People 無限乱数式暗号 System

Ver.1

取扱説明書

1. ソフトウェアの概要

オンザフライ暗号化システム「PeopleLock&Commander」の支援ツールです。
乱数パッケージ「SRG-SDK Prime」を使用して作成していま す。

1. 電子メールのやりとりなど、外部の PC との通信を前提とした暗号システムです。。
2. 論理的に解読不可能を論理証明されている「無限乱数式」を採用しています。

重要機密を電子メールで送付したい時に使用してください。
本システムは、10の27000乗バイトの周期を持つ乱数表を×10の27000乗個内蔵しています。
※実際にはこのうち、19000乗個を使用します。
※「SRG-SDK Prime」は最大27000乗個の乱数列の生成能 力を持ちます。
一度使った乱数は2度と使わないように設計しています。

本システムは、メールへの添付を前提にしているのでアプリケーションスタイルです。
USB メモリ、HDD を前提とした暗号化については、完全自動化動作する「PeopleLock&Commander」を使用ください。

本ソフトは、ドラッグ＆ドロップ形式にて簡単に文書を暗号化するもので す。

2. 簡単な暗号化方法

一番簡単な暗号化方法を説明します。パソコン上のデスクトップ上に出現している。
「People 無限暗号」のアイコンを確認してください。

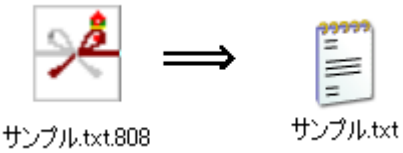
このアイコンに暗号化したい文書をドロップして下さい。

ここでは、「サンプル.txt」という文書をドロップしています。
すると、「サンプル.txt.808」という暗号化した文書が出来ます。これで暗号化は完了です。
※Windows の設定によっては拡張子、ファイル名の最後の. txt、.808 の文字が出ない場合があります。

暗号化した文書は、電子メールなどに添付して相手に贈るなどの使い方をしてください。
お使いのパソコンのディスクを暗号化したいという用途には向きません。この場合は、
「PeopleLock&Commander」
をお使いください。

2. 簡単な解読方法

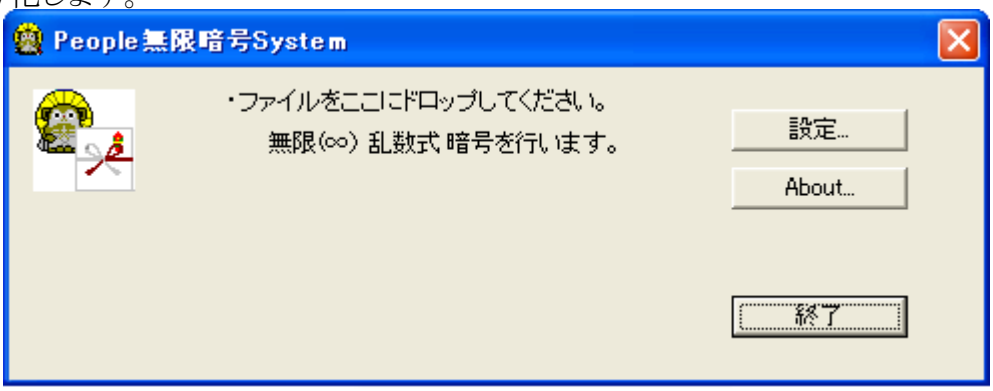
解読は、暗号化された文書をダブルクリックしてください。
自動的に解読を行い、元の文書を生成します。
文書を生成するフォルダは、暗号文と同じフォルダ位置に保存します。



3. より便利な暗号化

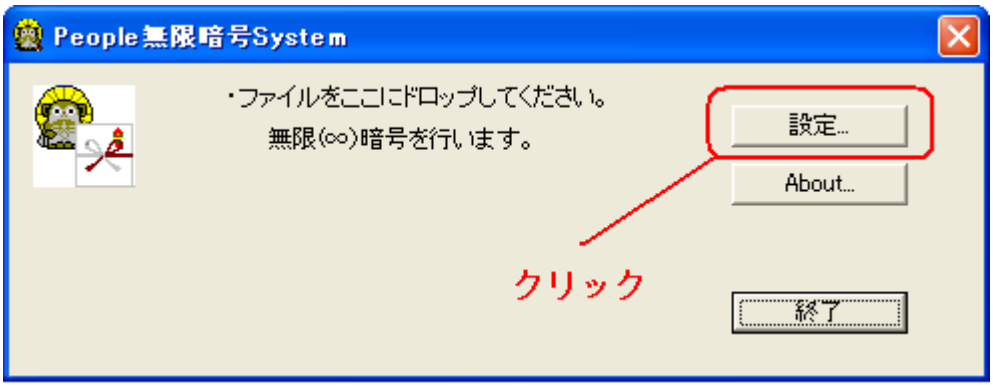
当システムは利便性を高めるために、複数の暗号化方法があります。
①「右マウスの送る」による方法
暗号化したい文書を選択し、「右マウスの送る」より選択してください。
慣れるともっとも便利な使い方です。

