

ファイル暗号化ツール Encrypt Ver.2.0 取扱説明書

2005年9月24日

弁理士 神谷 岳

目次

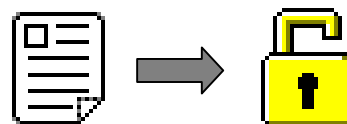
1. はじめに.....	2
2. 使用上の注意点・サポート.....	3
3. Encrypt のインストール.....	4
3.1. 動作環境.....	4
3.2. インストール.....	4
4. ファイル暗号化手順.....	5
4.1. 暗号化の準備.....	5
4.2. Encrypt の実行.....	5
4.3. 暗号化するファイルやパスワードを指定する.....	6
4.4. ファイルの暗号化を実行する.....	8
5. ファイル暗号化解除手順.....	10
5.1. 暗号化解除の準備.....	10
5.2. パスワードの入力・暗号化解除.....	10
5.3. 復元されたファイルの利用.....	11
6. ファイル暗号化の詳細.....	12
7. ファイル暗号化解除の詳細.....	14



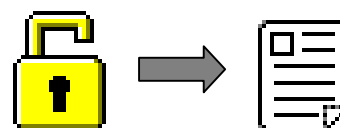
Encrypt Ver.2.0

1. はじめに

Encrypt は、任意のファイルにパスワードを設定して暗号化をするソフトウェアです。



暗号化したファイルは実行形式ファイルⁱⁱになり、それ自体を実行してパスワードを入力すれば暗号化を解除できますので、暗号化の解除を行うコンピュータには特別なソフトウェアはインストールされていなくてもかまいません。また、複数のファイルを1つにまとめて暗号化することもできますし、暗号化を解除した際にディレクトリ構造を復元することも可能です。暗号化自体も、Blowfishⁱⁱⁱアルゴリズムを用いた非常に堅固なものです。



近年、光ディスクの類やいわゆる USB メモリ (USB ストレージ) などの大容量の記録メディアにデータを格納して携帯する機会が増えています。これら記録メディアは小型・軽量で便利なのですが、うっかり紛失してしまうこともありえるでしょう。記録メディアを紛失するだけならまだしも、記録していた機密情報が漏洩してしまうことは非常に危険です。例えば、特許事務所の弁理士は時にクライアントに特許出願前の発明について記載のある電子情報を記録メディアに保存して携帯せざるを得ない場合がありますが、運悪くこの記録メディアを紛失してしまい、記録されている情報が漏洩してしまうと特許が取得できなくなってしまう場合もあります^{iv}。

記録メディアの紛失に十分注意することはもちろんですが、万一紛失してしまった場合にも記録している機密情報を読み取られないようにするため、情報を保存する際にあらかじめパスワードで強力な暗号化を施したうえで記録メディアに保存することができると便利な場合がしばしばあります。そこで、このような処理を実現する簡単なソフトウェア (**Encrypt**) を製作しました。このソフトウェアはフリーソフトウェアとして公開致しますので、どなたでも、商用・非商用に関わらず自由に使用・複製・配布していただいても結構です。ただし、**Encrypt** による暗号化を実行できるのは Microsoft 社製の Windows[®] 2000 や Windows[®] XP 以上の環境のみですのでご了承下さい(暗号化したファイルの復元は Windows[®] 98 等でも問題ありません)。

本書では、ファイル暗号化ツールである **Encrypt** の使用手順を説明します。本書をよく読まれて、**Encrypt** を活用していただければ幸いです。

2. 使用上の注意点・サポート

本ソフトウェア(Encrypt のプログラム本体及び本取扱説明書を含みます)は注意深く製作いたしましたが、個人でのソフトウェア開発ですので動作確認などの徹底には限界があります。とくに、さまざまなバージョンの OS やハードウェアでの動作確認は不可能です。

