

스팸 릴레이 기술적 예방대책

김상철

Kims@certcc.or.kr

kims@kisa.or.kr

한국정보보호진흥원

배경

- 스팸, 웜바이러스, 해킹 사례가 증가하여 주변 국가를 보안을 위협
 - 초·중·고교, PC방 중소기업등이 정보보호 인식부족 과 투자/관리 소홀
- 초고속국가망의 위신 뿐만 아니라 국가 전체의 이미지를 실추
- 설정 오류의 프락시 서버와 메일 서버
 - 잘못 설정된 프락시서버, 메일서버를 운영하면서 스팸메일을 중계하여 기관전체가 스팸머로 오인

배경

- 스팸 메일로 인한 민원이 증가하는 가운데, 초중고 메일서버의 중계기능을 악용하는 스팸 릴레이에 대한 외국의 항의 폭주
 - 미국 Anti-Spam 단체의 Jean Hunter
 - 미국 monkeys.com과 덴마크 Top point사 등
- 일부 국외 기관에서는 한국으로부터 전송되는 모든 메일을 차단하겠다고 경고

현황

□ 학교 및 릴레이 서버의 현황

- 초·중·고교는 유지/구입비용이 상대적으로 방화벽보다 저렴한 프락시 서버(리눅스 기반)를 도입
- 중소기업은 관리자의 관리설정 부재
 - 잘못 설정된 프락시서버, 메일서버를 운영하면서 스팸메일을 중계

□ 해킹바이러스상담지원센터 릴레이점검서비스

- 5월 부터 6월까지의 웹기반의 무료 스팸릴레이 원격 점검서비스
 - 17191건의 점검서비스 중 1418개의 서버 스팸릴레이 허용
 - 8.2%

원인분석

- 프락시 서버 설정 오류를 이용한 IP 도용
- 메일 서버의 구성 및 설정 오류로 인한 스팸메일 중계
- 관리자의 전문성 부족
- 지도 기관/유지보수업체의 인식 및 인력 부족
- 서버 애플리케이션 개발 업체/ISP의 능동적인 보안강화 활동

유관기관 대응현황

(6/28일 기준)

구분	대상 서버수	해결		주체	비고
		서버수	진도율		
Proxy 서버	4,586(82.4%)	4,577	99.8%	업체	현장 : 487개
방화벽 서버	603(10.8%)	275	45.6%	업체	
KISA 원격/현장점검	376(6.8%)	342	91.0%	KISA	현장 : 89개 원격 : 253개
계	5,565(100%)	5,194	93.3%		

※ 방화벽서버와 Proxy서버가 중복될 수 있음

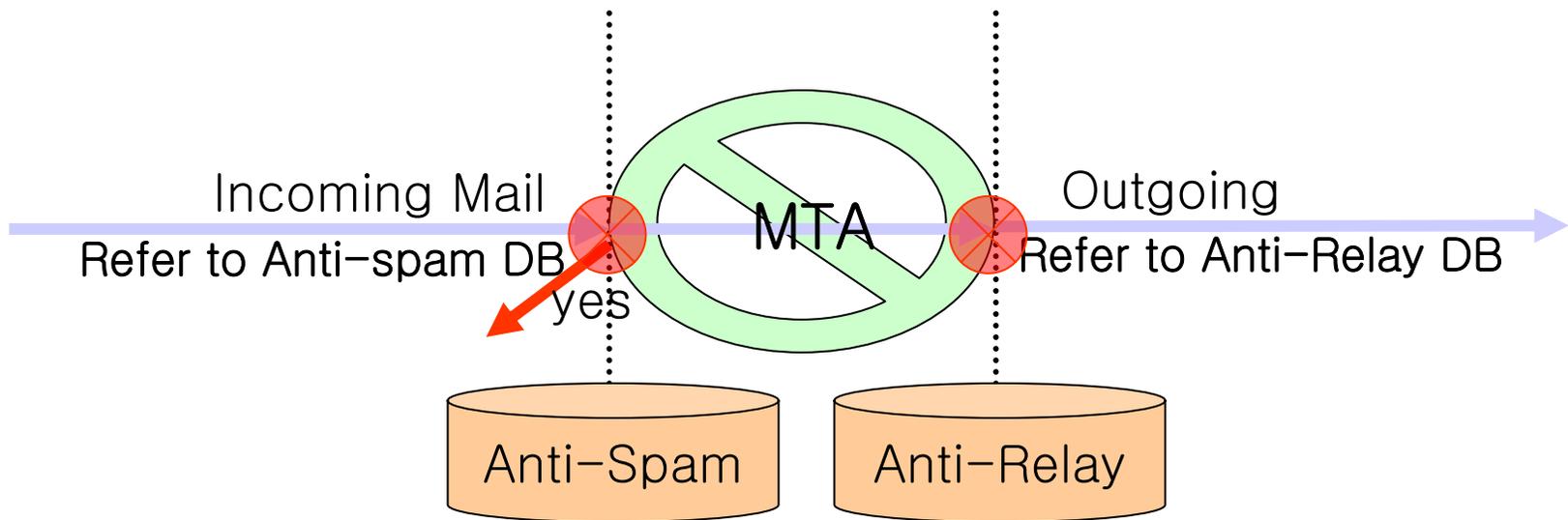
유관기관 대응현황

(6월 28일 기준)

