擬似乱数生成の評価
連性テスト
PANAMA(MULTI-S01)編

平成 13 年 1 月 18 日

1 取得条件

FIPS 140 と同様に 20000 bits をサンプリングして，その中で同一 bits (gaps, blocks) の長さを評価する．長さは 1,2,3,4,5,6 以上の 6 通りに分割し，各々の出現頻度を評価する．FIPS 140 を合格する条件は全てのサンプルに対して， 1,2,3,4,5,6 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「PANAMA の評価に利用した鍵の種類」にある組み合わせ (秘密鍵を 999 通り，乱数列番号を 100 通り) を対象とし，各々の出力の先頭 20000bits を対象に評価を行った．

つまり，このテストでは計約 10 万件のテストを行ったことになる．

2　テスト結果

テスト結果の一部を示す．左から順に bits 数，0 ビットの数，1 ビットの数である．

01, 2574, 2560
02, 1271, 1262
03, 659, 631
04, 302, 307
05, 135, 165
06, 64, 81
07, 38, 33
08, 13, 19
09, 12, 11
10, 3, 3
11, 4, 3
12, 0, 1
13, 0, 0
14, 0, 0
15, 1, 0
01, 2467, 2491
02, 1261, 1287
03, 672, 608
04, 319, 288
05, 127, 159
06, 86, 89
07, 38, 46
08, 15, 13
09, 6, 11
10, 5, 5
11, 2, 3
12, 1, 0
13, 3, 1
14, 0, 1
01, 2539, 2439
02, 1246, 1247
03, 635, 673
04, 308, 314
05, 145, 170
06, 57, 74
07, 40, 38
08, 16, 26
09, 10, 15
10, 4, 3
11, 2, 2
12, 0, 1
13, 0, 0
14, 0, 0
15, 1, 1

