educhan 上で bsfilter を使用する方法

教育学研究科 コンピュータ運営委員会

本ドキュメントは、bsfilter を educhan 上で使う方法について書かれています。UNIX に関する知識、telnet、ssh、ftp 等に関する知識が必要です。bsfilter の公式ホームページは、
http://bsfilter.org/
です。まずは上記サイトの内容を読んでください。

1. "educhan.p.u-tokyo.ac.jp"へ telnet、ssh 等でログインします(ssh 推奨)。

2. "/usr/bin/bsfilter"、"/usr/bin/procmail"にパスが通っていることを確認します。パスが通っていれば、"bsfilter --help"と入力すると、オプションの一覧を見ることができます。

3. 通常の(=spam でない)メール(以下、"clean"と表記)を学習させます。
clean なメールを「mbox 形式」で用意できる場合、ファイル名を"your_clean_mbox"等として保存し、

```
bsfilter -c --mbox your_clean_mbox
```

を実行します。
「1 メール 1 ファイル」の形式でファイルを用意できる場合は、~/Mail/inbox/等に保存した上で

```
bsfilter -c ~/Mail/inbox/*
```

4. 同様の操作により、spam を学習させます

```
bsfilter -s --mbox your_spam_mbox
```
(mbox 形式の場合)

あるいは

```
bsfilter -s  ~/Mail/spam/*
```
(1 メール 1 ファイル形式の場合)

5. 単語ごとに clean/spam な確率を求め、データベースを更新します

bsfilter -u

6. ".procmailrc"という名前のファイルをホームディレクトリに作成します。以下に例を示します(以下の例にある| /usr/bin/bsfilter から--insert-probability までは 1 行で書いてください。途中に改行を入れると正常に動作しません)。

--".procmailrc"ここから----------

```
MAILDIR=$HOME/Mail/
SENDMAIL=/opt/postfix/sendmail
LOGFILE=$MAILDIR/procmail.log
LOCKFILE=$MAILDIR/.lockmail
DEFAULT=/var/mail/yamamoto

# bsfilter preprocess, cutoff level of 0.4 seems to work fine (initially)
:0 fw
| /usr/bin/bsfilter -a --pipe --insert-flag --spam-cutoff 0.4
--insert-probability

# bsfilter
:0
* ^X-Spam-Flag: Yes
probably.spam

# clean mail, transfer to the mailbox
:0
$DEFAULT
```

--".procmailrc"ここまで----------

(注)

・MAILDIR の指定先はホームディレクトリの中であればどこでも構いませんが、事前に作成する必要があります。もし上記の.procmailrc をそのまま使用する場合は"mkdir $HOME/Mail"を実行しておきます。

・DEFAULT の指定先は educhan のアカウント名(=メールアドレスの「@」以前)に変更する必要があります。

・フィルタの動作に大きく影響を与えるのは"--spam-cutoff"で指定する値です。例えば、"--spam-cutoff 0.4"は、「"spam probability"の値が 0.4 を超えたら spam と判定する」ことを意味します。4000 通の clean なメール、400 通の spam を学習させた結果では、新たに到着するクリーンなメールに関しては、"spam probability"の値は適切な値(0.0 に近い値)が得られます。既に学習された spam と同一内容、あるいは「ほとんど」同一内容の spam の受信時は、"spam probability"の値は 1.0 に近くなり、新たな(=bsfilter のデータベース上に類似する spam が存在しない)spam に関しては 0.5 近辺の値になるようです。したがって、"--spam-cutoff"の値を 0.4 に設定すれば、ほぼ完璧なフィルタリングができるようになります。ここ数日に届いた 500 通以上のメールのうち、spam が clean と誤判定されたメールが 1 通、clean が spam と誤判定されたメールが 1 通という結果が出ています。
しかしながら、bsfilter への初期の学習結果によっては異なる結果になる可能性があります。特に、clean なメールが spam と誤判定されると、重要なメールを見逃す可能性が生じ、時に深刻な影響を及ぼすため、最初のうちは--spam-cutoff の値を大きめ(0.6 等)にすることも検討してください。いずれにしても、フィルタが学習していくにつれて、判定率は高くなっていきます。学習については後述します。

7. "$HOME/.forward"ファイルを以下のような内容で作成します(ダブルクオーテーションを含めて入力してください)。

--".forward"ここから----------
```
"|IFS=' ' && exec /usr/bin/procmail -f- || exit 75 #yamamoto"
```
--".forward"ここまで----------

a) ".forward"内の"yamamoto"は各ユーザのアカウント名に書き換える必要があります。

b) このファイルを作成すると同時に bsfilter が動作を開始します。

c) メールが educhan に到着する毎に、"$MAILDIR/procmail.log"に以下のようなログが作成(すでにこのファイルが存在していれば追記)されます。

