스팸릴레이 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 인식부족과 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

- 스팸메일로 인한 민원이 증가하는 가운데, 초중고 메일서버의 중계기능을 악용하는 스팸릴레이에 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 원격점검서비스
    - 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

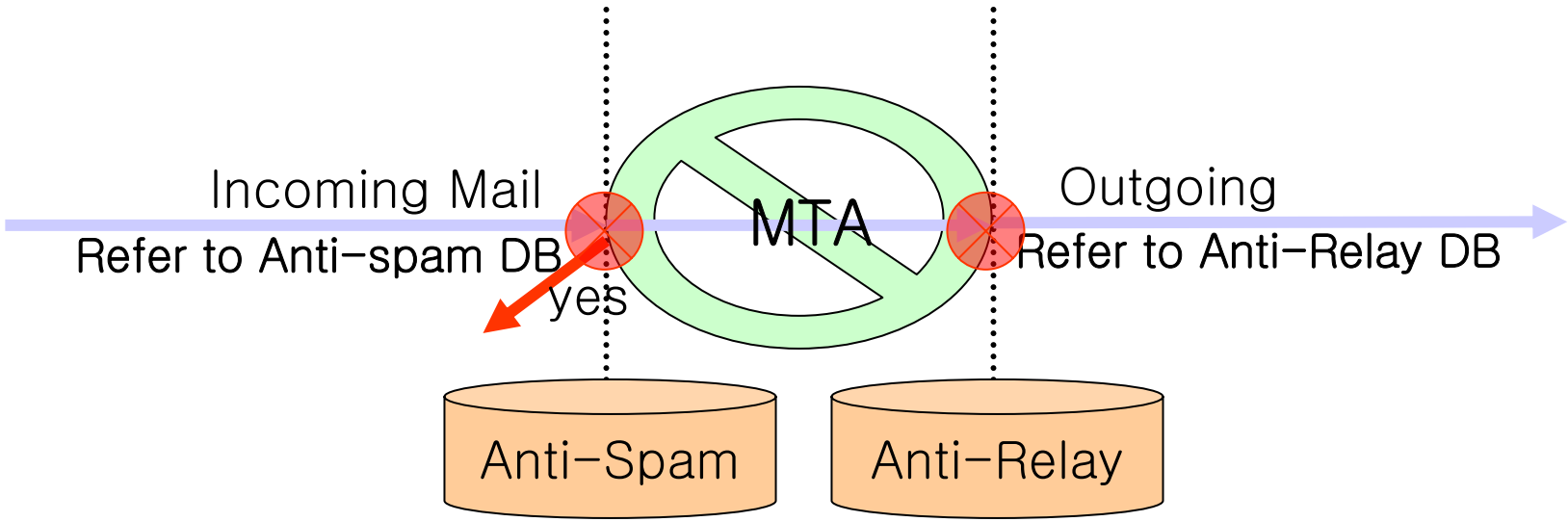
유관기관 대응현황

(6월 28일 기준)

구분	[redacted]					프락시서버 업체					CERT 사고접수			합계
	경기	강원	충북	울산	제주	[redacted]					몽키닷컴	탑포인트	기타	
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

스팸릴레이 Basic Algorithm

- 메일서버의 스팸릴레이



스팸릴레이 점검방법

- 메일서버의 스팸릴레이 점검
  - 수동점검
  - 제3자 서비스 점검
  - 보안취약성 점검도구를 이용한 점검

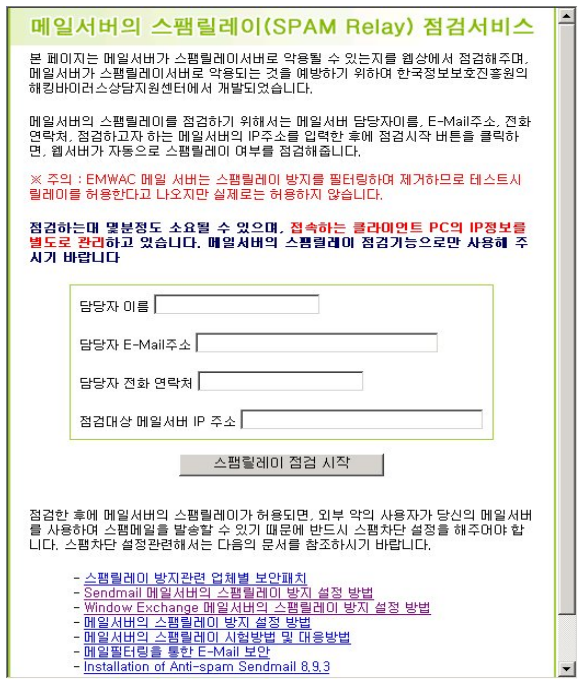
스팸릴레이 점검(수동점검)