次に，以下に度数分布を示す．

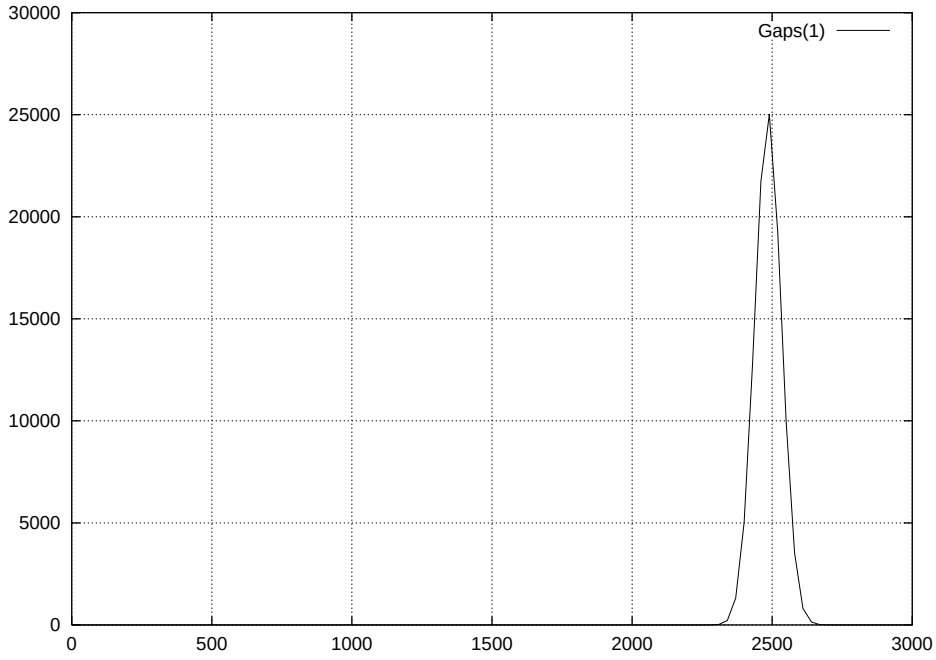

図 1: 長さ 1 の OFF bit(=0) の度数分布

3 評価

約 10 万件全ての検査結果は FIPS 140 の条件をクリアした．連性テストに関しては，擬似乱数の条件を満たすと判断する．

