실시간 스팸차단리스트(RBL)
이용 방법

(https://www.kisarbl.or.kr)

qmail(1.03) 사용 설명서

KISA 한국인터넷진흥원/스팸대응팀

< 목 차 >

Ⅰ. 개요

실시간 스팸차단리스트(RBL)는 메일서버를 운영하는 누구나 손쉽게 효과적으로 스팸 수신을 차단하는데 이용할 수 있도록 한국인터넷진흥원(KISA)에서 관리·운영하여 무료로 제공하고 있습니다.

국내·외로부터 스팸정보를 실시간으로 취합하고 이를 다양한 기준에 따라 분석한 결과, 스팸전송에 관련된 것으로 확인된 IP를 리스트로 생성하여 1시간 단위로 제공합니다.

실시간 스팸차단리스트(RBL)를 이용하면 수신되는 모든 이메일의 발송IP 확인을 통해 스팸여부를 판단하여 즉각 차단하므로 메일서버 등 자원의 불필요한 소모를 방지할 수 있습니다.

실시간 스팸차단리스트(RBL) 간편 설정은 이메일 수신량이 1일 10만 통 이하인 곳에서 사용이 적합하며, 이메일이 수신될 때마다 한국인터넷진흥원 RBL서버에 직접 질의하여 스팸 여부를 확인합니다.

별도로 소프트웨어를 설치할 필요가 없고, 메일서버가 RBL 서버를 참조하도록 설정하여 간편하게 이용할 수 있습니다.

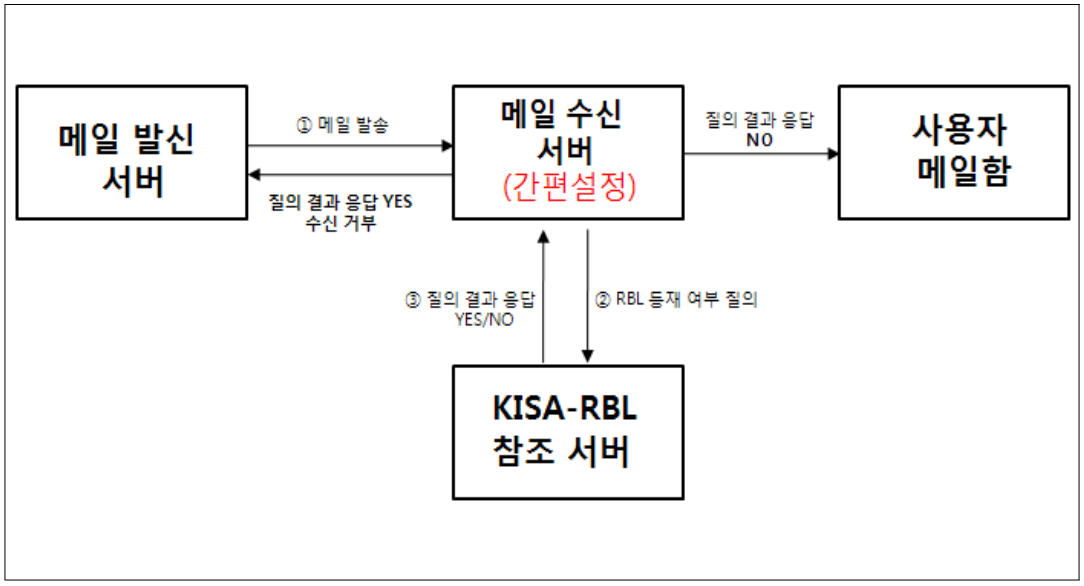
본 매뉴얼은 실시간 스팸차단리스트(RBL)를 이용하여 스팸메일 수신을 차단하는 방법을 소개합니다.

Ⅱ. 실시간 스팸차단리스트(RBL) (간편설정)

실시간 스팸차단리스트(RBL) 간편 설정은 이메일 수신량이 1일 10만 통 이하인 곳에서 사용이 적합하며, 이메일이 수신될 때마다 한국인터넷진흥원 RBL서버에 직접 질의하여 스팸 여부를 확인합니다.

별도로 소프트웨어를 설치할 필요가 없고, 메일 서버의 설정 파일에 한 줄의 옵션을 추가하면 메일서버가 RBL서버를 참조하도록 변경하여 간편하게 이용할 수 있습니다.

단, 전체 3등급 중에서 1등급에 해당하는 RBL만 제공되므로, 보다 많은 스팸메일을 차단하거나 자신의 정책에 맞게 RBL을 선택적으로 사용하고자 하는 경우에는 RBLDNSD 이용방법을 참고합니다.



