

暗号通信(Protected Communication System) Ver.2.1.0

特許権、著作権：宇山 靖政

ソフトウェアの名称：暗号通信(Protected Communication System)

1. ソフトの概要

暗号メールの送受信をするソフトです。クラウド暗号化ツールとしても利用できます。

暗号方式と鍵を自分で設定できます。Neko, AES, Camellia, Misty, Twofish, Serpent, Mars, Bitoma による 2 段階の多重暗号化、RSA 暗号、楕円曲線暗号による対称鍵の交換ができます。貿易管理令の例外適用を受けるために、ソースファイルをホームページで公開し、公知の技術とします。ソースファイルは公開しますが、特許権と著作権は宇山靖政が所有します。

* SMTP で 25 番ポート、SMTP-AUTH で 587 番ポートへの接続ができます。

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/> (ソースファイル)

3. 取り扱い種別(シェアウェア)

金額 (税抜き)：500 円 (本体価格 500 円+税+ベクターの手数料 となります。)

送金方法：ベクターレジサービス

試用制限：試用期間中は、復号化ソフトと復号化鍵は自由に設定できます。

暗号化ソフトと暗号化鍵は Bmp56EC.exe と “1234567” です。

試用期間中では、復号化を Bmp56DC.exe、鍵を “1234567” に

しておかないと、試用版から送信されたものを復号化出来ません。

試用期限：期限無し。

試用制限を解除するには、送金後にベクターから送られてくるライセンスキー、

“userkey.dat” で、ATMailSys の中のものを上書きする。

購入したライセンスキーは、同時に 1 台のマシンにおいてのみ使用を許可します。複数台のマシンにおいて本ソフトウェアのライセンスキーを登録する場合は、マシンの台数分のライセンスキーを購入してください。

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

6. インストール・アンインストール方法

インストール：ATMailPac.zip を解凍すると、このマニュアルの他に、

ATMailSys.zip (暗号メールソフトと関連するフォルダ、ファイル)

暗号ソフト.zip (暗号化ソフトと復号化ソフト)

鍵の見本.zip (暗号化鍵と復号化鍵の見本)

鍵作成ソフト.zip (暗号化鍵と復号化鍵を作成するソフト)

が現れます。さらに、ATMailSys.zip を解凍すると、“ATMailSys” 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 “ATMailJ.exe” へのショートカットを作成してください。

起動後に、SMTP、POP3 の設定をします。

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。

7. 最初の、“動かしてみよう！” を読めば動かせます。にやん語メールもできます。

暗号通信(Protected Communication System) Ver.2.1.0

目次

0.	動かしてみよう！	4
0.1	解凍	4
0.2	SMTP-AUTH、SMTP、POP3 の設定	11
0.3	アドレス帳の設定	14
0.4	暗号メール送信	15
0.5	暗号メールの受信	16
0.6	受信したメールの表示	17
0.7	にゃん語メールの送信と受信	19
	あなたの猫にメールを運んでもらうには？	19
	アドレス帳の設定と送受信（暗号通信でも可能です。）	24
	送信したデータの確認（“暗号通信”ではこの機能は利用できません。）	25
	スーパーにゃん語機能	27
0.8	暗号(クラウド)ツール	31
1.	保証および法的責任の放棄	35
1.1	ご利用は自己責任です。	35
1.2	日本国内でのみご利用ください。	35
2.	はじめに	37
2.1	目的	37
2.2	(Web)フリーメールの暗号化	38
2.3	他のメールソフトとの連携	42
2.4	UserKey.dat	43
2.5	暗号ソフト	44
2.6	鍵作成について	46
2.7	RSA 暗号を使った鍵交換の手順	55
2.8	楕円曲線暗号を使った対称鍵の交換	61
2.9	暗号ソフト、暗号鍵の変更について	64
2.10	暗号化鍵、復号化鍵の USB メモリーへの保管	65
3.	初期設定	67
3.1	解凍	67
3.2	初期設定する項目	67
4.	操作の詳細	70
4.1	メイン画面	70
4.1.1	ファイル	71
4.1.2	表示	71
4.1.3	設定	71
4.1.4	ヘルプ	71
4.2	アドレス帳	72
4.2.1	ファイル	77
4.2.2	編集	77
4.2.3	アドレス帳の圧縮	77
4.2.4	表示	77

4.2.5	メール	77
4.2.6	ウインドウ	77
4.2.7	ヘルプ	77
4.2.8	設定	77
4.3	メールボックス	78
4.3.1	ファイル	79
4.3.2	編集	79
4.3.3	お気に入り	79
4.3.4	Go	79
4.3.5	表示	79
4.3.6	メール	80
4.3.7	暗号(クラウド)ツール	81
4.3.8	ウィンドウ、ヘルプ、設定	91
4.4	ダミーテキスト編集	91
5	暗号ソフトのソースコード	92
5.1	Camellia 暗号ソースコード	92
5.2	AES 暗号ソースコード	92
5.3	Twofish 暗号ソースコード	92
5.4	RSA 暗号ソースコード	93
6	暗号ソフトを作成される方に	94
6.1	使用できる暗号の種類と特徴:	94
6.2	暗号ソフトの呼び出しコード	95
7.	特許について	95
8.	利用しているソフトについて	95
9.	バージョンアップについて	96

0. 動かしてみよう！

0.1 解凍

インストール：ATMailPac.zip を解凍すると、このマニュアルの他に、

ATMailSys.zip

暗号ソフト.zip

鍵の見本.zip

鍵作成ソフト.zip

が現れます。さらに、ATMailSys.zip を解凍すると、“ATMailSys” 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設定した”メール用”というフォルダを作り、その中に置いてください。

さらに、このフォルダをデスクトップ等の適当な場所に設定した”鍵交換用”というフォルダを作り、その中にも置いてください。

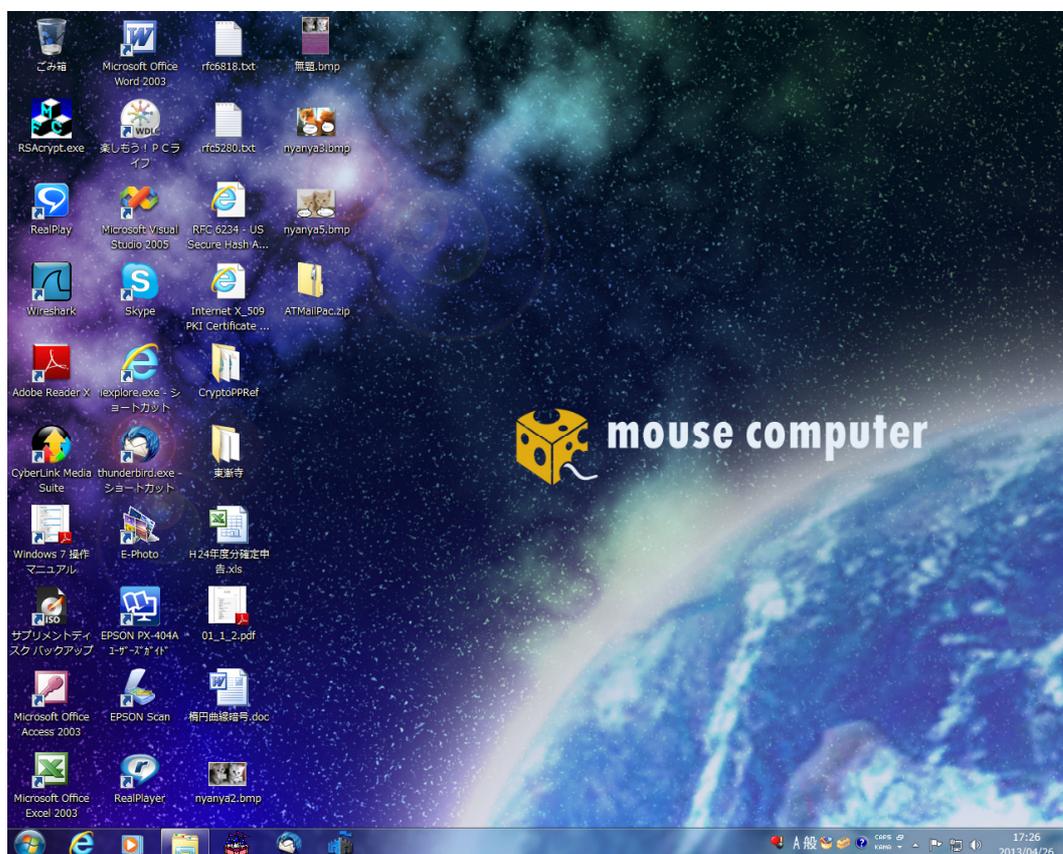
最初は、この”メール用”の中での作業です。

まず、”メール用”の中にある

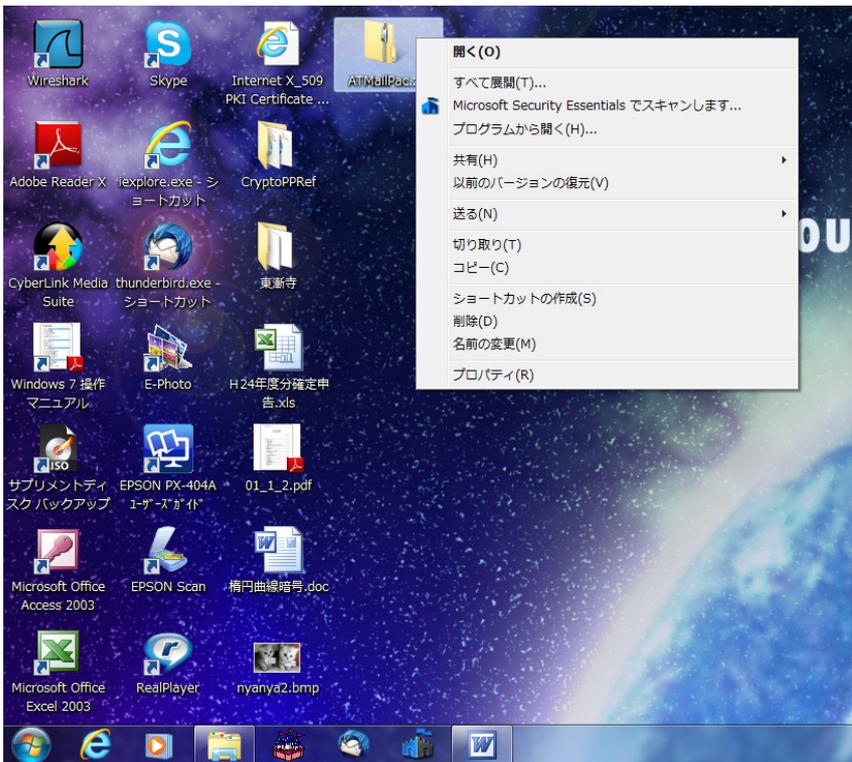
“ATMailJ.exe”へのショートカットを作成してください。

起動後に、SMTP-AUTH、SMTP、POP3 サーバーの設定をします。

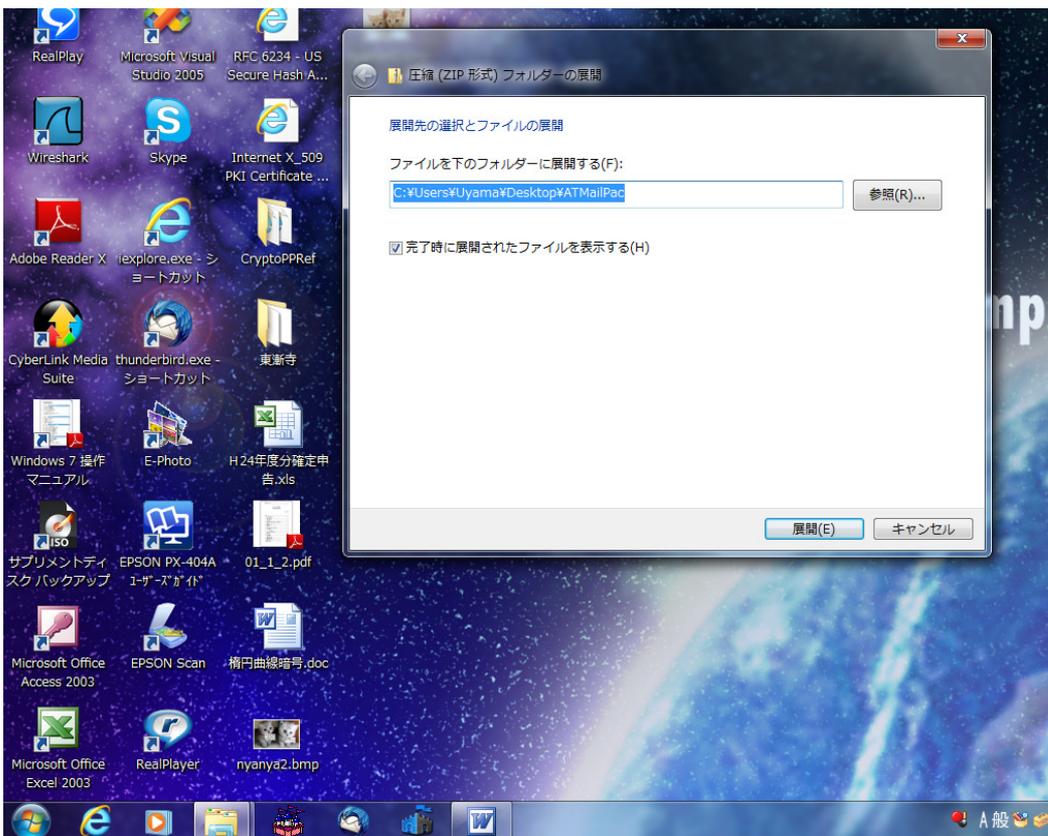
ATMailPac.zip をダウンロードしたら、デスクトップに貼り付けてください。
もちろん、適当なフォルダを作ってその中で作業していただければかまいません。



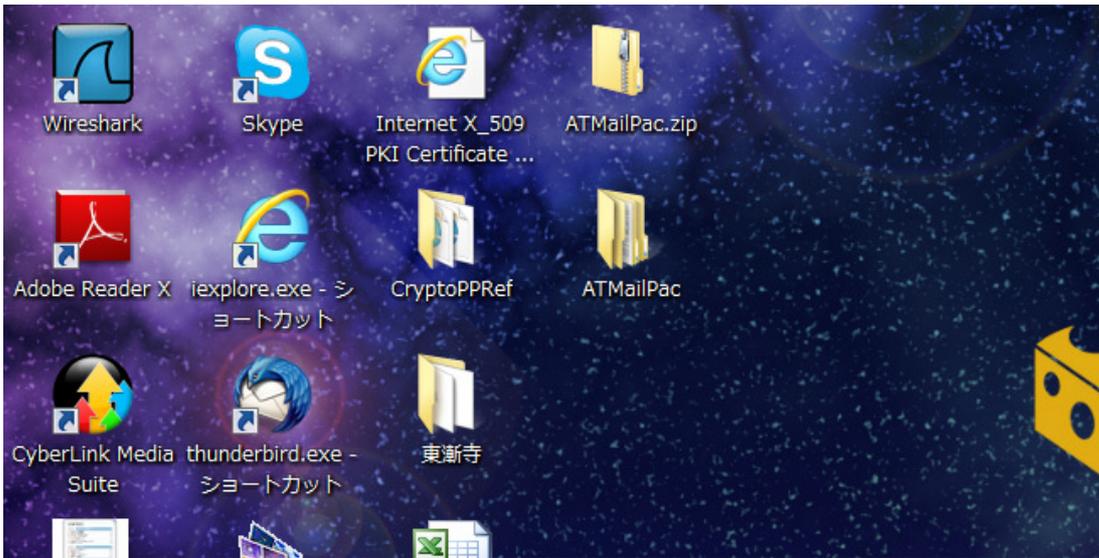
ATMailPac.zip を右クリックしてください。



すべて展開 (T) を左クリックして、

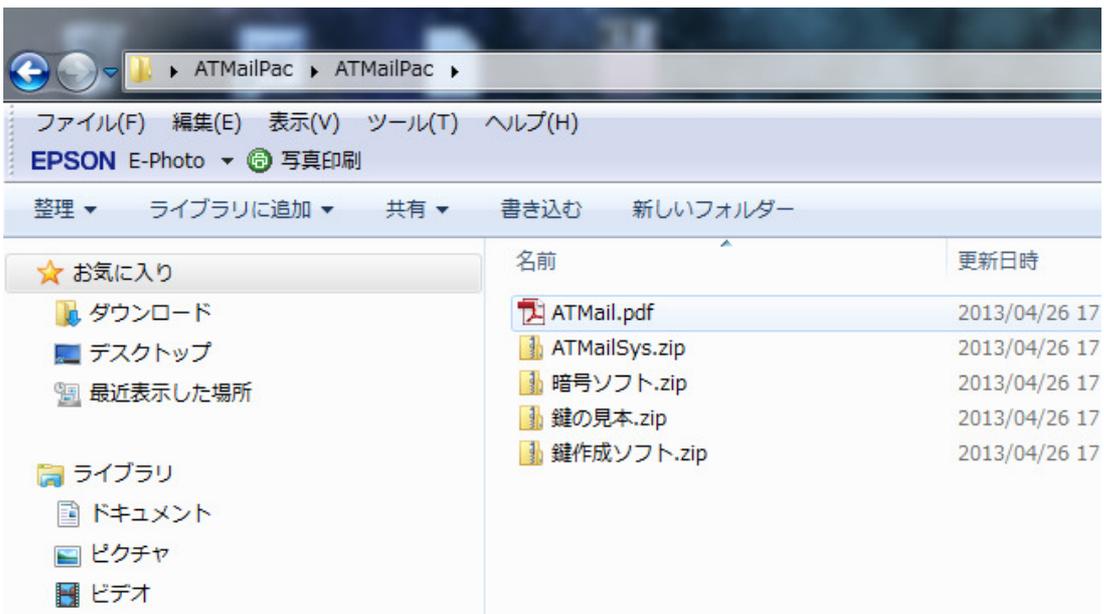


右下の展開を左クリックしてください。

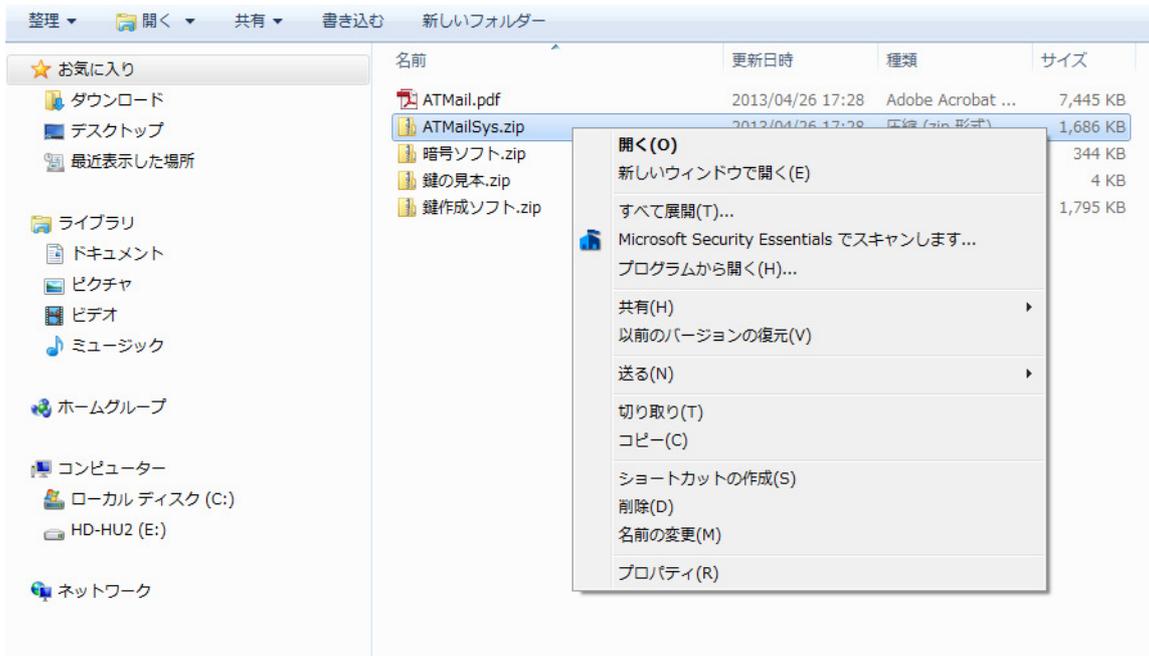


ATMailPac というフォルダが現れます。

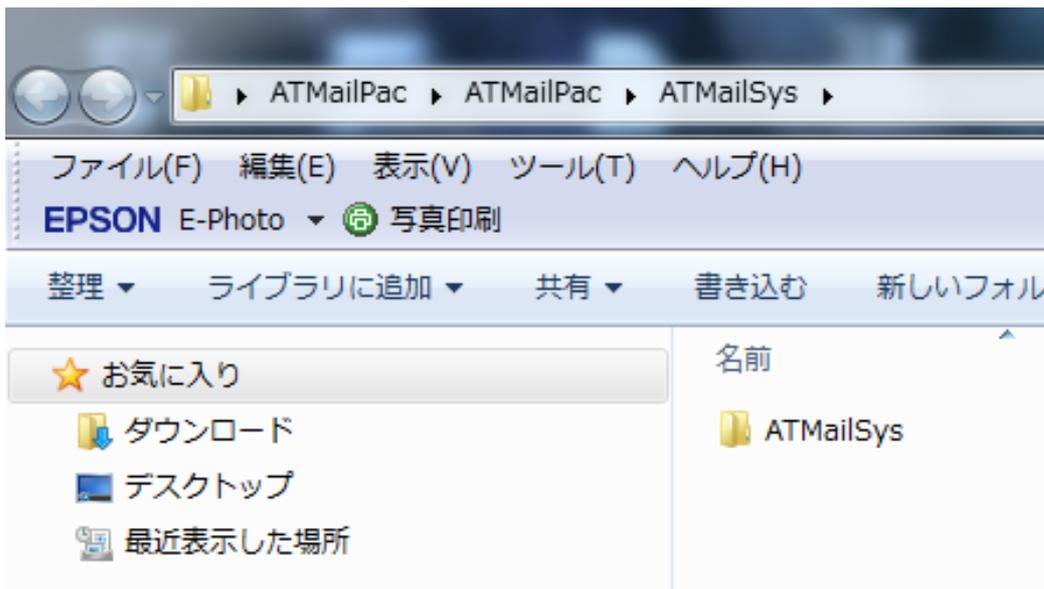
そこを、ダブルクリックすると、



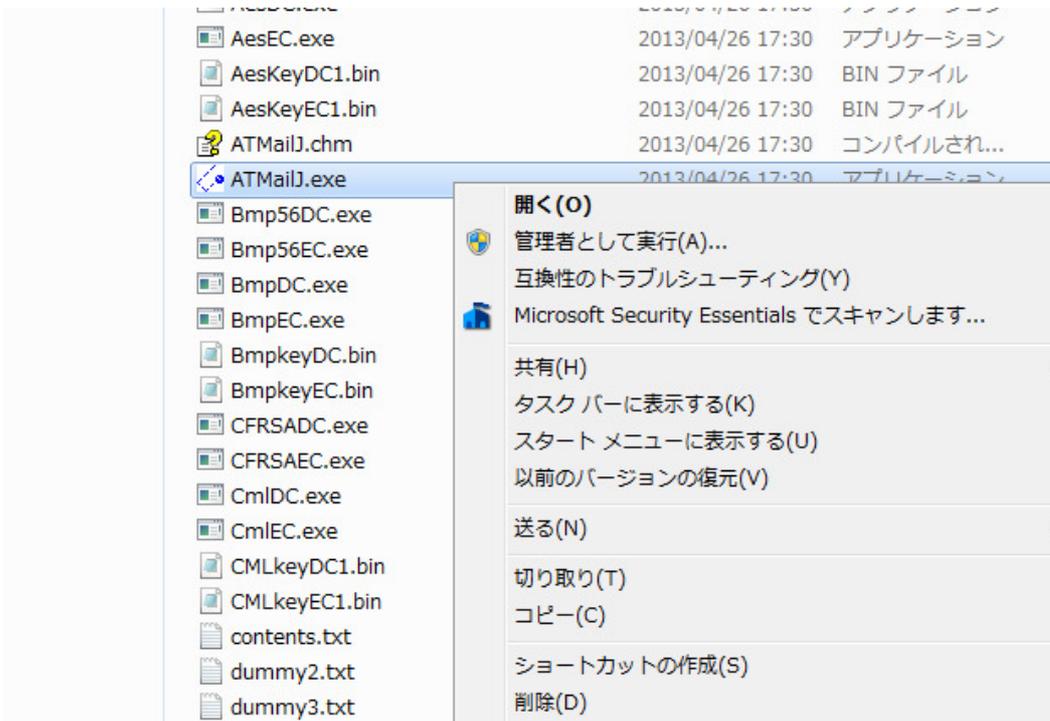
そのなかに、ATMailSys.zip が現れます。右クリックすると



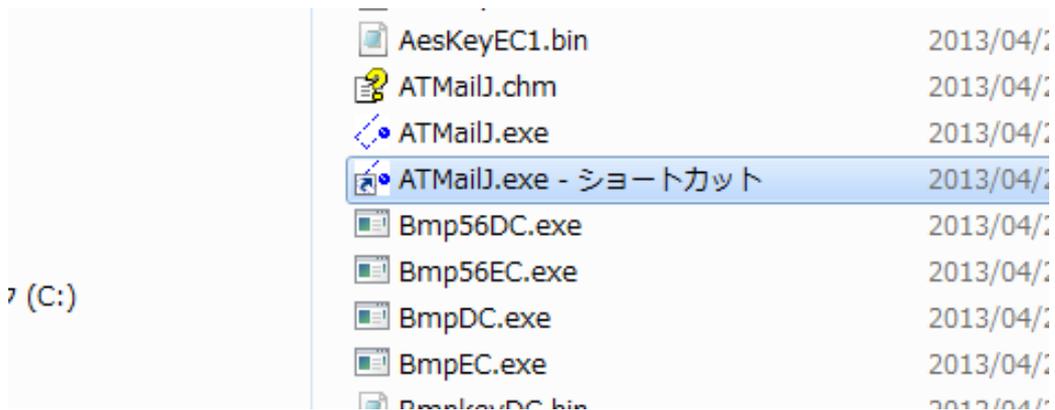
となりますので、さらに、すべて展開（T） とし、展開してください。



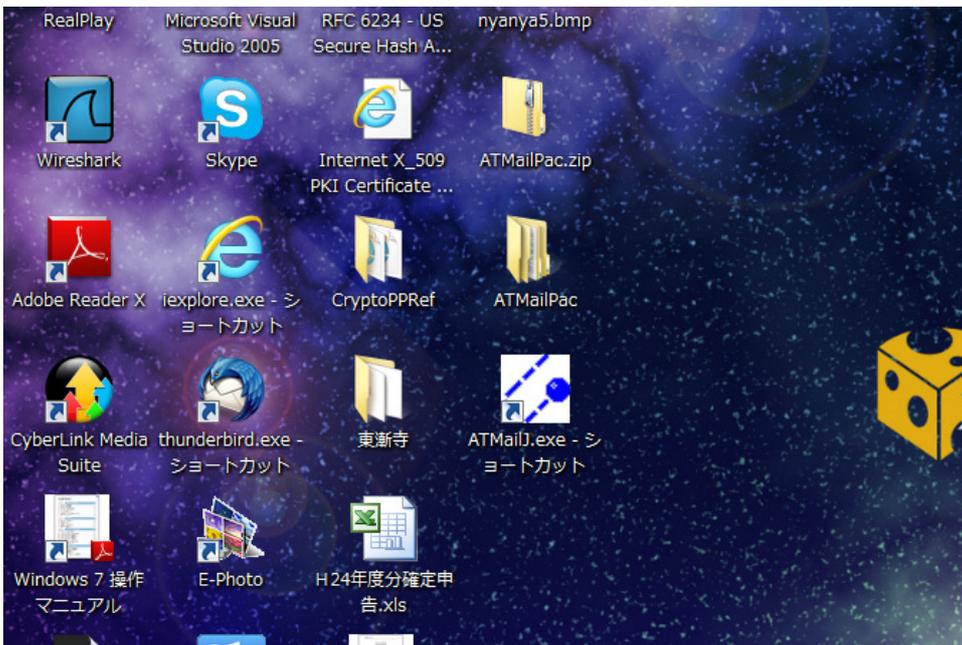
ATMailSys フォルダがあらわれます。この中の、



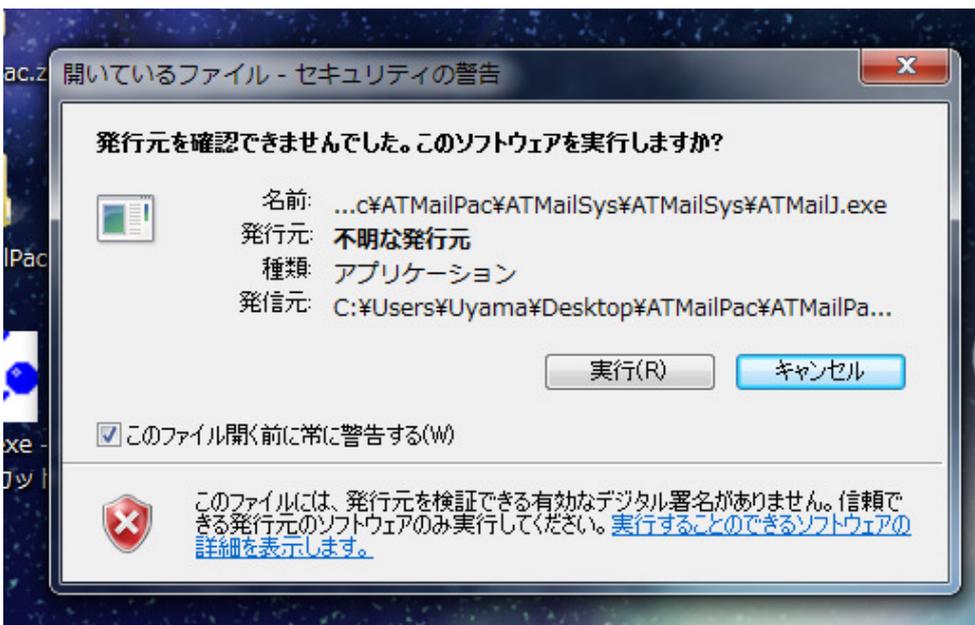
ATMailJ.exe を右クリックして、ショートカットの作成を選んでください。