구분						프락시서버 업체					CERT 사고접수			합계
	경 기	강 원	충 북	울 산	제 주						몽 키 닷 컴	탑 포 인 트	기 타	
갯수	687	558	886	262	386	2,243	1,172	489	357	156	975	180	49	8,400
메일 서버 릴레이	1	0	2	0	0	2	1	1	0	0	3	0	0	10
프락시서버 Open	2	0	4	0	0	3	1	0	2	0	12	0	0	24
계	3	0	6	0	0	5	2	1	2	0	15	0	0	34

스팸 릴레이 Basic Algorithm

☐ 메일서버의 스팸 릴레이



스팸릴레이 점검방법

- 메일 서버의 스팸릴레이 점검
 - 수동점검
 - 제3자 서비스 점검
 - 보안취약성 점검도구를 이용한 점검

스팸릴레이 점검(수동점검)

- 내부 도메인 및 내부 IP주소가 아닌 곳에서의 스팸릴레이를 점검

```
[tomcat:root]:/ > telnet 172.16.4.140 25
Trying 172.16.4.140...
Connected to 172.16.4.140.
Escape character is '^]'.
<<< 220 certlinux.certcc.or.kr ESMTP Sendmail 8.11.0/8.11.0; Sun, 18 Feb 2001 23:54:18 +0900
>>> helo kisa
<<< 250 certlinux.certcc.or.kr Hello tomcat.cyber118.or.kr [211.252.150.7], pleased to meet you
>>> mail from:<ksch@certlinux.certcc.or.kr>
<<< 250 2.1.0 <ksch@certlinux.certcc.or.kr>... Sender ok
>>> rcpt to:<ksch90@korea.com>
<<< 550 5.7.1 <ksch90@korea.com>... Relaying denied
>>> rset
<<< 250 2.0.0 Reset state
```

스팸릴레이 점검(제3자서비스)

스팸릴레이 점검서비스를 무료로 제공해주는 사이트를 활용

<http://www.certcc.or.kr/spamrelay.html>

<http://www.whchang.com/netprg/is-relay.pl>

메일서버의 스팸릴레이(SPAM Relay) 점검서비스

본 페이지는 메일서버가 스팸릴레이서버로 작동될 수 있는지를 웹상에서 점검해주며, 메일서버가 스팸릴레이서버로 작동되는 것을 예방하기 위하여 한국정보보호진흥원의 해킹바이러스상담지원센터에서 개발되었습니다.

메일서버의 스팸릴레이를 점검하기 위해서는 메일서버 담당자이름, E-Mail주소, 전화연락처, 점검하고자 하는 메일서버의 IP주소를 입력한 후에 점검시작 버튼을 클릭하면, 웹서버가 자동으로 스팸릴레이 여부를 점검해줍니다.

※ 주의 : EMWAC 메일 서버는 스팸릴레이 방지를 필터링하여 제거하므로 테스트시 릴레이를 허용한다고 나오지만 실제로는 허용하지 않습니다.

점검하는데 몇분정도 소요될 수 있으며, 접속하는 클라이언트 PC의 IP정보를 별도로 관리하고 있습니다. 메일서버의 스팸릴레이 점검기능으로만 사용해 주시기 바랍니다

담당자 이름

담당자 E-Mail주소

담당자 전화 연락처

점검대상 메일서버 IP 주소

스팸릴레이 점검 시작

점검한 후에 메일서버의 스팸릴레이가 허용되면, 외부 악의 사용자가 당신의 메일서버를 사용하여 스팸메일을 발송할 수 있기 때문에 반드시 스팸차단 설정을 해주어야 합니다. 스팸차단 설정관련해서는 다음의 문서를 참조하시기 바랍니다.

- 스팸릴레이 방지관련 업데이트 보안패치
- Sendmail 메일서버의 스팸릴레이 방지 설정 방법
- Window Exchange 메일서버의 스팸릴레이 방지 설정 방법
- 메일서버의 스팸릴레이 방지 설정 방법
- 메일서버의 스팸릴레이 시형방법 및 대응방법
- 메일필터링을 통한 E-Mail 보안
- Installation of Anti-spam Sendmail 8.9.3

파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(D) 도움말(H)

뒤로 앞으로 검색 즐겨찾기 목록보기

주소(D) <http://www.whchang.com/netprg/is-relay.pl> 이동 연결

메일중계기능 검사 (Checking Mail Relay)

STMP Server (to be checked) **점검**

주소

- 메일중계기능이 허용되어 있는 경우 귀하의 메일서버가 스팸메일발송자들에 의해 도용되고, 그로 인해 서버에 부하가 발생하거나, 또는 다른 ISP에 의해서 서비스가 차단되는 상황을 맞이하게 될 수 있습니다.
- 따라서 귀하의 메일서버에서 반드시 메일중계기능을 차단해 줄 것을 권고합니다.
- 관련자료는 <http://notice.inempire.com/svc-relay.html>를 참고하시기 바랍니다.
- 이 점검 프로그램이 정확하게 동작하지 않는다고 판단되는 경우 whchang@bora.net로 알려주시면 감사하겠습니다.

