Web 暗号通信(フリーメール)　簡単ガイド

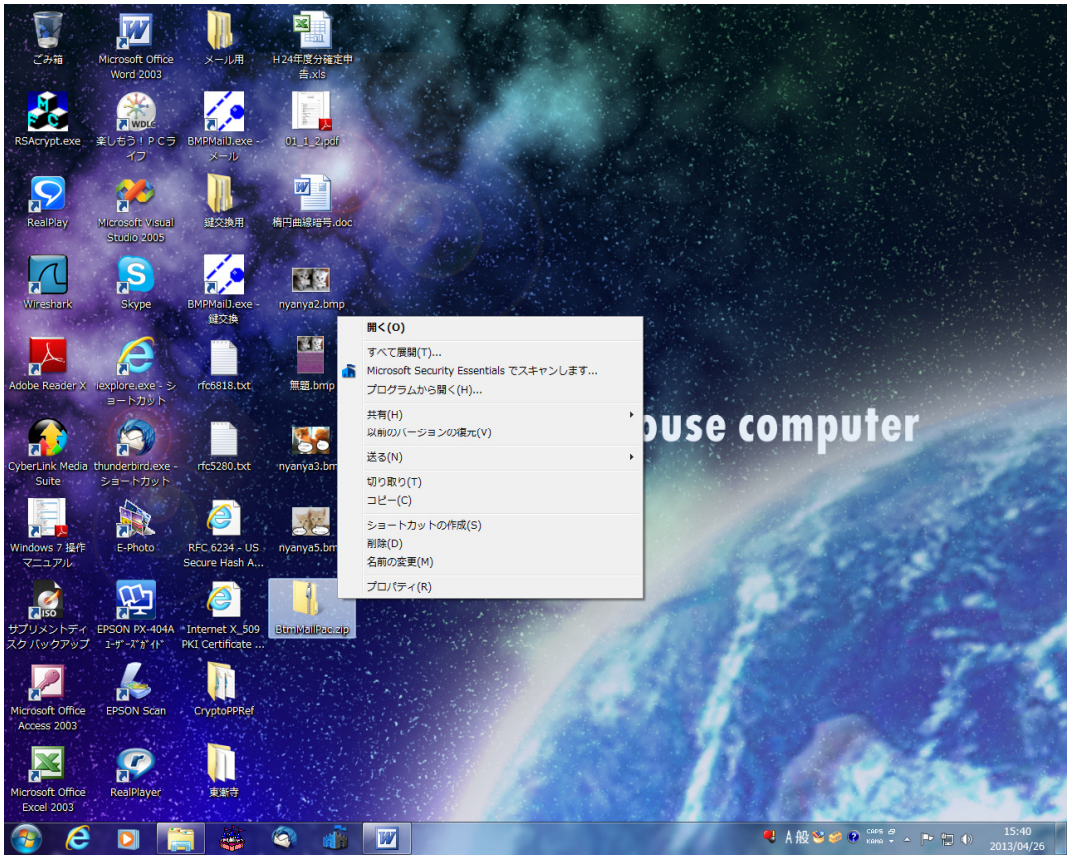
（C）：宇山　靖政

0.　動かしてみよう！（ヤフーメールの暗号化）

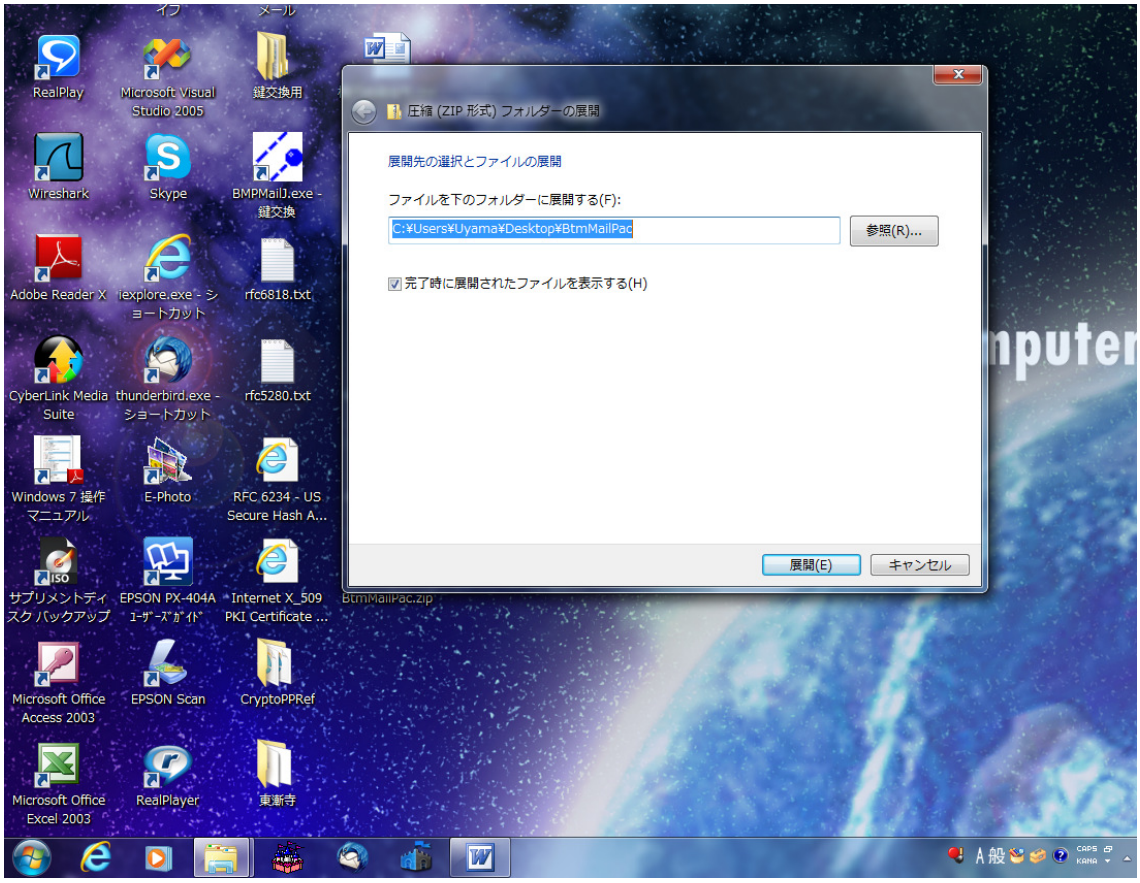
0.1　解凍

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。



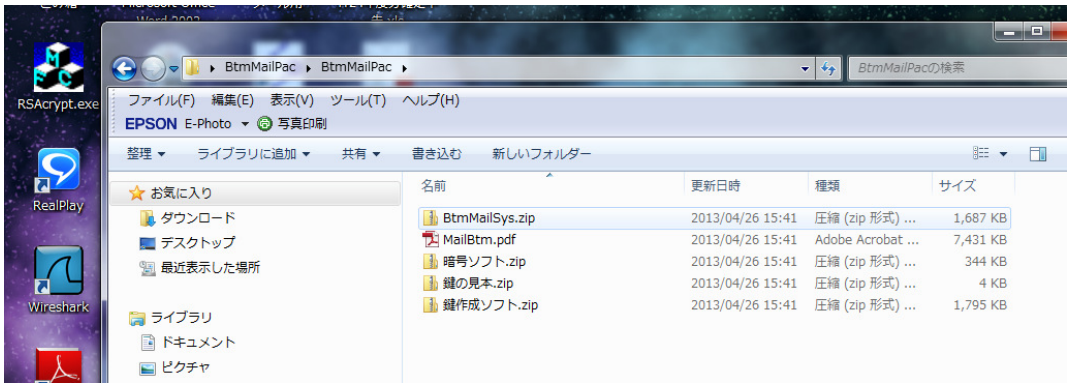
すべて展開（T）　を左クリックして、



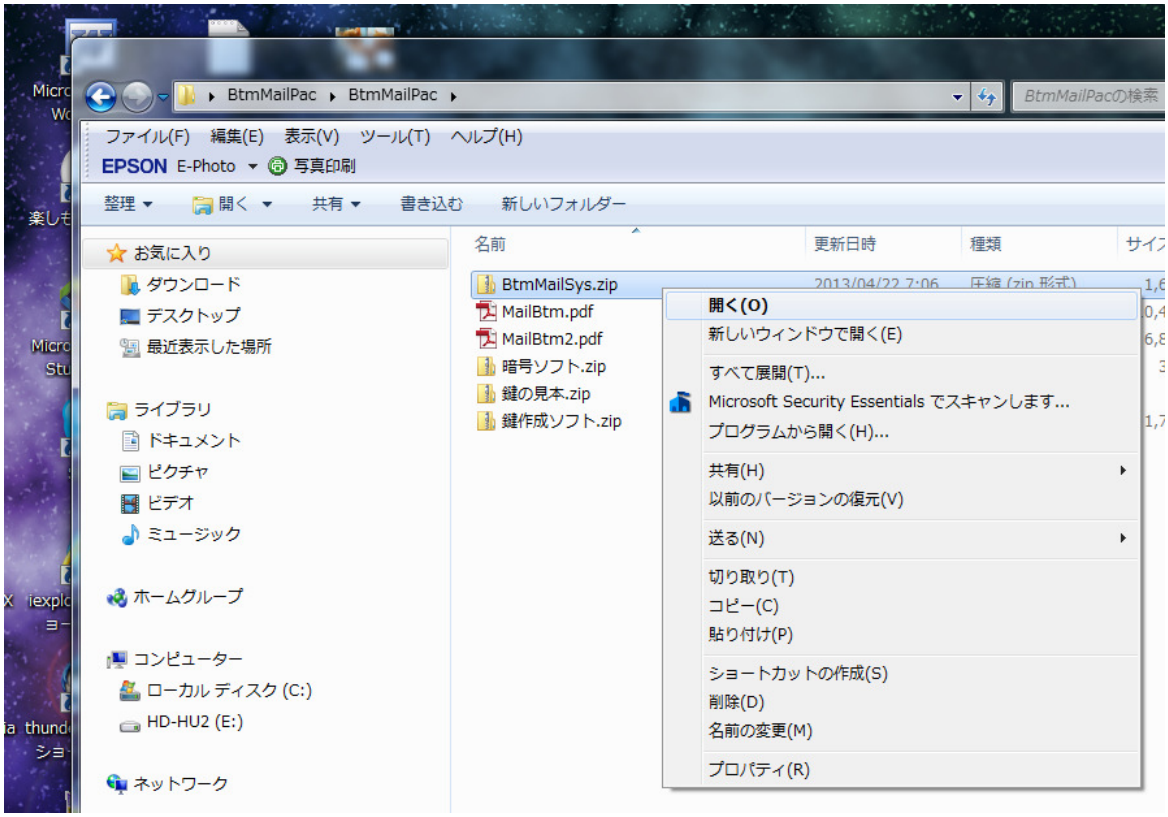
