「經營情報硏究」 第4號
大韓經營情報學會
2000年 6月

컴퓨터 유저의 해커행위와 가치관에 대한 고찰

정 혜 선*

〈목 차〉

Ⅰ. 문제의 제기

전세계 200만명의 통신서비스 업체는 웹기술(World Wide Web)을 이용하여 지구촌을 한지붕으로 거대한 데이터베이스가 되었다. 인종과 연령, 시간과 공간을 초월한 통신서비스 시스템이 된다. 이제 우리는 컴퓨터와 데이터통신을 하루도 떠나서는 살 수 없는 가정까지 생활필수품의 도구가 되었다. 특히 전문가들인 정치가, 역사가, 과학자, 의학자, 법학자 관광문화가 그리고 설계자, 산업디자인, 수출입의 무역인까지도 한눈 안의 인터넷정보로 해결된다. 외국 출장차 또는 관광차 세계현장을 돌아보지 않더라도, 사이버넷은 많은 시간과 경제적 이윤과 효율성을 낳는 것만은 아니다.

광랄한 빛깔 뒤에는 그림자가 있듯이, 통신사이버의 음란물과 지적재산권 침해는 사생활의

* 포항1대학 경영정보과 조교수

방해까지 끝없이 행해지는 해킹은 한계성의 정도가 넘었다. 이제, 전세계 해커인구는 9만명, 그 중 우리 나라 해커 인구만도 2천명이다. 이와 같이 늘어나는 신종해킹의 활동을 차단하기 위한 정보범죄 수사를 발동하고, 네트워크 보안망과 해커추적 그리고, 해커잡는 해커를 양성하고 있다. 이외도 또한 인력양성 사이버 공간에서 성행되는 S/W 불법복제거래, ID도용, 음란물유포, 통신상의 성희롱, 정보문화에 역행하는 행위들을 막기 위하여 보안차단 S/W, 암호 System, 신원인증제도 등 새로운 보안 차단장치가 개발 출시되고 있다.

그리고, 미국의 경우도 청소년 문제로 통신품위법(CDA-2)의 입법을 추진하여 법제화하고 있으며, 국내에서도 한국정보보호센터에서 캠페인과 함께 전기통신 사업법 제정이 실현되면서 법제화되고 있다. 전기통신사업법이 제정되면서 최하 3~10년 징역 그리고 최하 300~1,000만원의 벌과금이 부과되고 있다. 연령대는 주로 13~17세의 청소년들이며, 이들의 처벌이 급증하고 있다. 그러나, 첨단사회가 다가올수록 새로운 신종해킹과 더불어 강력한 해킹 차단기법이 새롭게 탄생되고 있으나, 이렇게 끝없는 해킹과 고도의 차단망 개발 이전에, 인간 그 자체 본성을 회복시켜야 할 것으로 판단된다. 수많은 해커자신의 인간심성(人間心性) 회복과 윤리관, 도덕관을 되찾아서 해킹을 앞서가는 자성(自省)의 가치관(價値觀)만이 그 해결의 도구가 될 것이다.

따라서 본 연구는 해커행위에 대한 보안 및 차단장비 개발이나 정보범죄의 수사인력 양성보다 컴퓨터 유저들의 윤리관이나 도덕성, 가치관과 해커행위와의 상관관계를 밝히는데 그 목적을 둔다.

이 연구목적을 수행하기 위하여 현재 해킹이 일어나고 있는 현황과 그 사례를 살펴보고 해커발생에 따른 사회적 문제 및 그 행위에 대한 유저들의 심리를 분석함이다. 아울러 해커행위를 방지하기 위하여 진행되고 있는 각종 방지 기술개발 및 인력양성을 한계점으로 분석함으로써 새로운 대안에 대한 시사점을 주고자 한다.

Ⅱ. 유저의 해커행위와 사회적 문제

1. 해커행위에 대한 인간의 심리

컴퓨터 범죄자는 죄의식이 전혀 없고, 자신의 우월능력을 과시하고 영웅심리에 사로잡혀서 스스로 만족감을 만끽하며 게으른 편이다. 그리고, 컴퓨터 지식과 경험이 풍부하고 두뇌가 명석하고, 도전정신이 왕성하여 개척정신이 내재되어 있다. 게임과 도박을 즐기며, 경제적으로 빈

곤하지 않지만 사회에 불만을 갖고 타인과의 다른 행위로 대리만족 및 인정받고 싶은 자기 현시욕이 강하다. 단순 시스템 파손을 예술로 보는가 하면 비행기 납치사건처럼 확신범의 영역에 포함된다. 문제는 대다수 컴퓨터 사용자가 컴퓨터 범죄를 범죄시 생각하지 않고 과시욕이 강하다는 점이다.

컴퓨터 조작행위의 계속성과 반복성이 규칙적으로 엄격히 조직화되어 임의로 이용된다. 형법 전에 규정된 범죄명이 아니고, 컴퓨터 범죄는 컴퓨터 행위를 수단목적으로 하여 형사 처벌할 가치가 있는 범죄를 의미한다. 이는 그 행위가 컴퓨터의 자료처리기능과 관련되는 기준인 자료의 부정조작 및 자료의 부정입수와 컴퓨터의 무권한 컴퓨터 파양의 4유형으로 분류되고 있다.

또한 컴퓨터 윤리(computer moral)를 벗어난 행위의 예를 들면, 급여 라인에서 친구의 보수를 슬쩍 할 수도 있고, 군사적 비밀을 외국에 팔아먹을 수도 있다. 일반인도 컴퓨터와 매일 접하고 있다면 일반인도 여러 파일에 접속할 수가 있고, 부주의하게 다루어질 가능성은 얼마든지 있다. 데이터는 복원하기가 가장 어려운 자원인데 수많은 사람들의 데이터 접촉은 보안담당자들에게 여간 신경이 쓰이는 일이 아니다. 학생들도 윤리적인 문제에서 예외가 아니다. 동료가 아닌 학생들이 학교 컴퓨터시스템의 보안장치를 피해 들어가서 여러분과 그 친구의 학점을 슬쩍 바꾸어둔 사실을 알았다면 어떻게 하겠는가? 컴퓨터 장난을 좋아하는 친구가 소프트웨어를 수집하려고 수업시간에 사용한 소프트웨어 디스켓을 복사해 달라면 어떻게 하겠는가?

특히, 데이터의 어떤 손상도 보통 심각한 윤리적 행동에 반한다는 사실을 명심해야 한다. 어떤 회사는 이런 윤리적 문제를 잘 준수할 것을 공식적으로 요구하면서 서약의 표시로 서명을 하도록 하고 있다. 직장에서 컴퓨터와 관련한 가장 시끄러운 윤리적 문제는 소프트웨어의 무단 복사이다. 하지만 일반적인 네티즌간에는 보통 시스템 관리자의 권한을 불법적으로 획득한 경우, 또 이를 악용해서 다른 사용자에게 피해를 준 경우를 해킹이라고 정의하고 있다. 예를 들면 추측이나 해킹을 통해서 다른 사용자의 패스워드를 알게 되어 도용을 하는 경우이다. 진정한 고부가가치 통신은 바람직한 정보사회의 실현을 위해서 누가 정보과정과 삶의 질을 누릴 것인가 이다.

정보통신윤리는 2백여년 전에 시작되었던 사회계몽주의 이후에 윤리학에서 가장 중요한 발전이였다. 칸트와 벤담은 인쇄기술과 산업기술에 의해서 변화된 새로운 혁명적인 세계에 대한 대응책으로서 그들의 윤리학을 발전시켰다. 다시 말하면 그들의 윤리학은 합리적이고 계산적 능력을 갖춘 서구 개인의 개념을 바탕으로 전개되었던 것이다. 그러나 이제는 컴퓨터와 정보통신 기술의 비약적인 발전에 따라 텔레커뮤니케이션과 가상현실(virtual reality), 시뮬레이션, 원격교육과 진료, 사이버섹스(cybersex)까지 가능한 정보통신 사회와 공동체로 도래하고 있다.

이 때문에 그러한 사회와 공동체를 인도하고 행동과 의사결정 과정에 지침이 되는 새롭고 강력한 윤리체계가 필요하다.

2. 해커발생에 따른 사회적 문제

해킹의 끝없는 조작은 정보통신 발달과 함께 비례하는 초고속정보도로망, 즉 Internet이다. 더욱 심각한 것은 인터넷의 전자상거래이다. 무인결제의 사인과 인장이 없는 확인결정이 문제이다. 다만 인터넷상으로 클릭만으로 대금결제가 이루어지는 전자상거래는 신속성과 편리성만이 능사가 아닌 것으로, 그 뒷부분의 검은 그림자가 드리워져 있음이 문제이다. 자칫 남의 구좌로 흘러 들어가는 인터넷 사기행각은 끔찍하기만 하다.

이미 세상에 알려진 공개키 64KB는 미국에서 공식화되어 있지만, 비밀히 개발된 공개키(key) 128KB는 명실공히 깊숙이 보관되어 있다고 보아야 한다. 이미 세계는 한눈 안에 훤하게 들여다 볼 수 있는, 강대국에 놀아나는 것이 현실이다. 현재 우리 나라에서는 이미 해커인구 2천만이 넘어서는 세계에서 2위를 앞질러 미국 다음으로 일본이 우리 다음으로 심각한 지경에 와있다. 우수한 두뇌와 창의적인 아이디어를 새로운 해킹 조작자로 전략하는 정보범죄자들이 수효적으로 늘어만가는데 위험성이 뒤따른다.

인터넷 전산망의 심각성은 청소년 범죄에서부터 PC방까지 음란물과 포르노가 범람하고 있다. 정보통신부 산하에는 캠페인이 한창이다. "해커가 되지 말고, 전문적인 기술인이 되자" 는 유인물이 배부되고 있다. 가장 심각한 것은 청소년 문제이다. 맞벌이 부부를 위한 자녀방치에서 몰래보는 섹스통신의 차단망에 대한 무료배포와 엄밀한 공간의 PC방을 위한 원격 차단망을 설치하고 무료지원되고 있다. 그리고, 정보통신부 산하에서는 틈새 없이 이루어지는 전산망 탐색작전은 정보범죄감시단원의 몫이 된다.

정보화 사회로 진입된 지금은 정보통신망이 거미줄처럼 깔리고, 미래에는 컴퓨터와 다양한 형태의 통신 네트워크들이 그 자리를 대신할 것이다. 우리 주변에서 이미 인터넷을 통한 정보수집과 금융 및 행정전산망 등이 일반화되었고, 우리의 생활패턴도 편리하게 윤택한 방향으로 변화시켜 왔다. 정보통신시스템에 대한 의존도가 커지면 커질수록 정보의 교환과 유통과정에서 발생하는 부작용도 크다.

