POSTECH 보안서버(SSL 인증서)
구축 가이드

2022. 06

학술정보처 정보시스템팀

제•개정 이력

2010. 10 월 제정	구축 가이드 제정
2012. 03 월 개정	인증서 갱신 내역 추가
2013. 11 월 개정	상용인증서 설치 내역 추가
2022. 06 월 개정	교육부 인증서 설치 내용 삭제
	최신 WAS 적용 내용 업데이트

<차례>

I. 보안서버 구축 개요

1. 추진목적

- 개인정보를 취급하는 정보시스템에 대한 보안서버 구축 및 적용확대를 통하여 건전하고 안전한 교육 사이버 환경 조성
- 교육기관에 대한 SSL 인증서 기반 보안서버 구축을 통하여 개인정보유출 방지 및 경쟁력 강화

※ 보안서버(SSL 인증서 기반) 정의

인터넷상에서 사용자 PC 와 웹서버 사이에 송/수신되는 개인정보를 암호화하여 전송하는 표준 보안기술로서, 개인정보를 암호화하여 전송함으로써 해킹 시에도 개인정보가 안전하게 보호됨

2. 관련근거

- 개인정보보호법, 교육부 정보보안 기본지침

3. 구축대상

- 교내 서버로 등록된 대상 중 개인정보를 취급하는 웹 서버

※ 구축 가능 웹 서버 : IIS, Apache, Tomcat, SunOne, WebtoB, Weblogic, IBM, Oracle-HTTP

II. 보안서버 구축 시 주의사항

1. SSL 인증서 적용 범위 설정

   SSL 인증서를 홈페이지 전체에 적용할지 일부에만 적용할지를 고려해야 함

   - 전체 적용 시
     . 전체 페이지를 암호화하여 통신하므로 사용자가 많을 시 서버 과부하 발생
     . 사용자가 적을 경우 서버 설정을 통해 간단하게 적용 가능
   - 부분 적용 시
     . 회원가입 페이지, 로그인 프로세스, 회원정보 수정 부분에만 적용
     . 사용자가 많아도 서버 과부하가 발생하지 않지만 소스코드 수정이 필요

   연구실 홈페이지의 경우 사용자가 많지 않을 것으로 보여 SSL 인증서를 홈페이지 전체에 적용하는 것을 권장 드립니다.(구축 가이드에 서버 설정 참조)

2. 무료게시판 이용 홈페이지

   PHP, ASP 등으로 만든 무료게시판을 이용하는 홈페이지에서 SSL 인증서를 적용하려면 게시판 설정 수정이 필요

3. 웹서버 최신 버전 유지

   교내 홈페이지의 개인정보를 보호하기 위해서는 웹서버의 보안 취약점 제거도 병행되어야 합니다. 웹서버의 최신 버전을 사용하면 우선적으로 취약한 일부 제거할 수 있습니다.

   - Apache, Tomcat, IIS 최신 버전으로 업데이트(OpenSSL 최신 업데이트 포함)
   - 제로보드 최신 버전으로 업데이트

   ※ 추후 웹서버 보안설정 가이드 제작하여 배포 예정

III. Apache SSL 인증서 설치

※ 사전 확인 사항 ※

인증서 설치시 SSL 관련 설정은 기존 apache 1.x 에서는 httpd.conf 파일에서 해주었으나 Apache 2.x 에서는 ssl.conf, apache 2.2x 에서는 httpd-ssl.conf 파일에서 설정해 주시면 됩니다.

참고 1. Apache 의 경우 기본적으로 mod_ssl 모듈이 설치되어 있어야 합니다.
참고 2. Windows 계열의 경우 설치방법이 상이할 수 있으니 참고하시기 바랍니다.

처음 Apache 설치(compile)시 mod-ssl 의 활성화를 위해서 (--enable-ssl)를 추가시켜줘야 합니다.

Mod_SSL 설치 확인($ /usr/local/apache/bin/httpd –l)

```
[root@168 bin]# ./httpd -l
Compiled in modules:
  core.c
  mod_access.c
  mod_auth.c
  mod_include.c
  mod_log_config.c
  mod_env.c
  mod_setenvif.c
  mod_ssl.c
```

[인증서 설치하기]

1. 인증서 복사
   - **1) thawte_postech.pem ➔ SSL 인증서**
   - **2) thawte_postech_key.pem ➔ 개인키 (※ Passphrase: postech2022)**
   - **3) DigiCertCA.pem ➔ 체인인증서**

2. Apache 서버의 적절한 위치에 저장
   Ex) /etc/httpd/conf/cert/

3. 설정파일 수정(httpd.conf)
   설정파일을 열어서 다음과 같이 내용을 수정
   LoadModule ssl_module modules/mod_ssl.so --> SSL 모듈추가 (mod_ssl.c 가 없을 경우)
   Include conf/extra/httpd-ssl.conf --> SSL 설정파일을 include
   ** 주석처리가 되어 있다면 주석제거

4. 설정파일 수정(ssl.conf 또는 httpd-ssl.conf 수정)
   가. 설정파일을 열어서 다음과 같이 VirtualHost 의 내용을 수정
   - Apache 1.x 는 httpd.conf

- Apache 2.0 은 ssl.conf
- Apache 2.2 이상은 httpd-ssl.conf
- Apache 2.4 는 httpd-ssl.conf

** Tomcat, Weblogic 등의 WAS 연동시 해당 Module 부분을 추가 설정

```
Listen 443
NameVirtualHost IP:443

<VirtualHost IP:443>
DocumentRoot "/xxx/1.html"
ServerName www.test.co.kr
ServerAdmin admin@test.co.kr
SSLEngine on

SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite HIGH:MEDIUM:!SSLv2:!PSK:!SRP:!ADH:!AECDH

SSLCertificateFile /usr/local/apache/conf/ssl/ thawte_postech.pem          (인증서파일)
SSLCertificateKeyFile /usr/local/apache/conf/ssl/ thawte_postech_key.pem (키파일)
SSLCertificateChainFile /usr/local/apache/conf/ssl/ DigiCertCA.pem        (체인인증서파일)

<VirtualHost IP:443>
DocumentRoot "/xxx/2.html"
ServerName login.test.co.kr
ServerAdmin admin@abc.co.kr
SSLEngine on

SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite HIGH:MEDIUM:!SSLv2:!PSK:!SRP:!ADH:!AECDH

SSLCertificateFile /usr/local/apache/conf/ssl/ thawte_postech.pem          (인증서파일)
SSLCertificateKeyFile /usr/local/apache/conf/ssl/ thawte_postech_key.pem (키파일)
SSLCertificateChainFile /usr/local/apache/conf/ssl/ DigiCertCA.pem        (체인인증서파일)
```

5. 웹 서버 재구동

```
[root@tmp-web conf]# service httpd restart
httpd 를 정지함:                                           [  확인  ]
httpd (을)를 시작합니다: Apache/2.0.52 mod_ssl/2.0.52 (Pass Phrase Dialog)
Some of your private key files are encrypted for security reasons.
In order to read them you have to provide the pass phrases.

Server cee.postech.ac.kr:443 (RSA)
Enter pass phrase:

OK: Pass Phrase Dialog successful.
                                                           [  확인  ]
[root@tmp-web conf]# _
```

➔ Enter pass phrase: postech2022

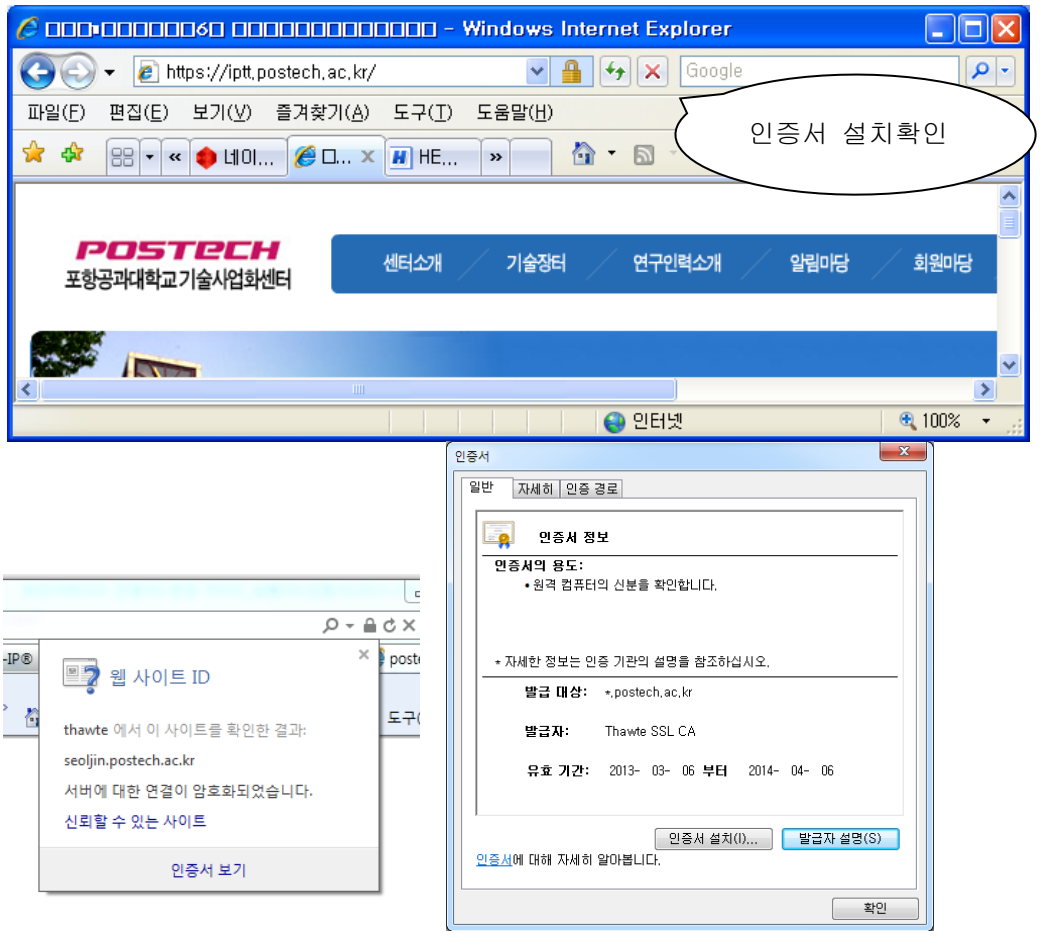
6. 인증서 설치 확인

가. 인증서 Port LISTEN 확인

```
[root@168 bin]# netstat -na | grep 443
tcp        0      0 :::443                      :::*                        LISTEN

unix  3      [ ]         STREAM     CONNECTED     543443 /tmp/orbit-root/linc-ca4-0-67
4efd6510ec
[root@168 bin]# netstat -na | grep 444
tcp        0      0 :::444                      :::*                        LISTEN
```

나. 웹페이지에서 인증서 설치 확인



7. 패스워드 수동입력 없이 웹 서비스 자동 실행하기

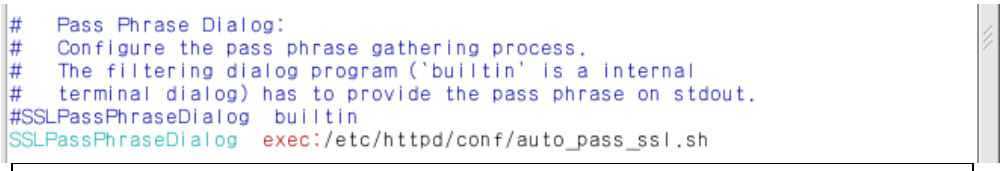
- SHELL 을 통한 키값 출력프로그램 작성

```
# vi auto_pass_ssl.sh
#!/bin/sh
 echo 'postech2022'
```

- 해당 프로그램 실행모드로 전환

  # chmod 755 auto_pass_ssl.sh

- ssl.conf 파일 수정




```
SSLPassPhraseDialog    exec:/etc/httpd/conf/auto_pass_ssl.sh
```

※ SSL 암호화 설정

인증서를 설치하고 나면 http 와 https 로의 접속이 모두 가능합니다. http 로의 접속을 계속 허용할 경우 SSL 인증서를 설치한 효과가 없습니다. 그러나, 일반 사용자 대부분이 http 로 접속을 하기 때문에 http 로의 접속을 차단하는 대신 https 로 전환시켜 주어야 합니다.

