暗号化ソフトEDご利用マニュアル

オンラインで最新マニュアルもご利用下さい

目次

1、はじめに

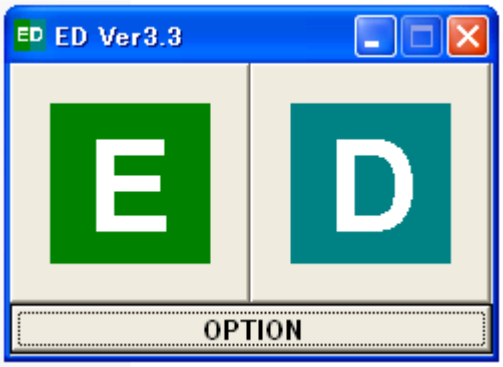
2、動作環境

3、インストール

4、操作方法

5、その他

1、はじめに



ED（イーディー）は強力な暗号化アルゴリズムと、使い勝手重視のシステムがウリの、Windows 用フリーウェアファイル暗号化ツールです。簡単な操作で、ファイルを自在に暗号化することができます。例えばディレクトリごと暗号化してハードディスクの中身を保護したり、インターネットで秘密のファイルを送りたい場合などに最適です。暗号化されたファイルは暗号化時に設定したパスワードを用いて復号（元にもどす）するまで全く意味を成さなくなります。

こういったツールはこれまでにもあったのですが、例えばPGPに見られるように、テキストの暗号化機能や公開鍵暗号などがごっちゃになっていて初心者には非常に使いづらかったり、そうかと思うと、使い勝手はそこそこ良いのだけれども、暗号強度に問題があったりして、とても大事なファイルを託すことができない場合がしばしばありました。さらにシェアウェアである場合も多いので、ネットワーク等を介して利用してもらう場合などには不向きでした。

その点EDは、鍵長最大 256 ビット暗号アルゴリズムをベースにした、解読不可能レベルの暗号化も可能である強力な暗号強度を保っているにも関わらず、その操作システムは極めて単純で、随所に説明を入れてありますので、少し Windows に触ったことのある人なら、このマニュアルを読まなくてもすぐに使いこなすことが可能です。さらにパスワードのヒントを付加できる機能や、多様な入力インターフェイス、セキュリティレベル設定による安全なパスワード入力、ファイル名隠蔽・復元機能、日付復元機能、パスワード誤入力防止機能、経過データ完全抹消機能など、便利で個性的な機能を思いつく限り備えました。

また Ver3.0 からは、ユーザが分かって選べるセキュリティをコンセプトに、3種類の暗号アルゴリズム（TwoFish、Rijndael、GOST 28147-89）から使用するアルゴリズムを選択できる機能を付加しました。いずれも非常に強力な暗号アルゴリズムですが、中でも Rijndael は、2000 年 10 月にアメリカ合衆国政府の公認暗号に選出されています。さらに設計の大幅な見なおしを行った結果、強度を落とさずに高速な暗号化を行うことに成功しましたので、ブロードバンドの普及に伴う、大容量データ保護のニー

ズにも耐えるものとなりました。さらに Ver3.3 系列からは、2GB を超える、超大容量のファイルの快適な処理に対応するべく、機能の拡張を行いました。

さらに2009年からは、より便利なソフトになるよう、ユーザの皆様のご意見を頂きながら、より挑戦的な取り組みも行っています。

情報化の時代と言われる今日この頃ですが、このツールが皆様の情報のプロテクトに少しでも貢献できることを期待しています。

作者

2、動作環境

ソフトウェア環境

OS

Microsoft　Winows95または98、ME、NT4.0、2000、XP、Vistaまたはこれらの上位互換 OS。

ハードウェア環境

上記ソフトウェア環境が維持できるハードウェア

３－１、本ソフトのインストール

インストールと言っても、基本的にこのソフト自体は、.LZH ファイル内の全てのファイルを同一フォルダ（ディレクトリ）に入れればインストール完了です。

頻繁に使ってあげようという有難い方は、デスクトップや「プログラム」などに
E_D.EXE のショートカットを登録すると、起動が楽になります。

実行方法

３－２、実行方法

基本的には、実行ファイルである E_D.EXEをエクスプローラーでダブルクリックするなどして実行するだけです。

応用として、コマンドラインオプションに対応しています。

Note：

実行ファイル名に含まれる_（アンダーバー）は、凝っているのではありません。以前単に ED.exe にするとなぜか Norton CleanSweep にインストールプログラムとして検知されてしまっていたからです（笑）。

３－３、コマンドラインオプション

指定するオプションの数により、操作におけるそれぞれの段階を指定できます。コマンドラインによる操作は慣れると多彩な使用法ができますが、確認ダイアログがでないために危険でもあり、上級者向けです。操作を良く把握して、さらにテストを行ってから実行するようにして下さい。

■方法１

暗号化　：　-E
復号　　：　-D
抹消　　：　-W

ここまでだけの指定で起動すると起動直後に E または D を押したときのファイル選択ダイアログが開きます。

■方法２

暗号化：　-E [ファイル or フォルダ名 1] [ファイル or フォルダ名 2] ...
復号　：　-D [ファイル or フォルダ名 1] [ファイル or フォルダ名 2] ...
抹消　：　-W [ファイル or フォルダ名 1] [ファイル or フォルダ名 2] ...

ここまでだけの指定で起動するとそれぞれのモードにおけるファイルを選択したときの確認ダイアログが開きます。

■方法３

暗号化：　-E -F -P [パスワード] -H [ヒント] [ファイル or フォルダ名 1] [ファイル or フォルダ名 2] ...
復号　：　-D -F -P [パスワード] [ファイル or フォルダ名 1] [ファイル or フォルダ名 2] ...
抹消　：　-W -F [ファイル or フォルダ名 1] [ファイル or フォルダ名 2] ...

