

POSTECH 보안서버(SSL 인증서)

변경 가이드

- 상용 SSL 인증서 변경 -

2013. 10

학술정보처 정보기술지원팀

<차례>

- I. Apache 서버에서 SSL 보안서버 변경하기
- II. Apache Win 서버에서 SSL 보안서버 변경하기
- III. Tomcat 서버에서 SSL 보안서버 변경하기
- IV. IIS 5.1 SSL 인증서 변경하기
- V. IIS 7.0 및 7.5 SSL 인증서 변경하기

※ 본 가이드는 교육부 SSL 인증서에서 상용 SSL 인증서로 변경하는 가이드임.

I. Apache 서버에서 SSL 인증서 변경하기

[인증서 변경하기]

기존에 설치되어 있는 인증서 파일 중 루트 인증서를 제외하고 해당 파일 교체

1. 인증서 파일을 교체 3 개파일)

- 1) SSL 인증서 : postech.crt → thawte_postech.cer 로 변경
- 2) 개인키 : postech.key → thawte_postech_key.pem 으로 변경
- 3) 체인인증서 : caChain.crt → thawte_Chain.cer 로 변경
- 4) 루트인증서 : rootca.crt → 파일 삭제

2. ssl.conf 파일에서 루트인증서 설정 주석처리

```
# Server Certificate:보안서버 인증서 설정
SSLCertificateFile /etc/httpd/conf/cert/thawte_postech.cer
# Server Private Key:보안서버 인증서 개인키 설정
SSLCertificateKeyFile /etc/httpd/conf/cert/thawte_postech_key.pem
# Server Certificate Chain:체인 인증서 설정
SSLCertificateChainFile /etc/httpd/conf/cert/thawte_Chain.cer
# Certificate Authority (CA):최상위 인증기관(루트 인증서) 인증서 설정
#SSLCACertificateFile /etc/httpd/conf/cert/rootca.crt
```

※ 상용 SSL 인증서의 루트인증서는 기본적으로 탑재되어 있음

3. 웹서버 재구동

II. Apache Win 서버에서 SSL 인증서 변경하기

[인증서 변경하기]

기존에 설치되어 있는 인증서 파일 중 루트 인증서를 제외하고 해당 파일 교체

1. 인증서 파일을 교체(3 개파일)

- 1) SSL 인증서 : postech.crt → thawte_postech.cer 로 변경
- 2) 개인키 : postech.key → thawte_postech_key.pem 으로 변경
- 3) 체인인증서 : caChain.crt → thawte_Chain.cer 로 변경
- 4) 루트인증서 : rootca.crt → 파일 삭제

2. httpd-ssl.conf 파일에서 루트인증서 설정 주석처리

나머지 파일은 경로 및 파일명에 맞게 수정

```

# General setup for the virtual host
DocumentRoot (http 설정과 동일한 디렉토리)
ServerName (인증서 적용 도메인)
ServerAdmin root@(domain)
ErrorLog "C:/Apache2.2/logs/error.log"
TransferLog "C:/Apache2.2/logs/access.log"
.....
SSLCertificateFile /(인증서 저장 경로)/(인증서 파일명)
.....
SSLCertificateKeyFile /(개인키 저장 경로)/(개인키 파일명)
.....
SSLCertificateChainFile /(저장경로)/(중개인증서 파일명)
.....
#SSLCACertificateFile /(저장경로)/(루트인증서 파일명)
.....
</VirtualHost>

```

3. 웹서버 재구동

III. Tomcat 서버에서 SSL 인증서 변경하기

[인증서 변경하기]

