

# **Windows Server 2003**

## **IIS6**

### **(Multi)**

# **SSL 인증서 갱신 설치 가이드**

본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로  
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다.

**[고객센터]**  
**한국기업보안. 유서트 기술팀**  
**02-3442-7230**



**한국기업보안**  
Korea Corporation Security

※ 이 문서는 일반적인 설정이며 서버 및 네트워크 환경에 따라 달라질 수 있습니다.

인증기관 별 Root & Chain 인증서 구분 방법입니다.

※ 발급 받은 인증서를 아래 표를 참고하여 Root 및 Chain 인증서를 구분 합니다.

**[GlobalSign] - 인증기관**

설정구분	인증서 형식
중간 인증 기관	GLOBALSIGN_RSA_DV_SSL_CA_2018.crt [DV] GLOBALSIGN_RSA_OV_SSL_CA_2018.crt [OV] ALPHASSL_CA_SHA256_G2.crt [Alpha] GLOBALSIGN_EXTENDED_VALIDATION_CA_SHA256_G3.crt [EV] GLOBALSIGN.crt
신뢰할 수 있는 루트 인증 기관	GLOBALSIGN Root CA.crt

**[Comodo] - 인증기관**

설정구분	인증서 형식
중간 인증 기관	SECTIGO_RSA_DOMAIN_VALIDATION_SECURE_SERVER_CA.crt USERTRUST_RSA_CERTIFICATION_AUTHORITY.crt
신뢰할 수 있는 루트 인증 기관	AAA Certificate Services.crt

**[Digicert] - 인증기관**

설정구분	인증서 형식
중간 인증 기관	THAWTE_RSA_CA_2018.crt
신뢰할 수 있는 루트 인증 기관	DIGICERT_GLOBAL_ROOT_CA.crt

www.ucert.co.kr

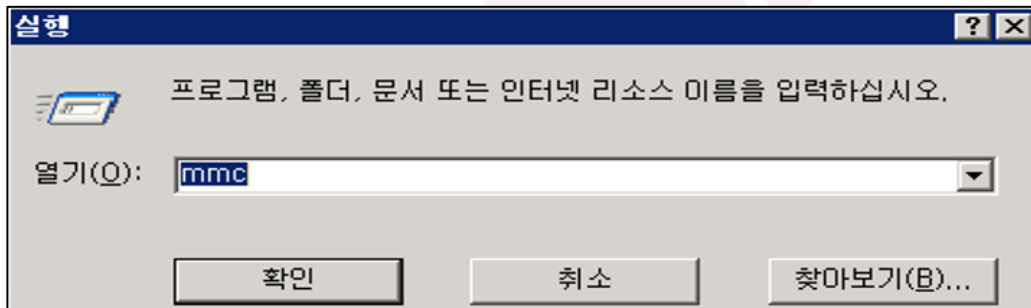


본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로  
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

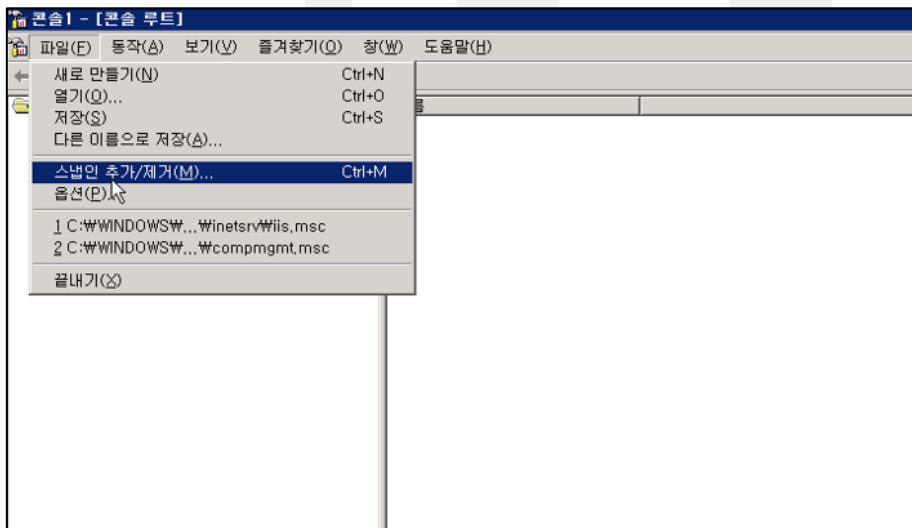
Copyright 2018-2023. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

## 1. MMC 콘솔을 실행하여 인증서 Import 작업을 실행 합니다.

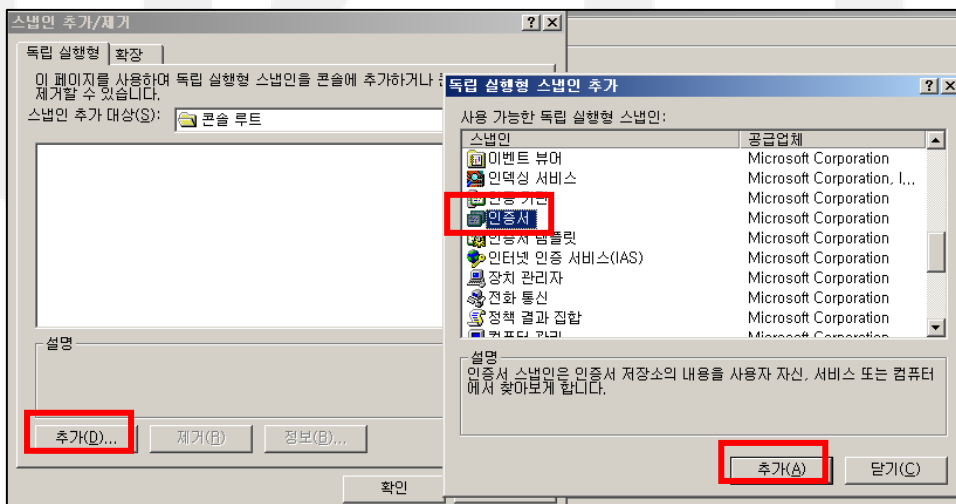
1). "실행" 창을 실행하여 MMC 를 실행 합니다. [Windows 키 + R 키 > mmc]



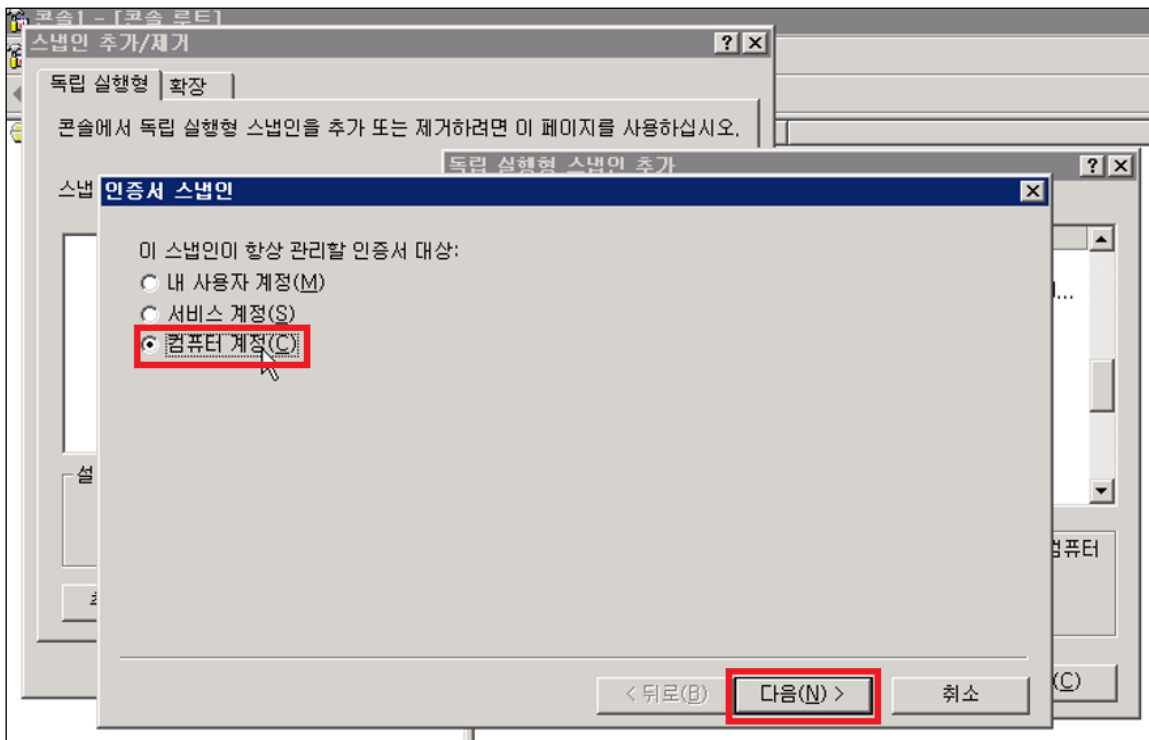
2). "파일"> "스냅인 추가/제거"를 선택 합니다.



