메일서버등록제(SPF) 인증 기능 적용 안내서

(SunOS - qmail)

	OS	Mail Server	SPF 적용 모듈 (C언어 기반)
작성기준	SunOS 5.10 32bit	qmail 1.03	qmail-spf-rc5 patch

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. qmail, 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 제거

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

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-3.00# telnet 0 25 (메일서버 25번 포트 접속)
Trying 0.0.0.0...
Connected to 0.
Escape character is '^]'.
220 spf.kisa.or.kr ESMTP Sendmail 8.13.8+Sun/8.13.8; Mon, 5 Jul 2010 00:38:27 +0900 (KST)
quit (접속 종료)
221 2.0.0 spf.kisa.or.kr closing connection
Connection to 0 closed by foreign host.
```

아래와 같이 패키지 관리 도구인 'pkgrm'을 이용하여 기존에 설치된 'sendmail'을 삭제한다.

```
bash-3.00# pkgrm SUNWsndmu
bash-3.00# pkgrm SUNWsndmr
```

2. gcc 설치

2.1 gcc 설치 여부 확인

qmail의 기본 패키지에는 SPF 인증 기능이 포함되어 있지 않으므로 SPF 라이브러리를 통합하여 qmail을 구성해야 한다. qmail 설치 시 소스코드를 컴파일해서 설치해야 하기 때문에 아래와 같이 gcc 설치 여부를 확인한다.

```
bash-3.00# gcc --version
gcc (GCC) 3.4.6
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.
```

2.2 다운로드 및 설치

gcc가 설치되어 있지 않다면 SunOS용 프리웨어 다운로드 사이트인 'http://www.sunfreeware.com'에서 x86용 'libiconv', 'libintl', 'gcc'를 다운로드 한다.

```
bash-3.00# wget ftp://ftp.sunfreeware.com/pub/freeware/intel/10/libintl-3.4.0-sol10-x86-local.gz
bash-3.00# wget ftp://ftp.sunfreeware.com/pub/freeware/intel/10/libiconv-1.13.1-sol10-x86-local.gz
bash-3.00# wget ftp://ftp.sunfreeware.com/pub/freeware/intel/10/gcc-3.4.6-sol10-x86-local.gz
```

아래와 같이 gunzip 명령어를 이용하여 파일 압축을 해제한 후 SunOS 패키지 관리 도구인 pkgadd를 이용하여 설치한다.

```
bash-3.00# gunzip libintl-3.4.0-sol10-x86-local.gz libiconv-1.13.1-sol10-x86-local.gz \
gcc-3.4.6-sol10-x86-local.gz-bash-3.00# pkgadd -d /src/libintl-3.4.0-sol10-x86-local
.................. (중략)
bash-3.00# pkgadd -d /src/libiconv-1.13.1-sol10-x86-local
.................. (중략)
bash-3.00# pkgadd -d /src/gcc-3.4.6-sol10-x86-local
.................. (중략)
```

※ '/usr/local/bin' 디렉토리에 실행파일이 설치된다.

3. ucspi-tcp 설치

qmail은 단독 데몬 프로세스로 동작하지 않기 때문에 ucpsi-tcp와 같은 네트워크 데몬 형태의 포트 서비스 프로그램을 필요로 한다.

※ ucpsi-tcp는 유닉스 계열 클라이언트/서버 프로그램으로서 tcpserver와 tcpclient 프로그램을 생성한다. tcpserver는 동시 접속 제한 및 프로세스와 메모리를 보호하는 역할을 하게 된다.

3.1 다운로드 및 압축 해제

아래와 같이 wget 명령어를 이용하여 'ucspi-tcp-0.88' 패키지를 다운로드 한 후 압축을 해제한다.

```
bash-3.00# wget http://cr.yp.to/ucspi-tcp/ucspi-tcp-0.88.tar.gz
http://cr.yp.to/ucspi-tcp/ucspi-tcp-0.88.tar.gz
..... (중략)
bash-3.00# gunzip ucspi-tcp-0.88.tar.gz
bash-3.00# tar xf ucspi-tcp-0.88.tar
```

압축 해제 후 소스 패키지를 설치하면 '/usr/local' 디렉토리에 실행 파일 및 라이브러리 등이 설치된다.

3.2 컴파일 및 설치

설치된 glibc 버전이 2.3.1 이상이면 컴파일 과정에서 에러가 발생하므로 패키지에 포함된 error.h의 파일에 '#include <errno.h>'를 추가한다.

```
bash-3.00# cd ucspi-tcp-0.88
bash-3.00# vi error.h
#include <errno.h>
#ifndef ERROR_H
..... (중략)
:wq!
```

※ 주의) '#include <errno.h>' 항목이 추가가 되지 않았을 경우 '/usr/bin/ld: errno: TLS definition in /lib/libc.so.6 section .tbss mismatches non-TLS reference in tcpserver.o'과 같은 에러가 발생한다.

아래와 같이 ‘make’, ‘make setup check‘를 입력하여 설치를 완료한다.

```
bash-3.00## make
( cat warn-auto.sh; \
        echo 'main="$1"; shift'; \
        echo exec "`head -1 conf-ld`" \
..................  (중략)
./load install hier.o auto_home.o unix.a byte.a
./compile instcheck.c
./load instcheck hier.o auto_home.o unix.a byte.a
[root@spf ucspi-tcp-0.88]# make setup check
./install
./instcheck
..................  (중략)
```

※ ‘/usr/local/bin’ 디렉토리에 프로그램이 설치된다.

4. daemontools 다운로드 및 설치

daemontools는 Unix 서비스를 감시하는 프로그램으로서 네트워크 포트 데몬으로 동작하는 서비스가 죽거나 반응이 없으면 해당 데몬을 자동으로 재시작 하는 기능을 제공하는 도구이다.

4.1 설치 디렉토리 생성

daemontools를 설치하기 위해서 아래와 같이 ‘/package‘ 디렉토리를 생성하고 권한을 부여한다.

```
bash-3.00# mkdir /package
bash-3.00# chmod 1775 /package/
bash-3.00# cd /package/
```

※ 주의) daemontools는 임의의 네트워크 데몬을 감시할 수 있는 프로그램이므로, 보안을 위해서 디렉토리에 ‘t 퍼미션(sticky bit)’을 부여해야 한다.

4.2 다운로드 및 압축 해제

아래와 같이 'daemontools-0.76'을 다운로드 한 후 압축을 해제한다.

```
bash-3.00# wget http://cr.yp.to/daemontools/daemontools-0.76.tar.gz
http://cr.yp.to/daemontools/daemontools-0.76.tar.gz
Resolving cr.yp.to... 131.193.36.21
Connecting to cr.yp.to|131.193.36.21|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 36975 (36K) [application/x-gzip]
Saving to: `daemontools-0.76.tar.gz'
`daemontools-0.76.tar.gz' saved [36975/36975]
bash-3.00# gunzip daemontools-0.76.tar.gz
bash-3.00# tar xf daemontools-0.76.tar
```

4.3 컴파일 및 설치

설치된 glibc 버전이 2.3.1 이상이면 컴파일 과정에서 에러가 발생하므로 패키지에 포함된 error.h의 파일에 '#include <errno.h>'를 추가한다.

```
bash-3.00# cd admin/daemontools-0.76/src/
bash-3.00# vi error.h
#include <errno.h>
#ifndef ERROR_H
#define ERROR_H
.................. (중략)
:wq!
```

아래와 같이 디렉토리 이동 후 설치 스크립트를 실행한다.

```
bash-3.00# cd /package/admin/daemontools-0.76/
bash-3.00# package/install
Linking ./src/* into ./compile...
.................. (중략)
Creating /service...
Adding svscanboot to inittab...
init should start svscan now.
```

아래와 같이 '/etc/inittab' 파일의 마지막 라인에 위치한 실행 스크립트를 변경한다.

```
bash-3.00# vi /etc/inittab
.................. (중략)
SV:123456:respawn:/command/svscanboot </dev/null >/var/log/svscan 2>&1
```

qmail을 설치하기 전에 '/etc/inittab'에 등록된 'daemontools'의 실행을 위하여 시스템을 재시작 한다.

```
bash-3.00# reboot
```

5. qmail 설치 및 SPF 패치

5.1 qmail 다운로드

qmail 원본 소스를 아래와 같이 wget 명령어를 이용하여 다운로드 한다.

※ 각테일, knetqmail 등의 사용자 패치는 미 적용하였다.

```
bash-3.00# cd /src
bash-3.00# wget http://cr.yp.to/software/qmail-1.03.tar.gz
http://cr.yp.to/software/qmail-1.03.tar.gz
Resolving cr.yp.to... 131.193.36.21
Connecting to cr.yp.to|131.193.36.21|:80... connected.
HTTP request sent, awaiting response... 200 OK
..... (중략)
Saving to: `qmail-1.03.tar.gz'
qmail-1.03.tar.gz' saved [220668/220668]
```

5.2 qmail-spf 패치 파일 다운로드

아래와 같이 wget 명령어를 이용하여 'qmail-spf-rc5' 패치 파일을 다운로드 한다.

```
bash-3.00# wget http://www.saout.de/misc/spf/qmail-spf-rc5.patch
http://www.saout.de/misc/spf/qmail-spf-rc5.patch
Resolving www.saout.de... 78.46.99.52, 2001:6f8:13b1:3::2:1
Connecting to www.saout.de|78.46.99.52|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 63582 (62K) [text/plain]
Saving to: `qmail-spf-rc5.patch'
qmail-spf-rc5.patch' saved [63582/63582]
```

5.3 qmail-spf 패치

아래와 같이 qmail 소스 파일을 압축 해제 한 후 소스 디렉토리로 이동하여 patch 명령어를 실행한다.

※ patch는 원본 소스와 수정된 소스를 비교(diff)해서 패치파일을 적용하는 스크립트이다.

```
bash-3.00# gunzip qmail-1.03.tar.gz
bash-3.00# tar xf qmail-1.03.tar
bash-3.00# cd qmail-1.03
bash-3.00# /usr/local/bin/patch -p1 < ../qmail-spf-rc5.patch
patching file byte_cspn.c
patching file byte.h
patching file byte_rcspn.c
..... (중략)
patching file TARGETS
patching file tcp-env.c
```

※ 주의) patch 옵션과 디렉토리가 다르면 패치 과정에서 오류가 발생한다.
http://www.sunfreeware.com에서 SunOS용 GNU patch 프로그램을 다운 받아서 패치를 해야 한다.

5.4 qmail 디렉토리 및 계정/그룹 생성

qmail을 컴파일하기 전에 아래와 같이 사용자 계정과 그룹을 생성한다.

```
bash-3.00# mkdir /var/qmail
bash-3.00# groupadd nofiles
bash-3.00# useradd -g nofiles -d /var/qmail/alias alias
bash-3.00# useradd -g nofiles -d /var/qmail qmaild
bash-3.00# useradd -g nofiles -d /var/qmail qmaill
bash-3.00# useradd -g nofiles -d /var/qmail qmailp
bash-3.00# groupadd qmail
bash-3.00# useradd -g qmail -d /var/qmail qmailq
bash-3.00# useradd -g qmail -d /var/qmail qmailr
bash-3.00# useradd -g qmail -d /var/qmail qmails
```

5.5 컴파일 및 설치

설치된 glibc 버전이 2.3.1 이상이면 컴파일 과정에서 에러가 발생하므로 패키지에 포함된 error.h의 파일에 '#include <errno.h>'를 추가한다.

```
bash-3.00# cd qmail-1.03
bash-3.00# vi error.h
#include <errno.h>
#ifndef ERROR_H
#define ERROR_H
.................. (중략)
:wq!
```

아래와 같이 'make', 'make setup check', './config-fast 도메인명'을 입력하여 컴파일/설치를 한다.

※ 도메인명은 FQDN(Fully Qualified Domain Name의 약자)을 입력한다.

```
bash-3.00# ln -s /usr
/local/bin/gcc /usr/local/bin/cc
bash-3.00# make
( cat warn-auto.sh; \
        echo CC=\'`head -1 conf-cc`\'; \
.................. (중략)
bash-3.00# make setup check
bash-3.00# ./config-fast mail.testdomain.com
```

※ '/var/qmail' 디렉토리에 실행/설정파일들이 설치된다.

5.6 구동 스크립트 디렉토리 생성

qmail 구동 스크립트를 작성하기 위하여 아래와 같이 디렉토리를 생성한 후 't 퍼미션(sticky bit)'을 부여한다.

```
bash-3.00# mkdir -p /var/qmail/supervise/qmail-send/log
bash-3.00# mkdir -p /var/qmail/supervise/qmail-smtpd/log
bash-3.00# chmod +t /var/qmail/supervise/qmail-send
bash-3.00# chmod +t /var/qmail/supervise/qmail-smtpd
```

5.7 구동 스크립트 작성

각 qmail 구동 스크립트의 작성 방법과 의미는 다음과 같다.

- /var/qmail/rc :
  qmail의 기본 구동 스크립트

```
bash-3.00# cd /var/qmail/
bash-3.00# vi rc
#!/bin/sh
exec env - PATH="/var/qmail/bin:$PATH" qmail-start ./Maildir/
bash-3.00# chmod 755 rc
```

- /var/qmail/supervise/qmail-send/run :
  메일 발송을 담당하는 스크립트

```
bash-3.00# cd /var/qmail/supervise/qmail-send/
bash-3.00# vi run
#!/bin/sh
exec /var/qmail/rc
bash-3.00# chmod 755 run
```

o /var/qmail/supervise/qmail-send/log/run :

메일 발송 시 로그를 기록하는 스크립트

```
bash-3.00# cd /var/qmail/supervise/qmail-send/log/
bash-3.00# vi run
#!/bin/sh
exec /usr/local/bin/setuidgid qmaill  /usr/local/bin/multilog t /var/log/qmail
bash-3.00# chmod 755 run
```

o /var/qmail/supervise/qmail-smtpd/run :

메일 수신을 위한 서비스를 실행하는 스크립트

```
bash-3.00# cd /var/qmail/supervise/qmail-smtp
bash-3.00# vi run
#!/bin/sh
Q_UID=`/usr/xpg4/bin/id -u qmaild`
Q_GID=`/usr/xpg4/bin/id -u qmaild`
exec /usr/local/bin/softlimit -m 2000000 \
    /usr/local/bin/tcpserver -vHRl 0 -x /etc/tcp.smtp.cdb \
    -u $Q_UID -g $Q_GID 0 25 /var/qmail/bin/qmail-smtpd 2>&1
bash-3.00# chmod 755 run
```

※주의) SunOS의 경우 Q_UID, Q_GID 변수 설정 시 프로그램의 위치가 다르므로 구동 스크립트를 수정한다.

o /var/qmail/supervise/qmail-smtpd/log/run :

메일 수신시 로그를 기록하는 스크립트

```
bash-3.00# cd /var/qmail/supervise/qmail-smtp/log
bash-3.00# vi run
#!/bin/sh
exec /usr/local/bin/setuidgid qmaill \
    /usr/local/bin/multilog t /var/log/qmail/smtpd
bash-3.00# chmod 755 run
```

5.8 로그 디렉토리 생성

로그를 기록하기 위해서 아래와 같이 디렉토리를 생성하고 접근 권한을 부여한다.

```
bash-3.00# mkdir -p /var/log/qmail/smtpd
bash-3.00# chown -R qmaill /var/log/qmail
bash-3.00# ln -s /var/qmail/supervise/qmail-send \
/var/qmail/supervise/qmail-smtpd /service
```

5.9 반송 메일 수신 계정 생성

반송 메일 수신을 위해서 root, postmaster 계정으로 수신되는 메일을 관리자 계정으로 포워딩을 할 수 있도록 아래와 같이 설정을 한다.

※ 예시의 주소 'admin@example.com' 계정 대신에 실제 메일서버 관리자 계정을 입력한다.

```
bash-3.00# echo admin@example.com > /var/qmail/alias/.qmail-root
bash-3.00# echo admin@example.com  > /var/qmail/alias/.qmail-postmaster
```

5.10 릴레이 허용을 위한 IP 설정

아래와 같이 localhost(127.0.0.1)와 메일 서버 IP의 릴레이를 허용한다. tcprules 명령어를 이용하여 DB화한 파일을 생성한다.

```
bash-3.00# vi /etc/tcp.smtp
127.0.0.1:allow,RELAYCLIENT=""
192.168.1.1:allow,RELAYCLIENT=""
bash-3.00# tcprules /etc/tcp.smtp.cdb /etc/tcp.smtp.tmp < /etc/tcp.smtp
```

5.11 서비스 구동 스크립트 다운로드

아래와 같이 wget 명령어를 이용하여 qmail 서비스 구동 스크립트를 다운로드 한 후 스크립트의 이름을 변경하고 실행 권한을 부여한다.

※주의) SunOS의 경우 'QMAILDUID', 'NOFILESGID' 변수 설정 시 프로그램의 위치가 다르므로 구동 스크립트를 수정한다.

```
bash-3.00# cd /etc/init.d
bash-3.00# wget http://lifewithqmail.org/qmailctl-script-dt70
.................. (중략)
`qmailctl-script-dt70' saved [3053/3053]
root@spf:/etc/init.d# mv qmailctl-script-dt70 qmail
bash-3.00# vi /etc/init.d/qmail
.................. (중략)
QMAILDUID=`/usr/xpg4/bin/id -u qmaild`
NOFILESGID=`/usr/xpg4/bin/id -g qmaild`
.................. (중략)
:wq
bash-3.00# chmod 755 qmail
```

5.12 qmail 시작

아래와 같이 qmail 구동 스크립트를 실행한 후 tcp/25번 포트에 접속하여 정상적으로 qmail이 실행되고 있는지 확인한다.

```
bash-3.00# /etc/init.d/qmail start
Starting qmail
bash-3.00# telnet 0 25
Escape character is '^]'.
220 kisarbl.or.kr ESMTP
quit
```

III. SPF 적용 여부 확인 및 차단

1. SPF 판별을 위한 판정값 설정

qmail에 적용되는 차단 레벨을 설정하기 위해서 '/var/qmail/control' 디렉토리의 spfbehavior 파일에서 레벨을 지정할 수 있다.

아래는 SPF fail 시 메일 수신을 거부(reject) 하는 값인 '3'을 적용한 예시이다.

```
bash-3.00# cd /var/qmail/contorl
bash-3.00# vi spfbehavior
3
```

SPF 판정값은 '0~6'까지 지정할 수 있으며 각각의 의미는 아래와 같다. 상위 판정값은 하위 판정값을 포함한다. 즉, 판정값 '6'은 하위 '0~5' 판정값을 포함한다.

판정값	의미
0	SPF 확인하지 않음, SPF-Received 헤더 추가하지 않음
1	SPF-Recevied 헤더만 추가, 메일거부기능 사용하지 않음
2	DNS 서버의 다운으로 인해 조회가 되지 않는 경우 Temperr (451 SPF lookup failure과 같이 응답을 하면서 거부)
3	'**fail**' 판정시 거부(**reject**)
4	'**Soft-fail**' 판정시 거부(**reject**)
5	'**neutral**' 판정시 거부(**reject**)
6	'**pass**' 이외의 모든 상태 거부(**reject**)

※ 주의) 판정값을 변경한 이후에는 qmail을 재시작 한다.

2. 차단 확인

메일 서버에 SPF 적용이 완료되었으면, 아래와 같이 telnet 명령어를 이용하여 SPF 인증 기능이 적용된 메일서버로 접속해 본다.

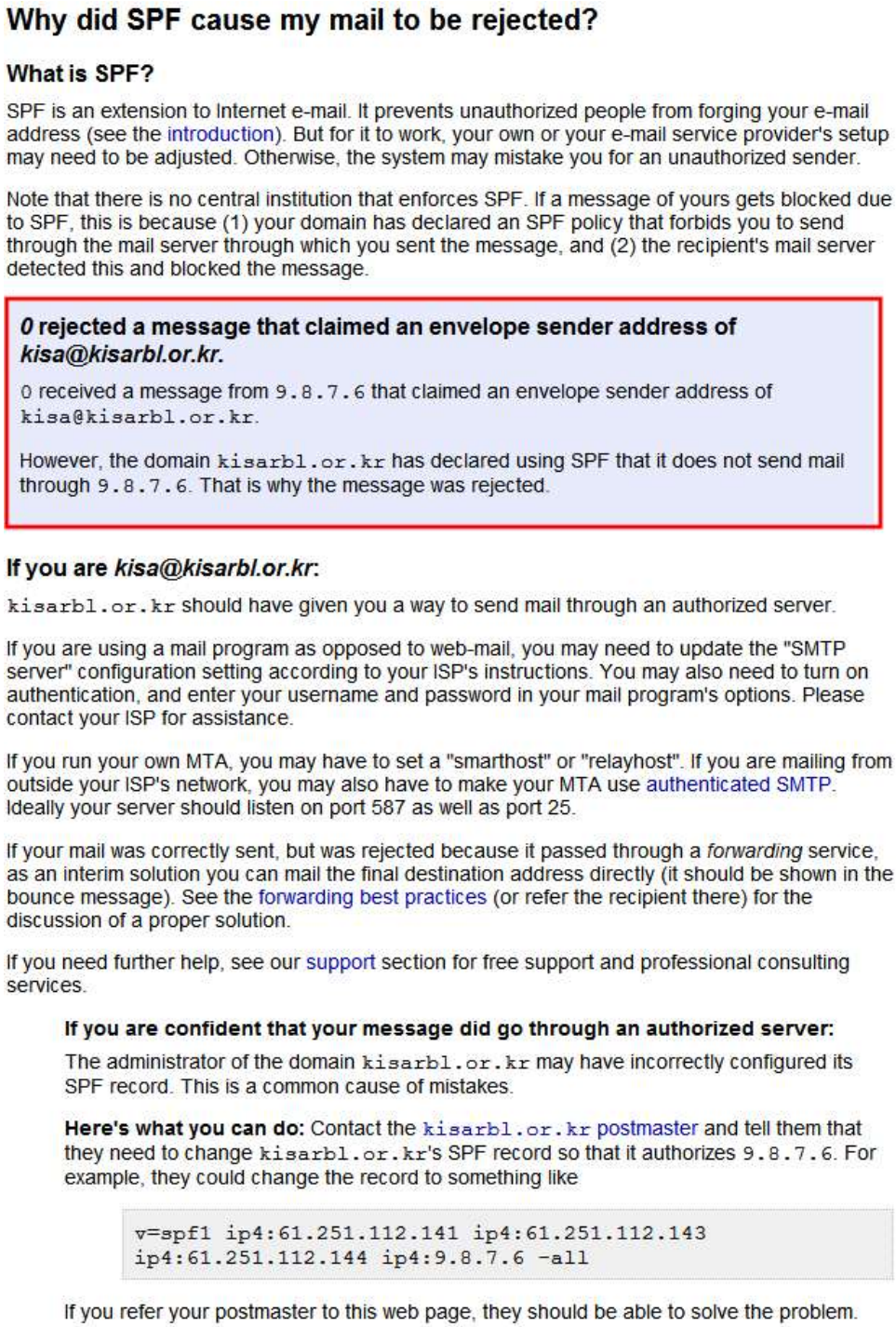
메일 발송 IP와 SPF 레코드의 IP가 일치하지 않으면 메일 수신 주소를 입력하는 단계에서 SPF 인증이 실패하여 메일 전송이 차단되는 것을 확인할 수 있다.

'550 See http://spf.pobox.com/why.html?sender=kisa%40kisarbl.or.kr&ip=9.8.7.6 &receiver=0 (#5.7.1)'와 같은 오류 코드가 나타나며 표시되는 URL에서 상세 내용을 확인할 수 있다.

```
bash-3.00# telnet 메일서버IP 25 (공인 IP만 가능하며, 127.0.0.1은 확인 불가)
Trying 1.2.3.4...
Connected to your (1.2.3.4).
220 mail.yourdomian.com ESMTP
Escape character is '^]'.
ehlo test.com
250 kisarbl.or.kr
mail from: test@kisarbl.or.kr (메일 발신 주소)
250 ok
rcpt to: test@yourdomain.com (메일 수신 주소)
550 See http://spf.pobox.com/why.html?sender=kisa%40kisarbl.or.kr&ip=9.8.7.6
&receiver=0 (#5.7.1)  (차단되었음을 확인 할 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 시 차단 확인 페이지