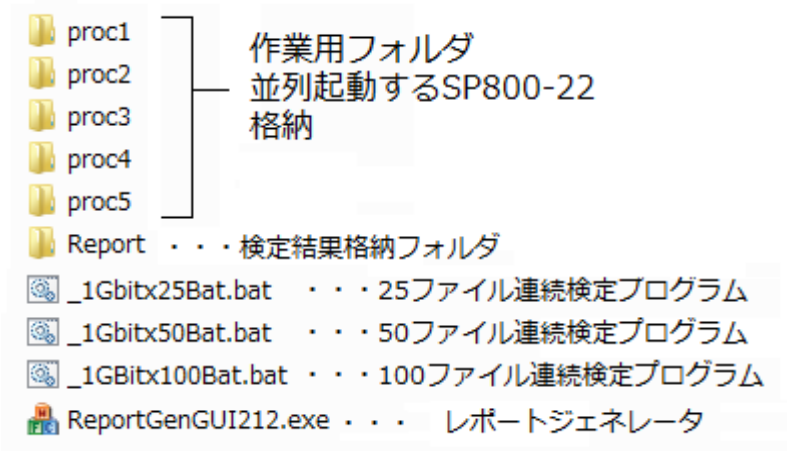
SP800-22 STS 2.1.2 x 100 説明書

1. 全体の構成



レポートジェネレータ以外は BAT ファイルで記述しています。

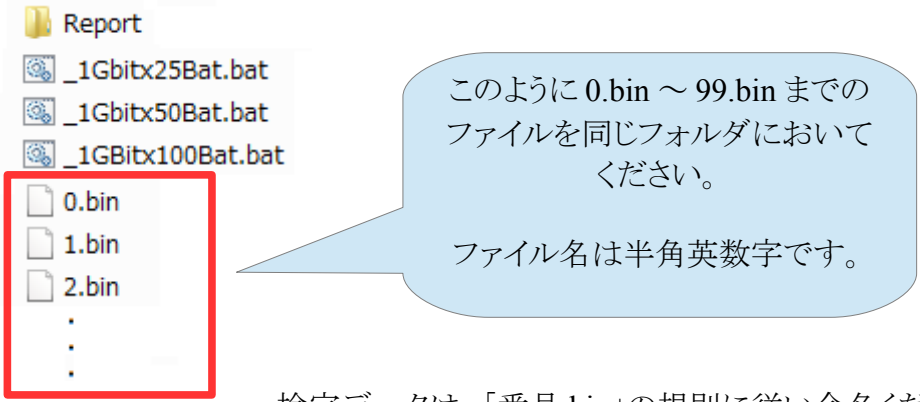
2. 100 ファイルの連続検定

2.1 掃除

Report　　**Report フォルダを消すか名前を変えてください。**

前回のレポートデータが残っていると結果がまざる場合があります。

2.2 乱数ファイルを用意



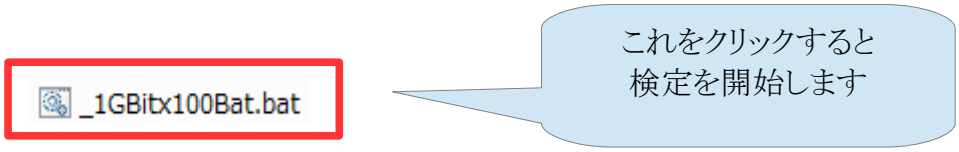
検定データは、「番号.bin」の規則に従い命名ください。

ファイルは **1GBit(125MB)のバイナリファイル**で用意ください。

余裕を持ち少し大きめにすると安全です。

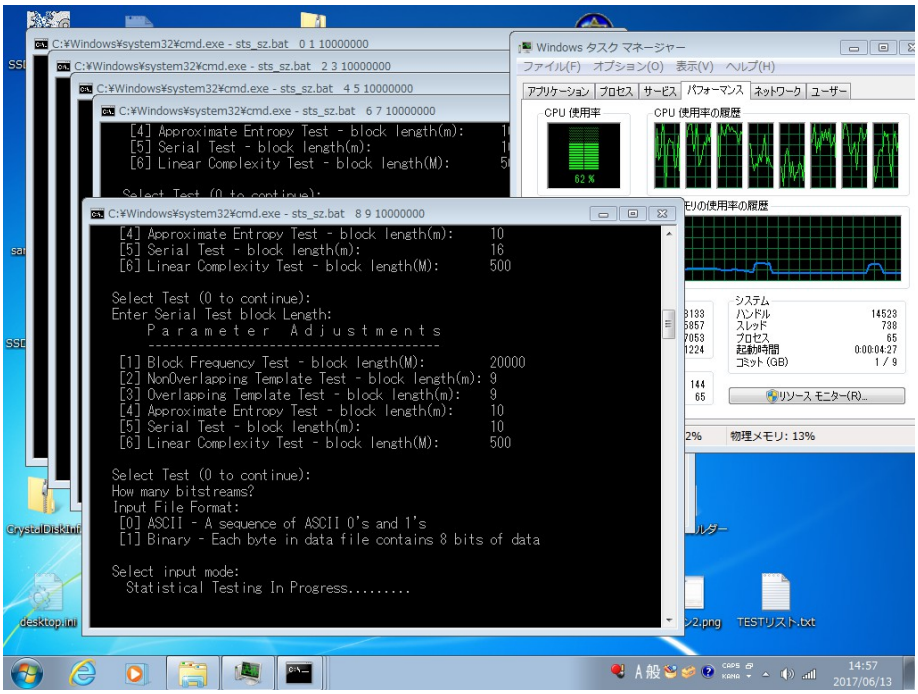
1K バイトを 1000 とするか 1024 とするかの解釈が混乱があるので 1024 にすると安心です。