不具合の修正や御要望に対する対応は出来る限り行いますが、これを約束する物ではありません。Encrypt 製作者はこれらについて何ら義務を負わないものとします。もちろん出来る範囲でサポートは行うつもりですが、個人では限界があり大手メーカーのような徹底したサポートは不可能であることを御了承下さい。特に、本業が忙しい時期や出張で不在にしているときには一時的に全く対応できない期間も発生する可能性があります。

また、万一、本ソフトウェアを使用されることで直接的・間接的を問わずいかなる被害をこうむられたとしても、本ソフトウェアの製作者は一切責任を負いません。使用者の責任の範囲内で本ソフトウェアを使用することを承諾頂ける場合のみ、本ソフトウェアを使用してください。

本ソフトウェアについての不具合について御報告をいただいたり、サポートを御依頼される前に、もう一度「ファイル暗号化ツール Encrypt Ver.2.0 取扱説明書」(本書)に目を通して、勘違いなどが無いことを御確認下さい。その際は、使用しているコンピュータ名、メモリ容量、ハードディスク容量と空き容量、OS のバージョン、そして、本ソフトウェアのバージョン(メインウインドウのタイトルバーに表示されています)程度は少なくとも御連絡ください。また、不具合等を再現させるもっとも簡潔な手順を知らせていただければ早い対応が可能になると思います。

サポートは、神谷岳特許事務所(<http://www2s.biglobe.ne.jp/~gkami/kamipat/>)で行っています。できる限り、こちらにアクセスして掲示板に用件を書き込んでください。なお、急を要する場合や、2週間程度経過しても返答が無い場合などやむを得ない場合には電子メールで弁理士 神谷 岳(kamipat@xqe.biglobe.ne.jp)宛にご連絡願います。もちろん、サポート以外の内容、例えば、使用した際の感想や御意見などもお聞かせ願えれば幸いです。

3. Encrypt のインストール

3.1. 動作環境

ファイル暗号化ツール **Encrypt** を使用するには以下の動作環境が必要です。

暗号化処理

Microsoft® Windows® 2000 以上が快適に動作する環境(Microsoft Windows® XP 等)



暗号化解除処理

Microsoft® Windows® 98 以上が快適に動作する環境

上記のとおり、OS が快適に動作する程度の CPU 速度とメモリ容量を備えていれば、**Encrypt** 自体の動作にはまず問題を発生することはないでしょう。もちろん、より高速なコンピュータを使用されれば、処理はより高速になります。また、**Encrypt** はせいぜい数 10Mbytes 程度の大きさのファイルの暗号化を行うことを前提に設計しています。数 100Mbytes 以上などの非常に大きなファイルの暗号化もできるとは思いますが、処理効率が低下しますので、このような大きなファイルを扱う必要がある場合には他の大きなファイルの処理に適したソフトウェアを使用されることをお勧めいたします。

3.2. インストール

ファイル暗号化ツール **Encrypt** は次の 2 つのファイルから構成されています。これらのファイルを適当なディレクトリにコピーすればインストールは完了です。コピーした **Encrypt.exe** をマウスでダブルクリックするなどして実行してください。また、簡単に **Encrypt** を実行できるように、**Encrypt.exe** へのショートカットをスタートメニューやデスクトップに登録すると便利です。この手順については、Windows®のヘルプで「ショートカット」等をキーワードに検索して調べてください。

アイコン	ファイル名	説明
 Encrypt.exe	Encrypt.exe	Encrypt のプログラム本体です。このファイルをダブルクリックすると、 Encrypt を実行できます。
 Encrypt.pdf	Encrypt.pdf	Encrypt の説明書(本書)です。内容を表示するには、Adobe Systems 社の Adobe® Reader®がお使いのコンピュータにインストールされている必要があります。 Encrypt のメインウインドウの「Show Help」ボタンを押すと表示されます。

4. ファイル暗号化手順

4.1. 暗号化の準備

まず、暗号化したいファイルを作らなければなりません。これは、ワープロソフトや CAD ソフト等、任意のソフトウェアをお使い下さい。ここでは、「秘密文書.doc」というワープロソフトのファイルを暗号化する場合を例に取ります。

