KISA 안내 • 해설 제 2010-17호

보안서버구축 안내서

2009.12

KISA
한국인터넷진흥원

제·개정 이력

순번	제·개정일	변경내용	발간팀	연락처
1	2007.2월	최초 제정	개인정보보호기술팀	405-4724
2	2008.7월	보안서버 목적, 구축 방법 등 개정	개인정보보호기술팀	405-4724
3	2009.12월	암호화 필요한 서비스의 범위 등 개정	개인정보보호기술팀	405-4724

주 의 사 항

○ 이 안내서는 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』 등 관계법령의 규정을 토대로,

- 개인정보를 취급하는 사업자가 보안서버 구축함에 있어 언제든지 쉽게 참고할 수 있는 정보를 제공하며,
- 동 정보에 대한 올바른 이해를 통하여 사업자의 개인정보보호조치 이행을 지원하기 위하여 발간하였습니다.

○ 이 안내서에서 안내하고 있는 제품이나 예시 등은 각 사업자에 있을 수 있는 고유한 환경을 고려하지 않았으므로 실제 환경에서 그대로 적용되지 않을 수 있습니다.

- 따라서 기준을 이행하는 데 필요한 제품이나 구축 방법을 결정하기 전에 각 기업의 환경에 적합한 제품을 찾아 확인하는 절차가 필요하며, 담당자의 신중한 판단이 요구됩니다.

※ 이 안내서의 내용에 대하여 문의가 있거나 오류를 발견한 경우에는 홈페이지(www.kisa.or.kr – 보안서버 안내) 또는 이메일(taej@kisa.or.kr)로 문의하여 주시기 바랍니다.

안내서의 구성

본 안내서는 사용자들의 이해를 돕기 위하여 다음과 같이 구성되어 있습니다.

Ⅰ 장과 Ⅱ 장은 사용자들이 반드시 알아야 하는 기본적인 사항들입니다. 꼭 읽어보시고 각 업체의 환경에 적합한 보안서버를 선택해야 합니다.

보안서버 구축 방법을 선택하였다면, Ⅲ 장 ~ Ⅴ 장 중 상황에 맞는 내용을 참조하시면 됩니다. 각 장에 소개되는 설치 방법과 오류시 대처방법을 숙지한 후 보안서버 구축 전문 업체에 연락하시면 보다 자세한 안내를 받을 수 있습니다.

Ⅵ 장은 보안서버를 구축한 후, 실제 웹페이지에서 수정해야 할 내용에 관한 안내서입니다. 웹페이지 적용 방법과 실제 사례를 포함하고 있으며, 보안서버가 적용되었는지 확인하는 방법을 알아보실 수 있습니다.

Ⅶ 장은 방송통신위원회에서 추진하고 있는 보안서버 구축 확대에 관한 FAQ를 정리한 것입니다. 2005년부터 현재까지 웹사이트 운영자들이 자주 질문하신 내용을 정리한 것이므로 우선 궁금하신 내용이 있는지 확인한 후 추가적인 문의는 보안서버 안내 홈페이지(www.kisa.or.kr → '보안서버 안내')를 참조하거나 taej@kisa.or.kr로 연락하시기 바랍니다.

부록에는 SSL 가속기에 대해서 설명이 되어 있습니다.

Contents

Contents

Contents

Contents

Contents

그림 목차

Contents

그림 목차

Ⅰ. 보안서버(Secure Server)란

1. 보안서버의 정의
2. 보안서버 구축의 필요성
3. 보안서버 관련 법률
4. 보안서버 적용 범위

Ⅰ. 보안서버(Secure Server)란

1. 보안서버의 정의

보안서버란 인터넷 상에서 개인정보를 암호화하여 송수신하는 기능이 구축된 웹사이트를 의미한다. 보안서버는 독립적인 하드웨어를 따로 설치하는 것이 아니라 이미 사용하고 있는 웹서버에 SSL(Secure Sockets Layer) 인증서나 암호화 소프트웨어를 설치하여 암호통신을 지운하는 것을 의미한다. SSL 인증서의 경우 해당 전자상거래 업체의 실존을 증명하는 과정을 거쳐 발급되기 때문에 웹사이트에 대한 인증 기능도 일부 가지고 있습니다.

인터넷 상에서 송수신되는 개인정보의 대표적인 예로는 로그인 시 ID, 패스워드, 회원가입시 이름, 전화번호, 인터넷 뱅킹 이용 시 계좌번호, 계좌 패스워드 등이 있다. 암호화되지 않은 개인정보는 해킹을 통해 유출될 경우 심각한 피해를 초래할 수 있다. 보안서버는 이러한 위협을 방지하기 위한 방법의 하나로, 개인정보를 암호화하여 송수신함으로써 유출을 막는다. 그러나 보안서버의 구축 및 운영방법은 업체에 따라 많은 차이점이 있으며, 잘못된 보안서버의 구축 및 운영은 개인정보의 유출을 초래할 수 있다.

인터넷 상에서 암호화되지 않은 개인정보는 가로채기 등의 해킹을 통해 해커에게 쉽게 노출될 수 있으나, 웹 서버에 보안서버 솔루션을 설치하면 해커가 중간에 데이터를 가로채도 암호화 되어 있어 개인정보가 노출되지 않게 된다.

2. 보안서버 구축의 필요성

인터넷은 개방된 시스템입니다. 인터넷상에서 송수신되는 이용자, 사업자 및 컴퓨터의 신원정보(Identity)를 확인하는 것은 어렵지 않습니다. 더욱이 송수신 경로가 본질적으로 안전하지 않습니다. 모든 송수신은 도청자가 송수신자간 전달되는 메시지를 중간에 가로 채어 수정할 수 있는 위험에 노출되어 있습니다.

인터넷 통신은 종종 전통적인 우편시스템에서 우편엽서의 사용과 비유되곤 합니다. 만일 공격자가 적시에 적절한 장소에 있다면, 공격자는

- 당신의 우편엽서를 읽고, 당신의 대화에 훔칠 수 있으며,
- 당신의 우편엽서를 수정하고, 당신의 대화를 뒤엎을 수 있으며,
- 당신 또는 대화 대상자에게 우편엽서를 송부하여, 양 당사자를 흉내낼 수 있습니다.

비록 그러한 위협은 일반적으로 드물고 수행하기 어렵지만, 인터넷에서 전송되는 정보의 가치 및 민감 정도는 잠재적 이득을 원하는 자에게 동기를 부여할 수 있다. 실제로 인터넷 패킷을 캡쳐하는 프로그램을 이용하면 내가 속한 네트워크를 지나가는 대부분의 패킷 내용을 쉽게 열어볼 수 있습니다.

이러한 문제점을 해결하기 위한 보안서버는 네트워크 응용프로그램간의 통신에 대하여 프라이버시, 인증, 신뢰를 보장해주는 것을 목표로 하고 있습니다. 이를 위한 SSL 프로토콜은 어떤 TCP/IP 기반의 통신에도 유용하게 적용될 수 있으나, HTTP(웹사이트 트래픽)를 보호하는데 특히 많이 사용되고 있습니다.

SSL 기반의 통신은 개인적으로 이루어집니다. 암호화는 도청자에 대하여 통신을 안전하게 보호해 줍니다. 그리고 통신하는 양자가 신뢰 기반의 구조를 공유하여 인증이 될 수 있습니다.

보안서버는 네트워크 통신에서 다음의 장점을 제공한다.

2.1 정보유출 방지(sniffing 방지)

사용자가 웹사이트에 접속해서 로그인 또는 전자상거래를 위해 ID, 패스워드, 신용카드번호 등의 각종 중요한 개인정보를 입력하여 해당 사이트로 정보를 전송하게 됩니다. 이 때 악의적인 해커들이 설치한 정보유출 프로그램에 의해 사용자의 ID와 패스워드 등의 중요한 개인정보를 도청하는 것이 스니핑입니다.

일반적인 웹사이트에 로그인할 때 아이디와 비밀번호가 평문 형태로 전송된다. 이를 다른 사람이 중간에서 훔쳐볼 수 있는 스니핑 툴(sniffing tool)은 인터넷에서 손쉽게 구할 수 있습니다. 학교, PC방, 회사 등의 공용 네트워크에서는 스니핑 툴을 이용하여 타인의 개인정보를 쉽게 수집할 수 있다. 그러나 웹사이트에 보안서버가 구축된 경우에는 개인정보가 암호화되어 전송되므로 이러한 노출 위협으로부터 안심할 수 있습니다. 따라서 보안서버는 개인정보보호를 위한 필수적이며 기본적인 수단이다.

〈그림 1-1〉 보안서버 구축의 필요성

2.2 위조사이트 방지(phishing 방지)

피싱(Phishing)이란 개인정보(private data)와 낚시(fishing)를 합성한 조어입니다. 이는 인터넷 이용자에게 이메일이나 링크를 전송하여 금융기관이나 합법적인 기관으로 가장한 허위 웹사이트로 접속하게 한 후, 이용자가 입력한 비밀번호나 개인정보를 추출하여 금융 사기 등으로 악용하는 사기 기법입니다. 현재 피싱수법이 점점 교묘해져 가고 피해자가 속출하고 있는 상황으로 사용자가 개인정보를 입력시 해당 페이지가 신뢰할 수 있는 인증서가 설치되어 있는지 확인하는 등의 사용자의 주의가 필요합니다.

보안서버를 구축하기 위해서는 SSL인증서를 공인인증기관으로부터 발급받아야 합니다. 발급받기 위해서는 도메인 정보 등을 제공해야 하며, 발급받은 인증서에는 도메인 정보가 포함되어 있습니다. 평상시 접속하는 웹페이지에서 자물쇠 이미지를 확인하거나 개인정보 입력 시 암호화 호출(https://), 암호화 모듈 로딩 화면 등을 확인하였다면 유사하게 구성된 피싱 사이트를 쉽게 구별할 수 있습니다. 따라서 해커 등의 제3자가 유사사이트를 만들어 피싱을 시도하더라도 SSL 인증서가 진짜 사이트임을 증명하므로 피싱으로 인한 피해를 줄일 수 있습니다.

2.3 기업의 신뢰도 향상

사회에 대해서도 깊은 관심과 책임감을 가져야 한다는 사회책임경영의 중요성이 나날이 커져 나가고 있습니다. 사회책임경영은 기업의 사회적 책임감을 의미하는 것으로 기업의 존재기반인 사회에 대해서도 깊은 관심과 책임감을 가져야 한다는 기업경영의 화두입니다. 이에 대한 관심이 점차 높아지고 있으며, 많은 기업들이 이미 적극적으로 사회책임경영에 입각한 경영을 펼치고 있습니다.

보안서버의 설치는 고객에게 개인정보를 안전하게 관리하는 사회책임경영을 하는 기업이라는 이미지를 부각시킬 수 있습니다. 웹사이트상 보안서버 인증마크는 개인정보보호의 신뢰성을 사용자에게 보여줄 수 있으며, 가시적인 홍보효과 또한 얻을 수 있습니다.

3. 보안서버 관련 법률

1. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

▶ 제28조 (개인정보의 보호조치) ①정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실 · 도난 · 누출 · 변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적 · 관리적 조치를 하여야 한다.

4. 개인정보를 안전하게 저장 · 전송할 수 있는 암호화기술 등을 이용한 보안조치

▶ 제64조의3 (과징금의 부과 등) ① 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 전기통신사업자에게 위반행위와 관련한 매출액의 100분의 1 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 다만, 제6호에 해당하는 행위가 있는 경우에는 1억원 이하의 과징금을 부과할 수 있다.

6. 제28조제1항제2호부터 제5호까지의 조치를 하지 아니하여 이용자의 개인정보를 분실 · 도난 · 누출 · 변조 또는 훼손한 경우

▶ 제73조 (벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

1. 제28조제1항제2호부터 제5호까지(제67조에 따라 준용되는 경우를 포함한다)의 규정에 따른 기술적 · 관리적 조치를 하지 아니하여 이용자의 개인정보를 분실 · 도난 · 누출 · 변조 또는 훼손한 자

2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

▶ 제15조(개인정보의 보호조치) ④법 제28조제1항제4호에 따라 정보통신서비스 제공자등은 개인정보가 안전하게 저장 · 전송될 수 있도록 다음 각 호의 보안조치를 하여야 한다.

3. 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신 · 수신하는 경우 보안서버 구축 등의 조치

3. 개인정보의 기술적 · 관리적 보호조치 기준

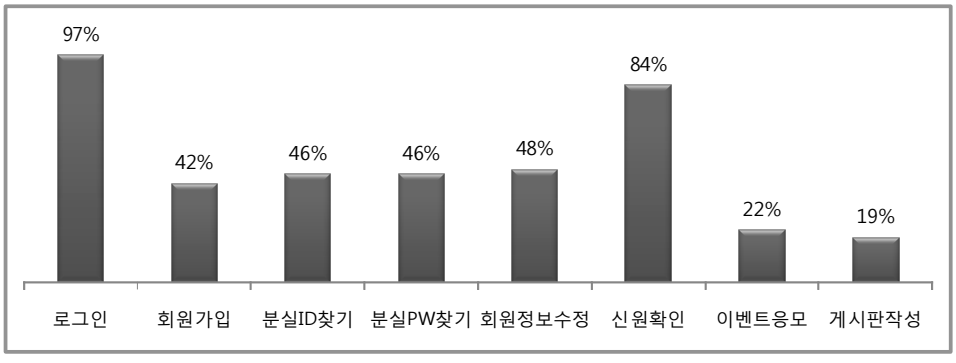
▶ 제5조(개인정보의 암호화) ②정보통신서비스제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송 · 수신할 때에는 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호의 어느 하나의 기능을 갖추어야 한다. 〈개정 2008.5.19〉

1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 개인정보를 암호화하여 송·수신하는 기능
2. 웹서버에 암호화 응용프로그램을 설치하여 개인정보를 암호화하여 송·수신하는 기능

4. 보안서버 적용 범위

일반적으로 '개인정보'라 함은 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보를 말합니다. 인터넷에서 사용되는 대표적인 개인정보의 예로는 로그인시 ID, Password, 회원가입 시 주민등록번호, 인터넷뱅킹 시 계좌번호, 계좌 Password 등이 해당됩니다. 또 게시판 등에서 사용하는 성명, 이메일, 연락처 등도 개인을 식별할 수 있는 정보로서 개인정보에 해당합니다.

이러한 개인정보를 안전하게 관리하기 위해서는 해당 개인정보를 포함하고 있는 웹페이지에 대해 암호화 통신을 적용해야 합니다. 아래 그림은 SSL 방식 보안서버에서 암호화 통신이 적용된 비율을 나타냅니다.



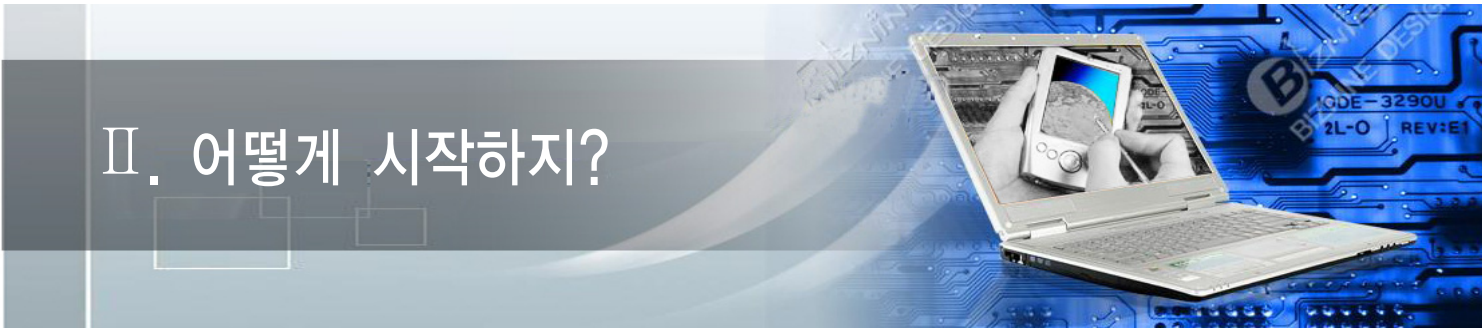
〈그림 1-2〉 SSL 방식 보안서버에서 암호화 통신이 적용된 비율

위 비율은 한국인터넷진흥원에서 보안서버를 사용하는 국내 웹사이트를 대상으로 조사를 한 내용입니다. 결과를 살펴보면 로그인 과정과 신원확인 과정의 보안서버 적용비율이 높은데 비해 회원가입, 분실ID찾기, 회원정보수정 등의 경우 보안서버 적용비율이 낮음을 확인할 수 있습니다. 이처럼 보안서버를 구축하고 있어도 암호화 통신을 하지 않으면 개인정보 유출될 수 있습니다. 그러므로 웹사이트에서 제공하는 서비스 중 개인정보를 포함하고 있는 서비스에 대해서는 보안서버의 적용이 반드시 이루어져야 합니다.

Ⅱ. 어떻게 시작하지?

1. 보안서버의 종류
2. 보안서버 구축 전문 업체
3. 보안서버 구축 절차 흐름도

Ⅱ. 어떻게 시작하지?



1. 보안서버의 종류

보안서버는 구축 방식에 따라 크게 「SSL 방식」과 「응용프로그램 방식」 2가지로 구분할 수 있습니다. 보안서버를 구별하는 방법은 아래와 같습니다.

1.1 SSL 방식

「SSL 인증서」를 이용한 보안서버는 사용자 컴퓨터에 별도의 보안 프로그램 설치가 필요 없으며, 웹 서버에 설치된 「SSL 인증서」를 통해 개인정보를 암호화하여 전송합니다. 보안서버 구축에 소요되는 비용이 상대적으로 저렴하지만 주기적으로 인증서 갱신을 위한 비용이 소요됩니다.

로그인 페이지 등 보안이 필요한 웹페이지에 접속한 상태에서 브라우저 하단 상태 표시줄에 자물쇠 모양의 마크로 확인할 수 있으며, 웹사이트의 구성 방법에 따라 자물쇠 모양의 마크가 보이지 않을 수 있습니다.

〈그림 2-1〉 SSL 방식의 보안서버 실행 확인

1.2 응용프로그램 방식

암호화 응용프로그램을 이용한 보안서버는 웹 서버에 접속하면 사용자 컴퓨터에 자동으로 보안 프로그램이 설치되고 이를 통해 개인 정보를 암호화하여 전송합니다.

웹사이트 접속 시 초기화면이나 로그인 후 윈도우 화면 오른쪽 하단 작업표시줄 알림영역에 다음 그림과 같은 암호화 프로그램 실행여부를 확인할 수 있으며, 응용프로그램 방식의 솔루션에 따라 모양은 다르게 나타날 수 있습니다.

〈그림 2-2〉 응용프로그램 방식의 보안서버 실행 확인

2. 보안서버 구축 전문 업체

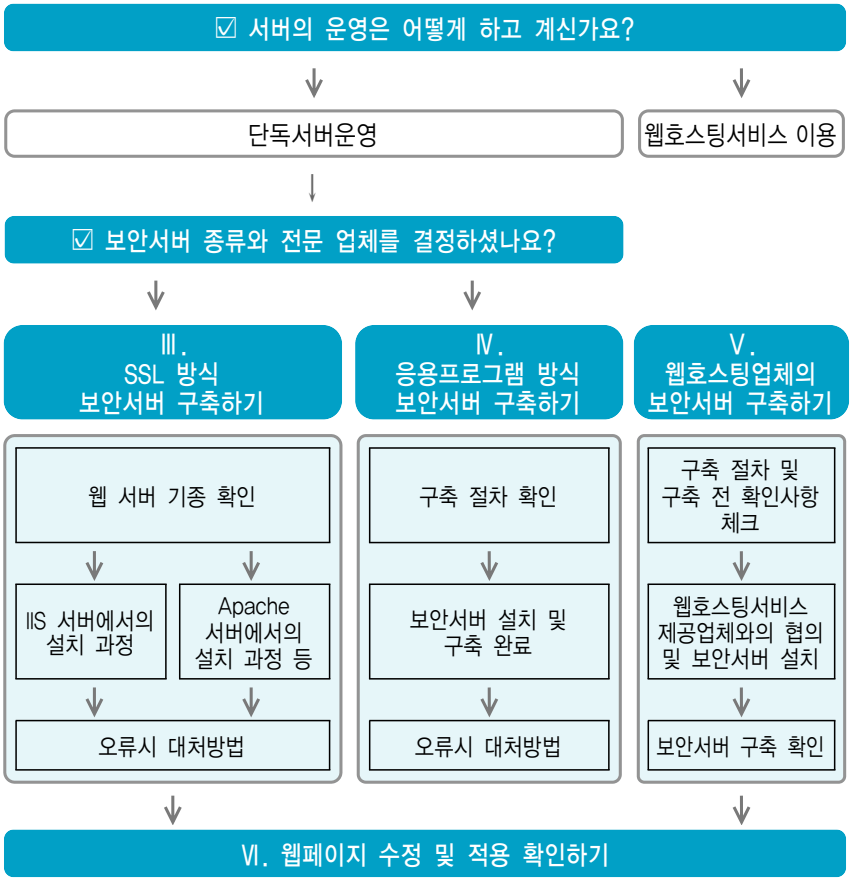
보안서버 구축 방법과 절차에 관한 보다 구체적인 내용은 다음의 「보안서버전문협의회」 회원사 중 선택하여 문의하면 자세한 설명을 받을 수 있습니다. 「보안서버전문협의회」에 소속되지 않은 전문 업체를 이용하셔도 무방합니다.

(의장사, 간사 외 회원사 가나다순)

회사명	홈페이지	연락처
SSL 방식 솔루션 공급 업체		
한국전자인증(주)	www.crosscert.com	1588-1314
한국정보인증(주)	www.kica.net	(02) 360-3065
나인포유(주)	www.certkorea.co.kr	(02) 3444-2750
(주)닷네임코리아	www.anycert.co.kr	070-7090-0800
(주)아이네임즈	cert.inames.co.kr	(02) 559-1006
(주)온오프비즈컨설츠	www.ucert.co.kr	(02) 514-7786
(주)이모션	www.trust1.co.kr	(02) 508-1222
(주)한국무역정보통신	www.tradesign.net	(02) 6000-2093
(주)한비로	www.comodossl.co.kr	1544-4755
응용프로그램 방식 솔루션 공급 업체		
한국전자인증(주)	www.crosscert.com	1588-1314
한국정보인증(주)	www.signgate.com	(02) 360-3065
(주)온오프비즈컨설츠	www.ucert.co.kr	(02) 514-7786
이니텍(주)	www.initech.com	(02) 2140-3553
드림시큐리티	www.dreamsecurity.com	(02) 2233-5533
소프트포럼	www.softforum.co.kr	(02) 526-8423
엠큐릭스(주)	www.mcurix.com	(02) 2253-8882
유넷시스템(주)	www.unetsystem.co.kr	(02) 390-8000
(주)케이사인	www.ksign.com	(02) 564-0182
(주)코스콤	www.signkorea.co.kr	(02) 767-7229
펜타시큐리티시스템(주)	www.pentasecurity.com	(02) 780-7728

3. 보안서버 구축 절차 흐름도

지금까지 보안서버의 개념과 종류 등 보안서버를 구축하기 전에 필요한 사항들을 간단하게 알아보았습니다. 이제부터는 본격적으로 보안서버 구축 방법에 대하여 알아보겠습니다. 현재 기업의 상황을 확인하시고 아래 절차 흐름도를 참고하여 자신에게 필요한 내용을 찾아 각 장으로 이동하시면 됩니다.



〈그림 2-3〉 보안서버 구축 절차 흐름도

Ⅲ. SSL 방식 보안서버 구축하기

1. 소개 및 보안서버 구축 절차
2. 설치 과정
3. 기타 SSL 인증서 소개
4. 오류 발생시 대처방법
5. 웹사이트 운영·관리상의 유의사항
6. Windows Vista에서 Internet Explorer 7 이용 시 유의사항
7. 국산 SSL 인증서 보안경고창 해결방법

Ⅲ. SSL 방식 보안서버 구축하기

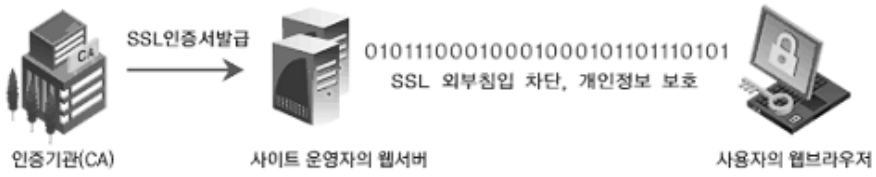
1. 소개 및 보안서버 구축 절차

1.1 개요

SSL은 Secure Sockets Layer의 약자이며, 1994년 Netscape에 의해 개발되어 현재 전 세계적인 표준 보안 기술이 되었습니다.

SSL 방식은 웹 브라우저와 서버간의 통신에서 정보를 암호화함으로써 도중에 해킹을 통해 정보가 유출되더라도 정보의 내용을 보호할 수 있는 기능을 갖춘 보안 솔루션으로 전 세계적으로 수 백 만개의 웹사이트에서 사용하고 있습니다.

아래는 SSL 보안에 대해 그림으로 간단하게 설명해 놓은 것입니다.

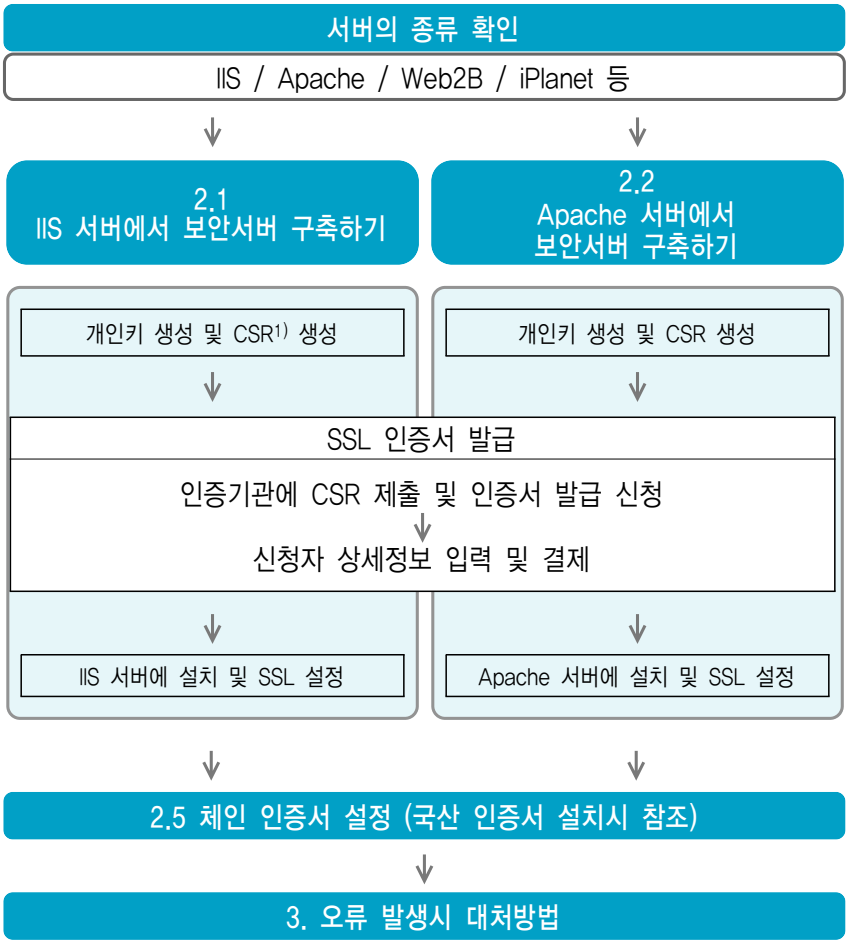


〈그림 3-1〉 SSL 방식의 보안서버 개념도

인증기관(Certification Authorities)에서 제공하는 SSL 인증서를 발급받아 웹 서버에 설치하게 되면 웹사이트 이용자들의 거래, ID/패스워드, 개인정보 등을 암호화하여 송수신할 수 있습니다.

1.2 보안서버 구축 절차

SSL 방식의 보안서버 구축 절차는 다음과 같습니다.



〈그림 3-2〉 SSL 방식 보안서버 구축 절차

1) Certificate Signing Request의 약자로써 SSL서버를 운영하는 업체의 정보를 암호화하여 인증기관으로 송부하는 인증서 신청서

① SSL 방식의 보안서버를 사용하기 위해서는 운영하고 있는 웹 서버에 보안서버 인증서가 설치되어야 합니다. 보안서버 인증서는 운영 중인 웹 서버에서 '인증서 만들기'를 이용하여 생성합니다.

※ 발급이 완료된 인증서는 재발급 또는 변경이 불가능하기 때문에 새로 발급받으셔야 하며, 새로 발급받을 시 비용이 발생할 수 있으니 CSR 생성시 **절대 주의** 바랍니다.

② 먼저 운영하는 웹 서버에서 개인키를 만든 후, CSR 파일을 생성하여 인증기관에 보안서버 인증서 발급을 신청합니다.

CSR(Certificate Signing Request)에는 운영하는 URL 및 운영하는 회사의 정보 등이 입력됩니다.

③ 인증기관에 CSR을 이용하여 인증서를 신청할 때 회사의 담당자 정보 등을 입력합니다. 인증서 발급 심사 후에 신청 시 입력한 담당자의 E-mail 주소로 인증서가 발급됩니다.

④ 발급받은 인증서를 운영 중인 웹 서버에 설치하게 되면 SSL 방식의 보안서버 설정을 완료하게 됩니다. SSL 인증서가 설치된 후 관리·운영 시 인증서의 유효성에 따라 보안경고창이 발생할 수 있으니 '4. 웹사이트 운영·관리상의 유의사항'을 확인하시기 바랍니다.

서버호스팅 서비스를 받고 있는 고객의 경우에는 서버에 대한 관리자 권한이 고객에게 있기 때문에 고객이 직접 CSR 생성 및 인증서 발행 후에 설치를 진행해야 하며, 호스팅 서비스 제공업체에게 보안서버 구축 대행을 요청하게 되면 설치대행비가 부과될 수 있습니다.

SSL 방식의 보안서버 구축은 서버의 운영체제에 따라 적용절차가 모두 다르므로 업체의 서버 종류를 파악한 후, 각 서버의 설치과정을 참고하시기 바랍니다. 본 가이드에서는 IIS, Apache, Web2B, iPlanet 서버에서 SSL 인증서를 이용하여 보안서버를 구축하는 방법을 소개하고 있으며, 향후 다른 종류의 서버에 SSL 방식의 보안서버를 설치하는 방법을 지속적으로 추가해 나갈 예정입니다.

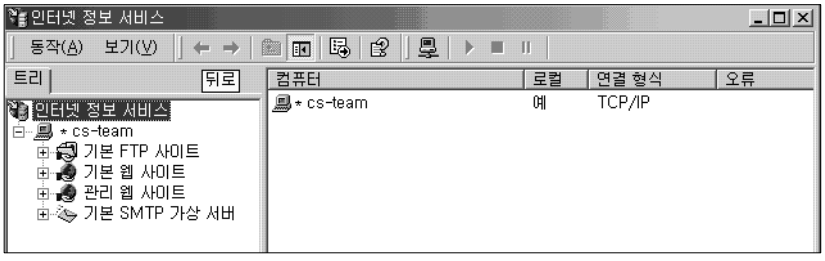
2. 설치 과정

2.1 IIS 서버에서 보안서버 구축하기

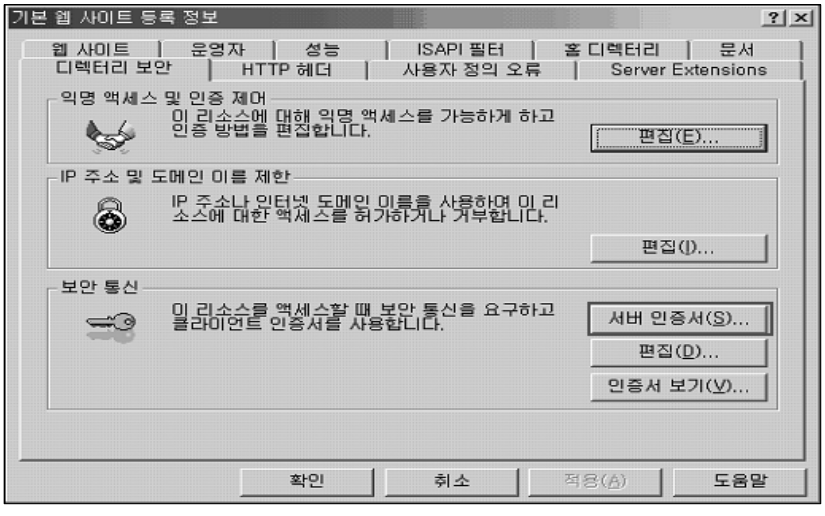
가. 개인키 생성 및 CSR 생성 방법

① 웹사이트 속성 메뉴를 선택합니다.

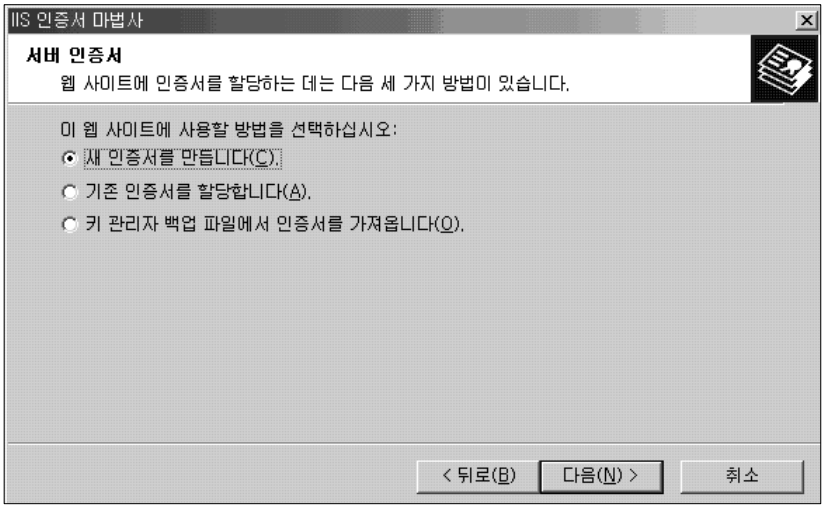
시작→프로그램→관리도구→인터넷 서비스 관리자→웹사이트→속성



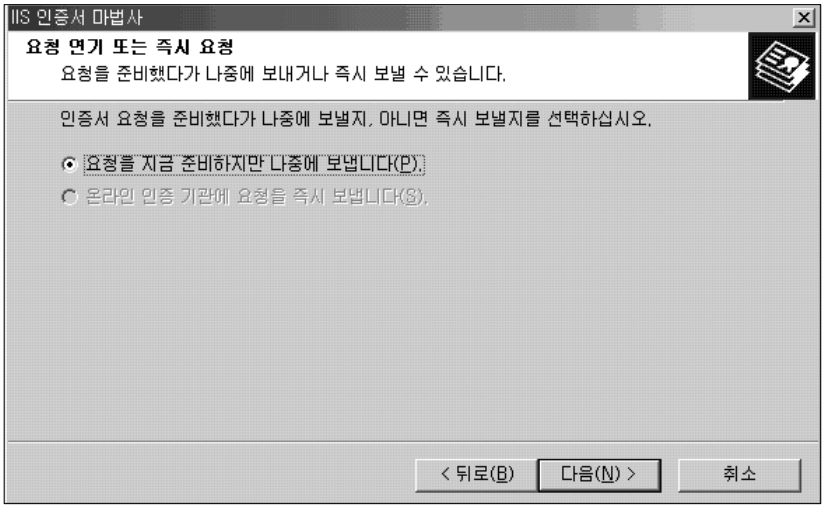
② 등록정보 화면에서 디렉토리 보안을 클릭한 후 서버 인증서를 클릭합니다.



③ 웹 서버 인증서 마법사를 시작합니다. '새 인증서를 만듭니다'를 선택합니다.

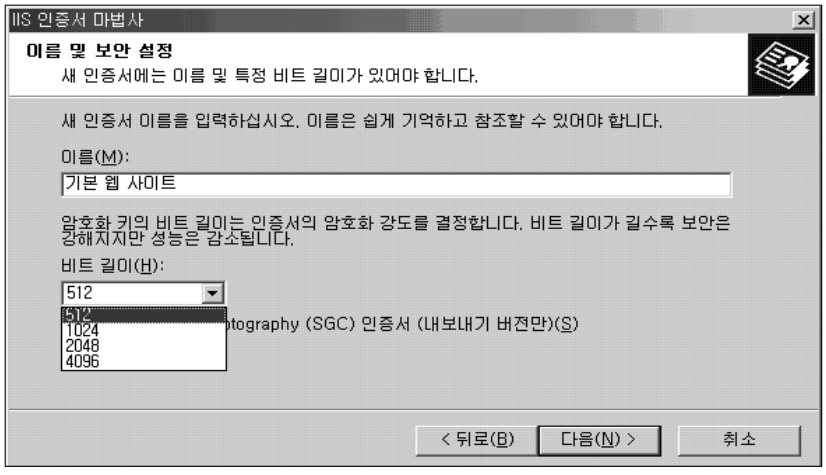


④ '요청을 준비하지만 나중에 보냅니다'를 선택합니다.



