Web 暗号通信　簡単ガイド

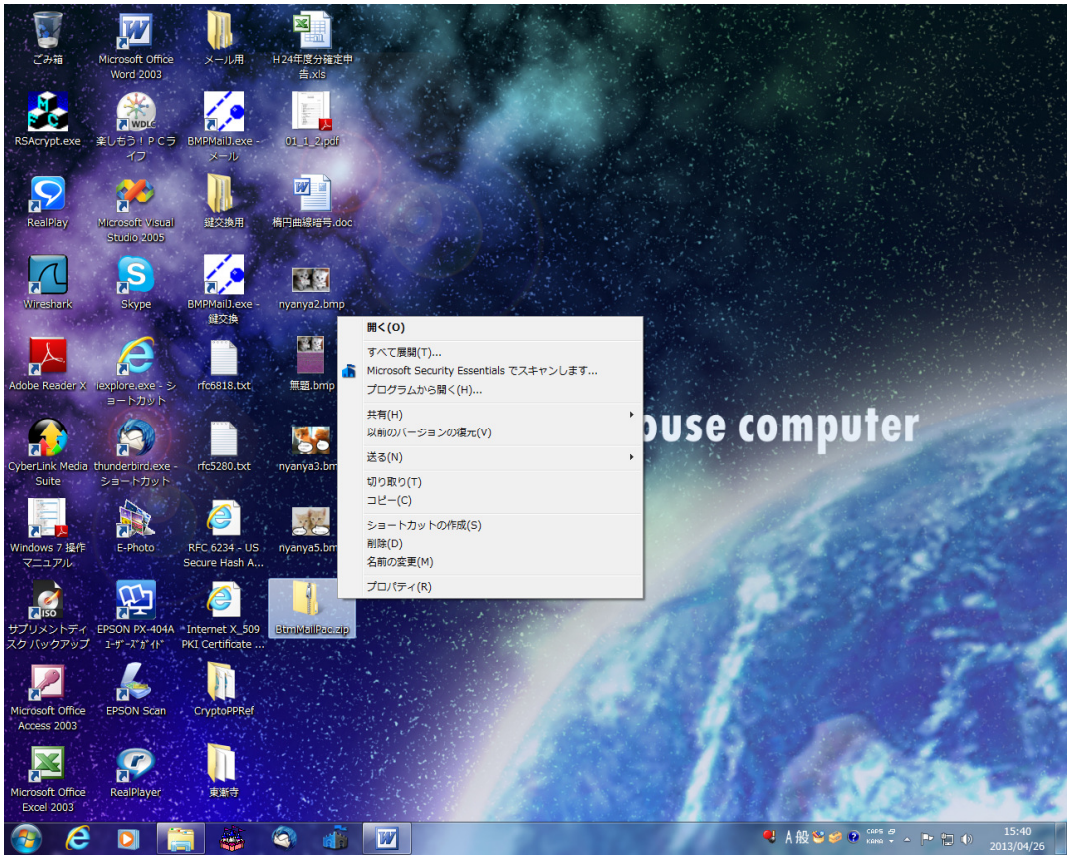
（C）：宇山　靖政

0.　動かしてみよう！（にゃん語メールを送る）

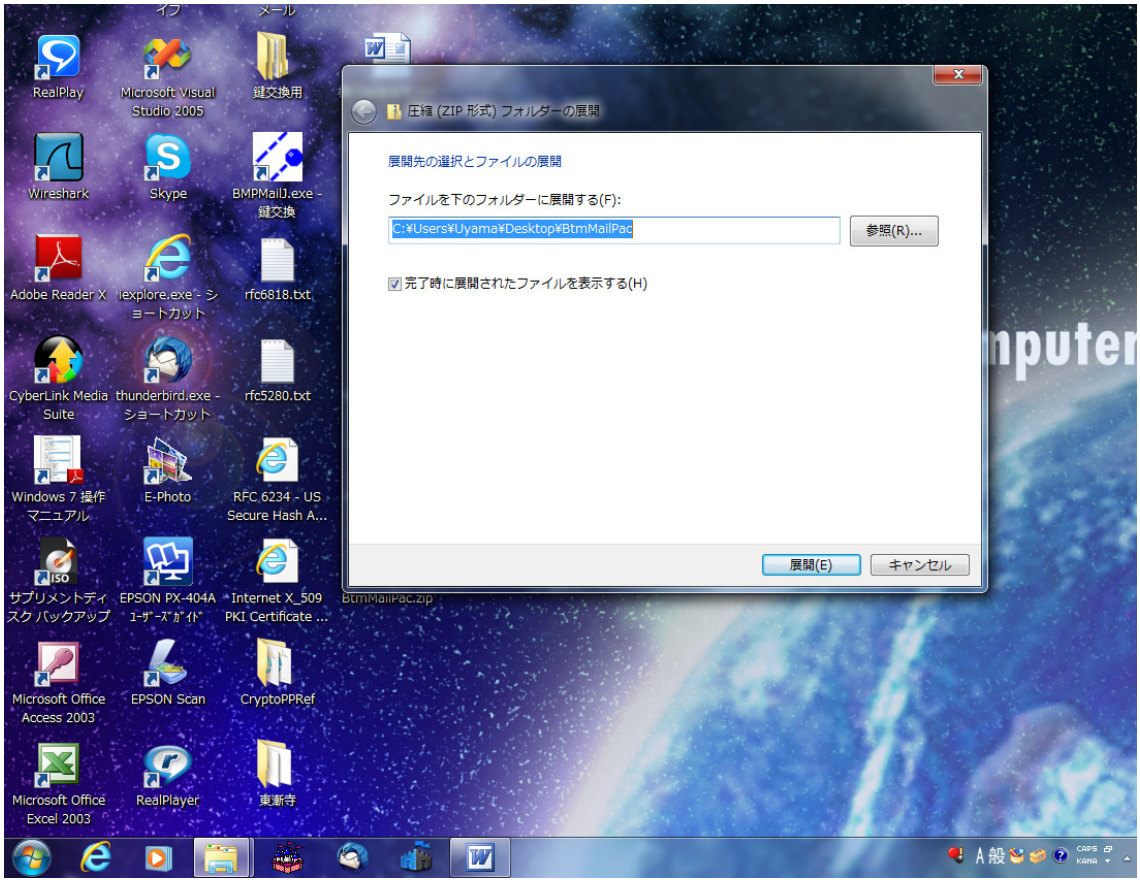
0.1　解凍

WebATJPac.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。

WebATJPac.zip　を右クリックしてください。



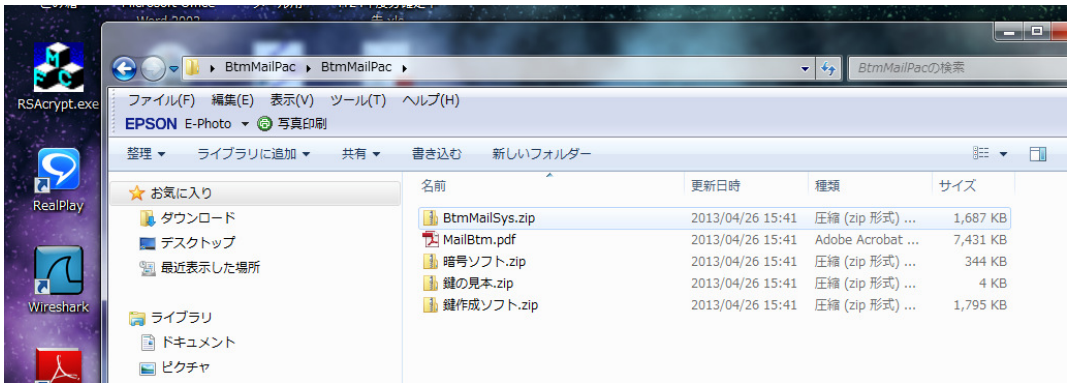
すべて展開（T）　を左クリックして、



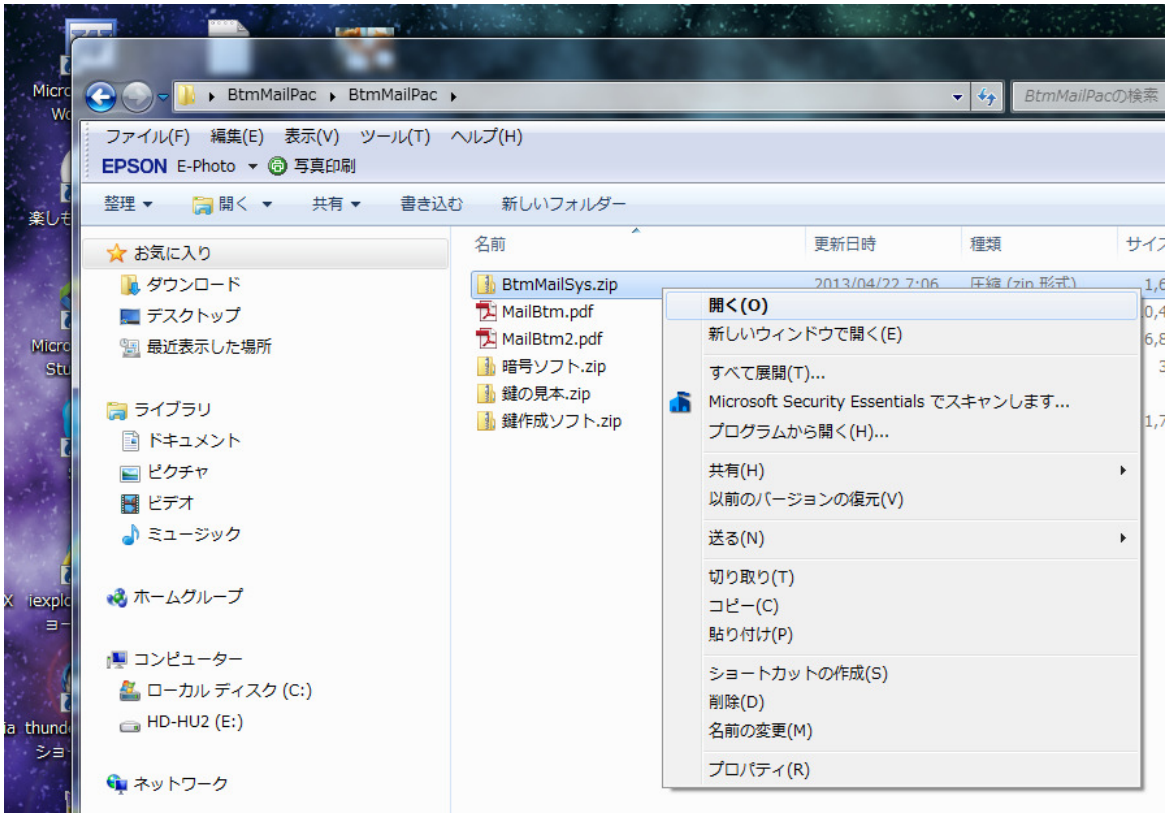
右下の展開を左クリックしてください。

