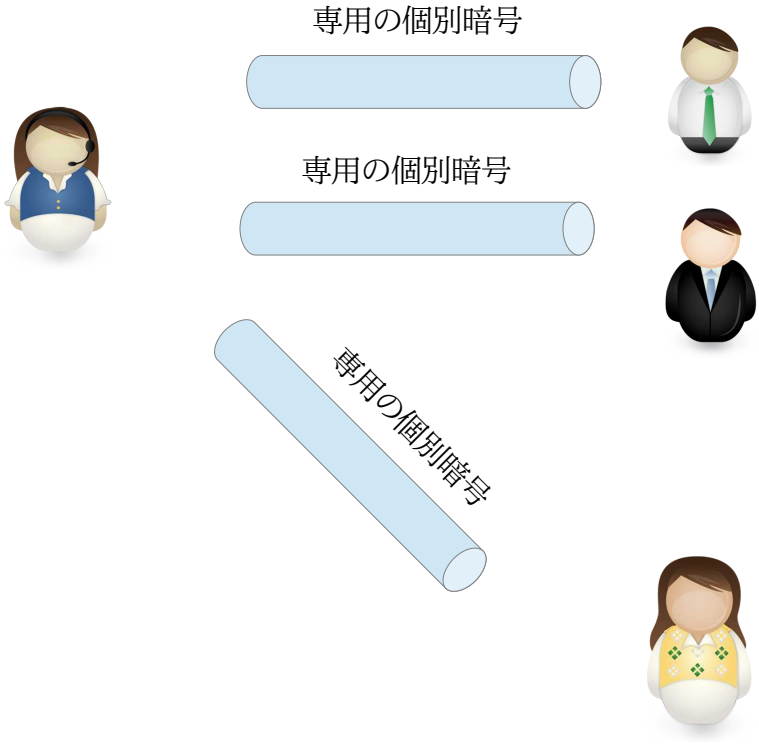
People 無限暗号 **system**

Ver.2 NxN(多数×多数)

