ストリーム暗号の評価
連性テスト
MULTI-S01 編

平成 13 年 1 月 21 日

1　取得条件

FIPS 140 の乱数性評価テストと同様に 20000 bits をサンプリングして，そのデータに含まれる gaps (0 が連続して並ぶ)，および blocks(1 が連続して並ぶ) の存在分布を調べる．調査対処がストリーム暗号であるため，平文 C と暗号文 M との排他的論理和 $C \oplus M$ の連性テストを行った．FIPS 140 検査に合格する条件は全てのサンプルに対して， 1,2,3,4,5, および 6 以上の 6 種類の gaps, blocks の値が下記の表の範囲内に含まれることである．

長さ	範囲
1	2267-2733
2	1079-1421
3	502-748
4	223-402
5	90-223
6 以上	90-223

鍵は，別冊「MULTI-S01 暗号評価に使用したデータについて」に記載した組み合わせ (秘密鍵 C を 400 通り，乱数列番号 D を 25 通り，冗長度 R を 10 通り，合計 100,000 通り) に対し，同別冊に記載したデータに対する暗号化を行い，評価を行った．

つまり，このテストでは 20000 bits のデータを $100,000 \times 1000$ 件生成し，連性テストを行ったことになる．

2　テスト結果

以下に度数分布を示す．

度数分布は理想的な値を示しているが，細かくみると，FIPS140 の条件を満たさないデータが存在することがわかった．

3　評価

FIPS 140 の条件をクリアできないものが 34 件発生した．従って (平文 $\oplus$ 暗号文を乱数と見なした場合)，連性テストに関しては，FIPS 140 検査を合格しない．

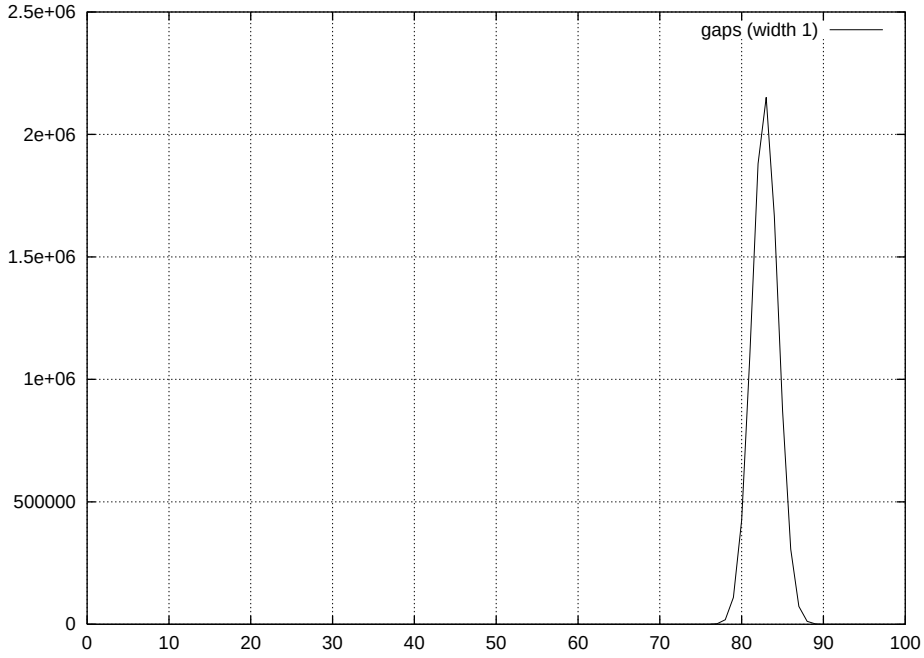

図 1: gaps (長さ 1) の分布

なお，付録に示した異常が発生したパターンでは，次のものに相関を見ることができる．

平文 1 ビット違い 秘密鍵，乱数列番号，冗長度が cm0a5, da008, ra001 のものについては，異常が 20 件発生する．平文は pr381 から pr400 であり，先頭 2 バイト以外は同じである． MULTI-S01 暗号では，先頭以外が同じ平文を，同一鍵 (秘密鍵，乱数列番号，冗長度) で暗号化すると，最初以外は全く同じ暗号文が生成される．cm0a5, da008, ra001, pr281 の組では長さ 1 の gap の数に偏りがあったため不合格が多発したと思われる．