WebATJPac　というフォルダが現れます。

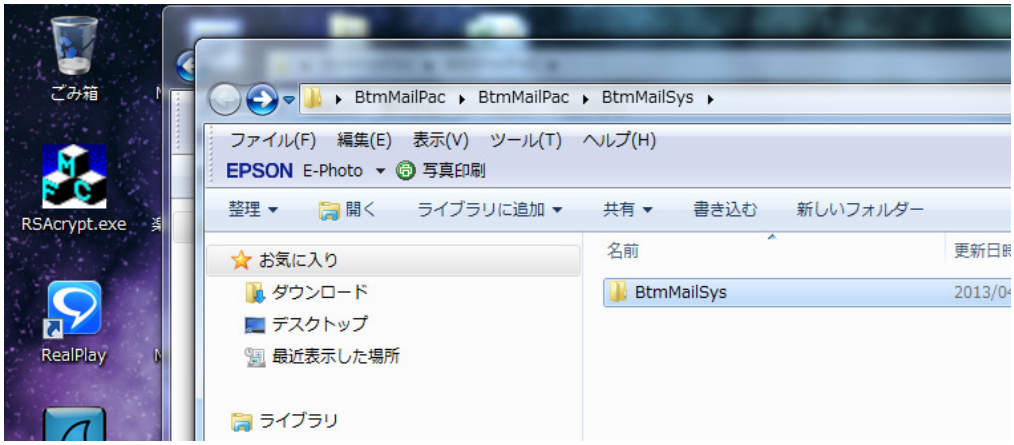
そこを、ダブルクリックすると、



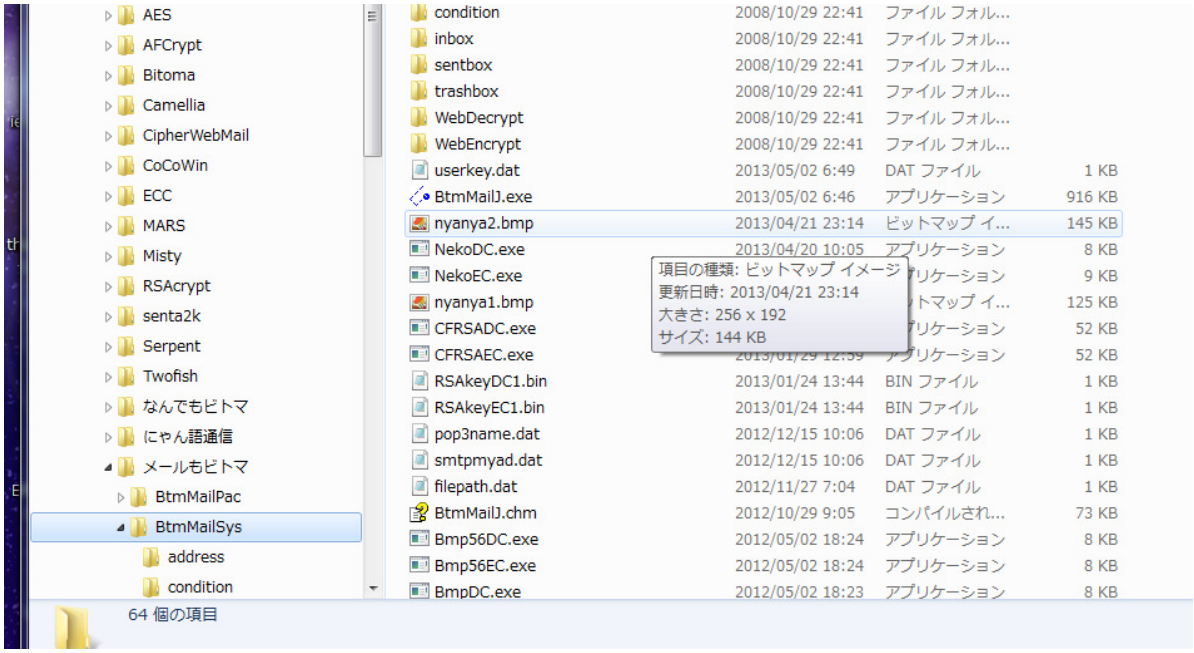
そのなかに、WebATJSys.zip が現れます。右クリックすると



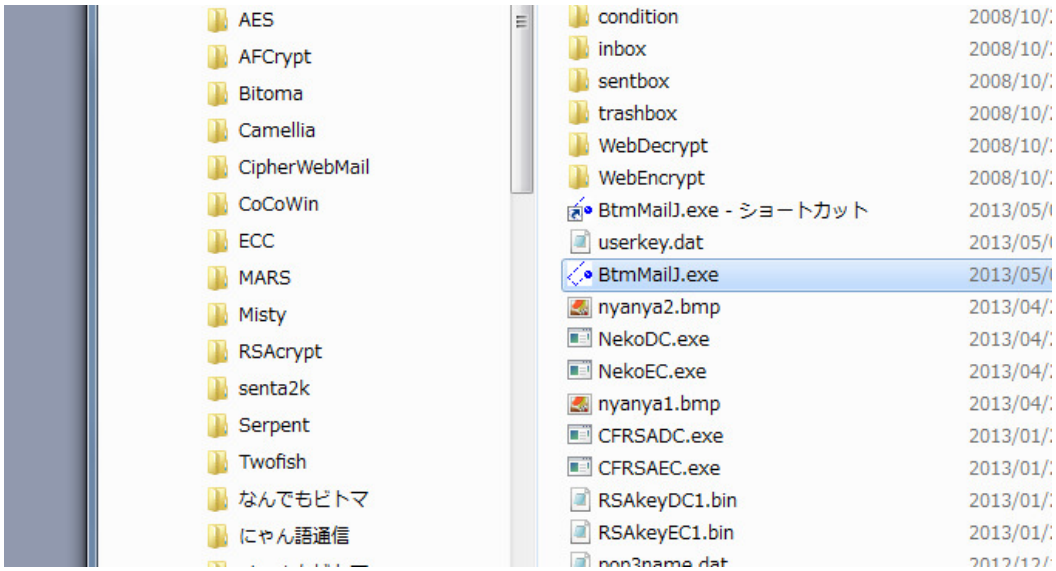
となりますので、さらに、すべて展開（T）　とし、展開してください。



WebATJSys　フォルダがあらわれます。この中の、

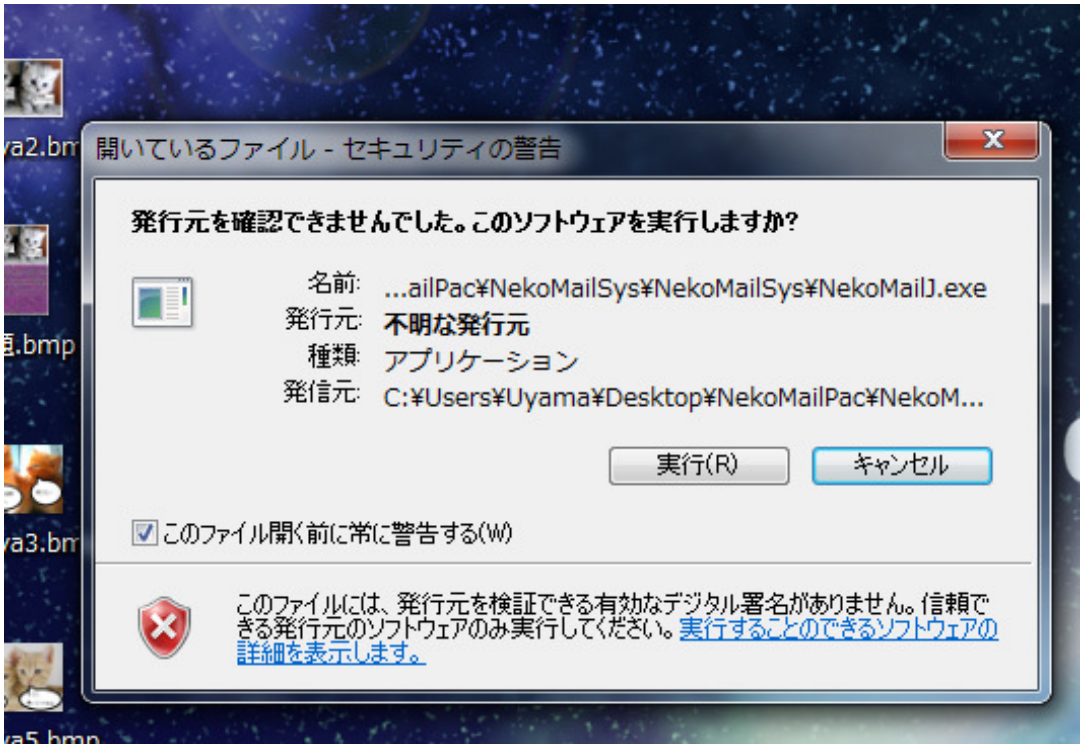


WebATJ.exe を右クリックして、ショートカットの作成を選んでください。



