集中企画

高度なメールの使い方FAQ

1. パソコン通信とインターネットでバイナリーファイルはやり取りできるか。
2. メールのプライバシーは守れるのか。
3. 新しいメールソフトに替えるとき、前のデータは移行できるのか。
4. 会社のパソコンと自宅のパソコンでメールは共有できるのか。

電子メールのここが知りたい

E-mail

Q1：パソコン通信とインターネットでバイナリーファイルをやり取りできますか？

Frequently Asked Question

A：面倒だけどできます。

回答：いとう くにお

大手パソコン通信ネットのほとんどがインターネットとの接続を果たした結果、いまではインターネットやほかのパソコン通信ネットとの間で自由に電子メールがやり取りできるようになっている。パソコン通信ネットからインターネットのメーリングリストに参加しているという人も少なくない。

しかし、そのように電子メールを使いこなしていても、いざバイナリーファイルをネットワーク経由で送るというときには、インターネットではなくパソコン通信のバイナリーメール機能に頼るという人が多いようだ。筆者の知る印刷・出版業界では「画像データは通信で送っておきます」というと、ほとんどの場合それはニフティサーブのバイナリーメールで送ることを意味する。

それではインターネットとパソコン通信の間ではバイナリーファイルをやり取りすることはできないのだろうか？

この答えは「できる」だ。インターネットとパソコン通信の間ではバイナリーファイルもテキスト化することで送信できるし、その逆も可能になっている。つまり、インターネットの電子メールソフトが自動的に行っている、バイナリーファイルのテキスト化と復元（エンコード／デコード）を、変換ソフトを使って手動で行えばいいわけだ。

ただし、パソコン通信ネットには、送信できるメールの行数制限など、ネット固有の制限があるので注意が必要だ（表1参照）。たとえば、ニフティサーブでは送受信できるテキストメールは78文字×3000行までとなっている。これはバイト数に換算すると230Kバイト程度なので、あまり大きなファイルは一度に送れないということになる。ニフティサーブ内なら3Mバイトまで送れるのだが。

パソコン通信ネットによっては、インターネットとのバイナリーファイルのやり取りに配慮した機能をもっているところもある。その代表がASAHIネットとPeopleだ。両ネットは、ネット内の会員どうしの場合とまったく同じ手順でインターネットとバイナリーファイルをやり取りできる。これは両ネットのホストコンピュータが、MIME（Base64）というエンコード方式でバイナリーファイルのテキスト化および復元を自動的に行うようになっているからだ。MIME（Base64）に対応した電子メールソフトなら、ASAHIネットやPeopleから送られたバイナリーファイルを添付ファイルとして認識してくれるし、逆にその電子メールソフトから送ったMIME（Base64）形式のメールは、パソコン通信ネット内のバイナリーメールと同じようにASAHIネットやPeopleの会員に届く。

PC-VANも送信のみだが、同様の機能を持っている。PC-VANからバイナリーファイルをインターネットへ送信するとUUENCODEというエンコード方式でテキスト化される。

インターネットとのバイナリーファイルのやり取りに関しては、大手のパソコン通信ネットの中でニフティサーブがもっとも後手に回っている。送信の場合も受信の場合も、変換ソフトを使ってのエンコード／デコードの作業が必要だ。その一連の手順について、次ページから詳しく説明する。

表1●大手パソコン通信ネットのインターネットメール機能

	メール1通の長さ制限 送信時	受信時	バイナリーデータの自動変換方式 送信時（encode）	受信時（decode）	その他インターネットとのやり取りでの注意
NIFTY-Serve	78字×3000（行）	78字×3000（行）	×	×	宛先メールアドレスに「INET:」を付けて送信
PC-VAN	500Kバイト	500Kバイト	uuencode	×	宛先メールアドレスに「INET #」を付けて送信
ASAHI-NET	80字×1000（行）	80字×1000（行）	Base64	Base64	送信時はメール1通に64Kバイト以下のファイルを最高5つまで添付可能
People	80字×1000（行）	特になし	Base64	Base64	送信時はメール1通に200Kバイト以下のファイルを最高2つまで添付可能
アスキーネット	127字×5000（行）	特になし	×	×	

ニフティサーブからインターネットへバイナリーファイルを送信

Windows95でニフティサーブからインターネットにバイナリーファイルを送る手順を説明する。ほかのOSの場合もおおよその手順は同じだ。大まかに言うと、次の3ステップになる。

❶バイナリーファイルの圧縮
❷変換ソフトによるテキスト化(エンコード)
❸インターネットに送信

バイナリーファイルの圧縮は、ファイルサイズを小さくすることで通信時間を短縮し、課金を抑える意味があるが、パソコン通信ネットのファイルサイズの制限を超えないようにするうえでも有効だ。

step1:WinZipで圧縮

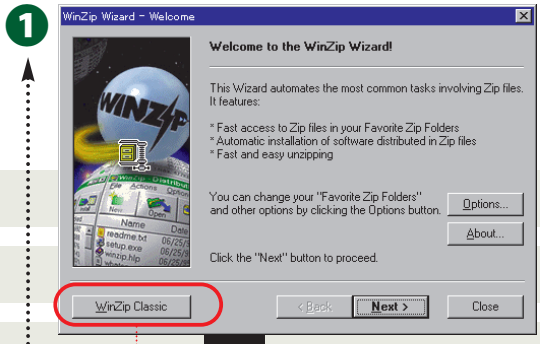
❶まず圧縮ソフトを起動する。Windows95ならシェアウェアのWinZipが使いやすい。WinZipは最新のバージョン6.1からウィザード形式と従来の形式(WinZip Classic)の2つのインターフェイスが選べるようになっているが、圧縮作業ではWinZip Classicを使う必要がある。

❷WinZip Classic形式のウィンドウ。ここで「New」ボタンをクリックする。

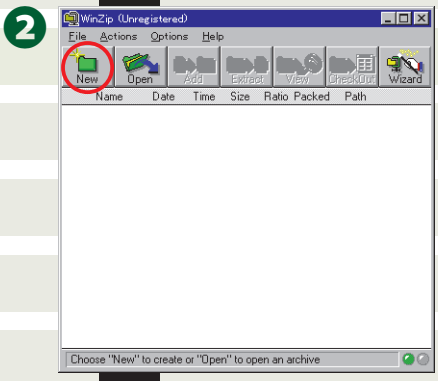
❸圧縮ファイルを作るフォルダーとファイル名を指定する。ファイル名に漢字(全角文字)を使うと文字化けする可能性があるので、半角英数字にしておくのが無難だ。

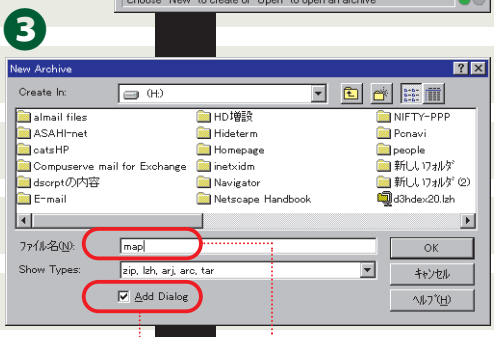
❹圧縮したいファイルをダイアログでクリックし、「Add」ボタンをクリックする。

❺選択したファイルが圧縮され、WinZipのウィンドウに表示される。これでWinZipを終了する。



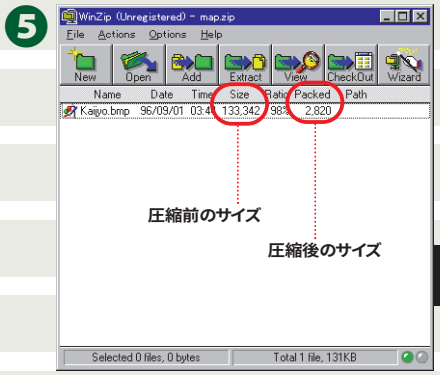
起動時にウィザード画面が表示された場合は、このボタンをクリック。ウィザードでは圧縮作業は行えない。