出来上がったショートカットを、デスクトップにドラッグしてください。

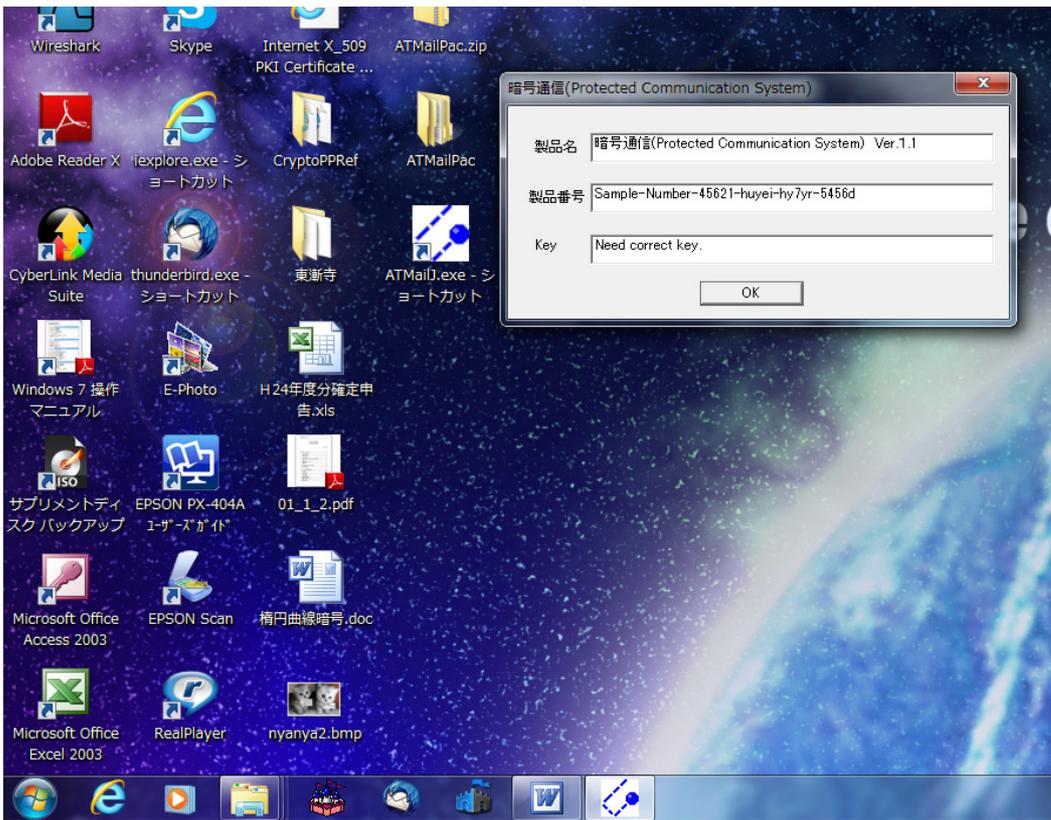


このショートカットをダブルクリックすると、

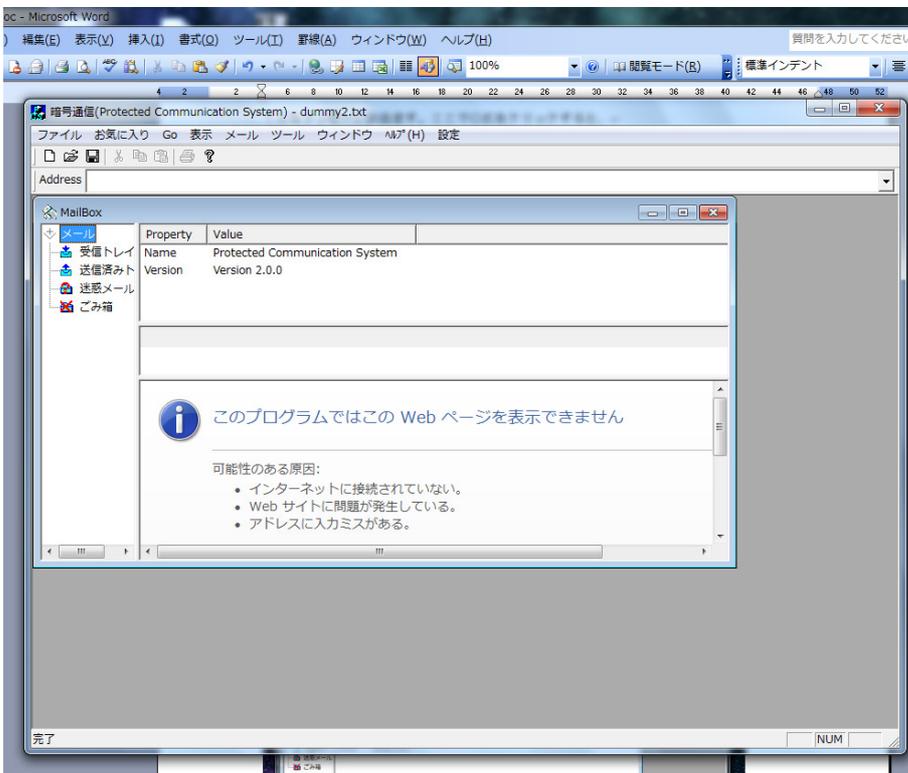


製作者が有名ではないので、警告がでます。でも、実行をクリックすると、

(左下の、このファイルを開く前に常に警告する (W) のチェックをはずしていただければ、次からはこの警告が出なくなります。)



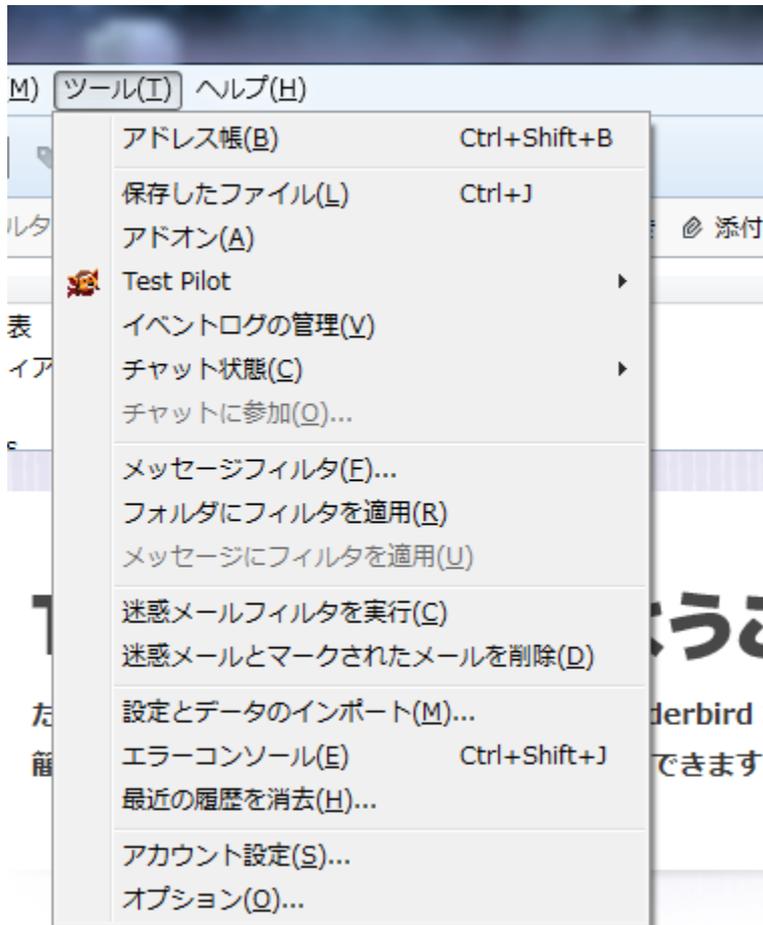
こんなメッセージが出ます。ここでOKをクリックすると、



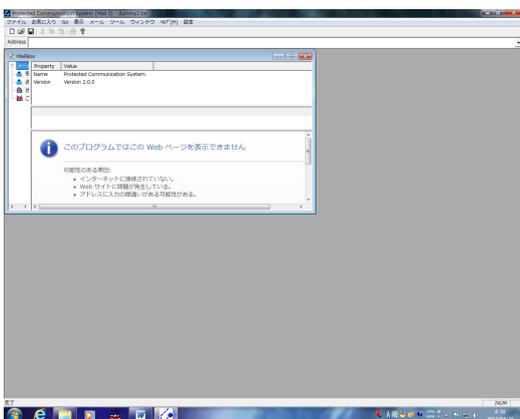
となって、ソフトが動き始めます。

0.2 SMTP-AUTH、SMTP、POP3 の設定

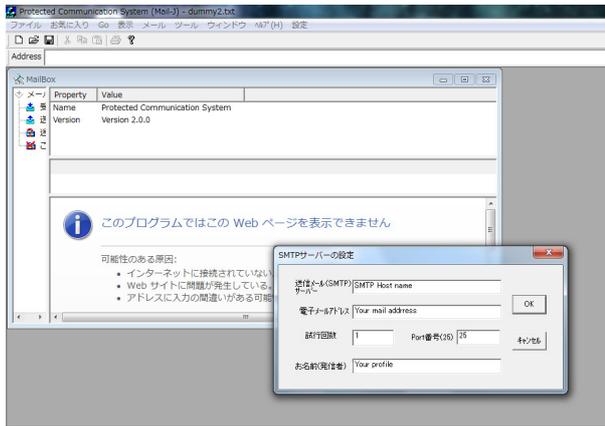
他のメールソフトの、アカウント設定を参考にすると楽に出来ます。下は、サンダーバードの場合です。ツールからアカウント設定を選んでその内容を見ながら設定してください。



起動すると、最初にユーザー確認のメッセージが出ます。OK をクリックします。すると次の画面が現れます。



右上の、設定から、SMTPHost 設定を選んでください。



ここで、

送信メールサーバー (SMTP) (SMTP-AUTH)
電子メールアドレス
試行回数
Port 番号
お名前 (発信者)

を設定しますが、試行回数はそのままです。

Port 番号は SMTP では 25、SMTP-AUTH では 587 です。

SMTP-AUTH の場合

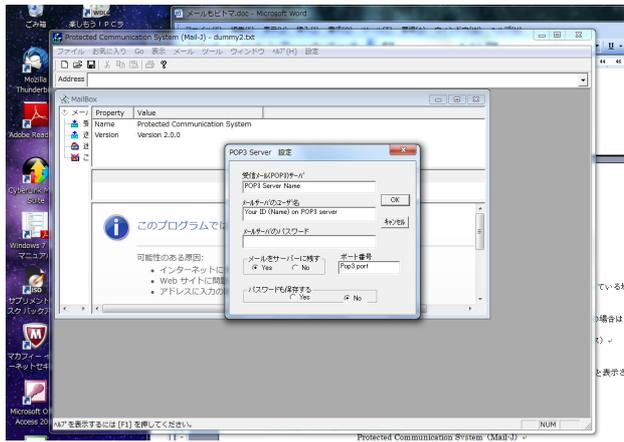
Port 番号が、“587”で、送信メールサーバーのところを、“smtp-auth.xyz.ne.jp”として下さい。
(サーバー名はプロバイダーによって異なります。プロバイダーの設定マニュアルを参照してください。)
電子メールアドレスの所を abcd@efg.xyz.ne.jp (あなたのメールアドレス)
として下さい。

SMTP の場合

あなたの利用しているプロバイダーが”xyz.ne.jp”で、メールアドレスが “abcd@efg.xyz.ne.jp” の場合は、
送信メールサーバー (SMTP) の所を efg.xyz.ne.jp (@の右側)
電子メールアドレスの所を abcd@efg.xyz.ne.jp (あなたのメールアドレス)
とすれば、Port 番号を 25 として接続できます。

お名前 (発信者) に 山田太郎 と入れると、受信者のメーラーに、差出人として 山田太郎 と表示されます。

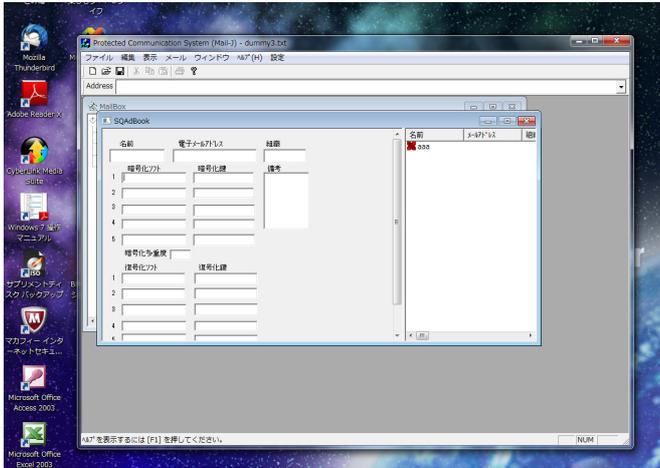
さらに、POP3 サーバーの設定です。



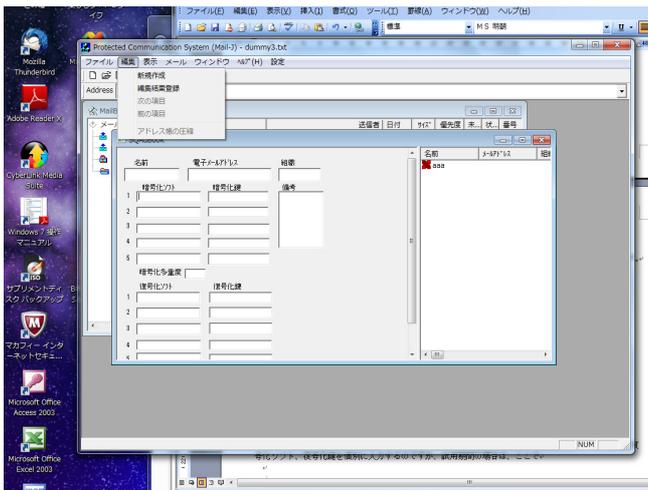
受信メール(POP3)サーバー：efg.xyz.ne.jp (@の右側)
メールサーバーのユーザー名：abcd (@の左側)
メールサーバーのパスワード：これは、プロバイダーからの書類にあるものです。
ポート番号：110
としてください。
メールはサーバーに残す設定にして、普段のメールソフトで処理してください。
パスワードも保存してください。

0.3 アドレス帳の設定

メニューの左端の、ファイルをクリックしてから、SQアドレス帳を選ぶと次のような画面になります。



右の、aaa の行をクリックすると、左側の項目にデータが反映されます。左側で、メールの送信相手の名前、メールアドレスを入力します。本来は、暗号化ソフト、暗号化鍵、復号化ソフト、復号化鍵を個別に入力するのですが、試用期間の場合は、ここで



メニューの2つ目の編集から、編集結果登録をクリックしてもらえば、暗号化の部分は入力されます。

つぎに、編集から、新規作成を選ぶと、右側に、名前の欄にマークのついている空の行ができます。その行をクリックしてから、新しい送信先の、名前、メールアドレスを入力して、編集から編集結果登録とすれば右側に編集結果が現れます。

ついでに、自分のアドレスや、自分のフリーメールアドレスも登録してください。この右側の内容が、アドレスブックに登録されている内容を表示します。

試用期間中は、暗号化ソフト(Bmp56EC.exe)、復号化ソフト(Bmp56DC.exe)の組み合わせで暗号化と復号化が体験できます。この場合は暗号化、復号化の鍵は 1234567 から変更はできません。

ただし、復号化だけは自由に設定できます。制限が解除されれば、全ての項目が自由に設定できるようになります。

伊藤さんから山田さんに暗号化したメールを送るには、伊藤さんのアドレス帳で

氏名 山田
電子メールアドレス yamada@yahoo.jp
暗号化ソフト Bmp56EC.exe
暗号化鍵 1234567
とします。

山田さんから伊藤さん宛てに暗号化されて送られてきたものを伊藤さんが受け取るには伊藤さんのアドレス帳で、山田さんのところに

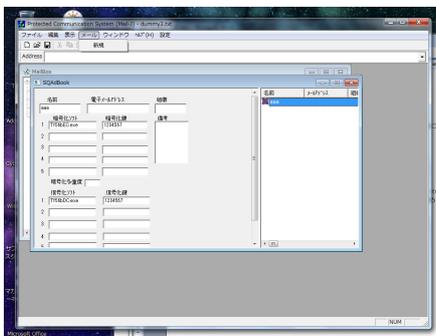
復号化ソフト Bmp56DC.exe
復号化鍵 1234567
とします。(試用期間中は自動的に入力されます。)

さらに、山田さんのアドレス帳では
氏名 伊藤
電子メールアドレス itou@goo.jp
暗号化ソフト Bmp56EC.exe
暗号化鍵 1234567
復号化ソフト Bmp56DC.exe
復号化鍵 1234567
のように設定します。

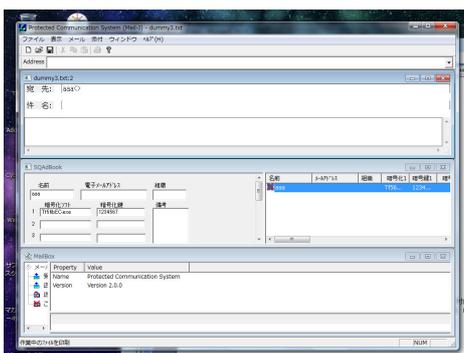
これで暗号通信ができます。最初は自分宛に、そして自分のフリーメールアドレス宛に送ってみましょう。

0.4 暗号メール送信

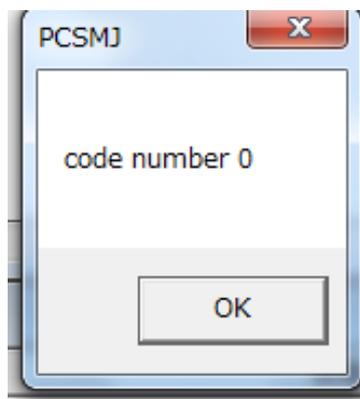
アドレス帳の右側で、メールを送る相手をクリックします。



つぎに、メニューのメールをクリックして新規をクリックすると、



宛先が入力済みの、メール用のエディタが一番上に現れます。
件名の入力と、その下の部分に本文を入力します。その後、メニューのメールから送信を選んでクリックしその後 OK をクリックすればメールが暗号化されて送信されます。



送信成功の場合は、コード 0 となります。OK をクリックすれば送信完了です。

ただし、本文の内容は暗号化されますが、件名は暗号化されません。
添付ファイルの内容は暗号化されますが、そのファイル名は暗号化されません。
暗号化されたときのデータ形式は、暗号化の最後に **Bmp56EC.exe** を使ったときはビットマップ形式になっています。

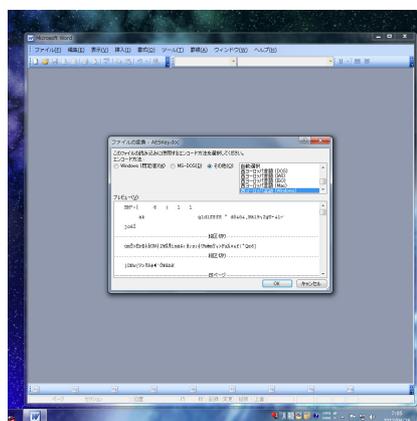
0.5 暗号メールの受信

メールボックスだけ残して他は閉じます。メニューで メール から 取り込み とすれば、メールが取り込めます。取り込みの後で、メールボックスの左の 受信箱 をクリックしてから、右の受信メールの行をクリックしてください。下に復号化された本文、またはダミーテキストが表示されます。

設定で、ダミー表示の所を切り替えると本文が復号化されて表示されるか、ダミーテキストが表示されるかの切り替えができます。

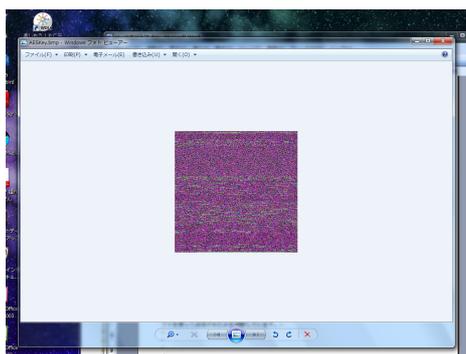
復号化ソフト復号化鍵が送信者の暗号化に対応してきちんと設定されていなくてはなりません。

ご自分のフリーメールアドレス宛に送信して、その結果もご確認ください。
添付ファイル(test.doc)を付けて、送信した場合は同じ名前のファイルが送られてきますが、そのファイルを保存して、ワードで開こうとすると、下の図のようになり、



開いてもうまく表示できません。

このファイルの拡張子を、bmp にかえて、test.bmp を開くと



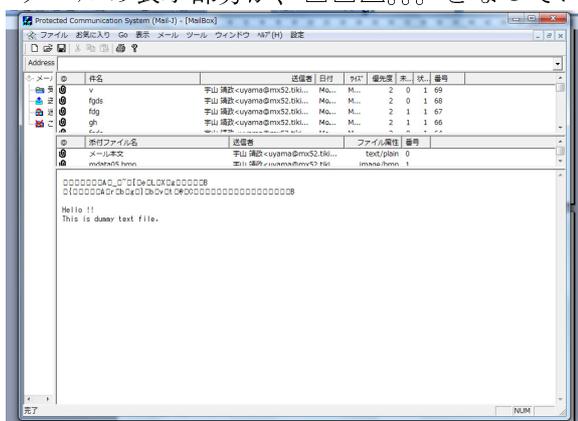
となって、データ形式がビットマップ形式になっていることが分かります。

拡張子を doc に戻してから、ツールの機能を使えば本来のワード文書にもどります。

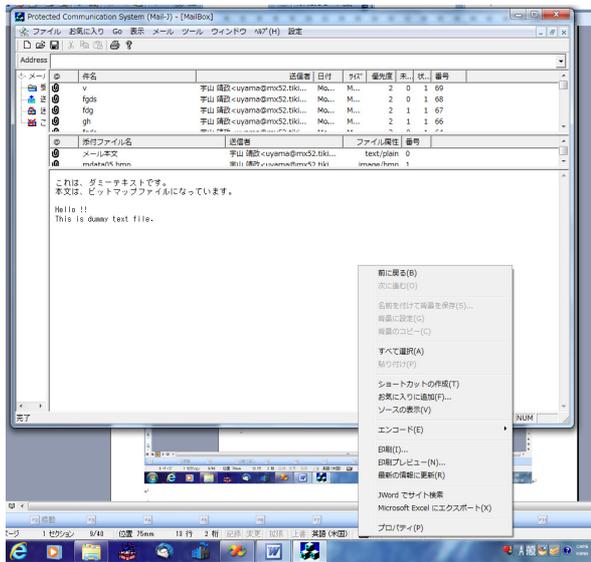
同じメールアドレスから送信されたものでも、このメーラーを使った場合は自動的に復号化されますが、別のメールソフトから送信されたものは復号化されないで普通に表示されます。内部で、どんなメールソフトを使って送信されたかを判断しています。

0.6 受信したメールの表示

メールの表示部分が、□□△。。となっているときは、表示部分を右クリックして、



エンコード — 日本語（自動選択）として下さい。（または、日本語（シフト JIS）として下さい。）



以上、お試しください。

0.7 にゃん語メールの送信と受信

あなたの猫にメールを運んでもらうには？

世界初の猫語理論による、日本語から猫語への変換と猫語を記録したファイルを猫の写真と共に送信するソフトです。(??????)

すでに、猫の画像は入っていますので、ヤフーメールなどに送信すると、



のような画像の添付ファイルとなって届きます。

にゃん語でのメールを多く使うときは、ダミーテキストを次のように変えると、良いと思います。

読めなかったら、
近くにいる猫に翻訳してもらってください。
猫がいなかったら、
にゃん語通信(Protected Communication System)
を使ってください。

いかがでしょうか？

紫色の部分が、あなたのメールが猫語に翻訳されたものです。
メールの本文が短いと、紫色の部分は1列か2列の点線のようになります。

受信される方が、猫語を日本語に戻す場合は、ソフトの機能は無料で利用できます。
無料で、ベクターからダウンロードして使えます。

もちろん、

世界で一番賢くて、世界で一番かわいいのはあなたの飼っている猫です。

その猫に、メールを運んでもらうには次の作業が必要です。

猫の写真を、横幅が 256 ピクセルくらいで、縦幅が 166 ピクセルくらいの大きさで、1 ピクセルの情報が 24 ビットのデータで決定されるビットマップファイルに変換します。

難しそうですが、やってみれば簡単です。次の手順で作業を進めてください。

1. 写真をパソコンに取り込む。
デジカメで写真を撮ってください。
USBケーブルでパソコンとつないで、写真をデスクトップに置いてください。
写真を右クリックして下さい。



ここで、プログラムから開く(H)を左クリックして下さい。

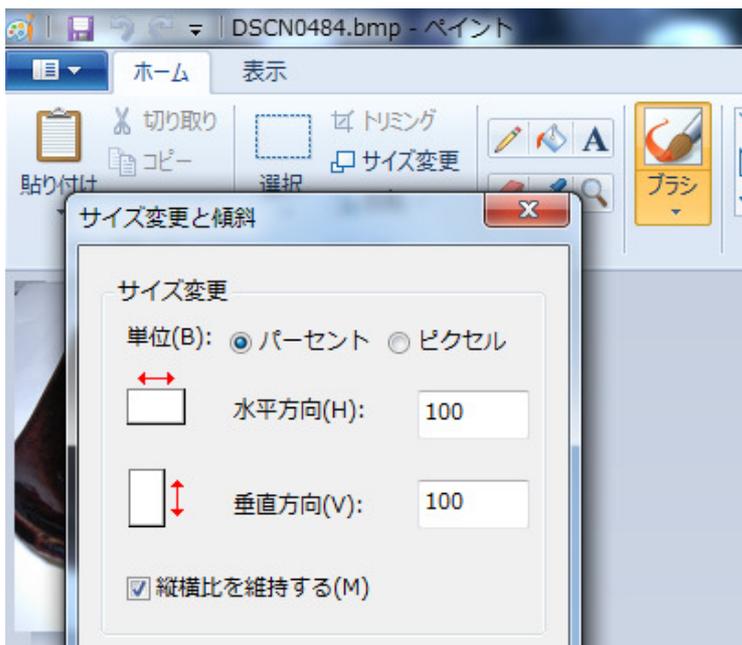


さらに、ペイントの所を左クリックしてください。

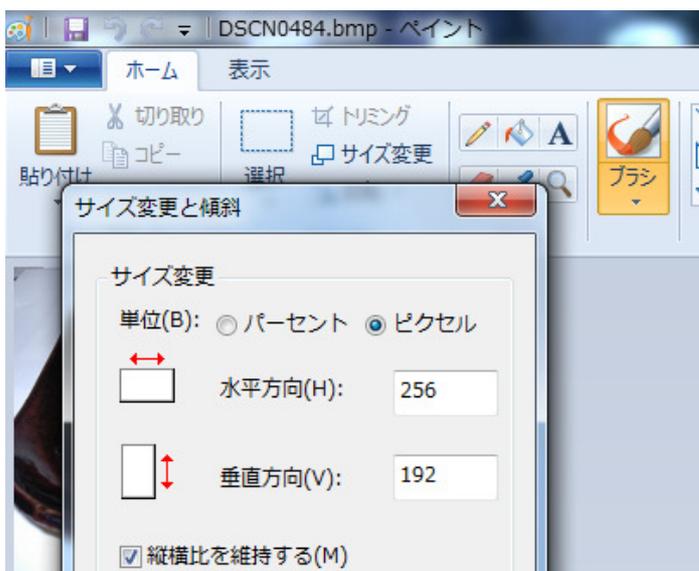
2. ペイントで修正し、保存する。
 ペイントのツールを使って、必要な吹き出しを作ってください。
 (Aのところや、□の所を適当に使う。)



吹き出しの作成後、サイズ変更をクリックします。



上の図は、Windows7 のものです。この場合は、右のピクセルの部分をクリックして、水平方向のところを、256 としてください。



他のバージョンでは、変形のサイズ変更を選択し、サイズ変更で、水平方向、垂直方向の所の値を 50 とか 30 にして、縮小します。横幅の見た目が 5～6 センチ程度になるように調整してください。大きすぎなければ適当でかまいません。

次の作業は最も大切です。正確に行ってください。

適当に縮小したら、ファイルに名前を付けて保存します。



ファイルの種類を、

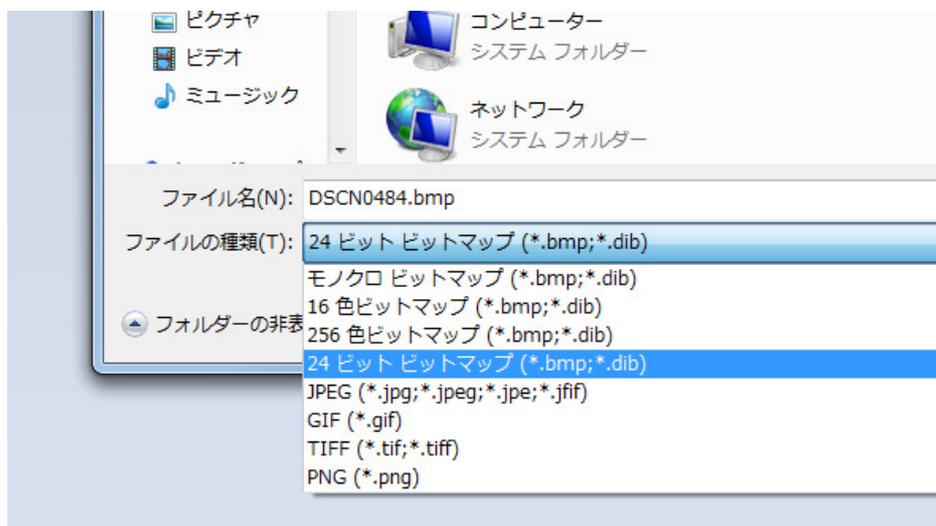
24 ビット ビットマップ (*.bmp;*.dib)

にしてください。

ファイル名は、必ず

nyanya2.bmp

にしなくてはなりません。(犬が好きな人もこの名前をお願いします。ごめんなさい。)



nyanya2.bmp

のデータサイズは、100KB から 300KB 程度にしてください。

(画像を右クリックしてプロパティを見て確認してください、)

3. データを、指定されてフォルダに置く。

フォルダー、ATMailSys のなかには、すでに、nyanya2.bmp
が入っていますので、あなたの画像で上書きしてください。

アドレス帳の設定と送受信（暗号通信でも可能です。）

暗号化ソフト		暗号化鍵	
1	nekoEC.exe	bmpkeyec.bin	
2			
3			
4			
5			
復号化ソフト		復号化鍵	
1	nekodc.exe	bmpkeydc.bin	