ここまでだけの指定で起動するとパスワードの照合、セキュリティレベルのチェックなどの確認作業を何も行わずに全処理を一気に行い、全てのファイルについて処理が成功すれば自動的に終了します。

この第3の方法は、全ての操作が自動的に行われるため、非常に強力です。具体的な応用方法としては、予めコマンドラインを含めたリンクを作成しておくことにより、そ

れを押すだけでロック・アンロック・抹消が出来る工夫や、他のアプリケーションを組み合わせたセキュリティシステムなどが考えられます。

■方法4

暗号化： -E -F -P [パスワード] -H [ヒント] -A [結果保存先ファイル名] [暗号化対象ファイル名]
復号 ： -D -F -P [パスワード] -A [結果保存先ファイル名] [復号対象ファイル名]

通信を行うファイルの暗号化の際など、処理対象のファイルに変更を加えたくない場合は、-A オプションを用いると処理結果の保存先ファイル名を指定することが出来ます。この方法を用いた場合、方法3と同様、一気に処理が行われます。なお性質上、一度に指定できる処理対象/保存先ファイルは一つで、複数のファイルやフォルダなどは指定できません。

■その他

-I オプションをつけると、処理終了後に自動終了するようになります。

Important:

コマンドラインオプションは多くの可能性をもたらしてくれますが、ED を組み込んだシステムや製品（これには ED を単体で販売する場合を含みますが、雑誌・書籍等への転載は含みません）を販売または有償で開発するためには、それが ED を別途用意するように指示がついたものであっても、作者の事前許可が必要になります。詳しくは FAQ をご覧ください。

４－１、ファイルを暗号化するには（ロックする）

（1）暗号化するファイルを指定する

「E」ボタンを押すとお馴染みのファイルを開くダイアログが出てきますので、暗号化するファイルを選択してください。CTRL や SHIFT キーを押しながらの複数選択が行えます。選択したら「開く」を押します。

この操作の他に、ドラックアンドドロップが使えます。エクスプローラー等で暗号化したいファイルやフォルダを選択した後、それを「E」ボタン上にドロップしてあげるだけです。フォルダをドロップした場合、そのフォルダの中の全てのファイルが選択されます（さらにサブフォルダを含めるかどうかは、オプションで設定できます）。

なお、コマンドラインオプションとともにファイルを指定して指定して実行した場合は、本操作は必要ありません。EDは下記（2）の状態で起動します。

Note:

Windows共通の方法ですが、EDが他のウインドウの影に隠れてしまったり、タスクバーにアイコン化してしまってドロップできない場合は、ドラックしてきたままマウスカーソルをタスクバー上のEDのアイコンの上で数秒間静止していれば、EDのウインドウが開きます。

Important:

Windows の仕様上（？）、ドラックアンドドロップ以外の方法で、大量の（4、5 百個以上）のファイルを ED へ一度に渡そうとすると、全て正しく渡せないことがあります。その場合はドラックアンドドロップを使うようにしてください。

安全のため、処理対象ファイル名（パスを含まない名前+拡張子部分）には文字数制限（半角の場合で 200 文字未満）が Ver3.3 よりつきました。なお、この制限を越える長さの名前のファイルをドラックアンドドロップで渡そうとすると、リストに正しく表示されませんのでご注意下さい。

（2）指定されたファイルを確認する

（1）の操作を行うと、選択されたファイルのリストが表示されているウインドウが開きますので、確認してください。もし取り消したいファイルがある場合は、選択して

Delete キーを押すことでそのファイルをリストから外すことが出来ます。リストの選択は CTRL キーや SHIFT キーによる複数選択が可能です。

確認し終わったら、OKを押して次に進みます。

（3）パスワードを入力する

（2）の操作を行うと、暗号化に必要なパスワードの入力を行うダイアログが開きます。パスワードは誤入力防止のため、入力と再入力の2つの項目に同じパスワードを入れる必要がありますので、それぞれ入力してください。また同様の理由により、カナ漢字変換機能（IME）は利用できなくなっていますが、全角文字を入力したい場合はカット＆ペーストすれば可能です。（ただし、パスワードに全角文字を用いることは一般的ではなく、推奨されません。）

次に「ヒント」という項目がありますが、これはファイルにかかっているパスワードについてのヒントを、付加できる機能によるものです。付加されたヒントは復号時に誰にでも見ることができます。この機能は、ネットワークを通じて公開する場合のクイズ的な使い方や、「20年前に飼っていた猫の名前を逆さにして3回」（笑）のように自分だけがわかる情報をいれておき、パスワードの損失を防ぐといった使い方などが考えられます。必要に応じて入力してください（必要ない場合は空白でOKです）。

一番下の「パスワードの照合」という項目は、日常使っているパスワードとは異なったパスワードを入力してしまい、さらにそれに気づかずにいるという事態を防ぐためのものです。使い方は簡単で、現在入力したパスワードを日常使っているパスワードと照合したい場合は「照合用ハッシュと照合する」に、現在入力したパスワードを日常使っているパスワードとして登録したい場合は、「照合用ハッシュを登録」に、なにもしない場合は、「なにもしない」にそれぞれチェックを入れてください。

Note：

登録したパスワードは特殊な方法（SHA-1 ハッシュ：不可逆な要約情報化）で加工したのち、INIファイルに保存されますので、登録してもパスワード自体が保持されるようなことはありません。保持されるのは照合にしか役立たない情報です。安心してご利用ください。（登録したハッシュをクリアすることもできます。）

全てよければ、OKを押します。その際、入力されたパスワードが、オプションで設定されたセキュリティレベルの必要とする文字数より少なかったり、パスワード照合機能（下記）を利用していて、入力したパスワードが登録されているものと異なる場合、再入力を促すメッセージが表示されますのでご注意ください。

（4）暗号化・終了

（3）で入力されたパスワードが有効であれば、ファイルが暗号化されます。経過が表示され、終了するとその旨通知されます。

ファイルのアクセスが制限されているなどの理由で暗号化に失敗することがあった場合は、リストの当該ファイルに＊暗号化失敗＊などと表示されますので確認してください。

Note：

オプション設定で暗号化後に元ファイルを抹消する設定になっていると、1ファイルの処理が終わるたびに抹消処理が行われます。もし大容量ファイルの処理中などで（セキュリティを差し置いてでも）この処理をスキップしたくなった場合は、「抹消をスキップ」ボタンを押すことで、抹消処理をすぐに中断し、残りを通常の方法で削除した後、次の処理へ進むことができます。

全て終了したら、「閉じる」を押して最初の画面に戻ります。

暗号化したファイルの復号方法

４－２、ファイルを復号するには（ロックを解除する）

（１）復号できるファイルとは

復号するEDと同一又はそれより下のバージョンのEDで暗号化されたファイルです。ただし、例外として、Ver3.0 より暗号化手順が大幅に変更されましたので、Ver3.0 以上と Ver2.1 以下のバージョンとの互換性はありません。（その場合は一旦 Ver2.1 を使用して既存のファイルを解読した後、最新版に乗りかえるようにすると良いでしょう。なお Ver2.1 は WEB サイト または作者にメールにて入手できます。）

