메일서버등록제(SPF) 인증 기능 적용 안내서

(SunOS - postfix)

	OS	Mail Server	SPF 적용 모듈 (Perl 기반)
작성기준	SunOS 5.10 32bit	Postfix 2.4.6	postfix-policyd-spf-perl 2.007

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.

SunOS 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. postfix, SPF 인증 모듈 설치

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

1. postfix 설치

SunOS에는 sendmail이 기본적으로 설치되어 있다. postfix를 설치하면 tcp/25번 포트 충돌이 발생하므로 제거하도록 한다.

아래와 같이 svcadm 명령어를 이용하여 sendmail 서비스를 종료하고 패키지 관리 도구인 pkgrm을 이용하여 sendmail을 삭제한다.

```
bash-3.00# svcadm disable sendmail (sendmail 서비스 종료)
bash-3.00# pkgrm SUNWsndmu (sendmail 패키지 삭제)
bash-3.00# pkgrm SUNWsndmr (sendmail 패키지 삭제)
```

1.1 pkg-get 설치

아래와 같이 pkgadd를 이용하여 pkg-get을 설치한다.

```
bash-3.00# pkgadd -d http://www.opencsw.org/pkg_get.pkg
..............(중략)
all packages). (default: all) [?,??,q]:  (엔터)
..............(중략)
이 디렉토리를 지금 만들겠습니까? [y,n,?,q] y
..............(중략)
## setuid/setgid 프로그램 점검
<CSWpkgget>(을)를 계속 설치하겠습니까 [y,n,?] y
..............(중략)
<CSWpkgget>(이)가 성공적으로 설치되었습니다
```

1.2 다운로드 및 설치

아래와 같이 pkg-get을 이용하여 postfix를 설치한다.

※ -i 옵션은 다운로드와 동시에 설치하는 옵션이다.

```
bash-3.00# pkg-get -i postfix
No existing install of CSWpostfix found. Installing...
http://mirrors.ibiblio.org/pub/mirrors/opencsw/current/i386/5.10/postfix-2.4.6,REV=
2008.05.28-SunOS5.8-i386-CSW.pkg.gz [following]
.............(중략)
HTTP request sent, awaiting response... 200 OK
Length: 9846280 (9.4M) [application/x-gzip]
Saving to: `postfix-2.4.6,REV=2008.05.28-SunOS5.8-i386-CSW.pkg.gz'
.............(중략)
Linking /usr/lib/sendmail to /opt/csw/sbin/postfix
Linking /usr/bin/newaliases to /opt/csw/bin/newaliases
Linking /usr/bin/mailq to /opt/csw/bin/mailq
.............(중략)
Installation of <CSWpostfix> was successful.
```

2. pm_mailspf 모듈 설치

postfix에서 SPF 인증 기능을 적용할 수 있는 라이브러리로는 perl 스크립트로 작성된 'postfix-policyd-spf-perl'이 있다.

이 모듈을 사용하기 위해서는 'Mail::SPF' perl 모듈이 설치되어 있어야 한다.

해당 모듈은 'pm_mailspf' 패키지에 포함되어 있으므로 아래와 같이 패키지 관리 도구인 pkg-get을 이용하여 설치한다.

```
bash-3.00# pkg-get -i pm_mailspf
No existing install of CSWperl found. Installing...
Removing invalid local file
perl-5.10.1,REV=2009.12.15-SunOS5.8-i386-CSW.pkg.gz
..............(중략)
/opt/csw/share/perl/csw/Mail/SPF/v2/Record.pm
[ verifying class <none> ]
Installation of <CSWpmmailspf> was successful.
```

3. postfix-policyd-spf-perl 설치 및 연동

3.1 다운로드 및 압축 해제

아래와 같이 wget 명령어를 이용하여 'postfix-policyd-spf-perl'을 다운로드 한 후 압축을 해제한다.

```
bash-3.00#  wget \
http://launchpad.net/postfix-policyd-spf-perl/trunk/2.007/download/postfix-policyd-spf-perl-2.007.tar.gz
bash-3.00# gunzip postfix-policyd-spf-perl-2.007.tar.gz
bash-3.00# tar xf postfix-policyd-spf-perl-2.007.tar
```