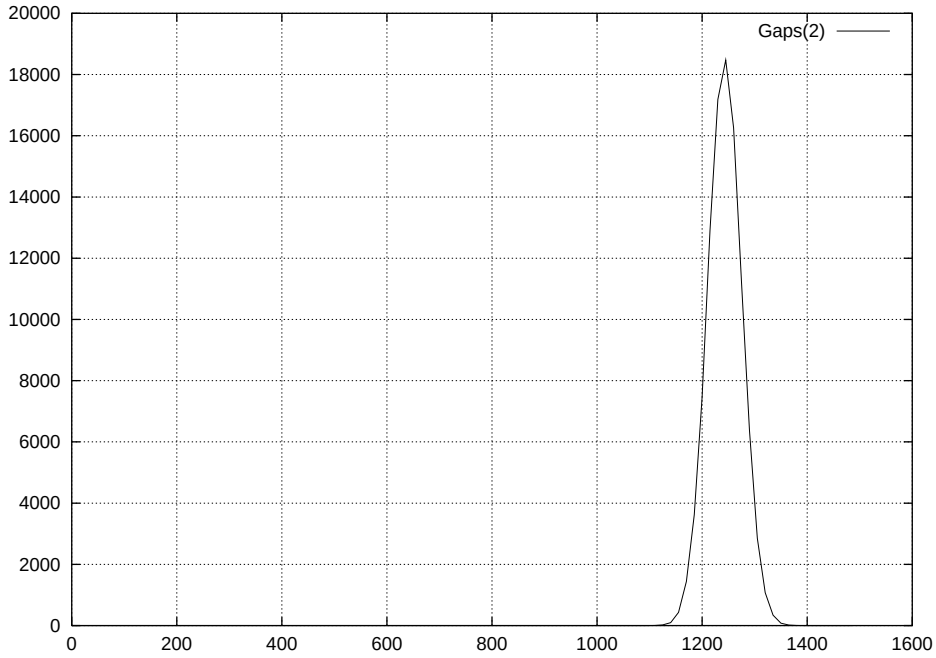

図 2: 長さ 2 の OFF bit(=0) の度数分布

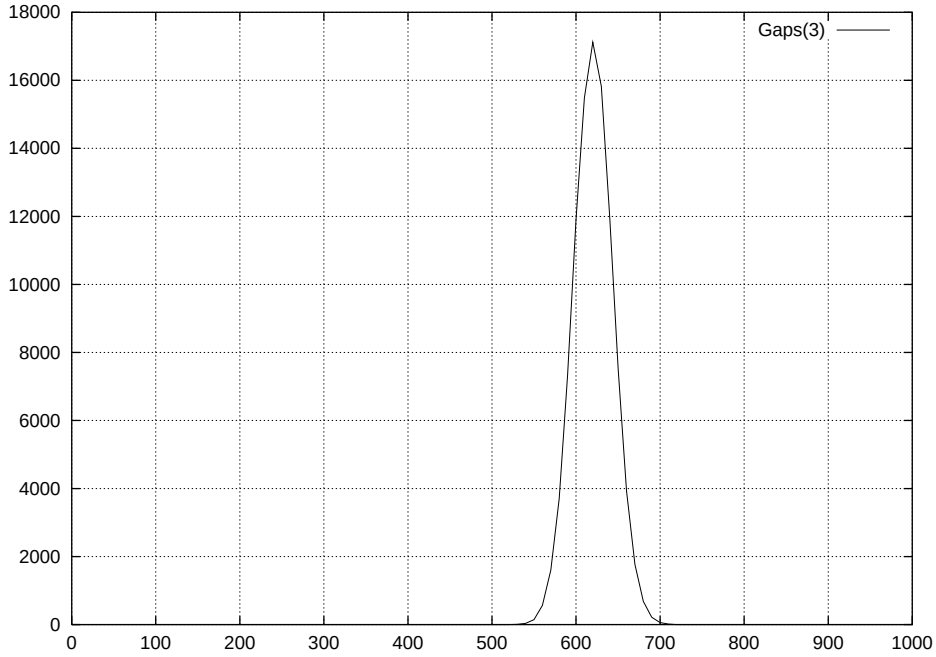

図 3: 長さ 3 の OFF bit(=0) の度数分布