Updates

- Aug 31, 2001: InterScan 점검시 오류 수정
- June 13, 2001: Microsoft SMTP MAIL 와 NTMail Server 점검시 오류 수정
- June 12, 2001: IMS SMTP Receiver 점검시 오류 수정

Written by whchang@bora.net (1998.1.26)
Last updated at June 13, 2001

인터넷

스팸릴레이 점검(점검도구활용)

- 상용화된 취약성 점검도구나 공개용 취약성 점검도구 활용

The screenshot displays two windows from a security assessment tool. The left window shows a 'Manager Description' for a vulnerability identified as '5021 Sendmail Relaying Allowed'. The right window shows a terminal session where a user runs a script to test this vulnerability on two hosts.

Manager Description:

5021 Sendmail Relaying Allowed

Risk Factor: Low
Complexity: Low
Popularity: Popular
Impact: Accountability
Root Cause: Misconfiguration
Ease of Fix: Simple
Description: This module determines whether you gateway or relay. When used as a m... to "spammers" relaying mail through audience. For example, if an outside as being to "target%somedomain.co... could be re-transmitted to the target from your mail server.
Security Concerns: Allowing mail to be relayed through
 1. It increases the load on your mail... hundreds of thousands of messages... the victims mail server to relay the
 2. It insinuates that your mail server mail which was sent out.
 Neither of these are desirable, and pr... your mail servers from this type of a

Terminal Output:

```
[penguin:root]:/user1/ksch/school/itop> cat ip.txt
210.97.106.4
211.252.150.1
[penguin:root]:/user1/ksch/school/itop> spamrelay.pl
Host List File Name(동일 디렉토리의 IP주소나 도메인명을 포함하고 있는 파일명): ip.txt
HELO Domain(Helo 도메인명을 입력): KISA
Mail From: root@certcc.or.kr
Rcpt To: kims@certcc.or.kr
Log Session(동일 디렉토리의 log파일을 사용)
Log File [log]:
210.97.106.4# 8080
211.252.150.1# success relay

Finished Scanning. 1 out of 2 hosts will relay.

[penguin:root]:/user1/ksch/school/itop>
```

스팸릴레이설정방법

□ Sendmail

□ 8.9.0 이상의 버전 사용

□ Sendmail이 참조하는 Access DB사용

➤ **spam@hacker.com** **REJECT**

➤ **spammail.com** **REJECT**

➤ **useful.org** **OK**

➤ **172.16** **RELAY**

□ 스팸릴레이설정 참조 사이트

➤ http://www.certcc.or.kr/paper/tr2002/tr2002_04/sendmail_spam.htm

➤ <http://www.sendmail.org/tips/relaying.html>

➤ <http://www.sendmail.org/m4/anti-spam.html>

스팸 릴레이 설정 방법

□ Sendmail

```
[penguin:root]:/etc/mail> ls -al access*
-rw-r--r-- 1 root other 71 5월 3일 17:25 access

[penguin:root]:/etc/mail> cat access
spam@hacker.com REJECT
spammail.com REJECT
useful.org OK
172.16 RELAY

[penguin:root]:/etc/mail> makemap dbm /etc/mail/access < /etc/mail/access

[penguin:root]:/etc/mail> ls -al access*
-rw-r--r-- 1 root other 71 5월 3일 17:25 access
-rw-r--r-- 1 root other 0 5월 3일 17:27 access.dir
-rw-r--r-- 1 root other 024 5월 3일 17:27 access.pag

[penguin:root]:/etc/mail> cat access.pag
衆詳鳩픈
RELAY172.16OKuseful.orgREJECTspammail.comREJECTspam@hacker.com
```

스팸릴레이 설정방법

□ EXIM

- Download
 - ✓ <http://www.exim.org>
- 스팸릴레이 설정
 - ✓ <http://www.exim.org/howto/relay.html>

□ EMWAC

- DownLoad
 - ✓ <http://www.l7.net/cgi-bin/archives.cgi?template=archives&path=archives/emwac/server>
- **IMS**에 필터링 기능을 부여해주는 **SCMSFILTER**
 - ✓ <http://www.sica.com/freestuf/scsmfilt.htm>
- **Antirelay Plugin** 설치방법
 - ✓ <http://www.orca.bc.ca/win95/antirelay.zip>

스팸 릴레이 설정 방법

□ Microsoft Exchange Server

- 5.5버전부터 relay를 예방 기능지원

□ Anti-Relay에 대한 상세한 설명

- <http://www.microsoft.com/technet/exchange/relay.asp>

□ 광고용 전자 메일 메시지 릴레이(Relay) 방지

- <http://support.microsoft.com/default.aspx?scid=/isapi/goms.com.asp?target=/korea/support/xmlkb/kr193922.asp&LN=KO>

