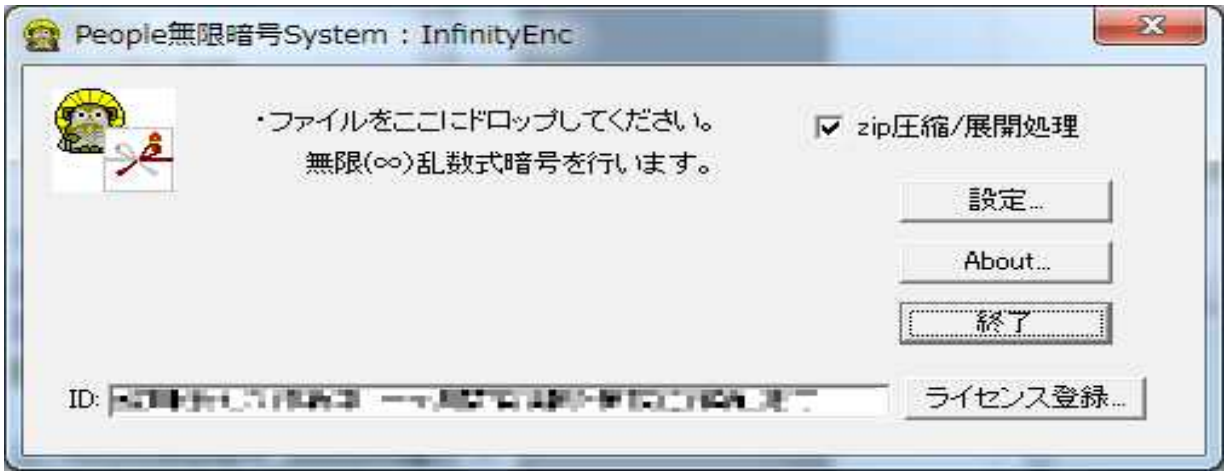
People 無限暗号 system

Ver.2

取扱説明書

（2020/09/19 版）



使用許諾書

「People無限暗号」の使用条件を規定します。

1. 個人（自然人）の使用。
　本ソフトウェアは個人が使用する場合、無料で使用できます。

2. 法人の使用。
　本ソフトウェアを法人はフリーウェアとして使用できません。
　別途、有償の使用ライセンスが必要になります。詳細は下記までご連絡ください。

3. 教育、医療、福祉関連組織、その他団体での使用。
　文末の連絡先までお問い合わせください。「その組織内で使用すると意思決定を行った方」の名義で使用ライセンスを、いくつでも発行することが可能です。通常は、お使いいただく組織の最高責任者、または情報システム管理部門長の名義になります。なお、その方が導入と使用に関する全責任を負う形になります。

4. フリーウェアですので、テクニカルサポートはいたしません。
　本ソフトウェアの使用によって生じた、いかなる損失に関しても弊社は何ら保証いたしません。
　有償の使用ライセンスにもテクニカルサポートは付帯しません。別途サポートライセンスをお求めください。
　サポートライセンスに関するお問い合わせは弊社

5. 本ソフトの転載・転売・リバースエンジニアリングを禁じます。
　雑誌などメディア関連の方で、転載を希望する場合には、
　下記までご連絡ください。

【使用許諾者】【各種お問い合わせ先】
　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)6721-6703　PM1：00～17：00
　　Web-Mail：　https://dnki.co.jp/w2/2016/06/15/mail/

　　URL：https://www.dnki.co.jp/w2/

１．はじめに

「ピープル無限暗号システム」はストレスなく簡単に、ドラッグ＆ドロップ操作でファイルを暗号化／復号化して、情報漏洩を防止するソフトウェアです。
２つの機能を持っています。

１:ファイル単位で簡単、高速に暗号化できます。
２:解読不可能と論理証明されている「無限乱数式暗号方式」を採用しています。

※「ピープル無限暗号システム」は乱数パッケージ「SRG-SDK Prime」を使用しています。
※「ドライブ単位でファイルを暗号化したい」、「より厳密で高度な自動セキュリティ・システムが欲しい」場合には、弊社製品「PeopleLock」の導入を御検討ください。お問い合わせは弊社まで連絡ください。