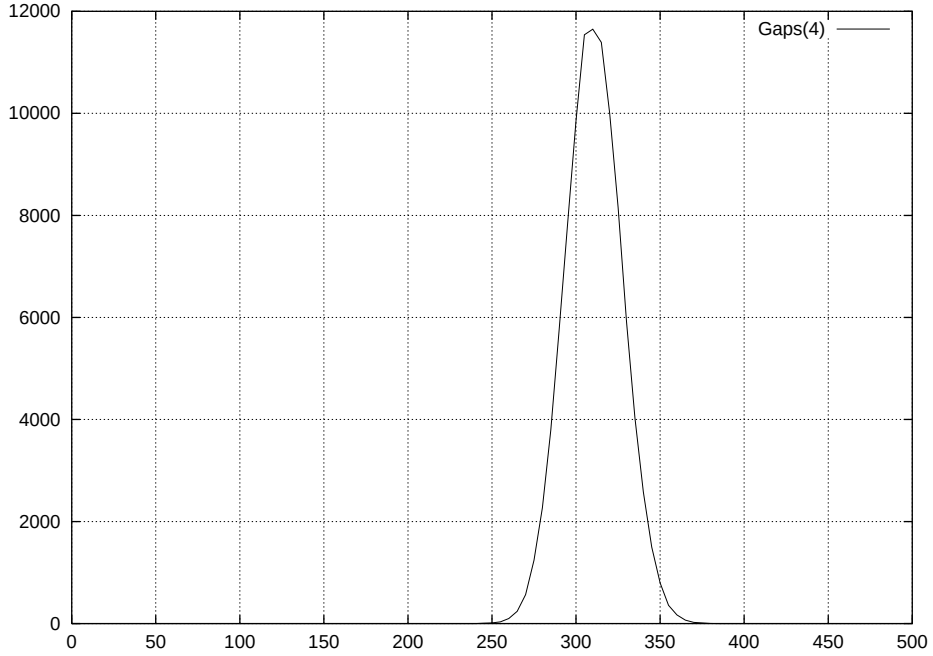

図 4: 長さ 4 の OFF bit(=0) の度数分布

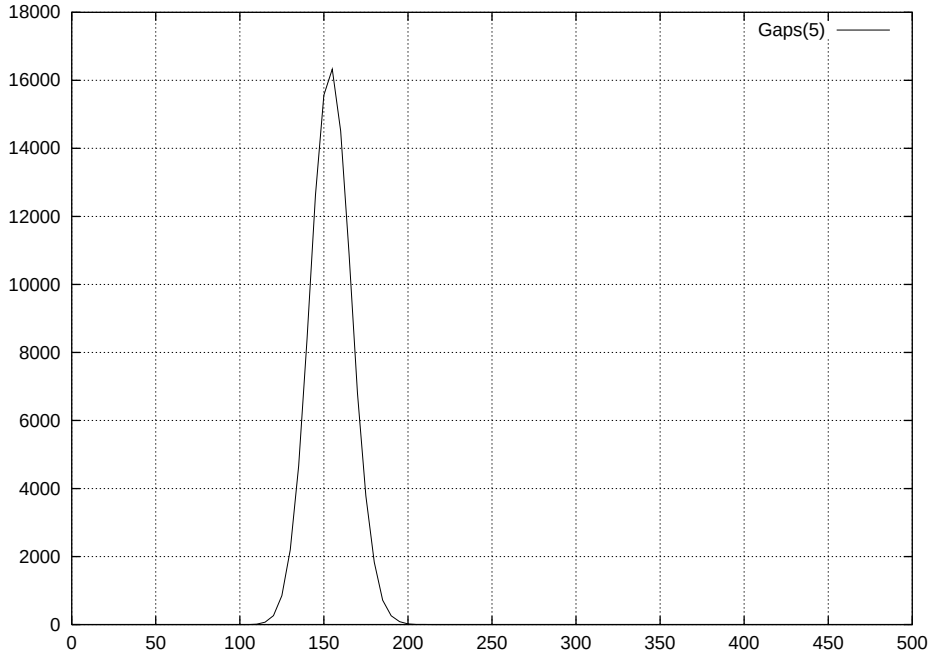

図 5: 長さ 5 の OFF bit(=0) の度数分布

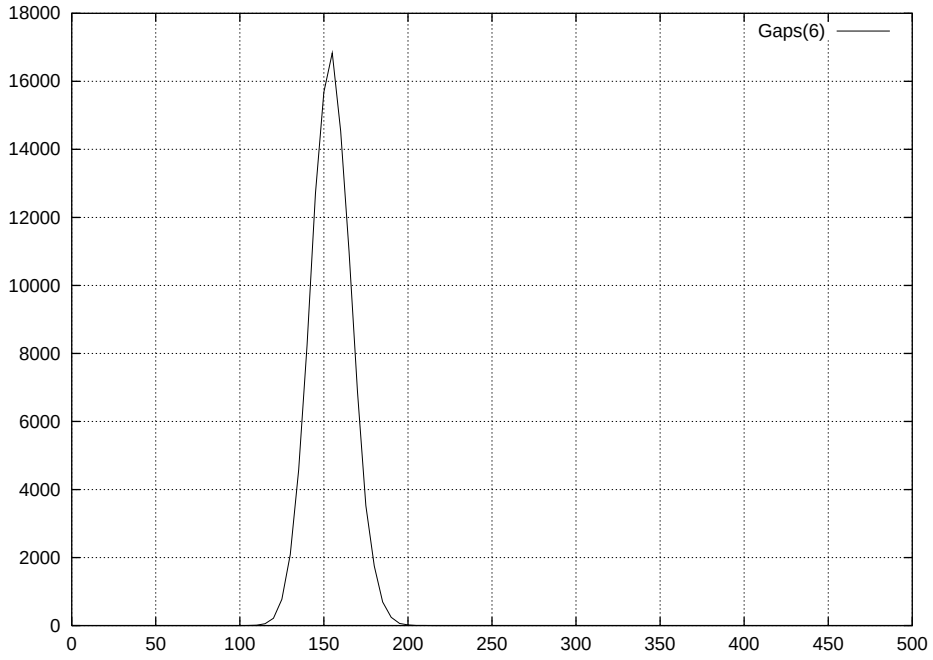