よく分からない場合は、暗号化にしたのと同じバージョンのEDを使用するようにすれば問題ないと思います。

なおEDで暗号化されたファイルであるかや、暗号化したEDのバージョンが知りたい場合は、調べたいファイルをワードパッドや秀丸などのテキストエディタで開いてみてください。EDが出力したファイルには、先頭に ED の名前とバージョンが書いてあります。

（２）復号するファイルを指定する

「D」ボタンを押すとお馴染みのファイルを開くダイアログが出てきますので、復号（暗号化したファイルを元に戻す）するファイルを選択してください。CTRL や SHIFT キーを押しながらの複数選択が行えます。選択したら「開く」を押します。

この操作の他に、ドラックアンドドロップが使えます。エクスプローラー等で復号したいファイルやフォルダを選択した後、それを「D」ボタン上にドロップしてあげるだけです。フォルダをドロップした場合、そのフォルダの中の全てのファイルが選択されます（さらにサブフォルダを含めるかどうかは、オプションで設定できます）。

なお、コマンドラインオプションとともにファイルを指定して指定して実行した場合は、本操作は必要ありません。EDは（２）の状態で起動します。

Note：

Windows共通の方法ですが、EDが他のウインドウの影に隠れてしまったり、タスクバーにアイコン化してしまってドロップできない場合は、ドラックしてきたままマウスカーソルをタスクバー上のEDのアイコンの上で数秒間静止していれば、EDのウインドウが開きます。

Important:

Windows やハードウェアの仕様上、ドラックアンドドロップ以外の方法で、大量の（4、5 百個以上）のファイルを ED へ一度に渡そうとすると、全て渡せないことがあります。その場合はドラックアンドドロップを使うようにしてください。

安全のため、処理対象ファイル名（パスを含まない名前+拡張子部分）には文字数制限（半角の場合で 200 文字未満）が Ver3.3 よりつきました。なお、この制限を越える長さの名前のファイルをドラックアンドドロップで渡そうとすると、リストに正しく表示されませんのでご注意下さい。

（3）指定されたファイルを確認する

（1）の操作を行うと、選択されたファイルのリストが表示されているウインドウが開きますので、確認してください。もし取り消したいファイルがある場合は、選択して Delete キーを押すことでそのファイルをリストから外すことが出来ます。リストの選択は CTRL キーや SHIFT キーによる複数選択が可能です。

リストのファイルの中で、本ソフトのパスワードヒント機能によりヒントが付加されているものは、リストの右側の部分にそれぞれ表示されます。

確認し終わったら、OKを押して次に進みます。

（4）パスワードを入力する

（2）の操作を行うと、暗号化に必要なパスワードの入力を行うダイアログが開きますので入力してください。なお誤入力防止のため、カナ漢字変換機能（IME）は利用できなくなっていますが、全角文字を入力したい場合はカット＆ペーストすれば可能です。

全てよければ、OKを押します。

（5）復号・終了

（3）で入力されたパスワードが有効であれば、ファイルが復号されます。経過が表示され、終了するとその旨通知されます。

パスワードが違っているなどの理由で暗号化に失敗することがあった場合は、リストの当該ファイルに＊復号失敗＊などと表示されますので確認してください。

全て終了したら、「閉じる」を押して最初の画面に戻ります。

（6）再暗号化機能について（オプション）

オプション設定で「再暗号化機能」が有効になっている場合、復号後に、当該ファイルリストを再暗号化するボタンが使用可能になります。このボタンを押すと、そのダイアログに表示されていたリストの復号済みファイルが、復号時のパスワードと、前回設定したヒントで一気に再暗号化されます。これは、普段は暗号化しているファイルを一時的に開いて作業し、また暗号化するという作業が多い方に便利な機能かと思います。

Note：

Ver2．0より、ファイルの日付を復号時に復元する機能が実装されておりますが、Norton Utilities などのシステム保護系のソフトをご使用の環境におきましては、日付の復元がされない場合があります。

Note：

オプション設定で復号後に元ファイルを抹消する設定になっていると、1ファイルの処理が終わるたびに抹消処理が行われます。もし大容量ファイルの処理中などで（セキュリティを差し置いてでも）この処理をスキップしたくなった場合は、「抹消をスキップ」ボタンを押すことで、抹消処理をすぐに中断し、残りを通常の方法で削除した後、次の処理へ進むことができます。

４－３、ファイルを抹消するには

（１）削除とは

削除とは、普通、Windows 上でファイルを選択して Delete キーを押すなどし、ゴミ箱に入れ、そのゴミ箱を空にすることなどをさします。この方法でファイルを消去しても、多くの場合、ファイルのデータそのものが無くなったわけではなく、「**そのファイル を使わなくなり、またそのディスクスペースを他の用途に利用できるように解放（空き領域）する**」だけです。

これは例えていえば、賃貸マンションの部屋がファイルだとすると、削除は、「**今後部屋を利用せず、空き物件として、不動産会社に登録する**」だけのようなもので、中の家財道具は次の入居までそのままになっているようなものです。

この方法を使えば、すばやく「空き部屋」を作ることが出来るので便利ですが、だれかが強引にその部屋に入ると、大切なものを盗まれたりする可能性があります。ファイルの場合も全く同様で、 削除であれば高速にディスクを「空ける」ことができるものの、次にその領域に新しいデータが格納されるまで、**削除されたファイルのデータは残っていることがあり、専用のツールなどで復元されてしまう恐れ**があります。

（２）抹消とは

これに対し、**「抹消」は、通常の削除の後、ファイルが存在していた領域を単調なデータで一回上書きします**。これは、先ほどの部屋のたとえでいうのであれば、部屋の退去の際、家財道具を全て壊してしまうようなもので、ただの削除の場合と比べ、 処理に時間はかかるものの、中のデータ（家財道具）を利用されにくくする効果があります。

ED では、ここで説明する、ファイルを直接指定して抹消する機能の他に、暗号化時に元ファイルを自動的に抹消する機能があります。（この抹消も、ここでの抹消も、同じ仕組みを用いています。）

