정보보호와 뉴 패러다임에 관한 연구

A Study on the Information Security and New Paradigm

장우권, 중앙대학교 문헌정보학과, 박성우, 전남대학교 문헌정보학과

Chang Woo Kwon, Dept. of LIS, Chungang University
Park Sung Woo, Dept. of LIS, Chonnnam National University

21세기는 사이버공간의 확대, 선점이 곧 국가와 기업 그리고 개인의 생존경쟁력의 바로미터가 될 것이다. 그러나 사이버공간에서 발생되고 있는 정보화의 역기능들은 갈수록 빈번하고 지능화 되고 있어 심각한 사회적 혼란과 국가의 전략적, 행정적, 경제적으로 막대한 손실은 물론 군사활동마저 마비시키고 있는 실정이다. 따라서, 본 글에서는 사이버 공간에서의 범죄행위를 예방하고 차단시킬 수 있는 정보보호기술과 패러다임을 조사 분석하여 정보보호산업의 현황을 알아본 다음 정보보호기술의 측면에서 활성화 방안을 제시한다.

I. 서론

인터넷의 개방성 글로벌성, 접근용이성이 기술, 산업 그리고 문화의 새로운 융합과 발전을 구축하는 중심 축이 되고 있는 21세기는 사이버공간의 확대, 선점이 곧 국가와 기업 그리고 개인의 생존경쟁력의 바로미터가 될 것이다.

그러나, 사이버공간에서 발생되고 있는 정보화의 역기능들은 갈수록 빈발하고 지능화 되고 있어 심각한 사회적 혼란과 국가의 전략적, 행정적, 경제적 막대한 손실은 물론 군사활동마저 마비시키고 있는 실정이다.

아무리 훌륭한 지식과 정보시스템이라 할지라도 심각한 범죄를 야기한다면 무슨 소용이 있겠는가.

따라서, 본 논문에서는 이러한 사이버공간에서의 범죄행위를 예방하고 차단시킬 수 있는 정보보호와 기술 그리고 그 패러다임을 조사 분석하여 기술하고 정보보호산업 현황을 알아본 다음 정보보호기술의 측면에서 활성화방안을 내놓고자 한다.

II. 정보보호와 기술의 뉴 패러다임

2.1 정보사회의 출현과 역기능

최근의 여러 통계에 의하면, 미국에서 5천만명의 사용자를 확보하는데 걸리는 시간을 조사했더니 전화는 25년, 라디오는 38년, TV는 13년, 케이블 TV 10년이 걸렸으나 인터넷은 불과 5년이 걸렸다고 한다. 또한 인터넷 거래가 100일마다 2배가된다는 통계와 2000년 5월말 현재 국내 인터넷 이용자 수가 1500만 명에 이르렀다니 정보통신의 혁명적 발전에 의한 인터넷 세상이 되고 있는 것이다.

그러나, 지식정보화에 의한 생활의 편리성이 진전될수록 인터넷을 통한 각종범죄(사기, 매춘, 스토킹), 정보시스템 불법 침입 및 파괴(해킹과 바이러스 유포), 불건전정보의 유통, 개인의 프라이버시 침해, 개인정보의 오남용과 내부상의 중요기밀문서가 외부로 유출되는 등의 사생활 침해와 경제적 손실 등의 정보화의 역기능이 날로 증가되고 있어 심각한 사회문제가 되고 있다.

2.2 정보보호란 무엇이고 왜 필요한가

정보보호(Information Security)란 사이버공간에서 일어나는 불법적인 해킹, 바이러스 유포, 기업과 개인정보의 유출과 파괴로부터 보호하는 것이다. 또한 위에서 언급한 정보화의 역기능을 순기능으로 바꾸는 것이라고 할 수 있다.

그렇다면 정보보호가 왜 필요한가. 인터넷은 모든 사람들에게 공개되어 있는 사이버공간이기 때문에 지역과 거리, 시간의 개념이 존재하지 않으며, 언제, 어디서, 누가, 어떤 경로를 통해서든 공격할 대상의 취약점이 발견되면 수초이내에 공격하여 상황을 종료해버린다는 것이다. 오랫동안 심혈을 기울여

구축한 시스템 자원이라면, 어떻게 될 것인가를 상상해 보라. 지식정보의 유무형의 가치 및 의미를 상실하게 될 것임은 물론 이에 따른 정신적·물질적 피해보상은 어떻게 받을 것인가.

