Comodo Korea
국제표준인증 제휴기관

- IIS 7.0(Microsoft Internet Information Server 6.0)신규

고객님께서는 이전에 CSR 생성 과정을 진행해 주셨습니다.
그래서 IIS 인터넷 서비스 관리자에서 "새 인증서를 만듭니다"를 통해서 서버 암호화 키(개인키)를 생성하였고, 생성된 암호화 키(개인키)를 토대로 CSR(Certificate Signing Request)을 저희 코모도코리아로 보내 주셨습니다. 그리고
코모도코리아에서는 서버 암호화 키(개인키)와 키쌍(key pair)을 이루는 고객님의 정식 웹 서버인증서를 발급하게 됩니다.
이제 고객님의 IIS 7.0 서버인증서 관리자에서 서버 암호화 키(개인키)와 정식 웹 서버 인증서를 조합하는("인증서 요청 완료") 작업을 하시면, IIS 7.0 서버에 SSL 설치는 마치게 됩니다.

※ IIS 7.0 웹 서버의 인증서 설치 순서

1. 발급된 인증서 확인
2. IIS 7.0 웹 서버에 인증서 설치하기
3. IIS 7.0 웹 서버에 인증서 설치 확인하기
4. 웹사이트에 인증서 설정하기
5. SSL 구동 확인하기
6. 키 쌍(key pair, 인증서 및 개인키) 백업 하기

---

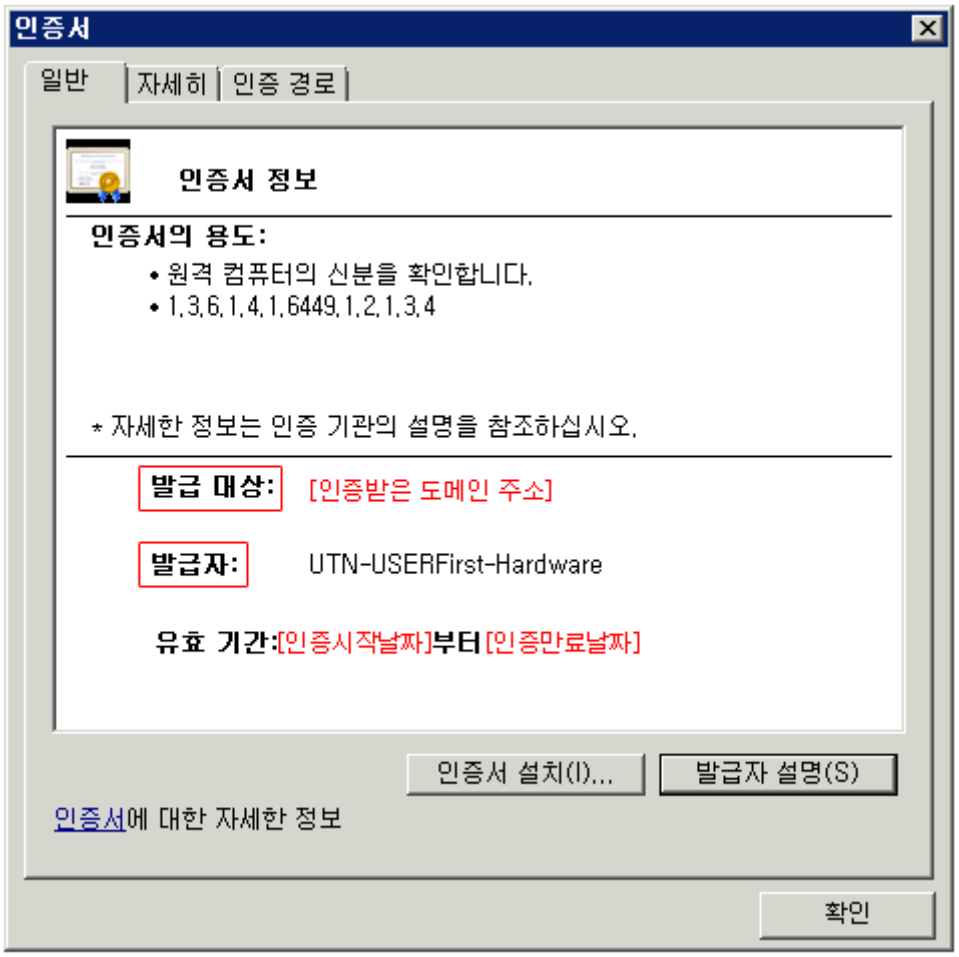
1. 발급된 인증서 확인

먼저 발급된 웹 서버 인증서를 확인합니다. 웹 서버 인증서는 인증받은 도메인이름으로 발급됩니다.

웹 서버 인증서: [인증 받은 도메인 이름으로 된].cer

위의 발급된 인증서는 코모도코리아에서 고객님께 전자 메일로 발급해 드립니다. 그러므로 전자 메일에 발급된 인증서 항목을 알려드리며, 발급된 인증서는 첨부파일로 첨부되어있습니다.

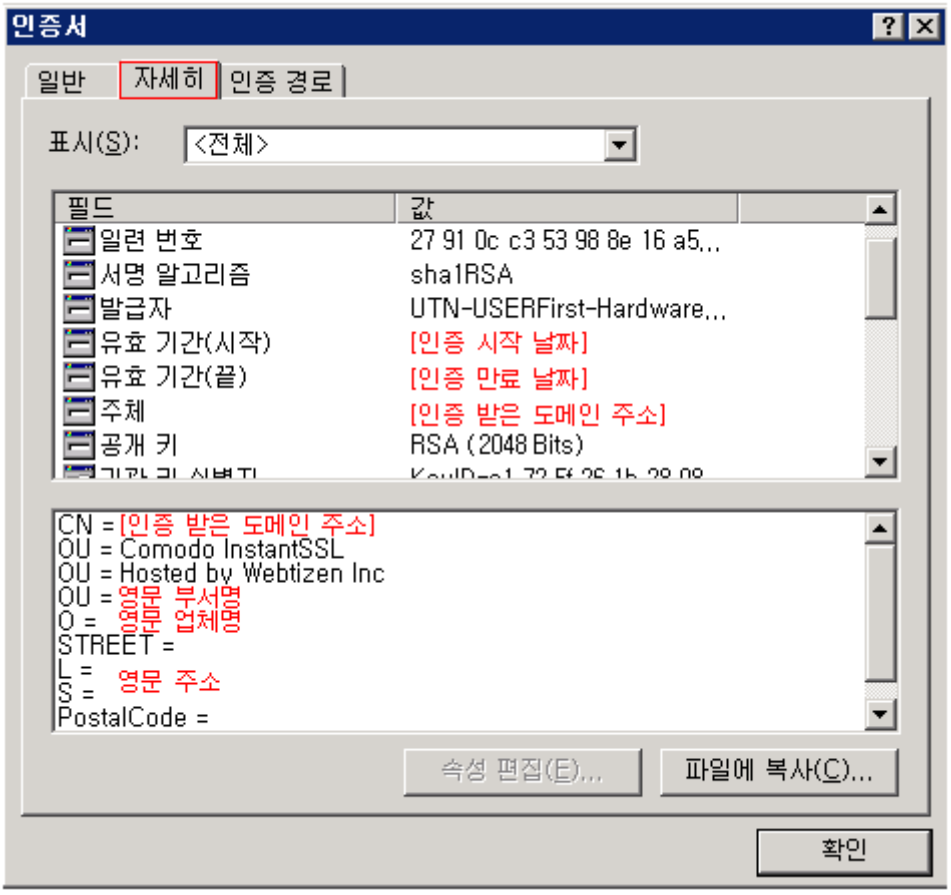
윈도우 PC 에서 발급 받으신 웹 서버 인증서([인증 받은 도메인 이름으로 된].cer 파일)를 열어서(double click) 내용을 확인합니다.(메모장이나 울트라 에디터에서 열지 않습니다.)
웹 서버 인증서를 열게 되면 다음과 같은 내용을 확인하실 수 있습니다.



[인증서 보기 – 일반]

발급 대상에서 고객님이 인증 받은 도메인 주소로 신청하신 도메인 주소가 맞는지 확인합니다.

다음으로는 [자세히] 탭 부분에서



[인증서 보기 - 자세히]

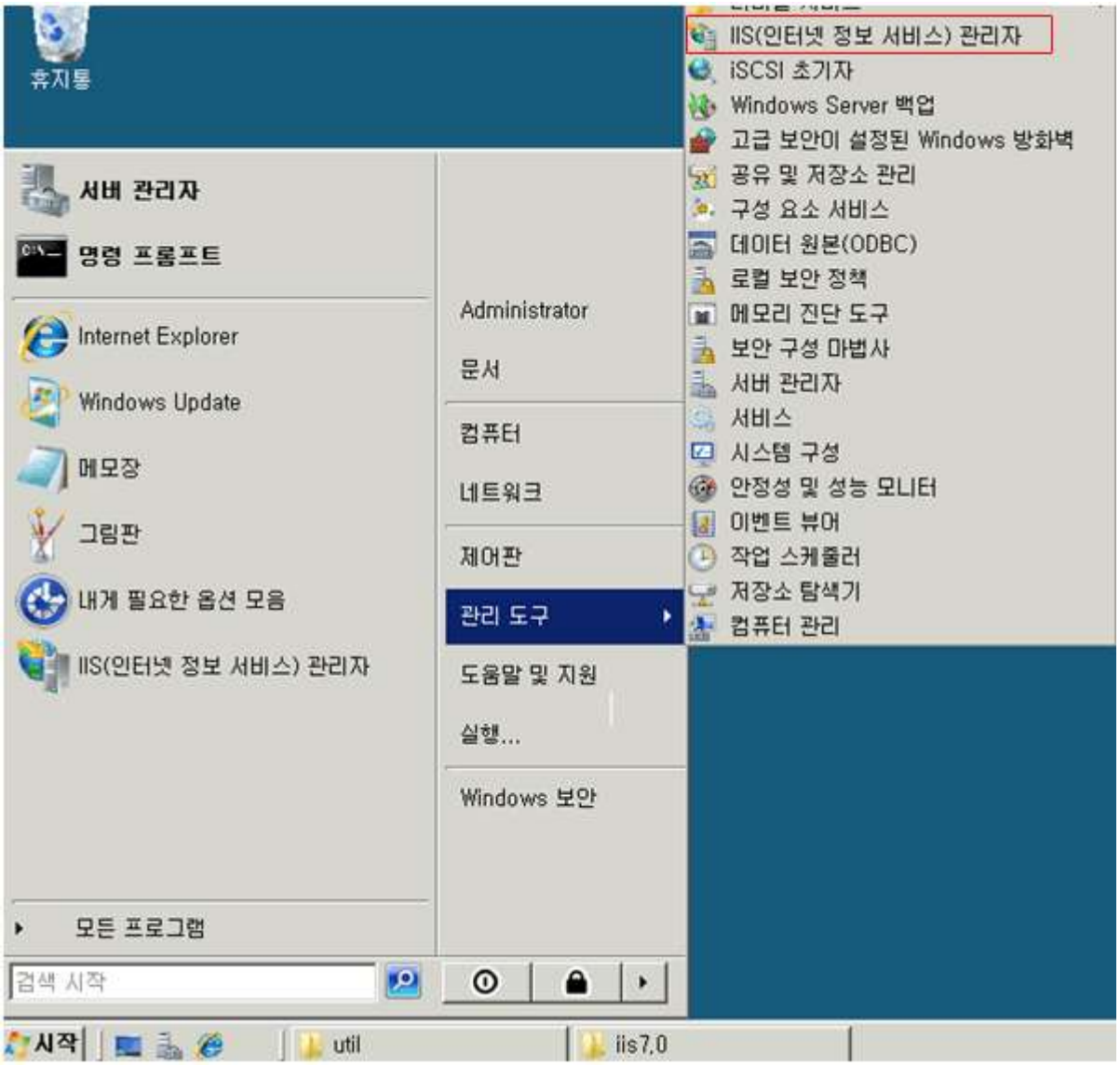
발급한 웹 서버 인증서의 유효기간을 확인합니다. (유효 기간(시작)과 유효 기간(끝) 정보를 확인합니다.)
그리고 공개 키 부분에서 RSA (2048 Bits) 를 확인합니다. 코모도코리아에서 발행되는 인증서는 2048 Bits 키를 권고합니다. 꼭 확인해 주시기 바랍니다.

2. IIS 7.0 웹 서버에 인증서 설치하기

IIS 서버에서는 인증서 관리를 IIS(인터넷 정보 서비스) 관리자에서 관리하게 됩니다. 기존에 CSR 생성 과정으로 생성된 서버 암호화 키(개인키)에 정식 웹 서버 인증서를 조합하는("인증서 요청 완료") 작업을 진행합니다.
다음의 순서를 밟아 주시기 바랍니다.

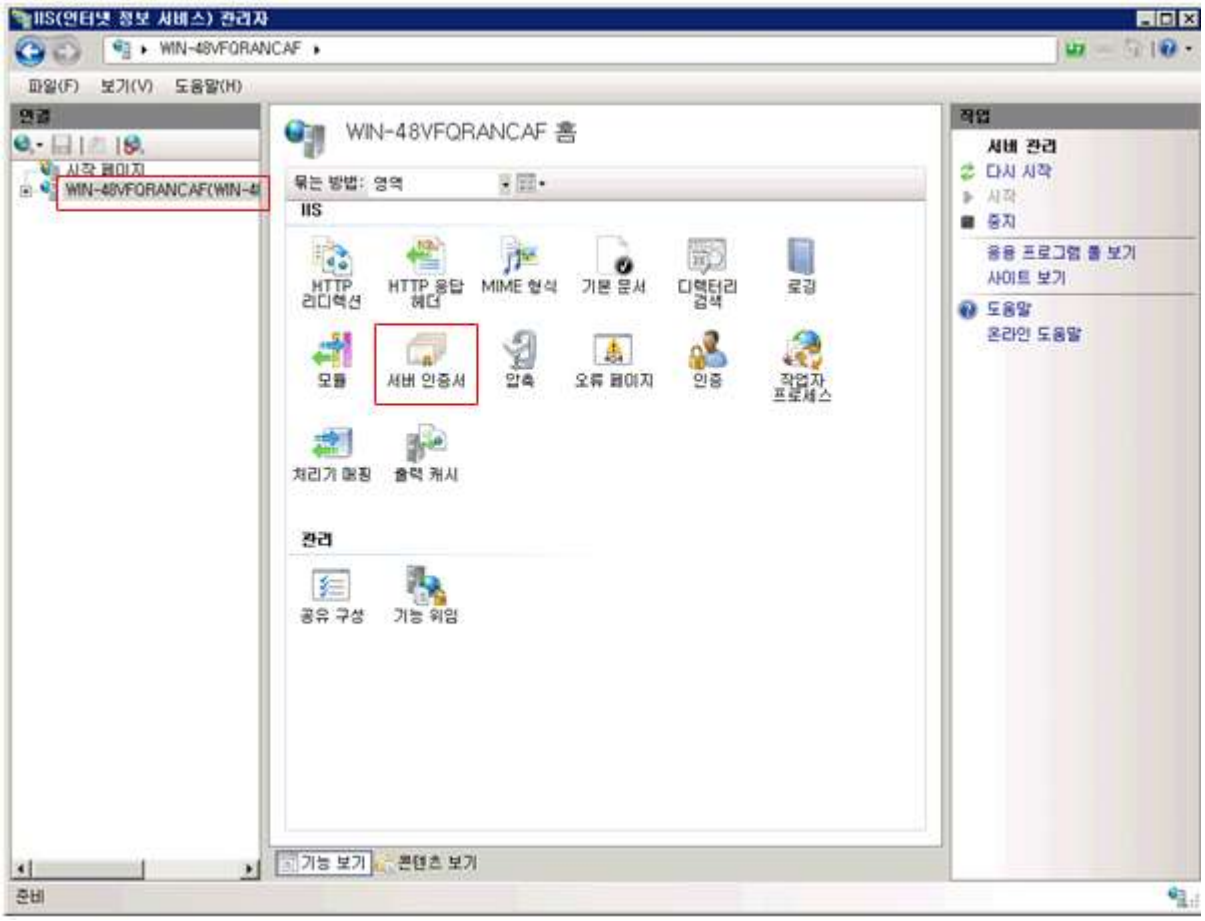
① IIS(인터넷 정보 서비스) 관리자 열기

[시작] -> [관리도구] -> [IIS(인터넷 정보 서비스) 관리자]를 선택합니다.



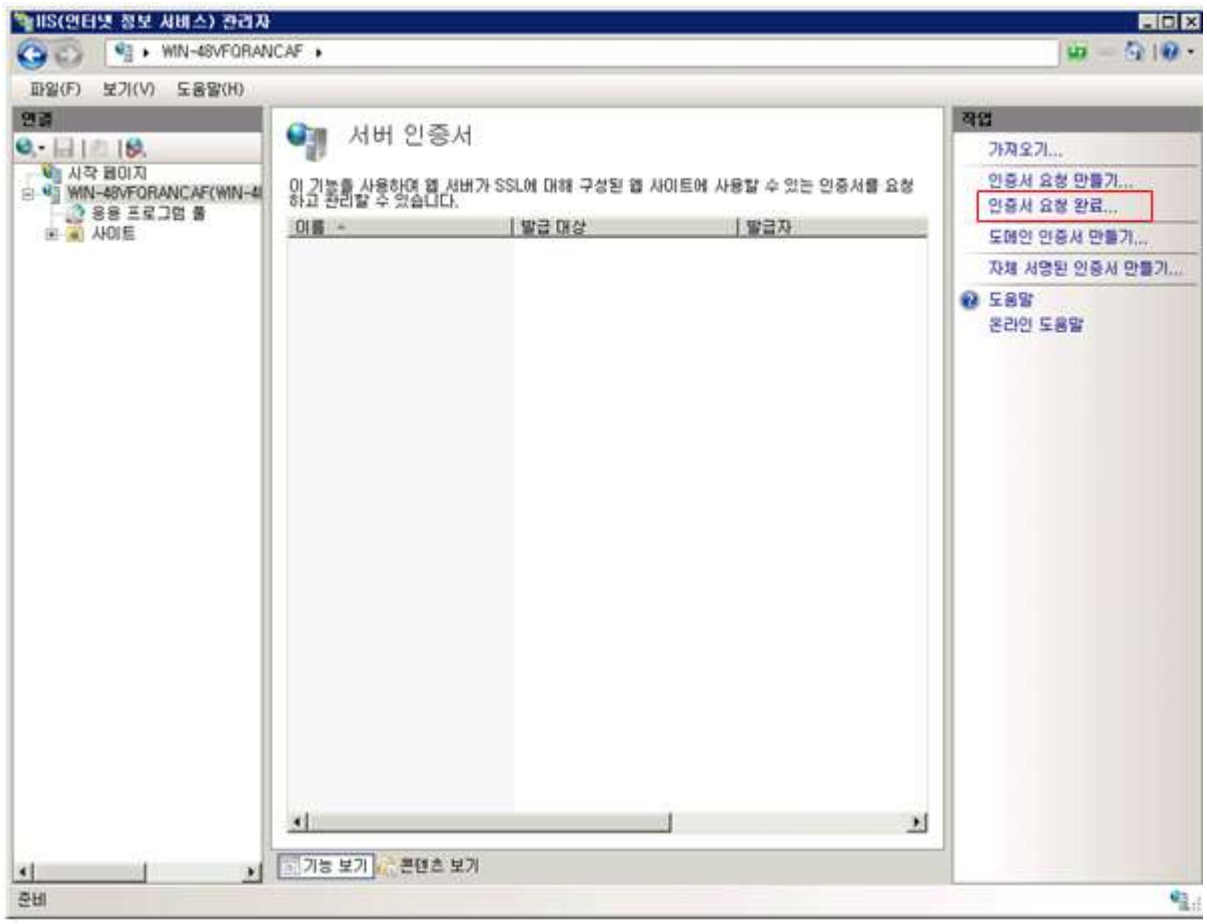
② 인증서 설치할 서버에서 서버 인증서 선택하기

[인증서를 설치할 서버] 에서 [서버인증서]를 엽니다.



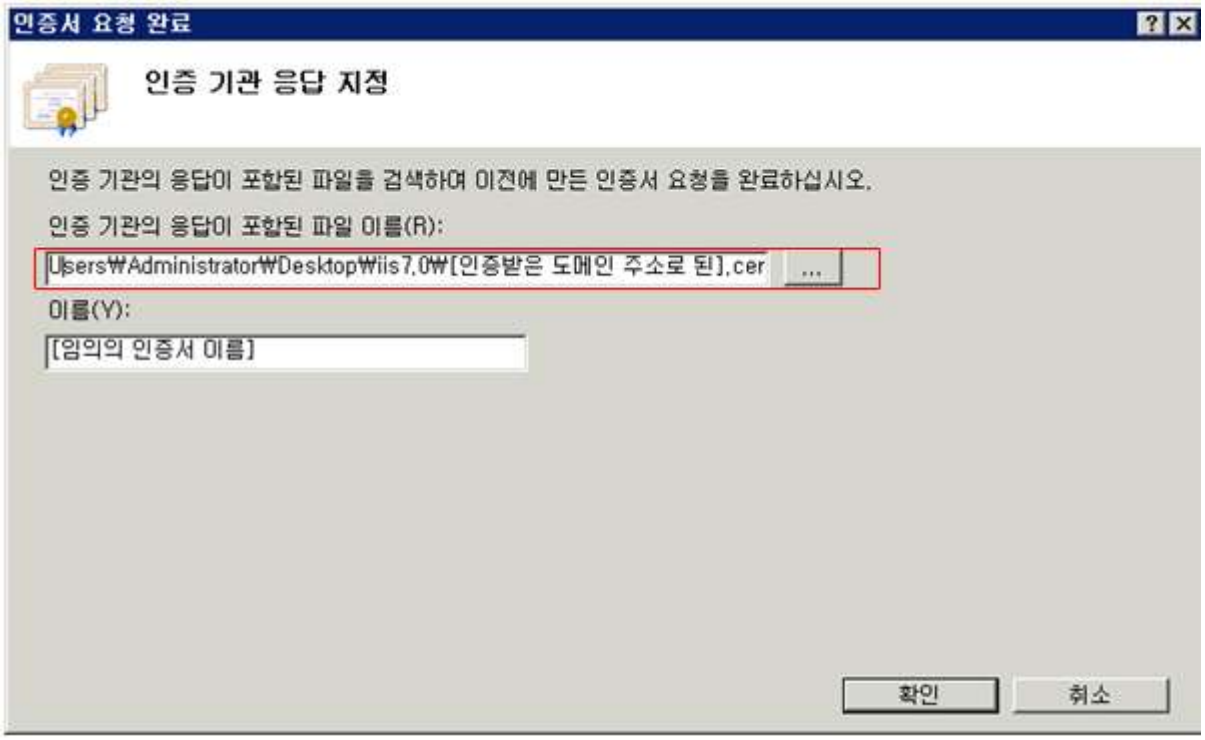
③ 서버 인증서에서 [인증서 요청 완료] 열기

서버 인증서의 오른쪽 메뉴에서 [인증서 요청 완료] 을 선택합니다.



④ 발급 받은 인증서 선택하기

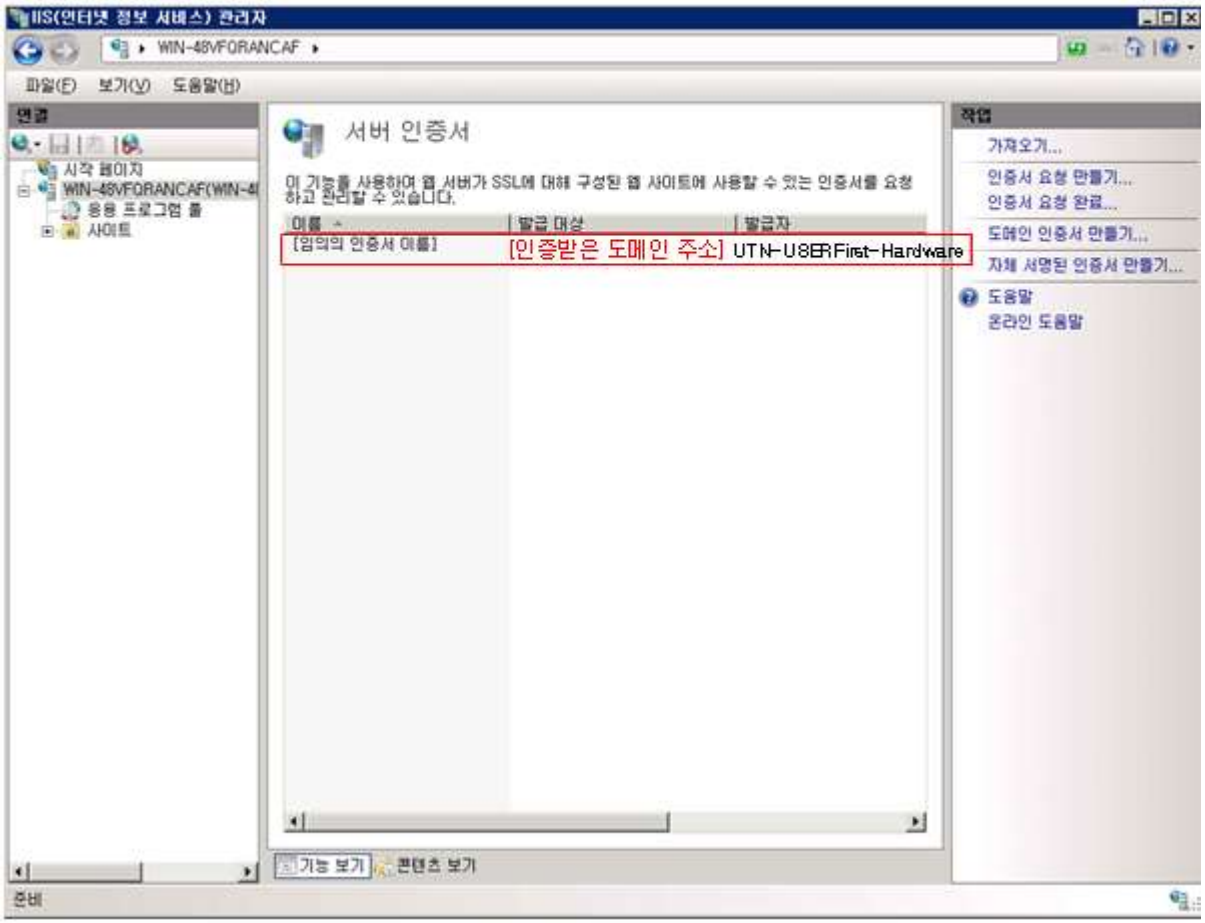
코모도코리아에서 발급받은 웹 서버 인증서([인증받은 도메인 주소로 된].cer 파일) 을 선택합니다.
이름 에는 원하시는 임의의 이름을 적어줍니다. 서버에서 사용되는 이름이므로 두 개 이상의 인증서를 사용할 경우 구별할 수 있도록 설정합니다.