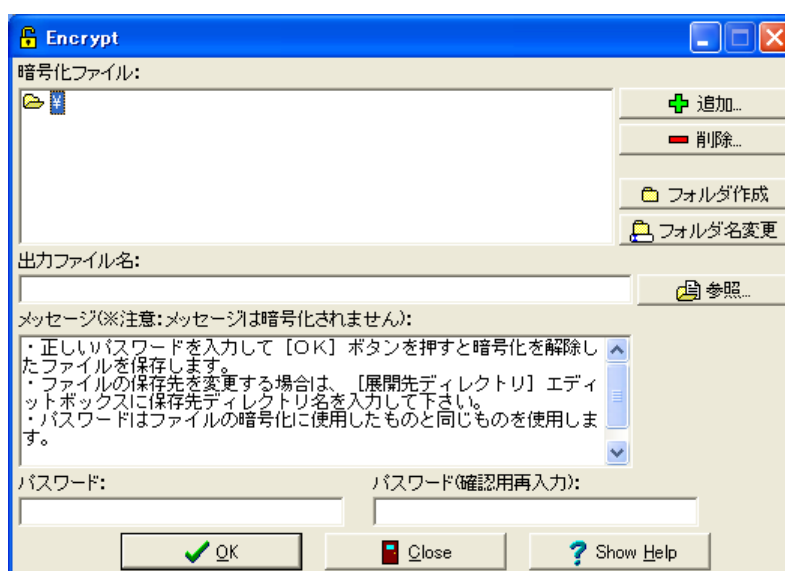
暗号化したいファイル「秘密文書.doc」を例えば「マイドキュメント」フォルダに保存しているとしましょう。また、**Encrypt** のプログラム自体も同じ場所にコピーしているとします。この場合、「マイドキュメント」フォルダは次のような状態になっています。



※この例では、**Encrypt** のプログラム本体である **Encrypt.exe** と暗号化するファイルを同じフォルダにコピーしていますが、これらを同じフォルダにコピーする必要は全くありません。詳しい方は、**Encrypt** をスタートメニューに登録するなど、使いやすいようにしてご利用下さい。

