

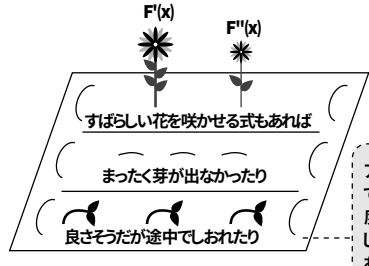
従来のモンテカルロ法で使われていたサイコロも決してイカサマサイコロではなかったが、満足できる結果を得るためには、十分な計算資源を費やして、多数回の試行を繰り返す必要があった。いっぽうで、計算機のスピードアップがあまりに急速であるため、従来とは試行回数をケ

「株式会社カオスウェア取締役副社長」の梅野健氏。CRL所内の1室に構えられたオフィスの壁と机は、特許証書で埋めつくされていた。

図説　デジタルカオス乱数の作り方と実例、そして用途



知られている「カオス関数式」をいくつも用意し、パラメーターを変えながらコンピュータ上で試行。



より良い乱数列を生成する式を見つけ、パラメーターに調整を加えながら育種を続け、見込みのありそうな関数式を選び出す。

アナログでは優秀なカオスでも、デジタルでは有限精度の問題で周期性が出てしまい、役に立たないこともある。

アナログ世界（無限小の概念が通用する）で最適なカオス関数式とはまったく異なる、デジタル世界（最小単位は1ビット）用のカオス関数式を、品種改良を重ねて目的とする用途（CDMAや暗号など）にマッチする形で作り出した。

たいへんよく育ちました

カオス暗号用デジタルカオス関数式の誕生

$$f(x_{n+1})=(2x_n^2+px_n) \bmod 2^{32}$$

「○○ mod 2^{32}」は「○○を2の32乗で割った余り」を表す剰余式。

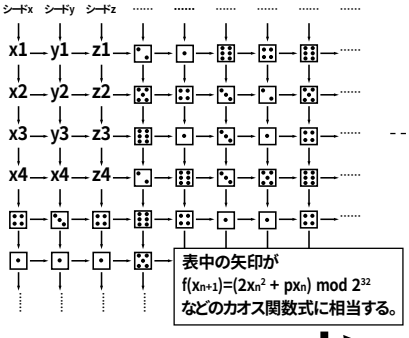
上位32ビットを切り捨て、下位32ビットのみを使用する。

パラメーターpは「2k+1」を満たす数

下位2ビットを「01」にする。

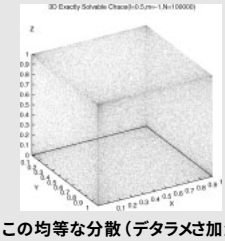
カオスによる多次元のランダムなベクトル列の生成

このデジタルカオス関数式を使って「ランダムなベクトル列」を生成する。
タテ、ヨコ、ナナメとどこをどうとっても関連性の見いだしにくい、しかもシード（乱数を生成する元になる数字）の1ビットの変化が全体に影響を及ぼす乱数の行列となる。
式が簡単なので、ソフトウェアでもハードウェアでも実現でき、かつ高速に処理できる。



表中の矢印が
$f(x_{n+1})=(2x_n^2 + px_n) \bmod 2^{32}$
などのカオス関数式に相当する。

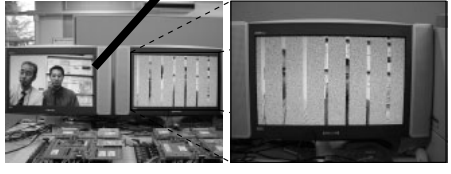
デジタルカオスで生成した3次元ベクトル列をプロットしてみると……



この均等な分散（データメさ加減）がCDMAの電波利用効率の向上に役立つ。カオスCDMAは実現されれば3.5世代の携帯電話などに利用可能。

ハイビジョン映像をリアルタイムに暗号化

リアルタイムに復号
部分的な復号もできる



計算効率（暗号化効率）の高い「梅野式デジタルカオス」の暗号化回路を並列化し、ハードウェア実装（チップ化）したことで、HDテレビ10放送分に相当するデータストリーム（14.85Gbps、世界最高速）を、リアルタイムで暗号化・復号できる。