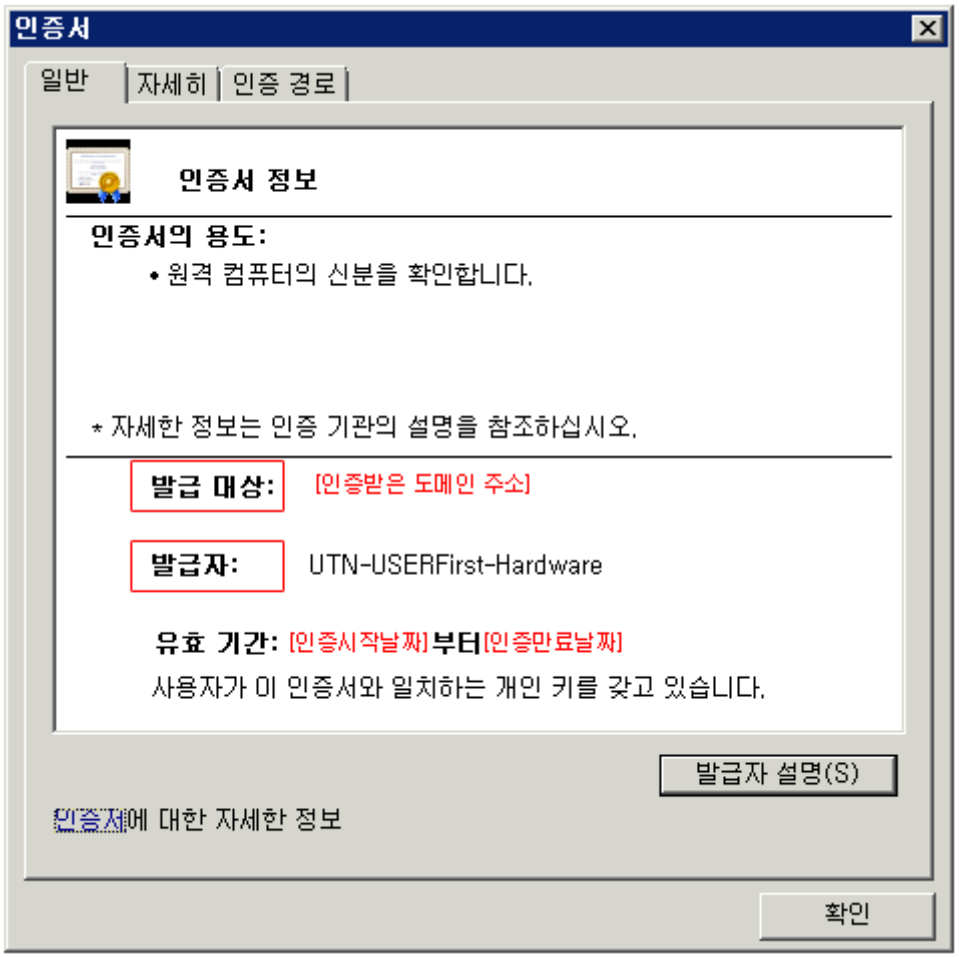
3. IIS 7.0 웹 서버에 인증서 설치 확인하기

서버 인증서 리스트에서 등록 된 인증서를 확인 할 수 있습니다. 해당 인증서를 더블 클릭합니다.

Comodo Korea
국제표준인증 제휴기관



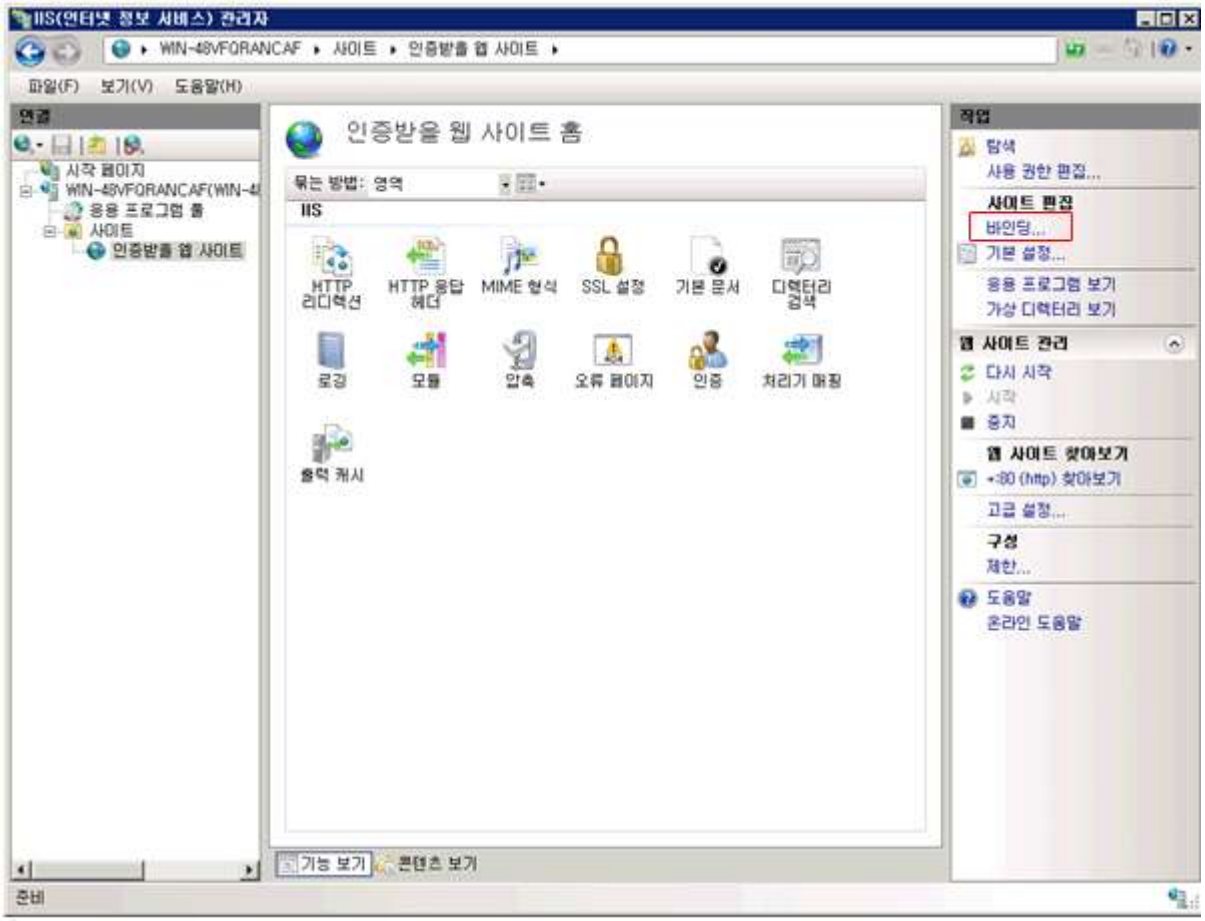
다음과 같이 웹 서버에 설치된 인증서 정보를 확인해야 합니다.
[발급 대상]에서 [인증 받은 도메인 주소]를 확인해 주시고, 설치된 인증서의 유효기간 확인해 주십니다.
마지막으로 제일 중요한 부분인 [사용자가 이 인증서와 일치하는 개인 키를 갖고 있습니다.] 항목을 확인해 주셔야 합니다.
[사용자가 이 인증서와 일치하는 개인 키를 갖고 있습니다.] 항목이 확인 되지 않는다면, 웹 서버에 설치된 인증서는 서버키(암호키)와 웹 서버인증서(공개키)
간의 조합된 RSA - SSL 암호화 통신이 되지 않습니다.



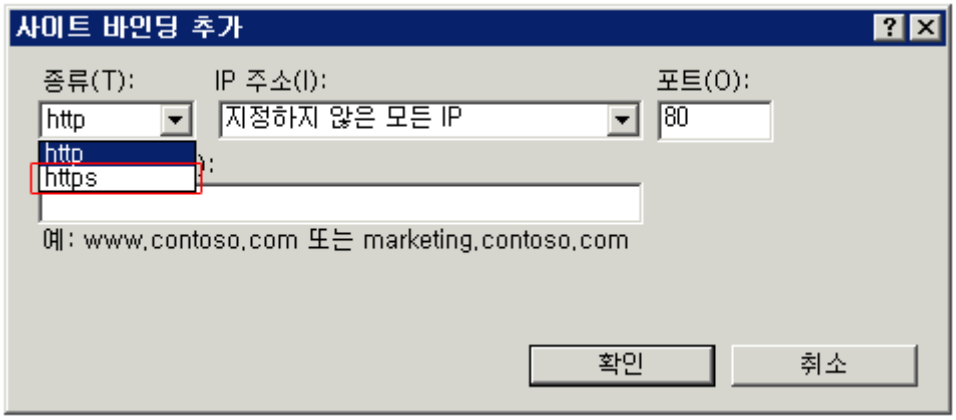
4. 웹사이트에 인증서 설정하기

웹 서버에 인증서 설치를 완료했다면, 해당 웹사이트에 설치한 인증서를 설정해야 합니다.

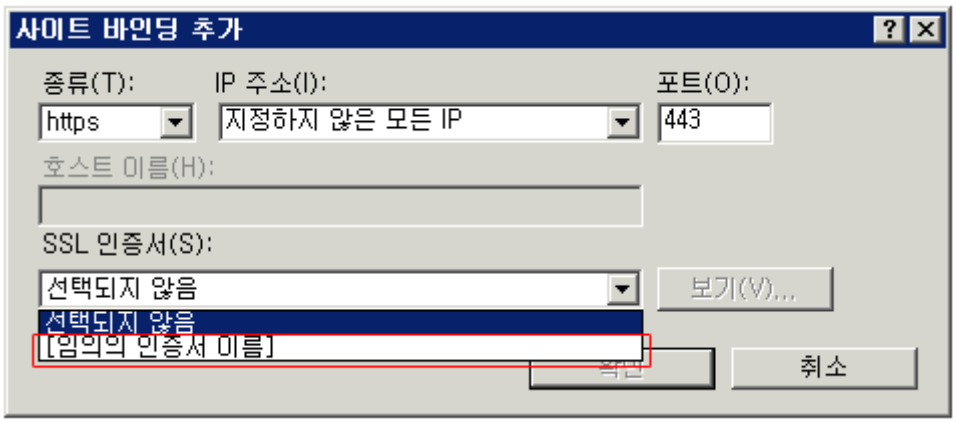
[인증받을 웹 사이트]를 선택한 후, 우측 상단에 있는 [사이트 편집] -> [바인딩...]을 실행합니다.



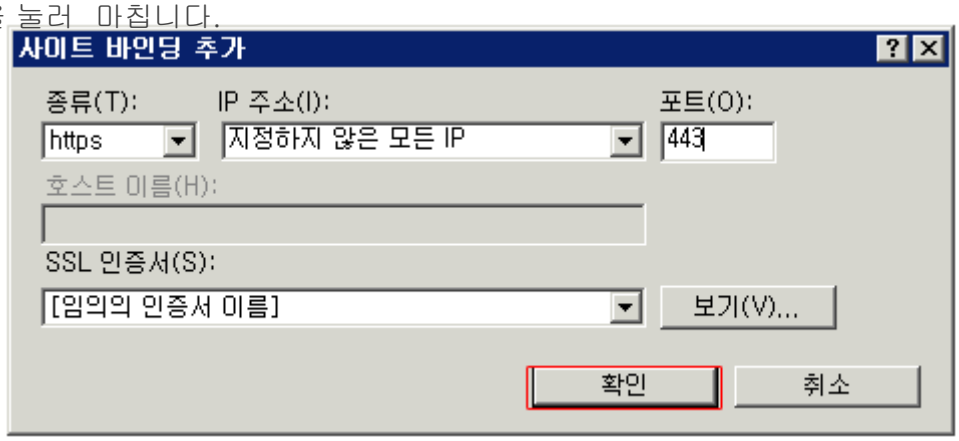
[사이트 바인딩 추가]에서 [종류] -> [https]를 선택합니다.



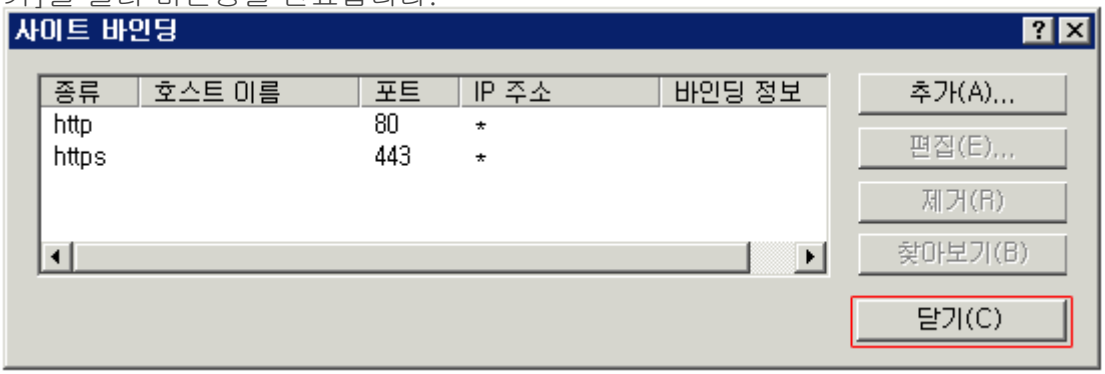
[SSL 인증서] -> [[임의의 인증서 이름]]을 선택합니다.



[확인]을 눌러 마칩니다.



[닫기]를 눌러 바인딩을 완료합니다.

