Windows XP
보안가이드라인

머 리 말

❑ 목적

- ❍ 본 가이드라인은 Windows XP(SP1 및 SP2 포함)를 사용하는 컴퓨터의 환경을 가급적 안전하게 유지하기 위한 방법들을 설명하고 있습니다.

❑ 대상

- ❍ 본 가이드라인은 Windows XP를 사용하는 사용자들 중에서 컴퓨터 관련 지식이 많지 않은 초보자들을 대상으로 하여 작성되었습니다.
- ❍ 화면을 활용한 설명을 위주로 하여 초보자들도 쉽게 따라 할 수 있도록 하였습니다.

❑ 구성

- ❍ 가이드라인은 크게 다섯 부분(사용자 계정 보안, 네트워크 보안, 시스템 유지/관리 보안, 바이러스/웜 보안, 문제점 해결)에 총 25개 항목으로 구성되어 있습니다.
- ❍ 본 가이드라인의 설명과정에서 활용된 응용 프로그램들은 설명의 이해도를 높이기 위해 단순 참고로 사용한 것으로 국가기관 및 공공기관이 관련제품을 사용하고자 할 경우 국가정보원 IT보안 인증사무국(www.kecs.go.kr)의 내용을 참조하시기 바랍니다.

목 차

I. 사용자 계정 보안

1. 로그온 패스워드 사용(1/6)

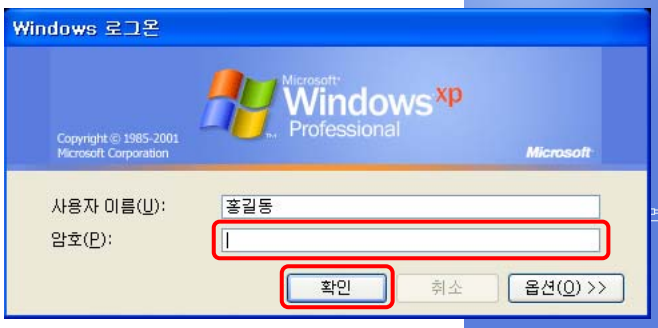
개 요

- 로그온 패스워드란 사용자가 컴퓨터 사용이 허용되어 있는 지를 확인하는 수단으로써, 등록된 사용자만 컴퓨터를 사용할 수 있도록 해주는 기능입니다.
  - 이 항목에서 보여지는 창 혹은 화면에서는 "암호"라는 용어를 사용하고 있으나, 일반적으로 "패스워드"라는 용어가 많이 사용되므로, 설명에서는 "패스워드"를 사용합니다.
- Windows XP는 두 가지 종류의 로그온 화면을 제공합니다. 하나는 Windows 2000까지 써오던 「Windows 로그온」 창이고, 다른 하나는 Windows XP부터 제공하는 「시작화면」입니다.
- 「시작화면 」에서는 자신의 "사용자 이름(ID)"를 선택하고 "암호(패스워드)"를 입력하면 되고 「Windows 로그온」 창에서는 자신의 "사용자 이름(ID)"과 "암호(패스워드)"를 입력하여 컴퓨터에 접근하게 됩니다.

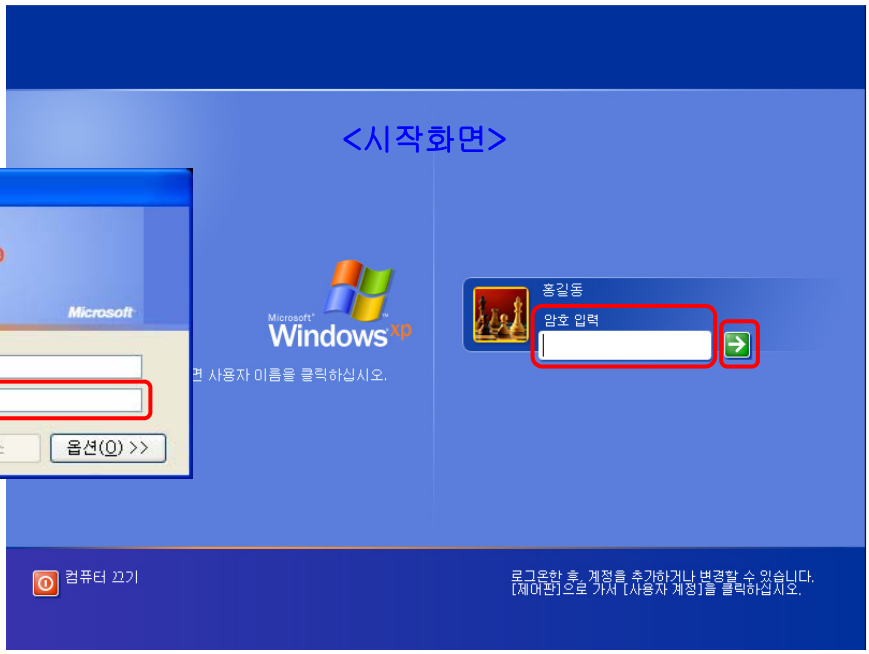
미사용시의 문제점

- 로그온 패스워드를 사용하지 않으면 부팅 중에 다음의 그림과 같은 「Windows 로그온」 창이나 「시작화면」이 나타났을 때 패스워드를 입력하지 않고 "확인" 또는 "화살표" 버튼을 선택해서 인증과정 없이 로그온할 수 있습니다.
- 결과적으로 불순한 의도를 가진 사용자를 포함하여 누구나 컴퓨터를 불법적으로 사용할 수 있는 환경이 제공됩니다.

<로그온 창>



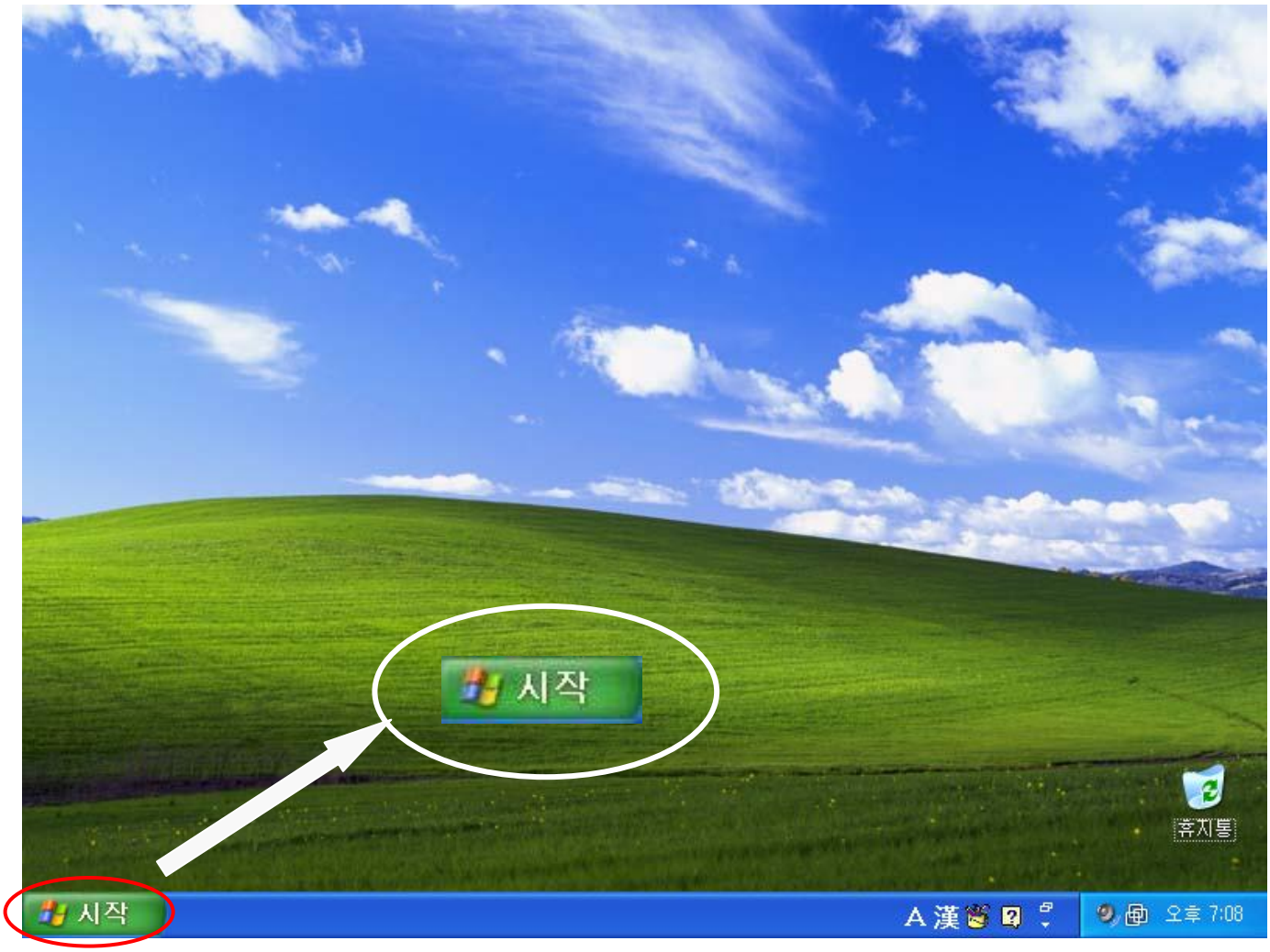
<시작화면>



1. 로그온 패스워드 사용(2/6)

설정방법

- 현재 로그온한 사용자의 패스워드를 설정해야 합니다. 패스워드의 설정은 「제어판」에서 설정할 수 있습니다.
- 「제어판」 창 열기
  - 로그온 패스워드 사용 뿐만 아니라 다른 보안항목들을 설정하기 위해서는 제어판을 사용해야 하는 경우가 많습니다.
  - 바탕화면의 좌측 하단에 있는 "시작" 버튼을 찾아 선택합니다.

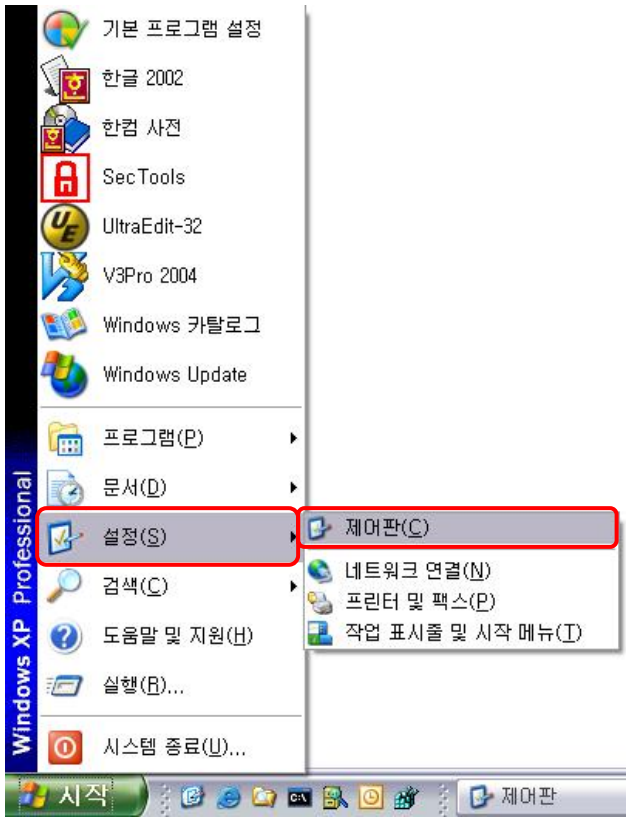


1. 로그온 패스워드 사용(3/6)

- Windows XP의 시작메뉴는 설정에 따라 다음 그림처럼 두 가지입니다. Windows XP에서 사용하기 시작한 시작메뉴와 Windows 98 혹은 2000에서 사용하던 예전 형태의 시작메뉴가 그것인데, 설명에서는 「Windows XP 시작메뉴」를 기준으로 설명합니다.
- "시작" 버튼 선택 후 보이는 메뉴에서 "제어판" 혹은 "설정" → "제어판"을 선택합니다.

<Windows XP 시작메뉴>

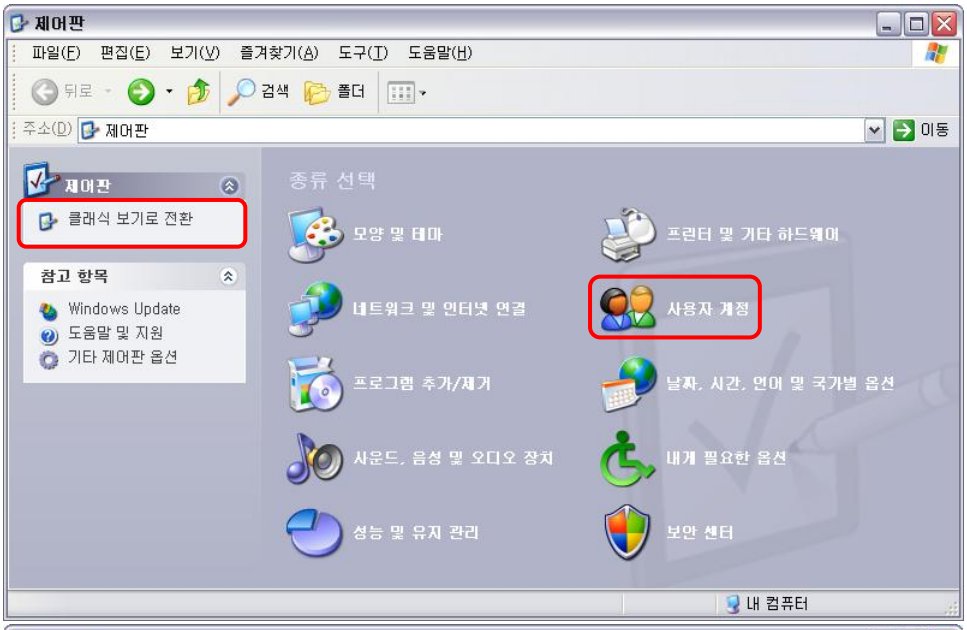
<Windows 98 혹은 2000 형태의 시작메뉴>



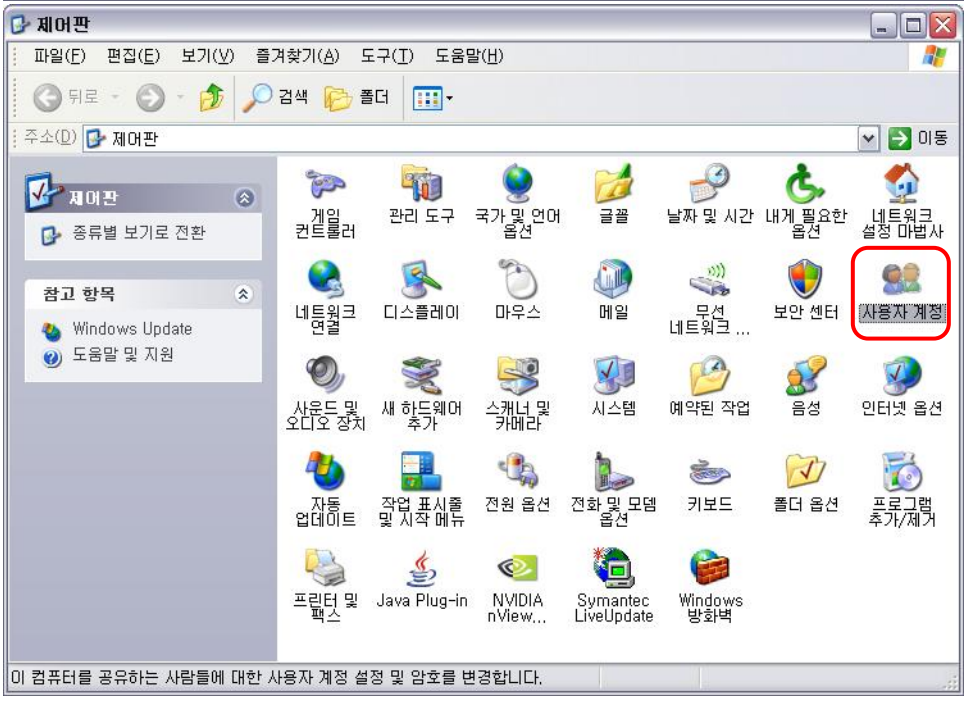
1. 로그온 패스워드 사용(4/6)

❍ 패스워드 설정

- Windows XP의 「제어판」 창은 설정에 따라 다음 그림처럼 두 가지입니다. “종류별 보기”와 “클래식 보기”가 그것인데 설명에서는 “클래식 보기”를 기준으로 설명합니다. “종류별 보기” 상태에서 좌측에 보이는 “클래식 보기로 전환”을 선택하면 “클래식 보기” 상태로 변경할 수 있습니다.
- 「제어판」 의 “클래식 보기”에서 “사용자 계정” 항목을 선택하여 실행합니다.



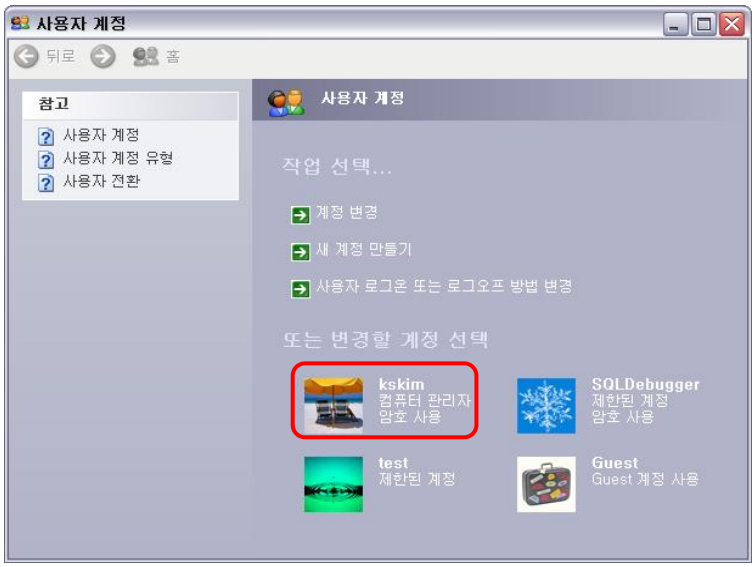
<종류별 보기>



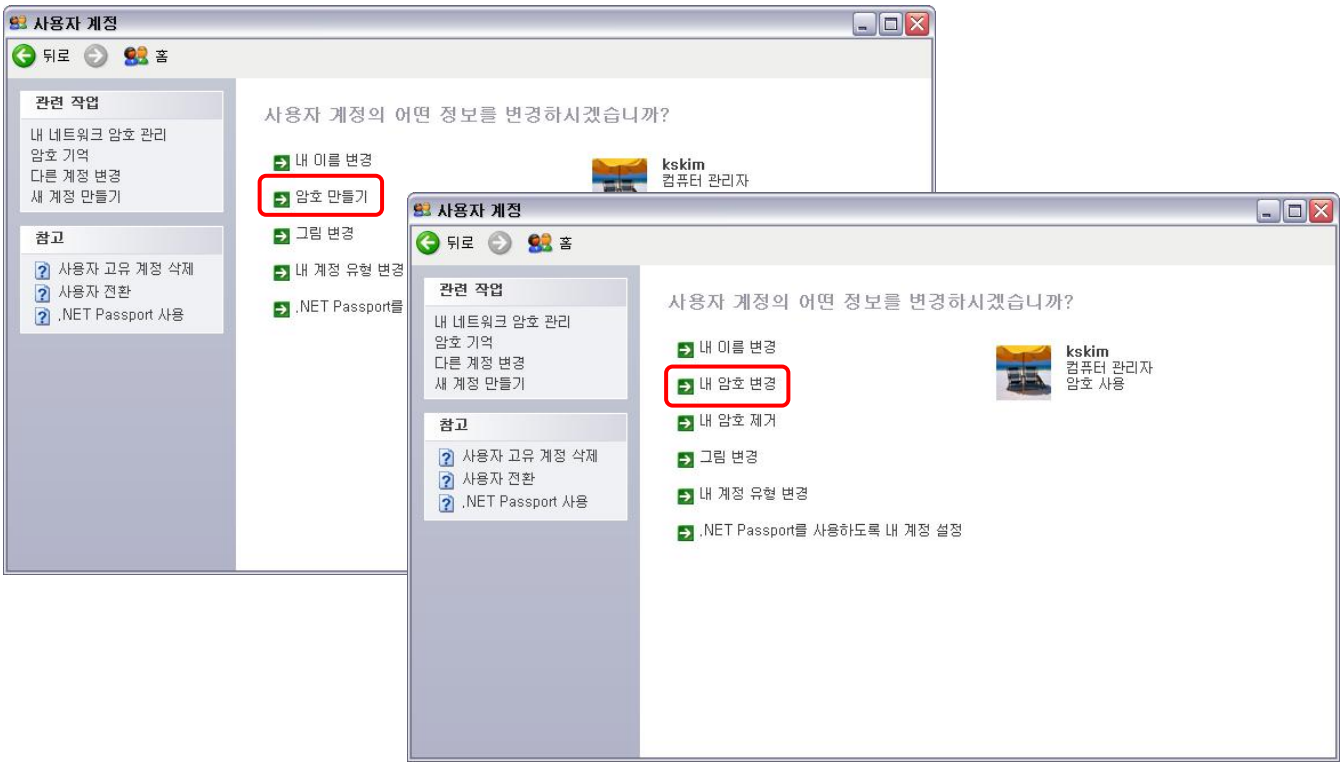
<클래식 보기>

1. 로그온 패스워드 사용(5/6)

- 「사용자 계정」 창이 열리며 현재 컴퓨터에 등록되어 있는 사용자의 목록이 보입니다. 현재 사용하는 계정을 선택합니다.

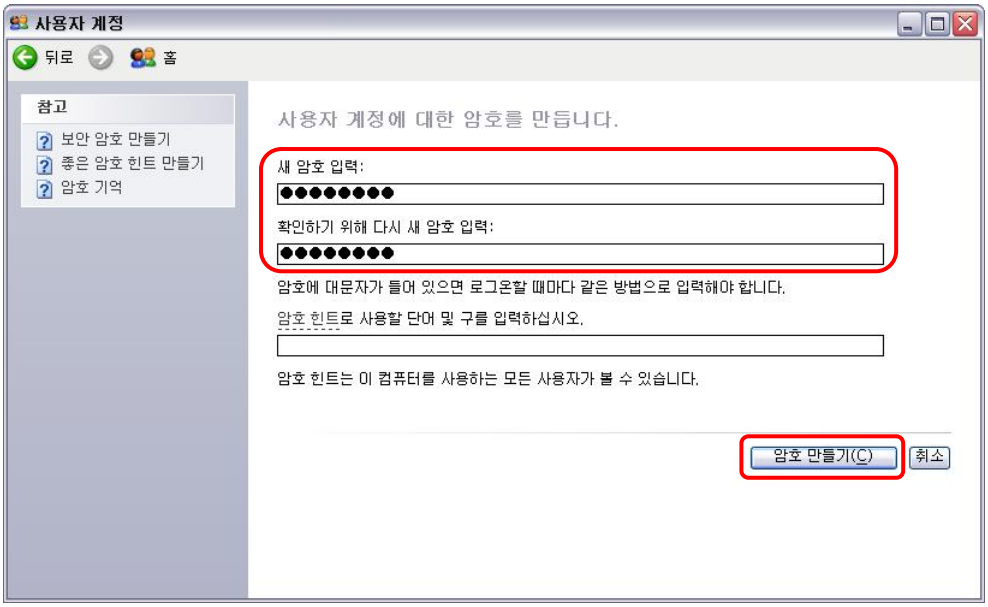


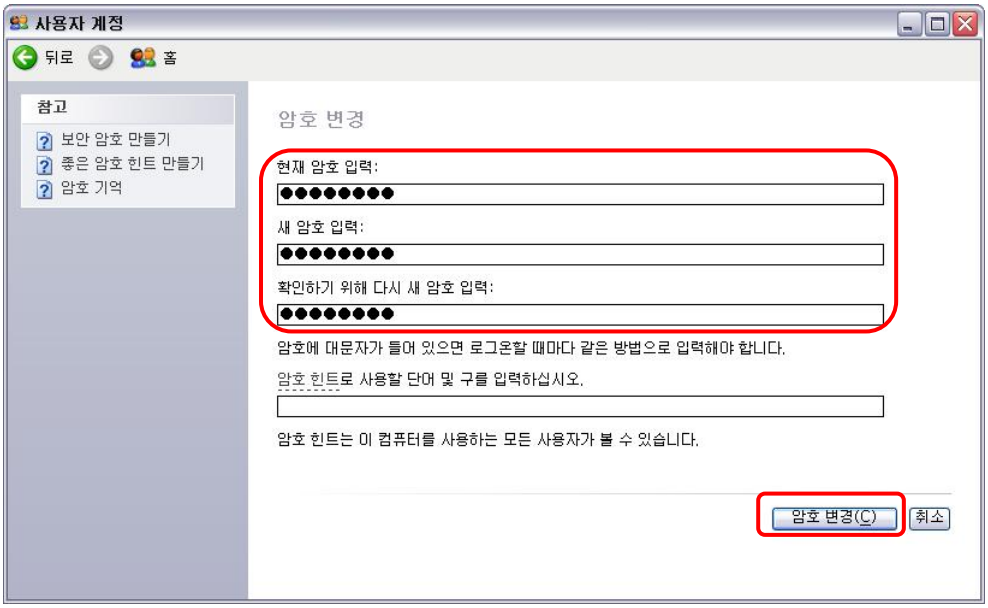
- 사용하던 패스워드의 존재 여부에 따라 다음 두 화면이 나타날 수 있습니다. 사용하던 패스워드가 있으면 “내 암호 변경”, 없으면 “암호 만들기”를 선택합니다.



1. 로그온 패스워드 사용(6/6)

- “암호 만들기”를 선택하였다면 “새 암호 입력”과 “확인하기 위해 다시 새 암호 입력”을 입력하고 “암호 만들기” 버튼을 선택하고, “내 암호 변경”을 선택하였다면 “현재 암호 입력” 부분도 입력을 하고 “암호 변경” 버튼을 선택합니다.





2. 로그온 패스워드 사용 기간 제한(1/1)

개 요

- 복잡한 패스워드를 사용하고 있어도 하나의 패스워드를 너무 오랜 기간 사용하게 되면 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 소통되는 데이터의 내용을 공격자에게 불법적으로 전달해 주는 기술입니다.
  - 패스워드도 스니핑에 의해 네트워크에서 노출될 수 있습니다.

3. 로그온 패스워드 복잡도 강화(1/1)

개 요

- 컴퓨터에서 사용하는 패스워드로 단순한 조합이나 연속된 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 추측하여 악용할 수 있습니다.

안전한 패스워드 사용방법

- 숫자/문자(대문자, 소문자 구별)/특수문자를 조합하여 최소 8자리 이상으로 사용하십시오.
- 다음은 주요문서에서 권장하는 패스워드의 조건입니다.
  - 패스워드의 최소 길이는 8자이어야 함 (DISA Windows XP Security Checklist)
  - 패스워드는 추측하기 힘들어야 하고 대문자, 소문자, 숫자, 특수문자를 반드시 포함해야 함 (Microsoft 기술문서)
  - 최소 패스워드 길이는 12자이어야 함 (NSA Guide to Securing Microsoft Windows XP)
  - 패스워드 길이를 수학적으로 계산한 결과, 권장하는 패스워드의 최소길이는 8자임 (DoD Password Management Guideline)

4. 최근 로그온 패스워드 기억(1/1)

개 요

- 로그온 패스워드의 사용 기한을 제한하여 로그온 패스워드를 변경하게 되어도 최근에 사용한 로그온 패스워드를 재사용한다면 로그온 패스워드의 사용 기한을 제한하는 목적을 이룰 수 없습니다.

패스워드 재사용시 문제점

- “2. 로그온 패스워드 사용기간 제한”에서 언급한 바와 같이 동일한 패스워드를 장기간 이용하게 되면 패스워드가 노출될 수 있으므로 패스워드의 사용 기한을 제한하는 것이 좋습니다.
- 패스워드의 사용 기한을 제한하여도 변경 시에 동일한 패스워드를 사용한다면 동일한 패스워드를 장기간 이용하게 되는 것과 같습니다.
- 최근에 사용한 로그온 패스워드를 재사용하지 말고 새로운 패스워드를 이용해야 합니다.

5. Guest 계정 비활성화(1/6)

개 요

- Windows XP 운영체제에는 설치 시에 자동으로 생성되는 Guest라는 계정이 존재합니다. 기본값으로 비활성화되어 있으나, 사용자가 프린터나 폴더 공유기능을 사용할 때 자동으로 활성화될 수 있습니다.
- Guest 계정은 사용하지 않는 것이 안전합니다.

