# Postfix のログ解析ツール導入

教育研究支援センター
内藤岳史

## 1. はじめに

スパムの数は減ることを知らない。最近ではウィルスが添付されているスパムが多く，一日に 500 件以上届いている状況である。

本校宛のメールは，対外向けメールサーバから，ウィルス・スパム対策アプライアンスであるセキュリティゲートウェイを経由し，学内メールサーバに配送される。

学内にスパムを通さないようにし，ネットワークやセキュリティゲートウェイに無駄な負荷をかけないようにするため, 対外向けメールサーバで稼動している MTA である Postfix において，スパムを拒否するよう設定を施している。しかしログを見ただけでは，この設定によって送られてくるメールの内，どれだけのメールが拒否されたかを知ることは困難である。そこで，ログを解析し管理者に情報を与えてくれるログ管理ツールを導入する。今回は AWStats と pflogsumm の 2 つを実際に使用し，その使い勝手を見る。

## 2. AWStats

AWStats は Web サーバのログ解析を行って HTML を生成する CGI であり, Perl で書かれている。Analog や Webalizer など，ほかにもツールは存在するが，デフォルトで MTA のログ解析ができるという特徴がある。

### 2-1. AWStats の導入

① AWStats のホームページからソースをダウンロードし，展開する。現時点での安定版はバージョン 6.6 である。

```
#wget http://prdownloads.sourceforge.net/awstats/awstats-6.6.tar.gz
#tar zxvf awstats-6.6.tar.gz
#mv awstats-6.6 awstats
```

② 設定ファイル awstats.conf を編集する。

Postfix のログを AWStats で扱えるように，maillogconvert.pl で形式を変換する。ローテーションされた過去のログも解析されるように，LogFile ディレクティブを設定する。ログのローテーションは環境によって異なるため，注意する必要がある。

**リスト** 2：awstats.conf

```
LogFile="(cd /var/log; cat maillog.5 maillog.4 maillog.3 maillog.2
 maillog.1  maillog)"|  perl  /awstats-dir/tools/maillogconvert.pl
 standard |"
LogType=M
SiteDomain="fukui-nct.ac.jp"
HostAliases="REGEXP[^.+¥.fukui-nct.ac.jp]"
LogFormat="%time2 %email %email_r %host %host_r %method %url %code
 %bytesd"
LevelForBrowsersDetection=0
LevelForRefererAnalyze=0
LevelForRobotsDetection=0
LevelForWormsDetection=0
LevelForSearchEnginesDetection=0
LeverForFileTypesDetection=0
ShowMenu=1
ShowSummary=HB
ShowMonthStats=HB
ShowDaysOfMonthStats=HB
ShowDaysOfWeekStats=HB
ShowHoursStats=HB
ShowDomainsStats=0
ShowHostsStats=HBL
ShowAuthenticatedUsers=0
ShowRobotsStats=0
ShowEMailSenders=HBML
ShowEMailReceivers=HBML
ShowSessionsStats=0
ShowPagesStats=0
ShowFileTypeStats=0
ShowFileSizesStats=0
ShowBrowsersStats=0
ShowOSStats=0
ShowOriginStats=0
ShowKeyphrasesStats=0
ShowKeywordsStats=0
ShowMiscStats=0
ShowHTTPErrorsStats=0
ShowSMTPErrorsStats=1
Lang="jp"
DirCgi="/awcgi-bin"
DirIcons="/awicon"
```

③　Apache を設定する。内部ネットワークからのみアクセスを許可する。

**リスト** 3：httpd.conf

```
<Directory "/awstats-path/awstats/wwwroot">
       Options None
       AllowOverride None
       Order allow,deny
       Allow from 10.0.0.0/8
</Directory>
```

④　Apache を実行する。

```
#/etc/init.d/httpd start
```

⑤　Web ブラウザで http://Web サーバ/awstats/awcgi-bin/awstats.pl にアクセスする。

⑥　解析結果の更新を cron に登録する。

```
#crontab –e
```

リスト 4：crontab

```
0 0 * * * /awstats-path/awstats/wwwroot/cgi-bin/awstats.pl –update
–config=fukui-nct.ac.jp > /dev/null 2&>1          （毎日 0 時更新）
```

