

국경간 해킹 · 스팸 메일 대책

1. 검토배경

인터넷을 통해 우리나라에서 외국으로 나가는 웜바이러스 및 스팸메일이 증가하여 한국의 이미지가 훼손될 뿐 아니라 초·중·고교, PC방, 중·소 기업 등이 정보보호에 대한 투자와 사전·사후관리가 미흡하여 정보보호 취약부문에 지적(해킹 및 스팸메일의 경유지로 이용되는 사례 발생)되고 있다.

이에 정보화 수준에 부합하는 정보보호 환경을 조성하기 위한 대책을 수립·시행하고자 한다.(특히 취약부문을 중점대상으로 하여 해킹 및 스팸메일의 경유지 이용 차단대책을 마련)

2. 현황

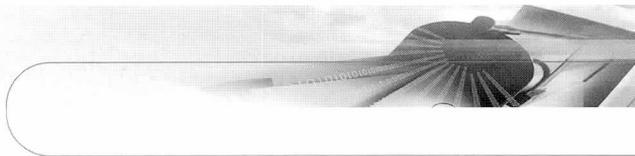
■ 웜바이러스 피해

신종바이러스는 줄어들고 있지만, 인프라 고도화와 인터넷 인구 확산으로 웜바이러스 확산이 용이, 피해 신고가 늘고 있다.

자료 : 한국정보보호진흥원

구 분	1998	1999	2000	2001
신종 바이러스 건수	276	379	572	194
바이러스피해 신고 건수 (웜바이러스)	-	39,248	50,124	65,033 (35,157)

※ CodeRed, Nimda 등 웜바이러스는 일단 감염되면 자동으로 다른 대상을 스캐닝하여 2차 감염을 시도.



웬바이러스의 2차 감염을 위한 자동스캐닝 시도에 의하여 우리나라가 보안위협 상위국가로 지목되는 사례가 증가하고 있다.

2001년에는 CodeRed, Nimda 등 웬바이러스의 감염이 높아 미국의 보안전문업체인 Riptech사에 의해 보안위협 근원지 2위로 지적됐는가 하면, 미국 Predictive System사의 2001년 4/4분기 로그 분석결과, 미국에 이어 한국이 스캐닝 시도 2위 국가로 기록됐으며, 미국의 SANS(System Administration, Networking and Security)사가 집계하는 「주별 스캐닝 시도 Top10」(2001)에 7·0초등학교 등이 여러 주에 걸쳐 상위에 랭크되었다.

■ 해킹의 중간경유

한국정보보호진흥원(KISA)에서 처리한 2001년도 해킹신고건수는 2000년 대비 174%가 증가한 5,333건이다.

자료 : 한국정보보호진흥원

구 분	1998	1999	2000	2001
해킹신고 처리건수	158	572	1,943	5,333

※ 총 신고건수는 5,508건(국내신고 401건, 해외신고 5,107건)이나 이중 피해조사처리가 곤란한 175건(국내→국외)을 제외

2001년 신고처리 건수의 69%인 3,664건이 스캐닝 시도 신고이다.

자료 : 한국정보보호진흥원

스캐닝	불법침입	홈페이지변조	불법사용	자료변조	DoS	자료유출	시스템 파괴오류	계
3,664	1,240	212	86	59	58	7	4	5,333

※ 스캐닝 시도는 해킹을 하기 위하여 상대 시스템의 취약점을 확인하는 작업

해킹경로가 확인된 1,157건 중 국경간 해킹은 국내해킹을 제외한 872건으로, 국경간 해킹 중 한국이 경유지가 되어 국외로 공격한 경우가 약 47%에 이르고 있어, 국내의 초고속망을 활용하여 단시간에 해킹 효과를 극대화하고 있다는 것을 알 수 있다. 반면 가해건수(175건)는 피해건수(697건, 경유지 포함)의 1/4에 불과하다.

자료 : 한국정보보호진흥원

유 형	경 로	사고발생건수
경유지	국외→국내→국외	408건(46.8%)
순수 가해자	국내→국외	175건(20.1%)
순수 피해자	국외→국내	289건(33.1%)
계		872건(100%)

해킹당한 서버 내에 잔존하는 악성코드에 의해 무작위적으로 선정된 IP 주소를 대상으로 취약점 스캐닝이 시도한 결과, 국내 45개 사이트가 미국 Rice 대학 및 일본 ISP인 SecomJ로부터 인터넷 접속 차단 조치를 당했다.