□ Exchange 2000 Server 운영 지침

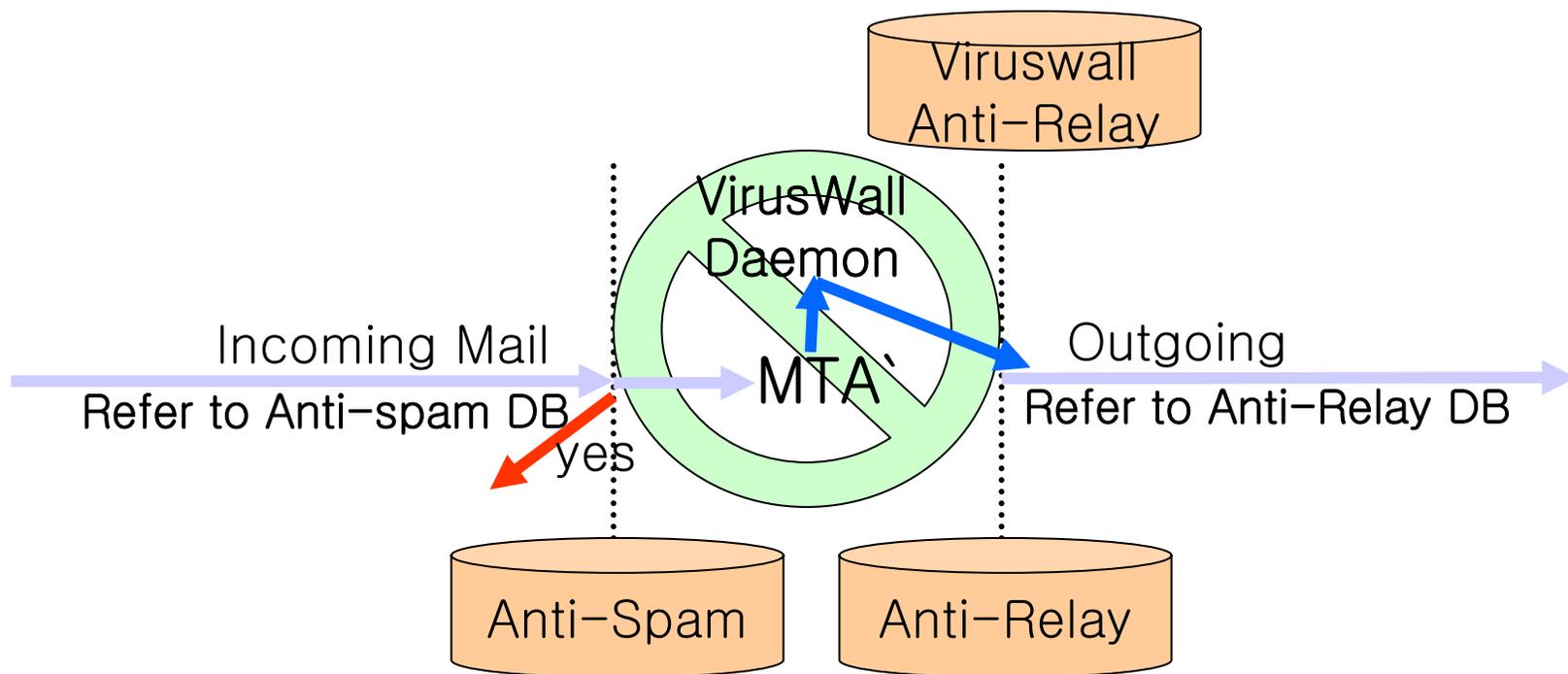
- <http://www.microsoft.com/korea/technet/prodtechnol/exchange/maintain/operate/opsguide/default.asp>

□ 기타 MTA (Mail Transmit Agent)

- <http://www.whitehats.com/library/mailrelay/repair-mailrelay.html>

스팸릴레이 설정방법 (Viruswall)

□ Viruswall의 Anti-Virus기능 사용시



광고성 스팸메일 차단방법

- ❑ 메일 헤더에 대한 점검룰셋(Check Ruleset)을 지원
 - Sendmail.cf에 적용
- ❑ 메일 헤더에 대한 필터링 기능을 이용
 - HSubject: \$>check_subject ==> 메일의 제목에 대한 헤더 (가장 많이 사용)
 - HContent-Type: \$>check_ct
 - Hdate, HX-Mailer, HX-MimeOLE, HMessage-Id, Hcomments
- ❑ 수신거부 및 에러메시지에 매크로 정의
 - D{Msg_adv}"553 광고성 스팸메일(Advertisement mail) not accepted."
 - D{Msg_master}"If you have questions, please email postmaster@\$j."

광고성 스팸메일 차단방법(예)

- ❑ 머릿글(subject)에 광고문구가 달린 스팸메일 수신거부
 - HSubject: \$>check_subject
 - D{Msg_adv}"553 광고성 스팸메일(Advertisement mail) not accepted."
 - D{Msg_master}"We denied your mail because of advertisement(ADV) mail\n If you have questions, please email postmaster@\$j."