기존에 설치되어 있는 상태에서 keystore 파일 교체와 keystorePass 변경하면됨

1. 인증서 파일을 서버의 적절한 위치에 저장

가. Thawte_postech.jks → Java keytool 로 SSL 인증서, 개인키, 체인, 루트 인증서를 합쳐놓은 파일

나. keystorePass="00100243" 으로 변경

2. 웹서버 설정 변경

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
```

아래부분내용 ==> 주석해제 및 수정

```

<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
    maxThreads="150" scheme="https" secure="true"
    keystoreFile="/usr/local/tomcat/conf/ssl/thawte_postech.jks"(파일 저장경로)
    keystorePass="00100243"
    clientAuth="false" sslProtocol="TLS" />

```

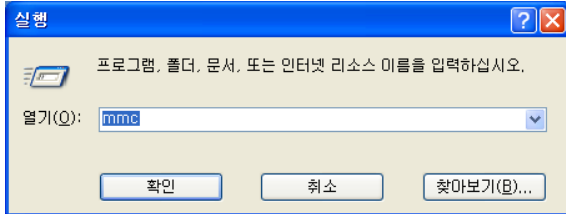
3. 웹서버 재구동

IV. IIS 5.1 SSL 인증서 변경하기

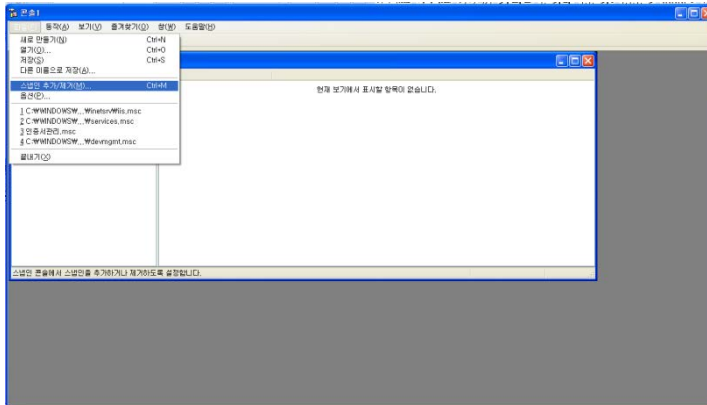
윈도우 인증서 항목에 상용 SSL 인증서를 가져오기하여 운영중인 홈페이지에 적용하면 됨(thawte_postech.pfx 파일을 가져와서 설치)

[SSL 인증서 가져오기]

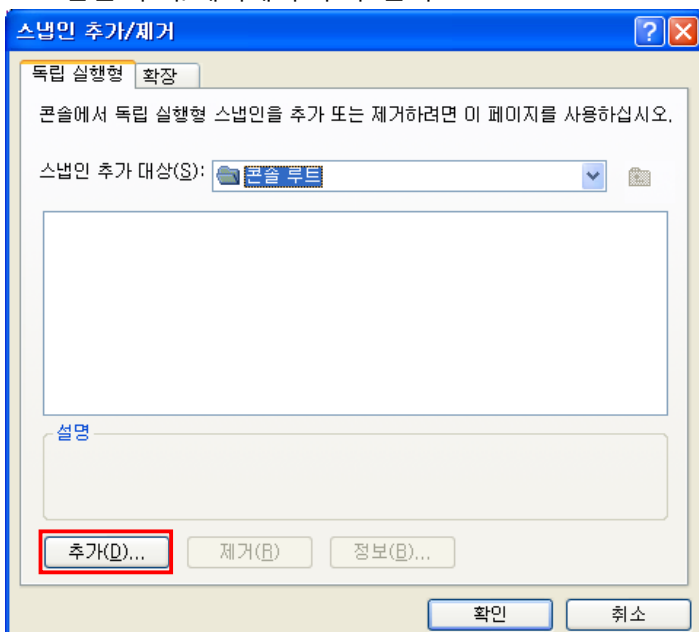
1. 시작->실행->윈도우관리자 콘솔(mmc) 실행



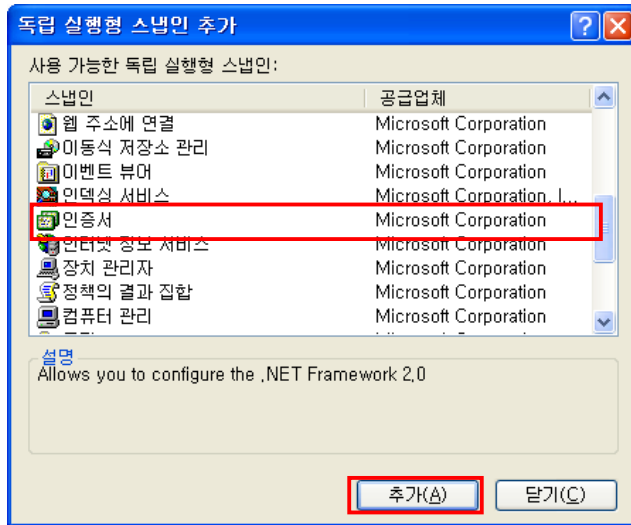
2. 콘솔창이 열리면 파일 -> 스냅인 추가/제거 선택



