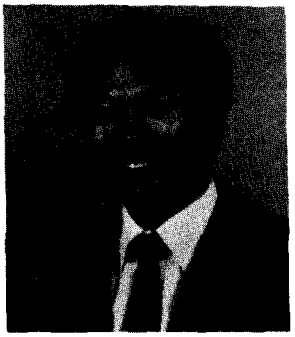

컴퓨터 바이러스 : 現況과 對策
COMPUTER VIRUS

金 麗 腥*
Kim, Ryo Sung

目 次

Ⅰ. 序 言

바이러스(Virus)는 濾過性病原體로서 크기와 모양은 매우 다양하며, 이 병원체는 단순한 것으로 부터 다소 복잡한 구조로 구성된 超顯微鏡的인 微粒子로 알려져있다.

그러나 컴퓨터 바이러스(Computer virus)는 이런 病原體인 바이러스와는 전혀 다르다.

컴퓨터 바이러스는 病原體처럼 컴퓨터를 만질때 감염되거나 컴퓨터 사용자에게 병을 옮기는 것이 아니고 단지 컴퓨터를 작동시키는 프로그램(program)의 일종일 뿐이다.

컴퓨터 바이러스는 프로그램이므로 일반적으로 개인용 컴퓨터(PC)에서 사용하는 보조기억장치인 디스켓(diskette)에 저장되어 있다가 이 디스켓을 컴퓨터에 넣고서 작동시키면 그때부터 우리(使用者)가 원하지 않는 여러가지 나쁜 作動(bad operation)을 시작하게 된다.

그 나쁜 작동이란 컴퓨터바이러스 프로그램이 컴퓨터를 움직이는 基本運營 프로그램들을 變形시켜서 자기자신(virus program)을 複製시키는 것이다. 또 어떤 바이러스 프로그램은 일정기간이 지난후 디스켓에 저장된 내용을 사용하지 못하게 지워버리므로써 컴퓨터內의 귀중한 프로그램을 파괴하기도 한다.

컴퓨터 바이러스는 개인용컴퓨터 뿐만 아니라 컴퓨터 단말기나 通信네트워크등, 여러가지 經路를 통해서 컴퓨터(mainframe)에 보관된 다양한 정보를 공격하고 있다.

이런 다양한 정보는 컴퓨터를 잘 작동토록하는 運營體制(OS), 컴퓨터에 보관시킨 프로그램이나 중요한 資料(data)가 컴퓨터바이러스의 主要한 공격목표가 되고 있다.

이런 컴퓨터바이러스에 대해서 그 발생경위, 바이러스의 종류, 바이러스 감염과 그 증상 그리고 바이러스 예방대책에 대해서 차례로 살펴보도록 하자.

Ⅱ. 歷 史

1970년대말 미국의 세계적 通信會社인 「AT

* 情報處理 技術士(電子計算機組織應用) 韓國證券電算(株) 企劃部長

& T」社의 「Bell」연구소에서 "core war"라는 프로그램이 제작되어 연구소에서 일하는 연구원들에게 전달·유포되었다. 밤늦게까지 일해야 하는 연구원들의 무료함을 달래기 위해 프로그램間 決鬪式 게임프로그램이 사용되고 있었다.

이 게임 프로그램은 벨연구소의 연구원으로 있던 더글러스 맬로이(H. Douglas Mellroy), 빅터 비소스키(Victor Vysottsky)와 로버트 모리스(Robert Morris)에 의하여 만들어졌다. 이들은 프로그램 스스로가 프로그램을 파괴하는 명령어를 가질 수 있다는 점에 착안하여 컴퓨터 프로그램끼리 상대의 프로그램을 파괴하는 게임을 만들었다.

즉 두사람의 프로그래머가 각각의 기억장소내에 증식하는 벌레(worm)프로그램을 만들어 증식시킨 후 어떤 신호가 주어지면 그때부터 이 두 프로그램은 서로 다른 프로그램을 파괴하는 것이다. 일정한 시간이 경과한 후에 파괴행위는 중지되고 그 시점에서 보다 많은 수가 살아 남은 프로그램을 만든 쪽이 勝者가 되는 게임이다.

이러한 自己複製 결투식 게임프로그램의 비밀이 알려진 것은 1983년 켄 톰슨(Ken Thompson)이 터닝(Turning)상을 받고나서 수상기념연설에서 그 제작방법까지를 일반 대중에게 공개해 버린때 부터이다.

「core war」를 제작한 당시에는 거의 모든 컴퓨터들이 서로 연결되지 않은 상태로 운영되고 있어서 그 복제되는 상태가 다른 시스템에 영향을 주지않고 제한되어 운영되고 있었다. 이경우 게임 프로그램의 제작자는 그 위험정도를 충분히 인식하고 있어서 벌레프로그램의 活動범위를 이 컴퓨터시스템만으로 철저히 제한하고 있었기 때문에 감염의 위험도 없고 자체 시스템의 파괴도 미리 배제할 수가 있었다.

또한 이 프로그램의 진행 결과로 기억장치(memory)의 내용이 뒤엉켰을 경우 단지 셧다운(shut down)시킴으로써 기억장치에 뒤엉킨 내용을 모두 지워버리고 디스크에 보관된 오염되지 않은 새로운 運營體制(OS)를 다시 記憶裝置에 복구시킴으로써 정상운영이 가능해지는 것이다.

그런데 최근 여러 곳에서 산발적으로 발견되고 있는 컴퓨터 바이러스들은 대부분 이렇게 「core war」 프로그램처럼 自己複製式 原理에 그 기초를 두고 있으며 그 활동범위를 확장시켜 補助기억장치에 보관된 내용까지 변형시켜 나가고 있는 것이다.

1987년 가을 이스라엘의 「Hebrew」대학에서 발견된 바이러스는 그 模倣의 초보적 단계를 잘 나타내주는 좋은 例가 될 것이다. 감염 主對象을 디스크에 보관된 프로그램(program)으로 정하고, 끊임없이 自己複製를 해나가다가, 지정된 날자에 감염된 프로그램들이 모든 디스크 화일(file)[1]을 일시에 지워버리도록 설계되어 있었다. 그러나 감염 여부를 구분하지 않고 맹목적으로 自己複製를 반복한 결과 디스크의 과다소비가 초래되어 더 이상 복제할 수 있는 여유가 없어서 目的이 達成되기 전에 발각되어 제거당했다.

