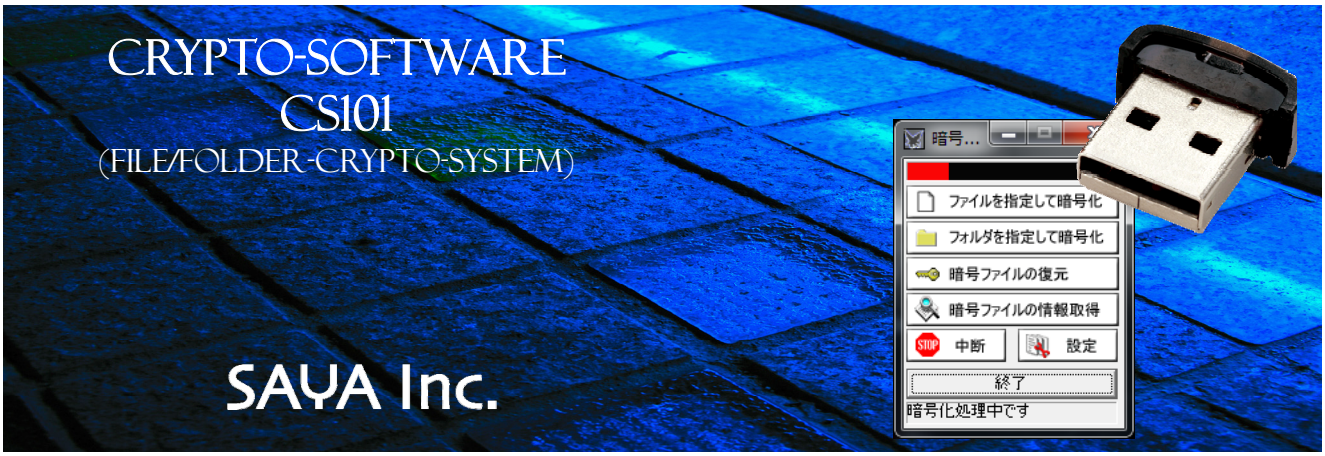


目次

1.概要

本ソフトウェアは、極めて強固なエヌクリプト社製暗号アルゴリズムを搭載した、ファイル及びフォルダ暗号圧縮ソフトウェアです。本製品の暗号アルゴリズムには以下の特徴があります。

暗号アルゴリズムの特徴

エントロピー制御

平文（元ファイル）のエントロピーに依存せず、暗号化ファイルのエントロピーを一定の目標値に制御します。更に同じ平文を暗号化した場合でも毎回異なる結果になります。また、0 が続くような単純なパターンの平文を暗号してもパターン性のない複雑なファイルになります。

既存の暗号アルゴリズムを多数内蔵

一般的な暗号アルゴリズムを複数実装しており、独自の暗号アルゴリズムを組み合わせ、様々な暗号アルゴリズムのメリットを共有します。内部に組み込まれている暗号アルゴリズムは最低 7 種類に及び、これらの組み合わせて暗号化します。

暗号鍵に関する独自のアルゴリズム

鍵の非転送、多重鍵、可変長鍵などを組み合わせ、暗号強度のボトルネックになる鍵についての問題にも切り込んでいます。

独自の非線形暗号アルゴリズム

再現性や周期性の殆ど存在しない強固な暗号アルゴリズムを随所に導入しています。

パスワードのみに依存しないセキュリティ

専用の USB デバイスが暗号紋（個性）の役割を果たしており、パスワードが一致しても、この USB デバイスがないと暗号が解除できない仕組みです。この USB デバイスは 1 台 1 台に暗号紋（個性）が割り振られており、同じモノが存在しません。

優れたセキュリティポリシーと使い勝手

暗号ファイルの復元期限（賞味期限）を設定できる。暗号ファイルの復元回数制限を設定できる。暗号紋（個性）を無効にしてグループ ID を割り振る事が出来るので、特定グループで使用ができる。パスワード不一致が指定回数を超えると復元できなくなる。USB デバイスを紛失した場合のレスキューが可能・・・・・など単なる暗号アルゴリズムだけではなく、周辺のセキュリティ機能が充実している。