2.3 検定開始

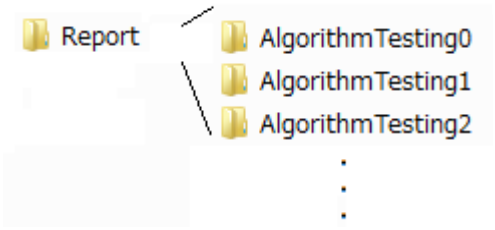


次の画像のように5つの SP800-22 が並行起動して計算を始めます。

30 時間ほどお待ちください Zzzz・・・。



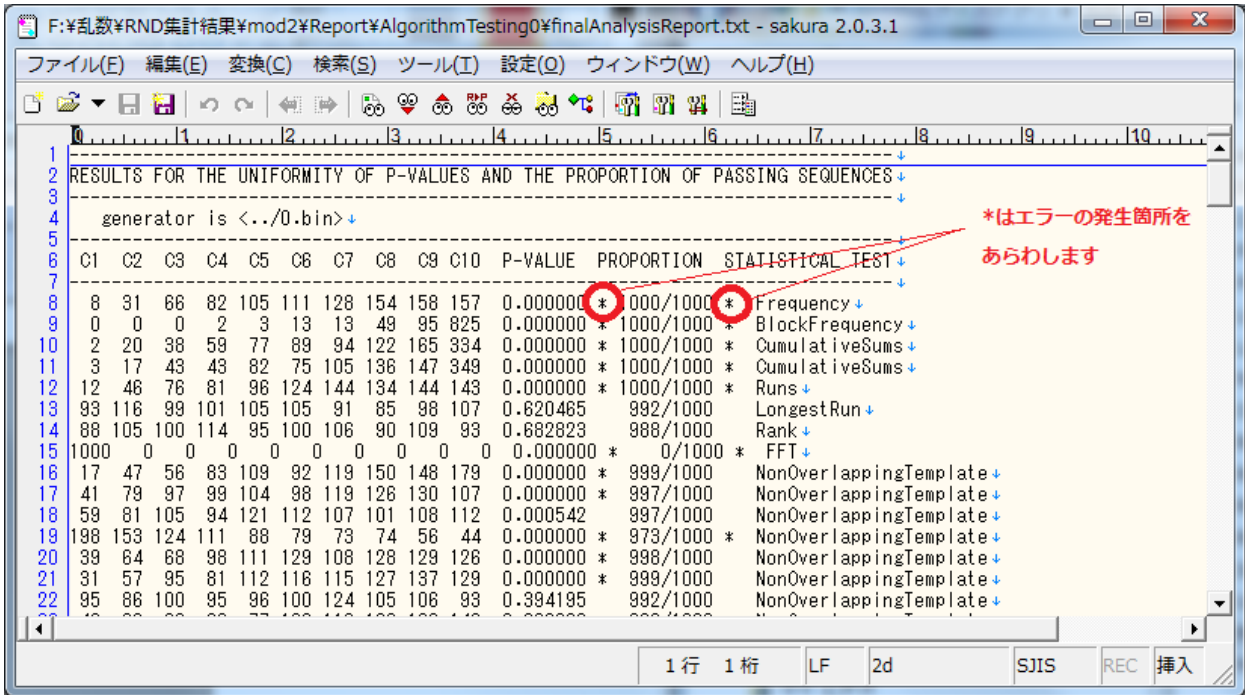
2.4 検定終了



検定結果は Report フォルダの下にこのように出来ます。

検定したファイルの数だけできます。

このファイルは Unix 系ファイルなので改行が LF コードです。LF に対応したエディタ／ワープロで開いてください。



これはフリーウェアのサクラエディタで開いたところです。