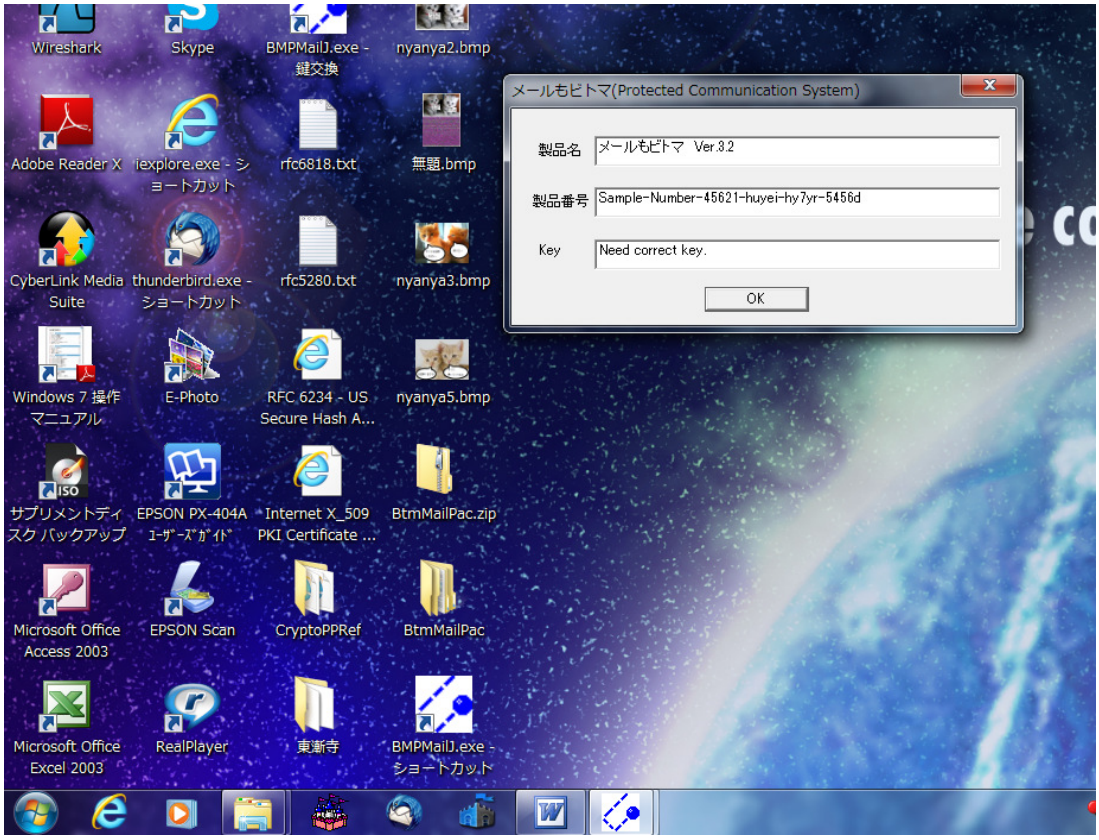
出来上がったショートカットを、デスクトップにドラッグしてください。

このショートカットをダブルクリックすると、

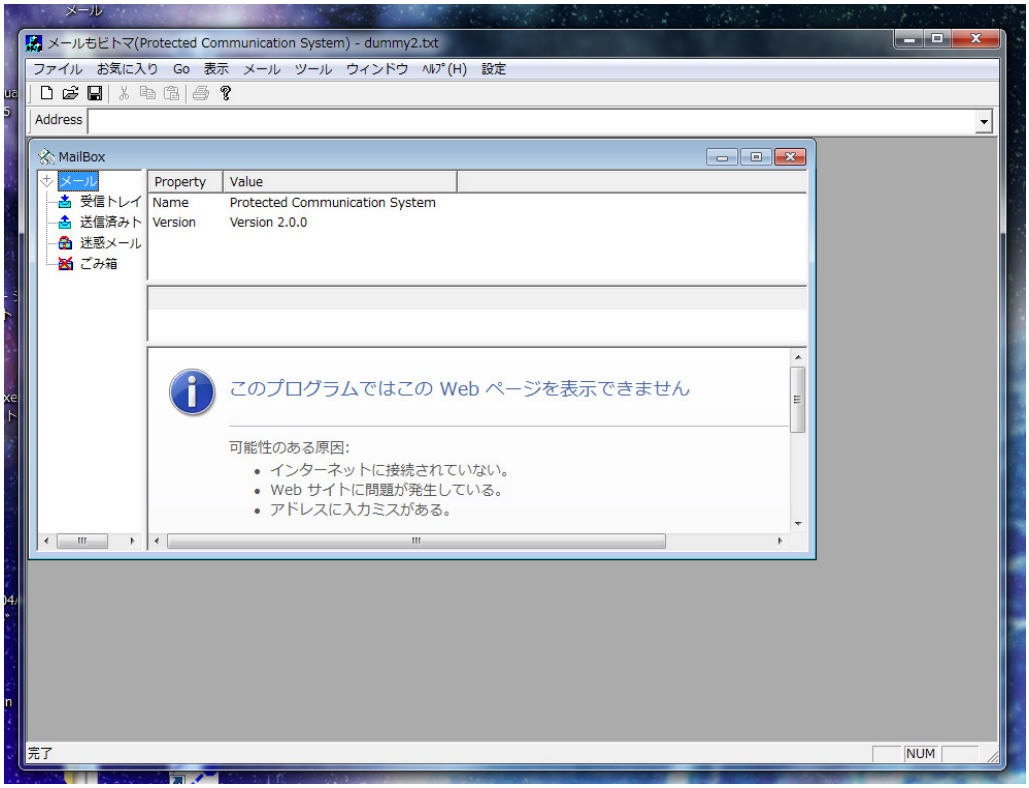


製作者が有名ではないので、警告がでます。でも、実行をクリックすると、

（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、

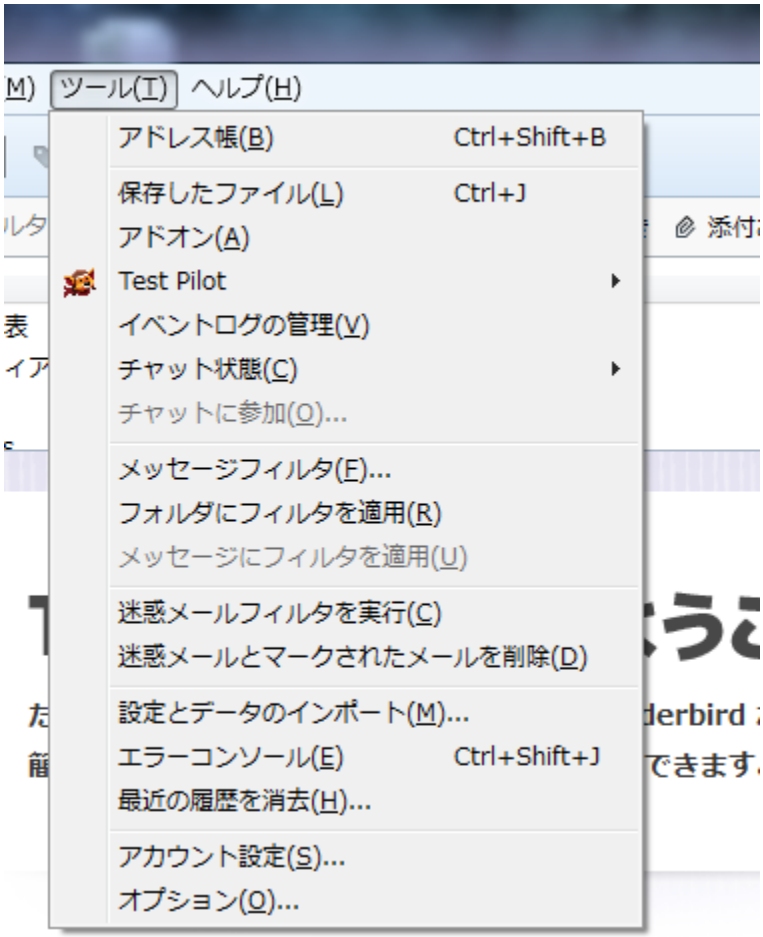


となって、ソフトが動き始めます。

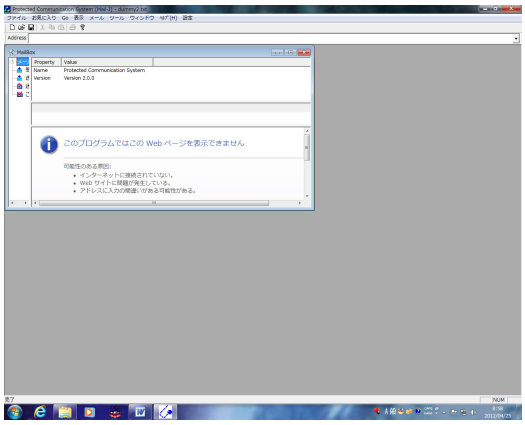
インストール：WebATJPac.zip を解凍すると、このマニュアルの他に、