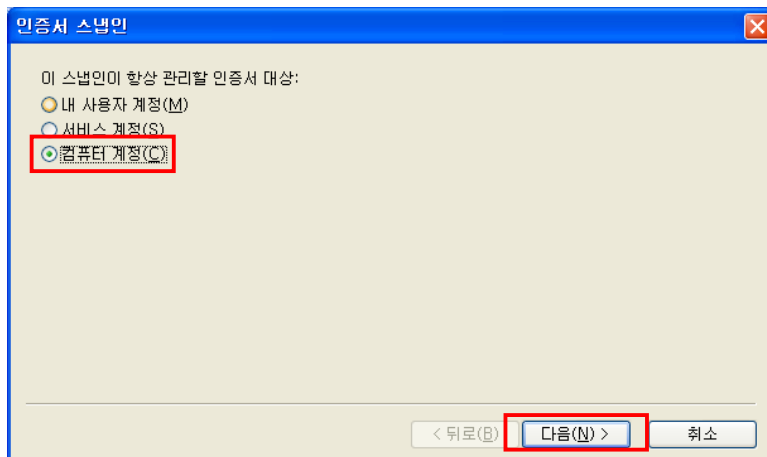
3. 스냅인 추가/제거에서 추가 클릭



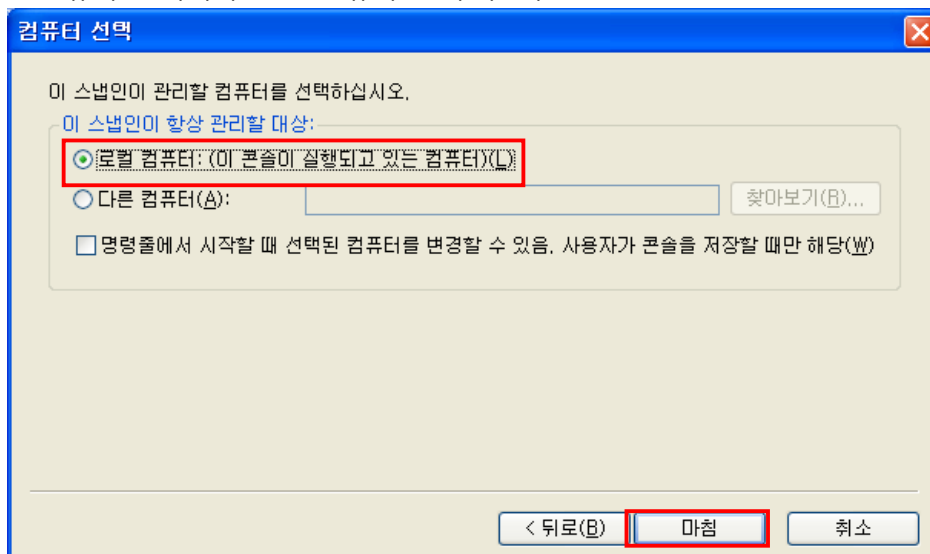
4. 독립 실행형 스냅인 추가에서 인증서 추가



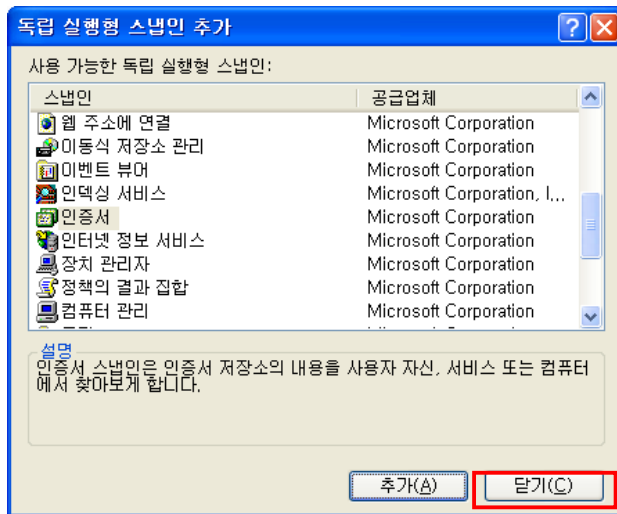
5. 인증서 스냅인에서 컴퓨터 계정 선택



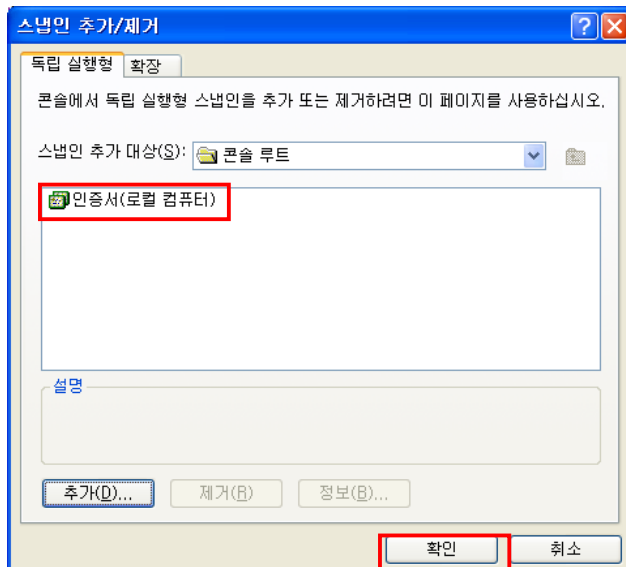
6. 컴퓨터 선택에서 로컬 컴퓨터 선택 후 마침



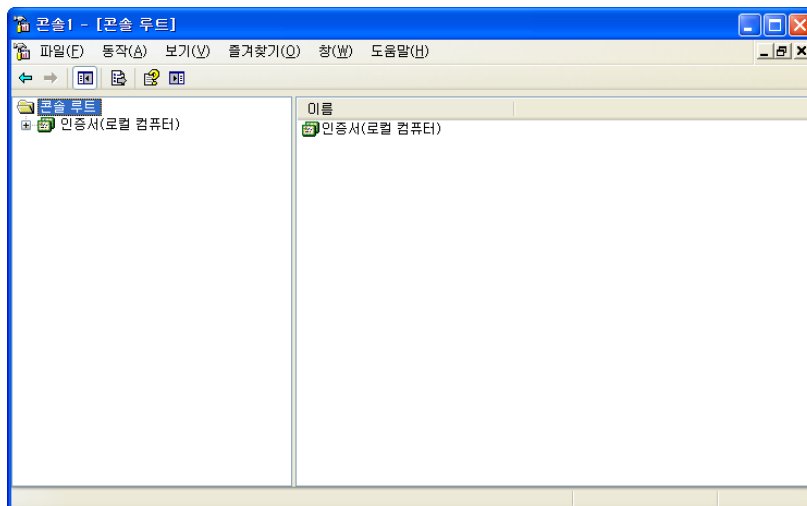
7. 독립 실행형 스냅인 추가에서 닫기 클릭



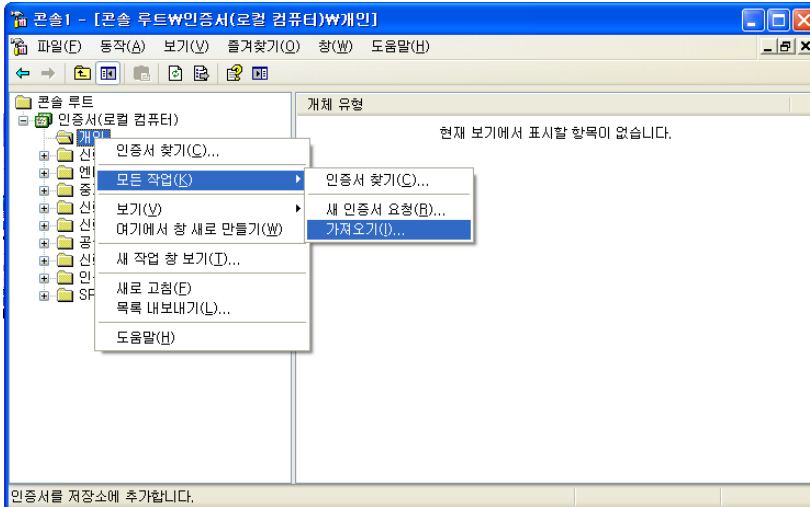
8. 스냅인 추가/제거에서 인증서 항목이 추가된 것을 확인 후 확인 클릭



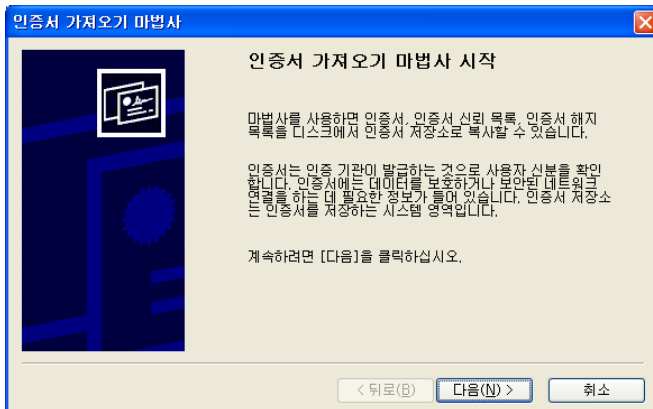
9. 콘솔창에서 인증서 항목이 추가된 것을 확인



