特輯

국가전산망의 정보보호

李 在 雨
韓 國 電 算 院

Ⅰ. 서 론

그동안 국가 전산화는 민간분야(Private sector) 뿐아니라 공공분야(Public sector)에 이르기 까지 국가사회 총체적으로 이루어져 왔다. 정보화사회는 국가의 선진화나 국제화를 위해서도 필수 불가결한 요건이 된 것이다. 국가 전산화의 대표적인 예는 5대 기간 전산망을 들 수 있다. 이것은 행정, 금융, 교육, 국방 및 공안 전산망을 의미한다.

그중 행정전산망의 경우를 보면 국민의 일상 생활과 직접적으로 관련되는 주민등록 부동산 자동차 고용 통관 경제통계 등 6개 우선 추진 업무를 1985년부터 중점적으로 개발하여 우리에게 신속한 민원업무 처리 등 많은 편의를 제공하고 있는 것이다. 특히 1992년 부터는 국민복지 업무, 우체국 종합서비스, 해상화물 관리등 7개 전산화 사업을 새로이 시작하고 국가 초고속 통신망 사업도 추진하고 있어 우리의 사회는 머지않아 21세기형의 고도화된 정보화 사회가 이룩될 전망이다.

그러나 모든 현상에는 빛과 그림자의 명암이 있듯이 정보화 사회의 이점 뒤에는 분명히 단점이 있기 마련이다. 그것이 바로 정보화의 역기능 현상이라고 할 수 있다. 그 역기능의 경우 시스템의 중요성과 정보내용의 중요도에 따라 그 피해의 심각성은 더욱 커지게 된다. 오늘날 국가전산망과 공공정보의 보호에 대한 중요성이 크게 부각되고 있는 당위성도 여기에 있는 것이다. 따라서 본고에서는 국가전산망의 역기능 방지와 정보 보호에 대한 안전.보안 업무를 중 점적으로 살펴보고 향후의 추진 계획에 대해서도 고찰해보고자 한다. 지면의 제약으로 국방망과 공안망에 대해서는 다음 기회로 미룬다. 우선 국가전산망의 안전.보안 업무의 직접적인 이해에 필요한 일반 이론을 기술하고 이어 국가전산망의 현황과 추진계획을 기술할 계획이다. 아울러 그동안 발생했던 공공분야의 컴퓨터 범죄 현황도 부표로 제시코자 한다.

Ⅱ. 시스템 안전 • 보안 이론의 일반적 개요

1. 국가사회 정보화의 역기능

공업화 사회의 대표적인 역기능이 공해에 의한 환경의 파괴로 대표 되듯이 정보화 사회의 역기능은 컴퓨터 범죄로 통칭되고 있다. 우리는 그동안 언론 매체를 통하여 "컴퓨터를 이용한 금융 범죄, 선거 개표 컴퓨터 조작설, 전산망에 의한 프라이버시 침해, 전산조작에 의한 입시부정, 핵커에 의한 국가정보의 유출 기도" 등 많은 범죄 기사에 접해 왔다. 이처럼 우리에게도 컴퓨터 범죄가 스며든지 오래여서 컴퓨터 범죄는 사회에 큰 물의를 일으키고 있는 중요한 역기능임이 분명한 것이다. 정보화의 역기능은 컴퓨터 범죄 이외에도 사회적 역기능 문화적 역기능 윤리적 역기능 등 그 종류가 다양하여 적절한 대비책을 강구하지 못할 경우 더욱 심각한 국가사회의 문제를 야기시킬 수 있는 것이다.

그 종류와 내용을 살펴보면 다음과 같다.

1) 범죄적 역기능

범죄적 역기능은 컴퓨터의 부정조작 오용 파괴 등의 경우와 데이타의 변조 훼손 절도 부정유출 및 복제 등의 범죄적 행위가 주종을 이루고 있다. 바이러스(virus)와 핵커 (hacker)들의 시스템 침투로 인한 범죄적 행위도 신종 역기능으로 등장하고 있으며 최

근에는 정보통신망을 통하여 특정 대상인을 음해하거나 비방 위협하는 등의 가해 행위가 발생하고 있다. 또한 공공시스템의 파괴로 인한 사회적 혼란기도와 각종 CD 범죄 등의 역기능 현상도 부각되고 있다.

2) 사회적 역기능

사회적 역기능에는 개인정보(privacy)의 침해에 따른 역기능을 한 예로 들 수 있다. 공공기관은 물론 금융기관이나 각종 단체 등에서 사용하고 있는 신상기록의 부정유출은 개인적인 피해는 물론 사회적 물의를 야기시키고 있는 것이다. 자동차 등록 대장의 임의 열람으로 외제 고급 승용차의 소유주를 파악하여 범행을 저지른 사례나 신상기록을 통하여 직업이나 가족 관계를 파악하여 취약한 틈을 타 범행을 저지른 경우 등의 예가 바로 그것이다. 또한 자동화로 인한 실업자의 유발, 전산망을 통한 공공정보나 산업정보의 도절로 인한 사회적 혼란, SI로 인한 산업구조의 변동과 구조적 체제의 갈등 등은 사회적 역기능 현상으로 인식되고 있다. 그 외에도 정보 도용으로 인한 지적 소유권 문제, 정보화의 불균형으로 인한 지역적 현대화의 격차 유발, 국제화 정보통신망을 통한 저속한 외국문화 정보의 유입 및 국가 주요 정보의 유출, 정보기술의 범죄수단 역이용, 조직의 통제수단으로의 역이용, 정보통신망의 마비에 의한 사회적 혼란과 피해등은 사회적 역기능으로 평가되고 있다.

3) 문화적 역기능

문화적 역기능의 대표적인 예로는 컴퓨터 오락 및 게임 문화의 역작용을 들 수 있다. 물론 긍정적인 이점도 있지만 지나친 도취나 저속한 게임 놀이 등은 분명한 문화적 역기능 현상인 것이다. 기계화, 자동화에 따른 비인간화, 세대간 계층간의 컴퓨터 소외감의 격차, 컴퓨터 작동에 수반되는 건강문제 유발 등도 컴퓨터 문화의 역기능 들이다.