（３）ED の抹消機能についての注意事項

ただし、ED に付属の抹消機能は、**完全なものではありません**。ディスクの種類やファイルシステムや、それらの環境設定次第では、抹消したはずのデータが残ってしまう可能性もあります。また、抹消に成功していたとしても、単調なデータで上書き１回というのは、特に磁気ディスクの場合、特殊で高価な装置を用いて時間をかければ、復元されてしまう恐れがあります。

従って、この ED 付属の抹消機能は、あくまで、メディアからデータを不正に取り出そうとする者に対して、「**通常の削除よりも非常に大きなコストと手間を強い、ゆえに多くの場合で不正利用を断念させるための、補助的な機能**」として認識し、より完璧な抹消を求める場合は、**市販などされている専用の抹消ツールを併用**されることを推奨します。

いずれにしても、この抹消の点のみならず、**機密ファイルについては、暗号化されてないファイルが存在する(していた)場所を、極力少ない範囲にする**ことが、効果的なデータ防衛のための重要な心がけといえます。たとえば、USB メモリや USB-HDD などのリムーバブルストレージ(ディスク)へファイルを格納するために暗号化する場合は、ファイルをリムーバブルストレージへコピーしてから暗号化するよりも、安全な PC 上でファイルを暗号化し、その暗号化されたファイルをリムーバブルストレージへ移動する方が、より安全です。これは復号の際も同様で、リムーバブルストレージ上で復号するのではなく、暗号化されたファイルを、安全な PC 上に移してから、それを復号する方が安全です。

(4)ファイルの抹消方法

ED を起動し、「OPTION」ボタンを押します。するとオプション画面が開きます。エクスプローラー等で抹消したいファイルやフォルダを選択した後、それをその中の抹消ゴミ箱という部分の、白い領域に、ドロップすると、ダイアログが開いて抹消操作を確認しますので、画面の指示に従って確認・実行してください。なおフォルダをドロップした場合、そのフォルダの中の全てのファイルが選択されます(さらにサブフォルダを含めるかどうかは、オプションで設定できます)。

または、抹消ゴミ箱の右にあるボタンを押すとお馴染みのファイルを開くダイアログが出てきますので、抹消するファイルを選択してください。CTRL や SHIFT キーを押しながらの複数選択が行えます。選択したら「開く」を押すと、ドロップの場合と同じダイアログが開きますので、画面の指示に従って確認・実行してください。

Note:

この抹消ゴミ箱は、起動時の TOP 画面の下にもってくることもできます。その場合、そのボタンは、同じ TOP 画面にある、「E」(暗号化)や「D」(復号)のボタンのように、クリックするとダイアログが開き、ドロップもできる仕様になっています。詳しくはオプション設定の項をご覧下さい。

なお、その他、コマンドラインオプションで実行することもできます。

Note:

Windows共通の方法ですが、EDが他のウインドウの影に隠れてしまったり、タスクバーにアイコン化してしまってドロップできない場合は、ドラックしてきたままマウスカーソルをタスクバー上のEDのアイコンの上で数秒間静止していれば、EDのウインドウが開きます。

Important:

Windows やハードウェアの仕様上、ドラックアンドドロップ以外の方法で、大量の（4、5百個以上）のファイルを ED へ一度に渡そうとすると、全て渡せないことがあります。その場合はドラックアンドドロップを使うようにしてください。

安全のため、処理対象ファイル名（パスを含まない名前+拡張子部分）には文字数制限（半角の場合で 200 文字未満）が Ver3.3 よりつきました。なお、この制限を越える長さの名前のファイルをドラックアンドドロップで渡そうとすると、リストに正しく表示されませんのでご注意下さい。

４－４、オプション画面（各種設定）

「OPTION」ボタンを押すと開くオプション設定ウインドウでは、EDに関する様々な設定等が行えます。設定はINIファイルに保存されますので、次回起動時にも有効です。

・「ファイル選択の時にサブフォルダも含める」チェックボックス

この部分にチェックを入れると、ドラッグ＆ドロップなどでフォルダを選択した場合、その中のファイルのほかに、その階層以下に入っている全てのサブフォルダの中身を選択することが出来るようになります。ハードディスクの内容をそのまま秘匿化したい時などに便利です。

チェックが外れていると、選択されたフォルダ内のファイルのみが選択されます。

・「暗号化後に元ファイルを抹消する」チェックボックス

この部分にチェックを入れると、ファイルを暗号化した際に、その元となるファイルを抹消します。

抹消作業を自分で行いたい場合や、通信に使うための暗号ファイルを作成する場合等 、特にEDで抹消する必要が無い場合は、チェックを外しておくと、処理が速くなるので良いでしょう。

・「復号後に元ファイルを抹消する」チェックボックス

この部分にチェックを入れると、ファイルを復号した際に、その元となるファイルを抹消します。

抹消作業を自分で行いたい場合等、特にEDで抹消する必要が無い場合は、チェックを外しておくと 、処理が速くなるので良いでしょう。

・「メイン画面を常に前面に表示する」チェックボックス

この部分にチェックをいれると、メイン画面（通常起動直後の画面）が常に前面に表示されるようになります。他にウインドウ部分が重なるアプリケーションがあっても、（相手が同じような属性のウインドウでない限り）下に隠れてしまうことがありません。主にドラック＆ドロップで処理ファイルを指定する方で、タスクバー上のアイコン部分にもっていくのが難しい方はチェックすると便利です。

・「使用中は前回のパスワードをメモリから消去しない」チェックボックス

ED を日常的に使用するようになると、重要なファイルを普段は暗号化し、編集や閲覧の必要が生じた場合にのみ復号してアプリケーションで開き、作業が終わったら再び暗号化するという使い方が多くなってくることがあります。その場合、この部分にチェックをいれると、ED を閉じるまでは、前回のパスワードが入力欄に残っているようになりますので、パスワードを入力することなく再暗号化することができます。

Important:

上記のオプション機能は便利ですが、例えば ED を開いたまま離席した場合などに、他の悪意のある人がパスワードを入力することなく、あなたが暗号化したファイルを復号したり、専用のツールを使用してメモリからパスワードを取得することを可能にしてしまう恐れがありますので十分注意してください。

・「前回入力したパスワードのヒントを記憶する」チェックボックス

同じパスワードで連続して暗号化する場合など、同じヒントを何度も入れるのが煩雑な場合にチェックすると、前回入力したヒントをメモリと設定ファイルに保存するようになりますので便利です。