② プログラムを起動する方法
当ソフトを起動してください。
次の画面が出ます。ここに、暗号化したい文書をドロップしてください。
暗号化します。

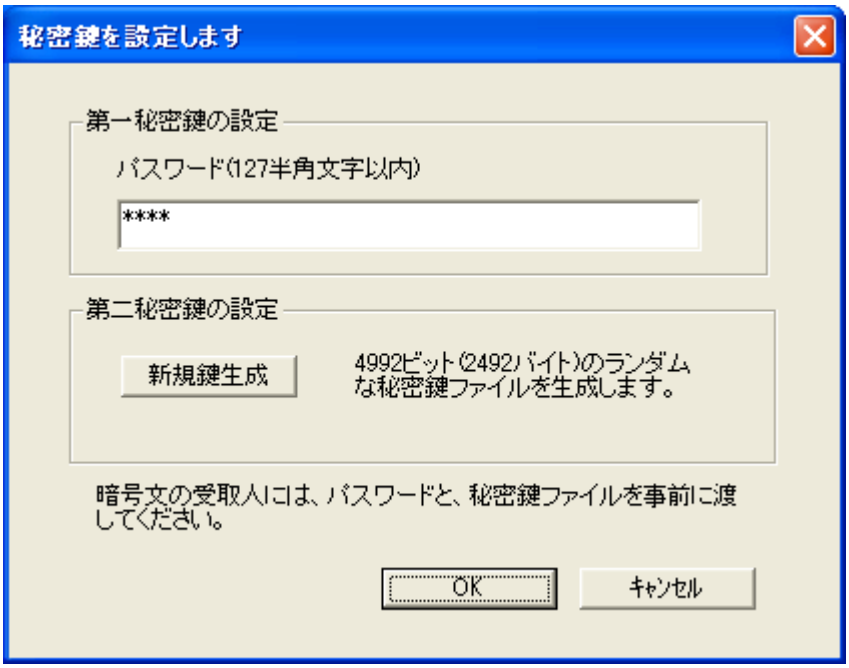


4. 暗号化鍵の設定

暗号鍵の設定方法を説明します。当ソフトを起動してください。

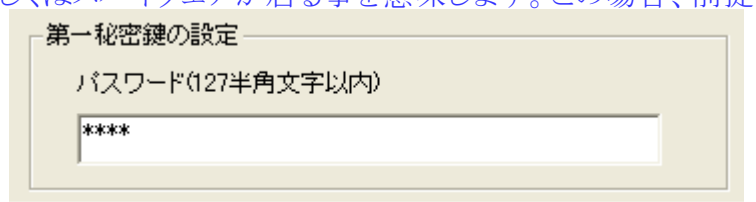


当ソフトを起動して、「設定」を選択してください。
これが当ソフトの秘密暗号鍵、つまり暗号化ルールを決定する画面です。
※当システムは、これとは別に暗黙の上で公開鍵を自動生成しています。
これは利用者は意識する必要はありません。



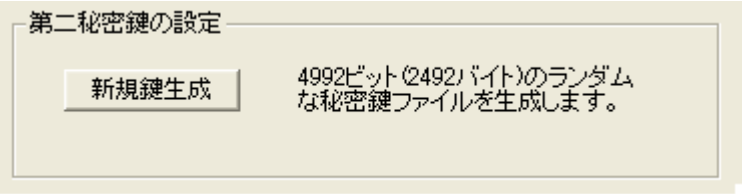
4－1. 第一秘密鍵の設定

暗号化のパスワードを入力してください。
工場出荷状態では、”1234”を設定しています。
パスワードは判り易い文字を選んでください。長さにより暗号強度は変化しません。
※第二秘密鍵が盗まれない限りはパスワードの長短は強度に変化を与え ません。
第二秘密鍵が盗まれた時は、長い方が頑丈です。この時は、事務所内に内通者もしくはスパイウェアが居る事を意味します。この場合、前提が崩れます。