平文の残骸が残らない

暗号化した後に、平文（元ファイル）の置いてあったセクタに残る情報も完全に消し去る、ディスククリーナーが連動します。（元ファイルは消し去っても、セクタに残骸が残っています、本ソフトウェアはこの残骸も消し去ります）

高速・大容量

極めて複雑なアルゴリズムであるにも関わらず、高速処理です。また 2GByte を超える大容量ファイルも扱えます。これらによって、大容量の DTP コンテンツや動画コンテンツなどのバックアップにも最適です。

ハードウェア暗号版もラインナップ

ソフト・ハード混在暗号が可能な上位版があります。このバージョンではコンピュータのタイマを使わないので、暗号解除可能な復元期日（賞味期限）の設定を確実に守る事が出来ます。更に暗号アルゴリズムをハードウェアとソフトウェアに分散しており、クラッキングに強い設計です。詳細はお問い合わせください。

ソフトウェアの特徴

超簡単操作・インストール不要

ある程度コンピュータに慣れている人であれば、本製品のソフトウェアは殆どマニュアルなしで短時間で使いこなす事が出来ます。またUSB デバイスから起動するか、或いはハードディスクにコピーするだけで使えるので、OS にインストール（セットアップ）する必要がありません。移植は USB デバイスと本製品のアプリケーションフォルダを移動するだけです。

ファイルとフォルダの暗号に徹したシンプル設計

ファイルを暗号するか、それともフォルダを圧縮して暗号するかを選択できます。ファイルは暗号化した後に、元ファイルを完全削除する設定を選択できます。（フォルダの場合にはこの設定はできません）

各種設定が可能

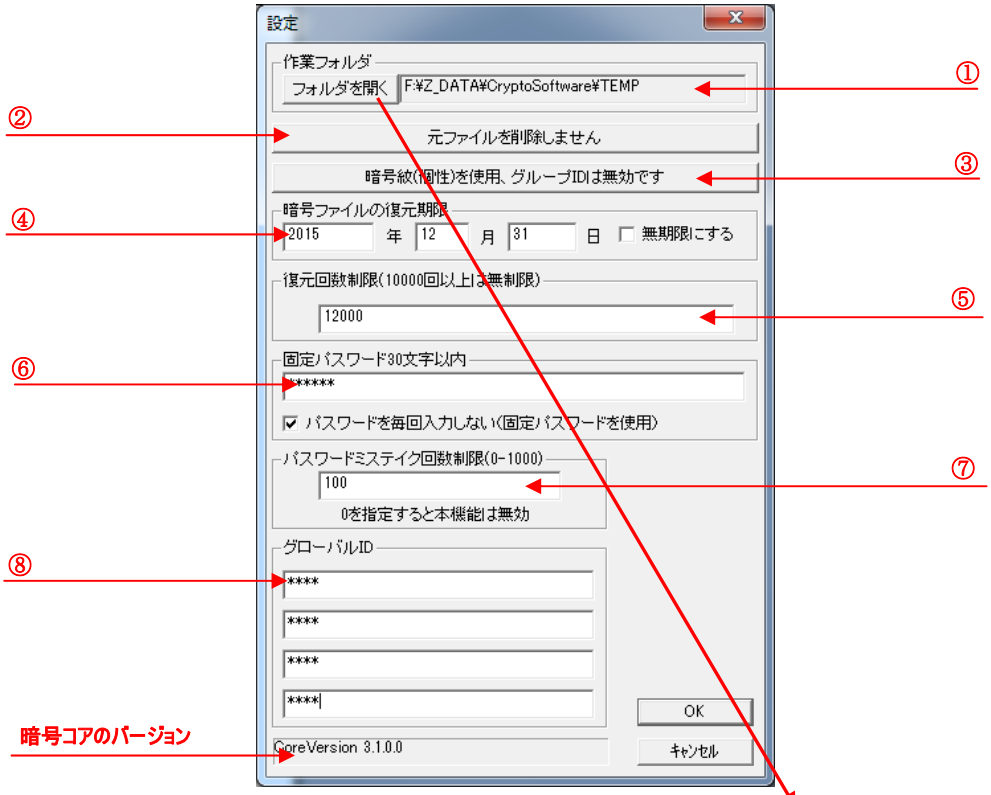
暗号ファイルの復元期限（賞味期限）、暗号ファイルの復元回数制限、グループ ID、パスワードの自動入力、ワークディレクトリの指定など、利用者の使い勝手に合わせた各種設定・保存が可能です。

