# Fractal File Cryptographer 2.0 マニュアル

鈴置友也 (cso237taeb)

2014 年 6 月 28 日

# 目次

# 第 1 章

# Fractal File Cryptographer 2.0 について

## 1.1 はじめに

このプログラムは、ファイルの暗号化と復号化を行うツールです。

次のような特徴があります。

① フラクタル関数によるシームレスなキーにより、ファイル長に左右されず、キーを反復することなくエンクリプトすることにより、暗号化ファイルの解析を難しくします。

② それに加えて、従来の 256 バイトのテーブルを使用した暗号化も多重処理することにより、より複雑な暗号化結果を返します。

③ CRC チェックなどを敢えて行わない様にすることにより、パスワード解析ソフトなどをつかったパスワード解析を不可能にし、セキュアな暗号化が可能になります。

④ マイナーな暗号化ソフトを使用することにより、暗号化されたファイルを可能な限り秘密に管理することができます。

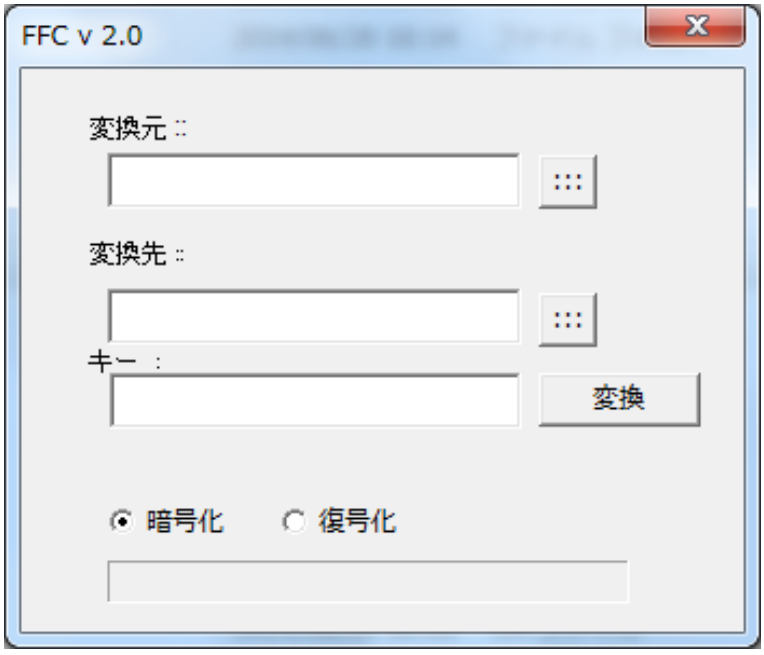
⑤ コマンドライン・インターフェイスも装備しているので、スクリプトからの呼び出しも可能です。

# 第 2 章

# FFC を実行する

## 2.1　起動画面

FFC.exe をダブルクリックしてください。こんな画面が出るはずです。




・変換元 の欄には暗号化／復号化したいファイルのパスを入力します。

・変換先 の欄には暗号化／復号化した結果のファイルのパスを入力します。

・キー 暗号化に使用するキーを設定します。実際の暗号はこの値に基づきフラクタルの暗号を生成するシードになります。

・暗号化／復号化 ファイルを暗号化する場合には [暗号化] を、復号化するには [復号化] を選択します。この値を誤るとデータを破壊しますの慎重に選択してください。

・変換 で暗号化／復号化を開始します。

# 第 3 章

# テスト結果

## 3.1　エンクリプション・テスト

例えば、次のようなテキストを暗号化するとします (test.txt)。

hi this is a test これはテストです!!
これを暗号化する前と、暗号化した後でダンプをとった結果は、次のようになります。

```
DUMP v0.1 by Tomonari Suzuoki
DUMP file :test.txt
-------------------------------------------------------------------------------
Address|00|01|02|03|04|05|06|07|08|09|0A|0B|0C|0D|0E|0F|SUM+0123456789ABCDEF+
-------------------------------------------------------------------------------
000000:  68 69 20 74 68 69 73 20 69 73 20 61 20 74 65 73 592 hi this is a tes
000010:  74 0D 0A 82 B1 82 EA 82 CD 83 65 83 58 83 67 82 7A8 t これはテスト・
000020:  C5 82 B7 21 21 0D 0A 82 CD 83 65 83 58 83 67 82 6D5 す!!  はテスト・
-------------------------------------------------------------------------------
page :1
DUMP v0.1 by Tomonari Suzuoki
DUMP file :test.txt.ffc
-------------------------------------------------------------------------------
Address|00|01|02|03|04|05|06|07|08|09|0A|0B|0C|0D|0E|0F|SUM+0123456789ABCDEF+
-------------------------------------------------------------------------------
000000:  53 B0 39 DC 67 C0 8C 1C 81 4A 0F 8A DF 64 3E 89 755 S9g・゛ 玩 d>・
000010:  32 79 E7 45 DB 0D 92 46 60 DF 11 17 A4 A8 88 3E 710 2y 憂 巽 ‘ ・
000020:  B0 F1 B2 FA 54 30 7D 46 60 DF 11 17 A4 A8 88 3E 80D     0}F‘ ・
-------------------------------------------------------------------------------
page :1
```

何度か出てくる T の文字、スペース、s,i などの文字列も、単純テーブル変換では同じ値になりますが、フラクタルキーによって暗号化されているので同一文字でも値が変わっています。
このテキストを他のキーでエンクリプトした場合には次のようになります。

```
DUMP v0.1 by Tomonari Suzuoki
DUMP file :test.txt.ffc
-------------------------------------------------------------------------------
Address|00|01|02|03|04|05|06|07|08|09|0A|0B|0C|0D|0E|0F|SUM+0123456789ABCDEF+
-------------------------------------------------------------------------------
000000:  D8 B6 32 79 CE D2 1C DF 38 53 EE 09 67 BE BC 4D 884 2y 8S・gM
000010:  82 2A 83 00 F7 91 39 A5 90 80 0F 77 64 13 99 41 67C ・・  9 逗 wd 僊
000020:  5B 06 92 22 FF F0 E9 A5 90 80 0F 77 64 13 99 41 779 [ ・  逗 wd 僊
-------------------------------------------------------------------------------
```

値がキーによって全く変わっていることに気づくと思います。
暗号化キーはファイルの復号に必要なりますので、紛失しないように、必ず大切に保管するようにお願いします。キー紛失によるデータの破壊等のお問い合わせはご遠慮ください。

# 第 4 章

# 詳細なガイド

## 4.1　FFC.exe コマンドライン

FFC はコマンドプロンプトから読み出して使うことができます。書式は、以下のようになります。

FFC.exe d または e パスワード 変換元ファイル 変換先ファイル

・最初の第 1 引数はスイッチです。e で暗号化、d で復号化を行います。

・第 2 引数はパスワードを指定してください。スペースを含むパスワードは使用できません。

・第 3 引数は暗号化／復号化するファイルを指定します。

・第 4 引数は保存する変換先ファイルを指定します。この値は省略できます

## 4.2　このソフトについて

本ソフトウェアはフリーウェアです。ソースは公開しません。

## 4.3　ご連絡

このソフト使用中に発生した障害について、わたくしは如何なる責任を負うものでもありません。AS IS でお願いします。

CsO237(taeb) こと鈴置友也 (cso236@gmail.com)