작성자 : 기술지원부 조 태 준 tedcho@nextline.net

목 차

1. 레지스트리 수정내용
2. 보안 설정 내용
3. Next_filter (IPSEC)

Window 2003 Server 제품의 종류

windows server 2003 제품군은 Web Edition, Standard Edition, Enterprise Edition, Datacenter Edition의 네가지 제품군으로 나뉘며 각제품군의 특징은 다음과 같습니다.

1. Windows server 2003 Web Edition

배포 및 관리가 용이한 서버 운영체제이며, 최적화된 웹 호스팅 패키지입니다. Windows server 2003 Web Edition을 실행하는 서버는 도메인에 합류될 수는 있지만 도메인 컨트롤러 역할을 할 수 없으며, 인증서 서비스, Microsoft Exchange Server 또는 Microsoft SQL Server 와 같은 기타 서버 응용 프로그램에 대한 호스트를 구성될 수 없습니다.

2. Windows server 2003 Standard Edition

소규모 기업에 사용할 수 있도록 설계되어 있으며, 가장 일반적인 기능을 가진 서버입니다. Windows 2000 Standard Edtion 에서는 NLB가 기본적으로 지원되지 않았으나 Windows Server 2003 Standard Edition에서는 기본 지원되며, POP3 또한 지원됩니다.

3. Windows server 2003 Enterprise Edition

중간 또는 대기업 대상을 설계되었으며, 클러스터를 여전히 지원합니다. Windows Server2000 버전에서는 Advance Edition 으로 불리였고, 다시 Server2003에서는 Enterprise Edition으로 이름이 바뀌었습니다.

4. Windows server 2003 Datacenter Edition

가장 높은 수준의 확장성, 가용성 및 안전성을 요구하는 기업용으로 설계되었으며 Windows 2000 Datacenter 버전과 같이 OEM 파트너를 통해서만 구입이 가능합니다. 64bit용 Datacenter 버전의 경우 최대 512GB 의 RAM과 최대 64개의 CPU를 지원합니다.

DNS 서버 구축 및 설정

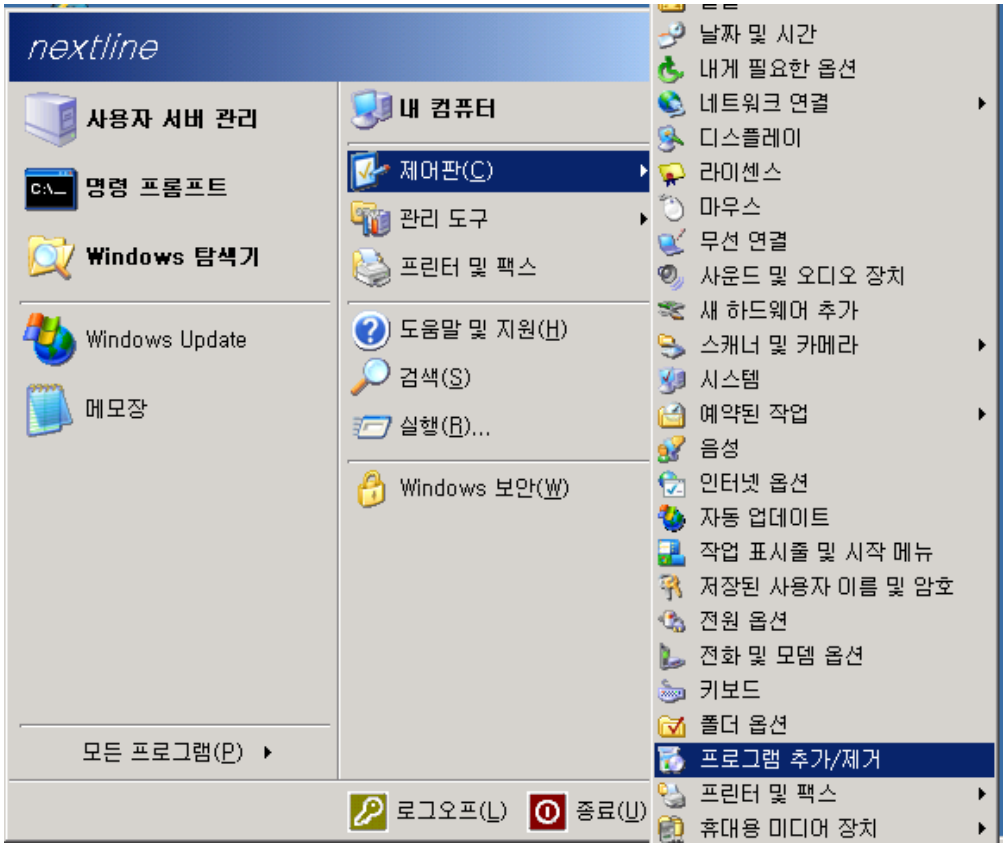
1. DNS란?

DNS는 도메인의 계층 구조로 구성된 컴퓨터 및 네트워크 서비스를 명명하는 시스템으로 DNS(Domain Name System)라고도 합니다.

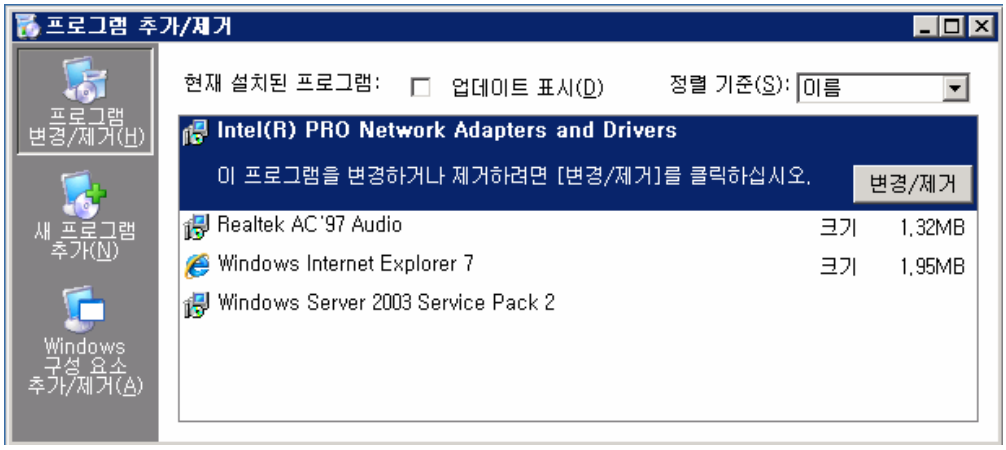
TCP/IP 기반의 네트워크에서는 서버 간에 IP 주소를 이용하여 통신하기 때문에 서버마다 고유한 IP 주소를 가지고 있는데, IP 주소는 61.100.191.44와 같은 숫자로 구성되어 있어서 일반 사용자들이 쉽게 기억하지 못하는 단점이 있습니다. 그래서 사용자들이 좀더 쉽게 사용할 수 있도록 DNS를 이용하여 숫자로 구성된 주소를 도메인 주소로 연결시켜 주도록 하는 것 입니다.

2. DNS(Domain Name System)설치방법

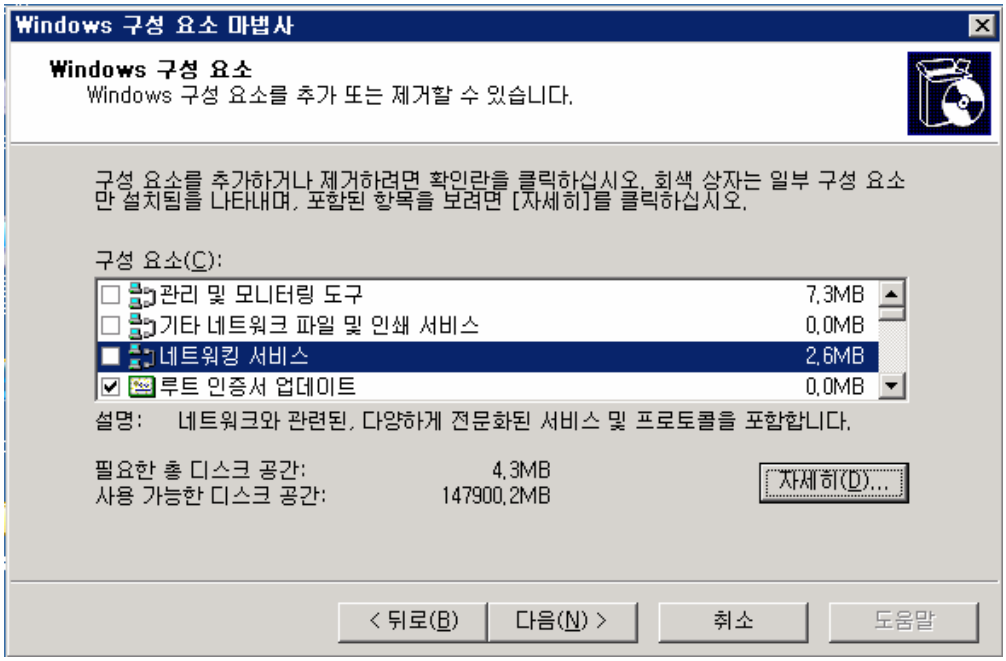
1) [시작]-[제어판]-[프로그램추가/제거]를 선택 합니다.



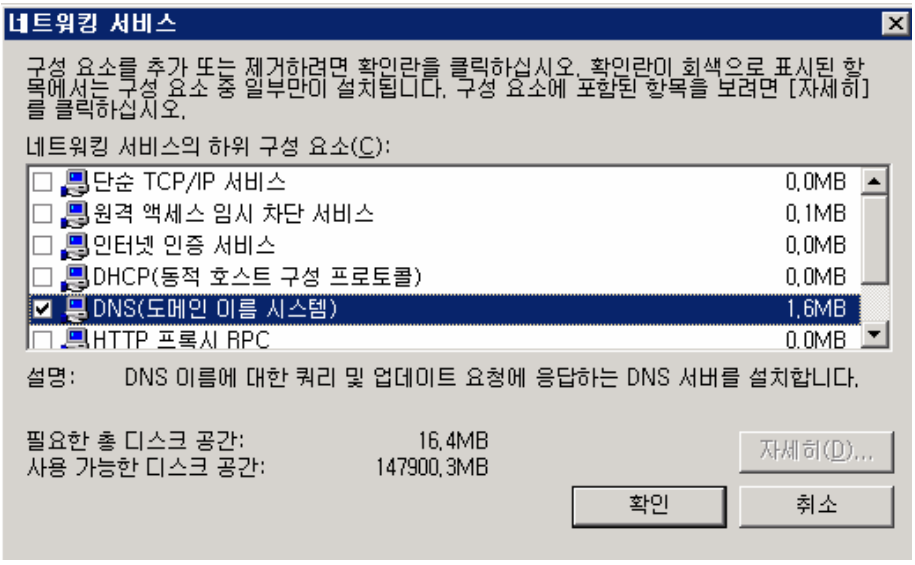
2) [Windows구성요소 추가/제거]를 선택 합니다.



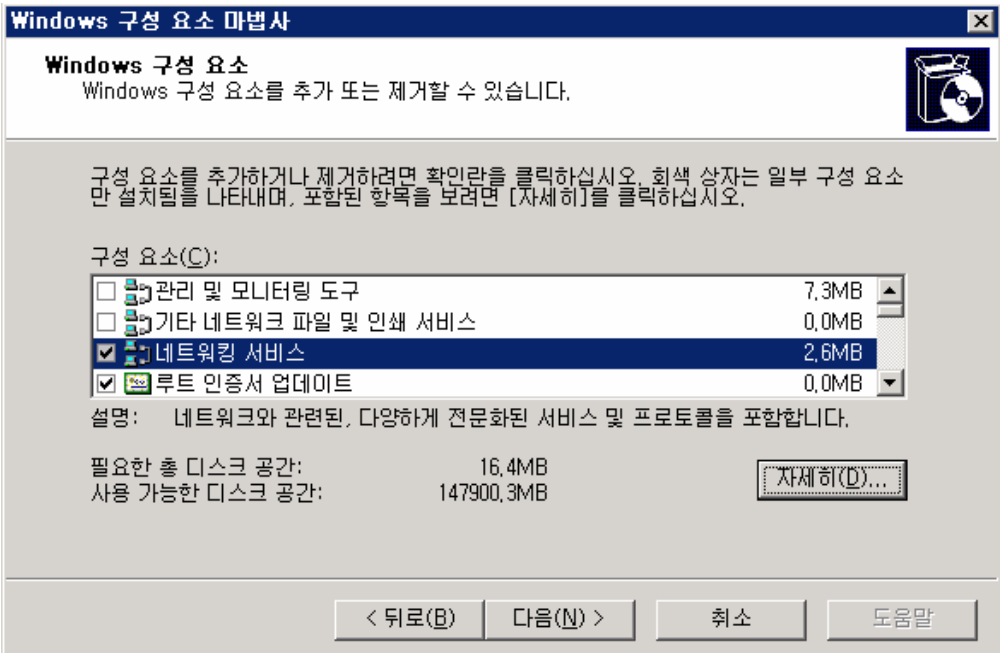
3) [네트워킹 서비스]를 선택 후 [자세히] 버튼을 클릭합니다.



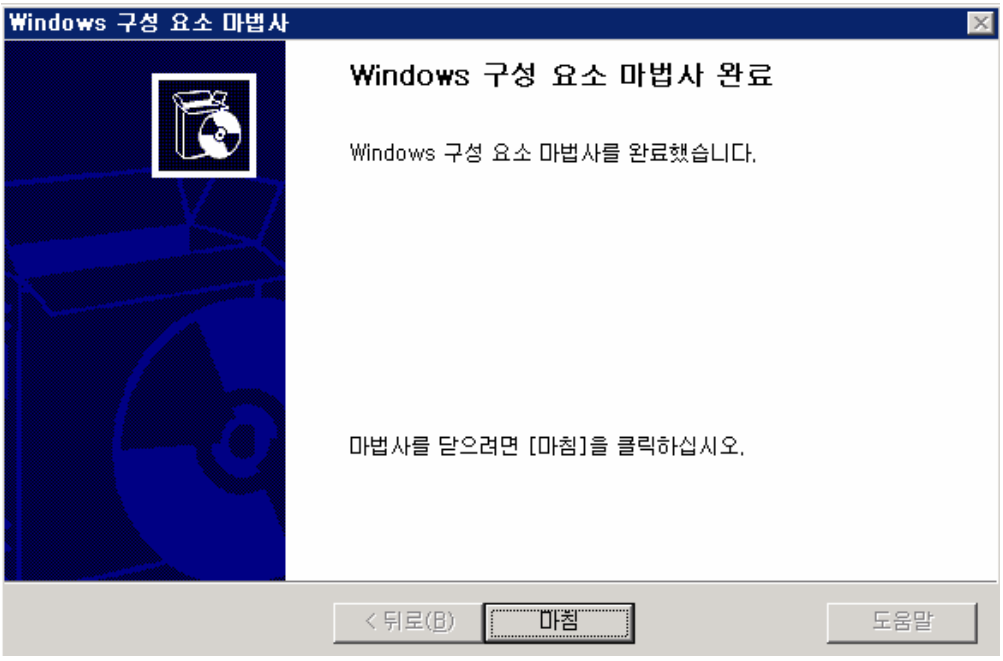
4) [DNS(도메인 이름 시스템)]를 선택 후 확인 버튼을 클릭합니다.



5) [네트워킹 서비스]의 체크 박스에 체크가 된 것을 확인 후 [다음] 버튼을 클릭합니다.

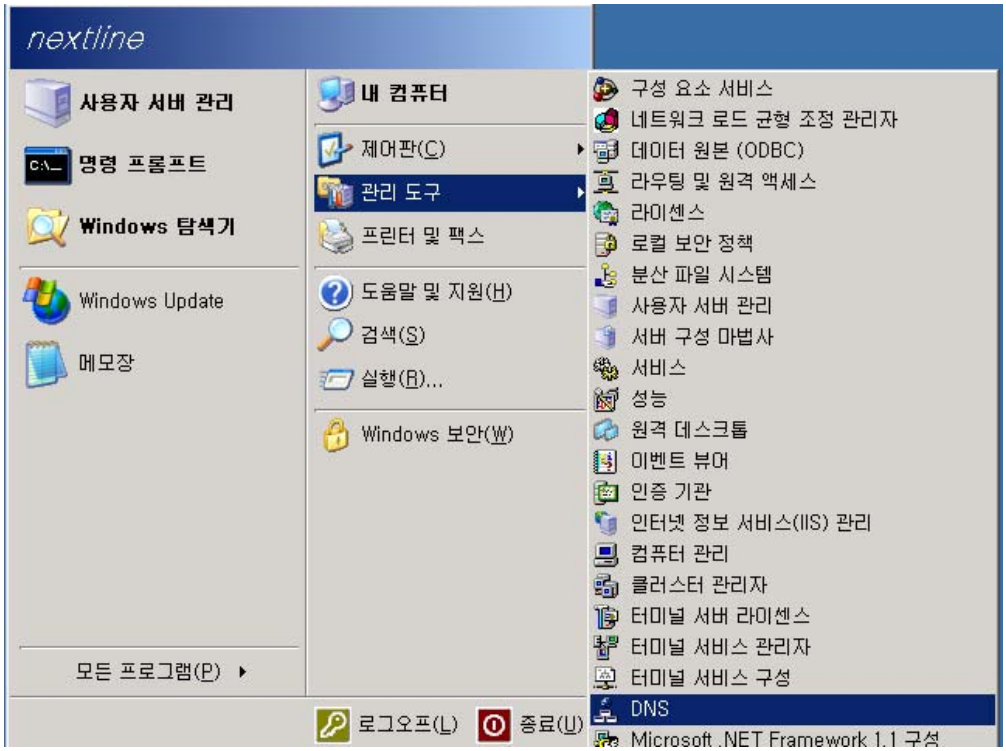


6) [DNS(도메인 이름 시스템)]의 설치가 완료 되었습니다.

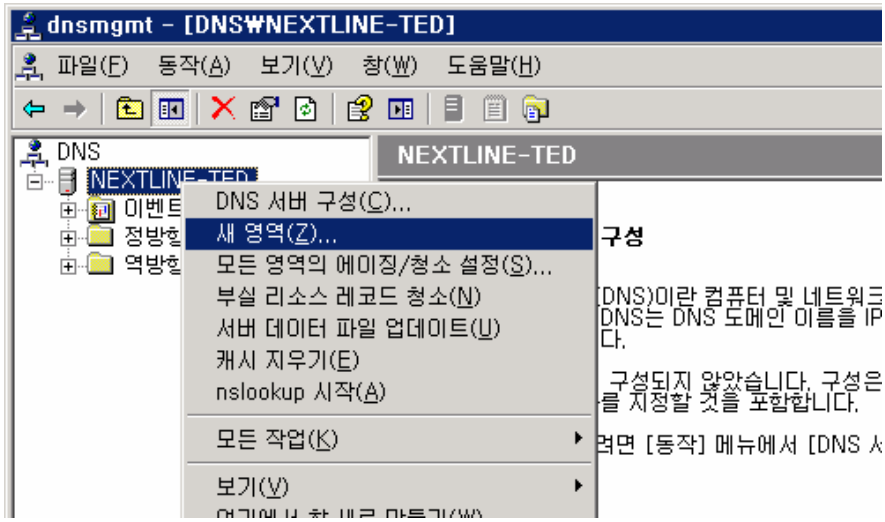


3. DNS(Domain Name System) 설정방법

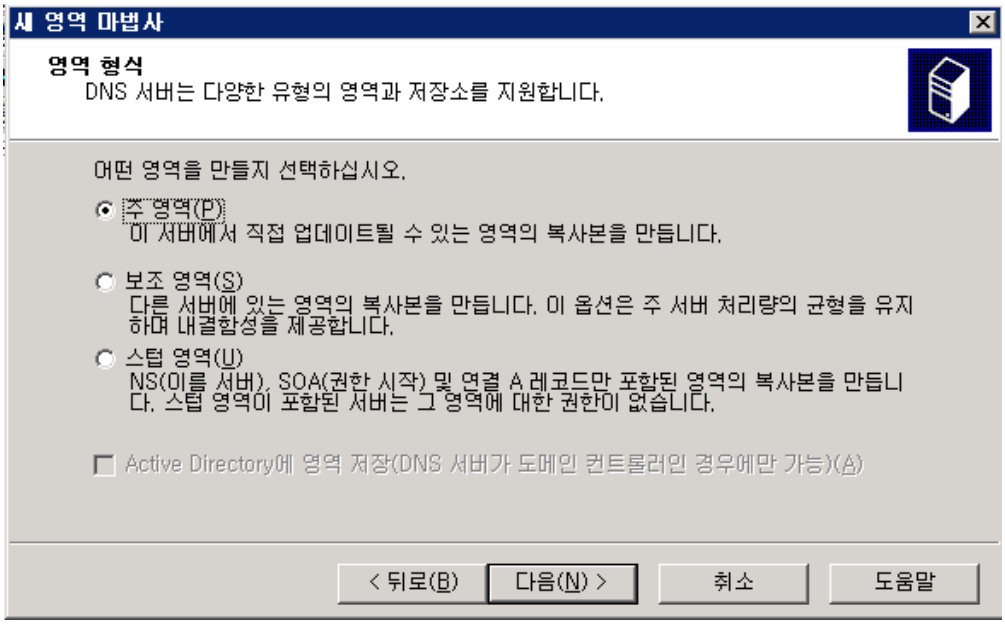
1) [시작]-[관리도구]-[DNS]를 선택합니다.



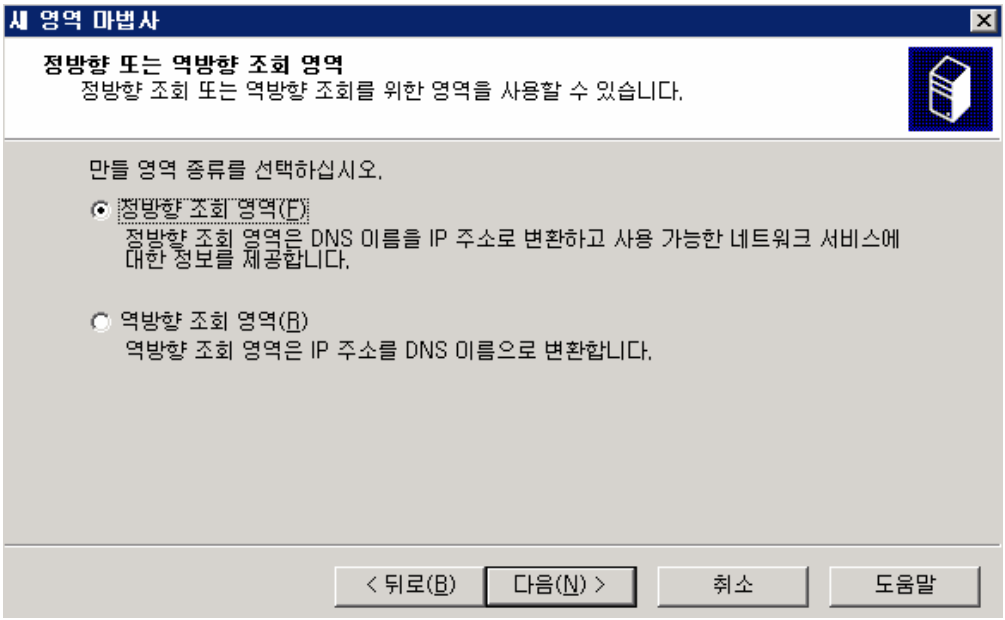
2) 컴퓨터명 선택 후 오른쪽 마우스 버튼을 클릭한 후[새 영역]을 선택합니다.



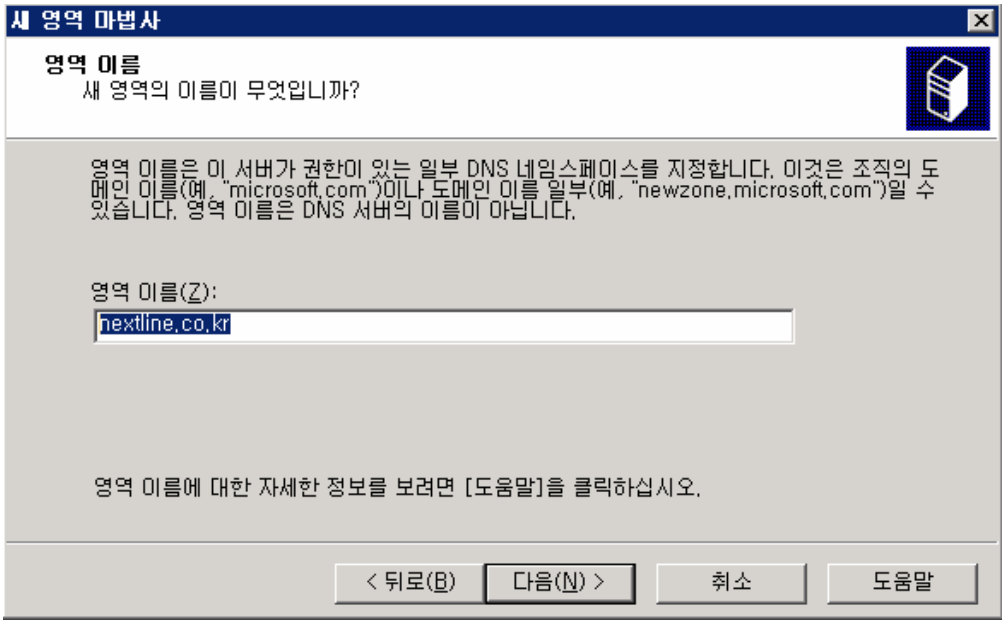
3) [주 영역]을 선택 후 [다음]버튼을 클릭합니다.



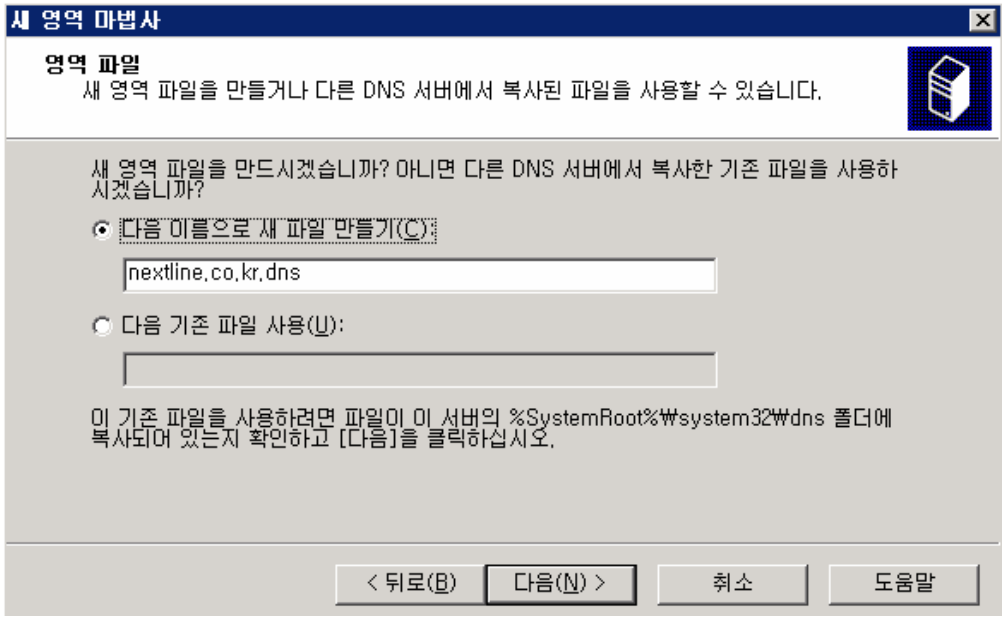
4) [정방향 조회 영역]을 선택 후 [다음]버튼을 클릭합니다.



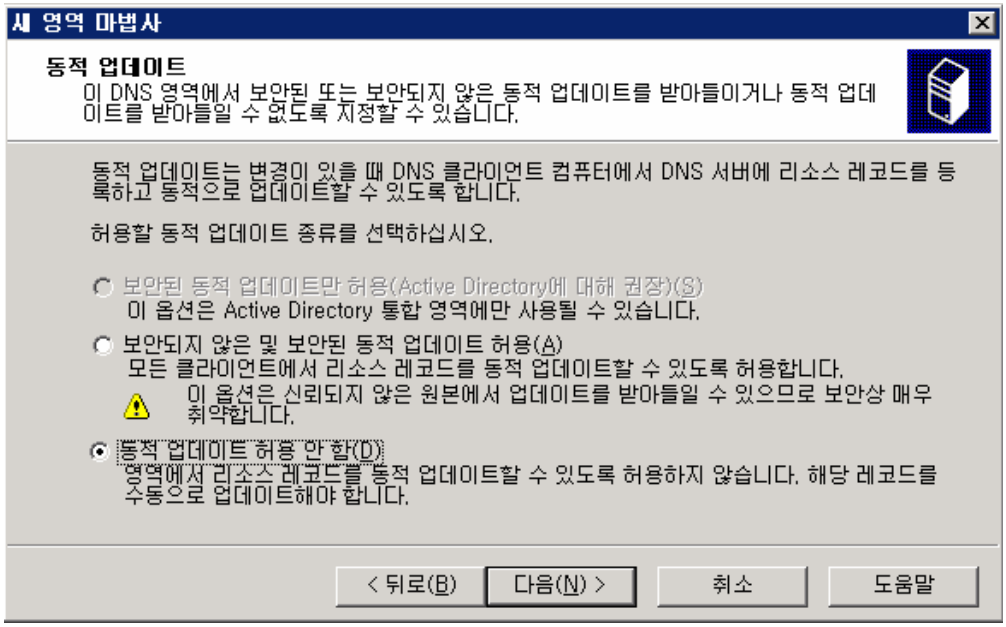
5) [영역이름]란에 설정할 도메인명을 입력한 후 [다음] 버튼을 클릭합니다.



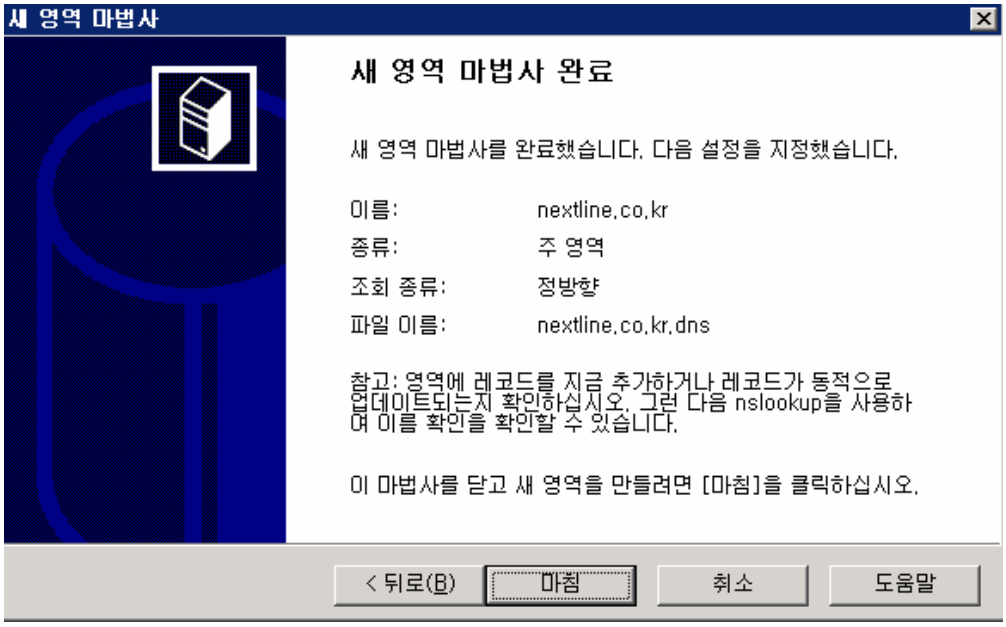
6) [다음 이름으로 새 파일 만들기]란에 설정 도메인을 확인 후 [다음]버튼을 클릭합니다.



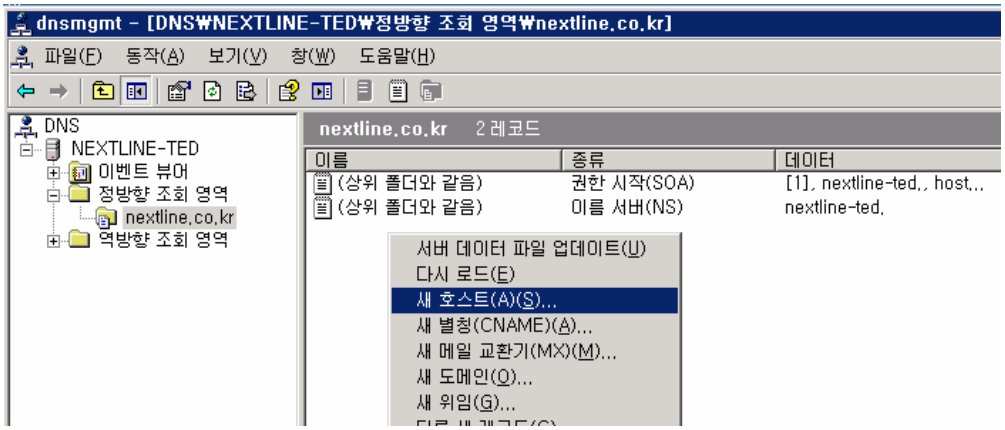
7) [동적 업데이트 허용 안함] 선택 후 [다음]버튼을 클릭합니다.



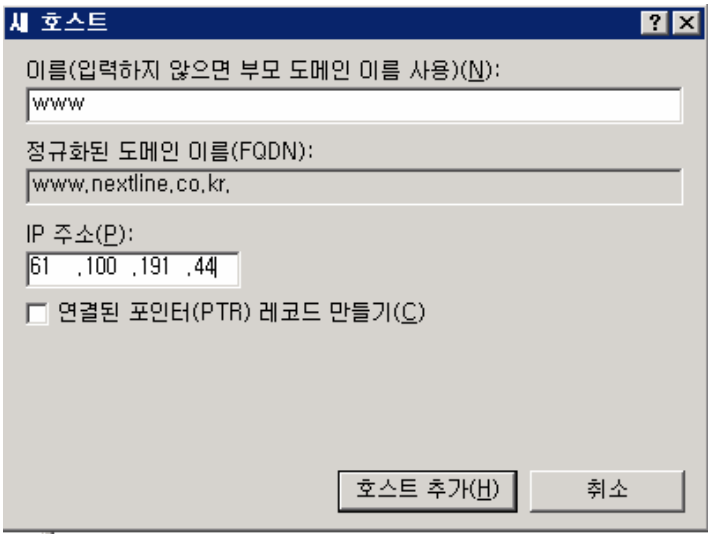
8) 새 영역 설정 마법사가 완료 확인 후 [마침]버튼을 클릭합니다.



9) [정방향 조회 영역]하위에 설정한 nextline.co.kr 도메인을 확인 후[새 호스트]/[메일 교환기]등을 등록합니다.



10) [새 호스트]추가 선택 후 [이름]항목에 호스트 입력 및 IP 주소 설정 후 [호스트 추가] 버튼 클릭 합니다.



11) NSLOOKUP을 통하여 설정한 정보를 확인 할 수 있습니다.

```
> ls -d nextline.co.kr

 nextline.co.kr.        SOA     nextline-ted admin. <12 900 600 86400
 nextline.co.kr.        A       61.100.191.44
 nextline.co.kr.        NS      nextline-ted
 nextline.co.kr.        MX      10      mail.nextline.co.kr
 www                    A       61.100.191.44
```

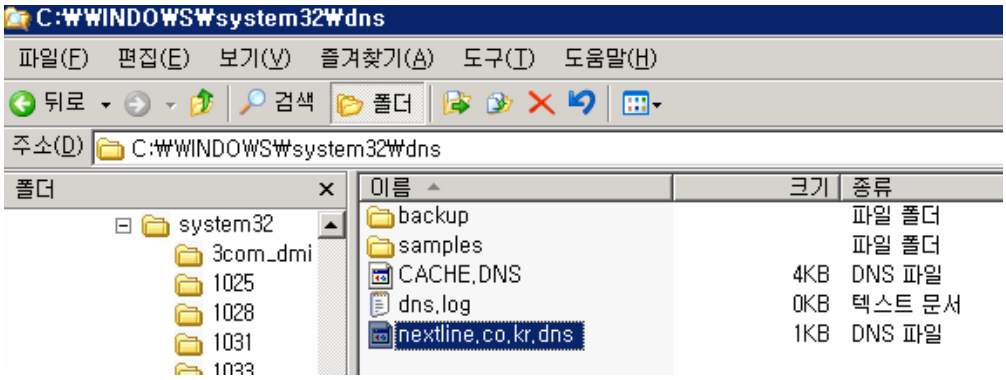
4. DNS 백업 및 복원

시스템을 운영하다 보면 재설치나 하드웨어 오류로 인하여 시스템을 복원해야 하는 경우가 생깁니다. 이럴 경우에 백업이 되어 있지 않는 경우라면 일일이 수동으로 모든 것을 설정하고 혹은 복원을 할 수 없는 경우도 발생합니다.

DNS 역시 1~2개의 도메인만 사용한다면 수동으로 재설정하는 것이 어렵지 않겠지만 수십 혹은 수백 개의 도메인을 운영한다면 일일이 하나씩 설정하는데 많은 시간이 소요될 것입니다. 여기서 간단한 방법으로 DNS를 백업/복원하는 방법에 대해서 안내해드리겠습니다.

1) DNS 백업하기

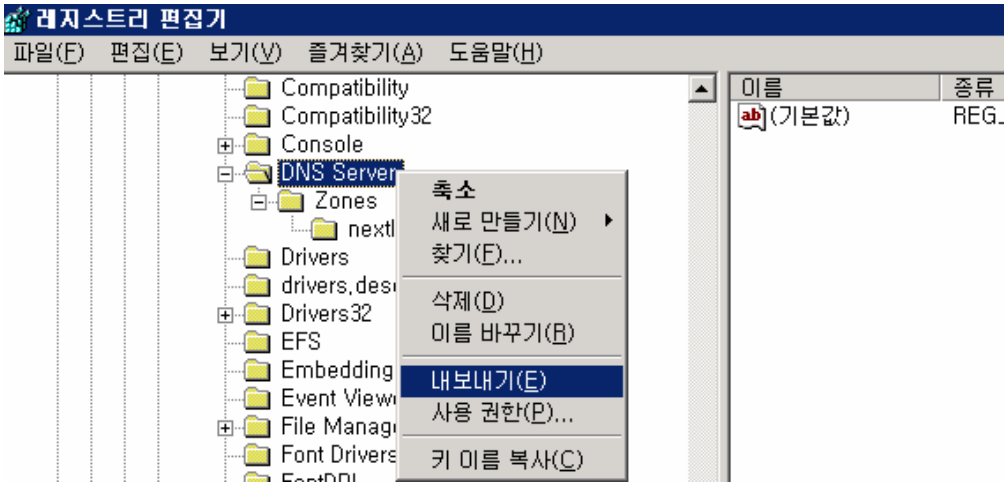
① 탐색기에서 %systemRoot%₩system32₩dns 디렉토리로 이동하면.dns 확장자를 가진 파일들이 보일 것입니다. 해당 파일들을 모두 백업받습니다.



② regedit를 실행하여 다음과 같은 경로로 이동합니다.

[시작]-[실행]-[regedit]- 내 컴퓨터₩HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩DNS Server

③ DNS Server에서 마우스 오른쪽 버튼을 클릭하여 [내보내기]를 선택하여 백업합니다. ([내보내기]하여 받은 파일은 .reg 파일로 받아집니다. Ex, dns.reg).



④ 이제 DNS에 필요한 파일은 모두 백업받았으니 안전한 곳으로 백업 파일을 이동합니다.

2) DNS 복원하기

① DNS 백업하기에서 백업받은 .dns 확장자를 가진 파일들을 %systemRoot%₩system32₩운 에 복사하여 붙여넣습니다.

② 백업받은 dns.reg 파일을 더블 클릭하여 레지스트리에 추가합니다.

③ [시작]-[관리도구]-[서비스]에서 DNS Server를 재 시작합니다.

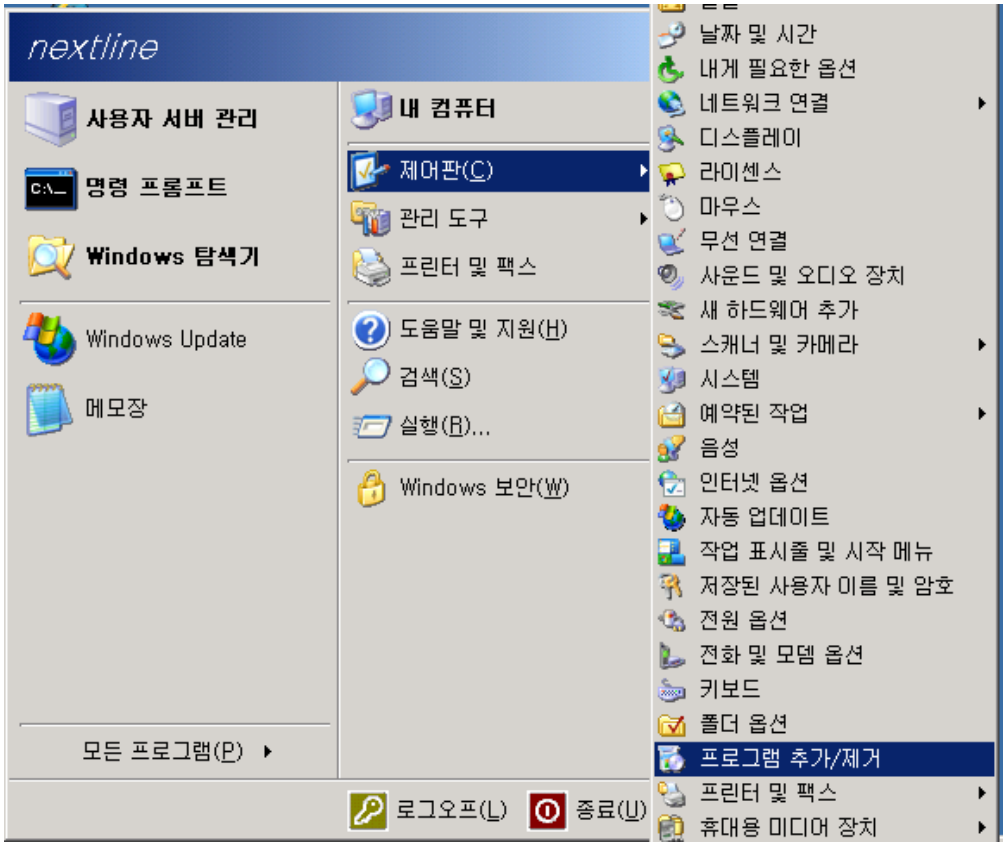
④ 복원이 모두 완료되었으므로 DNS 서비스를 확인해보시면 됩니다.

FTP 서버 구축 및 설정

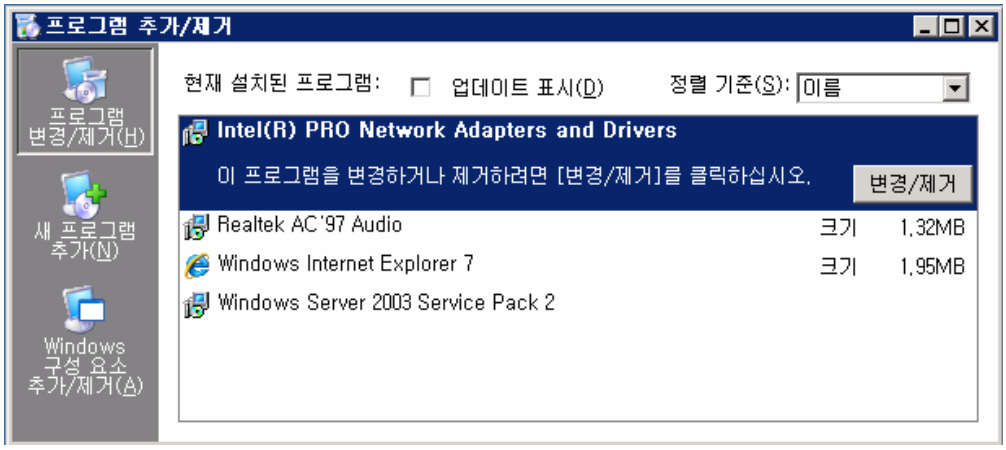
FTP(File Transfer Protocol)란 파일을 전송하는 프로토롤로 인터넷을 통하여 파일을 송, 수신할 수 있도록 지원하는 통신 규약입니다.

1. FTP 서버 설치하기

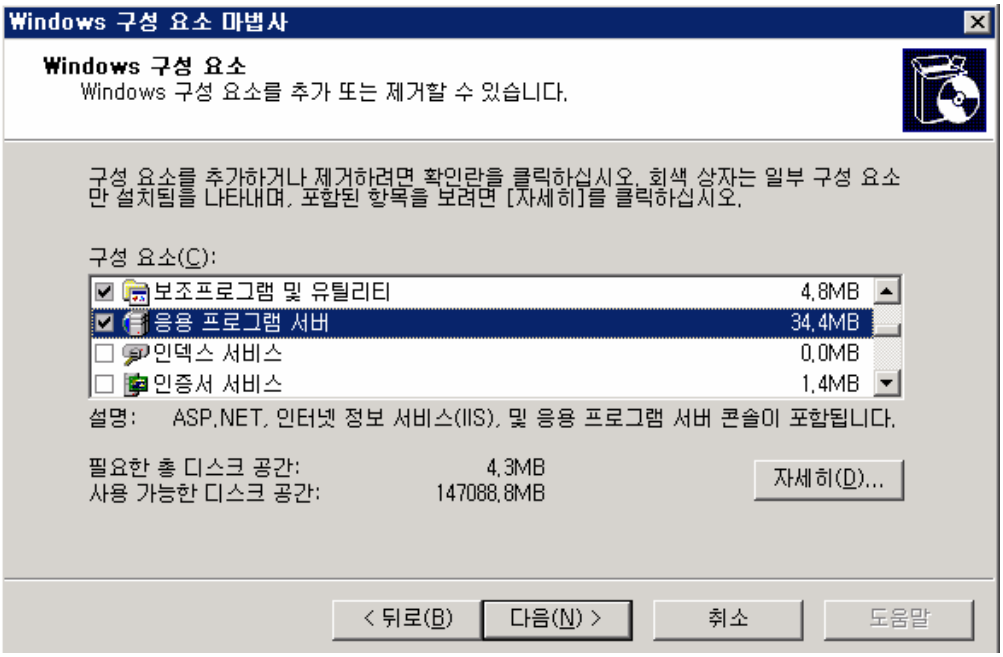
1) [시작]-[제어판]-[프로그램 추가/제거] 클릭 합니다.



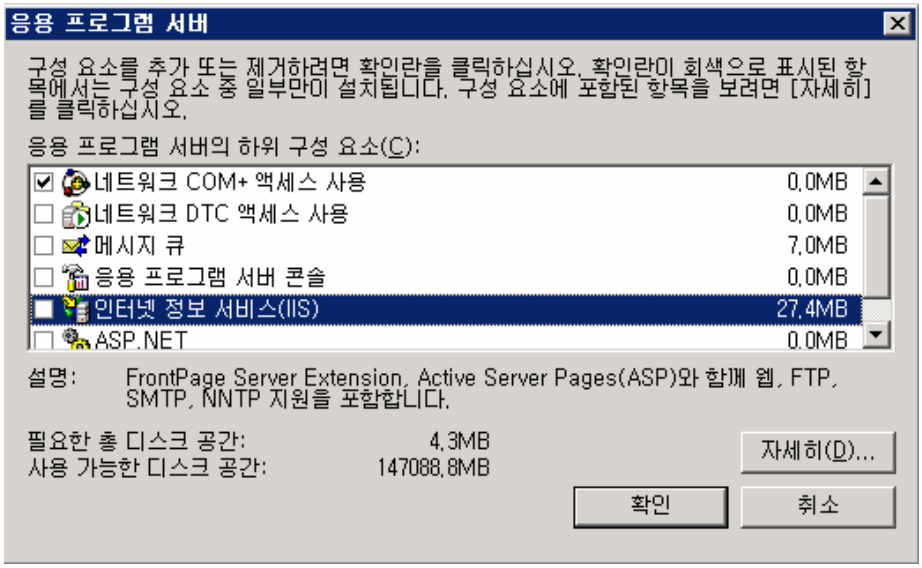
2) [Windows 구성 요소 추가/제거]를 클릭합니다.



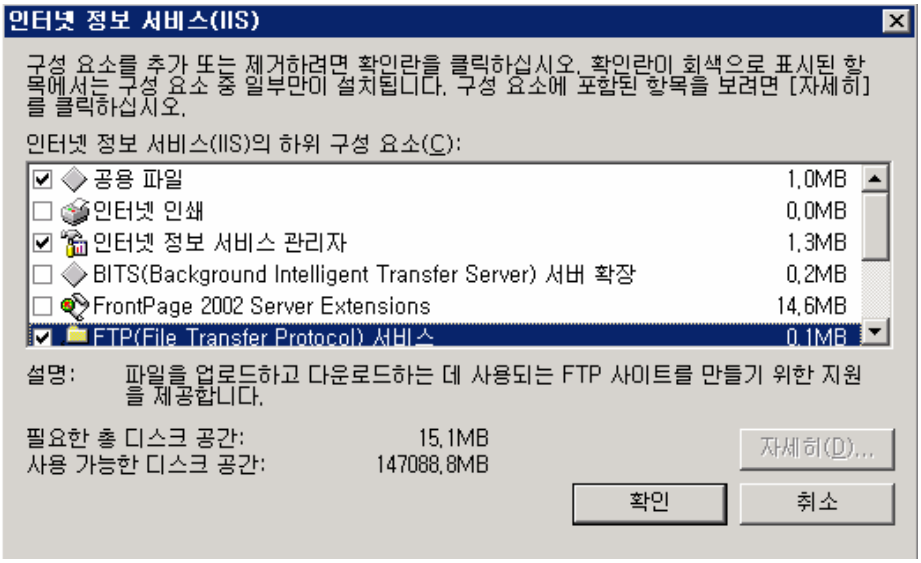
3) 구성 요소 목록에서 [응용 프로그램 서버] 를 클릭하고 [자세히]를 클릭합니다.

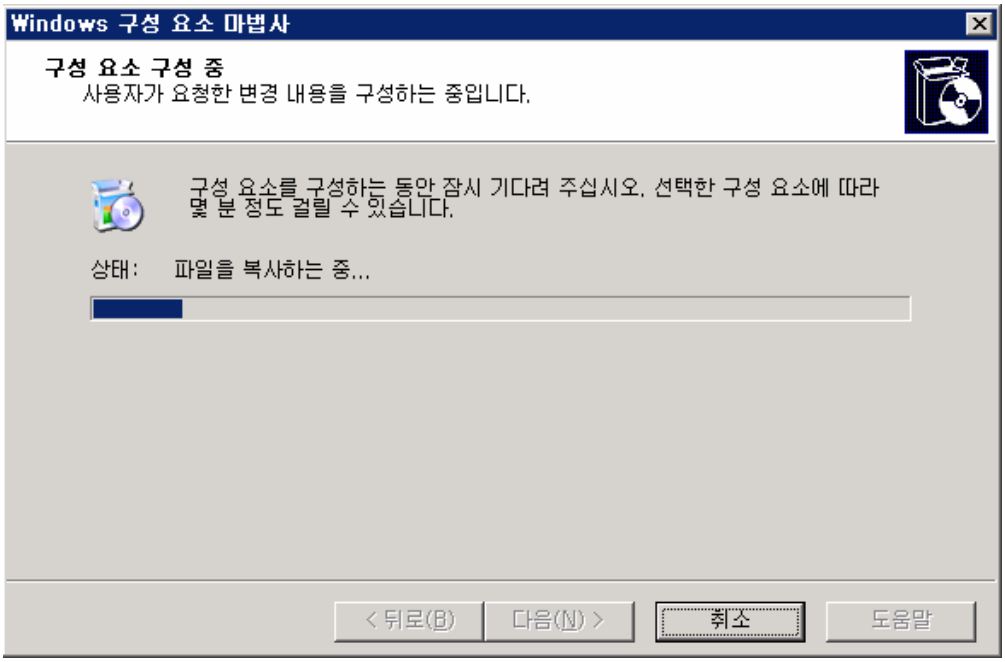


4) [인터넷 정보 서비스(IIS)] 를 클릭한 후 [자세히]를 클릭합니다.

