서 울 중 앙 지 방 법 원

제 7 7 민 사 부

판 결

사 건 2003가합32082 손해배상(기)

원 고 ○○연대 외 1,586(별지 1. 내지 7. 참조)

소송대리인 법무법인 한결

담당변호사 윤복남

피 고 1. 주식회사 ○○

성남시 분당구 ○○

대표이사 이○○

소송대리인 법무법인 태평양

담당변호사 류광현, 김남희

2. ○○ 주식회사

서울 중구 ○○

대표이사 캐나다국인 ○○영

소송대리인 법무법인 광장

담당변호사 고환경

3. 정리회사 주식회사 ○○의 관리인 박○○

성남시 분당구 ○○

소송대리인 법무법인 태평양

담당변호사 류광현, 김남희

4. 주식회사 ○○

서울 강남구 ○○

대표이사 박○○

5. ○○ 주식회사

서울 송파구 ○○

대표이사 이○○

6. 주식회사 ○○의 소송수계인

정리회사 주식회사 ○○의 관리인 황○○

성남시 분당구 ○○

피고 4. 내지 6.의 소송대리인 법무법인 광장

담당변호사 고환경

7. 대한민국

법률상 대표자 법무부장관 김성호

소송대리인 변호사 한택근

8. ○○ 코퍼레이션

미합중국 와싱톤주 ○○

(○○ WA ○○, U.S.A)

송달장소 서울 강남구 ○○

주식회사 ○○

소송대리인 변호사 한상호, 이능규, 김성진

변 론 종 결　　2006. 10. 13.

판 결 선 고　　2006. 11. 3.

주　　문

1. 원고들의 피고들에 대한 청구를 모두 기각한다.

2. 소송비용은 원고들이 부담한다.

청 구 취 지

[주위적 청구취지]

피고들은 각자

가. 별지 1-1, 1-3, 2-1, 2-3, 3-1, 4-1, 4-3, 5-1, 5-3, 6-1, 6-3, 7 기재 각 원고들에게 각 5만 원,

나. 별지 1-2, 4-2, 5-2, 6-2 기재 각 원고들과 별지 2-2 기재 1. 내지 11, 13. 원고에게 각 30만 원,

다. 원고 주식회사 ○○에게 2천만 원

및 위 각 돈에 대하여 2003. 1. 25.부터 이 사건 청구취지 및 원인변경신청서 부본 송달일까지는 연 5%의, 그 다음날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라.

[예비적 청구취지]

가. 피고 주식회사 ○○는 별지 1-1, 1-2, 1-3 기재 각 원고들에게 별지 1-1, 1-2, 1-3의 각 '청구금액'란 기재 돈,

나. 피고 ○○ 주식회사는 별지 2-1, 2-2, 2-3 기재 각 원고들에게 별지 2-1, 2-2, 2-3 기재 각 '청구금액'란 기재 돈,

다. 피고 정리회사 주식회사 ○○의 관리인 박○○은 별지 3-1 기재 각 원고들에게 별지 3-1의 각 '청구금액'란 기재 돈,

라. 피고 주식회사 ○○은 별지 4-1, 4-2, 4-3 기재 각 원고들에게 별지 4-1, 4-2, 4-3의 각 '청구금액'란 기재 돈,

마. 피고 ○○ 주식회사는 별지 5-1, 5-2, 5-3 기재 각 원고들에게 별지 5-1, 5-2, 5-3 기재 각 '청구금액'란 기재 돈,

바. 피고 정리회사 주식회사 ○○의 관리인 황○○은 별지 6-1, 6-2, 6-3 기재 각 원고들에게 별지 6-1, 6-2, 6-3의 각 '청구금액'란 기재 돈

및 위 각 돈에 대하여 2003. 1. 25.부터 이 사건 청구취지 및 원인변경신청서 부본 송달일까지는 연 5%의, 그 다음날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라.

이 유

1. 기초사실

가. 피고들의 지위

⑴ ① 피고 주식회사 ○○(이하 '피고 ○○'라 한다), ② 피고 ○○ 주식회사(2004. 12. 16. 변경되기 전 상호 ○○ 주식회사, 이하 '피고 ○○'이라 한다), ③ 피고 정리회사 ○○의 관리인 박○○(주식회사 ○○은 2003. 3. 27. 이 법원 2003회5호로 회사정리절차개시결정을 받고, 박○○이 그 관리인으로 선임되었다, 이하 '피고 ○○'이라 한

다), ④ 피고 주식회사 ○○(이하 '피고 ○○'이라 한다), ⑤ 피고 ○○ 주식회사(이하 '피고 ○○'이라 한다), ⑥ 피고 주식회사 ○○의 소송수계인 정리회사 주식회사 ○○의 관리인 황○○(주식회사 ○○은 2003. 5. 9. 수원지방법원 2003회1호로 회사정리절차개시결정을 받고 황○○이 그 관리인으로 선임되었다. 이하 '피고 ○○'이라 한다)은 모두 자신들이 구축한 인터넷망을 통하여 계약자들에게 인터넷통신망 서비스를 제공하는 회사들(Internet Service Provider, 이하 위 피고들을 통칭하여 '피고 ISP들'이라 한다)이다.

⑵ 피고 ○○ 코퍼레이션(이하 '피고 ○○'라 한다)은 하드웨어 및 소프트웨어의 제조·판매업을 하는 회사이다.

나. 원고들 중 별지 1-1, 2-1, 4-1, 5-1, 6-1, 2-2의 순번 5, 11, 12, 13. 기재 원고들

⑴ 별지 1-1. 기재 원고들은 피고 ○○와, 별지 목록 2-1. 기재 원고들은 피고 ○○과, 별지 4-1. 기재 원고들은 피고 ○○과, 별지 5-1. 기재 원고들은 피고 ○○과, 별지 6-1. 기재 원고들은 피고 ○○과 각 인터넷 서비스 이용계약을 맺고 피고 ISP들이 제공하는 인터넷통신망 서비스를 이용하고 있는 이용자들이다.

⑵ 별지 2-2. 중 순번 5, 11, 13. 원고들은 피고 ○○의 PC방용 서비스에 가입하여 피씨(PC)방을 운영하는 사업자들이다. 원고 주식회사 ○○는 2002. 1. 31. 피고 ○○과 사이에, 위 피고로부터 계약기간은 2년으로 정하여 대용량 인터넷 통신망서비스인 광이더넷서비스를 제공받기로 서비스이용계약을 체결하고, 이를 제공받아 PC방 업자들에게 재판매하고 있는 사업자이다.

다. 인터넷 침해사고의 개요

⑴ 2003. 1. 25. 14:30경 미국, 호주 등으로부터 유입된 악성 프로그램인 슬래머 웜

(Slammer Worm)은 초당 1만 내지 5만 개의 404바이트(Byte) 패킷(packet, 정보를 일정 크기로 분할하고 각각에 송수신 주소를 부가하여 만든 데이터 블록)을 대량 생성하여 무작위의 IP주소로 발송함으로써 네트워크의 과부하를 유발시켜 인터넷 장애사태를 초래하였다(이하 2003. 1. 25. 14:30경 슬래머 웜에 의하여 유발된 인터넷 침해사태를 '이 사건 인터넷 침해사고'라 한다).

⑵ 경과

㈎ 피고 ○○은 2003. 1. 25. 14:10경 최초로 인터넷 트래픽(traffic: 착발신 신호의 수)에 이상 징후가 발생한 것을 발견하였는데, 2003. 1. 25. 14:35경부터 국제회선 및 ○○나라 주요 ISP의 DNS(Domain Name System) 서버[1], IDC(Internet Data Center)[2] 내부망에 과부하 현상이 발생하였다.

㈏ 피고 대한민국 산하 정보통신부는 2003. 1. 25. 15:30경 위 인터넷 장애현상을 인지하고 긴급대책반을 구성하였고, 한국정보보호진흥원은 같은 날 16:00경 위 인터넷 장애현상이 피고 ○○가 제작, 배포한 MS SQL 2000 서버의 취약점을 이용한 공격으로 추정하고 각 ISP에 UDP(User Datagram Protocol) 1433, 1434번 포트를 차단할 것을 권고하였다.

---

1) DNS(Domain Name System)
사람이 쉽게 이해할 수 있도록 만들어진 영문자, 숫자 등으로 이루어진 웹 사이트 주소(도메인이름)를 컴퓨터가 인식할 수 있는 4단위 IP(Internet Protocol) 주소로 변환하여 연결하는 장치. 인터넷 이용자들이 도메인이름을 웹브라우저의 주소창에 입력하면 해당 사용자의 인터넷통신환경에 설정된 해당 DNS서버에 도메인이름을 질의하고, DNS서버는 사용자가 요청한 주소 정보를 시스템 내의 Cache DB에서 우선 검색하고 그 결과를 사용자에게 전송하게 되며, DNS서버의 Cache DB에서 검색하지 못한 주소정보는 DNS서버에서 'Root DNS, Top DNS, 2차 DNS, 3차 DNS' 순으로 검색하여 최종결과를 사용자에게 전송하고, 동일한 도메인에 대한 주소정보요청에 대하여 재사용이 가능하도록 Cache DB에 일정기간 저장하게 된다.

2) IDC(Internet Data Center)
컨텐츠 제공자(Contents Provider) 및 기업고객 등의 정보제공자와 정보를 사용하는 정보이용자간 정보유통을 위한 플랫폼으로 고객들에게 서버 등의 전산환경을 일괄제공하고 관리해 주는 곳을 의미한다.

㈐ 이에 각 ISP는 2003. 1. 25. 15:40경부터 17:00경 사이에 긴급조치를 실시하여 백본라우터의 UDP 1433, 1434 포트를 차단하였다.

㈑ 정보통신부와 한국정보보호진흥원은 2003. 1. 25. 20:00경 위 인터넷 장애의 원인을 MS SQL 슬래머 웜으로 확정하고, 같은 날 21:00경 메일링리스트, 시큐어메신저 홈페이지를 통해 대처방안을 공지하고 긴급경보를 발령하였다.

라. 이 사건 인터넷 침해사고의 원인: 슬래머 웜의 유입 및 전파

⑴ 슬래머 웜은 UDP 1434 포트를 통해 전파되는 404 바이트(Byte) 크기의 메모리 상주형 웜으로, 2002. 7. 24. 피고 ○○가 공표한 "MS SQL 서버 및 MSDE 2000 시스템(이하 'MS SQL 서버'라고 통칭한다)[3]의 버퍼 오버플로우 취약점[4]"을 이용하여 전파된다.

⑵ 슬래머 웜은 MS SQL 서버의 위 취약점에 대한 보안패치를 적용하지 않은 서버 중 외부로부터 UDP 1434 포트에 대한 접근이 가능한 경우에 감염되므로(방화벽에서 UDP 1434 포트를 차단한 경우에는 감염되지 않음), 슬래머 웜의 재감염과 확산을 근본적으로 예방하기 위해서는 피고 ○○에서 제공하는 MS SQL 서버용 보안패치나 MS SQL 서비스 팩3을 내려받아 설치하여야 한다.