앞에서 설명한 벨연구소의 「core war」 프로그램의 경우 이외에도 몇가지 사실을 우리는 想起해 볼 필요가 있다.

그것은 1970년대 중반 미국 제록스(Xerox)사의 팔로·알토(Palo Alto)연구소의 연구원인 「John Shoch」와 「Ion Hupp」가 컴퓨터 바이러스를 시험적으로 개발하였다는 것이다.

또한 1970년대 중반 美國 국방성의 대규모 通信네트워크 시스템중 「ARPANET」에 벌레(worm)프로그램이 침입하여 여기저기에서 증식하고 있었다. 이때 이 벌레(worm) 프로그램은 다음과 같은 文句를 제시하였다.

「I'm creeper, catch me if you can!」

이 벌레(worm)프로그램을 없애기 위하여 「ARPANET」의 시스템 관리자들은 리퍼(Reaper)라는 벌레제거 프로그램을 개발하였다.

이것이 바로 최초의 백신(vaccine) 프로그램으

註1 : 화일(File) : 서로 관련있는 정보의 集合

로, 크리퍼(creeper)를 추적하여 없애버리는 역할을 수행하였던 것이었다.

한편 1983년 11월 3일 신시내티(Cincinati) 대학의 한 연구팀은 프로그램 自身을 다른 화일에 複製시키고 때에 따라서는 스스로 進化할 수도 있는 컴퓨터바이러스를 한 실험을 통해 만들어 보았다.

이 연구팀은 여러가지 컴퓨터에 移植하기 쉬운 運營體制인 유닉스(UNIX)下에서 「VAX 11/750」컴퓨터시스템을 이용해 8시간의 작업끝에 성공적으로 바이러스 프로그램을 개발하였다. 이 연구팀은 바이러스 프로그램이 외부로 流出되는 것을 철저히 봉쇄하고 완벽한 追跡기능을 도입한 후 이 바이러스를 컴퓨터내의 한 프로그램에 슬쩍 심어 놓았다. 이 바이러스에는 물론 破壞기능은 첨부되지 않았다. 5번에 걸쳐 실험이 수행되었는데 모두 한시간 이내에 운영체제 프로그램을 감염시켜서 전체시스템을 마음대로 통제하는데 성공하였다. 이 바이러스에 파괴기능을 첨부하였다면 컴퓨터시스템의 全面的 파괴가 쉽사리 이루어질 수 있었던 것은 당연한 일이다.

그후 이 연구팀은 각종 여러가지 컴퓨터 시스템에서의 바이러스 전염정도에 대한 실험을 수행하였는데 그 결과는 표 1과 같다.

연구팀은 이 실험내용을 1984년 컴퓨터 保安관련학회에 발표하면서 바이러스 프로그램의 出現가능성과 가공할 위험성을 경고하고 이에 대한 對應策 수립을 주장하였으나 대부분 이러한 위협에 대해 안이하게 생각하였고 다만 극소수의 사람들에게만 흥미의 대상이 되어 왔다.

Ⅲ. 定　　義

컴퓨터 바이러스의 정의는 아직도 확실히 정립되어 있지않다. 그러나 최근에 발표되는 여러가지 논문이나 記事로 미루어 보건대 대체로 다음과 같이 定義해 볼 수 있겠다.

「컴퓨터 바이러스란 프로그램의 일종으로서 컴퓨터를 작동시키는 基本運營 프로그램이나 資料를 변형시켜서 시스템의 資源(resource), 컴퓨터內의 프로그램 또는 情報를 담아 둔 화일(file)을 파괴시키거나 運營에 제한을 가한다. 그리고 같은 機種의 컴퓨터나 연결된 通信網을

표 1 컴퓨터 바이러스 실험자료

환경 / 내용	PC-DOS	BASIC	UNLX.C	UNIX SHELL	VAX / VMS
프로그램 소요시간	4시간	4시간	8시간	15분	30분
감염소요시간	2초	10초	0.5초	1초미만	1초미만
프로그램 줄 수	25줄	100줄	200줄	7줄	9줄
시도한 횟수	100번이하	—*	5번		—
공격자에게 모든 권리를 허용하는데 소요되는 최소시간	2초	—	5분	—	—
공격자에게 모든 권리를 허용하는데 소요되는 평균시간	2초	—	30분	—	—
공격자에게 모든 권리를 허용하는데 소요되는 최대시간	2초	—	60분	—	—

註 : — 는 적용할 수 없거나 해당사항이 없음.

통하여 바이러스 프로그램인 自己自身을 複製시켜 나가거나 또 情報를 저장중인 資源인 디스크(disk)나 디스켓(diskette)을 차례로 감염시켜 나가는 프로그램을 우리는 컴퓨터 바이러스라고 부른다.」

그러면 누가 이러한 「컴퓨터 바이러스」라는 말을 처음으로 사용하였을까?

컴퓨터 바이러스란 用語를 처음으로 紹介한 사람은 美國의 캘리포니아(Southern Califona) 대학의 프레드 코헨(Fred Cohen)교수이다. 그는 1983년 11월 미국의 한 컴퓨터 안전에 관한 세미나에서 "Computer Virus : theory and Experiment" 라는 논문에서 처음으로 컴퓨터 바이러스는 어떻게 동작할 수 있는가를 밝혔다. 그는 또 이사실을 1984년 캐나다의 토론토에서 열린 IFIPS (International Federation of Information Processing Societies : 국제정보처리학회)의 컴퓨터에 관한 세미나에서도 이내용을 발표하였다.

그 당시만 하더라도 대부분의 컴퓨터 保安전문가들은 컴퓨터 바이러스란 것이 재미있는 개념이기는 하지만 실제적으로 중요성은 별로 없을 것이라고 생각했었다.

그러나 1987年末에 러하이(Lehigh)대학에서 파괴적인 악성 바이러스의 出現이 보고되면서 그 중요성이 처음으로 일반에게 인식되었고 1988년부터 수많은 바이러스가 일반 사용자들에게 퍼지기 시작하면서 컴퓨터 바이러스를 새롭게 인식하기 시작하였다.

그리고 최근에는 미국이나 다른 선진국에서 컴퓨터 바이러스에 의한 피해가 심각한 문제로 대두되고 있으며 특히 國防이나 국가 기밀사항등을 처리하는 컴퓨터가 이러한 컴퓨터 바이러스에 감염된다면 컴퓨터시스템을 정지시키거나 주요한 정보를 수록한 화일을 완전히 지워버릴 수도 있으므로 이에 대한 위협이 대단히 심각하다고 하겠다.

그런데 세계적으로는 컴퓨터 바이러스와 비슷한 유형의 프로그램 종류가 약 200가지 이상 활동중인데 이들을 우리는 크게 몇가지 類型으로 분류하고 있다.

최근에 'Flu Shot plus'라는 그 유명한 백신(Vaccine) 프로그램을 만들어서 완성시킨 製作者 로스 그린버그(Ross Greenberg)는 'Computer virus myths'라는 글에서 惡性컴퓨터 프로그램을 대체로 3가지 종류로 分類하고 있다.

○ 트로이 木馬(Trojan horse) 프로그램

旣存의 유용한 프로그램 내부에 새로운 프로그램 몇 줄을 숨겨 놓아서 그 프로그램이 실행되면 사용자가 모르고있는 다른 기능을 시스템이 수행하도록 하는 프로그램이다.

이는 고대 그리스시대의 아가멤논 장군이 트로이城을 공격할때 木馬의 배속에 군사를 싣고 들여보내 트로이 城을 함락시켰다는데서 연유한 것으로서 부정한 목적의 프로그램이 마치 트로이 木馬속의 병정이 된 셈이다.

그러나 이 트로이 木馬프로그램은 숨겨진 내용의 기능만을 수행할 뿐 증식하지는 않으며 더구나 다른 프로그램에 複製시키는 기능은 없는 단순한 몇줄의 質이 나쁜 프로그램일 뿐이다.

○ 벌레(worm)프로그램

이 '벌레프로그램'은 컴퓨터 내의 다른 시스템에는 직접적인 영향을 미치지 않고, 단순히 기억장소내에서 自己自身을 계속 복사시키는 프로그램이다. 이것은 다른 시스템에 직접적인 영향을 미치지 않는다는 점에서 '트로이 木馬 프로그램'과는 다르며 다른 프로그램내에 포함되지 않는다는 점에서 '컴퓨터 바이러스'와도 틀리다.

컴퓨터 通信네트워크를 통하여 전파되는 벌레(worm)프로그램은 감염된 컴퓨터시스템에 過負荷를 걸어서 시스템이 정지되도록 한다. 벌레(worm)프로그램은 컴퓨터를 파괴시키지는 않으나 단순히 기억장소 內에서 자기자신을 계속 복사시키므로써 시스템의 活動을 정지시키기도 한다.

이 벌레(worm)프로그램은 스스로 作動(run)이 가능하며, 다른 컴퓨터 시스템으로 복사본을

전파할 수도 있는데 제록스(Xerox)社의 PARC (Palo Alto Research Center) 연구원들이 1970년대말에 실험적으로 제작하여 본 實例가 있었다.

실제로는 1970년대에 미국 국방성 네트워크중 「ARPANET」에 침입한 크리퍼(Ceeper)가 바로 벌레(worm)프로그램중에 대표적인 프로그램이다.

○ 컴퓨터 바이러스(Computer Virus)

컴퓨터 바이러스란 컴퓨터의 運營體制나 情報가 보관된 화일(file)을 變形시켜서 自身을 그곳에 포함시키는 複製形 프로그램을 말한다.

컴퓨터 바이러스는 앞에서 설명한 '트로이木馬' 프로그램의 특별한 형태로서 運營體制(OS)나 다른 프로그램內部에 자기자신을 감염시키는 質이 나쁜 프로그램이다. 이 컴퓨터 바이러스는 시스템에 직접적인 영향을 미친다는 점에서 벌레(worm) 프로그램과는 差異가 있음을 알 수가 있다.

로스 그린버그(Ross Greenberg)의 정의에 따르면 과거에는 막연히 컴퓨터 바이러스로 분류되던 여러종류의 質이 나쁜 프로그램들이 벌레(worm)프로그램이나 단순한 트로이木馬프로그램으로 分類될 수 있음을 알려 주었다.

컴퓨터 바이러스는 보통 널리 퍼질때까지 파괴행위를 하지 않는 것이 보통이며, 트로이木馬 프로그램中에는 이러한 전략을 사용하는 것들이 있다.

컴퓨터 바이러스가 파괴행위를 할 시점을 판단하는 논리에 따라 '時限폭탄(Time bomb)'과 '論理폭탄(Logic bomb)'으로 구분하는 사람들도 있다. '時限폭탄'을 일정한 날짜가 되면 파괴를 시작하는 것으로, 이에 속하는 유명한 바이러스는 '이스라엘 바이러스'가 있다. 이 바이러스는 이스라엘의 히브류(Hebrew)대학에서 발견되었는데 '88년 5월 13일(금요일)을 D-day로 하여 컴퓨터에 있는 모든 화일을 파괴하도록 하는 時限폭탄형이었다.

論理폭탄은 프로그램내에서 계산을 하다가 어떤 일정한 값에 도달하거나 또는 프로그램을 일정한 횟수만큼 사용하였을때 파괴를 시작하는 것으로 '러하이(Lehigh)바이러스'가 여기에 속한다.

1987년말 미국의 펜실바니아주 러하이대학에서 처음 발견되었는데 학생과 교수 대출용 디스켓(diskette)을 사정없이 손상시킨 것을 이대학의 컴퓨터사용자 고문인 케니스 반 · 윅(Kenneth R. van Wyk)이 발견하였다. 이 바이러스는 잠복기간이 상당히 길어서 일명 「피시 에이즈」(PC AIDS)라고도 불리우고 있다.

일반적으로 바이러스(virus)는 크게 良性(benign) 바이러스와 惡性(malignant, malicious) 바이러스로 나눈다.

1) 良性바이러스 : 데이타나 시스템을 파괴하지 않는 바이러스를 말한다. 이 바이러스는 보통 감염시킨 후에 自身의 존재를 알리는 메시지를 出力하는 것이 대부분이다. 그러나 이 바이러스도 불필요한 코드(code)를 시스템내에 증식시켜 컴퓨터 시스템의 처리속도를 저하시키며 사용가능한 메모리(memory)와 디스크(disc)의 空間을 줄인다. 다른 경우에는 시스템을 정지시키거나 데이타를 파괴하는 경우도 있다.

2) 惡性바이러스 : 데이타나 시스템을 파괴하는 바이러스를 말한다. 이런 악성바이러스로는 「Lbc」바이러스, 「Scores」바이러스, 변형 브레인 바이러스 등이 있다.