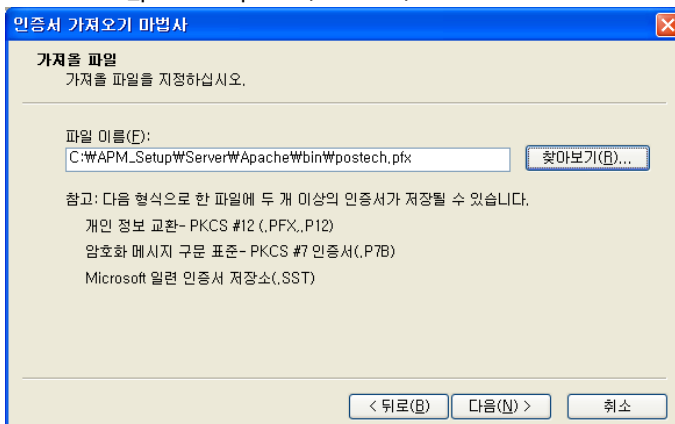
10. 콘솔 루트 -> 인증서 -> 개인 항목에서 마우스 오른쪽 클릭, 모든 작업 -> 가져오기 선택



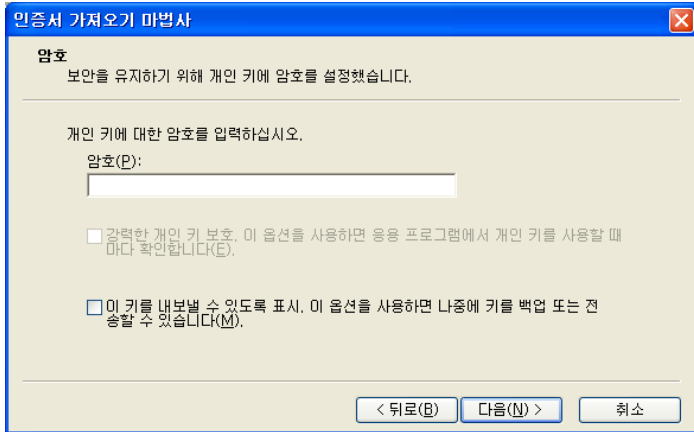
11. 다음 클릭



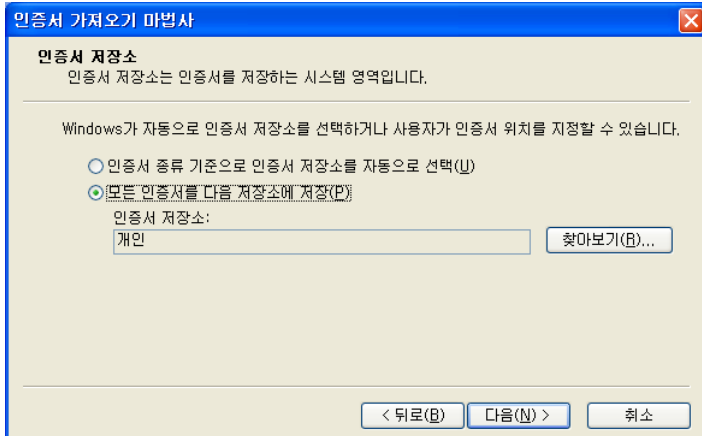
12. thawte_postech.pfx 파일 선택



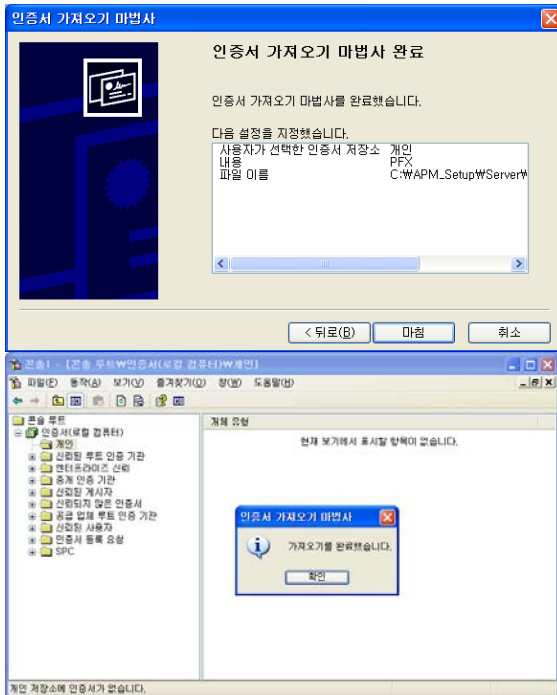
13. 개인키에 대한 암호 입력(암호 : 00100243) 후 다음 클릭



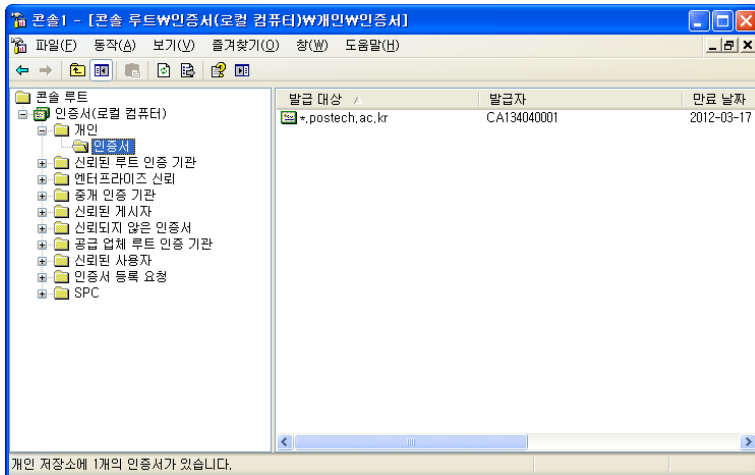
14. 모든 인증서를 다음 저장소에 저장 선택 후 다음 클릭



15. 마침 클릭하여 가져오기 완료

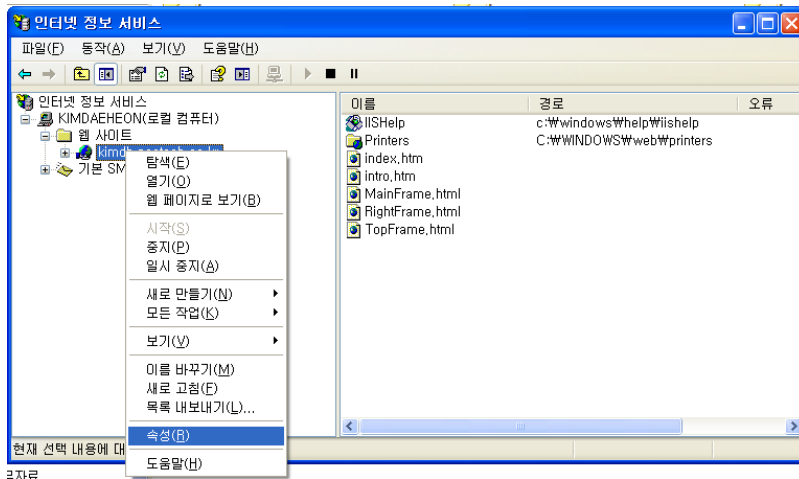


16. *.postech.ac.kr 상용인증서(발급자:thatwe)가 설치되어 있는지 확인

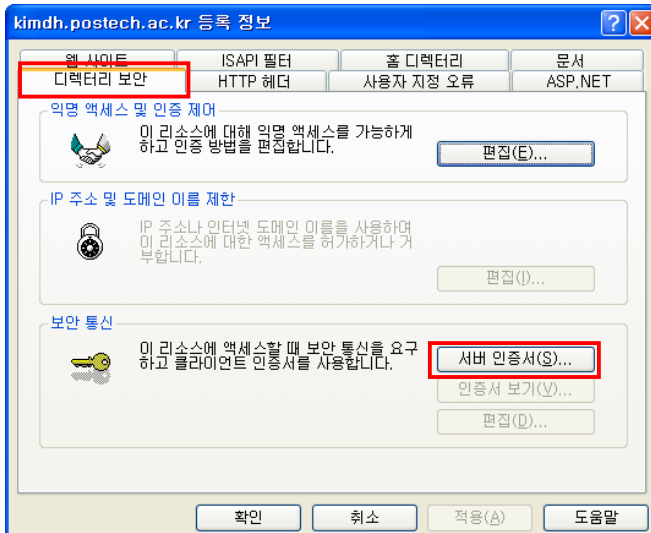


[인증서 설치 후 웹사이트에 적용]

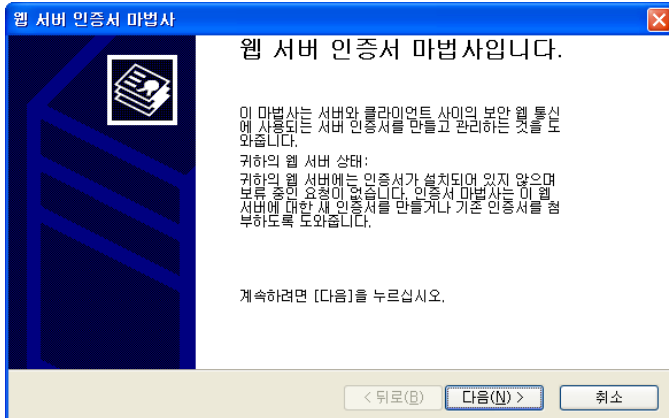
1. 인터넷 정보 서비스 실행(IIS) 후 해당 웹사이트 선택 후 마우스 오른쪽 클릭하여 속성 선택



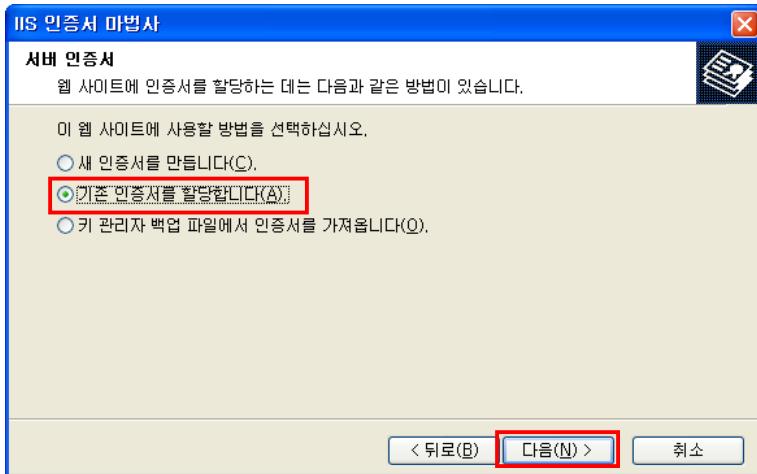
2. 등록정보에서 디렉터리 보안 탭에서 서버 인증서 클릭



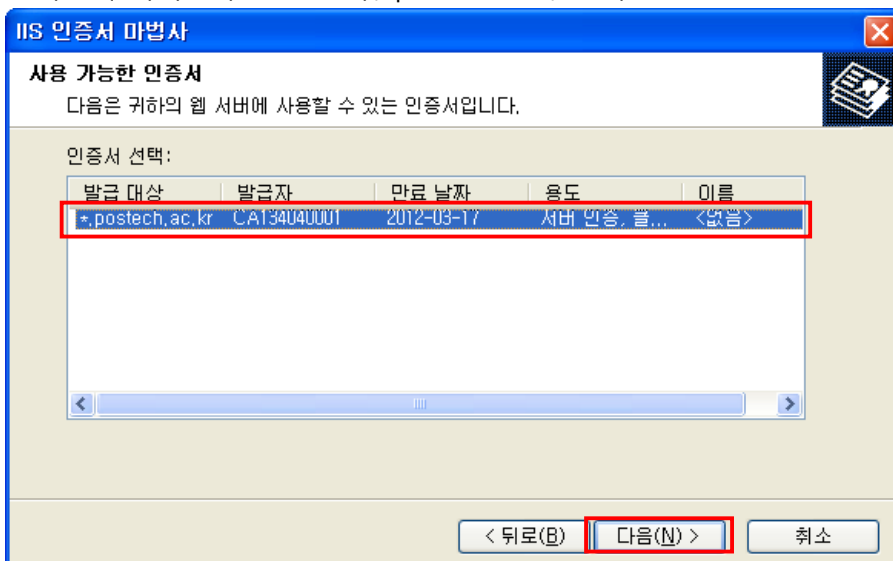
3. 웹 서버 인증서 마법사에서 다음 클릭



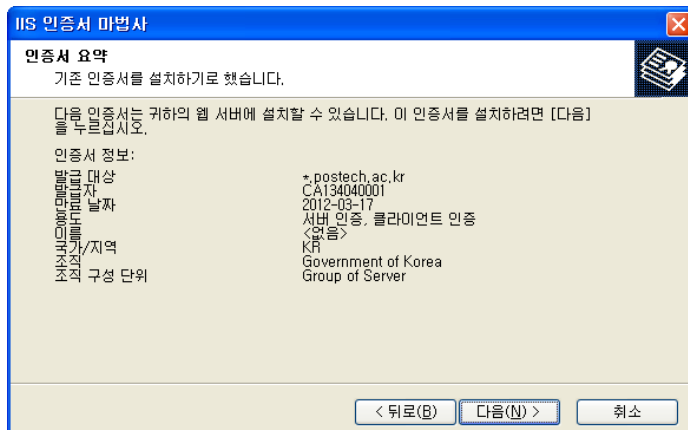
4. IIS 인증서 마법사에서 '기존 인증서를 할당합니다.' 선택 후 다음 클릭



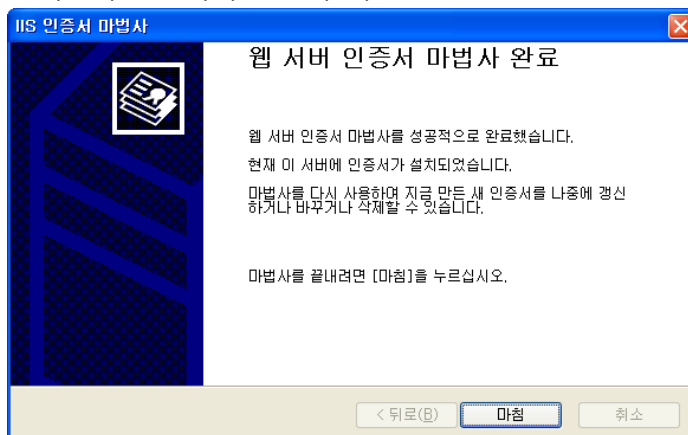
5. 사전에 가져오기 한 인증서(*.postech.ac.kr) 선택



6. 다음 클릭



7. 마법사 완료하여 인증서 적용 완료

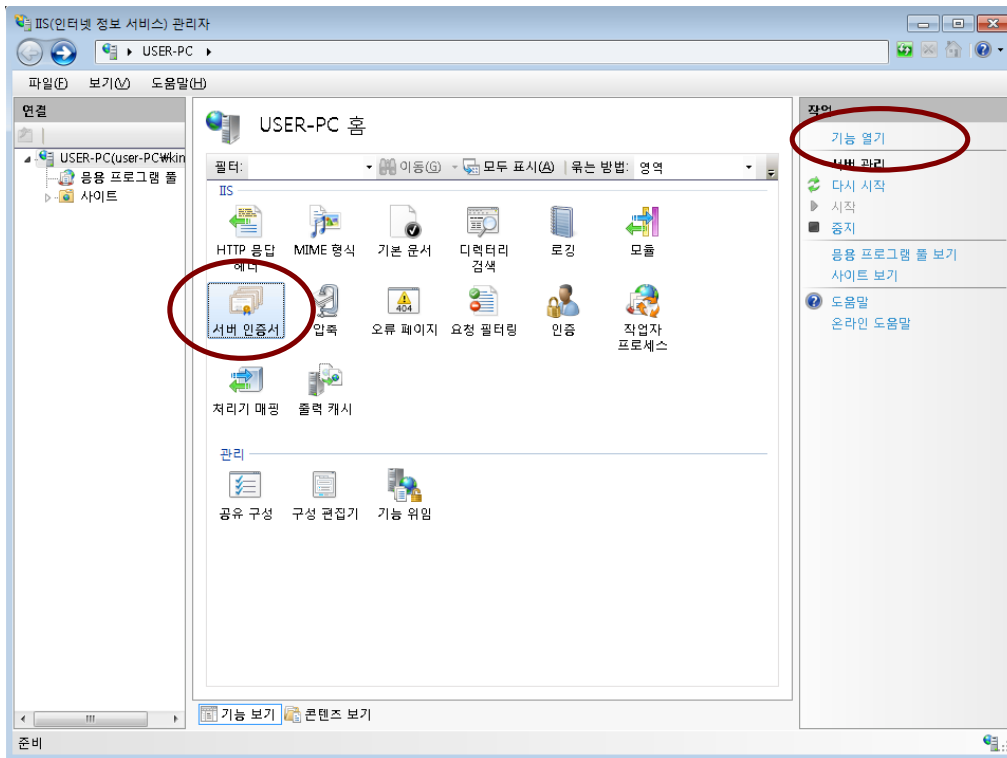


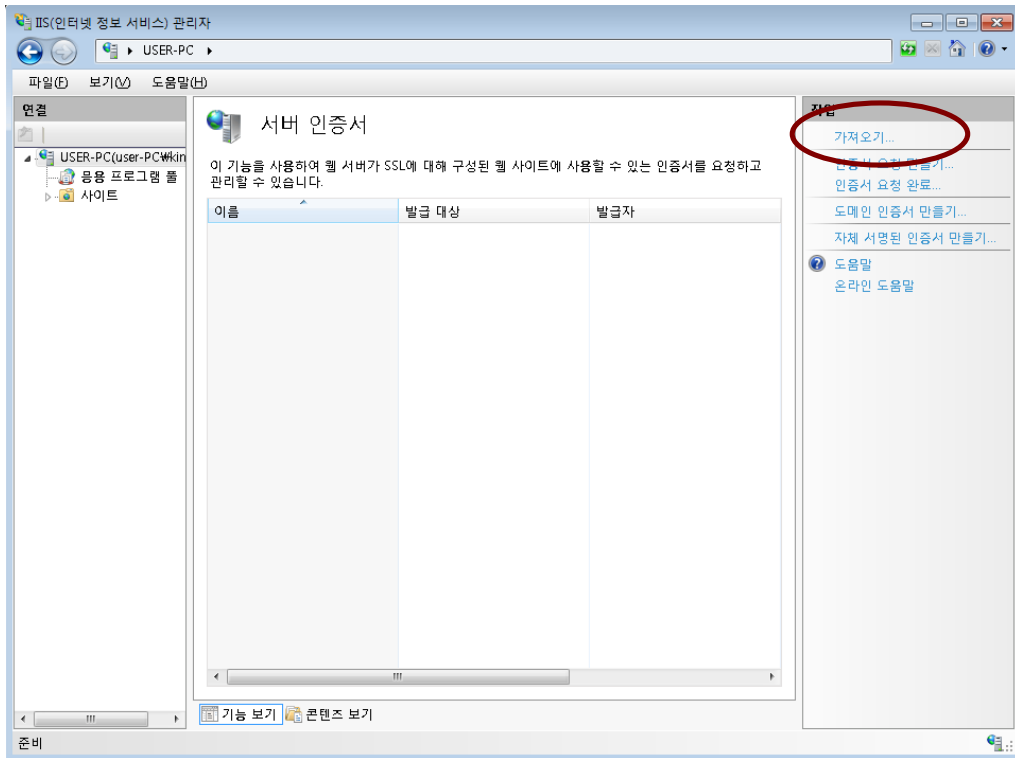
V. IIS 7.0 및 7.5 SSL 인증서 변경하기

윈도우 인증서 항목에 상용 SSL 인증서를 가져오기하여 운영중인 홈페이지에 적용하면 됨(thawte_postech.pfx 파일을 가져와서 설치)

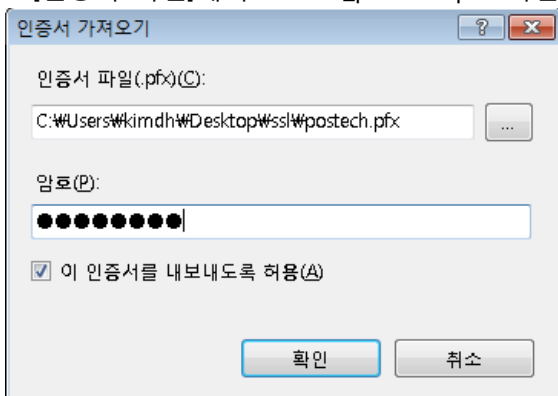
[SSL 인증서 가져오기]

1. [관리도구]→[IIS(인터넷 정보 서비스) 관리자]→[서버 인증서]→우측 작업 탭에서 기능열기→가져오기



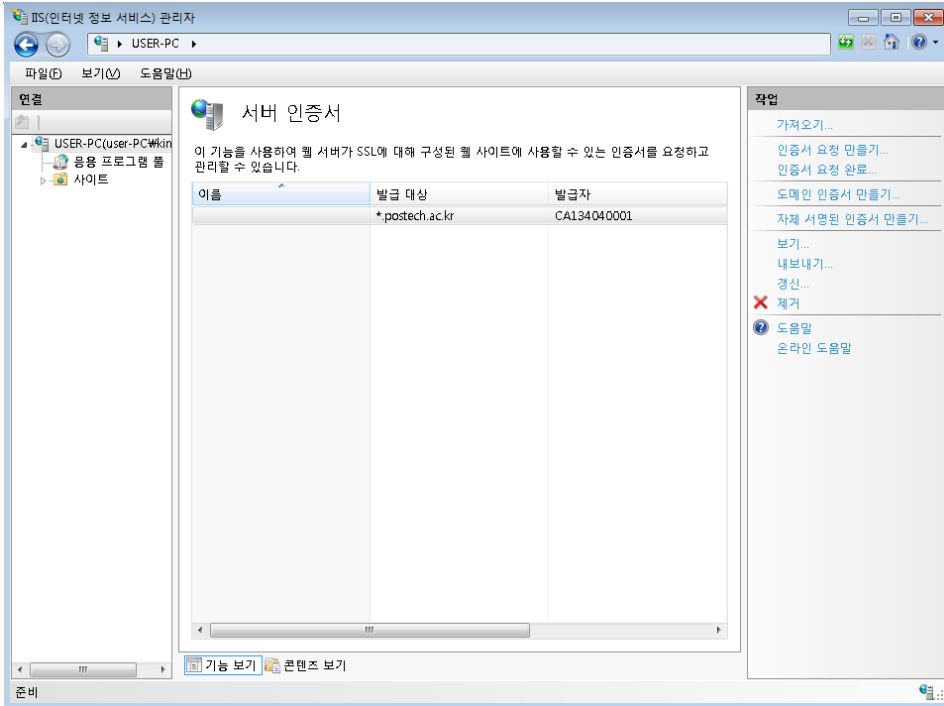


