

# 決定論的カオスと「RanSure」による乱数の特性評価

梅野 健

独立行政法人情報通信研究機構 新世代ネットワーク研究センター

〒184-8795 東京都小金井市貫井北町 4-2-1

E-mail: [umeno@nict.go.jp](mailto:umeno@nict.go.jp)

## 1. はじめに

決定論的カオスとは、微分方程式や差分方程式の様に自然現象を記述する決定論的メカニズムの中に潜むランダム現象のことであり、多くの物理現象・自然現象で観測されるランダムネスの普遍的な力学的起源あるいは力学的メカニズムといてよい。だが、リアプノフ指数、コルモゴロフ＝シナイエントロピー等のエントロピー量等のカオス性の指標は与えられていたが、カオスの持つランダムネスそのものの評価は殆ど省みられていなかった。その理由の一つは、米国政府標準調達暗号 AES 選定の際に評価基準として用いられ、一般のランダムネスの評価方法として広く知られている方法(NIST SP 800-22)でも、理論的誤りがあったり、またその誤りを除去した後でも米国国立標準局 NIST からダウンロード可能なプログラムに致命的なバグがあったりという理由で、理論的にも正しく更に、きちんとした運用可能な評価ツールが無かったからである。本報告では、決定論的カオスのランダムネスそのものに着目し、特に、その暗号・モンテカルロ法への期待から、カオスのランダムネス特性を評価する際、同 NIST SP 800-22 の理論的誤りを除去し、更に、プログラムのバグをフィックスしたツール「RanSure」により、他の擬似乱数や物理乱数との比較も含めて乱数特性を評価した結果を報告する。

## 2. カオス暗号の安全性と乱数性評価

ある決定論的カオスに基づく暗号(ここでは、これ以降“カオス暗号”と呼ぶ)

が安全であると証明するにはどの様にすればよいのだろうか？通常の暗号の世界で言われている常識「暗号が安全か否かは、その暗号アルゴリズムが公開され専門家によるテストが可能で尚且つ検証に耐えたか否かで論じられる」が、そのまま通用するのだろうか？2001年独立行政法人通信総合研究所(現独立行政法人情報通信研究機構)のカオス暗号チッププロジェクト[8]が発足した際、本著者は、一般の物理乱数でも評価可能な乱数評価基準によって、まずカオス暗号の乱数性と既存の暗号の乱数性とを比較することにより、カオス暗号と通常の暗号との“違い”を見極めようとした。これは、上記の常識は、あくまでもアルゴリズムを明示的に与えることにより、不特定多数の専門家による攻撃により脆弱性が検知できる例をあらかじめ排除できる、ということの意味するにすぎず、カオス暗号をストリーム暗号として用いる場合にそれが安全か否かは、本質的にアルゴリズムが公開可能か否かではなく、結果として得られたデータが、パターンの無い予測不可能な乱数性を持っているか否かが重要であり、他のカオス以外の物理乱数にも適用可能な一般性を持つと考えたからである。そこで我々は乱数性評価専門部隊を作り、ありとあらゆる乱数とカオス暗号との比較をするために、当時の標準的乱数性評価テスト NIST SP 800-22 にかけていった。結果は、予想に反して、乱数性評価テスト NIST SP 800-22 のテスト項目自身に理論的な誤り(離散フーリエ変換テストと Lempel-Ziv テストの2つに理論的誤りがあった)とが

あるということを見出し、2003年12月の電子情報通信学会にて報告した[1]。その結果の意味するところは、AES選定の基準として用いられた評価方法自身に誤りがあるということであり重要であると考えたからである。我々は、[1]の報告の後、すぐにNISTにも連絡をとり(その返事は無かったが)、その後、2004年12月9日に、NIST SP 800-22 の評価テストから、[1]で主張した通り、Lempel-Zivテストの削除、離散フーリエ変換テストのパラメータの変更が version 1.7 に変更する際に反映され、テスト項目のメジャーな理論的な誤りが無くなった。が、それで問題が解決した訳ではなかった。まずその変更の際して、NIST 側ではその変更の根拠は一切示されなかった。従って、使うユーザーにとって見れば何故その変更をしたのか不明なままの開示となった点が問題として残り、更により現実に影響を与えている問題と思われるのが、現在2005年3月22日にNISTからリリースした version 1.8 プログラムを最新版の評価ツールとして公開配布している中で、後で詳述する様に、そのプログラム自身にも致命的なバグがあることである。