⑶ 슬래머 웜은 UDP의 특성을 이용해 공격을 감행하므로 확산속도가 매우 빨라[5],

3) MSDE 2000 시스템(Microsoft SQL Server 2000 Desktop Engine)
개인용 PC에서는 잘 이용되지 않고 회원관리나 매출관리 등 많은 데이터 관리가 필요한 대형사업체들의 경우 널리 보급되어 있고, ○○나라의 경우 대부분의 검색 사이트나 인터넷 쇼핑몰, 뉴스 사이트 등 주요 사이트들이 대부분 MS SQL 서버 2000을 사용하고 있다.

4) 버퍼 오버플로우 취약점
버퍼란 장치들이나 프로그램들 사이에서 데이터를 주고받기 위한 임시 기억장소를 말하고, 버퍼 오버플로우란 Stack 영역에 위치한 동적 변수의 값이 할당된 영역 크기 이상으로 입력되고 그 데이터의 한계치를 체크하지 않는 경우, 정상적인 영역을 넘어 버퍼의 리턴 어드레스(Return Address) 저장 영역까지도 다른 데이터가 입력될 수 있고, 함수의 실행 후 돌아올 리턴 어드레스에서 해커가 원하는 명령어를 실행할 수 있게 되는 취약점을 말한다.

5) TCP 포트에서는 세션을 설정한 후 통신을 시작하지만, UDP에서는 세션을 설정하지 않고 데이터를 상대 주소로 전송하므로 상대방의 상황에 관계없이 패킷의 발송이 가능하여 확산속도가 빠르다.

슬래머 웜의 출현으로 전 세계의 취약점이 존재하는 MS SQL 서버의 90%가 10분 이내에 감염되었고, 국내에서는 전 세계 감염시스템의 11.8% 정도인 8,800여 개가 감염되었다.

마. 슬래머 웜에 의한 인터넷 장애

⑴ 국제회선 장애

감염된 서버로부터 발생한 공격패킷의 목적지 IP 주소는 임의로 부여되는데, 국제인터넷 주소 할당 분포상 확률적으로 93.2%의 패킷이 국제관문국에 집중되므로 각 ISP의 국제관문국에서 심한 병목현상을 유발하였으며, 이로 인해 외국으로 인터넷 접속장애 및 국내 DNS서버의 과부하를 초래하였다.

⑵ 국내 인터넷사이트 이용 장애

㈎ 슬래머 웜은 취약점이 있는 MS SQL 서버를 감염시키는데, 슬래머 웜이 작동하면 감염된 서버의 성능 및 네트워크 환경에 따라 초당 약 1만 개에서 5만 개의 UDP 패킷이 생성되어 무작위의 IP 주소로 보내진다. 공격패킷의 유입으로 감염된 서버는 다른 서버로 웜을 전파하기 위하여 공격패킷을 반복적으로 생성·전송하여, 다른 일을 하지 못하는 과부하가 발생하고 결과적으로 서버에 대한 서비스거부(Denial Of Service) 공격을 받은 것과 같은 결과를 초래한다.

㈏ 슬래머 웜에 감염된 MS SQL 서버는 무작위의 IP 주소를 선택하여 공격패킷을 발송함으로써 네트워크 과부하를 초래하여 서버 주변에 위치한 다른 비감염 서버로 접속하는 것도 불가능하게 된다. 즉 IDC 내의 일부 서버가 슬래머 웜에 감염된 경우 내부망의 트래픽 폭증으로 입주한 주요 사이트(포탈, 게임, 쇼핑몰 등)에 대한 외부 접속이 곤란해지고, 대학·연구소·기업 등의 일부 서버가 슬래머 웜에 감염된 경우도 해

당 기관 LAN의 내부 사용자는 인터넷 서비스의 이용이 곤란해진다.

㈐ 이 사건 인터넷 침해사고 당시 주요 인터넷 기간망은 DNS 응답지연 및 가입자망의 혼잡 등으로 가입자별로 상이한 인터넷 접속환경을 유발하였다. 일부 가입자는 인터넷의 접속이 지연되거나 불가능하였고 일부 가입자는 접속이 원활하였다. 2005. 1. 25. 인터넷 장애발생 초기에 많은 인터넷 사용자가 심각한 지연 및 소통 장애로 불편을 겪었으나, 슬래머 웜에 감염되지 않은 서버는 지속적으로 서비스 제공이 가능하였다. 예컨대 유닉스 버전을 사용하는 인터넷 우체국(e-Post)의 경우 속도지연은 일부 있었으나 이 사건 인터넷 침해사고에도 민원이 한 건도 없었다. 유닉스 서버를 이용하는 한미르 사이트(www.hanmir.com)의 경우 2004. 1. 25. 14:30 이후 위 사이트를 이용한 결제횟수는 1,304건, 매출액은 4,092,580원에 달하였다.

⑶ 주요 ISP들의 DNS 서버의 서비스 지연

슬래머 웜이 유발한 과다한 트래픽으로 인한 국제회선 장애로 해외 DNS 서버로 향한 정상적인 질의의 처리도 늦어져 재시도 질의(Retry Query)[6]가 급증함으로써 국내 DNS 서버 CPU의 과부하가 초래되었고 그 결과 국내 인터넷 접속도 지연되었다.

바. 이 사건 인터넷 침해사고에 대한 조사결과

피고 대한민국 산하 정보통신부의 침해사고 합동조사단은 2003. 2. 18. 이 사건 인터넷 침해사고에 대한 조사결과를 발표하였는데, 대한민국이 큰 피해를 입은 이유에 대하여, 외국에 비해 많은 MS SQL 서버가 슬래머 웜에 감염된 점, 국제회선 포화 및 Root DNS 서버의 부재에 따른 국내 DNS 서버의 과부하 현상이 외국에 비해 상대적으

6) 재시도 질의(Retry Query)
DNS가 질의를 한 후 응답이 오지 않을 경우 세 번 더 질의를 재시도(Retry)하면서 75초간 머물게 돼 그 만큼 DNS 서버 CPU의 부하를 증가시킨다. 정상적인 경우 통상 0.1초만에 처리되므로 이에 비해 750배 CPU 부하가 증가된다.

로 심각했던 점, 초고속통신망 및 정보보호가 취약한 IDC를 통한 급속한 확산, 낮은 정보보호 의식 등을 그 이유로 들었다.

[인정근거] 다툼 없는 사실, 갑 제1, 11, 17 내지 22호증(가지번호 있는 것은 가지번호 포함), 을가 제13호증, 을바 제1호증의 각 기재, 증인 오○○, 이○○의 각 증언, 변론 전체의 취지

2. 원고들의 주장

가. 주위적 청구

⑴ 피고 ISP들

피고 ISP들은 이 사건 인터넷 침해사고를 예방하기 위하여 DNS 서버의 분리·독립된 구축, 적절한 예비용량 유지, 사고 발생에 대한 적절한 대응책 마련, 모니터링 활동 등을 할 의무가 있음에도 이를 소홀히 하여 이 사건 인터넷 침해사고가 발생하였고, 이 사건 인터넷 침해사고 발생 이후에 피해의 확산을 막기 위한 적절한 조치를 취하지 아니하여 그 피해가 확산되었다.

⑵ 피고 대한민국

피고 대한민국은 정보통신망 이용촉진 및 정보보호에 관한 법률 및 정보통신기반보호법에 따른 인터넷 통신망 사업자들에 대한 적절한 관리·감독 및 인터넷 통신망의 안정적 운용계획의 수립, 침해사고 대응에 대한 준비 등을 게을리 함으로써 피고 ISP의 위와 같은 불법행위를 방치하였고, 나아가 그 이후의 복구대책의 수립과정에서도 충분한 주의의무를 기울이지 않았다.

⑶ 피고 ○○

피고 ○○가 제조, 배포한 MS SQL 서버에는 설계상의 결함 및 표시상의 결함이 있

으므로 피고 ○○는 제조물책임법 또는 일반 불법행위법에 의하여 손해배상책임이 있다.

⑷ 피고들의 고의 또는 과실에 의한 위와 같은 불법행위로 2003. 1. 25. 14:10경부터 24:00경까지 원고들이 인터넷을 이용하는 것이 불가능하였다. 따라서 피고들은 각자 ① 인터넷이용자인 별지 1-1, 1-3, 2-1, 2-3, 3-1, 4-1, 4-3, 5-1, 5-3, 6-1, 6-3, 7. 기재 각 원고들에게 재산상 손해 및 위자료로서 각 5만 원씩을, ② PC방 사업자인 별지 목록 1-2, 4-2, 5-2, 6-2. 기재 원고들 및 별지 2-2. 중 순번 1. 내지 10, 13. 원고들에게 영업손실로 인한 재산상 손해 및 위자료로서 각 30만 원씩을, ③ 원고 주식회사 ○○(별지 목록 2-2 중 순번 12.임, 이하 '원고 ○○'라 한다)에게 영업손실로 인한 재산상 손해 및 위자료로서 2,000만 원을 각 배상할 의무가 있다.

나. 피고 ISP들에 대한 예비적 청구

별지 1-1, 1-2, 1-3, 2-1, 2-2, 2-3, 3-1, 3-2, 4-1, 4-2, 4-3, 5-1, 5-2, 5-3, 6-1, 6-2, 6-3. 기재 각 원고들(별지 7. 기재 원고들 제외)은 피고 ISP들과 인터넷통신서비스 계약을 맺고 있으므로 피고 ISP들은 약관에서 정한 손해배상 약정에 따라 서비스이용 불능 시간에 따른 사용료의 3배에 해당하는 돈을 원고들에게 지급하여야 한다.

3. 원고들 중 별지 1-2, 2-2 중 순번 1. 내지 4. 6. 내지 10, 4-2, 5-2, 6-2, 1-3, 2-3, 3-1, 4-3, 5-3, 6-3, 7 기재 원고들의 청구 부분에 관한 판단

가. 주장

별지 1-3. 기재 원고들은 피고 ○○에, 별지 2-3. 기재 원고들은 피고 ○○에, 별지 3-1. 기재 원고들은 피고 ○○에, 별지 4-3. 기재 원고들은 피고 ○○에, 별지 5-3. 기재 원고들은 피고 ○○에, 별지 6-3. 기재 원고들은 피고 ○○에 각 가입하여 인터넷

통신망 서비스를 이용하고 있는 자이고, 별지 목록 7. 기재 원고들은 다른 인터넷통신망 서비스 제공업체에 가입하는 등의 방법으로 인터넷을 사용하고 있는 일반 인터넷 이용자들이라고 주장한다.