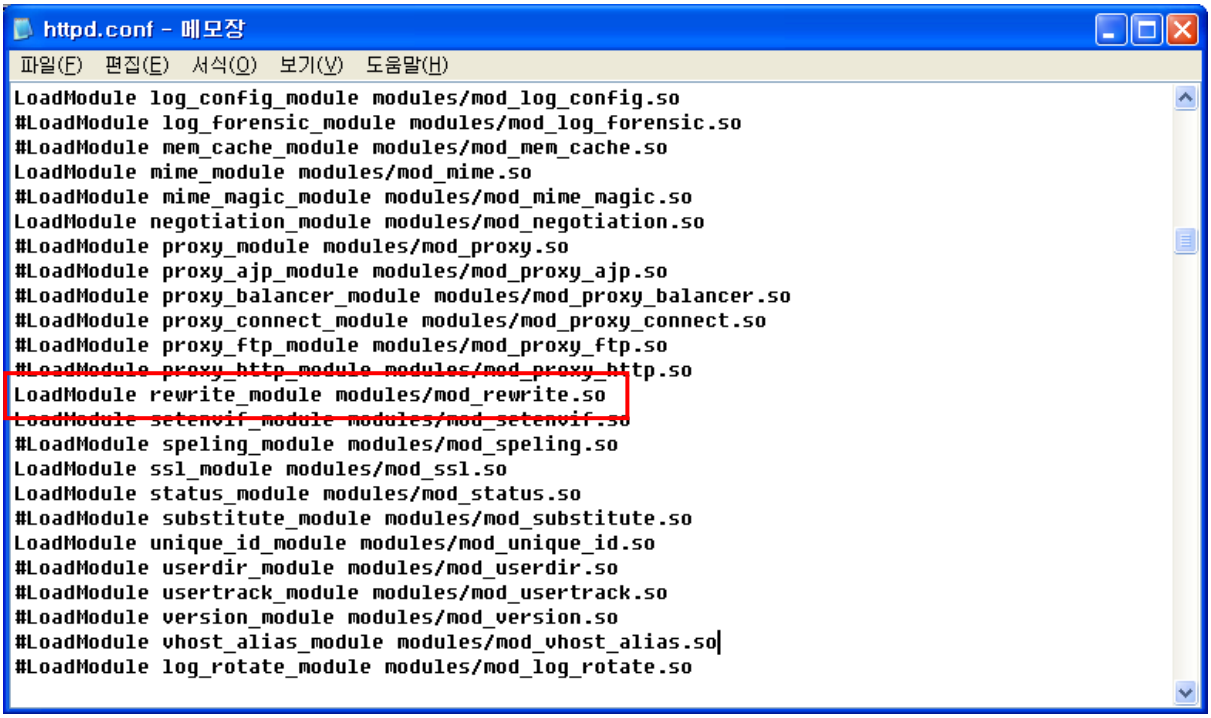
[http → https 전환하기]

1. Apache 서버의 경우 rewrite 모듈을 이용하여 전환

환경설정 파일 httpd.conf 에 다음 추가

```
    RewriteEngine On
    RewriteCond %{HTTPS} off
    RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
```

2. rewrite 모듈 주석 해제하여 활성화하기


httpd.conf - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
LoadModule log_config_module modules/mod_log_config.so
#LoadModule log_forensic_module modules/mod_log_forensic.so
#LoadModule mem_cache_module modules/mod_mem_cache.so
LoadModule mime_module modules/mod_mime.so
#LoadModule mime_magic_module modules/mod_mime_magic.so
LoadModule negotiation_module modules/mod_negotiation.so
#LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
#LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
#LoadModule proxy_connect_module modules/mod_proxy_connect.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
#LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule setenvif_module modules/mod_setenvif.so
#LoadModule speling_module modules/mod_speling.so
LoadModule ssl_module modules/mod_ssl.so
LoadModule status_module modules/mod_status.so
#LoadModule substitute_module modules/mod_substitute.so
LoadModule unique_id_module modules/mod_unique_id.so
#LoadModule userdir_module modules/mod_userdir.so
#LoadModule usertrack_module modules/mod_usertrack.so
#LoadModule version_module modules/mod_version.so
#LoadModule vhost_alias_module modules/mod_vhost_alias.so
#LoadModule log_rotate_module modules/mod_log_rotate.so

IV. Tomcat 서버에서 SSL 보안서버 구축하기

[웹서버 설정하기]

**** 본문서는 Tomcat(WAS) 단독으로 운영 시 적용 가능합니다.**

(Ex. Apache + Tomcat 연동의 경우 SSL 인증서는 Apache 쪽에 설치해 주시면 됩니다.)

1. 인증서 복사

   가. keystore ← Java keytool 로 SSL 인증서, 개인키, 체인, 루트 인증서를 합쳐놓은 파일

2. 서버의 적절한 위치에 저장

   Ex) /usr/local/tomcat/ssl/keystore

3. 환경설정파일 수정(server.xml)

   (Ex. /usr/local/tomcat/conf/server.xml)

- **Tomcat 5.x** 의 경우(Connector부분 주석처리 없애고 keystore파일과 패스워드 입력)

```
<Connector port="443" maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
           enableLookups="false" disableUploadTimeout="ture"
           acceptCount="100" debug="0" scheme="https" secure="true"
           keystoreFile="/path/keystore 파일명" keystorePass=" postech2022 "
           clientAuth="false" sslProtocol="TLS" />
</Connector>
```

- **Tomcat 6.x(7.x/8.0)**의 경우(Connect부분 주석처리 없애고 keystore파일과 패스워드 입력)

```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
           maxThreads="150" scheme="https" secure="true"
           keystoreFile="/path/keystore파일명" keystorePass=" postech2022 "
           clientAuth="false" sslProtocol="TLS" />
```

- **Tomcat 8.50이상**의 경우(Connect부분 주석처리 없애고 keystore파일과 패스워드 입력)

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
           maxThreads="150" SSLEnabled="true" >
    <SSLHostConfig>
        <Certificate certificateKeystoreFile="/path/keystore파일명"
                     certificateKeystorePassword=" postech2022"
                     certificateKeyAlias="alias명"  type="RSA" />
    </SSLHostConfig>
</Connector>
```

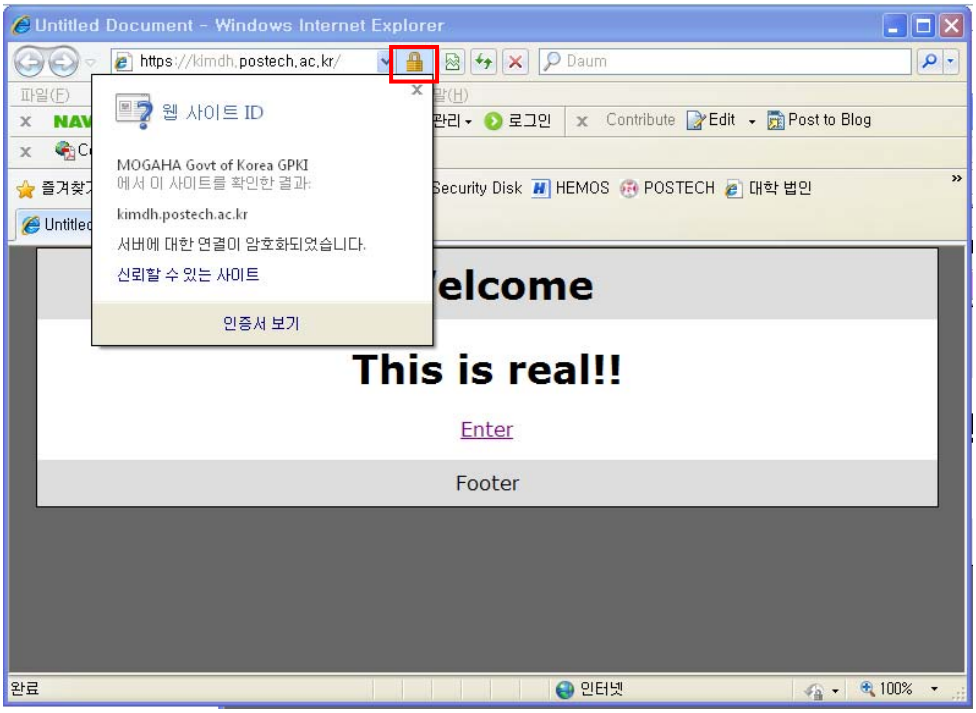
3. 웹서버 재구동

[인증서 설치 후 설치 확인]

1. 인증서 Port LISTEN 확인

```
[root@localhost bin]# netstat -na | grep 443
tcp        0      0 :::443                      :::*                        LISTEN
unix  2      [ ACC ]     STREAM     LISTENING     11443  /tmp/orbit-root/linc-d5e-0-dda64722ba08
[root@localhost bin]# netstat -na | grep 444
tcp        0      0 :::444                      :::*                        LISTEN
unix  2      [ ACC ]     STREAM     LISTENING     11840  /tmp/orbit-root/linc-d81-0-5389aaf1e6444
```

2. https:// 로 접근하여 웹페이지가 올바로 열리는지 확인하여 인증서 설치 확인



※ SSL 암호화 설정

인증서를 설치하고 나면 http 와 https 로의 접속이 모두 가능합니다. http 로의 접속을 계속 허용할 경우 SSL 인증서를 설치한 효과가 없습니다. 그러나, 일반 사용자 대부분이 http 로 접속을 하기 때문에 http 로의 접속을 차단하는 대신 https 로 전환시켜 주어야 합니다.

[Tomcat 서버 http → https 전환하기]

1. 아래의 <security-constraint> 항목을 <servlet-mapping> 항목 다음에 추가

```
<!-- SSL settings. only allow HTTPS access to Web -->

<security-constraint>
<web-resource-collection>
<web-resource-name>Entire Application</web-resource-name>
```