컴퓨터와 정보통신 기술을 악용한 사기나 절도사건 그리고, 프라이버시 침해와 정보파괴 등은 그 대표적인 역기능들이다. 이런 문제는 1차적으로 사용자 개개인의 "정보윤리"에 달린 문제임이 틀림없지만, 범국가적인 차원에서 다루어져야 할 중대한 문제다. 이제 초고속정보통신망이 구축되고 활용되므로 통신정보보안이 사회적인 문제로 더욱 심각해진다.

〈표 1〉 해킹의 월별 현황

구분	계	학교	기업	ISP	비영리기관	금융기관	기타	국외	구성비율(%)
계	153	95	39	2	2	2	4	6	100%
1	18	16	1	1					11.76
2	1							1	0.65
3	97	62	33					2	63.4
4	2					1		1	1.31
9	31	16	3	1	1	4	4	2	20.27
10	2	1	1						1.31
11	1				1				0.65
12	1		1						0.65

자료 : 대검찰청 정보범죄 대책본부, 이정남(1999. 3)

"택일공"은 가정에서 청소년들의 음란 사이트 접속을 차단할 수 있는 S/W인, 녹스 S/W를 1999년 12월 31일까지 약 8개월간에 홈페이지(www.techol.com)를 통하여 무료배포 중이며, 맞벌이 부모님 2만 5천 가구 중 음란사이트 접속장치를 설치하여 재조사한 결과 1년간('89. 12 ~ '99. 12.)에 약 390만 건의 음란사이트 접속건수를 분석하였다. 하루 중에 시간대의 결과를 보면, 약 87%가 오후 6시~8시, 밤 10시~새벽 1시까지 채팅한다. 그 중에 1% 가량이 청소년이 찾는 음란 사이트를 채팅하고 있다고 한다. 더욱 적나라한 것은 성행위 장면이 3%로 가장 많았고, 가학성 변태장면이 23%이며, 몰래카메라가 20% 순서로 나타났다.

또한, 작년에는 정부가 소프트웨어 불법복제와의 전쟁을 선포하여 1999년 3월 31일 한국경제신문에서는 일제히 조사를 실시하였다. 정부의 S/W 불법복제 및 사용으로 인하여 중소기업 부도위기와 지적재산권 침해 회수가 한계에 이르게 되자, 전국 검찰에서는 대대적인 단속 지시로서 합동반에 발동이 걸렸다. 그리고, 대검에서는 합동단속반의 조사에 의하면 복제율이 전체 물량에서 70%로 불법복제국란 불명예를 안았다. 대상의 민간기업과 공공기관의 불법복제품 사용 여부와 음란물제작 및 유통과정에 관한 건. 그리고 조직 폭력배의 개입 여부와 대학교재의 무단복사 판매(상표도용, 영업 및 침해행위)를 대대적인 처벌강화로 지시되고 있다. 개정 컴퓨터의 프로그램 보호법의 WD역형, 벌금형 처벌강화로서 검찰은 지적재산 침해행위와 관련범인을 입건하여 고액의 벌금형을 처벌하고, 침해물품의 제작기기(製作機器)를 압수하였다.

국세청 통보의 고액 세금징수는 검찰의 국내 불법 복제율을 미국 수준인 27%로 낮출 경우에 기업의 매출이 늘어나서 고용창출의 기대효과를 높이고, 2001년까지는 2만 8천개의 추가

고용효과와 1조 5백억원의 추가세금으로 수입액이 늘어난다는 추산이다. 1998년말에는 지적재산권 침해에 대한 사범은 1만 7천여 명이며, 이 중에서 저작권법 위반이 8천2백여명으로 가장 많았고, 상표법 '부정경쟁방지법' 위반이 4천5백명과 음반 및 비디오 법률위반 건수가 2천5백명이 였으며, 특허위반건이 약 1천2백여명이다. 특히 대학가 교재무단 복제건수는 5백여 건으로서 출판사는 1천5백억원의 손해로 집계되었다. 그리고, 증권거래소 내에서 전산망의 해커가 침입하여 시스템을 교란시키는 행위와 증권감독원에서는 사이버거래 투자자보호문제로 투자자들의 교육이 문제였다. 정부 감독당국은 미국증권관리위원회(SEC)의 투자자에 대한 온라인 문제가 발생되었다.

예를 들면, 1만원 주식을 11,000원대로 매수가 한정되어 있다면 주문할 때 가격이 급증일 경우에만 비싼 값으로 구입하고, 계좌 현금잔고가 없을 때는 회사에서는 주식을 팔 권리를 가진다는 '98. 인터넷 사기와의 전쟁을 벌림(Internet sweep)에서 보고되었다. 또 (주)디지털미디어는 1암호를 이용한 보안기능을 갖추어서 게임방 원격제어 S/W인 "넷매니저"을 개발하여 출시하고 원격으로서 게임방 컴퓨터를 제어하여 일별 월별로 매회 매출 계산자료를 그래픽 자료로 출력하고 있다.

예를 들면, 주부 정보통신윤리위원회에서 학부모 정보감시단위원 음란물을 인터넷 사이트에 올리는 사람들과 음란 CD를 사고 파는 이들을 대상을 하고 대화방에서 음란대화를 나누는 이용자들을 탐색하는 고발대와 비정서적인 음란물 퇴치 및 유익한 정보발굴의 필요한 정보를 모니터하는 정보감시단은 밤시간대에 게릴라식 적발을 하고 있다고 1999년 4월 5일자 한국일보에서 보고되고 있다.

그리고, 정보의 바다에서는 해적 잡는 10대 사이버캅스는 3년째 청소년 정보감시단을 발동하고, 사이버공간에서 거래되는 S/W 불법복제거래 및 해킹과 ID도용 그리고, 음란물 유포 등 통신상의 성희롱과 건전한 정보문화에서 역행하는 행위들을 감시하고 고발하는 일을 담당하면서 청소년들이 스스로 고쳐나가려는 자구책의 노력이 필요함을 인식시키고 있다. 또한 결성자 원봉사 단체인 "Cyber Youth Cop(CYC)"인 청소년정보감시단의 활동하다. 사이버공간에서 이루어지는 부정적인 사고(思考)와 역행을 재인식시키는 자각과 개선의 노력을 하도록 하는 미래지향적인 봉사단체이다.

이제 정보통신상의 해커 인구가 5백만이 넘고 있는 우리 나라 인구의 15%가 통신해커 인구이다. 작년 1999년도에 92명의 여중생 자살 등 PC통신을 통한 각종사건이 보도되고 있다.

가령, 운전면허 취득자는 늘어나고 교통문화는 후진국이듯이, 컴퓨터사용과 교육의 부재로서 후진성을 면치 못하고있는 바이다. PC통신의 go youth 21C인 청소년정보감시단을 발동하고 청소년 문화연구소로 맹활약을 하고 있음은 정보통신 시대의 꽃이라고 할 수 있다. 불법음란물 연결의 벌금을 2~300백만원으로 정하고, 한국통신회선의 전화선으로 차단되었으며, 10차례 이

상씩 적발함에도 불구하고, 시정되지 않는 경찰의 근본적인 해결책이 필요하다고 한다(중앙일보 1999. 4. 8.).

1999년 3월 31일에 우리별 해커적발 3호에는 KAIST(한국과학기술원) 국산인공위성연구팀의 개인연구원의 컴퓨터에 침입(우리별 3호)하여 위성의 제원과 임무 등의 자료를 빼낸 해커 최모 씨는 올해 24세인 서울 K대학교 컴퓨터학과 4년은 경찰청 컴퓨터 범죄수사대에 적발된 사실도 뒤늦게 밝혀진다.

이같이 인간의 신체를 좀먹는 수많은 질환들의 전쟁에서 오늘의 첨단적 의술로 대체하고 해결하듯이, 새로운 기법의 해킹은 끝이 보이지 않는 정보두뇌 싸움이 된다.

3. 해킹방어와 가치관의 한계점

정보화사회 이후에 해커행위의 신종 범죄군에 대한 대처방안은 기술적인 정보범죄예방의 프로그램과 컴퓨터 범죄수사 전문가 양성 또한 형법에 의한 범죄처벌로 다양하게 다루어져야 한다. 앞서 순기능을 창출하기 위하여는 올바른 사용과 인간성 회복으로 가치관 높은 인식전환이 필요하다.

해킹의 침투가 가능한 환경적인 배경은 전산시스템 서버들의 기기중간접속 클라이언트-서버 접속과 호스트접속의 상호간에 정보교환에서 온다. 또한 과거와는 달리 사용자의 아이디와 패스워드의 등급별로 운영체제와 유틸리티 그리고 응용프로그램의 권한이 엄격하게 관리되었으나, 최근에는 전산망의 접속형태가 LAN, Lan to Lan, WAN, ISDN의 다양화로 발전되어 가면서 다종의 신종해킹들이 생성되고 있다

해킹(Hacking)은 컴퓨터 통신을 네트워크 조작방법과 시스템의 용량확장 방법을 알아내어서 보안의 허점과 불법적인 비전문적인 방법을 사용하는 행위이다.

크래커(Cracker)와 해커(Hacker)는 많은 차이가 있다. 해커는 단말기 또는 다른 컴퓨터 시스템에 침투하여 여러 가지 유형의 범죄를 저지르는 H/W적 정보 범죄인이다. 예를 든다면, 컴퓨터 통신의 네트워크 조작방법과 시스템 용량의 확장방법 그리고, 보안의 허점과 불법적인 행위이다. 그러나, 크래커는 해커보다 더욱 심각한 파괴적인 행위로서 시스템에 해를 끼치는 S/W적 정보범죄 이다. 즉, 복사방지 소프트웨어를 임의로 변경하고 불법적으로 프로그램에 영향을 주는 사람이다.

그리고, 정보를 지키고자 하는 노력의 정보보안은 정보통신망을 통해 유통되고 있는 정보들 가운데 비밀유지가 필요하거나 가치성과가 있는 정보를 보호하는 조치를 말한다. 해킹(Heaking)의 비상으로 인한 개인정보가 새고 있다. 국내 전산망보안 긴급진단에서 해외의 해

킹들의 홈페이지에는 국내 BBS와 해킹동호회에서 해킹프로그램을 다운 받아서 평범한 사람도 해커가 되기 쉽다. 시험삼아 경험으로 컴퓨터 시스템을 넘나들면서 쾌감을 맛보다가 완전범죄에 빠질 수도 있다.