별지 목록 1-2. 기재 원고들은 피고 ○○의, 별지 2-2. 중 순번 1. 내지 4, 6. 내지 10. 기재 원고들은 피고 ○○의, 별지 4-2. 기재 원고들은 피고 ○○의, 별지 5-2. 기재 원고들은 피고 ○○의, 별지 6-2. 기재 원고들은 피고 ○○의 PC방용 서비스에 가입하여 PC방을 운영하는 사업자들이라고 주장한다.

나. 판단

그러나 이러한 원고들의 주장을 인정할 만한 아무런 증거가 없는바, 원고들이 피고 ISP들의 가입자이거나, 기타 인터넷 이용자임을 전제로 원고들의 청구는 더 나아가 살펴 볼 필요 없이 이유 없다. 따라서 이하에서는 그 외 원고들의 청구에 대하여만 판단한다.

4. 피고 ISP들에 대한 청구에 관한 판단

가. 인정사실

(1) 피고 ISP들의 인터넷망의 구성 및 관리현황

㈎ 피고 ○○

피고 ○○의 인터넷망은 크게 백본망[7], 국내연동망[8], 국제연동망[9], 가입자망, DNS, IDC로 구분된다.

---

7) 백본망
백본망은 계층구조로 이루어진 인터넷망에서 주요 노드들을 고속의 통신회선으로 상호 접속하여 망 전체의 데이터를 전송하는 중추회선망임.

8) 국내연동망
국내의 다른 ISP의 인터넷 망과 트래픽을 전달하기 위하여 구성된 망임.

9) 국제연동망
국제인터넷서비스를 제공하기 위한 네트워크 장비 및 회선.

① 백본망

-범위: 센터노드(혜화・구로)와 전국 20개 주지역 노드의 40개 중계라우터간과 센터IDC(혜와・구로) 사이의 인터넷 트래픽을 중계하는 회선망까지로 주지역노드 하단의 가입자망 및 국내외 연동망과 연동되어 있음.

-회선의 트래픽 현황: 백본망의 입・출력 트래픽은 관리기준(회선용량의 50%를 적정 운용치, 회선용량의 70%를 운용임계치로 설정)보다 낮은 이용율을 유지하고 있음.

-관리시스템: 일종의 경보관리시스템으로서 라우터와 교환기 등 장비의 장애관리, 성능 및 트래픽 관리 등을 구현하여 각각 발생한 관리기준지표 초과 정보들을 통합적으로 조회할 수 있도록 구성된 종합운용관리시스템(KOSMOS)을 운용하고 있으며, 인터넷의 속도측정을 위해 DQMS(Data network Quality Management System), CQMS(Customer Quality Management System), 속도측정시스템을 구축하여 운영 중임.

② 국내연동망

-범위: 센터노드(혜화・구로), 센터IDC(혜화・구로), KIX(Kornet Internet eXchanger: 혜화・구로) 사이의 회선, KIX에서 다른 ISP 등과 연동된 회선까지임.

-회선의 트래픽 현황: 센터노드에서 KIX까지 회선용량 대비 트래픽은 입・출력 각각 11.8%, 38.7%를 유지하고 있고, KIX라우터에서 센터IDC 라우터까지는 입・출력 각각 34.7%, 2.2%를 유지하고 있음. KIX에서 다른 ISP 라우터까지 회선용량 대비 트래픽은 입・출력 각각 38.6%, 18.9% 수준임.

-관리시스템: 국내연동망을 포함한 코넷망을 관리하기 위해 종합운용관리시스템 KOSMOS를 운영.

③ 국제연동망

-범위: 센터노드와 연결된 국제허브, 스위치(L2), 국제 G/W(Gate Way), 해외 POP(Point Of Presence) 및 외국 ISP 사이의 장비와 회선까지임.

-회선의 트래픽 현황: 2003년 1월경 센터노드에서 국제허브까지 회선용량 대비 평균 트래픽은 회선용량의 33~40%로 50% 이하로 유지됨. 국제회선의 경우 회선당 70%를 기준으로 증설여부를 결정함.

-관리시스템: 국제 연동망을 포함한 코넷망을 관리하기 위해 종합운용관리시스템 KOSMOS를 운영.

④ 가입자망

-범위: 지역기간망(주노드와 지역노드간의 중계망으로 센터노드와 접속되지 않음)과 가입자 Access망(노드와 가입자를 수용하는 망이며 ADSL, Ntopia 등 인터넷 서비스 상품별로 구분)까지임.

-관리시스템: 각 지사에 NAS-EMS(Equipment Management System), DSLAM-EMS 등을 설치하여 장비 및 회선의 이상유무를 감시하고 있음.

⑤ DNS

-범위: 백본 라우터, L4스위치, DNS 서버군 및 이들 장비 사이의 회선까지임. 전국에 20대의 서버가 있음.

-회선의 트래픽 현황: DNS 회선의 트래픽은 회선용량의 35% 수준을 유지하고 있음.

-관리시스템: SMS(서버관리시스템)을 통해 DNS 운용상태 정도(CPU 부하율, 메모리사용율, 디스크사용율 등)을 종합적으로 관리하고 있음.

⑥ IDC

-범위: 혜화 및 구로 센터라우터와 연결된 수도권 IDC 4개와 백본에 직접 연결된 지역

IDC 8개 등 12개로 구성됨.

-회선의 트래픽 현황: 12개 IDC는 전체적으로 가입자스위치와 중계스위치간은 회선용량 대비 최번시 트래픽이 16.5%, 중계스위치와 백본라우터간은 25.5%, 백본라우터와 코넷라우터간은 모두 50% 이하를 유지하고 있음.

-관리시스템: IDC 상황실에서 백본라우터와 중계스위치간 네트워크 연결회선, 중계스위치와 가입자스위치간 네트워크 연결회선, 가입자스위치와 고객서버간 네트워크 연결회선을 관리하고 있음.

㈏ 피고 ○○

피고 ○○의 인터넷망은 크게 백본망, 국내연동망, 국제연동망, 가입자망, DNS, IDC로 구분된다.

① 백본망

-범위: 센터노드(동작·서초)와 전국 10개 주지역노드의 20개 중계라우터간의 인터넷 트래픽을 중계하는 회선망까지로 국내연동망, 국제연동망, 가입자망, IDC와 연동되어 있음.

-회선의 트래픽 현황: 센터노드와 주지역노드간의 입·출력 트래픽은 최대 68% 정도이며, 피고 ○○의 관리기준상의 운영임계치 70%를 초과하지는 않음.

-관리시스템: 백본망 전체 장비에 대한 장애 및 성능상태, 네트워크 회선별 트래픽 변동상태 등에 대한 정보를 표시하고, 이상 발생시 가시경보와 가청경보를 통해 알려주는 종합망관리시스템을 서울 동작국사 2층 종합망상황실에 설치·운용하고, 운용요원에 의하여 24시간 모니터링 체제를 시행함.

② 국내연동망

-범위: 백본망 센터노드(동작・서초)와 국내 G/W 센터노드(동작・서초)간의 라우터와 이들 장비 간의 회선, 국내 G/W 센터노드와 국내의 다른 ISP의 라우터와 이들 장비 간에 연동된 회선까지임.

-관리시스템: 국내연동망을 포함한 하나넷 망을 관리하기 위한 종합관리시스템을 운용하고 있음.

③ 국제연동망

-범위: 동작 센터라우터와 연결된 L4 스위치, 국제 G/W, 해외 POP 및 이들 장비간의 회선을 포함함.

-회선의 트래픽 현황: 동작센터와 국제 G/W까지 회선용량 대비 최번시 트래픽은 25%, IDI와 국제 G/W 간은 8%로 내부망 관리기준 50%이하로 유지됨.

-관리시스템: 국제연동망을 포함한 하나넷 망을 관리하기 위한 종합관리시스템을 운용하고 있음.

④ 가입자망

-범위: 백본라우터 하단에 연동되는 모든 망장비 및 회선까지임.

-회선의 트래픽 현황: 평상시 트래픽이 회선용량의 50% 이내임.

-관리시스템: 가입자망을 포함한 하나넷 망을 관리하기 위한 종합관리시스템을 운용하고 있음. 각 지역국사에서 각 장비의 EMS 서버들을 통해 B-RAS(또는 가입자 수용라우터, 가입자집선 스위치)이하 구간의 장비를 관리하고 있으며, 종합망관리시스템에 접속하여 관할 지역 장비들의 이상유무를 점검할 수 있음.

⑤ DNS

-범위: 백본 라우터, LBS스위치, L4스위치, DNS서버군 및 이들 장비 사이의 회선까지

임. 23대의 DNS 서버가 있음.

-회선의 트래픽 현황: DNS 서버와 L4 스위치간 트래픽은 개인가입자용 1차 서버의 경우 회선용량 대비 0.1% 수준임.

-관리시스템: DNS 서버를 포함하여 인터넷 서비스 제공과 관련된 서버의 CPU 사용율, 네트워크 통계 등 상태정보와 성능정보를 모니터링하기 위한 서버 시스템 모니터링 시스템을 24시간 운용하고 있음.

⑥ IDC

-범위: 서울에 1개소 존재.

-회선의 트래픽 현황: 회선용량대비 50% 이하임.

-관리시스템: IDC 내의 관리시스템을 통해 백본라우터부터 백본스위치의 연결회선까지를 관리하고, 관리시스템은 주요네트워크 구간 트래픽 및 네트워크장비 감시 등의 역할을 수행하며, 종합망상황실과 연동하지 않고 IDC 상황실에서 별도로 24시간 운용하고 있음.

㈐ 피고 ○○

피고 ○○의 인터넷망은 크게 백본망, 국내 연동망, 국제 연동망, 가입자망, DNS, IDC로 구분된다.

① 백본망

-범위: 센터노드(서울센터)와 전국의 6개 주지역노드(국제노드 포함) 및 2개의 보조지역노드 중계라우터 사이의 인터넷 트래픽을 중계하는 회선망까지임.

-회선의 트래픽 현황: 피고 ○○의 트래픽 관리기준인 회선사용율 50% 미만임.

-관리시스템: 서울센터 내에 구축되어 있는 NOC 관제센터에서 백본망 및 전국 주요

국사의 모든 상황을 실시간 감시할 수 있는 시스템을 구축하여 운용하고 있으며, 주지역노드에서 가입자단 라우터까지 모든 인터페이스에 대한 트래픽 추이를 실시간 모니터링하고 있음.

② 국내연동망

-범위: 센터노드의 라우터와 국내 다른 ISP사이에 연동된 회선까지임.

-회선의 트래픽 현황: 센터노드에서 다른 ISP 사이 회선의 회선용량 대비 트래픽은 입·출력 각 97.7%, 54.8%로 회선용량 대비 트래픽 비율이 높음. 그러나 이 구간은 연동된 사업자와의 협의에 의하여 증설이 결정됨.

-관리시스템: 국내 연동망을 포함한 전체망 관리를 위해 종합관제센터에 관리시스템을 설치하여 운용함.