右下の展開を左クリックしてください。

WebATJPac　というフォルダが現れます。

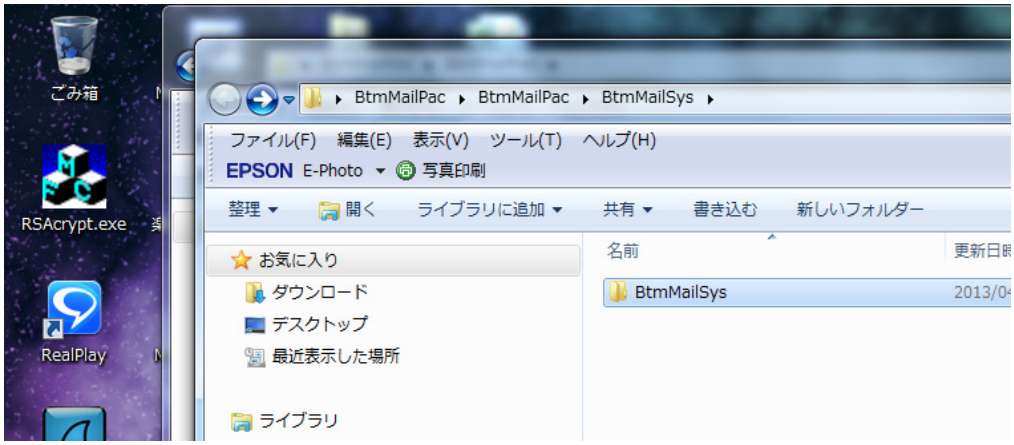
そこを、ダブルクリックすると、



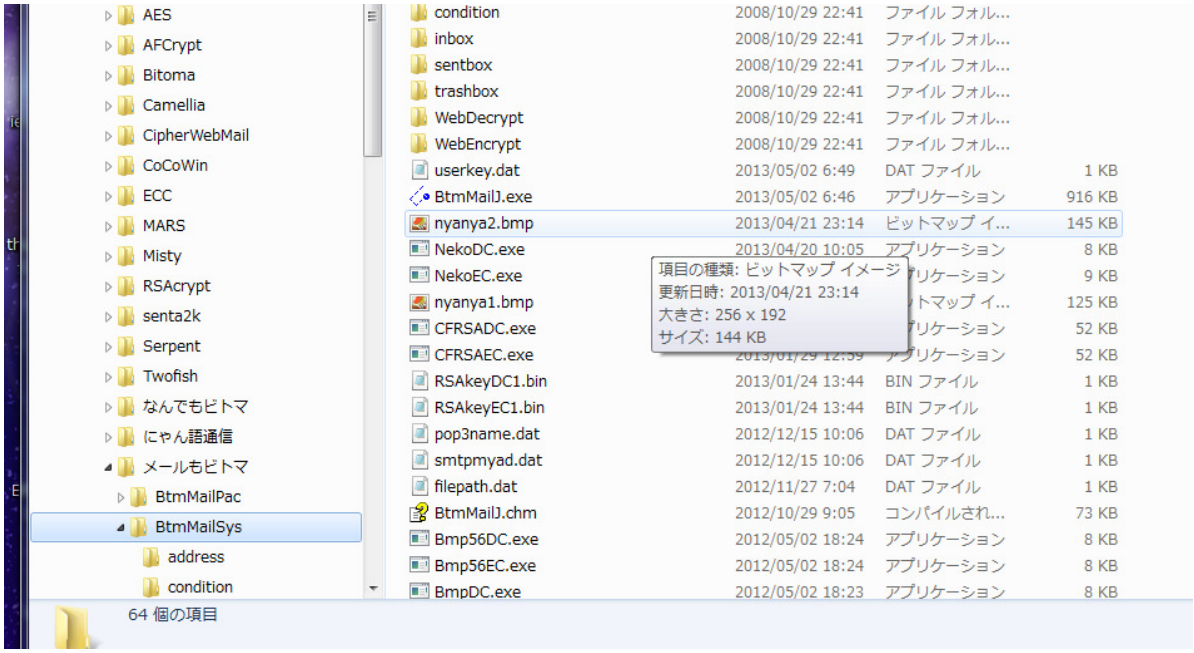
そのなかに、WebATJSys.zip が現れます。右クリックすると



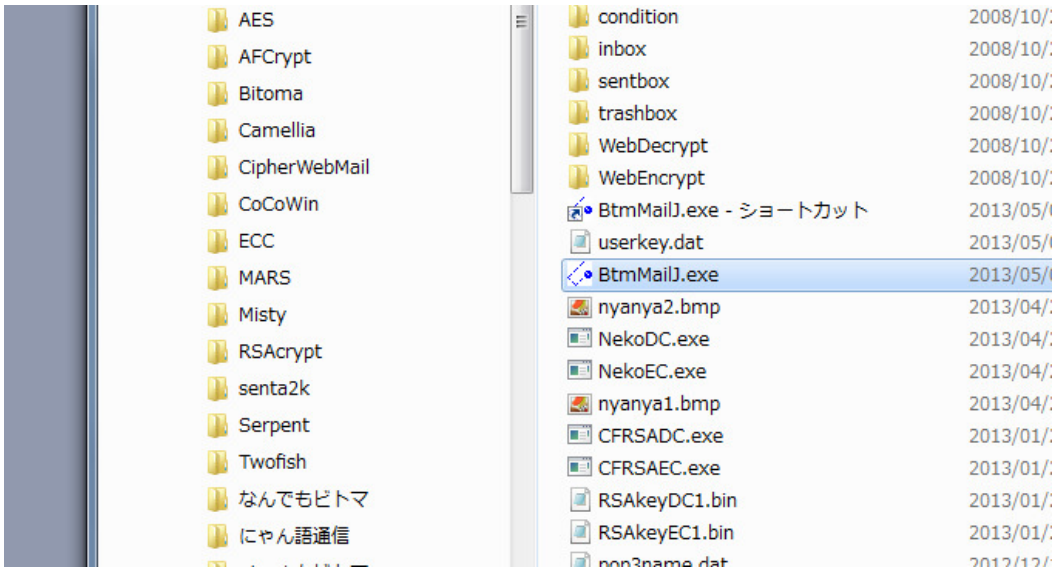
となりますので、さらに、すべて展開（T）　とし、展開してください。



WebATJSys　フォルダがあらわれます。この中の、

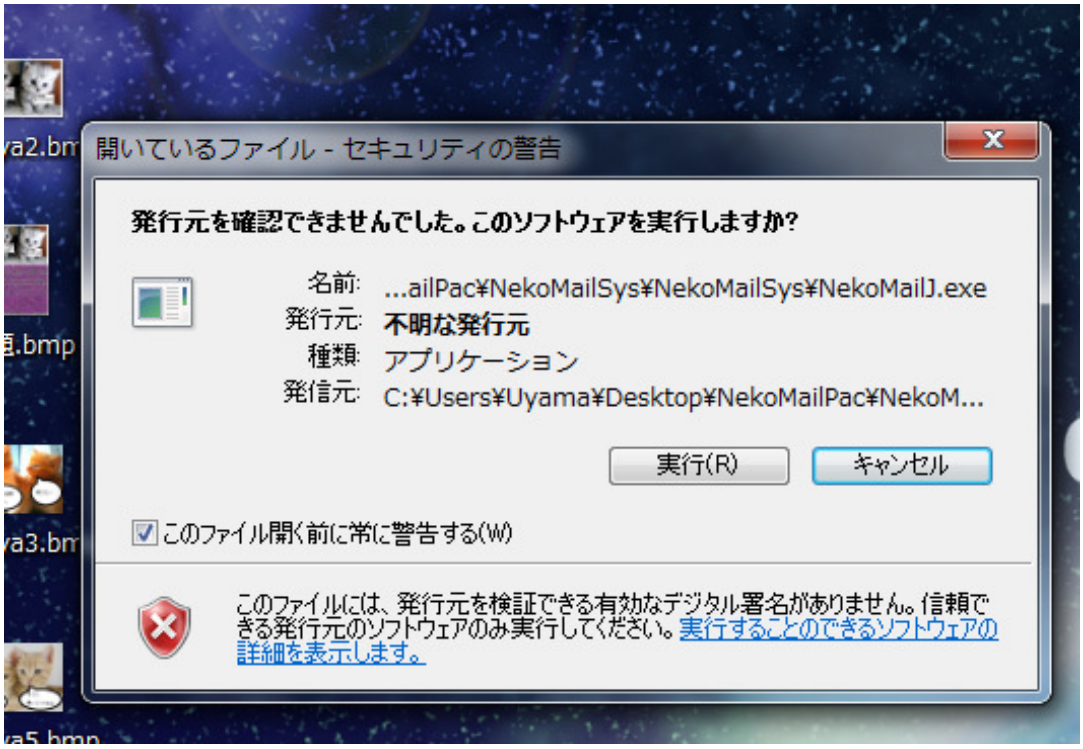