미사용시의 문제점

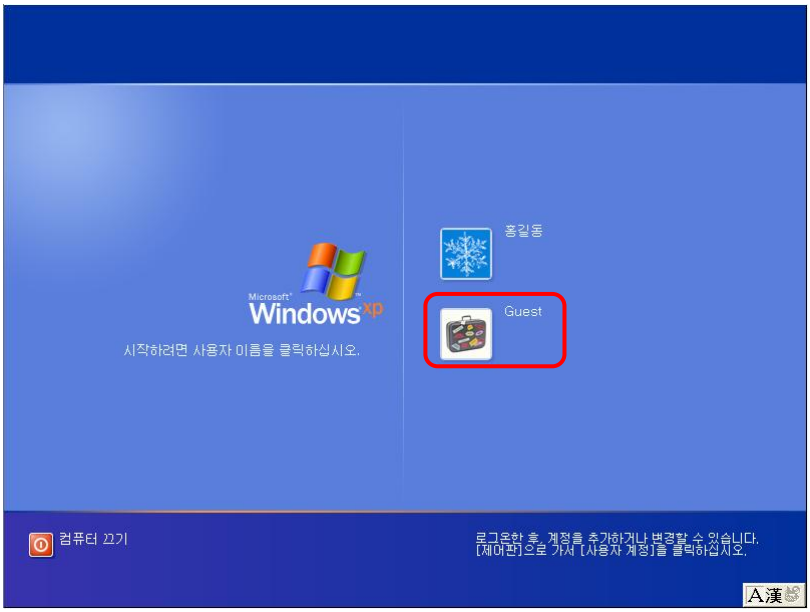
- 모든 사용자가 Guest 계정을 이용해 시스템에 접근할 수 있습니다.
- 원격으로 시스템에 접근할 경우 시스템 정보 및 내부자료 유출이 가능합니다.

설정방법

- Guest 계정은 두 가지의 상태가 있습니다. 켜기/끄기 상태와 활성화/비활성화 상태가 그것입니다.
- 켜기(Turn on)/끄기(Turn off)
  - Guest 계정이 Windows의 시작화면에 표시될 지 여부를 결정합니다.
  - Guest 계정을 켜기(Turn on) 상태로 하면 자동으로 활성화(Enable) 상태가 됩니다.
- 활성화(Enable)/비활성화(Disable)
  - Guest 계정의 사용 여부를 나타냅니다.
  - Guest 계정을 비활성화(Disable)시키면 자동으로 끄기(Turn off)상태가 됩니다.
- 다음 페이지부터 차례로 설정방법을 설명합니다.

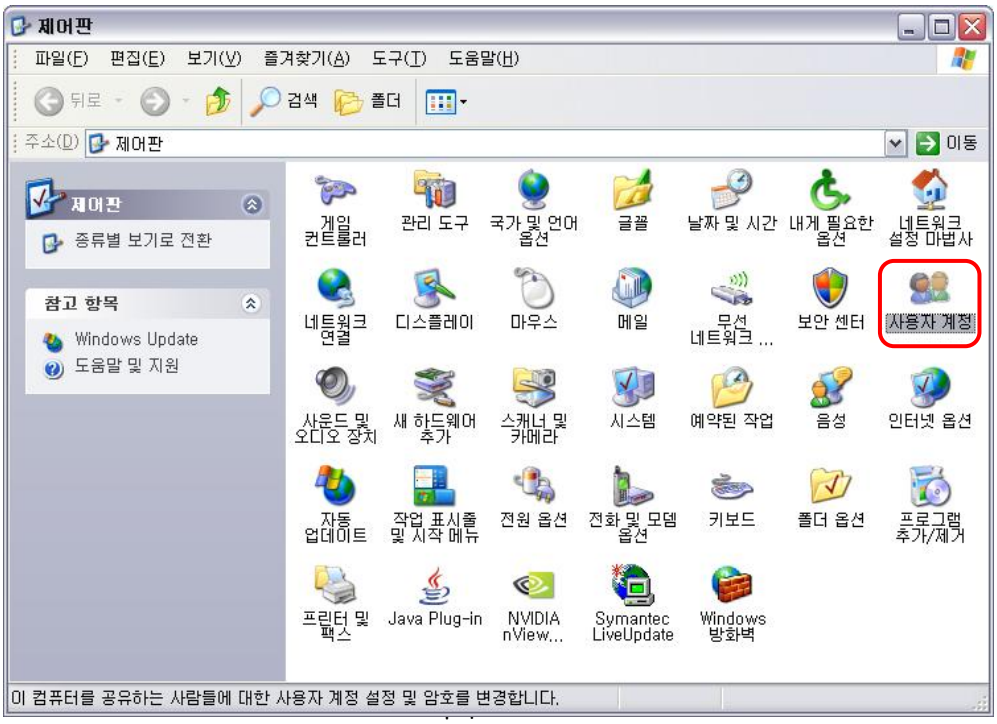
5. Guest 계정 비활성화(2/6)

❍ Guest 계정을 켜기 상태로 한 시작화면



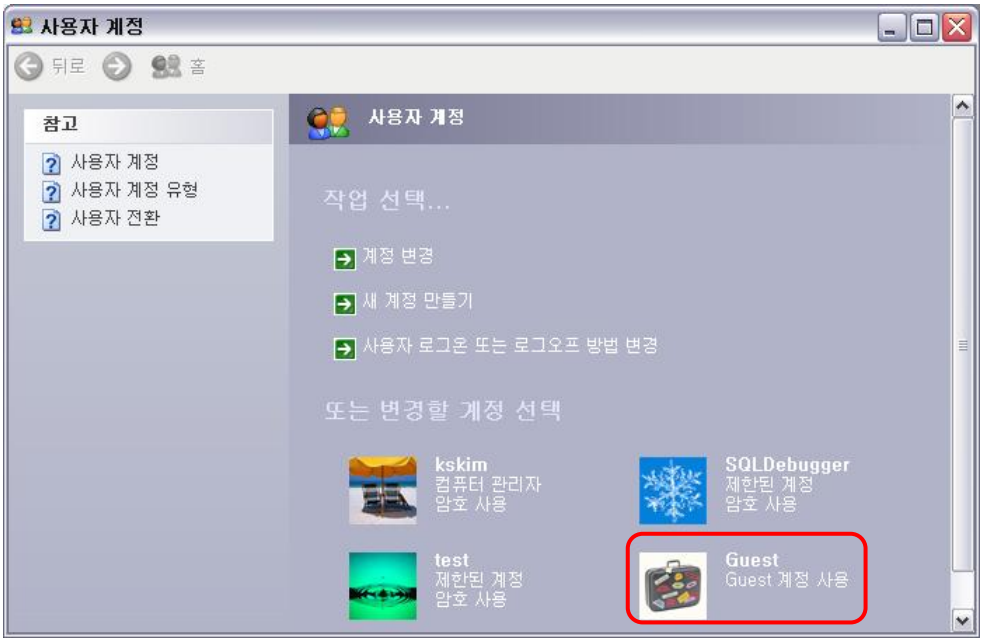
❍ Guest 계정 켜기/끄기 상태 설정을 위한 창으로 이동

- 「제어판」을 열어 “클래식 보기” 상태로 합니다.
- 「제어판」의 “클래식 보기”에서 “사용자 계정”를 선택하여 실행합니다.



5. Guest 계정 비활성화(3/6)

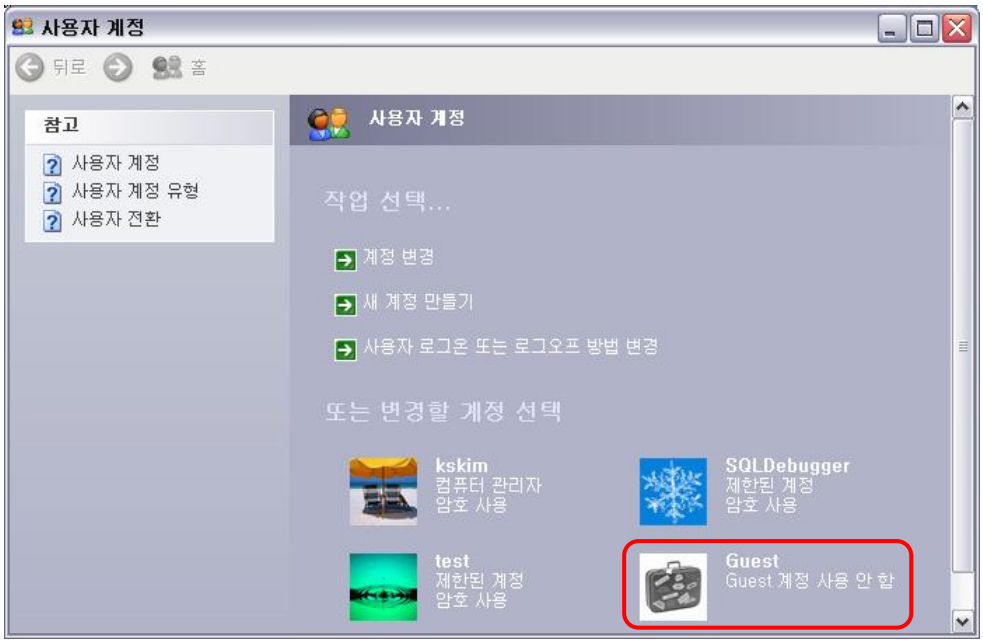
- 「사용자 계정」 창이 열리며 현재 컴퓨터에 등록되어 있는 사용자의 목록이 보입니다. Guest 계정을 선택합니다.
  - 현재는 Guest 계정 사용(켜기) 상태로 설정되어 있습니다.



- Guest 계정 끄기를 선택합니다.

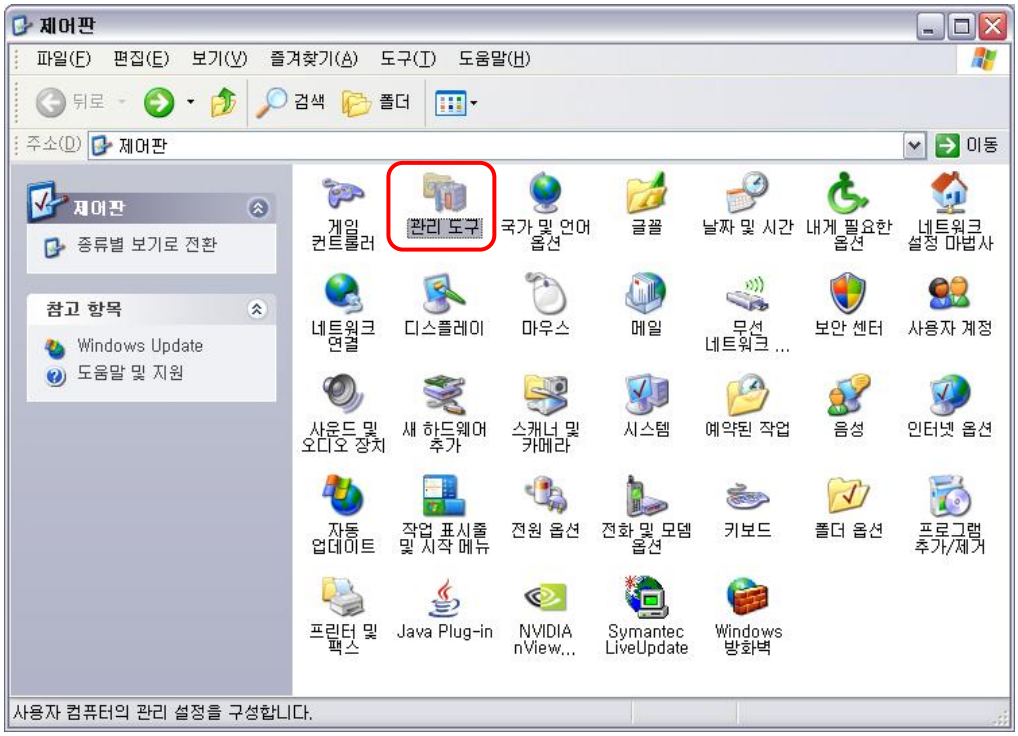
5. Guest 계정 비활성화(4/6)

- “Guest 계정 사용 안 함”(끄기)으로 설정되어 있음을 확인할 수 있습니다.



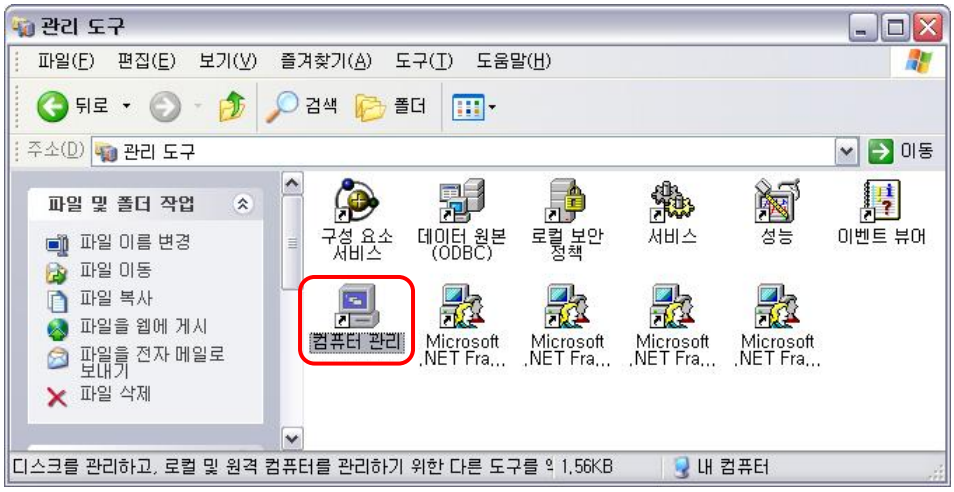
❍ Guest 계정 활성화/비활성화 상태 설정을 위한 창으로 이동

- Windows XP Home에서는 설정할 수 없습니다. 비활성화시키기 위해서는 PCChecker의 자동 수정 기능을 이용해야 합니다.
- 「제어판」을 열어 “클래식 보기” 상태로 합니다.
- 「제어판」의 “클래식 보기”에서 “사용자 계정”를 선택하여 실행합니다.

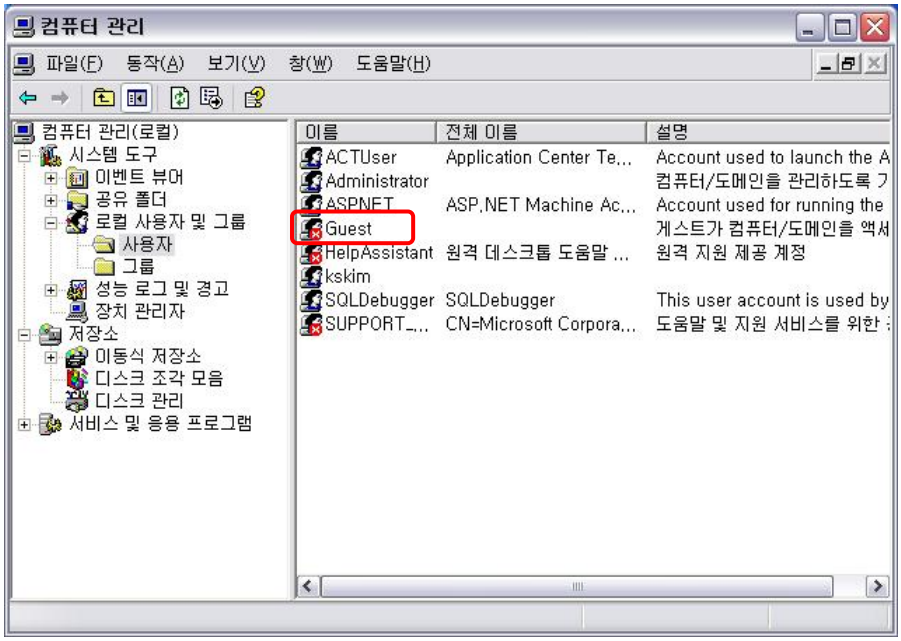


5. Guest 계정 비활성화(5/6)

- 「관리 도구」 창에서 “컴퓨터 관리”를 선택하여 실행합니다.

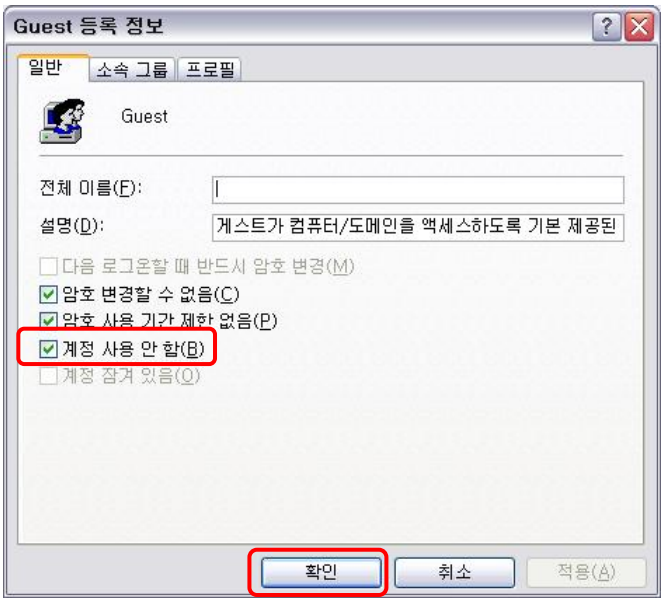


- 「컴퓨터 관리」 창에서 “컴퓨터 관리(로컬)”→”시스템 도구”→”로컬 사용자 및 그룹”→”사용자” 항목으로 이동하고 “Guest”를 선택하여 실행합니다.



5. Guest 계정 비활성화(6/6)

- 「Guest 등록 정보」 창에서 “계정 사용 안 함”(비활성화)을 선택하고 “확인”을 선택합니다.



6. BIOS 비밀번호 사용(1/4)

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

- 부팅시의 사용자 확인을 로그온 패스워드에만 의존하게 되어 사용자 확인 강도가 약해집니다.

설정방법

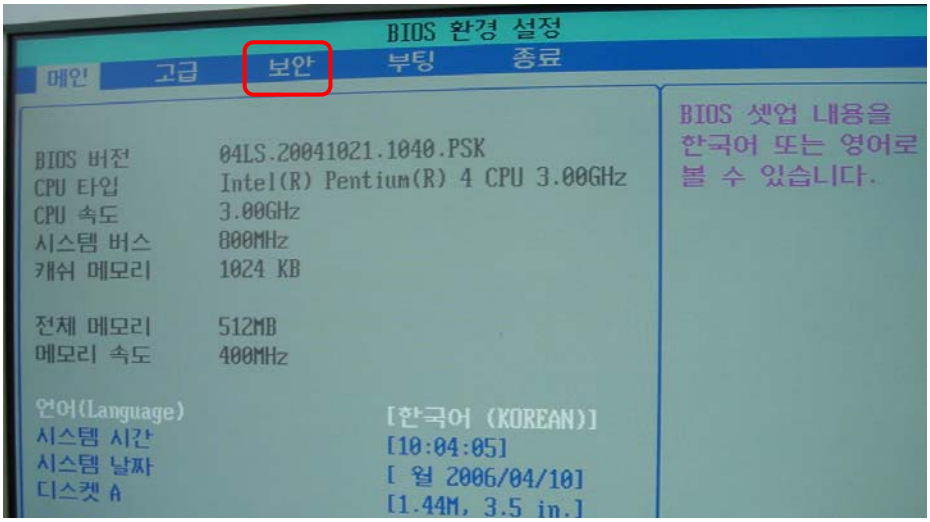
주의사항

- BIOS 셋업은 주요 하드웨어에 관한 설정값들이 존재하기 때문에 숙련자가 아니면 Password 이외의 값을 수정해서는 안되므로 주의가 요구됩니다.
- 설명에 활용한 화면은 피닉스 BIOS입니다.

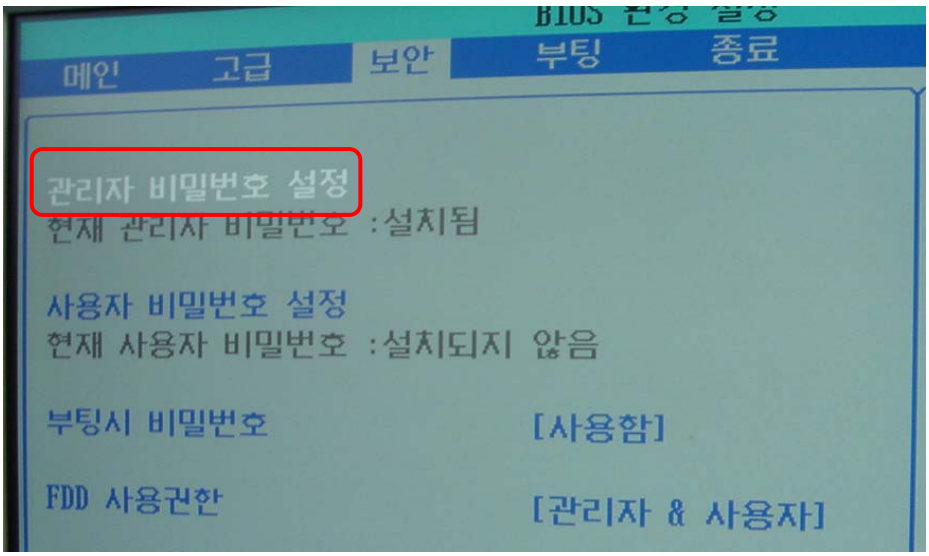
6. BIOS 비밀번호 사용(2/4)

❍ 피닉스 BIOS인 경우

- PC를 켠 후, 부팅 도중에 [F2]키를 누르면 다음과 같은 화면이 시작됩니다.

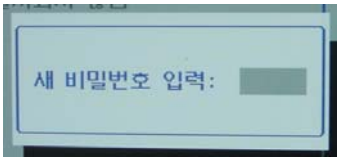


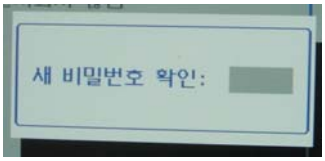
- BIOS 환경을 설정하는 화면으로 그림의 것은 한글로 설명되어 있으나, 컴퓨터의 기종에 따라 영어로 설명되어 있을 수도 있습니다.
- 보안(Security) 항목을 선택하면 다음의 화면이 시작됩니다.
- 항목 선택은 화살표 또는 탭(Tap)키를 이용합니다.



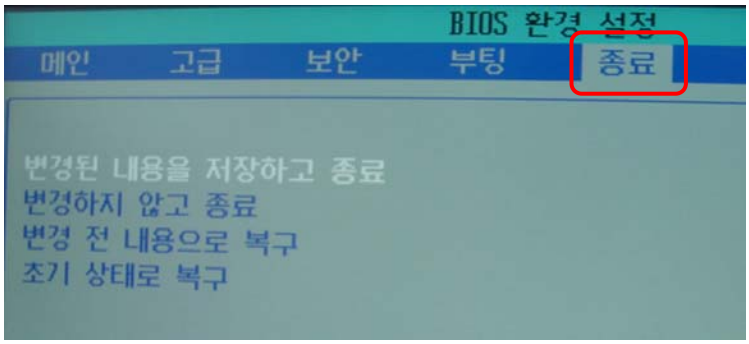
6. BIOS 비밀번호 사용(3/4)

- 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.





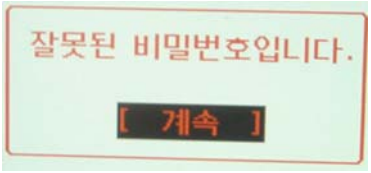
- 종료(Exit) 메뉴에서 “변경된 내용을 저장하고 종료(Save Change & Exit)”를 선택하여 빠져 나옵니다.



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

6. BIOS 비밀번호 사용(4/4)

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



❍ 어워드 BIOS인 경우

- PC를 켬과 동시에 [DEL](또는 [F1])키를 누릅니다.(윈도우 창이 뜨기 전)
- Bios features setup 항목에서 두번째인 Security option을 선택합니다.
- System을 선택합니다.
- Supervisor passwd 항목에서 암호를 입력합니다. – Confirm passwd 에 한번 더 입력하여 확인합니다.
- Save & Exit[F10]하여 종료합니다.

❍ 아미 BIOS인 경우

- PC를 켠후 [DEL]키를 누릅니다.
- CMOS 설정화면(메인화면)이 시작됩니다.
- Setup 항목으로 들어갑니다.
- Advanced 항목에서 Password check 항목을 Always로 선택합니다.
- [ESC]를 눌러 상위항목(메인화면)으로 이동합니다.
- Security 항목으로 이동합니다.
- Supervisor를 선택합니다.
- Password를 설정합니다.
- Exit 항목에서 Save Change & Exit를 선택하여 빠져 나옵니다.

II. 네트워크 보안

7. 공유 폴더 사용 제한(1/7)

개 요

- Windows XP에서는 사용의 편의를 위해 파일이나 프린터를 다른 사용자들과 공유하여 사용하는 기능을 제공합니다. 그러나 공유 기능을 부적절하게 사용할 경우 정보유출이나 해킹 등의 문제를 발생시킬 수 있습니다.
- 공유 기능을 사용하지 않는 것이 안전합니다.

부주의한 공유의 문제점

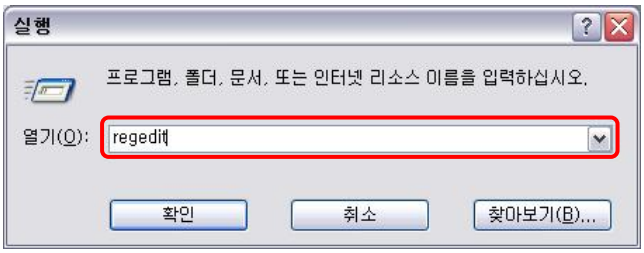
- 중요정보가 유출될 수 있습니다. 잠깐 동안의 공유를 위해 설정한 후에, 해제하지 않은 상황에서 공유폴더에 중요자료를 저장할 수 있으며, 공유 사실을 잊게되면 그 위험성은 더욱 커지게 됩니다.
- 해킹의 수단이 되기도 합니다.

공유를 차단하는 방법

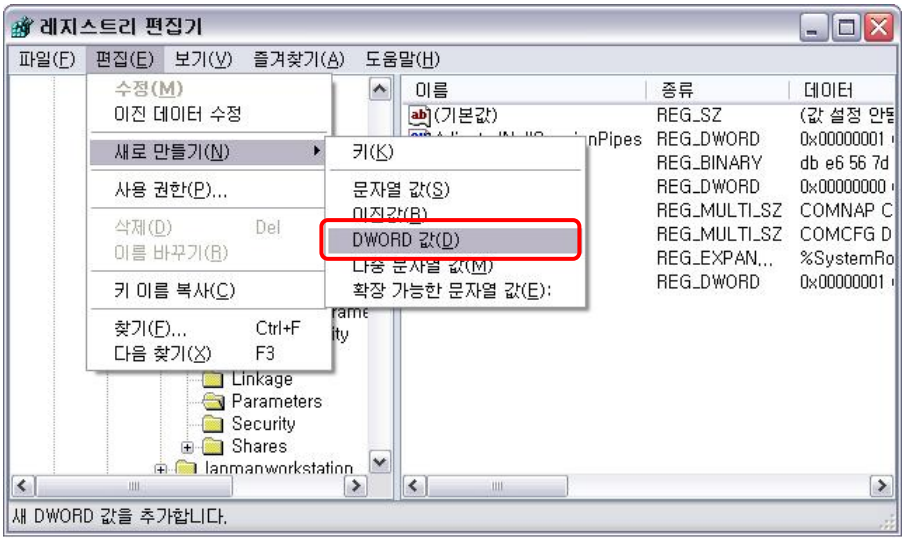
- 관리용 공유폴더를 차단하는 방법
  - 레지스트리 편집을 통해 차단할 수 있습니다.
  - "시작" → "실행" 메뉴를 선택합니다.

7. 공유 폴더 사용 제한(2/7)

- 「실행」 창이 열리면 “regedit” 명령어를 입력하고 “확인” 버튼을 선택합니다.

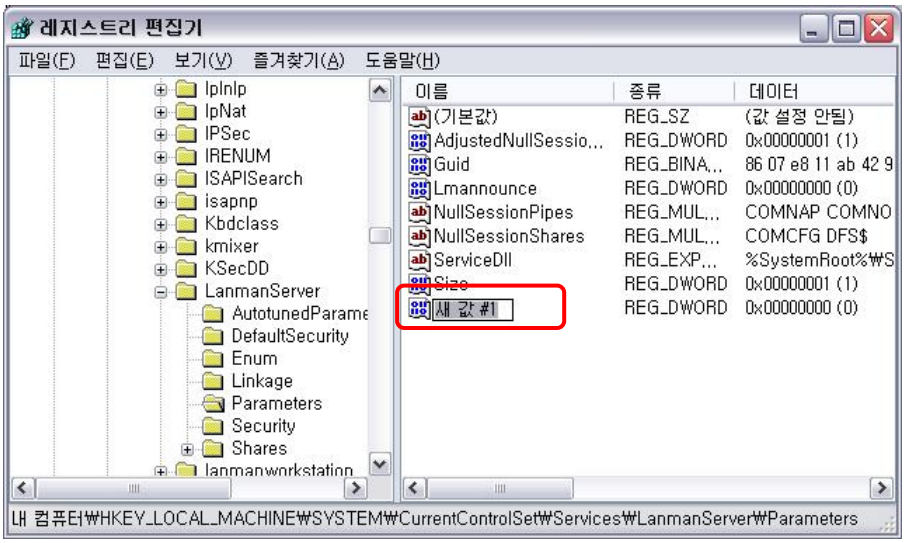


- 「레지스트리 편집기」 창에서 “HKEY_LOCAL_MACHINE” → “System” → “CurrentControlSet” → “Services” → “LanmanServer” → “Parameters”를 선택합니다.
- “편집” → “새로 만들기” → “DWORD 값”을 선택합니다.