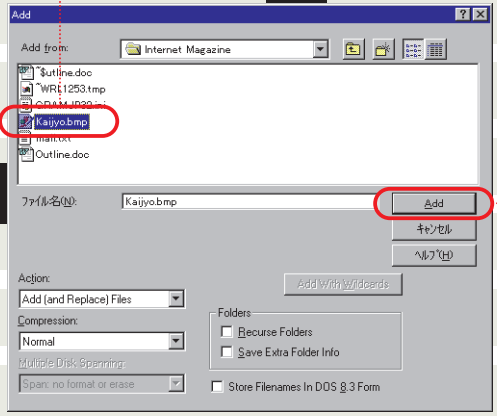


このファイル名を入力。拡張子を付けなければ自動的に.zipが付加される。

ここにチェックマークが付いていると、このダイアログの次に圧縮対象を指定するダイアログが表示される。

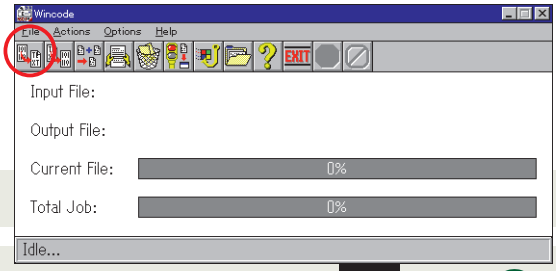


圧縮したいファイルをクリックし選択。



選択したファイルが圧縮される。

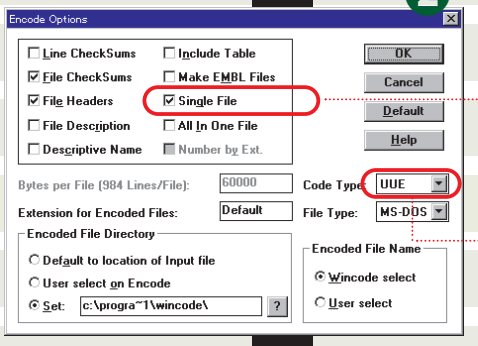
step2：Wincodeで変換（エンコード）



❶WinZipで作成した圧縮ファイルをテキスト化（エンコード）するためにWincodeを起動する。Wincodeはエンコード／デコード用ソフトの定番フリーソフトだ。

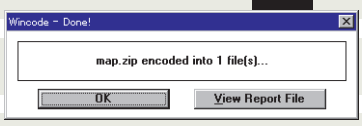
❷「Options」メニューから「Encode」を選択し、エンコード方式を指定する。受け手の電子メールソフトが対応している方式を選択する必要がある。はじめはUUE（UUENCODE）になっている。続いて❶の画面のツールバー左端のアイコンをクリックして、エンコードするファイルを選択する。エクスプローラからWincodeのウィンドウにファイルをドラッグする方法もある。

❸これが出たらエンコードは終了。はじめの設定では、エンコードされたファイルはWincodeのフォルダーの中にできている。ファイルの拡張子は、UUENCODEでは.uue、Base64では.b64となる。



パソコン通信の制限によってファイルを分割して送りたいときは、このチェックマークをはずす。ただし、分割した場合は受け手の電子メールソフトによっては正しく受信できないこともある。

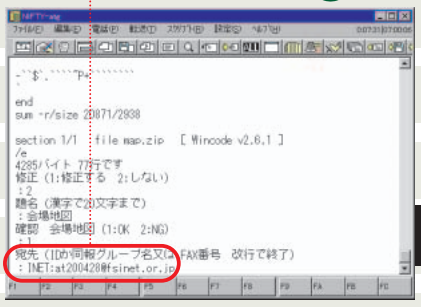
エンコード方式を選択する。



step3：送信

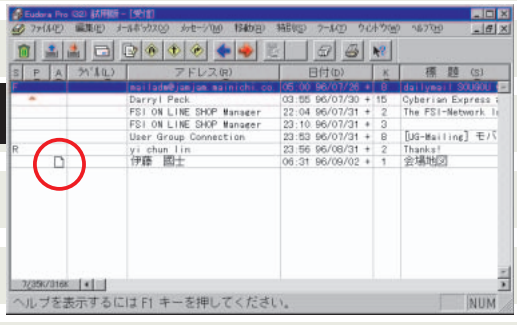
通信ソフトを起動し、ニフティサーブに接続する。この例ではシェアウェアの秀Termを使う。ニフティサーブに接続してプロンプト＞が表示されたら「MEXP」と入力する。これによりメールの行数制限が300行から3000行に拡張される。この設定はログインするごとに設定する必要があるので注意。ちなみにNIFTY ManagerのWindows3.1版では300行以上のメールは送れない。Windows95版なら設定しなくても3000行送ることができる。

ニフティサーブからインターネットへのメールの宛先は先頭に「INET:」を付ける。

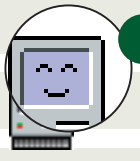


❶ニフティサーブ上でメールを作成する。エンコードによってできたファイルの内容を本文として入力する。秀Termの場合は、「転送」メニューの「テキスト送信」によりテキストファイルの内容を先頭から順に入力することができる。そのような機能のない通信ソフトの場合は、ファイルをテキストエディターで開いてコピーし、通信ソフトにペーストして送信する。

❷インターネット側で受信すると、添付ファイルとして認識される。



マックならこのツール



DropStuff

圧縮ソフトとしてはStuffItシリーズのものが使いやすい。中でもシェアウェアのDropStuffは、ファイルをDropStuffにドラッグして重ねるだけで、ファイルの圧縮とエンコード（UUENCODE）を自動的にやってくれるので便利。ただし、圧縮方法はマックでしか使われていないStuffIt形式なので、相手がマックのとき用と考えたほうがいいだろう。

MacLHA

Windowsマシンへ送る場合なら、圧縮ソフトとしてはMacLHAが安心だ。DOSやウィンドウで広く使われている.lzh形式の圧縮ファイルが作れる。

Mpack

エンコード／デコード用のソフトとしてはMpackがある。これはMIME（Base64）専用だ。

インターネットから送られてきたバイナリーファイルをニフティサーブで受信

インターネットから送られたバイナリーファイルをニフティサーブで受信し、元のバイナリーファイルに復元する手順を説明する。Windows95を例とするが、ほかのOSの場合も基本的な手順は同じだ。送信の場合と同じく、大きく分けて3つのステップを経る。