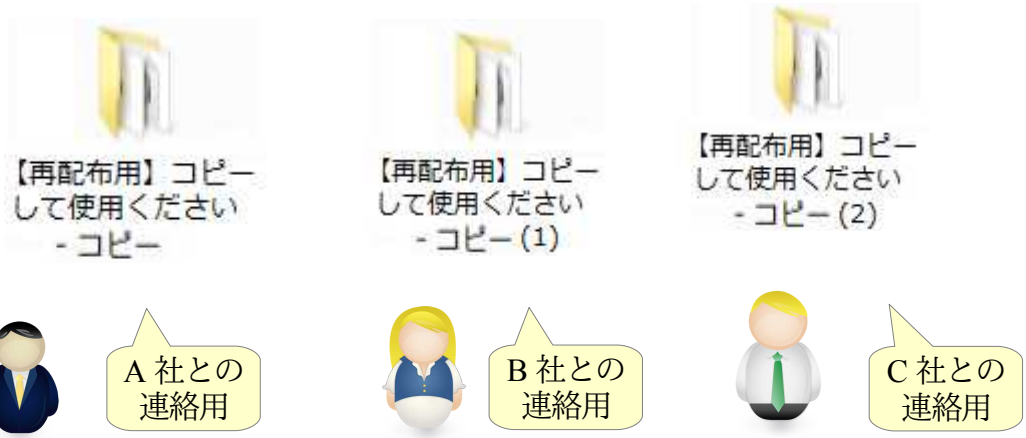
取扱説明書



複数の人／会社とそれぞれ異なる暗号通信をしたい時に利用します。
それぞれ個別に共通暗号鍵を用意します。
多数のグループ、多数の個人と暗号通信に向いています。

1．多数×多数との暗号通信の簡単な実現方法

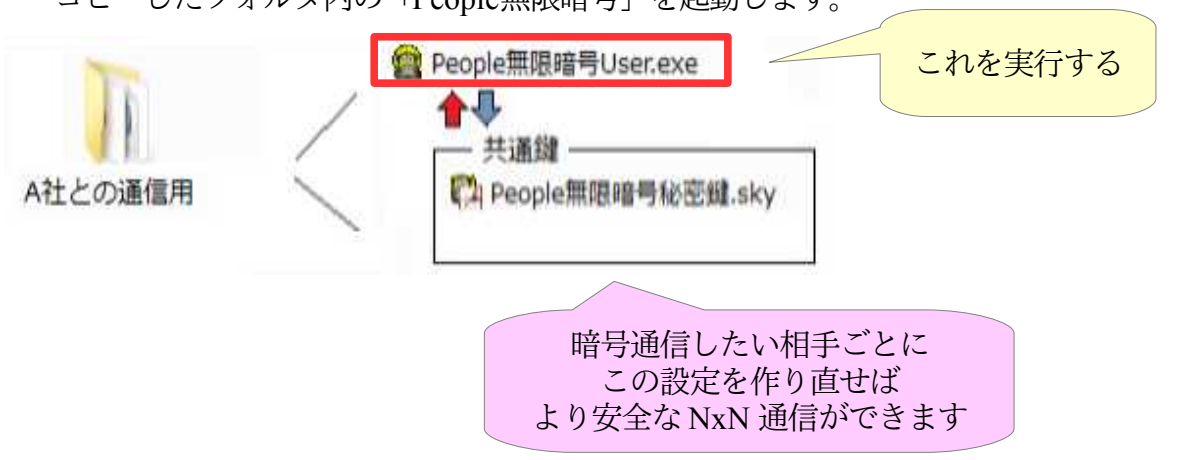
暗号化したい相手ごとにフォルダーをコピーしてください。**コピー先はユーザ権限で書き込みできる場所ならどこでも良いです**。