・「再暗号化機能を使用する」チェックボックス（実行中パスワード保持）

ED を日常的に使用するようになると、重要なファイルを普段は暗号化し、編集や閲覧の必要が生じた場合にのみ復号してアプリケーションで開き、作業が終わったら再び暗号化するという使い方が多くなってくることがあります。その場合、この部分にチェックをいれると、ED を閉じるまでは、前回のパスワードを内部に保持するようになり、復号後にその処理対象のファイルを一括して再暗号化する機能が有効になります。（再暗号化機能については復号の項もご覧ください。）

Important:

上記のオプション機能は便利ですが、例えば ED を開いたまま離席した場合などに、他の悪意のある人がパスワードを入力することなく、あなたが暗号化したファイルを復

号したり、専用のツールを使用してメモリからパスワードを取得することを可能にしてしまう恐れがありますので十分注意してください。

・「抹消ゴミ箱をメイン画面に出す」チェックボックス

このチェックボックスを有効にすると、通常はオプション画面に存在する「抹消ゴミ箱」が、起動時の TOP 画面の下に現れるようになります。頻繁に抹消を行う方は便利かと思います。

Note:

このオプションを有効にした場合、ヒントは設定ファイルに平文で保存されます。

・抹消ゴミ箱

白い部分にファイルをドラック&ドロップするか、その右のボタンを使ってファイルを選択すると、暗号化や復号時と同じようなダイアログが現れて、抹消したいファイルの確認を行います。ここでOKボタンを押せば、選択されたファイルは抹消され、復活できなくなります。

Note:

ファイルの抹消＝削除ではありません。通常の方法で削除されたファイルは、Norton Utilities 等で簡単に復活することができるからです。これに対し、抹消（wipe）は一旦ファイルを無効なデーターで塗りなおしてから削除するので、復活が困難になります。ですので、不要となった秘密ファイルは出来る限りこれで削除するようにしてください。ちなみに本ソフトでは、暗号化/復号処理時に行う、作業ファイル又は元ファイル等の削除にもこの機能を用いていますので、安心です。

なお、この機能は動作環境やメディアによっては、完全に働かないことがあります。また、ハードディスクの空き領域にデータが残っている場合もありますので、不安な方は専用のツールなどを併用されることをお勧めします。

抹消機能についてはこちらもご参照ください。

・暗号化したファイルの設定

これは、ED が暗号化したファイルの名前や拡張子をどのようにするかの設定です。それぞれ以下のようになっておりますので、必要に応じて設定して下さい。なおこれは

復号には関係ありません。どのモードで暗号化したファイルでも、現在のモードに関係無く復号できます。

元の名前 + 標準拡張子（.ENC）にチェックした時　：

(例) abc.txt → abc.txt.enc

元の名前 + [入力ボックス]にチェックして、入力ボックスに".jpg"を入力した時　：

(例) abc.txt → abc.txt.jpg

ランダム名 + [入力ボックス]にチェックして、入力ボックスに".jpg"を入力した時　：

(例) abc.txt → 6kmpmo9.jpg　や 8r35p8k.jpg　等（ランダム）

Note：

最後の「ランダム名」は、ファイル名から内容が推測されたり、重要度がわかってしまって集中的な攻撃の対象になりやすいファイルの暗号化時に最適です。ちなみに当然の事ながらファイル名は復号時に元に戻されます。

・「アルゴリズム・セキュリティレベルの変更」ボタン―セキュリティレベル

一般的にパスワードは長ければ長いほど良いのですが、暗号化する情報には、個人的な日記もあれば、企業秘密もあるわけで、場合によって必要とするセキュリティレベル（＝パスワードの長さ）は異なってくるでしょう。それに対処するため、EDには、予め必要なセキュリティの程度を設定し、それによって入力されたパスワードの文字数をチェックしたり、暗号化方法を変える機能がついています。

このボタンを押すと、設定ウインドウが開きますので、その中にある調節バーを１～４のうちのどれかにあわせてください。４が最高度のセキュリティです。調節バーを変更する度に、そのセキュリティレベルの説明が下の部分に表示されますので、参考にして設定してください。

Note：

セキュリティレベルとは、パスワードの入力時の最小文字数制限の設定ですので、暗号化方法そのものには違いはありません。つまり、セキュリティレベル１でパスワード

20 文字を入力するのと、セキュリティレベル4でパスワードを同じく 20 文字入力するのは全く同じことです。

・「アルゴリズム・セキュリティレベルの変更」ボタン―アルゴリズム

Ver3.0 より、ユーザが暗号アルゴリズムを選べるようになりました。暗号アルゴリズムとは、ファイルを暗号化する時の手順のことで、これによってその暗号の強度が左右されます。本ソフトに搭載されているアルゴリズムはいずれも十分な強度を持つとされていますので、デフォルトの TwoFish のままで全く問題はないと思われますが、暗号通な方はご利用下さい。変更方法はボックスから必要な暗号を選ぶだけです。

Note:

この機能は暗号化時にのみ適用される機能です。復号時はファイルよりアルゴリズムを自動判別して適用しますので、わざわざ ED を暗号化時に使用したアルゴリズムに設定する必要はありません。

・「登録されているパスワード照合用ハッシュとヒントをクリア」ボタン

このボタンを押すと、暗号化時に登録したパスワード照合用ハッシュと、(オプション設定で保存する設定になっている場合には)パスワードのヒントを、メモリと設定ファイルからクリア(空文字列扱い)することができます。

・「SHA-1 ハッシュ計算」ボタン

このボタンを押して開いたウインドウの「対象ファイル選択・SHA-1 ハッシュ計算」ボタンで任意のファイルを選択すると、そのファイルについての 160 ビット SHA-1 ハッシュ値を計算し、結果をテキスト出力することができます。データチェックなどにご利用ください。なお出力フォーマットは計算された 160 ビットハッシュを 32 ビットずつに 5 分割し、それぞれ 16 進表記で順番に並べたものです。(半角スペースで区切られています。)

Important:

