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
- II. 보안서버 구축 시 주의사항
- III. Apache SSL 인증서 설치
- IV. Tomcat SSL 인증서 설치

V. Windows IIS SSL 인증서 설치

I. 보안서버 구축 개요

1. 추진목적

개인정보를 취급하는 정보시스템에 대한 보안서버 구축 및 적용확대를 통하여 건전하
 고 안전한 교육 사이버 환경 조성

- 교육기관에 대한 SSL 인증서 기반 보안서버 구축을 통하여 개인정보유출 방지 및 경쟁 력 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)

- 무료게시판 이용 홈페이지
 PHP, ASP 등으로 만든 무료게시판을 이용하는 홈페이지에서 SSL 인증서를 적용하려면 게 시판 설정 수정이 필요
- 3. 웹서버 최신 버전 유지 교내 홈페이지의 개인정보를 보호하기 위해서는 웹서버의 보안 취약점 제거도 병행되어 야 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 합니 다. Mod_SSL 설치 확인(\$ /usr/local/apache/bin/httpd -l) [root8168 bin]# ./httpd -1 Compiled in modules: core.c mod access.c mod auth.c mod include.c mod_log_config.c mod env.c

[인증서 설치하기]

mod ssl.c

geterwif.c

1. 인증서 복사

hod

- 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.pe	m (키파일)
SSLCertificateChainFile /usr/local/apache/conf/ssl/ DigiCertCA.pem	(체인인증서파일)

<VirtualHost IP:443> DocumentRoot "/xxx/2.html" ServerName login.test.co.kr ServerAdmin <u>admin@abc.co.kr</u> 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: httpd (을)를 시작합니다: Apache/2.0.52 mod_ssl/2.0.52 (Pass Some of your private key files are encrypted for security i In order to read them you have to provide the pass phrases	[Ph reas	확인 hrase [sons.] Dialog)
Server cee.postech.ac.kr:443 (RSA) Enter pass phrase:			
OK: Pass Phrase Dialog successful.	r	#L 01	1
[root@tmp-web_conf]#	L	확인	1

→ Enter pass phrase: postech2022

6. 인증서 설치 확인

가. 인증서 Port LISTEN 확인

[root	0168	bin]#	net	stat -na grep	443	Technology	
tcp		0	U	:::443		:::*	LISTEN
unix Aefd5	3 510e]]	STREAM	CONNECTED	543443	/tmp/orbit-root/linc-ca4-0-67
[root	0168	bin]#	net	stat -na grep	444		
tcp		0	C	:::444		:::*	LISTEN