平文 1 ビット違い (その 2) 秘密鍵，乱数列番号，冗長度が ca350, da020, ra001 のものについては，異常が 6 件発生する．平文は pr284, pr288, pr292, pr293, pr297, pr298 であり，先頭 2 バイト以外は同じである．MULTI-S01 暗号では，先頭以外が同じ平文を，同一鍵 (秘密鍵，乱数列番号，冗長度) で暗号化すると，最初以外は全く同じ暗号文が生成される．ca350, da020, ra001, pr281 の組では長さ 1 の gap の数に偏りが (合否すれすれ近くまで) あり，そのうち失格ラインを越えたものが現れたと判断する．

なお，上記の異常多発域では，平文はいずれも pr281 と 1 ビット違いのものばかりである．しかし，この平文は C 言語の random 関数を用いて用意したもので，オール 0 とかオール 1 という特殊なものではない．

同一鍵 (秘密鍵，乱数列番号，冗長度) で暗号化を行うことはないので，異常が発生した件数は，12 件と見なすことができる．この 12 個のパターンでは，鍵，冗長性，平文に相関はみられない．

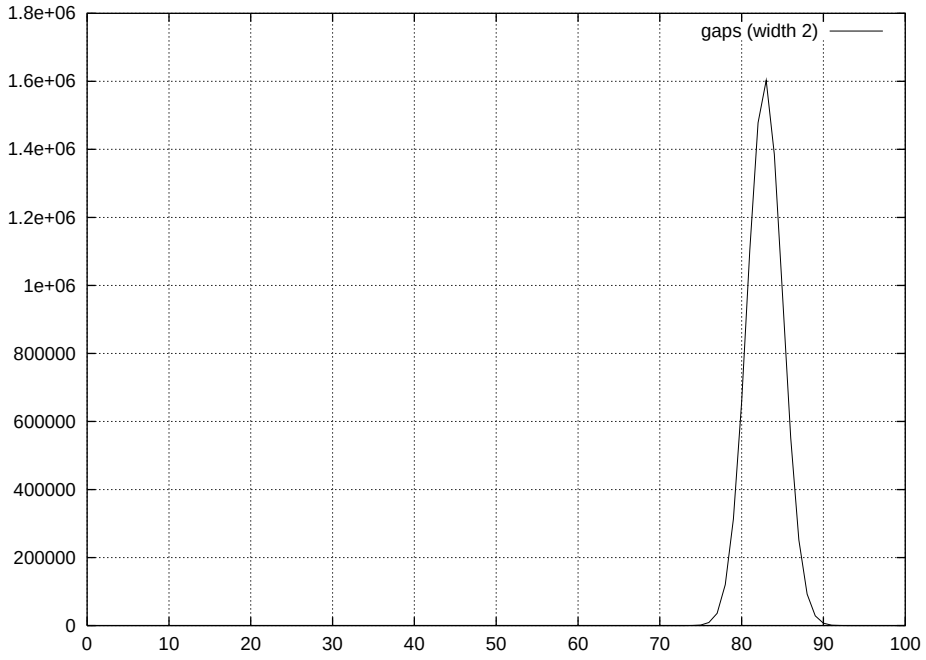

図 2: gaps (長さ 2) の分布

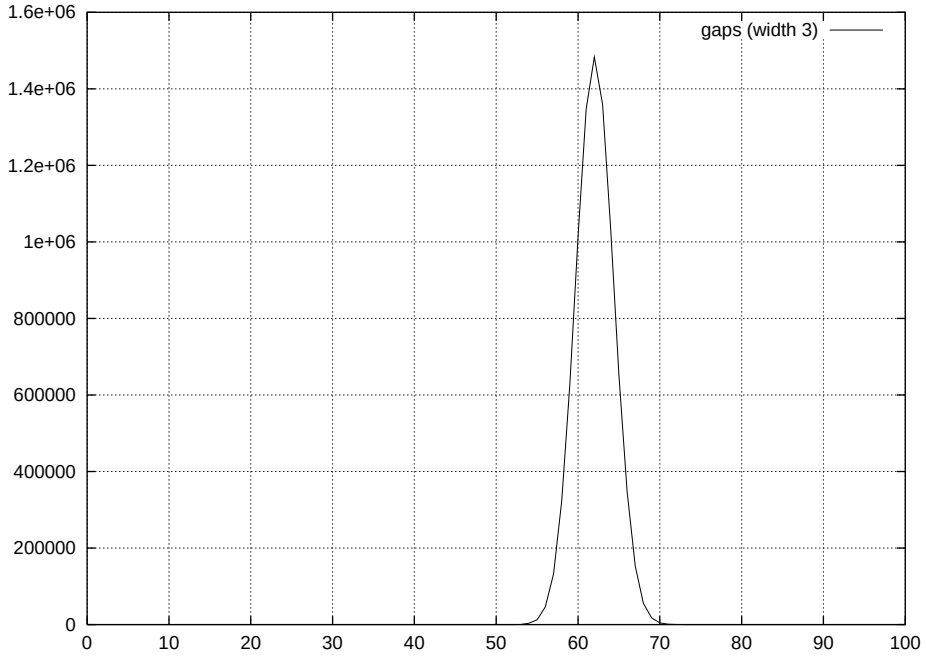

図 3: gaps (長さ 3) の分布