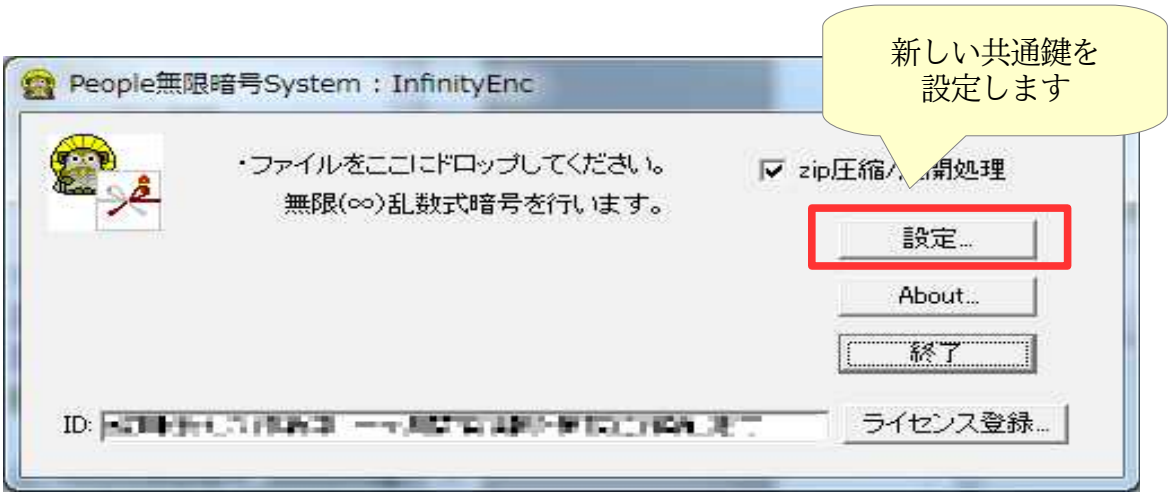


名前は自由に変更できます

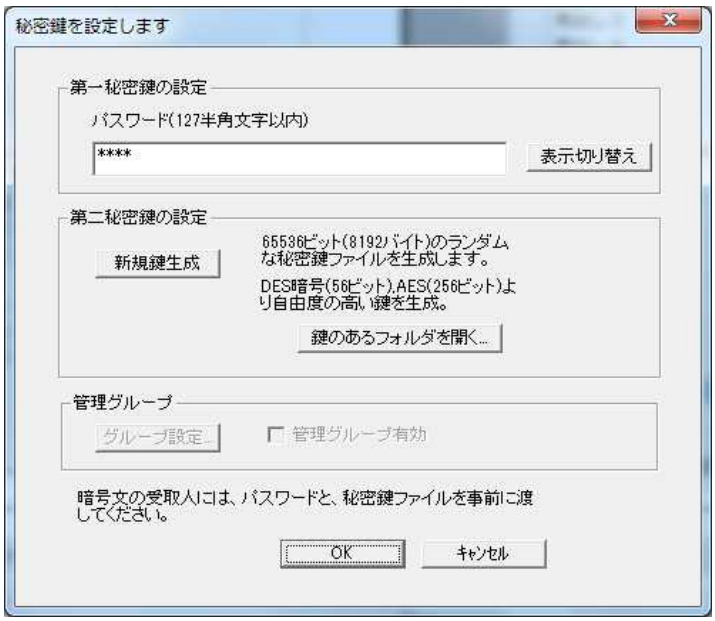
2．フォルダごとに異なるオリジナル暗号鍵の作成

コピーしたフォルダ内の「People無限暗号」を起動します。





「秘密鍵を設定します」画面が出現します。



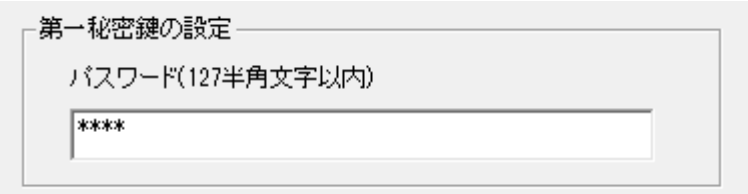
この画面で、オリジナルの暗号鍵を生成します。

【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。

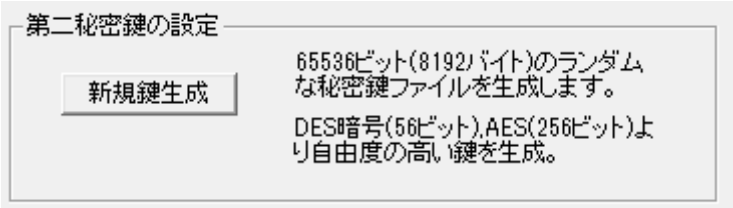
２．１．第一秘密鍵の設定

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。

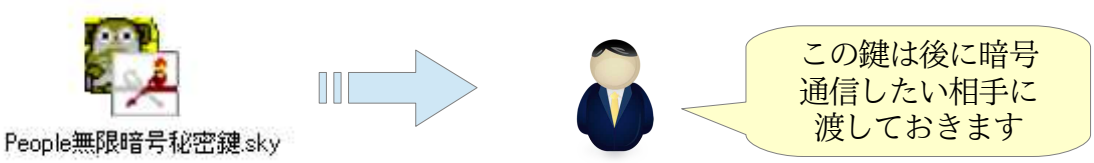


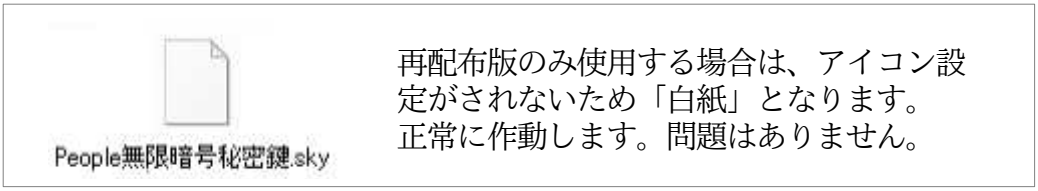
２．２．第二秘密鍵の設定

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「People無限暗号秘密鍵.sky」ファイルという名前で同じフォルダに生成します （Windowsの設定によっては、「.sky」という拡張子は表示されません）。