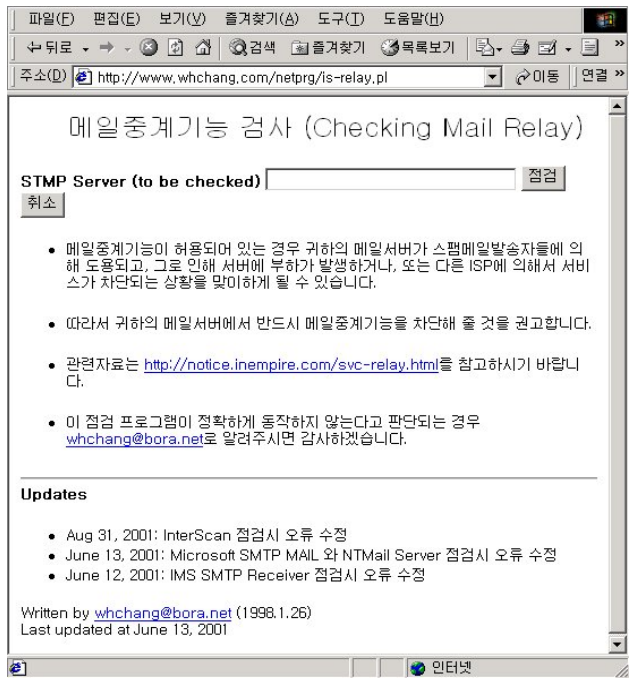
- 내부 도메인 및 내부 IP주소가 아닌 곳에서의 스팸릴레이를 점검

```
[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)

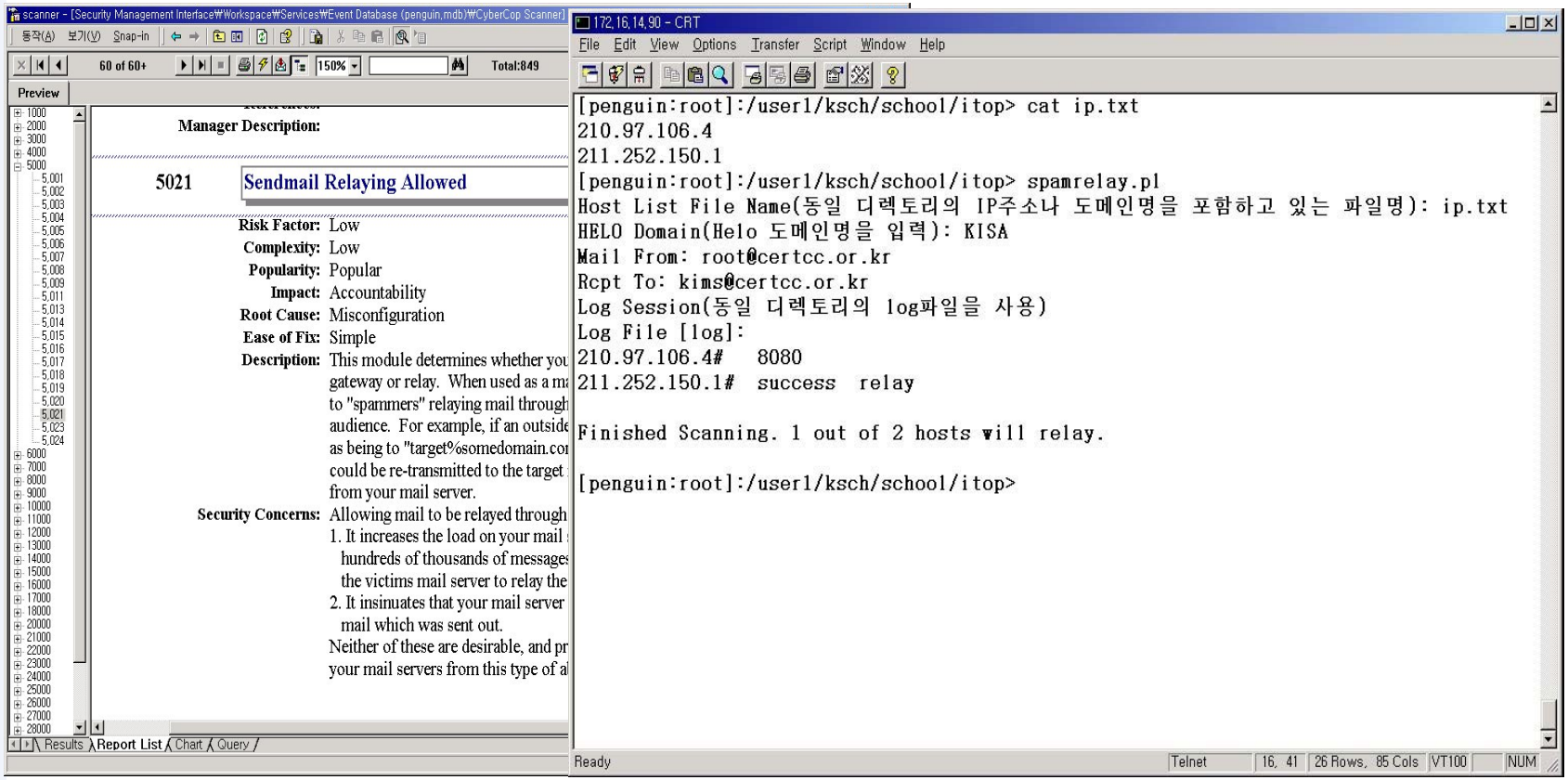
- 스팸릴레이 점검서비스를 무료로 제공해주는 사이트를 활용
  - http://www.certcc.or.kr/spamrelay.html
    http://www.whchang.com/netprg/is-relay.pl





스팸릴레이 점검(점검도구활용)

- 상용화된 취약성점검도구나 공개용 취약성 점검도구 활용



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

스팸릴레이설정방법

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

豪詳鳩픈
RELAY172.16OKuseful.orgREJECTspammail.comREJECTspam@hacker.com
```

