► SSL 설치 매뉴얼

매뉴얼 구성

1. SSL 설치

Microsoft Windows server 설치방법

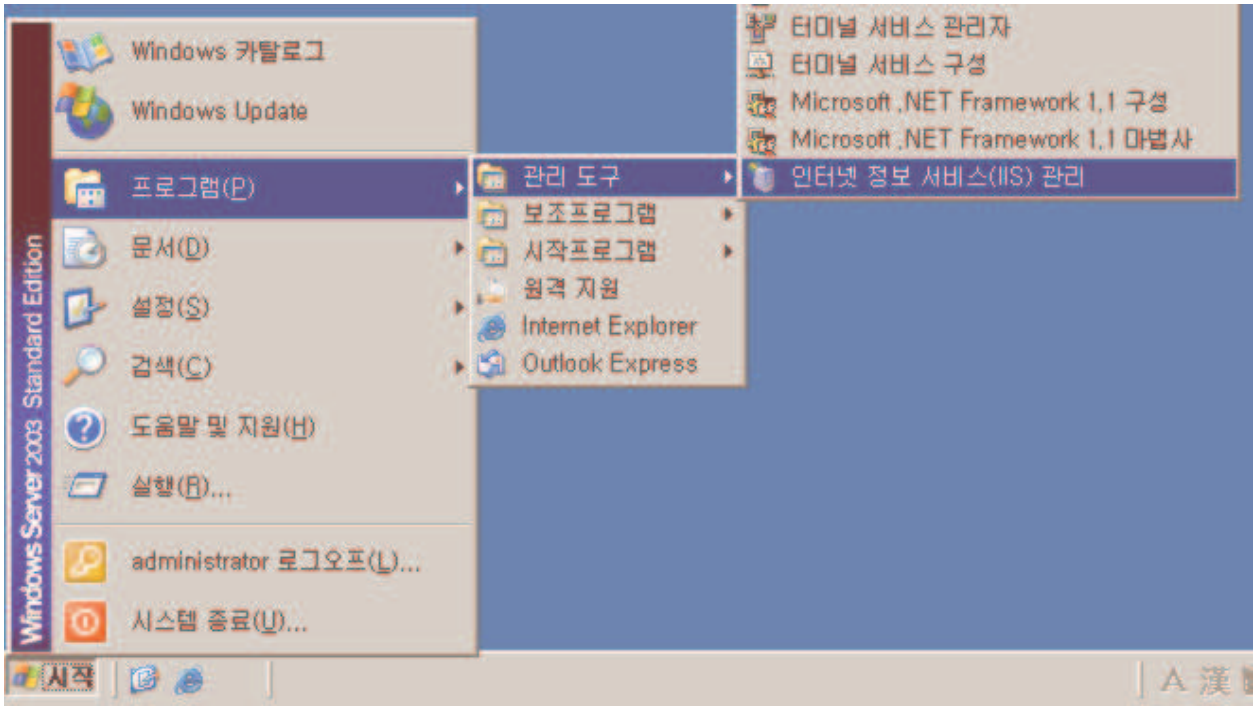
SSL을 사용하기 위하여 공인 인증키가 사용자 컴퓨터에 있어야 합니다.

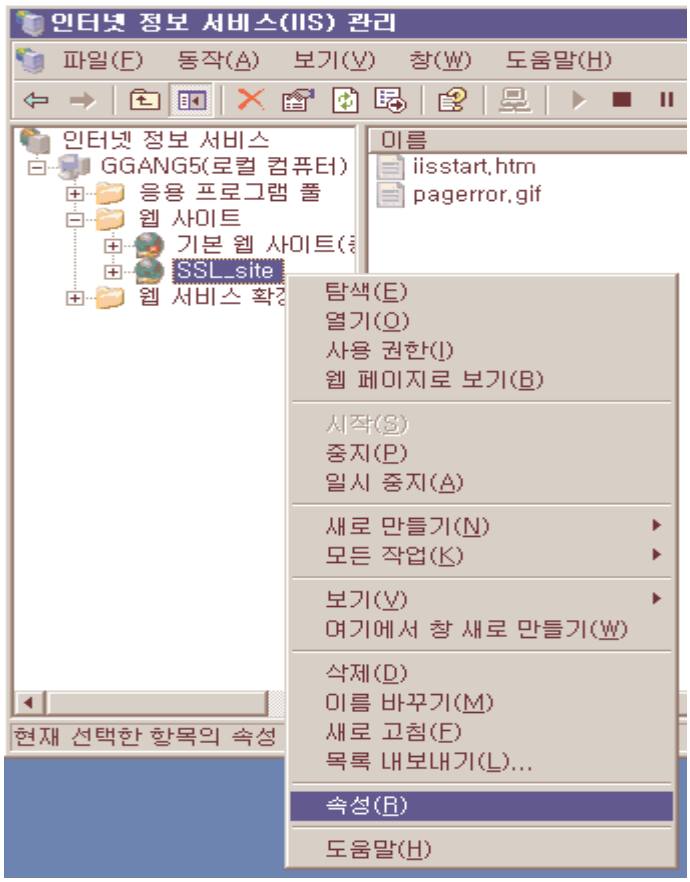
공인 인증키는 '새 인증서 만들기'를 이용하여 개인키 생성 후 CSR(Certificate Signing Request)를 인증기관에 보냅니다.

사용자는 인증 기관에서 확장자.crt 의 파일을 받아 서버에 설치 하게 됩니다.

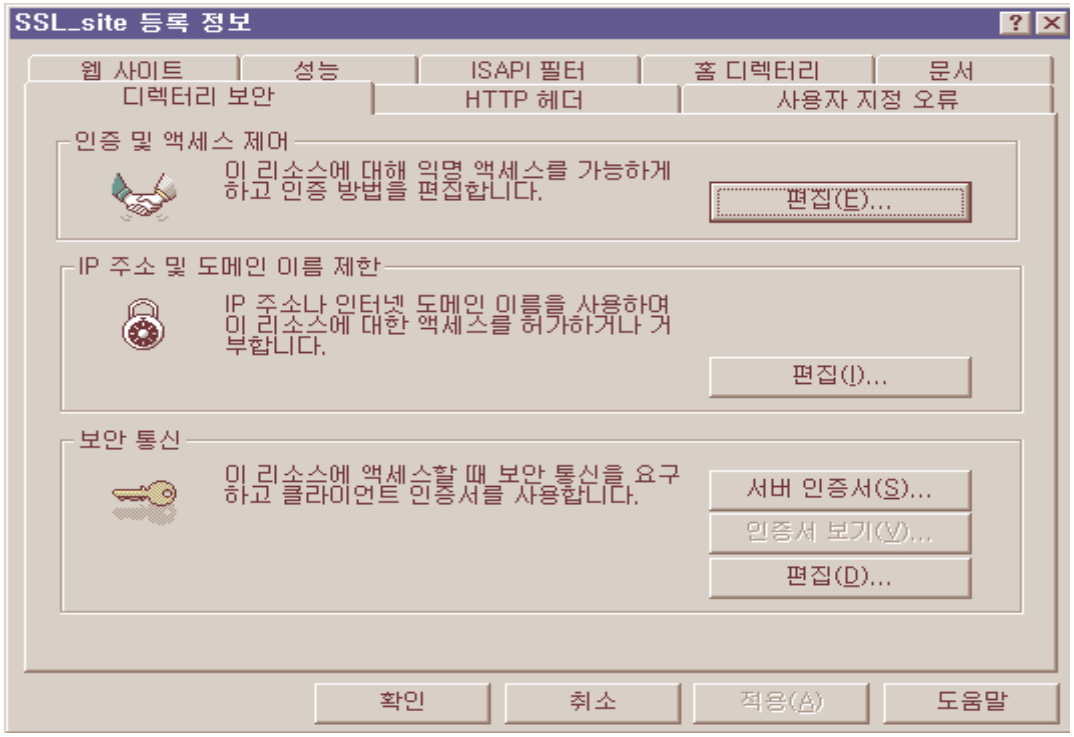
[1] 개인키 생성과 CSR 파일 생성

1. 시작 > 프로그램 > 관리도구 > 인터넷 서비스 관리자 > 웹사이트 > 속성

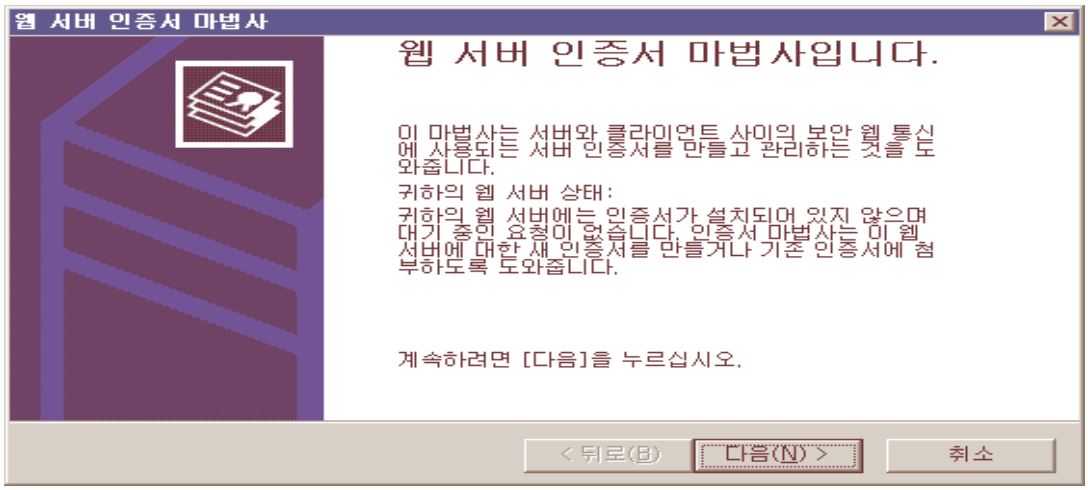




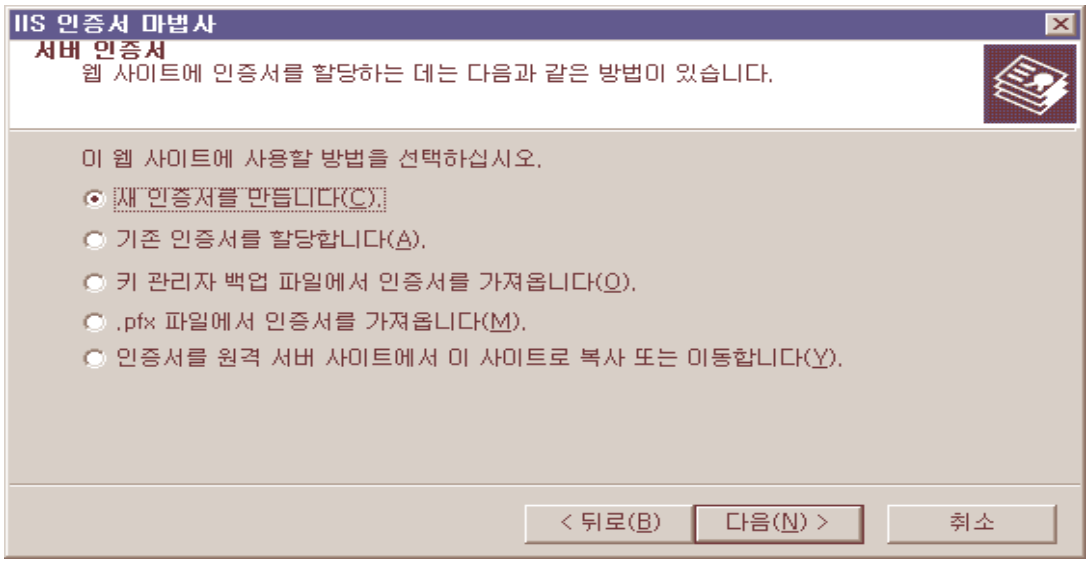
3. '등록 정보' 화면에서 '디렉토리 보안'을 클릭 후 '서버 인증서'를 클릭합니다.