```
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

V. IIS SSL 인증서 설치

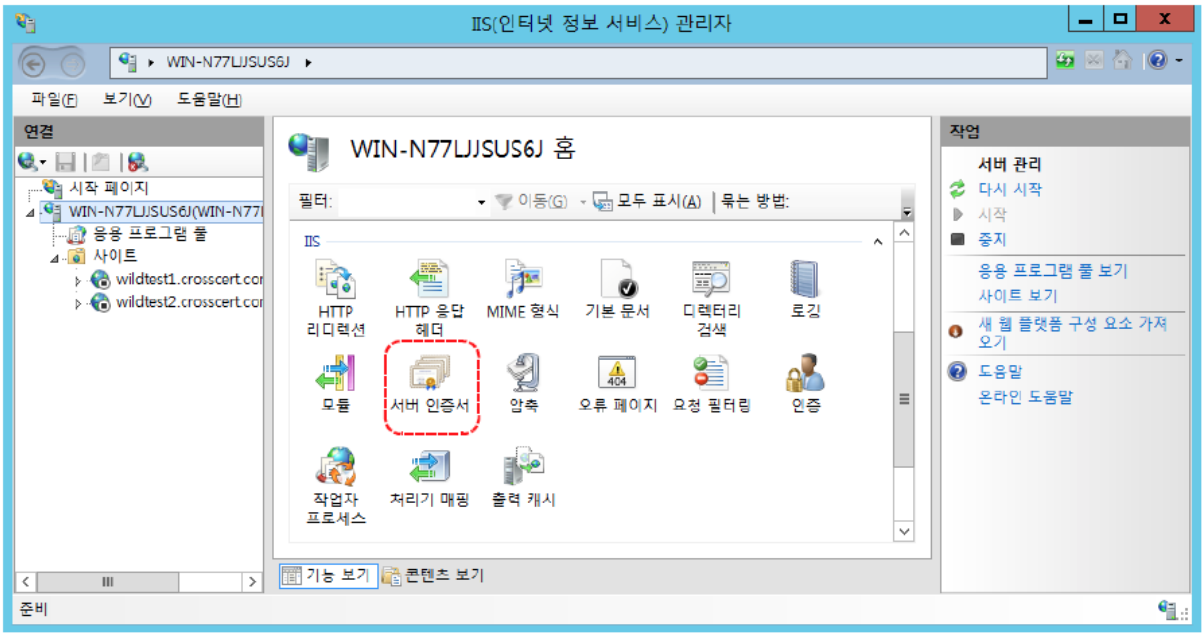
※ IIS 의 경우 인증서와 체인인증서 2 개를 설치하여야 함

thawte_postech.pfx → SSL 인증서 파일

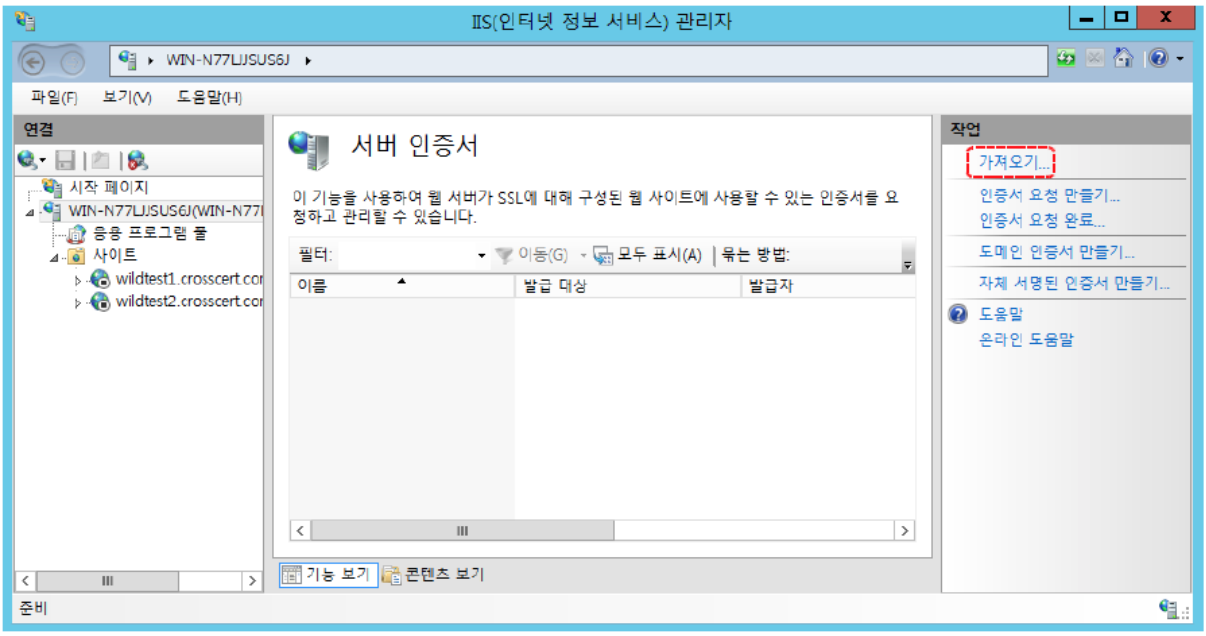
DigiCertCABundle.p7b → 체인인증서 파일

[SSL 인증서 설치하기]

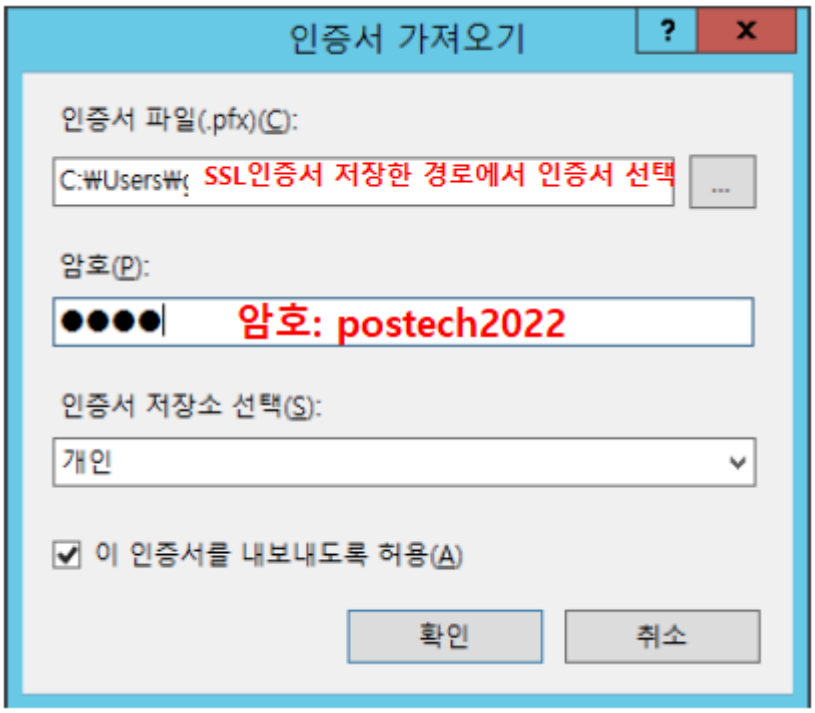
1. IIS(인터넷 정보 서비스)관리자 실행 후 '서버 인증서' 를 실행