SHA-1 計算機能は、あまり巨大なファイルには対応していませんのでご注意下さい。

全ての設定を完了したら、「閉じる」を押して最初の画面に戻ります。

５－１、暗号技術について

EDで使用できる暗号技術は以下の通りです。かなり贅沢なラインナップと言えましょう。なおこの情報はこのヘルプ改訂時（2009 年 1 月）のものです。

TwoFish 共通鍵暗号

Bruce Schneier 氏を中心とするチームによって開発された TwoFish は、NIST（米国商務省標準化局）による政府標準暗号（AES）選考の最終四候補の中の一つです。TwoFish は選出された Rijndael アルゴリズムに勝るとも劣らない強度と高速性を有しており、前作 BlowFish とともにフリーウェア暗号アルゴリズムの定番ともいえる地位を獲得しています。（本ソフトでの仕様：最大鍵長 256 ビット、実質鍵長 160 ビット、ブロックサイズ 128 ビット、CBC モード）

Rijndael 共通鍵暗号(AES)

1997 年、NIST（米国商務省標準化局）は、これまで利用されてきたものの、強度面での問題が生じてきた、DES 暗号に代わる新たな暗号方式（AES）の採用を公募によって行いました。TwoFish を含めた多くの応募の中、ベルギー人の暗号技術者、ヨアン・ダーメンとビンセント・ライメンによって開発された、この Rijndael（ラインダール）アルゴリズムは、その洗練された設計を認められ、2000 年 10 月、アメリカ合衆国政府の公認暗号の座を獲得しました。（本ソフトでの仕様：最大鍵長 256 ビット、実質鍵長 160 ビット、ブロックサイズ 128 ビット、CBC モード）

GOST 28147-89 共通鍵暗号

GOST 28147-89 は、旧ソビエト連邦の政府標準暗号です。Zabotin、Glazkov、Isaeva によって開発され、1989 年に制定されました。かつては最高機密として鉄のカーテンの裏側で厳重に管理されていたであろうこの暗号アルゴリズムの仕様も、まもなく起こったソ連邦の崩壊によって容易に入手出来るようになっています。なお GOST 28147-89 は Twofish や Rijndael に比べると解読攻撃に対する強度が低いとされていますが、通常の使用には問題ないと思われます。（本ソフトでの仕様：最大鍵長 256 ビット、実質鍵長 160 ビット、ブロックサイズ 64 ビット、CBC モード）

暗号技術は戦略物資です

５－２、暗号技術は戦略物資です

本ソフトウェア(ファイル暗号化ソフト「ED」)は日本国の法律に基づいて作成されています。本ソフトウェアは１６０ビットメッセージダイジェスト暗号及び最大鍵長２５６ビット、実質鍵長１６０ビット、ブロックサイズ１２８または 64 ビットという、極めて高レベルの共通鍵暗号を使用しており、国によっては本ソフトウェアは戦略物資として厳しい取り締まりの対象となる場合があります。

- 日本国外で使用する場合は、必ず、その使用する国の法令に従ってください。
- 日本国内においても、本ソフトウェアで使用している暗号技術の使用が禁止された場合は、直ちに本ソフトウェアの使用を中止し、本ソフトウェアを完全に削除・廃棄してください。
- 本ソフトウェアを日本国外に持ち出し、または輸出（インターネットでの送受信を含む）する場合は、必ず最新の関係法令を調べ、遵守してください。

以上の点を含む、本ソフトウェアを使用して起こったいかなる現象の責任も開発元は負いません。

５－３、著作権・免責事項等について

著作権を含む、本ソフト、ED（本体及び付属ファイル）についてのあらゆる権利は作者である、Type74 Software こと、H.Katayama が保持しています。しかしながら、各暗号アルゴリズム及び一部コードに関しては、それぞれの著作権者が著作権を有しており、それを使用フリー又は特許未出願又は使用料金納付済みにより正当に使用しています。

なお、このプログラムの使用によって生じた損害等については、

- 万一、暗号強度に問題があり解読された場合。
- 万一、暗号や復号に失敗してファイルが破損または失われた場合。
- このソフトを利用して、犯罪またはそれに類する行為が行われた場合。

以上の場合を含め、**いかなる場合も責任を作者は負いません**。予めご了承下さい。（しかしながら、これはバグやご要望に対する作者としての前向きな対処まで放棄するものではありません。）

また、本ソフトは以下の方々にお世話になりました。

・梅木泰宏 氏のヘルプ作成ツール
ヘルプカード97
（ホームページ： http://www2b.meshnet.or.jp/~mono/）

→このマニュアルがヘルプファイルだった際に使用させて頂きました。

・FDEPHIをはじめとする NIFTY-Serve 会議室の皆様

→行き詰まった時にはこれが一番の解決手段でした。（2009年追記：NIFTY-Serve、懐かしい！）

・Moo 様
→Ver3.4b から html 形式になった本マニュアルを、PDF 化してくださいました。

・そのほか、様々な形でご支援下さり、そして今も支援して下さります多くのユーザの皆様

以上、この場にて、厚く御礼申し上げます。

５－４、転載、再配布について

本ソフトの、雑誌や書籍などへの転載（掲載）および、WEB での配布を含む、不特定多数への再配布は、良識と常識の範囲内なら、自由に行って頂いて構いません。ただし、事後で構いませんので、作者に連絡をお願いします（掲載書籍・雑誌等の献本は歓迎します。^^）。なお、事前連絡はすぐにお返事できない場合がございますのでご了承ください。

WEB で再配布する場合は、出来る限り最新版の ED を公開するようお願いします。

いずれの場合でも、ソフトの性質上、作者の供給する圧縮ファイル以外の形態で転載、再配布すること（改造・逆コンパイル・ドキュメントの改訂を含む）は、一切許可しません。事情によりどうしても必要な場合は、作者にその旨連絡し、確認・許可を得てからにして下さい。

コマンドラインオプションを利用した本ソフトの「組みこみ」には一定の制限が設けてあります。

５－５、FAQ（よくあるご質問と回答）

今までに頂いたご質問などの例とその回答です。

Q ： ED を雑誌/書籍に掲載したいのですが？
A ： ありがとうございます。こちらをご参照ください。

Q ： ED を雑誌/書籍に掲載したいのですが、事前承諾が欲しいです。いついつまでに返事をください。
A ： 申し訳ありませんが、期限までにお返事できない場合がございます。