4) 윤리적 역기능

정보통신망을 통한 저속한 정보의 유포나 비윤리적 가해 행위 등에 의한 청소년 들의 정서 저해 행위는 분명한 윤리적 차원의 역기능들이다. 현재 BBS를 운영하는 정보통신 사업자의 일부 부도덕한 상행위로 사회적 물의가 자주 일어나고 있다. 또한 정보통신망을 통한 음난 정보의 유통이나 저속한 CD-ROM의 피해도 역시 윤리적 역기능으로 평 가되고 있는 것이다.

2. 정보의 특성과 보안

국가전산망의 정보의 특성을 이해하기 위하여 정보의 질과 취약성에 대한 기본적인 개념을 살펴보자.

1) 정보의 질(Qualities of Information)과 보안

정보에는 보호되어야 할 세가지의 질이 있다. 즉 무결성(Integrity) 비밀성 (Confidentiality)및 가용성 (Availability or Continuity)이다. 이것은 컴퓨터에 대한 보안정책의 기본이념(Cornerstone)이 되는 것이며 국가전산망의 정보 보호를 위해 서도 중요한 항목들이다. 그 첫째의 무결성이란 "정보는 원형대로 보존되어야 한다"는 것이다. 그것은 우발적 이건 악의적이건간에 허가없이 변경 되어서는 안된다는 원칙이다. 무결성이란 정보의 정확성과 신뢰성의 척도가 된다. 둘째 비밀성이란 "정보는 소유자가 원하는 대로 비밀이 유지되어야 한다"는 것이다. 따라서 소유자의 인가를 받은 사람만이 보아야 하며 인가되지 않은 공개는 절대로 방지되어야 한다는 원칙이다. 셋째 가용성이란 정보는 "필요로 할때 언제든지 가용하여야 한다"는 것이다. 적시적절하게 사용할수 없다면 그 정보는 소유의 의미를 잃게 되거나 정보자체의 가치를 상실하게 되기 때문이다.

2) 정보시스템의 취약성 (Vulnerability of System Security)

(1) 기술적 측면에서 본 취약성:정보시스템은 대량 데이타의 고속처리로 인하여 오류 발견과 복구가 곤란하고 데이타의 불가시성으로 수정 변경의 증거 수집이 곤란하며 기능과 데이타의 집중으로 인해 피해를 받게 될 경우에는 매우 취약하다. 또한 온라인 시스템의 접근이 용이 하며 자료의 균일적 처리로 인한 취약성을 갖고 있다.

(2) 조직적 측면에서 본 취약성:소수인원에 의한 데이타 처리의 장점은 내부통제가 취약하면 부정 사용의 위협을 유발할 가능성이 있으며 전문가에게만 블랙복스화되어 있는 장점은 내부통제가 취약하면 부정조작의 위협을 유발할 우려가 있다.

(3) 사회적 측면에서 본 취약성:사회전체의 의존도가 높아져 고장 발생시에는 큰 혼란과 손실을 야기시키며 네트 워크화가 됨에 따라 시스템의 신뢰성이 연쇄적으로 영향을 받게 된다.

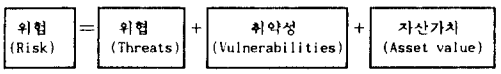
3) 정보시스템상의 위협(Threats to System) 정보시스템에 대한 위협은 다음과 같은 세분류(Three main categories)가 있다. 첫째 우발적인 위협 (Accidental threats to computer security) 둘째 자연에 의한 위협 (Natural hazards to computers) 셋째 인간의 행위에 의한 위협등이다.

인간에 의한 위협에는 정보활동 (Intelligence)상의 임무에서 오는 위협과 범행을 기도하는 종업원으로 부터의 위협이 있으며 바이러스나 핵킹 행위로 부터의 위협과 사용자의 불법 행위나 테러리스트 조직으로 부터의 위협이 있다. 또한 범죄자(Criminal)로 부터의 위협이 있다.

3. 시스템 위험 분석 (Assessing the Risks)

1) 위험의 정의

시스템의 위험(Risk)이란 시스템의 취약성과 위협과 위험에 노출되는 정보자산의 가치 (Asset value)의 총합이다.



위험분석은 문제의 정확한 인식을 위하여 반드시 수행하여야 할 과정이다. 이것은 국가전산망의 경우에도 예외일 수는 없는 것이다. 사고가 발생한 후의 조치보다는 끊임 없는 위험 분석을 통한 대응책 마련으로 문제를 사전에 예방하는 것이 더욱 중요하기 때문이다.

2) 위험분석 기법

분석기법은 세 분류로 크게 나눌 수 있다. 첫째 기법은 계량적 분석(Quantitative analysis)기법이고 둘째 기법은 자동화 기법(Automated risk analysis methodologies) 을 활용하는 것이다. 위험분석을 위한 자동화 도구는 여러가지가 있으나 보편화 된 도구의 하나로는 영국의 CRAMM (CCTA Risk Analysis and Management Method)이 있다 셋째 기법은 재래식 방법이다. 즉 역사적 데이타를 수집하여 분석하는 방법과 공식을 적용하는 방법이 있으며 주관적 위험의 추정 방법과 시뮬레이션/시나리오 방법 등이 있다.