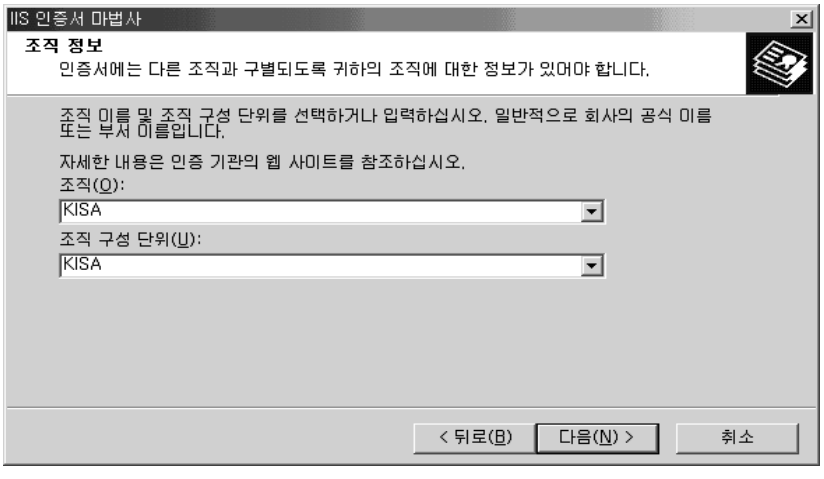
⑤ 인증서를 만들 이름을 입력하시기 바랍니다.

이름은 인증서의 별칭이므로 쉬운 것으로 입력하여 주시기 바랍니다. 인증서 키의 길이는 1,024비트가 일반적입니다. 비트 길이가 너무 크면 서버에서 인지하지 못하는 경우도 있습니다.

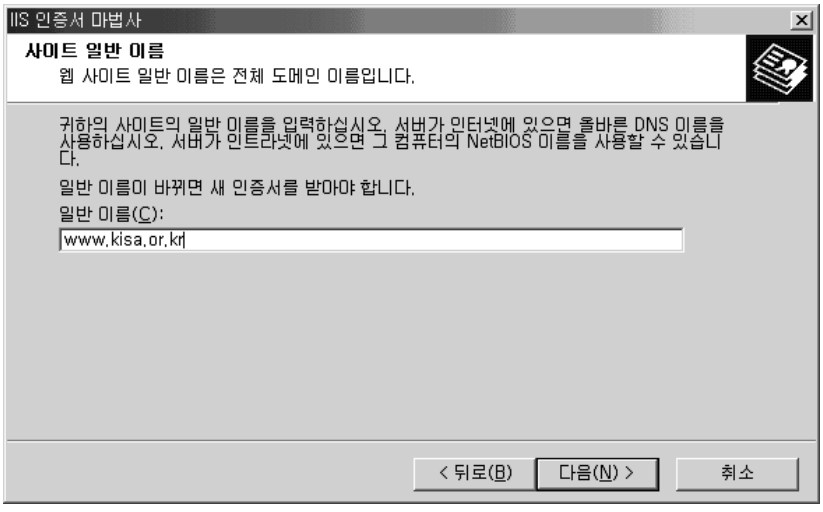


⑥ 조직 및 조직 구성 단위를 입력합니다.

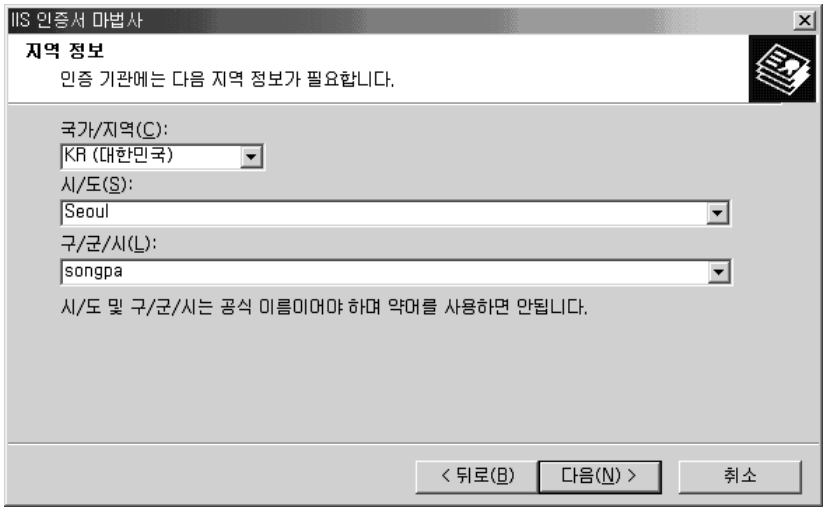
조직은 회사의 영문 전체 이름을 입력하고, 조직 구성단위는 영문 부서명을 입력합니다. (모든 내용은 영문으로 입력합니다)



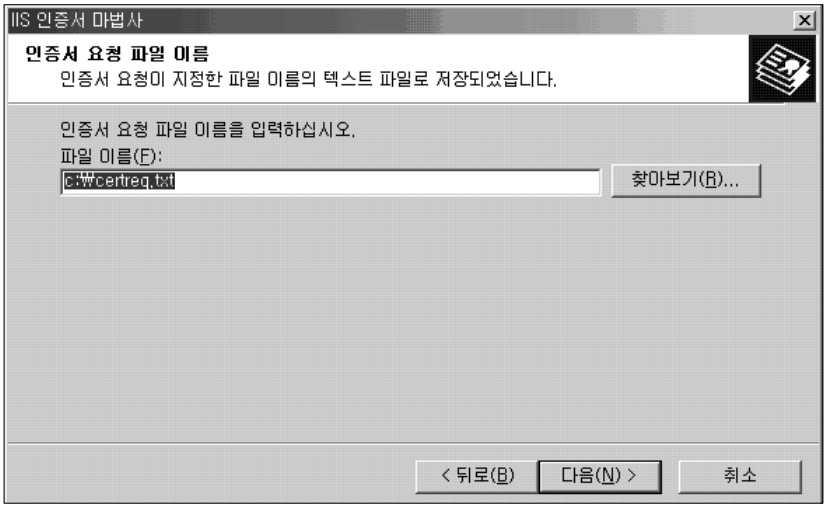
⑦ 인증받을 도메인 이름을 입력하시기 바랍니다.



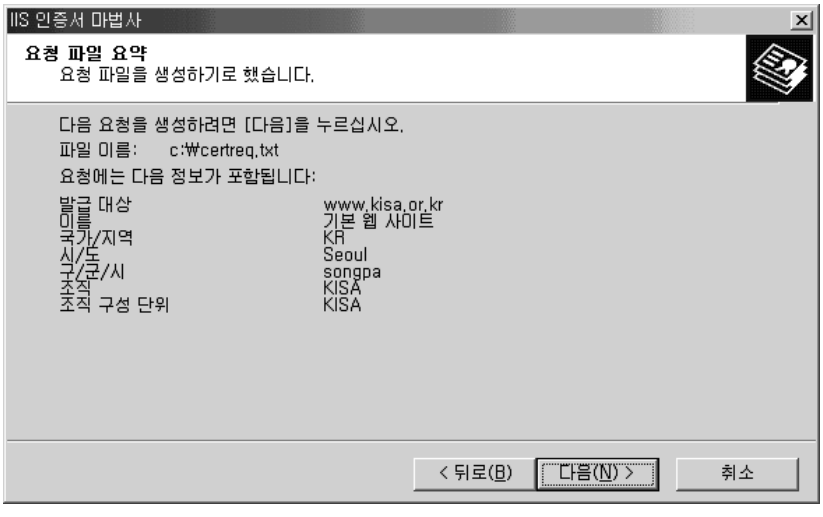
⑧ 지역 정보를 입력합니다.(모든 내용은 영문으로 입력합니다.)



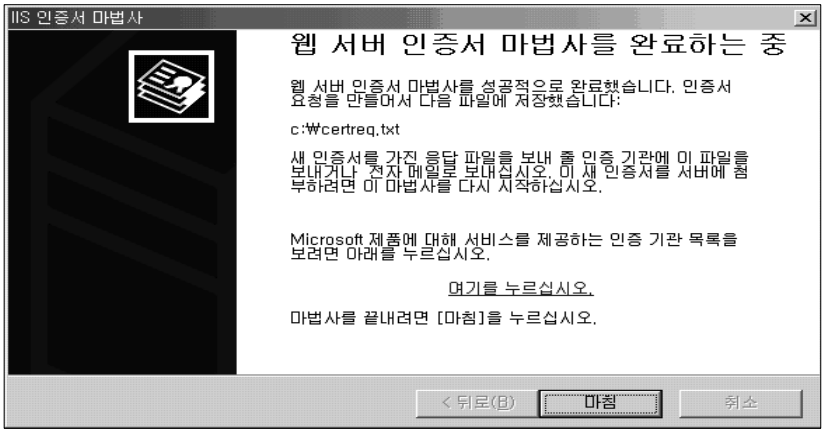
⑨ 인증서 요청파일(CSR)을 저장합니다.



⑩ 신청한 내용을 다시 한 번 확인합니다.



⑪ 인증서 신청을 완료합니다.



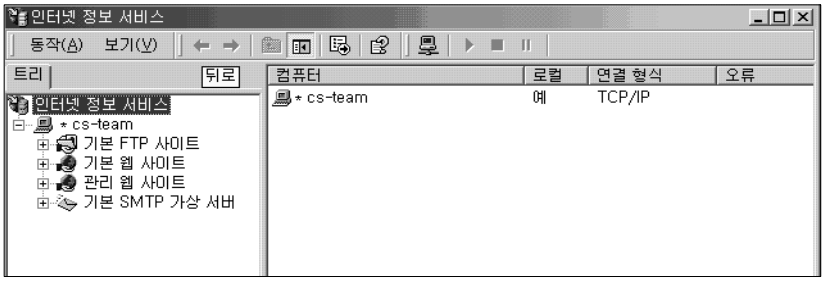
⑫ CSR 내용을 인증기관에게 메일로 송부하시던지 인증서 신청화면에 붙여 넣으신 후 인증서 신청을 진행하시면 됩니다.

자, 이제 인증기관의 발급 절차에 따라서 인증서가 발급됩니다.

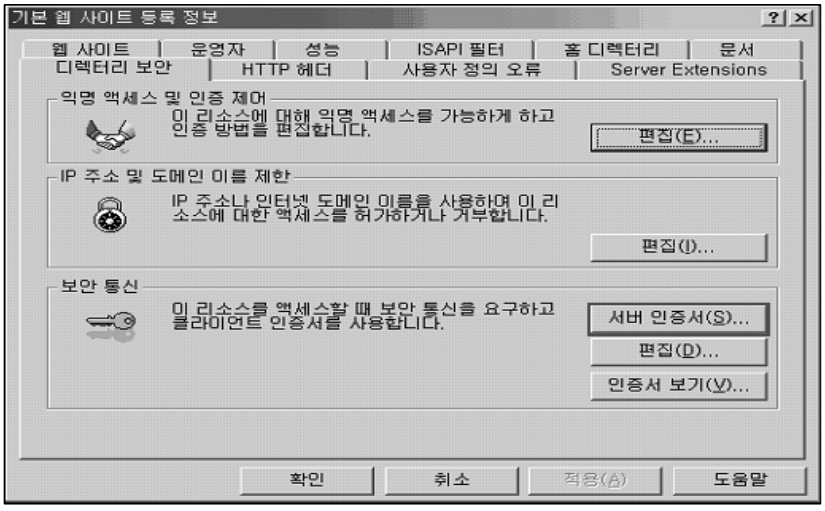
나. SSL 설정

① 웹사이트 속성메뉴를 선택합니다.

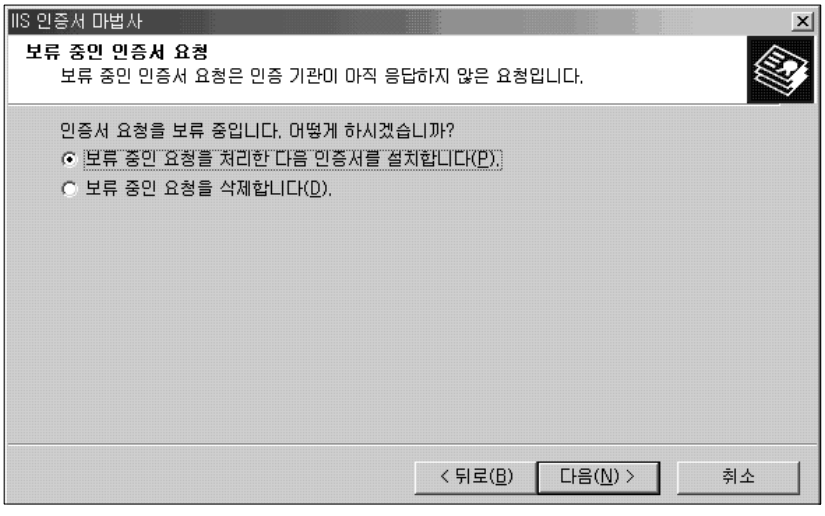
시작→프로그램→관리도구→인터넷 서비스 관리자→웹사이트→속성



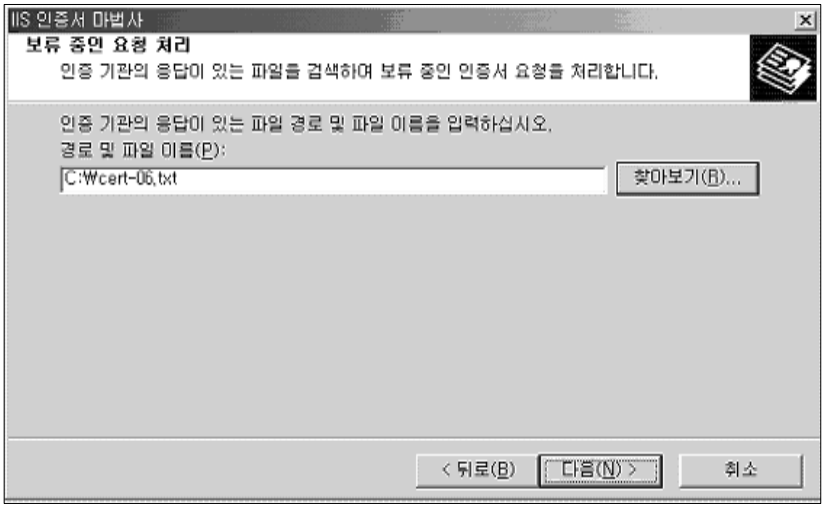
② 등록정보 화면에서 디렉토리 보안을 클릭한 후 서버 인증서를 클릭합니다.



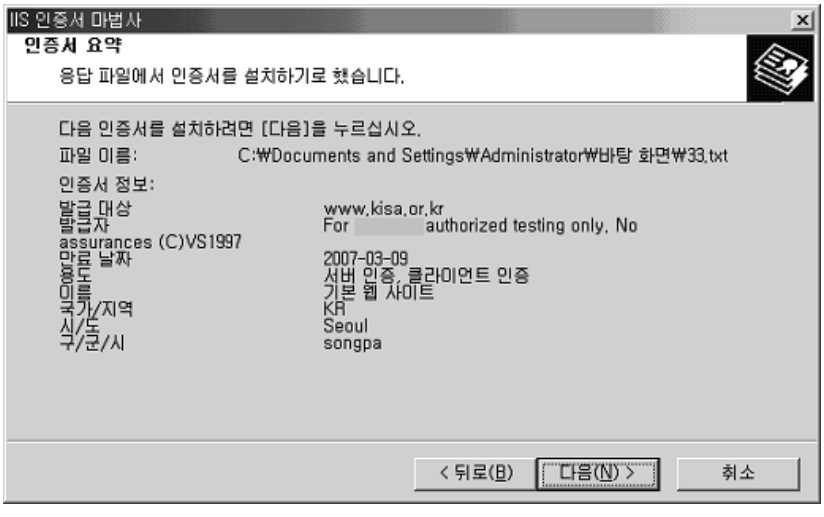
③ 보류중인 요청을 처리합니다.



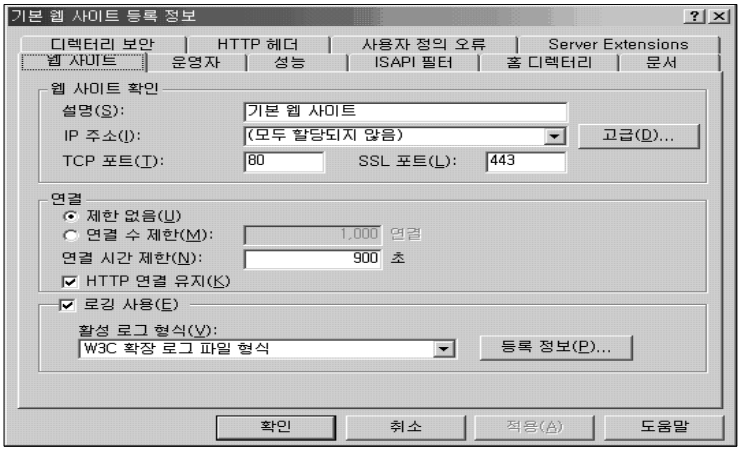
④ 보류 중인 요청 처리–메일을 통하여 받은 인증서(———begin 부터 end———까지)를 저장한 파일을 선택합니다. 인증서 파일을 선택한 후 다음 버튼을 누릅니다.



⑤ 인증서 요약 – 현재 설치하시고자 하는 인증서의 내용이 보여 집니다.
만약에 신청하신 내용과 일치하지 않으면 경고 메시지가 뜨며, 인증서가 설치되지 않습니다.
그럴 경우에는 현재의 요청을 삭제하신 후, 새로운 인증서를 신청하셔야 합니다.



⑥ 인증서 설치 후의 설정 – 기본 웹 사이트의 등록정보에서 웹사이트 탭을 선택합니다. 웹 사이트 확인 섹션에서 고급 버튼을 클릭해서 SSL 포트에 443을 설정해줍니다. (기본적으로 443을 사용하지만, 사이트 운영자가 1~65535 범위 내에서 임의로 포트 번호를 설정할 수 있습니다)



⑦ 인증서 설치 확인 – 인증서가 정확히 설치되었는지 인증서가 설치된 홈페이지를 통해 확인할 수 있습니다.

https://인증서 신청 URL에 접속해서 하단에 노란자물쇠 버튼이 뜨는지 확인합니다. 만일 443이 아닌 다른 포트로 SSL 포트를 적용하였을 경우에는 주소창 뒤에 포트번호를 지정해야 확인할 수 있습니다. (예: https://www.kisa.or.kr:442)

⑧ 이제 SSL 인증서의 설치가 완료되었습니다. 다음에는 웹페이지를 수정해야 하며, 수정방법은 Ⅵ장에 있습니다.

2.2 Apache 서버에서 보안서버 구축하기

가. Apache 서버에 OpenSSL과 mod_ssl의 설치 방법

Apache 서버에서 SSL 통신을 가능하게 하기 위해서는 OpenSSL과 mod_ssl이 필요합니다.

우선, 현재 서비스 중인 Apache 서버에 mod_ssl이 설치되어 있는지를 httpd -l 옵션을 사용하여 mod_ssl.c 또는 mod_ssl.so가 있는지 확인하시기 바랍니다. 만일 설치되어 있다면 Apache 서버의 버전에 맞는 개인키 생성 및 CSR 생성 방법 과정으로 이동하시기 바랍니다.

〈그림 3-3〉 mod_ssl 설치 확인 예

OpenSSL은 Apache 버전과 mod_ssl의 버전을 확인한 후에 알맞은 OpenSSL을 설치해야 합니다. 예를 들어 Apache 1.3.3 버전에는 mod_ssl 2.1.6 (또는 2.1.7)을 설치해야 하고, mod_ssl 2.1.6은 OpenSSL 0.8.1b와 0.9.1c 버전 사이에서만 동작합니다. 버전을 확인하지 않고 OpenSSL과 mod_ssl을 설치하면 Apache 컴파일 과정에서 오류가 발생합니다.

mod_ssl은 반드시 Apache 버전에 맞는 것을 설치하셔야 하며 www.modssl.org에서 Apache 버전을 확인한 후 그에 맞는 mod_ssl을 다운받아 설치하시기 바랍니다.

mod_ssl에서 지원하는 apache 버전 및 OpenSSL의 버전은 mod_ssl 소스의 README.Versions에서 확인할 수 있으며, www.openssl.org에서도 확인할 수 있습니다.

① OpenSSL의 설치(www.openssl.org)

압축풀기

```
$ gzip –cd openssl–0.9.6.tar.gz | tar xvf –
```

$ ./config$ make$ make installconfig

☞ prefix를 주지 않았을 때에는 /usr/local/ssl 디렉토리에 설치가 됩니다.

다른 디렉토리에 설치를 하고자 한다면 다음과 같이 설치합니다.

$ ./config –-prefix=/usr/local –-openssldir=/usr/local/openssl

☞ OpenSSL의 실행파일은 /usr/local/ssl/bin에 설치되고 인증서비스를 위한 파일들은/usr/local/openssl 아래의 디렉토리에 생성됩니다.

② mod_ssl의 설치 (www.modssl.org)

압축풀기

```
$ gzip –cd apache_1.3.19.tar.gz | tar xvf
$ gzip –cd mod_ssl–2.8.1–1.3.19.tar.gz | tar xvf
```

파일의 다운로드와 압축풀기가 끝나면 mod_ssl 설정을 합니다.

mod_ssl 설정

```
$ cd mod_ssl–2.8.1–1.3.19
$ ./configure ₩
–-with–apache=../apache_1.3.19 ₩
–-with–ssl=../openssl–0.9.6 ₩
–-prefix=/usr/local/apache
```

③ Apache 서버 설치(www.apache.org)

```
$ cd ../apache_1.3.x
$ SSL_BASE=../openssl-0.9.6 ₩
./configure ₩
--prefix=/usr/local/apache ₩
--enable-module=ssl ₩
$ make
$ make certificate
$ make install
```

나. Apache 1.3.X 버전에서 보안서버 구축하기

(1) 개인키 생성 및 CSR 생성 방법

① 랜덤 넘버 생성

```
$ openssl md5 * 〉rand.dat
```

② 키 쌍 생성

```
$ openssl genrsa -rand rand.dat -des3 -out 1024 〉key.pem
```

☞ 개인키 비밀번호를 입력하며 반드시 기억해야 합니다. (암호를 분실할 경우 SSL 사용을 위한 apache를 구동할 수 없습니다)

③ 생성된 키 쌍을 이용하여 CSR 생성

```
$ openssl req -new -key key.pem 〉csr.pem
```

☞ 여기서 key.pem은 단계 ②에서 생성한 키 이름이며 csr.pem은 출력 CSR 파일의 이름입니다.

다음 정보를 입력하라는 메시지가 나타납니다. (모든 내용은 영문으로 작성해야 하며, 아래는 입력 예입니다)

```
Country(국가 코드) : KR
State/province (시/도의 전체 이름) : Seoul
Locality(시,구,군 등의 이름) : Songpa-gu
Organization(회사 이름) : Korea Information Security Agency
Organization Unit(부서명) : Policy Development Division
Common Name (host name + domain name) : www.kisa.or.kr
```

'추가 속성'을 입력하라는 메시지가 나타나면 그냥 넘어가셔도 무방합니다.

④ CSR 제출

생성된 CSR(예:csr.pem)의 내용은 다음과 같습니다.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBETCBvAIBADBXMQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEh
MB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMRAwDgYJKoZIhvcNAQkB
FgFgMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL6nPTy3avNgbubx+ESmD4LV1LQG
...
AaAAMA0GCSqGSIb3DQEBBAUAA0EAXcMsa8eXgbG2ZhVyFkRVrl4vT8haN39/QJc9
BrRh2nOTKgfMcT9h+1Xx0wNRQ9/SIGV1y3+3abNiJmJBWnJ8Bg==
-----END CERTIFICATE REQUEST-----
```

CSR 내용을 인증기관에게 메일로 송부하거나 인증서 신청화면에 붙여 넣으신 후 인증서 신청을 진행하시면 됩니다.

인증기관의 발급 절차에 따라서 인증서가 발급됩니다.

(2) 인증서 설치 방법

① 메일로 받은 인증서를 복사하여 파일로 저장합니다.(예: Cert.pem)

```
------BEGIN CERTIFICATE------
MIIBETCBvAIBADBXMQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZT
EhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMRAwDgYJKoZIhvcNAQ
kBFgFgMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL6nPTy3avNgbubx+ESmD4LV
...
AAaAAMA0GCSqGSIb3DQEBBAUAA0EAXcMsa8eXgbG2ZhVyFkRVrl4vT8haN39/QJc
9BrRh2nOTKgfMcT9h+1Xx0wNRQ9/SlGV1y3+3abNiJmJBWnJ8Bg==
------END CERTIFICATE------
```

② Apache 서버의 적절한 위치에 저장합니다.

③ 환경설정 파일(httpd.conf 또는 ssl.conf)을 수정합니다. 다음은 설정 예입니다.

```
〈VirtualHost _default_:443〉
#  General setup for the virtual host
DocumentRoot /Apache/htdocs
ServerName www.kisa.or.kr:443
ServerAdmin admin@kisa.or.kr
ErrorLog logs/error_log
TransferLog logs/access_log
SSLCertificateFile /Apache/ssl/cert.pem → 인증서 파일 경로
SSLCertificateKeyFile /Apache/ssl/key.pem → 개인키 파일 경로
```

④ Apache 서버를 재구동합니다.

```
./apachectl startssl
```

Apache 서버에서 SSL을 사용하기 위한 시작 명령어인 startssl을 실행하면 개인키의 비밀번호를 묻는데, 이 비밀번호는 이전의 설치과정 '개인키 생성 및 CSR 생성 방법' 중 ② 키 쌍 생성 시 입력한 개인키 비밀번호를 입력하시면 됩니다.

⑤ 이제 SSL 인증서의 설치가 완료되었습니다. Ⅵ장으로 이동하셔서 실제 웹페이지를 어떻게 수정해야 하는지 알아보겠습니다.

다. Apache 2.X 버전에서 보안서버 구축하기

(1) 개인키 생성 및 CSR 생성 방법

① 랜덤 넘버 생성

개인키 생성 시 사용할 랜덤 정보를 생성합니다. 생성된 rand.dat 파일이 중요하지 않다고 판단될 때, 언제든지 이 파일을 삭제, 변경할 수 있습니다.

```
$ openssl sha1 * 〉 rand.dat
또는
$ cat file1 file2 file3 〉 rand.dat
```

② 키 쌍 생성

```
$ openssl genrsa -rand rand.dat -des 1024 〉 key.pem
```

☞ 개인키 비밀번호를 입력하며 반드시 기억해야 합니다. (암호를 분실할 경우 SSL 사용을 위한 apache를 구동할 수 없습니다)

☞ 개인키를 분실하신 경우, 백업된 개인키를 사용해야 하므로, 생성한 개인키의 백업 복사본은 별도의 저장매체에 보관하여 주시기 바랍니다.

③ 생성된 키 쌍을 이용하여 CSR 생성

```
$ openssl  req  -new  -key  key.pem  -out  csr.pem
```

☞ 여기서 key.pem은 단계 ②에서 생성한 키 이름이며 csr.pem은 출력 CSR 파일의 이름입니다.

다음 정보를 입력하라는 메시지가 나타납니다. (모든 내용은 영문으로 작성해야 하며, 아래는 입력 예입니다)

```
Country(국가 코드) : KR
State/province (시/도의 전체 이름) : Seoul
Locality(시,구,군 등의 이름) : Songpa-gu
Organization(회사 이름) : Korea Information Security Agency
Organization Unit(부서명) : Policy Development Division
Common Name (host name + domain name) : www.kisa.or.kr
```

'추가 속성'을 입력하라는 메시지가 나타나면 그냥 넘어가셔도 무방합니다.

④ CSR 제출

생성된 CSR(예:csr.pem)의 내용은 다음과 같습니다.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBETCBvAIBADBXMQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEh
MB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMRAwDgYJKoZIhvcNAQkB
FgFgMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL6nPTy3avNgbubx+ESmD4LV1LQG
...
AaAAMA0GCSqGSIb3DQEBBAUAA0EAXcMsa8eXgbG2ZhVyFkRVrl4vT8haN39/QJc9
BrRh2nOTKgfMcT9h+1Xx0wNRQ9/SlGV1y3+3abNiJmJBWnJ8Bg==
-----END CERTIFICATE REQUEST-----
```

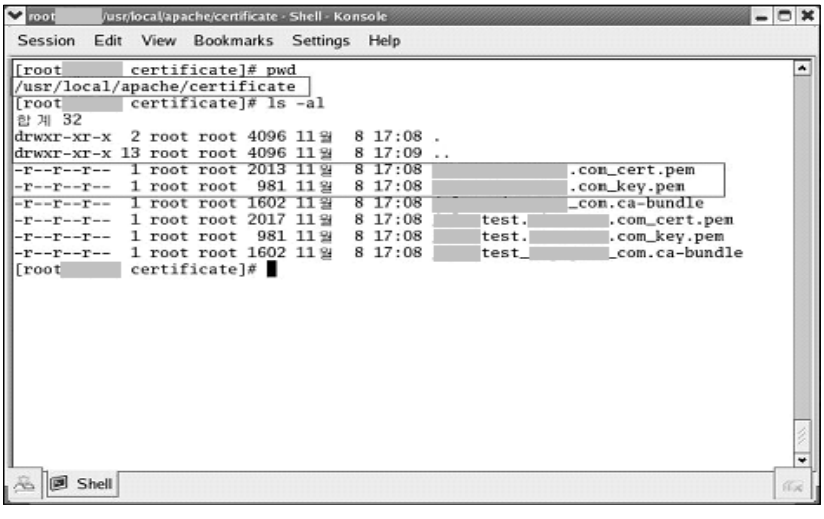
CSR 내용을 인증기관에게 메일로 송부하거나 인증서 신청화면에 붙여 넣으신 후 인증서 신청을 진행하시면 됩니다.
인증기관의 발급 절차에 따라서 인증서가 발급됩니다.

(2) 인증서 설치 방법

① 메일로 받은 인증서를 복사하여 파일로 저장합니다.(예: Cert.pem)

```
------BEGIN CERTIFICATE------
MIIBETCBvAIBADBXMQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZT
EhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMRAwDgYJKoZIhvcNAQ
kBFgFgMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL6nPTy3avNgbubx+ESmD4LV
...
AAaAAMA0GCSqGSIb3DQEBBAUAA0EAXcMsa8eXgbG2ZhVyFkRVrl4vT8haN39/QJc
9BrRh2nOTKgfMcT9h+1Xx0wNRQ9/SIGV1y3+3abNiJmJBWnJ8Bg==
------END CERTIFICATE------
```

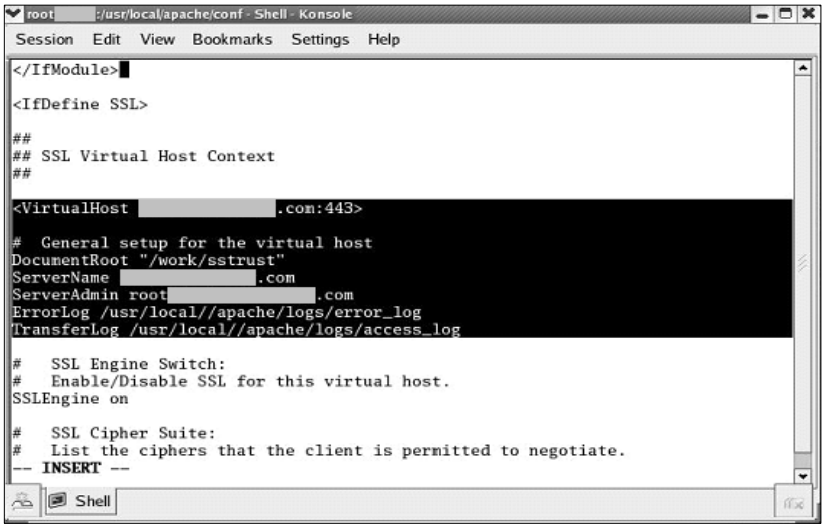
② Apache 서버의 적절한 위치에 저장합니다.



③ ssl.conf 수정 (virtual host 설정)

ssl.conf의 https(SSL)을 사용하기 위해 구성된 virtual host 부분을 http 설정 부분과 동일하게 수정합니다. 다음은 설정 예입니다.

```
〈VirtualHost www.kisa.or.kr:443〉
# General setup for the virtual host
DocumentRoot /usr/local/apache/htdocs
ServerName www.kisa.or.kr:443
ServerAdmin root@kisa.or.kr
ErrorLog /usr/local/apache/logs/ssl_error_log
TransferLog /usr/local/apache/logs/ssl_access_log
```

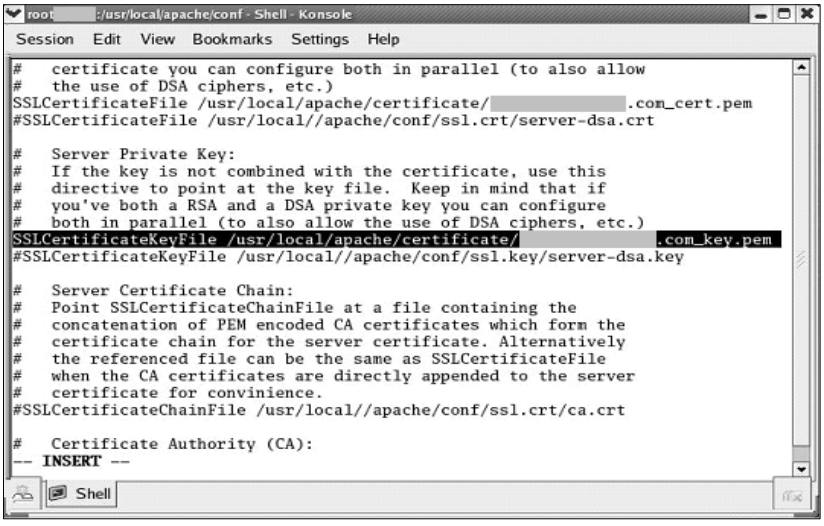


④ ssl.conf 수정 (키 파일과 인증서 설정)

ssl.conf 파일에서 인증서 파일과 개인키 파일의 위치와 이름을 알맞게 수정합니다.

인증서 설정 : SSLCertificateFile /usr/local/apache/cert/(domain name)_cert.pem

개인키 설정 : SSLCertificateKeyFile /usr/local/apache/certificate/(domain name)_key.pem



⑤ 웹 서버 재구동

– httpd.conf 파일에 오류가 없는지 확인

/usr/local/apache/bin/apachectl -t

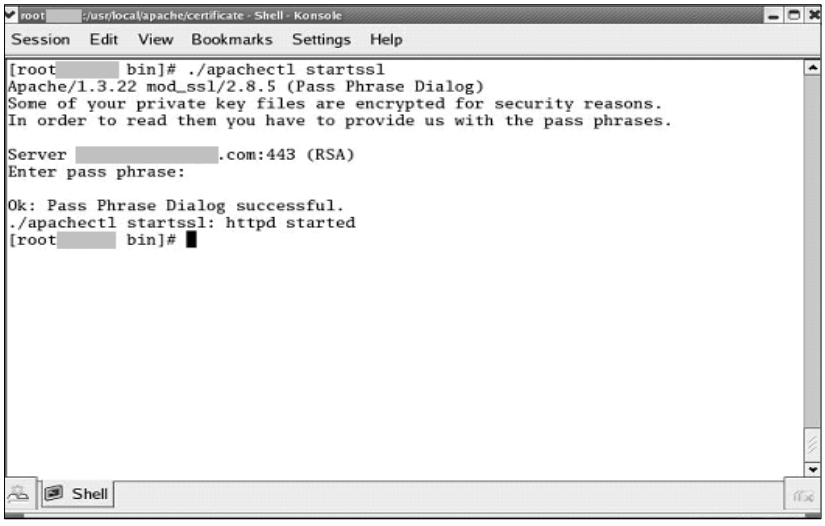
Syntax OK 라고 나오면 오류가 없습니다.