나. 웹페이지에서 인증서 설치 확인



7. 패스워드 수동입력 없이 웹 서비스 자동 실행하기

- SHELL을 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

```
    # Pass Phrase Dialog:
    # Configure the pass phrase gathering process.
    # The filtering dialog program (`builtin' is a 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

※ 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 하 기 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.conf에 다음 추가

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

2. rewrite 모듈 주석 해제하여 활성화하기

🧂 httpd.conf - 메모장	
파일(E) 편집(E) 서식(<u>O</u>) 보기(⊻) 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	
<pre>#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 spling_module modules/mod_spling.so LoadModule ssl_module modules/mod_ssl.so</pre>	
LoadModule status_module modules/mod_status.so #LoadModule substitute_module modules/mod_substitute.so LoadModule unique_id_module modules/mod_userdir.so #LoadModule userdir_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 <u>keystore파일</u> 과 <u>패스워드</u> 입력)				
<connector <b="">port="443" maxThreads="150" minSpareThreads="25" maxSpareThreads="75"</connector>				
enableLookups="false" disableUploadTimeout="ture"				
acceptCount="100" debug="0" scheme="https" secure="true"				
keystoreFile="/path/keystore 파일명" keystorePass=" postech2022 "				
clientAuth="false" sslProtocol="TLS" />				
• Tomcat 6.x(7.x/8.0)의 경우(Connect부분 주석처리 없애고 keystore파일과 패스워드 입력)				
<connector <="" port="443" protocol="HTTP/1.1" sslenabled="true" td=""></connector>				
maxThreads="150" scheme="https" secure="true"				
keystoreFile="/path/keystore파일명" keystorePass=" ^{postech2022} "				
clientAuth="false" sslProtocol="TLS" />				
• Tomcat 8.5이상의 경우(Connect부분 주석처리 없애고 keystore파일과 패스워드 입력)				
<connector <="" port="443" protocol="org.apache.coyote.http11.Http11NioProtocol" td=""></connector>				
maxThreads="150" SSLEnabled="true" >				
<sslhostconfig></sslhostconfig>				
<certificate <="" certificatekeystorefile="/path/keystore파일명" td=""></certificate>				
certificateKeystorePassword=" postech2022"				
certificateKeyAlias="alias명" type="RSA" />				

3. 웹서버 재구동

[인증서 설치 후 설치 확인]

1. 인증서 Port LISTEN 확인

[root	:@loca	lhost bin]#	netstat —na	grep 443		
tcp		0 0:	::443		::: *	LISTEN
unix	2	[ACC]	STREAM	LISTENING	11443	/tmp/orbit-root/linc-d5e-0-dda64722ba08
[root	:@loca	lhost 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 허용 할 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.