我々はこれらの経験を契機として、当初の目的通り、カオス暗号と既存暗号の真の乱数特性を評価するため、自前で乱数性評価ツールを持たなければいけないと考えた。このツールは、独立行政法人通信総合研究所カオス暗号チップのスピノフ企業である株式会社カオスウェアで誤りを修正した評価ツール「RanSure」として、より多くのユーザーからの乱数性評価の要望に応えるべく、2005年1月から同社から販売した。これが、本報告の一つの主題である乱数特性評価ツール「RanSure」の由来である。

### 3. RanSure について

RanSure とは、第2節で詳説した様に、乱数系列のランダム性評価を実施する Windows2000/XP/Vista で動作する乱数評価用ソフトウェアである。

RanSure では、NIST SP800-22 で行われる統計テストの内、誤りが指摘されたテスト自身の修正を加え、更に、現在 NIST から提供されているプログラムそのものにも存在するランダム性判定のプログラムの誤りを修正したものである [1]。

また、日本語による GUI を実装し、乱数検定について予備知識の無いユーザーも利用が行える上、乱数検定の結果もグラフィカルなレポートとして一望できる様に実装されている。

図1に RanSure による乱数検定が完了した際のスクリーンショットを示す。画面左上が乱数の一様性を示したグラフ、左下が乱数検定のサクセス率の分布を示したグラフを示しており、併せて合格基準となる閾値が同時に示されている。画面右側には行ったテストの項目数と検定結果が示される。また、検定結果はテキストファイルでも出力が行われる。出力されたテキストファイルの一例を図2に示す。RanSure が出力するレポートファイルには、以下の様な情報が出力される。

- 乱数検定評価日時
- 行った乱数検定項目数と合格数
- サンプル数
- 1 サンプルあたりの乱数性評価対象となるビット数
- 乱数性評価対象ファイル名
- 各テスト項目に対する評価結果の詳細(P-Value と Proportion)
- 乱数検定の評価基準