Web-Mail： https://dnki.co.jp/w2/2016/06/15/mail/

URL： https://www.dnki.co.jp/w2/

２．インストール

２．１．　編集中のデータを保存し、使用中のアプリケーションを終了します。
２．２．　ウィルス対策ソフトの常駐を停止します。
２．３．　「ピープル無限暗号システム」フォルダ内の”Setup.exe”をダブルクリッ クします。
２．４．　続けて出現する画面の指示に従ってインストールを進めます。
２．５．　再起動後にインストールが完了し、デスクトップに下のアイコンを表示します。

重要！　インストール後には本マニュアルを一読してください。
暗号化を試して操作を把握した後、第7章の「オリジナル暗号鍵の作成」を行います。
「オリジナルの暗号鍵」がなければ、暗号化をしても機密を保持することはできません。

※インストールできない場合には、別のパソコンなどで第10章の「対策方法　その2:「ピープル無限暗号システム」の手動セットアップ」をお試しください。

３．アンインストール

「コントロールパネル」の「アプリケーションの追加と削除」から「ピープル無限暗号システム」をアンインストールします。

４．簡単な暗号化方法

4．１．　右 クリックメニューから暗号化する（通常暗号）

※共通鍵を持っている人だけが解読できる盗聴不可能な方式です。
暗号化したいデータを選択し、マウスを右クリックし「右クリックメニュー」画面を表示します。
「送る」メニューから「People無限暗号」を選択すると暗号化します。

すると「のし袋」のアイコンをした暗号化ファイルができます（下図参照）。

4. 2.　右 クリックメニューから暗号化する（割符暗号）

※電子メールの盗聴さえ防げれば良い簡単な暗号方式です。

このように2つの暗号化ファイルができます。この2つのファイルが揃うと解読できます。
この2つのファイルを個別のメールで先方に送ってください。インターネット中継サーバーの盗聴防止用の簡易暗号です。