③ 국제연동망

-범위: 서울 IDC 내에 설치되어 있는 2대의 백라우터, 국제 G/W라우터, 이들 사이에 설치되어 있는 L7스위치 및 L2스위치, 미국 POP에 설치되어 있는 2대의 POP라우터 및 이들 장비간의 회선과 해외 ISP간의 연동망을 포함.

-회선의 트래픽 현황: 피고 ○○의 국제회선 관리기준인 80% 이하임.

-관리시스템: 국제 연동망을 포함한 전체망 관리를 위해 종합관제센터에 관리시스템을 설치하여 운용함.

④ 가입자망

-범위: 연동망, 백본, 스위치, CMTS(Cable Modem Termination System)까지는 중앙관리시스템에서 관리하고 있으며, 가입자망 관리에 대해서는 기본적으로 무인국사 기준으로 장애 발생시 중앙관리센터 요원이 1차 원격조치를 실시하고 조치가 불가능할 경

우 각 지사의 요원이 현장으로 출동하여 조치함. 월1회씩 각 국사 방문점검 실시.

⑤ DNS

-범위: 2대의 백본라우터, 2대의 L4스위치, 1대의 L2스위치, 11대의 DNS 서버로 구성.

-회선의 트래픽 현황: 라우터와 L4스위치간 평균트래픽은 회선용량 대비 1.6% 수준임.

-관리시스템: DNS 시스템 내부에 서버의 운영상태 등을 모니터링하는 응용프로그램을 설치하여 DNS 서버를 관리하고 있음.

⑥ IDC

-범위: 서울에 1개.

-회선의 트래픽 현황: 구간 전체적으로 볼 때 회선의 트래픽은 50% 이하임.

-관리시스템: 종합망상황실에서 IDC의 트래픽 및 네트워크상태, 장애 등 모든 상황을 종합적으로 관리하고 있음.

㈑ 피고 ○○

피고 ○○의 인터넷망은 크게 백본망, 국내 연동망, 국제 연동망, DNS, INC로 구분된다.

① 백본망

-범위: 센터노드(분당 1・2), 전국의 16개 주지역노드, 25개 중계라우터간과 국제 연동망, 국내 연동망, IDC망을 수용하는 백본스위치간의 인터넷 트래픽을 중계하는 회선망까지로서 주지역노드 하단에 위치한 가입자망(MISP)과 국내 타 ISP의 인터넷망, 국제 연동망, IDC망과 연동됨.

-회선의 트래픽 현황: 피고 ○○은 회선용량의 80%를 운용임계치로 설정하여 운영하는데, 백본망의 트래픽은 회선용량의 80% 이하임.

-관리시스템: 접근제어시스템(TACACS)을 상시 운영함으로써 외부의 침입으로부터 백본라우터를 보호하고, What's Up이라는 상용소프트웨어를 이용하여 주노드구간으로 연결된 회선단위별로 입출력 트래픽 상태를 감시하며, 회선별로 아이콘을 생성하여 접속불가시 알람이 발생하도록 설정함. 백본망의 트래픽은 MRTG를 이용하여 일간, 주간, 월간, 년간으로 관리중이며, 회선별로 일간 최대트래픽을 별도 데이터베이스화하여 회선증설을 위한 검토자료로 관리하고 있음.

② 국내연동망

-범위: 피고 ○○의 중계노드에서 다른 ISP까지 평소 트래픽은 전체 연동망 대비 82.7%로 자체기준 80%를 초과하지만 이 구간은 사업자들간 협의에 의하여 증설이 결정되어 피고 ○○이 회선용량을 임의로 정할 수 없음.

-관리시스템: What's Up이라는 상용 소프트웨어를 이용하여 국내구간으로 연결된 회선단위별로 입출력 트래픽 상태를 감시하고, 트래픽은 MRTG를 이용하여 일간, 주간, 월간, 년간으로 관리중이며, 회선별로 일간 최대트래픽을 별도 데이터베이스화하여 회선증설을 위한 검토자료로 관리하고 있음.

③ 국제연동망

-범위: 국제G/W와 미국POP 라우터를 중심으로, 센터노드 스위치와 국제G/W간 회선, 국제G/W와 해외 ISP간 회선, 미국POP와 미국ISP간 회선으로 구성됨.

-회선의 트래픽 현황: 피고 ○○의 자체기준인 회선용량대비 80% 미만임.

-관리시스템: What's Up이라는 상용 소프트웨어를 이용하여 국제구간으로 연결된 회선단위별로 입·출력 트래픽 상태를 감시하고, 트래픽은 MRTG를 이용하여 일간, 주간, 월간, 년간으로 관리중이며, 회선별로 일간 최대트래픽을 별도 데이터베이스화하여

회선증설을 위한 검토자료로 관리하고 있음.

④ DNS

-범위: 백본스위치, L4스위치, DNS서버군 및 이들 장비 사이의 회선까지이며, 2대의 백본스위치, 2대의 L4스위치, 7대의 DNS서버로 구성되어 있음. DNS서버는 유닉스 장비임. 다른 ISP들과 다르게 데이터베이스서버와 캐쉬(Cache) 서버를 구분하지 않고 있음.

-회선의 트래픽 현황: 백본스위치와 L4스위치간의 회선용량 대비 평균트래픽은 3.4%, 백본스위치와 DNS서버간의 평균트래픽은 1.49%, DNS서버와 L4스위치간 평균트래픽은 1.31%임.

-관리시스템: 백본스위치에서 DNS 질의값이 아닌 패킷에 대하여 필터링하고 있고, DNS 시스템 내부에 서버의 운영상태 등을 모니터링하는 응용프로그램을 설치하여 DNS서버를 관리하고 있음.

⑤ IDC

-범위: 분당본사 1개, 부산 1개.

-회선의 트래픽 현황

분당IDC: 회선용량대비 평균트래픽이 중계스위치와 백본스위치간은 11.2%, 백본스위치와 백본망간은 18.7%, 중계스위치와 고객서버와는 4.6%임.

부산IDC: 회선용량대비 평균트래픽이 중계스위치와 백본스위치간은 10%, 백본스위치와 백본망간은 23%, 중계스위치와 고객서버와는 4.2%임.

-관리시스템: 인터넷망운영실에서 트래픽 및 네트워크장비감시, 장애감시 등 네트워크의 모든 상황을 실시간으로 24시간 감시하고 있음.

⑵ 대응조치(2003. 1. 25.)

㈎ 피고 ○○

14:31 인터넷망관리센터에서 KOSMOS의 발생경보 및 트래픽 모니터링을 통하여 국제 인터넷망의 이상발생을 인지함.

15:25 IDC에서 1차로 이상 패킷을 발생시키는 353개의 포트를 선별하여 고객의 동의를 얻은 후 서비스를 중단시킴.

15:31 UDP 1434 포트를 통한 유해 트래픽 제거를 위해 국제백본의 허브에 ACL(Access Control List)를 적용하여 허브 이후부터의 병목현상을 차단.

16:45 국제허브에 연결된 GIX를 통해 나오는 슬래머 웜을 차단하기 위하여 GIX에 연결된 국제 G/W의 포트를 차단함.

15:43~18:14 백본망의 주노드 중계 라우터에 슬래머 웜 패킷을 차단하기 위하여 ACL 조치를 시행하여 슬래머 웜이 백본망 내로 유입되지 못하게 함.

17:00~18:30 IDC에서 이상패킷의 확산방지를 위하여 기가라우터 및 기가스위치에 ACL을 적용하여 UDP 1434 포트의 유입 및 출입을 차단함.

22:00~23:00 IDC 주요감염서버 고객을 대상으로 전화, 메일, 홈페이지를 통하여 지속적으로 패치를 독려하고, IDC 홈페이지에 신종 슬래머웜에 대한 경보게재 및 MS 서비스 팩 및 슬래머 웜 백신프로그램 다운로드 설정, 패치 적용방법 지원 및 패치여부 확인 등을 시행하고, 패치가 완료된 서버는 네트워크를 재연결하여 서비스 정상화를 유지함.

㈏ 피고 ○○

14:40경 트래픽관리시스템, Ping 감시시스템, 라우터CPU, 감시시스템 경보발생을 통해

전체 백본망 및 국내 연동망, 국제 연동망의 이상 발생 확인.

15:00 네트워크 비상대책반 및 재해대책반 가동, 비상연락망을 이용하여 내부인력, 보안업체, 네트워크 업체 비상출동.

16:00 장애의 원인이 UDP 1434 포트의 트래픽 급증임을 파악.

16:24 추가적인 이상 트래픽의 확산 방지를 위해 국제 연동망 구간 차단조치 실시.

16:40 국내연동망 구간 차단조치 실시.

16:45 IDC 백본라우터에 UDP 1434 포트 차단을 위한 ACL을 적용함.

16:45~17:30 전체 백본망과 국내연동망, 국제연동망, 전국 가입자 수용라우터의 이상트래픽 관련 UDP 1434 포트에 대한 ACL을 적용함.

18:00 국내연동망 구간 복구.

19:35 국제연동망 구간 복구.

18:00 IDC 내부 트래픽을 분석하여 이상 패킷을 발생시키는 305개의 서버를 차단하고 서비스를 중단시킴.

20:00 포트차단 및 MS SQL 패치를 입수한 후 감염서버를 보유한 122개 고객사에 비상연락망을 가동, 홈페이지 팝업창을 통한 긴급 패치 고지를 함.

㈐ 피고 ○○

14:34 DOC 모니터링시스템의 서울노원, 동대문 장애발생으로 장애상황 인지.

15:15~16:00 서울센터의 백본라우터에 해당 UDP 패킷을 차단하는 ACL을 적용하고, Netflow 장비의 ACL Log 확인결과 목적지 주소와 포트가 모두 1434 임을 파악.

16:20~17:00 백본 및 전체지역에 ACL을 적용함.

16:20~18:30 IDC 내부 트래픽을 분석하여 19개의 고객서버에서 이상 패킷의 발생을

확인하고 고객동의를 받은 후 감염서버 포트의 제거 및 서비스를 중단하고, 감염서버의 포트제거 후 서비스를 정상복구함.

17:00~18:30 일부 지역 CMTS의 경보 발생, 슬래머웜의 확산 및 장애재발 방지를 위해 CMTS의 UDP 1434 포트의 차단을 실시.

19:00~21:00 포트차단 후 주요 감염서버 고객을 대상으로 전화, 메일, 홈페이지를 통해 패치를 독려함.

㈑ 피고 ○○

14:30 이상 패킷 확인

14:45 정보보호기술팀, 정보망운용팀, DNS서버운용팀 비상근무 체제로 전환

15:00 DNS 과부하

17:00 DNS 서버 3대 추가

15:00~17:30 국제G/W, 주요G/W구간 백본에서 UDP 1434 포트 차단

19:00 DNS 부하증가

22:00 DNS 서버 4대 추가

23:30 DNS CPU 정상회복

㈒ 피고 ○○

14:10 국제망 트래픽의 속도저하 이상 발견

14:40 방화벽 집중관리 요청 및 한빛 NOC로 전문보안 담당자 출동요청

18:30 국제망 및 이상 트래픽가입자 포트 필터링, 과다 트래픽 발생 가입자 포트 차단

18:45 국내 인터넷 정상 작동, 일부 타 ISP 문제로 연동망 접속 안됨.

19:35 피고 ○○ 국제연동망 구간 복구(피고 ○○은 피고 ○○의 회선을 임차하여 사

용하고 있음)

㈐ 피고 ○○

14:40 인터넷망운용실의 장애관리시스템에서 국제망의 이상패킷 증가 등을 감지.

15:40~17:00 분당 IDC 내부 트래픽을 분석하여 150개 고객서버에서 이상 패킷을 발생시키는 것을 확인하고 이상패킷을 유입시키는 150개의 포크를 우선 제거한 후 고객에게 통보함.

17:48~17:50 국제연동망 라우터에 ACL을 적용.

18:13~18:19 국내연동망 라우터에 ACL을 적용.

18:43~19:33 분당2 스위치 2대 및 IDC망 스위치 2대에 ACL을 적용.

2003. 1. 25. 17:00~1. 26. 18:00 IDC 감염서버의 고객에서 전화를 통해 패치를 설치하도록 하고, 서비스 팩 및 패치를 완료한 고객에 한하여 네트워크 포트에 재연결.

⑶ DNS 서버 실험

정보통신부의 담당자와 한국정보통신기술협회의 전문가들은 이 사건 인터넷 침해사고와 관련하여 2003. 8. 12. 99%의 부하에서 피고 ○○의 DNS 서버가 정상적으로 동작할 수 있었는지에 대한 실험을 실시하였다. 이 사건 인터넷 침해사고 당시와 동일한 DNS 서버는 CPU 부하율이 99% 이상인 상황에서도 평균 응답율이 94% 이상이었다.

⑷ 슬래머 웜에 대한 대응조치

슬래머 웜에 의한 확산을 근본적으로 예방하고 재확산을 막기 위해서는 MS SQL 서버에 보안패치를 설치해야 한다. 한편 네트워크에서 슬래머 웜을 차단할 수 있는 조치로는 ACL(Access Control List)로서 이는 라우터에서 트래픽에 대한 제어를 할 수 있는 방법이다. ACL을 이용하여 1434 포트가 할당된 IP 주소를 차단하는 것이 가능하

나, 이러한 차단방법은 사후적으로만 가능하다. 슬래머 웜의 확산 이전에 13만 개에 달하는 서비스포트 중 사전에 특정 서비스포트를 차단하는 조치를 할 수는 없다.

⑸ 피고 ISP들의 이용약관

㈎ 피고 ○○

제21조(손해배상)

① ○○는 고객에게 책임 없는 사유로 서비스를 이용하지 못한 사실을 고객이 ○○에 통지한 때(그 전에 ○○가 그 사실을 안 경우는 알게된 때)로부터 3시간 이상 계속 서비스를 제공하지 못하거나 월 누적장애 시간이 24시간을 초과하여 고객이 손해를 입은 경우 고객의 청구에 의하여 배상합니다.

② 제①항의 손해배상금액은 고객이 청구 받은 최근 3개월분(3개월 미만인 경우에는 해당기간 적용) 요금의 일 평균액을 24로 나눈 시간당 평균액에 이용하지 못한 시간 수를 곱하여 산출한 금액의 3배를 이용고객과 협의하여 배상합니다.

③ 단, 서비스장애가 이용고객이 직접 구입한 단말장치 등의 불량으로 발생하거나, 서비스를 제공하지 못할 불가항력 또는 이용 고객의 고의나 과실로 인하여 발생한 경우에는 그러하지 아니합니다.

㈏ 피고 ○○

제20조(손해배상)

① ○○은 고객에게 책임이 없는 사유로 서비스를 이용하지 못한 사실을 고객이 ○○에 통지한 때(그 전에 ○○이 그 사실을 안 경우는 알게된 때)로부터 3시간 이상 계속 서비스를 제공하지 못하거나 월 누적 장애시간이 24시간을 초과하여 고객이 손해를 입은 경우 고객의 청구에 의하여 배상합니다. 다만, 그 손해가 천재지변 등 불가항력이나 고객의 고의 또는 과실로 인하여 발생한 경우, 또는 전기통신서비스의 특성상 불가피한 사유나 타사 서비스 및 단말기기 등의 장애에 의해 통합서비스를 이용하지 못한 경우에는 그렇지 않습니다.

② 제1항의 손해배상금액은 고객이 청구받은 최근 3개월(3개월 미만인 경우에는 해당기간 적용) 요금의 일 평균액을 24로 나눈 시간당 평균액에 이용하지 못한 시간수를 곱하여 산출한 금액의 3배를 고객과 협의하여 배상합니다. 이 경우 이용하지 못한 시간이 1시간 미만인 경우에는 1시간으로 봅니다.

제21조(면책)

① ○○은 서비스 이용장애가 천재지변 또는 이에 준하는 사유로 인하여 불가항력적으로 발생한 경

우와 서비스의 효율적 제공을 위한 초고속 정보교환망 관련 공사 등의 사유로 고객에게 사전 통보한 이후 발생한 경우에는 그 책임이 면제됩니다.

㈐ 피고 ○○

제31조(손해배상의 범위)

① 회사의 귀책사유로 이용자가 서비스를 이용하지 못하는 경우에는 이용자가 그 사실을 회사에 통보하여 확인한 때(그 전에 회사가 그 사실을 알았거나 알 수 있게 된 때)로부터 3시간 이상 정상적인 사용이 불가할 경우 이용 요금을 기준으로 시간당 요금의 3배까지 보상하되 당월 이용요금의 범위 내에서 적용합니다. 단수가 1시간 미만인 경우에는 1시간으로 합니다. 배상기준: 시간당 배상=기본이용료/30(31)일/24시간, 단, 방문이 필요한 AS에 대해서는 고객과 ○○간의 방문약속 시간을 기준으로 합니다. 하기의 사유에 대해서는 배상에서 제외합니다.

ㄱ. 공지된 예정된 장애로 인한 서비스 중단 및 AS 지연

ㄴ. 고객의 귀책사유로 인해 AS가 지연되는 경우(PC, O/S, 고객의 AS 연기요청, 고객과의 연락두절 및 이와 유사한 사유로 판단되는 경우)

② 회사가 제공하는 서비스 중 무료 서비의 경우에는 손해배상에 해당되지 않습니다.

③ 회사는 그 손해가 천재지변 등 불가항력이거나 이용자의 고의 또는 과실로 인하여 발생한 때에는 손해배상을 하지 아니합니다.

㈑ 피고 ○○

제38조(손해배상의 범위)

① 회사는 회사의 귀책사유로 이용고객이 서비스를 이용하지 못하는 경우, 이용고객이 그 사실을 회사에 통보하여 확인한 때(그 전에 회사가 그 사실을 알았거나 알 수 있게된 때)로부터 계속 3시간 이후의 서비스 중지시간 및 월별(매월 1일부터 말일 기준) 서비스 장애발생 누적시간이 24시간을 초과할 경우에는 기본이용료를 포함한 최근 3개월(3개월 미만인 경우는 해당기간 적용)의 1일 평균요금을 24로 나눈 요금에 서비스제공 중지시간을 곱하여 산출한 금액의 3배를 배상합니다. 이 경우 단수가 1시간 미만인 경우에는 1시간으로 합니다.

② 회사는 그 손해가 천재지변 등 불가항력이거나 이용고객의 고의 또는 과실로 인하여 발생한 때에는 손해배상을 하지 아니합니다.

㈒ 피고 ○○

제38조(손해배상의 범위)

① 회사의 귀책사유로 이용자가 서비스를 이용하지 못하는 경우에는 이용자가 그 사실을 회사에 통보하여 확인한 때(그 전에 회사가 그 사실을 알았거나 알 수 있게된 때)로부터 계속 3시간 이상의 서비스 중지시간 및 월 장애 누적시간 24시간을 초과한 경우에 대하여 기본이용료를 포함한

최근 3개월(3개월 미만인 경우에는 해당기간 적용)의 1일 평균요금에 서비스 제공 중지시간을 24로 나눈 수를 곱하여 산출한 금액의 3배를 배상합니다. 이 경우 단수가 1시간 미만인 경우에는 1시간으로 합니다. 단 4시간 이하일 경우에도 일정규모 지역장애의 경우 홈페이지 공지를 통해 보상할 수 있습니다.

② 회사는 상기의 규정에도 불구하고 다음 각호의 1의 사유를 입증하는 경우에는 요금감면 또는 손해배상책임이 감면될 수 있습니다.

ㄱ. 전시, 사변, 천재지변 또는 이에 준하는 국가비상사태 등 불가항력으로 인한 경우

ㄴ. 전기통신서비스의 특성상 불가피한 사유로 서비스 제공이 불가능한 경우

ㄷ. 이용자의 고의 또는 과실로 인하여 발생한 경우

㈏ 피고 ○○

제39조(손해배상의 범위)

① 회사의 귀책사유로 이용고객이 연속하여 3시간 이상 혹은 월별(매월 1일부터 말일기준) 누적시간 24시간을 초과하여 서비스를 이용하지 못할 경우 회사는 배상책임이 있습니다.

② 손해배상액의 기준 적용은 다음의 조건에 따릅니다.

ㄱ. 배상시간은 서비스를 이용하지 못하는 경우, 이용자가 그 사실을 회사에 통보하여 확인한 때(그 전에 회사가 그 사실을 알았거나 알 수 있게된 때)로부터 연속하여 3시간 이상 서비스를 이용하지 못하는 시간으로 합니다.

ㄴ. 손해배상은 1일 평균요금에 서비스 중지시간을 24로 나눈 수를 곱하여 산출한 금액의 3배로 합니다. 이 경우 단수가 1시간 미만인 경우에는 1시간으로 합니다.

③ 1년 이상의 장기계약을 한 이용자가 계약기간 중에 해지할 경우, 회사는 이용자에게 회사가 별도로 정하는 바에 의하여 위약금을 부과하며, 이용자가 위약금을 납부하지 않을 경우에는 계약의 해지가 성립되지 아니합니다.

④ 이용자에게 요금 등의 체납이 있는 경우, 회사는 이용자에 대한 손해배상액에서 체납금액을 우선 공제 후, 잔여액을 이용자에게 배상합니다.

⑤ 회사는 그 손해가 천재지변 등 불가항력적이거나 이용자의 고의 또는 과실로 인하여 발생한 경우 및 무료서비스인 경우에는 손해배상을 아니합니다.

제41조(면책)

① 회사는 천재지변 또는 이에 준하는 불가항력, 국가기간통신망의 이상으로 인하여 서비스를 제공할 수 없는 경우에는 책임을 면합니다.