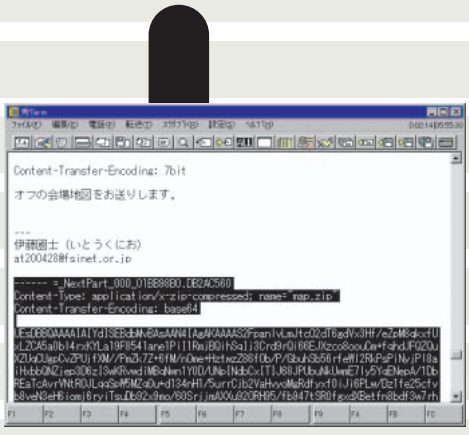
❶ パソコン通信でエンコードされたデータを受信
❷ 変換ソフトでバイナリーファイルに復元（デコード）
❸ 圧縮されている場合はファイルを伸張

```
3 INET GATE      INE00103      96/09/02 10:13
  題名：会場地図

Date: Mon, 2 Sep 1996 09:25:53 +0900
From: ITO Kunio <at200428@fsinet.or.jp>
To: '伊藤國士'<mgh00253@niftyserve.or.jp>

------ =_NextPart_000_01BB98B0.DB2AC560
Content-Type: text/plain; charset="ISO-2022-JP"
Content-Transfer-Encoding: 7bit

オフの会場地図をお送りします。
---
伊藤國士（いとうくにお）
at200428@fsinet.or.jp

------ =_NextPart_000_01BB98B0.DB2AC560
Content-Type: application/x-zip-compressed; name="map.zip"
Content-Transfer-Encoding: base64

UEsDBBQAAAAIAIYdlSEBdbMvBAsAAN4lAgAKAAAAS2FpanlvLm
JtcO2dT6gdVx3Hf/eZpM8qkxfUxLZCA5a0bl4rxKYLa19F8541ane1
Pil1RmjBQihSqIj3Crd9rQi66EJXzco8oouCm+fqhdJFQZQu
XZUqCUgpCvZPUjfXM//PmZk7Z+6fM/nOme+HztwzZ86fOb/P/Gbuh
Sb56rfeWl2RkPsPiNyjPl8aUEsDBBQAAAAIAIYdlSEBdbMvBAsAAN4lAgA/
                .
                .
JavTehQ9ir7L/tN32Weyl1Rg311IhnGUnAyM8Gln9BHinZiH0V4fbpq
xlH1398xEhYu0vrJWv1ezu7fcRnsWGS61gBela08rPqOK9ZW1ev2
0vEhv6ooRJAmxMUhVK+YFubnQBQ50gQNd4EAXONAFDnSB
A13gQBc4KBf/B1BLAQIyCxQAAAAIAIYdlSEBdbMvBAsAAN4lAgA
KAAAAAAAAAAAAIAC2gQAAAABLYWlqeW8uYm1wUEsFBgAAA
AABAAEAOAAAACwLAAAAAA==sDBBQAAAAIAIYdlSEBdbMvBA
------ =_NextPart_000_01BB98B0.DB2AC560--
```

エンコードデータ（バイナリーファイルをテキスト化したもの）

メールの本文

❶



❷

step1:受信

❶インターネットから添付ファイルとして送られたバイナリーファイルは、ニフティサーブに本文＋エンコードデータの形式で届く。エンコードデータの先頭部分を見ると、そのデータがどういう方式でエンコードされているかがわかる。

begin 644: → UUENCODE
Content-Transfer-Encoding: base64 → MIME（Base64）
（This file must be converted with BinHex 4.0） → BinHex

❷ファイルが複数に分割されて届いた場合は、順番にメールを読み出していく。通信ログからエンコードデータ部分を取り出し、テキストファイルに保存する。秀Termの場合なら、受信したメールをウィンドウ内で選択し、「編集」メニューから「ファイルにコピー」を選択する。エンコードデータの前後に関係のない文字（例えば別のメールなど）が入っていてもかまわない。変換ソフトはエンコードされている部分だけを探し出してバイナリーファイルに復元するからだ。ただし複数のメールに分割されている場合は注意が必要。AL-Mailなどで分割されたメールは中間のメールにヘッダーがないため、メール間の余分な文字を削除し、1本のメールのように編集してやる必要がある。

step2:Wincodeで復元（デコード）

❶Wincodeを起動する。

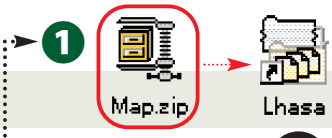
❷「Options」メニューから「Decode」を選択し、デコードするファイルのエンコード方式を指定してOKボタンをクリックすると❶の画面に戻る。
ツールバーの左から2番目のボタンをクリックし、復元するファイルをダイアログで選択すればいい。

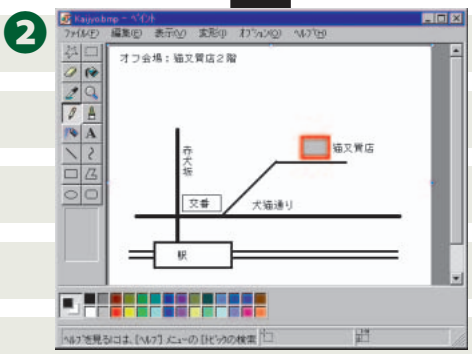
マックならこのツール

StuffIt Expander

StuffIt Expander

エンコードデータの復元と圧縮ファイルの伸張をまとめて面倒みてくれるフリーソフトウェアがStuffIt Expanderだ。BinHexとUUENCODEの復元、およびStuffItとCompact Proの圧縮ファイルの伸張が、ドラッグ＆ドロップでできる。さらにシェアウェアのDropStuff with Expander Enhancerをインストールすると、ZIPやARCなどDOSの圧縮ファイルも伸張できるようになる。

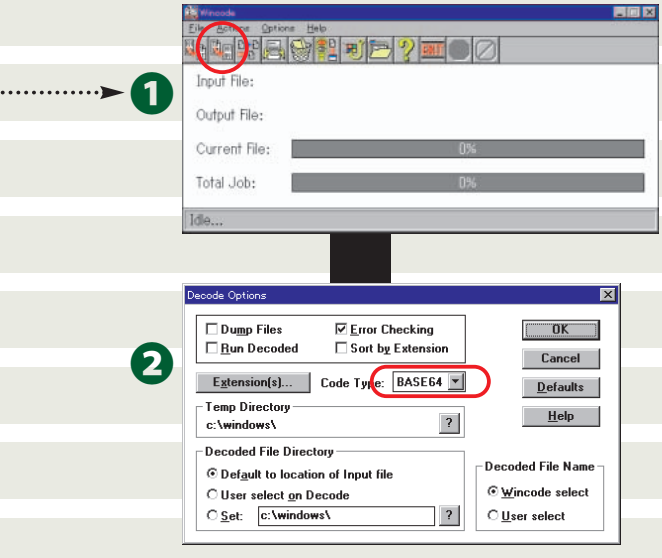




step3:圧縮ファイルの伸長

❶復元したファイルが圧縮されている場合は、伸張を行う。お勧めは、1本で.zipファイルと.lzhファイルの伸張ができるLhasa（らさ）。圧縮ファイルをドラッグしてLhasaに重ねるだけで伸張が行われる。Lhasaはショートカットをデスクトップに置いておくと便利だろう。

❷バイナリーファイルが伸張できたら、ファイルを開いて内容を確認する。



Windows ∞ Macintosh間でバイナリーファイルをやり取りするならここに注意!!!

異機種間でバイナリーファイルをやり取りするケースは少なくない。たとえばマックで作ったGIFファイルをWindowsに送るとか、WindowsのMicrosoft Wordで書いた原稿をマック側に送るといったようなケースだ。ここでは、このように異機種間でバイナリーファイルを送る場合のポイントをまとめた。

●相手の環境を考えてエンコード方式を選択する

エンコード方式は、WindowsではMIME（Base64）とUUENCODEが主流だが、マックではBinHexが主流。それを考慮し、受け手が復元しやすいエンコード方式を使うほうが親切だ。たとえばマックで広く普及しているフリーソフトウェアの電子メールソフトEudora-Jでは、BinHex以外のエンコード方式には対応していない。Eudora-Jユーザーにバイナリーファイルを送るにはBinHex形式を使いたい。Windowsの電子メールソフトではAL-Mail、Eudora ProなどがBinHexに対応している。

●圧縮ファイルを自己解凍にしない

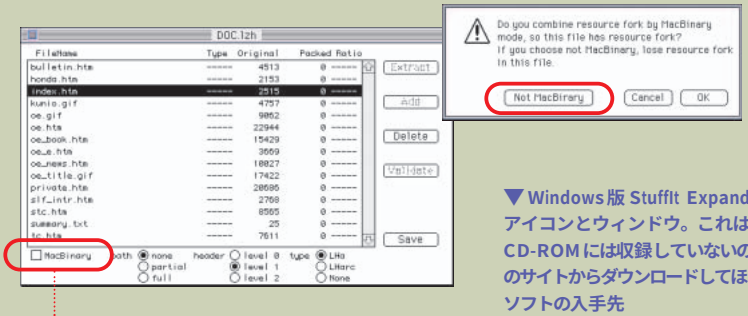
ダブルクリックすると自動的に伸張が行われる、いわゆる自己解凍形式は異機種間では意味がない。原則的に、Windowsで実行できるプログラムはマックでは実行できないし、その逆も無理だからだ。伸張ソフトによっては、自己解凍形式のファイルを伸張することもできるが、自己解凍形式にすることによって若干ファイルサイズが増えることも考えると、異機種へ送信するファイルでは自己解凍形式は避けたほうがいいだろう。