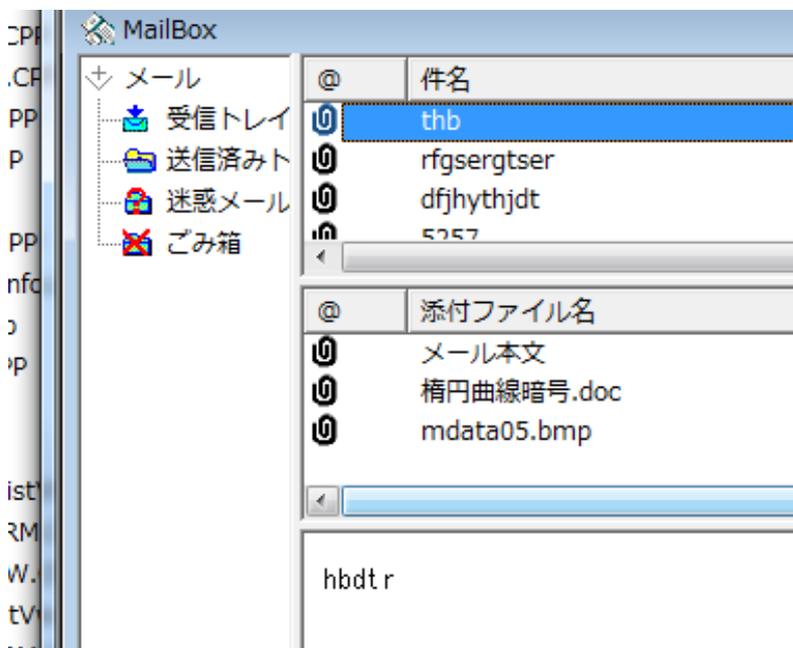
暗号化ソフトの場所に、nekoEC.exe 暗号化鍵のところは、bmpkeyec.bin
復号化ソフトの場所に、nekoDC.exe 暗号化鍵のところは、bmpkeydc.bin

とします。

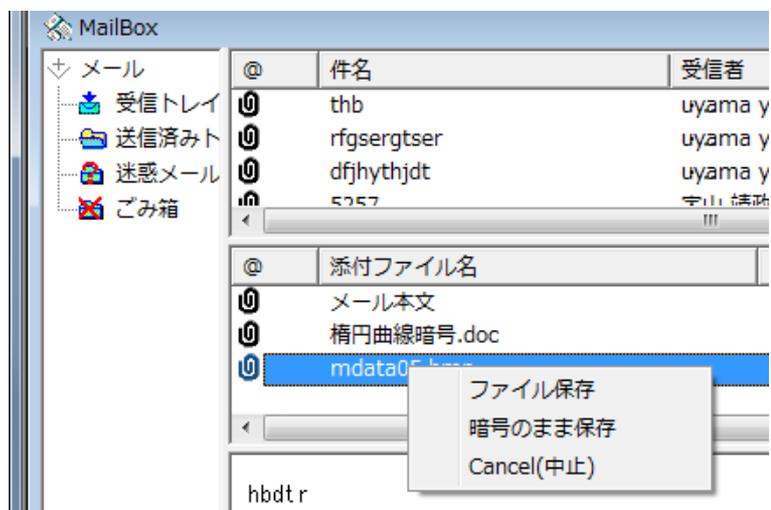
機能制限が解除されている期間や、あなたがベクターから正規ユーザーのキーファイルを購入
していればこのような設定ができます。

送信したデータの確認（“暗号通信”ではこの機能は利用できません。）

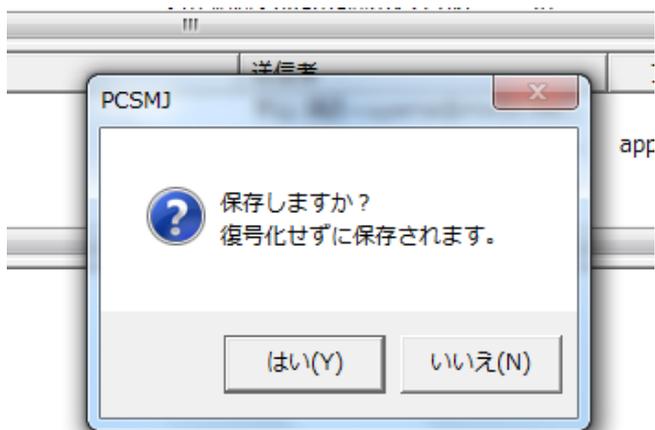
とりあえず、自分の名前と、自分のフリーメールアドレスを記入してから編集結果を保存してください。そして、自分のフリーメールに向けてメールを送信してみてください。
あなたの猫が、猫語で書かれたメールを届けていることでしょう。
普通は、送信したデータの内容は、送信済みトレイをクリックすると、あなたが記入した最初の日本語の形で表示されます。



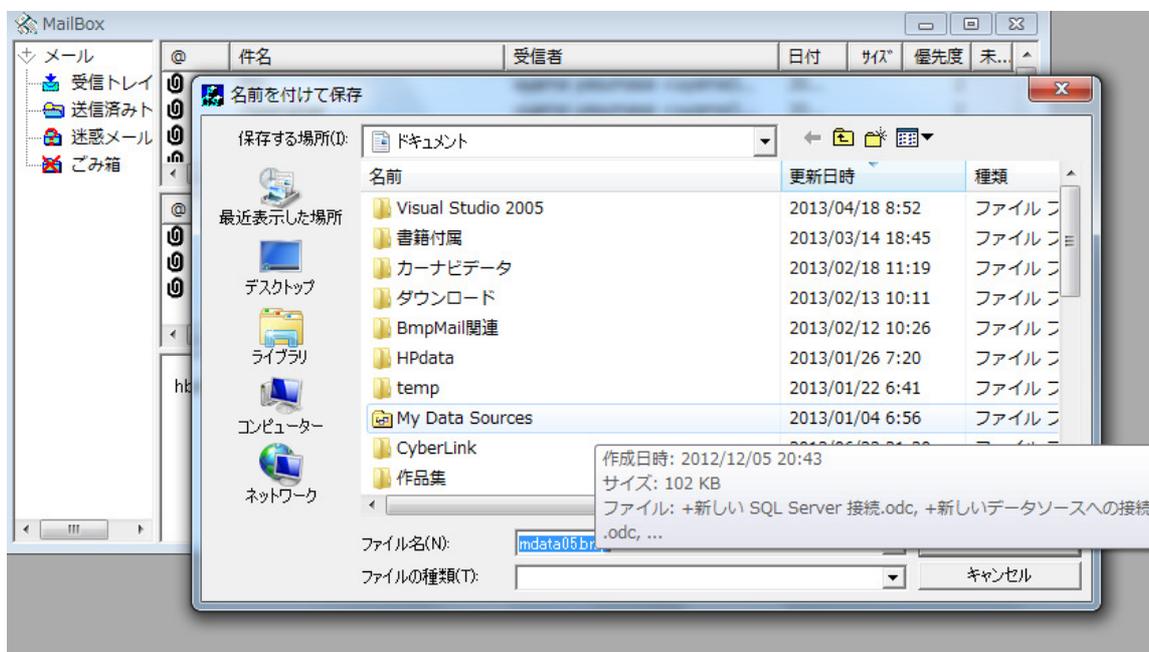
あいてに、どんな形で届いているかを確認するには、



添付ファイル名 の **mdata05.bmp** の部分を右クリックしてください。
暗号のまま保存
を選択すると、次のようになりますので、



となりますので、デスクトップにでも保存してください。
相手に送信されてもものと同じ画像が保存されます。



その画像をダブルクリックすれば、大きく表示されます。

この機能は、“にゃん語通信”と“メールもビトマ”に追加された機能です。“暗号通信”にはありません。

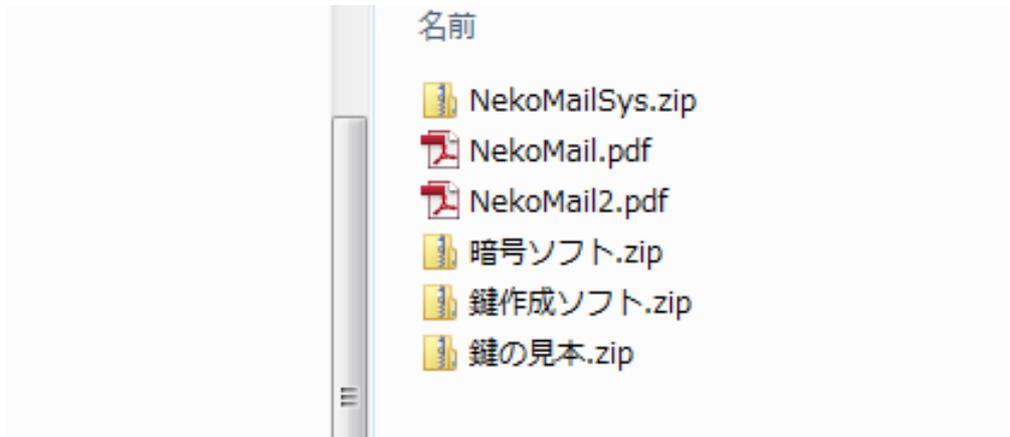
賢くてかわいい、あなたの猫がメールを猫語で伝えてくれます。楽しいメールにしてください。

将来は、泣き声に変換して伝えるように改良したいと思っています。

スーパーにゃん語機能

もし、あなたの猫が猫王国の機密事項を運ぶときには、次のようにしてスーパーにゃん語機能を利用してください。

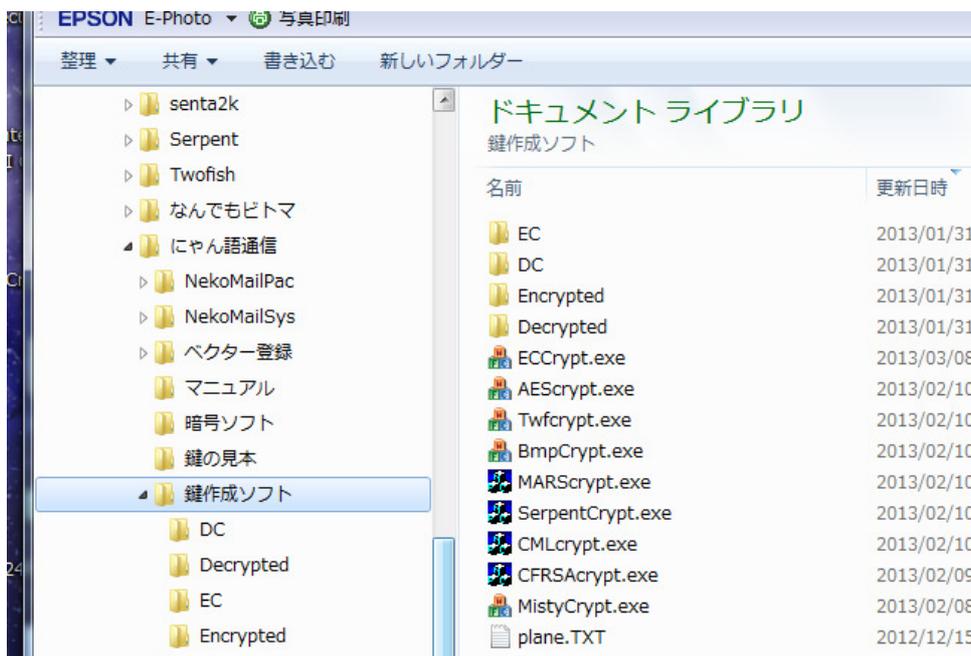
鍵作成ソフト.zip を開くと、



鍵作成ソフトのフォルダの中に、暗号鍵を作成するソフトが現れます。

ここでは、AESCrypt.exe と CMLcrypt.exe を使いましょう。

CMLcrypt.exe は日本で開発されたカメラ暗号の鍵を作るソフトです。



CMLcrypt.exe をダブルクリックすると、

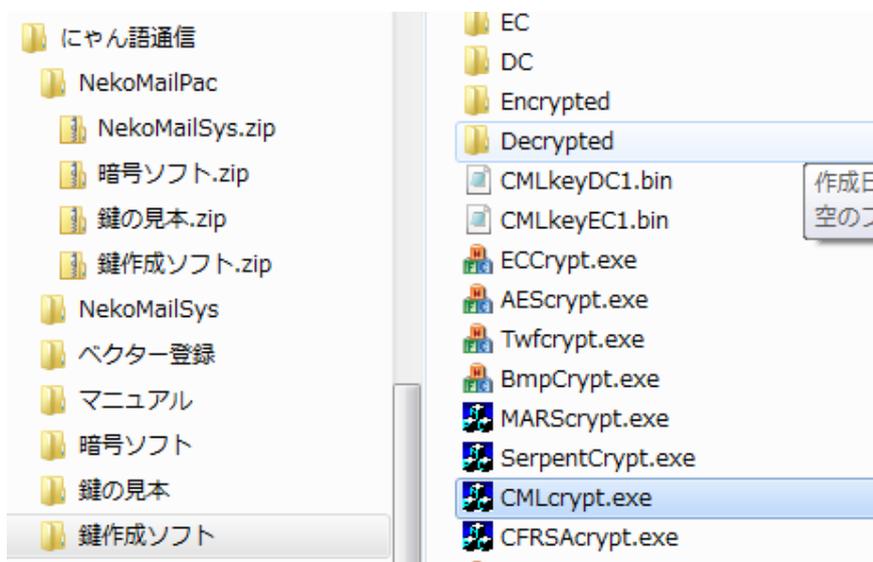


鍵の長さは、**256bit**、の所をクリックして、次に暗号化鍵名、復号化鍵名を決めます。分かりやすい名前であまり長すぎないようにしてください。

鍵を生成、をクリックすると鍵が作成されます。

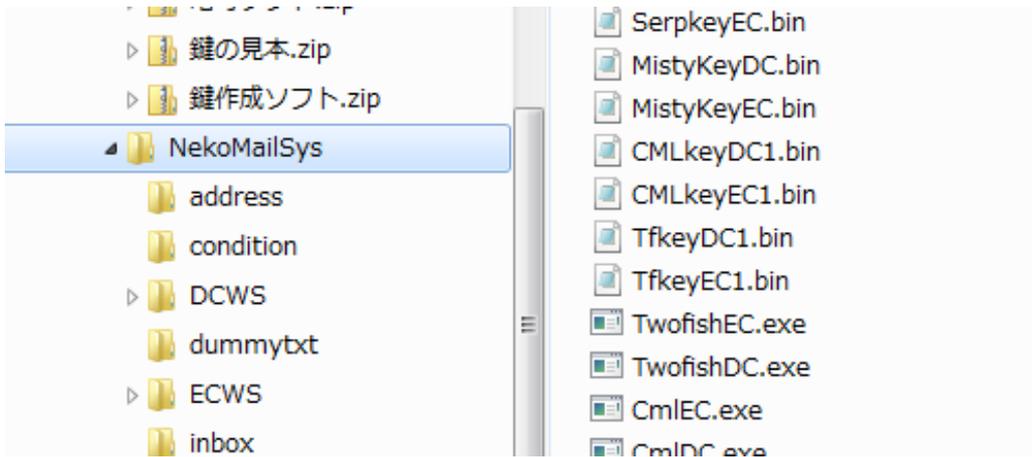
保存終了、をクリックすると、

暗号化鍵のファイル **CMLkeyEC1.bin** と復号化鍵のファイル **CMLkeyDC1.bin** ができます。



本来は、これを **NekoMailSys** フォルダのなかに移動するか、USBメモリーに保存して使うのですが、その場合は、通信相手との鍵交換が必要となります。鍵交換は直接あって交換するか、公開鍵暗号を利用して交換することになります。

今回は、すでに入っているものとそのまま使うことにしますので、せっかく作った鍵ですが削除してください。



つぎに、AESCrypt.exe をダブルクリックすると、次の画面が現れます。

ブロックサイズの種類や鍵の長さの種類が普通のAESよりも多くなっています。これはコンテストに参加したときのままのソースコードを使っているからです。Rijndael (ラインダール) のソースコードは、

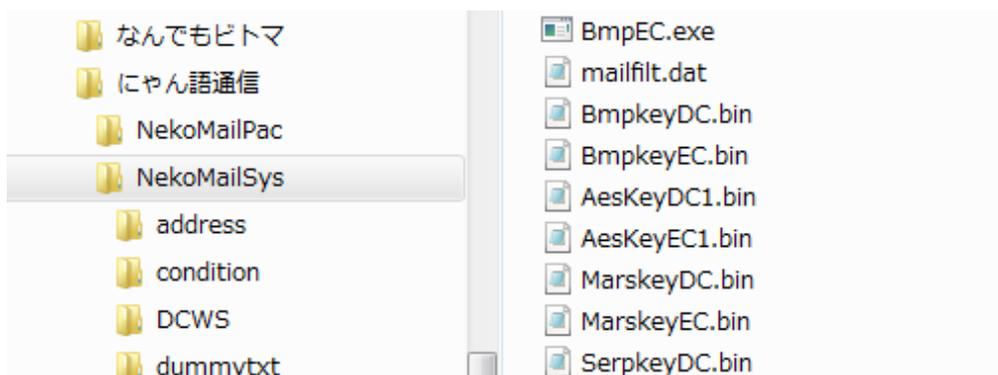
**The Design of Rijndael: AES - The Advanced Encryption Standard
(Information Security and Cryptography)**

に載っていますが、数箇所の誤りがあり修正しました。この修正に関しては著者からその修正が必要であることの確認をとってあります。

可能ならば、ブロックサイズをカメラの 256bit と変えて、224 か 192bit にして下さい。
この場合は、解読のために扱うブロックのサイズが最小公倍数の 1792bit になります。



でも、すでに存在する、



AesKeyEC1.bin と AeaKetDC1.bin を使うことにしましょう。

アドレス帳の設定は、次のようになります。



アルファベットは全て小文字にしてもかまいません。

このように設定してから、送信すればカメラ暗号とAES暗号で2段階に暗号化されたデータがさらに、にゃん語に変換されて相手に届くことになります。

これを、スーパーにゃん語機能とよびます。

0.8 暗号(クラウド)ツール

クラウドに関しては、次のような心配があります。

1. 従業員によるデータの盗み見
2. 業務上のルーチンワーク内での閲覧
3. 政府機関による監視・閲覧
4. ID とパスワードを盗まれて、ほかの PC から覗き見される。

これらの心配を完全とは言えませんが、1,2についてはかなりの程度防御できると考えています。標準とされる暗号方式での多重暗号化を提供します。たとえ、AES が総当たり攻撃で1秒で解けたとしても、AES、カメラ、RSA などでも3段階の多重暗号化をすれば、総当たり攻撃には耐えられると思います。

クラウドでのデータ保存機能を利用されている方に、強力な暗号機能を提供します。このメールソフトは、送信者と受信者の順序対ごとに暗号化方式、暗号化鍵、多重度を設定できます。これをクラウドでのデータに適用すれば、次のことが可能となります。

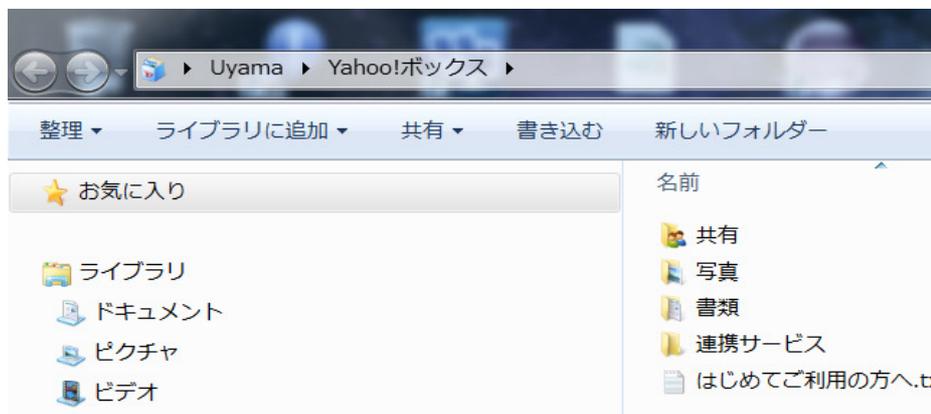
1. 自分用に保存するデータを強力に多重暗号化できます。
2. 特定のグループの構成員だけが閲覧できるように設定できます。グループごとに設定できます。
3. 特定の個人だけが閲覧できるように設定できます。公開鍵暗号が利用できます。

これらについて、説明いたします。

ヤフーボックスを導入するとします。

”ヤフーボックス”では、見かけ上、自分のコンピュータの中にフォルダが出来ただけのように見えます。エクスプローラを使って、ファイルのドラッグやコピー、貼り付けなどが自由にできます。エクスプローラから扱えるので、自分の PC 内のフォルダと見てプログラムを書くことが出来ます。しかしながら、ヤフーボックス内のデータはクラウド上に保存され自分の PC 内には、関連を示すデータが保存されます。

導入したヤフーボックスをクリックすると、下の図のようになります。



これらのフォルダにデータを移動させるときに暗号化をするのですが、**フォルダを選択するにはその中にあるファイルをクリックしなくてはならないので、サンプルピクチャを各フォルダに1つずつ配置してください。**

最初に、作ったときの機能は、

ある人から暗号化されたものがWebメールのアドレス宛に送られてきたときにその人用の復号化ソフトを使って暗号化された添付ファイルを復号化する機能です。復号化された結果は、標準では WebDecrypt というサブフォルダに保存されます。

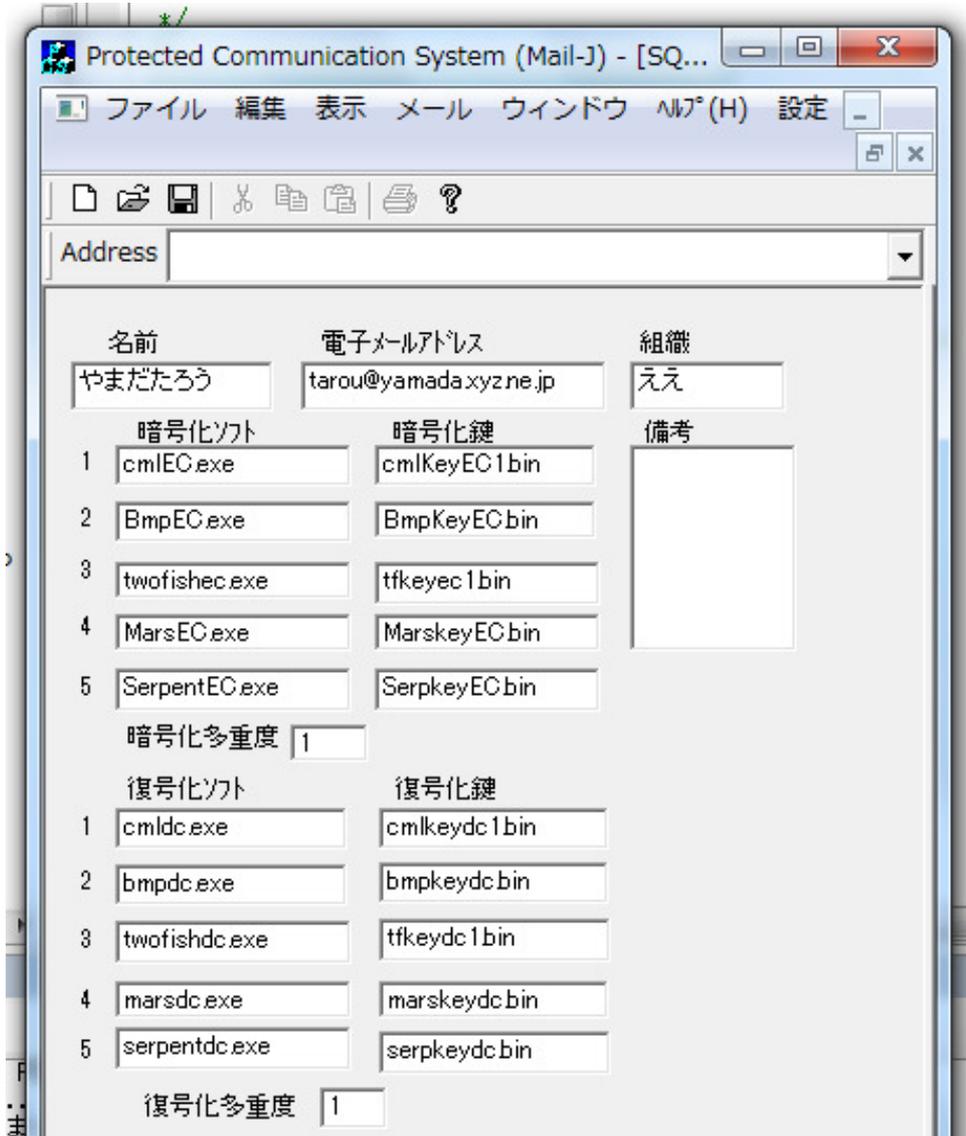
ある人に暗号化したものを送るのにまとめて暗号化しその結果を確認してから、暗号化されたものをWebメールのアドレス宛に送ることができます。その人用の暗号化ソフトを使ってファイルを暗号化する

機能です。暗号化された結果は、標準では **WebEncrypt** というサブフォルダに保存されます。
というものでしたが、それを改良して現在は、

クラウドにデータを預けるときに、暗号化しながら移すことができます。
この機能を、5段階の暗号化による強力な暗号化機能をもったクラウド暗号化ツールとして利用できます。

1. 暗号化(アップロード)

アドレス帳の自分の項目が下の図のように設定されているとします。



暗号化ソフト、暗号化鍵、復号化ソフト、復号化鍵の登録の様子をしっかりと確認してください。
この画面での、暗号ソフト、暗号鍵の登録は、大文字、小文字のどちらを使ってもかまいません。暗号化では、EC、復号化では、DCが入っているのが特徴です。

	暗号化ソフト	暗号化鍵
1	CmlEC.exe	CmlkeyEC1.bin
2	BmpEC.exe	BmpkeyEC.bin
3	TwofishEC.exe	TfkeyEC1.bin

4	MARSEC.exe	MarskeyEC.bin
5	SerpentEC.exe	SerpKeyEC.bin
	復号化ソフト	復号化鍵
1	CmlDC.exe	CmlkeyDC1.bin
2	BmpDC.exe	BmpkeyDC.bin
3	TwofishDC.exe	TfkeyDC1.bin
4	MARSDC.exe	MarskeyDC.bin
5	SerpentDC.exe	SerpKeyDC.bin

となっています。暗号化と復号化の対応関係に注意してください。

あなたのお名前が、やまだたろう、電子メールアドレスが、tarou@yamada.xyz.co.jp だったとします。

暗号(クラウド)ツール で **暗号化(アップロード)** を選択すると次の画面が現れます。

電子メールアドレスの項目 には、暗号化に利用する暗号化ソフトと暗号化鍵が登録されている **あなたのメールアドレス** を入力します。

クラウドでの共有では、メールアドレスの項目に入力してあるグループ名などを入力します。

The screenshot shows a window titled 'MailBox' with a sub-window 'SQAdBook'. It contains a table with columns for '名前' (Name) and '電子メールアドレス' (Email Address). Below this, there are two columns for '暗号化ソフト' (Encryption Software) and '暗号化鍵' (Encryption Key). The first entry shows 'ヤフーBOX' (Yahoo! Box) with email 'picture1', using 'Bmp56EC.exe' as the software and '1234567' as the key. A second entry is partially visible.

たとえば、ヤフーボックスの写真のフォルダに写すときに使う暗号の設定がアドレス帳で電子メールアドレスの項目に、**picture1** と記入してあれば、**picture1** と入力します。

保存 ボタンをクリックすれば、入力したアドレスを 10 個まで保存することも出来ます。また、一度入力して保存したものは、履歴として残っていますので、履歴の所のドロップボックスの三角印で表示して、クリックすれば、選んだものが入されます。

次に、暗号化するファイルを選択します。

検索(ファイル) をクリックするとエクスプローラの画面からファイルを選択できます。

複数個のファイルを登録でき、同時に暗号化と移動が行われます。

The screenshot shows a dialog box titled '暗号化(アップロード)'. It has a '電子メールアドレスの項目' (Email address item) field with a '保存' (Save) button and a '履歴(10個)' (History 10 items) dropdown. Below is a '暗号化するファイル' (Files to encrypt) section with a '検索(ファイル)' (Search files) button and a list area with '追加' (Add) and '削除' (Delete) buttons. At the bottom, there is an '出力(クラウド)フォルダ' (Output cloud folder) field with a '検索(フォルダ)' (Search folder) button and 'OK' and 'キャンセル' (Cancel) buttons.