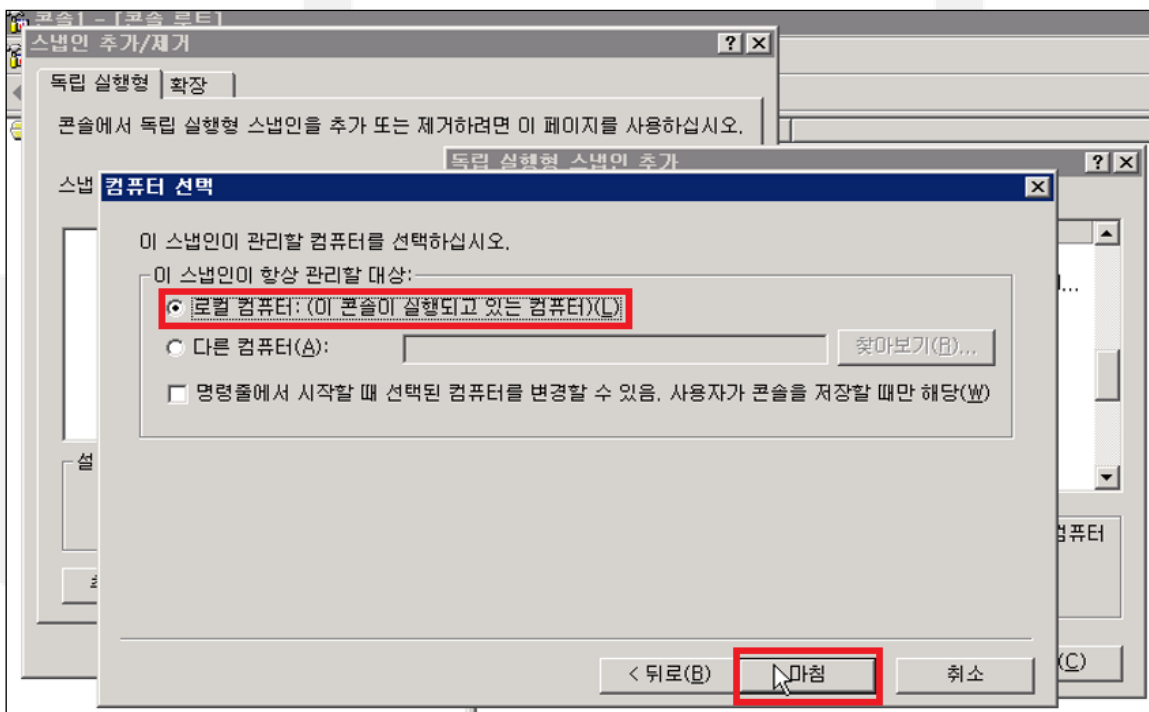
3). "추가"를 선택하여 "인증서"를 선택 후 추가 합니다.

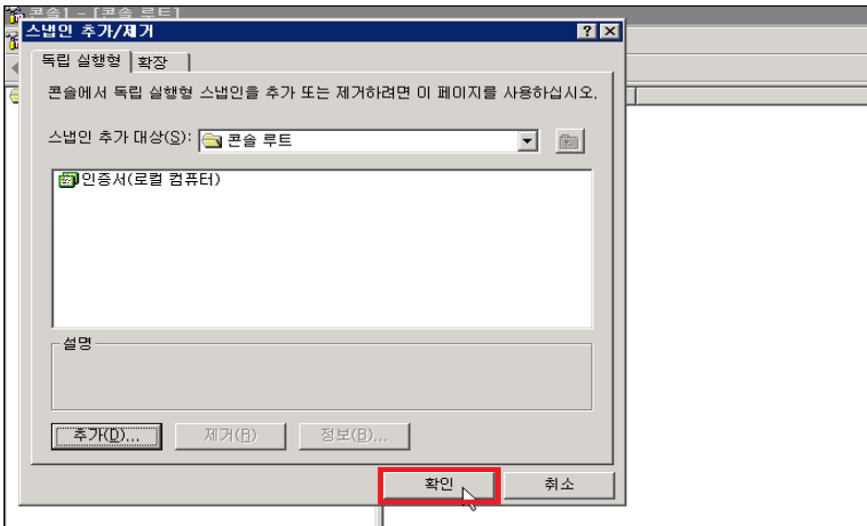


4). "컴퓨터 계정" 선택 합니다.

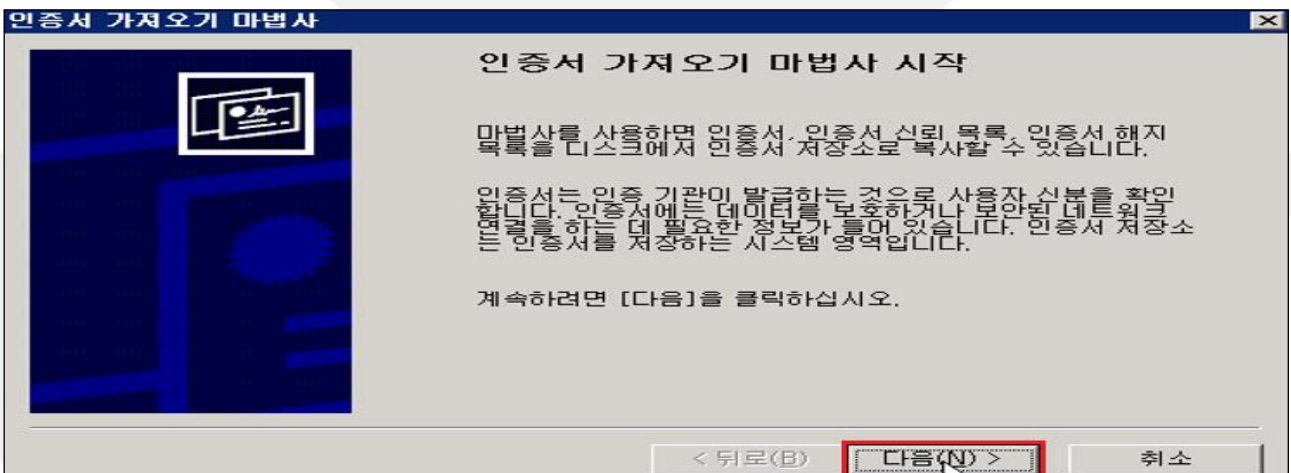
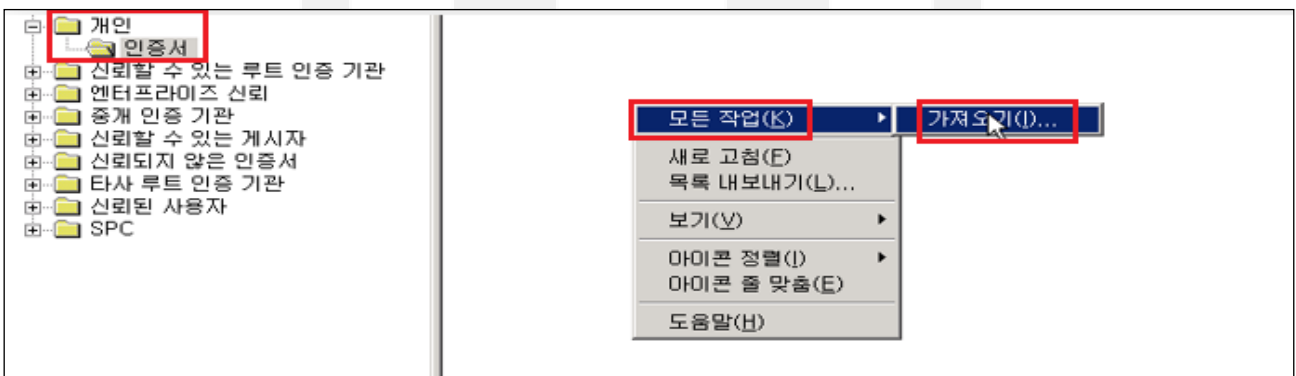


5). "로컬 컴퓨터" 선택> 다음> 확인을 눌러 완료 합니다.