WebATJSys.zip
暗号ソフト.zip
鍵の見本.zip
鍵作成ソフト.zip
が現れます。WebATJSys.zip を解凍すると、“WebATJSys”フォルダが出来ます。このフォルダをデスクトップ等の適当な場所に置いてください。
“WebATJ.exe”へのショートカットを作成してください。
起動後に、SMTP-AUTH、SMTP、POP３サーバーの設定をします。

0.2　SMTP-AUTH、SMTP、POP3 の設定

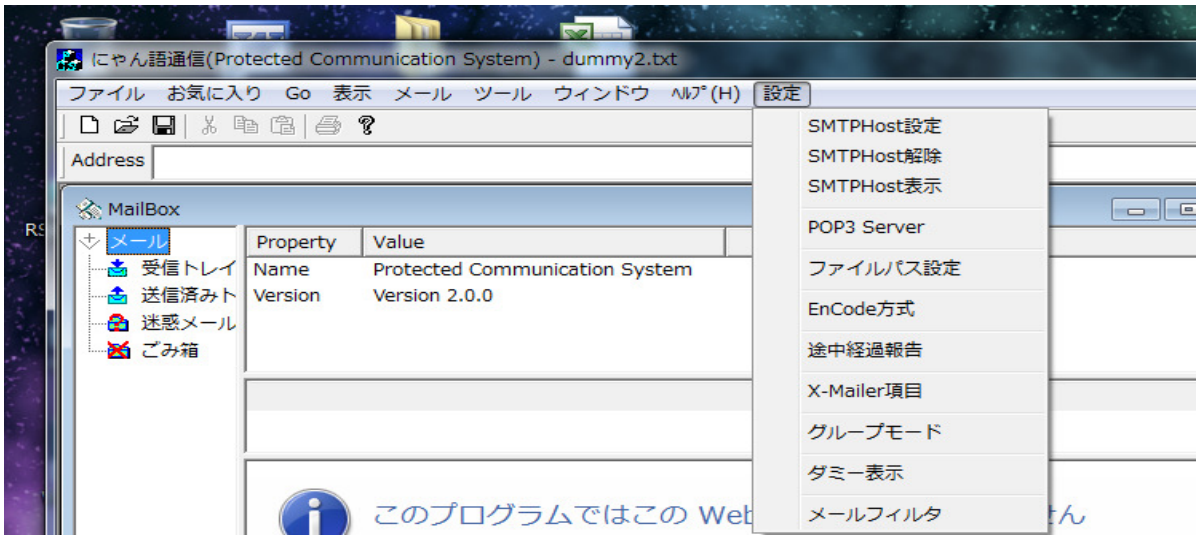
他のメールソフトの、アカウント設定を参考にすると楽に出来ます。下は、サンダーバードの場合です。ツールからアカウント設定を選んでその内容を見ながら設定してください。