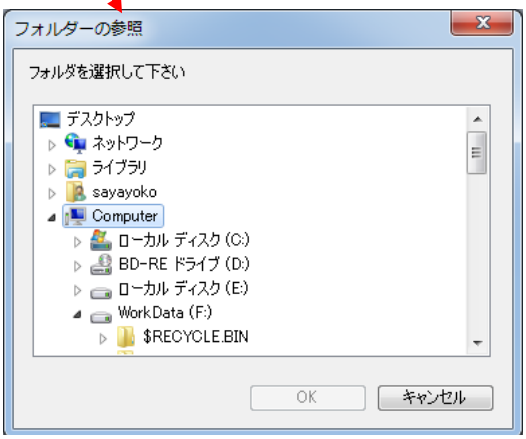
対応 OS

WindowsXP(32Bit), WindowsVista(32Bit/64Bit), Windows7(32Bit/64Bit),
Windows8(32Bit/64Bit), Windows8.1(32Bit/64Bit), Windows10(32Bit/64Bit)
で動作可能です。

2.インストールと設定

特にインストール作業はありません。製品として提供される USB デバイスの USB¥CryptoConsole の中身を任意のフォルダにコピーしてください。或いは USB デバイス自体から起動させてもかまいません。アプリケーション(USB¥CryptoConsole¥CryptoConsole.exe)を起動して“設定”ボタンをクリックしてます。以下の画面が開きますので、ここで基本的な設定を行ってください。設定は後から何度でも変えることが出来ます。
これらの設定情報は、CryptoConsole.exe と同一フォルダの CryptoConf.bin に保存されます。





①作業フォルダの指定: “フォルダを開く”ボタンをクリックすると、“フォルダの参照”ダイアログボックス(右図)が開きますので、作業フォルダを指定して OK をクリックします。ファイルの暗号化やフォルダの暗号化、暗号ファイルの復元を行う場合、ここで指定した“フォルダ”を優先して参照します。作業フォルダは“フォルダを開く”ボタン右のテキストボックスにフォルダ名が現れます。フォルダ名が長い場合、このテキストボックスに入りきれない事がありますが、その場合には隠れている方向にドラッグすれば、スクロールして見えない部分が現れます。

②暗号化後の元ファイルの扱い: このボタンをクリックして元ファイル(平文)を削除するか否かを切り替えます。元ファイルが削除できるのは、ファイルの暗号の場合のみで、フォルダの暗号では元ファイルは自動では削除されません。元ファイルを削除する場合、ファイルが消えるだけでなく、ファイルのあったセクタの残像情報も完全に消去します。

③暗号紋とグループ ID の切替: 鍵要素の一部に、暗号紋(USB デバイスの個性)を方法、グローバル ID を使う方法を選ぶ事が出来ます。例えば暗号ファイルをメールで知人に送る場合には、同じ暗号紋の USB デバイスは存在しませんから、この場合にはグローバル ID を使わなければ成りません。知人とのグローバル ID が一致していれば、あとはパスワードをクリアすれば暗号ファイルを復元することが出来ます。暗号紋を使った場合、その USB デバイス以外では例えパスワードが一致しても、暗号ファイルを復元することは出来ませんから、暗号強度を高めることが可能です。

④暗号ファイルの復元期限: ここで指定した期日(半角英数字)を過ぎると、暗号ファイルの復元を阻止します。一番右のチェックボックス(無期限にする)を選択すると、復元期限の設定は無効になり、永久に復元できるようになります。

⑤復元回数制限: 暗号ファイルの復元回数を制限します。ここで指定した回数(半角英数字)を超えると、復元はできなくなります。10000 回を超える設定を行うと、この設定は無効になり、実質無限回数になります。この機能を有効にしている場合、CD や DVD 等の書き換え不可能な光学メディア等での作業はできなくなります。この場合、HDD や USB ストレージなど書き換え可能なディスク、メディアで運用すれば暗号ファイルの復元が可能になります。