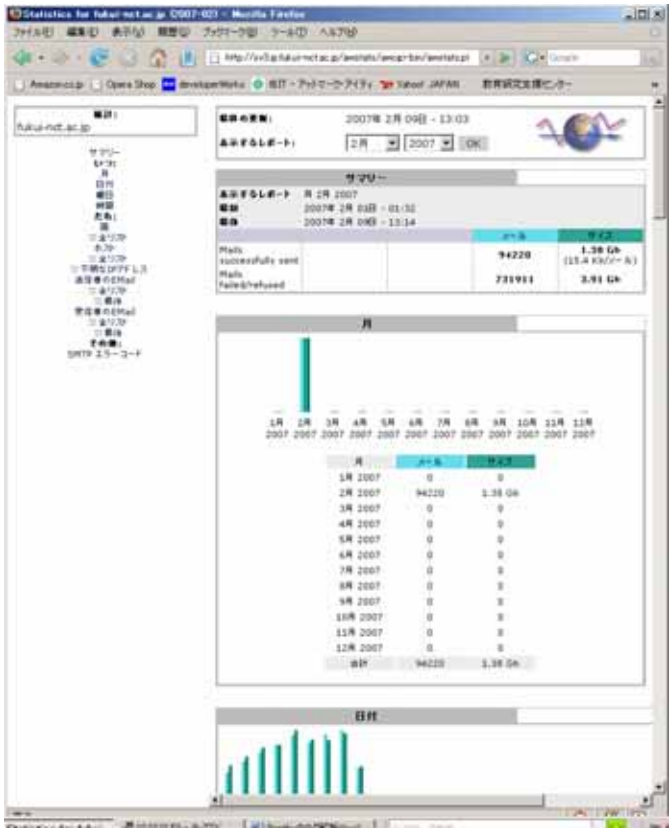

図 1：AWStats メインページ

### 2-2. AWStats を使用して

AWStats を使用し，特徴として以下のことが挙げられる。

・月，曜日，日，時間単位で送受信メール数の表示が可能(月単位)

・送受信ホスト名の上位 10

・送信者，受信者の各上位 10
・国別リスト
・不明な IP アドレスのリスト
・SMTP エラーの一覧

グラフィカルに解析情報を見れるため，現在の状況を把握しやすい。また以前の情報も見ることができるので，過去に遡っての解析も可能である。しかし，もともとは Web サーバのログ解析ツールであるため，時間単位でのメールの拒否数等の統計や，警告メッセージなど詳細な情報を知ることはできない。

## 3. pflogsumm

pflogsumm は Perl で書かれたスクリプトであり，結果をテキストで出力する。AWStats のように視覚的に結果を表示することはできないが，他のシェルコマンドと組合わせることで，管理者へのメール通知等を実行することが可能である。

### 3-1. pflogsumm の実行

ソースをダウンロード後，解凍し実行する。

```
#wget http://jimsun.linxnet.com/downloads/pflogsumm-1.1.0.tar.gz
#tar zxvf pflogsumm-1.1.0.tar.gz
#mv pflogsumm-1.1.0.tar.gz pflogsumm
#cd pflogsumm
```