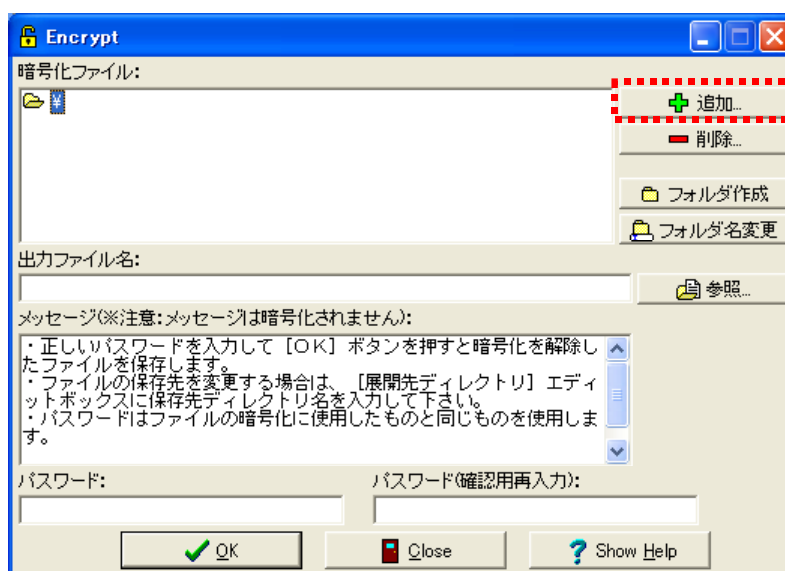
4.2. **Encrypt** の実行

Encrypt.exe をダブルクリックして、**Encrypt** を実行します。次のようなウィンドウが表示されます。

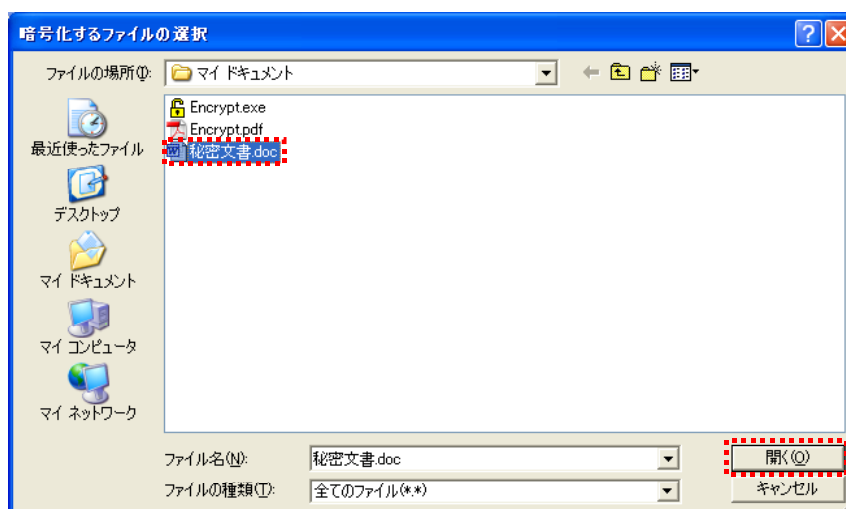


4.3. 暗号化するファイルやパスワードを指定する

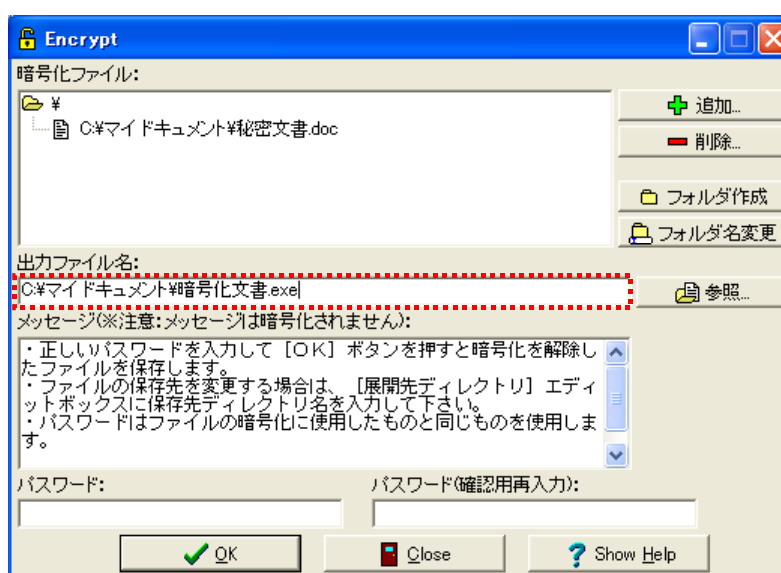
暗号化したいファイルを指定します。今の場合、「秘密文書.doc」を暗号化したいので、「暗号化ファイル」にこのファイルを指定するのですが、それには「追加」ボタンを押します。