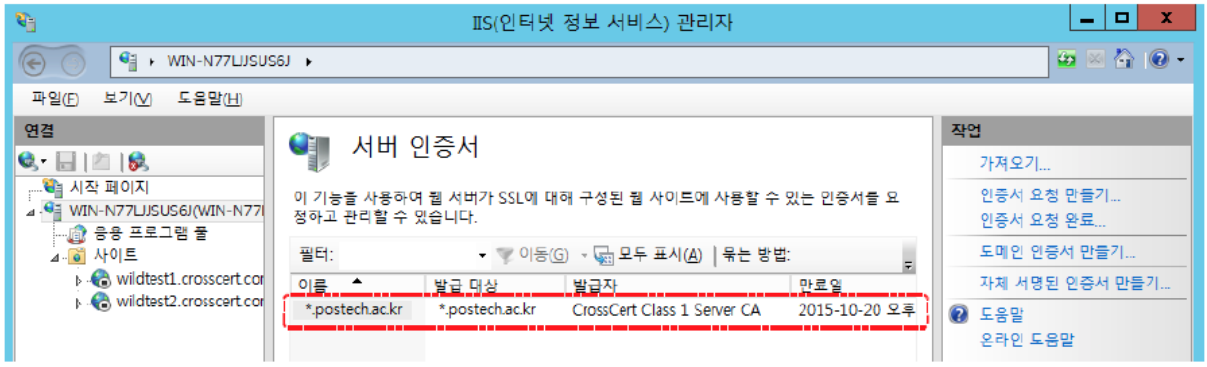
2. '가져오기' 클릭



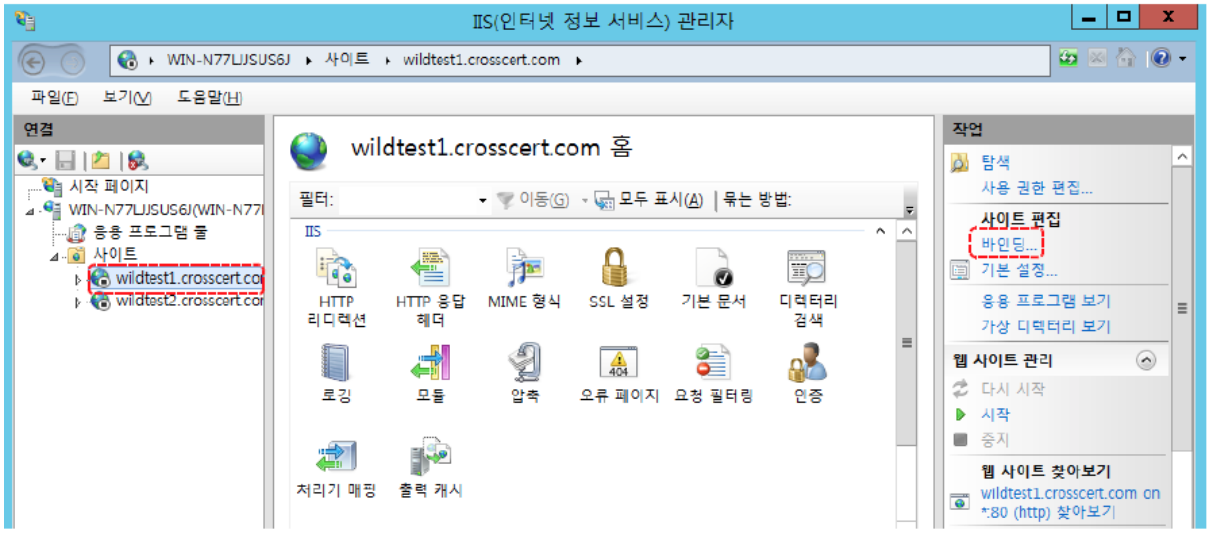
3. 해당 인증서(.pfx) 파일을 선택 및 암호 입력 후 확인



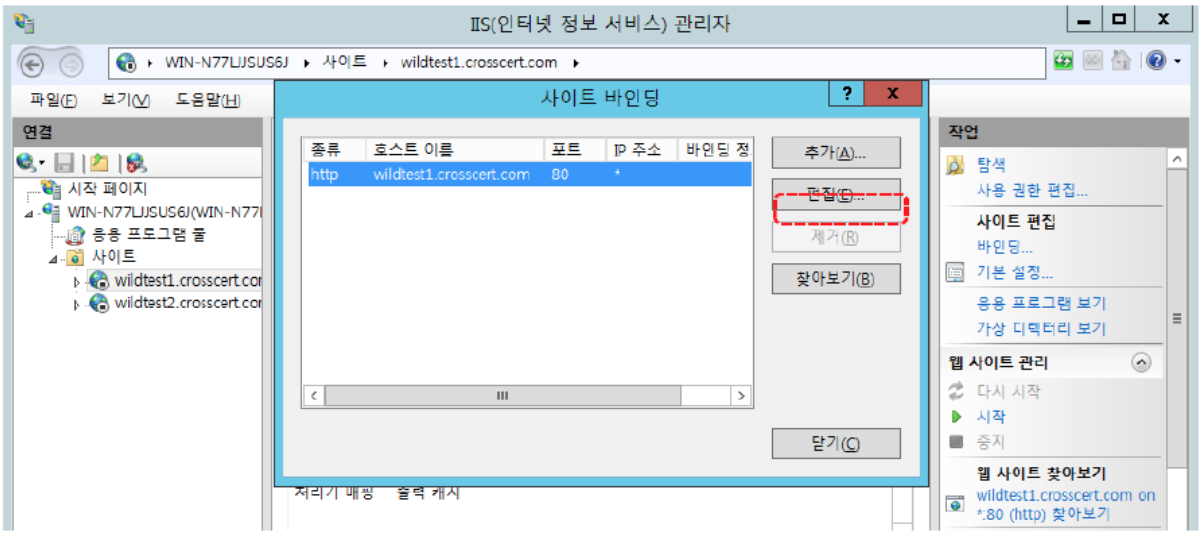
4. 아래와 같이 인증서 Import 확인



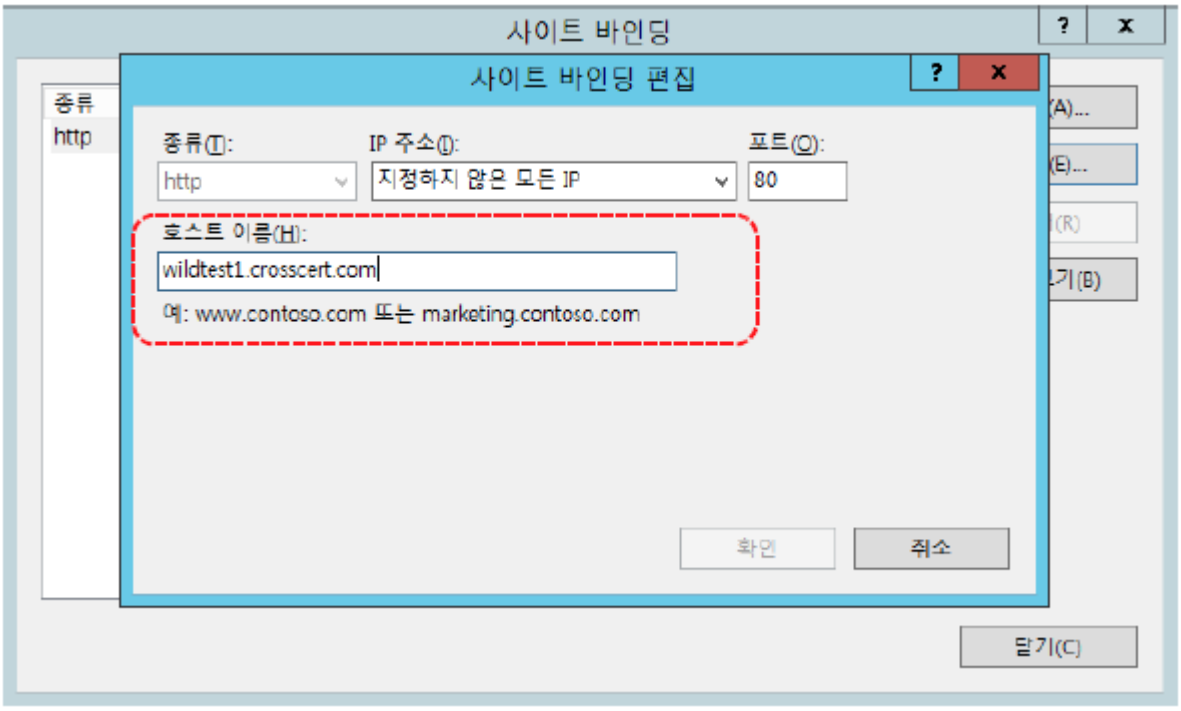
5. 인증서를 적용할 사이트(Ex. Server1)를 선택 후 '바인딩..' 실행



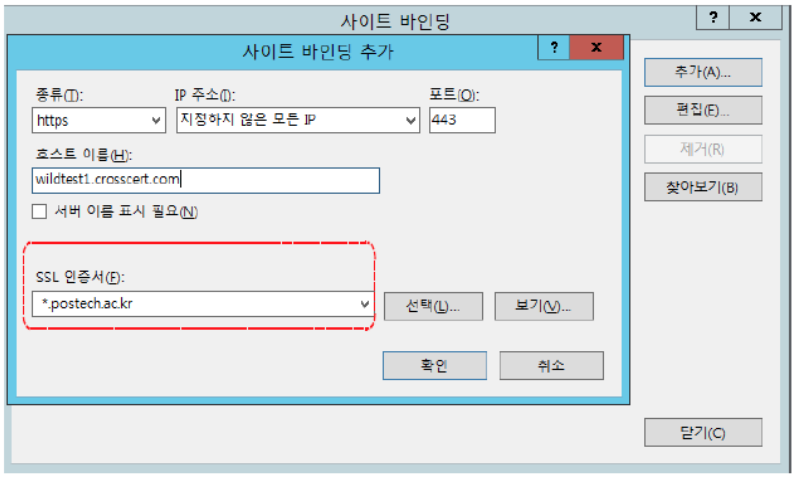
6. http 를 선택 후 '편집' 클릭



7. '호스트 이름'에 입력된 URL '확인' (공란일 경우 브라우저에서 접속하는 URL 입력)



8. '추가'를 클릭 → 정보를 입력한 뒤 인증서 선택 후 '확인'



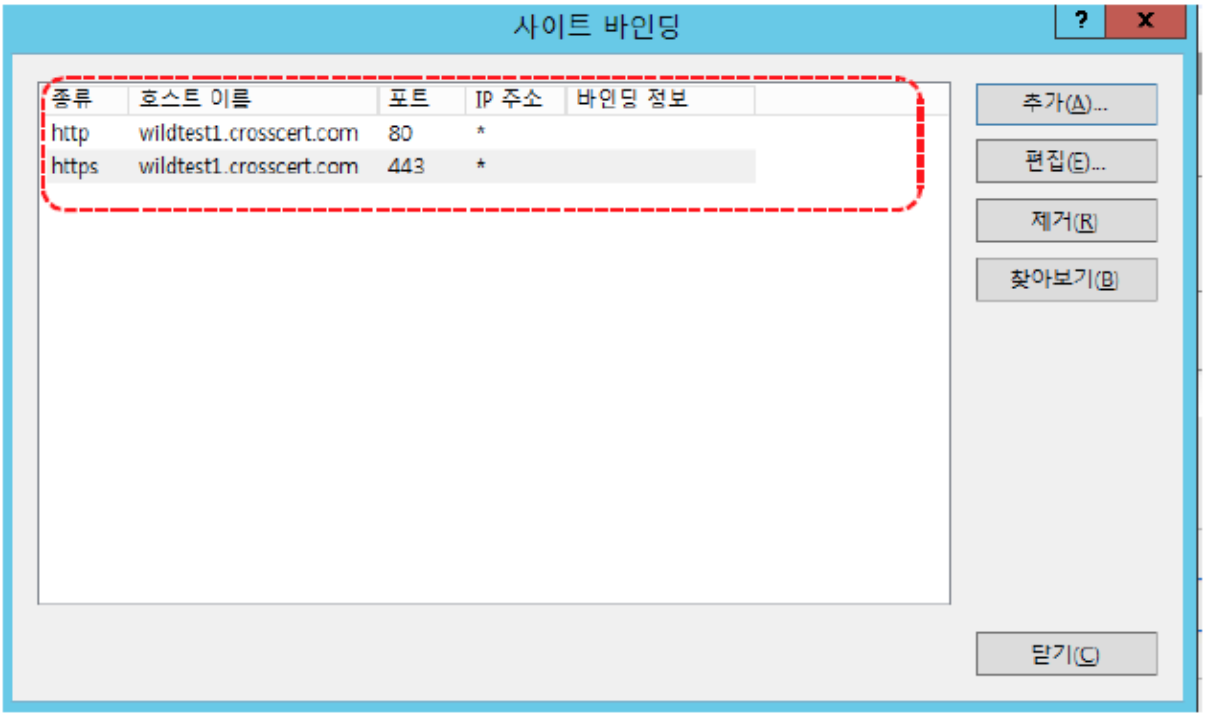
종류 : https

포트 : 기본 443

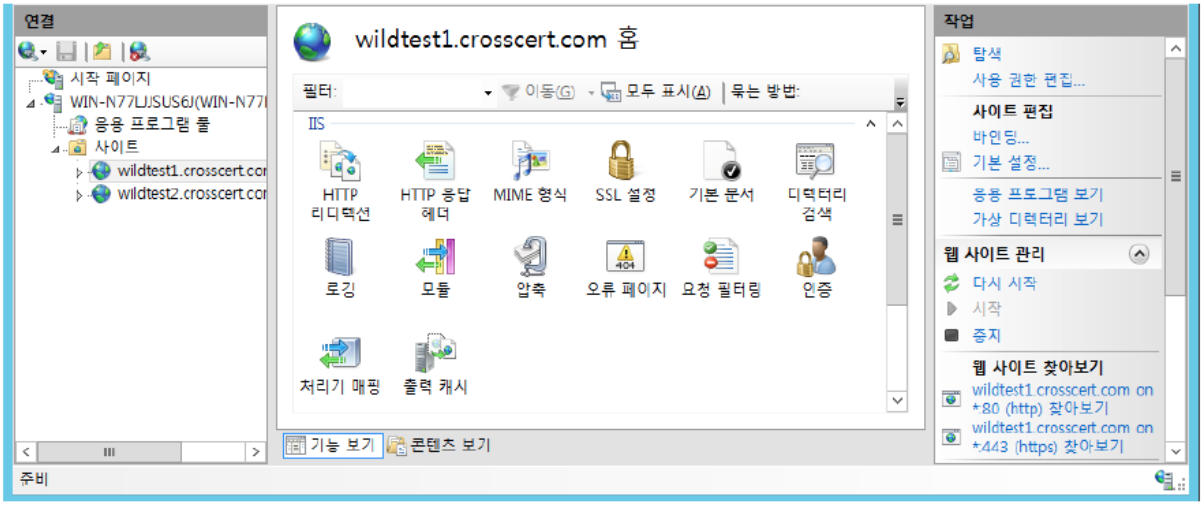
호스트 이름 : 해당 URL

SSL인증서 : 해당 인증서

9. 확인 후 '닫기'



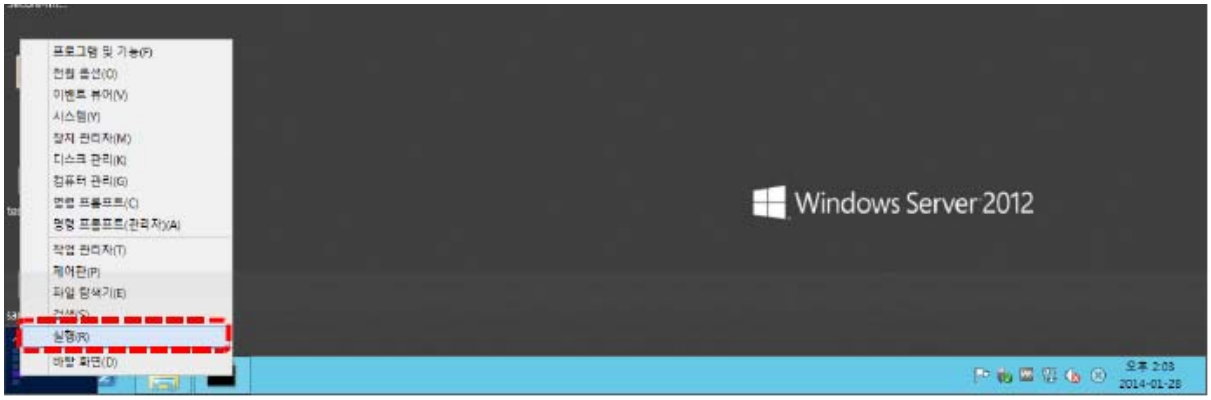
10. IIS 에서 해당 사이트 재구동



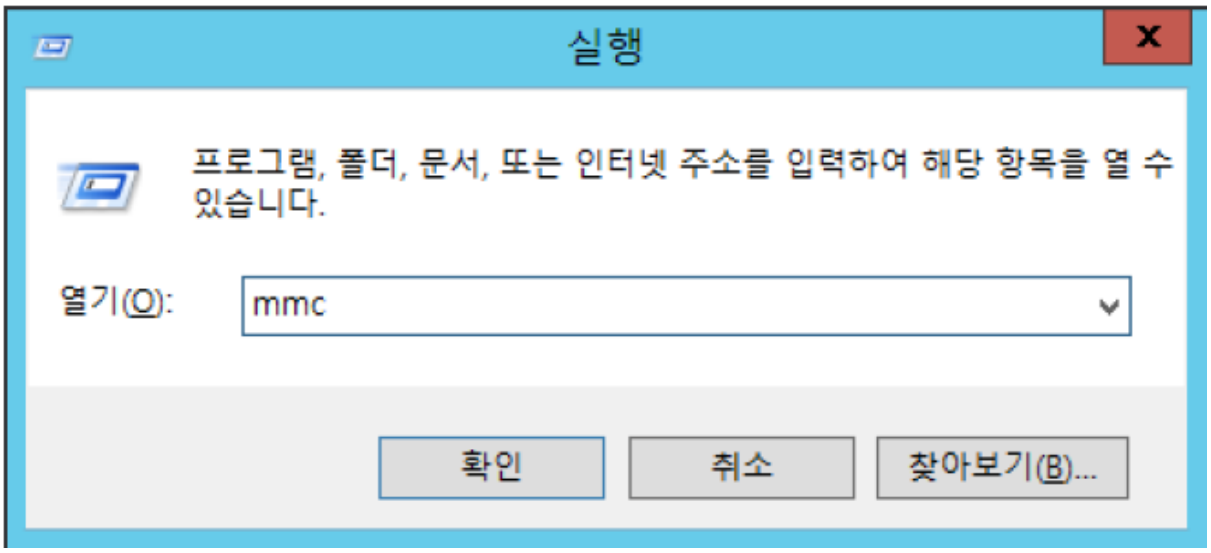
[체인 인증서 설치]