[인정근거] 갑 제1, 6호증, 을가 제1 내지 4, 5, 6, 11호증, 을나 제1 내지 5호증(가지번호 있는 것은 가지번호 포함)의 각 기재, 증인 이○○, 한○○의 각 증언, 변론 전체

의 취지

나. 불법행위에 기한 손해배상청구에 관한 판단

⑴ 원고들은 피고 ISP들의 DNS 관리실패가 이 사건 인터넷 침해사고의 유발 및 그 확대 원인이라고 주장하나 이를 인정할 만한 증거가 없고, 오히려 위 기초사실 및 인정사실에서 본 바와 같은 다음과 같은 사정, 즉 슬래머 웜에 감염된 서버는 DNS 서버를 경유하지 않고 무작위의 숫자를 조합하여 만든 임의의 IP 주소로 끊임없이 패킷을 발송하므로 슬래머 웜으로 인한 인터넷 장애와 DNS는 직접적인 관련은 없는 점, 슬래머 웜으로 인해 피고 ISP들의 DNS 서버 자체가 다운되어 서비스를 제공하지 못하였던 것은 아니고 슬래머 웜에 의해 유발된 과도한 트래픽으로 국외회선에 장애가 발생하면서 정상적인 DNS 서버의 서비스까지도 지연된 것에 불과했던 점, 피고 ○○을 제외한 나머지 피고 ISP들은 이 사건 인터넷 침해사고 당시 DNS 서버와 IDC 서버를 분리하여 운영하고 있었고, 피고 ISP들의 평소 DNS의 트래픽은 모두 관리 기준 이하로 피고 ISP들은 DNS의 트래픽의 이상 유무, 트래픽량 등을 감시하여 회선의 증선여부를 판단할 수 있는 관리시스템을 구축하고 있었던 점, 피고 ISP들이 DNS 서버의 용량을 확장하더라도 초당 약 1만 내지 5만 개의 UDP 패킷을 생성하여 무작위의 IP 주소로 보내는 슬래머 웜의 특성상 과다 트래픽으로 인한 시스템 장애를 예방할 수는 없는 점 등을 고려할 때 피고 ISP들의 DNS의 관리 실패가 이 사건 인터넷 침해 사고의 발생 및 확대의 원인이라고 보기는 어렵다.

⑵ 또한 원고들은 피고 ○○의 경우 국제관문국라우터에서 미할당된 IP주소에 대한 트래픽을 차단하도록 설정하여 국제회선 자체에 대한 소통장애가 없었으므로 이러한 조치를 취하지 아니한 다른 피고 ISP들은 슬래머 웜의 확산에 과실이 있다고 주장한

다. 갑 제1호증의 기재에 의하면 피고 ○○의 경우 이 사건 인터넷 침해사고 당일 다른 ISP에 비해 국제망으로 유출된 트래픽의 변동폭이 적었다는 것은 인정된다. 그러나 이러한 조치로 인하여 국제회선의 장애에 따른 DNS 서버의 영향도 없었다는 것인지 여부가 불명할 뿐더러, 을가 제7호증의 1, 을나 제4호증의 22의 각 기재에 의하면 피고 ○○도 2002. 5. 3. 이미 미할당된 IP 주소에 대한 트래픽을 차단하도록 설정하고 있었던 사실, 원고들이 주장하는 조치를 취한 피고 ○○도 2003. 1. 25. 15:00 DNS의 과부하로 서버를 증설한 사실이 인정될 뿐인바, 피고 ISP들에게 미할당된 IP 주소를 차단하지 아니한 과실이 있다고 보기 어렵다.

⑶ 나아가 위 기초사실 및 위 인정사실에 나타난 다음과 같은 사정, 즉 이 사건 인터넷 침해사고의 1차적인 책임은 MS SQL 서버의 취약점을 악용한 슬래머 웜의 배포자 및 MS SQL 서버의 취약점이 알려졌음에도 보안패치를 설치하지 않은 인터넷 업체의 서버관리자들에게 있는 점, 피고 ISP들은 이 사건 인터넷 침해사고가 발생한 직후 관리시스템을 통해 이상패킷을 확인하고 그 원인파악에 착수하여 슬래머 웜의 감염통로인 UDP 1434 포트를 차단하는 등 응급조치를 취한 점, 슬래머 웜의 재감염과 확산을 근본적으로 예방하기 위해서는 피고 ○○에서 제공하는 MS SQL 서버용 보안패치나 MS SQL 서비스 팩3을 설치하여야 하는데, 피고 ISP들은 인터넷 업체들에게 인터넷을 이용하는데 필요한 환경만 제공할 뿐이므로 자신들이 관리하는 IDC 입주업체들에게는 전화나 이메일 등을 통해 보안패치 등의 설치를 독려하거나 홈페이지 게시 등을 통하여 자신들의 관리범위 내에서 슬래머 웜의 재감염 및 확산을 방지하기 위한 노력을 다하였다고 보이는 점 등을 고려할 때 피고 ISP들이 이 사건 인터넷 침해사고의 유발 및 그 확산에 대하여 어떠한 과실이 있다고 보기는 어렵다.

⑷ 그러므로 피고 ISP들에 대한 불법행위에 기한 손해배상청구는 이유 없다.

다. 약관에 기한 손해배상청구에 관한 판단

⑴ 피고 ISP들은, '고객에게 책임없는 사유로 3시간 이상 계속 서비스를 이용하지 못한 사실을 통지받고도 3시간 이상 계속 서비스를 제공하지 못한 경우, 고객이 청구받은 최근 3개월분 요금의 일 평균액을 24로 나눈 시간당 평균액에 이용하지 못한 시간수를 곱하여 산출한 금액의 3배를 배상'하기로 약관에 규정하고 있는바, 이러한 약관규정은 일종의 손해배상액의 예정으로서, 채권자는 채무자의 채무불이행 사실을 증명하면 손해의 발생 및 그 액을 증명하지 아니하고 예정배상액을 청구할 수 있다(대법원 2000. 12. 8. 선고 2000다50350 판결 등 참조).

그런데 피고 ISP들의 약관규정은 위 피고들의 의무불이행 즉 3시간 이상의 서비스 제공불능을 그 요건으로 하면서 통상적인 채무불이행에 의한 손해배상 범위라 할 수 있는 이용하지 못한 시간 동안의 이용요금을 넘어서서 3배의 배상을 규정하고 있는바, 피고 ISP들에게 약관상 손해배상책임이 인정되기 위해서는 적어도 피고들의 귀책사유로 3시간 이상 서비스를 제공하지 못한 경우를 그 요건으로 한다고 봄이 상당하다.

⑵ 먼저 이 사건 인터넷 침해사고 당시 피고 ISP들의 의무이행불능이 있었는지 여부에 관하여 본다. 위 인정사실에서 본 바와 같이 이 사건 인터넷 침해사고 당시 슬래머 웜이 유발한 과도한 트래픽의 영향으로 국제회선에 장애가 발생하고 이로 인하여 국내 DNS 서버의 과부하로 국내 인터넷 접속이 지연되는 등 피고 ISP들이 제공하는 인터넷 서비스에도 장애가 발생한 점은 인정된다. 그러나 이러한 사정만으로 이 사건 인터넷 침해사고 당시 피고 ISP들이 원고들에게 인터넷 서비스를 제공하지 못하였다는 것을 인정하기에 부족하고 달리 이를 인정할 만한 증거가 없다.

오히려 위 기초사실 및 인정사실에 나타난 다음과 같은 사정 즉, 인터넷은 ISP 사업자들이 운영하는 인터넷 망이나 기업들이 보유하고 있는 LAN 등이 결합하여 서로 유기적으로 연결되어 있는 개별 통신망의 집합체인 점, 피고 ISP들의 의무는 정상적인 환경에서 인터넷 통신망을 사용할 수 있도록 인터넷 통신망을 제공하는 것이지 그 외에 개별 사이트들의 접속 여부까지 가능하도록 하는 것은 아닌 점, 슬래머 웜으로 인해 피고 ISP들의 DNS 서버 자체가 다운되어 서비스를 제공하지 못하였던 것은 아니고 슬래머 웜에 의해 유발된 과도한 트래픽으로 국제회선에 장애가 발생하면서 정상적인 DNS 서버의 서비스까지도 지연된 것에 불과했던 점, 피고 ISP들이 자신이 관리하는 통신망 내로 슬래머 웜이 유입되는 것을 차단하는 ACL 조치를 취한 이후에도 통신망 내에 남아있던 슬래머 웜의 유해 패킷으로 인해 인터넷 장애사태가 정상화되는 데는 시간이 걸렸으며 문제가 된 MS SQL 서버에 패치를 계속 함에 따라 비로소 인터넷 소통이 원활하게 된 점, 실제로 이 사건 인터넷 침해사고 당시 MS SQL 서버를 사용하지 아니하였던 사이트는 정상적으로 작동하였던 점, 피고 ISP들의 사용자는 인터넷 접속 지연 정도의 차이는 있으나 인터넷 연결이 가능한 부분도 있었고 다만 감염된 IDC 입주업체 또는 감염된 독립서버의 인터넷 사이트에 접속하고자 하는 사용자들은 접속장애를 체감하였던 점 등을 고려할 때, 이 사건 인터넷 침해사고 당시 피고 ISP들의 서비스 자체는 제공되었고, 다만 슬래머 웜의 영향을 받은 인터넷 사이트 등 개별 인터넷 접속 환경에 따라 원고들과 같은 인터넷 이용자들이 장애를 느꼈던 것으로 봄이 상당하다.

⑶ 또한 위 나.항에서 살펴본 바와 같이 피고 ISP들에게 이 사건 인터넷 침해사고의 유발 및 그 확산에 대하여 어떠한 과실이 있다고 보기도 어렵다.

⑷ 따라서 피고 ISP들의 귀책사유에 의한 서비스제공불능을 전제로 위 피고들에게 약관에 기한 손해배상을 구하는 원고들의 이 부분 청구는 이유 없다.

5. 피고 대한민국에 대한 청구에 관한 판단

가. 관련 법률 규정

⑴ 정보통신망 이용촉진 및 정보보호에 관한 법률(2004. 1. 29. 법률 제7139호로 개정되기 전의 것, 이하 '정보이용법'이라 한다)

제4조 (정보통신망 이용촉진 및 정보보호 등에 관한 시책의 강구)

① 정보통신부장관은 정보통신망의 이용촉진 및 안정적 관리·운영과 이용자의 개인정보의 보호 등(이하 "정보통신망 이용촉진 및 정보보호 등"이라 한다)을 통하여 정보사회의 기반을 조성하기 위한 시책을 마련하여야 한다.

② 제1항의 규정에 의한 시책에는 다음 각호의 사항이 포함되어야 한다.

8. 정보통신망의 안전성 및 신뢰성 제고

제15조 (인터넷서비스의 품질개선)

① 정보통신부장관은 인터넷서비스 이용자의 권익 보호와 인터넷서비스의 품질향상 및 안정적 제공을 보장하기 위한 시책을 마련하여야 한다.