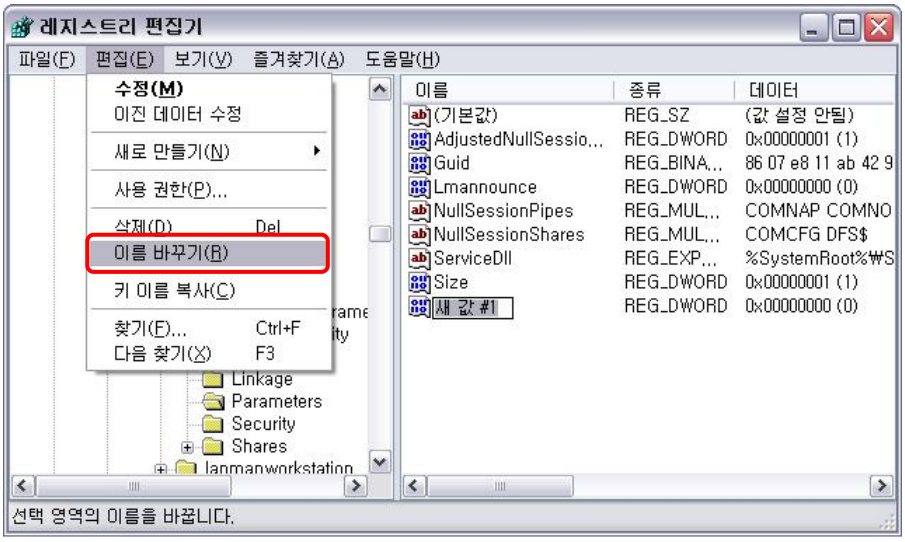


7. 공유 폴더 사용 제한(3/7)

- "새 값 #1" 값이 생성됩니다.

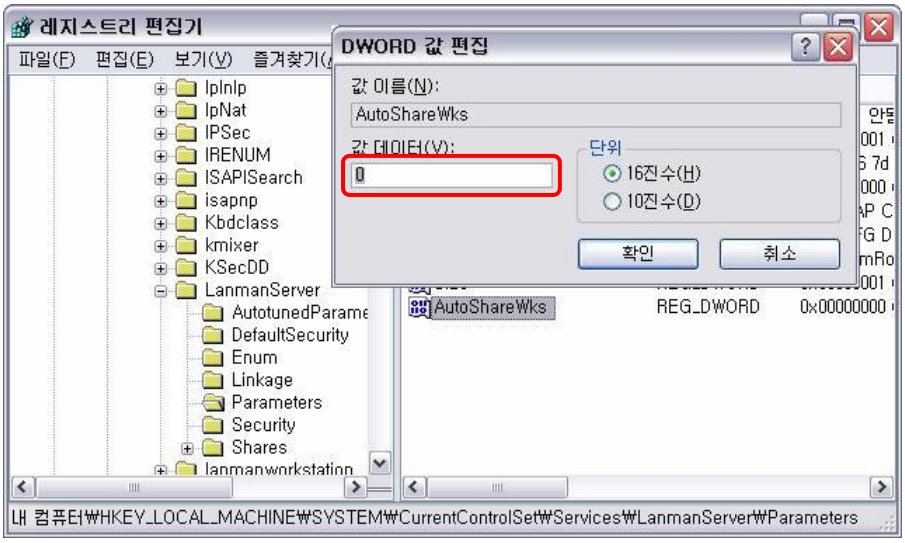


- 생성된 "새 값 #1"을 선택하고, "편집" → "이름 바꾸기"를 선택하여 이름을 "AutoShareWks"로 변경합니다.



7. 공유 폴더 사용 제한(4/7)

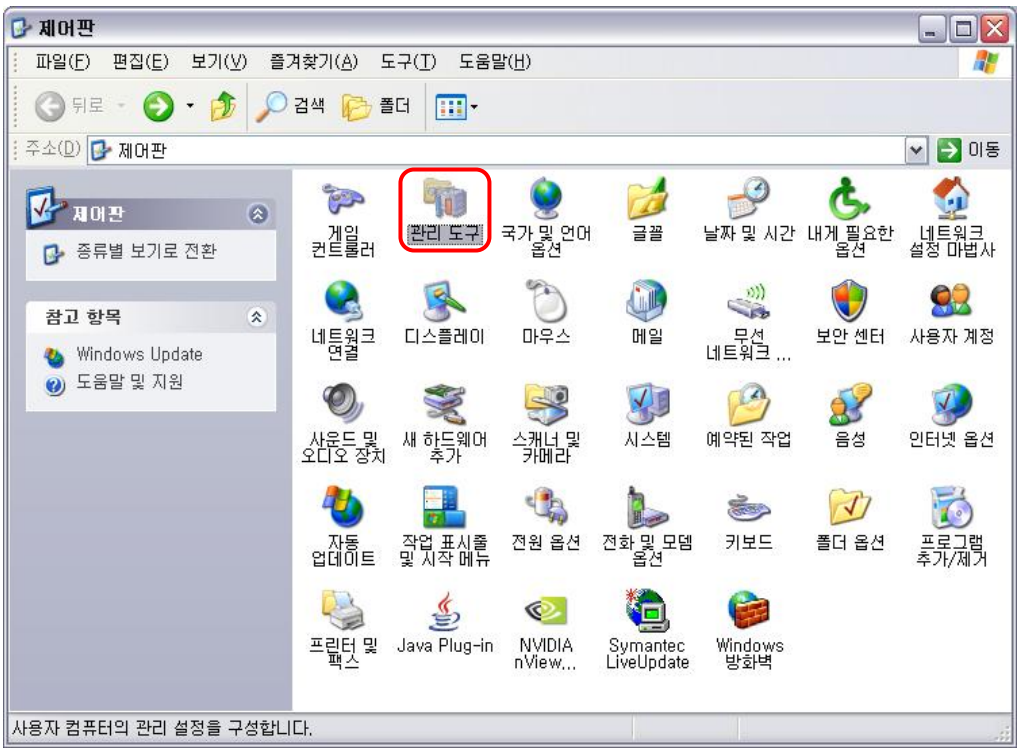
- “AutoShareWks”항목을 선택하고 “편집” → “수정”을 선택합니다.
- “값 데이터” 부분을 “0” 로 설정합니다.



- 레지스트리 값을 변경한 후 시스템을 재부팅해야 합니다.

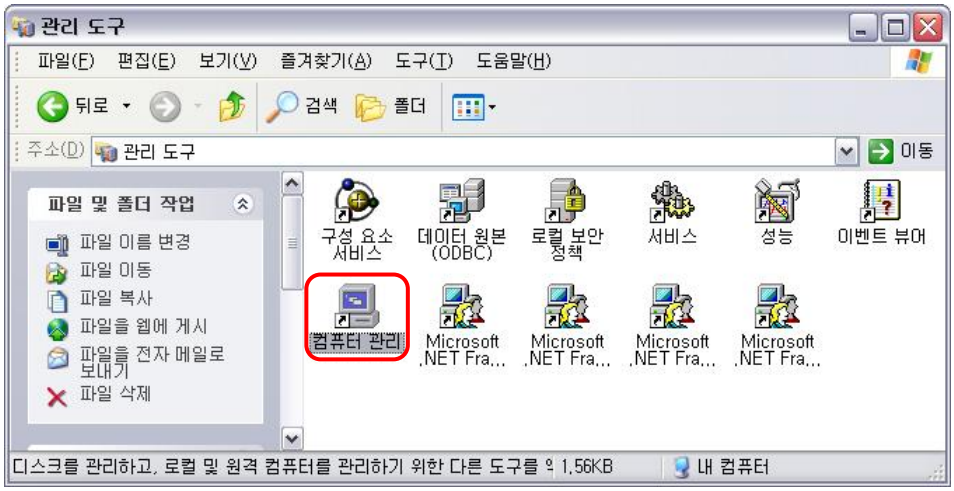
❍ 사용자가 생성하는 공유폴더를 제거하는 방법

- 「제어판」을 열어 “클래식 보기” 상태로 합니다.
- “관리 도구”를 선택하여 실행합니다.

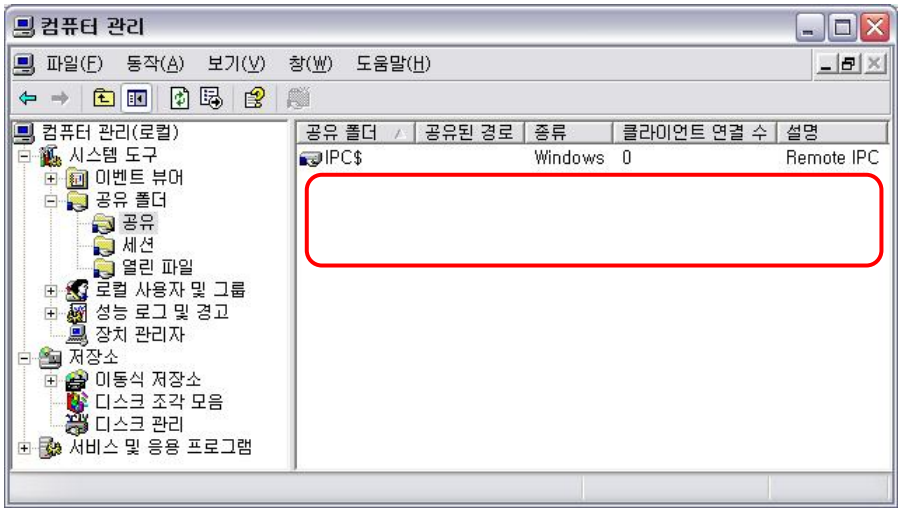


7. 공유 폴더 사용 제한(5/7)

- 「관리 도구」 창이 열리면 “컴퓨터 관리”를 선택하여 실행합니다.

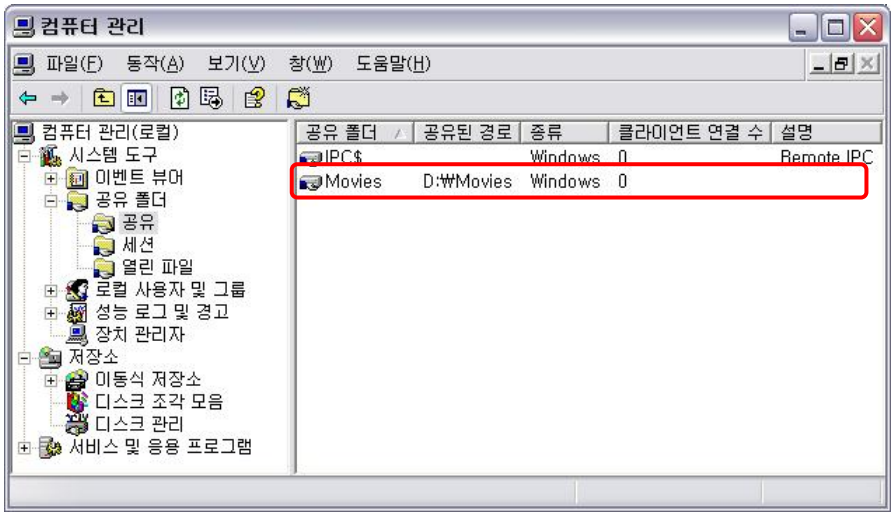


- “컴퓨터 관리” 창이 열리면 “컴퓨터 관리(로컬)” → “시스템 도구” → “공유 폴더” → “공유”로 이동합니다.
- 등록된 폴더가 없으면 사용자가 생성한 공유가 없다는 의미이므로 제거할 필요가 없습니다.(IPC$와 print$는 예외입니다.)

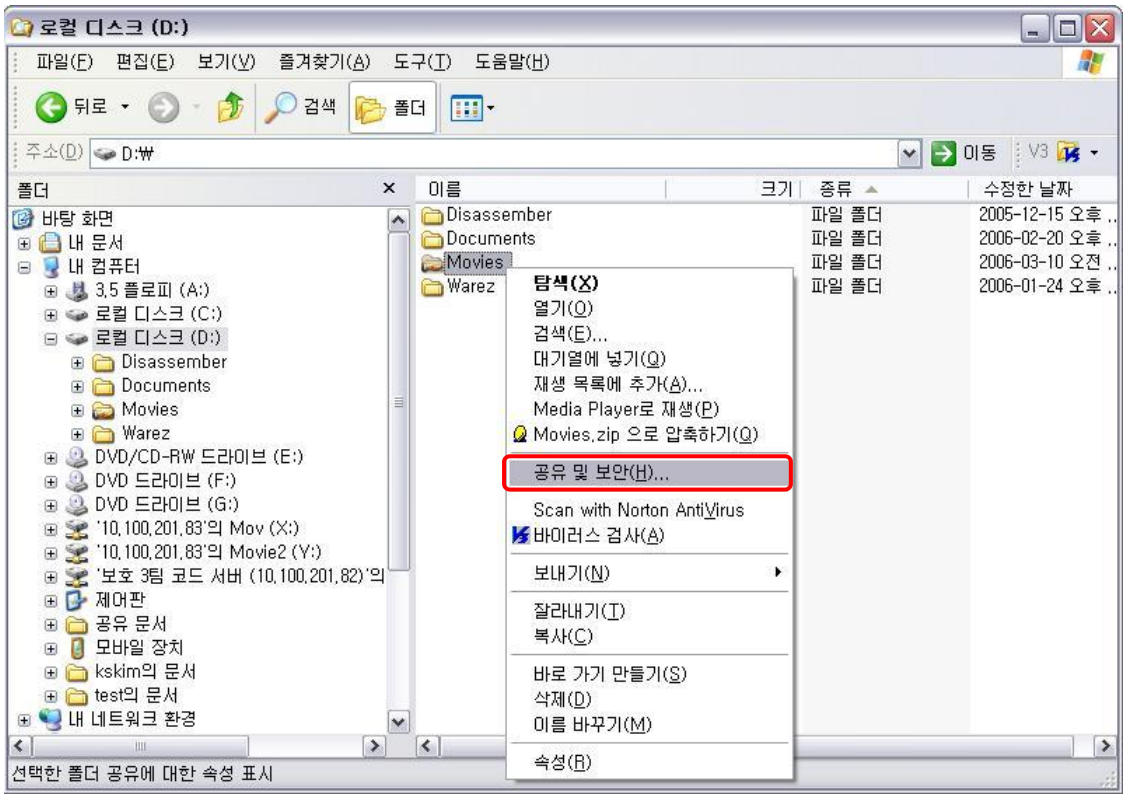


7. 공유 폴더 사용 제한(6/7)

- 다음 그림처럼 등록된 폴더가 있다면 직접 제거해야 합니다.

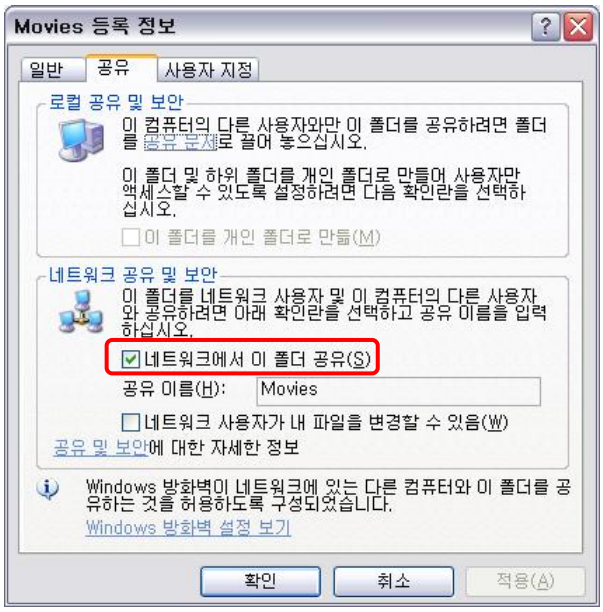


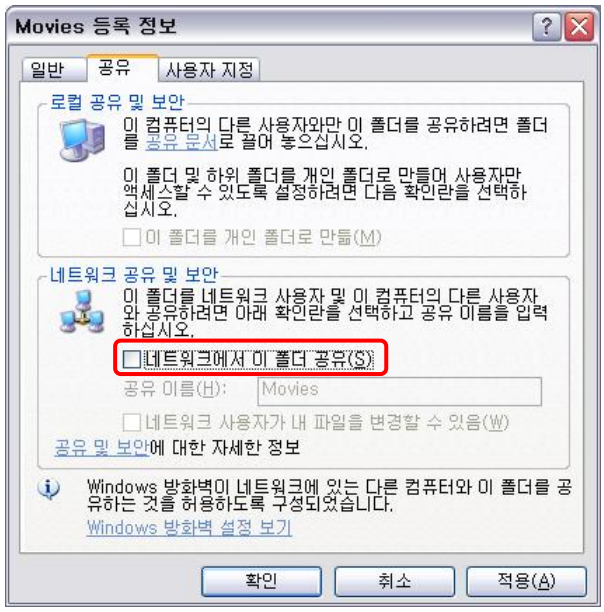
- "Windows 탐색기"를 실행시키고 공유된 경로를 참고하여 해당 폴더를 마우스 우측버튼으로 선택합니다.
- 나타나는 메뉴에서 "공유 및 보안"을 선택합니다.



7. 공유 폴더 사용 제한(7/7)

- 시스템의 설정에 따라 두 가지의 대화상자를 볼 수 있습니다.
  - 첫번째 다음과 같은 대화상자에서는 “네트워크에서 이 폴더 공유”의 체크박스를 해제합니다.





  - 두번째 다음과 같은 대화상자에서는 “이 폴더를 공유하지 않음”의 라디오 버튼을 선택합니다.

8. Windows 보안 센터 참조(1/3)

개 요

주의사항

➢ Windows 보안 센터는 Windows XP SP2 이상에서만 제공됩니다.

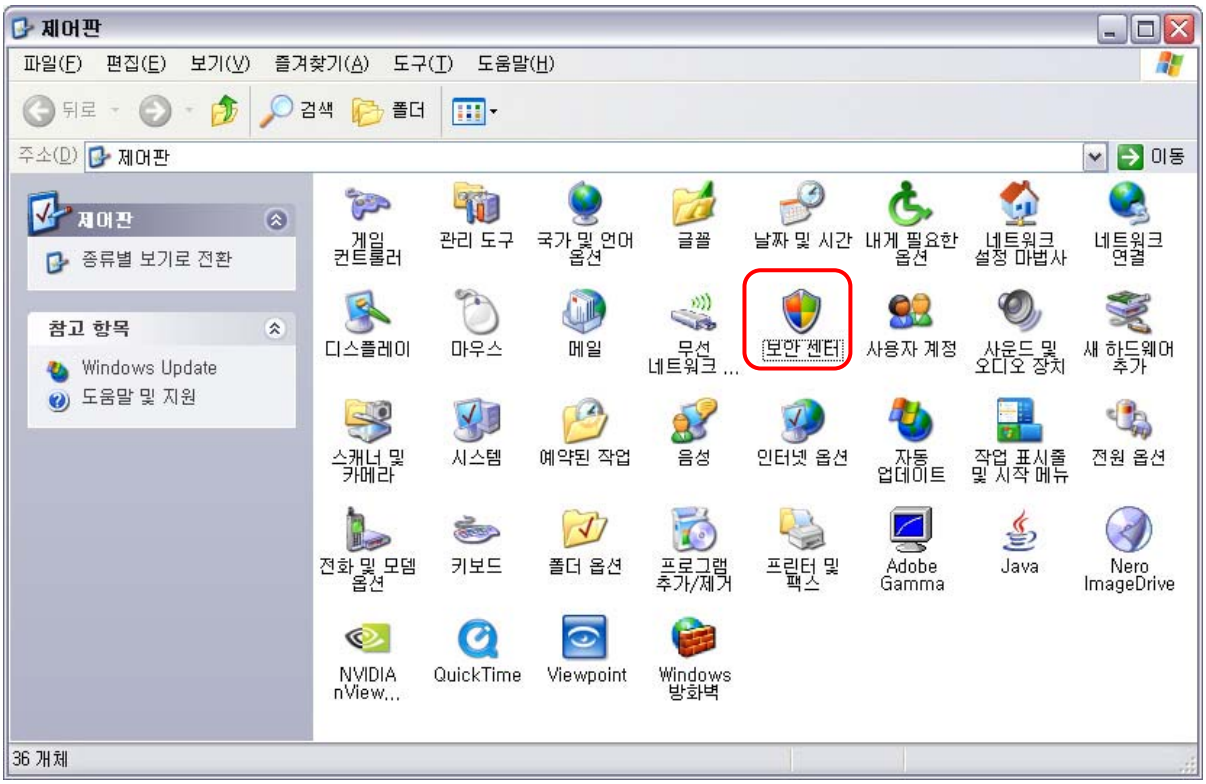
❍ Windows 보안 센터는 보안 상태를 확인하고, 보안 설정을 변경하며, 여러 가지 보안 문제에 대한 정보를 얻을 수 있는 곳입니다.

❍ Windows 방화벽, 자동 업데이트, 바이러스 백신의 상태를 알 수 있고, 설정 값을 변경할 수 있는 화면으로 연결되는 버튼이 있습니다.

이용 방법

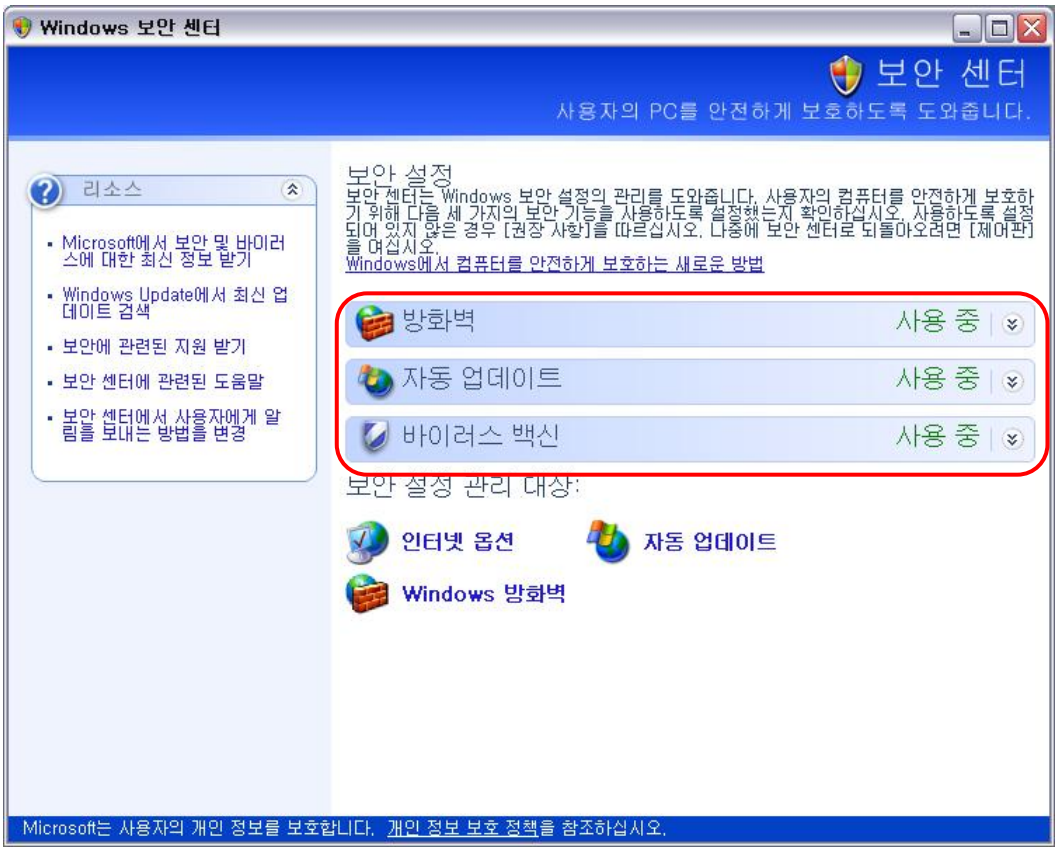
❍ 보안 상태 확인 방법

- 「제어판」을 열어 "클래식 보기" 상태로 합니다.
- 「제어판」의 "클래식 보기"에서 "보안 센터" 항목을 선택하여 실행합니다.



8. Windows 보안 센터 참조(2/3)

- 「Windows 보안 센터」 창이 열리며 현재 컴퓨터의 보안 설정 상태가 보입니다.
- 다음 그림은 “방화벽”, “자동 업데이트”, “바이러스 백신”이 올바르게 설정되어 있고 동작중임을 나타냅니다.



❍ 보안 센터는 백그라운드 프로세스로 실행되면서 다음 3가지 보안 구성 요소의 상태를 지속적으로 점검합니다.

- Windows 방화벽
  - 인터넷에 연결되어 있을 때 방화벽이 작동되지 않고 있으면 해커가 사용자의 컴퓨터에 액세스해서 파일을 손상시키거나 오작동을 유발시킬 수 있는 악성 코드를 설치할 수 있습니다.
  - Windows 방화벽은 기본적으로 활성화된 상태로 SP2와 함께 제공됩니다. 보안 센터는 Windows 방화벽이 켜져 있는 지를 지속적으로 점검하여 방화벽이 꺼지면 경고를 표시합니다.

8. Windows 보안 센터 참조(3/3)

- 자동 업데이트
  - Windows 보안 센터는 자동 업데이트에 “자동으로 업데이트를 다운로드하고 사용자가 지정한 일정에 업데이트를 설치합니다.”라는 권장 설정이 지정되었는지 확인하고, 자동 업데이트가 꺼져 있거나 권장 설정으로 지정되지 않은 경우 경고를 표시합니다.
- 바이러스 예방
  - Windows 보안 센터는 바이러스 백신 소프트웨어가 설치되어 있는지를 확인할 뿐만 아니라 이 소프트웨어의 버전이 최신인지 그리고 실시간 점검 기능이 켜져 있는지 확인합니다.

❍ Windows 보안 센터는 이러한 보안 구성 요소 중 하나라도 설치되어 있지 않거나 구성 요소의 보안 설정이 권장 설정보다 낮게 지정되어 있으면 알림 영역에 빨간색 방패 아이콘을 표시하고 사용자가 로그온할 때 경고를 표시합니다.

❍ 이 방패 아이콘이나 경고를 선택하면 Windows 보안 센터가 열리고, 여기에 관련 문제에 대한 메시지와 권장 해결 방법이 나타납니다.

9. Windows 방화벽 사용(1/4)

개 요

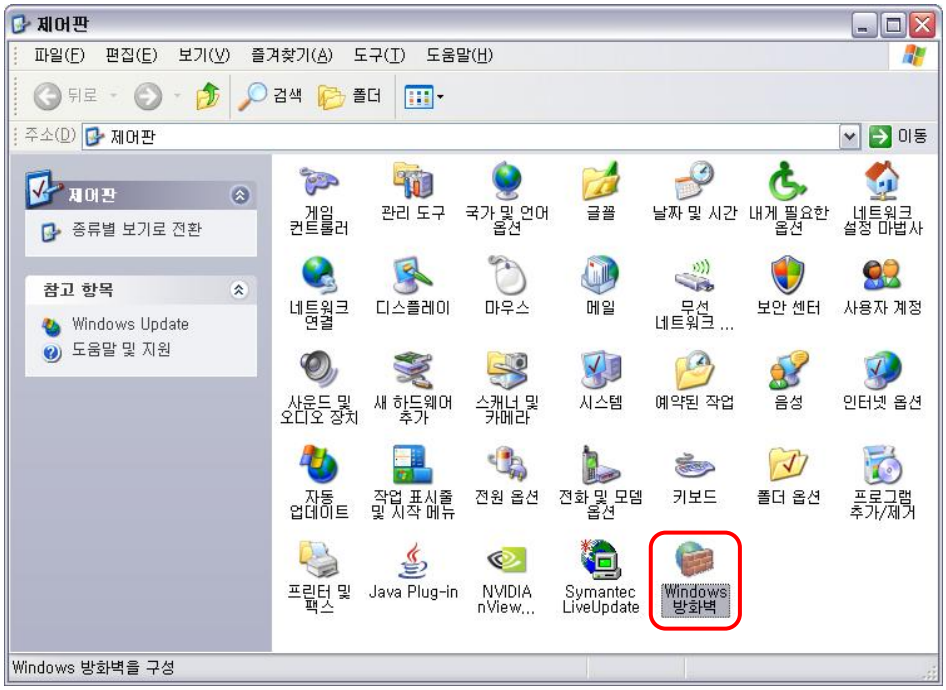
- 네트워크 방화벽 이외에 개인이 사용하는 컴퓨터에 별도의 방화벽을 사용하면 더욱 안전합니다.
- 이전 버전의 Windows에서도 방화벽 기능이 있었으나 Windows XP SP2에서는 "Windows 방화벽"이라는 이름을 사용하는 기능이 강화된 방화벽이 있습니다.

네트워크 방화벽의 한계

- 제한적 기능
  - 웜·바이러스를 차단하기가 어렵습니다.
- 내부 네트워크에서의 공격
  - 내부 네트워크에 있는 공격자는 네트워크 방화벽의 통제를 받지 않고 다른 사용자의 PC 등에 공격 수행이 가능합니다.

