fml のセキュリティ設定

fml の設定

・fml は，各メーリングリスト毎に ” config.ph ” ファイルで設定を行っている。

config.ph ファイル

・config.ph は，fml の動作を指定するための基本となる設定ファイル。
・makefml config(コマンド) による設定変更も，実際には，config.ph ファイルを変更することで設定を反映している。
  ・makefml（コマンド）は，config.ph の元となる cf というファイルを生成し，さらにそのファイルから config.ph を生成するスタイルをとっている。
  ・config.ph をエディタで編集した後，makefml config（コマンド）を使って設定を変更しようとすると，設定が上書きされてしまいうまくいかない。→注意
  ・一旦，エディタによる config.ph の編集を始めたら，それ以降は，makefml config（コマンド）には頼らずに設定するつもりでいなければならない。

config.ph の設定変更により，セキュリティを高める。以下，処方箋。

・メールサイズを制限する

$INCOMING_MAIL_SIZE_LIMIT 変数にメールサイズの上限を設定する。
単に数値を設定するか，「10K」，「1M」等の単位で指定する事が可能。
この変数を未定義にすると，このメッセージサイズの制限機能が停止する。

例：40KB に制限するときは，config.ph に以下の設定を追加する。

```
$INCOMING_MAIL_SIZE_LIMIT = "40K"; # maxsize = 40k bytes
```

・リモートコマンドを制限する

自動登録の公開メーリングリストの場合，アドレスリストを取得することだけを目的とした参加者が，メンバーリストを取得して即退会するといったことが起こり得る。
このような場合，参加者が使えるリモートコマンドを制限するという方法を取ると良い。
@DenyProcedure 配列を使って members コマンド等を使えないように設定する。
members コマンドは，member という別名もあるので，両方設定しないと意味がない。
actives，active，stat などメンバーに関するコマンドをすべて禁止する。

例：

```
@DenyProcedure = ('member','active','members','actives','status','stat');
```

又，さらに制限して get，summary，skip，noskip 以外は許さないといった場合には，@PermitProcedure を使って次のように設定する。

```
@PermitProcedure = ('get','mget','summary','skip','noskip');
```

・メーリングリストの存在を知られたくない

メンバー以外のアドレスから投稿やコマンドが送られたときに,「あなたはメンバーではない」と

いうようなメッセージを返す（reject）のではなく，単に無視（ignore）したほうが良い。その為の設定は，次のようになる。これは，makefml config のメニューでも設定可能。

例：
$REJECT_POST_HANDLER　= "ignore";
$REJECT_COMMAND_HANDLER = "ignore";

・メール爆弾を排除する（短期間に大量にメールを通知する場合注意）

fml は，メールの流量情報（MTI:Mail Traffic Information）を使ってメール爆弾を判定する機能が組み込まれている。
その仕組みは，「一定の短時間にどのくらいの量のメールが到着したか」を評価する機能。
ただし，オフラインでメールを書いてからインターネットに接続し，メールをまとめて発信するという方法は，一般的なので，それをメール爆弾と認識しないように Date: ヘッダの時刻も考慮に入れて評価を行っている。
判定基準は，次の通り。

（１）もし，Date: ヘッダの時刻で一定時刻あたりのメール数がある値（$MTI_BURST_SOFT_LIMIT）よりも多い場合，メール爆弾と判断。
（２）（１）の条件に当てはまらない場合でも，Date: ヘッダや fml メールへの到着数が一定値（＄MTI_BURST_HARD_LIMIT）を超えたらメール爆弾とみなす。

この２つのしきい値は，libmti.pl において次のように初期設定されている。

$MTI_BURST_SOFT_LIMIT=(5/5)
$MTI_BURST_HARD_LIMIT=(2*5/5)

（１）の条件がおおむね５秒あたり５通
（２）の条件が５秒あたり１０通を超えるとメール爆弾と認識する値。

　いったん，メール爆弾であると判定されると，$MTI_EXPIRE_UNIT 変数で設定された（設定されていない場合は，3,600 秒）間は，メール爆弾の送信元と判定されたアドレスから投稿しても配信がまったく行われない。