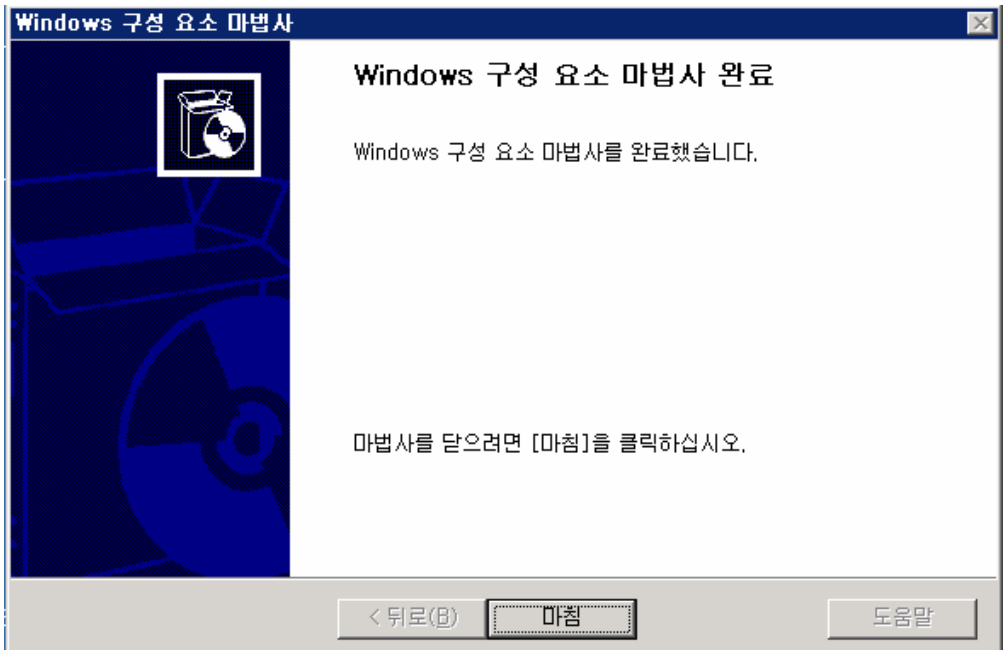


5) [FTP(File Transfer Protocol) 서비스] 를 클릭하면 설치가 진행됩니다.



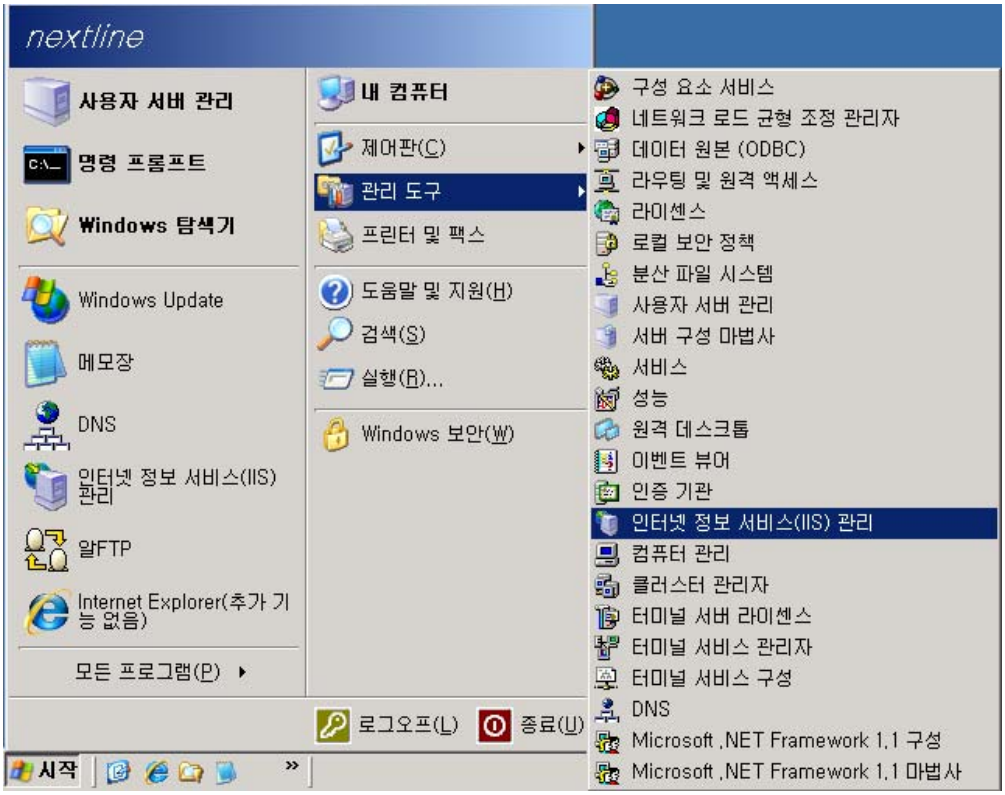


6) 설치 완료된 화면 입니다.

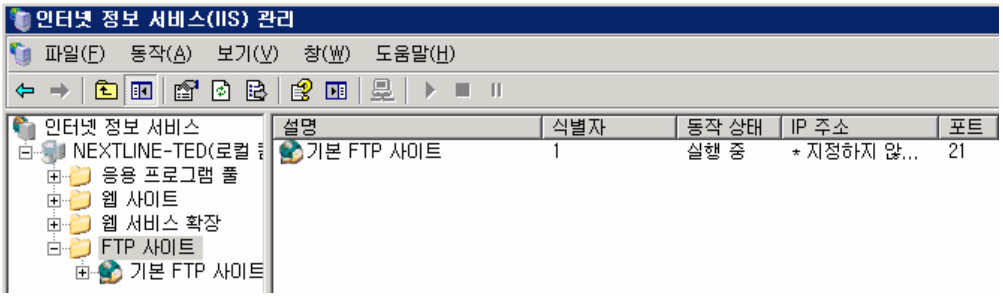


2. FTP 서비스 확인하기

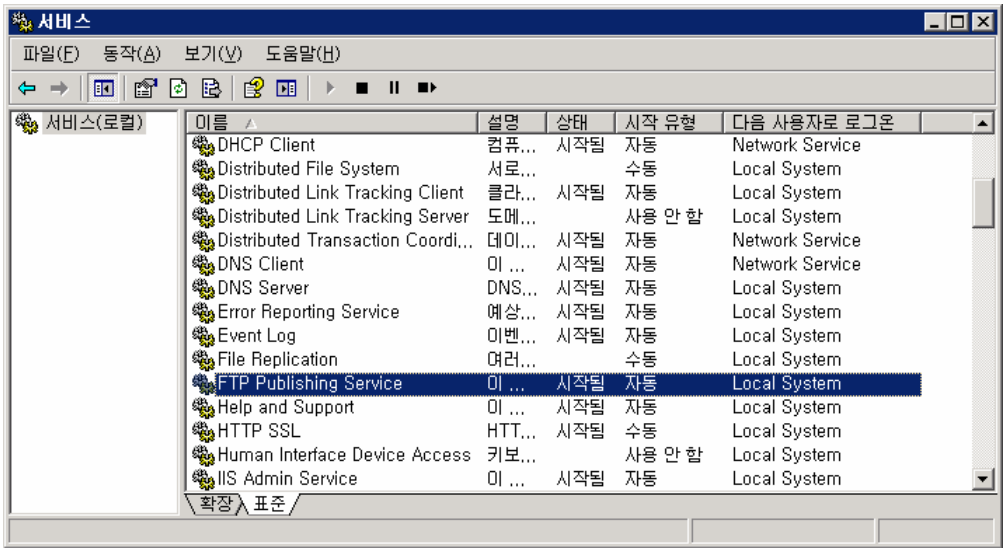
1) [시작]-[관리도구]-[인터넷 정보 서비스(IIS) 관리]를 클릭합니다.



2) [FTP 사이트]를 클릭합니다.

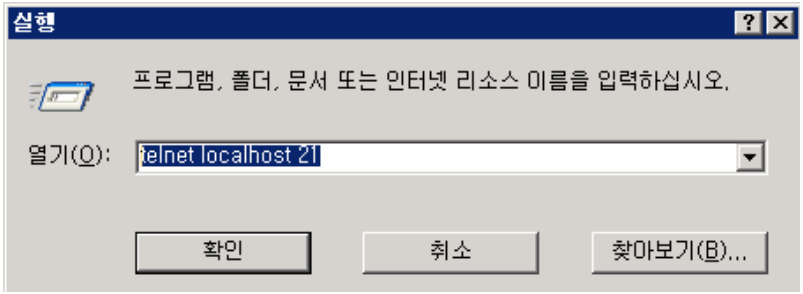


3) [시작]-[관리 도구]-[서비스] 에서 [FTP Publishing Service]가 [시작 유형] 이 [자동], [상태]가 [시작됨]인지 확인합니다.

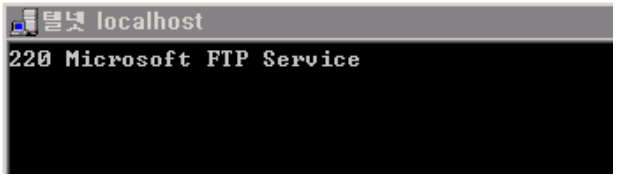


4) 기본 FTP 서비스가 실행되고 있는 서버에서 Telnet을 이용하여 확인합니다.

[시작]-[실행] 에서 "telnet localhost 21" 을 입력합니다.

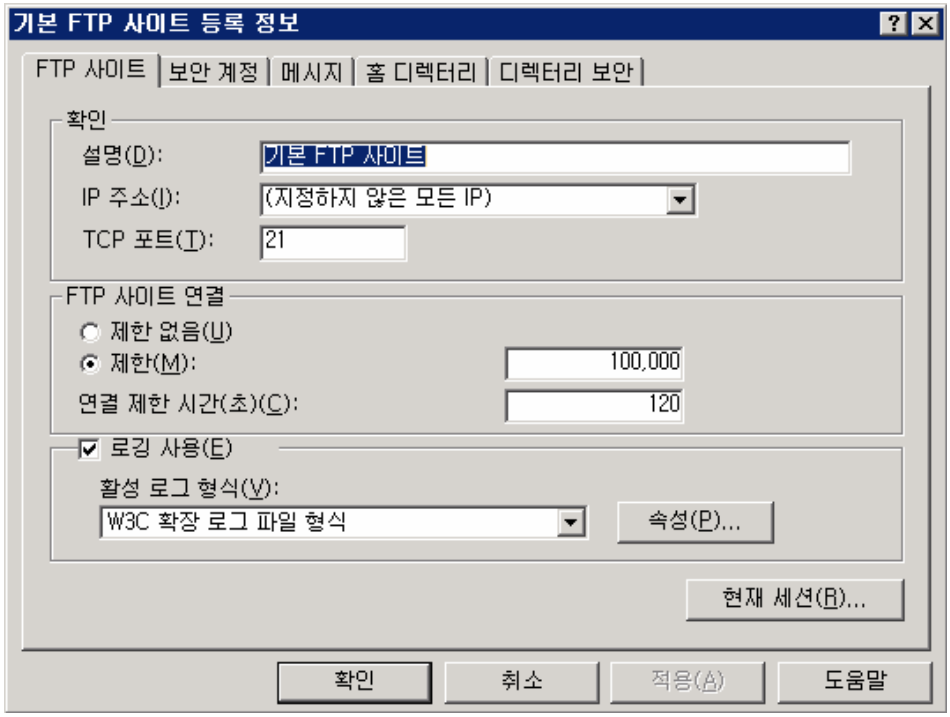


5) FTP 서비스가 정상적으로 설정되어 있음을 확인할 수 있습니다.



3. FTP 사이트 구성

1) FTP 사이트



• 설명 : 인지하기 쉽도록 원하는 대로 지정할 수 있습니다.

• IP 주소 : 이 사이트에 접속할 수 있는 IP 주소를 지정합니다. 지정하지 않은 모든 IP를 선택하면 이 컴퓨터가 가지고 있는 모든 IP 주소로 접속할 수 있습니다.

• TCP 포트 : FTP 서버의 포트를 결정합니다. 기본적으로 21번을 사용합니다.

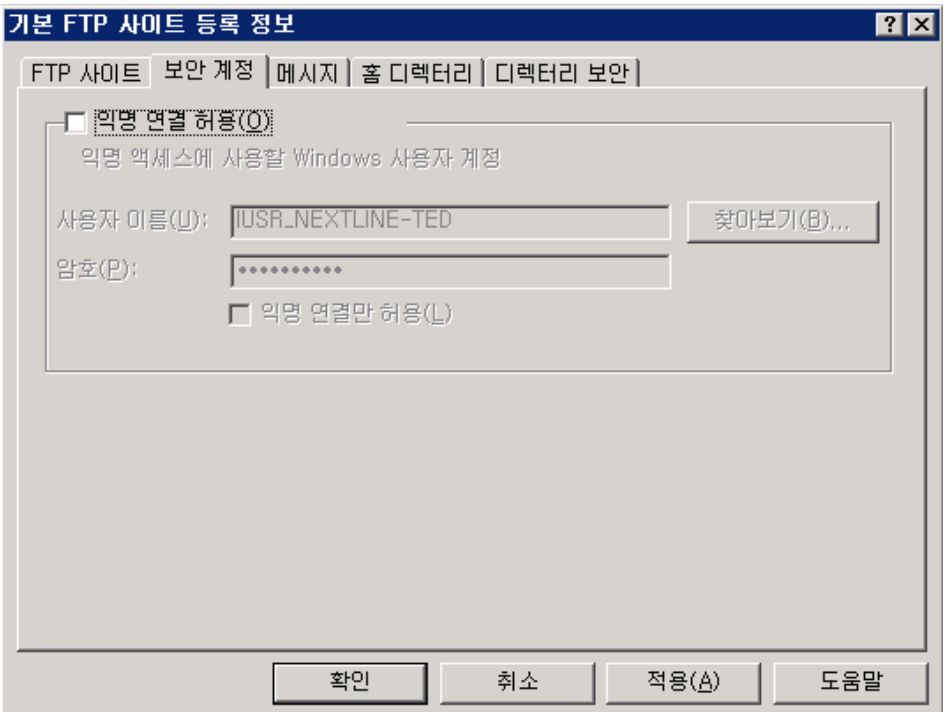
• FTP 사이트 연결 : '제한 없음' 또는 '제한' 을 선택할 수 있으며, '제한' 을 선택할 경우, 서버에 대한 동시 연결 수를 선택할 수 있습니다.

• 연결 제한 시간 : 서버가 비활성 사용자의 연결을 끊을 때까지 시간을 설정할 수 있습니다.

• 로깅 사용: FTP 사이트의 로그를 남기려면 이 옵션을 선택합니다. '속성' 을 통하여 좀 더 상세한 로그를 만들 수 있습니다.

• 현재 세션 : 사이트에 현재 연결된 사용자의 목록을 표시합니다.

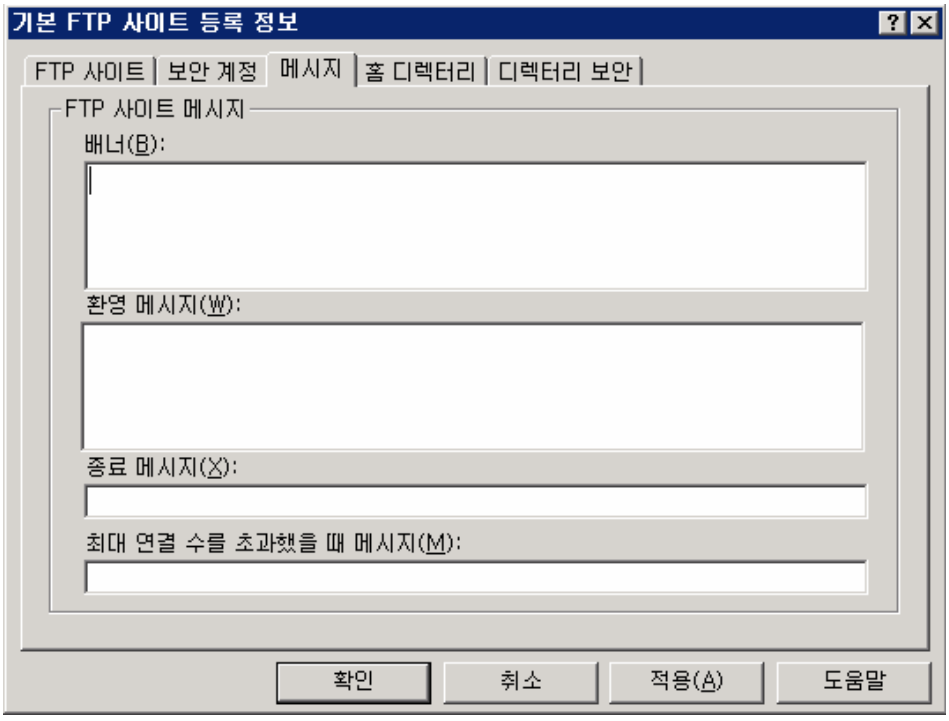
2) 보안 계정



보안상 “익명 연결 허용”은 체크를 하지 않음을 권장합니다. FTP 접속 사용자를 생성하여 접속하는 것을 권장합니다.

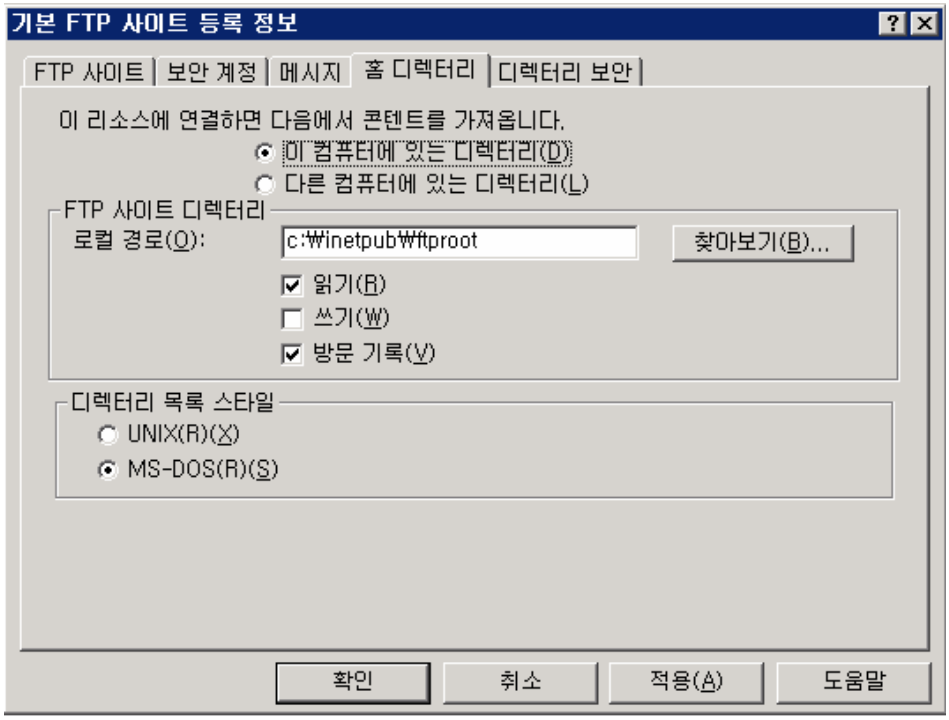
3) 메시지

사용자들이 접속했을 경우나 연결을 끊었을 경우에 출력하는 메시지를 관리할 수 있습니다.



4) 홈 디렉터리

FTP에 접속하였을 경우, 홈 디렉터리와 해당 디렉터리의 권한을 설정할 수 있습니다.



• FTP 사이트 디렉터리 : 로컬 디렉터리의 경우 전체 경로를 입력하고, 네트워크 공유의 경우 UNC(Universal Naming Convention)서버 및 공유 이름을 사용합니다.

• 읽기 : 사용자가 홈 디렉터리나 가상 디렉터리에 저장된 파일을 읽거나 다운로드 할 수 있습니다.

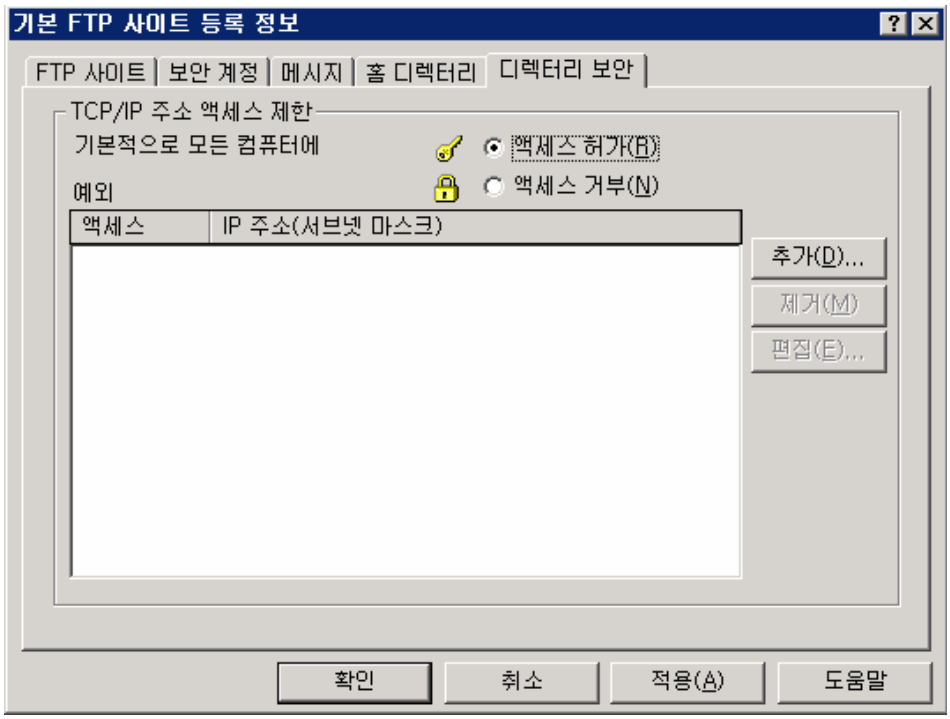
• 쓰기 : 사용자가 해당 서버에 허용된 디렉터리에 파일을 업로드 및 삭제할 수 있습니다.

• 방문 기록 : 이 디렉터리에 방문한 내역을 로그 파일에 기록합니다.

• 디렉터리 목록 스타일 : UNIX/MS-DOS 디렉터리 형식으로 FTP 사용자에게 보낼 디렉터리 목록 스타일을 변경합니다.

5)디렉터리 보안

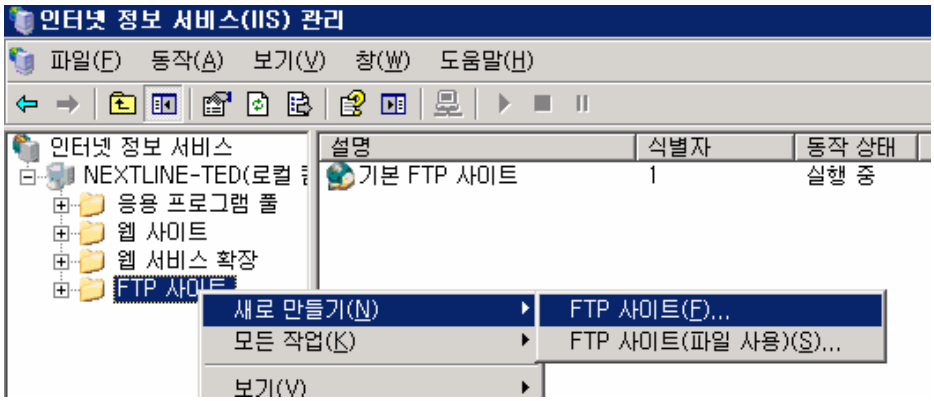
특정 컴퓨터나 그룹이 FTP 사이트에 접근하는 것을 거부 또는 엑세스하는 것을 허용하여 사용할 수 있습니다.



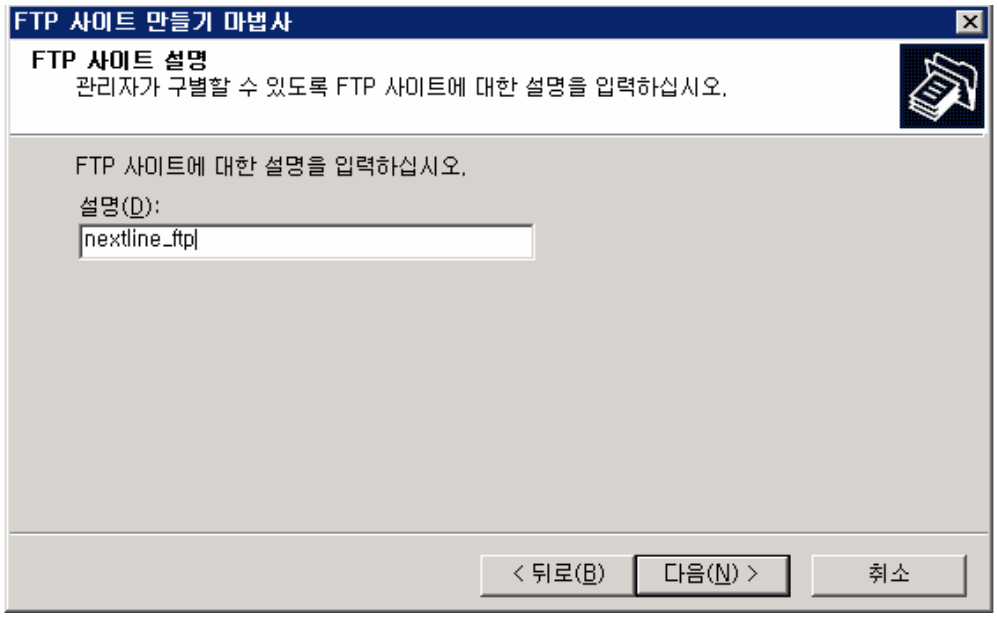
4. FTP 사이트 만들기

1) 기본 FTP 사이트를 중지한 후, 새로운 FTP 사이트 만들기를 합니다.

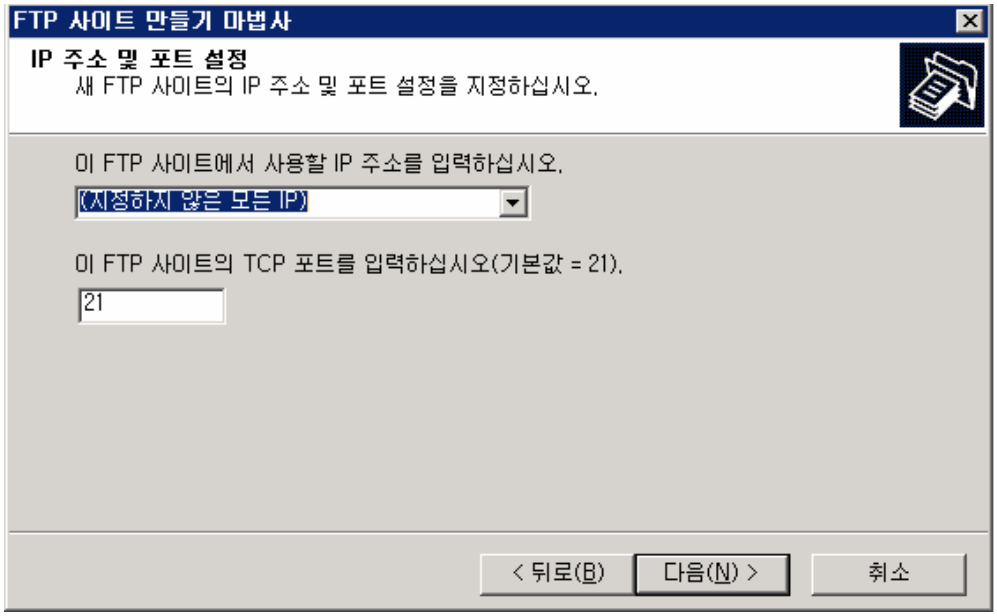
2) 로컬 컴퓨터에서 [FTP 사이트]폴더를 선택한 후 마우스 오른쪽 버튼을 클릭하여[새로 만들기]를 선택하고, [FTP 사이트]를 실행합니다.



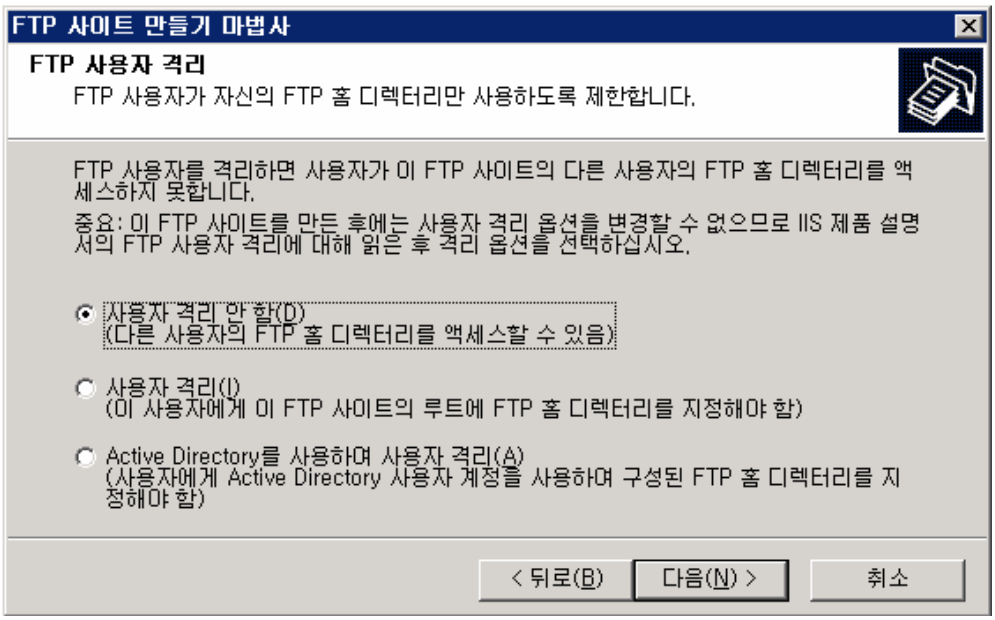
3) FTP 사이트 설명을 입력한 후, [다음]을 선택 합니다, FTP 사이트를 참조할 때 사용할 이름을 지정하는 것입니다.



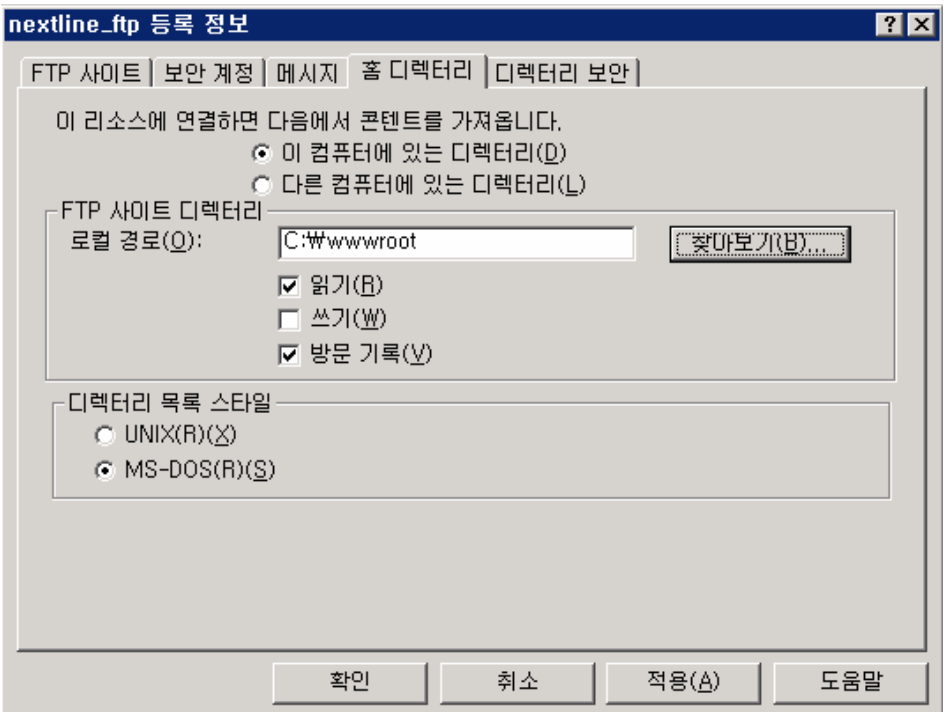
4) IP 주소 및 포트를 입력한 후 [다음]을 선택합니다. FTP 사이트를 사용하지만 기본값 포트 21번을 사용하지 않고 변경해서 사용할 수 있습니다.



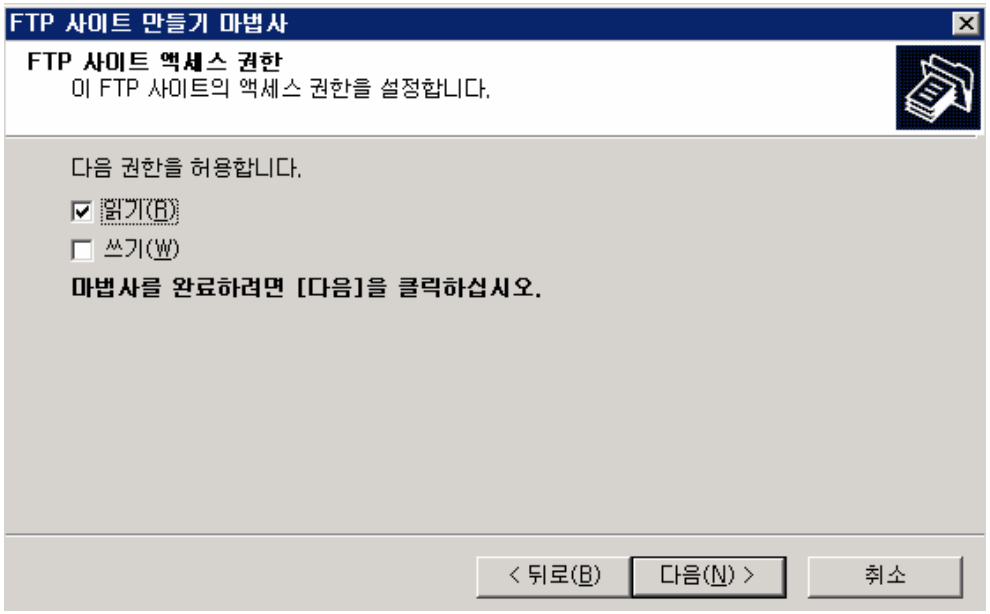
5) FTP 사용자 격리 여부를 선택한 후 [다음]을 클릭합니다. “사용자 격리 안 함” 을 선택하여 FTP 사이트를 생성합니다.



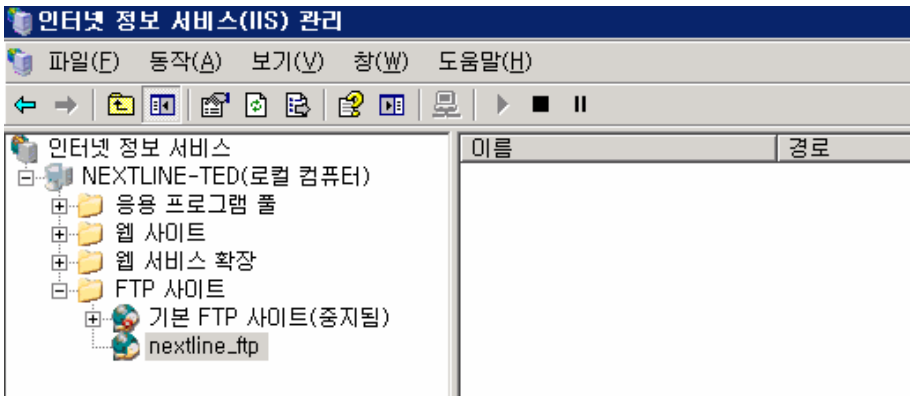
6) 사이트의 홈 디렉터리 경로 지정한 후 다음을 선택합니다. FTP 사용자가 서버에 연결되면 시스템의 홈 디렉터리에 위치하게 되어 사용자의 자체 루트 디렉터리가 됩니다.
홈 디렉터리 경로는 하드 디스크에 이미 존재하는 경로이어야 합니다. 만약 하드 디스크에 존재하지 않는 경로를 입력하면 '경로가 없거나 디렉터리가 아닙니다.' 라는 메시지를 출력하게 됩니다.



7) 기본적으로 FTP 사이트 엑세스 권한은 '읽기' 만 설정되어 있습니다. '쓰기' 권한을 주지 않으면 파일을 업로드 할 수 없습니다.

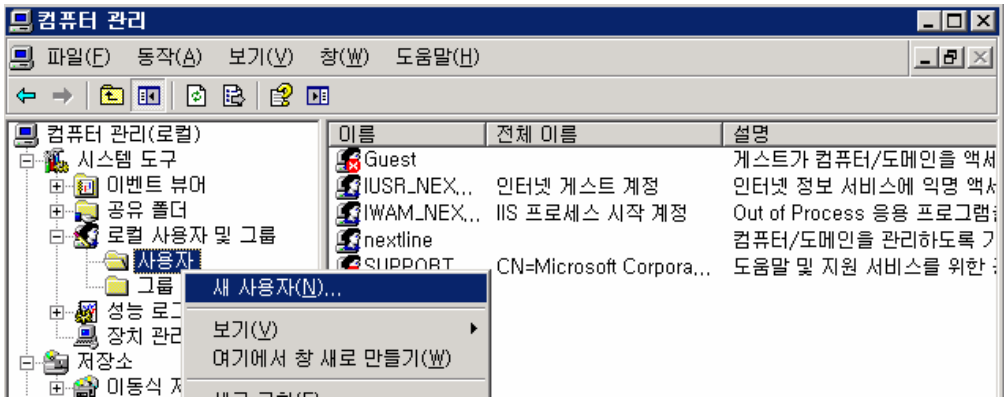


8) nextline_ftp 사이트가 생성된 것을 확인할 수 있습니다.

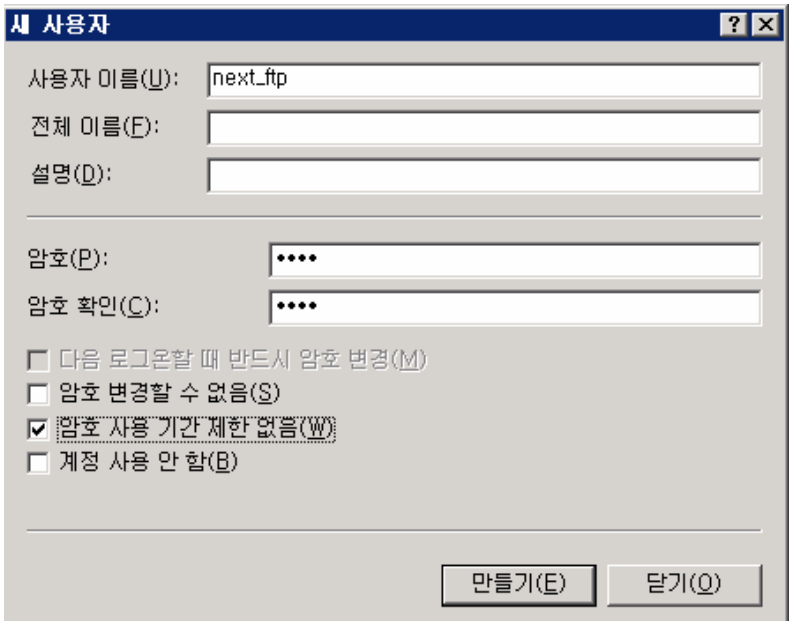


9) nextline_ftp 접속할 사용자 next_ftp를 생성하겠습니다.

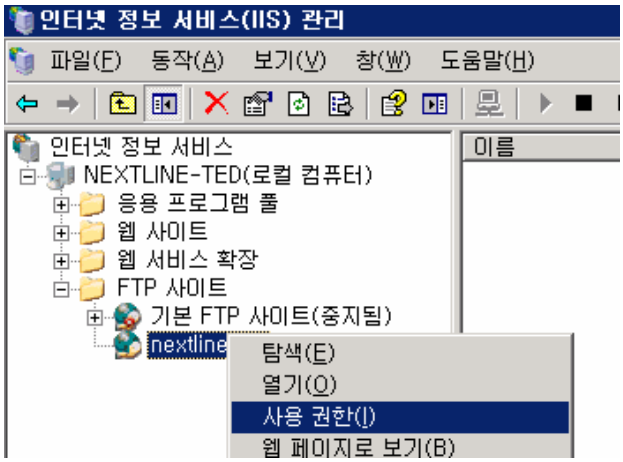
[로컬 사용자 및 그룹]-[사용자]-[새 사용자]를 선택합니다.



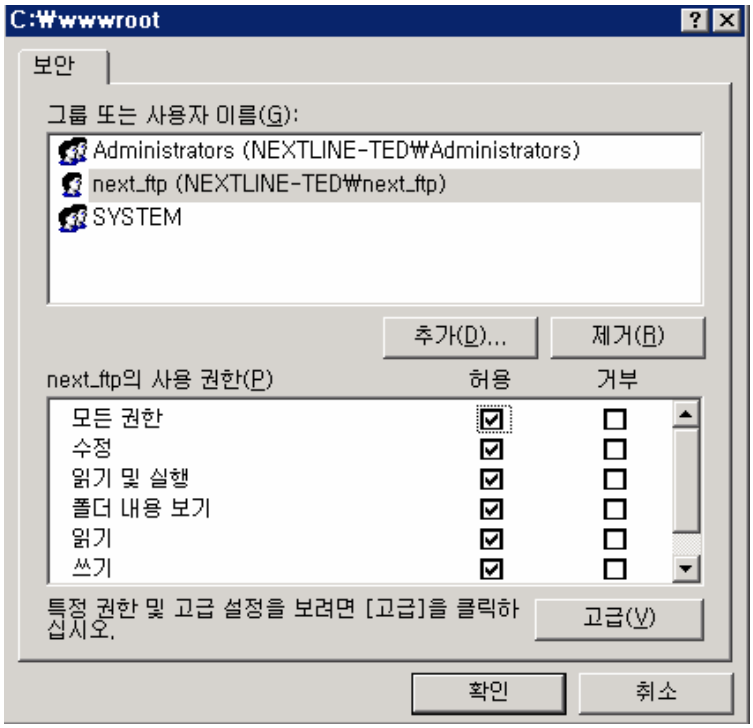
10) [사용자 이름]에 “next_ftp” 아이디를 입력합니다., [암호] 입력 후 [암호 사용 기간 제한 없음]에 체크를 한 후, [만들기]를 클릭합니다.



11) next_ftp 사이트에 마우스 오른쪽 버튼을 클릭하여 [사용 권한]을 실행합니다.

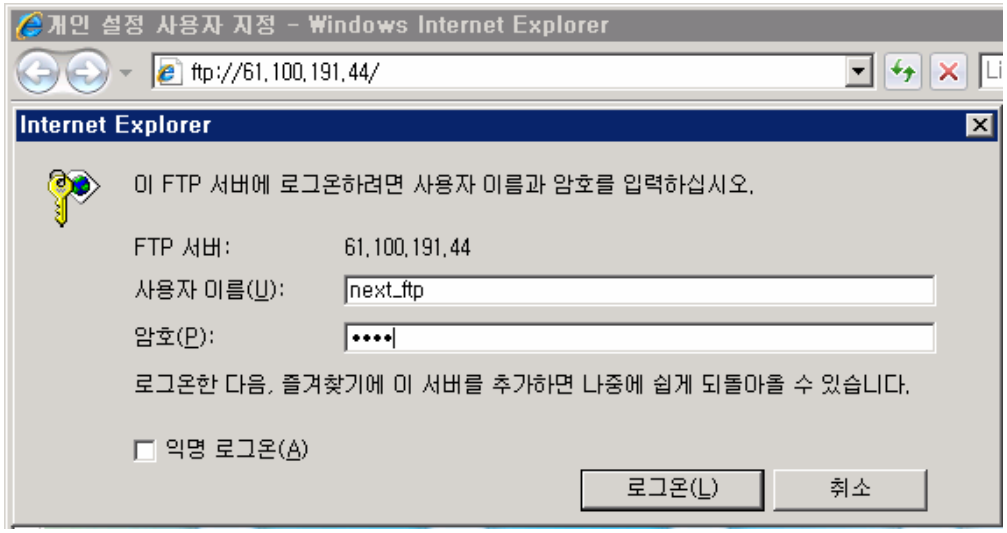


12) next_ftp 사이트 홈 디렉터리 접근할 수 있는 사용자는 next_ftp 입니다. 사용자를 추가한 후, 권한 설정을 합니다.



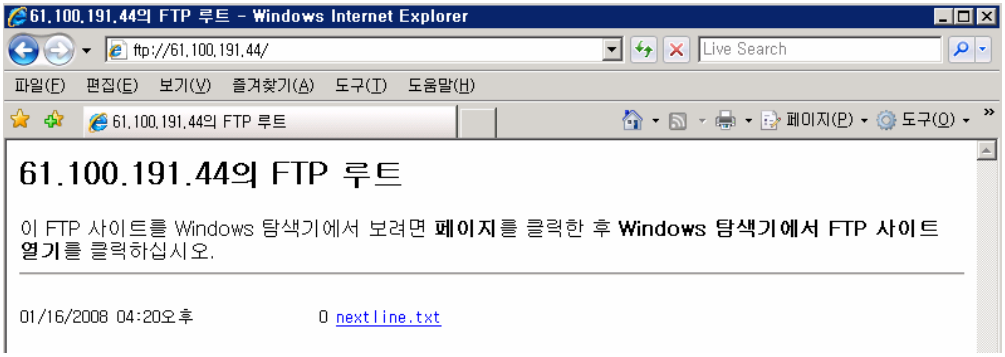
13) 익스플로러를 사용하여 next_ftp 에 접속하기 위해 익스플로러를 실행합니다. 익스플로러 주소창에 “ftp://IP 주소 또는 도메인” 을 입력합니다

ftp 사이트를 개별 포트 21로 설정했을 경우 접속 주소에 포트를 입력하지 않아도 됩니다. 하지만 개별 포트 21이 아닌 다른 포트로 사용 시에는 접속 수조에 “ftp://IP 주소:포트” 를 입력합니다.



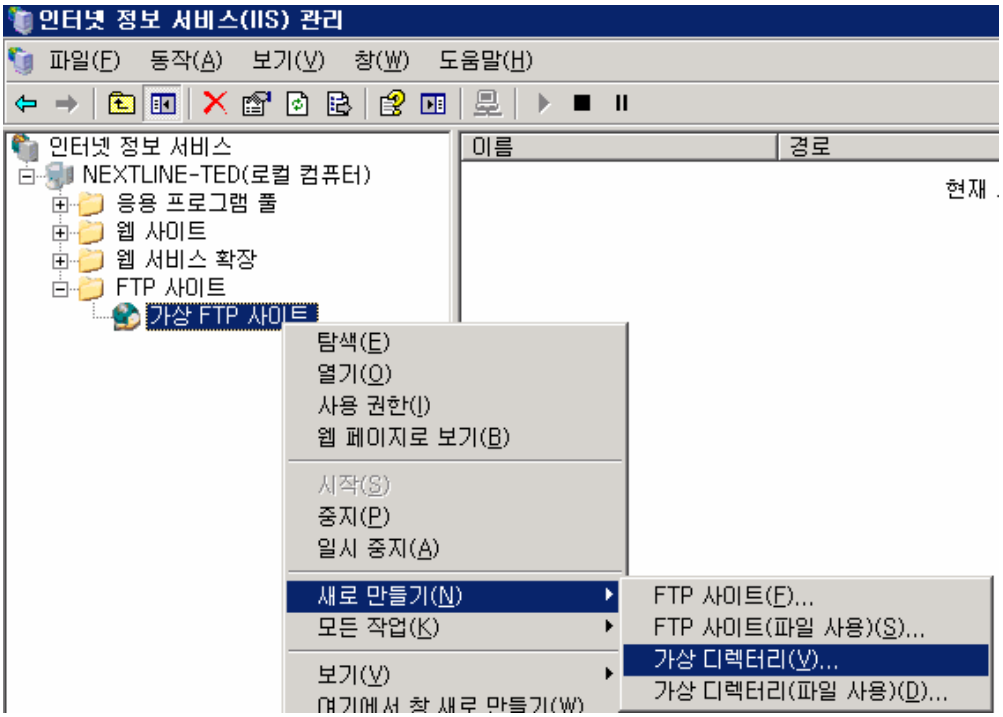
위와 같은 로그인 창에 사용자 “next_ftp” 와 설정한 암호를 입력합니다.

Next_ftp 접속을 완료하였습니다. Nextline_ftp 사이트의 데이터 파일을 확인할 수 있습니다. 파일을 업로드 및 다운로드 할 수 있습니다.

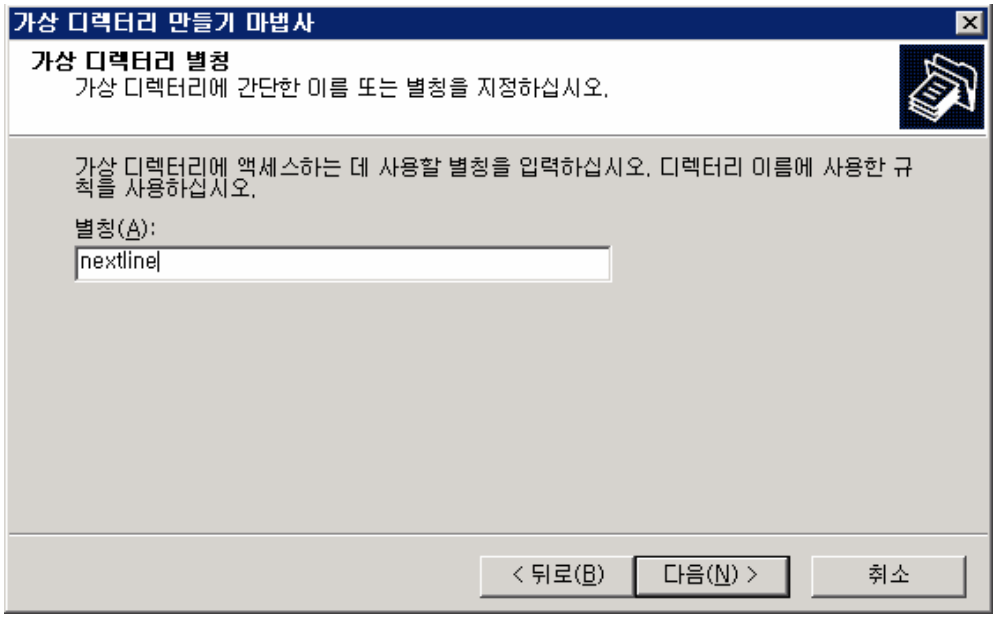


5. 가상 FTP 구성하기

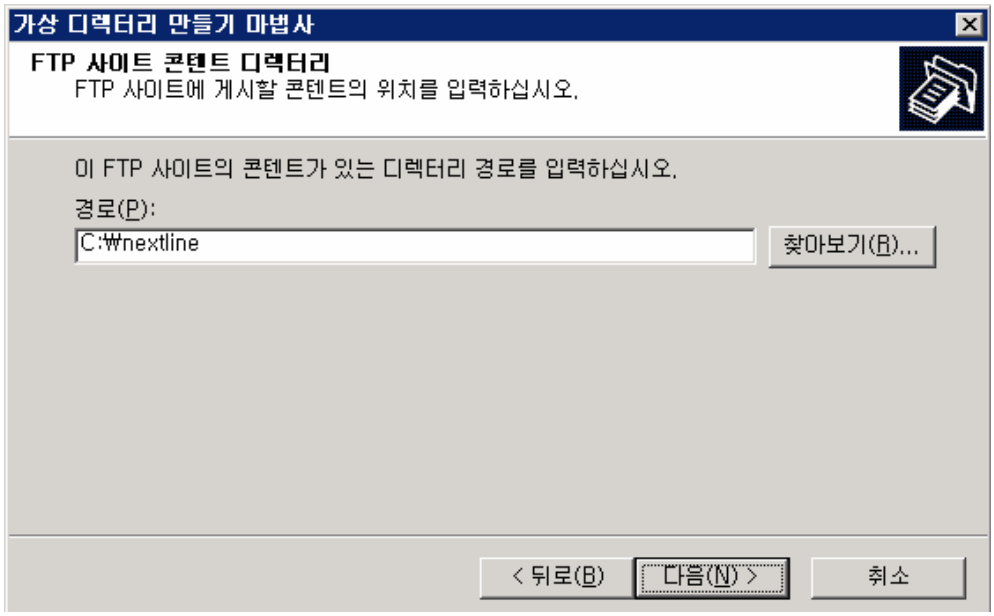
1) 해당 [가상 FTP 사이트] 하위 디렉터리에 가상 디렉터리 만들기를 합니다.



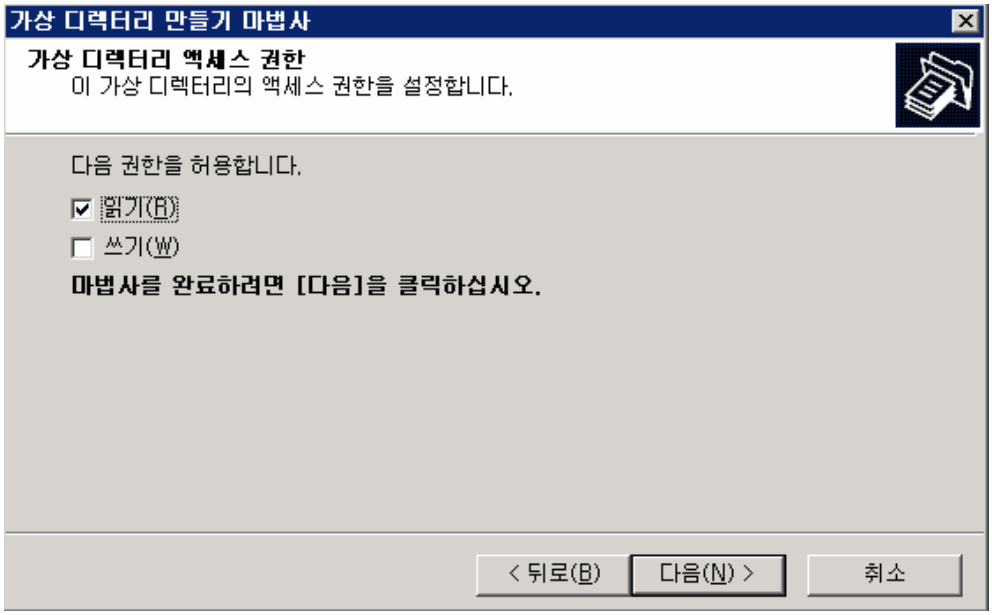
2) 별칭은 FTP 사용자가 디렉터리에 접근하기 위해서 사용하는 디렉터리 이름입니다. 별칭과 접속 사용자는 동일해야 합니다. "nextline" 이라는 별칭을 사용하도록 하겠습니다. 다음을 클릭합니다.