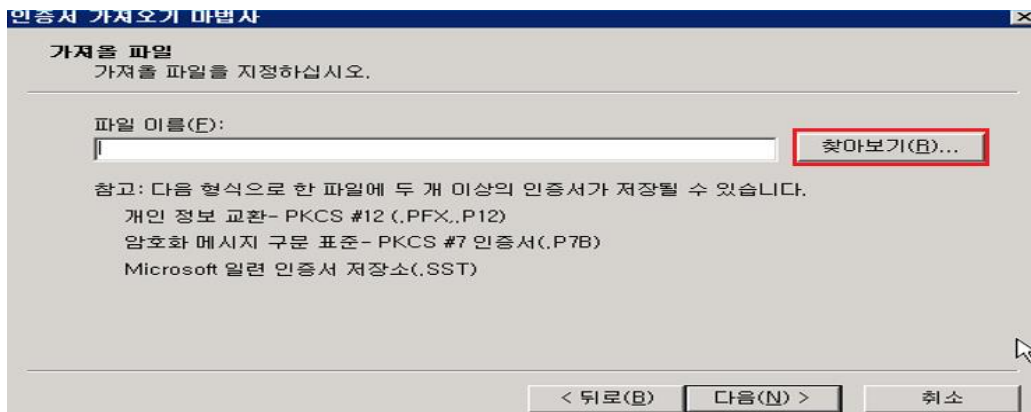


6). "개인" > "인증서"를 선택하여 빈 공간에 마우스 우클릭을 하여 "모든 작업" > "가져오기"를 선택 합니다.

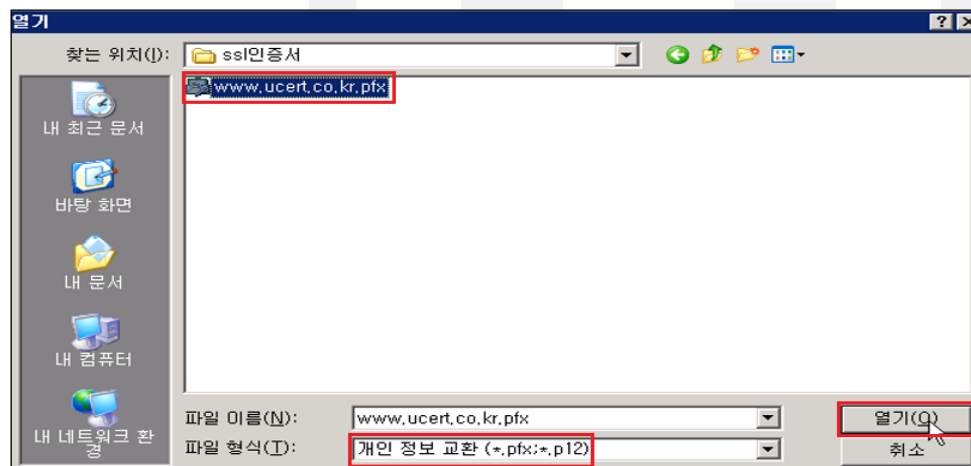


www.ucert.co.kr

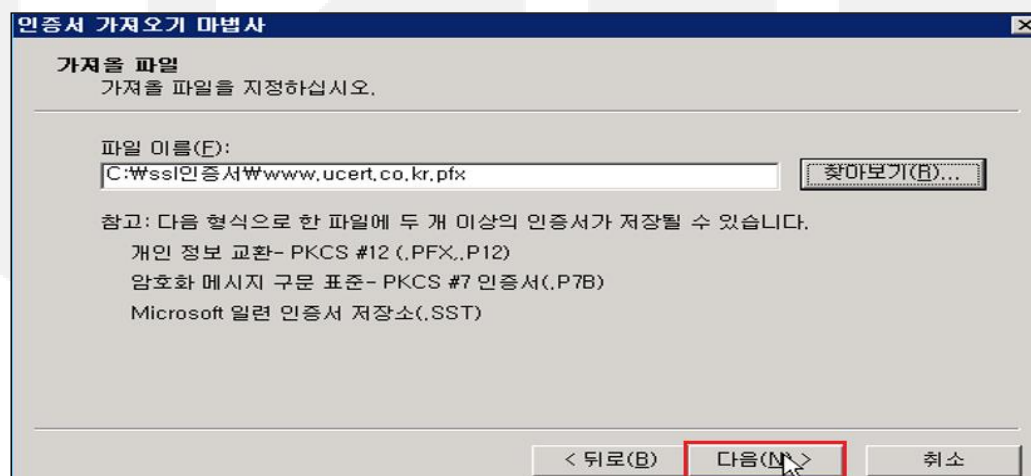
7). 인증서 가져오기 마법사가 실행되면 "찾아보기"를 선택하여 인증서를 불러 옵니다.



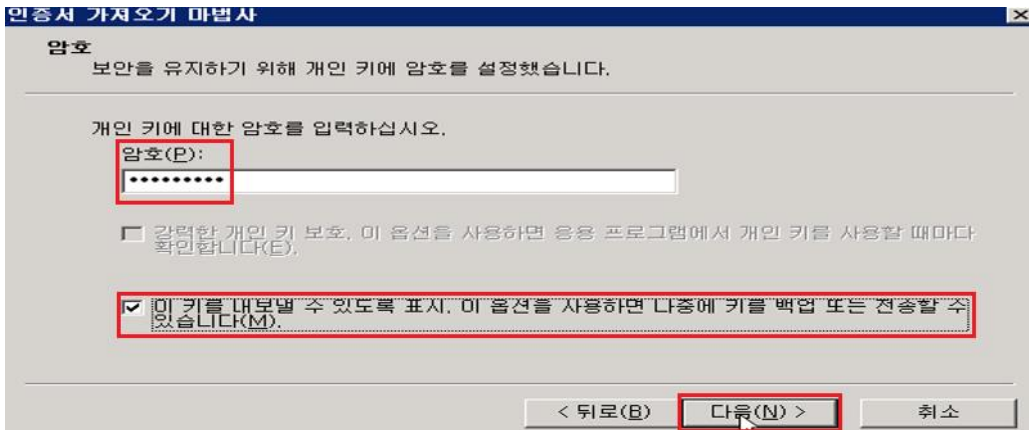
8). 서버에 업로드 한 인증서 경로에서 파일 형식에서 ".pfx" 지정하여 인증서를 불러온 후 다음을 클릭 합니다.



※ (필수)파일 형식을 개인 정보 교환으로 변경 시 PFX파일 확인 가능



9). 인증서 비밀번호를 입력하고 체크박스를 선택하여 다음을 클릭 합니다.