データベースをカラム単位で暗号化

個人番号	氏名	住所	電話番号
10011	佐藤一郎	東京都渋谷区	03-0223-9876
20112	山田和男	東京都渋谷区	03-0234-8765
20234	大田かおり	東京都目黒区	03-0345-7654
30005	山本友子	東京都品川区	03-0567-6543
30103	鈴木次郎	東京都品川区	03-0578-5432

個人番号	氏名	住所	電話番号
10011	佐藤一郎	pouyrewwqgnv1	lokitgfr9ds5
20112	山田和男	zxcvbnm6p8w9e	titi098titwm
20234	大田かおり	0a9s8d7e6v5fcl	lkwiy7a2mkl
30005	山本友子	jovdkjhhkuirkjt0	dft:poi87gst
30103	鈴木次郎	nldfn8d99ndvnr	dgvlds:;p@d

ベクトルストリーム暗号を使ってデータベースの部分暗号化を高速に行うソフト（世界初）がすでに商品化されている（eCipherGate※）。高速な処理が必要なデータベースでも性能を損なわない暗号化方式だ。

※eCipherGateはジャパン・インフォメーションテクノロジー（株）の登録商標

タ違いに増やすこともできるようになった。すると、いままでは十分間に合っていた乱数生成器にも、乱数性が破れてくるものが出てきた。現実のサイコロで言うなら、振られすぎてキズや欠けが出てしまい、使い物にならなくなる、というようなことが起こってきたのである。

梅野氏のカオスサイコロは、カオス関数式に基づいて生成される数列を次々に生み出していく。ここで生成される数列は、従来の乱数より「乱数性が良い」もので、しかもモンテカルロ法に適用すれば計算効率が上がるのだと言う。つまりデジタルのビット列としてより良い乱数生成器を作ったわけである。

「これを持って、最新の金融工学の現場を訪ねました。モンテカルロ法を使っているデリバティブなどのシミュレーションを行っている研究機関です」

いわば道場破りだ。で、結果は？

「十分評価し、価値も認めてもらった。ただそこの親会社の銀行が合併を控えて混乱しており、それどころじゃなかった」

会社のほうが、すでにカオスだったのだ。

返す刀で通信工学を撃破

カオスモンテカルロの法成果をひっさげ、梅野氏は理研から通信総合研究所（CRL）に移り、カオス乱数の通信工学分野への応用に取り組む。それが、CDMAへのカオスの適用だった。

「従来の乱数を使うモンテカルロ法より、カオス乱数を使うカオスモンテカルロ法のほうが、パフォーマンスが高いことがわかった。そしてこのカオス乱数はモンテカルロ法だけでなく、広く他の用途にも一般化できるということもわかってきた。

たとえば、それの1つが第3世代携帯電話に使われているCDMAという通信方式です。モンテカルロ法で起こるある種のエラーは、CDMAでたくさんのユーザーが基地局にアクセスするときに基地局が受けるエラー（干渉雑音）と数学的には等価だったりするんですよ」

CDMAでは広い周波数帯域に信号を分散させるが、その分散のさせ方がより「バラバラ」であるほど電波の干渉が減り、利用効率が高まる。その「バラバラ」の状態を作り出すには、従来はホワイトノイズ（白色雑音。あらゆる周波数成分を同量ずつ含む）が最もふさわしいとされてきた。

だがこの「バラバラ」作りでも、カオス乱数がホワイトノイズより優れていたのだった。梅野氏はホワイトよりカオスが優れていることを証明したばかりでなく、カオスより優れた方法は存在しないということまで証明してしまったのだという。これまでの取材で、筆者は通信工学や情報通信理論の研究者から「第3世代CDMAはもう終わっていますから」とよく聞かされてきたが、それは単に実用化の段階に入ったから研究は終わっているというだけではなく、その研究にトドメを刺した人がいたからだったのだろうか、梅野さん？

「えー、ある部分ではそうも言えると思います」

カオスCDMAで電波の利用効率が上がれば、たくさんの人が同時に回線を利用できることになる。同じ設備でより多くのユーザーを見込めるから、通信事業者にとっての経済的インセンティブも働くわけで、カオスの実利用に向け注目度が一気に高まった。そして梅野氏も、巨人の肩の上にかなり近づいているようなのだ。