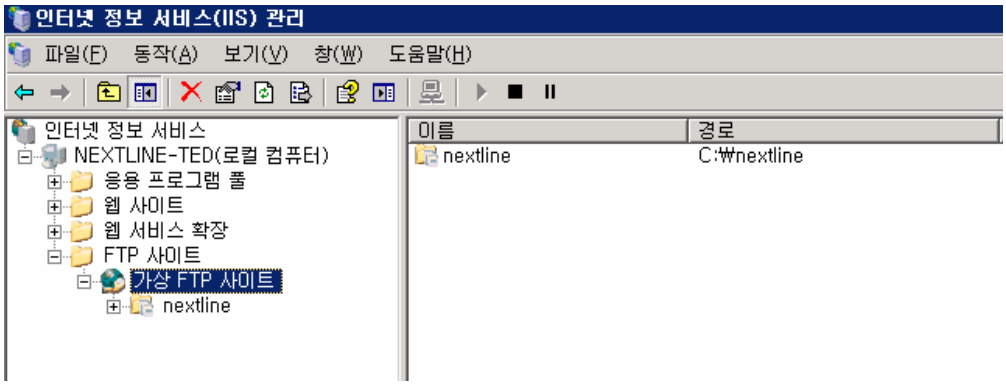
3) FTP 사이트의 디렉터리 경로를 지정합니다. 별칭과 파일이 위치한 디렉터리 이름이 일치할 필요는 없습니다.



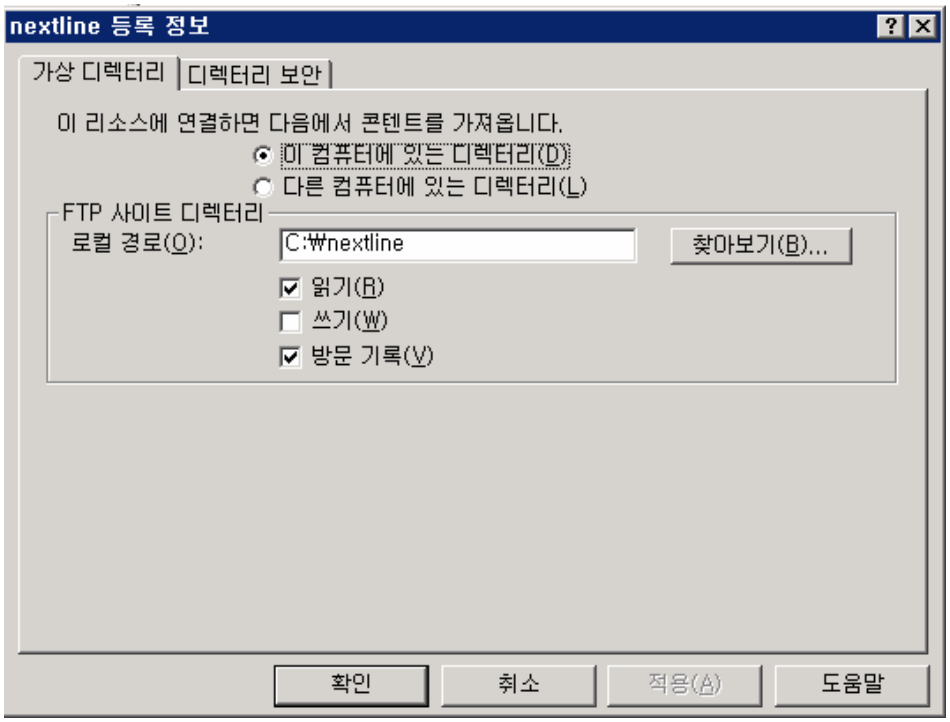
4) FTP 사이트 만들기에서 내용과 동일합니다. 읽기 또는 쓰기 권한을 설정합니다.



5) nextline 별칭의 가상 디렉터리가 생성되었습니다.

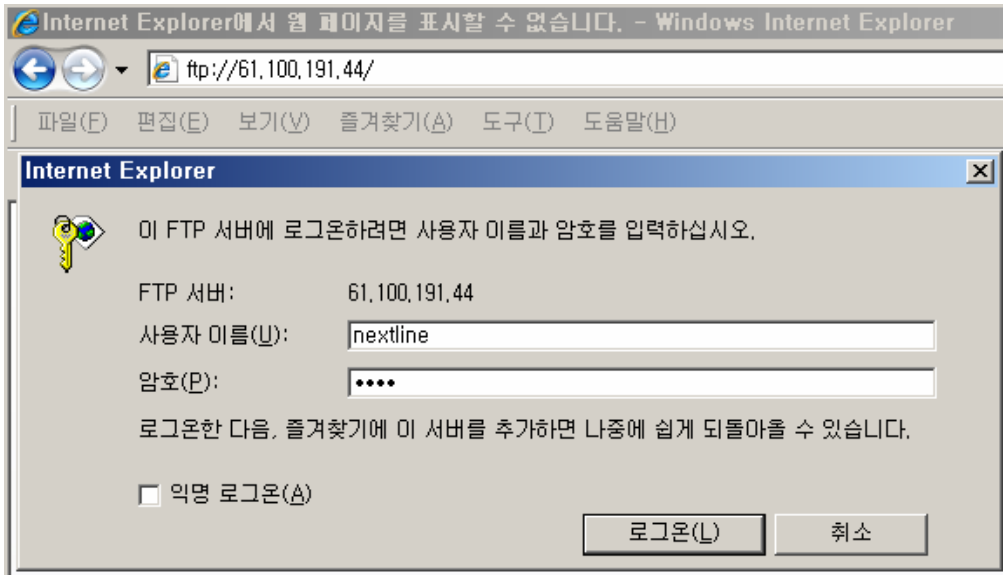


6) FTP 사이트 가상 디렉터리 속성은 다음과 같습니다.



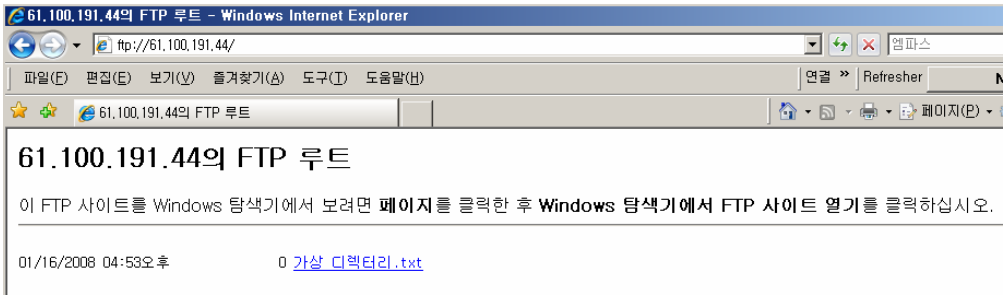
7) 익스플로러를 사용하여 nextline 에 접속하기 위해 익스플로러를 실행합니다. 익스플로러 주소창에 "ftp://IP 주소 또는 도메인" 을 입력합니다

ftp 사이트를 개별 포트 21로 설정했을 경우 접속 주소에 포트를 입력하지 않아도 됩니다. 하지만 개별 포트 21이 아닌 다른 포트로 사용 시에는 접속 수조에 "ftp://IP 주소:포트" 를 입력합니다



위와 같은 로그인 창에 사용자 "nextline" 와 설정한 암호를 입력합니다.

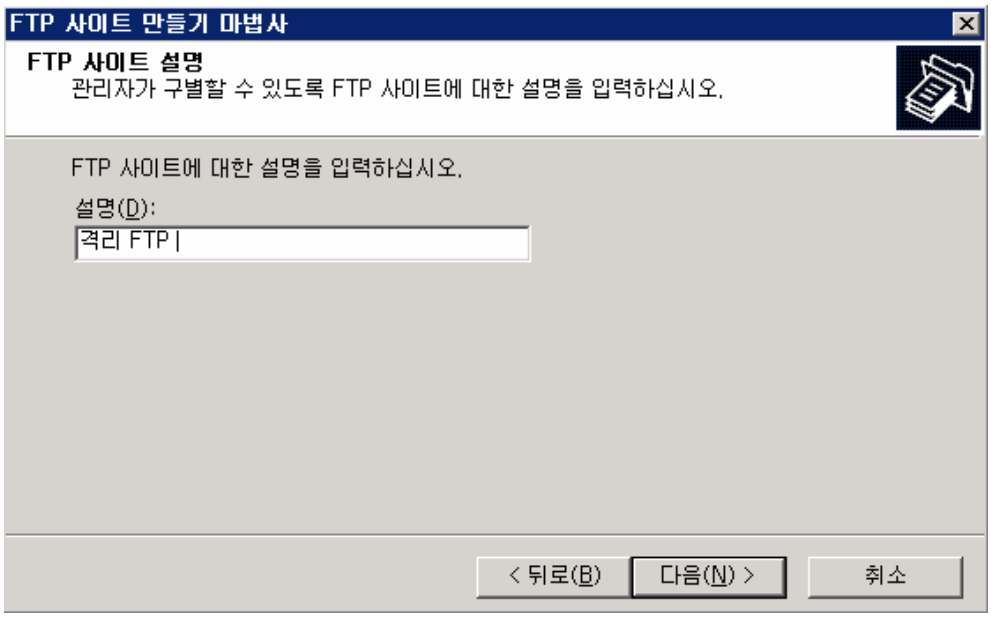
Nextline 접속을 완료하였습니다. Nextline 가상 디렉터리 사이트의 데이터 파일을 확인할 수 있습니다. 파일을 업로드 및 다운로드 할 수 있습니다



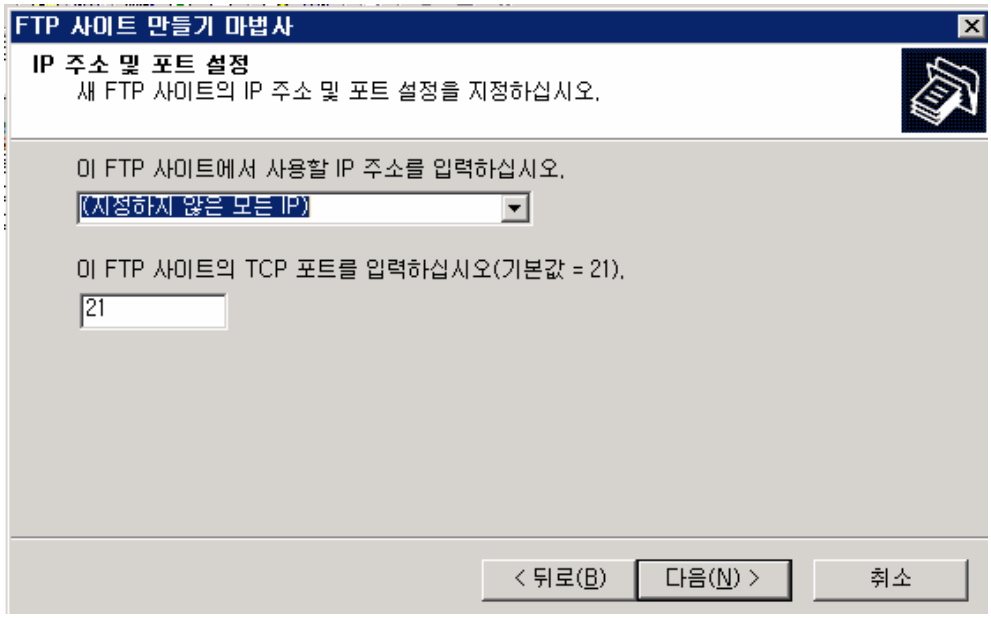
6. 격리 FTP 구성하기

1) 사용자 격리 모드는 먼저 사용자를 로컬 또는 도메인 계정에 대해 인증한 다음에만 자신의 이름에 대응하는 홈 디렉터리에 접근할 수 있습니다. 모든 사용자의 홈 디렉터리는 단일 FTP 루트 디렉터리 아래의 디렉터리 구조로 되어 있고, 각 사용자는 자신의 홈 디렉터리에 놓이고 제한됩니다. 사용자는 자신의 홈 디렉터리 외부는 탐색 할 수 없습니다. 사용자가 전용 공유 폴더에 접근해야 하는 경우에는 가상 루트를 설정할 수도 있습니다. 이 모드는 Active directory 서비스에 대한 인증은 제공하고 있지 않습니다.

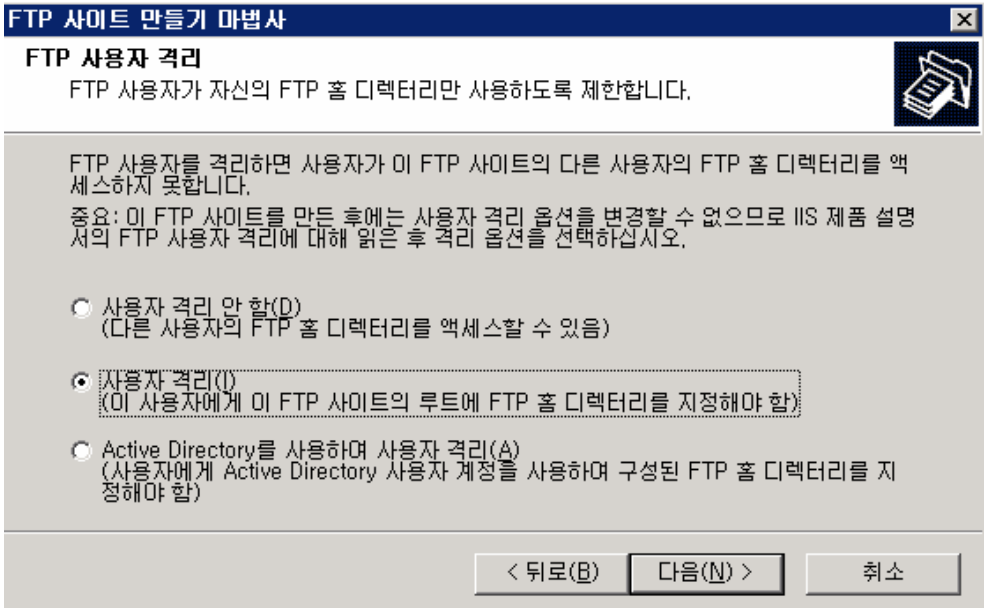
2) FTP 사이트 만들기 마법사를 실행하여 설명에 “격리 FTP” 를 입력합니다.



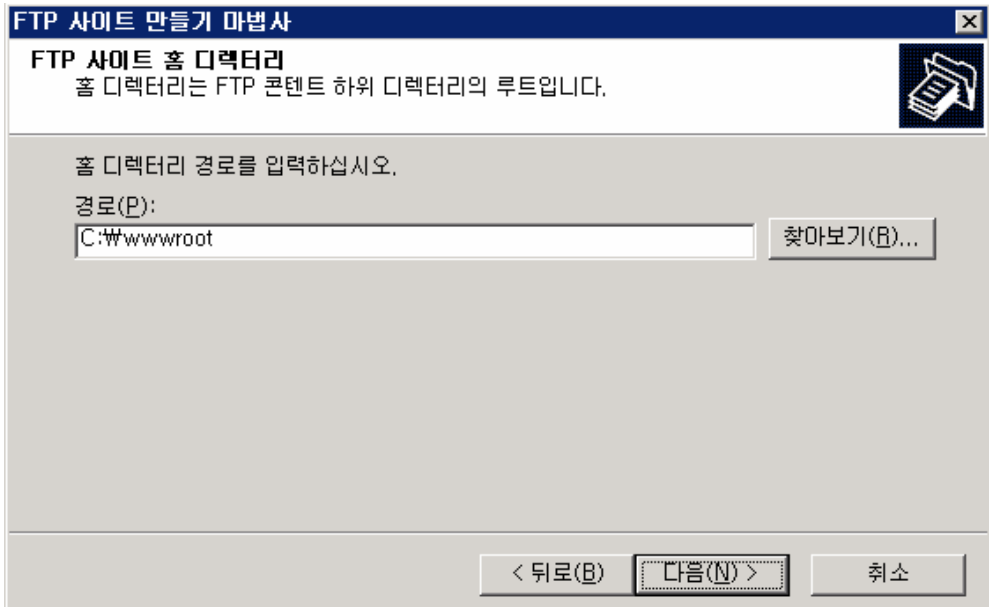
3) FTP 사이트에서 사용할 IP 주소를 설정하고, 포트를 설정하고, [다음]을 클릭합니다.



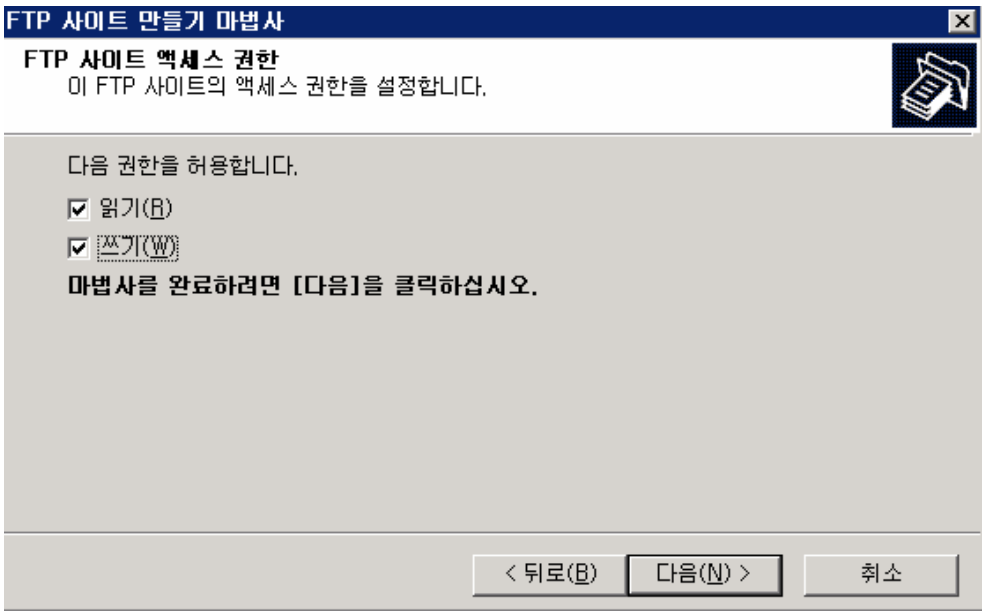
4) 사용자 격리를 사용하여 FTP 사이트를 구축 합니다. [다음]을 클릭합니다.



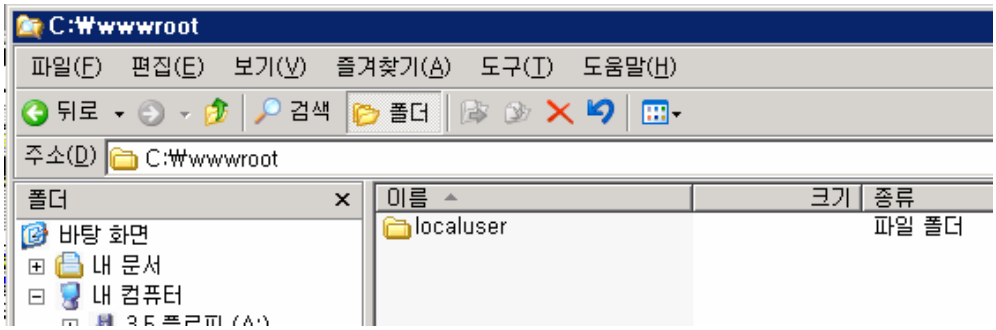
5) 홈 디렉터리 경로는 하드 디스크에 이미 존재하는 경로이어야 합니다. 만약, 하드디스크에 존재하지 않는 경로를 입력하면 '경로가 없거나 디렉터리가 아닙니다.' 라는 메시지를 출력하게 됩니다.



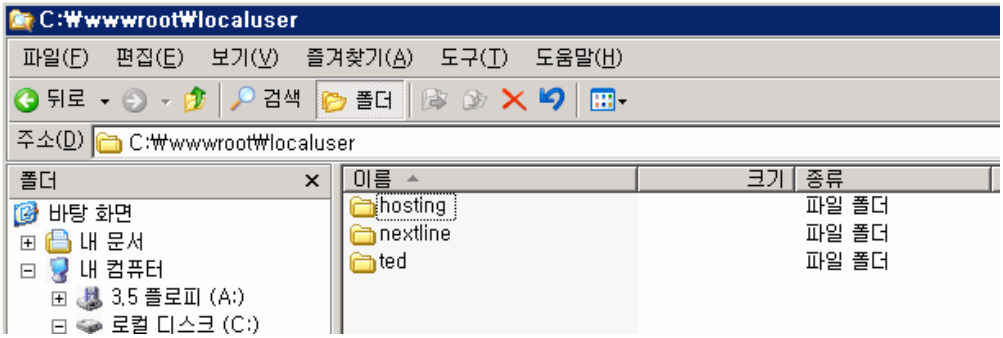
6) 기본적으로 FTP 사이트 엑세스 권한은 '읽기' 만 설정되어 있습니다. 격리 FTP 경우 사용자는 지정된 디렉터리에만 접근할 수 있기 때문에 읽기와 쓰기를 모두 허용해도 다른 사용자의 디렉터리를 읽거나 쓸 수 없습니다.



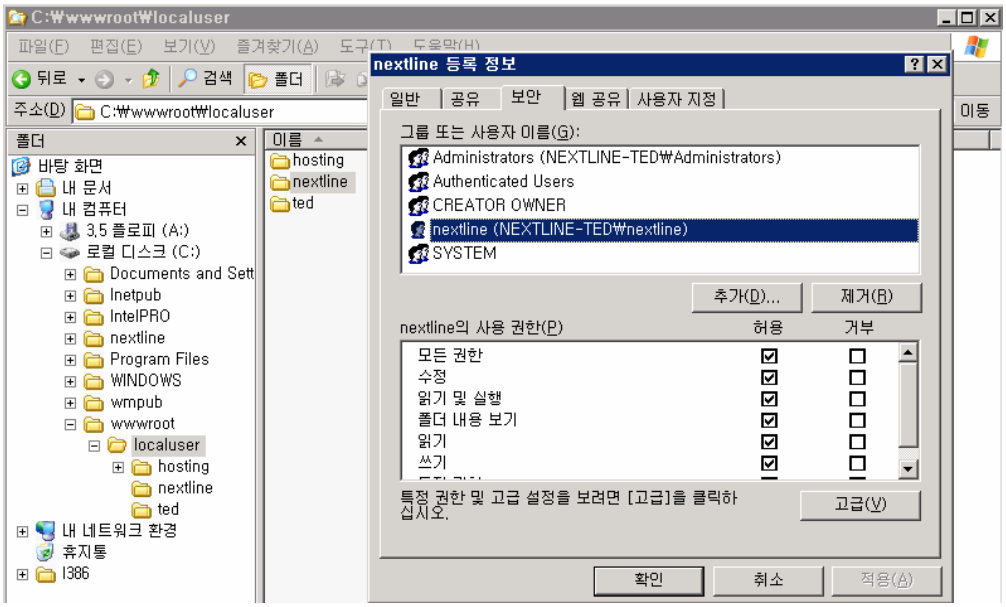
7) 디렉터리 경로 c:₩wwwroot 에 Localuser 라는 하위 디렉터리를 생성합니다.



8) c:₩wwwroot₩Localuser 안에 격리 FTP 사이트에 접근할 사용자의 이름으로 하위 디렉터리를 생성합니다. (디렉터리 이름과 로컬 사용자 및 그룹에서 생성한 사용자 이름이 일치해야 합니다.)

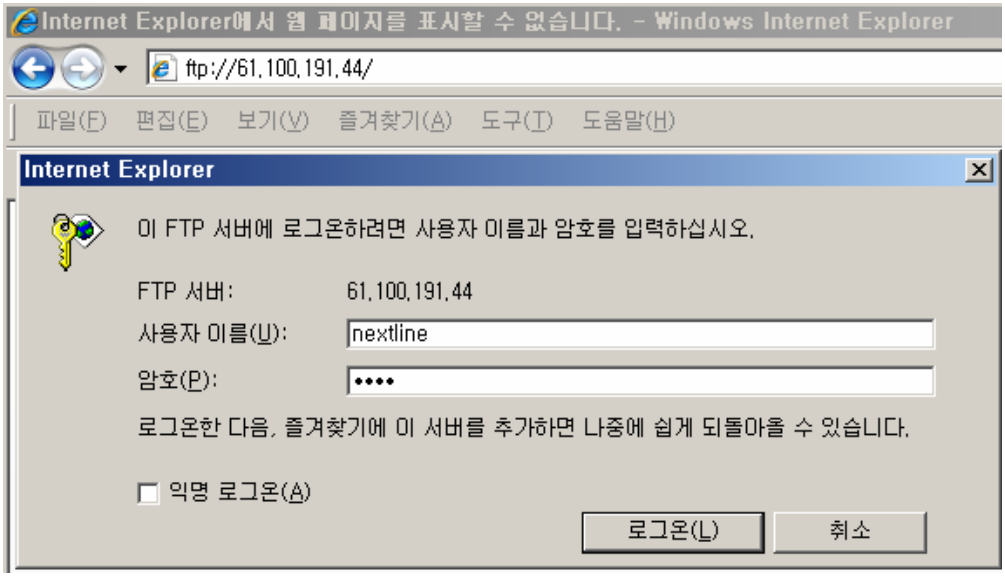


9) 사용자에게 필요한 접근 허용하기 위해 각 하위 디렉터리에 사용 권한을 지정합니다.



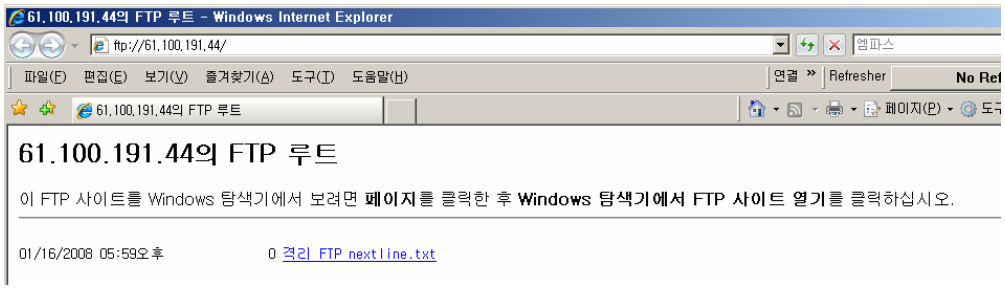
10) 익스플로러를 사용하여 nextline 에 접속하기 위해 익스플로러를 실행합니다. 익스플로러 주소창에 "ftp://IP 주소 또는 도메인" 을 입력합니다

ftp 사이트를 개별 포트 21로 설정했을 경우 접속 주소에 포트를 입력하지 않아도 됩니다. 하지만 개별 포트 21이 아닌 다른 포트로 사용 시에는 접속 수조에 "ftp://IP 주소:포트" 를 입력합니다



위와 같은 로그인 창에 사용자 “nextline”와 설정한 암호를 입력합니다.

Nextline 접속을 완료하였습니다. Nextline 가상 디렉터리 사이트의 데이터 파일을 확인할 수 있습니다. 파일을 업로드 및 다운로드 할 수 있습니다.



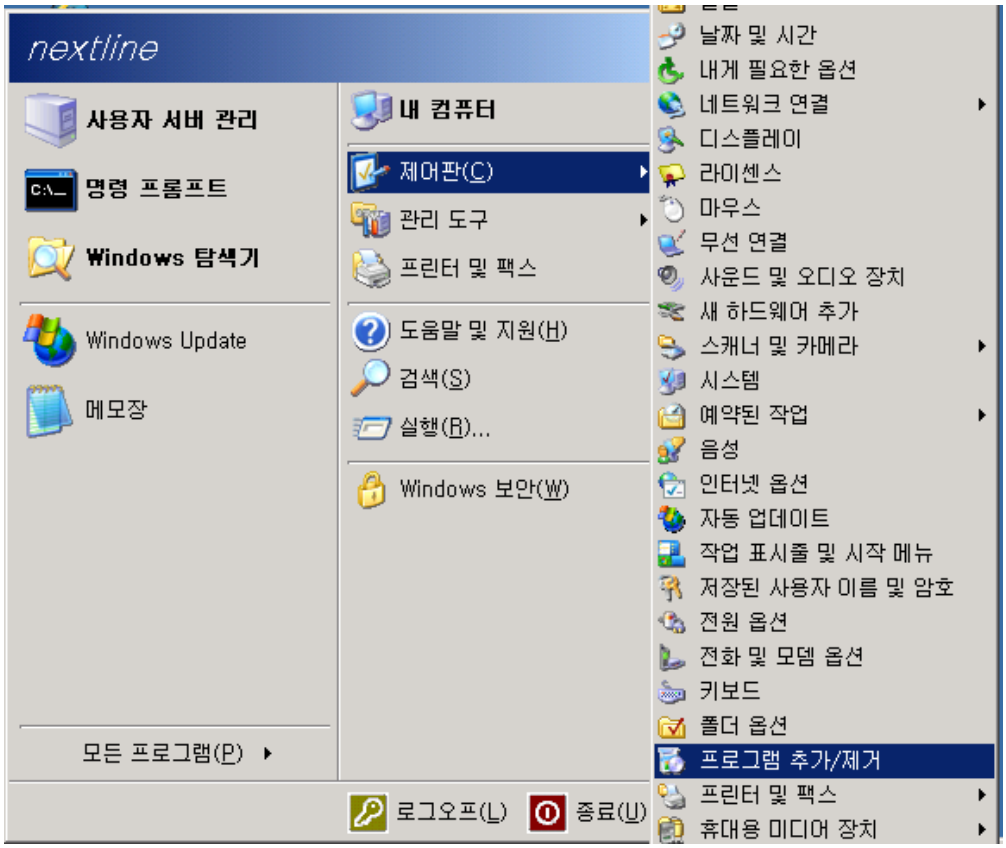
WEB 서버 구축 및 설정

IIS 6.0은 기본 Windows 커널인 HTTP.sys를 사용할 수 있게 다시 디자인되었습니다. 이로 인해 기본으로 제공된 응답/요청 캐시와 큐를 사용할 수 있으며, 응용 프로그램 프로세스 요청을 작업 프로세스들로 직접 전달하여 안정성과 성능을 개선했습니다 IIS 6.0에는 응용 프로그램 환경 구성을 위한 두 가지 작업 모드인 작업자 프로세스 격리 모드와 IIS 5.0 격리 모드가 도입되었습니다. 작업자 프로세스 격리 모드와 IIS 5.0의 격리 모드를 구성하는

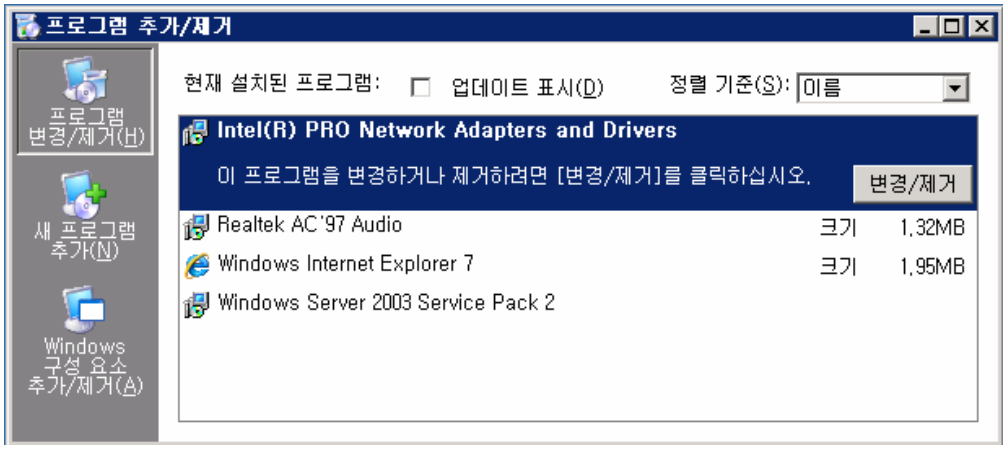
방법에 대해서는 “IIS 서버의 구성 옵션”에서 확인할 수 있습니다.

1. WEB 서버 설치하기

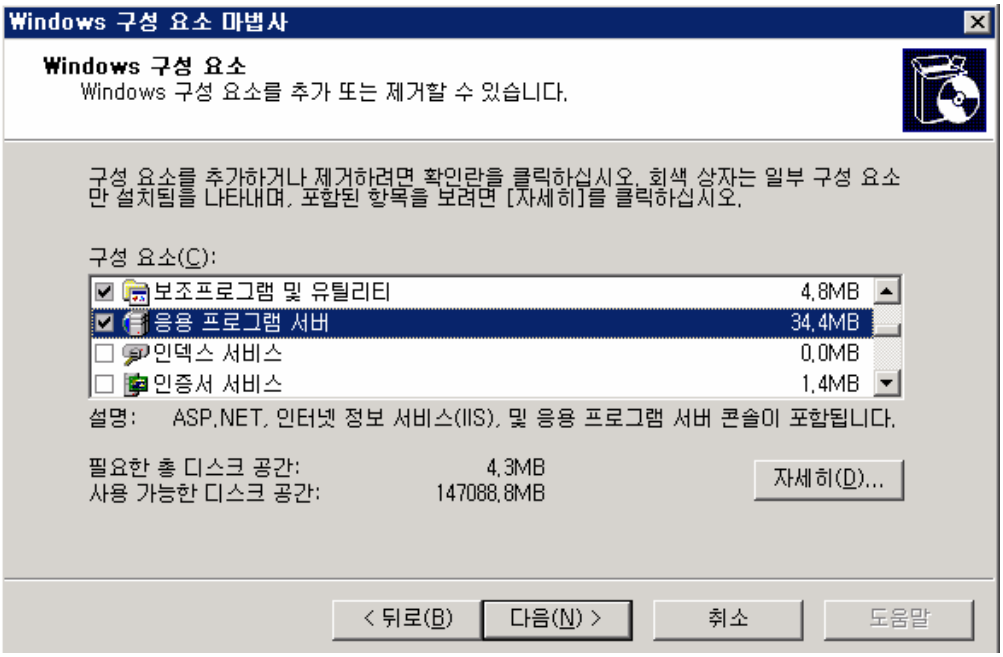
1) [시작]-[제어판]-[프로그램 추가/제거] 클릭 합니다.



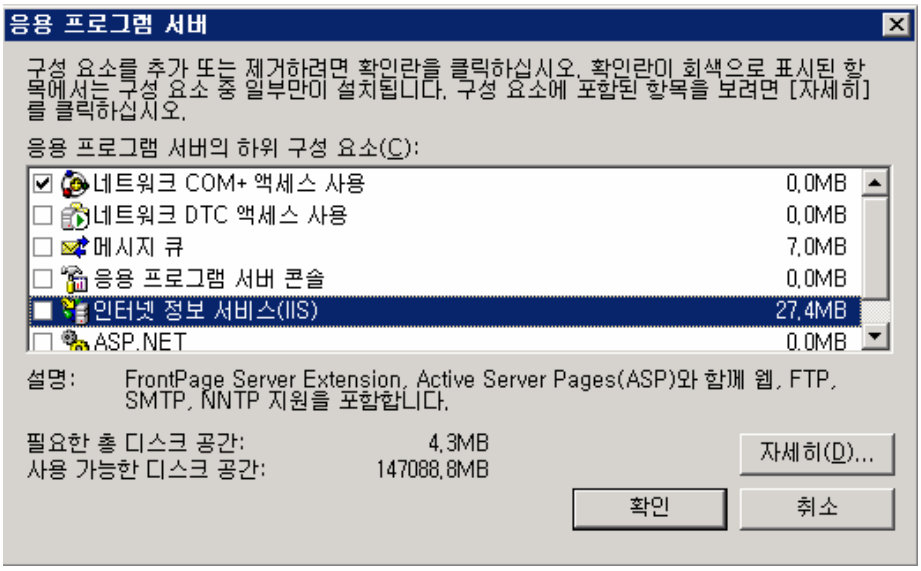
2) [Windows 구성 요소 추가/제거]를 클릭합니다.



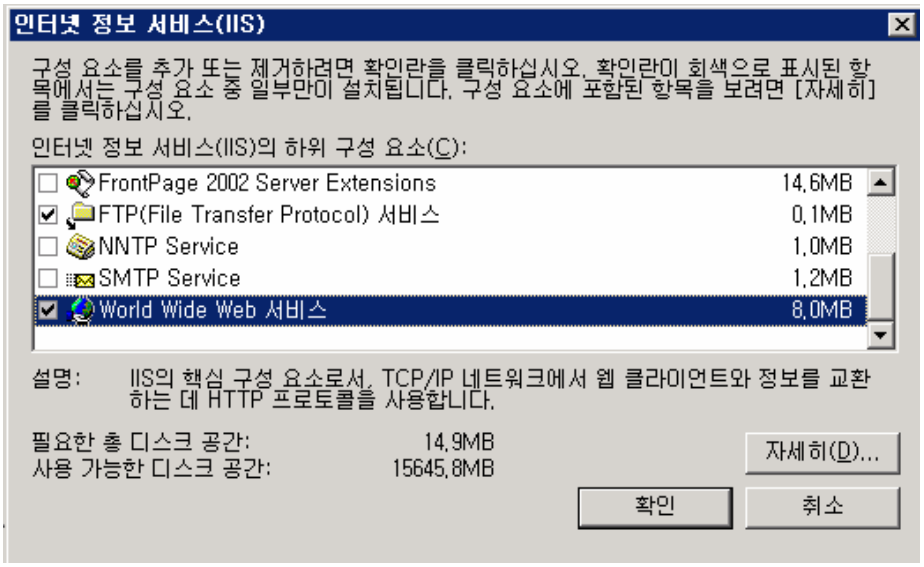
3) 구성 요소 목록에서 [응용 프로그램 서버] 를 클릭하고 [자세히]를 클릭합니다.



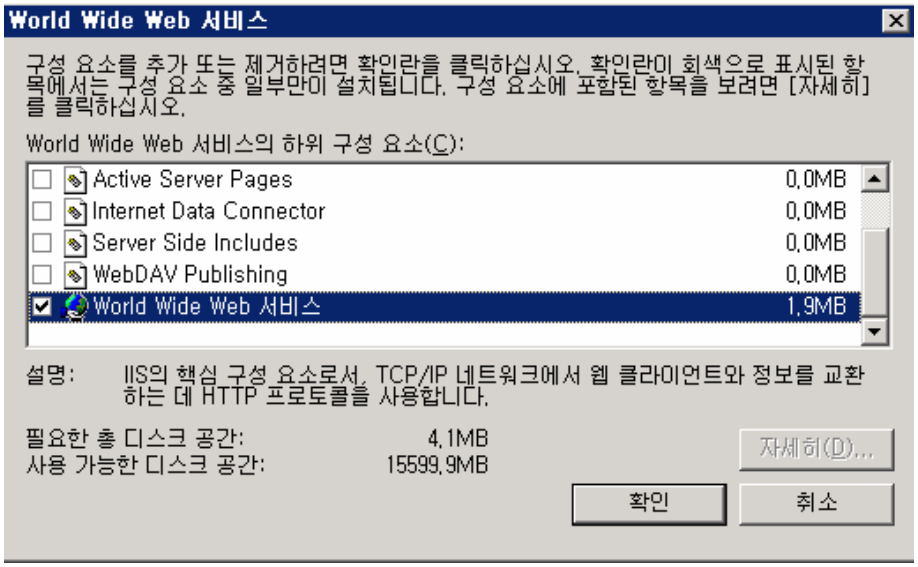
4) [인터넷 정보 서비스(IIS)] 를 클릭한 후 [자세히]를 클릭합니다.



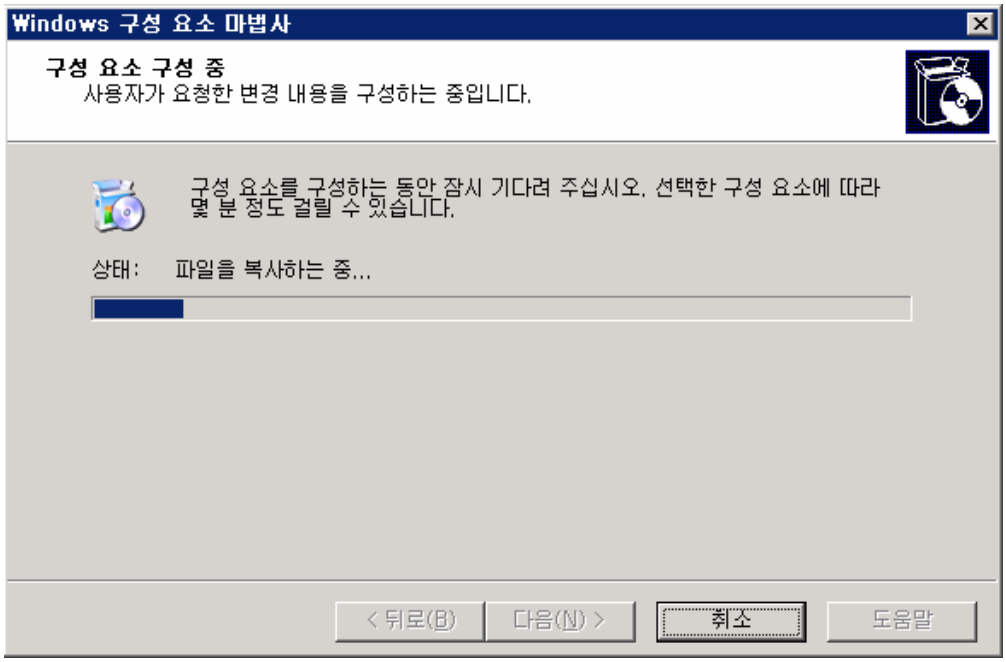
5) [World Wide Web] 를 클릭한 후 [자세히]를 클릭합니다.



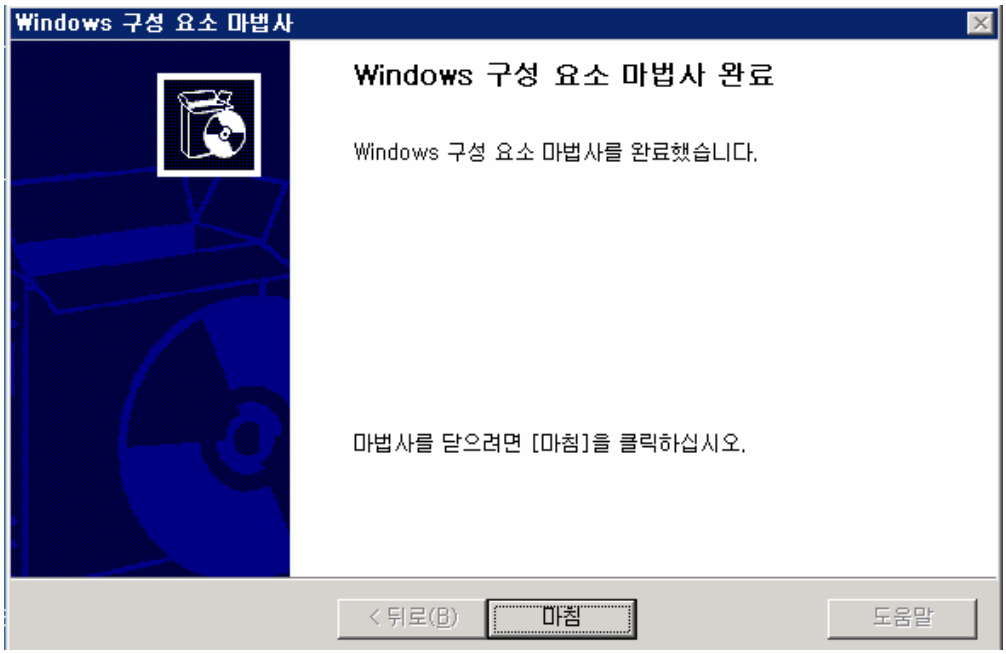
6) [World Wide Web 서비스] 하위 구성 요소는 IIS 관리 콘솔에서 웹 서비스 확장 노드를 통해 사용 혹은 사용 금지시킬 수 있습니다.



7) 확인을 클릭하면 설치를 진행 합니다.

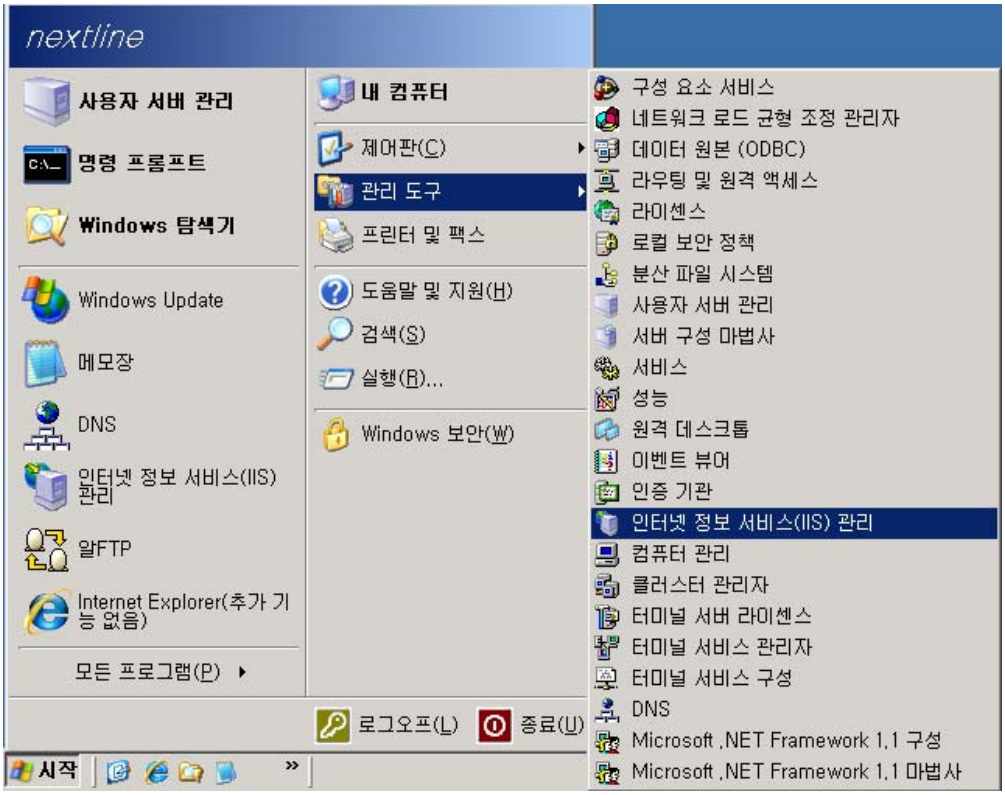


8) 설치 완료된 화면 입니다.

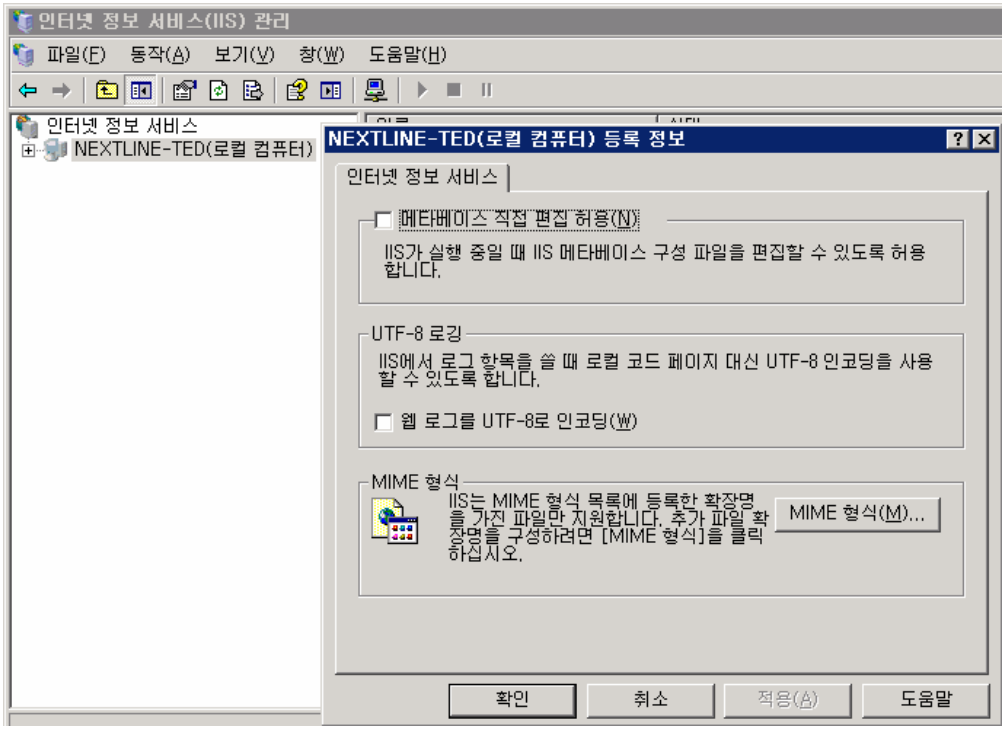


2. WEB 서비스의 구성 확인하기

1) [시작]-[관리도구]-[인터넷 정보 서비스(IIS) 관리]를 클릭합니다.



2) [서버 이름(로컬 컴퓨터)]을 클릭하여 등록 정보를 살펴봅니다.

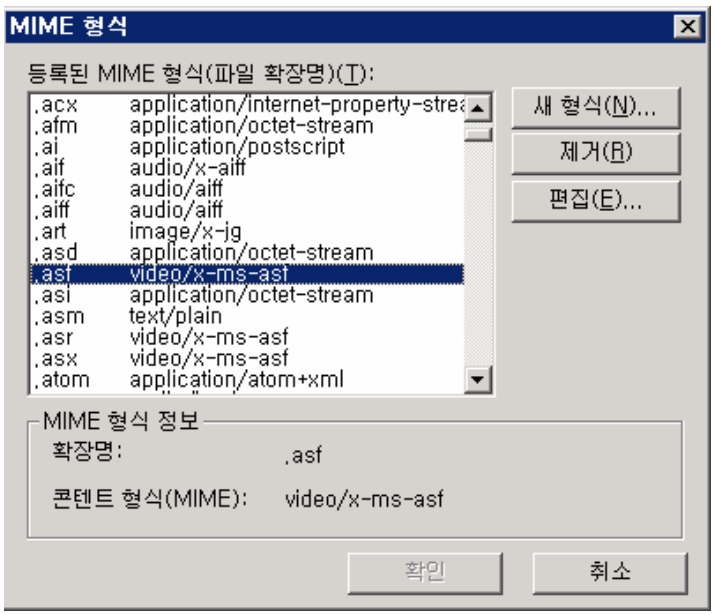


• 메타베이스 직접 편집 허용 : 메타베이스 직접 편집 하용 체크박스를 선택할 경우 IIS가 실행 중일 때 메타베이스 편집이 가능 하도록 하는 옵션입니다.

• UTF-8 : ASCII 코드 로컬 코드 페이지를 사용하지 않는 환경을 지원하기 위해서 UTF-8 형식의 로그 파일을 사용할 수 있게 합니다.

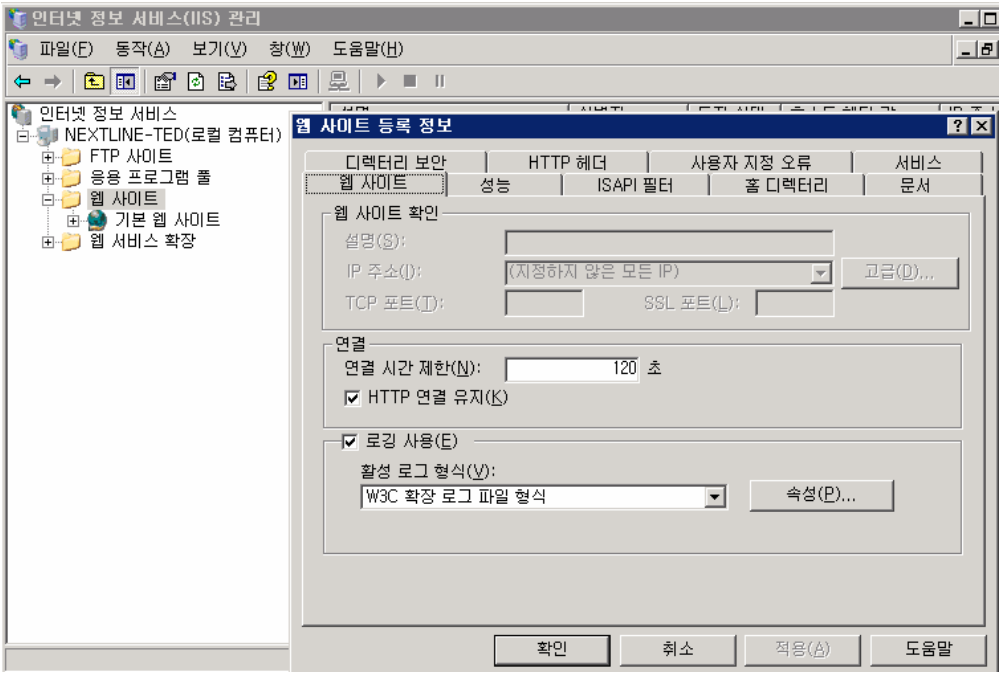
• MIME 형식 : MIME(Multipurpose Internet Mail Extension)은 클라이언트의 브라우저에서 파일을 웹 서버에 요청했을 때 MIME 매핑을 사용하여 클라이언트 브라우저에 어떤 식으로 보여줄지에 대한 파일 형식을 보내주는 것입니다.