1. 체인인증서 파일(DigiCertCABundle.p7b)을 임의의 폴더에 저장

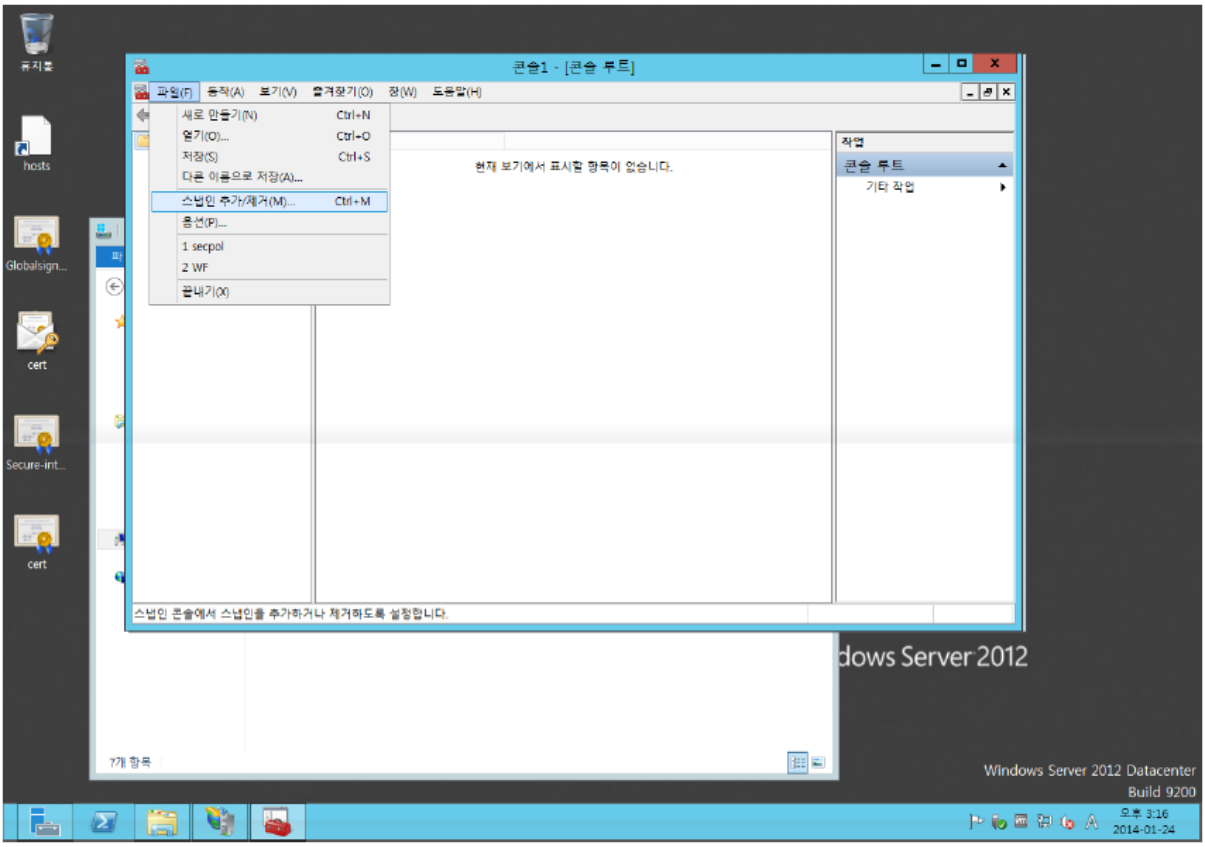
2. 시작 → '실행' 클릭



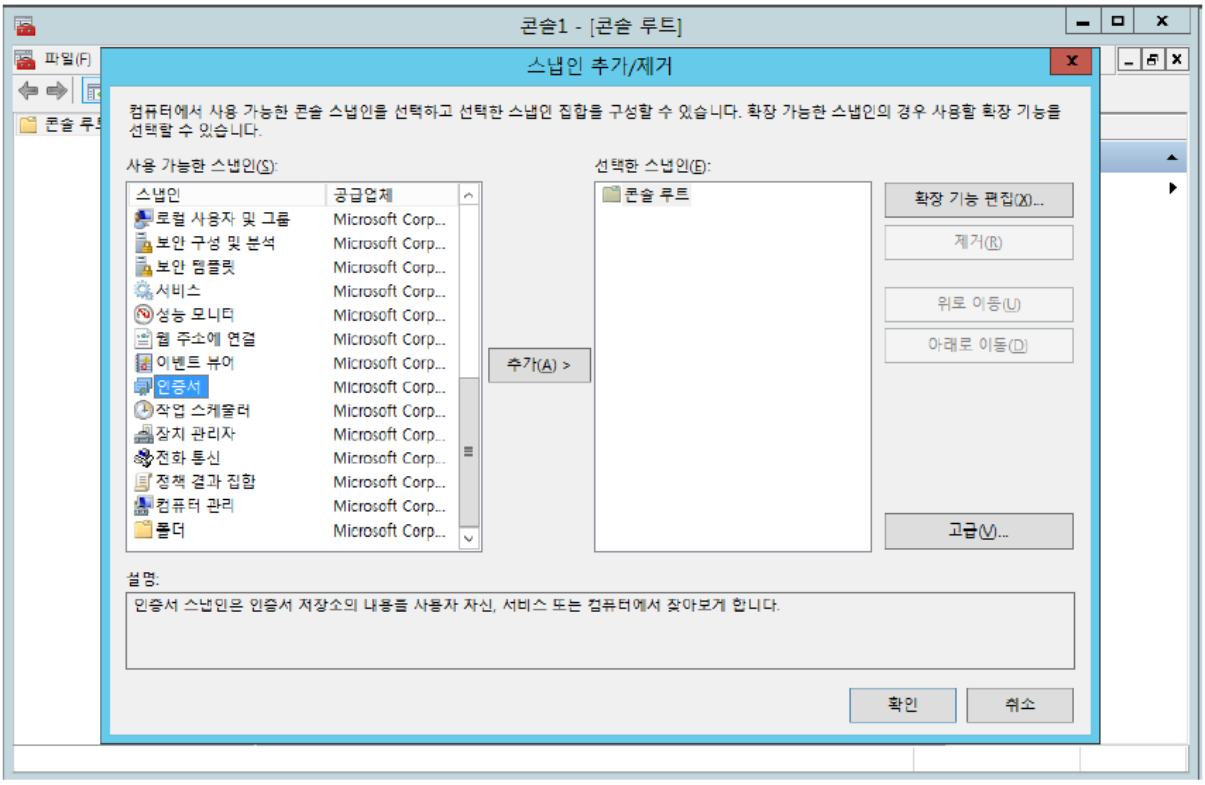
3. mmc 입력 후 '확인'



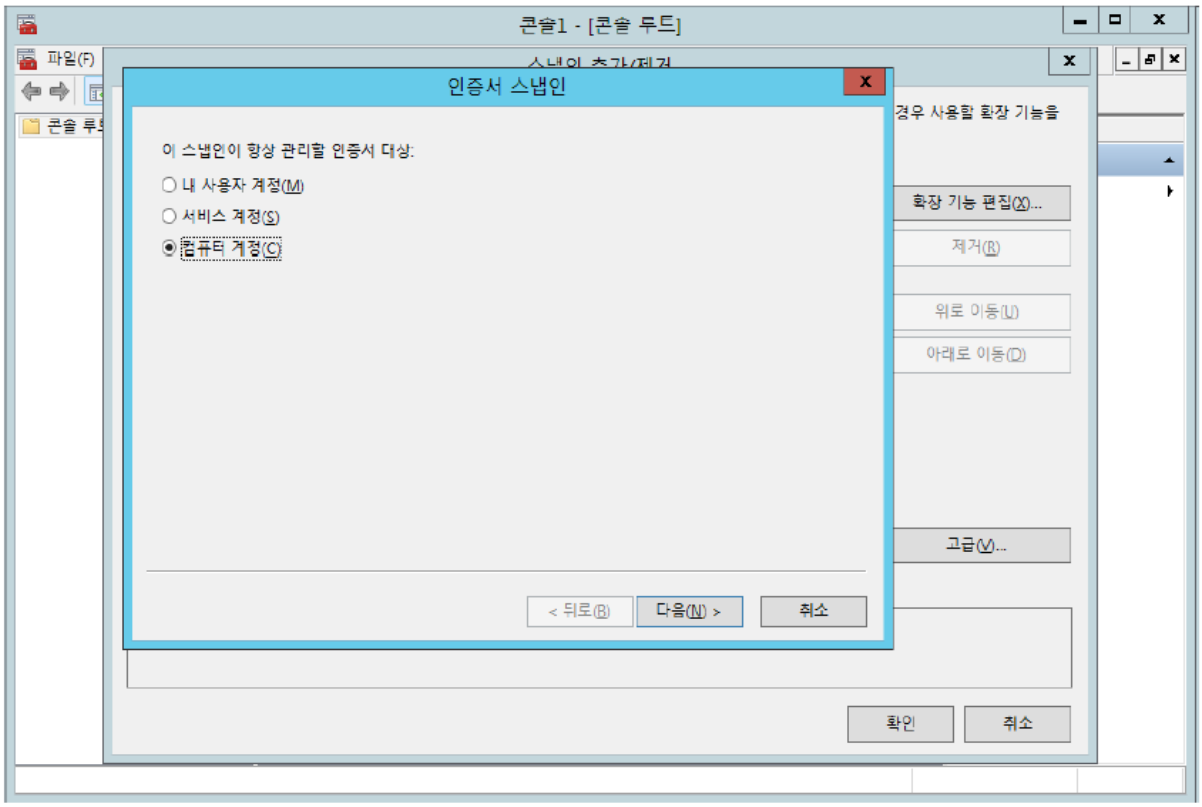
4. 해당 콘솔에서 '파일' → '스냅인 추가/제거' 클릭



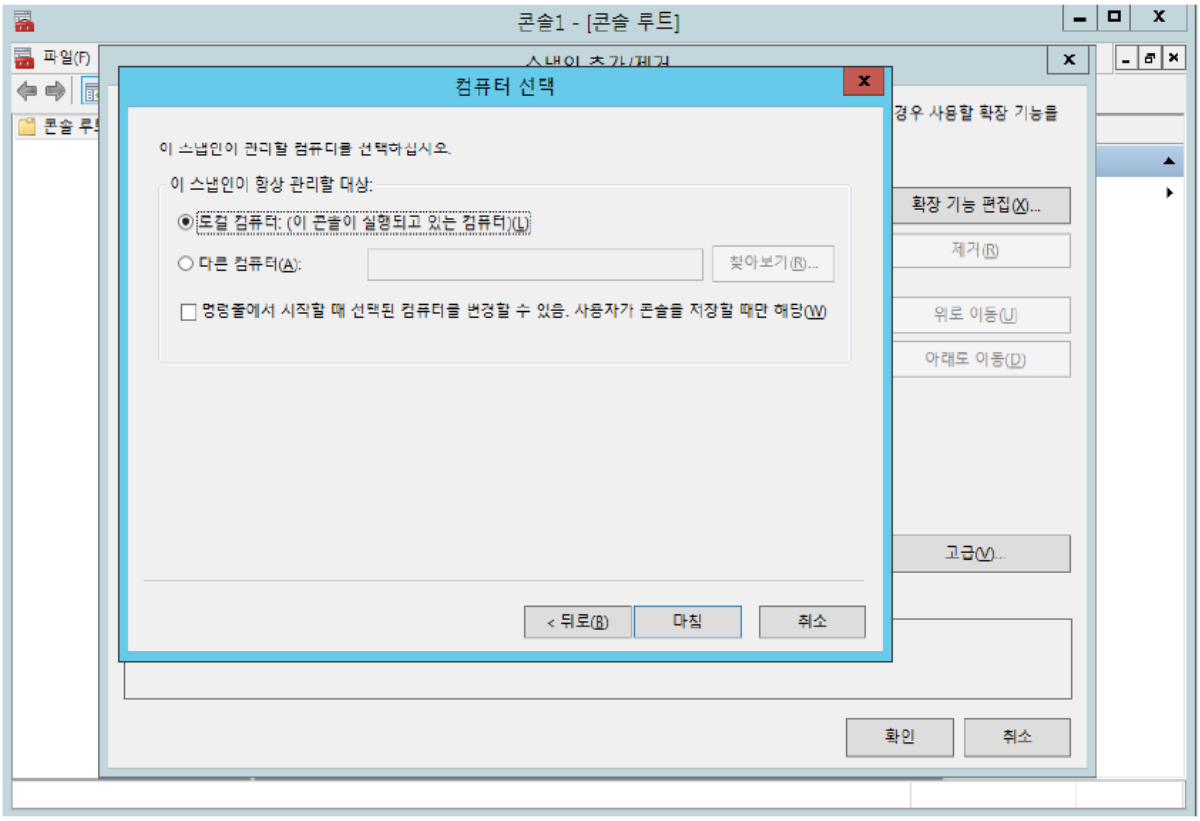
5. '인증서' 선택 후 '추가'



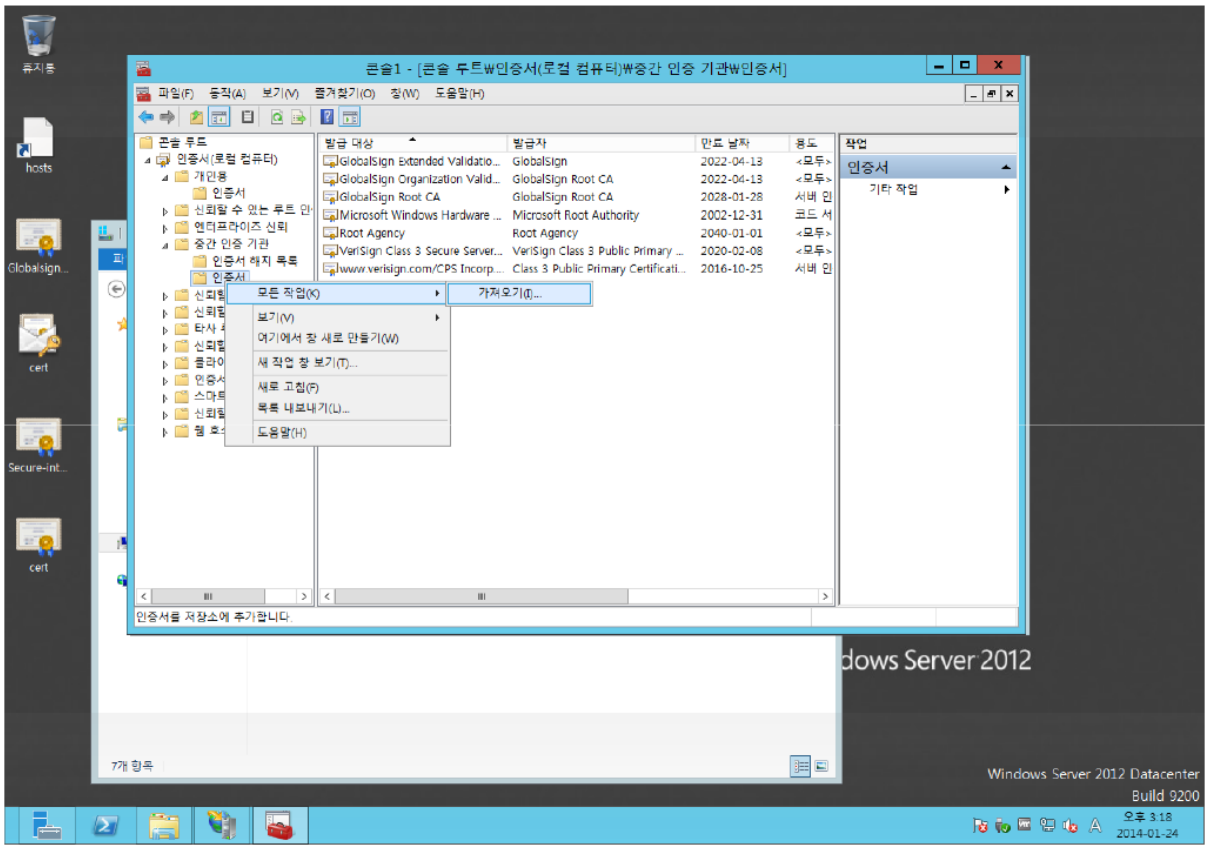
6. '컴퓨터 계정' 선택 후 '다음' 클릭



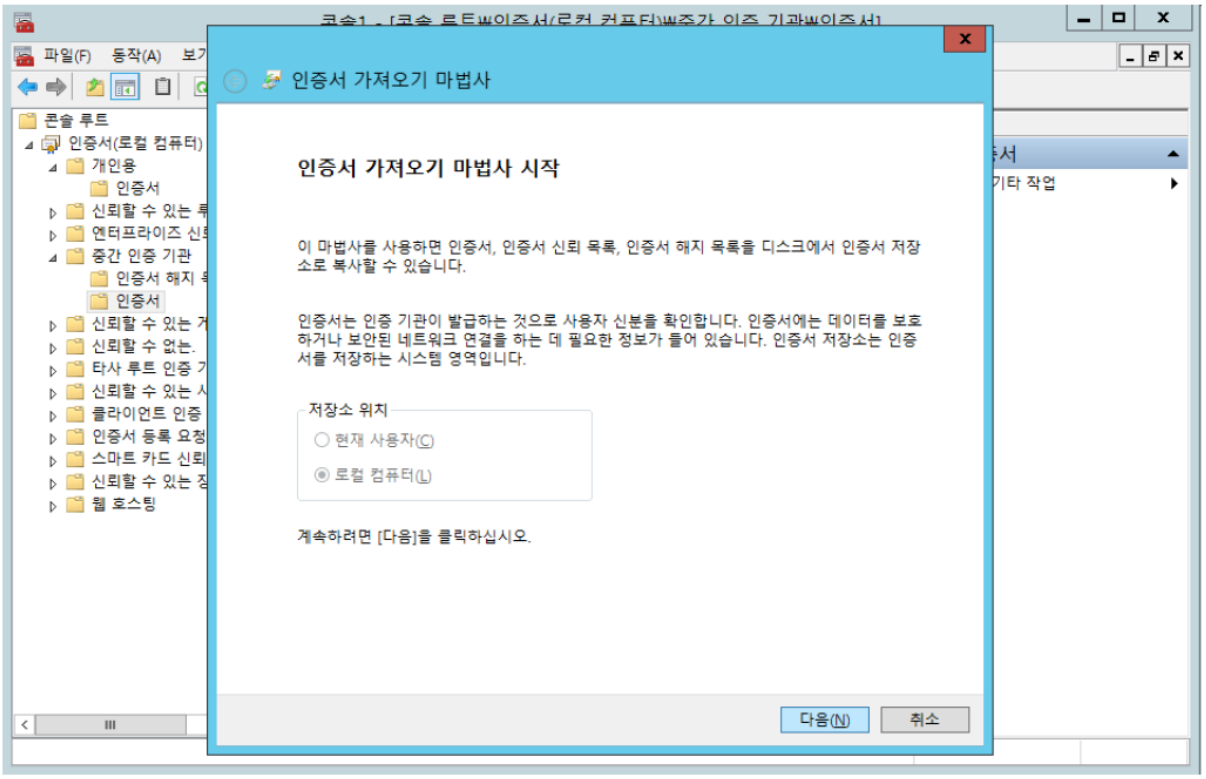
7. '로컬 컴퓨터' 선택 후 '마침' 클릭



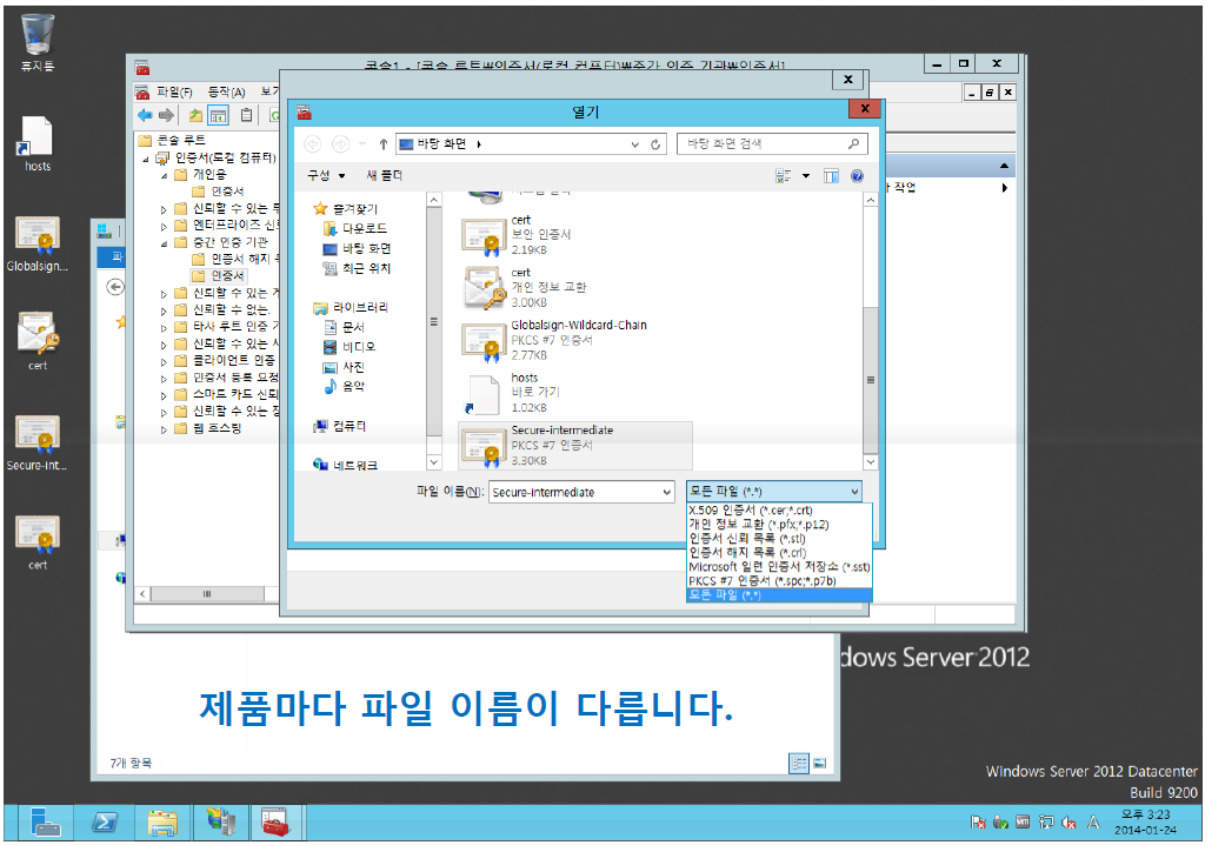
8. '중간 인증 기관'에 '인증서'를 우클릭 후 '모든작업'에 '가져오기' 클릭