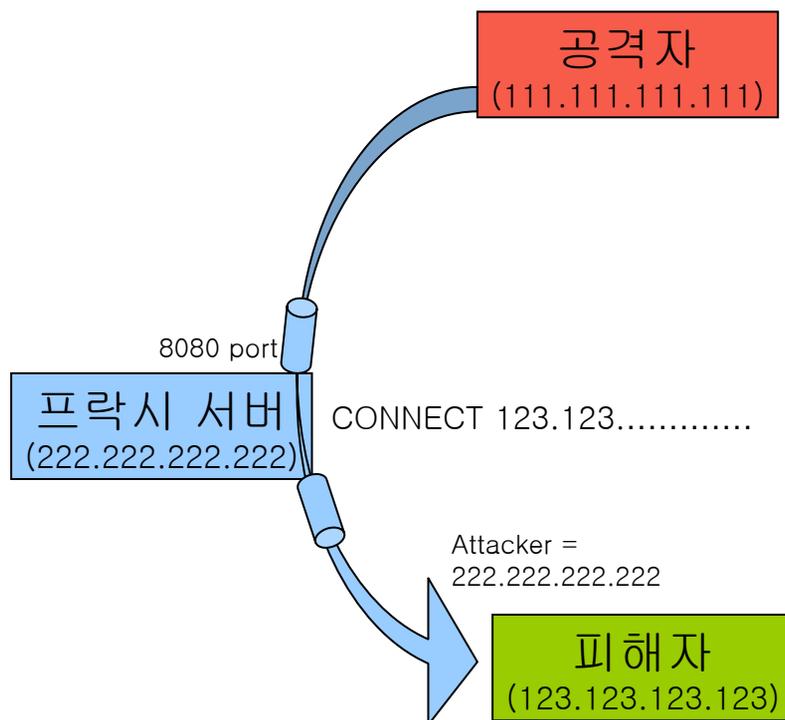
 - Scheck_subject
 - R<광고:\$*> \$#error \$: 550 \${Msg_master}
 - R\$*광고\$* \$#error \$: 550 \${Msg_master}
 - R[광고] \$#error \$: 550 \${Msg_master}
 - R<광고>\$* \$#error \$: 550 \${Msg_master}
 - R\$*[광-고]\$* \$#error \$: 553 D{Msg_adv}
 - R\$*[광고]\$* \$#error \$: 553 D{Msg_adv}
 - R\$*[광고]\$* \$#error \$: 553 D{Msg_adv}
 - R\$*[-광-고]\$* \$#error \$: 553 D{Msg_adv}
 - ** 기타 필요한 표현을 추가해 주면 됨

스팸메일서버로 악용되고 있을 때

- 스팸 블랙리스트를 관리하는 대표적인 사이트
 - <http://www.mail-abuse.org>
 - <http://www.orbs.org>
 - <http://maps.vix.com>
 - <http://www.imrss.org>
- 메일서버의 스팸메일 릴레이 기능을 처리하고 해당사이트에서 스팸메일 릴레이서버 리스트에서 삭제해 달라는 요구