● Windows用のStuffIt Expanderも便利

StuffIt Expanderといえばマック用の圧縮ファイル伸張ソフトの定番だが、Windows版もあり、これがなかなか便利。マックで普及しているStuffIt形式の圧縮ファイルや、Zip、Arj、Arc、gzipの圧縮ファイルが伸張できるのに加え、UUENCODEとBinHexのエンコードデータを復元できる。使い方は簡単で、伸張・復元したいファイルをドラッグしてStuffIt Expanderのアイコンまたはウィンドウに重ねるだけだ。伸張と復元をいっきにやってくれる点も魅力。たとえばZip形式の圧縮ファイルをUUENCODEでエンコードしたものをStuffIt Expanderにドラッグすると、UUENCODEの復元後に自動的にZip形式の伸張が行われる。手間いらずのツールだ。

● MacLHAを使うときは注意

Windowsとマックでデータをやり取りするときには.lzh形式も利用可能だ。DOSやWindowsで幅広く利用されているLHAだが、マックでもフリーソフトウェアのMacLHAによって.lzhファイルの作成と伸張ができる。Windowsに送信するデータをMacLHAで圧縮する場合は、MacLHAのウィンドウで図のように［MacBinary］のチェックマークをはずしておくこと。これは圧縮するファイルを指定する前に行う必要がある。



チェックマークをはずすこと。

▲MacLHAのウィンドウ

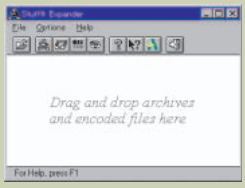
この状態で圧縮するファイルを指定すると、注意メッセージが表示されることがあるが、そのときは［Not MacBinary］ボタンをクリックすること。このようにしないと、圧縮されたファイルの先頭にマック用の属性データが入り、Windowsのアプリケーションでの使用に差し支える場合がある。たとえばテキストファイルの先頭に不要なデータが入ったりする。

▼Windows版StuffIt Expanderのアイコンとウィンドウ。これは本誌CD-ROMには収録していないので次のサイトからダウンロードしてほしい。

ソフトの入手先

URL http://www.aladdinsys.com/

Expander.exe



Q2：インターネットを流れるメールのプライバシーは守れますか？

Frequently Asked Question

インターネットの普及に伴って、電子メールの利用も急増している。200万人の会員を抱える商用パソコン通信との相互接続や、企業ではLANメールからのゲートウェイ接続の普及もある。インターネットの電子メールアカウントさえ持っていれば、世界中の電子メール利用者と文書のやり取りをすることが可能になってきている。また、MIME形式をサポートする電子メールソフトの増加により、いままでテキストだけであった電子メールがバイナリーファイルのデータや画像データ、音声データを添付したマルチメディア化された電子メールへと変わろうとしている。その流れのなか、多くの組織は、企業内と外との通信手段としてインターネットの電子メールを採用し始めた。手軽に、即時に、コンピュータで作成した内容のまま送信でき、受け取った側もその内容を他の作成文書に再利用できる利点に多くの人が虜になっている。そのため、本来ならば封書で送付するべき機密性の高い内容までも、電子メールで送ってしまうことが頻繁になっている。電子メールを使った通信は、これほどまでに安全なのだろうか。プライバシーは守れるのだろうか。

インターネットの３つの恐怖

●盗聴

インターネット上を流れるデータは電子メールの形式になっているが、中身はテキストデータとして読むことが可能なデータである。WWWでの通信販売でクレジットカードの番号をインターネットで送るのはいけないと言われるように、電子メールでもそのまま機密データをインターネットに流すことは、いわば、ハガキの状態でデータが送られているようなもので、悪意を持った第三者に読まれる（盗聴される）危険をはらんでいる。 企業がインターネットで人材を募集するときの履歴書などの個人情報、弁護士事務所が顧客の相談を受けるときのプライバシーに関わる情報などは、常に盗聴の危険にさらされる。

A：暗号化すれば安心です。

回答：菊地宏明

●改竄（かいざん）

盗聴の危険とともにあるのが改竄である。通信途中で電子メールを抜き取り、内容を変更して再び送信されると、電子メールへの信頼はなくなる。一般の企業でも営業情報、開発情報は盗聴の危険だけでなく、改竄されることも考えられる。

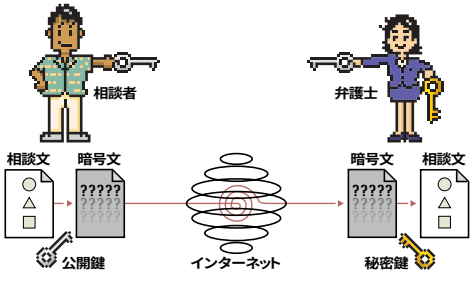
●スプーフィング

そして、スプーフィングの脅威も見逃せない。スプーフィングは、電子メールの制御情報を操作して、他人になりすます卑劣な行為だ。誰かがあなたになりすまして会社の上司に辞表を出しているかもしれないし、悪い噂を流しているかもしれない。

対抗策は暗号技術

盗聴に対抗する方法としてとられているのが、暗号化である。暗号化することで、電子メールの内容は厳重に封印された封書で郵送するかのように、暗号解読の鍵を持

図１●公開鍵暗号方式



たない者から保護される。

現在、普及している暗号化方法は、公開鍵暗号方式というもので、機密保護をする者（情報の受取り人）が暗号化専用鍵（公開鍵）と解読専用鍵を作成し、暗号化専用鍵を通信する相手にあらかじめ配付しておく。

送信者は、同じ暗号化方式を用い、暗号化専用鍵で暗号文に変換した内容を電子メールにして送る。暗号文の受取人は対になる解読専用鍵で暗号文をもとの平文に解読して使う。暗号と解読には2つの専用の鍵を使い、暗号文は解読専用鍵でしかあけられないようになっているので、暗号化専用鍵を公開しても暗号文を読まれることはない。

改竄に関しては、電子署名で対抗することができる。送信側で、送信者の情報と送られるテキストのダイジェスト情報を演算によって導き出し、その情報を変更されないように暗号化して内容に添付して送る。受け取った側で、その内容と、ダイジェスト情報を比較し、途中で改竄されていないかを確認することができるしくみになっている。

さて、最も面倒なのは、スプーフィングへの対策である。公開鍵が偽者から公開されたのでは、暗号化しても役に立たない。そこで、公開鍵の作成を信頼ある機関が行うことが考えられる。市役所で印鑑登録をするように、鍵の申請者が本人であることが証明されれば信頼性は向上する。

PEM、PGP、KPSのシステム

電子メールに暗号システムを組み合わせると、盗聴や改竄に有効だ。現在普及している暗号システムはいくつかある。（表1）

❶ メールを作成し「暗号」ボタンをクリックすると、ボタンが「暗号OK」という表示に変わるので、ここで送信ボタンを押す。

❷ 暗号メールが届くと受信リストに鍵マークが表示される。受信した時点でメールは自動的に復号されるので特別な操作はいらない。

図2●KPS方式を採用した東芝情報システムのCypherMailは、暗号メールをもっとも手軽に利用できるメールソフトだ。専用の鍵生成アルゴリズムを認証センターとなっているアドバンス社（http://www.advance.co.jp/）に申し込んで入手し、インストールしておく必要がある。