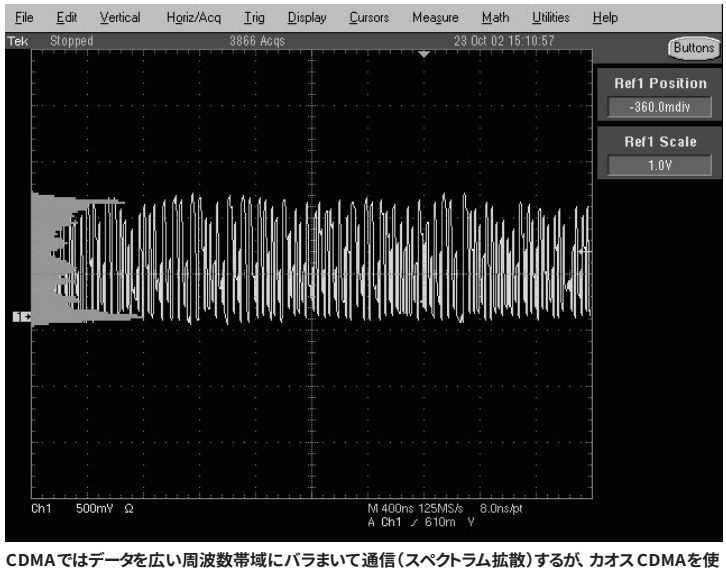
世界最高速で暗号業界に降臨

さらに梅野氏は、カオス乱数の新たなアプリケーションにも挑戦した。そして生まれたのが世界最高速を実証した「カオス暗号」だった。

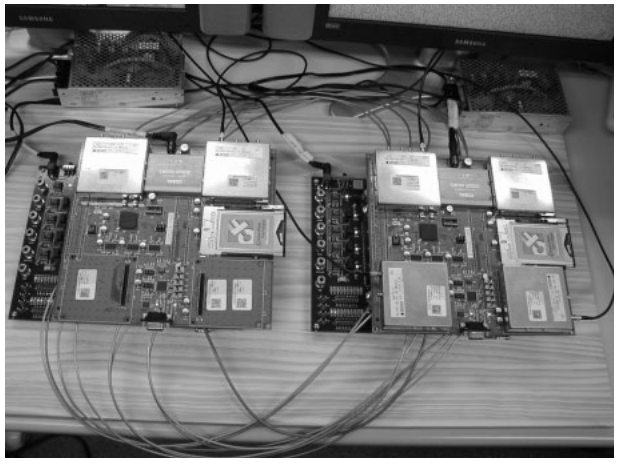
この暗号方式を実現しているのも「大量のデタラメを高速に作りだす」ことのできるカオス乱数生成器だ。

ちょっと古い方ならご存じかもしれないが、かのタモリ（森田一義）の、イグアナの形態模写と並ぶデビュー時の持ちネタに「多言語マージャン」というのがあった。中国語、ロシア語、スペイン語など各面子がてんでバラバラの言語で罵りあうマージャン卓が次第に混乱に陥っていく、という一人芝居。そこでの「会話」はどの言語を母国語とする人にもまったく理解不能だ。それでいて特定の言語のように聞こえるものだった。そのデタラメさ加減はミュージシャンとしてのバックグラウンドも持つタモリの、鋭い音感によるものだったのだろう。

いや、つまり何が言いたいのかというと、少なくともマージャン卓を囲む4人分の、互いに脈絡も関連性もないデタラメな音韻列を奏で続けることができるというタモリの能力が、この芸のおもしろさを支えて



CDMAではデータを広い周波数帯域にバラまいて通信（スペクトラム拡散）するが、カオスCDMAを使うと、現在のW-CDMAと比べて15パーセントも同時利用可能なユーザー数を増やせる。基地局リソースの効率的な利用やコスト削減につながる。



ハイビジョンテレビ10本分の信号をリアルタイムで暗号化・復号できるシステムの心臓は、カオスを利用した高速ストリーム暗号用の「VSC」チップだ。乱数列により並列で暗号化の処理を行えるのが高速化のポイント。