4. 컴퓨터 범죄(Computer Crime)

1) 컴퓨터 범죄의 개념

컴퓨터 범죄의 학설에는 부정설 긍정설 협의로 파악하는 설의 세가지 유형이 있다. 부정설에 의하면 컴퓨터 범죄는 컴퓨터의 기술적 특수성이 개입된 것이 아니라 기존의 범죄 유형에 불과하다는 것이고 긍정설에 의하면 컴퓨터 범죄란 컴퓨터를 행위의 수단으로 하거나 목적으로 하여 형사처벌 되거나 형사처벌할 가치가 있는 행위의 총체를 의미한다는 것이다. 또한 협의설에 의하면 컴퓨터 자료와 관련하여 발생한 재산적 침해 행위를 야기시키는 고의의 범죄 행위의 총체라는 것이다. 컴퓨터 범죄의 특징면에서 보면 전통적 범죄는 일반 관습법의 범죄인데 반하여 컴퓨터 범죄란 과학기술의 부흥과 함께 생긴 비전통적 범죄로서 기술과 지성을 사용하는 범죄이기 때문에 일명 화이트 칼라 범죄(White collar crime)라고도 말하고 있다. 컴퓨터 범죄는 범행자의 직업, 환경, 범죄수법, 자산손실의 형태, 시간규모(Time scales)지역조건(Geography), 사라지는 흔적등에 의한 색출의 어려움 등 재래식 범죄와는 다른 특성을 지니고 있는 것이다.

2) 범죄 수법(Modi Operandi)의 종류

국가전산망에서도 일어날 수 있는 범죄 행위의 대책을 강구하기 위하여 여러가지의 수법들을 간략히 살펴본다.

(1) 데이타의 조작자(Data Manipulator)에 의한범죄

① 데이타 디들링(Data Diddling)

이것은 가장 간단하고 보편적으로 쓰이는 범죄 수법으로서 컴퓨터에 자료를 입력하기 전이나 입력하는 동안에 자료를 변경시키는 것이다. 소스입력 위반(Source entry violations)등이 그 예이다.

② 사라미 테크닉(Salami Techniques)

이것은 어떤 일을 정상적으로 수행하면서 관심밖에 있는 작은 이익을 긁어 모으는 수법이다. 은행에서 소수점 이하의 타인 예금을 자기구좌로 긁어 모으는 수법 등을 말한다.

③ 수퍼잽핑(Superzapping)

컴퓨터는 때로는 정상적인 복구 혹은 재시도 절차로는 극복할 수 없는 상태에 놓이거나 작동 중단되거나 고장이 나는 경우가 있다. 이러한 경우 Universal Access program이 필요한데 이것을 범행에 이용하는 수법이다.

④ 어싱크러너스 어택크(Asynchronous Attacks)

이것은 컴퓨터 OS의 비동기식 기능 (Asynch-ronous Functioning)의 이점을 이용한 범죄 수법이다.

⑤ 시뮬레이션 및 모델링(Simulation and Modeling)

이것은 정상적인 업무처리를 위하여 시뮬레이션 또는 모델링하는 것처럼 하면서 실제로는 자기의 범죄 목적을 위해 작업함으로서 그것을 범죄 도구로 이용하는 수법이다.

(2) 보복 및 손상(Retribution and Damage)을 목적으로 하는 범죄

① 토로잔 호스(Trojan Horse)

이것은 프로그램을 기반으로 하는 사기행위나 사보타지의 가장 보편적인 수법으로 컴퓨터가 본래의 기능을 발휘하면서도 비인가된 기능을 수행하도록 프로그램 속에 범죄자만 아는 비밀 작업지시를 넣어두는 수법이다.

② 트랩 도어(Trap Doors)

대규모 프로그램 개발과정에서 디버깅등을 위해 넣어둔 프로그램 수정 명령을 개 발후에 삭제하지 않고 두었다가 범행에 이용하는 수법이다.

③ 로직 밤(Logic Bombs)

이것은 트로잔 호스 수법과 비슷한 것으로 프로그램내에 비밀 조건을 넣어두고 그 조건과 같은 상황이 되면 자동적으로 불법행위가 이루어지도록 하는 수법이다.

(3) 스파이나 눕(Spies and Snoops)에 의한 범죄

① 스카벤징(Scavenging)

이것은 쓰레기통이나 작업주변에서 카피, 카본페이퍼 등을 습득하거나 작업후 컴퓨터에 남아 있는 잔여 데이타(risidual data)를 습득하는 수법이다.

② 데이타 리키지(Data Leakage)

이것은 인위적 또는 시스템의 기술상으로 정보를 누출시켜 범죄에 이용하는 수법이다.

③ 피기백킹이나 임퍼스네이션(Piggybacking and Impersonation)

이것은 인가된 출입자에 묻혀 슬적 스며 들어가거나 다른사람의 패스워드나 비밀번호 등을 도용하여 범행을 자행하는 수법이다.

④ 와이어 탭핑(Wiretapping) 이것은 유무선을 통해 송수신되는 정보통신 내용을 도청하는 수법이다.

(4) 밴덜이나 불량자들(Vandals and Hooligans)에 의한 범죄

① 바이러스(Viruses)

프로그램을 파괴하거나 교란하거나 시스템을 다운시켜 피해를 주는 등의 범죄성 바이러스를 말한다. 웜 프로그램(Worm program), 트로잔 호스 프로그램, 오버라이팅 바이러스 (O verwritting Virus), 콜링 바이러스(Calling Virus)메모리 상주 바이러스 등이 있다.

② 범죄성 핵킹(Vindictive Hacking)

네트워크를 통한 핵캥으로 자료를 훔치거나 교환하거나 파괴하는 등의 수법으로 큰 피해를 주는 신종 범죄이다. 시스템 핵킹, 록(Lock)풀기 수법, 프로그램 변형 수법 등이 있다.

(5) 파괴분자나 테러에 의한 범죄(Sub-versive /Terror)

재래식 개념의 범죄성 파괴 또는 정치적 이념적 테러행위에 의한 파괴를 의미한다. 그러한 행위에 의한 시스템의 불시 중단 또는 통신망의 불시 마비 등을 의미한다.

(6) 불법적 복사(Illegal copying)

직업적 불법복사를 통하여 경제적 이익을 추구하며 지적소유권이나 개인정보 침해등 의 물의를 일으키는 행위를 의미한다.

5. 시스템을 애워싼 계층별 보안대책(Numerous Layers of Protection)

국가전산망에 적용될 보안대책을 위하여 시스템을 에워싼 계층별 보안대책을 고찰해 보면 다음과 같다.