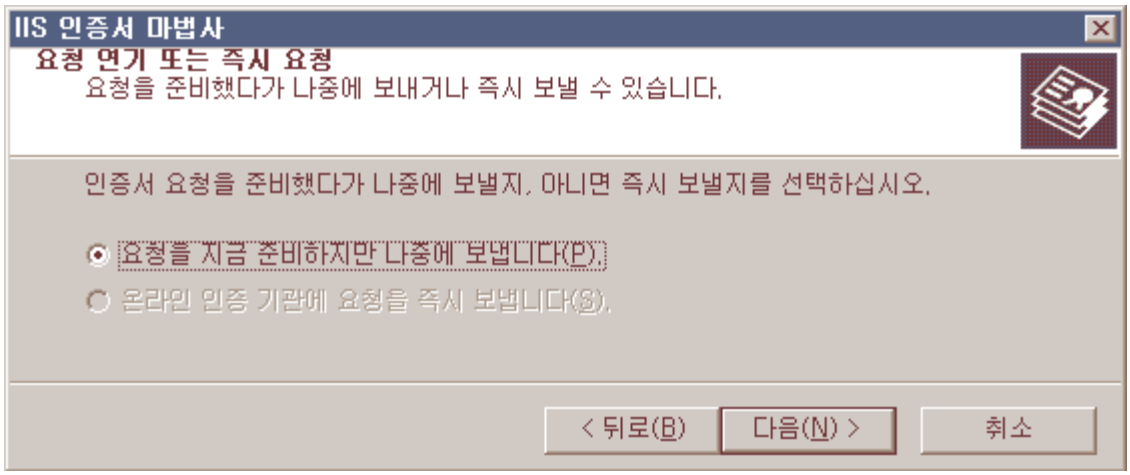
4. '웹서버 인증서 마법사'를 시작합니다. '다음'을 선택합니다.



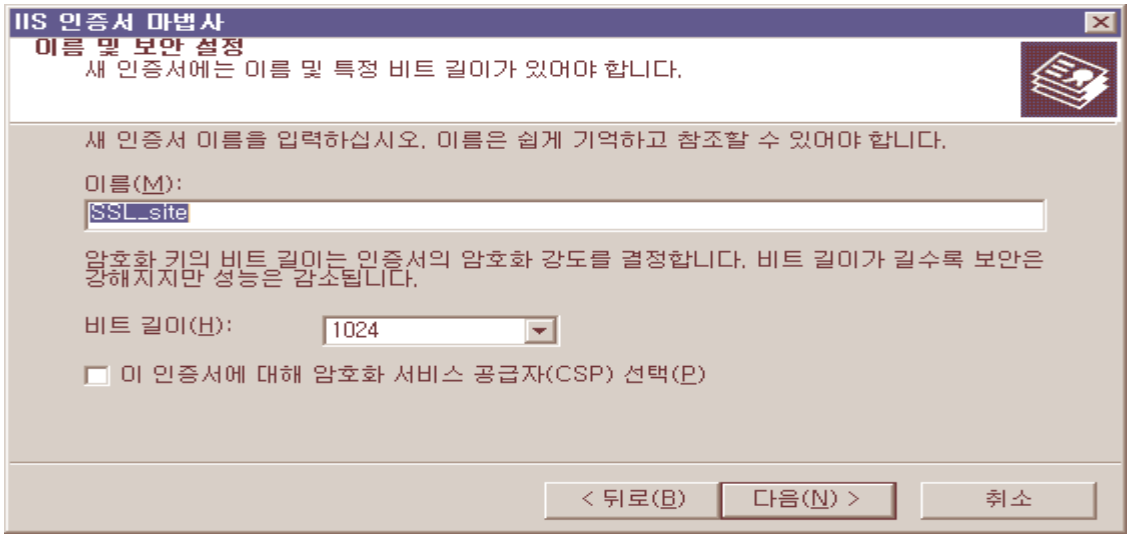
5. '새 인증서를 만듭니다'를 체크 후 '다음'을 선택합니다.



6. '요청을 지금 준비하지만 나중에 보냅니다' 를 체크 후 '다음'을 선택합니다. (CSR 파일 생성)



7. 새 인증서 이름을 정해주기 위해 적당한 단어를 넣어 줍니다.

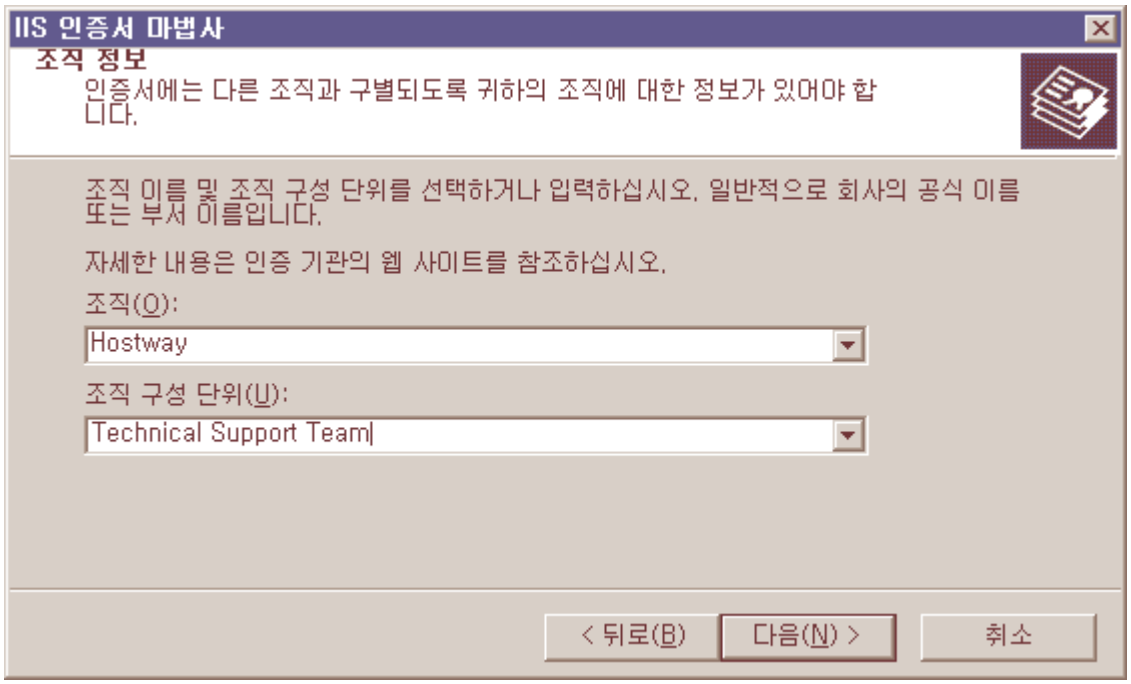


8. '조직 정보'를 입력 합니다.

조직(회사)명, 조직구성 단위(부서명)을 영문으로 입력합니다.

인증 받기 위한 도메인의 등록 정보를 반드시 참조하여 입력해야 합니다.

(특수 문자 (< > ~ ! @ # $ % ^ * / ₩ ( ) ?) 는 사용 할 수 없습니다.)

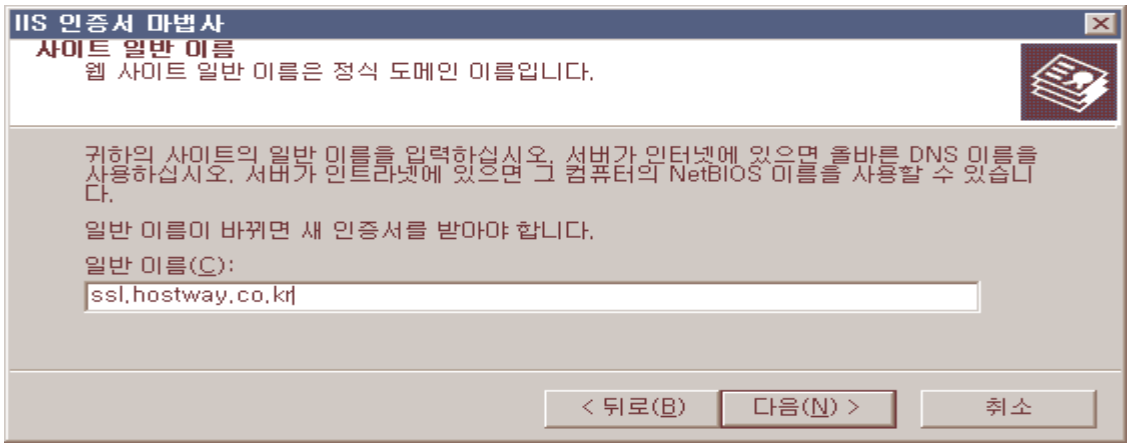


9. 인증 받을 도메인 이름을 입력 합니다.

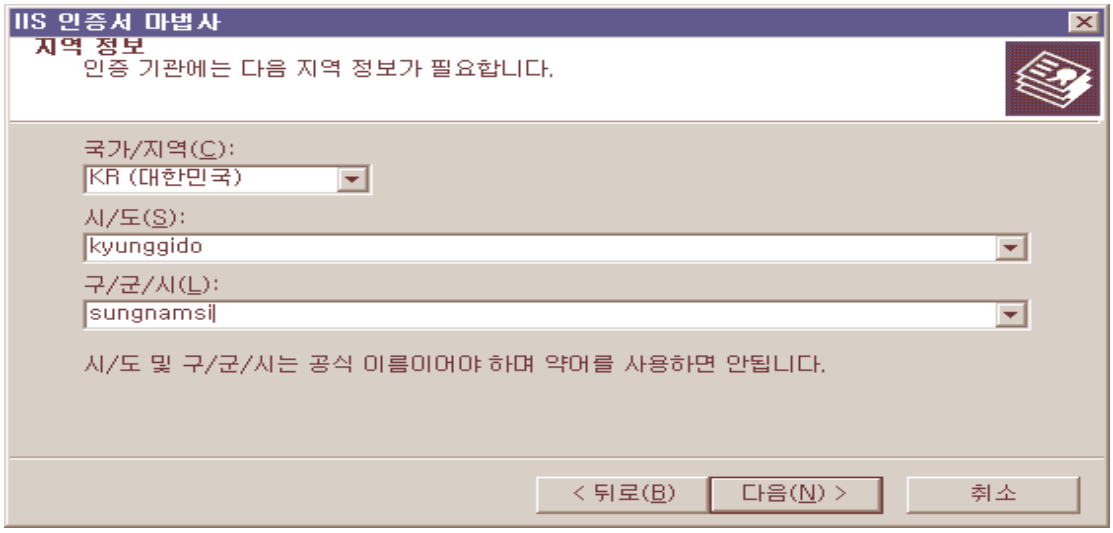
* 발급 완료된 인증서는 재발급 또는 변경이 불가능 합니다. CSR 생성시 주의 하시기 바랍니다.

* "일반이름" 의 hostway.co.kr / hostway.co.kr 은 서로 다른 인증서가 되므로, 적용할 웹사이트의 도메인주소와

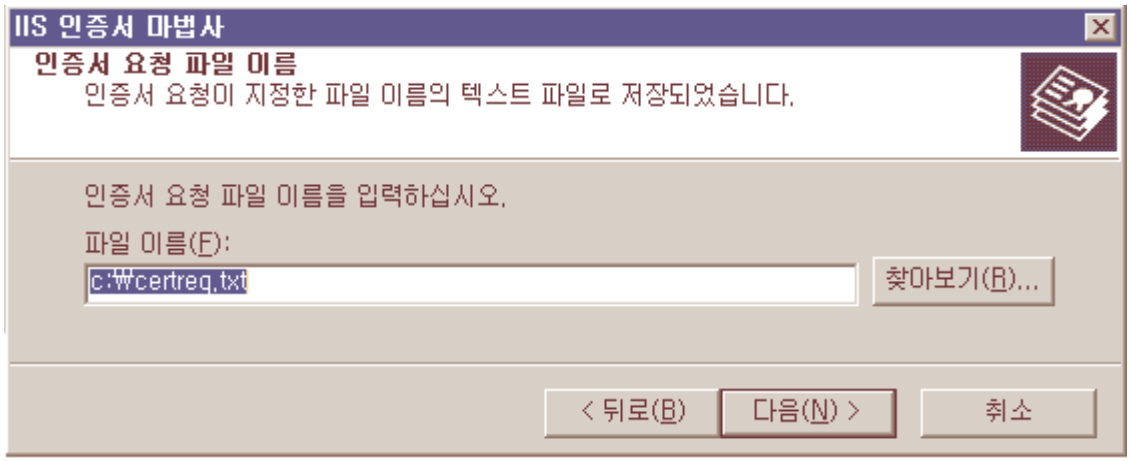
동일하게 입력 합니다.



10. '지역 정보'를 입력합니다.

