Mac OS によるセキュアなメールサーバの構築[1]

神戸大学大学院経済学研究科　玉岡　雅之

EIMS is the best mail server I've ever known.

以下では，Mac OS で動く代表的なメールサーバである Eudora Internet Mail Server （以下，EIMS と略します）3.0.3 [2]を使って，セキュアなメールサーバを構築する方法について考えてみます。メールサーバのセキュリティについてはいろいろな点を考慮しないといけませんが，以下では

・不正中継の防止
・SPAM メール受け取りの許否
・ウイルスメール対策
・メールサーバ自身に対する攻撃の防御

の４点を主に考えます。

まず最初に EIMS のインストールから始めて，最初の話題である不正中継の防止についての設定に進みます。その後で，SPAM メール受け取りの許否，ウイルスメール対策，メールサーバ自身に対する攻撃の防御の順に話を進めていきます。

１．インストールとアカウントの設定

EIMS を動かすのに必要な条件ですが，Administrator's Guide によると

・Macintosh 68040, PowerPC or later
・Macintosh System 7.5.5 or later
・8 Megabytes of RAM
・Open Transport 1.1.2 or later
・Access to DNS
・TCP/IP connection

---

[1]本稿作成に際し，石津広也氏，田中求之氏，前薗健一氏より大変有益なコメントをいただきました。また，細かなバグリポートに対してもいつも返事をくださる EIMS の作者 Glenn Anderson 氏にはすばらしい製品とともに感謝いたします。そして本稿をそもそも書くきっかけを与えたくださった湖内夏夫氏にも感謝いたします。もちろんあり得べき間違いはすべて筆者の責任です。
[2] EIMS は http://www.eudora.com/eims/ から入手可能な製品です。

となっています[3]。ユーザの数が多くなるほど，より速いプロセッサとより速いハードディスク（出来れば高速の SCSI ディスク），より多くのメモリが必要となります。

インストールが終わるとインストール先のフォルダに「EIMS Server」という次のようなプログラムができます。

このプログラムをダブルクリックすると下図のようになります。

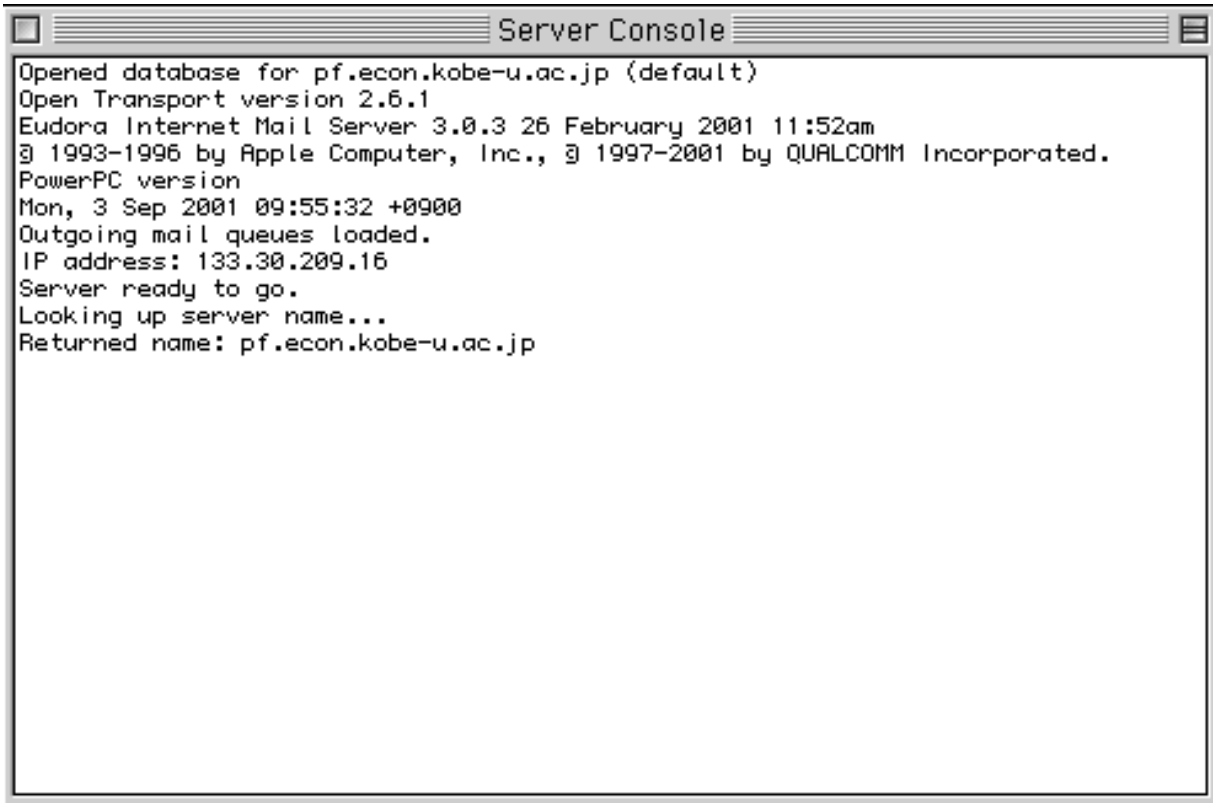
この画面は EIMS を管理するために EIMS Admin というプログラムを動かしますが，その Admin プログラムを使って管理したい EIMS Server にアクセスするときのパスワードを設定するものです。同じものを上段と下段に入力してください。

すると下図のようなコンソールウインドウが現れます。

---

[3]ちなみに Glenn Anderson さんの勧めるシステムは，
Mac OS 7.5.5 (680030 と 680040 マシン， PowerPC マシンでは 7.6.1 以降)
Mac OS 7.6.1 (もしサポートされているなら 680030 と 680040 マシンで)
Mac OS 8.1（出来るなら 8.6 まで上げた方がよい）
Mac OS 8.6
Mac OS 9.0.4
Mac OS 9.1

となっています。メールサーバを始めとするサーバの運用にとってシステムの安定性は何よりも大事です。



次にサーバ自体の設定に入ります。やるべきことはアカウントの作成と不正中継に利用されないための設定です。以下ではこの順番で説明しますが，順番を逆に設定した方がよりセキュアです。

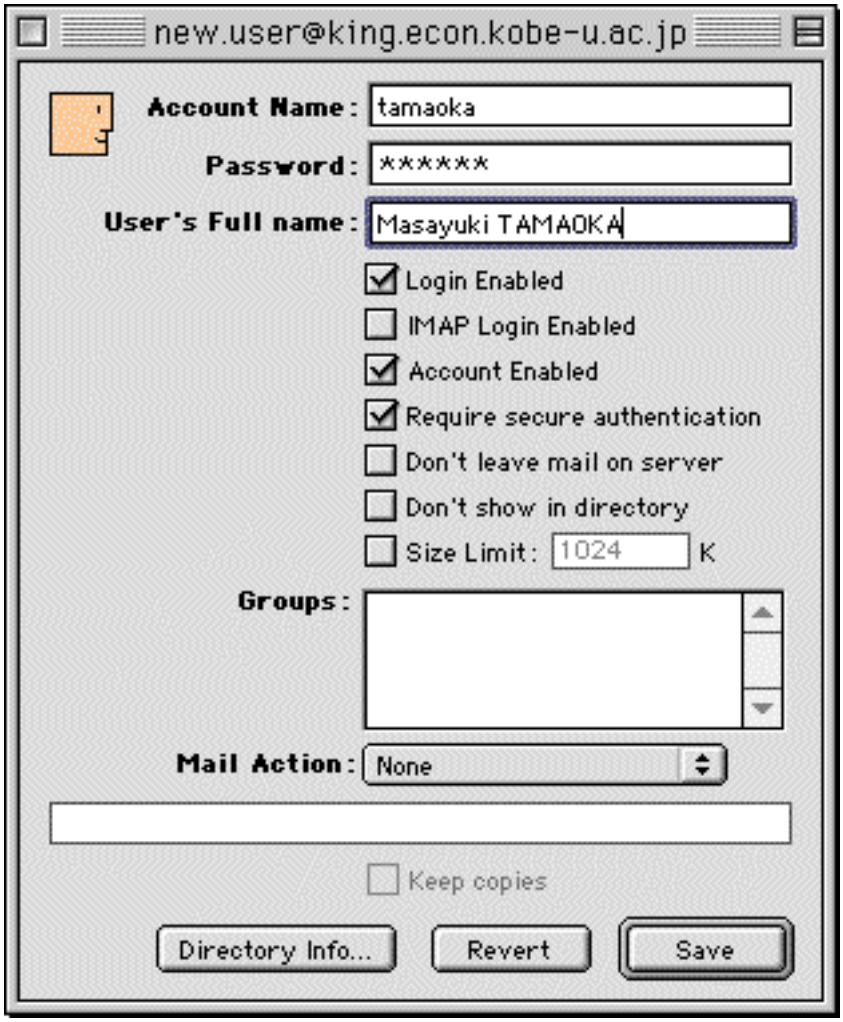
まず下図にあるような EIMS Admin プログラムを動かします（なお，EIMS Server とか EIMS Admin のプログラム名は変更しない方がよいでしょう。プログラムのアップデートがあるときにこの名前のプログラムを探しますので，名前を変えるとアップデートされないことがあります)。