Ⅳ. 症　　狀

앞에서도 설명한바와 같이 컴퓨터 바이러스는 自己複製性(또는 自己增植性)과 不必要한 행위(보통은 誤動作과 運營體制의 破壞)를 한다고 했다.

그러면 컴퓨터 바이러스에 감염되면 어떤 현상이 나타나는가? 바이러스의 종류에 따라 여러가지 증상이 있을 수 있는데 대체로 다음과 같은 증상으로 설명할 수 있겠다.

① 바이러스 프로그램이 컴퓨터의 메모리(memory) 를 채운다.

바이러스는 일반적으로 자신을 계속 복제해 나간다. 따라서 디스켓 어딘가에 저장돼 있는 바이러스 코드는 컴퓨터의 메모리인 램(RAM : Random Access Memory)이나 보조기억장치인 디스켓의 사용 가능한 메모리의 量을 계속 줄여 나가게 된다. 이렇게 되면 컴퓨터 作動時 그 性能이 급격히 떨어지게 된다.

② 화일(file)의 크기나 內容을 변경시킨다.

디스크내에 있는 旣存의 화일을 액세스(access) 하여 크기나 內容을 일부 변경시키거나 기존의 화일에 붙어서 그 크기를 증가시키는 경우가 많다.

또 어떤 바이러스는 디스크 上의 화일의 일부를 파괴하거나 화일 전부를 지워버리는 경우도 있다.

③ 부트 레코드(boot record)를 바꾸거나 파괴한다.

컴퓨터를 처음으로 작동시키기 위해 읽혀드리는 명령어群(약간의 기계어)이 부트 레코드(boot record)이다. 이 부트레코드는 한 바이트(byte)만 수정해도 부팅(booting)이 않되도록 할 수가 있다. 부팅이 안되면 컴퓨터는 전혀 작동이 불가능하게 된다.

④ 화일저장주소(FAT)를 변경시키거나 파괴한다.

FAT(File Allocation Table)는 화일이 연결된 상태가 저장된 부분인데 이 테이블에 의해서만 화일이 보관된 주소를 알 수가 있다.

이 영역은 기계어 수준에서 읽고 쓰기 때문에 초보자들은 이곳을 건드리기 어렵다.

이 FAT가 변경되거나 파괴되면 컴퓨터내에 보관된 화일들을 읽어낼 수가 없으므로 컴퓨터 처리가 정상적으로 이루어 질리가 없다.

⑤ 디스크의 디렉토리(directory)를 바꾸거나 파괴한다.

디렉토리(directory)는 보조기억장치에 저장되어 있는 데이타화일과 프로그램화일들의 이름과 여러가지 특징들이 기록된 화일의 目錄이다. 예를들면, 마이크로 컴퓨터 사용자는 디스켓에 보관돼 있는 각종 화일을 검색하는데 디렉토리를 확인하면서 쉽게 찾아낼 수가 있는 것이다. 디렉토리는 결국 디스켓에 저장된 정보를 찾아 내도록 하는 索引 目錄이라고 보면 된다.

이 디렉토리가 변경되거나 파괴되면 컴퓨터를 이용하는 정보처리가 원만하지 못할 것은 당연한 이치다.

⑥ 디스크의 볼륨 라벨을 바꾼다.

디스크의 볼륨 라벨(Volume label)은 집주인

트랙	사이드	0									1								
	섹터	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9
0		IPL	FAT		FAT 의복사		디렉토리 (directory)				데이타 영역								
1		데이타 영역									데이타 영역								
2		데이타 영역									데이타 영역								
.		.									.								
.		.									.								
.		.									.								
39		데이타 영역									데이타 영역								

그림 MS-DOS 360 Kbyte형(5¼"2D) 플로피 디스크 배치(layout)

※IPL : Initial Program Loader, Bootstrap Loader

(시스템을 초기에 로드시키는 Boot record가 들어 있다)

을 알리는 문패와 같다. 문패를 바꿔 놓으면 우편 배달부가 엉뚱한 곳에 소포를 전달하게 될 것이 틀림없다. 이와같이 볼륨라벨을 변경하여 컴퓨터 작업을 혼란에 빠트리려는 전략이다.

⑦ 디스크의 특정 트랙(track) 혹은 전체 디스크를 포맷(format)한다.

포맷(format)이란 사용자가 정보내용을 단위별로 규정화하여 의미를 부여시키는 일이다. 그런데 컴퓨터 바이러스가 이일을 대신하여 사용자를 혼란에 빠뜨리는 경우가 있다.

⑧ 필요없는 메시지(message)를 出力한다.

컴퓨터를 사용해 업무를 처리하고 있는 도중에 필요없는 메시지가 出力된다면 이것도 역시 거리의 落書들 처럼 公害가 될 것이다. 그래도 이런 類의 컴퓨터 바이러스는 위에서 예를 든 증상에 비해서는 그래도 낭만적인 편이다.

⑨ 處理速度를 저하시킨다.

정상적으로 보관시킨 프로그램外에 追加的인 코드(컴퓨터 바이러스)가 부가됨으로써 처리속도를 저하시키게 된다.

⑩ 컴퓨터를 리셀(reset)시킨다.

컴퓨터를 作動시키려면 보통 2~3개의 키(Key)를 리셑시켜야 한다. 하지만 컴퓨터 바이러스는 몇개의 코드(code)로 이와 똑같은 기능을 수행해서 컴퓨터를 리셑(reset)시킬 수 있다.

⑪ 키(key)를 다시 정의한다.

컴퓨터는 사용자가 입력한 키보드의 신호로써 정보를 받아 들인다. 하지만 어떤 컴퓨터 바이러스는 입력 키보드를 재정의하여 사용자와 컴퓨터를 혼란에 빠뜨린다.

⑫ 키보드(key board)를 잠궈 버린다.

컴퓨터 바이러스가 키보드를 정의한 내용을 없애 버리면 컴퓨터 키보드로부터 사용자가 어떤 키를 입력해도 그 정보를 받아 들일 수가 없다.

지금까지 설명한 症狀외에도 디스크 드라이브(disk drive)를 공회전시킴으로써 디스크를 빨리 낡게 만든다든가, 또는 화일의 크기를 바꾼다든가, 램(RAM)에 상주하고 있는 프로그램의 실행을 중지시키며 심지어는 시스템을 아예 정지시켜 버리는 등 여러가지로 컴퓨터의 正常的인 動作을 방해하고 있다.

V. 種　　類

1983년 처음으로 컴퓨터 바이러스를 일반에게 소개할 때만 하드라도 일반인은 물론이고 컴퓨터 보안전문가마저도 재미있는 개념이긴 하지만 실제적으로 중요성은 별로 없을 것이라고 생각했었다. 그러나 1987년말부터 각종 컴퓨터 바이러스가 만연되고 있을 뿐만 아니라 더욱더 새롭고 강력한 바이러스가 탄생하고 있어 이에 대한 새로운 인식이 요구되고 있다.

그동안 발생했었던 컴퓨터 바이러스중 중요한 것을 발췌하여 간략히 소개하고자 한다.

(1) 러하이 바이러스(Lehigh Virus)

미국의 펜실바니아(Pensilvania)주에 위치하는 러하이 대학의 컴퓨터 센터에서는 도서관에서 册을 빌려 주듯이 학생들에게 프로그램 디스켓(diskette)을 대여해 주었다. 이러한 디스켓들은 학생들이 대학의 실험실 혹은 집에서 숙제를 하는데 주로 사용되었다. 1987년말에 이곳에서 근무하는 아르바이트 학생들은 많은 수의 디스켓이 손상된 상태로 반환된다는 사실을 발견했다. 이러한 디스켓들은 부팅(booting)이 되지 않았으며 디렉토리(directory)도 볼 수 없게 손상되어 있었다. 이와 비슷하게 대학실험실에서도 하드디스크(hard disk)들이 부팅되지 않고 데이타들도 복구될 수 없을 정도로 망가지는 일이 빈번해졌다. 이에 따라 대학의 컴퓨터 담당자인 케니스 밴 윅(kenneth van cyk)과 학생들은 컴퓨터센터에 남아있는 디스켓들을 자세히 조사하여 개인용 컴퓨터(PC)에 命令을 제어하는 시스템 프로그램(COMMAND. COM)에 300바이트(byte)정도의 바이러스 프로그램이 존재하고 있음을 확인하게 되었다.

참으로 놀라운 일이었다.

하지만 이때는 이미 컴퓨터 센터에 있는 수백장의 디스켓과 하드디스크(hard disk)와 학생 및 교수들이 가지고 있던 수 많은 디스켓들이 피해를 입은 후였다. 또한 인근에 있는 대학에서도 이 바이러스가 퍼져서 많은 피해를 입은 것을 알게 되었다.

이에 따라 케니스 밴 윅은 대학間 네크워크인 「BINET」에 컴퓨터 바이러스가 出現되었다는 경고 메시지를 띄웠고 백신 프로그램을 제작하기에 이르렀다. 이 백신(Vaccine)프로그램은 부팅될 때 시스템 프로그램(COMMAND. COM)을 검사하여 바이러스가 존재하면 이를 제거하는 형식으로 되어 있었다.

또한 이때부터 컴퓨터 센터의 貸出用 디스켓들은 학생들에게 쓰기방지 탭(write-protect tab)을 사용하도록 적극적으로 권장하였다.

러하이(Lehigh)바이러스는 최초로 발견된 惡性바이러스로 유명하며 최근에는 시스템 프로그램(COMMAND. COM)에 날짜를 바꾸지 않는 변형된 러하이 바이러스가 발견되어 많은 사람들의 주목을 끌고 있다.

(2) 브레인 바이러스(Brain Virus), 파키스탄 바이러스

브레인 바이러스가 一名 파키스탄(Pakistan) 바이러스라고 불리우는 이유는 이것을 만든 사람들이 파키스탄 사람들이기 때문이다.

26세의 앰자드 알비(Amjad Farooq Alvi)와 19세의 배시트 알비(Basit Farooq Alvi)가 바로 브레인 바이러스의 제작자들이다. 이들은 兄弟로서 파키스탄의 라허(Lahore)란 도시에서 중류층 집안에 태어났다. 兄인 앰자드는 대학에서 물리학을 전공한 후 독학으로 컴퓨터의 하드웨어와 프로그램 작성법을 익혔고, 처음에는 컴퓨터 修理를 전문으로 하다가 1985년경부터 프로그래머로 직업을 전환하였다.

하지만 앰자드는 自身이 작성한 프로그램이 함부로 不法複製되어 유통되는 것을 알고 이때부터 그는 이를 보복할 수 있는 방법을 찾기 시작했다고 한다. 파키스탄에서는 그 당시 프로그램에 대한 著作權을 법적으로 보호받지 못했기 때문이다.

그후 이들 형제는 'Brain computer store'라는 컴퓨터 가게를 만들어 자기들이 만든 프로그램을 팔고 로터스(Lotus) 123과 같은 미국의 프로그램들을 1달러50센트에 복사해 주는 장사를 시작하였다. 이때가 1986년 초이다.

이들은 파키스탄 사람이 프로그램을 복사해 갈때는 원본 그대로를 복사해 주고, 外國人이 프로그램을 복사해 갈때는 몰래 바이러스 프로그램을 같이 넣어 주었다고 한다. 이들이 이렇게 한 이유는 파키스탄 인들은 法的으로 프로그램을 복사해도 불법이 아니지만, 미국사람들은 불법인 줄 뻔히 알면서도 프로그램을 복사해 가는 것이기 때문에 처벌을 받아야 한다는 이상한 論理에서 비롯되었다고 한다. 이렇게 몰래 복사해 준 바이러스 프로그램이 미국의 덜러웨이(Delaware) 대학에서 처음으로 발견되어 보고되었고 죠지 워싱턴 대학에서도 1만장 정도의 디스켓이 감염되었다고 한다. 이 바이러스 이름은 알비형제가 운영하던 가게이름과 같이 "브레인 바이러스"라고 부르게 되었다.

그후에도 피츠버그대학, 죠지타운대학, 펜실바니아대학, 마이아미대학등에서도 발견되었으며 미국 전체에 최소한 10만장이상은 이 브레인바이러스에 감염된 것으로 推算되고 있다.

1987년말에 알비형제는 프로그램을 불법복사하는 사람들에게 충분한 교훈을 주었다고 생각하고 바이러스 프로그램을 퍼뜨리는 일을 중지하였다고 한다.

이브레인 바이러스는 우리나라에도 상륙하여 사회적인 문제로 대두되어 세운상가 컴퓨터업자등 개인용컴퓨터(PC)사용자에게 경각심을 높여주었다. 우리나라 신문들은 이 바이러스를 (C)브레인이라고 소개하였기 때문인지 국내에서는 계속 '(C)브레인 바이러스'라고 부르고 있는 것 같다.

이 브레인 바이러스는 한 종류만 있는 것이 아니라 조금씩 다른 세가지 종류의 變型바이러스가 존재한다고 알려져 있다.

보통의 브레인 바이러스는 볼륨 라벨(Volume label)을 '(C) brain'이라고 바꾸지만 펜실바니아 대학에서 발견된 브레인 바이러스는 볼륨라벨을 'Ashar'로 바꾸며, 또 'Bufued'라고 바꾸는 것도 보고되었다.

이 브레인 바이러스는 부트 레코드(boot record) 를 감염시키고 불량 클러스터(Cluster)를 만든 후, 거기에 바이러스 프로그램을 상주시킨다. 최근에는 변형된 브레인 바이러스가 무척 많이 발견되고 있다.

(3) 히브류 바이러스(Hebrew Virus)

이스라엘의 히브류대학에서 발견되었기 때문에 '히브류 바이러스', '이스라엘 바이러스' 또는 '13일의 金曜日바이러스', '예루살렘 바이러스'라고 부르기도 한다.

1988년초 이스라엘의 히브류(Hebrew)대학에서는 매주 금요일과 매달 13일마다 컴퓨터 시스템들의 동작이 눈에 띄게 둔화되고 있으며 디스크의 사용가능영역이 줄어드는 등의 현상이 발생하였다. 이러한 일이 빈번해지자 대학의 컴퓨터 프로그래머인 이스라엘 라대(Yisrael Radai)는 이러한 현상의 원인을 조사하기 시작했다. 이틀 동안 시스템을 조사한 후 그는 바이러스 프로그램의 존재를 확인할 수 있게 되었다.

그 바이러스는 매주 금요일과 매달 13일이 되면 기억장소내에서 증식하여 시스템의 처리속도를 떨어뜨리고 시스템內의 디스크들을 감염시키는 코드(code)를 가지고 있었고, 끔찍하게도 이스라엘의 독립 40주년 기념일인 1988년 5월 13일에 컴퓨터시스템內의 모든 화일(file)을 지워버리는 코드(命令語)를 가지고 있었다.

이 당시에는 벌써 대학내의 1,000여대의 컴퓨터와 많은 교수, 학생들의 디스크가 감염되어 있었으므로 대학의 컴퓨터 센터는 非常이 걸렸고, 많은 사람들의 노력으로 5월 13일 이전에 겨우 이 바이러스를 제거할 수 있었다.

이 히브류바이러스를 발견하여 제거할 수 있었던 이유는 바이러스 제작자의 실수때문인 것으로, 한번만 감염시키고 잠복하고 있었다면 발견하기가 쉽지 않았을텐데 계속적으로 감염시킴으로써 기억장소와 디스크 사용영역이 눈에 띄게 줄어들었기 때문이다.

히브류대학의 바이러스는 그 성격상 時限폭탄(time bomb)이라는 별명으로도 많이 불리우며 그후로는 이 惡性바이러스가 또 出現되었다는 보고는 없었다.

히브류 바이러스에 감염되면 'EXE'화일은 1808바이트, 'COM' 화일은 1813바이트씩 증가한다. 또한 한번 감염된 화일에도 계속 감염되기 때문에 심한 경우에는 시스템 메모리(system memory)에 로드(load)가 되지 않는다. 그리고 컴퓨터 수행속도를 최고 1/5까지로 떨어 뜨리는 경우가 있다.

러하이 바이러스나 브레인 바이러스는 시스템 프로그램인 운영체제(Operating System)에 감염되지만 히브류 바이러스는 실행화일(Execution file)에 감염되는 것이 서로 다르다.

(4) 버클리 유닉스(Berkeley Unix) 바이러스

1988년 11월 2일과 3일사이에 미국 국방성의 주요 네트워크인 「ARPANET」, 「Milinet」와 「NSF(National Science Foundation)Net」로 침범해 들어가서 핵무기 연구기관인 로렌스 리버모어 연구소, NASA, MIT, 하바드 대학, 스탠포드대학 및 코넬대학 등으로 확산되어 네트워크에 연결된 컴퓨터의 10%가량인 6천대의 컴퓨터를 감염시켰다.

이 바이러스는 유닉스중 버클리 버전(Berkeley version)에만 감염이 되며, 유닉스 보안시스템의 허점을 교묘히 이용해서 전자사서함을 통해 다른 시스템을 감염시켜 나갔다.

또한 이 바이러스 프로그램은 자기 자신을 암호화시켜 저장하고 있다가 수행시에만 한줄씩 암호를 풀어 실행하게 되어 있었다고 한다.

이 바이러스가 기존의 바이러스와 다른 점은, 사용자의 컴퓨터 사용여부와는 관계없이 자기 스스로 증식한다는 점이다.

이 바이러스를 제거하기 위하여 이들 네트워크에 연결된 수많은 컴퓨터들이 폐쇄됨에 따라

국방부 및 연구소들은 막대한 피해를 입었다고 한다. 다행히 이 바이러스는 良性(benign)이었기 때문에 더 이상의 피해는 입지 않았으며 11월 5일 경에는 거의 제거되었다.

특히 다행인 것은 국방부의 일급 비밀을 다루고 있는 컴퓨터는 그당시 이 바이러스로부터 침입을 받지 않았다고 전한다. 이사건 이후 「NSF」(National Science Foundation)에서는 전자사서함을 수정해서 더 이상 이런 종류의 바이러스가 시스템에 침입하지 못하도록 조치를 취했다.

이 바이러스 제작자는 당시 23세의 코넬 대학교 전산학과 대학원생인 로버트 모리스(Robert T.Morris)로 밝혀졌다.

한가지 아이러니칼한 것은 모리스의 아버지가 「NSF」의 국립컴퓨터 보안센터 책임자라는 사실이다.

이바이러스가 발견된 이유는 프로그래밍상 에러(error) 때문으로, 너무 빨리 自己複製를 시도한 나머지 시스템의 속도를 크게 떨어 뜨려서 시스템 관리자에게 쉽게 발각되었기 때문이다.

한 관계자는 이 바이러스의 잠복기가 조금만 길었드라도 아마 쉽게 발견되기는 힘들었을 것이라면서 최근 컴퓨터 바이러스의 피해에 대해서 상당한 우려를 표명하였다.

이 바이러스는 유닉스 화일중 디렉토리(directory) 에 이상한 화일을 생성시키며 전자사서함의 「log File」에 이상한 메시지를 생성시키면서 시스템이 이 바이러스에 감염되면 시스템처리속도가 급격히 늦어지는 현상을 유발시킨다.

이 버클리 유닉스 바이러스를 제작한 모리스(Morris)는 재판에 회부되어 5년의 금고형을 언도 받았다. (단지 그는 자신의 컴퓨터 실력이 남들보다 훌륭하다는 것을 자랑하기 위해서 이런 프로그램을 만들었다고 한다.)

로스 그린버그(Ross Green berg)의 정의에 따르면 이 바이러스는 인터네트 벌레프로그램(Internet worm)이라고 분류된다.

(5) 엘비시 바이러스(Lbc Virus)

출처가 알려지지 않은 이 바이러스 프로그램은 브레인 바이러스와 함께 우리나라에 가장 많이 퍼져있다

「하드 디스크 귀신」이라고 불리는 엘비시(Lbc) 바이러스는 하드 디스크(hard disk)에 잠복, 밖으로 드러나지 않고 있다가 디스켓을 부팅(booting)하는 순간 하드 디스크에 저장된 정보를 전부 못쓰게 하는 惡性(malignant)바이러스다.

소련산 게임용 소프트웨어 「테트리스」를 통해 전염되고 있는 것으로 알려진 엘비시바이러스는 개발자나 유통경로등이 전혀 밝혀져 있지 않을 뿐만 아니라 그 피해 정도가 매우 커 컴퓨터 사용자들을 긴장시키고 있다. 이미 설명한 것처럼 이 바이러스는 가공할 파괴력을 가지고 있으므로 특히 행정 전산망을 비롯해서 5대 국가기간전산망이 구축된 후 이것이 공격을 가한다면 심각한 사회문제로 비화될 가능성이 있음을 인식하고 우리는 이에 대비하여야 한다.

이 바이러스는 브레인 바이러스 코드를 再구성하여 만든 것이지만 브레인바이러스와는 달리 하드 디스크에 分割表(Partition Table)를 포함하고 있는 主부트 섹터(Master Boot Sector) 와 「FAT」(File Allocation Tabel)를 파괴하여, 하드 디스크가 부팅되지 않음은 물론 인식도 되지 않도록 하여 화일도 복구하기 힘들게 만든다.

하지만 5 ¼인치 플로피 디스크에서는 부트 섹터에 기생하며 루트 디렉토리(root directory)의 가장 마지막 섹터를 파괴하기 때문에 화일의 수가 아주 많은 경우를 제외하고는 데이타를 파괴하지 않는다. 최근 국내 개인용 컴퓨터(PC) 사용자의 하드 디스크(HDD)에 가장 많이 발생하고 있다.

지금까지 소개한 바이러스 外에도 일일이 열거하기 어려울 정도로 많은 컴퓨터 바이러스가 있지만 여기에서는 별표와 같이 일부 代表的인 바이러스名만 소개하기로 한다.

바이러스(VIRUS)의 종류

- ○ 러하이 바이러스(Lehigh Virus)
- ○ 브레인 바이러스(Brain Virus, Pakistani Virus)
- ○ 히브류 바이러스(Hebrew University Virus, Israeli Virus, Black Friday Virus, Jerusalem Virus)
- ○ 버클리 유닉스 바이러스(Berkeley Unix Virus)
- ○ 엘비시 바이러스(Lbc Virus)
- ○ 일요일 바이러스(Sunday Virus)
- ○ 스코러 바이러스(Scores Virus, Macintosh Virus)
- ○ 크리스마스 메시지 바이러스(IBM Christmas Tree Virus)
- ○ 스톤 바이러스(Stoned Virus)
- ○ Flu-shot 4 Virus
- ○ 아미가 바이러스(Amiga Virus)
- ○ Alameda Virus
- ○ nVIR Virus

etc

Ⅵ. 豫防法

바이러스의 종류와 기법은 날로 다양하고 高度化되고 있으므로 모든 바이러스에 대한 根本的인 예방책은 현재로서 어떤것도 완벽하다고 말할 수 없겠다. 다만 바이러스가 발견되면 찾아내서 고치는 수밖에는 없다. 그래서 궁여지책으로 자료가 들어 있는 디스켓을 백업(back-up)하는 것 이외에는 모두 안전하지 못하다는 점에 留意하여야 한다.

어떠한 바이러스 프로그램이 만연되어 이에 대한 새로운 백신 프로그램(Vaccime program)이 만들어져 사용된다 할지라도 얼마 안되어 또 누군가가 다른 바이러스를 만들어 낼 것이기 때문에 각 바이러스에 대한 백신 프로그램개발은 지극히 비효율적이며 소모전에 불과할 것이다.

하여튼간에 바이러스에 대한 피해를 막기 위한 몇가지 방법을 소개하기로 하자.

① 중요한 데이타는 반드시 백업(BACK-UP)해 둔다.

② 운영체제가 있는 디스켓(DOS)원본은 반드시 백업(BACk-UP)을 하며 쓰기(Write)방지 탭을 붙여 놓는다.

③ 새로운 디스켓은 대리점이나 믿을 만한 업체에서 구입한다.

④ 새로 구입한 디스켓이나 프로그램은 즉시 바이러스 감염여부를 테스트해 본다.

⑤ 새로운 프로그램에 대한 테스트는 하드디스크(hard disk)가 없는 시스템에서 실시한다.

⑥ 새로 구입한 디스켓은 백업(back-up)을 해서 안전한 장소에 보관한다.

⑦ 화일 비교 프로그램을 이용하여 백업하여 둔 화일과 사용하고 있는 화일에 차이점이 생겼는지 정기적으로 검사한다.

⑧ 만약 바이러스 검사 프로그램이 있다면 이것을 이용하는 것이 좋다.

⑨ 무료로 제공되는 소프트웨어나 무단복제

프로그램은 가능한한 사용하지 않는다.

⑩ 명령을 제어하는 시스템 프로그램(COMMAND. COM)을 읽기 專用으로 만들어 놓으면 상당수의 바이러스 침투를 방어할 수 있다.

⑪ 화일 단위로 전염되는 바이러스 프로그램은 플러샷 플러스(FLU SHOT PLUS)와 같은 백신 프로그램(Vaccine program)을 사용하는 것이 좋다.

Ⅶ. 結　　言

현재 시중에서는 몇가지의 백신프로그램(Vaccine program)들이 판매되고 있다. 이들 백신 프로그램의 기능은 바이러스를 豫防하거나 診斷하거나 治療하는 기능을 갖는 것으로 나눌 수 있다. 하지만 이들 백신 프로그램을 사용할 때 한가지 유의할 점은 백신 프로그램을 너무 믿어서는 안된다는 것이다.

바이러스는 컴퓨터의 여러가지 부분을 다양한 전략을 사용하여 침입하기 때문에 어떤 한두가지 가정에 근거하여 작성한 백신프로그램이 모든 바이러스에 대하여 효과가 있으리라고 생각할 수는 없기 때문이다.

일찌기 미국 신시내티(Cincinnati)대학의 프레드 코헨(Cohen)교수도 일정시간 동안에 컴퓨터 바이러스의 감염여부를 알 수 있는 백신프로그램을 만드는 것은 불가능하다는 것을 수학적으로 증명했다고 한다.

또한 백신프로그램이 모든 바이러스 프로그램에 만병통치가 아니라는 것을 이해하여야 하며 앞으로 발생되어질 가공할 바이러스 쇼크(Shock) 에 어떻게 대처하는 것이 좋을지 우리모두 人智를 모아야 할 때 라고 생각한다.

지금까지 제작된 백신프로그램(Vaccine program)의 種類와 기능소개는 紙面관계상 後日로 미루기로 한다.

참 고 문 헌

· 안철수(서울의대 생리학교실),
"컴퓨터바이러스 블랙리스트",
– 마이크로 소프트웨어, 1989. 6월호
page 88~93.
"컴퓨터바이러스의 현주소를 찾아서",
– 마이크로 소프트웨어, 1989. 1월호
page 130~144
"(C) Brain의 분석과 대책",
– 마이크로 소프트웨어 1988. 7월호
page 52~67
"브레인 바이러스와 LBC바이러스 퇴치프로그램",
– 마이크로 소프트웨어 1989.11월호
page 214~224
· 최철용(부산 유일컴퓨터)
"바이러스 예방주사",
– 마이크로 소프트웨어 1988. 7월호
page 68~73
· 안철수(단국대 의대 생리학교실 전임강사)
"예루살렘 바이러스퇴치기능이 추가된 백신Ⅱ PLUS", – 마이크로 소프트웨어 1989.12월호
Page 282~284
· Ross Greenburg(byte誌, 컬럼니스트)
"바이러스 해부 퍼레이드",
(Know Thy Viral Enemy)
– Computer magazine July 1989.
page 66~73
· 김한수(한양대 HY–CORA)
"브레인 변형 바이러스와 하드 디스크의 예방 및 데이타의 복구방법",
– Computer magazine october 1989.
page 157~164
· 한근희(KIST 시스템공학센터 교육연구망실)
"Software Virus–New Computer Crisis",
"Computer Network에서의 Virus",
· 정승민(아주대 수학과)
"컴퓨터 바이러스 백서",
– 퍼스널 컴퓨터 1990. 2
page 149~182
· 한근희(KIST 시스템공학센터 교육연구망)
"컴퓨터 바이러스",
· 김세헌(KAIST 경영과학과 교수)
"컴퓨터 바이러스 피해현황과 시스템보안대책",
– 정보산업 1988. 9월호
page 4~6
· 정건수(기자)
"컴퓨터 바이러스 갈수록 심각",
– 한국경제신문 1988.11. 3일자 8면

· 금기현(기자)
"컴퓨터 바이러스 초비상",
— 전자시보 1988. 7.21자.
· 김세헌(KAIST 경영과학과 교수)
"컴퓨터 바이러스 : 현황과 대책",
— 경영과 컴퓨터 1988.10월호
page 180~182
· 삼보컴퓨터 편집자.
"컴퓨터 바이러스",
· 이기성(동국대 정보산업대학원 교수)
"정보화시대의 골칫거리, 컴퓨터 바이러스",
— 企業經營, 1990. 2월호
page 81~86
· 김범룡(정부전자계산소 전산처리관)
"컴퓨터 바이러스 피해현황과 대책",
— 행정과 전산 1988.12월호 Vol.10 No.4
page 135~137
· 김한수(프로그래머)
"당신의 하드디스크는 안전합니까?",
— 매경 PC저널 '89.10
page 32~45

1990年度 技術士補修教育案内

國家技術資格法 第4條의 3 및 同法施行令 第12條의 2의 規定에 依한 1990年度 技術士補修教育을 아래와 같이 實施하오니 錯誤없으시기 바랍니다.(1989年 12月 9日字 서울신문 公告)

—아 래—

1. 補修教育 對象者 : 1) 1985年度 技術士資格取得登錄者
2) 1985年度 補修教育履修後 同年度에 更新登錄者
3) 1985年度 以前 資格取得登錄者로서 當該年度 補修教育 未履修者
2. 補修教育 對象種目및 教育機關

對 象 種 目	教育機關(電話番號)	受講申請期間	教育期間
安全管理技術士 (消防設備)	韓國消防安全協會 (634—5801)	'90. 5. 1~5. 31	5月~8月사이 실시(일자미정)
國土開發技術士 (測 地)	大韓測量協會 (671—8939, 0921)	'90. 5. 1~5. 31	6月末(論文提出)
土木技術士(施 工) 建築技術士(施 工) 機械技術士(建設機械)	建設技術教育院 (032—423—4901 435—4901~3)	'90. 2. 5~3. 17	建設業法 및 建設技術管理法: 10. 22부터 2週間,國家技術資格 法:5. 31~6. 1(2日間)
技術士 全種目 (土木施工, 建築施工, 建設機械, 地域 및 都市計劃, 造景, 測地, 産業衛生管 理, 가스 除外)	韓國技術士會 (566—5875, 557—1352)	'90. 5. 1~5. 31	7. 12~7. 13(2일간)

* 1) 其他 자세한 事項은 當該 教育機關으로 問議하시기 바랍니다.
2) 各 教育機關別 受講申請期間內에 受講申請을 畢하여야만 教育에 參加할 수 있으므로 留意하시기 바랍니다.