⑥固定パスワード: データのバックアップなど、毎回同じ作業を行う場合、パスワードの入力が面倒ですし、入力ミスの可能性も高まります。そこで、この部分のチェックボックス(パスワードを毎回入力しない)をチェックしておくと、パスワードは毎回自動入力されるようになります。自動入力するパスワードは、この部分のエディットボックスに 30 文字(半角英数字)で入力してください。この機能は外出用のノート PC など用途によっては、セキュリティを低めることになるのでご注意下さい。(パスワードを毎回入力しない)のチェックを外すと、毎回パスワード入力画面が現れます。

⑦パスワードミステイク制限回数: パスワードエラーが、このエディットボックスの回数(半角英数字)を超えると、暗号ファイルは復元できなくなります。回数を 0 にすると、この機能は使われず、何度でもパスワードミスを許容します。

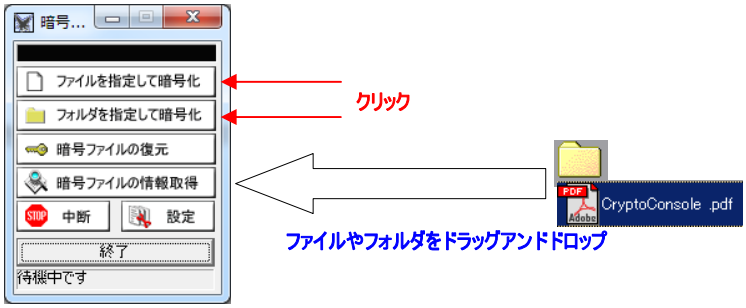
⑧グローバル ID： ここではグループ ID の 128Bit を 32Bit4 桁に分けて設定します。各エディットボックス毎に半角英数字で 0～4294967295 を指定して下さい。0,0,0,0 となったグループ ID は破損とみなされますので、この値は設定しないで下さい。

暗号紋とグループ ID の違いについて

CS101 で提供される USB デバイスは全て個性を持っており、1 台として同じものは存在しません。本ソフトウェアでは、これを暗号ファイルの鍵の生成要素に使うため、暗号化したファイルを復元するには、必ず同じ USB デバイスが必要です。よって暗号ファイルとパスワードが情報流出したとしても USB デバイスが盗まれなければ、その暗号ファイルは安全です。但し、これではメールやイントラネットを通じて、複数の人で暗号情報を共有することはできませんから、この暗号紋の代わりに、グループ ID を使用することが可能です。グループ ID は、128Bit で、設定の都度時間がかかりますから、数値の自動生成ツールを使って解析するのは困難です。

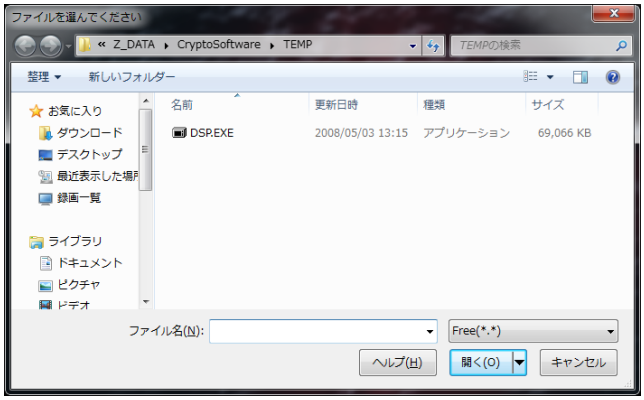
3.ファイルやフォルダの暗号化

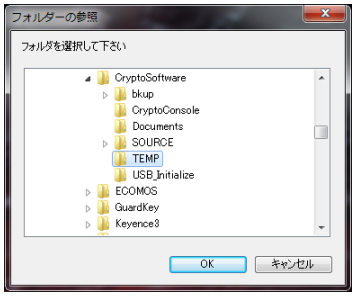
アプリケーションに平文（元ファイルや元フォルダ）をドラッグアンドドロップするか、“ファイルを指定して暗号化”又は“フォルダを指定して暗号化”ボタンをクリックしてください。



設定画面で、“パスワードを毎回入力しない“のチェックボックスが無効であれば以下のようなパスワード入力画面が現れますので、ここで半角英数字で 30 文字以内のパスワードを入力してください。