– 기존 아파치 서비스 중단

/usr/local/apache/bin/apachectl stop

– http, https 웹 서버를 구동

/usr/local/apache/bin/apachectl start 실행 후 인증서 개인키 패스워드 입력하면 http(80)과 https(443) 두 서비스가 실행



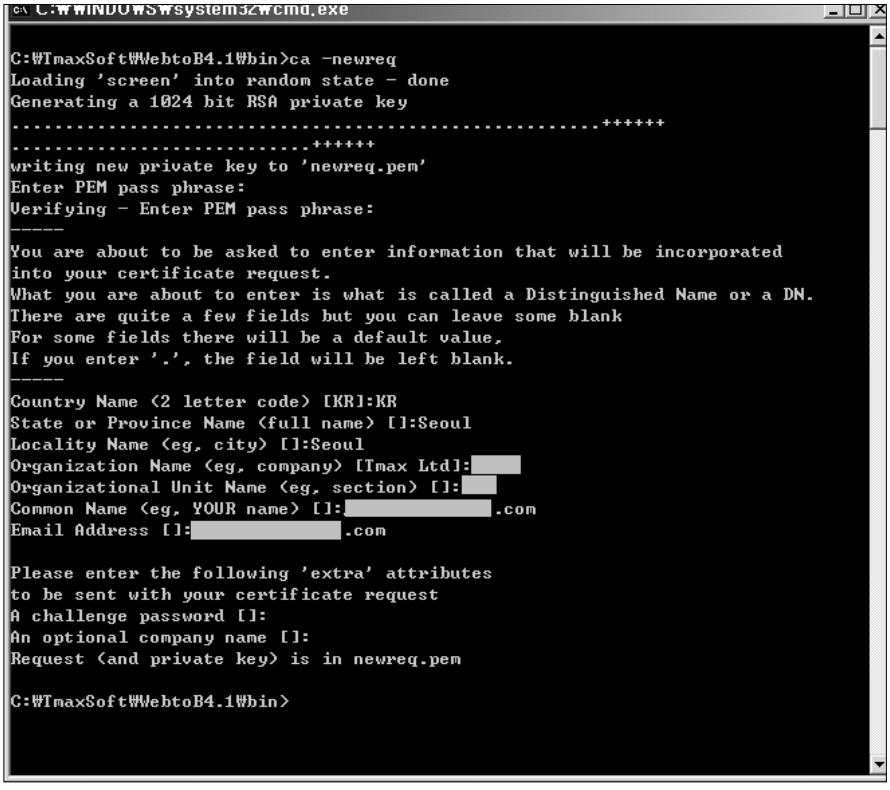
⑥ 이제 SSL 인증서의 설치가 완료되었습니다. Ⅵ장으로 이동하셔서 실제 웹페이지를 어떻게 수정해야 하는지 알아보겠습니다.

2.3 Web2B 서버에서 보안서버 구축하기

가. 개인키 생성 및 CSR 생성 방법

① CSR 정보 입력

Web2B 웹 서버의 홈 폴더 아래에 bin 폴더에 'CA' 명령어를 실행하여 CSR을 생성합니다.



※ Pass phrase : 개인키 비밀번호로 SSL 기동 때 확인

※ Common Name : 해당 웹 사이트의 도메인 명

② CSR 추출

생성된 newreq.pem에는 (암호화된) 개인키와 CSR의 정보가 함께 포함되어 있습니다.
CSR 정보는 다음과 같습니다.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIByzCCATQCAQAwgYoxCzAJBgNVBAYTAktSMQ4wDAYDVQQIEwVTZW91bDEOMAwG
A1UEBxMFU2VvdWwxDTALBgNVBAoTBEtJQ0ExDDAKBgNVBAsTA0lDQzEbMBkGA1UE
AxMSamNsZWUuc2lnbmdhdGUuY29tMSEwHwYJKoZIhvcNAQkBFhJqY2xlZUBzaWdu
...
JSHC5uBNGVCOoUOEtSEkUfTi7a5Nt+2/4R/dy+z/SQ==
-----END CERTIFICATE REQUEST-----
```

CSR 내용을 인증기관에게 메일로 송부하거나 인증서 신청화면에 붙여 넣으신 후 인증서 신청을 진행하시면 됩니다.
인증기관의 발급 절차에 따라서 인증서가 발급됩니다.

나. 인증서 설치 방법

① 메일로 받은 인증서를 저장합니다.

CSR 생성 과정에서 만들어진 newreq.pem 파일의 내용 중 위 부분의 개인 키와 인증기관에서 발급받은 (domain_name).crt의 내용을 합쳐서 cert.pem이란 새 이름으로 저장합니다.

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,885B4E9CEAF5B262

lMVVcOgjOXGFB7vS+7NhOVKjoC6tFaANiX1WkOpea49fp7cVKWlYEWYJ3Exf8zsB
4DEypbzv5ToHHuvOU5mbTdrSIqpBJWAIdL1AEiDYam6OqSCdgCZcJYvC4y/SJgfc
ZittzyL+kNMKlRzeS4EDLEBLvcvP8kFmuT3f/LIVWYdDAzO7NYi6c1VPaNacJ6nI
ztrAGvzwodzLCmvNynAvyDKDFu1k2zPWM1TkwKVRLcnWMq1qImvelXJ/QuAy+XM1
KoKYWPmALryNH/4mEgpOCbZ/33d+sACKUhXpm/NFWP1ZqDS/NoljYQsfQiVM3vcK

8JTq2vR1D/A1trcpzv1u8oqBnXXbXXJ4qAB4DEuh5o9BOOhI3hLTEwIvu6UYiLBn
RFuRwgjiUR7dcfYVVg8v9N/uF+yc+oGIEiXe1eoVmmuzeKULnkZwxHfzQlC1Ss1f
qyVo5GCTNAd7ydNwhzhp1/8+ffmCzO7MtoXjSMtnZj7hVe/WWhOREWdMOukwtBcP
y3NDzsMHFLk5cVVrMeaTdcIkFY/scqGJ23y5MejgJ54FaIWJe75OMyLG3BYPPYZV
PNC/l3ed4hJFoVfaoGOt/jkTB+YLbU9Vbbw8HymqV7l7t+7U2Zr/F+7AHEXoGTTv
Dg9Ocb2LyOL7bt837FQ8O9talydkcrhHa3KkMyP6/kuJDStj9KN54EoU+AoS9TsT
ge97ADIrKa/ASftv6gjT1mdOOFZEqNgvLYiUD1XRCtEtngPymDF6cA==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIEpjCCA46gAwIBAgIQRurwlgVMxeP6ZepunOLGZDANBgkqhkiG9w0BAQUFADBv
MQswCQYDVQQGEwJTRTEUMBIGA1UEChMLQWRkVHJ1c3QgQUIxJjAkBgNVBAsTHUFk
ZFRydXNOIEV4dGVybmFsIFRUUCBOZXR3b3JrMSIwIAYDVQQDExlBZGRUcnVzdCBF
eHRlcm5hbCBDQSBSb290MB4XDTA1MDYwNzA4MDkxMFoXDTIwMDUzMDEwNDgzOFow
gZMxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJVVDEXMBUGA1UEBxMOU2FsdCBMYWtl
IENpdHkxHjAcBgNVBAoTFVRoZSBVUOVSVFJVU1QgTmVOd29yazEhMB8GA1UECxMY
aHROcDovL3d3dy51c2VydHJ1c3QuY29tMRswGQYDVQQDExJVVE4gLSBEQVRBQ29y
cCBTROMwggEiMAOGCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDf7lgQoituVcSO
vy5GCefgCA8uK3oTlBu99raAjmUFkwAevK/iD44ZDRJH7Kyto/oucPjebvtWQhWe
L1zvI94huQV2JxkPT9bDnLS+lBlj8qYRCutTSJy+8ik7FugaoEymyfQYWWjAcPJT

zBfAssDO/jI/KSqVe9jypO4PVHyhDYCzCQPB/1zdXpo+vK68R4pqrnHKH7EquF9C
BQvsRjDRcgvK6VZt9e/feL5hurKlrgRMvKisaRWXve/rtIy/NfjUw9EoDlw6n3AY
MyB3xKKvAgMBAAGjggEXMIIBEzAfBgNVHSMEGDAWgBStvZh6NLQm9/rEJlTvA73g
JMtUGjAdBgNVHQ4EFgQUUzLRs89/+uDxoF2FTpLSnkUdtE8wDgYDVR0PAQH/BAQD
AgEGMA8GA1UdEwEB/wQFMAMBAf8wIAYDVR0lBBkwFwYKKwYBBAGCNwoDAwYJYIZI
AYb4QgQBMBEGA1UdIAQKMAgwBgYEVR0gADB7BgNVHR8EdDByMDigNqAOhjJodHRw
Oi8vY3JsLmNvbW9kb2NhLmNvbS9BZGRUcnVzdEV4dGVybmFsQOFSb290LmNybDA2
oDSgMoYwaHR0cDovL2NybC5jb21vZG8ubmVOLOFkZFRydXNORXhOZXJuYWxDQVJv
b3QuY3JsMAOGCSqGSIb3DQEBBQUAA4IBAQBjhpIQsRP6N76OKrYbikP1XK4OFN/3
aUB/vxpxAAnYv9QkSr/gk/8B2AvGD+x+R5ywXfd8FJ38wDOShFvSg/RS4iJYdPxD
Gz+no1jaA/288Drk7cwSu8m5rnsEoARyv+neLdKnUWYAc9K9fqqeU5Z9abIYPo6t
VlB+99Ww/zliZYKMllfDj/dg9sKNNIf8TOPl278cqvaGzebfET+NB/dtgxPAOIg5
YKF+MOHjiD6ku2NvLOmKaCzulmmsBGHhTO4OnXJM9nk4yMdIaW+UD3SOvMjPVO25
dXGWDYoGC+vdOPA8fcYumEZqOMcCtci4smV13tqQCLZ3uFMAJctHynNf
```

② Config 설정

SSL은 443 포트를 사용하기 때문에 버추얼 호스트 노드를 하나 추가해야 합니다.

아래는 SSL을 적용시킨 config 파일 예입니다.

```
*DOMAIN
webtob1

*NODE
IISTest         WEBTOBDIR="C:/TmaxSoft/WebtoB4.1",
                SHMKEY = 54000,
                DOCROOT="C:/TmaxSoft/WebtoB4.1/docs",
                PORT = "80,443",
                HTH = 1,
                NODENAME = "$(NODENAME)",
                LOGGING = "log1",
                ERRORLOG = "log2"

*VHOST
ssl1
                NODENAME ="IISTest",
                HostName="IITest.signgate.com",
                DOCROOT="C:/TmaxSoft/WebtoB4.1/docs",
                PORT="443",
                SSLFLAG=Y,
                SSLName=ssl1

*SVRGROUP
htmlg           NODENAME = "IISTest", SVRTYPE = HTML
cgig            NODENAME = "IISTest", SVRTYPE = CGI
ssig            NODENAME = "IISTest", SVRTYPE = SSI

*SERVER
html            SVGNAME = htmlg, MinProc = 2, MaxProc = 10
cgi             SVGNAME = cgig, MinProc = 4, MaxProc = 10
ssi             SVGNAME = ssig, MinProc = 2, MaxProc = 10
```

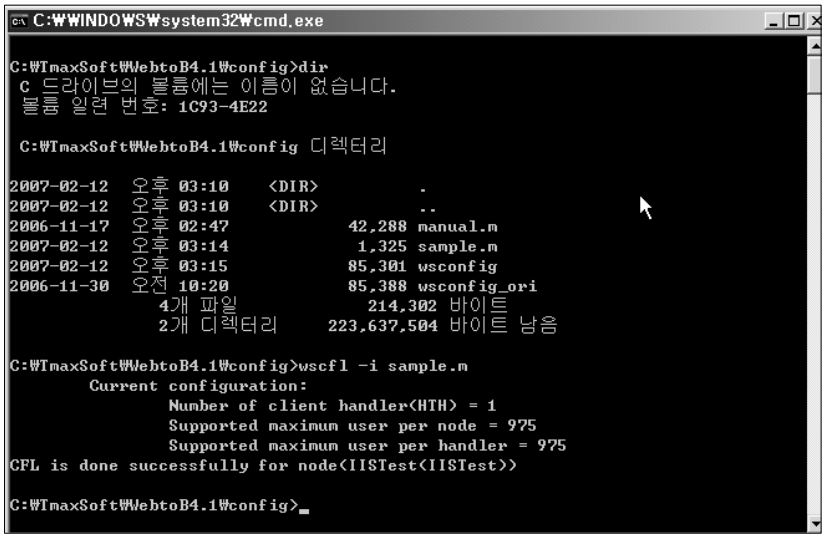
```
*SVRGROUP
htmlg           NODENAME = "IISTest", SVRTYPE = HTML
cgig            NODENAME = "IISTest", SVRTYPE = CGI
ssig            NODENAME = "IISTest", SVRTYPE = SSI

*SERVER
html            SVGNAME = htmlg, MinProc = 2, MaxProc = 10
cgi             SVGNAME = cgig, MinProc = 4, MaxProc = 10
ssi             SVGNAME = ssig, MinProc = 2, MaxProc = 10

*URI
uri1            Uri = "/cgi-bin/*",   Svrtype = CGI

*ALIAS
alias1   URI = "/cgi-bin/", RealPath = "C:/TmaxSoft/WebtoB4.1/cgi-bin/"

*LOGGING
log1            Format = "DEFAULT", FileName = "C:/TmaxSoft/WebtoB4.1/log/access.log",
                Option = "sync"
log2            Format = "ERROR", FileName = "C:/TmaxSoft/WebtoB4.1/log/error.log",
                Option = "sync"

*SSL
ssl1            CertificateFile="C:₩TmaxSoft₩WebtoB4.1₩ssl₩cert.pem",
                CertificateKeyFile="C:₩TmaxSoft₩WebtoB4.1₩ssl₩cert.pem"
                #CaCertificateFile="C:/Documents and Settings/Administrator/바탕 화면/IITest_[redacted]/rootca.

*EXT
htm             MimeType = "text/html", SvrType = HTML
```

※ 네모로 표시된 부분을 추가해 주셔야 하며, 주석 처리되어 있는 CaCertificateFile 부분(#)은 생략 가능합니다.

③ Config 컴파일

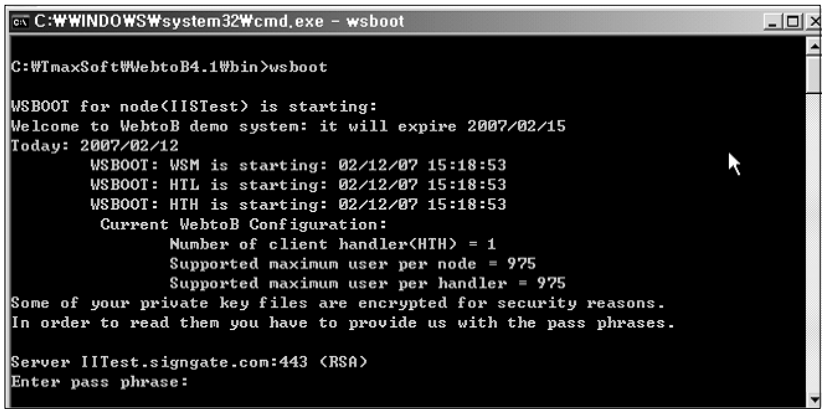
수정된 sample.m파일을 웹 서버에서 사용할 수 있도록 wscfl 명령어를 사용하여 컴파일 하는 과정이 필요합니다.

예) wscfl -i sample.m



④ 웹 서버 구동

Wsboot 명령어를 사용하여 서버를 구동하고, 인증서 생성과정에서 입력했던 개인키 비밀번호를 입력하시면 됩니다.



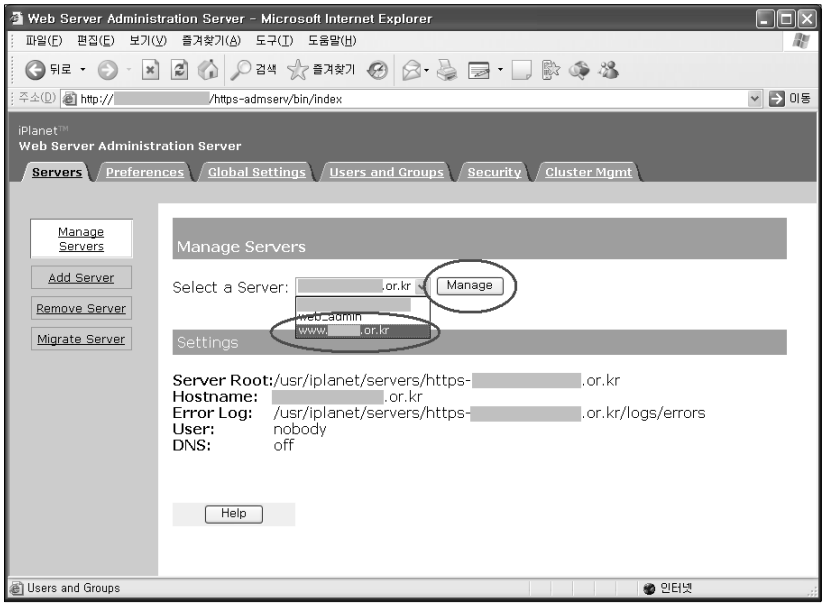
⑤ 이제 SSL 인증서의 설치가 완료되었습니다. Ⅵ장으로 이동하셔서 실제 웹페이지를 어떻게 수정해야 하는지 알아보겠습니다.

2.4 iPlanet 서버에서 보안서버 구축하기

가. 개인키 생성 및 CSR 생성 방법

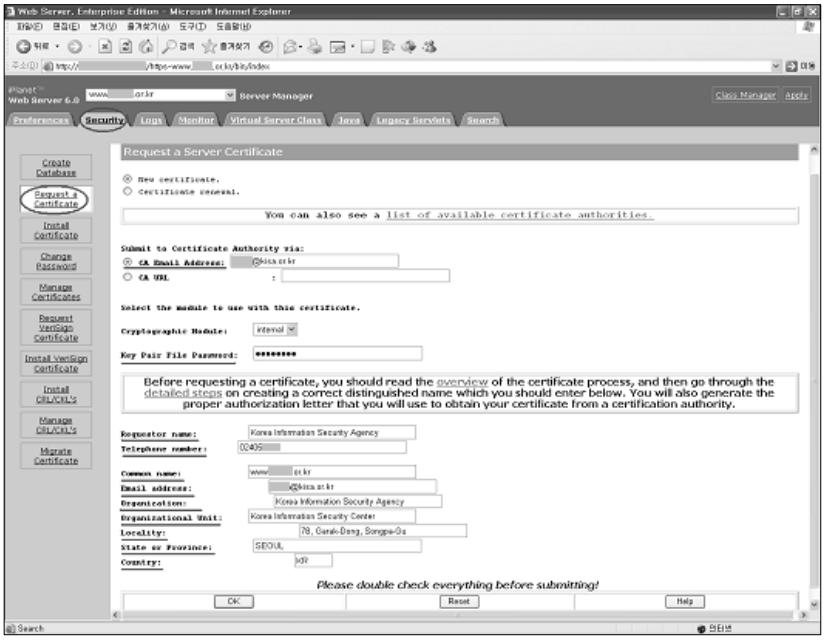
① 서버관리 화면에서 서버 선택

서버관리 화면의 콤보박스에서 보안서버를 구축하고자 하는 웹 서버를 선택하고 'Manage' 버튼을 누릅니다.



② CSR 생성을 위한 정보 입력

Security Tab을 누르고 왼쪽 메뉴에서 'Request a Certificate'를 선택하여 필요한 정보를 입력한 후 'OK' 버튼을 선택합니다.



입력해야 할 정보는 다음과 같습니다. (그림의 밑줄 참고)

- CA Email Address : 관리자의 이메일 주소
- Key Pair File Password : 관리 패스워드
- Requestor Name : 회사명
- Telephone Number : 관리자의 전화번호
- Common Name : 웹서버의 주소
- Email Address : 관리자의 이메일 주소
- Organization : 회사명(Full Name 입력)
- Organization Unit : 부서명

- Locality : 주소
- State or Province : 도시명
- Country : KR(대한민국)

③ CSR 생성

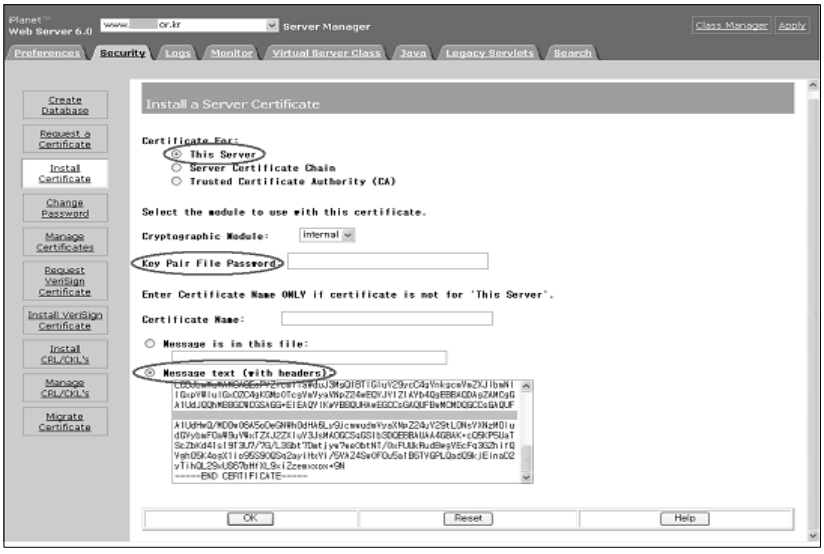
'OK' 버튼을 선택하면 다음과 같은 정보가 생성됩니다. CSR 내용을 인증기관에게 메일로 송부하거나 인증서 신청화면에 붙여 넣은 후 인증서 신청을 진행하면 됩니다. 인증기관의 발급 절차에 따라서 인증서가 발급됩니다.

```
Your certificate request has been sent.
When the response arrives, you can use the Install Certificate page to put it in place.
A copy of the certificate request has been saved in the file:
/tmp/mailtmp.18623

To:      @kisa.or.kr
Subject: Certificate request
Email:       @kisa.or.kr

Webmaster:       @kisa.or.kr
Phone:  02405

Common-name: www.       .or.kr
Email:       @kisa.or.kr
Organization: Korea Information Security Agency
Org-unit: Korea Internet Security Center
Locality: 78, Garak-Dong, Songpa-Gu
State: SEOUL
Country: KR

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB8jCCAVsCAQAwgbExCzAJBgNVBAYTAktSMQ4wDAYDVQQIEwVTRU9VTDEiMCAG
A1UEBxMZNzgsIEdhcmFrLURvbmcsIFNvbmdwYS1HdTEqMCgGA1UEChMhS29yZWEg
SW5mb3JtYXRpb24gU2VjdXJpdHkgQWdlbmN5MScwJQYDVQQLEx5Lb3J1YSBJbnRl
cm5ldCBTZWN1cml0eSBDZW50ZXIxGTAXBgNVBAMTEHd3dy5rcmNlcnQub3Iua3Iv
g28wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALFkqpG1imUdrqWWUTO0yc7wOkvv
G2rmFVHomEazWwkGHjGF1ue48m4SuxJyoo1ESAHtv6HoMbw3w7xsEgK0aG9QUkRZ
rFUNPblUAEA1umphAgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQChDN7KiFT5+1ak
hwNsyAzPiRkIvKogSMyz10sVmIEHUvf48jCEa7W1I9dTkTf+r1268p5G9oZjYBEy
9NdlcYNdTLc8HiJp+ucg9ZR2/hR+0ySRAMSAphk5SP/LnOIr1hpEurLf0xtHZycC
Izrycu6KwFHUcK1qVoaBAp1abQeAAQ==
-----END NEW CERTIFICATE REQUEST-----
```

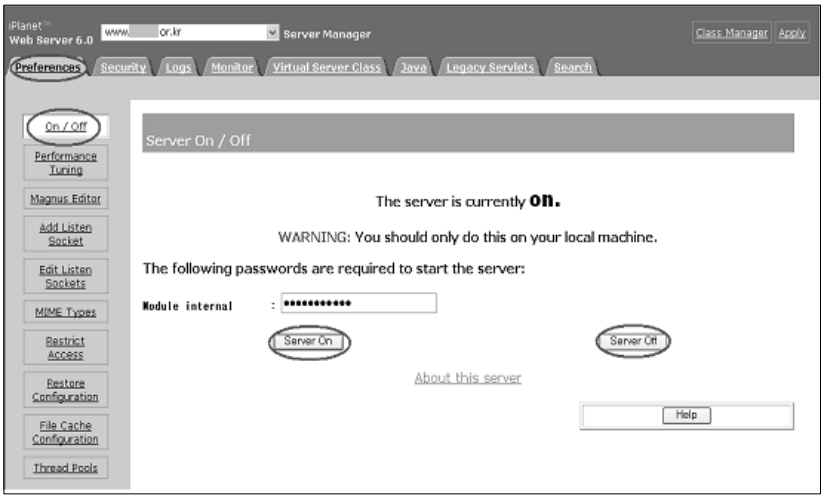
나. 인증서 설치 방법

① Server Certificate를 iPlanet 웹 서버에 설치

관리자 화면에서 Security → Install a Certificate를 선택한 후, 아래 화면에서 표시된 부분의 정보를 채워 넣습니다.

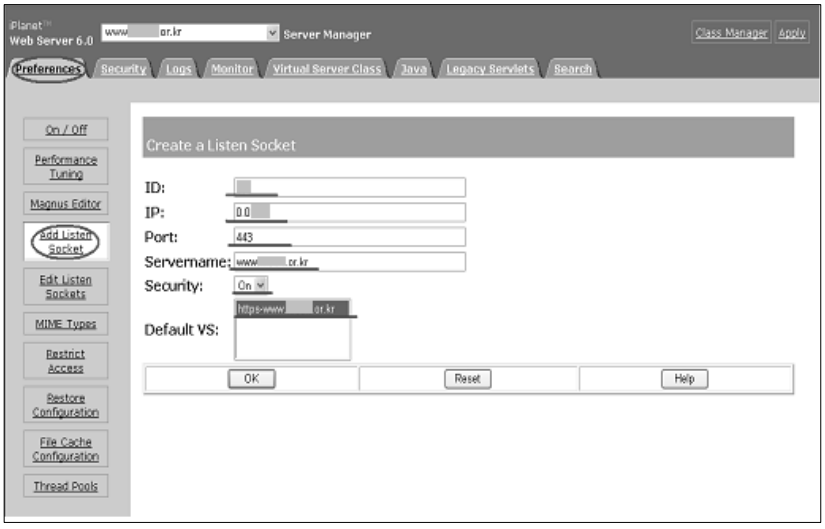


② iPlanet 웹 서버를 재시작 (Server Off → Server On)



③ iPlanet 웹 서버 설정 변경

iPlanet서버에 인증서를 설치가 완료됐다면, 서버에서 443 포트에 대하여 대기(Listen)할 수 있도록 설정을 변경해야 합니다. 웹서버 관리자 화면에서 Preference → Add Listen Socket을 선택하여 아래와 같이 정보를 입력한 후 'OK' 를 선택합니다.

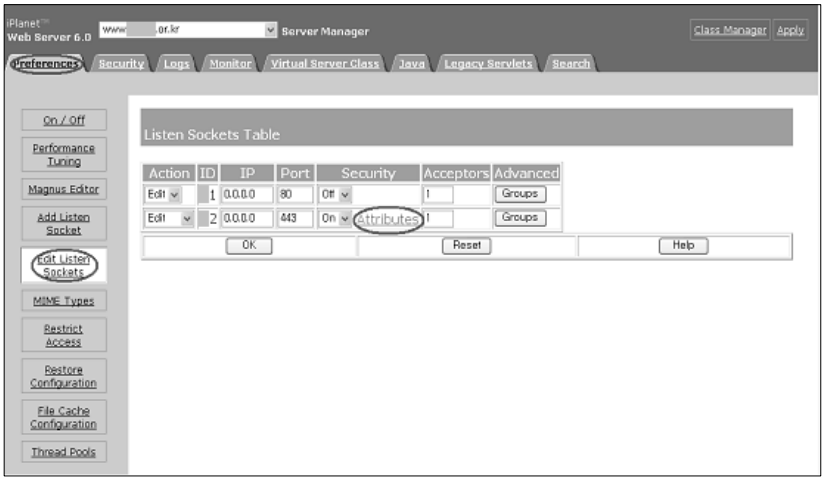


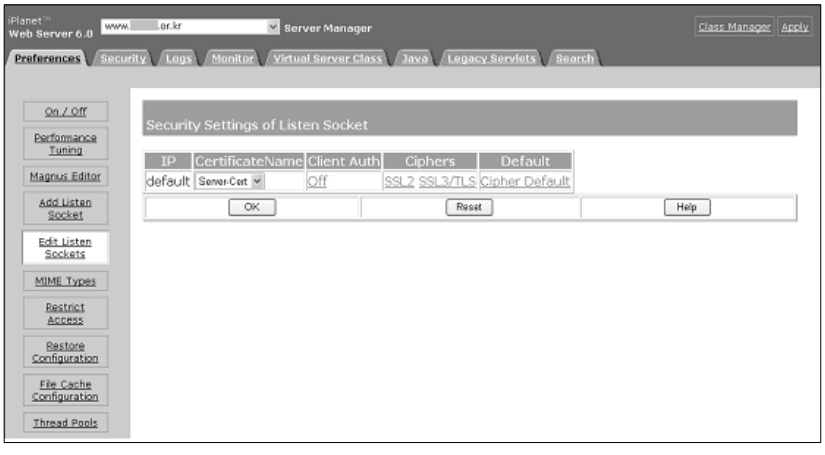
입력해야 할 정보는 다음과 같습니다. (그림의 밑줄 참고)

- ID : 이전 80포트에 대한 ID를 참고하여 SSL 포트를 위한 ID를 부여
- IP : 0.0.0.0 / any 로 설정
- Port : 443, SSL 포트는 443이 디폴트 포트이며, 서버 관리자와 상의하여 다른 포트를 사용하도록 설정 변경도 가능
- Servername : 웹서버명
- Security : 'On' 선택
- Default VS : 디폴트로 사용할 Virtual Server url을 입력

④ iPlanet 웹 서버 설정 추가변경

SSL에 대한 443 Listen 기능을 입력한 후, 추가로 설정해야 할 부분이 있다면 동일 화면에서 'Edit Listen Sockets'를 선택한 후 'Attributes' 링크를 클릭하여 수정합니다. 이 화면에서 SSL2, SSL3/TLS에 대한 설정을 변경하거나 iPlanet 기본 설정값으로 리셋할 수 있습니다.





⑤ 이제 SSL 인증서의 설치가 완료되었습니다. Ⅵ장으로 이동하셔서 실제 웹페이지를 어떻게 수정해야 하는지 알아보겠습니다.

2.5 체인 인증서 및 루트 인증서 설정하기

가. 인증서 종류 및 설치 이유

체인 인증서와 루트 인증서는 국산인증서와 신뢰형성을 구축하기 위하여 설정하는 부분입니다. 체인 인증서와 루트 인증서는 업체에서 보안서버 인증서 발급 시 함께 받을 수 있습니다.

〈그림 3-4〉 브라우저 경고창 발생 예시

Windows XP SP2 미만 버전을 사용하는 사용자는 MS에서 업데이트를 제공하고 있지 않기 때문에 국산인증서의 경우 신뢰되지 않는 인증기관에서 발급받은 인증서로 인식하여 브라우저에 〈그림3-4〉와 같은 경고창이 발생하게 됩니다.

서버에서 체인 인증서와 루트 인증서를 설정하게 되면 Windows XP SP2 미만 익스플로러(IE) 6.0 또는 7.0버전을 사용하는 사용자도 국산인증서를 신뢰된 인증서로 인식하게 되어 브라우저에 경고창이 발생하는 불편을 제거 할 수 있으므로 반드시 설정하시기를 권장하는 바입니다.

※ 익스플로러(IE) 이외 일부 웹 브라우저 및 운영환경에 따라 경고창이 발생할 수 있습니다.

〈그림 3-5〉 인증서의 인증경로

① 루트 인증서	② 체인 인증서	③ SSL 인증서
인증서 체인의 맨 위에 있는 신뢰된 최상위 인증서	인증서 발급기관이 서명한 일련의 계층적 인증서	웹서버의 CSR값을 기반으로 생성된 인증서

단, 모든 국산인증서가 경고창이 발생하는 것은 아닙니다. 국산인증서는 2006년 2월에 인터넷 익스플로러(IE) 브라우저의 신뢰된 루트 인증기관으로 등록되었으며 Windows XP SP2 버전 이상부터는 국산인증서가 신뢰된 기관에서 발급받은 인증서로 인식되기 때문에 경고창이 발생하지 않습니다.

웹 서버의 종류에 따라 키 체인 인증서와 루트 인증서를 설정하는 방법이 모두 다르므로 본 가이드에서는 가장 대표적인 웹 서버인 Apache 서버, IIS 서버, 톰캣(Tomcat) 서버에서 체인 인증서 설정방법을 설명하겠습니다. 이 외 서버의 경우는 보안서버 구축 전문 업체에서 제공하는 설치방법 및 온라인 지원을 이용하시기 바랍니다.

나. Apache 서버의 체인 및 루트 인증서 설정방법

Apache 서버에서는 인증서 설치 후 httpd.conf (또는 ssl.conf) 파일을 수정하여 체인 인증서를 설정합니다.

국산 보안서버 인증서인 경우 체인 인증서 및 루트 인증서를 설정 하여야 합니다. 다음과 같이 설정하시면 됩니다.

```
# 보안 서버 인증서 설정
SSLCertificateFile /usr/local/apache2/cert/test.kisa.or.kr_cert.pem
# 보안서버 인증서 개인키 설정
SSLCertificateKeyFile /usr/local/apache2/cert/test.kisa.or.kr_key.pem
# 체인 인증서 설정
SSLCertificateChainFile /usr/local/apache2/cert/chan_Cert.pem.cer
# 최상위 인증기관(루트 인증서) 인증서 설정
SSLCACertificateFile /usr/local/apache2/cert/KISA_ROOTCA_3.cer
```

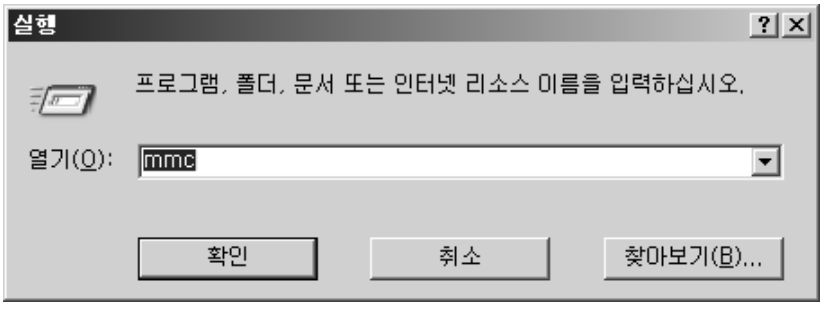
```
<VirtualHost 111.111.111.111:443>
ServerAdmin webmaster@test.net
DocumentRoot "/usr/local/apache2/htdocs"
ServerName test.kisa.or.kr:443
ErrorLog logs/ssl_error_log
#TransferLog /usr/local/httpd2/logs/access_log

SSLEngine on
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

#보안서버 인증서 파일 설정
SSLCertificateFile /usr/local/apache2/cert/test.kisa.or.kr_cert.pem
#보안서버 인증서 개인키 설정
SSLCertificateKeyFile /usr/local/apache2/cert/test.kisa.or.kr_key.pem
#체인 인증서 설정
SSLCertificateChainFile /usr/local/apache2/cert/ chain_Cert.pem.cer
#루트인증서(최상위 인증기관 인증서) 설정
SSLCACertificateFile /usr/local/apache2/cert/KISA_ROOTCA_3.cer
```

※ 체인 인증서의 파일명은 발급기관에 따라 위 내용과 다를 수 있습니다.

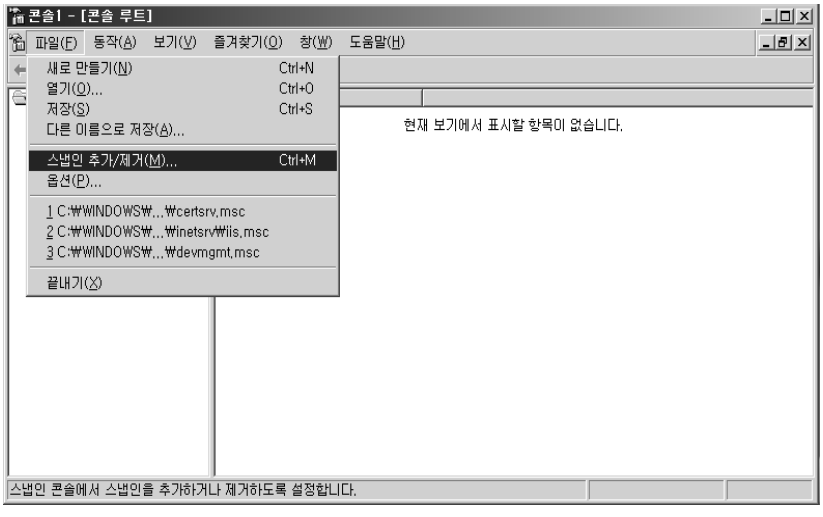
다. IIS 서버에서 체인 및 루트 인증서 설정방법

(1) 윈도우 관리자 콘솔(mmc)을 이용한 인증서 스냅인 추가

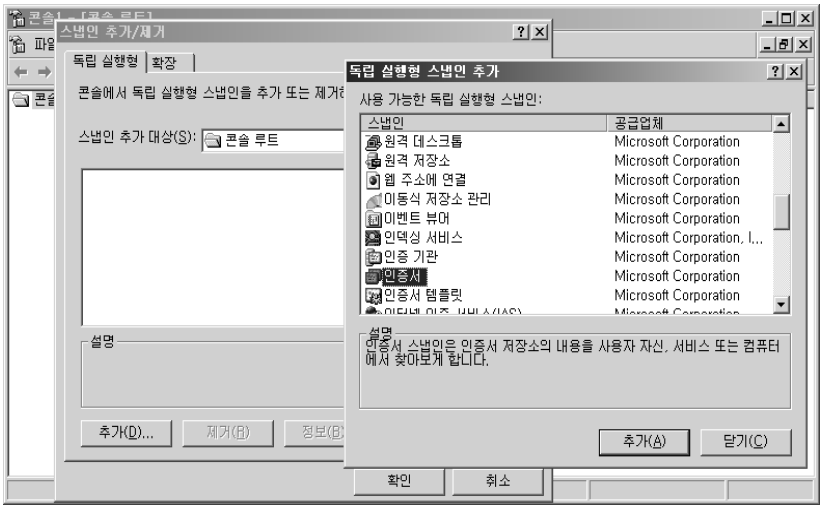
① 웹 서버에 설치된 인증서를 관리하기 위하여 인증서 스냅인을 추가하기 위해 윈도우 실행 창에서 다음과 같이 명령어를 입력합니다.