[그림2-1] 실시간 스팸차단리스트(RBL) (간편설정) 흐름도

1. 메일 서버 (qmail 1.03) 설정 변경

qmail에서 RBL 참조서비스를 사용하기 위해서는 rblsmtpd 프로그램이 설치되어 있어야 합니다.

rblsmtpd는 ucspi-tcp 패키지에 포함되어 있으므로, 아래와 같이 wget 명령어를 이용하여 최신 버전의 ucspi-tcp 패키지를 다운로드합니다.

```
# cd /home/
# wget http://cr.yp.to/ucspi-tcp/ucspi-tcp-0.88.tar.gz
--15:03:09--  http://cr.yp.to/ucspi-tcp/ucspi-tcp-0.88.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: 53019 (52K) [application/x-gzip]
Saving to: `ucspi-tcp-0.88.tar.gz'

100%[=========================>] 53,019        65.9K/s    in 0.8s

15:03:11 (65.9 KB/s) - `ucspi-tcp-0.88.tar.gz' saved [53019/53019]
```

[그림2-2] wget 명령어를 사용하여 ucspi-tcp 패키지 다운로드

다음 [그림2-3]과 같이 다운로드한 ucspi-tcp 패키지를 압축 해제하고 소스코드를 컴파일 합니다.

```
# gunzip ucspi-tcp-0.88.tar.gz
# tar xvf ucspi-tcp-0.88.tar
# cd ucspi-tcp-0.88
# make
-------------------- 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
```

[그림2-3] 파일 압축 해제 및 소스코드 컴파일

다음 [그림2-4]와 같이 ucspi-tcp 패키지를 설치합니다.

```
# make setup check
./install
./instcheck
```

[그림2-4] ucspi-tcp 설치

다음 [그림2-5]와 같이 rblsmtpd가 정상적으로 설치되었는지 확인합니다.

```
# ls -al /usr/local/bin/rblsmtpd
-rwxr-xr-x    1 root     bin         34616 2009년  1월  1일 /usr/local/bin/rblsmtpd
```

[그림2-5] rblsmtpd 설치 확인

다음 [그림2-6]과 같이 qmail 설치 과정에서 생성한 run 파일을 편집합니다.

'-b' 옵션은 IP주소가 RBL에 등재되어 있는 경우 '553'에러를 표시하며,

'-r' 옵션 다음에는 RBL-BLOCK을 위한 RBL 베이스를 지정합니다.

RBL 베이스는 실시간 스팸차단리스트(RBL)를 참조할 경우 'spamlist.or.kr'을 지정하며, 다른 RBL을 함께 참조할 경우에는 '-r' 옵션 다음에 해당 RBL 베이스를 추가 입력합니다.

(Ex. -r bl.spamcop.net, -r cbl.abuseat.net, -r zen.spamhaus.org, ...)

```
# cd /var/qmail/supervise/qmail-smtpd
# vi run
<run 파일 내용 중에서>
#!/bin/sh
exec /usr/local/bin/softlimit -m 3000000 \
/usr/local/bin/tcpserver -v -p -x \
/etc/tcp.smtp.cdb -u 102 -g 101 0 25 \
/usr/local/bin/rblsmtpd -b -r spamlist.or.kr -r bl.spamcop.net  \    (추가된 부분)
/var/qmail/bin/qmail-smtpd 2>&1
```

[그림2-6] run 파일에 rblsmtpd 설정

다음과 같이 qmail 데몬을 재시작 한 후, 서비스가 정상적으로 실행 중인지와 25번 포트가 정상적으로 열려있는지 확인합니다.

```
# /etc/init.d/qmaild stop   (중지)
# /etc/init.d/qmaild start  (시작)
# ps -ef | grep qmail       (qmail 프로세스 확인)
# netstat -an | grep 25     (포트가 열려있는지 확인)
```

[그림2-7] qmail 재시작 및 프로세스 확인

2. 스팸 차단 테스트

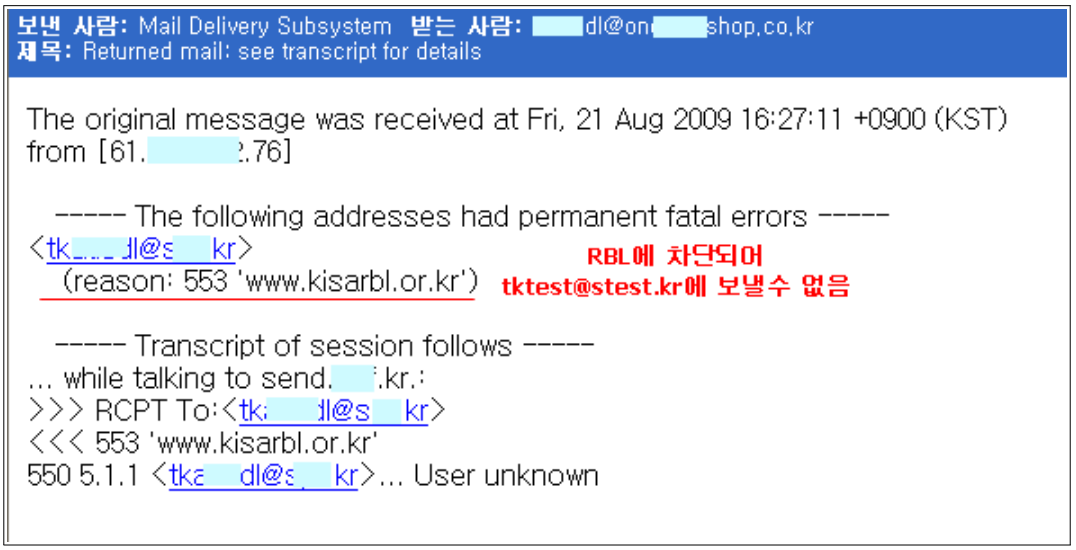
간편 설정이 적용된 메일 서버의 메일로그에서 다음과 같이 스팸 차단 여부를 확인 할 수 있습니다. 61.x.x.83 IP에서 발송된 메일이 실시간 스팸차단리스트(RBL)에 의하여 차단된 내용을 보여줍니다.

```
#cd /var/adm/log/qmail/smtpd
#vi current
<current 내용 중에서>
tcpserver: pid 28940 from 61.x.x.83
tcpserver: ok 28940 :61.x.x.103:25 :61.x.x.83::33373
rblsmtpd: 61.x.x.83 pid 28940: 553 'www.kisarbl.or.kr'
tcpserver: end 28940 status 0
tcpserver: status: 0/40
```