するとログイン画面が現れますので，上段のアドレス欄には EIMS Server が走っている管理するホスト名を入力し，下段にはさきほど設定したパスワードを入力します。

うまく接続できると下のようなドメインウインドウが現れます。アカウントの設定等をまだしていませんので，postmaster アカウントだけが見えます。

メニューバーの Users & Groups から Adding New User を選ぶと下のようなウインドウが現れますので，アカウント名，パスワード等の情報を入力します。アカウント名は OS の制約から 31 文

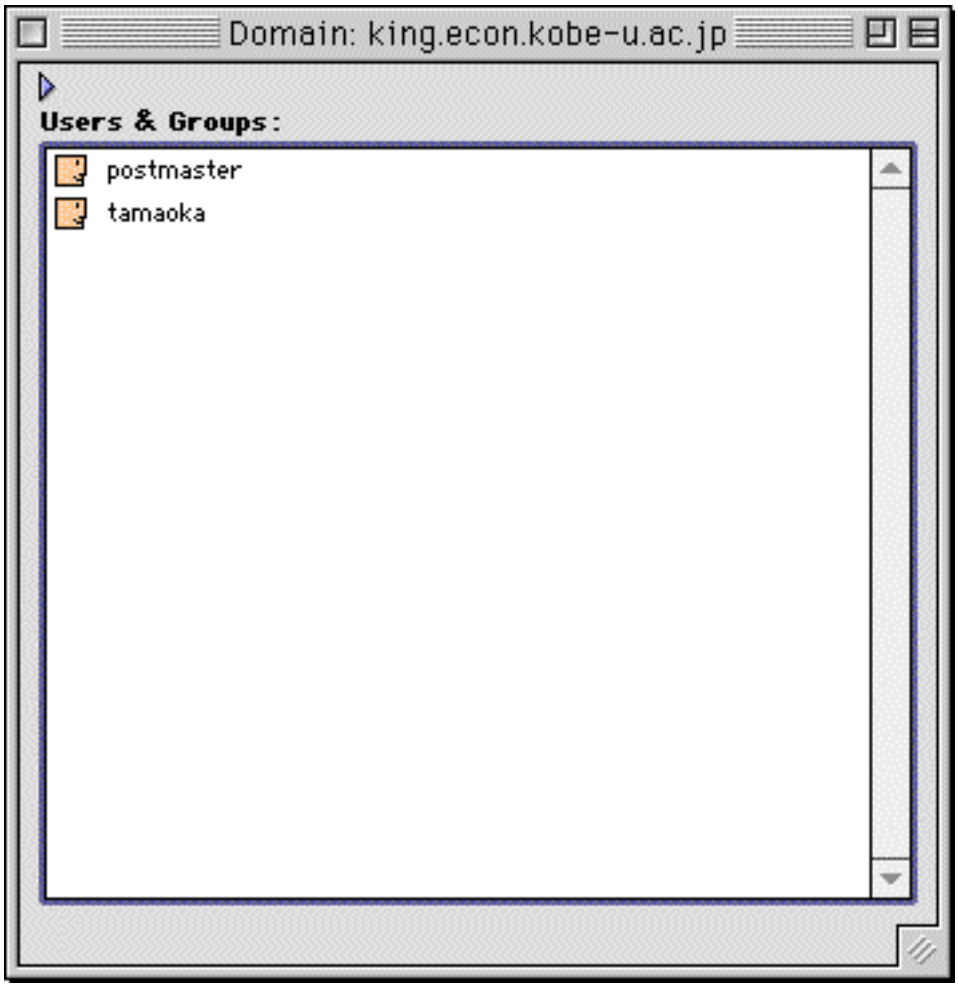
字までの長さを受け付けます。



この画面で注意すべき点が３つあります。１つ目は「Account Enabled」にチェックをいれないとアカウント自体が有効にならない，つまりこのアカウント名でメールを受け取ることができないということです。２つ目は「Login Enabled」の欄です。EIMS 3 ではこの欄をチェックしないとメールのリレー（自ドメインから他ドメインへのメールの配送）ができませんので注意してください（副次的な目的としては，postmaster アカウントについてアカウントは有効にするが，ログインを認めない設定にしていると，後の節で述べる不正中継調査機関の postmaster アカウントを使ったテストを排除できます)。３つ目は「Require secure authentication」の欄です。EIMS 3 ではメール確認（POP3 or IMAP4 を使う）とメール送信（SMTP を使う）の際に暗号を用いることができるようになっています。この欄にチェックを入れると，POP3 でメールの確認をするときは APOP 認証を行い，IMAP4 でアクセスするときには CRAM-MD5 で認証を行います。またメール送信の際には，この欄にチェックが入っていると，RFC2554 で定められている SMTP Authentication（以下，SMTP 認証と呼びます）を使うことになります。EIMS 3 では SMTP 認証として，CRAM-MD5, PLAIN, LOGIN の３方式に対応しています。また TLS 認証については将来的に対応する予定だそうです。

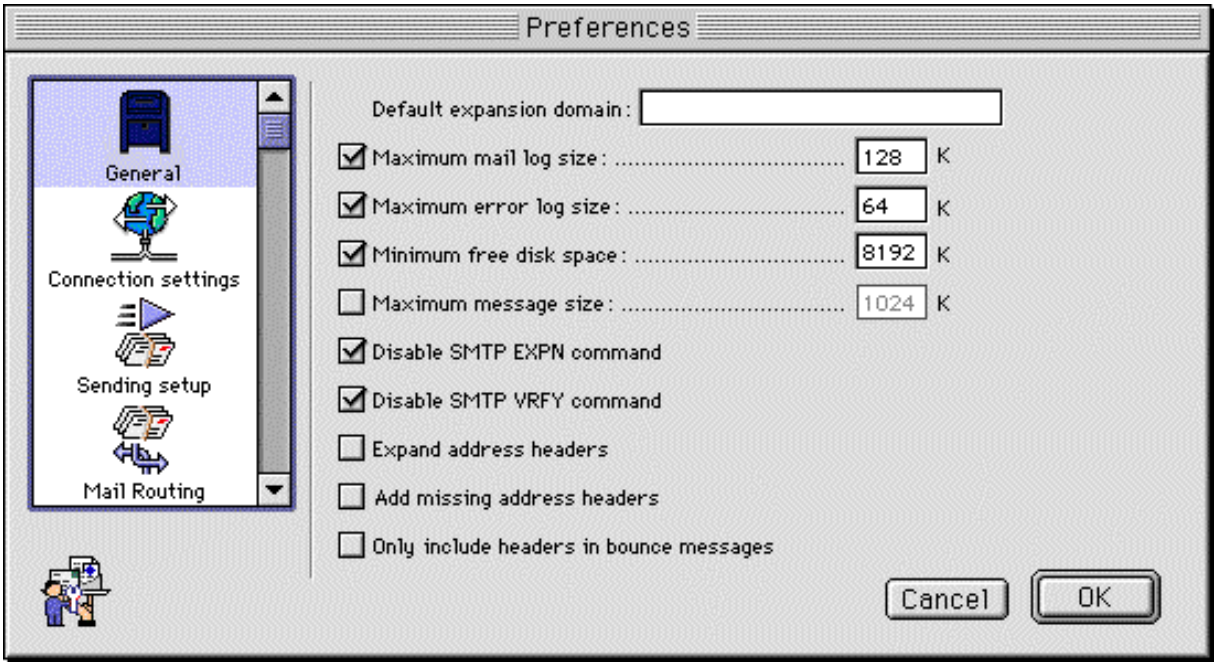
設定が終わると下図のようになり，新たに加えられたユーザはメールの送受信を行う準備ができま