--"procmail.log"の例ここから----------
```
>From Natelson@njneuromed.org  Tue Aug  8 06:57:48 2006
 Subject:
```

```
  Folder: /var/mail/yamamoto
3014
>From remediosogumbs@appliedhealth.com  Tue Aug  8 09:17:51 2006
 Subject: Re: fouuiVIsAGRA
  Folder: probably.spam
2963
```

--"procmail.log"の例ここまで----------

最初のものは clean と判定されたメールであり、メールボックスに送られたものです。次は spam と判定され、"probably.spam" というファイルに保存されています。既に "probably.spam"というファイルが存在する場合は追記されます。

8. clean と判定されたメールは次のような内容です

--clean の例ここから----------

```
>From Natelson@njneuromed.org  Tue Aug  8 06:57:48 2006
X-UIDL: X)#"!8O+"!oM[!!RPh!!
X-Original-To: yamamoto@p.u-tokyo.ac.jp
Delivered-To: yamamoto@p.u-tokyo.ac.jp
X-MimeOLE: Produced By Microsoft Exchange V6.5.7226.0
Content-class: urn:content-classes:message
MIME-Version: 1.0
Subject:
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
thread-index: Aca6bK9p2UKuMS0RQ6665r546yL0hQ==
To: <yamamoto@p.u-tokyo.ac.jp>
X-Spam-Flag: No
X-Spam-Probability: 0.000000

This is a multi-part message in MIME format.

------_=_NextPart_001_01C6BA6C.B133B7E7
Content-Type: text/plain;
       charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
```

Hi Yoshi:
(中略)

Best,

b

Benjamin H. Natelson, MD
Professor of Neurosciences
    UMDNJ-New Jersey Medical School
(後略)
--clean の例ここまで----------

a) ヘッダ部分にある、"X-Spam-Flag"と"X-Spam-Probability"により、このメールが clean と判定されたことがわかります。

b) 上述した".procmailrc"内の bsfilter のオプションに"-a"が指定してあるため、spam 判定データベースはメールを読み込むごとに自動的に学習していきます。従って、判定ミスがあったときには早めにデータベースの更新作業を行わないと、判定ミスがどんどん増えてしまいます。

c) もし spam を clean なメールと誤判定してしまった場合(これを"false negative"といいます)、以下の手順で bsfilter のデータベースを更新する必要があります。
・当該メールをテキストファイルとして保存し(ここではファイル名を"your_tn"とします)
・"bsfilter -C -s -u your_tn"を実行
この操作により、データベースが更新されます。

9. spam として判定されたメールは次のような内容です。(mailx -f probably.spam により得たもの)

--spam の例ここから----------
>From remediosogumbs@appliedhealth.com Tue Aug 8 09:17:51 2006
X-Original-To: yamamoto@p.u-tokyo.ac.jp
Delivered-To: yamamoto@p.u-tokyo.ac.jp
To: yamamoto@p.u-tokyo.ac.jp

```
Subject: Re: fouuiVIsAGRA
MIME-Version: 1.0
X-Priority: 3
X-MSMail-Priority: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1106
X-Spam-Flag: Yes
X-Spam-Probability: 0.500480

This is a multi-part message in MIME format.

------=_NextPart_000_0001_01C6BA45.50E59210
Content-Type: text/plain;
       charset="us-ascii"
Content-Transfer-Encoding: quoted-printable

Hi,

CIsALIS from 3, 75 $
VIsAGRA from 3, 35 $
AMsBIEN
VAsLIUM from 1, 25 $

http://www.uthunamde.com
[後略]
```
--spam の例ここまで----------

a) ヘッダ部分にある、"X-Spam-Flag"と"X-Spam-Probability"により、このメールが spam と判定されたことがわかります。

b) もし clean なメールが spam と誤判定されてしまった場合(これを"false positive"といいます)、以下の手順で bsfilter のデータベースを更新する必要があります。
・当該メールをテキストファイルとして保存し(ここではファイル名を"your_fp"とします)
・"bsfilter -c -S -u your_fp"を実行
この操作により、データベースが更新されます。

spam 判定データベースはメールを読み込むごとに自動的に学習していきます。一度 spam

と判定されたメール(の中の単語)は、データベースに spam 確率が高いものとして登録されるので、次回同じ単語を多く含むメールが来ると、より高い確率で spam らしいと判断されるようになります。逆も同じです。誤判定があった場合は手順 8、9 により手動でデータベースを更新します。これらの繰り返しにより、bsfilter の判定精度が上がっていきます。