出力されるレポートは、検定を行う際

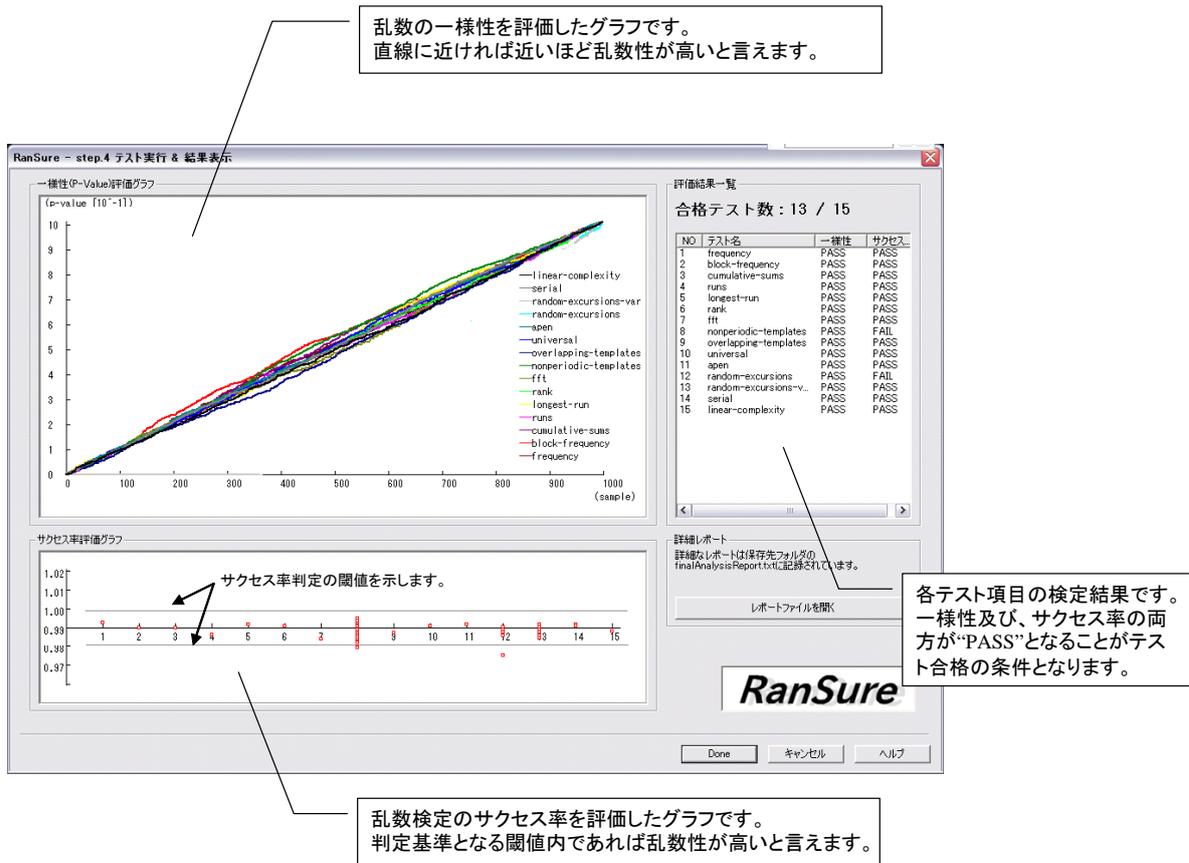


図 1. RanSure のスクリーンショット

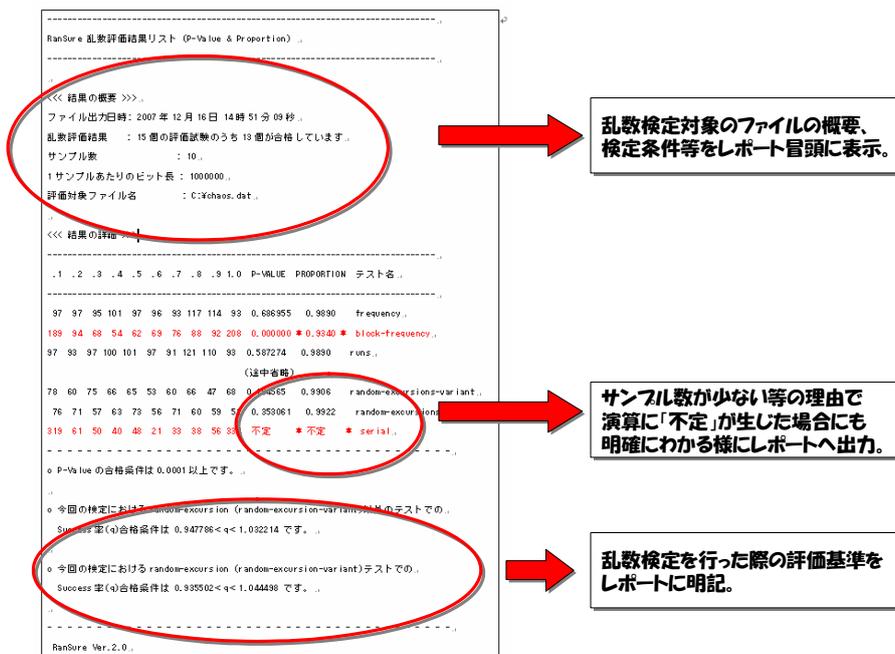


図 2. ファイルとして出力されるレポートの出力例

に設定した箇所に出力させることが出来る上、出力先には検定を行った乱数が記載されたファイル名等と評価を行った日時から自動的にレポート格納用のフォルダが作成され、結果が格納される。

また、FIPS 140-2 の乱数性評価プレテストを用意し、あらかじめ乱数性が悪い系列の評価をストップさせることで、テスト時間を節約できる様になっている。

#### 4. RanSure による各種乱数器のランダム性評価

RanSure で行われるランダム性評価は以下の15項目について行われている。テスト項目を表 1 に示す。

表 1 「RanSure」ランダム性試験項目一覧

テスト番号	テスト名
1	Frequency
2	Block Frequency
3	Runs
4	Longest Run
5	Binary Matrix Rank
6	Discrete Fourier Transform
7	Non-overlapping Template Matching
8	Overlapping template matching
9	Universal
11	Linear complexity
12	Serial
13	Approximate Entropy
14	Cumulative Sums
15	Random Excursions
16	Random Excursions Variant

表 2 及び表 3 に比較的ランダム性が

良いとされている擬似乱数発生器のテスト結果を示す。

表中において「全てパス」とは、NIST 検定項目 15 項目に全てパスしたことを示し、数字が記載してあるものについては、記載した番号のテストがパスしなかったことを示す。また、7 番の

Non-overlapping Template Matching テストにおいては、RanSure が推奨する”パラメータ 9”を利用した場合、148 種類のテンプレートを用いてパターンマッチングを行うが、その際、テンプレート毎にサクセス率が計算されるため、完全にランダムな場合でもパスしない確率が 0.0027 であるため、148 個のテンプレートの内、数個がパスしないことが生じうる[2]。1 回のテスト(1パターン)