す。

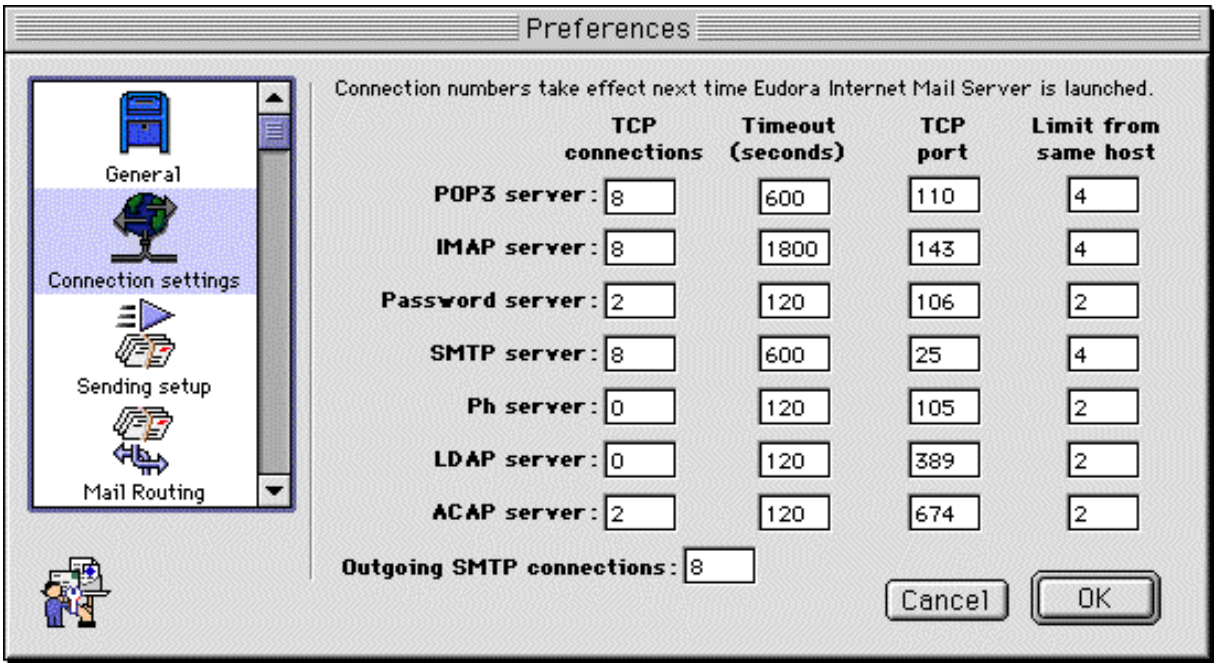


２．EIMS の基本設定

まず最初に Admin メニューから，Preferences を選択します。その中の General の項では一般的な項目の設定を行いますが，この中の「Maximum message size」の欄では受け取ることのできるメッセージのサイズの上限を定めることができます。メール爆弾等を防ぐのに有効でしょう。ユーザさんと相談して適当なサイズにするのがよいでしょう（デフォルトではオフになっています）。



次に Connection settings の項に移ります。ここでは，EIMS が提供するサービス（POP3，IMAP4，Password，SMTP，Ph，LDAP，ACAP）について同時にどれだけの接続を認めるか（TCP connections），それぞれのサービスについてのタイムアウトの時間はどれだけか，それぞれのサービスの使用するポート番号は何番か，それぞれのサービスに対して同じホストからアクセスできる数はどれだけか，等の設定を行います。不要なサービスはコネクションの数をゼロにして閉じるとともに，より多くのユーザが利用するサービス（例えば POP3）については数字を大きめにとってください（数字を大きくした場合は EIMS に割り当てるメモリを増やしてください）。



３．不正中継の防止

インターネットが現在のように普及する以前から電子メールという仕組みはありました。当時は世界のあらゆるところから自分のアカウントがおいてあるサーバ（多くは UNIX が走っていました）にリモートからログインし，自分のアカウントに届いているメールを読んだり書いたりすることができました。またしばらくしてパソコン上で手軽に扱える電子メール用のソフト，いわゆるメールソフトが普及し始め，まるでワープロを扱うように手軽に電子メールの送受信が出来るようになりました。アカウントをもっている人は誰でもどこからでもサーバにある自分のアカウントに届いている電子メールを読んだり，サーバを使って電子メールの送信を行うことができました。

ところが，インターネットが爆発的に普及し，商用にも広く用いられはじめた頃から思わぬ事態が起こってきました。それは俗に SPAM メールといわれる多くは宣伝用のメールが大量に発信され，ユーザの側では受け取りたくないメールを多量に受け取るということが起こったのです。さらに厄介なことには，これらの SPAM メールは発信者が自分のアカウントのあるメールサーバを使ってメールを発信してくるのではなく，自分とは全く関係のない他人のメールサーバを使って発信するので発信元を偽ることができるということです。これは電子メールを送信する際のプロトコルである SMTP (Simple Mail Transfer Protocol) が電子メールを送信する際には認証が必要ではないという仕組みから来ています。メール受信の際にはパスワードが必要であるという事実と好対照です。かつては世界中のどこからでも自分のメールサーバを使って電子メールの送信ができた仕組みを悪用された訳です。SPAM メールが大量に送付されると受け取り元のメールサーバがパンクすることもありますし，spammer（SPAM メールを送りつける人を指します）に抗議するメールをメールサーバの管理者宛に出したところが実際にはそのサーバのユーザが出していないにもかかわらず，抗議のメールが殺到してやはりメールサーバが機能しないという副作用も出ます。

そこで SPAM メールの発信に自分のメールサーバが使われないようにしようという動きが強まってきました。つまり何らかの方法で正規のユーザであることを確認した上でメール送信を行えるような方法を考えたのです。その方法として使われたのは

１．メールの発信元がメールサーバが扱っているドメイン名を名乗る
２．メールの発信元が許可された IP の中にある

の２つです。SPAM メールは自分とはまったく関係のないドメインからドメイン宛にメールが中継される[4]訳ですから，１によって自分のメールサーバとは関係のない第３者が第３者の名前を語って(多くの場合は実際には存在しないメールアドレスを語ります）自分のメールサーバを送信（他ドメインへのメールのリレー）に利用しようとするのを防ぐ訳です。ただし，１の設定だけでは spammer が

[4]このことを第３者間中継あるいは「不正中継」と呼びます。不正中継という用語はもともと unauthorized relay という単語に由来しています。本来は認められていないメールの中継という意味なのですが，いつからか SPAM メールと同一視されて，不正中継という用語が使われるようになりました。

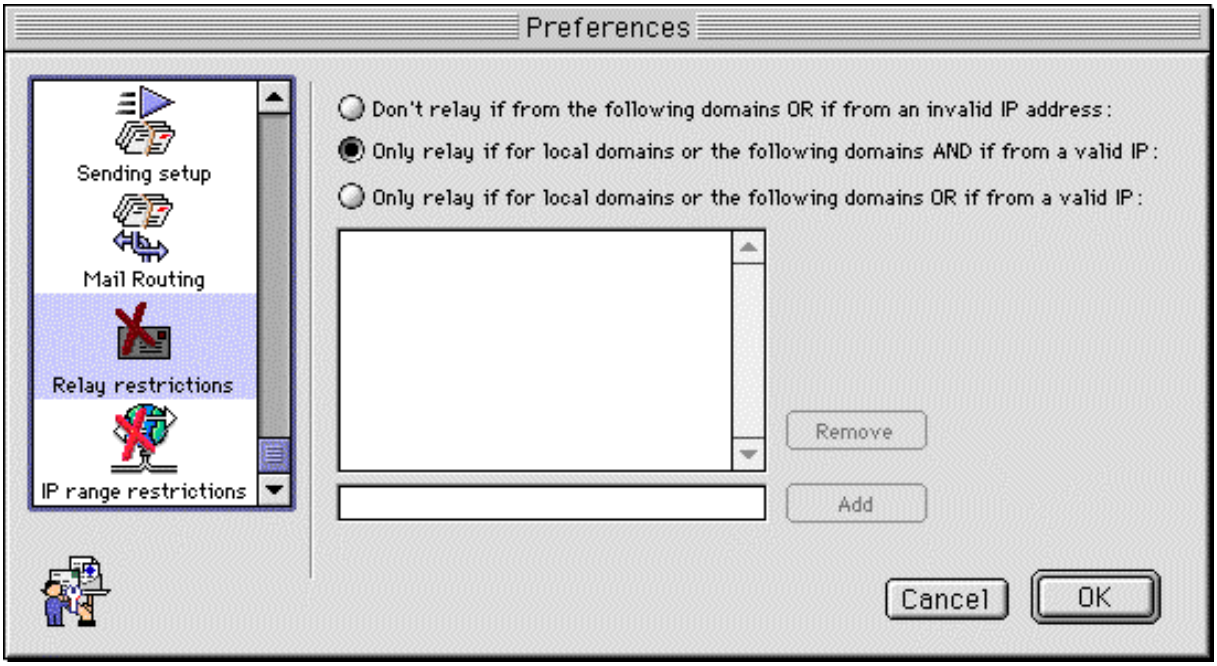
自ドメインのユーザである（例えば Postmaster を名乗る）ようになりすましてメールの送信を行うのを防ぐことはできません。そこで２の設定が必要となります。学内であるとか自社内であるとか，とにかく許可された IP アドレスの中から発信されたメールであれば正規のユーザからのメールであるとみなして，メールのリレーを認めようという考えです。これら２つの条件を同時に満たしたときにのみメールのリレーを認めるのです。