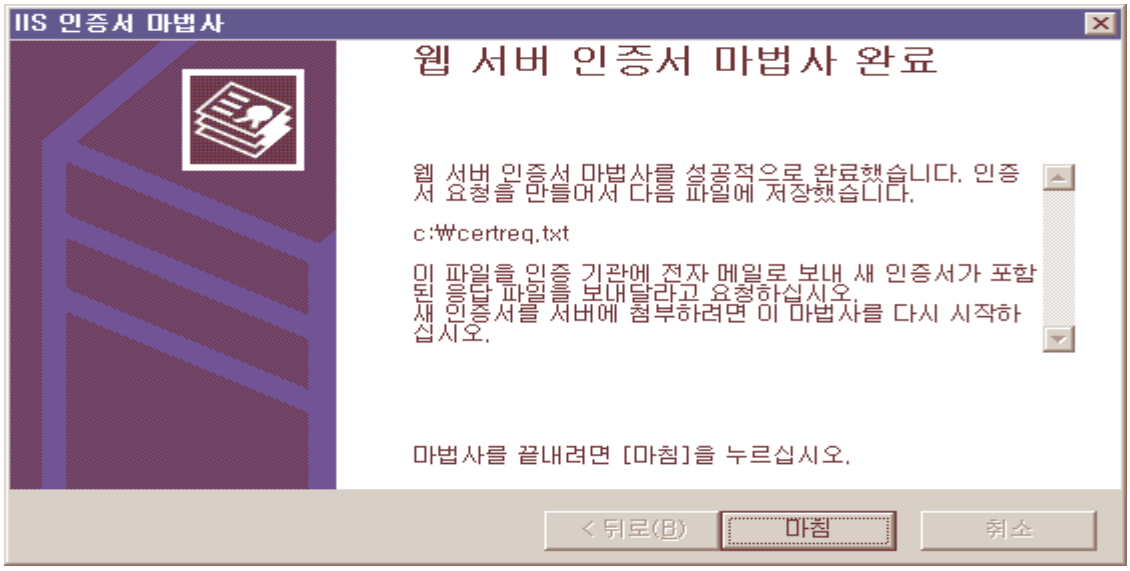


11. CSR(Certificate Signing Request)인증서 요청 파일 이름을 입력합니다.



12. '요청 파일 요약'에서 인증서 요청 정보가 정확한지 확인합니다.

13. '마침'을 클릭한 후 지정한 경로에 저장된 파일을 확인합니다. C:₩certreq.txt

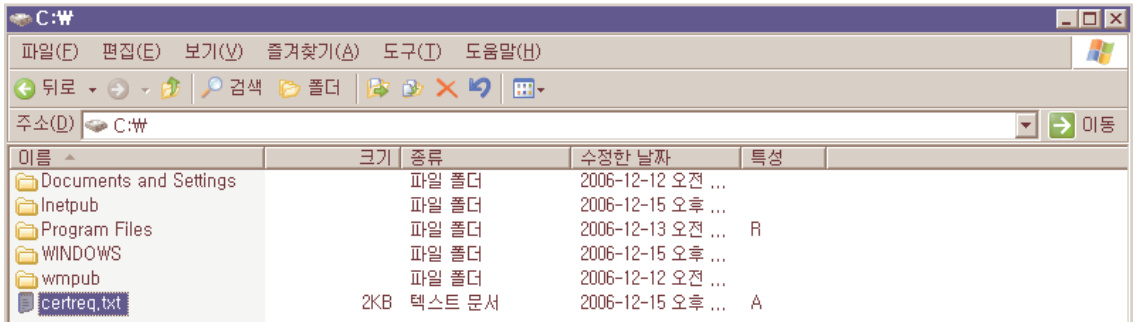


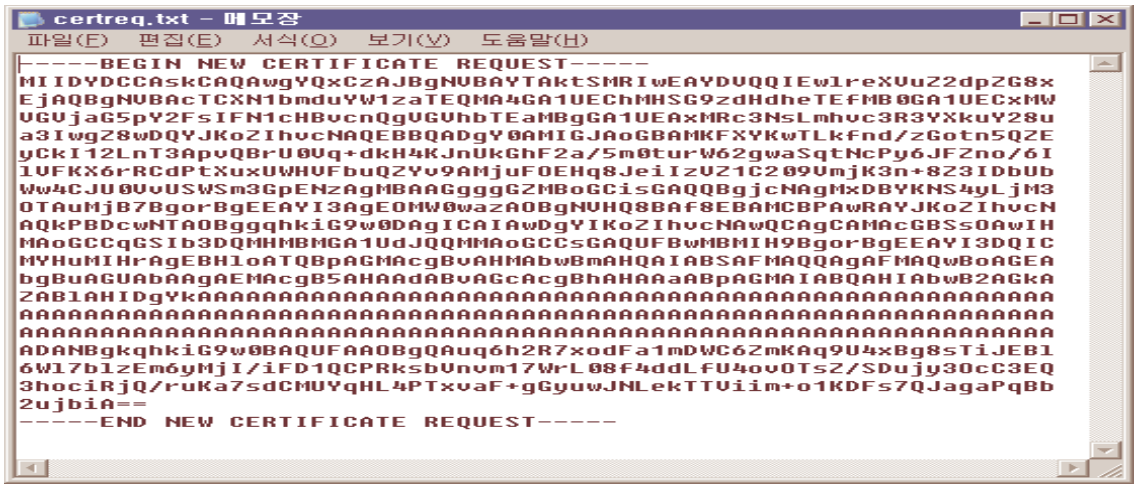
14. 지정하신 경로에 생성된 certreq.txt 파일을 열어 -BEGIN NEW CERTIFICATE REQUEST 부터 -END NEW CERTIFICATE REQUESET 까지 모두 복사 합니다.

CSR(Certificate Signing Request)접수를 위해 복사한 내용을 인증기관의 메일 또는 관련 웹사이트에 붙여 넣기 하여 발송/신청 합니다.

인증 기관의 인증 절차가 끝나면, 인증 기관의 답신 메일로(인증 기관에 따라 다를 수 있음) 확장자가 .crt 인 파일을 받을 수 있습니다.

* Multi-Domain SSL 의 경우 1개의 웹 사이트에서만 CSR값 을 생성합니다.

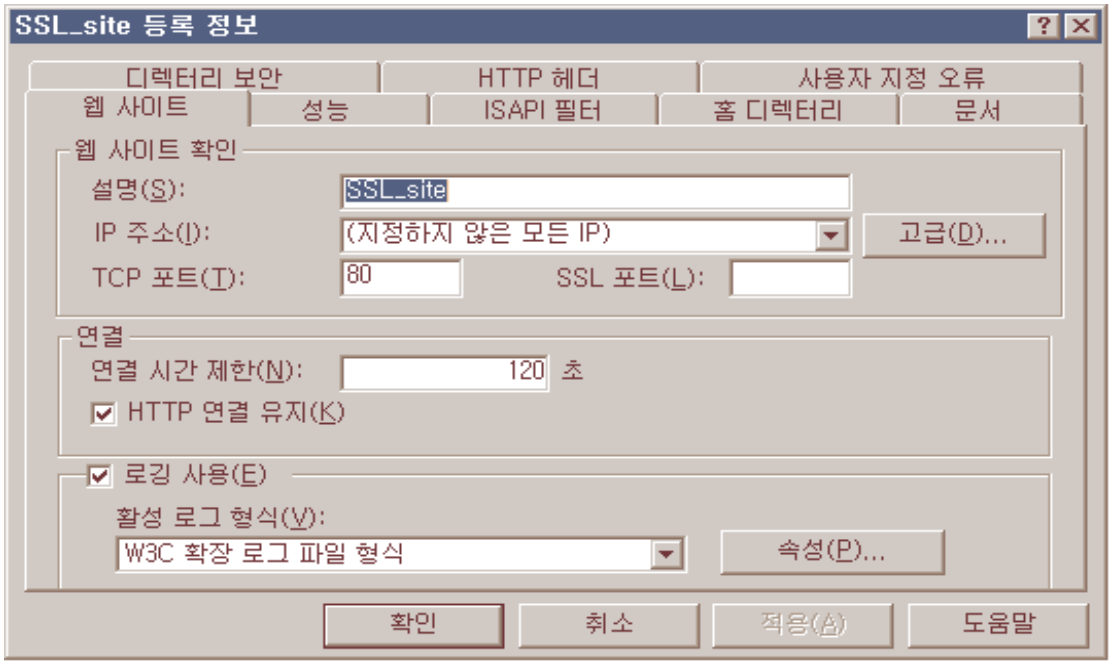

C:₩
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로 검색 폴더
주소(D) C:₩
이동
이름 크기 종류 수정한 날짜 특성
Documents and Settings 파일 폴더 2006-12-12 오전 ...
Inetpub 파일 폴더 2006-12-15 오후 ...
Program Files 파일 폴더 2006-12-13 오전 ... R
WINDOWS 파일 폴더 2006-12-15 오후 ...
wmpub 파일 폴더 2006-12-12 오전 ...
certreq.txt 2KB 텍스트 문서 2006-12-15 오후 ... A


certreq.txt - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDYDCCAskCAQAwgYQxCzAJBgNVBAYTAktSMRIwEAYDVQQIEwlreXVuZ2dpZG8x
EjAQBgNVBAcTCXN1bmduYW1zaTEQMA4GA1UEChMHSG9zdHdheTEfMB0GA1UECxMW
VGVjaG5pY2FsIFN1cHBvcnQgVGVhbTEaMBgGA1UEAxMRc3NsLmhvc3R3YXkuY28u
a3IwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMKFXYKwTLkfnd/zGotn5QZE
yCkI12LnT3ApvQBrU0Vq+dkH4KJnUkGhF2a/5m0turW62gwaSqtNcPy6JFZno/6I
1VFKX6rRCdPtXuxUWHVFbuQZYv9AMjuFOEHq8JeiIzVZ1C209VmjK3n+8Z3IDbUb
Ww4CJU0VvUSWSm3GpENzAgMBAAGgggGZMBoGCisGAQQBgjcNAgMxDBYKNS4yLjM3
OTAuMjB7BgorBgEEAYI3AgEOMW0wazAOBgNVHQ8BAf8EBAMCBPAwRAYJKoZIhvcN
AQkPBDcwNTAOBggqhkiG9w0DAgICAIAwDgYIKoZIhvcNAwQCAgCAMAcGBSsOAwIH
MAoGCCqGSIb3DQMHMBMGA1UdJQQMMAoGCCsGAQUFBwMBMIH9BgorBgEEAYI3DQIC
MYHuMIHrAgEBH1oATQBpAGMAcgBvAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEA
bgBuAGUAbAAgAEMAcgB5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkA
ZAB1AHIDgYkAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ADANBgkqhkiG9w0BAQUFAAOBgQAuq6h2R7xodFa1mDWC6ZmKAq9U4xBg8sTiJEB1
6W17blzEm6yMjI/iFD1QCPRksbVnvm17WrL08f4ddLfU4ovOTsZ/SDujy3OcC3EQ
3hociRjQ/ruKa7sdCMUYqHL4PTxvaF+gGyuwJNLekTTViim+o1KDFs7QJagaPqBb
2ujbiA==
-----END NEW CERTIFICATE REQUEST-----

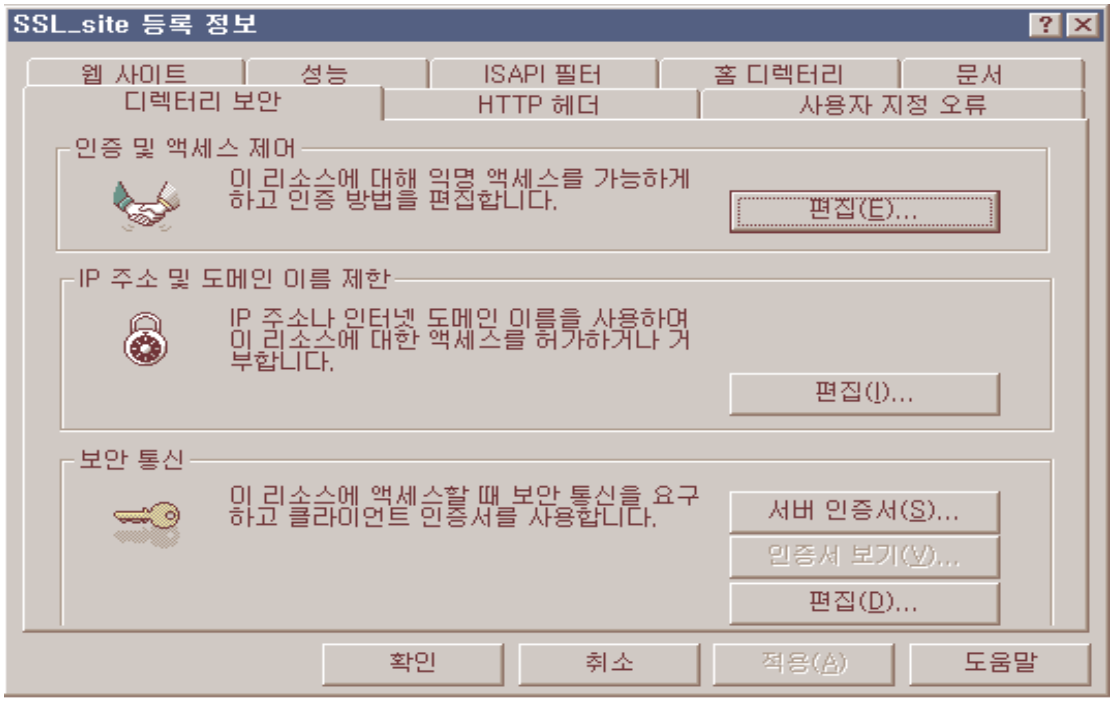
2. 웹 서버에 인증서 설치

1. 인증 기관에서 회신 받은 파일 (도메인.crt)을 서버에 복사 합니다.

