실시간 스팸차단리스트(RBL)
이용 방법

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

Exchange Server 2007 사용 설명서

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)

1. 메일 서버 (Exchange Server 2007) 설정 변경

RBL 참조 기능을 사용하기 위해서는 'Edge 전송 서버' 또는 'Hub 전송 서버'가 설치되어 있어야 합니다. 본 매뉴얼에서는 'Hub 전송 서버'만 설치하였습니다.

※ Edge 전송서버 : http://technet.microsoft.com/ko-kr/library/bb124701.aspx

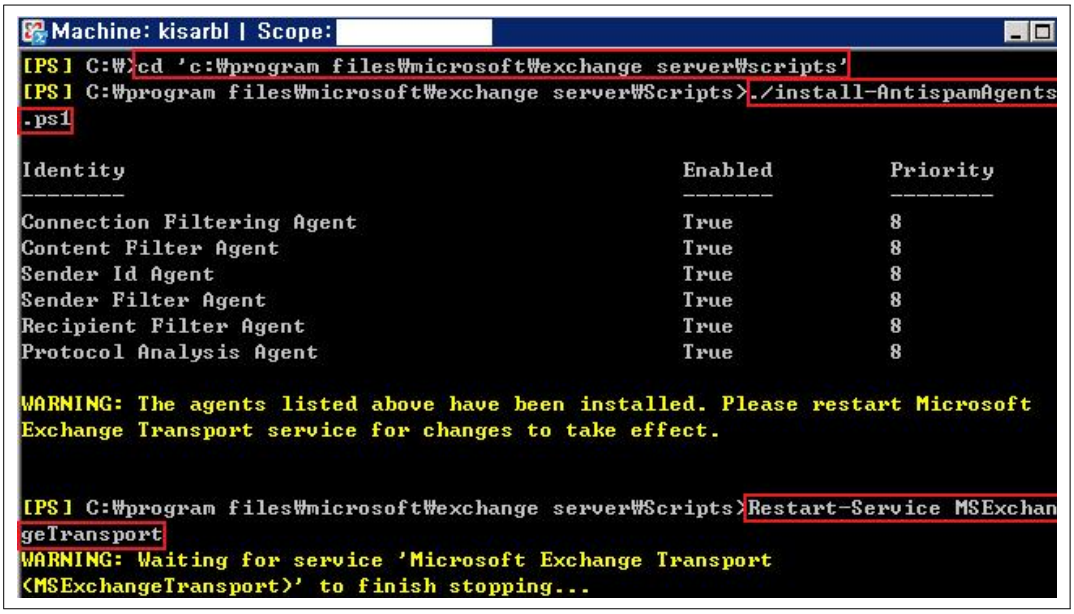
※ Hub 전송서버 : http://technet.microsoft.com/ko-kr/library/bb123494.aspx

Anti-spam 기능을 사용하기 위하여, '시작' > '프로그램' > 'Microsoft Exchange Server 2007' > 'Exchange 관리 셸'을 실행한 후, 아래와 같이 AntispamAgents를 설치합니다.

출처 : http://technet.microsoft.com/en-us/library/bb201691.aspx

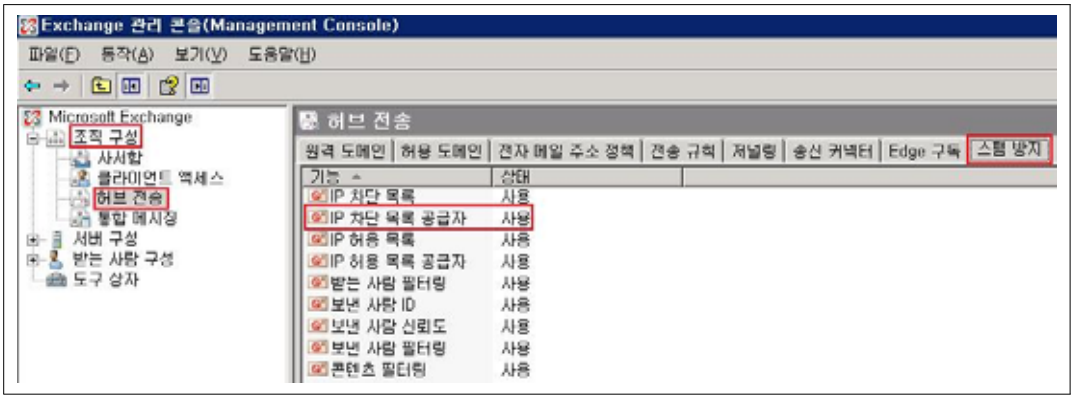
```
> cd 'c:\program files\microsoft\exchange server\scripts'    (디렉터리 이동)
> ./install-AntispamAgents.ps1                              (설치)
> Restart-Service MSExchangeTransport                       (서비스 재시작)
```