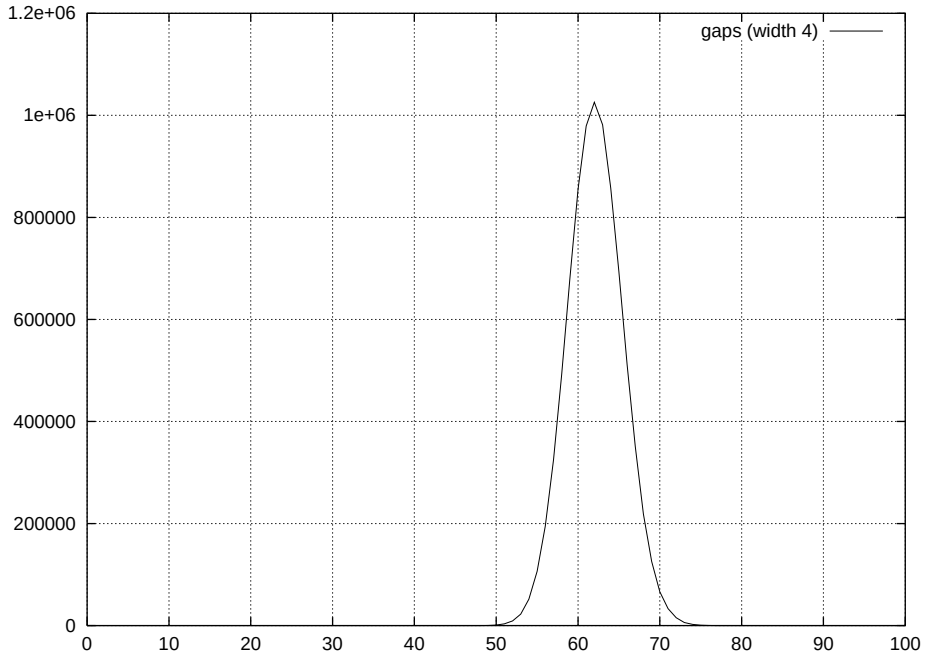

図 4: gaps (長さ 4) の分布

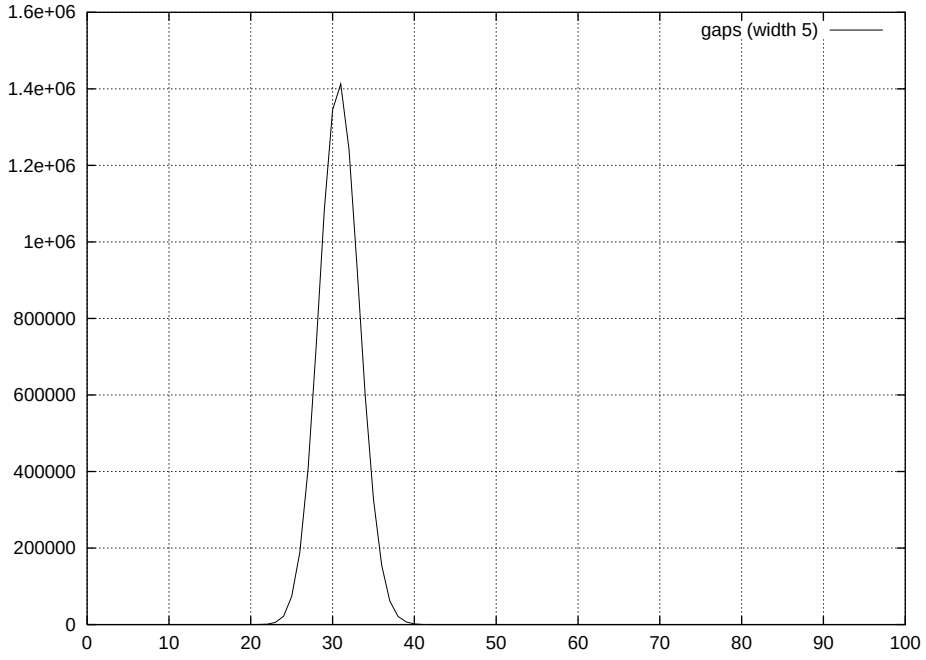

図 5: gaps (長さ 5) の分布

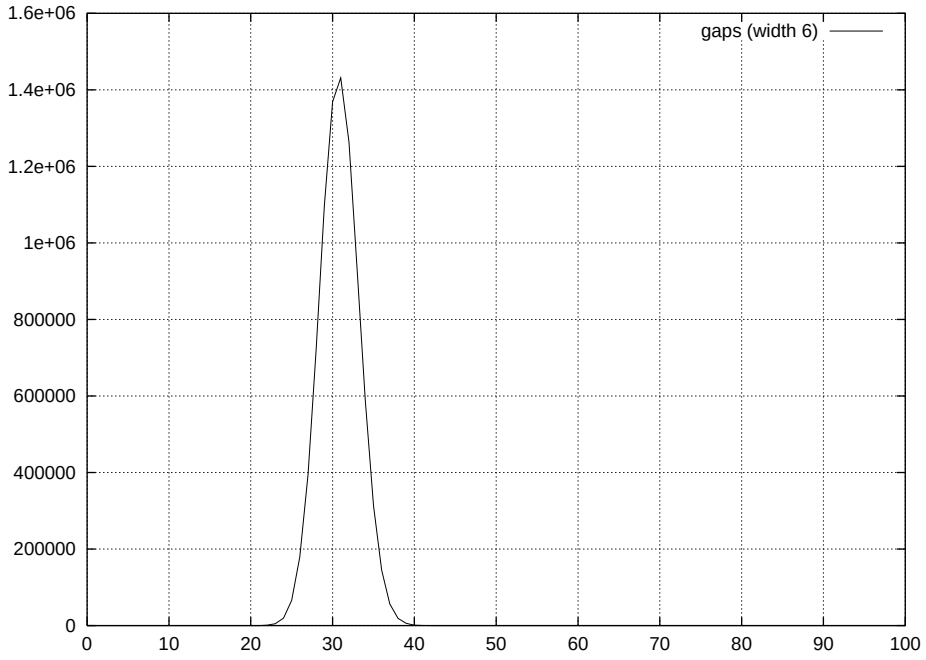

図 6: gaps (長さ 6 以上) の分布

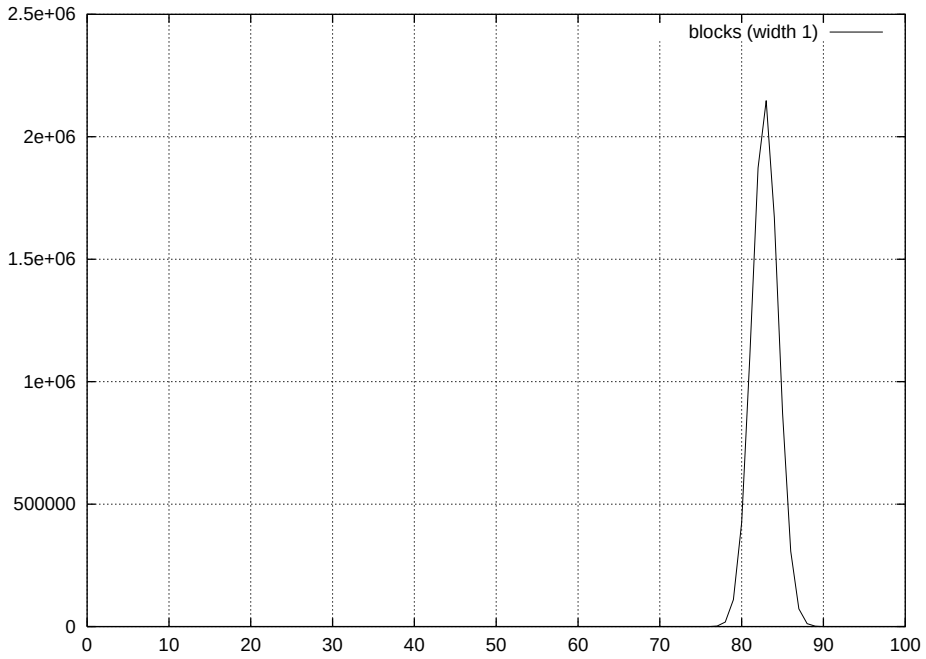

図 7: blocks (長さ 1) の分布

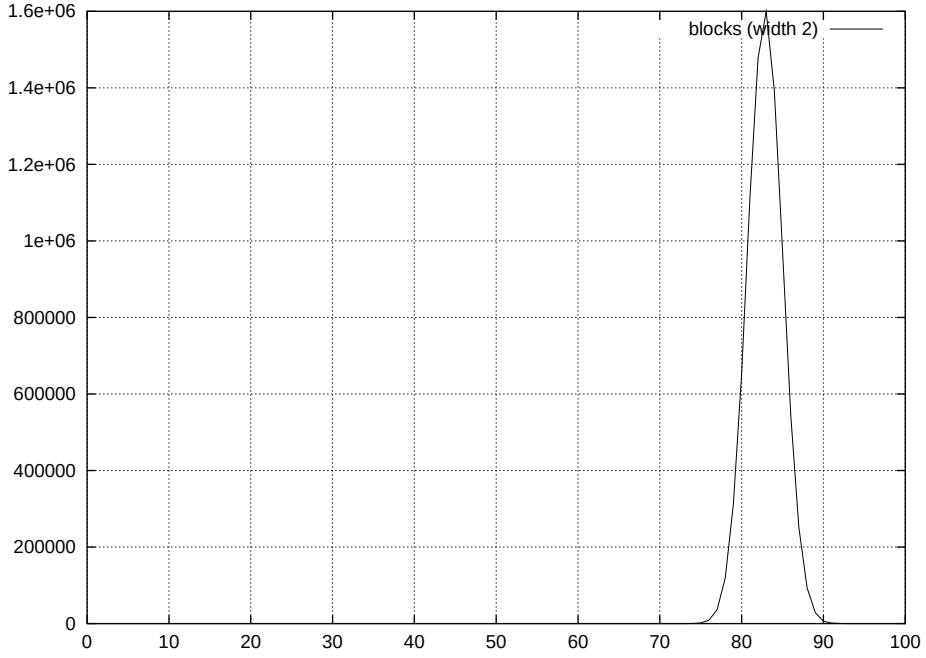

図 8: blocks (長さ 2) の分布

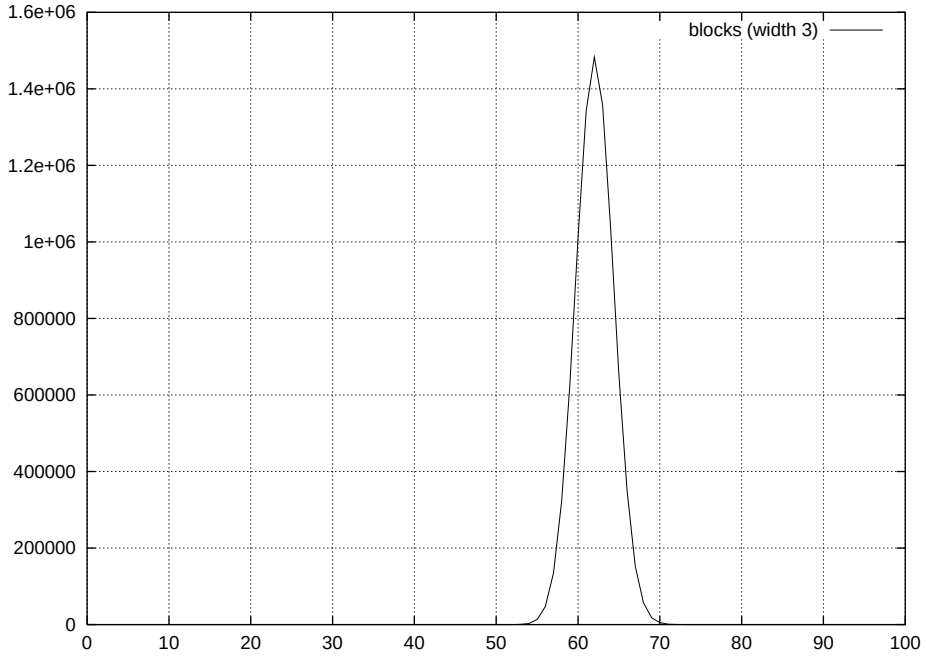

図 9: blocks (長さ 3) の分布

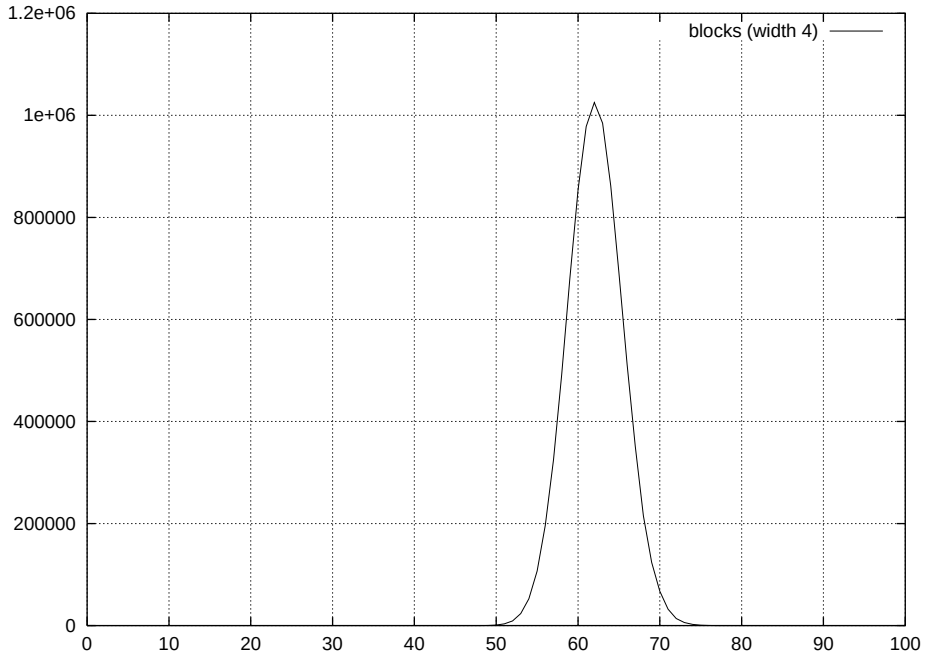

図 10: blocks (長さ 4) の分布

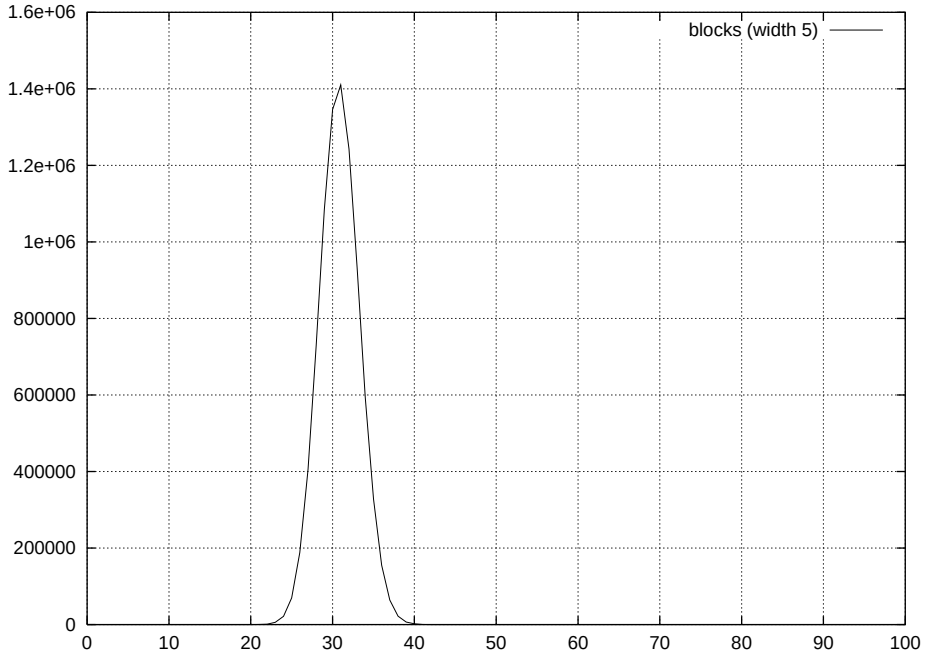

図 11: blocks (長さ 5) の分布

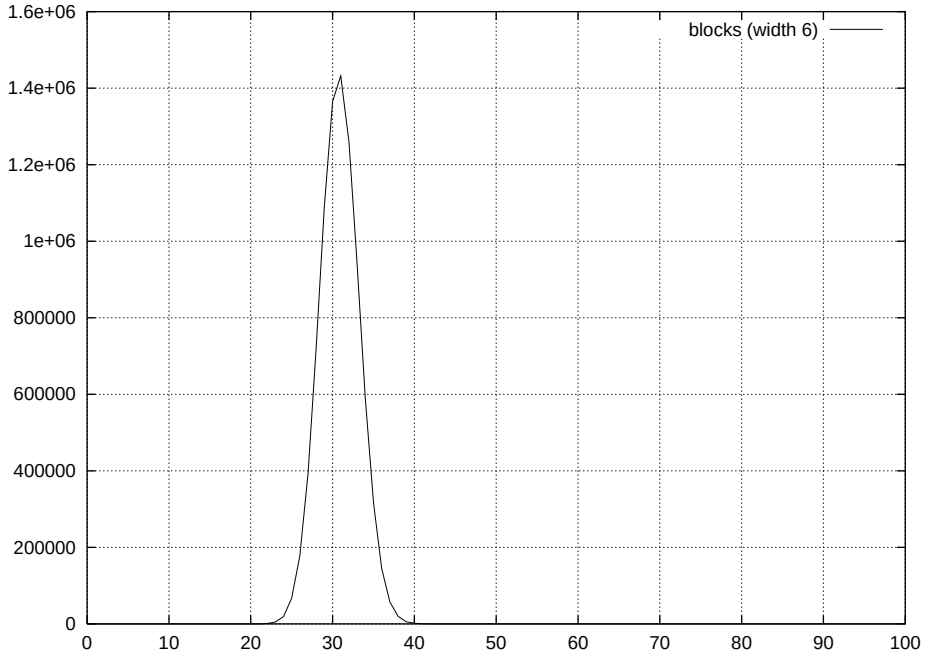

図 12: blocks (長さ 6 以上) の分布

異常が発生した例

フォーマットは下記の通り
1. # コメント
2. runs の長さ, gaps, blocks
