컴퓨터 바이러스 현황과 대책

안철수 대표(안철수컴퓨터바이러스연구소)

이전에는 주로 플로피 디스켓을 통하여 부분적으로 바이러스가 전파되었으나, 네트웍 구축과 인터넷 이용이 보편화한 후에는 감염되는 속도가 매우 빠르고, 피해 범위도 훨씬 광범위해졌다. 정보화 시대가 주는 당근과 채찍, 빛과 그림자, 순기능과 역기능인 셈이다.

컴퓨터 바이러스는 컴퓨터가 있는 곳이면 어느 곳에서나 문제가 될 수 있고, 특히 컴퓨터 활용도가 높은 전자산업 분야의 경우 문제가 더욱 커질 수 있다.

■ 바이러스 정의

컴퓨터 바이러스는 일종의 프로그램으로 다른 프로그램들과 달리 사용자 몰래 자신을 다른 곳에 복사하는 명령어를 가지고 있다.

바이러스라는 이름이 붙은 이유는 생물학적인 바이러스가 자신을 복제하는 유전인자를 가지고 있는 것처럼 컴퓨터 바이러스도 자신을 복사하는 명령어들을 가지고 있기 때문이다.

따라서 컴퓨터 바이러스라는 말보다는 바이러스 프로그램이라는 말이 더 정확한 표현이다.

또한 컴퓨터 바이러스는 자기 복제 능력 외에도 실제 바이러스와 같이 부작용(side effect)를 가지고 있는 경우가 많다.

이러한 부작용은 컴퓨터를 느리게 하는 경우도 있지만 때로는 파일에 손상을 주거나 하드 자체를 사용하지 못하도록 하는 경우도 있다.

즉 감기를 생각해 보면 내가 걸리면 내 주변에 많은 사람들이 감기에 걸릴 수 있듯이 컴퓨터 바이러스를 컴퓨터 세계의 감기라고 생각하면 된다.

하나의 컴퓨터가 바이러스에 걸리면 그 컴퓨터와 통신이나 자료를 주고받는, 즉 대화를 하는 다른 컴퓨터도 감기에 걸릴 확률이 높다.

감기에도 목감기, 기침감기 등 여러 가지가 있듯이 컴퓨터 바이러스에도 단지 감염만 시키는 경우도 있고 자료를 파괴하는 경우도 있고 더 나아가서 컴퓨터 하드웨어 자체에 손상을 주는 바이러스도 있다.

■ 바이러스 분류

컴퓨터 바이러스는 크게 4가지로 구분할 수 있다. 부트영역에 감염되는 부트 바이러스와 파일에 감염되는 파일 바이러스, 그리고 부트와 파일에 모두 감염되는 부트/파일 바이러스 그리고 최근 발견된 엑셀, 워드 등에서 사용되는 매크로를 통하여 감염되는 매크로 바이러스가 있다.

· 부트 바이러스(Boot virus)

컴퓨터를 처음 켰을 때 디스크의 가장 처음 부분인 부트 섹터(Boot Sector)에 위치하는 프로그램이 가장 먼저 실행되는데, 이곳에 자리잡는 컴퓨터 바이러스를 부트 바이러스라고 한다. 예로는 국내 최초로 88년에 발견된 바이러스인 뇌(Brain) 바이러스가 있으며 이후 발견된 미켈란젤로(Micahelangelo),

LBC, 양파 및 지금까지도 많은 피해를 주고 있는 원숭이 바이러스 및 감염 빈도가 높은 Anti-CMOS 바이러스 등을 들 수 있다.

· 파일 바이러스(File virus)

파일 바이러스란 일반적인 프로그램에 감염되는 컴퓨터 바이러스를 말한다. 이때 감염되는 프로그램은 COM 파일, EXE 파일 등의 실행 파일 및 오버레이(Overlay) 파일, 그리고 주변기기 구동 프로그램(Device driver) 등이며 현재 컴퓨터 바이러스의 80% 정도가 파일 바이러스에 속한다.

국내에서는 예루살렘(Jerusalem), 일요일(Sunday) 바이러스를 시작으로 잘 알려진 전갈(Scorption), 까마귀(Crow), 알트X(Alt_X), 해골(Leech), 회오리(Eddy), 매독(Pox), PS-MPC, NRLG, IVP 그리고 전율(Tremor), 시스터보(SysTurbo) 바이러스 등을 들 수 있다.

· 부트/파일 바이러스 (Multipartite virus)

부트·파일 바이러스는 부트 섹터와 파일에 모두 감염되는 바이러스로 대부분 크기가 크며 피해 정도가 큰 것이 특징이다. 국내에서는 90년의 침입자 바이러스를 시작으로 나타스(Natas), TPVO, 안락사(Euthanasia), Cri-Cri 바이러스 등 복잡하면서 많이 확산되어 피해가 컸던 바이러스들이 있으며 최근 발견된 에볼라(Ebola) 바이러스도 이에 속한다.

· 매크로 바이러스(Macro virus)

최근 발생한 새로운 형태의 파일 바이러스로 감염 대상이 실행 파일이 아니라 마이크로소프트사의 엑셀과 워드 프로그램에서 사용하는 문서 파일이라는 점과 응용 프로그램에서 사용하는 매크로(간이언어)를 통하여 감염되는 형태로 해당 프로그램 사용할 때에만 감염될 수 있다. 대표적인 예로는 확산 정도가 큰 ExcelMacro.Laroux 바이러스를 들 수 있으며, 최근 Word 5 Marcro.Class가 발견되면서 매크로 바이러스도 다형성을 가지게 되었다.