[그림2-1] AntispamAgents 설치



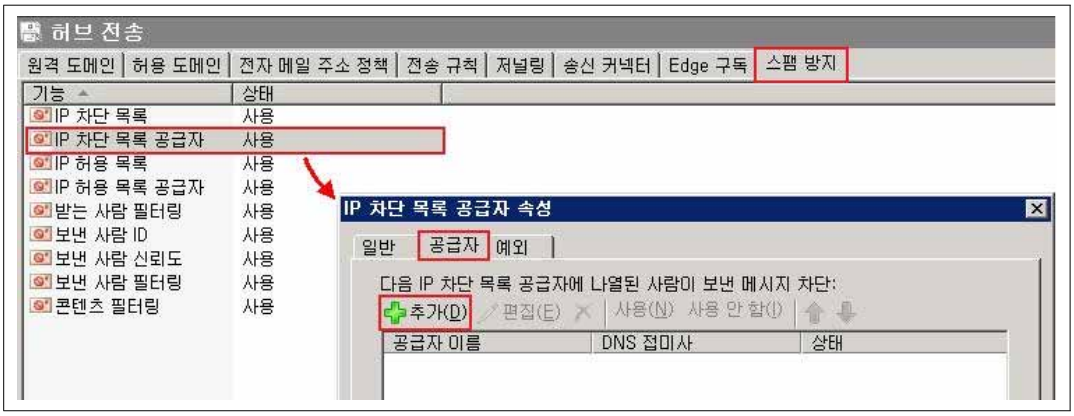
[그림2-2] AntispamAgents 설치 결과

AntispamAgents가 설치되면, 아래의 [그림2-3]과 같이 'Exchange 관리 콘솔'의 '조직 구성' > '허브 전송' 메뉴에 '스팸 방지' 탭이 추가됩니다.



[그림2-3] '스팸 방지' 탭 활성화

'IP 차단 목록 공급자' 항목을 더블클릭하면 'IP 차단 목록 공급자 속성' 대화상자가 나타납니다. '공급자' 탭 선택 후 '추가' 버튼을 클릭하면 'IP 차단 목록 공급자 추가' 대화상자가 나타납니다.