[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 2개를 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

8]	IIS(인터넷 정보 서비스) 관리자	_ D X
🕤 🎙 🕨 WIN-N77LIJSUS	6J >	🏧 🖾 🏠 🔞 🗸
파일(F) 보기(V) 도움말(H)		
연결	✔ ✔ ✔ ♥ ● ♥ ● ♥ ● ● ♥ ●	작업 기져오기) 인증서 요청 만들기 인증서 요청 완료 도미인 인증서 만들기 자체 서명된 인증서 만들기 안 도응말 온라인 도움말
준비		• <u>⊒</u> .:

3. 해당 인증서(.pfx) 파일을 선택 및 암호 입력 후 확인

인증서 가져오기 ? ×
인증서 파일(.pfx)(<u>C</u>):
C:\Users\; SSL인증서 저장한 경로에서 인증서 선택
암호(만):
●●●● 암호: postech2022
인증서 저장소 선택(<u>S</u>):
7개인 ~
✓ 이 인증서를 내보내도록 허용(<u>A</u>)
확인 취소

4. 아래와 같이 인증서 Import 확인

₹j	IIS(인터넷 정보 서비스) 관리자	_ D X
WIN-N77LIJSU	56J >	🔤 🛛 🟠 🔞 🗸
파일(E) 보기(<u>V</u>) 도움말(<u>H</u>)		
연결	비즈이 비니 📫	작업
🕏 - 🔚 🖄 😽	시미 인증시	가져오기
월 시작 페이지 ▲ · ● WIN-N77LJSUS6J(WIN-N77I	이 기능을 사용하여 웹 서버가 SSL에 대해 구성된 웹 사이트에 사용할 수 있는 인증서를 요 정하고 관리할 수 있습니다.	인증서 요청 만들기 인증서 요청 완료
	필터: ▼ ♥ 이동(G) → Gal 모두 표시(A) 묶는 방법:	도메인 인증서 만들기
wildtest1.crosscert.cor	이름 수 발급 대상 발급자 만료일	자체 서명된 인증서 만들기
թ. Ƙoð wildtest2.crosscert.cor	*.postech.ac.kr *.postech.ac.kr CrossCert Class 1 Server CA 2015-10-20 오후	 도움말 온라인 도움말

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

6	IS(인터넷 정보 서비스) 관리자	_ D X
💽 🔞 🕨 WIN-N77LIJSU	S6J 🕨 사이트 🔸 wildtest1.crosscert.com 🕨	🔤 🖾 🟠 🔞 •
파일(E) 보기(⊻) 도움말(H)		
연결 ⓒ - 🔛 🖄 😽	🧼 wildtest1.crosscert.com 홈	작업
································	필터: ▼ ♥ 이동(G) ▼ ↓ 모두 표시(A) ↓ 묶는 방법: IIS ▲ ▲	사용 권한 편집
▲ 급 사이트 ▶ Co wildtest1.crosscert.co		<u>마인리…</u>] [1] 기본 설정… 유유 프리그램 비기
y windesiz.crosscercco	리다면 헤다 31 351 28 가는 편지 나라지 하다.	가상 디렉터리 보기
	루기 모등 아초 으로 페이지 유청 폭탄리 이주	웹 사이트 관리 💿
		▶ 시작 ■ 중지
	지리기 매핑 출력 캐시	웹 사이트 찾아보기 ♥ Wildtest1.crosscert.com on ★80 (http) 찾아보기

6. http 를 선택 후 '편집' 클릭

\$ _j	IIS(인터넷 정보 서비스) 관리자	_ 🗆 X
🕞 🕤 🛛 WIN-N77LIJSUS	5J > 사이트 > wildtest1.crosscert.com >	🔤 🔤 🟠 I 🔞 🗸
파일(E) 보기(⊻) 도움말(H)	사이트 바인딩 ? 🗙	Γ
연결 • · · · · · · · · · · · · · · · · · · ·	종류 호스트 이를 포트 IP 주소 바인딩 정 http wildtest1.crosscert.com 80 * 제거(B) 젖아보기(B)	작업
		 ◇ 다시 시작 ▶ 시작 ● 중지 입 사이트 찾아보기 wildtest1.crosscert.com on *:80 (http) 찾아보기

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

	사이트 바인딩	? X
주르	사이트 바인딩 편집 ? ×	
http	종류([]: IP 주소([): 포트(Q): http v 지정하지 않은 모든 IP v 80	(E)
	호스트 이름(H): wildtest1.crosscert.com 예: www.contoso.com 또는 marketing.contoso.com	(R) 17(B)
	확인 쥐소	7(C)

8. '추가'를 클릭 -> 정보를 입력한 뒤 인증서 선택 후 '확인'

사이트 바인딩	? X	
사이트 바인딩 추가 ? 🗙	추가(A)	
종류([]: IP 주소(): 포트[Q):	편집(E)	
[https: ▼ [사장약자 많은 또는 ☞ ▼ [백45]] 호스트 이름(H):	제거(R)	종류 : https