1) 시스템 운영상의 기술적 안전•보안 대책(System Operation Technical Security)

시스템상의 기술적 접근 통제방법, OS 보안기능상의 기술, 정보통신 및 네트워크상의 보안기술 패스워드상의 기술, 암호화 기술, 보안장비상의 기술, 시스템 차단 추적 진단을 위한 유틸리티상의 기술 등이 있으며 바이러스 방지(백신포함)와 핵킹 방지 기술이 있다.

2) 물리적•안전.보안대책(Physical Safety and Security)

시스템과 시설에 대한 물리적 접근 및 출입통제와 불법 침입자의 통제(Intruders Control) 화재 예방, 자연 재난 대책, 시스템 및 시설 보안대책 등이 있다.

3) 행정적 안전•보안대책(Administrative Safety and Security)

운영상의 보안과 로그작성 통제, 문서보안(Document Security), 라이브러리 관리 시스템, 유지 보수상의 보안절차, 평가 인가 기준, 통신상의 보안 및 위험분석 절차 등이 있다.

4) 인적 보안 대책(Personnel Safety and Security)

범죄행위 유발 억제 대책과 직원으로 부터의 정보보호 대책 및 직원 관리상의 보안대책 등이 있다.

6. 암호화 대책

암호화는 정보보호를 위한 유용한 대책중의 하나이다. 암호화는 데이타의 보호, 불법 액세스의 방지,

전자거래 결제에서의 서명등 여러가지 역할을 할 수 있어 통신보안, 파일보안 통신상대의 인증, 디지틀 서명 등에 폭넓게 응용 된다. 현대의 암호 방식으로는 관용 암호방식(Conventional Encryption System), 공개 키 암호방식, 공개키 배분시스템(Public Key Distribution System), 비밀키 분할 소유방식, 제로지식 프로토콜(Zero Knowledge Interactive Proof), 식별정보에 입각한 암호방식, 암호 알고리즘의 해독 등 여러가지 방법이 있다. 국가전산망에서도 암호화의 대책은 매우 중요하므로 상세한 설 명이 요구되나 특집의 전문연구난으로 미룬다.

Ⅲ. 국가전산망의 안전·보안업무 계획 및 현황

1. 범죄 발생 현황 및 시행 법령

1) 컴퓨터 범죄 발생 현황

1992. 9.21 현재 대검찰청 형사정책 연구원 등의 조사집계에 따르면 그간 국가사회적으로 발생한 컴퓨터 범죄의 총 건수는 45건으로 매년 30%정도씩 증가하고 있는 것으로 분석되었다. 그중 금융기관에서 발생한 사고 건수는 35건으로서 77.8%의 대종을 이루고 있다. 그후 1994. 4 현재까지 33 건이 추가로 발생함으로써 노출된 총 사고 건수는 78 건에 이르고 있다. 그중 국가전산망을 포함하여 공공전산시스템에서 발생한 각종 사고의 사례를 분석해 보면 부표 1과 같다.

2) 보안관련 법령 및 표준화 현황

(1) 법령 및 기준

- 공공기관의 개인정보보호에 관한 법률(총무처 1994.1.7 공고) (1995.1.7 시행)
- 통신 비밀 보호법 (체신부 1993.12.27 공고) (1994.6.28 시행)
- 전산업무 보안관리 지침(안기부 1988. 8)
- 컴퓨터 시스템 안전 관리기준(과기처 1989.9)
- 전산처리되는 개인정보 보호를 위한 관리지침(총무처 1991.5)
- 행정전산망 안전관리 지침(총무처 1991. 10)
- 전산망 안전·신뢰성 기준(체신부 1993. 2) 2)

(2)전산망 안전.보안 표준

- 전산망보안관리를 위한 기술지원서: 총론(체신부 전산망 표준 1993.2)
- 전산망보안관리를 위한 기술지원서: 물리적 보안(체신부 전산망 표준 1993.2)
- 국가전산망 패스워드 활용 표준(체신부 전산망 표준 1993.2)

2. 국가전산망의 안전.보안 업무 방침

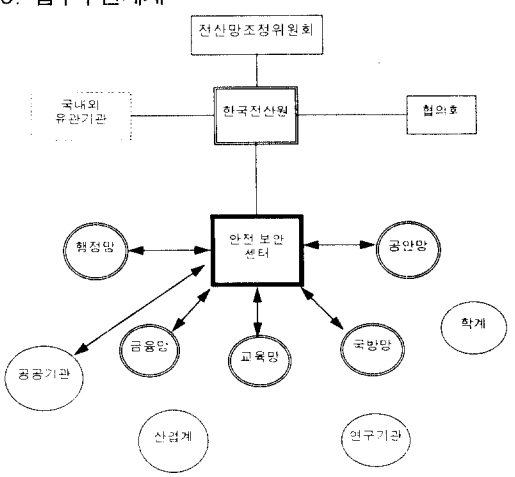
1) 목표

국가전산망의 목표는 국가사회정보화의 역기능을 방지하고 전산망의 안전.보안 업무 체계를 정립하여 시스템상의 기술적 물리적 행정적 인적 차원의 대응책을 강구함으로써 전산망의 안전성, 신뢰성, 보안성을 확보함을 목표로 한다.