스팸릴레이설정방법

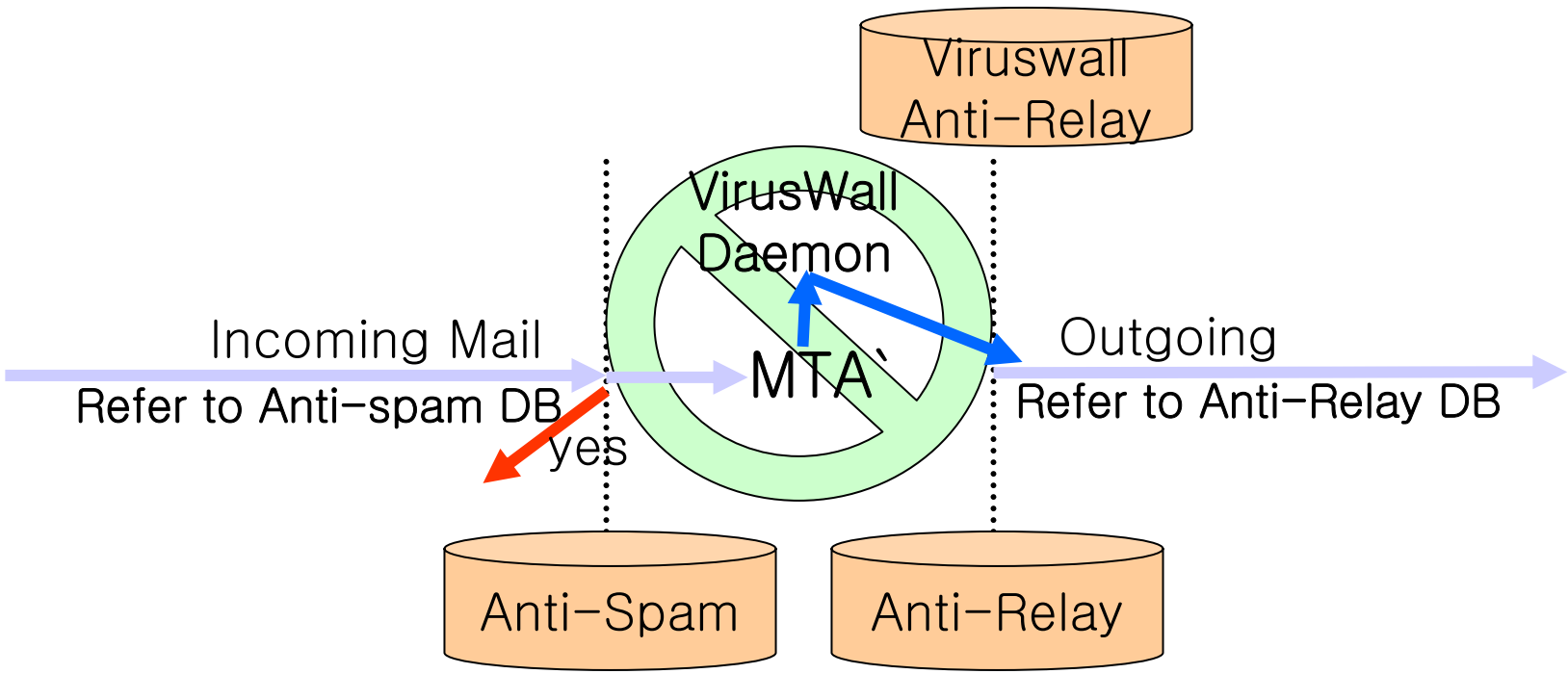
- EXIM
  - Download
    - ✓ http://www.exim.org
  - 스팸릴레이 설정
    - ✓ http://www.exim.org/howto/relay.html
- EMWAC
  - DownLoad
    - ✓ http://www.l7.net/cgi-bin/archives.cgi?template=archives&path=archives/emwac/server
  - **IMS**에 필터링 기능을 부여해주는 **SCMSFILTER**
    - ✓ http://www.sica.com/freestuf/scsmfilt.htm
  - **Antirelay Plugin** 설치방법
    - ✓ **http://www.orca.bc.ca/win95/antirelay.zip**

스팸릴레이설정방법

- 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/gomscom.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

스팸릴레이설정방법(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."

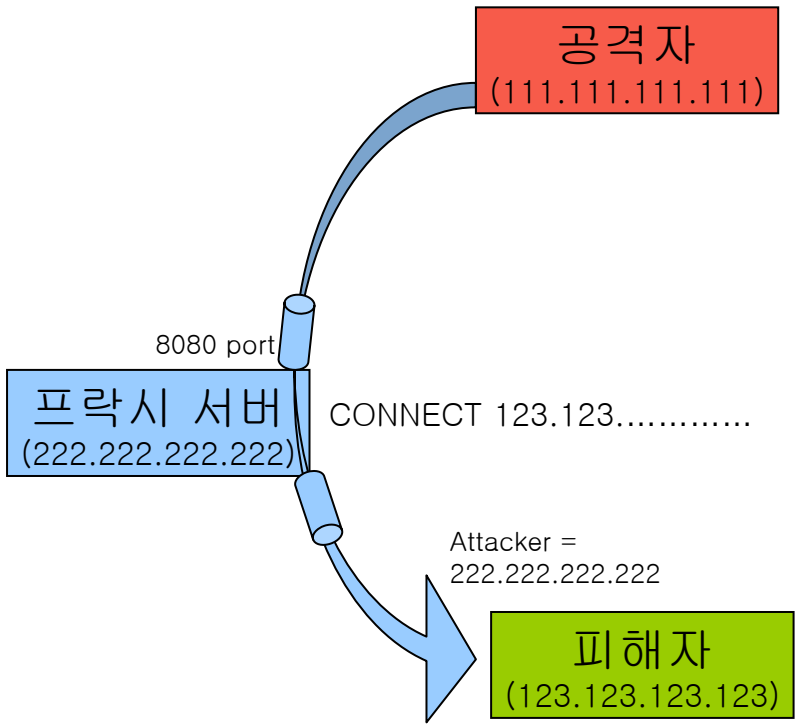
  - Scheck_subject
  - R<광고:$*> $#error $: 550 ${Msg_master}
  - R$*광고$* $#error $: 550 ${Msg_master}
  - R[광고] $#error $: 550 ${Msg_master}
  - R<광고>$* $#error $: 550 ${Msg_master}
  - R$*[광-고]$* $#error $: 553 D{Msg_adv}
  - R$*[광고]$* $#error $: 553 D{Msg_adv}
  - R$*[괌고]$* $#error $: 553 D{Msg_adv}
  - R$*[-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