図 6: 長さ 6 以上の OFF bit(=0) の度数分布

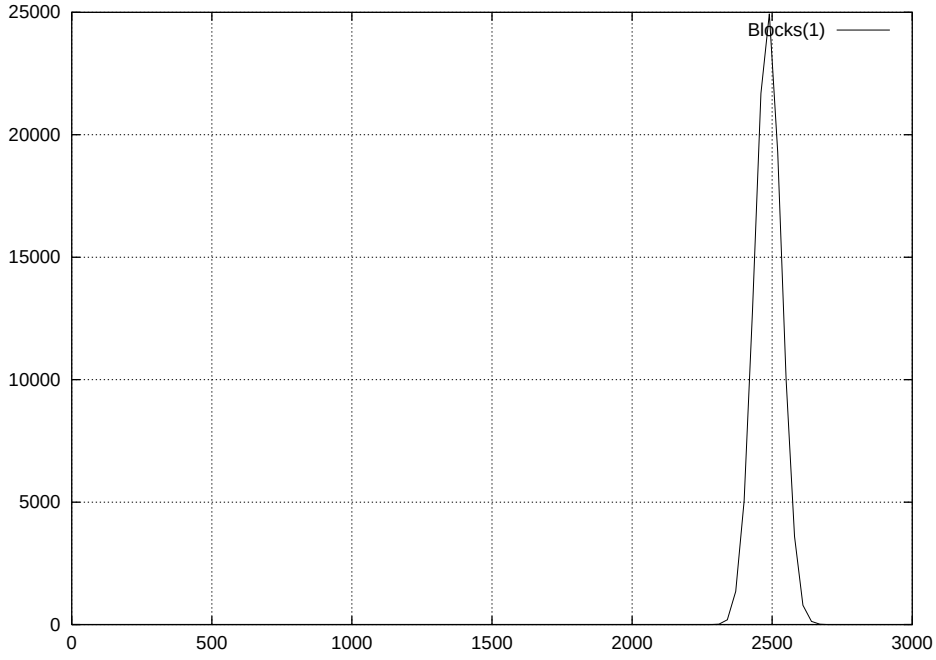

図 7: 長さ 1 の ON bit(=1) の度数分布

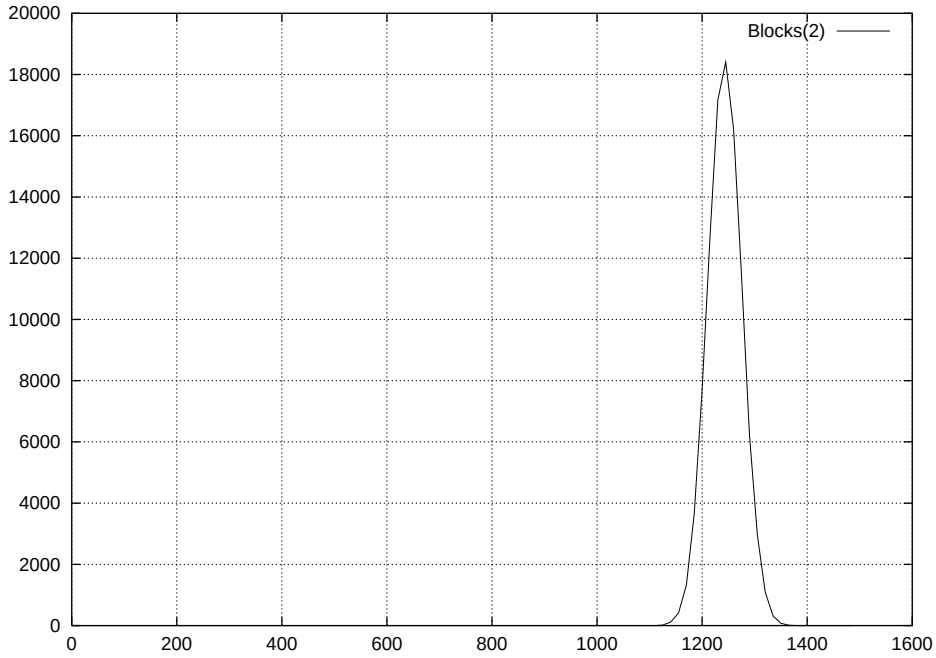