wildtest1.crosscert.com	찾아보기(B)	
☐ 서버 이름 표시 필요(N)		포트 : 기본 443
SSL 민증서(F):		ㅎㅅㅌ 이르 · 해다 니미
*.postech.ac.kr V 선택(L 보기(M		
································		SSL인증서 : 해당 인증서
	닫기(C)	

9. 확인 후 '닫기'

			사이	트 바인딩	? X
종류 http https	호스트 이름 wildtest1.crosscert.com wildtest1.crosscert.com	포트 80 443	IP 주소 * *	바인딩 정보	추가(<u>A</u>) 편집(E) 제거(<u>R</u>) 찾아보기(<u>B</u>)
					닫기(C)

10.IIS에서 해당 사이트 재구동

연결	🦚 wil	dtest1 cro	osscort c	· · · · ·				작	업	
🔩 - 🔚 🛯 🖄		alesti.cr	JSSCELLC						탐색	^
·····································	필터:		- 🐨 이동(G)	- 급모두표	시(A) 묶는 병	방법:			사용 권한 편집	
⊿·Ч WIN-N//LJSUSU(WIN-N//	TIS				- (사이트 편집	
⊿◙ 사이트		-	-	0	A	1			바인딩	
Wildtest1.crosscert.cor	- -		3 22		0				기본 설정	_ =
▷· Idtest2.crosscert.cor	HTTP	HTTP 응답	MIME 형식	SSL 설정	기본 문서	티텍터리			응용 프로그램 보기	
	니니텍신	에니	0		_	- 24	=	_	가상 디렉터리 보기	
			2	404	8			웹	사이트 관리 🛛 🐼	
	로깅	모듈	~~~~ 압축	오류 페이지	요청 필터링	인증		2	다시 시작	
								₽	시작	
									중지	
									웹 사이트 찾아보기	
	저리기 배평	꿀덕 개시					~		wildtest1.crosscert.com or *80 (http) かいせフ	
								-	wildtest1.crosscert.com or	, I
< III >	💷 기능 보기	💼 콘텐츠 보기	I						*.443 (https) 찾아보기	_ ~
준비										€ 1.:

[체인 인증서 설치]

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

2. 시작 🗲 '실행' 클릭



3. mmc 입력 후 '확인'

E	실행	x
	프로그램, 폴더, 문서, 또는 인터넷 주소를 입력하여 해당 항목을 있습니다.	열 수
열기(<u>O</u>):	mmc	~
	확인 취소 찾아보기(<u>B</u>)	

4. 해당 콘솔에서 '파일' → '스냅인 추가/제거' 클릭

R 1 R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + FL] R 201 - [20 + [20 + FL] R 201 - [20 + [20 + FL] R 201 - [20 + [20 + [20 + FL] R 201 - [20 + [20	1						
····································	류지를				콘술1 - [콘술 루트]		_ 🗆 X
Image: Second control of the secon		🚟 파일(F) 등작(A) 보기(V) 출격찾기(0) 장(W) 도움말(H)			_ # ×
Nots 환기(0) Ctrl-0 Nots 전설인 주가/제기(N) Ctrl-3 관련 변호교 환체 보기에서 표시할 형후이 없습니다. 위험 환화 bilingm. 문 여름으로 지않(A) 전설인 주가/제기(N) Ctrl-M 물 선명 물 여태 전 년 주도 기타 작업 로 다 문 여름으로 지않(A) 전 년 주도 전 년 주도 오 년 주가/제기(N) Ctrl-M 물 현 제 보기 및 현 취 및 한 (D) 전 년 전 년 전 년 전 년 한 후가/제기(N) 중 ctrl 문 한 대 전 년 전 년 전 년 전 년 한 후가/제기(N) Ctrl-M 중 ctrl		🕼 새로 만들기	(N) Ctrl+	N			
Nots 편값 변환 응답 등 모르 환체 보기에서 표시할 형국이 있습니다. 관측 후트 · ····································		열기(0)	Ctrl+	0		작업	
Image: Second synthesis and the synthesynthesis and t	hosts	저장(S)	Ctrl+	S එ	재 보기에서 표시할 항목이 없습니다.	콘술	루트 🔺
Image: Control (Control (나른 이름으	.로 서상(A)			2	타작업 ▶
Image: Second secon		스냅인 추가	/제거(M) Ctrl+	м			
		음껀(P)					
Image: Image	Slobalsion	1 secpol					
