ウィルスメールチェックモジュール　feplg_smtp.so

http://www.nsl.tuis.ac.jp/
mailto:iseki@rsch.tuis.ac.jp

０．免責＆ライセンス

このソフトウェアは全くの無保証であり，このソフトウェアを使用することによって，メールが届かなかったり，メールが破壊される等の損害が生じても，作者は何の保証も行ないません．使用する場合は，これらメールの不達，破壊が十分起こりうる現象であることを認識して，自己責任でお使いください．また，改造・再配布に伴い発生する問題に関しても，作者は一切の責任を負いません．

このプログラムは商用以外ではフリーです．再配布・ライブラリの再利用（改造を含む）は自由ですが，再配布する場合は，配布されたものを完全な形で再配布してください．ライブラリの再利用では Copyrightを明記してください．

商用に利用する（このソフトウェアに対して対価を要求する）場合はご連絡ください．

１．概要

基本的な動作のアルゴリズムは非常にシンプルである．このモジュールは通常はクライアントとメールサーバプログラム間の通信をそのまま中継する．クライアントからの”DATA”コマンドをメールサーバプログラムに渡し，354の応答（メール本文の受信準備完了の応答）を受信すると，モジュールは次の通信からメールサーバへの中継を一時中止し，通信内容（メールの内容）を作業ファイルに書き込む．

クライアントから”<CR><LF>.<CR><LF>”を受け取ると(それも作業ファイルに書き込んでから)，作業ファイル内をチェックし添付ファイル名を抜き出す．次に添付ファイル名の拡張子のチェックを行い，登録されているものと一致した場合，添付ファイルの拡張子の一部を書き換え，また拡張子を書き換えた旨の文章をメールに追加してメールサーバへ転送する．

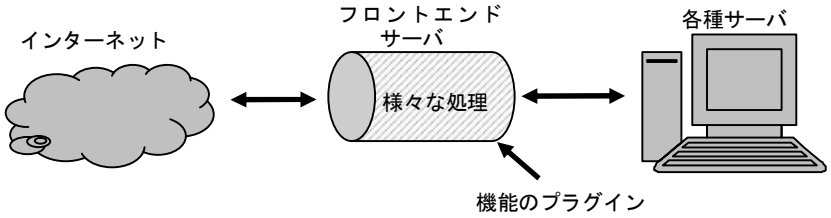
添付ファイルに問題が無い場合は，作業ファイルの内容をそのままサーバに送信して，以後はまた通常通りクライアントとメールサーバの間で通信を中継する．

”RSET”コマンドの受信では，メールサーバプログラムに”RSET”を中継し，成功応答(250)を受信した時点で自らの内部状態も初期化する．

メールサーバプログラムから見ると，フロントエンドサーバがメールを送信しようとしているように見えるため，このモジュールにはアクセスコントロールの他にメールリレーチェック用の機能が必要である．アクセスコントロールではアクセス許可リストと禁止リストをファイルとして作成して置き，プログラム起動時にこれを読み込み，接続相手のIPアドレスから接続の可否を決定している．現在の所では，許可リスト優先で，許可リストがあればそのリストに登録されてるアドレス以外のマシンからの接続を拒否している．

またリレーチェック用についても，ローカルグループリストと配送許可アドレスリストをファイルとして作成しておき，これも起動時に読み込む．ローカルグループのチェックではクライアント接続時に，配送許可アドレスリストのチェックでは”RCPT TO:”コマンド受信時にそれぞれ行い，二つの結果からリレーの可否を判断している．

しかしながら，メールのリレー制限についてさらに複雑な制御を行ないたい場合は，受信用と送信用の２つのメールサーバを用意するなどの対応が必要となる．



フロントエンドサーバの概要

２．インストール方法

このプログラムはコンパイルに JunkBox_Lib を必要とする．JunkBox_Lib の最新版は Feserver をダウンロードしたページと同じページ(http://www.nsl.tuis.ac.jp/)でダウンロードできる（もしくは同梱されている場合もある）．

ファイルを展開し,Feserver ディレクトリに移動する.Makefile を環境に合わせて編集し,make, make insall でインストール可能である.