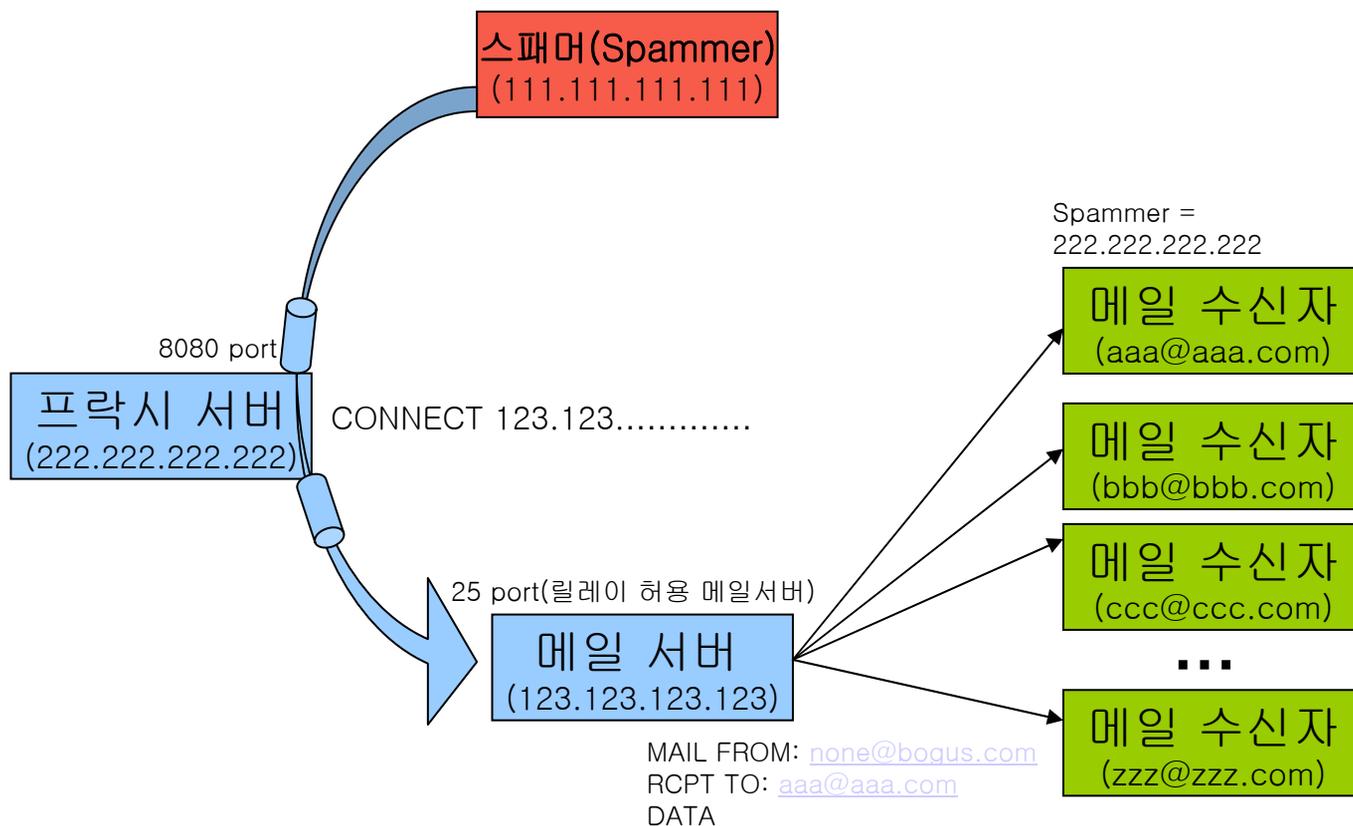
프록시 서버의 TCP Relay 문제점

- HTTP CONNECT 방법을 지원
 - 모든 TCP 포트에 HTTP CONNECT 방법을 이용하여 접속을 맺을 수 있도록 default 설정