예를 들어, .asf 파일을 웹에서 불렀을 때 비디오가 재생되는 것이 MIME 형식에 .asf가 video 가 등록되어 있기 때문입니다.



3) 웹 사이트의 등록 정보

① 웹 사이트 정보

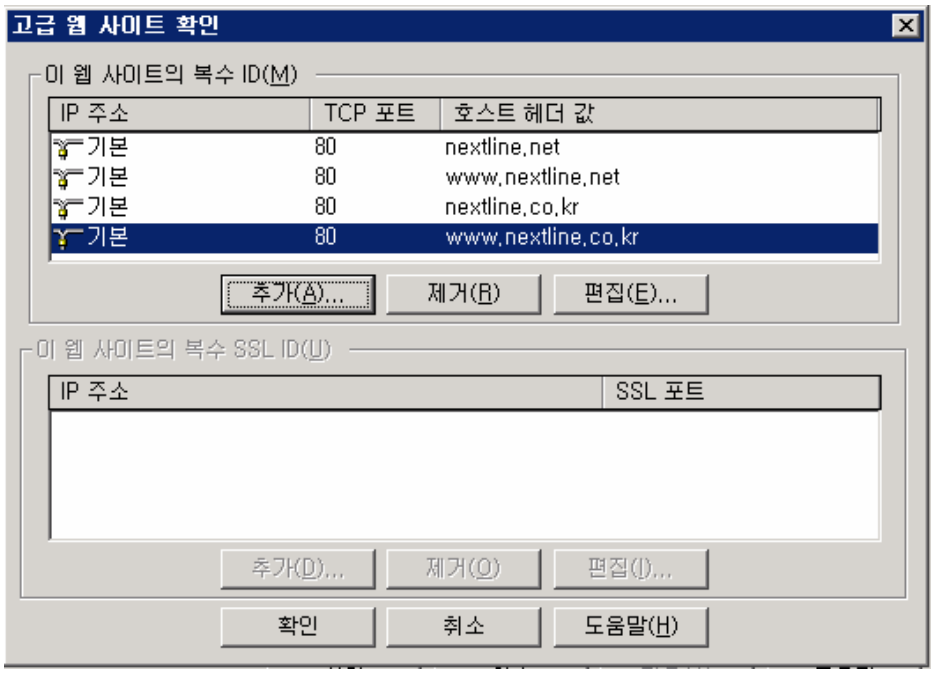


• 설명 : 웹 사이트를 대표할 이름 혹은 도메인과 같이 사이트의 내용을 한눈에 알아볼 있는 내용을 입력합니다. 이는 관리자가 쉽게 알아볼 수 있도록 하기 위함입니다.

• IP 주소 : IP 주소에는 서버에 등록되어 있는 모든 고정 IP 주소가 나타나는데 웹 사이트에 연결할 IP 주소로 지정합니다. 만약 (지정하지 않은 모든 IP)를 선택할 경우 서버에 등록되어 있는 모든 IP 주소로 접속이 가능하게 됩니다.

• SSL 포트 : Secure Sockets Layer로 서버 인증서를 설치하여 사용할 때 사용합니다. 기본적인 포트는 443포트이며, 클라이언트 PC에서 서버로 정보(예를 들어, 로그인 아이디/패스워드 혹은 신용카드 정보)를 입력하게 될 때 중간에 해커가 가로챌 수 없도록 암호화시켜 전송하는 방법이며, 별도의 인증서를 서버에 설치해야 사용할 수 있습니다.

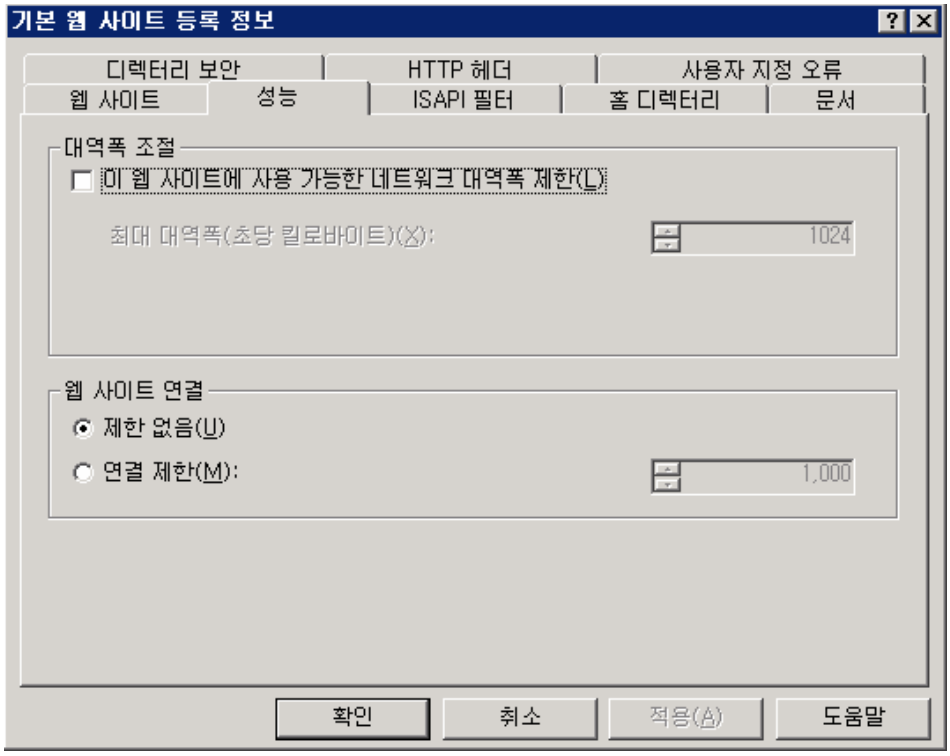
• 고급 : 사이트에 연결할 도메인을 입력하는 부분입니다. 호스트 헤더 값에 아래 그림과 같이 메인을 여러 개 추가하게 돌 경우 추가한 도메인은 모두 해당 사이트로 연결되게 됩니다. 즉 nextline.ne, www.nextline.net, nextline.co.kr, www.nextline.co.kr 을 하나의 사이트로 연결시킬 수 있는 방법이 이 호스트 헤더 값을 이용한 것입니다.



• 연결 : 클라이언트 브라우저에서 서버로 연결된 HTTP 연결을 언제까지 서버에서 유지하게 할 것 인가를 설정하는 옵션입니다. 만일 연결 시간 제한을 두지 않게 된다면 유휴 상태의 연결도 지속적으로 서버에 영향을 주므로 서버에 부하가 생길 수 있습니다. 따라서 연결 제한 시간을 설정하여 유휴 상태의 연결을 특정 시간이 지나면 끊어지도록 하는 것이 좋습니다. HTTP 연결 유지는 클라이언트 브라우저에서 페이지를 불러오면 서버는 여러 이미지나 파일들을 클라이언트에게 보내는데 이때 HTTP 연결을 유지해야 합니다. 만약 HTTP 연결 유지를 하지 않는다면 이미지나 파일 개별로 서버에 연결 요청을 하여 서버에 무리가 가게 되므로 HTTP 연결을 유지하여 사용하는 것이 서버의 성능에 좋습니다.

• 로깅 사용 : 클라이언트가 웹을 통해 서버에 접속했을 때의 클라이언트 정보를 남길 수 있도록 하는 기능입니다. 즉, 사용자의 IP 주소 및 사용자 이름 등에 대한 자료가 남으므로 로그 파일의 데이터를 통해 공격의 출처에 대한 정보를 얻을 수 있도록 접속자가 많아 시스템에 무리가 갈 정도로 로그가 쌓이는 경우가 아니라면 웹 로그를 남기는 것이 좋습니다. 로그 정보를 좀더 자세히 남기기를 원한다면 [속성]을 클릭하여 고급 부분에서 필요한 정보를 선택하여 남기게 할 수 있습니다. 로그 파일 형식 중에 W3C 확장 형식은 원래 GMT(그리니치 표준시간)와 같은 UTC(Universal Time Coordinated)를 사용합니다. 로그 파일에 표시된 시간은 서버에서 요청 및 응답을 처리하는 데 사용한 시간을 나타내고 클라이언트로의 네트워크 이동 시간이나 클라이언트 처리 시간은 포함되지 않습니다. 로깅 사용의 속성을 클릭하여 “파일명명 및 롤 오버에 현지 시간 사용(T)”를 사용하면 한국 시간으로 자정에 로그 파일이 새롭게 생성되나 로그 파일 안에 기록되는 로그 내용에는 적용되지 않으므로 “+09:00”를 해주어야 합니다.

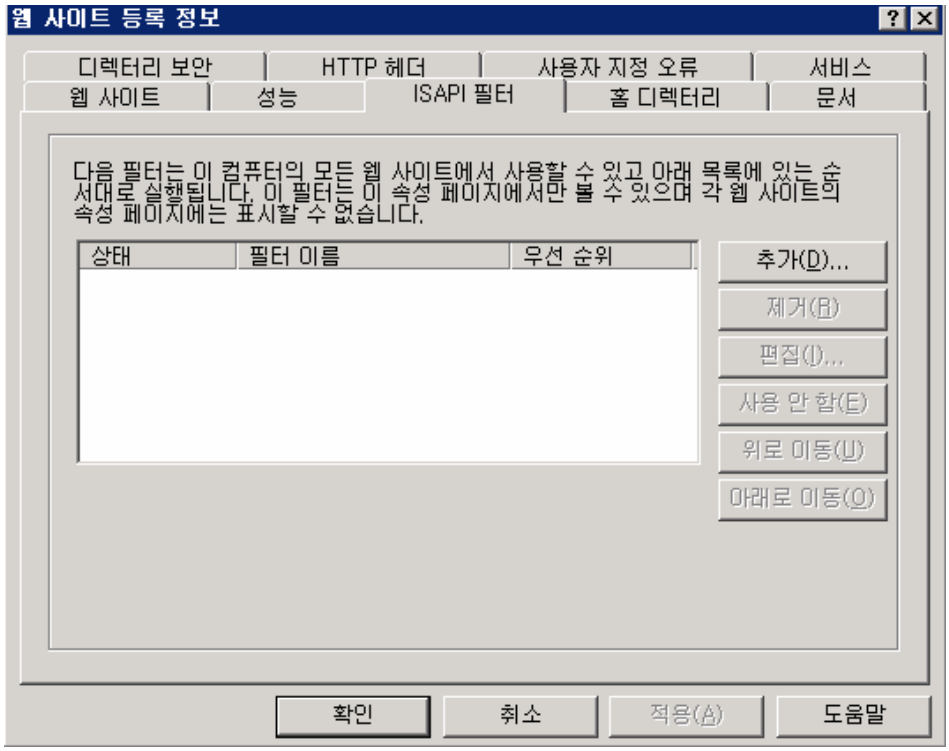
② 성능



• 대역폭 조절 : 개별 사이트마다 대역폭의 양을 제어할 수 있는데, 이는 대역폭 조절 기능을 이용하여 가능합니다. 사이트 전체의 대역폭을 조절하고 싶을 경우, 상위 웹 사이트 등록 정보에서 설정이 가능합니다.

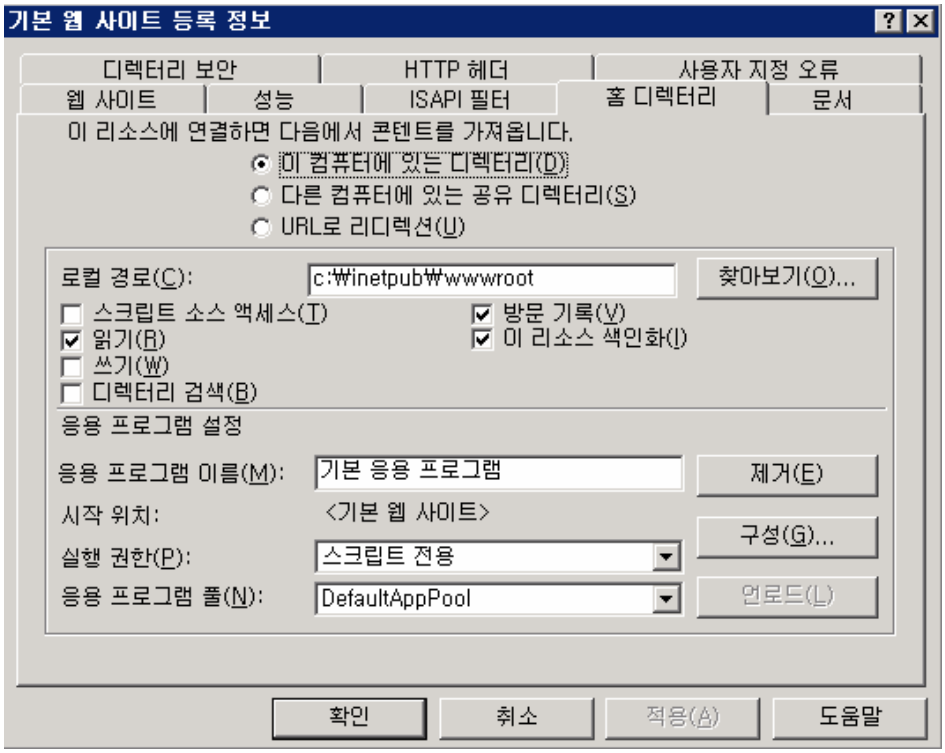
• 웹 사이트 연결 : 웹 사이트의 동시 접속자를 제한하도록 설정하는 부분입니다. 제한 숫자에 사용자가 도달하게 될 경우 동시 접속자가 많으므로 나중에 접속을 시도하라는 메시지를 남기게 됩니다.

③ISAPI 필터



• ISAPI 필터 : HTTP의 요청을 가장 먼저 처리하여 클라이언트에게 응답을 하기 전에 이벤트에 대한 정보를 변경할 수 있습니다. 해당 웹 사이트로 들어오는 HTTP의 요청이 모두 ISAPI 필터를 거치기 때문에 필터를 과도하게 할 경우에는 서버 성능에 지장을 줄 수 있습니다.

④ 홈 디렉터리



• 이 컴퓨터에 있는 디렉터리 : 사이트의 홈 디렉터리가 로컬에 존재할 때 경로를 지정해주면 됩니다.

• 다른 컴퓨터에 있는 공유 디렉터리 : 사이트의 홈 디렉터리가 로컬에 존재하지 않을 경우 UNC경로(₩₩{SERVER / {SHARE}) 를 입력하고 연결 계정을 클릭하여 네트워크 사용자의 이름과 암호를 입력해 주어야 합니다.

• URL로 리디렉션 : 웹 사이트의 호스트 헤더 값에 등록되어 있는 모든 도메인이 URL로 리디렉션한 도메인으로 바로 연결되게 됩니다.

• 스크립트 소스 액세스 : 읽기 또는 쓰기 권한이 활성화 되어있을 때 사용 가능하며, 소스 코드에 액세스가 가능하게 합니다. 이 옵션은 ASP에 포함된 스크립트도 액세스 가능합니다.

• 읽기 : 웹 서버의 파일을 읽을 수 있도록 합니다.

• 쓰기 : 웹 서버의 파일을 업로드하거나 글을 쓸 수 있도록 합니다. 해당 권한을 웹 사이트 상위에 설정할 경우, 보안상 취약한 문제가 발생하므로 하위 디렉터리에 쓰기 권한이 필요한 곳에만 설정해 주는 것이 좋습니다.

• 디렉터리 검색 : 웹 서버의 디렉터리 목록을 볼 수 있게 합니다.

• 방문 기록 : 방문자에 대한 로그 파일을 기록합니다.

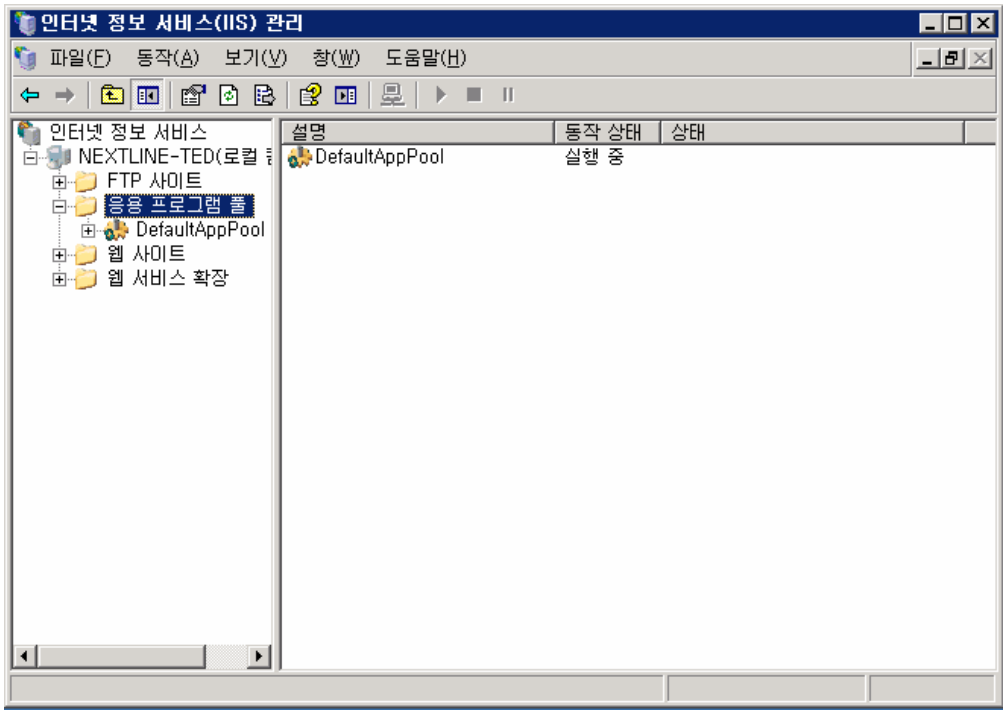
• 이 리소스 색인화 : 텍스트의 검색 속도를 높입니다. 이 옵션을 사용하려면 인덱싱 서비스가 실행되고 있어야 합니다.

• 응용 프로그램 이름 : 응용 프로그램 풀에 이미 만들어져 있어야 사용이 가능합니다.

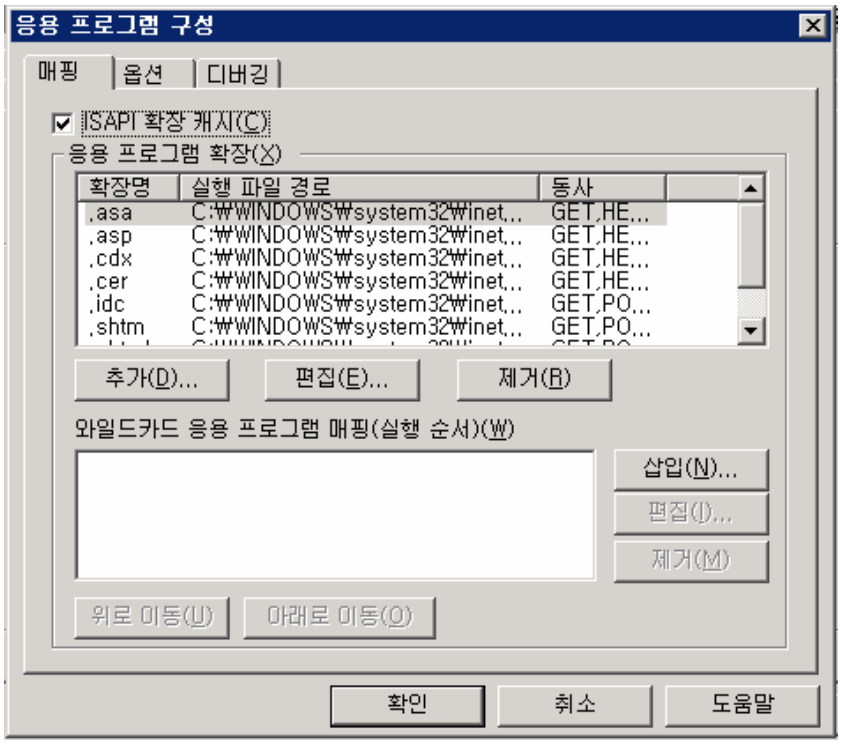
• 실행 권한 : 사이트에 허용되는 프로그램 실행 수준을 설정합니다. HTML 파일만 사용할 경우 스크립트 권한이나 실행 권한을 줄 경우 불법적인 파일을 업로드하여 실행이 가능하게 되므로 필요한 곳에만 실행 권한을 주는 것이 좋습니다.

• 응용 프로그램 풀 ; 새 응용 프로그램 풀을 만들어 웹 사이트와 응용 프로그램을 할당하

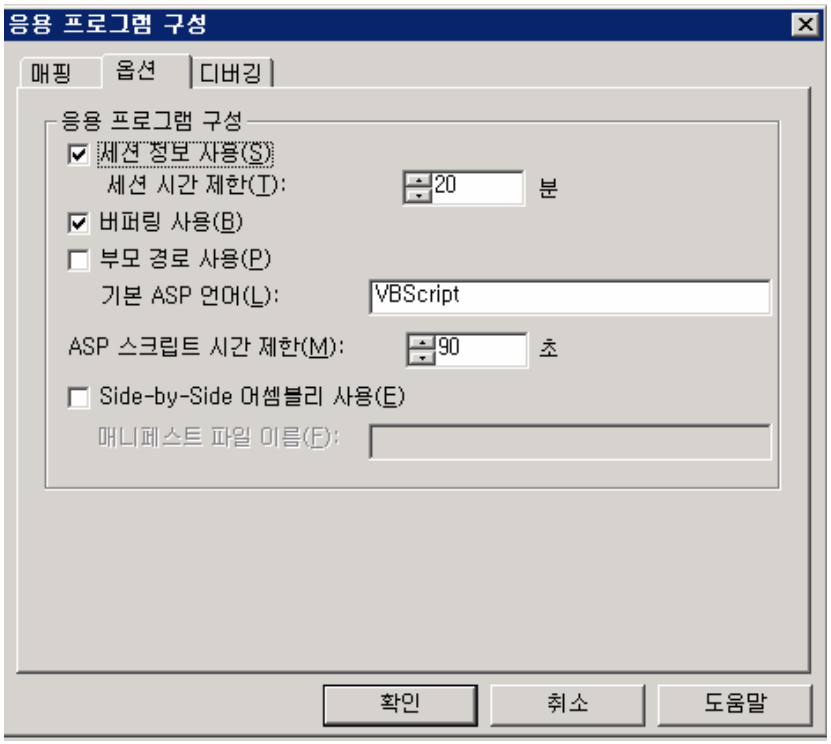
면 서버를 보다 효율적이고 안정적으로 사용할 수 있습니다. 또한, 새 응용 프로그램 풀의 응용 프로그램이 종료되더라도 다른 응용 프로그램은 항상 사용 가능한 상태로 유지할 수 있습니다.



기본 웹 사이트 옆의 [구성] 버튼을 누르면 다음 과 같은 응용 프로그램 구성 정보가 나타납니다.



• 매핑 : 매핑은 .asp .aspx 와 같이 프로그래밍 언어의 확장명을 매핑하는 곳입니다. Windows에서 기본 설치외 지원 않는 언어 .php 나 .pl과 같은 언어는 서버에 설치 후 이곳에 확장자를 추가해 주어야 합니다.



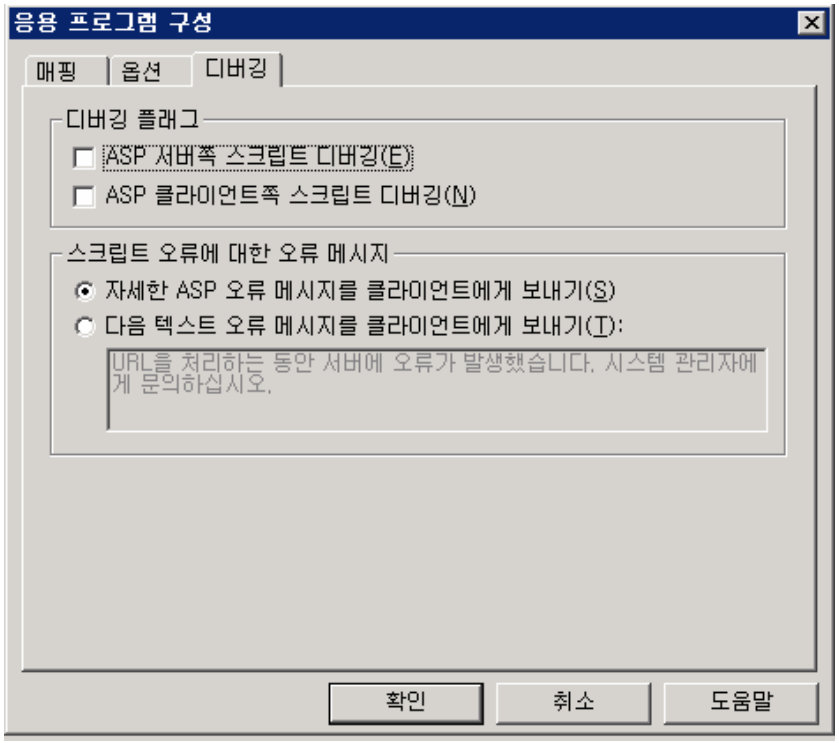
• 옵션 : 세션은 클라이언트가 응용 프로그램을 요청하지 않거나 새로 고침을 하지 않으면

“세션 시간 제한” 만큼 대기 후에 세션이 끊어집니다.

• 부모 경로 사용 : 현재 디렉터리에서 상대 경로를 허용하기 위해 사용하는 옵션으로 상위(..) 경로로 올라갈 수 있도록 설정하는 부분입니다.

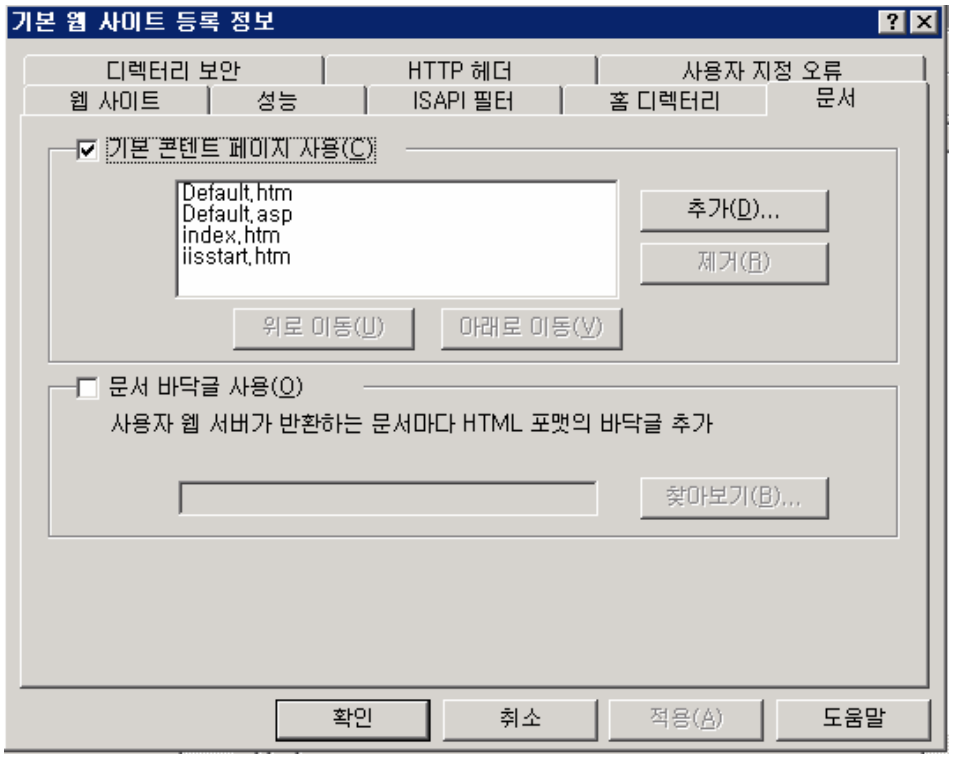
상대 경로는 최상위 디렉터리까지 올라갈 수 있기 때문에 중요 파일이나 시스템 시스템 파일까지 접근 할 수 있게 되므로 보안상 매우 취약합니다. 따라서 부모 경로는 되도록 사용하지 않을 것을 권장 합니다.

• 스크립트 시간 제한 : ASP가 스크립트 실행의 허용 시간을 지정합니다. 시간 제한 기간이 끝날 때 까지 스크립트 실행이 끝나지 않으면 스크립트를 중지하고, 이벤트 로그에 이벤트를 기록합니다. Server.ScriptTimeout 메소드를 사용하면 이 옵션을 무시할 수 있습니다.



• 자세한 ASP 오류 메시지를 클라이언트에게 보내기 : ASP 오류가 발생할 때 브라우저에 오류 발생 파일 이름 및 오류 메시지, 오류 메시지가 발생한 줄 번호까지 상세하게 클라이언트 브라우저에 전송합니다.

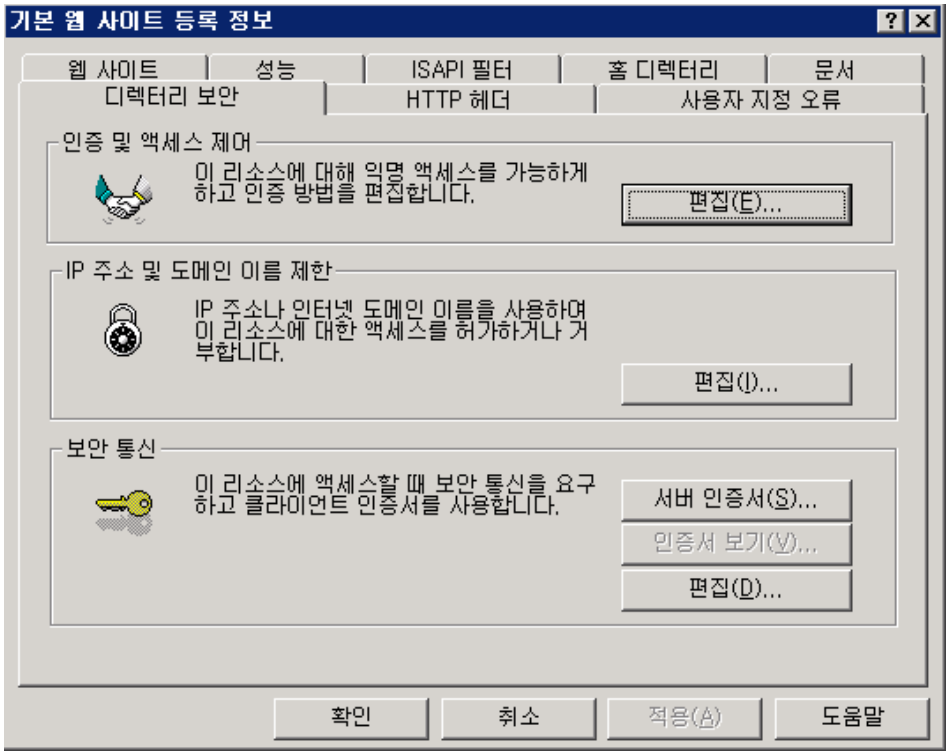
⑤ 문서



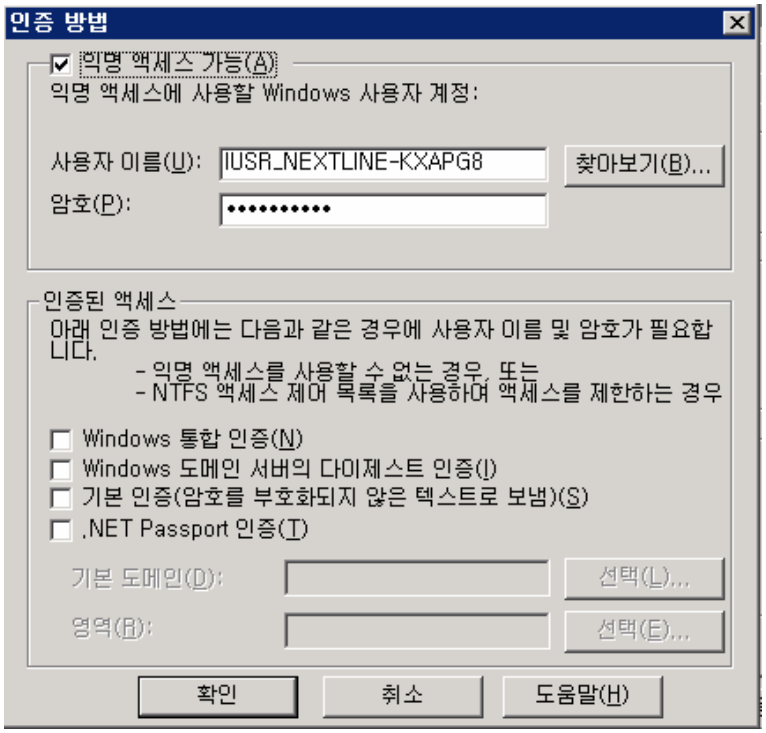
• 기본 콘텐트 페이지 사용 : 사이트에 기본 페이지를 정의합니다. 브라우저에서 http://nextline.co.kr 을 입력했을 때 http://nextline.co.kr/default.htm 처럼 default.htm 을 바로 찾을 수 있는 이유가 기본 페이지에 등록되어 있기 때문입니다. 기본 페이지 이름은 원하는 이름으로 추가가 가능하며, 등록된 이름이 여러 개 있을 경우 상위에 있는 이름을 먼저 인식하게 됩니다.

• 문서 바닥글 사용 : 웹 사이트 하단에 .html 형식의 바닥글을 넣고 싶을 경우에 사용 가능합니다.

⑥ 디렉터리 보안



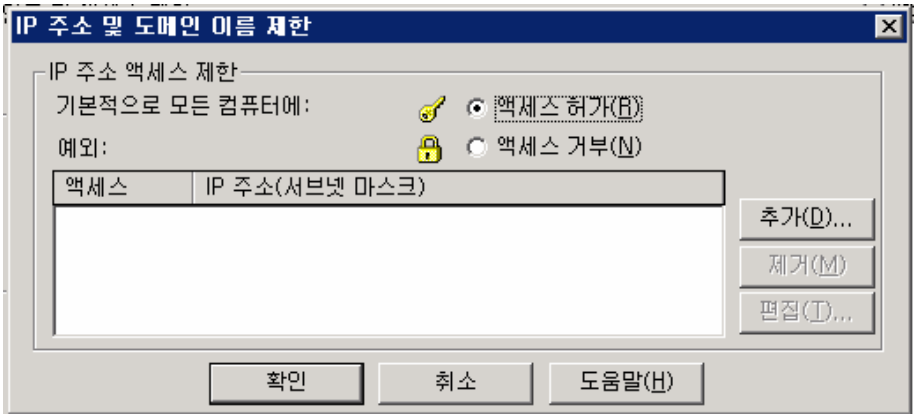
• 인증 및 액세스 제어 : 리소스에 대한 익명 액세스 혹은 인증된 액세스를 선택할 수 있습니다.



• 익명 액세스 가능 : 서버에 설정되어 있는 사이트를 접속할 때 암호 없이 바로 접속이 가능한 것이 이 익명 액세스 사용 가능하도록 설정되어 있기 때문에 가능한 것입니다. 익명

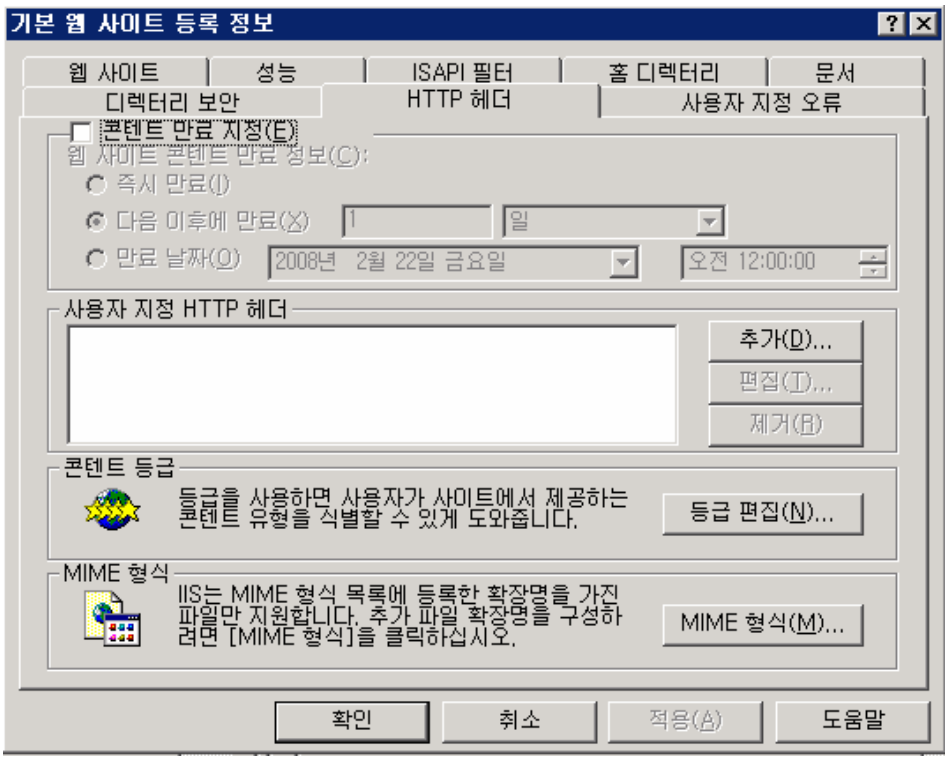
액세스에 시용하는 계정은 IIS가 설치될 때 자동으로 생성됩니다.

• 인증된 액세스 : 익명 액세스와 달리 인증된 사용자만이 접속할 수 있도록 하는 방식입니다.



• IP 주소 및 도메인 이름 제한 : 웹 사이트를 접속하는 사용자를 IP 주소 혹은 도메인으로 제한할 수 있습니다. 방화벽은 서버 전체에 대한 접근/거부를 설정할 수 있지만, IP 주소 및 도메인 이름 제한을 이용하면 각 사이트 별로 액세스 제한 설정이 가능합니다.

⑦ HTTP 헤더



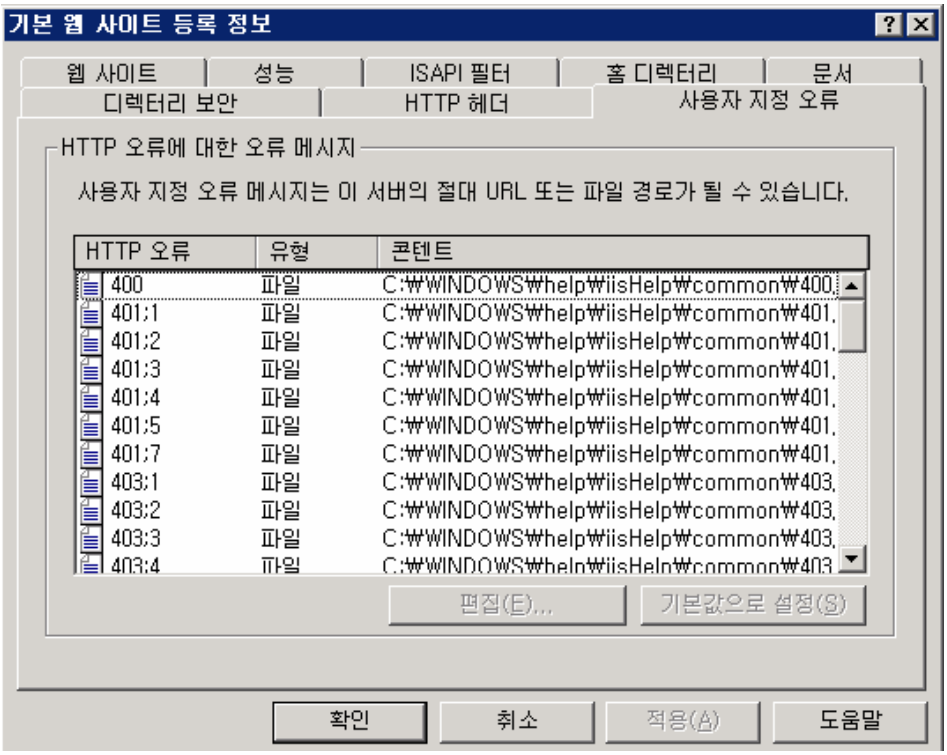
• 콘텐트 만료 지정 : 캐시된 페이지를 얼마 후에 업데이트된 페이지로 보여줄 것인지를 설정해 줍니다.

• 콘텐트 등급 : HTTP 헤더에 설명 레이블을 포함합니다.

• MIME 형식 : MIME 매핑은 앞에서 다른 것과 같이 클라이언트 브라우저에 파일을 어떤 형

식으로 보여줄 것인지를 설정하는 부분입니다. 앞에서 설정한 MIME 또는 사이트 전체의 설정이 적용되며, 특정 사이트에만 MIME 매핑을 추가하고자 할 경우, 설정하면 됩니다.

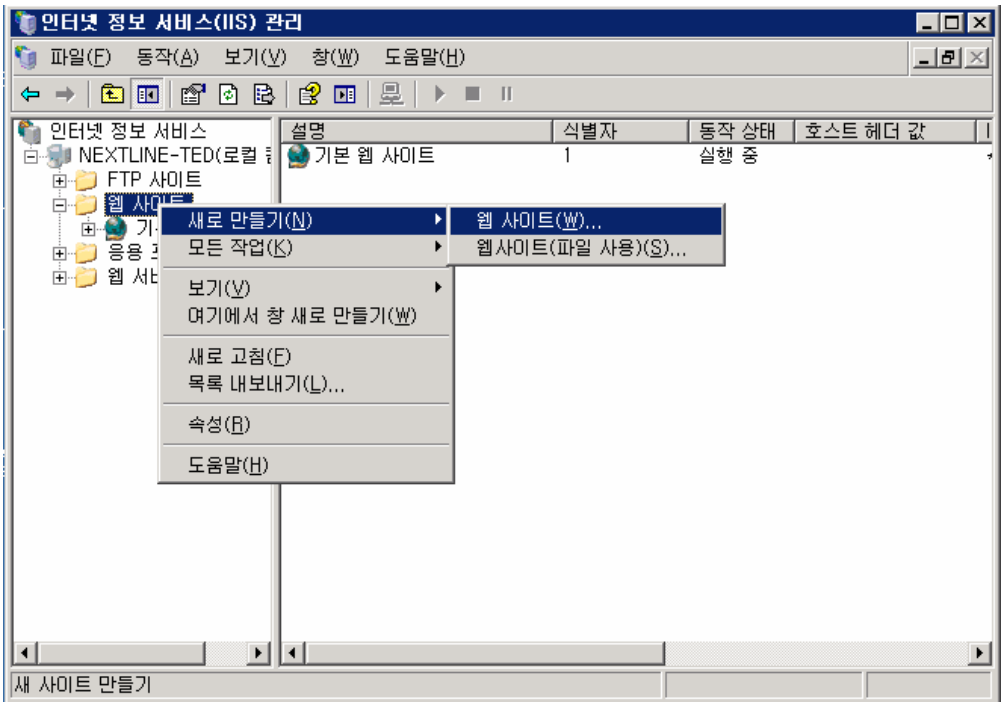
⑧ 사용자 지정 오류

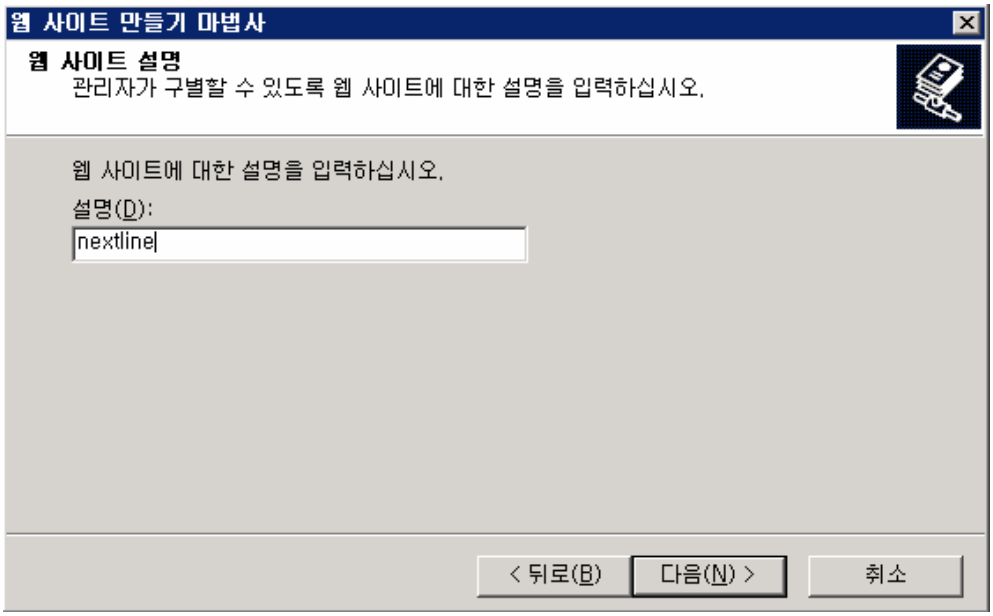


클라이언트가 HTTP 연결을 요청할 때 페이지가 없거나 오류가 발생할 때 이곳의 설정으로 오류 메시지를 보여주게 됩니다. 이 오류 내용은 편집이 가능합니다.

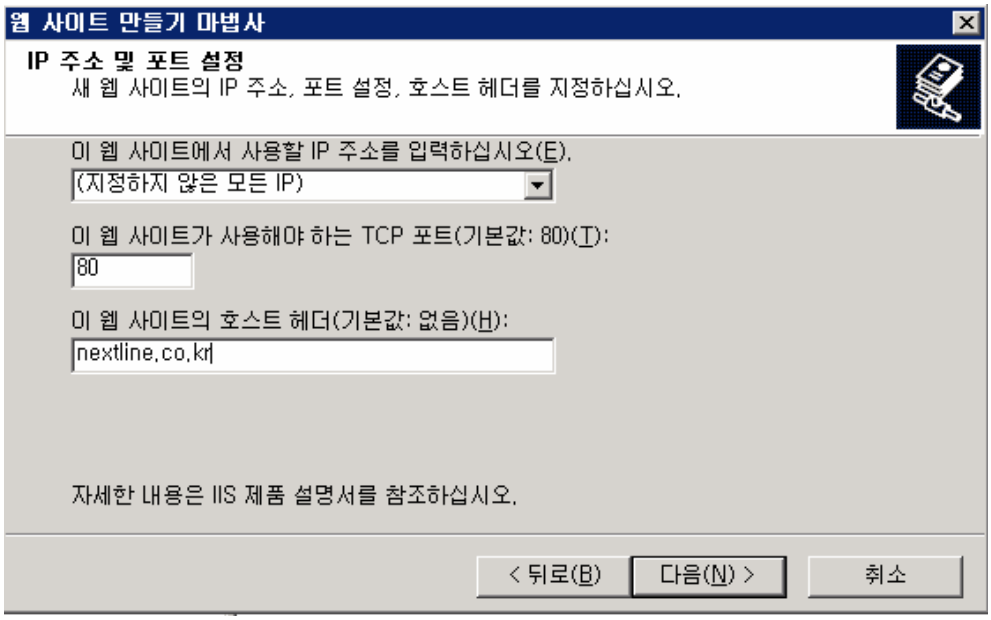
4) 웹 사이트 구축하기

① 웹 사이트 [새로 만들기]를 실행 합니다. 웹 사이트 설명에는 사이트를 대표할 설명이나 도메인을 입력합니다.

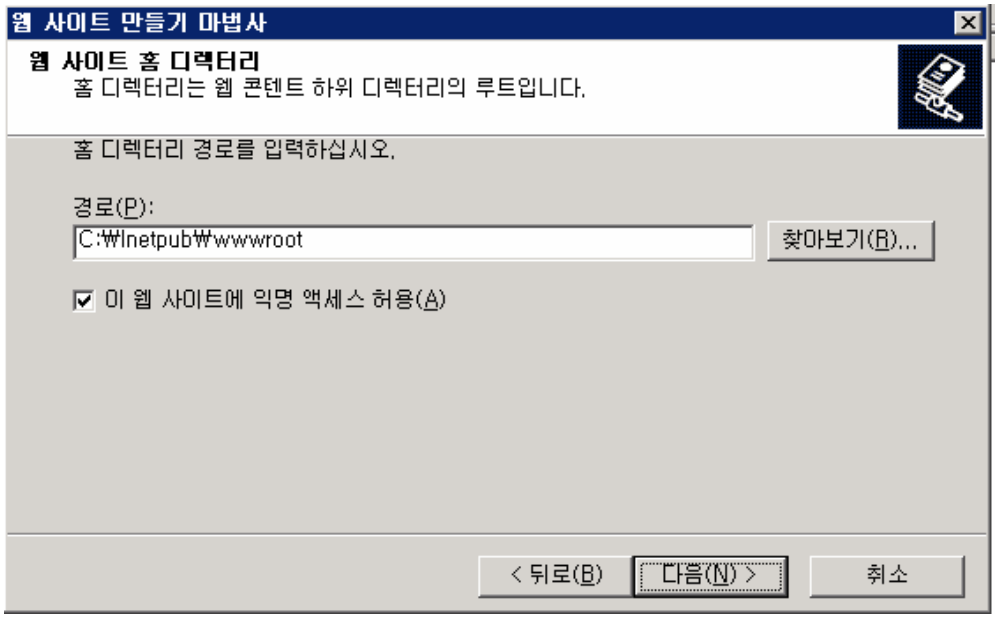




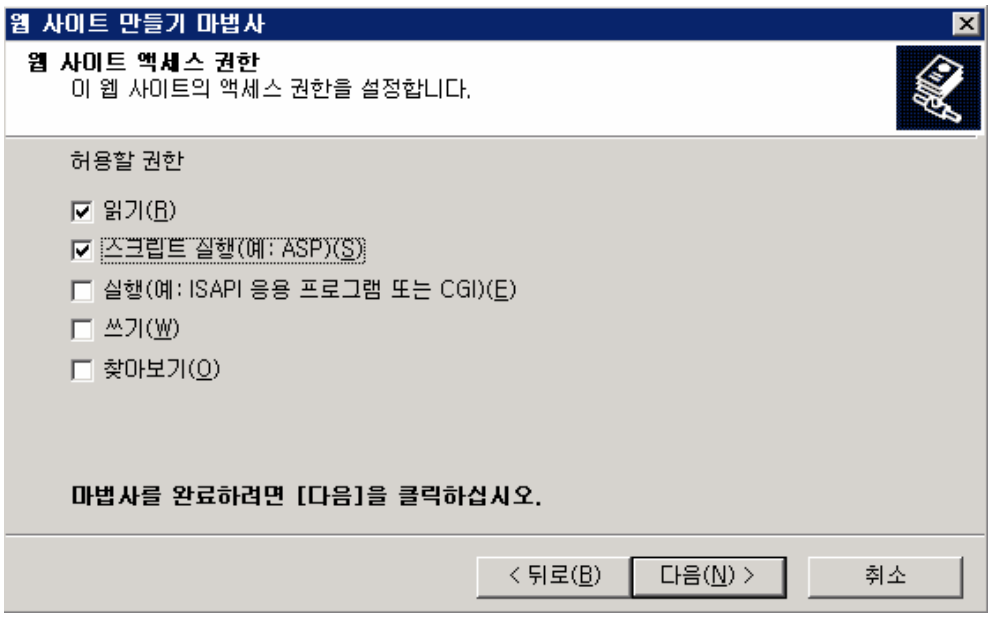
② 연결할 도메인의 IP 주소를 할당해주고 호스트 헤더 값에는 이 사이트에 연결할 도메인을 입력합니다. 도메인을 여러 개 연결하고자 할 경우 추후에 추가가 가능하므로 우선 대표 도메인만 넣고 [다음]을 클릭합니다.



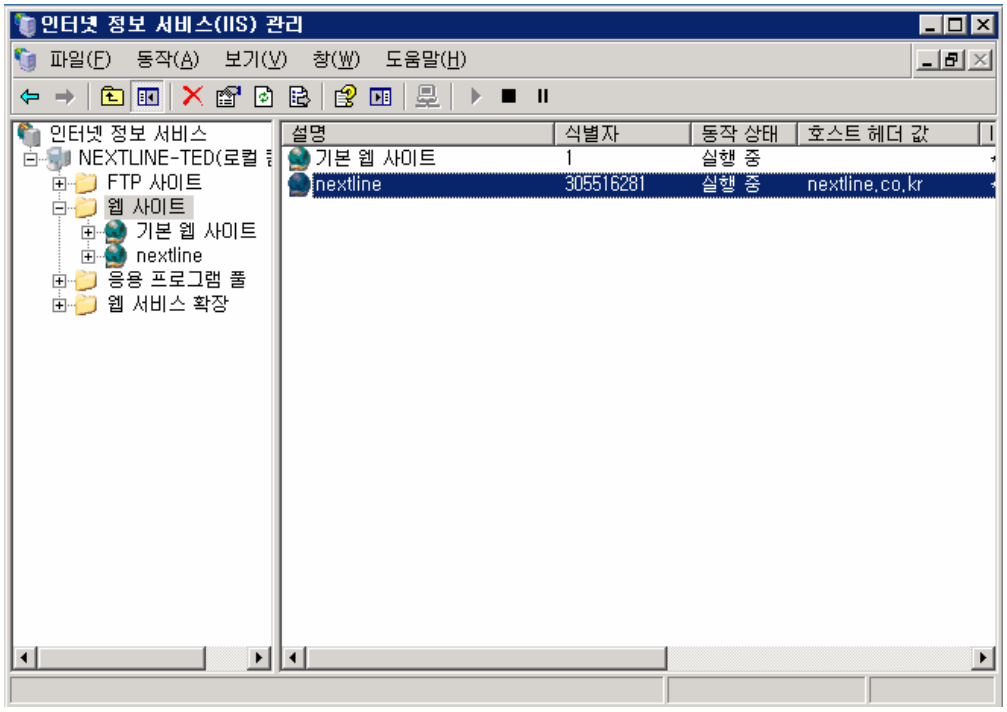
③ 사이트의 홈 디렉터리를 지정합니다.



④ HTML 파일만 있을 경우 읽기 권한으로 사이트 운영이 가능하지만 ASP를 사용하려면 적어도 스크립트 권한이 필요하므로 “스크립트 실행”에 체크합니다.

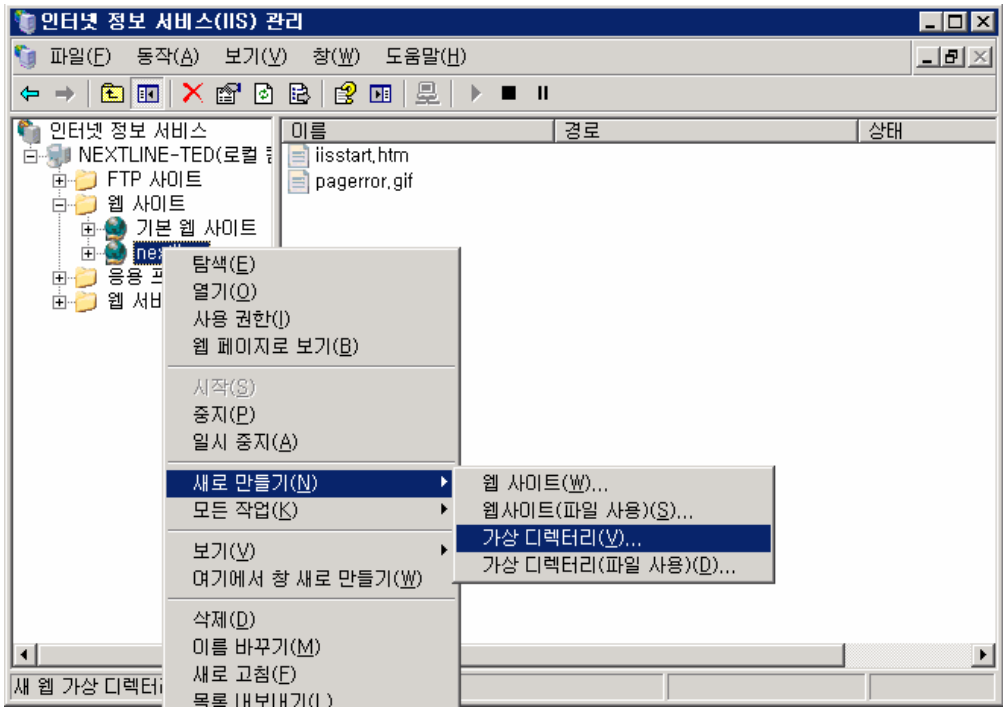


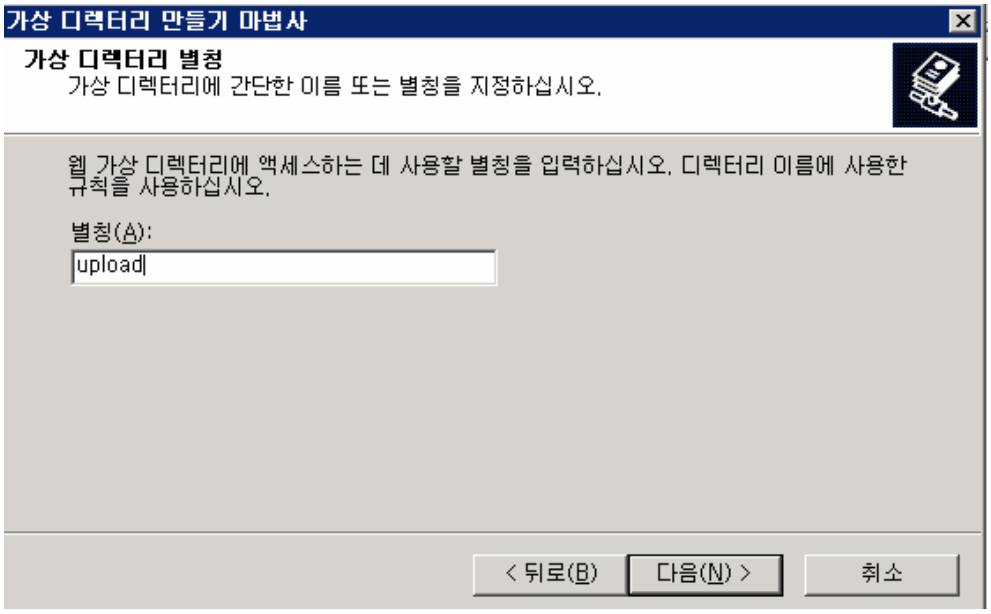
⑤ 사이트 설정이 완료되면 아래와 같은 화면이 나타납니다.



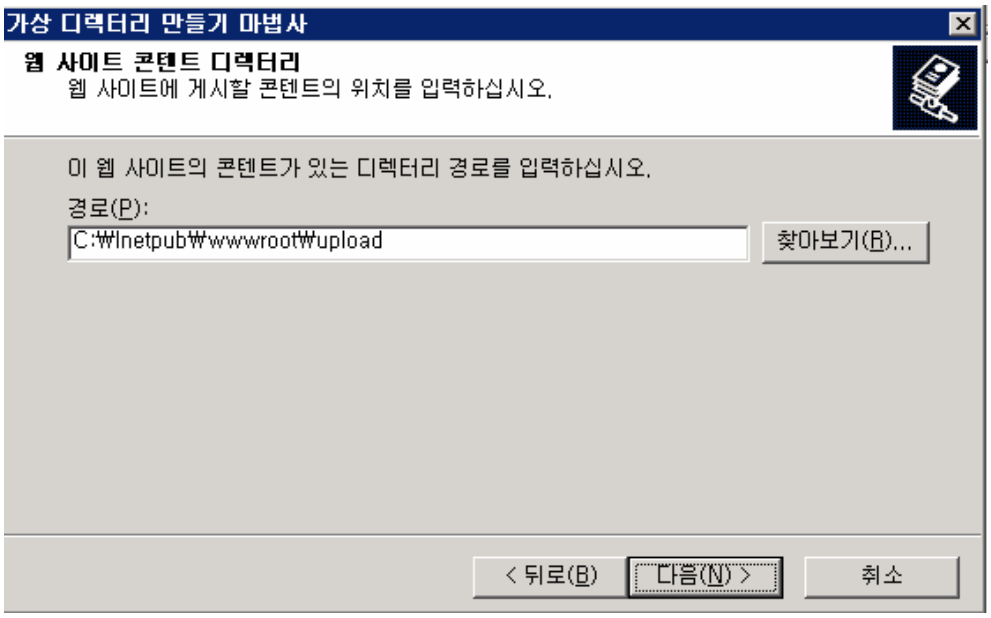
6) 가상 디렉터리 만들기

① 앞에서 생성한 웹 사이트의 마우스 오른쪽 버튼을 클릭하여 [가상 디렉터리 만들기]를 실행하여 가상 디렉터리 이름을 지정하고, 입력합니다.

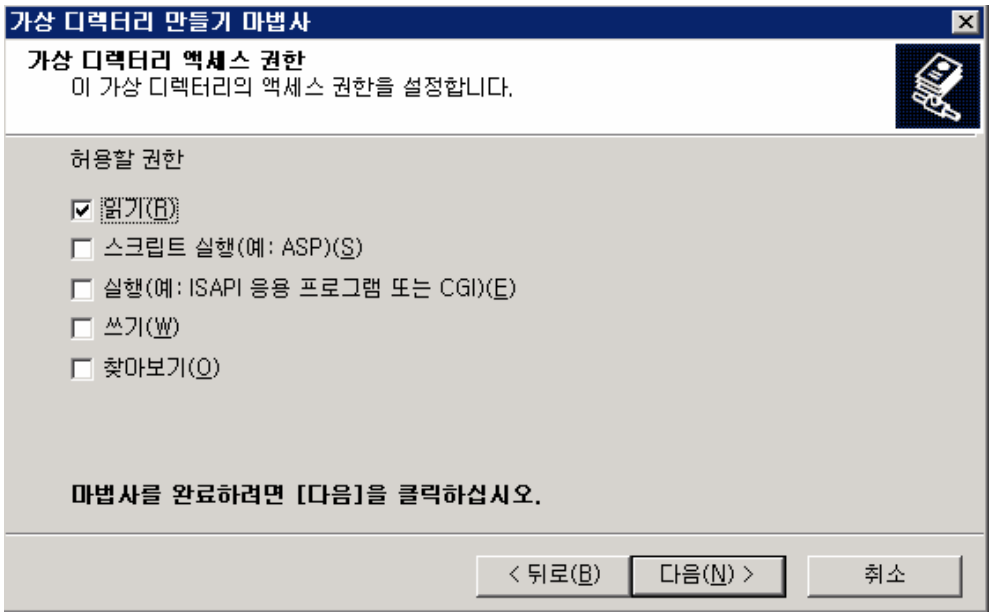




② 가상 디렉터리의 실제 로컬 경로명을 지정합니다.



③ 가상 디렉터리의 권한을 설정합니다. 가상 디렉터리에 html이나 image 파일만 업로드될 것이라면 “읽기” 권한만 있으면 됩니다. 만일 ASP까지 사용한다면 “스크립트 실행”권한까지 체크해야 합니다.



④ 이제 설정이 완료되었습니다.

서버 보안

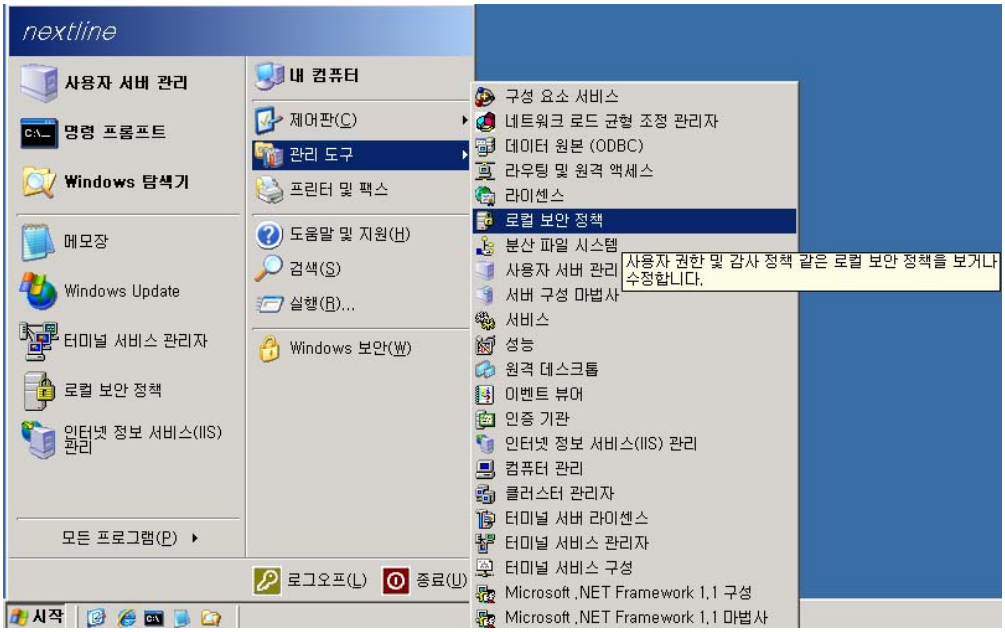
1. 사용자 계정관리

1) 기본 계정 명 변경

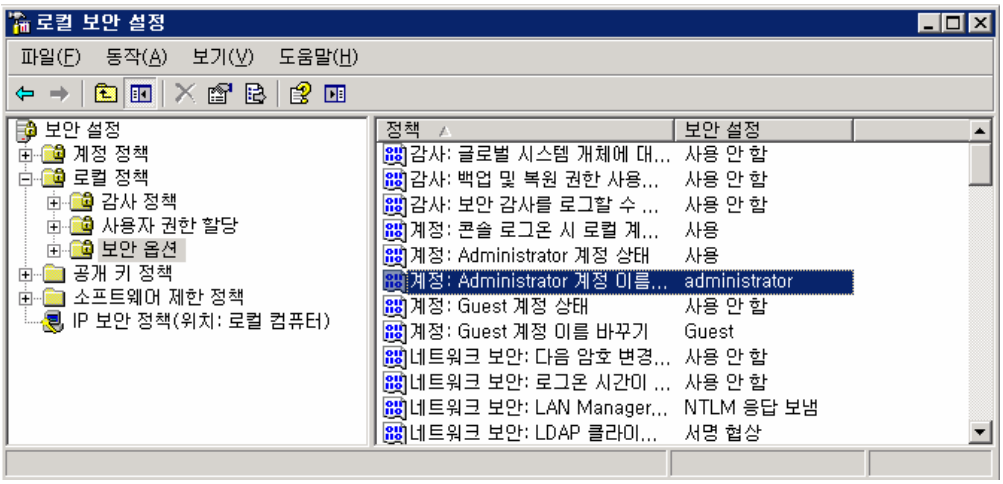
시스템 설치 시 기본적으로 생성되는 두 기본계정의 이름을 변경한다.

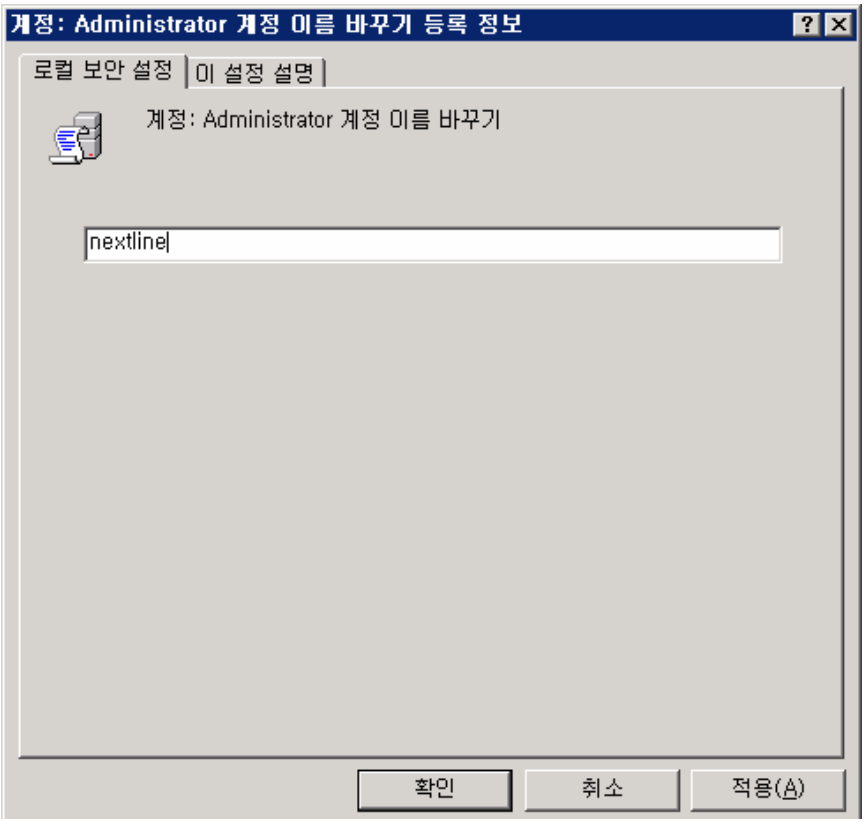
① Administrator 계정 이름 변경

Administrator : [시작]-[관리도구]-[로컬 보안 정책]



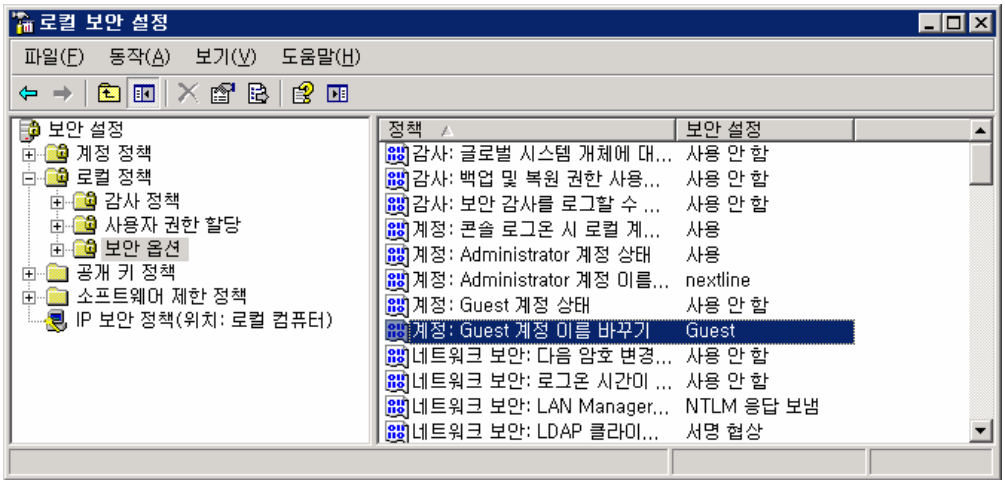
[로컬정책]-[보안옵션]-[계정:Administrator 계정 이름 바꾸기]-[속성]에서 이름을 변경 합니다.

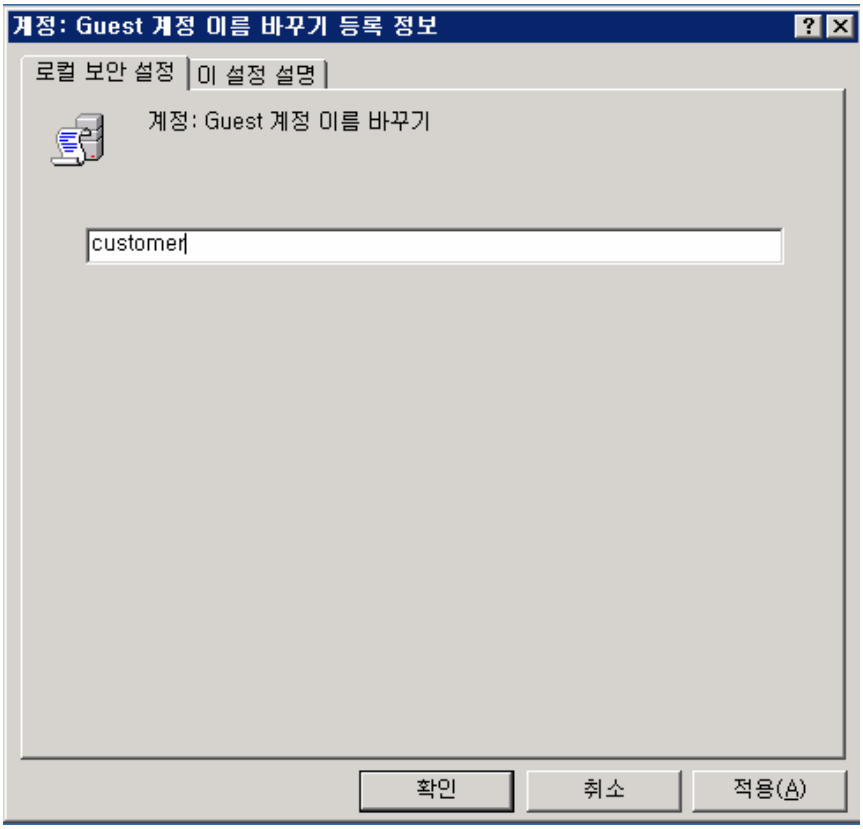




② Guest 계정 이름 변경

Guest : [시작]-[관리도구]-[로컬 보안 정책]-[로컬정책]-[보안옵션]-[계정 : Guest 계정 이름 바꾸기]-[속성]에서 이름 변경

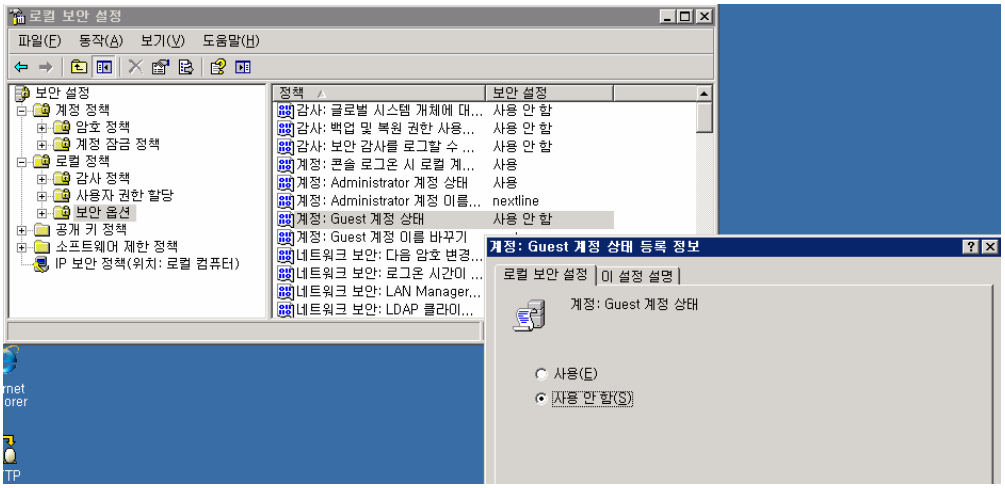




2) Guest 계정 비활성화

Guest 계정은 컴퓨터에 익명 접속을 연결할 때 사용되는 데 이를 비활성화하여 익명 연결을 제한한다.

[시작]-[설정]-[제어판]-[관리도구]-[로컬보안설정]-[로컬정책]-[보안옵션]-[계정:Guest 계정 상태]-[속성] 에서 사용 안함 으로 변경



3) 사용하지 않는 계정 제거

서버에서 사용되지 않는 계정들은 공격자가 이 계정을 이용하여 접근할 수 있으므로 제거를 합니다. 또한 단순하거나 쉬운 패스워드는 무차별 대입 공격(brute force)이나 사전 공격(dictionary attack)에 취약하므로 복잡한 패스워드를 사용합니다.

계정관리는 최소한의 계정과 최소한의 권한만을 부여합니다.

4) 기본 익명 계정(IUSE_Machine)대신 사용자 정의한 계정 사용

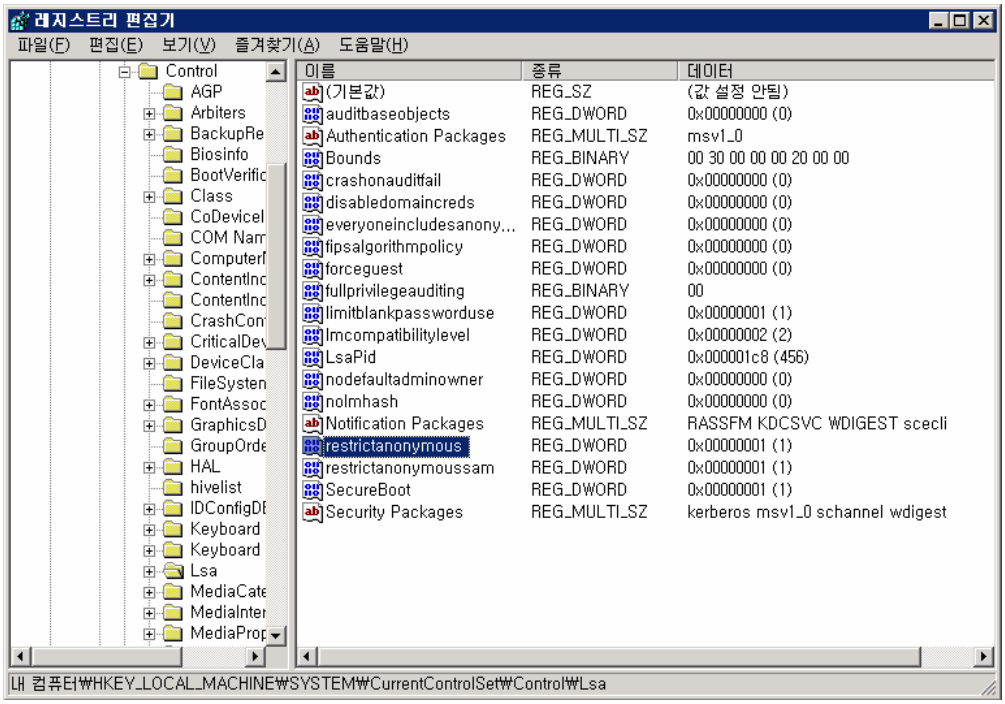
인터넷으로 익명 접근하는 사용자들은 IIS 설치시 기본적으로 생성되는 IUSR_Machine(서버의 NetBIOS명) 계정으로 접근하게 됩니다. 예를 들어 'SMILE' 라는 이름의 서버에는 'IUSR_SMILE' 이라는 계정이 생성됩니다. 이 계정을 비활성화 하고 웹 서버의 익명 접속에 사용할 계정을 직접 재정의 합니다.

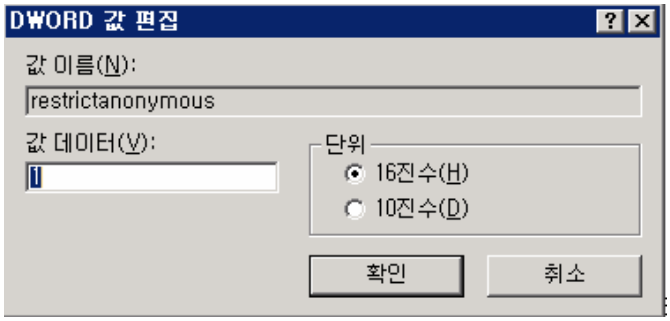
웹 어플리케이션의 기능을 제공하는데 필요한 최소한의 권한을 가지는 계정을 만들고, 인터넷 정보 서비스 관리에서 웹 어플리케이션 별로 직접 정의한 계정을 지정하면 서버상에 여러 개의 웹 사이트를 운영하는 경우 로그 분석에도 용이 합니다.

[인터넷정보서비스관린]-[해당사이트의 속성]-[디렉토리보안]-[인증 및 엑세스]-[편집]- 익명사용자 계정변경

5) 익명 로그온(Null Session) 비활성화

널 세션(Null Session) 접속은 인증을 받지 않은 상태에서 해당 컴퓨터에 접근하는 것을 의미하며, 해커들은 이를 이용해서 원격 컴퓨터의 정보를 제공 받을 수 있고, 특정 권한으로 승격하거나 DoS 공격을 수행할 수도 있습니다. 널 세션 접속을 허용하지 않으려면 레지스트리 편집기([시작]-[실행]-[regedit])를 이용해서 'HKEY_LOCAL_MACHINEWSYSTEMWCurrentControlSetWControlWLsa' 키의 restrictanonymous 값을 '1' 로 설정한다





2. 패스워드 관리

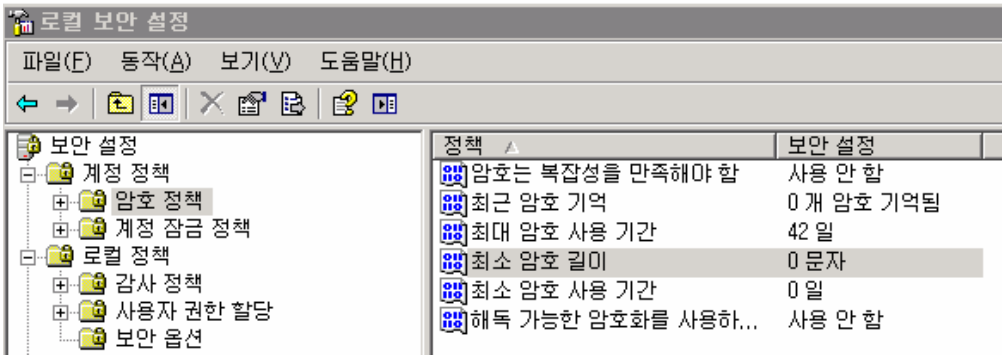
계정 암호에 대한 무차별 대입 공격이나 사전 공격을 막기 위해 암호의 최소 길이나 특수 문자의 사용여부 들을 지정하여 보다 강화된 정책을 사용합니다.

패스워드는 C:₩Windows₩system32₩config₩SAM 파일에 저장되며 운영체제가 동작중에는 시스템 계정 외에는 접근이 금지됩니다.

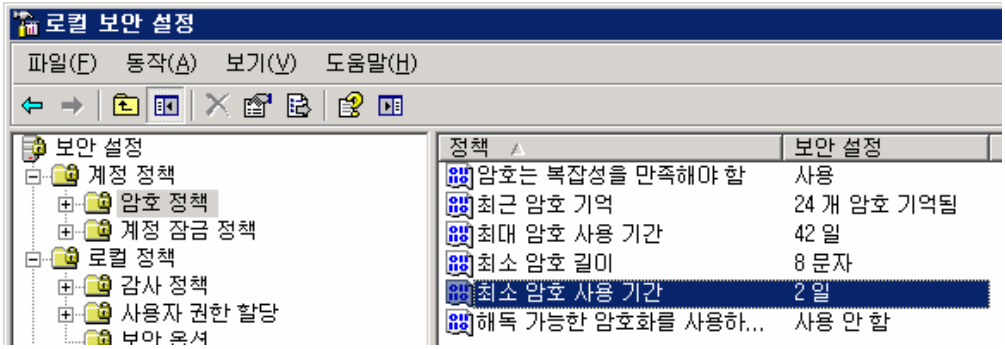
1) 암호정책

[시작]-[제어판]-[관리도구]-[로컬보안설정]-[계정정책]-[암호정책]

기본 정책은 아래와 같습니다.



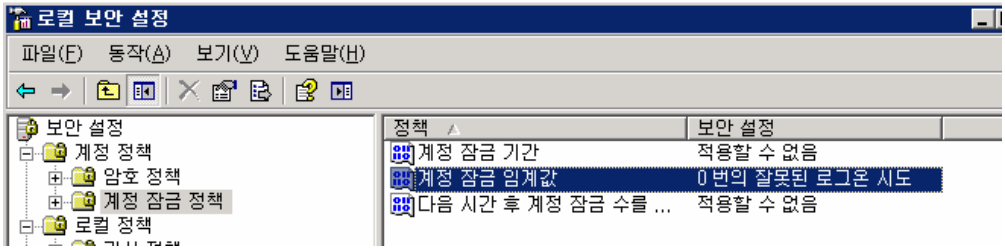
권장 설정 사항은 아래와 같습니다.



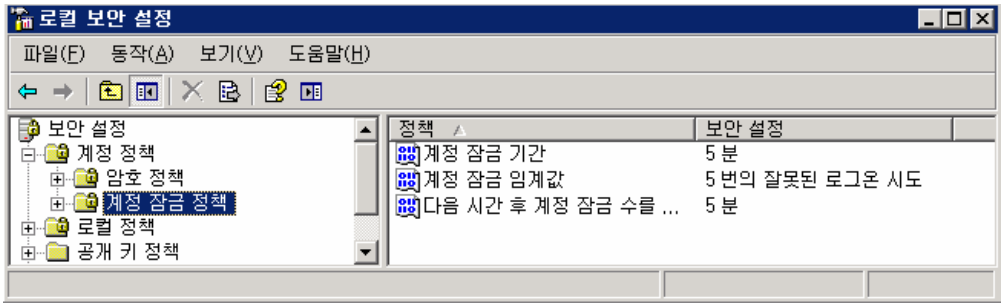
2) 계정 잠금 정책

[시작]-[제어판]-[관리도구]-[로컬보안설정]-[계정정책]-[계정 잠금 정책]

기본 정책은 아래와 같습니다.



권장 설정 사항은 아래와 같습니다.



3. 시스템 실행명령어 권한 설정

C:₩Windows 밑에 explorer.exe 와 링크파일인 explorer 의 속성을 선택한 뒤 [보안]탭에

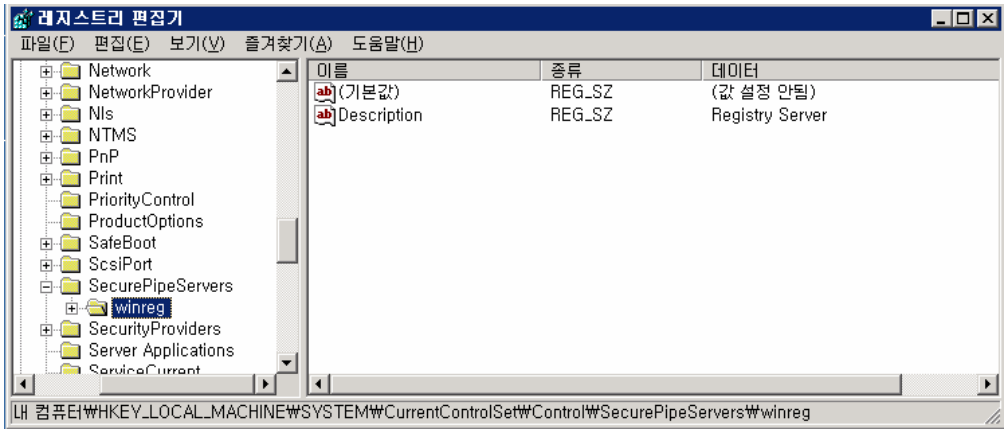
서 Administrator을 제외하고 나머지 계정은 삭제한다. 특히 바이러스의 경우 해당 Explorer.exe 를 변경을 시키거나 복제를 시켜 윈도우 사용에 지장을 초래하거나 사용자가 모르는 불법적인 코드가 explorer.exe에 첨부될 수 가 있으니 권한 제조정을 통해 바이러스 감염 및 침입자의 이용으로부터 막도록 합니다.

C:₩Windows₩system32₩cmd.exe 등의 시스템 명령어도 Administrator 계정 외에는 접근을 제한한다. 실제적으로 서버관리자를 제외하고는 대부분의 사용자들은 위의 파일을 실행시킬 필요성이 없습니다. 각종 웜 바이러스 및 코드 레드의 경우 cmd.exe 파일을 복제하여 권한을 획득하는 경우가 다반사이기 때문에 근본적으로 접근자를 제외하고는 나머지 권한은 제거해주는 것이 좋습니다.

예) %systemroot%₩system32₩cmd.exe -> [속성]-[보안]탭 -> Administrator 외의 계정 제거

4. 레지스트리 보호

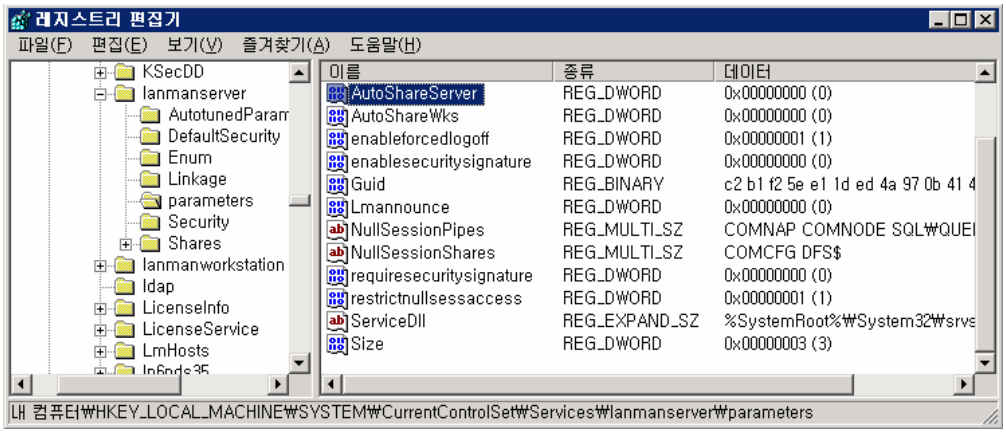
레지스트리의 원격 액세스 권한은 관리자에게만 부여되어 있는지 확인합니다. HKEY_LOCAL_MACHINE₩System₩CurrentcontrolSet₩Control₩SecurePipeServers₩winreg 의 키값이 생성 되어 있는지, 사용권한은 Administrator외의 사용자나 그룹이 등록되어 있지는 않는지 확인을 합니다.



5. 공유

서버에서 사용되지않는 공유를 제거하고 사용중인 공유 자원에 대해서는 NTFS권한을 부여하여 자원을 보호합니다. 특히 기본적으로 공유가 생성될 때 모든 사용자들에게 모든 권한이 부여되므로 NTFS권한을 적용해서 필요한 사용자에게만 접근을 허용하도록 관리해야 합니다.

또한 관리목적에서 사용되는 C$, ADMIN$와 같은 관리 공유를 사용하지 않는다면 제거하는 것을 권장됩니다. 관리 공유를 사용하지 않으려면 레지스트리 편집기를 이용해서 'HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩lnmanserver₩parameters' 키에 AutoShareServer와 AutoShareWks 값을 REG_DWORD로 만들고 '0' 으로 설정 합니다.



6. 보안패치 및 서비스 팩 설치

윈도우 업데이트는 주기적으로 실시하여 줍니다.

7. 패킷 필터링

IPSEC(인터넷 프로토콜 보안)을 이용한 필터링은 InBound와 OutBound 되는 패킷 모두에 eoo서 제어가 가능 하므로, 서버관리자도 모르는 사이에 자신의 서버가 다른 서버를 공격하는데 이용되는 것을 방지 할 수 있습니다. 액티브 디렉토리로 바꾼 사용자는 로컬 보안 정책(secpol.msc) alc 도메인 보안정책(dompol.msc), 도메인 컨트롤러 보안정책 이 2가지가 추가로 생기게 되는데 특히 로컬 보안 정책보다 도메인 보안 정책이 우선 순위가 있어 액티브 디렉토리 사용자는 도메인 보안 정책에서 IPSec을 구성합니다.

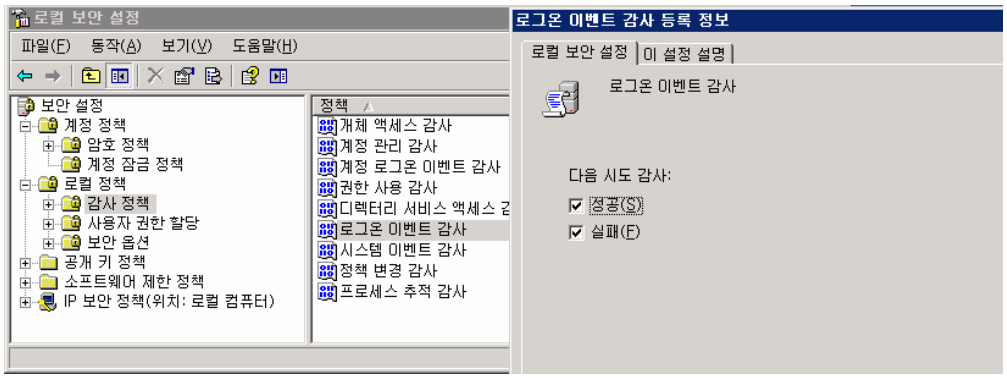
8. 감사 관리

감사는 시스템 공격을 막지는 못하지만 진행중인 공격이나 침입자를 인식하고 공격의 흔적을 추적하는데 많은 도움을 줍니다. 웹 서버의 감사정책 수준을 높이고 HTFS 권한으로 로그 파일을 보호함으로써 공격자가 로그파일을 지우거나 변조하는 것을 방지하는 것도 필요합니다.

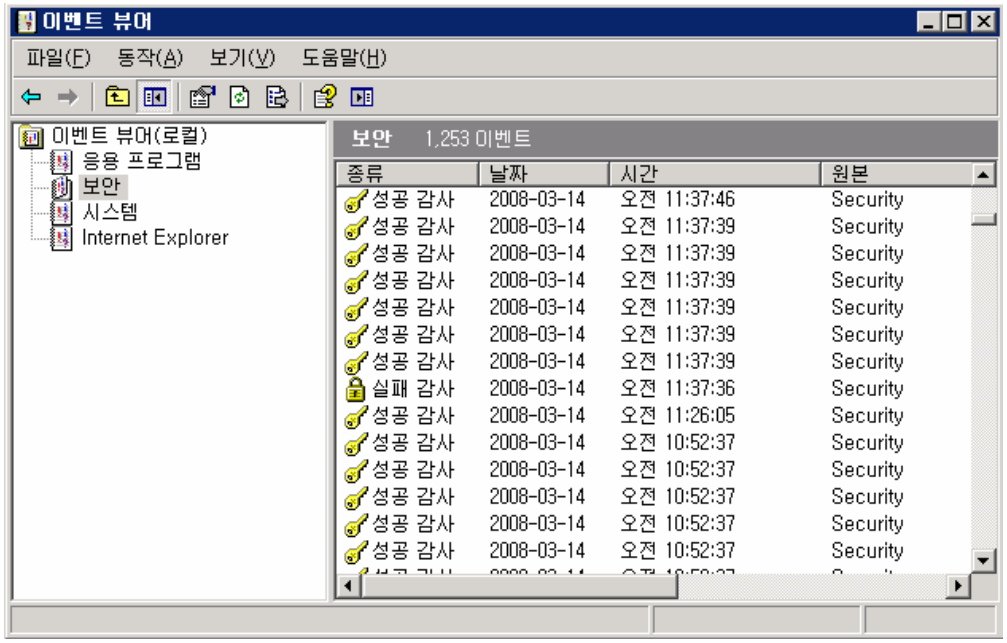
1) 로그인 실패 로그 기록

시스템에 로그인 하는데 실패한 이벤트에 대해서는 반드시 로그를 기록해야 합니다. 로그를 통해서 암호에 대한 무차별 대입 공격이나 사전 공격의 흔적을 찾을 수 있으며 공격자가 어떠한 계정으로 접근을 시도했는지도 알 수 있습니다.

[시작]-[관리도구]-[로컬 보안 설정]-[로컬 정책]-[감사 정책]-[계정 로그온 이벤트 감사]-[속성]-[실패] 항목에 체크합니다.



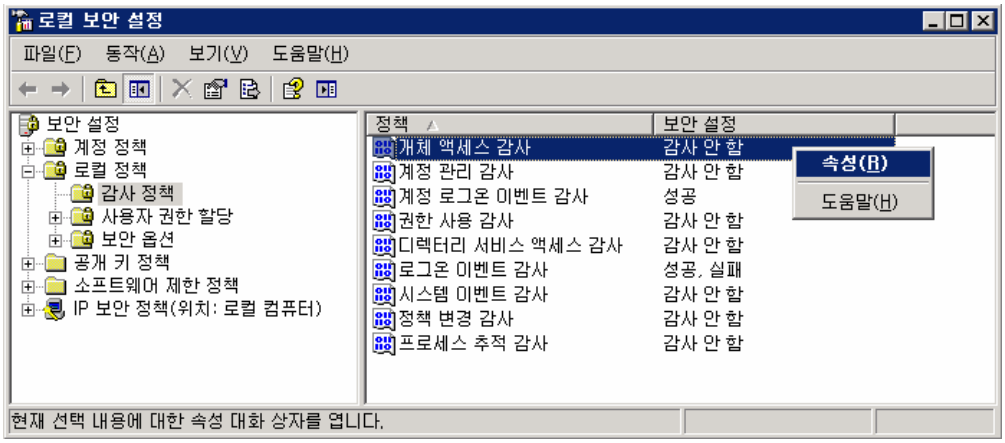
이후에 발생하는 로그인 실패 이벤트에 대한 내역은 [시작]-[관리도구]-[이벤트 뷰어]-[보안]로그 목록에서 확인 가능합니다.

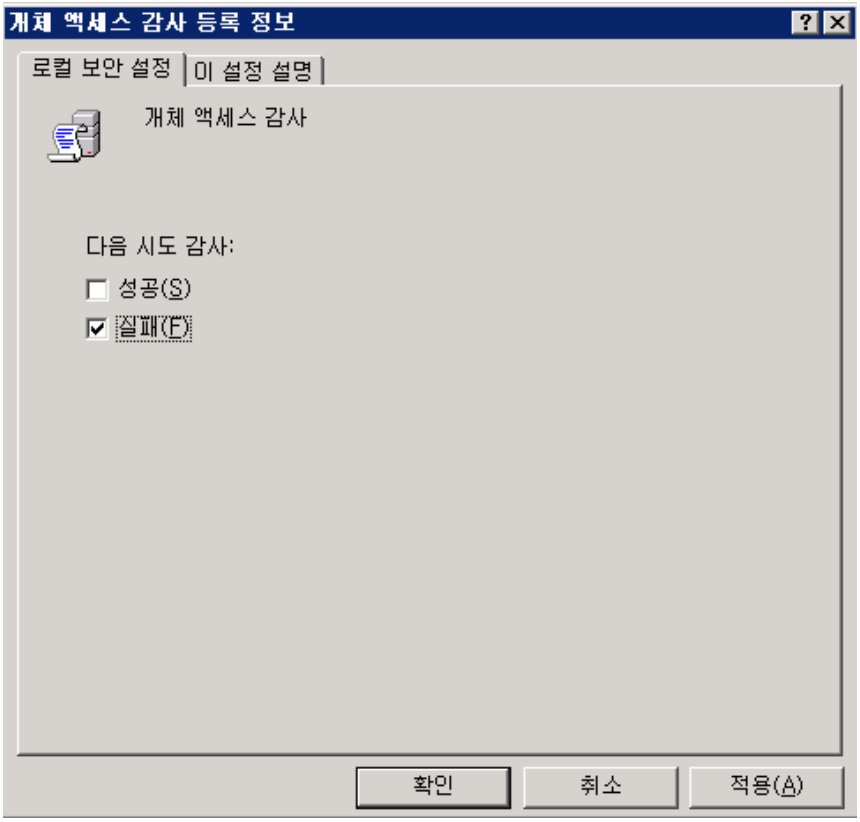


2) 개체 접근 로그 실패 기록

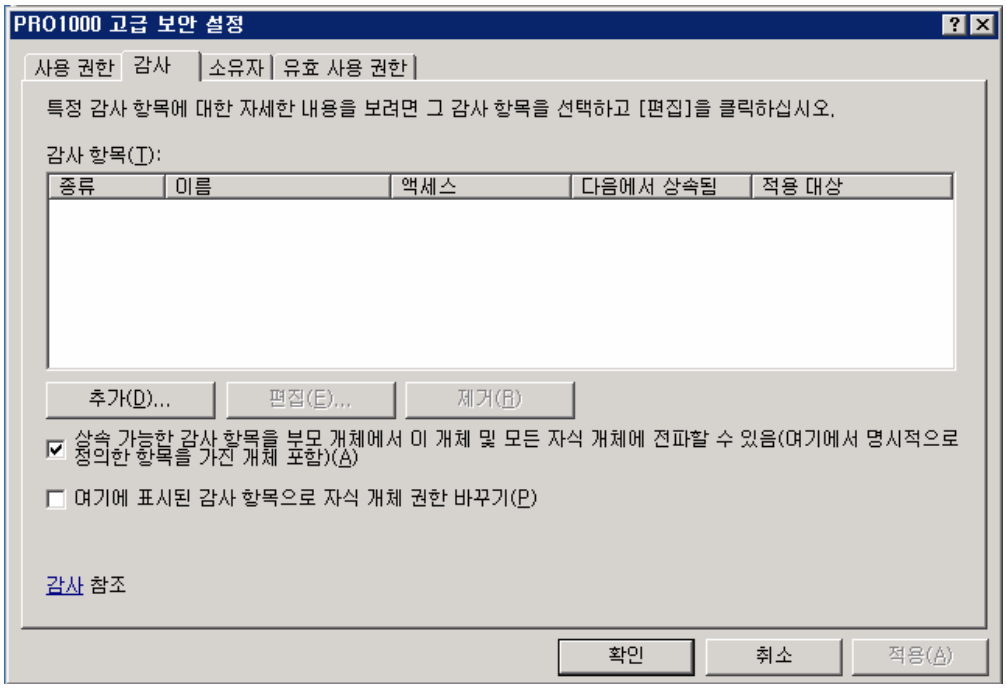
파일이나 폴더 등의 개체에 대한 악의적인 접근 시도에 대하여 감사기록을 합니다. 개체 액세스에 대한 감사기능은 해당 디스크 볼륨이 NTFS파티션일 경우에만 사용할 수 있습니다. NTFS 파일 시스템은 FAT와 비교했을 때 파일 및 폴더 단위의 권한 부여 및 관리가 용이하므로 웹 서버의 자원이 저장되는 파티션은 NTFS를 사용하는 것이 좋습니다.

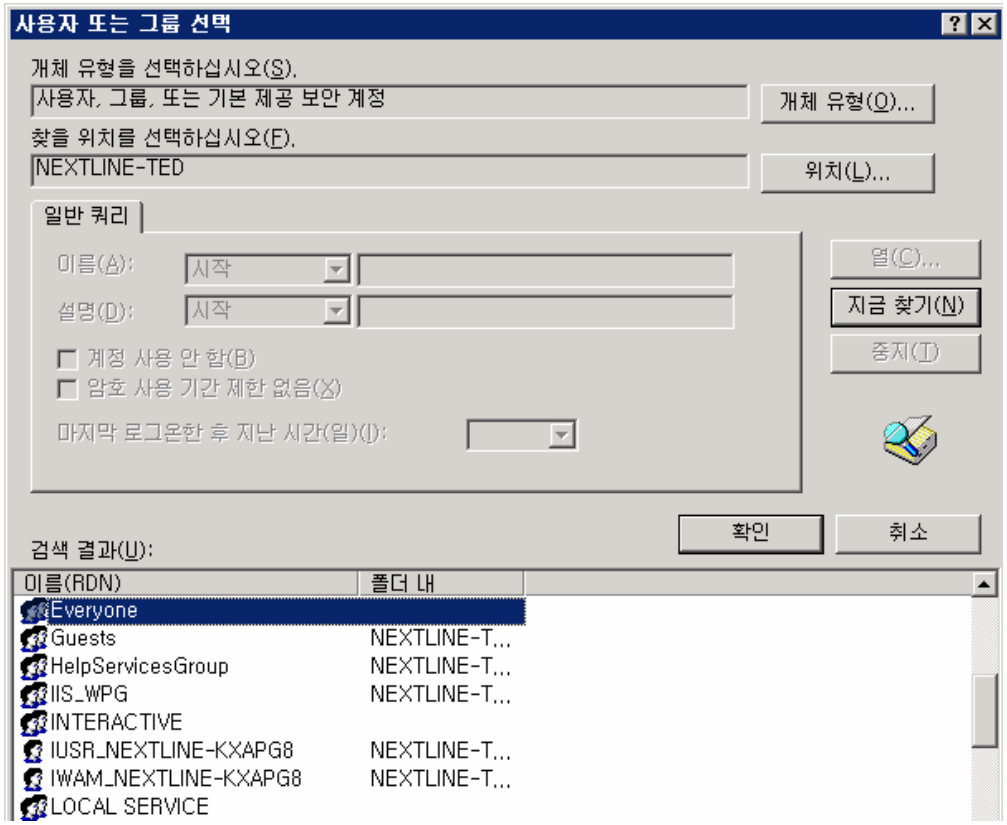
① [시작]-[관리도구]-[로컬 보안 설정]-[감사 정책]-[개체 액세스 감사]-[속성]-[실패] 항목에 체크 합니다.

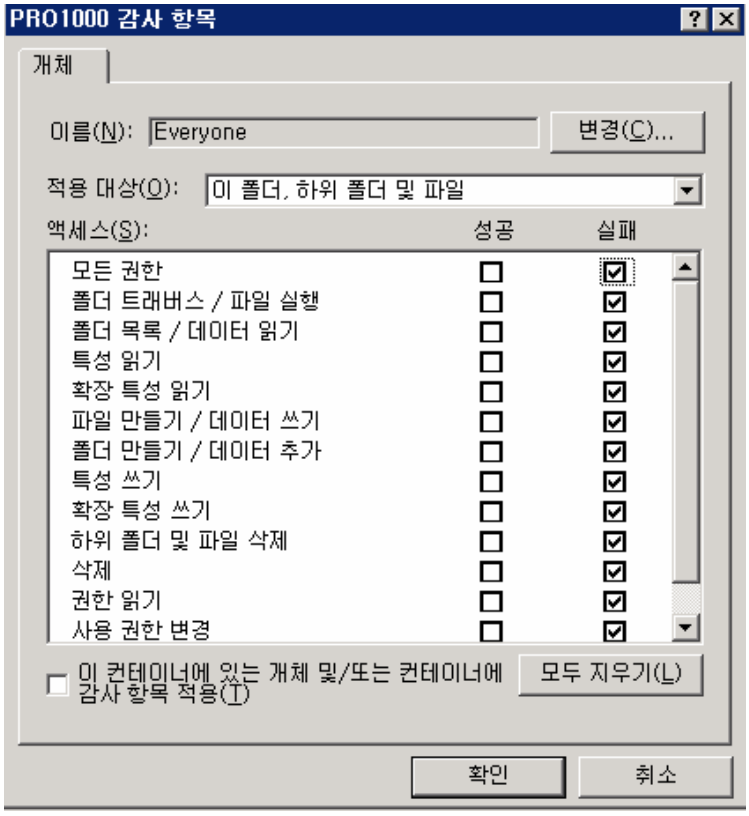


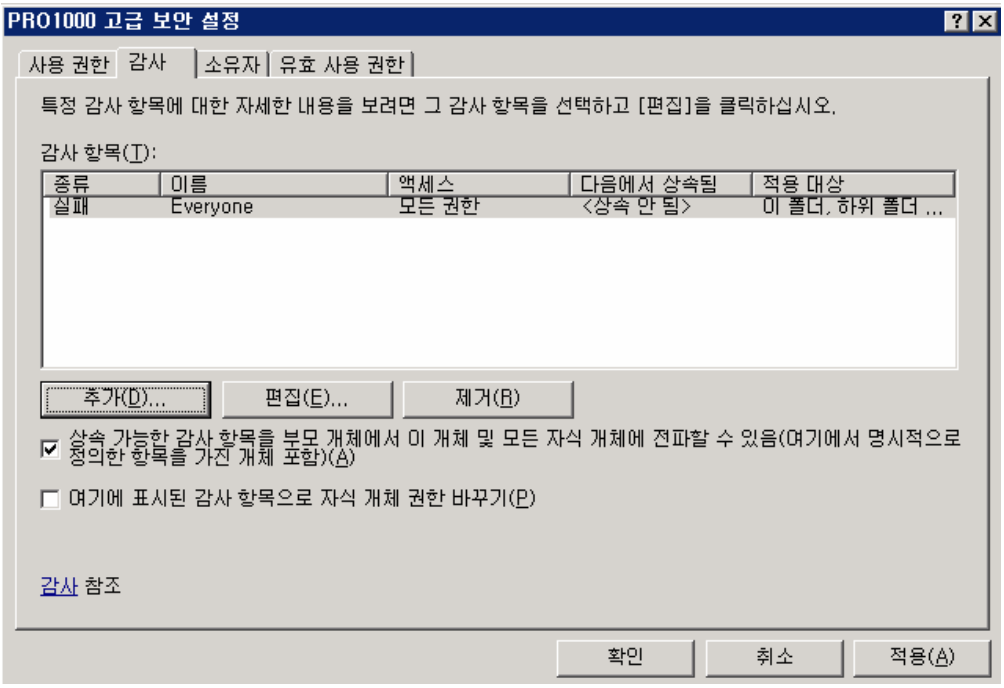


② 감사하려는 대상 폴더나 파일을 탐색기에서 선택 [속성]-[보안]탭-[고급]-[감사]탭-[추가]- ‘Everyone’ 그룹에 대한 모든 실패 이벤트를 기록하도록 감사 항목을 설정 합니다.


PRO1000 고급 보안 설정
사용 권한
감사
소유자
유효 사용 권한
특정 감사 항목에 대한 자세한 내용을 보려면 그 감사 항목을 선택하고 [편집]을 클릭하십시오.
감사 항목(T):
종류
이름
액세스
다음에서 상속됨
적용 대상
추가(D)...
편집(E)...
제거(R)
상속 가능한 감사 항목을 부모 개체에서 이 개체 및 모든 자식 개체에 전파할 수 있음(여기에서 명시적으로 정의한 항목을 가진 개체 포함)(A)
여기에 표시된 감사 항목으로 자식 개체 권한 바꾸기(P)
감사 참조
확인
취소
적용(A)


사용자 또는 그룹 선택
개체 유형을 선택하십시오(S).
사용자, 그룹, 또는 기본 제공 보안 계정
개체 유형(O)...
찾을 위치를 선택하십시오(F).
NEXTLINE-TED
위치(L)...
일반 쿼리
이름(A):
시작
설명(D):
시작
계정 사용 안 함(B)
암호 사용 기간 제한 없음(X)
마지막 로그온한 후 지난 시간(일)(I):
열(C)...
지금 찾기(N)
중지(T)
확인
취소
검색 결과(U):
이름(RDN)
폴더 내
Everyone
Guests
NEXTLINE-T...
HelpServicesGroup
NEXTLINE-T...
IIS_WPG
NEXTLINE-T...
INTERACTIVE
IUSR_NEXTLINE-KXAPG8
NEXTLINE-T...
IWAM_NEXTLINE-KXAPG8
NEXTLINE-T...
LOCAL SERVICE





9. IIS 로그파일 위치 변경 및 NTFS 권한 적용

기본적으로 IIS 로그파일은 '%systemroot%₩system32₩LogFiles'에 사이트 별로 저장되는데 이를 다른 폴더에 저장하거나 이름을 변경함으로써 공격자가 로그 파일을 변경하거나

삭제하는 것을 어느 정도 막을 수 있습니다. 가능하면 이 로그 파일이 저장되는 디렉토리를 웹 사이트가 외치한 디스크와 다른 볼륨을 사용하고 NTFS 권한을 Administrator(모든 권한), System(모든 권한)로 지정하여 다른 계정에서 로그 파일에 접근하는 것을 막는 것이 좋습니다.
[시작]-[관리도구]-[인터넷정보서비스관리]-[각 웹사이트]-[속성]-[웹사이트]탭-로깅사용 [속성]-로그파일 디렉토리 변경

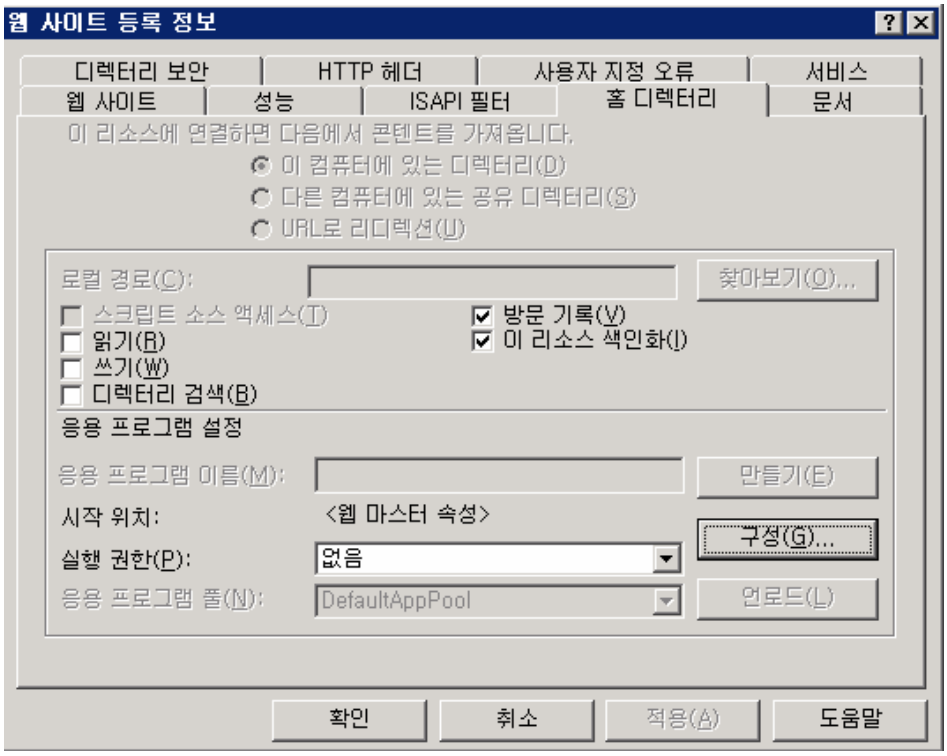
10. IIS 보안
1) IIS 보안 점검 항목
• 가상 디렉토리에 대한 적절한 ACL 설정
• IIS 로그 파일에 대한 ACL 설정
• 로깅 사용
• 사용하지 않는 예제 프로그램 삭제
• 가상 디렉토리 삭제
• 사용하지 않는 스크립트 매핑 삭제

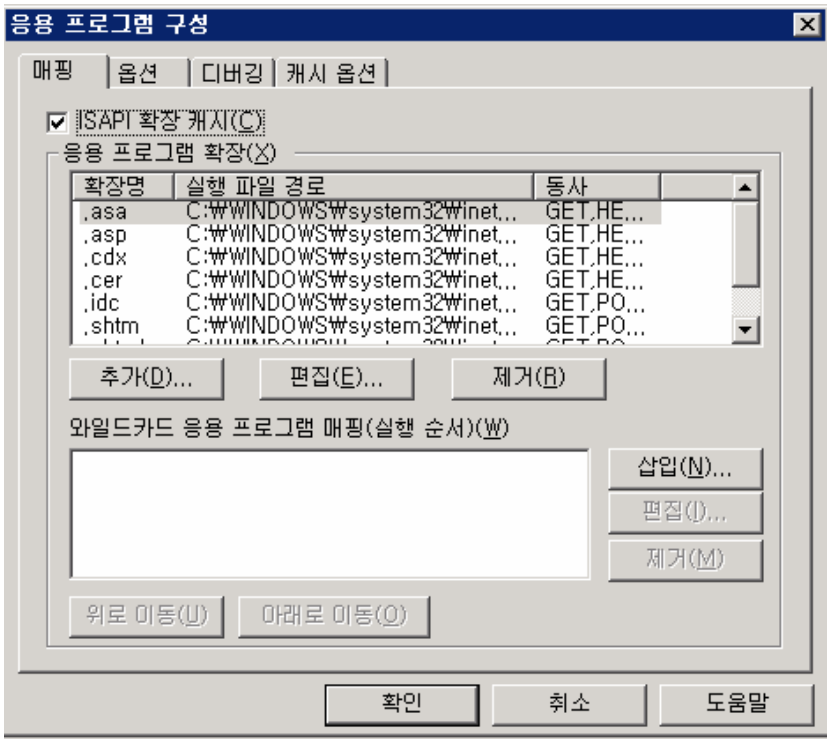
2) 불필요한 폴더 제거
• IIS 예제 : iissamples
• IIS 설명서 : iishelp
• 데이터 액세스 : MSDAC

3) 파일 권한
CGI(.exe, .dll, .cmd, .pl), 스크립트파일(.asp, .aspx), Include 파일(.inc, .shm, .shtml)등의 파일에는 Everyone에게 권한을 주지 않습니다.
일반 파일(.txt, .gif, .jpg, .html)에는 Everyone 에게 읽기 권한을 부여합니다.파일 종류에 따른 파일 권한을 설정할 수 있도록 각각 종류에 디렉토리를 생성하여 관리합니다.

삭제됨:

4) 불필요한 매핑 제거
전체 웹사이트에 적용시 : [인터넷정보 서비스관리]-[웹사이트]-[속성]-[홈디렉토리]탭-[구성]-[매핑]탭
개별 적용시에는 각 사이트의 매핑탭에서 설정합니다.
매핑탭을 보면 많은 수의 파일매핑이 되어 있는데 실제로 웹 서버에서 사용하는 .asp, .asa를 제외하고는 모두 제거하는 것이 좋습니다. 적용 대상서버가 웹 서버가 아닌 파일 서버 및 DB전용의 서버라면 모든 매핑파일 자체가 필요가 없습니다.
* 제거 권고 매핑
• 웹기반 암호 재설정 : .htr
• IIS커넥터 : .idc
• Server Side Includes : .stm, .shtm, .shtml
• 인쇄 : .printer
• 인덱스 서버 : .htw, .ida, .idq



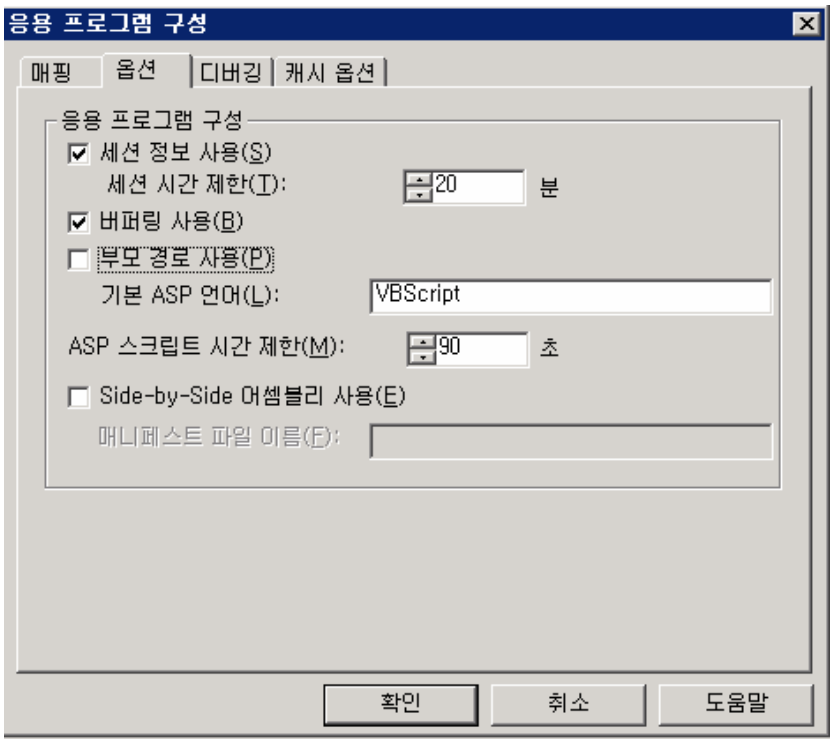


5) 상위 경로 접근 제거

시스템 파일 및 명령어를 삽입하기 위해 ../../../ 등의 패턴 입력을 제한합니다.

[시자]-[관리도구]-[인터넷정보서비스관리]-[웹사이트]-[속성]-[홈 디렉토리]탭-[구성]-[옵

션]탭-[부모경로사용]체크 해제



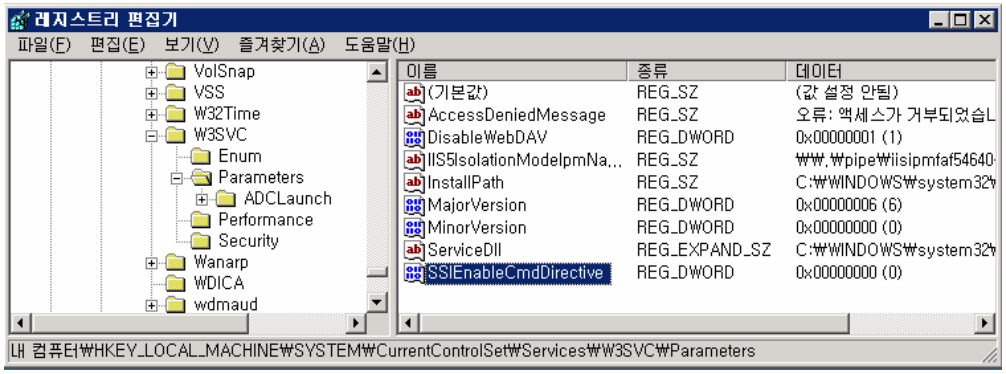
6) 컨텐츠 디렉토리 권한

[시작]-[관리도구]-[인터넷정보서비스관리]-[웹사이트]-[속성]-[홈 디렉토리]탭-읽기, 방문기록, 이리소스색인화 외에는 체크하지 않습니다. 즉 읽기 정보의 권한만 할당 합니다.

7) #exec 명령쉘 호출 중지

명령어가 웹서버에서 임의의 명령을 호출하도록 사용될 수도 있습니다. IIS는 디폴트로 이것이 중지되어 있으며 이를 가능하게 하는 레지스트리 키가 '0"로 셋팅되어 있는지 확인합니다.

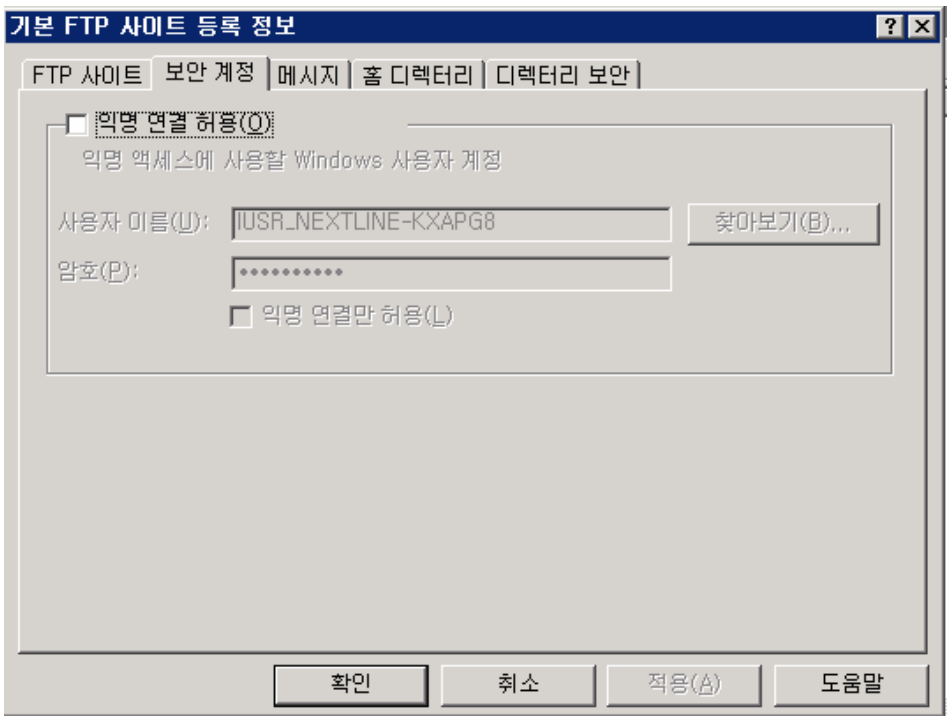
HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Service₩W3SVC₩Parameters₩SSIEnableCmdDirective



11. FTP 익명 접속 거부

FTP 서비스에 익명접속을 허용하지 않도록 설정합니다.

[시작]-[관리도구]-[인터넷정보서비스관리]-[해당FTP 사이트]-[속성]-[보안계정]-[익명연결 허용]체크 해지-[적용]-[확인]



12. 네트워크 보안

1) NetBIOS 비활성화

NetBIOS는 별개의 컴퓨터 상에 있는 애플리케이션들이 근거리통신망 내에서 서로 통신할 수 있게 해주는 프로토콜로서 Windowns에 의해 채택되어 있습니다. 만약 웹 서버에서 네트워크를 통한 다른 컴퓨터와의 공유가 필요없다면 NetBIOS를 제거함으로써 DDos(Distributed Denial of Service) 공격이나 호스트 열거(host enumeration)에 대한 위험 요소를 줄일 수 있습니다. NetBIOS는 다음과 같은 포트를 사용합니다.

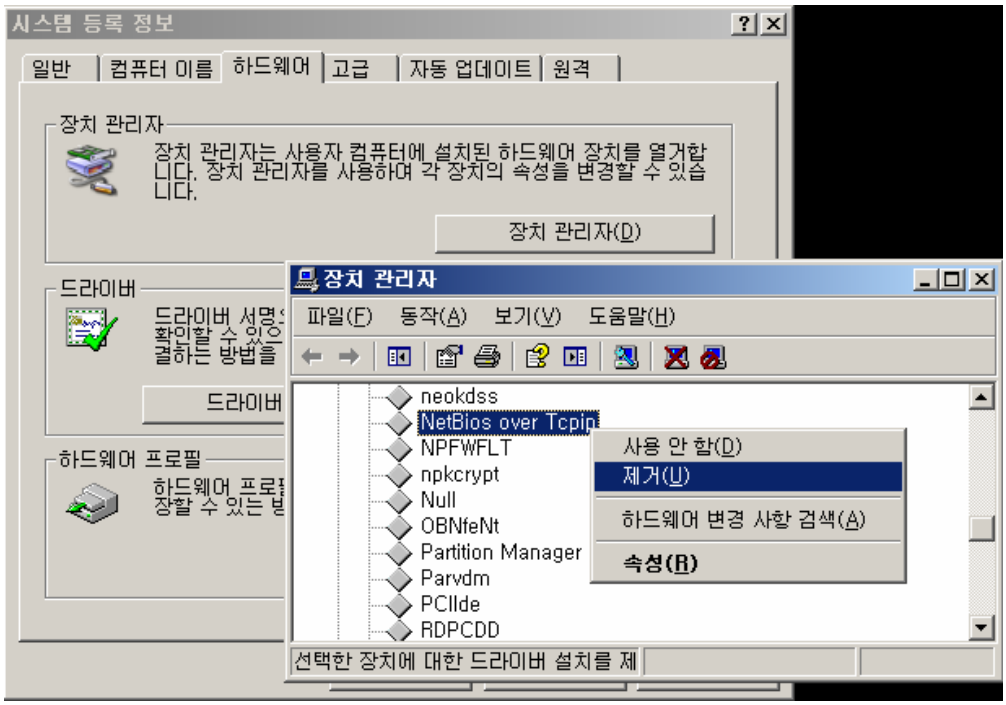
TCP/UDP 137번 (NetBIOS name service)

TCP/UDP 138번 (NetBIOS datagram service)

TCP/UDP 139번 (NetBIOS session service)

TCP/UDP에서 NetBIOS를 비활성화하는 방법은 아래와 같습니다.

[내 컴퓨터]-[속성]-[하드웨어]탭-[장치관리자]-[보기]메뉴-[숨김 장치표시]-[비 플러그 앤 플레이 드라이버]-[NetBios over Tcpip]-[제거]



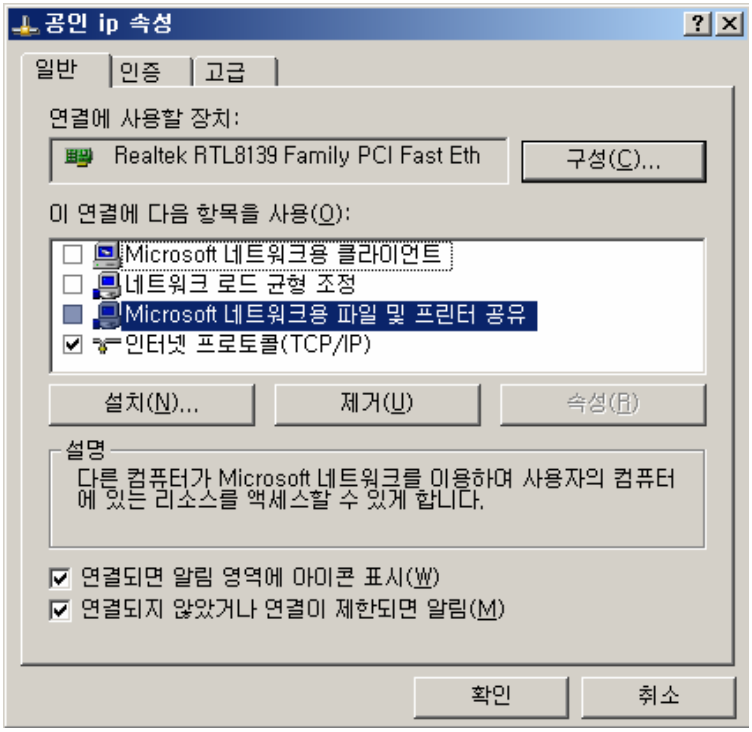
2) SMB 비활성화

SMB(Session Message Block) 프로토콜은 Windows에서 디스크와 프린터를 네트워크 상에서 공유하는데 사용됩니다. SMB는 다음과 같은 포트를 사용합니다.

TCP 139번 포트

TCP 445번 포트

SMB를 비활성화 하려면 다음과 같은 방법으로 TCP/IP에서 SMB를 언바인드 시키면 됩니다. [내 네트워크 환경]-[속성]-[로컬영역연결]-[속성]-[Microsoft 네트워크용 클라이언트] 와 [Microsoft 네트워크용 파일 및 프린터 공유] 항목의 체크 해제 - [확인]



3) TCP Stack 강화하기

레지스트리로 제공되는 TCP/IP와 관련된 매개변수의 설정을 변경함으로써 SYN Floods, ICMP, SNMP 공격과 같은 네트워크 레벨에서의 DoS(서비스 거부)공격을 막을 수 있습니다.

① SYN Floods공격 방어

SYN 공격은 TCP/IP 에서 연결을 맺는 매카니즘의 취약점을 대상으로 하며, 공격자는 TCP의 SYN 요청을 위도적으로 발생시키는 프로그램을 이용해서 서버상의 커넥션 큐를 넘치게 만듭니다. SYN Floods 공격으로부터 웹 서버를 보호하려면 레지스트리 편집기를 이용해서 HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩services₩Tcpip₩Parameters 키에 다음과 같은 항목에 대한 값을 지정하면 됩니다.

항목	권장	범위	설명
SynAttackProtect	2	0-2(활성)	SYN공격에 대한 보호 기능을 활성화시킨다.SYN-ACKS의 재전송을 적게 조절함으로써 SYN 공격을 막는다. TcpMaxHalfOpen나 TcpManHalfOpenRetried 설정과 함께 사용되어야 한다
TcpMaxPortsExhausted	5	0-65535	SYN Floods 공격이 발생했음을 판단하는데 기준이 되는 TCP 연결의 최대값
TcpMaxHalfOpen	500	100-65535	SYN 공격이 동작하기 전에 SYN_RCVD 상태에서 연결을 허용할 최대값. 이를 적용하려면 먼저 SynAttackProtect가 활성화되어 있어야 한다.
TcpManHalfOpenRetried	400	80-65535	SYN 공격이 동작하기 전에 SYN_RCVD 상태에서 연결을 허용할 최대값. SYN_RCVD는 SYN 공격에 대한 방어가

			동작하기 전에 적어도 한번의 SYN 플래그를 재전송한다. 이를 적용하려면 먼저 SynAttackProtect가 활성화되어 있어야 한다.

② AFD.SYS 설정

FTP 서버 및 웹 서버와 같은 Windows 소켓 응용 프로그램에서는 연결 시도를 Afd.sys에서 처리합니다. Afd.sys도 HKEY_LOCAL_MACHINEWSYSTEMWCurrentControlSetWServicesWAFDWParameters 키에 대하여 다음 항목을 적용합니다.

항목	권장	범위	설명
EnableDynamicBacklog	1	0(사용안함) 1(사용)	많은 양의 SYN_RCVD 연결에 대해서 능동적으로 대처할 것이지에 대한 AFD.SYS 기능의 활성화 여부를 지정한다.
MinimumDynamicBacklog	20	0-4294967295	Listening endpoint에서 허용하는 접속의 최소 수를 저정한다. 접속수가 설정된 값 이하가 되면 새로운 스레드에서 추가 연결을 생성한다.
MaximumDynamicBacklog	20000	0-4294967295	Listening endpoint에서 허용하는 'Quansi-free' 연결의 최대수를 지정한다. 'Quansi-free'는 SYN_RCVD 상태의 연결과 free connections를 더한 값이다.
DynamicBacklogGrowthDelta	10	0-4294967295	추가적인 연결이 필요할 때 생성되는 free connections의 수를 지정한다.

③ ICMP 공격 방어

ICMP(Internet Control Message Protocol)는 호스트 서버와 인터넷 게이트웨이 사이에서 메시지를 제어하고 에러를 알려주는 프로토콜입니다. 대표적인 예로 ping 명령어는 인터넷 접속을 테스트하기 위해 ICMP를 사용합니다.

HKEY_LOCAL_MACHINEWSYSTEMWCurrentControlSetWservicesWAFDWParameters 키에서 다음 항목을 설정합니다.

항목	권장	범위	설명
EnableICMPRedirect	0	0(사용안함) 1(사용)	이 값을 0으로 설정함으로써 ICMP 리디렉트 패킷을 수신했을 때 호스트 경로를 생성하지 않게 하여 부하를 줄일 수 있다

④ SNMP 공격 방어

SNMP(Simple Netword Management Protocol)는 네트워크를 관리하기 위한 프로토콜로서 망 관리를 위해 SNMP manager와 agent가 서로 통신하는데 사용됩니다. 그러나 SNMP을 악용하면 네트워크를 연결 장비를 무력화시킬 수 있을 뿐만 아니라 장비를 직접 조작하거나 서비스 거부 공격으로 웹사이트를 마비시킬 수 있습니다.

항목	권장	범위	설명
EnableDeadGWDetect	0	0(사용안함 1(사용)	공격자가 2차 게이트웨이로 스위칭하는 것을 막는다. 이값을 1로 설정하면 TCP는 dead-gataway 탐지를 수행한다

13. 터미널 서비스 포트 변경하기

윈도우 서버에 설치된 터미널서비스의 포트번호를 변경하여 사용합니다.

변경 후 엔 IPSEC등에 변경된 포트정보를 꼭 수정합니다.

1) 포트 번호 변경

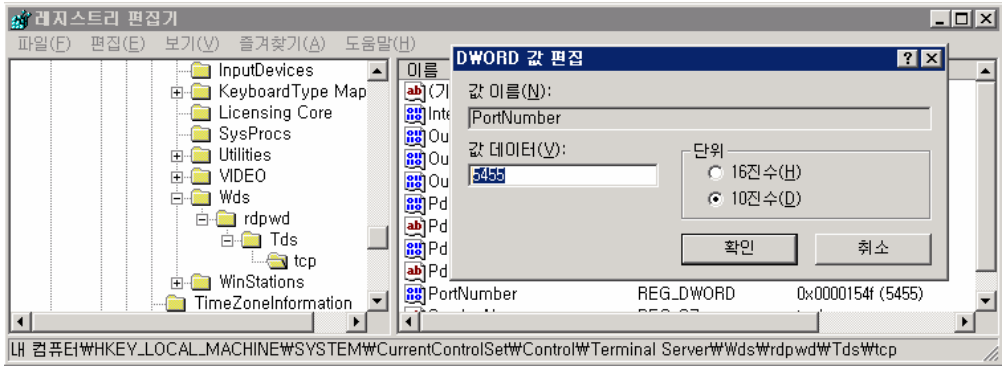
① [시작]-[실행]-[redgeid]입력-[확인]을 눌러 레지스트리 편집기를 실행 합니다.

②

HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩TerminalServer₩Wds₩rdpwd₩Tds₩tcp

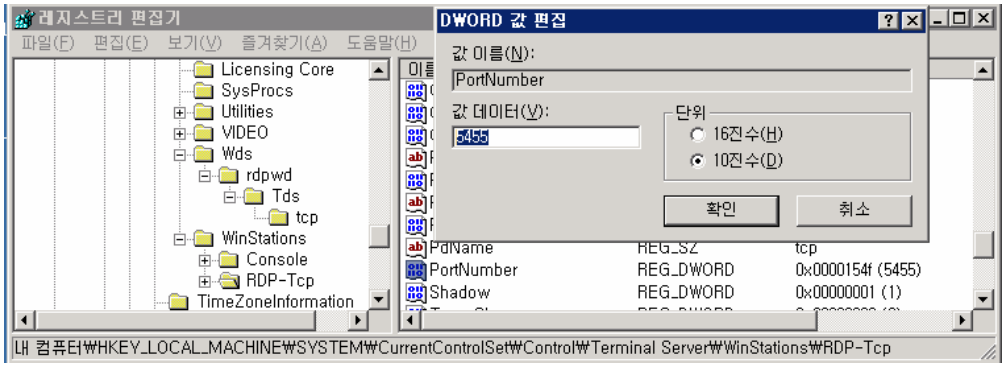
로 이동합니다.

③ PortNumber REG_DWORD 0x00000d3d(3389) 수정모드에서 10진수를 선택하고 원하는 포트번호를 입력합니다.



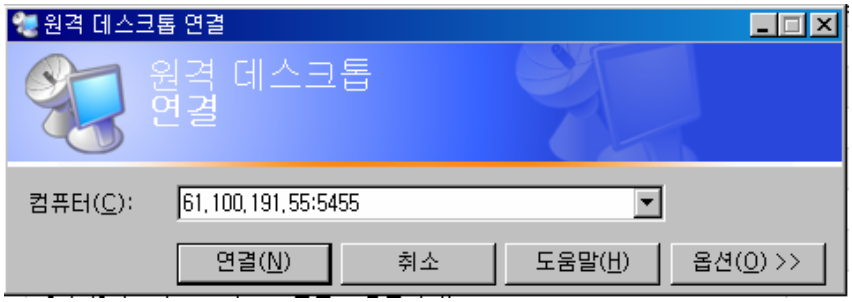
④ HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩TerminalServer₩WinStations₩RDP-Tcp로 이동합니다.

⑤ PortNumber REG_DWORD 0x00000d3d(3389) 수정모드에서 10진수를 선택하고 원하는 포트번호를 입력합니다.



2) 클라이언트에서 서버 접속하기

원격데스크탑 연결창에서 '서버주소:변경된포트번호'를 입력 후 접속합니다.



Nextline 스크립트 보안 설치사항

1 레지스트리 수정내용

1) os/2, posix 관련 레지스트리 삭제

2) rds(remote data services) 레지스트리 삭제

3) 관리공유(admin$,c$,ipc$,fax$,print$ 등) 사용중지

- 기본 공유되어있는 폴더의 사용중지

4) null session 사용중지

- 기본 등록된 사용자외 null 세션 사용중지

5) webdav 사용중지

- 웹폴더 사용중지

6)웹으로부터 command shell(cmd.exe) 접근제한

- 웹에서 cmd 명령어 사용금지, Administrator 만 권한을 소유함

7) internet explorer 자동완성 설정 제거

- 인터넷 익스플로워의 자동완성 기능 사용금지

8) syn 공격시 차단

- sync 공격시 차단설정

9) icmp 공격시 차단

- icmp 공격시 차단설정

10) snmp 공격시 차단

- snmp 공격시 차단설정

11) afd.sys 보호

- winsoket 에서 메모리 누수되는 현상을 보호함.

12) automatic updates

- 업데이트시 자동업데이트 설정

13) messenger

- 메신저 서비스 사용안함 설정

14) print spooler

- 서버상 프린터 사용안함 설정

15) remote registry service

- 원격지의 레지스트리 서비스 사용한함

16) routing and remote access

- 라우팅 및 원격지 접속 사용안함

17) smart card

- 스마트 카드 사용안함

18) wireless configuration

- 무선 컴피그레이션 사용안함

19) terminal port

- 기본 3389번 포트를 5455번으로 변경

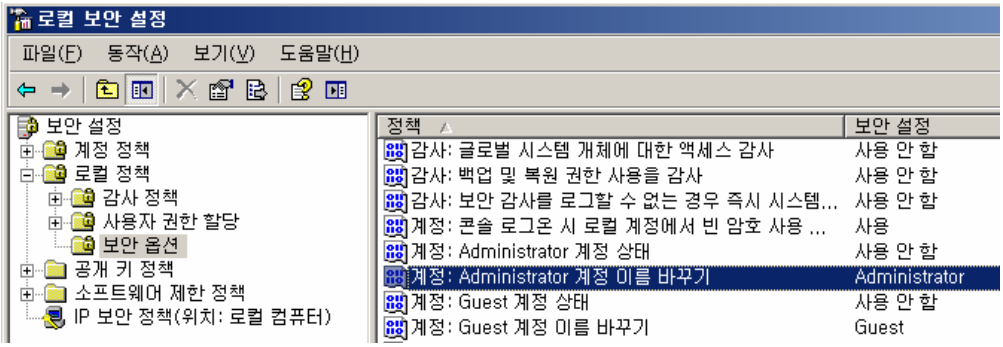
2. 보안 설정 내용

1) [계정정책 변경]

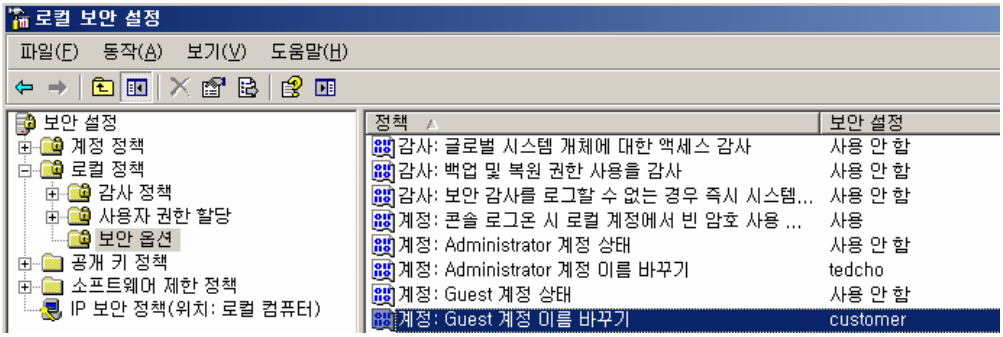
[시작]-[제어판]-[관리도구]-[로컬보안설정]-[로컬정책]-[보안옵션]에서

Administrator ➔ 넥스트라인 홈페이지 로그인하는 고객 아이디로 변경합니다.

Guest ➔ customer 로 변경합니다.

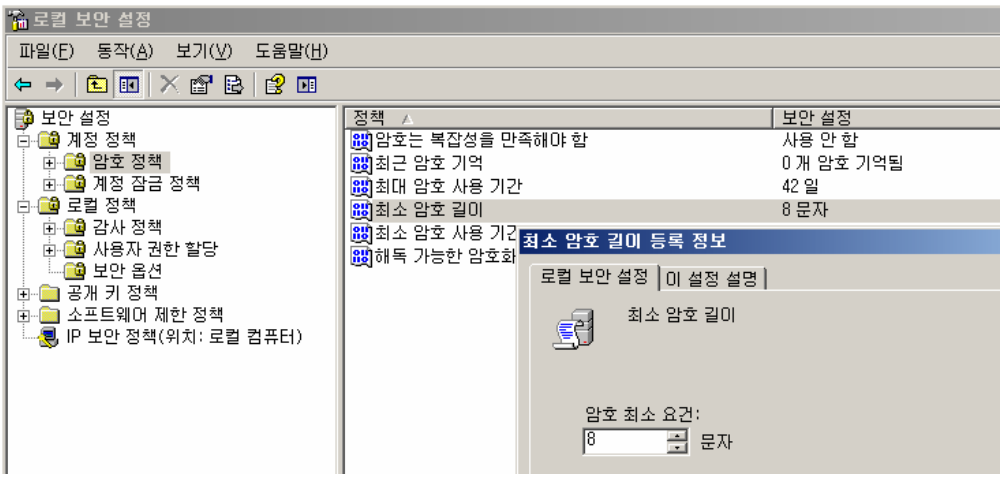


에서 고객ID 로 변경 (ex. tedcho)



2) [암호정책 변경]

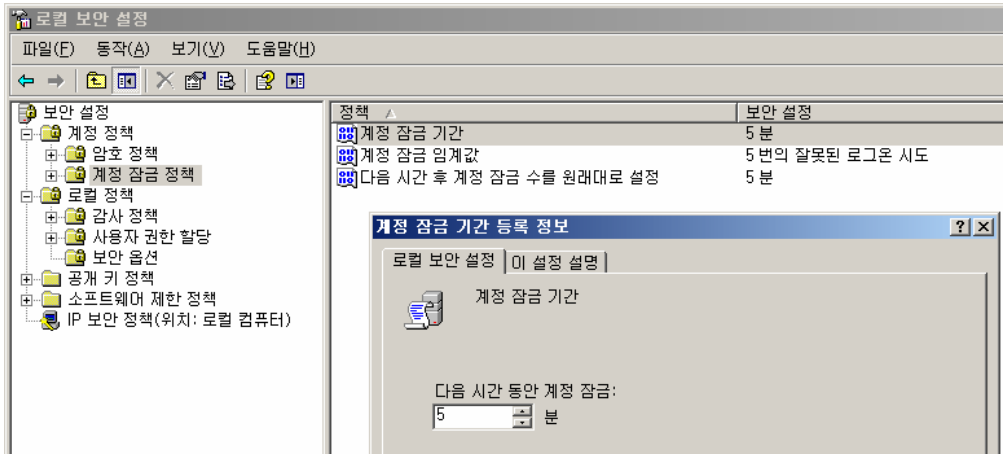
[시작]-[제어판]-[관리도구]-[로컬보안정책]-[계정정책]-[암호정책] ➔ 최소 암호 길이 "8문자" 로 설정 합니다.



3) [계정 잠금 정책]

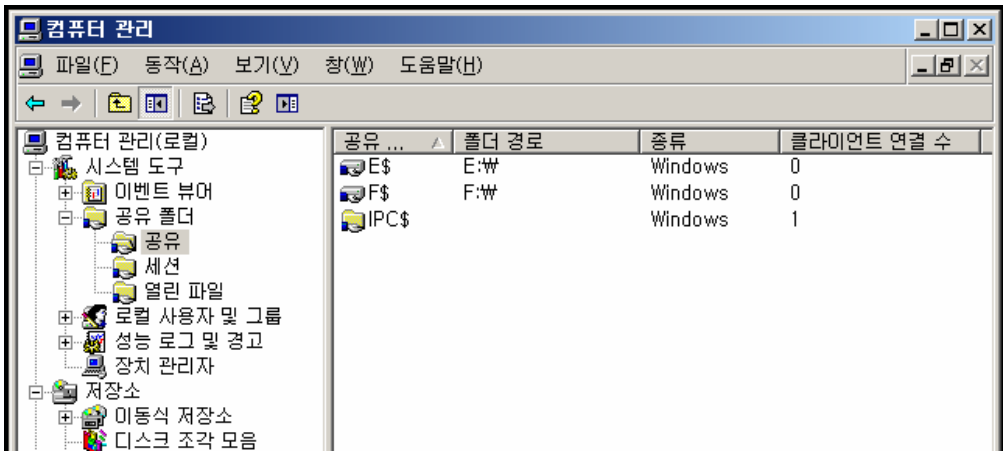
[시작]-[제어판]-[관리도구]-[로컬 보안 설정]-[계정정책]-[계정 잠금 정책]을 클릭 후 아래 내용으로 설정 합니다.

- 계정 잠금 기간 : 5분
- 계정 잠금 임계 값 : 5번의 잘못된 로그온 시도
- 다음 시간 후 계정 잠금 수를 원래대로 설정 : 5분

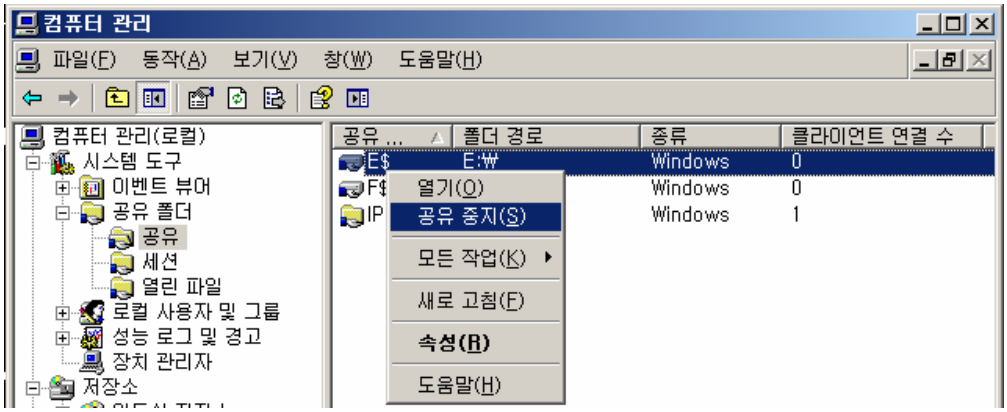


4) [공유 디렉토리 삭제]

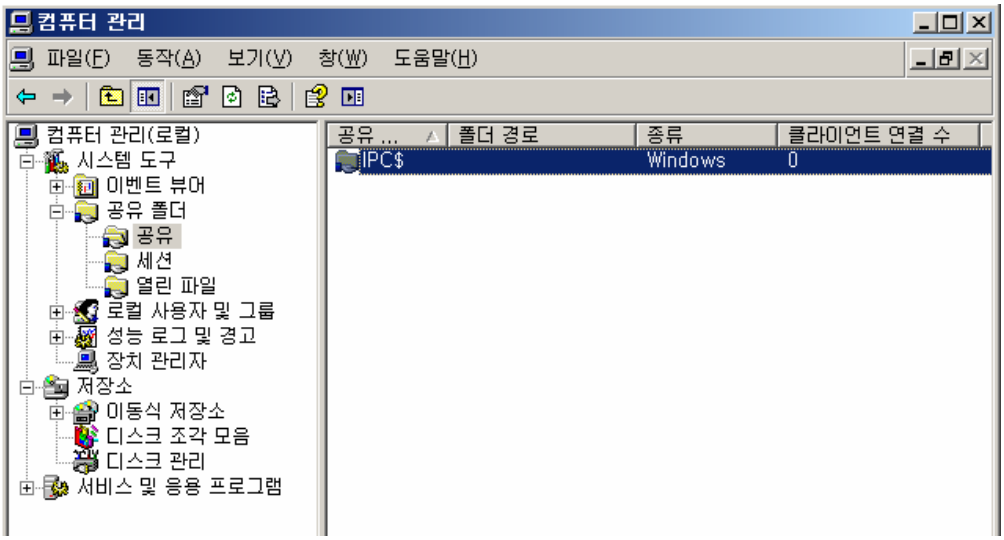
[내 컴퓨터]-[관리]-[공유 폴더]-[공유] ➔ 모두 삭제 합니다.



• 해당 드라이브의 공유를 삭제합니다.



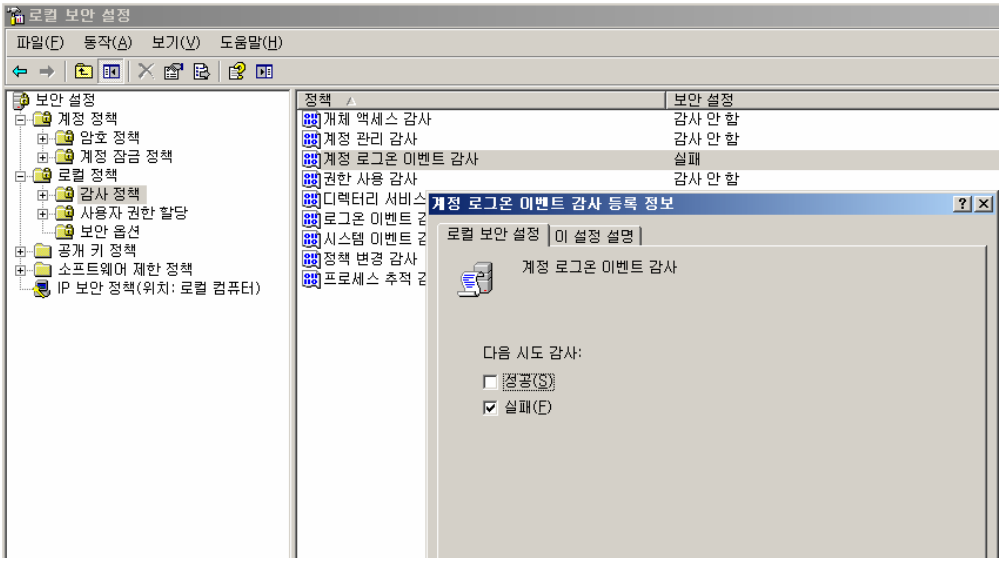
• IPC$ 는 공유서비스의 기본공유로 삭제가 안됩니다.



감사관리 및 계정 보안설정

5) [로그인 실패 로그 기록]

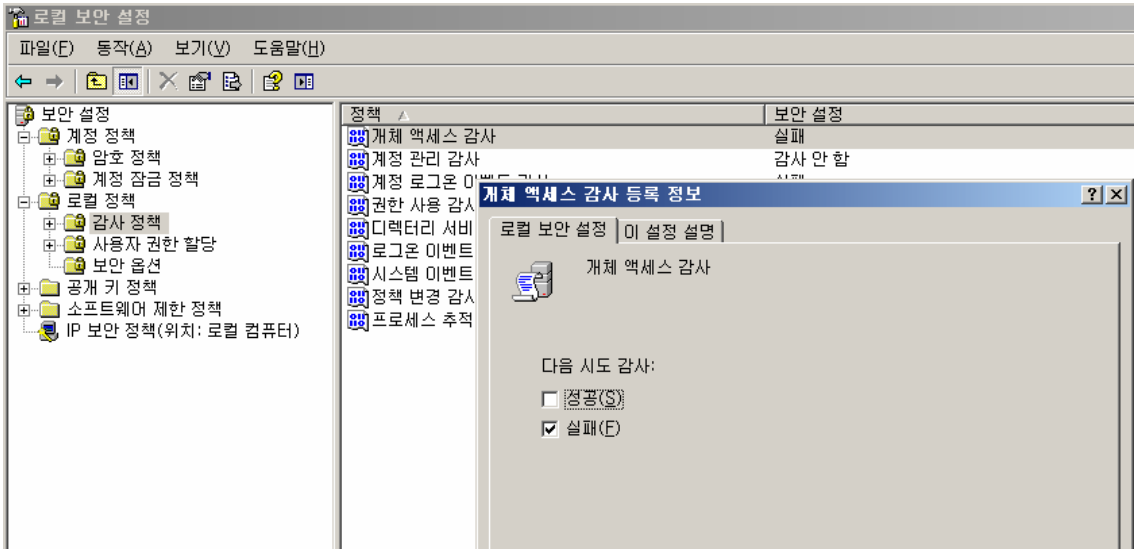
[관리도구]-[로컬보안정책]-[로컬정책]-[감사정책]-[계정 로그온 이벤트 감사] ➔ 속성(실패 항목 체크 합니다.)



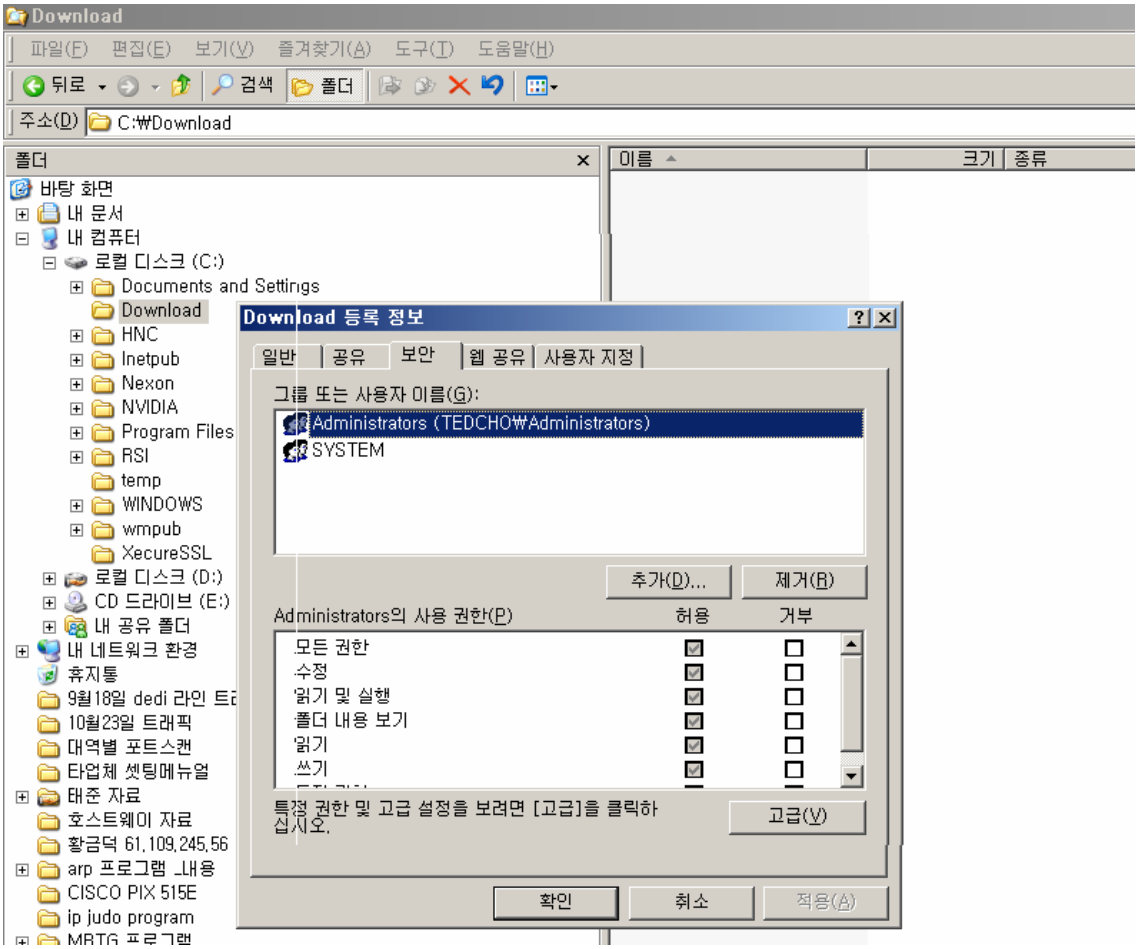
➔ 확인은 관리도구 - 이벤트 뷰어 - 보안 목록에서 확인가능 합니다.

6) [개체 접근 실패 로그 기록]

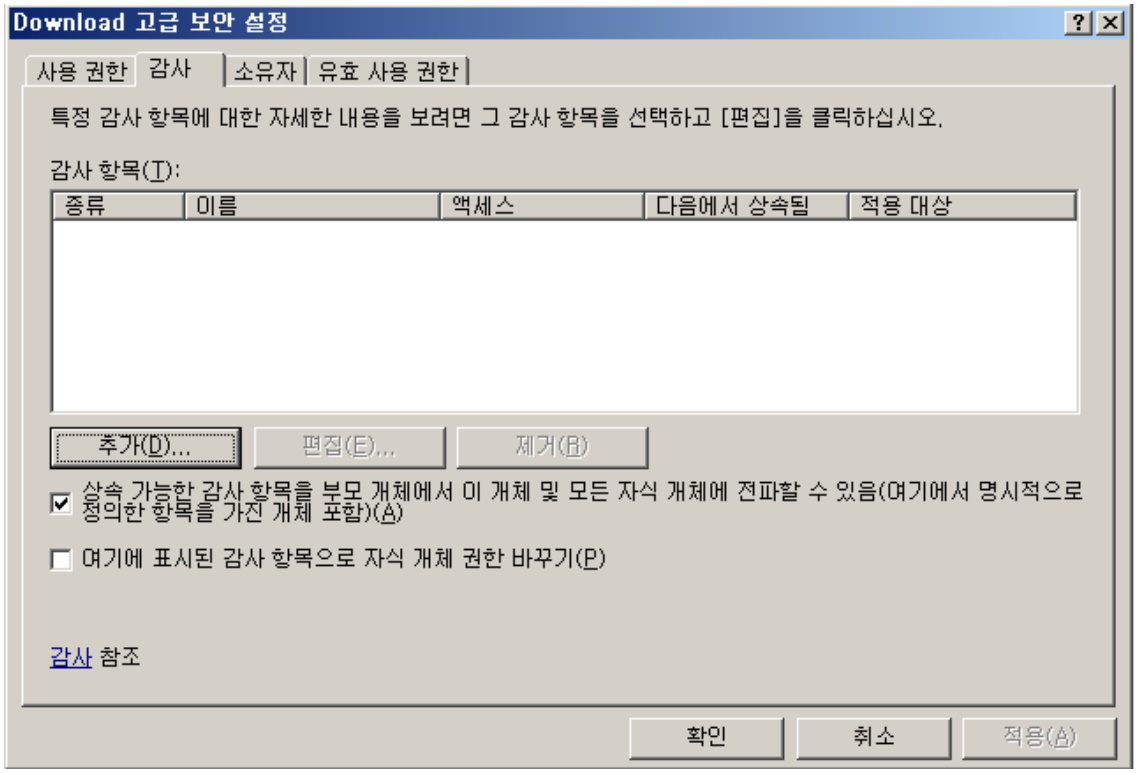
[관리도구]-[로컬보안정책]-[로컬정책]-[감사정책]- [객체 액세스 감사] ➔ 속성(실패 항목 체크 합니다.)

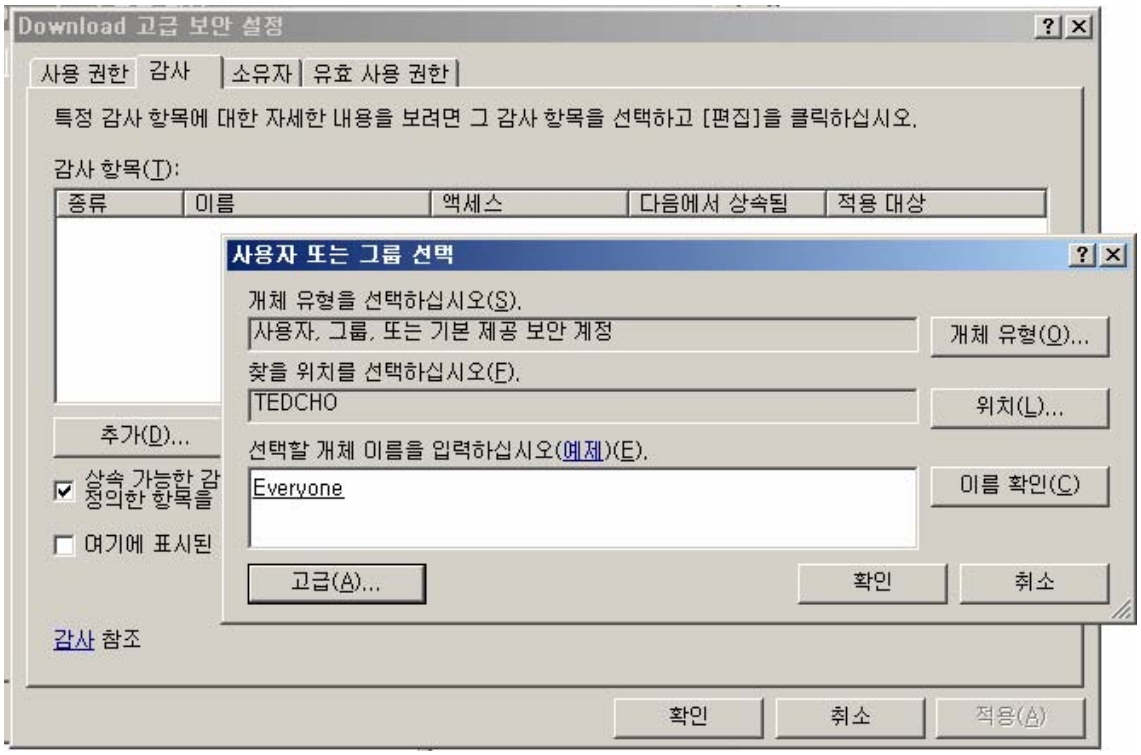


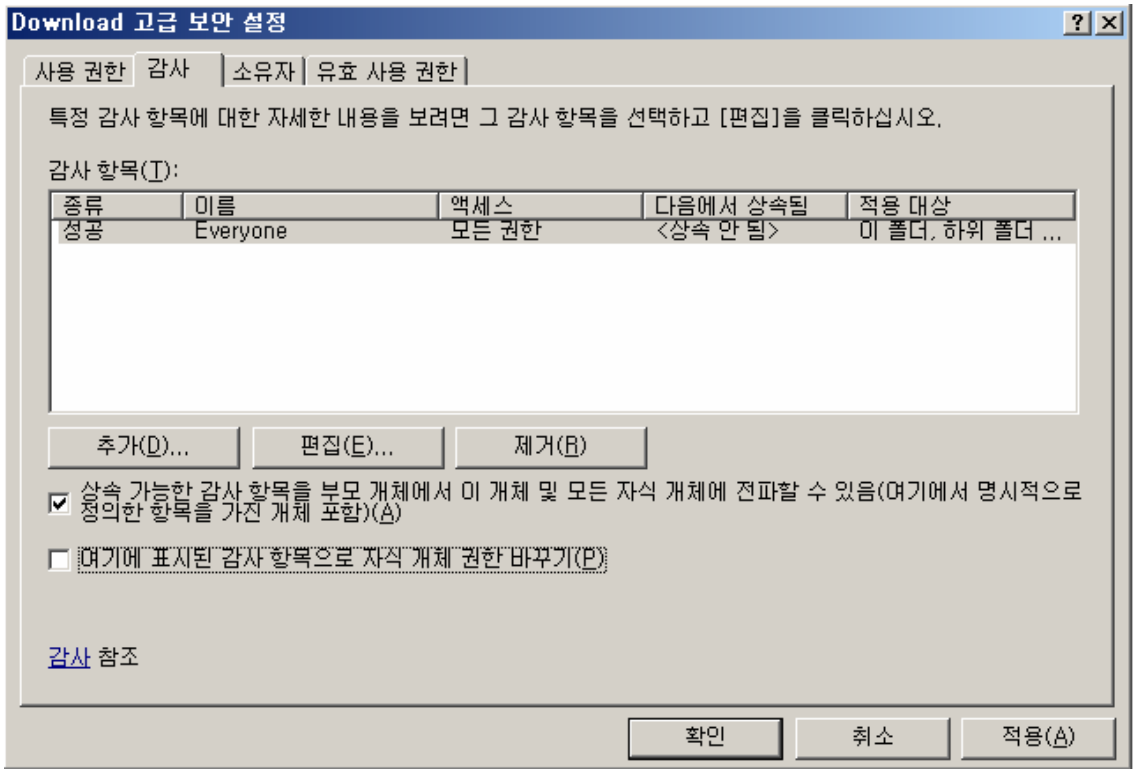
• 감사하려는 대상 폴더나 파일을 탐색기에서 선택합니다.



[속성]-[보안]-[고급]-[감사]-[추가] ➔ “Everyone 그룹”에 대한 모든 실패 이벤트를 기록하도록 [감사항목] 설정 합니다.


Download 고급 보안 설정
사용 권한
감사
소유자
유효 사용 권한
특정 감사 항목에 대한 자세한 내용을 보려면 그 감사 항목을 선택하고 [편집]을 클릭하십시오.
감사 항목(T):
종류
이름
액세스
다음에서 상속됨
적용 대상
추가(D)...
편집(E)...
제거(R)
상속 가능한 감사 항목을 부모 개체에서 이 개체 및 모든 자식 개체에 전파할 수 있음(여기에서 명시적으로 정의한 항목을 가진 개체 포함)(A)
여기에 표시된 감사 항목으로 자식 개체 권한 바꾸기(P)
감사 참조
확인
취소
적용(A)


Download 고급 보안 설정
사용 권한
감사
소유자
유효 사용 권한
특정 감사 항목에 대한 자세한 내용을 보려면 그 감사 항목을 선택하고 [편집]을 클릭하십시오.
감사 항목(T):
종류
이름
액세스
다음에서 상속됨
적용 대상
추가(D)...
감사 참조
확인
취소
적용(A)
사용자 또는 그룹 선택
개체 유형을 선택하십시오(S).
사용자, 그룹, 또는 기본 제공 보안 계정
개체 유형(O)...
찾을 위치를 선택하십시오(F).
TEDCHO
위치(L)...
선택할 개체 이름을 입력하십시오(예제)(E).
Everyone
이름 확인(C)
고급(A)...
확인
취소

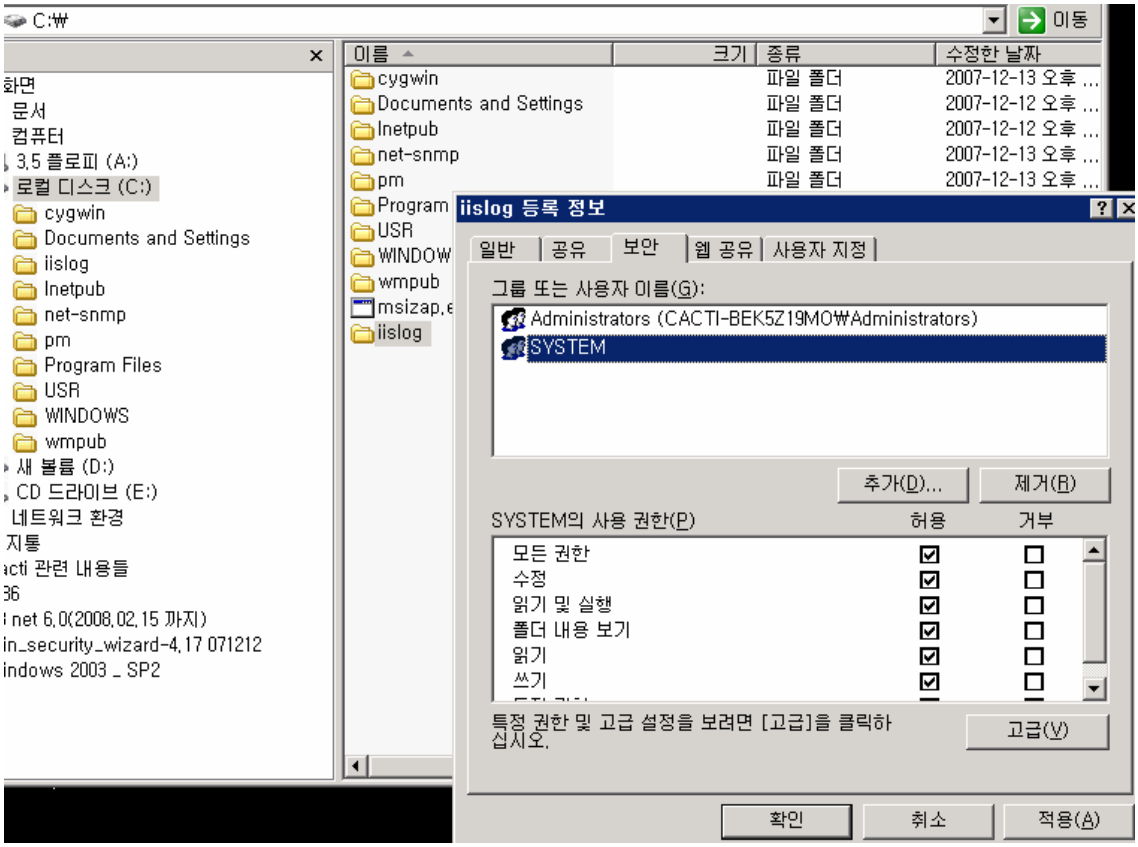


7) [IIS 로그파일 위치 변경]

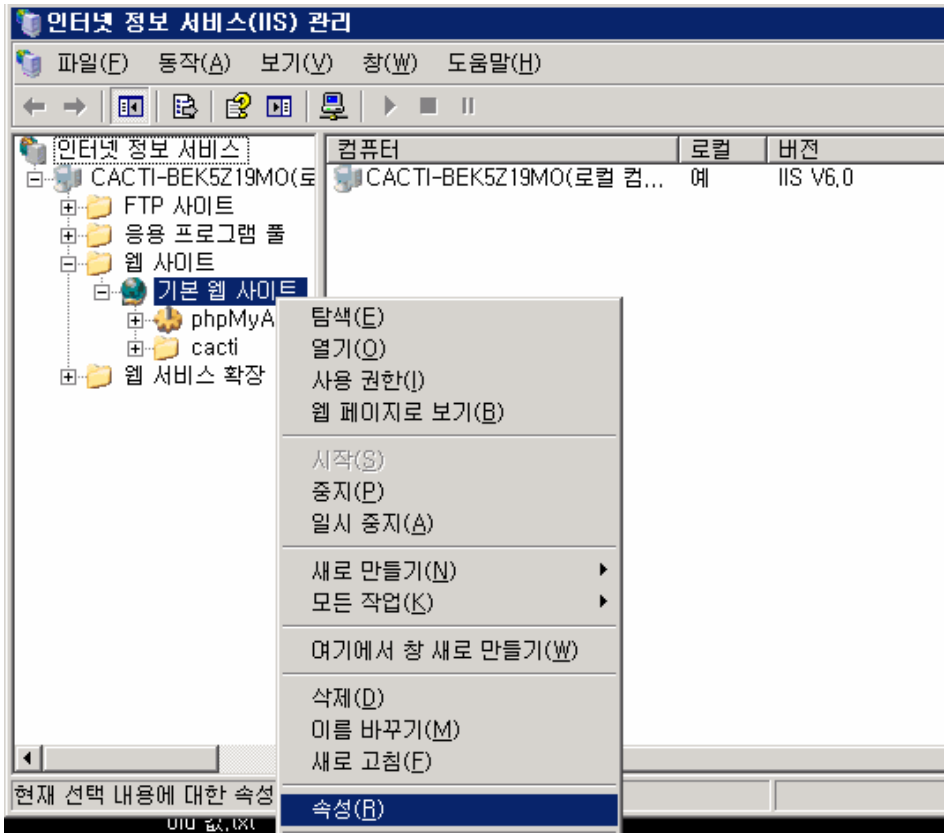
기본설정 디렉토리 C:₩WINDOWS₩system32₩LogFiles 에서 c:₩iislog 디렉토리 생성합니다.

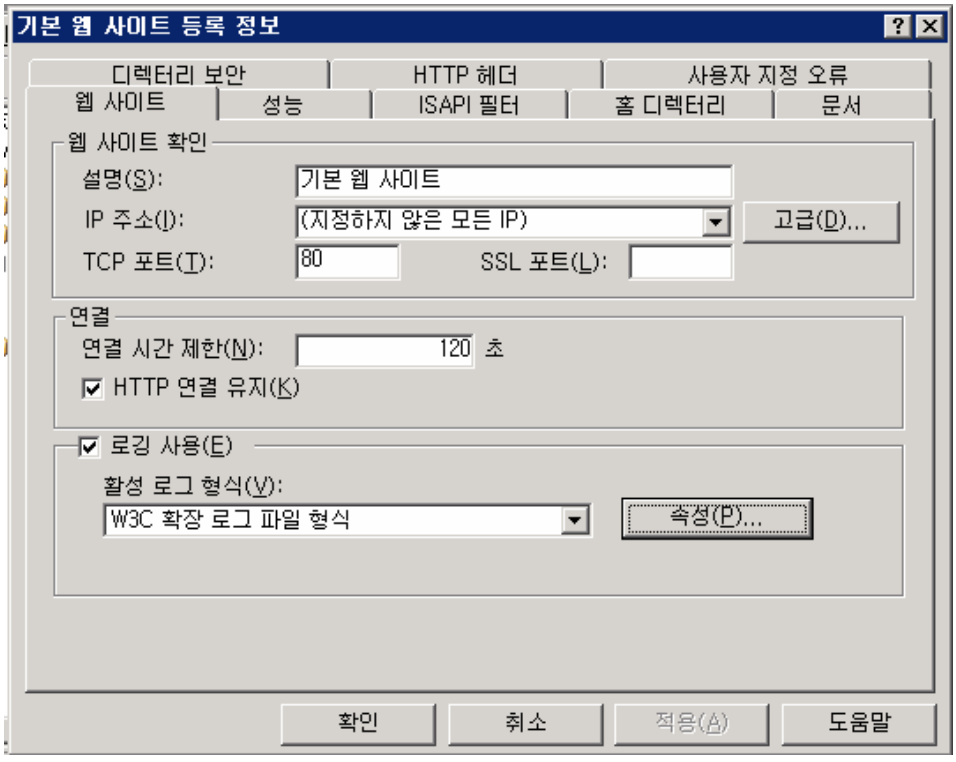
c:₩iislog 디렉토리의 속성에서 administrator, system 계정만 접근할 수 있도록 권한 변경 합니다.

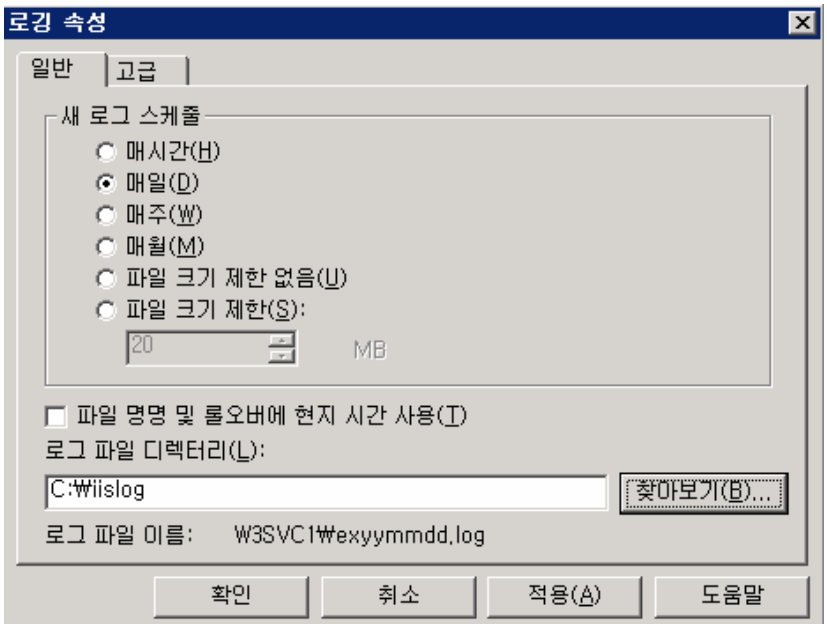
(로그 파일을 삭제 할 수 없도록 보안강화를 위함 입니다.)



[iis 관리]-[각 웹사이트]-[속성 클릭]-[로그 파일 디렉터리]-[찾아보기]- [C:₩iislog]폴더 선택 후 확인을 클릭합니다.

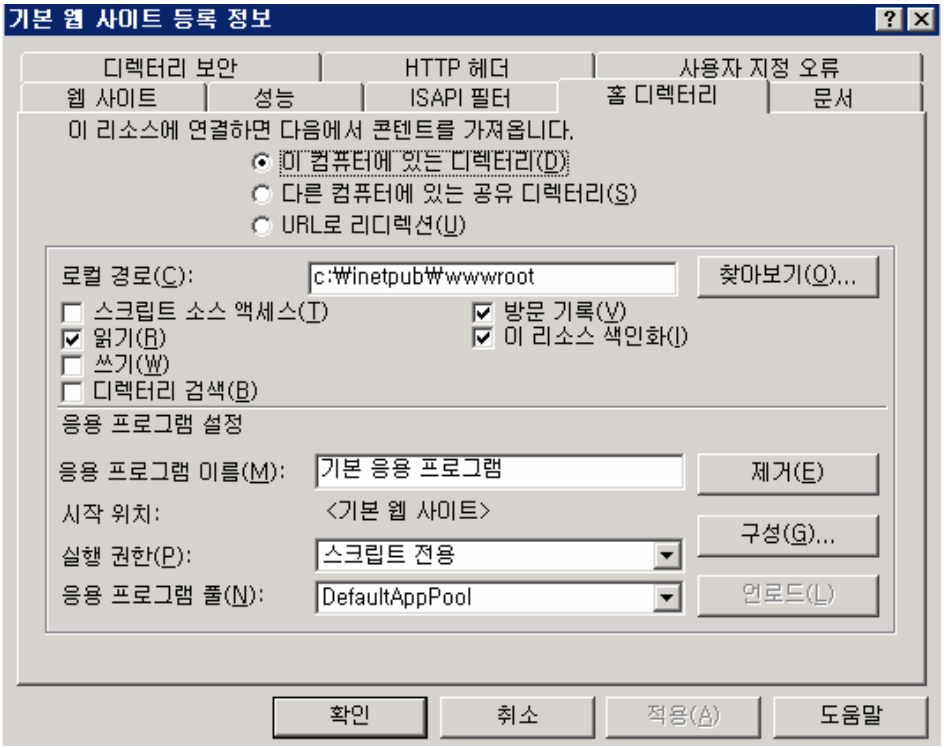

인터넷 정보 서비스(IIS) 관리
파일(F) 동작(A) 보기(V) 창(W) 도움말(H)
인터넷 정보 서비스
CACTI-BEK5Z19MO(로
FTP 사이트
응용 프로그램 풀
웹 사이트
기본 웹 사이트
phpMyA
cacti
웹 서비스 확장
컴퓨터
로컬
버전
CACTI-BEK5Z19MO(로컬 컴...
예
IIS V6.0
탐색(E)
열기(O)
사용 권한(I)
웹 페이지로 보기(B)
시작(S)
중지(P)
일시 중지(A)
새로 만들기(N)
모든 작업(K)
여기에서 창 새로 만들기(W)
삭제(D)
이름 바꾸기(M)
새로 고침(F)
속성(R)
현재 선택 내용에 대한 속성

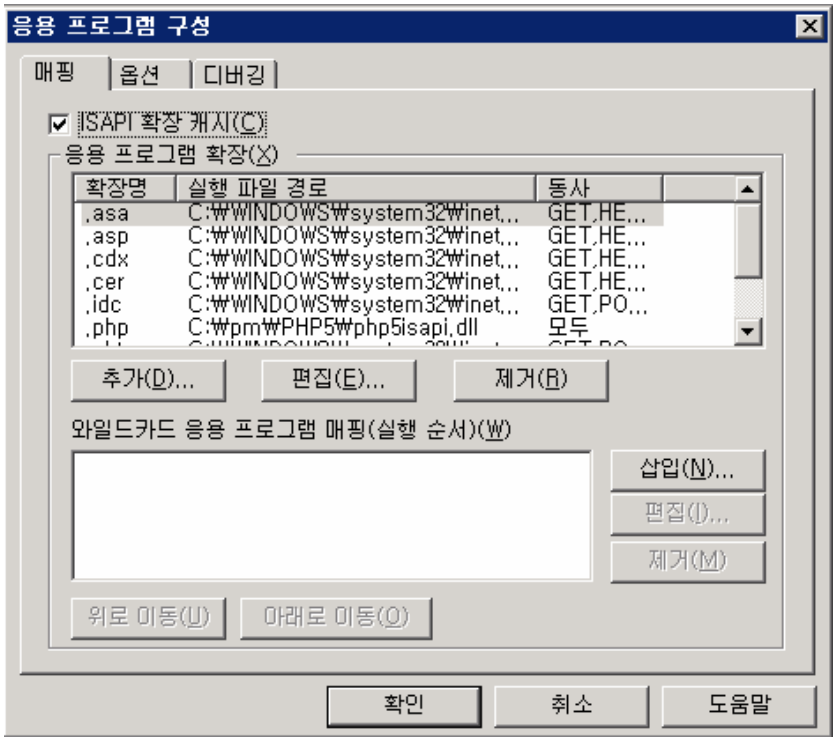

기본 웹 사이트 등록 정보
디렉터리 보안
HTTP 헤더
사용자 지정 오류
웹 사이트
성능
ISAPI 필터
홈 디렉터리
문서
웹 사이트 확인
설명(S):
기본 웹 사이트
IP 주소(I):
(지정하지 않은 모든 IP)
고급(D)...
TCP 포트(T):
80
SSL 포트(L):
연결
연결 시간 제한(N):
120
초
HTTP 연결 유지(K)
로깅 사용(E)
활성 로그 형식(V):
W3C 확장 로그 파일 형식
속성(P)...
확인
취소
적용(A)
도움말



8) [매핑 제거]

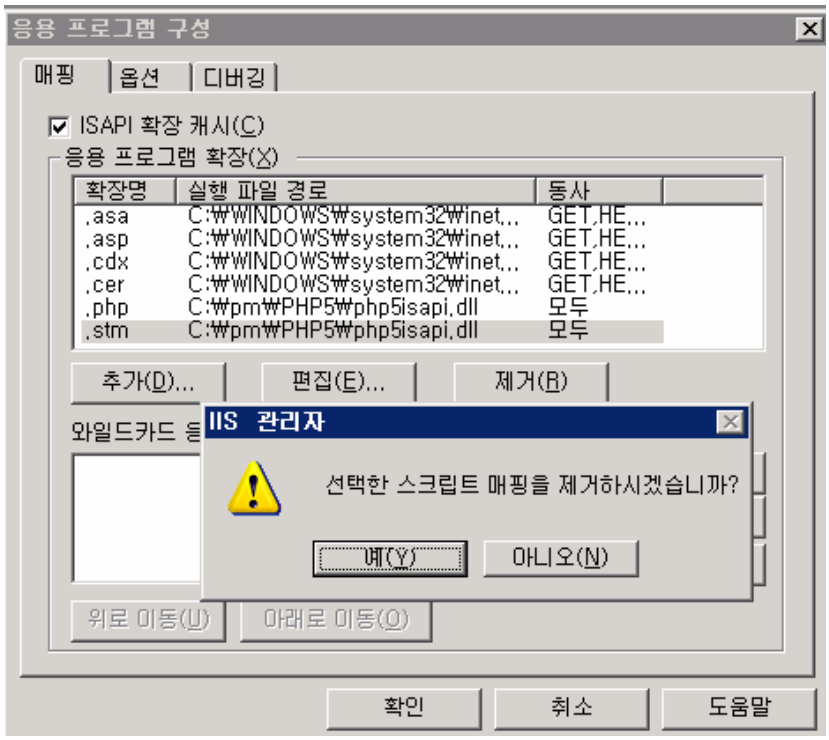
[인터넷 정보 서비스]-[웹사이트]-[등록정보]-[홈 디렉토리]-[구성]-[응용프로그램] ➔ "매핑" 을 클릭 합니다.

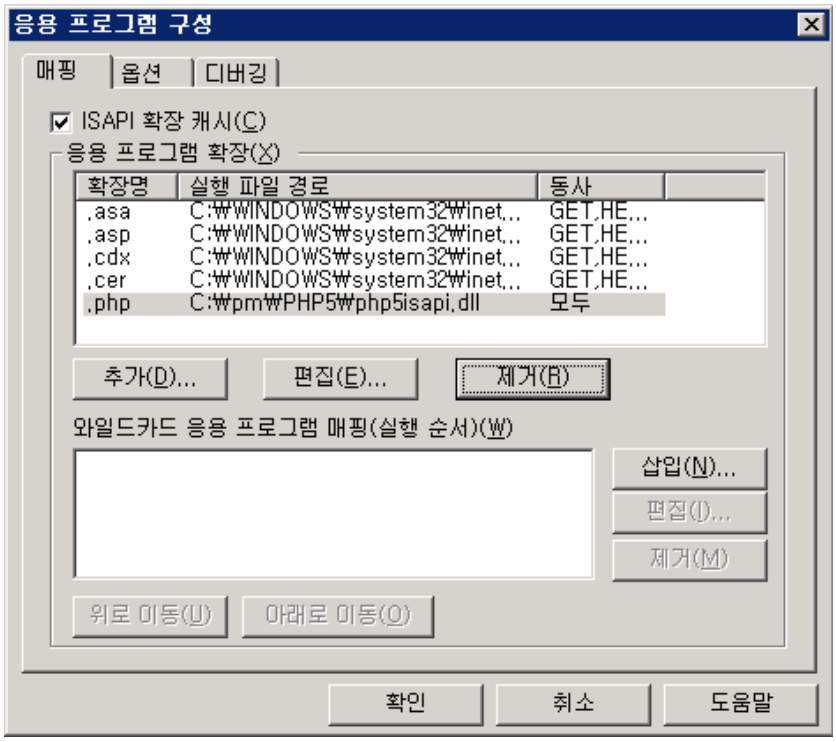




응용 프로그램 확장에서 웹 서버의 경우 기본적으로 .htr, .idc, .stm, .shtm, .shtml, .printer, .htw, .ida, .idq 제거합니다.

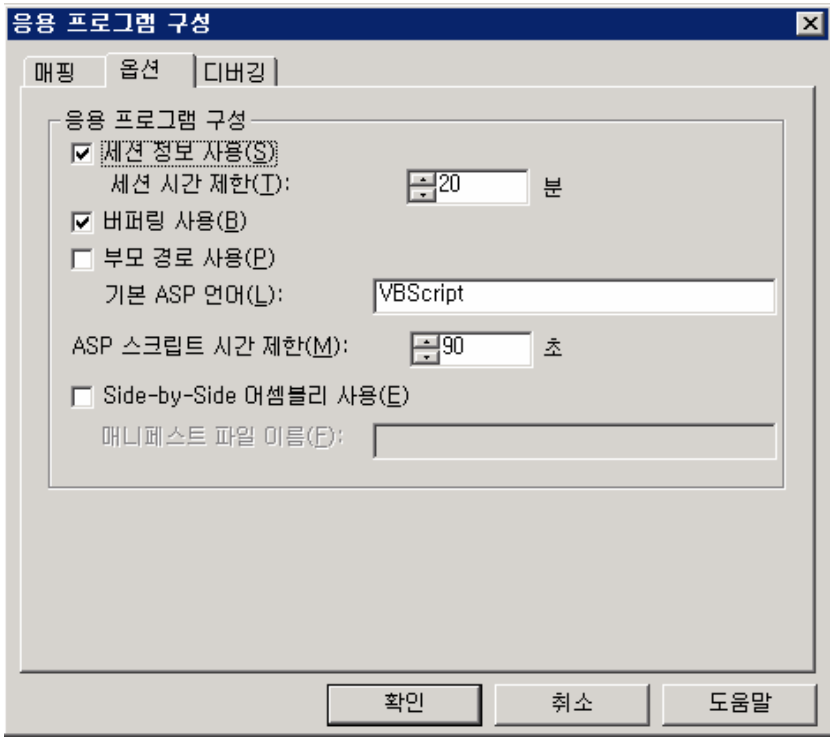
파일서버, db서버일 경우 모두 제거 하는게 좋습니다.





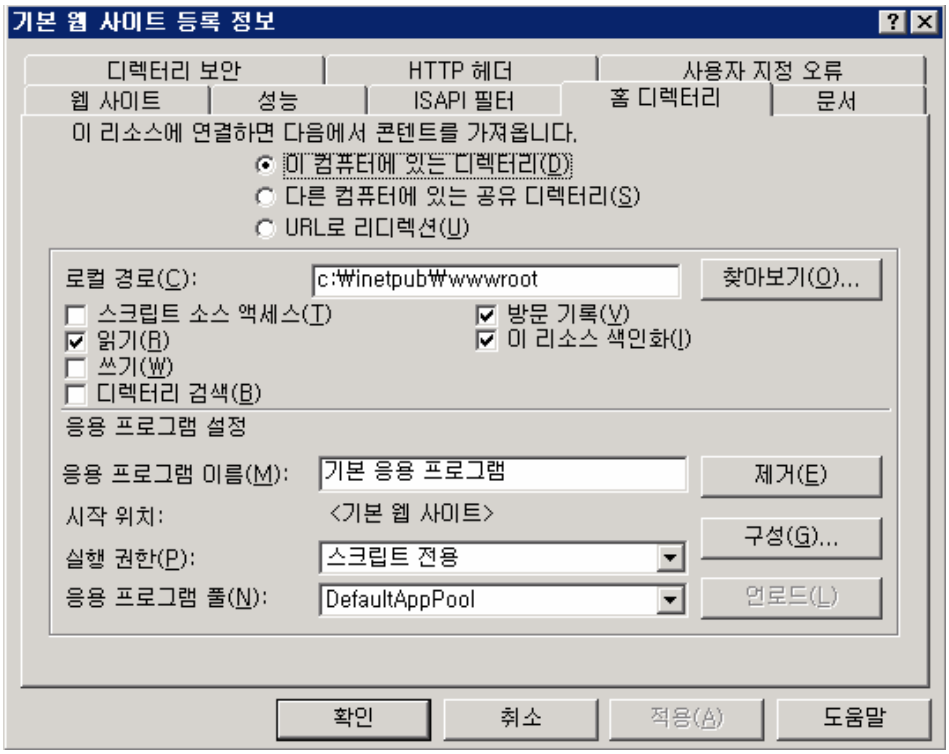
9) [iis 기본설정]

[인터넷 정보 서비스]-[웹사이트]-[등록정보]-[홈 디렉토리]-[구성]-[응용프로그램]-[옵션]-[부모 경로 사용] ➔ "체크해제" 후 확인을 클릭합니다.



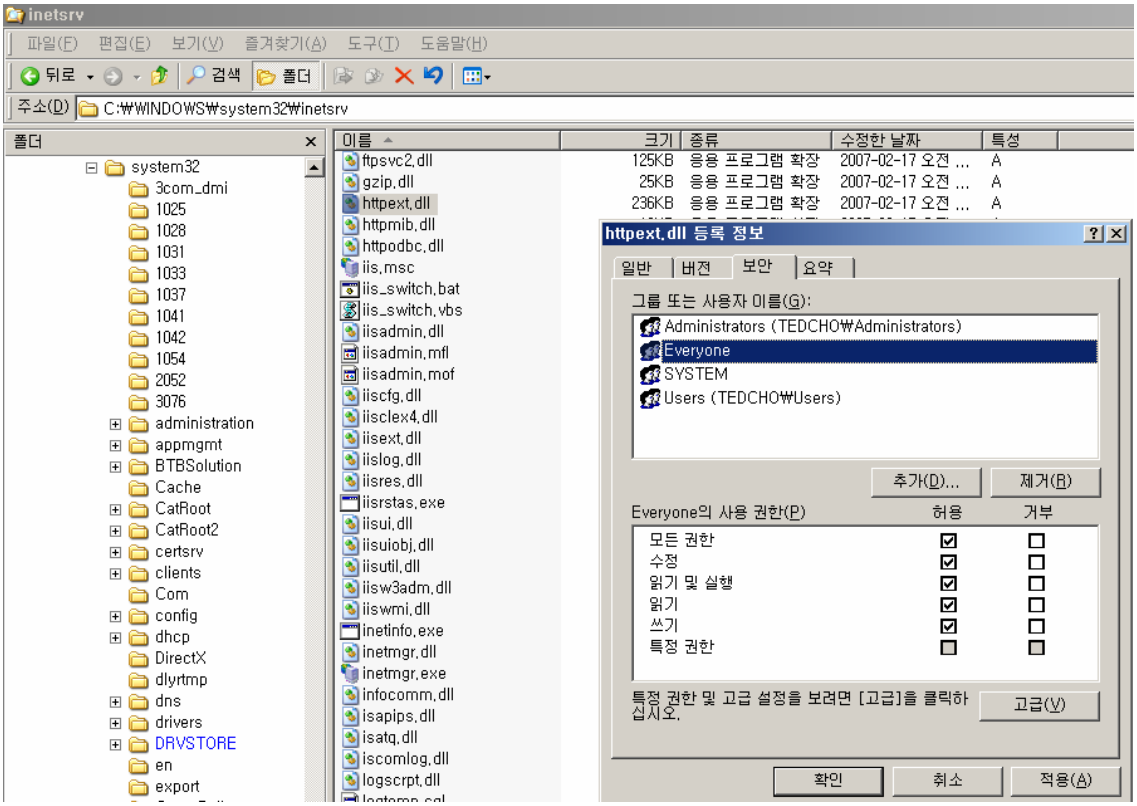
10) [컨텐츠 디렉토리 권한]

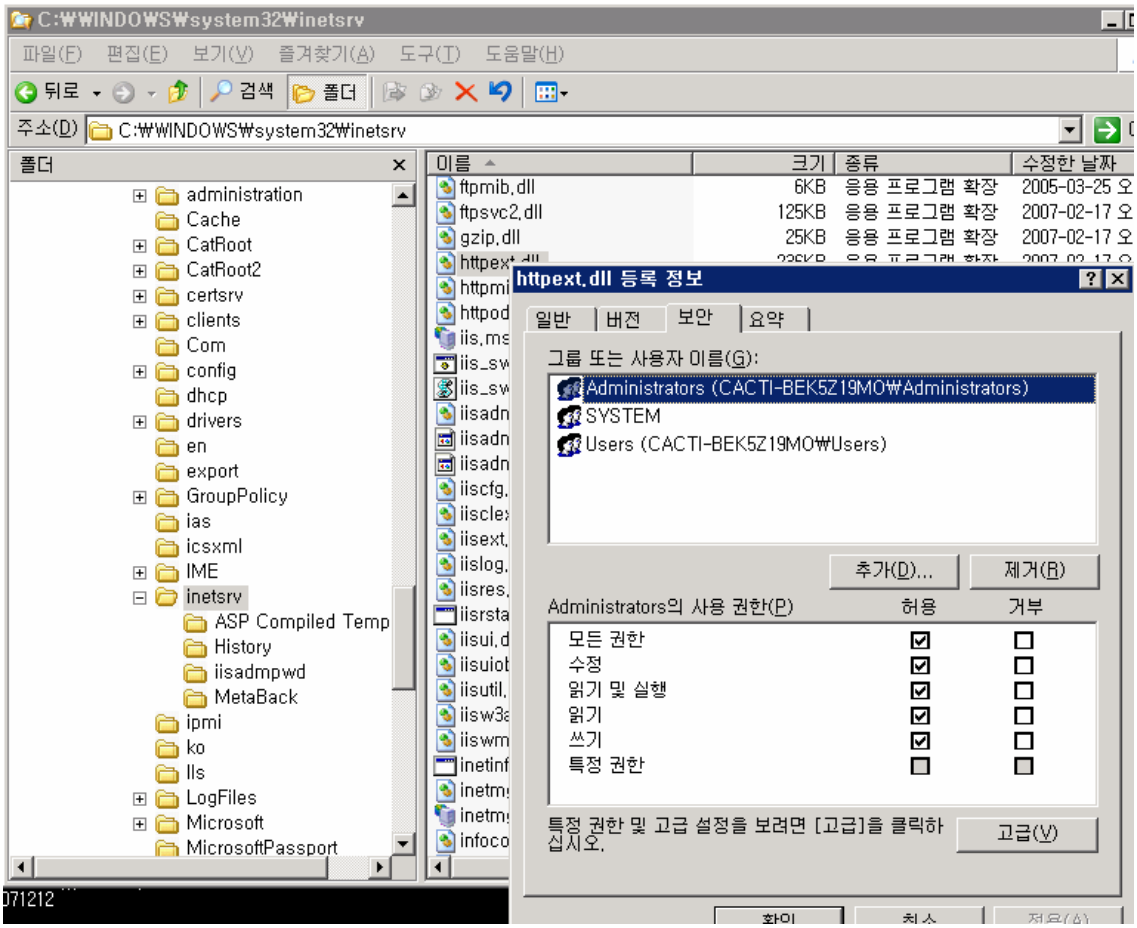
[인터넷정보서비스]-[웹사이트]-[등록정보]-[홈 디렉토리] ➔ "읽기, 방문기록, 이 리소스 색인화" 3개만 체크 합니다.



11) [WebDAV 비활성화]

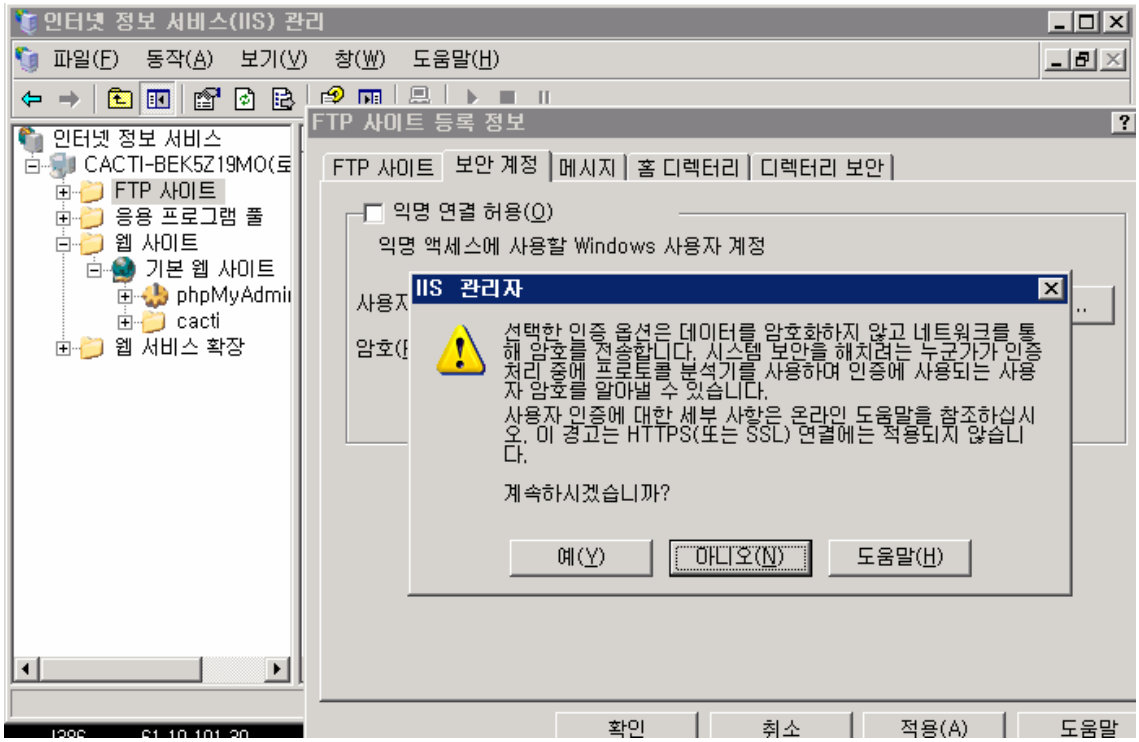
c:/windows/system32/inetsrv/httpext.dll에 everybody 권한 제거합니다.


inetsrv
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로 검색 폴더
주소(D) C:₩WINDOWS₩system32₩inetsrv
폴더
system32
3com_dmi
1025
1028
1031
1033
1037
1041
1042
1054
2052
3076
administration
appmgmt
BTBSolution
Cache
CatRoot
CatRoot2
certsrv
clients
Com
config
dhcp
DirectX
dlyrtmp
dns
drivers
DRVSTORE
en
export
이름 크기 종류 수정한 날짜 특성
ftpsvc2.dll 125KB 응용 프로그램 확장 2007-02-17 오전 ... A
gzip.dll 25KB 응용 프로그램 확장 2007-02-17 오전 ... A
httpext.dll 236KB 응용 프로그램 확장 2007-02-17 오전 ... A
httpmib.dll
httpodbc.dll
iis.msc
iis_switch.bat
iis_switch.vbs
iisadmin.dll
iisadmin.mfl
iisadmin.mof
iiscfg.dll
iisclex4.dll
iisext.dll
iislog.dll
iisres.dll
iisrstas.exe
iisui.dll
iisuiobj.dll
iisutil.dll
iisw3adm.dll
iiswmi.dll
inetinfo.exe
inetmgr.dll
inetmgr.exe
infocomm.dll
isapips.dll
isatq.dll
iscomlog.dll
logscrpt.dll
httpext.dll 등록 정보
일반 버전 보안 요약
그룹 또는 사용자 이름(G):
Administrators (TEDCHO₩Administrators)
Everyone
SYSTEM
Users (TEDCHO₩Users)
추가(D)... 제거(R)
Everyone의 사용 권한(P) 허용 거부
모든 권한
수정
읽기 및 실행
읽기
쓰기
특정 권한
특정 권한 및 고급 설정을 보려면 [고급]을 클릭하십시오.
고급(V)
확인 취소 적용(A)



12) [ftp 익명접속 거부]

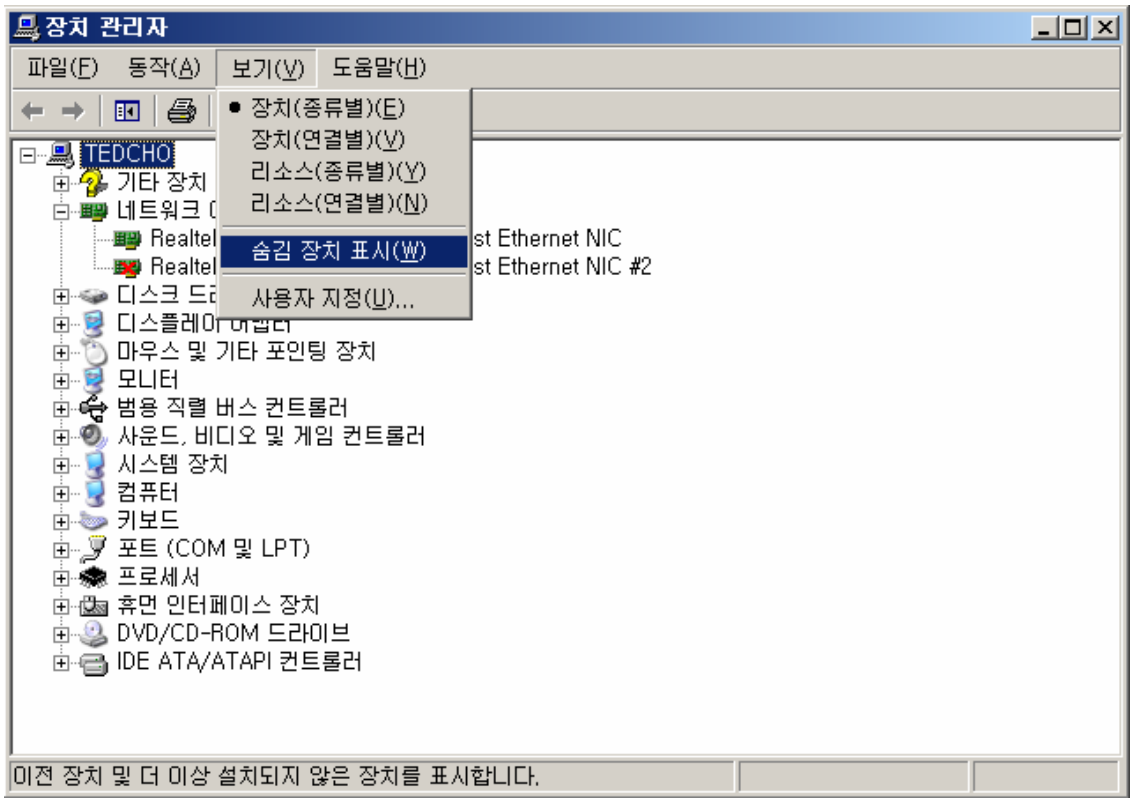
[인터넷정보서비스]-[해당 ftp 사이트]-[속성]-[보안계정]-[익명연결허용] 체크해제 합니다.

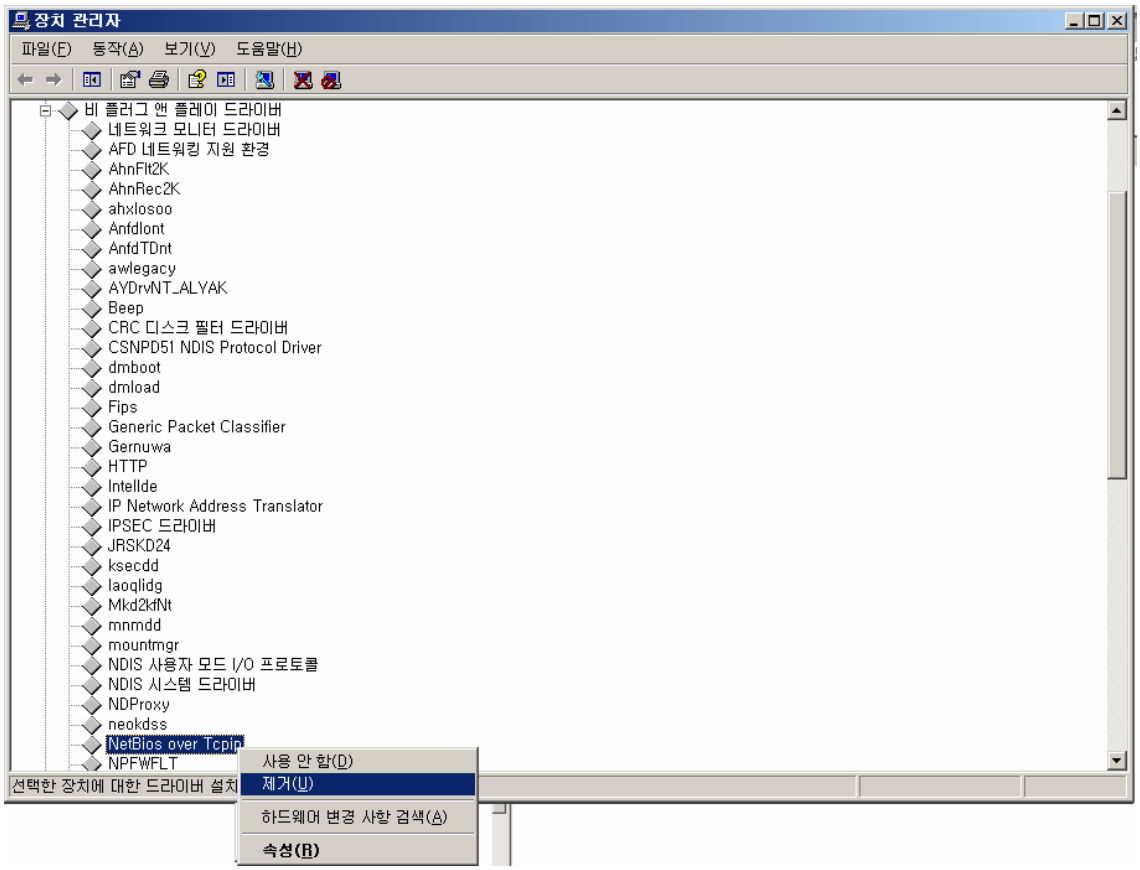

인터넷 정보 서비스(IIS) 관리
파일(F) 동작(A) 보기(V) 창(W) 도움말(H)
인터넷 정보 서비스
CACTI-BEK5Z19MO(로
FTP 사이트
응용 프로그램 풀
웹 사이트
기본 웹 사이트
phpMyAdmi
cacti
웹 서비스 확장
FTP 사이트 등록 정보
FTP 사이트
보안 계정
메시지
홈 디렉터리
디렉터리 보안
익명 연결 허용(O)
익명 액세스에 사용할 Windows 사용자 계정
사용자
암호(P
IIS 관리자
선택한 인증 옵션은 데이터를 암호화하지 않고 네트워크를 통해 암호를 전송합니다. 시스템 보안을 해치려는 누군가가 인증 처리 중에 프로토콜 분석기를 사용하여 인증에 사용되는 사용자 암호를 알아낼 수 있습니다.
사용자 인증에 대한 세부 사항은 온라인 도움말을 참조하십시오. 이 경고는 HTTPS(또는 SSL) 연결에는 적용되지 않습니다.
계속하시겠습니까?
예(Y)
아니오(N)
도움말(H)
확인
취소
적용(A)
도움말

네트워크 보안설정

13) NetBIOS 비활성화 방법

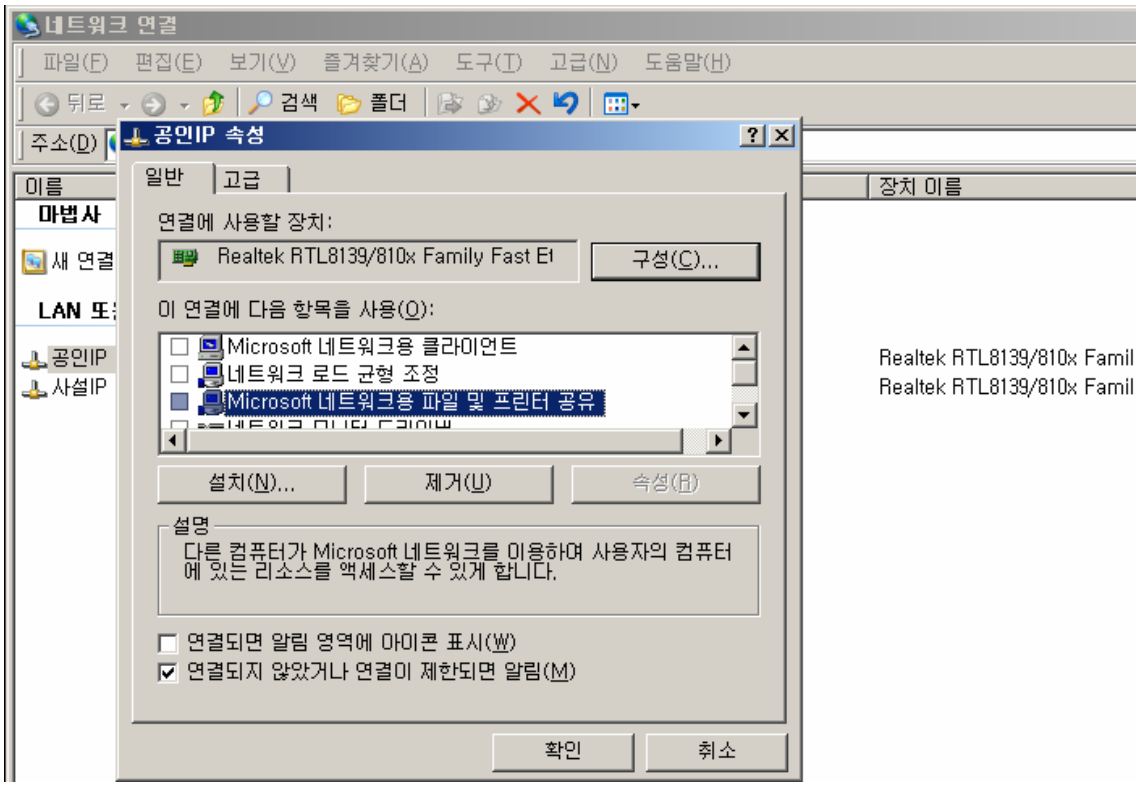
[내 컴퓨터]-[속성]-[하드웨어 탭]-[장치관리자]-[보기]-[숨김 장치 표시]-[비 플러그 앤 플레이 드라이버] ➔ "NetBios over Tcpip " 를 제거 합니다.