대학전산망에 해커들의 온상이 되는 이유는 학생들의 BBS나 동호회의 동아리에서 운영하는 시스템의 패스워드가 간단하고, 보안관리가 이루어지지 않는 시스템에서 해킹기술의 실습장이 된다. 대학전산망 시스템은 도립 적으로 운영해야 함은 "96년 조사에 의하면 62%가 대학에서 이루어진다는 통계적인 결과가 나왔다. 이를 보완하기 위해서는 학생과 교수 그리고, 행정직원 중 담당책임이 명확해야 한다. 캠퍼스종합망을 구성할 때 학사행정 및 관리시스템 또한 교수연구실의 연구개발 및 학술용 시스템 등 대학을 대표하는 홈페이지나 메일서버 그리고, 네트워크 관리시스템 등 학생들의 실습용 시스템의 용도에 따라 적절한 전산망구성과 보안대책도 선행되어야 한다.

해커행위의 보안차단 방지책은 더욱 절실해진다. 아직도 일부 몰지각한 해커들은 자신의 행위에 대한 단순한 컴퓨터 실력과시와 영웅심리로 착각하고 아무런 죄의식을 느끼지 않는데 문제가 있다. 역기능의 발단은 유치원 교육에서부터 습관과 환경의 적응 그리고, 사고(思考)의 인식에서 비롯되는 것이다. TV 방송매체와 매스미디어 그리고, 뉴미디어까지도 그 역기능의 심각함은 세계인의 논제가 되고 있다.

Ⅲ. 해킹의 일반적 사례

1. 국내사례

사례 1 : 갑돌이가 을순이에게 연애편지를 보낸다면 다른 사람이 볼는지,

다른 사람에게 들어가는지, 내용의 무결성(integrity)이 보장될는지의 걱정을 해결해 주는 것이 정보 보안기술인 암호학이다. 다시 말하면, 정보를 보호하는 정보인 평문을 허용된 사람 이외에는 알아볼 수 없는 형태의 신호인 암호문(cryptogram,cipher-tex)으로 바꾸어주는 변환과정이다. 반대로 복호화는 허용된 사람이 암호문으로부터 평문을 끌어내는 역변환 과정이다. 암호화를 위해서는 해독자(cryptanalyst)가 암호를 해독하기 어렵게 하기 위한 방법을 비밀로 해야 한다. 비밀은 있을 수 없기 때문에 전혀 새로운 암호화를 해야 한다(1999. 3 .31 한겨레신문).

사례 2 : 사이버 테러

교통수단과 통신기술의 발전은 산업사회 발전에 기여하였지만, 그것에 걸맞는 정보욕구로서 컴퓨터와 통신기술이 오늘날 주류를 이룬다. 대중화된 교통수단, 첨단화, 고속화가 인간의 편리와 함께 인명을 앗아가고 무서운 무기로 변해만 간다. 미국의 의학계는 "암보다 무서운 것이 교통사고다"라고 했듯이 신속함과 편리함인 정보통신에도 많은 피해가 꼬리를 문다.

네트워크를 통해 다른 컴퓨터를 통해 중요한 데이터 파괴와 남의 은행구좌에 침입하여 현금을 인출한 사건은 매일 보도되고 있다. 컴퓨터 조작으로 항공기를 추락시키고, 병원의 전산망 침입으로 환자의 치료를 방해하여 생명을 앗아가는 일들이 외국 영화가 아닌, 현시로 다가오고 있다.

개인과 공공사업 분야에 비뚤어진 정보윤리관으로 범죄나 사생활 침해의 수단으로 악용되기 때문이다. 총이나 칼로 위협하던 때와는 달리 은밀한 공간에서 아무도 몰래 조작된 컴퓨터 프로그램은 무서운 범죄 도구가 되어 사이버 테러가 자행된다.

우리 나라에서도 국가 안보망에 침입한 해커를 대기업의 특채로 채용하고, 다시 새 정부에서는 특별 국가공무원으로 재 임용한 사실이 신문에 보도되었다. 자칫 특혜가 정보윤리 불감증을 가진 일부 컴퓨터 해커들이 자기실력을 공인받을 수단으로 착각할까 두렵다(동의대 컴퓨터공학과 김태석 박사).

사례 3 : 99. 3. 31 "우리별 해커적발 3호"

KAIST(한국과학 기술원)국산 인공위성 인구팀 연구원의 개인 컴퓨터에 침입(우리별 3호) 위성의 제원과 임무 등 자료를 빼낸 해커인 최모(24세 서울 k대 컴퓨터학과 4년) 씨를 경찰청 컴퓨터 범죄수사대에 적발되었다.

국내 해킹사건 1997년(64건), 1998년(153건), 1999년 3월(91건) 약 1달 평균 30.33건으로 급증세로 늘어난다. 전문가들이 보는 접수 사건수는 전체 5% 정도이다. 실제는 20배 가량을 초과됨을 분석되고 있다. 특히 해외 해커가 국내전산망을 우회(迂廻)침투경로로 활용한 경우가 전체 해킹사건의 70% 이상을 차지해서 국내 전산망이 다른 나라에 비하여 무방비상태로 허술함을 지적하고 있다. 1998년 전체 해킹사건 중 80% 가량이 해당기관에서 전혀 눈치채지 못하거나, 외국해킹 수사기관의 통보를 받고서야 해킹당한 사실을 알 정도로 국내전산망은 무방비 상태이다. 해킹사건이 급증하자 정보보호센터는 대학을 중심으로 활용중인 해커를 "제도권"내로 끌어들여 전산망 보안 진단전문가 그룹의 "타이거팀"을 활용할 계획임을 밝혔다. 정보통신부에 따르면 전세계 해커인구 9만명, 국내에 2천명으로 추산하고 있다(1999. 4. 19 인터넷 사냥).

사례 4 : 21세기를 맞아 요즘 해킹은 지구촌 사회의 새로운 문화로 자리잡아가고 있는 느낌이다. 다른 사람의 전산망에서 정보를 빼내 이를 이용하거나 남에게 팔아 돈을 챙기려는 절도성 해킹에서부터 다른 나라 정부의 전산망에 침투해 국방력에 타격을 가하려는 테러 해킹, 특정 홈페이지의 내용을 바꿔치기 하면서 해당기업이나 기관에 항의하는 시위성 해킹, 자신의 능력을 시험하기 위해서 도전하는 테스트 해킹, 해킹방법을 담은 책을 보고 심심풀이로 시도하는 초보해킹 등 세계의 전산망은 언제나 해커들의 표적이 되고 있다.

이동통신과 인터넷은 20세기 정보통신 기술의 "결정판"인 효용가치는 으뜸이다. 정보의 바다로 불리는 인터넷은 수십년 동안 백과사전의 대명사로 꼽히던 "브리테니커"를 밀쳐냈다. PCS와 셀룰러 등 이동통신은 무한 자유통신을 무기로 우리의 생활공간을 무한대로 넓혀가고 있다. 제1의 목표가 정보통신을 이용한 유토피아 구현이란, 사실에 비춰보면 우리의 삶은 분명 더욱 윤택하고 편리해질 것이다. 빛이 있으면 그림자도 있게 마련이다. 정보가 지닌 영향력과 중요성이 커질수록 그에 따르는 부작용도 만만치 않을 것이기 때문이다. 우리가 그동안 정보사회의 긍정적인 모습만을 보려고 애써 왔던 탓에 크게 부각되지 않을 뿐 "그림자"는 사실 오래 전부터 있어 왔다.

실제로 PC통신 등 정보통신망은 최근 각종 컴퓨터 범죄로 인해 그 순수성을 잃어가고 있고, 사이버 음란물 유통과 사생활 침해사례도 도를 넘는 수준에 이르렀다. 정보사회의 도래와 함께 등장한 이같은 문제들은 기존 가치관으로는 도저히 재단키 어려운 복잡성을 지니고 있다. 이 때문에 기존 가치와 정보통신 기술이 조화된 윤리적 기준, 즉 정보윤리란라는 새로운 개념이 탄생했다.

사례 5 : 정보통신의 익명성이 범죄 "부채질"

정보통신 기술과 관련 산업이 발전을 거듭하면서 등장한 사이버스페이스(가상공간)는 익명성을 특징으로 한다. 가상공간에서 벌어지는 다양한 유형의 범죄에 일일이 대응하기도 어려울 뿐만 아니라, 설령 발견했다 하더라도 적용할만한 법규정이 미비하다는 맹점이 있다. 어쨌거나 정보통신 관련 범죄의 개념정립은 모호하나 갈수록 심각해진다는 사실만은 분명하다. 대표적인 범죄유형으로는 악성 메일이나 바이러스를 입력해 다른 사람들의 컴퓨터 시스템을 파괴하거나, 타인의 사생활을 침해하는 사례를 꼽을 수 있다. 또 지적재산권 침해와 인터넷 포르노그라피는 (음란물) 정보사회의 대표적인 부작용들이다. 포르노그라피는 특히 인터넷이 개방형 구조를 갖고 있다는 점 때문에 규제가 어렵다.

우리 나라도 법적 제재가 효과적인 방안이라는 점은 인정하고 있으나, 현행 법제상 미비점이 많고, 기술적인 일괄 규제도 어려워서 구두선에서 그치고 있다는 적지 않은 질책으로 집계됐다. 특히 올해 들어서는 월별 위반사례와 음란물 유통 정보통신부에서는 이와 관련해서 지난

95년 4월, 불건전 정보의 유통을 막고 건전한 정보문화를 정착시키자는 취지 아래 정보통신 윤리위원회를 발족했다.

불건전 정보신고센터를 상시운영하고 있는 정보통신윤리위원회는 최근 사법기관과의 협조체제를 구축하는 등 보다 적극적인 대처방안을 마련 활발하게 활동하고 있다. 정보통신윤리위원회가 집계한 지난 1997년의 위반사례를 보면, 언어폭력이 31.90%로 가장 많았고, 음란물 유통(16.6%)과 불법 복제물 판매 광고(10.8%)가 뒤를 이었다.

이밖에 음란물 판매광고와 선거법 위반, 정크메일, 통신방해, 통신사기 등도 증가하고 있어 심각성을 더하고 있다. 한편 미국에서는 최근 들어 외설물이 범람하고 청소년문제가 심각해지면서 통신품위법(CDA-2)의 입법을 추진하고 법제화를 눈앞에 두고 있다.

사례 6 : 해킹, 사이버 테러리스트의 "파열경쟁"

아무리 좋은 문명의 이기(利器)라도 "야누스의 얼굴"을 갖고 있기 마련이다.