PEM（Privacy Enhanced Mail）は、RFC1421～1424で標準化されている電子メール暗号化形式で、日本でもインターネットの実験場というべきWIDEプロジェクトで公開実験が行われている。これは、UNIXマシンへの実装は多いが、パソコン向けはまだ少なく、マック、UNIX用に「魔法便」という製品がNTTエレクトロニクステクノロジ社から発売される予定だ。この公開鍵暗号方式の証明書には、RSA公開鍵暗号方式の発行機関であるベリサイン社の証明書が使えるようになる。

PGP（Pretty Good Privacy）は、フリーソフトウェアとして、日本で使えるバージョン2.6.3iが入手できる。次ページで詳しく解説するが、初めて使うときは、設定・操作がかなり難しい。このPGPは、特定の機関が証明書の発行を行っていない。そのため、公開鍵に信頼のある人物の電子署名が付けて証明しようとしている。

また、国内で考えられた暗号システムKPS（Key Predistribution System）方式を使ったものとして、マック用のフリーソフトウェアEudora-J KPS（別途ハードウェア必要）や、東芝情報システムから発売されているDOS、Windows用の製品CypherMailがある。これらのユーザー認証は、株式会社アドバンスのKPSセンター（http://www.advance.co.jp/）で行われている。

以上の暗号システムを用いてプライバシーを守るのが最善策だといえるが、異なる暗号システムでは互換性がない。つまり、電子メールを送り合う利用者同士が同じ暗号システムである必要がある。これが、今後の課題になるだろう。

なお、暗号化アルゴリズムは国防上の理由で国外持ち出し禁止になっている場合があるので、暗号化システムをダウンロードするときは、国内のサーバーから行うとよい。

表1●インターネットで入手できる暗号システム

	ソフト名	暗号方式	対応機種	入手先	配布形式
暗号化ツール	PGP2.6.3i	PGP	Dos/Windows	ftp://pr.aist-nara.ac.jp/pub/Security/tool/pgp/dos/	フリーソフトウェア
	MacPGP2.6.3i	PGP	Macintosh	http://ac3.aimcom.co.jp/~macpgp/macpgp.html	フリーソフトウェア
暗号化機能付きメールソフト	CypherMail	KPS	Windows	http://cmall.tjsys.co.jp/cyber/tjsoft/network/cypher.htm	試用版（市販価格は7500円）
	Eudora-J KPS	KPS	Macintosh	http://www.advance.co.jp/KPS/kps04_j.html	フリーソフトウェア（専用ハードを別途購入）

MacPGPで暗号メールに挑戦

使い方がよくわからないという声が多いMacPGPだが、次の流れにそって暗号メールに挑戦してみよう。まず、前ページの表で紹介したサイトから、MacPGP2.6.3iをダウンロードして解凍する。セットアップしてこのアイコンが出たら、ダブルクリックで起動する。

MacPGP 2.6.3ia

step1: 鍵の作成

暗号システムを使うために必要な公開（暗号化）鍵と秘密（復号）鍵のペアを作成する。

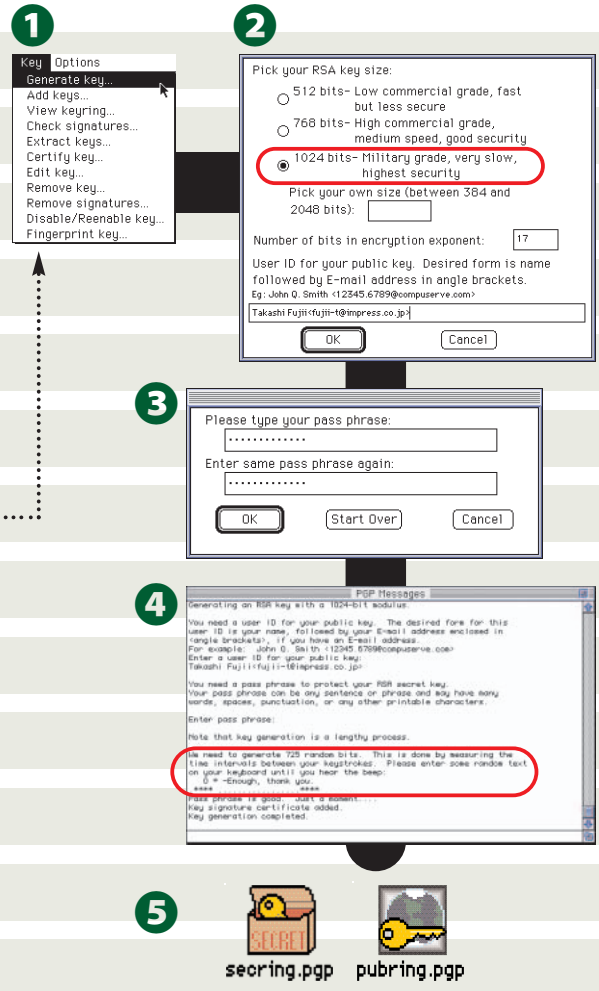
❶Key メニューのGenerate Key...項目を選択し、作成する鍵の設定を行う。

❷キーのサイズがセキュリティーの強さに関わり、1024bits のボタンを選ぶのがいいだろう。User ID 欄には、自分の名前と電子メールアドレスを書式に従って入力し、OK ボタンを押す。

❸続くウィンドウで、盗まれにくいパスフレーズ（パスワードよりも長い暗号句）を入力する。下の欄には確認のため、同じパスフレーズを入力する。OK ボタンのクリックをする。