図 8: 長さ 2 の ON bit(=1) の度数分布

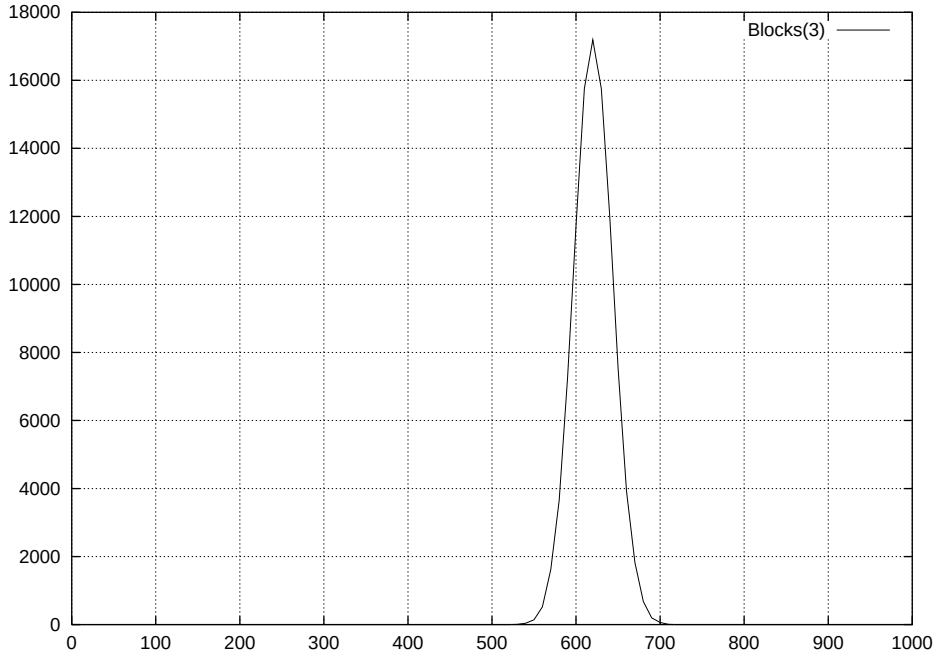

図 9: 長さ 3 の ON bit(=1) の度数分布

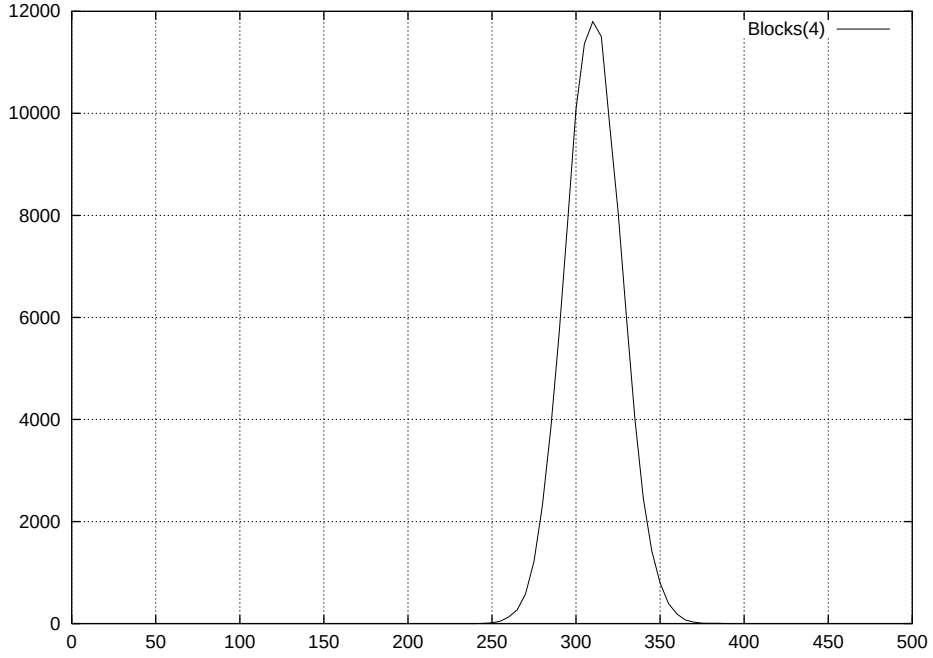

図 10: 長さ 4 の ON bit(=1) の度数分布