Q ： ED のアーカイブを私のホームページからダウンロードできるようにしたいのですが？
A ： こちらをご参照ください。

Q ： ED を職場（会社・学校・公共機関・政府機関・軍隊 etc..）で使用したいのですがいいでしょうか？

A ： 問題ございません。連絡、ライセンス料などもいりません。ただし免責事項にはご留意下さい。

Q ： ED を友人（同僚・知人・得意先 etc..）に送りたいので、再配布を許可してください。
A ： 許可は必要ありません。不特定多数向けの再配布ではないので、連絡も必要ありません。

Q ： 商品を ED で暗号化しておいて、そのパスワードを有料販売する商売を行っています。問題ありませんか？
A ： ED の利用に関しては問題ありません。暗号化された商品といっしょに ED の改変されていないアーカイブを配布しても構いません。

Q ： ED を開発中のシステムに組み込んで販売または納品(有償)したいのですが？
A ： 事前連絡・許可が必要となります。詳しくはこちらをご覧ください。

Q ： ED を営利目的のシステムに組み込んで自社で運用するのは構いませんか？
A ： それは職場での使用に準じた用途なので、問題ありません。連絡も必要ありません。

Q ： ED 単体をパッケージ販売したいのですが？
A ： 事前連絡・許可が必要となります。

Q ： 会社で使用しているのですが、特別の用途に使いたいので有償で改造してもらえますか？

A ： メールにてご相談下さい。

Q ： Ver2.1 以前で暗号化したファイルが解読できません。
A ： こちらをご覧下さい。

Q ： パスワードを忘れてしまったのですが、解読方法はありませんか？
A ： 申し訳ありませんが、パスワードを入力する以外の解読方法はございません。

Q ： 暗号化できません。or 絶対正しいパスワードなのに復号できません。
A ： 一番多いのが、CD-R などに保存していたファイルで、読み出し専用(Read only)がついていたケースです。必ず解除して下さい。

Q ： Windows2000 や XP などの「暗号フォルダ」内でも使用できますか？
A ： 基本的に使用でき、セキュリティ向上が望めますが、環境などによっては不具合がでる可能性がありますので 、予め不要なファイルなどで暗号化・復号が問題なくできることを確認した上で使用することをお勧めします。

Q ： パスワードを全角で設定 or 入れたいのですが。
A ： カット＆ペーストすれば可能なはずですが、出来ないケースが報告されております。その場合はコマンドラインオプションをご利用ください。

Q ： 関連付けしたいのですが？
A ： ED は拡張子が一定というわけではないので、コマンドラインオプションを参考にユーザ様の方で設定してください。

Q ： 多重起動の防止機能を切る方法はありませんか？
A ： ED.ini の[SYSTEM]項目に DBCHK=0 を追加して下さい。（未推奨、上級者向け）

Q ： 2GB 以上のファイルを処理できますか？
A ： Ver3.21 までの ED は、仕様(32bit 変数で構成されている)により 2GB 以上のファイルを処理すると表示がおかしくなっていましたが、Ver3.3b より 2GB 以上のファイルも対応するようになりました。

Q ： Ver3.3b からはどのくらいの大きさのファイルまで処理できるようになりましたか？
A ： プログラムだけ考慮した場合の理論上の推測上限値は 2,305,843,009,213,693,951 バイト＝大体二百万テラバイト程度ですが、現実的にはファイルシステムや OS、そしてなによりもハードウェア的な制限があるかと思いますので一概にはいえません。未知の大きさのファイルを ED で処理する時は、バック

アップをとってテストするなど、より一層慎重に使用してください。（逆にこんな「大きなファイルを処理しています」というお話をお寄せ頂ければ参考になります。）

Q ： 実質鍵長ってなんですか？
A ： パスワードは 160bit メッセージダイジェスト暗号でハッシュ化されますので、実質的な強度（実質最大鍵長）は 160bit(半角 20 文字)までとなります。

Q ： PGP とどっちが安全でしょうか？
A ： まず ED には公開鍵暗号がついていないという点で用途が大きく異なります。共通鍵暗号については実質的にどちらも安全と思われます。

Q ： イーディーという名称は不快なのでやめてください。
A ： それは製薬会社様へ(^^;;;)。（エドと呼んでもらうことも検討しましたが、やめました。^^;）

Q ： 暗号技術を配布することは犯罪を助長していることにならないか？
A ： クレジットカード決済やネットバンキングなどで利用されている SSL(ブラウザの鍵マーク)のように、暗号技術は今やなくてはならない存在となっています。むしろ暗号技術が存在しないほうが、犯罪のリスクは高まるのではないでしょうか。

Q ： リストを送ってください。or 私の住所は●×□です。or まだ届かないのですが？
A ： 申し訳ありませんが、当方は単なる暗号化ソフトウェア作成・公開元以上の何者でもありません(^^;;;;;)。

Q ： 抹消機能の仕様を教えてください。これはどのくらい安全なんですか？
A ： 抹消機能は単調なデータで一回上書きするという簡単なものです。通常はこれで十分ではないかと思いますが、不安な方は他の専用ツールを併用されることをお勧めします。詳しくはこちら。

Q ： Ver3.2 で加えられた抹消機能の改善点とはなんですか？（ていうかそれ以前はどうだったんだじゃあ？）
A ： Ver3.2 より前のバージョンでは、上述の上書きが正しく行われていない場合があるとのご報告を頂きましたので、その点を改善しました。（その場合でもファイルサイズ等の消去は行っていたので、一定の秘匿効果はありました。）また Ver3.2 以降でも、不具合がありましたらご連絡ください。(^^;)

Q ： 抹消機能と暗号化強度に直接の関連性はありますか？
A ： ありません。抹消機能は PC を中古に出した時や、HDD ごと盗難にあった場合、悪意のある人間と PC や記録媒体（HDD、FDD、USB メモリなど）を共有する可能性がある場合などに対処するための機能です。例えば、暗号化したファイルをインターネット経由で送信する場合、抹消機能は通常関係ありません。詳しくはこちら。

Q ： 暗号化/復号/抹消速度を速くする方法はありますか？

A ： ED.ini の[SYSTEM]項目に PROCESSMSGINTV=(0～10000 程度の整数値)を追加してください。この値はブロック処理毎にメッセージ処理を行うタイミングを規定しており、デフォルト値は 30 です。この設定値がデフォルト値より大きいほどメッセージ処理が行われる間隔が長くなりますので、その分暗号化/復号/抹消速度がデフォルト設定時より向上する可能性がありますが、その一方で ED が固まったようになり、経過も分かりづらくなっていく上、単位時間当たりのリソース消費量も多くなります。（未推奨、上級者向け、変更時は運用前に必ず不要ファイルでテストして下さい。）