につき、使用サンプル数を1000、1サンプルあたりの生成ビット数を100万ビットとした。

RanSure で設定されているパラメータ及び、推奨する乱数列の長さ及びサンプル数で乱数性評価を行った場合、10 個の独立な鍵を用いて生成された 10 パターンの乱数列のうち、経験的に 7 回以上パスするアルゴリズムが良いランダム性を有しているといえることができる。

表 2 乱数性評価結果 (AES)

パターン	サクセス率	P-Value 一様性
1	全てパス	全てパス
2	全てパス	全てパス
3	15	全てパス
4	全てパス	全てパス
5	7	全てパス
6	14	全てパス
7	7,8	全てパス
8	全てパス	全てパス
9	全てパス	全てパス
10	全てパス	全てパス

表 3 乱数性評価結果 (SHA1)

パターン	サクセス率	P-Value 一様性
1	全てパス	全てパス
2	全てパス	全てパス
3	7	全てパス
4	7	全てパス
5	全てパス	全てパス
6	7,15,16	全てパス
7	7	全てパス
8	7	全てパス
9	全てパス	全てパス
10	全てパス	全てパス

以下、表 4 にカオス暗号 VSC128 の乱数検定結果[2]を示す。10 回行った検定の内、7 回は全てのテストを通過しており、且つ、テストを通過しなかったものについても通過しなかった項目が”Template Matching テスト”であるため、良いランダム性を持っていると結論できる。

表 4 乱数性評価結果 (VSC)

パターン	サクセス率	P-Value 一様性
1	7	全てパス
2	全てパス	全てパス
3	全てパス	全てパス
4	全てパス	全てパス
5	全てパス	全てパス
6	全てパス	全てパス
7	8	全てパス
8	全てパス	全てパス
9	全てパス	全てパス
10	7	全てパス

また、カオス暗号 VSC128 には、擬似乱数生成器部分にアーノルドのキャットマップを用いた”2次元キャットマップを用いた2次元 VSC 暗号方式”も荒木・山

口によって提案されている[9]。また同様に擬似乱数生成部分を多次元のカオス写像を用いた場合の安全性解析についても行われている[10]が、

ここでは、2次元キャットマップを用いた VSC 暗号方式による乱数検定結果を表 5 に示す。

表 5 乱数性評価結果 (2次元キャットマップ版 VSC)

パターン	サクセス率	P-Value 一様性
1	7,16	全てパス
2	全てパス	全てパス
3	7	全てパス
4	全てパス	全てパス
5	全てパス	全てパス
6	全てパス	全てパス
7	全てパス	全てパス
8	全てパス	全てパス
9	7	全てパス
10	全てパス	全てパス

また、アルゴリズムは現在非公開であるが、カオスウェアが評価受託した中で、同様のテストで10回中8回パスした暗号化エンジン[Infinity エンジン]も存在することがわかっている[6]。

以上の結果から、NIST SP 800-22 を修正した乱数性評価ツール RanSure を用いた暗号の評価で、標準暗号として認定されている AES よりも評価が高いカオス暗号が存在することを示し、そのテスト結果を紹介した。これが意味することは、2000年-2001年の AES 選定時に乱数性評価で導入された NIST SP 800-22 が、当時誤っていたため、正しく使われず、乱数性評価については、AES 候補アルゴリズムの中で最適化が行われていなかった可能性を示唆する。

## 5. 最新版 NIST SP 800-22 v. 1.8 と RanSure との違いが大きくでている物理乱数について

NIST SP 800-22 は、物理乱数にも良く用いられているので、最後に、公開(販売)されている物理乱数で、NIST SP 800-22 の最新版と RanSure との評価結果で違いが大きく出ているという結果 [7]を示す。

物理乱数	NIST SP 800-22 v. 1.8での合格パターン数	RanSure V2.0での合格パターン数
FDK Random Streamer (PRG102) 250kbps [5]	10 回中 10 回パス	10 回中 3 回パス
某社 非売 物理乱数	10 回中 10 回パス	10 回中 5 回パス

これらの結果を見ると、明らかにこれらの物理乱数は、NIST SP800-22 テストに合格する様チューニングされたものであることがわかるが、同 NIST SP800-22 version 1.8 テストプログラム自身がまだ誤りがあるため、完全にチューニングされておらず、RanSure によれば、カオス暗号や AES 等と比較しても同程度かより低い乱数性しか有していないことが結論付けられる。