3. レポートジェネレータ／自動分析プログラム

100本の検定結果を個別に確認していたら大変です。

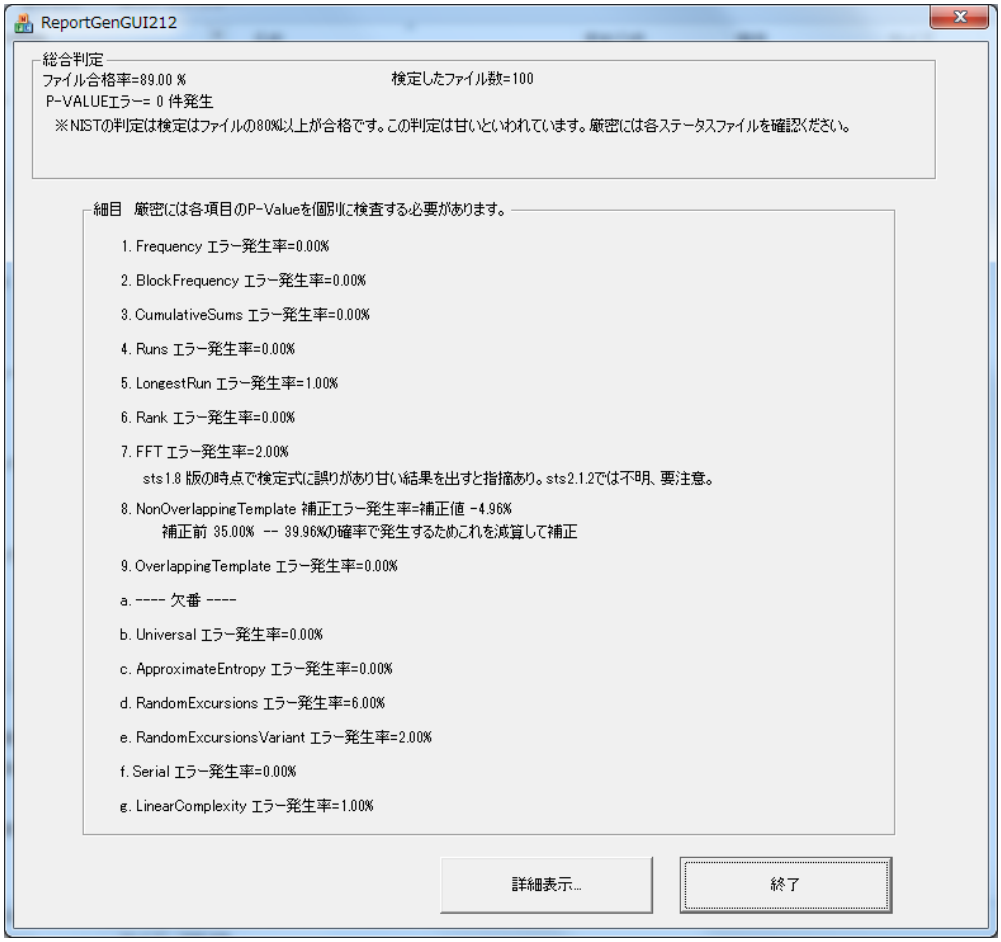
ここではレポートジェネレータが活躍します。

ReportGenGUI212.exe ・・・ レポートジェネレータ

これをクリックすると
自動分析開始

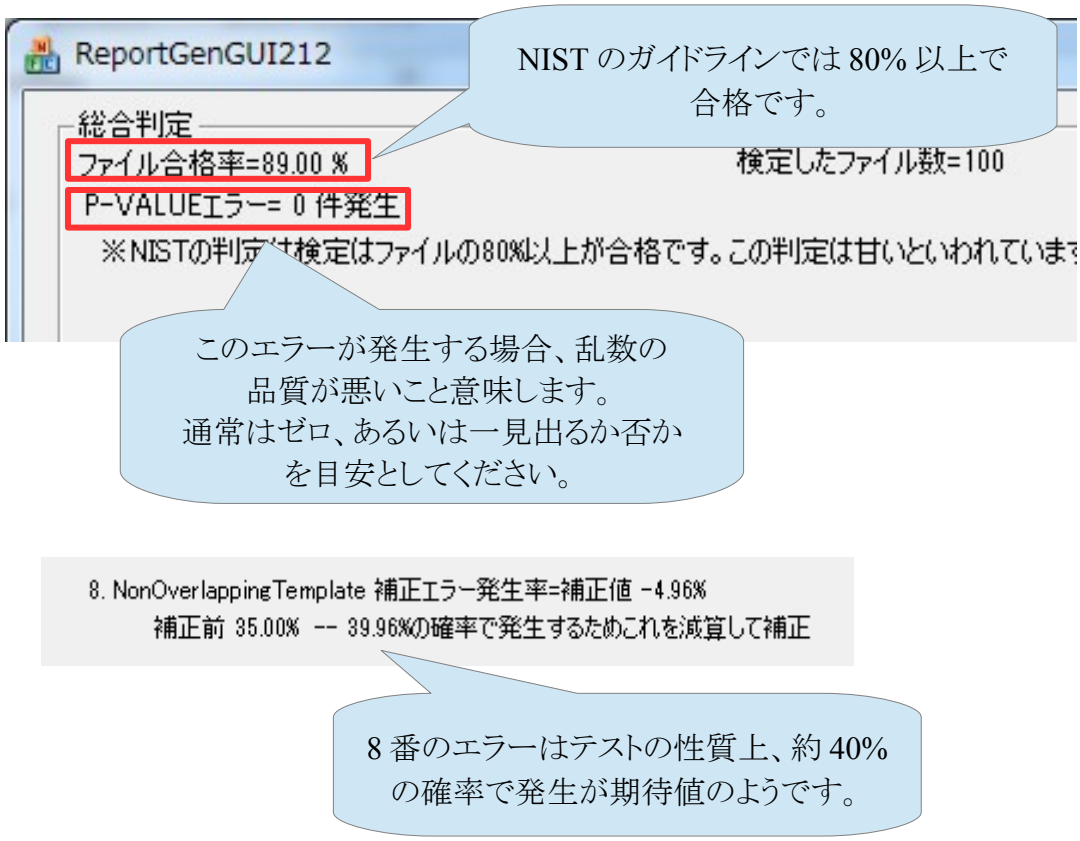
起動後処理に1～2分かかります。お待ちください。

さすがに検定結果100ファイル＋各個別ファイル合計 3000 個の集計には時間がかかります。



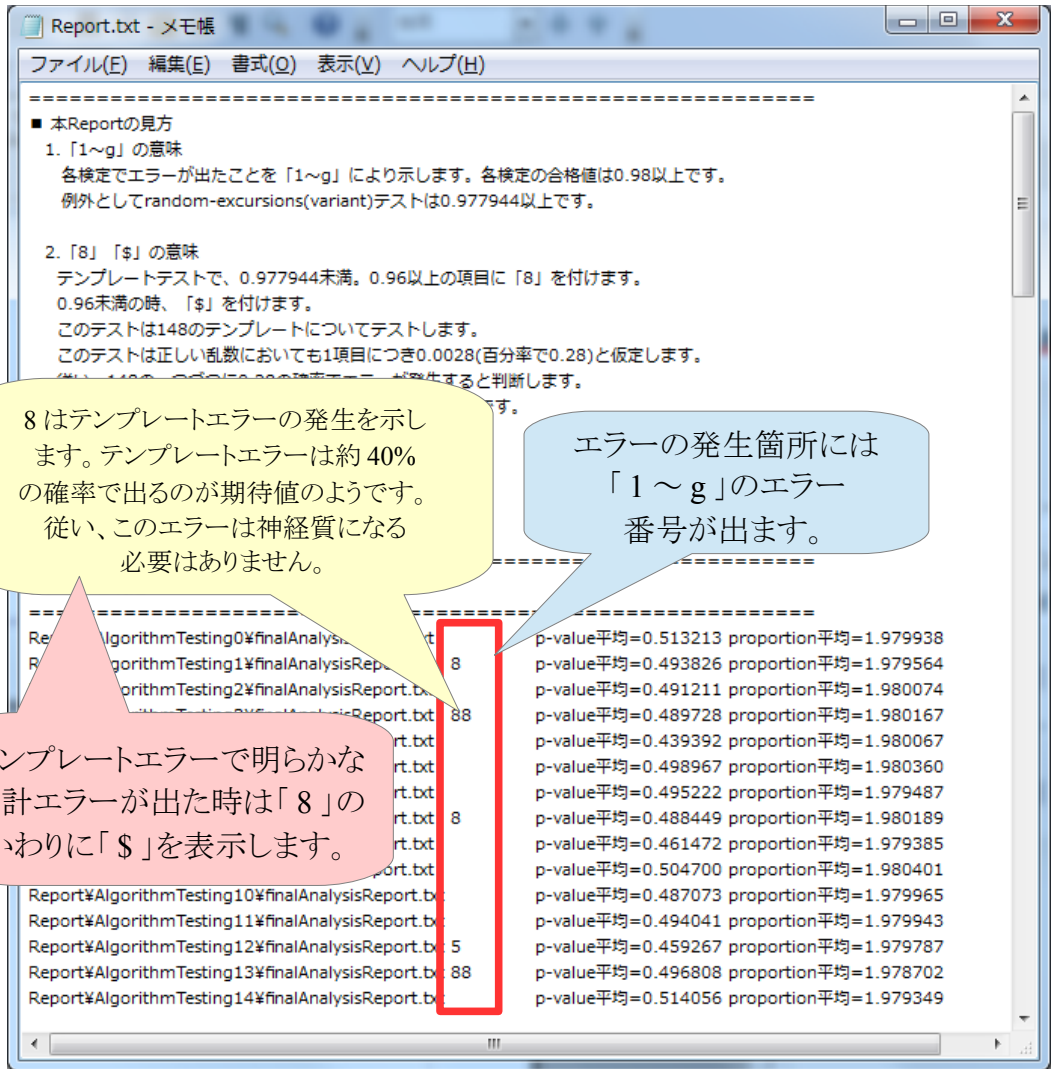