OK ボタンを押すと次に進みます。設定画面で、“パスワードを毎回入力しない“のチェックボックスが有効であれば、この工程は省略されます。次に”ファイルを指定して暗号化“の場合には以下左のダイアログが出ますので、暗号化したいファイルを選択して、開くボタンをクリックするか、選択ファイルをダブルクリックして次に進みます。また”フォルダを指定して暗号化“を選択した場合には以下右のダイアログが出ますので、フォルダを指定して下さい。OK をクリックして次に進みます。

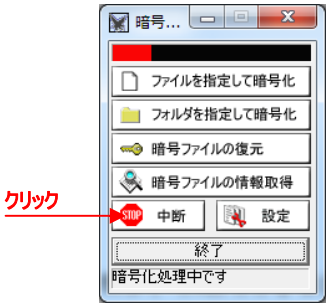




ファイル選択またはフォルダ参照ダイアログでファイルやフォルダを選択すると、元の画面に戻り、進捗状況がプログレスバーで表示されます。圧縮中は黄色（フォルダの暗号のみ）、暗号化中は赤のプログレスバーです。圧縮時のプログレスバーは通常何回も往来します。暗号化のプログレスバーは 0-100%の進捗状況を表すので、ちょうど真中で 50%です。

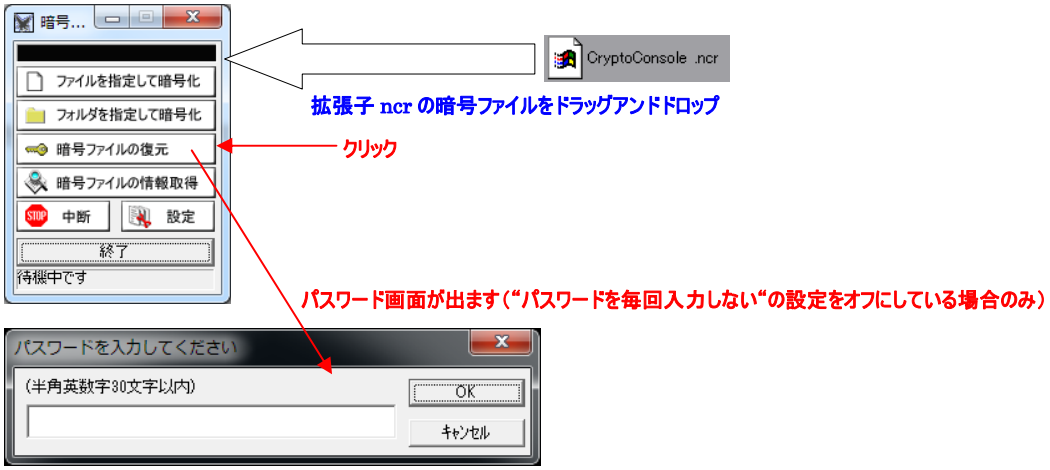
最後に以下のメッセージボックスが出ますので、OK をクリックして下さい。

途中で処理を中断には、“中断”ボタンをクリックしてください。処理中の内容によっては中断まで時間がかかる場合があります。

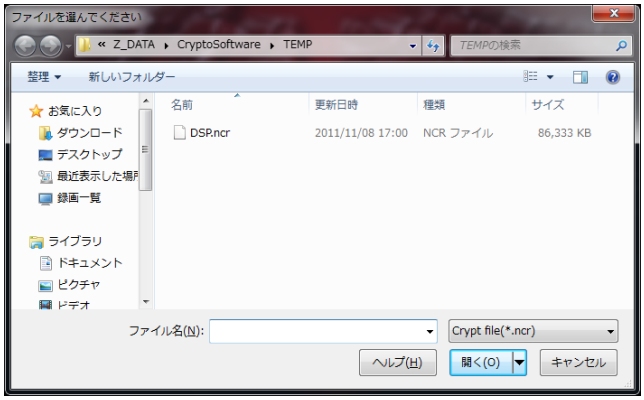


4.暗号化ファイルの復元

“暗号ファイルの復元”ボタンをクリックしてください。設定画面で、“パスワードを毎回入力しない“のチェックボックスが無効であれば以下のようなパスワード入力画面が現れますので、ここで半角英数字で 30 文字以内のパスワードを入力し OK ボタンをクリックてください。設定画面で、“パスワードを毎回入力しない“のチェックボックスが有効であれば、この工程は省略されます。