■ 국내 컴퓨터 바이러스의 발견 추세 및 단계적 변화

우리나라에서는 매년 상당한 수의 바이러스가 발견되고 있다. 지난해만 해도 276종의 신종 바이러스가 발견되었는데, 이는 평균 1주일에 5종의 바이러스가 제작된 셈이다.

특징적인 것으로는 국내에서 제작된 바이러스가 외국에서 제작된 바이러스 수보다 2배 가까운 수치를 나타내고 있다. 98년 한 해 동안 많은 피해를 주었던 바이러스들은 대체로 외국산보다는 국산 바이러스들이 많았다. 국산 바이러스는 앞으로 다양한 환경에서 많이 나타날 것으로 보이므로 각별한 유의가 필요하다.

다음은 국내에서 발견된 바이러스에 대한 단계별 분류이다. 이 단계적 분류는 순차적인 경우도 있지만 단순히 분류에 의미를 둔 경우도 있다.

따라서 꼭 단계적 발전을 의미하는 것이 아니라 특징에 따른 단계적 변화라고 할 수 있다.

· 1단계(1988-1989) : 부트 바이러스.

국내에서 최초로 발견된 바이러스는 뇌(Brain) 바이러스이며 이 시기에 발견된 바이러스들은 대체적으로 간단하며 부트 바이러스가 주종을 이루고 있다.

이 시기에는 바이러스에 대한 별다른 지식이나 정보가 없어서 확산 정도가 컸다. 예로는 (C)Brain , LBC , 미켈란젤로 바이러스 등을 들 수 있다.

· 2단계(1989) : 파일 바이러스 출현

주로 파일을 감염시키는 바이러스로 파일에 붙어서 파일 실행에 영향을 미치지 않은 채 기

생하는 형태의 바이러스들이 나타나게 되었다.

예로는 예루살렘, 일요일 바이러스와 PS-MPC나 IVP 등을 들 수 있다.

· 3단계(1990) : 본격적인 메모리 상주형 바이러스의 출현

바이러스가 메모리에서 상주하여 파일 및 부트영역을 감염시키는 형태로 발전이 되었으며 기존의 형태와는 다른 암호화 기법이 구현되어 본격적인 바이러스와 백신과의 소득없는 소모전이 시작되었다고 볼 수 있는 시기이다. 예로는 11월30일, 자유, NRLG 바이러스를 들 수 있다.

· 4단계(1993) : 은폐기능을 사용하는 바이러스의 출현

바이러스들은 메모리에 상주하여 감염된 파일을 사용하고자 할 때 이를 바이러스에 감염되지 않은 파일인 것으로 속이는 은폐기능이 본격적으로 구현되어 외형적으로는 바이러스가 없는 것으로 생각하게 만들었다.

이 시기에는 파일뿐만 아니라 부트 바이러스들도 은폐기능을 사용하였으며 결국 백신에서 메모리에 있는 바이러스를 제거하기 전에는 파일에 감염된 바이러스를 찾아낼 수 없게 되었다. 예로는 돌(Stone), 매독, 원숭이 바이러스 등을 들 수 있다.

· 5단계(1993) : 암호화 바이러스의 출현

지금까지 바이러스들은 단순한 형태로 고정적인 암호화 루틴을 가지고 있었다. 하지만 이 시기에 출현한 바이러스들은 복수의 암호키를 사용하거나 암호화 방법이 감염시마다 변하는 형태의 바이러스들이 출현하여 백신의 제작을 지연시켰다.

예로는 몰타아메바, 온타리오.1024 바이러스 등을 들 수 있다.

· 6단계(1995) : 다형성 바이러스의 출현

백신은 대체적으로 코드의 특징을 찾아 검색하는 것이 알려지면서 바이러스 제작자들은 암호화 및 암호화 루틴을 구성하는 코드들을 변화시켜 특징을 찾기 어렵도록 하여 백신의 검색을 피할 수 있도록 발전시켰다.

이로 인하여 백신은 바이러스에 동일한 암호 해제 루틴을 가져야 하므로 백신 개발이 상당히 지연되고 크기도 커지게 되었고 검색 속도가 늦어지기 시작했다. 예로는 나타스(Natas), 전율(Tremor), 코니II, 커피숍II 바이러스 등을 들 수 있다.

· 7단계(1996): 메모리 은폐형 바이러스 출현

상주형 바이러스의 경우는 메모리에 상주하고 있는 바이러스를 제거하지 않고 파일에 감염된 바이러스를 치료할 수 없다는 점에서 그동안 백신들은 어렵지 않게(간단한 파일 바이러스를 검사하는 수준에서) 바이러스들을 진단하여 치료했으나 바이러스 몸체가 암호화하여 은폐시킴으로써 백신에서 메모리 내에서 바이러스를 검사할 수 없도록 하여 분석 및 백신제작을 지연시키는 결과를 가져왔다.

예로는 먹개비 바이러스를 들 수 있다.

· 8단계(1997) : 다형성 바이러스의 기술적인 발전

예전의 다형성 바이러스들은 이제는 간단한 형태의 바이러스로 취급당하기 쉽다. 최근 발견된 FCL 바이러스는 바이러스에서 코드를 만들어내는(프로그래밍을 하는) 수준의 바이러스로 평가되고 있다.

이전의 바이러스들은 제한된 범위 내에서 변화하는 최소한의 규칙을 가지고 있었지만 이제는 그 최소한의 규칙마저도 없어져 백신으로서는 최대의 위기를 맞은 셈이다.

백신의 입장에서는 프로그램을 분석하는 수준의 새로운 기술을 요구하게 된 시기로 앞으로의 백신과 바이러스와의 전쟁이 쉽지 않을 것이라는 예상을 하게 만들었다.

· 9단계(1997) : 새로운 개념의 바이러스 출현

문서편집기 등에서는 사용자의 편의를 위하여, 또한 하드웨어 환경에 구애받지 않는 운영체제(윈도우 NT 등)가 만들어지면서 좀더 편리하게 사용할 수 있는 간이언어(매크로)를 사용한다.

이를 이용해 제작된 워드매크로와 엑셀매크로 바이러스가 최근 기업에서 많은 피해를 일으키고 있다.

이는 앞으로 바이러스들이 어떠한 환경에서도 작동할 수 있다는 것을 의미하므로 주의를 요한다.

· 10단계(1997) : 새로운 운영체제 하의 바이러스 출현

윈도 95가 출현하면서 PC 환경에 많은 변화가 일어났다. 많은 사람과 기업이 도스 환경에서 탈피하여 윈도우 환경으로 넘어가기 시작했다.

윈도우 환경은 운영체제가 실행하는 영역을 보호하는 형태로 운영되어 바이러스로부터 안전하리가 기대했지만 97년부터 현재까지 많은 윈도우용 바이러스가 발생하였으며 그 피해 정도가 크고 시스템 파괴라는 극단적인 상황까지도 발생할 수 있는 증상을 가진 바이러스도 나타나게 되었다.

현재 윈도 95용 바이러스는 아편걱정(Anxiety_Poppy), 마르부르크(Marburg) 가 있으며 국산으로는 전갈.1275가 최근 발견되었다.

현재 국내에서 발견되는 바이러스들은 대체적으로 1-5단계에 해당하는 바이러스들로 외국산 바이러스의 정보가 공개되어 이를 변형한 바이러스들이며, 이의 제작자들은 지식이나 프로그래밍 실력 면에서는 다소 열등하며 단순 과시용으로 바이러스를 제작해 유포한다.

최근 발생하는 바이러스들이 가지는 특징은 크게 두 가지로 볼 수 있다. 하나는 윈도우 95/98 환경에서 작동하는 윈도

■ 최근 동향

〈표 1〉 88~98년의 출처별 바이러스 동향

	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	총계
한국산		3	8	5	10	17	40	81	152	170	162	648
외국산	1	3	20	16	7	17	36	47	74	86	114	421
합계	1	6	28	21	17	34	76	128	226	256	276	1069

〈표 2〉 88~98년의 종류별 바이러스 동향

	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	총계
부트	1	4	8	5	5	10	13	18	8	15	14	101
파일		2	18	15	11	23	60	105	188	220	219	861
매크로									1	16	36	53
부트/파일			2	1	1	1	3	5	29	5	7	54
합계	1	6	28	21	34	34	76	128	226	256	276	1069

우 바이러스이고 그 다음으로는 MS 오피스 제품군에서 작동하는 워드매크로 및 엑셀매크로 바이러스이다.

이 두 가지 모두 바이러스의 수는 적으나 감염시 피해 정도가 크다는 점과 감염이 광범위하게 일어난다는 점도 큰 특징이라고 할 수 있다.

· 윈도우 바이러스

최초의 윈도우용 바이러스는 WinVir로 1992년에 발견되었다. 국내에 처음 발견된 것은 1996년에 발견된 보자(Boza)로 아주 간단한 바이러스였고 한글 윈도우에서는 실행이 되지 않았다. 하지만 Tentacle(윈도우3.1용)이 나오면서 윈도우 바이러스의 본격적인 출발이 시작되었다.

이후 아편걱정(Anxiety_Poppy) 바이러스 그리고 1998년 후반기에 발견되어 그 피해가 많았던 CIH 바이러스, 그리고 윈도우 바이러스에서 다형성 기법이 적용된 HPS, 영국 PC Gamer지 부록 CD에 감염되어 퍼지기 시작한 마르부르크(Marburg) 바이러스, 그리고 최근 발견된 파다니아(Padania) 등의 윈도우 바이러스가 계속 나타나고 있다.

얼마 전 국내 최초의 윈도우 바이러스인 전갈.1275가 나타나 국내에서도 윈도우 바이러스가 제작이 시작되었음이 밝혀졌다.

· 워드/엑셀매크로 바이러스

국내 기업 환경에서 많이 사용하는 MS워드나 엑셀의 매크로 언어를 기반으로 한 바이러스가 유포되고 있다.

현재 Word97Macro.CLASS, ExcelMacro.Extras 등 다형성 바이러스까지 등장한 상태이다. 바이러스 유형에서 다형성 바이러스가 가장 복잡하다는 점을 감안할 때 매크로 바이러스의 발전 정도가 매우 빠르다는 것을 알 수 있다.

1998년에는 국내에서 변형 제작된 ExcelMacro.Laroux.Kr이 발견되어 매크로 바이러스 영역에서도 국내 바이러스 제작자들이 활동하고 있음이 알려졌다.

· 유틸리티로 가장한 바이러스

최근 발생하는 바이러스들의 특징으로 유용한 유틸리티로 가장한 경우를 들 수 있다. 윈도우 바이러스로 피해를 많이 준 CIH는 MoviePlay 1.46버전과 함께 유포가 되었고 98년 맹위를 떨쳤던 알트엑스도 V31200.EXE으로 V3+의 최신버전을 가장하여 유포가 되었으며 전갈(Scorpion) 등은 세어웨어 프로그램을 정품 프로그램으로 만들어주는 크랙 프로그램을 통하여 유포되었다.

따라서 결국 이러한 것은 사용자가 조금만 주의하면 바이러스 감염을 막을 수 있다.

■ 앞으로의 바이러스

지금까지 발견된 바이러스들은 대체로 특정한 운영체제(윈도우 혹은 도스)에서 작동하는 것이 일반적이다. 그러나 최근의 바이러스는 매크로 바이러스에서 볼 수 있듯이 운영체제 환경이 아닌 범용적인 환경에서 작동할 것으로 보인다.

현재 많은 사람들이 사용하는 윈도우 환경도 얼마 전까지는 안전한 운영체제로 인식되었지만 최근 많이 발생하고 있는 윈도우 바이러스로 인하여 그 안전성에 의심이 가게 되었고 앞으로도 상당수의 윈도우용 바이러스가 나타날 것으로 예측된다.

또한 그간 바이러스와는 관계가 없을 것 같은 HTML 환경도 바이러스가 나타나고 있다는 점에서 앞으로도 새로운 환경에서의 바이러스가 계속 출현할 것으로 추측된다.

국내 상황이 경우 그간 외산 바이러스에 대한 변형이 주를 이루고 있었지만 1997년 이후 순수 국내 제작으로 바뀌고 있으며 더욱더 복잡해져 가고 있어 그 피해가 우려된다.

미래의 바이러스는 여러 신기술을 가지게 되어 사이버 공간에서 활발히 활동할 것이다.

즉 현재와 같이 컴퓨터 사이의 통신 및 자료 교환을 통해서만 감염이 되는 것이 아니라 광범위하게 초고속정보통신로 혹은 그에 상응하는 통신 경로를 통하여

더욱 짧은 시간에 많은 사람이 감염되는 상황이 생길 것이다. 올해 3월 말에 발견된, E-메일을 통해 자동 유포되는 멜리사 바이러스가 그 물꼬를 텄다고 할 수 있다.

지금은 컴퓨터 사용자의 잘못된 사용(불법복제 혹은 부주의)에 의하여 감염되는 것이 일반적이지만 미래에는 바이러스 스스로 판단하고 자신을 변형하는 등 더욱 지능적으로 바뀔 것이다. 하지만 그에 반하여 백신도 마찬가지로 지능을 갖게 되어 그 싸움이 더 치열해질 것이다.

현재의 바이러스는 누군가 실행을 해주어야 작동을 하며 제한적인 범위(메모리 영역 또는 바이러스의 몸체가 저장되어 있는 영역) 내에서만 활동을 한다. 하지만 그런 컴퓨터 바이러스가 생명력을 가지면 그 피해 정도는 더 커질 것이며 심지어 인간에게까지 도전하는 상황이 생길지도 모른다.

영화에서도 가끔 나오는 컴퓨터들의 반란이 어쩌면 가상 속의 얘기가 아닐지도 모른다.

바이러스는 그 활용 범위가 크다. 우리가 영화에서 보듯이 침투한 외계인과 싸우기 위해 우주선에 바이러스를 침투시켜 우주선을 무력화하는 등 실제로 미래에 있을 법한 예기들이다. 다만 그 시기가 먼 미래일 수도 있고 실현되지 못할 수도 있다.

지독한 독감에 걸리지 않기 위해 독감 예방 주사를 맞듯이 컴퓨터 바이러스에 걸리지 않기 위해서는 컴퓨터 바이러스 예방주사를 맞아야 한다.

바이러스에 대하여 너무 겁을 먹을 필요는 없다. 몸에 감기가 들었다면 치료할 수 있듯이 컴퓨터에서 바이러스는 감기와 같은 것으로 생각하면 된다. 감기가 폐렴이 되어 죽는 사람도 있을 수 있듯이 컴퓨터에서도 바이러스에 의하여 하드디스크 자료가 파괴되는 경우도 있다. 하지만 이는 극소수의 바이러스만이 그런 증상을 가지고 있으므로 주의만 하면 별다른 피해를 당하지 않는다.

■ 컴퓨터 바이러스의 감염 경로

컴퓨터 바이러스는 컴퓨터에서 저절로 생기는 것이 아니라 누군가에 의해서 고의로 만들어진 후 여러 경로를 통해서 다른 사용자에게 전파된다. 바이러스를 예방하려면 우선 이 감염 경로를 잘 파악해야 한다.

컴퓨터 바이러스의 감염 경로는 다음의 5가지 정도로 요약할 수 있다.

(1) 불법 복사

대부분의 경우가 소프트웨어, 특히 게임 소프트웨어 등의 불법 복사에 의한 감염이다.

소프트웨어는 불법으로 복사되면서 여러 사람의 컴퓨터를 거치게 되는데, 도중에 어떤 사용자의 고의 또는 실수에 의해 컴퓨터 바이러스에 감염되거나, 자신의 컴퓨터가 감염된 사실을 알지 못하고 다른 사람에게 프로그램을 복사해 준다면, 그 다음 사용자부터는 꼼짝없이 컴퓨터 바이러스의 피해를 입게 되는 것이다.

게임 소프트웨어에서 컴퓨터 바이러스가 많이 발견되는 이유는 그 소프트웨어 자체에 문제가 있는 것이 아니라 불법 복사가 가장 많이 행해지는 소프트웨어의 하나이기 때문이다.

때로는 프로그램이 많이 복사될수록 시스템 안정성이 떨어져 바이러스에 치명적으로 약해지는 경우도 있다.

(2) 컴퓨터 통신

컴퓨터 통신에서 받은 프로그램을 통해 감염되는 경우가 있다.

특히 최근에는 컴퓨터 통신을 이용하는 인구가 급증해 통신망을 통해 바이러스가 유포되는 사례가 증가하고 있다.

고의로 바이러스를 제작한 후 다른 프로그램인 것처럼 속여 공개자료실에 올려 놓는 사람도 있지만, 자신의 파일이 컴퓨터 바이러스가 감염된 사실을 모른 채 통신망에 올려 놓는 사람도 있다.

95년 시스터보(Systurbo) 바이러스, 96년 세발(Sebal) 바이

러스 등이 대표적인 통신망을 통한 감염 사례이다.

컴퓨터 통신망에 감염된 프로그램이 등록되면 컴퓨터 바이러스가 단시일에 전국적으로 유포될 수 있다.

이런 경우를 최소화하기 위해서는 최근에 등록된 소프트웨어는 바로 받지 말고 일주일 정도 기다리는 여유가 필요하다.

또한 이러한 프로그램은 대부분 굉장히 유용한 프로그램이라고 선전하기 때문에 주의해야 한다.

일주일 정도 지난 다음 아무런 피해 사례가 보고되지 않았을 때 이용한다면 피해 입을 확률이 훨씬 줄어들 것이다.

최근에는 PC 통신 및 인터넷을 통해 '메일폭탄(Mail Bomb)'이 나타나곤 하는데, 이것은 일반 메일인 것처럼 가장해 특정인에게 보내지는 것으로, 메일을 열어보면 바로 시스템에 특정한 이상 증상을 일으키는 악성 프로그램이다.

메일로 보내지는 것은 컴퓨터 바이러스일 경우도 있지만 트로이 목마인 경우가 많다.

(3) 컴퓨터의 공동 사용

직접 불법 복제를 하지 않더라도 한 컴퓨터를 여러 명이 사용하는 학교, 학원이나 회사에서는 바이러스 감염에 특히 신경을 써야 한다.

다른 사람이 사용한 컴퓨터를 그대로 사용한 경우, 앞서 컴퓨터를 사용한 사람이 고의 또는 실수로 감염된 프로그램을 사용하면 기억 장소에 컴퓨터 바이러스가 존재하게 된다.

그 컴퓨터를 그대로 사용하면 해당 컴퓨터에 바이러스가 감염되는 것은 불을 보듯 뻔하다.

따라서 컴퓨터를 공동으로 사용하는 경우에는 백신으로 자주 검색하거나 컴퓨터를 일단 끈 다음에 자신이 가지고 있는 도스 디스켓으로 다시 부팅을 시켜서 사용하는 것이 좋다.

(4) LAN(Local Area Network)

LAN으로 연결된 컴퓨터들은 많은 프로그램을 공유함은 물론 많은 자료를 고속으로 교환할 수 있기 때문에, 한 곳에 침투한 컴퓨터 바이러스가 순식간에 다른 컴퓨터를 감염시킬 수 있다. 최근 들어 사내 전산망 구축을 위해 LAN을 도입하는 경우가 많아 피해 사례가 급증하고 있다.

(5) 상업용 소프트웨어 등

아주 드물지만 정식으로 구입한 상업용 소프트웨어를 통해서도 감염된다.

상업용 소프트웨어가 아니더라도 컴퓨터 잡지에 부록으로 끼워주는 CD에서 컴퓨터 바이러스가 발견되기도 한다. 따라서 잡지 부록 소프트웨어나 상업용 소프트웨어라 할 지라도 자신의 컴퓨터에서 처음 실행하는 소프트웨어의 경우에는 반드시 최신 버전의 백신 프로그램으로 진단하는 것이 바람직하다.

■ 바이러스 증상

컴퓨터 바이러스에 감염되면 감염된 바이러스 종류에 따라 여러 가지 증상이 나타난다.

바이러스 때문에 나타나는 증상은 일일이 열거할 수 없을 정도로 다양하지만, 자세히 살펴보면 몇 가지 공통적인 특징을 발견할 수 있다.

따라서 바이러스의 종류를 잘 파악하고 있다면 신종 컴퓨터 바이러스도 조기에 발견, 치료할 수 있을 것이다.

컴퓨터 바이러스는 정상적인 프로그램의 실행 과정을 가로챔으로서 여러 가지 증상과 바이러스 프로그램 자체에서 만든 여러 가지 부작용을 불러일으킨다.

특히 다음과 같은 증상이 나타나면 컴퓨터 바이러스를 의심해 보아야 한다.

바이러스에 의한 증상은 일일이 열거할 수 없을 정도로 다양하지만, 공통적인 것을 모아서 분류하면 다음의 4가지로 나눌 수 있다.

(1) 속도 저하

컴퓨터 바이러스는 정상적인

프로그램 실행 과정을 가로채서 자기가 먼저 실행된 다음에 원래의 프로그램을 실행시키기 때문에, 그만큼 실행 속도가 저하된다. 부트 바이러스에 감염되었을 경우에는 부팅 시간이 길어지며 디스크를 읽거나 쓰는 속도가 떨어지게 된다.

파일 바이러스에 감염된 경우에도 프로그램을 처음 시작할 때 불러들이는 속도가 현저히 떨어진다.

때로는 도스에서 DIR 명령으로 디렉토리를 보려고 할 때 화면에 나타나는 시간이 오래 걸리기도 한다.

(2) 감염 흔적

컴퓨터 바이러스는 감염되는 과정에서 여러 가지 흔적을 남긴다.

기억 장소에서 실행되어야 하므로 사용 가능한 기억 장소의 크기가 줄어들며, 파일 바이러스의 경우에는 파일의 길이가 커지거나 파일 작성일이 변경되기도 한다.

(3) 파괴 증상

프로그램이나 디스크의 특정 영역에 대한 파괴 증상을 나타내기도 한다.

감염 후 프로그램이 갑자기 실행되지 않거나 시스템이 다운되는 등 이상한 동작을 보일 경우가 있다. 또한 의도적으로 프로그램을 지워버리거나 하드 디스크의 논리적 구조를 파괴하여 인식되지 않게 만드는 경우도 있다.

디스크의 부트 레코드 내용 및 FAT(File Allocation Table) 내용을 변경하거나 파괴하며 디스크의 디렉토리 내용도 변경하거나 파괴한다.

디스크의 볼륨 라벨을 변경하며 디스크에 불량 섹터를 만들기도 한다.

(4) 바이러스별 특이 증상

컴퓨터 바이러스 제작자가 컴퓨터 바이러스에 의도적으로 포함시킨 특징적인 증상 또는 부작용이 나타날 수 있다.

이상 증상으로는 컴퓨터 바이러스의 종류에 따라 화면에 엉뚱한 메시지를 출력하는 등의 단순한 것부터 깃발, 벌레 등의 그래픽을 출력하는 것, 나아가 하드 디스크 전체 자료를 지워버리는 직접적인 파괴 행위에 이르기까지 매우 다양하다.

다시 말하면 컴퓨터 바이러스도 일종의 프로그램이기 때문에 프로그램에서 가능한 정도의 특이한 증상들을 나타내는 것이다.

예를 들어서 탁구(Pingpong) 바이러스의 경우에는 화면에 까만 점 하나가 탁구공처럼 돌아다니는 것이 주요 증상이며, 크리스마스 인사 바이러스는 'Merry Christmas and Happy New Year!'이라는 메시지와 함께 '고요한 밤 거룩한 밤'이라는 캐롤송을 들려준다.

컴퓨터 바이러스에 감염되었을 때 나타나는 증상을 설명하기 전에 한 가지 알아두어야 할 점은 부트 섹터나 실행 파일에 바이러스가 감염되었다고 해서 항상 다른 곳으로 전염시키지는 않는다는 것이다.

부트 바이러스는 감염된 디스크로 부팅시켜야만 감염되고, 파일 바이러스는 감염된 파일을 실행시켜야 컴퓨터 바이러스가 다른 곳으로 전염될 수 있다.

따라서 감염되지 않은 디스크로 부팅을 시킨 다음에는 부트 바이러스에 감염된 디스크를 사용해도 아무런 문제를 일으키지 않는다.

또한 파일 바이러스에 감염된 프로그램을 사용하지 않는 한, 그 프로그램이 디스크에 존재하고 있더라도 다른 프로그램에는 아무런 영향을 미치지 못한다.

사용자가 간과하기 쉬운 것이 있는데 컴퓨터에 이상 증상이 나타난다고 해서 모두 컴퓨터 바이러스인 것은 아니라는 점이다. 컴퓨터 바이러스를 의심하기 전에 사용자는 컴퓨터를 잘못 조작하지 않았는지 한 번쯤 생각해 보아야 한다.

하드웨어 자체나 디스켓에 이상이 없는지를 검사하고, 만약 사용자의 조작 실수나 하드웨어의 잘못이 없을 때는 단지 프로그램의 버그(Bug)인지 아니면

트로이 목마(Trojan Horse) 프로그램인지를 구분해야 해결책을 찾기 쉽다.

■ 바이러스 예방법

컴퓨터 바이러스로 인한 피해는 개인의 경우도 그러하지만, 특히 기업의 전산 환경에 바이러스가 침투했을 경우 그 규모가 더욱 커진다.

업무 파일이 지워지거나 시스템이 다운되는 것은 물론 모든 전산 환경이 마비되어 큰 낭패를 보는 경우도 있다.

한때 각 증권사의 공동전산화를 담당하고 있는 모 기업의 전산 시스템이 크리스마스 인사 바이러스에 감염된 적이 있었다. 각 증권사의 단말기 작동이 정지되어 증권시세 등을 볼 수 없게 되었고, 고객들의 불만이 빗발쳤다.

결국 이런 사실이 언론에 보도되면서 그 업체는 사태 수습을 위해 동분서주하게 되었다.

대부분의 사용자들이 컴퓨터 바이러스를 예방하는 데 노력을 기울이지 않는다.

기업에서도 수천만 원 또는 수억 원을 들여 보안 시스템 마련에 머리를 싸매지만 정작 바이러스 예방에 대해서는 적극적으로 나서지 않는 실정이다. 바이러스를 치료하는 것도 중요하지만 '소잃고 외양간 고치는 일'이 없으려면 사전에 철저한 대비책을 세워놓아야 한다.

바이러스 예방법이라고 해서 안전성이 100% 보장되는 것은 아니다.

이제까지 알려진 컴퓨터 바이러스의 감염 경로나 특성에 따라 대책을 세웠기 때문에 향후 다양하고 복잡한 제작 기법의 컴퓨터 바이러스가 발견될 경우에는 무용지물이 될 가능성도 있다. 그러나 다음의 바이러스 예방법만이라도 잘 지킨다면 결과를 예측할 수 없는 각종 바이러스 피해로부터 안전할 수 있을 것이다. 예방법을 알아보자.

우선 정품 소프트웨어를 구입해 사용하는 것이 중요하다. 불법 복사한 소프트웨어는 많은 사람의 손을 거치기 때문에 자연히 바이러스에 쉽게 노출되며, 바이러스가 감염되었을 경우 책임 소재도 가릴 수 없으므로 반드시 정품 소프트웨어를 사용해야 한다. 불법 복사가 성행하는 오락 및 게임 프로그램의 상당수가 컴퓨터 바이러스에 감염되어 유통된다고 한다.

한두 대의 컴퓨터를 여러 사람이 공동으로 사용할 때는 다른 사람이 사용하고 난 뒤에 반드시 전원을 끈 다음 자신의 부팅 디스켓으로 부팅시킨 후 사용한다. 이 방법은 아직도 하드 디스크가 없이 사용하는 PC에 해당되며, 하드 디스크가 있는 경우에는 하드 디스크로 부팅하면 된다.

이렇게 하지 않으면 어떤 경로든지 컴퓨터에 침투해 메모리에 상주한 바이러스가 이후에 사용하는 모든 사용자의 디스켓을 감염시키기 때문이다.

이때 아무 디스켓으로나 부팅하지 말고 자신의 부팅 전용 디스켓 한 장을 만들어 쓰기방지 탭을 붙여 놓는 것이 중요하다. '깨끗한 부팅 디스켓 만들기'는 뒤에 설명하겠다. 아울러 수시로 시스템을 최신 버전의 백신으로 검사해 바이러스 침투를 예방하는 것도 매우 중요하다.

PC 통신이나 인터넷을 통하여 프로그램을 받을 때는 신뢰할 수 있는 유명 통신망이나 동호회, 포럼 자료실 또는 인터넷 홈페이지에서 받도록 한다. 이런 곳은 자료실 담당자가 불법 복사물인지, 바이러스에 감염된 파일인지 등을 확인한 뒤 등록하기 때문에 바이러스에 노출될 확률이 적다.

사설 BBS의 경우가 위험한데, 잘 알려지지 않은 곳에서는 가급적 자료 받기를 삼가는 것이 좋다. 또 한번 내려받은 프로그램은 최신 버전의 백신 프로그램으로 바이러스 감염 여부를 확인한 후에 사용하는 것이 안전하다.

기업 환경에서의 LAN(Local Area Network)을 통한 바이러스 감염은 피해 정도 및 규모로 보아 매우 위험하다. LAN으로 연결된 컴퓨터들은 많은 프로그램을 공유함은 물론 방대한 자료

교환이 고속으로 이루어지기 때문에, 한 곳에 침투한 컴퓨터 바이러스가 순식간에 많은 컴퓨터를 감염시켜 버린다. 시스템 파괴를 비롯해 업무를 마비시켜 재산상의 큰 피해를 가져오는 것이다.

지금까지 국내에 알려진 컴퓨터 바이러스 중에서 대표적인 특정일 활동 바이러스로는 3월 6일에 활동하는 미켈란젤로 바이러스와, 13일의 금요일에 활동하는 예루살렘 바이러스, 4월 26일에 활동하는 CIH 바이러스를 들 수 있다.

대부분의 컴퓨터 바이러스가 감염과 동시에 바이러스 자체의 특징이 나타나는 데 비해, 특정일 활동 바이러스는 특징적인 증상이 나타나거나 더욱 심해지는 특정한 시기가 있기 때문에 사용자를 긴장하게 만든다.

따라서 정상적인 PC도 특정일 활동 바이러스가 피해를 입히는 날이 되면 자동으로 바이러스에 감염된다고 생각하는 사용자가 있는데, 이는 사실이 아니다.

특정일에 활동하는 바이러스도 최신 버전의 백신 프로그램으로 퇴치가 가능하다. 그러므로 바이러스 활동일이 다가온다고 걱정하지 말고 최신 버전의 백신 프로그램을 이용하여 미리 진단을 해놓도록 하자.

■ 백신 프로그램의 요건

네트웍 환경에서는 어떤 클라이언트로부터 감염되기 시작했는지 감염 경로를 정확하게 확인할 수 없어 감염 원인 파악과 예방이 어렵고, 치료할 때도 네트웍에 연결된 모든 컴퓨터 시스템을 동시에 치료하지 않을 경우 재발될 가능성이 매우 높다.

감염된 한 대의 클라이언트가 네트웍에 연결된 모든 컴퓨터 시스템을 감염시키므로 네트웍에서 바이러스를 막기 위해서는 연결된 모든 클라이언트가 감염되지 않도록 해야 한다.

그러나 이것은 현실적으로 거의 불가능하기 때문에 적절한 안티바이러스 대책이 필요하다.

개별 클라이언트는 물론 파일 서버나 웹 서버, E-메일 서버, 그룹웨어 서버 등 바이러스가 침투할 수 있는 모든 환경에 적절한 백신을 설치해 두어야 빈틈없는 방역을 할 수 있다.

특히 네트웍 환경에서 인터넷을 이용할 경우 한 개인이 잘못 전송받은 바이러스가 네트웍을 타고 전사적으로 확산될 우려가 있기 때문에 더욱 주의해야 한다.

웹브라우저, FTP 유틸리티 등에서 파일을 다운로드하거나 E-메일로 받은 데이터로 인해 바이러스가 감염될 수 있으므로 다운로드 도중 바이러스 감염 여부를 체크할 수 있는 백신이 있으면 원천적으로 바이러스 침투를 막을 수 있다. 일단 다운로드한 파일이라도 실행하기 전에 백신으로 검사하면 된다.

백신 프로그램은 구입보다 지속적인 유지보수가 중요하며, 유사시의 큰 피해에 대비하기 위해 투자한다는 차원에서 보험과 같다. 백신 프로그램을 도입할 때 고려해야 할 사항은 다음 세 가지이다.

가장 중요한 점은 백신 프로그램 제작사에서 신종 바이러스가 출현했을 때 얼마나 빨리 대응조치를 취할 수 있는가 하는 점이다.

컴퓨터 바이러스가 사내에 퍼졌을 때는 빨리 조치를 취하지 않으면 매시간 피해액수가 기하급수적으로 늘어나게 된다.

따라서 백신 프로그램의 경우에는 단순한 가격비교는 아무런 의미가 없고, 얼마나 빨리 대응조치를 할 수 있는 능력이 있는가가 가장 중요하다.

컴퓨터 바이러스에 대응하는 데 소요되는 시간은 두 가지 요소의 합으로 결정된다.

즉, 얼마나 빨리 신종 바이러스를 수집할 수 있는지, 그리고 얼마나 빨리 분석해서 백신 프로그램을 만들어서 공급할 수 있는지를 합산하면 대응에 걸리는 시간을 계산할 수 있다.

필자의 연구소가 경쟁사들보다 앞서갈 수 있었던 이유도 이 시간이 가장 짧기 때문이다.

우리 나라에서는 컴퓨터 바이러스가 처음 발견되면 안철수연

구소로 가장 먼저 신고가 들어올 수밖에 없으며, 개발인원도 가장 많기 때문에 24시간 이내에 대응할 수 있는 체계가 갖추어져 있다.

반면에 경쟁사들은 신고를 받는 것조차 힘든데다, 개발인원도 아예 없거나 많아야 4-5명에 불과해서 대응할 수 있는 여력이 부족한 실정이다.

백신 프로그램을 선택할 때 두 번째로 고려해야 할 점은 서버용 백신 프로그램의 도입이다.

결론적으로 관공서, 기업, 학교 등 단체로 컴퓨터를 사용하는 환경에서는 PC용 백신뿐만 아니라 서버용 백신 프로그램도 도입하는 것이 한 컴퓨터의 피해가 다른 컴퓨터로 파급되는 것을 막을 수 있는 방법이다.

백신 프로그램은 크게 나누어서 각 개인들이 사용하는 컴퓨터에서 동작하는 클라이언트(client)용 백신 프로그램과 파일 서버, 인터넷 서버, e-mail 서버, 그룹웨어 서버 등에서 동작하는 서버(server)용 백신 프로그램으로 나눌 수 있다.

컴퓨터 바이러스는 클라이언트에서만 동작하고 감염되며, 서버에서 동작하고 감염되는 경우는 없다. 컴퓨터 바이러스의 파괴활동도 클라이언트에서 일어난다.

따라서 서버용 백신 프로그램의 역할은 감염된 파일이 한 클라이언트에서 서버를 통해서 다른 클라이언트로 넘어가는 일이 없도록 중간에서 차단하는 일을 하는 것이다.

서버용 백신 프로그램이 존재하더라도 디스켓이나 CD-ROM을 통한 감염이나 모뎀을 사용하여 PC 통신에 접속하는 경우 등 서버를 통하지 않는 바이러스 감염은 차단할 수 없다는 단점이 있다.

따라서 클라이언트를 보호하고 컴퓨터 바이러스에 의한 피해를 막기 위해서는 클라이언트용 백신 프로그램이 필수적이다.

반면에, 모든 사용자가 최신 버전의 클라이언트용 백신 프로그램을 사용하는 것은 아니기 때문에, 관리자의 입장에서는 서버용 백신 프로그램만 최신 버전으로 관리하면 한 클라이언트가 감염되더라도 다른 클라이언트로 넘어가는 것을 방지해서 피해를 최소화할 수 있다는 장점이 있다.

따라서 백신 프로그램을 선택할 때는 클라이언트용 백신 프로그램은 필수적인 것이며, 서버용 백신 프로그램은 관리자 입장에서 보조적인 것으로 생각하는 것이 좋다. 그러나 사용하는 컴퓨터의 수가 많아지고 네트웍의 규모가 커질수록, 클라이언트용 백신 프로그램과 서버용 백신 프로그램을 같이 사용하는 것이 좋다.

백신 프로그램을 도입할 때 세 번째로 고려해야 할 사항은 업데이트 주기이다.

최근에는 거의 매일 새로운 컴퓨터 바이러스가 등장하는 추세이기 때문에, 매주 업데이트를 하는 것이 세계적인 추세이다. 따라서 매주 업데이트가 되지 않는 제품은 사용하지 않는 것이 바람직하다.

또한 사용자들은 매주 업데이트된 백신 프로그램을 사용해서 자신의 컴퓨터를 직접 검사하는 습관을 가지는 것이 중요하다. 즉, 특정한 요일 및 시간을 정해놓고 새로운 백신 소프트웨어를 받아서 검사하는 것을 습관화해야 한다.

또 다른 방법으로, 바이러스의 활동일을 명시해놓은 바이러스 캘린더를 보면서 표시된 날마다 검사하는 것도 좋다.