사용방법

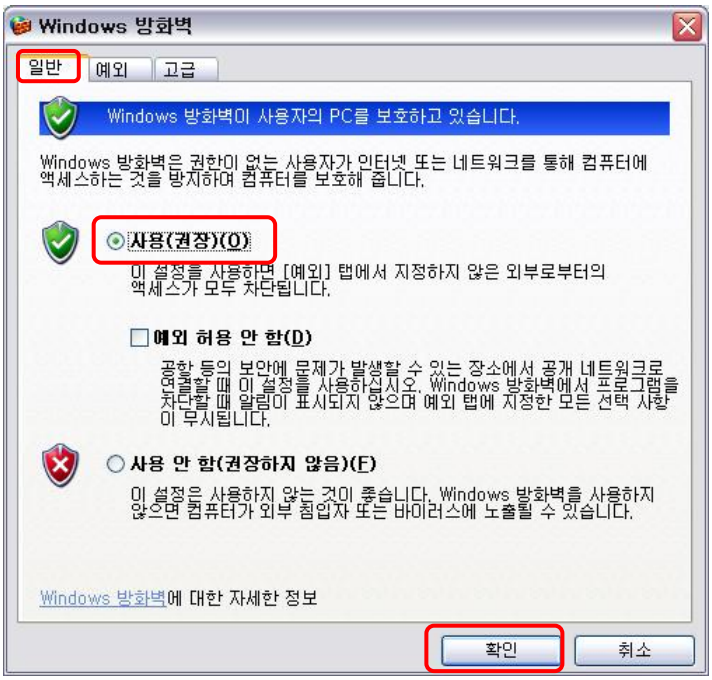
- 「제어판」을 열어 "클래식 보기" 상태로 합니다.
- 「제어판」 의 "클래식 보기"에서 "Windows 방화벽" 항목을 선택하여 실행합니다.



9. Windows 방화벽 사용(2/4)

❍ Windows XP SP2 방화벽 사용

- Windows 방화벽 창에서 일반 탭을 선택한 후 사용(권장)을 선택하고 확인을 선택합니다.



특 징

❍ 기본적으로 활성화됨

- SP2 이전의 Windows XP에서는 방화벽이 기본적으로 비활성화된 상태로 제공되었습니다. 즉, 방화벽을 작동하기 위해서는 마법사를 실행하거나 네트워크 연결 폴더를 검색해 수동으로 실행시켜 주어야 했습니다.
- SP2를 설치하면 Windows 방화벽이 자동으로 작동되기 때문에 모든 새로운 설치 및 업그레이드에 대한 보호 수준이 향상될 뿐 아니라 시스템에 새롭게 추가되는 네트워크 연결도 보호됩니다.

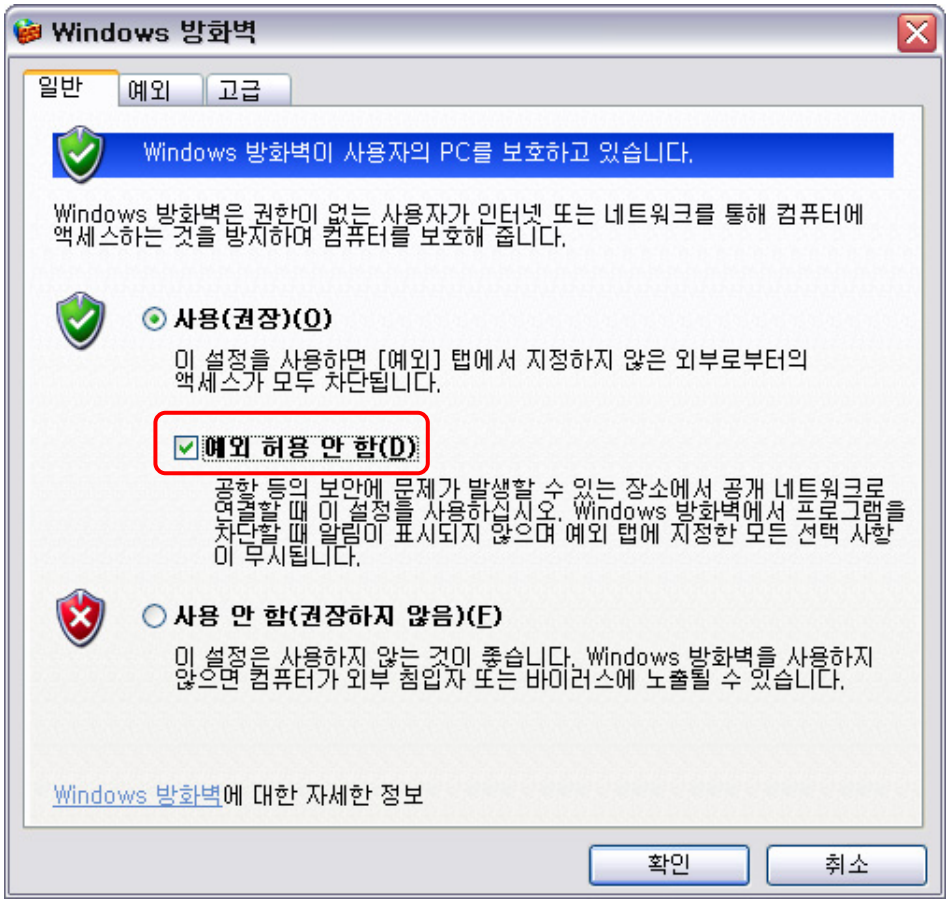
9. Windows 방화벽 사용(3/4)

❍ 부팅 시 보안 유지

- 이전 버전까지의 Windows에서는 네트워크가 시작된 후 방화벽이 활성화되기까지 약간의 시간 간격이 있었으며, 그 짧은 시간 동안 컴퓨터가 취약한 상태에 놓여 있었습니다.
- SP2에서는 부팅 시간 필터라고 하는 방화벽 규칙을 사용하여 컴퓨터를 시작하고 종료하는 짧은 시간 동안에 발생할 수 있는 공격을 방지합니다.
- 일단 Windows 방화벽이 완전히 실행되면 사용자 지정 방화벽 설정이 로드되고 부팅 시간 필터가 제어됩니다.

❍ "예외 허용 안 함"

- 이 기능을 사용하면 Windows 방화벽 예외 목록의 모든 예외 항목을 쉽게 끌 수 있습니다. 특정 프로그램을 사용하기 위해 이러한 예외 항목이 필요하기는 하지만 보안을 강화하기 위해 모든 예외 항목을 꺼야 하는 경우에 사용할 수 있습니다.

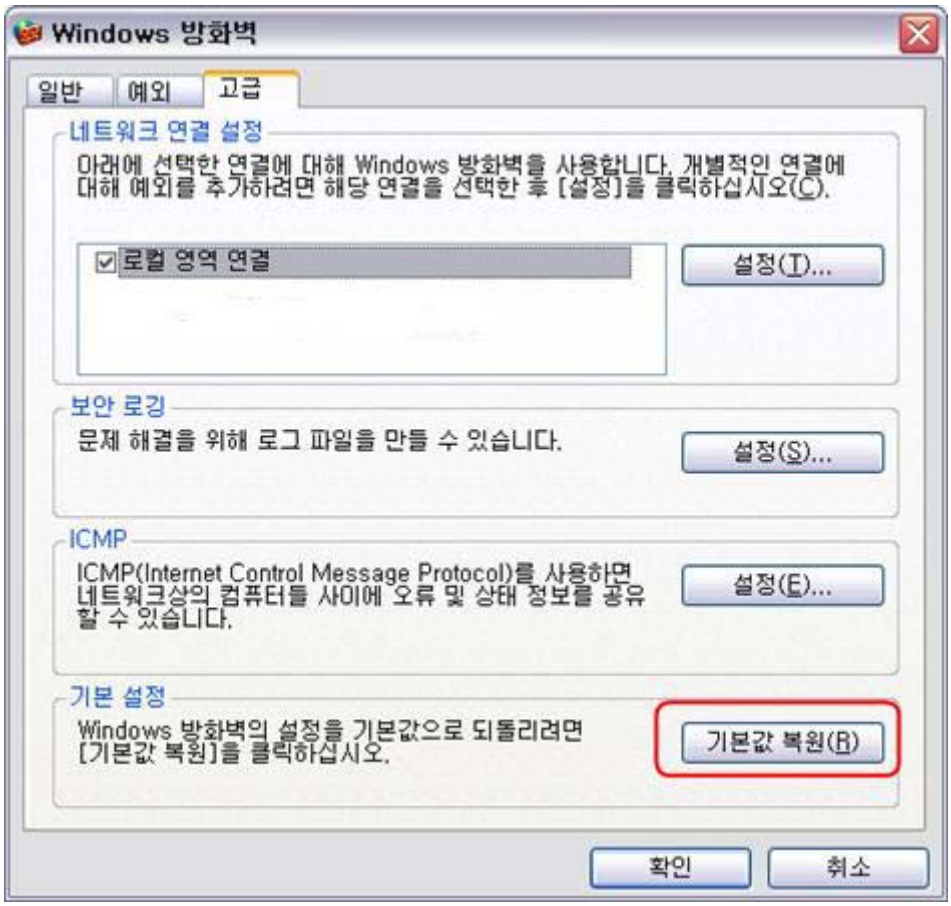


9. Windows 방화벽 사용(4/4)

- 공공 장소에서 컴퓨터를 사용할 때마다 Windows 방화벽을 “예외 허용 안 함”으로 설정하면 해커의 공격 위험을 줄일 수 있습니다.

❍ 기본값 복원

- SP2 이전의 Windows XP의 방화벽에는 원래 설정으로 쉽게 복원할 수 있는 방법이 없었습니다.
- 그러나 오랜 기간 동안 Windows 방화벽 예외 목록에 프로그램이나 포트를 추가하다 보면 Windows 방화벽이 부주의하게 구성되어 컴퓨터 보안을 위협하는 악의적인 트래픽이 허용될 수 있습니다. 이 옵션으로 Windows 방화벽을 기본 설정으로 복원할 수 있습니다.



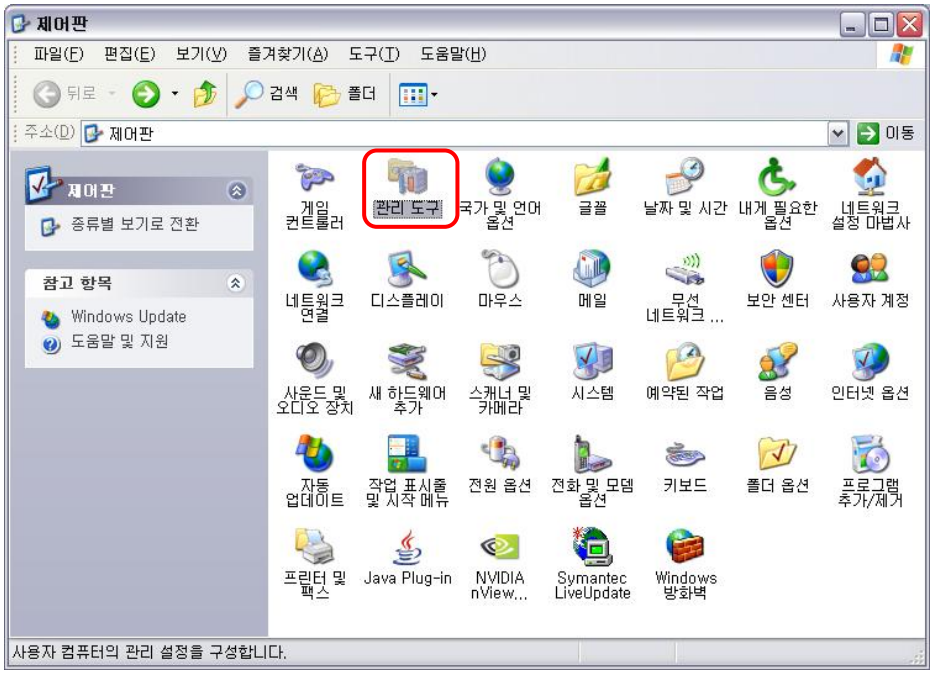
10. 위험한 서비스 비활성화(1/5)

개 요

- 서비스는 시스템 백그라운드에서 실행되는 응용 프로그램으로서 UNIX 데몬 응용 프로그램과 비슷합니다.
- 서비스는 웹 서빙, 이벤트 로깅, 파일 서빙, 도움말 및 지원, 암호화 및 오류 보고와 같은 운영 체제의 핵심 기능을 제공합니다.
- 서비스를 사용하면 편리한 점도 있지만, 서비스 자체가 취약한 부분을 포함하고 있거나 관리의 허술함으로 공격 지점이 될 수 있으므로 사용자의 환경에서 필요하지 않은 모든 서비스는 사용하지 않아야 합니다.
- 보안 계정 관리자 등의 일부 서비스를 사용하지 않으면 컴퓨터를 다시 시작할 수 없으므로 설명에서 언급하지 않은 서비스의 설정은 함부로 조작하지 않는 편이 좋습니다.

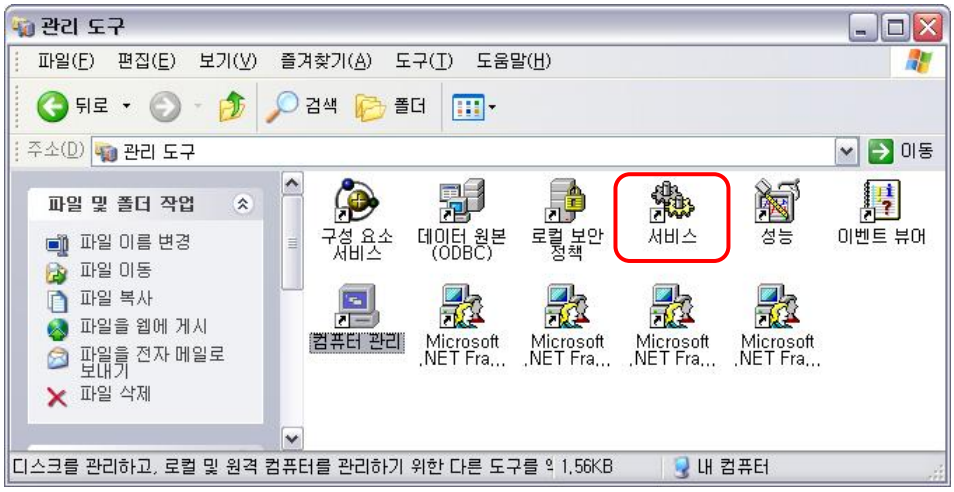
서비스 관리

- 서비스의 목록 보기
  - 「제어판」을 열어 "클래식 보기" 상태로 합니다.
  - 「제어판」의 "클래식 보기"에서 "관리 도구" 항목을 선택하여 실행합니다.



10. 위험한 서비스 비활성화(2/5)

- 「관리 도구」 창이 열리면 “서비스” 항목을 선택하여 실행합니다.

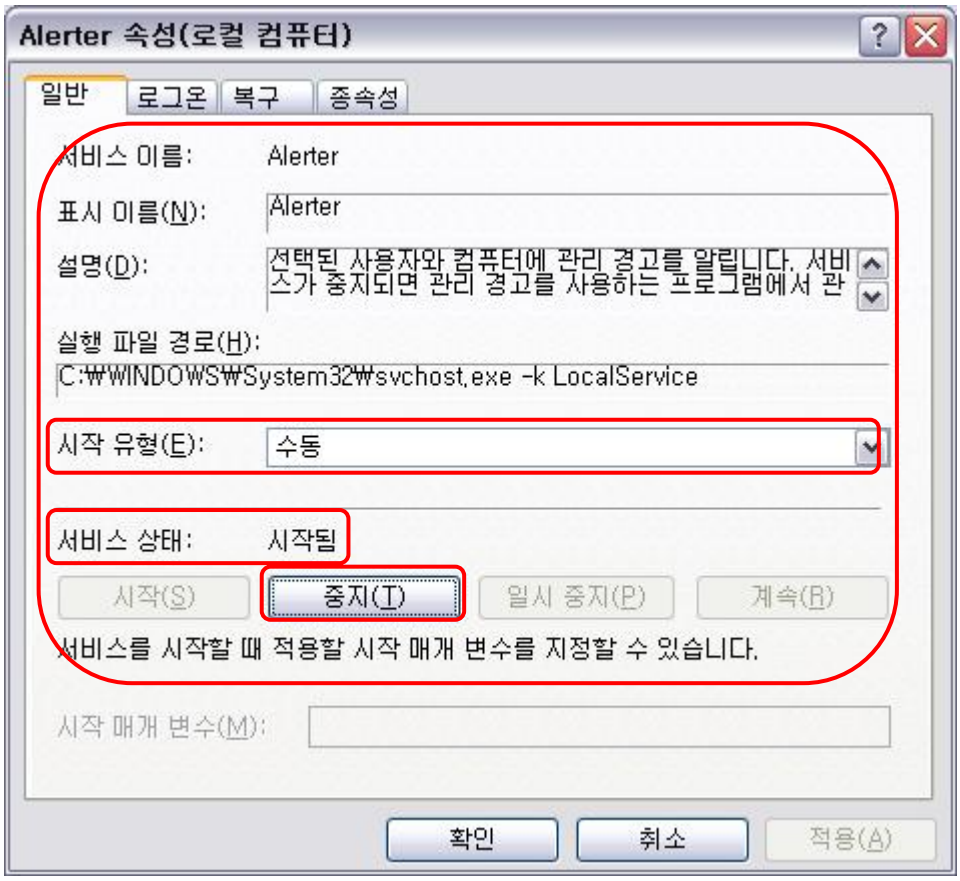


- 「서비스」창이 열리면 시스템에 등록되어 있는 서비스의 이름, 설명, 상태, 시작 유형 등에 대한 목록을 확인할 수 있습니다.

10. 위험한 서비스 비활성화(3/5)

❍ 서비스 관리

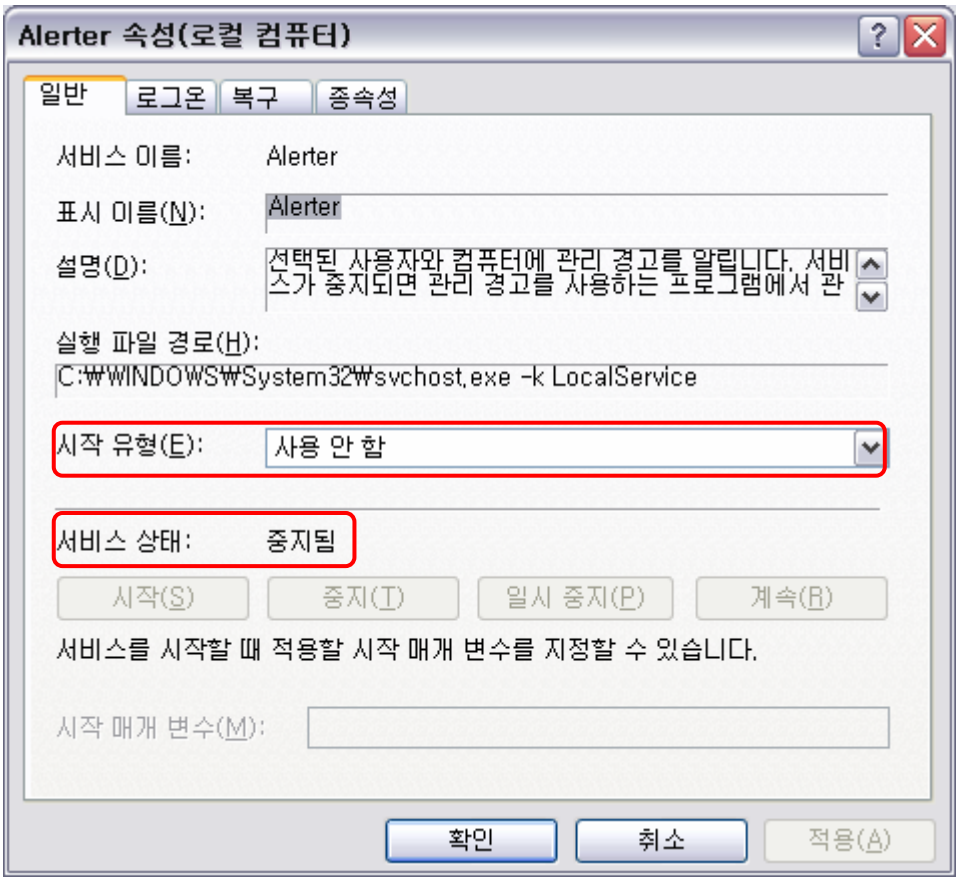
- 관리하고자 하는 서비스를 선택하여 실행합니다.
- 본 설명에서는 Alerter를 예로 듭니다.



- 「Alerter 속성」 창이 열리며 서비스의 이름, 표시 이름, 설명, 실행 파일 경로, 시작 유형, 서비스 상태 등을 표시합니다.
- 위험한 서비스를 "사용 안 함"으로 설정한다는 의미는 위험한 서비스를 선택하여 실행 한 후 "서비스 상태"를 "중지됨", "시작 유형"을 "사용 안 함"으로 설정한다는 의미입니다.
- 현재 Alerter는 "시작 유형"이 "수동"이고 "서비스 상태"가 "시작됨"입니다.
- "중지" 버튼을 선택하여 "서비스 상태"를 "중지됨"으로 만들고, "시작 유형"의 콤보 박스를 이용하여 "사용 안 함"으로 선택합니다.

10. 위험한 서비스 비활성화(4/5)

- 해당 과정을 마치면 아래 와 같이 “시작 유형”이 “사용 안 함”이며, “서비스 상태”가 “중지됨”으로 설정됨을 확인할 수 있습니다.



위험한 서비스의 종류

❍ 아래에 설명하는 서비스는 위험하거나 잠재적으로 위험할 수 있는 서비스이므로 “사용 안 함”으로 설정하는 것이 좋습니다.

- Alerter 서비스
  - 연결된 다른 컴퓨터에 관리 경고 메시지를 보내는 서비스입니다.
  - 공격자가 사회공학적 방법으로 일반 사용자에게 해를 끼칠 수 있는 메시지를 송신하는데 이용될 수 있으므로 사용하지 않을 것을 권장합니다.

10. 위험한 서비스 비활성화(5/5)

- Computer Browser
  - 네트워크에 있는 모든 컴퓨터의 목록을 갱신하고 관리하며 이 목록을 브라우저로 지정된 컴퓨터에 제공합니다.
  - 네트워크 상에 가용한 자원을 볼 수 있게 하여 공격의 가능성이 증가하므로 사용하지 않을 것을 권장합니다.
- Fast User Switching Compatibility
  - 여러 사람이 공동으로 사용하는 PC에서 PC를 이용하던 이용자가 로그오프하지 않은채 다른 사용자가 로그온하여 PC를 사용할 수 있게 합니다.
  - 보안상 취약한 Terminal Service를 이용하는 서비스이므로 사용하지 않을 것을 권장합니다.
- Messenger
  - 네트워크상에서 메시지를 전달하는 기능을 하는 서비스입니다.
  - 성인광고 등의 스팸메시지가 이 서비스를 통해 보내어지기도 하므로 사용하지 않을 것을 권장합니다.
  - MSN 메신저, Windows 메신저와는 상관이 없습니다.
- Netmeeting Remote Desktop Sharing
  - 자신의 컴퓨터에 원격으로 접근할 수 있도록 허용하고 다른 컴퓨터와 바탕 화면 원격 공유를 사용할 수 있게 하는 서비스입니다.
  - 원격에서 이 서비스를 통해 공격이 가능하다고 알려져 있으므로 사용하지 않을 것을 권장합니다.
- Telnet
  - 원격 사용자가 로그온하여 커맨드라인에서 콘솔 프로그램을 실행시킬 수 있게 하는 서비스입니다.
  - 시스템 자원에 직접 접근하는 것을 허락하는 서비스이므로 사용하지 않을 것을 권장합니다.
  - Windows XP Home에서는 제공하지 않습니다.

Ⅲ. 시스템 유지/관리 보안

11. 자동 로그온 비활성화(1/2)

개 요

❍ 자동 로그온이 설정되어 있으면 시스템의 전원을 켜고 부팅과정이 진행중일 때 「Windows 로그온」 창이나 「시작화면」에서 "사용자이름"과 "패스워드"의 입력없이 자동으로 로그온이 된다.

❍ 자동 로그온을 해제하여 자동으로 로그온되지 않도록 설정해야 한다.

미사용시의 문제점

❍ 자동 로그온을 설정해두면 인증과정없이 로그온할 수 있습니다.

❍ 결과적으로 불순한 의도를 가진 사용자를 포함하여 누구나 컴퓨터를 불법적으로 사용할 수 있는 환경이 제공됩니다.

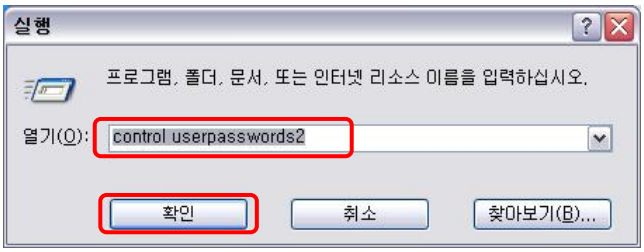
설정방법

❍ 자동 로그온 상태 설정을 위한 창으로 이동

- 바탕화면의 좌측 하단에 있는 "시작" 버튼을 찾아 선택합니다.
- "시작" 버튼 선택 후 보이는 메뉴에서 "실행"을 선택합니다.

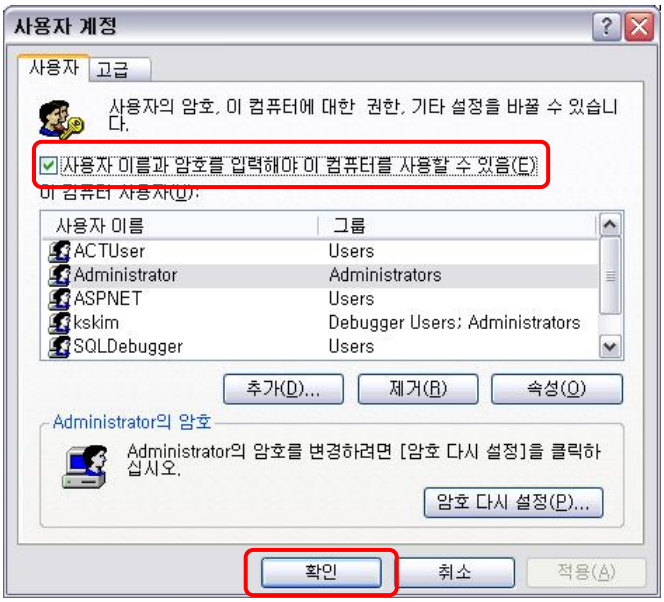
11. 자동 로그온 비활성화(2/2)

❍ 「실행」 창이 열리면 “control userpasswords2” 명령어를 입력하고 “확인” 버튼을 선택합니다.



❍ 「사용자 계정」 창이 열리며 현재 컴퓨터에 등록되어 있는 사용자의 목록이 보입니다.

❍ “사용자 이름과 암호를 입력해야 이 컴퓨터를 사용할 수 있음” 체크박스를 선택하고 “확인” 버튼을 선택합니다.



12. 화면보호기 사용 및 잠금(1/2)

개 요

❍ 일정시간 동안 사용자의 동작이 없는 경우에 운영체제는 이를 사용자가 자리에 없는 것으로 판단하고, 모니터 화면에 보여지고 있는 내용의 노출과 불법사용자에 의한 컴퓨터 사용을 방지하기 위하여 특정 영상을 화면에 보여주는 기능을 수행하는데, 이를 화면보호기라고 합니다.

❍ 사용자가 자리에 없는 것으로 판단하는 대기 시간과 보호화면의 종류 그리고, 패스워드의 적용 여부는 사용자가 선택할 수 있습니다.

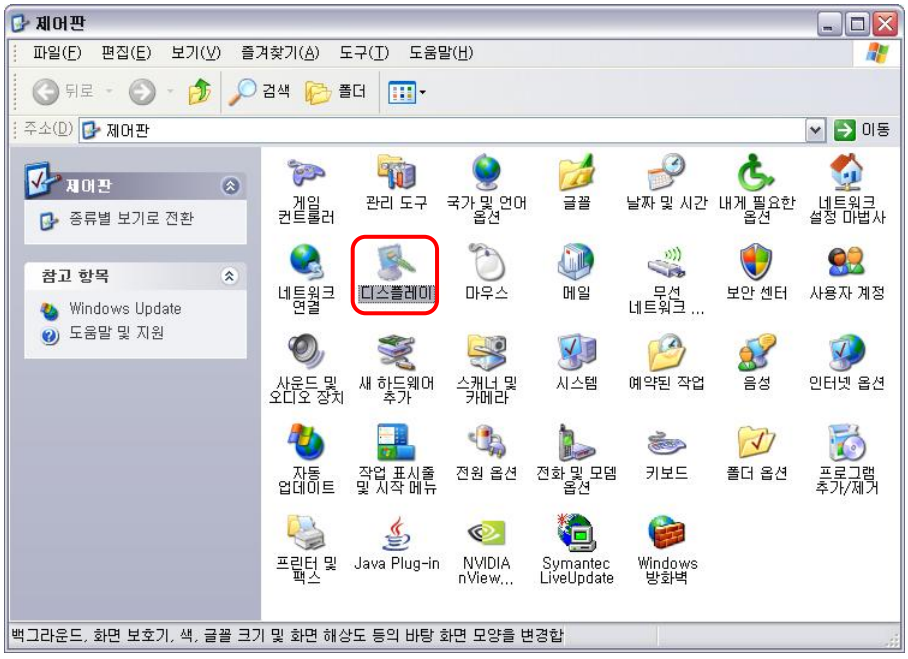
미사용시의 문제점

❍ 화면에 보여지는 내용을 모든 사람이 열람할 수 있으며, 불법적인 사용자에 의한 컴퓨터 사용이 가능해집니다.

설정방법

❍ 화면보호기 설정을 위한 창으로 이동

- 「제어판」을 열어 "클래식 보기" 상태로 합니다.
- 「제어판」의 "클래식 보기"에서 "디스플레이"를 선택하여 실행합니다.



12. 화면보호기 사용 및 잠금(2/2)

❍ 「디스플레이 등록 정보」 창이 열리며 “테마” 탭이 활성화됩니다.

❍ 화면보호기 설정은 아래와 같은 순서로 합니다.

① 「디스플레이 등록 정보」 창에서 “화면보호기” 탭을 선택합니다.

② “화면보호기”에서 원하는 보호화면을 선택합니다.

③ “대기”에서 원하는 대기시간을 분단위로 선택합니다.

- 선택한 시간 동안 사용자의 동작이 없으면 화면보호기가 작동됩니다.

④ “다시 시작할 때 암호로 보호”의 체크박스를 설정합니다.

- 이를 설정하지 않으면 누구나 동작중인 화면보호기를 해제할 수 있습니다.
- 시스템의 설정에 따라 “다시 시작할 때 [시작 화면] 표시”라고 표시될 수도 있습니다. 기능은 동일합니다.

⑤ “확인”을 선택합니다.

13. 패치 업데이트(1/4)

개 요

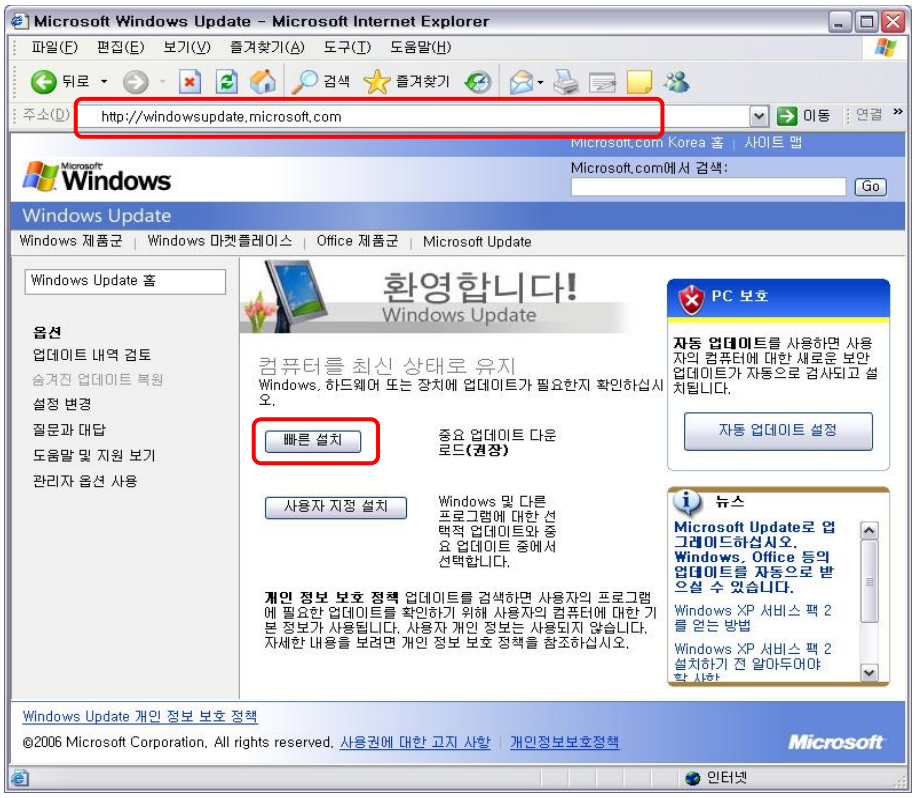
- 마이크로소프트에서는 새롭게 발견되는 취약점과 같은 문제점을 해결하기 위해 패치 서비스를 실시하고 있습니다.
- 패치란 Windows 운영체제나 응용 프로그램의 오류나 취약한 부분을 보완해주는 여러 가지 수정 프로그램을 말합니다.
- 마이크로소프트가 제공하는 패치 프로그램을 설치하는 것은 운영체제를 안전하게 운영하는 데 필수적입니다.

미사용시의 문제점

- 패치를 설치하지 않으면 이미 발견된 취약점에 무방비로 노출되고, 시스템 안정성에 문제가 발생할 수 있으며 상대적으로 해킹 공격에 취약해집니다.

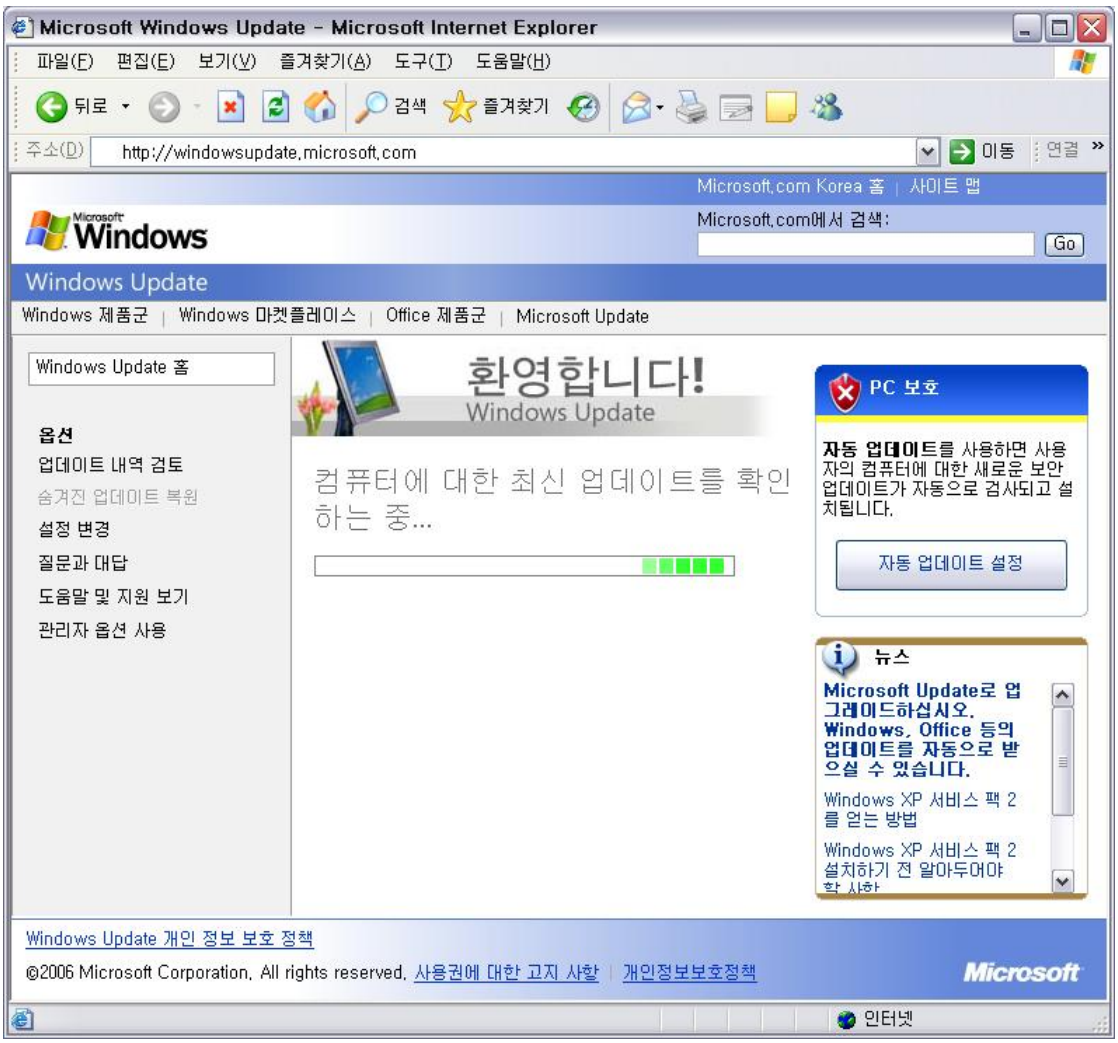
업데이트 방법

- 인터넷 익스플로러에서 http://windowsupdate.microsoft.com으로 이동합니다.



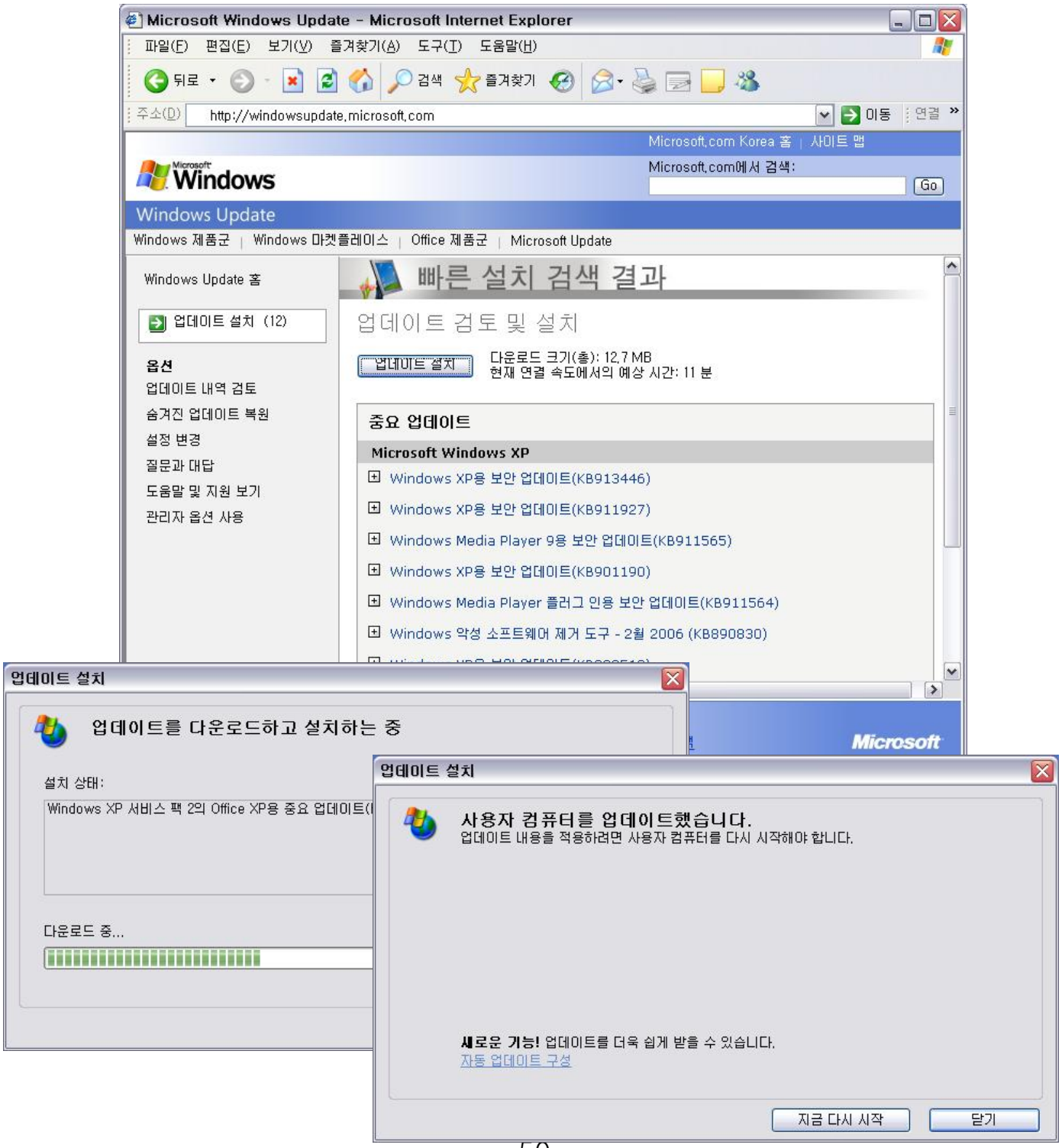
13. 패치 업데이트(2/4)

❍ 마이크로소프트에서 제공하는 업데이트 페이지로 자동으로 이동합니다. 앞 페이지의 그림과 같이 보이면 "빠른 설치" 버튼을 선택합니다. 아래와 같은 화면을 볼 수 있습니다.



13. 패치 업데이트(3/4)

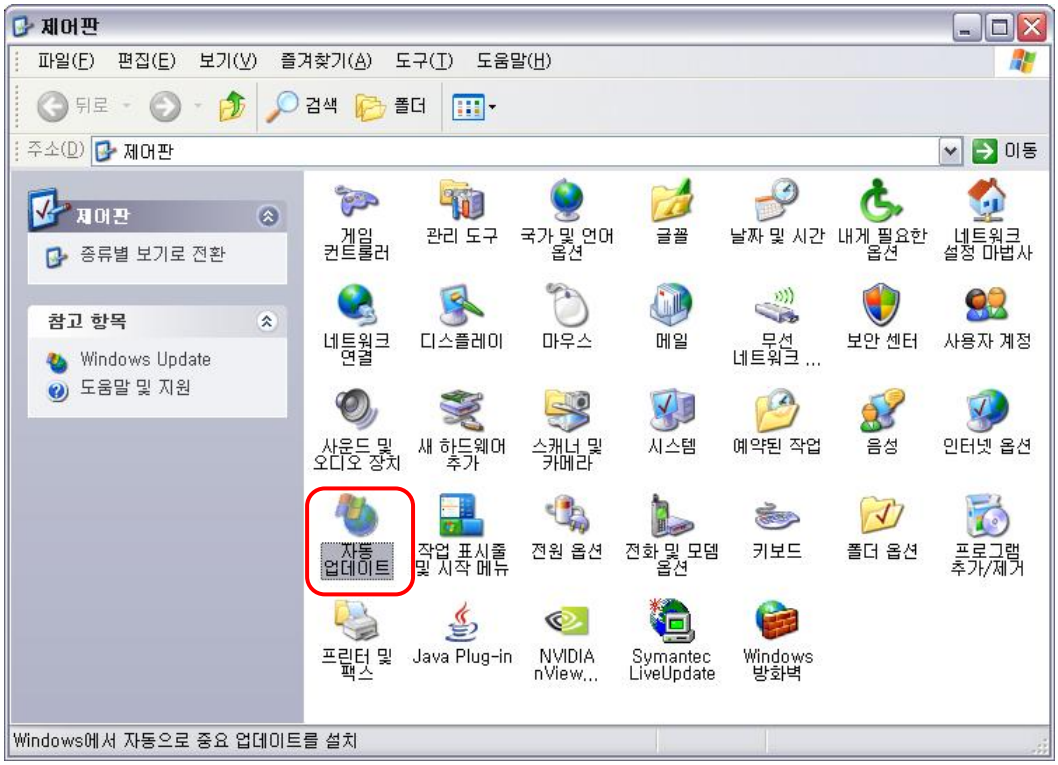
❍ 빠른 설치 검색 결과 화면에서 설치할 패치들이 나타납니다. “업데이트 설치”를 선택합니다. “사용자 컴퓨터를 업데이트했습니다.”라는 메시지를 볼 수 있습니다.



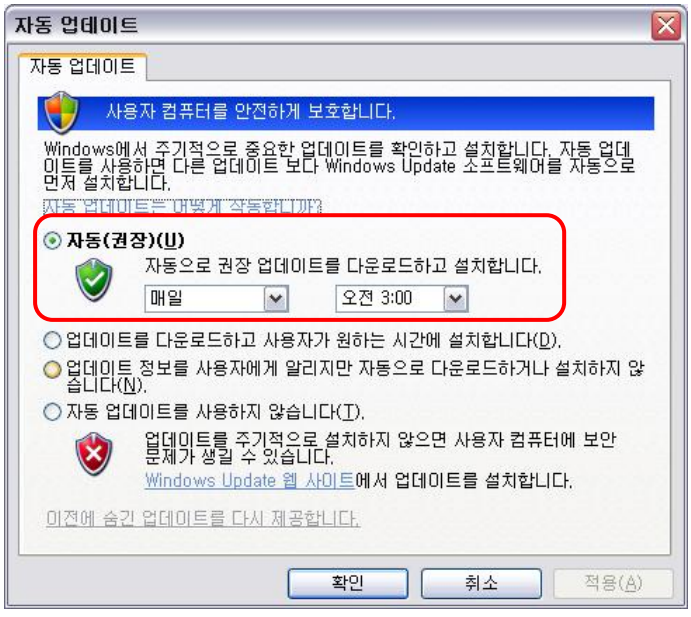
13. 패치 업데이트(4/4)

❍ 자동 업데이트를 설정해 두면 이와 같은 과정을 자동으로 처리할 수 있습니다.

- 「제어판」을 열어 "클래식 보기" 상태로 합니다.
- 자동 업데이트를 선택하여 실행합니다.



❍ 자동 업데이트 창에서 자동(권장)을 선택하고 설치할 시간을 선택하고 "확인" 버튼을 선택합니다.



14. 메일 클라이언트의 보안설정 강화(1/8)

개 요

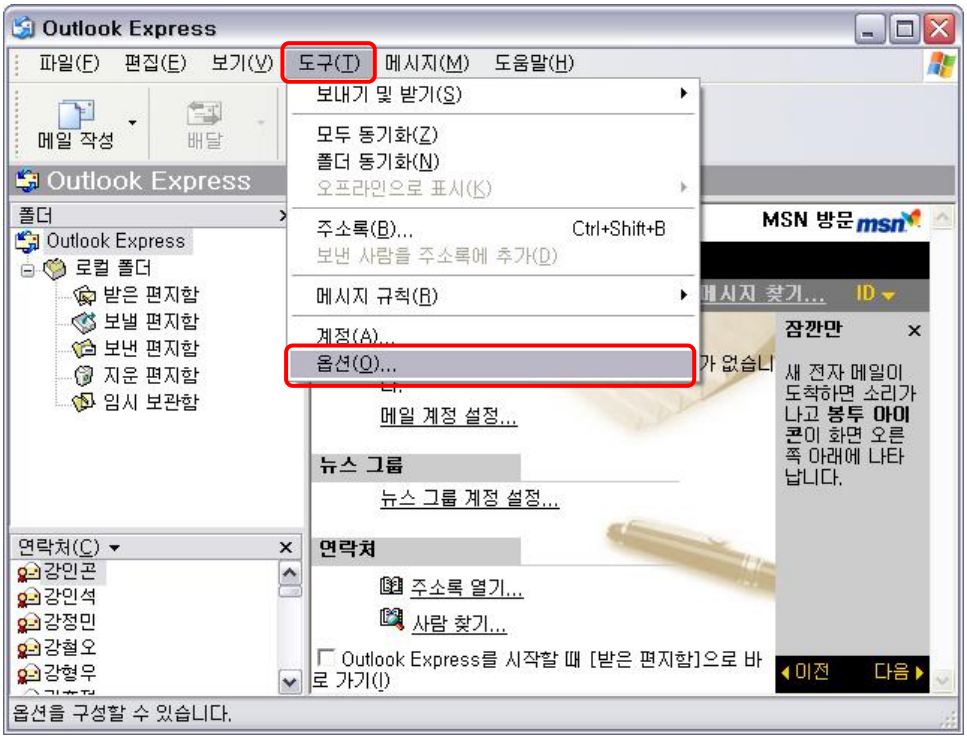
❍ 메일 클라이언트 프로그램은 사용자 설정에 따라서 취약한 부분이 존재할 수 있습니다. 따라서, 메일 클라이언트 프로그램에서 제공하는 보안 기능의 설정을 통해 보안성을 강화할 필요가 있습니다.

보안설정 강화방법

❍ 본 가이드라인에서는 Windows XP 시스템에 기본적으로 포함되어 있는 Outlook Express와 마이크로소프트의 MS Office에 포함되어 있는 Outlook에 대해 차례로 설명하겠습니다.

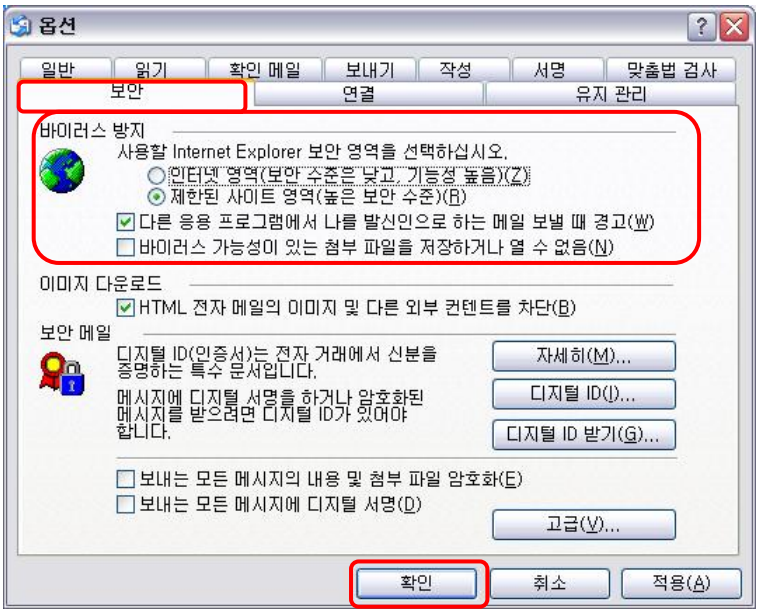
❍ Outlook Express 6

- 보안설정
  - Outlook Express 6을 실행합니다.
  - “도구” 메뉴에서 “옵션”을 선택합니다.



14. 메일 클라이언트의 보안설정 강화(2/8)

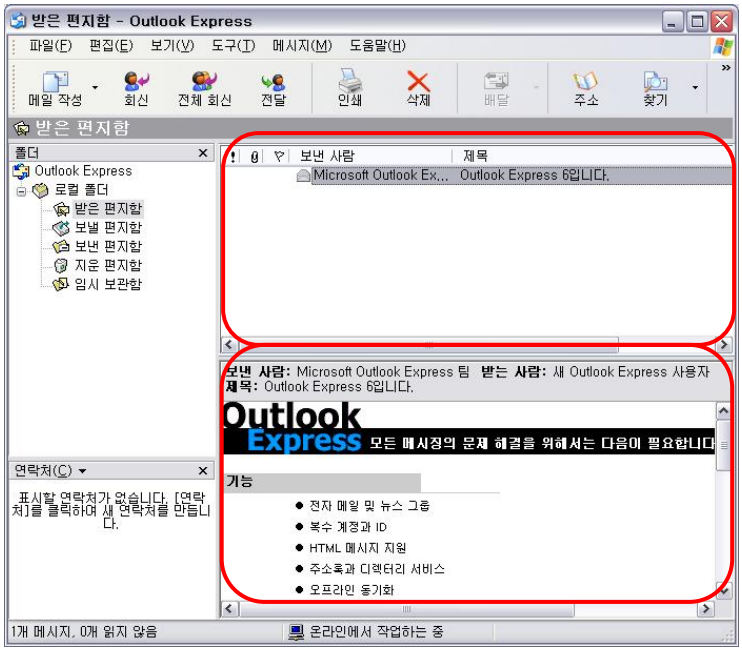
– 「옵션」 창이 열리면 “보안”탭을 선택한 후 아래 그림과 같이 설정하고 “확인”을 선택합니다.



- “미리보기” 해제

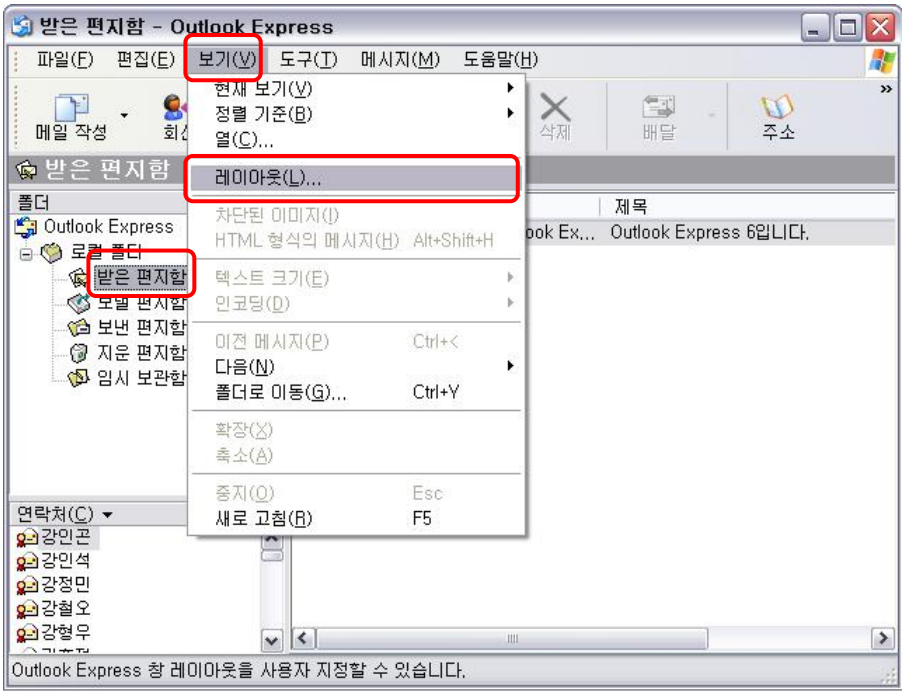
– 미리보기 기능을 해제하여 본문에 숨어 있을 수 있는 악성코드의 실행을 방지합니다.

– 기본적으로 Outlook Express는 상단에는 이메일의 리스트를, 하단에는 해당 이메일의 미리보기를 보여주도록 설정되어 있습니다.

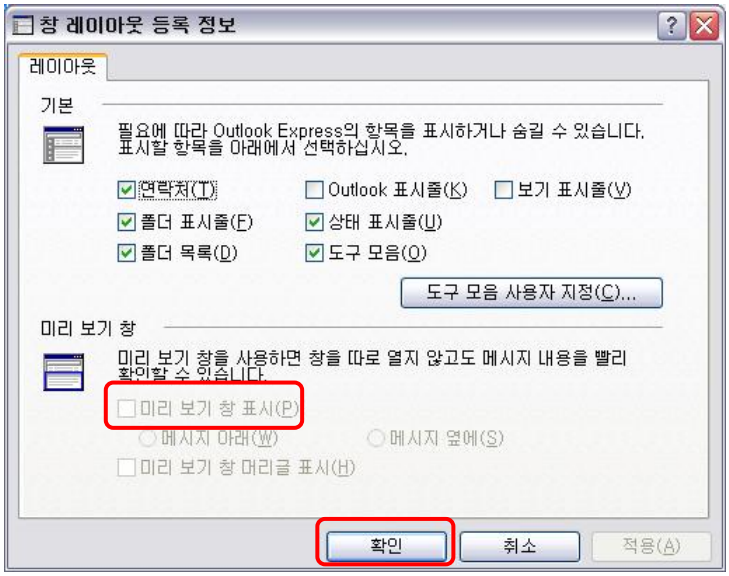


14. 메일 클라이언트의 보안설정 강화(3/8)

– 화면 좌측 폴더에서 “받은 편집함”을 선택하고 “보기”메뉴에서 “레이아웃”을 선택합니다.



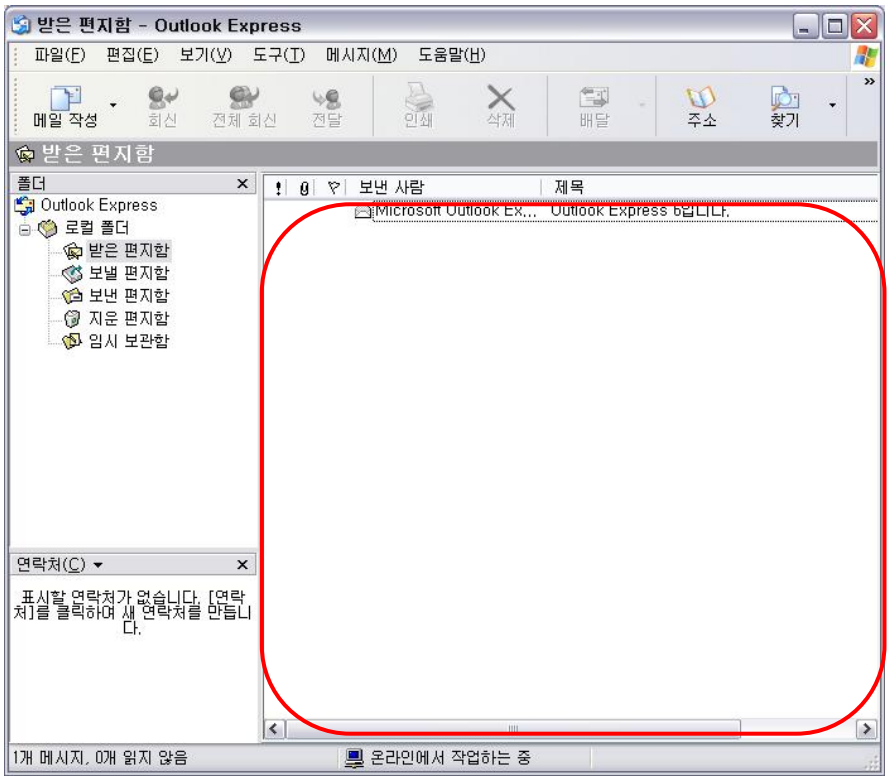
– 「창 레이아웃 등록 정보」 창에서 “미리 보기 창 표시”의 선택을 해제하고 확인버튼을 선택합니다.



• 설정 변경 사항을 적용하기 위해 프로그램을 종료합니다.

14. 메일 클라이언트의 보안설정 강화(4/8)

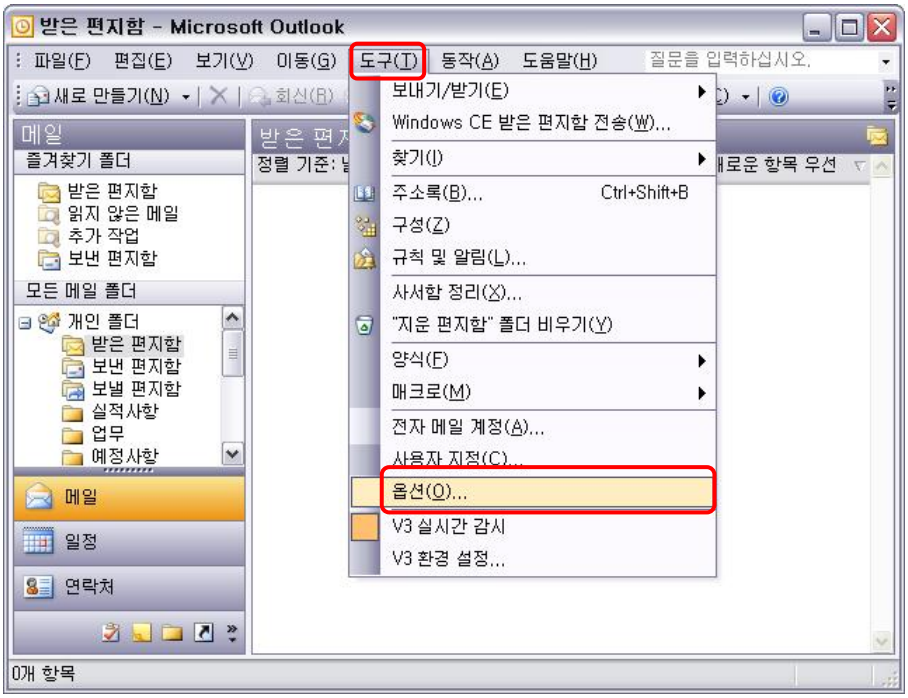
- 미리보기를 해제하면 「Outlook Express」 창에서 이메일의 내용을 미리 보여주는 기능이 해제된 것을 확인할 수 있습니다.



14. 메일 클라이언트의 보안설정 강화(5/8)

❍ Outlook 2003

- 보안설정
  - Outlook 2003을 실행합니다.
  - 도구 메뉴에서 옵션을 선택합니다.



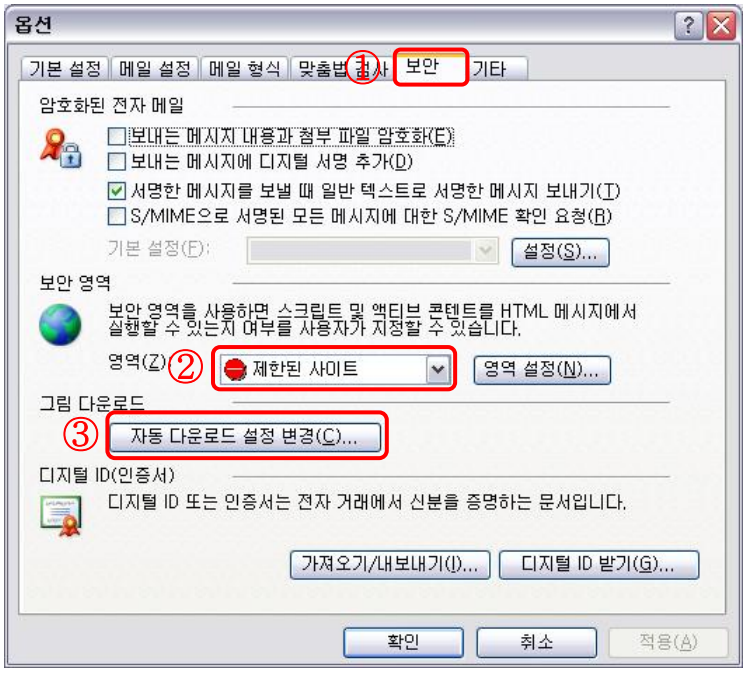
14. 메일 클라이언트의 보안설정 강화(6/8)

– 「옵션」 창이 열리면 “보안”탭을 선택한 후 아래 그림과 같이 설정하고 “확인”을 선택합니다.

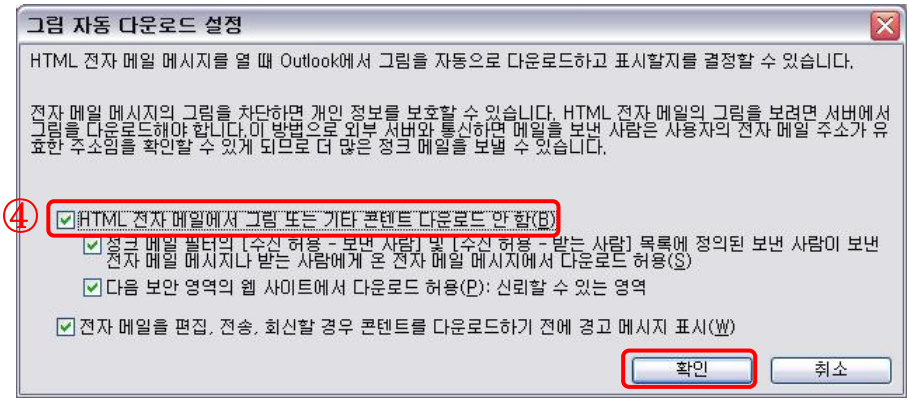
① “보안” 탭을 선택합니다.

② “보안 영역”의 “영역”을 “제한된 사이트”로 설정합니다.

③ “자동 다운로드 설정 변경” 버튼을 선택합니다.

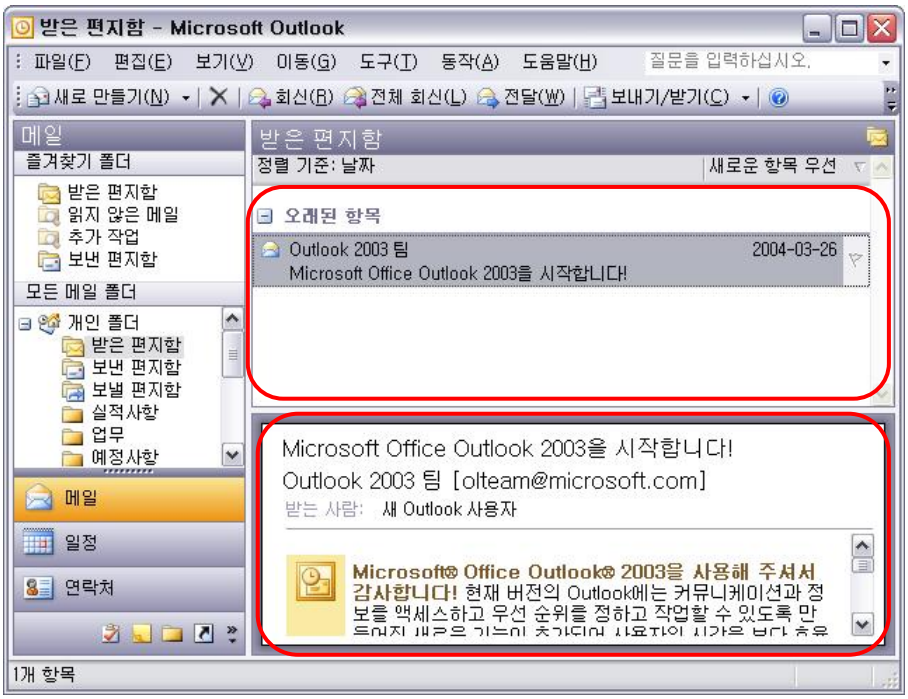


④ 「그림 자동 다운로드 설정」 창이 열리면 “HTML 전자 메일에서 그림 또는 기타 콘텐츠 다운로드 안 함”을 선택하고 “확인”을 선택합니다.



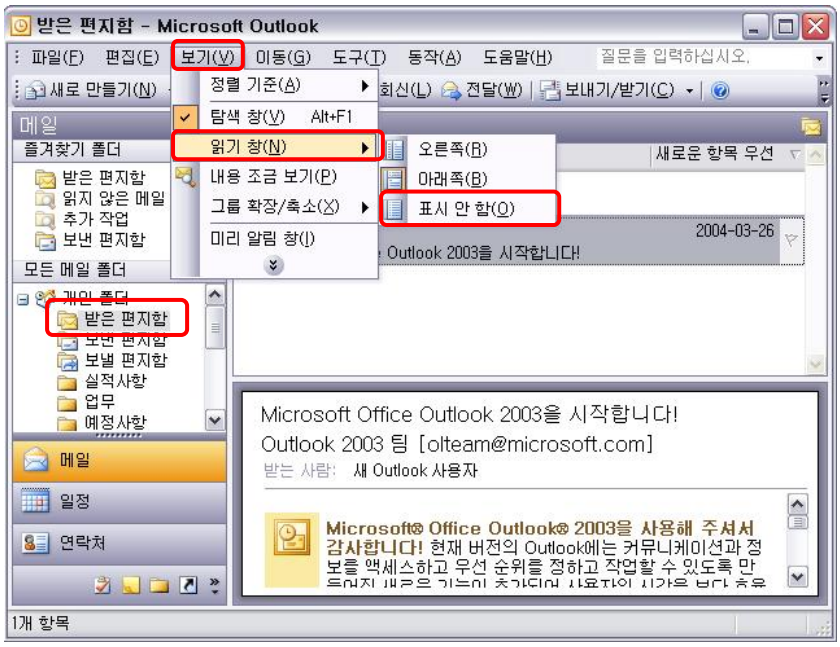
14. 메일 클라이언트의 보안설정 강화(7/8)

- “미리보기” 해제
  - 미리보기 기능을 해제하여 본문에 숨어 있을 수 있는 악성코드의 실행을 방지합니다.
  - 기본적으로 Outlook 2003은 상단에는 이메일의 리스트를, 하단에는 해당 이메일의 미리보기를 보여주도록 설정되어 있습니다.

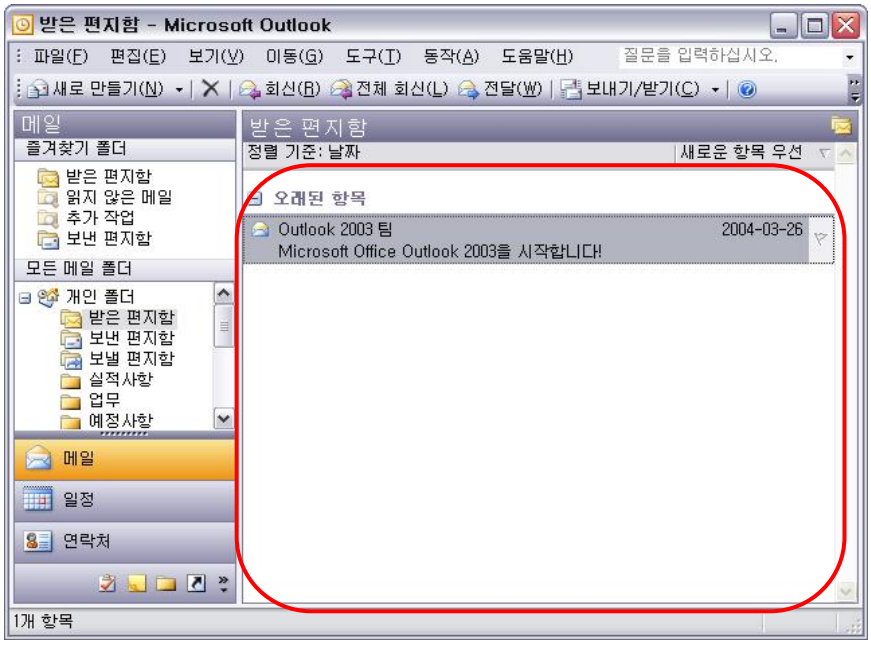


14. 메일 클라이언트의 보안설정 강화(8/8)

- 화면 좌측 폴더에서 “받은 편집함”을 선택하고 “보기” 메뉴에서 “읽기 창”→” 표시 안 함”을 선택합니다.



- 미리보기를 해제하면 아래 그림처럼 이메일의 내용을 미리 보여주는 기능이 해제된 것을 확인할 수 있습니다. 현재 “받은 편지함”에 대해서만 미리 보기 기능이 해제되었습니다. 화면 좌측 폴더 모두에 대해 같은 방법으로 설정하는 것이 좋습니다.
- 설정 변경 사항을 적용하기 위해 프로그램을 종료합니다.



15. 파일이 첨부된 이메일 열람 주의(1/1)

개 요

- 공격자는 이메일(E-Mail)에 웜·바이러스를 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, 내부에 숨겨진 웜·바이러스로 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 감시 기능을 사용하십시오.(89페이지 참조)
- 메일 클라이언트의 보안설정을 강화하십시오.(56페이지 참조)

16. 웹 브라우저의 보안설정 강화(1/7)

개 요

❍ 인터넷 익스플로러는 사용자의 설정으로 보안 기능이 강화될 수 있습니다. 웜·바이러스의 설치를 막거나 보안되지 않는 기능을 막을 수 있으므로 가능한 보안설정을 실행하는 것이 좋습니다.

보안기능 미설정시의 문제점

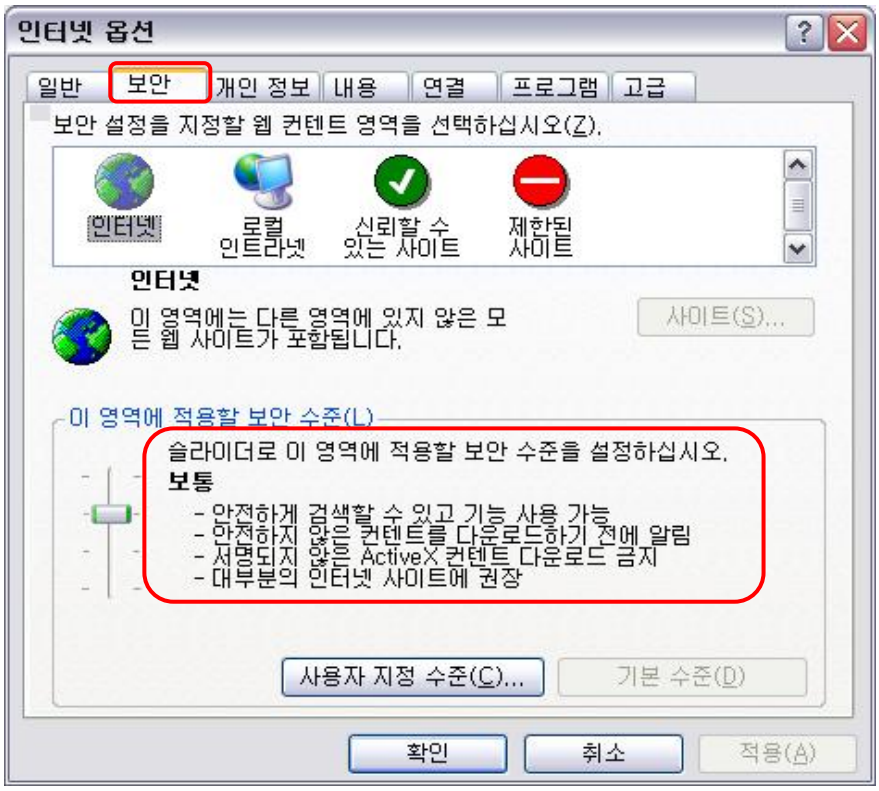
❍ 인터넷 상의 프로그램들을 가리지 않고 설치하거나 실행하게 되어, 컴퓨터가 웜·바이러스에 감염될 수 있습니다.

보안설정 강화방법

❍ 브라우저의 "도구(T)" → "인터넷 옵션(O)"을 선택합니다.

16. 웹 브라우저의 보안설정 강화(2/7)

❍ 「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.

16. 웹 브라우저의 보안설정 강화(3/7)

❍ 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.

16. 웹 브라우저의 보안설정 강화(4/7)

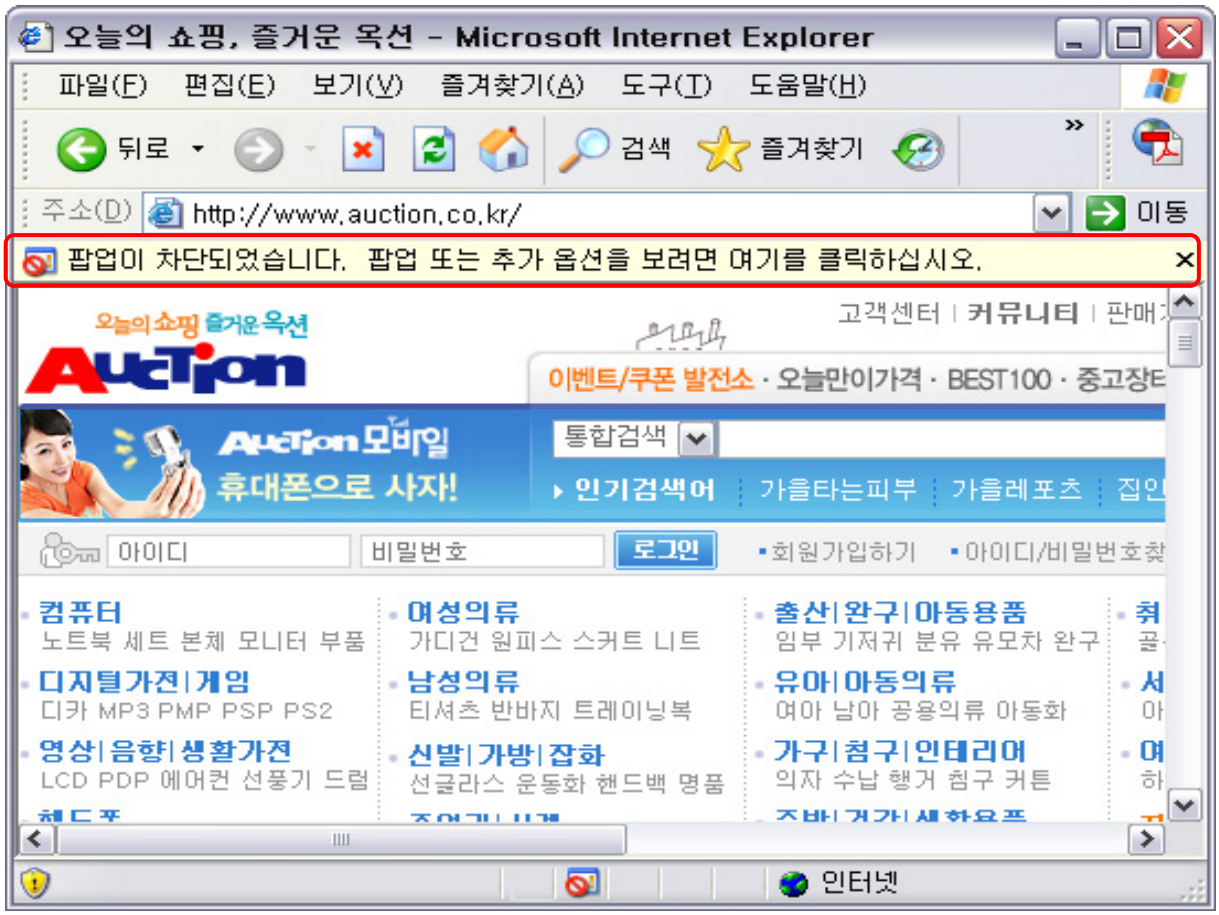
SP2의 특징

주의사항

➢ 아래에 설명하는 특징은 Windows XP SP2 이상에서만 제공됩니다.

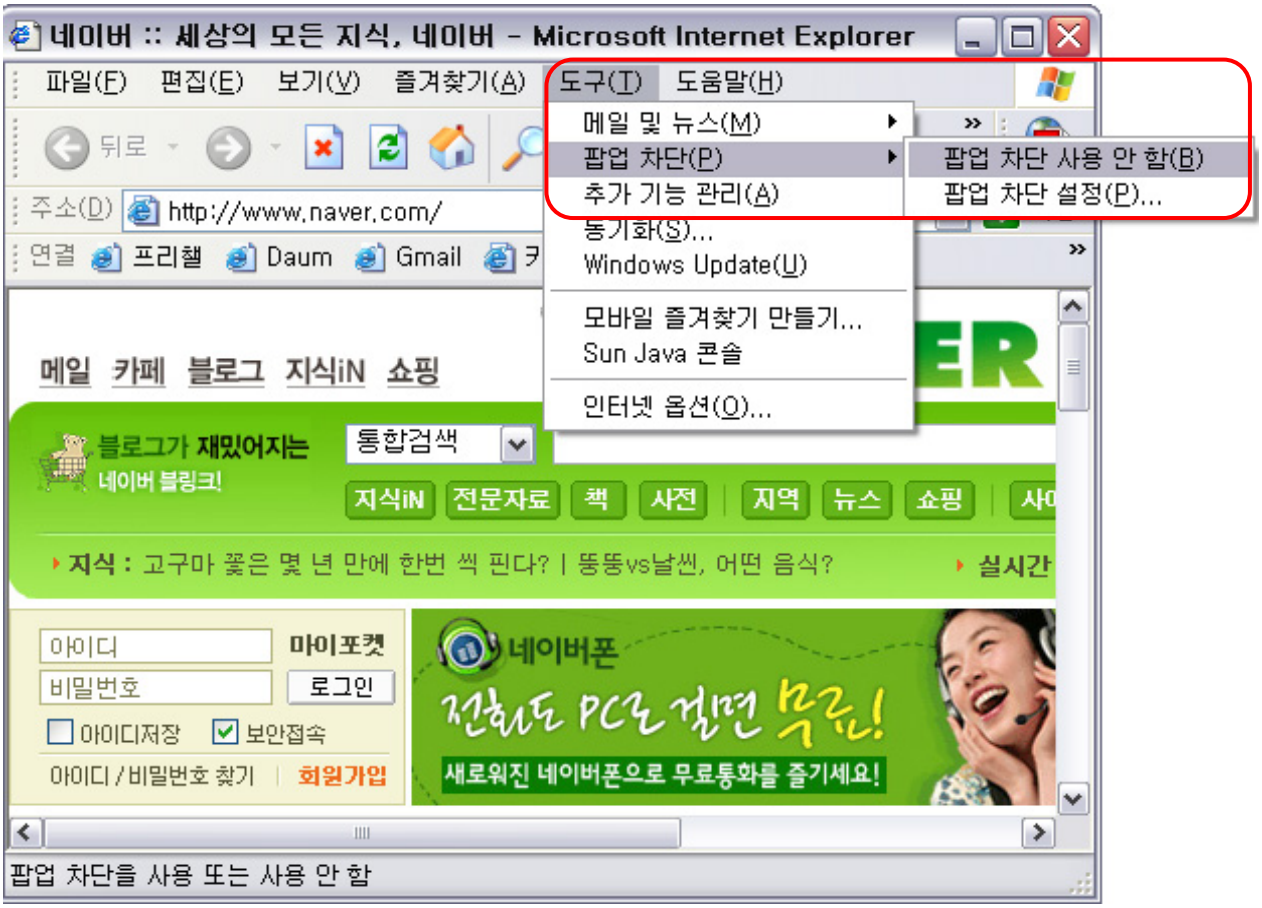
❍ 인터넷 익스플로러 팝업 차단

- SP2에서 새롭게 제공되는 인터넷 익스플로러 팝업 차단 기능은 원하지 않는 팝업 창이 뜨는 것을 대부분 막아줍니다.
- 인터넷 익스플로러 팝업 차단이 활성화되어 있으면 웹 사이트의 팝업 창이 열리려 할 때 인터넷 익스플로러 "알림 표시줄"에 이에 대한 알림이 나타나고 경고음이 재생됩니다.



16. 웹 브라우저의 보안설정 강화(5/7)

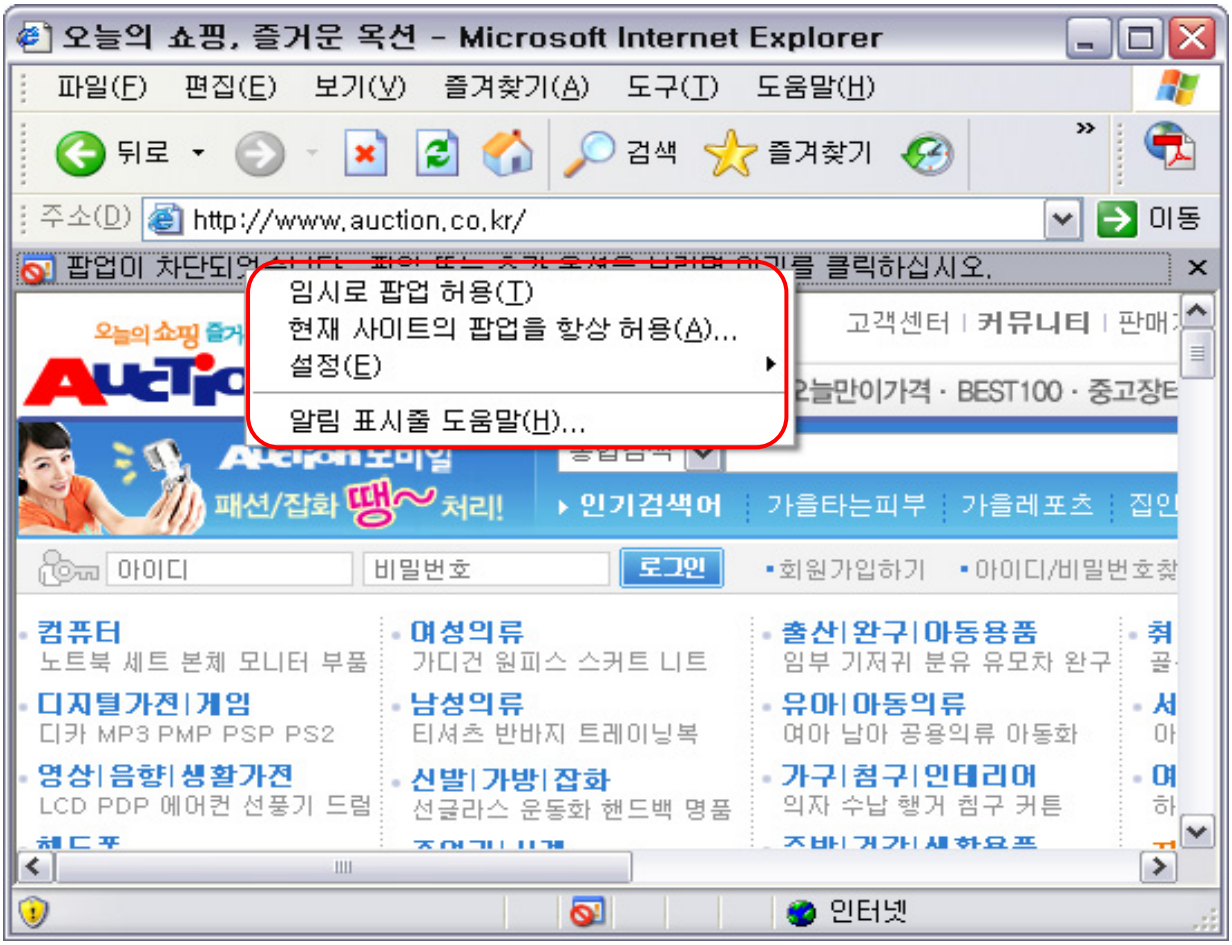
- 이 기능은 인터넷 익스플로러 의 “도구” 메뉴를 통해 사용할 수 있으며 대부분의 웹 사이트 팝업을 차단하면서 원하는 웹 사이트의 팝업은 허용하는 강력한 브라우징 제어 방법입니다.