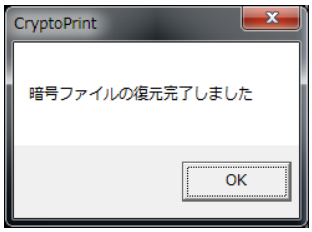


次に案暗号ファイルを選ぶ為、以下のダイアログが出ますので、暗号ファイルを選択して、開くボタンをクリックするか、選択ファイルをダブルクリックして次に進みます。(暗号ファイルの拡張子は ncr)

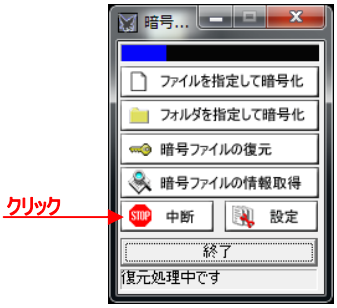


暗号ファイルを指定すると元の画面に戻り、進捗状況がプログレスバーで表示されます。暗号ファイル復元中は青、圧縮ファイル解凍中は黄色（フォルダの暗号のみ）のプログレスバーです。圧縮解凍時（黄色）のプログレスバーは通常何回も往来します。復元時のプログレスバー（青色）は0-100%の進捗状況を表すので、ちょうど真中で 50%です。

最後に以下のメッセージボックスが出ますので、OK をクリックして下さい。

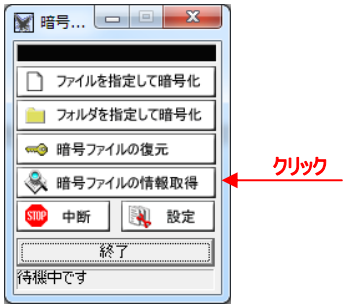


途中で処理を中断するには“中断”ボタンをクリックしてください。処理中の内容によっては中断まで時間がかかる場合があります。

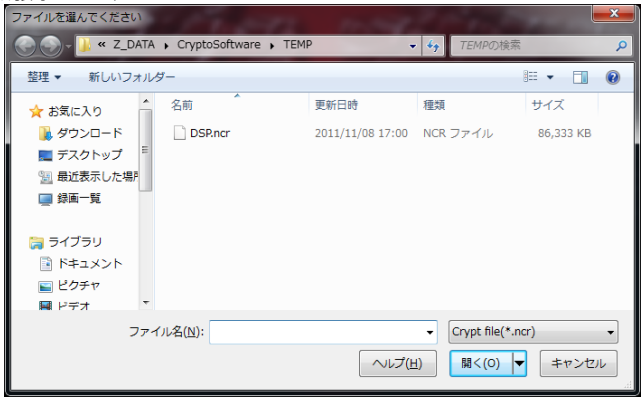


5.情報の取得

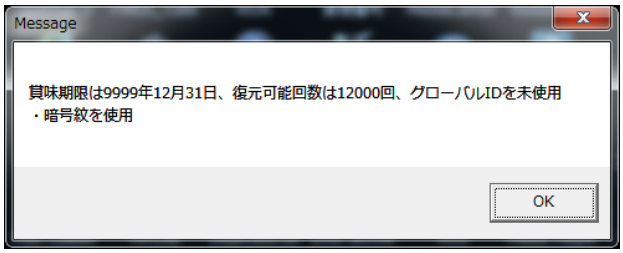
暗号ファイルの暗号化設定情報を表示することが出来ます。“暗号ファイルの情報取得”ボタンをクリックしてください。



暗号ファイルを選ぶ為、以下のダイアログが出ますので、暗号ファイルを選択して、開くボタンをクリックするか、選択ファイルをダブルクリックして次に進みます。（暗号ファイルの拡張子は ncr）