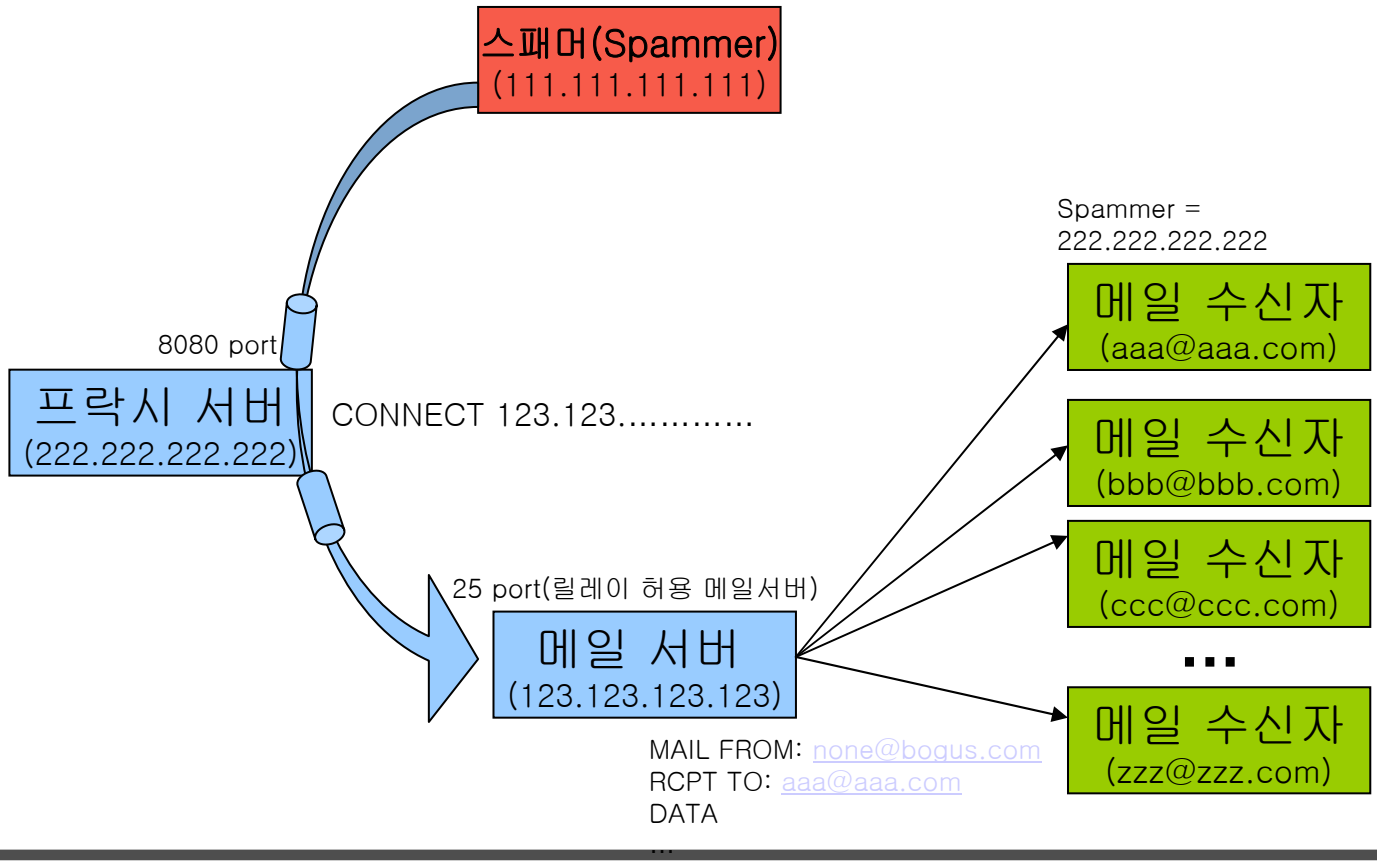
프록시 서버의 TCP Relay 문제점

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