- 인터넷 익스플로러 팝업 차단은 기본적으로 활성화되어 있으며 다음과 같은 경우에 팝업 창 표시를 예외적으로 허용합니다.
  - 팝업을 띄운 사이트가 허용된 사이트 목록에 추가되어 있는 경우
  - 신뢰 받는 사이트 또는 로컬 인트라넷 영역에 포함된 사이트에서 팝업을 연 경우
  - 웹 사이트에서 초기화된 ActiveX 컨트롤이 팝업을 연 경우

16. 웹 브라우저의 보안설정 강화(6/7)

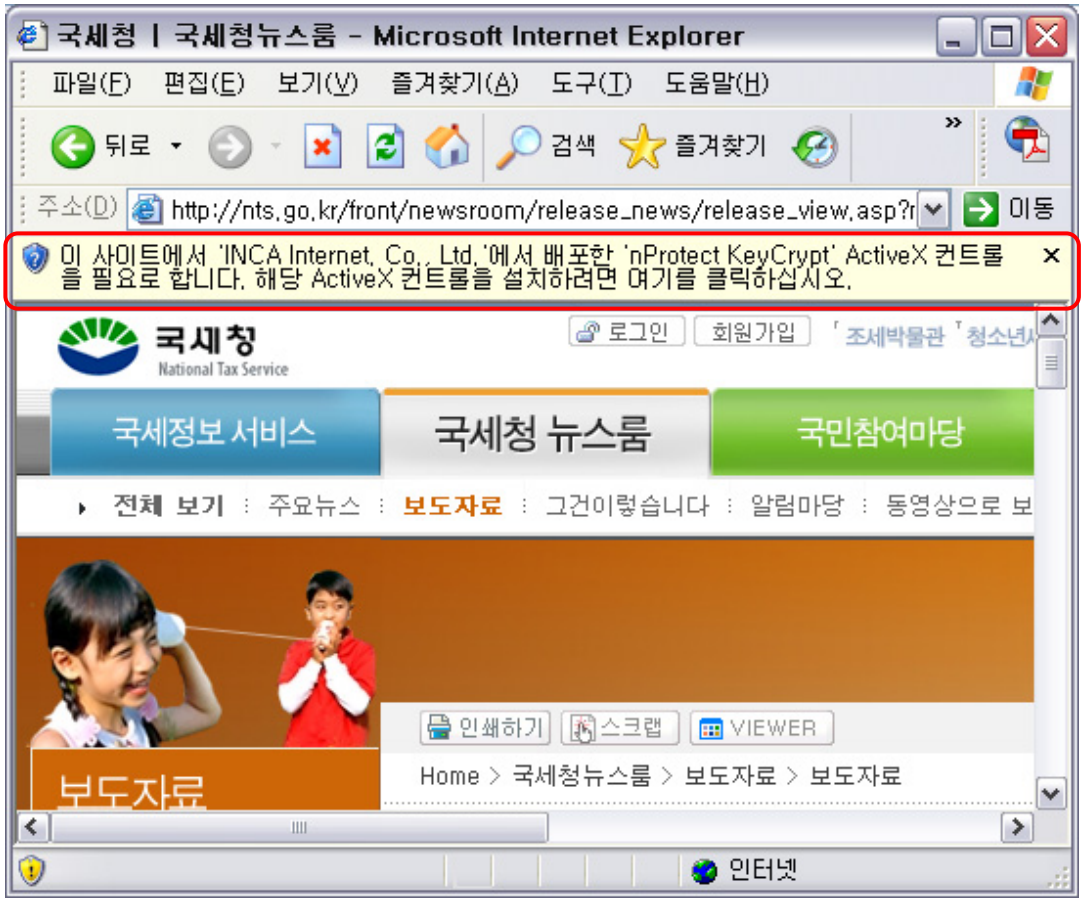
- 알림을 선택하면 다음 옵션을 선택할 수 있는 화면이 나타납니다.
  - 임시로 팝업 허용
  - 현재 사이트의 팝업을 항상 허용
  - 설정



16. 웹 브라우저의 보안설정 강화(7/7)

❍ 인터넷 익스플로러 알림 표시줄

- SP2를 설치하면 인터넷 익스플로러의 기본 설정에 의해 특정 콘텐츠의 설치가 차단됩니다.
- 인터넷 익스플로러 알림 표시줄에는 차단되고 있는 콘텐츠에 대한 경고와 함께 옵션이 제공되어 콘텐츠를 보거나, 제한을 유지하거나, 관련 설정을 조정할 수 있습니다.



- 모든 경고는 인터넷 익스플로러 도구 모음과 웹 페이지 사이에 나타나며 다른 페이지로 이동하면 사라집니다.
- 알림 표시줄의 텍스트는 주어진 경고에 따라 다양하게 나타나는데, 예를 들어 "이 사이트에서 ... ActiveX 컨트롤을 필요로 합니다...."라는 공통 메시지가 나타날 수 있습니다.
- 인터넷 익스플로러 알림 표시줄을 선택하면 해당 경고와 관련된 메뉴가 나타나며, 이 메뉴에서 표시할 콘텐츠와 차단할 콘텐츠를 결정할 수 있습니다.

17. 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 MS의 프로그램 기술 중 하나로, 이를 통해 웹사이트는 사용자 컴퓨터에 특정 프로그램을 설치하고 실행할 수 있습니다.
- 하지만 이러한 인터넷상의 프로그램에 웜·바이러스(스파이웨어 등)가 숨어 있을 수 있을 수 있습니다.
- 따라서 인터넷상의 프로그램을 설치할 때는 주의가 필요합니다.

부주의시의 문제점

- 인터넷을 이용하면서 설치하라는 프로그램들을 주의없이 설치하면 스파이웨어 등 웜·바이러스가 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.

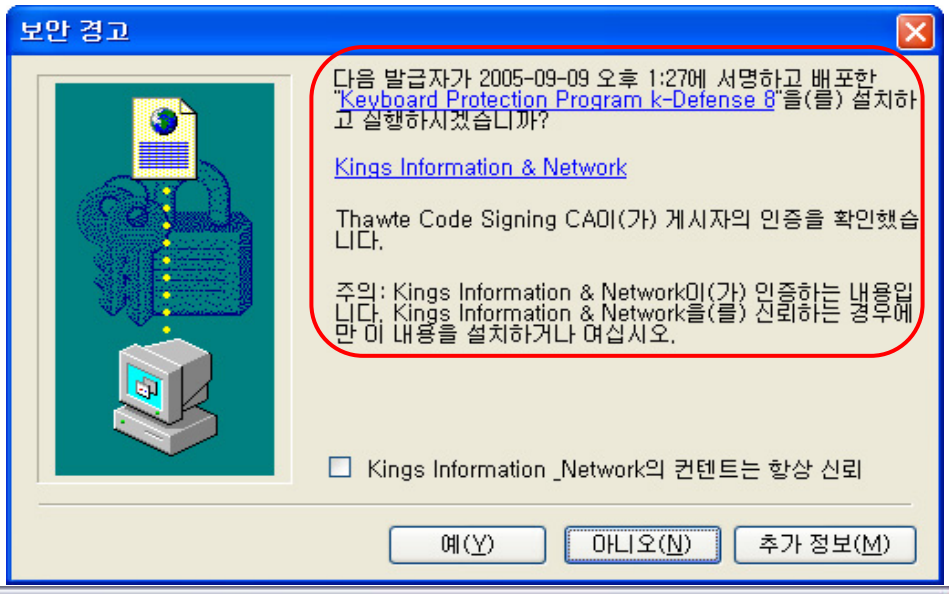
대응 방법

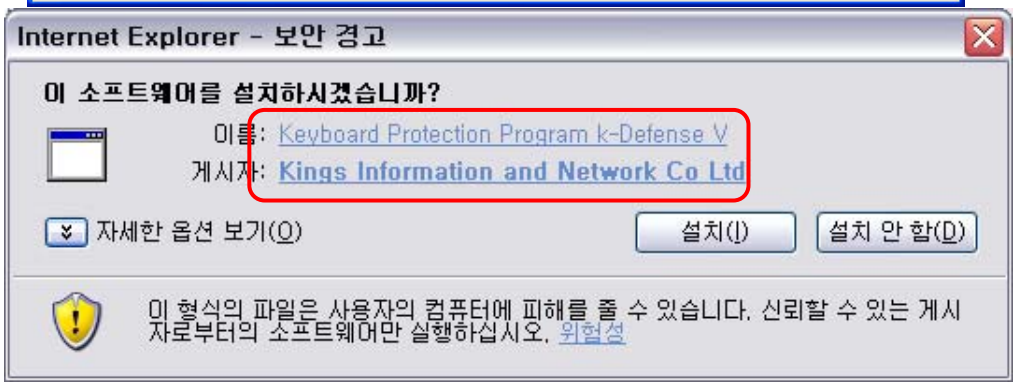
- 웹사이트 방문 시 설치하는 프로그램은 인증서 및 디지털 서명을 참조하여 신뢰성 확인 후 설치하십시오.
- 웹 브라우저의 보안설정을 강화하십시오.(66페이지 참조)

17. 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. Windows XP의 버전에 따라 다음 두 가지 형태일 수 있습니다.
- "Kings Information and Network Co Ltd" 회사에서 만든 "Keyboard Protection Program k-Defense 8(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.(89페이지 참조)

18. 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
- 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, 악성코드가 포함되어 있는 파일이 다른 사용자들에게 전파되는 감염경로로 이용되기도 합니다.

18. P2P 프로그램의 사용 제한(2/2)

P2P 사용으로 인한 문제

- 자료 유출
  - 공유를 위한 폴더 하위의 자료는 인터넷에 공개되어 있는 것과 같습니다.
- 악성코드 유포
  - P2P는 파일의 이름으로만 파일을 구별할 수 있습니다.
  - 누군가 인기가 많은 파일에 웜·바이러스를 포함시킨 뒤, 이를 P2P를 통해 유포하면, 피해자들은 아무런 의심을 갖지 않고 이 파일을 다운로드하여 실행하게 되어 결국에는 웜·바이러스에 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. (77페이지 참조)
  - 해당 프로그램 제거
    - P2P 프로그램을 발견하게 되면 해당 프로그램을 제거합니다. (77페이지 참조)

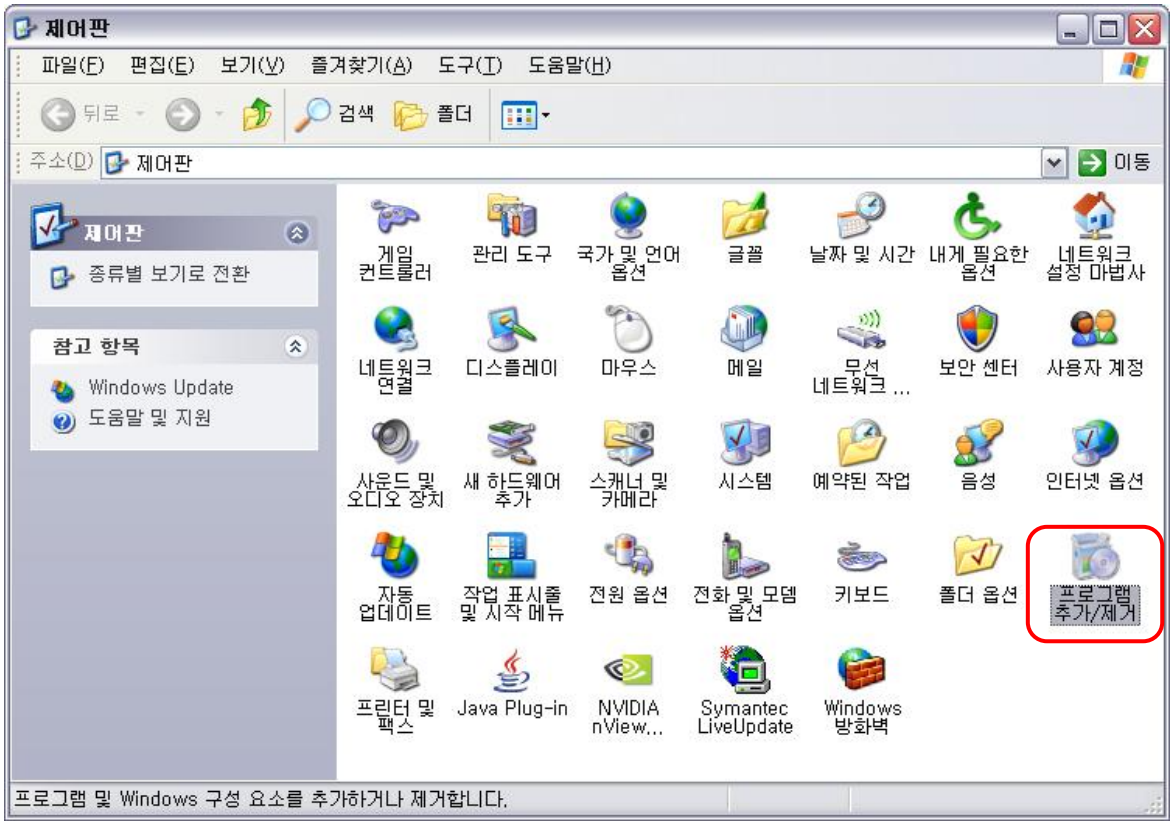
19. 불필요한 프로그램 제거(1/2)

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.

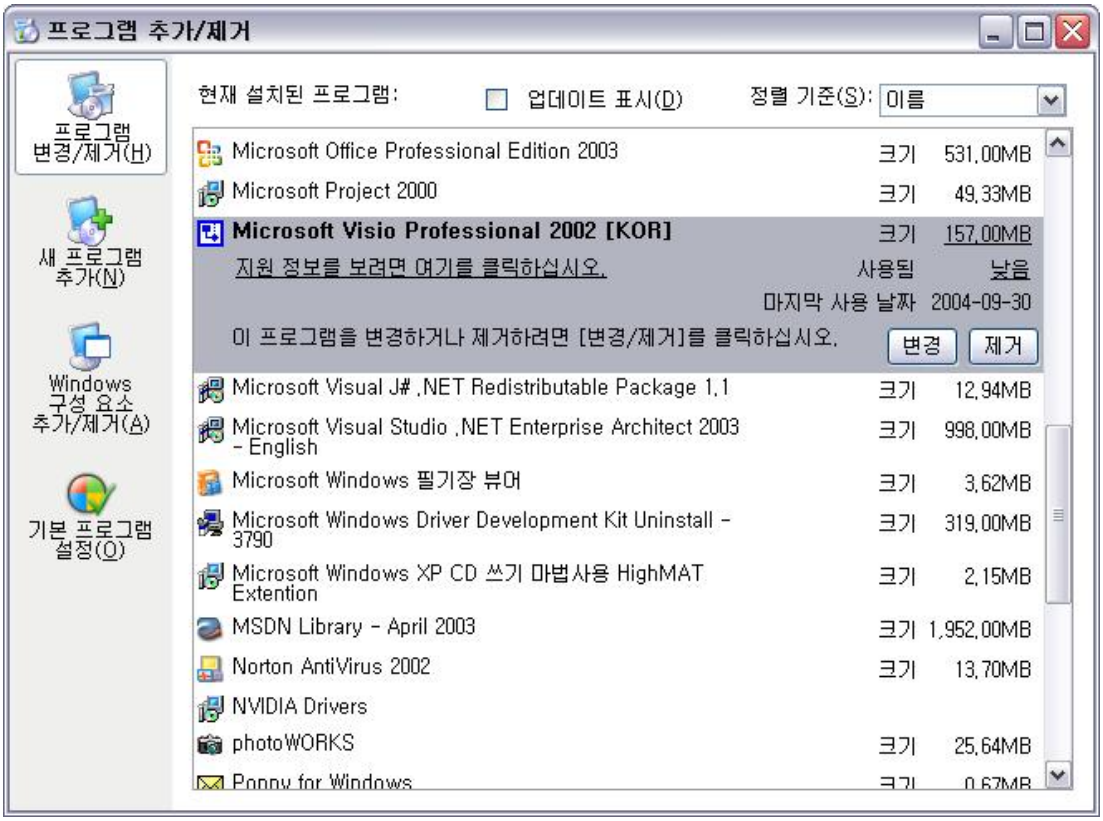
탐지 및 제거방법

- 현재 설치되어 있는 프로그램 확인 및 제거 방법
  - 「제어판」을 열어 "클래식 보기" 상태로 합니다.
  - 「제어판」의 "클래식 보기"에서 "프로그램 추가/제거"를 선택하여 실행합니다.



19. 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 “제거” 혹은 “변경/제거” 버튼을 선택하면 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.

Ⅳ. 바이러스/웜 보안

20. 백신 프로그램 사용(1/1)

개 요

❍ PC에 감염될 수 있는 웜·바이러스를 사전에 탐지하거나 이미 감염되어 있는 웜·바이러스를 제거해 주는 프로그램이 백신(Anti-Virus) 프로그램입니다.

- 웜·바이러스란 컴퓨터에서 동작하는 일종의 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.

21. 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"를 통과한 백신 프로그램 제품은 아직 없는 상태이나, 설명의 이해도를 높이기 위하여 "V3 Pro 2004"를 기준으로 설명하였습니다.
- 이는 이해도를 높이기 위한 방법이며, 특정제품의 사용을 권장하는 것은 아닙니다.

미사용시의 문제점

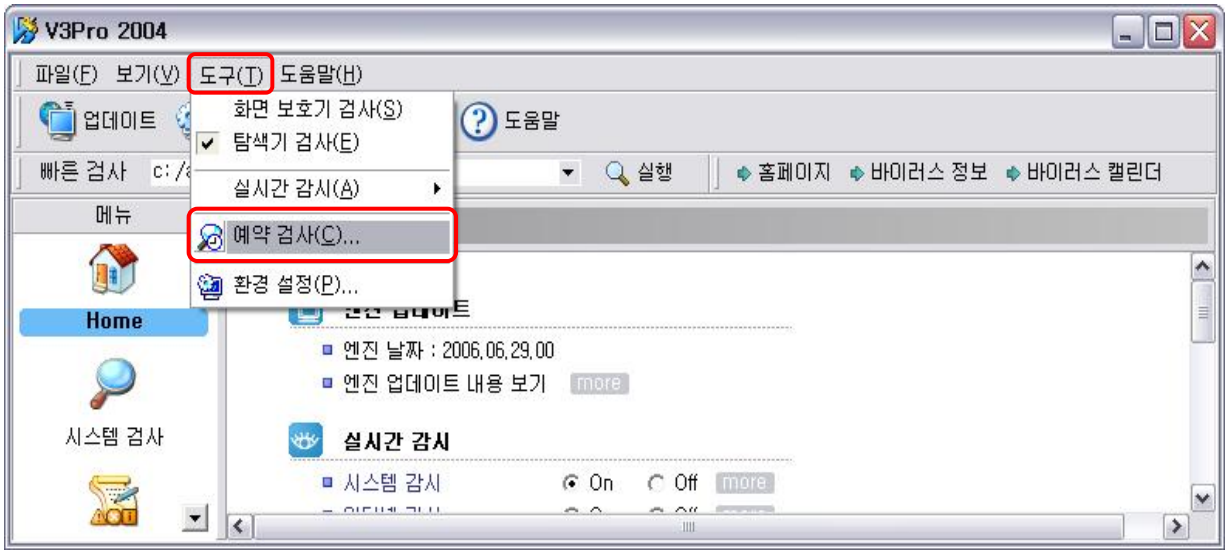
- 웜·바이러스는 매일 신종이 발생되어 전파되기 때문에 백신 프로그램을 오래 전에 수행한 결과는 의미가 없습니다.

21. 주기적 바이러스 검사(2/3)

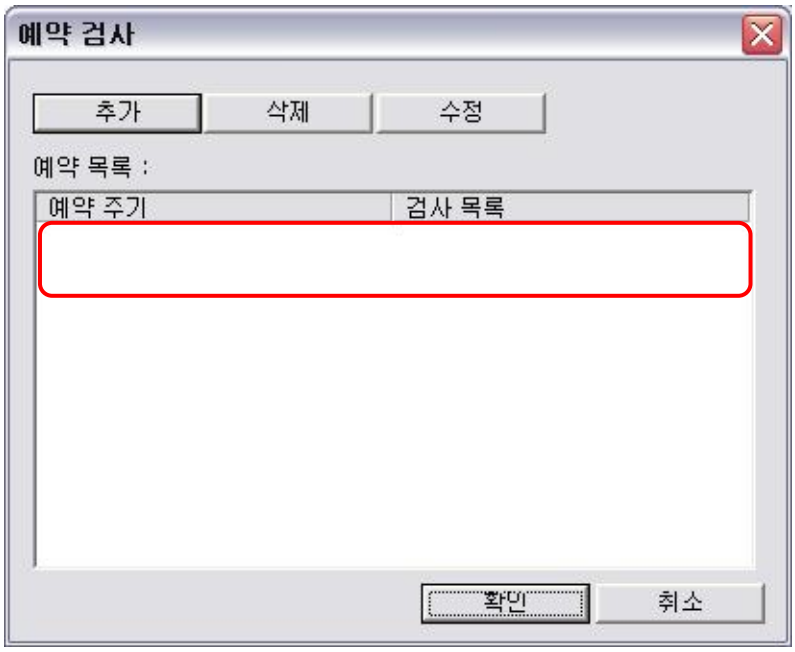
검사방법

❍ 「예약검사」 창 열기

· V3Pro 2004 프로그램에서 "도구(T)" → "예약검사(C)"를 선택합니다.



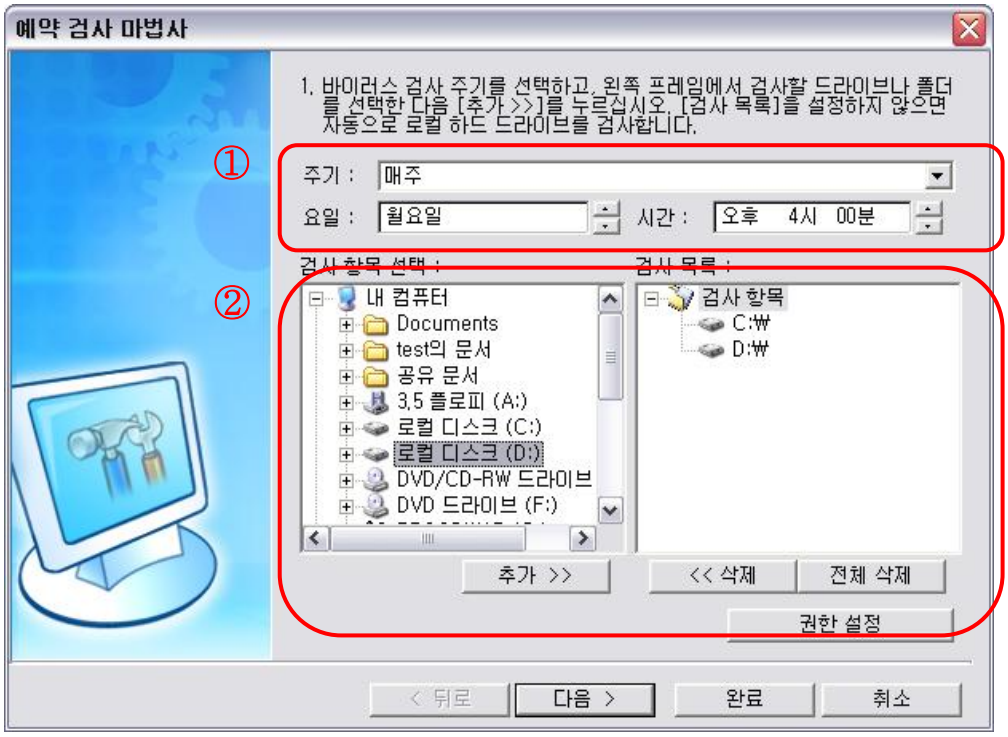
· 현재는 예약이 설정되어 있지 않습니다.



21. 주기적 바이러스 검사(3/3)

❍ 검사 예약 설정하기

- 「예약 검사」 창에서 "추가" 버튼을 선택합니다.



- ①번에서는 검사주기를 선택할 수 있는 데, 매주 월요일 오후 4시에 검사를 시작하는 것으로 설정하였습니다.
- ②번에서는 검사대상을 선택할 수 있는 데, "C:\", "D:\"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.

22. 최신 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.

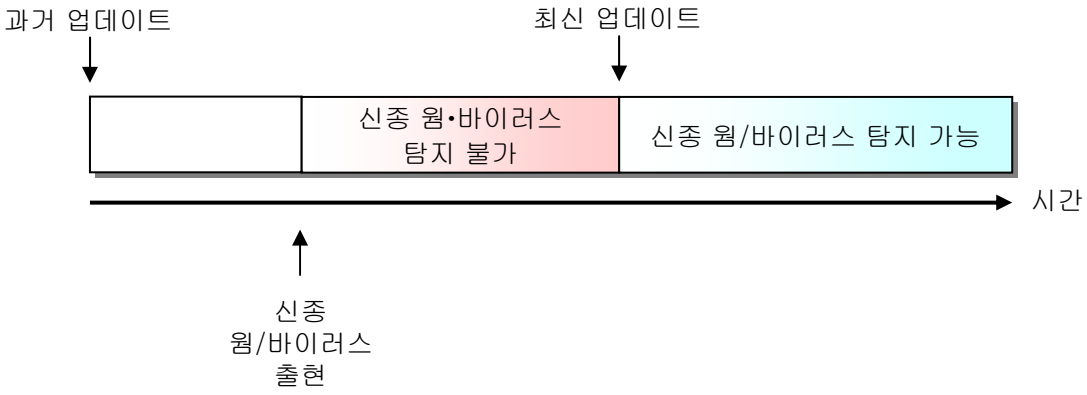
주의사항

➢ "상용 정보보호 시스템 적합성 검증제도"를 통과한 백신 프로그램 제품은 아직 없는 상태이나, 설명의 이해도를 높이기 위하여 "V3 Pro 2004"를 기준으로 설명하였습니다.

➢ 이는 이해도를 높이기 위한 방법이며, 특정제품의 사용을 권장하는 것은 아닙니다.

미사용시의 문제점

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

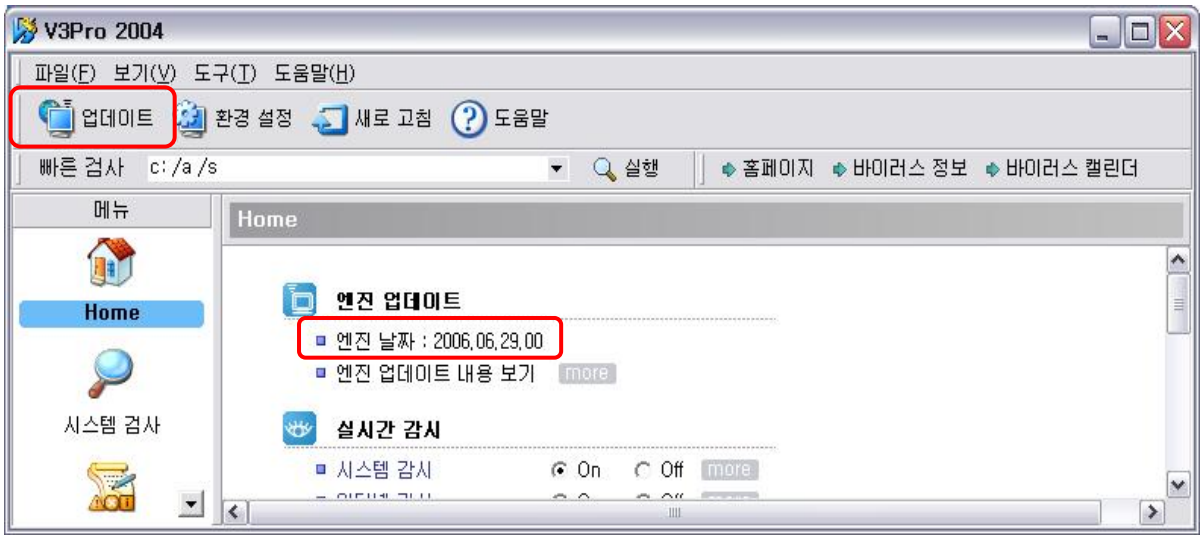


22. 최신 백신 엔진 업데이트(2/5)

업데이트 방법

❍ 대부분의 백신 프로그램은 인터넷을 통해 자동으로 엔진 업데이트를 수행할 수 있습니다.

❍ 엔진 날짜 확인하기

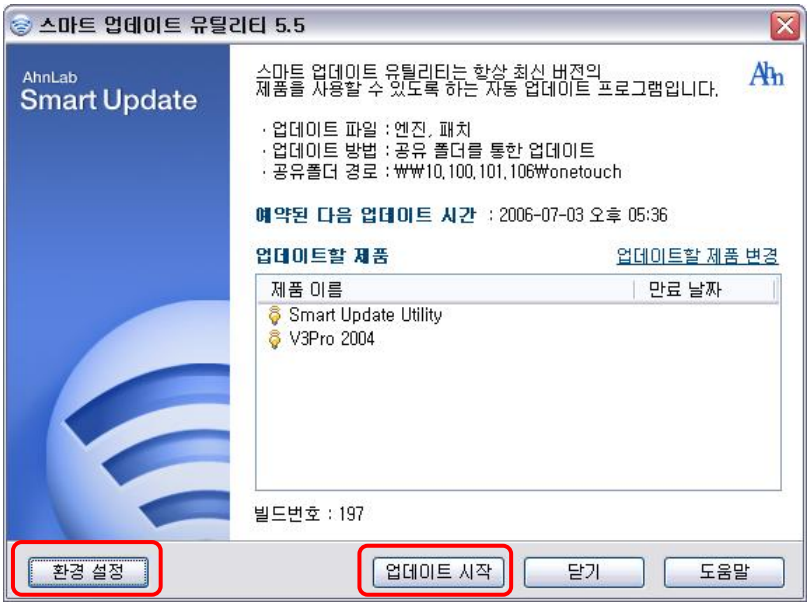


- 「V3Pro 2004」 창에서 현재 엔진의 날짜를 확인할 수 있습니다.
- 현재의 것은 2006년 6월 29일의 것으로 이 엔진으로는 이후에 작성된 웜·바이러스를 탐지할 수 없으므로 엔진을 최신의 것으로 업데이트 해야 합니다.

