Vol.2012-MPS-91 No.33
Vol.2012-BIO-32 No.33
2012/12/7

乱数度計RMTテストの実データへの応用 ～ハッシュ値とTick株価～

楊　欣[1,a)]　三賀森　悠大[1]　田中　美栄子[1,b)]

概要：以前我々が提案した新しい乱数度評価法 RMT テストは，実数・整数を問わず長い時系列の乱数度を判定できる利点を持ち，擬似乱数や物理乱数の乱数度を比較するにも有効であった．しかし，実用的観点からは，もっと乱数度の低い実データに適用できる点にこそ本手法の利点があると考えられる．そのような応用として，本稿ではハッシュ関数の安全性判定と株の安全性判定の 2 例に対しての結果を報告する．いずれも乱数度の高い方の安全性が高いと想定される．まず，セキュリティー分野でよく使われる SHA-1 と，それより古い MD5 との二つのハッシュ関数の出力データの乱数度を RMT テストにより比較すると，確かに SHA-1 の方が乱数度が高く安全性の高いことが確認できた．次に，2007 年から 2009 年までの TOPIX500 の株価ティックデータの乱数度を測定し，翌 2010 年と 2011 年の収益との関連性を調査し，多くの場合に乱数度の高い株の安全性が高いという結果を得た．

キーワード：ランダム行列理論，RMT テスト，乱数度，ハッシュ値，株の安全性

Application of the RMT-test on Real Data: Hash Function and Tick Data of Stock Prices

Xin Yang[1,a)]　Yuta Mikamori[1]　Mieko Tanaka-Yamawaki[1,b)]

Abstract: The RMT-test, that we have proposed earlier as a tool to measure the randomness of long sequences, is applicable on various data types, integer or real, independent of the length of sequences. We have shown its effectiveness by comparing the degrees of randomness among pseudo-random generators as well as physical random generators. From the practical point of view, however, the advantage of this RMT-test resides in its applicability on real-world data, whose randomness level is far below the reach of the conventional randomness tests, such as NIST or JIS. In this paper, we present our result on applying the RMT-test on two examples: the choice of hash functions and the stock prices, assuming that the high randomness of the sequences indicates the high security level in both cases. In the first example, we compare two popular hash functions, the SHA-1 and the older MD5. The result of the RMT-test shows that the randomness of the output sequences of SHA-1 is indeed higher than the output of MD5. In the second example, we compare the performance of various stock prices in relation to their randomness and show that the stock prices of higher randomness perform better than the stocks of lower randomness, for the stocks in TOPIX500 in the year 2010 and 2011 based on their randomness in the previous three years, 2007-2009.

Keywords: Random matrix theory, RMT-test, Randomness, Hash value, Safetiness of Stocks

1. はじめに

乱数の良否を調べるためには， 統計的な手法を使って，その性質を解析するという手段が一般的であり，様々な統計的検定法が提案されている．例えば，シミュレーション

[1] 鳥取大学大学院工学研究科情報エレクトロニクス専攻
Tottori University, Graduate School of Engineering, Department of Information and Electronics
[a)] yx0709@ike.tottori-u.ac.jp
[b)] mieko@ike.tottori-u.ac.jp

Vol.2012-MPS-91 No.33
Vol.2012-BIO-32 No.33
2012/12/7

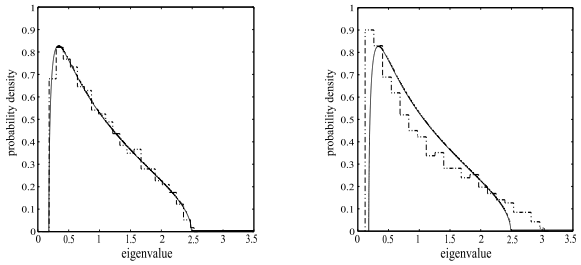

図 1 RMT テストの定性評価例（左：合格，右：不合格）
Fig. 1 Example of the qualitative evaluation of the RMT-test (left: passed, right: failed)

用の乱数に対する検定法である PLAB，乱数生成器や圧縮アルゴリズムなどの評価法である ENT，暗号分野で利用される NIST-SP 800-22 や DIEHARD などがある．しかし，ツールごとに採用している検定の種類や数が異なり，使いにくい難点がある [1]-[4].

