

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

#### 1. ソフトの概要

暗号に楽しさを加えようと思って、どんなファイルもビットマップファイルに変換するソフトを作りました。暗号化鍵の長さは、128、192、256 ビットから選択できます。電子メールの添付ファイルの暗号化にご利用ください。普通に暗号化するよりはちょっと楽しいかなと思って作りました。

このソフトを利用して、メールに添付するデータを画像として暗号化してから送信できます。このソフトで暗号化されて送られてきたデータは、拡張子を **bmp** にすれば、画像として表示されます。ほかのメールソフトで受信すれば単に画像ファイルの拡張子が不適切なものが送られてきたということになります。

暗号化の過程では乱数を利用して、同一データも暗号化する時間が異なれば結果も異なりますので、暗号化されたものが同一化データか否かは判定が難しくなっています。

このソフトでは、ビットマップファイルを 16 進数で表示します。ベクターからフリーソフトとして公開している“何でもビットマ”では、直接画像として表示します。もちろん、画像データファイルとして保存されていますので、拡張子が **bmp** になっていることを確認するか、または、**bmp** に変更してから、保存された画像ファイルをダブルクリックすれば、画像として表示されます。

#### 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 : **BmpCryptPac.zip** を解凍すると、このマニュアルの他に、**BmpCryptSys.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、**BmpCryptSys.zip** を解凍すると、“**BmpCryptSys**” 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

“**BmpCrypt.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、4 つのフォルダを削除してください。

使い方：

1. 適当な場所に、“BmpCryptSys” フォルダをつくり、BmpCrypt.exe へのショートカットをつくる。
2. 暗号化したいファイルを同じフォルダに入れる。
3. BmpCrypt.exe を起動して、  
平文の所に暗号化したいテキストファイル名を記入する。

暗文の所に暗号化されたファイルの名前を記入する。

”EC¥encrypt.bmp”とするとサブフォルダ”EC”の中にこの名前のファイルとして暗号化されたものが作成される。

復文の所に平文のテキストファイル名とは別の名前を記入する。(フォルダが異なるので同名でも良い。) ”dc¥decrypt.txt”とするとサブフォルダ”DC”の中に復号化されたファイルが作成される。

4. 鍵の長さ (128、192、256 ビット) を指定する。
5. 鍵を作る ボタンをクリックする。
6. 暗号化と復号化のテスト ボタンをクリックする、
7. 鍵を保存して終了。

が基本操作です。



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。

連続変換では、ファイル名は変更されません。暗号化したものは“**Encrypted**”サブフォルダに置かれます。これを検索して指定してから、連続して復号化すれば“**Decrypted**”のなかに復号化されたものが作成されます。もとのものをコピーしているのではありません。

非表示で、操作すれば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。

なお、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。著作権は放棄していませんので、ご注意ください。

参考：

安全保障貿易に係る機微技術管理ガイダンス  
(大学・研究機関用)

改訂版

平成22年2月

経済

Ⅱ－５．規制の許可例外について

貿易関係貿易外取引等に関する省令（平成10年通商産業省令第8号。以下「貿易外省令」という。）第9条において、安全保障貿易管理の観点から特に支障が無いと認められるため許可を必要としない技術提供が規定されています。代表的なものとしては以下のようなものがあります。

○ 公知の技術を提供する取引又は技術を公知とするために当該技術を提供する取引であって、以下のいずれかに該当するもの（第2項第9号）

- － 新聞、書籍、雑誌、カタログ、電気通信ネットワーク上のファイルなどにより、既に不特定多数の者に対して公開されている技術を提供する取引
- － 学会誌、公開特許情報、公開シンポジウムの議事録など不特定多数の者が入手可能な技術を提供する取引
- － 工場の見学コース、講演会、展示会などにおいて不特定多数の者が入手又は聴講可能な技術を提供する取引
- － ソースコードが公開されているプログラムを提供する取引
- － 学会発表用の原稿又は展示会などでの配布資料の送付、雑誌への投稿など、当該技術を不特定多数の者が入手又は閲覧可能とすることを目的とする取引

著作権、特許権を放棄してはいませんのでご注意ください。貿易管理令にあわせるために公開しているだけです。メールソフト“メールもビットマ”、“Cipher Web Mail”では、AES (Rijndael) ,Twofish なども利用できます。これらの暗号による多重暗号化が可能です。

本格的な暗号通信、暗号メールにはこちらをご利用ください。単なる暗号化ツールとしても5段階の暗号化が可能であり、USB メモリーに鍵を保存し、その USB メモリーが刺さっていないと復号化出来ないようにも設定できます。

\* 詳しくはホームページをご覧ください。

特許：

暗号通信の方式に関してはヨーロッパ、アメリカで特許を取得しました。