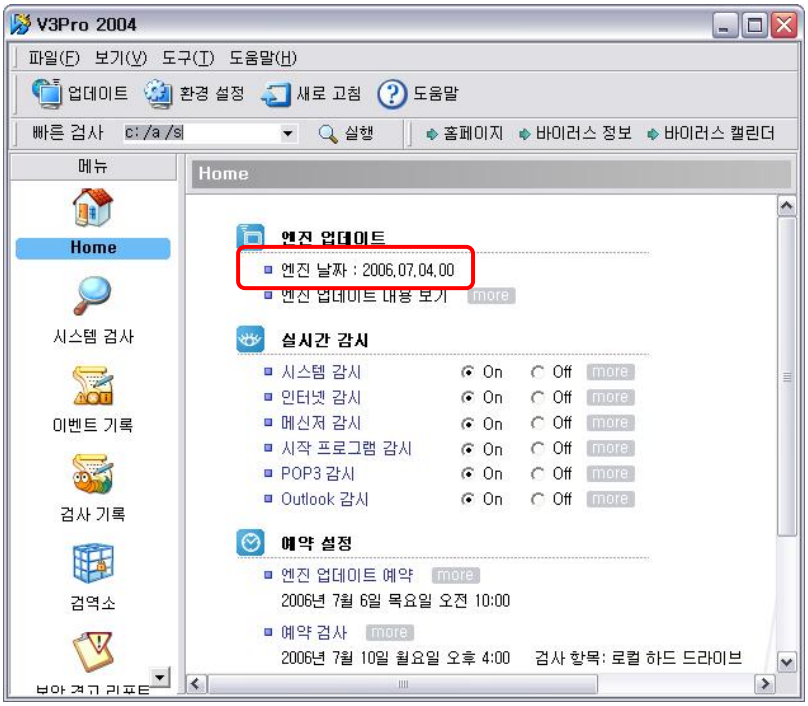
22. 최신 백신 엔진 업데이트(3/5)

❍ 업데이트 시작하기

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



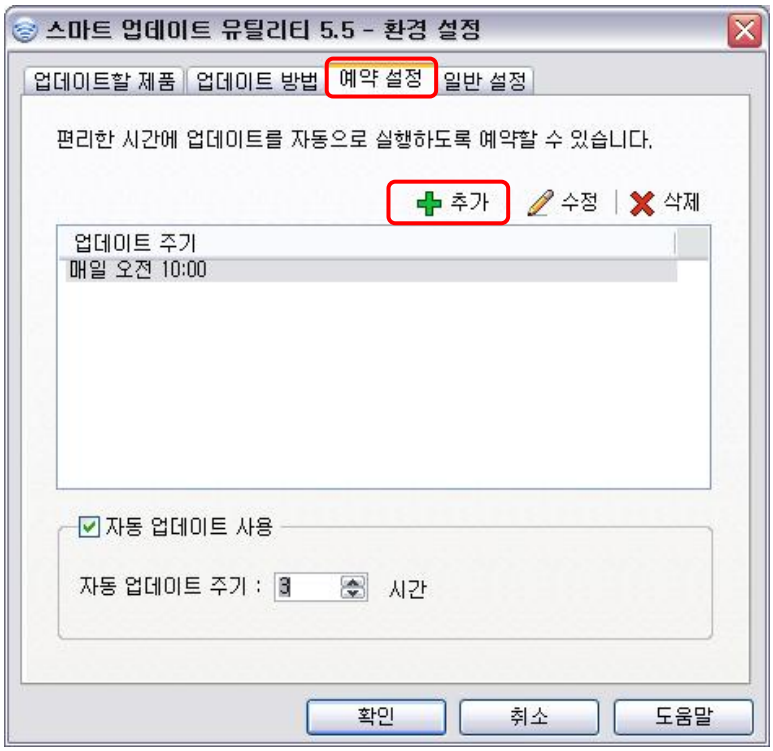
- 「스마트 업데이트 유틸리티」 창에서 "시작" 버튼을 선택하면 업데이트가 시작됩니다.
- 업데이트 완료 후에 "V3Pro 2004" 프로그램을 시작하면 다음과 같이 엔진의 날짜가 최신의 것으로 변경되어 있는 것을 확인할 수 있습니다.



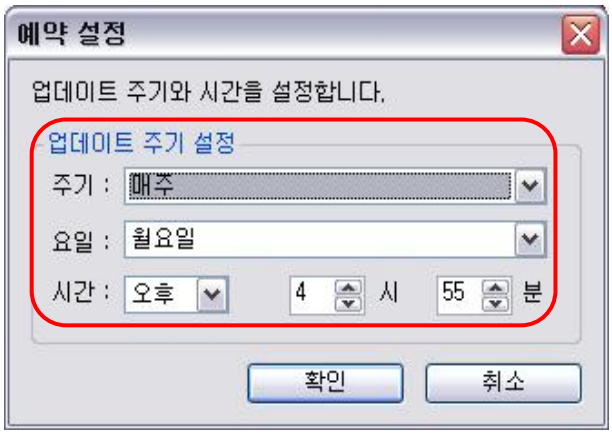
22. 최신 백신 엔진 업데이트(4/5)

❍ 업데이트 예약 설정하기

- 「스마트 업데이트 유틸리티」 창의 “환경설정” 버튼을 선택하여 열리는 창에서 “예약 설정”탭을 선택하고, “추가” 버튼을 선택합니다.

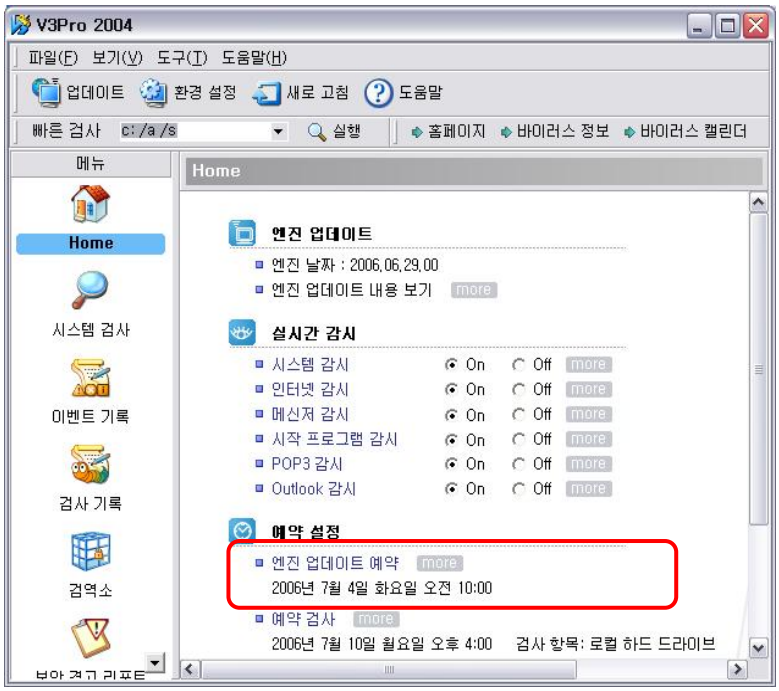


- 「예약 설정」 창이 나타나면 “주기”, “요일“, “시간”을 설정하고 “확인”을 누르면 예약이 설정됩니다.

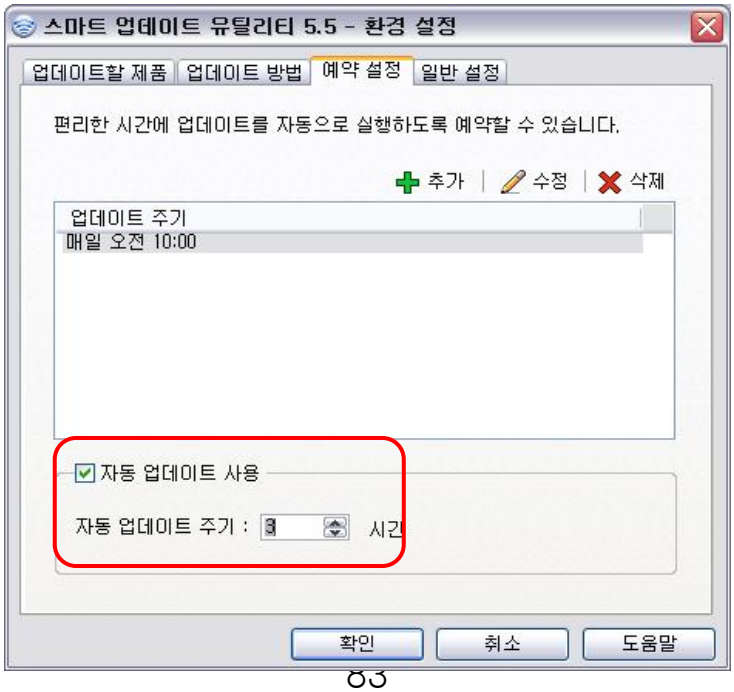


22. 최신 백신 엔진 업데이트(5/5)

- 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.



23. 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"를 통과한 백신 프로그램 제품은 아직 없는 상태이나, 설명의 이해도를 높이기 위하여 "V3 Pro 2004"를 기준으로 설명하였습니다.
- 이는 이해도를 높이기 위한 방법이며, 특정제품의 사용을 권장하는 것은 아닙니다.

미수행시의 문제점

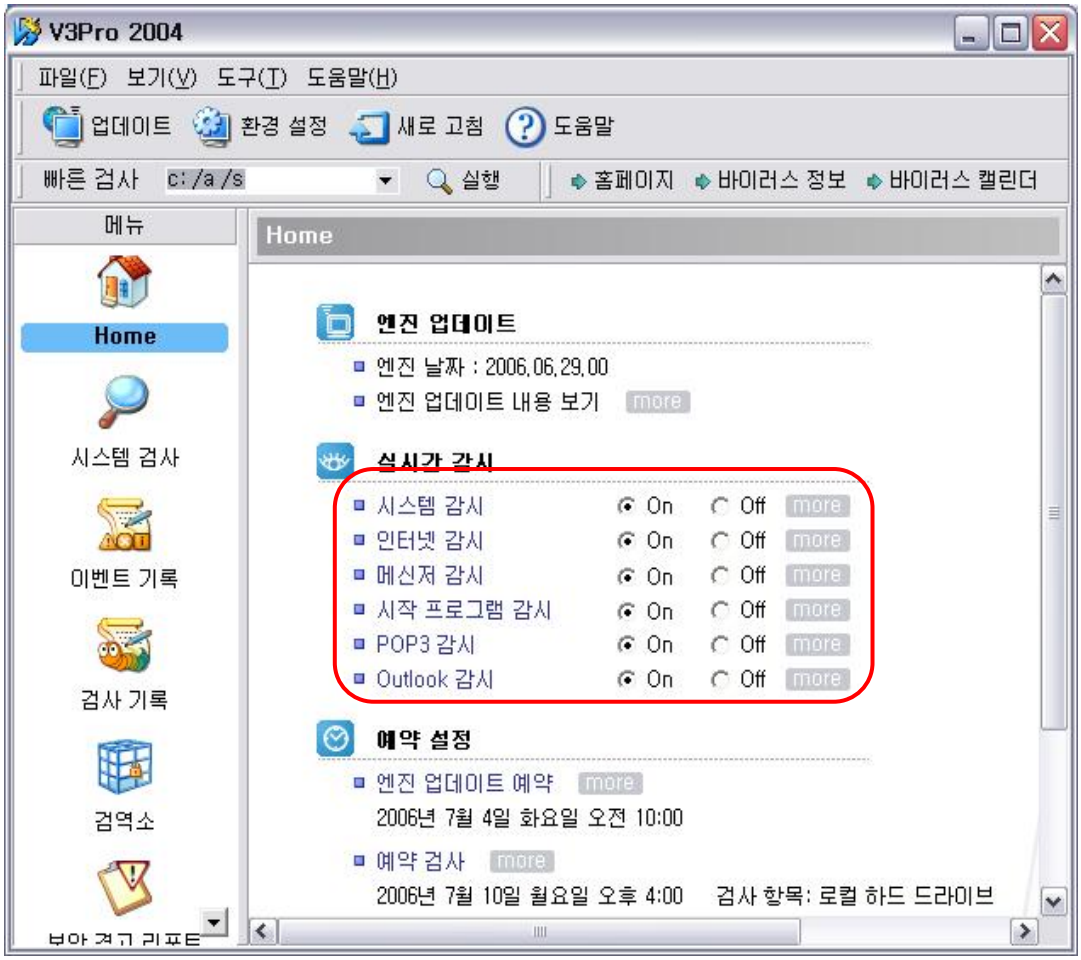
- 지금까지의 백신 프로그램 사용은 평상시에는 웜·바이러스를 탐지하지 않다가 특정 시각이 되면 시스템 전체를 대상으로 웜·바이러스를 탐지하는 형태입니다.
- 이미 감염된 웜·바이러스를 탐지하는 것보다 사용자의 컴퓨터에 침입하려는 웜·바이러스를 즉각 차단하여 애초에 컴퓨터에 침입할 수 없게끔 하는 것이 더 좋은 방법이 될 수 있습니다.
  - 네트워크와 보조기억매체의 발달로 인해 다양한 형태의 정보가 실시간으로 교환·공유·전파되는 환경에서는 실시간 점검이 큰 역할을 수행할 수도 있기 때문입니다.

23. 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.

23. 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 악성코드를 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 악성코드 확산 방지에 유용합니다.
- Outlook 감시
  - 마이크로소프트 Outlook 메일 프로그램(MS Outlook 2000 이상)을 통해서 들어오는 메일들을 실시간으로 검사합니다.
  - 첨부파일을 통한 악성코드 확산 방지에 유용합니다.

V. 문제점 해결

24. 프린터 공유 시의 문제 해결 방법(1/1)

상황 개요

- 로컬 프린터를 직접 연결하여 공유를 제공하는 PC에서 PCChecker 1.0을 수행하고, "Guest 계정 점검" 항목을 자동수정할 경우 원격 프린터 사용자가 프린터를 사용할 수 없는 현상이 발생할 수 있습니다.
- 원격 공유 프린터를 사용하고자 하는 PC는 "Guest 계정 점검" 항목을 자동수정해도 프린터 사용에 문제가 없습니다.

발생 원인

- 다른 PC에 연결된 프린터를 사용하고자 하는 PC(이하 "클라이언트 PC")가 출력을 시도하면 프린터 공유를 제공하는 컴퓨터(이하 "서버 PC")의 Guest 계정으로 연결되어 프린터 출력이 이루어지는데, 서버 PC의 Guest 계정이 비활성화되어 있으므로 서버 PC로의 접속이 이루어질 수 없기 때문에 발생하는 현상입니다.
- 원인은 서버 PC에서 Guest 계정이 비활성화 즉, Guest 계정을 통한 외부 접근을 제한하게 되어 발생하며, 그 결과 클라이언트 PC가 공유 프린터를 통해 이전에 사용하고 있던 프린트 기능을 사용하지 못하는 것입니다.

해결 방법

- 서버 PC가 Windows XP Home인 경우
  - 서버 PC의 Guest 계정을 다시 활성화시켜야 합니다.
    - 5. Guest 계정 비활성화에서 Guest 계정을 켜기 상태로 만들면 Guest 계정이 활성화됩니다.
  - 클라이언트 PC의 사용방법은 변경이 없습니다.

  ※ Guest 계정이 활성화되므로 PC 보안관리에 주의가 요구됩니다.
- 서버 PC가 Windows XP Professional인 경우(2. 안전한 프린터 공유를 위한 계정 생성/사용 방법 참조)
  - 서비 PC의 Guest 계정 비활성화는 유지하고, 프린터 사용을 위한 계정을 생성한 후, 이를 클라이언트 PC 사용자들에게 공지하여 사용합니다.
  - 클라이언트 PC는 부팅 시에 서버 PC에 대한 사용자 인증을 수행한 후부터 프린터를 사용할 수 있습니다.

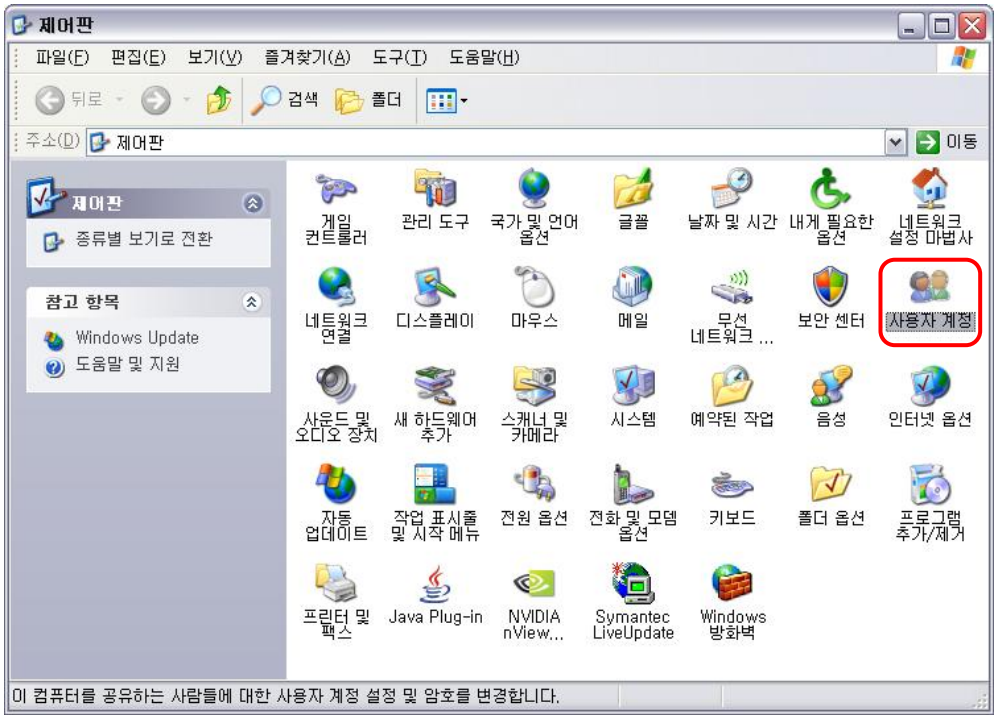
25. 프린터 공유를 위한 계정 생성 방법(1/7)

❍ 서버 PC가 Windows XP Professional인 경우에 사용하는 방법으로 다음의 세 가지 동작을 수행해 주어야 합니다.

- 서버 PC에서 프린터 전용 계정을 생성
- 서버 PC의 로컬 보안정책 변경
- 클라이언트 PC의 사용자 인증 수행

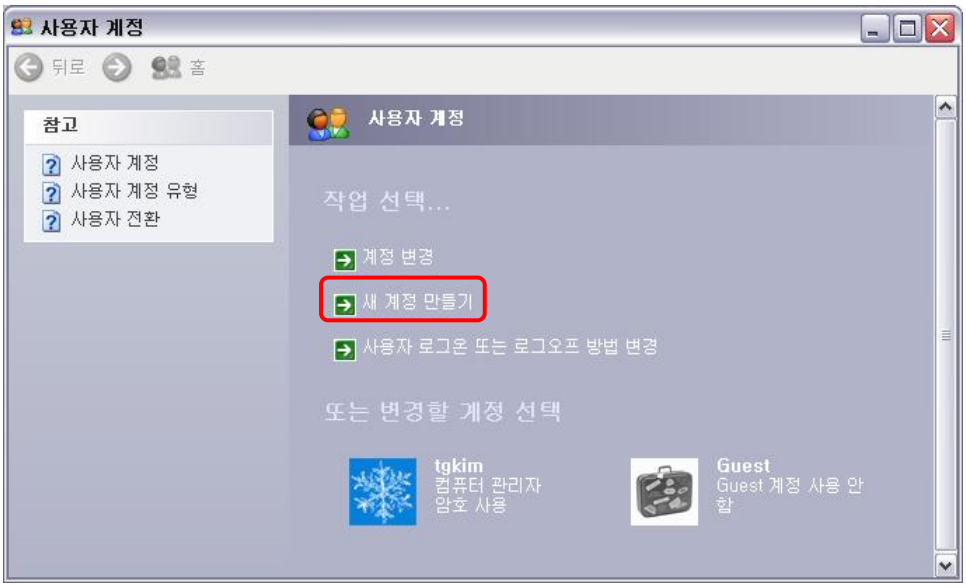
❍ 서버 PC에서 프린터 전용 계정을 생성하는 방법

- 「제어판」을 열어 "클래식 보기" 상태로 합니다.
- 「제어판」의 "클래식 보기"에서 "사용자 계정"를 선택하여 실행합니다.

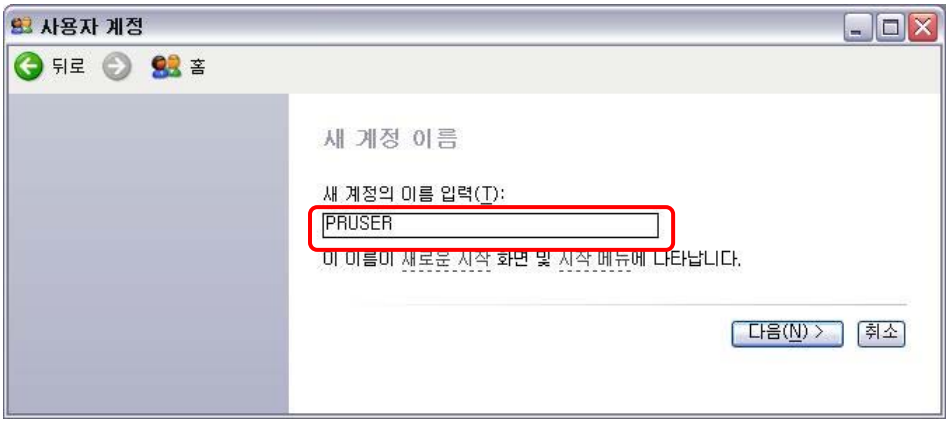


25. 프린터 공유를 위한 계정 생성 방법(2/7)

- “사용자 계정” 창이 나타나면 “새 계정 만들기” 메뉴를 선택합니다.



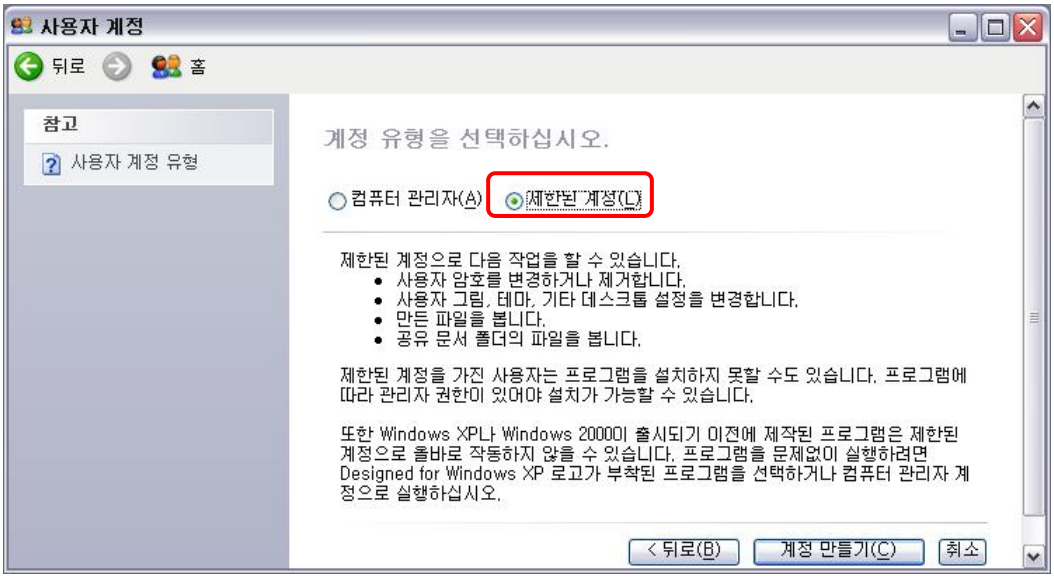
- “새 계정 이름 입력” 란에 프린터 출력 시에만 사용할 전용 아이디(예: PUSER)를 입력하고 “다음” 버튼을 선택합니다.



25. 프린터 공유를 위한 계정 생성 방법(3/7)

- “제한된 계정”을 선택한 후, “계정 만들기” 버튼을 선택합니다.

  ※ 프린터 출력 시에만 사용할 전용 아이디를 “제한된 계정”으로 생성함으로써 관리자 권한의 계정 오용을 방지할 수 있습니다.



- 앞에서 생성한 프린터 출력 시에만 사용할 전용 아이디(예: PUSER)의 로그온 패스워드를 생성합니다.(1. 로그온 패스워드 사용 참조)

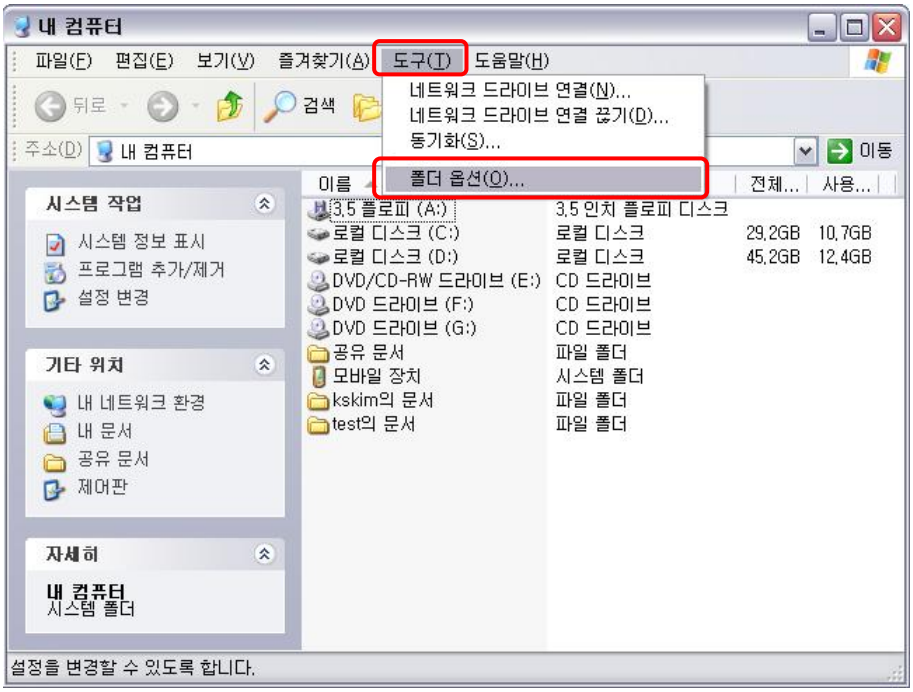
❍ 서버 PC의 로컬 보안정책 변경 방법

- 다음 페이지에서 계속 설명합니다.

25. 프린터 공유를 위한 계정 생성 방법(4/7)

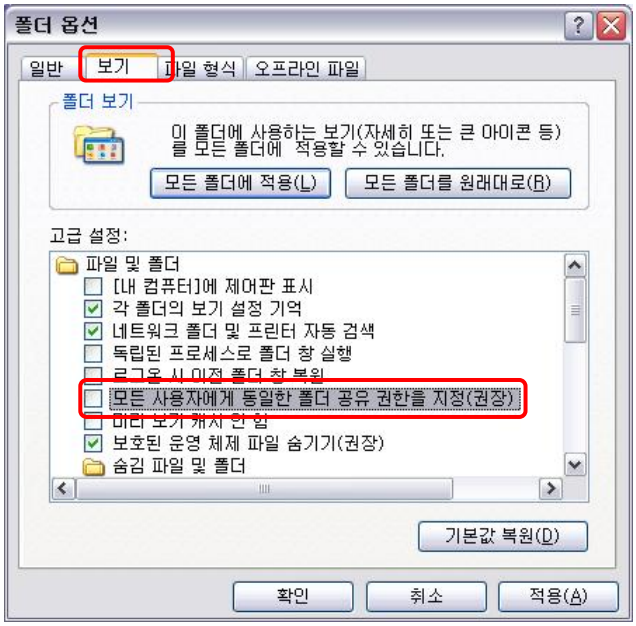
- "시작" → "내 컴퓨터" 메뉴를 선택합니다.

- "내 컴퓨터"의 "도구" 메뉴에서 "폴더 옵션..."을 선택합니다.



25. 프린터 공유를 위한 계정 생성 방법(5/7)

- “폴더 옵션”에서 “보기” 탭을 선택하고 “고급 설정”에서 “모든 사용자에게 동일한 폴더 공유 권한을 지정(권장)”을 “해제”한 뒤 “확인”을 선택합니다.



- 서버 PC 관리자가 설정된 아이디와 패스워드를 프린터를 사용할 사용자에게 공지함으로써 서버 PC의 설정은 종료됩니다.

25. 프린터 공유를 위한 계정 생성 방법(6/7)

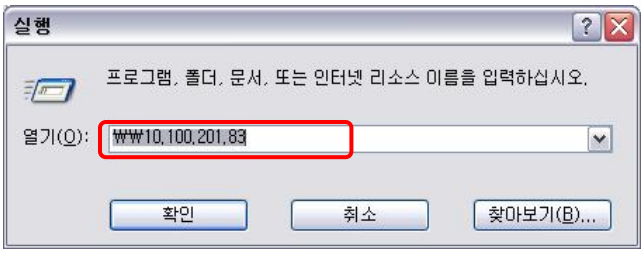
❍ 클라이언트 PC의 사용자 인증 수행 방법

- 서버 PC에서 계정 생성과 보안정책 변경이 완료되면, 서버 PC는 프린터 사용을 위한 준비가 완료된 것입니다.
- 클라이언트 PC는 다음에 설명하는 동작수행을 통해 서버 PC에게 자신을 인증해야 합니다.
- 다음에 설명되는 동작을 PC 부팅 후 1회는 수행해야 공유 프린터를 사용할 수 있습니다.

- "시작" → "실행" 메뉴를 선택합니다.

25. 프린터 공유를 위한 계정 생성 방법(7/7)

- "실행" 대화상자에서 \\서버의 IP주소(예: 10.100.201.83)를 입력하고 "확인"을 선택합니다.



- 일정 시간(수초)이 지나면 아이디와 패스워드를 입력해야 하는 대화상자가 나타나는데, 이곳에 서버 PC 관리자가 알려준 프린터 전용 아이디와 패스워드를 입력합니다.

※ 이와 같이 수행하면 공유 프린터 사용을 위한 클라이언트 PC의 사용자 인증은 완료되며 이후로 공유 프린터를 이용하여 프린터 출력을 사용할 수 있습니다.