❹キーボードからの入力が要求される。キー入力のタイミングで乱数を作るため、OK がでるまでキー入力を行う。

❺これで、あなたの公開鍵（ファイルpubring.pgp の中）と秘密鍵（ファイルsecring.pgp の中）が作成された。



step2: 自分の公開鍵を送る

公開鍵を暗号通信する相手に渡せる形態にする。

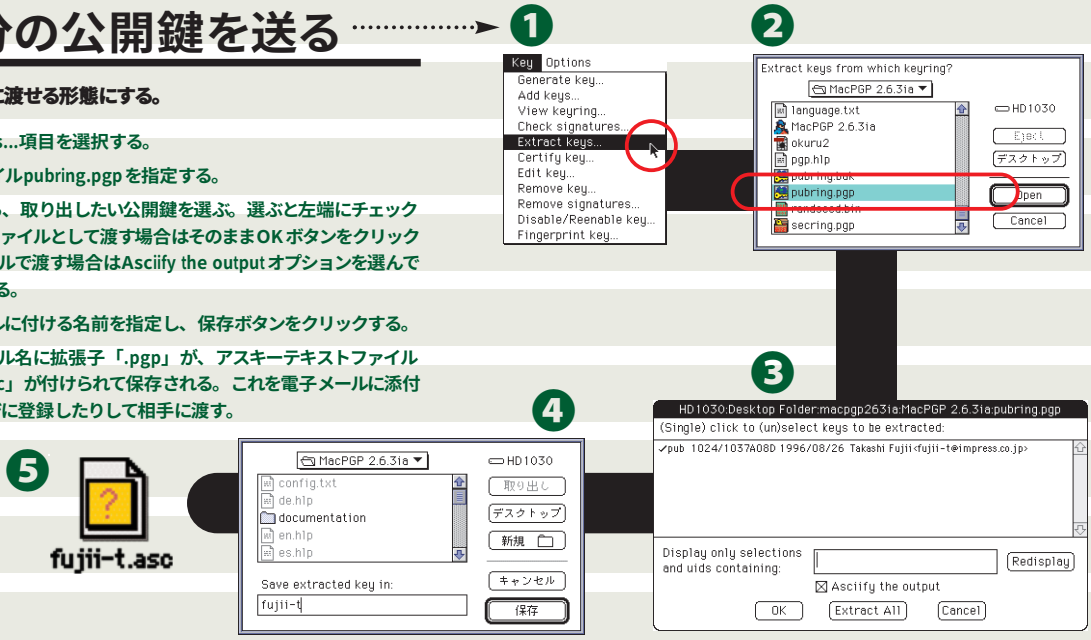
❶Key メニューのExtract Keys...項目を選択する。

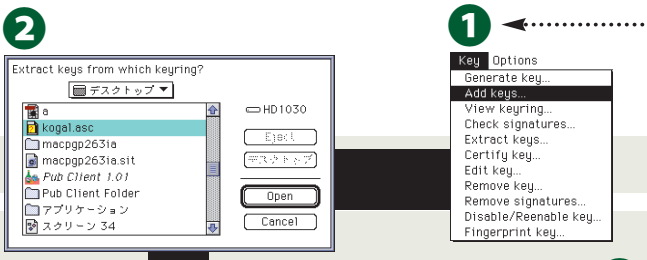
❷公開鍵が置かれているファイルpubring.pgp を指定する。

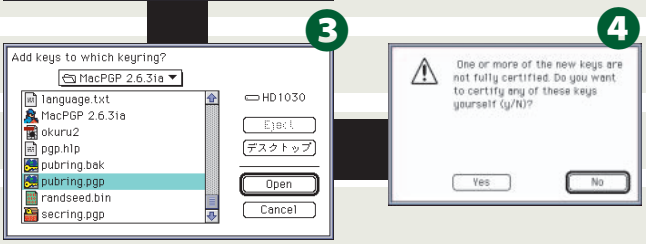
❸表れる公開鍵リストの中から、取り出したい公開鍵を選ぶ。選ぶと左端にチェックマークが付く。バイナリーファイルとして渡す場合はそのままOK ボタンをクリックし、アスキーテキストファイルで渡す場合はAsciify the output オプションを選んでからOK ボタンをクリックする。

❹取り出した公開鍵のファイルに付ける名前を指定し、保存ボタンをクリックする。

❺バイナリーファイルはファイル名に拡張子「.pgp」が、アスキーテキストファイルはファイル名に拡張子「.asc」が付けられて保存される。これを電子メールに添付したり、自分のホームページに登録したりして相手に渡す。







step3: 入手した公開鍵の登録

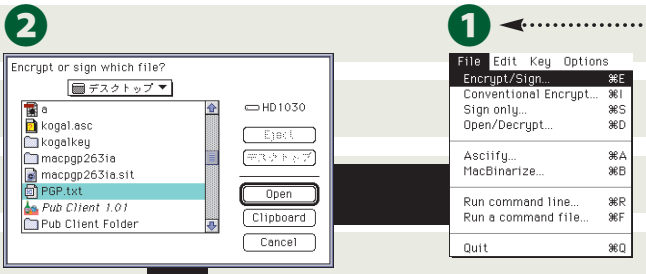
電子メールやホームページから入手した公開鍵を登録し、暗号通信可能な相手として登録する。

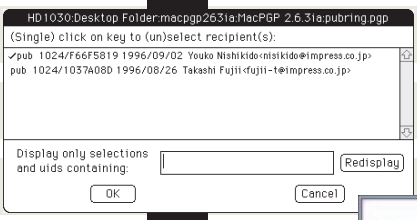
❶Key メニューのAdd Keys...項目を選択する。

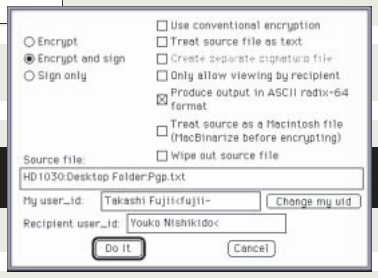
❷○○.pgp または○○.asc という拡張子を持つ、入手した公開鍵ファイルを指定する。

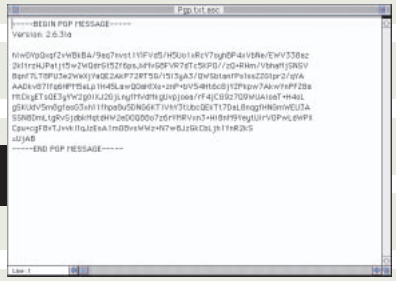
❸公開鍵を束ねているファイルpubring.pgp を指定する。

❹束ねようとした公開鍵が誰かによって保証されていない場合、その公開鍵をあなたが保証するか尋ねてくる。本人から直接渡されたなど保証できるならばYes ボタンを、保証できない場合はNo ボタンをクリックする。









step4: 暗号化

情報を送る相手の公開鍵を使って、平文を暗号データにする。

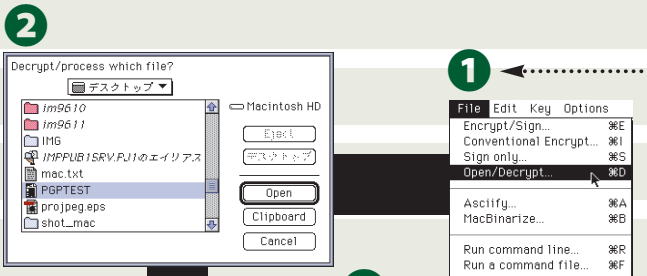
❶File メニューのEncript/Sign...項目を選択する。

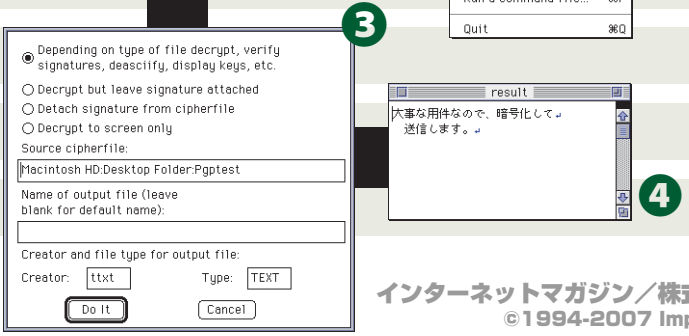
❷暗号化したいファイルを選ぶ。

❸送る相手の公開鍵を選んで、OK ボタンをクリック。

❹暗号化の設定で電子署名も同時に行うならばEncrypt and sign ボタンを選び、電子メールで送ることを考えてテキストファイルにするためProduce output in ASCII radix-64 format オプションを選ぶ。Mac のファイルとして送るならば、MacBinary 形式にするTreat source as a Macintosh file オプションも忘れずに設定し、最後にDo It ボタンをクリックする。

❺拡張子「.asc」が付いた暗号化されたファイルが作成される。あとは、この内容を電子メールに貼り付けるなり、添付するなりして送ろう。





step5: 復号

相手に渡してある公開鍵で暗号化された情報を、自分の秘密鍵で平文に戻す。

❶File メニューのOpen/Decrypt...項目を選択する。

❷復号させたい暗号ファイルを選ぶ。

❸Do It ボタンをクリックしてパスフレーズを入力し、OK ボタンをクリックする。

❹PGP Messages ウィンドウに電子署名の情報が表示され、暗号ファイルは復号化されてテキストファイルとして保存される。暗号化のときにMacBinary 形式のオプションが設定されているとそのときのファイル形式で保存される。

Q3：新しいメールソフトに替えるとき前の受信データを移行できますか？

Frequently Asked Question

A：一部のソフト間では可能です。

回答：山本貴信

読者の皆さんは、どんなメールソフトを使っているだろうか。マックユーザーなら、たぶんEudoraだろう。Windowsユーザーの人たちは何だろうか。昔はWindows用の日本語メールソフトは存在しなかったが、2～3年頃からWinBiff、AL-Mail、We Mailが出現し、最近ではEudora Pro、ネットスケープメール、マイクロソフトインターネットメールなど、私が知っているだけでも十数種類のメールソフトが存在しており、これらは各々に特徴を持っている。