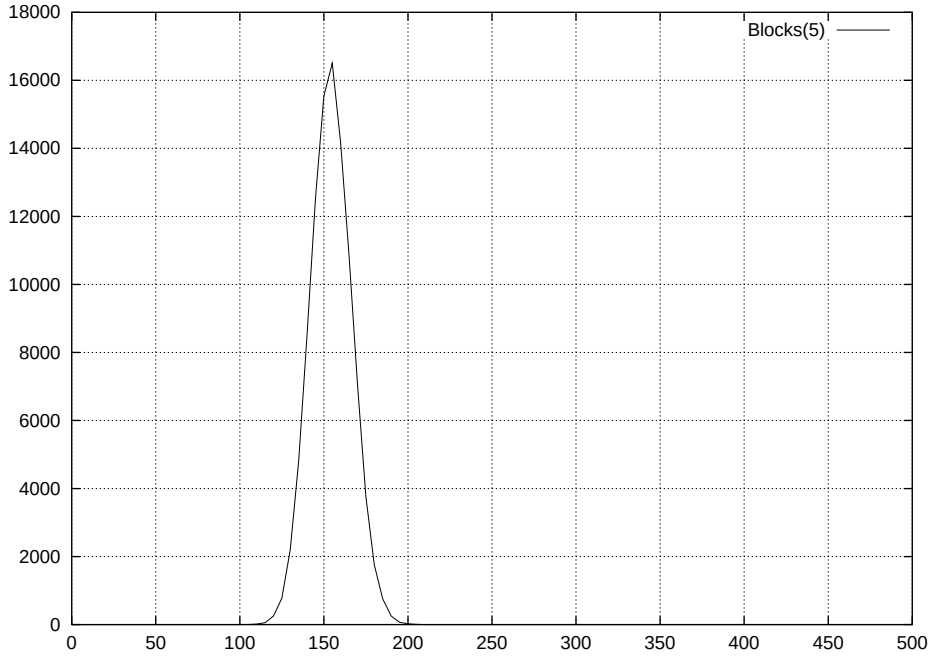

図 11: 長さ 5 の ON bit(=1) の度数分布

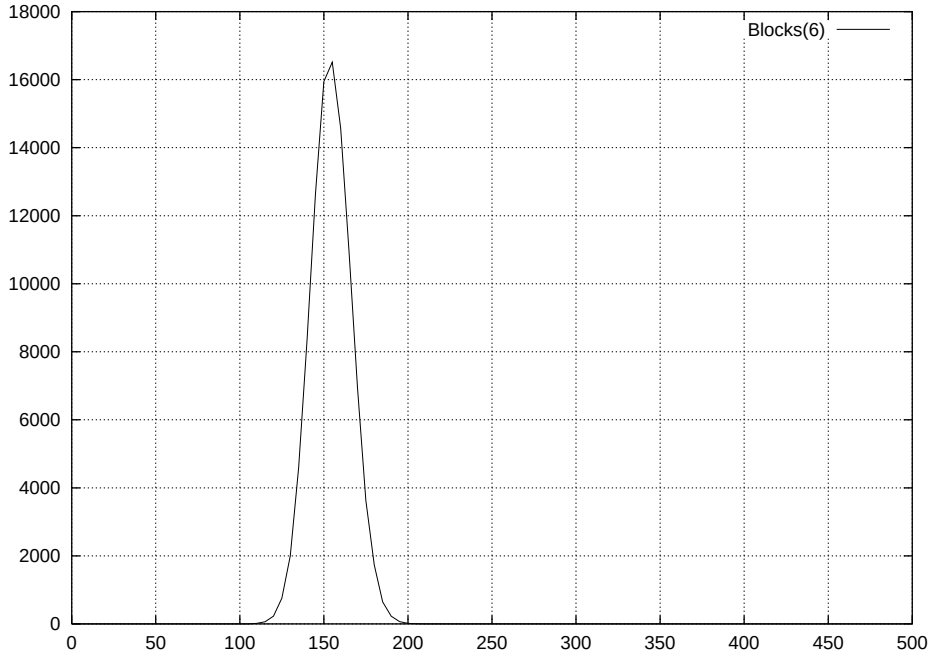

図 12: 長さ 6 以上の ON bit(=1) の度数分布