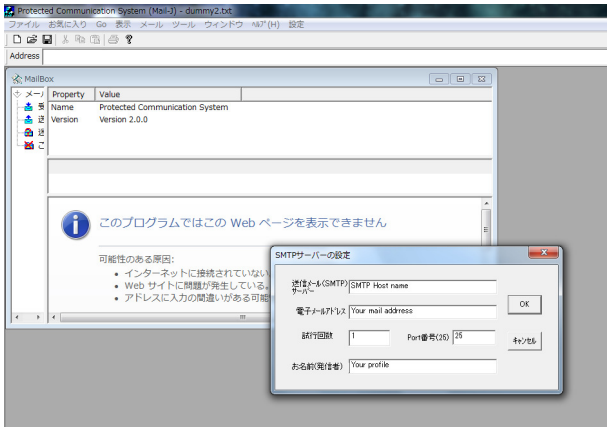
起動すると、最初にユーザー確認のメッセージが出ます。OK をクリックします。すると次の画面が現れます。



右上の、設定から、SMTPHost 設定を選んでください。



ここで、さいしょのメールの行き先である、SMTP サーバーの設定に入ります。



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。

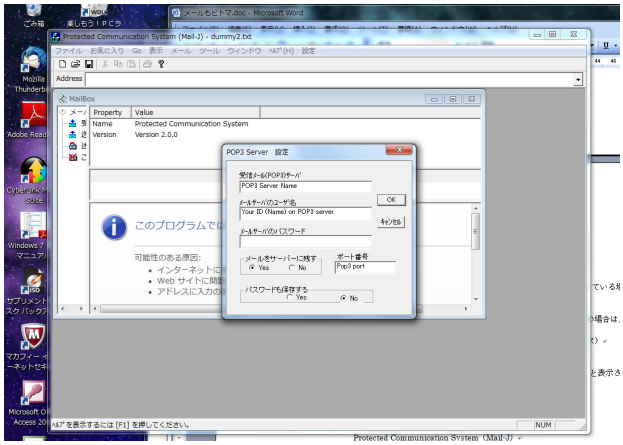
Port 番号は SMTP では 25、SMTP-AUTH では 587 です。

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。

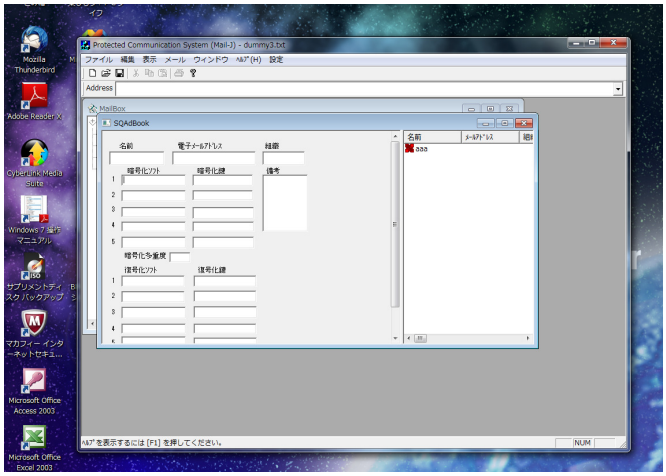
さらに、POP3 サーバーの設定です。



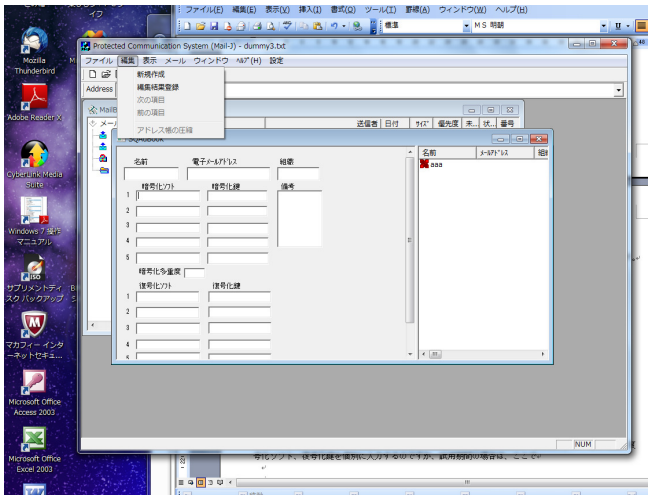
受信メール(POP3)サーバー：efg.xyz.ne.jp　　（@の右側）
メールサーバーのユーザー名：abcd　　（@の左側）
メールサーバーのパスワード：　これは、プロバイダーからの書類にあるものです。
ポート番号：110
としてください。
メールはサーバーに残す設定にして、普段のメールソフトで処理してください。
パスワードも保存してください。

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します。

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

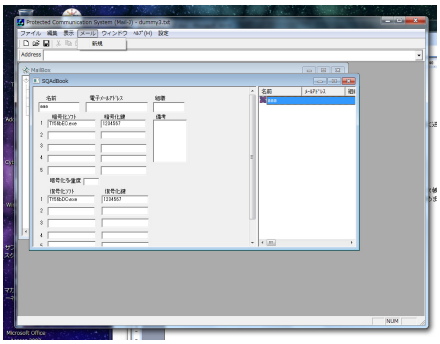
復号化ソフト　Bmp56DC.exe
復号化鍵　1234567
とします。(試用期間中は自動的に入力されます。)

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。

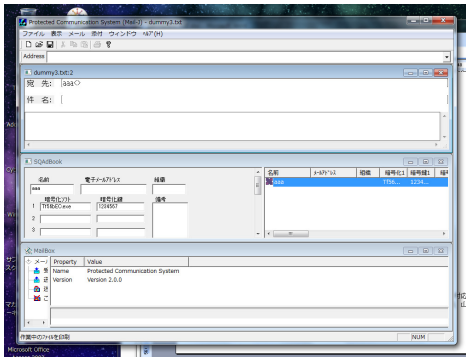
これで暗号通信ができます。最初は自分宛に、そして自分のフリーメールアドレス宛に送ってみましょう。

0.4　暗号メール送信

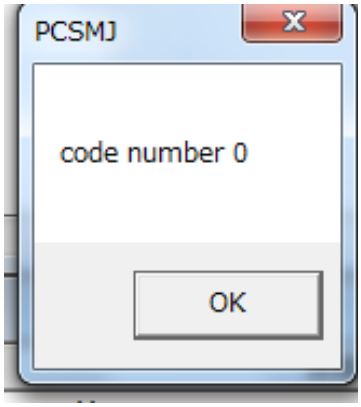
アドレス帳の右側で、メールを送る相手をクリックします。



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 をクリックして送信完了です。

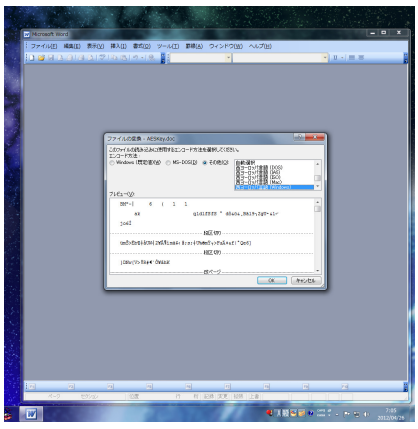
ただし、本文の内容は暗号化されますが、件名は暗号化されません。
添付ファイルの内容は暗号化されますが、そのファイル名は暗号化されません。
暗号化されたときのデータ形式は、暗号化の最後に Bmp56EC.exe を使ったときはビットマップ形式になっています。

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。

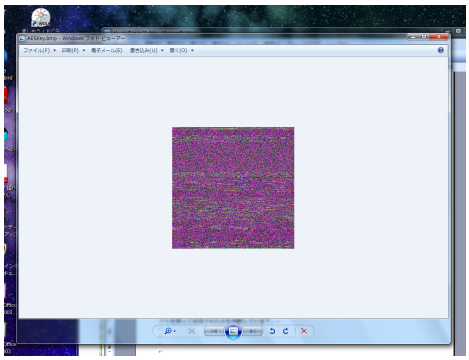
　復号化ソフト復号化鍵が送信者の暗号化に対応してきちんと設定されていなくてはなりません。

