메일서버등록제(SPF) 인증 기능 적용 안내서

(CentOS - Sendmail)

	OS	Mail Server	SPF 적용 모듈 (C 언어 기반)
작성기준	CentOS 5.4 32bit	sendmail 8.13.8	spfmilter 0.97

2016년 6월

KISA 한국인터넷진흥원

목 차

I. 개요

1. SPF(메일서버 등록제)란?

메일서버등록제(SPF: Sender Policy Framework)는 메일서버 정보를 사전에 DNS에 공개 등록함으로써 수신자로 하여금 이메일에 표시된 발송자 정보가 실제 메일서버의 정보와 일치하는지를 확인할 수 있도록 하는 인증 기술이다.

대다수 스팸발송자가 자신의 신원을 감추기 위하여 발송자 주소나 전송 경로를 허위로 표기하거나 변경하는 경우가 많다는데 착안되었다.

※ SPF를 DNS에 설정하는 방법은 http://www.kisarbl.or.kr > White Domain 등록 > SPF 작성도우미 메뉴를 참고한다.

SPF를 이용하여 스팸메일을 차단하기 위해서는 메일서버에 SPF 인증 기능이 적용되어 있어야 한다.

CentOS 환경에서 기본적으로 설치된 메일서버에는 SPF 인증 기능이 적용되어 있지 않으므로 SPF 모듈 설치 및 패치를 해야 한다. 본 안내서는 메일 수신 서버에 SPF 인증 기능을 쉽게 적용하는 방법을 소개한다.

2. SPF를 이용한 이메일 인증 절차

발신자 : 자신의 메일서버 정보와 정책을 나타내는 SPF 레코드를 해당 DNS에 등록
수신자 : 이메일 수신시 발송자의 DNS에 등록된 SPF 레코드를 확인하여
해당 이메일에 표시된 발송IP와 대조하고 그 결과값에 따라 수신여부를 결정
(메일서버나 스팸차단솔루션에 SPF 인증 기능이 설치되어 있어야 함)

[그림 1] SPF 인증 흐름도

II. sendmail, SPF 인증 모듈 설치

본 안내서는 운영체제 및 메일서버를 처음 구축하는 것을 기준으로 작성하였다. 설치 과정에서 사용하는 모든 명령어는 root 권한으로 실행해야 한다.

1. sendmail 설치 여부 확인

CentOS에는 sendmail이 기본적으로 설치되어 있다. 아래는 telnet 명령어를 이용하여 tcp/25번 포트에 접속하여 메일 전송 프로그램(MTA: Mail Transfer Agent)이 동작하고 있는 상태를 확인하는 것으로써 sendmail이 동작하고 있음을 알 수 있다.

```
[root@spf ~]# telnet 0 25
Trying 0.0.0.0...
Connected to 0 (0.0.0.0).
Escape character is '^]'.
220 spf.kisa.or.kr ESMTP Sendmail 8.13.8/8.13.8; Thu, 1 Jul 2010 21:20:22 +0900
quit
221 2.0.0 spf.kisa.or.kr closing connection
```

2. sendmail-devel 설치

sendmail에는 SPF 인증 기능이 포함되어 있지 않으므로 libspf 라이브러리를 통합하여 구성해야 한다. libspf를 컴파일하기 전에 아래와 같이 패키지 설치/삭제 도구인 yum을 이용하여 'sendmail-devel' 패키지를 설치한다.

```
[root@spf ~]# yum install -y sendmail-devel
Loaded plugins: fastestmirror
.................. (중략)
  Installing       : sendmail-devel                                      1/1
Installed:
  sendmail-devel.i386 0:8.13.8-8.el5
```

3. gcc 설치

3.1 gcc 설치 여부 확인

추가적으로 libspf2, spfmilter 라이브러리를 설치하기 위해서 소스코드를 컴파일 해야 한다. 아래와 같이 gcc 설치 여부를 확인한다.

※ libspf2, spfmilter는 sendmail에서 제공하는 기본적인 '메일 필터 플러그인 채널(milter)'을 통해서 SPF 인증 기능을 수행하는 라이브러리이다.

```
[root@spf ~]# gcc --version
gcc (GCC) 4.1.2 20080704 (Red Hat 4.1.2-48)
Copyright (C) 2006 Free Software Foundation, Inc.
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
```

3.2 설치

gcc가 설치되어 있지 않다면 아래와 같이 yum을 이용하여 설치한다.

```
[root@spf ~]# yum install -y gcc
Loading mirror speeds from cached hostfile
 * addons: mirror.khlug.org
 * base: mirror.khlug.org
.................. (중략)
Running Transaction
  Installing                                                  :                  gcc
          1/1
Installed:
  gcc.i386 0:4.1.2-48.el5
```

4. libspf2 설치

'libspf2'는 spfmilter를 이용하여 SPF 인증 기능을 적용하기 위한 필수 라이브러리이다.