WebATJ.exe を右クリックして、ショートカットの作成を選んでください。



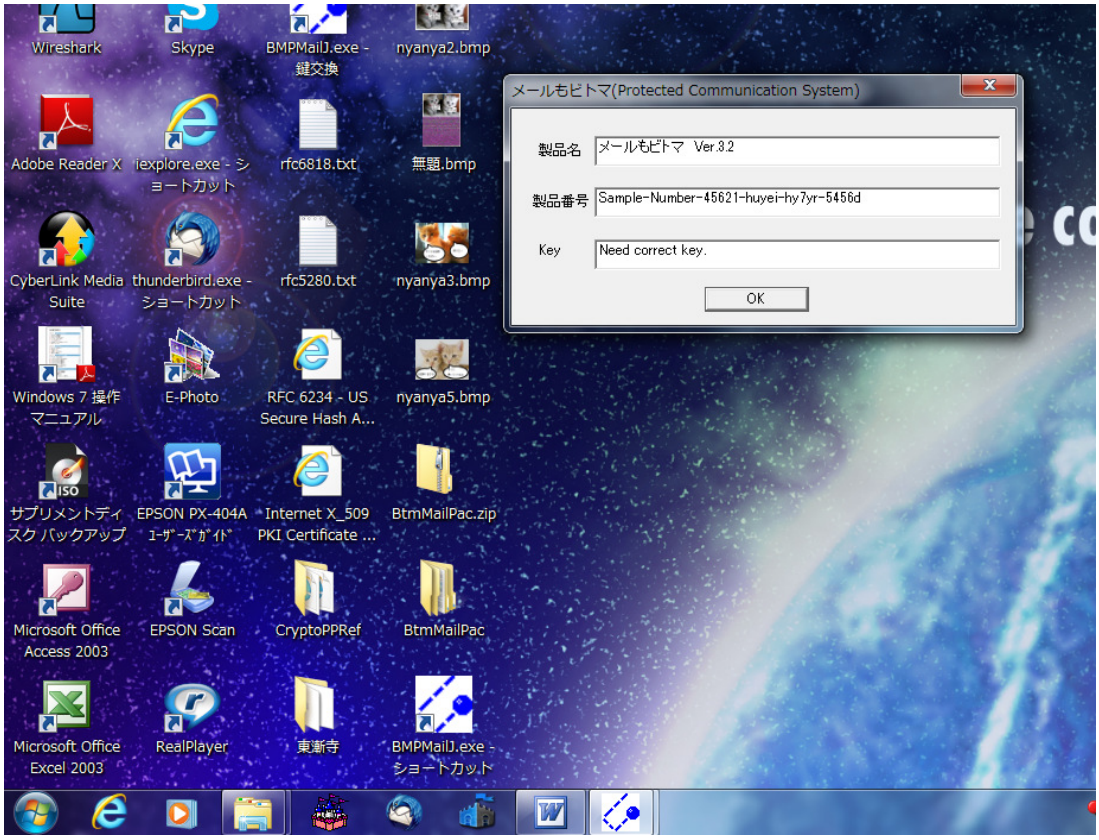
出来上がったショートカットを、デスクトップにドラッグしてください。

このショートカットをダブルクリックすると、

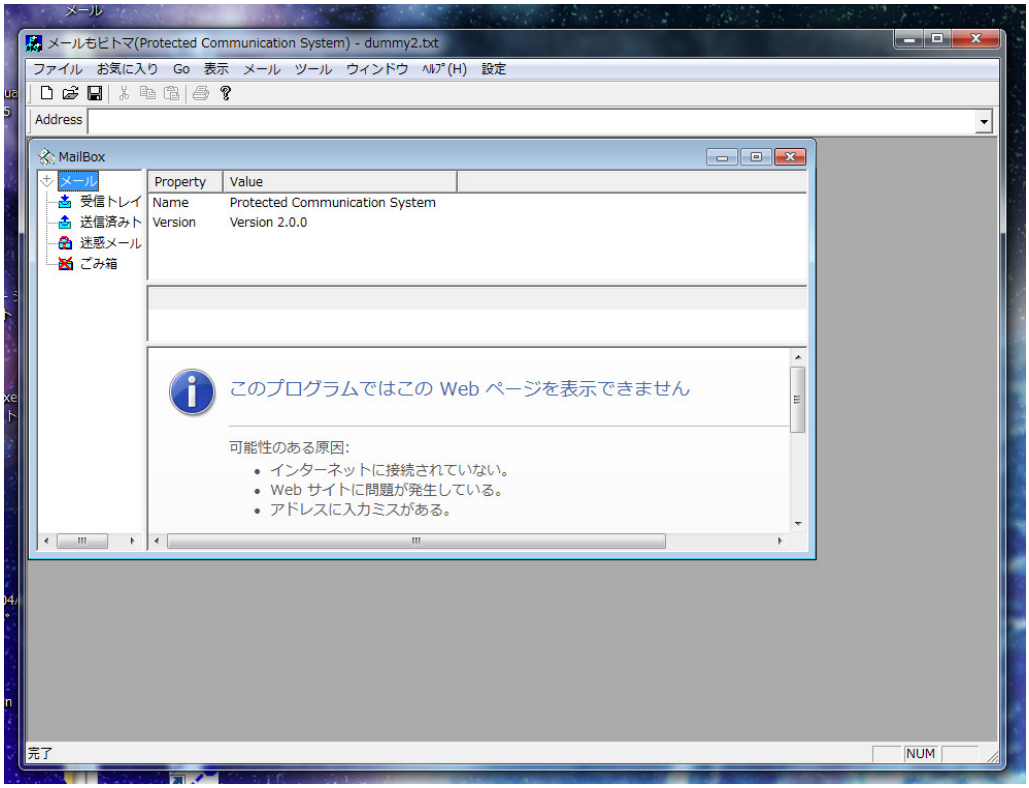


製作者が有名ではないので、警告がでます。でも、実行をクリックすると、

（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、