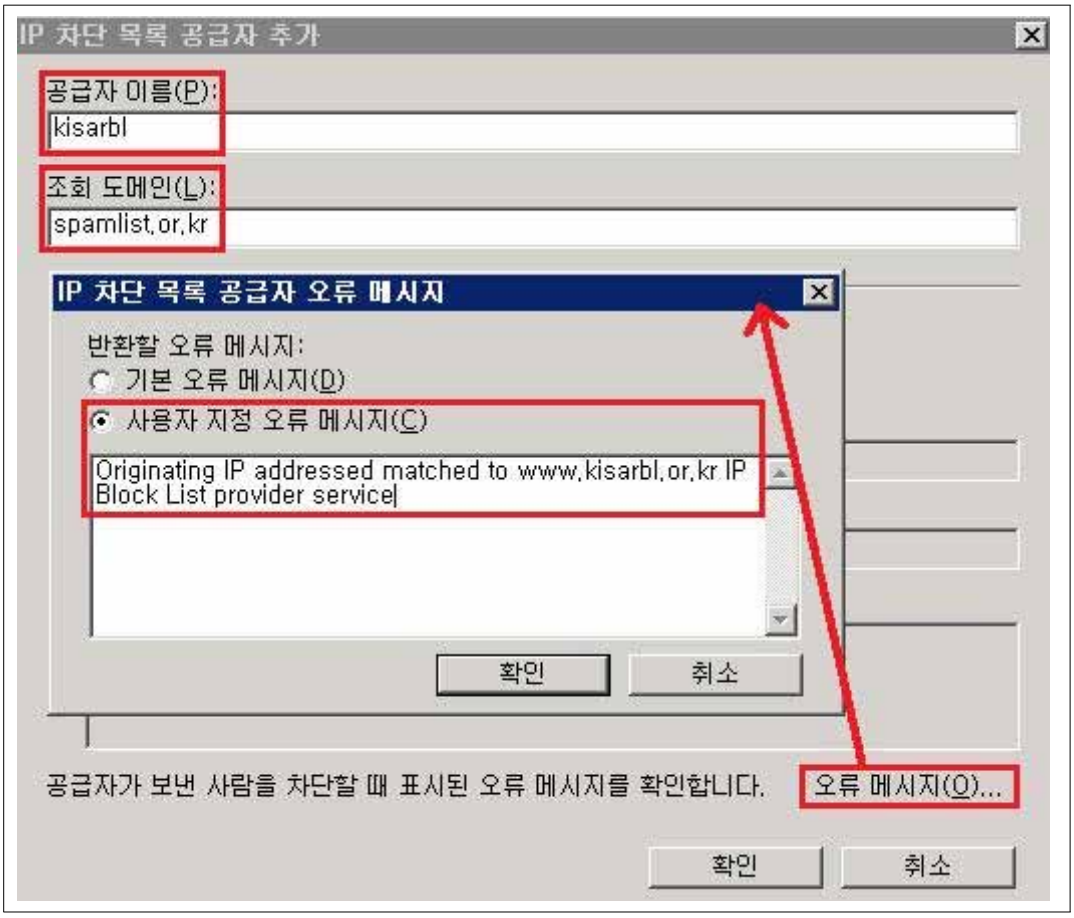
[그림2-4] Add-IPBlockListProvider 실행 (GUI)

다음과 같이 IP 차단 목록 공급자 구성을 추가합니다. [그림2-5]와 같이 GUI 메뉴에서 설정하거나 [그림2-6]과 같이 명령어 모드에서 설정하는 것을 선택할 수 있습니다.

o GUI 설정

아래의 [그림2-5]와 같이 'IP 차단 목록 공급자 추가' 대화상자에서 '공급자 이름'을 입력합니다. 임의로 입력 가능하며, 여기서는 'kisarbl'을 입력하였습니다. 조회 도메인은 'spamlist.or.kr'을 지정하여 실시간 스팸차단리스트(RBL)를 참조할 수 있도록 합니다.

'오류 메시지'를 클릭하면 'IP 차단 목록 공급자 오류 메시지' 대화상자가 나타나며 '사용자 지정 오류 메시지'를 선택하여 SMTP 연결 실패 시 표시할 메시지를 입력합니다.



[그림2-5] Add-IPBlockListProvider 실행 (GUI)

o 명령어 모드 설정

아래의 [그림2-6]과 같이 공급자 이름(name)은 'kisarbl'을 입력하고, 조회 도메인(LookupDomain)은 'spamlist.or.kr'을 지정하여 실시간 스팸차단리스트(RBL)를 참조할 수 있도록 합니다. 사용자 지정 오류 메시지(RejectionResponse)는 SMTP 연결 실패 시 표시할 메시지를 입력합니다.

http://technet.microsoft.com/ko-kr/library/bb124358.aspx
> *Add-IPBlockListProvider -Name:kisarbl -LookupDomain:spamlist.or.kr -RejectionResponse "Originating IP addressed matched to www.kisarbl.or.kr IP Block List provider service"*