4.1 다운로드 및 압축 해제

아래와 같이 wget 명령어를 이용하여 'libspf2-1.0.4' 라이브러리를 다운로드 한 후 압축을 해제한다.

```
[root@spf ~]# wget http://www.libspf2.org/spf/libspf2-1.0.4.tar.gz
http://www.libspf2.org/spf/libspf2-1.0.4.tar.gz
.................. (중략)
`libspf2-1.2.5.tar.gz' saved [517945/517945]
[root@spf ~]# tar xzf libspf2-1.0.4.tar.gz
```

4.2 설치

아래와 같이 libspf2를 설치한다.

```
[root@spf ~]# cd libspf2-1.0.4
[root@spf libspf2-1.0.4]# ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
.................. (중략)
config.status: executing depfiles commands
[root@spf libspf2-1.0.4]# make && make install
make  all-recursive
.................. (중략)
```

※ '/usr/local/bin' 디렉토리에 프로그램이 설치된다.

5. spfmilter 설치

spfmilter는 sendmail 기반에서 사용되는 오픈소스 기반의 'mail filter' 프로그램이다.

5.1 다운로드 및 압축 해제

아래와 같이 'spfmilter-0.97'을 다운로드 한 후 압축을 해제한다.

```
[root@spf ~]# wget http://www.acme.com/software/spfmilter/spfmilter-0.97.tar.gz
Resolving www.acme.com...
.................. (중략)
`spfmilter-0.97' saved [56280/56280]
[root@spf ~]# tar xzf spfmilter-0.97.tar.gz
```

5.2 설치

아래와 같이 spfmilter를 설치한다.

```
[root@spf ~]# cd spfmilter-0.97
[root@spf spfmilter-0.97]# ./configure
checking for gcc... gcc
checking for C compiler default output... a.out
.................. (중략)
configure: creating ./config.status
config.status: creating Makefile
[root@spf spfmilter-0.97]# make && make install
make[1]: Entering directory `/root/spfmilter-1.0.8'
/bin/sh ./mkinstalldirs /usr/local/sbin
  /usr/bin/install -c spfmilter /usr/local/sbin/spfmilter
/bin/sh ./mkinstalldirs /usr/local/man/man8
 /usr/bin/install -c -m 644 ./spfmilter.8 /usr/local/man/man8/spfmilter.8
make[1]: Leaving directory `/root/spfmilter-1.0.8'
```

※ '/usr/local/bin' 디렉토리에 프로그램이 설치된다.

6. spfmilter 연동

6.1 MILTER 설치 여부 확인

sendmail과 spfmilter를 연동하기 위해서는 MILTER가 설치되어 있어야 한다. 아래와 같이 MILTER의 설치 여부를 확인한다.

```
[root@spf ~]# sendmail -d0.1 -bt < /dev/null | grep MILTER
 MATCHGECOS MILTER MIME7TO8 MIME8TO7 NAMED_BIND NETINET NETINET6
```

6.2 sendmail.cf 설정 변경

sendmail과 spfmilter의 연동을 위해서 아래와 같이 sendmail의 설정 파일인 sendmail.cf의 마지막 라인에 설정을 추가한다.

```
[root@spf ~]# cd /etc/mail
[root@spf mail]# vi sendmail.cf
.................. (중략)
dnl MAILER(cyrusv2)dnl
INPUT_MAIL_FILTER(`spfmilter',`S=unix:/var/run/spfmilter.sock, T=S:4m;R:4m')
[root@spf mail]# m4 < sendmail.mc > sendmail.cf
```

6.3 spfmilter 실행 및 sendmail 재시작

spfmilter가 sendmail보다 먼저 실행되어야 정상적으로 동작하므로 아래와 같이 순서에 맞게 데몬을 구동한다.

```
[root@spf ~]# /usr/local/sbin/spfmilter unix:/var/run/spfmilter.sock -d
[root@spf ~]# serivce sendmail restart
```

※ 주의) spfmilter 실행시 'spfmilter: error while loading shared libraries: libspf2.so.1: cannot open shared object file: No such file or directory' 과 같은 에러가 발생하게 될 경우 아래와 같이 환경변수를 설정한다.

```
[root@spf ~]# export LD_LIBRARY_PATH=/usr/local/lib
```

III. SPF 적용 여부 및 차단 확인

SPF 인증 결과, 메일 발송 IP와 SPF 레코드에 지정된 IP의 일치 여부에 따라서 'SPF pass'와 'SPF fail/softfail'로 구분된다. 확인 방법은 다음과 같다.