⑵ 정보통신기반보호법(2005. 3. 31. 법률 제7428호로 개정되기 전의 것)

제5조 (주요정보통신기반시설보호 대책의 수립 등)

① 주요정보통신기반시설을 관리하는 기관(이하 '관리기관'이라 한다)의 장은 제9조 제1항의 규정에 의한 취약점 분석·평가의 결과에 따라 소관 주요정보통신기반시설을 안전하게 보호하기 위한 물리적·기술적 대책을 포함한 관리대책을 수립·시행하여야 한다.

제9조 (취약점의 분석·평가)

① 관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다.

제14조 (복구조치)

① 관리기관의 장은 소관 주요정보통신기반시설에 대한 침해사고가 발생한 때에는 해당

정보통신기반시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 한다.

나. 판단

⑴ 인정사실

㈎ 정보통신부장관은 1996년 4월경 한국정보보호진흥원을 설립하여 해킹·바이러스 예보·경보 및 복구지원, 대응기술개발 등을 추진토록 하는 등 정보통신망 안정성 확보를 위한 전문 기술지원기관을 설립·운영하여 오고 있고, 2000년 9월경 '정보통신서비스 정보보호지침'을 고시하여 ISP가 준수하여야 할 정보보호 기준을 제시하였다.

㈏ 2001년 1월에는 정보통신기반보호법이 제정되어 국가, 사회적으로 중요한 주요 정보통신기반시설을 보호할 수 있는 법률적 근거가 마련하였다.

㈐ 정보통신부장관은 정보통신기반보호법 제8조 제1항에 근거하여, 2001년 1월경 정보통신부고시 2001-123호로 피고 ○○의 인터넷접속망(○○), 피고 ○○의 인터넷접속망(○○), 피고 ○○의 인터넷접속망(○○), 피고 ○○의 인터넷접속망(○○), 한국전산원의 인터넷교환시스템(KIX), 재단법인 한국인터넷정보센터의 인터넷주소자원관리시스템 등 17개를 정보통신기반보호법상 주요정보통신기반시설로 각 지정하였다.

㈑ 정보통신부는 2002년 해킹·바이러스에 취약한 초중고교, PC방 사업자 등에 대한 원격점검 및 을지훈련 기간 중 민간업체에 대한 모의사이버테러 대응훈련을 실시하고, 대학(학내 전산망 Lab실 보호 지침서), 전자상거래업체(전자상거래업체보안 및 대응지침), 컴퓨터사용자(안전한 컴퓨터 사용을 위한 정보보호 지침)에게 정보보호지침을 만들어 보급하였다.

㈒ 정보통신부는 2002년 7월경 한국정보보호진흥원의 홈페이지를 통하여 MS SQL 서버의 취약점과 이를 보완할 수 있는 방법을 안내하고, 주요 서버관리자로 구성된 메일링 리스트를 이용하여 이메일로 그 사실을 통보하였다.

㈐ 이 사건 인터넷 침해사고 발생 당일의 조치

일시	내용
2003. 1. 25. 15:30	정보통신부 정보보호기획과에서 전국의 산발적인 인터넷접속 이상 현상의 발생을 인지하고 긴급대책반을 구성
2003. 1. 25. 16:00	피고 ISP들과 접촉 후 특정 포트 트래픽의 이상 현상을 확인, MS SQL 관련 취약점을 이용한 공격으로 추정하고, 피고 ISP들에게 UDP 1433, 1434 포트의 차단을 권고
2003. 1. 25. 17:30	장관 및 관계 실·국장 회의를 개최하여 이 사건 인터넷 침해사고의 원인분석 및 긴급복구를 지시하고 한국정보보호진흥원이 피고 ○○의 혜화전화국에 기술요원을 파견
2003. 1. 25. 20:00	이 사건 인터넷 침해사고의 원인을 UDP 1434 포트를 이용한 신종 웜 바이러스로 확정
2003. 1. 25. 21:00	한국정보보호진흥원이 메일링 리스트, 시큐어 메신저, 홈페이지 등을 통해 긴급경보를 발령
2003. 1. 26. 9:00	장관주재 관계기관 합동회의
2003. 1. 26. 11:00	장관 기자회견 및 대국민 행동요령 배포
2003. 1. 27. 09:00	긴급대책반을 확대하여 정보통신망침해사고 대책본부 구성

㈑ 한편, 피고 대한민국은 정보통신부 및 그 산하기관 중 MS SQL 서버로 운용되고 있는 정보통신부본부 및 정보통신부전산관리소에 대하여 2002. 7. 29. 모두 보안패치를 설치하였다.

[인정근거] 다툼 없는 사실, 을사1 내지 7의 각 기재, 변론 전체의 취지

⑵ 정보이용법상의 의무 위반 여부에 관한 판단

위에서 본 정보이용법 규정에 의하면 피고 대한민국은 정보통신망의 안전성 및 신

뢰성 제고를 위한 시책 및 인터넷서비스 이용자의 권익 보호와 인터넷서비스의 품질향상 및 안정적 제공을 보장하기 위한 시책을 마련할 의무가 있다. 그러나 나아가 피고가 위와 같은 시책을 마련하지 않았다는 점을 인정할 아무런 증거가 없고, 오히려 피고 대한민국이 정보통신망의 안정성 및 신뢰성 제고, 인터넷서비스 이용자의 권익 보호, 인터넷서비스의 품질향상 및 안정적 제공을 위하여, 한국정보보호진흥원을 설립하고, 관련법령을 정비하였으며, 정보보호지침을 만들어 보급한 사실은 위에서 본 바와 같으므로, 피고 대한민국이 정보이용법상의 의무를 위반하였음을 전제로 하는 원고들의 이 부분 주장은 더 나아가 살필 필요 없이 이유 없다.

⑶ 정보통신기반보호법 위반 여부

위에서 본 정보통신기반보호법 규정에 의하면 정보통신부장관에게 소관 주요정보통신기반시설인 피고 ISP들의 인터넷접속망을 안전하게 보호하기 위한 물리적·기술적 대책을 포함한 관리대책을 수립·시행하고, 이에 대한 침해사고가 발생한 때에는 해당 정보통신기반시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 할 의무가 있다. 그러나 나아가 피고 대한민국이 피고 ISP들의 인터넷접속망을 안전하게 보호하기 위한 물리적·기술적 대책을 포함한 관리대책을 수립·시행할 의무를 이행하지 않았다거나, 이 사건 인터넷 침해사고 발생 이후 위 인터넷접속망의 복구 및 보호에 필요한 조치를 취할 의무를 이행하지 않았다는 사실을 인정할 아무런 증거가 없고, 오히려 피고 대한민국이 해킹·바이러스 예보, 경보 및 복구지원, 대응기술개발 등을 위하여 한국정보보호진흥원을 설립하고, '정보통신서비스 정보보호지침'을 고시하였으며, 민간업체에 대한 모의사이버테러 대응훈련을 실시하고, 특정분야에 대한 정보보호지침을 제정하였으며, 피고 ○○의 MS SQL 서버에 취약점이 있다는 사실이 밝혀진 무렵인 2002년 7월경 한

국정보보호진흥원의 홈페이지를 통하여 MS SQL 서버의 취약점과 이를 보완할 수 있는 방법을 안내하는 등 이 사건 인터넷 침해사고 발생 이전에 주요통신기반시설의 보호를 위한 물리적·기술적 대책을 포함한 관리대책을 수립·시행하였으며, 피고 대한민국이 이 사건 인터넷 침해사고 발생 직후 이 사건 인터넷 장애 발생을 인지하고 긴급대책반을 구성하고, 같은 날 16:00경 피고 ISP들에게 UDP 1433, 1434 포트를 차단할 것을 권고하였으며, 그 이후에 재발 방지를 위한 여러 조치를 취하였음은 앞에서 본 바와 같으므로, 피고 대한민국이 정보통신기반보호법을 위반하였음을 전제로 하는 원고들의 이 부분 주장도 더 나아가 살필 필요 없이 이유 없다.

6. 피고 ○○에 대한 청구에 관한 판단

가. 제조물책임법에 의한 책임의 인정 여부

⑴ '제조물'인지 여부

제조물책임법 제2조 제1호에 의하면 '제조물이란 다른 동산이나 부동산의 일부를 구성하는 경우를 포함한 제조 또는 가동된 동산'을 말하고, 제8조에서는 '제조물의 결함에 의한 손해배상책임에 관하여 이 법에 규정된 것을 제외하고는 민법의 규정에 의한다'고 규정하고 있는바, 결국 제조물책임법이 적용되는 객체는 민법 제98조 및 제99조 제2항에 따른 '동산' 즉, '유체물 및 전기 기타 관리할 수 있는 자연력 중 토지 및 그 정착물인 부동산을 제외한 것'으로 봄이 상당하다.

이 사건 MS SQL 서버가 제조물에 해당하는지 여부에 관하여 본다. 살피건대, 서비스 또는 물건을 만드는 방법 등과 같은 단순한 정보는 타인의 편의를 위한 유·무형의 산물로서 그 결과가 확정되어 있는 것이 아니어서 이를 제조 또는 가공된 동산으로 파악하기는 어려울 것이다. 그러나 피고 ○○는 MS SQL 서버를 전자서적과 같은 형태로

씨디-롬(CD-ROM)이나 디스켓 등과 같은 일정한 저장매체에 저장하여 공급하거나, 웹사이트를 통하여 라이센스를 부여하고 프로그램을 다운로드받게 하는 형태로 공급하는데, 전자의 경우 저장장치와 소프트웨어를 일체로서의 유체물로 볼 수 있어 그 소프트웨어 역시 제조물로 볼 수 있고, 후자의 경우 디지털 형태로 공급되는 소프트웨어를 이용하기 위해서는 하드디스크 등과 같은 다른 저장 매체에 저장되어야만 사용할 수 있고 일단 소프트웨어의 공급이 완료된 시점에서 결국 그 소프트웨어가 일정한 저장매체에 담겨져 있는 상태로 되며, MS SQL 서버는 대량으로 제작·공급되는 것이어서 제조물책임법이 적용되는 제조물에 포함시키는 것이 제조물책임법의 제정목적에도 부합되므로, MS SQL 서버를 제조물로 봄이 상당하다.

⑵ 설계상의 결함이 존재하는지 여부

㈎ 제조물책임법 제2조 제2의 나항에 의하면 '설계상의 결함'이라 함은 '제조업자가 합리적인 대체설계를 채용하였더라면 피해나 위험을 줄이거나 피할 수 있었음에도 대체설계를 채용하지 아니하여 당해 제조물이 안전하지 못하게 된 경우를 말한다.'고 규정하고 하고 있고, 제조물에 이러한 설계상의 결함이 있는지 여부는 제품의 특성 및 용도, 제조물에 대한 사용자의 기대와 내용, 예상되는 위험의 내용, 위험에 대한 사용자의 인식, 사용자에 의한 위험회피의 가능성, 대체설계의 가능성 및 경제적 비용, 채택된 설계와 대체설계의 상대적 장단점 등의 여러 사정을 종합적으로 고려하여 사회통념에 비추어 판단하여야 한다(대법원 2003. 9. 5. 선고 2002다17333 판결 등 참조).