(繰り返し)

パターン 1

```
#  cm06eda007ra001p-jpg.aa
1 2518 2479
2 1250 1427
3 642 597
4 303 265
5 166 153
6 83 48
7 44 46
8 18 15
9 9 4
10 8 7
11 2 2
12 1 3
13 2 0
```

パターン 2

```
#  cm0c1da007ra001pm0fb
1 2434 2405
2 1278 1245
3 606 575
4 307 403
5 147 190
6 84 69
7 35 29
8 25 18
9 16 4
10 2 1
11 5 2
12 2 0
13 1 1
```

パターン 3

```
#  cm0a5da008ra001pr281
1 2546 2741
2 1305 1145
3 639 609
4 293 316
5 157 143
6 71 85
7 40 31
8 24 13
9 9 7
10 7 6
11 4 1
12 4 0
13 0 1
14 0 1
```

パターン 4

```
#  cm0a5da008ra001pr282
1 2548 2743
2 1305 1148
3 641 607
4 293 316
5 157 143
6 70 85
7 41 31
8 24 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 5

```
#  cm0a5da008ra001pr283
1 2551 2742
2 1308 1147
3 639 610
4 293 317
5 157 143
6 69 85
7 40 31
8 24 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 6

```
#  cm0a5da008ra001pr284
1 2547 2739
2 1303 1145
3 641 607
4 293 317
5 157 144
6 71 85
7 40 32
8 24 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 7

```
#  cm0a5da008ra001pr285
1 2545 2741
2 1305 1146
3 642 608
4 296 317
5 157 143
6 69 85
```

```
7 40 31
8 24 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 8

```
#  cm0a5da008ra001pr286
1 2544 2741
2 1309 1146
3 638 608
4 296 315
5 156 143
6 70 87
7 40 31
8 24 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 9