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。

3．暗号化、復号化方法

ここにある「People 無限暗号 User」に暗号化したいフォルダをドラッグ&ドロップしてください。これだけで暗号化できます。

※Windows の設定によっては、「.txt」・「.808」という拡張子は表示されません。

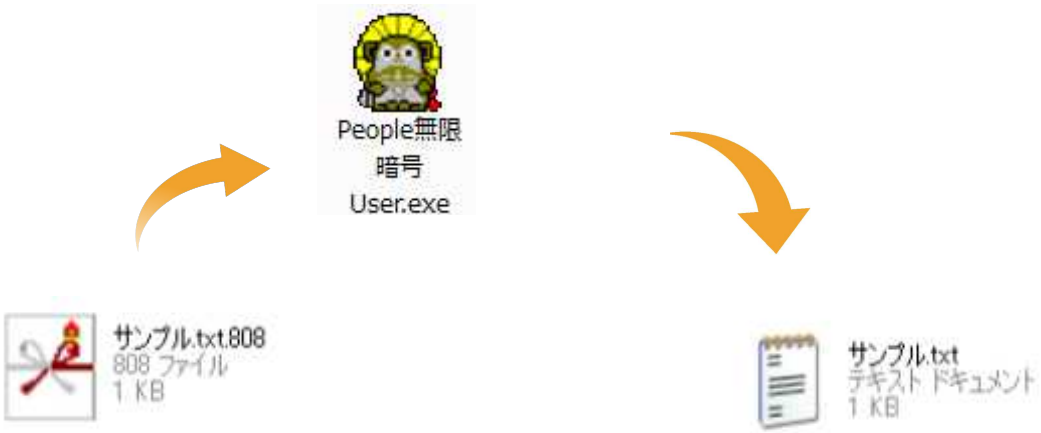
■暗号化方法

暗号化したいファイルを本ソフトにドロップしてください。

再配布版のみ使用する場合は、アイコン設定がされないため「熨斗」アイコンが出ず「白紙」アイコンになります。

■復号化方法

復号化したいファイルを本ソフトにドロップしてください。



再配布版のみ使用する場合は、アイコン設定がされないため「熨斗」アイコンが出ず「白紙」アイコンになります。

４．オリジナル暗号鍵の共有

前章で作ったフォルダを暗号通信したい相手に送付ください。これでNxNの通信ができます。

4. 1. 一番安全な方法

USB, CD-R などで設定した暗号用フォルダを丸ごと渡すのが簡単です。

4. 2. インターネットによる場合

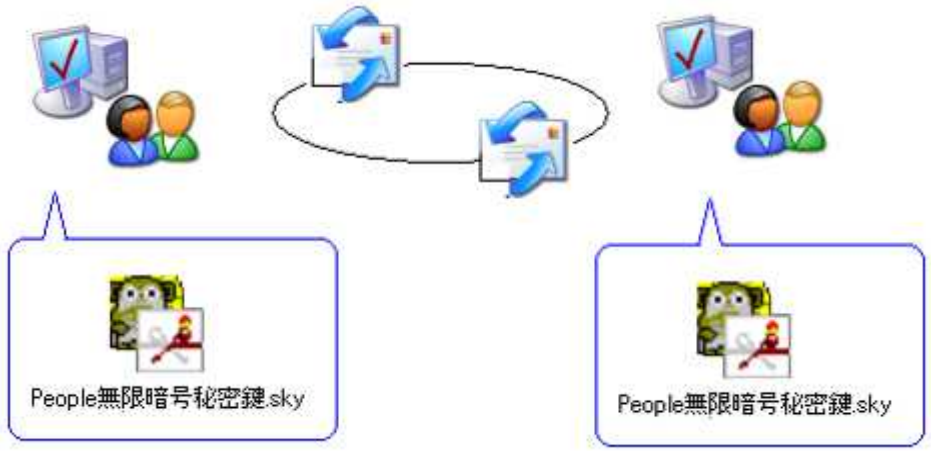
このようにインターネットは中継サーバにえ盗聴の危険があります。ですからインターネットによる共通鍵の送付は**非推奨です**。
ここでは電話とメールによる「より安全」な手順を紹介します。

(1)まず先方に本ソフトの入手してもらいます

・再配布用のフォルダをインターネットで先方に送付ください。
・もしくは次のURLからダウンロードして貰ってください。
https://dnki.co.jp/w2/2020/10/04/peoplemugen/

(2)「 People無限暗号秘密鍵.sky」の送付

次に、3章にて作成した「 People無限暗号秘密鍵.sky」を電子メールにて送付ください。



(3)パスワードの送付

５．仕様と詳細

５．１．１．　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。

５．１．２．　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。

５．１．３．　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。

５．１．４．　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。

５．１．５．　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。

５．２．　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。

６．お問い合わせ

試用版の場合はノーサポートです。
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フラットウェル高輪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/