4. 3. 電子メールによる簡単な暗号文の送信

現在一般的なパスワードを掛けたzipファイルの添付があります。パスワードは時間を掛けて2通目に入れて送付する方式です。

割符による暗号化はこのような使い方をワンタッチで行うものです。

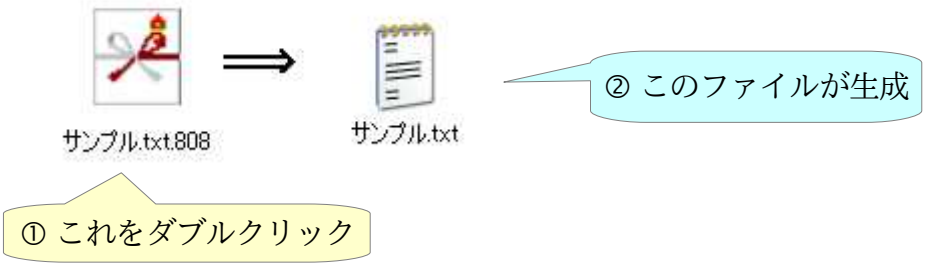
暗号化して出来た2つのファイルを異なるメールにて送付してください。

共通鍵を共有する程ではないが軽い暗号化を掛けたい時に使用します。

５．簡単な復号化方法（簡単な解読方法）

暗号化ファイルをダブルクリックしてください。
自動的に復号化し、元のファイルに解読します。

■通常の暗号ファイルの復号方法



「のし袋」のアイコンをダブルクリックしてください。元のファイルを作ります。

■割符による暗号ファイルの復号方法

同じフォルダに1組のファイルを事前に配置しておいてください。

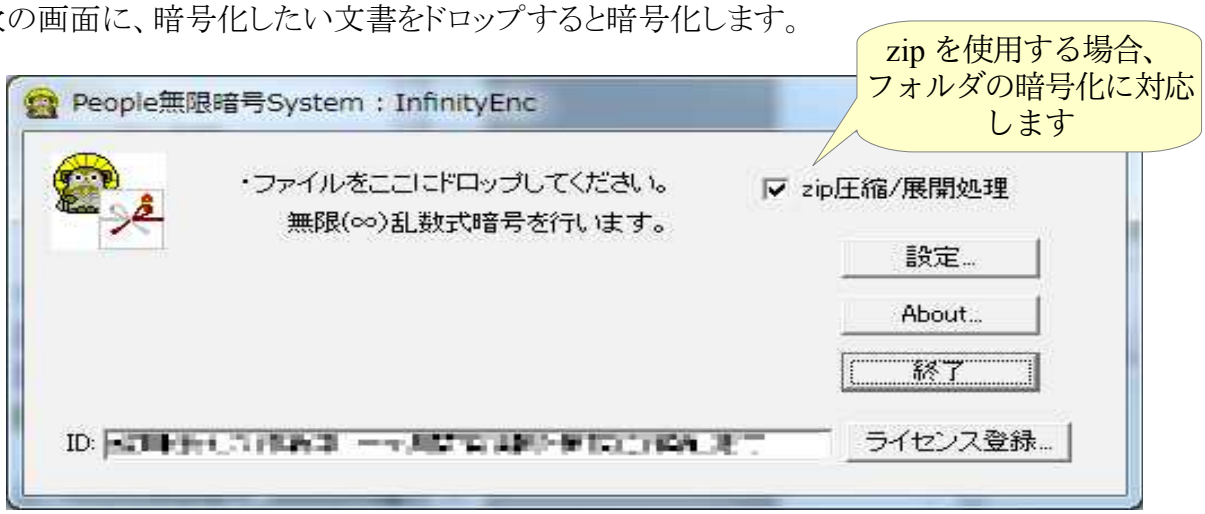
６．その他の暗号化方法

「ピープル無限暗号システム」は複数の暗号化方法を搭載しています。
使いやすい方法で暗号化または復号化してください。

６．１．「ピープル無限暗号システム」画面から暗号化する

はじめに「ピープル無限暗号システム」を起動します。

次の画面に、暗号化したい文書をドロップすると暗号化します。



７．オリジナル暗号鍵の作成

オリジナルの暗号鍵の生成によって初めて、機密を保持する暗号化ファイルを作ることが可能になります。

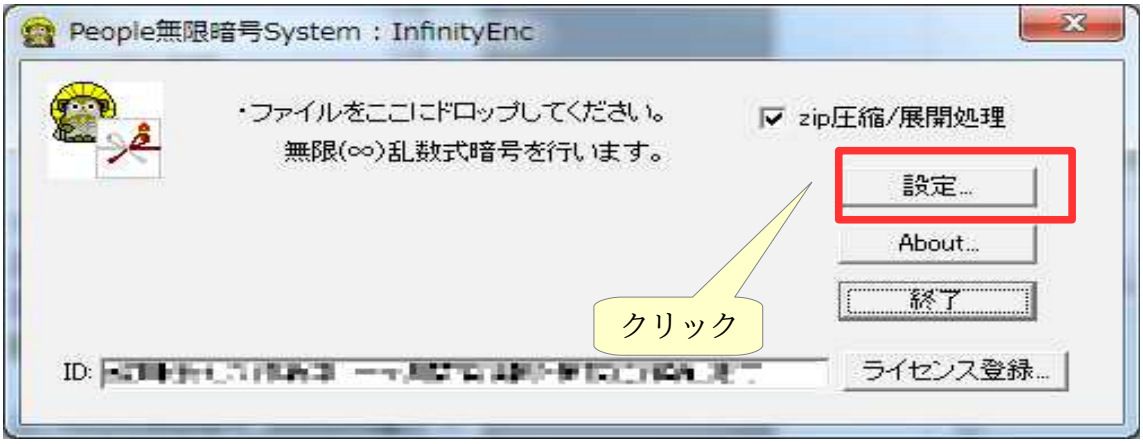
情報を共有したい人物に安全にオリジナルの暗号鍵を渡すことで、電子メールなど情報秘匿性の低い通信システムを用いても機密性を持ったまま情報をやりとりできます。（第8章で説明しています）