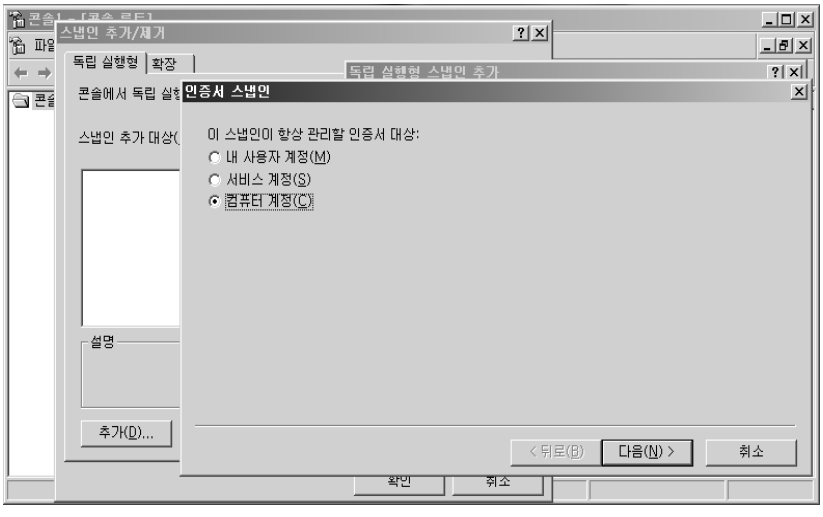
② 콘솔 창이 열리면 파일→ 스냅인 추가/제거를 클릭합니다.



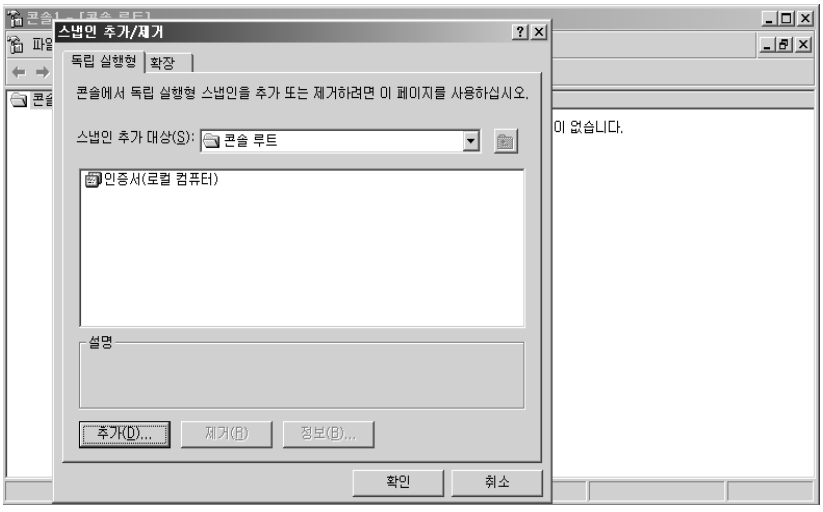
③ 추가할 스냅인의 목록 중 인증서 항목을 선택합니다.



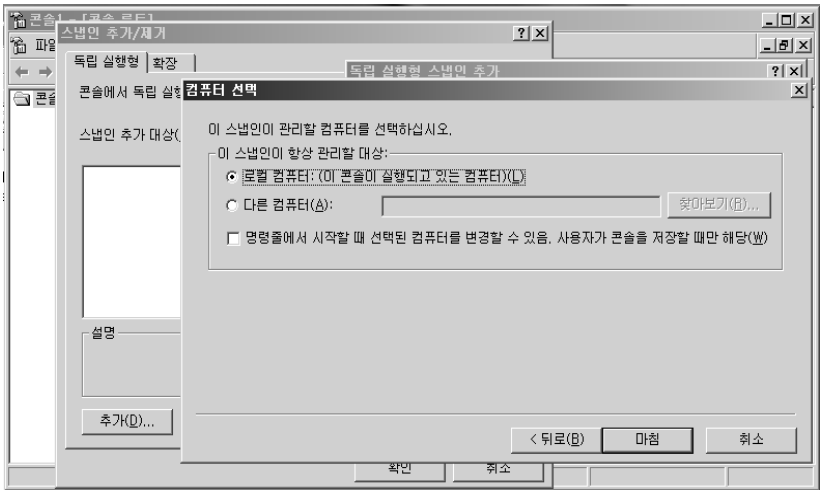
④ 관리할 인증서 대상을 선택하는 창이 열립니다. 실제 웹 서버가 실행되고 있는 컴퓨터 계정에 대한 관리를 선택합니다.



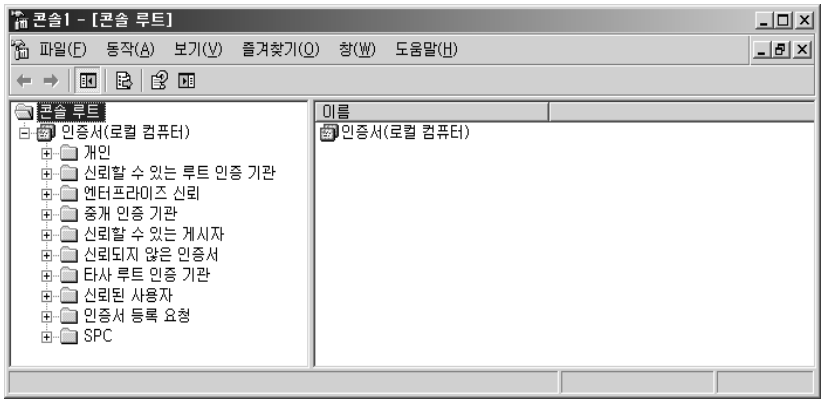
⑤ 스냅인이 추가 되어있는 것을 확인 할 수 있습니다.



⑥ 스냅인이 관리할 컴퓨터를 선택하는 창이 열어 실제 실행되고 있는 로컬 컴퓨터를 선택합니다.

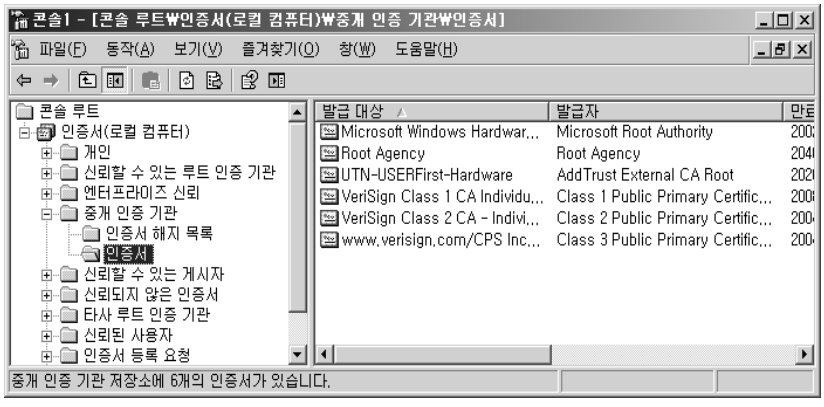


⑦ 위 과정으로 인증서 스냅인 추가가 완료되었습니다.

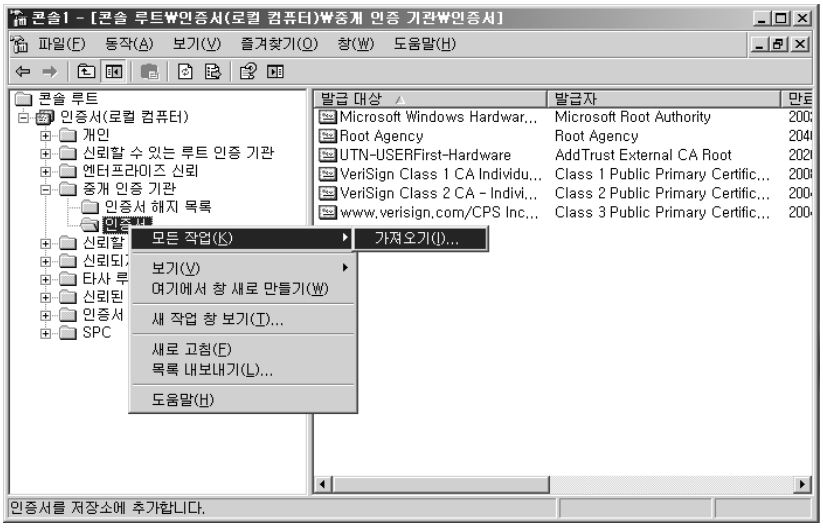


(2) 체인 인증서 설치하기

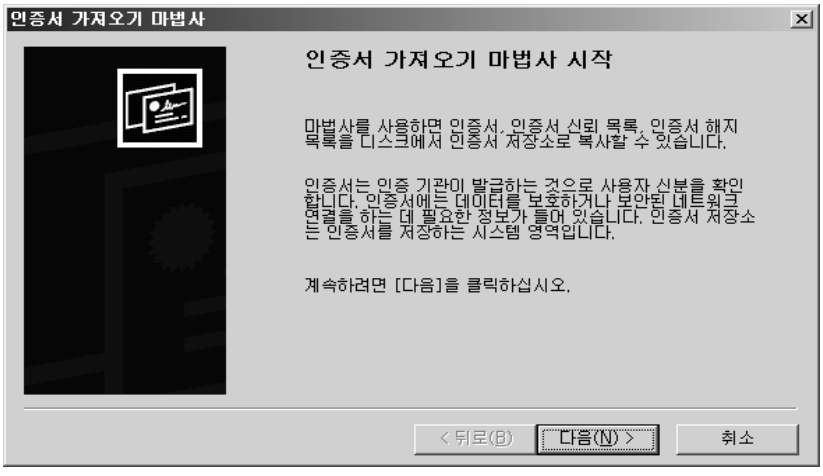
① 인증서 스냅인의 하위 목록 중 “중개 인증기관” 항목을 확장하면 다음과 같이 인증서 해지 목록과 인증서 목록이 있습니다.



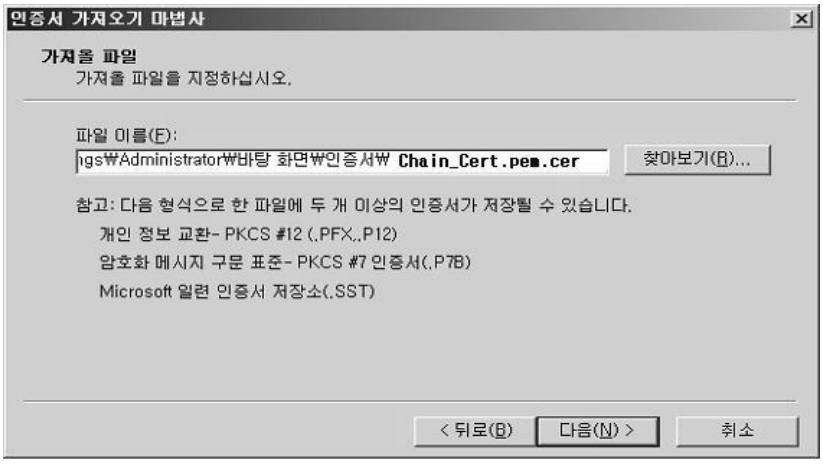
② 인증서 항목에서 오른쪽 마우스 버튼을 클릭하시면 '모든 작업 → 가져오기' 항목을 선택할 수 있습니다.



③ 가져오기를 실행하면 인증서 가져오기 마법사가 시작됩니다.

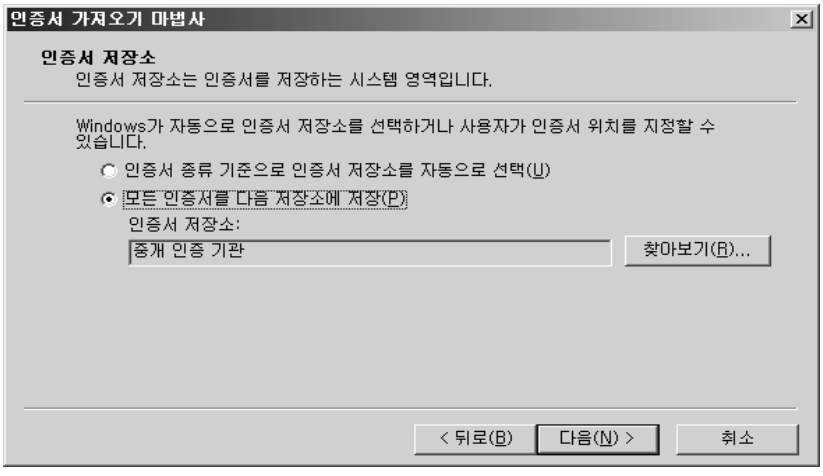


④ 가져올 파일을 선택하는 창에서 체인 인증서의 위치를 선택한 후 다음 버튼을 클릭합니다.

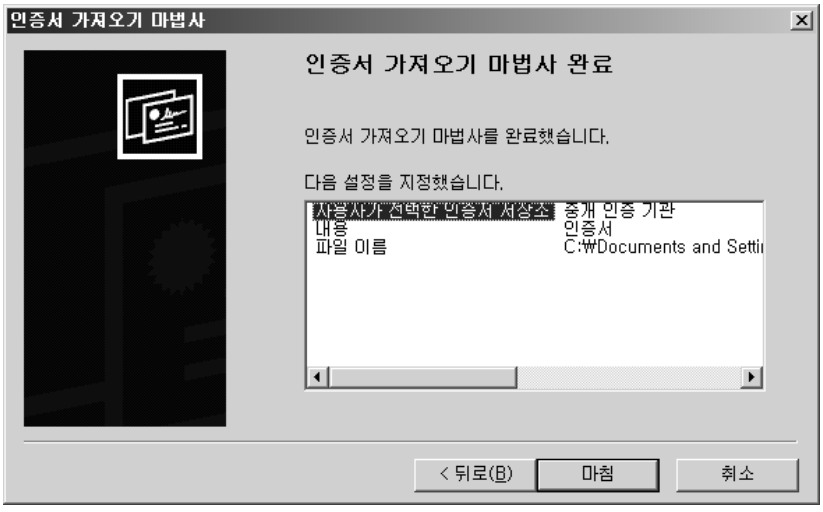


※ 체인 인증서의 파일명은 발급기관에 따라 위 내용과 다를 수 있습니다.

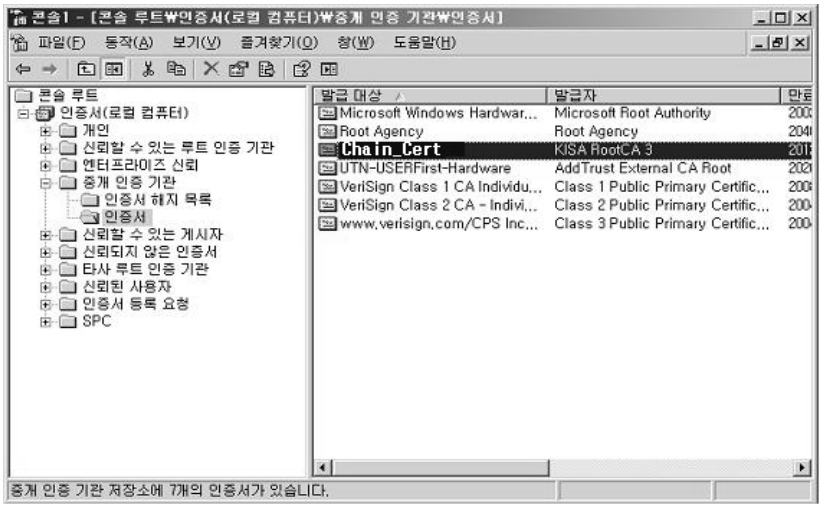
⑤ 체인 인증서를 웹 서버의 어느 위치에 저장할지 선택합니다. 인증서의 저장 위치가 "중개 인증기관" 인지 확인합니다.



⑥ 인증서 가져오기 마법사가 완료되었습니다.



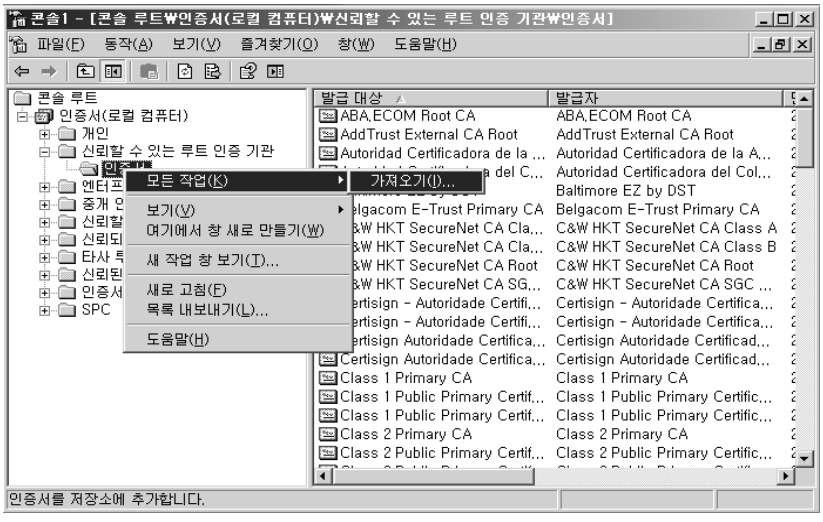
⑦ 다음 그림과 같이 “중개 인증기관”의 인증서 목록에 체인 인증서가 설치 된 것을 확인할 수 있습니다.



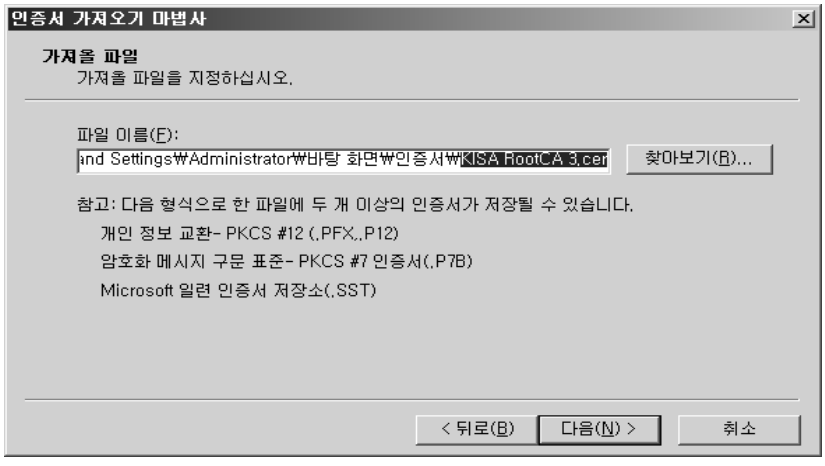
(3) 루트 인증서 설치하기

루트 인증서 설치는 체인 인증서 설치와 동일합니다.

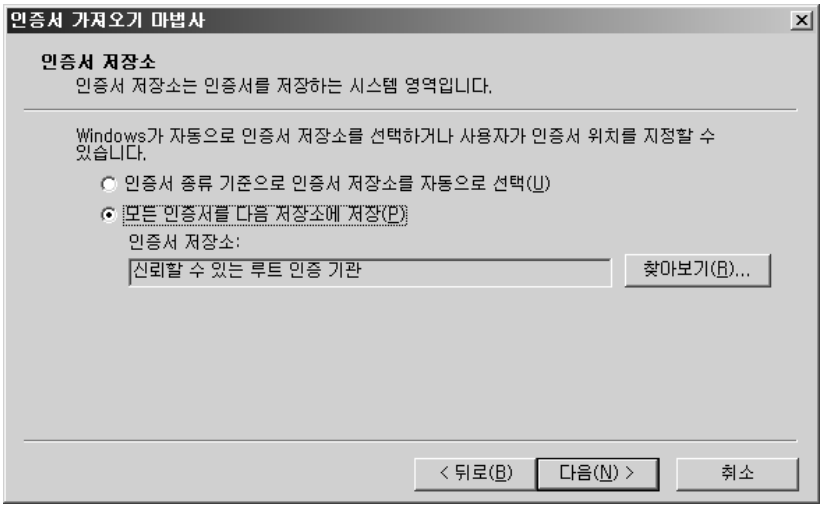
① 인증서를 인증서 스냅인의 목록 중 “신뢰할 수 있는 루트 인증기관”항목의 인증서 항목에서 오른쪽 마우스 버튼을 클릭하면 ‘모든 작업→가져오기’를 실행 할 수 있습니다.



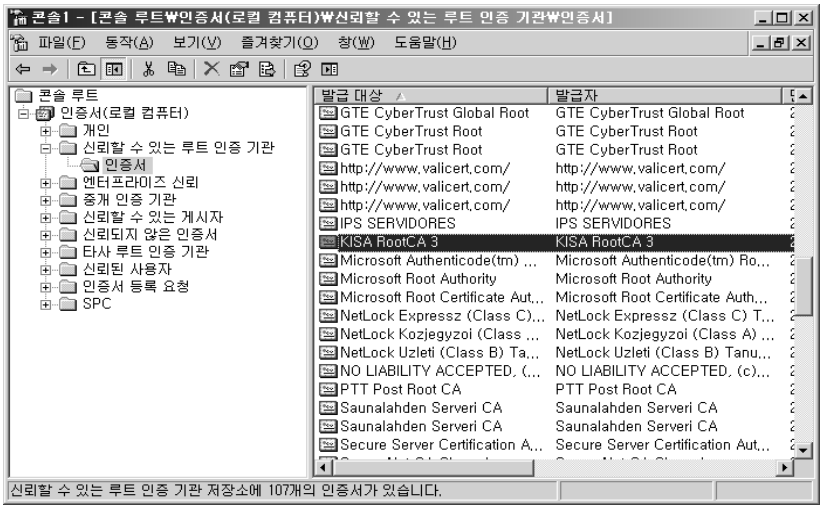
② 가져올 루트 인증서를 선택합니다.



③ 인증서가 저장될 위치가 “신뢰할 수 있는 루트 인증기관”인지를 확인합니다.



④ 루트 인증서 가져오기 마법사가 완료되고 다음 그림과 같이 “신뢰할 수 있는 루트 인증기관”의 인증서 목록에 루트 인증서가 추가된 것을 볼 수 있습니다.



라. 톰캣(Tomcat) 서버에서 체인 및 루트 인증서 설정방법

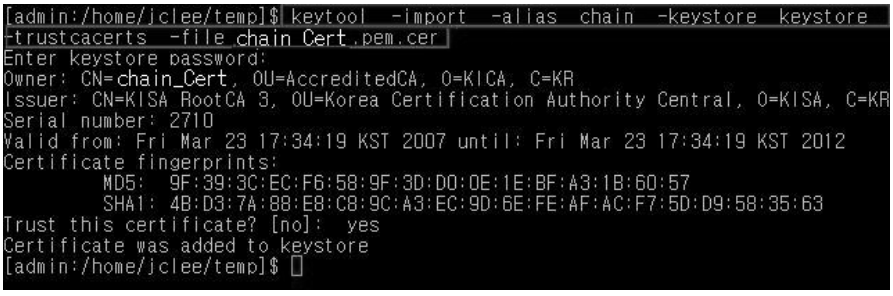
① 체인 인증서 설치

체인 인증서를 keystore에 import 합니다.

keytool의 사용 옵션은 다음과 같습니다.

```
keytool –import –alias 〈별칭 명〉 –keystore 〈keystroe 파일명〉 –trustcacerts
–file 〈체인 인증서 파일〉
```

EX) keytool –import –alias chain –keystore keystore –trustcacerts –file chain_Cert.pem.cer



※ 체인 인증서의 파일명은 발급기관에 따라 위 내용과 다를 수 있습니다.

② 루트 인증서 설치

루트 인증서를 keystore에 저장합니다.

```
keytool –import –alias 〈별칭 명〉 –keystore 〈keystroe 파일명〉 –trustcacerts
–file 〈루트 인증서 파일〉
```

keytool –import –alias root –keystore keystore –trustcacerts –file KISA_ROOTCA_3.cer

```
[admin:/home/jclee/temp]$ keytool -import -alias root -keystore keystore
-trustcacerts -file KISA_RootCA_3.cer
Enter keystore password:  ehfthl2231
Owner: CN=KISA RootCA 3, OU=Korea Certification Authority Central, O=KISA, C=K
R
Issuer: CN=KISA RootCA 3, OU=Korea Certification Authority Central, O=KISA, C=
KR
Serial number: 2
Valid from: Fri Nov 19 15:39:51 KST 2004 until: Wed Nov 19 15:39:51 KST 2014
Certificate fingerprints:
         MD5:  93:EB:36:13:0B:C1:54:F1:3E:75:05:E5:E0:1C:D4:37
         SHA1: 5F:4E:1F:CF:31:B7:91:3B:85:0B:54:F6:E5:FF:50:1A:2B:6F:C6:CF
Trust this certificate? [no]:  yes
Certificate was added to keystore
[admin:/home/jclee/temp]$
```

※자바 버전에 따라 위 메시지와 다른 메시지가 출력될 수 있습니다.

③ 설치 확인

다음과 같은 명령어로 keystore에 체인과 루트 인증서가 정상적으로 설치되었는지 확인 할 수 있습니다.

```
keytool –list –keystore ./keystore
```

```
[admin:/home/jclee/temp]$ keytool -list -keystore ./keystore
Enter keystore password:  ehfthl2231

Keystore type: jks
Keystore provider: SUN

Your keystore contains 3 entries

root, Jun 11, 2008, trustedCertEntry,
Certificate fingerprint (MD5): 93:EB:36:13:0B:C1:54:F1:3E:75:05:E5:E0:
1C:D4:37
chain, Jun 11, 2008, trustedCertEntry,
Certificate fingerprint (MD5): 9F:39:3C:EC:F6:58:9F:3D:D0:0E:1E:BF:A3:
1B:60:57
tomcat, Jun 11, 2008, keyEntry,
Certificate fingerprint (MD5): 12:A8:CA:29:1E:83:67:B4:2F:69:63:61:7F:
9D:A2:24
[admin:/home/jclee/temp]$
```

3. 기타 SSL 인증서 소개

3.1 멀티도메인 SSL 인증서

가. 인증서 목적 및 소개

지금까지의 SSL 인증서는 하나의 도메인에 대해서만 인증을 해주고 있기 때문에, 한 대의 서버에서 한 개의 인증서만을 사용하는 것이 일반적이었습니다.

웹 서버 암호화 통신을 위해서 https가 응답하게 되는 기본적인 443 포트를 하나의 도메인만이 소유하고 사용할 수가 있기 때문에, 하나의 서버에 여러 개의 도메인이 존재하고 모든 도메인이 https를 사용하고자 하면, 아래의 두 가지 방법을 사용하였습니다.

첫 번째는 한 대의 서버에 도메인 개수만큼의 각기 다른 IP를 부여하는 것입니다. 즉, 한 대의 서버에서 운영이 되지만 하나의 도메인에 하나의 IP를 할당하는 것으로 도메인이 10개가 있다면, IP 역시 10개가 필요한 방식입니다. 이 방식은 홈페이지가 운영되는 서버의 대수를 줄일 수는 있지만, IP 고갈을 이유로 잘 사용되지 않습니다.

나머지 한 가지는 가장 많이 사용하는 방식으로 기본 https 포트인 443이 아닌, 다른 포트를 사용해야 하는 것입니다.

예를 들면, https://domain.co.kr이 아닌, https://domain.co.kr:444 등으로 특정 포트를 직접 지정하여 접속을 해야 하는 불편함이 존재합니다. 즉, 기존에는 IP 고갈이나 다른 포트로 접속 등으로 인해서 웹호스팅 서버 또는 한 대의 서버에서 여러 개의 도메인을 사용하는 서버에서는 https를 사용하는데 불편함이 있었습니다.

멀티도메인 SSL 인증서는 기존의 단일 도메인 인증으로 인한 불편함을 없애고, 웹호스팅 서버나 한대의 서버에서 여러 개의 도메인을 운영하는 서버들에게 IP의 추가나 443이

아닌 다른 포트를 사용하지 않고 웹 서버 암호화 통신을 위해서 동일한 443 포트를 공유해서 사용할 수 있도록 편리함을 제공할 수 있는 인증서입니다.

멀티도메인 SSL 인증서는 1년 동안의 인증기간을 갖는데, 그 인증기간 안에는 언제든지 최대 100개까지의 도메인을 추가할 수 있고, 또한 제거할 수도 있습니다. 기본적으로 도메인을 추가할 때는 도메인 하나당 추가 비용이 따로 청구되고 삭제 때는 청구가 되지 않지만, 실수로 삭제한 경우 다시 추가를 하려면 다시 비용을 내야 하므로 삭제시에는 주의해야 합니다.

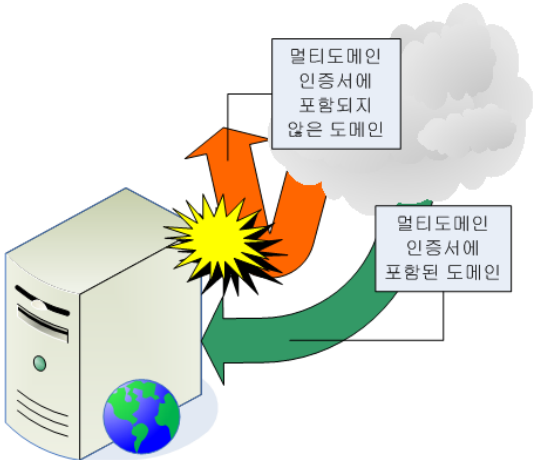
나. 멀티도메인 SSL 인증서 구동 방식

멀티도메인 SSL 인증서는 인증서가 필요한 다수의 도메인을 한 대의 서버에서 운영해야 하는 경우 유용한 인증서 서비스입니다. 인증서가 필요한 다수의 도메인을 운영하고 있는 웹호스팅 서비스 제공 서버나 여러 도메인을 운영하는 서버의 여러 문제를 해결할 수 있는 방법이 될 수 있습니다.

멀티도메인 SSL 인증서가 여러 개의 도메인을 인식할 수 있는 방법은 CN(Common Name)[2] 변수를 도메인 수만큼 여러 개 생성하여 인증서에 포함시켜 두고, 클라이언트가 암호화된 통신으로 웹 서버에 접속했을 때 웹 서버는 암호화 통신된 내용을 복호화하여, 클라이언트에서 요청한 도메인이 자신의 인증서에 있는 CN과 일치하는지 확인한 뒤 일치하면 보안 통신을 허가하는 방식으로 구동을 하게 됩니다.

이런 방법은 단일 도메인 인증서에서도 마찬가지로, 멀티도메인 인증서는 단지 인증서 안에 여러 개의 CN을 포함하고 있다는 것 외에는 방식이나 기술의 차이는 없습니다.

2) 인증서를 설치한 도메인의 이름



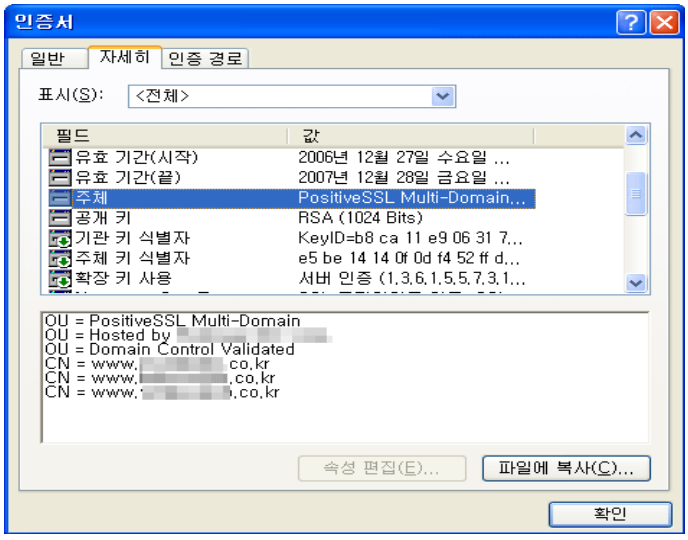
〈그림 3-6〉 멀티도메인 SSL 인증서의 CN이 있는 도메인과 없는 도메인의 동작

〈그림 3-7〉는 멀티도메인 SSL로 보호된 웹사이트 방문시에도 단일 도메인 SSL 방식으로 보호된 웹사이트와 마찬가지로 자물쇠 모양으로 현재 보안통신이 이루어지고 있음을 보여주고 있습니다.

〈그림 3-7〉 암호화 통신이 이루어지고 있음을 보여주는 자물쇠 이미지

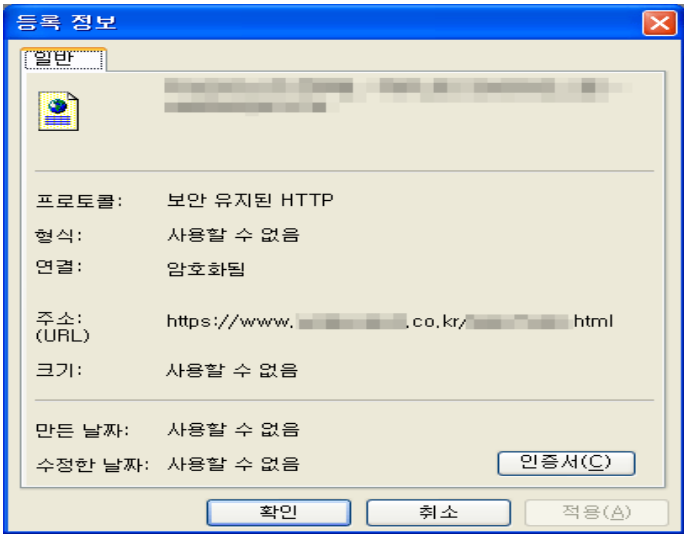
자물쇠 모양을 더블클릭하여 인증서를 자세히 보도록 하겠습니다.

인증서의 속성을 확인해보면 다수의 CN이 존재하는 것을 확인할 수 있습니다. 이 CN 변수에 값으로 설정된 도메인에 대해서만 암호화 통신이 가능합니다.



〈그림 3-8〉 다수의 CN이 포함된 멀티도메인 SSL 인증서

이미 단일 SSL이 적용된 웹페이지 속성에서 확인하였듯이 웹페이지의 속성을 확인하면 보안이 유지된 상태로 통신이 이루어지고 있음을 확인할 수 있습니다.



〈그림 3-9〉 보안이 적용된 웹페이지 속성 확인

다. Apache 서버의 멀티도메인 SSL 인증서 설정방법

멀티도메인 SSL 인증서를 적용하기 위해서는 기존에 이미 설정되어 있던 평문 통신을 위한 http(80)의 가상호스팅 설정을 변경해야 합니다.