1. SPF pass인 경우

아래와 같이 '/var/log/syslog' 파일에서 SPF 인증이 통과(pass)된 로그의 내용을 확인할 수 있다. 해당 메일은 정상적으로 수신되었다.

```
Jul 19 17:28:50 spf sendmail[5447]: o6L8SoeM005447: Milter add: header: Received-SPF: pass (kisarbl.or.kr: domain of test.com designates x.x.x.x as permitted sender) receiver=kisarbl.or.kr; client-ip=x.x.x.x; helo=example.com; envelope-from=xxx@kisarbl.or.kr; x-software=spfmilter 0.93 http://www.acme.com/software/spfmilter/;
```

2. SPF fail/softfail인 경우

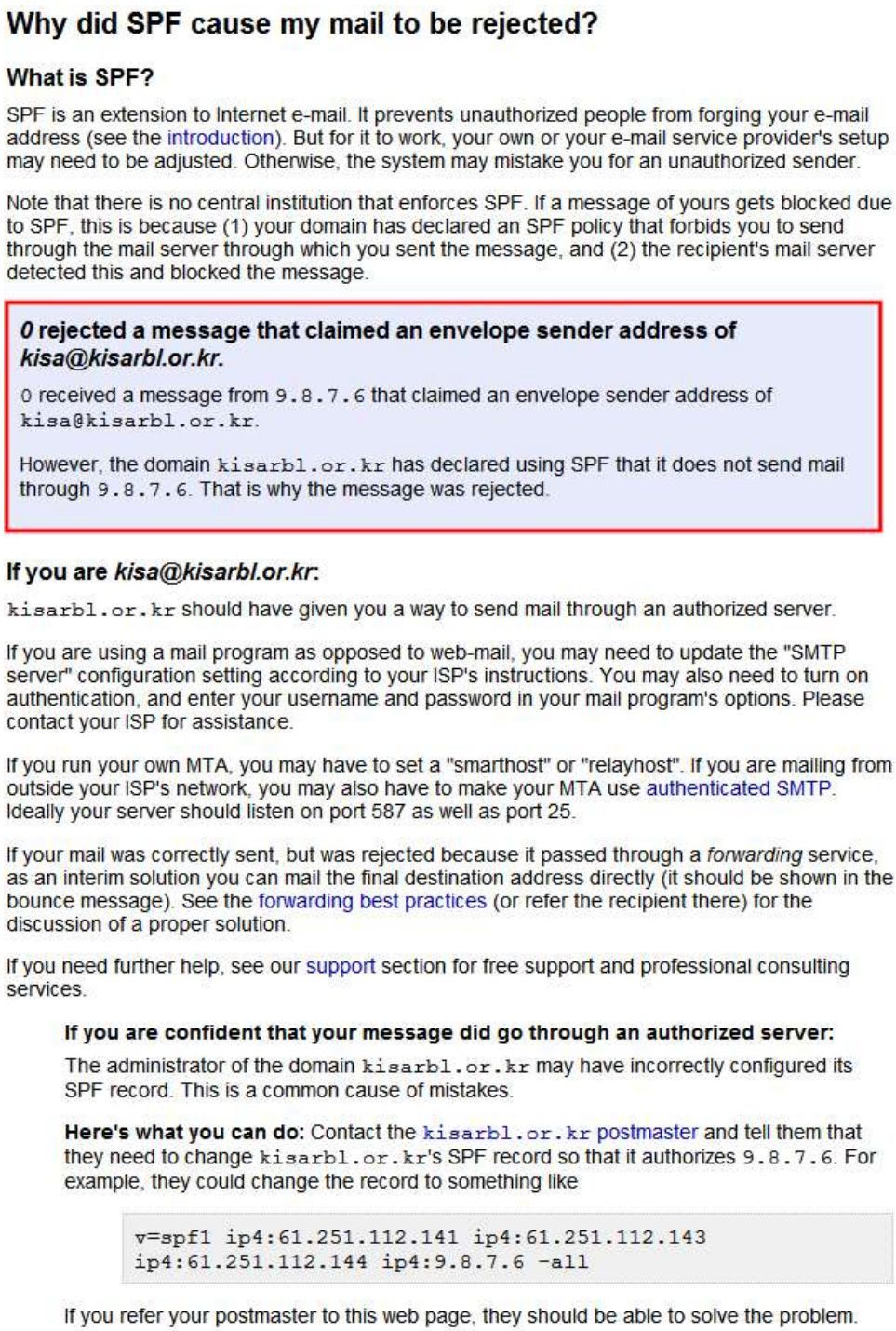
아래는 telnet 명령어를 이용하여 SPF 인증 기능이 적용된 메일서버로 접속하여 메일 발송을 테스트하는 과정이다. 메일 발송 IP와 SPF 레코드의 IP가 일치하지 않기 때문에 메일 수신 주소를 입력하는 단계에서 차단된 것을 확인할 수 있다.