[그림2-8] maillog 확인

※ OS 및 메일서버 로그 레벨, 설정에 따라 로그 디렉터리 위치와 내용이 다르게 보일 수 있습니다.

아래는 스팸리스트에 등록된 61.x.x.83 IP에서 메일을 발송하였을 때 반송된 메일이며, 실시간 스팸차단리스트(RBL)에 의하여 차단된 것을 확인 할 수 있습니다.


보낸 사람: Mail Delivery Subsystem 받는 사람: dl@on shop.co.kr
제목: Returned mail: see transcript for details

The original message was received at Fri, 21 Aug 2009 16:27:11 +0900 (KST)
from [61. .76]

----- The following addresses had permanent fatal errors -----
<tk dl@s kr>
(reason: 553 'www.kisarbl.or.kr')

RBL에 차단되어
tktest@stest.kr에 보낼수 없음

----- Transcript of session follows -----
... while talking to send. .kr.:
>>> RCPT To:<tk dl@s kr>
<<< 553 'www.kisarbl.or.kr'
550 5.1.1 <tk dl@s kr>... User unknown

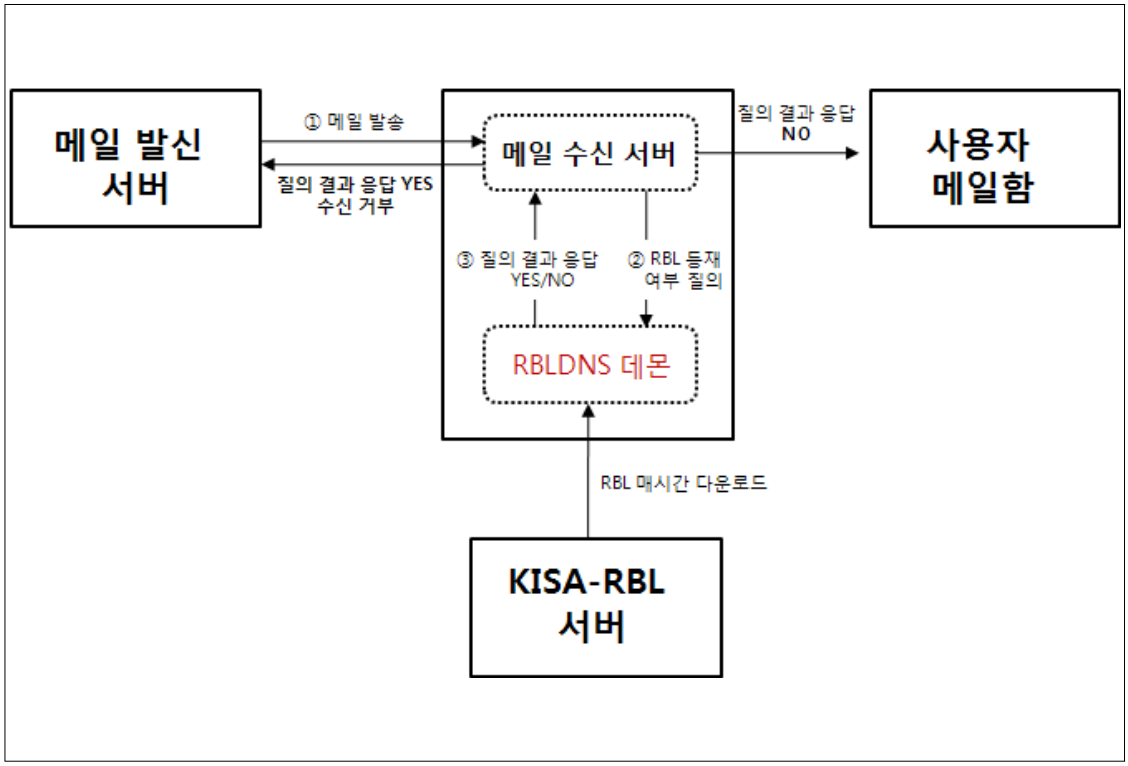
[그림2-9] 블랙IP 반송 메일

Ⅲ. 실시간 스팸차단리스트(RBL) (RBLDNSD 이용)

내부 시스템에 RBLDNS 데몬을 설치하여 이용하는 방법이며, 매시간 업데이트된 RBL 파일을 다운로드 받아 메일서버에 반영하고, 이메일 수신시마다 자체적으로 RBL을 대조하여 스팸메일을 차단하는 방법입니다.