つぎに、移動先のフォルダを決定します。検索(フォルダ)をクリックして、目的のフォルダ (ヤフーボックスのフォルダ) の中にあるファイルをクリックしてから開くをクリックすると、そのファイルが入っているフォルダが選択されます。

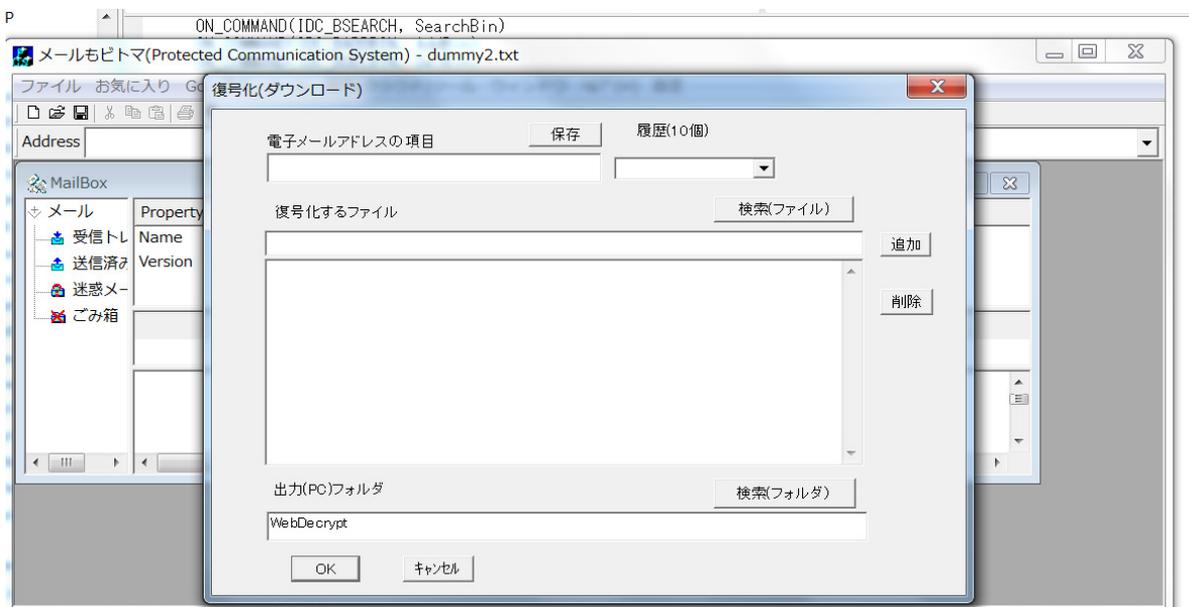
そして、OK ボタンをクリックすれば、選択したファイルが暗号化されてから目的のフォルダ (ヤフーボックスのフォルダ) に移ります。このとき、元のファイルは変更されません。削除もされません。コピーしたのに対して暗号化と移動が行われます。

暗号化されたものは、指定されたサブフォルダの中に入ります。

2. 復号化(ダウンロード)

アドレス帳の自分の項目や、ヤフーBOX の所には、復号化が暗号化に対応する形で設定されていますので。

暗号(クラウド)ツール から 復号化(ダウンロード) を選び、



あなたのメールアドレス (または picture1) を入力し、復号化するデータを選択してから、OK ボタンをクリックすれば、サブフォルダ WebDecrypt の中に復号化されたものが現れます。

特徴：

クラウド上の複数のサブフォルダに対してそれぞれ異なった方式での暗号化を選択できます。

グループごとに暗号化を分けるときは、そのグループでの復号化鍵をグループの構成員に配布しておく必要があります。

また、RSA 公開鍵暗号も利用できますので、特定の人から受け取った公開鍵で暗号化すれば、それに対応する秘密鍵を持っている人しか暗号化を解除できません。

ここからは、マニュアルの本文です。

1. 保証および法的責任の放棄

このソフトウェアの名称は、“メールもビットマ”です。暗号メールに関する特許の内容を実現したものです。

1.1 ご利用は自己責任です。

このソフトウェアに関する本文書の内容には信頼性があり、また正確であるものと確信しております。しかし、著者 宇山靖政 は、いかなる誤り、抜け落ち、また不正確さに対しても、その責任を負うことはありません。

著者 宇山靖政 は本マニュアルの内容およびそこに記述するソフトウェアに関して特定の機能に対する市場性および適合性の保証を始めとして、いかなる、またあらゆる明示的または暗黙の保証を放棄します。

本製品の品質および性能に関する危険（リスク）は本製品の購入者またはユーザーに帰属することになります。著者 宇山靖政 が事前にその可能性について通知を受けている場合においても、かような情報およびソフトウェアの使用に起因するような特殊なまたは結果的な損害を始めとして、いかなる損害に対しても法的責任を負うことはありません。

1.2 日本国内でのみご利用ください。

このメールソフトは、暗号技術の扱いに関する基本技術の特許内容として公開しています。更に次のホームページ (<http://uyama22.pa.land.to/>) でメールソフトのソースファイルや暗号ソフトのソースファイルを公開し、その内容を“公知の技術”としています。

“経済産業省の安全保障貿易管理の手引き”では、

2. 技術の提供の場合の主な例(関係法令:貿易外省令第9条)

ア. 公知の技術(※1)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)

- a. 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
- b. 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
- c. 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
- d. 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
- e. 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

※1 貿易外省令第9条第2項第9号でいう「公知の技術」とは、「不特定多数の者に公開されている技術又は不特定多数の者が入手可能な技術」と規定されています。これは安全保障貿易管理の観点から定義しているものであり、守秘義務の有無にかかわらず、特定少数の者しか知り得ない場合は「公知である」と判断されません。なお、例えば特許法では、社会に対する技術の新規性の観点から「公知」について規定しており、特定少数の者しか知り得ない場合でも、その者に守秘義務が無ければ「公知である」と判断されることとなります。

となっています。したがって、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になります。

しかしながら、暗号通信に関する法律的な規制は国によって異なります。日本国内に住んでいられる皆

様が日本国内でご利用になるのは自由に出来ます。したがって、日本に住んでおられる方々の情報は強力的に保護できます。

海外出張のためパソコン(外為法の暗号機能に該当のもの)を持ち出す場合、自分が使用するためだけに持ってゆき、他人に売ったり譲渡したりせずに持ち帰る場合は、経済産業省の許可を得なくてもよいという特例があります。ヤマハのヘリコプターの事件もありましたので、事前に経済産業省に確認を取ったほうが安全です。

国によっては、全ての通信を傍受してチェックするために、暗号通信の利用に強い制限がかかっている場合もありますので、外国での使用に関しては、慎重にお願いします。

日本では、憲法に

第21条〔表現の自由〕

- 1 集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。
- 2 検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

とあります。このメールソフトを使うと、“通信の秘密は、これを侵してはならない。”の部分が実現できる可能性が強まります。

質問がありましたら、作者(宇山靖政) (uyama33@yahoo.co.jp) まで、お問い合わせください。ただし、暗号技術に関する質問には個別にはお答え出来ません。ホームページに質問内容と回答を掲載します。

2段階の暗号化が可能です。ブロックサイズや鍵の長さを変えて多重暗号化をすれば暗号の強度は飛躍的に増大します。あくまでも、プライバシーを守ることや個人情報の保護などの平和的な目的に沿って利用して下さるようお願いします。

対称鍵(秘密鍵)の交換には、RSA 暗号(2560bit)と楕円曲線暗号(521bit)が利用できます。

2. はじめに

2.1 目的

盗聴に対抗できる安全な通信方法を実現する方法として、Protected Communication System を考え始めたのは 2000 年 4 月でした。これを特許申請して、2007 年 2 月 14 日にヨーロッパ特許庁からの正式認定を受け取りました。また、アメリカにおける特許も認められました。電子メールと電話に関する特許認定を受けています。

この通信方法を実現したものがこのメールソフトです。したがって、このソフトの目的は、--- “すべてのメールでの通信を強力に暗号化する。” --- ことです。暗号化の方針は、

1. 暗号化鍵を他人に預けない。(SSL では、サーバーに暗号の鍵があります。)
2. 鍵の長さに制限をつけない。
3. アルゴリズムの種類を限定せず、最新アルゴリズムがすぐに利用できる。
4. 暗号化、復号化は自分の端末機と相手の端末機で行ない、平文データが流れる経路を無くす。
5. 十分な多重暗号化が可能である。
6. 暗号アルゴリズムは送信者と受信者の順序対ごとに独立している。

となります。

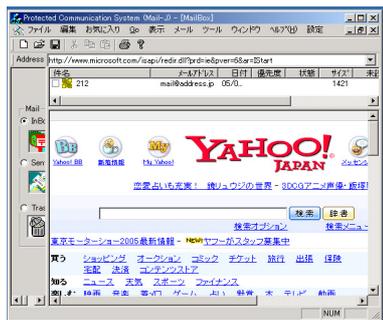
このような機能を持ったメールソフトです。電話などでもこの機能は必要であると考えます。現在は、電子メールソフトとしてのみ提供されているのですが、すべての通信が上の 6 つの原則の上に実現されるように願っています。

特許取得の過程は、“特許貧乏物語” に書いてありますので、これから、特許を取ろうとお考えの皆様は参考にしてください。(ホームページに置いてあります。) 必要な費用、手続き、時間などの部分は参考になると思います。

電話については、アンドロイド携帯では、パケット通信を利用した音声通話が可能だと思いますので、アンドロイド携帯で、この特許による暗号電話の開発は可能だと思っています。

この“メールもビットマ”では、楽しさを求めて、データを画像にする形の暗号化方式を利用できるようにしました。単に強力な暗号メールというだけでは肩がこります。そのうちに音楽ファイルの形式にして、暗号化データを音楽として聴けるようにしたいと思っております。楽しみにお待ちください。

2.2 (Web)フリーメールの暗号化



Hotmail や Yahoo メール などの、無料のメールサービスが提供されています。この無料アドレスを使用する場合について考えます。

無料の理由は、ユーザーのメールの内容を解析して、商業活動に役立てるためです。

さらに、サーバーが攻撃されてログイン ID とパスワードが大量に公開されてしまって、他の人に乗っ取られたり、メールの内容を見られたりしています。

たとえ、無料のメールサービスでも暗号化しておくほうが安全です。この“メールもビトマ”では、アドレス帳を適切に設定して多重暗号化をす

ることができます。

この“メールもビトマ”を使ってウェブサイトにアクセスできます。メールボックスを開いてから、“GO — Start Page” とするか、“お気に入り”からウェブサイトを選びます。そして、表示される Web ページから自分のメールボックスを開き、添付ファイル“mdata05.bmp”を自分のコンピュータにダウンロードします。ここでは、“mdata05.bmp”がダウンロードのフォルダーに収納されたとします。

メール本文については、“ファイル — 暗号 Web メール表示”として、送信者のメールアドレスと、“mdata05.bmp”をセットすれば、本来のメール本文が復号化されてから表示されます。

本来の添付ファイルに関しては、“ツール” — “復号化”として、ダイアログボックスの指示に従えば、送信者のアドレスに対応した復号化ソフトを使って復号化が行われます。そしてダイアログボックスで指定したフォルダに復号化されたファイルが収納されます。

復号化したファイルは他の適切なフォルダに移動してください。そうしないと、さらに同じ作業を繰り返したときに、上書きされてファイルが失われることとなります。

現在は、クラウドシステムのように、大量のデータが自分の手を離れた形で保存されている状態があります。このようなデータは、しっかりと暗号化されている必要があります。このときの暗号化方式や暗号強度は自由に設定できなくてはなりません。

これらについては、次の方法でより安全にできます。

アリスがボブのフリーメールのアドレスに暗号メールを送るとします。

設定方法

4. アリスは、アドレス帳にボブのフリーメールアドレスを登録します。
そして暗号化項目に **cmlEC.exe** (試用期間は、暗号化項目 **Bmp56EC.exe**、暗号化鍵 **1234567**) を登録したとします。このときの暗号化鍵に対する復号化鍵をボブに届けておきます。
さらに、ボブの普通のメールアドレスの暗号化項目もボブの **Gmail** のものと一致させます。

アリスさんのアドレス帳では、

名前	電子メールアドレス
ボブさん	bob@xyz.co.jp

	暗号化ソフト	暗号化鍵	
1	cmlEC.exe	cmlkeyEC.bin	(試用期間は、Bmp56EC.exe、1234567)
2			
3			

	復号化ソフト	復号化鍵	
1	cmlDC.exe	cmlkeyDC.bin	(試用期間は、Bmp56DC.exe、1234567)
2			
3			

さらに、アリスさんのアドレス帳で、

名前	電子メールアドレス
Web ボブさん	webbob@yahoo.co.jp

	暗号化ソフト	暗号化鍵	
1	cmlEC.exe	cmlkeyEC.bin	(試用期間は、Bmp56EC.exe、1234567)
2			
3			

	復号化ソフト	復号化鍵	
1	cmlDC.exe	cmlkeyDC.bin	(試用期間は、Bmp56DC.exe、1234567)
2			
3			

としておきます。

2. ボブはアリスのアドレスの項目を作り、そのアドレスに関する復号化のソフトの項目に、cmlDC.exe (試用期間は、復号化項目 Bmp56DC.exe、復号化鍵 1234567) を登録し、アリスからもらった復号化鍵も登録しておきます。

ボブさんのアドレス帳では、

名前	電子メールアドレス
アリスさん	alice@pqr.com

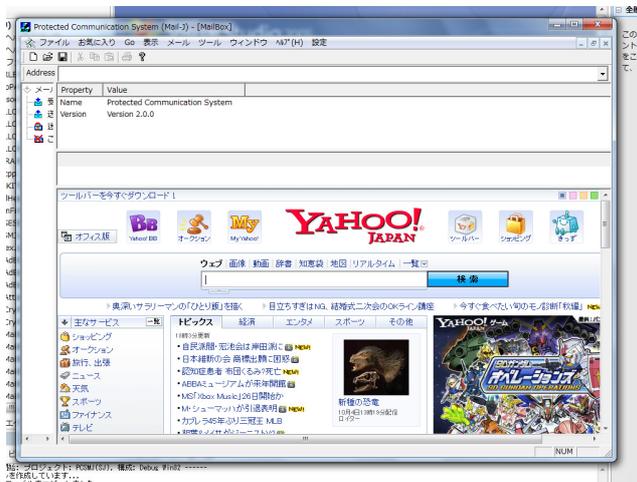
	暗号化ソフト	暗号化鍵	
1	cmlEC.exe	cmlkeyEC.bin	(試用期間は、Bmp56EC.exe、1234567)
2			
3			

	復号化ソフト	復号化鍵	
1	cmlDC.exe	cmlkeyDC.bin	(試用期間は、Bmp56DC.exe、1234567)
2			
3			

3. アリスがボブの Gmail アドレスに向けて送信すると、そのデータは cmlEC.exe (試用期間は、暗号化項目 Bmp56EC.exe、暗号化鍵 1234567) で暗号化されてボブのフリーメールアドレスに届きます。本来の添付ファイルと、メール本文が暗号化されて出来たファイル “mdata05.bmp” がついています。次のようにして、本文を表示できます。

4. メール本文は、次の手順で直接表示できます。

(4-1) Go - Start Page とすると、

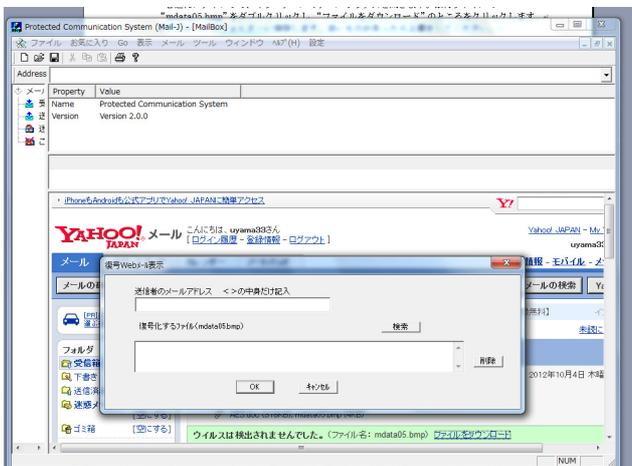


となって、インターネットエクスプローラと同じ画面が表示されます。

普通にログインして、ヤフーメールのメールボックスを開きます。添付ファイルの“mdata05.bmp”をクリックし、“ファイルをダウンロード”のところをクリックします。ダウンロードのフォルダに保存します。古いものがあつたら上書きしてください。

さらに、送信者のメールアドレスをコピーしてください。

(4-2) ファイル - 暗号 Web メール表示
とします。

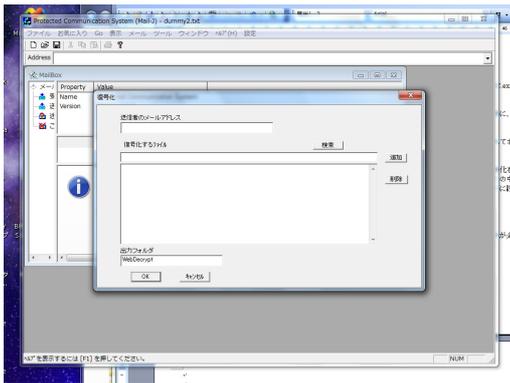


この簡単な場合では、ヤフーメールを表示したときに現れる、送信者のメールアドレスをそのままコピーして利用できます。ただし<>の中身だけを使ってください。先ほどコピーしたものを貼り付けます。

つぎに、検索で、ダウンロードのフォルダにある“mdata05.bmp”を探してセットしたら OK をクリックしてください。メール本文が復号化されて表示されます。

5. 本来の添付ファイルについても、暗号化されて届いています。データを保存した後に、ツールの復号化を利用して復元できます。このときに、利用する復号化で使うソフトは、ボブのアドレスブックの中の、アリスのアドレスの項目に登録されている復号化ソフト cmlDC.exe (試用期間は、復号化項目 Bmp56DC.exe、復号化鍵 1234567) を使うように設定すれば復号化できます。下の図の送信

者のメールアドレスの項目にアリスのアドレスを設定します。そうすると復号化では、アリスのアドレスに登録されている復号化ソフトと復号化鍵が使われます。



これによって、フリーメールも暗号化フリーメールになります。

2.3 他のメールソフトとの連携

皆様が、すでに使われているメール用のソフトがあると思います。下の図はサンダーバードです。



このようなメールソフトを使って、送られてきたメールを受信することが多いと思います。

受信したメールがサーバーに残っていれば、“メールもビットマ”でもう一度受信すればよいのですが、サーバーに受信済みのメールを残さない設定にしている方も多いことでしょう。

暗号化されているメールを、サンダーバードで受信してしまった場合は次のようにします。
添付ファイルを保存します。(ダウンロードのフォルダだとします。)

メール本文の内容は、必ず“**mdata05.bmp**”という名前のファイルになっています。拡張子は **bmp** ですが、暗号化の方法によって、必ずしもビットマップファイルになっているわけではありません。

これを見るには、フリーメールの場合と同様です。

“ファイル — 暗号 Web メール表示”として、送信者のメールアドレスと、“**mdata05.bmp**”をセットすれば、本来のメール本文が復号化されてから表示されます。

本来の添付ファイルに関しては、“ツール” — “復号化”として、ダイアログボックスの指示に従えば、送信者のアドレスに対応した復号化ソフトを使って復号化が行われます。そしてダイアログボックスで指定したフォルダに復号化されたファイルが収納されます。本来の添付ファイルは、ファイル名や拡張子はもとのままで変更はされていません。

復号化したファイルは他の適切なフォルダに移動してください。そうしないと、さらに同じ作業を繰り返したときに、上書きされてファイルが失われることとなります。

2.4 UserKey.dat

現在、ATMailSys フォルダにある”userkey.dat”というファイルは正式のものではありません。ベクターに送金後に入手できる同名のファイルで、上書きすれば機能制限が解除されます。

購入したライセンスキーは、同時に 1 台のマシンにおいてのみ使用を許可します。複数台のマシンにおいて本ソフトウェアのライセンスキーを登録する場合は、マシンの台数分のライセンスキーを購入してください。

試用期間中の動きは次のようになります。

1. 登録できる暗号化ソフトは **Bmp56EC.exe** だけです。さらに、暗号化鍵は “1234567” だけです。復号化は 5 段階まで自由に設定でき、復号化鍵は自分で作成したものが利用できます。
2. このとき、本文と添付ファイルは、データ内容がビットマップ形式として暗号化された添付ファイルとして送信されます。また、本文の代わりにダミーテキストが送られます。

正しい”userkey.dat”がある場合は、次のようになります。

1. 暗号化、復号化を 5 段階まで自由に設定できます、暗号化鍵は自分で作成したものが利用できます。暗号化ソフトがアドレス帳の受信者となる人の欄に登録されている場合
本文の代わりにダミーテキストが送信されます。本文と添付ファイルを暗号化したものが送信されません。
2. 暗号化ソフトが登録されていない場合
本文はそのまま暗号化されずに送信されます。添付ファイルも暗号化されません。

2.5 暗号ソフト

付属する暗号ソフト Neko, Bitoma, AES, Twofish, Serpent, MARS, Camellia, Misty, RSA, ECC については、ホームページに、この暗号メーカーで使用できる形にしたソースコードを掲載してあります。このメーカーで使用するために変更した部分もありますので、安全性などに関しては本来の公開されているソースコードと比較検討されて、十分納得された上でご利用ください。

自分宛のメールで、大きな添付ファイルを送ってみて処理速度、安定性を確認のうえで本格的な使用を開始してください。

暗号ソフト.zip を開くと、このソフトで利用する暗号化ソフト、復号化ソフトが現れます。
EC.exe が暗号化ソフト、DC.exe が復号化ソフトです。

データの形式がビットマップ形式になるのは、
NekoEC.exe (復号化には NekoDC.exe を使います。)
Bmp56EC.exe (復号化には、Bmp56DC.exe を使います。)
BmpEC.exe (復号化には、BmpDC.exe を使います。)
です。

これらを、多段階の暗号化の最後の段階で利用すれば図形となったデータが相手に届くことになります。

NekoEC.exe (復号化には NekoDC.exe を使います。) による、にゃん語通信では、日本語が猫語になるのはもちろんですが、猫語にするまえに、AES 暗号で暗号化して、さらに Camellia 暗号で暗号化してから、最後に、にゃん語に直すことが出来ます。にゃん語になったデータは、あなたの可愛い猫の写真と一緒に相手が届きます。前もって暗号化した場合は、AES、Camellia の鍵を受信者に送っておく必要があります。このためには、公開鍵暗号である RSA 暗号と楕円曲線暗号を利用できます。

でも、そのまえに、かわいいあなたの猫の写真を撮ることをお忘れなく。

にゃん語への翻訳が間違っていると言う猫がいたらその猫とは裁判所で戦います。犬の写真にすれば、わん語通信になるかもしれませんが、これについてはまだ研究中です。

BmpEC.exe (復号化には、BmpDC.exe を使います。) では、メールデータが四角い抽象画になって相手に届きます。

NekoEC.exe (復号化には NekoDC.exe を使います。)
BmpEC.exe (復号化には、BmpDC.exe を使います。)

では、共通の暗号化鍵、復号化鍵を使います。この鍵は、BmpCrypt.exe で作成します。

Bmp56EC.exe (復号化には、Bmp56DC.exe を使います。) はデータを抽象画に変えますが鍵は変更できません。

Bitoma, Neko は、どのクラスにも一人くらいはいた、“お茶目なやつ” と思ってください。処理速度に問題はありますが、データサイズが 2 倍になります。

高速な処理が可能な対称鍵暗号で、世界的にも評価の高い暗号ソフトとしては、
AesEC.exe (復号化には、AesDC.exe を使います。) —— AES 暗号
TwofishEC.exe (復号化には、TwofishDC.exe を使います。) —— Twofisah 暗号
SerpentEC.exe (復号化には、SerpentDC.exe を使います。) —— Serpent 暗号
MarsEC.exe (復号化には、MarsDC.exe を使います。) —— Mars 暗号

CmlEC.exe (復号化には、CmlDC.exe を使います。) —— Camellia 暗号
MistyEC.exe (復号化には、MistyDC.exe を使います。) —— Misty 暗号
が入っています。

このうちで、AES、Camellia、Misty は有名ですが、他のソフトも優秀です。

AES は、アメリカの新暗号規格 (Advanced Encryption Standard) として規格化されたものです。
Twofish, Serpent, MARS などは AES の良きライバルです。

Camellia は AES と同等の安全性があり、さらにサイズが小さく、高速な暗号化、復号化が可能です。

欧州の [NESSIE](#) プロジェクトや日本の [CRYPTREC](#) が作成した「電子政府推奨暗号リスト」に採用されています。

MISTY は三菱電機が開発した秘密鍵暗号アルゴリズムにより、128bits の暗号化鍵を持つ 64bits ブロック暗号。大量の平文と暗号文の組み合わせを使って暗号を解読する差分解読法や線形解読法を応用した、独自の暗号強度評価指標に基づいて設計され、DES などをしてのぐ安全性と実用性を実現している。W-CDMA の標準仕様に採用されて、日本初の世界標準暗号となりました。暗号化ソフトでのデータサイズの増加量は暗号化のときのブロックサイズ以下です。

各アルゴリズムとも、平文ファイルを暗号化する暗号化ソフト、暗号化されたファイルを復号化する復号化ソフト、暗号化鍵や復号化鍵を作る鍵作成ソフトの 3 つからなっています。暗号ソフトと復号化鍵はすでに、ATMailSys フォルダに入っています。

各暗号ソフトの詳しい説明は、ホームページ (<http://uyama22.pa.land.to/>) で確認してください。

これらの暗号ソフトを、5 段階まで適用して 5 重に暗号化できます。様々な暗号技術を多重に適用して通信の秘密を守ります。最新の暗号技術の発展に合わせて使用する暗号化ソフトを簡単に変更できます。

このソフトによって、アドレス帳に暗号化ソフト名、暗号化鍵のファイル名、復号化ソフト名、復号化鍵のファイル名を登録するだけで、様々な暗号技術を簡単に利用できるようになります。

また、暗号ソフトをどのような形式で作成したらこのソフトで利用可能となるかを説明してありますので、独自に開発した暗号を利用できます。もちろんこの暗号通信で使用している暗号ソフトのソースコードは公開してあります。

この方式は、さまざまな暗号化方式のソフトが利用できるので、情報を強力に暗号化して送信できるようになります。利用者はそれぞれの目的にあった形で十分な暗号強度を持ったものを利用できるようになります。

これらの暗号で使う対称鍵を互いに交換しなくてはなりません。鍵交換で利用する公開鍵暗号のソフトが、

CFRSAEC.exe (復号化には、CFRSADC.exe を使用します。) — ARS 暗号

です。

RSA 公開鍵方式、楕円曲線暗号での暗号化や復号化は処理時間が長くなるので、大きなデータを送信するときの、送信途中での暗号化には向きません。

鍵交換のために、楕円曲線暗号(ECC)のソフトも追加しました。

共通鍵 (秘密鍵) 方式のものでも処理速度には差があります。利用可能なものの中では、Serpent がやや時間がかかるようです。ご自分のコンピュータで十分テストしてください。

暗号化のときには、黒い画面が出てきます。処理に長時間かかるときはその画面が消えるまでしばらくお待ちください。

暗号メールに楽しさを加えようと考えて作った NekoEC.exe, BmpEC.exe ですが、画像として暗号化したときのデータサイズが大きくなってしまいます。鍵作成ソフトを使ってご自分で確認してください。

アドレス帳に自分のアドレスを登録し、自分宛に暗号化したデータを送信してみて添付するファイルの現実的な大きさを見極めてください。

2.6 鍵作成について

サンプルの暗号鍵は、すでに ATMailSys に入っています。

鍵を新たに作成する場合は、“鍵作成ソフト.zip”を解凍します。そして鍵作成ソフトのフォルダの中に入っている鍵作成ソフトを起動します。

たとえば、BmpCrypt.exe を起動すると、下の図のようになります。



操作手順：

1. 暗号化鍵ファイル名、復号化鍵ファイル名を入力する。
鍵のファイルは基本的には、鍵作成ソフトと同じフォルダに作成されます。
以前作ったmのと名前が同じだと前のものが上書きされて消えてしまいます。
5. 鍵の長さを決定する。
ボタンをクリックしてください。
6. 暗号化した後のファイルの拡張子を決定する。
この場合は、暗号化した後ではファイルはビットマップファイルという画像ファイルになります。

拡張子が **bmp** にしてあれば画像として扱われ暗号化後のファイルを画像として見ることができます。

7. 鍵を生成

鍵を生成 のボタンをクリックしてください。鍵が作成されます。もう一度クリックすると別の鍵が作成されます。

8. 保存終了

鍵作成ボタンをクリックしてから、保存終了をクリックすれば同じフォルダに鍵が保存されます。

9. 鍵のテスト

鍵のテストボタンをクリックすると、作成した鍵による暗号化と復号化の様子が一番下の窓に表示されます。テキストファイルしか表示できませんので、もとのデータがワードの文書のような場合はうまく表示できません。暗号化した結果は変換後のデータを **16** 進数で表示します。

10. 途中経過の表示

表示 の部分の選択で、暗号化、復号化のと中継かを表示するか否かを選べます。表示には長い時間と大きなメモリーが必要です。途中経過を表示しなくても結果は直接確認できます。

ここで、鍵作成とその鍵を使った暗号化と復号化のテストができます。鍵作成ボタンをクリックしてから、保存終了をクリックすれば同じフォルダに鍵が保存されます。他の鍵作成ソフトも同様です。

鍵の長さは可能な範囲で自由に設定できます。鍵を生成するときは鍵の名前に十分注意してください。同じ名前で作成された鍵はすでに使っているものを上書きしますので、復号化が出来なくなる可能性があります。鍵ファイルの最後の数字を変えるか、もっと分かりやすい名前にするか工夫してください。

本格的な運用では、鍵は新たに作成したものをお使いください。作成した鍵を **BmpMailSys** フォルダにコピーしてください。または、**USB** メモリの中にフォルダを作って分類した形で保存することもできます。この場合は、アドレス帳の設定にドライブとフォルダと鍵のファイル名を記載する必要があります。

順序対形式にこだわるなら、暗号化鍵だけでよいのですが、送信後に送信内容を確認するならば復号化鍵もコピーしておく必要があります。

使用する暗号と鍵を決めたら、アドレス帳に登録します。あなたが、**MistyEC.exe** と **MistykeyEC.bin** を使って暗号化したデータを、**B** さんに送るなら、**B** さんに **MistykeyEC.bin** と同時に作成されたところの、**MistykeyDC.bin** を事前に **B** さんに手渡してください。そして **B** さんのアドレス帳のあなたの項目で、復号化のところを、**MistyDC.exe**、**MistykeyDC.bin** と設定してもらってください。

直接会って鍵交換するのが難しい場合は、公開鍵暗号 **RSA** がありますので、それを利用してください。使い方や設定方法は、鍵の交換の項目で詳しく記載します。

B さんは、あなたから受け取った **MistykeyDC.bin** を **BmpMailSys** の中に入れます。名前がぶつかるなら、ファイル名を **BmpkeyDC2.bin** などと変更し、復号化鍵の登録内容も **BmpkeyDC2.bin** と変えます。

グループモードなどをテストするときは、貴方のお名前とメールアドレスも登録しておいてください。グループモードで送られてきた場合は、貴方のお名前とメールアドレスが、アドレス帳に記載されていることが同一グループに属する条件になります。

暗号通信をする相手の方が、貴方に送るデータを暗号化するように設定してもらってください。もちろん暗号化ソフト、復号化ソフトを自作し、暗号化部分を通信相手に直接に手渡しておくのが一番よい方法です。通信する本文や添付ファイルの暗号化に **RSA** 公開鍵方式を利用されてもかまいませんが、暗号化にとっても長い時間がかかります。