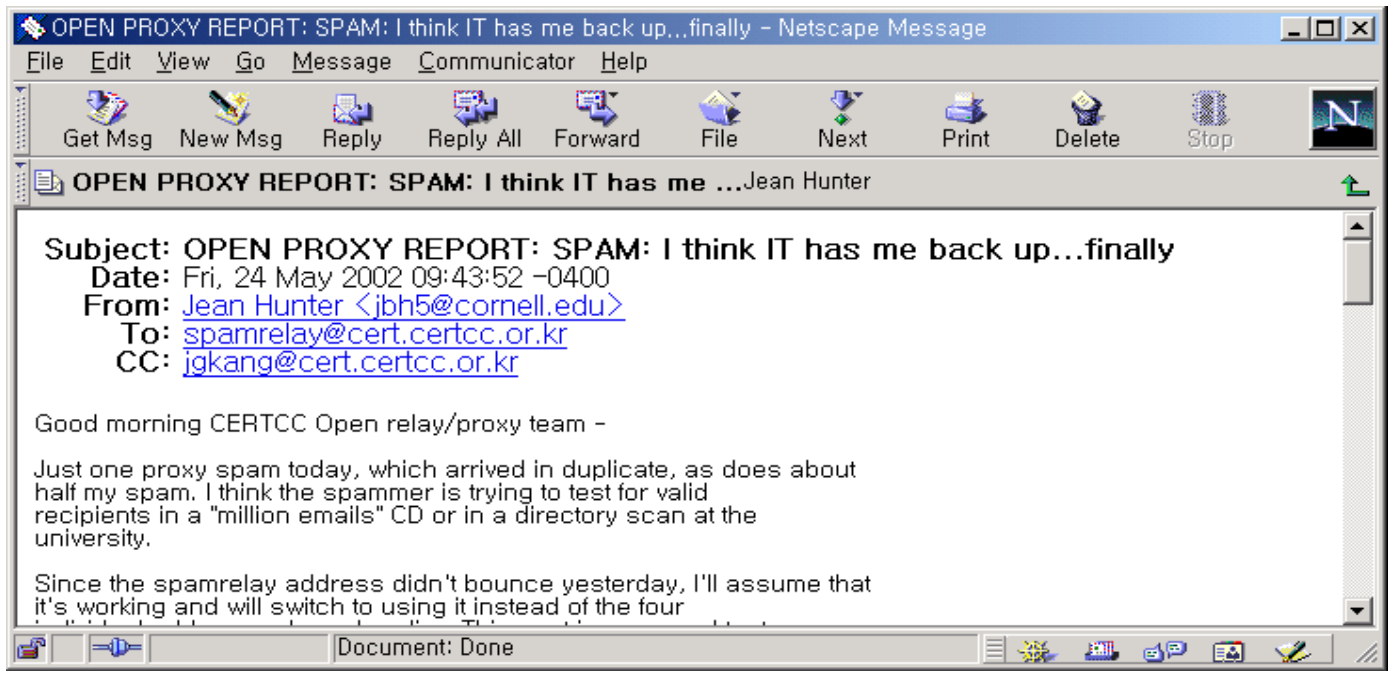
프록시 서버의 TCP Relay 문제점

- 프락시 서버의 주소를 사용함으로써 이를 우회하여 메일서버를 이용

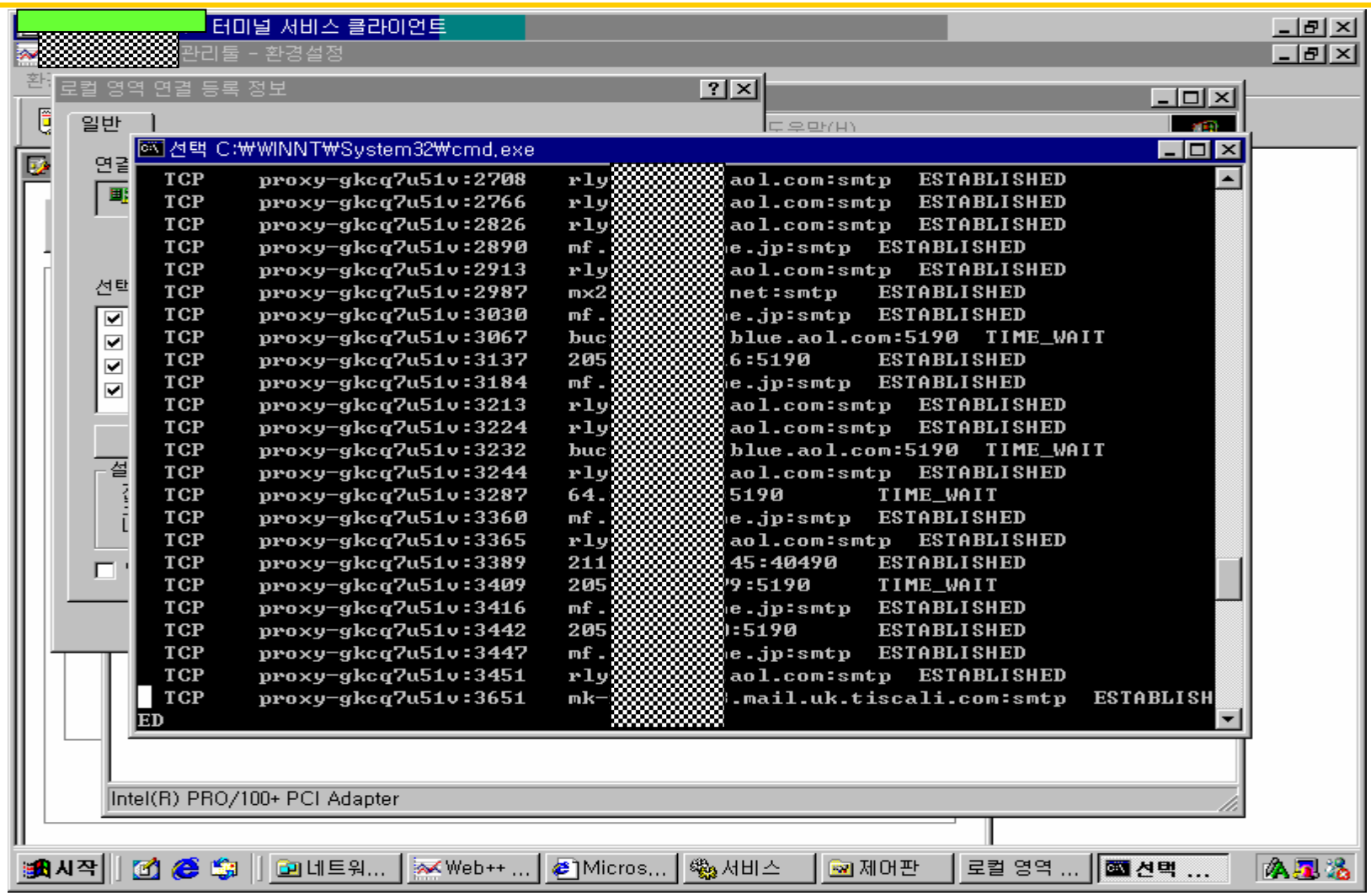