2) 안전.보안업무 방침

이와 같은 목표 달성을 위하여 다음과 같은 방침아래 안전.보안업무를 추진한다. 국가사회 정보화의 역기능 방지를 위한 종합대책을 수립하고 국가전산망 및 공공전산 시스템의 정보 보호를 위한 기술적 대책을 연구하며 국가전산망 안전.보안성 기준 및 평가절차를 표준화한다. 그리고 안전.보안에 관한 관련 법규(안)과 정책방안을 연구하고 사고발생 사례 및 기술적 자문요청을 센터에서 접수하여 조치한다. 또한 국내외 전산화의 안전.보안에 관한 자료를 수집하여 분석 관리하고 예견되는 문제점에 대한 선행연구를 실시하며 국내외 관련기관과의 유기적인 협조체제를 유지하고 실무협의회를 구성하여 효율적인 업무 추진을 도모한다. 안전 보안에 관한 홍보활동을 강화하여 국가 사회적으로 전산망에 관한 안전.보안의식을 고취시키고 중요한 정책사항에 대해서는 국가전산망조정위원회의 의결을 거쳐 시행한다. 한국전산원은 전산망 조정위원회의 지침아래 국가전산망 안전.보안센터의 기능을 수행하여 목표를 성공적으로 달성한다.

3. 업무추진체계



4. 전산망별 현황 및 추진계획

1) 행정전산망

(1) 안전•보안 업무 현황

① 행정전산망에서는 안전관리나 개인정보 보호를 위한 제도적 관리지침 및 법률을 입법 조치하여 시행하고 있다.

② 기술적 대책을 포함한 세부지침 현황은 다음과 같다. 접근 통제에 대한 조치로 감시용 폐쇄회로를 가동하고 출입문 보안키를 설치 하였으며 패스워드 프로그램을 3급 비밀화하여 취급하고 패스워드를 수시 변경 시키고 있다. 각 단말기로 부터의 주전산기 접근기록을 자동유지토록 조치하고 기록 내용을 정기 분석하여 불법접근 여부를 확인하고 있다.

③ 기타 안전.보안 업무 추진 현황은 다음과 같다. 행정전산망의 안전.보안관리 실태조사를 실시하여 미흡한 기관은 행정지도를 하고 우수기관은 수범 사례를 발굴하여 포상하고 있으며 컴퓨터 범죄, 바이러스, 핵커 침해 등에 대한 예방 홍보 활동을 강화하고 총무처 전자계산소 전산교육 과정에 행정전산망 운영요원의 안전.보안 관리 교육을 편성하여 실시하고 있다.

(2) 안전•보안업무 발전 방안 추진 계획

① 안전•보안관리 평가기법을 개발하여 보급한다. 평가 대상 항목을 선정하고 체계적으로 분류하여 선정항목별 평가수단을 결정토록할 계획이다. 예를 들면 결정론적 평가법(체크리스트에 의한 종합평점)을 적용하고 소프트웨어 수단으로 종합평가가 가능한 공통활용 팩키지를 개발하여 기계적 수단으로 장치.장비 등을 설치하도록 한다.

② 계층별 안전.보안관리 대책을 강화한다. 기술적 대책으로 시스템 접근제어 프로그램을 개발하고 바이러스 예방과 치료에 대한 대책을 강구하여 송수신 자료를 암호화 한다.

③ 안전.보안관리 교육과 홍보의 활성화를 위하여 전산교육을 확대 실시하고 보도 매체를 적극 활용한다.

④ 안전.보안관리의 과학화 자동화를 위하여 평가기법을 개발 보급하고 접근제어와 비밀보호를 위한 기기를 개발 보급한다.

2) 금융전산망

(1) 안전.보안업무 현황

① 금융전산망에서는 창구단말의 보안, CD의 부정사용 방지, 무자격자의 단말접근, 통제 통신회선의 보안, 시스템의 보안, 소프트웨어의 보안 및 정보의 누설 방지 등에 대한 철저한 보안 대책을 전제로 하고 있다. 따라서 다음과 같은 업무별 안전.보안 대책을 추진하고 있다.

(가) CD 공동망

CD 카드의 보안을 위하여 CD카드 발급시 비밀번호를 M/S상에 Encoding하지 않 도록 하여 비밀번호의 노출을 방지한다. 비밀번호 확인은 개설은행에서만 가능토록 조치하고 현금카드를 고객에게 직접 교부 할때 까지 원장 화일에 미교부 표시를 하여 카드 교부전 부정사용을 방지한다. 금액 검증을 위하여 취급은행으로 부터 현금지급 요청을한 전문상의 거래금액과 개설 은행에서 통보한 현금지급 승낙보고 전문이 상이할시 에러 처리를 한다

(나) 타행환 공동망은 은행별 전문관리 번호를 부여하여 관리하고 참가은행과 중계 센터에서 각각 전문 검증을 하도록 한다.

(다) 자동 응답 서비스(ARS) 공동망은 고객관리 번호의 통지용 전화 번호를 검증하고 전문 관리 번호도 검증 한다.

② 중계센터의 보안대책

(가) 시스템 사용자는 중계 시스템실의 등록절차에 따라 등록하고 시스템 운영자는 관리책임자가 인정하는 USER-ID에 등록시에만 사용을 허용토록 한다

(나) 시스템 패스워드는 중계시스템실 관리책임자와 OS 관리자만 숙지하여 무허가 시스템 접근을 방지한다.

(다) 데이타 화일에 보안 번호를 부여하여 데이타 화일의 위 변조를 방지한다.

(라) 메인 시스템의 CPU 및 디스크의 예비 체제를 가동 운영하고 데이타의 소산등으로 H/W 운영상의 안정성 확보 및 S/W 수정시 프로그램 등록절차의 규정화 등으로 S/W 신뢰성을 확보한다. 시스템 운영 관리요원의 교육 훈련을 강화하고 출입문 자동제어 시스템, 폐쇄회로 TV 설치, 출입자 명부 유지 관리, 카드 키 및 카드키 패스워드 관리 등으로 출입자를 통제한다.

(마) 동기전송기술을 이용한 고속전송, 블럭화된 전문전송, 금융기관 공동업무 표준 CCITT X.25 사용, 포인트 투 포인트 방식의 전용회선망 구축, 예비회선 설치 및 중요 통신제어 장치에 대한 예비장치를 확보하고 9600 BSP 급의 전용회선을 사용한 지능모뎀(Intelligent Modem) 및 회선관리 시스템(Network Management System) 이용으로 회선상태를 감시하고 CD 중계센터의 S/W인 Base 24-ATM으로 라인

탭핑(Line Tapping)을 감시토록 한다.

(2) 안전·보안업무 발전 방안 추진계획

① CD 공동망 시스템의 안전, 보안 업무를 강화한다. 현금카드의 보안 방법으로 마그네틱 스트라이프의 데이타도 암호화하고 CD자체에서의 보안 유지를 위하여 CD기자체 에서의 검증 강화를 위한 규격화와 계좌번호의 암호화를 추진한다. 통신회선상의 보안대책으로는 전문의 노출 및 도청 방지를 위한 대책을 수립한다. 또한 보안성 향상을 위해서 고객 정보에 대한 암호화를 강화하고 각행 시스템과 중계센터 시스템상에서의 보안 유지책을 강구한다.

② 타행환 공동망 시스템 및 ARS 공동망 시스템의 보안 절차를 강화한다.

③ 센터시스템의 향상 방안으로 네트워크상의 보안대책, H/W상의 보안대책 테스트, 운영, 프로그램 변경 관리를 포함 하는 S/W보안의 강화 대책을 강구한다.

3) 교육연구 전산망

(1) 안전·보안 업무 현황

교육연구전산망에서는 국내외 최신 학술정보의 적시 활용 체제를 구축하고 수퍼컴퓨 터의 컴퓨팅 파우어와 S/W의 공동활용 체제 확립을 목적으로 다음과 같은 안전.보안 대책을 추진하고 있다. 전산자원의 보안을 위하여 수퍼컴퓨터 사용자의 관리와 통신 시설의 보호관리를 하고 있으며 네트워크 보안을 위하여 네트워크 서비스 중 취약 부분을 패쇄하고 Router에서의 서비스를 선별적으로 제공하며 보안사고 발생시 역추적을 통한 문제 해결을 하고 있다. 시스템 보안으로는 패스워드 관리, 주요화일의 점검, 불법 특권 사용자 색출, Back door 색출 및 시스템 관리자의 24시간 감시관리 체제를 운영하고 있으며 보안 S/W를 개발하여 적용하고 있다. 기타 보안관련 자료를 수집 배포하고, 대내외 보안 그룹 활동 및 보안교육을 강화해 나가고 있다.

(2) 안전·보안 업무 발전 방안 추진 계획

가) 교육 연구 전산망의 보안센터를 구축하여 다음과 같은 기능을 수행한다.

① 보안사고 피해의 사전방지와 최소화를 위하여 보안 정책을 결정하고 가입기관을 위한 보안지침서를 제작 배포하며 가입기관의 보안관리자와의 연락 체제를 유지한다. 또한 Key 관리 센터의 역할을 한다.

② 보안사고 처리기능을 위하여 보안사고 처리절차를 체계화하고 보안사고 해결을 위한 전문가 그룹을 형성 하여 국내외 보안센터와의 연계체계 구축과 보안 사고 해결 방안의 문서화를 실시한다.

③ 보안정보의 체계적인 서비스를 위하여 보안사고 사례 및 처리에 관한 정보, 보안관련 기술 및 기기 정보, 해외 유관기관의 보안업무에 관한 정보 등을 수집한다.

④ 보안관련 기술증대를 위하여 보안관련 기술을 연구개발하고 국내외 보안활동 참가 및 워크샵을 개최한다. 또한 보안기술 교육을 실시한다.

Ⅴ. 안전·보안 대책 시행사례

행정전산망에서는 기술적 안전.보안 대책의 하나로 주전산기1용 보안 유틸리티를 개발하여 시행하고 있다. 행정전산망은 X.25 공중망을 통하여 전국적으로 연결되어 있기 때문에 일반인은 물론 특정 목적을 가진 범죄자에게 노출될 가능성이 높은 취약성을 가지고 있음으로 현실적으로 실질적이고 기술적인 대책을 수립하여 시행하고 있음은 큰 의미를 가지고 있다고 판단된다.

1. 보안 유틸리티 개발 구현 방향

행정전산망의 기술적인 보안대책은 주전산기인 톨러런트 시스템이 제공하고 있는 기본 기능에만 주로 의존하여 왔음으로 시스템 자체의 보안기능 향상을 목표로 하는 유틸리티 개발이 시급한 실정이었다. 따라서 다음과 같은 세가지 기능의 보완을 목표로 개발하였다.

○ 주전산기인 톨러런트 시스템에서 제공하고 있는 보안관련 유틸리티의 기능 개선

○ 톨러런트 시스템의 보안 취약점을 보완할 수 있는 유틸리티 개발

○ Internet의 공개 소프트웨어 중 보안 유틸리티의 연구 및 이식

2. 보안 유틸리티 기능의 종류

개발한 유틸리티의 기능은 첫째 시스템 침입자의 차단 기능, 둘째 시스템 침입자의 추 적 기능, 셋째 시스템 보완 상태의 진단 기능 등이다.

3. 기능별 개발유틸리티의 내용

1) 시스템 침입자의 차단 기능 관련 유틸리티

(1) 패스워드 보안

패스워드 보안의 일반적인 기능은 시스템 사용자의 패스워드 등록 변경과 점검기능 제공으로서 이제까지 구현된 보안기능은 톨러런트에서 제공하는 패스워드 암호화의 기본기능만을 제공하였다. 따라서 단순한 몇가지의 패스워드 등록절차를 제공하기 위해서 패스워드 도용 및 추정에 의한 시스템 침입의 위험성이 상존하였다. 예를들면 한문자만으로도 패스워드 등록이 가능하였고 노출되기 쉬운 자신의 Login-ID로도 패스워드 등록이 허용되었으며 동일한 문자를 연속적으로 나열한 단순한 패스워드 등록도 허용하고 패스워드 변경시 기존 패스워드와 동일하게 변경 하는 경우에도 변경이 허용되었다. 따라서 이러한 문제점을 보완하기 위하여 유닉스 시스템에서 일반적으로 적용하고 있는 패스워드 등록기능을 구현하였다. 예를들면 최소 6자이상 8자 이하의 패스워드만 등록을 허용하고 자신의 Login-ID 및 Login-ID를 순환시킨 패스워드는 등록을 불허하며 최소 1자 이상의 특수 문자를 포함해야 등록이 허용되도록 하였다. 또한 패스워드 변경시 기존 패스워드와 최소 3자이상 달라야 등록이 허용되도록 하였다.