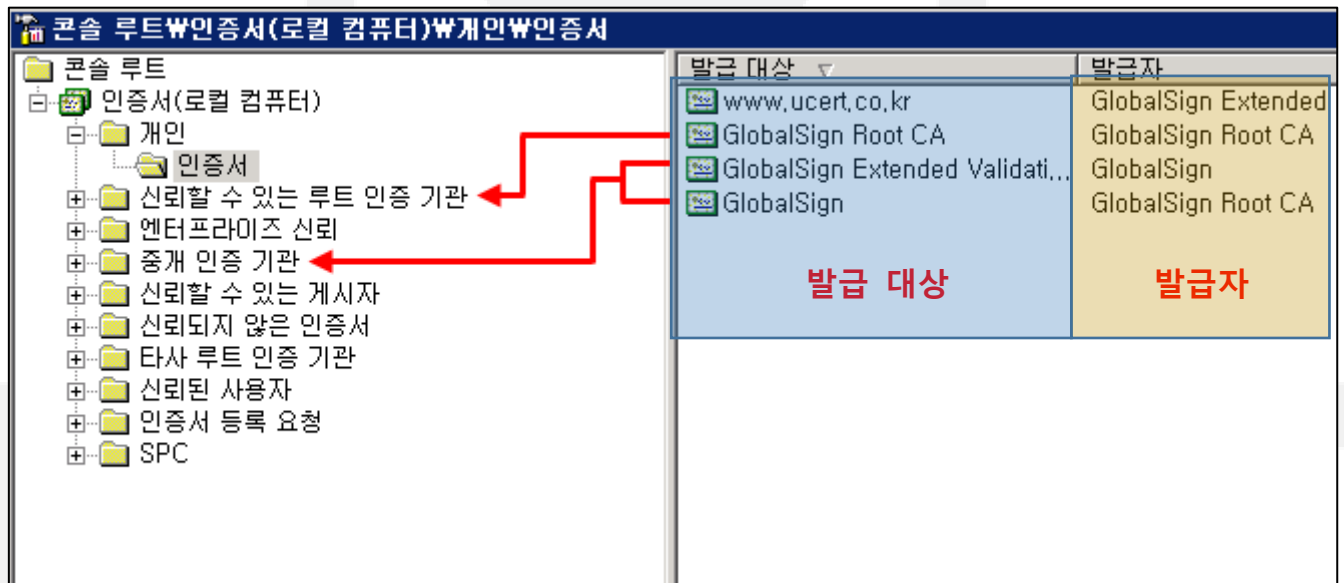
10). 인증서 중 각각의 인증서를 위의 [표\(2 페이지\)](#)에 맞추어 옮기도록 한다.

※간단하게 구분하는 방법

개인 → 인증서 : 발급 대상이 도메인으로 된 인증서

신뢰할 수 있는 루트 인증 기관 → 인증서 : 발급 대상과 발급자가 동일한 인증서

중간 인증 기관 → 인증서 : 발급 대상과 발급자가 동일하지 않은 인증서

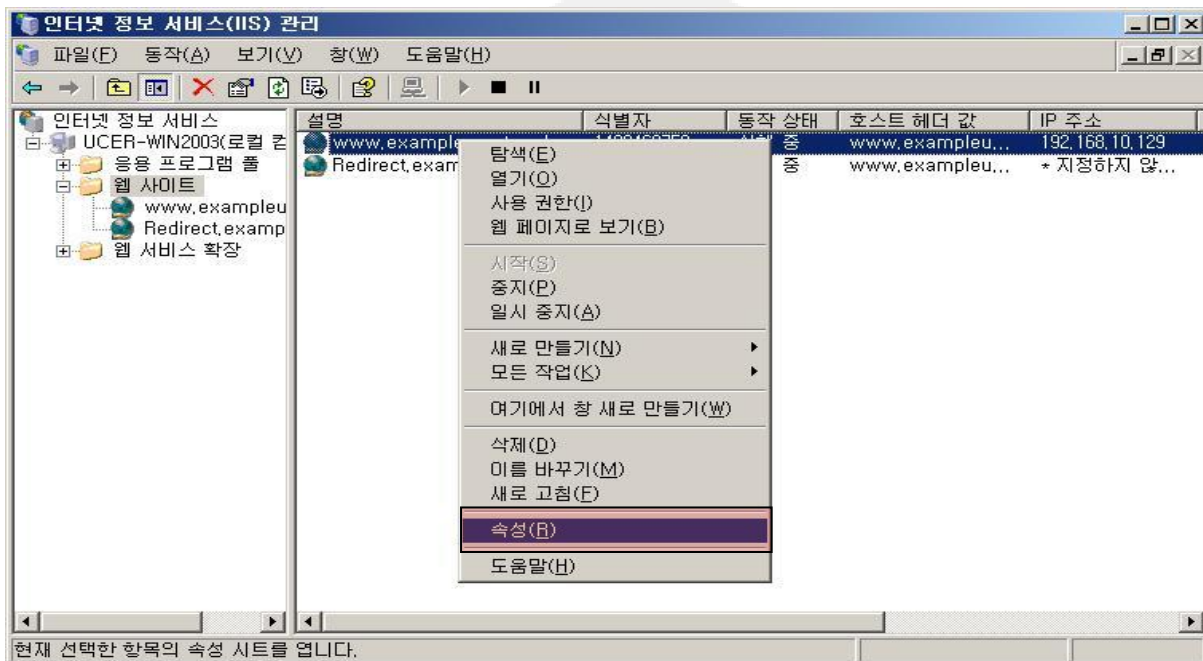


※ ucert 에서 판매량이 많은 GlobalSign 인증서 기준이며 인증서별로 이름은 달라질 수 있습니다.

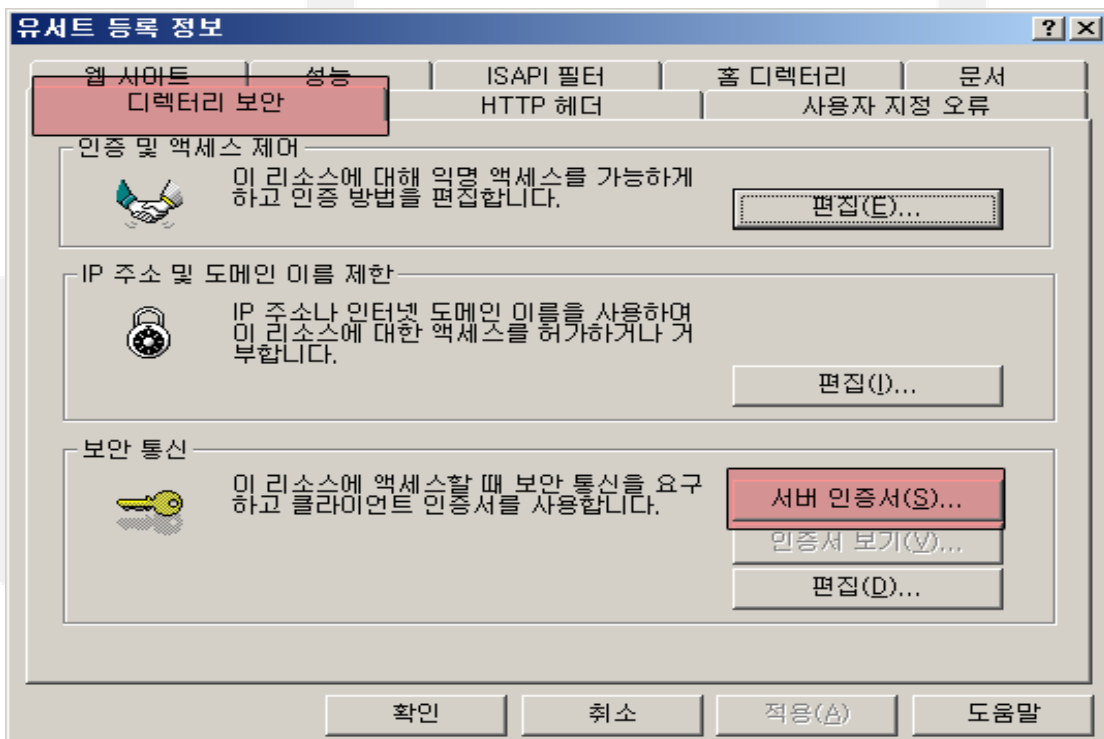
www.ucert.co.kr

## 2. 인터넷 정보 서비스(IIS) 관리를 실행하여 인증서를 설치 합니다.

1). SSL 인증서를 적용할 도메인의 사이트를 선택 후 "속성"을 선택 합니다.

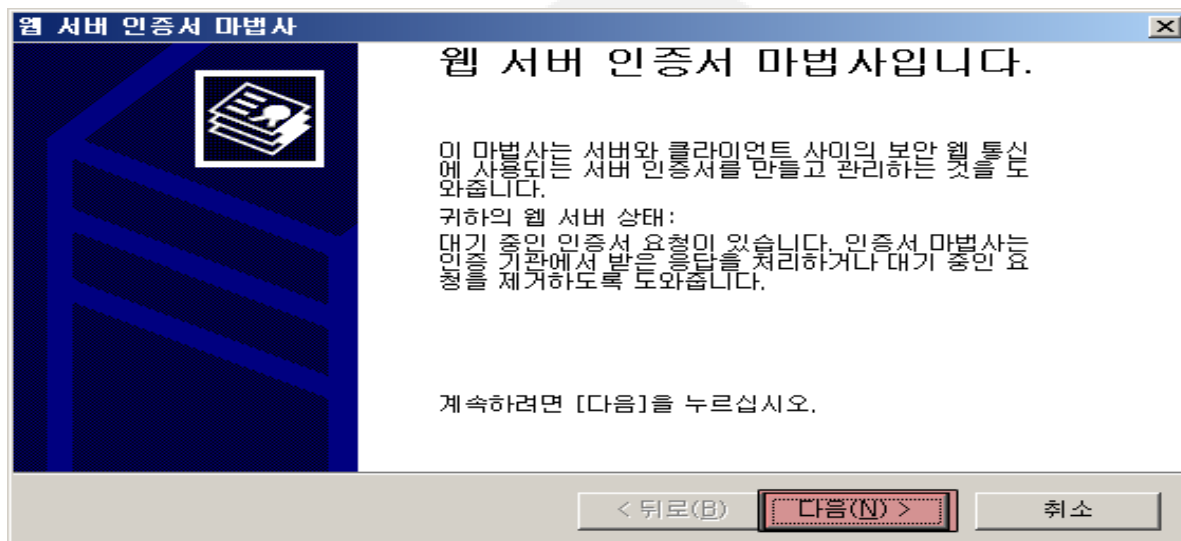


2). "디렉토리 보안" 탭으로 이동하여 "보안 통신"의 서버인증서(S)를 클릭 합니다.

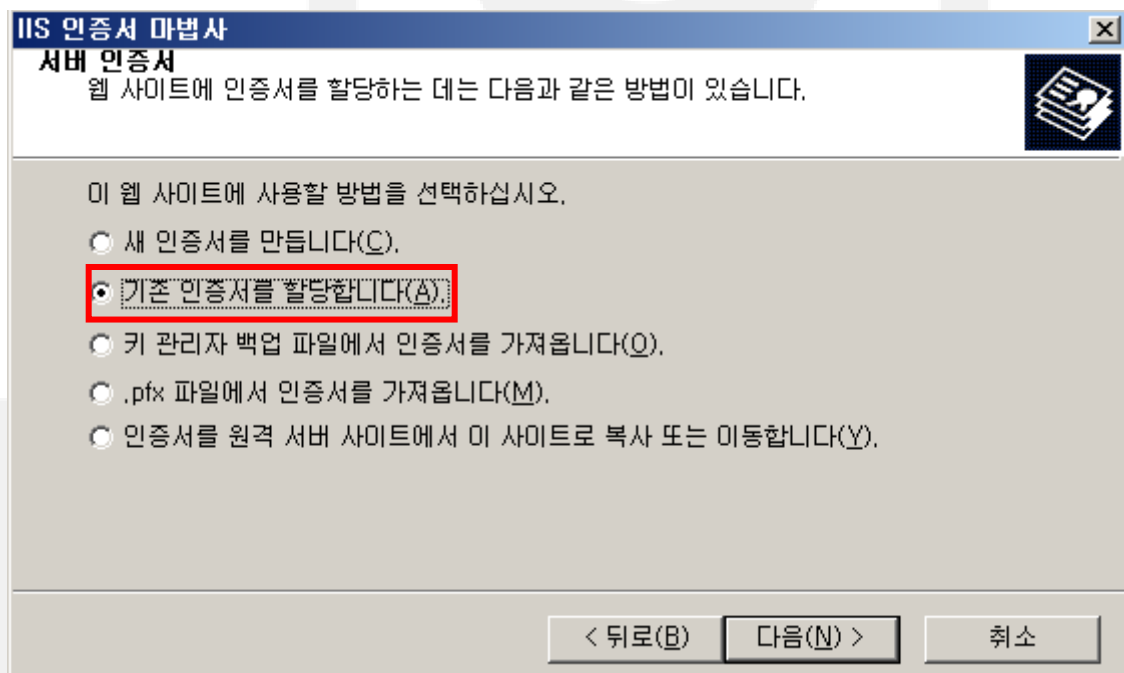




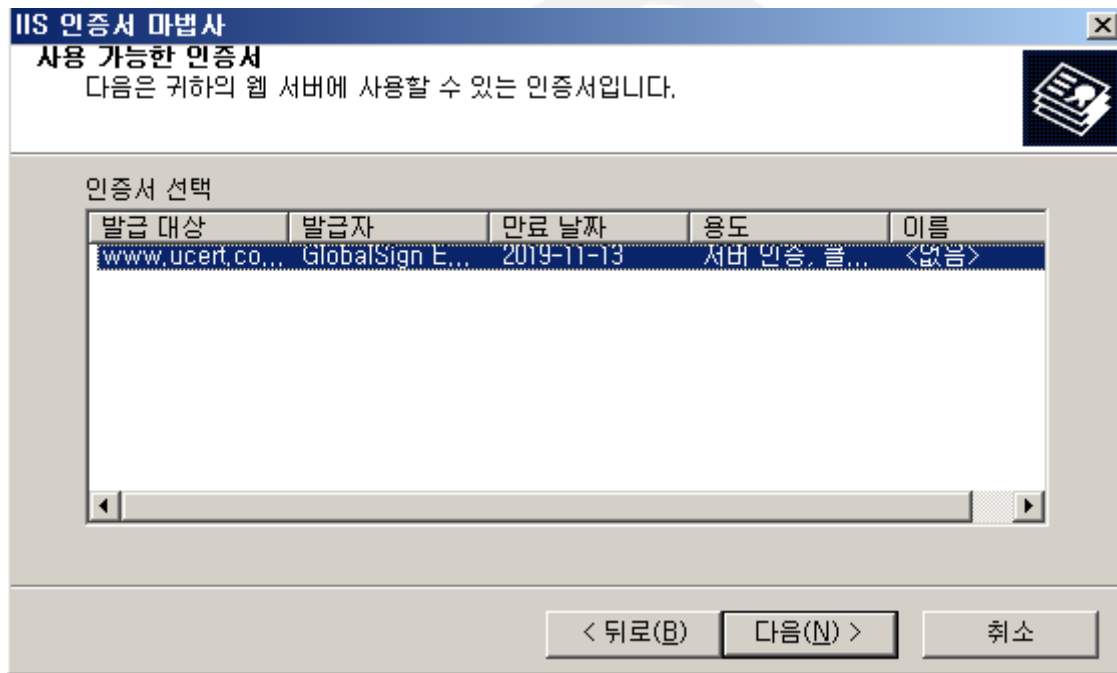
3). 서버 인증서 마법사가 실행되면 다음을 클릭 합니다.