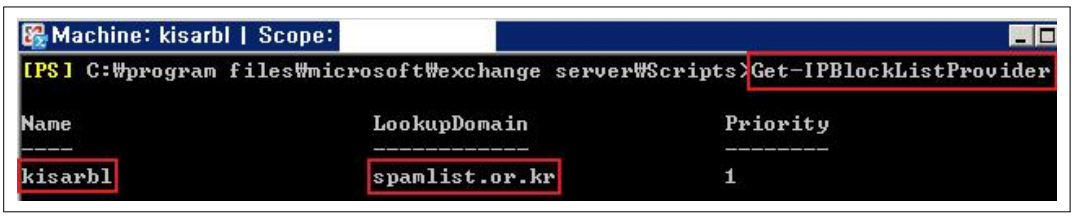
[그림2-6] Add-IPBlockListProvider 실행

[그림2-7] Add-IPBlockListProvider 실행 결과

다음과 같이 IP 차단 목록 공급자의 구성을 확인할 수 있습니다.

출처 : http://technet.microsoft.com/ko-kr/library/aa996590.aspx
> *Get-IPBlockListProvider*

[그림2-8] Get-IPBlockListProvider 실행

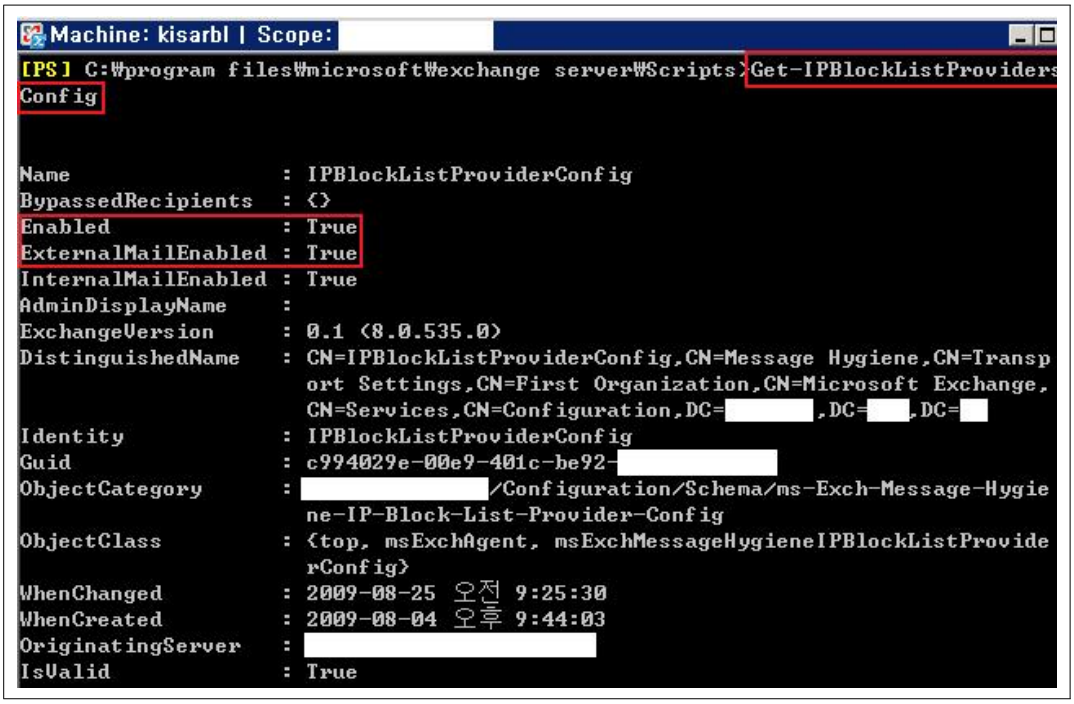


[그림2-9] Get-IPBlockListProvider 실행 결과

아래의 [그림2-10], [그림2-11]과 같이 IP 차단 목록 공급자에 대한 구성 정보를 확인할 수 있습니다.