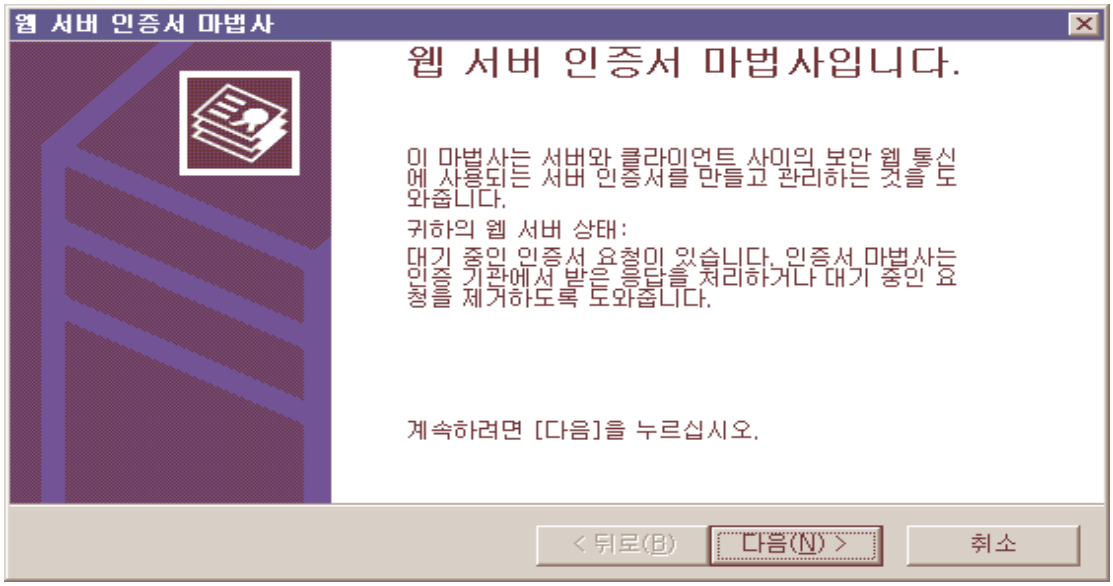
2. 시작 > 프로그램 > 관리도구 > 인터넷 서비스 관리자 > 등록할 웹 사이트의 등록정보를 확인 합니다.



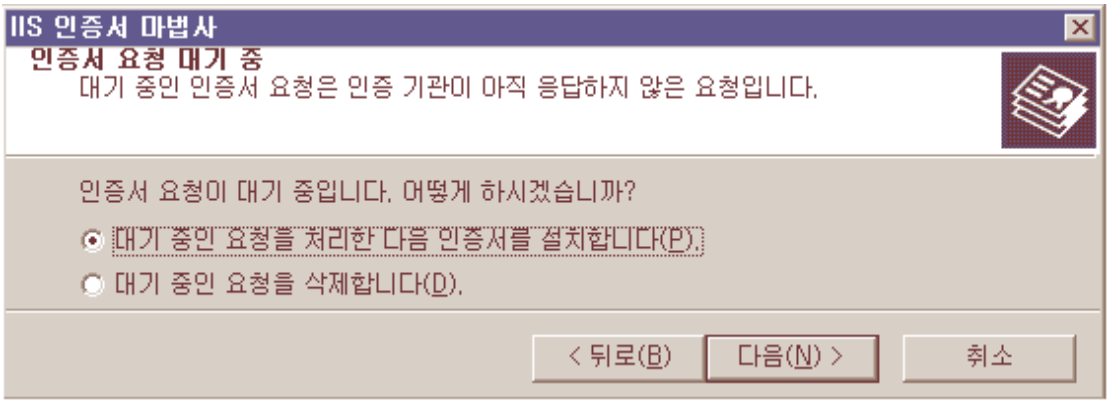
3. '디렉터리 보안'에 '서버 인증서'를 선택하여 '웹 서버 인증서 마법사'를 시작 합니다.



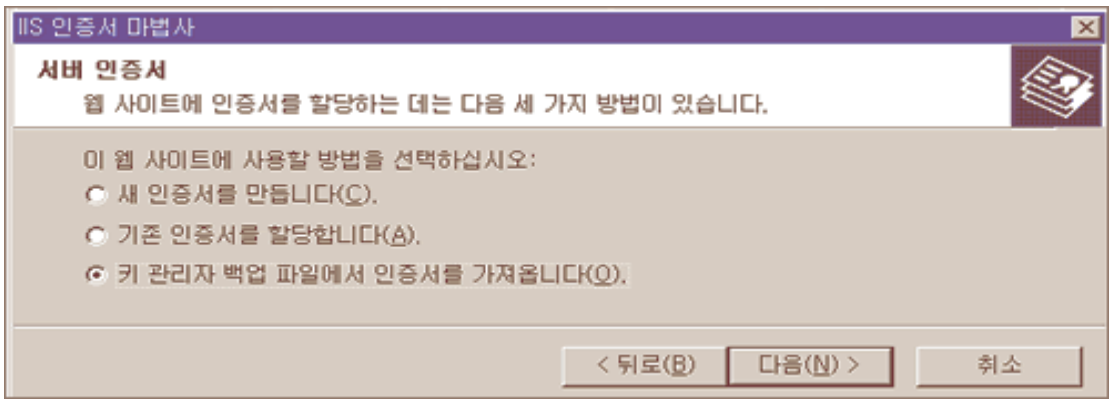
4. '웹 서버 인증서 마법사'를 시작 합니다.



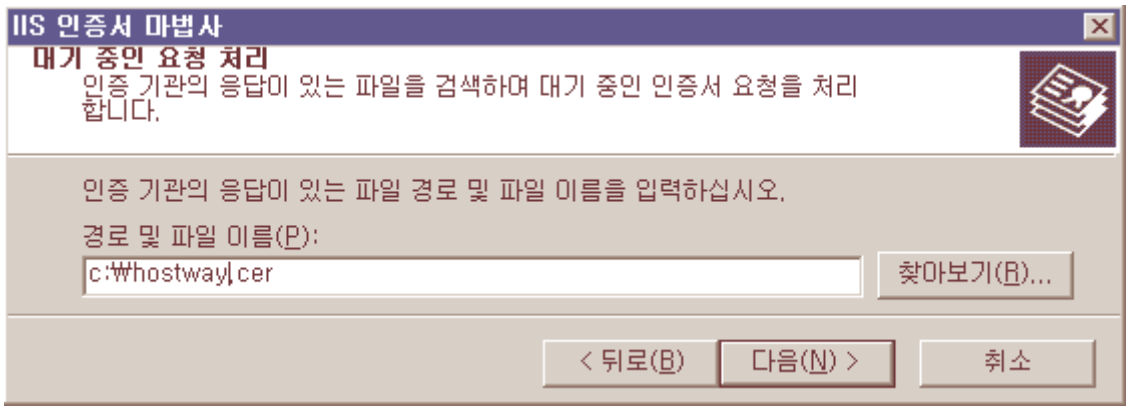
5. '보류 중인 요청을 처리한 다음 인증서를 설치합니다.'를 선택합니다.



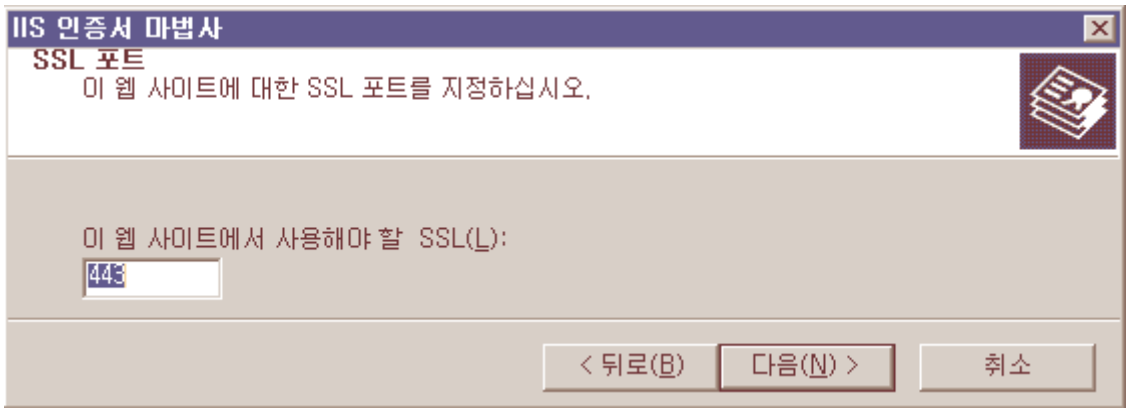
** 이미 인증서가 설치된 서버에서는 다음과 같은 메세지가 나타납니다. (처음 설치 서버 제외)



6. "대기 중인 요청 처리"에 인증 기관에서 발급된 파일의 경로를 지정하여 파일을 불러옵니다.

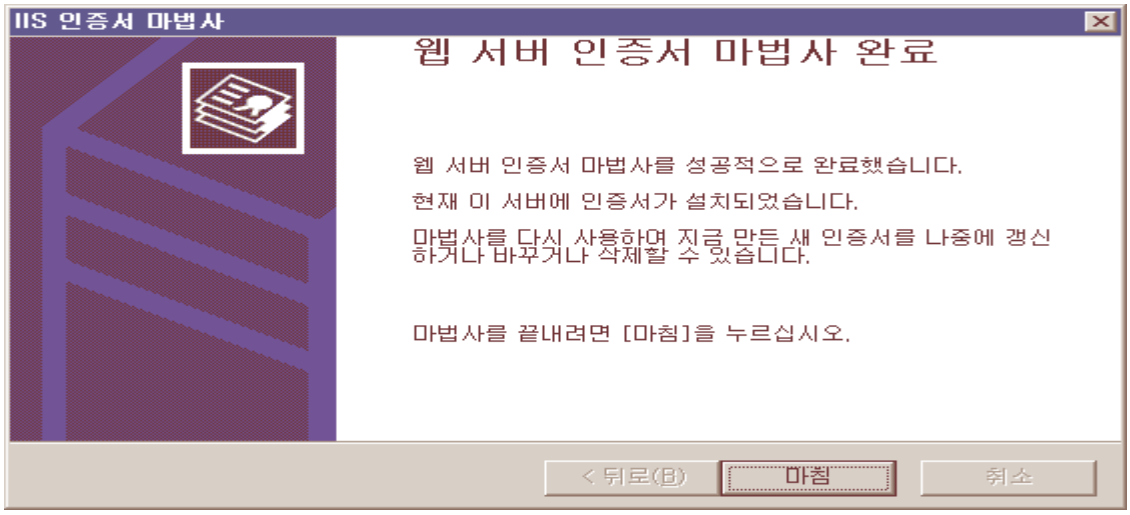


7. 'SSL 포트'를 지정 합니다.



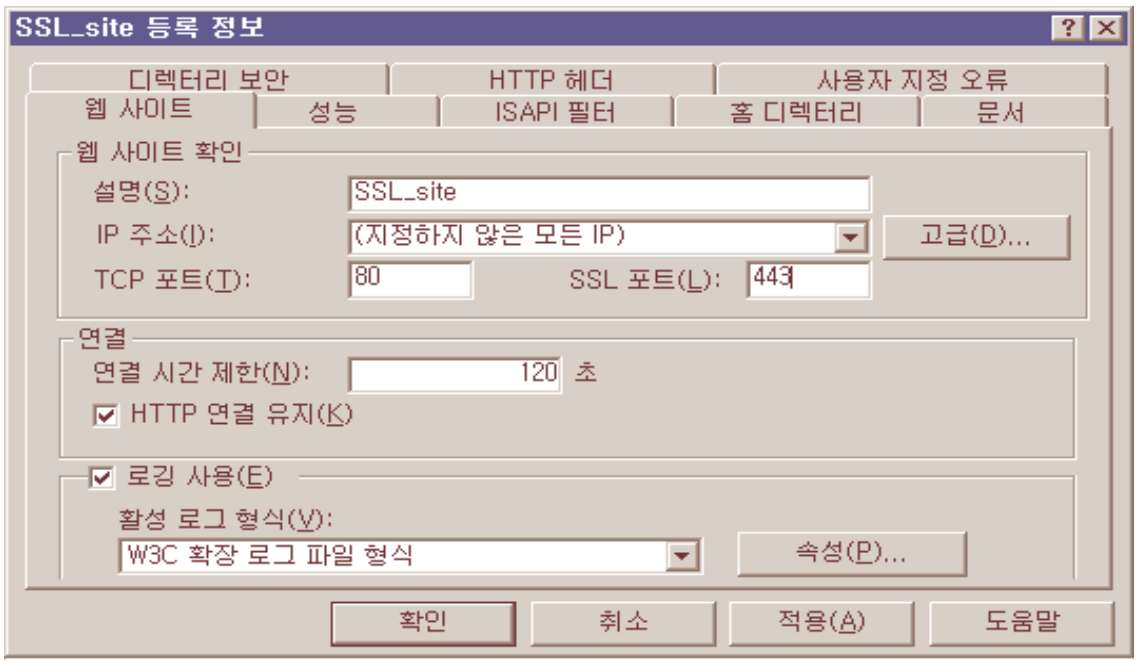
8. 인증서에 대한 상세 정보를 확인 할 수 있습니다.

9. 인증서 마법사가 완료 되었습니다.



10. 인증할 웹사이트의 등록 정보를 보면 SSL포트란이 활성화 되어 있습니다.

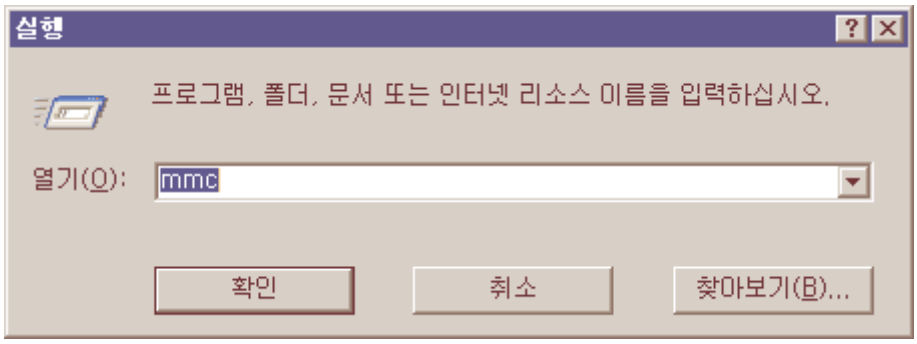
SSL포트에 443을 입력하고 '확인'을 선택합니다. (방화벽이 사용시 TCP 443 port open)



3. 루트 CA 인증서 설치

인증기관에서 받은 인증서 파일을 설치 합니다.

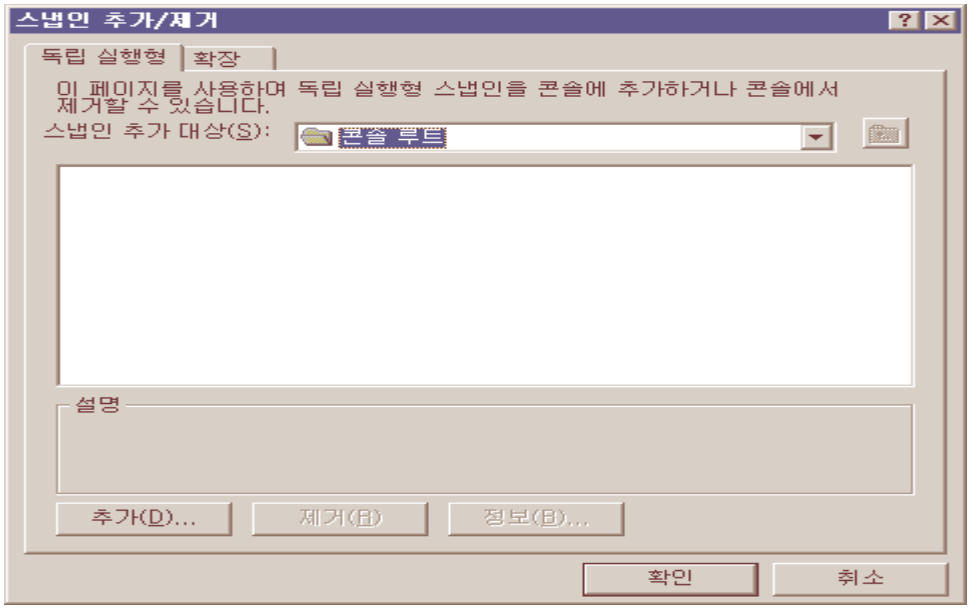
1. 시작 > 실행 > mmc 를 입력 후 확인을 선택 합니다.



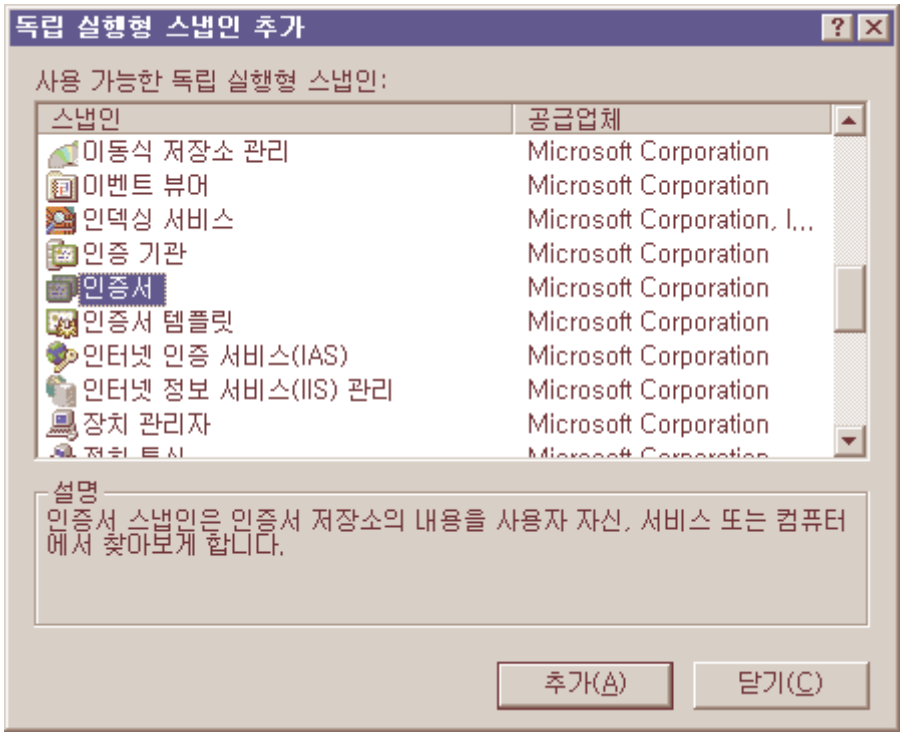
2.'콘솔' 창이 활성화 됩니다.

'파일'에서 '스냅인 추가/제거'를 선택 합니다.

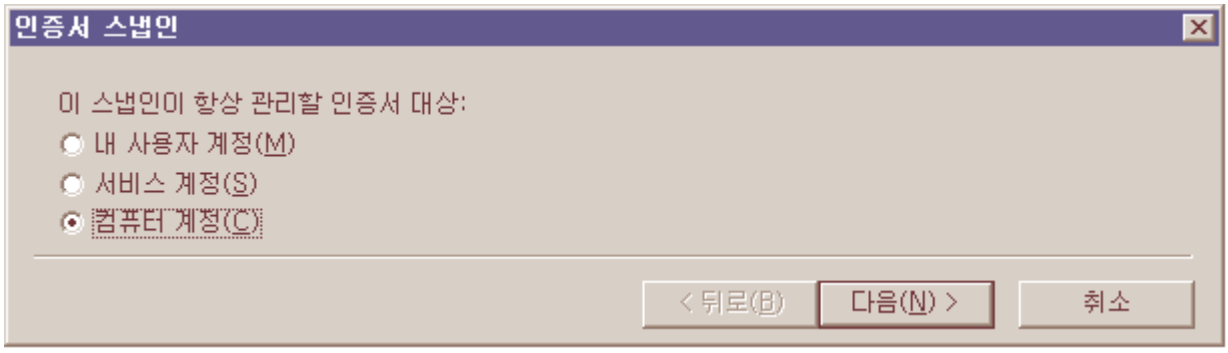
3.'스냅인 추가/제거'에서 '추가'를 클릭합니다.



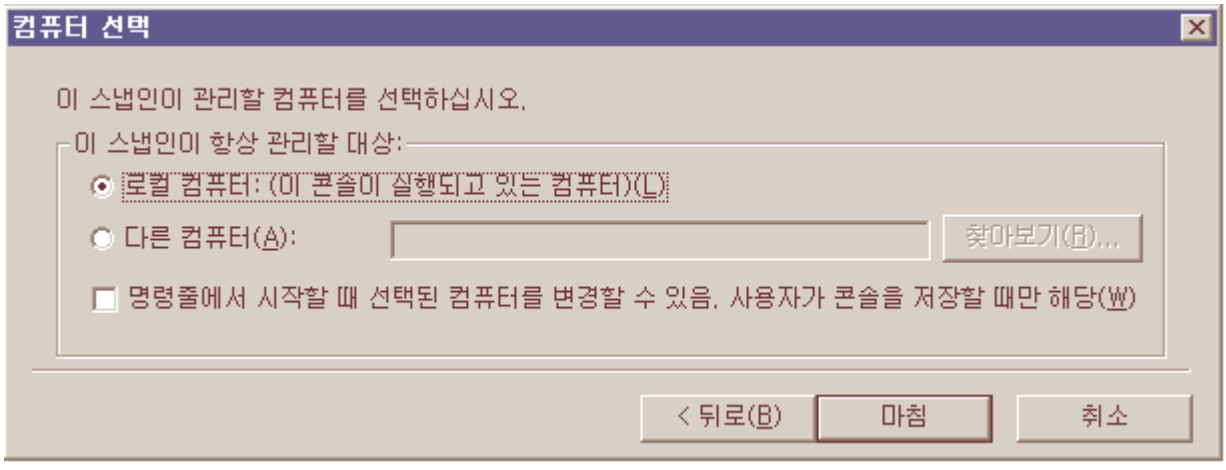
4.'독립 실행형 스냅인 추가' 에서 '인증서'를 선택 후 '추가'를 클릭 합니다.



5.'인증서 스냅인'에서 '컴퓨터 계정'을 선택 후 '다음'을 클릭 합니다.

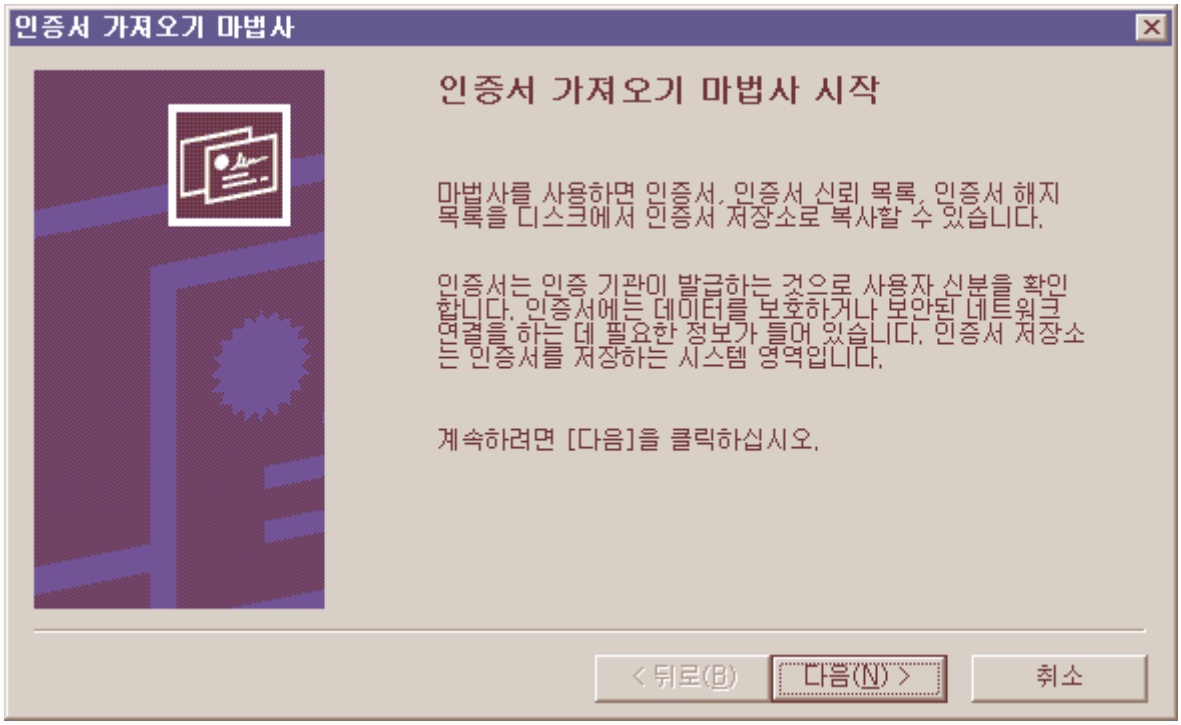


6.'컴퓨터 선택' 에서 '로컬 컴퓨터:(이 콘솔이 실행되고 있는 컴퓨터)'를 선택 후 '마침'을 클릭합니다.

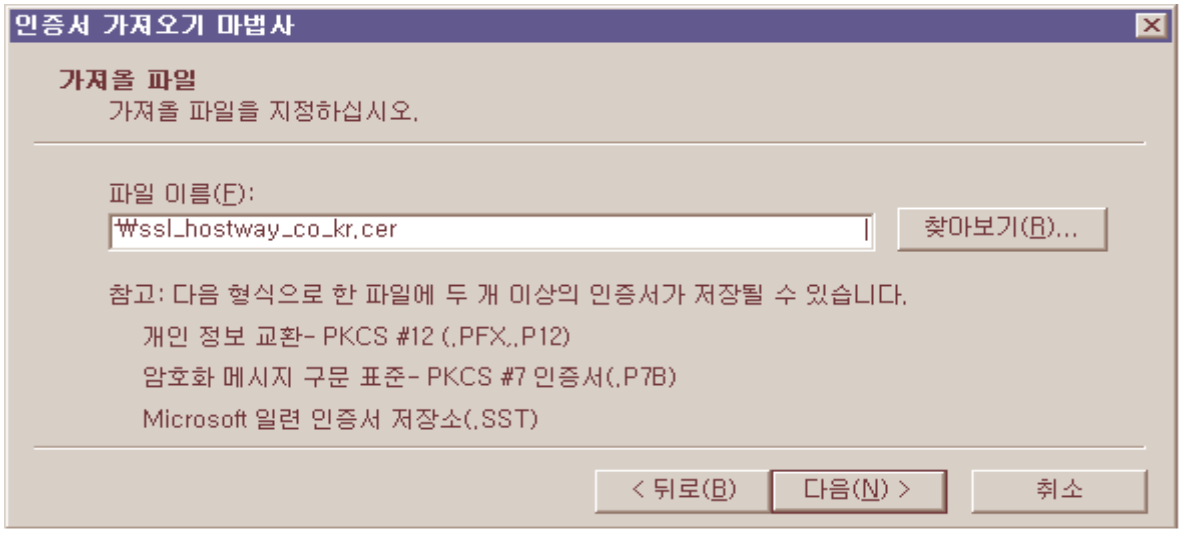


7. 콘솔의 '신뢰할 수 있는 루트 인증 기관'->'인증서'에 오른쪽 마우스를 클릭하여 '모든 작업'->'가져오기'를 클릭합니다

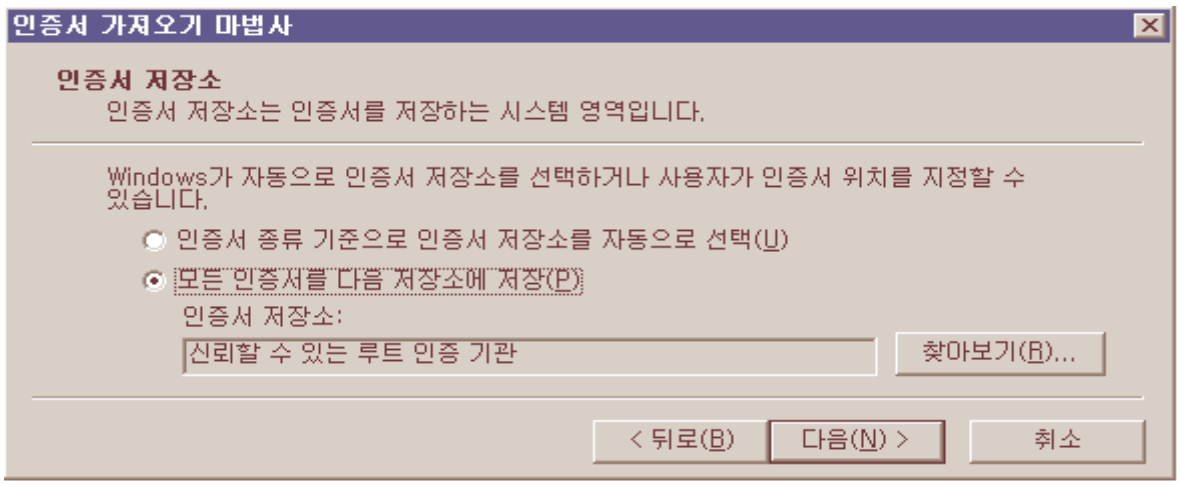
8.'인증서 가져오기 마법사'가 시작 됩니다.



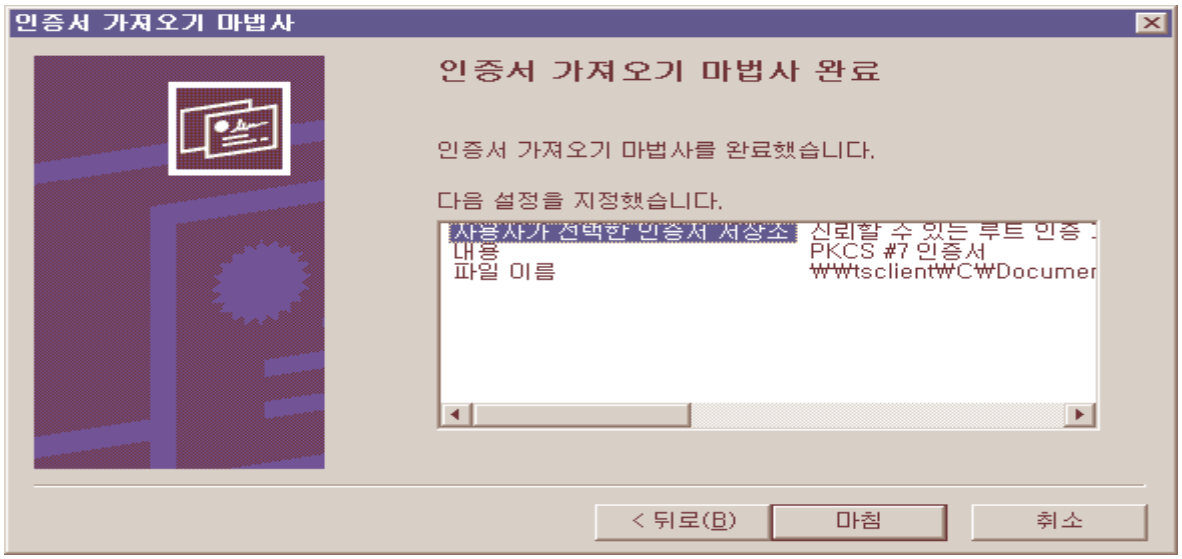
9.'찾아보기'를 클릭하여 인증서가 위치한 경로를 지정합니다.



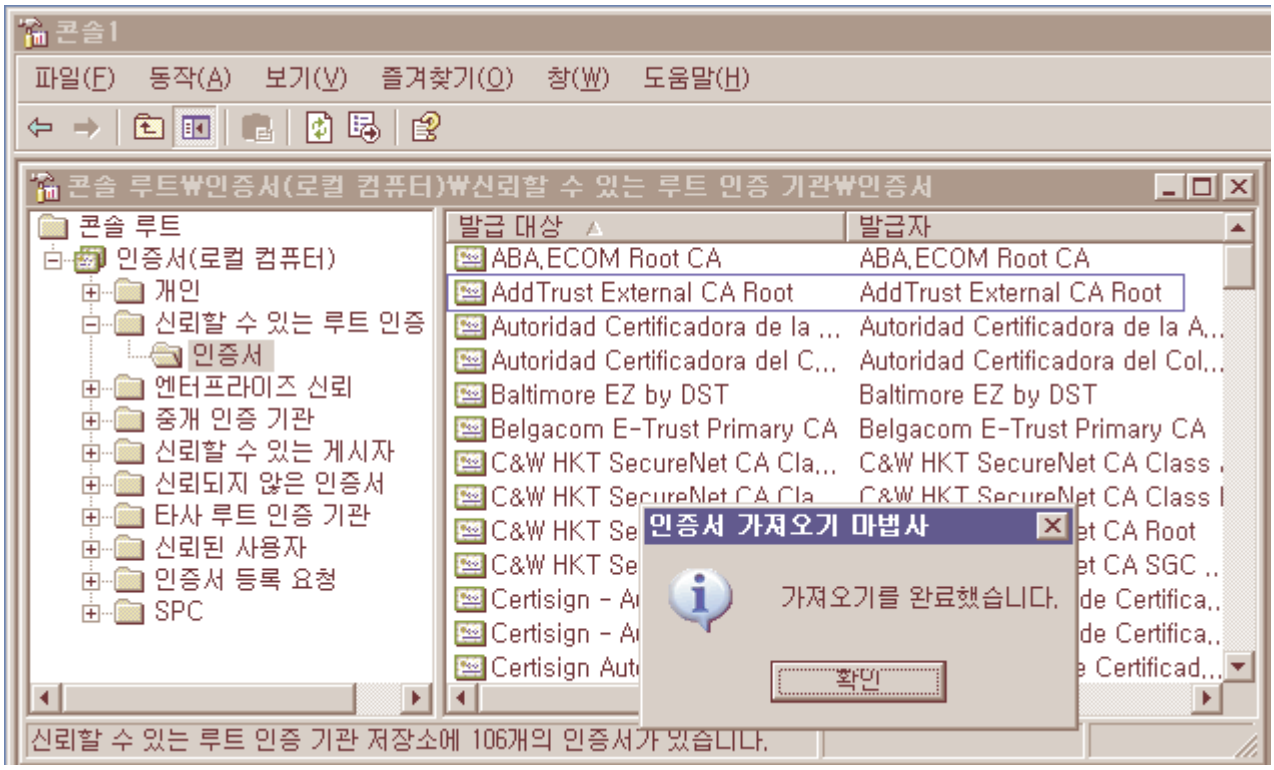
10.'모든 인증서를 다음 저장소에 저장'을 체크 하고 '다음'을 클릭합니다.



11.'인증서 가져오기 마법사'를 완료 하였습니다.



12. '완료' 메세지 입니다.

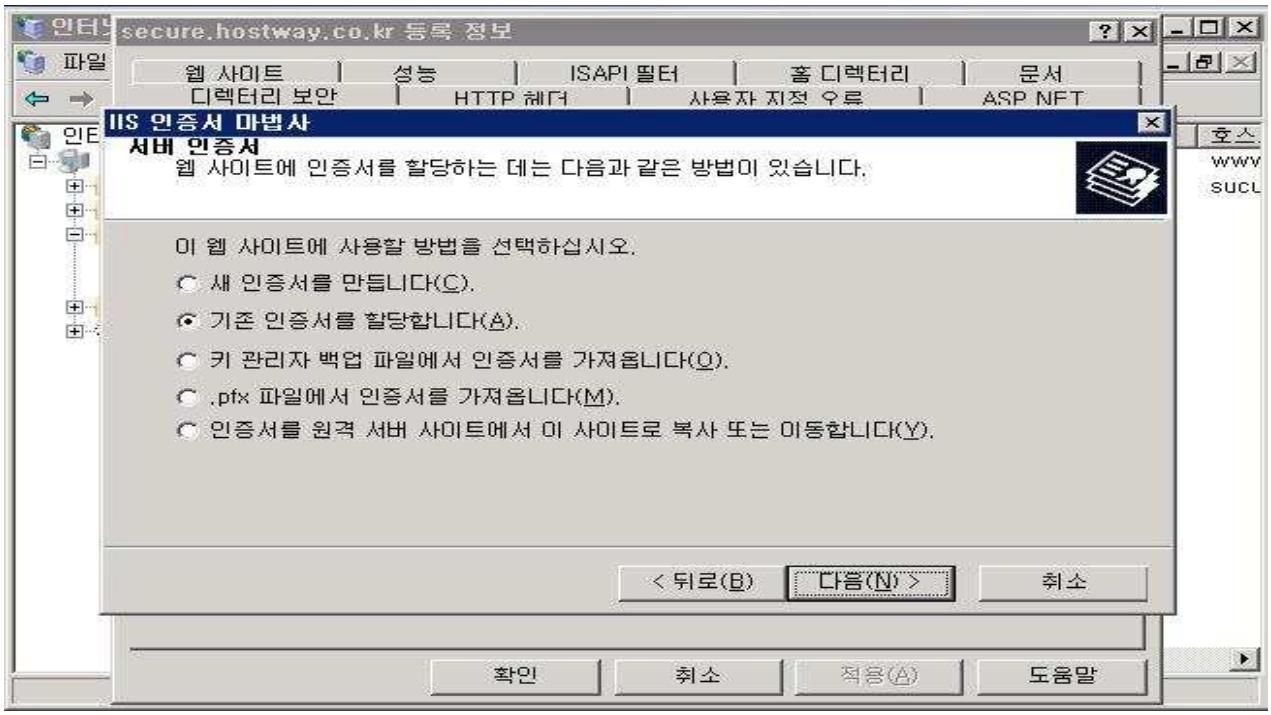


루트 인증서가 완료되면 'AddTrust External CA Root'가 등록이 되었습니다.

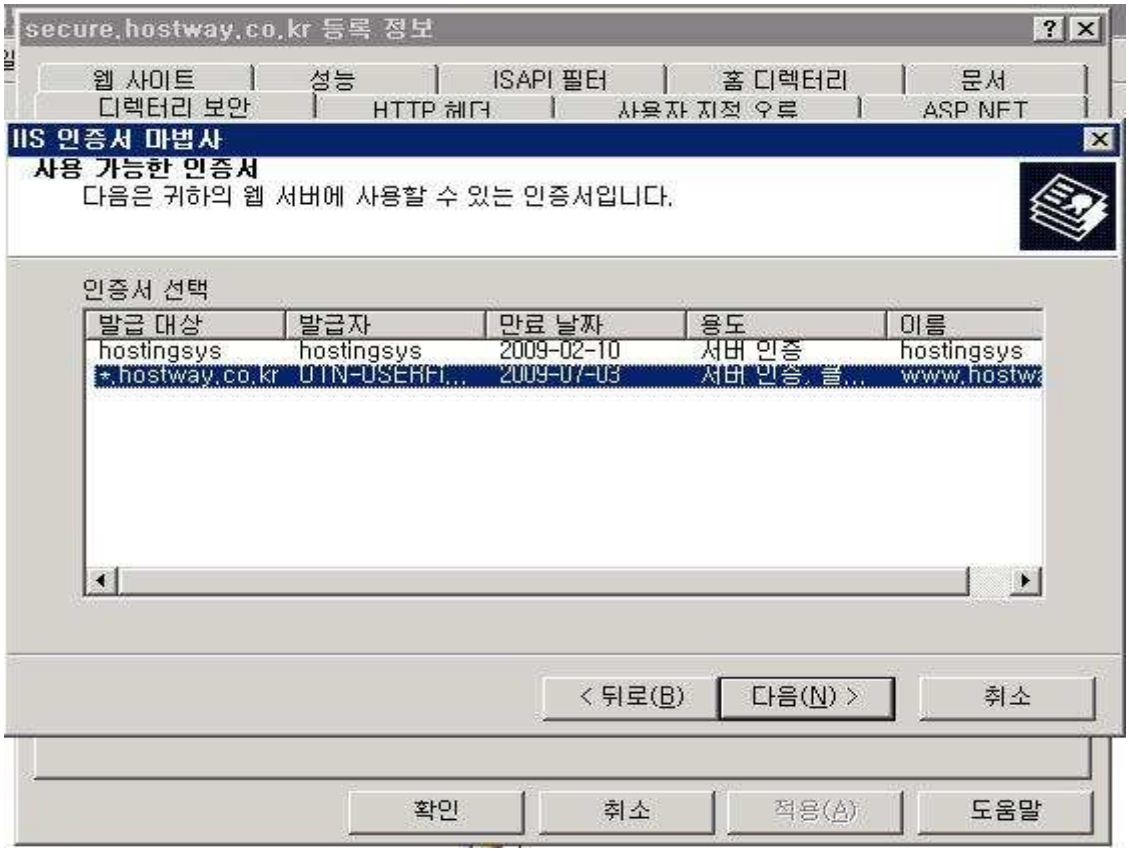
13. 모든 사항이 적용된 후 IIS service를 다시 시작합니다.

4. 멀티 인증서 추가 설치 (Windows 2000, iis 5.0지원 안함.)

1.'디렉토리보안' 기존인승서 할당 선택을 합니다.

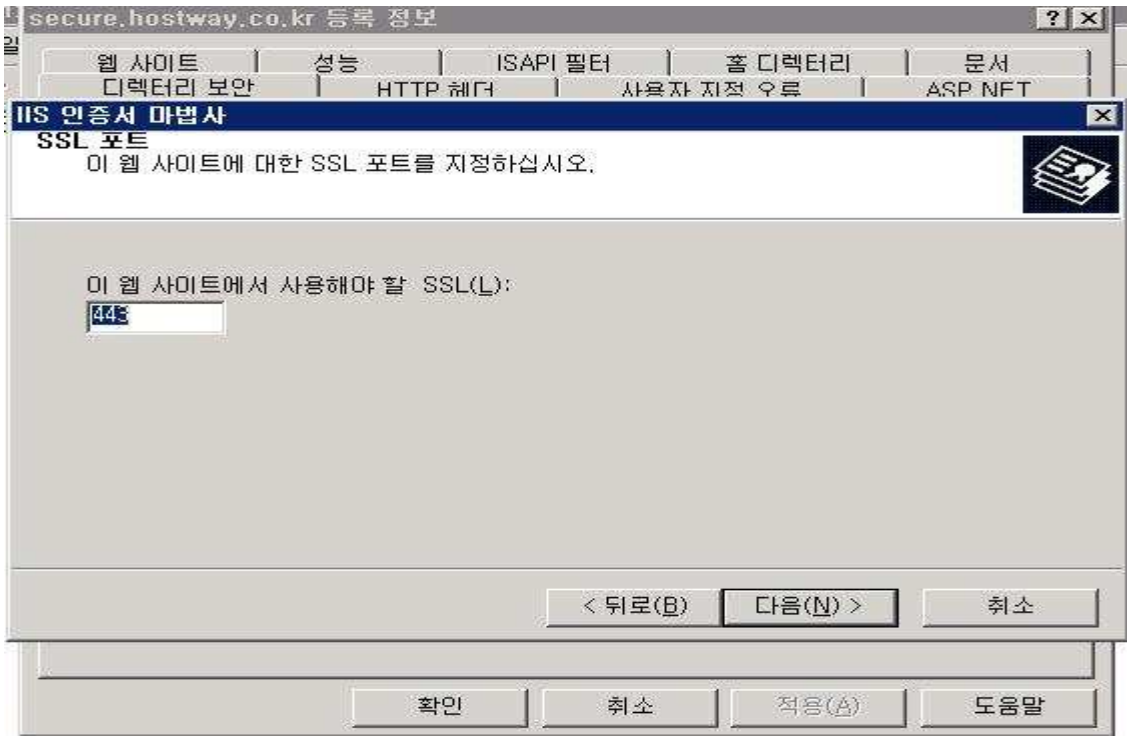


2.'적용하고자 하는 인증리스트 확인' 도메인 선택 후 다음 클릭합니다.

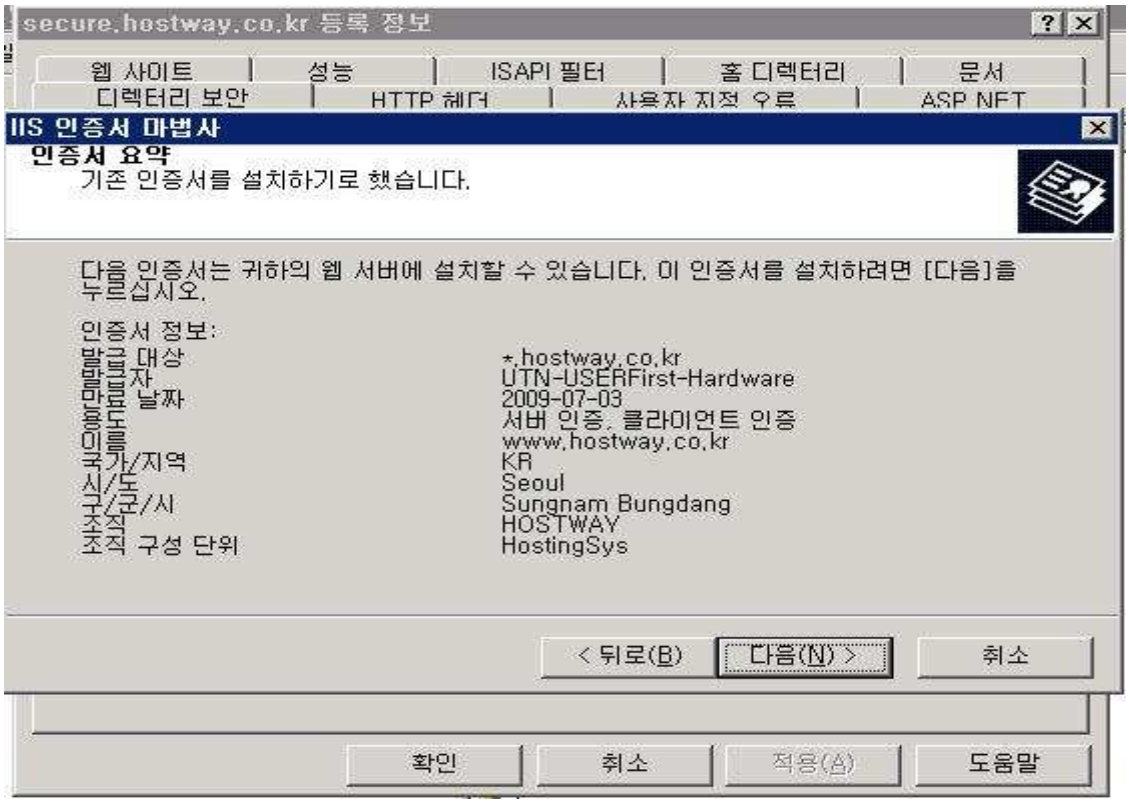


3. 임시 443 포트를 적용 합니다.