さて EIMS を使った不正中継防止のための設定に移ります。要点は２つあります。今述べたように設定上注意すべき点は，

・ドメインレベルでの第３者間リレーの禁止
・IP アドレスレベルでの第３者間リレーの禁止

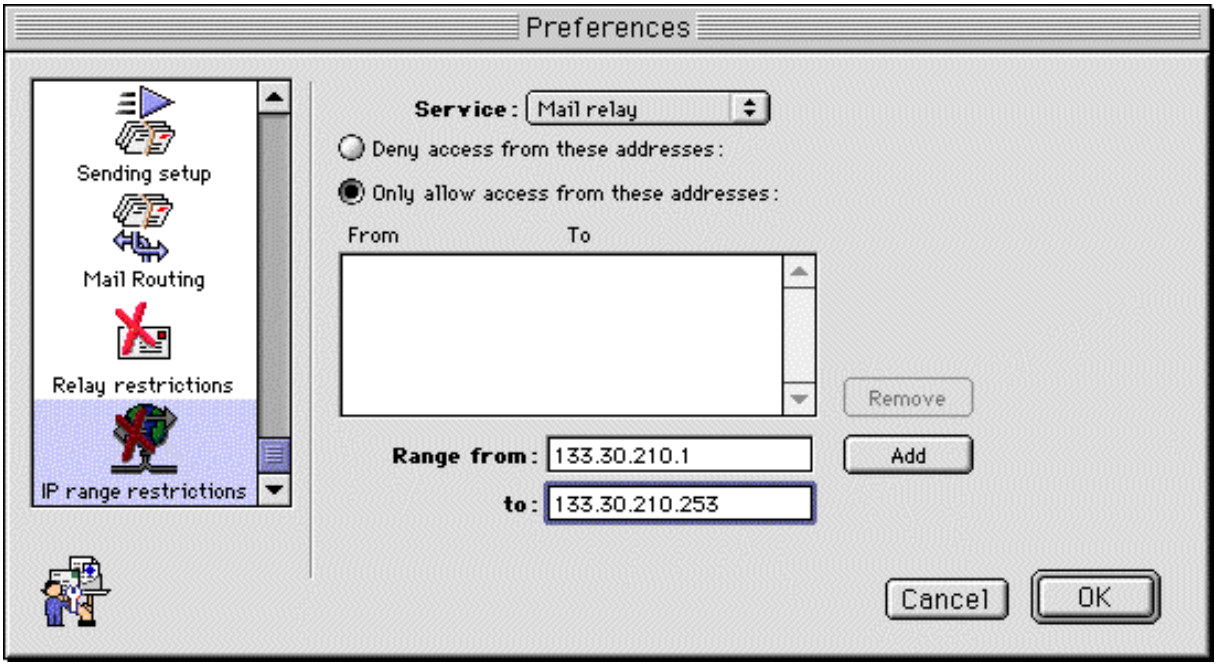
の２つです。これら２つを適切に設定しないとメールサーバが不正中継に利用されてしまいます。

まず最初にドメインレベルでの第３者間リレーの禁止を設定します。Preferences から「Relay restrictions」を選択してください。この中に３つのオプションがありますが，この中の２番目「ローカルなドメインか（下段で設定する）認められたドメインであり**かつ**認められた有効な IP アドレスであるときにのみリレーを許可する」にチェックを入れてください。ここでいうローカルなドメインとは EIMS がサービスを提供している自ドメインのことです。例えば学内や社内であっても EIMS で定義しているドメイン名と違えば第３者になってしまいます。学内や社内の違うドメインからも EIMS を利用したい場合には，ここでその他のドメイン名を記述し，かつ認められた IP アドレスを書くことで実現できますが，後に述べる SMTP 認証を用いたリレーの方がよりセキュアです。

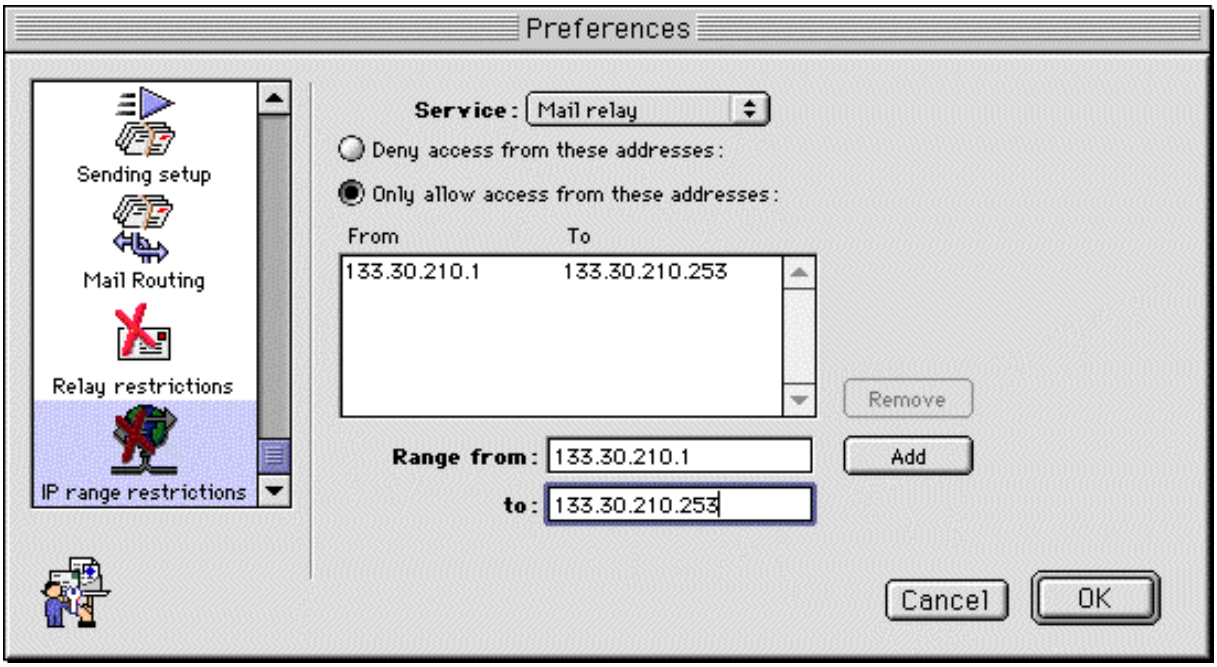


次に IP アドレス単位でのリレーの許可の設定に入ります。同じく Admin の Preferences から「IP range restrictions」を選択してください。上段の Service というところで「Mail relay」を選

んでください。すぐ下のところにチェックボックスがありますが，「Only allow access from these addresses:」にチェックをし，下の方にある 「Range from:」「 to: 」の欄に EIMS を利用するユーザの IP アドレスを記入してください。ここでは連続したアドレスを書いていますが，１個単位でも記述できますので，面倒くさがらずにユーザのアドレスをもれなく記入してください。記入ができると右側の「Add」ボタンをクリックしてください。



すると，下図のようになります。



以上で設定は終わりです。Admin プログラムを終了してください。

４．よりセキュアな通信方法

３で行った設定によって，不正中継を防ぐことができるようになります。ただし認められた IP アドレスのみからしかメール送信ができませんので，例えば自宅にいる場合や出張中には EIMS を使ってメール送信を行うことはできません。

現在外部から内部のメールサーバを使ってメール送信をする方法として代表的なものに次の２つがあります。

・POP before SMTP
・SMTP 認証

POP before SMTP はまず最初に自分のアカウントにあるメールの受信に成功した場合，一定時間の間は正規のユーザとして扱われ，（自分は外部ネットワークにいるのに）内部にあるメールサーバを使ってメールを送信できるという仕組みです。現在日本の ISP でも多く使われている仕様です。ところが次のような１例を考えてみてください。

> 日本の某社。アドレス不足のため，NAT （Network Address Translation ）でアドレスを共有。
> 昼休みにＡさんが契約しているプロバイダＢ（POP before SMTP 採用）にメールを読みに行き，Ｂのサーバを使って返事を出す。
> それを横で見ていたインターネットに詳しいＣさん（Ｂのユーザではない）は自分のＰＣでＢのサーバを使っていたずらメールをＤさんに出した。

非常に便利な仕組みですが，このように潜在的な穴をもっています。RFC2476 でも推奨されていません。

これに対して RFC2554 で規定されている SMTP 認証は本命ともいえる業界標準の仕様となってきています。かつては対応するメールソフト が少なかったり，また MTA（Mail or Message Transfer Agent，電子メールを配送するためのプログラム）側の対応もされていなかったのですが，現在のメジャーなメールソフトの多くが SMTP 認証に対応しています[5]し，sendmail をはじめ，Postfix，qmail 等でも対応できるようになっています。SMTP 認証はメールを送信する際に正規のユーザであることを認証してから送信できる仕組みで，たとえ外部のネットワークにいたとしても認証することを通じて正規のユーザとして扱われます。３節の方法（ドメイン名と IP アドレスの組み合わせ）を使っても，ドメイン名と IP アドレスさえ合致すれば他人になりすましてメールを送信することができますが，SMTP 認証を使うとなりすましを行うことは難しくなります（厳密に言うと，現在の多