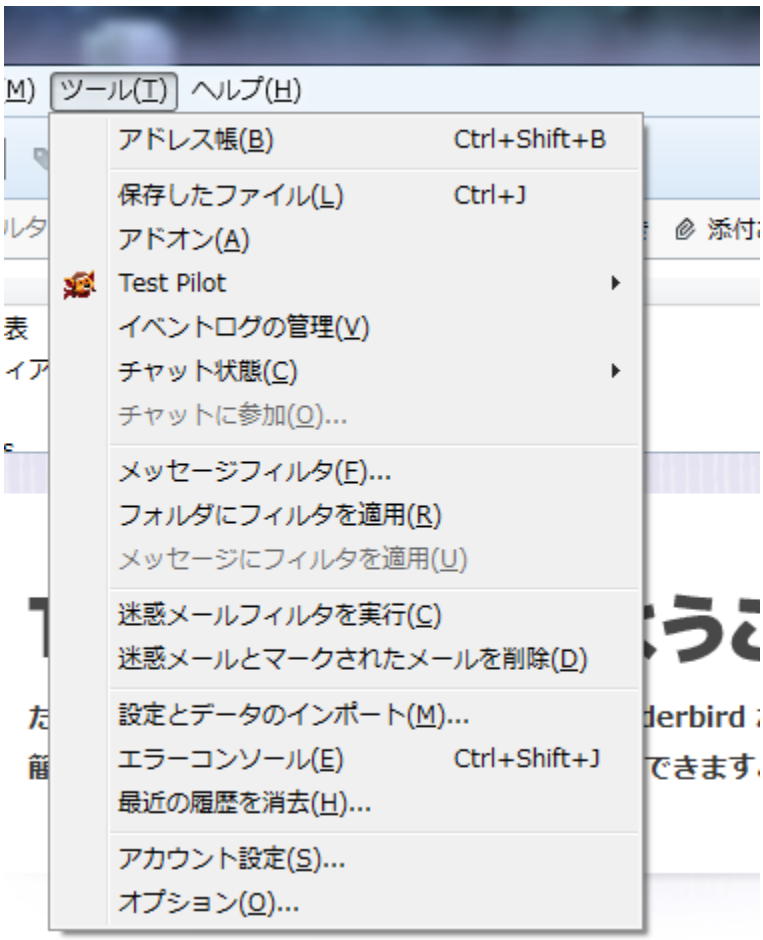


となって、ソフトが動き始めます。

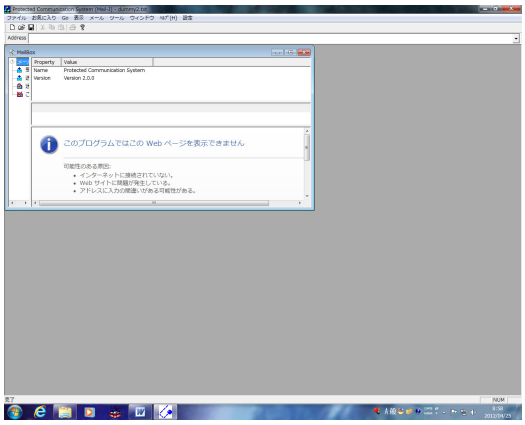
インストール：WebATJPac.zip を解凍すると、このマニュアルの他に、
WebATJSys.zip
暗号ソフト.zip
鍵の見本.zip
鍵作成ソフト.zip
が現れます。WebATJSys.zip を解凍すると、“WebATJSys”フォルダが出来ます。このフォルダをデスクトップ等の適当な場所に置いてください。
“WebATJ.exe”へのショートカットを作成してください。
起動後に、SMTP-AUTH、SMTP、POP３サーバーの設定をします。