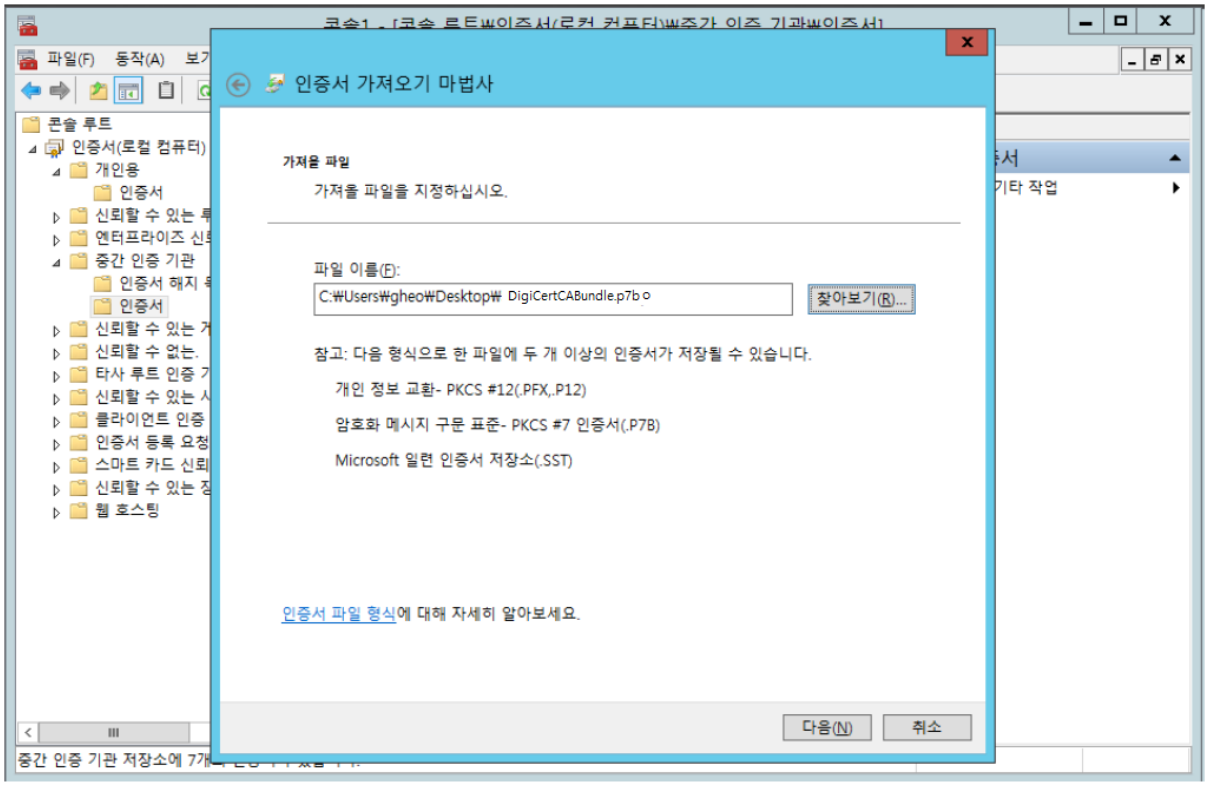
9. 인증서 가져오기 마법사 시작 확인 후 '다음'



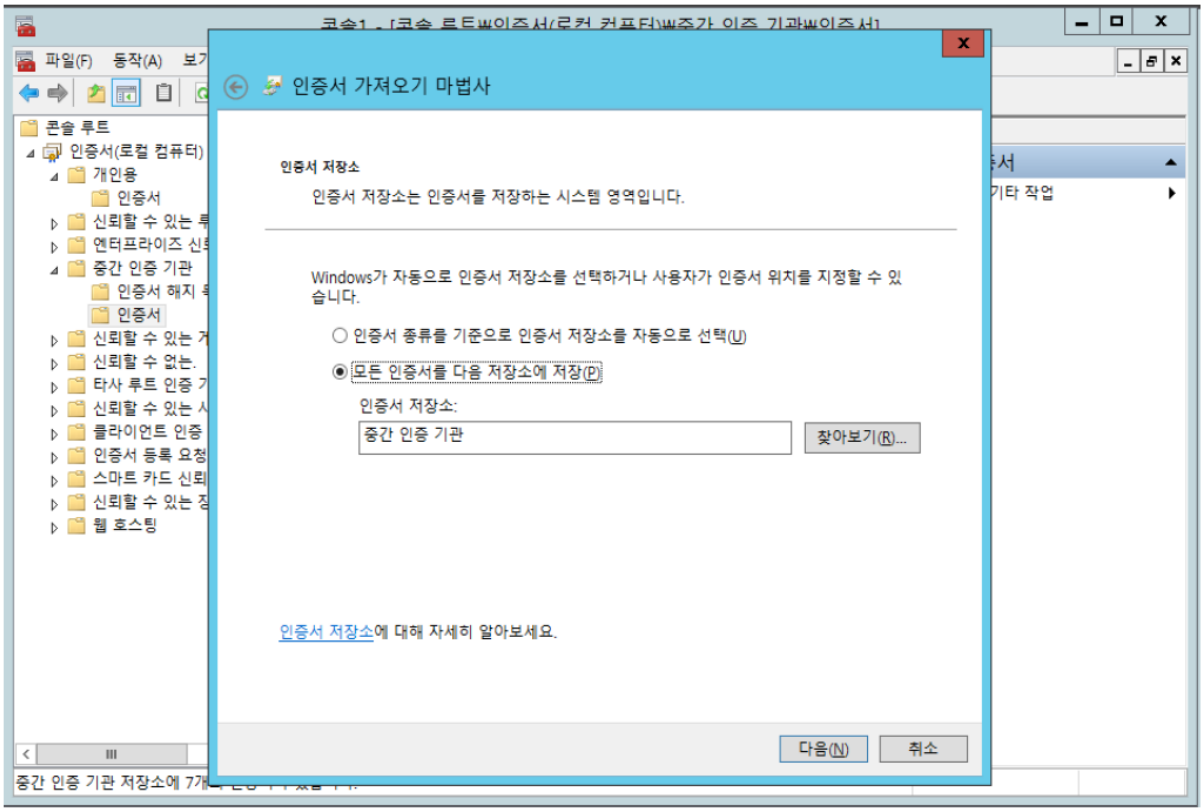
10. 임의의 폴더에 저장된 체인인증서(DigiCertCABundle.p7b)를 선택