[5]Windows 用のメールソフトについては，例えば http://www.emaillab.org/win-mailer/ をご覧ください。

くの MTA の仕様では SMTP 認証を使っても自ドメインの他のユーザになりすましてメールを送信することは可能です)。

EIMS では EIMS 2 の時代より他の MTA に先がけてこの SMTP 認証を実装していました（ただし，EIMS 2 では CRAM-MD5 認証のみ)。EIMS 3 では認証方式として CRAM-MD5，PLAIN，LOGIN の３方式に対応しています。このうちで暗号をかけて認証するのは CRAM-MD5 方式だけです。上の３で定義した IP アドレス以外から EIMS を使って送信するには，この SMTP 認証を使うとよいでしょう。ユーザがすべて SMTP 認証でメールを送信し，メールの受信も APOP 認証を行うのであれば，アカウント設定の所で「Require secure authentication」にチェックを入れてください。そうではなくて，内部からは通常の送信方法をとるが，外部からは SMTP 認証と APOP 認証を行うという場合には，「Require secure authentication」のチェックを外してください。ここのチェックを外していても，SMTP 認証や APOP 認証を行ってくるクライアントには EIMS はそれぞれの方式で対応します。非常に柔軟性に富んでいます。

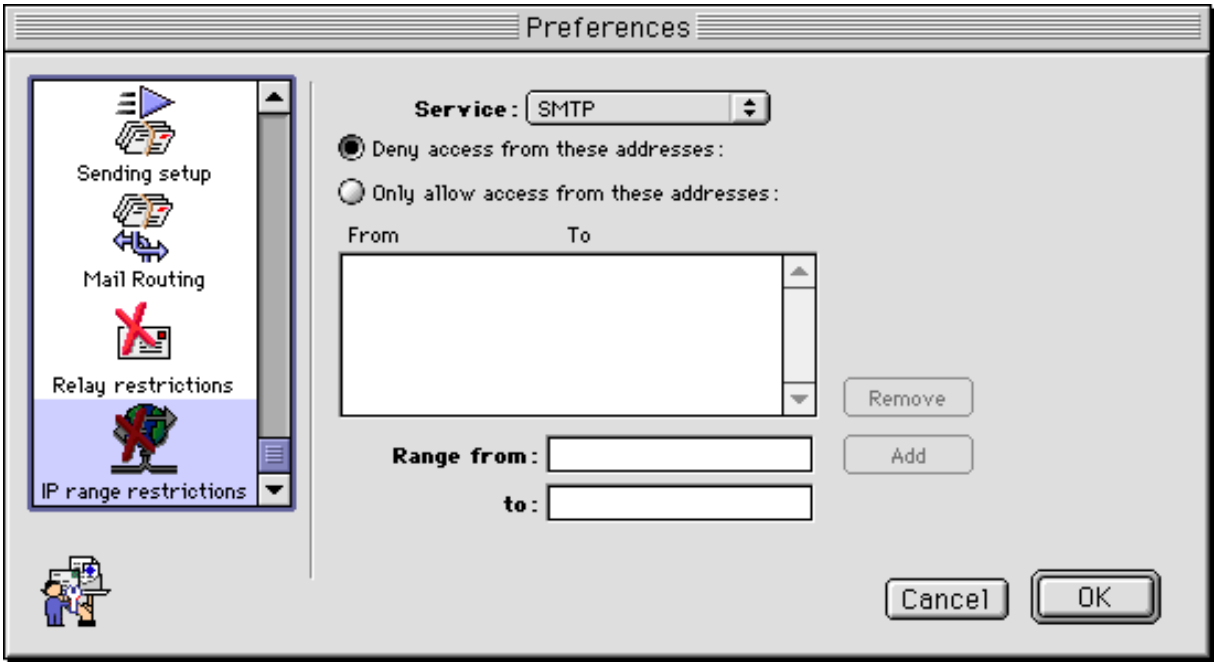
さらに一歩進めば次のような設定ができます。そして管理上は非常に楽になります。それは３の設定の認められた IP アドレスのところをブランクにすることです。こうするとユーザはどこにいようと SMTP 認証を使わなければメールの送信ができなくなりますので，いわゆる「なりすまし」などによるメールの送信が内部の者であっても行いにくくなります。

５．SPAM メール受け取りの許否

SPAM メールという言葉を聞くようになって久しいですが，サーバ管理者にとってはこの言葉は２通りの意味をもっています。１番目は自分の管理するサーバを踏み台にして SPAM メールを第３者にばらまかれる，いわゆる不正中継を許すという意味です。この意味の SPAM メール（の中継）を防ぐ方法は上に述べたとおりです。もう１つの意味は，SPAM メール（unsolicited commercial email，UCE）自体を自分の管理するサーバが受け取ってしまうという意味です。本節ではこの２番目の意味の SPAM メールの問題について考えます。

・known spammer の場合

ほとんどあり得ないケースだと思いますが，まれに存在するケースです。spammer が同一のホストから繰り返し SPAM メールを送ってくる場合には，EIMS Admin の Preferences の IP range restrictions でサービス名「SMTP」を選び，「Deny access from these addresses:」をチェックして，下欄にアクセスを禁止したいホストの IP アドレスを追加します（下図参照)。



・unknown spammer の場合

厄介なのがこのケースです。spammer が自分自身のサーバを使ってメールを送信するのではなく，オープンリレーになっているサーバを探し出して，そのサーバを使って送ってくるケースです。上に述べたケースと同様にして逐一オープンリレーのサーバをアクセス禁止にすることもできますが，違うオープンリレーのサーバを探し出してメールを送ってきますので徒労に終わる可能性が大です。

EIMS はこの手の SPAM メールの受信を拒否するために「フィルター」と呼ばれる一種の plug-in （本体の機能を拡張するもの）をもっています。これらのフィルターも３種類程に分類できます。

1) SPAM メールだとおぼしきメールの受け取りを拒否するフィルター
2) オープンリレーになっていると思われるサーバからのメールの受け取りを拒否するフィルター
3) SPAM Trap フィルター
4) 後述するウイルス用のフィルター

です。ここでは，1)，2)，3)について述べます。まず 1)については以下のようなフィルターがあります。

・ Advertisement フィルター： サブジェクトが，AD:，ADV:，ADVERTISEMENT で始まるメッセージの受け取りを拒否するフィルターです。
・ Message-ID フィルター： Message-ID に「@」のないメールの受け取りを拒否するフィルターです。
・ Route Address フィルター： アドレスの中に 「% 」や「!」があったり，「@」で始まるメッセージをはじくフィルターです。

・Space Patrol フィルター：　EIMS の作者の Glenn Anderson さんの　Filters for EIMS 2.2 and later（http://www.mactcp.org.nz/eims/eimsfilters.html）で入手出来ます。サブジェクトに連続して８文字以上のスペースがあるメッセージの受け取りを拒否するフィルターです。

使用方法は簡単です。EIMS Server が入っているフォルダに「Filters (Disabled)」というフォルダがあります。デフォルトでは，この中にすべてのフィルターが入っており，必要に応じて「Filters 」フォルダーに放り込みます。いったん放り込んだら，EIMS 自体を再起動するとフィルターが有効になります。

次に 2)です。EIMS 本体に発信元がオープンリレーのサーバ経由かどうかを判断する機能はありません。他の MTA と同様です。発信元がオープンリレーのサーバ経由かどうかを調べるのに，いわゆる第３者間リレー（あるいは不正中継）調査機関のもっているデータベースを参照する方法があります。有名なものには，Mail Abuse Prevention System (MAPS) があります。

・MAPS RBL フィルター：　MAPS Realtime Blackhole List を参照して，SPAM メールの受け取りを拒否するフィルターです。
・MAPS DUL フィルター：　MAPS Dial-up User List を参照して，Dial-up 経由で発せられる SPAM メールの受け取りを拒否するフィルターです。
・MAPS RSS フィルター：　MAPS Relay Spam Stopper を参照して，オープンリレーのメールサーバ経由で発せられる SPAM メールの受け取りを拒否するフィルターです。

MAPS の上記データベース参照はこれまで無料でしたが，2001 年 7 月末をもって，そのサービス利用が基本的に有料となりました。無料で利用できる不正中継調査機関と EIMS 用のフィルターの一覧については，dr.moensted さんの　dr.moensted's Eudora Internet Mail Server page (http://www.moensted.dk/eims/)等をご覧ください。

ただし注意しないといけないのは，これらのデータベースは各調査機関が独自のテストや判断基準で不正中継を判断したり，場合によっては不正中継は行われていないのに，上位のプロバイダが不正中継をしていて不正中継を改めないために，下流のプロバイダがたとえ不正中継を許していない設定になっていてもブラックリストに載せられるようなことがあるということです。したがって SPAM メールではないような正当なメールであっても，サーバが何らかの理由でこれらのリストに載っているというだけで受け取りを拒否してしまいますので，十二分に注意をしてください。

最後に 3)です。spammer はいろいろな方法でメールアドレスを集めます。一昔前であればニュースグループ等から集めましたが，現在有効な方法の１つに Spambot などといわれるインターネット上を徘徊するロボットがウェブサイトからアドレスを収集するものがあります。Spam Trap はこの手法の逆手を取るものです。つまり，偽のアドレスをウェブのページに埋め込んでおいて，ロボットが拾ってきたそのアドレスを含む EIMS の管理するユーザ宛に spammer が SPAM メールを送ってきたときに，送ってきたメールすべてをシャットアウトする方法です。いわば EIMS の管理するド