```
#  cm0a5da008ra001pr287
1 2546 2742
2 1309 1149
3 642 609
4 293 315
5 156 143
6 70 85
7 40 31
8 24 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 10

```
#  cm0a5da008ra001pr288
1 2548 2740
2 1304 1150
3 641 606
4 296 316
5 156 144
6 71 85
7 39 31
8 24 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 11

```
#  cm0a5da008ra001pr289
1 2545 2739
2 1309 1143
3 639 608
4 293 318
5 156 145
6 71 85
7 39 32
8 24 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 12

```
#  cm0a5da008ra001pr290
1 2547 2740
2 1304 1146
3 637 607
4 295 318
5 158 143
6 70 85
7 40 31
8 25 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 13

```
#  cm0a5da008ra001pr291
1 2547 2744
2 1309 1143
3 639 609
4 293 316
5 156 143
6 70 85
7 41 32
8 24 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 14

```
#  cm0a5da008ra001pr292
1 2552 2743
2 1306 1149
3 638 607
4 295 316
5 156 144
6 70 85
```

```
7 40 31
8 24 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 15

```
#  cm0a5da008ra001pr293
1 2551 2739
2 1302 1144
3 639 608
4 294 317
5 157 145
6 70 85
7 40 32
8 24 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 16

```
#  cm0a5da008ra001pr294
1 2547 2743
2 1308 1145
3 639 610
4 294 316
5 156 143
6 71 85
7 40 31
8 24 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 17