만일 평문 통신의 가상호스팅 설정을 변경하지 않으면, 보안통신을 위해서 https를 호출했지만 https가 응답을 하지 않고 일반 평문을 위한 http 프로토콜이 응답을 하는 등 에러가 발생할 수 있기 때문에, 평문은 http(80)에서, 암호화된 통신은 https(443)에서 호출하라고 확실히 구분을 해주어야 합니다. 아래의 〈그림 3-10〉과 〈그림 3-11〉이 Apache 서버의 설정파일(httpd.conf)에서 각각 평문 통신과 암호화 통신으로 구분한 설정 예입니다.

```
NameVirtualHost [redacted]:80

<VirtualHost [redacted].com:80>
        ServerAdmin webmaster@[redacted].com
        DocumentRoot /home/[redacted]/public_html
        ServerName [redacted].com
        ScriptAlias /cgi-bin/ "/home/[redacted]/cgi-bin/"
        ServerAlias [redacted].com www.[redacted].com
        ErrorLog /var/log/[redacted].com-error_log
        CustomLog /var/log/[redacted].com-access_log common
</VirtualHost>

<VirtualHost [redacted].co.kr:80>
        ServerAdmin webmaster@[redacted]com
        DocumentRoot /home/[redacted]/public_html
        ServerName [redacted].co.kr
        ScriptAlias /cgi-bin/ "/home/[redacted]/cgi-bin/"
        ServerAlias [redacted].co.kr www.[redacted].co.kr
        ErrorLog /var/log/[redacted].co.kr-error_log
        CustomLog /var/log/[redacted].co.kr-access_log common
</VirtualHost>
```

〈그림 3-10〉 Apache 서버에서 평문 통신을 위한 가상호스팅 설정

```
NameVirtualHost [redacted]:443

<VirtualHost www.[redacted].co.kr:443>
DocumentRoot "/home/[redacted]/public_html"
ServerName www.[redacted].co.kr
ServerAlias www.[redacted].com
ScriptAlias /cgi-bin/ "/home/[redacted]/cgi-bin/"
ServerAdmin webmaster@[redacted]
ErrorLog /usr/local/apache/logs/error_log
TransferLog /usr/local/apache/logs/access_log

SSLEngine on
SSLCipherSuite [redacted]
SSLCertificateFile /usr/local/apache/conf/ssl.crt/[redacted]
SSLCertificateKeyFile /usr/local/apache/conf/ssl.key/[redacted].key

<Files ~ "\.(cgi|shtml|phtml|php3?)$">
    SSLOptions +StdEnvVars
</Files>
<Directory "/usr/local/apache/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>
SetEnvIf User-Agent ".*MSIE.*" \
         nokeepalive ssl-unclean-shutdown \
         downgrade-1.0 force-response-1.0
SetEnvIf User-Agent "LWP::" get_lost
SetEnvIf User-Agent "lwp-trivial" get_lost
CustomLog /usr/local/apache/logs/ssl_request_log \
          "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
```

〈그림 3-11〉 Apache 서버에서 암호화 통신을 위한 가상호스팅 설정

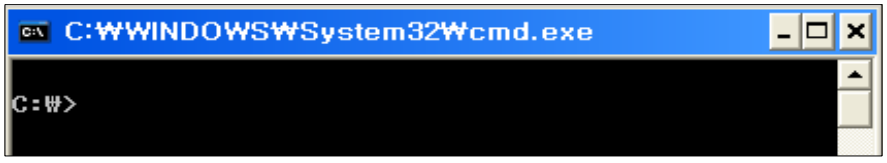
라. IIS 서버의 멀티도메인 SSL 인증서 설정방법

(1) IIS 서버 6.0 이상

IIS에서 멀티도메인 SSL 인증서를 사용하는 방법은 Apache 서버보다 좀 더 까다롭습니다. IIS에서는 동일한 443 포트를 여러 도메인이 쓰고자 한다면, IIS의 80 포트에 대한 가상호스팅 설정을 하는 것이 아니라 SecureBindings라는 작업을 거쳐야 합니다.

SecureBindings는 443 포트를 여러 도메인이 쓸 수 있도록 설정해 주는 것을 뜻하며, 다음과 같은 절차를 통해서 설정합니다.

① 시작 → 실행 → 'cmd '(명령프롬프트) 명령 입력
명령이 정상적으로 수행이 되었다면, 그림과 같이 명령 프롬프트 창이 뜹니다.



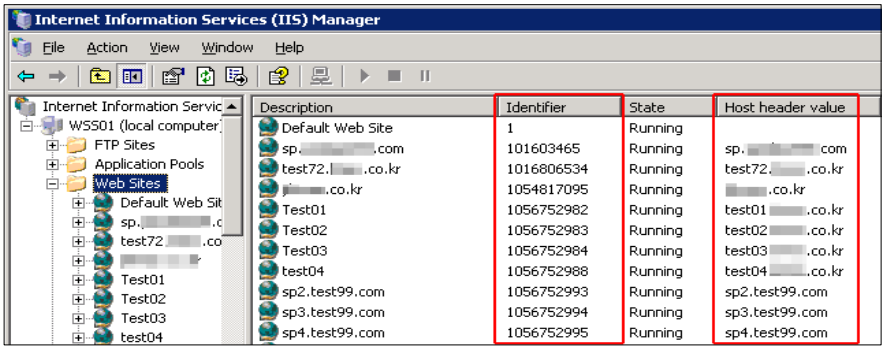
〈그림 3-12〉 CMD command 실행 모습

② 다음 명령창에 SSL 호스트 헤더에 대한 SecureBindings의 메타베이스 속성을 설정하기 위해서 아래와 같은 형식의 명령을 입력합니다.

```
cscript.exe adsutil.vbs set /w3svc/〈site identifier〉/SecureBindings ":443:〈host header〉"
```

* 〈site identifier〉는 도메인의 식별자 번호
* 〈host header〉는 웹사이트의 호스트 헤더
* 〈그림 3-13〉 참고

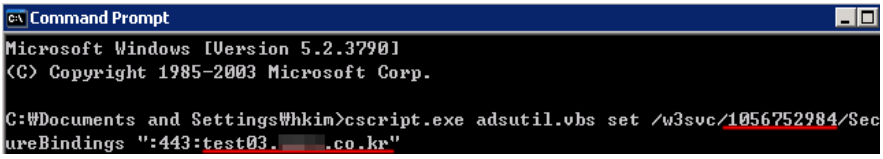
③ 〈그림 3-13〉의 화면을 보기 위해서는 '시작 → 프로그램 → 관리도구 → Internet Information Service (IIS) 관리자' 를 수행



〈그림 3-13〉 IIS 관리자에서 Site Identifier와 Host header 값 확인

그림에서 첫 번째 네모상자가 〈Site Identifier〉이고 두 번째 네모상자가 〈host header〉입니다. 〈Site Identifier〉는 시스템에 의해서 자동으로 부여되며, 〈host header〉는 SSL 인증서를 신청할 때 사용하는 도메인 주소입니다.

④ 아래 〈그림 3-14〉는 〈그림 3-13〉의 test03.xxx.co.kr이 443을 사용하기 위해서 SecureBindings 메타베이스를 속성을 설정하는 과정입니다.



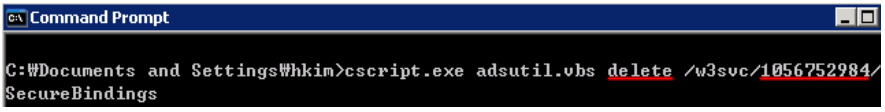
〈그림 3-14〉 SecureBindings 메타베이스 추가

〈그림 3-14〉를 정상적으로 수행하면, test03.xxx.co.kr이 443 포트에 binding 됩니다. 그 결과를 〈그림 3-15〉에서처럼 IIS 관리자에서 확인해보면, test04.xxx.co.kr과 test03.xxx.co.kr이 암호화 통신을 위해서 같은 443 포트를 사용하고 있음을 확인할 수 있습니다.

Description	Identifier	State	Host header value	IP address	Port	SSL Por
Default Web Site	1	Running		* All Unassigned *	80	
sp.[redacted].com	101603465	Running	sp.j[redacted].com	* All Unassigned *	80	
test72.[redacted].co.kr	1016806534	Running	test72.[redacted].co.kr	* All Unassigned *	80	
[redacted].co.kr	1054817095	Running	[redacted].co.kr	* All Unassigned *	80	
Test01	1056752982	Running	test01.[redacted].co.kr	* All Unassigned *	80	
Test02	1056752983	Running	test02.[redacted].co.kr	* All Unassigned *	80	
Test03	1056752984	Running	test03.[redacted].co.kr	* All Unassigned *	80	443
test04	1056752988	Running	test04.[redacted].co.kr	* All Unassigned *	80	443

〈그림 3-15〉 SecureBindings을 통한 443 포트 공유

만일 binding된 도메인을 지워야 할 경우에는 〈그림 3-16〉과 같이 delete 옵션을 이용하여 SecureBindings 메타베이스 속성에서 특정 사이트에 binding된 것을 해제(삭제)할 수 있습니다.



〈그림 3-16〉 SecureBindings 제거

(2) IIS 서버 5.0에서의 멀티도메인 SSL 인증서 제약 사항

IIS 5.0에서는 SecureBindings을 지원하고 있지 않기 때문에, 멀티도메인 SSL 인증서를 같은 443 포트에서 사용할 수가 없습니다.

다만, IIS 5.0은 기존의 단독 SSL 방법과 같이 포트를 다르게 하는 방법을 사용해서 멀티도메인 SSL 인증서를 사용할 수 있습니다.

마. 멀티도메인 SSL 인증서의 문제점

지금까지 멀티도메인 SSL 인증서의 특징을 소개했는데, 다른 인증서들이 장단점을 가진 것과 마찬가지로 멀티도메인 SSL 인증서도 구조상 문제점을 가지고 있습니다.

① 모든 도메인 리스트 출력

같은 멀티도메인 SSL 인증서를 쓰는, 다시 말하면 한 대의 서버 내에서 운영되고 있는 https를 사용하는 모든 도메인이 노출될 수 있습니다.

② 동일한 만료기간

멀티도메인 SSL 인증서의 가장 큰 구조적 문제점이라고 볼 수 있는 것으로, 인증서 내에 포함되어 있는 각 도메인들의 SSL 서비스 만료 기간이 메인 인증서의 발급시기에 좌우된다는 것입니다.

다시 말하면, 멀티도메인 SSL 인증서의 최초 발급일자가 2007년 1월 1일 이라면, 1년이 되는 2008년 1월 1일에는 인증서에 속해있는 모든 도메인이 만료가 되어지는 것입니다.

예를 들어 최초 발급일자가 2007년 1월 1일인 멀티도메인 SSL 인증서에 2007년 1월에 포함된 도메인과 2007년 11월에 포함된 도메인이 모두 만료 일자가 2008년 1월 1일이라는 것입니다.

도메인마다 단독 SSL 인증서를 사용하면 각각 1년의 서비스 기간이 보증되는데 반해서 (계약에 따라서 더 길수도 있다), 멀티도메인 SSL 인증서의 경우에는 일정 비용을 지불하지만, 1년이라는 서비스 기간을 보장받지 못할 수 있습니다.

③ 인증서 비용 문제

앞서 설명했듯이 도메인을 추가할 때마다 일정 비용을 지불해야 하고, 만료기간이 되어 멀티도메인 SSL 인증서를 갱신하고자 할 때에는 현재 멀티도메인 SSL 인증서에 포함되어 있는 모든 도메인에 대해서 각각 일정 비용을 지불해야 하므로, 늦게(만료일에 가깝게) 추가한 도메인에 대해서는 인증유지를 위해서 짧은 기간에 두 번의 비용을 지불해야 합니다.

3.2 와일드카드(Wildcard) SSL 인증서

와일드카드 인증서는 도메인은 같으나 호스트네임이나 서브 도메인이 다른 여러 페이지를 인증하고자 할 경우에 사용됩니다. 와일드카드 인증서를 이용하게 되면 서브 도메인과 같은 다양한 형태의 도메인에도 인증서를 적용하여 효과적으로 관리할 수 있습니다.

예를 들어 같은 2단계 도메인에 있는 서브도메인의 예는 다음과 같습니다.

www.kisa.com

mail.kisa.com

secure.kisa.com

login.kisa.com

와일드 카드는 다음과 같이 세 개 이상이 될 수도 있습니다.

..domain.com 이나 *.*.*.domain.com

위와 같이 같은 도메인을 사용하고 있는 경우 서브 도메인의 숫자에 관계없이 모두 사용할 수 있어 유연성을 제공하게 됩니다. 와일드카드 인증서 사용을 위해서는 먼저 구축된 환경 검토하시고 다른 인증서와 가격 및 여러 가지 요소를 비교, 검토 하신 뒤 선택하시어 사용하시기 바랍니다.

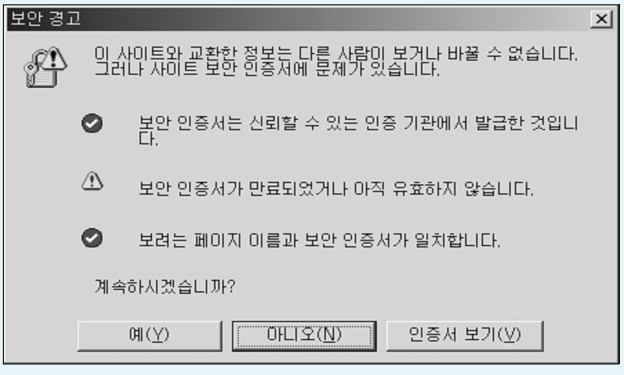
4. 오류 발생 시 대처방법

4.1 인증서 관련

① 인증서를 발급받은 사이트 주소와 실제로 접속한 사이트 주소가 다른 경우

예를 들어 www.kisa.or.kr로 인증서를 발급받아 설치한 후 실제 적용은 login.kisa.or.kr로 설정하여 인증서를 발급받은 주소와 실제로 접속한 주소가 다른 경우에 위와 같은 경고창이 나오게 됩니다.

② 인증서가 유효하지 않은 경우



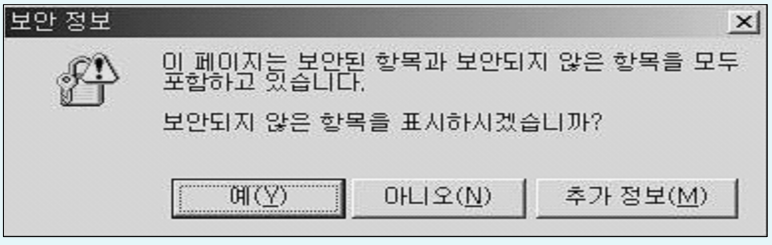
인증서의 유효기간이 지난 인증서를 계속 설치해 두는 경우에 나오는 경고창입니다. 그러나, 일반적으로 인증서가 설치된 사이트에 접속하는 PC의 날짜가 잘못되어 있어서 생기는 경우가 가장 많습니다.

③ 브라우저가 웹 서버 인증서를 신뢰할 수 없는 경우

이 경우는 웹 서버 인증서를 발급한 인증기관을 웹 브라우저가 인식하지 못하는 경우로써, 브라우저에는 기본적으로 신뢰할 수 있는 인증기관 리스트가 내장되어 있는데 그 리스트에 없는, 즉 신뢰할 수 없는 인증기관에서 발급된 인증서를 설치한 경우에 발생하는 경고창입니다. 실제로는, 웹 서버에서 자체적으로 만든 인증서를 설치한 경우에 가장 많이 생깁니다.

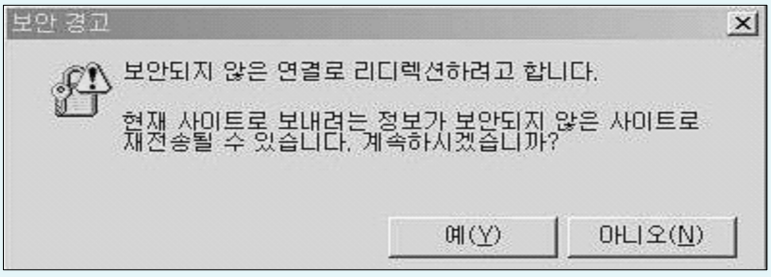
4.2 보안되지 않은 항목의 표시 · 연결 관련

① 보안된 항목 https와 보안되지 않은 항목 http를 모두 포함하는 경우



말 그대로 보안된 항목 https와 보안되지 않은 항목 http를 모두 포함하고 있어 나타나는 보안경고창입니다. https://를 이용해서 암호화 통신을 하고자 하는 페이지의 소스에 http://를 이용하여 호출하는 이미지 등이 존재할 때 보안경고창이 나타나는 것입니다.
이 경우 '아니오' 버튼을 눌러 표시되지 않는 http 항목의 소스를 절대경로를 써서 https로 호출하시면 됩니다.

② 한 페이지에 http://와 https://의 두 프로토콜이 존재하는 경우



한 페이지 안에 http://와 https://의 두 프로토콜이 존재하기 때문입니다. 예를 들어, http://www.kisa.or.kr에서 로그인을 위해 https://www.kisa.or.kr/login.jsp로 접속할 때 /login.jsp안에 http://www.kisa.or.kr로 호출하는 직접적인 소스가 있기 때문입니다.

이러한 경우 HTML 파일 중에 HTML 헤더 부분에 다음의 스크립트를 넣어주시면 됩니다.
META HTTP-EQUIV="REFRESH" CONTENT="0; URL=http://(해당 URL)"

이 스크립트는 https 페이지에서 로그인한 후, https로 암호화되는 임의의 페이지를 하나 만들어 이동을 하되 그 페이지에서 메타태그를 이용하여 원하는 http 페이지로 리프레쉬하게 만드는 것입니다.

보통의 CGI 프로그래밍에서의 리다이렉션 함수(메소드)나 또는 HTTP Location 헤더를 직접 가지고 보안되지 않은 곳으로 리다이렉션하면 보안되지 않은 곳으로 간다고 경고가 나오지만, HTTPS 서버의 HTML을 읽게 한 후 그 HTML 내에서 META 태그를 이용해서 리다이렉션하게 되면, 브라우저는 일단 그 HTML이 HTTPS 서버에서 읽은 것으로 간주하고 보안 경고가 뜨지 않으며 HTML의 META 태그로 리다이렉션하는 경우에는 브라우저가 리다이렉션한 것처럼 동작되게 되어 경고가 뜨지 않습니다.

③ https로 접속하면 페이지를 표시할 수 없다는 페이지가 보이는 경우

이 에러는 아래와 같은 이유로 발생합니다.
ⅰ. https 디렉토리에 파일이 존재하지 않을 경우
ⅱ. 서버나 end-user의 방화벽에서 443 포트가 차단되었을 경우
ⅲ. https 서버가 다운되었을 경우
ⅳ. SSL Certificate 파일이 정상적이지 않을 경우
ⅴ. 웹 브라우저에서 ssl 3.0으로 셋팅이 되어 있지 않을 경우

인증서가 정상적으로 설치되었는지를 확인하시고 서버에서 https를 위한 포트가 활성화 되었는지 확인하시기 바랍니다. 또한 방화벽과 L4 스위치 등 보안장비가 있다면 https를 위한 해당 포트를 모두 허용해 주어야 합니다. IIS 서버의 경우 'Netstat -na | findstr 포트번호', Apache 서버의 경우 'Netstat -na | grep 포트번호' 명령어를 이용하여 https를 위한 포트가 활성화되어 있는지 확인할 수 있습니다. 위의 모든 내용을 확인한 후에도 정상적으로 동작하지 않을 경우 해당 업체에게 문의하시기 바랍니다.

4.3 웹서버 기종 변경 관련

① 운영중인 웹 서버를 같은 기종으로 변경하려 하는 경우

개인키와 인증서를 백업하신 후 재설치하여 사용이 가능합니다. 서버 이전 또는 변경 전 설치 업체에게 반드시 사전 문의 후 작업을 진행하시기 바랍니다.

② 운영중인 웹 서버 종류를 다른 기종으로 변경하려 합니다.

개인키와 인증서를 백업하신 후 재설치하여 사용이 가능합니다. 다만 일부 웹 서버 종류는 인증서 및 개인키의 호환이 안되는 경우가 있으니 서버 이전 또는 변경 전 설치 업체에게 반드시 사전 문의 후 작업을 진행하시기 바랍니다.

4.4 CSR 생성 관련

① CSR 생성이 정상적으로 되지 않습니다.

CSR을 생성하실 경우 해당 정보는 모두 영문으로 작성하여 주셔야 하며 특수문자는 사용하시면 안 됩니다. 또한 입력을 요청하는 모든 내용을 입력하시고 다시 한 번 작업을 하시기 바랍니다.
위의 모든 내용을 확인한 후에도 정상적으로 동작하지 않을 경우 해당 업체에게 문의하시기 바랍니다.

② 인증서 기간이 만료되어 새로 발급받으려고 하는데 CSR 파일을 전에 사용하던 것으로 가능한가요?

보통 웹 서버에서 예전에 사용하던 CSR 파일의 사용이 가능합니다. 그러나 보안상의 이유로 추천하지 않습니다. 인증서를 갱신하실 때마다 새로이 CSR 파일을 생성하시는 것이 좋습니다. 또한 웹 서버 종류마다 반드시 CSR을 생성해야 하는 서버가 있으니 새로 발급받으시기 전에 전문 업체에게 문의하시기 바랍니다.

4.5 IP 관련

① 아직 도메인이 없는데 IP를 대상으로 인증서 발급이 가능합니까?

인증서는 고유의 식별자를 대상으로 발급됩니다. 즉 개인은 주민등록번호를 기준으로 발급되며 법인은 사업자등록번호로 발급되고, 서버는 도메인을 기준으로 발급되기 때문에 IP 또는 서버이름으로는 발급되지 않습니다. 따라서 도메인을 등록하시거나 서버의 호스트 이름으로 인증서를 신청하셔야 합니다. 단, 인트라넷 등 사설 IP를 통해 서비스를 운영하시는 경우 일부 인증서의 발급이 가능하니 전문 업체에 문의하시기 바랍니다.

② SSL 인증서를 발급받았는데 도메인의 IP를 변경해도 괜찮은가요?

인증서는 특정 IP로 제한하여 발급되지 않으며, www.kisa.or.kr처럼 도메인 이름으로 발급이 됩니다. 따라서 IP를 변경해도 무관합니다.

4.6 보안서버 구축 확인 관련

① 보안서버가 구축되었는지 확인을 어떻게 하나요?

일반적으로 보안서버가 구축되어 있으면 https://URL로 확인이 가능합니다. 하지만 https://URL을 통해서도 확인이 되지 않는 경우가 있으니 전문 업체에게 확인을 하시면 보다 정확하게 진단을 받으실 수 있습니다.

② 인증서를 설치하면 보안서버 구축이 완료되나요?

인증서를 설치하면 암호화통신을 위한 기초적인 작업이 완료됩니다. 하지만 실제로 암호화통신을 하기 위해서는 인증서 설치 후 웹페이지를 수정하여 https 프로토콜을 호출하는 작업이 필요합니다.

https를 호출하는 작업이 완료되어야만 보안서버가 완전하게 구축, 운영될 수 있습니다. 각 작업은 프로그램 소스를 변경하여 주는 작업이므로 'Ⅵ장 웹페이지 수정 및 적용 확인하기' 내용을 참고하여 웹사이트 운영자가 직접 수행하셔야 합니다.

4.7 기타

① 서브(Secondary) 도메인에 대해서도 보안서버를 적용하고 싶습니다. 어떤 방법이 있을까요?

일반적인 보안서버 인증서는 Host*Domain 단위로 발급됩니다. 예를 들어 www.kisa.or.kr와 login.kisa.or.kr에 보안서버를 구축하고자 한다면 각각의 인증서가 필요합니다. 동일 도메인 이름을 사용하는 여러 개의 Host에 대해서 보안서버를 구축하고자 한다면 그에 적합한 제품을 선택하여 보안서버를 구축하시기 바랍니다.

서브 디렉토리의 경우에는 별도의 인증서가 없어도 암호화가 가능합니다. 즉, www.kisa.or.kr 사이트에 보안서버가 구축되어 있다면 www.kisa.or.kr/login/이나 www.kisa.or.kr/member/ 등의 하위 디렉토리는 해당 소스코드의 수정만으로 보안서버 적용이 가능합니다.

② 한 도메인의 운영을 위해 다수의 서버를 사용하고 있거나 반대로 하나의 서버에 다수의 도메인을 운영하는 경우는 어떻게 하나요?

SSL 인증서는 도메인 단위로 발급되며, 하나의 도메인 운영을 위해 다수의 서버를 운영하는 경우에는 하나의 인증서를 구매하고 추가 서버대수 만큼의 라이센스를 받아야 하므로 사전에 확인하시기 바랍니다.
반대로 하나의 서버에 다수의 도메인을 운영하는 경우 각 도메인별로 SSL 인증서를 발급받으셔야 합니다.

③ 우리가 사용하고 있는 서버에 보안서버 설치가 가능한가요?

기본적으로 모든 웹 서버에는 인증서 방식의 보안서버가 설치 가능하지만 서버 환경에 따라서 별도의 작업이 필요할 수도 있습니다. 보안서버 신청 및 설치 전에 전문 업체에게 문의하신 후 작업을 진행하시기 바랍니다. 반드시 확인이 필요한 서버는 Apache, Tomcat 등이 있습니다.

5. 웹사이트 운영·관리상의 유의사항

5.1 인증서 유효성의 확보

앞에서도 언급하였다시피 SSL 인증서 설치의 오류에 따라 보안경고창이 발생하여 이용자들에게 '접속한 웹사이트 보안 인증서에 문제가 있음'을 경고하며, 웹사이트에 대한 신뢰도를 하락시키고 이용자들에게 심리적 부담감을 주게 됩니다. 따라서 보안서버 구축·관리 시 신뢰할 수 있는 인증기관, 발급 사이트 이름, 인증서 유효기간 등을 확인하여 보안서버 구축의 유효성을 유지하는 것이 매우 중요합니다.

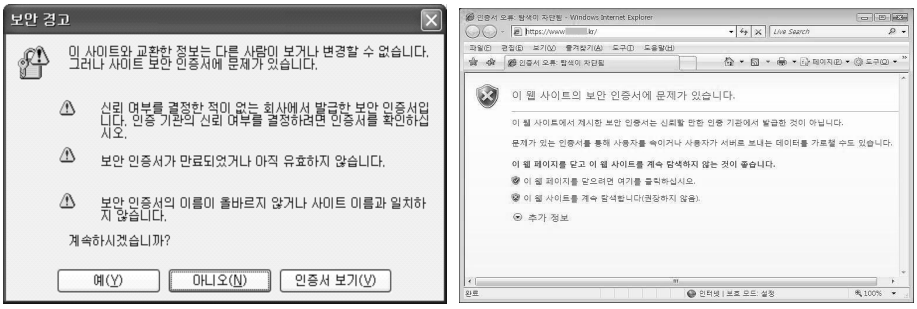
보안경고창이 발생하는 원인을 간략히 요약하면 다음과 같습니다.

① 인증서 발급기관의 신뢰성 여부
: 웹브라우저에 해당 인증서가 탑재되지 않아서 이를 발급한 기관을 신뢰할 수 없는 경우

② 인증서 유효기간의 적정성 여부
: 발급된 인증서의 유효기간이 만료되거나 아직 유효하지 않은 경우

③ 인증서 발급대상과 설치된 웹사이트와의 일치성 여부
: 인증서에 명시된 발급대상 사이트와 실제로 설치된 사이트가 일치하지 않는 경우

특히, 윈도우 비스타에서 Internet Explorer 7을 사용하는 경우 탐색이 차단되고 보안 경고 페이지가 나타나며, 계속 진행하면 보안 상태 표시줄이 붉게 표시되기 때문에 사용자들에게 더욱 강력한 경고를 주게 되어 웹사이트 접속을 기피하게 되므로 인증서 유효성 확인에 대한 주의가 필요합니다. 다음 그림은 보안경고창과 IE 7에서의 보안 경고 페이지의 예입니다.



〈그림 3-17〉 보안 경고창과 보안 경고 페이지 예

5.2 위·변조 웹사이트로 의심받을 가능성

인증서에 명시된 발급대상 사이트와 실제로 설치된 사이트가 일치하지 않을 경우, 중간에 해킹을 통해 위·변조된 피싱 사이트로 이용자들에게 의심받을 가능성이 높습니다.

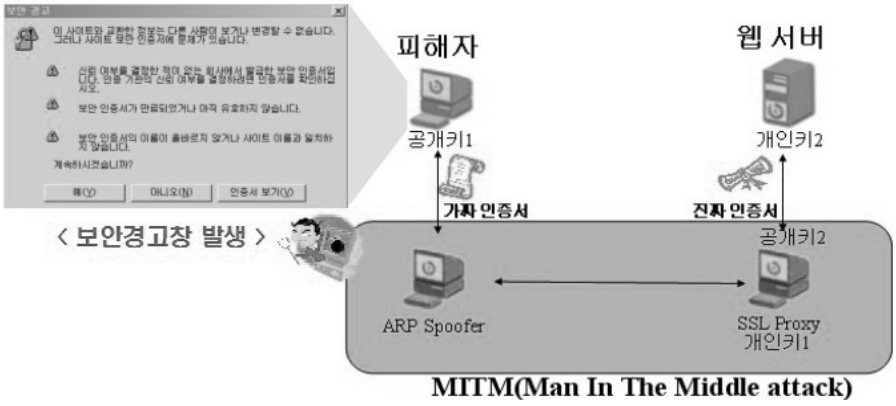
특히 해커가 사용자 PC와 보안서버의 중간에서 프록시 서버를 통해 MITM(Man in the Middle) 공격을 할 경우, 유일한 보호수단은 사용자 PC에서 발생하는 보안경고창입니다. 따라서 정상적인 웹사이트지만 SSL 인증서 유효성의 오류로 인해 보안경고창이 발생하는 것은 사용자들이 정상 웹사이트를 해커의 공격을 받은 웹사이트로 혼동하게 될 소지가 큽니다.

또한 보안서버 구축 가이드 및 리플렛, 안내 홈페이지를 통하여 보안경고창 발생 시 주의할 것으로 지속적으로 안내하고 있기 때문에, 이러한 안내를 받은 이용자가 위·변조된 사이트나 피싱 사이트 등의 불법 웹사이트로 오인하여 접속을 기피하는 현상이 발생할 수 있습니다.

따라서 보안경고창이 발생하지 않도록 보안서버 구축 웹사이트의 SSL 인증서 유효성을 확인하고 웹사이트를 수정하는 등 사전에 확인 조치가 필요합니다.

5.3 유효하지 않는 SSL 인증서 사용시 보안경고창 발생

해커가 사용자 PC와 보안서버의 중간에서 프록시 서버를 통해 MITM(Man in the Middle) 공격을 할 경우, 임의로 발급한 SSL 인증서를 사용함으로 사용자 PC에 보안경고창이 발생하게 됩니다. 따라서 보안경고창은 사용자가 해킹을 인지할 수 있는 수단으로 널리 인지되어 있으며, 사용자가 웹사이트 이용시 정보보호를 위한 기본적으로 확인하는 사항입니다.



〈그림 3-18〉 ARP 스프핑을 이용한 MITM 공격

정상적인 웹사이트지만 다음과 같이 유효하지 않는 SSL 인증서를 사용할 경우 보안경고창이 발생하여 사용자들이 해커의 공격을 받은 웹사이트로 오인하게 될 소지가 큽니다.

① 인증서 발급기관이 웹브라우저의 신뢰기관 목록에 탑재되지 않아서 발급한 기관을 신뢰할 수 없는 경우
(ex: 자체 발급 인증서, 인증기관인 아닌 업체에서 발급한 인증서)
② 발급된 인증서의 유효기간이 만료되거나 아직 유효하지 않은 경우
③ 인증서에 명시된 발급대상 사이트와 실제로 설치된 사이트가 일치하지 않는 경우

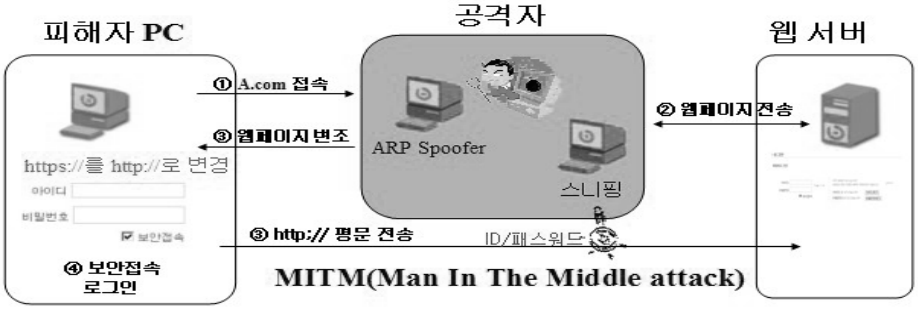
〈 대책 〉

1) SSL 인증서 발급시 다음 사항을 점검한다.
 ① 주요 웹브라우저에서 신뢰기관으로 등록된 인증기관에서 발급된 인증서 인가?
 ② SSL 인증서내 도메인 명과 웹사이트 명이 일치하는가?
 ③ SSL 인증서내 유효기간이 정확한가?
2) 보안서버 구축 후 다음 사항을 점검한다.
 ① 내·외부 네트워크에서 웹사이트를 접속하여 보안경고창이 발생하는지 확인한다.
 ② IE, 파이어 폭스, 사파리 등 주요 웹브라우저에서 보안경고창이 발생하는지 확인한다.

5.4 암호화 통신과 일반 통신의 혼용된 방식의 위험성

최근 MITM(Man in the Middle) 공격의 변형된 방법으로 사용자 PC에 보이는 html 문서를 변경하는 해킹기법이 보고되어 SSL 방식의 보안서버 구축시 각별한 주의가 요구됩니다.

예를 들면 로그인과정에서 보안접속 선택시 실행되는 「https://」를 해킹 도구를 사용하여 「http://」로 변경할 경우 사용자가 보안접속을 선택하여도 일반접속으로 로그인이 진행되어 ID, 패스워드가 인터넷 통신과정에서 평문으로 전송됩니다.



〈그림 3-19〉 ARP 스프핑과 데이터 변조를 통한 MITM 공격

이러한 해킹이 가능한 원인은 웹사이트에서 일반접속과 보안접속을 모두 가능한 형태로 서비스를 제공하고 있기 때문입니다.

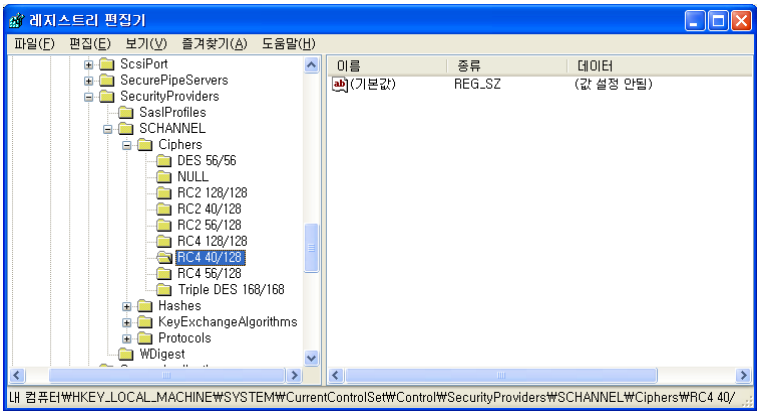
〈 대책 〉

1) 로그인, 회원가입 등 개인정보를 전송하는 경우 보안접속(암호화 전송)만 가능하게 구축
2) 보안접속만 가능한 페이지를 평문 접속(http://)으로 요청할 경우 접속을 제한하거나 특정 페이지로 강제 이동하도록 홈페이지 소스 수정.

5.5 SSL ciphersuite 취약성 해결 방안

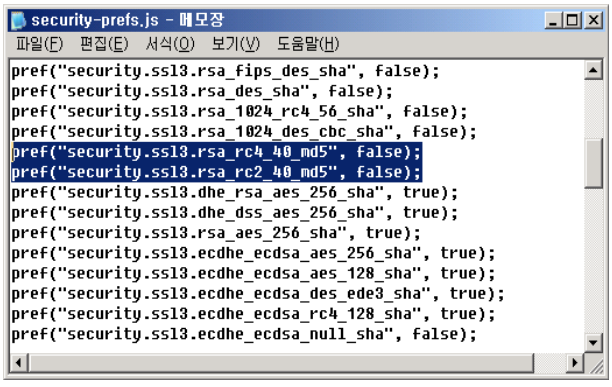
SSL 프로토콜의 취약점 중 하나는 별다른 제약 없이도 Ciphersuite의 수정이 가능하다는 것입니다. 공격자는 이 취약점을 이용하여 사용자의 Ciphersuite 설정을 키 길이가 짧은 대칭키 알고리즘으로 변경할 수 있습니다. 키 길이가 짧은 대칭키 알고리즘으로 암호화된 내용은 공격자가 쉽게 복호화할 수 있기 때문에, 서비스 제공자는 사용자의 Ciphersuite 설정이 키 길이가 짧은 암호화 알고리즘으로 되어있을 경우를 대비해야 합니다.

Ciphersuite는 익스플로러의 경우 레지스트리 편집기를 사용하여 HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩SecurityProviders₩SCHANNEL₩Ciphers 경로를 찾아가면 아래 그림과 같이 수정이 가능합니다.



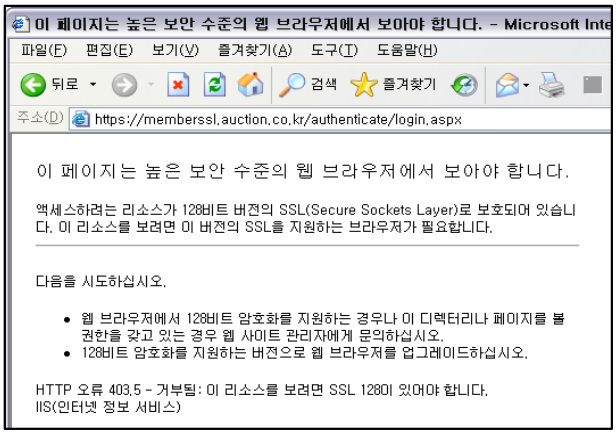
〈그림 3-20〉 익스플로러의 Ciphersuite 수정

파이어폭스는 C:₩Program Files₩Mozilla Firefox₩greprefs₩security-prefs.js파일을 수정하면 〈그림 3-8〉과 같이 메모장을 통해 수정이 가능합니다.