10. 以上の手順で、bsfilter は正常に動作します。ただし、"procmail.log"や"plobably.spam"ファイルはメールが届くたびに書き足されるため、そのままではどんどんファイルが大きくなってしまいます。定期的にファイルを削除してもいいのですが、以下のようなシェルスクリプト"report_rotate.sh"を$MAILDIR内に作成すると自動的にファイルを削除することができます。

--"report_rotate.sh"ここから----------

```
#! /bin/sh
#
# First report current log
#
LOGDIR=$HOME/Mail
LOG=spamlog
if [ -d $LOGDIR ]; then
  cd $LOGDIR
  LOG0=procmail.log
  if [ -f $LOG0 ]; then
    cp /dev/null $LOG
    chmod 600 $LOG
    echo "Subject: Procmail report" > $LOG
    echo "Content-Type: text/plain;" >> $LOG
    echo >> $LOG
    cat $LOG0 >> $LOG
    /usr/local/bin/nkf    -m    $LOG    |    /opt/postfix/sendmail
yamamoto@p.u-tokyo.ac.jp
  fi
fi
#
# Then rotate procmail.log
#
LOGDIR=$HOME/Mail
```

```
LOG=procmail.log
if test -d $LOGDIR
then
   cd $LOGDIR
   if test -s $LOG
   then
      test -f $LOG.6 && mv $LOG.6  $LOG.7
      test -f $LOG.5 && mv $LOG.5  $LOG.6
      test -f $LOG.4 && mv $LOG.4  $LOG.5
      test -f $LOG.3 && mv $LOG.3  $LOG.4
      test -f $LOG.2 && mv $LOG.2  $LOG.3
      test -f $LOG.1 && mv $LOG.1  $LOG.2
      test -f $LOG.0 && mv $LOG.0  $LOG.1
      mv $LOG   $LOG.0
      cp /dev/null $LOG
      chmod 644    $LOG
      sleep 40
   fi
fi
#
# Then rotate probably.spam
#
LOGDIR=$HOME/Mail
LOG=probably.spam
if test -d $LOGDIR
then
   cd $LOGDIR
   if test -s $LOG
   then
      test -f $LOG.6 && mv $LOG.6  $LOG.7
      test -f $LOG.5 && mv $LOG.5  $LOG.6
      test -f $LOG.4 && mv $LOG.4  $LOG.5
      test -f $LOG.3 && mv $LOG.3  $LOG.4
      test -f $LOG.2 && mv $LOG.2  $LOG.3
      test -f $LOG.1 && mv $LOG.1  $LOG.2
      test -f $LOG.0 && mv $LOG.0  $LOG.1
```

```
      mv $LOG    $LOG.0
      cp /dev/null $LOG
      chmod 644    $LOG
      sleep 40
   fi
fi
```

--"report_rotate.sh"ここまで----------

このようなファイルを作成し、コマンド"crontab -e"により次のような行を挿入します。(crontab の操作はエディタ vi と同じです)

```
   0 4 * * * $HOME/Mail/report_rotate.sh
```

a) 上記のスクリプトは、"procmail.log"を yamamoto@p.u-tokyo.ac.jp 宛に送信するようになっているため、かならずご自分のアドレスに書き換えてください。書き換えずに使った場合、みなさんのメールのログが yamamoto@p.u-tokyo.ac.jp に送信されてしまいます!!

b) 上記のスクリプトでは、spam が格納されたファイルと"procmail.log"は 7 日間保存されます。

c) 最初の「0 4」は、毎日 4 時 0 分にこのスクリプトを動作させることを意味します。多くのユーザーが一斉にスクリプトが起動させると educhan への負荷がかかりますので、最初の「0」は 0〜59 の間で適当な数字を設定することを推奨します。cron の詳しい説明はコマンド"man crontab"で見ることができます。

11. 今までに spam を手動で削除していた場合など、手順 3〜5 で用いる spam が手元にない場合、こちらで作成したデータベースをお送りすることができます。ただし、clean なメールの内容はユーザーによって異なるため、データベースも本来はユーザー固有に持っていることが望ましいです。したがって、可能な限り clean および spam ファイルは自身で用意してください。bsfilter のドキュメントおよびレビューによれば、clean、spam 共に数百通あれば問題なく bsfilter の初期設定が可能のようです。