すると、ファイル選択ダイアログが表示されますので、「秘密文書.doc」を選択して「開く」ボタンを押します。

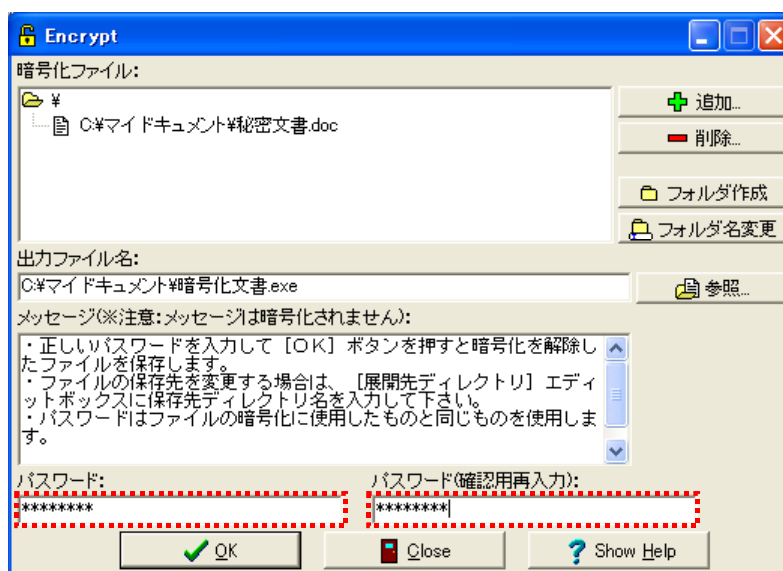


これからファイルの暗号化をするわけですが、暗号化後のファイルの名前はデフォルトでは暗号化するファイル(この例では「秘密文書.doc」)に「.exe」をつけた「秘密文書.doc.exe」になります。わかりやすい名前ではありますが、「秘密文書.doc」という名前の文書が存在することは一目瞭然のファイル名でもあります。どのような名称の文書が存在することすら機密である場合はこのままでは不都合です。そこで、暗号化後のファイル名は「暗号化文書.exe」とすることにしましょう。それには、「出力ファイル名」に表示されている「秘密文書.doc.exe」を「暗号化文書.exe」に書き換えます。



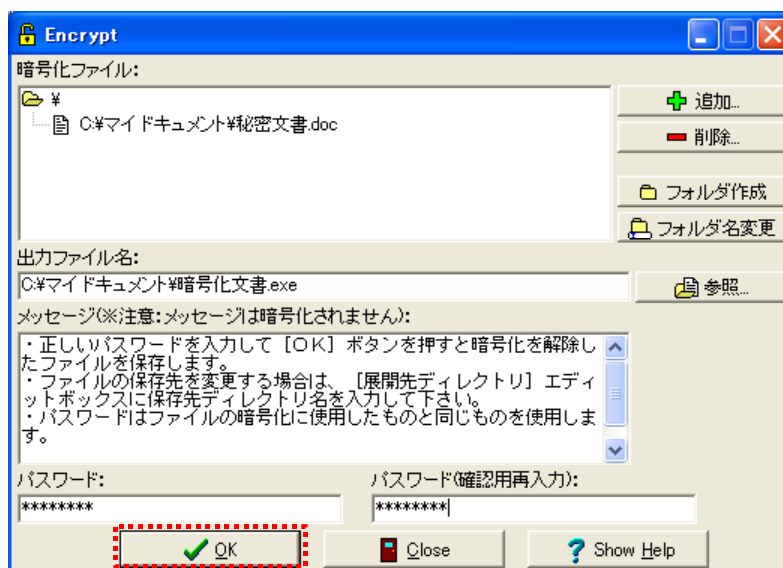
つぎに、「パスワード」を4文字以上の長さの英数字で指定します。パスワードがあまり短いとどうしても第三者に推測されたりしやすくなりますから、できれば英字と数字を織り交ぜて8文字以上程度にされることをお勧めします。なお、パスワードは大文字と小文字が区別され、これを間違えると暗号化を解除できなくなりますので注意しましょう。ま

た、パスワードのタイプミスによって暗号化したファイルが開けなくなるなどの事故防止の為、「パスワード(確認用再入力)」にも同じパスワードを入力してください。ここでは、パスワードに「ABCD1234」を指定しました(画面には「ABCD1234」ではなく「*****」と表示されます)。



