

ソフトウェアの名称 : Protected Communication System (Twfencrypt)

#### 1. ソフトの概要

電子メールでの添付ファイルの暗号化に Twofish 暗号を利用してください。鍵の長さが長いので貿易管理令に違反しないように HP でソースコードを公開しています。

Twofish 暗号は、「Blowfish」暗号の考案者として知られる Bruce Schneier 氏が考案した、秘密鍵暗号方式の一つです。鍵長は 128、192、256 ビットの 3 種類で、128 ビットのブロックごとに暗号化を行ないます。高速な暗号化と復号化が特徴です。アルゴリズムはライセンスフリーで公開されていて、誰でも自由に使うことができます。

米国商務省標準技術局(NIST)の新世代暗号標準「AES」の候補として最終選考まで残っていましたが、ベルギーの研究者が考案した別の方式 (Rijndael) が採用され、惜しくも標準の座は逃しました。

ソースコードについては、参考文献の最後や、つぎの場所にあります。

[Twofish source code](#)

参考文献

[The Twofish Encryption Algorithm: A 128-Bit Block Cipher \(ハードカバー\)](#)

[John Kelsey](#)

このソフトでは、ファイルの暗号化、復号化がまとめて出来ます。さらに非表示での変換で処理速度が確認できます。電子メールの添付ファイルの暗号化にご利用ください。

送信相手ごとに鍵を変更したり、メールアドレスの管理をしながら暗号メールを利用する場合は、“メールもビットマ”、または、“Cipher Web Mail” をご利用ください。Serpent や AES、RSA などでの 5 段階の多重暗号化が可能です。暗号メールソフトとして機能するのはもちろんですが、暗号化、復号化ルーツとしても機能します。

#### 2. 作者への連絡先(メールアドレス、ホームページ)

メールアドレス : uyama33@yahoo.co.jp (宇山 靖政)

ホームページ : http://uyama22.pa.land.to/ (ソースコード)

#### 3. 取り扱い種別(フリーウェア)

#### 4. 動作環境

Windows Vista Home Premium 32 ビット

Windows 7 Home Premium 64 ビット

の上で動きます。

#### 5. 別途必要なソフト : 特になし (暗号ソフトとして単独で動きます。メール機能はありません。)

#### 6. インストール・アンインストール方法

インストール : TwofishPac.zip を解凍すると、このマニュアルの他に、TwofishSys.zip (暗号ソフトと関連するフォルダ、ファイル) が現れます。

さらに、TwofishSys.zip を解凍すると、“TwofishSys” フォルダが出来ます。このフォルダをデスクトップ等の適当な場所に置き、その中にある

“Twfencrypt.exe” へのショートカットを作成してください。

#### 7. アンインストール : 作成したショートカットと、フォルダを削除してください。

使い方：



1. “TwofishSys” フォルダに、Twfcrypt.exe を置く。
2. 暗号化したい添付ファイルを同じフォルダに入れる。
3. Twfcrypt.exe を起動して、平文の所に暗号化したいファイル名を記入する。  
暗号化されたものの所に暗号化されたファイルの名前を記入する。  
復号化されたものの所に平文のファイル名とは別の名前を記入する。
4. <鍵を作成>のボタンをクリックする。
5. <鍵のテスト>ボタンをクリックして正常に暗号化、復号化出来るか確認
6. 暗号化されたものを添付ファイルとして送信。
7. 相手にもこのソフトをダウンロードしてもらって、鍵を教える。  
復号化鍵を相手の方に前もって届けて置いてください。そのためには、RSA 暗号をご利用ください。  
フリーソフト Protected Communication System(AFCrypt) が利用できます。
8. 相手は、<鍵読込>のボタンをクリックする。
9. 暗号化されたファイル名を正しく入力する。または検索で指定して一括して復号化する。
10. <復号化>をクリックする。
11. 相手は添付ファイルを復号化できる。  
となります。

暗号化鍵、復号化鍵を読み込んでから、暗号化するものを検索して、リストボックスにその一覧を表示しておけば、連続して暗号化、復号化が行えます。

暗号化したものが置かれるフォルダをしっかりと確認してください。この暗号化されたものを復号化することになります。

非表示で、操作すれば **Twofish** 暗号の高速処理が確認できます。この処理速度ならば電子メールを送信する途中で本文や添付ファイルを暗号化できます。

電子メールでの扱いには、メールアドレスとの関連が問題になります。“メールもビットマ”、または“**Cipher Web Mail**”を利用すれば、送信アドレスごとに暗号化鍵、復号化鍵、暗号化アルゴリズムを5段階で設定できます。

電子メールの添付ファイルを暗号化するときは、復号化鍵を相手の方に前もって届けて置いてください。そのためには、**RSA** 暗号をご利用ください。フリーソフト **Protected Communication System(AFCrypt)** が利用できます。

参考：

**Protected Communication System** に関しては、ヨーロッパ、アメリカでの特許を取得いたしました。