선행 작업으로 프로그램(RSYNC, RBLDNS Daemon)을 설치하고, 실시간 스팸차단리스트(RBL)를 이용할 수 있도록 메일 서버에 필요한 설정을 해야 합니다.

KISA에서 3등급으로 나누어 제공하는 RBL을 자신의 정책에 맞게 선택하거나 수정하여 사용할 수 있으며, 실시간 스팸차단리스트(RBL) 간편설정 방법에 비해 대용량 메일처리가 용이합니다.



[그림3-1] 실시간 스팸차단리스트(RBL) (RBLDNSD 이용) 흐름도

1. 시스템 환경 및 프로그램 상세 내역

본 매뉴얼은, 운영체제 Solaris 10을 기준으로 작성 되었으며, 상세 버전은 아래와 같습니다.

프로그램	상세 버전
운영 체제	Solaris 10 (SunOS 5.10)
메일 서버	qmail 1.03
스팸리스트 다운로드 프로그램	rsync 3.0.6
RBLDNS Daemon	rbldnsd 0.996b

[표1] 시스템 환경 및 프로그램 상세 내역

2. 실시간 스팸차단리스트(RBL) 사이트 회원 가입

실시간 스팸차단리스트(RBL)를 다운로드 하기 위해서는 사전에 회원가입을 해야 합니다.

가입 신청 완료 후, KISA 운영자에 의해 가입이 승인되어야 최종적으로 가입이 완료됩니다.

가입 승인 후, 다운로드 받을 서버의 IP와 호스트명을 등록하며, 등록된 서버에서만 스팸리스트(RBL)를 다운로드 받을 수 있습니다.

회원 가입은 스팸리스트(RBL)를 다운로드 받기위해 서버 정보를 등록하는 곳이며, **화이트도메인 등록 신청과는 무관**합니다.

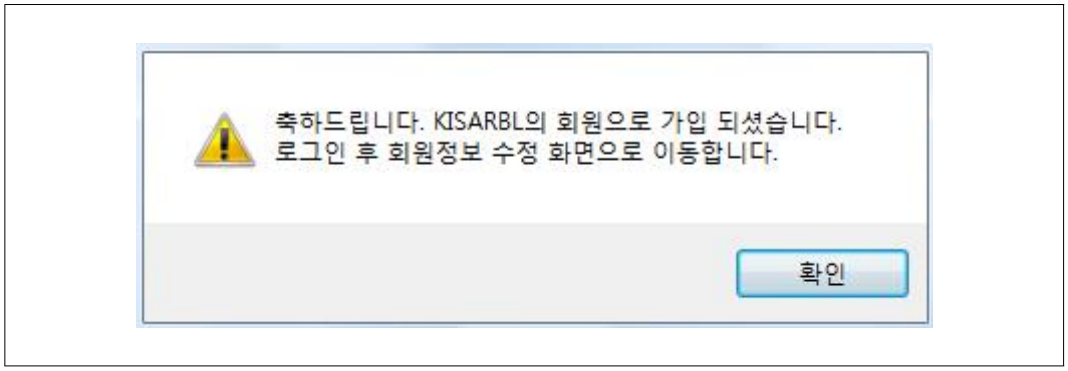
2.1 회원 가입 신청

회원 가입은 [https://www.kisarbl.or.kr > KISA-RBL 참조 서비스 > RBLDNSD 이용 > 회원가입] 에서 등록 신청 합니다.

아래와 같이 회원 가입 정보를 입력합니다.

[그림3-2] 회원 가입 정보 입력

회원 가입 신청이 완료되면, 아래와 같이 팝업창이 나타납니다.



[그림3-3] 회원 가입 신청 완료

o 운영자 승인

실시간 스팸차단리스트(RBL) 운영자가 가입 승인을 완료하면, **등록 시 입력하였던 이메일 주소로 가입완료 통보 메일이 발송** 됩니다.

회원 가입 승인을 위해서는, 등록 신청 정보에 허위 내용이 없어야 하며, 등록 신청한 사이트에 불법적인 내용(도박, 대출, 성인 광고 등)이 없어야 합니다. 이러한 사유로 회원 가입 승인이 유보되는 경우에는 운영자(ksrt@kisa.or.kr)에게 문의하시기 바랍니다.

o 회원 로그인

다음과 같이 [https://www.kisarbl.or.kr > KISA-RBL 참조서비스 > RBLDNSD 이용 > 회원로그인]에서 로그인 합니다.

[그림3-4] 회원 로그인 페이지

2.2 다운로드용 서버정보 등록

KISA 승인 후, 로그인하여 아래 [그림3-5]와 같이 회원정보 수정 페이지에서 실시간 스팸차단리스트(RBL)를 다운로드 받을 서버의 IP주소와 호스트명(별칭)을 등록합니다.

[그림3-5] 다운로드 받을 서버의 IP주소와 호스트명 입력

아래는 'IP'와 '호스트'가 추가된 화면이며, '전송상태'는 정상적으로 다운로드가 되었는지 나타나는 항목입니다.