4－2. 第二秘密鍵の設定

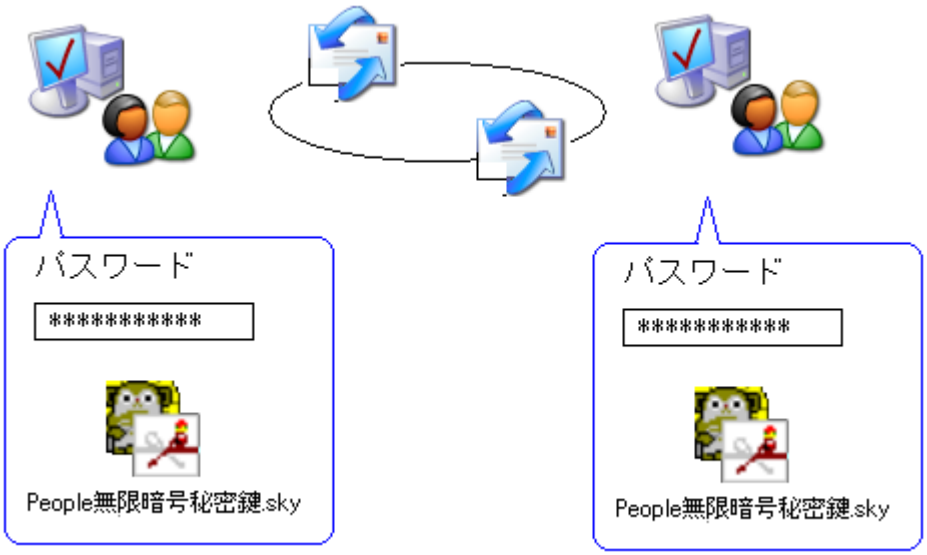
「新規生成」ボタンを押すと、第二秘密鍵を自動生成します。
第二秘密鍵は、毎回異なる情報を作ります。再現性がないので注意してください。
新しく生成すると、以前の暗号化文書は解読できなくなります。



第二秘密鍵は、次の位置に、図のアイコンにて生成します。
※Windows の設定によっては拡張子、ファイル名の最後の. sky の文字が出ない場合があります。

5. 暗号化鍵の共有

暗号化文書の送信人と受信人は事前に秘密の暗号化鍵を共有して置いてください。
秘密鍵が同一の人同士で解読が可能です。
①パスワードを同じにします。
② 同一の「People 無限暗号秘密鍵.sky」ファイルを、「C:\Program Files\People 無限暗号」に保存しておいてください。



6. 暗号強度／無限乱数式について

6－1. 当システムの仕様

- 無限乱数式
  乱数表のうち、一度でも使用した箇所は2度と使用しない方式です。
- 乱数表は10の27000乗バイト列×10の19000乗個
  ※乱数エンジン「SRG-SDK Prime」は最大 27000乗個の乱数列の生成能力を持ちます。

1. 10の27000乗バイトの範囲内では周期のない乱数表を使用しています。

2. 10の27000乗バイトの空間において、無秩序性な乱数です。

・ 共通鍵方式を採用
秘密鍵と公開鍵の組み合わせで、使用する乱数表の位置を決定。

1. 公開鍵
・暗号化する文書ファイルから自動決定。

2. 秘密鍵
・第一暗号鍵にパスワードを採用。
・第二暗号鍵に鍵ファイルを採用。

6－2. 暗号強度

単純な順列組み合わせでの解読は、10の27000乗の繰り返しを行えば解読できる可 能 性があります。
※無限大数が10の68乗です。

また、「平文＋乱数表＝暗号文」の公式より、平文と乱数表の両方が不明な時は 解読は不可能です。
本システムの暗号化強度は、使用する乱数表に依存していると言えます。
本システムの乱数表は内部に 98304 ビット（12288 バイトのワークメモリ）を備えており、十分強力なものです。

本システムは 98304 ビットのうち 65536 ビット（8192 バイト）を使用し 10 の19000乗の 異なる乱数を生成します。
※ち なみに、DES 暗号は56ビット。AES で256ビット。
無限乱数式は外務省の HP に詳しく説明しています。
http://www.mofa.go.jp/mofaj/annai/shocho/e_seifu/toukou2004.html

7. より高度な暗号化

当システムは常識的には十分強力な暗号システムです。しかし、次の懸念があります。
1. 事務所内に内通者（スパイ）がおり、当システムの秘密鍵を抜き取られる場合。
2. スパイウェアがパソコンに混入し、知らない間に秘密鍵を抜き取られる場合。

対策1：
総合的なセキュリティソフト「PeopleLock&Commander」の 導入を推奨します。

対策2：
当システムは、利便性を追求しインストーラにより簡単操作を実現しています。
これを止め、手動により当システムを運用する。

当システムを USB メモリ等、よりセキュリティの高いディスクに保存し、使用してください。
安全性が増します。
標準で、次のファイルを USB などに保存して使用してください。

注意：

1. こ の時は、安全のために2つのファイルをコピーした後、当システムを
   アンインストールしてください。非常に危険です。

2. 「ダブルクリック」、「右ボタン送る」、「ショートカットへのドロップ」は、
   インストーラ標準の当システムを利用します。
   この結果、オリジナルと複製どちらを使ったか判らなくなり解読できなくなります。

8. アンインストール

①[コントロールパネル]の中にある[アプリケーションの追加と削除]より本ソフトを削除してください。

9. お問い合わ せ

有限会社電机本舗
〒108-0074 東京都港区高輪 1-2-16 鈴木ビル 6A
電話(03)5449-7057 PM1：00～17：00
e-mail：tec@dnki.co.jp
URL： http://www.dnki.co.jp/

※ 当ソフトはノーサポートフ リーウェアです。