고대 전 고대 전 <t< td=""><td>(e</td><td>2 WF</td><td></td><td></td><td></td><td></td><td></td></t<>	(e	2 WF					
Image: Secure Int. Image: Secure Int. Image: Int.		=41/1(X)					
cet Image: Cet		4					
eer Secure-int. eer eer eer - 법인 분들에서 스냅인을 추가하거나 체계하도록 설정합니다. - 건 한 분들에서 스냅인을 추가하거나 체계하도록 설정합니다. - 건 한 분들에 사 스냅인을 추가하거나 체계하도록 설정합니다. - 전 0 분들에 사 스냅인을 추가하거나 체계하도록 설정합니다. - 전 0 분들에 사 스냅인을 추가하거나 체계하도록 설정합니다. - 전 0 분들에 사 스냅인을 추가하거나 체계하도록 설정합니다.							
iccure-int. ert cet Tr 관목 Tr 관육 Tr 관	cert						
ecurs-int. ecurs-int. cer 7개 함독 전철 문화에서 스냅인을 추가하거나 체거하도록 설정합니다. 7개 함독 전철 문화에서 스냅인을 추가하거나 체거하도록 설정합니다. 전 (Mindo							
ecure-int. eet eet et et et et et et et et et et e							
ecure-int. cet Cet Cet Cet Cet Cet Cet Cet Cet Cet C	1200 I						
er cr cr cr cr cr cr cr cr cr c	ecure-int						
· · · · · · · · · · · · · · · · · · ·							
· · · · · · · · · · · · · · · · · · ·							
ert 이 소법인 문율에서 스냅인을 추가하거나 제거하도록 설정합니다. 	E .	•					
스냅인 콘솔에서 스냅인을 추가하거나 체거하도록 설정합니다. dows Server 2012 7/I 항목 III III III IIII IIIIIIIIIIIIIIIIIIII	cert						
스냅인 문술에서 스냅인을 추가하거나 체거하도록 설정합니다. dows Server 2012 7개 항목 () 2011 () 2012 () 2013 () 2014 () 2015 () 2015 () 2016 () 2017 () </td <td></td> <td>1</td> <td></td> <td></td> <td></td> <td></td> <td></td>		1					
dows Server 2012 7개항육 IIII Windo		스냅인 콘솔에서 스냅	인을 추가하거나 제거하	도록 설정합니다.			
7개 함독 Windo						dov	ws Server 2012
7개 함독 Windo						201	V3 5CT VCI 2012
7개 함축 Windo							
7개 함축 Windo							
	T ^P	개항목					Windo
	- 2	- in the second					P 🐻 🖬

5. '인증서' 선택 후 '추가'

-			콘솔1 -	[콘솔 루트]	_	D X
🌇 파일(F)			스냅인	추가/제거	X	_ 5 X
← ➡ ►	컴퓨터에서 사용 가능한 콘 선택할 수 있습니다.	솔 스냅인을 선택하고 선택	⁴ 한 스냅인 집합	을 구성할 수 있습니다. 확장 가능한 스냅인	!의 경우 사용할 확장 기능을	
	사용 가능한 스냅인(<u>S</u>):			선택한 스냅인(E):		^
	스냅인	공급업체 ^		🎬 콘솔 루트	확장 기능 편집(<u>X</u>)	•
	중 로컬 사용자 및 그룹 ᠍ 보안 구성 및 분석 ■ 보안 템플릿	Microsoft Corp Microsoft Corp Microsoft Corp			제거(<u>R</u>)	
	않 서비스 (1) 성능 모니티	Microsoft Corp Microsoft Corp			위로 이동(U)	
	 법 주소에 연결 값 이벤트 뷰어 값 인물서 관 작업 스케울러 관 작업 스케울러 관 자리자 	Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp	추 ⁷ †(<u>A</u>) >		아래로 이동([])	
	867 전화 동신 [1] 정책 결과 집함 [2] 컴퓨터 관리 [2] 폴더	Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp			ਹਜ਼ੂ⊘	
	설명: 민중서 스냅인은 민중서 저	장소의 내용을 사용자 자	신, 서비스 또는 :	컴퓨터에서 잦아보게 합니다.	확인 취소	

6. '컴퓨터 계정' 선택 후 '다음' 클릭

1	콘솔1 - [콘솔 루트]		-	□ X	
🚡 파일(F)	∧ 내이 ᄎ가/제거		x	- 8	×
♦	인증서 스냅인				
📔 콘솔 루텍	이 스냅인이 항상 관리할 인증서 대상:	경우 사용할 확장 기용물			
	○ 내 사용사 게입()//)	확장 기능 편집(<u>X</u>)		1	*
	 컴퓨터 계정(C) 	제거(<u>R</u>)			
		위로 이동(山)			
		아래로 이동(D)			