3.2 policyd-spf-perl 모듈 설치

아래와 같이 'postfix-policyd-spf-perl' 스크립트를 '/usr/local/lib' 디렉토리에 복사한다.

```
bash-3.00# cd postfix-policyd-spf-perl-2.007
bash-3.00# cp postfix-policyd-spf-perl-2.007 /usr/local/lib/policyd-spf-perl
```

3.3 master.cf 설정 변경

postfix를 구동할 때 사용되는 master 프로세스의 설정 파일인 master.cf 파일의 마지막 라인에 아래와 같이 추가한다.

```
bash-3.00# vi /etc/postfix/master.cf
..............(중략)
policy unix - n n - 0 spawn (엔터)
(한 칸 공백)user=nobody argv=/usr/sbin/postfix-policyd-spf-perl
```

※ 주의) 'user=nobody'로 시작하는 라인의 첫 한 칸을 공백으로 둔다.

3.4 main.cf 설정 변경

postfix의 설정 파일인 main.cf의 마지막 라인에 아래와 같은 설정을 추가하고 postfix 서비스를 재시작 한다.

```
bash-3.00# vi /etc/opt/csw/postfix/main.cf
 ..................(중략)
smtpd_recipient_restrictions =
          reject_unauth_destination
          check_policy_service inet:127.0.0.1:9998
bash-3.00# svcadm restart cswpostfix
```

III. SPF 적용 여부 확인 및 차단

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.

```
bash-3.00# cat /var/log/syslog | grep pass
Jul 15 15:09:22 spf postfix/policy-spf[4463]: q1234: Policy action=PREPEND
Received-SPF: pass (kisarbl.or.kr: x.x.x.x is ..... (중략)
helo=test.com; client-ip=x.x.x.x
```