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



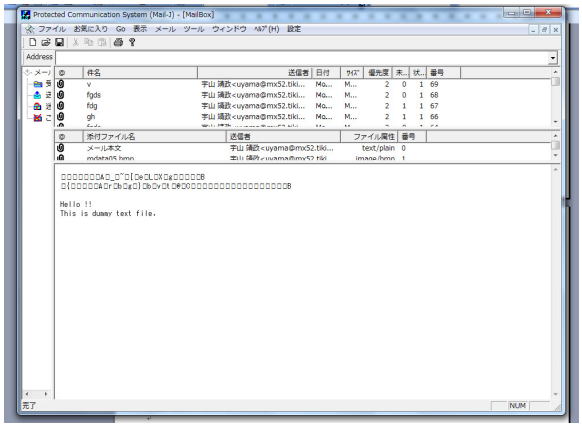
となって、データ形式がビットマップ形式になっていることが分かります。

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

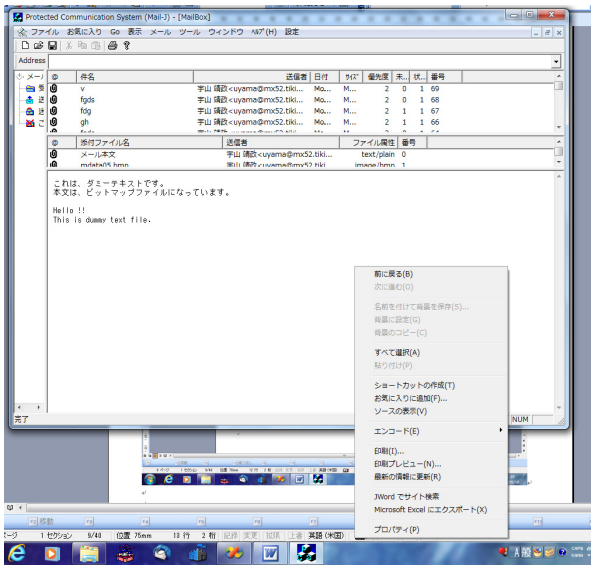
同じメールアドレスから送信されたものでも、このメーラーを使った場合は自動的に復号化されますが、別のメールソフトから送信されたものは復号化されないで普通に表示されます。内部で、どんなメールソフトを使って送信されたかを判断しています。

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。)


Protected Communication System (Mail-J) - [MailBox]
これは、ダミーテキストです。
本文は、ビットマップファイルになっています。
Hello !!
This is dummy text file.

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、

のような添付ファイルと、次のメール本文

読めなっかったら、
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。

が届きます。

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。

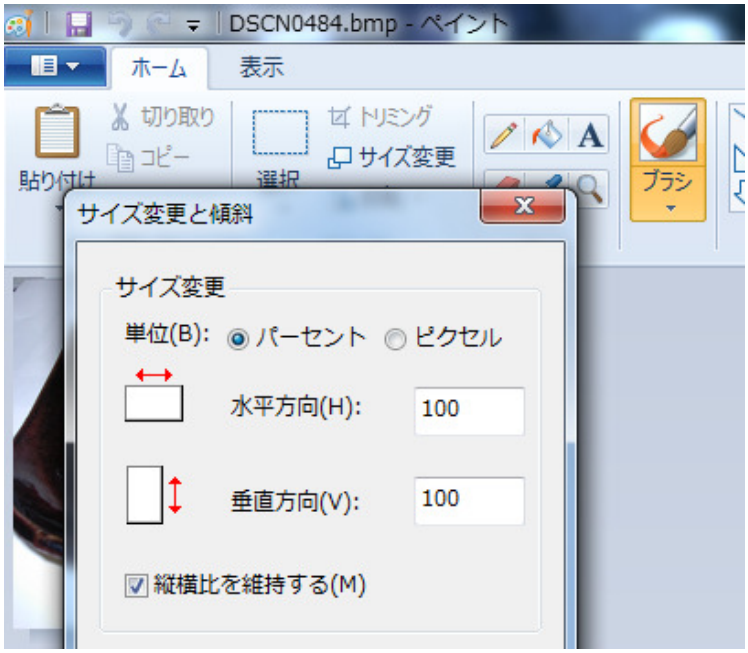
１．　写真をパソコンに取り込む。
デジカメで写真を撮ってください。
ＵＳＢケーブルでパソコンとつないで、写真をデスクトップに置いてください。
写真を右クリックして下さい。

ここで、プログラムから開く(H)を左クリックして下さい。

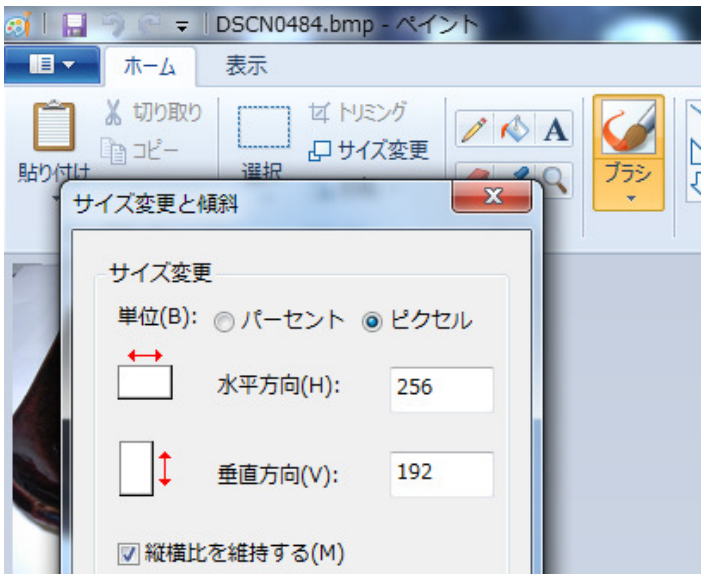
さらに、ペイントの所を左クリックしてください。

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。

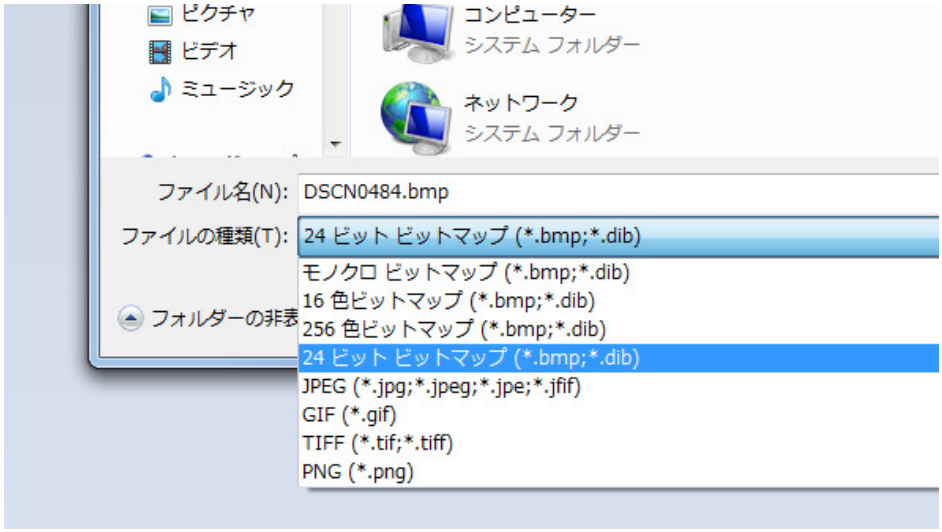


他のバージョンでは、変形のサイズ変更を選択し、サイズ変更で、水平方向、垂直方向の所の値を 50 とか 30 にして、縮小します。横幅の見た目が 5～6 センチ程度になるように調整してください。大きすぎなければ適当でかまいません。

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;*.db）
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でお願いします。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ー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、NekoMailSys 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

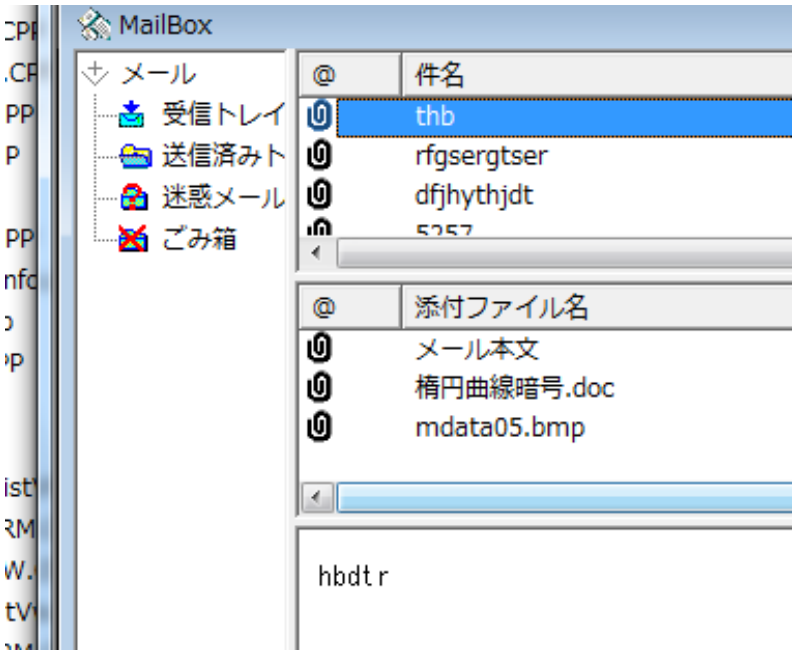
とします。機能制限が解除されている期間や、あなたがベクターから正規ユーザーのキーファイルを購入していればこのような設定ができます。

あなた自身の普通のメールアドレスとあなたのフリーメールアドレスも登録して、どちらも同様の内容で設定して置いてください。

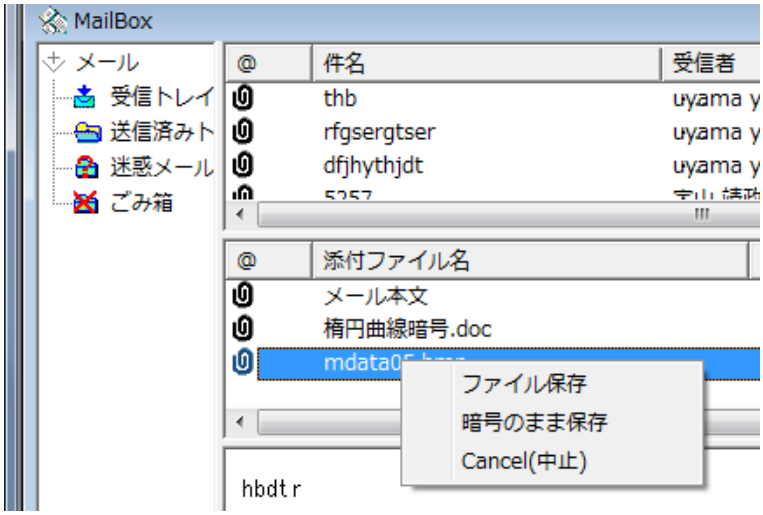
ここで使用する暗号化鍵は、Bitoma 暗号で使うものと共通です。新しく鍵を作るときは、BmpCrypt.exe をご利用ください。作成した鍵を受信者と交換するには、RSA 暗号と楕円曲線暗号が使えます。マニュアルの本文をお読みください。

送信したデータの確認

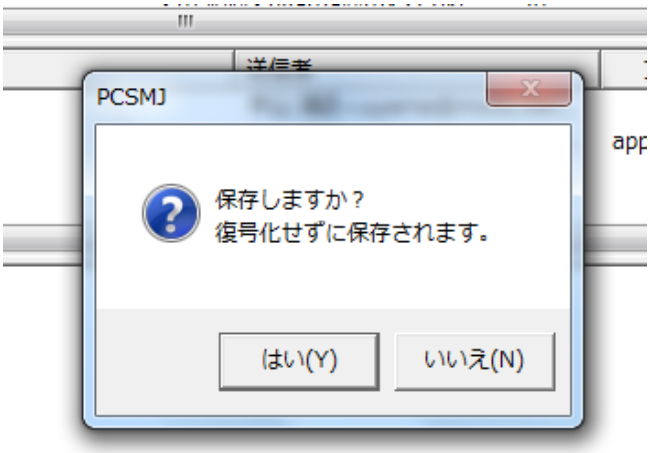
とりあえず、自分の名前と、自分のフリーメールアドレスを記入してから編集結果を保存してください。そして、自分のフリーメールに向けてメールを送信してみてください。
あなたの猫が、猫語で書かれたメールを届けていることでしょう。
普通は、送信したデータの内容は、送信済みトレイをクリックすると、あなたが記入した最初の日本語の形で表示されます。



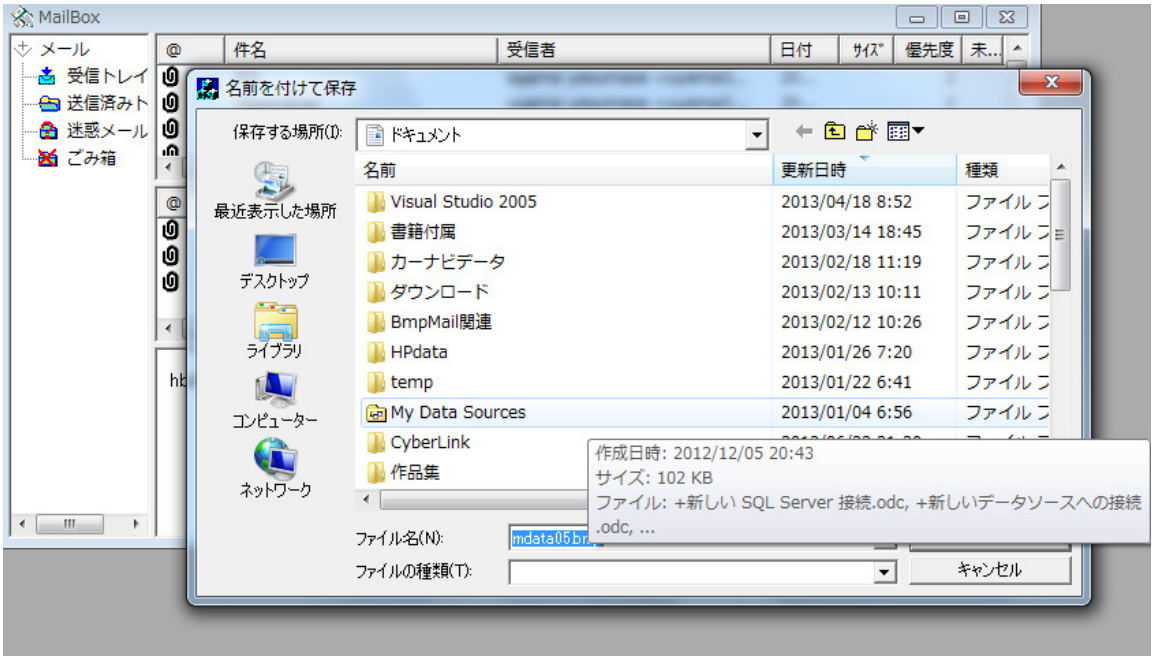
あいてに、どんな形で届いているかを確認するには、



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。

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下さい。
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。

他の添付ファイルも内容はビットマップファイルですが、ファイル名は元のままです。
たとえば、楕円曲線暗号.doc　は、暗号化したままで保存してから、拡張子を bmp に変更して
楕円曲線暗号.bmp　とすれば、図形として表示されます。

にゃん語メールの日本語への変換と表示

このソフトで直接受信すれば、にゃん語は自動的に日本語に変換されます。

ヤフーメールのような場合は次のようにします。

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。

“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、日本語のメール本文が表示されます。

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になります。

このソフトを使ってウエッ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”からウエッ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。