서울과 부산을 5시간에 달릴 수 있도록 만든 자동차는 종종 살인무기로 돌변한다. 칼은 식당에서 당근을 요리해야하지만 때로는 사람을 찌르기도 한다. 컴퓨터도 예외가 아니다. 정보통신 기술은 현대문명의 꽃이다. 현대사회의 거의 모든 생활시스템은 이제 정보통신 기술을 기반으로 형성되고 있다. 특히 인터넷의 등장은 정보통신을 더욱 빠르게 대중 속으로 파고 들게 하고 있다. 이미 우리는 정보통신의 굴레에서 벗어나 하루도 견디기 어려운 시대에 살고 있다.

그 주역인 컴퓨터는 우리 경제생활에 깊숙하고 폭넓게 들어와 있다. 컴퓨터 버튼 하나만 누르면 개인신상이 적힌 주민등록등본이 흘러나온다. 집에서 PC로 세금을 낼 수 있다. 국민과 정부는 이제 인터넷을 통해 서로 정보를 교환한다. 사무실에서는 종이가 사라지고 있다. 상사에게 올리는 보고서 결재는 이제 컴퓨터의 몫이다. 회사정보는 모두 네트워크를 통해 흘러 다닌다. 사무실에 앉아 컴퓨터로 수출입 관련업무를 처리할 수 있다. 은행이나 선박회사를 찾아갈 필요도 없다. 백화점이 아닌 사이버공간에서 물건을 구입하고 팔고 대금을 거둬들일 수 있다. 가정도 변하고 있고, 주부는 번잡한 백화점에서 인파에 시달리지 않고도 집에 앉아서 컴퓨터로 시장을 볼수 있다.

컴퓨터가 알려주는 여행코스를 따라 가족여행을 즐긴다. 학생들은 책 대신에 CD롬 타이틀로 다양하고도 생생한 학습기회를 갖는다. 인터넷폰으로 이민간 친구에게 마음껏 전화할 수도 있다. 정부, 기업, 소비자 등 모든 경제주체들은 컴퓨터 네트워크에서 다양한 질 높은 삶을 누리고 있다. 야누스가 갖는 밝은 쪽의 얼굴이다.

그러나 어둠의 세계로 들어가면 정보통신은 전혀 다른 모습으로 우리를 위협하고 있다. 밤의 세계에서 활약하는 존재들은 마치 암세포처럼 확산되고 있다. dlemv은 해커, 바이러스, 테러리스트, 사기꾼 등의 모습으로 컴퓨터 주위를 돌면서 이런저런 해약을 만들어내고 있다.

지난 1995년 국내최초 K대학 공대전산실 침입하여 시스템을 흔들어 놓고 빠져나갔다. 이제 P대학 시스템으로 보복을 했다. 장난으로 시작된 해킹은 절도, 사기 등 범죄로 발전하는 갈수록 과감해진다. 인터넷 사업자의 홈뱅킹시스템을 해킹해서 불법계좌 이체를 시도한 사건(96), 망사업자의 게시판 자료삭제 사건(97), 대학의 주요 프로젝트 자료삭제 사건(96)이 최근 표면화된 문제들이다. 또 사이버 테러리스트도 등장하여 프로그램을 망가뜨리는 바이러스를 만들어 유포시킨다. 정부기관, 금융업체, 항공사 등의 대형 전산시스템에서 누가 더 많은 실적을 올렸는지를 네트워크에서 파열경쟁을 벌이곤 한다.

PC통신과 인터넷은 청소년들의 건전한 정서를 해치기도 한다. 음란물 유통으로 성에 대한 의식을 왜곡시킨다. 전화방 등의 음성폰팅은 위험수준에 달했다. 비틀린 속이 비어가서 네트워크를 타고 청소년들의 언어문화를 거칠게 한다.

2. 국외사례

사례 1 : MS 골탕먹이기(짙은 의혹)

'멜리사'를 만든 범인 미국 수사진의 추적(컴퓨터바이러스 이름) 안창수 컴퓨터 바이러스 연구소의 고정 연구원은 31일 "멜리사는 마소의 독점 전권횡을 '증오'하는 높은 수준의 프로그래머가 제작했을 가능성이 크다"고 추정한다. 이는 마소의 제작문서 편집 프로그램인 워드와 전자메일 프로그램(아웃룩 익스프레스)을 통하여 전염된다.

"워드 2000, 워드 97을 주력함"의 판매상품에서만 바이러스가 감염됨을 추정하고, 이유는 전산망을 교란하기 위해서라면 최신버전과 특정 프로그램을 선택하지 않았을 것이라고 한다. 마소 빌게이츠 회장 부인이름과 같은 점도 추정하고, 회장을 조롱하기 위해서 그 부인이름을 본따서 바이러스 이름에다 붙였을 것으로 사료된다. 마소 사용자의 반감이 유럽전체에서 높다는 점을 감안하여 망신 주려는 의도가 보인다고 추정한다.

또 E-메일로 음성변조로 직장분위기를 흐리게 한다. USA 투데이 5일 보도에서 인터넷 사용업체에서 근무자 직원 중 절반 이상이 근무 중 음란성 농담과 성차별 인정차별적인 언사가 담긴 E-메일을 받은 사실이다. 살로먼 스미스 바니사 Emapdlfdp 포르노물을 전파한 2명의 간부사원을 파면시키고, 음란성농담이나 중요성 발언의 검색에 나서 적발될 경우 즉시 해고된다고 경고를 하였다.

한편 모건스탠리딘 워터사의 두 전직 흑인직원들은 인종차별적 농담을 E-메일로 받은 뒤 회사를 상대로 소송제기하고, 노동관계 전문가들은 컴퓨터 속성의 면전에 대고 하기 어려운 말도 마음대로 하게 만든다면서 직장내 음란 메일이 날로 증가됨을 지적되었다.

사례 2 : 해커 대역습인 유고 해커 NATO 웹사이트 공격(99. 4. 1)

북대서양 조약기구의 웹사이트가 유고 해커들로 보이는 컴퓨터 전문가들의 공격으로 당일 일시 마비(영국 BBC방송 3. 31).

제이미시어 나토 대변인은 해커들이 인터넷을 통해 빈 문서 수천 건을 나토 컴퓨터에 한꺼번에 보내는 이른바, '다니엘 서비스'로 인터넷사이트의 작동을 중단시키는 사건, 또 베오그라드의 한 컴퓨터에서 하루 2천건 이상의 E-메일이 송신되어, 나토의 E-메일 속도가 크게 떨어졌으며, 멜리사 바이러스와 비슷한 것이 E-메일에 첨부된 문서를 통해서 나토 컴퓨터에 침입했다고 시어 대변인이 밝혔다. 이런 컴퓨터 오작동 현상은 일시적으로 인터넷파일을 모두 삭제한 뒤 해결되었으나, 또 다른 바이러스가 컴퓨터에 침투했다고 사용자들이 보고하였다.

사례 3 : 해커영화(테트)

미국 뉴욕 맨허튼의 어둠침침한 사무실의 한 젊은 여성이 컴퓨터 키보드를 두드리고 있다. 공공기관 전산시스템에 침입한 해커악당을 잡아내는 게 그의 일이다. 악당들은 항공관제시스템을 해킹하고, 여객기의 고도를 마음대로 조종해 추락시킨다. 병원 프로그램을 바꿔 환자에게 엉뚱한 약물이 투여되도록 해서 결국은 죽음으로 이르게 한다. 그녀는 악당과 힘겨운 네트워크 싸움을 벌인 끝에 결국은 승리하게 된다. 그녀는 "우리의 모든 생활은 컴퓨터에 담겨 있다. 컴퓨터에 의해 우리 생활은 철저하게 파괴될 수 있다"는 대사를 남긴다.

얼마 전 개봉된 영화 〈테트〉의 한 장면이다. 이 영화는 컴퓨터가 얼마나 무서운 존재인지를 잘 묘사하고 있다.

3. 사례를 통한 시사점

이제 날이 더해갈 수록 늘어만가는 우리 나라의 사이버 통신네트워크 기술은 세계적이며, 미국 일본보다 해가 거듭할수록 통신인구는 늘어만 간다. 또한 이에 맞서는 신종해킹도 증가되고 새로운 차단방어 프로그램이 쏟아져 나와서 인터넷 통신망을 어지럽힌다. 인간의 건강을 해치는 불치의 병균처럼, 이름 모를 병명을 난발시키듯이 인간을 불안과 죽음으로 몰고 가는 불치의 병을, 오늘도 세계적인 석학들은 밤새워 연구진에 몰두하고 인명을 구조하고 있다. 의술은 전문의를 끝없이 도전시키고, 영약의 특효약을 개발하고 있다. 이처럼 만물의 영장인 인간들이 일부 몰지각한 해킹행위자는 개인적인 흥미와 사기행각적인, 허욕과 망상에 젖은 해커는 이 시간에도 독버섯처럼 생성되고 있다.

이미 우리는 세계적인 통신기술에서 우수성을 평가를 받고 있다. 최초 게임으로 경기하는

아이디어와 정보통신의 인터넷을 연결한 폰을 개발하여 세계인을 집중하게 하는 38세의 우리나라 사람이다. 세계 인터넷 통신인구는 벌써, 세계 2위, 창의적인 아이디어와 새로운 도메인 탄생도 세계인을 경악과 감탄하게 한다.

미래 학자들은 우리국민의 평가를 이미 양극을 달린다는 천리마로 정평이 나있다. 순기능의 측면에서 보는 전문가들은 개인과 창업의 새로운 지적재산형성과 일상생활의 편의성 향상과 생산성 그리고, 전자민주주의 확산과 전자게시판과 대화형 도구 활용에 의한 관료주주의 쇠퇴 등은 지식과 정보에 의존하는 새로운 경제모델로 촉진될 것이라고 강조하고 있다.

반면 역기능이 갖는 부정적 측면을 경고하는 지나친 기술 의존에서 오는 인간의 상실과 정부 그리고, 대기업들이 개인의 사생활까지 감시할 수 있는데 따른, 새로운 형태의 독재와 지적재산권의 무분별한 도용 및 복제로 인한 경제적 무질서는 원격민주주의가 초래할 가능성이 있는 우민(愚民)화, 정보의 부자와 빈자 사이에 생기는 국가간 세대간 그리고, 계급간 분쟁확대 등에 대한 우려이다.

결국 이같은 순기능과 역기능의 공존은 피할 수 없는 것이 된다. 중요한 것은 순기능을 극대화시키고, 역기능을 최소화해야 한다. 이것을 위해서는 정보화사회에서는 적합한 새로운 윤리의식과 가치관 정립이 요구된다. 인간의 심성과 도덕관이 서지 않는다면 정보통신산업, 나아가서 인간의 생존에까지 크게 위협을 받게 될 것이다.