この混沌とした状況で、新しいメールソフトのほうが機能が豊富みたいだし、乗り換えたいと思っている人も多いことと思う。しかし、そういう人たちの最大の関心事は、どのメールソフトがどれだけ優れているかということより、今まで受信したメールをどうやって読むかということだ。

メールボックスの形式には、UNIXの世界ではUNIX形式が、マックの世界ではEudoraの形式が、それぞれ普及している。幸か不幸か、マックの世界では最近まで使えるメールソフトはEudoraしか存在しなかった。そのおかげで、Eudora形式が「標準になった」と言っても過言ではないだろう。その証拠というわけではないが、最近発売されたDOLPHINという市販ソフトは、はじめからEudora形式のメールボックスを取り込む機能が付いている。

では、Windowsの世界ではどうだろうか。残念ながら、Windowsのメールボックスの標準形式というのがまだ存在しない。まだ創世期のためか、ほかのメールソフトのメールボックス形式に書き出すことはもちろん、読み込むことさえできないことが多い。

しかし、いくつかのソフトの間ではすでに実現されている。意外と知られていない情報だが、ネットスケープメールの内部のしくみは、Eudoraと同じ形式になっている。これは、フォルダーファイルを移動するだけで移行が可能だということを意味する。また、新登場のマイクロソフトインターネットメールは、自社製品であるマイクロソフトエクスチェンジからメールを読み込むことも、書き出すことも可能だ。

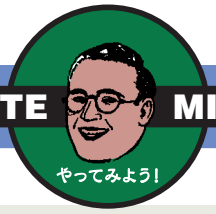
そして、最近登場したBecky!1.9Jというメールソフトは、さまざまなメールソフトのメールボックスを取り込むためのツールが付属している。移行が可能なメールソフトを整理してみると、表1のとおりになる。これに加え、Eudoraは、Windows版とマック版も受信データはテキスト形式で保存されているので、パソコンを買い替えてもOSをまたがって移行することができる。

では、ほかのメールソフトで移行したいときの手段はあるだろうか。メールボックスの形式は、非常にシンプルな場合が多いので、メールボックスの移行ツールを自作するというのも手だが、書き出しにはそのメールソフト独自のいろいろなルールが複雑に絡んでくるので、あまりお勧めしない。昔のメールを読み返す機会は少ないので、思い切って昔のメールは捨ててしまうか、本当に残しておきたいかどうか考えて、それでも必要だと考える分だけそのまま残しておき、今まで使用していたメールソフトは昔のメールのビューワーとして使ってみてはいかがだろう。

Becky!みたいなメールソフトの登場により、これからはほかのソフトのメールボックスのデータの読み込み機能が当たり前のように付いてくるだろう。あなたの気に入るメールソフトが、次期バージョンでは昔の受信メールを取り込めるようになるかもしれない。

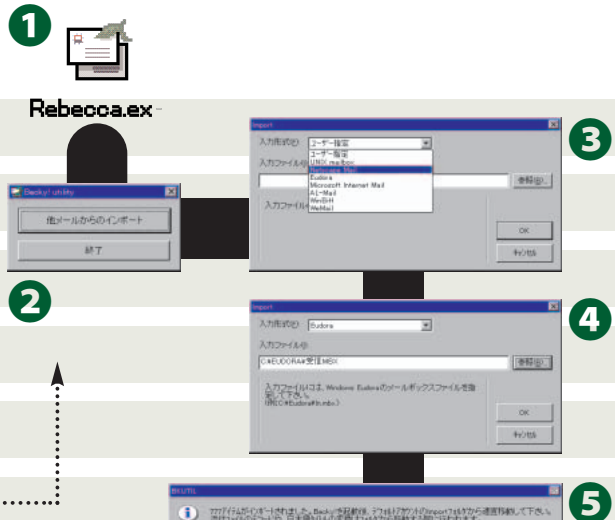
表1●編集部で確認できた受信データの移行が可能なメールソフト

このソフトから	このソフトへ	方法
Eudora Pro（Mac）	DOLPHIN（Mac）	DOLPHIN付属の機能を使う
Eudora Pro（Windows、Mac）	ネットスケープメール（Windows、Mac）	受信ファイルを所定場所に置く
ネットスケープメール（Windows、Mac）	Eudora Pro（Windows、Mac）	受信ファイルを所定場所に置く
マイクロソフトエクスチェンジ	マイクロソフトインターネットメール（Windows）	インターネットメールのファイルメニューからインポートを選ぶ
UNIX形式	Becky!1.9J（Windows）	Becky!付属のユーティリティーを使う
Eudora形式	Becky!1.9J（Windows）	Becky!付属のユーティリティーを使う
AL-Mail（Windows）	Becky!1.9J（Windows）	Becky!付属のユーティリティーを使う
WinBiff（Windows）	Becky!1.9J（Windows）	Becky!付属のユーティリティーを使う
WeMail（Windows）	Becky!1.9J（Windows）	Becky!付属のユーティリティーを使う
マイクロソフトインターネットメール（Windows）	Becky!1.9J（Windows）	Becky!付属のユーティリティーを使う



2つのソフト間で受信データを移行

これまで使っていた電子メールソフトで受信したデータを、新しいメールソフトに取り込む実際の操作を2つの事例で紹介する。どちらのケースも今すぐにできる簡単なものだ。



case1: Eudora Proのデータを Becky! に取り込む

❶Becky!のプログラムのあるフォルダーに、このアイコンがあるのでダブルクリックで起動する。

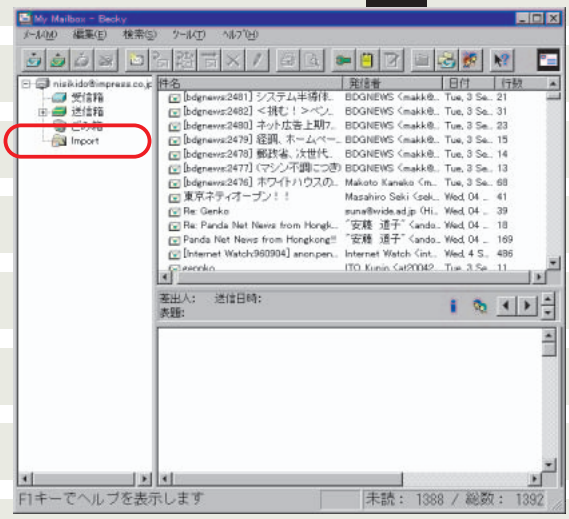
❷この画面が現れるので他メールからのインポートを選ぶ。

❸入力形式のメニューからEudoraを選ぶ。

❹参照ボタンを押してEudoraのフォルダーの中の拡張子.mbxのファイルの中から移したいデータを選び、OKボタンをクリックする。

❺この表示が出たら成功。

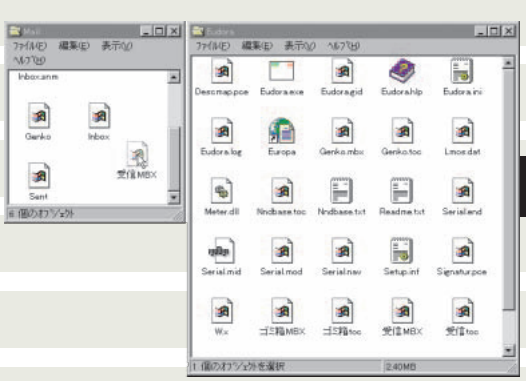
❻Becky!1.9Jを起動するとimportという新しいフォルダーが作成されており、メールを読み出すことができる。