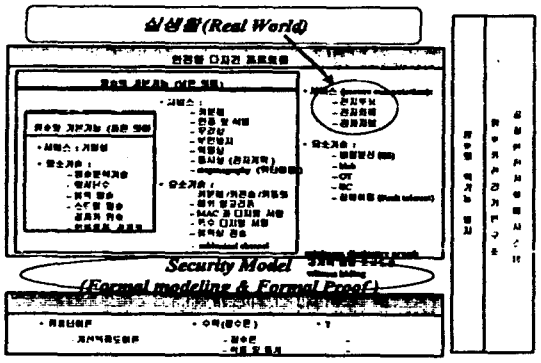
따라서, 안정된 지식정보사회를 구축하는데 필수적인 정보를 보호하지 않으면 안될 이유와 그 필요성이 여기에 있는 것이다.

2.3 정보보호기반기술

암호화된 메시지로 정보의 안전성과 신뢰성을 보장하는 수단인 암호기술, 메시지의 변경이 없다는 메시지 무결성(integrity)을 인증(Authentication)하는 인증서비스기술, 분산환경하에서 데이터전송시 사용자가 요구하는 수준의 비밀성 보장과 무결성, 비보호, 비밀성, 무결성 및 비밀성 등과 같은 파라미터를 갖는 QoP(Quality of Protection) 기능을 지원하는 CORBA(Common Object Request Broker Architecture)의 관리 및 제어에 의한 보안서비스 등의 접근통제기술, 그리고 네트워크 보안기술 등은 정보를 보호하는 기반기술이다.

① 암호기술과 응용서비스

암호기술은 인터넷을 이용한 사이버업무를 변환될 때 야기되는 여러 가지 문제를 해결해 주는 툴로써, 통신의 주체인 송신자와 수신자를 제외한 제3자로, 전송로상의 정보를 위조/변조 유출하려는 부정한 사용자(dishonest user)를 막기 위한 기술이다. (현대사회에서 정보보호의 핵심인프라).



(그림1) 암호기술의 분류 1)

암호기술의 응용서비스는 (그림1)의 공통기반기술에 의한 사용자 인증기술, 전자서명기술, 대칭 키 공개 키 암호알고리즘 및 주어진 암호기술의 신뢰성 검증을 위한 전자상거래, 가상기업, 가상대학, 가상정부 등 다양한 분야에서 응용되고 있다.

② 인증서비스기술(전자상거래)

인증기술이란 네트워크환경에서 자신이 누구인지를 상대방 또는 제 3자에게 증명하는 기술을 말하며 전자문서 형태로 서로의 신분을 증명할 수 있는 인증서(Certificate)를 사용한다. 인증서를 등록하고 발급 또는 조회하는 조직을 인증기관(CA)이라고 한다. 인증서를 활용하는 분야는 대표적으로 전자상거래이다. 전자상거래의 안정성과 신뢰성을 위해서는 고객의 신용정보와 개인정보 그리고 실시간으로 이루어지는 결재정보 등이 인터넷상에서 보호되어야 한다.

여기에서 중요한 것은 상거래상에서 필수적인 신분증명을 어떻게 할 것 인가이다. 법률적으로는 1999년 7월 1일에 『전자서명법』, 『전자거래법』 등이 제정되어 시행되고 있다. 미국에서는 2000년 6월 14일 상·하 양원에서 압도적으로/만장일치로 승인되어 오는 10월 1일부터 효력을 발휘하게 된다. 2)

전자서명(Digital Signature)은 공개키 기반구조(PKI : Public Key Infrastructure)로 되어있다. 이것은 서로의 신뢰가 생성됨을 뜻하며, 서로간의 상호인증과 상호인정에 의한 기술, 정책, 서비스가 갖추어진 인증서 교환이 이루어져야한다.