(2) root 권한 취득 차단 기능

○ txlogin, login

시스템 침입자가 일정횟수 이상 패스워드 입력 실패시 해당 터미날의 기능을 정지시키는 기능을 구현하였으며 /etc/securetty화일에 등록되어 있지 않은 터미널에서 root login을 시도하여 실패 했을 때는 그 실패 이유를 출력토록 하였다.

○ su(substitute user)

사전에 허가된 터미널에 대해서만 root login을 허용하는 etc/securetty 파일 의 기능과 같이 사전에 허가된 사용자에게만 root-ID를 취득할 수 있는 기능을 구현하였으며 root 권한이 필요한 경우도 root 패스워드 점검절차 없이 명령어 수행시에만 일시적으로 권한을 부여하는 기능을 구현하였다.

(3) 터미널 자동 Log out 기능

○ Kcsh, csh

일정시간 사용하지 않고 있는 터미널에 대해서는 유휴시간 (idle time)을 점검하여 자동 logout 시키는 기능을 구현하였다.

2) 시스템 침입자의 추적기능 관련 유틸리티

(1) X.25 관련 유틸리티: X.25 공중망 사용자는 각각 자신의 고유한 X.25 주소를 가지고 있음으로 X.25 공중망을 경유한 시스템 침입자의 주소 검출 기능을 구현하였다.

(2) TCP/IP 및 UDP/IP 관련 유틸리티: TCP/IP 및 UDP/IP 프로토콜을 이용하는 전산망에서는 호스트마다 자신의 고유한 IP 주소를 가지고 있음으로 시스템 침입자의 IP 주소 검출기능을 구현하였다.

3) 시스템 보안상태 진단 관련 유틸리티: 톨러런트 시스템의 운영체제에서 제공하는 보안수준이 미약하므로 운영체제에서 관리하지 못하는 시스템 보안 공백을 유틸리티 수준에서 진단하여 문제점을 경고할 수 있는 기능을 구현하였다.

Ⅳ. 결 론

이상 정보화의 역기능 현상과 위험분석을 고찰해 보았으며 암호화 기법과 컴퓨터 범죄 방지를 위한 계층별 안전.보안 대책 등 국가전산망에 적용될 일반적 이론을 고찰해 보았다. 아울러 국가전산망의 안전.보안업무의 현황과 추진방침 및 향후의 추진계획 등 을 각 망별로 고찰해 보았다. 그동안 국가전산망에서는 안전 보안성을 중요시하고 각종 절차의 표준화와 기술적 보안 대책을 다각적으로 강구 해왔음이 사실이다. 그러나 그 대책수립의 전제조건이 되었어야 할 시스템의 위험분석과 데이타의 암호화, 컴퓨터 범죄의 수법별 세부 대책등은 아직 미흡한 상태에 있다. 우리는 부표 1의 사례에서 볼 수 있듯이 우리나라의 컴퓨터 범죄 수준은 기술적으로 아직은 기초적 수준에 이르고 있음을 알 수 있다. 따라서 환경과 여건이 더 악화되기 전에 첨단기술에 부응하고 역작용이나 범죄수법에 선행하는 내실있는 안전.보안 대책을 더욱 심도있게 강구해 나가야 할 것으로 믿는다. 또한 향후의 보안대책은 어느 한 망만의 보안이 아니라 국가사회 전체 시스템의 균형있는 보안대책으로 국가총체적 전산화의 안전성.보안성이 이룩되어야 할 것을

표 1. 공공분야 컴퓨터 범죄 발생사례

순번	기관	구분	시기	내 용
1	과기처 중앙전자계산소	데이타변조	73.10	국내 최초의 컴퓨터범죄로 서울 반포 AID 차관 아파트 입주자 추춤 부정사건이 발생함. 과기처 중앙전자계산소 프로그래머가 입주자 당첨과 관련된 프로그램을 조작하여 9세대를 부정 당첨 시킴.
2	외무부 여권과	타인명의도용 데이타변조	92.4	외무부 여권과에 근무하는 노씨는 부로커의 청탁을 받고 92년 4월부터 여권발급이 불가능한자에게 타인의 주민등록번호와 이름을 도용 30여회에 걸쳐 여권을 부정 발급함.
3	우체국	컴퓨터 부정조작	92.4	범행자는 영광군 불갑우체국에 들어가 체신부 감사라고 신분을 속이고 1만원이 입금된 자신의 통장에 30억원이 입금된 것 처럼 조작하여 횡령한 사건임.
4	군청	부정입력	92.10	엄씨는 자기소유의 밭 5236평방미터를 사전에 형질변경하고 여주군청의 토지대장 공무원과 결탁하여 컴퓨터에 입력된 토지의 지목을 갑종지로 수정 입력해 전매 차익을 챙긴 사건임.
5	학교	컴퓨터부정조작	93.2	광운대학 전산실 관리자들은 학교측으로 부터 특수수험생들으 명단을 넘겨 받아 총점이 수록된 디스켓에서 객관식 점수를 고쳐 탈락생을 합격권 안에 들도록 한 사건임.
6	데이콤 천리안. 망	ID도용	93.2	3수행 김재열은 재무부 국제심판소 이씨의 ID를 도용해 데이콤의 천리안에 등록된 청와대 비서실의 비밀번호를 바꾸도록한 뒤 청와대 비서실을 칭하여 금융및 정보통신기관의 기밀 자료를 빼내려 한 사건임.
7	경찰서	부정입력	93.2	주거침입절도 피의자 신씨에 대한 컴퓨터 조회를 하다 동명이인의 사기기소 중지 부분을 첨가하고 그 사실이 밝혀지자 의경이 컴퓨터 범죄 경력조회 잘못을 비관하고 자살한 사건임.
8	법원	데이타변조	93.2	서울지검 남부지검 남부지청 이검사는 피해자에 붙잡혀 관악경찰서를 통해 넘겨 받은 상습 피의자 강씨를 지난해 수배 고소가 취하 되었다며 귀가조치, 항의를 받자 컴퓨터 범죄 경력 조회자료로 부터 청량리 경찰서 수배부분을 빼버린 사건임.
9	한국통신 하이텔망	사기횡령	93.7	가명 강선진 사건으로 타인의 전화선을 도용 하이텔을 이용하고 전화요금을 남에게 전가시키고 현금을 사취하였으며 하이텔 계시화면에 관련기기들을 헐값에 판다고 속여 은행계좌를 이용 신청자들로 무터 5백만원을 사취한 사건임.
10	우체국	컴퓨터부정조작	94.1	전 부안 우체국 예금 보험계장인 고씨는 예금보험계장 겸 수표발행 담당자로 근무하며 직위를 이용 자기앞 수표를 임의로 발생한 뒤 잔고가 있는것 처럼 컴퓨터를 조작하여 국고 46억원을 횡령한 사건임. (자수 94.1)
11	경찰	컴퓨터오용	94.3	경찰이 각 파출소와 연결된 행행망용 컴퓨터를 통해 개인 전과 기록과 주민 조회 기록 등을 불법 흥신

순번	기관	구분	시기	내 용
				사업자에게 팔아넘긴 사건임.
12	차량등록 관리사무소	컴퓨터오용	94.4	자동차 관리 전산망을 통한 차량 등록 원부의 열람으로 외제 고급승용차의 차주를 확인하여 강도 대상으로 삼은 사건임.
13	법원	바이러스	92.7	대하소설 태백산맥의 저자가 출판사를 상대로 낸 2천만원 청구소송 선고를 위한 서울 민사지법 주심판사의 판결문이 바이러스로 지워져 선고를 연기한 사건임.
14	국립중앙 도서관	바이러스	93.10	국립중앙도서관이 지난 7월에 설치한 전자도서실에 바이러스가 침입하여 모든 자료를 지우고 본체까지 훼손한 사건임.
15	서울대 교육전산망	핵킹	92.7	서울대 교육전산망에 컴퓨터 핵커가 침입해 6대 W/S에 수록되어 있던 자료를 전부 파괴한 사건임.
16	서울대	핵킹	93.4	서울대 인사자료와 성적등을 종합관리하는 내부 전산망에 컴퓨터 핵커가 침입해 시스템의 모든 자료를 파괴시킨 사건임.

參 考 文 獻

[1] Baker, Richard H. *Computer Security Handbook*. New York: McGraw-Hill, Inc., 1991.

[2] Bureau of Justice Statistics. *Computer Crime-Criminal Justice Resource Manual*

[3] Washington D.C.: U.S. Department of Justice, 1979.

[4] Collinson, Helen. *Computer Fraud & Security*. England: Elsevier Science Ltd., 1994.

[5] Fites, Philip E.; Kratz, Martin P.J.; Brebner, Alan F. *Control and Security of Computer Information Systems*. New York: Computer Science Press, Inc., 1989.

[6] Forester, Tom; Morrison, Perry. *Computer Ethics*. Massachusetts: The MIT Press, 1990.

[7] Lane, V.P. *Security of Computer Based Information Systems*. London: Macmillan Education Ltd., 1985.

[8] Parker, Donn B. *Managers Guide to Computer Security*. Virginia:Prentice-Hall, Inc. 1981.

[9] Pfleeger, Charles P. *Security in Computing*. NJ:Prentice-Hall, Inc., 1989.

[10] Smith, Martin. *Commonsense Computer Security*. New York:McGraw-Hill, Inc., 1993.

[11] Tapper, Colin *Computer Law*. New York:Longman, 1989.

[12] 김문일. 『컴퓨터 범죄론』. 서울:법영사, 1992.

[13] 김세헌. 『컴퓨터 범죄와 프라이버시 침해』. 서울:희성출판사, 1989.

[14] 김진식. 『핵커들의 핵킹기법』. 서울:연암출판사, 1993.

[15] 노연후. 『컴퓨터 범죄』. 서울:하이테크정보,1992.

[16] 박명순. 『컴퓨터 바이러스』. 서울:기한제, 1990.

[17] 이형원. 『정보시스템 안전대책』. 서울:영진출판사, 1993.

[18] 전산망조정위원회. 『국가전산망 기본계획』. 서울:전산망조정위원회, 1990.

[19] 한국전산원. 『국가기간전산망 세미나(Ⅱ)』. 서울:한국전산원, 1994.
[20] 한국전산원. 『주민관리전산망 보안대책에 관한 연구』. 서울:한국전산원, 1990.
[21] 한국전산원, 『주전산기 I용 보안 유틸리티 개발 보고서』. 서울:한국전산원, 1993.
[22] 한국전산원. 『컴퓨터 보안관리 지침 연구』. 한국전산원서울:, 1990.
[23] 한국전자통신연구소. 『컴퓨터 범죄와 암호와 대책』. 대전:한국전자통신 연구소, 1990.

筆者紹介

李 在 雨
1934年 9月 4日生
1979年 8月 서울대학교 행정대학원 수료
1984年 6月 University of Southern Calofonia (석사)
1992年 8月 건국대학교 대학원 행정학 (박사)

1983年 1月 ~ 1984年 12月 판문점 군사정전위원회 한국군 수석대표
1987年 1月 ~ 1992年 6月 한국전산원 기획조정실장
1988年 1月 ~ 1993年 12月 국가전산망 조정위원회 실무 추진위원
1988年 1月 ~ 1993年 12月 행정전산망 추진위원회 추진위원

주관심 분야 : 정보체계(시스템 안전보안, 전산감리)