ライブラリをコンパイルするには，openSSLがインストールされていなければならない．しかし，fepleg_smtp.so ではopenSSLの機能を使用していないので,openSSLをインストールするのが面倒な場合は,ライブラリのMakefile でこれらを使用しているファイルをコンパイルしないように指定することも可能である．（詳しくはMakefile,ソースファイルを見よ）

openSSLを使用しているファイル：JunkBox_Lib/xLib/ssl_tool.c, JunkBox_Lib/xLib/isnet.c

インストール手順

```
su
tuis_lib, feserver を同じディレクトリで展開
cd Feserver
vi Makefile
make
make install
```

３．機能

.COM, .EXE, .SCR, .VBS, .PIF, .BAT, .DLL, .ZIP の拡張子の付いたファイルを添付してきた場合，拡張子を変更する．また変更した旨を伝えるメッセージをメール本文に追加する．これ以外の拡張子を禁止したい場合，feplg_smtp_tool.hのBADEXTENTIONS マクロを書き換える（スペースの挿入なしで，前後の．は必ず必要）．

```
#define  BADEXTENTIONS  ".COM.EXE.SCR.VBS.PIF.BAT.DLL.ZIP."
```

４．アクセス制御

SMTPにFEServer を使用すると,SMTPサーバ本来のIPアドレスによるアクセス制御ができなくなる．そのため feplg_smtp.so には必要最低限のアクセス制御機能が実装されている．feplg_smtp.so のアクセス制御は以下のファイルにより行われる．

/etc/feserver/smtp/allow.list

アクセス許可リスト．1行に1つのIPアドレス（サブネット付きまたはCIDR表記可），またはFQDN

を指定する．このファイルを作成した場合，このファイルに記載されていないサーバからの接続を禁止する．SMTPサーバの通常の運用では不必要だと思われる．制御を行わない場合はファイルを作成しないこと．

例）
192.168.1
192.168.3.1/255.255.255.240
202.26.144.0/20
smtp.coolmail.com

/etc/feserver/smtp/deny.list
　アクセス禁止リスト．1行に1つのIPアドレス（サブネット付きまたはCIDR表記可），またはFQDNを指定する．allow.listと全く同じ書式で記述する．このファイルを作成した場合，このファイルに記載されているサーバからの接続を禁止する．allow.listとdeny.listの両方を作成した場合は，allow.listを優先し（allow.list以外は全て禁止するので），deny.listは無視する．SPAMメールサーバなどからの接続を拒否する場合に指定する．

/etc/feserver/smtp/localip.list
　ローカルグループリスト．1行に1つのIPアドレス（サブネット付きまたはCIDR表記可），またはFQDNを指定する.SMTPサーバがメール配送（リレー）を受け付けるアドレスを指定する．通常は自組織のIPアドレス（Networkアドレス）を指定する．作成しなかった場合はデフォルトでFEServerが属する Networkアドレスを配送受付範囲とする．

/etc/feserver/smtp/mydest.list
　配送（リレー）許可アドレスファイル．メールを受け取るメールアドレス（の一部）を記述する．そのメールアドレス(を含むアドレス)は自組織のメールアドレスとして取り扱う(リレーを行う)．省略不可．ファイルが無い場合はプログラムは停止する．

例）
tuis.ac.jp

例の説明）tuis.ac.jp を含むアドレス（edu.tuis.ac.jp，rsch.tuis.ac.jp等）を自組織のメールアドレスとして，このメールアドレスへのメールの配送（リレー）を許可する．

リレーの可否の判断　○：アドレスがファイル中にある　×：ファイル中にない．

ローカルグループ	配送許可アドレス	リレーの可否
○	○	可
○	×	可
×	○	可
×	×	否

　アクセス制御は重要な機能であり，ファイルの記述ミスにより思わぬ動作をしないように，アクセス制御ファイルのチェックコマンド print_smtpacs が付属している．このコマンドを実行すると，feplg_smtp.soと同じようにアクセス制御ファイルを読み込み，その内部表現（解釈結果）を表示する．

アクセス制御ファイル（及び後述のメッセージファイル）のディレクトリを変更するには，make する前に feplg_smtp.h を書き換える．

このシステムは POP before SMTP 環境下では使用できない．また，feplg_smtp.soが提供するアクセス制御とは別のアクセス制御を行ないたい場合も，このシステムを使用することはできない．ただし，自分でプログラムを作成し，機能を追加するという手段は残されている．

５．メッセージファイル

/etc/feserver/smtp/rwmessage.text

feplg_smtp.soにより，添付ファイルの拡張子が書き換えられた場合に，メールに挿入する文章．自分で記述する場合は，JIS漢字コードで記述する．必須ファイルであり，存在しない場合はプログラムは停止する．

/etc/feserver/smtp/vrmessage.text

feplg_smtp.soにより，書き換えるべき添付ファイルの拡張子を見つけたが，アルゴリズムが貧弱なため拡張子を書き換えられなかった場合（恐らくはファイル名のエンコードに失敗）に，メールに挿入する文章．プログラマのへぼさを暴露するメッセージ．自分で記述する場合は，JIS漢字コードで記述する．必須ファイルであり，存在しない場合はプログラムは停止する．