〈그림 3-21〉 파이어폭스의 Ciphersuite 수정

이처럼 Ciphersuite의 수정을 통한 낮은 암호화 알고리즘의 강제사용을 막기 위해서 서버관리자는 일정 강도 이상의 암호화 알고리즘 사용을 강제할 필요가 있습니다. 또, 낮은 암호화 알고리즘을 사용하는 경우 사용자에게 높은 강도의 암호화 알고리즘을 사용할 것을 권장하는 경고메시지를 사용할 필요가 있습니다. 〈그림 3-9〉는 높은 강도의 암호화 알고리즘을 사용할 것을 권장하는 경고메시지의 예입니다.



〈그림 3-22〉 Ciphersuite 키 길이에 대한 보안 경고

6. Windows Vista에서 Internet Explorer 7 이용 시 유의사항

최근 마이크로소프트가 발표한 Internet Explorer 7는 피싱(Phishing) 및 개인 정보를 도용하는 불법 웹 사이트로부터 사용자를 보호하고 개인 정보 유출의 위험 없이 안전하게 인터넷 상거래를 이용할 수 있는 보안 기능을 대폭 강화하였습니다. 이에 따라 SSL 인증서와 관련하여 이전 버전과는 다르게 보안경고 형태, SSL 인증서 프로토콜 설정 등이 수정되었으며, 간단하게 내용을 정리하면 다음과 같습니다.

6.1 보안 경고의 강화

이전 버전에서는 SSL 인증서가 유효하지 않은 경우, 유효하지 않은 이유를 설명하는 보안경고창이 발생하였으나, Windows Vista에서 Internet Explorer 7을 사용하는 경우 잘못된 인증서를 가진 웹사이트는 탐색이 완전히 차단되면서 '이 웹사이트의 보안 인증서에 문제가 있습니다.' 라는 경고 페이지가 보입니다. 인증서 오류의 원인을 간략하게 보여주며 사용자를 속이거나 데이터를 가로챌 수 있다는 경고 문구를 보여줍니다. 사용자의 판단에 따라 '이 웹사이트를 계속 탐색합니다' 를 선택하여 웹페이지에 접속하더라도 보안 상태 표시줄(주소 표시줄)이 빨간 색으로 표시되면서 인증서 오류를 경고하게 됩니다.

이것은 이전 버전의 보안경고창보다 강력한 경고 형태로써 이용자에게 '안전하지 않은 사이트에 접속해 있다' 는 것을 지속적으로 경고하게 되므로 웹사이트에 대한 신뢰도를 하락시키고 이용자들에게 심리적 부담감을 주게 됩니다. 따라서 보안서버 구축·관리시 신뢰할 수 있는 인증기관, 발급 사이트 이름, 인증서 유효기간 등을 확인하여 보안서버 구축의 유효성을 유지하는 것이 매우 중요합니다. 다음은 인증서 오류로 인한 보안 경고 페이지와 보안 상태 표시줄이 빨간 색으로 표시되는 예입니다.

〈그림 3-23〉 인증서 오류로 인한 보안 경고 페이지 예

〈그림 3-24〉 보안 상태 표시줄이 빨간 색으로 표시되는 예

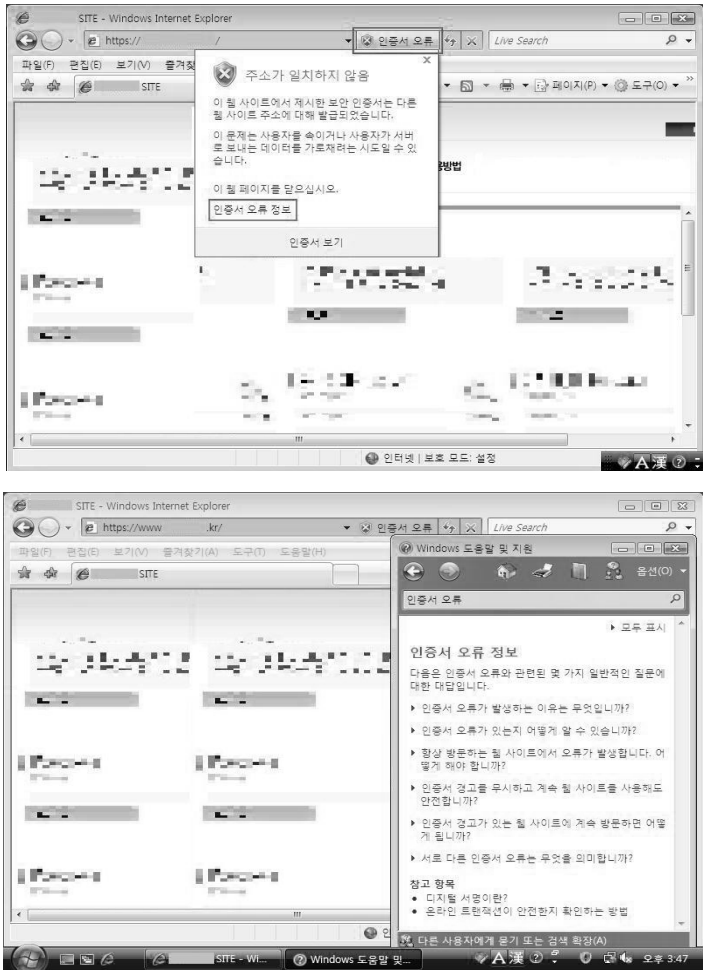
보안 상태 표시줄은 인증 조직에서 수행한 유효성 검사의 수준을 표시합니다. 보안 상태 표시줄 아이콘 색이 의미하는 내용은 다음과 같습니다.

색	의 미
빨강	인증서가 오래되었거나, 유효하지 않거나, 오류가 있습니다.
노랑	인증서 또는 인증서를 발급한 인증기관의 신뢰성을 확인할 수 없습니다. 인증기관의 웹 사이트에서 문제가 있음을 나타낼 수 있습니다.
흰색	인증서의 유효성이 보통 수준입니다. 즉, 브라우저와 웹 사이트 사이의 통신이 암호화되어 있습니다. 인증기관에서 웹 사이트의 정해진 업무 관례에 대해 특별한 문제를 표시하지 않습니다.
녹색	인증서에서 확장된 유효성 검사를 사용합니다. 즉, 브라우저와 웹 사이트 간의 통신이 암호화되어 있으며 인증기관에서 해당 웹 사이트가 인증서 및 보안 상태 표시줄에 표시된 규칙에 부합하는 합법적인 조직에 의해 소유 및 운영되고 있음을 확인했습니다. 인증기관에서 웹 사이트의 정해진 업무 관례에 대해 특별한 문제를 표시하지 않습니다.

* 출처 : Internet Explorer 7 도움말

6.2 인증서 오류에 대한 설명 강화

인증서 오류에 대한 자세한 내용은 보안 상태 표시줄에 나타나는 인증서 오류를 클릭하여 오류의 원인을 확인할 수 있습니다. 보다 자세한 오류의 원인에 대하여 확인하고 싶다면 인증서 오류 정보를 누르면 도움말 화면을 통하여 각 오류의 원인을 확인할 수 있으며, Windows 도움말에 설명된 인증서 오류는 다음과 같습니다.

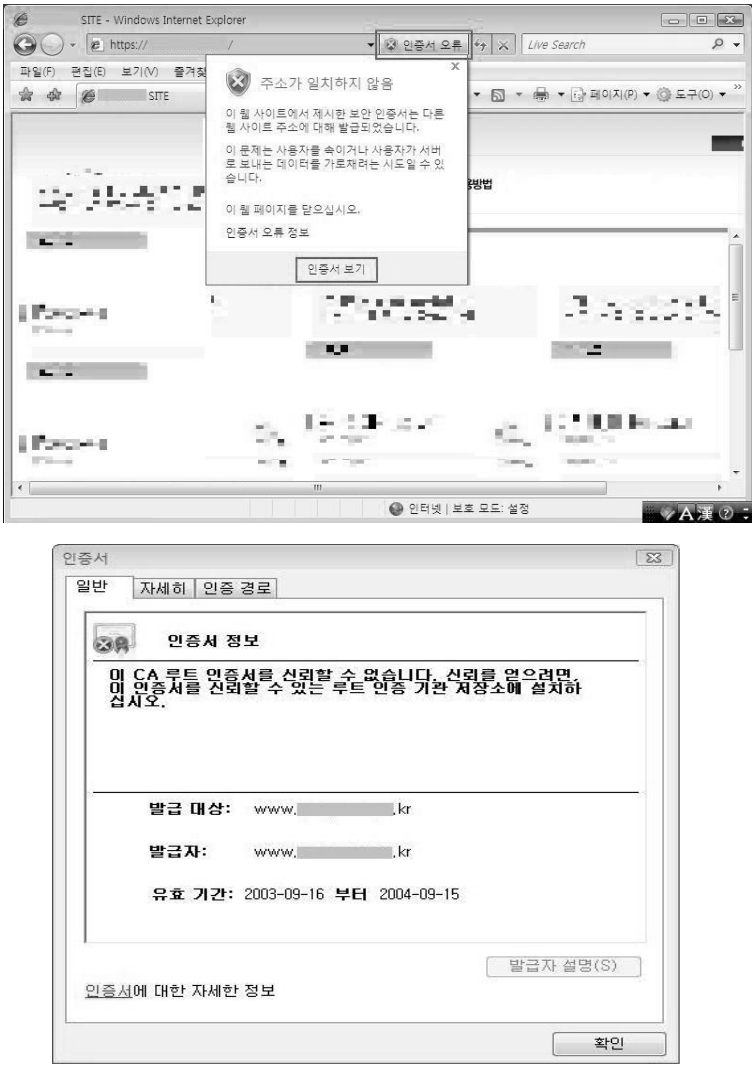


〈그림 3-25〉 인증서 오류 정보 확인 방법

오류 메시지	의 미
이 웹 사이트의 보안 인증서가 해지되었습니다.	이 웹 사이트를 신뢰하지 마십시오. 이 오류는 종종 웹 사이트에서 부정한 방법으로 보안 인증서를 얻었거나 사용했음을 의미합니다. 인증서에서 지정된 암호화 키가 손상되었거나 인증서에 나열된 사용자에게 사용 권한이 없을 수도 있습니다. 인증서를 발행한 인증기관은 해지된 목록을 보관하며 Internet Explorer는 해당 목록을 확인합니다.
이 웹 사이트의 보안 인증서가 만료되었습니다.	이 오류는 현재 날짜가 인증서 유효기간의 이전이나 이후인 경우에 발생합니다. 웹 사이트의 인증서를 인증기관과 함께 갱신하여 최신 상태를 유지해야 합니다. 기한이 지난 인증서에는 보안 위험이 있을 수 있습니다. 인증서가 만료된 후에는 인증서를 발행한 인증기관에서 인증서의 잘못된 사용에 대해 책임지지 않습니다.
이 웹 사이트의 주소가 보안 인증서의 주소와 일치하지 않습니다.	이 오류는 웹 사이트가 다른 웹 주소에 발행한 디지털 인증서를 사용하고 있음을 나타냅니다. 회사가 여러 웹 사이트를 소유하며 한 웹 주소에 발행한 인증서를 다른 사이트에서 사용하는 경우에도 이 오류가 발생할 수 있습니다. 이 오류는 해당 사이트가 실제로 인증서의 웹 사이트와 관련이 있다고 확신하는 경우에만 무시하십시오.
이 웹 사이트의 보안 인증서가 신뢰할 수 있는 소스에서 발행한 것이 아닙니다.	이 오류는 Interner Explorer 7가 인식하지 못하는 인증기관에서 인증서를 발행한 경우에 발생합니다, 이런 오류는 법률 관련 업무나 은행 사이트에서는 잘 발행하지 않습니다. 위조된 인증서를 사용하려고 하는 피싱 사이트에서 이런 오류를 발생시키는 경우가 자주 있습니다.
이 웹 사이트의 보안 인증서 문제가 발견되었습니다.	이 오류는 Interner Explorer 7가 다른 오류 조건에 맞지 않는 보안 인증서 문제를 찾았을 때 발생합니다. 이 오류는 인증서가 손상되거나 변조 또는 알 수 없는 형식으로 작성되거나 읽을 수 없는 경우에 발생할 수 있습니다. 인증서에 이 오류가 있으면 사이트의 ID를 신뢰하지 마십시오.

* 출처 : Internet Explorer 7 도움말

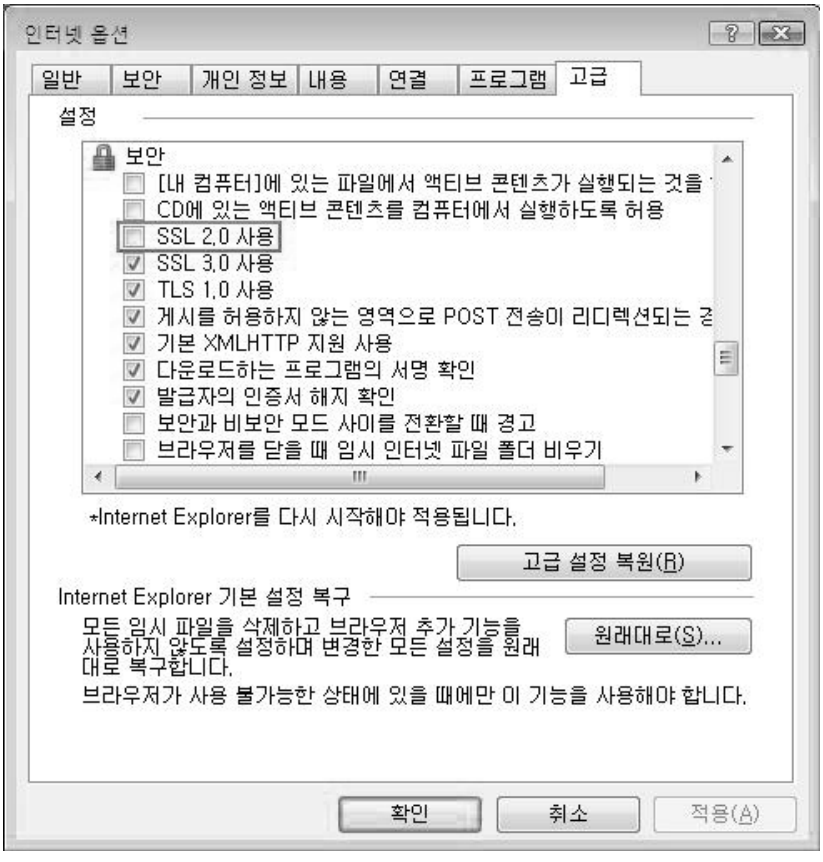
또한 인증서 정보를 확인하고 계속 접속해도 되는 사이트인지 판단하고자 한다면 하단의 인증서 보기를 눌러 인증서 발급기관, 발급대상 사이트 명, 유효기간 등을 직접 확인한 후 접속여부를 결정할 수 있습니다.



〈그림 3-26〉 인증서 오류 원인 확인 방법

6.3 인증서 프로토콜 기본 설정 변화

Internet Explorer 7에서는 인증서 프로토콜 기본값으로 SSLv2 대신 TLSv1을 사용하기 때문에 SSLv2를 사용하는 사이트의 경우 보안 경고 페이지가 표시됩니다. 이 문제를 해결하기 위해서 Internet Explorer 7 이용자들은 메뉴 중 도구 → 인터넷 옵션 → 고급 탭을 선택하여 보안 내용 중 SSL 2.0을 사용하는 것으로 설정하면 됩니다.



〈그림 3-27〉 IE 7의 인증서 프로토콜 기본 설정

7 .국산 SSL 인증서 보안경고창 해결방법

국산 SSL 인증서가 2006년 2월에 인터넷 익스플로러(IE) 브라우저의 신뢰된 루트 인증기관으로 등록되었기 때문에 그 이전부터 사용되어온 웹브라우저 및 운영체제에 반영되지 않아 보안경고창이 발생하는 경우가 있습니다. 보안경고창이 발생하는 경우를 살펴보고 각 원인별 해결방법을 설명하겠습니다.

7.1 Windows 98을 사용

가. 발생 원인

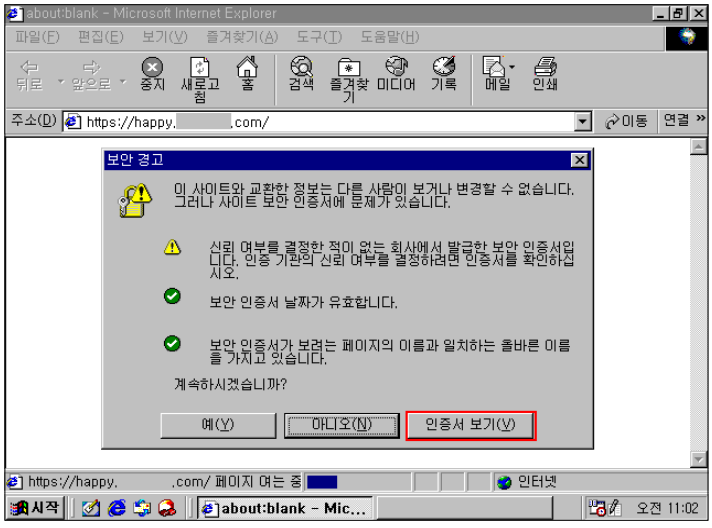
Windows 98 사용자가 국산 SSL 인증서를 이용하여 보안서버를 구축한 웹사이트에 접속하는 경우 보안경고창이 발생하게 됩니다.

그 이유는 국산 보안서버용 루트 인증서가 2006년 2월에 MS의 신뢰된 루트 인증기관 목록에 탑재되었으나, 윈도우즈 98은 더 이상 패치를 제공하지 않아 해당 내용이 반영되지 못하기 때문입니다. 보안경고창 확인 후 계속 진행하여도 전송되는 데이터는 암호화되며, 국산 보안서버용 루트 인증서를 등록하여 줌으로써 향후 보안경고창이 발생하지 않도록 조치할 수 있습니다.

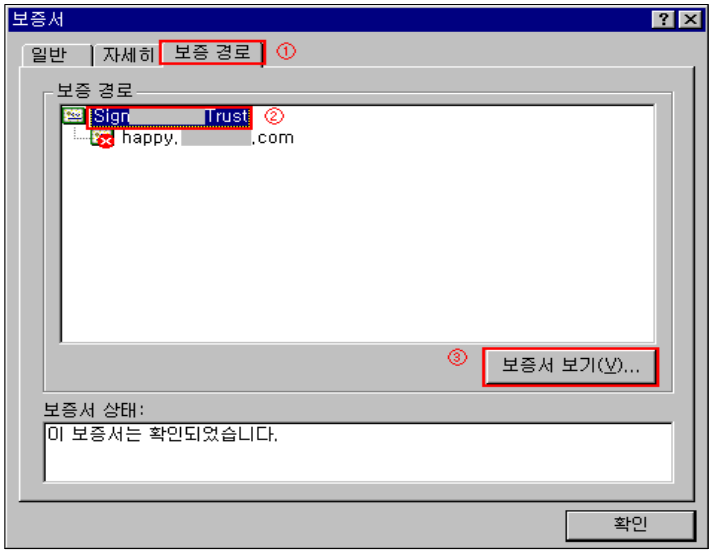
나. 해결방법

① 보안경고창 발생시 '인증서 보기'를 클릭합니다.

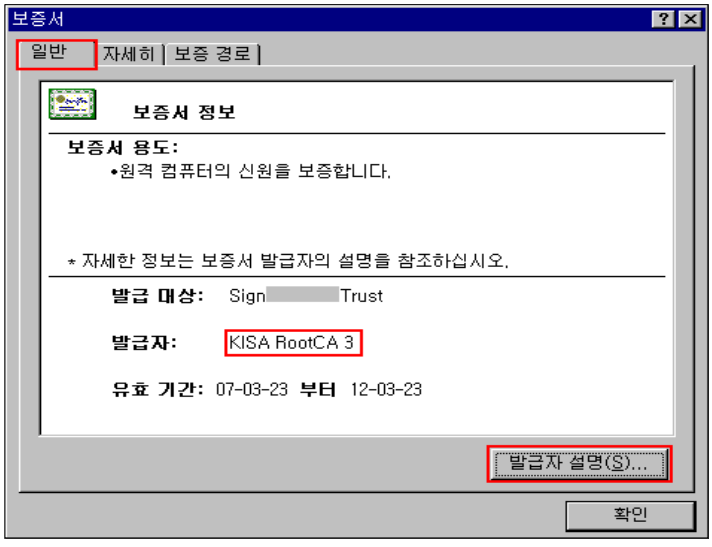
경고창 내용 중 인증서 날짜가 유효하고, 방문하는 웹 페이지와 동일한 이름을 가지고 있는지 확인 후 '인증서 보기'를 클릭합니다. 만약 인증서 날짜가 유효하지 않거나 방문하려는 웹페이지와 이름이 다르다면 해당 웹사이트에서 유효하지 않는 인증서를 사용 중인 것이므로 접속에 유의하시기 바랍니다.



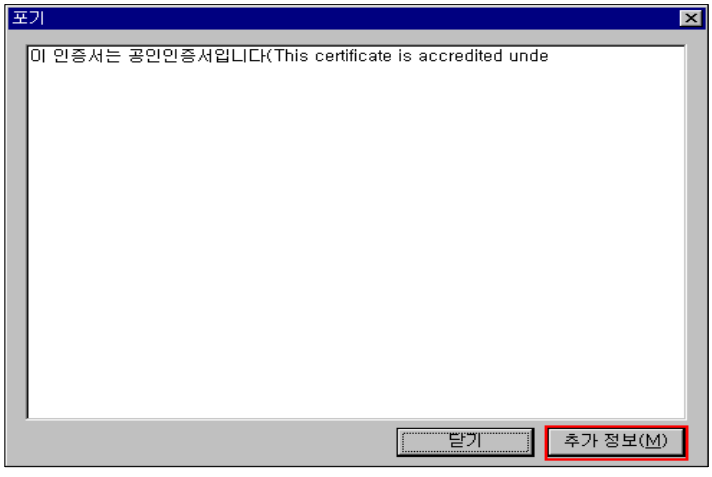
② 보증서(인증서) 정보 중 '보증 경로' 탭을 확인합니다.
보증경로에서 접속한 웹사이트 상위 단계의 보증서(인증서)를 선택한 후 '보증서 보기'를 클릭합니다.



③ 보증서 '일반 탭'에서 보증서 정보를 확인합니다.
발급자가 'KISA RootCA 1' 또는 'KISA RootCA 3'로 되어 있으면 '발급자 설명' 버튼을 클릭합니다.



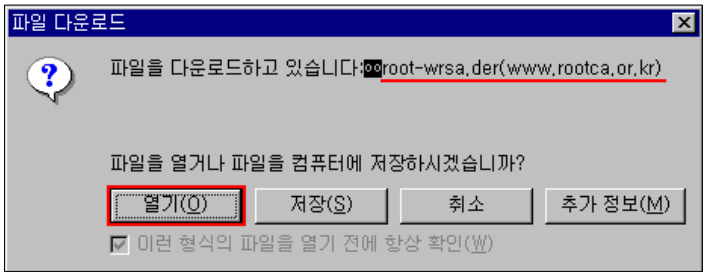
④ 공인 인증서(보증서)임을 확인하시고 '추가정보' 버튼을 클릭합니다.
국산 보안서버용 루트 인증서를 설치할 수 있는 전자서명인증관리센터 홈페이지(http://www.rootca.or.kr/rca/cps.html)로 이동합니다.



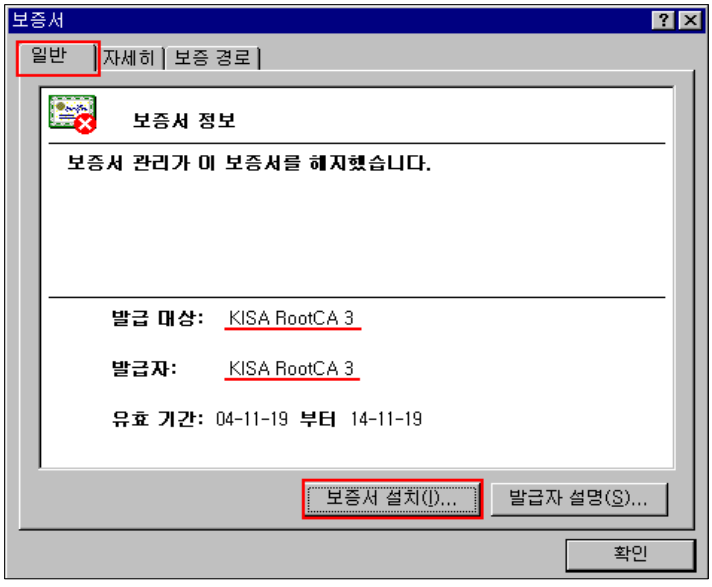
⑤ '보안서버 루트 인증서 설치' 버튼을 클릭합니다.

웹페이지 화면 좌측 하단에 있는 '보안서버용 루트 인증서 설치' 버튼을 눌러 안내에 따라 인증서를 설치합니다.

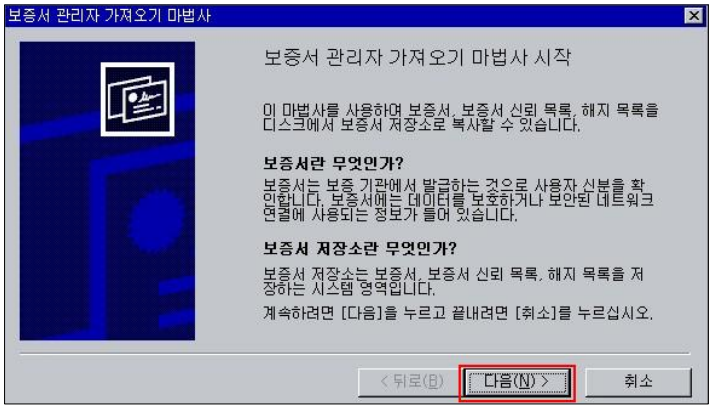
⑥ 대화창의 '열기'를 클릭합니다.



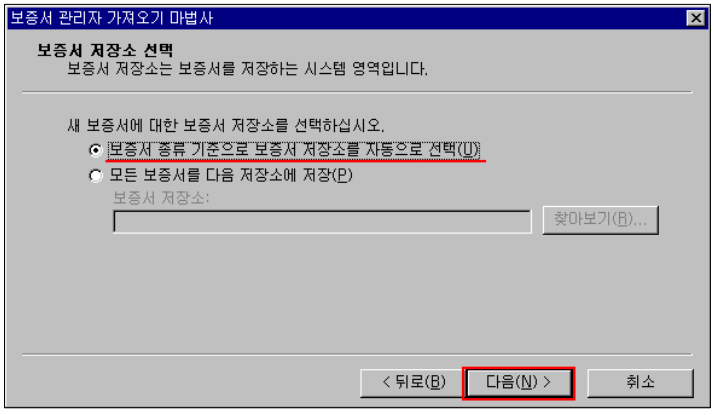
⑦ 보증서 '일반 탭'에서 보증서 정보를 확인합니다.
발급대상과 발급자가 'KISA RootCA 1' 또는 'KISA RootCA 3'인지 확인한 후 '보증서 설치' 버튼을 누릅니다.



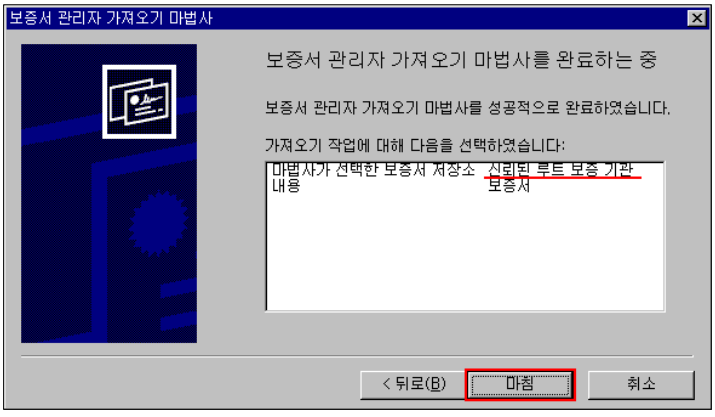
⑧ 보증서 관리자 가져오기 마법사가 시작되면 '다음'을 클릭합니다.



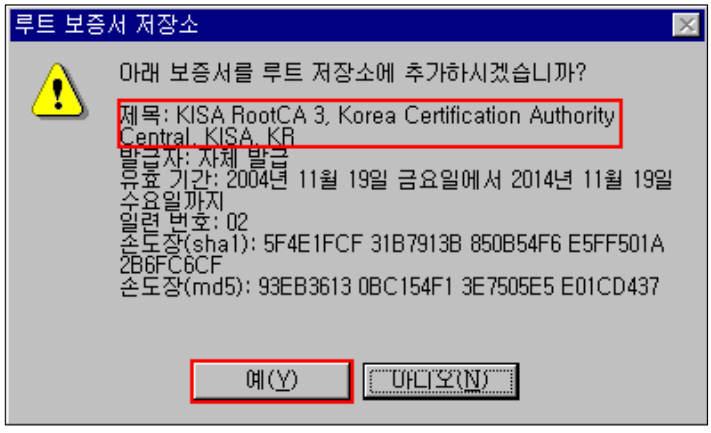
⑨ 「보증서 종류 기준으로 보증서 저장소를 자동으로 선택」 을 선택하고 '다음'을 클릭합니다.



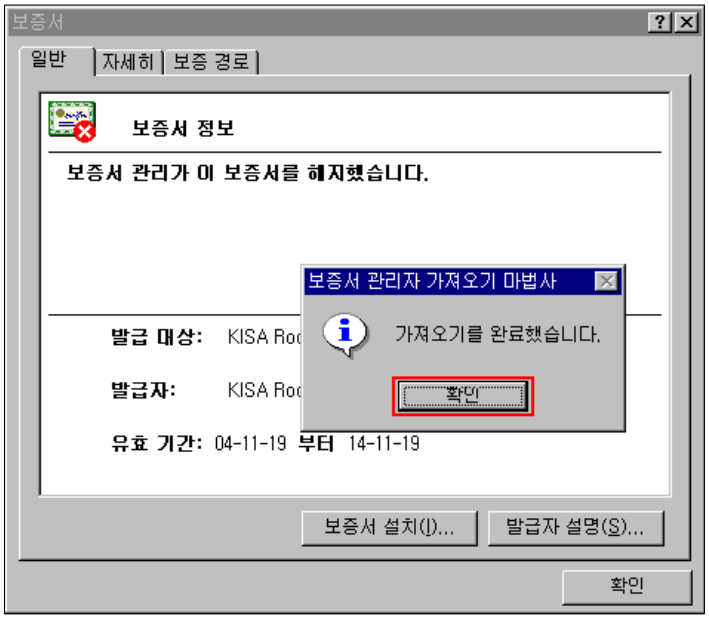
⑩ 보증서 저장소 위치가 「신뢰된 루트 보증 기관」 인지 확인하고 '마침'을 클릭합니다.



⑪ 아래 화면 내용을 확인하시고 '예'를 클릭합니다.

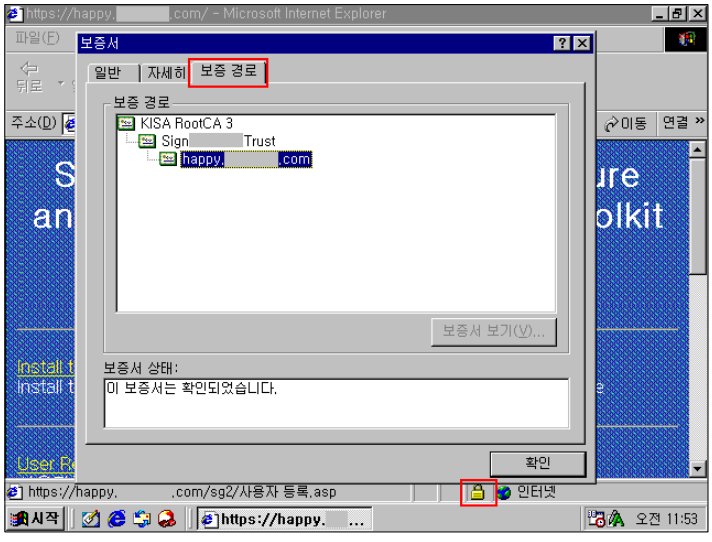


⑫ '확인'을 클릭하면, 보증서 관리자 가져오기가 완료됩니다.



⑬ 인증서 설치를 완료한 후 웹 사이트 접속을 시도하던 웹 브라우저를 종료하고 다시 웹사이트에 접속하면, 보안경고창 없이 사이트에 접속할 수 있습니다.

⑭ 접속한 페이지 하단의 노란색 자물쇠 이미지를 더블 클릭하고 보증경로 탭을 눌러 국산 보안서버용 루트 인증서 설치를 확인합니다.
'KISA RootCA 1' 또는 'KISA RootCA 3'이 설치되어 있는지 확인합니다.



7.2 Windows XP Sevice Pack 1 이하의 운영체제를 사용

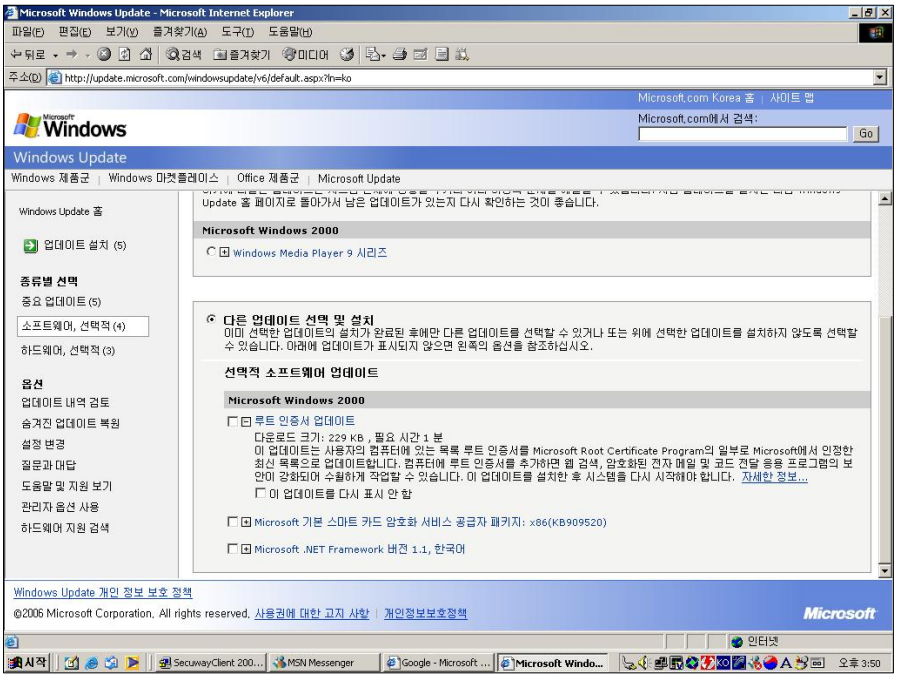
가. 발생 원인

Windows XP Sevice Pack 1 이하의 운영체제하에서 보안경고창이 발생하는 경우는 사용자 업데이트를 제대로 설치하지 않았기 때문입니다. Windows XP Service Pack 2 버전부터는 인증서 신뢰목록에 국산 SSL 인증서가 포함되어 있지만, 그 이전 버전에서는 Microsoft사가 제공하는 업데이트를 설치하여 인증서 신뢰목록을 갱신하거나 국산 보안서버용 루트 인증서를 등록하여 줌으로써 향후 보안경고창이 발생하지 않도록 조치할 수 있습니다.

나. 해결방법

Microsoft사에서 제공하는 업데이트를 설치하지 않아 보안경고창이 발생하는 것이므로 윈도우 업데이트를 실행한 후 국산 SSL 인증서를 이용한 보안서버 구축 웹사이트에 접속하면 보안경고창이 발생하지 않습니다. 또는 '가. Windows 98을 사용하는 경우'와 마찬가지로 보안경고창이 발생하는 웹사이트의 SSL 인증서 발급자 정보를 확인한 후 루트 인증서를 설치하거나 전자서명인증관리센터(www.rootca.or.kr/rca/cps.html)내의 보안서버용 루트 인증서를 설치하면 보안경고창이 발생하지 않습니다.

윈도우 업데이트를 하고자 하는 경우, 윈도우 시작 버튼을 눌러 Windows Update를 실행한 후 사용자 정의 업데이트 중 루트 인증서 업데이트를 선택하여 해당 파일을 설치하면 됩니다.