[그림3-6] IP주소와 호스트명이 추가되었음

위 그림[3-6]과 같이 'IP'를 클릭하면, 아래와 같이 스팸리스트 다운로드 로그 정보를 확인 할 수 있는 팝업창이 나타납니다.

[RSYNC LOG 조회화면]

시작 시간	종료 시간	IP주소	<수신/발신>	상태	전송량
2009-10-27 13:00:13.0	2009-10-27 13:00:26.0	61.251.	send	success	11751342
2009-10-23 13:00:04.0	2009-10-23 13:00:13.0	61.251.	send	success	11891409
2009-10-11 13:00:53.0	2009-10-11 13:01:02.0	61.251.	send	success	10373355

[그림3-7] RSYNC 다운로드 이력 확인

3. RSYNC 설치 및 활용

RSYNC는 KISA에서 제공하는 스팸리스트를 다운받기 위하여 사용하는 프로그램이며, 다음은 RSYNC 설치와 활용법을 설명합니다.

KISA에 회원가입 후 등록한 서버에서만 RSYNC를 통하여 스팸리스트를 다운로드 할 수 있습니다.

3.1. RSYNC 설치

wget 명령어를 사용하여 rsync 공식 배포 사이트에서 rsync 프로그램을 다운로드하거나, 홈페이지에서 받을 수 있습니다.

```
# cd /home/user/
# wget http://www.samba.org/ftp/rsync/rsync-3.0.6.tar.gz
--14:25:48--  http://www.samba.org/ftp/rsync/rsync-3.0.6.tar.gz
Resolving www.samba.org... 216.83.154.106
Connecting to www.samba.org|216.83.154.106|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 778927 (761K) [application/x-gzip]
Saving to: `rsync-3.0.6.tar.gz'
100%[================================>] 778,927       463K/s    in 1.6s
14:25:52 (463 KB/s) - `rsync-3.0.6.tar.gz' saved [778927/778927]
```

[그림3-8] wget을 사용하여 rsync 프로그램을 다운로드

아래와 같이 gunzip, tar 명령어를 이용하여 파일 압축을 해제하고, make 명령어를 통하여 소스 코드를 컴파일 합니다.

```
# cd /home/user/
# gunzip rsync-3.0.6.tar.gz
# tar xvf rsync-3.0.6.tar
# cd /home/user/rsync/
# ./configure
# make
# make install
```

[그림3-9] 파일 압축 해제

3.2. RSYNC 다운로드 테스트

o RSYNC 실행

다음과 같이 명령어를 사용하여 스팸리스트(RBL)파일을 다운로드하며, 성공할 경우에는 아래와 같은 메시지가 나타납니다.

```
#cd /download
#/usr/local/bin/rsync -avz www.kisarbl.or.kr::spamlist /download
receiving file list ... done
./
spamlist1.txt
spamlist2.txt
spamlist3.txt

sent 153 bytes  received 1990046 bytes  265359.87 bytes/sec
total size is 18021047  speedup is 9.05
```

[그림3-10] spamlist 다운로드 성공 결과

실시간 스팸차단리스트(RBL) 홈페이지에서 회원 가입하여 서버 정보를 입력하지 않았다면, 아래와 같이 오류메시지가 나타나며 2.1을 참고하여 다시 다운로드 테스트를 진행 합니다.

```
#/usr/local/bin/rsync -avz www.kisarbl.or.kr::spamlist /download
@ERROR: access denied to spamlist from unknown (2.3.4.5)
rsync error: error starting client-server protocol (code 5) at main.c(1503)
[receiver=3.0.6]
```

[그림3-11] spamlist 다운로드 에러 메시지

스팸리스트를 정상적으로 다운로드 하였다면, 다음과 같이 다운로드된 스팸리스트를 확인합니다.

```
# cd /download
# ls -al spamlist*
-rw-r--r-- 1 1003 wheel 3019047  7월 22 20:07 spamlist1.txt
-rw-r--r-- 1 1003 wheel 1379735  7월 22 20:07 spamlist2.txt
-rw-r--r-- 1 1003 wheel 1585802  7월 22 20:07 spamlist3.txt
```

[그림3-12] spamlist 파일의 정보를 조회

다음과 같이 다운로드한 스팸리스트 파일 내용을 확인할 수 있습니다.

```
# more spamlist3.txt
<spamlist 파일의 내용 중에서>
:127.0.0.2
123.123.124.2 'www.kisarbl.or.kr'
123.123.123.0/24 'www.kisarbl.or.kr'
234.234.234.0/24 'www.kisarbl.or.kr'
```

[그림3-13] 스팸리스트 파일 내용 확인

spamlist 파일의 내용은 일반적인 RBL 파일의 형태와 동일하며, 좌측에는 개별 IP 또는 대역이 명시되고, 우측은(공백구분) 'www.kisarbl.or.kr' 등과 같이 RBL을 제공하는 사이트의 주소가 표기 됩니다.

o 스팸리스트 다운로드(crontab 이용)

다음은 유닉스 시스템에 크론텝(crontab)을 이용한 다운로드 스크립트를 설정하는 방법을 설명합니다.

실시간 스팸차단리스트(RBL)는 매시간 스팸리스트가 갱신되므로 crontab을 이용하여 업데이트된 스팸리스트를 다운로드하여 반영을 해야 합니다. 제때 스팸리스트를 반영하지 않아 스팸리스트에서 제외된 IP가 차단되는 경우가 발생할 수 있습니다.

아래와 같이 crontab 편집 모드로 들어간 후 rsync 다운로드 명령어를 삽입합니다.

```
# crontab -e
00 * * * * /usr/local/bin/rsync -avz www.kisarbl.or.kr::spamlist /download
```

[그림3-14] crontab 설정

매시간 정각 rsync 명령어가 실행되어 지정한 경로에 스팸리스트가 다운로드 됩니다.

4. RBLDNSD 설치

o RBLDNSD 란?

유닉스용 DNS 데몬으로 일반적으로 알고 있는 네임서버(DNS)와 작동 원리는 같으며, 스팸메일 차단 전용으로 RBL DNS 데몬을 메일 서버에 설치하여 사용합니다.

RBLDNSD 이용은 일일 메일 수신량이 10만 통 이상인 경우 직접 설치하는 것을 권장하며, 스팸리스트를 자신의 정책에 맞게 선택하거나 수정하여 사용할 수 있습니다.

4.1. RBLDNSD 다운로드 및 설치

배포 사이트를 직접 방문하거나, 아래와 같이 wget 명령어를 이용하여 최신 버전의 RBLDNSD 프로그램을 다운로드 합니다.※

배포 사이트 : http://www.corpit.ru/mjt/rbldnsd.html
https://www.kisarbl.or.kr

```
# cd /home/user/
# wget http://www.corpit.ru/mjt/rbldnsd/rbldnsd_0.996b.tar.gz
--15:17:07--  http://www.corpit.ru/mjt/rbldnsd/rbldnsd_0.996b.tar.gz
Resolving www.corpit.ru... 81.13.33.159
Connecting to www.corpit.ru|81.13.33.159|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 113128 (110K) [application/x-gzip]
Saving to: `rbldnsd_0.996b.tar.gz'

100%[==============================>] 113,128       70.7K/s    in 1.6s

15:17:11 (70.7 KB/s) - `rbldnsd_0.996b.tar.gz' saved [113128/113128]
```

[그림3-15] wget을 사용하여 RBLDNSD 프로그램을 다운로드

다음 같이 다운로드한 프로그램을 압축 해제하고 소스코드를 컴파일 하면 rbldnsd 실행파일이 생성됩니다.

```
# cd /home/user/
# gunzip rbldnsd_0.996b.tar.gz
# tar xvf rbldnsd_0.996b.tar
# cd /home/user/rbldnsd-0.996b/
# ./configure
# make
```

[그림3-16] RBLDNSD 설치

4.2. RBLDNSD 실행

아래와 같이 명령어를 이용하여 rbldnsd 데몬을 실행 합니다.

```
# cd /home/user/rbldnsd-0.996b/
# ./rbldnsd -b 127.0.0.1/53 -p /tmp/rbldnsd.pid -l /tmp/rbldnsd.log \
  kisarbl:ip4set:/download/spamlist1.txt
```

[그림3-17] RBLDNSD 실행 명령어

※ "ps -ef |grep rbldnsd"검색 후 kill -9 PID 통하여 RBLDNSD 실행 중지

RBLDNSD 실행 과정에서 아래와 같은 에러 메시지가 나타나는 경우에는 'rbldns' 유저를 생성하고 다시 실행합니다.

```
rbldnsd: unknown user `rbldns'
# useradd rbldns
```

[그림3-18] rbldns 유저 생성

< RBLDNSD 실행 옵션 설명 >

-b : 서버 IP와 포트 지정
※ 동일 머신에 DNS와 함께 운영하면 다른 포트(예: 5353)를 사용합니다.
-p : RBLDNSD 프로세스 PID 지정
-l : 로그파일을 지정
-h : rbldnsd 도움말

kisarbl:ip4set:/download/spamlist1.txt
RBL베이스 주소와 IPv4를 사용, 스팸리스트 파일을 지정합니다.

※ RBL 베이스란 RBL 룩업을 수행하는 기본 주소이며, KISA에서 제공하는 기본 RBL 베이스는 'spamlist.or.kr'입니다. 로컬에서 RBLDNSD를 사용할 경우 임의 문자(예: kisarbl)를 사용하여도 무방하지만, 메일서버 설정 값과 같은 이름으로 지정해줘야 합니다. (4.4 참고)

RBLDNSD가 정상적으로 실행된 경우에는 아래와 같은 메시지가 나타납니다.

```
rbldnsd: listening on 127.0.0.1/53
rbldnsd: ip4set:/download/spamlist1.txt: 20090715 051918:
e32/24/16/8=2/132/0/0
rbldnsd: zones reloaded, time 0.0e/0.0u sec
rbldnsd: rbldnsd version 0.996b (29 Mar 2008) started (1 socket(s), 1 zone(s))
```

[그림3-19] RBLDNSD 정상 실행 결과

메일 MTA가 제일 먼저 RBLDNSD를 참조하도록 resolv.conf 파일을 편집합니다. 상단에 RBLDNSD 데몬 실행 시 입력한 IP주소를 추가합니다.

```
# vi /etc/resolv.conf
nameserver      127.0.0.1 or 서버 IP (RBLDNS 데몬 실행시 지정한 IP)
nameserver      (기존 DNS IP)
```

[그림3-20] resolv.conf 파일 RBLDNSD 네임서버 IP 추가

4.3. RBL lookup 테스트

RBLDNSD는 일반적인 네임서버(DNS)와 달리 특정 IP의 RBL 리스트 등재 여부만을 확인하기 때문에 RBL lookup만 지원합니다.

RBL lookup이란, 기존의 DNS 표준에 크게 어긋나지 않게 약간

변형된 형태로 DNS 질의를 합니다. 일반적인 DNS lookup은 'nslookup hostname.domain.com'과 같은 형식으로 질의를 하지만, RBLDNSD에서는 IP주소를 이용, 역순으로 질의 합니다.

RBLDNSD가 정상 동작하는지 확인하기 위하여 샘플 spamlist1.txt를 생성하고, RBLDNSD 실행 방법을 참고하여 다시 실행합니다.

```
#vi spamlist1.txt
:127.0.0.2 (DNS A 레코드 반환 값 : 127.0.0.2)
1.2.3.4 'www.kisarbl.or.kr'
211.212.211.33 'www.kisarbl.or.kr'
```

[그림3-21] 샘플 IP 입력

다음은 nslookup 명령어를 이용하여 정상적으로 응답하는지 확인합니다. 질의하고자 하는 IP가 1.2.3.4이면, 역순으로 4.3.2.1과 RBLDNSD 실행시 지정 했던 RBL 베이스 'kisarbl'을 입력합니다.

아래와 같이 나타나면 스팸리스트에 등재되어 있는 상태를 의미하며 응답 값이 없으면 등재 되어 있지 않은 상태를 의미합니다.

```
# nslookup 4.3.2.1.kisarbl (질의하려는 IP를 역순으로 입력한 후, RBL 베이스를 입력)
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   4.3.2.1.kisarbl
Address: 127.0.0.2 (127.0.0.2 리턴  1.2.3.4 IP가 RBL에 등재 되었음을 의미)
```

[그림3-22] nslookup 명령어로 RBL lookup 실행

다음은 dig 명령어를 사용하여 확인합니다.

```
# dig 4.3.2.1.kisarbl
; <<>> DiG 9.3.4-P1 <<>> 4.3.2.1.kisarbl
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 784
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;4.3.2.1.kisarbl.                IN      A

;; ANSWER SECTION:
4.3.2.1.kisarbl.        2100    IN      A       127.0.0.2
(A 레코드 127.0.0.2 리턴 1.2.3.4 IP가 RBL에 등재 되었음을 의미)
```

[그림3-23] dig 명령어로 RBL lookup 실행

4.4. 메일 서버 (qmail 1.03) 설정 변경

qmail에서 RBL 참조서비스를 사용하기 위해서는 rblsmtpd 프로그램이 설치되어 있어야 합니다.

rblsmtpd는 ucspi-tcp 패키지에 포함되어 있으므로, 아래와 같이 wget 명령어를 이용하여 최신 버전의 ucspi-tcp 패키지를 다운로드합니다.

```
# cd /home/
# wget http://cr.yp.to/ucspi-tcp/ucspi-tcp-0.88.tar.gz
--15:03:09--  http://cr.yp.to/ucspi-tcp/ucspi-tcp-0.88.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: 53019 (52K) [application/x-gzip]
Saving to: `ucspi-tcp-0.88.tar.gz'

100%[======================>] 53,019        65.9K/s    in 0.8s

15:03:11 (65.9 KB/s) - `ucspi-tcp-0.88.tar.gz' saved [53019/53019]
```

[그림3-24] wget 명령어를 사용하여 ucspi-tcp 패키지 다운로드

다음 [그림3-25]와 같이 다운로드한 ucspi-tcp 패키지를 압축 해제하고 소스코드를 컴파일 합니다.

```
# gunzip ucspi-tcp-0.88.tar.gz
# tar xvf ucspi-tcp-0.88.tar
# cd ucspi-tcp-0.88
# make
-------------------- 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
```

[그림3-25] 파일 압축 해제 및 소스코드 컴파일

다음 [그림3-26]과 같이 ucspi-tcp 패키지를 설치합니다.

```
# make setup check
./install
./instcheck
```

[그림3-26] ucspi-tcp 설치

다음 [그림3-27]과 같이 rblsmtpd가 정상적으로 설치되었는지 확인합니다.

```
# ls -al /usr/local/bin/rblsmtpd
-rwxr-xr-x    1 root     bin         34616 2009년  1월  1일 /usr/local/bin/rblsmtpd
```

[그림3-27] rblsmtpd 설치 확인

다음 [그림3-28]과 같이 qmail 설치 과정에서 생성한 run 파일을 편집합니다.

'-b' 옵션은 IP주소가 RBL에 등재되어 있는 경우 '553'에러를 표시하며,

'-r' 옵션 다음에는 RBL-BLOCK을 위한 RBL 베이스를 지정합니다.