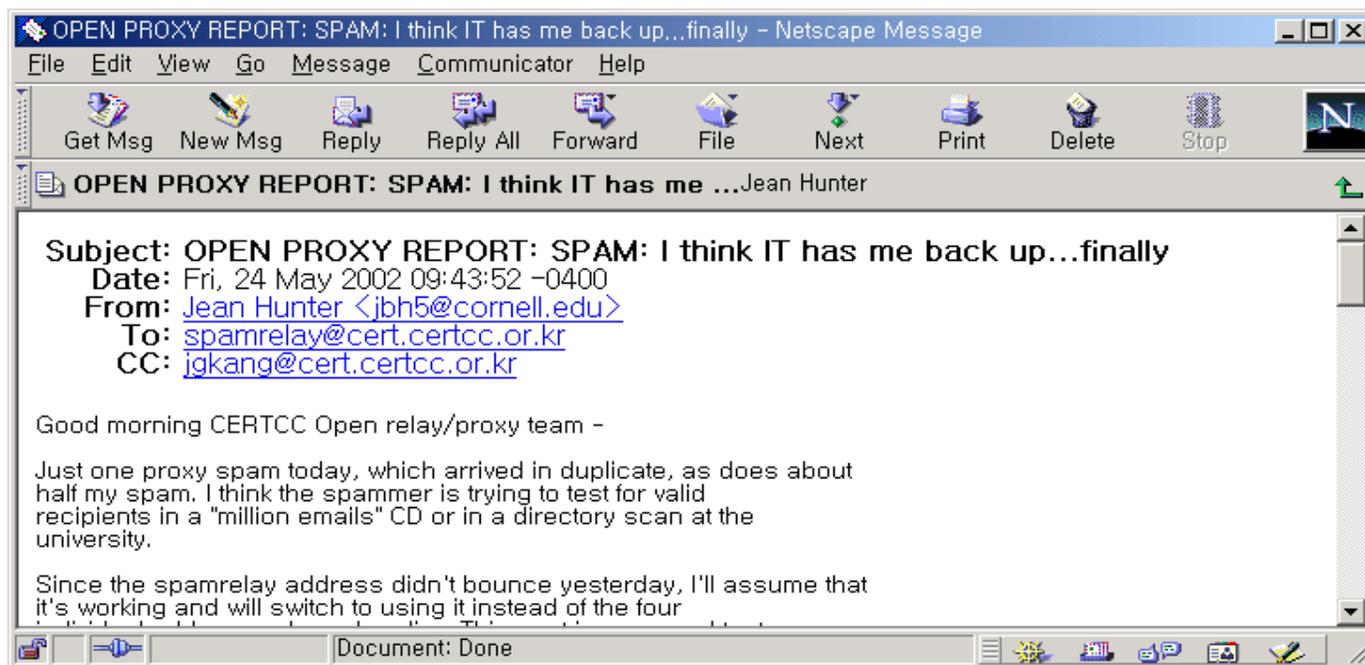
프록시 서버의 TCP Relay 문제점

- 프락시 서버의 주소를 사용함으로써 이를 우회하여 메일서버를 이용

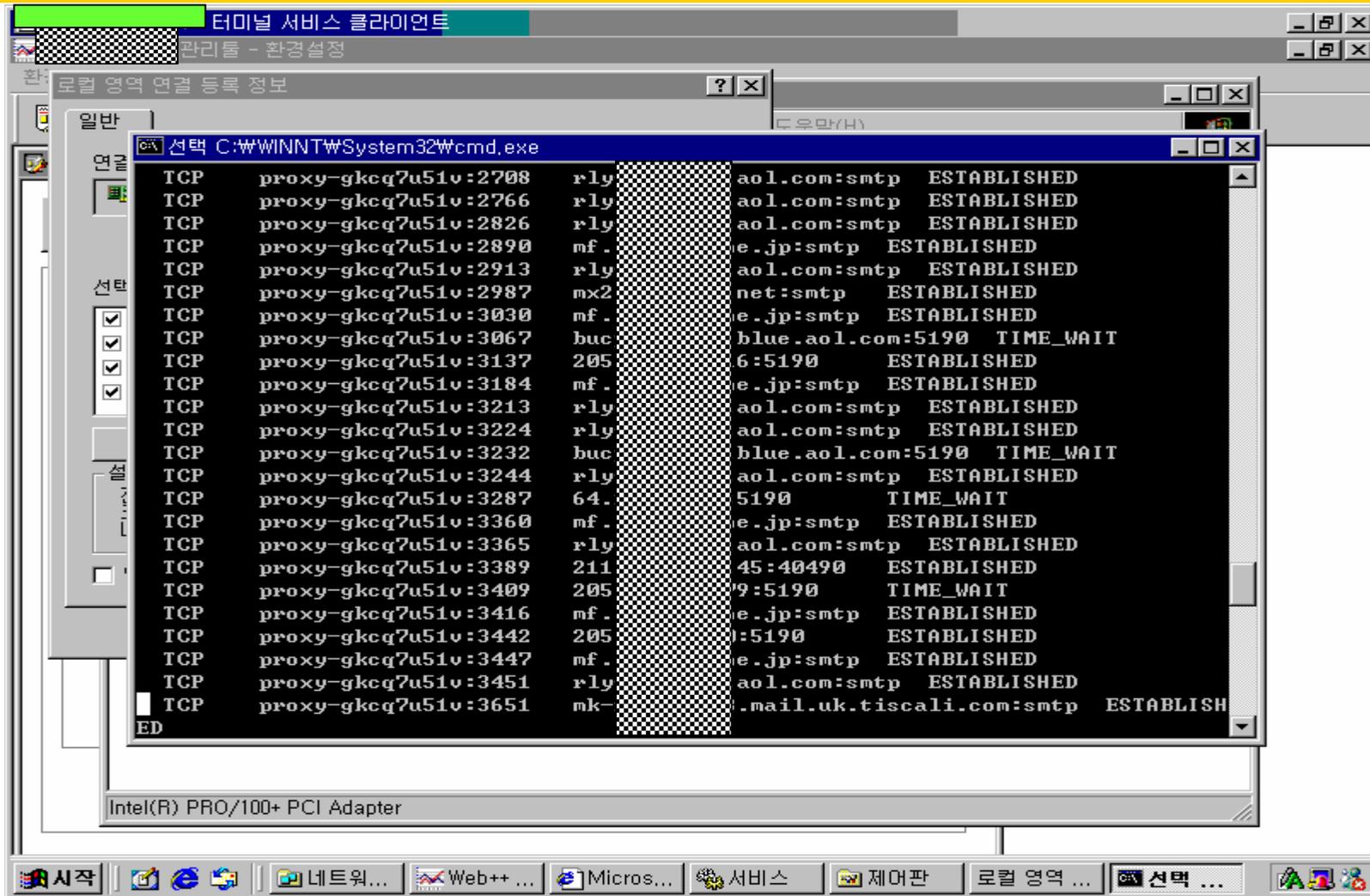


프록시 서버의 TCP Relay 피해사례

- 국외로부터 접수된 프락시 서버에 대한 항의 메일



프록시 서버의 TCP Relay 피해사례



프록시 서버의 TCP Relay 피해사례

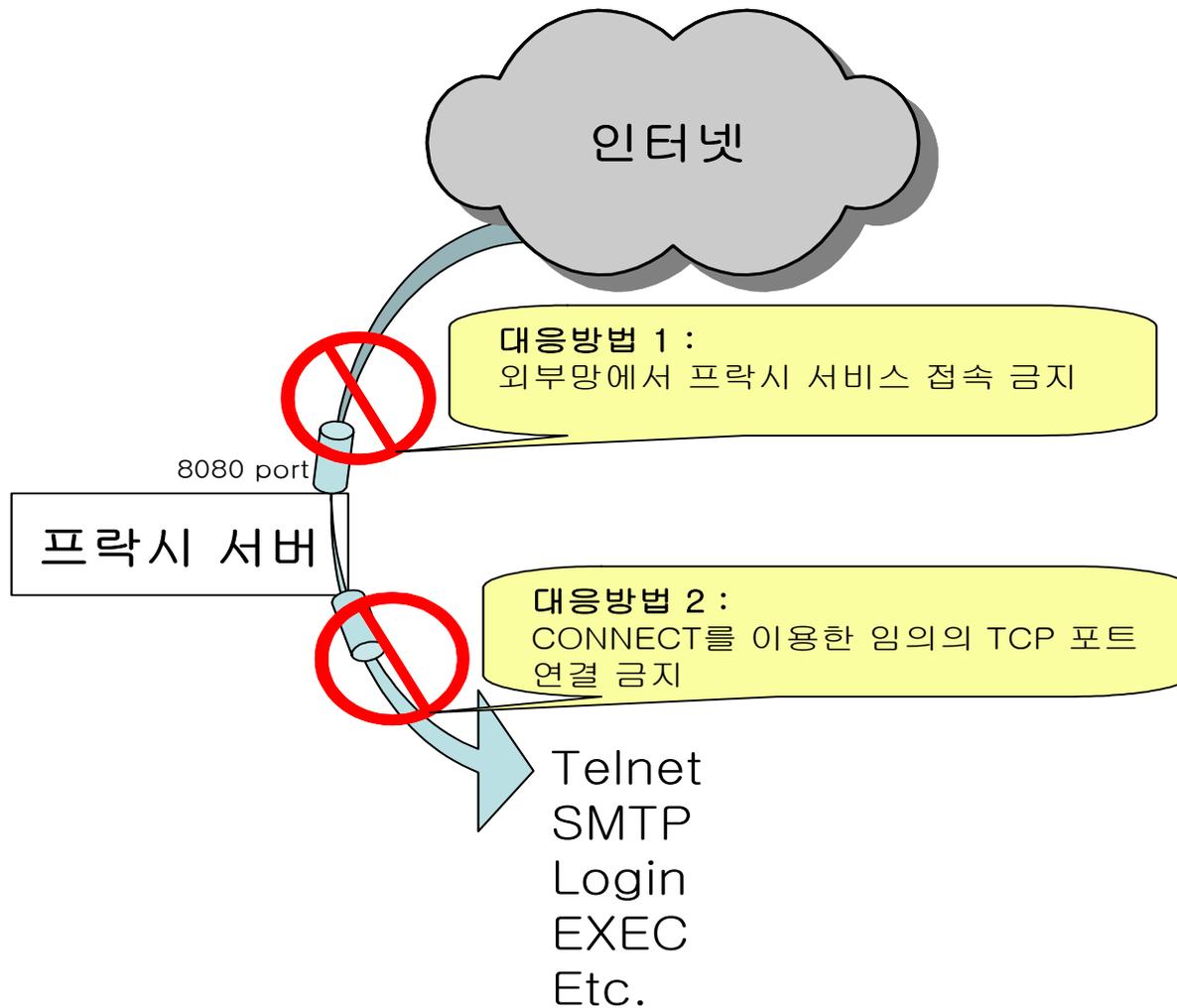
The screenshot shows the Netscape Messenger interface. The left pane displays a folder tree with 'Local Mail' expanded, showing subfolders like 'inbox', 'Trash', and '내AA'. The main pane shows a list of messages with columns for Subject, Sender, and Date. The selected message is:

Subject: 섯heck_subject
Date: Fri, 7 Jun 2002 11:02:14 +0900 (KST)
From: kims@kisa.or.kr

The body of the message contains the text: "SPAM Relay Test. Proxy Agent Vul."

At the bottom of the window, it shows "Total messages: 773" and "Unread messages: 100".

프록시 서버의 TCP Relay 대응