프록시 서버의 **TCP Relay** 피해사례

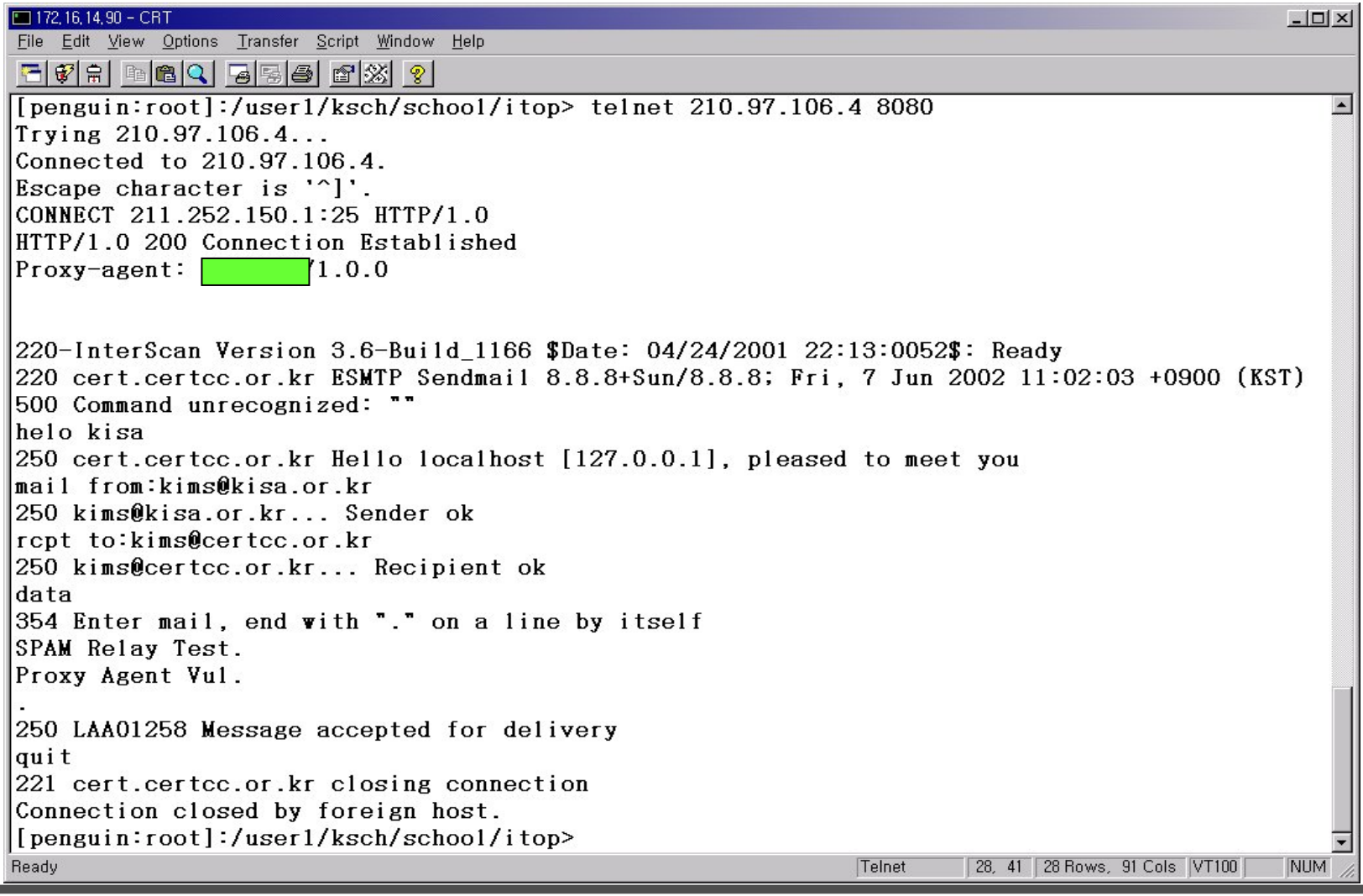
- 국외로부터 접수된 프락시 서버에 대한 항의 메일



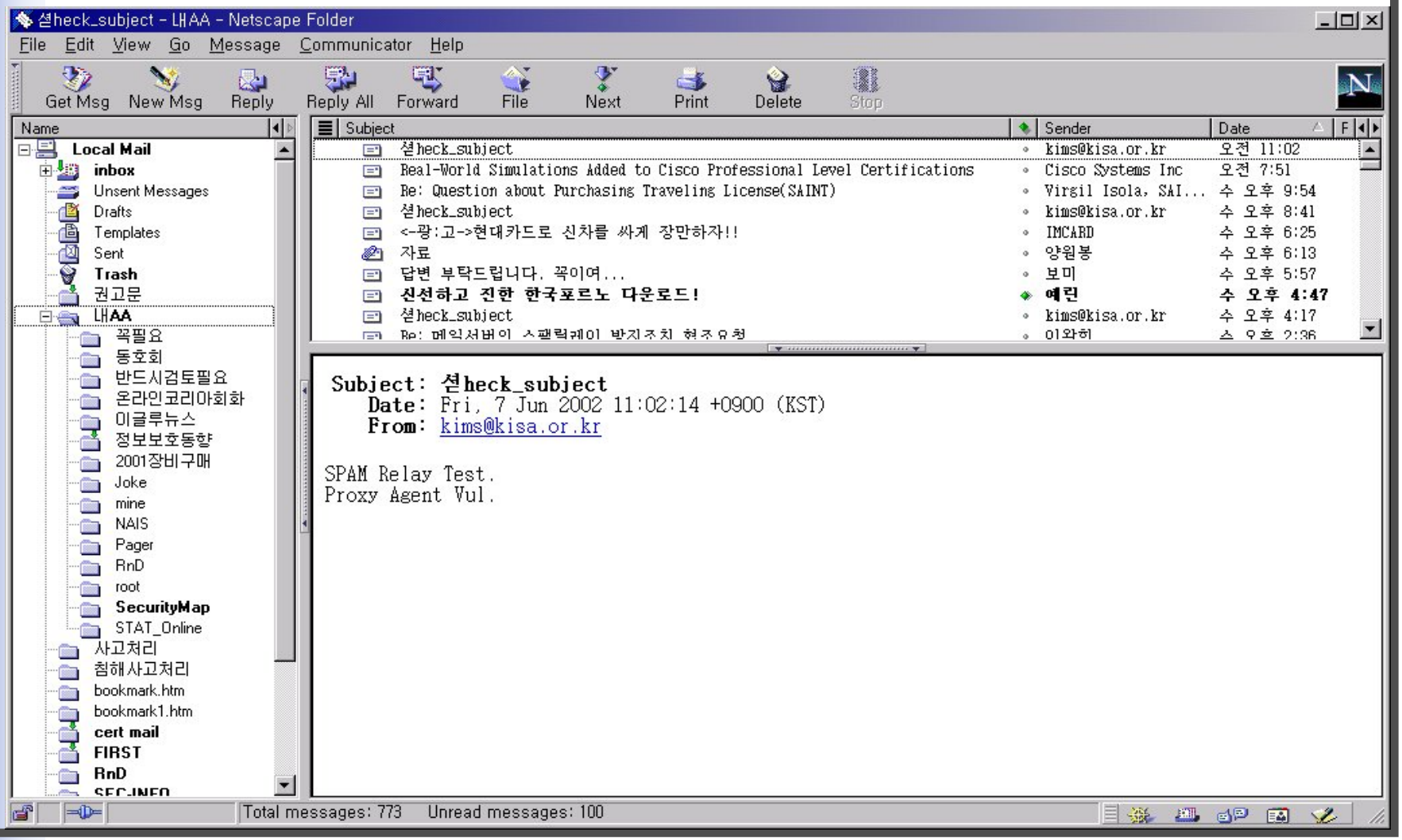