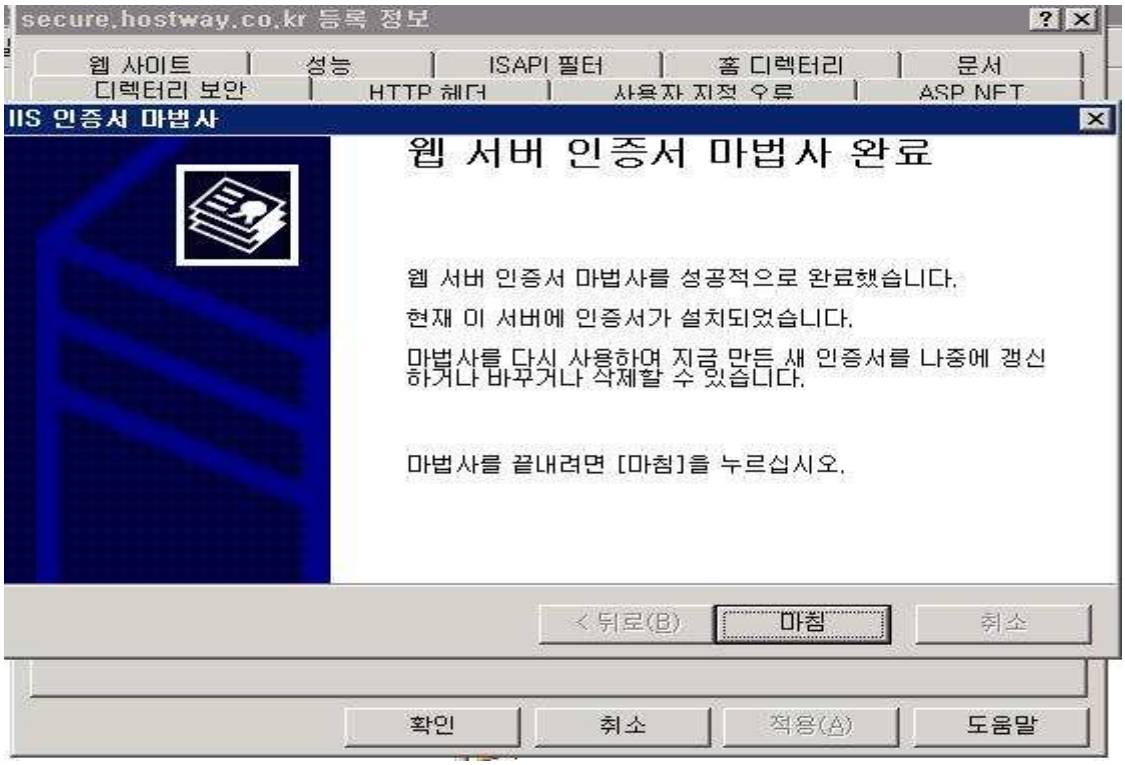
SecureBindings 적용은 반드시 443 포토를 추후 웹사이트에서 삭제하시고 적용하셔야 합니다.



4. 인증서에 대한 상세 내력이 아래와 유사하게 나옵니다.

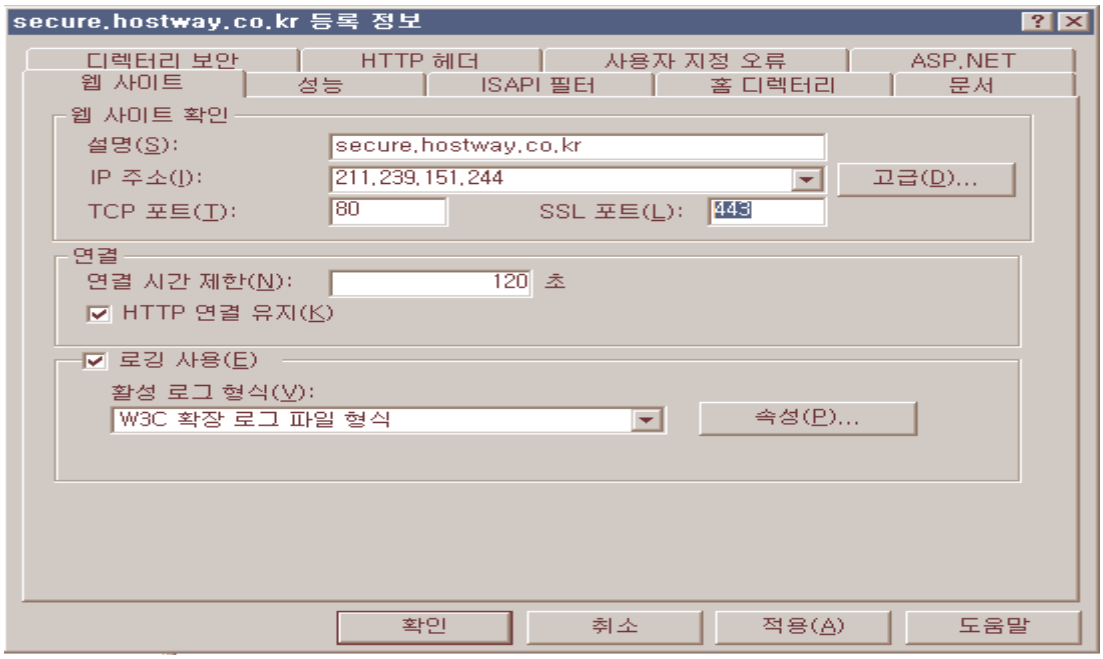


5. 인증서 마법사를 완료했다는 창이 나타납니다.

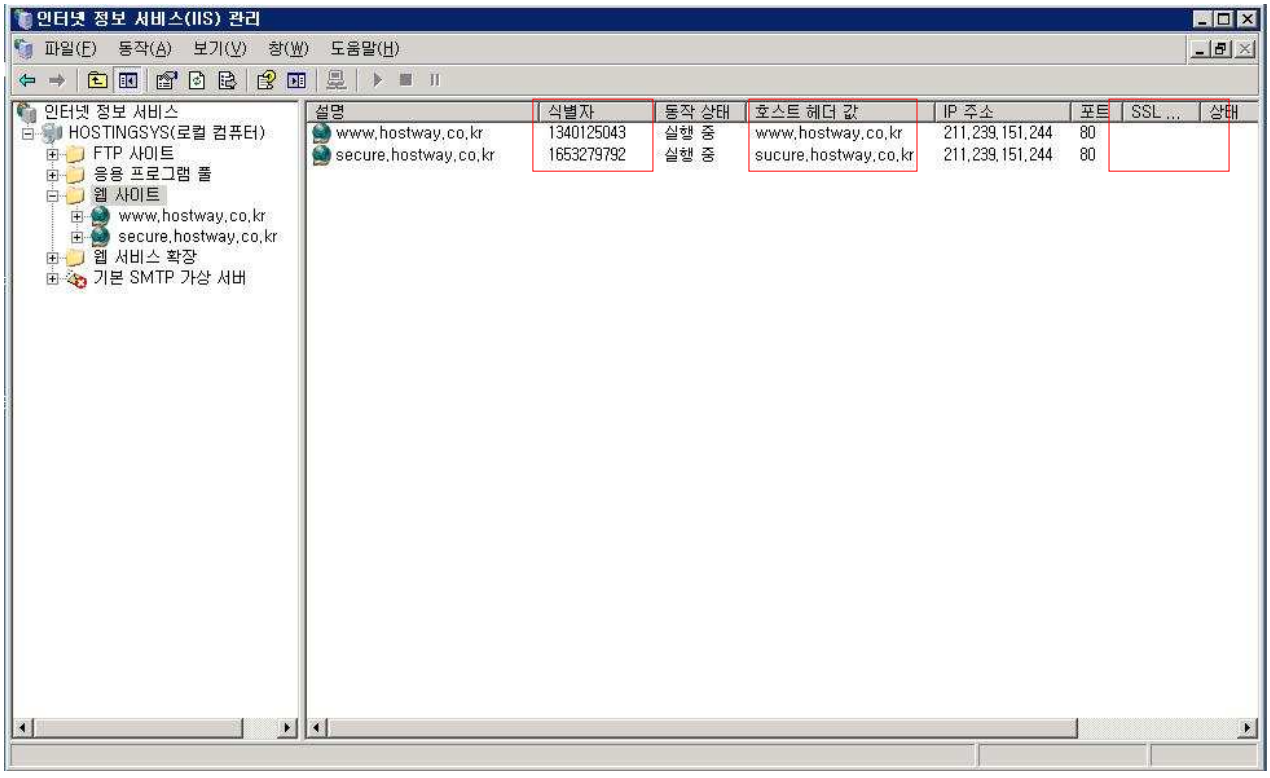


5. SecureBindings 적용(443 포트 공유) (windwos2000 iis 5.0 지원안함)

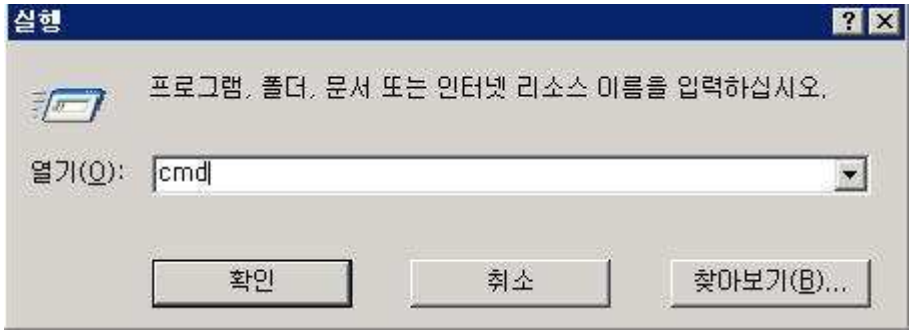
1. SecureBings 적용 전 이미 443포트 적용했던 것을 반드시 삭제하여 줍니다.



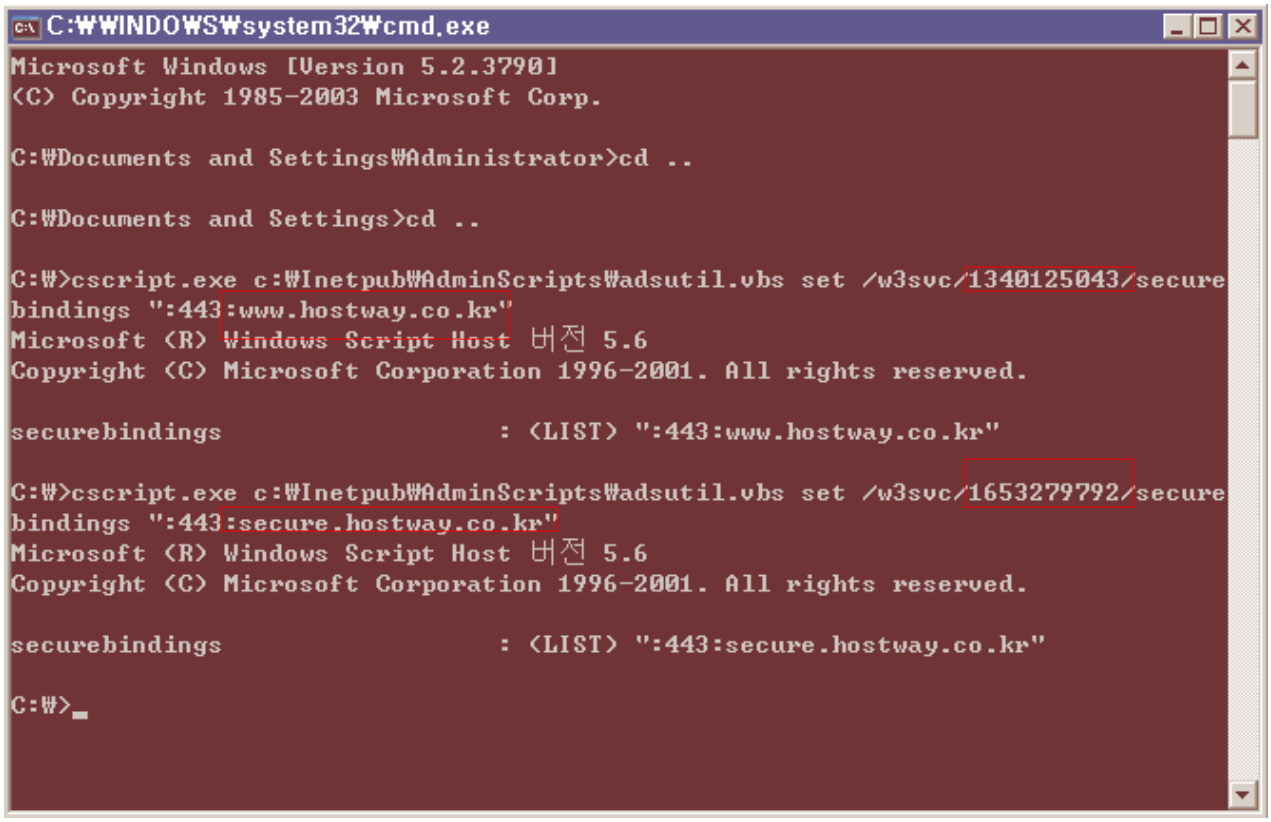
2. 식별자,호스트 헤더값, SSL 포트 삭제 여부를 확인



3. '시작 -> 실행 -> cmd ' cmd 창 띄웁니다.



4.C:₩>cscript.exe c:₩Inetpub₩AdminScripts₩adsutil.vbs set /w3svc/<식별자>/ securebindings":443:<호스트 헤더 값>"



5. Securebindings 적용 이후에 IIS를 재시작 하여 줍니다.

6. ‘Securebindings’ 적용 후 아래에서 처럼 443 포트가 공유된 것을 확인하면 정상적으로 적용이 된것입니다.