메일서버등록제(SPF) 인증 기능 적용 안내서

(AIX - sendmail)

	OS	Mail Server	SPF 적용 모듈 (Perl 기반)
작성기준	AIX 5.3	sendmail 8.13.4	spf-filter 1.0

2016년 6월

KISA 한국인터넷진흥원

목 차

Ⅰ. 개요 ····· 1

1. SPF(메일서버 등록제)란? ····· 1
2. SPF를 이용한 이메일 인증 절차 ····· 1

Ⅱ. sendmail, SPF 인증 모듈 설치 ····· 2

1. sendmail 확인 ····· 2
2. procmail을 이용한 스팸 차단 방법 ····· 2
3. spf-filter 다운로드 및 설치 ····· 4
4. 룰셋 설정 ····· 4

Ⅲ. SPF 인증 결과 로그 확인 ····· 5

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.

AIX 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 확인

Aix에는 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.

```
bash-4.00# telnet localhost 25
220 spf.kisa.or.kr ESMTP Sendmail Thu, 22 Jul 2010 13:52:49 +0900
quit
221 2.0.0 spf.kisa.or.kr closing connection
```

2. procmail을 이용한 스팸 차단 방법

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

procmail을 spf-filter와 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.

2.1 procmail 다운로드

아래와 같이 wget 명령어를 이용하여 procmail의 바이너리 파일을 다운로드 한다.

※ 'http://bio.gsi.de/DOCS/AIX/aixpdslib.seas.ucla.edu/packages/procmail.html' 페이지에서 AIX 버전에 맞는 파일을 선택하여 다운로드 할 수 있다.

```
bash-4.00# wget \
http://computer-refuge.org/classiccmp/aixpdslib/pub/procmail/RISC/5.3/exec/procmail.3.22.tar.Z
```

2.2 procmail 설치

아래와 같이 파일 압축 해제 후 '/usr/local' 디렉토리로 복사한다.

```
bash-4.00# gunzip procmail.3.22.tar.Z
bash-4.00# tar xf procmail.3.22.tar
bash-4.00# cp -R usr/local/* /usr/local
```

2.3 sendmail.cf 설정 변경

sendmail과 procmail의 연동을 위한 설정이 필요하므로 아래와 같이 sendmail.cf 파일의 가장 마지막 라인에 설정을 추가한다.

```
bash-4.00# vi /etc/mail/sendmail.cf
.................. (중략)
Mlocal,          P=/usr/local/bin/procmail, F=SAw5/@glDFMPhsfn, S=10/30, R=20/40,
                 T=DNS/RFC822/X-Unix,
                 A=procmail -Y -a $h -d $u
```

3. spf-filter 다운로드 및 설치

'spf-filter'는 procmail과 연동하여 스팸 차단에 활용할 수 있다. SPF 인증이 실패(fail/softfail)하였을 경우에 메일 제목에 [SPAM] 태그를 추가하여 스팸으로 분류할 수 있다.

파일은 'http://blog.daum.net/effortless/7864600'에서 다운로드 가능하다.

다운로드한 'spf-filter' 파일을 아래와 같이 압축 해제 후 디렉토리를 이동시키고 권한 설정을 한다.

```
bash-4.00# gunzip spf-filter.zip
bash-4.00# mv spf-fitler /usr/local/bin/spf-filter
bash-4.00# chmod 755 /usr/local/bin/spf-filter
```

4. 룰셋 설정

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

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

```
bash-4.00# vi /etc/procmailrc
# The lock file ensures that only 1 spf-filter invocation happens
# at 1 time, to keep the load down.
#
:0fw: spf-filter.lock
| /usr/local/bin/spf-filter
# All mail tagged as spam (eg. with a score higher than the set threshold)
# is moved to "probably-spam".
:0:
* ^X-SPF-Filter: Fail
probably-spam
```

III. SPF 인증 결과 로그 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-4.00# cat /var/log/procmail
procmail: Extraneous locallockfile 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 locallockfile 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
```