```
#  cm0a5da008ra001pr295
1 2545 2736
2 1304 1147
3 640 607
4 294 319
5 157 143
6 70 85
7 40 31
8 25 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 18

```
#  cm0a5da008ra001pr296
1 2551 2741
2 1307 1149
3 637 606
4 296 318
5 156 143
6 69 86
7 40 31
8 24 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 19

```
#  cm0a5da008ra001pr297
1 2545 2736
2 1306 1149
3 639 608
4 294 317
5 157 143
6 70 85
7 40 31
8 25 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 20

```
#  cm0a5da008ra001pr298
1 2545 2736
2 1304 1145
3 637 607
4 295 317
5 156 143
6 71 85
7 41 31
8 24 14
9 9 8
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 21

```
#  cm0a5da008ra001pr299
1 2551 2739
2 1306 1146
3 639 606
4 293 319
5 155 144
6 70 87
```

```
7 40 31
8 24 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 22

```
#  cm0a5da008ra001pr300
1 2545 2740
2 1306 1144
3 641 610
4 294 316
5 156 144
6 71 85
7 40 31
8 24 13
9 9 7
10 7 6
11 3 1
12 4 0
13 0 1
14 0 1
```

パターン 23

```
#  cm031da013ra001pm016
1 2413 2497
2 1186 1239
3 603 574
4 345 311
5 234 158
6 71 77
7 40 38
8 17 16
9 12 8
10 2 6
11 6 3
12 1 1
13 0 0
14 0 1
15 1 1
```

パターン 24

```
#  cm034da013ra001pm02a
1 2631 2734
2 1322 1214
3 597 594
4 315 286
5 134 162
6 78 86
7 37 32
8 11 21
9 8 10
10 4 4
11 5 2
12 2 1
13 1 0
14 0 0
15 1 0
```

パターン 25

```
#  cm0f9da014ra001p-pdf.ar
1 2641 2734
2 1317 1246
3 616 602
4 312 296
5 146 159
6 60 63
7 43 41
8 19 15
9 9 3
10 5 6
11 2 2
12 0 1
13 0 0
14 0 0
15 0 0
16 0 1
```

パターン 26

```
#  cm0acda015ra001pr234
1 2616 2735
2 1217 1241
3 660 571
4 334 292
5 131 135
6 95 75
7 35 43
8 19 11
9 7 10
10 5 7
11 4 2
12 2 2
13 0 1
```

パターン 27

```
#  cm04cda018ra001pm0c5
1 2408 2473
2 1215 1242
3 595 623
4 404 285
5 173 154
6 80 75
7 28 39
8 17 25
9 6 6
10 7 10
11 2 2
12 3 1
13 0 1
14 1 2
```

パターン 28

```
#  ca350da020ra001pr284
1 2737 2555
```

```
2 1223 1325
3 577 657
4 320 292
5 141 141
6 70 85
7 35 32
8 17 19
9 6 10
10 1 9
11 2 1
12 1 3
13 0 2
14 1 0
```

パターン 29

```
#  ca350da020ra001pr288
1 2735 2557
2 1226 1325
3 578 659
4 318 292
5 141 140
6 71 85
7 35 32
8 17 18
9 6 10
10 1 9
11 2 1
12 1 3
13 0 2
14 1 0
```

パターン 30

```
#  ca350da020ra001pr292
1 2735 2553
2 1227 1323
3 577 661
4 317 294
5 142 140
6 70 85
7 35 32
8 17 18
9 6 10
10 1 9
11 2 1
12 1 3
13 0 2
14 1 0
```

パターン 31

```
#  ca350da020ra001pr293
1 2735 2553
2 1225 1324
3 579 660
4 317 293
5 140 140
6 71 85
7 35 33
8 17 18
9 6 10
10 1 9
11 2 1
12 1 3
13 0 2
14 1 0
```

パターン 32

```
#  ca350da020ra001pr297
1 2735 2555
2 1227 1325
3 578 658
4 318 294
5 140 140
6 71 85
7 35 32
8 17 18
9 6 10
10 1 9
11 2 1
12 1 3
13 0 2
14 1 0
```

パターン 33

```
#  ca350da020ra001pr298
1 2734 2555
2 1225 1325
3 579 659
4 317 292
5 141 140
6 72 85
7 35 32
8 17 18
9 6 10
10 1 9
11 2 1
12 1 3
13 0 2
14 1 0
```

パターン 34

```
#  ca293da021ra001pi201
1 2423 2253
2 1217 1282
3 584 663
4 333 316
5 157 168
6 72 87
7 44 45
8 16 20
9 8 17
10 4 4
11 2 4
12 2 4
13 2 0
14 0 0
15 0 2
```