출처 : http://technet.microsoft.com/ko-kr/library/bb123884.aspx
> *Get-IPBlockListProvidersConfig*

[그림2-10] Get-IPBlockListProvidersConfig 실행



[그림2-11] Get-IPBlockListProvidersConfig 실행 결과

연결 필터링 기능(실시간 스팸차단리스트(RBL) 참조)을 적용하기 위해서는 IPBlockListProvidersConfig의 'Enabled'과 'ExternalMailEnabled'의 매개 변수가 '$true'로 설정되어 있어야 하며, 만약 '$false'로 설정되어 있는 경우에는 다음과 같이 설정을 변경합니다.

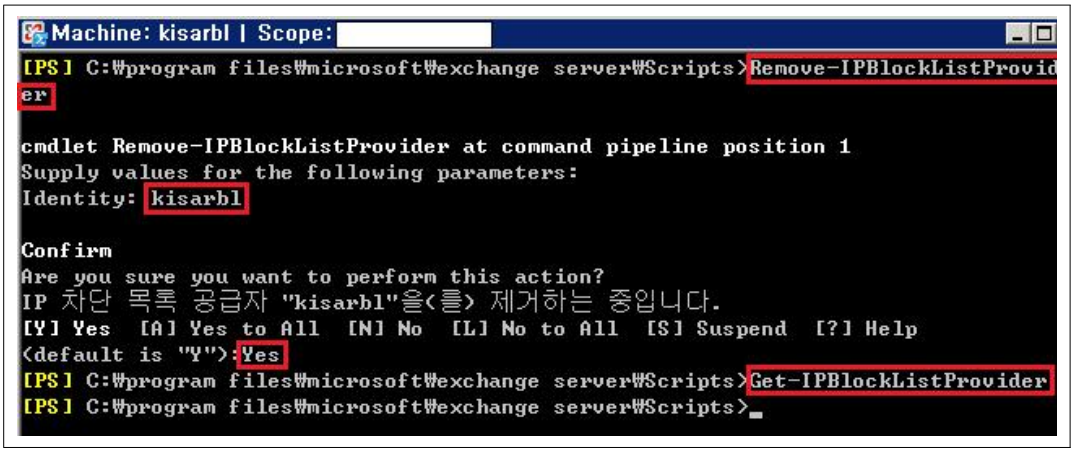
출처 : http://technet.microsoft.com/ko-kr/library/aa998543.aspx
> *Set-IPBlockListProvidersConfig -Enabled:$true -ExternalMailEnabled:$true*

[그림2-12] IPBlockListProvidersConfig 설정

다음과 같이 특정 IP 차단 목록 공급자 구성에 대한 구성 정보를 제거할 수 있습니다.

출처 : http://technet.microsoft.com/ko-kr/library/bb123768.aspx
> *Remove-IPBlockListProvider -Identity kisarbl*

[그림2-13] Remove-IPBlockListProvider 실행



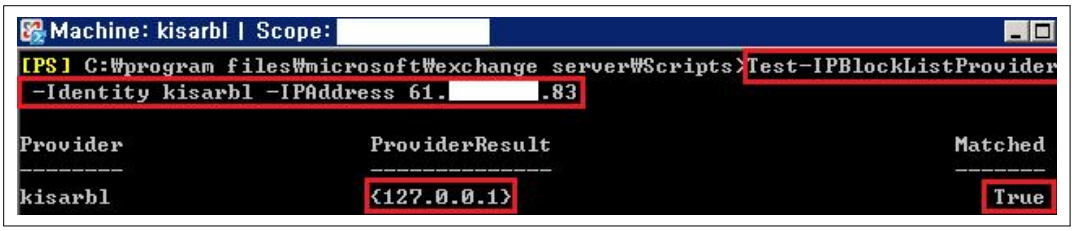
[그림2-14] Remove-IPBlockListProvider 실행 결과

2. 스팸 차단 테스트

다음과 같이 특정 IP 차단 목록 공급자 구성에 대한 구성을 테스트 할 수 있습니다.