7.3 Firefox 등 MS Internet Explorer 외의 브라우저를 사용

가. 발생 원인

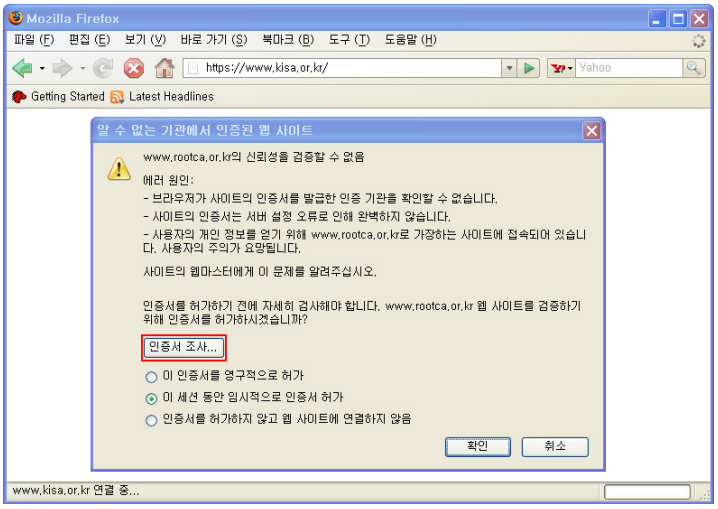
국산 보안서버용 루트 인증서가 MS Internet Explorer의 신뢰된 루트 인증기관 목록에 탑재되었으나, Mozilla Firefox, Netscape Navigator 등 일부 웹브라우저에는 탑재되지 않아 이들 웹브라우저를 이용하여 보안서버 구축 웹사이트에 접속할 경우 '신뢰된 인증서 발급기관이 아니다'라는 보안경고창이 발생하는 경우가 있습니다. 국내 사용자가 상대적으로 많은 웹브라우저에 대한 인증서 탑재를 우선 추진하여 일부 누락된 경우가 있으니, 불편하더라도 국산 SSL 인증서 발급기관을 확인 절차를 거쳐 경고창이 발생하지 않도록 조치할 수 있습니다.

나. 해결방법

보안경고창을 확인 후 계속 진행하여도 전송되는 데이터는 암호화되며, 다음과 같이 KISA 인증서에 대하여 사용을 허가하면 향후 보안 경고창이 발생하지 않도록 조치할 수 있습니다. 본 가이드에서는 Internet Explorer 외의 웹브라우저 중 국내에서 많이 사용되는 FireFox를 중심으로 설명하며, Firefox와 동일한 소스를 사용하는 Netscape Navigator의 경우 같은 방법으로 문제를 해결할 수 있습니다.

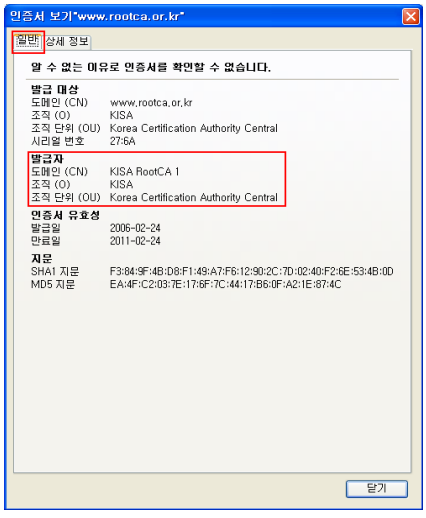
① 보안경고창 발생시 '인증서 조사'를 클릭합니다.

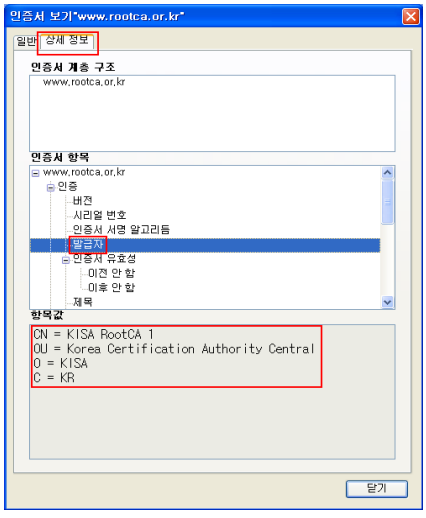
'알 수 없는 기관에서 인증된 웹 사이트'라는 경고창이 발생하면 '인증서 조사'를 눌러 인증서의 내용을 확인합니다. 만약 '서버 인증서가 만료되었습니다', '보안 경고: 도메인 명이 맞지 않음' 내용의 보안경고창이 발생한다면 해당 웹사이트에서 유효하지 않는 인증서를 사용 중인 것이므로 접속에 유의하시기 바랍니다.



② '인증서 보기'에서 인증서 정보를 확인합니다.

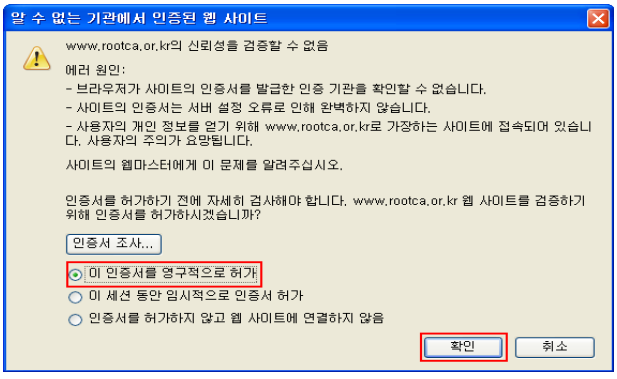
일반 탭을 선택하여 발급자 정보를 확인하면 KISA에서 발급한 인증서라는 것을 확인할 수 있습니다. 상세정보 탭을 선택하여 보다 자세한 인증서 정보와 발급자 정보를 확인할 수 있습니다.





③ 인증서 정보를 확인한 후, 인증서 사용을 허가합니다.

'이 인증서를 영구적으로 허가'를 선택한 후 확인을 누르면 웹브라우저의 신뢰된 인증기관 목록에 KISA를 추가하면 향후 보안경고창이 발생하지 않게 됩니다.



④ 웹사이트에 재접속하여 인증서 사용을 확인합니다.

https://를 이용하여 보안접속하면 보안경고창 없이 접속되는 것을 확인할 수 있습니다.

또한 주소입력창 오른쪽과 웹브라우저 하단 오른쪽에서 자물쇠 모양의 아이콘을 확인할 수 있습니다.

Ⅳ. 응용프로그램 방식 보안서버 구축하기

1. 소개 및 보안서버 구축 절차
2. 설치 과정
3. 오류 발생 시 대처방법
4. 응용프로그램 방식의 보안서버 개발 시 점검 항목

Ⅳ. 응용프로그램 방식 보안서버 구축하기

1. 소개 및 보안서버 구축 절차

1.1 개요

응용프로그램 방식의 경우 SSL 방식과는 달리 제공되는 솔루션마다 설치 방법과 사용방법이 서로 다릅니다. 따라서 본 절에서는 공통적인 설치 과정과 응용프로그램 방식만이 가지는 특징에 대해서 설명하겠습니다.

응용프로그램 방식은 SSL 방식과 같이 클라이언트와 서버간의 데이터를 암호화하는 기능을 제공하고 있습니다. SSL 방식이 웹 브라우저와 웹 서버가 기본적으로 가지고 있는 SSL 기능을 이용하는 것과는 달리 응용프로그램 방식은 웹 브라우저와 웹 서버에 별도의 모듈을 추가하여 데이터를 암호화하는 기능을 제공합니다.

대부분의 웹 브라우저는 기능을 향상시키기 위한 나름대로의 확장기능을 제공합니다. 인터넷 사용시 볼 수 있는 플래쉬나 미디어플레이어 등이 이러한 확장기능을 이용하는 대표적인 예라고 볼 수 있습니다.

응용프로그램 방식은 웹 브라우저와 웹 서버가 기본적으로 제공해 주지 않는 추가적인 기능으로 동작하기 때문에 이러한 확장기능을 통하여 기능을 제공합니다.

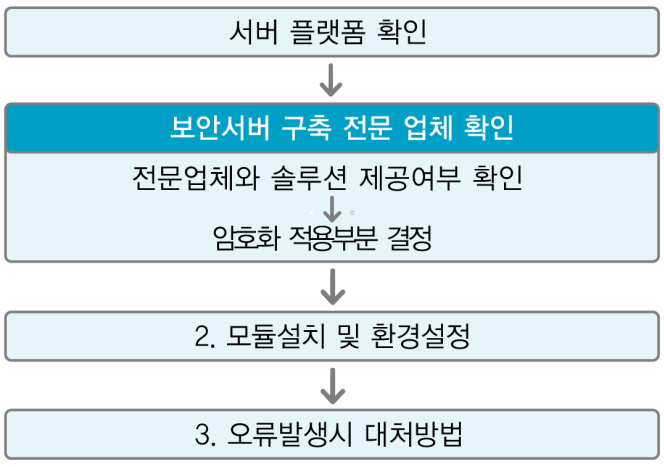
웹 브라우저 확장기능을 이용해 만든 것을 클라이언트 모듈이라고하고, 웹 서버의 확장기능을 이용해 만든 것을 서버 모듈이라고 합니다. 클라이언트 모듈은 일반적으로 Active-X 형태로 제공되며, 서버 모듈은 Java의 경우 Java Servlet Filter 혹은 Jar 파일로 제공되며, IIS의 경우 Filter 혹은 DLL 형태로, PHP의 경우 확장 모듈 형태로 제공됩니다.

1.2 보안서버 구축 절차

응용프로그램 방식은 웹 서버에 서버 모듈을 설치해야 하고, 웹 브라우저에 클라이언트 모듈을 다운로드하여 설치해야 하는 방식이므로 SSL 방식과는 다른 절차가 필요합니다.

SSL 방식의 경우 웹 서버에 인증서를 설치한 후 설정 부분을 수정하고, 실제 사용할 부분의 URL 부분을 수정해 주어야 하는 것과는 달리 응용프로그램 방식은 웹 서버 혹은 웹 어플리케이션 서버에 모듈을 설치하는 과정이 필요하므로 구축 전문 업체와의 협력을 통해 설치가 진행됩니다.

일반적인 응용프로그램 방식의 구축 절차는 다음과 같습니다.

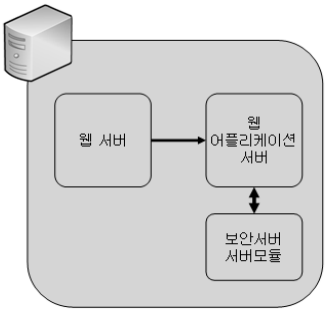


〈그림 4-1〉 응용프로그램 방식 보안서버 구축 절차

① 서버 플랫폼 확인

보안서버를 응용프로그램 방식으로 구축하기로 결정하셨다면 그 다음으로 할 일은 서버 플랫폼을 확인하는 단계입니다. 응용프로그램 방식은 보안서버 서버모듈을 설치

해야 하기 때문에 서버 플랫폼으로 어떤 것을 사용하느냐에 따라 각각에 맞는 서버모듈을 제공하게 됩니다.



〈그림 4-2〉 서버 플랫폼의 구성

서버 플랫폼은 통상 「웹 서버」와 「웹 어플리케이션 서버」로 나누어질 수 있습니다.

보안서버의 서버모듈은 일반적으로 웹 어플리케이션 서버와 연동됩니다. 따라서 어떤 웹 어플리케이션 서버를 사용하느냐에 따라 제공되는 보안서버 서버모듈도 달라집니다.

웹 서버는 일반적으로 Apache 웹 서버를 많이 사용하고 웹 어플리케이션 서버로는 자바계열의 톰캣(Tomcat), 제이보스, 웹로직 등이 있고, MS 계열의 ASP와 .Net이 있으며, 그 밖에 PHP 등이 많이 사용되고 있습니다.

② 보안서버 구축 전문 업체 확인

현재 운영되고 있는 서버플랫폼을 확인하셨다면 보안서버 구축 전문 업체 등을 통해 해당 서버 플랫폼에 맞는 응용프로그램 방식의 솔루션을 제공해 줄 수 있는지 확인해야 합니다.

③ 암호화 적용부분 결정

보안서버 구축 전문 업체가 결정되었으면 보안서버 구축 전문 업체와 함께 암호화를 적용할 부분을 결정해야 합니다. 응용프로그램 방식에서의 암호화 부분은 텍스트로 전송되는 부분만을 암호화하여, 이미지와 같이 암호화가 불필요한 부분은 제외시킬 수 있습니다.

④ 모듈설치 및 환경설정

암호화 적용 부분까지 결정되었다면 보안서버 구축 전문 업체와 함께 서버 모듈을 설치해야 합니다. 이와 함께 필요한 환경설정도 진행되게 됩니다. 환경설정 부분은 제공되는 보안서버 전문 업체의 솔루션마다 조금씩 다를 수 있습니다.

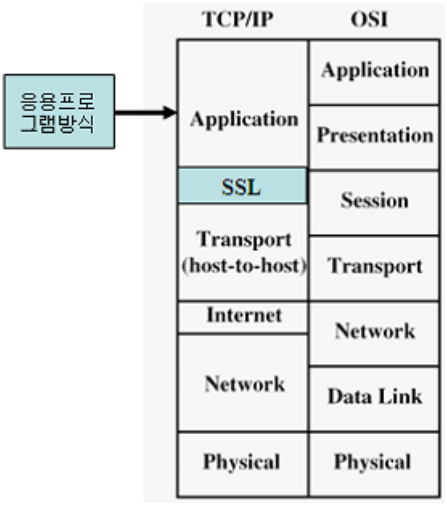
⑤ 구축완료

이제 응용프로그램 방식의 보안서버 구축이 완료되었습니다.

1.3 프로토콜 설명

응용프로그램 방식에서 암호화된 데이터를 전달하는 프로토콜은 SSL 방식과는 달리 Application 계층에서 이루어집니다.

SSL 방식의 경우 Application과 Transport 계층 사이에 SSL이라는 별도의 계층으로서 데이터를 전달합니다. 이 방법의 경우 Application에서 암호화할 때 계층을 설정해 주는 일 이외에는 별다른 작업이 필요 없는 장점을 가지고 있습니다. 하지만, 계층으로서 데이터를 전송하기 때문에 암호화할 부분을 선택적으로 전송할 수 없어 불필요한 이미지나 동영상과 같은 데이터도 암호화하여 전송할 수밖에 없습니다.



〈그림 4-3〉 응용프로그램 방식 프로토콜

응용프로그램 방식의 경우는 별도의 계층이 아닌 Application 계층에서 동작합니다. 이러한 방식의 장점은 필요한 부분만 암호화하여 전달할 수 있다는 점입니다. Application에서 필요한 부분만을 적용하여 암호화하여 불필요한 리소스 낭비를 줄일 수 있습니다.

하지만 Application에서 동작하기 위해서는 Application과의 연동 작업이 필요합니다. 즉, 웹 서버쪽 프로그램 일부의 수정작업이 필요합니다. 응용프로그램 방식을 제공하는 업체에 따라 수정작업의 범위나 양은 많은 차이가 있습니다. 일부 응용프로그램 방식의 경우 SSL 방식과 유사한 형태의 암호화 방식을 취하면서도 선택적 암호화가 가능한 기능을 제공하는 제품도 있습니다.

2. 설치 과정

2.1 클라이언트 모듈 설치

앞서 설명된 것처럼 응용프로그램 방식에서는 클라이언트 모듈의 설치가 필요합니다. 클라이언트 모듈이 설치되는 것은 사용자 PC의 웹 브라우저이지만 이를 위해서는 사용자가 웹 서버에 접속했을 때 클라이언트 모듈을 다운로드하여 설치하게끔 하는 사전작업을 수행해야 합니다.

이것은 웹 포털이나 웹 서비스에 접속했을 때 해당 사이트에 플래쉬가 있을 경우 자동으로 플래쉬 구동 프로그램이 설치되는 것과 동일한 원리입니다.

이를 위해서는 웹 서버의 특정 부분에 클라이언트 모듈을 다운로드 및 설치하는 object 태그를 넣어 두어야 합니다.

하지만 이러한 태그를 설치자가 직접 작성하는 것은 아닙니다. 대부분의 응용프로그램 방식을 제공하는 업체들은 별도의 Javascript 파일을 만들어 이 안에서 자동으로 다운로드되고 설치되도록 만들어 두었습니다. 설치시는 이 Javascript 파일을 포함시키면 됩니다.

〈script language="javascript" src="/abc_plugin.js"〉〈/script〉

이 Javascript 파일을 포함 시킬 위치는 해당 솔루션을 공급하는 업체와 협의하여 진행하면 됩니다.

2.2 서버 모듈 설치

서버모듈의 설치는 응용프로그램 방식을 공급하는 업체별로 또한 사용하는 웹 어플리케이션 서버의 종류에 따라 많은 차이가 있습니다. 따라서 대부분의 응용프로그램 방식을 제공하는

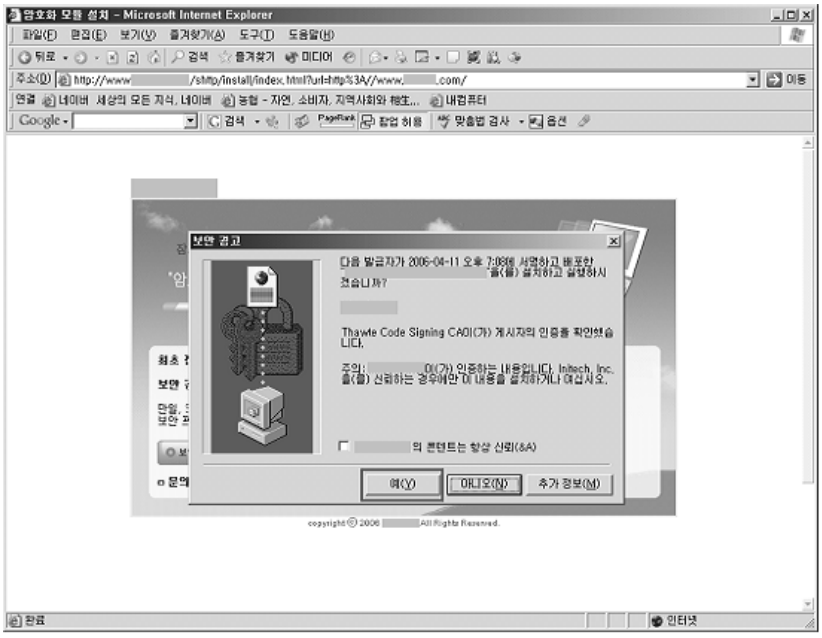
업체들이 서버모듈 설치 과정을 직접 지원하고 있습니다.

응용프로그램 방식을 사용하고자 한다면 전문 업체와 협의하여 해당 웹 어플리케이션 서버에 적절한 서버모듈을 설치하면 됩니다.

2.3 사이트 접속

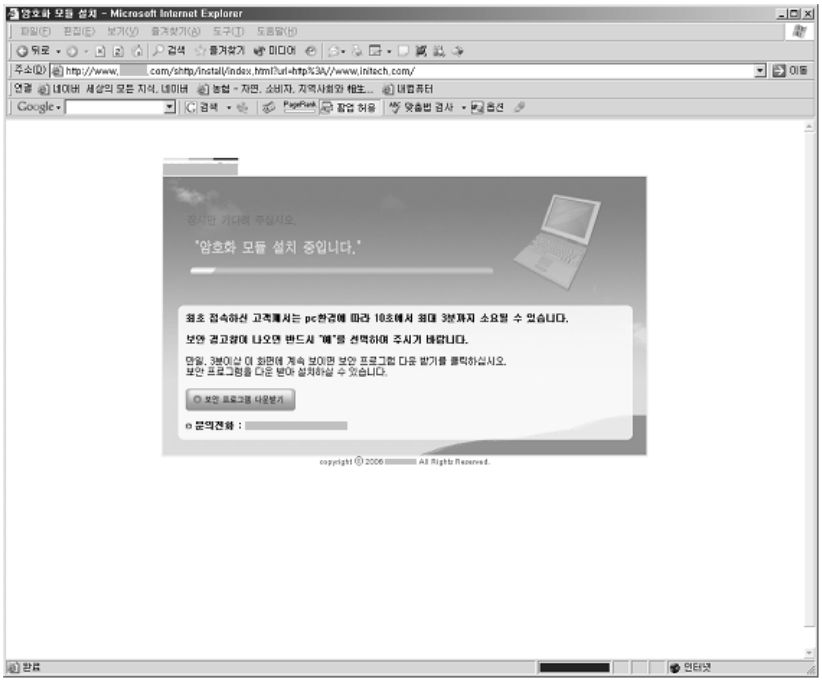
웹 브라우저를 열어 응용프로그램 방식의 보안서버가 구동중인 웹 서버에 접속하게 되면 아래 화면과 같이 클라이언트 모듈 설치에 대한 안내 화면이 나타나게 됩니다.

이 화면은 클라이언트 모듈 설치시 포함시킨 Javascipt 파일에서 자동적으로 동작하도록 구성되어 있기 때문에 필요시 내용을 수정할 수 있습니다.



〈그림 4-4〉 암호화 모듈 설치를 위한 보안경고창

사용자가 설치에 동의할 경우 다음 그림과 같이 자동적으로 클라이언트 모듈이 설치 및 로딩된 후에 사이트가 열립니다.



〈그림 4-5〉 암호화 모듈 설치

다음은 패킷 캡쳐를 통해 암호화 통신이 되는 것을 확인한 것입니다.

〈그림 4-6〉 암호화 통신 확인

3. 오류 발생 시 대처방법

3.1 OS 관련

① 클라이언트 모듈은 Windows 95 등 오래된 OS에서도 설치되나요?

대부분의 응용프로그램 방식 제공업체들은 상당기간에 걸친 기술 개발을 통해 Windows 95 버전 이상 대부분의 OS에서 설치 문제가 발생하지 않는 클라이언트 모듈을 제공하고 있습니다. 하지만 일부 고객들의 PC 이상으로 설치되지 않는 문제가 발생하는 경우 응용프로그램 방식 제공업체들의 고객지원 센터를 통해 기술 지원을 받으실 수 있습니다.

② MS Windows 이외의 OS 및 Firefox 등의 웹 브라우저에서도 클라이언트 모듈을 사용할 수 있나요?

일반적으로 클라이언트 모듈은 MS Windows의 Internet Explorer 브라우저용을 기본적으로 제공합니다. 일부 응용프로그램 방식 제공업체의 경우 Firefox 및 리눅스, 맥용 클라이언트 모듈도 제공하고 있습니다.

3.2 SSL 방식과의 비교 관련

① 응용프로그램 방식이 SSL 방식과 비교되는 장단점은 무엇인가요?

응용프로그램 방식의 경우 앞서 설명된 바와 같이 암호화할 부분을 선택할 수 있어서 암호화에 대한 서버의 부담을 줄일 수 있습니다. 또한 SSL방식에서는 기본적으로 제공하는 암호화 알고리즘 이외에 추가적인 암호화 알고리즘(국산 암호화 알고리즘인 SEED, ARIA 등)을 이용할 수 있습니다.
또한 공인인증서를 이용한 사용자 인증이나 전자서명과 같은 업무를 추가하신다면 응용프로그램 방식에 추가적인 지원이 가능합니다.
하지만 서버 모듈을 제공하여야 하고 상당부분의 기술지원이 필요하기 때문에 연간 서비스 형태로 제공되는 SSL에 비해서 구축비용이 많이 소요될 수 있습니다.

② SSL 방식은 HTTP 80 포트와는 별도로 443 등의 보안 포트를 사용합니다. 응용프로그램 방식은 어떻습니까?

> 앞서 설명드린대로 응용프로그램 방식은 Application 계층에서 사용되기 때문에 HTTP 80 포트를 그대로 사용합니다.
> 하지만, 일부 응용프로그램 방식의 경우 제품의 특성상 별도의 포트를 사용하는 제품도 있으니 전문 업체에 확인하시기 바랍니다.

③ 파일을 암호화하여 업로드하고 싶은데 응용프로그램 방식에서도 가능한지요?

> 응용프로그램 방식 제공업체에서는 별도의 추가 모듈로서 파일을 암호화하여 업로드하는 기능을 제공하고 있습니다. 솔루션 제공여부는 제공업체에 문의하시기 바랍니다.

4. 응용프로그램 방식의 보안서버 개발 시 점검 항목

응용프로그램 방식의 보안서버를 자체적으로 개발 시에는 다음과 같은 기준이 충족되도록 개발하여야 네트워크상에서 전송되는 데이터를 인가되지 않은 노출, 변경, 삭제 행위로부터 안전하게 보호할 수 있습니다.

4.1 비밀성

통신 상대방과 통신을 수행함에 있어 안전한 암호화 방법을 사용하여 데이터의 비밀성이 훼손되지 않도록 방어할 수 있어야 하며, 안전한 암호화를 위해서 사용되는 암호화 알고리즘은 전송계층보안(TLS : Transport Layer Security)에 대한 국제표준인 RFC2246 The TLS Protocol Version 1.0을 충족하여야 합니다. 암호화 알고리즘을 구현하는 경우 권장 사항은 다음과 같습니다.

① 안전한 암호화를 위해서는 SEED, AES 또는 이들의 안전성에 준하는 암호화 알고리즘을 사용

(SEED: 한국인터넷진흥원이 개발한 128비트 대칭형 블럭암호알고리즘,
AES: Advanced Encryption Standard, 미국의 표준 암호 알고리즘의 공식 명칭)

4.2 암호키 관리

키 관리 데이터의 무결성과 비밀성이 훼손되지 않도록 방어할 수 있어야 하고, 키의 적절하고 안전한 교환을 보장할 수 있어야 하며, 키 관리 데이터의 무결성, 키의 안전한 교환, 키의 안전한 생성 등 세부기준은 TLS 국제표준을 충족하여야 합니다. 키관리 방안을 구현하는 경우 권장 사항은 다음과 같습니다.

① 키 관리 데이터의 무결성을 제공하기 위해서는 RSA, KCDSA, ECKCDSA 등 1024 비트 이상 RSA 인터넷암호화 및 인증시스템에 준하는 전자서명알고리즘 또는 HAS-160, SHA-1 등 160비트 이상의 해쉬값을 생성할 수 있는 해쉬 알고리즘을 사용

(RSA: Rivest-Shamir-Adleman, 1977년에 개발된 알고리즘을 사용하는 인터넷 암호화 및 인증 시스템으로 가장 보편적으로 사용되는 공개키 암호 알고리즘, KCDSA, ECKCDSA: 인증서기반 국내 표준 전자서명알고리즘)

② 키의 안전한 교환을 위해서는 RSA, D-H 등 1024 비트 이상 RSA인터넷암호화 및 인증시스템의 안전성에 준하는 알고리즘을 사용

③ 키의 안전한 생성을 위해서는 암호학적으로 안전한 의사난수 생성 알고리즘을 사용

4.3 식별 및 인증

사용자 단말의 보안모듈은 암호화된 통신을 수행하기 전에 통신 대상 서버의 보안모듈을 유일하게 식별해야 합니다.

4.4 자체기능보호

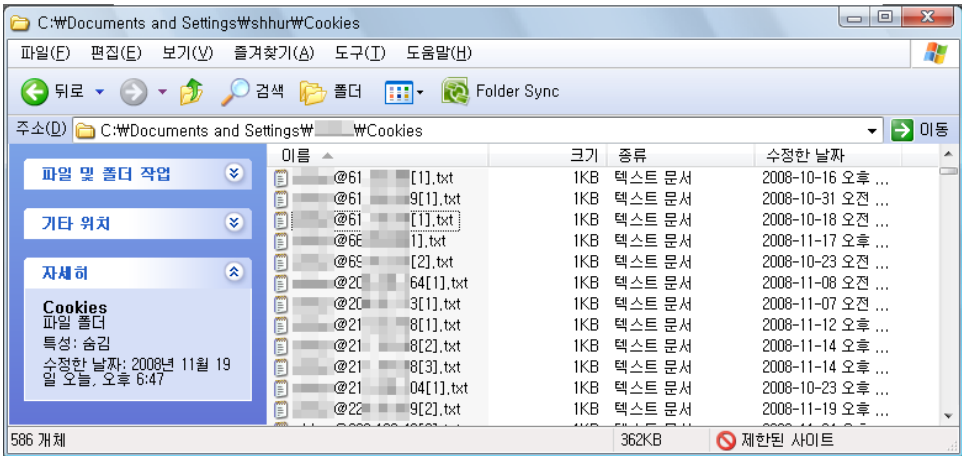
초기 시동할 때부터 제품의 보안기능 변경, 비활성화, 우회 시도 등으로부터 자체를 보호할 수 있어야 합니다.

4.5 배포 및 설치

보안서버 및 관련 사용자 프로그램은 안전한 방법으로 배포 및 설치되고, 인가된 관리자에 의해 안전한 방식으로 구성, 관리, 사용되어야 합니다.

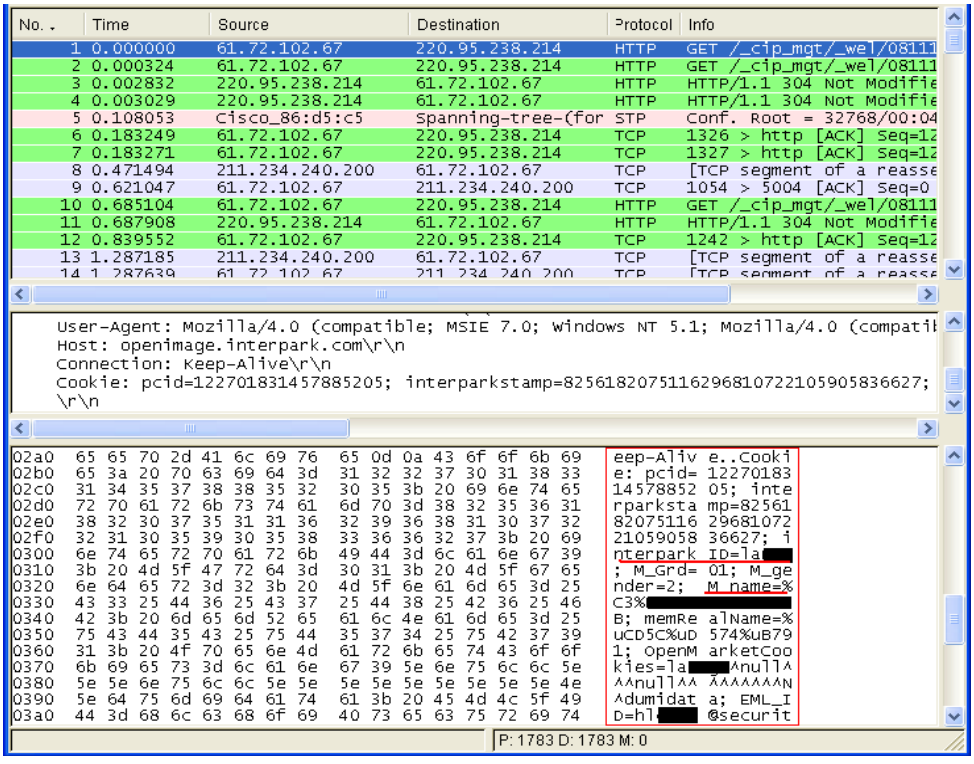
4.6 쿠키 및 파일

쿠키는 서버에서 사용자의 컴퓨터에 설치하는 기록 정보 파일로서, 웹 브라우저의 신속성을 위해 널리 사용되고 있으며 〈그림 4-7〉과 같이 저장위치가 알려져 있습니다.



〈그림 4-7〉 쿠키의 알려진 저장 위치

따라서 공격자가 손쉽게 쿠키를 가로챌 수 있기 때문에, 쿠키에 개인정보를 암호화하지 않고 저장하게 되면 다음 그림과 같이 개인정보가 노출될 수 있습니다. 〈그림 4-8〉은 쿠키파일을 스니핑을 통해 획득한 후 내용을 확인한 것입니다. 사용자 ID와 성별 등과 같은 개인정보가 여과없이 드러남을 확인할 수 있습니다.



〈그림 4-8〉 가로챈 쿠키의 개인 정보 노출

따라서 응용 프로그램이 쿠키에 개인정보를 쓸 때에는 개인정보를 암호화하여 쿠키에 써야 합니다.

쿠키를 암호화 하는 방법은 각 보안서버가 사용하는 스크립트 언어에서 제공하는 암호화 함수를 사용하면 됩니다. 방법은 각 언어별로 조금씩 차이가 있습니다. 아래 그림은 PHP를 사용하여 쿠키를 암호화 하는 방법입니다.

```
[!--- cookie.php ----]
[?
//암호화를 위한 초기값 생성
$iv = mcrypt_create_iv(mcrypt_get_iv_size(MCRYPT_RIJNDA
EL_256, MCRYPT_MODE_ECB), MCRYPT_RAND);
//해독을 위한키
$key = "jdng5jfdpfe519f2dkdh3kdhabc35dfc4";
//문자열의 암호화
$cookietext = "securityserver";
$cipher = mcrypt_encrypt(MCRYPT_RIJNDAEL_256, $key, $co
okietext, MCRYPT_MODE_ECB, $iv);
//쿠키생성
setcookie("username", $cipher, mktime(0,0,0,11,11,2008), "/login
.php");
?]
```

PHP에서는 mcrypt_encrypt()함수를 사용하여 쿠키를 암호화 합니다. 먼저 Initial Vector(IV)를 생성하고 암호화에 사용할 키를 임의로 지정합니다. 그리고 mcrypt_encrypt()함수를 사용하면 평문으로 전송되는 쿠키를 암호화 할 수 있습니다.

암호화된 쿠키를 복호화 하려면 mcrypt_decrypt()함수를 사용하면 됩니다. 먼저 Initial Vector(IV)을 생성하고 mcrypt_decrypt() 함수의 입력값으로 암호화에 사용된 키와 암호문을 사용하면 됩니다. 복호화된 쿠키는 웹브라우저를 통하여 평문형태로 출력됩니다. 쿠키를 복호화 하는 방법은 다음과 같습니다.

```
[!--- login.php ----]
[?
 $iv = mcrypt_create_iv(mcrypt_get_iv_size(MCRYPT_RIJNDA
EL_256, MCRYPT_MODE_ECB), MCRYPT_RAND);
 $valid_user = mcrypt_decrypt(MCRYPT_RIJNDAEL_256, "jdn
g5jfdpfe519f2dkdh3kdhabc35dfc4", $username, MCRYPT_MOD
E_ECB, $iv);
echo ("$valid_user 님이 접속하셨습니다. ");
?]
```

이처럼 쿠키를 암호화하여 전송하면 쿠키를 통한 개인정보의 유출을 막을 수 있습니다.

Ⅴ. 웹호스팅업체의 보안서버 구축하기

1. 보안서버 구축 절차
2. 보안서버 구축 전 확인사항 체크
3. 웹호스팅서비스 제공업체의 고려사항
4. 보안서버 구축상태 확인

Ⅴ. 웹호스팅업체의 보안서버 구축하기

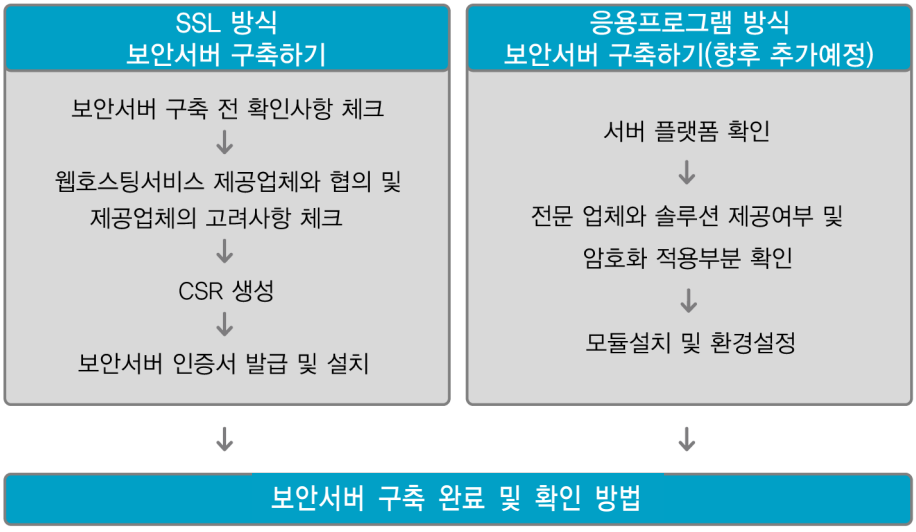
1. 보안서버 구축 절차

단독 서버가 아닌 웹호스팅 서비스를 받고 있는 사이트의 경우, 직접 웹 서버를 수정할 권한을 가지고 있지 않으며, 보안서버 구축을 위한 기술력을 갖추지 않은 경우가 대부분이기 때문에 웹호스팅 서비스 제공업체와의 협의를 통하여 보안서버를 구축하게 될 것입니다.

따라서 원활한 보안서버 구축을 위하여 본격적인 구축 이전에 확인할 사항과 보안서버 구축 이후에 암호화 적용 여부를 확인할 수 있는 방법을 중심으로 설명하고자 합니다.

그리고 웹호스팅 서비스 제공업체 또한 고객사에서 보안서버 구축을 요청할 경우 서버환경과 서비스 제공 가능성 확인 등 고려해야 할 사항을 정리하였습니다.

보안서버 구축은 각 업체마다 구체적인 환경에 따라 달라지지만, 일반적으로 다음과 같은 절차를 따르게 됩니다. 이번 가이드에서는 웹호스팅업체들이 주로 사용하고 있는 SSL 방식의 보안서버 구축 방법을 알아보고, 향후 응용프로그램 방식의 보안서버 구축 방법을 가이드에 추가하도록 하겠습니다.