2. SPF fail/softfail인 경우

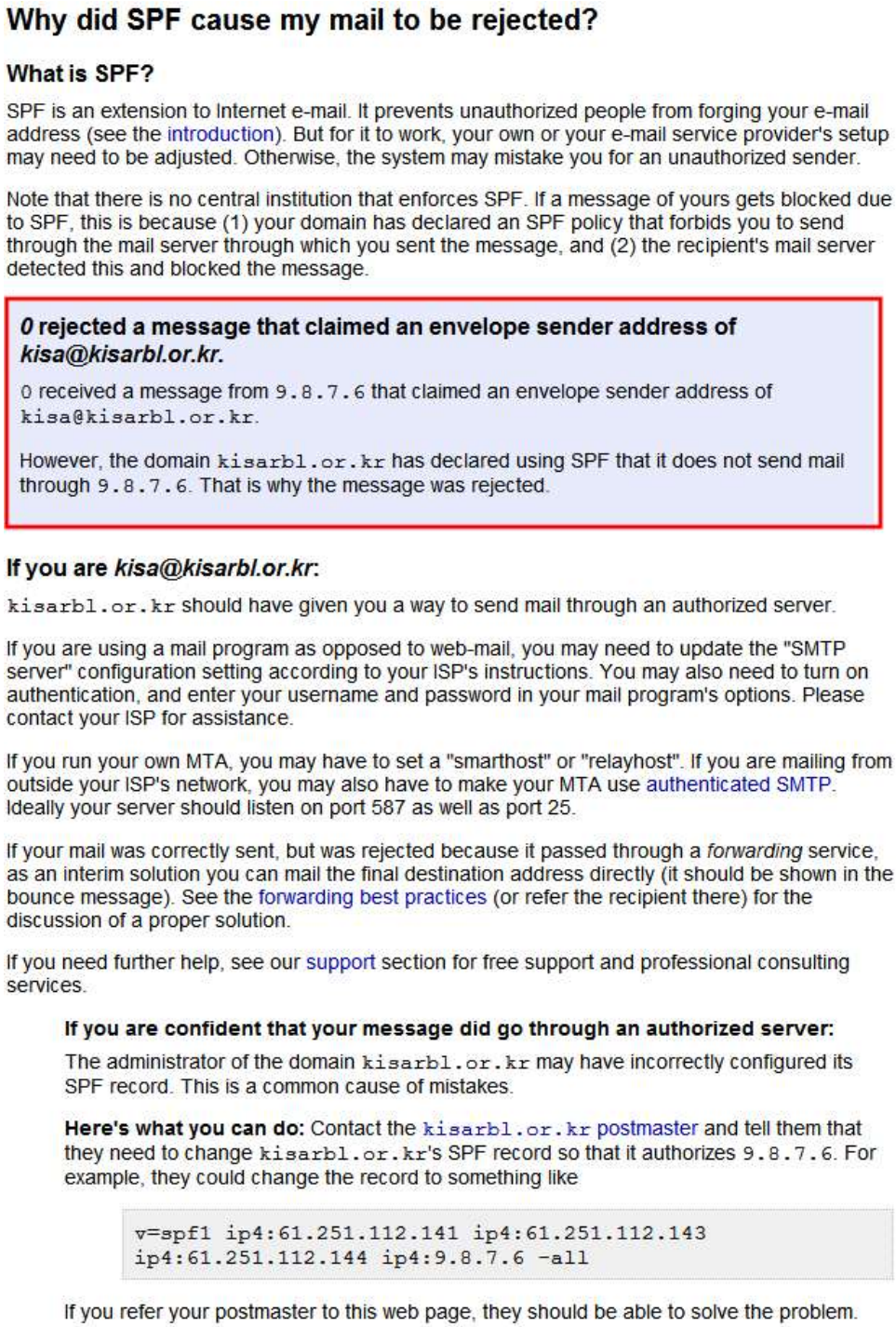
아래는 telnet 명령어를 이용하여 SPF 인증 기능이 적용된 메일서버로 접속하여 메일 발송을 테스트하는 과정이다. 메일 발송 IP와 SPF 레코드의 IP가 일치하지 않기 때문에 메일 수신 주소를 입력하는 단계에서 차단된 것을 확인할 수 있다.

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

```
bash-3.00# telnet mail.yourdomain.com 25
Connected to your (1.2.3.4).
220 mail.yourdomain.com ESMTP Postfix
ehlo kisarbl.or.kr
250 mail.yourdomian.com Hello mail.funix.net [1.2.3.5], pleased to meet you
mail from: test@kisarbl.or.kr
250 2.1.0 Ok
rcpt to: root@kisarbl.or.kr
550 5.7.1 <root@kisarbl.or.kr>: Recipient address rejected: Please see
http://www.openspf.org/Why?s=mfrom;id=test@%
40kisarbl.or.kr;ip=9.8.7.6
```

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 wget 명령어를 이용하여 procmail을 다운로드한다.
파일 압축 해제 후 패키지 관리 도구인 pkgadd를 이용하여 설치한다.

```
bash-3.00# wget \
ftp://ftp.sunfreeware.com/pub/freeware/intel/10/procmail-3.22-sol10-x86-local.gz
bash-3.00# gunzip procmail-3.22-sol10-x86-local.gz
bash-3.00# pkgadd -d `pwd`/procmail-3.22-sol10-x86-local
```

3.3 main.cf 설정 변경

postfix의 설정 파일인 main.cf에 아래와 같은 설정을 추가하고 postfix 서비스를 재시작 한다.

```
bash-3.00# vi /etc/opt/csw/postfix/main.cf
#mailbox_command = /some/where/procmail -a "$EXTENSION"
mailbox_command = /usr/local/bin/procmail -a "$EXTENSION"
# The mailbox_transport specifies the optional transport in master.cf
bash-3.00# /etc/init.d/postfix restart
```

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.

```
bash-3.00# 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.

```
bash-3.00# 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
```