いた、ということだ。

そして梅野氏のカオス暗号も、デタラメな数列を、それも多次元のベクトル列（*m*列*n*行のワークシートを埋め尽くす乱数）として高速に吐き出し続けることができる性能が、他の暗号手段と一線を画する特徴なのである。

品種改良でデジタルカオスを作り出す

この「高速」という特徴を支えるのは、もともとカオスを生み出すための関数式が非常にシンプルなものであることによっている。

たとえば代表的なカオス関数式は「y=4x(1-x)」というような、式を見せられれば中学生でもグラフが描けてしまうかんたんなものだったりする。だがそのアナログ世界でのカオス関数式をデジタル世界にそのまま持ち込むと、プログラムを走らせた途端に「複雑で、予想もつかない結果をもたらす」というカオス本来の特徴が失われてしまうのである。針の飛んだレコードのように、同じパターンで繰り返される数列が吐き出されてくるだけになってしまうのだ。これでは乱数としてはとても使えない。

そこで梅野氏は、デジタル処理に向く「カオス関数式」を、まるで植物の育種のような手法で見出した（157ページの図を参照）。さまざまにパラメーターを変えたカオス関数式を走らせ、数列の繰り返しパターンがより長くなる式を探していった。いわばより高く茎の伸びるタネを、実際に育ててみることで選び出したのである。さらにその式にデジタル回路で高速に処理できるような工夫も加えている。アナログの世界でいう「無限小の概念」が、デジタルの世界には存在しない。いくら小さくなっても最小単位は1ビットで、それより小さいものは存在しない。畑が違うのだから、「無限小」がなくてもよく育つよう関数式に“品種改良”を加えたわけである。

2003年8月号のこのページで「絶対に解読不能な量子暗号」を取り上げた。数学的にも量子力学的にも「絶対」が証明されている暗号方式だ。だが、別の意味で最強の暗号も存在する。それが「1回限りの使い捨て乱数を暗号化に使用する」というバーナム暗号である。ハイビジョン映像のような高いビットレートに匹敵するレートで、理想的な乱数列を生成することができれば、それは量子暗号とはまた別の意味で、最強の暗号となるのだ。暗号化と復合には乱数発生の種（シード）となる秘密鍵を送り手と受け手が共有し、その種から同じ乱数列を生成させればよい。これをデジタル回路に実装可能な形に編み上げたのが「梅野式デジタルカオス暗号」なのであった。

◇ ◇ ◇

所内での研究成果を実用につなげるため、CRLは2001年度から「プレベンチャー制度」という所内ベンチャー起業支援制度を立ち上げた。「自分自身の研究成果の実用化を、CRLにおける自身の業務として行えるようにする」というものだ。わかりやすく言うと「自身も出資して会社を起こしていいですよ。一発当たれば創業者利益でガッポリもアリですよ」という夢と実益を両立させてくれる制度だ。その第1号に、梅野氏が資本金1,000万円の半分を出資した「株式会社カオスウェア」が選ばれている。

「500万円のうち200万円は取得した特許の権利の一部で現物出資しています。私個人とCRLとで半々の持ち分になっている特許のうち、私の持ち分のさらに半分に、自分で100万円の値段を付け、それを株式会社カオスウェアに渡した。それが2件あるので200万円分ということです。ホントは数億円分の価値があるんですが、とりあえずキリのいいところで（笑い）」

自分の作品に自分で値段を付けられる愉快……。ある高みまで登り詰めた者しか、これは味わえまい。

次回は「ポッケルスでポン！」に行く（予定）

喜多充成（きた みつなり）

1964年石川県生まれ。
産業技術・モノ作りを10年来のテーマとする技術系ライターで、本誌草創期からの執筆陣の1人。連載「インターネットビジネス利用の現場から」（1995～）、「2005年へ光る道」（1998～）、「超未来ラボ」（2001～）、特集「電子メール革命」（1995）、「いまそこにある定額制」（1999）などを担当。ウェブ上ではインターネットウォッチ『あるウイルス感染者の告白』などがある。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp