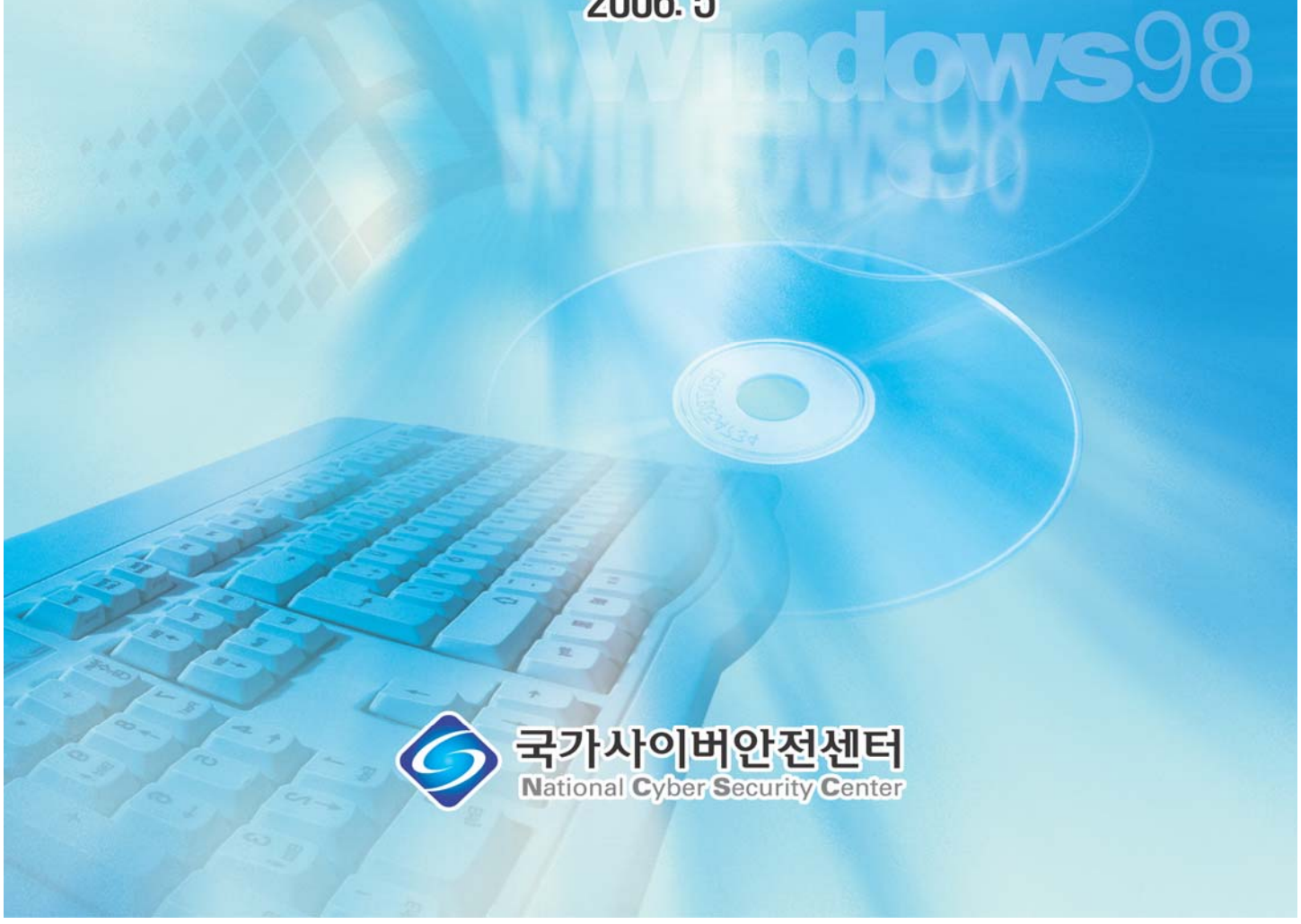
Windows98
보안 가이드라인

2006. 5



국가사이버안전센터
National Cyber Security Center

머 리 말

목적

- 본 가이드라인은 Windows 98을 사용하는 컴퓨터의 환경을 가급적 안전하게 유지하기 위한 방법들을 설명하고 있습니다.

대상

- 본 가이드라인은 Windows 98 운영체제를 사용하는 사용자들 중에서 컴퓨터 지식이 많지 않은 초보자들을 기준으로 하여 작성되었습니다.

- Windows 98 계열 중에서도 가장 널리 쓰이고 있는 Windows 98 SE (Second Edition)를 대상으로 하였습니다.

구성

- 가이드라인은 크게 네 부분(계정/패스워드 보안, 네트워크 보안, 바이러스/스파이웨어 보안, 유지/관리 보안)에 총 21개 항목으로 구성되어 있습니다.

- 화면을 활용한 설명을 위주로 하여 초보자들도 쉽게 따라 할 수 있도록 하였습니다.

- 본 가이드라인의 설명 중에 활용된 응용 프로그램들은 이의 사용을 권장하는 것이 아니며, 설명의 이해도를 높이기 위해 사용한 것입니다. 국가·공공기관에서 보안제품을 사용하기 위해서는 국가정보원 IT보안 인증사무국 (www.kecs.go.kr)을 참조하십시오.

목 차

항 목		페이지
Ⅰ. 계정/패스워드 보안	1. BIOS 비밀번호 사용	4
	2. 화면보호기 패스워드 사용	9
	3. 패스워드 복잡도 강화	13
	4. 패스워드 유효기간 제한	14
	5. 로그온 패스워드 사용	15
Ⅱ. 네트워크 보안	6. 파일 및 프린터 공유 제어	30
	7. 개인방화벽 사용	34
	8. 파일이 첨부된 이메일 열람 주의	42
	9. 메일 클라이언트의 보안설정 강화	43
	10. 웹 브라우저의 보안설정 강화	49
	11. 인터넷을 통한 프로그램 다운로드 주의	54
	12. P2P 프로그램의 사용 제한	56
	13. 시스템 원격 관리 해제	58
Ⅲ. 바이러스/스파이웨어 보안	14. 컴퓨터 백신 프로그램 사용	61
	15. 주기적 바이러스 검사	62
	16. 최신 컴퓨터 백신 엔진 업데이트	65
	17. 컴퓨터 백신 프로그램의 실시간 감시 수행	70
	18. 스파이웨어 탐지/제거 프로그램 사용	73
Ⅳ. 유지/관리 보안	19. 패치 업데이트	75
	20. CD-ROM 자동실행 해제	80
	21. 불필요한 프로그램 제거	83

I. 계정/패스워드 보안

1. BIOS 비밀번호 사용(1/5)

개 요

- BIOS 비밀번호는 하드웨어 즉, 컴퓨터의 메인보드에서 사용자를 확인하는 수단입니다.
  - 패스워드와 비밀번호는 동일한 의미를 가지나, 이 항목의 그림에서 비밀번호라는 용어를 사용하므로 이번 항목에서는 비밀번호라는 용어를 사용합니다.
- BIOS 비밀번호는 메인보드에서 관리하므로 컴퓨터에 전력을 공급하면 바로 입력해야 합니다.

미사용시의 문제점

- 부팅 시 올바른 사용자인지 확인하는 방법이 없습니다.
- 불법적인 사용자에 의한 컴퓨터 사용이 가능해집니다.

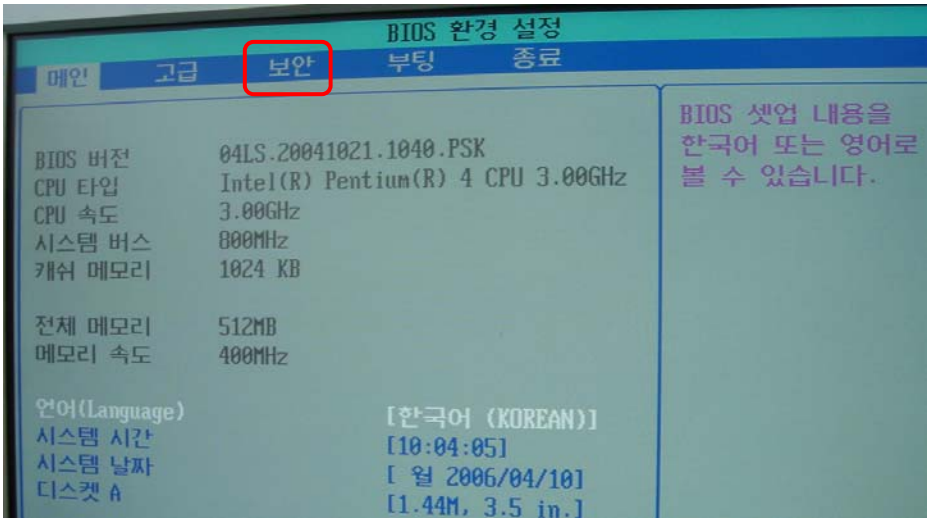
설정방법

주의사항

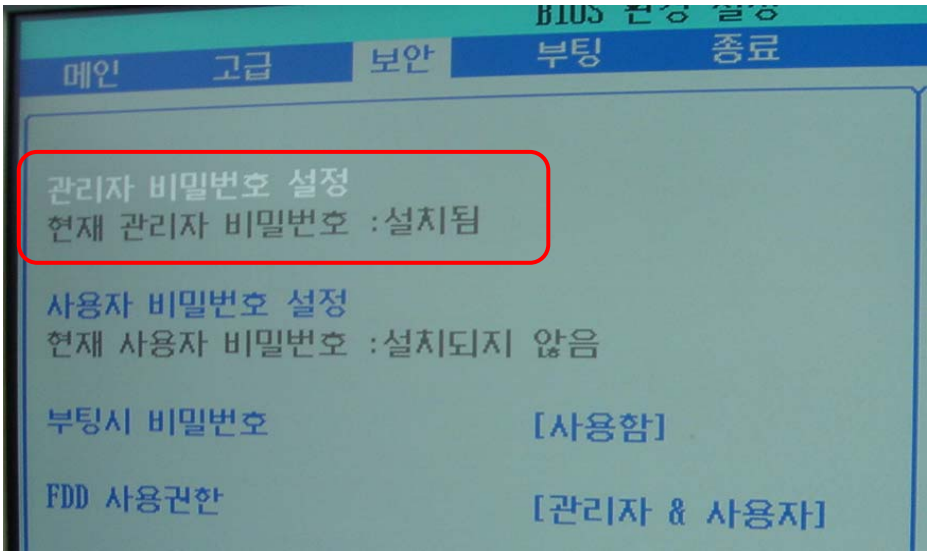
- BIOS 셋업은 주요 하드웨어에 관한 설정값들이 존재하기 때문에 숙련자가 아니면 Password 이외의 값을 수정해서는 안되므로 주의가 요구됩니다.
- 컴퓨터에 따라 BIOS 셋업 화면은 조금씩 다르게 구성되어 있을 수 있습니다.
- 설명에 활용한 화면은 Phoenix BIOS입니다.

1. BIOS 비밀번호 사용(2/5)

- Phoenix BIOS인 경우
  - 기타 다른 종류의 BIOS를 사용하는 경우에는 7~8페이지를 참조하십시오.
  - PC를 켠 후, 부팅 도중에 [F2]키를 누르면 다음과 같은 화면이 시작됩니다.

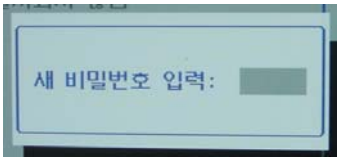


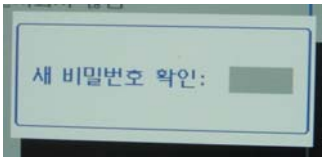
  - BIOS 환경을 설정하는 화면으로 그림의 것은 한글로 설명되어 있으나, 컴퓨터의 기종에 따라 영어로 설명되어 있을 수도 있습니다.
  - 보안(Security) 항목을 선택하면 다음의 화면이 시작됩니다.
  - 항목 선택은 화살표 또는 탭(Tap)키를 이용합니다.



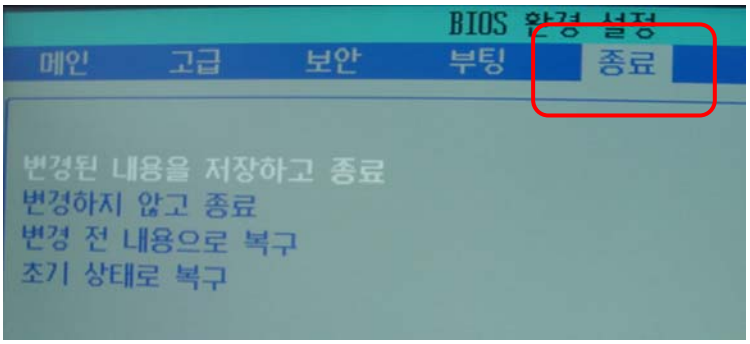
1. BIOS 비밀번호 사용(3/5)

- 현재는 “관리자 비밀번호 설정(Set password)”이 설치되어 있는 것으로 나오는 데, 비밀번호가 설정되어 있지 않은 경우에는 “설치되지 않음”으로 표시됩니다.
- “관리자 비밀번호”를 설정하기 위해서 “관리자 비밀번호 설정”에서 엔터키를 입력하면 다음의 화면처럼 비밀번호를 입력하라는 화면이 보이고, 이 화면에 비밀번호를 입력하면 재확인 화면이 다시 보이며, 이 화면에도 동일한 비밀번호를 입력해야 합니다.





- 종료(Exit) 메뉴에서 “변경된 내용을 저장하고 종료(Save Change & Exit)”를 선택하여 빠져 나옵니다.

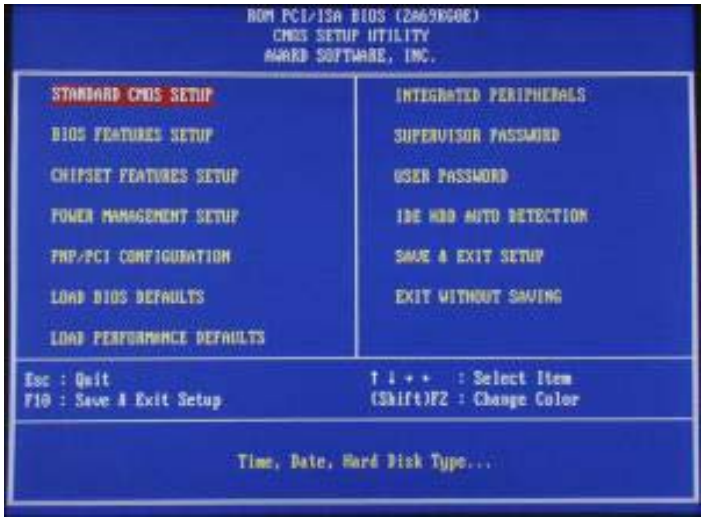


- 비밀번호가 설정된 후부터는 컴퓨터를 부팅하려면 다음의 화면과 같이 비밀번호를 입력하는 화면이 보입니다.

1. BIOS 비밀번호 사용(4/5)

- 이때에 올바른 비밀번호를 입력하지 못하면 다음과 같은 메시지가 보이며, 올바른 비밀번호를 입력할 때까지 부팅이 이루어지지 않으므로, 사용한 비밀번호는 반드시 기억하고 있어야 합니다.

◆ Award BIOS인 경우



- PC를 켬과 동시에 [DEL](또는 [F1])키를 누릅니다.(윈도우 창이 뜨기 전)
- BIOS Features Setup 항목에서 Security Option을 선택합니다.
- System을 선택합니다.
- Supervisor Password 항목에서 패스워드를 입력합니다.
- Confirm Password에 한번 더 입력하여 확인합니다.
- Save & Exit[F10]하여 종료합니다.

1. BIOS 비밀번호 사용(5/5)

◆ AMI BIOS인 경우

- PC를 켠 후 [DEL]키를 누릅니다.
- CMOS 설정화면(메인화면)이 시작됩니다.
- Advanced BIOS Features 항목에서 Password Check 항목을 Always로 선택합니다.
- [ESC]를 눌러 상위항목(메인화면)으로 이동합니다.
- Set Supervisor Password에서 패스워드를 설정합니다.
- Save & Exit[F10]하여 종료합니다.

2. 화면보호기 패스워드 사용(1/4)

개 요

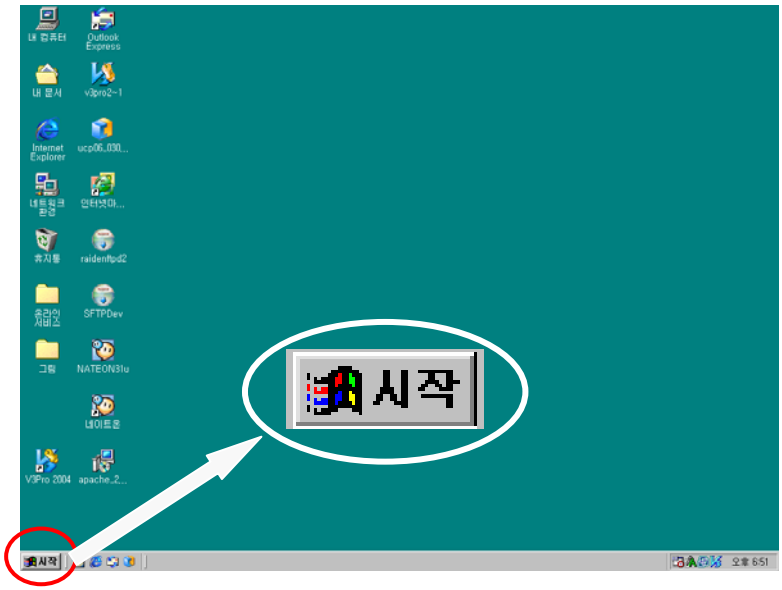
- 일정시간 동안 사용자의 동작이 없는 경우에 Windows 98 운영체제는 이를 사용자가 자리에 없는 것으로 판단하고, 모니터 화면에 보여지고 있는 내용의 노출과 불법사용자에 의한 컴퓨터 사용을 방지하기 위하여 특정 영상을 화면에 보여주는 기능을 수행하는 데, 이를 화면보호기라고 합니다.
- 사용자가 자리에 없는 것으로 판단하는 대기 시간과 보호화면의 종류 그리고, 패스워드의 적용 여부는 사용자가 선택할 수 있습니다.

미사용시의 문제점

- 사용자가 없을 때 화면에 보여지는 내용을 모든 사람이 열람할 수 있으며, 불법적인 사용자에 의한 컴퓨터 사용이 가능해집니다.

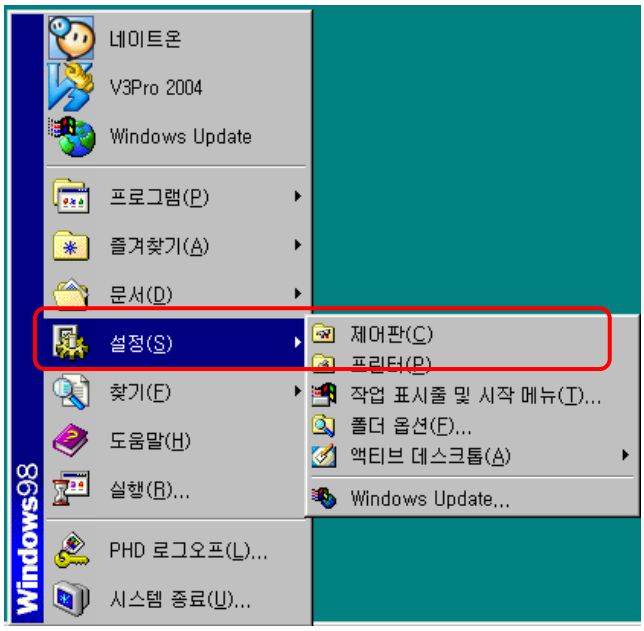
설정방법

- 「제어판」 창 열기
  - 바탕화면의 좌측 하단에 있는 "시작" 버튼을 찾아 클릭합니다.



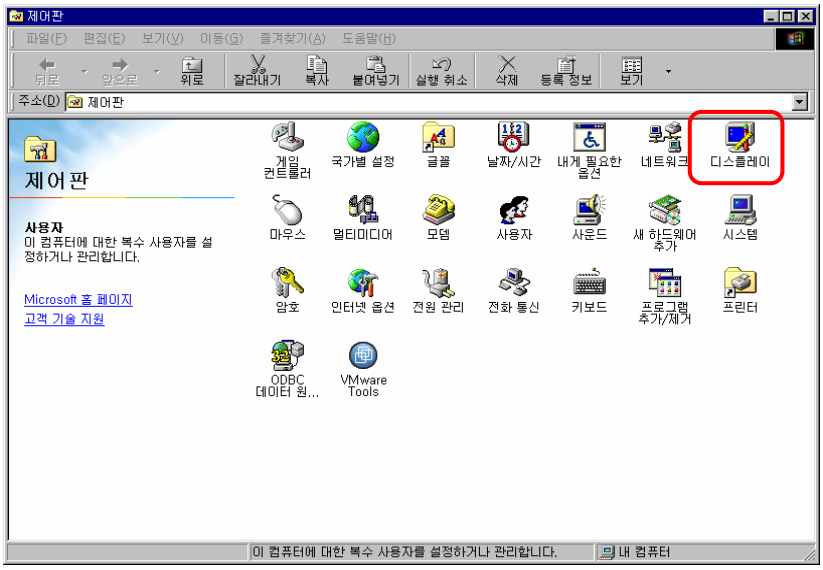
2. 화면보호기 패스워드 사용(2/4)

- "시작" 버튼 클릭 후 보이는 메뉴에서 "설정" → "제어판"을 클릭합니다.



◆ 화면보호기 설정을 위한 창으로 이동

- 「제어판」 창에서 "디스플레이"를 선택합니다.



2. 화면보호기 패스워드 사용(3/4)

◆ 화면보호기 설정

① 「디스플레이 등록 정보」 창에서 "화면보호기" 탭을 선택합니다.

② "화면보호기(S)"에서 원하는 보호화면을 선택합니다.

③ "대기(W)"에서 원하는 대기시간을 분단위로 선택합니다.

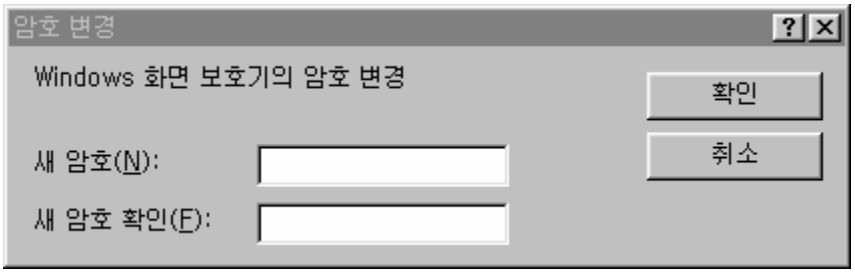
- 선택한 시간 동안 사용자의 동작이 없으면 화면보호기가 작동됩니다.

④ "암호사용(P)"의 체크박스를 설정합니다.

- 이를 설정하지 않으면 누구나 동작중인 화면보호기를 해제할 수 있습니다.

2. 화면보호기 패스워드 사용(4/4)

⑤ “변경(C)...” 을 클릭하면 다음의 「암호 변경」 창이 시작되며, 이곳에 화면보호기 암호를 입력합니다.



- Windows 98은 로그온 패스워드(15페이지 참조)와 화면보호기 패스워드가 별개이므로 두 개를 별도로 설정해 주어야 합니다.

3. 패스워드 복잡도 강화(1/1)

개 요

- 컴퓨터에서 사용하는 패스워드는 복잡한 것을 사용할수록 안전합니다.
- 단순한 조합이나 일련의 번호/문자들은 공격자가 쉽게 추측할 수 있어서 패스워드 본래의 기능을 제공하지 못합니다.
- 특히, 복잡한 패스워드를 사용한다고 하여 어딘가에 패스워드를 적어 놓는 행위는 가장 위험한 것 중의 하나이므로 조심해야 합니다.

미사용시의 문제점

- 복잡하지 않은 패스워드를 사용하면 공격자가 패스워드를 쉽게 추측할 수 있어 이를 악용하여 컴퓨터 해킹이 가능합니다.

안전한 패스워드 사용방법

- 숫자/문자(대문자, 소문자 구별)/특수문자(!@#$%^&* 등등)를 조합하여 최소 8자리 이상으로 사용하십시오.
- 로그온 패스워드 변경방법은 “5. 로그온 패스워드 사용(15 페이지)”를 참조하십시오.
- 화면보호기 패스워드 변경방법은 “2. 화면보호기 패스워드 사용(9페이지)”를 참조하십시오.

4. 패스워드 유효기간 제한(1/1)

개 요

- 복잡한 패스워드를 사용하고 있어도 하나의 패스워드를 너무 오랜 기간 사용하게 되면 다른 사람에게 노출될 가능성이 높아집니다.
- 하나의 패스워드가 사용되는 기간을 제한하고, 그 이후에는 다른 패스워드로 변경하여 노출 가능성을 감소시켜 안전성을 높일 필요가 있습니다.

장기간 사용시의 문제점

- 주위 인물에 의한 추측 가능
  - 비교적 긴 길이의 패스워드라 할지라도 입력하는 모습을 주위 사람이 반복하여 보게 되면 추측이 가능할 수 있습니다.
- 스니핑에 의한 노출 가능
  - 해킹기술의 일종인 스니핑은 일종의 도청기술로, 사용자의 컴퓨터에서 송·수신되는 데이터의 내용을 공격자에게 불법적으로 전달해 주는 기술입니다.
  - 패스워드도 스니핑에 네트워크에서 노출될 수 있습니다.

설정방법

- 모든 패스워드는 3개월을 주기로 변경해 주는 것이 안전합니다.

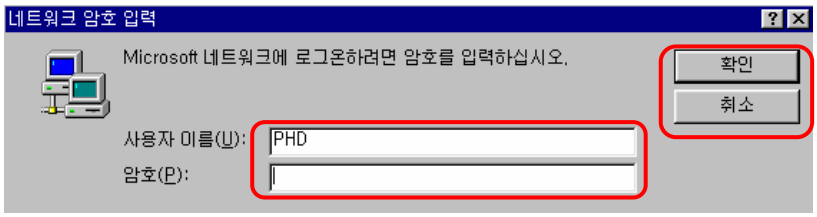
5. 로그온 패스워드 사용(1/14)

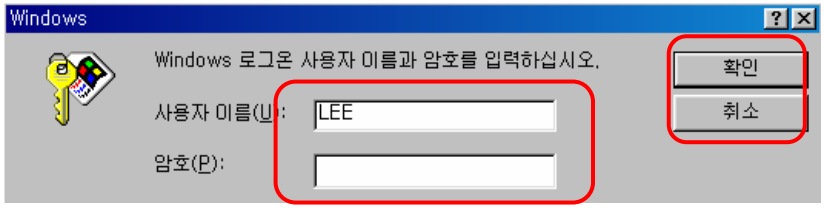
개 요

- 로그온 패스워드란 컴퓨터가 사용자를 확인하는 수단으로써, 등록된 사용자만 컴퓨터를 사용할 수 있도록 해주는 기능입니다.
  - 이 항목에서 보여지는 창에서는 "암호"라는 용어를 사용하고 있으나, 일반적으로 "패스워드"라는 용어가 많이 사용되므로, 설명에서는 "패스워드"를 사용합니다.
- 로그온 창에서 사용자는 자신의 "사용자 이름(ID)"과 "암호(패스워드)"를 입력하여 컴퓨터에 접근하게 됩니다.
- Windows 98은 로그온 패스워드 기능 없이 컴퓨터를 사용할 수 있어서 보안상의 많은 문제점을 유발시키고 있습니다.

미사용시의 문제점

- 로그온 패스워드를 사용하지 않으면 부팅중에 다음의 그림과 같은 「네트워크 암호 입력」 창이나 기본 로그온 창이 열릴 때에, 패스워드를 입력하지 않고 "확인" 또는 "취소" 버튼을 클릭해서 사용자 확인을 피할 수 있습니다.
- 결과적으로 불순한 의도를 가진 사용자를 포함하여 누구나 컴퓨터를 불법적으로 사용할 수 있는 환경이 제공됩니다.





5. 로그온 패스워드 사용(2/14)

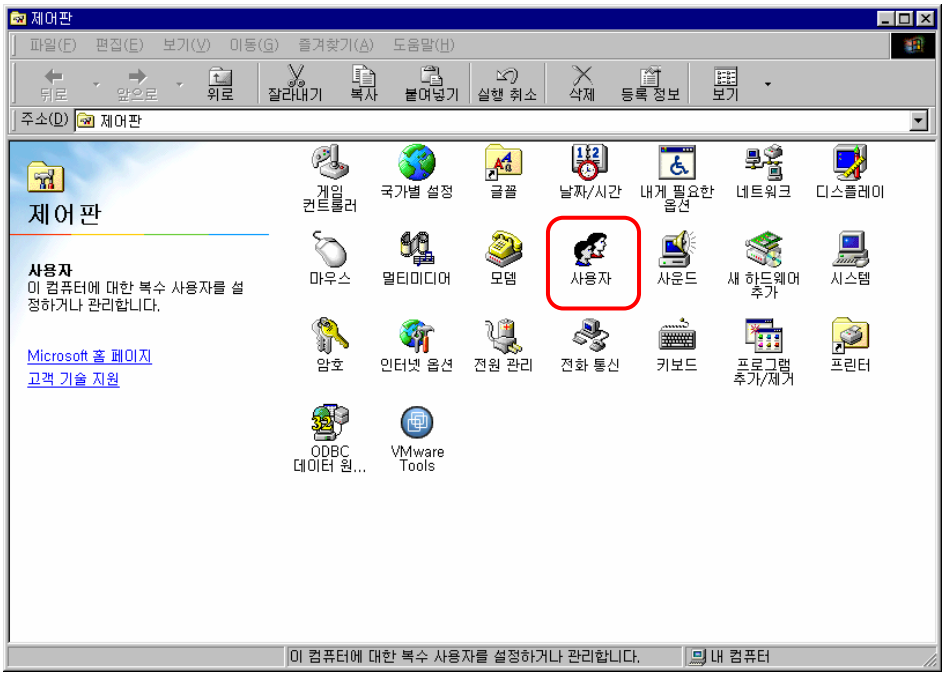
설정방법

경 고 문 : 다음 사항을 꼭 읽어 주십시오!

- 컴퓨터 관리 담당자와 상의 후에 이 항목을 설정하십시오.
- 이 항목을 설정하려면 Windows 98 SE 설치 CD가 반드시 있어야 합니다.
- 설치 CD가 없는 경우에는 이 항목을 설정하지 마십시오.
- 설명된 순서가 지켜지지 않으면 컴퓨터 사용이 불가능해질 수도 있습니다.

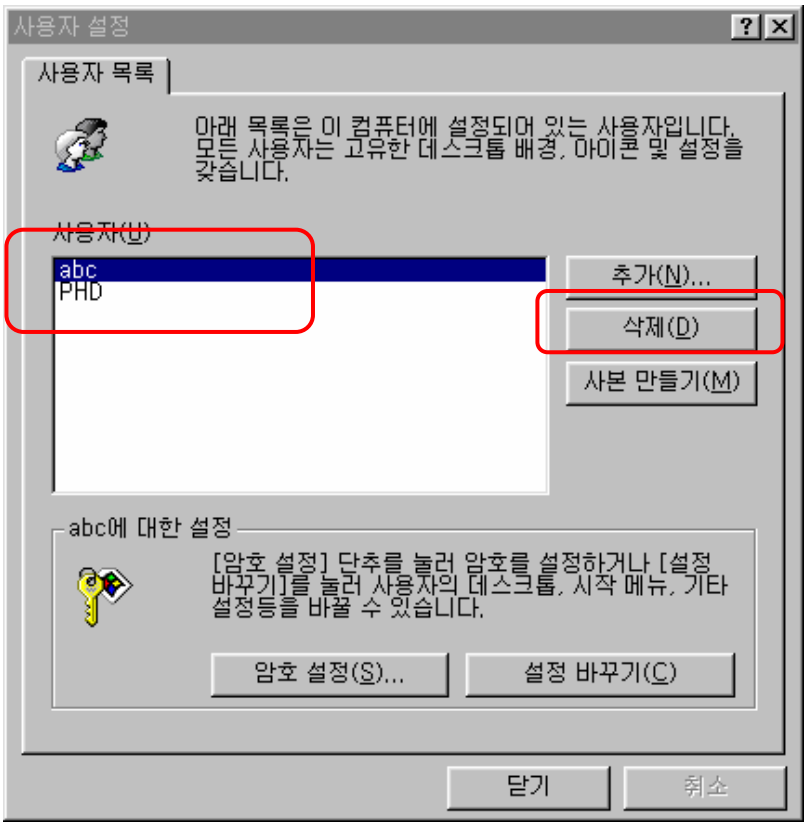
5. 로그온 패스워드 사용(3/14)

- 로그온 패스워드를 설정하기 위해서는 “사용자 정리”, “Microsoft 패밀리 로그온 설치”, “레지스트리값 변경” 과정을 모두 수행해야 합니다.
- 등록된 사용자가 없거나 변경해야 하는 경우에는 “사용자 추가” 과정이 필요합니다.
  - “사용자 추가”의 설명에 패스워드를 설정하는 설명도 포함되어 있습니다.
- 사용자 정리
  - 로그온 패스워드를 사용할 사용자만 남기고 나머지 계정을 모두 지우는 과정입니다.
  - 「제어판」 창에서 “사용자” 항목을 선택하여 실행합니다.



5. 로그온 패스워드 사용(4/14)

- 「사용자 설정」 창이 열리며 현재 컴퓨터에 등록되어 있는 사용자의 리스트가 보입니다.

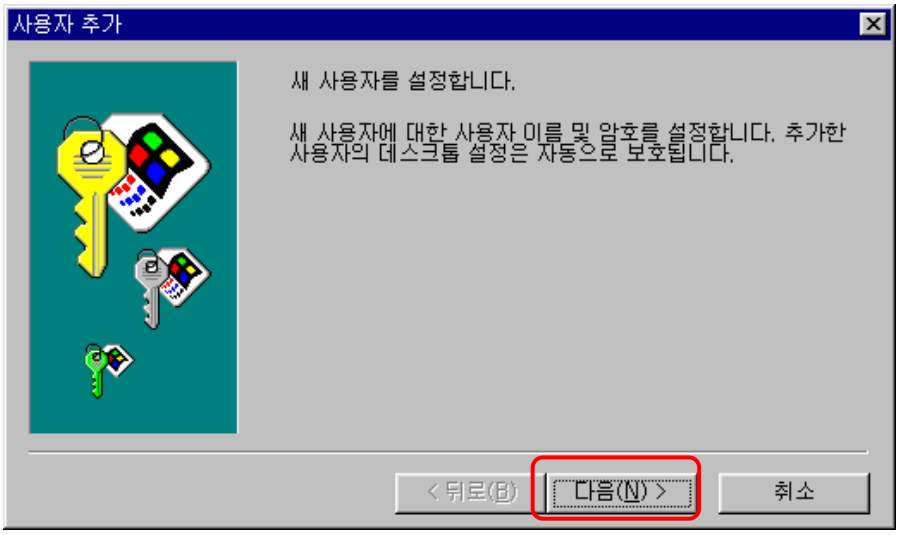


- 시스템에 등록되어 있는 사용자들 중에서 불필요한 사용자를 제거합니다.
- 불필요한 사용자를 선택하고 “삭제(D)”를 클릭하면 선택된 사용자가 제거됩니다.

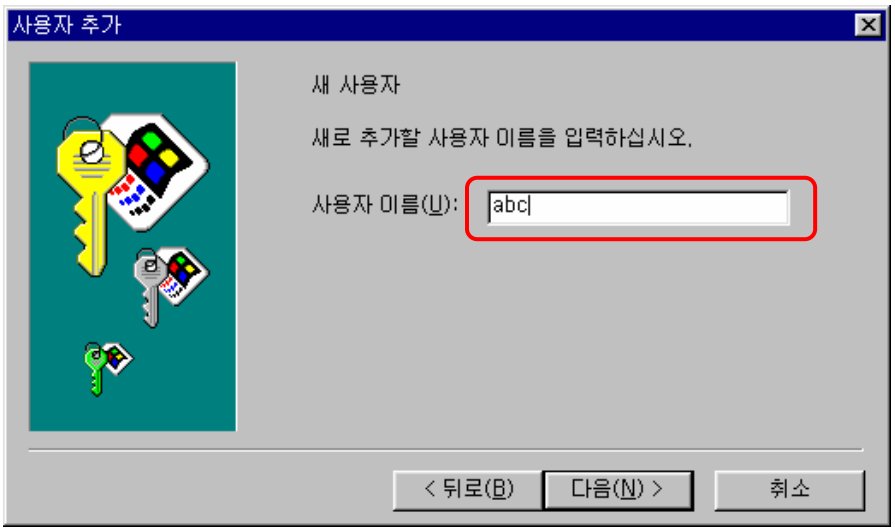
5. 로그온 패스워드 사용(5/14)

◆ 사용자 추가

▶ 시스템에 등록되어 있는 사용자가 없거나 새롭게 사용자를 추가하는 경우에는 18페이지의 「사용자 설정」 창에서 "추가(N)" 버튼을 클릭하면 다음과 같은 「사용자 추가」 창이 열리며, 이 창에서 "다음(N)" 버튼을 클릭합니다.

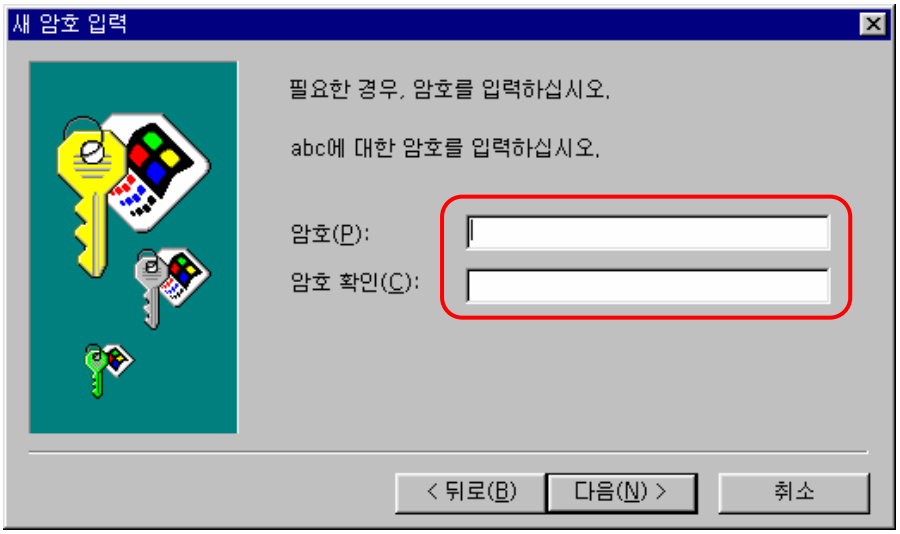


▶ 아래 그림의 창에서 사용할 사용자 이름을 입력하고 "다음(N)" 버튼을 클릭합니다.

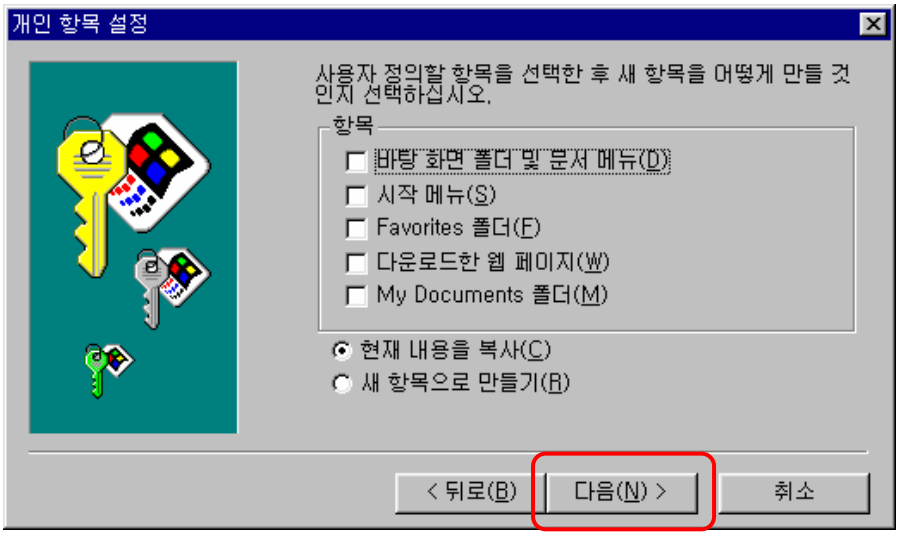


5. 로그온 패스워드 사용(6/14)

- 사용자 이름을 입력한 후에는 암호를 입력하는 「새 암호 입력」 창이 열리는데, 이 창에서 암호를 입력하고 "다음(N)"을 클릭합니다.

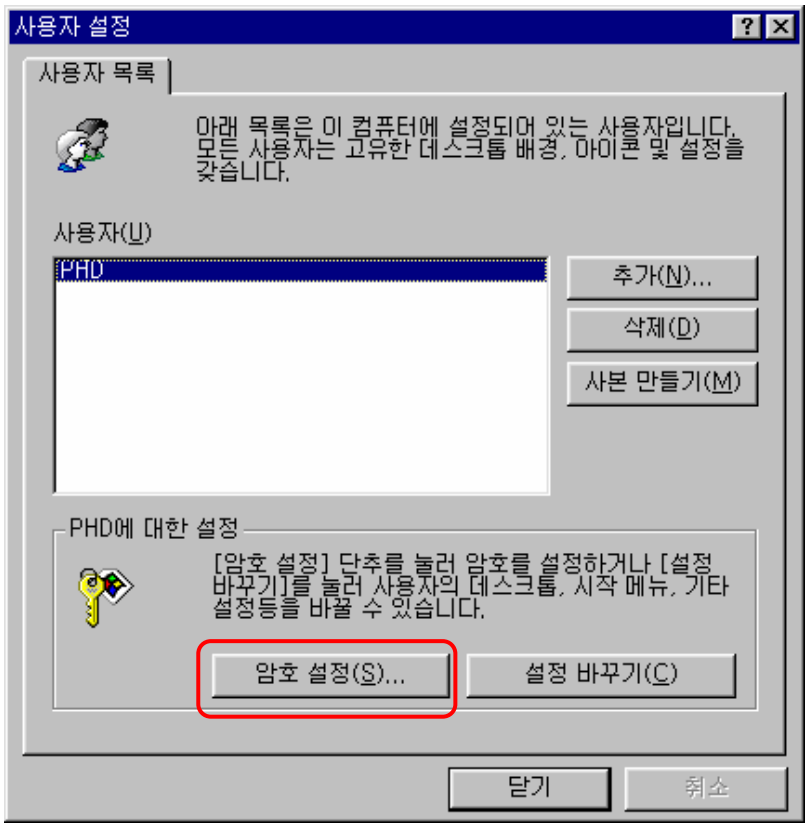


- 암호를 입력한 후에 나오는 「개인 항목 설정」 창에서 "다음(N)" 버튼을 클릭합니다.

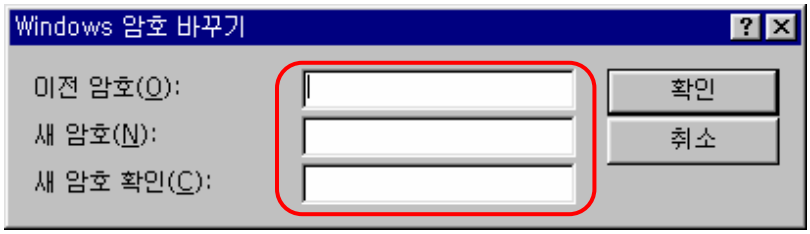


5. 로그온 패스워드 사용(7/14)

- 이미 등록되어 있는 사용자의 패스워드를 변경하기 위해서는 「사용자 설정」 창에서 사용자를 선택한 후, "암호 설정(S)" 버튼을 클릭합니다.

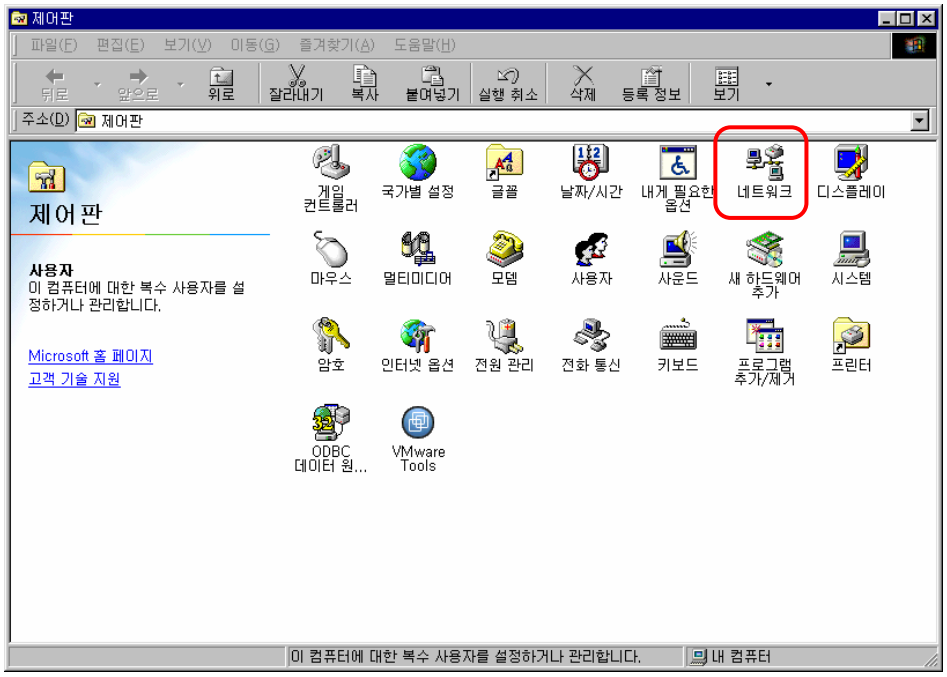


- 「Windows 암호 바꾸기」 창에서 "이전 암호(O)"와 "새 암호(N)", "새 암호 확인(C)"을 차례대로 입력하고 "확인" 버튼을 클릭합니다.

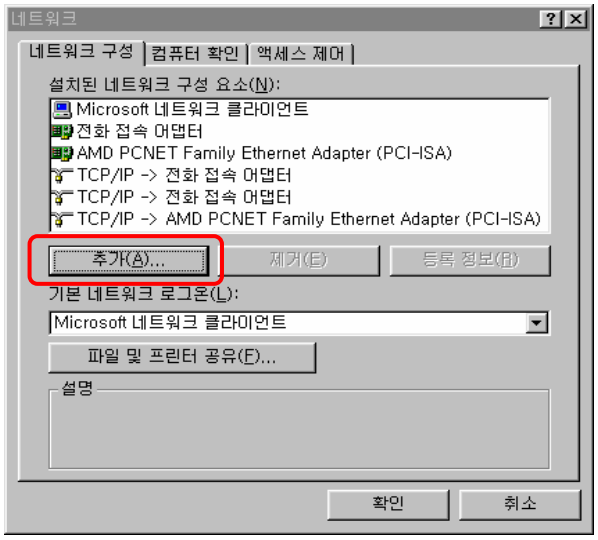


5. 로그온 패스워드 사용(8/14)

- Microsoft 패밀리 로그온 설치
  - 「제어판」 창을 엽니다.(9페이지 참조)
  - 「제어판」 창에서 "네트워크" 아이콘을 선택하여 실행합니다.

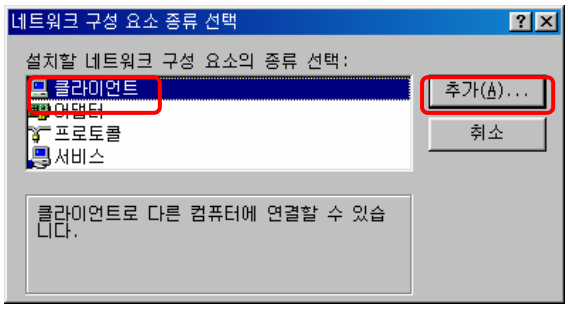


  - 「네트워크」 창에서 "추가(A)" 버튼을 선택하여 실행합니다.

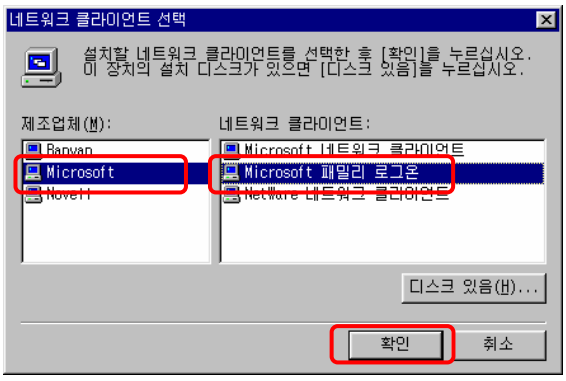


5. 로그온 패스워드 사용(9/14)

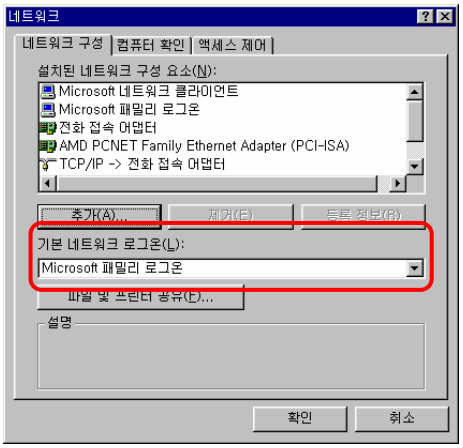
- 「네트워크 구성 요소 종류 선택」 창에서 “클라이언트”를 선택하고 “추가(A)” 버튼을 클릭합니다.



- 제조업체를 “Microsoft”로 선택하고 “네트워크 클라이언트”에서 “Microsoft 패밀리 로그온”을 선택하고 “확인”을 클릭합니다.
- 프로그램 설치를 위해서는 Windows 98 SE 의 설치 CD가 필요합니다.



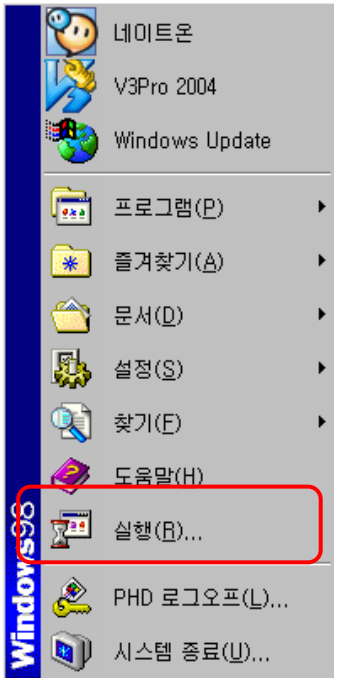
- 재부팅 이전에 「네트워크」 창에서 “기본 네트워크 로그온”을 반드시 “Microsoft 패밀리 로그온”으로 설정해야 합니다.



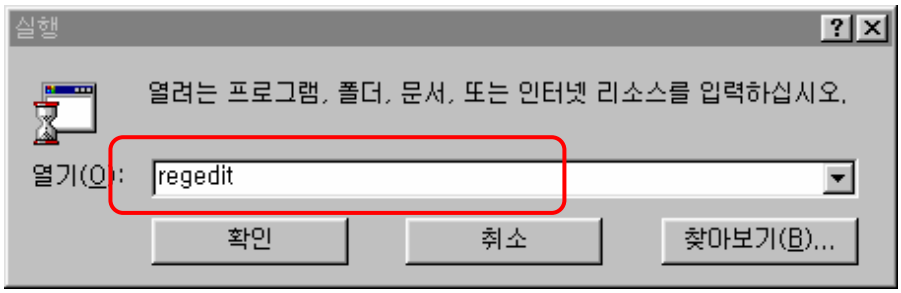
5. 로그온 패스워드 사용(10/14)

◆ 레지스트리값 변경

▶ “시작” → “실행” 메뉴를 클릭합니다.

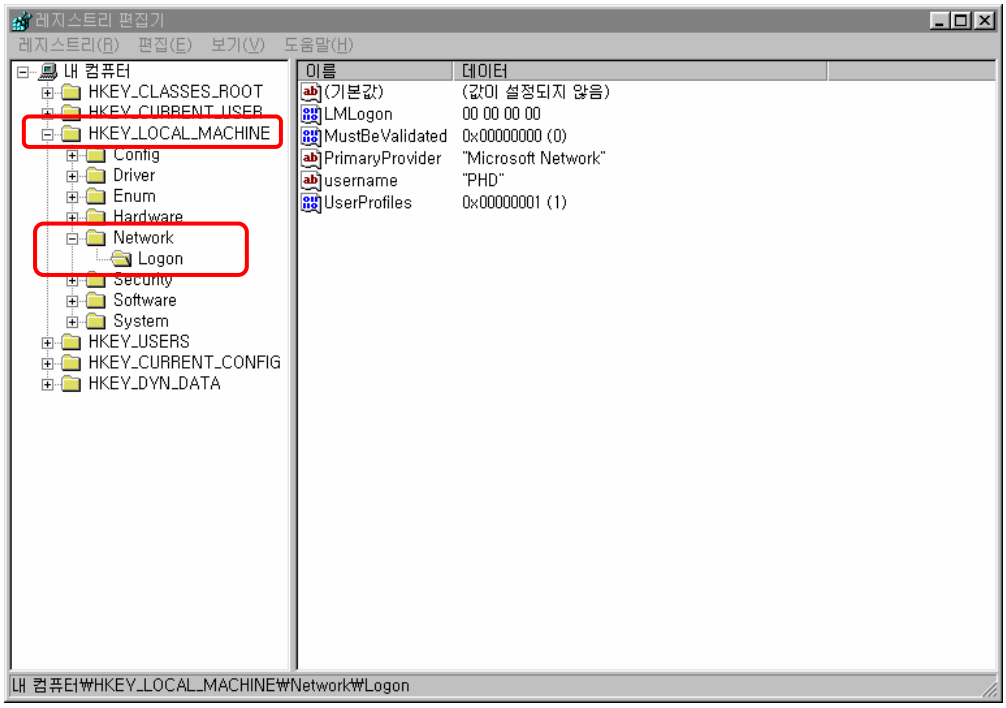


▶ 「실행」 창이 열리면 “regedit” 명령어를 입력하고 “확인” 버튼을 클릭합니다.

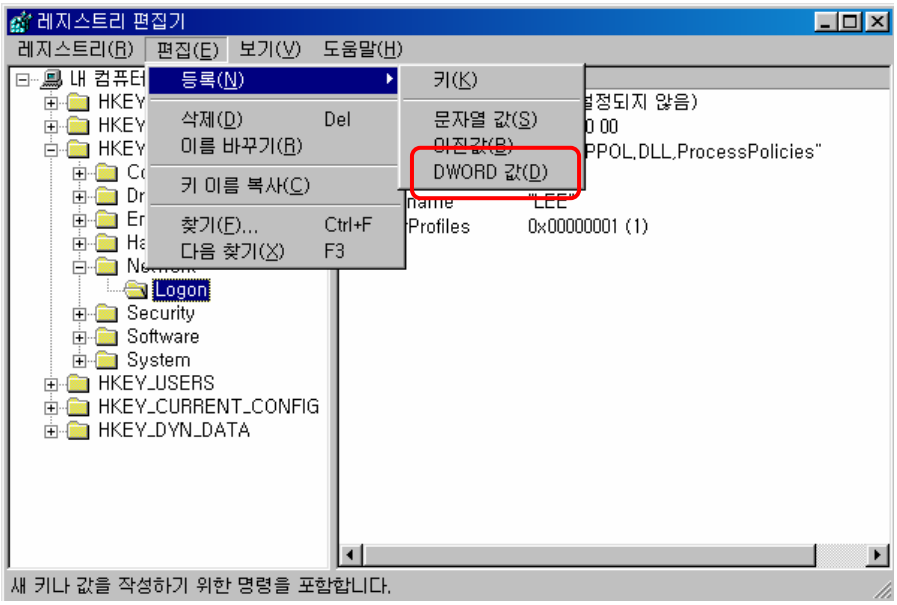


5. 로그온 패스워드 사용(11/14)

- 「레지스트리 편집기」 창에서 “HKEY_LOCAL_MACHINE” → “Network” → “Logon”을 선택합니다.

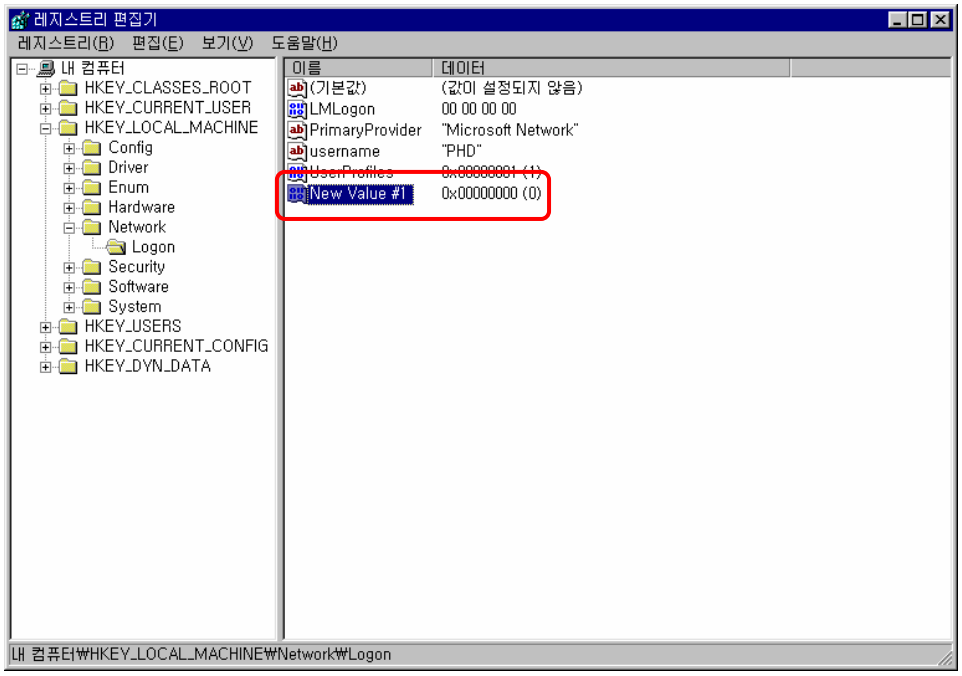


- “편집(E)” → “등록(N)” → “DWORD값(D)”을 선택합니다.

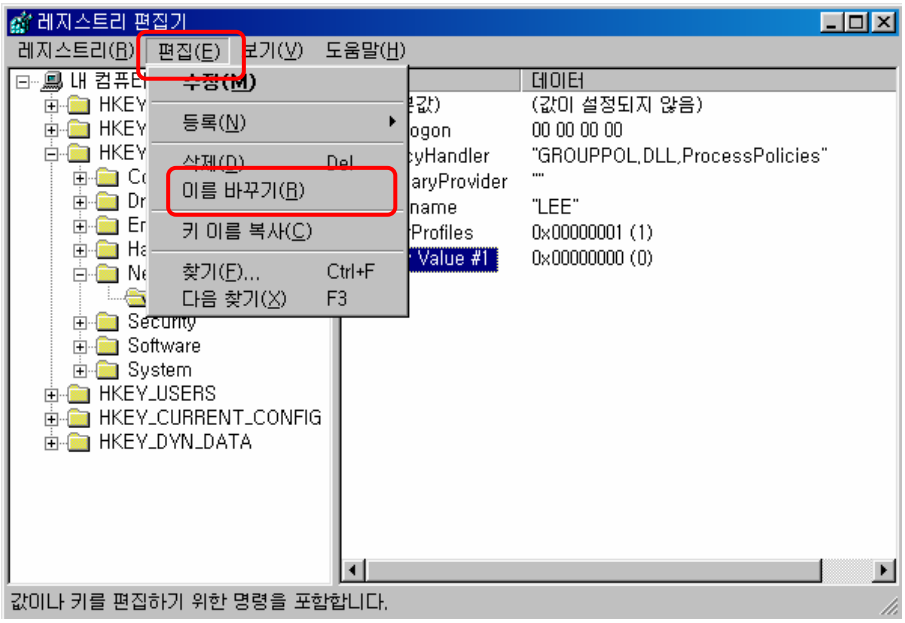


5. 로그온 패스워드 사용(12/14)

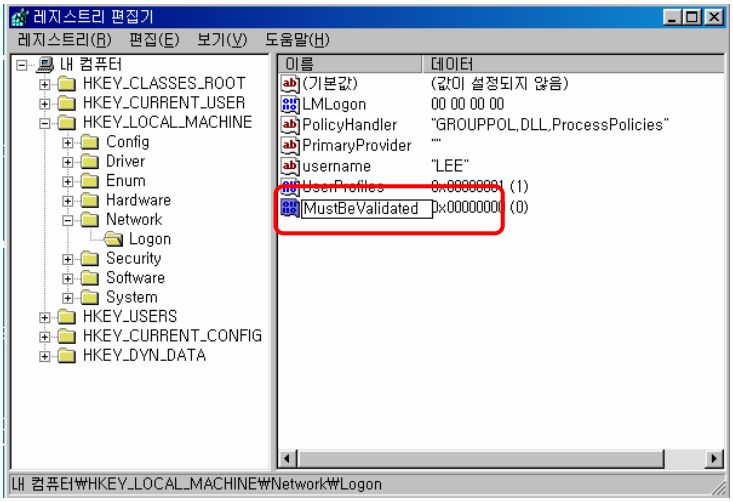
- "New Value #1" 항목이 생성됩니다.



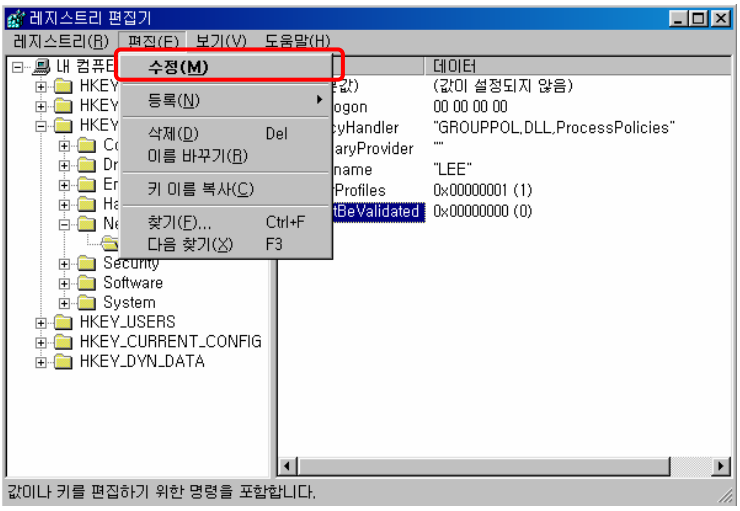
- 생성된 "New Value #1"을 선택하고, "편집(E)" → "이름바꾸기(R)"를 선택하여 이름을 "MustBeValidated"로 변경합니다.



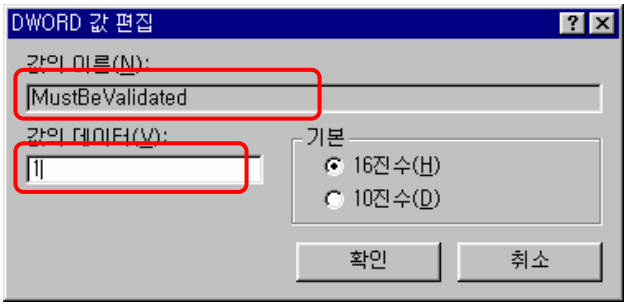
5. 로그온 패스워드 사용(13/14)



- "MustBeValidated"항목을 선택하고 "편집(E)" → "수정(M)"을 선택합니다.

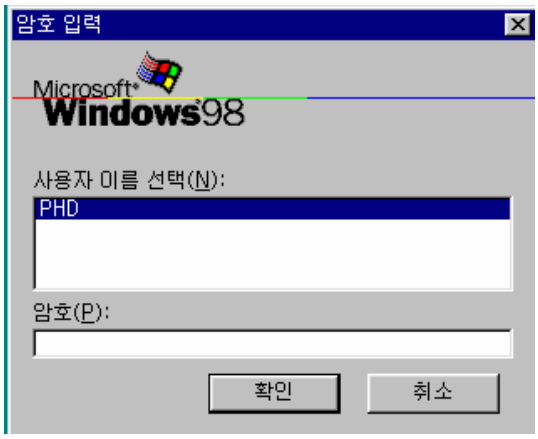


- "값의 데이터(V)" 부분을 "1" 로 설정하여 레지스트리값 변경을 완료합니다.



5. 로그온 패스워드 사용(14/14)

- 설치 및 설정을 완료하고, 컴퓨터가 재부팅되면 다음과 같은 「암호 입력」창이 보이는 데, 이 창에서 정확한 암호(패스워드)를 입력해야 컴퓨터를 사용할 수 있습니다.
  - 사용자가 여러 명인 경우에는 사용자를 선택하고 그에 맞는 암호(패스워드)를 입력해야 합니다.



II. 네트워크 보안

6. 파일 및 프린터 공유 제어(1/4)

개 요

- Windows 98 에서는 사용의 편의를 위해 파일이나 프린터를 다른 사용자들과 공유하여 사용하는 기능을 제공합니다.
- 그러나 공유 기능의 부주의한 사용은 정보 유출 등의 문제를 발생시킬 수 있습니다.
- 가급적 공유 기능을 사용하지 않는 것이 안전하며, 불가피하게 파일을 공유하고자 하는 경우에는 안전대책을 마련한 후에 사용하는 것이 바람직합니다.

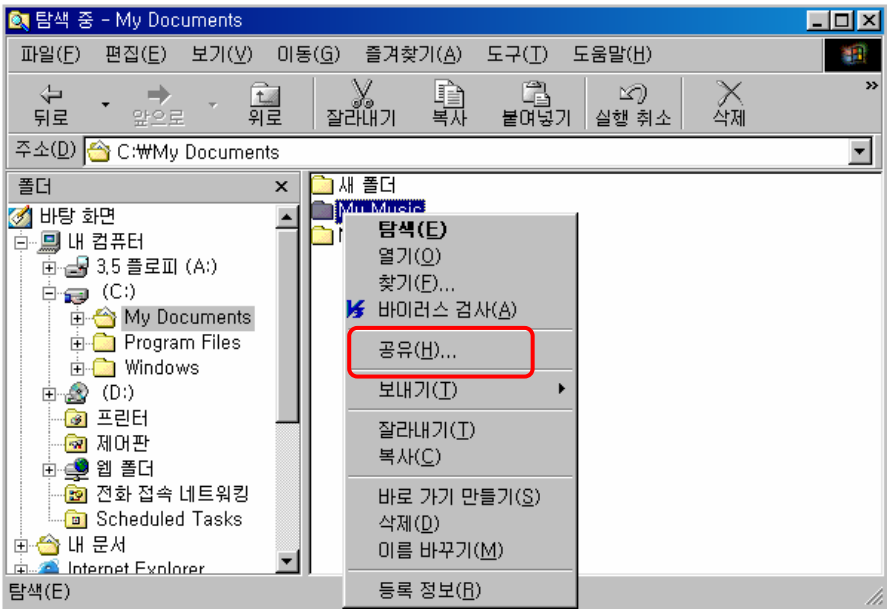
부주의한 공유의 문제점

- 중요정보가 유출될 수 있습니다.
- 잠깐 동안의 공유를 위해 설정한 후에, 해제하지 않은 상황에서 공유폴더에 중요자료를 저장할 수 있으며, 공유를 위한 패스워드를 설정하지 않았다면 관계없는 타인이 중요자료를 가져갈 수 있어 그 위험성은 더욱 커지게 됩니다.
- 해킹의 수단이 되기도 합니다.

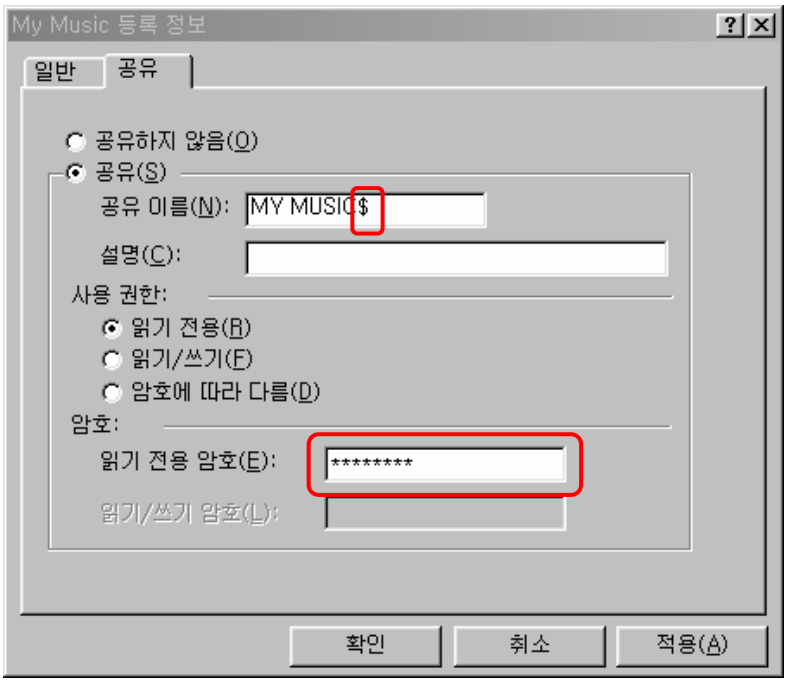
권장하는 공유 방법

- 공유가 불가피하게 필요한 경우에는 이 방법을 따라 주십시오.
- 「Windows 탐색기」에서 공유를 원하는 폴더를 찾아 폴더 위에 마우스 포인터를 위치한 다음 오른쪽 마우스 버튼을 클릭하고, “공유”를 선택합니다.

6. 파일 및 프린터 공유 제어(2/4)



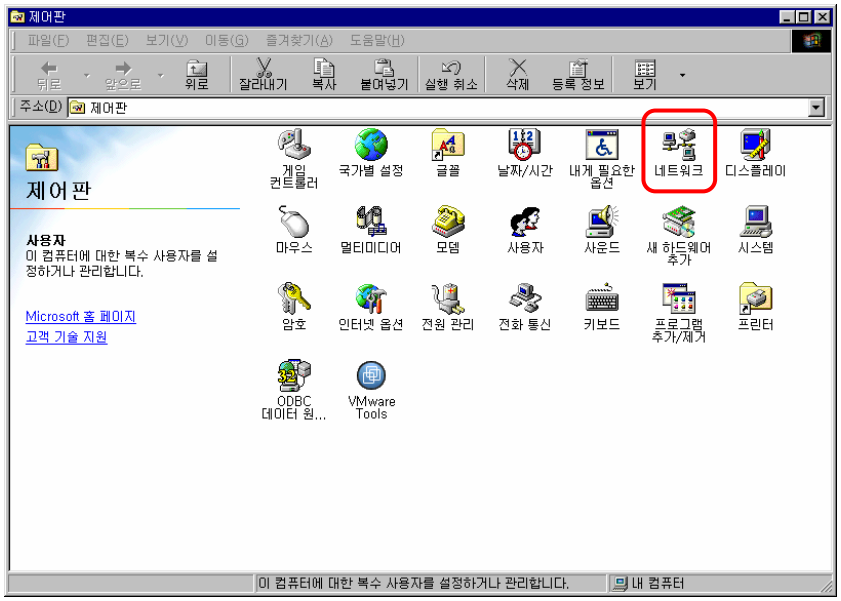
- 공유이름 뒤에 “$”표시를 붙이고, 암호를 설정하시시오.
  - 다른 컴퓨터에서는 이 공유폴더가 보이지 않게 되어, 공유폴더의 이름을 아는 사용자만 접근할 수 있게 보호됩니다.

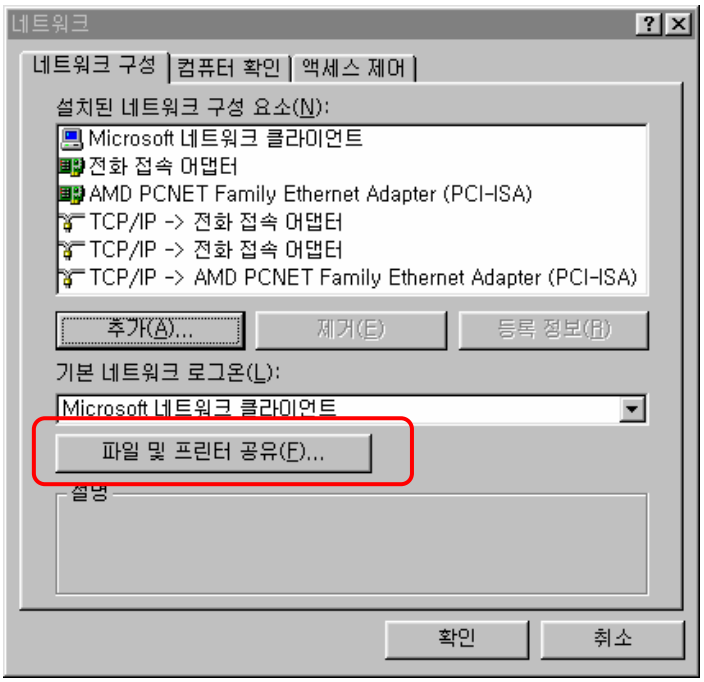


6. 파일 및 프린터 공유 제어(3/4)

공유를 차단하는 방법

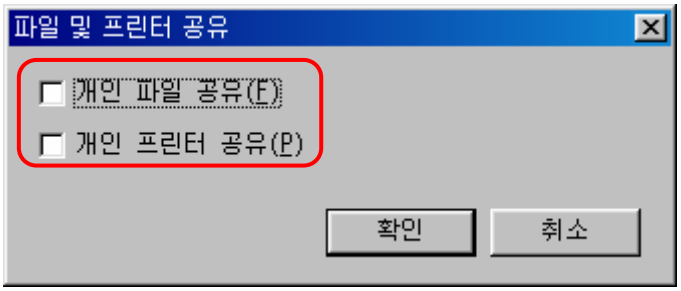
- 「제어판」 창을 엽니다.(9페이지 참조)
- 「제어판」 창에서 “네트워크”를 선택하여 「네트워크」 창을 엽니다.



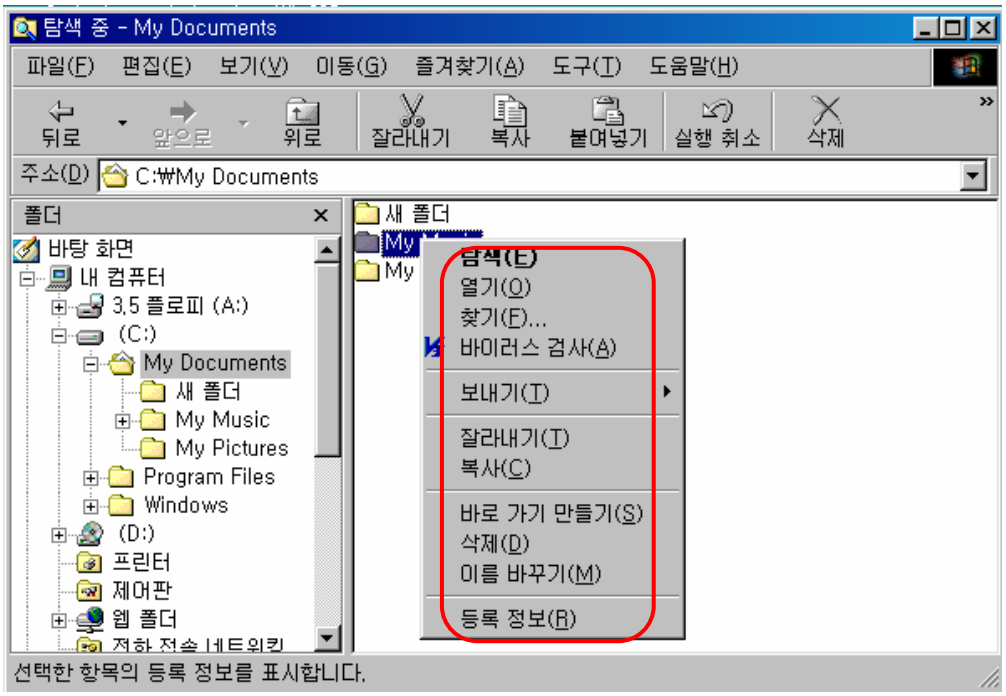


6. 파일 및 프린터 공유 제어(4/4)

- 「네트워크」 창에서 “파일 및 프린터 공유(F)”를 선택합니다.



- “개인 파일 공유”와 “개인 프린터 공유” 모두를 해제합니다.
- 설정한 후에 컴퓨터를 재부팅합니다.
- 파일이나 폴더의 공유를 위한 메뉴가 보이지 않게 됩니다.



7. 개인방화벽 사용(1/8)

개 요

- 네트워크 방화벽 이외에 개인이 사용하는 컴퓨터에 별도로 방화벽 프로그램을 설치하여 더욱 안전하게 할 수 있습니다.
- Windows 98은 방화벽을 제공하지 않습니다. 따라서 보안을 위해서 개인방화벽을 설치하여 사용하는 것이 더욱 안전합니다.

주의사항

- "상용 정보보호 시스템 적합성 검증제도"란 국가·공공기관이 도입하고자 하는 상용 정보보호 시스템의 보안기능과 국가정보통신망에 대한 적합성을 검증하기 위해 『국가 정보보안 기본지침』(06.1.1)에 의거하여 시행하는 제도입니다.
- "상용 정보보호시스템 적합성 검증제도"를 통과한 제품에 대한 정보는 국가정보원 IT보안 인증사무국(www.kecs.go.kr)에서 열람할 수 있습니다.
- 본 가이드라인에서는 Zone Alarm 프로그램을 이용하여 설명하고 있습니다. 이는 개인 방화벽에 대한 이해도를 높이기 위한 방법이며, 반드시 이 제품의 사용을 권장하는 것은 아닙니다.
- 프리웨어 제품은 개인적 용도와 비사업용으로만 사용해야 합니다.

네트워크 방화벽의 한계

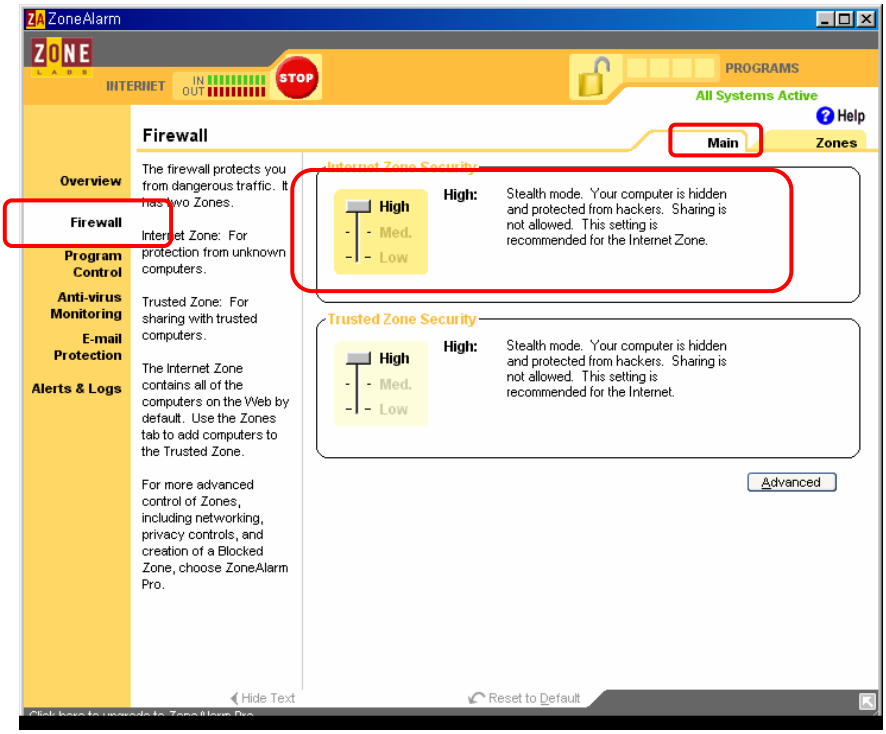
- 제한적 기능
  - 웜·바이러스를 차단하기가 어렵습니다.

7. 개인방화벽 사용(2/8)

- 내부 네트워크에서의 공격
  - 내부 네트워크에 있는 공격자는 네트워크 방화벽의 통제를 받지 않고 다른 사용자의 PC 등에 공격 수행이 가능합니다.

사용방법

- 등급조정

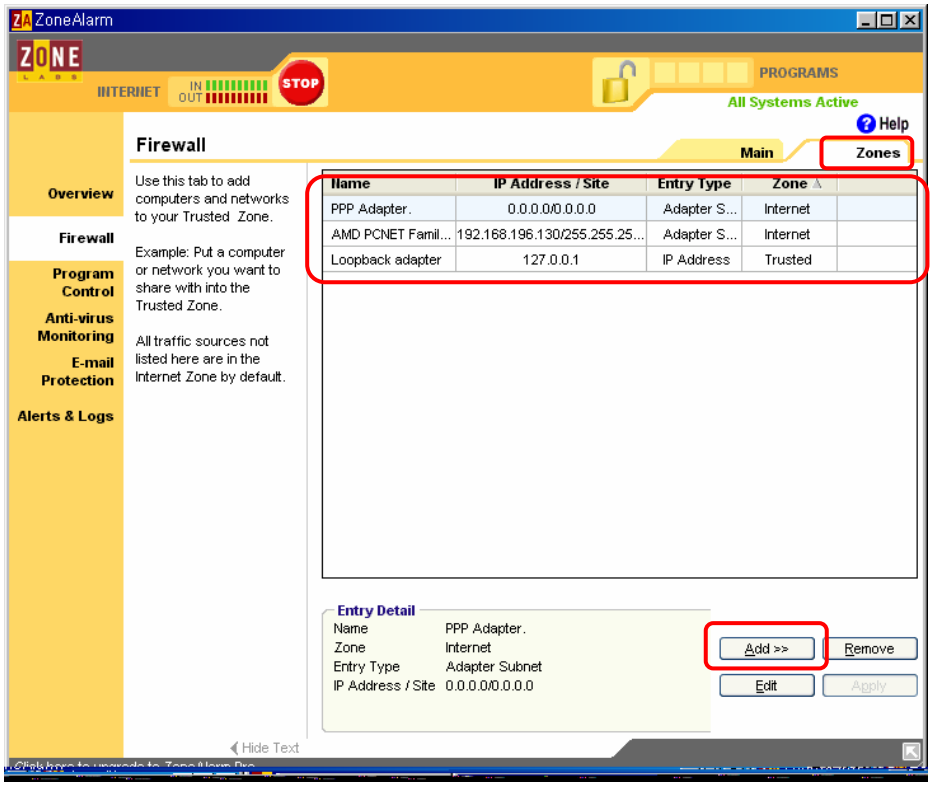


  - 개인방화벽의 접근통제 수준을 지정하는 화면입니다.
  - 창 우측 상단의 “Main”탭을 선택하여 지정합니다.
  - “High”, “Medium”, “Low”로 구분되며, “High”일수록 강력한 접근통제를 실시하여 안전합니다.

7. 개인방화벽 사용(3/8)

◆ 세부 설정

▶ 앞페이지의 창 우측 상단의 “Zones”탭을 선택하면 다음의 창이 시작됩니다.



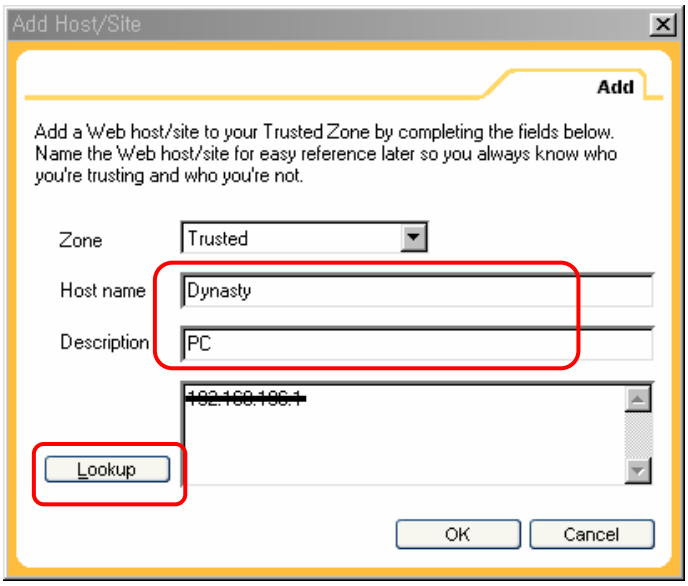
▶ 사용자가 특별히 접근을 허용할 컴퓨터들을 지정할 수 있습니다.

▶ 이미 지정되어 있는 세 개의 값은 기본값으로 변경할 수 없습니다.

▶ 화면 우측 하단의 “Add”를 선택하여 새로운 값을 추가할 수 있는 데, “Host/Site”, IP Address, IP Range, Subnet”으로 구분하여 등록할 수 있습니다.

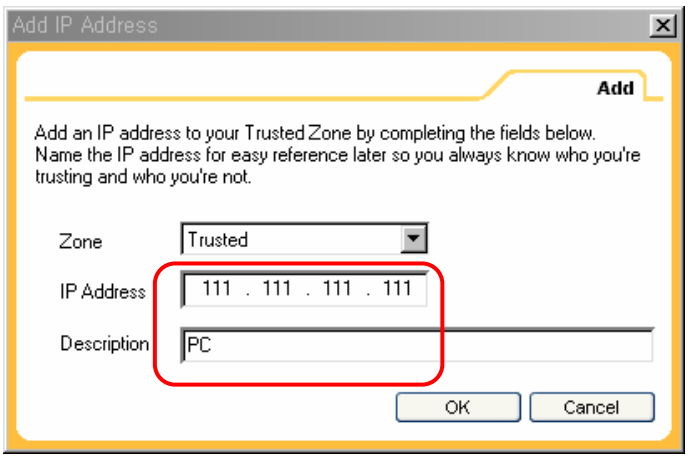
7. 개인방화벽 사용(4/8)

- Host/Site 지정



  - Host name에 컴퓨터 이름을 입력하고, Lookup을 누르면 IP가 찾아집니다.
  - "OK"를 누르면 해당 컴퓨터의 접근을 허용합니다.

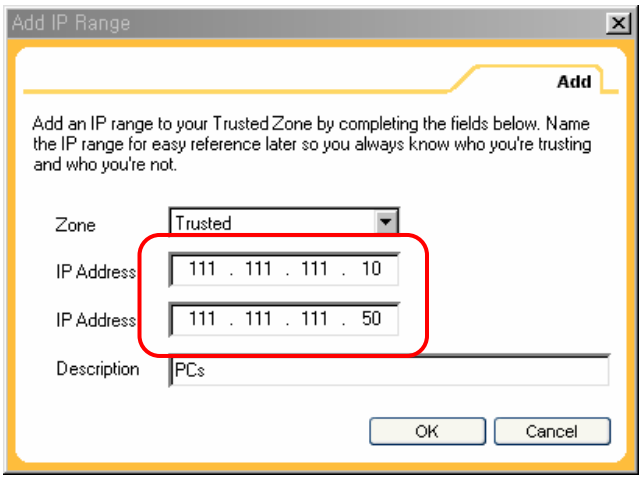
- IP Address 지정



  - IP Address에 IP주소를 입력합니다.
  - "OK"를 누르면 해당 컴퓨터의 접근을 허용합니다.

7. 개인방화벽 사용(5/8)

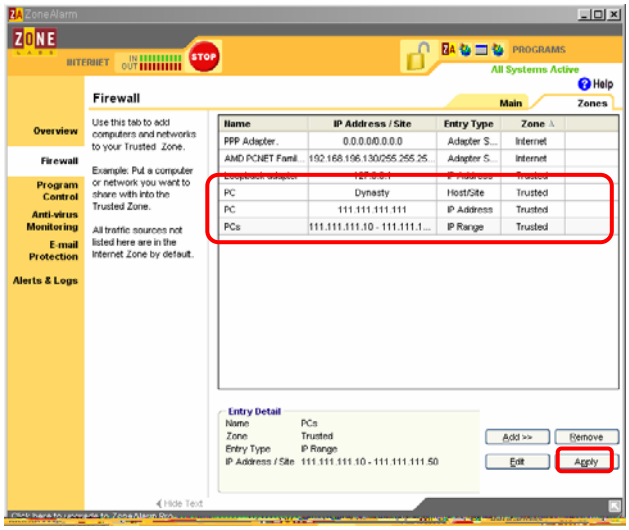
- IP 범위 지정



  - 위의 IP Address에는 네트워크 범위의 시작 IP 주소를, 아래의 IP Address 에는 네트워크 범위의 마지막 IP 주소를 입력합니다.
  - "OK"를 누르면 해당 컴퓨터의 접근을 허용합니다.

- Subnet으로 지정하는 방법은 일반적으로 사용이 많지 않으며, 부주의 시에 개인방화벽의 기능을 훼손할 수 있으므로 설명을 생략합니다.

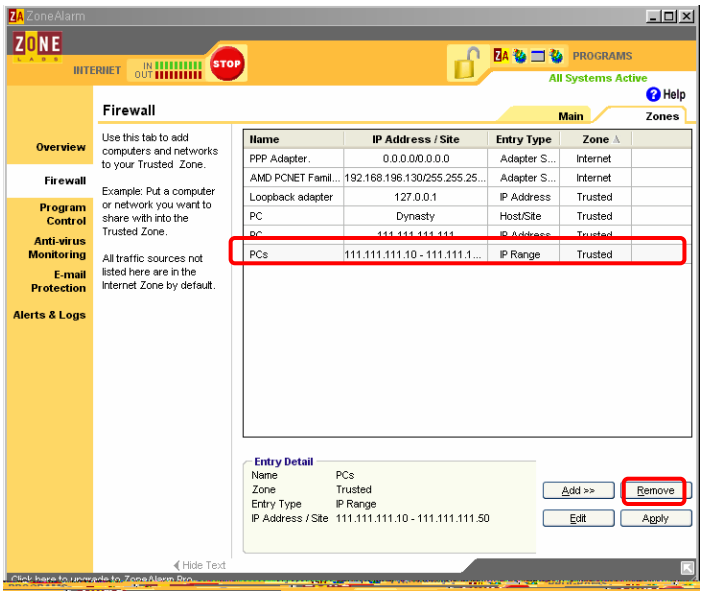
- 적용결과 확인



- 허용할 컴퓨터를 지정한 결과를 확인하고 "Apply"를 클릭하면 지정한 접근 정책이 적용됩니다.

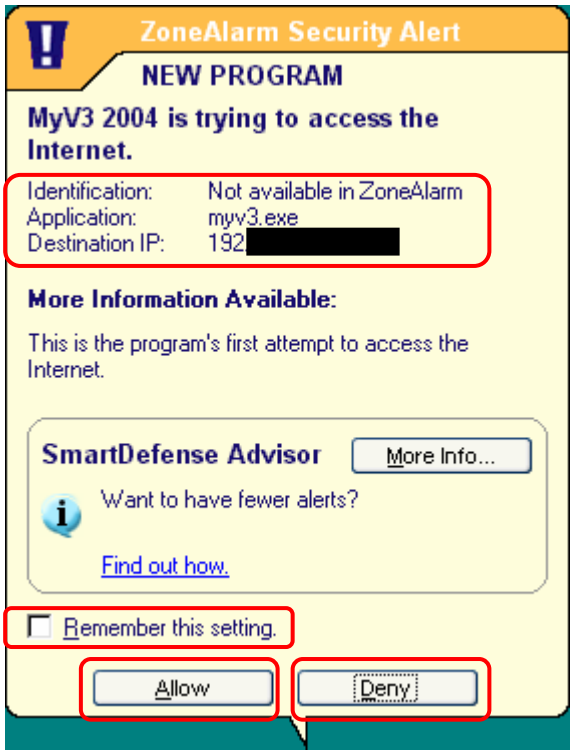
7. 개인방화벽 사용(6/8)

- 허용 지역 제외
  - 제외하고자 하는 리스트를 선택한 후에 화면 좌측 하단의 “Remove” 버튼을 클릭하면 선택된 리스트가 삭제됩니다.



7. 개인방화벽 사용(7/8)

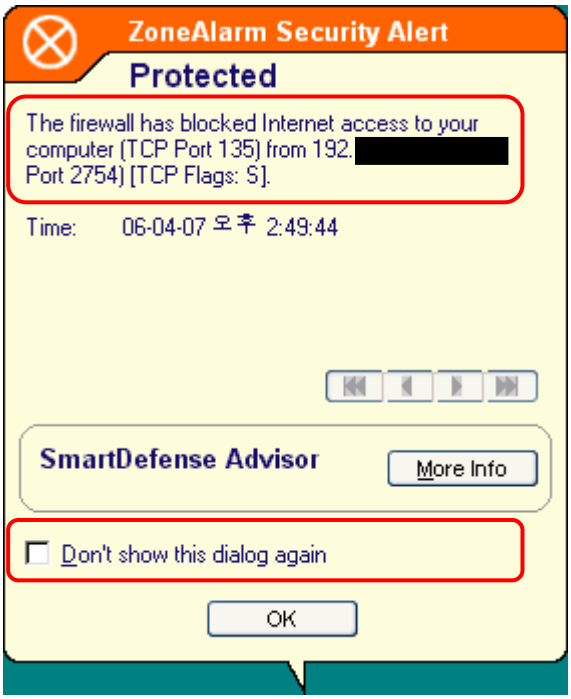
◆ 외부방향 통신 통제



- 컴퓨터 내부에서 외부로의 통신시도를 탐지하고 허용여부를 사용자에게 확인하는 화면입니다.
- "myv3.exe"라는 사용자의 컴퓨터에 설치되어 있는 응용 프로그램이 192.XXX.XXX.XXX로 통신을 시도하는 데, 이를 허용할 것인지를 묻고 있습니다.
- 사용자는 이를 확인하여 정상적인 통신인 경우에는 허용(Allow)하고, 확인되지 않아 의심되는 통신이라면 거부(Deny)할 수 있습니다.
- 지속적으로 허용/거부 할 것인가에 대해 하단에 위치한 "Remember this setting" 박스를 체크해서 결정할 수 있습니다.

7. 개인방화벽 사용(8/8)

◆ 내부방향 통신 통제



- 외부에서 컴퓨터로의 통신시도가 있어서 이를 차단했다는 내용을 나타내는 화면입니다.
- IP주소가 192.XXX.XXX.XXX인 외부의 컴퓨터에서 사용자의 컴퓨터로 135번 포트를 통해 접속시도가 탐지되어 이를 차단했다는 내용입니다.
- 마찬가지로 하단에 위치한 “Don’t show this dialog again”을 설정하면 이와 같은 시도가 다시 발생할 때에는 사용자에게 이러한 메시지를 보여 주지 않고 자동으로 통신시도를 차단한다는 의미입니다.

8. 파일이 첨부된 이메일 열람 주의(1/1)

개 요

- 공격자는 이메일(E-Mail)에 웜·바이러스나 악성 프로그램을 숨겨놓기도 합니다.
- 사용자가 이를 열람하면 자신도 모르는 사이에 피해를 입게 됩니다.
- 따라서 의심되는 이메일은 열어보지 않는 주의가 필요합니다.

부주의시의 문제점

- 이메일 혹은 첨부된 파일을 열 때, 웜·바이러스에 감염될 수 있고 내부에 숨겨진 악성 프로그램으로 인하여 해킹 피해를 당할 수 있습니다.
- 단순히 사용자의 컴퓨터만이 피해를 입는 경우도 있지만, 또 다른 공격을 하기 위한 해킹경유지로도 악용될 수 있습니다.

대응 방법

- 이메일을 보낸 사람의 ID, 이메일의 제목 등이 정상적이지 않다고 판단되면 열람하지 말고 삭제하십시오.
  - 선정적이거나 사행심을 조장하는 제목, 광고 등은 특히 주의하십시오.
  - 평범한 문서파일로 보이는 파일들도 실제로는 악성 프로그램일 가능성이 있으니 주의하십시오.
- 이메일을 보낸 사람의 신원이 확실할 때에만 열람하도록 하십시오.
  - 단, 이메일을 보낸 사람도 악성 프로그램의 피해자일 수 있습니다.
- 첨부된 파일을 열기 전에 바이러스 검사를 수행하십시오.
- 백신 프로그램에서 실시간 감시를 설정하십시오.(70페이지 참조)
- 메일 클라이언트의 보안설정을 강화하십시오.(43페이지 참조)

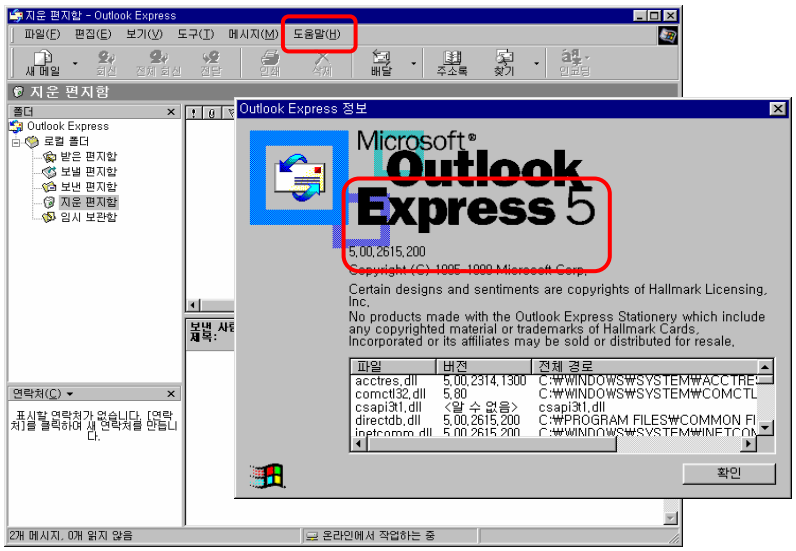
9. 메일 클라이언트의 보안설정 강화(1/6)

개 요

- Windows 98 SE 를 설치하면 메일 클라이언트 프로그램으로 Outlook Express 5.0 이 기본으로 설치됩니다.
- Outlook Express 5.0 은 보안상 취약한 부분이 존재하므로, 6.0 버전으로 업데이트 하고 보안설정을 강화할 필요가 있습니다.

보안설정 강화방법

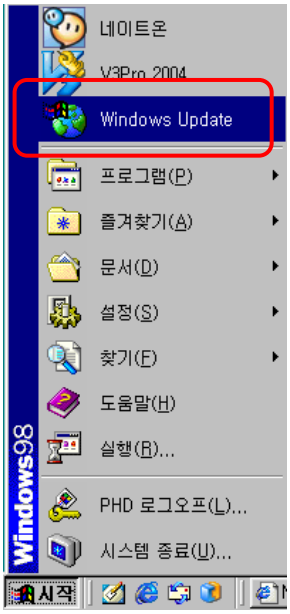
- Outlook Express 6.0 으로 업데이트
  - 설치된 Outlook Express의 버전을 확인합니다.
    - 「Outlook Express」 창에서 "도움말" → "Microsoft Outlook Express 정보(A)"를 클릭하면 현재 설치되어 있는 Outlook Express의 버전을 확인할 수 있습니다.



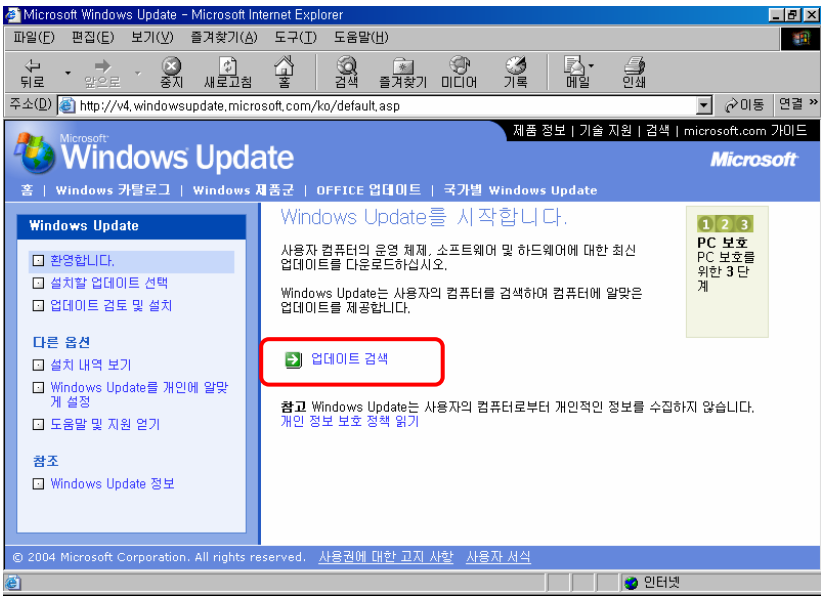
- 버전이 6.0 이하라면 업데이트가 필요합니다.
- 6.0이 이미 설치되어 있다면 이후의 과정은 생략하고, 보안설정(45 페이지) 단계로 넘어가십시오.

9. 메일 클라이언트의 보안설정 강화(2/6)

- Windows Update를 통해 Outlook Express 6.0으로 업데이트합니다.
  - 바탕화면 좌측 하단의 “시작”버튼에서 “Windows Update”를 선택합니다.

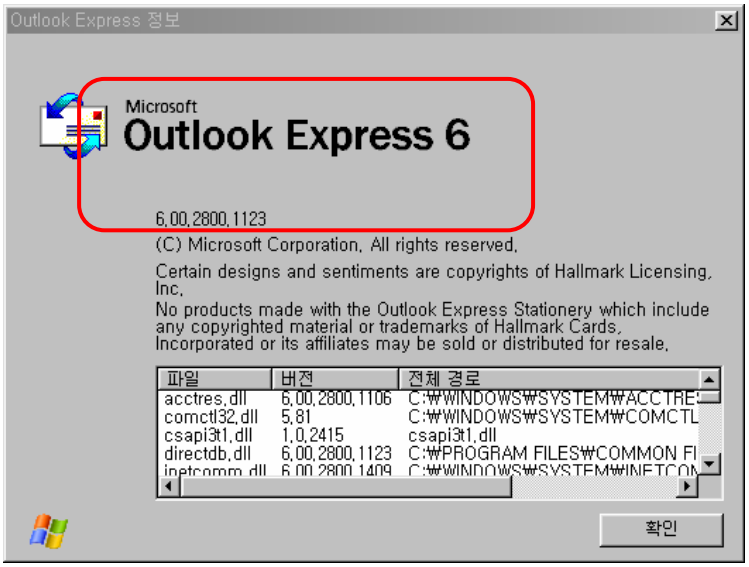


  - Windows Update 홈페이지에서 업데이트를 수행합니다.(자세한 내용은 75페이지를 참조하십시오.)



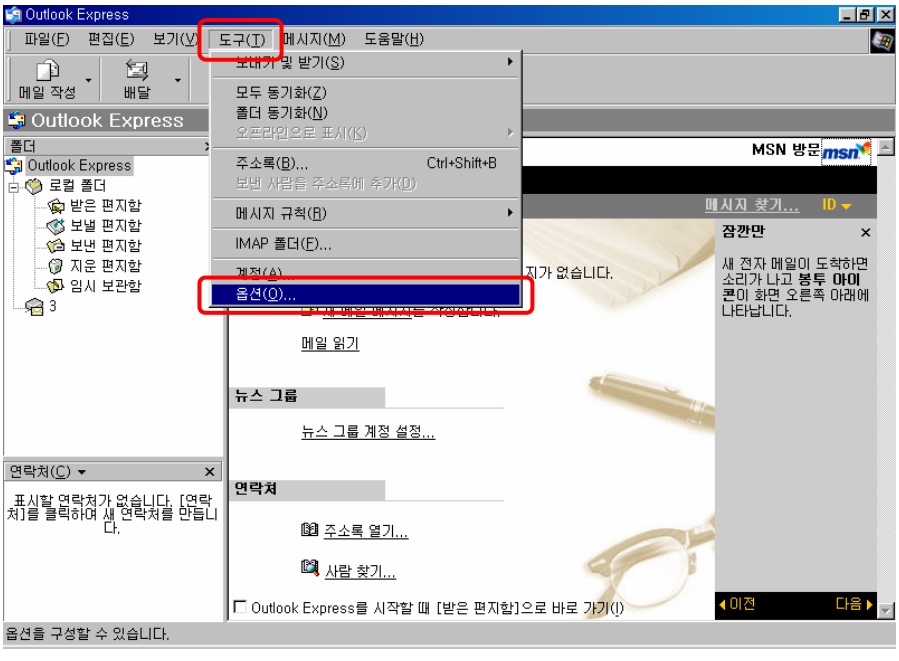
9. 메일 클라이언트의 보안설정 강화(3/6)

- 「Outlook Express」 창에서 “도움말” → “Microsoft Outlook Express 정보(A)”를 클릭하여, Outlook Express의 버전이 6.0으로 업그레이드된 것을 확인합니다.



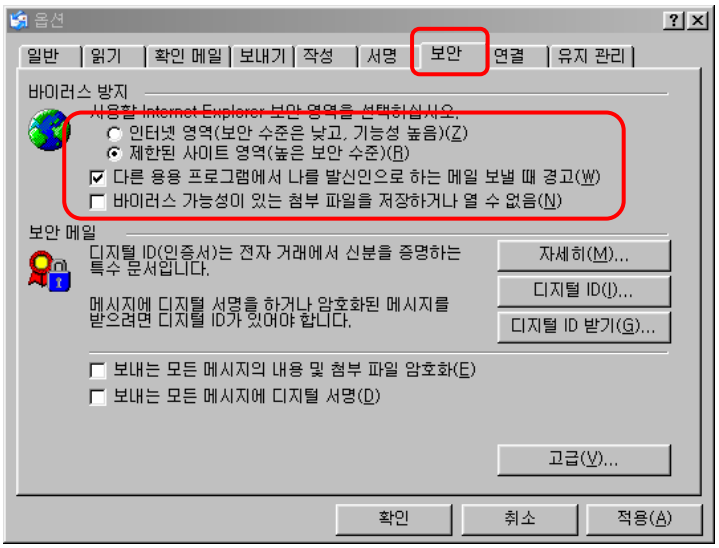
보안설정

- 「Outlook Express」 창 메뉴에서 “도구(T)” → “옵션(O)”을 클릭합니다.

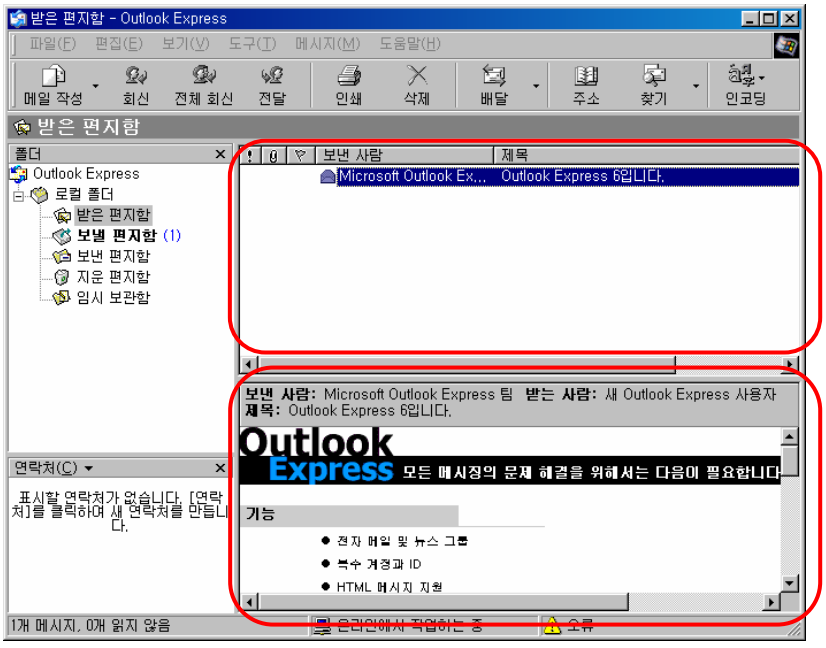


9. 메일 클라이언트의 보안설정 강화(4/6)

- 「옵션」 창에서 "보안" 탭을 누른 후, 아래 그림과 같이 설정합니다.

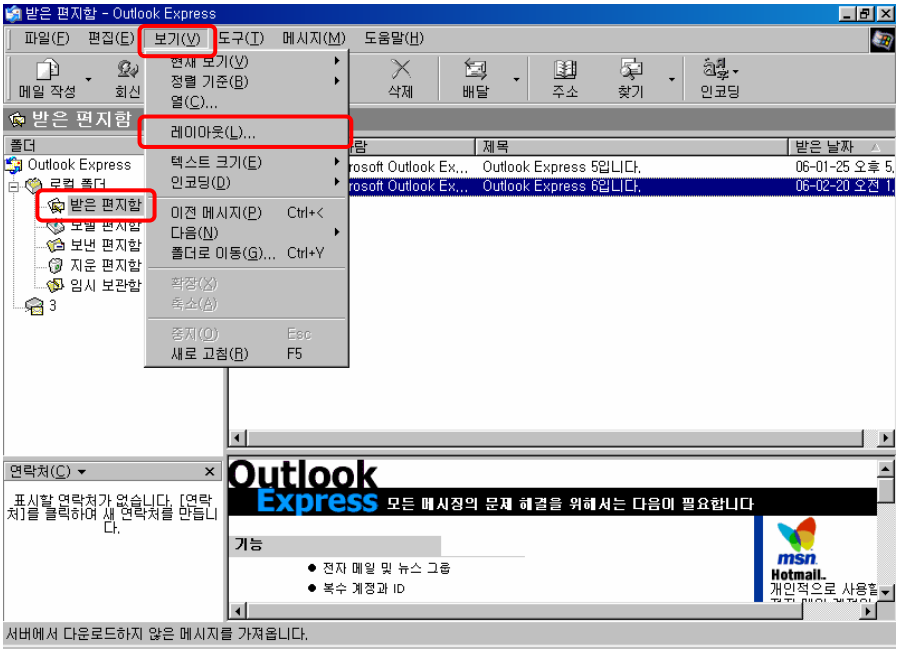


- "미리보기" 해제
  - 미리보기 기능을 해제하여 본문에 숨어 있을 수 있는 악성 프로그램의 실행을 방지합니다.
  - 기본적으로 Outlook Express는 상단에는 이메일의 리스트를, 하단에는 해당 이메일의 미리보기를 보여주도록 설정되어 있습니다.

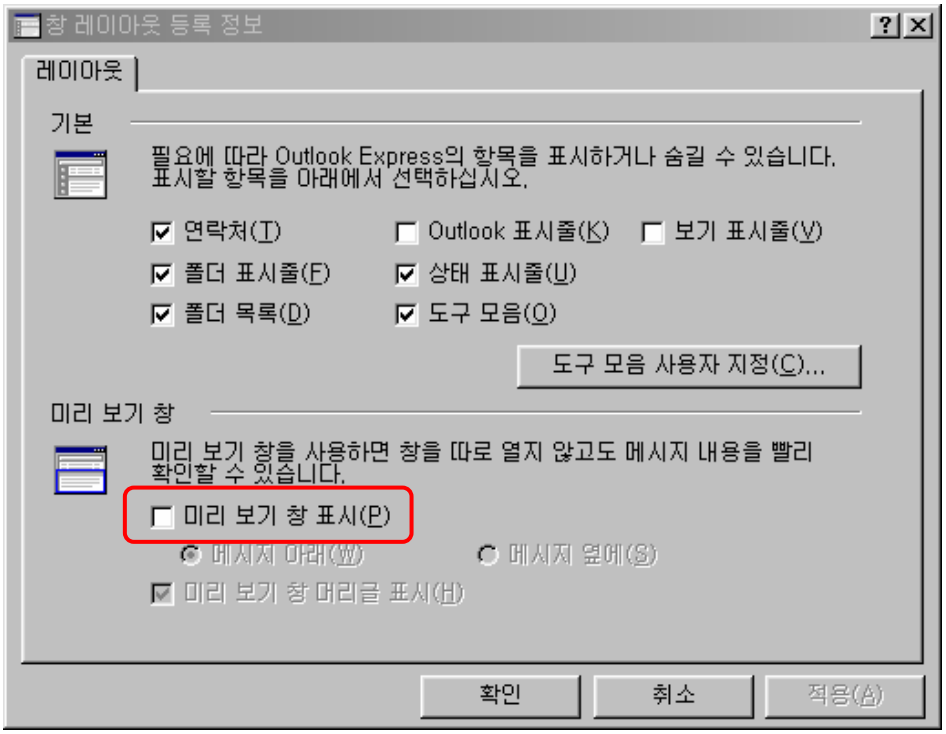


9. 메일 클라이언트의 보안설정 강화(5/6)

- 이를 해제하기 위해서 “받은 편지함”을 클릭한 후, “보기(V)” → “레이아웃(L)”을 선택하여 「창 레이아웃 등록정보」 창을 엽니다.

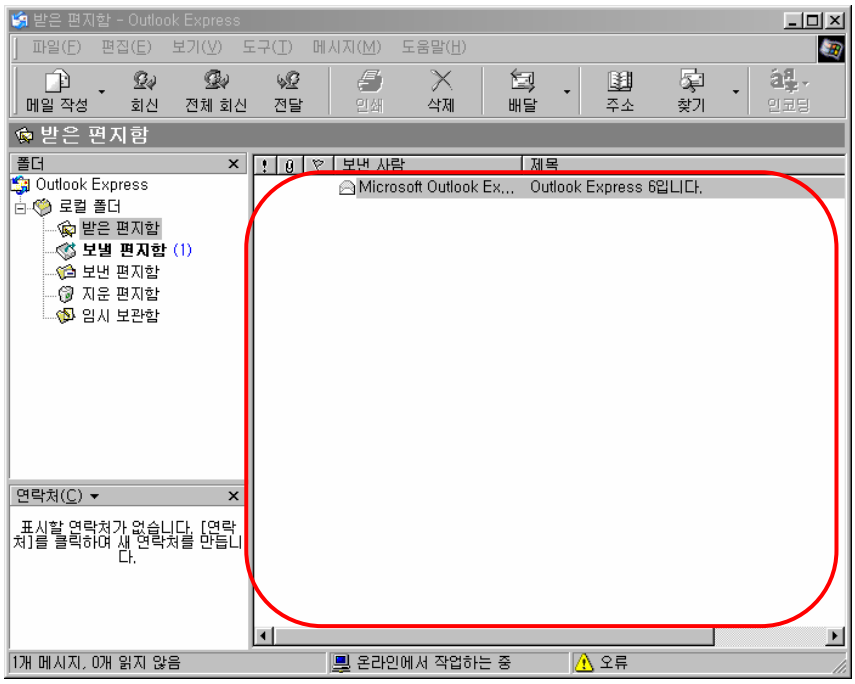


- “미리 보기 창 표시(P)” 부분을 해제시키십시오.



9. 메일 클라이언트의 보안설정 강화(6/6)

- 미리보기를 해제하면 「Outlook Express」 창에서 이메일의 내용을 미리 보여주는 기능이 해제된 것을 확인할 수 있습니다.



10. 웹 브라우저의 보안설정 강화(1/5)

개 요

- Windows 98 SE 를 설치하면 인터넷을 사용하기 위한 웹 브라우저로 인터넷 익스플로러 5.0 이 기본으로 설치됩니다.
- 인터넷 익스플로러 5.0 은 보안상 취약한 부분이 존재하므로, 6.0 버전으로 업데이트 하고 보안설정을 강화할 필요가 있습니다.

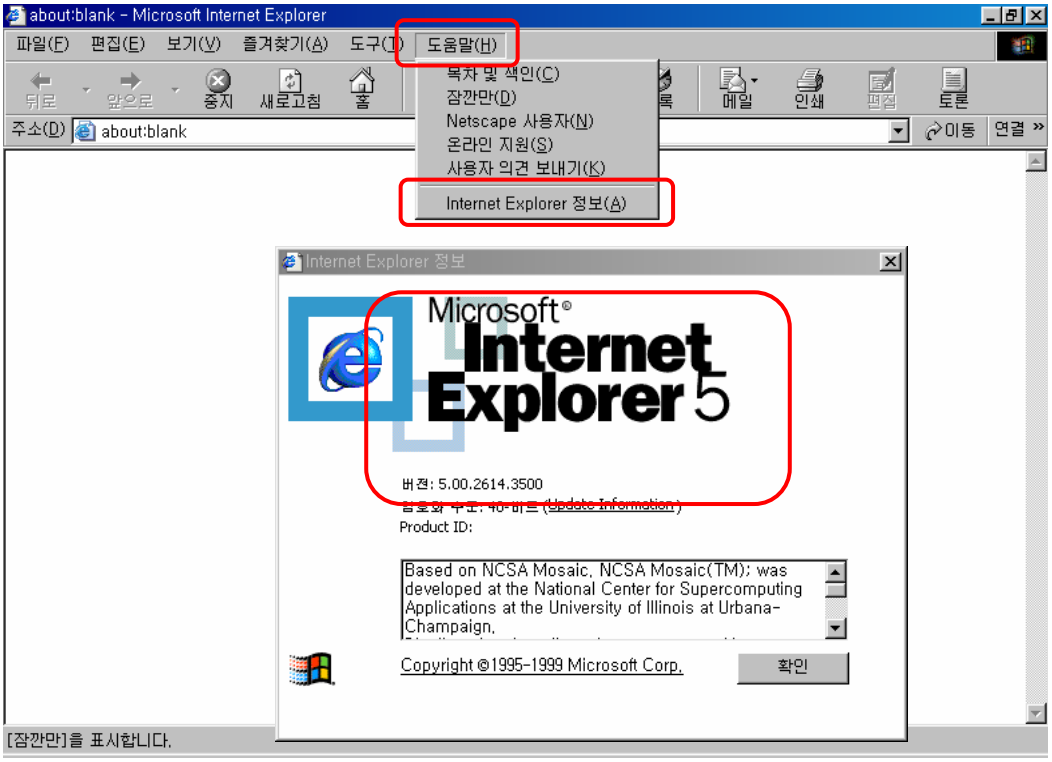
보안기능 미설정시의 문제점

- 인터넷 상의 프로그램들의 안정성 여부를 확인하지 않고 설치하거나 실행하게 되어, 컴퓨터가 악성 프로그램에 감염될 수 있습니다.

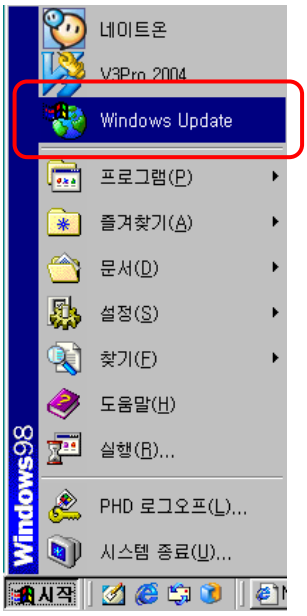
보안설정 강화방법

- 인터넷 익스플로러 6.0 으로 업데이트
  - 설치된 인터넷 익스플로러의 버전을 확인합니다.
    - 「인터넷 익스플로러」 창에서 "도움말" → "Internet Explorer 정보(A)"를 클릭하면 현재 설치되어 있는 인터넷 익스플로러의 버전을 확인할 수 있습니다.
    - 버전이 6.0 이하라면 업데이트가 필요합니다.
    - 6.0이 이미 설치되어 있다면 이후의 과정은 생략하고, 보안설정(52 페이지) 단계로 넘어가십시오.

10. 웹 브라우저의 보안설정 강화(2/5)

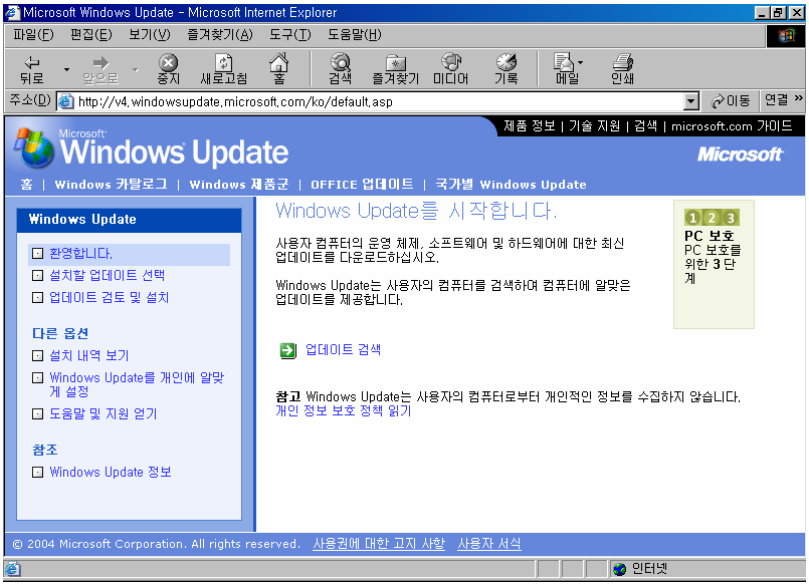


- Windows Update를 통해 Outlook Express 6.0으로 업데이트합니다.
  - 바탕화면 좌측 하단의 “시작”버튼에서 “Windows Update”를 선택합니다.

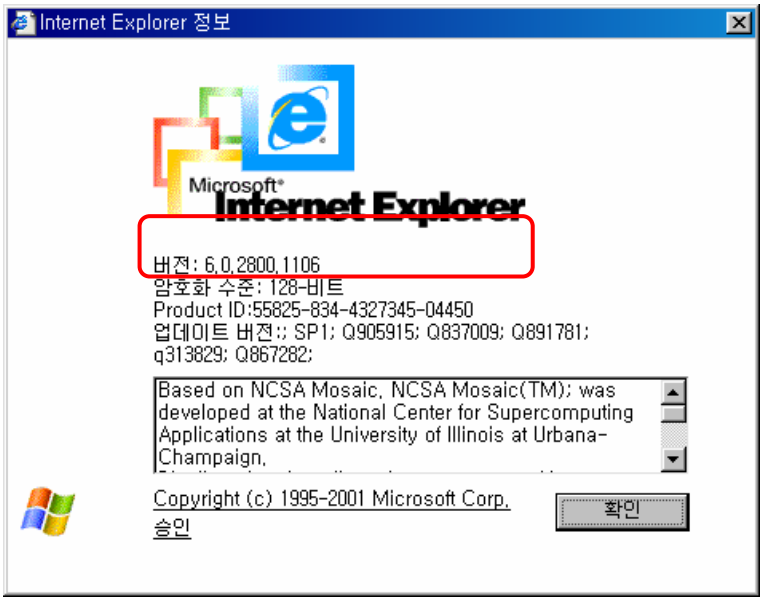


10. 웹 브라우저의 보안설정 강화(3/5)

- Windows Update 홈페이지에서 업데이트를 수행합니다. (자세한 내용은 75페이지를 참조하십시오.)



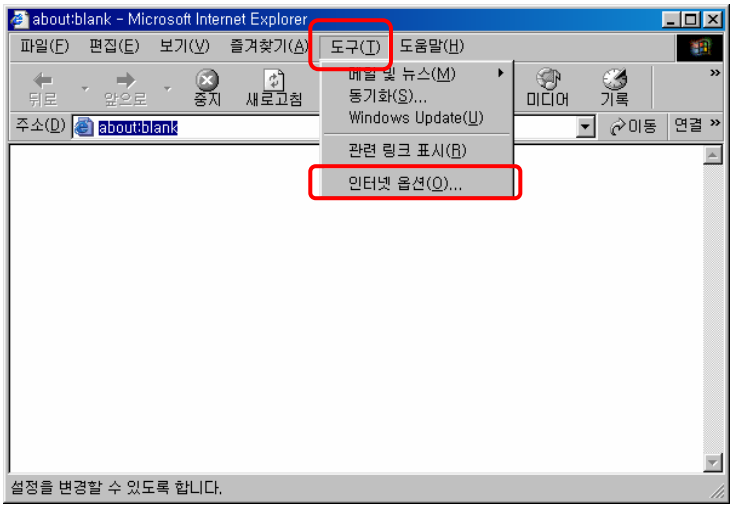
- 「인터넷 익스플로러」 창 메뉴에서 "도움말" → "Internet Explorer 정보(A)"를 클릭하여, 인터넷 익스플로러의 버전이 6.0으로 업그레이드된 것을 확인합니다.

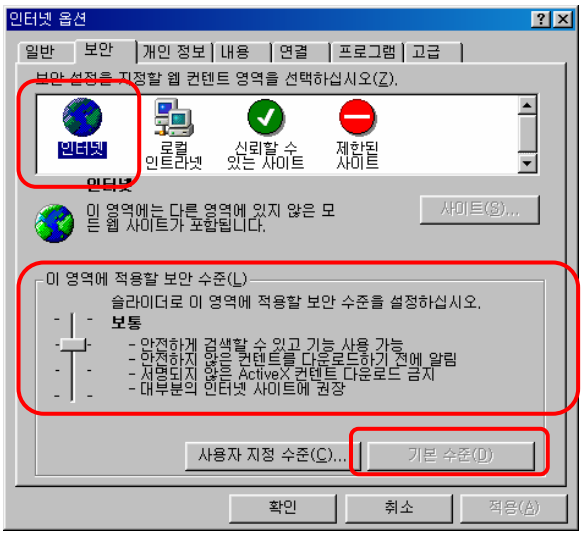


10. 웹 브라우저의 보안설정 강화(4/5)

보안설정

- 브라우저의 “도구(T)” → “인터넷 옵션(O)”을 선택하면 열리는 「인터넷 옵션」 창에서 “보안” 탭을 선택합니다.





- 현재, 이 웹 브라우저는 인터넷 영역에서 “보통” 등급의 보안수준이 설정되어 있는 것을 확인할 수 있습니다.
- 좌측의 슬라이드를 이용하여 보안수준을 “높음”, “보통”, “낮음”, “최소”로 설정할 수 있습니다.
- 보안수준을 “보통” 혹은 “높음” 으로 설정하는 것을 권장합니다.

10. 웹 브라우저의 보안설정 강화(5/5)

- 각 보안수준의 내용을 정리하면 다음과 같습니다.
  - 높음 :
    - 가장 안전한 검색 방법이지만 가장 낮은 기능을 제공받습니다.
    - 위험하다고 판단되는 사이트에서의 사용을 권장합니다.
  - 보통
    - 일반적으로 가장 많이 사용되는 수준입니다.
    - 대부분의 인터넷 사이트에서의 사용을 권장합니다.
  - 낮음
    - 허용여부를 묻는 것을 제외하고는 보통 보안 수준과 동일합니다.
    - 어느 정도 믿을 수 있는 로컬 네트워크(인트라넷) 사이트에서의 사용을 권장합니다.
  - 최소
    - 최소 보안 수준을 제공합니다.
    - 사용자 허가 없이 대부분의 프로그램 다운로드하여 실행하므로 항상 신뢰하는 사이트에서의 사용을 권장합니다.

11. 인터넷을 통한 프로그램 다운로드 주의(1/2)

개 요

- 인터넷 웹사이트들의 대부분은 더 나은 기능을 제공하기 위하여 ActiveX 컨트롤 등과 같은 여러 종류의 프로그램을 설치하도록 요구합니다.
  - ActiveX 컨트롤이란 웹사이트에서 사용자 PC에 설치/실행되는 프로그램으로, 이를 통해 사용자는 웹사이트의 다양한 기능을 제공받을 수 있습니다.
- 하지만 이러한 인터넷상의 프로그램에 악성 프로그램이나 스파이웨어가 숨어 있을 수 있을 수 있습니다.
- 따라서 인터넷상의 프로그램을 설치할 때는 주의가 필요합니다.

부주의시의 문제점

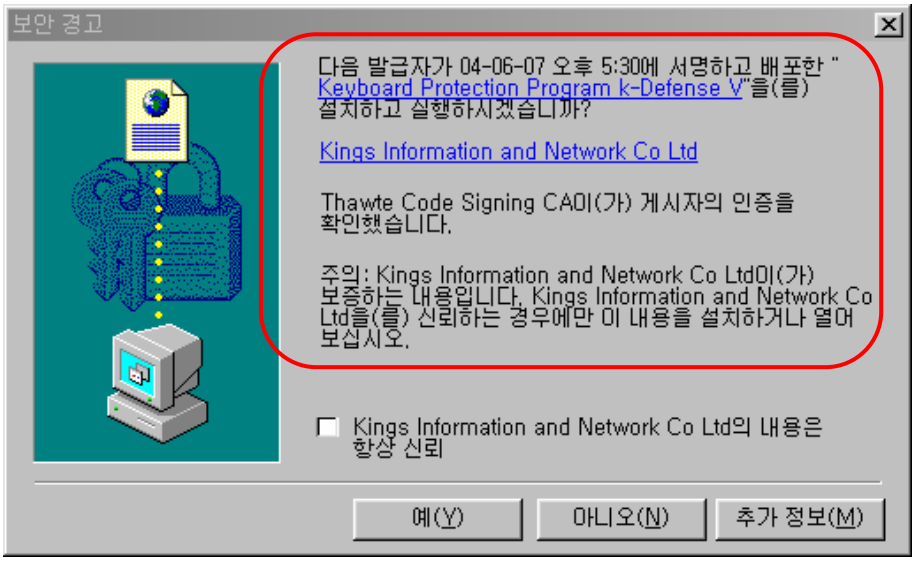
- 인터넷을 이용하면서 설치하라는 프로그램들을 주의없이 설치하면 스파이웨어가 설치되어 광고창에 시달리게 되거나, 웹 시작 페이지 변조, 개인 정보 유출 등 악성 프로그램의 피해를 당할 수 있습니다.
- 웜·바이러스에 감염되거나 해킹 피해를 당할 수도 있습니다.

대응 방법

- 웹사이트 방문 시 설치하는 프로그램은 인증서 및 디지털 서명을 참조하여 신뢰성 확인 후 설치하십시오.
- 인터넷 익스플로러의 보안설정을 강화하십시오.(49페이지 참조)

11. 인터넷을 통한 프로그램 다운로드 주의(2/2)

- 인터넷 익스플로러의 「보안 경고」 창을 통해 이런 신뢰성을 어느 정도 확인할 수 있습니다.
  - 아래 그림은 「보안 경고」 창의 예입니다.
  - "Kings Information and Network Co Ltd" 회사에서 만든 "Keyboard Protection Program k-Defense V" 라는 프로그램을 설치할 것인지를 묻고 있으며, "이 회사가 만든 프로그램이 맞다" 라는 인증을 "Thawte Code Signing" 기관에서 수행 했다라는 내용입니다.
  - 프로그램 설치 시 이러한 내용을 잘 읽어보시고 설치 여부를 선택하셔야 합니다.

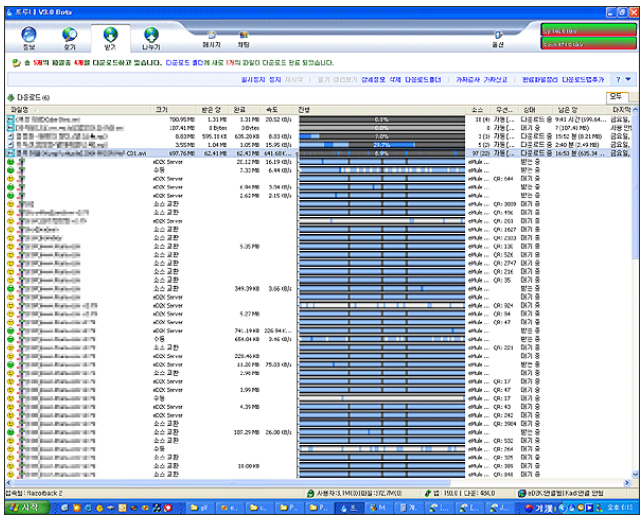


- 인터넷상의 파일을 다운로드 하면 바이러스 검사를 수행하십시오.(70페이지 참조)

12. P2P 프로그램의 사용 제한(1/2)

개 요

- P2P(Peer-To-Peer) 프로그램은 컴퓨터 사용자들끼리 자신이 보관하고 있는 자료를 다른 사용자들과 공유하기 위해 사용하는 프로그램입니다.
- P2P 프로그램의 종류
  - P2P 프로그램은 매우 다양한 종류가 있으며, 다음에 열거한 프로그램이 국내에서 많이 사용되는 것들입니다.
    - 프루나(Pruna)
    - 당나귀(eDonkey)
    - 몽키(Monkey) 3
    - 파일구리(FileGuri)
    - Azureus
    - BitComet
    - 동키호테(Donkeyhote)
    - eMule(이뮬)
    - myPMC
    - LimeWire Basic



<P2P 프로그램인 프루나의 화면>

12. P2P 프로그램의 사용 제한(2/2)

- 하지만 P2P는 음악, 영화 등과 같은 저작권에도 문제가 있고, 부주의한 사용으로 중요한 자료가 다른 사용자들에게 전송되는 문제도 유발할 수 있으므로 업무용 PC에서는 사용하지 않는 것이 안전합니다.
- 또한, 악성 프로그램이 포함되어 있는 파일이 다른 사용자들에게 전파되는 감염경로로 이용되기도 합니다.

P2P 사용으로 인한 문제

- 자료 유출
  - 공유를 위한 폴더 하위의 자료는 인터넷에 공개되어 있는 것과 같습니다.
- 악성 프로그램 유포
  - P2P는 파일의 이름으로만 파일을 구별할 수 있습니다.
  - 누군가 인기가 많은 파일에 악성 프로그램을 포함시킨 뒤, 이를 P2P를 통해 유포하면, 피해자들은 아무런 의심을 갖지 않고 이 파일을 다운로드하여 실행하게 되어 결국에는 악성 프로그램에 감염됩니다.

제한방법

- P2P를 제한하는 기술적인 방법은 없으며, 사용자 스스로가 자신의 컴퓨터에 P2P 프로그램이 설치되어 있는 지를 확인하여, 설치되어 있는 경우에는 이를 삭제해야 합니다.
  - 설치여부 확인 방법
    - 현재 컴퓨터에 설치되어 있는 프로그램들 중에서 P2P 프로그램이 있는 지를 확인합니다. (83페이지 참조)
  - 해당 프로그램 제거
    - P2P 프로그램을 발견하게 되면 해당 프로그램을 제거합니다. (83페이지 참조)

13. 시스템 원격 관리 해제(1/2)

개 요

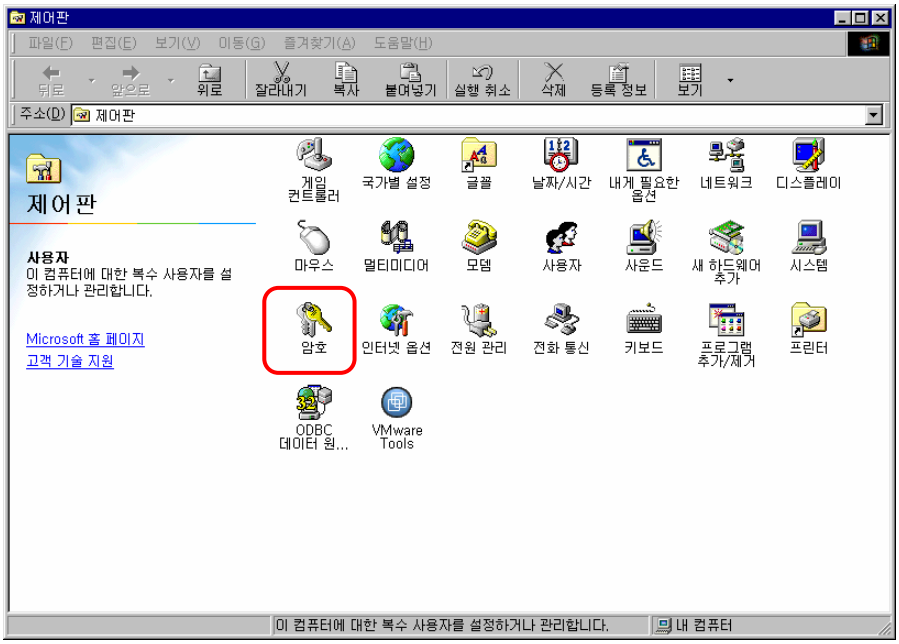
- 필요에 의해 원격의 다른 사용자가 자신의 컴퓨터에 접근할 수 있다면 이는 편의성 측면에서는 좋은 방법이라고 할 수 있지만, 보안상으로는 매우 취약합니다.
- 암호를 설정하여 접근하는 사용자를 확인한다 하더라도 불법적으로 접속할 수 있는 경로가 존재하므로, 시스템 원격 관리를 사용하지 않는 것이 안전합니다.

원격관리 사용시의 문제점

- 시스템 원격 관리가 허용되어 있는 경우에는 다른 컴퓨터에서 사용자의 컴퓨터로 ADMIN$ 의 계정을 통해 접속할 수 있습니다.
- 사용자의 모든 파일이 노출되며, 악성 프로그램이 설치/실행 될 수 있습니다.

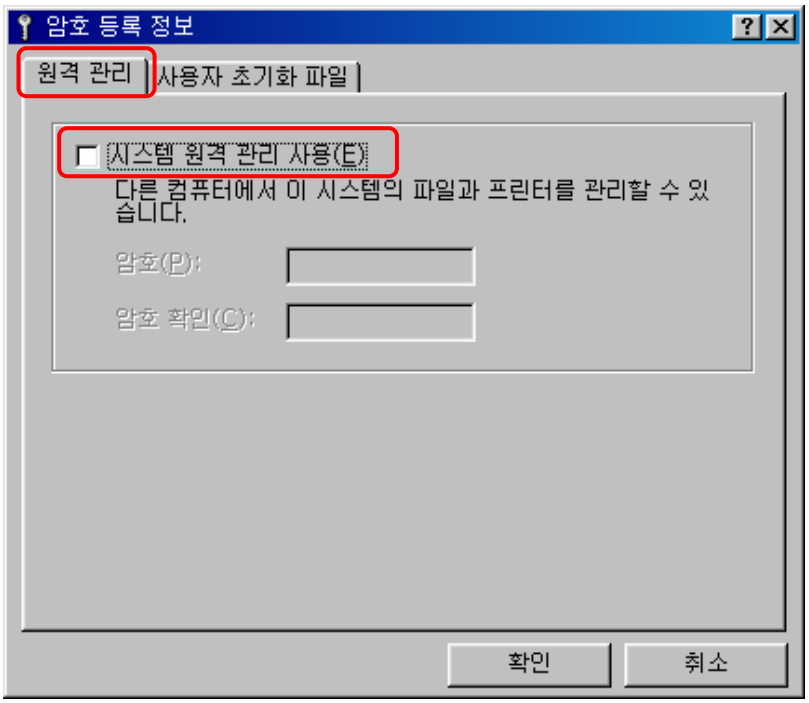
해제방법

- 「제어판」 창을 엽니다.(9페이지)
- 「제어판」 창에서 "암호"를 선택합니다.



13. 시스템 원격 관리 해제(2/2)

- "원격 관리" 탭을 선택합니다.
  - "원격 관리" 탭이 없다면 사용자 컴퓨터에서는 시스템 원격 관리를 할 수 없으므로 이하의 과정이 필요 없습니다.



  - "시스템 원격 관리 사용(E)"를 해제합니다.

Ⅲ. 바이러스/스파이웨어 보안

14. 컴퓨터 백신 프로그램 사용(1/1)

개 요

- PC에 감염될 수 있는 웜·바이러스를 사전에 탐지하거나 이미 감염되어 있는 웜·바이러스를 제거해 주는 프로그램이 컴퓨터 백신(Anti Virus) 프로그램입니다.
  - 웜·바이러스란 컴퓨터에서 동작하는 일종의 악성 프로그램으로 자료를 손상시키거나 다른 프로그램을 파괴하여 정상적인 작업을 방해하는 프로그램이라고 할 수 있습니다.

미사용시의 문제점

- 사용하는 컴퓨터가 웜·바이러스에 감염되면 다음과 같은 문제가 발생합니다.
  - 컴퓨터의 파일이 사용자 모르게 외부로 유출됩니다.
  - 컴퓨터에 저장되어 있는 주소록을 이용하여 다른 사용자의 컴퓨터로 웜·바이러스가 확산됩니다.
  - 하드디스크에 저장되어 있는 파일들이 삭제됩니다.
  - 메모리나 파일 시스템을 파괴하여 컴퓨터의 정상적인 사용이 불가능하게 됩니다.
  - 네트워크에 비정상적인 활동이 많이 일어나 정상적인 네트워크 사용이 불가능하게 됩니다.

사용방법

- 백신 프로그램은 정품소프트웨어를 구입하거나 또는 업체가 제공하는 프리웨어를 다운로드하여 활용하는 방법이 있습니다.
  - 프리웨어 제품은 개인용, 비사업용 목적으로만 사용할 수 있음을 주의해야 합니다.

15. 주기적 바이러스 검사(1/3)

개 요

- PC를 안전하게 운영·유지하기 위하여 백신 프로그램을 주기적으로 수행해 주어야 합니다.
- 사용자가 수동으로 검사하는 방법도 있지만, 백신 프로그램에 자동수행을 설정하는 방법이 보안에 도움이 됩니다.

주의사항

- "상용 정보보호 시스템 적합성 검증제도"란 국가·공공기관이 도입하고자 하는 상용 정보보호 시스템의 보안기능과 국가정보통신망에 대한 적합성을 검증하기 위해 『국가 정보보안 기본지침』(06.1.1)에 의거하여 시행하는 제도입니다.
- "상용 정보보호시스템 적합성 검증제도"를 통과한 제품에 대한 정보는 국가정보원 IT보안 인증사무국(www.kecs.go.kr)에서 열람할 수 있습니다.
- 본 가이드라인에서는 "V3 Pro 2004" 프로그램을 이용하여 설명하고 있습니다. 이는 설명의 이해도를 높이기 위한 방법이며, 반드시 이 제품의 사용을 권장하는 것은 아닙니다.

미사용시의 문제점

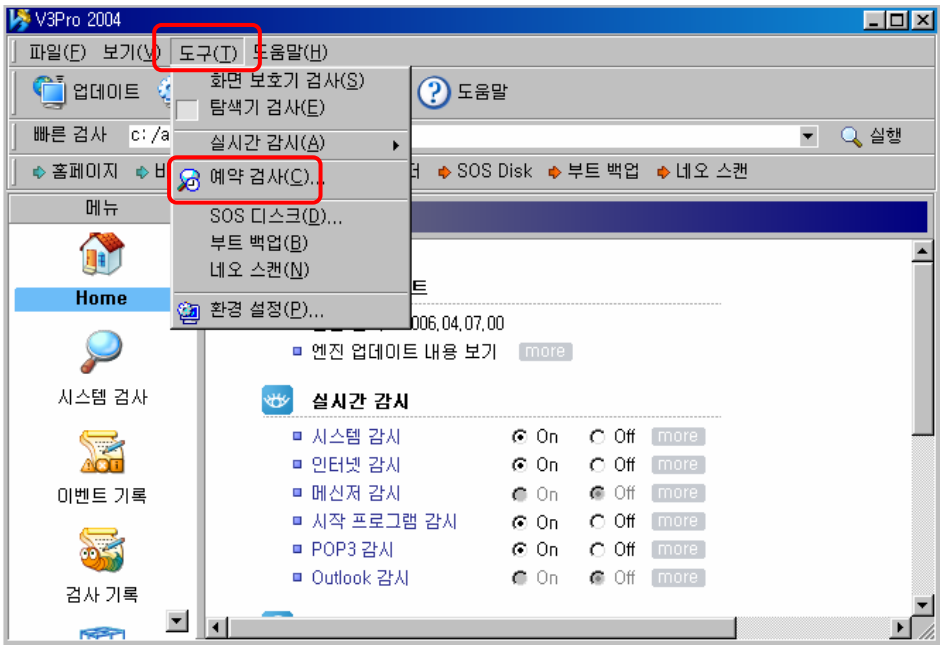
- 웜·바이러스는 매일 신종이 발생되어 전파되기 때문에 백신 프로그램을 오래 전에 수행한 결과는 의미가 없습니다.

15. 주기적 바이러스 검사(2/3)

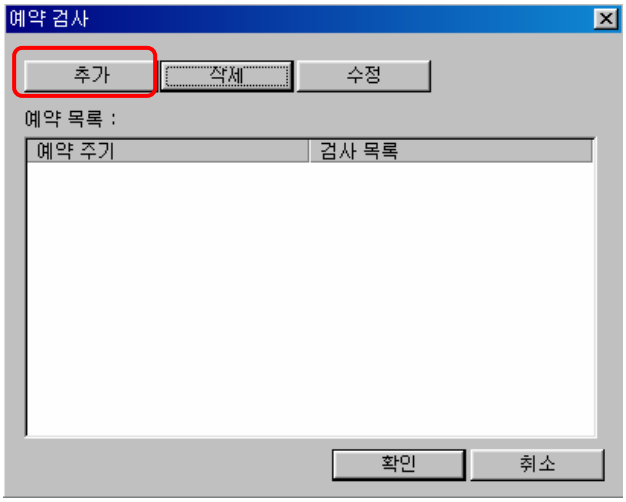
검사방법

◆ 「예약검사」 창 열기

▶ V3Pro 2004 프로그램에서 “도구(T)” → “예약검사(C)”를 선택합니다.



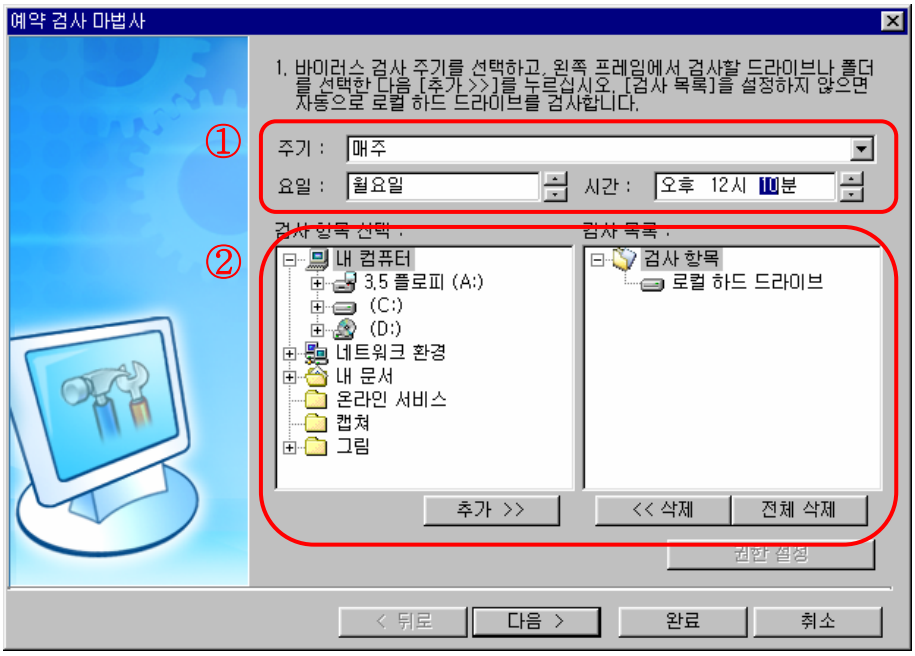
▶ 현재는 예약이 설정되어 있지 않습니다.



15. 주기적 바이러스 검사(3/3)

◆ 검사 예약 설정하기

▶ 「예약 검사」 창에서 “추가” 버튼을 클릭합니다.



▶ ①번에서는 검사주기를 선택할 수 있는 데, 매주 월요일 오후 12시 10분에 검사를 시작하는 것으로 설정하였습니다.

▶ ②번에서는 검사대상을 선택할 수 있는 데, “로컬 하드 드라이브”를 검사하는 것으로 설정하였습니다.

▶ ①, ②번 부분의 내용을 사용자의 환경에 적합하도록 설정하여 주기적으로 백신 프로그램이 수행될 수 있도록 설정합니다.

▶ 컴퓨터가 꺼져 있는 상태에서는 동작하지 않으며, 사용 중에 수행되면 업무에 영향을 끼칠 수 있으므로 점심시간 등 컴퓨터를 사용하지 않는 동안에 동작하도록 설정하는 것이 유용합니다.

16. 최신 컴퓨터 백신 엔진 업데이트(1/5)

개 요

- 웜·바이러스는 신종 또는 기존 것의 변형이 매일 출현하기 때문에 백신 프로그램이 새로운 웜·바이러스를 탐지하기 위해서는 백신업체가 제공하는 최신 엔진을 항상 유지해야 합니다.
- 컴퓨터가 인터넷에 연결되어 있다면 매우 간단한 방법으로 자동 업데이트를 수행할 수 있습니다.

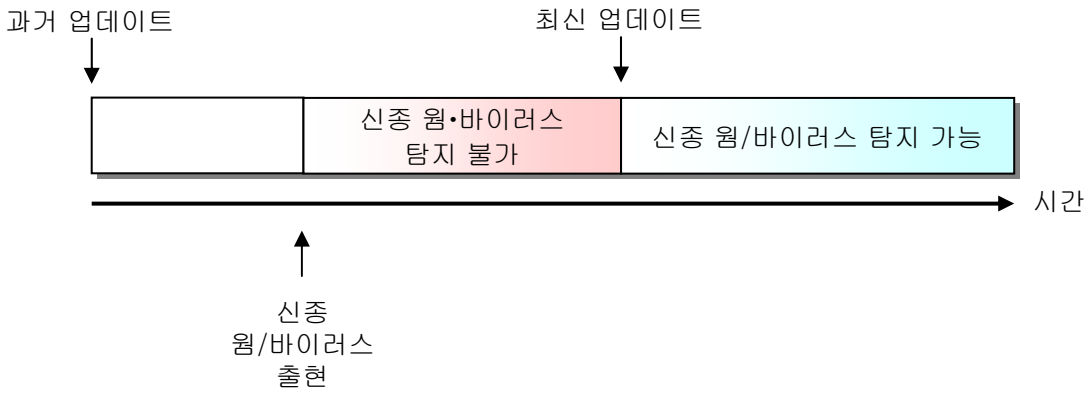
주의사항

- "상용 정보보호 시스템 적합성 검증제도"란 국가·공공기관이 도입하고자 하는 상용 정보보호 시스템의 보안기능과 국가정보통신망에 대한 적합성을 검증하기 위해 『국가 정보보안 기본지침』(06.1.1)에 의거하여 시행하는 제도입니다.
- "상용 정보보호시스템 적합성 검증제도"를 통과한 제품에 대한 정보는 국가정보원 IT보안 인증사무국(www.kecs.go.kr)에서 열람할 수 있습니다.
- 본 가이드라인에서는 "V3 Pro 2004" 프로그램을 이용하여 설명하고 있습니다. 이는 설명의 이해도를 높이기 위한 방법이며, 반드시 이 제품의 사용을 권장하는 것은 아닙니다.

미사용시의 문제점

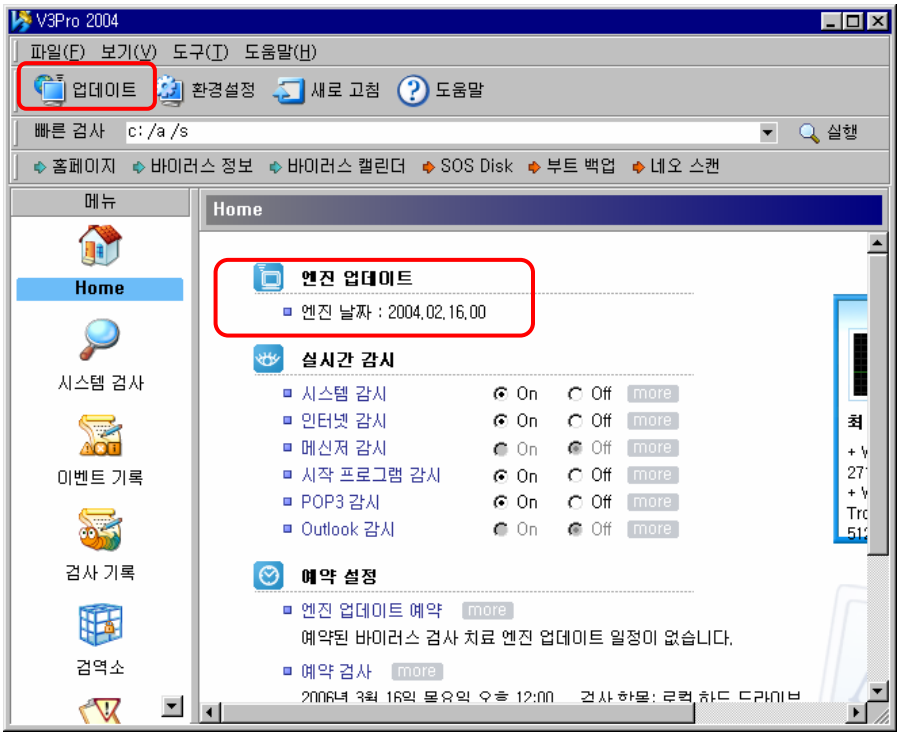
- 이전 버전의 엔진이 탑재된 백신 프로그램으로는 자주 검사한다 하더라도 새로운 웜·바이러스는 탐지할 수 없습니다.

16. 최신 컴퓨터 백신 엔진 업데이트(2/5)



업데이트 방법

- 대부분의 백신 프로그램은 인터넷을 통해 자동으로 엔진 업데이트를 수행할 수 있습니다.
- 엔진 날짜 확인하기

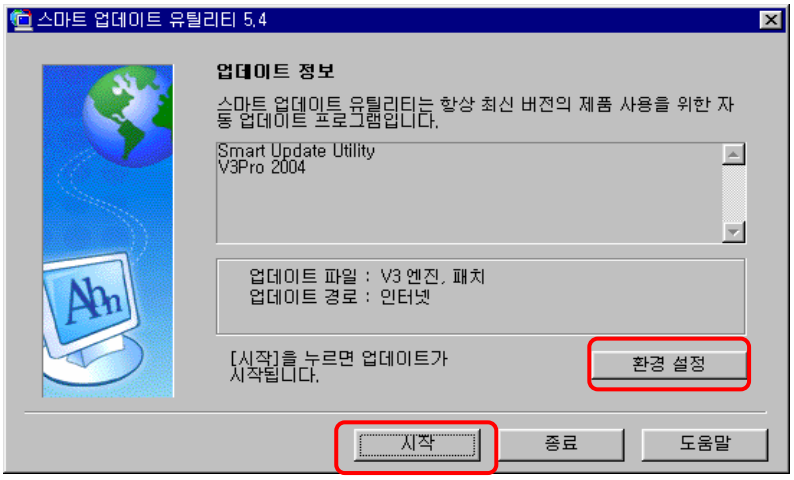


16. 최신 컴퓨터 백신 엔진 업데이트(3/5)

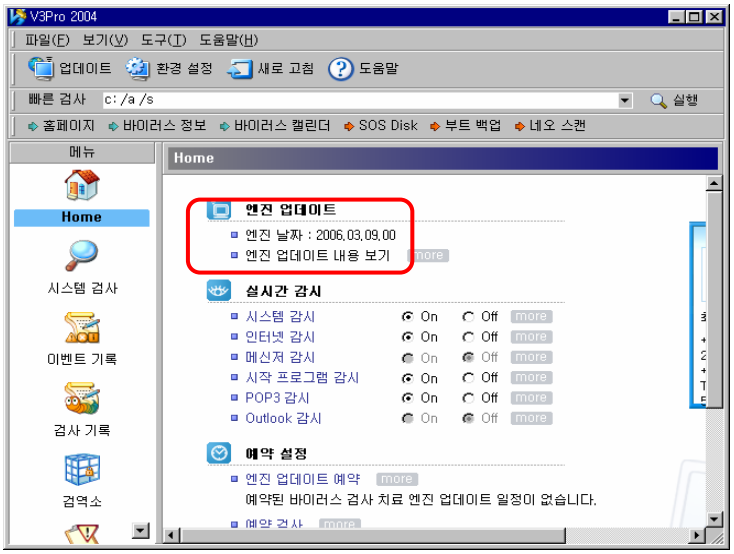
- 「V3Pro 2004」 창에서 현재 엔진의 날짜를 확인할 수 있습니다.
- 현재의 것은 2004년 2월 16일의 것으로 이 엔진으로는 이후에 작성된 웜·바이러스를 탐지할 수 없으므로 엔진을 최신의 것으로 업데이트 해야 합니다.

◆ 업데이트 시작하기

- 「V3Pro 2004」 창의 좌측 상단에 있는 "업데이트" 버튼을 클릭합니다.



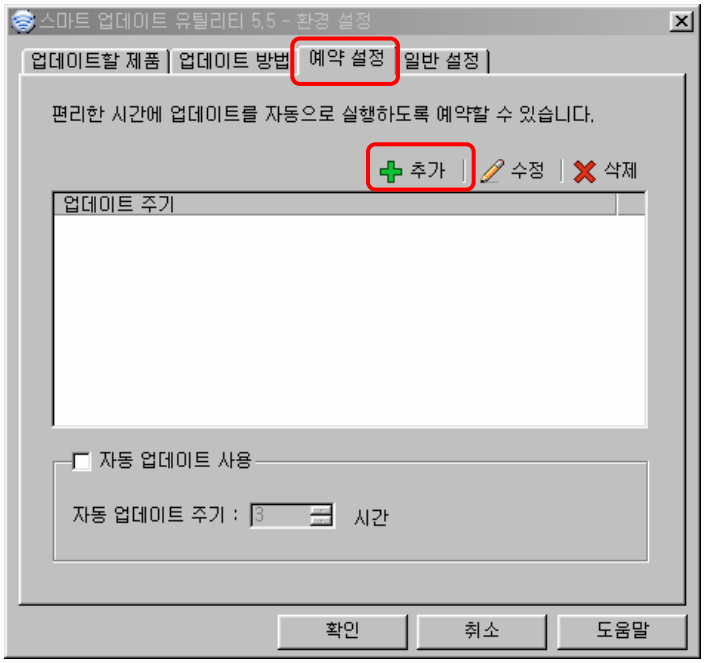
- 「스마트 업데이트 유틸리티」 창에서 "시작" 버튼을 클릭하면 업데이트가 시작됩니다.
- 업데이트 완료 후에 "V3Pro 2004" 프로그램을 시작하면 다음과 같이 엔진의 날짜가 최신의 것으로 변경되어 있는 것을 확인할 수 있습니다.



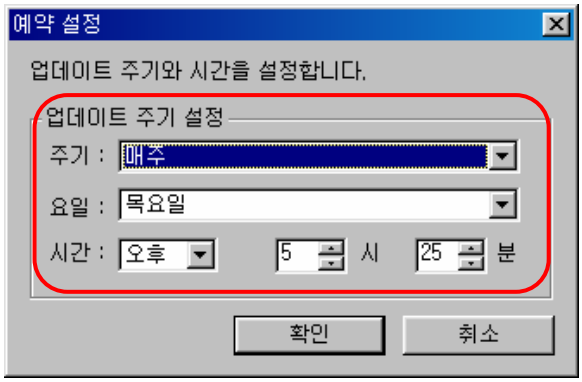
16. 최신 컴퓨터 백신 엔진 업데이트(4/5)

업데이트 예약 설정하기

- 「스마트 업데이트 유틸리티」 창의 “환경설정” 버튼을 클릭하여 열리는 창에서 “예약 설정”탭을 선택합니다.



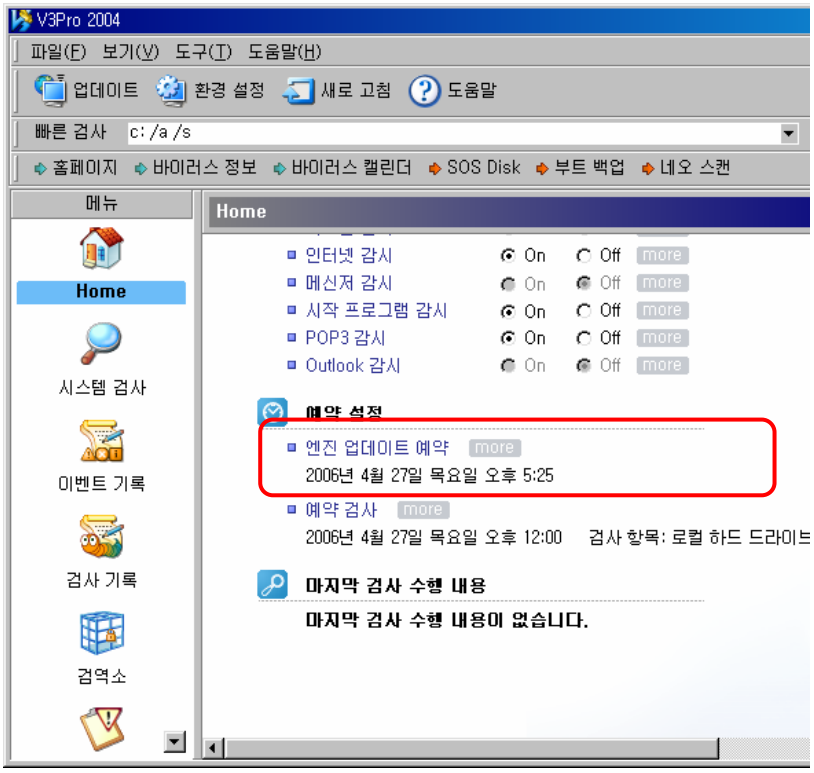
- “추가” 버튼을 합니다.



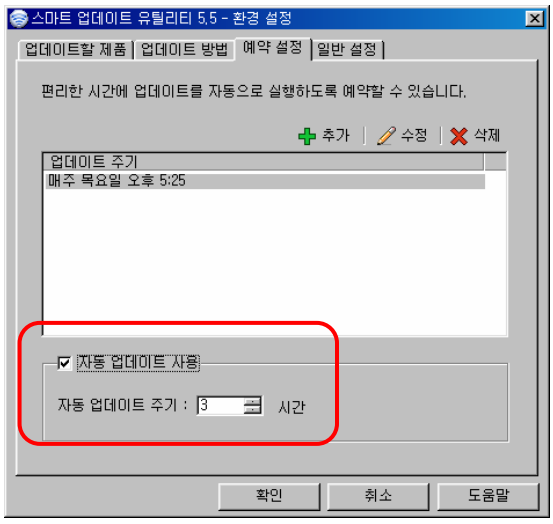
- “주기”, “요일“, “시간”을 설정하고 “확인”을 누르면 예약이 설정됩니다.

16. 최신 컴퓨터 백신 엔진 업데이트(5/5)

- 설정된 예약 상황을 확인할 수 있습니다.



- 다른 방법으로 「스마트 업데이트 유틸리티 - 환경설정」창에서 "자동 업데이트 사용" 항목을 설정하고, 시간을 지정하면 지정된 시간 주기로 엔진 업데이트를 수행합니다.



17. 컴퓨터 백신 프로그램의 실시간 감시 수행(1/3)

개 요

- 실시간 감시 기능은 컴퓨터 사용 중에 웜·바이러스가 발견되면 이의 활동을 차단하고 자동적으로 감염파일을 치료하는 기능입니다.
- 웜·바이러스로 인한 피해상황 발생을 미연에 방지할 수 있는 핵심 기능입니다.

주의사항

- "상용 정보보호 시스템 적합성 검증제도"란 국가·공공기관이 도입하고자 하는 상용 정보보호 시스템의 보안기능과 국가정보통신망에 대한 적합성을 검증하기 위해 『국가 정보보안 기본지침』(06.1.1)에 의거하여 시행하는 제도입니다.
- "상용 정보보호시스템 적합성 검증제도"를 통과한 제품에 대한 정보는 국가정보원 IT보안 인증사무국(www.kecs.go.kr)에서 열람할 수 있습니다.
- 본 가이드라인에서는 "V3 Pro 2004" 프로그램을 이용하여 설명하고 있습니다. 이는 설명의 이해도를 높이기 위한 방법이며, 반드시 이 제품의 사용을 권장하는 것은 아닙니다.

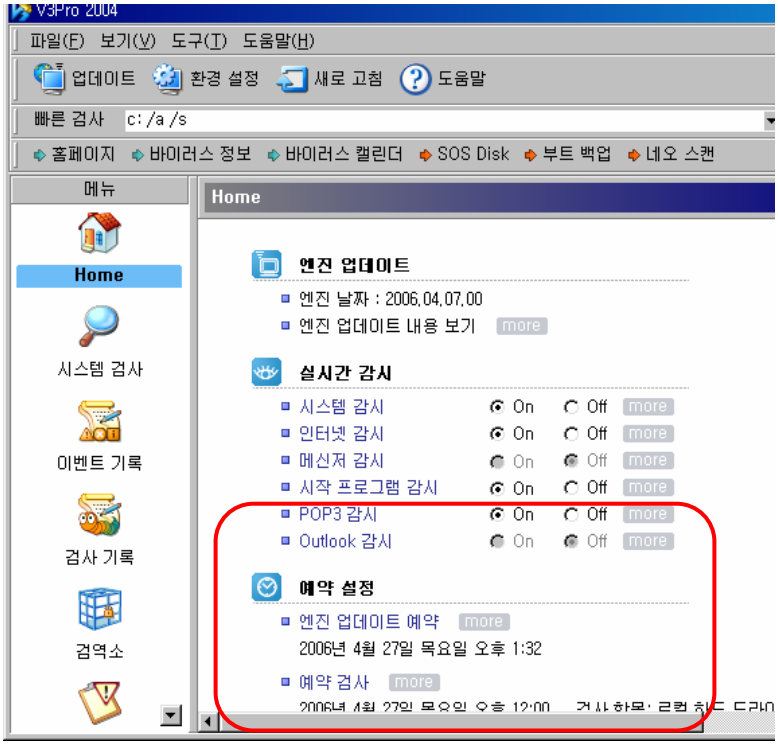
미수행시의 문제점

- 지금까지의 백신 프로그램 사용은 평상시에는 웜·바이러스를 탐지하지 않다가 특정 시각이 되면 시스템 전체를 대상으로 웜·바이러스를 탐지하는 형태입니다.
- 이미 감염된 웜·바이러스를 탐지하는 것보다 사용자의 컴퓨터에 침입하려는 웜·바이러스를 즉각 차단하여 애초에 컴퓨터에 침입할 수 없게끔 하는 것이 더 좋은 방법이 될 수 있습니다.
  - 네트워크와 보조기억매체의 발달로 인해 다양한 형태의 정보가 실시간으로 교환·공유·전파되는 환경에서는 실시간 점검이 큰 역할을 수행할 수도 있기 때문입니다.

17. 컴퓨터 백신 프로그램의 실시간 감시 수행(2/3)

수행방법

- "실시간 검사" 설정
  - 「V3Pro 2004」 창에서 "실시간 검사" 부분을 보면 실시간으로 검사하고 있는 항목을 확인할 수 있습니다.



  - 현재 "시스템 감시", "인터넷 감시", "시작 프로그램 감시", "POP3 감시"가 설정되어 있습니다.
  - "On"과 "Off"를 선택할 수 있으며, 선택할 수 없는 항목은 해당 프로그램이 컴퓨터에 설치되어 있지 않은 것이므로, 해당 프로그램을 설치한 이후에는 "On", "Off"를 선택할 수 있습니다.

17. 컴퓨터 백신 프로그램의 실시간 감시 수행(3/3)

- 실시간 검사의 각 항목에 대한 설명은 다음과 같습니다.
  - 시스템 감시
    - 일반 응용 프로그램에서 접근하는 모든 파일 및 데이터를 실시간으로 검사합니다.
  - 인터넷 감시
    - 인터넷 웹 브라우저를 통해서 다운로드 되는 모든 데이터 및 파일들을 실시간으로 검사합니다.
    - 홈페이지에 숨어있는 악성 프로그램을 탐지할 수 있습니다.
  - 메신저 감시
    - 메신저 프로그램을 통해서 다운로드되는 데이터 및 파일들을 실시간으로 검사합니다.
    - 메신저를 이용한 파일 교환이 많은 경우에 매우 중요한 역할을 수행합니다.
  - 시작 프로그램 감시
    - 시작 프로그램의 레지스트리, 시작 프로그램 폴더, 시스템 파일에 등록된 시작 프로그램들을 시작할 때마다 자동으로 검사합니다.
  - POP3 감시
    - 메일 클라이언트 프로그램의 POP3 계정을 통하여 들어오는 모든 메일들을 실시간으로 검사합니다.
    - 이메일 첨부파일을 통한 악성 프로그램 확산 방지에 유용합니다.
  - Outlook 감시
    - 마이크로소프트 Outlook 메일 프로그램(MS Outlook 2000 이상)을 통해서 들어오는 메일들을 실시간으로 검사합니다.
    - 첨부파일을 통한 악성 프로그램 확산 방지에 유용합니다.

18. 스파이웨어 탐지/제거 프로그램 사용(1/1)

개 요

- 스파이웨어(Spyware)란 사용자 모르게 설치되어 특정기능을 수행하는 소프트웨어를 의미합니다.
- 사용자가 원하지 않는 팝업창이 나타나는 단순한 수준에서부터 웹 브라우저의 제어권을 완전히 획득하는 심각한 수준까지 다양한 피해를 발생시킵니다.
- 이러한 스파이웨어가 컴퓨터에 설치되어 있는 지를 확인할 수 있는 스파이웨어 탐지/제거 프로그램을 설치·운영하여 컴퓨터의 안전성을 높일 필요가 있습니다.

미사용시의 문제점

- 사용자들은 브라우저를 이용한 인터넷 검색 중에 특정 프로그램을 설치해야 한다는 안내가 나오면 의심 없이 해당 프로그램을 설치하는 것이 일반적인데, 이러한 프로그램들 중에 스파이웨어가 포함되어 있을 가능성이 높습니다.
- 더구나, 최근의 스파이웨어는 설치되는 데에 사용자의 허가 또는 상호동작 없이 설치되는 것도 있으므로, 결국 스파이웨어가 설치된 것을 사용자가 전혀 인지하지 못할 수도 있다는 것에 주목해야 합니다.

사용방법

- 상용 또는 무료로 사용할 수 있는 제품들이 있으니 설치하여 사용해 주십시오.
- 무료제품 중에는 그 자체가 스파이웨어인 것도 존재하므로 사용에 주의해야 합니다.

Ⅳ. 유지/관리 보안

19. 패치 업데이트(1/5)

개 요

- 프로그램 출시 후에 발견되는 취약점과 같은 문제점을 해결하기 위해 마이크로소프트에서는 패치 서비스를 실시하고 있습니다.
- 패치란 Windows 98 운영체제나 응용 프로그램의 오류나 취약한 부분을 보완해 주는 여러 가지 수정 프로그램을 말합니다.
- 마이크로소프트가 제공하는 패치 프로그램을 설치하는 것은 운영체제를 안전하게 운영하는 데 필수적입니다.

주의사항

- 2006년 7월부로 Windows 98 의 패치 서비스가 중단됩니다.
- 이는 더 이상의 패치가 나오지 않는다는 의미로, 기존의 패치 서비스가 사라진다는 의미는 아닙니다.
- 지금까지 배포된 패치는 사용자가 모두 업데이트 하셔야 합니다.

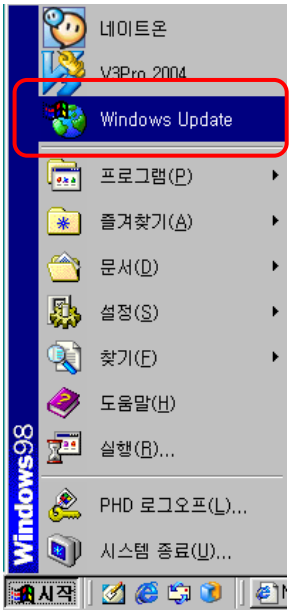
미사용시의 문제점

- 패치를 설치하지 않으면 이미 발견된 취약점에 무방비로 노출됩니다.
- 패치를 설치하지 않으면 시스템 안정성에 문제가 있으며 상대적으로 해킹 공격에 취약해집니다.

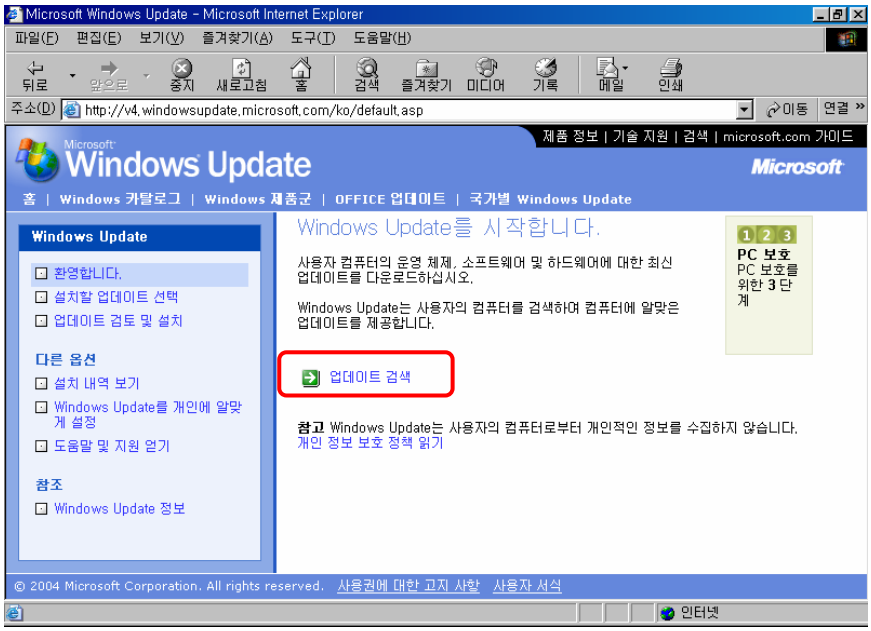
19. 패치 업데이트(2/5)

업데이트 방법

- 바탕화면 좌측 하단의 “시작”에서 “Windows Update”를 선택합니다.

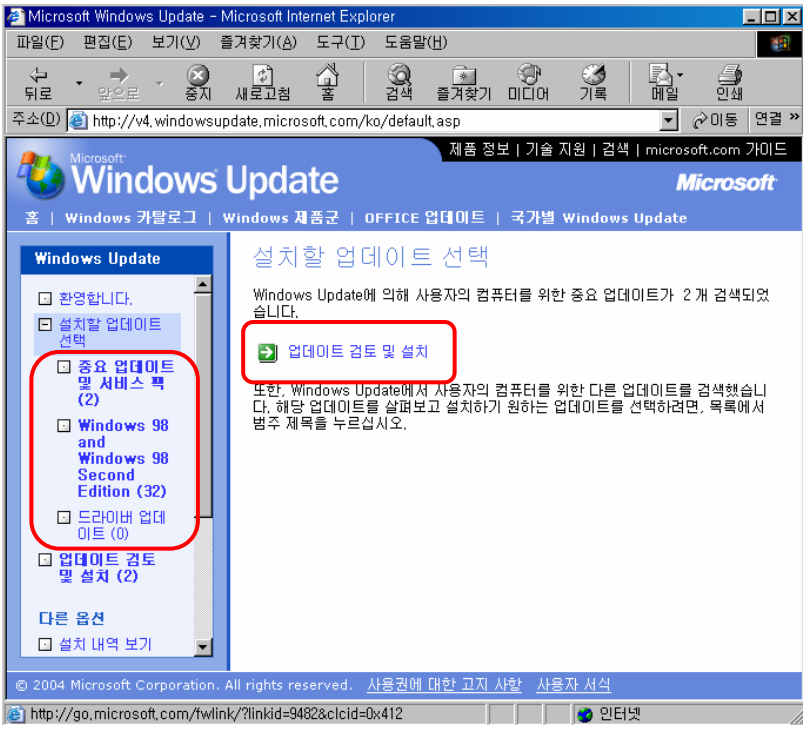


- 마이크로소프트에서 제공하는 업데이트 페이지로 자동으로 이동합니다. 아래 그림과 같이 보이면 “업데이트 검색”을 클릭합니다.



19. 패치 업데이트(3/5)

◆ "업데이트 검토 및 설치"를 클릭합니다.

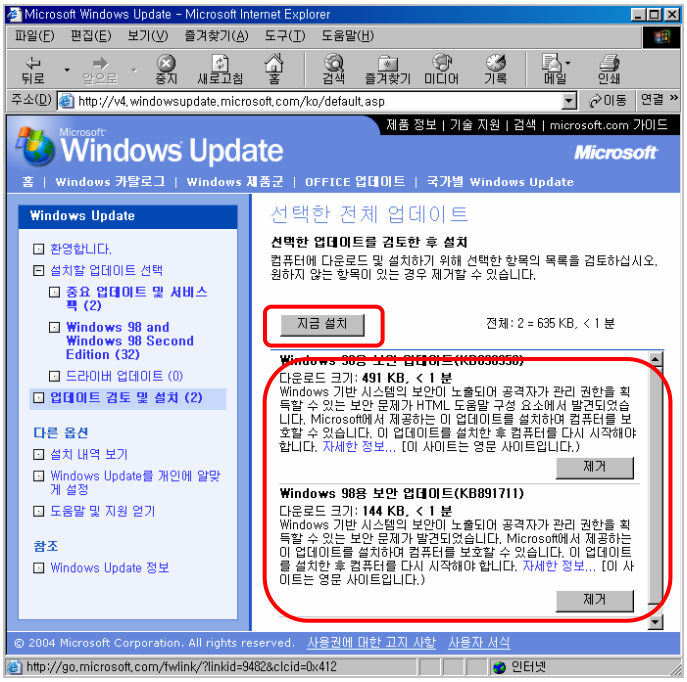


▶ 업데이트 종류

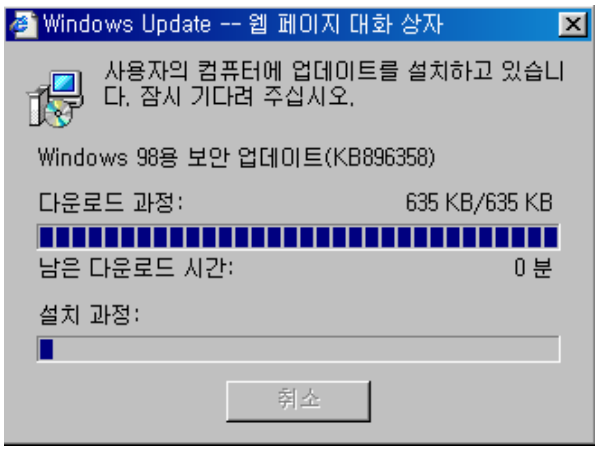
- 중요 업데이트 및 서비스 팩 : 필수적으로 설치해야 하는 패치입니다.
- Windows 98 and Windows 98 Second Edition : 컴퓨터 기능의 확장을 위한 패치입니다.
- 드라이버 업데이트 : 하드웨어 장치(모뎀, 네트워크 카드, 프린터 등)의 올바른 동작으로 위한 패치입니다.

19. 패치 업데이트(4/5)

- “설치가 필요한 패치의 내용이 설명됩니다.
  - “지금 설치”를 클릭합니다.



- 패치가 설치됩니다.



- 설치된 패치의 종류에 따라 컴퓨터를 재부팅 해야 하는 경우도 있습니다.

19. 패치 업데이트(5/5)

주의사항

- 앞에서 설명한 방법으로 패치 업데이트가 수행되지 않는 경우에는 마이크로소프트의 "다운로드센터(www.microsoft.com/downloads)"에 접근하여 "Internet Explorer 6 SP 1"을 먼저 설치하십시오.
- 이후에는 앞에서 설명한 방법으로 자동적인 패치 업데이트가 가능합니다.
- "현재 사용 가능한 중요 업데이트가 없습니다." 라는 메시지가 나올 때까지 반복합니다.

20. CD-ROM 자동실행 해제(1/3)

개 요

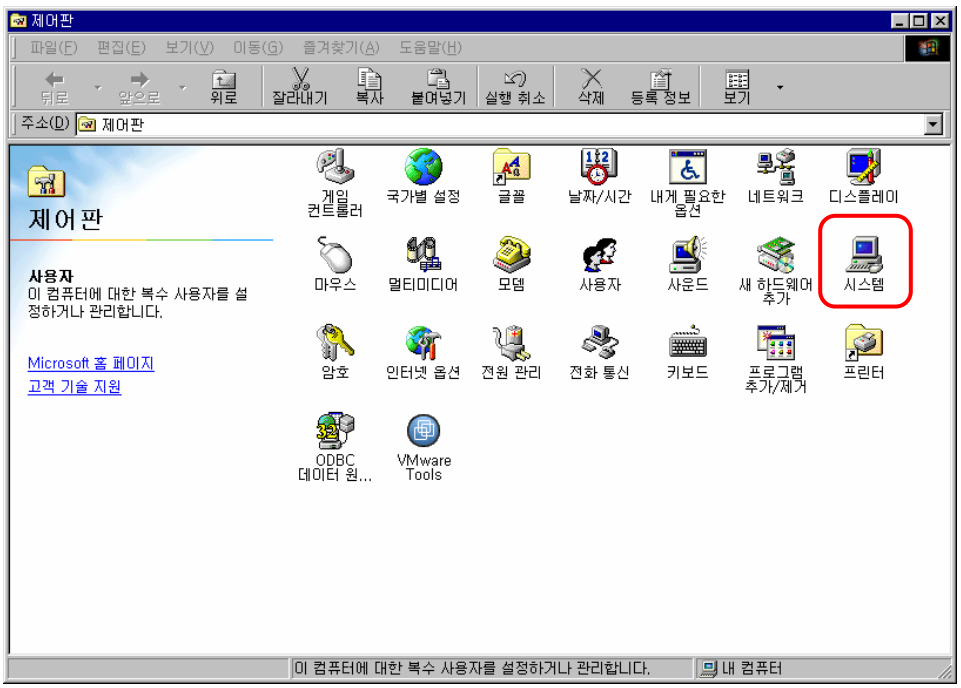
- Windows 98은 사용자 편의를 위해 CD를 넣으면 자동으로 실행을 시키는 기능을 제공하고 있습니다.
- 그러나 이 기능은 CD를 통한 악성 프로그램 설치 및 실행을 가능하게 합니다.
- 따라서 CD-ROM 자동실행을 해제하는 것이 바람직합니다.

미사용시의 문제점

- CD를 통해 사용자가 인식하지 못한 상태에서 컴퓨터가 웜·바이러스 등에 감염될 수 있습니다.

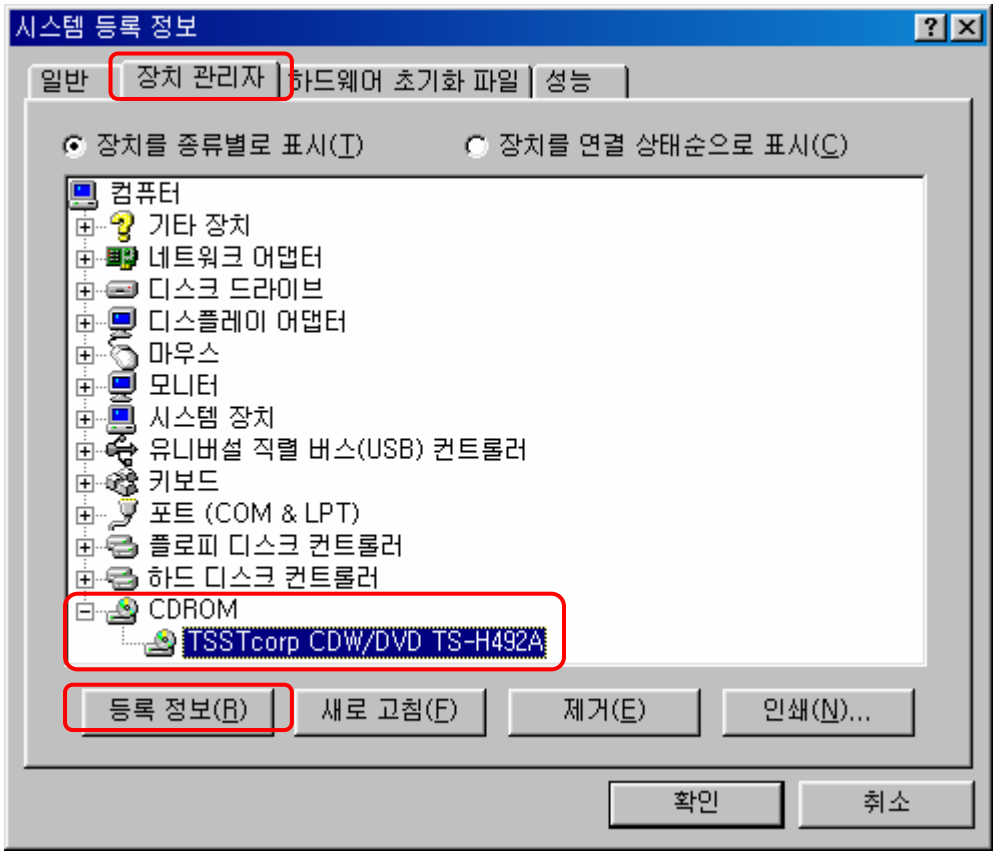
통제방법

- 「제어판」 창을 엽니다.(9페이지 참조)
- 「제어판」 창에서 "시스템" 항목을 선택합니다.



20. CD-ROM 자동실행 해제(2/3)

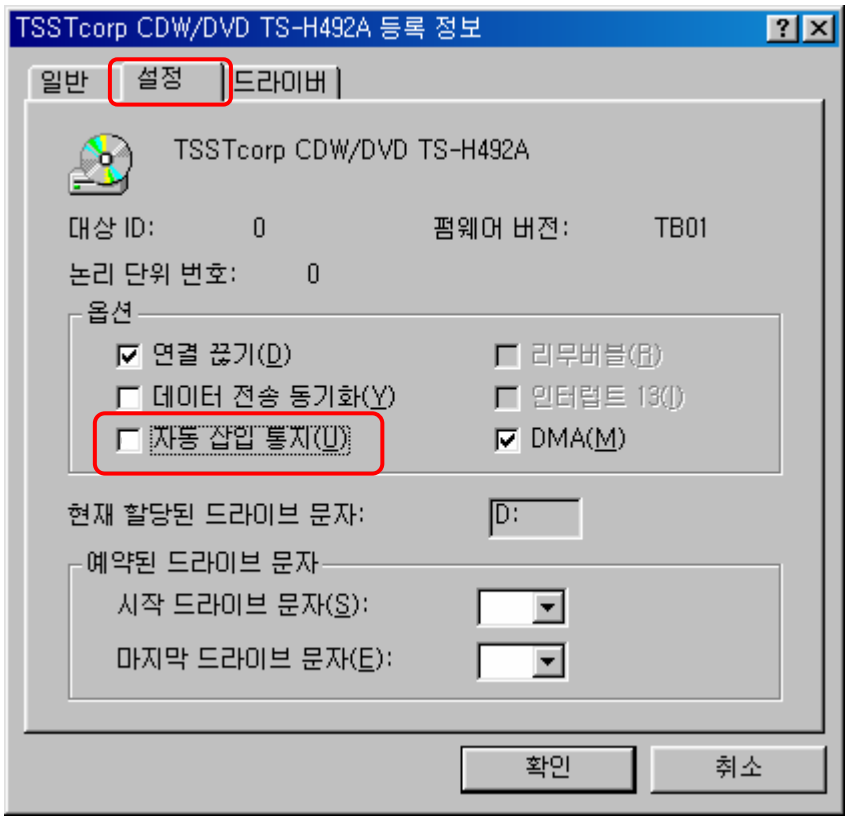
◆ 「시스템 등록 정보」 창에서 “장치관리자” 탭을 선택하면 다음과 같은 화면이 보입니다.



◆ 설치되어 있는 CDROM을 선택하고 “등록정보(R)”를 선택합니다.

20. CD-ROM 자동실행 해제(3/3)

- 현재 설치되어 있는 CD-ROM의 등록정보가 보이는 데, 이중에서 "설정" 탭을 선택합니다.



- 위 그림과 같이 "자동 삽입 통지(U)" 항목의 설정을 해제합니다.
- 설정을 해제한 후에는 "확인"을 누르고 컴퓨터를 재부팅 합니다.

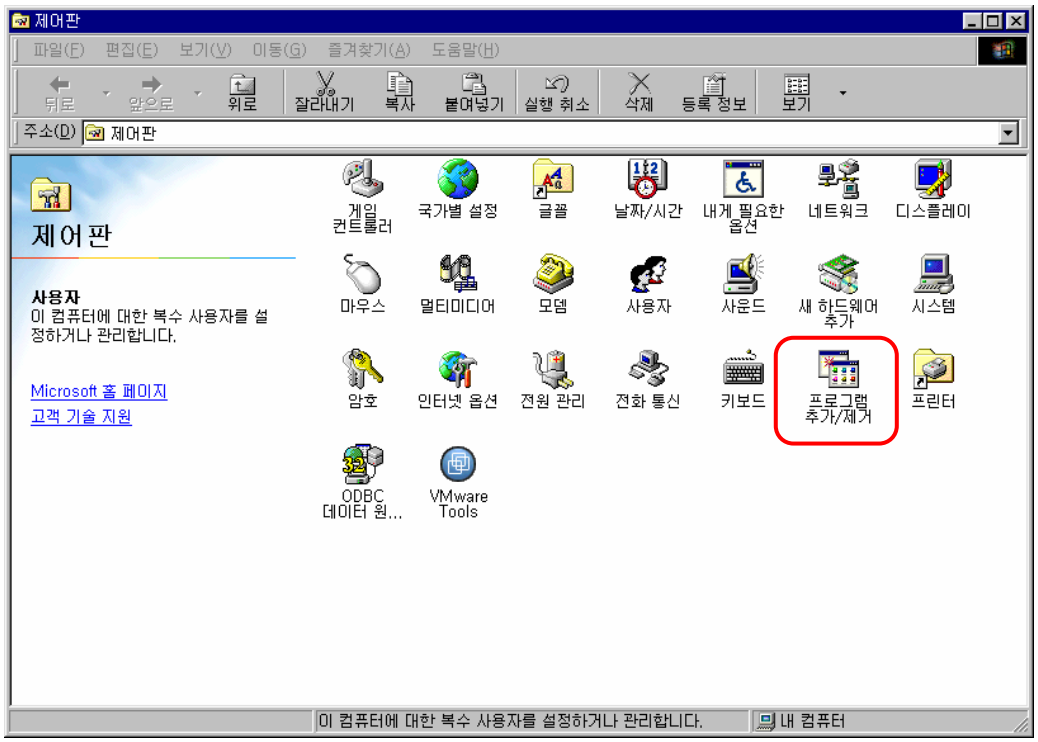
21. 불필요한 프로그램 제거(1/2)

개 요

- 컴퓨터를 이용하다 보면 많은 프로그램들을 설치하게 됩니다. 또한 사용자가 모르는 사이에 설치되는 프로그램들도 있습니다.
- 설치된 프로그램들 중에서 일부는 불필요한 것들이며, 컴퓨터 성능을 떨어뜨리거나 보안환경을 위협하는 요소로 작용합니다.
- 반드시 필요한 프로그램 이외의 것들은 가급적 삭제하는 것이 바람직합니다.

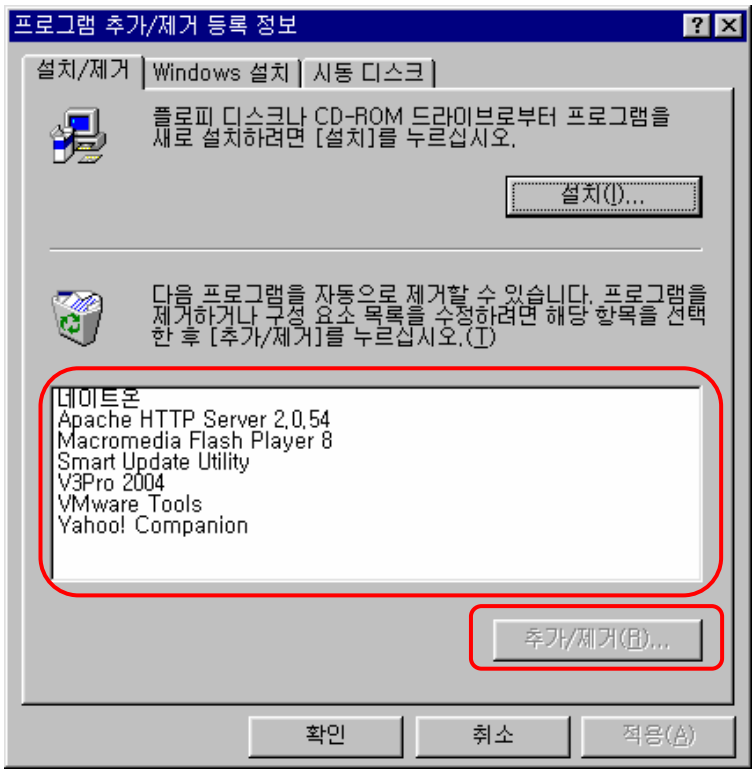
탐지 및 제거방법

- 현재 설치되어 있는 프로그램 확인 및 제거 방법
  - 「제어판」 창을 엽니다.(9페이지 참조)
  - 「제어판」 창에서 "프로그램 추가/제거"를 선택합니다.



21. 불필요한 프로그램 제거(2/2)

- 「프로그램 추가/제거 등록 정보」 창이 열립니다.



- 이 창에는 현재 컴퓨터에 설치되어 있는 프로그램들이 나열됩니다.
- 제거하고자 하는 프로그램을 선택한 후에 "추가/제거(R)..." 버튼을 클릭하면 해당 프로그램을 제거하는 절차가 시작됩니다.
- 제거 작업이 완료된 후에, 설치되어 있는 프로그램을 다시 확인하면 해당 프로그램이 리스트에 없는 것을 확인할 수 있습니다.

주의사항

- 설치되어 있는 프로그램을 함부로 제거하지 마십시오!
- 프로그램을 제거하기 전에 컴퓨터 관리 담당자와 상의를 하고 제거할 프로그램을 결정하십시오.