표시된 URL에서는 SPF 인증이 실패(fail/softfail)하여 거부된 상세 사유를 확인할 수 있다.

```
[root@ ~]# telnet 메일서버IP 25 (공인 IP만 가능하며, 127.0.0.1은 확인불가)
Connected to your (1.2.3.4).
Escape character is '^]'.
220 mail.yourdomian.com ESMTP Sendmail 8.13.8; Wed, 28 Jul 2010 15:56:42 +0900
ehlo test.com
250 mail.yourdomian.com Hello example.com [1.2.3.5], pleased to meet you
mail from: test@kisarbl.or.kr (메일 발신 주소)
250 ok
rcpt to: test@yourdomain.com (메일 수신 주소)
550 5.7.1 test@kisarbl.or.kr...
Please see http://spf.pobox.com/why.html?sender=test@kisarbl.or.kr&ip=
9.8.7.6&receiver=spf.kisa.or.kr (차단되었음을 확인할 수 있음)
quit (접속종료)
```

2.1 reject 사유 페이지 확인

'http://spf.pobox.com/why.html?sender=kisa%40kisarbl.or.kr&ip=x.x.x.x&receiver=0' 페이지에서 거부(reject) 사유와 해결 방법을 확인할 수 있다.



Why did SPF cause my mail to be rejected?

What is SPF?

SPF is an extension to Internet e-mail. It prevents unauthorized people from forging your e-mail address (see the introduction). But for it to work, your own or your e-mail service provider's setup may need to be adjusted. Otherwise, the system may mistake you for an unauthorized sender.

Note that there is no central institution that enforces SPF. If a message of yours gets blocked due to SPF, this is because (1) your domain has declared an SPF policy that forbids you to send through the mail server through which you sent the message, and (2) the recipient's mail server detected this and blocked the message.

***0* rejected a message that claimed an envelope sender address of *kisa@kisarbl.or.kr*.**

0 received a message from 9.8.7.6 that claimed an envelope sender address of kisa@kisarbl.or.kr.

However, the domain kisarbl.or.kr has declared using SPF that it does not send mail through 9.8.7.6. That is why the message was rejected.

If you are *kisa@kisarbl.or.kr*:

kisarbl.or.kr should have given you a way to send mail through an authorized server.

If you are using a mail program as opposed to web-mail, you may need to update the "SMTP server" configuration setting according to your ISP's instructions. You may also need to turn on authentication, and enter your username and password in your mail program's options. Please contact your ISP for assistance.

If you run your own MTA, you may have to set a "smarthost" or "relayhost". If you are mailing from outside your ISP's network, you may also have to make your MTA use authenticated SMTP. Ideally your server should listen on port 587 as well as port 25.

If your mail was correctly sent, but was rejected because it passed through a *forwarding* service, as an interim solution you can mail the final destination address directly (it should be shown in the bounce message). See the forwarding best practices (or refer the recipient there) for the discussion of a proper solution.

If you need further help, see our support section for free support and professional consulting services.

If you are confident that your message did go through an authorized server:

The administrator of the domain kisarbl.or.kr may have incorrectly configured its SPF record. This is a common cause of mistakes.

Here's what you can do: Contact the kisarbl.or.kr postmaster and tell them that they need to change kisarbl.or.kr's SPF record so that it authorizes 9.8.7.6. For example, they could change the record to something like

```
v=spf1 ip4:61.251.112.141 ip4:61.251.112.143
ip4:61.251.112.144 ip4:9.8.7.6 -all
```

If you refer your postmaster to this web page, they should be able to solve the problem.