処理速度、変換前と変換後のデータサイズの変化について、十分注意して確認してください。

送信する相手のコンピュータの処理速度、相手のプロバイダーで受信できる添付ファイルの大きさの上限についても配慮してください。

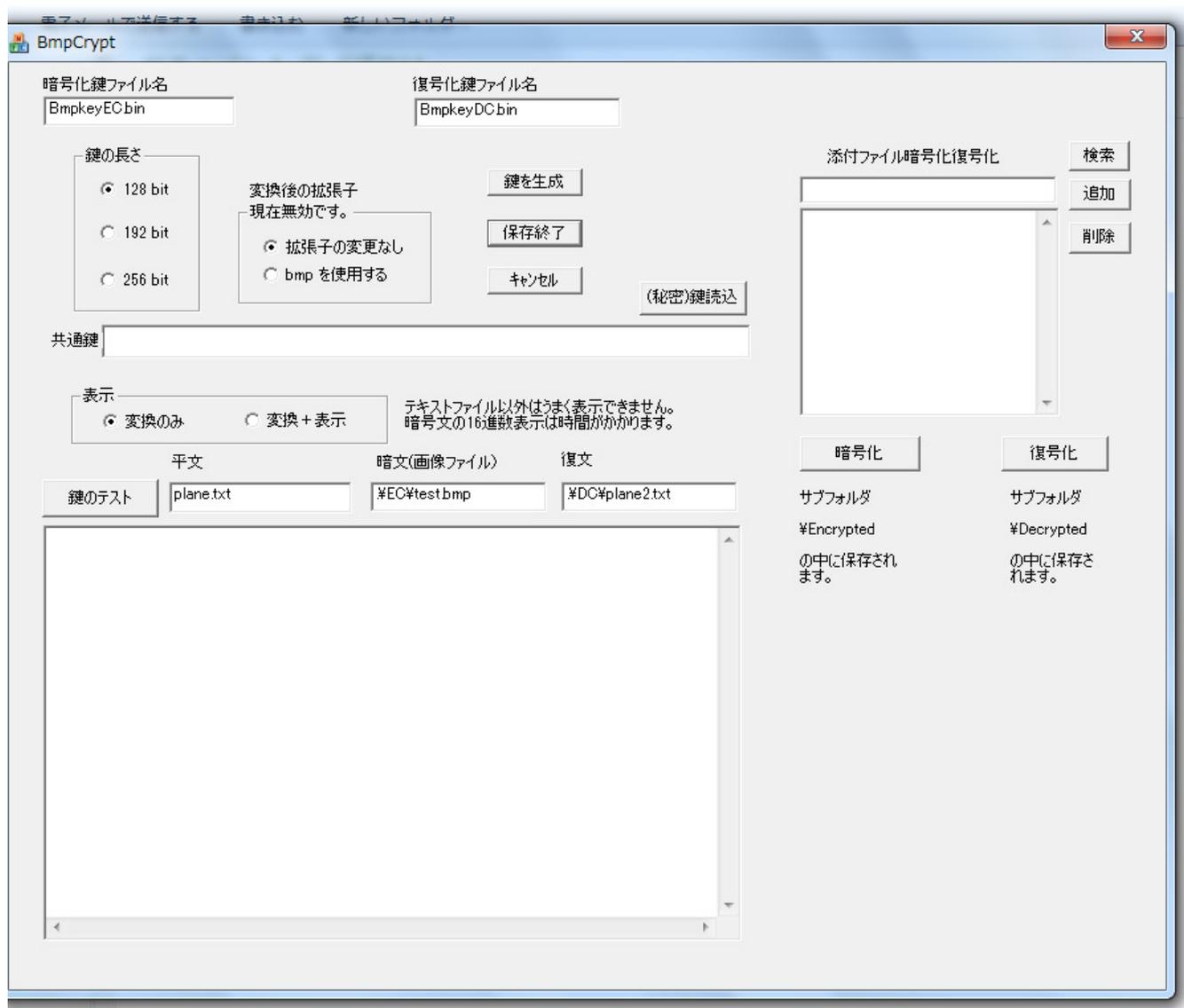
鍵作成ソフトのフォルダには、AESKey.exe, BmpKey.exe, CMLkey.exe, MarsKey.exe, MistyKey.exe, SerpentKey.exe, TwofishKey.exe, CFRSAKey.exe が入っています。それぞれが、対応する暗号化ソフト、復号化ソフトのための鍵を作成します。ひとつひとつ確認しておきます。

AEScript.exe, は AesEC.exe, AesDC.exe で使う暗号化鍵と復号化鍵を作ります。



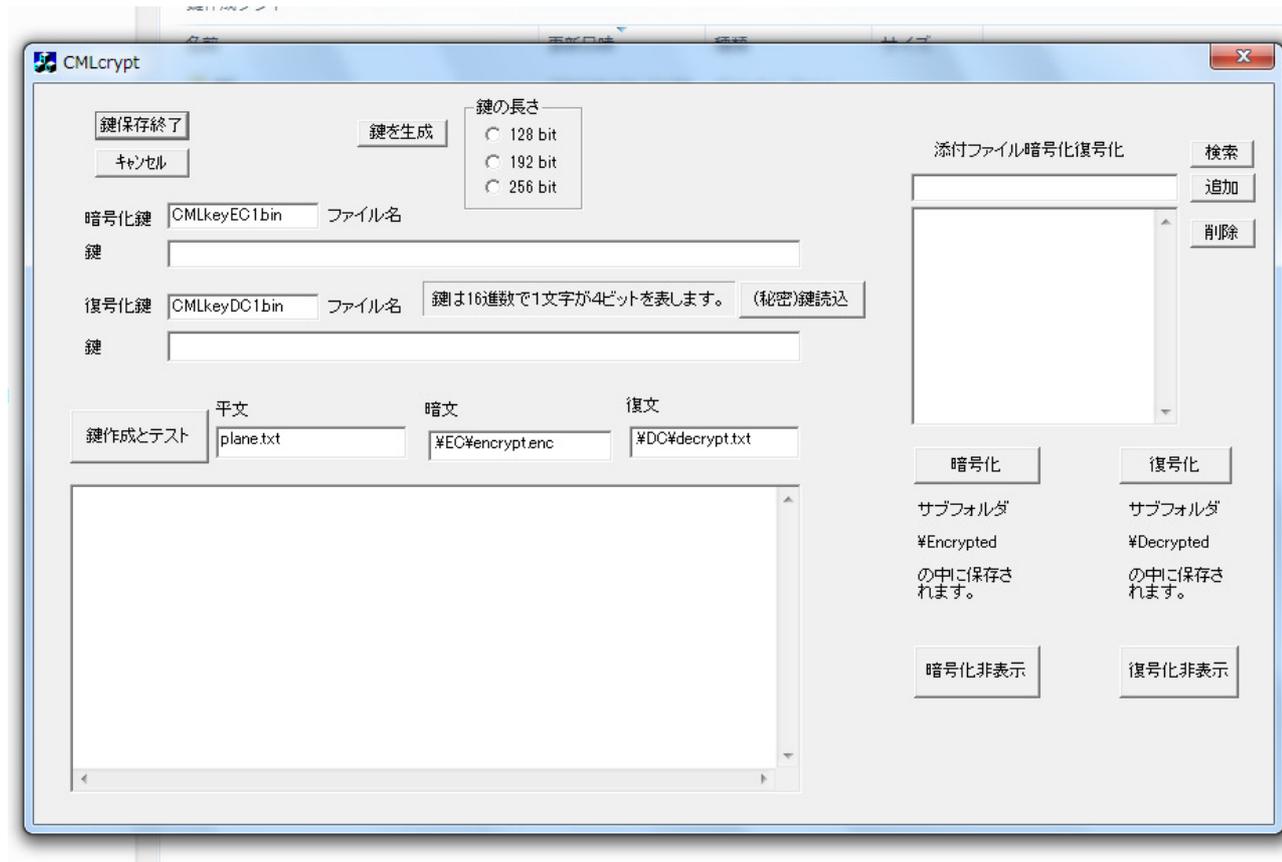
これは、アメリカの新暗号規格 (Advanced Encryption Standard) AES として規格化されたものよりも、鍵のサイズ、ブロックサイズの種類が多くなっています。応募したときの古い形のままにしました。多重暗号化したときに、ブロックサイズが互いの異なるほうが解読しにくくなると思います。

BmpCrypt.exe, は BmpEC.exe, BmpDC.exe および NekoEC.exe, NekoDC.exe で使う暗号化鍵と復号化鍵を作ります。



このソフトでは、変換後のデータサイズが 2 倍近くなってしまいます。画像としての扱いはよいのですが、メールサーバでのデータサイズの上限にはご注意ください。

CMLcrypt.exe, は CmlEC.exe, CmlDC.exe で使う暗号化鍵と復号化鍵を作ります。



鍵の長さを選んでから鍵を生成します。鍵の表示場所が 2 箇所ありますが、共通鍵ですから同じ値になります。

鍵のテストでは、平文にエクセルファイルや、ワード文書を選ぶと表示はうまくできませんが、暗号化は行われていますのでご安心ください。

カメリアは日本で作られた優秀な暗号ソフトです。

MarsCrypt.exe, は MarsEC.exe, MarsDC.exe で使う暗号化鍵と復号化鍵を作ります。



これは、IBM が作成した暗号ソフトです。AES 暗号の候補でもありました。

他のものより設定が複雑ですが、あまり気にしないでクリックして下さい。
設定するのは、ファイル名、鍵の長さ、モード、初期値です。
初期値は、CipherInit 変更 をクリックするだけです。何回かクリックしてみてください。
モードは
暗号文に変換するときの方法を決めます。これも適当に設定してください。
鍵の長さは、長くすると計算時間が少し長くなります。気にするほどではありません。
そして、テストしてから、鍵保存終了 で終わりです。

MistyCrypt.exe, は MistyEC.exe, MistyDC.exe で使う暗号化鍵と復号化鍵を作ります。



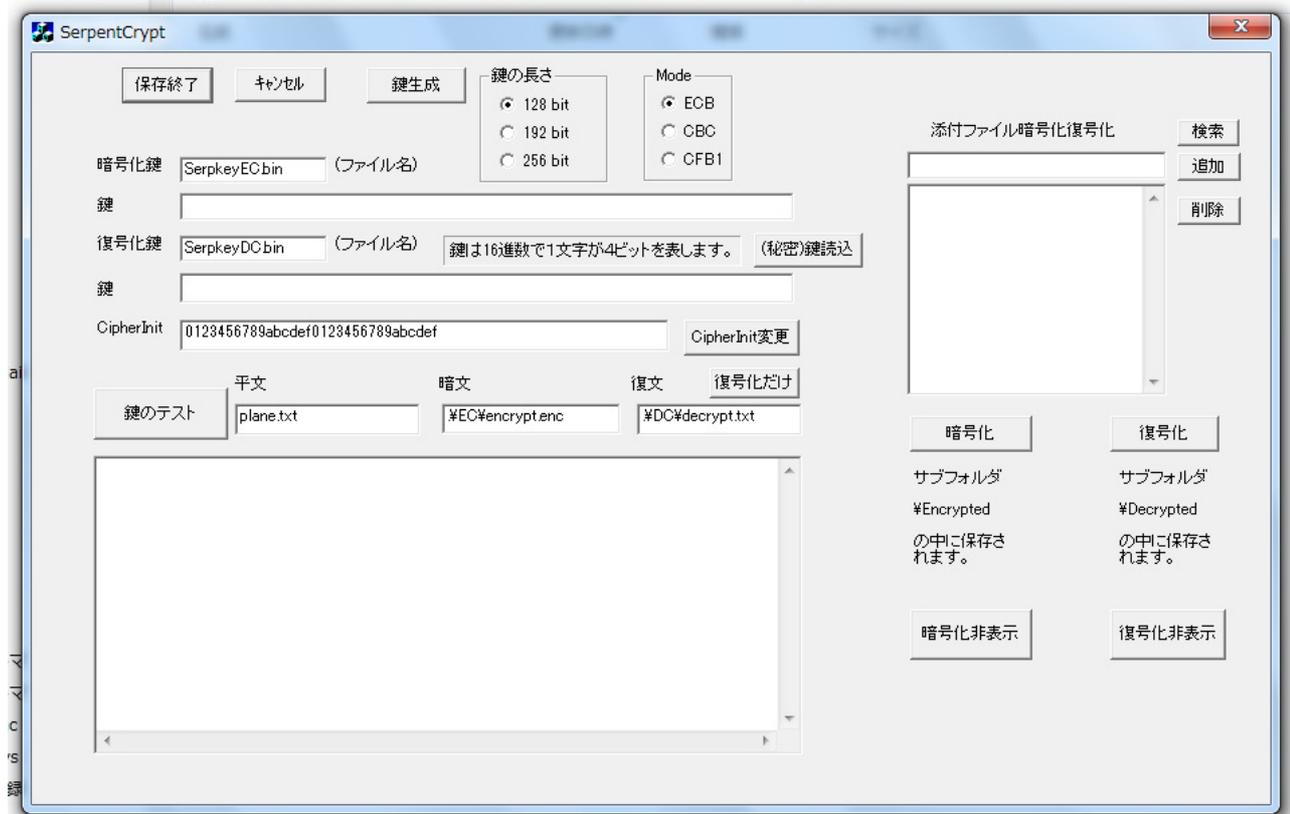
日本製の、軽量で高速な暗号ソフトです。

鍵作成は、鍵作成ボタンをクリックします。クリックするたびに新しい鍵が作成されます。

Test をクリックすると、暗号化の様子だけが表示されます。

そして、保存終了 で鍵のファイルが同一のフォルダに保存されます。

SerpentCrypt.exe, は SerpentEC.exe, SerpentDC.exe で使う暗号化鍵と復号化鍵を作ります。



他のものより設定が複雑ですが、あまり気にしないでクリックして下さい。
設定するのは、ファイル名、鍵の長さ、モード、初期値です。
初期値は、CipherInit 変更 をクリックするだけです。何回かクリックしてみてください。
モードは
暗号文に変換するときの方法を決めます。これも適当に設定してください。
鍵の長さは、長くすると計算時間が少し長くなります。気にするほどではありません。
そして、テストしてから、鍵保存終了 で終わりです。

TwfCrypt.exe, は TwofishEC.exe, TwofishDC.exe で使う暗号化鍵と復号化鍵を作ります。



設定するのは、ファイル名、鍵の長さ、モードです。
モードは、暗号文に変換するときの方法を決めます。これも適当に設定してください。
鍵の長さは、長くすると計算時間が少し長くなります。気にするほどではありません。

そして、テストしてから、鍵保存終了 で終わりです。

ただし、Bmp56EC.exe, Bmp56DC.exe のための暗号鍵は、作成できません。
また、RSA 暗号、楕円曲線暗号に関連するものは次の項目で説明します。

2.7 RSA 暗号を使った鍵交換の手順

現在、Gmail や Yahoo メールなどのフリーメールが盛んに利用されていますが、たとえ SSL で通信経路は安全だと宣伝されていても、メールサーバの中ではデータは暗号化されていません。そればかりではなく、利用者に対して効果的な宣伝を送信するために、利用者のメール本文の解析が行われています。

もし、あなたがプライバシーを守りたいならば、この暗号通信システムをご利用ください。無料の試用期間で、簡単な暗号化であったとしても、このシステムはメール本文の解析を防ぎます。ぜひ、ご利用ください。

たとえ簡単な暗号化であったとしても、暗号化してあるものを本来の受け取り手以外のものが復号化すると法律に違反すると思います、

公開鍵暗号 RSA 方式のソフトです。“メールもビトマ”、“Cipher Web Mail”における共通鍵（対称鍵）の交換のために作成しました。もちろん貿易管理令に違反しないようにソースコードを HP で公開します。

他の作者の方の作品では、鍵の長さが不十分なので、512 ビット、1024 ビット、1536 ビット、2048 ビット、2560 ビットの鍵を扱えるようにしました。（鍵を作成するのに要する時間はそれぞれ、30 秒、10 分、40 分、2 時間、3.5 時間です。メモリーの量や CPU の性能で異なります。）

公開鍵暗号は処理速度が遅いので、メールの送信途中での暗号化に利用すると、時間がかかりすぎてサーバーとの接続が切れてしまう恐れがあります。小さなデータの交換に利用するか、事前に暗号化したものを添付ファイルとして送信するようする必要があります。

2セット用意して、普通のメール用と、鍵交換専用のものに分けて使うのが便利な方法だとかんがえます。“メール用”、“鍵交換用”の二つのフォルダを用意してその中にそれぞれ“BtmMailSys”をコピーします。

公開鍵暗号の暗号化機能と復号化機能を分離したものを用意してありますので、鍵交換用に用意し他フォルダの中での、メールもビトマのアドレス帳にそれらを登録してご利用ください。

あるいは、この鍵作成ソフトは公開鍵、秘密鍵を別々に登録し、別々に機能させることもできますので、相手から受け取った公開鍵で、必要なファイルを暗号化してから、相手に送信すれば”鍵交換用”のシステムを用意しなくてもかまいません。

2.6 で扱っているソフトは、共通鍵方式（対称鍵方式、秘密鍵方式）と呼ばれます。この共通鍵を秘密にしておかなくてはなりません。自分が作成した鍵をどのようにして相手に届けるかが問題となります。

会社で直接会ってお互いに受け渡しができるのであればそれがかまいませんが、なかなか会えない場合には公開鍵暗号を利用します。

RSA 公開鍵暗号を用意いたしましたのでお使いください。欠点は時間がかかることです。鍵作成では、512 ビット鍵の作成は焼く 1 分、1024 ビット鍵の作成は約 15 分、1536 ビット鍵の作成は約 40 分、2014 ビット鍵の作成は約 2 時間です。

公開鍵の性質上、頻繁に変更するものでもありませんので、長めの鍵を作ったらそれをしばらく利用できます。

さらに、公開鍵暗号方式を使用して電子署名というものが実現できます。この仕組みを、PKI といいます。これは公開鍵暗号の有効な使用方法だと言えます。

RSA 暗号では、公開鍵で暗号化したものを秘密鍵で復号化することが基本ですが、逆に秘密鍵で暗号化したものを、公開鍵で復号化できます。

秘密鍵は、鍵を作成した人だけが所有し、秘密にしておく性質のものです。セットになっている公開鍵で復号化出来るのは、セットになっている秘密鍵で暗号化されたものだけです。もし、秘密鍵が盗難にあっていなければ、不正にコピーなどされていなければ、公開鍵で復号化できるデータは、秘密鍵の所有者によって暗号化されたと言えます。

RSA 暗号では、「片方の鍵を使って暗号化したものはそれと対になっているもう一方の鍵を使用しなければ復号化できない」のです。これはすなわち、公開鍵で暗号化したものは秘密鍵でしか復号化できないということとともに、秘密鍵で暗号化したものは公開鍵でしか復号化できないということでもあります。電子署名ではこれを利用します。

「公開鍵はだれにでも公開しているものなんだから、秘密鍵で暗号化することって意味がないんじゃないの？」と思われる方もいるかもしれませんが、ところが、これが大いに意味があるのです。

電子署名の原理は、A さんが B さんにある文書を送ろうとしている。この文書（平文）とともに、文書を自分の秘密鍵で暗号化したものを一緒に送るのです。この 2 つを受け取った B さんは、まず暗号化された文書を A さんの公開鍵で復号化する。それと平文を比較する。これが一致したとき、どのようなことが言えるだろうか。それは、「その文書は A さん以外のだれかによって改ざんされていない」ということが言えるのである。なぜならば、公開鍵を用いて復号化できる＝それは対応する秘密鍵、すなわち A さんのみが持つ秘密鍵で暗号化された＝暗号化したのは A さんに間違いなし、という考え方が成り立つからです。（図 1）

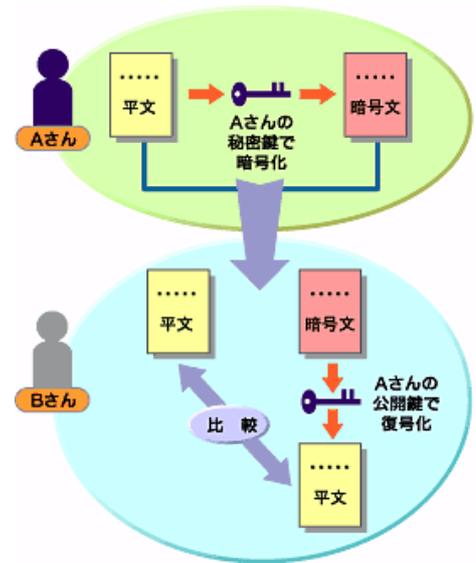


図 1 電子署名の考え方

しかし、この方法には大きな欠点があります。

それは、安全性を求めて鍵の長さを大きくすると暗号化や復号化に時間がかかるのです。電子メールで大きなデータを扱うときは、送信の途中で暗号化したり、受信の途中で復号化したりしようとするれば、タイムアウトでサーバーとの接続が切れてしまう恐れがあります。

そこで、ハッシュ関数を使ってもとの文章から得られた小さなデータ（ハッシュ値）を秘密鍵で暗号する方法を取ります。

ハッシュ関数とは、以下のような特徴を持つ関数です。

元データの長さに関係なく、ハッシュアルゴリズムの出力値（これをハッシュ値という）は必ず決められた長さ（128 ビットや 160 ビット）になる。

元データが少しでも異なれば、ハッシュ値は大きく異なる。

ハッシュ値から元データを推測することはほぼ不可能である。

このような理由から、平文のハッシュ値を平文の代わりに秘密鍵で暗号化するという形が一般的です。（図 2）

A さんは、平文から、ハッシュ関数を使ってハッシュ値を計算します。ハッシュ関数には、MD5, SHA-1, SHA-2 などいろいろありますが、SHA-1, SHA-2 が使えます。さらに、SHA-2 には、4 種類の関数があります。

この電子署名によって、「なりすまし」「改ざん」のリスクを回避することができ、結果として「否認」のリスクも回避することができることとなります。

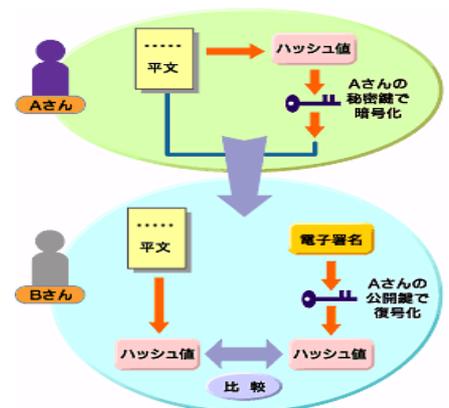


図 2 ハッシュ関数での電子署名

日本でも電子署名法（正式には「電子署名及び認証業務に関する法律」）が国会で可決され、施行されます。

この電子署名法は、電子データの文書に電子署名がされた場合、押印がされたものと同等の効力を持たせること、そして特定の基準を満たした認証局については「特定認証業務」というお墨付きを与えようと

いうものです。

もちろん、認証局を使っていないので法律的な効力はありません。しかし、改ざんを防ぐことに関しては、十分な強さを持っていると考えます。

具体的な手順を見てゆきます。

電子署名の作成

実際に電子署名を付加する手順を確認します。

- (1) 相手に送信したい情報（平文）のハッシュを作成する。（SHA-2 を利用）
- (2) 作成したハッシュの内容を自分の(RSA 暗号の)秘密鍵で暗号化する（これが電子署名となる）
- (3) 平文と電子署名のペアを相手に送る

電子署名の検証

受け取った側の検証手順は次のようになります。

- (1) 相手の公開鍵を入手する
- (2) その公開鍵で送付された電子署名を復号化する
- (3) 送付された平文から、相手と同じアルゴリズムを用いてハッシュを作成する
- (4) (2) の結果と (3) で作成したハッシュを比較する

2 つの値を比較した結果、両者が一致すれば送り手が署名してから受け手が署名を検証するまでの間にその文書が改ざんされていないことが検証されたことになります。

公開鍵と秘密鍵の持ち主は誰か？

公開鍵と電子証明書

公開鍵はだれが入手してもよく、どんな方法で相手に渡してもかまわないのです。では、公開鍵を受け取った人は、どのような方法でその持ち主を確かめるのでしょうか？

公開鍵の持ち主（＝その公開鍵に対応した秘密鍵の持ち主）を証明するものとして「電子証明書」というものが存在し、その証明書を発行する機関を「認証局」という。A さんの公開鍵を受け取ったら（実際には証明書の中に公開鍵が含まれた形になっている）、証明書の内容に不備がないか、そしてその証明書を発行した認証局が信頼できる認証局かどうかで確認するということになるのですが、認証局による身元調査の確実性はどの程度なのでしょう？

身元調査の仕方にはいろいろあります。個人なら戸籍謄本、職場での素行調査、資産調査、生育暦に沿った経歴調査、指紋や DNA での確認、兄弟や親との DNA 比較などです。

犯罪ですが、戸籍を買うこともできますので、本人確認はかなり難しいことになります。どこまでやるかで費用もだいぶ違ってきます。日本の戸籍を持っていた外国のスパイの例もあります。買い取った戸籍に記載された人物として普通に仕事や生活をしていたら、本来の戸籍の持ち主の指紋でもない限り、嘘を見破ることはできません。生まれたときに全員の指紋と DNA を登録させれば判別できるようになります。

したがって、証明書の効力についても、しっかり考える必要があります。

”メールもビットマ”では、知り合いや信頼できる相手との通信を想定していますので、本人確認の電子証明書は扱いません。外部に対して、情報が漏れるのを防ぐことと、改ざんの防止、に焦点をあてて電子署名を扱います。

最初は、鍵作成ソフトの機能から説明します。

これは、"CFRSAEC.exe","CFRSADC.exe"で使う暗号化、復号化の鍵を作成します。



操作について

1. 鍵のビット数

あなたがお使いのコンピュータばかりではなく相手の使用しているコンピュータの計算能力を考慮する必要があります。長い鍵ではメモリーの量が問題になります。鍵を作るための時間ほどではありませんが、暗号化、復号化にも時間がかかります。

ですが、相手に合わせて何種類も作成すると区別するのが大変になります。その場合は鍵交換用のシステムを利用してください。

2. 鍵を作る をクリックしてしばらくお待ちください。

3. 暗号化と復号化のテスト これをクリックすると暗号化、復号化が連続して行われます。

表示できるのはテキストファイルです。暗号化したものは16進数で表示されます。

4. 暗号化 暗号化の過程を表示しながら暗号化します。

5. 暗号化非表示 暗号化の過程を表示しないで暗号化を実行します。

6. 復号化 復号化の過程を表示しながら復号化します。

7. 復号化非表示 復号化の過程を表示しないで復号化します。

8. (公開) 暗号化鍵読込 暗号化に使う公開鍵を読み込みます。

これが、読み込んであれば、暗号化、暗号化非表示 ができます。

9. (秘密) 復号化鍵読込 復号化に使う秘密鍵を読み込みます。

これが、読み込んであれば、復号化、復号化非表示 ができます。

この鍵作成ソフトだけで処理する場合は、次のようになります。

あなた（アリス）が相手（ボブ）に、対称鍵暗号（秘密鍵暗号）で使う暗号化の鍵を送りたいときは次の手順になります。

1. 相手に送る秘密鍵作成します。この鍵作成ソフトと同一のフォルダに置いてください。
2. ボブに、**RSA** で使う鍵を作成してもらい、公開鍵をメールの添付ファイルとして送ってもらいます。この公開鍵は秘密にする必要はありません。
3. 受け取った公開鍵のファイルを、同一フォルダの置いてください。
4. （公開）暗号化鍵読込 をクリックして、受け取った公開鍵を登録します。
5. 平文 の所のファイル名を鍵ファイルの名前にしてください。たとえば、"eckey.bin"とします。
6. 暗文 の所にファイル名は必ず異なる名前にしてください、たとえば、"eckey2.bin"などです。
7. これを、相手に普通のメールソフトを使って添付ファイルとして送信します。そのとき、相手に、本来のファイル名を伝えること、復号化は使っている公開鍵のファイルに対応した秘密鍵を使って実行するように依頼してください。
8. 相手（ボブ）に、メール用のシステムでの、アドレス帳におけるあなたの項目において、復号化した鍵を登録してくれるように依頼します。

対称鍵（共通鍵）が5種類あるときは面倒になりますので、鍵交換用のフォルダを作って鍵交換専用のシステムを作って利用するほうが便利です。

注意：

鍵のセットを作成したらどの鍵がセットになっているかを間違えないようにしてください。作成した暗号化鍵を相手に送ります。秘密鍵を他人に知られてはいけません。相手から、公開鍵を受け取ったらそれを使って共通鍵を暗号化します。暗号化した共通鍵を相手におくります。公開鍵が誰から送られてきた公開鍵かが分からないと大変です。自分の公開鍵で暗号化されて送られてきた共通鍵は、公開鍵とセットに秘密鍵で復号化します。相手に合わせて公開鍵と秘密鍵のセットを作る場合はセットの管理にご注意ください。鍵交換用のフォルダを作り、鍵交換専用のシステムでの管理を薦めます。

まとめ：

1. 暗号通信の送受信者がそれぞれ公開鍵暗号 **RSA** での公開鍵を作成し、相手にそれぞれ送ります。
2. それぞれが、対称鍵による暗号化アルゴリズムを決定しその暗号化鍵のファイルを作成します。
3. 1で受け取った公開鍵で、暗号化鍵ファイルを暗号化して相手に送ります。
4. 3で受けとったファイルを復号化して、暗号化ソフトとセットにしてアドレス帳に登録します。