우리 나라는 국가 최상위 인증기관으로서 전자서명인증관리센터가 1999년 7월 7일자로 설립되어 운영되고 있다.

2.3 시스템 및 네트워크 보호기술

1) 인터넷 관련보안

웹을 항해할 때 외부로부터 보호할 수 있는 기능들을 살펴보면;

① 아이콘에 의한 암호화된 통신지원(보안지시자)

○ 넷스케이프 네비게이터(Netscape Navigator)

4.0이상에 보안 기능들이 내장되어 있으며, 브라우저와 서버가 동시에 SSL 기능을 제공하면 HTTP 메시지는 암호화되어 전송한다. 이때 "http"대신에 "https"를 사용한다. 브라우저의 왼쪽아래에 있는 "보안아이콘"에서 파란색 아이콘은 보안채널로 연결되어 있다는 것이고 회색아이콘(부러진 열쇠모양)은 보안이 되지 않았다는 것을 의미한다.

○ 인터넷 익스플로러

4.0이상에는 하단의 상태표시줄 중앙에 열쇠아이콘이 나타나며, 클라이언트와 서버 인증을 효과적으로 수행하기 위해 인터넷 사이트를 인터넷 영역, 로컬인트라넷 영역, 신뢰할 수 있는 사이트 영역, 제한된 사이트 영역이라는 4개의 영역으로 나누어 사용자가 보안수준을 각 영역별로 지정할 수 있도록 하였다. 정보는 상태표시줄 오른쪽에 나타나 있다.

② 전자우편(E-mail) : 송신자의 이름과 주소의 위조를 용이하게 사용자를 가장한 공격의 수단으로 역이용될 수 있다. ③ History와 Helper Application :

공격자에 의한 사용자의 방문사이트에 대한 정보 유출로 프라이버시를 침해 할 수 있다. ④ 쿠키(Cookie) : 쿠키가 서버로 전송되어질 때 IP주소, 사용증인 브라우저, 운영체제와 같은 개인정보가 유출될 수 있다. ⑤ 캐시(Cache) : 공격자가 사용자의 관심사항 및 브라우징 습관을 파악할 수 있어, 자바를 사용하여 악성코드를 캐시에 저장토록 한 후 코드를 실행하여 피해를 줄 수 있다. ⑥ 프락시(Proxy)서버 : 공격자에 의해 프락시 설정이 바꾸어진다면 사용자의 웹 탐색습관이나 비밀정보(패스워드)를 유출시킬 수 있다. ⑦ 자바애플릿 및 자바스크립트 : 사용자 시스템자원을 불법적으로 획득하는 비밀성(secrecy) 침해공격, 사용자시스템자원을 불법적으로 수정 또는 변경하는 무결성(integrity) 침해공격(예, 프로세스/쓰레드, 메모리 등), 사용자시스템자원을 과도하게 사용하여 사용자의 정상적인 사용을 방해하는 가용성(availability) 침해공격, 웹사용자에게 수많은 윈도우나 프레임을 생성시켜 사용상의 불편을 끼치거나 원하지 않은 음향을 지속적으로 발생시키고, 사용자에게 불쾌감을 유발시키는 경우가 있다. ⑧ 액티브 X(Active X) : 윈도우즈 95를 정지시키거나, 악성 액티브 X 컨 트롤을 배포한 사건(CCC: Chaos Computer Com)의 예에서 보듯이 안전성을 보장하는데 한계가 있다는 것이다. ⑨ 사용자 ID와 패스워드 : 사용자를 가장하여 공격할 시 사용자의 시스템용 로그인 계정과 패스워드가 도난당하여 프라이버시 침해와 막대한 경제적 손실을 초래할 수 있다. ⑩ 인증서(Certificate) : 넷스케이프 브라우저에서 인증서를 획득할 수 있으며 자신, 타인, 웹사이트, 인증서 서명자의 인증서 등으로 나누어 관리한다. 인터넷 익스플로러에서 인증서를 발급 받을 수 있으며 DER, Base 64로 인코딩된 X.509와 PKCS # 7 인증서 형태로 저장관리된다. 클라이언트/서명인증, 프로그램코드서명, 안전한 전자우편/타임스탬핑, MS 신뢰목록 서명/MS 타임스탬핑, IPsec 종단시스템, IPsec 종단/IPsec 사용자에 대한 인증, 파일시스템 암호화, 윈도우 하드웨어 드라이버 검증, 윈도우 시스템 컴퍼넌트 검증 등으로 이용되고 있다. ⑪ 웹 브라우저 보안 옵션관리 : 넷스케이프 네비게이터 4.0이상과 인터넷익스플로러 4.0이상은 위에서 기술한 각 기능별로 보안옵션을 설정하여 관리할 수 있다. ⑫ 인터넷 웹브라우저 보안에 가장 많은 영향을 끼치고 있는 기구는 IETF의 WK(Working Group)과 ISO/IEC JTC1이다.

2) 시스템보호와 침입탐지시스템

인터넷의 응용기술발전으로 외부인에 의한 시스템 불법침입에 의한 사고가 국내외에서 동시다발적으로 빈번히 일어나고 있다. 이에 대한 적극적인 대처방법은 시스템 보호기술개발이다. 특히, 침입탐지와 차단기술은 안전한 지식정보화 환경구축을 위한 핵심기술중의 하나이다.

(1) 침입탐지 기술

어떤 침입자가 컴퓨터시스템에 특정의 목적을 위해 불법적으로 접속하여 시스템을 사용하거나 오남용하는 것을 탐지하고 그 문제점을 처리하는 기술.

① 침입탐지기술의 문제점과 해결방안

기존의 침입탐지기술로는 해커로부터 시스템을 보호하기 위해서는 방화벽(Firewall)만으로는 충분하지못하며, 단일시스템 환경에 적용되어 대규모 네트워크 확장시 또는 다른 기존시스템들을 재사용시 어려움이 따른다(예, 메시지 처리방식, 패킷스니퍼링, CRACK, send mail공격, NFS공격, IP Spoofing 등).

이러한 문제점을 해결하기 위해 첫째, 침입차단시스템과의 연동을 통한 접근제어, 둘째, TCP Wrapper 과의 연동을 통한 서비스 접근제어, 셋째, 침입자를 역추적하기 위해 로그, 호출자, 판별, 모니터링과 같은 기술사용, 넷째, 공격형 정보보호기술로서 부정행위자 신분확인시스템, 다섯째, 방화벽이 감지하지 못하는 공격에 대해 인식할 수 있고 이전에 경험하지 못한 공격에 대해서도 이를 감지하여 퇴치할 수 있는 IDS시스템을 사용한다.

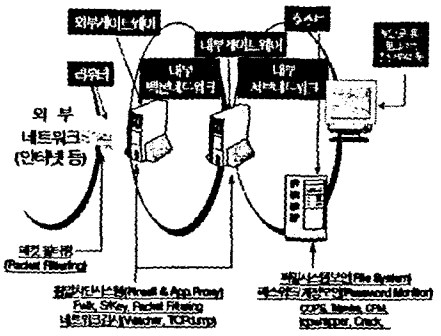
최근에는 새로운 공격유형에 탐지력을 높이는 수단으로 인체면역메카니즘을 적용한 인체면역시스템을 적용하려는 연구를 계속하고 있다.

② 침입탐지기술의 응용분야

침입탐지기술은 전자상거래(실시간 경보, 서비스거부행위, 정보를 탈취하거나 파괴, 변조하는 행위 등), 금융기관(예금관련 DB감시, 고객정보유출방지, 웹서버 등 사내전산자원의 불법사용 여부 판단), 교육기관으로서 도서관(학술정보 DB감시, 연구자료와 수서/정리자료에 대한 불법적인 유출방지, 도서관 시스템에 대한 유해행위 방지, 대출/반납자료에 대한 파괴와 변조, 탐지결과에 대한 적절한 대응), 관리대상의 정보가 대량화, 다양화되고 있는 대규모 인트라넷에서 응용, 수많은 정보침해유형(예, 바이러스, 서비스거부공격 등)에 적절히 대응하여 안전한 사이버공간의 구축과 이용활성화에 응용되고 있다.

③ 침해사고방지와 탐지기술의 적용

다음은 침해사고방지와 탐지기술의 적용 예를 나타내고 있다.(그림2)

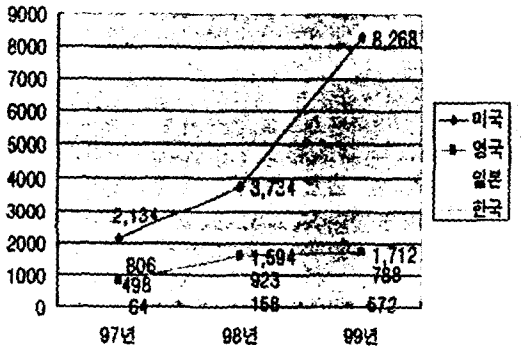


(그림2) 침해사고방지와 탐지기술의 적용 예 3)

3) 해킹현황과 보안대책

최근에 해킹기법은 더욱 복잡해지고 다양화되고 프로그램화되어 자동화되고 있으며 심지어 MS 윈도우 시스템을 다운시키는 등 피해사례가 속출하고 있다. 정보통신부에 따르면, 국내의 해킹사고는 1997년에 64건에 불과하던 것이 '98년에 158건, 지난해 572건으로 늘어난데 이어 올들어 상반기(2000. 1-6월)에만 721건이 발생했다. 이러한 현상은 (그림 3)와 같이 미국, 일본, 영국 등과 마찬가지로 전 세계적으로 크게 증가하고 있음을 알 수 있다.

1999년 기관별 해킹피해건수를 비교 분석한 결과 전체 572건중 대학이 252건(45.8%)으로 가장 많은 피해를 보았으며 그 다음에 일반기업 248건(43.4%) 순 이었다. 또한 국내·국제간의 피해관계를 비교·



(그림3) 국외해킹사고 증가추이 4)

분석해보면, 국내에서 국내로 해킹 시도 및 공격이 48건(8.1%), 국내에서 국외로 24건(4.0%)인데 비하여 국외에서 국내로가 91건(15.3%), 국외에서 국내로 다시 국외로가 183건(30.7%)이 발생한 걸로 집계되었다. 여기에서 한국의 인터넷 보안상태가 심각하다는 외국전문가의 조사결과를 인지하고 이에 대한 대책을 세워나가야 한다.

1999년에 해킹사고에 사용된 기법들을 비교·분석하면 취약점 정보수집에 272회, 버퍼오버플로우 취약점에 214회, 악성 프로그램에 58회, 사용자 도용에 68회, E-mail 관련공격에 20회, 서비스거부공격에 16회, 사회공학에 4회, S/W 보안오류이용에 3회, 구성·설정오류에 2회순으로 나타났다.

대표적인 피해사례를 살펴보면;

-. 분산서비스 공격사례 : 2000년 7월 31일 정보통신부의 발표에 의하면, 해커가 미국 버지니아주에 있는 인터넷접속서비스업체(ISP)에 전화로 접속해 인터넷을 통해 강원도 강릉소재 한 PC방의 리눅스 서버를 해킹한 후, 이 PC방을 거점으로 대학30개, 기업200개, 공공기관 20개 등 국내 250여곳 서버에 침입한 후 서버를 마비시켜 서비스를 불가능하게 만드는 사고가 발생.5)

이에 대한 보안 대책으로는 다음과 같다.

-. 유닉스버퍼오버플로우 경우 : 첫째, 보안패치를 적용. 둘째, 불필요한 프로그램을 정지. 셋째, 버퍼오버플로우차단 프로그램을 설치 운영한다.

-. 윈도우즈 트로이 목마인 경우 : 첫째, 통신망, 인터넷을 통한 파일다운로드 주의, 둘째, 출처가 불투명한 첨부파일 실행주의, 셋째, 최신백신 소프트웨어사용, 넷째, PC의 물리적 보안강화(예, ROMBIOS 패스워드), 다섯째, 네트워크 모니터링을 통한 침입감시, 여섯째, 정품소프트웨어를 사용한다.

-. 해킹보안기술 : Firewall, 침입탐지시스템, 해킹취약점 분석, 진단 및 복구기술(이동에이전트 기술), 클라이언트-서버환경기반 보안관리기술, 역추적기술, 컴퓨터포렌식스(법적증거물), 인공지능기술, 면역기술, 신경망기술 등이 연관된 많은 기술개발이 이루어지고 있고 이에 대한 제품들이 출시되고 있다.

-. 해킹·보안관련 검색엔진을 활용한다. 예를 들면, 아스탈라비스타(http://www.Astalavista.box.sk)

4) 바이러스 현황과 대응

컴퓨터바이러스는 컴퓨터의 프로그램이나 실행가능한 부분을 변형하여 고의로 제작·유포하여 피해를 주는 프로그램으로 그 감염속도가 생물학적 바이러스 질병처럼 매우 빨라 수시간/수일내에 E-mail이나 인터넷을 통해 전세계에 전파한다.

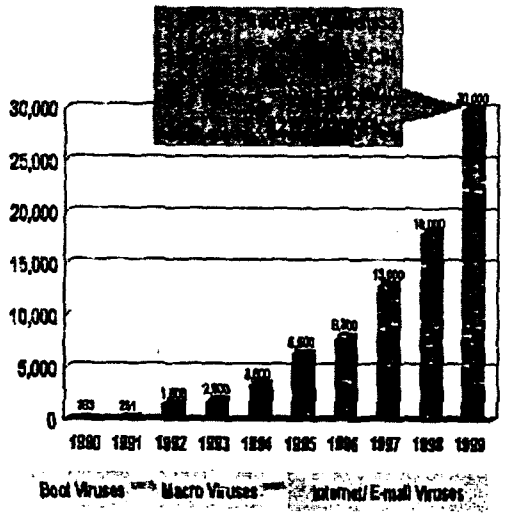
최근에는 "ExploreZip", Win32-Worm, "love", "CIH바이러스" 등의 신종 및 변종 바이러스가 출현

하여 바이러스 백신기술의 향상에도 불구하고 세계 곳곳에서 많은 피해를 주고 있는 실정이다.

○ 국외 컴퓨터바이러스 발생현황분석 6)

최근 미국의 ICSA의 분석보고서에 따르면, 1997년부터 1999년 2월까지 26개월간 300여개조직에 806,614대 PC로부터 263,784개의 컴퓨터바이러스를 발견할 수 있었으며, 조사기간 중 한달에 1,000대의 PC에서 평균 13개의 컴퓨터바이러스가 발견되어, 컴퓨터바이러스 전파속도가 매우 빠르게 진행되고 있음을 알 수 있다. 또한 컴퓨터바이러스 발생유형별로 보면 파일이나 부트바이러스→매크로바이러스→인터넷 E-mail를 이용한 바이러스로 전파경로가 이동되고 있음을 보여주고 있다.

또한 보고서에 나타난 감염경로를 비교 분석하여 보면 299명의 응답자중 컴퓨터바이러스 감염매체로 E-mail(메일 첨부파일)에 의한 경우가 가장 많았으며 그 다음은 디스켓> BBS, 통신다운로드> unknown>웹(홈페이지)사용>공개용 프로그램 사용>FTP, BBS Host 다운로드> 복구, 서비스 순으로



(그림5) 유형별 년간 컴퓨터바이러스 발생추세

나타났으며, 일반기업의 PC사용자가 피해를 입은 유형을 복구소요 시간과 노력, 비용측면에서 분석하여 보면, 생산성 저하, 파손 및 삭제 등의 파일변조, 파일판독불능, 메시지 화면출력, 간섭현상, 화면잠금, 파일저장 불능, 사용자에게 PC자원의 가용성 제거, 시스템 내 사용자의 주요기밀정보 손실, 서버에 있는 데이터액세스 제한, 응용프로그램의 신뢰성 저하, 데이터 손실, 출력상의 제한, 시스템 붕괴, 순으로 나타났다.

○ 국내 컴퓨터바이러스 발생현황분석 7)

국내에서 발생한 컴퓨터바이러스는 다양한 종류와 양적인 증가(예, 매크로바이러스, 윈도우바이러스, 웜), 그리고 그 위험성이 날로 높아가고 있다.

1999년 한해에 발생한 컴퓨터바이러스를 유형별로 분석하여 보면; 첫째, MS Word, Excel 등의 MS 오피스 대상의 공격형 매크로바이러스가 36%, 해킹기법을 이용한 트로이목마 등의 유포가 26%, 전자우편, IRC (Internet Relay Chat) 등의 전송 매커니즘 등을 이용한 네트워크상의 대규모적인 인터넷 ExploreZip, 웜(Worm)이 2%, 윈도우스크립트인 VBS(Visual Basic Script)를 이용한 신종 컴퓨터바이러스가 2% 순으로 출현하였다.

○ 최근의 변종바이러스

가장 최근에 CIH바이러스 변종 Win95/CIH.1042가 발견되었다. 특징은 매달 4일 활동하고(원형은 매달26일 활동), 윈도우 95, 98에서만 작동하며 윈도우 NT2000에서는 작동하지 않는다.

감염파일 내부에는 "Go away fuck up by *NetCracker1*"이라는 문자가 나타난다.

이 바이러스는 하드디스크 정보를 삭제하고 플래시 메모리 기본입출력장치(BIOS)를 손상시켜 컴퓨터를 부팅조차 안되게 만든다.

○ 국내 컴퓨터바이러스 대응현황

1995년 5월 한국정보보호센터 침해사고대응지원팀(CERTCC-KR)내에 컴퓨터바이러스 전담반이 구성되어 첫째, 국가적인 컴퓨터바이러스 종합대응체계 구축, 운영. 둘째, 컴퓨터바이러스 종합상황실 운영. 셋째, 선도적인 차세대 악성 컴퓨터바이러스 대응 기술연구개발. 넷째, 컴퓨터바이러스방지 관련, 법·제도 및 지침서 개발. 다섯째, 컴퓨터바이러스 대응기술교육 및 대 국민 홍보활동 등을 중심으로 운영되고 있다.

III. 국내외정보보호산업의 패러다임과 활성화방안

3.1 국내외 정보보호기술과 산업패러다임

①국외

세계 각국은 자국의 주요산업기반구조를 보호하기 위한 노력으로 암호 알고리즘설계·분석, 키 관리 및 전자서명인증기술, 각종 네트워크를 이용한 각종 서비스에 대한 네트워크 보안기술과 PC, 서버 차원의 시스템보안기술, 네트워크를 이용한 각종 서비스에 대한 보안기술 및 행정, 보건, 교육, 금융서

비스와 전자상거래, 전자지불보안과 같은 정보보호 기술개발을 국가 주도로 적극 추진하고 있다.

미국은 이를 위해 각계 의견을 수렴하여 2000년 1월 7일 『국가 주요기반시설 보호계획』을 발표하였다. 2003년 5월까지 완벽한 운영능력을 확보하여 주요 정보시스템에 대한 보호대책을 구축하는 것이다. 국가계획은 준비 및 예방, 탐지 및 대응, 튼튼한 기반구축의 3가지 목적을 가진 10개의 실행 프로그램과 세부 실행계획을 제시하였다(자세한 내용은 참고문헌 참조) 8)

② 국내 : 국내의 정보보호산업의 발전패러다임을 시기별로 살펴보면 ; 9)

첫째, 도입기(~'97.10). 정보제품을 외국에서 들여와 국내에 소개하는 수준이었으며 정보통신부가 1997년 9월에 "정보보호산업 발전대책" 수립을 천명

둘째, 침체기('97.11~'98.8). IMF에 의한 투자가 위축되었고, 매출의 성장세가 크게 둔화되었다. 해킹과 바이러스 등에 의한 여러 산업망들이 피해를 당했음에도 이에 대한 예방과 치료 대책을 소홀히 함.

셋째, 회복기('98.9~'99.10). 이 시기에는 정보보호산업이 본격적으로 형성되었으며, 민간부문에서 신규 사업 모델링이 도입되었다. 인터넷 해킹대책이 세워졌으며, 전자서명법, 전자거래법 등이 제정되어 시행되었고, 정보보호 인식의 척도인 "인증서"를 발급 받을 수 있는 인증기관이 설립되었고 전자상거래에 대한 마인드가 확산되었으며, e-business 패러다임이 정착되면서 IT에 대한 정보통신분야의 투자분위기도 형성되었다.

넷째, 도약기('99.11 ~). "정보보호"가 인식되었고, 전자상거래 시장이 활성화되었다. 또한 국내기술들의 시장검증 프로세스가 가속화되었으며, 이는 인터넷 산업의 견실한 인프라가 갖추어지게 되었다.

보고에 의하면 올해는 약 1000억원 정도의 시장규모가 형성될 것으로 예측하고 있다. 다른 산업에 비하여 액수가 적으나 기술개발 제품 출시면에서, 다른 어떤 산업보다 빠른 신장세를 보이고 있다.

3.2 정보보호기술과 산업의 활성화방안

이제 정보보호기술과 산업은 누구도 부인하기 어려운 국가경쟁력의 핵심분야가 되고 있다. 따라서, 정보통신망을 백본으로 한 국가 정보화산업의 기반을 구축하기 위해서는 정부의 정책입안과 의지만 갖고 되는 것이 아니며, 전국민적 정보화 마인드에 대한 공감대가 형성되어야 한다.

정보보호산업 활성화 대책을 제시하면 다음과 같다.

첫째, 정부는 정보보호에 대한 확고한 정책을 수립하고 이를 실천할 수 있는 의지가 있어야 한다.

둘째, 정보보호를 위한 전문인력을 양성해야 한다.

셋째, 정보보호에 대한 공감대가 형성되어야한다.

(정보보호인프라를 구축)

넷째, 연구개발을 통한 산업체의 기술개발을 지원해야 한다.

다섯째, 정보보호산업이 국제적 경쟁력을 가져야 한다. 정보보호산업은 개방된 네트워크를 통하여 정보를 공유하며 이를 바탕으로 새로운 부가가치서비스를 창출하는 산업이다. 글로벌경제시대에 정보보호산업을 국제 경쟁력이 있는 산업으로 육성하기 위해서는 정보화 촉진에 대한 강력한 의지와 우수한 정보보호통신 인력과 과감한 투자로 시장을 리더해 가는 장단기적 성장전략이 필요하다.

IV. 결론

인간의 소유욕구가 충만한 나머지, 건전한 사이버문화가 사이버테러로 변질되어 세계 곳곳의 통신망을 통한 프라이버시 침해와 국가 기밀정보를 훔쳐갈 뿐만 아니라 아예 시스템 망을 파괴시키고 있다.

이에 우리 나라를 비롯한 각국은 자국의 이익과 국민 사생활의 보호를 위해 여러 가지 대책을 수립하고 시행하고 있다. (사이버공간의 위협으로부터 보호받을 수 있는 정보보호 기술과 산업의 활성화)

사용자 개개인은 정보보호의 심각성을 깨우쳐, 자신의 재산은 자신이 보호하는 책임을 가져야 하며 해킹과 바이러스의 침입으로부터 보호받을 수 있는 기본적인 정보보호지식을 가져야 한다.

기업과 국가는 정보보호산업 육성에 아낌없는 투자를 해야하고, 전문인력을 양성하고 국제 경쟁력을 갖출 수 있도록 여러 가지 제도적 세제지원과 정책수립으로 우수한 정보보호기술이 개발될 수 있도록 적극적 지원이 이루어져야 한다.

우리가 명심해야할 것은 "해킹과 바이러스는 국경이 없으며 수 시간 내에 우리의 모든 재산을 파괴시킨다".

(참고문헌)

1), 3-4), 6-7), 9) 한국정보보호센터. 정보보호뉴스 (*http://www.kisa.or.kr*)

5) 정보통신부. (*http://www.mic.go.kr*)

8) National Plan for Information System Protection Ver.1.0, Jan.2000. (*http://www.ciao.ncr.gov*)

10) The Netcraft Web Server Survey, (*http://netcraft.com/survey/2000.2*)

11) Advanced Encryption Standard(AES) Development Effort. (http://csrc.nist.gov/encryption/aes/1999)