メイン単位での防御方法といってよいでしょう。

設定方法ですが，

・EIMS 上で，SpamTrap をしかけるアカウントを作成する（例：trash@mydomain.com)。
・ Web ページ上で，コメント文で「trash@mydomain.com」を埋め込む。
・このアカウントが有効で，サイズ制限がないことを確かめる。
・ResEdit （http://developer.apple.com/tools/ResEdit213.hqx）で SpamTrap フィルターを開き，STR# リソース ID 128 の 1 番目(string 1) に，つくったアカウントのフルのアドレスを書く。
・このフィルターを，Filters フォルダに入れる。
・ EIMS をいったん終了し，もう 1 度起動する。

の手順を踏むと有効になります。

余談ですが，Spambot などにアドレスを集められない方法としては

・メールアドレスを文字ではなく gif のファイルなどにしてウェブのページに張り付ける
・username@host.** という形式ではなく，たとえば username AT host などや username @ host などのブランクをおいた表示形式にする

等があります。一番いいのはメールアドレスをウェブのページに載せないことですが，無理な場合にはこのような方法があります。

６．ウイルス対策[6]

SPAM メールとともに管理者を悩ませるのが，ウイルスメール対策です。MTA 自身でウイルスメール対策ができるのは現時点ではないと思います。多くの場合，他のプログラムをプラグインとして組み合わせたり，ゲートウェイ専用のサーバを設けるなどしてチェックをしています。

EIMS の場合は上で述べたフィルターを使ってファイル名やファイルの拡張子，サブジェクトに特定の文字が含まれている場合にメールの受け取りを拒否します。例えば次のようなフィルターがあります。

・EXE Filter： 拡張子に EXE をもった添付ファイル付きのメールをはじくフィルターです。
・ Melissa Virus フィルター，Happy99 Virus フィルター，Papa Virus フィルター： それぞれのウイルスを含んだメールをはじくフィルターです。

---

[6] コンピュータウイルスが何故つくられるのか，またユーザの側で何故容易に退治できないのかについて本稿では詳しく述べることはできません。中村(2001)を読むことをお勧めします。

・VBS/Loveletter Virus フィルター，VBS フィルター： ILOVEYOU ウイルスや，visual basic script の添付ファイルを含んだメールをはじくフィルターです。

デフォルトでは，Filters (Disabled) フォルダにこれらのフィルターがありますが，見あたらないものがあれば，EIMS の作者の Glenn Anderson さんの Filters for EIMS 2.2 and later（http://www.mactcp.org.nz/eims/eimsfilters.html）で入手出来ます。また dr.moensted's Eudora Internet Mail Server page (http://www.moensted.dk/eims/) にも数多くのウイルス用のフィルターがあります。

メールの中身を見るのではなく，あくまでも文字列を頼りにウイルスメールかどうかの判断をしますので，他の方法と同様に新規のウイルスには威力が余りありませんが，サーバにかけるオーバーヘッドははるかに少なくて済みます。また新しいウイルスが出現しても，ResEdit を使ってフィルターを自分自身でカスタマイズできますので，速やかな対応が可能となっています。

ただし，ウイルスが実際には含まれていなくても該当する文字列があればはじいてしまいますので，特に EXE フィルターなどを適用するときは前もってユーザに周知徹底しておく方がよいでしょう。

７．メールサーバ自身に対する攻撃の防御

ひとえにメールサーバに対する攻撃といってもメール爆弾をはじめいろいろなものがあると思います。ここでは最近多く見られるようになってきたいわゆる Rumplestiltskin Attacks に対する防御法を考えてみます。

Rumplestiltskin Attacks とは，メールサーバに対する古典的な攻撃方法の１つである dictionary attack の変種です。もともとは SPAM メールを送りつける有効なアドレスを得るために，手当たり次第にターゲットとなるホストにメールを送りつけ，アドレスを得るのが目的でしたが，非常に短時間に無数のコネクションを張ることを要求してきますので，攻撃対象となったサーバの側では応答するのに精一杯となってメールサーバとしての機能がダウンしてしまうことになります。

次の表はこのアタックを受けたときのサーバ側に記録されるログの一例です。MTA は sendmail を想定しています。

```
Dec 16 211601 king.econ sendmail[5119] VAA05119 <mark@king.econ.kobe-u.ac.jp>... User unknown
Dec 16 211601 king.econ sendmail[5120] VAA05120 <brian3@king.econ.kobe-u.ac.jp>... User unknown
Dec 16 211602 king.econ sendmail[5119] VAA05119 <mark1@king.econ.kobe-u.ac.jp>... User unknown
Dec 16 211602 king.econ sendmail[5120] VAA05120 <brian4@king.econ.kobe-u.ac.jp>... User unknown
Dec 16 211606 king.econ sendmail[5120] VAA05120 <brian5@king.econ.kobe-u.ac.jp>... User unknown
Dec 16 211607 king.econ sendmail[5119] VAA05119 <mark2@king.econ.kobe-u.ac.jp>... User unknown
Dec 16 211607 king.econ sendmail[5126] VAA05126 <smith@king.econ.kobe-u.ac.jp>... User unknown
Dec 16 211608 king.econ sendmail[5126] VAA05126 <smith1@king.econ.kobe-u.ac.jp>... User unknown
Dec 16 211610 king.econ sendmail[5126] VAA05126 <smith2@king.econ.kobe-u.ac.jp>... User unknown
Dec 16 211610 king.econ sendmail[5135] VAA05135 <wilson3@king.econ.kobe-u.ac.jp>... User unknown
Dec 16 211611 king.econ sendmail[5137] VAA05137 <me@king.econ.kobe-u.ac.jp>... User unknown
Dec 16 211613 king.econ sendmail[5119] VAA05119 <mark3@king.econ.kobe-u.ac.jp>... User unknown
```

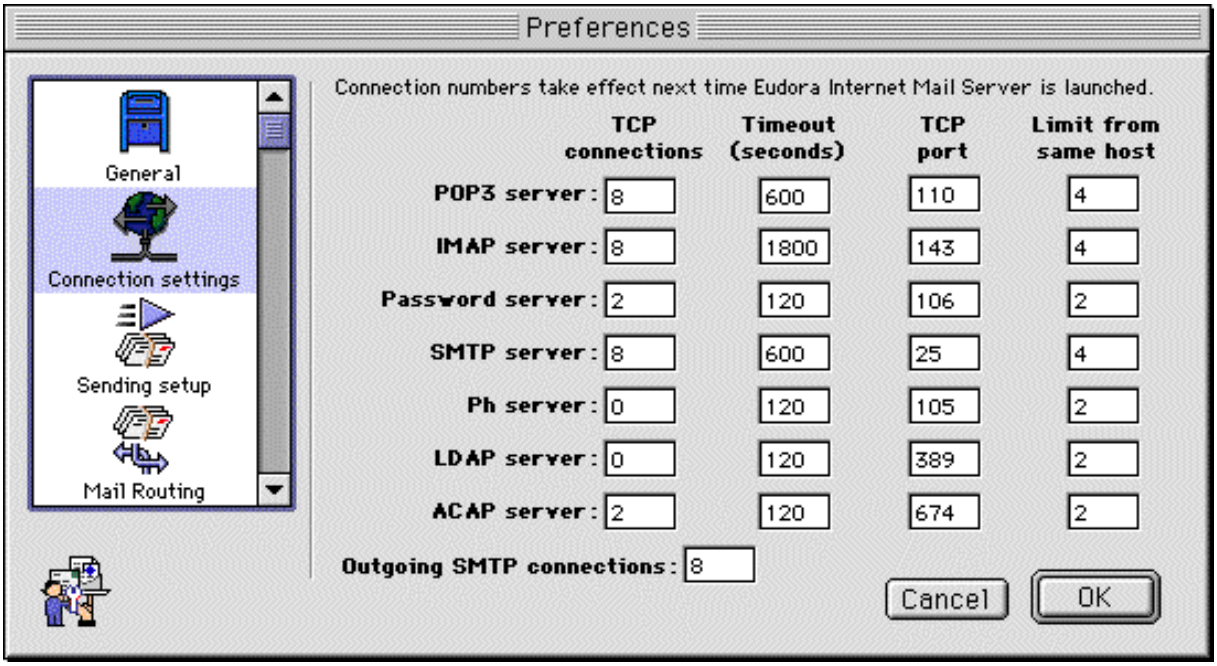
このアタックで困ることは,

・RCPT TO: コマンドで宛先を書いてくるが，pipelining の処理により，サーバ側が反応を返す前に処理を続けるので，サーバ側のレスポンスが極端に悪くなる（場合によってはダウンする)。
・メッセージ自体は送りつけてこず，コネクションをきちんと切ってくれない。
・多くの MTA では特定のアドレスから単位時間あたりに入ってくる SMTP の incoming connection を制限することは出来ない（EIMS と Stalker Internet Mail Server (SIMS, http://www.stalker.com/SIMS/)は例外)。またタイムアウトの時間をかなり長く取っているので，タイムアウトを迎える前にサーバとしての機能がダウンする。