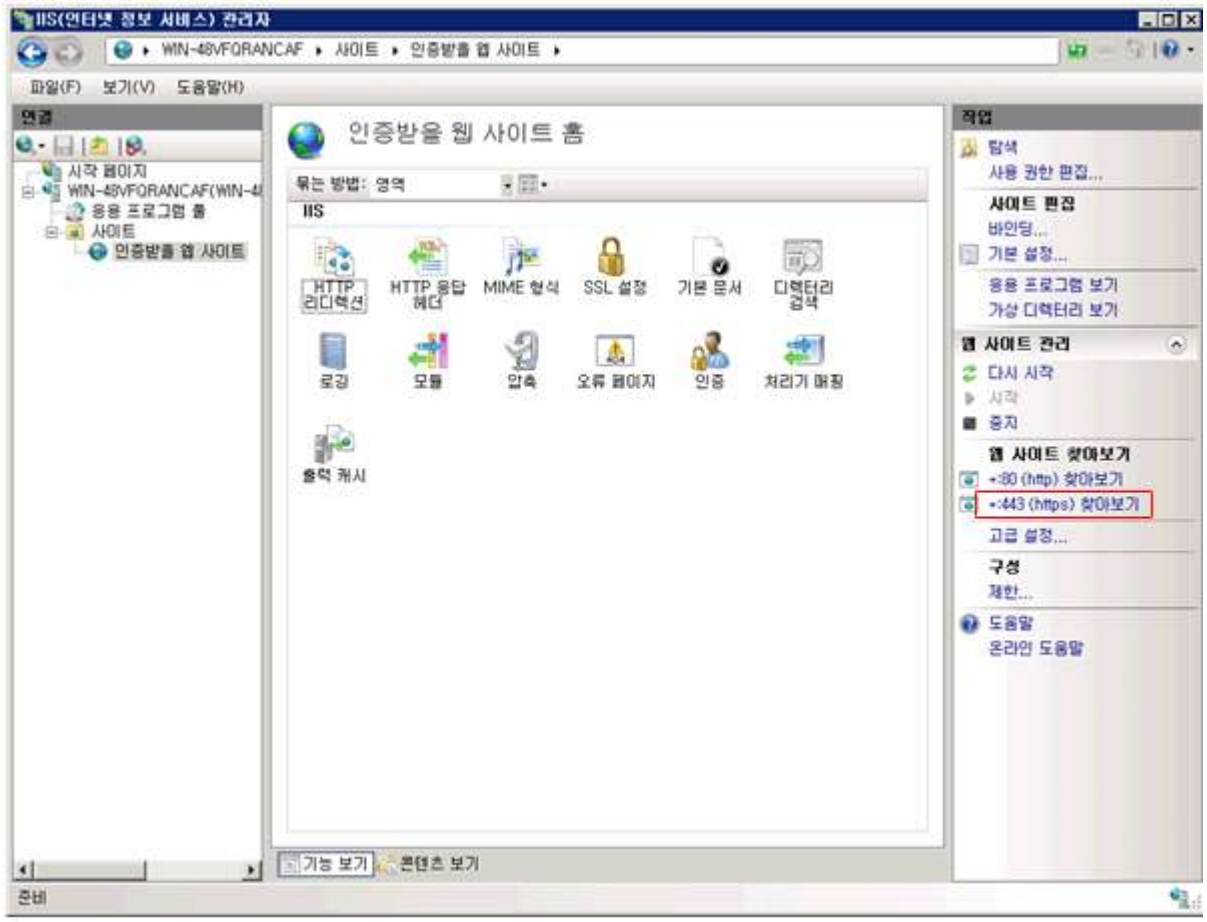


5. SSL 구동확인하기

① 로컬접속 확인

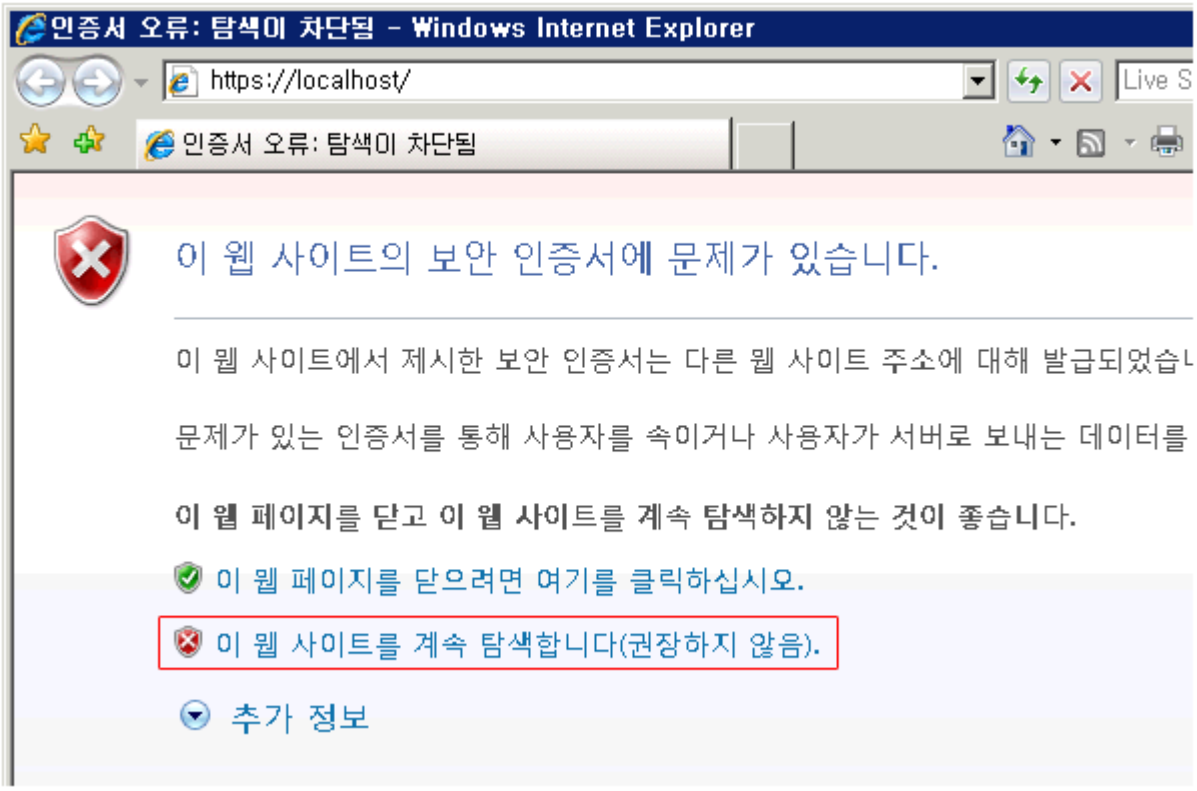
Comodo Korea
국제표준인증 제휴기관

웹 사이트 찾아보기에 추가된 [443(https) 찾아보기]를 클릭합니다.

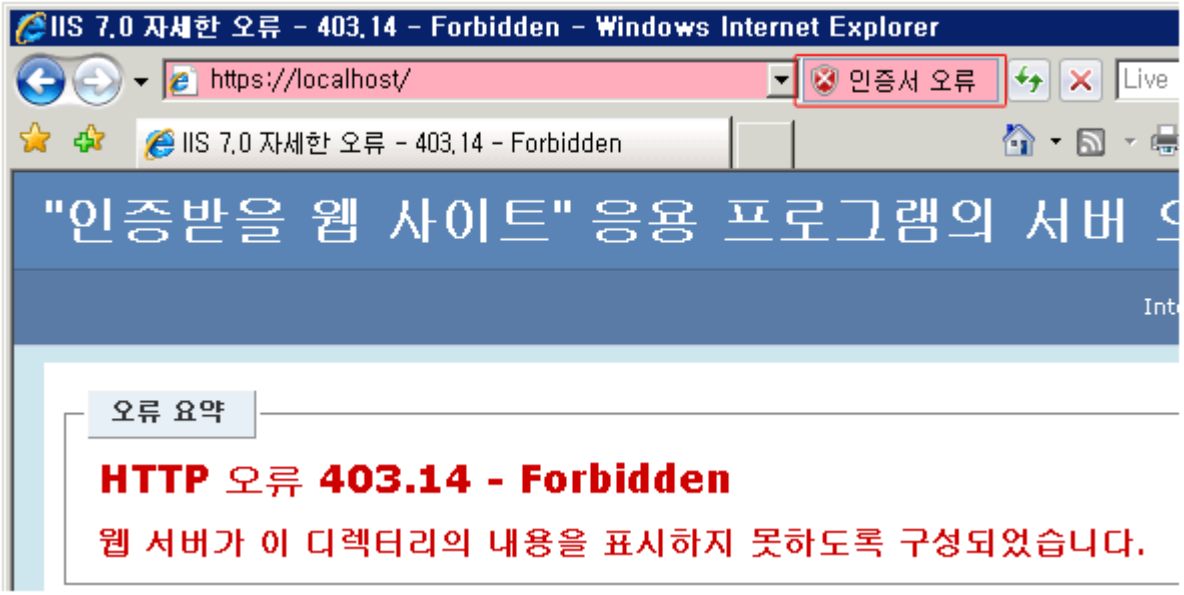


[이 웹사이트를 계속 탐색합니다.]를 클릭합니다.

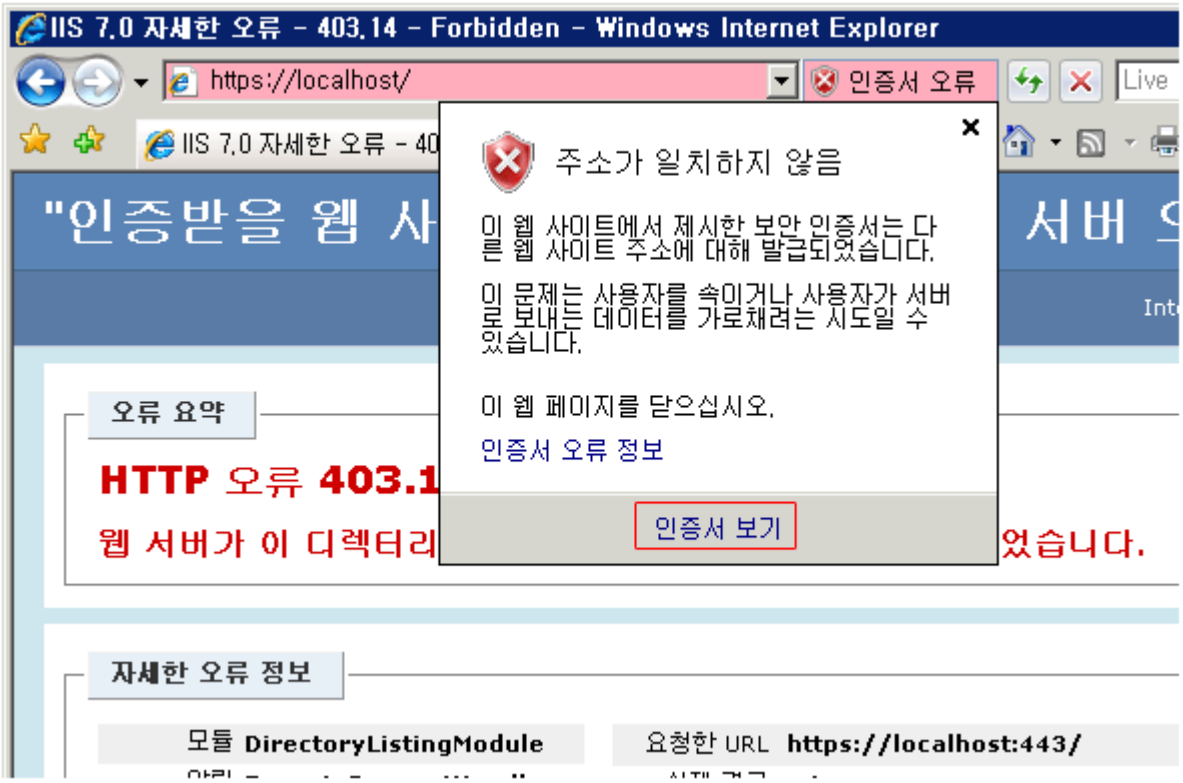
Comodo Korea
국제표준인증 제휴기관



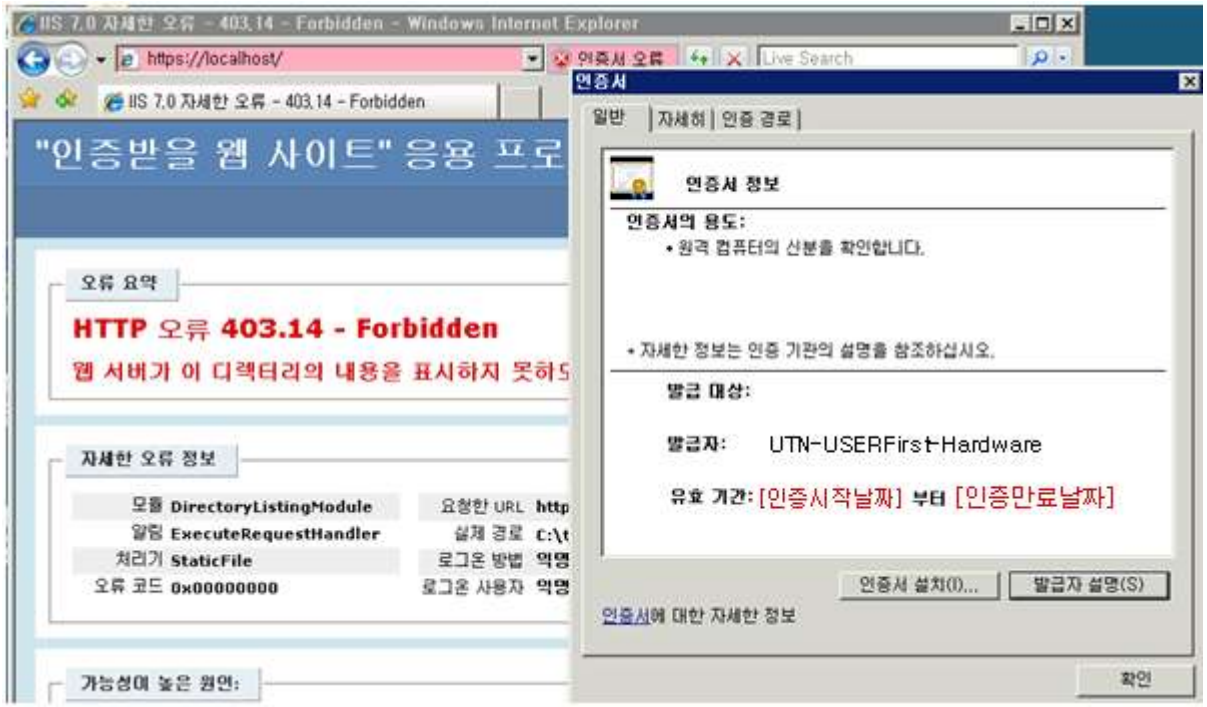
주소표시줄 오른쪽에 있는 [인증서 오류]를 클릭합니다.



[인증서 보기]를 클릭합니다.

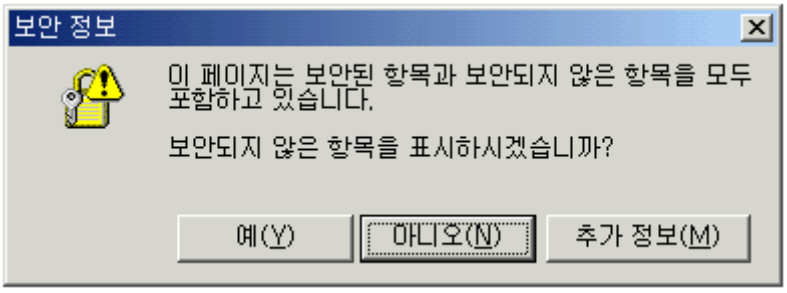


정상적으로 인증서가 설치 되었음을 확인할 수 있습니다.



② 외부 접속 확인

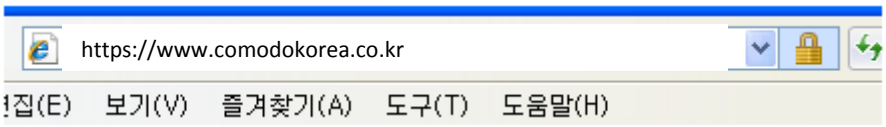
웹 브라우져를 통해서 https://[인증 받은 도메인]/[테스트페이지].html 페이지를 확인해 봅니다.



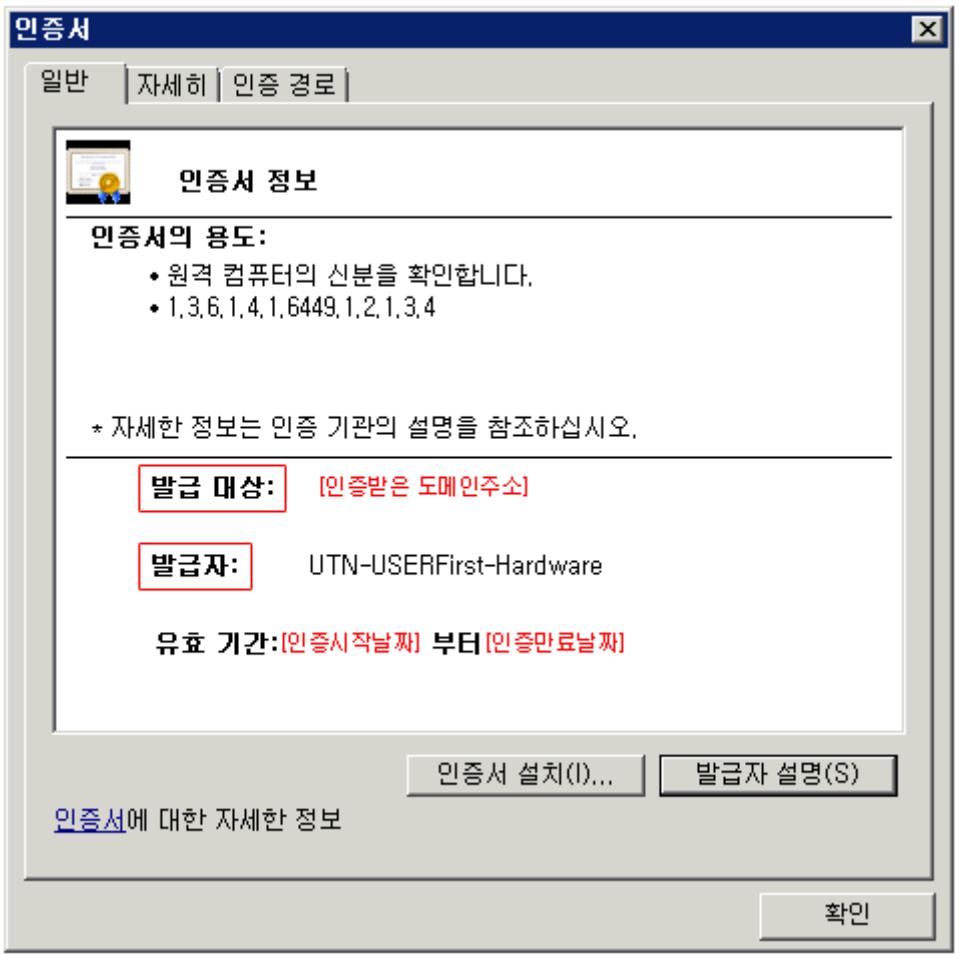
[보안정보 확인창]

접속시에 위와 같은 보안정보 확인 창을 보실 수도 있으나, 이것은 전체 페이지를 암호화 처리했을 경우에 몇몇 이미지나 object 태그의 codebase 부분에 절대경로가 설정된 경우에 보안 정보를 나타내는 정보 창이므로, [아니오]를 선택합니다.

그러면, 웹 브라우져 상단 주소표시줄 오른쪽에 HTTPS 암호화 상태를 나타내는 노란 자물쇠를 확인해 보실 수 있습니다.

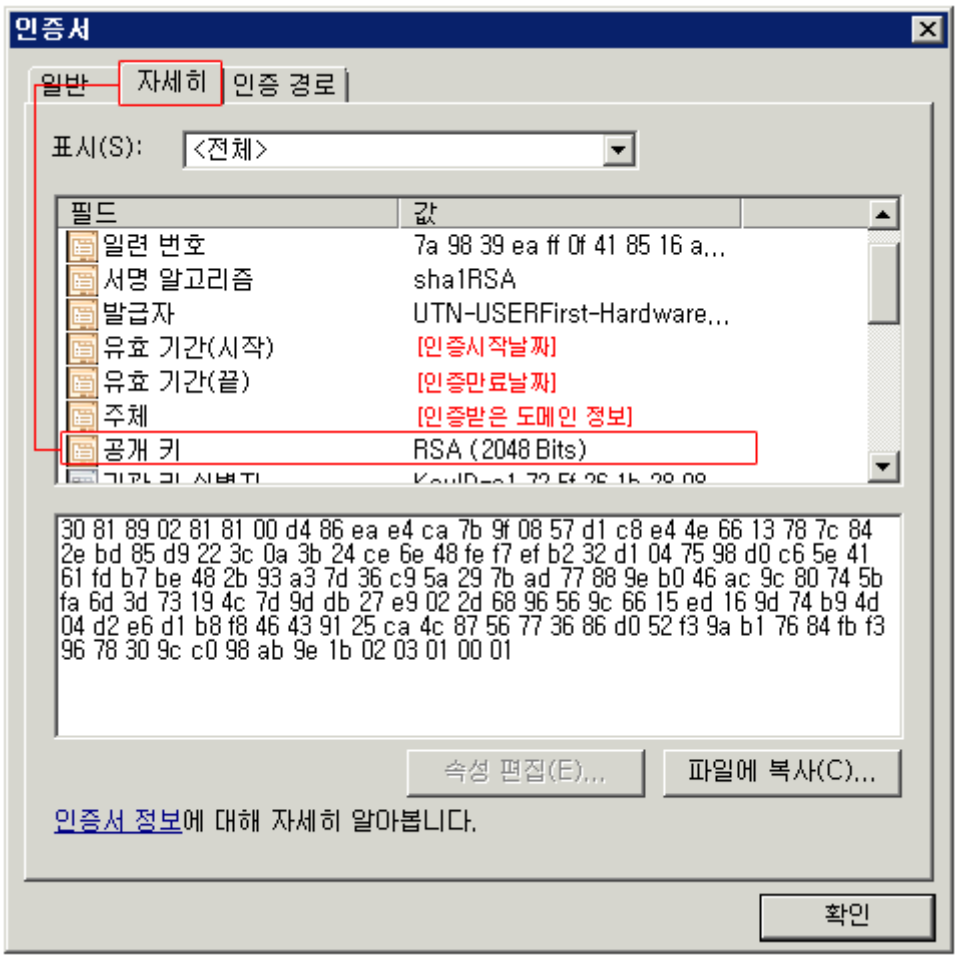


그리고 노란 자물쇠를 클릭 후, [인증서 보기]를 클릭하면, 서버에 설치된 인증서를 확인해 보실 수 있습니다.



[인증서 보기 - 일반]

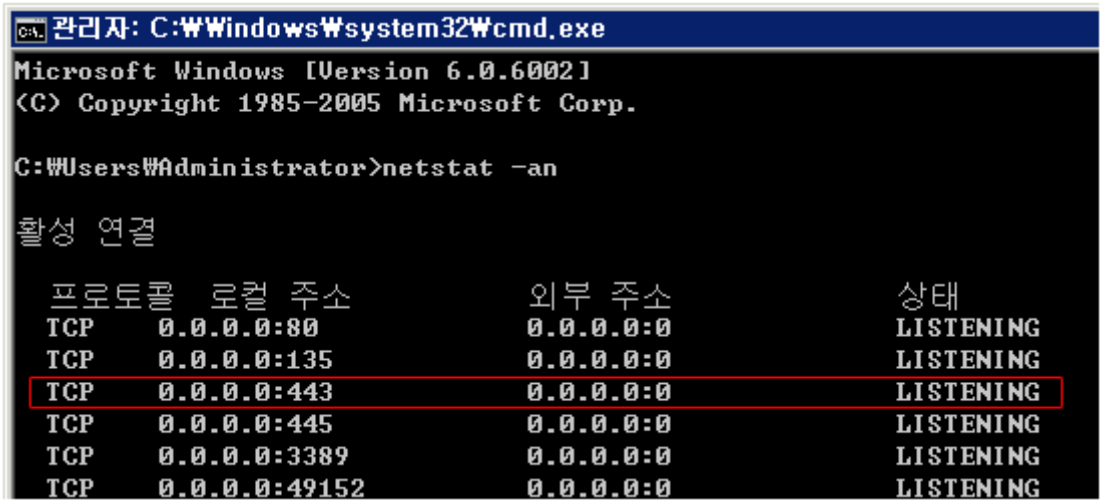
인증서 용도가 [● 원격 컴퓨터의 신분을 확인합니다.] 라는 웹 서버 인증서로
설정된 것을 확인할 수 있습니다.
다음으로 인증서 자세히 보기 부분에서 설치된 웹 서버 인증서의 유효기간을 확인합니다.
(유효 기간(시작)과 유효 기간(끝) 정보를 확인합니다.) 그리고 공개
키 부분에서 RSA (2048 Bits) 를 확인합니다.



[인증서 보기 - 자세히]

* SSL 접속이 되지 않을 경우

① 443 포트(HTTPS 통신) 네트워크 활성 확인



② 방화벽과 L4 Switch 장비 설정 확인

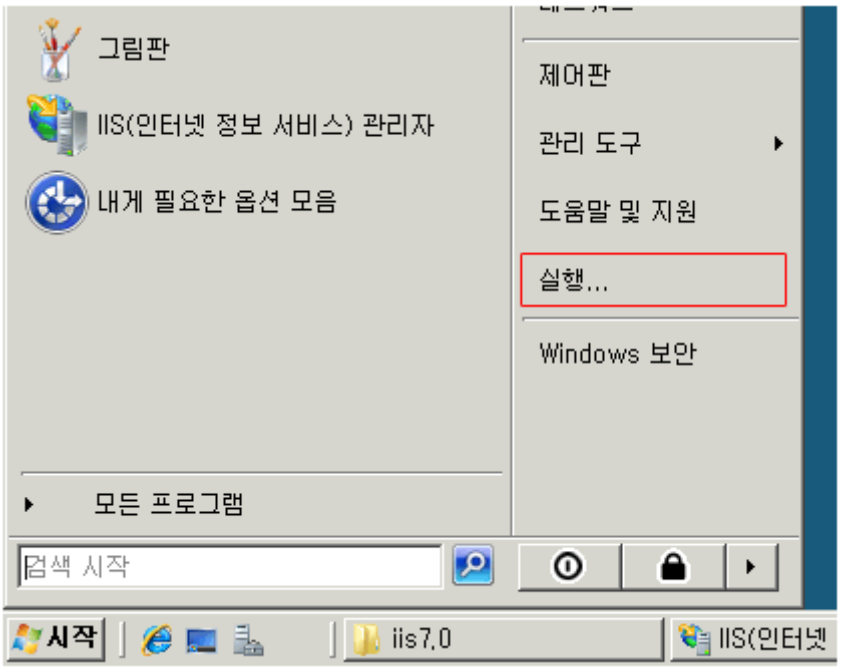
고객님의 웹 서버와 연계되어 설정된 방화벽 장비와 L4 Switch 장비의 설정을 80 포트 설정된 것 같이 443 포트에도 설정되어야 합니다.

6. 키쌍(key pair, 인증서 및 개인키) 백업 하기

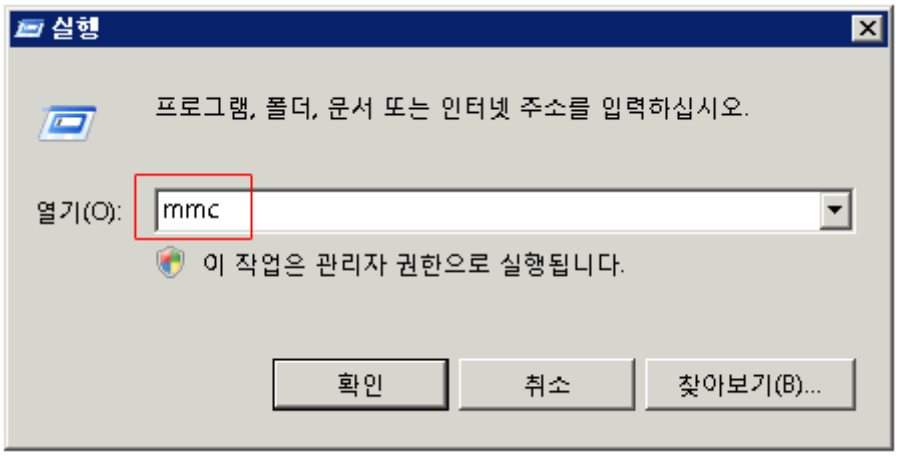
혹시라도 모를 재해를 대비해서 시스템에 설치된 키쌍(key pair, 인증서 및 개인키)을 백업합니다.
(시스템에 설치된 암호화 키(개인키)와 웹 서버인증서(공개키)는 MMC 콘솔로 관리됩니다.)
<인증서는 개인키와 함께 꼭 백업을 해두셔야 하며, 백업을 하지 않아 발생하는 문제에 대해서는 재발급 비용이 추가될 수 있습니다.>

IIS 서버에서는 CSR 생성할 때에 시스템에 암호화 키(개인키)를 생성합니다.
IIS 서버는 웹 서버인증서(공개키)가 설치되면서 이미 생성된 암호화 키(개인키)와 웹 서버인증서(공개키)를 하나의 키쌍(key pair, 인증서 및 개인키)으로 조합됩니다.
그래서 다음과정으로 키쌍(key pair, 인증서 및 개인키)을 백업 받습니다.

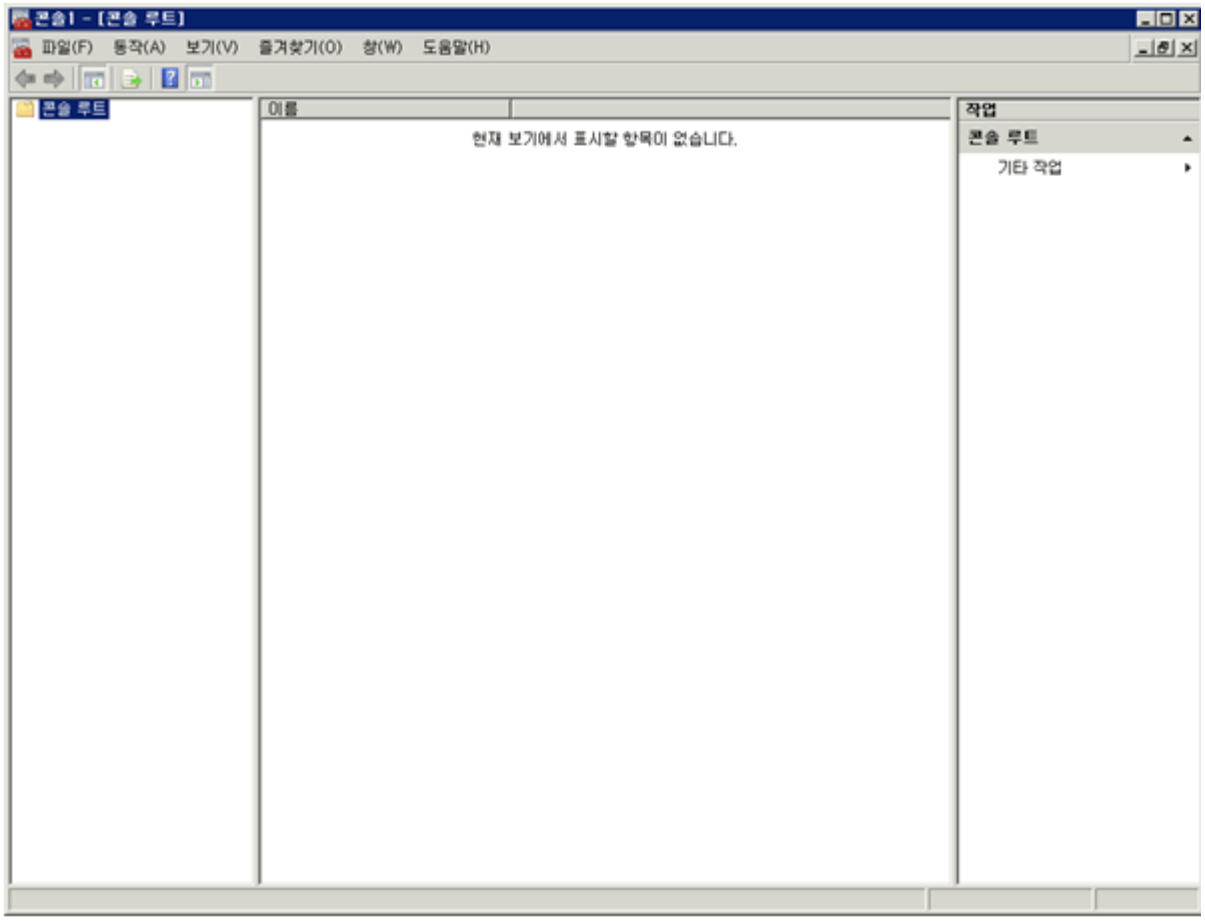
[시작] -> [실행]을 선택합니다.



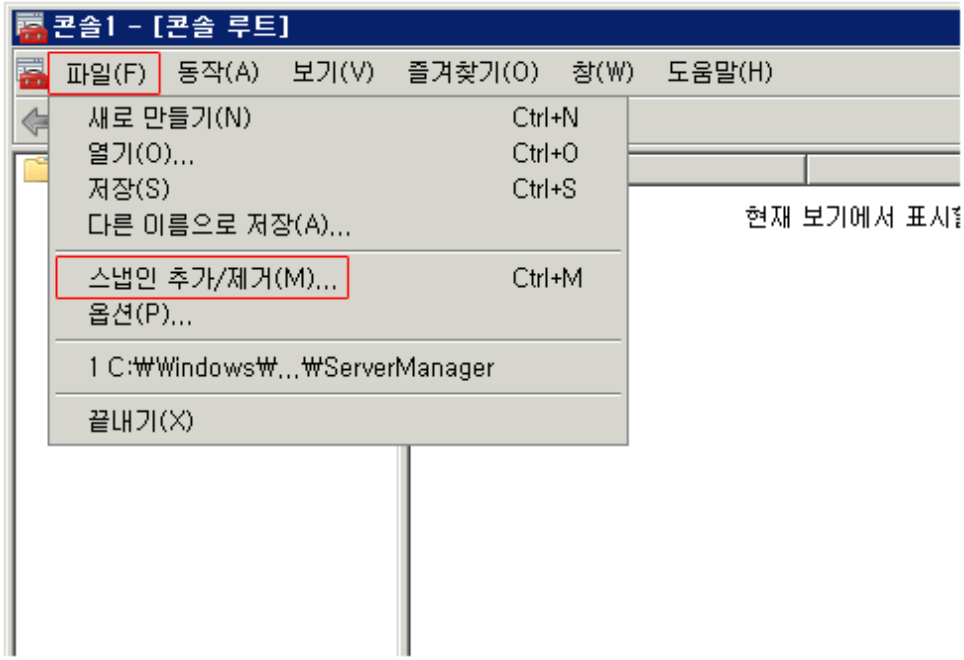
[실행] 창에서 mmc 을 입력하고 실행합니다.



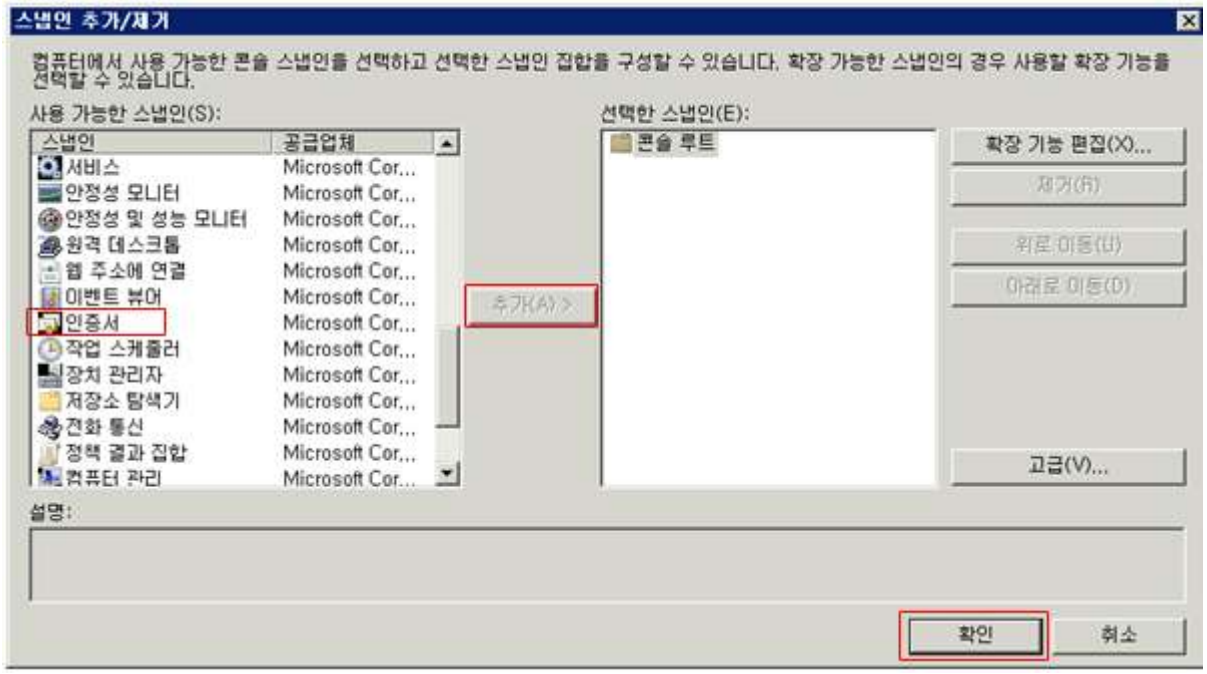
기본 mmc 콘솔 창 보실 수 있습니다.

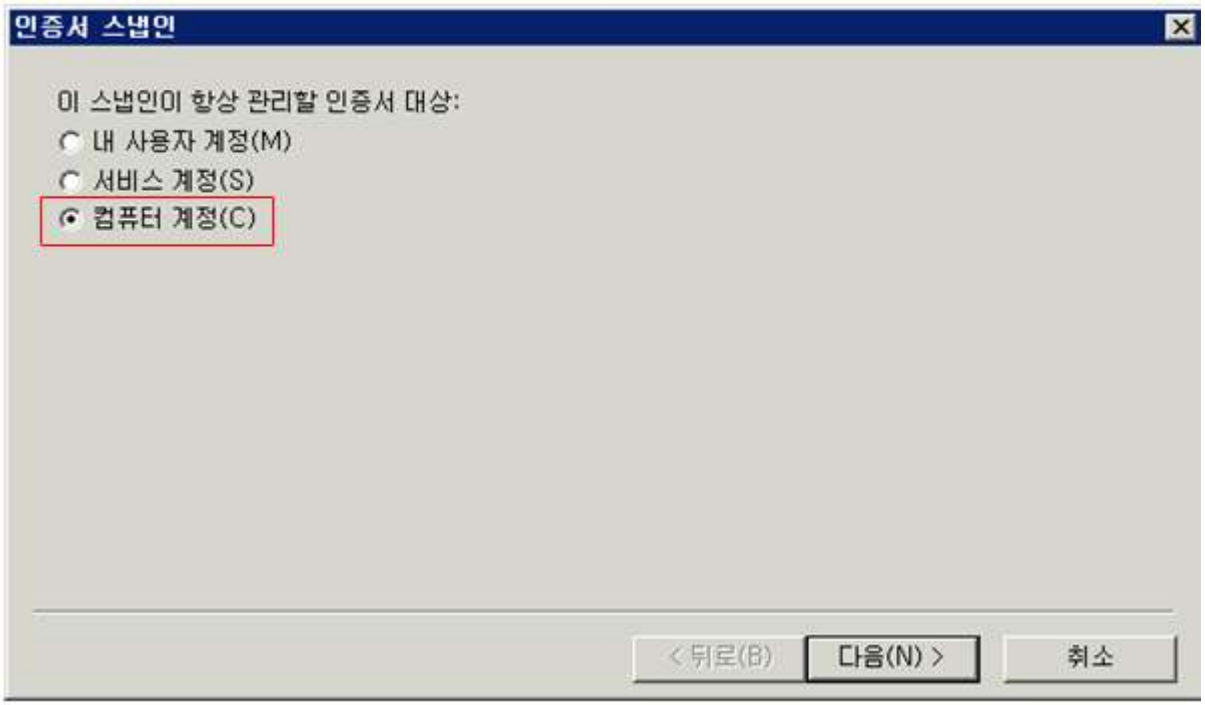


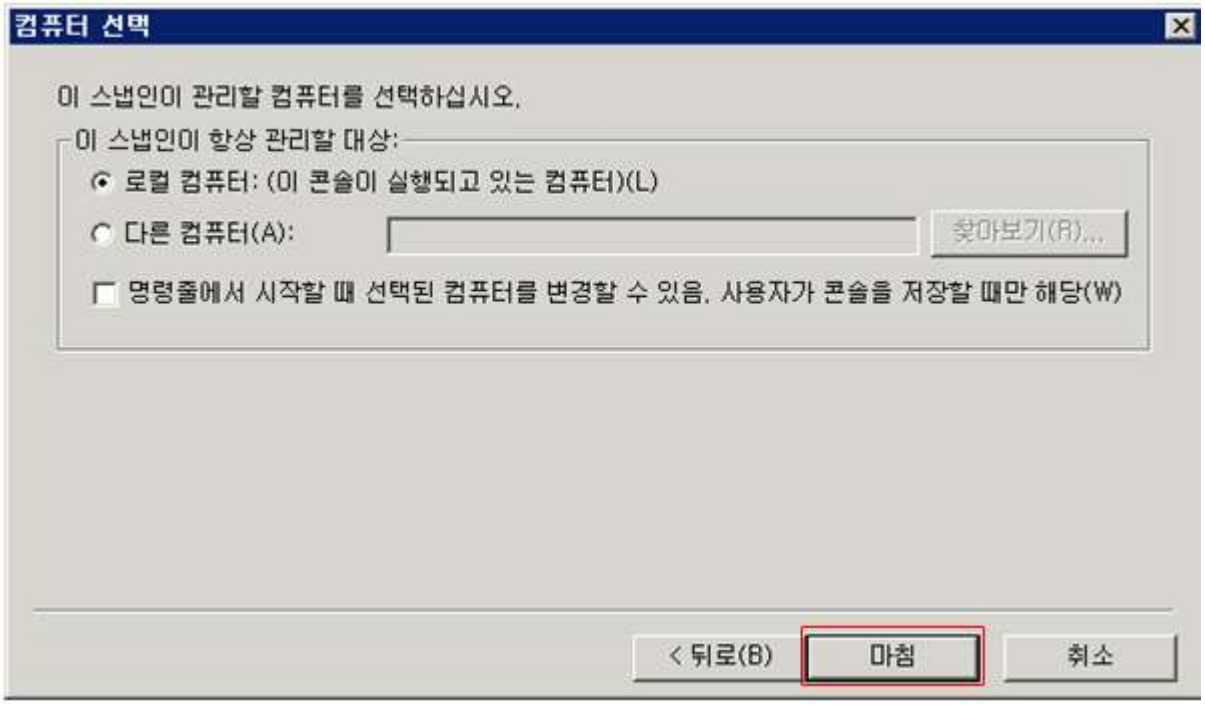
기본 mmc 콘솔 창에서 [콘솔] -> [스냅인 추가/제거]를 선택합니다.

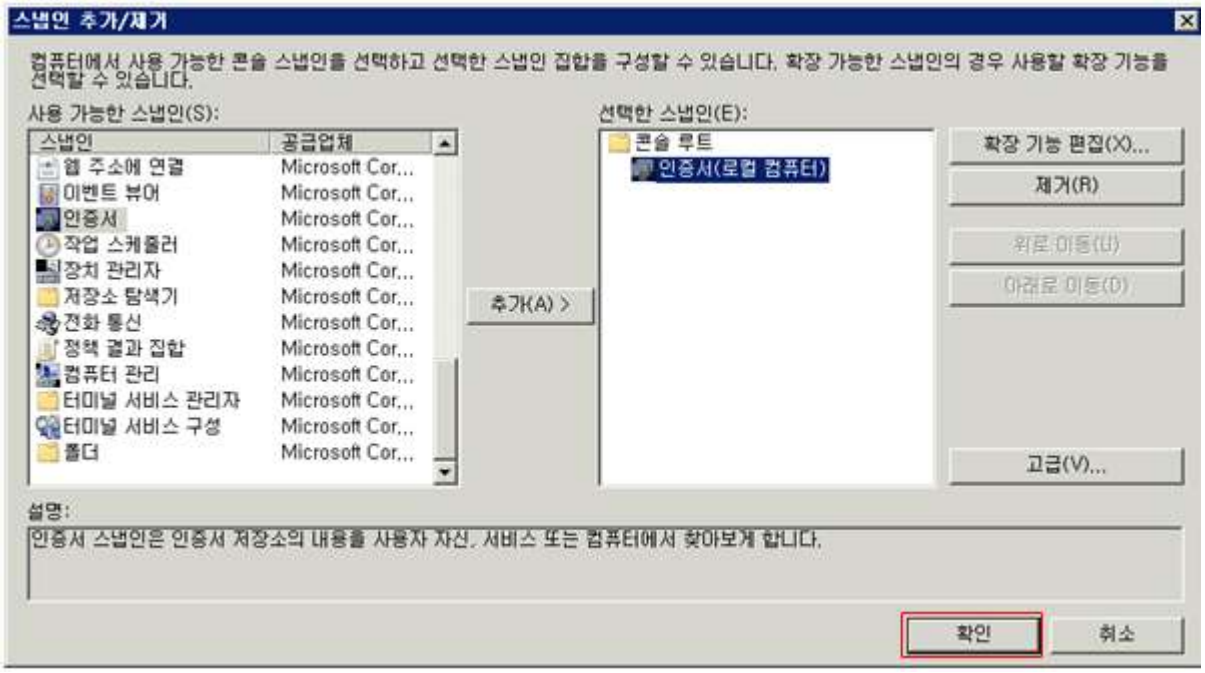


[스냅인 추가/제거] 창에서 [인증서]->[추가]->[확인]을 선택합니다.





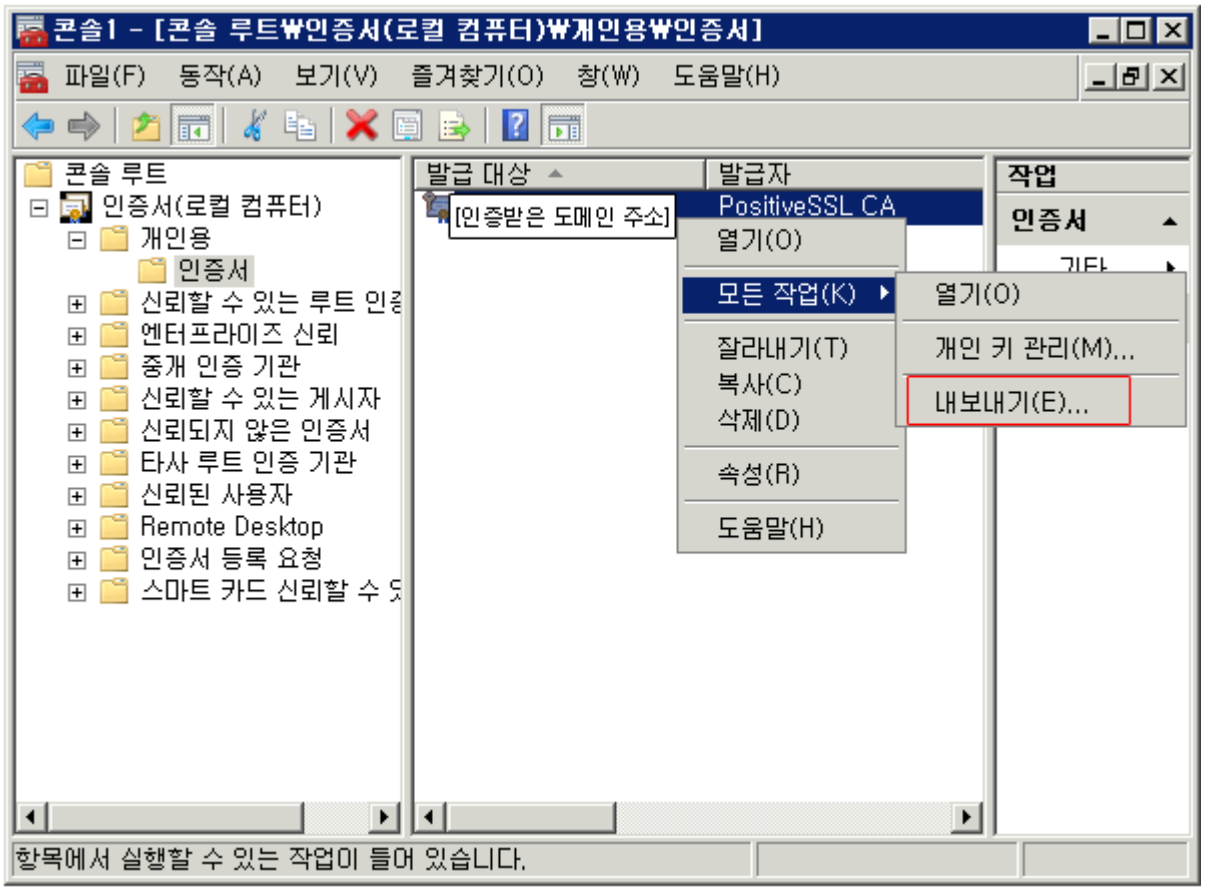




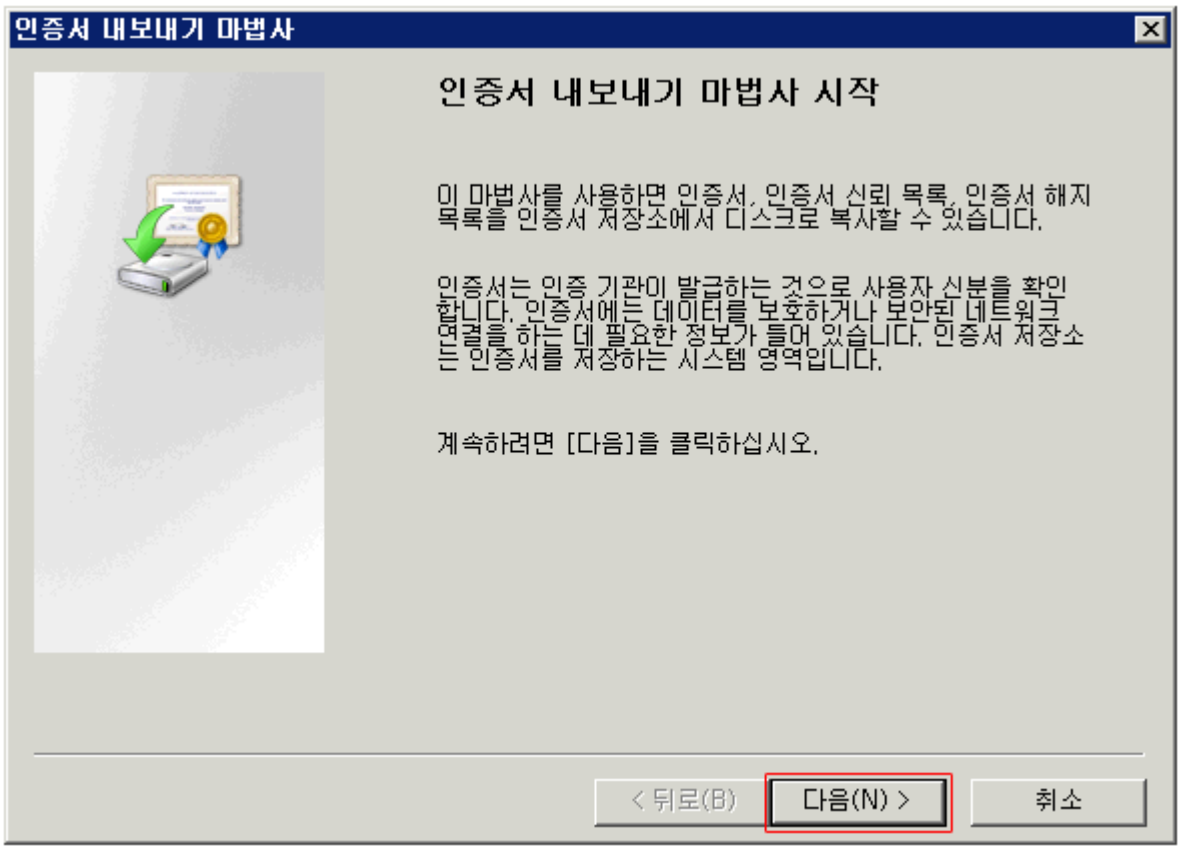
[인증서(로컬 컴퓨터)]에서 [개인] -> [인증서] 항목에 3. IIS 7.0 웹 서버에 인증서 설치하기에서 생성한 키쌍(key pair, 인증서 및 개인키-인증받은 도메인 이름으로 표시됩니다)을 볼 수 있습니다.

키쌍(key pair, 인증서 및 개인키)을 선택하고, 마우스 오른쪽 버튼으로 빠른 메뉴를 엽니다.

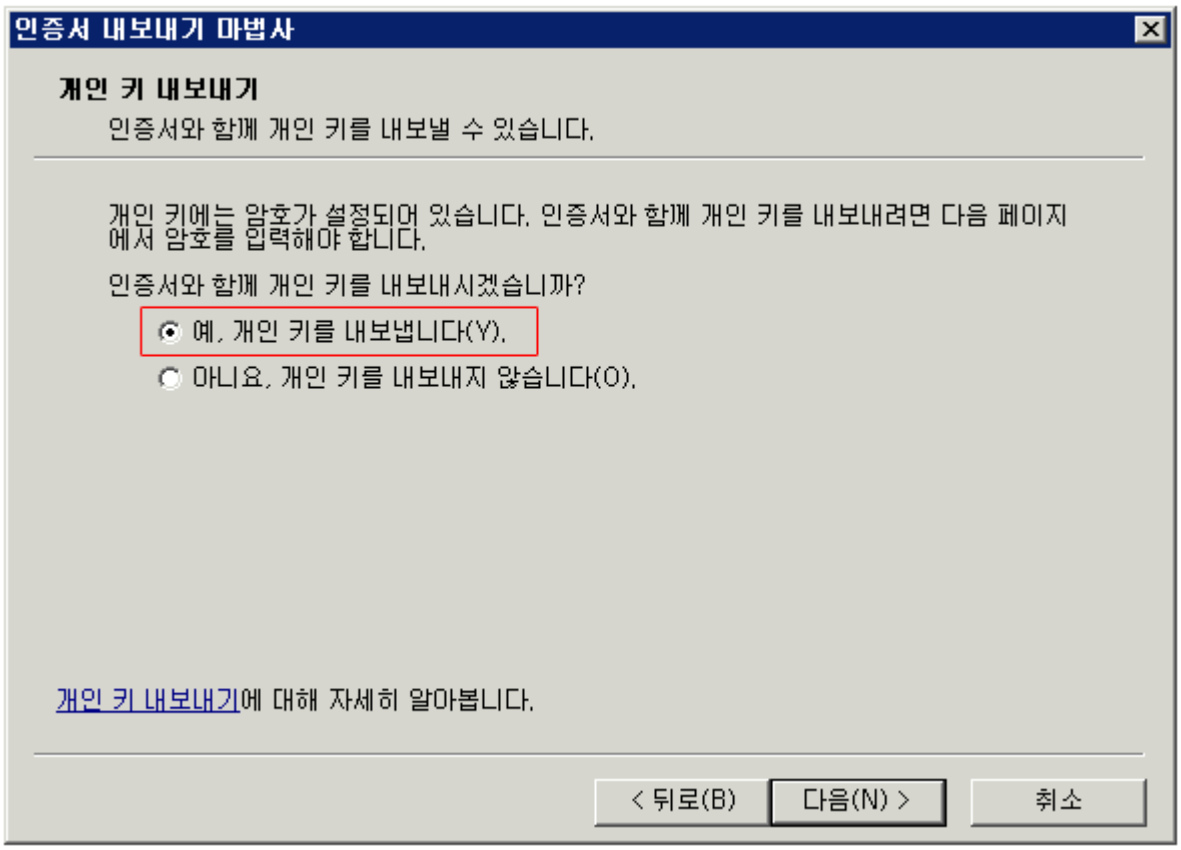
빠른 메뉴에서 [모든 작업] -> [내보내기]를 선택합니다.