0.2　SMTP-AUTH、SMTP、POP3 の設定

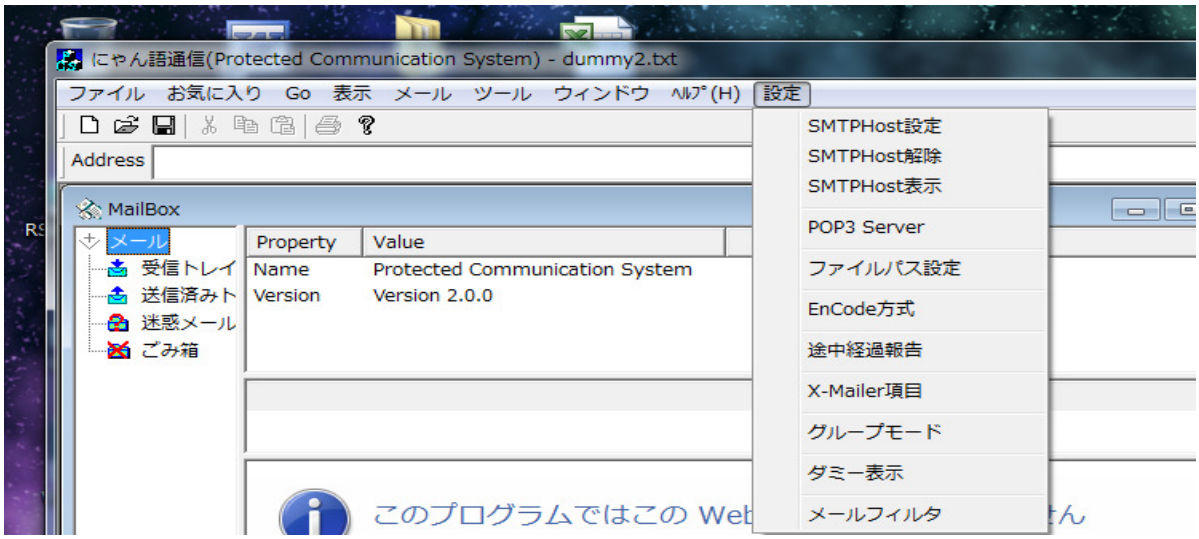
他のメールソフトの、アカウント設定を参考にすると楽に出来ます。下は、サンダーバードの場合です。ツールからアカウント設定を選んでその内容を見ながら設定してください。



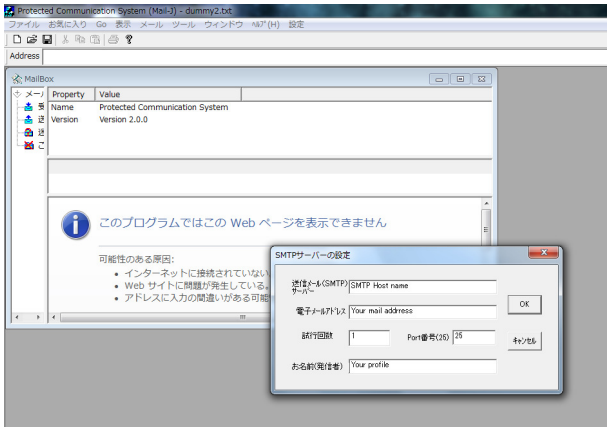
起動すると、最初にユーザー確認のメッセージが出ます。OK をクリックします。すると次の画面が現れます。



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。

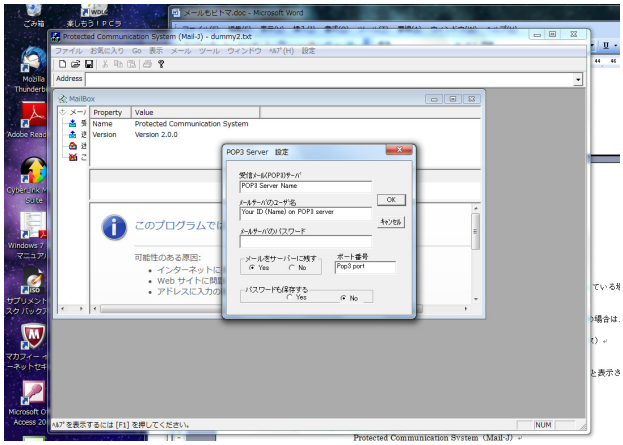
Port 番号は SMTP では 25、SMTP-AUTH では 587 です。

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。

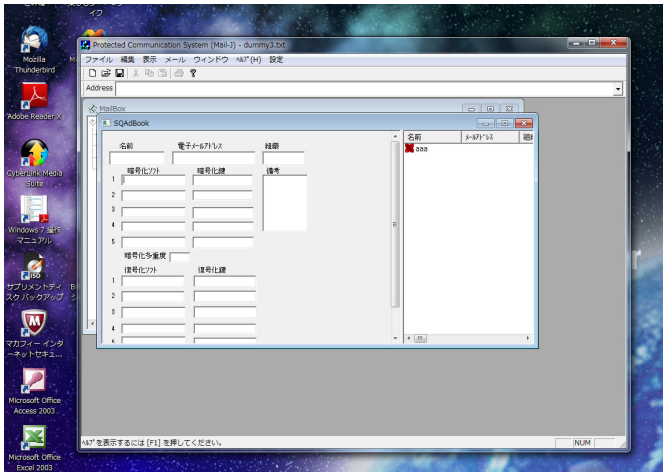
さらに、POP3 サーバーの設定です。



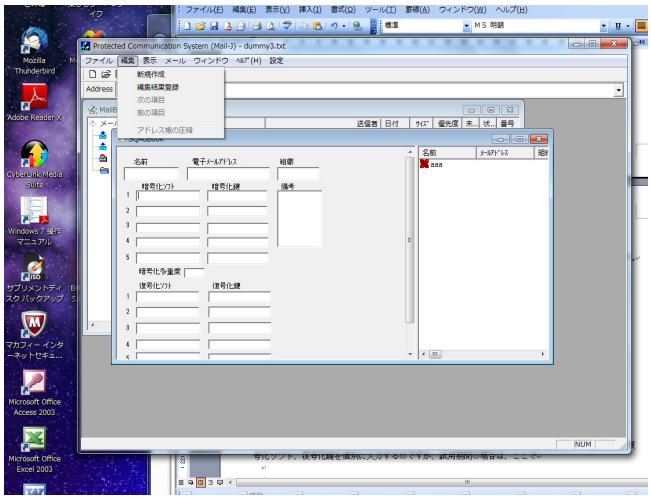
受信メール(POP3)サーバー：efg.xyz.ne.jp　　（@の右側）
メールサーバーのユーザー名：abcd　　（@の左側）
メールサーバーのパスワード：　これは、プロバイダーからの書類にあるものです。
ポート番号：110
としてください。
メールはサーバーに残す設定にして、普段のメールソフトで処理してください。
パスワードも保存してください。

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

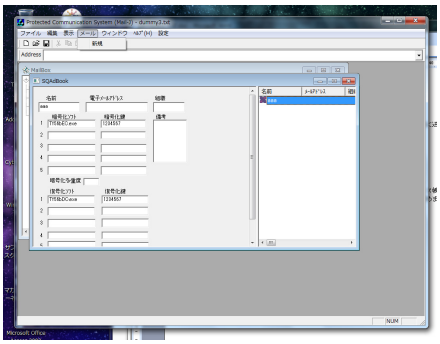
復号化ソフト　Bmp56DC.exe
復号化鍵　1234567
とします。(試用期間中は自動的に入力されます。)