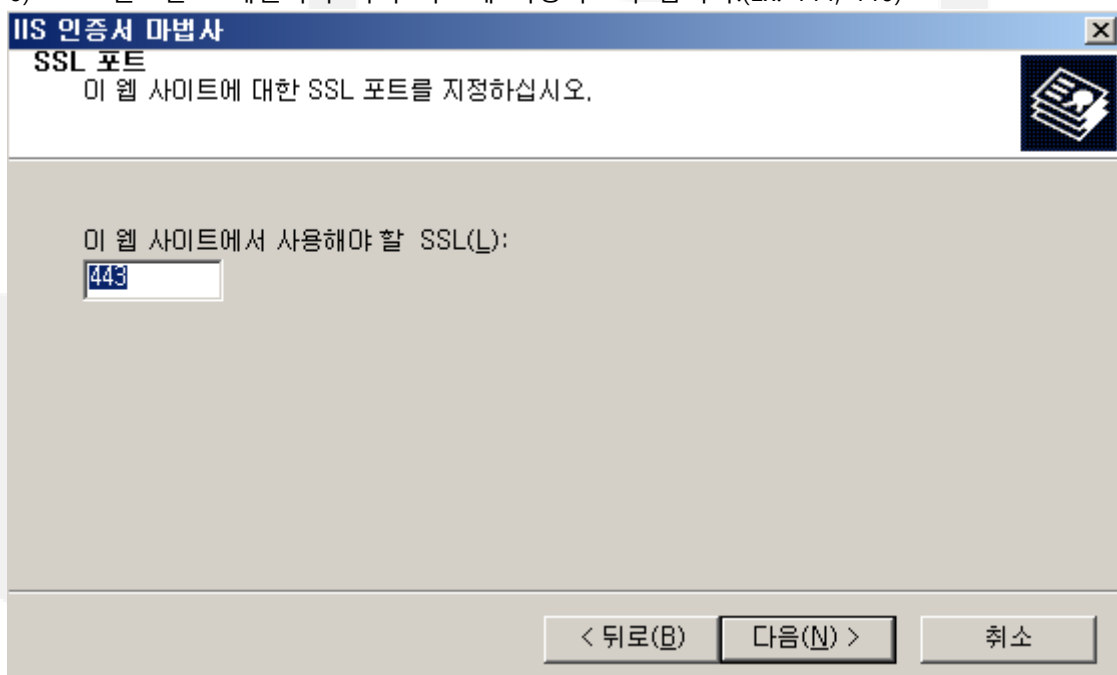
4) "기존 인증서를 할당합니다"를 선택 후 다음을 클릭 합니다.



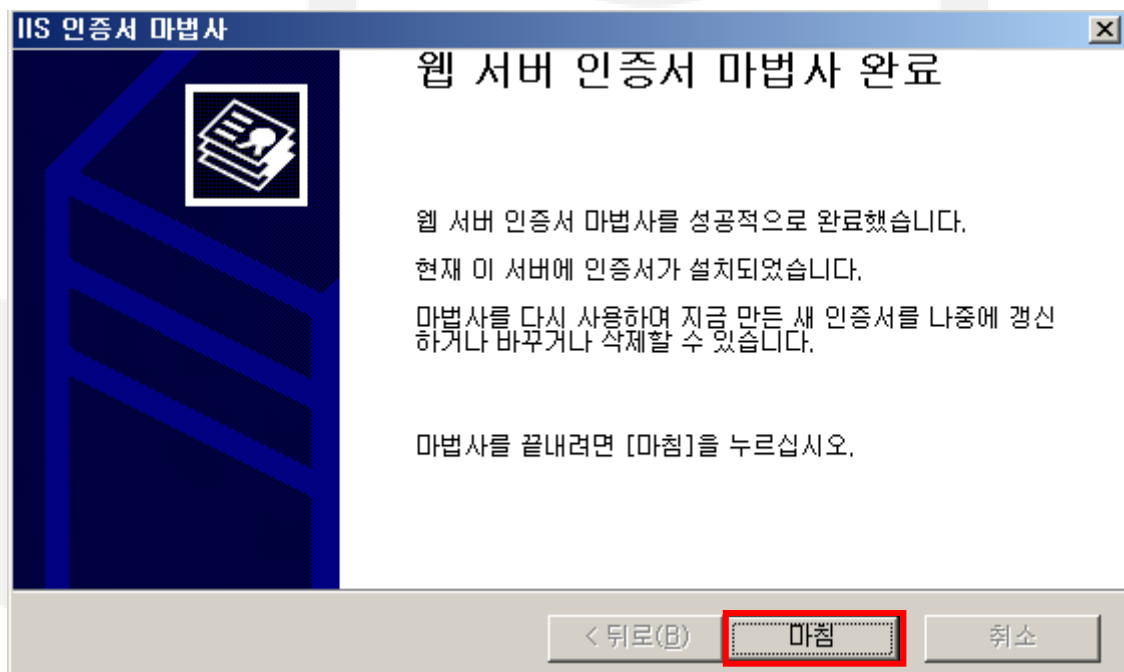
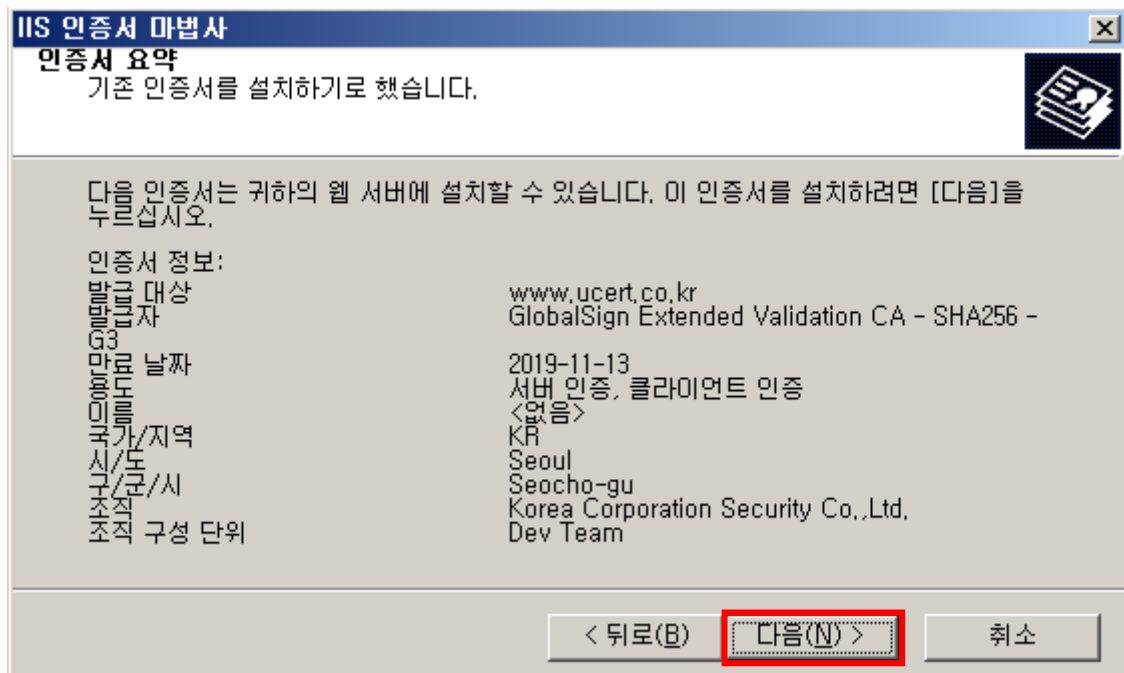
5) 사용 할 인증서를 선택하고 다음으로 넘어가고 인증서를 사용 할 포트번호를 입력합니다.



6) 포트번호는 도메인마다 각자 다르게 지정하도록 합니다.(Ex. 444, 446)



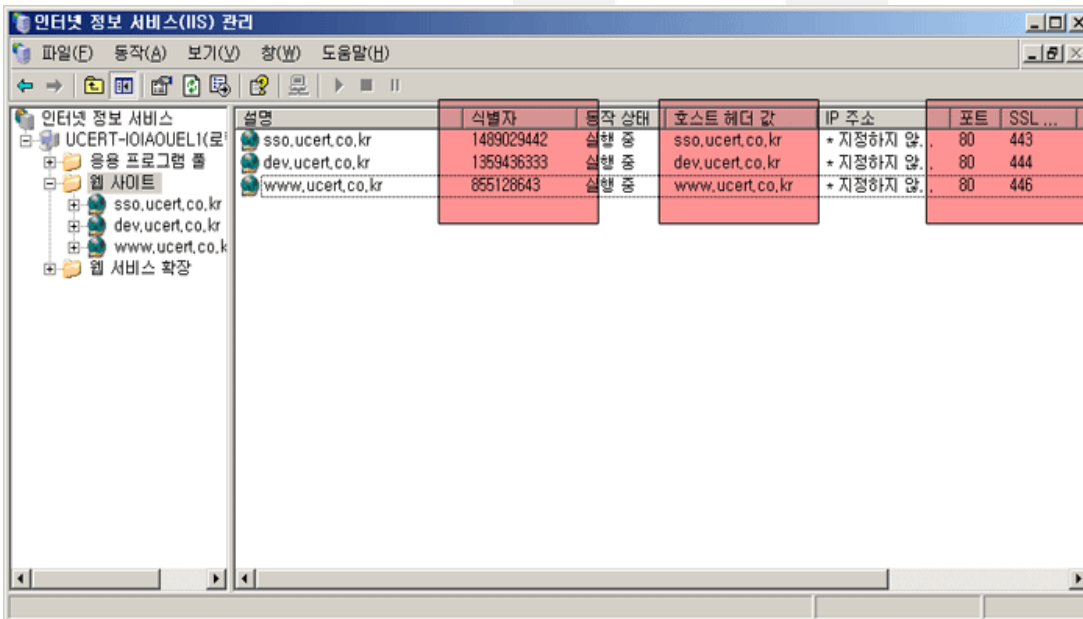
7) 인증서 정보가 맞는지 확인 후 다음을 선택하여 마침을 눌러 작업을 완료 합니다.



※ 위 과정을 나머지 적용하셔야 할 사이트도 동일하게 진행하시되 SSL 포트는 444, 446 등 다르게 세팅합니다.  
만약 동일하게 세팅하면 포트 충돌이 일어나서 사이트가 중지되기 때문에 먼저 포트를 나누신 후  
Securebinding 작업으로 중복포트 설정 작업을 진행 합니다.

### 3. Securebinding 작업을 통하여 중복 포트를 설정 합니다.

1) 적용하실 사이트와 매칭되는 식별자 번호를 확인합니다.



설명	식별자	동작 상태	호스트 헤더 값	IP 주소	포트	SSL ...
sso.ucert.co.kr	1489029442	실행 중	sso.ucert.co.kr	* 지정하지 않.	80	443
dev.ucert.co.kr	1359436333	실행 중	dev.ucert.co.kr	* 지정하지 않.	80	444
www.ucert.co.kr	855128643	실행 중	www.ucert.co.kr	* 지정하지 않.	80	446

2) cmd 창을 열어서 중복포트 설정을 합니다.

[명령어 형식]

cscript.exe C:\inetpub\AdminScripts\adsutil.vbs set w3svc/[식별자]/SecureBindings ":443:[호스트 헤더 값]"

[참고] 작업 진행하시기 전에 메모장에 위 명령어를 복사하셔서 적용하실 사이트들과 식별자를 입력 후  
복사하셔서 cmd창에서 한 번에 적용하시는 것을 추천드립니다.

예)

cscript.exe C:\inetpub\AdminScripts\adsutil.vbs set w3svc/1489029442/SecureBindings ":443:sso.ucert.co.kr"

cscript.exe C:\inetpub\AdminScripts\adsutil.vbs set w3svc/1359436333/SecureBindings ":443:dev.ucert.co.kr"

C:\Documents and Settings\Ucert>cd W

C:\W>cscript.exe C:\inetpub\AdminScripts\adsutil.vbs set w3svc/1489029442/SecureBindings  
":443:sso.ucert.co.kr"

Microsoft (R) Windows Script Host 버전 5.6

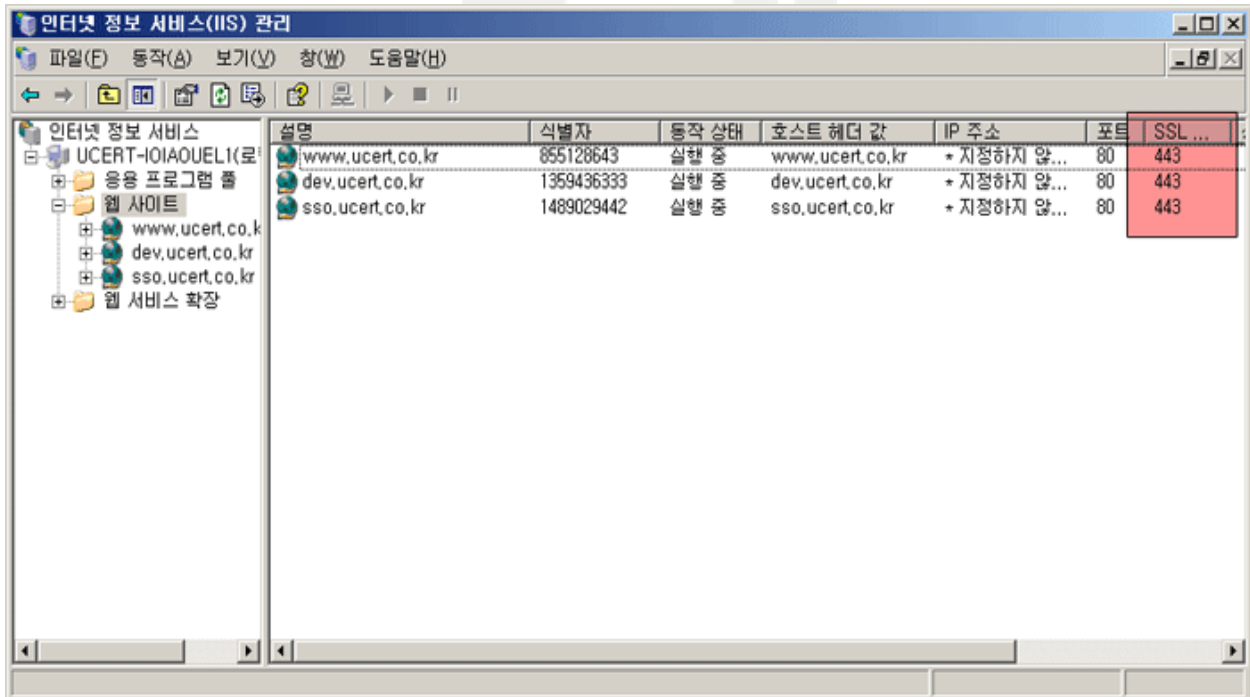
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

SecureBindings : (LIST) ":443:sso.ucert.co.kr"

C:\W>cscript.exe C:\inetpub\AdminScripts\adsutil.vbs set w3svc/1359436333/SecureBindings  
":443:dev.ucert.co.kr"