「ピープル無限暗号システム」には2つの暗号鍵を設定することができます。ひとつはパスワードの「第一秘密鍵」、もうひとつは鍵ファイル形式の「第二秘密鍵」です。

以下に設定と作成手順を説明いたします。

はじめに「ピープル無限暗号システム」を起動します。

次に「設定」をクリックします。



「秘密鍵を設定します」画面が出現します。

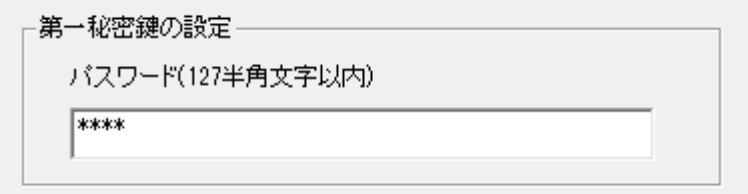
この画面で、オリジナルの暗号鍵を生成します。

【コラム】

「ピープル無限暗号システム」は、この手順で作成・設定するオリジナルの暗号鍵とは別に、公開鍵を自動生成していますが、利用者は特に意識する必要はありません。

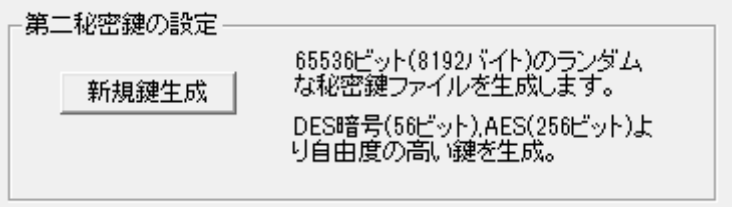
７．１．第一秘密鍵の設定

第一秘密鍵はパスワードの形になっています。
127文字以内、半角英数字の任意の文字列をパスワードとして入力します。
パスワードは紛失や第三者に盗まれないよう記憶するか、金庫などで大切に保管してください。
※工場出荷状態は”1234”です。



７．２．第二秘密鍵の設定

第二秘密鍵は鍵ファイルの形で作成します。鍵ファイルは盗難や紛失が無いよう保管、管理してください。



「新規鍵生成」ボタンを押すと、「プログラムフォルダ」の中の「People無限暗号」フォルダの中に「 People無限暗号秘密鍵.sky」ファイルという名前で生成します。（Windowsの設定によっては、「.sky」という拡張子は表示されません）
なお、インストール時にインストール先を変えた場合は、インストール先のフォルダの中に生成されます。ここでは32bit_OSの例で示します。

注意！　第二秘密鍵は、かならずバックアップしてください。
理由！　同じ第二秘密鍵を二度と作ることはできないためです。
「新規鍵作成」ボタンを押すたびに、毎回異なる新しい第二秘密鍵が生成され、以前の第二秘密鍵を用いた暗号化ファイルの解読ができなくなります。
このため第二秘密鍵を新しく作り直す場合、「全てのデータを復号化」した後に行うか、以前の第二秘密鍵を保存しておく必要があります。