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。

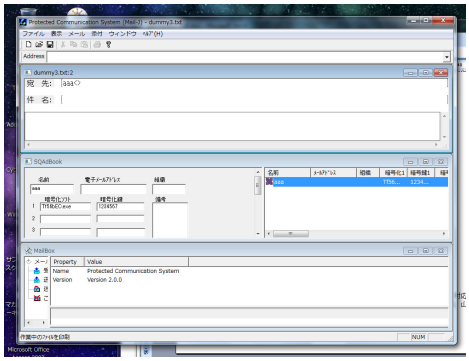
これで暗号通信ができます。最初は自分宛に、そして自分のフリーメールアドレス宛に送ってみましょう。

0.4　暗号メール送信

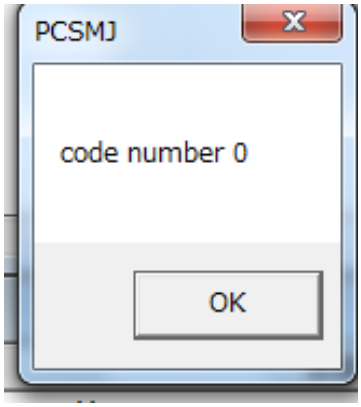
アドレス帳の右側で、メールを送る相手をクリックします。



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。

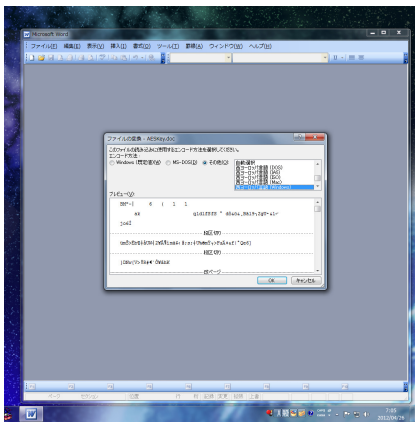
ただし、本文の内容は暗号化されますが、件名は暗号化されません。
添付ファイルの内容は暗号化されますが、そのファイル名は暗号化されません。
暗号化されたときのデータ形式は、暗号化の最後に Bmp56EC.exe を使ったときはビットマップ形式になっています。

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。

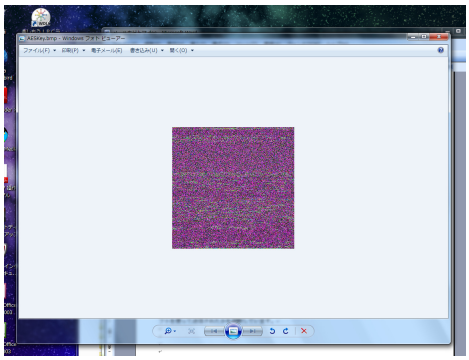
　復号化ソフト復号化鍵が送信者の暗号化に対応してきちんと設定されていなくてはなりません。

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



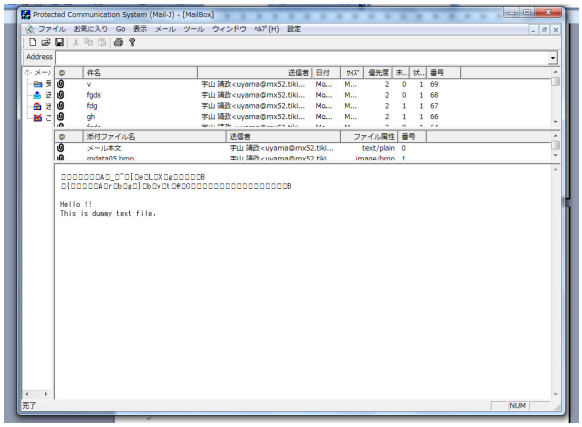
となって、データ形式がビットマップ形式になっていることが分かります。

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。

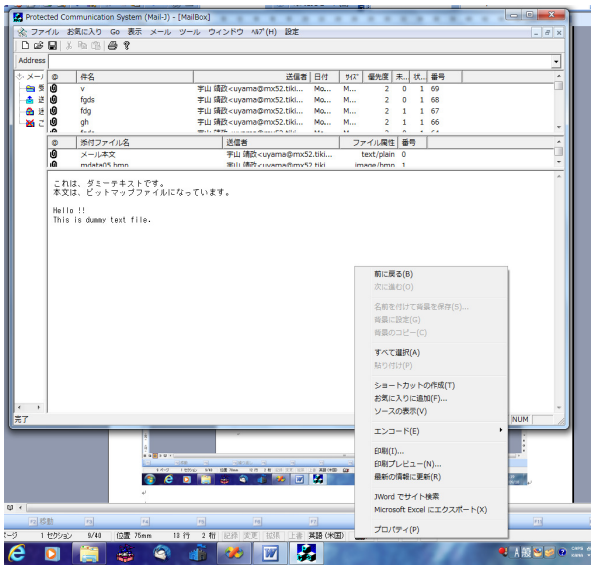
同じメールアドレスから送信されたものでも、このメーラーを使った場合は自動的に復号化されますが、別のメールソフトから送信されたものは復号化されないで普通に表示されます。内部で、どんなメールソフトを使って送信されたかを判断しています。