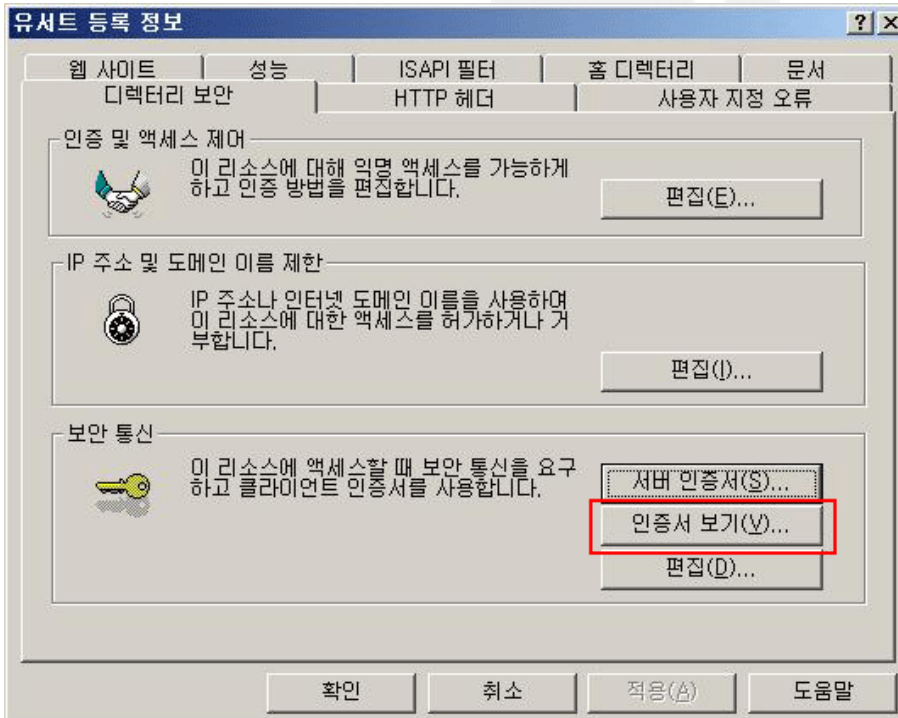
Microsoft (R) Windows Script Host 버전 5.6  
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.  
SecureBindings : (LIST) ":443:dev.ucert.co.kr"

3) IIS에서 웹사이트 선택 후 새로 고침하여 중복 포트 설정이 됐는지 확인 합니다.

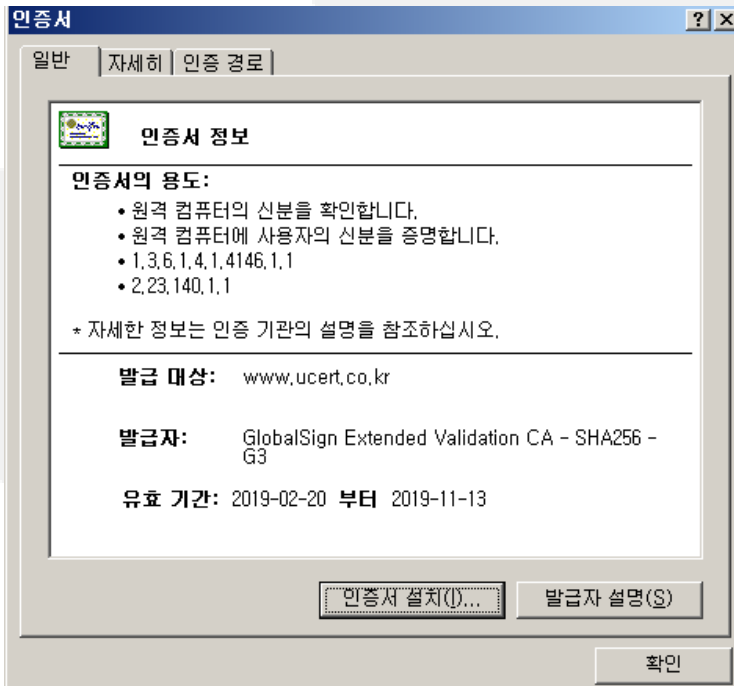


#### 4. 인증서 확인

1). "디렉터리 보안 탭에서 "인증서 보기"를 클릭 합니다.



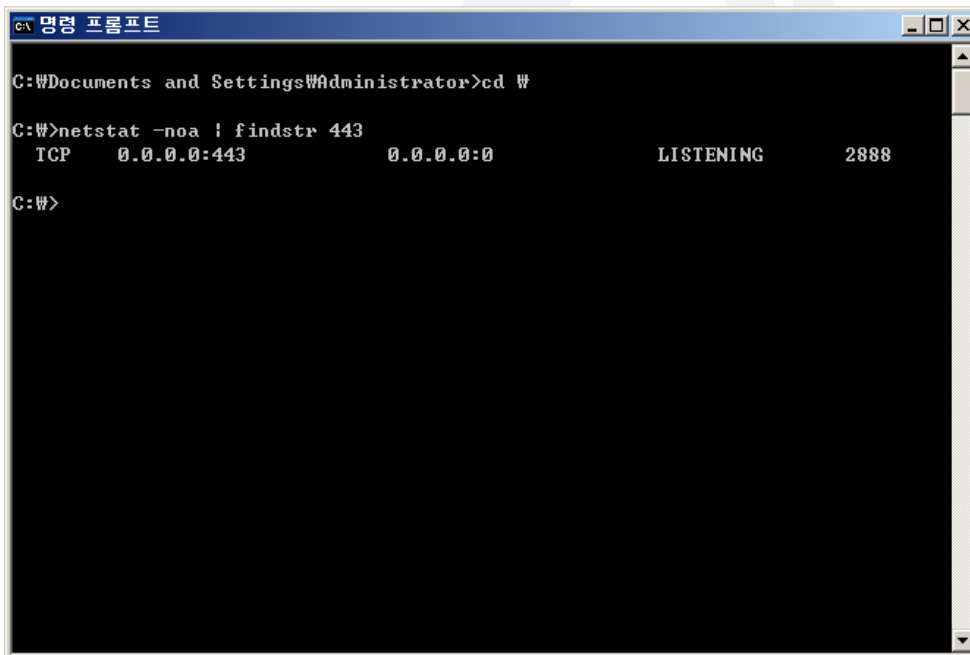
2). 발급 대상과 유효기간이 올바른지 확인 합니다.



3). 지정한 SSL 포트를 확인 합니다.

- cmd 실행 후 **netstat -noa | findstr 443**

명령어로 인증서를 설치 한 포트가 Listen 상태인지 확인 합니다.



```
C:\Documents and Settings\Administrator>cd W

C:\W>netstat -noa | findstr 443
TCP      0.0.0.0:443          0.0.0.0:0           LISTENING      2888

C:\W>
```

- 내/외부 방화벽에 SSL포트(기본443)가 비활성화 상태일 경우 SSL포트(기본443)를 활성화 합니다.

\* 웹 방화벽이 있을 경우 ucert@ucert.co.kr로 웹 방화벽용 인증서를 신청하여 발급 받으신 후 웹 방화벽에 인증서를 설치 합니다.

- 외부에서 웹 브라우저로 [https://\[해당도메인\]:\[SSL포트\]](https://[해당도메인]:[SSL포트]) 로 접속하여 SSL포트가 열려있는지 확인합니다.

예:) <https://www.ucert.co.kr> or <https://www.korsec.co.kr:444>

4) 웹페이지에서 인증서 확인을 합니다.

익스플로러 확인 방법 <https://www.ucert.co.kr> 접속 예

도메인 접속 후에 Alt 키를 누르고  
파일 → 속성 → 인증서  
클릭 후 인증서 보기를 선택하시면  
인증서정보를 확인 할 수 있습니다.

발급 대상 과 유효 기간이 맞는지  
확인합니다.

속성

일반

UCERT

프로토콜: HyperText Transfer Protocol with Privacy

유형: Chrome HTML Document

연결: TLS 1.2, AES - 256비트 암호화 (높음); DH - 1024비트 교환

영역: 인터넷 | 보호 모드: 설정

주소 (URL): <https://www.ucert.co.kr/>

크기: 알 수 없음

만든 날짜: 2016-06-02

수정된 날짜: 2016-06-02

인증서(C)

확인 취소 적용(A)

인증서 정보

인증서의 용도:

- 원격 컴퓨터의 신분을 확인합니다.

• 자세한 정보는 인증 기관의 설명을 참조하십시오.

발급 대상: www.ucert.co.kr

발급자: GlobalSign Extended Validation CA - SHA256 - G2

유효 기간: 2015- 11- 09 부터 2016- 08- 12

발급자 설명(S)

인증서에 대해 자세히 알아보십시오.

확인