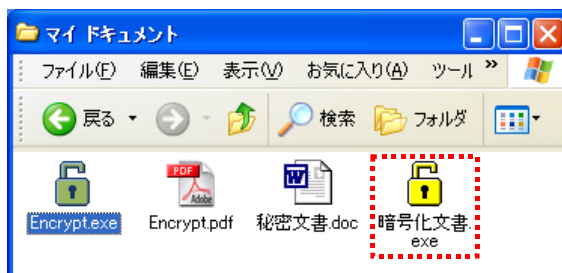
4.4. ファイルの暗号化を実行する

以上で「秘密文書.doc」を暗号化して「暗号化文書.exe」にする準備が完了しました。「OK」ボタンを押してください。暗号化処理が始まります。



正常に暗号化が完了すれば、次のように「暗号化文書.exe」が作成されているはずです。

この「暗号化文書.exe」はパスワードを入力しない限り内容を読み取ることは非常に困難です。この「暗号化文書.exe」を、記録メディアに保存したり、電子メールなどに添付して送れば、このファイルが何らかの事情で第三者の手に渡ったとしても「秘密文書.doc」の内容を読み取られることが無いわけです。電子メールへのファイルの添付方法はお使いのメールソフトによって異なりますので、電子メールソフトのヘルプ機能で「ファイル」「添付」等をキーワードにして検索してみてください。



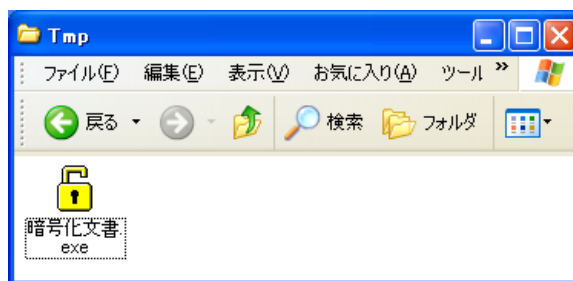
※当たり前の注意点ですが、「暗号化文書.exe」の暗号化を解除して「秘密文書.doc」を得るには、暗号化の際に使用したパスワードが必要です。パスワードを忘れてしまうと、暗号化を解除することは不可能ですのでパスワードの管理には十分ご注意ください(ご相談いただいても対応不可能です)。また、パスワードを第三者の目に触れるところに書き留めておいたり電子メールでパスワードを連絡したりすることは、パスワード漏洩の恐れがあり危険です。十分に注意してください。

5. ファイル暗号化解除手順

5.1. 暗号化解除の準備

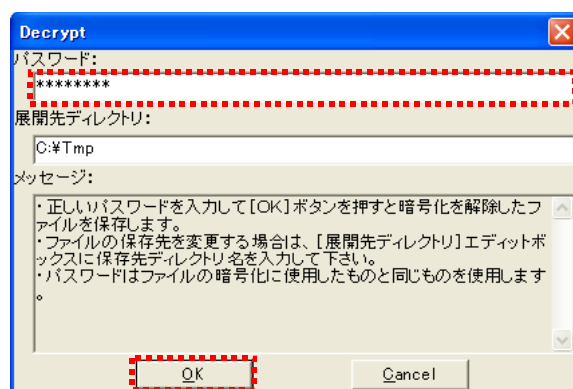
まず、暗号化されたファイルを適当なディレクトリにコピーしなければなりません。電子メールの添付ファイルとして暗号化されたファイルを手入手した場合、お使いの電子メールの説明書などにしたがってこのファイルを適当なディレクトリに保存してください。

今回は、「C:\¥Tmp」ディレクトリに電子メールで受信した「暗号化文書.exe」をコピーしたとします。下のような状態になっているはずです。



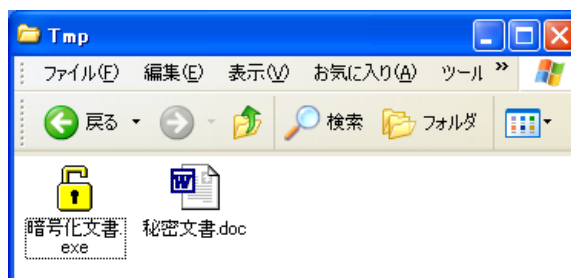
5.2. パスワードの入力・暗号化解除

次に、「暗号化文書.exe」を実行します。エクスプローラなどでこのファイルをダブルクリックすると良いでしょう。すると、次のようなウインドウが表示されます。ここで、この文書を暗号化した際に使用したパスワードを入力します。今回の例ではパスワードは「ABCD1234」でした。パスワードを入力して「OK」を押すと、暗号化ファイルの復元が始まります。