14) [SMB 비활성화]

[내 네트워크 환경]-[속성]-[로컬영역연결]-[속성] ➔ "Microsoft 네트워크용 클라이언트, Microsoft 네트워크용 파일 및 프린터 공유 항목" 을 체크 해제 합니다.



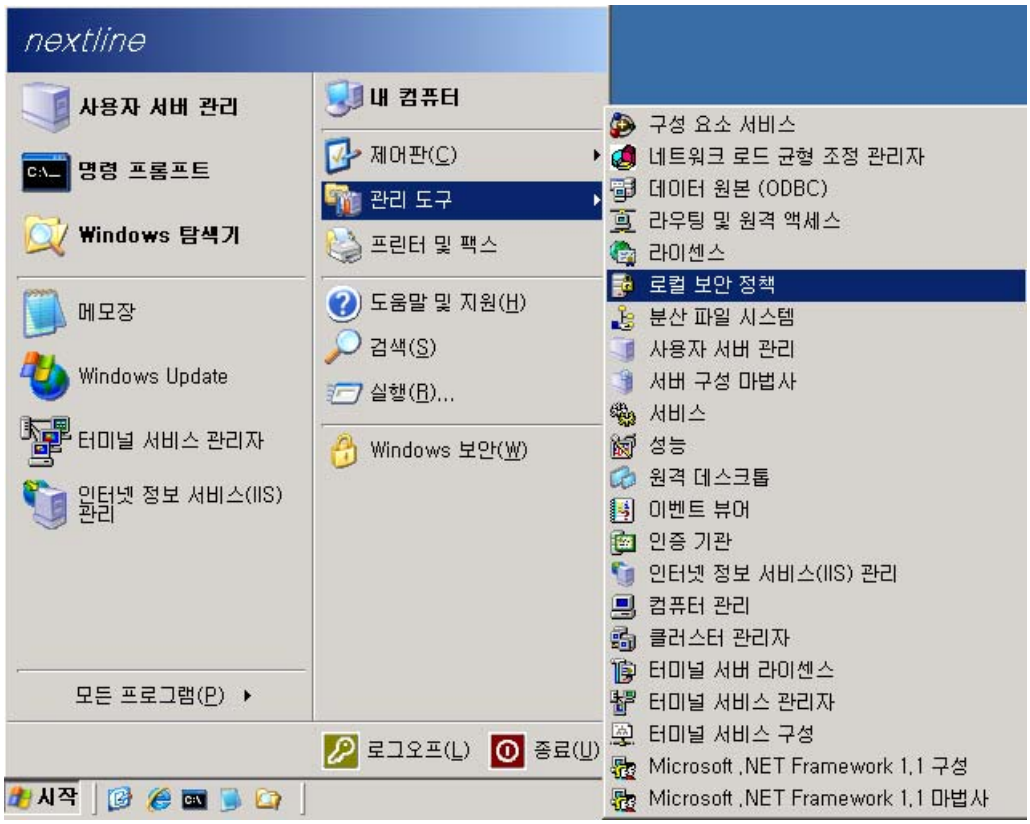
3. Next_filter 이란 ?

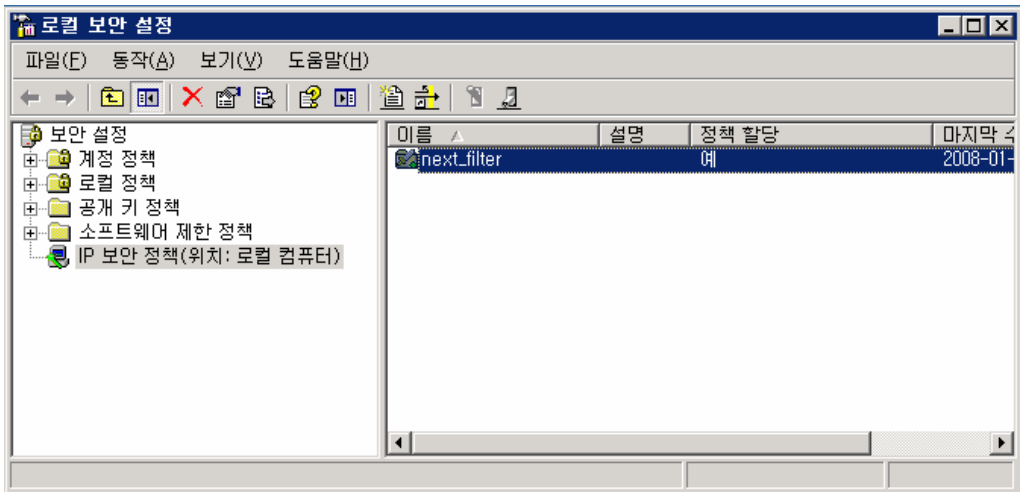
Microsoft 및 Cisco Systems, Inc. 에서 개발한 IPSec (인터넷 프로토콜 보안) 을 이용한 필터로 원하는 ip나 포트에 대해서 차단 및 해제를 손쉽게 할 수 있는 보안정책 입니다.

IPSec(인터넷 프로토콜 보안)은 암호화 보안 서비스를 사용하여 인터넷 프로토콜 네트워크를 통한 안전한 개인 통신을 보장하는 개방형 표준 보안 체계입니다. IPSec에는 IP 패킷의 콘텐트 보호와 패킷 필터링 및 트러스트된 통신의 강화를 통하여 네트워크 공격에 대한 방어를 제공하고자 하는 목적이 있습니다.

1) Next_filter 확인

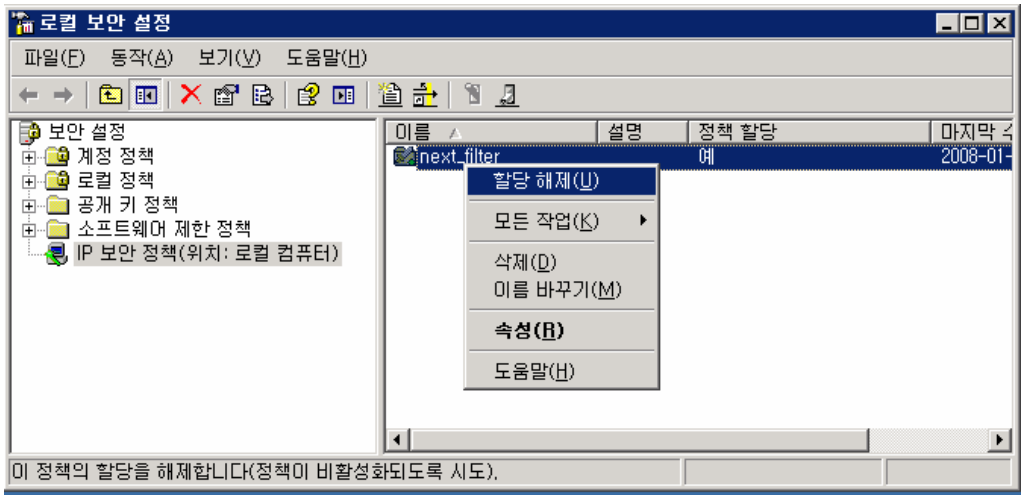
[시작]-[모든 프로그램] – [관리도구] – [로컬 보안 정책] 클릭합니다.





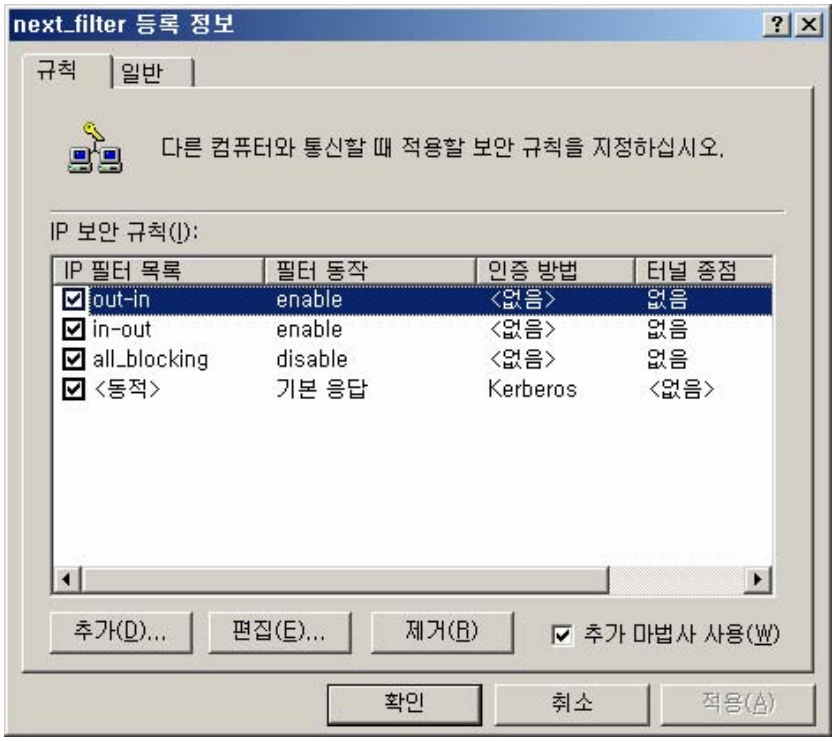
2) Next_filter 적용과 해제

[Next_filter] 마우스 우 클릭 – [할당](할당 해제)



3) Next_filter 설정 내용 확인

[Next_filter] 마우스 우 클릭 – [속성]



• out-in : 외부에서 내부로 접속 가능한 아이피 나 포트를 등록 할 수 있습니다.

• in-out : 내부에서 외부로 접속 가능한 아이피 나 포트를 등록 할 수 있습니다.

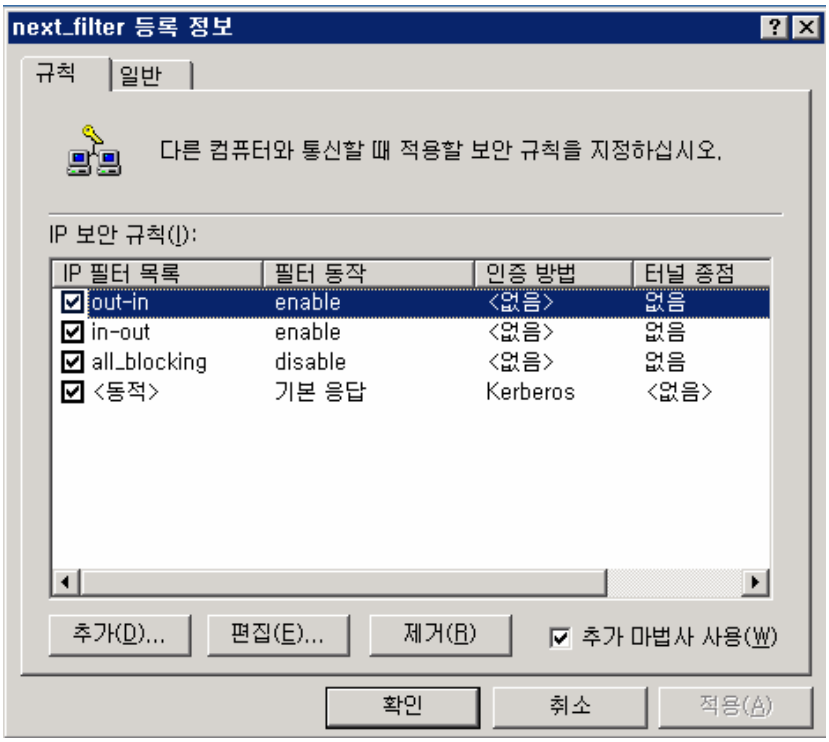
• all_blocking : out-in과 in-out에서 오픈 하여 준 아이피 와 포트 이외에 나머지를 차단하여 줍니다.

•<동적> : 다른 컴퓨터와 협상할 때 사용하는 보안방법과 컴퓨터 간의 신뢰 성립방법인 인증 방법을 설정합니다.

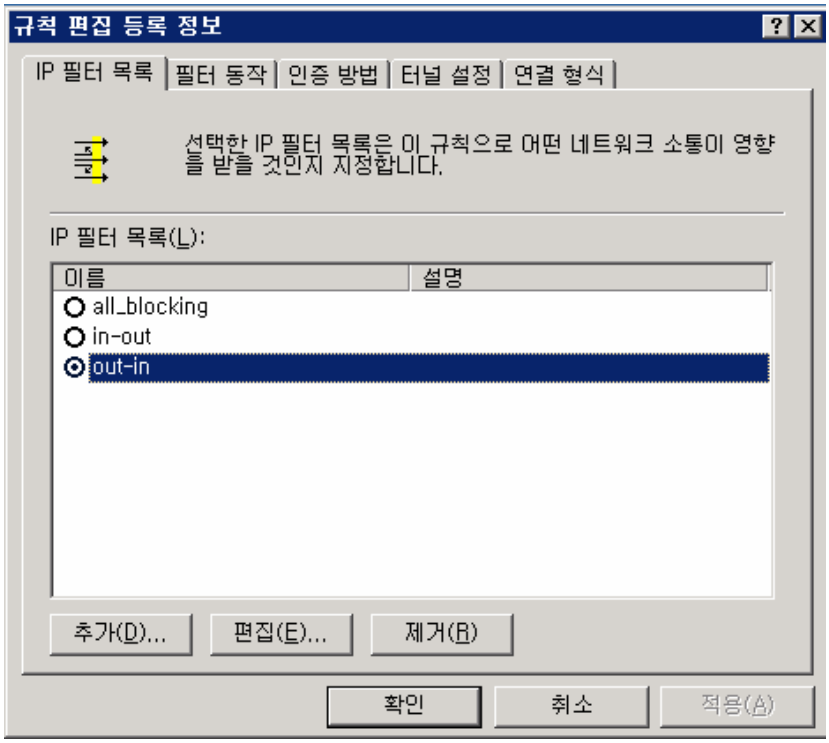
4) Out-in 확인 및 추가 방법

접근을 허용하고자 하는 아이피 나 포트에 대해 Out-in을 오픈 하여 줍니다.

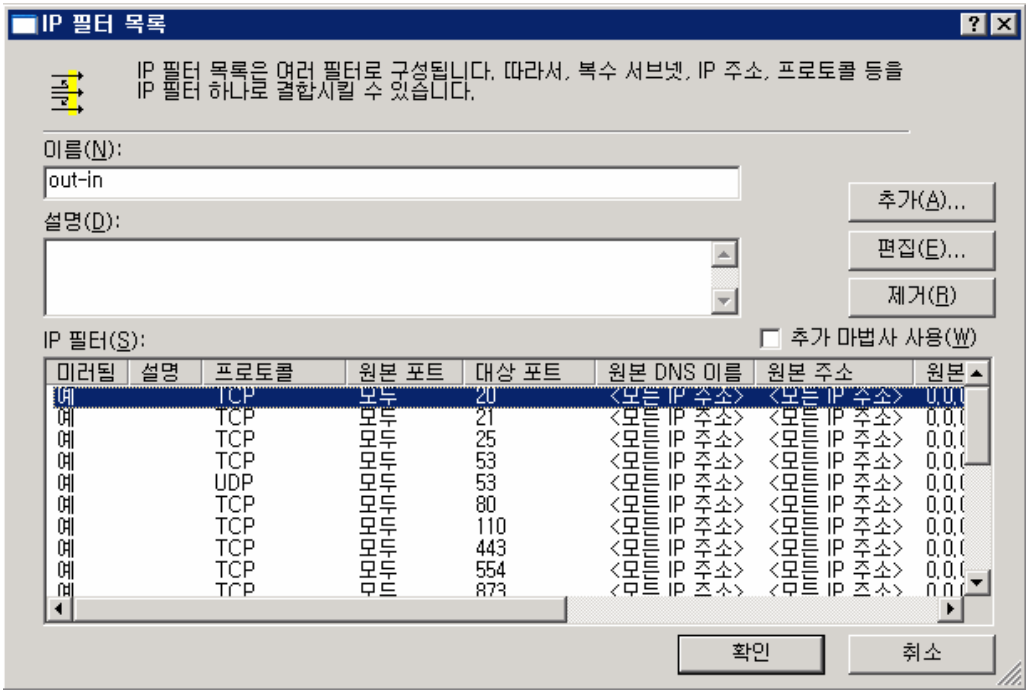
① [Out-in]을 선택하고 [편집]을 클릭



② [Out-in] 을 선택한 후 [편집]을 클릭

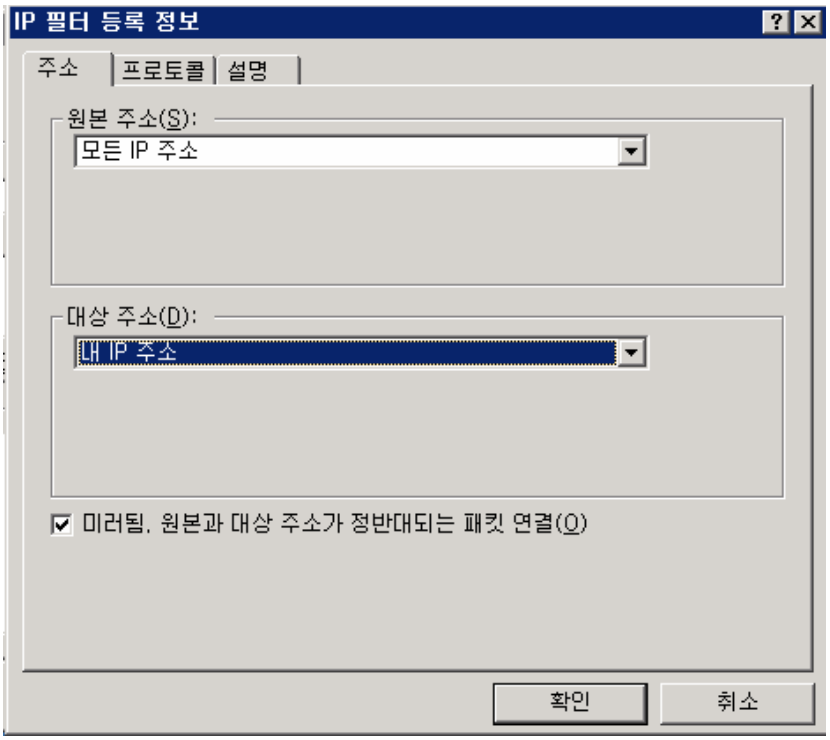


③ 이 화면에서 각 IP 필터를 추가하거나 편집 제거가 가능합니다.



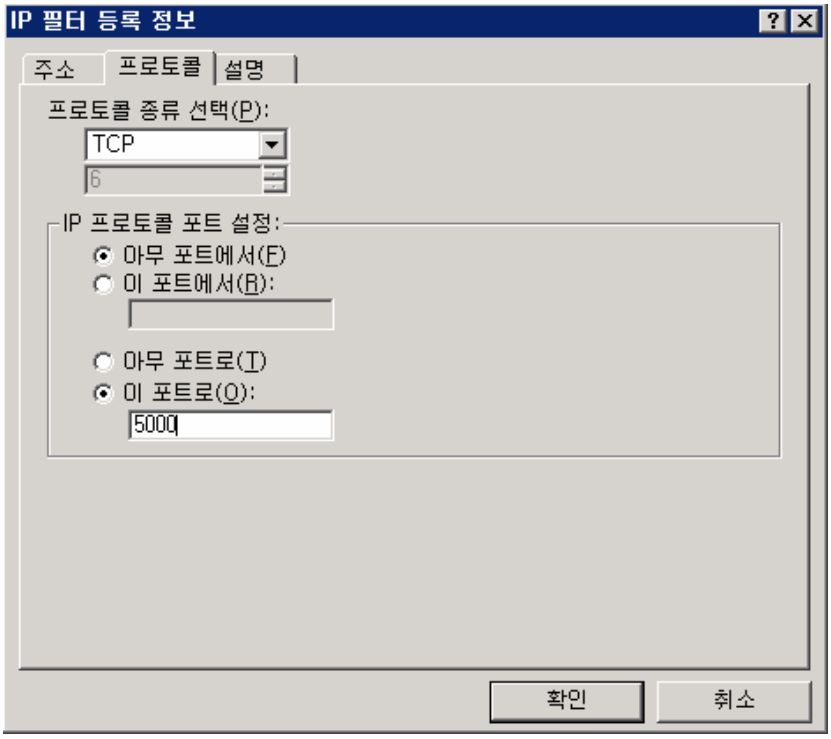
④ 상기 화면에서 [추가] 를 클릭합니다.

⑤ [주소]탭 → Out-in 설정시 원본주소에는 [모든 IP주소] 대상주소에는 [내IP주소]로 선택 합니다.

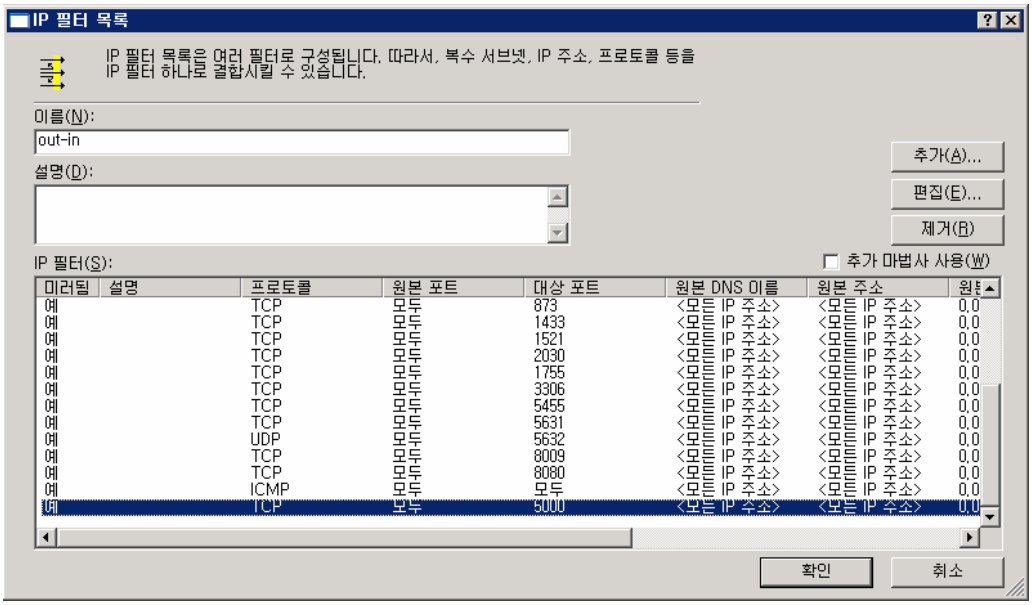


⑥ [프로토콜] 탭 → [프로토콜 종류 선택] – [IP 프로토콜 포트 설정]에서 [아무

포트에서] [이 포트로] 선택 – 오픈 하여 줄 포트(ex. 5000)를 입력한 후 확인버튼을 클릭해 줍니다.



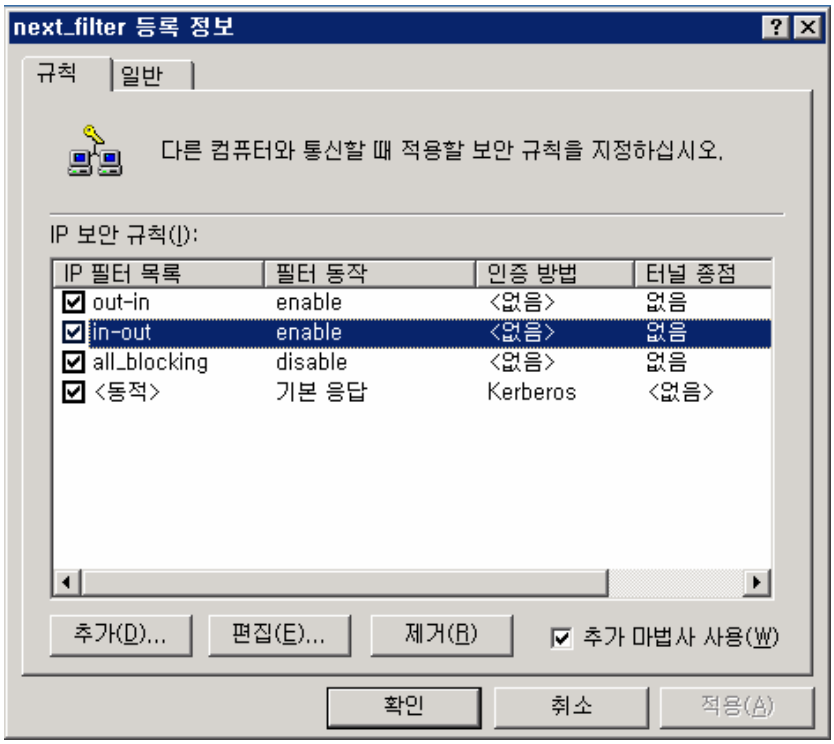
⑦ TCP 5000 포트 추가 완료된 상태 입니다.



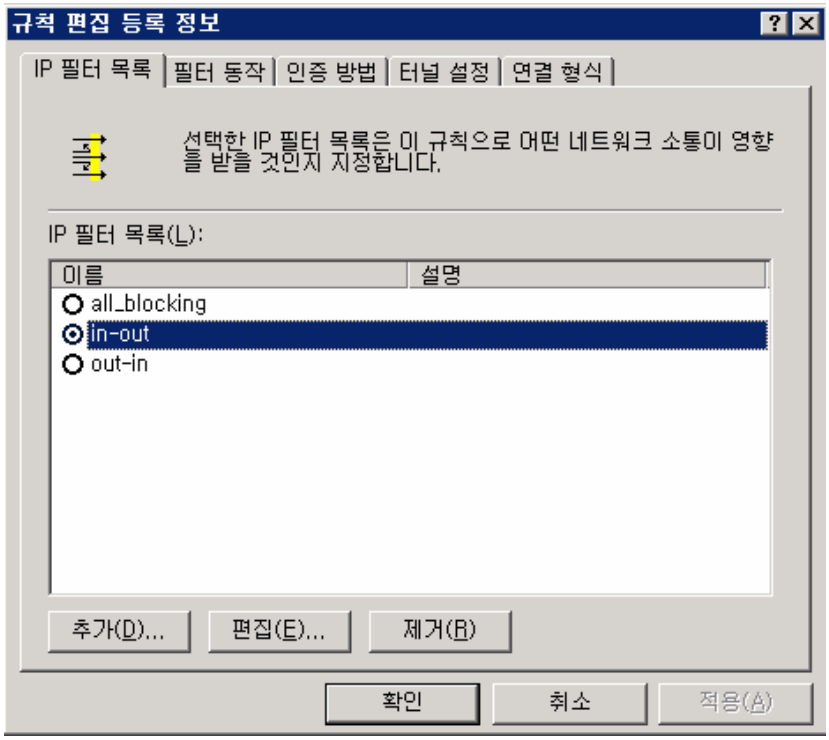
추가 완료 후 [확인] – [닫기] – [확인] 을 클릭 합니다.

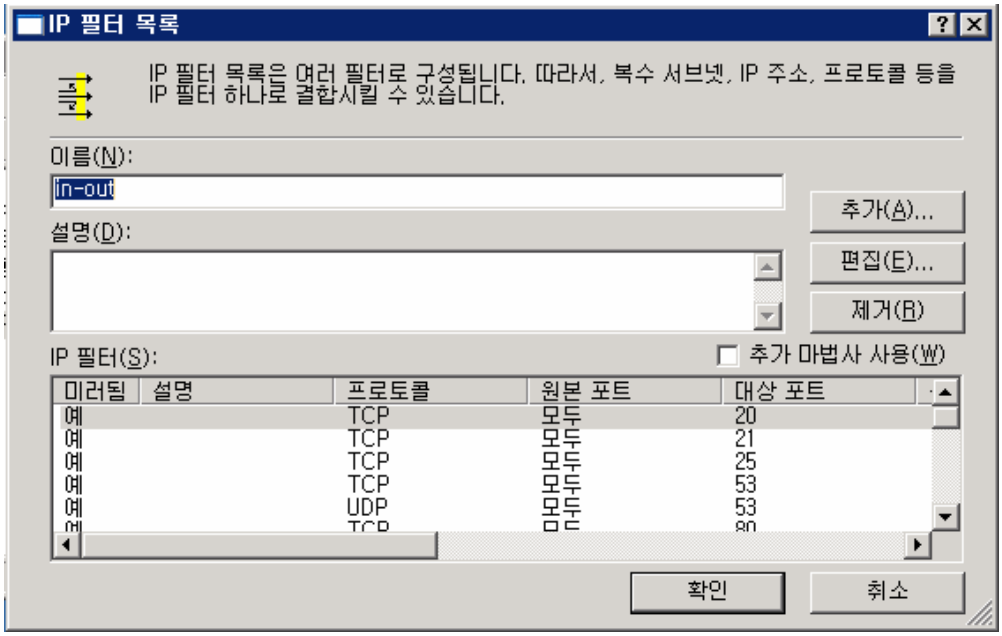
5) In-Out Port추가 방법

① [In-out]을 선택하고 [편집]을 클릭 합니다.



② [In-out] 을 선택한 후 [편집]을 클릭 합니다.

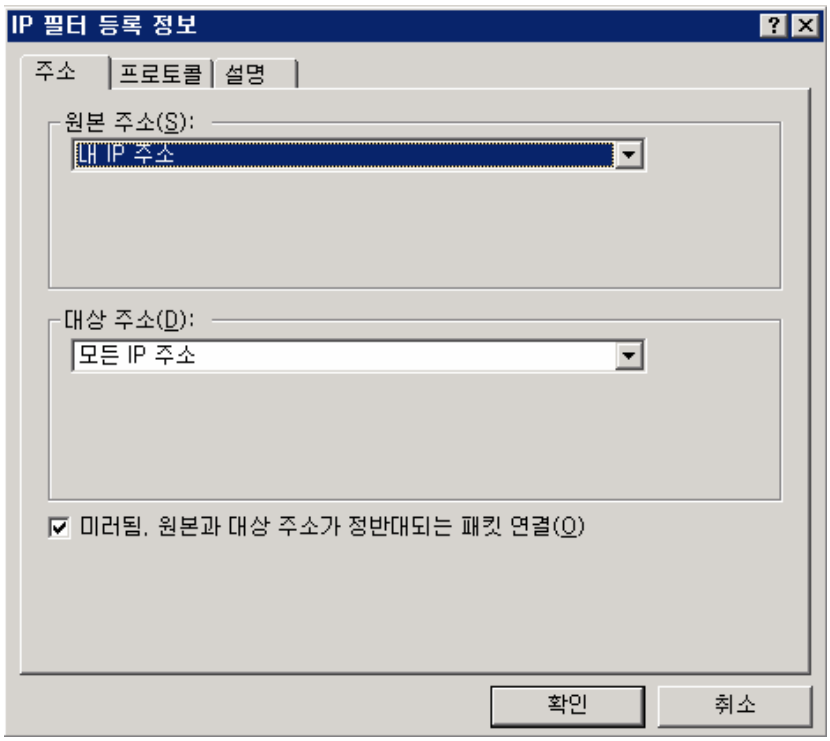




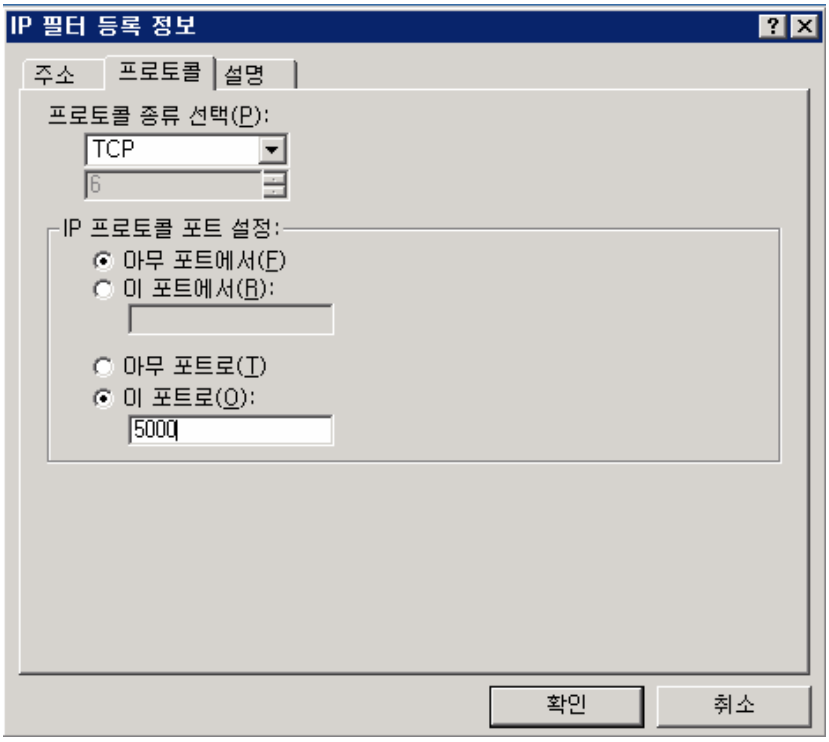
이 화면에서 각 IP 필터를 추가하거나 편집 제거가 가능합니다.

③ 상기 화면에서 [추가] 를 클릭합니다.

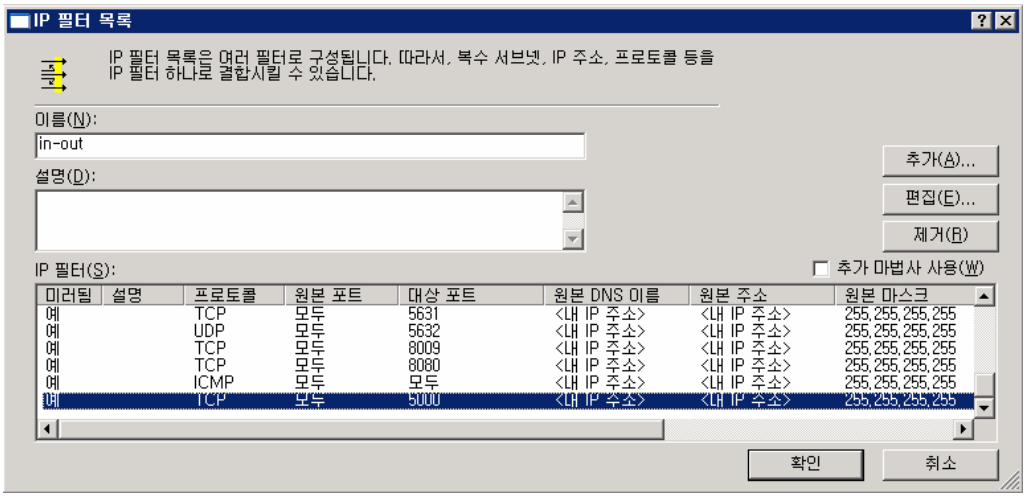
④ [주소] 탭 → In-out 설정 시 원본주소에는 [내 IP주소] 대상주소에는 [모든 IP주소]로 선택 합니다.



⑤ [프로토콜] 탭 → [프로토콜] 종류 선택 – [IP 프로토콜 포트 설정]에서 [아무 포트에서] [이 포트로] 선택 – 오픈 하여 줄 포트(ex. 5000)를 입력한 후 [확인]버튼을 클릭해 줍니다.



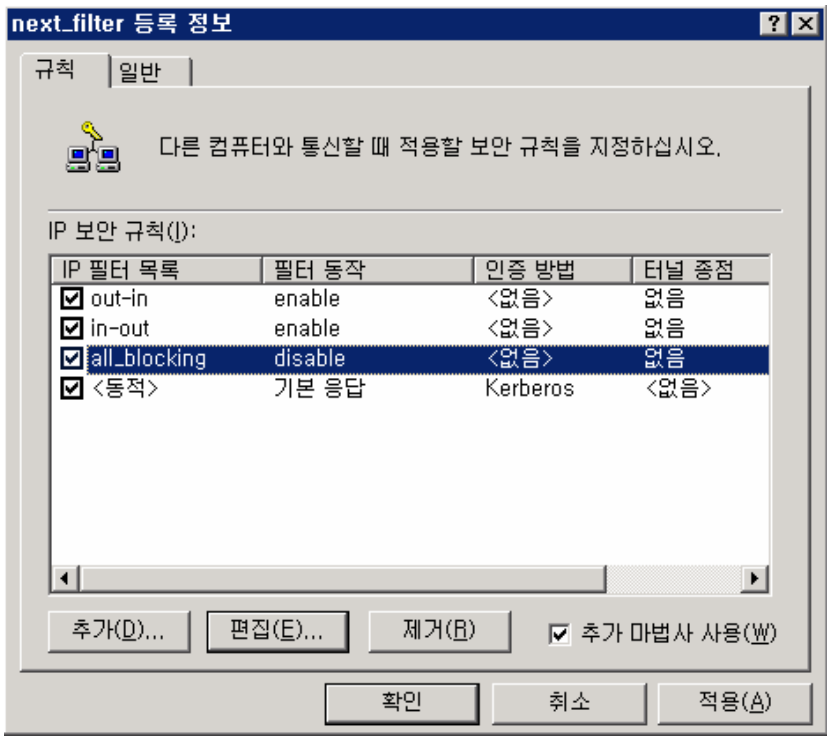
⑥ TCP 5000 포트 추가 완료된 상태 입니다.



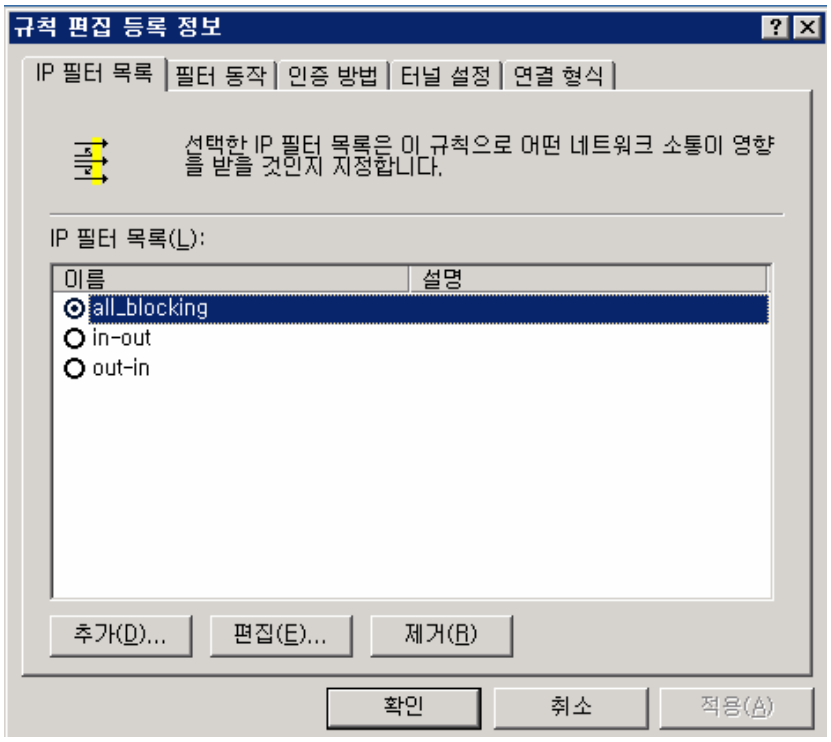
6) All_blocked (특정 아이피 차단하기)설정하기

기본 적으로 All_blocked는 위에서 오픈 하여 준 포트 외에 나머지 포트를 차단하는데 여기에 추가로 특정 아이피 전체를 차단 할 시에는 필터 등록 정보에 아래와 같이 차단시킬 아이피를 설정하여 줍니다.

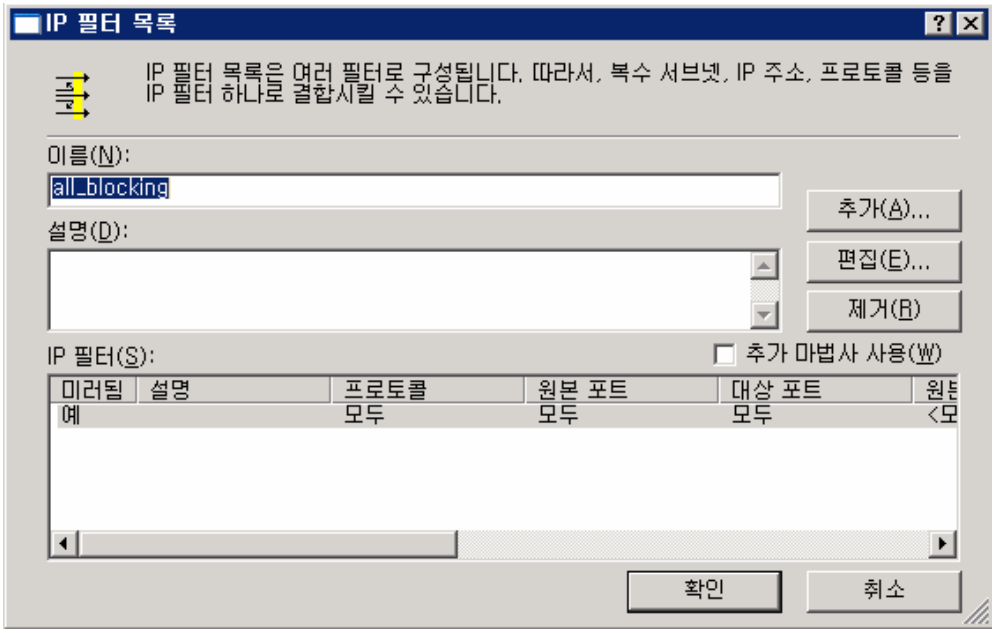
① [all_blocking] 를 선택 후 [편집] 을 클릭합니다.



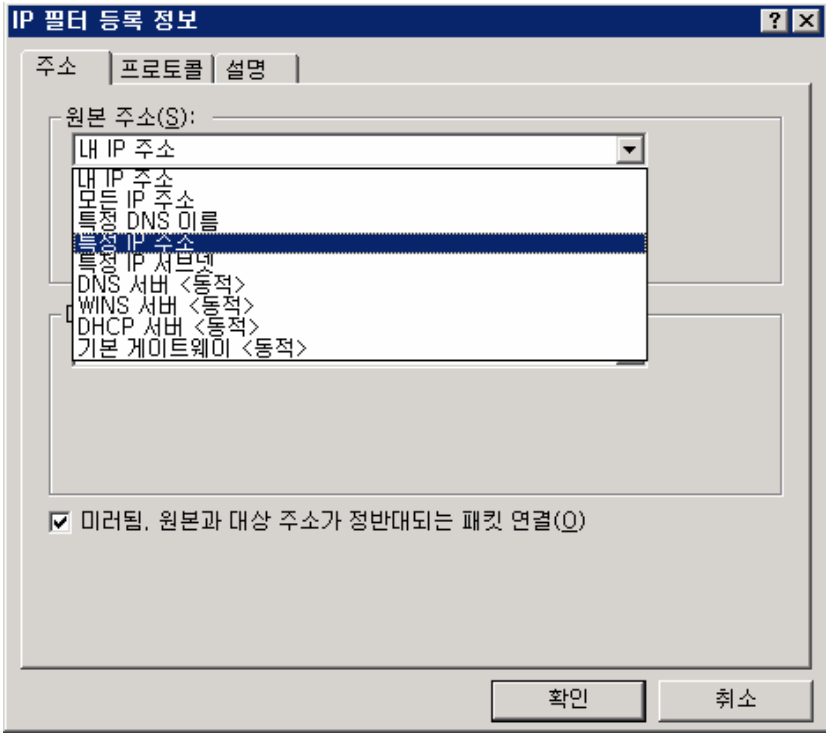
② [all_blocking] 을 선택 후 [편집] 을 클릭합니다.

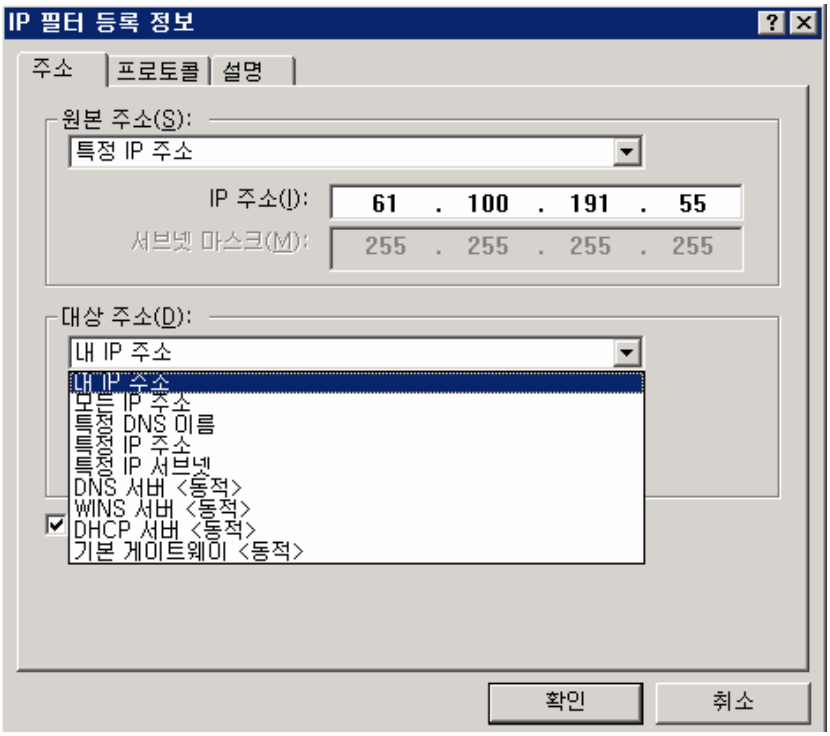


③ [추가] 를 클릭 합니다.

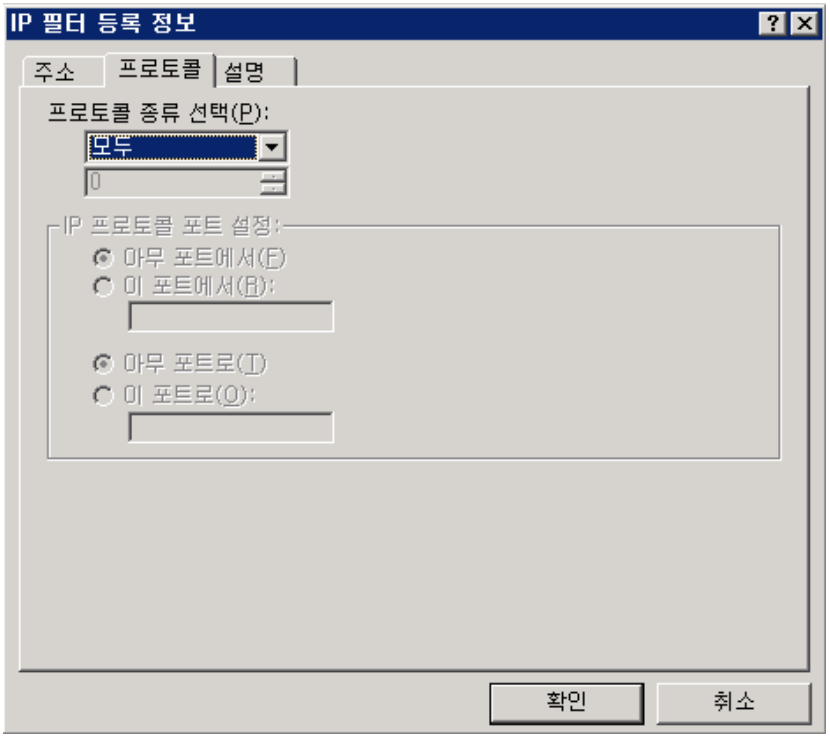


④ [주소] 탭에서 [원본주소]에 차단하고자 하는 IP(ex. 61.100.191.55) 를 입력, [대상주소]에 [내 IP 주소]를 선택 합니다.

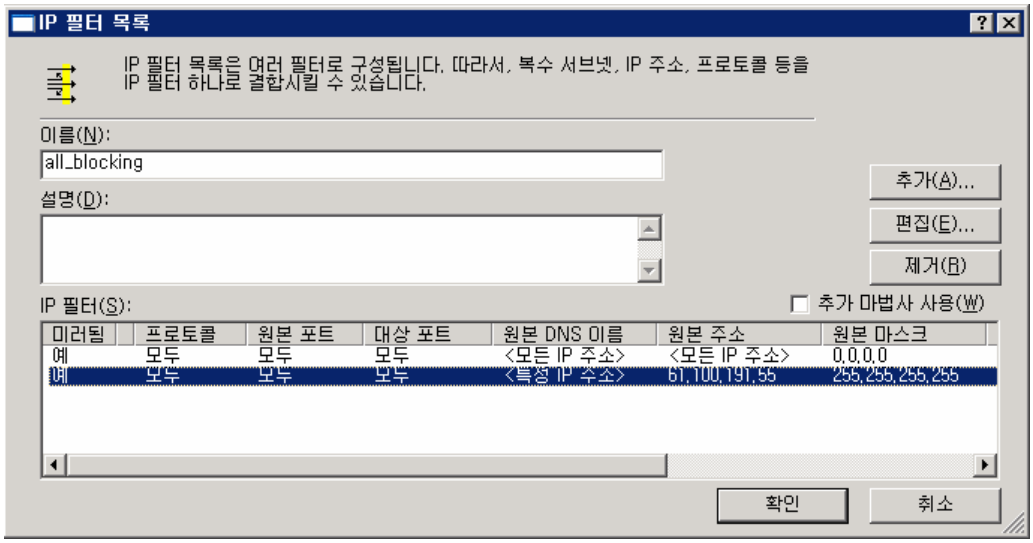




⑤ [프로토콜] 텝에서 [프로토콜 종류 선택]의 종류는 [모두] 를 선택 후 [확인]을 클릭 합니다.



⑥ IP 차단 완료된 상태 입니다.



⑦ 특정 IP가 아닌 IP 대역을 차단 하고자 할 경우 " 4) " 에서 설정한 부분에 아래와 같이 [특정 IP 서브넷]을 선택 후 해당 IP 블록을 설정하면 됩니다.