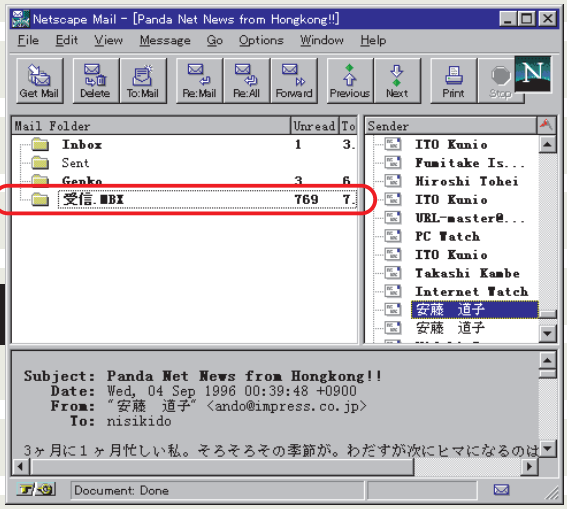


case2: Eudora Proのデータを ネットスケープメールに 取り込む

❶Eudoraのフォルダーの中にある拡張子.mbxのファイルの中から、移したいデータを選び、Netscapeのフォルダーの中のMailのフォルダーに移す。

❷ネットスケープメールを起動すると移したファイルの名前のフォルダーが作成されていて、中のメールを読める。次に起動すると、拡張子.mbxの部分がフォルダー名から消えて、「受信」フォルダーができている。





Q4：会社のパソコンと自宅のパソコンでメールは共有できますか？

Frequently Asked Question

A：読むことはできます。
回答：インターネットマガジン編集部

電子メールを仕事の連絡手段として使っていると、メールを読めない環境にいるわけにはいかない。インプレスの編集スタッフは、取材のアポ取りから企画の打ち合わせ、原稿の催促や受け取り、読者の苦情への対応まで、ほとんどの連絡にインターネットメールを使っているので、出張で会社を離れたり、病気で会社を休んだりしても、最低メールの確認だけはしたいと思っている。外からPHSを使ってモバイルコンピューティングをしようという大げさなものではなく、ただ自宅でメールを読みたい、そういう欲求が自然に出てくるのである。では、自宅でメールを読むにはどんな方法があるだろうか。

パソコン通信でTELNET

ニフティサーブやPeople、PC-VANなどインターネットが利用できるパソコン通信サービスに入っているなら、もっとも簡単な方法だ。パソコン通信サービスに入り、そこからTELNETというリモートログイン機能を使ってインプレスのサーバーにログインする。TELNETはインターネットの基本機能なので、ニフティサーブ、PC-VAN、People、日経MIX、アスキーネットなどインターネットに接続している大手のパソコン通信サービスで利用できる。

ただし、ふだん会社で使っているEudoraやネットスケープメールなどのメールソフトが利用できるわけではない。メールサーバーにログインしてUNIXの操作をしないといけないので、Windowsやマック用のグラフィカルなメールソフトしか使ったことがない人には、返事を書いたりする作業がつらいかもしれない。また、外部からのTELNET接続を受け入れる態勢を会社側で用意している必要がある。

会社のPPPサーバーにつなぐ

Eudoraなどふだん使っているメールソフトを使いたいなら、会社が用意したPPPサーバーに直接ダイアルアップ接続する方法がある。PPP接続のためのサーバー側のソフトとしては、WindowsNTに標準添付されているRAS（リモートアクセスサービス）がある。これは、ユーザーがマックでもWindowsでも両方から利用できるうえ、DOS/Vパソコンを1台PPPサーバー用に開放するだけですむので手軽に導入できるだろう。ユーザー側は、次ページで紹介しているように、インターネットプロバイダーにつなぐのと同じ手順でPPP接続すればいい。

マックだけのネットワークなら、遠隔地のパソコン同士でファイルを共有するためのソフトARA（アップルリモートアクセス）でインターネットプロトコルを利用できるようにすることができる。管理者側でこのインターネットプロトコルを使う設定がされていれば、ユーザーはARAを使って会社のサーバー接続し、メールソフトを使うことができる。

プロバイダーを使う

ダイアルアップでPPP接続するなら、会社に直接つなぐより最寄りのプロバイダーに接続したほうが電話代が安くつく場合もあるだろう。出張時には使いたい方法だが、ファイアーウォールで外部からの接続を遮断している場合もあるので、利用したい場合はネットワーク管理者に相談しよう。

データを共有するには

リモートアクセスでメールの読み書きは楽にできるようになっても、1つ問題がある。自宅で読んだメールは自宅のパソコンに、会社のパソコンで読んだメールは会社のパソコンにと、データが2か所に散らばってしまい、一元管理ができない。この対策はどうしたらいいのだろうか。ほとんどのメールソフトでは、一度パソコンで読み出したメールをメールサーバーから削除するか、それともサーバーに残したままにするか、設定できるようになっている。一度読んだメールを会社のメールサーバーに残したままにしておくのはサーバーの容量の無駄使いなので、インプレスでもサーバーに「残さない」と設定するように指導されている。

しかし、一元管理をするには、やむをえず自宅で読んでしまったメールを会社のパソコンでも読めるようにしたい。そこで、インプレスのスタッフは以下のように設定する。

●自宅のパソコンでは「サーバーに残す」設定
●会社のパソコンは「サーバーに残さない」設定

これで、自宅でもメールの読み出しが可能、しかもそのメールは会社にもどったら未読メールとしてまた読み出しが可能ということになる。

図1●WindowsNTのRAS

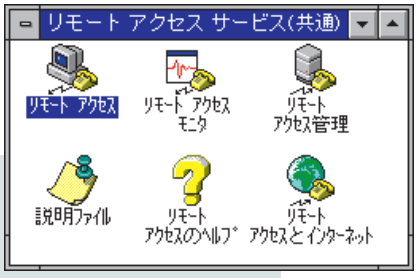
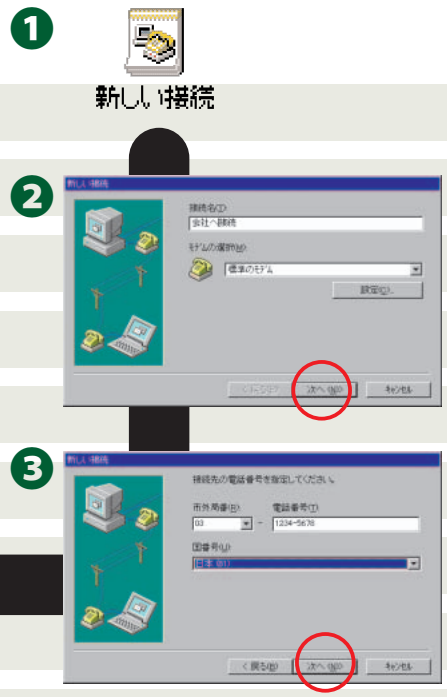


図2●Eudoraでは「環境設定」メニューの「メールの確認でサーバーに残すかを設定できる。メールソフトの多くは初めは「残さない」ように設定されている。

YA TTE MI SO ! やってみよう!

会社のサーバーへダイアルアップ接続

Windows95の場合、プロバイダーに接続するのと同じ手順でできる。Windows95同士なら、会社の自分用のパソコンをサーバーにすればハードディスクの中を見ることもできるが、その話はここでは割愛する。



case1: Windows95のリモートアクセス

ここでは「ダイアルアップネットワーク」をすでにインストールしている場合という前提で解説する。インストールしてしていない場合は巻末のデータページにある接続マニュアルのWindows95編を参考にしてほしい。

❶ダイアルアップネットワークのこのアイコンをダブルクリックする。

❷「会社へ接続」と入力して設定開始。

❸会社のサーバーの電話番号を指定する。

❹「完了」をクリックする。

❺ダイアルアップネットワークにこのアイコンができているので選択する。マウスを右クリックしてプロパティを選ぶ。

❻サーバーの種類は「〜インターネット」を選択する。

❼「TCP/IP設定」を選択する。

❽ネームサーバーアドレスに、会社のパソコンで設定しているとおりのIPアドレスを指定してOKボタンをクリックする。

❾❺のアイコンを再びクリックすると、このウィンドウが現れて接続を開始する。接続後はメールソフトを起動すればOK。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp