

**POSTECH 보안서버(SSL 인증서)
구축 가이드**

2012. 03

학술정보처 정보시스템팀

<차례>

- I. 보안서버 구축 개요
- II. 보안서버 구축 시 주의사항
- III. Apache 서버에서 SSL 보안서버 구축하기
- IV. Apache Win 서버에서 SSL 보안서버 구축하기
- V. Tomcat 서버에서 SSL 보안서버 구축하기
- VI. IIS 5.1 SSL 인증서 설치
- VII. IIS 7.0 및 7.5 SSL 인증서 설치

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

- “공공기관의 개인정보보호에 관한 법률” 제 9 조

공공기관의 장은 개인정보를 처리하거나 개인정보파일을 “전자정보법” 제 2 조제 7 호에 따른 정보통신망(이하 “정보통신망”이라 한다)에 의하여 송/수신하는 경우 개인정보가 분실/도난/누출/변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 강구하여야 한다.

- 동법 시행령 제 10 조 2(홈페이지 개인정보보호)

공공기관의 장은 그 기관의 홈페이지를 구축/운영하는 과정에서 개인정보가 노출 또는 유출되지 아니하도록 관리적/기술적 조치를 취하여야 한다.

3. 구축대상

- 교내 서버로 등록된 대상 중 개인정보를 취급하는 웹 서버

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

※ <http://www.epki.go.kr> -> 자료실 -> 프로그램 및 설명서 -> 18 번 교육기관 보안서버 구축 가이드 V3.0 참고

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

- 제로보드 4 : 소스코드 수정필요
- 제로보드 XE : 관리자페이지에서 SSL 설정 적용
- 그누보드 : 소스코드 수정필요

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 서버에서 SSL 보안서버 구축하기

[인증서 설치하기]

1. 인증서 복사(4 개파일)

- 1) postech.crt → POSTECH 인증서
- 2) postech.key → Key 값
- 3) caChain.crt → 체인 인증서
- 4) rootca.crt → 루트 인증서

2. Apache 서버의 적절한 위치에 저장

```
파일(F) 편집(E) 보기(V) 터미널(T) 가기(G) 도움말(H)
[root@tmp-web cert]# ls -al
합계 28
drwxr-xr-x  2 root root 4096 2월  4 16:12 .
drwxr-xr-x  8 root root 4096 2월  6 19:12 ..
-rw-r--r--  1 root root 1600 2월  4 16:12 caChain.crt
-rw-r--r--  1 root root 1662 2월  4 16:12 postech.crt
-rw-r--r--  1 root root  958 2월  4 16:12 postech.key
-rw-r--r--  1 root root 1310 2월  4 16:12 rootca.crt
[root@tmp-web cert]# pwd
/etc/httpd/conf/cert
[root@tmp-web cert]#
[root@tmp-web cert]#
[root@tmp-web cert]#
```

3. ssl.conf 수정(Virtual host 설정)

```
NameVirtualHost 141.223.1.151:443 ← 해당 서버 IP

##
## SSL Virtual Host Context
##

<VirtualHost 141.223.1.151:443> ← 해당 서버 IP

# General setup for the virtual host, inherited from global configuration
DocumentRoot /home/ipitt/new_htdocs2 ← 홈페이지 파일이 있는 디렉토리
ServerName ipitt.postech.ac.kr ← 홈페이지 도메인
ServerAdmin hemos@postech.ac.kr
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
```

4. ssl.conf 수정(키 파일과 인증서 설정)

```
# Server Certificate:보안서버 인증서 설정
SSLCertificateFile /etc/httpd/conf/cert/postech.crt
# Server Private Key:보안서버 인증서 개인키 설정
```

```

SSLCertificateKeyFile /etc/httpd/conf/cert/postech.key
# Server Certificate Chain:체인 인증서 설정
SSLCertificateChainFile /etc/httpd/conf/cert/caChain.crt
# Certificate Authority (CA):최상위 인증기관(루트 인증서) 인증서 설정
SSLCACertificateFile /etc/httpd/conf/cert/rootca.crt

```

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

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

```

→ Enter pass phrase: 00100243 (← 키값입력 8 자리임)

6. 인증서 설치 확인

The screenshot shows a Windows Internet Explorer browser window displaying the POSTECH website (https://iptt.postech.ac.kr/). A callout bubble points to the address bar with the text "인증서 설치확인". Below the browser window, there are two overlapping windows:

- 웹 사이트 ID (Website ID):** A notification from MOGAHA Govt of Korea GPKI stating that the website (iptt.postech.ac.kr) is secure and can be trusted.
- 인증서 (Certificate):** A dialog box showing certificate details:
 - 인증서 정보 (Certificate Info)
 - 인증서의 용도 (Certificate Purpose): 원격 컴퓨터의 신분을 확인합니다. (Verify the identity of a remote computer.)
 - 발급 대상 (Issued To): *.postech.ac.kr
 - 발급자 (Issued By): CA134040001
 - 유효 기간 (Validity Period): 2009-12-17 부터 2012-03-17
 - Buttons: 인증서 설치(O)... (Install Certificate...), 발급자 설명(S) (View Certificates...), 확인 (OK)

7. 패스워드 수동입력 없이 웹 서비스 자동 실행하기

- SHELL 을 통한 키값 출력프로그램 작성

```
# vi auto_pass_ssl.sh
#!/bin/sh
echo '00100243'
```

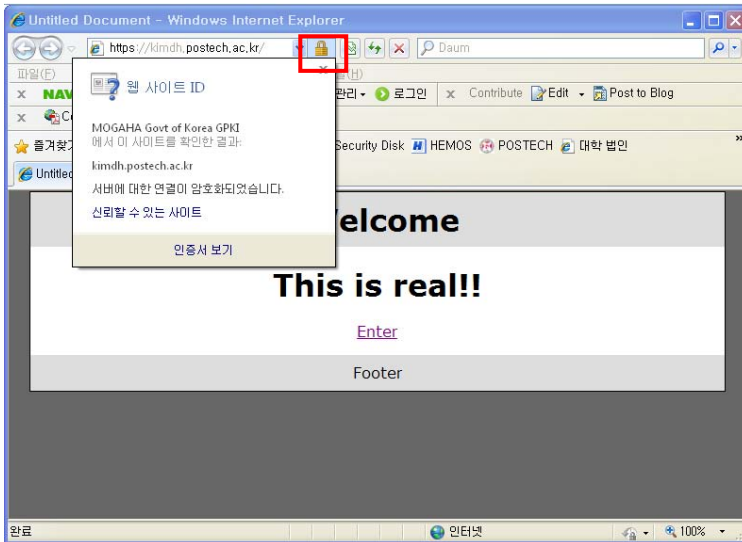
- 해당 프로그램 실행모드로 전환
 - # chmod 755 auto_pass_ssl.sh
- ssl.conf 파일 수정

```
# Pass Phrase Dialog:
# Configure the pass phrase gathering process.
# The filtering dialog program ('builtin' is an internal
# terminal dialog) has to provide the pass phrase on stdout.
#SSLPassPhraseDialog builtin
SSLPassPhraseDialog exec:/etc/httpd/conf/auto_pass_ssl.sh
```

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

[인증서 설치 후 설치 확인]

https:// 로 접근하여 웹페이지가 올바르게 열리는지 확인하여 인증서 설치 확인



※ SSL 암호화 설정

인증서를 설치하고 나면 http 와 https 로의 접속이 모두 가능합니다. http 로의 접속을 계속 허용 할 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]

Apache 서버의 경우 rewrite 모듈을 이용하여 전환

1. httpd.conf 에서 AllowOverride 항목의 옵션을 All 로 변경

```
<Directory "/web/mediawiki-1.15.2"> ← 홈페이지 파일이 들어있는 루트디렉토리
    Options Indexes FollowSymLinks
    AllowOverride All
```

```
Order allow,deny
Allow from all
</Directory>
```

2. .htaccess 파일을 아래와 같이 만들어 루트디렉토리에 저장

```
# mod_rewrite
<IfModule mod_rewrite.c>
  # Enable mod_rewrite engine
  RewriteEngine on
  RewriteCond %{HTTPS} off
  RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</IfModule>
```


IV. Apache Win 서버에서 SSL 보안서버 구축하기

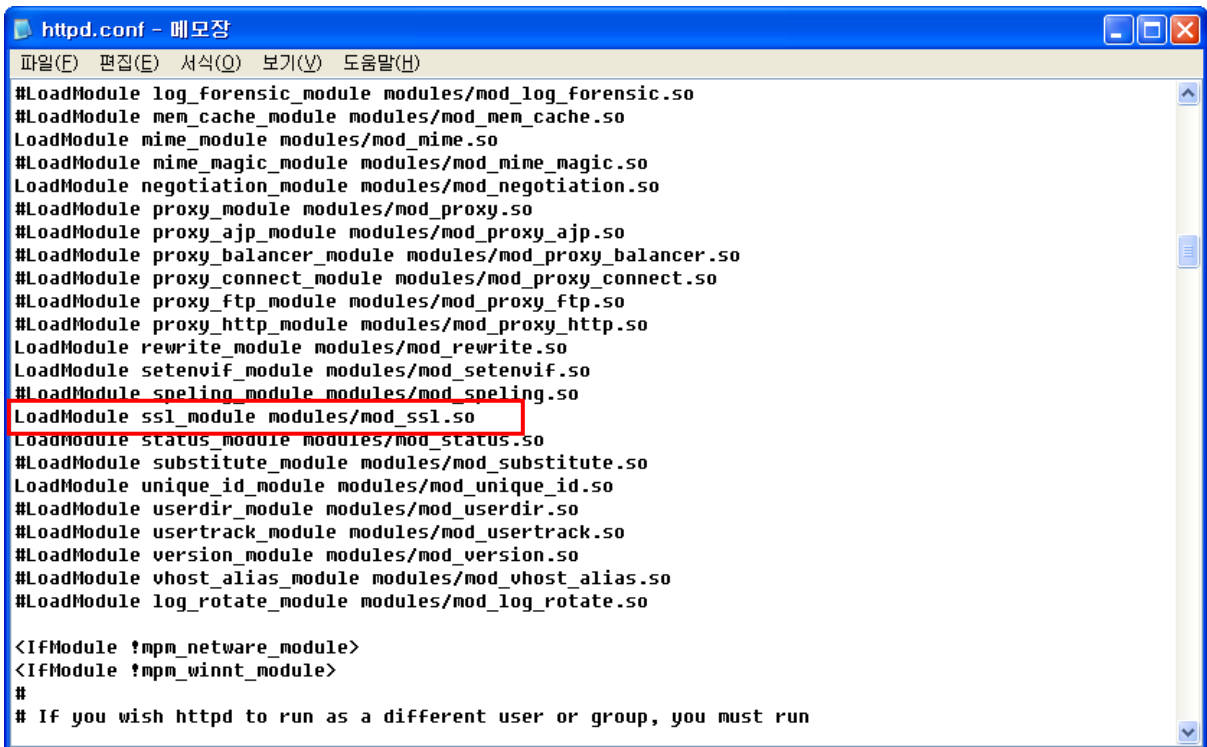
[웹서버 설정하기]

1. 인증서 파일을 서버의 적절한 위치에 저장(4 개 파일)

- 가. postech.crt → SSL 인증서
- 나. postech.key → 개인키
- 다. caChain.crt → 체인 인증서
- 라. rootca.crt → 루트 인증서

2. 웹서버 환경설정 파일 httpd.conf 수정

LoadModule ssl_module modules/mod_ssl.so 부분 주석 해제하여 활성화



```
httpd.conf - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
#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 spelling_module modules/mod_spelling.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

<IfModule !mpm_netware_module>
<IfModule !mpm_winnt_module>
#
# If you wish httpd to run as a different user or group, you must run
```

3. SSL 환경설정 파일(ssl.conf 또는 httpd-ssl.conf)을 "Include"하는 부분을 찾아 아래와 같이 주석 해제하여 SSL 설정 활성화, "SSLRandomSeed" 부분 수정

```
# Secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>
```

```
httpd.conf - 메모장
파일(E) 편집(E) 서식(O) 보기(V) 도움말(H)

# ServerAlias
Include conf/extra/httpd-alias.conf

# Virtual hosts
#Include conf/extra/httpd-vhosts.conf

# Local access to the Apache HTTP Server Manual
#Include conf/extra/httpd-manual.conf

# Distributed authoring and versioning (WebDAV)
#Include conf/extra/httpd-dav.conf

# Various default settings
Include conf/extra/httpd-default.conf

# Secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf
#
# Note: The following must must be present to support
#       starting without SSL on platforms with no /dev/random equivalent
#       but a statically compiled-in mod_ssl.
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>
```

4. SSL 환경설정 파일 httpd-ssl.conf 수정

SSL 을 적용할 포트(default 443) 설정

```
httpd-ssl.conf - 메모장
파일(E) 편집(E) 서식(O) 보기(V) 도움말(H)

# Manual for more details.
#
#SSLRandomSeed startup file:/dev/random 512
#SSLRandomSeed startup file:/dev/urandom 512
#SSLRandomSeed connect file:/dev/random 512
#SSLRandomSeed connect file:/dev/urandom 512

#
# When we also provide SSL we have to listen to the
# standard HTTP port (see above) and to the HTTPS port
#
# Note: Configurations that use IPv6 but not IPv4-mapped addresses need two
#       Listen directives: "Listen [::]:443" and "Listen 0.0.0.0:443"
#
Listen 443

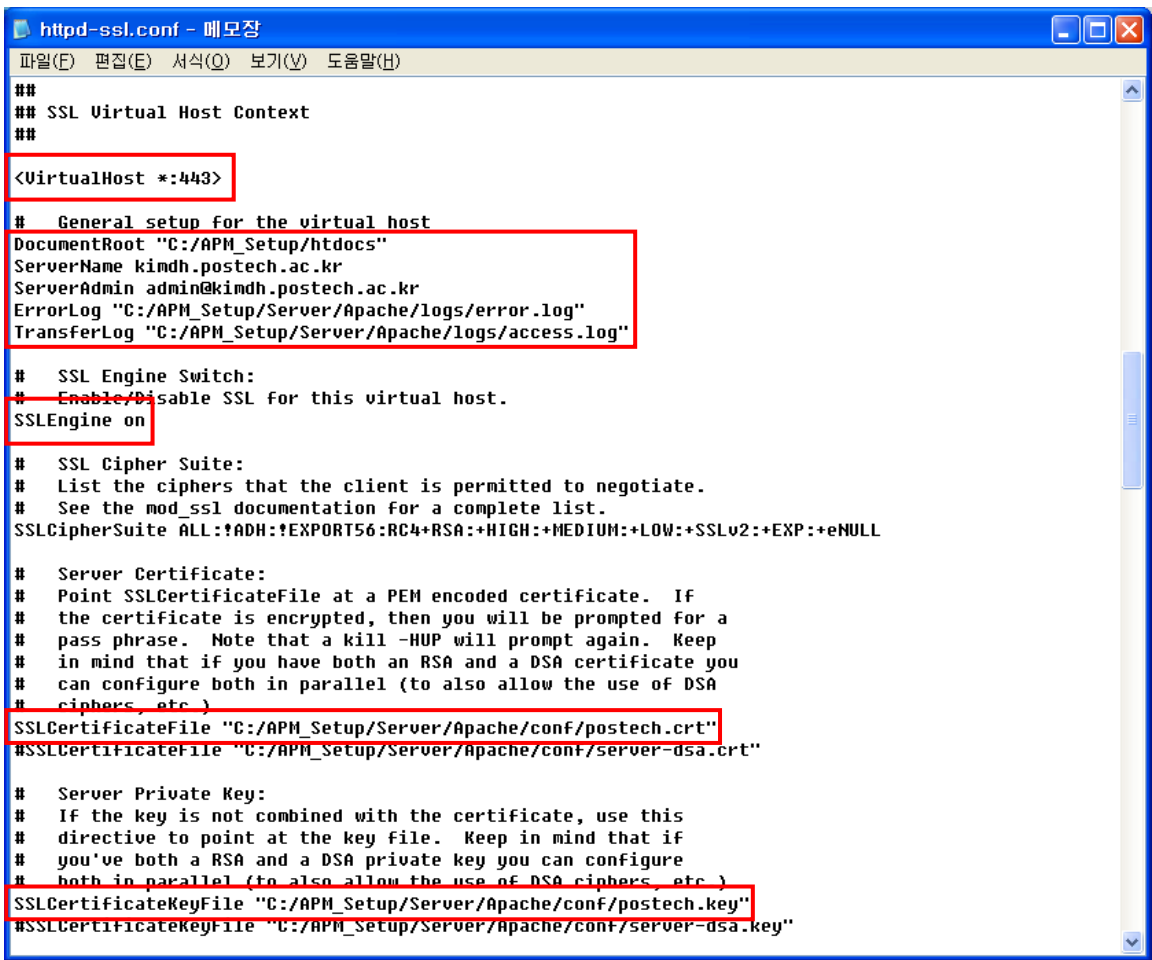
###
###  SSL Global Context
###
###  All SSL configuration in this context applies both to
###  the main server and all SSL-enabled virtual hosts.
###

#
#  Some MIME-types for downloading Certificates and CRLs
#
AddType application/x-x509-ca-cert .crt
```

※ SSL 보안서버는 기본적으로 443 을 사용하지만, 사이트 운영자가 1~65535 범위 내에서 임의의 포트번호를 설정할 수 있습니다. ex> 444, 445, 447 등등

5. SSL 을 사용하기 위해 구성할 Virtual Host 부분을 아래와 같이 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>
```



```

httpd-ssl.conf - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convenience.
SSLCertificateChainFile "C:/APM_Setup/Server/Apache/conf/caChain.crt"

# Certificate Authority (CA):
# Set the CA certificate verification path where to find CA
# certificates for client authentication or alternatively one
# huge file containing all of them (file must be PEM encoded)
# Note: Inside SSLCACertificatePath you need hash symlinks
# to point to the certificate files. Use the provided
# Makefile to update the hash symlinks after changes.
SSLCACertificatePath "C:/APM_Setup/Server/Apache/conf/ssl.crt"
SSLCACertificateFile "C:/APM_Setup/Server/Apache/conf/rootca.crt"

# Certificate Revocation Lists (CRL):
# Set the CA revocation path where to find CA CRLs for client
# authentication or alternatively one huge file containing all
# of them (file must be PEM encoded)
# Note: Inside SSLCARevocationPath you need hash symlinks
# to point to the certificate files. Use the provided
# Makefile to update the hash symlinks after changes.
SSLCARevocationPath "C:/APM_Setup/Server/Apache/conf/ssl.crl"

```

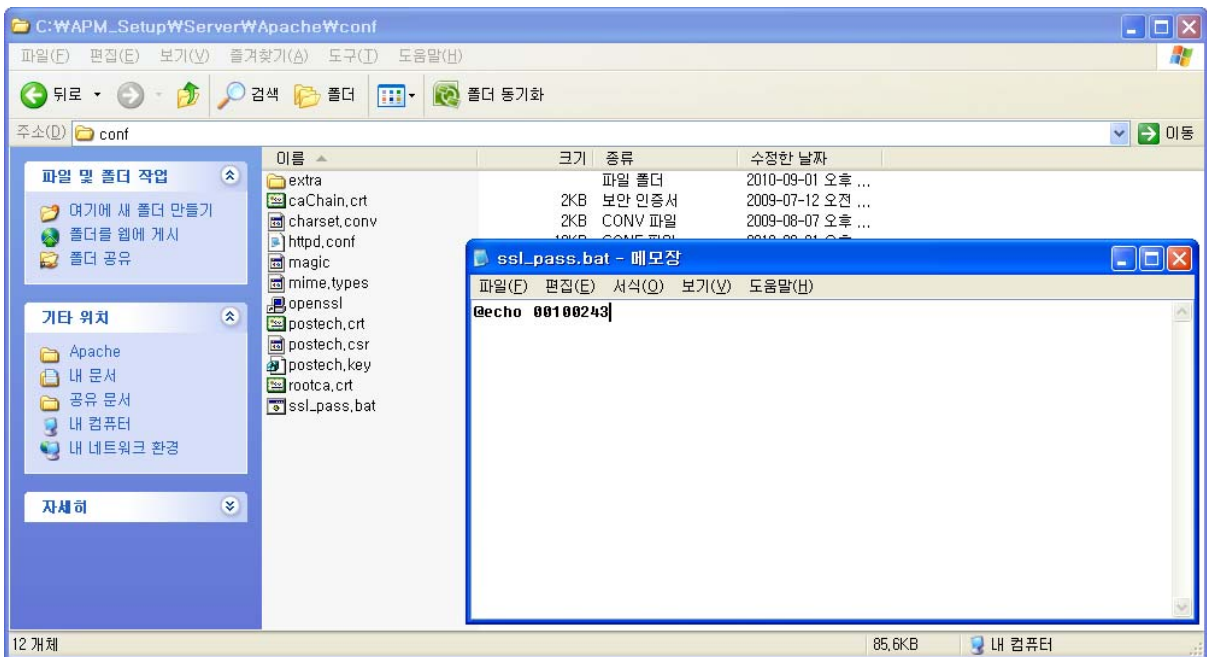
6. SSL 인증서 개인키 암호 설정

인증서 비밀키에 대한 암호문을 자동으로 입력하는 설정 필요

인증서 비밀키 암호저장 파일 만들기(암호 : 00100243)

```
@echo 00100242
```

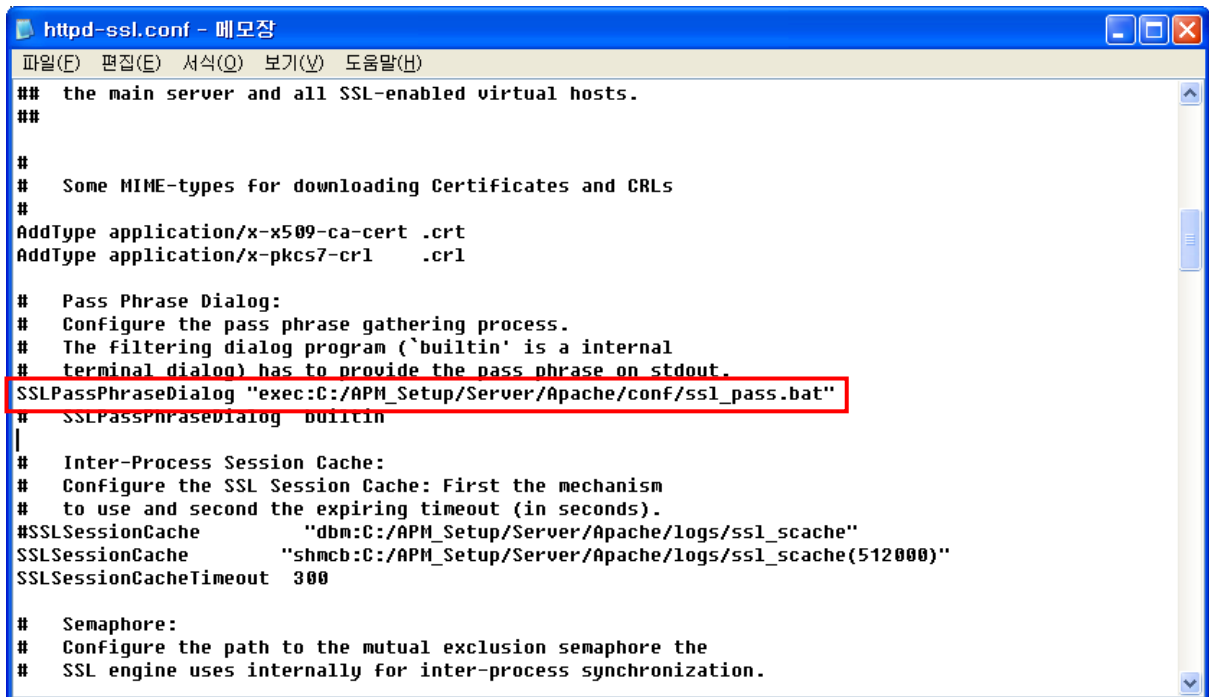
예) 파일명 : ssl_pass.bat / 파일내용 : @echo 00100243



7. 웹서버 인증서 비밀키 자동입력 설정

```
SSLPassPhraseDialog "exec:(절대경로)/ssl_pass.bat
```

기존의 "SSLPassPhraseDialog builtin" 설정문은 주석 처리



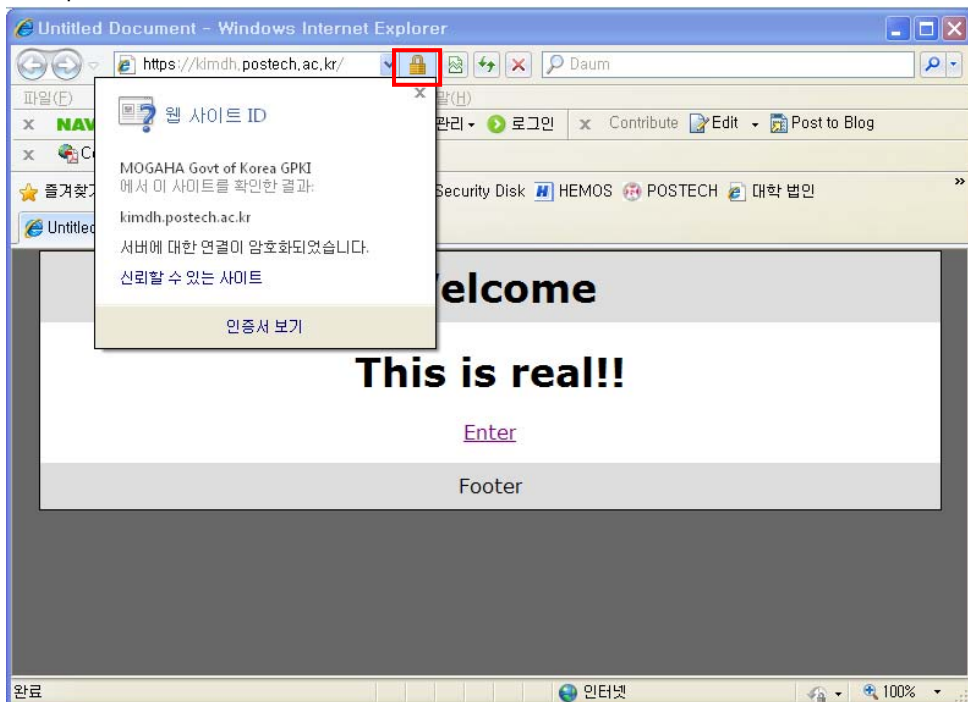
```
httpd-ssl.conf - 메모장
파일(E) 편집(E) 서식(O) 보기(V) 도움말(H)
### the main server and all SSL-enabled virtual hosts.
###
#
# Some MIME-types for downloading Certificates and CRLs
#
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-cr1 .cr1

# Pass Phrase Dialog:
# Configure the pass phrase gathering process.
# The filtering dialog program ('builtin' is an internal
# terminal dialog) has to provide the pass phrase on stdout.
SSLPassPhraseDialog "exec:C:/APM_Setup/Server/Apache/conf/ssl_pass.bat"
# SSLPassPhraseDialog builtin
|
# Inter-Process Session Cache:
# Configure the SSL Session Cache: First the mechanism
# to use and second the expiring timeout (in seconds).
#SSLSessionCache "dbm:C:/APM_Setup/Server/Apache/logs/ssl_scache"
SSLSessionCache "shmcb:C:/APM_Setup/Server/Apache/logs/ssl_scache(512000)"
SSLSessionCacheTimeout 300

# Semaphore:
# Configure the path to the mutual exclusion semaphore the
# SSL engine uses internally for inter-process synchronization.
```

[인증서 설치 후 설치 확인]

1. https:// 로 접근하여 웹페이지가 올바르게 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.

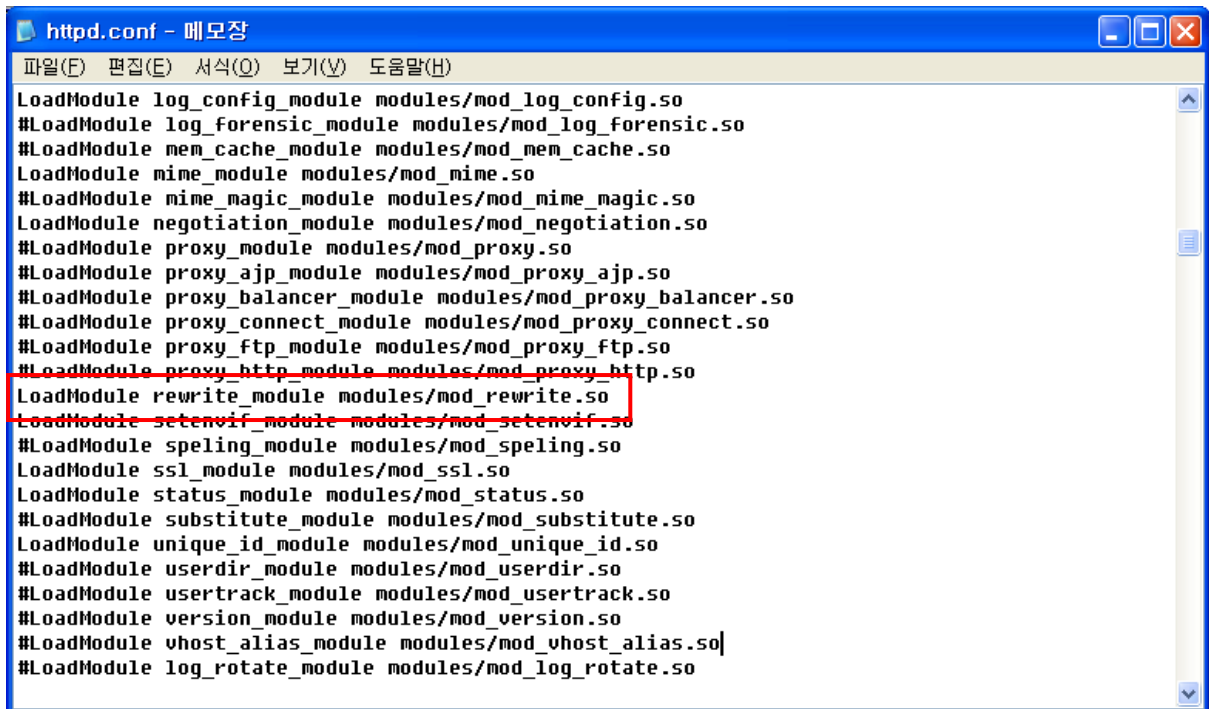
[http → https 전환하기]

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
```

V. Tomcat 서버에서 SSL 보안서버 구축하기

[웹서버 설정하기]

1. 인증서 파일을 서버의 적절한 위치에 저장

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

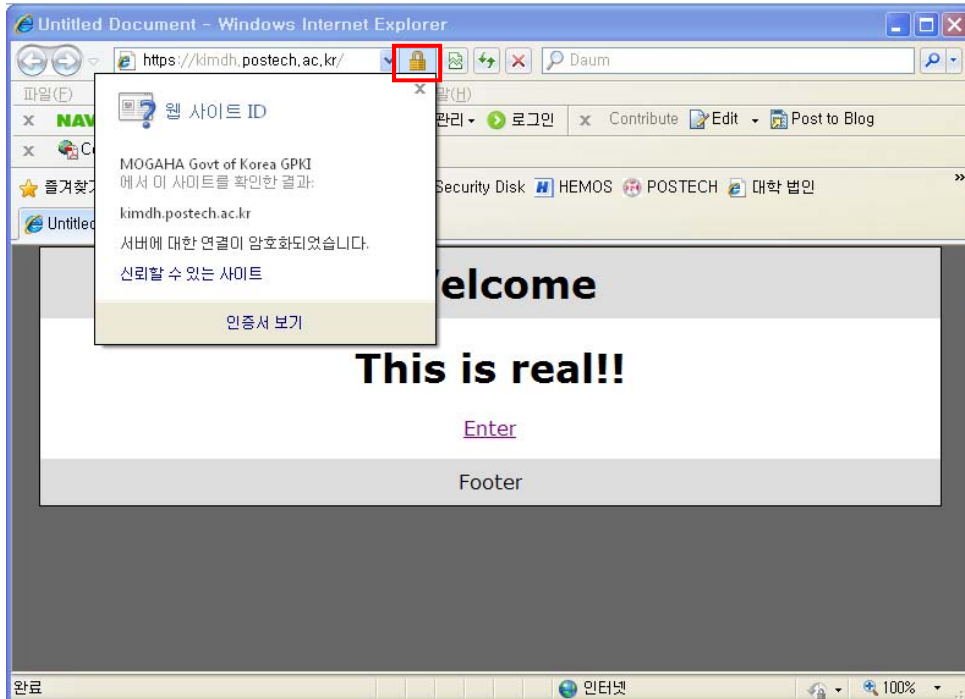
2. 웹서버 설정 변경

server.xml 을 수정하여 포트 8443 주석처리 해지하여 keystoreFile, keystorePass 설정 추가
Connector port="443"으로 설정

```
<!-- 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/keystore"  
    keystorePass="postech1!"  
    clientAuth="false" sslProtocol="TLS" />
```

[인증서 설치 후 설치 확인]

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



※ SSL 암호화 설정

인증서를 설치하고 나면 http 와 https 로의 접속이 모두 가능합니다. http 로의 접속을 계속 허용 할 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

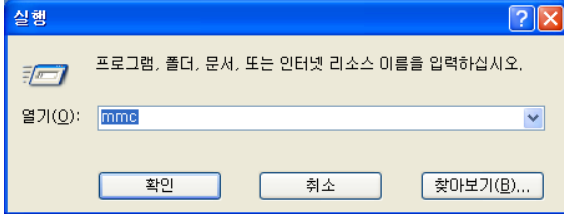
```
<!-- SSL settings. only allow HTTPS access to Web -->

<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>
```

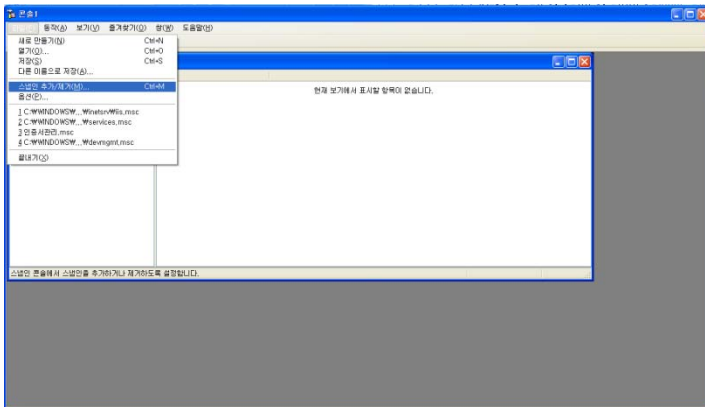

VI. IIS 5.1 SSL 인증서 설치

[SSL 인증서 가져오기]

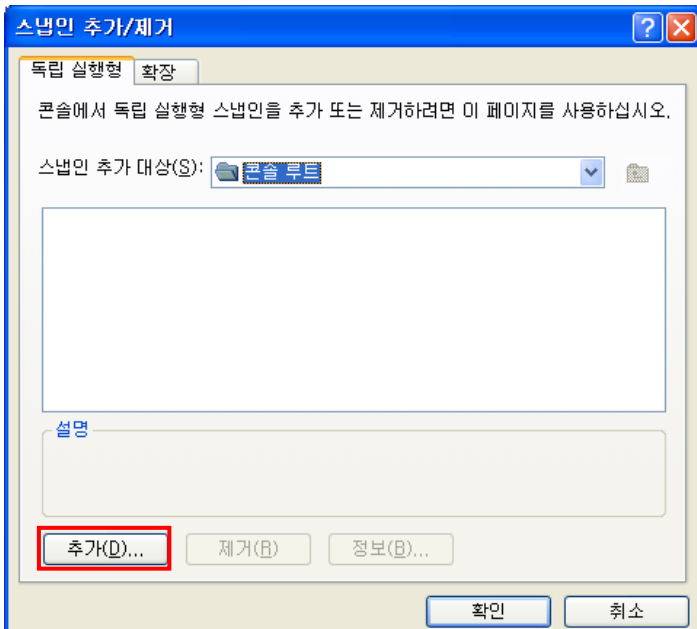
1. 시작->실행->윈도우관리자 콘솔(mmc) 실행



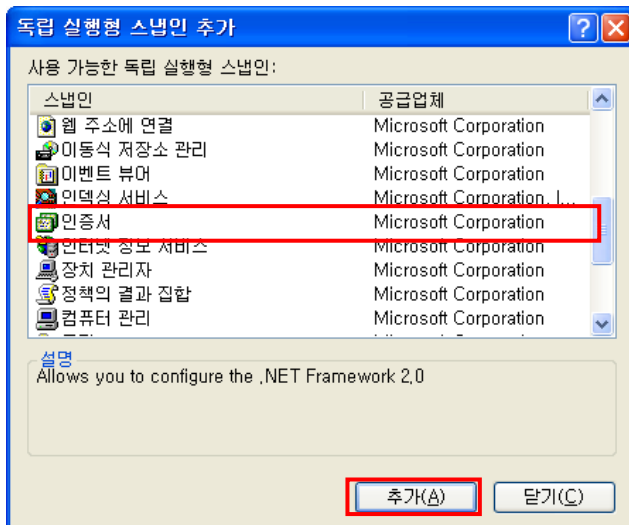
2. 콘솔창이 열리면 파일 -> 스냅인 추가/제거 선택



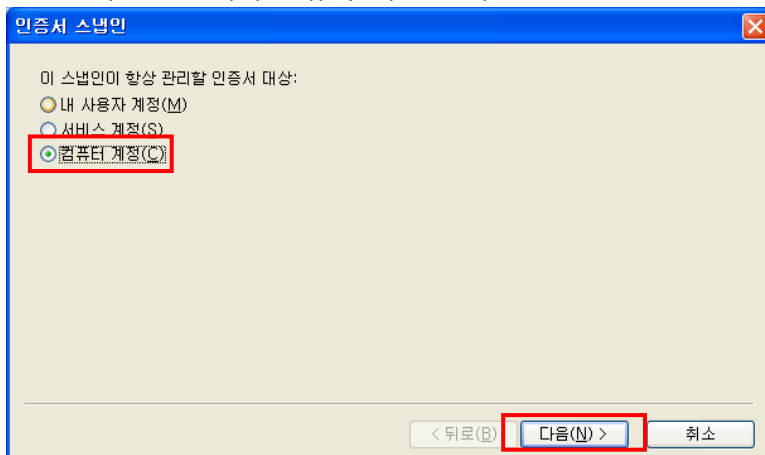
3. 스냅인 추가/제거에서 추가 클릭



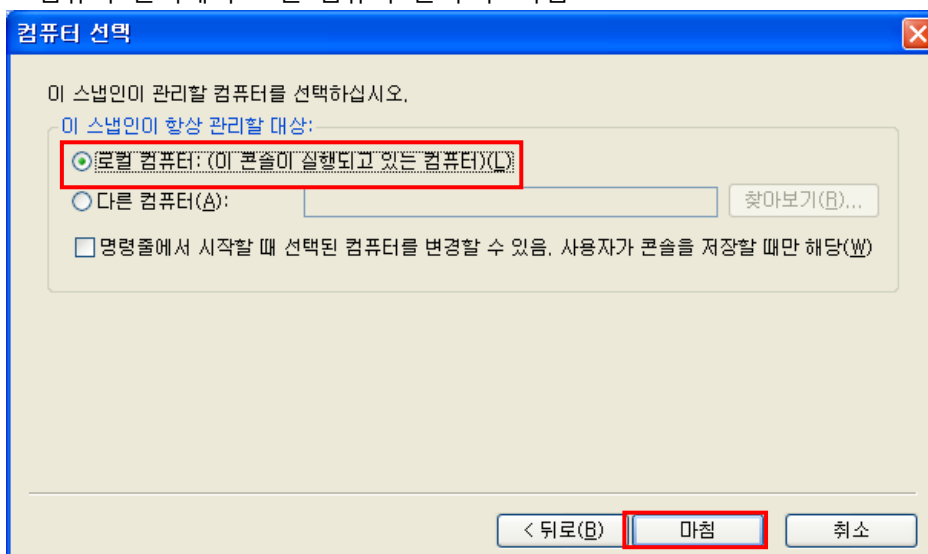
4. 독립 실행형 스냅인 추가에서 인증서 추가



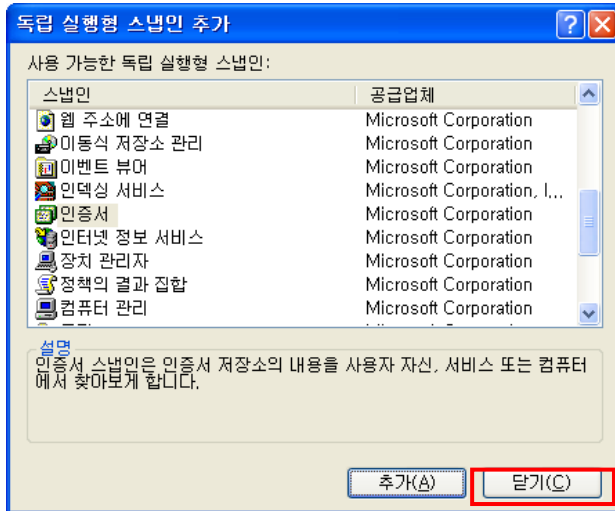
5. 인증서 스냅인에서 컴퓨터 계정 선택



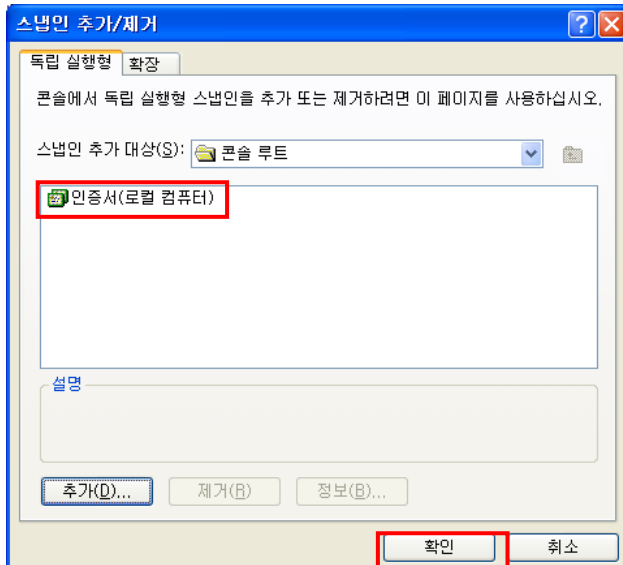
6. 컴퓨터 선택에서 로컬 컴퓨터 선택 후 마침



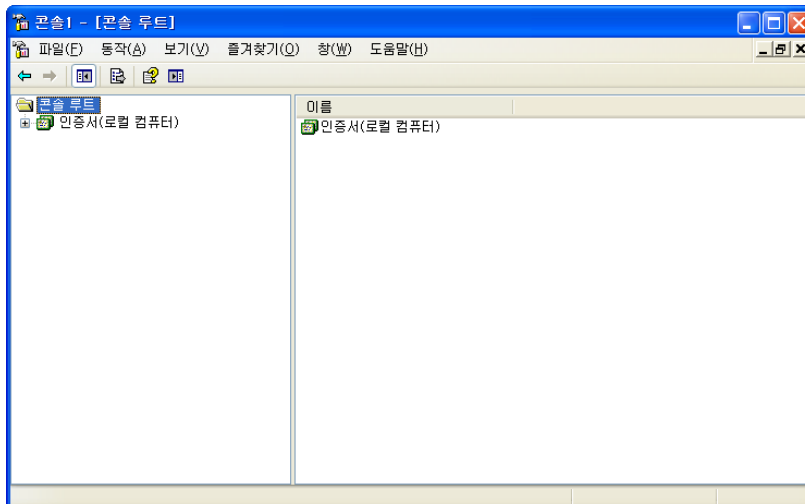
7. 독립 실행형 스냅인 추가에서 닫기 클릭



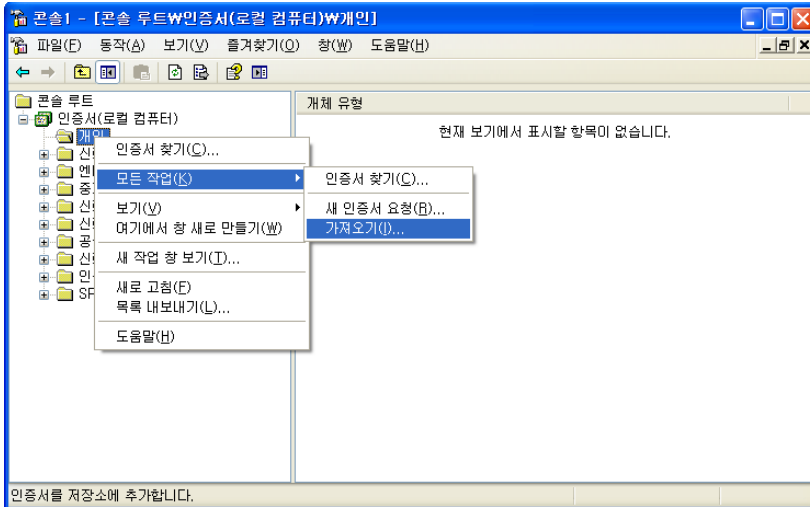
8. 스냅인 추가/제거에서 인증서 항목이 추가된 것을 확인 후 확인 클릭



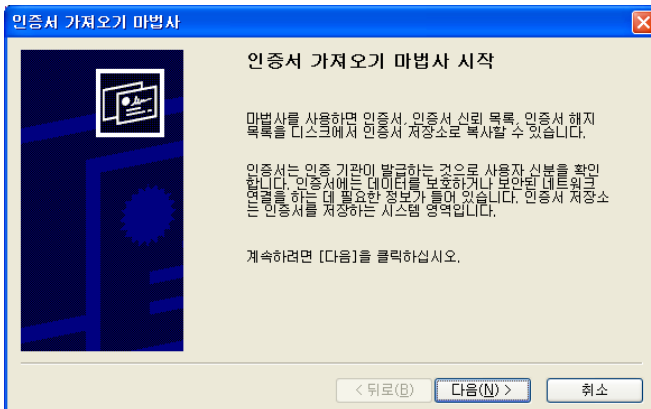
9. 콘솔창에서 인증서 항목이 추가된 것을 확인



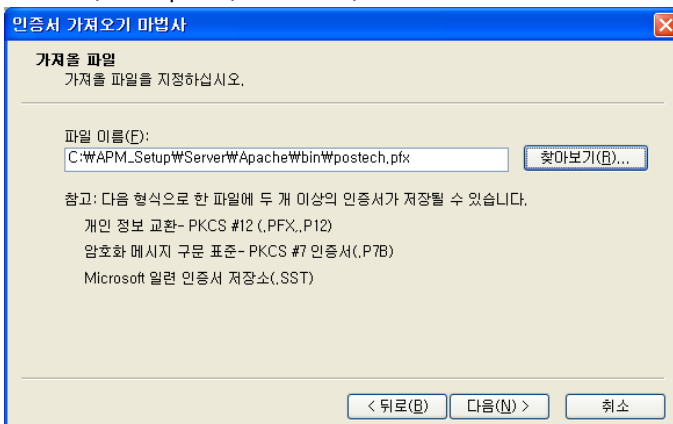
10. 콘솔 루트 -> 인증서 -> 개인 항목에서 마우스 오른쪽 클릭, 모든 작업 -> 가져오기 선택



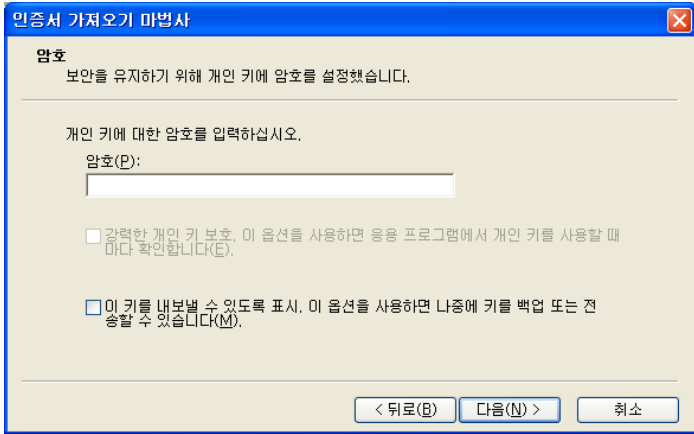
11. 다음 클릭



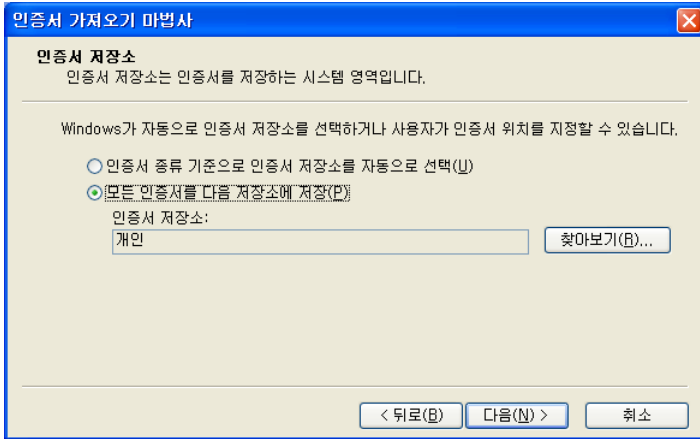
12. 보내드린 pfx 파일을 선택



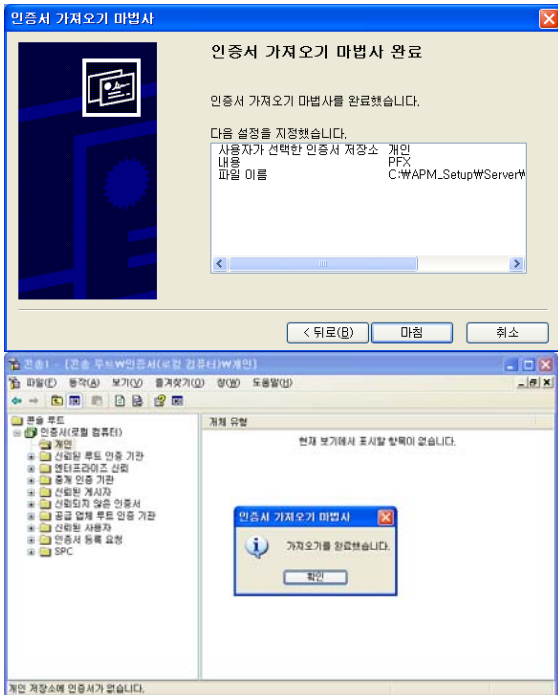
13. 개인키에 대한 암호 입력(암호 : 00100243) 후 다음 클릭



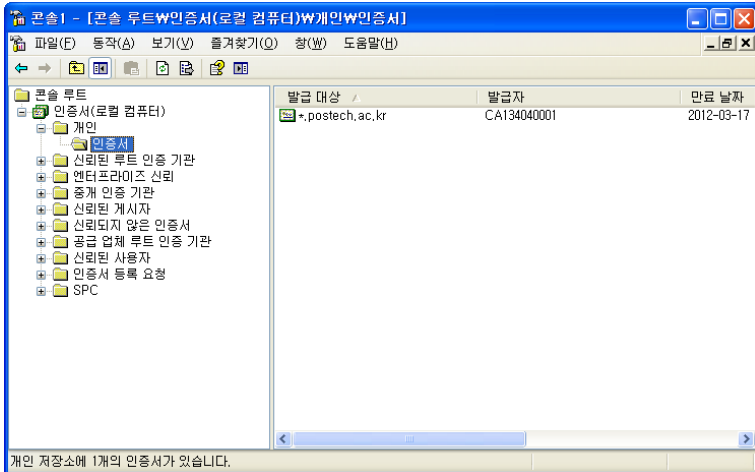
14. 모든 인증서를 다음 저장소에 저장 선택 후 다음 클릭



15. 마침 클릭하여 가져오기 완료

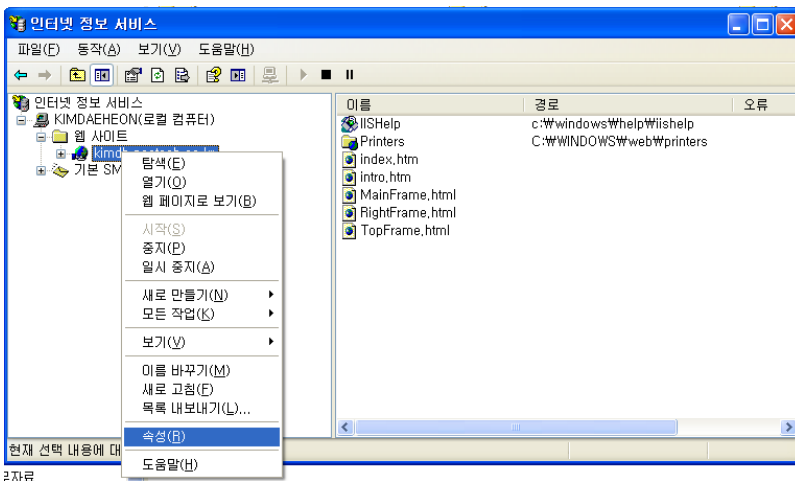


16. *.postech.ac.kr 인증서가 설치되어 있는지 확인

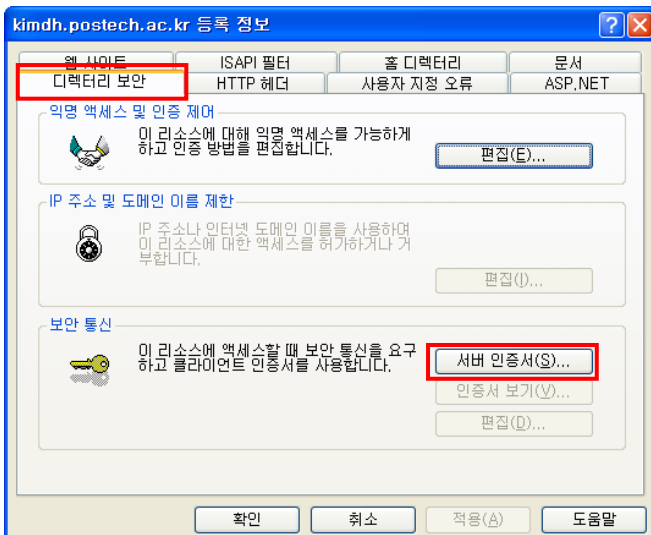


[인증서 설치 후 웹사이트에 적용]

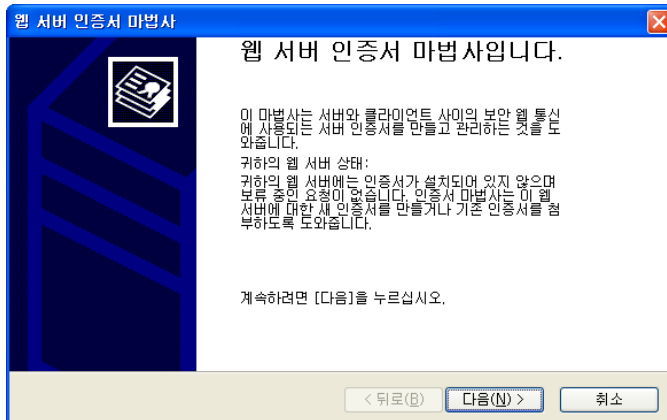
1. 인터넷 정보 서비스 실행(IIS) 후 해당 웹사이트 선택 후 마우스 오른쪽 클릭하여 속성 선택



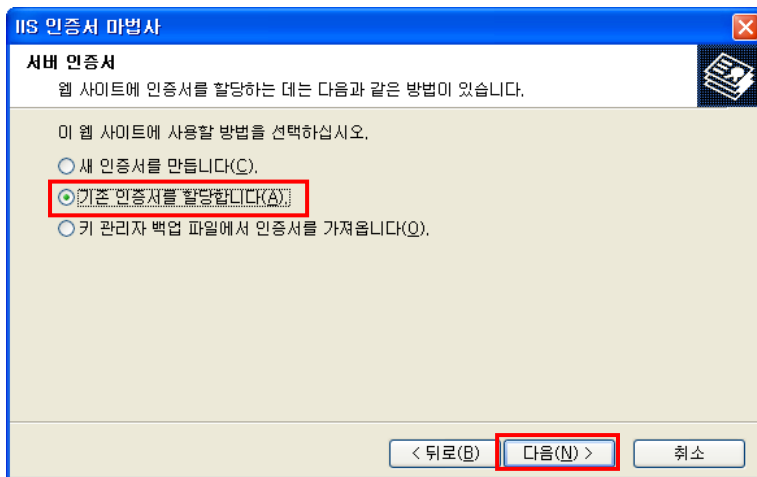
2. 등록정보에서 디렉터리 보안 탭에서 서버 인증서 클릭



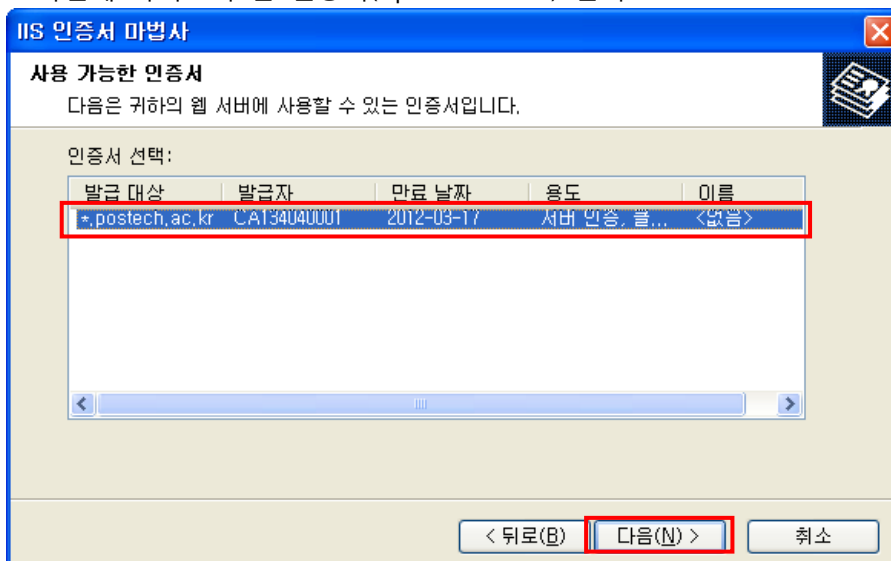
3. 웹 서버 인증서 마법사에서 다음 클릭



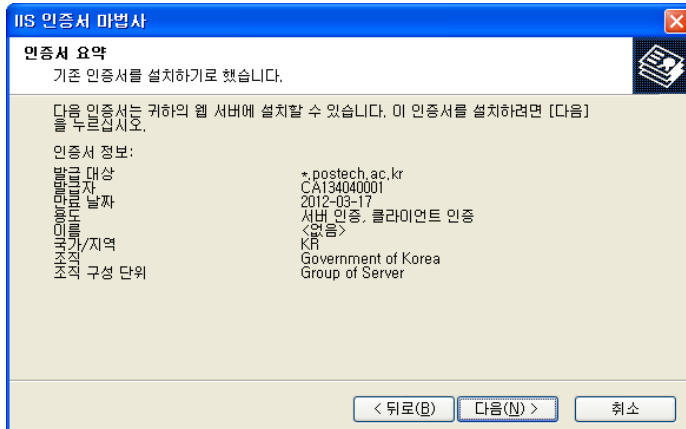
4. IIS 인증서 마법사에서 '기존 인증서를 할당합니다.' 선택 후 다음 클릭



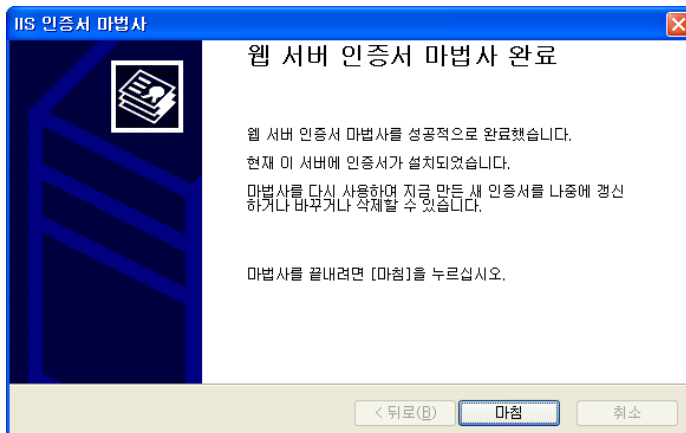
5. 사전에 가져오기 한 인증서(*.postech.ac.kr) 선택



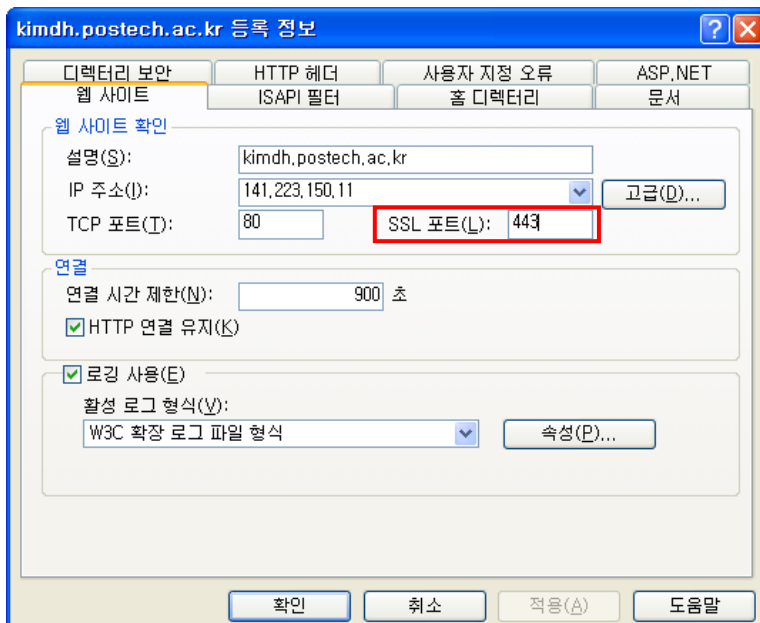
6. 다음 클릭



7. 마법사 완료하여 인증서 적용 완료

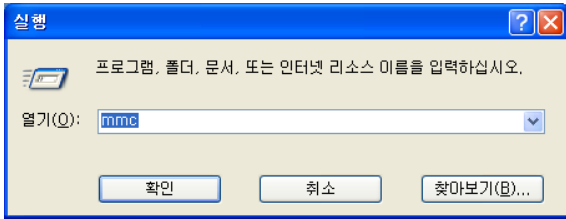


8. 등록정보의 웹사이트 탭에서 SSL 포트 정보 확인

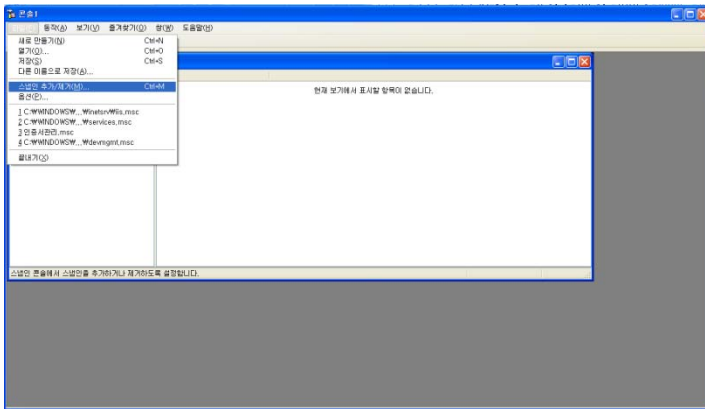


[루트 인증서와 체인 인증서 설치]

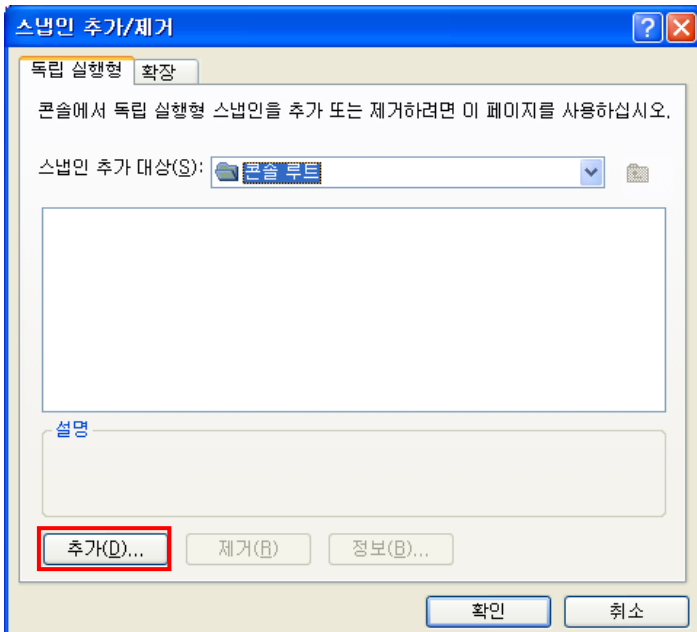
1. 시작->실행->윈도우관리자 콘솔(mmc) 실행



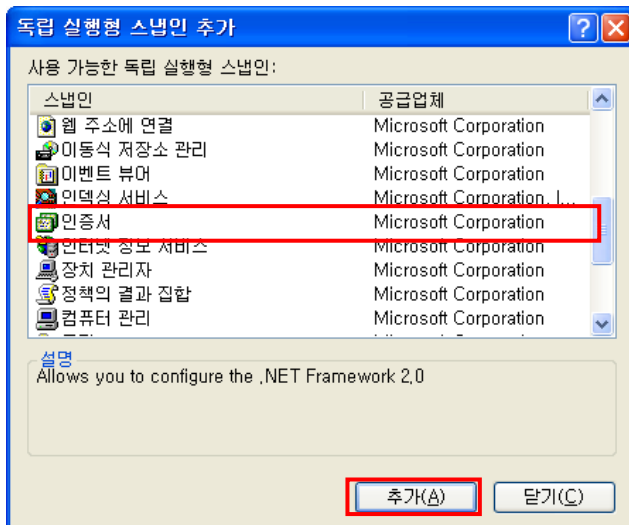
2. 콘솔창이 열리면 파일 -> 스냅인 추가/제거 선택



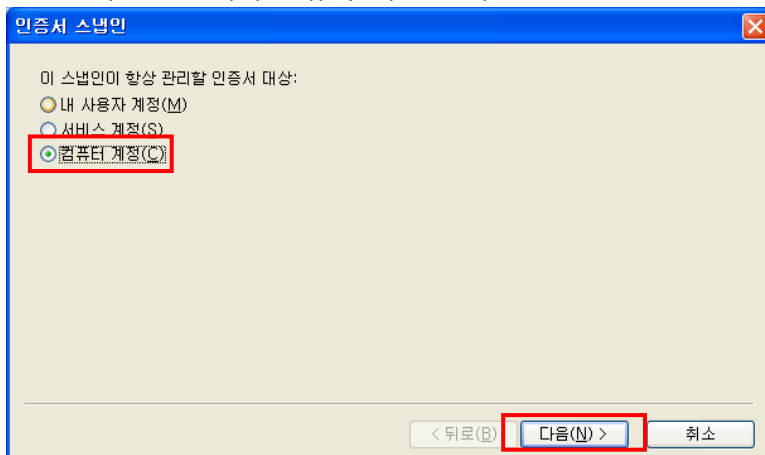
3. 스냅인 추가/제거에서 추가 클릭



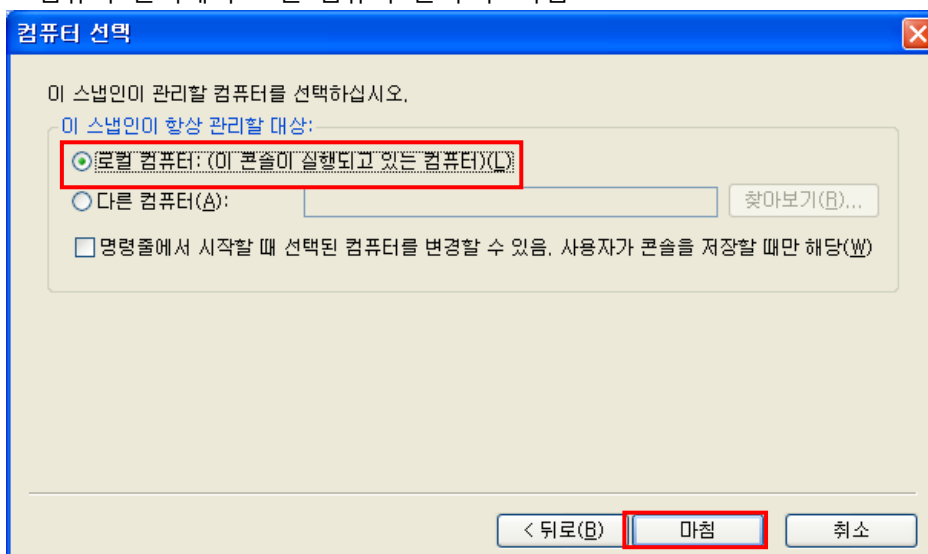
4. 독립 실행형 스냅인 추가에서 인증서 추가



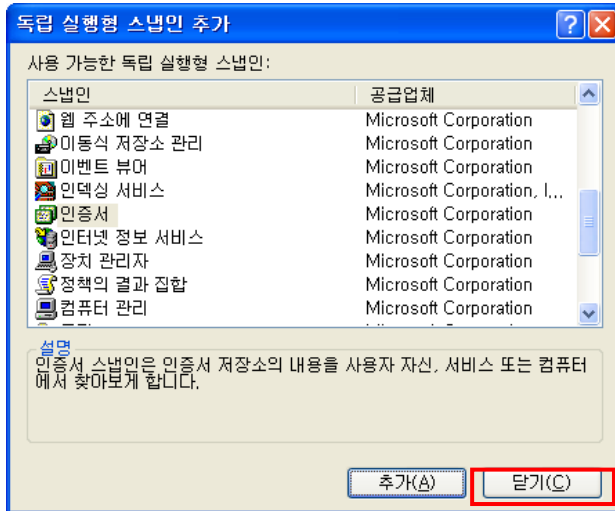
5. 인증서 스냅인에서 컴퓨터 계정 선택



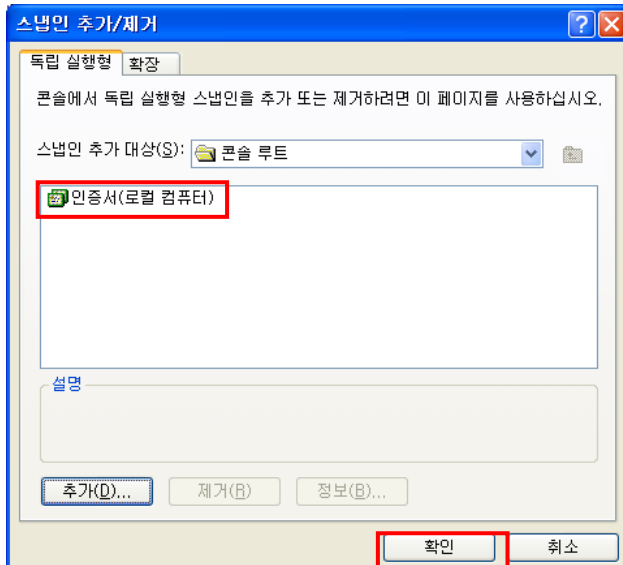
6. 컴퓨터 선택에서 로컬 컴퓨터 선택 후 마침



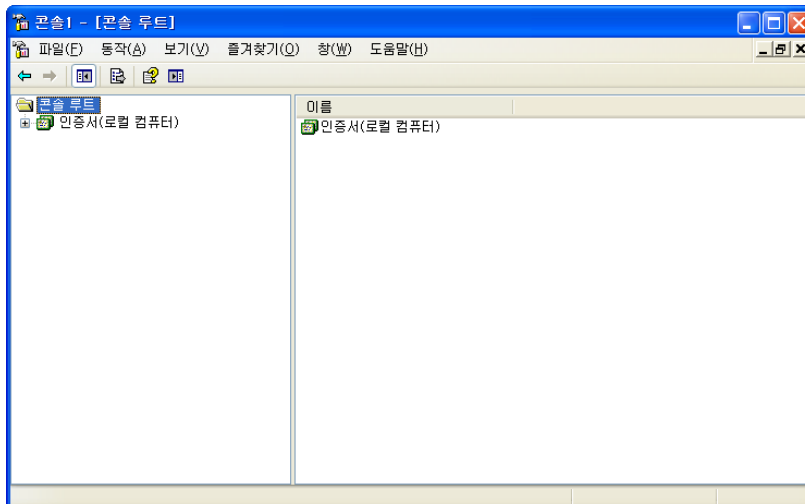
7. 독립 실행형 스냅인 추가에서 닫기 클릭



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

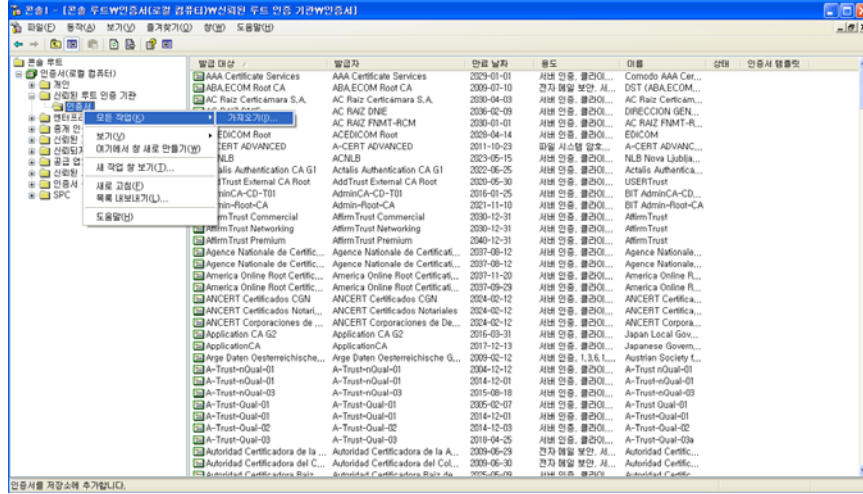


9. 콘솔창에서 인증서 항목이 추가된 것을 확인

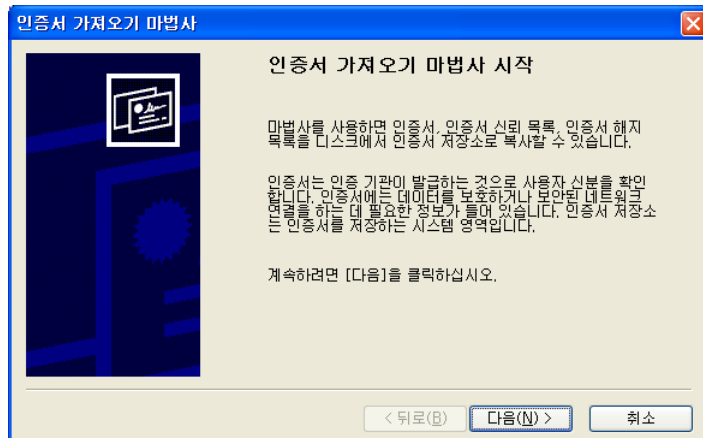


10. 루트인증서를 설치

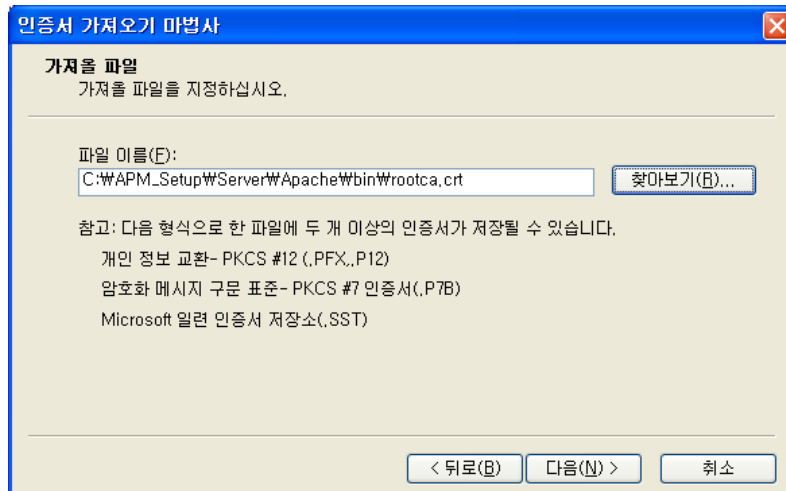
신뢰된 루트 인증 기관 -> 인증서 항목에서 마우스 오른쪽 클릭 -> 모든 작업 -> 가져오기 선택



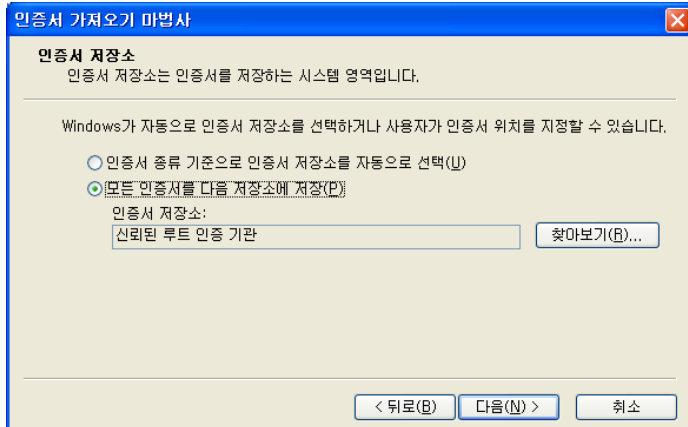
11. 다음 클릭



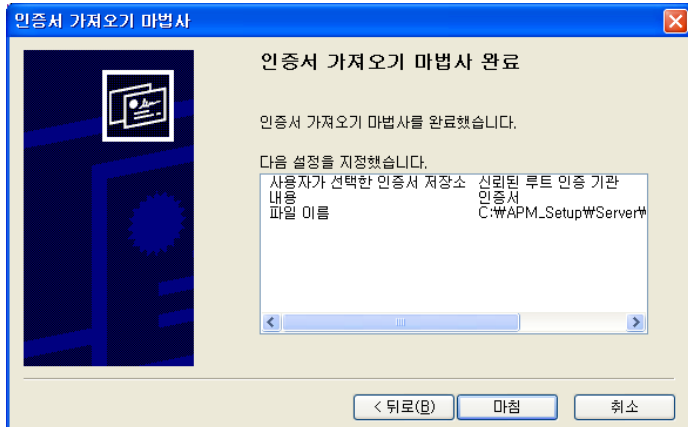
12. 인증서와 같이 보낸 rootca.crt 을 선택하여 다음 클릭



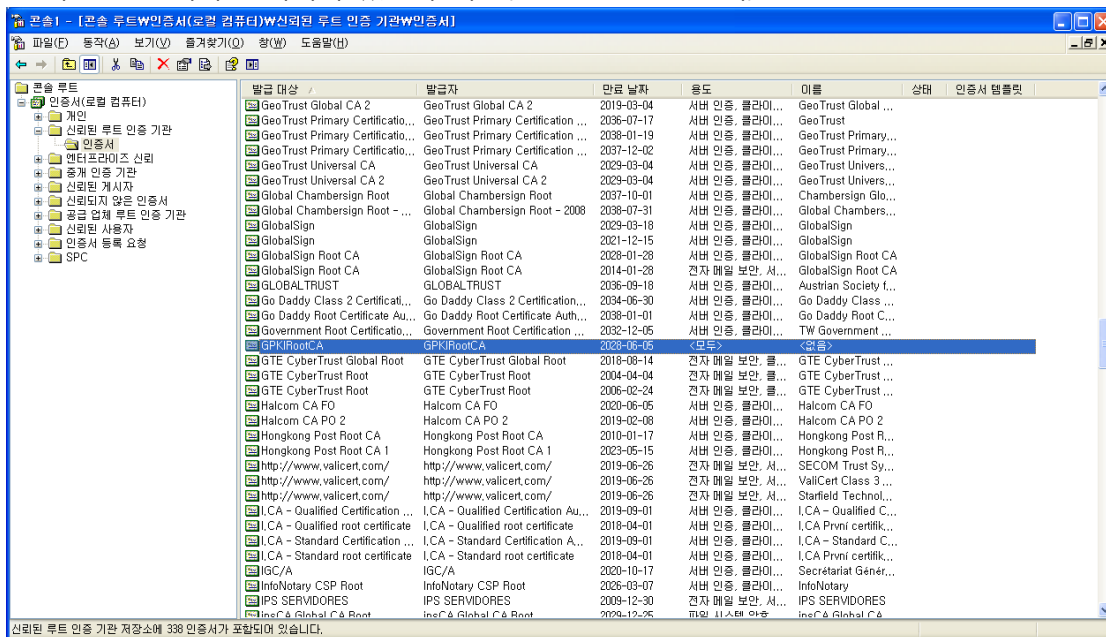
13. 모든 인증서를 다음 저장소에 저장을 선택하고 인증서 저장소가 신뢰된 루트 인증 기관인지 확인하여 다음 클릭



14. 마침 클릭하여 루트 인증서 설치 완료

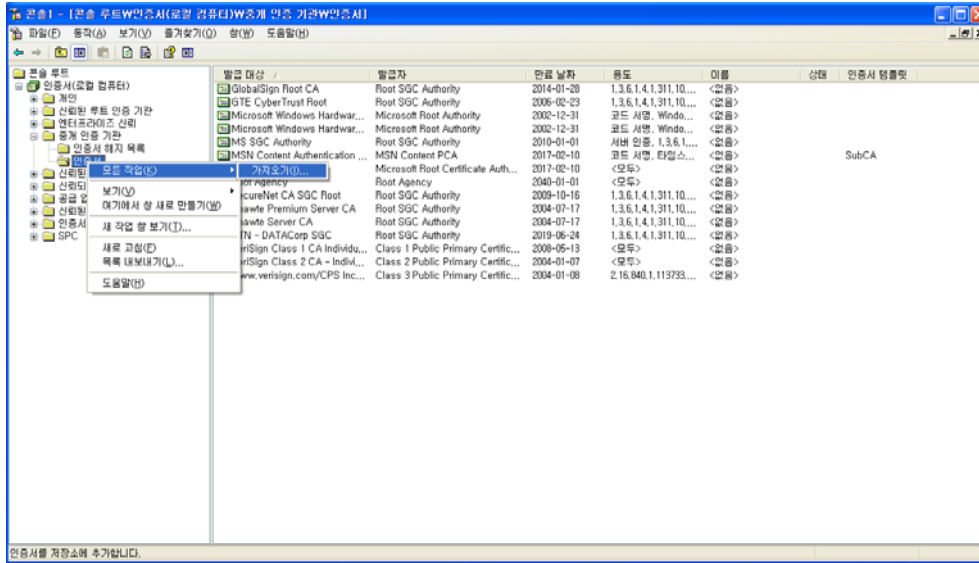


15. 루트 인증서가 설치되어 있는지 확인(GPKIRootCA 인증서)

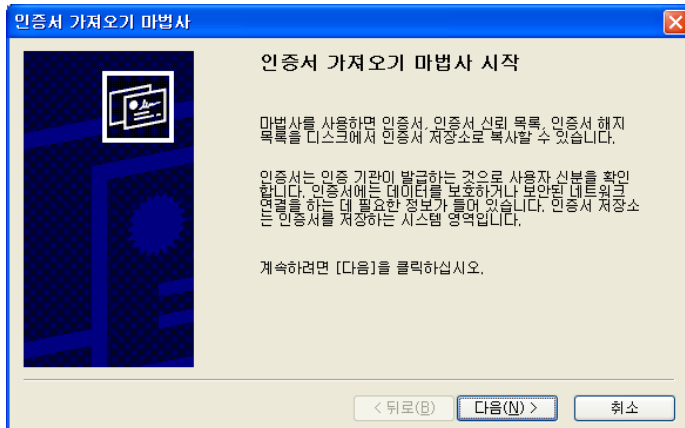


16. 체인 인증서 설치

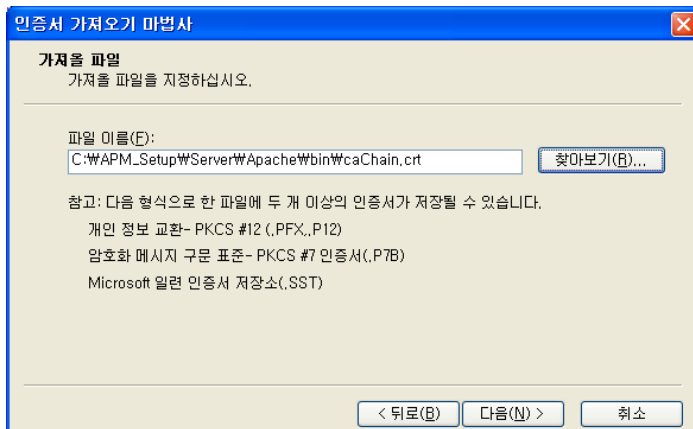
중개 인증 기관 -> 인증서 항목에서 마우스 오른쪽 클릭 -> 모든 작업 -> 가져오기 선택



17. 다음 클릭

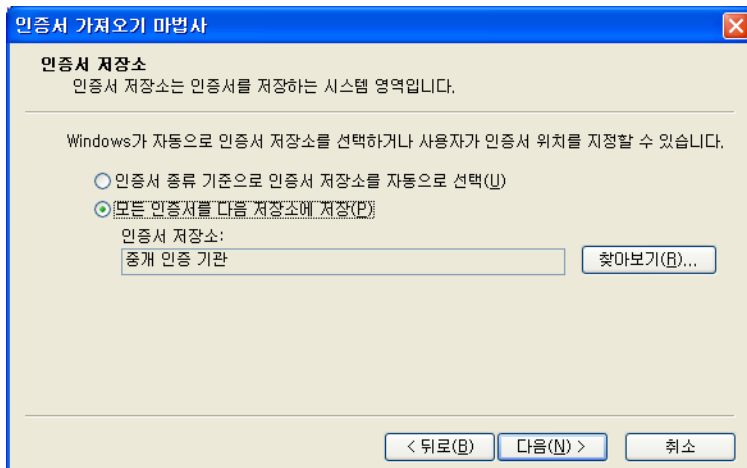


18. 인증서와 같이 보낸 caChain.crt 파일 선택

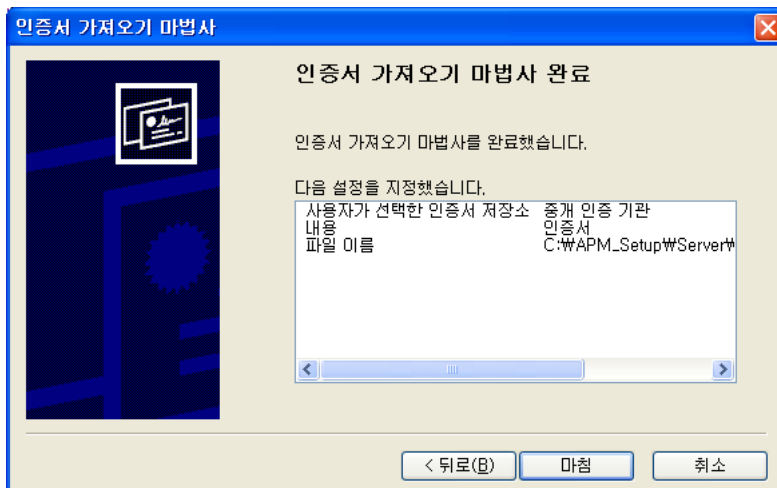


19. 모든 인증서를 다음 저장소에 저장 선택하여 인증서 저장소가 중개 인증 기관인지 확인하여

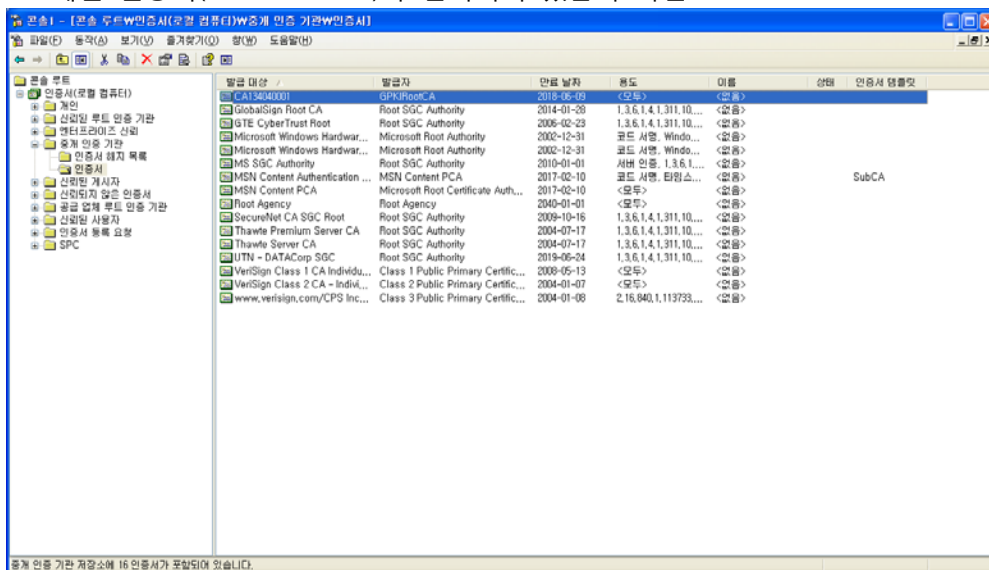
다음 클릭



20. 마침 클릭하여 체인인증서 가져오기 완료

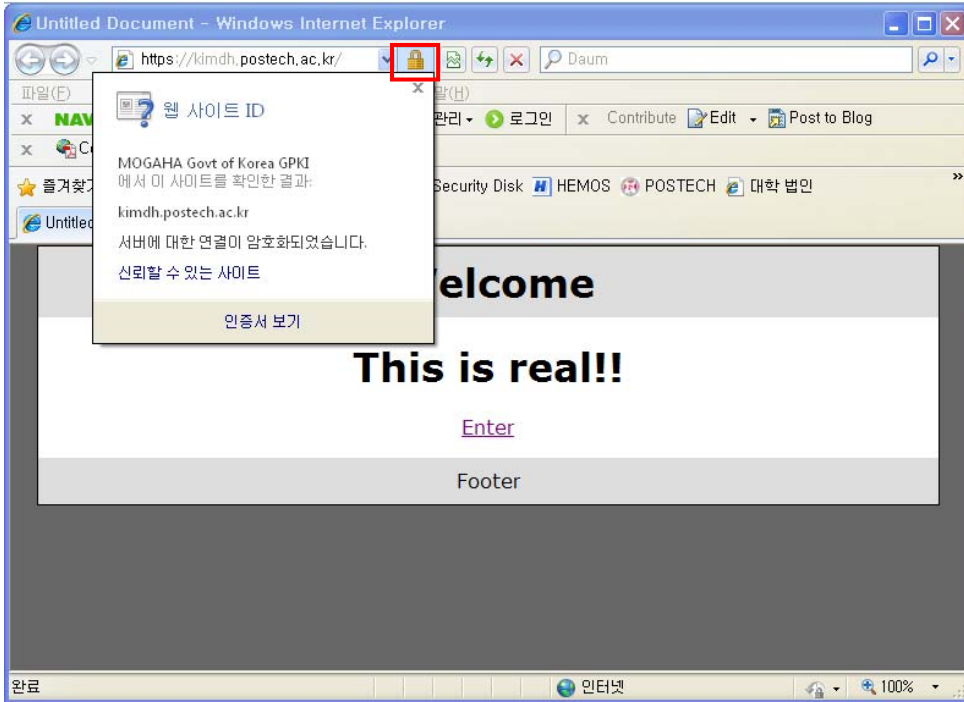


21. 체인 인증서(CA134040001)가 설치되어 있는지 확인



[인증서 설치 후 설치 확인]

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



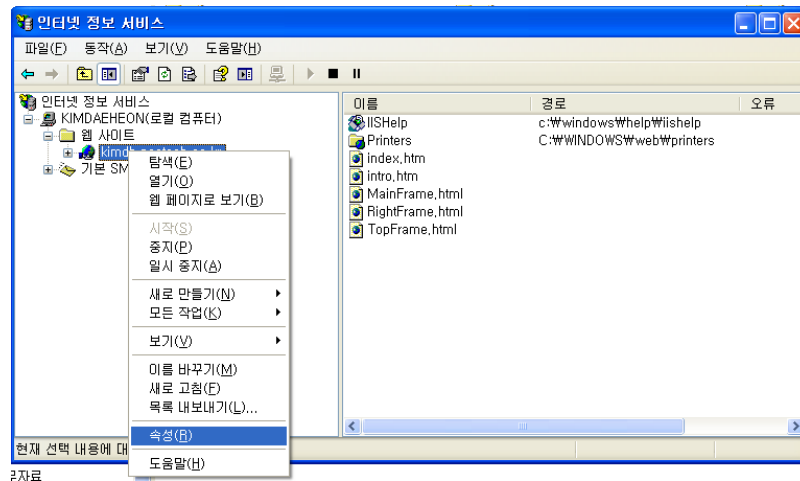
※ SSL 암호화 설정

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.

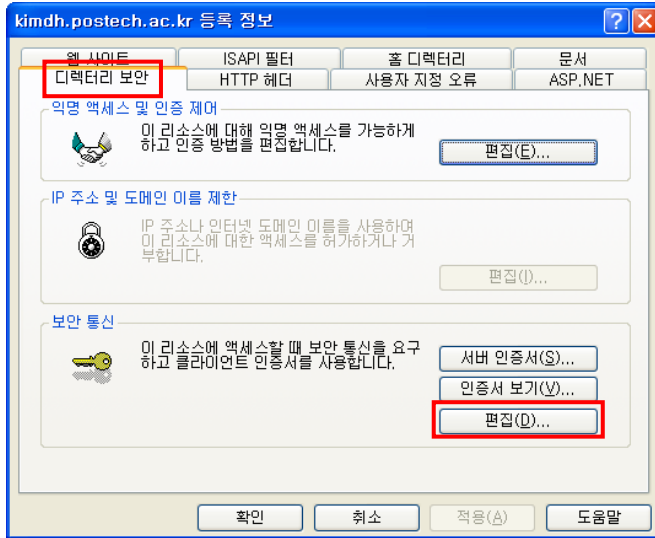
[https 리다이렉션 방법]

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

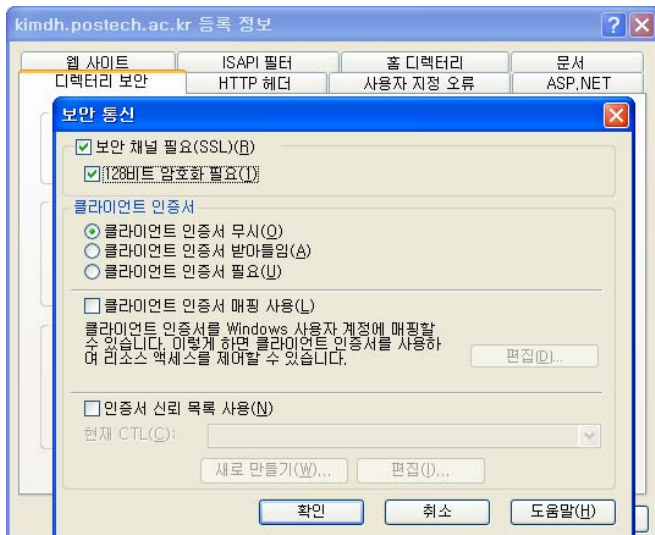
1. 인터넷 정보 서비스 실행(IIS) 후 해당 웹사이트 선택 후 마우스 오른쪽 클릭하여 속성 선택



2. 등록정보에서 디렉터리 보안 탭에서 편집 클릭



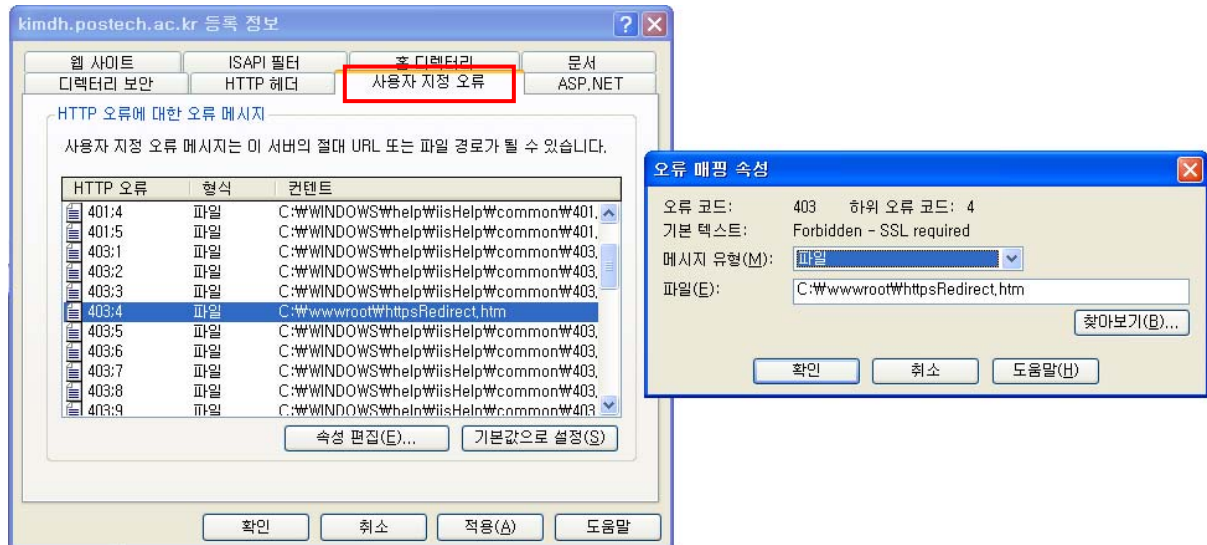
3. 보안 채널 필요(SSL) 체크 -> 128 비트 암호화 필요 체크, 그 외 설정은 그대로 둬



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>
```

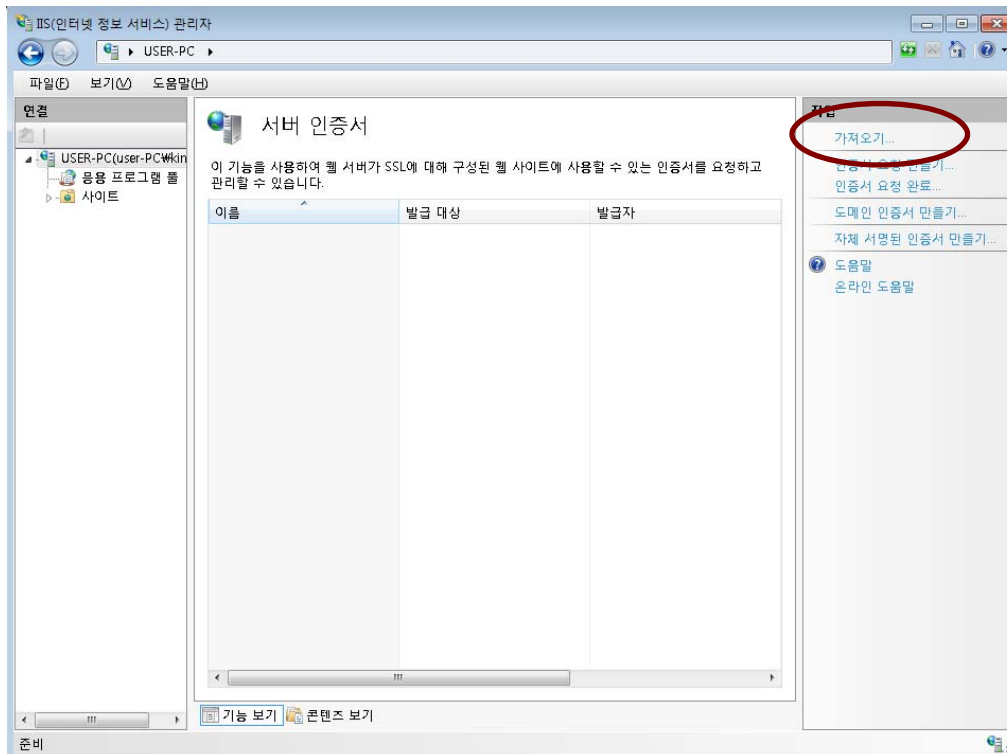
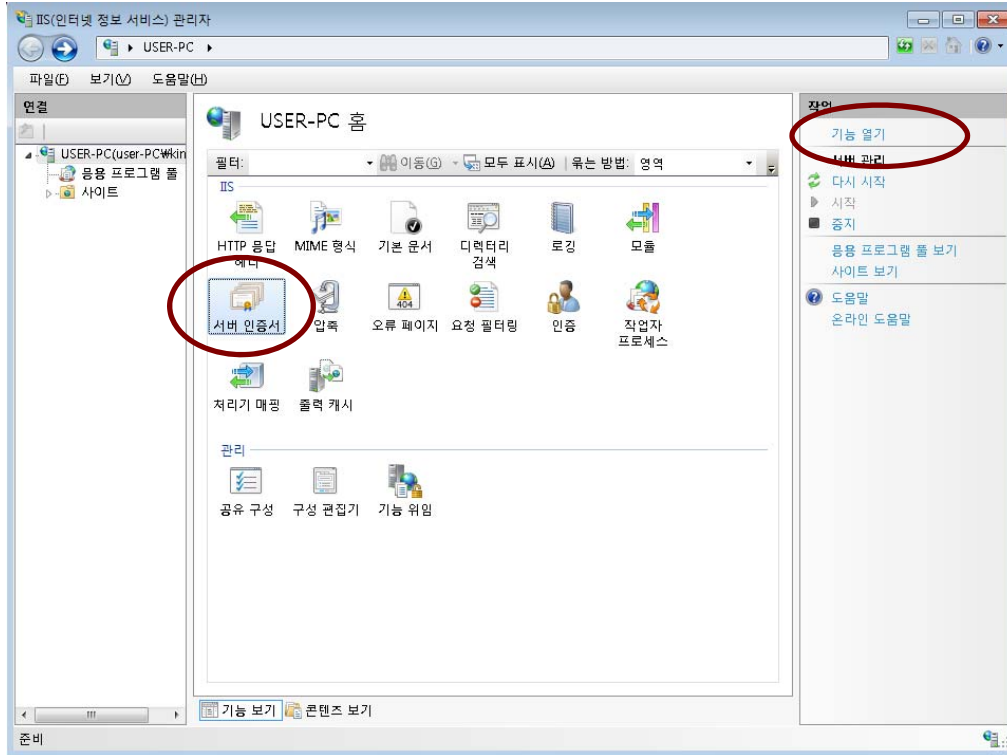
5. 등록정보의 사용자 지정 오류 탭에서 403;4 오류 메시지를 선택하여 작성한 httpRedirect.htm 로 지정하여 확인



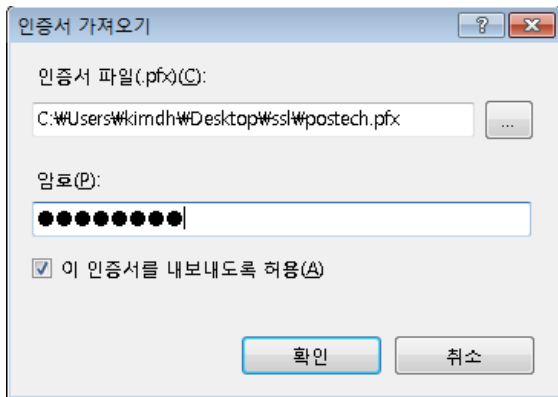
VII. IIS 7.0 및 7.5 SSL 인증서 설치

[SSL 인증서 가져오기]

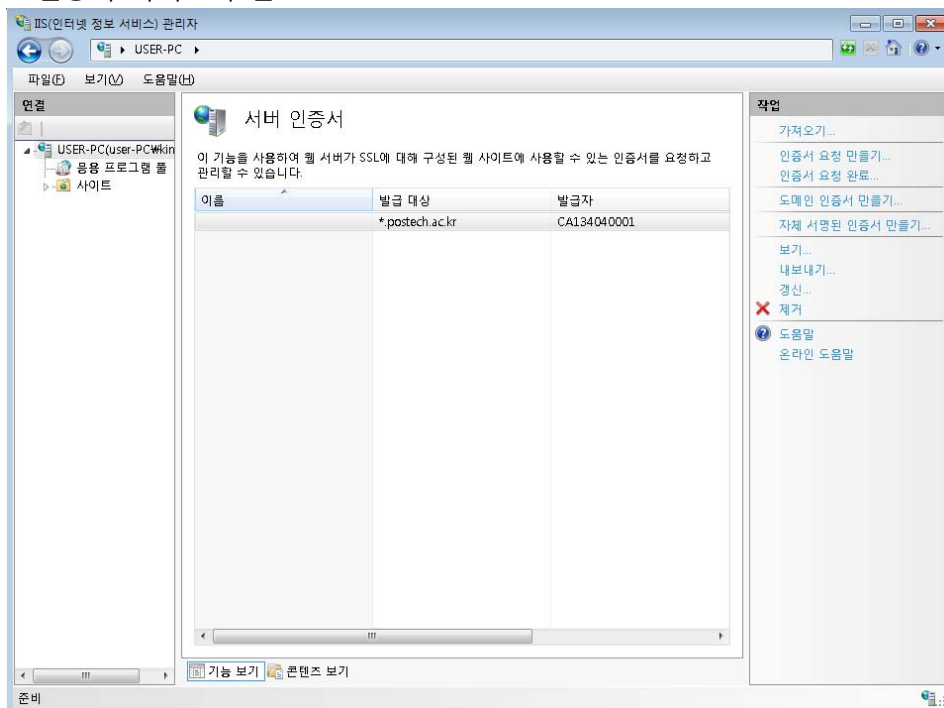
1. [관리도구]→[IIS(인터넷 정보 서비스) 관리자]→[서버 인증서]→우측 작업 탭에서 기능열기→가져오기



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

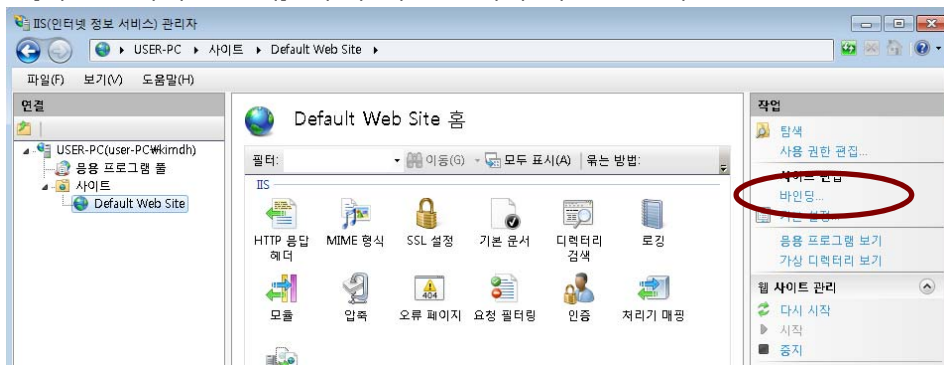


3. 인증서 가져오기 완료



[인증서 설치 후 웹사이트에 적용]

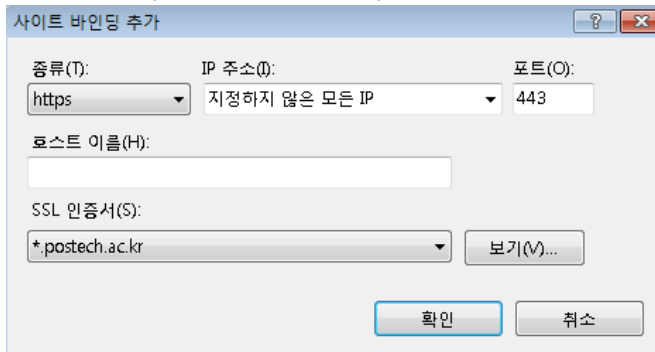
1. [해당 웹사이트 선택]→우측 작업 탭에서 바인딩 선택



2. 사이트 바인딩 추가



3. 종류 : https, SSL 인증서 : *.postech.ac.kr 선택

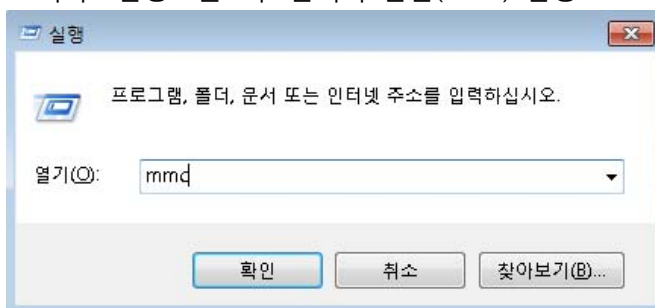


4. 인증서 적용 완료

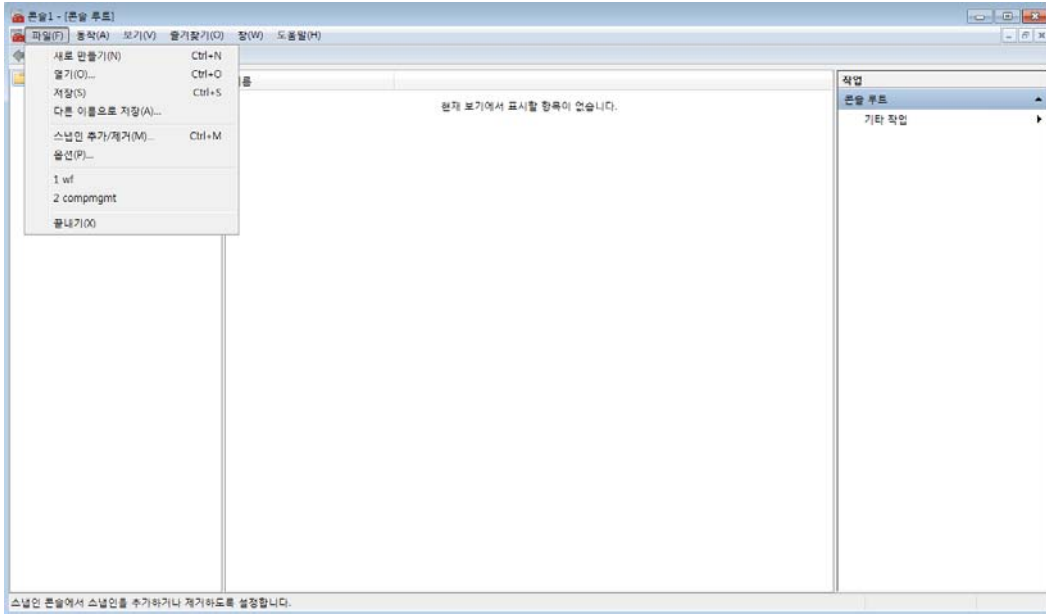


[루트 인증서와 체인 인증서 설치]

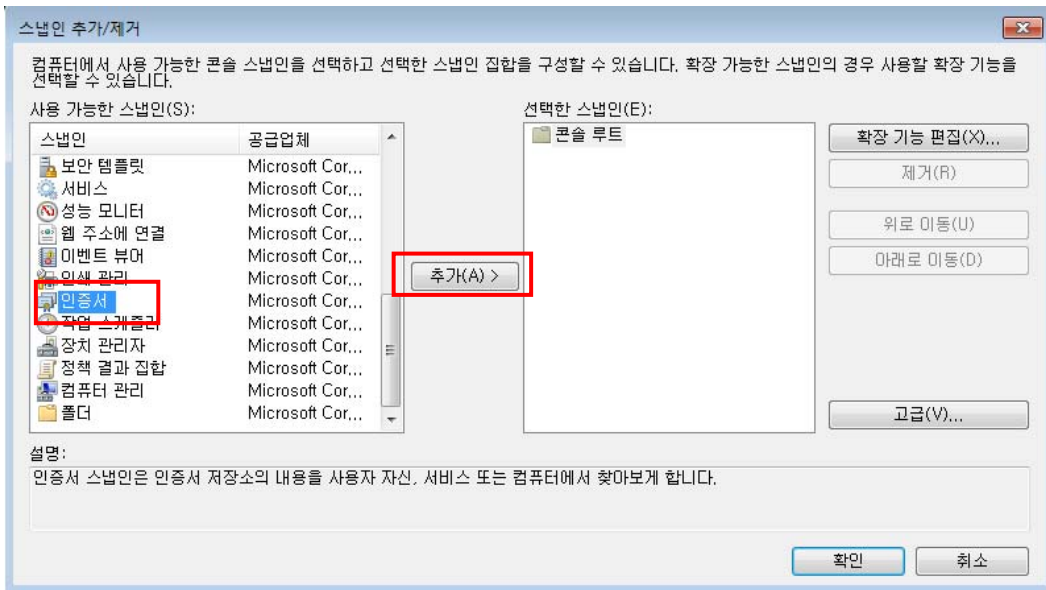
1. 시작→실행→윈도우 관리자 콘솔(mmc) 실행



2. 콘솔 창이 열리면 파일→ [스냅인 추가/제거] 선택



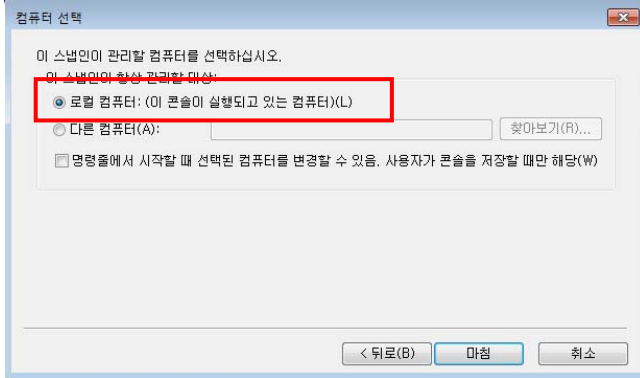
3. 스냅인 창에서 인증서 추가



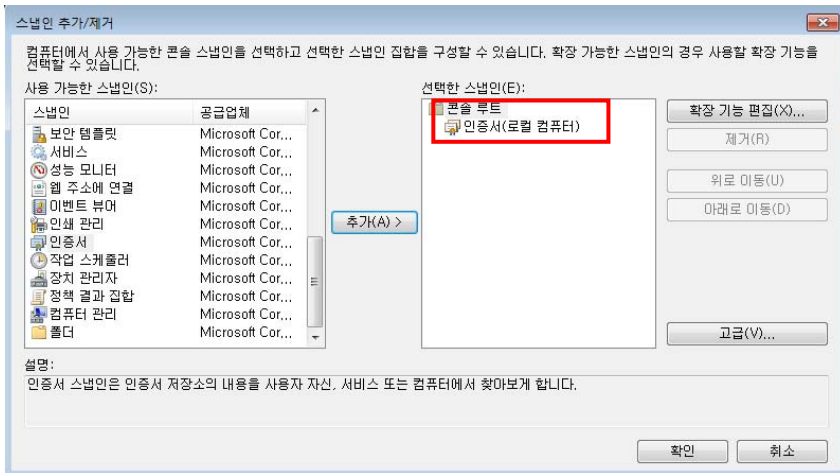
4. 인증서 스냅인에서 [컴퓨터 계정] 선택



5. 로컬 컴퓨터 선택 후 마침

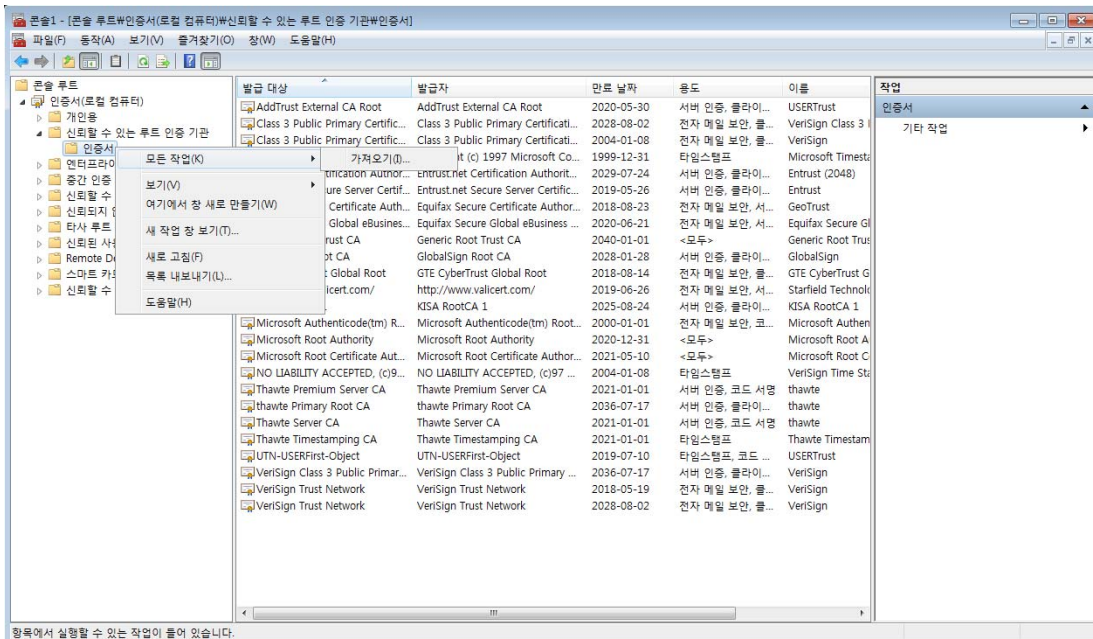


6. 선택한 스냅인 항목에서 인증서 항목 확인

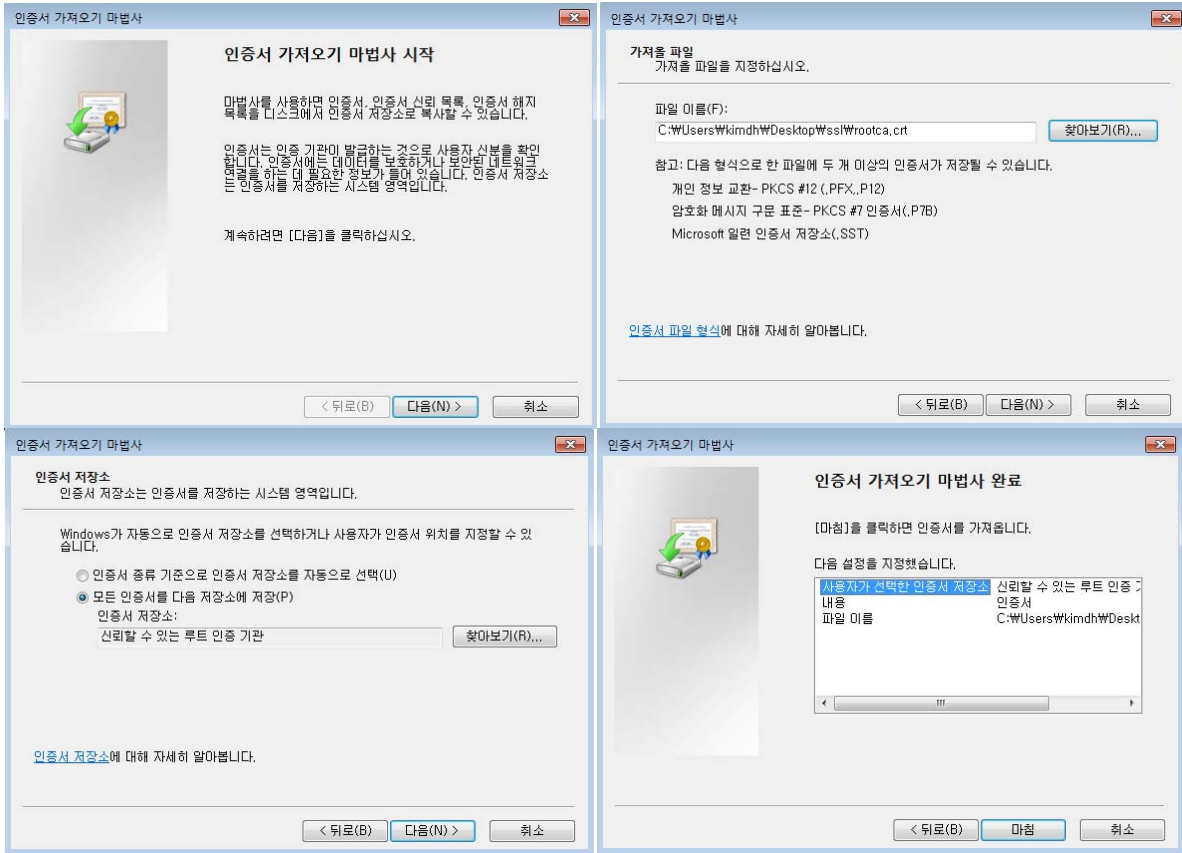


7. 루트인증서 설치

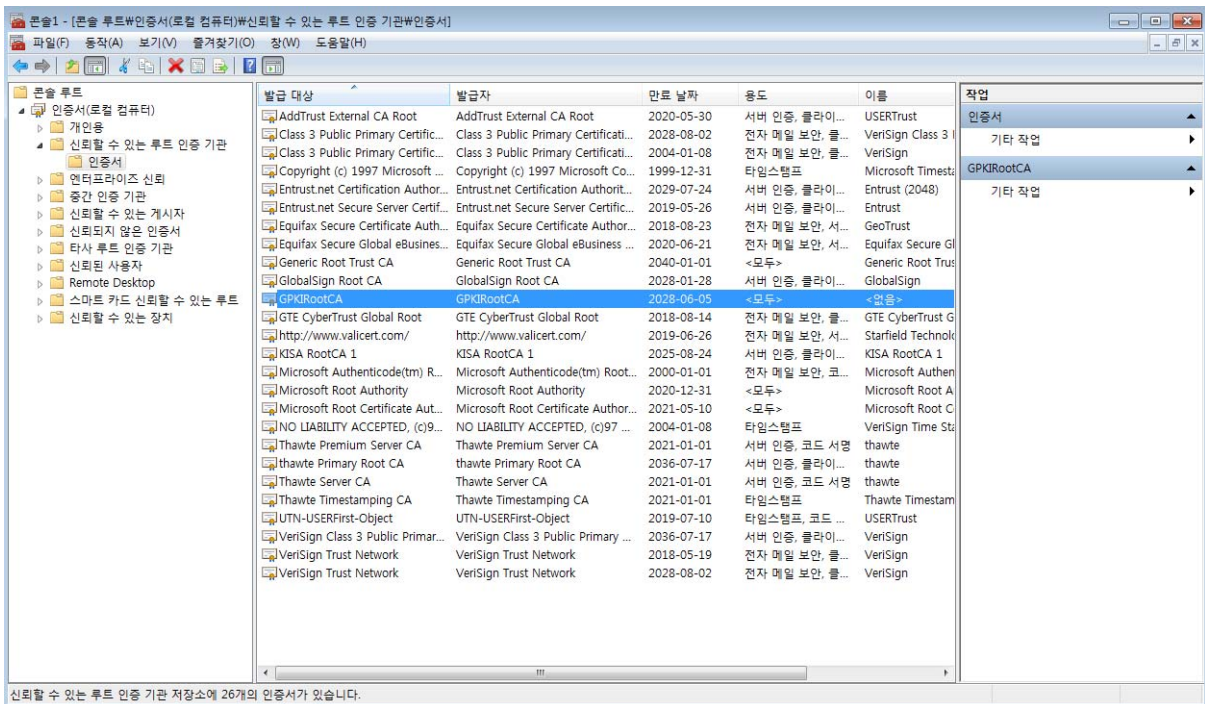
신뢰할 수 있는 루트 인증기관→인증서 선택후 마우스 오른쪽 클릭→모든 작업→가져오기



8. 인증서와 같이 보낸 rootca.crt 파일 선택

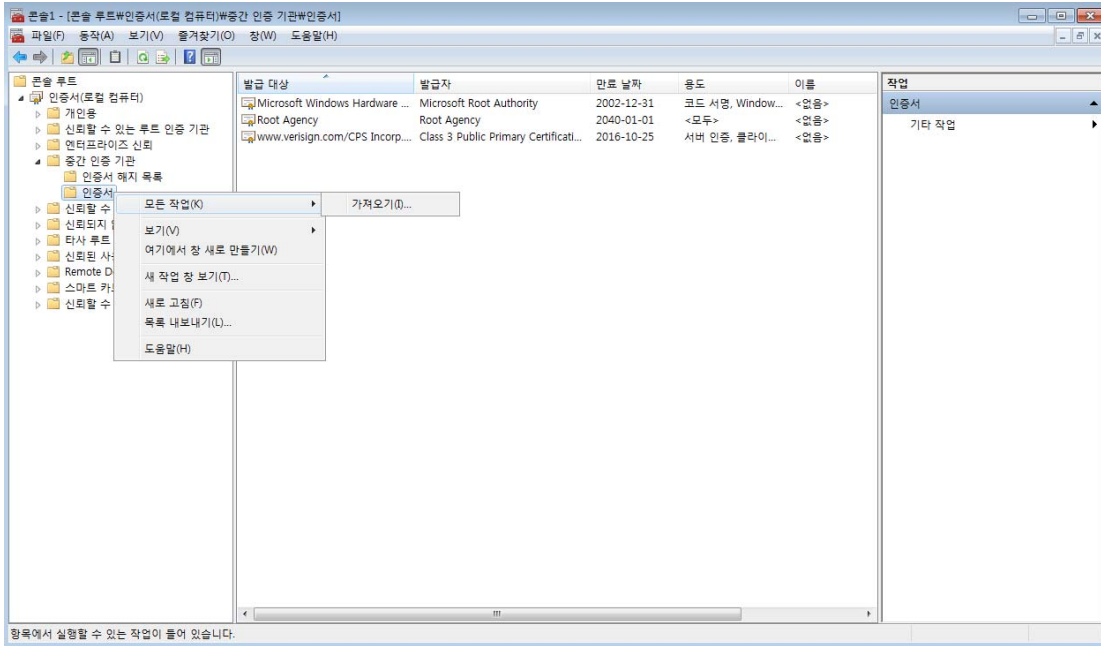


9. 설치 완료된 루트 인증서(GPKIRootCA)

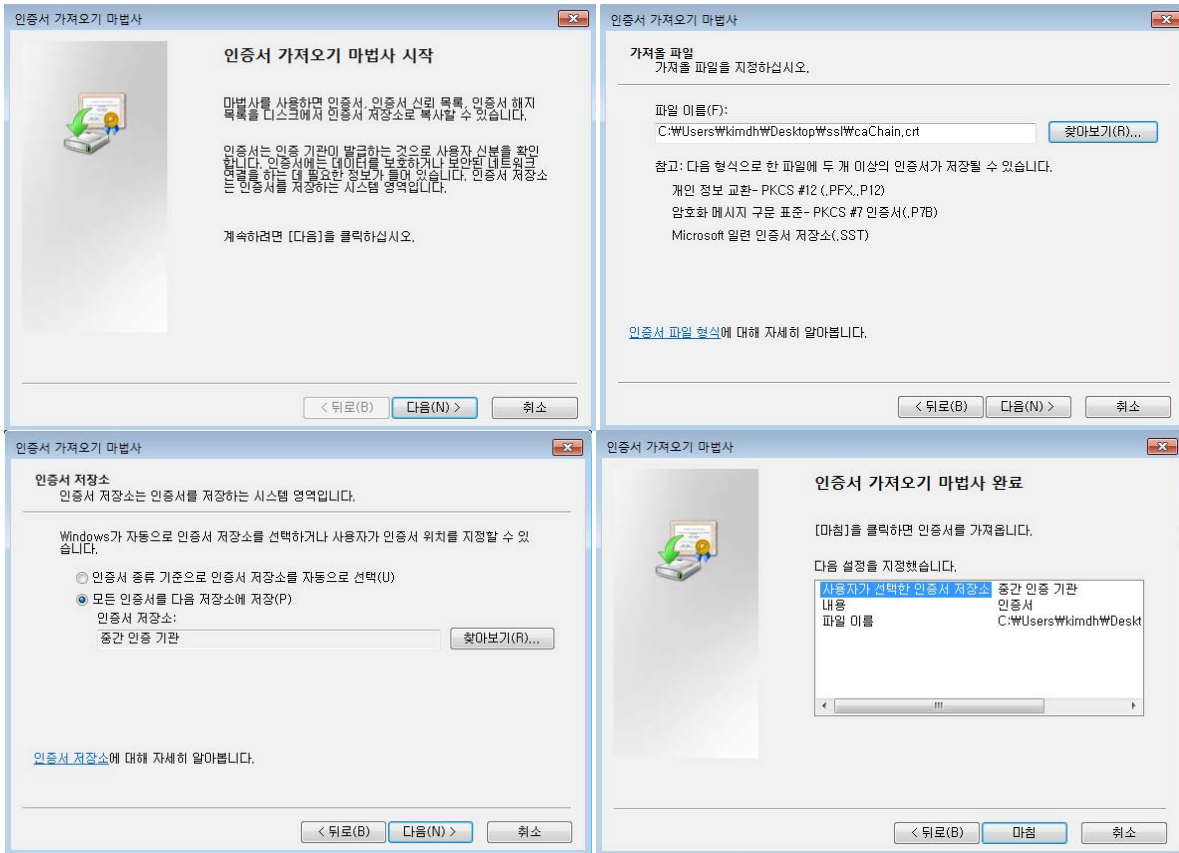


10. 체인 인증서 설치하기

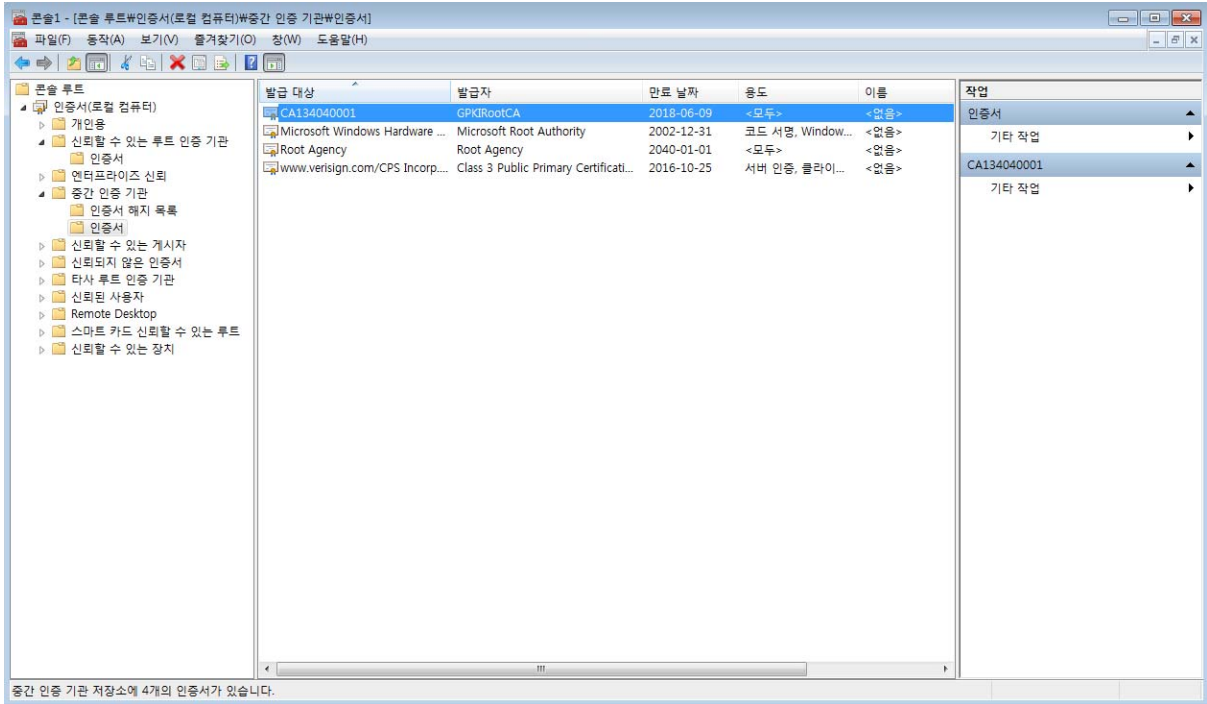
중간 인증 기관 → 인증서 선택 후 마우스 오른쪽 클릭 → 모든 작업 → 가져오기



11. 인증서와 같이 보낸 caChain.crt 파일 선택

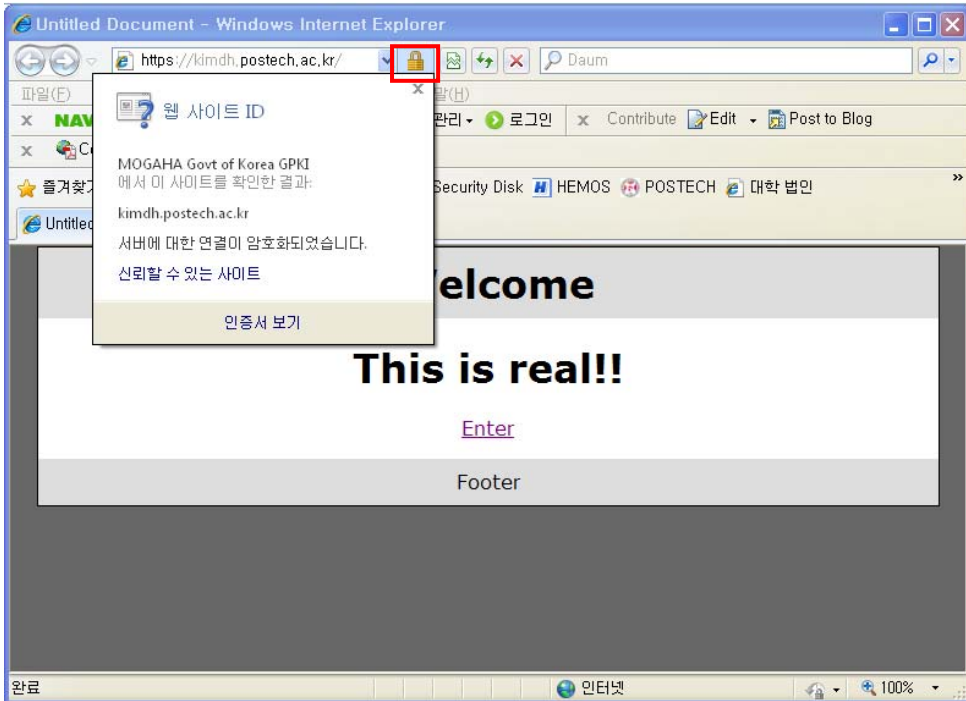


12. 설치 완료된 체인 인증서(CA134040001)



[인증서 설치 후 설치 확인]

1. <https://> 로 접근하여 웹페이지가 올바르게 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 하

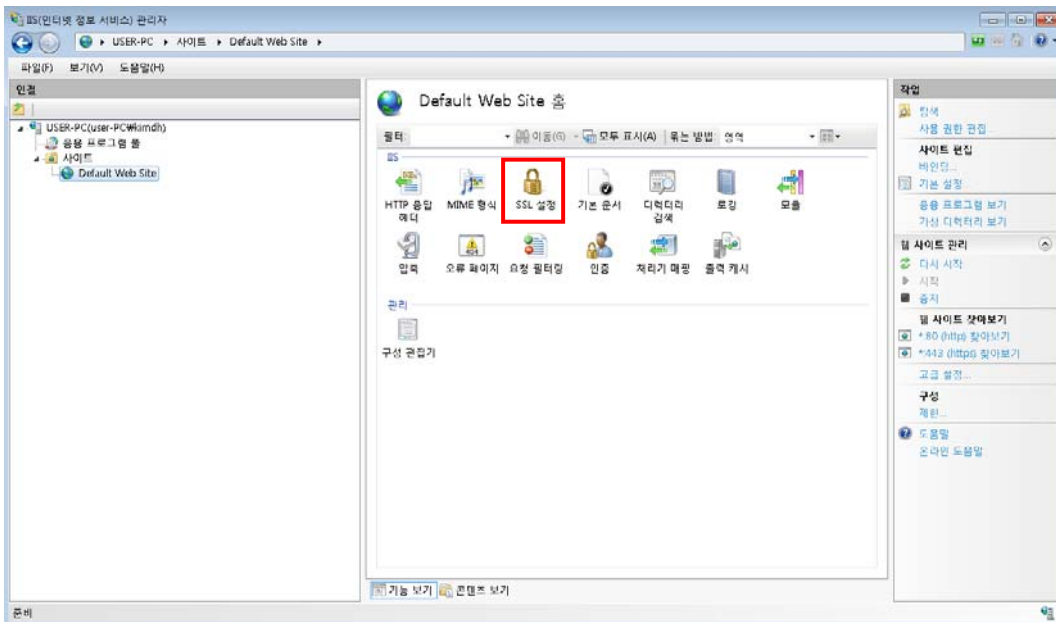
기 때문에 http 로의 접속을 차단하는 대신 https 로 전환시켜 주어야 합니다.

[https 리다이렉션 방법]

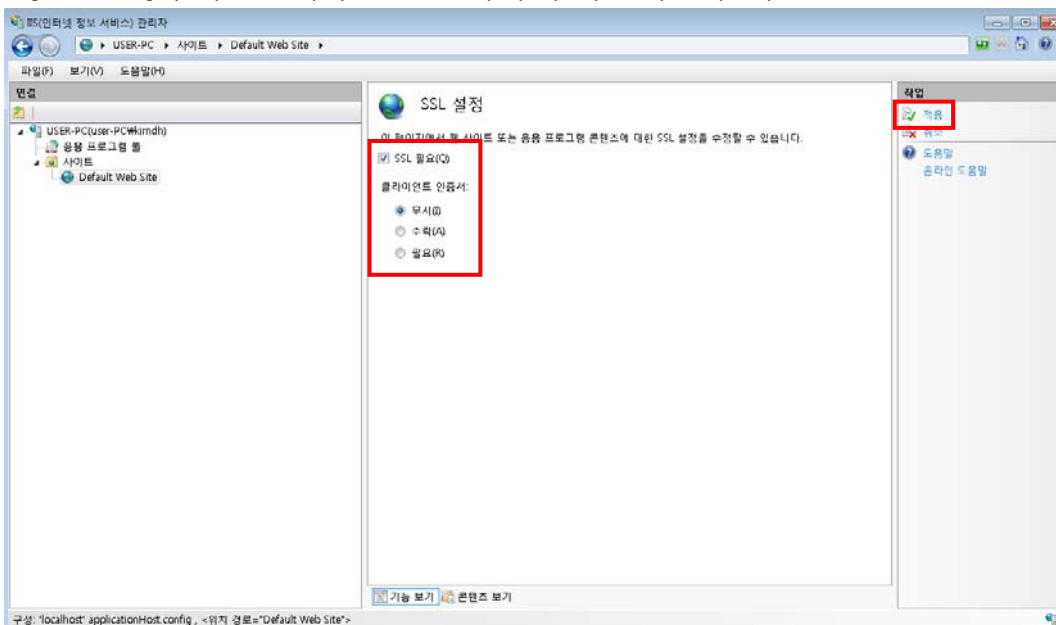
SSL 암호화를 설정하면 http 로의 접근이 차단되어 오류페이지를 호출하게 됩니다. 이때 호출하는 오류페이지를 https 로 리다이렉트 시켜주는 페이지로 대체하여 자동으로 전환하도록 합니다.

1. SSL 설정 적용

해당 웹사이트를 선택하여 [SSL 설정] 더블클릭



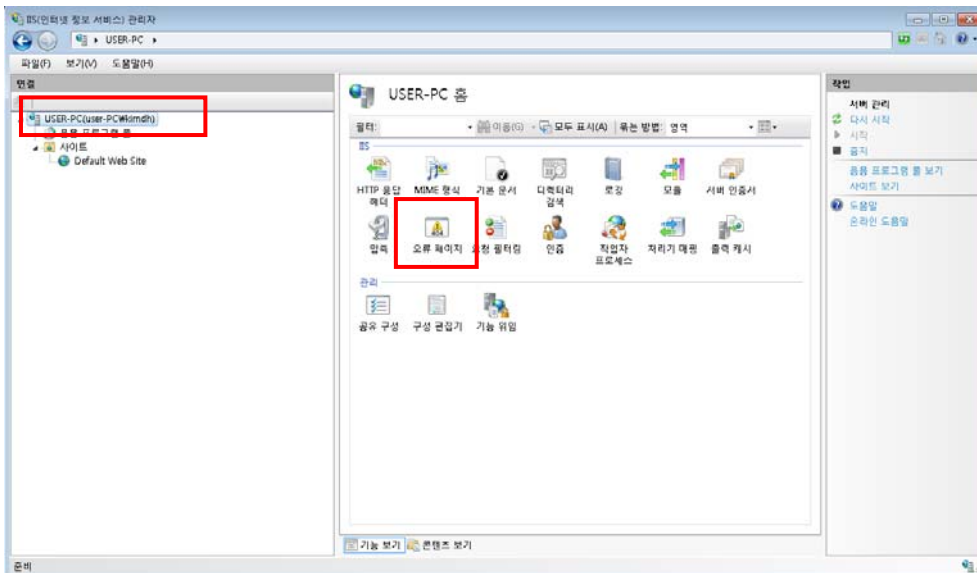
2. [SSL 필요]에 체크, 클라이언트 인증서 무시 체크 확인 후 적용 완료



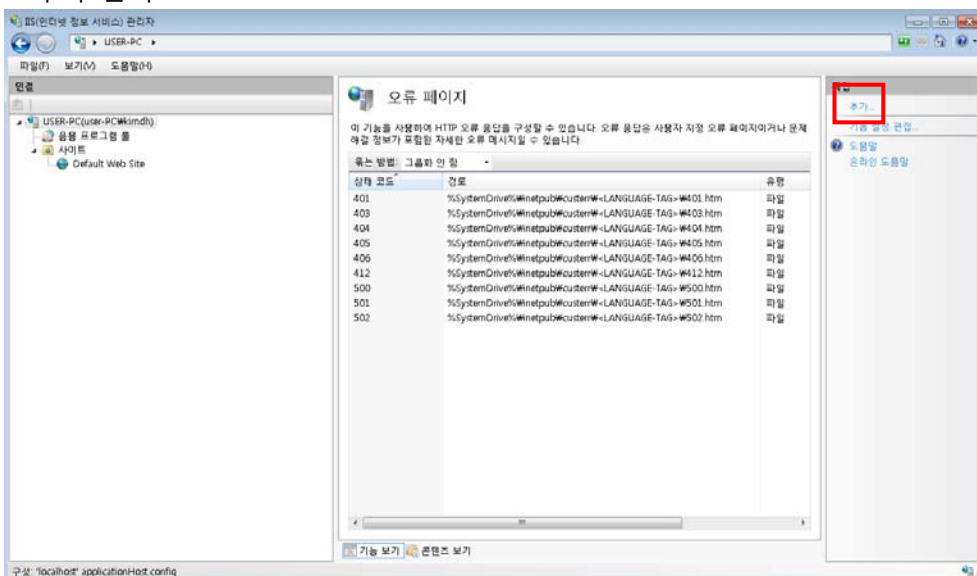
3. 아래와 같이 httpsRedirect.htm 파일을 생성하여 적당한 경로에 저장

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

4. [최상위 메뉴]→[오류 페이지]



5. 추가 클릭



6. 사용자 지정 오류 페이지 추가

상태코드 : 403.4

응답작업 : 오류 응답에 정적 파일의 콘텐츠 삽입(앞서 작성한 httpsRedirect.htm 선택)

사용자 지정 오류 페이지 추가

상태 코드(C):
403.4
예: 404 또는 404.2

응답 작업

오류 응답에 정적 파일의 콘텐츠 삽입(I)

파일 경로(F):
C:\inetpub\wwwroot\ko-KR\httpsRedirect.htm

클라이언트 언어로 된 오류 파일 반환 시도(T)

이 사이트에서 URL 실행(E)

URL(사이트 루트 기준)(U):
예: /ErrorPages/404.aspx

302 리디렉션으로 응답(R)

절대 URL(A):
예: http://www.contoso.com/404.aspx

7. 추가한 오류페이지 선택 후 [기능 설정 편집] 클릭

오류 페이지

이 기능을 사용하여 HTTP 오류 응답을 구성할 수 있습니다. 오류 응답은 사용자 지정 오류 페이지이거나 문제 해결 정보가 포함된 자세한 오류 메시지일 수 있습니다.

유는 방법: 그룹화 안 함

상태 코드	경로	유형
401	%SystemDrive%\inetpub\wwwroot\<LANGUAGE-TAG>\401.htm	파일
403	%SystemDrive%\inetpub\wwwroot\<LANGUAGE-TAG>\403.htm	파일
403.4	C:\inetpub\wwwroot\ko-KR\httpsRedirect.htm	파일
404	%SystemDrive%\inetpub\wwwroot\<LANGUAGE-TAG>\404.htm	파일
405	%SystemDrive%\inetpub\wwwroot\<LANGUAGE-TAG>\405.htm	파일
406	%SystemDrive%\inetpub\wwwroot\<LANGUAGE-TAG>\406.htm	파일
412	%SystemDrive%\inetpub\wwwroot\<LANGUAGE-TAG>\412.htm	파일
500	%SystemDrive%\inetpub\wwwroot\<LANGUAGE-TAG>\500.htm	파일
501	%SystemDrive%\inetpub\wwwroot\<LANGUAGE-TAG>\501.htm	파일
502	%SystemDrive%\inetpub\wwwroot\<LANGUAGE-TAG>\502.htm	파일

기능 보기

작업

- 추가...
- 편집...
- 상태 코드 변경
- 제거
- 기능 설정 편집**
- 도움말
- 온라인 도움말

8. 오류 페이지 설정 편집 설정 후 확인

오류 페이지 설정 편집

오류 응답

서버 오류 발생 시 다음 반환:

- 사용자 지정 오류 페이지(C)
- 자세한 오류(D)
- 로컬 요청에 대한 자세한 오류와 원격 요청에 대한 사용자 지정 오류 페이지(E)

기본 페이지

경로(P):

C:\inetpub\wwwroot\httpsRedirect.htm

경로 유형(T):

파일

확인 취소

/종료/