（実行例）昨日のサマリーを生成

```
#pflogsumm –d yesterday /var/log/maillog
```

主なオプションは以下のとおりである。

表 1：pflogsumm オプション

| | |
|---|---|
| -d <today\|yesterday> | 今日または昨日のサマリーを生成 |
| --verbose_msg_detail | 詳細表示 |
| --problems_first | 警告等を先に表示 |
| --mailq | mailq コマンドを実行し終了 |

```
Postfix log summaries for Feb  9
Grand Totals
------------
messages

  43995   received
   9420   delivered
     13   forwarded
      0   deferred
  48376   bounced
  25719   rejected (73%)
      0   reject warnings
      0   held
      0   discarded (0%)

 231907k  bytes received
 150602k  bytes delivered
  17349   senders
  10395   sending hosts/domains
   8716   recipients
   4770   recipient hosts/domains

Per-Hour Traffic Summary
    time          received  delivered   deferred    bounced    rejected
    ------------------------------------------------------------------------
    0000-0100       2525       522         0       3122       1550
    0100-0200       3085       759         0       3738       1582
    0200-0300       3424       855         0       3742       1907
    0300-0400       3282       724         0       4262       1840
    0400-0500       3007       660         0       3982       1707
                                                    :
    2200-2300          0         0         0          0          0
    2300-2400          0         0         0          0          0

Host/Domain Summary: Message Delivery
 sent cnt  bytes   defers   avg dly max dly host/domain
 -------- -------  -------  ------- ------- -----------
   1159    26186k      0     6.6 s    5.8 m  fukui-nct.ac.jp
    406    12441k      0    12.8 s   10.6 m  ei.fukui-nct.ac.jp
                            :
Host/Domain Summary: Messages Received
 msg cnt   bytes   host/domain
 -------- -------  -----------
    686     5045k  fukui-nct.ac.jp
    417      962k  plimutfar.com
                  :
top 10 Senders by message count
-------------------------------
    108   from=<>
     35   0000digidigi@xxxxxx
                  :
top 10 Recipients by message count
----------------------------------
     17   naitou@xxxxxx
                  :
top 10 Senders by message size
------------------------------
  73700k  root@sv3.xxxxxx
   1742k  from=<>
                  :
    top 10 Recipients by message size
---------------------------------
   4203k  naitou@xxxxxx
                  :
message deferral detail: none
message bounce detail (by relay)
--------------------------------
  local (total: 1)
        1   unknown user: "r1.ru"
  secgw.ip.fukui-nct.ac.jp[10.10.21.55] (total: 48375)
     48033   Denied by policy.
       342   Syntax error - Badly formatted address.

smtp delivery failures: none
Warnings
--------
  local (total: 24)
       24   dict_nis_init: NIS domain name not set - NIS lookups disabled
  smtpd (total: 7154)
       49   66.11.122.167: hostname service66.11.122-167.serverprovider.com...
       27   209.51.190.110: hostname qsw-110-190.51.209-rf.ldnserve.net ver...
                                                  :
```

**図 2：**pflogsumm **実行結果**

### 3-2. pflogsumm を使用して

pflogsumm を使用し，特徴として以下のことが挙げられる。

- 1 時間単位での受信メール，配送メール，保留メール，送り返したメール，拒否メール数の表示
- 送り返したメールの詳細が分かる
- 送信者，受信者のメール数・メールサイズによるランキング
- smtpd の警告の詳細
- ホスト・ドメイン単位での配送遅延情報の表示

テキストでの出力となるので，一目で現在の状況を把握することは難しいが，詳細な情報を得ることができる。注意しなければならないのは，数日間に渡っての解析を行うと，時間単位でのメール数も数日間の合計となってしまうので，基本は 1 日単位での解析と考えたほうがよい。

## 4. まとめ

今回 AWStats と pflogsumm，2 種類のログ解析ツールを試験的に導入した。この他にも多くのツールが存在するので，用途や使い勝手に応じて選択したい。それぞれ一長一短あるので，欠点を補い合うため複数のツールを使用することも有効である。

今後は従来の syslog サーバである syslogd から，機能拡張やセキュリティが考慮された syslog-ng を導入し，各種サーバ等のログを安全に一元管理し，運用管理に役立てたい。

## 5. 参考文献等


1. AWStats official web site
   http://awstats.sourceforge.net/
2. AWStats 6.5 完全日本語化のページ
3. 「徹底解説！Postfix のログ解析」Software Design 2006 年 8 月号
4. JIMSUN Postfix Contrib
   http://jimsun.linxnet.com/postfix_contrib.html/