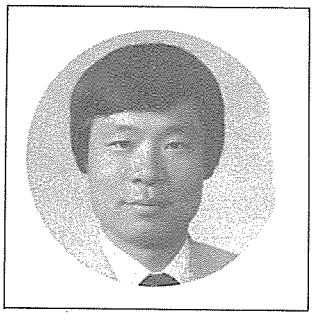
컴퓨터바이러스의 대처방안

效率的 검사와 처방 方法의 개발 시급



김 세 헌

〈韓國과학기술원 經營科學科교수〉

정보화시대에서 중요한 역할을 차지하고 있는 컴퓨터가 현재 바이러스의 위협을 받고 있다. 중요하고 가치있는 데이타가 대부분 화일속에 저장되어 있는 시스템에 있어서 데이타를 파괴하는 기능을 가진 바이러스의 등장은 매우 심각한 문제로 제기되고 있다. 현재 계속해서 바이러스의 종류가 늘어나 외국에서는 80여 종류의 바이러스가 존재한다는 것이 밝혀졌고 이 숫자는 계속해서 늘어날 전망이다. 우리나라도 현재까지는 그 종류가 그다지 많지 않지만 계속해서 늘어나고 있는 추세에 있으므로 이를 효율적으로 대처하는 방법이 필요하다.

여기서는 바이러스의 일반적인 성질을 개략적으로 살펴보고 이를 통해 컴퓨터 바이러스를 예방하는 방법과 이를 처방하는 방법을 살펴본다.

컴퓨터 바이러스의 성질

"컴퓨터 바이러스는 자신의 바이러스 프로그램을 다른 정상 프로그램에 주입함으로써 그 프로그램을 다시 바이러스가 되게 만드는 프로그램이다."

컴퓨터 바이러스는 기능적으로 두가지 특징을 가진다. 첫째로는 자기 복제기능으로서 자신의 바이러스 프로그램을 다른 프로그램에 계속해서 번식시켜 나간다. 둘째로는 어떤 조건이 만족되면 손상기능이 작동하여 시스템이나 화일에 손상을 가하는 특징을 가진다.

정상적인 프로그램이 컴퓨터 바이러스에 감염되는 절차는 〈그림-1〉과 같다.

제작자는 바이러스 프로그램을 포함시킨 프로그램을 만든다. 일반 사용자가 이 프로그램을 사용하면 바이러스 프로그램이 작동하여 컴퓨터 시스템(주기억장치)을 감염시킨다. 이후에 일반 사용자가 감염안된 다른 프로그램을 수행하게 되면 시스템에 있는 바이러스는 자신의 바이러스 프로그램을 이 프로그램에 주입시켜 바이러스로 만든

이 글은 박정근(한국과학기술원 경영학과 석사과정)씨와 공동집필임. ····· 〈편집자 註〉

후에 사용자가 내린 명령을 행한다. 따라서 사용자는 정상적인 명령을 행한 것으로 인식하여 자신의 화일이 바이러스에 감염되었는지를 깨닫지 못한다.

컴퓨터 바이러스는 감염시키는 부분에 따라 분류하면 크게 2종류로 구별할 수 있다. 즉 컴퓨터가 부팅될 때 사용되는 디스크의 부트섹터를 감염시키는 바이러스와 수행 화일(확장자가 EXE or COM)을 감염시키는 바이러스로 나누어진다.

컴퓨터 바이러스 프로그램의 구성은 시스템을 감염시키는 부분과 화일이나 디스크를 감염시키는 부분으로 나누어진다. 화일이나 디스크를 감염시키는 부분은 다시 3가지 부분으로 나누어진다. 첫째로 바이러스의 감염여부를 체크하는 부분이고 둘째로 자신의 바이러스 프로그램을 감염안된 프로그램에 복제하는 부분이고 마지막으로 여러 종류의 손상을 입히는 기능을 가진 부분이다.

바이러스가 포함되어 있는 프로그램을 수행하면 시스템을 감염시키는 부분이 작동한다. 메모리의 크기를 감소시키고 이 부분에 바이러스 프로그램을 옮겨놓아 바이러스 프로그램을 메모리에 상주하는 프로그램을 만든다. 그리고나서 정상적인 명령을 행한다. 이후에 감염안된 프로그램을 수행하게 되면 메모리에 있는 화일을 감염시키는 부분이 작동한다. 우선 이 화일이 바이러스에 감염되었는지를 체크하여 감염이 안되었으면 감염을 시킨다. 그리고 조건이 만족되면 손상시키는 서브루틴을 사용하여 화일이나 디스크를 손상시킨다.

컴퓨터 바이러스의 예방대책

컴퓨터 바이러스는 사용자가 화일을 다음과 같이 적절히 관리함으로써 예방할 수 있다.

① 부팅하는 디스켓을 따로 지정하는 것이 좋다.

(C) Brain 또는 LBC 바이러스는 부팅할 경우 바이러스가 주기억장치를 감염시키므로 부팅하는 디스켓을 따로 준비하여 그 디스켓으로만 부팅을 하면 부팅시 작동하는 바이러스를 예방할 수 있다. 만약 하드디스크가 있는 경우 부팅은 하드디스크로만 하는 것이 좋다.

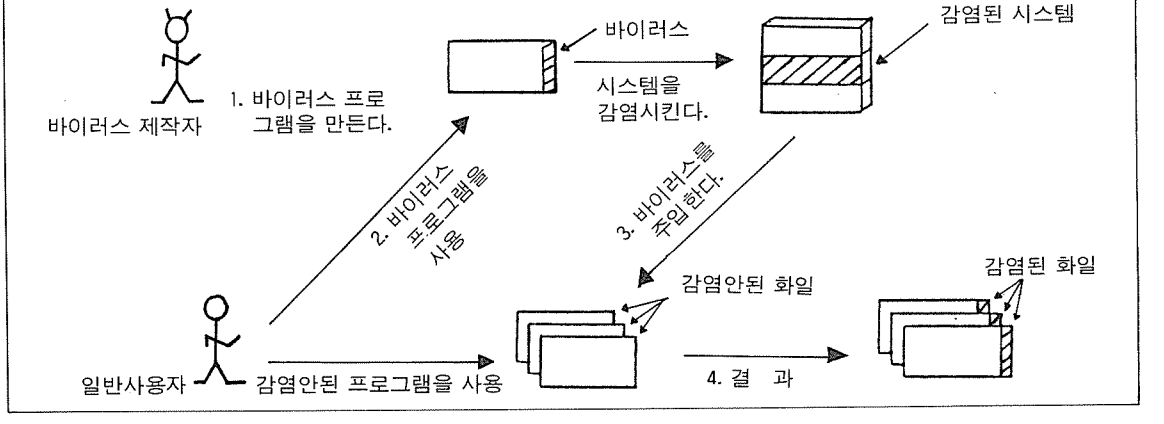
② 수행화일(확장자가 EXE or COM)을 읽기전용(Read-Only)으로 하면 수행화일을 감염시키는 바이러스를 예방할 수 있다.

읽기전용은 노턴 유틸리티를 이용하여 쉽게 만들 수 있다. 예로 LOTUS.EXE 화일을 읽기전용으로 하려면 아래와 같은 명령을 수행하면 된다.

C>FA LOTUS.EXE/R+

다른 방법으로는 수행화일과 데이타화일을 각각 다른 디스크에 보관함으로써 바이러스를 예방할 수 있다. 일반적으로 바이러스는 수행화일만을 감염시키고 데이타화일은 감염시키지 않으므로 수행화일만을 보관하고 있는 디스크에는 쓰기금지장치(Write Protector)를 하여 읽기전용으로 한

〈그림-1〉 컴퓨터 바이러스 감염절차



다.

③ 외부로부터 복사해온 디스켓은 우선 바이러스의 감염여부를 체크한 후 사용한다.

컴퓨터 바이러스를 체크하는 데에는 여러가지 방법이 있다. 첫째로, PCTOOL 또는 NORTON UTILITY를 이용하여 바이러스 프로그램에 있는 메시지를 알아내는 방법이 있고, 둘째로는 SCAN 프로그램으로 바이러스의 감염여부를 알아낼 수 있다.

컴퓨터 바이러스의 처방

디스크나 화일이 바이러스에 감염되었을 경우 이를 원래의 상태로 복구하는 방법이 필요하다. 이 장에서는 바이러스의 감염여부를 체크하고 감염된 경우 복구하는 방법을 설명하겠다.

바이러스 감염여부 체크

바이러스의 감염여부를 체크하는 팩키지로는 VIRUSCAN이 가장 널리 사용되고 있다. 이 프로그램으로 현재까지 73종류의 바이러스를 알아낼 수 있다. VIRUSCAN을 작동하기 위해서는 다음의 명령을 행한다.

SCAN d1: d2: ...dn: [/M /D /A /E [EXTENTION LIST] /nomem /many]

d1-dn : 드라이브 번호
/D : 감염된 화일을 자동적으로 지움
/M : 주기억장치를 체크
/A : 체크할 디스크의 모든 화일을 검색
/E : 리스트된 오버레이 화일들을 검색
/nomem : 주기억장치 검사를 생략할 경우
/many : 다수의 플로피를 검사하는 경우

예를 들어, A디스크의 TURBO디렉토리에 있는 TURBO.EXE를 검사할 때에는 다음과 같이 입력한다.

C>SCAN A:\TURBO5\TURBO.EXE

위의 팩키지를 이용하지 않고 쉽게 바이러스를 검사할 수도 있다. 미리 화일의 길이와 날짜를 메모하였다가 수행하려는 화일의 그것과 비교한다. 대부분의 바이러스는 바이러스에 감염되면 화일의 길이가 증가하거나 날짜를 바꾸는 성질을 가진다.

바이러스 프로그램을 제거하는 방법

앞에서 살펴본 바와 같이 바이러스는 주기억장치와 디스크를 감염시킨다. 주기억장치가 감염된 경우 시스템의 성질상 컴퓨터를 OFF시키면 바이러스는 주기억장치에서 사라지게 된다. 그러나 디스크가 감염된 경우는 계속해서 남아있게 되므로 이를 제거하는 방법이 필요하다. 여기서는 CLEAN- UP 팩키지를 소개한다.

CLEAN d1: d2: ...dn: [바이러스명] /a /many
/a : 모든 화일을 체크하는 경우
/many : 다수의 플로피디스크에서 바이러스를 제거하는 경우

우선 이 프로그램을 사용하기 위해서는 앞의 SCAN 프로그램을 사용하여 어떤 바이러스에 감염되었는지를 확인한 후 사용한다. 예를 들어 A디스크가 예루살렘 바이러스에 감염되었다면 다음과 같이 입력한다.

C>CLEAN A: [JERU]

이외에도 국내에 유행하는 바이러스를 검사하고 치료할 수 있는 V2PLUS가 있고 메모리에 상주시켜 바이러스의 감염을 예방할 수 있는 FLU-SHOT+ SCANRES 프로그램 등이 있다.

이러한 팩키지가 없는 경우에는 수행화일 들에 대해 미리 백업화일을 만들고 쓰기금지장치를 한다. 만약 화일이 바이러스에 감염된 경우 이 화일을 지우고 미리 갖고 있던 백업화일을 다시 복사하여 사용하면 바이러스를 제거할 수 있다.

결 론

앞에서 컴퓨터 바이러스를 예방하는 방법과 처방하는 방법을 살펴보았다. 그러나 위의 방법이 모든 바이러스에 효율적인 것은 아니다. 위에서 제시한 바이러스 검사방법과 처방하는 방법은 신종 바이러스에는 효과적이지 못하다. 앞으로의 연구는 신종 바이러스도 효율적으로 검사하고 처방하는 방법을 개발하는 것이 필요하다.