㈏ 인정사실

1) 피고 ○○는 1998. 11. 16. 기업체의 데이터 저장 기능을 제공하는 소프트웨어인 MS SQL 서버 버전 7.0을 출시한 직후 MS SQL 서버 2000을 개발하기 시작하여,

2000. 8. 7. MS SQL 서버 2000을 출시하였다.

2) 소프트웨어 공급업자들은 새로운 소프트웨어를 출시하기 위하여, 설계문서를 작성하고, 설계문서에서 규정하는 기능들을 실행하기 위하여 실제 프로그램 코드를 작성하며, 각 특징을 통합한 시스템이 제대로 작동되는지 여부를 검증하기 위하여 설계 및 테스트를 동시에 진행하고, 그 소프트웨어 프로그램의 '베타(beta)' 버전을 개발하여 일정한 기간 동안 프로그램을 테스트하기로 동의한 제3자들에게 무료로 배포하며, 테스트 팀과 베타버전 사용자들로부터 확인된 오류들에 대하여 필요한 조치를 취하고, 복제 및 출시를 위하여 소프트웨어를 준비하는 과정을 거친다.

3) MS SQL 서버는 데이터베이스 관리시스템으로서 대규모의 자료를 관리하는 본질적 특성상 그 내부적인 동작원리가 복잡하고, 다른 응용 프로그램과 끊임없는 상호작용을 통하여 시스템 자원과 운영체계의 기능을 이용할 수 있도록 하여 주는 개방구조(open structure)를 취하고 있어, 사용자의 입력, 운영체제 및 다른 소프트웨어와의 연계, 서버 관리자들의 행동 및 보안 의식, 네트워크 접근 등과 같이 다양한 외부환경과 연계되어 수행된다. 따라서 사전에 외부환경에 기인한 취약점을 모두 제거하는 것은 불가능하고 제품 테스트 단계에서는 에러(error) 없이 적정하게 동작하는지 여부만을 시험할 수밖에 없다.

4) 피고 ○○는 MS SQL 서버의 출시 전에 약 19개월 동안 품질보증 테스트를 수행하였으며, 베타테스팅을 위하여 수천명의 소비자에게 소프트웨어를 사전 배포하였다.

5) MS SQL 서버의 출시일로부터 2년 정도 경과된 2002. 7. 25. 보안업체인 NGS는 UDP 1434 포트와 관련된 MS SQL 서버의 잠재적인 보안상의 문제를 지적하였다. 피고 ○○는 NGS가 자신의 웹사이트에 위 취약점에 대한 글을 게시하기 전날인 2002.

7. 24. 피고 ○○의 웹사이트에 이에 관한 글을 게재하고 보안 패치 파일을 업로드시켰다.

6) 한편, 피고 ○○는 미국 국가안전보장국(U.S. National Security Agency) 및 국립표준기술연구소(U.S. National Institute of Standards and Technology)가 민간 사업체의 소프트웨어를 평가하기 위하여 마련한 신뢰기술평가프로그램(Trust Technology Assessment Program, TTAP)에 의하여 미국의 정부기관들이 요구하는 보안 수준인 "C2" 등급의 보안 평가를 받았다.

[인정근거] 을아 제 1 내지 8호증(가지번호 있는 것은 가지번호 포함)의 각 기재에 변론 전체의 취지

㈐ 판단

MS SQL 서버에 설계상의 결함이 있는지에 관하여 보건대, MS SQL 서버에 슬래머 웜의 공격대상이 될 수 있었던 '버퍼 오버플로우의 취약점'이 있었던 사실은 앞에서 본 바와 같다. 그러나 위 인정사실에서 나타난 다음과 같은 사정 즉, 인터넷 통신의 특성상 사전에 아무리 위와 같은 절차를 거쳐 테스트를 철저히 하더라도 해커들의 웜 또는 바이러스 유포하는 행위를 모두 미리 예상할 수 없는 점, MS SQL 서버의 사용자들은 거의 무한대에 가까울 만큼 다양한 방법으로 소프트웨어 프로그램을 이용하고 있어 과거에는 예상할 수 없었던 새로운 보안상 취약점이 야기되거나 초래될 가능성이 있는 점, MS SQL의 취약점은 MS SQL 서버 개발 당시에는 발견되지 않았고 그 출시로부터 2년 정도 지난 이후에서야 발견된 점, 피고 ○○가 제공한 보안 패치를 설치한 MS SQL 서버는 슬래머 웜의 감염으로부터 안전했던 점, 소프트웨어가 출시되었을 당시 알려지지 않은 보안상 취약점에 대한 모든 책임을 소프트웨어 개발업체들에게 지우는 것

은 소프트웨어 개발업체의 신기술 개발, 신제품 출시를 원천적으로 봉쇄하는 결과를 초래할 수 있는 점 등에 비추어 보면, 이 사건 인터넷 침해사고 발생 시점에는 합리적인 대체설계 방안에 의하여도 슬래머 웜의 위협 또는 결과를 제거하거나 감소시키지는 못했다고 봄이 상당하므로 이를 설계상 결함으로 보기 어렵다.

⑶ 표시상의 결함이 존재하는지 여부

㈎ 제조물책임법 제2조 제2의 다항에 의하면, '표시상의 결함'이라 함은 '제조업자가 합리적인 설명·지시·경고 기타의 표시를 하였더라면 당해 제조물에 의하여 발생될 수 있는 피해나 위험을 줄이거나 피할 수 있었음에도 이를 하지 아니한 경우를 말한다'고 규정하고 있고, 이러한 표시상의 결함이 존재하는지 여부에 대한 판단을 함에 있어서는 제조물의 특성, 통상 사용되는 사용형태, 제조물에 대한 사용자의 기대의 내용, 예상되는 위험의 내용, 위험에 대한 사용자의 인식 및 사용자에 의한 위험회피의 가능성 등의 여러 사정을 종합적으로 고려하여 사회통념에 비추어 판단하여야 할 것이다(대법원 2003. 9. 5. 선고 2002다17333 판결 등 참조).

㈏ 인정사실

1) 피고 ○○는 NGS가 MS SQL의 취약점을 발표하기 하루 전인 2002. 7. 24. 한국○○의 웹 사이트에 MS SQL 서버 2000의 보안상 문제점에 대한 설명의 글을 게재하고, 위 취약점을 심각한(Critical) 위험등급으로 표시한 다음 MS SQL 사용자들이 보안패치를 다운로드 받을 수 있도록 하였다.

2) 피고 ○○와 한국○○는 2002. 7. 31. ○○ 최신 소식을 통하여 한국인 구입자 약 200,000명에게 MS02-039 보안패치가 첨부된 이메일을 발송하고, 같은 날 MS SQL 서버 2000 보안권고라는 뉴스레터를 통해 한국인 약 28,000명에게 위와 같은 이메일을

발송하였으며, 2002. 8. 1. IT 전문가를 위한 'TechNet news service'를 통해 한국인 구독자 28,000명에게 위 보안패치가 포함되어 있는 MS02-061 보안패치를 이메일로 발송하였다.

3) 그 결과 한국○○의 웹사이트에서 이 사건 인터넷 침해사고 전날인 2002. 1. 24.까지 총 25,660건의 보안패치의 다운로드가 있었고, 이 사건 인터넷 침해사고 발생일인 2003. 1. 25. 19,540건, 2003. 1. 26.에는 129,280건의 보안패치의 다운로드가 있었다(한편 2002년말 경까지 국내에 공급된 MS SQL 서버는 22,054개에 불과하였다).

4) 이 사건 인터넷 침해사고 이후인 2003. 1. 26. 03:00경 한국○○의 대응팀은 주요 고객 및 보안전문기업 등을 방문하여 현황을 파악하고 같은 날 09:00경부터는 고객지원 핫라인을 통하여 전화상담을 하고, 같은 날 21:00경에는 중소기업 및 대기업 등 전 고객들에게 웜 바이러스 예방 및 복구방법에 관한 보안 메일을 재발송하였으며, 2003. 1. 27. 08:00경 국내 3대 보안 전문기업인 하○○, ○○연구소, ○○ 마이크로 및 한국정보보호진흥원의 웹사이트에 패치파일을 업로드시킬 수 있도록 하였다.

[인정근거] 을아 제1 내지 8호증(가지번호 있는 것은 가지번호 포함)의 각 기재, 변론 전체의 취지

㈐ 살피건대 위 인정사실에 의하면, 피고 ○○는 소프트웨어의 특성, 통상 사용되는 사용형태, 소프트웨어에 대한 사용자 기대의 내용, 그 위험에 대한 사용자의 인식 등에 비추어 합리적인 방법으로 고객에게 MS SQL 서버의 취약점에 대하여 위험성을 경고하고, 그 해결방법을 설명하는 등 의무를 다 하였다고 보인다. 원고들은 이에 더하여 피고 ○○가 MS SQL 서버의 사용자를 직접 방문하는 등 개별적인 접촉을 통하여 그 위험성을 알리고 보안 패치를 설치해 주어야 할 의무까지 있다고 주장하나 소프트웨어

의 특성, 사소한 보안점이 있을 때마다 개발되는 패치의 양, 더구나 피고 ○○가 MS SQL 서버를 공급받은 사용자들이 보안패치 파일을 다운로드하고 설치하는 것을 돕기 위해 모든 라이센스 소지자들에게 전화를 하고 방문하였다고 하더라도 피고 ○○로부터 라이센스를 부여받지 않은 불법 사용자들은 슬래머 웜의 공격에 무방비 상태로 남아있었을 것이라는 점 등을 고려할 때 피고 ○○에게 원고들이 주장하는 위와 같은 의무까지 있다고 보기는 어려워 결국 MS SQL 서버에 표시상의 결함이 있다는 원고들의 주장은 이유 없다.

나. 불법행위책임의 인정여부

위 가.항에서 살펴본 바와 같은 피고 ○○의 MS SQL 서버 개발과정, MS SQL 서버의 취약점이 발견된 이후 그 보안을 위하여 취한 조치, 이 사건 인터넷 침해사고 이후 대응과정 등을 고려할 때 피고 ○○의 고의 또는 과실로 이 사건 인터넷 침해사고가 발생 및 확대되었다고 보기 어려우므로 원고들의 이 부분 주장도 이유 없다.

7. 결론

그렇다면, 원고들의 피고들에 대한 청구는 모두 이유 없으므로 이를 기각하기로 하여 주문과 같이 판결한다.

재판장 판사 안영길 _____

판사 임종효 _____

판사 공현진 _____