などです。

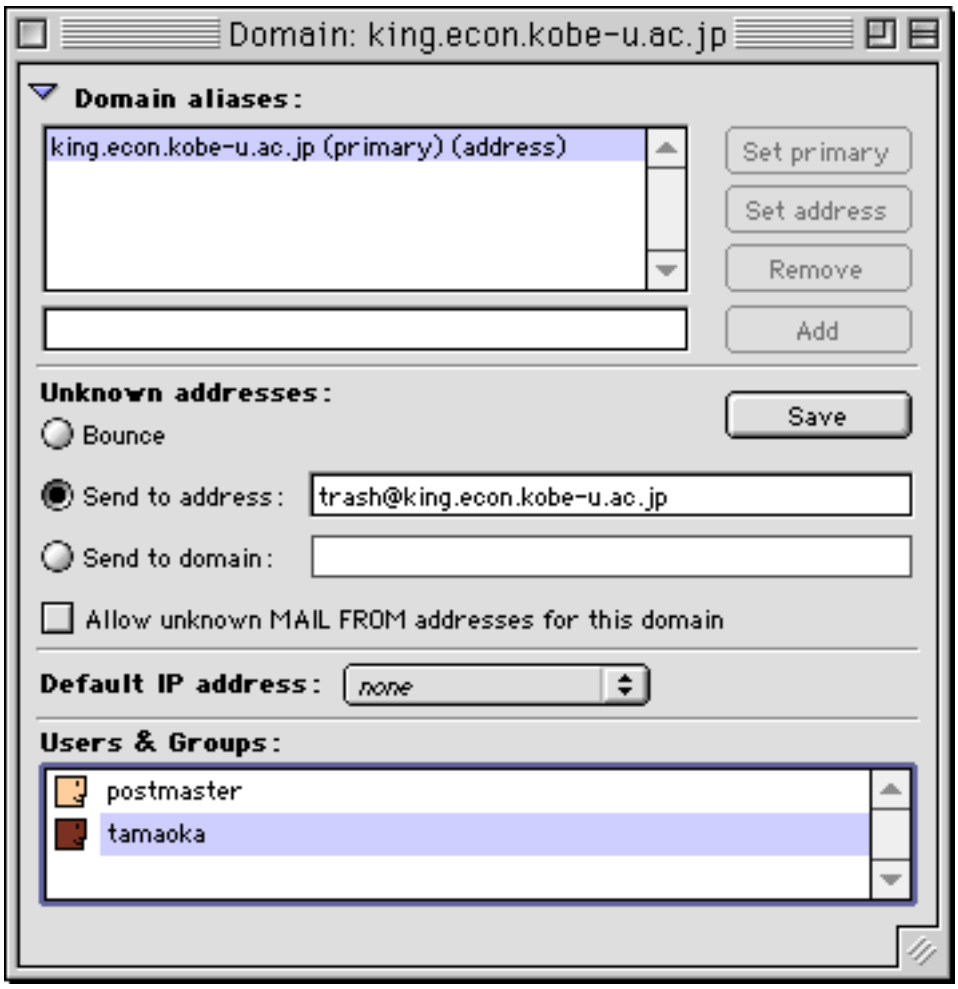
このアタックを根本的に防ぐ方法は現在のところありませんが，特定の IP アドレスから単位時間内にたくさんのコネクションが張られてくるので，そのような事態を避ける方策を施すとよいものと思われます。EIMS ではこの機能を実装していますので，設定方法を説明します。

EIMS Admin の Preferences から Connection setting を選びます。SMTP server のところに，Limit from same host がありますが，ここのところを出来るだけ低い数字にします。



ただし，これでも不十分だと思われるかもしれません。相手側の意図は使われている有効なアドレスを得ることにありますから，「User Unknown」の反応を返さない方法もあります。その方法の１つに，存在しないアドレス宛のメールはサーバ内部で処理してしまうというのがあります。

EIMS のドメインウインドウで Users & Groups のすぐ上に右向きの矢印がありますが，そこをクリックすると下図のようになります。真ん中に「Unknown addresses:」という項目があります。デフォルトでは「Bounce」が選択されており，存在しないアカウントに来たメールは送り主に戻されます。



この部分を真ん中の「Send to address:」にし，Unknown address に来たメールを指定したアドレスに転送することができます（ここのメールアドレスはホスト名まで含めたフルの形で書いてください)。Postmaster アカウントでもよいし，図のように使い捨てのアカウントでも構いません。ただしこの場合でもこのドメイン宛のすべての Unknown address 宛のメールが同様の扱いを受けますので，SPAM メールでない場合は管理者の側で適切な処理が必要となります。

最後にいわゆるゲートウェイサーバを設ける方法を EIMS を使って説明します。

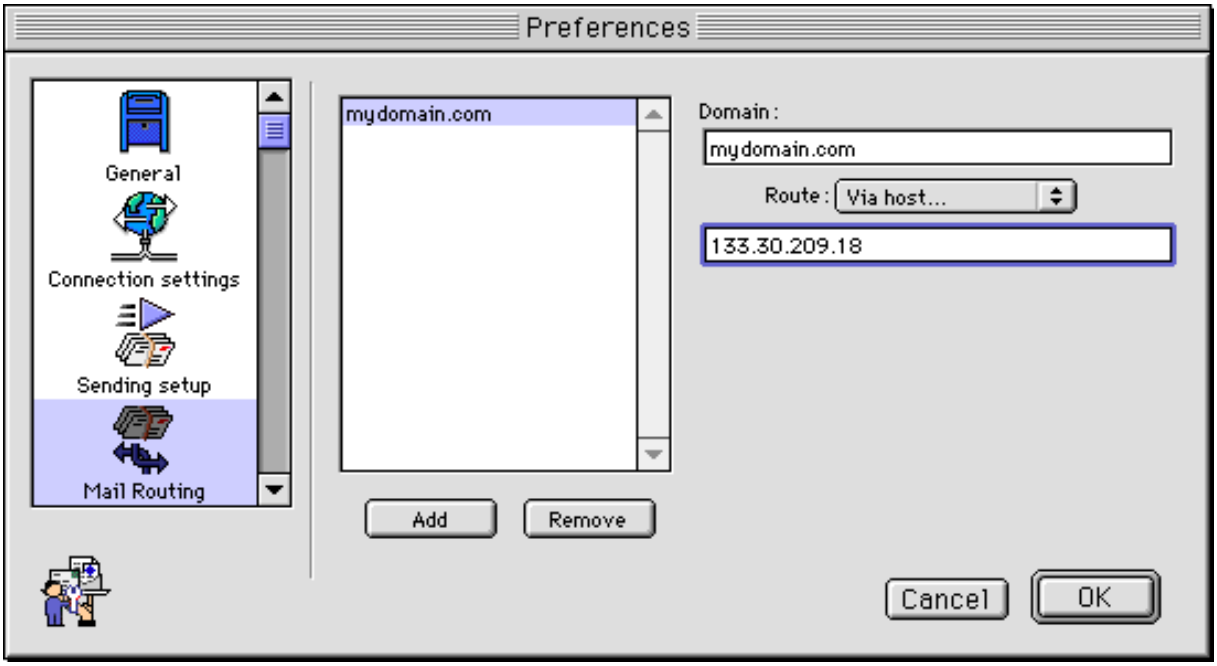
１．ユーザは「user@mydomain.com」というメールアドレスをもつ。ユーザの使う SMTP サーバと POP サーバは「mail2.mydomain.com」とする。
２．DNS の MX レコードを適切に設定して，外からみて受信専用のサーバ（ゲートウェイサーバ）をたてる（mail1.mydomain.com とする)。アカウントはもたない。
３．mail1.mydomain.com 宛のメールは EIMS のルーティングによってアカウントをもつ mail2.mydomain.com に渡される。このとき mail2.mydomain.com の SMTP 接続は mail1.mydomain.com のみから認めるようにする。
４．ユーザは mail2.mydomain.com を使ってメールの送受信を行う。