そこで，我々は，ランダム行列理論を用いて，理論的に解りやすく，目視で乱数度を判断でき，データ形式を選ばず，単一の評価基準を持つ新しい乱数度測定法（RMT テスト）を提案した [5]．本稿ではこの RMT テストの実データへの応用を考え，ハッシュ関数と株価ティックデータを使った実験を行う．

2. RMT テスト

2.1 RMT テストの定性評価

本稿で用いるのは Plerou 等により株式市場に応用された文脈 [6][7][8] に基づき，時系列の相関行列の固有値分布をランダム行列理論式と比較する方法である．以下に手法を概説する．時系列長 L の独立なデータ N 個から作成した相関行列の固有値を求める．このような相関行列の固有値分布は，データがランダム列であればランダム行列理論式に一致するはずである．ランダム行列理論（Random Matrix Theory：以下，RMT）によれば，相関行列の固有値分布は $N \to \infty$ でその統計性によらず $Q = L/N$ のみに依存する簡単な関数となる．

$$P_{RMT}(\lambda) = \frac{Q}{2\pi\lambda}\sqrt{(\lambda_+ - \lambda)(\lambda - \lambda_-)} \tag{1}$$

$$\lambda_\pm = \left(1 \pm \sqrt{\frac{1}{Q}}\right)^2 \tag{2}$$

この方法は，固有値分布のヒストグラムと式 (1) を目視により比較し，両者が一致すれば RMT テストに合格とし（**図 1** 左），逆に理論曲線からはみ出せば RMT テストに不合格とする（図 1 右）．この方法は直感的に見やすく，形状の特徴を把握しやすい利点がある．

2.2 RMT テストの定量評価

RMT テストの定性評価は可視化による直観性と分布の形状による特徴表現が可能な点により，経済・社会・医療データ等への応用が期待される．一方，機械乱数列のように乱数度の高い数列の乱数度を比較するためには，特徴を数値化することが必要である．そこで，定量評価手法を併用し，目視で差異を判別しにくい乱数間の乱数度を比較する．すなわち，固有値のモーメントを理論値と比較することで定量化を行う．具体的には，まず，固有値の実測値から k 次モーメントを計算する．

$$m_k = \frac{1}{N}\sum_{i=1}^{N}\lambda_i^k \tag{3}$$

次に，対応する理論値を式 (1) を用いて以下のように計算し，

$$\mu_k = E(\lambda^k) = \int_{\lambda_-}^{\lambda_+}\lambda^k P_{RMT}(\lambda)d\lambda \tag{4}$$

理論値と実測値の誤差絶対値

$$error_k = m_k/\mu_k - 1 \tag{5}$$

の小さい方を乱数度が高いと判定する．

定性評価の比較図を描くためには，N 個の固有値を全部求める必要があるが，RMT テストの定量評価だけならば，相関行列の k 乗の対角成分の和 (trace) の $1/N$ 倍として，k 次モーメントを

$$m_k = \frac{1}{N}\sum_{i=1}^{N}(C^k)_{i,i} = \frac{1}{N}\sum_{i=1}^{N}\lambda_i^k \tag{6}$$

として求めれば良く．行列サイズが大きい場合には，固有値の計算が省けて便利である [9].

モーメントの次数 k としてどの値が良いかを決めるため，2 つの擬似乱数（LCG と MT），及び 3 つの物理乱数（日立，東芝，東京エレクトロン）を使って誤差を算出し，乱数度を比較する．5 種類の乱数データの乱数度を $N = 500$, $Q = 3 \sim 6$（$L = 1500 \sim 3000$）について求め，500 サンプルの平均値と標準偏差の考察から，これらの 5 種類の乱数生成器の良し悪しを比較すると，$k = 5$ 以下だと明確な差が出にくく，$k = 6$ を使用するのが良いことがわかる，データのばらつきを考慮しても，データ長 75 万の乱数列に対し，6 次モーメントの誤差が 3%以下という基準を取れば，上記 5 種類の乱数データが全て合格することが分かった [10].

また，乱数列の長さ制限を緩和するため，$N = 200$, 300, 400（$Q = 3$, …, 10）の擬似乱数と物理乱数の 6 次モーメントの誤差を調査した．その結果，有意水準 $\alpha = 0.05$ の時に $N = 200$, $L = 600$（$Q = 3$）としても，6 次モーメントの誤差の絶対値を 5%以下に抑えることができることが判明した．これに基づき，RMT テストの定量評価基準を「$k = 6$, $x = 5$」と決定した．つまり，「6 次モーメントが理論式に 5%以下の誤差で一致すれば乱数度が高い」を

Vol.2012-MPS-91 No.33
Vol.2012-BIO-32 No.33
2012/12/7

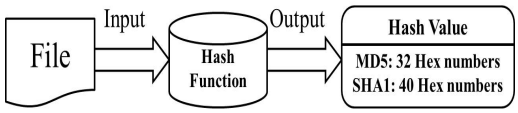

図 2 ハッシュ関数とハッシュ値
Fig. 2 Relation between a hash function and its hash value

RMT テストの定量評価基準とする．しかし，乱数列の長さが 12 万以下の乱数列にはこの基準を適用できない．例えば，$N = 100$（$Q = 3$）の乱数列の場合は，6 次以下のモーメントの理論式に対する誤差が 10%以下ではあるが 5%を越える値となってしまう．そこで，提案手法の定量基準の制限条件として $N \geq 200$，$L \geq 600$，つまりデータ全長が $N \times L = 12$ 万点以上となる [11].

3. RMT テストの実データへの応用

3.1 ハッシュ関数

ハッシュ関数を用いて，任意長のキーを固定長のメッセージへ変換することにより隠す，暗号学的ハッシュ関数は情報セキュリティー分野で様々に利用されており，ハッシュテーブルのインデックス，フィンガープリント，重複データの検出などの用途がある．

本稿では 2 つの暗号学的ハッシュ関数 MD5 と SHA-1 の出力データを利用して，その乱数度を RMT テストで測定する．暗号学的ハッシュ関数は多数存在するが，その多くは脆弱性が判明し，使われなくなっている．例えば，2004 年 8 月，当時よく使われていたハッシュ関数（SHA-0, RIPEMD，MD5 など）の弱点が判明した．このことから，これらのハッシュ関数から派生したアルゴリズム，特に SHA-1 と RIPEMD-128 の長期的なセキュリティーに疑問が投げかけられた．2009 年現在，最も広く使われている暗号学的ハッシュ関数は MD5[9] と SHA-1[10] である．しかし，MD5 は既に破られているため，安全性が高いと言えるのは SHA-1 である．

ここでは，ハッシュ関数の出力データのランダム性が高ければ暗号学的安全性も高いと考え，MD5 と SHA-1 の出力データのランダム性を比較し，安全性が高いほうの SHA-1 の出力データのランダム性が MD5 より高いと予想し，実験した．

MD5 と SHA-1 のハッシュ値は**図 2** に示す関係にある．定量評価基準の長さ制限が 12 万以上であるため，そこで，3750 個ファイルの MD5 のハッシュ値と 3000 個ファイルの SHA1 のハッシュ値でそれぞれの長さ 12 万の数列を取得できるよう，N = 200，Q = 3 と設定した．6 次モーメントの誤差の絶対値を 10%に対する平均値（標準偏差）として**表 1** に示す．MD5 と SHA-1 の両方に対して，MD5 の $k = 6$ を除く殆んでの場合に 2σ までの誤差を考慮した値が 5%以下となり，乱数度が高いと言える．また，SHA-1 の各次モーメントの誤差の絶対値は小さく，従って，予想の通り，MD5 より SHA-1 の出力データのランダム性が良いという結果がとなり，提案手法の有用性をチェックできた．

表 1 MD5 と SHA-1 の出力データの RMT テストによる定量評価結果：10 例の誤差平均値 (標準偏差)
Table 1 Quantitative evaluation of the output sequences from MD5 and SHA-1:The average(S.D.) over 10 samples

k	MD5	SHA-1
2	-.0017(.0030)	-.0003(.0016)
3	-.0044(.0078)	-.0006(.0039)
4	-.0074(.0139)	-.0005(.0069)
5	-.0106(.0211)	-.0001(.0106)
6	.0137(.0294)	-.0011(.0154)

3.2 株価変動のランダム性と株の安全性との関係

3.2.1 データの対数収益化による乱数度低下の検出

株式投資のパフォーマンスは株価の値そのものより何 % 上がったかが重要である．そのため，株価を処理するときは価格そのものでなく，その変化率である「収益率」が常用される．価格時系列 $(p_1, p_2, \ldots, p_L)$ に対しては，その収益率として

$$r_i = \ln p_i - \ln p_{i-1} \tag{7}$$

で表される対数収益の時系列 $(r_1, r_2, \ldots, r_{L-1})$ が使われる．

このとき特有の癖が時系列に付与される．これは，式 (7) を連続的に使うことによる重複が余分の相関となって，乱数度を下げる効果を出じる．この効果を積極的に利用して，乱数度の高すぎる数列から人為的に低乱数度の数列を作成する．LCG で生成した擬似乱数から以上の方法で乱数度を下げ，提案手法でその乱数度を検定した結果を $N = 500$，$L = 1500$ の場合について**図 3**（左）に示す．ランダム行列理論の許容範囲 $[\lambda_-, \lambda_+]$ から出ており，乱数度が低いと言える．

重複部分を削除すると，時系列のランダム性は戻る（図 3

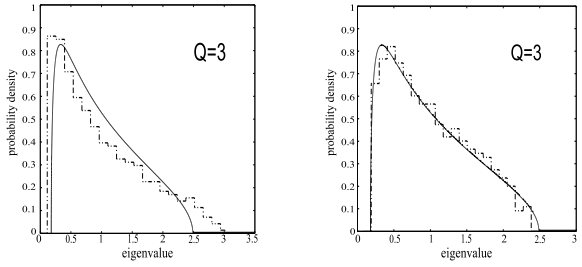

図 3 LCG の対数収益による評価結果：重複有り (左) と重複無し (右)
Fig. 3 Evaluation of LCG by means of log-return with overlapping (left) and non-overlapping (right)

表 3 TOPIX500 の高流動性の 14 業種を抽出
Table 3 14 industrial sectors having high liquidity

	業種	企業コード	銘柄数
1	食品	2002,22**,25**,28**,2914	20
2	化学	3405,3407,40**,41**,42**,44**,46**	40
3	医薬品	4151,45**	17
4	鉄鋼	54**,5541	14
5	電気機器	4062,4902,60**,65**,66**,67**,68**,69**,7276,77**,8035	54
6	機械	5631,61**,62**,63**,64**,6581,6586,70**	32
7	非鉄金属	57**,58**	11
8	輸送用機器	3116,6201,6902,6995,7003,7012,72**,73**	26
9	銀行	83**,84**,8522,8544	40
10	小売	26**,2730,30**,3382,7453,7532,7649,8028,8184,82**,98**,9983,9989	27
11	卸売	27**,7459,80**,9832,9962,9987	17
12	不動産	3231,4666,88**,89**,9706	11
13	情報通信	3626,46**,47**,8056,94**,96**,9766,9984	24
14	電気ガス	95**	13

右）[12]．**表 2** に重複有りと重複無しの対数収益時系列の RMT テストの定量評価結果を示す．重複無しの時系列に対し，6 次モーメントの誤差は 5%以下となる．この性質を利用し，株価の重複無し対数収益時系列のランダム性と株の安全性の関係を調査する．

3.2.2 株価の重複無し対数収益時系列の乱数度調査

株価時系列を用いその対数収益を取った時系列 R=$(r_1, r_2, \ldots, r_{L-1})$ を重複無しの二つの時系列 R_1=$(r_1, r_3, \ldots, r_{L-1})$ と R_2=$(r_2, r_4, \ldots, r_{L-2})$ に分離し (L は偶数)，R_1 と R_2 について 6 次モーメントの誤差を平均値により評価する．時系列 R の乱数度は RMT テストの定量評価で求める．

(1) 採用したデータ

ここで，2007 から 2009 年の東証 TOPIX500 の 3 年間 1 分毎のティックデータを採用する．東証市場第一部に上場している全銘柄（TOPIX の構成銘柄）を「証券コード協議会」が定める業種区分に基づき 33 業種に区分した．

TOPIX500 を構成する銘柄は本来流動性の高い上位 500 の銘柄であるが，市場の状況は刻々と変化しているため，時間の経過と共に市場の実状と株価指数の構成銘柄の特徴とが合わなくなってしまう，ということが起こり得る．そのような事態を回避し，市場の状況を忠実に反映した株価指数にするために，TOPIX500 の構成銘柄は年に 1 回見直される．そこで，銘柄数の多い業種は高流動性業種と考えられる．

また，RMT の適応条件として $N \to \infty$ と $L \to \infty$，つまり，長いデータ長が必要である．そこで，本稿では 33 業種の中から下記の 2 つの条件を満たす 14 業種を選んで「高流動性の業種」とした．即ち業種の銘柄数が 10 以上であることと，ティックデータ長が 17 万点以上あることが高流動性の 14 業種の条件である．これを**表 3** に示す．但し，2012 年現在上場廃止した銘柄は除外する．この 14 業種に対して各業種のなかで最長データを持つ 4 銘柄を使用し，計 56 銘柄を分析対象とする．

(2) 株価ティックデータの乱数度

ここで，3 業種の 12 銘柄を例として手法を説明する．まず，2007 年初から 2009 年末まで三年間の株価ティックデータを用い，RMT テストにより乱数度を算出する．

表 4 に示すように，2010 年の最初の取引日である 1 月 4 日に各業種の乱数度最高の株を購入する．つまり，化学業の 6988，医薬品の 4568 と卸売業の 8053 を購入する．**表 5** に各業種の損益を良い順に示す．表 5 の結果を見ると，購入した 3 株の全ての収益の業種内順位が 2 位以上になっている．つまり，業種内で 2 位以上の収益を得る確率が 100%である．逆に，各業種の乱数度が最低の株である 4063，4519 と 8031 の 3 株を購入すると，2010 年 1 月末日の収益は業種内 2 位以上となる株は 8031 のみとなる．つまり，業種内で 2

表 2 LCG と MT の対数収益の時系列の定量評価結果 (重複有り (左) と重複無し (右))
Table 2 Errors in RMT-test for the overlapping(left) and non-overlapping(right) log-return sequences

	重複有り		重複無し	
k	LCG	MT	LCG	MT
2	.1268	.1230	-.0013	-.0016
3	.3211	.3089	-.0039	-.0042
4	.5692	.5434	-.0072	-.0076
5	.8732	.8282	-.0112	-.0115
6	1.2416	1.1702	-.0156	-.0159

表 4 三業種のデータ長上位 4 社の乱数度結果 (Q=4) 誤差単位:%
Table 4 Errors in RMT-test for the data length which is the top 4 of each industrial sector

業種	コード (誤差)	業種	コード (誤差)	業種	コード (誤差)
化学	6988(1.9)	医薬業	4568(1.2)	卸売業	8053(0.9)
	4901(3.3)		4503(1.3)		2768(2.6)
	4185(3.6)		4502(1.9)		8058(5.6)
	4063(7.0)		4519(3.9)		8031(6.8)

表 5 2010 年 1 月 4 日に各株を購入し，2010 年 1 月末日に売却したときの対数収益結果
Table 5 Purchase all the stock in table 3 on January 4th2010,and calculate the log-return on the end of January 2010

業種	コード (収益)	業種	コード (収益)	業種	コード (収益)
化学	4901(.032)	医薬業	4568(1.2)	卸売業	8053(.052)
	6988(.019)		4503(1.3)		8031(-.002)
	4185(-.074)		4502(1.9)		2768(-.041)
	4063(-.121)		4519(3.9)		8058(-.058)

位以上の収益を得る確率が 33.3%である．

そこで，売る時点を各月末に設定し，乱数度が最高の株と乱数度が最低の株について各々が収益率において 1 位または 2 位となる確率を計算し，これを勝率として，**図 4** に示す．図 4 の横軸は 2010 年と 2011 年の TOPIX 500 の取引月末日の 24 時点を示し，乱数度が最高の株を H で，乱数度が最低の株を L で表す．乱数度が最低の株より乱数度が最高の株を購入する方の安全性が高いと言える．

(3) Q=4 を選択した理由

RMT テストはランダム行列理論を利用するため，$N \to \infty$ を条件として，$N \times N$ の相関行列の固有値分布を求める．**図 5** に LCG の同じ長さ (2 万) の数列を $N = 100$ と $N = 50$ とした場合の RMT テストの定性評価の結果を示す．$N = 50$（$Q = 8$）の方が $N = 100$（$Q = 2$）よりばらつきが大きいことを図 5 に示す．つまり，同じ時系列であれば Q が小さい方が良いと考え，$Q = 2$，3，4，5，6 を設定して，実験を行った．

その結果，$Q = 2$ については H と L を明確に分離できなかった．$Q = 3$ の場合，H と L の分離はできるものの，H と L の上下関係が途中で逆転する．また，$Q = 5$ になると L の方が H より上位に来る点が現れ始め，$Q = 6$ になると全体に L の方が H より上になる．結果として $Q = 4$ が 2 年間を通して H の方が L より高いパフォーマンスを得ることが分かる．また，3 月間や 6 月間など近い未来を予測すると，$Q = 3$ と 4 はほぼ同等である．本稿では，$Q = 4$ を選定し，株価のランダム性と安全性を調査する．

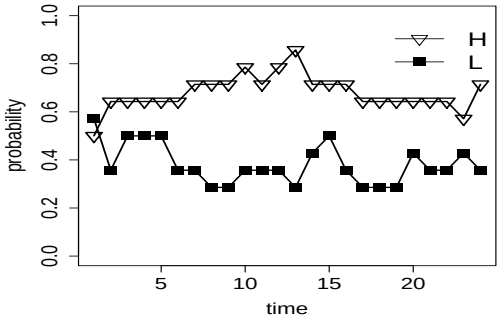

図 4 乱数度最高の株 (H) と最低の株 (L) についての勝率変化図 (Q=4)
Fig. 4 Probability of the profit and loss of stocks which is top 2 in each industrial sector for Q=4

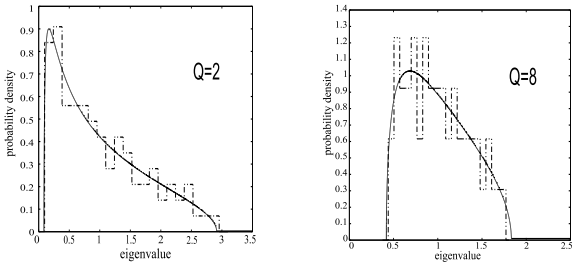

図 5 同じ数列の異なる Q に対する RMT テストの誤差比較 (Q=2(左)，Q=8(右))
Fig. 5 Comparison of Q=2 and Q=8 for the same data

3.2.3 株価時系列のランダム性と安全性の関係

2007-2009 の 3 年間のデータによる各銘柄の無重複対数収益時系列を利用し，RMT テストで各業種の銘柄毎の乱数度を計算した．一方，2010 年 1 月 4 日の時点で業種毎の乱数度が最高と最低の株を購入し，各時点で業種内収益が 2 位以上となる勝率図を作成した．その結果，乱数度が最高の株（H）を購入すると，その勝率は乱数度が最低の株（L）の勝率より 2 年間一貫して高いことが図 4 からわかる

また，順位だけではなく，購入した株の各時点の平均収益率も調査した．算術平均収益率 (r) は

$$r = \frac{1}{n}(r_1 + r_2 + r_3 + \cdots + r_n) \tag{8}$$

によって計算する．式中の n は業種数．2010 年から 2011 年までの 2 年間の各月末（24 時点）を図 4 と同様に H と L に対して，平均収益率を**図 6** に示す．**図 7** は株価市場の全体状況を反映する日経平均の経年変化図である．図 6 と図 7 の期間 A と B を比較すると，株価市場の全体的に下がる時期は，乱数度最高の株を購入すると損失は少なく，安全性が高いと言える．

4. 終わりに

先に提案した，RMT を用いた乱数度評価法 (RMT テス

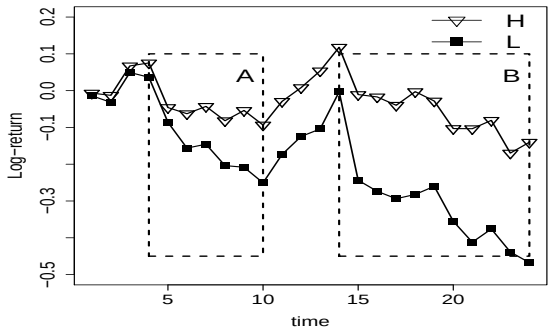

図 6 各時点の平均収益率：H：乱数度最高の株，L：乱数度最低の株
Fig. 6 Average Log-return of each month: H: highest randomness, L: lowest randomness)

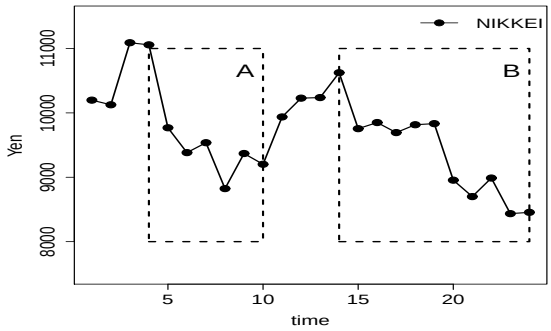

図 7 日経平均の経年変化図 (2010-2011)
Fig. 7 NIKKEI Average chart(2010-2011)

ト) の有用性をチェックするため，実データへの応用研究を行った．一つ目は，暗号学的ハッシュ関数 MD5 と SHA-1 の乱数度の比較であり，より安全性の高い SHA-1 の乱数度の方が MD5 に比べて高いことを示すことが出来た．二つ目は株価ティックデータの対数収益時系列の乱数度の比較であり，TOPIX 500 の異なる 14 業種から各 4 社を選んで乱数度と損益の関連性について調査したところ，各業種について 4 社の内で乱数度が最低の株が最も安全性が低いという結果となった．

参考文献

[1] Hannes,L.: *PLAB a System for Testing Random Numbers*, Proceedings of the International Workshop Parallel Numerics'94,pp.89-99(1994).
[2] ENT: *A Pseudorandom Number Sequence Test Program*(online), http://www.fourmilab.ch/random/).
[3] NIST: *A Statistical Test Suite* (online), csrc.nist.gov/groups/ST/toolkit/rng/documentation-software.html (2010.08.13).
[4] Dieharder: *A Random Number Test SuiteVersion 3.31.1* (online), http://www.phy.duke.edu/ rgb/General/dieharder.php.
[5] 田中　美栄子，糸井　良太，楊　欣：RMT 公式を用いた乱数度評価法の提案，情報処理学会論文誌数理モデル化と応用，Vol.5，pp.1-8 (2012).
[6] Laloux, L.,Cizeaux, P.,Bouchaud, J., Potters, M.: *Noise Dressing of Financial Correlation Matrices*,Physical Review L, Vol.83, pp.1467-1470 (1998).
[7] Plerou, V., Gopikrishnan, P., Rosenow, B., Amaral, L.A.N. and Stanley, H.E.: *Universal and Non-Universal Properties of Cross-Correlations in Financial Times Series*,Physical Review L, Vol.83, pp.1471-1474 (1999).
[8] Plerou, V., Gopikrishnan, P., Rosenow, B., Amaral, L.A.N. and Stanley, H.E.: *Random Matrix Approach to Cross Correlation in Fianancial Data*,Physical Review E, Vol.65, no.066126 (2002).
[9] 三賀森　悠大，楊　欣，糸井　良太，田中　美栄子：RMT テストの性能検証 ∼NIST 乱数検定との比較 ∼，研究報告数理モデル化と問題解決（MPS），2012-MPS-88(15).
[10] 楊 欣，糸井 良太，田中 美栄子：ランダム行列理論を用いた乱数度評価法の提案，統計数理研究所共同研究リポート，Vol.271「経済物理とその周辺（8)」，pp.19-31 (2012).
[11] Black, J., Cochran, M. and Highland, T.: *A Study of the MD5 Attacks: Insights and Improvements* (online), http://www.cs.colorado.edu/ jrblack/papers/md5e-full.pdf (2008.07.27).
[12] Locktyukhin, M. and Farrel, K.: *Improving the Performance of the Secure Hash Algorithm(SHA-1)* (online), http://software.intel.com/en-us/articles/improving-the-performance-of-the-secure-hash-algorithm-1/ (2010.03.29).
[13] Tanaka-Yamawaki, M., Yang, X. and Itoi, R.: *Moment Approach for Quantitative Evaluation of Randomness Based on RMT Formula*, Intelligent Decision Technologies Smart Innovation, Systems and Technologies, Vol.16, pp.423-432 (2012).