RBL 베이스는 RBLDNSD 실행 시 지정한 'kisarbl'을 입력합니다. 다른 RBL을 함께 참조할 경우에는 '-r' 옵션 다음에 해당 RBL 베이스를 입력합니다.

(Ex. -r bl.spamcop.net, -r cbl.abuseat.net, -r zen.spamhaus.org, ...)

```
# cd /var/qmail/supervise/qmail-smtpd
# vi run
<run 파일 내용 중에서>
#!/bin/sh
exec /usr/local/bin/softlimit -m 3000000 \
/usr/local/bin/tcpserver -v -p -x \
/etc/tcp.smtp.cdb -u 102 -g 101 0 25 \
/usr/local/bin/rblsmtpd -b -r kisarbl -r bl.spamcop.net \    (추가된 부분)
/var/qmail/bin/qmail-smtpd 2>&1
```

[그림3-28] run 파일에 rblsmtpd 설정

다음과 같이 qmail 데몬을 재시작 한 후, 서비스가 정상적으로 실행 중인지와 25번 포트가 정상적으로 열려있는지 확인합니다.

```
# /etc/init.d/qmaild stop   (중지)
# /etc/init.d/qmaild start  (시작)
# ps -ef | grep qmail       (qmail 프로세스 확인)
# netstat -an | grep 25     (포트가 열려있는지 확인)
```

[그림3-29] qmail 재시작 및 프로세스 확인

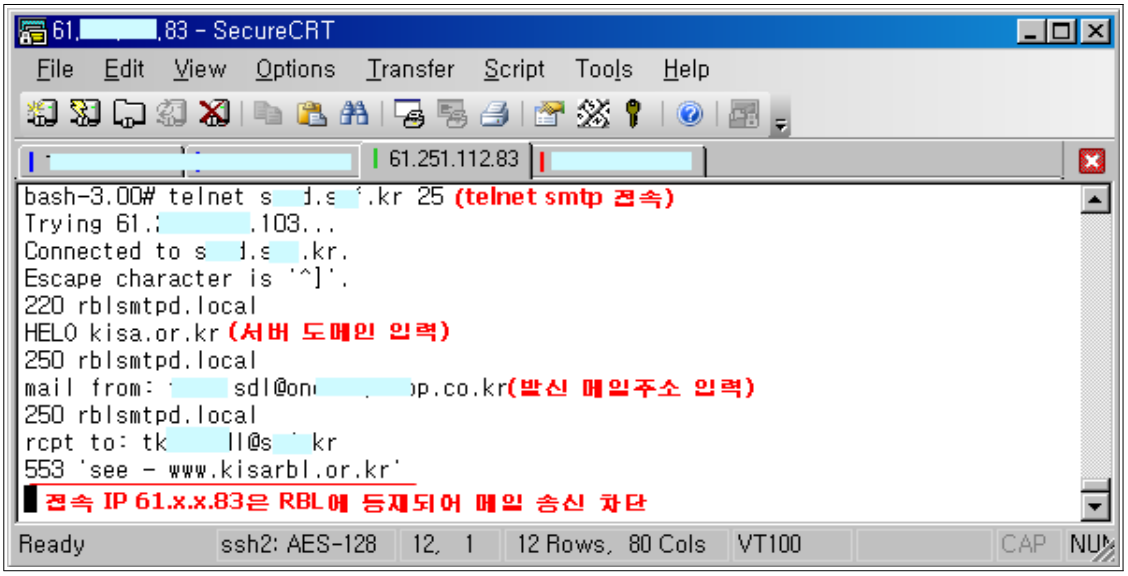
4.5. 스팸 차단 테스트

지금까지 RBLDNSD를 이용하여 스팸 차단 방법을 설명하였습니다. 다음은 실제 도메인과, 공인 IP를 이용하여 스팸차단 테스트 내용을 보여 줍니다.

RBLDNSD가 설치된 서버에 spamlist1.txt에 공인 IP를 추가하고, 공인 IP서버에서 telnet 명령어를 이용하여 RBLDNSD가 적용된 메일서버에 메일 송신 하였으나 차단된 것을 확인 할 수 있습니다.

```
#vi spamlist1.txt
:127.0.0.2
61.x.x.83 'see - www.kisarbl.or.kr' (공인 IP)
```

[그림3-30] 스팸리스트에 공인IP 등록



[그림3-31] telnet 통한 메일 발송 테스트

위 테스트결과 RBLDNSD는 정상적으로 spamlist1.txt를 참고하여 스팸IP를 차단하고 있음을 확인 할 수 있습니다.

다음은 qmail 로그에서 아래와 같이 차단 내역을 확인 할 수 있습니다.

```
# tail -f /var/log/syslog
<syslog 내용 중에서>
tcpserver: pid 29073 from 61.x.x.83
tcpserver: ok 29073 :61.x.x.103:25 :61.x.x.83::33376
rblsmtpd: 61.x.x.83 pid 29073: 553 'see - www.kisarbl.or.kr'
tcpserver: end 29073 status 0
tcpserver: status: 0/40
```

[그림3-32] qmail 스팸로그 차단 화면

※ OS 및 메일서버 로그 레벨, 설정에 따라 로그 디렉터리 위치와 내용이 다르게 보일 수 있습니다.