우리 나라는 좁고 부존자원이 빈약하나, 70%의 지형인 자연조건과 30%의 삶의 터전에서 우수한 두뇌로서 인구밀도만큼이나 다양한 소프트웨어가 된다. 이제, 세계인은 우리를 두려워한다. 끝없는 해킹행위를 중단하고 높은 가치관을 발휘하여 정보통신 종주국으로 한 단계 높이자.

Ⅳ. 해킹방지 프로그램 개발현황

1. 범국가적 차원의 정보안전장치

FBI의 추측에 의하면 컴퓨터 범죄의 10% 미만 정도가 감지되고 있고, 이들 중 일부만 보고되고 있다고 한다. 컴퓨터와 관련이 없는 사무직 범죄에 비해서 컴퓨터 범죄당 손실액은 200달러에서 거의 20억달러에까지 이르는 범위로서 매우 높은 편이 된다. 평균 손실액은 450,000달러로 다른 사무직 범죄보다 5배 정도가 높다. 미국내에서는 현재 FBI가 컴퓨터 범죄에 대한 전쟁을 벌이고 있으나, 이러한 종류의 범죄를 명확히 금지하는 연방법의 부재와 3/4 이상의

컴퓨터 비행이 법이 규정하는 완전히 기소할 수 없는 청소년 범죄에서 이루어진다는 사실에 어려움을 겪고 있다. 이 문제의 해결을 돕기 위해서 FBI와 여러 지방집행기관들은 훈련 프로그램을 제정하였다고 한다. 때로는 해커(hacker)또는 컴퓨터광을 고용해서 컴퓨터 범죄를 감지하거나 방지하는 일을 돕도록 하는 경우도 있다. 또한 그저 장난을 일삼는 행위 중에 이윤추구와 관련이 없는 컴퓨터 범죄도 있다. 컴퓨터 시스템내의 데이터에 대한 고의적이고 교묘한 손상은 많은 손실을 가져오고 감지하기도 어렵다. 그리고, 악의적인 손상 중에서 가장 심각한 유형이 자신을 다른 소프트웨어에 복사해서 소프트웨어를 못쓰게 만드는 로그프로그램인 컴퓨터 바이러스(virus)이다.

컴퓨터 바이러스는 정상적인 소프트웨어로 위장해서 무해한 프로그램인 것처럼 보인다. 그러나 이들의 목적은 의심하지 않는 사용자의 컴퓨터상의 로그프로그램과 데이터를 파괴하는데 있다. 바이러스 프로그램은 보통 공공도메인 소프트웨어를 교화할 수 있는 컴퓨터 게시판 상에서 유용한 프로그램 혹은 유틸리티라고 광고된 바이러스로 그 프로그램을 선택하게 된다.

이러한 프로그램을 실행시키면 모든 정보를 파괴하기 시작한다. 디스크에 저장된 모든 프로그램과 데이터를 황폐화시킬 수 있다. 대형 네트워크상의 모든 컴퓨터들은 1분 이내에 감염된다고 하며, 다중사용자 시스템은 5분 이내에 파손된다고 한다. 또한 바이러스 프로그램에게 시달리는 컴퓨터 게시판의 운영자들은 이미 확인된 디스크-파손 프로그램 목록을 사용자들에게 보내어 경고하고 있다. 대학 캠퍼스나 대형 사업체들의 조직된 컴퓨터센터 직원들은 사용자들에게 바이러스 프로그램의 잠재적인 위협을 경고하고 있다.

바이러스에는 두 가지 변형이 있다. 가장 단순한 변형의 예는 Egabtr이다. 화면 그래픽 기능강화 프로그램으로 가장(假裝)한 이 프로그램은 디스크 파괴 코드를 포함하고 있다. 이러한 프로그램은 매우 빠르고 치명적이다. 이들은 디스크에 저장된 정보를 즉시에 파괴해 버린다. 더 심한 것은 몇 주 또는 몇 달간 숨어서 하드디스크와 플로피 디스켓을 전염시킨다. 미리 지정된 시점에 도달하면 모든 감염된 소프트웨어가 무기력해 진다.

한 예로서 캘리포니아기술대학(C.I.T.)의 배리 사이몬(Barry M. Simon) 씨는 "고등교육의 연대기(the Chronicle of Higher Education)"에서 "바이러스를 작성하는 사람들은 자랑하기를 좋아한다라고 했고, 그들은 대개 자신이 한 일에 대해 어떤 실마리를 남겨 놓는다."고 말한다. 불행하게도, 이미 이러한 메시지가 나타날 때는 이미 늦은 상태라고 한다. 즉시 "Arf, Arf! Gotcha!"라는 단어를 화면에 표시한다고 한다. 컴퓨터로 짓궂은 장난을 하는 사람이 이미 수년 동안 대학캠퍼스에 있어왔다. 아직도 이러한 위협에는 더 이상 경계가 지워져 있지 않다.

다시 말하면, 바이러스는 모든 곳의 컴퓨터를 감염시킬 수 있고, 게시판을 사용하거나 컴퓨터 네트워크의 일부를 이루고, 다른 사람과 디스크를 공유하는 사용자들은 감염에 노출되어 있

다. 이에 대한 해결책은 아이디어와 정보의 공유를 잃게 만든다.

프로그램 디스크 쓰기를 방지하고, 언제나 백업을 받는 것이다. 동료나 게시판 또는 네트워크로부터 가져온 모든 프로그램은 하드드라이브를 끄고, 운영체제의 백업 사본을 준비한 상태에서 실행해 보아야 하며, 일시라도 방심하지 말아야 한다. 그러나 어떤 프로그램도 모든 바이러스에 대한 방지를 막아 줄 수는 없는 것이다. 항상 주의깊은 경계와 소프트웨어 및 주요 데이터에 대한 백업사본만이 컴퓨터 바이러스에 대한 유일한 보장방법이다. 바이러스 검사 소프트웨어는 "Data physician, C4Bomb, Disk Defender"이다.

〈표 2〉 보안의 분류

No	대분류	중분류	소분류	세분류
1	물리적 보안	액세스관리		
		정돈관리	입력, 출력, 매체, 환경	
		방재관리	방화, 방수, 방진, 가스방지	
		전원관리		
		백업관리		
2	논리적 보안	식별관리	패스워드	
			휴대품	신분증명서, 인감, 뱃지, 열쇠
			개인적 특징	얼굴, 목소리, 서명, 지문
		데이터파일보호관리	패스워드, 데이터 보호, 소프트웨어	
		라이브러리관리		
		암호관리		

2. 대상별 침해수법과 대책

대상별 침해수법에는 접속망 분리형의 보안장치를 출시하고, 전산환경에서는 자동적인 접속망에 대한 분리차단과 보안장치공급 S/W를 "레프네트"의 대표자인 김영근 사장이 개발했고, PC 접속장치인 "네스" 위치는 서울 비즈니스 네트워크 공급의 IP(체인저)를 내장하고, 네스 위치를 연결하여 한번의 클릭과 버튼작동이 이루어진다. 외부 해커 침입은 네트워크를 PC에 접속하여 보안대책이 이루어진다. 따라서 공공기관의 PC 사용자들은 인터넷과 내부 망의 변환

시에 일일이 수작업으로 포트접속을 조정하는 번거로움을 감수해야 한다.

항상 해킹의 수법과 대응하기 위하여 기본적인 대책을 강구해야 한다. 조직에서는 체계적인 보안정책을 수립하고, 안정된 firewall 설치를 하고, 정보의 보안 코드사용을 하여야 한다. 또한 주기적인 백업을 시도하면서 새로운 버그에 대비하여야 한다. 조직구성원의 철저한 기본교육과 각별한 관심을 두어서 침해 방안을 세운다.

또한 컴퓨터 시스템 안전대책에는 정보화사회의 컴퓨터, 단말기, 데이터 통신회선의 총체인 컴퓨터 시스템의 보급이 급속도로 진전되고 있다. 커뮤니케이션 시스템에 의한 데이터처리는 각종 산업행정업무를 컴퓨터 시스템에 의한 정보처리 자체에 의존하고, 다수인의 생명과 신체적 재산상의 안전을 컴퓨터 시스템에 의하여 처리되고 있다. 그러나 해킹침입을 당했을 때 사람의 생명이나 신체에 위험이 발생되고, 재산상의 막대한 손해와 사회질서의 혼란이 야기될 우려가 될 수도 있다는 것이다.

예를 들면, 자동열차운행과 제어시스템이나 항공관제 제어시스템 그리고, 원자력발전 제어시스템과 댐 수량관리 제어시스템 등은 모든 컴퓨터 시스템에 의하여 자동작동되므로 컴퓨터 범죄나 사고로서 데이터처리가 정상적으로 이루어지지 않을 경우에는 돌발적인 충돌과 폭발 그리고, 화재와 천재지변의 수해(水害)등의 대형사고가 발생할 위험성 있다. 은행업무나 종합 온라인시스템, 증권거래 온라인시스템, 크레디트카드 시스템 등의 범죄는 대부분이 규모도 크고, 교묘한 수법을 쓰고 있어서 발견이 어렵다. 피해자도 일반 절도범과는 달리 다수인에게 막대한 금전적 손실을 주게 되고, 그 나라의 경제질서와 혼란들은 이들 시스템에 대한 불신을 초래하게 한다.

그래서, 그 예방과 방지대책 수립에서는 안전대책과 물리적 대책 그리고 관리적 대책과 기술적 대책으로 분류하고 있다. 특히 물리적인 대책에는 고의적 우발적인 위험에 대처하기 위한 보호조치를 의미하며, 화재나 홍수, 사보타지, 폭동, 폭탄장비 등 불가항력적인 천재지변의 재해에도 신속히 대처해야하며, 데이터센터의 위험을 방지하고 위험발생을 최소화하고 사람과 재산을 보호해야 한다.

최신 해킹 테크닉은 Web 공격의 인터넷=WWW 공식처럼 Web 서비스의 중요성은 전자상거래의 주류를 이룬다. Web 기본통신이 갖는 프로토콜 TCP/IP를 악용하고, 서버/클라이언트 사이에 해커가 조작한 명령들을 삽입했다면 많은 혼란을 초래할 상거래가 될 것이다. 클라이언트 레벨에서의 해킹유형은 웹서비스를 이용하는 클라이언트내의 정보를 훔쳐내는 해킹의 경우에 두 가지가 있다.

첫째, 클라이언트내의 파일을 서버쪽에서 읽어 들임으로써 사용자의 패스워드나 신용카드번호, 전화번호 등의 중요한 파일들이 유출될 수 있다. 1999년 6월초 발견된 Shockwave Plug-in을 이용해서 사용자의 메일박스 내용을 해킹한 사건과, 둘째 클라이언트로 하여금 서

버가 명령하는 엉뚱한 Java Applet이나 악(惡)의적인 목적의 Java Applet을 실행하게 한 것 등이다. 또한 마이크로소프트사의 인터넷 탐색기에서 가장 처음 발견된 보안문제점도 LNK 파일을 이용하여 클라이언트 시스템내에서 임의의 명령이 수행되게 한 유형의 해킹이었다.

이의 해결책 1)에서,

클라이언트 레벨의 해킹에 대하여 특별히 사용자가 취해야할 사항들은 소프트웨어를 공급업체로부터 지원되는 최신 버전의 프로그램을 사용하거나 옵션에서 보안관련 부분을 최대한 강력하게 인증하는 방법이다.

다음은 사이버 레벨의 해킹은 특정 웹사이트를 해킹하려고 할 때 웹서비스 자체의 취약점을 공격할 수도 있지만, 웹사이트에서 외부에 공개되는 다른 서비스들을 이용하여 웹사이트내의 접근권한을 얻을 수도 있다. 특별히 UNIX 웹사이트일 경우에는 더욱 더 심하다. CGI를 이용하는 웹페이지에는 메타문자를 인자로 넘겨서 쉘이 실행되게 하고, 또는 웹사이트로 모든 접속을 가로채어서 중요한 정보만을 골라서 악용하는 해킹도 있다.

이의 해결책 2)에서,

웹서비스의 웹 문서나 웹사이트에 IP주소나 호스트 이름을 이용해서 웹사이트에 접근을 제한한다. 사용자명과 해당 암호를 이용해서 접근을 제한할 수도 있으며, 서버/클라이언트 사이에 오가는 패킷들을 SSL이나 SHTTP 같은 프로토콜을 이용하여 암호화시켜서 전송할 수도 있다. 이런 해결책들도 Spoofing이나 악의적인 Java Applet들을 이용하여 충분히 해킹할 수 있으므로 해결책은 On-Line 쇼핑몰로 차단된다.

그리고, 요즈음 전자상거래(EC), 인터넷이 급속히 확산되면서 올 상반기 국내 해킹 발생건수가 지난해보다 2배 이상 늘어나는 등 인터넷 보안에 적신호를 울리고 있다. 해가 거듭할수록 해킹기법도 점점 지능화되어서 대책마련이 더욱 심각하다.

한국정보보호센터에 따르면 올 들어 3월말까지 발생한 해킹사고 건수는 91건으로 지난해 같은 기간 24건보다 4배가 늘었다. 신종 해킹기법의 종류로 'S스캔 공격'은 네트워크의 허점을 자동으로 알아낸다. 침투방법은 '트로이목마 공격' 으로 유용한 프로그램처럼 가장해서 전산시스템에 침투하는 방법이며, 마지막으로 '바이러스 공격'에는 컴퓨터 바이러스를 이용해서 정보를 빼내는 신종해킹이 등장하고 있다. 1999년 3월에 발생한 신종해킹 back orifice(백오리피스)는 개인용 컴퓨터를 그대로 들여다보는 기능이므로 개인 정보유출이 우려되는 프로그램이다.

지난 1월 국내 처음 보고된 S스캔 공격은 원격지에서 불특정 다수의 전산 시스템을 대상으로 허점을 찾아내는 프로그램인 S스캔을 이용하여 취약점을 찾아내는 전산망으로 불법 침투하는 해킹 기법이다. 미국 해커로 추정되는 바하가 개발한 해킹용 프로그램 'S스캔'은 다수의 인

터넷 사이트를 대상으로 하여 운영체제의 종류와 취약점을 자동으로 파악하여 공격하는 위력을 갖추고 있다고 한다.

해커는 이 프로그램으로 취약점을 발견하면 바로 시스템에 침투하고 자료유출 또는 시스템 파괴 등의 활동을 할 수 있게 된다. 특히 트로이목마 공격은 해킹용 프로그램을 인터넷 검색 프로그램인 '익스플로러(파일명 ie0119.exe)'와 인터넷 보안용 프로그램인 '래퍼(파일명 tcp wrapper)' 등으로 위장해서 시스템에 침투시키는 방식이다.

만약 사용자가 이 프로그램을 전송받아서 자신의 컴퓨터에 설치하면 자동으로 해킹 프로그램이 작동되어 해커가 침투할 수 있는 길을 열어주게 된다. 그리고, 바이러스 공격은 전자우편에 기생하는 멜리사바이러스를 인터넷에 통하여 유포하여서 바이러스에 감염시킨다. 감염된 컴퓨터의 기밀문서를 자동으로 빼내어 갈 수 있도록 하는 해킹방식이다. 국내에서도 지난 3월에 물의를 일으켰던 것의 이 공격은 일단 바이러스에 감염되면, 자신도 모르는 사이에 컴퓨터에 보관된 기밀문서가 인터넷을 통하여 유출되어 나가는 심각한 피해를 일으킨다. 이를 막기 위해서 한국정보보호센터 관계자는 "해킹기법은 최근에 날로 지능화 되고, 국내기업과 대학에서도 대응책은 속수무책으로 제자리걸음이다."라고 발표하고 있다.

이제, 거액의 자금이 인터넷 전자상거래를 통하여 이동하기 때문에 해킹사고는 대형금융사고로 이어질 가능성이 높을 것으로 심각할 지경이다.

이의 해결책 3)에서,

방화벽 시스템에서 허락되는 서비스와 액세스를 정의하는 것 같은 보다 큰 보안정책의 수행을 도우며, 네트워크 구성을 하나 그 이상의 호스트 시스템 관리와 라우터의 안정된 패스워드에서 진보된 인증 같은 정책의 수행이다. 내부 네트워크 보호를 위해 외부의 불법적인 트래픽 유입을 막고, 허가되고 인증된 트랙팩만을 허용하려는 적극적인 방어대책이 필요하다.

첫째, 취약한 서비스로부터 보호

둘째, 호스트 시스템으로의 액세스 컨트롤

셋째, 보안의 집중

넷째, 확장된 프라이버시

다섯째, 네트워크 사용과 비사용에서의 로깅과 통계자료

여섯째, 정책시행으로서 방화벽 시스템의 기본 구성요소에는

1) 네트워크 정책(Network Policy)의 제한된 네트워크로부터 서비스를 허락할 것인가 또는 명확히 거부할 것인가를 정의하는 네트워크에서 액세스 정책에 대한 서비스를 허락할 것인가의 이러한 정책의 예에 대한 조건 등이다.

2) 방화벽 시스템의 사용자 인증시스템(Advanced Authorization)은 우수한 인증수단의

Stmartcards, Authentication tokens, Biomefrics 그리고, 소프트 메커니즘을 사용한다.

3) 패킷 필터링(Packet Filtering)은

- destination IP address
- TCP/IP source port
- TCP/IP destination port

4) 응용계층 게이트웨이(Application Lerel Gateway)의 가상서버(Proxy Server)라는 인터넷의 클라이언트/서버 개념에서 나온 서버기능을 제공하게 된다.

5) 스크린라우터(Screen Rauter)는 어느 정도 수준의 보안 접근제어를 통하여 방화벽시스템 환경을 구현할 수 있으나, 라우터에서 구현된 펌웨어 수준으로는 제한점이 많고 복잡한 정책을 구현하기 어려우므로, 보통 스크린라우터와 다음에서 설명하는 베스천호스트를 함께 운영한다.

6) 베스천 호스트(Bastion Hosts)

7) 이중네트워크 호스트(Dual-Hoaned Hosts)

8) 스크린서브네트(Screen Subnet) 등으로 방화시스템의 기본요소로 이루어진다.

3. 전자파 외부발산 차단방법

금속으로 코팅된 CRT 스크린 사용과 보호 케이블을 사용하고, 외부 케이블 연결시에는 전기 필터사용을 한다. 그리고 암호화된 화면 디스플레이에는 화면에 나오는 영상의 패턴순서를 바꾸는 방법이며, 코드 키를 사용하여 패턴순서를 바꾸는 방법을 계속하여 변화시킴으로써 수집된 전자기파를 분석하지 못하도록 한 것이다.

또한 컴퓨터 하드웨어에서는 디지털 장치에서 square wave 신호와 높은 스위칭 주파수는 UHF 영역의 주파수를 포함한 전자기파를 발산한다. 전자기기의 내부회로로부터 발산되는 전자기파는 주파수의 증가에 비례하여 강해지며, 전자기파를 수집하여 정보를 얻어내는 것이 가능하다고 한다. 미국에서는 템피스트(TEMPEST)의 코드명으로 전자장치 발산에 대한 전자기파의 제한기준을 만들었으며, 그 기준으로 미국의 NACSIM 5100A, NATOm의 AMSG 720B 등이 있다. 미국의 NASCM의 평가방법과 요구사항은 외부에 알려져 있지 않으며, 특별위원회인 TQSC에의해 인가된 장치는 "Tempest preferred product list"(PPL)에 올려지고, 미국 정부의 허가 없이는 일반인에게는 팔거나 수출하지 못하도록 되어 있다 한다.

NATO의 AMSG 기준은 군대와 정부의 전자장치에 대하여 적용되는 특별한 것이다. 모든 전자장치의 반도체 칩과 모니터 그리고 프린터 등으로 대기중의 전자기파를 발산하며, 이렇

게 발산되는 전자기파를 통한 정보유출의 위험성 때문에 외국의 경우에는 연구활동과 정책의 수립이 활발한 상태이다. 적절한 전자파의 차단기 장치를 하지 않는 상태에서 모니터에서 나오는 전자기파는 1km 이상의 먼거리에서도 수집 할 수 있고 분석이 가능하다고 한다.

예를 들면, 화상회의도 적절한 전자파 차단 장치를 하지 않으면 회의 내용중의 중요정보를 외부에서 탐지할 수 있게 된다. 개인용 컴퓨터를 사용해서 텔레뱅킹을 이용할 때에 개인의 계좌번호 비밀번호도 유출될 수도 있다.

첫째, 침해방법에는 간단한 방법으로 흑백 텔레비전이나 안테나 그리고 증폭기만으로 전자파를 이용한 정보탐지를 할 수 있으며, 현재 모니터링 장치로서도 Datascan과 Williams Van Eck System 등의 장치가 판매되고 있다. 이들의 장치를 이용하면 특정 장소로부터 나오는 전자기파를 분석하여 유용한 정보를 얻어 낼 수 있는데, 플라스틱으로 보호하고 있는 전자장치는 1cm 금속으로 보호할 때에는 200m 거리 밖의 전자파를 분석하고 그 내용을 알 수 있다고 한다.

둘째, 해결책으로서는 발산되는 전자기파의 세기 감소로는 회로가 동작에 필요한 속도보다 빠르게 스위칭 하는 디지털장비를 사용하지 않고, 전기회로 중에서 전자기파를 발산하는 부분을 가능한 적게 해야 한다. 특히 주의해야 할 점은,

- 전자장치의 내부 도선을 가능한 작게 한다.
- 모니터 주위에 전자기파 차단장치를 설치한다.
- 이때 전자기파 차단효율은 장치의 두께에 비례한다.
- 모니터 부분의 열려 있는 점
- 케이블의 차단장치를 뚫고 들어와야 하는 점
- 키보드나 통풍장치 부분이 열려 있는 점을 잘 관리해야 함이다.

또한 SYSTEM 개발용으로는 현재 사용되는 card system은 magnetic tape card와 IC card가 있으며, 자기카드는 은행에서 현금카드(신용카드)로 쓰이고, IC카드는 자기테이프 카드보다 보안에 유리하고 그 수명이 길고 안정적인 점으로 인하여 출입문의 제어와 정보의 안전한 전송과 버스카드 등, 여러 가지 용도로 사용되고 있으며, 최근에 전자주민카드를 이용하여 개발하고 있는 중이다.

그리고 침해방법으로는 첫째, 복제사용으로서 짧은 시간에 자기테이프 카드를 복제하여 사용하는 방법으로서 불법적 사용으로 금전적인 피해를 준다. 둘째, 카드리드 이용방법으로써 IC 카드를 카드리더기를 이용하여 저장된 정보를 열람하고 삭제와 수정할 수 있다. IC카드의 해킹 방법은 1997년 8월 HIP '97(Hacking In Progress '97)라는 컨퍼런스에서 시작되었으며, ISO 7816-3에 호환되는 모든 스마트카드가 해킹되어서 저장된 정보를 쉽게 변조한다고 한다. 변조도구는 Dumb mouse라는 카드 리더기가 SCAM(Smart Card Analyser and

Manipulator)의 S/W이다.

이의 해결책으로, 첫째 비밀번호 사용으로서 신용카드를 복제할 때 비밀번호의 여부와 사용방법에 대해서는 카드사마다 자체 개발하여 사용하고, 둘째 IC카드에 대한 대책은 ISO 7816-3을 도입한 IC카드는 모두 정보침해의 위험에 노출되어 있다고 할 수 있으며, 이런 위험에 대처하기 위해서는 IC카드의 보안을 암호화함에 대한 연구가 필요하며, IC카드 개발도 한 가지 방법이 된다.

4. 패스워드 해킹방지

해킹방지를 효과적인 방법은 아이디와 패스워드를 모두 다르게 만들어야 한다. 패스워드만은 반드시 틀리게 만들어야 하고, 불편하다면 거꾸로 조작하여 자신만의 암호화 기법으로 만들어야만 한다. 또한 인증되지 않은 기관에서 주민등록번호나 전화번호를 요구하는 곳은 될 수 있으면 사이트를 등록하지 말아야 한다. 그리고 나쁜 프로그램을 만들어 내는 해커는 반드시 인터넷이나 통신망에 접속할 때 그 사람의 ID와 Password를 도용한다.

우선 방화벽과 바이러스 방지 및 암호화 소프트웨어 등을 개발하는 벤처기업에 5백78억원을 지원하고, 관련 대학원 등에도 1백32억원을 투자해서 5천3백여명의 전문인력을 확보할 계획이다. 정보보호센터내에 정보보호 기술플라자를 설치해서 벤처기업과 교육기관에 정보보호 관련 최신 정보를 제공하는 범국가적 차원의 정보 보안장치가 필요하다.

대개의 해킹은 고난도의 기술을 요하지만 약간의 지식만으로도 간단한 해킹이 되는 취약한 시스템이 많은 것도 우리 나라의 현실이다. 컴퓨터에 대한 지나친 의존은 컴퓨터의 기능 장애나 고장시, 또한 권한이 없는 일당들이 회사의 컴퓨터 시스템에 저장된 데이터를 접근할 때 심각한 문제를 일으킬 수 있다. 회사의 공금을 개인의 계좌에 옮긴다든지 지적(知的)재산권이 있는 소프트웨어를 복사판매하는 등의 컴퓨터 범죄(computer crime)는 심각한 문제이다. 이러한 저장된 데이터의 무권한 사용 또는 도용은 대부분 감지하기도 어렵고, 법의 제정 속도가 느려서 수사하기도 어렵다.

1997년 11월 News 신간안내/해커를 해킹한다에서는 해킹을 이용한 새로운 사업이 창출되며, 웹사이트를 공격해서 취약성을 노출시키는 해킹사건에 신속하게 대처하는 컨설팅 수요가 증가하고 있다고 설명하고 있다. 해킹은 21C의 현실이며, 프라이스워트 하우스가 운영하는 타이거 팀은 보안전문가의 수를 지난 18개월 사이에 20명에서 200명으로 증원, 아이비엠은 최근 자사의 지구보안 분석연구소(GSAL)를 강화하기 위해 10명의 보안전문가를 충원하였다.

해킹 컨설팅을 의뢰하고 있는 고객은 전체기업 중 10%에 이르며, 18개월 전보다 30% 증

가한 수치이다. 미국 프루덴셜 보험은 외부 컨설턴트를 고용해서 자사의 정보기술 인프라를 조사하고, 취약점을 보완하고 돌발사태에 계획을 수립한다. 보안전문회사의 프라이스워터 하우스는 해킹에 대비하는 보안팀을 규정하였다.

- 보안시스템의 디폴트 계정을 무효화하거나 함께 제공된 패스워드를 변경한다.
- 보안과 같이 귀중한 정보를 담고있는 네트워크 서비스를 중지한다.
- 사용자들이 호스트 시스템에 직접 엑세스하지 못하도록 한다.
- 패스워드는 반드시 문자와 숫자를 섞어 지정한다.
- 네트워크로 전송할 때는 암호화를 이용한다.
- 사용자의 로그인 재시도 횟수를 제한한다.
- 보안위반은 기록하고, 로그들을 검사한다.
- 최신보안 패치 프로그램들을 설치한다.
- 사용자들이 패스워드 없이 호스트 시스템에 액세스할 수 있는 Host와 host.equiv파일의 사용을 금지한다.

컴퓨터 보안연구소(CSI)의 최근 조사에서 응답자의 42%가 지난해 자사 System침입 또는 불법사용이 발생했다고 밝혔다. 내부의 데이터절도, 외부 해킹, 바이러스, 암호화 등의 보안문제는 결국은 자신의 문제에 대한 책임이 된다. 국가보안에 사용되는 앤드 투 앤드 암호화 기법은 국가의 행정, 금융, 국방 등 국가와 국가간의 전산망에 접속되는 서버의 심각성 문제이다. 초기의 보안대책은 링크 암호화 기법을 적용하였으나, 현재는 앤드 투 앤드 암호화기법 적용으로 전산보안 침투에 만전을 기하고 있다.

링크 암호화란 ISO OSI Layer(물리적 접속기), Layer 2(데이터 링크)의 사이에 H/W적인 암호화(암호설정), 복호화(암호해제)기기를 접속하는 방법으로 제2차세계대전 이후 국방과 국가보안관련 정보통신 부문에서 가장 보편적으로 사용되지만, 통신망 이상 Layer3에서 Layer7단계에 이르기까지는 내부사용자로 가장해서 조작과 공격이 가능하기 때문에 시스템 운영자나 사용자가 특정 다수인의 경우에 행위자를 찾아낼 수 없는 문제점이 있었다. 앤드 투 앤드 암호화, 즉 최종 사용자가 암호와 복호화를 하기 때문에 타인 사용자의 남용을 방지하고 전자서명을 포함한 전자문서로서의 법적인 효력을 인정할 수 있도록 하고 있다. 해킹 전담처리 "정보범죄수사센터"를 출범하여 인터넷, LAN 등을 구축한다.

국내 PC보급이 400만대로 확산되면서, 4월 10일 서울지방검찰청은 형사계 6부에 "정보범죄수사센터를 설치 가동하여, 검사 2명, 수사관 1명, 검찰 일반직 6명으로 정보범죄수사팀을 구성하였다. 자문위원으로 S/W, H/W, 컴퓨터 네트워크, 시스템 보안체제, 컴퓨터 바이러스 등 13명으로 구성, 자문위원 중에는 한국과학기술원 백성주 교수와 컴퓨터 바이러스 전문가(연

구소장) 안철수 박사도 포함되며, 인터넷 전용회선과 근거리통신망 회선 및 통신시설이 설치된다.

1) 해킹들의 일반적인 동향의 수집과 전산망의 보안상태 및 피해사례를 수집한다.

2) 공공정보의 수출, 훼손, 변경에 관한 수사를 하여 마지막로 S/W의 불법복제, 개인 ID 도용에 관한 수사를 하며, 지방정보범죄수사지원 업무를 수행하며 정보범죄수사자료실, 검찰 인터넷 접속센터 및 정보범죄 피해신고센터도 함께 자행된다.

예를 들면, 해고된 직원이 치명적인 database를 암호화 해놓고 나가 버린다든지, 대학원생이 합법적으로 S/W를 수출할 수 있고, 암호화 코드를 파괴하는데 걸리는 시간이 3시간 30분 정도로 짧은 시간에 이루어지므로, 개인의 보안은 자신이 단속해야 함을 인식해야 한다. 컴퓨터 보안연구소(CSI)의 조사 응답자 42%가 자사 시스템에 침입 또는 불법사용한 사실이 밝혀졌다.

이들의 대비방안은,

1) 허술한 정문을 단속하라(전반적인 보안실태 점검).

2) IS를 방어를 철저히 할 것(기업의 정보는 자산).

3) 스스로 자신의 차단벽을 방어할 것.

4) 그룹웨어의 바이러스보호를 할 것.

5) 보안전문인의 상종가를 치달을 듯 우려됨(IS전문가 급진전).

전자상거래 전문업체인 Open Market의 다니엘 기어 엔지니어링 이사는 "부패한 내부자가 가장 큰 위험을 일으킨다"고 강조했다. 공급업체의 보안대책 미비는 백업시스템을 통한 접근을 용이하게 하고, 정상적 예산 프로토콜들은 무력화할 결과를 낳는다고 기어는 주장했다. S/W보다 H/W쪽에 관심이 높아지고 있으며, 정보시스템 책임자는 더 좋은 보안기능을 요구하고, 제품선적시 기능의 활성화와 적절한 문서화 역할이 중요하다. 해커의 출현배경과 사회적으로 어떤 의미를 가지는지 청소년들의 사회 윤리의식을 깨우치는 교육이 시급하다(1978, 최혜진).

미국 빌게이츠가 만든 마이크로소프트사의 OS 중에 WIN 95, 98는 창의적인 전략과 장사속으로 만들었고, 기술 과시욕과 조롱에 부쳐진 것으로 보인다. 왜냐하면 가장 해킹 당하기 쉬운 OS의 경우이다. NT 4.0은 미국의 국가정보보안센터(NCSC : National Computer Security Center)에서 C2 등급을 받으나, 마이크로소프트사에서 제공한 Option 4.0은 NT4.0에 셋업했고, IIS 4.0을 사용해서 ASP 웹사이트를 만들었을 때, ASP 소스가 그냥 훤하게 들여다 보이는게 문제가 심각하다. 이것은 ASP로 만든 문서의 사이트에 URL에 ::$DATA를 추가하면 모두가 환하게 보여지는 것이다.

ASP로 만든 문서의 소스가 보여지게 되면 Database 연결의 암호나 사용자 인증방법 등

얼마든지 해킹 당할 수 있기 때문이다. 그런데, ::$DATA는 버그가 아니라 마이크로소프트사에서 IIS 4.0에 장난을 친 것이 아닌가 추측된다. 또 하나는 E-Mail에서 중요한 정보를 수많은 서버 단계를 거치면서 비밀히 보장 될 수 없으므로 주의해야 한다. 혹시 자신의 정보누출이 우려되고 백업당하고 있는지 모르는 일이다.

미국의 MIT는 대학전산망의 3단계를 두고 망(網)서비스상의 인증서비스를 제공하는 DERBEROS라는 프로토콜을 제한하였다. 학사관리 대행시스템은 사용자의 접근제어기와 시스템안전보안관리가 이루어져야되고, 홈페이지나 교수연구실 시스템은 네트워크 규모가 있다면, 라우터 및 방화벽 시스템을 두고 외부에서 불법적인 접근을 막아야 한다. 내부에서 적절하게 외부로 나가는 트래픽을 보장할 수 있어야 한다. 또한 시스템 보안관리 및 백업이 잘 이루어져야 한다. 공중전화망으로 연결된 모뎀은 터미널 서버에 접근 가능한 시스템을 만들어서 쉽게 접근함을 막아야 한다.

통신망에서 교환되는 정보는 사용자의 과실이나 제3자의 부정행위 또는 자연재해 등에서 손상이 가능성이 크다. 정보보안은 안전장치를 마련하고 피해를 최소화하려는 노력이 필요하다. 전자상거래의 구현을 위한 전제조건으로는 평가를 받고 있는 정보보안기술은 크게 차단기술과 암호화, 인증기술 등 3가지로 구분된다. 차단기술은 정보통신시스템에 대한 인가자 이외의 불법침입을 사전에 막기 위한 소프트웨어로 방화벽(firewall)과 또한 정보보안의 핵심으로 지적되는 암호화(encryption, encipher) 기술은 일정한 약속에 따라 난수표를 이용하는 대칭 키 방식과 암호와 복호화(decryption, decipher)에 다른 키(key)알고리즘을 이용하는 디지털 서명방식이 있다.

인증기술은 시스템에 접근하려는 사용자의 신원을 확인한 뒤 사용권한을 부여하거나 거부하는 것으로 접속권한 또는 접속시간까지도 제어할 수 있다. 정보보안기술은 전세계적으로 미국 이스라엘, 호주 업체들이 상당한 수준에 올라 있으며, 국내에서도 사이버 게이트와 ISS 등 몇몇 중소기업들이 참여하고 있다.

시장점유 면에서는 최고의 기술력을 가진 미국업체들이 보안기술 수출 규제정책에 묶여 답보상태에 머물러 있는 반면 이스라엘과 호주 업체들이 왕성한 활동을 보이고 있다. 우리 나라에서도 정보보호 산업의 육성을 위해 오는 2002년까지 2천억원을 들여 기술개발과 인력양성을 지원할 계획을 세워두고 있다.

〈표 3〉 중요한 보안대책

No	기술항목	요 약 설 명
1	본인의 인식	패스워드, 식별코드, 성문, 지문, 수문, 동적 기호 등에 의해 정당한 또는 확인 권한을 가진 user 혹은 본인을 확인 또는 인식한다.
2	액세스컨트롤	컴퓨터 자원의 agemsrjt에 대해 액세스 자격을 미리 설정해 두고, 액세스가 발생한 시점에서 가격을 검사하고 부당한 액세스를 방지한다.
3	암호화	통신회선을 흐르는 통신정보나 중요한 프로그램, 데이터 등의 파일 내용을 암호화해 두고, 만약 그 정보가 누락된 경우에도 내용의 해독이 불가능하도록 한다.
4	모니터링	컴퓨터 시스템에 있어서 실행되고있는 처리의 실태를 감시기록하고, 그 기록을 분석함으로써 부정을 적발한다.
5	통신시스템의 보안	통신시스템에 있어서 통신상대가 부당한 자 인지의 여부를 확인, 통신메시지가 부당한 접속에 의한 개입이나 회선상을 흐르는 데이터의 도청을 방지한다.

그래서, 해커를 자행하는 행위는 그 나라를 좀먹고, 망국적인 행위를 자행하는 것이며, 신종 해킹의 한계점에 서서 인간의 본성인 윤리와 도덕적인 진리는 높은 가치관을 잉태한다. 모든 해커를 자행하는 자들은 결과보다는 과정을 중시하여야 한다.

인간 앞에 주어지는 수많은 과제들을 지혜와 전략적인 처세술로서, 관리하고 처리할 때, 희망 높은 미래를 정립한다고 자부한다. 일을 처리할 때에 힘이 들고 어렵다는 것은, 아직도 자신이 부족하다는 증거이다. 끝없는 노력과 피나는 의지로서 현실을 해결할 때 진정한 삶의 장(場)이 된다.

해커는 사기행각과 정보범죄자로서 죄의식을 전혀 느끼지 않는 인간심성의 파괴자이다. 이제는 도덕관과 윤리관으로 담장을 치고, 고정관념을 깨트리고 정의로운 순기능을 추구해야 함이다.

V. 결 론

컴퓨터는 사람이 만들어내는 없어서 안될 필수 불가결한 도구이다. 컴퓨터를 이용한 정보기술은 큰 효율성과 편리성을 낳는 거대한 데이터 뱅크이다. 반면에 인간의 윤리관과 도덕관을 헤치는 무서운 범죄로 번져만 가는 무서운 두뇌게임이다. 이제, 정보기술은 세계를 하나로 통

하는 개인의 편의성과 교육 그리고 과학 첨단까지도 없어서 안될 필수 도구가 된다. 우리 생활 깊숙하게 편의화와 생활화로 적응되어 간다. 정보화로 인한 자동화 첨단화는 인간의 노력과 피땀 그리고 기운과 체온을 느낄 수 있는 철학이 없는 학문이다. 그저 과정은 보이지 않고 결과만을 평가할 수 있는 오로지 로봇 프로그램의 명령에만 따르는 결과일 따름이다. 그러나, 세계는 정보기술 개발과 인터넷을 이용한 사이버 광고홍보, 판매전략, 사이버 마케팅, 정보지식의 제공, 문화와 가치관이 공유되는 한 지붕이 되었다.

한편 사이버 공간은 시간과 공간을 초월한 엄밀한 곳까지, 완전 범죄행위와 테러로 변하고 있다. 초등생부터 남녀노소는 국경 없는 지능범죄로 무서운 독버섯처럼 번져만 간다. 남의 중요한 정보를 삭제하는 바이러스와 비밀번호 남용에 횡포를 자행하는 인간심성 파괴자들은 살인무기로 변해간다. 전혀 범죄의식을 느끼지 않는 모험적으로 즐기고 있다. 그래서, 컴퓨터 유저의 해커행위와 가치관에 관계는 불가분의 관계이다.

해커의 심리적인 본성은 컴퓨터를 광기있게 좋아하고 장난기가 많고, 영웅심과 스스로 쾌감을 자행하는 게으름뱅이의 변태적인 사람이다. 새롭게 발생되는 해킹은 세계적인 이슈로 등제되며 끝없는 두뇌 게임이 된다. 개인주의와 노력의 대가없이 쉽게 얻어려는 N세대들에는 간혹 구미가 당기기가 일쑤이다. 정보통신망에 이루어지는 사기행각이 두렵다. 신종해킹과 가치관의 한계점은 인간의 본성인 윤리관와 도덕관의 참된 가치관에서 비롯된다. 국외의 보안망 방안은,

첫째, 패스워드 변경

둘째, 네트워크 서비스 중지

셋째, 유저들의 액세스 불가

넷째, 암호화 이용

다셋째, 최신보안 패치 프로그램 설치이다.

국내의 보안망 방안은,

첫째, 그룹웨어의 바이러스 보호

둘째, 보안실태 점검(정문단속)

셋째, 차단벽(방화벽) 방어

넷째, IS를 방어(기업정보)

다섯째, 보안전문가 양성이다.

그러나, 국내외의 끝이 없는 보안 차단망을 대비하기 이전에 해커는 해킹행위를 중지하고, 좀더 생산적이고, 고부가가치를 창출하는 진리를 깨우쳐야 한다. 이제는 고정관념을 깨트리고 정의감과 새로운 사고(思考)로서 허물어진 가치관을 바로 세워서 고정하고 담장을 치자 .

21세기 인류는 더불어 공존공생하는 하이터치 레벨로 지향되어야 하고, 국경 없는 지구촌에서는 그 나라 문화와 가치관의 바탕 위에서만이 이루어진다는 사실을 깨달아야 한다.

참 고 문 헌

1. Computers(이한출판사)
2. 전자계산기 일반(법흥사)
3. 샘들의 창(김태석 박사)
4. 문화일보(1992. 9. 1.)
5. 한국일보(1999. 4. 5.)
6. LG 텔레콤(비둘기 7. 8. 9. 10월)
7. 서울대학교 가상대학(http:\\snuvc.snu.ac.kr)
8. 열린 사이버대학
9. 컴퓨터 범죄(http:\\dci.sppo.go.kr/news/knews.htn)