프록시 서버의 TCP Relay 수동점검

```
172.16.14.90 - CRT
File Edit View Options Transfer Script Window Help
[ penguin:root ]:/user1/ksch/school/itop> telnet 211.252.139.1 80
Trying 211.252.139.1...
Connected to 211.252.139.1.
Escape character is '^]'.
CONNECT 61.77.199.65:23 HTTP/1.0

HTTP/1.0 200 Connection established
Proxy-agent: [redacted]ow-Proxy/1.0

User Access Verification

Password:
Router>en
Password:
Router#exit
Connection closed by foreign host.
[ penguin:root ]:/user1/ksch/school/itop> telnet 2[redacted]4 80
Trying 2[redacted]4...
Connected to 2[redacted]4.
Escape character is '^]'.
CONNECT 61.77.199.65:23 HTTP/1.0
Connection closed by foreign host.
Ready Telnet 21, 41 24 Rows, 83 Cols VT100 NUM
```

끝으로

- 국내 정보통신망에서 운영되는 메일서버가 외부의 악의 사용자로부터 스팸메일 릴레이 서버로 악용되는 피해를 예방
- 우리 기관에서 운영 중인 프락시 서버의 점검 및 대응을 통한 피해예방
- 모든 정보시스템 오남용에 대한 제도적인 대책