5.3. 復元されたファイルの利用

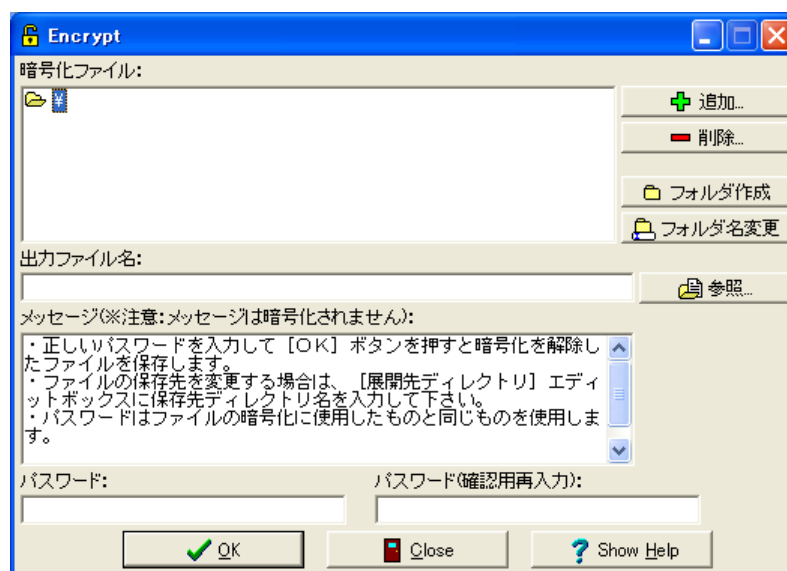
無事復元が完了すると、元のファイルが暗号化ファイルと同じディレクトリに作成されます。今回の例では下の様になります。復元された「秘密文書.doc」を使用してください。



なお、「秘密文書.doc」を復元した後は「暗号化文書.doc」はもはや必要ありませんので、削除してしまって結構です。

6. ファイル暗号化の詳細

Encrypt を実行すると以下のウインドウが表示されます。ここでは、ウインドウ中の各要素についての説明を行います。



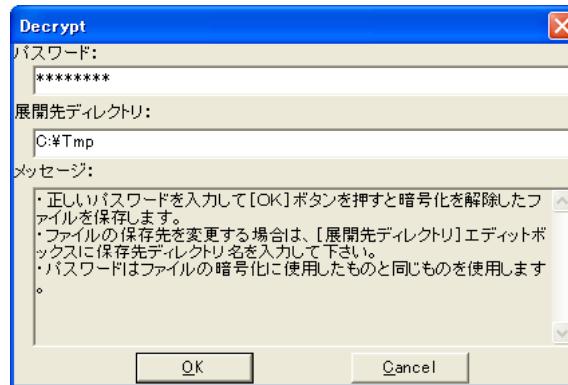
- 「暗号化ファイル」ビュー
暗号化ファイルに含めるファイルの一覧が表示されます。暗号化ファイル中のファイルはディレクトリ構造を持つことができ、暗号化を解除した際には「暗号化ファイル」ビューに表示されているディレクトリ構造がファイルの展開先に作られます。なお、「暗号化ファイル」ビューの「≡」(ルート)は、暗号化を解除する際には「展開先ディレクトリ」になります。
- 「追加」ボタン
「暗号化ファイル」ビューで選択されているディレクトリにファイルを追加します。このボタンを押すと、ファイル選択ダイアログが表示されます。ここで、暗号化したファイルを選択(複数のファイルの選択が可能)すると、選択したファイルが「暗号化ファイル」ビューに追加されます。
- 「削除」ボタン
「暗号化ファイル」ビューで選択されているファイルまたはディレクトリを削除します。
- 「フォルダ作成」ボタン
「暗号化ファイル」ビューで選択されているディレクトリの下に新しいディレクトリを作成します。
- 「フォルダ名変更」ボタン