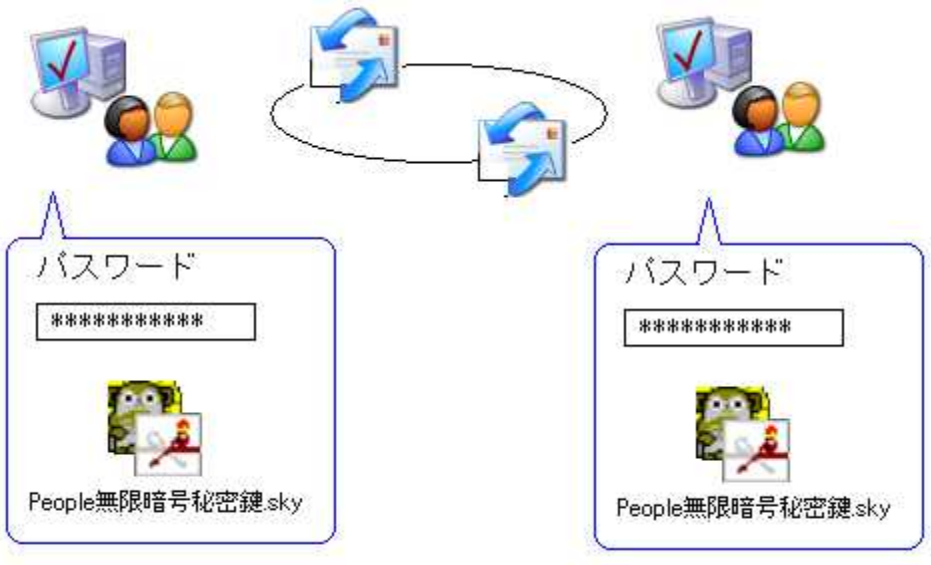
８．オリジナル暗号鍵の共有

本ソフトは2つの暗号鍵にて暗号化／復号化を行います。
送信人と受取人は事前にこの2つの鍵を共有しておいてください。
双方で事前に本ソフトの導入が前提となります。

「People無限暗号秘密鍵.sky」は「People無限暗号.exe」と同じフォルダに配置してください。
通常は次のパスとなります。

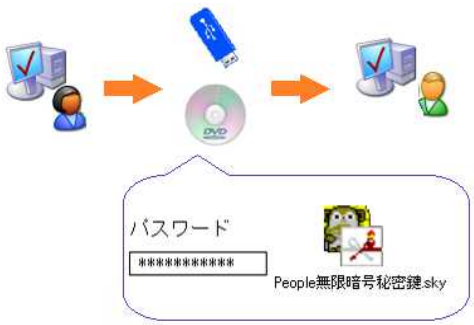
C:\Program Files\People無限暗号　　・・・32bit OSの場合
C:\Program Files(x86)\People無限暗号　　・・・64bit OSの場合