２の設定方法ですが，DNS で例えば次のように設定します。

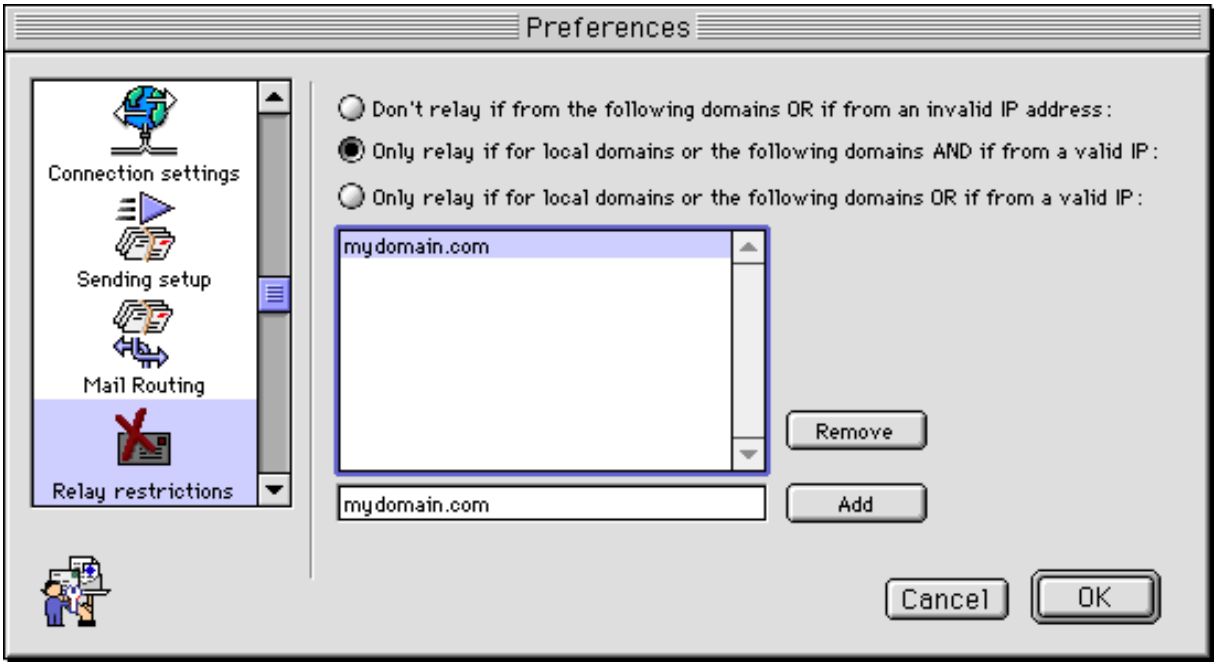
mydomain.com　MX　10　mail1.mydomain.com

こうすることにより，外側からは mydomain.com 宛のメールは mail1.mydomain.com が受け取ることになります。また次の 3 の設定によってユーザがメールの受け取りに使う mail2.mydomain.com には外側からは直接メールを送信できないようにします。

3 の設定方法は以下のようにします。EIMS Admin で mail1.mydomain.com に接続し，Preferences から Mail Routing を選びます。ここで Add ボタンをクリックし，右上の「Domain」の項にはメールアドレスとして指定してあるドメインの「mydomain.com」を入力し，Route: Via host... の下の空欄にはユーザの送受信用のサーバである mail2.mydomain.com の **IP アドレス**を入力します。

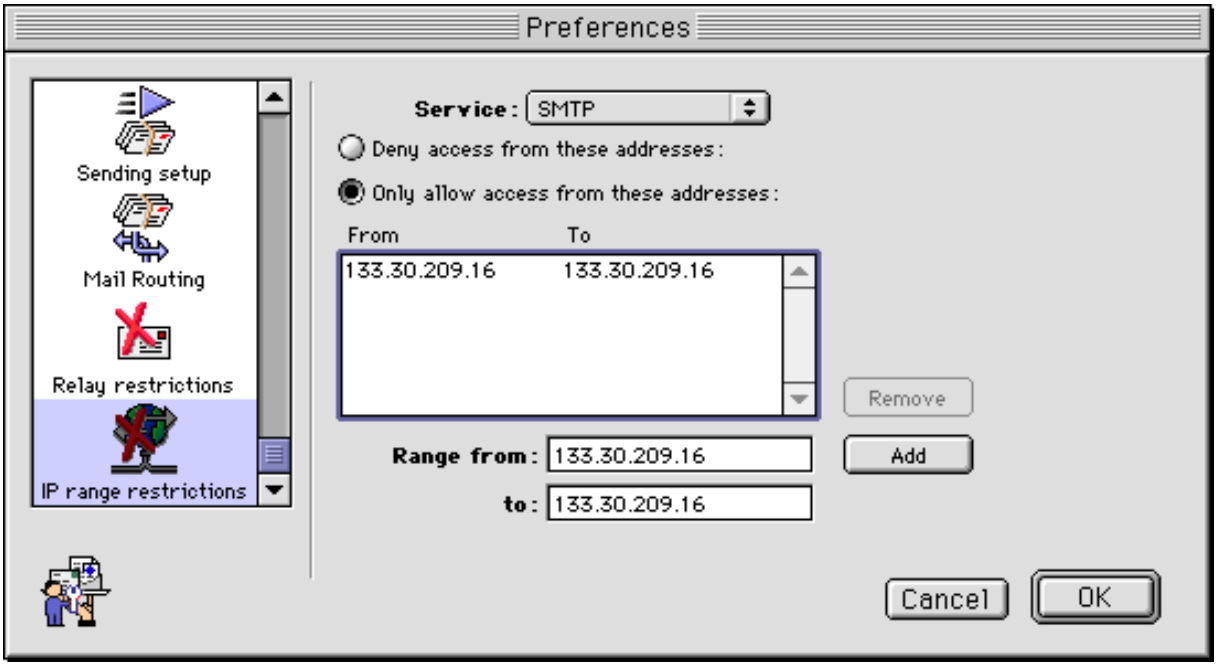


また mail1.mydomain.com の Relay restrictions のところでは，下図のようにユーザのメールアカウントのドメイン名である mydomain.com を Add します。mail1.mydomain.com から見れば，自分で受けた mydomain.com 宛のメールは mail2.mydomain.com へのルーティングによってリレーとみなされるからです。



そして mail2.mydomain.com の SMTP 接続を mail1.mydomain.com のみから認めるようにするには，下図のように，EIMS Admin で mail2.mydomain.com に接続し， Preferences から IP range restrictions を選び，Service の SMTP で，「Only allow access from these addresses:」を選んで，mail1.mydomain.com の IP アドレスを Add します。

こうすることにより，外側から見えているサーバ宛のメールはすべて mail2.mydomain.com にルーティングされます。



上の設定を行うと

１．多くの dictionary attack は大量に RCPT TO コマンドを送るが，データを実際には送らないので，アカウント情報をもっていないゲートウェイサーバは User Unknown の返事を返すことがない。
２．万が一，実際にデータを送ってきたとしても，宛先は大量にあるが EIMS の管理するドメイン宛に同じメッセージが送られるときは，張られるコネクションの数は１となるので，ゲートウェイサーバがコネクションで溢れかえって機能停止に追い込まれることはない。ユーザは mail2 を使ってメール送受信を問題なく行える。

ということになります。またゲートウェイサーバはアカウントをもたず，mail2.mydomain.com へルーティングするだけですから，ライセンス上はバックアップメールサーバと同じ扱いになり，追加的なライセンスを払う必要がない（http://www.eudora.com/techsupport/kb/2147hq.html を参照）ことも魅力です。

８．最後に

EIMS は数ある MTA の中でもきわめて早い時期に SMTP 認証を実装するなど機能面，管理のしやすさ等を考えて現存する MTA の中でももっともバランスのとれたメールサーバであるといえます。EIMS ユーザの中には３万人ものユーザを扱っている方もおられます。

Mac OS 自体がその構造上不正侵入を受けにくいようになっていますが，メールサーバなどインターネット上でのサービスを提供する際は OS そのものではなくて，そのサーバがどのように設定されているかによって不正に利用されたりしますが，EIMS は不正中継を防ぐ設定も分かり易くできています。

また，他のプラットフォームから乗り換える際もユーザ名，パスワード名等の情報が分かっていれば手軽にそれらの情報をユーザのデータベースにインポートできます。

設定が容易でかつセキュアなサーバの構築は一見難しそうですが，EIMS であればそれが可能であると思います。デモ版が入手可能ですので，是非一度お試しください。

参　考　文　献

・ Eudora Internet Mail Server Version 3.0 Administrator's Guide, QUALCOMM Incorporated., 2000.

・Masayuki TAMAOKA, 私家版 EIMS FAQ ，http://pf.econ.kobe-u.ac.jp/mac/eims/eimsfaq.html

・Masayuki TAMAOKA, EIMS 3.0 運用メモ, http://pf.econ.kobe-u.ac.jp/mac/eims/eims3.html

・Masayuki TAMAOKA, Anti-Spam for Macintosh, http://pf.econ.kobe-u.ac.jp/mac/spam/anti-spam.html

・Masayuki TAMAOKA, ORBS メモ, http://pf.econ.kobe-u.ac.jp/mac/spam/orbs.html

・Masayuki TAMAOKA, Rumplestiltskin Attacks, http://pf.econ.kobe-u.ac.jp/mac/spam/Rumplestiltskin.html

・中村　正三郎『ウイルス、伝染るんです』（ISBN4-331-50771-8）廣済堂出版，2001.

・RFC2476, "Message Submission " , http://www.ietf.org/rfc/rfc2476.txt, 1998.

・RFC2554, "SMTP Service Extension for Authentication", http://www.ietf.org/rfc/rfc2554.txt, 1999.