「暗号化ファイル」ビューで選択されているディレクトリの名称を変更します。

- 「出力ファイル名」エディットボックス
暗号化したファイルを書き込むファイルを指定します。**Encrypt** では暗号化したファイルは、それ自体が暗号化を解除するためのプログラムでもありますので、ファイルの拡張子は「.exe」にしてください。
- 「参照…」ボタン
「出力ファイル名」エディットボックスにファイル名を指定する代わりに、既存のファイルの名前を「出力ファイル名」に入力する場合は、「参照…」ボタンを押して既存のファイルを選択します。
- 「メッセージ」エディットボックス
ここにメッセージを入力しておくと、ファイルの暗号化を解除するプログラムのメッセージ欄にこのメッセージが表示されます。暗号化を解除する人の為に、適切な説明を記載しておくといのですが、このメッセージはパスワードを入力しなくても表示されますので機密情報は記載しないように注意してください。
- 「パスワード」エディットボックス
ファイルの暗号化に使用するパスワードを 4 文字以上の英数字で入力します。パスワードは大文字・小文字が区別されますので注意してください。また、暗号化を解読されにくくするため、パスワードはできれば 8 文字以上の長さにされることをお勧めいたします。なお、「パスワード」エディットボックスには入力された文字はそのまま表示されず、すべて「*」記号として表示されます。
- 「パスワード(確認用再入力)」エディットボックス
パスワードの入力ミスを防ぐため、「パスワード」エディットボックスに入力したパスワードと同じパスワードを再入力します。
- 「OK」ボタン
ファイルの暗号化を実行します。
- 「Close」ボタン
Encrypt を終了します。
- 「Show Help」ボタン
Encrypt の取扱説明書(本書)を表示します。

7. ファイル暗号化解除の詳細

Encrypt で作成した暗号化ファイルを実行すると、以下のようなウィンドウが表示されます。ここでは、ウィンドウ中の各要素についての説明を行います。



- 「パスワード」 エディットボックス
ファイルの暗号化に使用したパスワードを入力します。パスワードは大文字・小文字が区別されますので注意してください。
- 「展開先ディレクトリ」 エディットボックス
暗号化を解除したファイルを格納するディレクトリを指定します。デフォルトでは、暗号化ファイルと同じディレクトリになっています。
- 「メッセージ」 エディットボックス
ファイルの暗号化時に「メッセージ」 エディットボックスに入力したメッセージがそのまま表示されます。ファイルを暗号化した人からのメッセージが表示されるだけで、ここにデータを入力することはできません。

以上

i 暗号化とは、ここでは通常の手段ではファイルを意味のある内容として解釈することが不可能な状態にすることを指しています。暗号化したファイルは、暗号化を解除することで再度その内容を意味のあるものとして利用できるようになります。

ii **Encrypt** では暗号化したファイルそのものがプログラムになります。そして、このプログラムを実行(エクスプローラ等でダブルクリックする)することで、暗号化を解除できます。暗号化したファイルがプログラムとしての機能を備えるためにややサイズが大きくなってしましますが、暗号化を解除するために特別なプログラムが不要ですから、客先のコンピュータでファイルの暗号化を解除する必要がある場合などは便利でしょう。

iii **Blowfish** とは、1993年に **Bruce Schneier** 氏によって設計された強力な暗号化アルゴリズムです。

iv 新しい発明をしたとしても、その発明が特許出願前に公知になってしまうと原則として

その発明について特許を受けることはできません。

▼ 拡張子とは、ファイル名の末尾の「.」（ピリオド記号）以下の部分のことで、この部分の文字列によってそのファイルの種類を識別します。例えば、拡張子が「.exe」になっているファイルは実行可能なプログラムであることを示します。