パスワードの設定は前の章を参照ください。



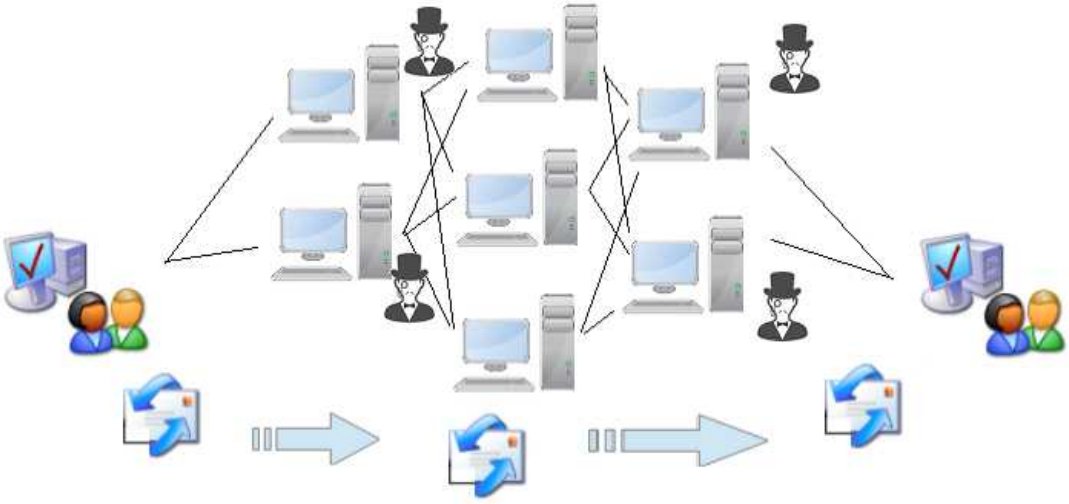
以後、盗聴解読不可能な暗号通信が可能となります。

共通鍵はUSB/DVD-ROMなどによる手渡しが安全です。



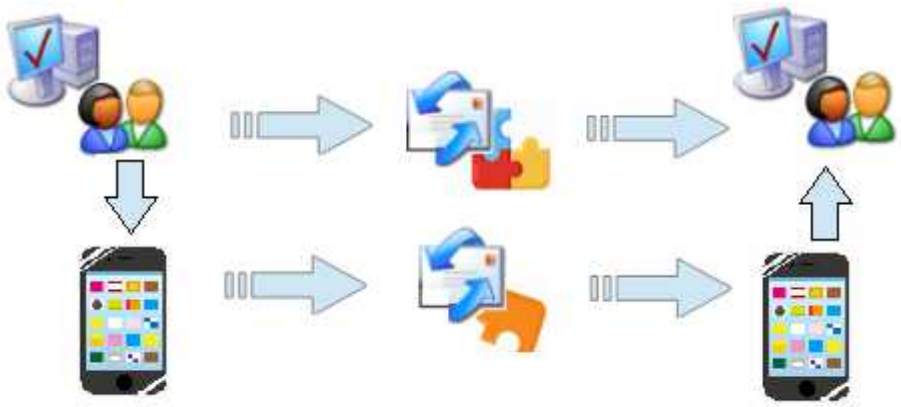
8. 1. 電子メールによるオリジナル暗号鍵の共有方法

電子メールによる共通鍵の送付は**非推奨です**。理由はインターネットの中継サーバーにて共通鍵を盗聴可能だからです。



非推奨ですが電子メールで共通鍵を送る場合、本ソフトの割符を使用して共通鍵を送付ください。

出来た2つのファイルは一方を電子メールで、残る一方をスマホで送信ください。



パスワードは厳密には電話、
略式では SMS が良いです。

９．仕様と詳細

９．１．１．　無限乱数式を採用

一度使用した乱数列を2度と使用しない無限乱数式を採用しています。

使っている乱数表は10の27000乗×10の大きさです。

９．１．２．　乱数エンジン「**SRG-SDK Prime**」を使用

「SRG-SDK Prime」は最大 10の27000乗の乱数列の生成能力を持ちます。

１：10の27000乗の周期性を持ちます。逆に10の27000乗の範囲内であれば周期性はありません。

２：NIST-SP-800-22検定プログラムにてテストを行っています。

※　無量大数が10の68乗です。SRG-SDKは、それよりも膨大な乱数の空間を持っています。

※　NIST-SP-800-22検定プログラムのテスト結果について知りたい方は、お手数ですが弊社のWebを確認ください。

９．１．３．　共通鍵方式を採用

秘密鍵と公開鍵の組み合わせで、暗号に使用する乱数を決定しています。

９．１．４．　公開鍵の生成方法

暗号化する文書ファイルから自動的に生成しています。

９．１．５．　秘密鍵の生成方法

第一暗号鍵は127文字以内、半角英数字の任意文字列のパスワードとして利用者が独自に設定できます。

第二暗号鍵は利用者が任意に生成可能です。鍵ファイルとして生成され、名称は「People無限暗号秘密鍵.sky」です。

９．２．　暗号強度

順列組み合わせで解読を試み、10の27000乗回に達した解読できる可能性があります。

しかし、平文（暗号前文書）と乱数表の両方が不明であるとき、解読は不可能です。

また、「ピープル無限暗号システム」の乱数表は98304ビット（12288バイトのワークメモリ）を備え、そのうち65536ビット（8192バイト）を使用。10の19000乗の乱数を生成して暗号化を行います。

※参考：一般的なDES暗号は56ビット、AES暗号256ビット。

１０．より高度な暗号化システムのご案内

「ピープル無限暗号システム」は強力な暗号システムです。
しかし、運用上の注意が必要です。
1:内部犯行やスパイ
　内部犯行者やスパイによって秘密鍵を盗まれた場合には、機密性が崩壊します。
　秘密鍵を盗難されない環境や状態で使用してください。
2:ウィルスや スパイウェア
　ウィルスやスパイウェアによって秘密鍵を盗まれた場合には、機密性が崩壊します。
　別途、ウィルスやスパイウェアへの対策を必要とします。

対策方法　その1　：「**PeopleLock**」(ピープルロック)の 導入

　弊社の総合セキュリティソフト「PeopleLock」は、主として物理的記憶装置による情報漏洩や盗難を防止する
ためのソフトウェアです。秘密鍵のインストールされたパソコンの利用者を制限できます。正規の権限を持つ
内部犯行者(要するに「裏切り者」です)が、ネット経由で行う情報漏洩に対して備えるものではありません。
　1:任意のUSB メモリなどをパソコンの物理的な鍵として利用できる(ログオンID、パスワードと併用可能)
　2:攻勢防壁機能により「People無限暗号」の動作を自動化することができます。
　3:外部からの記憶装置の持込み、内部からの記憶装置の持出しを無力化します。

対策方法　その2　：「ピープル無限暗号システム」の手動セットアップ

　プログラムを指紋認証USBメモリなどの、セキュリティ対策済みの記憶装置にコピーして使う方法です。
　インストール後にプログラムフォルダに生成される「People無限暗号」フォルダを、セキュリティ対策済みの記
憶装置にコピーします。次に「ピープル無限暗号システム」を「コントロールパネル」の「アプリケーションの追
加と削除」からアンインストールします。
　暗号化の際は・・・
　1:コピーした「People無限暗号」プログラムを起動して暗号化する。
　2:改めて作ったショートカットなどにドラッグする。
　・・・などの方法で、暗号化／復号化します。

１１．お問い合わせ

本ソフトウェアはノーサポートのフリーウェアですので、操作に関するお問い合わせにはお答えいたしません。
法人の有償使用、有償サポートライセンスなどのお問い合わせ、タイトルロゴの変更などのOEMのご相談、鍵生成機能を制限したバージョンなど、さまざまなカスタマイズについては下記まで御連絡ください。

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)6721-6703　PM1：00～17：00
Web-Mail：　https://dnki.co.jp/w2/2016/06/15/mail/

URL：https://www.dnki.co.jp/w2/