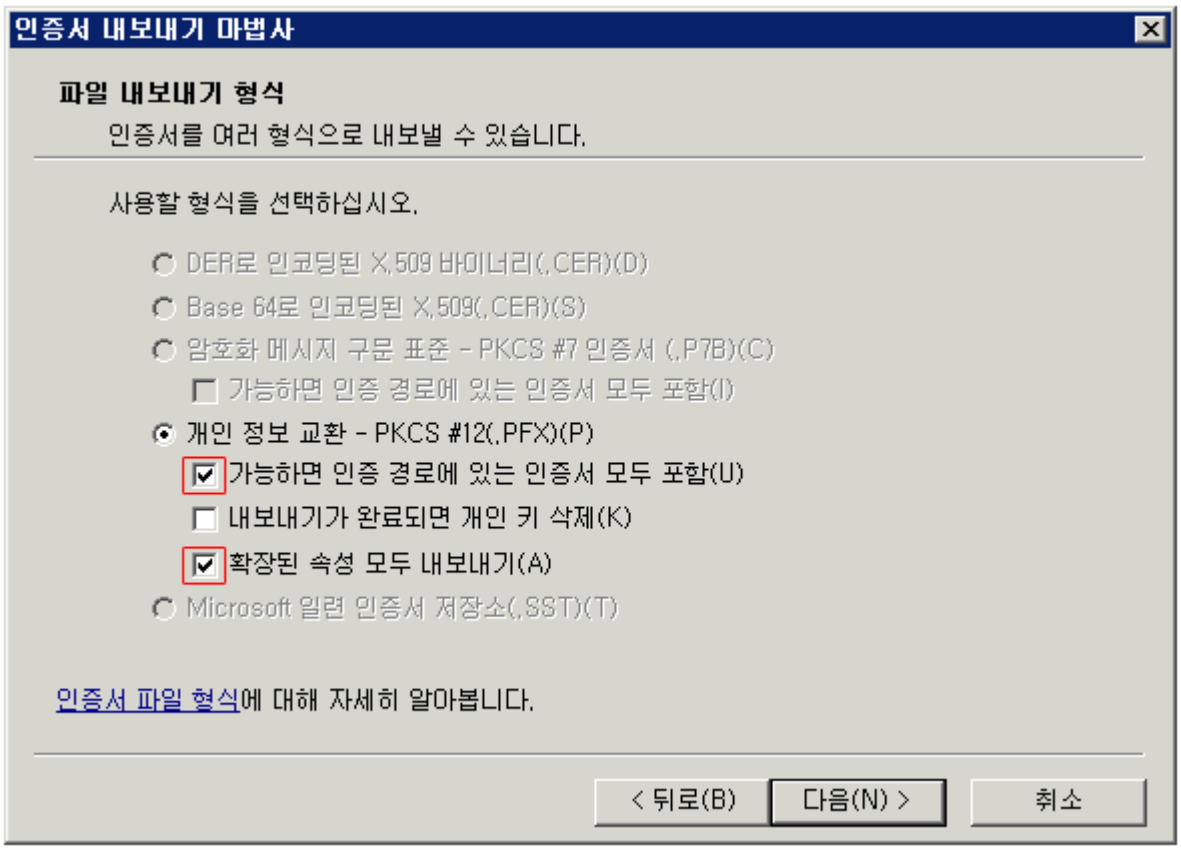
그러면 [인증서 내보내기 마법사] 창이 나타나며, 키쌍(key pair, 인증서 및 개인키)을 내보내는 백업 작업을 합니다.



키쌍(key pair, 인증서 및 개인키) 백업 옵션 [예, 개인키를 내보냅니다.]를 선택합니다.

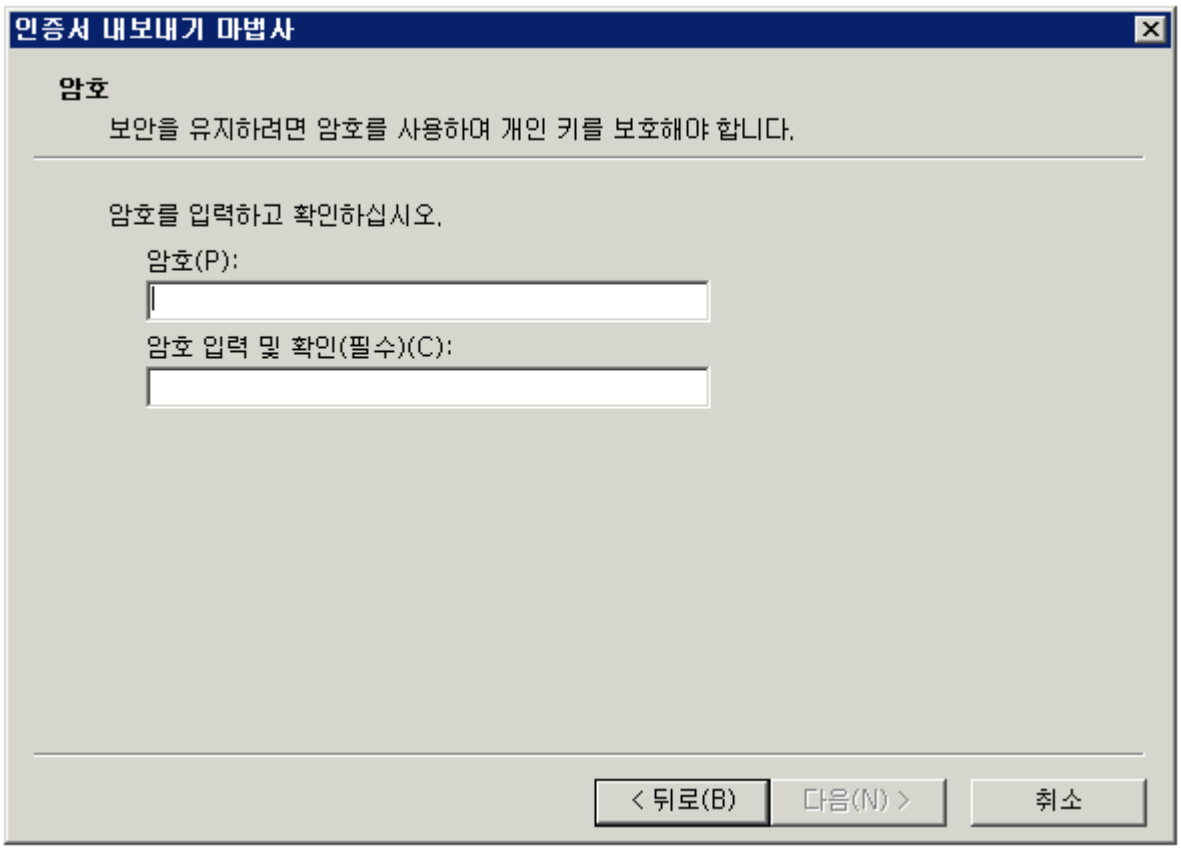


파일 내보내기 형식으로 [개인 정보 교환-PKCS #12(.PFX)]를 선택합니다.

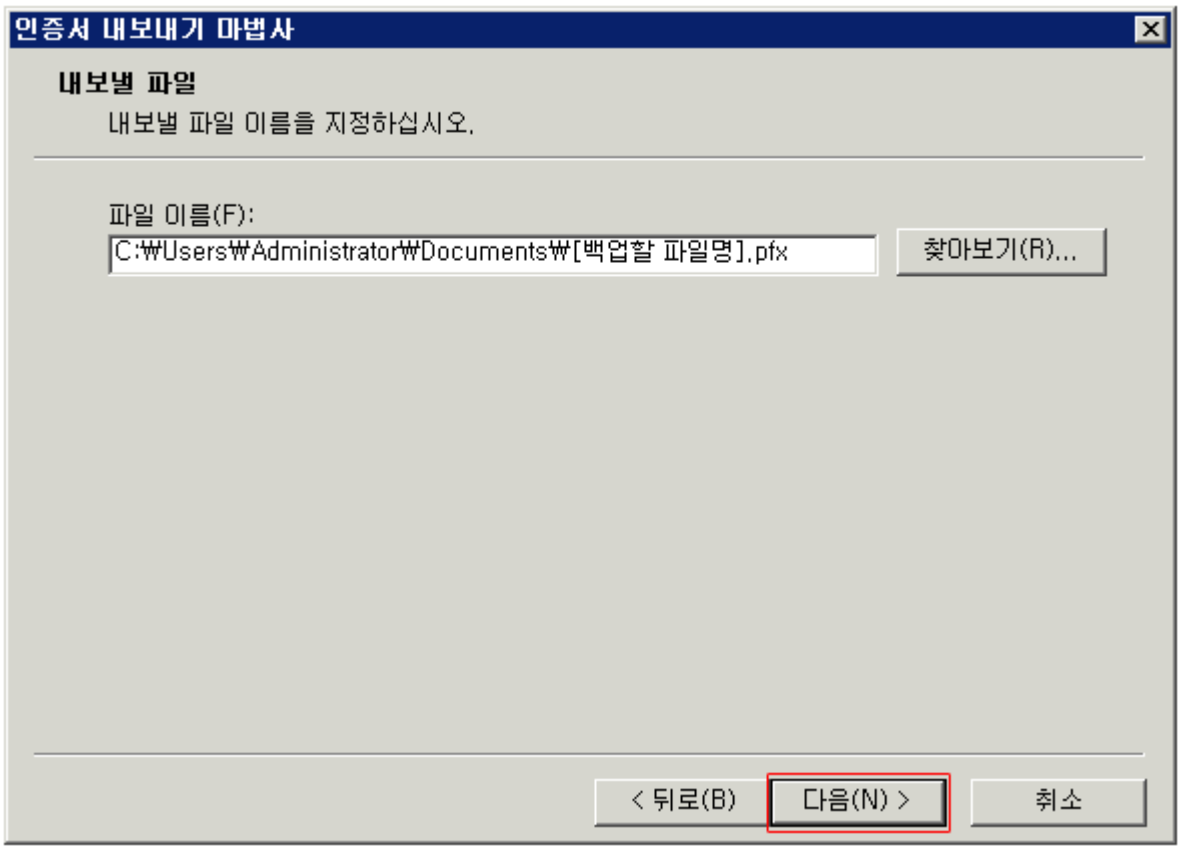


암호화 키(개인키)의 암호를 설정합니다.

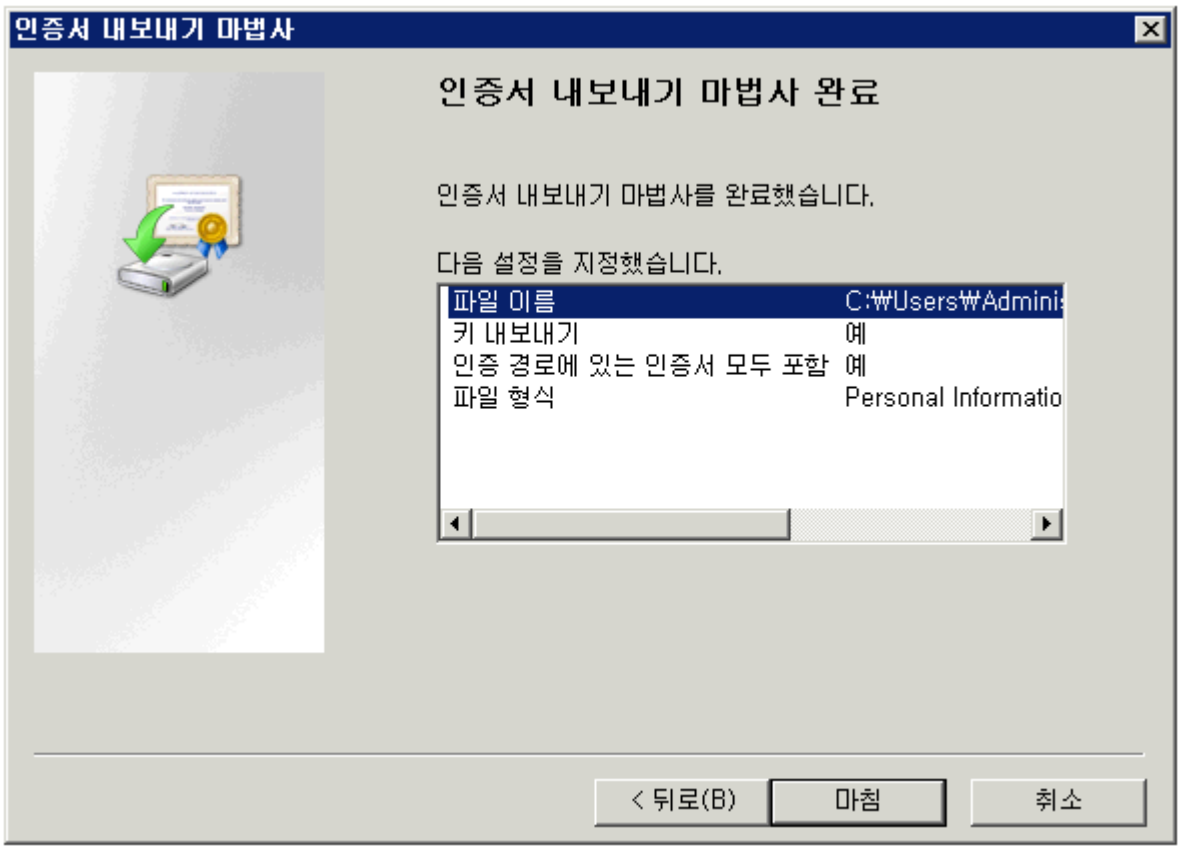
(암호화 키(개인키)의 암호는 반드시 기억하고 있어야 합니다. 암호화 키(개인키)의 암호를 분실하게 되면 백업하신 키쌍(key pair, 인증서 및 개인키)을 사용할 수 없게 됩니다.)



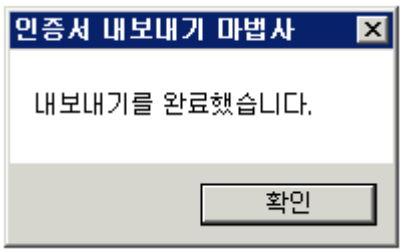
내보낼 키쌍(key pair, 인증서 및 개인키)의 파일이름을 입력합니다.



키쌍(key pair, 인증서 및 개인키) 내보내기를 완료합니다.



키쌍(key pair, 인증서 및 개인키) 내보내기를 결과를 확인합니다.



내보낼 키쌍(key pair, 인증서 및 개인키)의 파일이 생성되었습니다. 보안된 PC 의 저장장치 등 안전한 곳에 보관합니다.

SSL 설치가 완료 되었습니다.