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。

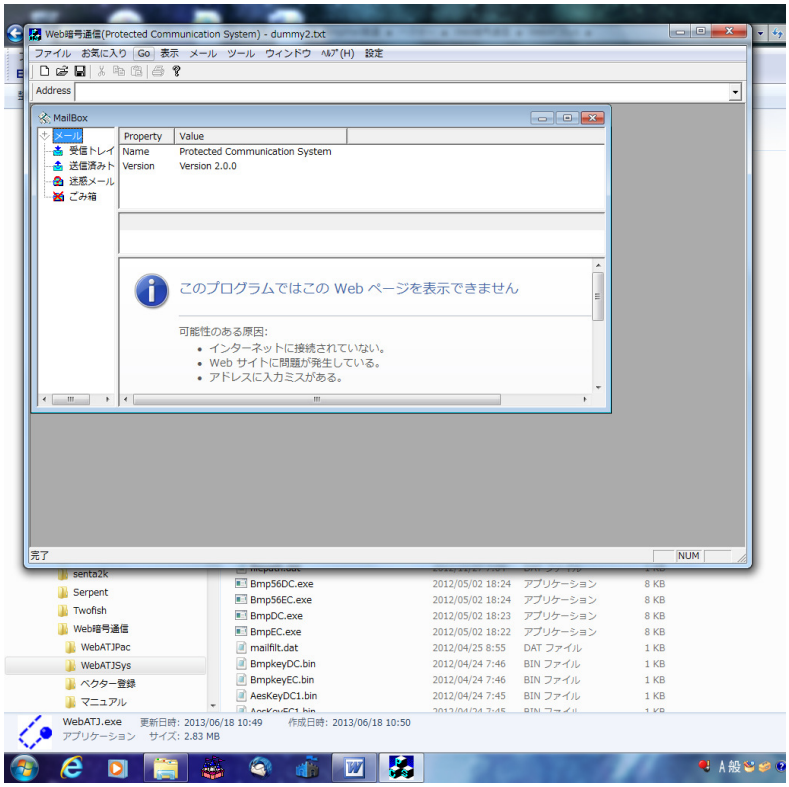
0.7　暗号化したヤフーメールの送信と受信

2.2　(Web)フリーメールの暗号化

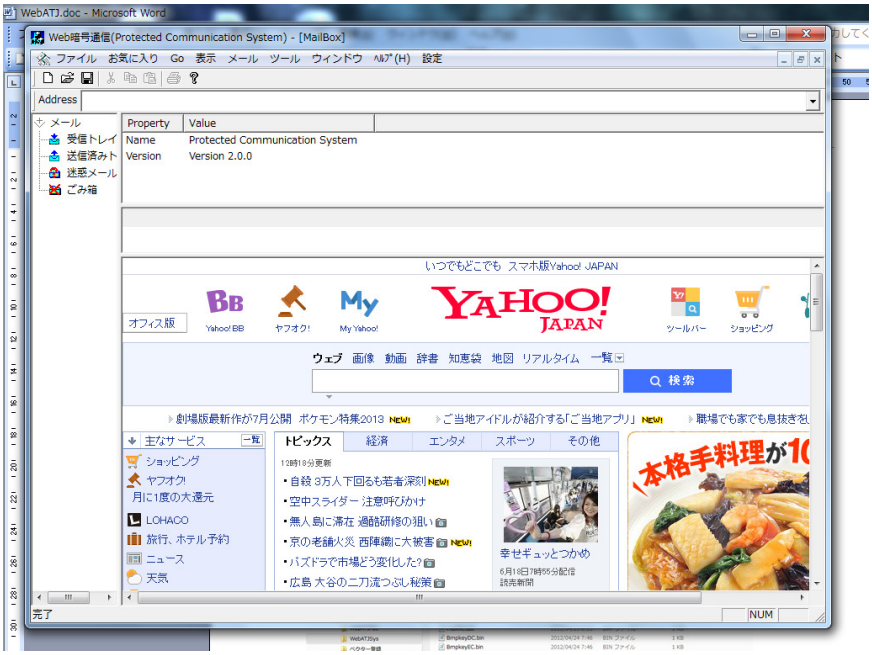
2.2.1 ヤフーメールの暗号化

インターネットエクスプローラ（IE）をつかって、ヤフーメールを操作する場合にかぎり、メールを直接的に暗号化できます。

ただし、受信者のアドレス、暗号化ソフト、暗号化鍵、復号化ソフト、復号化鍵を前もってアドレス帳へ登録しておくことが必要です。

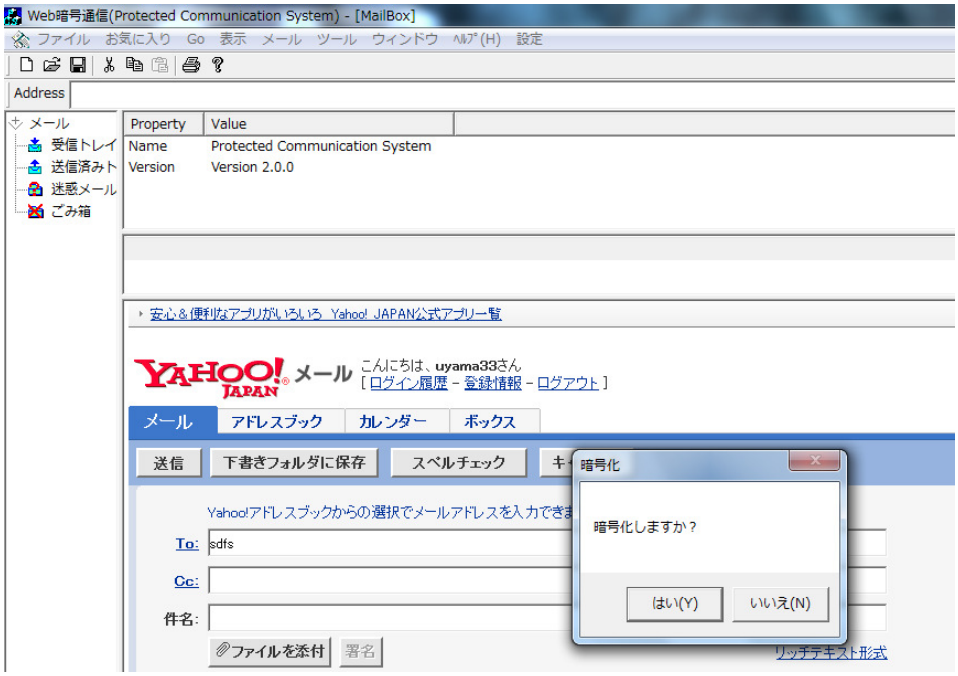


起動したら、GO－スタートページ　とすると、



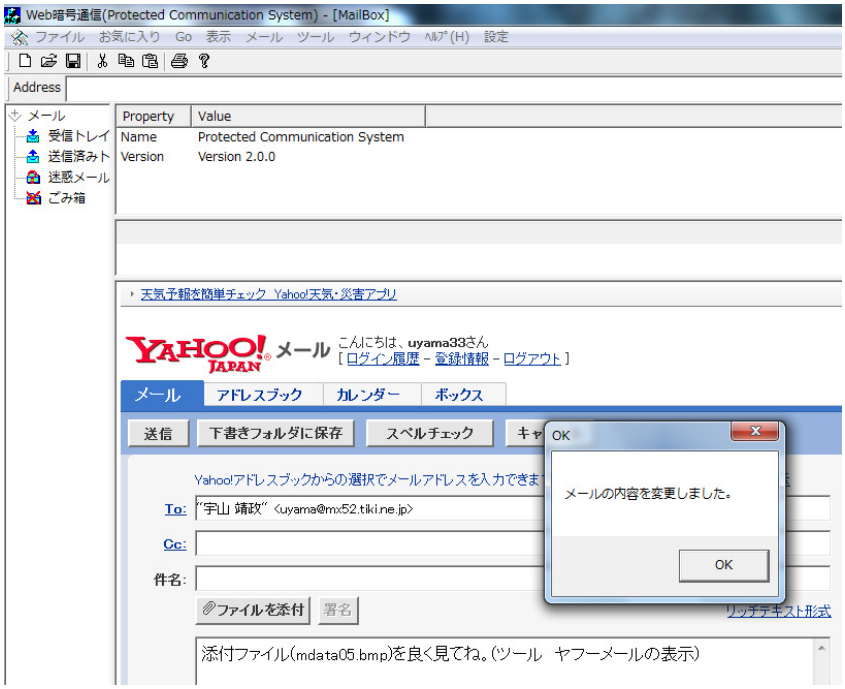
となります。右上の□をクリックして最大化して下さい。

ヤフーにログインしてください。



あて先、送信するメールの内容の入力が終わったら、メールの本文の上をダブルクリックして下さい。

メール本文を暗号化するか否かを聞いてきますので、はい　をクリックすると、



送信先がアドレス帳が正しく設定されていれば、

0． メール本文は、
添付ファイル(mdata05.bmp)を良く見てね。(ツール ヤフーメールの表示)

1． 入力してあった、メールの内容は、アドレス帳の設定に従って暗号化されて、
Mdata05.bmp というファイルになります。

2． ファイルを添付 ボタンをクリックして、mdata05.bmp を添付します。

これで、ヤフーメールのサーバーには、
添付ファイル(mdata05.bmp)を良く見てね。(ツール ヤフーメールの表示)
という本文と、
添付ファイル mdata05.bmp
が送られることになります。