프록시 서버의 TCP Relay 피해사례



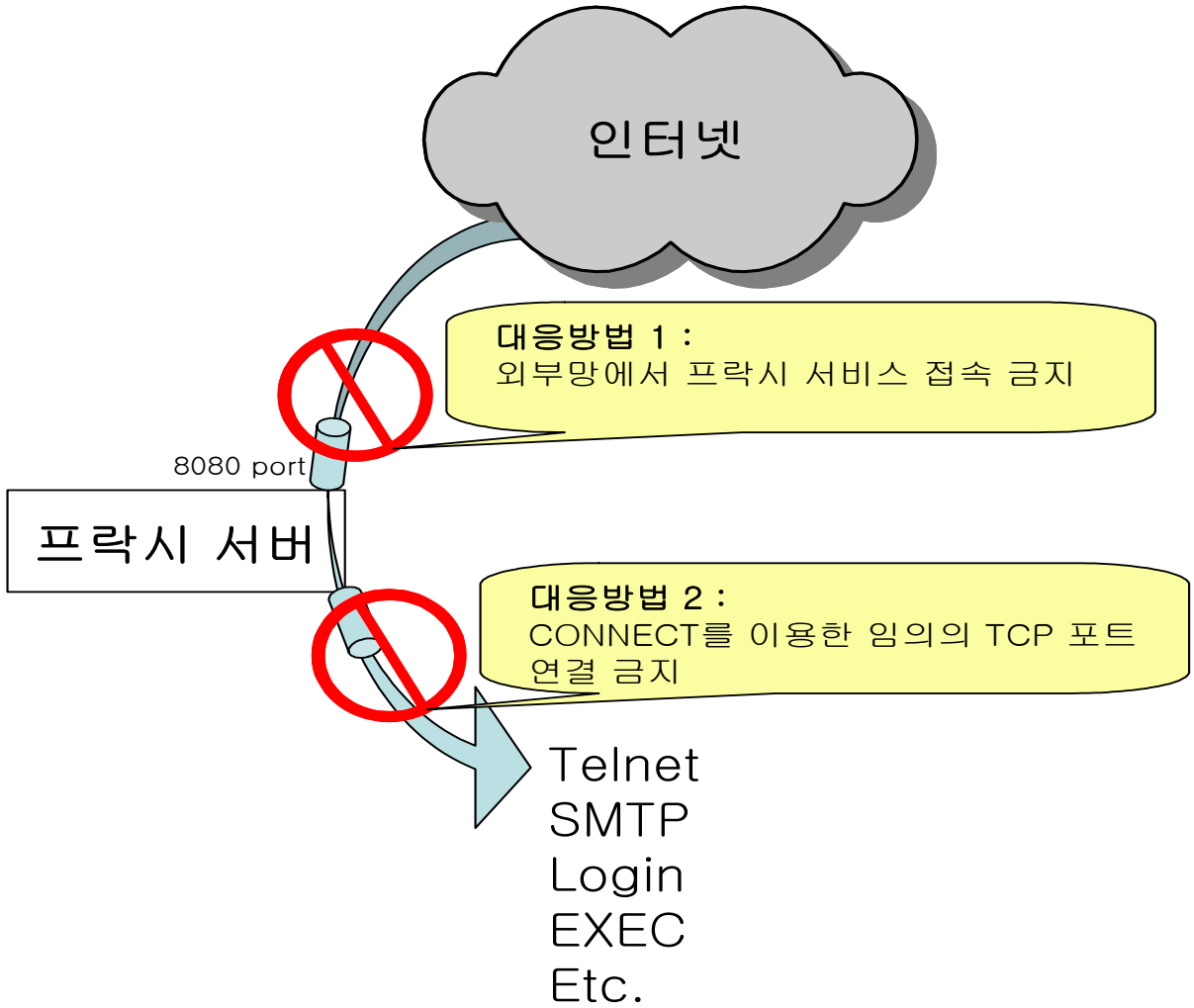
프록시 서버의 TCP Relay 피해사례



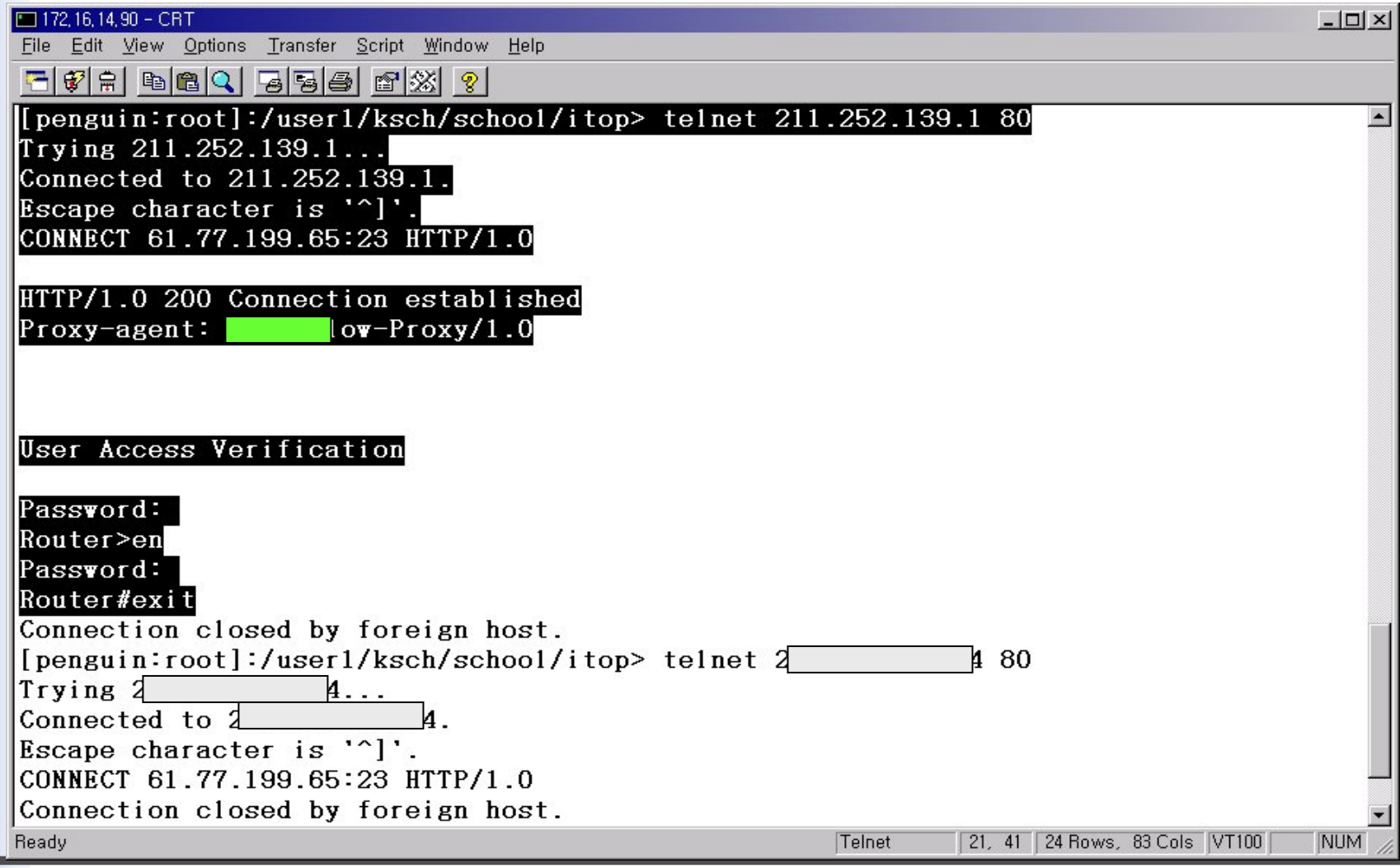
프록시 서버의 TCP Relay 피해사례



프록시 서버의 **TCP Relay** 대응



프록시 서버의 **TCP Relay** 수동점검



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