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。

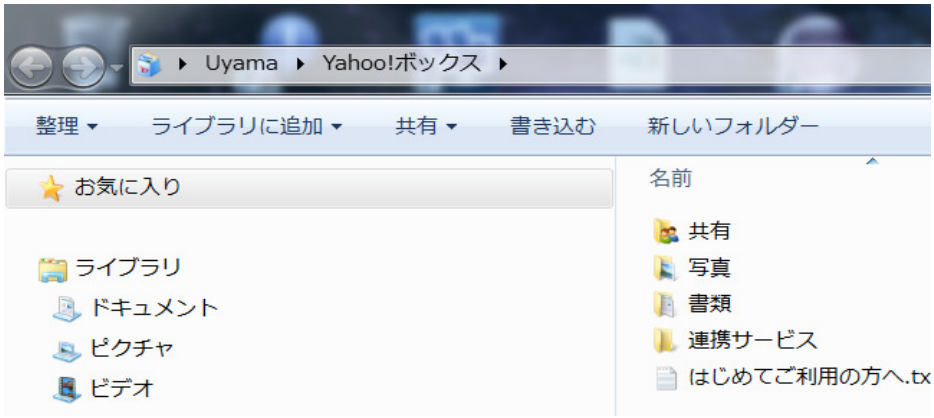
これらの心配を完全とは言えませんが、１,2 についてはかなりの程度防御できると考えています。
標準とされる暗号方式での多重暗号化を提供します。たとえ、AES が総当り攻撃で１秒で解けたとしても、AES、カメリア、RSA などで３段階の多重暗号化をすれば、総当り攻撃には耐えられると思います。

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 内のフォルダー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。



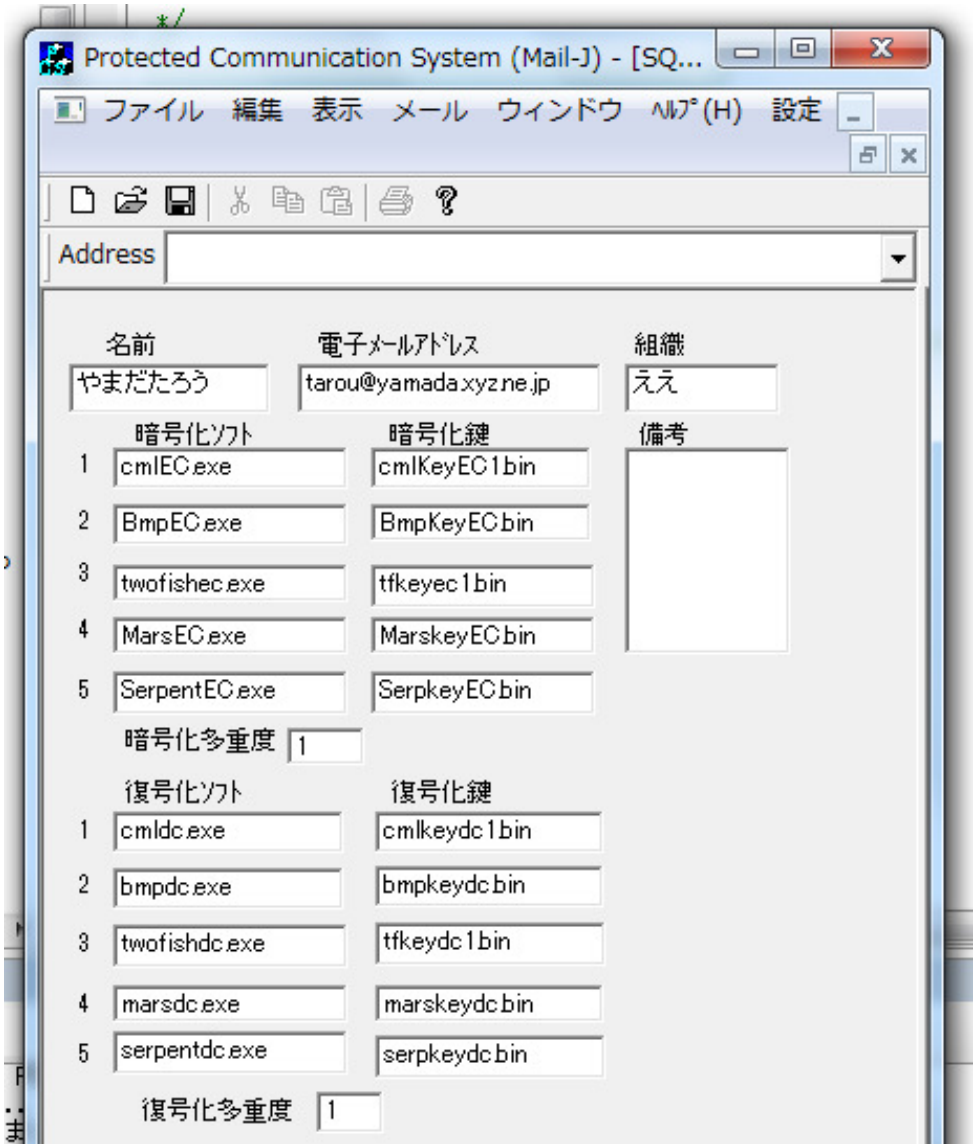
これらのフォルダにデータを移動させるときに暗号化をするのですが、**フォルダを選択するにはその中にあるファイルをクリックしなくてはならないので、サンプルピクチャを各フォルダに 1 つずつ配置してください。**

　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出来ます。
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。

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。

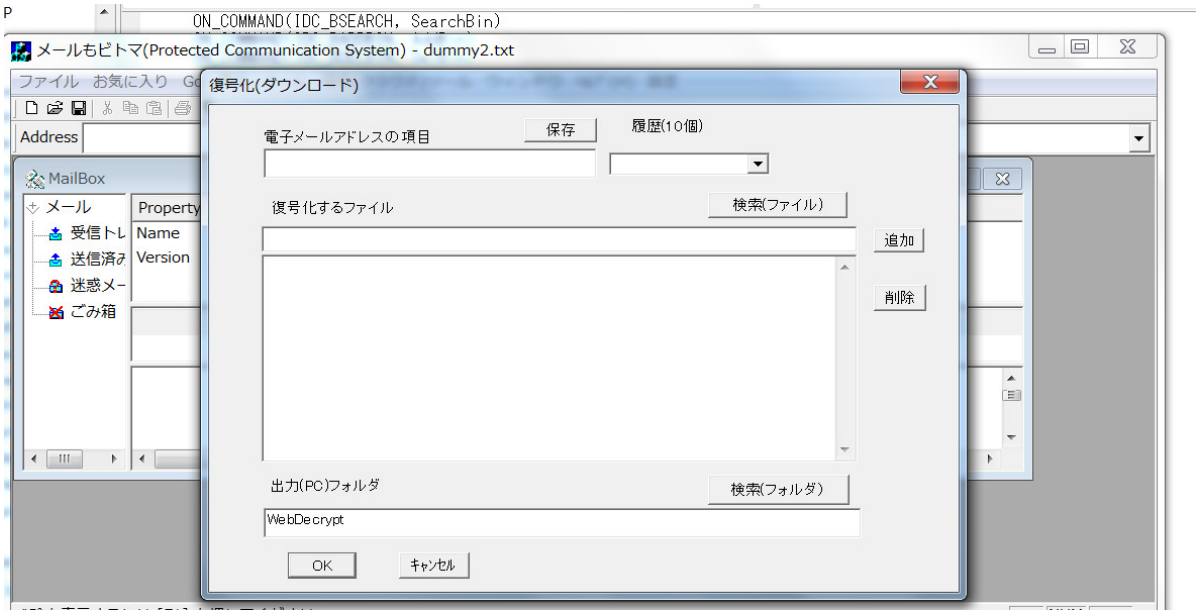
つぎに、移動先のフォルダを決定します。検索(フォルダ)をクリックして、目的のフォルダ（ヤフーボックスのフォルダ）の中にあるファイルをクリックしてから開くをクリックすると、そのファイルが入っているフォルダが選択されます。

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。コピーしたも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。

ク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。