2. [인증서 파일]에서 thawte_postech.pfx 파일 가져오기(암호:00100243)



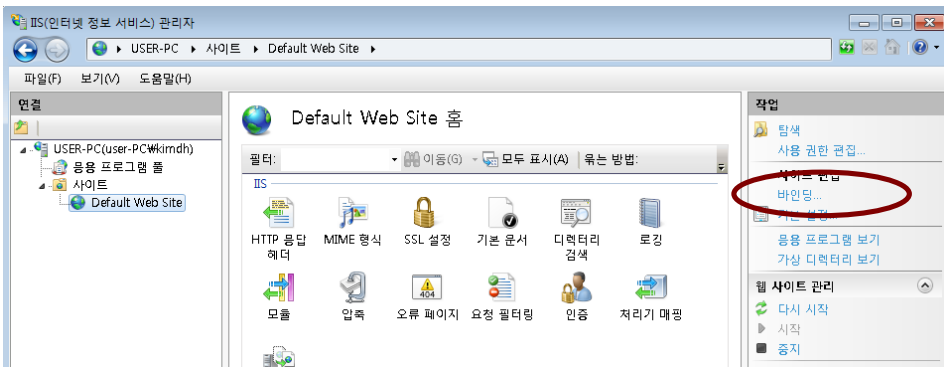
3. 인증서 가져오기 완료

- 발급자가 thawte 로 되어 있는 인증서 확인

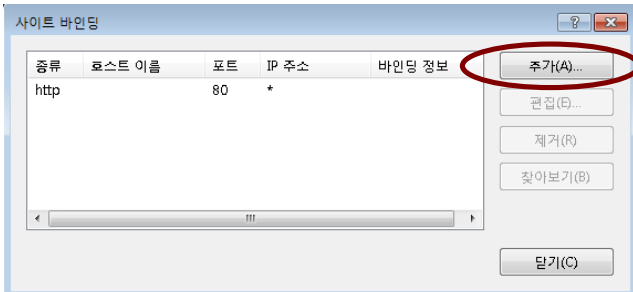


[인증서 설치 후 웹사이트에 적용]

1. [해당 웹사이트 선택] → 우측 작업 탭에서 바인딩 선택



2. 사이트 바인딩 추가



3. 종류 : https, SSL 인증서 : *.postech.ac.kr(발급자 thawte) 선택

사이트 바인딩 추가

종류(T): IP 주소(I): 포트(O):

호스트 이름(H):

SSL 인증서(S):

4. 인증서 적용 완료

사이트 바인딩

종류	호스트 이름	포트	IP 주소	바인딩 정보
http		80	*	
https		443	*	

/종료/