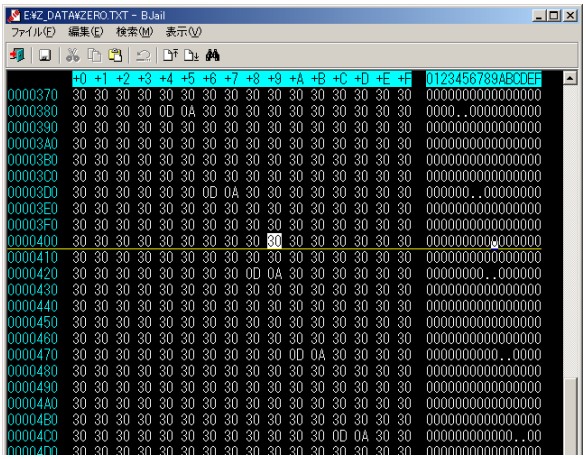


暗号ファイルを選択すると、以下のメッセージボックスが現れ、各種情報を表示します。

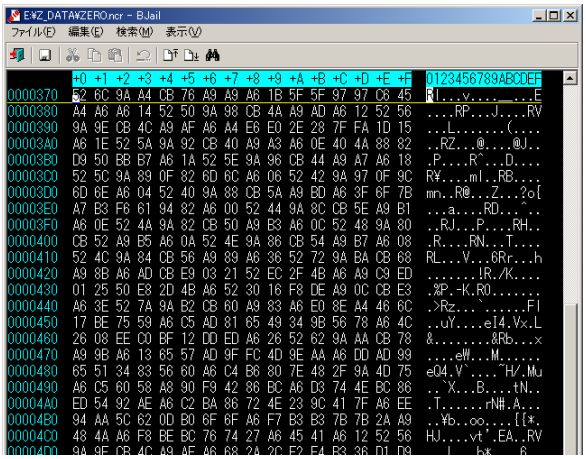


6.暗号前と暗号化後(簡単な効果の説明です)

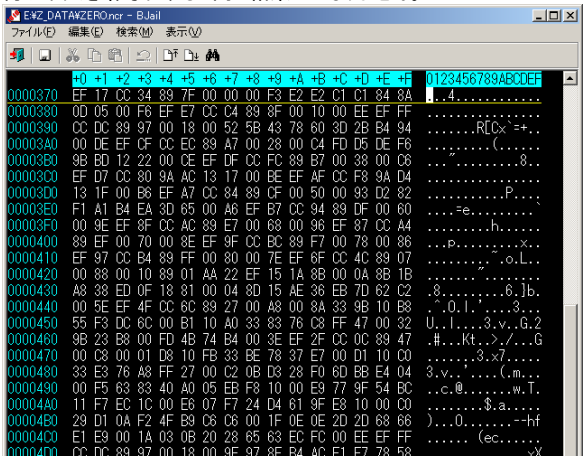
以下は暗号化前の平文(元ファイル)です。ひたすら 0 が続く単純なファイルのバイナリダンプ結果です。



これを暗号化した結果は次の通りです。単純なパターンは消失し、複雑で周期性のない数値が続きます。



再び平文を暗号化すると同じ結果にはなりません。



7.注意点・その他

7.1 本仕様書の扱い

＜製品との相違＞

本仕様書は、ご利用者が理解しやすいよう努力しておりますが、万一、本仕様書と製品が異なる場合には、製品を優先させていただきます。また、本仕様書の主観的解釈の可能な個所についても、同様に、製品を優先とさせていただきます。

＜品質と機能＞

本製品の品質および機能が、ご利用者の使用目的に適合することを保証するものではありません。従って、本製品の選択導入はご利用者の責任でおこなっていただき、本製品の使用や、その結果の直接的または間接的ないかなる損害についても弊社は保証致しません。

＜バージョンアップ＞

ドライバや仕様書のバージョンアップや修正などを、ホームページ、メール、CDROM の配布等の何らかの手法で提供いたします。ただし、弊社の諸事情により迅速な対応がとれない場合もあります。また、これらは、その遂行義務を弊社が負うものではありません。

7.2 工業所有権、著作権

本製品の使用により、第三者の工業所有権・著作権に関わる問題が生じた場合、弊社の製造、製法に関わるもの以外については、弊社はその責を負いませんのでご了承下さい。また、弊社の許可無しに、ソフトウェアに対するリバースエンジニアリングを禁止します。このような結果生じた損害についても、弊社はその責を負いません。