Q ： 暗号化/復号/抹消時のリソース消費量を減らす方法はありますか？
A ： ED.ini の[SYSTEM]項目に PROCESSMSGINTV=(0～10000 程度の整数値)を追加してください。この値はブロック処理毎にメッセージ処理を行うタイミングを規定しており、デフォルト値は 30 です。この設定値がデフォルト値より小さいほどメッセージ処理が行われる間隔が短くなりますので、その分 ED の単位時間当たりのリソース消費量が少なくなる可能性がありますが、その一方で処理にかかる時間は長くなっていきます。（未推奨、上級者向け、変更時は運用前に必ず不要ファイルでテストして下さい。）

５－６、開発履歴

●Ver1.0 (1999/10)

・公開

●Ver1.01 (1999/11)

・復号パスワード入力部分での不具合に対処

●Ver1.02 (2000/1)

・インターフェース部分の細かな修正
・出力ファイル名に関する設定オプションを追加

●Ver2.0 (2000/3)

・暗号化後のファイルを暗号化前のファイル名に変えてから「復号後に元ファイルを抹消」環境下で復号するとファイルが失われてしまう現象を改善
・拡張子を手動設定にして、なおかつなにも入力しないまま暗号化するとファイルが失われてしまう現象を改善

・暗号化前のファイルの日付時刻スタンプを復号時に復元するようにした

●Ver2.1 (2000/12)

・コマンドラインオプションの改善
・それに伴うヘルプ改訂

●Ver3.0b(2001/12)

・復号時の確認を１回にした（多くのご要望を頂きました^^;）
・「考課表」などの漢字名フォルダを含むパスが正しく処理されないバグの改善
・暗号化手順の変更による処理の高速化（２～３倍）
・大容量ファイルへの対処のため、ファイル毎に正確な経過を表示するようにした
・ヘッダ仕様の変更によるセキュリティの向上

・Rijndael、GOST 28147-89 アルゴリズムの追加
・アルゴリズム選択機能追加とそれに伴うダブルアルゴリズム機能の廃止（処理が遅い割にはあまり必要性が無く、またアルゴリズムを変えて再度暗号化することにより手動で実現できるので）
・RC6共通鍵暗号使用の停止（AES が終了し、パテントに問題がでてきたため）

・多重起動防止機能を切れるようにした（FAQ参照）
・それらに伴うヘルプ改訂

●Ver3.0(2003/8)

・久々に開発作業を行い、やっとβがとれました(大変お待たせしました)
・全ての処理に成功した場合に「失敗数」というメッセージを出さないようにしました

・コマンドラインオプションを直しました。
・読み取り専用で処理がエラーになったときにメッセージを表示するようにしました
・暗号化/復号/抹消処理中ののメッセージ処理を減らすことにより、処理の高速化をはかりました
・それらに伴うヘルプ改訂

●Ver3.1(2004/2)

・アーカイブ属性のフォルダが正しく処理できないバグを修正しました
・保存先を指定するコマンドラインオプション(-A)を追加しました
・オプション設定でメイン画面を常に前面に表示できるようにしました
・処理後ただちに終了するコマンドラインオプション（-I）を追加しました

・それらに伴うヘルプ改訂

●Ver3.2(2004/11)

・照合用ハッシュを用いた暗号化時にはパスワードを1回入力するだけで済むようにしました
・抹消機能に改善を加えました
・それらに伴うヘルプ改訂

●Ver3.21(2004/11)

・XP などでの暗号化時に照合オプションが変更できなくなる不具合を修正しました
・照合用パスワードハッシュのクリア機能を設けました
・汎用的に利用可能な SHA-1 ハッシュ計算機能を設けました
・それらに伴うヘルプ改訂

●Ver3.3b(2005/9)

・暗号化と復号において、2GB 以上のファイルに対応しました。

（プログラムだけ考慮した場合の理論上の推測上限値：2,305,843,009,213,693,951バイト＝大体二百万テラバイト程度）
・連続復号や再暗号化に便利なように、「使用中は前回のパスワードをメモリから消

去しない」オプションを設けました。
・「パスワードのヒントをメモリとファイルに記憶する」オプションを設けました。（記録したヒントの削除機能も設けました。）
・一部のボタンにポップアップヒントを付与しました。
・復号後に抹消するかどうかをオプションで選択できるようにしました。
・暗号化と復号化後に行われる抹消をその都度スキップできるようにしました。

・各種処理中の状況表示をよりわかりやすくしました。
・各種処理中にメッセージ処理を行うタイミングを設定ファイルで変更できるようにしました。
・暗号化先や復号先に同名ファイルがあると上書きされる点を改善しました。
（同名ファイルがあった場合は_RENAMED を付加。）
・オプションの部品配置を変更しました。
・WEB サイト移転に伴い、オプション画面とヘルプ中の URL を変更しました。
・それらに伴うヘルプ改訂

●Ver3.3(2005/10)

・Ver3.3b のベータ表示をとりました。
・初回起動時にメッセージが表示されるようにしました。

・暗号化/復号ファイル名に文字数制限（半角の場合で 200 文字未満）を設けました。
・ヘルプの FAQ 項目にメッセージ処理を行うタイミングの設定方法を追加しました。
・それらに伴うヘルプ改訂

●Ver3.4b(2009/2)

・再暗号化機能を追加しました。
・抹消ごみ箱をメイン画面の下部に出すオプションを設けました。
・抹消ごみ箱実行時、確認メッセージを２重に出すようにしました。
・ファイルをドラッグ＆ドロップした際に、処理画面がなるべく前面にでるようにしました。
・処理画面のレイアウトを少し調整しました。
・それらに伴うマニュアル改訂（およびHTML、PDF化）

５－７、作者連絡先・WEB サイト

バグのご報告、ご意見、ご感想、ご提案、ご質問 etcは WEB サイト、
http://type74.org/
の掲示板までどうぞ。最新版や他ソフトの公開なども行っておりますので、是非お越しください。

メールでのご連絡は
type74@ssbn.office.ne.jp
までお送りください。

□メールでのご質問は、FAQ や上記 WEB サイトの掲示板で解決しなかった場合にお願いします。また、頂いたメールにはほとんど全て目を通しておりますが、すぐにお返事できない場合がありますので予めご了承ください。