この様に、市販されている物理乱数の製品をもってしても RanSure と米国 NIST から普及されている誤った無償プログラム NIST SP800-22 との違いが、安全性に関して無視できない影響を及ぼし始めていると考えられる中、そ

の違いの原因を述べることは意味があることであろう。我々が調査したところ、原因は2つあり、一つは NIST SP 800-22 の合否の表示プログラムのミス (これは軽量の間違い)、もう一つは、15 及び 16 のテスト項目において、NIST SP 800-22 では、サンプル数の計算で、カウントすべきでないサンプル数までカウントしているため、合否の判定基準が狂ってしまっている (これは重度の間違い) からである。これらの NIST SP800-22 のプログラム上のミスは現時点でも解消されていない。我々は、2001 年から究極の物理乱数、カオス乱数を求めてやまないが、RanSure を使って評価する限り、まだ見つかっていない。

少なくとも RanSure に 10 回中 7, 8 回パスする擬似(カオス)乱数と匹敵する物理乱数があっても良いと考えるが、物理乱数生成器チューニング時に、既存の NIST SP 800-22 を使っている限り、評価自身が誤っているため無理であり、当該 RanSure を使ってチューニングすることにより、より良い物理乱数を“発見”できると考えられる。その上で、乱数生成の究極の問題、1 秒間に何ビット乱数性テストをパスする乱数を生成できるかという、通信システムでいうシャノン限界で与えられる様な物理法則に則した基本的な問いに実データで答えられるのではないかと考える。エントロピー生成は物理的に有限であり、物理乱数生成も、その物理法則に縛られると考えられるからである。がランダム性そのものは、究極的には計算機で判定不能であることが解っている。その意味で、乱数判定、乱数の特性評価はいくらでも改善する余地があることを意味し、本 RanSure も、今後の新しい乱数性評価テストの知見を入れ改良し、より精

緻なカオス暗号や物理乱数の評価が可能となることが期待されよう。

## 6. まとめ

本レポートでは、カオス暗号や既存の暗号を、NIST SP 800-22 という米国の標準乱数性テストの誤り（理論的な誤りとプログラム上の誤り）を修正したプログラム「RanSure」を用いて乱数特性を評価した結果を示した。更に、既存の NIST SP 800-22 評価プログラムの致命的な問題点をいくつかの物理乱数によって浮き彫りにした。

**謝辞**：非売品の物理乱数を共同研究先に提供していただいた会社の皆様、共同研究していただいた拓殖大学工学部内田敦史博士、福岡工業大学山口明宏博士、NIST SP 800-22 の評価からカオス暗号構築、RanSure 開発まで一貫して議論していただいた金成主博士に感謝いたします。

## 参考文献

- [1] 金 成主, 梅野 健, 長谷川 晃朗, “NIST のランダム性評価テストについて”, 電子情報通信学会技術報告 ISEC2003-87 (2003-12), PP. 21-27
- [2] 梅野 健, 金 成主, 長谷川 晃朗, “VSC128 仕様書”, <http://www.chaosware.com/vsc128.pdf> (2004).
- [4] 株式会社カオスウェア  
ソフトウェア製品 ”RanSure”  
<http://www.chaosware.com/ransure/>
- [5] FDK CORPORATION REPORT No. “The Evaluation of Randomness of RPG 100 by Using NIST and DIEHARD Tests”,  
<http://www.fdk.co.jp/cyber-e/pdf/>

[HM-RAE104.pdf](#)

- [6] 株式会社エンフォースデバイス  
Infinity-システム暗号  
<http://infinitym.enforce.jp/>
- [7] 井上真樹、内藤直、平野邦人、天野和也 「物理乱数に関する研究」  
拓殖大学工学部 2007 年度卒業論文  
(内田敦史 博士 指導)
- [8] 梅野健、” スケーラブルなカオス暗号とハードウェアの実装評価”,  
日経 LSIIP アワード IP 賞受賞論文  
[http://techon.nikkeibp.co.jp/award/papers/2003\\_co02.pdf](http://techon.nikkeibp.co.jp/award/papers/2003_co02.pdf)
- [9] 荒木 丈宏, “2 次元キャットマップを用いた VSC 暗号方式の擬似乱数性能評価”, 平成 17 年度福岡工業大学大学院工学研究科修士論文
- [10] 岩田 大輔, “多次元カオス写像を用いた暗号システムの安全解析”, 平成 18 年度福岡工業大学情報システム工学科卒業論文