연구전산망 Spam Mail 및 특정 Site 차단 기술

박 · 학 · 수(E-mail:hispark@kordi.re.kr)
연구개발정보센터 연구전산망운영실 선임연구원 ·

Ⅰ. Spam mail 개요 ·

스팸메일(Spam Mail)은 정크메일(Junk Mail), 벌크메일(Bulk Mail)이라고도 하는데 일반적으로 받기를 원치 않는 메일을 통틀어 일컫는 말이다. '스팸'은 미국의 'Hormel Foods사'에서 만든 먹는 '깡통에 든 햄'으로 '햄(Ham)'의 대명사이다. 그러나 이 회사가 '스팸'을 홍보하는 방법이 아주 유별났다. 모든 역량(?)을 광고에 집중했기 때문이다. 그래서 일반적으로 심한 광고로 인한 공해를 스팸이라는 말로 표현한다. 그리고 스팸메일을 보내는 사람을 스퍼머(spammer)라고 한다.

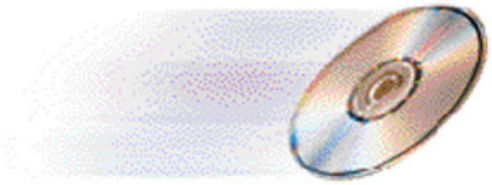
요즘들어 인터넷을 이용한 서비스 형태가 다양해지고 있으며 이로 인한 보안상 많은 문제점들이 대두되어지고 있어, 이로 인해 사회적으로 많은 문제점들이 나오고 있다. 이로 인한 문제로 대부분의 기관에서는 방화벽(Fire wall)이라는 장비를 도입하여 어느 정도 보안기능을 강화하여 각 기관들에 인터넷 해킹 등으로부터 보호하고 있다.

연구전산망/고성능전산망센터에서는 방화벽이 없는 기관에서 손쉽게 라우터를 이용하여 방화벽 역할을 할수 있도록 스팸메일 차단기술을 지원하고 있으며 정기적인 사이트 점검으로 게이트웨이에서 이를 예방해주고 있다.

Ⅱ. Access List를 이용한 Spam mail의 방지법

●Access List 선언시 유의사항 ·

- 빈번히 조건을 만족시킬만한 것을 먼저 선언 ·
- access-list의 마지막에 특별히 permit any를 지정하지 않는 한 기본적으로 deny any가 · 선언되어 있다는 사실을 잊지 말 것 ·
- access-list의 조건을 여러줄에 선언을 하는데 임의의 줄과 줄 사이의 것을 지우거나 수정할 수 없음. 새로 추가하는 것은 모두 마지막에 더 해줌 ·
  - 따라서 동일한 access-list number의 조건을 선언 할 때는 처음부터 차례로 전부 선언해 · 주는 것이 바람직함 ·



●Extended Access List 설정방법 ·

➔ Router#Router(config)# access-list *access-list-number* {permit | deny}
{protocol} {source-address wildcard-mask} {destination-address wildcard-mask} {options}

●[Sample]

```
Router(config)# access-list 100 deny ip 130.100.0.0 0.0.255.255 130.120.0.0 0.0.255.255
Router(config)# access-list 100 permit ip any any
Router(config)# int e 0
Router(config-if)# ip access-group 100 out
```

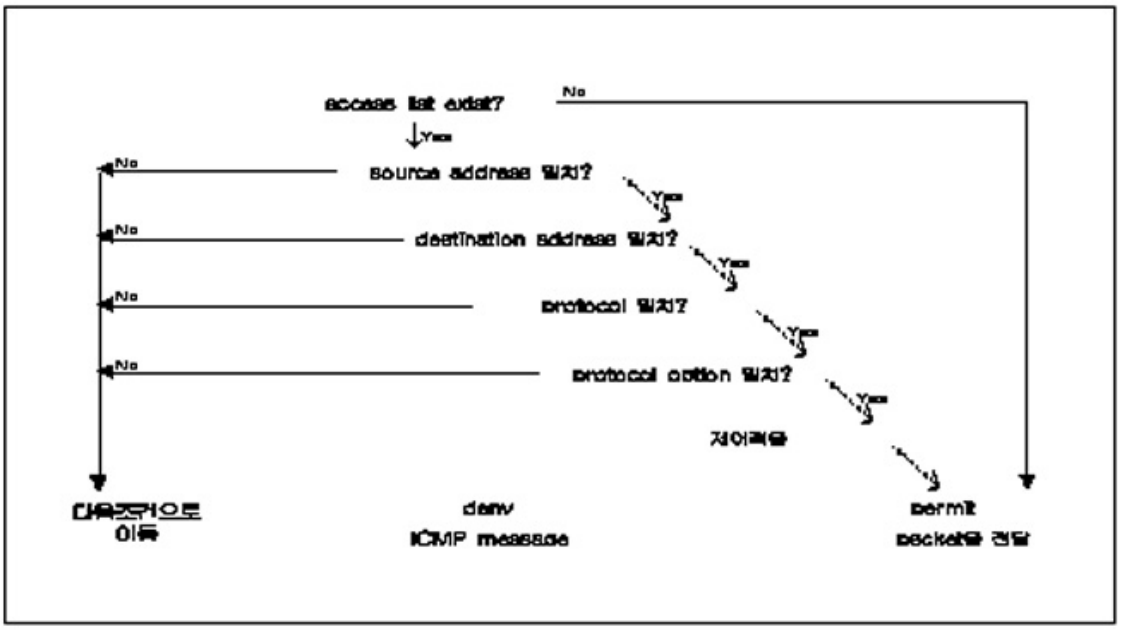
인터페이스 이더넷으로부터 나가는 외부망 ·130.100.0.0으로부터 내부망 130.120.0.0 네트워크로 인터넷의 모든 서비스를 차단하기 위해 설정된 값이며 나머지 네트워크는 허용한다.·

●연구전산망 / 고성능전산망에서 스팸메일 방지를 위한 Access-list 적용예 ·

```
router#access-list 101 deny   tcp any host 134.75.30.247 eq smtp
router#access-list 101 deny   tcp any host 134.75.55.2   eq smtp
router#access-list 101 deny   tcp any host 134.75.155.10 eq smtp
router#access-list 101 permit ip any any
```

위 적용된 내용은 연구전산망(KREONet)/고성능전산망(HPCNet) 게이트웨이 라우터에서 스팸 메일을 발생시키고 있는 연구전산망 가입기관의 Spam mail relay 서버를 찾아 연구전산망 Gateway 라우터에 적용함으로써 통신회선의 낭비를 예방하고 인터넷 사용자가 불필요한 메일을 수신하는 것을 예방하고 있는 사례이다.·

■ Extended Access List 적용과정



●특정 서비스만 허용한 예 ·

```
int Ethernet 0
ip access-group 101 out
access-list 101 permit tcp any any established
access-list 101 permit ip 150.183.0.0 0.0.255.255 210.178.52.0 0.0.0.255
access-list 101 permit udp any any
access-list 101 permit tcp any any eq smtp
access-list 101 permit tcp any any eq pop3
access-list 101 permit tcp any any eq www
access-list 101 permit tcp any any eq ftp
access-list 101 permit tcp any any eq ftp-data
access-list 101 permit icmp any any eq echo
access-list 101 permit icmp any any eq echo-reply
access-list 101 permit ip any any
```

인터페이스 이더넷으로부터 나가는 외부망 어드레스 130.100.0.0으로부터 내부망 어드레스 130.120.0.0 네트워크로 인터넷의 모든 서비스를 차단하기 위해 설정된 값이며 나머지 네트워크는 허용한다.