■ 스팸메일 중계(Spam-Relay)

스팸메일로 인한 민원이 증가하는 가운데 메일서버의 중계 기능을 이용하여 스팸메일을 보내는 사례가 급증하고 있다.

미국 시민단체인 Anti-spam은 2002년 3 ~ 4월간 조사결과, 국내 26개 사이트가 스팸메일 중계에 이용되고 있다고 신고했으며, 'to' 도메인 등록사인 미국 토닉사는 국내 wo.to 도메인이 스팸메일을 발송하였다는 신고를 받고 접속을 차단한 바 있다.

〈신고된 국내 Spam-Relay 사이트〉

공공기관	교육기관	민간기업	계
2	15	9	26

3. 문제점

■ 웹바이러스에 대비한 사전·사후 관리 소홀

웹바이러스를 예방·치료하는 백신S/W의 설치 및 관리소홀로 피해가 증가하고 있다.

초·중·고교, PC방 등의 백신 S/W 이용율은 높은 편이나 자동검색·갱신기능을 설정하지 않는 등 관리에 소홀하다.

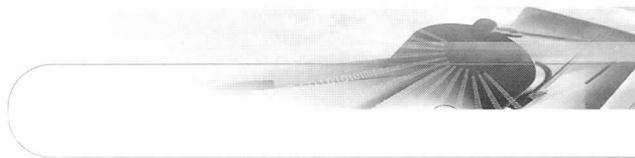
〈 PC방 백신프로그램 이용실태 〉

자료 : 한국정보보호진흥원

백신설치 유무			백신을 이용한 청소 및 사후관리				
설치	미설치	계	자동검색	일주일	비정기적	안함	계
203(76%)	62(24%)	265(100%)	0(0%)	75(37%)	55(27%)	73(36%)	203(100%)

불필요한 서버기능을 설치하여 사용하거나, 취약점 보완관리가 소홀하여 웹바이러스의 공격에 쉽게 노출되고 있다.

CodeRed와 Nimda는 일반 PC사용자가 무심코 설치한 Window NT 및 2000의 Web서버 기능을 이



용하여 감염되고 있으며, 감염시 백신으로 치료가 가능하지만 MS사의 IIS(Internet Information Server : MS사의 인터넷서버로서 버퍼오버플로우등의 각종 취약점 내재취약점)이 패치되지 않으면 재감염 발생 우려가 있다.

KISA와 MS사의 적극적인 패치 유도에도 불구하고 2001년 발생한 Nimda의 경우 아직까지 감염사례가 접수되고 있는 실정이다.

■ 해킹가능성을 차단하는 사후관리 미흡

경찰청 발표에 의하면 미국W사를 경유한 해킹사고의 주된 원인은 OS버전 갱신 및 취약점 보완 미비로 밝혀졌다.(2001. 8월 ~ 2002. 3월까지 20여명의 국제해커에 의해 국내 4,300여 서버가 해킹당함)

또한 PC내에 설치된 악성코드 등에 대한 정리작업을 소홀히 하여, 웜바이러스에 감염된 PC가 치료되지 않아 백도어를 통해 홈페이지 변조(미국 9.11사태 이후 정치적 목적으로 홈페이지 변조사건에 이용) 등 침해사고가 발생하고 있다.

PC방에 설치되었거나 다운로드된 파일 속에 숨겨진 트로이 목마를 이용하여 개인정보유출등의 해킹도 발생하고 있다.

■ 메일서버 구성·설정오류 등으로 인한 스팸메일 증계

불필요한 메일서버 설치와 이에 대한 보안관리가 이루어지지 않아 스팸메일 증계 등에 이용되는 사례가 발생하고 있다.

초·중·고교의 경우 자체 메일서버 운영도 하지 않으나 메일서버 기능은 설치되어 있고 이에 대한 관리도 미흡한 형편이며, 민간기업 등에서는 메일서버 구성·설정시 Mail-Relay기능을 제대로 설정하지 못하여 스팸 메일 증계에 이용당하고 있다.

■ 정보보호 의식 및 투자 부족

정보화에 비해 정보보호 의식수준이 낮고 전문 관리인력·능력이 부족하여 예방·사후관리대책의 실효성이 떨어진다. 여행사, 중·소업체 등을 대상으로 한 무상 정보보호점검 등이 업체의 호응부족으로 시행조차 어려운 실정이다.

최근 피해는 자료유출, 네트워크 성능저하 등 비가시적인 형태를 띠면서 관심도 적어 해킹 당한 사실도 모르는 경우가 많다.(경찰청 발표 자료에 의하면 국제해커들에 의해 집중 공격을 당한 78개 기관 중 4개 기관만이 피해사실을 인지)

대기업의 정보보호에 대한 투자는 증가하고 있으나 중소기업의 경우 백신 S/W를 제외한 Firewall, IDS 등의 사용은 저조한 편이다.

〈 민간기업 정보보호 실태 〉

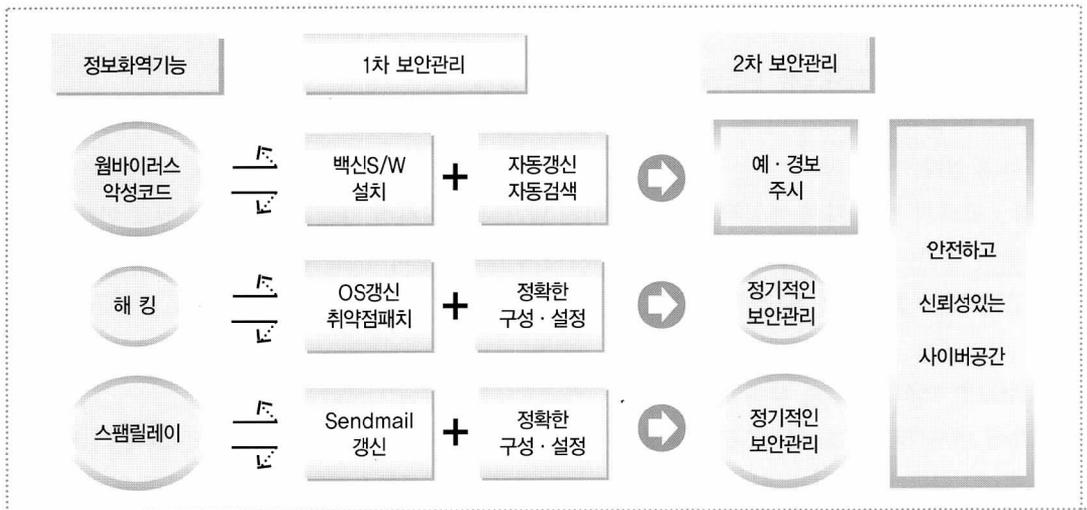
자료 : 한국정보보호진흥원(단위 : %)

구 분	방화벽 설치	백신설치	보안담당임명	정기적 보안점검
대기업	75.3	95.5	68.4	51.8
중소기업	30.3	86.4	47.0	39.8

- 설치된 IDS, Firewall등 보안장비의 지속적 사후관리도 미흡
- ※ 경찰청 발표자료에 의하면 침단보안시스템이 설치된 인터넷업체, 연구소 등이 국제해커들에 의해 해킹을 당함

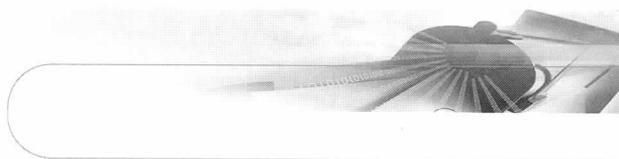
4. 대책

가. 웬바이러스 · 해킹 · Spam-Relay 퇴치방안



각종 바이러스와 악성코드 등을 예방·치료하기 위하여 백신 S/W 설치 및 자동 갱신·검색설정을 생활화 해야한다.(KISA에서「Secure Messenger」 「Sec-Info」를 통하여 실시간으로 제공하는 해킹바이러스 예·경보를 주시)

KISA나 공급사에서 제공하는 취약점 및 OS정보에 따라 시스템을 보완하고 불필요한 기본 옵션을 제거하여 해킹을 예방하는 한편 정기적으로 시스템·네트워크의 이상유무점검과 로그검사를 실시하여 안



전한 정보이용 환경을 구축해야 한다.

Spam-Relay를 방지하기 위하여 안전한 메일 S/W(Sendmail) 버전으로 패치하고 구성·설정 오류여부를 확인하는 한편 Firewall, IDS등 보안장비를 설치하고 지속적으로 사후관리를 해야 한다.

나. 세부대책

■ 각종 악성코드 대청소 실시

정보보호 취약부문을 대상으로 「해킹바이러스 예방의 날」에 단계적으로 대청소를 실시(관리자교육, 대청소지침서 배포, 희망기관 및 시범기관에 대한 현장방문 등을 통해 지원)하는 한편 초·중·고교는 전산담당 교사에 대한 교육을 실시하고 문제가 지적된 학교에 대하여 현장방문 지원할 예정이다.

한국정보교육학회를 통해 전산담당 교사를 대상으로 전국순회 교육을 실시(취약지역으로 지적되고 있는 경기지역의 전산담당교사(1,600여명)에 대해서는 집합교육 실시)하는 한편 대학생 정보보호 봉사대를 조직하여 현장방문을 지원한다.

이를 위해 우선 경기지역 600여개 학교를 대상으로 시범 실시하는 한편 Spam-Relay 원격진단에 의해 문제가 발견된 학교를 대상으로 정보보호 봉사대가 방학 중 현장방문 지원(대학생 정보보호 봉사대는 정보보호 동아리 구성원으로 구성하며 추가인력 소요시 전산·컴퓨터 관련 학과생을 대상으로 모집)할 예정이다.

또한 도메인을 보유한 중소기업을 대상으로 권역별 관리자 교육을 실시하고 대청소지침서 배포하는 한편 자체실행능력이 부족한 업체에 대하여는 KISA를 통해 기술상담지원을 하고 상황에 따라 현장방문 지원(KISA, 전문가등으로 순회봉사대를 조직하여 대청소를 지원하는 방안을 강구)할 예정이다.

인터넷 PC문화협회의 협조를 받아 PC방 관리자를 대상으로 대청소지침서를 배포하는 한편 자체실행능력이 부족한 업체에 대하여는 KISA를 통해 기술상담지원과 상황에 따라 현장 방문 지원할 예정이다.

참여기관의 호응도와 경각심을 높이기 위하여 희망기관에 대하여 의사-바이러스를 유포하여 대응정도를 확인하는 한편 확인결과를 바탕으로 대청소 우수실시 기관을 선정·포상 추진할 방침이다.

■ 취약 부문에 대한 원격진단서비스 실시

KISA홈페이지를 통해 원격 진단서비스를 희망·신청하면 원격진단을 실시하고 결과를 통보하여 취약점 보완 유도하는 등 Spam-Relay 여부 원격진단서비스 제공하고 국내 시장점유율이 높은 Solaris, Windows, Linux서버를 대상으로 취약점 원격진단서비스 개발·제공할 방침이다.(본서비스가 해커의 공격대상 서버 취약점탐지에 악용되는 것을 방지하기 위하여 인증절차 마련 후 서비스 제공)

또한 관계법령을 개정하여 Spam-Relay기능, 웹바이러스 및 취약점에 대한 원격진단을 불시에 실시

하는 방안도 검토되고 있다.(정보보호 경각심을 높이기 위해 취약점이 발견된 기관·기업 등에 대해 점검 결과를 통보하고 보완을 유도·지원)

■ 국경간 해킹·스팸메일 문제 대응체계 강화

KISA 기반보호사업단장을 반장으로 해킹바이러스상담지원센터와 정보보호업체·백신업체·정보보호 동아리로 국경간 해킹·스팸메일 대책반을 구성·운영할 예정이다.

이 대책반의 주요임무로는 ▲정보보호 취약 분야 실태조사 및 대응책 마련 ▲메일서버를 운영하는 각급 기관의 Spam-Relay 여부 원격진단서비스 실시 및 기술지원 ▲웹바이러스 등 각종 악성코드 근절을 위한 대청소 실시 지원 ▲쉽게 따라할 수 있는 맞춤형 정보보호 핸드북 제작·배포 등이다.

또한 정통부 주관 하에 ISP, 백신업체, KISA가 참여하는 분기별 정기회의를 개최하여 ISP의 자발적 협조를 유도하는 한편 사후대응체계 강화를 위한 국내·외 협조체계 마련할 방침이다. 이를 위해 국외기관과의 원활한 의사소통을 위해 CERTCC.KR의 영문 홈페이지를 개설하는 한편 한·중·일 3개국 대표 CERT와 정보교류 채널을 마련하고, 해킹 등의 발생시 FIRST(Forum of Incident Response & Security Teams), AVAR(Association of anti Virus Asia Researchers)등과 공동 대응을 추진할 방침이다.

※ JPCERT와 침해사고 공동대응을 위한 MOU체결 : 2002. 3

■ 예·경보 강화 및 관련 기술개발

ISP의 협조로 약 10만 여명에게 「Secure Messenger」을 보급 추진하고, 해킹바이러스 정보의 수집·분석·발령 등 분야별 모듈시스템을 통합하는 조기 예·경보 체계(e-WAS) 개발·구축할 예정이다.

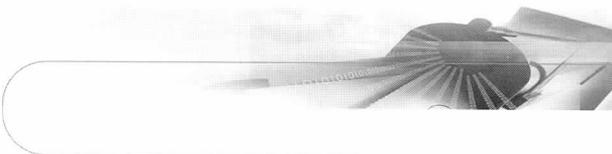
■ 정보보호 마인드 확산 및 관리자 교육 강화

민간의 자율적인 참여를 유도하는 「민간정보보호협의회(가칭)」를 구성하고 체계적인 정보보호 마인드 확산 운동을 추진할 예정이다.

공기업정보화협의회, 한국 CIO포럼 등을 통해 CEO, CIO 등에게 정보보호마인드를 확산하고 투자 제고를 유도하는 한편 대중매체를 활용하여 정보보호에 대한 경각심을 제고시킬 수 있는 적극적인 홍보대책을 수립·전개한다.

또한 KISA가 강사 및 교재개발을 지원하여 방학을 이용 '정보보호교사과정' 운영 추진하고, 교육부에서 점수가 부여되는 보안교육 과정을 개설하고, 정보화 평가기준에서 보안점수를 상향 조정하도록 유도하는 등 초·중·고교 보안담당교사의 기술능력 제고를 지원할 예정이다.

중·소기업 및 PC방 관리자들을 위한 정보보호 교육 프로그램 개발, 맞춤형 정보보호 핸드북을 배포하



고 상공회의소 및 한국인터넷 PC 문화협회와 협의하여 권역별 집합교육 실시를 추진한다.

■ Spam-Relay 차단 대책

각급 학교 서버의 Spam-Relay 이용여부를 확인하여 불필요한 메일서버 기능을 제거하거나 Spam-Relay를 차단하는 프로그램(Sendmail 8.9x 이상)으로 업그레이드하고 KISA는 희망 학교에 대하여 메일서버 구성설정에 대한 원격진단서비스를 제공할 예정이다.

민간기업 등의 메일서버의 Spam-Relay 방지를 위한 일제 정비작업을 실시하기 위해 Sec-Info 및 KISA 홈페이지를 통해 메일서버 정비작업에 대한 홍보를 실시하는 한편 메일서버의 문제점을 원격진단하고 OS의 취약점 패치 또는 업그레이드 방법을 안내할 예정이다.

5. 향후 추진일정

- 국경간 해킹 · 스팸메일 대책반 구성 · 운영 : 2002. 5~
- Spam-Relay 원격진단서비스 실시 : 2002. 5~
- 초 · 중 · 고교 대청소 실시
 - 전산담당교사 전국순회교육 실시 : 2002. 5
 - 경기지역 전산담당교사 집합교육 실시 : 2002. 7~8
 - 「대학생정보보호봉사대」 경기지역 시범 현장방문 지원 : 2002. 5~7
 - 「대학생정보보호봉사대」 방학 중 현장방문 지원 : 2002. 7~8
- 중 · 소기업 권역별 교육 및 지침서 배포 : 2002. 5~8
- PC방 대청소 지침서 배포 : 2002. 5~7
- 서버 등의 취약점 원격진단서비스 실시 : 2002. 11~
- 조기 예 · 경보체계 개발 · 구축 : ~ 2004. 11