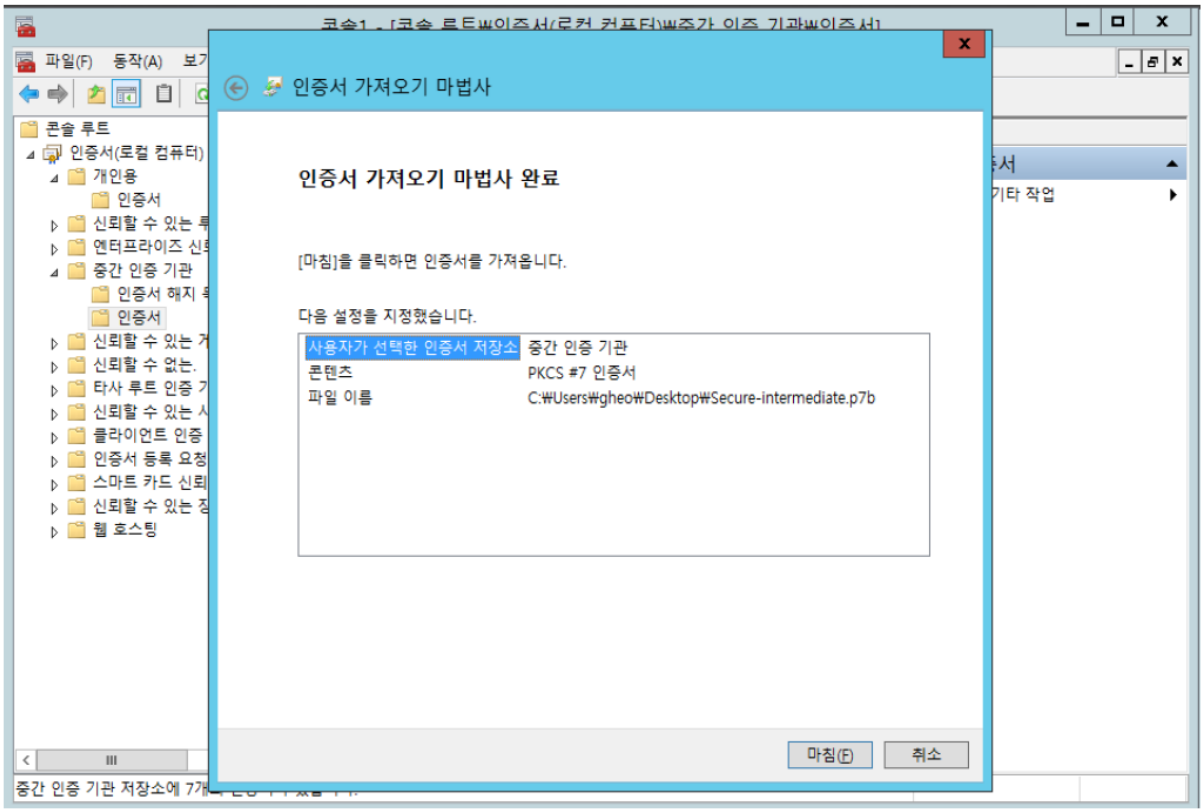
11. '다음' 클릭



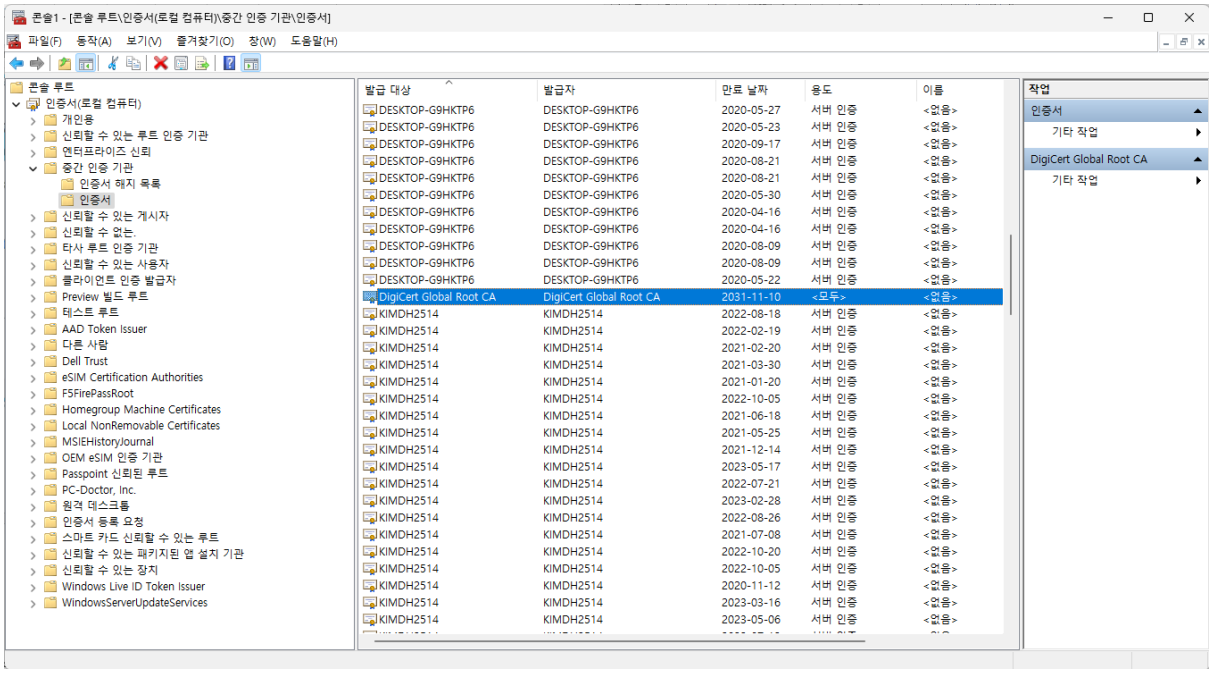
12. '모든 인증서를 다음 저장소에 저장' 선택 후 '중간 인증 기관' 확인 후 '다음'



13. 마법사 완료 확인 후 '마침' 클릭

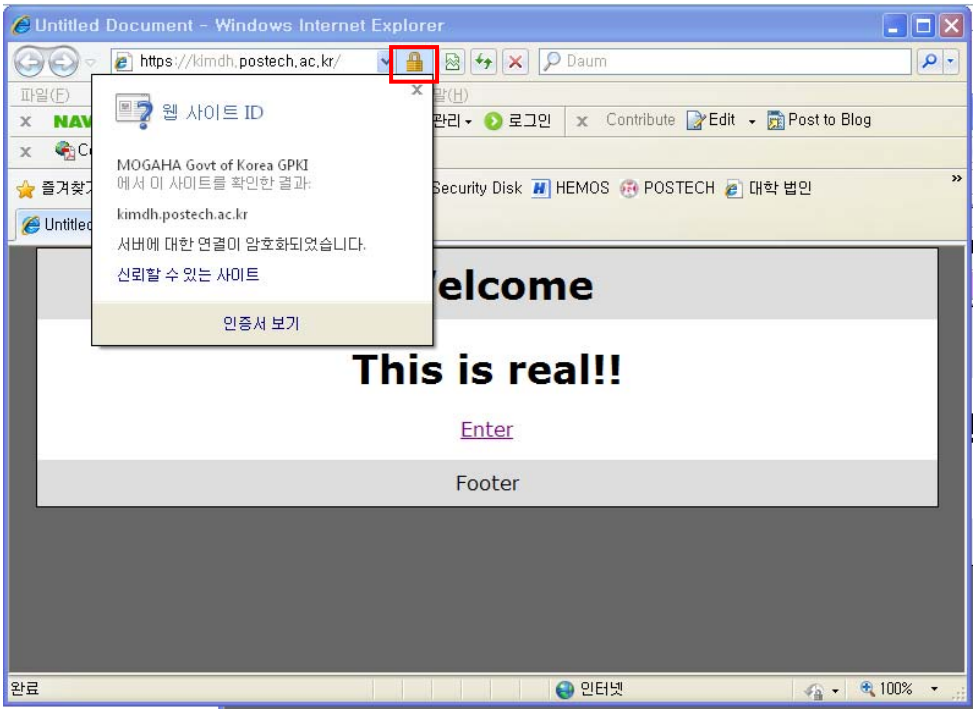


14. 설치한 체인인증서 파일을 확인



[인증서 설치 후 설치 확인]

1. https:// 로 접근하여 웹페이지가 올바로 열리는지 확인하여 인증서 설치 확인



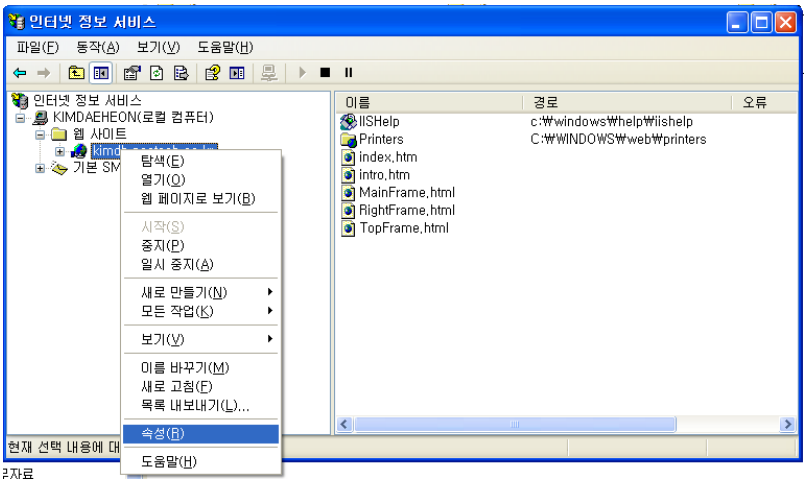
※ SSL 암호화 설정

인증서를 설치하고 나면 http 와 https 로의 접속이 모두 가능합니다. http 로의 접속을 계속 허용할 경우 SSL 인증서를 설치한 효과가 없습니다. 그러나, 일반 사용자 대부분이 http 로 접속을 하기 때문에 http 로의 접속을 차단하는 대신 https 로 전환시켜 주어야 합니다.

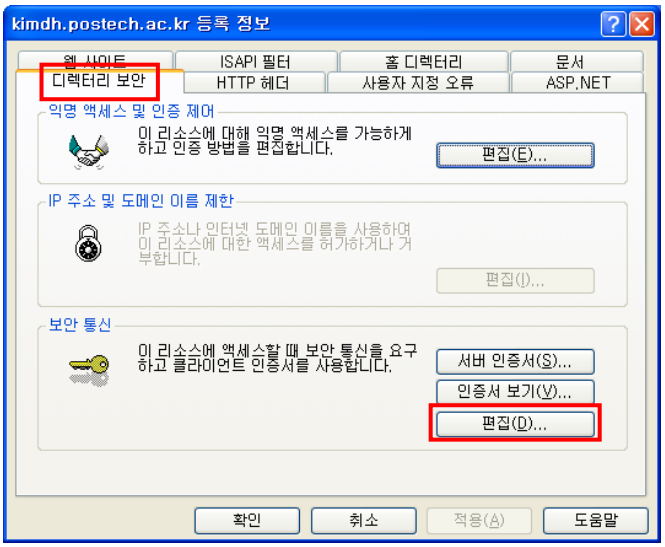
[https 리다이렉션 방법]

SSL 암호화를 설정하면 http 로의 접근이 차단되어 오류페이지를 호출하게 됩니다. 이때 호출하는 오류페이지를 https 로 리다이렉트 시켜주는 페이지로 대체하여 자동으로 전환하도록 합니다.

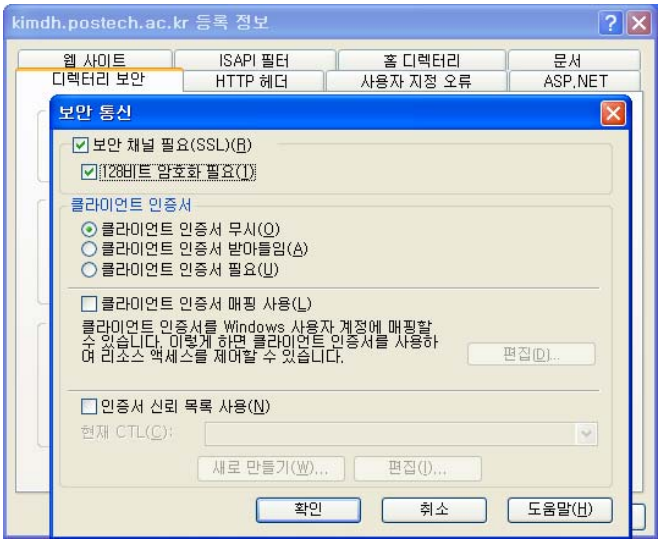
1. 인터넷 정보 서비스 실행(IIS) 후 해당 웹사이트 선택 후 마우스 오른쪽 클릭하여 속성 선택



2. 등록정보에서 디렉터리 보안 탭에서 편집 클릭



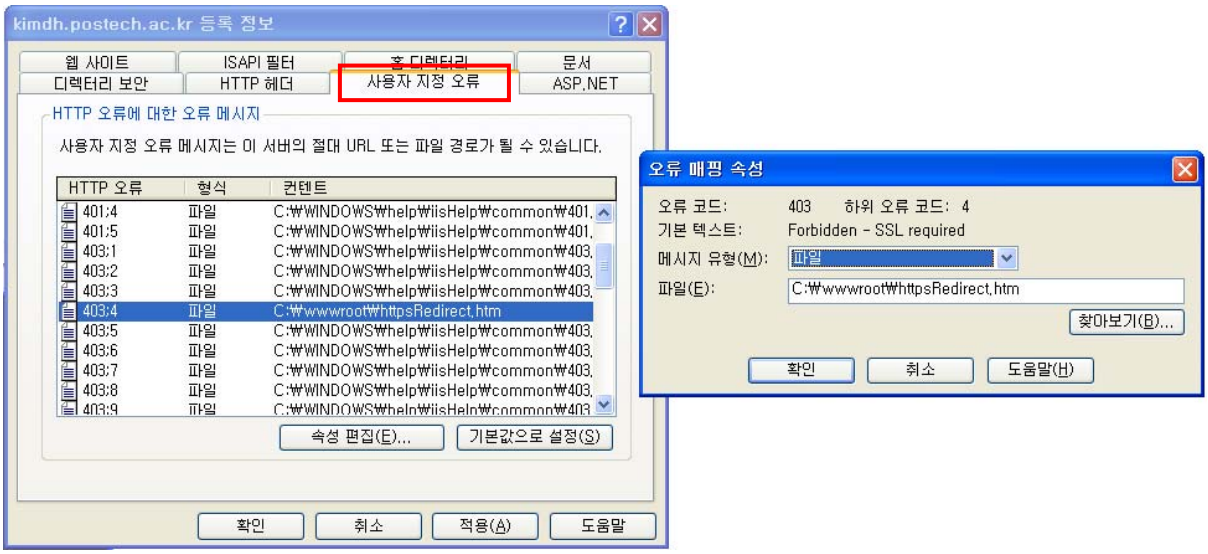
3. 보안 채널 필요(SSL) 체크 -> 128 비트 암호화 필요 체크, 그 외 설정은 그대로 둠



4. 아래와 같이 httpsRedirect.htm 파일을 생성하여 적당한 경로에 저장

```
<script type="text/javascript">
function redirectToHttps()
{
var httpURL = window.location.hostname + window.location.pathname;
var httpsURL = "https://" + httpURL ;
window.location = httpsURL ;
}
redirectToHttps();
</script>
```

5. 등록정보의 사용자 지정 오류 탭에서 403;4 오류 메시지를 선택하여 작성한 httpRedirect.htm 로 지정하여 확인



/종료/