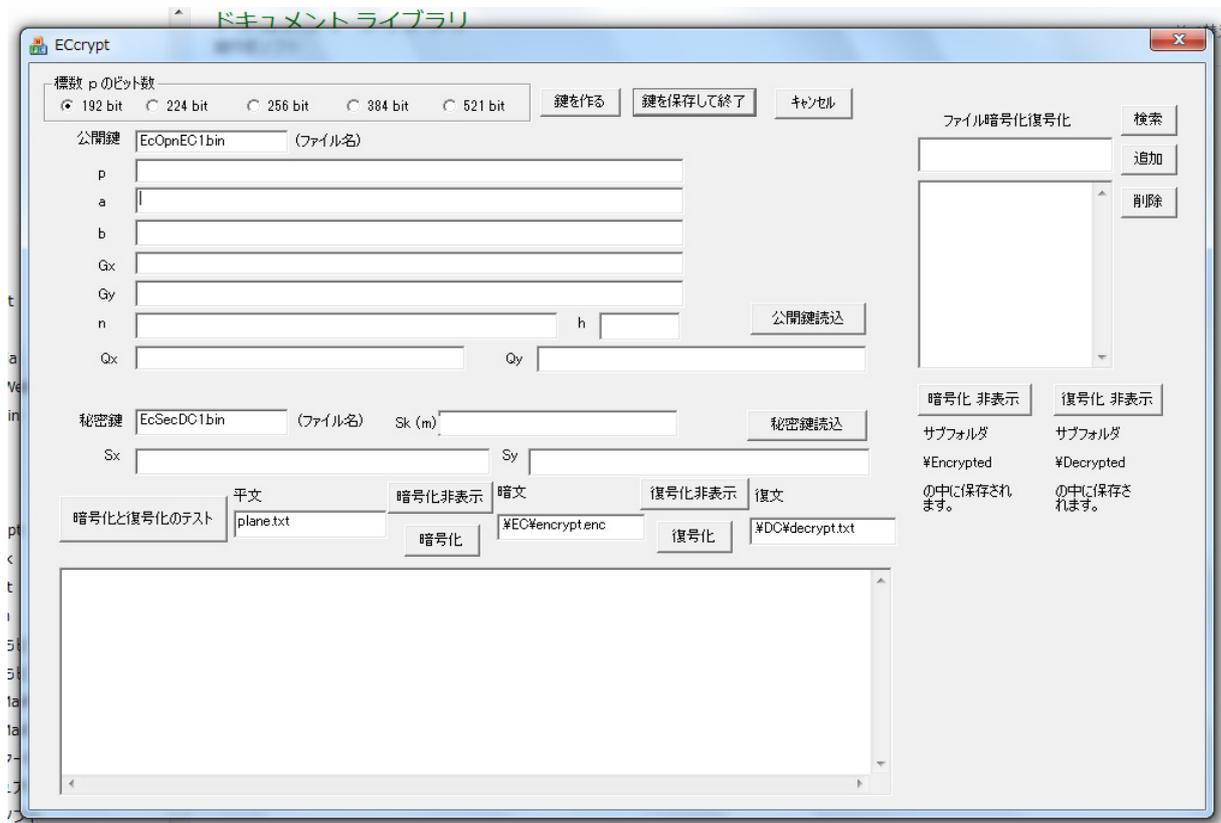
鍵交換用のフォルダを作って鍵交換専用のシステムを作って利用する場合。

1. 鍵交換用 というフォルダを作り、その中に“ATMailSys”をコピーします。
2. お互いに、“CFRSAKey.exe” を使って、それぞれが公開鍵と秘密鍵を作成します。
3. アリスが作成した公開鍵を“AOpenkey.bin”、秘密鍵を“ASeckey.bin”。
ボブが作成した公開鍵を“BOpenkey.bin”、秘密鍵を“BSeckey.bin”。とします。
4. アリスは、ボブから公開鍵を受け取ります。これは秘密にする必要がないので普通のメールに添付してかまいません。ボブもアリスからの公開鍵を受け取ります。
5. アリスは、“鍵交換用”フォルダにある、“暗号通信”のアドレス帳のボブの項目の暗号化ソフトの部分に、“CFRSAEC.exe”を登録します。暗号化鍵の部分には、ボブから受け取った“BOpenkey.bin”を登録します。これで、ボブから受け取った公開鍵で暗号化したデータをボブに送信できます。
復号化ソフトの部分には、“CFRSADC.exe”を登録します。この復号化で利用する鍵は、“ASeckey.bin”です。
6. ボブは、“鍵交換用”フォルダにある、“メールもビトマ”のアドレス帳のアリスの項目の暗号化ソフトの部分に、“CFRSAEC.exe”を登録します。暗号化鍵の部分には、アリスから受け取った“AOpenkey.bin”を登録します。これで、アリスから受け取った公開鍵で暗号化したデータをアリスに送信できます。
復号化ソフトの部分には、“CFRSADC.exe”を登録します。この復号化で利用する鍵は、“BSeckey.bin”です。
7. この設定によって、メールの文章、添付ファイルともに、RSA 暗号で暗号化されます。ただし、変換に時間がかかるので、データは最小にしてください。
添付するのは鍵のファイルのみ。文面は、使用する暗号方式と順序、対応する鍵の名前のみにしてください。
8. 鍵交換用のシステムで受け取った場合は、そのまま復号化できます。
9. ほかのメールソフトで受け取った場合は、添付ファイルを適当なフォルダに移動し、鍵交換用システムでのツールの復号化で復元できます。
10. 受け取った対称鍵（秘密鍵）をメール用のほうに移動してから、そちらで設定してから利用してください。

いくつかの公開鍵と秘密鍵のセットを利用する場合は鍵交換用のほうに登録しておくほうが便利です。

2.8 楕円曲線暗号を使った対称鍵の交換

ECCrypt.exe を起動すると次のようになります。



通信の仕方は次のようになります。

アリスの作業

1. 素数 p のビット数を決定する。192,244,256,384,521 ビットから選ぶ。
2. 鍵を作る ボタンをクリックする。
3. 公開鍵、秘密鍵の名前、 Ao^{***} , As^{***} を決める。
4. 鍵を保存して終了する。

注意：

現在は、素数のビット数を選ぶと、楕円曲線のパラメータ $T = (p, a, b, G, n, h)$ が1組決まります。秘密の値 m は乱数として決定されます。 m の値は、113 ビットから 392 ビットの間を設定しました。

この値 m は秘密にしておきます。

5. 相手 (ボブ) に、 (T, mG) を送る。(これが公開鍵)

ボブの作業

1. アリスから送られた公開鍵を読み込む。これで素数 p のビット数が決まる。
2. 鍵を作る ボタンをクリックする。
3. 公開鍵、秘密鍵の名前、 Bo^{***} , Bs^{***} を決める。
4. 鍵を保存して終了する。
5. アリスの公開鍵を読み込む。自分(ボブ)の秘密鍵を読み込む。

6. ECcrypt.exe と同じフォルダに対称鍵をおく。
7. 暗号化する対称鍵の名前を、平文のところに設定する。
8. 暗文、復文の名前も設定する。
9. 暗号化のボタンをクリックする。
10. 暗号化された対称鍵をアリスに送る。

アリスの作業

1. ボブから送られてきた暗号化された鍵を暗文のところにセットする。
2. 自分（アリス）の秘密鍵を読み込む。
3. 復号化のボタンをクリックする。
4. 復文の作成し、メールもビットマで利用する。

以上です。

ECcrypt のソースコードについては、著作権を主張します。

このソフトは、楕円曲線暗号の公開鍵と秘密鍵を作成し、暗号化、復号化の様子を確認するためのソフトです。暗号化したものは、16進数の列として表示します。

楕円曲線暗号での暗号化の仕組みは次のようになります。

アリスの作業

1. 楕円曲線のパラメータ $T = (p, a, b, G, n, h)$ を選ぶ。
2. 秘密の値 m を選ぶ。(これは秘密にしておく)
3. 相手 (ボブ) に、 (T, mG) を送る。(これが公開鍵)

(T, mG) を使って行われる、ボブの作業での、プログラムの動作

4. ファイル全体を分割する。
5. 分割した各部分を数値 $X1$ とみなす。
6. 整数値 $X1 + \alpha$ に対して、 $P = (X1 + \alpha, Y)$ が楕円曲線の上に乗るようにする。
7. 秘密の値 k を決める。
8. kG を作り、ファイルの先頭に置く。
9. アリスから受け取った、 (T, mG) を利用して、 $P + kmG$ を計算してファイルに書き込む。
10. ファイルの終わりまで繰り返し終了したら、それをアリスに送る。

アリスの作業でのプログラムの動き

- 1.1. ファイルの先頭から、 kG を取り出す。
- 1.2. 自分の持っている値 m を使って、 mkG を計算する。
- 1.3. ファイルの残りの各ブロックに対して、 $(P + kmG) - mkG = P$ を計算する。
- 1.4. P の x 座標 $(X1 + \alpha)$ を取りだして、 $X1 = (X1 + \alpha) - \alpha$ を計算して並べる。

これらの計算で、必要となるものは

1. 多倍長整数の計算
2. ヤコビ記号の計算
3. 平方根の計算
4. 楕円曲線上の点の k 倍の計算

です。

RSA 暗号を作るときに作成したものを少し変改し、さらに新しい関数を少し追加しました。

これは、楕円曲線暗号を利用した公開鍵暗号のソフトで、“メールもビトマ”、“Cipher Web Mail”における共通鍵の交換のために作成しました。パラメーターに関しては、

Standards for Efficient Cryptography
SEC 2: Recommended Elliptic Curve Domain Parameters
Certicom Research
Contact: Daniel R. L. Brown (dbrown@certicom.com)
January 27, 2010

にある値を利用しました。

GF_p での p の値は、192 ビットから、521 ビットの間です。 k および m の値は、113 ビットから 392 ビットの間を設定しました。

ファイル全体を暗号化出来ますが、とても時間がかかります。RSA 暗号が速く見えるほどです。したがって、対称鍵の暗号化にしか利用できません。もちろん貿易管理令に違反しないようにソースコードを HP で公開します。

多倍長整数の計算は、複素数の配列と多倍長整数の変換を適宜行う方法で全体を扱っています。さらに、3通りの乗法（複素数の普通の乗法、DFTによる乗法、FFTによる乗法）を用意して、扱う数の大きさによって切り替えて計算しています。除法と剰余は自分で考えた方法で計算しています。

ヤコビ記号の計算と平方根の計算、素数生成、最大公約数と逆数の計算は Menezes の Handbook of Applied Cryptography (Discrete Mathematics and Its Applications) にあった方法を少し変形して使っています。べき乗計算は FFT を主に利用しています。

全体的な流れは、

Journal of Applied Sciences 5 (4): 604-633, 2005
ISSN 1812-5654
© 2005 Asian Network for Scientific Information

Theory and Implementation of Elliptic Curve Cryptography

Kefa Rabah

Department of Physics, Eastern Mediterranean University, Gazimagusa, North Cyprus, via Mersin 10, Turkey

に沿って作成しました。ご指導いただいたことを感謝しております。

このソースコードについては、著作権を主張します。技術内容を公知の技術にするために、HP でソースファイルを公開します。

2.9 暗号ソフト、暗号鍵の変更について

しばらく使ってから、暗号ソフトを変更したり暗号化鍵を変更したりすると、それ以前に送受信したデータが読めなくなります。

どの鍵を使っていたかは、すぐ忘れてしまいます。変更する直前に使っていた、メールボックス、アドレス帳、暗号化ソフト、暗号化鍵、復号化ソフト、復号化鍵をセットにして、日付を付けたフォルダにそれらのコピーを保存しておけば、また見ることができます。メールボックスは、サブフォルダ (mailbox) の中に入っています。アドレス帳は、サブフォルダ (address) の中に入っています。見なくなったら、保存したものを元の場所に戻せば見ることができます。

元の場所に戻すときは、新しいアドレス帳と新しいメールボックスを上書きで無くさないように十分注意してください。

変更後に送受信したデータは読めますが、変更前の受信データや送信データが読めなくなります。また、ハングアップの原因にもなります。最初に、なるべく慎重に設定してください。

変更は、送受信する相手ごとにお互いに確認しあいながら同時に変更する必要があります。お互いの設定にずれがあると、復号化ができなくなります。

あるいは、全体をフォルダごとコピーして、それを圧縮して保存しておくのが簡単かもしれません。

2.10 暗号化鍵、復号化鍵の USB メモリーへの保管

暗号通信では暗号化 2 段階、復号化 5 段階の設定になります。

暗号化鍵の保存先のフォルダを指定できます。これを USB のドライブ内のフォルダに指定すれば、暗号化鍵、復号化鍵を USB メモリーなどに保管して普段は別の場所にしまっておけます。USB メモリーが無ければメールを読むことができなくなります。USB メモリーのドライブ名は挿入される場所で変わりますので同じ場所に挿してください。この場合は次のように設定します。

A さんのコンピュータで、USB が F ドライブになっていて、USB メモリーの中に k というフォルダを作りそこに暗号化鍵を保管する場合は、

A さんのアドレス帳では、

名前	電子メールアドレス
B さん	bsan@xyz.co.jp

	暗号化ソフト	暗号化鍵
1	cmlEC.exe	f:¥k¥cmlkeyEC.bin
2	BmpEC.exe	f:¥k¥bmpkeyEC.bin
3		
4		
5		

	復号化ソフト	復号化鍵
1	MistyDC.exe	f:¥k¥mistykeydc.bin
2	marsdc.exe	f:¥k¥marskeydc.bin
3		
4		
5		

とします。通信相手ごとにフォルダを作成し分類して鍵を保管することもできます。

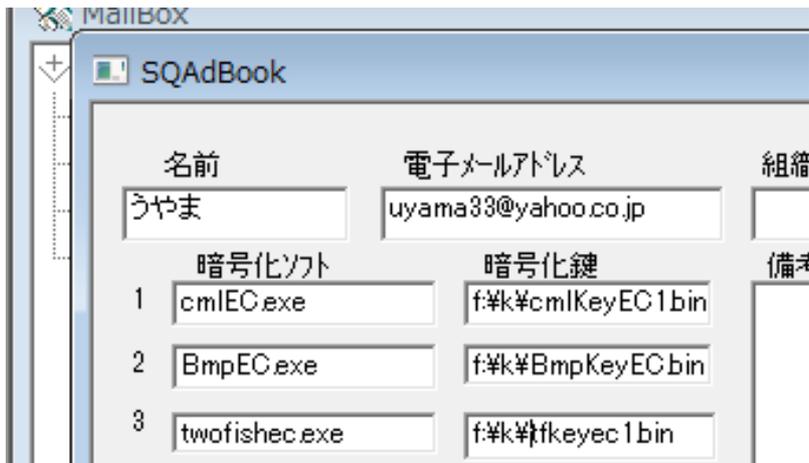
B さんのほうは、USB が G ドライブになっていて、その中にフォルダ r をつくりその中に鍵ファイルを保管するとします。

B さんのアドレス帳では、

名前	電子メールアドレス
A さん	asan@pqr.com

	暗号化ソフト	暗号化鍵
1	MistyEC.exe	g:¥r¥mistykeyec.bin
2	marsEC.exe	g:¥r¥marskeyec.bin
3		
4		
5		

	復号化ソフト	復号化鍵
1	cmlDC.exe	g:¥r¥cmlkeyDC.bin
2	BmpDC.exe	g:¥r¥bmpkeyDC.bin
3		
4		



これで、鍵ファイルの入った **USB** が正しいドライブに挿入されていない場合は暗号化や復号化はできなくなります。受信したメールも読めません。

3. 初期設定

3.1 解凍

ATMailPac.zip を解凍すると、このマニュアルの他に、

ATMailSys.zip
暗号ソフト.zip
鍵の見本.zip
鍵作成ソフト.zip

が現れます。さらに、ATMailSys.zip を解凍すると、“ATMailSys” 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“ATMailJ.exe”へのショートカットを作成してください。なお、このフォルダには、暗号化ソフト、復号化ソフト、暗号鍵のサンプルが全て入っています。

ATMailSys.zip：この中に最初からあるフォルダ、ファイルは決して削除しないでください。

暗号ソフト.zip：ここでは、暗号化ソフト（EC）と復号化ソフト（DC）が入っています。

鍵の見本.zip：暗号化鍵と復号化鍵の見本が入っています。

鍵作成ソフト.zip：暗号化鍵と復号化鍵を作成するソフトです。処理速度の確認もできます。

“ATMailJ.exe”の起動後に、SMTP、POP サーバーの設定をします。

3.2 初期設定する項目

デスクトップのアイコンをダブルクリックします。最初にユーザーID とキーの整合性を確認するダイアログボックスが現れます。文字の変更は可能ですが、変更すると暗号化の機能が失われます。表示される文字を見て確認したら OK ボタンをクリックしてください。

起動したら、いくつかの初期設定をします。初期設定は最初に1回すれば、その後は設定の必要はありません。

ここでは、ソネットの会員で、taro@aa2.so-net.ne.jp のメールアドレスを持っている人の場合で説明します。

メニューバーの設定をクリックしてください。

(1) SMTPHost 設定

(1-1) SMTP-AUTH の場合

設定 — SMTPHost 設定 を選んで、各項目を設定します。

項目：送信メール (SMTP) (SMTP-AUTH) サーバー には、パソコンから送信したメールを受け取るプロバイダーの

(SMTP-AUTH)サーバーの名前 smtp-auth.aa2.so-net.ne.jp となります。

項目：電子メールアドレス には、あなたのメールアドレスを記入してください。
taro@aa2.so-net.ne.jp となります。

項目：試行回数 は、メールの送信を試みる回数です。 1 で十分でしょう。

項目：Port 番号 は、587 としてください。

項目：お名前（発信者）はあなたのお名前を記入してください。

最後に、OK ボタンを押すと、この設定が有効となり、変更するまではそのまま使えます。

(1-2) SMTP の場合

設定 — SMTPHost 設定 を選んで、各項目を設定します。

項目：送信メール (SMTP) サーバー には、パソコンから送信したメールを受け取るプロバイダーの

(SMTP)サーバーの名前 **mail.aa2.so-net.ne.jp** となります。

他のプロバイダーでは、**aa2.so-net.ne.jp** のような形の場合もあります。

項目：電子メールアドレス には、あなたのメールアドレスを記入してください。

taro@aa2.so-net.ne.jp となります。

項目：試行回数 は、メールの送信を試みる回数です。 1 で十分でしょう。

項目：Port 番号 は、25 にしてください。

項目：お名前 (発信者) はあなたのお名前を記入してください。

最後に、OK ボタンを押すと、この設定が有効となり、変更するまではそのまま使えます。

プロバイダーからもらったメールアドレスで、自分のプロバイダーのサーバーに接続する場合には 25 番ポートが使えるようになっていたりするところもあります。

@nifty、ASAHI ネット、So-net、ODN、Plala、BIGLOBE(au ひかりを使わない)、OCN、Yahoo! BB Tikitiki などは、上記の条件でならば接続できます。

ただし、この接続方式は古いので、接続できないプロバイダーの場合も考えられます。

その場合は、SMTP-AUTH で接続してください。

(2) SMTPHost 解除

これを選択すると、今までの設定が解除されます。設定するには再度 (1) の設定で OK ボタンを押してください。

(3) SMTPHost 表示

設定内容が表示されます。

(4) POP3 Server の設定

設定 — POP3 Server を選んで、各項目を設定します。

項目：受信メール(POP3)サーバ には、**pop.aa2.so-net.ne.jp** と書き入れます。

プロバイダーによっては、**aa22.so-net.ne.jp** のように@の右側となる場合もあります。

項目：メールサーバーのユーザー名 には、**taro** (@の左側) と書きます。

項目：メールサーバーのパスワード には、あなたがメールを取り出すときのパスワード

(**taro@aa2.so-net.ne.jp**に対応するメールパスワード) を記入します。

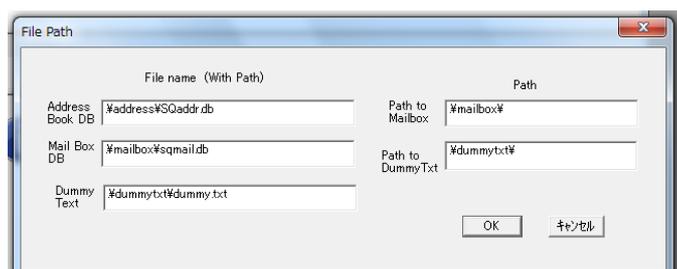
項目：メールをサーバーに残す は、メール受信のときに、受信の終わったメールを (POP) サーバーに残すか否かの設定で

す。ふだん他のメーラーも使うなら、**yes** にしてください。

最後に、OK ボタンを押してください。

(5) ファイルパス設定

サブフォルダを暗号化や復号化で利用していますので、このままで使ってください。



(6) EnCode 方式

Auto のままをお願いします。

(7) 途中経過報告

メーラーの動きを詳しく報告するメッセージを表示するかしないかです。好きなほうを選んでください。

(8) X-Mailer 項目

メールのヘッダー部分に記載される項目を長めに書くか、短くするかです。どちらでもかまいません。ここに記載された内容で、**BmpMailJ.exe** から送信されたものか否かを判断します。

(9) グループモード

グループモードのオン、オフや使用する暗号ソフト、暗号鍵を設定します。

メールアドレスの間違いによる情報漏洩を防ぐには、すべてのメールを暗号化してしまえばよい。そう考えてものがこのグループモードです。

設定—グループモードとして、グループモードのオン、オフや、グループモードで使う暗号化ソフト、暗号化鍵、復号化ソフト、復号化鍵を設定します。

グループモードがオンの場合は、送信するすべてのメールが、グループモードで設定された暗号化方式と暗号化鍵によって暗号化されて送信されます。

受信時では、受け取ったメールの発信者がこのソフトを使用していてしかも、自分のアドレス帳に登録されていれば、同じグループに属する人からのグループモードでのメールと見て復号化処理をします。アドレス帳に登録されていない場合や、他のメーラーで送信してきた場合には、暗号化されていないものとして扱い、復号化処理はおこないません。

本来の趣旨からすればこのモードは **off** にして、個別に暗号化の設定をするべきです。

(10) ダミー表示

他のメーラーで開いたときのように、ダミーテキストが表示されます。この設定は終了時点で解除されます。保存されませんので、必要ならば起動後に再度設定してください。

OFF の場合は、本来のメール本文が、復号化されてから表示されます。復号化のときに黒い窓が現れます。

(11) メールフィルター

メールフィルターが **ON** に設定されている場合は、アドレス帳に登録されていない人からのメールは全て迷惑メールとして扱われます。

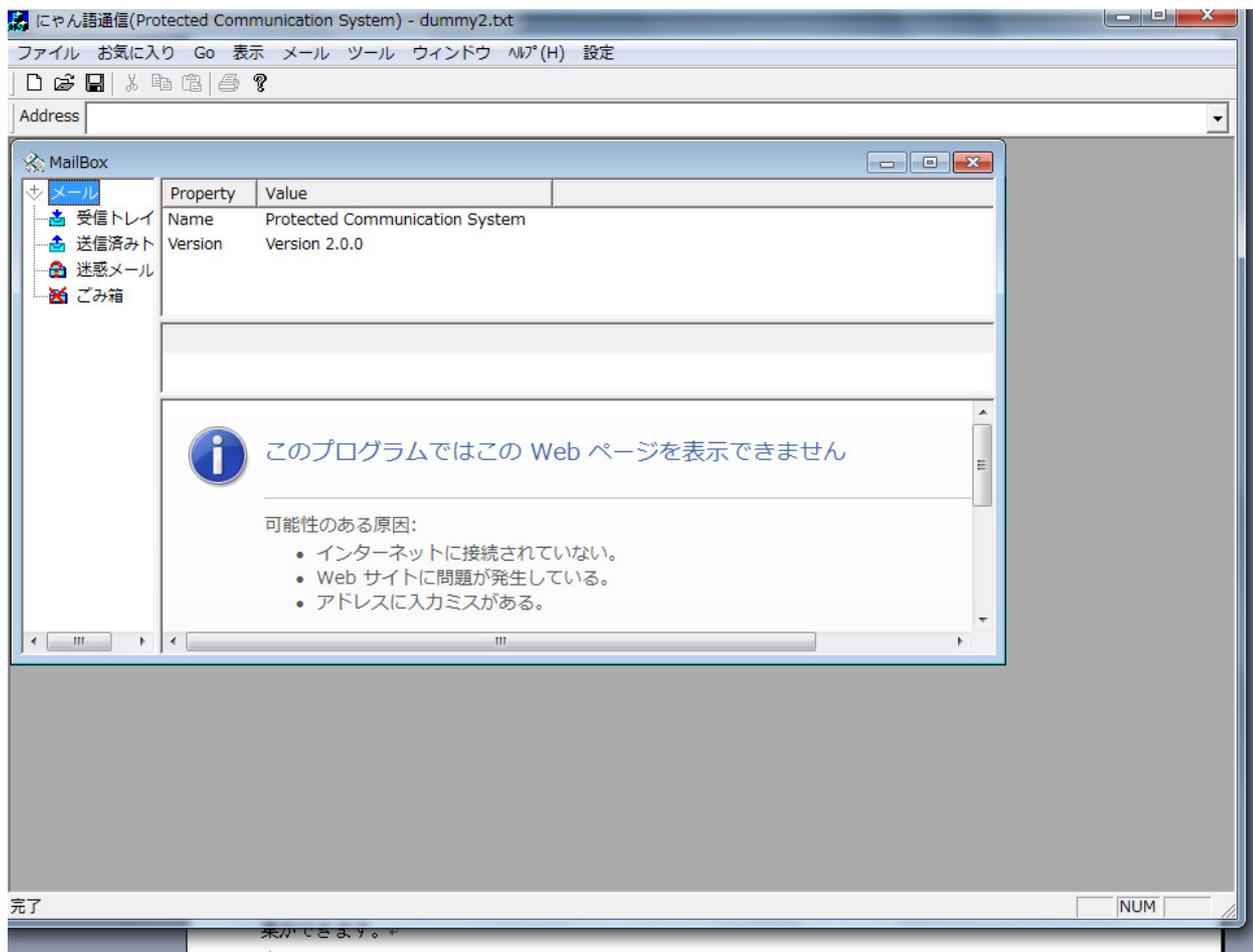
4. 操作の詳細

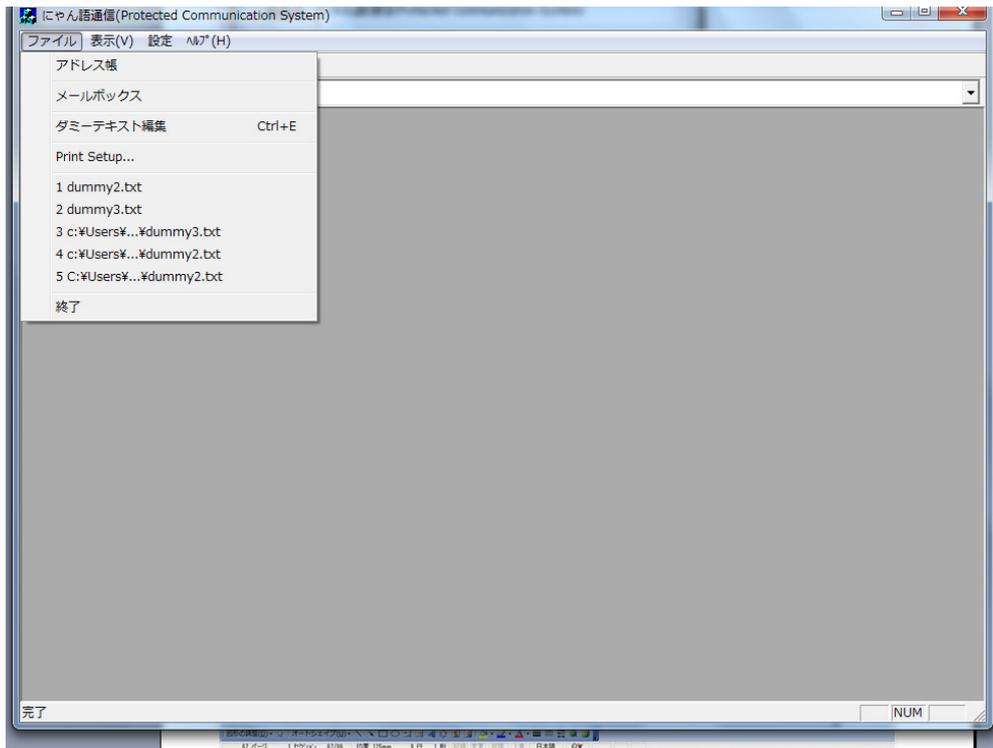
4.1 メイン画面

アイコンをダブルクリックするとユーザーIDを確認するダイアログボックスが現れます。ただ OK をクリックして下さい。



つぎに表示されるのは、メールボックスの画面です。このメールボックスを×で消せば基本画面が現れます。





上のほうにメニューが並びますので左から順に説明します。

4.1.1 ファイル

これをクリックするとアドレス帳、メールボックス、ダミーテキスト編集、Print Setup
ファイルの履歴一覧、Exit、を選択できます。

アドレス帳の項目をクリックすればアドレス帳が開き、メールアドレスの登録や暗号ソフト暗号鍵の登録や記録が残らない形のメールの送信ができます。

メールボックスをクリックするとメールボックスが開き、記録が残る形のメールの送信とメールの受信ができます。

ダミーテキスト編集をクリックすると、ユーザーがメール本文の代わりに送信されるダミーの文章を編集ができます。

Print Setup ではプリンターの設定ができます。

Exit をクリックすると、このプログラムを終了します。

4.1.2 表示

これをクリックすると、ツールバー、ステータスバーの項目が現れます。

ツールバーをクリックすると、画面の上のほうにあるツールバーが現れたり消えたりします。

ステータスバーをクリックすると、場面の下にあるステータスバーが現れたり消えたりします。

4.1.3 設定

これをクリックすると、このメーラーの初期設定ができます。これについては4の初期設定をご覧ください。

4.1.4 ヘルプ

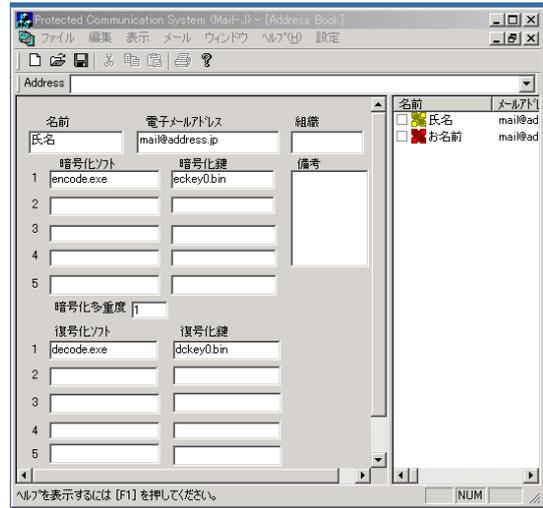
これをクリックするとヘルプトピックの検索とバージョン情報、特許申請の情報がご覧いただけます。

4.2 アドレス帳

暗号通信では暗号化2段階、復号化5段階の設定になります。

“ファイル” — アドレス帳 とすれば、アドレス帳が開きます。このアドレス帳は右側がアドレスの一覧で、左側に選択された人のデータが編集のために表示されます。

新規登録は、“編集” — “新規作成”として、新しく行を追加してください。その空の行をクリックしてから、左側の窓に移り、名前、メールアドレス、暗号化ソフトの名前、暗号化鍵のファイル名、復号化ソフトの名前、復号化鍵のファイル名、などを記入します。記入したら、“編集” — “編集結果登録”として、ください。編集結果が右側の行に反映されます。



暗号化機能を利用するとき、登録されていないとてはならない項目は、名前、メールアドレス、暗号化ソフトの名前、暗号化鍵のファイル名、の4項目です。

復号化機能を利用するとき、登録されていないとてはならない項目は、名前、メールアドレス、復号化ソフトの名前、復号化鍵のファイル名、の4項目です。

登録を削除するには、右側の窓で行を右クリックして、表示されるメッセージの指示に従って下さい。登録してあるものを編集しなおすときは、右側の窓で変更する行を左クリックして内容を左がわの窓に反映させてから、左側の窓で修正します。修正が完了したら “編集” — “編集結果登録” としてください。

特に注意するのは、暗号化と復号化の部分ですが、入手した暗号ソフトの暗号化部分のソフトと、暗号化で使う鍵を作成し、その鍵の暗号化で使うものを自分の通信相手に送ります。そして、相手の持っているソフトの暗号化の欄に登録してもらいます。

多重暗号化：

暗号化技術の発展は同時に解読技術の発展でもあります。これに対応するために多重暗号化を採用します。多重暗号化によって解読困難とする事が出来ます。このメーラーは送信する内容を異なる暗号ソフト、暗号化鍵を用いて5回まで多重暗号化できるようになっています。もちろん同じアルゴリズムと異なる鍵の組み合わせでの多重暗号化も可能です。

5回までの多重暗号化ですが、ビットマップにする暗号化を採用すると、データサイズが大きくなります。たとえば、5段階の暗号化で、2Mバイトのデータが5Mバイトのサイズになっていました。