集計が終わるとレポート画面を出します。

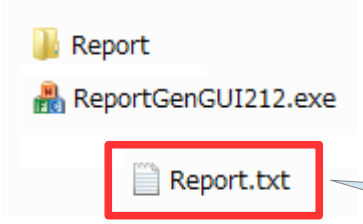
3. 1. レポートの簡単な見方



100 ファイルの検定を行い、ファイル合格率 80%以上、P-VAUE エラーがゼロあるいは1で合格と判断してください。

エラー発生箇所の詳細を知りたい時はこのボタンを押してください。どの検定ファイルでエラーが出たかわかります。





レポートジェネレータはカレントフォルダにある Report の中を自動検索して集計します。

詳細結果は同じフォルダに保存します。

4. 仕様

SP800-22 に指定するパラメータ

各パラメータは BAT ファイルで変更できます。詳細は BAT ファイル参照。

本ソフト出荷時は次の構成としています。

・1000 本　×　1000,000 ビット長のストリームで処理

・Frequency の数値は 20000

・LOngest Run of Ones の数値は 10

・これ以外の設定は SP800-22 の規定値

5. 弊社への問い合わせ

http://dnki.co.jp/w2/2017/06/14/nist_sp800-22sts212/

本ソフトの配布希望の窓口にカスタム希望とメールをください。

連続検定とレポートジェネレータは弊社でも業務でひつようなので適時改良していきます。