　この機能を使う為の config.ph は，次の通り

＄USE_MTI=1;
$MTI_BURST_SOFT_LIMIT=(5/5);# デフォルト値と同じ
$MTI_BURST_HARD_LIMIT=(3*5/5);# 条件を少し緩和している。

なお，この MTI によるメール爆弾の検出機構は，メールの無限ループの検出にも役立つ。
fml の通常の無限ループ検出では，Message-ID: が同じであることを検出して無限ループを止めるようになっているが，例えば，ユーザが作成したスクリプトの誤動作や，実装の悪い MTA 等が原因の場合には，毎回異なる Message-ID: を持つメールが送られることもある。このようなケースでは，MTI による判定機能でメールループを止めることができる。

・メールループを防ぐ

fml には，ループを防ぐ機構がいくつか組み込まれていて，もちろんデフォルトで機能している。

（ａ）Message-ID キャッシュ

メーリングリストのディレクトリ配下の var/run/ ディレクトリ（/home/ml/***/var/run/ となる）に，msgidcache というファイル名で fml が配信したメッセージの Message-ID が記録されている。fml は，このファイルの記録と新しく投稿されたメッセージの Message-ID を比較して，同じ場合，メールループと判定。これにより，配信されたメールがメーリングリストに戻ってきた（バウンス）しまっても，再度配信されることはない。この機能は，$CHECK_MESSAGE_ID 変数が 1 の時に有効で，デフォルトで有効になっている。

（ｂ）UNIX　From によるチェック

投稿者の UNIX　From が $MAINTAINER（つまり fml 自身）であるときは，ループと判断する。例えば，duke-ml@sushineta.com がメーリングリストアドレスのときは，$MAINTAINER は，duke-ml-admin@sushineta.com となるので，このアドレスから届いたメールは配信しない。

もし，この機能を停止する（ループチェックしない）のであれば，$NOT_USE_UNIX_FROM_LOOP_CHECK 変数に 1 をセットする。なお，これは，/etc/aliases で duke-ml-admin@sushineta.com のメールを実際に受け取っている人の実アドレスからのメールは，拒否しない。

あくまで，UNIX　FROM が duke-ml-admin@sushineta.com などとなっている場合にだけ制限がかかる。

（ｃ）投稿を認めないアカウント名

fml では，root や postmaster など，一般にユーザが使わないアカウントからの投稿は，認めないようになっている。

排除するアカウントは，$REJECT_ADDR に正規表現の形式「｜」で区切って登録する。config.ph のデフォルトでは以下のようになっている。

```
$REJECT_ADDR                                                    =
"root|postmaster|MAILER-DAEMON|msgs|nobody|news|majordomo|listserv|listproc|\S+\-help|\S+\-subscribe|\S+\-unsubscr
```

また，SPAM リストを使う方法もあります。投稿を認めないアドレスの正規表現を，spamlist ファイルに１行に１つずつ列挙して登録する。

```
$REJECT_ADDR_LIST = "$DIR/spamlist";
```

（ｄ）明らかに配信すべきでない From: を排除する。

From: が自分自身のアドレス（メーリングリストのアドレス）になっている等，明らかに不自然なヘッダを持つメールを排除する仕組みがある。

これは，外部からコントロールできるようにはなっていないが，fml.pl のループチェックの一連の処理の中で評価されている。

これは，$REJECT_ADDR などの設定とは関係なく有効。

以上，下記の参考書より抜粋。

参考図書
梅垣まさひろ『FreeBSD/Linux で始めるメーリングリスト管理者編』株式会社情報管理，1997 年
（173-266 頁の ｆｍｌ リファレンスが重宝。）

梅垣まさひろ・寺村綾子『ｆｍｌメーリングリスト管理』株式会社オーム社，2000 年
（227-231 頁がセキュリティについてよく記述されています。）

深町賢一『ｆｍｌバイブル』株式会社オライリー・ジャパン，2001 年
（257-312 頁のトラブルシューティング，日々の運用が有用。）

by 有限会社ケイアイエム（http://www.keiaiemu.com/)