米国での標準暗号(AES)や、ヨーロッパで採用された Camellia なども利用できますので、個人的な情報を守るには十分であると考えています。できるだけ最新の暗号化方式を組み合わせることをお勧めします。

多重暗号化では、

暗号化ソフトは送信するデータに対して、1, 2, 3, 4, 5の順で使われますが、

復号化では受信したデータに対して、5, 4, 3, 2, 1の順に使われます。

したがって、対応するソフトが同じ番号のところに設定されます。

これについては、(注意2)をご覧ください。

最後に、BmpEC.exeで暗号化された場合は、データの形式はビットマップ形式になっています。

ファイル名はもとのままです。したがって、ABC.docが元のデータで、多重暗号化の最後がBmpEC.exetとして送られてきたデータを他のメールソフトで受信して保存してから、拡張子をbmpに変更すれば図形としてみる事ができます。

このメールソフトで受信してそれを保存すると、保存の過程で復号化されて、本来のワードのデータになります。

送受信：

このメーラーを利用する上で、大切なことは送信者と受信者が暗号化に関して協調していることです。送信側で暗号化の設定をしているときは、受信側でも復号化の設定をして下さい。また、送信側で暗号化の設定をしていないときは、受信側でも復号化の設定をしないで下さい。

協調した形での設定がしてないと、暗号化されたものが復号化されなかったり、平文が復号化の操作を受けて読めなくなったりします。十分注意してください。

ここでは、強調した形での設定がしてある場合について説明します。

(1) 送信者側で暗号化の設定をし、受信者側で復号化の設定をしている場合

送信時にメール本文は暗号化された特別な添付ファイルとして送信されます。さらに、メール本文の代わりとして、**dummy.txt** の内容が平文として送信されます。本来の添付ファイルも暗号化されてから、添付ファイルとして同時に送信されます。

このメーラーで受信したときは、暗号化された本文は自動的に復号化されて表示されます。**dummy.txt** を表示することもできます。暗号化されて送信された本文や、添付ファイルは、添付ファイルの一覧として表示されます。保存するときに自動的に復号化されます。

本文を暗号化したものは、**mdata05.bin** という名前の添付ファイルです。

他のメーラーで受け取った時には、**dummy.txt** の内容が表示されます。メール本文は暗号化されたままの **mdata05.bin** という添付ファイルとして受信されます。本来の添付ファイルは暗号化されたままの添付ファイルとして受信されます。

(2) 両者ともに、暗号化の設定をしていない場合

メール本文が暗号化されないままで送信されます。本来の添付ファイルも暗号化されないままで送信されます。このメーラーで受信したときは本文が表示されます。本来の添付ファイルは、普通の添付ファイルとして受信されます。

注意 1：

通信時に使用する暗号化ソフトや復号化ソフトの特定はメールアドレスによって行いますので、このアドレス帳には同じメールアドレスを2つ以上登録してはいけません。同じ人が二つ以上のメールアドレスを持っている形の登録は可能で全く問題ありません。もちろん自分自身を登録して、自分宛に暗号メールを送信して確認することも可能です。

暗号ソフトで現在利用できるものは7種類です。このソフトの名前をアドレス帳に登録すれば暗号化の様子が確認出来ます。アドレス帳に自分自身の 名前、メールアドレス、暗号化ソフトの名前、暗号化鍵のファイル名、復号化ソフトの名前、復号化鍵のファイル名、を登録し自分に向けてメールを送信します。それを、このメールソフトで受信してみたり、他のメールソフトで受信してみたりすれば暗号化の様子が良く分かります。

お互いに、暗号化鍵、復号化鍵を作成し必要なものを相手に送り、それを使って、暗号化ソフト、復号化ソフト、暗号化鍵、復号化鍵の設定を正確に行ってください。

◎送信側と受信側で暗号化の設定がバラバラの場合には、通信エラーが起きます。

◎多重暗号化するときは、暗号化と復号化で順序が違っていると復号化できませんので、ご注意ください。1番と1番、2番と2番、のように、暗号化ソフトと復号化ソフトを対応させてください。

◎鍵の作成では鍵ファイルの名前に注意してください。別の鍵を作成するつもりで同じ名前のファイルを作って上書きしてしまうと、上書きされた鍵を使っていた暗号通信が出来なくなります。通信相手の名前とアルゴリズムなどを分かりやすく入れたものにして下さい。

注意 2 :

送信済みのメールの内容を見ないならば、自分が A さん、相手が B さんとしたとき、

A さんのアドレス帳では、

名前	電子メールアドレス
B さん	bsan@xyz.co.jp

	暗号化ソフト	暗号化鍵
1	cmlEC.exe	cmlkeyEC.bin
2	BmpEC.exe	bmpkeyEC.bin
3		
4		
5		

	復号化ソフト	復号化鍵
1	MistyDC.exe	mistykeydc.bin
2	marsdc.exe	marskeydc.bin
3		
4		
5		

となっていて、

B さんのアドレス帳では、

名前	電子メールアドレス
A さん	asan@pqr.com

	暗号化ソフト	暗号化鍵
1	MistyEC.exe	mistykeyec.bin
2	marsEC.exe	marskeyec.bin
3		
4		
5		

	復号化ソフト	復号化鍵
1	cmlDC.exe	cmlkeyDC.bin
2	BmpDC.exe	bmpkeyDC.bin
3		
4		
5		

これによって、A さんから、B さんあてに出されるメールは、暗号化ソフトの 1 によって、CmlEC.exe で暗号化されます。さらに、BmpEC.exe で 2 回目の暗号化がなされます。その後送信されます。

これを受け取った B さんのほうでは、A さんから来るデータは上のように暗号化されているので、A さんの項目の復号化部分が、番号の大きなものから適用されて、最初に BmpDC.exe で復号化されます。さらに、CmpDC.exe で復号化されます。これで、元に戻るなので、この復元されたデータがメールの内容として表示されます。

添付ファイルの場合も同様に暗号化に対応する復号化が行われて、B さんのパソコンに保存されることになります。

ですから、AさんがBさん宛てに送信したものを後で見る必要が無ければこれで十分です。

Aさんの送信済みトレイには、暗号化されて送信されたものが保存されています。

自分(A)がBさんに送ったメールは、自分の送信済みトレイに保存されるのですが、この内容は、データが最初はcmllec.exeで暗号化されて、次にbmppec.exeで暗号化されたものが保存されています。

その内容を見るには、bmpdc.exeで変換したものを、さらにcmldc.exeで変換しなくてはなりません。

自分のアドレス帳には、自分が送ったものを復号化するための復号化ソフトがありません。

もちろん、Bさんは、Aさんから来たデータを復号化するためのソフトを登録していますので、受信したデータを復元できます。これが、順序対方式での設定です。

どうしても、後で自分がBさん宛てに送信したデータの内容を見る必要がある場合には、次のように設定します。

Aさんのアドレス帳では、

名前	電子メールアドレス
Bさん	bsan@xyz.co.jp

	暗号化ソフト	暗号化鍵
1	cmlEC.exe	cmlkeyEC.bin
2	BmpEC.exe	bmpkeyEC.bin
3		
4		
5		

	復号化ソフト	復号化鍵
1	cmlDC.exe	cmlkeyDC.bin
2	BmpDC.exe	bmpkeyDC.bin
3		
4		
5		

として、さらに

Bさんのアドレス帳では、

名前	電子メールアドレス
Aさん	asan@pqr.com

	暗号化ソフト	暗号化鍵
1	cmlEC.exe	cmlkeyEC.bin
2	BmpEC.exe	bmpkeyEC.bin
3		
4		
5		

	復号化ソフト	復号化鍵
--	--------	------

1	cmlDC.exe	cmlkeyDC.bin
2	BmpDC.exe	bmpkeyDC.bin
3		
4		
5		

と設定し、順序対ごとに暗号化方式を設定するのではなく、集合{A,B}に対して暗号化方式を設定することになります。

こうすれば、Aさんから送られてきたデータをBさんが復号化して見ることもできるし、AさんがBさんに送ったデータを、後で確認することもできます。

送信済みトレイに保存されたデータに対して使われる復号化ソフトは、送信する相手の項目の、復号化の部分に登録されている内容が使われます。

Aさんが、Bさん宛てに送った物が送信済みトレイにある場合は、そのデータを復号化するときには、Aさんのアドレス帳における、Bさんの項目の中での復号化ソフト、復号化鍵が使用されます。

アドレス帳が開いたときに、現れるメニューを左から説明します。

4.2.1 ファイル

メールボックスをクリックするとメールボックスが開きメールの送受信が出ます。
閉じるをクリックするとアドレス帳が閉じます。
終了をクリックするとこのソフトが終了します。

4.2.2 編集

新規作成をクリックするとアドレスを追加するための空の行が右側の窓に追加されます。ここに記載するには、その空の行を右側の窓でクリックしてから、左の窓をクリックします。名前、メールアドレスなどの必要事項を記入します。

編集結果登録をクリックすると、左側の窓で記入した内容が登録されて右側の窓に反映されます。

4.2.3 アドレス帳の圧縮

これをクリックするとアドレス帳のデータベースの隙間を削除します。ただし、右側のリストのどれかをクリックしてから実行して下さい。

4.2.4 表示

これは、ツールバー、ステイタスバーの表示と非表示の切り替えです。

4.2.5 メール

新規をクリックするには、右側の窓で行を選択してからにしてください。編集—新規作成で作った空の行を選べばあて先は空欄になります。メールアドレスが記入された行を選べば宛先は選ばれた人のものが記入された新しいウインドウが開きます。これがメール送信用のウインドウです。件名、内容を記入してから、メール—送信を選べばメールが送信されます。暗号化の状況については、5基本構造と使い方をご覧ください。

4.2.6 ウインドウ

Cascade をクリックすると、多数の窓がずらして重ねた状態で表示されます。

Tile をクリックすると、窓がタイルを敷き詰めたような状態で表示されます。

複数の窓があるな場合には、下の部分をクリックするとフォーカスを持っている窓を切り替えることができます。

4.2.7 ヘルプ

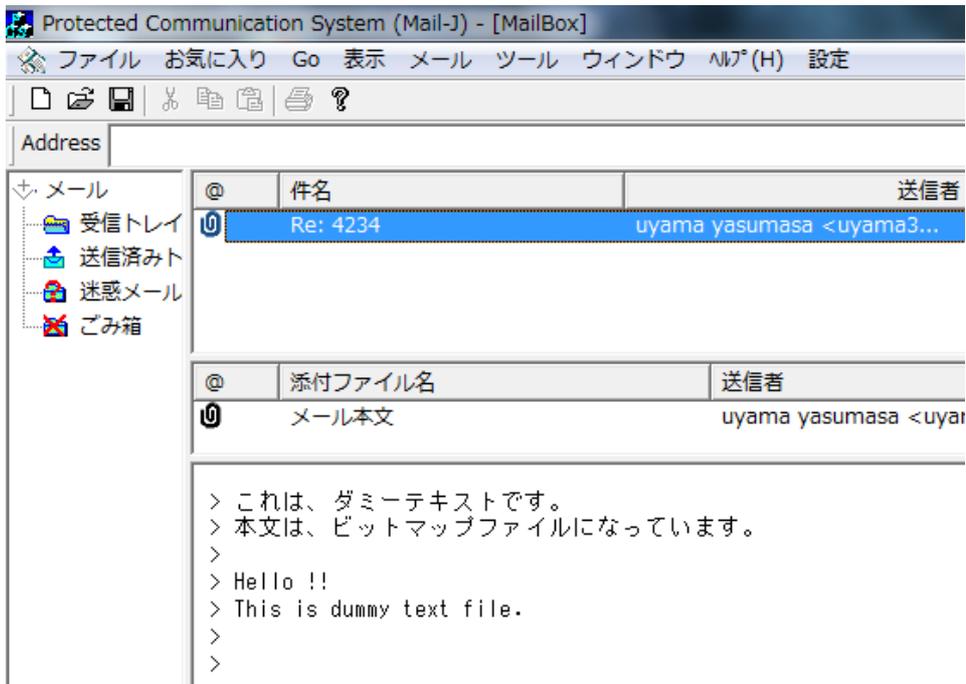
トピックの検索とバージョン情報が確認できます。

4.2.8 設定

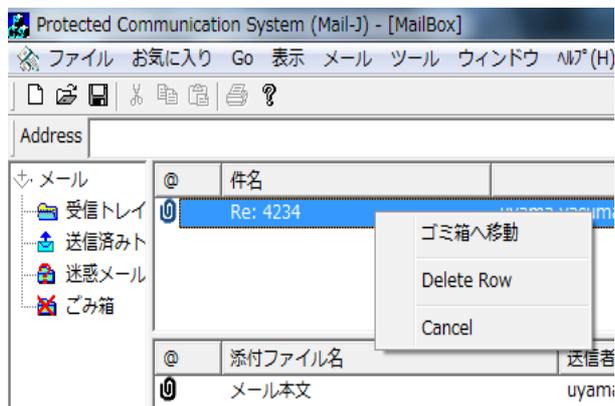
初期設定ができます。これについては4 初期設定をご覧ください。

4.3 メールボックス

メールボックスは3つの窓から構成されます。左の窓では 受信トレイ、送信済みトレイ、迷惑メール、ゴミ箱 の4つの項目があります。



受信トレイ： を選ぶと受信したメールの一覧が右上の窓に表示されます。表示されたメールの一覧から、1つを選んで左クリックすると右下の窓にはメールの内容が表示されます。右クリックすると、



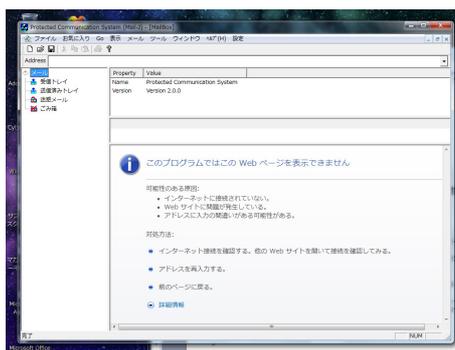
となり、ゴミ箱への移動、削除ができます。右の中央には、添付ファイルの一覧が表示されます。“メール本文”、“mdata05.bmp”以外のものが本来の添付ファイルです。それを、右クリックして保存を選べば、ファイルが自動的に復号化されてから保存されます

送信済みトレイ： を選ぶと送信済みのメールが表示されます。メールを選んで左クリックするとメールの内容が表示されます。右クリックすると、ゴミ箱への移動、削除ができます。

迷惑メール：を左クリックすると、迷惑メールと判断されたメールが表示されます。
この項目を右クリックすると一度にすべて削除することもできます。
それぞれのメールを右クリックすると受信トレイに戻すこともできます。
1つずつ削除することもできます。

ゴミ箱： の項目を左クリックするとゴミ箱の内容が表示されます。
項目を右クリックするとゴミ箱内のメールを一挙に削除出来ます。
復活出来なくなりますので、操作は慎重にしてください。
また、ゴミ箱内のメールを右クリックすると

メールは **SQLite** データベースとして保存されます。



4.3.1 ファイル

このメニューから表示されるサブメニューは、アドレス帳を開く、暗号 Web メール表示、メールボックスを閉じる、プリンターのセットアップをする、終了する、から構成されています。

4.3.2 編集

この項目は右上の窓に新しい行を加えたり、左側の窓で変更した内容を登録したり、編集対象となる行を変更したりできます。

4.3.3 お気に入り

このメニューを有効にするには、**Add List** をクリックします。すると、お使いのインターネットエクスプローラで、お気に入り に登録した内容が表示されます。再度クリックするとお気に入りに登録してある **URL** の内容を右下の窓に表示できます。右下に表示された **URL** の内容はインターネットエクスプローラと同様に操作できます。

4.3.4 Go

このメニューを有効にするには、お気に入り、**Add List** としてください。その後に **URL** 間の移動ができます。

4.3.5 表示

ツールバーやステータスバーの表示と非表示の他に、右下の窓をクリックしてある場合には表示する文字サイズの変更、再表示などができます。

4.3.6 メール

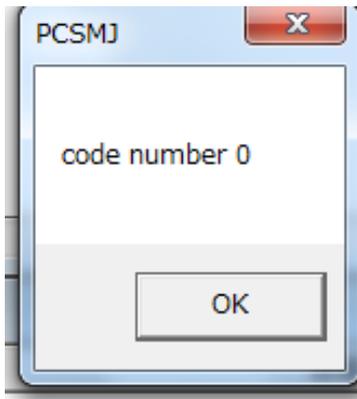
左の窓をクリックすると、メールの取り込みができます。

取り込みをクリックすると、メールが受信されます。自分当てに送信したものを他のメーラーで受信してみれば、暗号化の様子がはっきりと理解できます。

返信をクリックする前に、右上の窓でどのメールに対する返信なのかをマウスでクリックして指定してください。返信用のメールを書くための窓が開きます。宛先は自動的に記入されています。もちろんこの宛先を直接変更することも可能です。件名、内容を記載した後に再度“メール”をクリックして下さい。

“送信” をクリックするとメールと送信するためのダイアログボックスが現れます。現在、CC と BCC は使用できませんので必ず空欄にして下さい。

ファイルを添付して送信するには検索ボタンをクリックしてファイルを選んでください。最後に OK ボタンをクリックすればメールの送信が開始されます。暗号化のために少し時間がかかります。



最後に “code number 0” と書かれたメッセージが出たら終了です。

新規メール をクリックすると宛先が空欄のメール用の窓が開きます。

MailDB 圧縮 これをクリックするとメール用のデータベースの隙間を削除します。ただし右上のリストをクリックしてから実行して下さい。

4.3.7 暗号(クラウド)ツール

クラウドに関しては、次のような心配があります。

1. 従業員によるデータの盗み見

社員の一部は当然パスワードを知ることが業務上必然であり、また中身を見ることが必然の人がいるかもしれません。

通信教育大手「ベネッセホールディングス」(岡山市)の顧客情報漏えい事件で、元システムエンジニア(SE)、松崎正臣容疑者(39)が持ち出した顧客情報の転売に関わった東京都内の名簿業者の中に、ベネッセから流出した情報と知りながら取引をした。

ということもありました。

2. ルーチンワーク内での閲覧

データをクラウドで預かるサービス大手の会社でも、業務上データを見るのはやむを得ないと言っている会社もあります。そしてどうしても見られたくないというのであれば、自分で暗号化してから預けるようにとのことです。データ内容を機械的に検索すると公言している会社もあります。

3. 政府機関による監視・閲覧

米NSA(国家安全情報局)の社員だったスノーデン氏は、NSAのネット上での盗聴行為について次々と暴露しました。米国の大手IT企業のデータに比較的簡単にアクセスできる権限をNSAは持ち、実際にアクセスしていること。彼らの知らないところでも情報を勝手に傍受したり、勝手にアクセスしたりしていること。SSLは開発時にNSAが協力しており、バックドアが設けられていて、送金情報などが監視されていること。携帯電話の位置情報やメールも傍受していることなどがあり、AES暗号が総当たり攻撃で解読されているというニュースもありました。

4. IDとパスワードを盗まれて、ほかのPCから覗き見される。

太郎さんと花子さんは、昔お付き合いしていて分かれました。太郎さんは、密かに花子さんのIDとパスワードでログインし、電子メールやクラウドデータを静かに覗き見していましたとき。データに覗き見を加えない覗き見は見逃しがちです。

これらの心配を完全とは言えませんが、1,2についてはかなりの程度防御できると考えています。標準とされる暗号方式での多重暗号化を提供します。たとえ、AESが総当たり攻撃で1秒で解けたとしても、AES、カメリア、RSAなどで3段階の多重暗号化をすれば、総当たり攻撃には耐えられると思います。

クラウドでのデータ保存機能を利用されている方に、強力な暗号機能を提供します。このメールソフトは、順序対ごとに暗号化方式、暗号化鍵、多重度を設定できます。これをクラウドでのデータに適用すれば、次のことが可能となります。

1. 自分用に保存するデータを強力に多重暗号化できます。
2. 特定のグループの構成員だけが閲覧できるように設定できます。グループごとに設定できます。
3. 特定の個人だけが閲覧できるように設定できます。公開鍵暗号が利用できます。

これらについて、説明いたします。

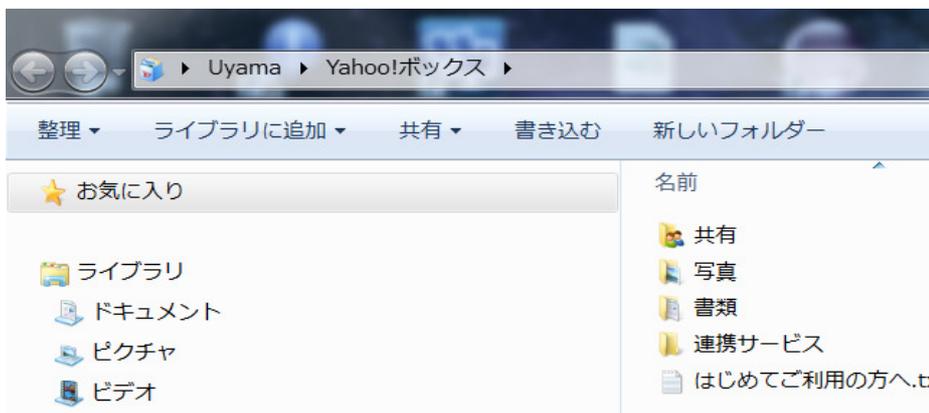
ヤフーボックスを導入するとします。



”ヤフーボックス”で検索して、上の画面で利用登録をクリックすれば、機能確認のスペースが確保できます。

見かけ上、自分のコンピュータの中にフォルダが出来ただけのように見えます。エクスプローラを使って、ファイルのドラッグやコピー、貼り付けなどが自由にできます。エクスプローラから扱えるので、自分のPC内のフォルダと見てプログラムを書くことが出来ます。しかしながら、ヤフーボックス内のデータはクラウド上に保存され自分のPC内には、関連を示すデータが保存されます。

導入したヤフーボックスをクリックすると、下の図のようになります。

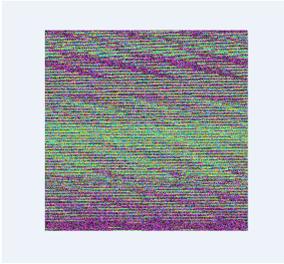


これらのフォルダにデータを移動させるときに暗号化をするのですが、**フォルダを選択するにはその中にあるファイルをクリックしなくてはならないので、サンプルピクチャを各フォルダに1つずつ配置してください。**

たとえば、PCでは猫の写真ですが、ビットマップファイルの場合には、画像としての暗号化ソフトを使えば



ヤフーボックスの中では、砂嵐のような画像（ビットマップファイル）になっています。



これは、**クラウド---復号化ダウンロード** によって元の猫の画像になって戻ってきます。
これを元に戻せるのは、復号化鍵をもっている人だけです。

最初に、作ったときの機能は、

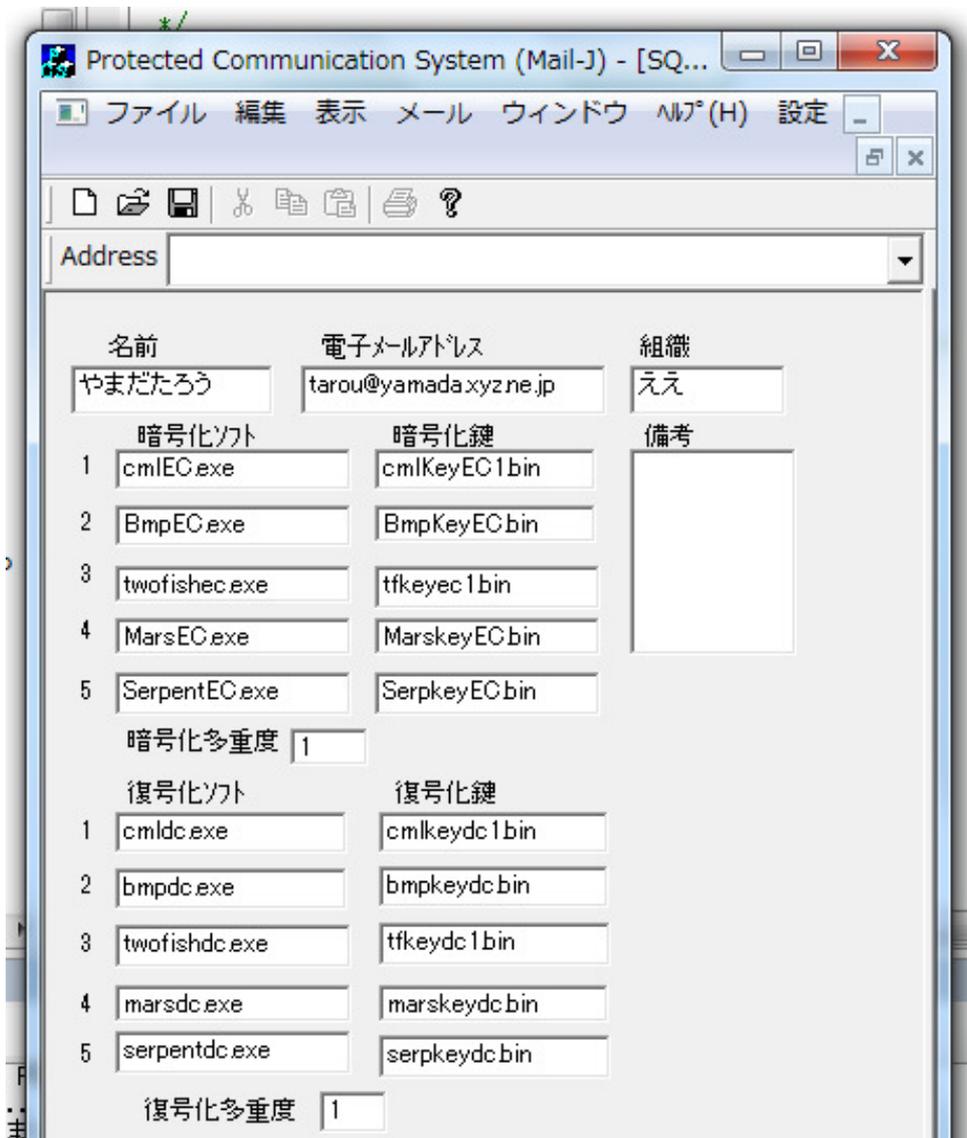
ある人から暗号化されたものが**Web**メールのアドレス宛に送られてきたときにその人用の復号化ソフトを使って暗号化された添付ファイルを復号化する機能です。復号化された結果は、標準では **WebDecrypt** というサブフォルダに保存されます。

ある人に暗号化したものを送るのにまとめて暗号化しその結果を確認してから、暗号化されたものを**Web**メールのアドレス宛に送ることができます。その人用の暗号化ソフトを使ってファイルを暗号化する機能です。暗号化された結果は、標準では **WebEncrypt** というサブフォルダに保存されます。
というものでしたが、それを改良して現在は、

クラウドにデータを預けるときに、暗号化しながら移すことができます。
この機能を、5段階の暗号化による強力な暗号化機能をもったクラウド暗号化ツールとして利用できます。

1. 暗号化(アップロード)

アドレス帳の自分の項目が下の図のように設定されているとします。



暗号化ソフト、暗号化鍵、復号化ソフト、復号化鍵の登録の様子をしっかりと確認してください。
この画面での、暗号ソフト、暗号鍵の登録は、大文字、小文字のどちらを使ってもかまいません。暗号化では、EC、復号化では、DCが入っているのが特徴です。

	暗号化ソフト	暗号化鍵
1	CmlEC.exe	CmlkeyEC1.bin
2	BmpEC.exe	BmpkeyEC.bin
3	TwofishEC.exe	TfkeyEC1.bin
4	MARSEC.exe	MarskeyEC.bin
5	SerpentEC.exe	SerpKeyEC.bin

	復号化ソフト	復号化鍵
1	CmlDC.exe	CmlkeyDC1.bin
2	BmpDC.exe	BmpkeyDC.bin
3	TwofishDC.exe	TfkeyDC1.bin
4	MARSDC.exe	MarskeyDC.bin
5	SerpentDC.exe	SerpKeyDC.bin

となっています。暗号化と復号化の対応関係に注意してください。

あなたのお名前が、やまだたろう、電子メールアドレスが、tarou@yamada.xyz.co.jp だったとします。

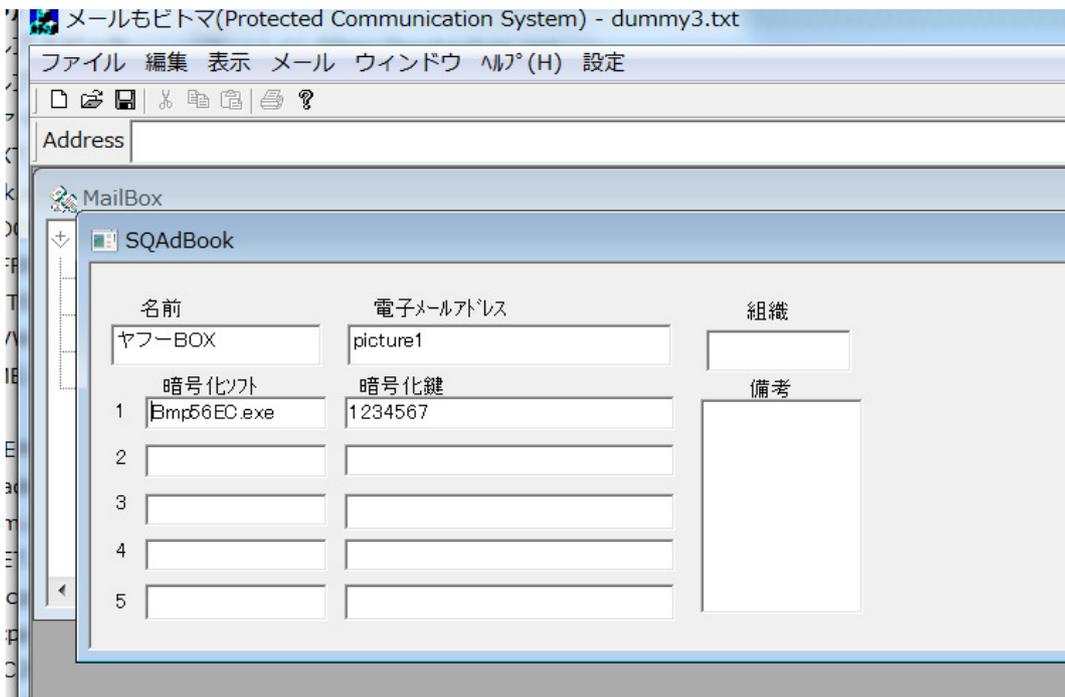
暗号(クラウド)ツールで暗号化(アップロード) を選択すると次の画面が現れます。