출처 : http://technet.microsoft.com/ko-kr/library/bb124998.aspx
> *Test-IPBlockListProvider -Identity kisarbl -IPAddress 61.x.x.83*

[그림2-15] Test-IPBlockListProvider 실행



[그림2-16] Test-IPBlockListProvider 실행 결과

테스트 결과, 위의 [그림2-16]과 같이 61.x.x.83 IP가 IP 차단 목록 공급자의 IP 주소와 일치(True)하는 것을 확인할 수 있습니다.

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.

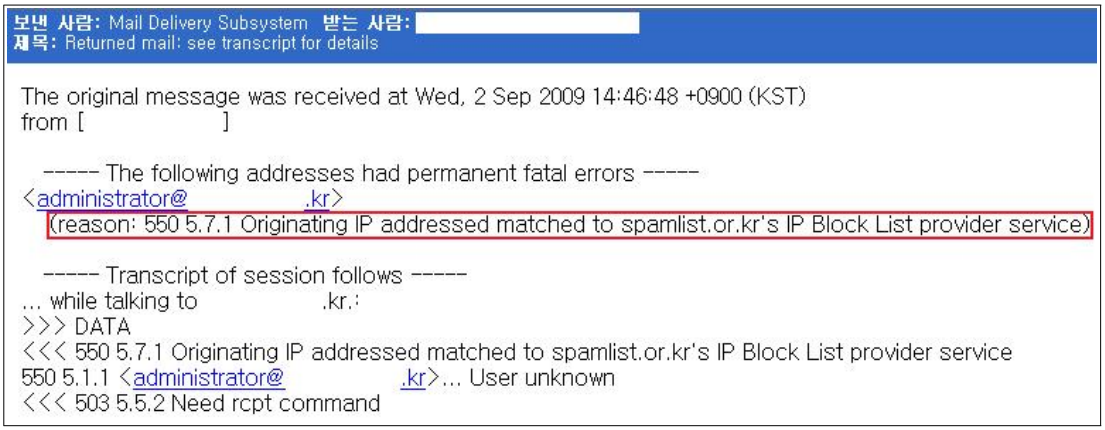
C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\AgentLog
<Log 파일 내용 중에서>
#Software: Microsoft Exchange Server
#Version: 8.0.0.0
#Log-type: Agent Log
#Date: 2009-09-02T05:09:25.839Z
#Fields:
Timestamp,SessionId,LocalEndpoint,RemoteEndpoint,EnteredOrgFromIP,MessageId,P1From Address,P2FromAddresses,Recipient,NumRecipients,Agent,Event,Action,SmtpResponse,Reason,ReasonData
2009-09-02T06:32:33.480Z,08CBF331BA1691C5,61.x.x.102:25,61.x.x.83:35609,61.x.x.83,,sender@example.com,,receiver@example1.com,1,Connection Filtering Agent,OnRcptCommand,RejectCommand,550 5.7.1 Originating IP addressed matched to www.kisarbl.or.kr's IP Block List provider service,BlockListProvider,kisarbl

[그림2-17] Agent Log 파일 확인

C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\ProtocolLog\SmtpReceive
<Log 파일 내용 중에서>
#Software: Microsoft Exchange Server
#Version: 8.0.0.0
#Log-type: SMTP Receive Protocol Log
#Date: 2009-09-02T05:01:54.542Z
#Fields:
date-time,connector-id,session-id,sequence-number,local-endpoint,remote-endpoint,event,data,context
<중략>
2009-09-02T06:32:38.495Z,KISARBL\SMTP 수신 커넥터,08CBF331BA1691C5,17,61.x.x.102:25,61.x.x.83:35609,>,550 5.7.1 Originating IP addressed matched to www.kisarbl.or.kr's IP Block List provider service,

[그림2-18] SmtpReceive Log 파일 확인

아래는 스팸리스트에 등록된 IP에서 메일을 발송 하였을때 반송된 메일이며, 실시간 스팸차단리스트(RBL)에 의하여 차단된 것을 확인 할 수 있습니다.



[그림2-19] 반송 메일