		고급(y) 확인 취소			

7. '로컬 컴퓨터' 선택 후 '마침' 클릭

*	콘솔1 - [콘솔 루트]	_	
🚟 파일(F)	∧내이 ᄎフレ/제거	x	_ & ×
	컴퓨터 선택 🔭	거 이 내 무추대하지, 기는 무	
· 문술 루:	컴퓨터 선택 적 이 스냅인이 컨리할 컴퓨터를 선택하십시오. 이 스냅인이 항상 관리할 대상: ④ 토질 컴퓨터: (이 끈슬이 실행되고 있는 컴퓨터)(①) ④ 다른 컴퓨터(Δ): ● 다른 컴퓨터(Δ): 찾아보기(①) □ 명령줄에서 시작할 때 선택된 컴퓨터를 변경할 수 있음. 사용자가 폰술을 저장할 때만 해당(①) · · · · · · · · · · · · · · · · · · ·	경우 사용할 확장 기능을 획장 기능 편집(&) 제가(R) 위로 이동(U) 아래도 이동(D)	, ,
		확인 취소	

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

류지동 프 순입 - [군순 두토 싸인증서(로걸 컴퓨터)\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	
월 파일(F) 등학(A) 보기(M) 중계정기(IO) 철(M) 도움말(H) (F) × ◆ 추 최 1 □ @ 과 월 1 □ 월 관람 무료 월 금 대상 ▲ 발급자 만료 날짜 용도 확업	
◆ → 최 □ ○ </td <td></td>	
· 관금 무드 발급 대상 · 발급자 만료 날짜 용도 작업	
hosts 4 및 반응세 도덜 검유비) GlobalSign Extended Validatio GlobalSign 2022-04-13 《모두》 인증서	
▲ · · · · · · · · · · · · · · · · · · ·	
▶ [신뢰일 수 있는 루트 안] [Microsoft Windows Hardware Microsoft Root Author 2002-01-23 저희 관]	
[나 이 아이크 및 · · · · · · · · · · · · · · · · · ·	
· · · · · · · · · · · · · · · · · · ·	
Cicloasign 인호쇄 Cinvw/versign.com/LPS Incolp Class 3 Public Primary Certificati 2016-10-25 지역 된	
○ ▶ 2 신뢰법 모든 삭업(<) ▶ 7/서오기(()	
cet p = = = = = = = = = = = = = = = = = =	
Secure-int	
cert	
인증서를 저장소에 추가합니다.	
dows Server 2012	
7/1 0.4	
Windows S	Server 2012 Datacenter
	Build 9200
🔚 🖉 🥵 🥵 🖓 👹	1 A 2014-01-24

9. 인증서 가져오기 마법사 시작 확인 후 '다음'

- E	코송1 - [코송 르트뉴이즈서/로커 커프티)뉴주가 이즈 기과프이즈서1	
파일(F) 동작(A) 보기	🖉 🥩 인증서 가져오기 마법사	_ & ×
 군술 루트 ▲ ♀ 인증서(로컬 컴퓨터) ▲ ○ 개인용 ④ 인증서 ▷ ○ 신뢰할 수 있는 록 ● ○ 신뢰할 수 있는 거 ● ○ 신뢰할 수 있는 거 ● ○ 신뢰할 수 있는 거 ● ○ 신뢰할 수 있는 시 	인증서 가져오기 마법사 시작 이 마법사를 사용하면 인증서, 인증서 신뢰 목록, 인증서 해지 목록을 디스크에서 인증서 저장 소로 복사할 수 있습니다. 인증서는 인증 기관이 발급하는 것으로 사용자 신분을 확인합니다. 인증서에는 데이터를 보호 하거나 보안된 네트워크 연결을 하는 데 필요한 정보가 들어 있습니다. 인증서 저장소는 인증 서를 저장하는 시스템 영역입니다. 저장소 위치 ○ 현재 사용자(<u>C</u>) ● 로컬 컴퓨터(<u>L</u>)	: <mark>서 ▲</mark> 기타 작업 ▶
< III	계속하려면 [다음]을 클릭하십시오. 다음(N) 취소	

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

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

	코송1 _ [코송 르티씨이즈서/로커 커프티\씨주가 이즈 기과씨이즈서]		_ 🗆 X
🚘 파일(F) 동작(A) 보기 (수 🔿 🖄 🔝 📋 🖸	 ④ 인증서 가져오기 마법사 		_ <i>8</i> ×
 같은 루트 같은 루트 같은 양서(로컬 컴퓨터) 같은 인증서 인증서 같은 신뢰할 수 있는 류 관 인증서 같은 장간 인증 기관 같은 양자 같은 양자 같은 가 인증 같은 가 인증서 같은 가 인증서 같은 가 인증서 같은 가 있는 가 같은 가 있는 가 같은 신뢰할 수 있는 가 같은 신뢰할 수 없는. 	가져울 파일을 지정하십시오. 파일 이름(F): C:#Users\#gheo\#Desktop\# DigiCertCABundle.p7b o 참고: 다음 형식으로 한 파일에 두 개 이상의 인증서가 저장될 수 있습니다.	5 서 기타 작업	,
 ▷ ○ 타사 루트 인증 기 ▷ 신뢰할 수 있는 시 ▷ ○ 신뢰할 수 있는 시 ▷ ○ 인증서 등록 요정 ▷ ○ 스마트 카드 신뢰 ▷ ○ 신뢰할 수 있는 징 ▷ ○ 웹 호스팅 	개인 정보 교환- PKCS #12(.PFX,.P12) 암호화 메시지 구문 표준- PKCS #7 인증서(.P7B) Microsoft 일련 인증서 저장소(.SST)		
< 배 중간 인증 기관 저장소에 7개	<u>인증서 파일 형식</u> 에 대해 자세히 알아보세요. 다음(N) 취소		



11. '다음' 클릭

파일(r) 등작(A) 보 ····································	a	코송1 - [코송 르트w이즈서/로커 커프터)ພ주가 이즈 기과w이즈서1		⊐ x
● 문송 무트 ● 10 ***********************************	플 파일(F) 동작(A) 보7 ◆ ➡ ▲ ☑ □ □ □	✓ 인증서 가져오기 마법사		- 8 ×
 ● 앱 연료프라이즈 신뢰 ▲ · · · · · · · · · · · · · · · · · · ·	 홈 운 루트 ▲ 교 인증서(로컬 컴퓨터) ▲ ¹⁰ 개인용 ¹⁰ 인증서 ▶ ¹⁰ 신뢰할 수 있는 루 	인증서 저장소 인증서 저장소는 인증서를 저장하는 시스템 영역입니다.	5 서 기타 작업	•
 ▲ 스마트 카드 신뢰 ▲ 신뢰할 수 있는 직 ▶ ○ 웹 효스팅 <u>인증서 저장소</u>에 대해 자세히 알아보세요. 	 ▷ ○ 엔터프라이즈 신뢰 △ ○ 중간 인증 기관 ○ 인증서 해지 월 ○ 신뢰할 수 있는 거 ▷ ○ 신뢰할 수 있는 거 ▷ ○ 타사 루트 인증 7 ▷ ○ 탄사 로트 인증 7 ▷ ○ 한사 등트 이증 7 ▷ ○ 한사 등트 이증 7 ▷ ○ 한사 등트 이증 7 	Windows가 자동으로 인증서 저장소를 선택하거나 사용자가 인증서 위치를 지정할 수 있 습니다. 인증서 종류를 기준으로 인증서 저장소를 자동으로 선택(U) 모든 인증서를 다음 저장소에 저장(P) 인증서 저장소: 중간 인증 기관 찾아보기(R)		
< III 「	▷ ○ 스마트 카드 신뢰 ▷ ○ 신뢰할 수 있는 징 ▷ ○ 웹 호스팅	<u>인증서 저장소</u> 에 대해 자세히 알아보세요. 다음(N) 취소		

13. 마법사 완료 확인 후 '마침' 클릭

.	코송1 _ [코송 르티웨이즈서/로커 커프터)웨주가 이즈 기과웨이즈서1		_ 🗆 X
🚡 파일(F) 동작(A) 보기 </td <td>📀 😔 인증서 가져오기 마법사</td> <td></td> <td>_ & ×</td>	📀 😔 인증서 가져오기 마법사		_ & ×
몬솔 루트 ▲ 및 인증서(로컬 컴퓨터) ▲ 월 개인용 일 인증서 ▷ 월 시뢰학 수 있는 특	인증서 가져오기 마법사 완료	:서 기타 작업	•
▶ 🖆 엔터프라이즈 신뢰 ▲ 😭 중간 인증 기관 @ 인증서 해지 최	[마침]을 클릭하면 인증서를 가져옵니다.		
[1] 인증서 ▷ 11 신뢰할 수 있는 거 ▷ 11 신뢰할 수 없는. ▷ 11 타사 루트 인증 7 ▷ 12 타사 루트 인증 7 ▷ 12 단사 등록 요청 ▷ 12 스마트 카드 신뢰 ▷ 13 신뢰할 수 있는 정 ▷ 13 한 직	다음 설정을 지정했습니다. 사용자가 선택한 인증서 저장소 중간 인증 기관 콘텐츠 PKCS #7 인증서 파일 이름 C:\Users\Userd\Users\Userd\Users\Users\Users\User		
< 배 중간 인증 기관 저장소에 7개	마침(E) 취소		

14. 설치한 체인인증서 파일을 확인

콘솔1 - [콘솔 루트\인증서(로컬 컴퓨터)\중간 인증 기관\인 	!증서]					- □ >
파일(F) 동작(A) 보기(V) 즐겨찾기(O) 창(W) 도·	움말(H)					- 6
🗢 🔿 📶 🦨 🗞 🗶 🗊 🗟 🖬 💼						
🤗 콘솔 루트	발급 대상 ^	발급자	만료 날짜	용도	이름	작업
이승서(로컬 컴퓨터)	DESKTOP-G9HKTP6	DESKTOP-G9HKTP6	2020-05-27	서버 인증	<없음>	인증서
> 🦳 개인용	DESKTOP-G9HKTP6	DESKTOP-G9HKTP6	2020-05-23	서버 인증	<없음>	
> 🔄 신뢰할 수 있는 루트 인증 기관	DESKTOP-G9HKTP6	DESKTOP-G9HKTP6	2020-09-17	서버 인증	<없음>	기리적답
> 엔터프라이스 신되	DESKTOP-G9HKTP6	DESKTOP-G9HKTP6	2020-08-21	서버 인증	<없음>	DigiCert Global Root CA
♥	DESKTOP-G9HKTP6	DESKTOP-G9HKTP6	2020-08-21	서버 인증	<없음>	기타 장역
	DESKTOP-G9HKTP6	DESKTOP-G9HKTP6	2020-05-30	서버 인증	<없음>	
. 12 전공직	DESKTOP-G9HKTP6	DESKTOP-G9HKTP6	2020-04-16	서버 인증	<없음>	
> III 근처를 두 쓰는 데이지 > III 시리한 스 어느	DESKTOP-G9HKTP6	DESKTOP-G9HKTP6	2020-04-16	서버 인증	~없음>	
> I 타사 루트 이증 기관	DESKTOP-G9HKTP6	DESKTOP-G9HKTP6	2020-08-09	서버 인증	~없음>	
› 🧰 신뢰할 수 있는 사용자	DESKTOP-G9HKTP6	DESKTOP-G9HKTP6	2020-08-09	서버 인증	~없음>	
> 🧰 클라이언트 인증 발급자	DESKTOP-G9HKTP6	DESKTOP-G9HKTP6	2020-05-22	서버 인증	~없음>	
> 🧰 Preview 빌드 루트	DigiCert Global Root CA	DigiCert Global Root CA	2031-11-10	<모두>	<없음>	
> 🧰 테스트 루트	KIMDH2514	KIMDH2514	2022-08-18	서버 인증	<없음>	
> 📫 AAD Token Issuer	KIMDH2514	KIMDH2514	2022-02-19	서버 인증	<없음>	
> 🧰 다른 사람	KIMDH2514	KIMDH2514	2021-02-20	서버 인증	<없음>	
> 🧮 Dell Trust	KIMDH2514	KIMDH2514	2021-03-30	서버 인증	<없음>	
> Cartification Authorities	KIMDH2514	KIMDH2514	2021-01-20	서버 인증	<없음>	
> EFSFirePassRoot	KIMDH2514	KIMDH2514	2022-10-05	서버 인증	<없음>	
> iii Homegroup Machine Certificates	KIMDH2514	KIMDH2514	2021-06-18	서버 인증	<없음>	
> Local NonRemovable Certificates	KIMDH2514	KIMDH2514	2021-05-25	서버 인증	<없음>	
> MSIEHistoryJournal	KIMDH2514	KIMDH2514	2021-12-14	서버 인증	<없음>	
> 🧰 OEM eSIM 인증 기관	KIMDH2514	KIMDH2514	2023-05-17	서버 인증	<없음>	
> Passpoint 신되뇐 루드	KIMDH2514	KIMDH2514	2022-07-21	서버 인증	<없음>	
> PC-Doctor, Inc.	KIMDH2514	KIMDH2514	2023-02-28	서버 인증	<없음>	
> 🛄 원격 네스크톱	KIMDH2514	KIMDH2514	2022-08-26	서버 인증	< 영음 >	
> 🔜 인당지 중독 보정 - 🤭 스마트 라드 시리하 스 이노 로트	KIMDH2514	KIMDH2514	2021-07-08	서버 인증	< 안음 >	
› 🔜 느릿도 키도 인죄될 두 있는 주도 > 😁 시리한 스 이노 패키지되 얘 성치 기과	KIMDH2514	KIMDH2514	2022-10-20	서버 인증	<없음>	
> 🔜 연파를 두 있는 해외직원 앱 열직 기원 > 🤗 시리한 스 이트 자치	KIMDH2514	KIMDH2514	2022-10-05	서비 인증	< 연음 >	
Vindows Live ID Token Issuer	KIMDH2514	KIMDH2514	2020-11-12	서비 인증	~ 었음>	
Windows Ere is token issuer	KIMDH2514	KIMDH2514	2023-03-16	서비 인증	~ 었음>	
	KIMDH2514	KIMDH2514	2023-05-06	서버 인증	~ 없음 >	
			2023-03-00		200	

[인증서 설치 후 설치 확인]

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



※ SSL 암호화 설정

인증서를 설치하고 나면 http와 https 로의 접속이 모두 가능합니다. http 로의 접속을 계속 허용 할 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. 인터넷 정보 서비스 실행(IIS) 후 해당 웹사이트 선택 후 마우스 오른쪽 클릭하여 속성 선택



무자료

2. 등록정보에서 디렉터리 보안 탭에서 편집 클릭



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

kimdh.postech.ac.kr 등록 정보 ? 🗙
웹 사이트 ISAPI 필터 홈 디랙터리 문서 디랙터리 보안 HTTP 헤더 사용자 지정 오류 ASP,NET
오 보안 통신 🛛 🔀
 ✓ 보안 채널 필요(SSL)(B) ✓ [1280] 트 암호화 필요(])
 클라이언트 인증서 ● 클라이언트 인증서 무시(Q) ● 클라이언트 인증서 받아들임(A) ● 클라이언트 인증서 필요(U)
☐ 클라이언트 인증서 매핑 사용(L) 클라이언트 인증서를 Windows 사용자 계정에 매핑할 수 있습니다. 이렇게 하면 클라이언트 인증서를 사용하 며 리소스 액세스를 제어할 수 있습니다. 편집 [D]
· · · · · · · · · · · · · · · · · · ·
새로 만들기(逊) 편집(!)
확인 취소 도움말(H)

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/