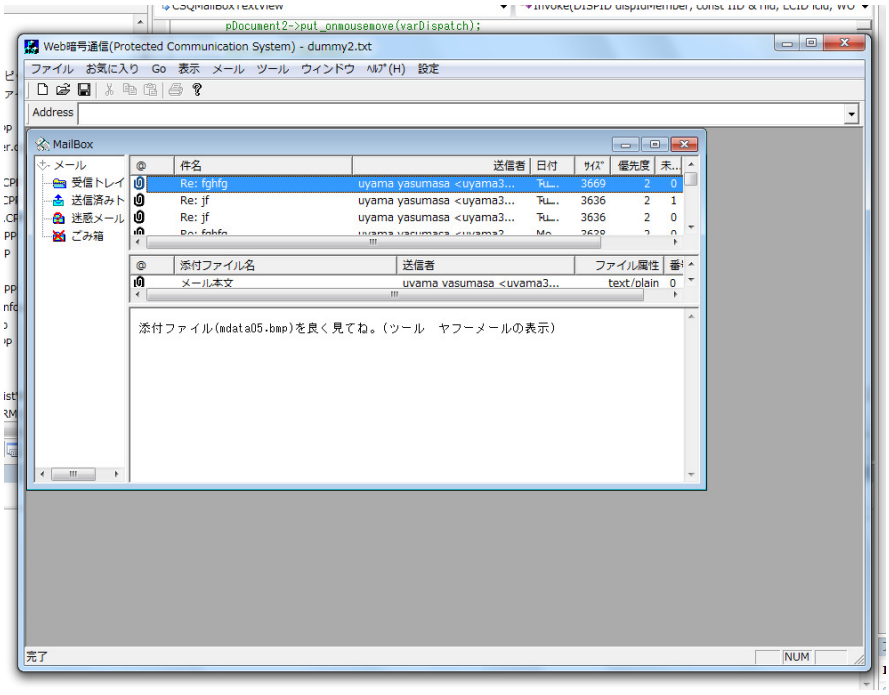
暗号化ソフトと暗号化鍵は 5 段階まで自由に設定できますので、ID とパスワードを乗っ取られても、メールの内容は読まれることはありません。

2.2.2　ヤフーメールの復号化

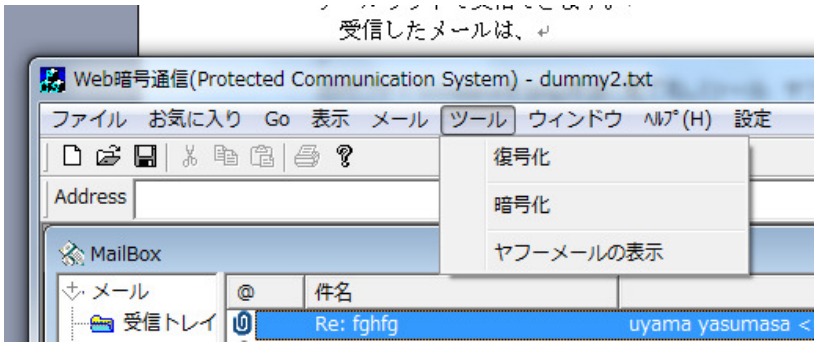
　暗号化されたヤフーメールが、自分のプロバイダーでのメールアドレスに届いた場合は、このメールソフトで受信できます。
　受信したメールは、

添付ファイル(mdata05.bmp)を良く見てね。(ツール　ヤフーメールの表示)

と表示されています。

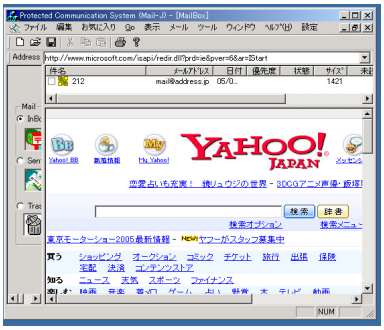


　ツール　ヤフーメールの表示
とすれば、



　表示されている文章が、自動的に変更されて本来のメールの内容が読めることになります。
(mdata05.bmp　が自動的に復号化されます。)

2.2.3　フリーメールの復号化



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。

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になります。

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

3．　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

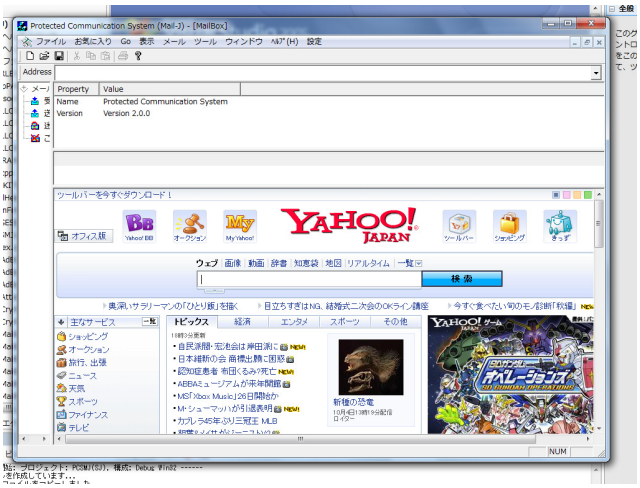
	暗号化ソフト	暗号化鍵	
1	cmlEC.exe	cmlkeyEC.bin	（試用期間は、Bmp56EC.exe、1234567）
2			
3			

	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。

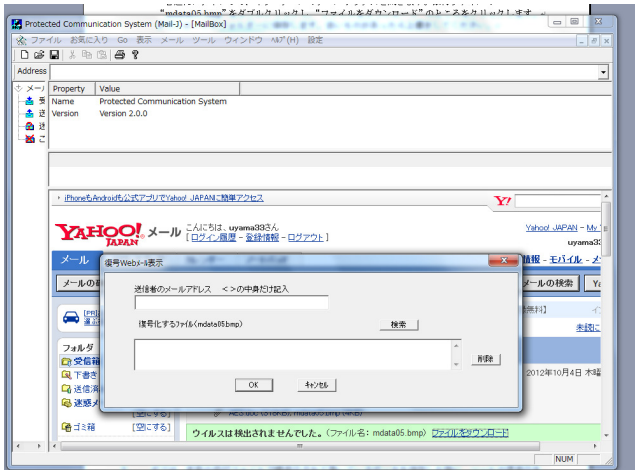
4．　メール本文は、次の手順で直接表示できます。

（4-1）Go　－　Start Page　とすると、



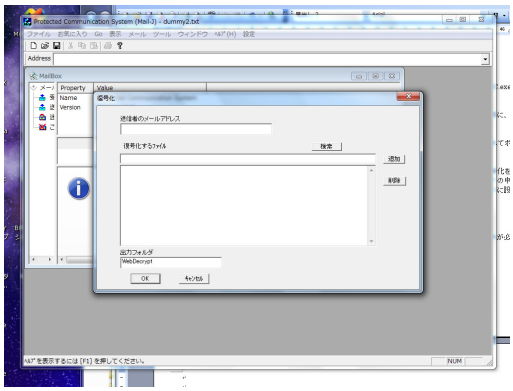
となって、インターネットエクスプローラと同じ画面が表示されます。
　普通にログインして、ヤフーメールのメールボックスを開きます。添付ファイルの“mdata05.bmp”をクリックし、“ファイルをダウンロード”のところをクリックします。ダウンロードのフォルダに保存します。古いものがあったら上書きしてください。
　さらに、送信者のメールアドレスをコピーしてください。

（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ーにある“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。