[그림 2] SPF fail/softfail 시 차단 확인 페이지

3. procmail을 이용한 스팸 차단 방법

3.1 procmail이란?

유닉스 계열에서는 메일을 수신한 후 메일 박스에 전달할 때 마지막 처리를 담당하는 MDA(Mail Delivery Agent) 프로그램으로서 procmail이 가장 널리 사용되고 있다.

procmail을 spfmilter와 연동하여 'SPF fail/softfail' 발생 시 메일을 차단하는 대신에 메일의 제목에 [SPAM] 태그를 추가하여 스팸 분류를 하도록 한다.

메일 사용자들이 '아웃룩 익스프레스' 등의 메일 클라이언트(MUA)를 이용하여 스팸으로 자동 분류를 할 수 있게 된다.

3.2 procmail 설치

아래와 같이 rpm 명령어를 이용하여 procmail의 설치 여부를 확인한 후 설치되어 있지 않으면 yum을 이용하여 설치한다.

```
[root@spf log]# rpm -qa | grep procmail
procmail-3.22-17.1.el5.centos
[root@spf log]# yum install -y porcmail
```

3.3 sendmail.cf 설정 확인

sendmail의 설정 파일인 sendmail.cf에 아래와 같은 설정이 존재하는지 확인한다.

```
[root@spf log]# vi /etc/mail/senmail.cf
Mprocmail, P=/usr/bin/procmail, F=DFMSPhnu9, S=EnvFromSMTP/HdrFromSMTP,
R=EnvToSMTP/HdrFromSMTP, T=DNS/RFC822/X-Unix,      A=procmail -Y -m $h $f $u
```

3.4 procmail 룰셋 작성

메일의 제목에 [SPAM] 태그를 추가하기 위한 룰셋을 아래와 같이 '/etc/mail/procmailrc' 파일에 작성한다.

※ '/etc/mail/procmailrc'는 모든 사용자에게 적용되는 필터를 정의할 때 사용하며,
만약 특정 사용자만 적용하려면,
해당 사용자의 '~/.procmailrc' 파일에 아래의 설정을 추가한다.

```
[root@spf log]# vi /etc/mail/procmailrc
LOGFILE=/var/log/procmail
VERBOSE=no
PATH=/usr/bin:/usr/local/bin:/bin
SHELL=/bin/sh
SPAM_SPF_LOG = "/var/log/SPAM_SPF.log"
:0 :
* ^Received-SPF: ₩/(fail|softfail)
{
        STAT = "$MATCH"
        # From
        :0
        * ^From: ₩/.*
        {
                FROM = "$MATCH"
        }
        # Subject
        :0
        * ^Subject: ₩/.*
        {
                SUBJECT = "$MATCH"
        }
        LOG="=====SPF_filter($STAT) F=$FROM, S=$SUBJECT"
        :0fwh
        * ^Subject: ₩/.*
        | formail -I "Subject: [SPAM] $SUBJECT"
        | $SPAM_SPF_LOG
}
```

3.5 스팸 차단 확인

다음과 같이 '/var/log/procmail' 파일에서 procmail의 로그를 확인할 수 있다. SPF 인증 결과가 'fail/softfail'인 경우에 해당 메일 제목에 [SPAM] 태그가 추가되었으며 사용자의 메일 박스(/var/mail/kisa)에 저장되었다.

```
[root@spf log]# cat /var/log/procmail
procmail: Extraneous lockfile ignored
=====SPF_filter(softfail)          F="TESTER"          <webmaster@kisarbl.co.kr>,
S==?ks_c_5601-1987?B?xde9usaulF8gc3BmlHNvZnQgZmFpbLfOlMDOx9EgU1BBTS
DFwg==?=          =?ks_c_5601-1987?B?sdfD37Ch?=
procmail: Skipped "| $SPAM_SPF_LOG"

From webmaster@kisarbl.or.kr  Wed Jul 21 18:24:46 2010
 Subject: [SPAM] =?ks_c_5601-1987?B?xde9usaulF8gc3BmlHNvZnQgZmFpbLfOlMDOx9EgU1B
  Folder: /var/mail/kisa                                          2295

procmail: Extraneous lockfile ignored
procmail: Skipped "| $SPAM_SPF_LOG"
From webmaster@kisarbl.or.kr  Wed Jul 21 18:25:49 2010
 Subject: 테스트 SPF pass인 경우
  Folder: /var/mail/kisa                                           766
```