電子メールアドレスの項目 には、暗号化に利用する暗号化ソフトと暗号化鍵が登録されているあなたの**メールアドレス**を入力します。

クラウドでの利用では、メールアドレスの項目に入力してあるグループ名などを入力します。

たとえば、ヤフーボックスの写真のフォルダに写すときに使う暗号の設定がアドレス帳で電子メールアドレスの項目に、**picture1**と記入してあれば、**picture1** と入力します。

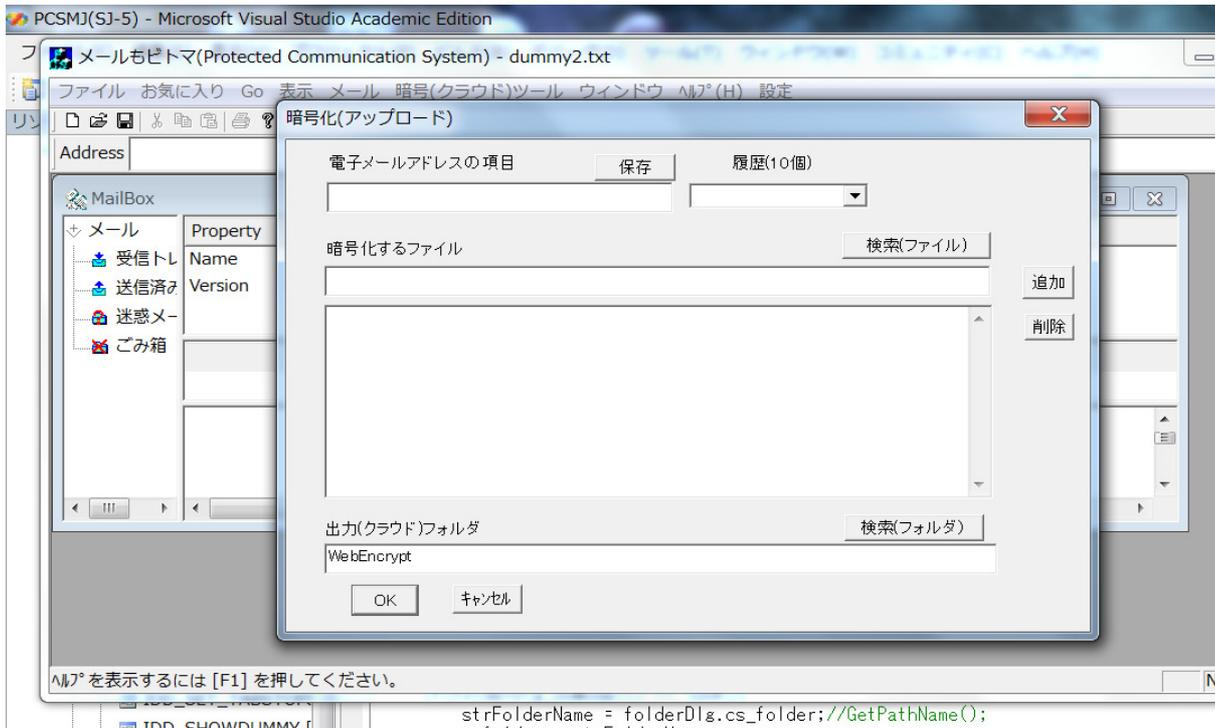
保存 ボタンをクリックすれば、入力したアドレスを10個まで保存することも出来ます。また、一度入力して保存したものは、履歴として残っていますので、履歴の所のドロップボックスの三角印で表示して、クリックすれば、選んだものが入されます。



次に、暗号化するファイルを選択します。

検索(ファイル) をクリックするとエクスプローラの画面からファイルを選択できます。

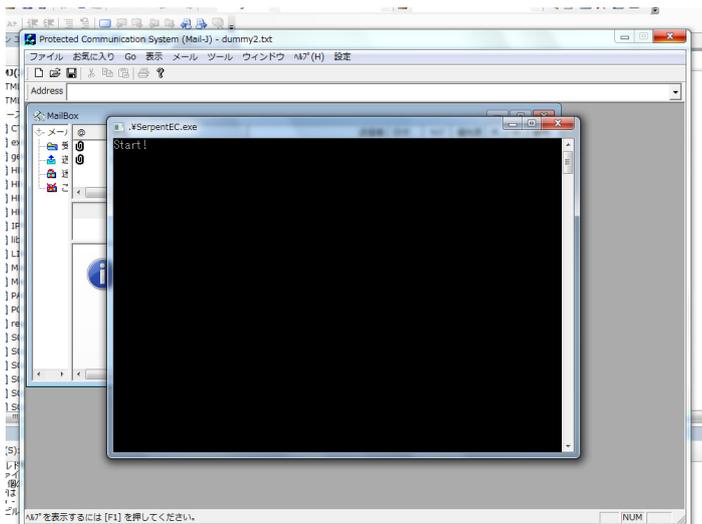
複数個のファイルを登録でき、同時に暗号化と移動が行われます。



つぎに、移動先のフォルダを決定します。検索(フォルダ)をクリックして、目的のフォルダの中にあるファイルをクリックしてから開くをクリックすると、そのファイルが入っているフォルダが選択されます。

そして、OK ボタンをクリックすれば、選択したファイルが暗号化されてから目的のフォルダに移ります。このとき、元のファイルは変更されません。削除もされません。コピーしたものに対して暗号化と移動が行われます。

ファイルサイズが大きいときは、変換途中での画面がしたの図のようになって現れる場合がありますので、そのときは、しばらくお待ちください。



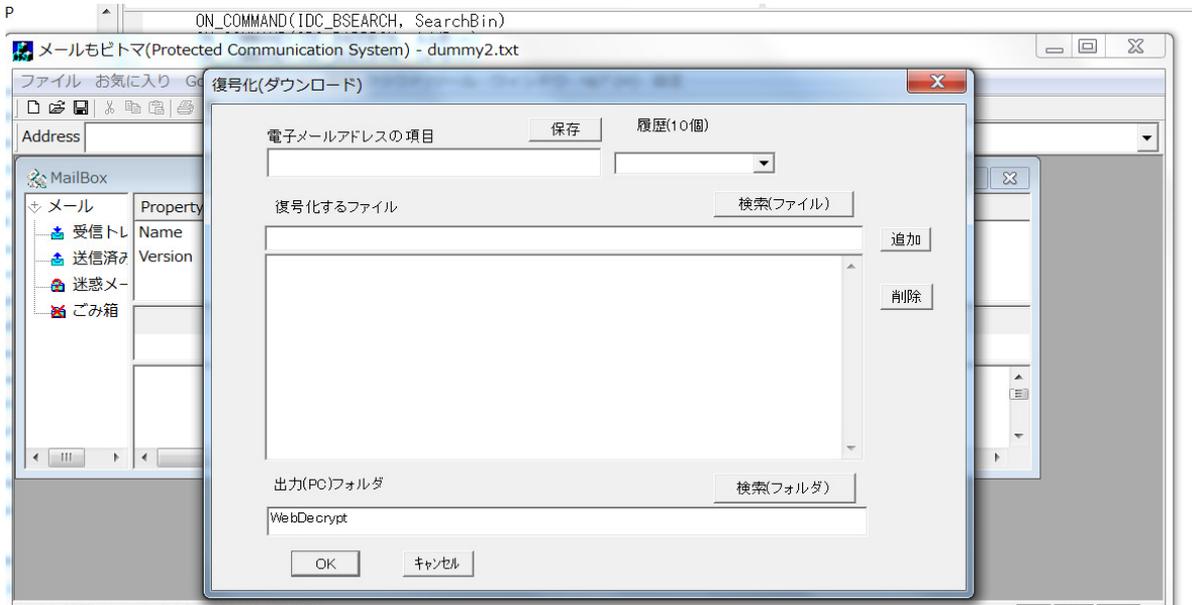
暗号化されたものは、指定されたサブフォルダの中に入ります。

(注意) 4 MB 程度のを暗号化すると、暗号化ソフトとして BmpEC.exe を利用すると 8 MB 程度の大きさになります。他の暗号化ソフトではサイズはほとんど変化しません。

2. 復号化(ダウンロード)

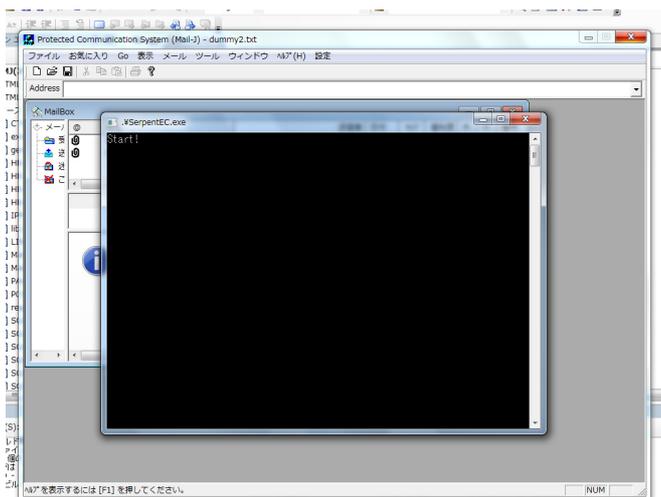
アドレス帳の自分の項目や、ヤフーBOX の所には、復号化が暗号化に対応する形で設定されていますので。

暗号(クラウド)ツール から 復号化(ダウンロード) を選び、



あなたのメールアドレス（または picture1）を入力し、復号化するデータを選択してから、OK ボタンをクリックすれば、サブフォルダ WebDecrypt の中に復号化されたものが現れます。

時間がかかるときは、復号化の途中で、次のような画面が現れます。



処理が終わるまでしばらくお待ちください。

8 MB のものが最初の 4 MB のデータに戻ります。BmpEC.exe を除けば、世界標準の暗号化方式による多重暗号化ですので、かなり強力のものとなっています。もちろん、本格運用では、暗号化鍵は新しく作ったものを使ってください。

クラウド上の複数のサブフォルダに対してそれぞれ異なった方式での暗号化を選択できます。

グループごとに暗号化を分けるときは、そのグループでの復号化鍵をグループの構成員に配布しておく必要があります。

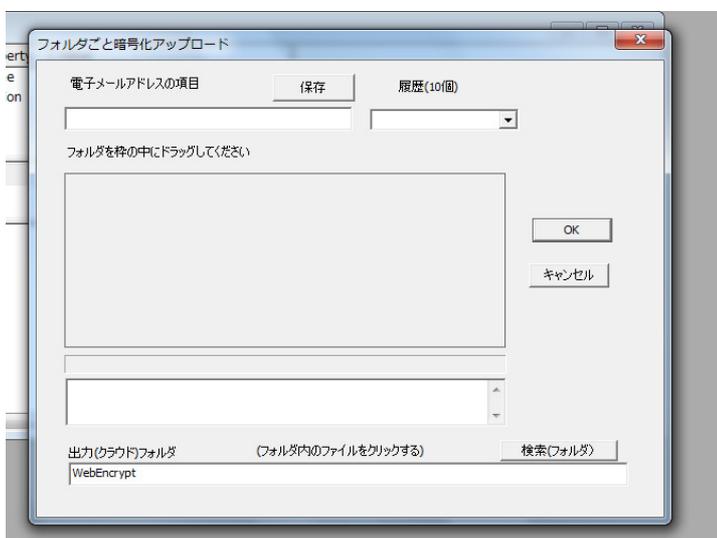
また、**RSA** 公開鍵暗号も利用できますので、特定の人から受け取った公開鍵で暗号化すれば、それに対応する秘密鍵を持っている人しか暗号化を解除できません。

3. フォルダ暗号化(アップロード)

選択したフォルダを1つのファイルにまとめてから、暗号化します。それを指定したフォルダ（クラウド上の場所）にアップする機能です。



フォルダ暗号化(アップロード) を選択すると、

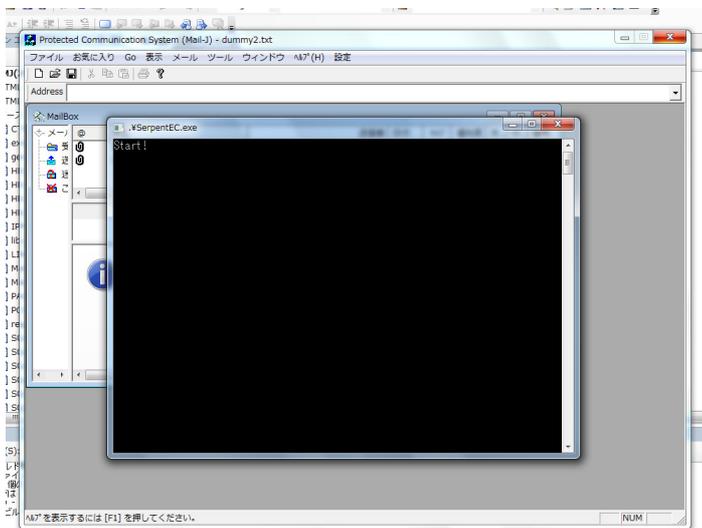


上のような画面になります。 目的のフォルダを枠内にドラッグしてください。(複数のフォルダが選択できます。暗号化と1つのファイルへのまとめは、フォルダごとに行われます。 複数個のフォルダを登録でき、同時に暗号化と移動が行われます。

つぎに、移動先のフォルダを決定します。検索(フォルダ)をクリックして、目的のフォルダの中にあるファイルをクリックしてから開くをクリックすると、そのファイルが入っているフォルダが選択されます。

そして、OK ボタンをクリックすれば、選択したフォルダが暗号化された1つのファイルになって、目的のフォルダに移ります。このとき、元のフォルダは変更されません。削除もされません。コピーしたものに対して暗号化と移動が行われます。

フォルダ内のデータサイズが大きいときは、変換途中での画面がしたの図のようになって現れる場合がありますので、そのときは、しばらくお待ちください。



暗号化されたものは、指定されたサブフォルダの中に入ります。
(注意) 4 MB 程度のを暗号化すると、暗号化ソフトとして **BmpEC.exe** を利用すると 8 MB 程度の大きさになります。他の暗号化ソフトではサイズはほとんど変化しません。

4. フォルダ復号化(ダウンロード)

アドレス帳の自分の項目や、ヤフーBOX の所には、復号化が暗号化に対応する形で設定されていますので暗号化に利用した電子メールアドレスの項目を使って復号化を行います。

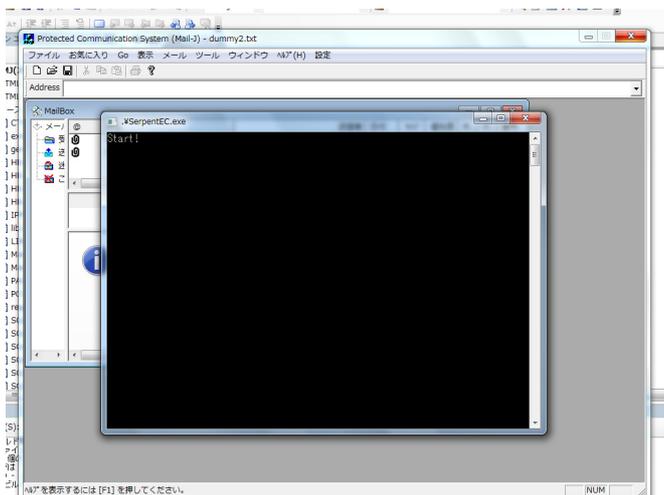
暗号化されたフォルダは、“フォルダ名. pcs” という名前のファイルになっています。この暗号化されたファイルを枠内にドラッグします。複数個の選択が可能です。

暗号(クラウド)ツール から フォルダ復号化(ダウンロード) を選ぶと次のようになります。



あなたのメールアドレス（または picture1）を入力し、復号化するデータを選択してから、OK ボタンをクリックすれば、サブフォルダ **WebDecrypt** の中に復号化されたファイルと展開されたフォルダものが現れます。復号化されたファイルは名前は“フォルダ名.pcs”のままですが、内容は復号化されています。ただし、複数のファイルが連結されているので直接読めない場合が多いです。

時間がかかるときは、復号化の途中で、次のような画面が現れます。



処理が終わるまでしばらくお待ちください。

8 MB のものが最初の 4 MB のデータに戻ります。BmpEC.exe を除けば、世界標準の暗号化方式による多重暗号化ですので、かなり強力なものとなっています。もちろん、本格運用では、暗号化鍵は新しく作ったものを使ってください。

クラウド上の複数のサブフォルダに対してそれぞれ異なった方式での暗号化を選択できます。

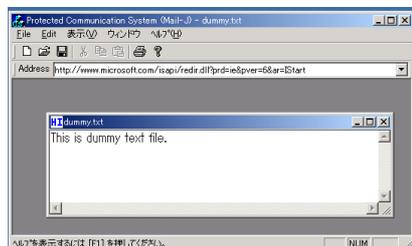
グループごとに暗号化を分けるときは、そのグループでの復号化鍵をグループの構成員に配布しておく必要があります。

また、RSA 公開鍵暗号も利用できますので、特定の人から受け取った公開鍵で暗号化すれば、それに対応する秘密鍵を持っている人しか暗号化を解除できません。

4.3.8 ウィンドウ、ヘルプ、設定

これは、すでに記載した内容と同じですので省略します。

4.4 ダミーテキスト編集



これは、暗号化メールで本文の代わりとして利用する内容を編集するものです。挨拶くらいにしておいてください。印刷のプレビュー、文字列の検索、置換などが行なえます。

“ファイル” – “ダミーテキスト編集” とすると、ファイル **dummy.txt** を編集する為のエディタが開きます。ここで編集して保存した内容が、正規のユーザーが暗号化機能を利用する場合に本文の身代わりとして送信されます。当り障りの無いものにしておいてください。

暗号化機能を利用する場合には、本来のメールの本文は暗号化された特別な添付ファイルとして送信されます。本文の無いメールは味気ないし、他のメーラーで受信したときに表示されるものが無いのも困るので、ダミーテキストを本来のメール本文の代わりに送ることにしました。暗号化機能を利用しない場合は、このダミーテキストは使われません。

5 暗号ソフトのソースコード

暗号ソフトはソースコードを公開してしまえば、公知の技術となって自由に使えるようになります。共通鍵方式の暗号ソフトで高性能のもののソースコードがいくつか公開されています。それらを、このソフトに組み込んで使うには修正が必要でした。

私は、Windows 上の 32 ビット CPU (Pentium など) で動くコンソールタイプの暗号ソフトに書き換えました。一部分本来のものと変更している部分があります。使用したコンパイラは VC++2005、OS は Vista(32 ビット)と Win7(64 ビット)です。ソースコードを見れば、皆様自身で新たなソフトを作成できると思います。参考にしてください。ただし、著作権、特許権を侵害しないようご注意ください。

法律の制限で個別の質問にはお答えできませんが、問題点などは HP に記載する形で解決してゆきたいと思っています。

暗号ソフトのうち、本来のソースコードが公開されている、Misty, Camellia, AES, Twofish, Serpent, MARS を利用したものについて、本来公開されているソースコードの一部を私に変更したものをホームページで公開しています。

私の変更に関して安全性に不安のある方は、私のホームページから本来のソースコードへのリンクが張ってありますので、それらを手に入られて、本来のものと変更したものの両方のソースコードを比較されて、ご自分で信頼できるものを作成し、御自分でコンパイルされて使用されることをお勧めします。

5.1 Camellia 暗号ソースコード

掲載したソースコードの大部分は NTT と三菱電機様が公開されたものですが、このメールシステムで利用するために少しだけ変更してあります。

安全性に関しては皆様が本来の Camellia 暗号のソースコードと比較されて確認して下さることを希望いたします。私のホームページからリンクが張ってありますのですぐに見つかると思います。

詳しいソースコードは、ホームページ (<http://uyama22.pa.land.to/>) で確認して下さい。

5.2 AES 暗号ソースコード

参考文献：The Design of Rijndael, AES - The Advanced Encryption Standard, Springer のソースコードには 2 箇所だけ誤りがあります。これに関しては著者が訂正しています。このソースコードを変形して、Protected Communication System で利用する形にしたものが以下のソースコードです。

この変形が安全性に影響を与えないと考えていますが、皆様自身で参考文献のソースコードとここに記載されているソースコードを比較されて安全性を確認してください。

詳しいソースコードは、ホームページで確認して下さい。

5.3 Twofish 暗号ソースコード

参考文献："The Twofish Encryption Algorithm", (WILEY)に記載されているものとほぼ同じですが、製作過程で内容がわかりやすくなるようにするために新たな変数を使用しました。

詳しいソースコードは、ホームページで確認して下さい。

これらの暗号ソフトを、簡単に 5 段階まで適用して 5 重に暗号化できます。このソフトによって、アドレス帳に暗号化ソフト名、暗号化鍵のファイル名、複号化ソフト名、復号化鍵のファイル名を登録するだけで、様々な暗号技術を簡単に利用できるようになります。

現在、対称鍵方式（共通鍵方式、秘密鍵方式）では、7種類（Bitoma, AES, Camellia, Twofish, Serpent, MARS, Misty）が利用可能です。

5.4 RSA 暗号ソースコード

公開鍵暗号 RSA のソフトです。“メールもビトマ”、“Cipher Web Mail”における共通鍵の交換のために作成しました。鍵の長さについては、512 ビット、1024 ビット、1536 ビット、2048 ビット、2560 ビットの鍵を扱えるようにしました。（鍵を作成するのに要する時間はそれぞれ、30 秒、10 分、40 分、2 時間です。メモリーの量や CPU の性能で異なる。）もちろん貿易管理令に違反しないようにソースコードを HP で公開します。

ソースコードの特徴は、複素数の配列と多倍長整数の変換を適宜行う方法で全体を扱っていることです。さらに、3 通りの乗法（複素数の普通の乗法、DFT による乗法、FFT による乗法）を用意して、扱う数の大きさによって切り替えて計算しています。

除法と剰余は自分で考えた方法で計算しています。特徴は筆算に似せた方法になっていることです。

素数生成および、最大公約数と逆数の計算は Menezes の Handbook of Applied Cryptography (Discrete Mathematics and Its Applications) にあった方法を少し変形して使っています。べき乗計算は FFT を主に利用しています。

全体的な流れは、橋本晋之介 氏の
”RSA 暗号技術の基礎から C++による実装まで”
の流れに沿って作成しました。ご指導いただいたことを感謝しております。

詳しいソースコードは、ホームページで確認して下さい。

現在、公開鍵方式では、RAS が利用できます。
亀のような速度ですが、楕円曲線暗号も追加しました。ソースコードはホームページにあります。

また、暗号ソフトをどのような形式で作成したらこのソフトで利用可能となるかは、ホームページの資料から理解できると思います。従って、皆様が独自に開発した暗号を利用するのも簡単にできます。

暗号ソフトとメールソフトは完全に別のソフトです。したがって、暗号を開発する人に対して適正な利益が得られる基盤が提供されます。この結果、沢山の暗号方式が発表され、情報を簡単に、しかも強力に暗号化して送信できるようになります。利用者は合理的な出費で、暗号強度が十分であるものを利用できるようになります。後ほど、暗号ソフトをどのように作成したらこのソフトで利用できて、販売が可能となるのかを詳しく示しますので、多くの暗号開発者の方々が参加されますようお願いいたします。

現在では暗号技術の変化がとても速いので、最新の理論や技術を利用した暗号化の方式も明日には解読されているかもしれません。この問題に対して3つの方法で対応します。

1. 最新の技術や理論を使った暗号化ソフトを簡単に組み込める仕組みを最初から用意します。
2. 多重暗号化によって解読を困難にします。
3. 鍵は利用者が自由に作成する。

この3つの方法によって、あなたの情報を盗聴から守ります。

6 暗号ソフトを作成される方に

6.1 使用できる暗号の種類と特徴：

暗号には、大きく分けて秘密鍵方式と公開鍵方式の2種類がありますが、どちらも利用可能です。

理論上は、暗号化鍵と暗号化ソフトを分離しなくても良いのですが、ハードウェアの現状に適しているとの理由で、暗号化鍵と暗号化ソフトを分離する方式について記述します。

暗号用の商用ソフトは、鍵生成ソフトと、暗号化ソフト、復号化ソフトのセットで、次のような構造を持つものとして制作されるべきです。

- (1) 暗号化鍵の作成機能をもち、暗号化鍵の自由な配布が認められている。
- (2) 暗号化ソフトの自由な再配布が認められている。
- (3) 復号化鍵の作成機能をもつ。
- (4) 復号化ソフトの再配布を禁止できる。

この、1から4を満たすようになっていれば秘密鍵方式でも、公開鍵方式でもどちらも利用することができます。このような構造で暗号ソフトを制作することは困難ではありません。

復号化ソフトの再配布が禁止できれば、暗号ソフトの利用者がそれぞれにソフトを購入することになりますので、商業的にソフトを制作販売することが可能となります。より優れた暗号ソフトの開発が可能となるのです。

安全な暗号ソフトを作成するのはかなりの時間と努力を必要とします。暗号ソフトは既にかんりの種類が存在し、専門家も作った社会的評価の高いものを選ぶのが現実的な選択です。

暗号化と復号化のソフトに関する要求。

1. 名前の変更が可能であること。
 2. 引数を3つもっていること。
 3. 暗号化ソフトの場合は、第1引数は、暗号化で使用する鍵を記録したファイル名、第2引数はこれから暗号化されるファイル名、第3引数は暗号化された結果のファイル名。
 4. 復号化の場合は、第1引数は、復号化で使用する鍵を記録したファイル名、第2引数は（暗号化されている）これから復号化するファイル名、第3引数は復号化されたデータを記録するファイル名
- 暗号化ソフト、復号化ソフトは、コンソールタイプアプリケーションとして開発して下さい。

暗号化、復号化のときの動きは次のようにして下さい。

暗号化の場合には、

暗号化ソフト(`encrypted.exe`)、暗号化鍵(`ekey.bin`)、平文ファイル(`plane.bin`)、暗号化したファイル(`encrypted.bin`)とすると、DOS ボックスから

```
encrypt(ekey.bin, plane.bin, encrypted.bin)
```

と呼び出したときには、2つのファイル(`ekey.bin`、`plane.bin`)をバイナリファイルとして読み込んで、与えられたファイル名(`encrypted.bin`)の暗号化されたバイナリファイルを生成する様に機能しなくなりません。

復号化の場合には、

復号化ソフト(`decrypt.exe`)、暗号化鍵(`dkey.bin`)、暗号化したファイル(`encrypted.bin`)、平文ファイル(`plane.bin`)、とすると、DOS ボックスから

```
decrypt(dkey.bin, encrypted.bin, plane.bin)
```

と呼び出したときには、2つのファイル(`dkey.bin`、`encrypted.bin`)をバイナリファイルとして読み込んで、与えられたファイル名(`plane.bin`)の復号化されたバイナリファイルを生成する様に機能しなくなりません。

暗号化や復号化が終了したら自動的に終了しなくなりません。コンソールタイプならそのように機能します。また計算過程を表示させるようにした方が、利用者が楽しめると思います。16進数で表示すると良いでしょう。暗号ソフトが多重暗号化のどの場面で利用されるかは分かりませんので、テキスト表示では問題が生じます。

暗号化、復号化のソフトを作成される場合には、データの長さにご注意ください。ブロック型の暗号ではブロック長の整数倍となるようにデータを加えて暗号化するので、どこかに元のデータサイズを記載し、復号時にはその数値を使って、元のデータサイズに調整する必要があります。

また、データファイルを開くときはバイナリデータとして開いてください。理由は、多重暗号化の場合、一度暗号化されたものはバイナリデータとして扱うことが必要だからです。データはバイナリデータとして開いて、バイナリデータとして保存してください。

鍵作成ソフトは、共通鍵方式の時も名前を変えた2つのかぎファイルを作成するようにして下さい。ダイアログボックスから暗号化鍵と復号化鍵のファイル名をそれぞれ入力できる様にして下さい。

鍵が単なる乱数のような場合は、暗号ソフトの利用者が自分で乱数を生成すればそれで済みますが、RSAの様な場合には、単純な乱数の組では機能しません。鍵生成ソフトが必要になります。鍵生成ソフトが認証用のファイルがないと動かないようにしておいて、認証用ファイルの入手時にソフト代を支払う様にすれば暗号ソフトの制作をする人にも収入が得られる用になります。

本来は単純な乱数で動く暗号化ソフトでも、鍵ファイルの中に埋め込まれた特別な値を確認してから動くように作っておけば、その特別な値を持っている鍵ファイルを作成する為の鍵生成ソフトが必要になります。この鍵生成ソフトを起動させるときに認証用ファイルが必要であるなら、その認証用ファイルを手にするときに、代金を支払ってもらうことができます。

6.2 暗号ソフトの呼び出しコード

暗号ソフトは次の様に呼び出されますので、参考にしてください。

```
1. Encryption (暗号化) では、
  if((strlen(ecp1)>0)&&(strlen(eck1)>0)){
    ret = _spawnl(_P_WAIT, ecp1, ecp1, eck1, ecpath0, ecpath1, NULL);
  }else{
    CopyFile(ecpath0,ecpath1, FALSE);
  }
```

の様に呼び出します。

```
2. Decryption (復号化) では、
  if((strlen(dcp5)>0)&&(strlen(dck5)>0)){
    ret = _spawnl(_P_WAIT, dcp5, dcp5, dck5, dcpath5, dcpath4, NULL);
  }else{
    CopyFile(dcpath5, dcpath4, FALSE);
  }
```

の様に呼び出します。

7. 特許について

2007年2月14日にヨーロッパ特許庁の特許認可が下りました。またアメリカでの特許も取得いたしました。(U.S.Patent US7219229 ; European Patent EP1244257)、詳しくは、ホームページ (<http://uyama22.pa.land.to/>) で確認してください。

8. 利用しているソフトについて

1. 文字コードの変換には株式会社ピーデーの川俣 晶氏が作成された tconvlib.dll を使わせていただいています。

この DLL はこのメーカーに不可欠のものでした。提供して下さったことに関して深く感謝いたします。ありがとうございます。

なお、著作権表示はバージョン情報の一部として記載しています。

2. データベースとして、SQLite も使用することにしました。使用できることを感謝しております。

3. 一部、LGPL の規定を受けるコードを利用しています。そのソースコードは与えられたままで使用しています。変更はしていないのですが、これも、公開しています。

9. バージョンアップについて

2012.9.19

SMTP-AUTH、587 番ポート に対応させました。

2012.10.04

Web メール の扱いを改良しました。

問題点がありましたら、お知らせいただければ改善に向けて努力いたします。

(uyama33@yahoo.co.jp : 宇山 靖政) まで連絡してください。

Ver.3.2 では、ヘルプを追加しました。

Ver.3.2 では、他のメールソフトとの連携を強化しました。

Ver.3.3.2 では、RSA 公開鍵暗号を追加しました。

Ver.3.3.7 では、にゃん語メールの送受信が可能となりました。

おわり。

宇山靖政