〈그림 5-1〉 웹호스팅업체의 보안서버 구축 절차

2. 보안서버 구축 전 확인사항 체크

2.1 보안서버 구축 지원 방식 확인

웹호스팅 서비스를 제공하는 업체가 보안서버 구축 서비스를 어떠한 방식으로 제공하는지를 가장 먼저 확인해야 합니다. 일부 웹호스팅 업체의 경우 웹호스팅 환경에 가장 적합한 멀티도메인 SSL 인증서를 이용하거나 응용프로그램방식을 이용하여 보안서버 구축 환경을 갖추는 등 웹호스팅 도메인에 대한 보안서버 구축을 지원하고 있습니다. 또는 각 도메인에 발급되는 단일 SSL 인증서를 이용한 보안서버 구축을 지원하기도 합니다. 따라서 사전에 웹호스팅 서비스 제공업체가 보안서버 구축 서비스를 어떠한 형태로 제공하는지 확인한 후, 사전 협의를 거쳐 보안서버 구축 방식과 절차를 결정하시기 바랍니다.

2.2 발급 도메인에 대한 정보 확인

보안서버 인증서 발급시 사전 정보를 확인하는 절차로 인증서를 신청하는 업체마다 필요로 하는 정보가 다를 수 있으니 미리 확인하시기 바랍니다.

① 보안서버 인증서 신청정보 확인

보안서버 인증서를 신청하기 전에 사업자 정보의 주소나 연락처 등을 현재 운영 중인 내용으로 수정하여 주시기 바랍니다.

정보 확인은 사용 중인 URL 확인과 실제 서비스를 하고 있는 업체를 구별하여 유령회사나 그와 유사한 업체를 사칭하여 인터넷을 이용한 범죄행위를 방지하기 위한 방법입니다.

② 신청사 도메인 정보 확인

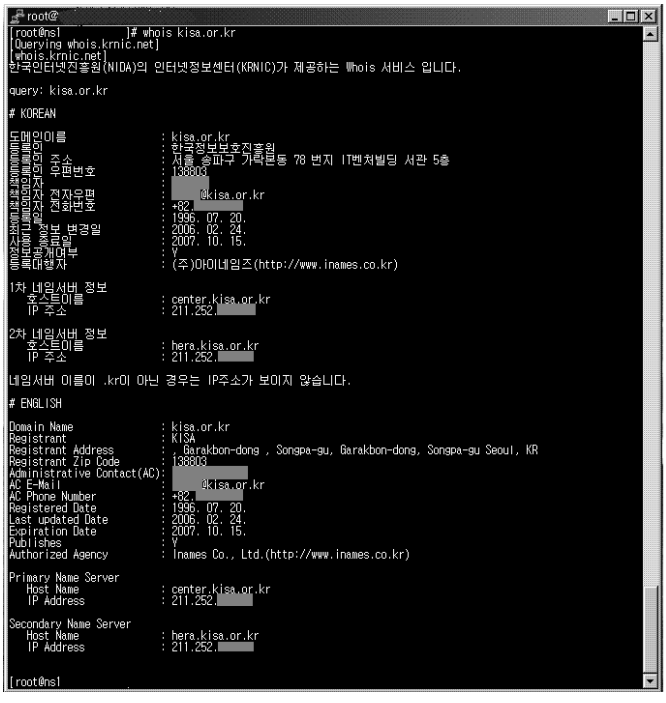
도메인 소유 확인을 통해 확인한 회사명과 소유자의 사업자 등록증상의 회사명과 동일한지 확인합니다. 동일하지 않다면 소유한 도메인 정보를 변경하여야 합니다. 일부 인증기관의 경우 신청사 도메인의 등록정보와 신청사의 웹 서버 정보가 다를 경우 인증서 발급이 되지 않을 수 있으니 사전에 확인하여야 합니다.

인증서를 신청하기 위해서는 기본적으로 도메인을 소유하고 있어야 합니다. 또한 인증서는 웹서비스의 실재성, 즉 도메인 소유자가 직접 서비스를 운영하는지, 운영자가 실존하는 단체나 회사인지를 확인하여 발급됩니다. WHOIS를 통해 보안서버 인증서 신청 도메인명에 대한 소유권을 미리 확인하기 바랍니다.

③ 신청사 권한 확인

인증기관은 보안서버 인증서를 발행하기 전에 인증서 신청업체가 등록 요청에 지정한 이름으로 사업을 할 수 있는 법적 권한이 있는지 여부를 확인합니다. 확인 절차 및 방법은 인증기관이 요구하는 절차에 따라 진행하시면 됩니다.(예 : 사업자 등록증, 대표자의 신분증 사본, 전화번호 영수증 등의 발송 요구)

경우에 따라서 인증기관의 확인절차 중 영문 사업자 등록증을 제출해야 경우가 있습니다. 영문 사업자등록증의 경우 관할세무서를 방문하시면 발급이 가능합니다. 관할 세무서에 대한 정보는 국세청 홈페이지(http://www.nts.go.kr)에서 확인할 수 있습니다.



〈그림 5-2〉 WHOIS를 통한 도메인 정보 확인

2.3 CSR 생성 및 보안서버 적용

CSR 생성 및 보안서버 적용에 대한 구체적인 절차는 'Ⅲ장 SSL 방식 보안서버 구축하기' 내용을 참고하여 작업하시기 바랍니다.

3. 웹호스팅서비스 제공업체의 고려사항

웹호스팅 서비스를 이용하고 있는 고객사로부터 보안서버 구축에 대한 의뢰가 들어오면 웹 호스팅 서비스 제공업체는 다음과 같은 사항들을 고려하여 보안서버를 구축해야 합니다.

3.1 서비스 제공 서버에서 개별 인스턴스로 서비스가 가능한지 여부

① 서버가 IIS 계열인 경우

웹호스팅 서비스 제공시 하나의 서버에서 호스트헤더 분리를 사용하여 여러 도메인을 서비스할 경우, 평문통신을 위한 80 포트에서는 다중 인스턴스로 운영이 가능하지만 암호화 통신을 위한 443 포트는 호스트헤더를 지원하지 않기 때문에 다중 인스턴스 운영이 불가능합니다.

따라서 한 개의 서버에서 여러 도메인을 서비스할 경우에는 인증서 서비스가 필요한 사이트를 개별 인스턴스로 분리하여야 합니다. 하나의 VirtualHost에 하나의 독립적인 IP를 제공하는 IP-based 가상호스팅 방식이나 한 대의 서버에서 하나의 IP를 가지고 다수의 도메인을 운영할 수 있게 해주는 Name-based 가상호스팅 방식을 통하여 개별 인스턴스로 분리하고 다수의 도메인를 인증할 수 있는 SSL 인증서나 응용프로그램 방식의 보안서버를 구축해야 합니다.

② 서버가 Apache 계열인 경우

Apache 서버에서는 VirtualHost를 한 개의 개별 인스턴스로 인식합니다. Apache 서버는 일반적으로 VirtualHost를 사용하여 여러 도메인을 서비스하고 있기 때문에 큰 무리없이 진행할 수 있습니다.

3.2 SSL 보안 포트 서비스 가능 여부

일반적으로 한 개의 IP에서는 SSL을 위한 보안포트가 중복되어 사용할 수 없습니다. 따라서 한 대의 서버에서 여러 도메인에 대한 SSL 보안을 서비스 하려면 보안 서비스를 제공하는 도메인 수만큼의 보안포트의 확보가 필요합니다.

다만, 멀티도메인 SSL 인증서를 사용하면 한 개의 IP에서 보안포트를 중복하여 사용할 수 있습니다. 보다 자세한 내용은 '부록 B. 멀티도메인 SSL 인증서 소개' 내용을 참조하시기 바랍니다.

보안포트가 확보되면 각 보안포트에 대해서는 방화벽 등의 보안장비에서 각 보안포트에 대해서 접근 허용 정책을 추가해야 합니다. 이는 각 서비스 업체의 보안정책과 관련된 사항이므로 사전에 충분히 검토하시기 바랍니다.

3.3 SSL 서비스 가능 여부

① 서버가 IIS 계열인 경우

IIS 계열은 기본적으로 모두 SSL 서비스를 제공하도록 구성되어 있습니다.

② 서버가 Apache 계열인 경우

Apache 서버에서 SSL 서비스를 제공하기 위해서는 반드시 mod_ssl이 설치되어 있어야 서비스 제공이 가능합니다.

현재 서비스 중인 Apache 서버에 mod_ssl이 설치되어 있는지를 httpd -l 옵션을 사용하여 mod_ssl.c 또는 mod_ssl.so 가 있는지 확인하고, 만일 mod_ssl이 설치되어 있지 않다면 'Ⅲ장 SSL 방식 보안서버 구축하기 중 Apache 서버에서 보안서버 구축하기'를 참고하여 설치하시기 바랍니다.

〈그림 5-3〉 mod_ssl 설치 확인 화면

3.4 인증서 신청하기

SSL 방식의 보안서버 인증서는 인증서의 소유가 호스팅 업체가 아닌 사이트 운영자가 소유하게 됩니다. 따라서 인증서를 신청을 하실 경우에는 서버를 소유하거나 운영 대행하는 업체의 정보가 아닌 실제 도메인을 소유하고 서비스를 제공하는 주체의 정보가 필요합니다.

① CSR 생성시 입력 정보

모든 정보는 영문으로 입력하셔야 하며 특수문자를 사용하시면 안됩니다.

CN=운영중인 URL
OU(조직구성단위)=영문 부서명
O(조직명)=도메인을 소유하고 서비스를 제공하는 회사의 영문 전체이름
L(구/군)=도메인을 소유하고 서비스를 제공하는 회사의 위치
S(시/도)=도메인을 소유하고 서비스를 제공하는 회사의 위치
C(국가코드)=KR(대한민국인 경우)

② 준비 서류

공통적으로 도메인을 소유하고 서비스를 제공하는 회사의 사업자 등록증을 준비해야 하며, 인증기관에 따라서 도메인 소유에 대한 확인 절차 및 전화 확인 절차가 있는 경우가 있습니다. 이런 경우에는 추가적인 서류가 필요할 수 있습니다.(예: 도메인 소유 확인증, 전화번호 영수증, 영문 사업자 등록증 등)

4. 보안서버 구축상태 확인

인증서 설치가 완료된 후 정상적으로 인증서가 발급되어 동작되는지 여부는 다음과 같은 방법으로 식별할 수 있습니다.

① 웹 브라우저에 도메인의 URL의 주소를 http가 아닌 'https'를 통해 연결을 시도합니다.

② SSL 인증서버의 경우 기본적으로 80번 포트가 아닌 보안포트를 사용하게 됩니다. https를 이용하여 접속하시면 보안 포트(기본 443번)로 연결이 되어 별다른 작업없이 SSL 인증서버를 통한 통신을 하게 됩니다.

③ 화면 아래에 잠겨진 자물쇠 아이콘이 있습니다.
보다 자세한 내용은 'Ⅵ장 웹페이지 수정 및 적용 확인하기'에서 다루겠습니다.

자, 이제 SSL 인증서의 설치가 완료되었습니다. Ⅵ장으로 이동하셔서 실제 웹페이지를 어떻게 수정해야 하는지 알아보겠습니다.

Ⅵ. 웹 페이지 수정 및 적용 확인하기

1. 웹 페이지 수정 방법 및 사례
2. 보안서버 적용 확인하기
3. 보안서버의 보안 취약성 해결 방안

Ⅵ. 웹페이지 수정 및 적용 확인하기

1. 웹페이지 수정 방법 및 사례

암호화 통신을 하기 위해서 보안 프로토콜을 호출하는 방법은 OS나 Program 언어를 가리지 않고 모두 동일합니다. 그 이유는 암호화 통신을 하기 위해 적용하는 부분이 특정 OS나 특정 Program 언어에 의존하지 않는, 모두가 공통으로 사용하는 HTML 언어이기 때문입니다.

본 절에서는 암호화 적용 범위에 따라 웹페이지 전체 혹은 일부를 암호화하는 방법과 이용자가 선별적으로 암호화를 선택하는 방법을 소개하겠습니다.

1.1 전체 페이지 암호화하기

① https 프로토콜 호출하기

https 프로토콜을 호출하여 웹페이지 전체에 적용하는 방법은 그림만으로도 곧바로 이해를 할 수 있을 정도로 아주 쉽습니다. 간단히 호출하는 프로토콜을 http://에서 https://로 수정해 주기만 하면 됩니다.

〈그림 6-1〉과 〈그림 6-2〉는 암호화 통신을 하기 위해 https 프로토콜을 호출하기 전과 호출한 후의 HTML 소스코드 예입니다.

```
if ($time3 == $time4) {
echo "
<p><a href='http://[redacted].co.kr/zboard/view.php?id=not
desc=asc&no=$no' target='_top'><font size=1 color='silv
:new::-></a></p> ";
} else {
echo "<p><a href='http://[redacted].co.kr/zboard/view.php?
adnum&desc=asc&no=$no' target='_top'><font size=1 color
}
```

〈그림 6-1〉 평문 통신을 위한 HTML 소스코드

```
if ($time3 == $time4) {
echo "
<p><a href='https://[redacted].co.kr/zboard/view.php?id=noti
&desc=asc&no=$no' target='_top'><font size=1 color='silve
::new::-></a></p> ";
} else {
echo "<p><a href='https://[redacted].co.kr/zboard/view.php?i
eadnum&desc=asc&no=$no' target='_top'><font size=1 color=
}
```

〈그림 6-2〉 https 프로토콜을 호출하기 위한 HTML 소스코드

② 리다이렉션(Redirection) 설정

앞서 설명을 하였듯이, 암호화 통신을 위해서는 https 프로토콜을 직접 호출을 해줘야 합니다. 하지만, 웹페이지에 접속하는 사용자들은 일일이 https 프로토콜을 붙여서 입력을 하지 않습니다. 대부분의 경우가 www.test.co.kr 또는 test.co.kr 도메인을 웹 브라우저의 주소창에 입력하고 접속하는 경우가 대부분일 것입니다. 이 때 웹 브라우저에 그냥 도메인 주소만 입력하면, 웹 브라우저는 해당 도메인 앞에 http://가 붙은 것으로 판단하고 평문 통신을 하도록 합니다.

평문 통신을 하는 경우라면 문제가 없지만, 암호화 통신을 해야 할 경우에는 https://를 직접 붙여서 입력해야 하므로 여간 불편해 하지 않습니다. 리다이렉션은 현재 접속한 도메인이나 혹은 웹페이지를 강제로 다른 주소나 다른 페이지로 변경해 줌으로써 사용자들의 불편함을 감소시켜주고 자연스럽게 암호화통신을 할 수 있도록 해주는 기능입니다.

〈그림 6-3〉은 Apache 서버에서 Redirect 지시자를 써서 http://test.co.kr 또는 http://www.test.co.kr로 들어온 사용자를 강제로 https:// www.test.co.kr로 리다이렉션시켜서 암호화 통신하는 예입니다.

```
<VirtualHost test.co.kr:80>
        ServerAdmin zmnkh@test.co.kr
        ServerName test.co.kr
        ServerAlias www.test.co.kr
        DocumentRoot /home/manpage
        CustomLog logs/test.co.kr-access_log common
        Redirect / https://www.test.co.kr/
</VirtualHost>
```

〈그림 6-3〉 Apache 서버에서의 Redirection

또 다른 방법으로는 OS나 Web Programming 언어의 종류에 상관없이 모두 공통적으로 사용하는 HTML tag를 이용한 방법으로써, 어떤 경우에서나 적용이 가능하기 때문에 가장 많이 이용되고 있습니다.

〈그림 6-4〉는 웹페이지의 index.html에 한 줄의 소스코드를 추가함으로써 http://URL로 접속하는 사용자들을 강제로 https://URL로 리다이렉션하는 예입니다.

```
<meta http-equiv='refresh' content='0; url=https://[redacted].co.kr/index.html' target='_top'>
```

〈그림 6-4〉 HTML Tag를 이용한 Redirection

위와 같이 Meta 태그를 이용하는 경우, 1초 정도 깜빡하는 현상이 나타나기 때문에 종종 Javascript를 이용하기도 합니다.

Meta tag를 이용한 html Redirection 방법과 동일하게, 사용자들이 익숙하게 접속하는 http://www.test.com의 index 페이지에 삽입해 두면, 사용자들이 불편하게 https://라는

프로토콜을 특별히 지정해 주지 않아도, 보안을 위해서 암호화 통신이 적용된 https://www.test.com으로 리다이렉션해주게 됩니다.

```
<script>
var url = "https://www.test.com";
window.location.replace(url);
</script>
```

〈그림 6-5〉 Javascript를 이용한 Redirection

1.2 페이지별 암호화하기

페이지별 암호화는 현재 위치하고 있는 페이지에서 다른 페이지로 이동할 때, 보안을 위해서 암호화된 전송을 할 것인지 아니면 평문 전송할 것인지를 선택하여 암호화하는 것을 말합니다.

부분적인 페이지 암호화를 사용하는 이유는 암호화 적용이 필요없는 부분까지 암호화를 하여 서버의 부하를 증가시키는 것을 최대한 줄일 수 있기 때문입니다.

다음 〈그림 6-6〉은 사이트의 메뉴 부분 예입니다. 이 중 '서버관련 강좌 & TIP' 메뉴를 클릭하여 이동을 하면 https가 호출되어 서버와 클라이언트간의 통신이 암호화되어 전송되고, 'Q&A' 메뉴를 클릭하여 이동하면 http가 호출되어 서버와 클라이언트간의 통신이 평문으로 이루어지게 하는 방법을 알아보겠습니다.

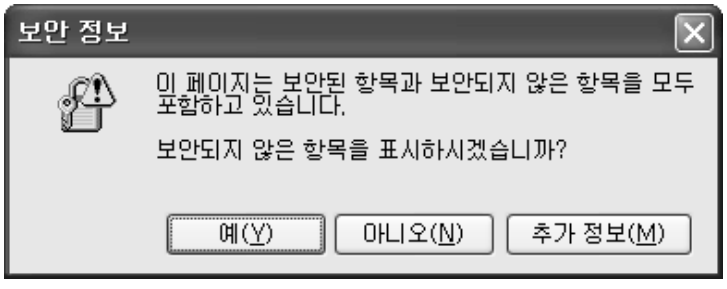
〈그림 6-6〉 페이지별 암호화 대상 메뉴

〈그림 6-7〉은 위 메뉴 부분의 소스코드입니다. 밑줄 부분 중 첫 번째 밑줄에 해당하는 부분이 현재 위치에서 메뉴를 클릭하여 이동할 때 암호화 전송을 하도록 하게끔 설정된 것이고, 두 번째 밑줄은 현재 위치에서 메뉴를 클릭하여 이동할 때 평문 전송을 하도록 설정된 것입니다.

```
<map name="ImageMap1">
<area shape="rect" coords="193, 74, 249, 90" href="onlinebook/online.ht
m" target="main">
<area shape="rect" coords="267, 75, 401, 89" href="https://[redacted].co.k
r/zboard/zboard.php?id=lecture" target="_top">
<area shape="rect" coords="423, 73, 479, 89" href="https://[redacted].co.k
r/zboard/zboard.php?id=problem" target="_top">
<area shape="rect" coords="497, 73, 537, 89" href="http://[redacted].co.kr
/zboard/zboard.php?id=qna" target="_top">
<area shape="rect" coords="555, 73, 609, 89" href="http://[redacted].co.kr
/zboard/zboard.php?id=down" target="_top">
<area shape="rect" coords="679, 5, 717, 23" href="index.html" target="_
top">
```

〈그림 6-7〉 페이지별 암호화 대상 메뉴의 소스코드

이렇게 페이지별로 암호화가 적용된 사이트를 방문해보면, 〈그림 6-8〉과 같은 경고창을 만나게 되는 경우가 있습니다.

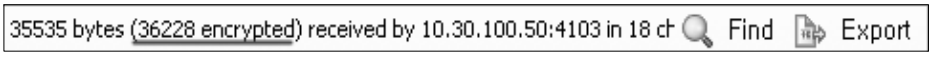


〈그림 6-8〉 SSL이 적용된 페이지의 경고창

이 경고창이 뜨는 것은 암호화 통신을 유지하기 위해서는 웹페이지내의 모든 URL의 호출이 https://로 이루어져야 하나, http:// 즉 평문 통신을 위한 웹페이지 URL이 포함되어 있다는 것을 의미합니다.

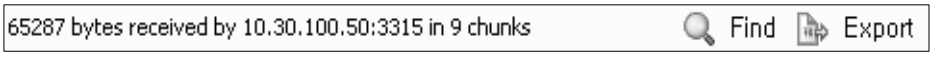
이런 경고창이 발생하는 웹페이지 속성을 보면 〈그림 6-9〉처럼 '암호화 안됨' 이라고 해서 마치 암호화가 되지 않은 평문 상태로 데이터가 전송되어지는 것처럼 생각되지만 웹페이지간 전송되는 데이터를 볼 수 있는 third-parth 툴을 이용해서 확인해 보면, 〈그림 6-10〉와 같이 암호화 통신이 이루어지고 있다는 것을 알 수 있습니다.

〈그림 6-9〉 http 평문 통신 주소가 호출되는 웹페이지의 속성



〈그림 6-10〉 https를 통한 암호화 통신

〈그림 6-11〉은 〈그림 6-10〉의 결과와 비교하기 위해서 암호화 되지 않은 평문 통신(http) 상태를 나타낸 그림입니다.



〈그림 6-11〉 http를 통한 평문 통신

하지만 〈그림 6-8〉과 같이 경고창이 발생하게 되면, 상세한 내용을 모르고 웹사이트에 접속하는 사용자들에게 보안이 되고 있지 않다는 불신을 줄 수도 있고, 또한 계속적인 경고창으

로 인해서 불편해 할 수 있으므로 가급적 발생하지 않도록 웹 페이지 내의 모든 URL을 https://로 바꿔주는 것이 좋습니다.

만일 절대경로로 호출하는 것이 아니라, 상대경로로 호출하는 것이라면 소스를 변경하지 않아도 됩니다.

※ 참고 : 절대경로와 상대경로

절대경로 호출과 상대경로 호출이란 무엇인가?
절대경로란 내가 열어보고자 혹은 내가 가고자 하는 웹페이지의 경로를 전체적으로 기술하는 것이고, 상대경로란 내가 현재 있는 위치를 기준으로 내가 열어보고자 혹은 내가 가고자 하는 웹페이지의 경로를 기술하는 것을 말한다.
아래 그림에서 첫 번째 밑줄 그은 부분이 상대경로로 호출하는 경우이고, 두 번째 밑줄 그은 부분이 절대경로로 호출하는 경우이다.
첫 번째의 경우에는 https 암호화 통신을 하더라도 소스코드 수정이 필요없는 부분이고,
두 번째의 경우에는 https 암호화 통신을 할 경우 호출 URL을 http에서 https로 바꿔줘야 한다.
만일 바꿔주지 않을 경우에는 〈그림 6-8〉과 같이 경고창이 뜨게 된다.

1.3 프레임별 암호화하기

SSL을 이용한 보안포트(443)를 웹페이지에 적용하는 방법을 앞서 소개하였습니다. 단순히 http를 https로만 바꾸어주면 보안포트를 이용해서 암호화 통신을 할 수 있었습니다.

하지만, 프레임이 삽입된 웹페이지의 경우에는 약간 적용하는 방식이 다르기 때문에 소개하

고자 합니다. 프레임이 적용된 페이지를 이용하면 암호화된 페이지와 비 암호화된 페이지를 각각 적용시킬 수 있습니다.

적용 시나리오는 〈그림 6-12〉과 같이 웹페이지(index.html)에 프레임으로 두 개의 페이지 topmenu.htm과 main.htm을 불러오는 소스코드가 있을 때 소스코드의 URL을 〈그림 6-13〉와 〈그림 6-14〉처럼 변경하고 웹 브라우저에서 http와 https로 각각 호출했을 때의 결과를 살펴보고자 합니다.

```
<html>

<head>
<meta http-equiv="content-type" content="text/html; charset=euc-kr">
<title>SSL Frame Test</title>
</head>
<frameset rows="100, 1*" border="1">
   <frame src="http://lab.[illegible].co.kr/test_ssl/topmenu.htm" scrol
ling="yes" name="top" namo_target_frame="main">
    <frame src="http://lab.[illegible].co.kr/test_ssl/main.htm" scrolli
ng="yes" name="main">
    <noframes>
    <body bgcolor="white" text="black" link="blue" vlink="purple" ali
nk="red">
    <p>SSL Frame Test의 페이지 입니다. <br> 이페이지를 보기 위해서는
       프레임을 볼수 있는 웹 브라우저가 필요합니다.</p>
    </body>
    </noframes>
</frameset>

</html>
```

〈그림 6-12〉 프레임이 포함된 웹페이지

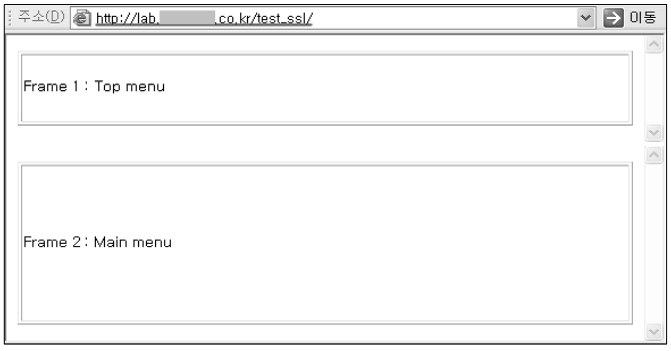
```
<html>

<head>
<meta http-equiv="content-type" content="text/html; charset=euc-kr">
<title>SSL Frame Test</title>
</head>
<frameset rows="100, 1*" border="1">
   <frame src="https://lab.[redacted].co.kr/test_ssl/topmenu.htm" scro
lling="yes" name="top" namo_target_frame="main">
    <frame src="http://lab.[redacted].co.kr/test_ssl/main.htm" scrolli
ng="yes" name="main">
    <noframes>
    <body bgcolor="white" text="black" link="blue" vlink="purple" ali
nk="red">
    <p>SSL Frame Test의 페이지 입니다. <br> 이페이지를 보기 위해서는
       프레임을 볼수 있는 웹 브라우저가 필요합니다.</p>
    </body>
    </noframes>
</frameset>

</html>
```

〈그림 6-13〉 topmenu.htm을 https로 호출하기

〈그림 6-14〉 topmenu.htm과 main.htm을 https로 호출하기

① 비암호화 통신(http)를 이용해서 호출하기

〈그림 6-15〉는 topmenu.htm과 main.htm을 모두 〈그림 6-12〉의 소스를 이용해서 호출한 경우입니다. 이 경우에는 모든 정보가 암호화되지 않고 〈그림 6-16〉과 같이 그대로 노출됩니다.



〈그림 6-15〉 비암호화된 페이지 호출하기

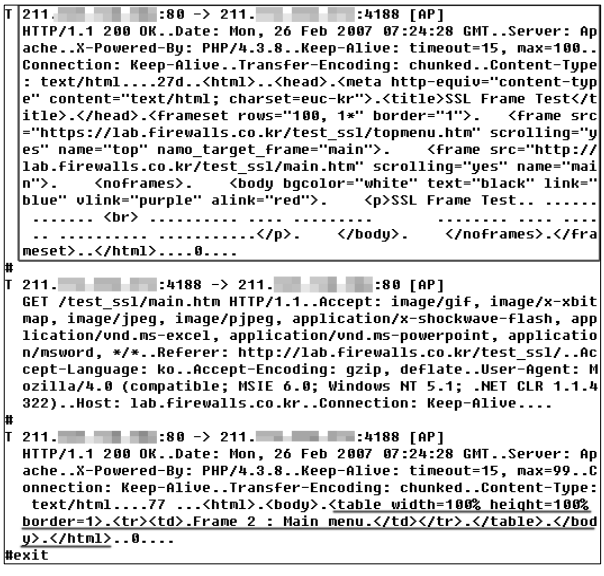
```
interface: namifw (211.[redacted]/255.255.254.0)
filter: ip and ( port 80 )
####
T 211.[redacted]:4185 -> 211.[redacted]:80 [AP]
  GET /test_ssl/ HTTP/1.1..Accept: */*..Accept-Language: ko..Accep
  t-Encoding: gzip, deflate..User-Agent: Mozilla/4.0 (compatible;
  MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)..Host: [redacted]
  [redacted]..Connection: Keep-Alive....
#
T 211.[redacted]:80 -> 211.[redacted]:4185 [AP]
  HTTP/1.1 200 OK..Date: Mon, 26 Feb 2007 07:22:59 GMT..Server: Ap
  ache..X-Powered-By: PHP/4.3.8..Keep-Alive: timeout=15, max=98..C
  onnection: Keep-Alive..Transfer-Encoding: chunked..Content-Type:
   text/html....27c..<html>..<head>.<meta http-equiv="content-type
  " content="text/html; charset=euc-kr">.<title>SSL Frame Test</ti
  tle>.</head>.<frameset rows="100, 1*" border="1">.   <frame src=
  "http://lab.firewalls.co.kr/test_ssl/topmenu.htm" scrolling="yes
  " name="top" namo_target_frame="main">.    <frame src="http://la
  b.firewalls.co.kr/test_ssl/main.htm" scrolling="yes" name="main"
  >.    <noframes>.    <body bgcolor="white" text="black" link="bl
  ue" vlink="purple" alink="red">.    <p>SSL Frame Test.. ..... .
  . ......... ..........</p>.    </body>.    </noframes>.</frame
  set>..</html>....0....
#
T 211.[redacted]:4186 -> 211.[redacted]:80 [AP]
  GET /test_ssl/topmenu.htm HTTP/1.1..Accept: image/gif, image/x-x
  bitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
  application/vnd.ms-excel, application/vnd.ms-powerpoint, applica
  tion/msword, */*..Referer: http://lab.firewalls.co.kr/test_ssl/.
  .Accept-Language: ko..Accept-Encoding: gzip, deflate..User-Agent
  : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.
  1.4322)..Host: [redacted]..Connection: Keep-Alive....
#
T 211.[redacted]:80 -> 211.[redacted]:4186 [AP]
  HTTP/1.1 200 OK..Date: Mon, 26 Feb 2007 07:22:59 GMT..Server: Ap
  ache..X-Powered-By: PHP/4.3.8..Keep-Alive: timeout=15, max=99..C
```

〈그림 6-16〉 HTTP 호출시 80 포트 모니터링 결과

다음으로는 〈그림 6-13〉의 소스코드를 적용하여 topmenu.htm만을 https로 호출을 하는 경우입니다.

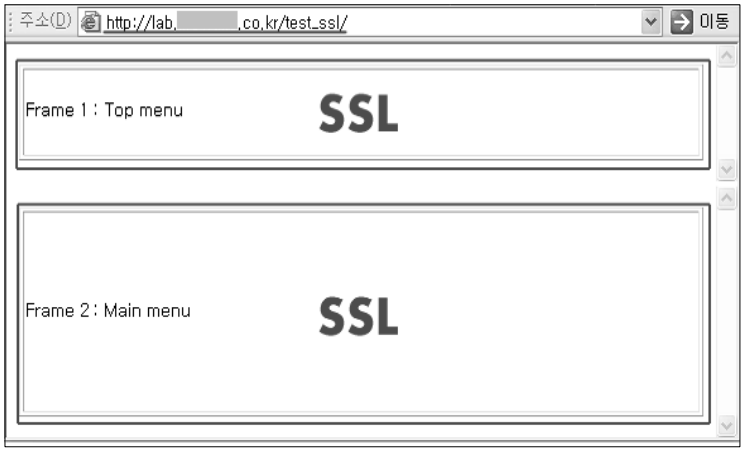
〈그림 6-17〉 topmenu.htm만 암호화하여 호출하기

프레임을 이용해서 호출하는 경우에는 아래 〈그림 6-18〉과 같이 암호화되지 않는 index.html (네모박스)의 내용과 main.htm의 내용만이 80 포트로 텍스트 전송되는 것을 확인할 수 있습니다. topmenu.htm의 내용은 암호화 전송되기 때문에 평문 전송되는 80 포트에서는 내용을 알 수 없습니다.



〈그림 6-18〉 topmenu.htm의 내용만 암호화된 모니터링 결과

마지막으로 〈그림 6-14〉와 같이, 호출하는 index.html을 제외하고 모든 프레임내의 호출페이지를 https를 통해서 호출하게 될 경우에는 아래와 같이 index.html의 내용만 평문으로 전송이 되고, 나머지 topmenu.htm과 main.htm은 암호화 되어서 전송됩니다.



〈그림 6-19〉 topmenu.htm과 main.htm을 https로 호출하기

```
interface: namifw (211.[redacted]/255.255.254.0)
filter: ip and ( port 80 )
########
T 211.[redacted]:4190 -> 211.[redacted]:80 [AP]
  GET /test_ssl/ HTTP/1.1..Accept: */*..Accept-Language: ko..Accep
  t-Encoding: gzip, deflate..User-Agent: Mozilla/4.0 (compatible;
  MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)..Host: lab.firewall
  s.co.kr..Connection: Keep-Alive....
##
T 211.[redacted]:80 -> 211.[redacted]:4190 [AP]
  HTTP/1.1 200 OK..Date: Mon, 26 Feb 2007 07:26:05 GMT..Server: Ap
  ache..X-Powered-By: PHP/4.3.8..Keep-Alive: timeout=15, max=100..
  Connection: Keep-Alive..Transfer-Encoding: chunked..Content-Type
  : text/html....27e..<html>..<head>.<meta http-equiv="content-typ
  e" content="text/html; charset=euc-kr">.<title>SSL Frame Test</t
  itle>.</head>.<frameset rows="100, 1*" border="1">.   <frame src
  ="https://lab.firewalls.co.kr/test_ssl/topmenu.htm" scrolling="y
  es" name="top" namo_target_frame="main">.    <frame src="https:/
  /lab.firewalls.co.kr/test_ssl/main.htm" scrolling="yes" name="ma
  in">.    <noframes>.    <body bgcolor="white" text="black" link=
  "blue" vlink="purple" alink="red">.    <p>SSL Frame Test.. .....
  . ....... <br> .......... .... .........        ........ .... ...
  . .. .......... ..........</p>.    </body>.    </noframes>.</fr
  ameset>..</html>....0....
####exit
```

〈그림 6-20〉 index.html의 내용만 모니터링된 결과

② 암호화 통신(https)을 이용해서 호출하기

앞에서와 같은 절차를 이용해서 https를 이용해서 〈그림 6-11〉과 같이 호출을 하게 되면, 프레임을 포함하고 있는 index.html은 URL을 https로 호출을 하게 되므로, 항상 암호화가 되어지고, topmenu.htm과 main.htm은 〈그림 6-12〉,〈그림 6-13〉,〈그림 6-14〉와 같이 암호화 적용 여부에 따라서, 평문 통신 또는 암호화 통신이 이루어집니다.

〈그림 6-21〉 https를 이용한 호출

```
interface: namifw (211.[redacted]254.0)
filter: ip and ( port 80 )
#####
T 211.[redacted]:4183 -> 211.[redacted]:80 [AP]
  GET /test_ssl/topmenu.htm HTTP/1.1..Accept: image/gif, image/x-x
  bitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
  application/vnd.ms-excel, application/vnd.ms-powerpoint, applica
  tion/msword, */*..Accept-Language: ko..Accept-Encoding: gzip, de
  flate..User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
   5.1; .NET CLR 1.1.4322)..Host: [redacted]..Connection:
   Keep-Alive....
##
T 211.[redacted]:80 -> 211.[redacted]:4183 [AP]
  HTTP/1.1 200 OK..Date: Mon, 26 Feb 2007 07:21:34 GMT..Server: Ap
  ache..X-Powered-By: PHP/4.3.8..Keep-Alive: timeout=15, max=100..
  Connection: Keep-Alive..Transfer-Encoding: chunked..Content-Type
  : text/html....76 ..<html>.<body>.<table width=100% height=100%
  border=1>.<tr><td>.Frame 1 : Top menu.</td></tr>.</table>.</body
  >.</html>...0....
####
T 211.[redacted]:4184 -> 211.[redacted]:80 [AP]
  GET /test_ssl/main.htm HTTP/1.1..Accept: image/gif, image/x-xbit
  map, image/jpeg, image/pjpeg, application/x-shockwave-flash, app
  lication/vnd.ms-excel, application/vnd.ms-powerpoint, applicatio
  n/msword, */*..Accept-Language: ko..Accept-Encoding: gzip, defla
  te..User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.
  1; .NET CLR 1.1.4322)..Host: [redacted]..Connection: Ke
  ep-Alive....
##
T 211.[redacted]:80 -> 211.[redacted]:4184 [AP]
  HTTP/1.1 200 OK..Date: Mon, 26 Feb 2007 07:21:35 GMT..Server: Ap
  ache..X-Powered-By: PHP/4.3.8..Keep-Alive: timeout=15, max=100..
  Connection: Keep-Alive..Transfer-Encoding: chunked..Content-Type
  : text/html....77 ...<html>.<body>.<table width=100% height=100%
   border=1>.<tr><td>.Frame 2 : Main menu.</td></tr>.</table>.</bo
  dy>.</html>..0....
##exit
```

〈그림 6-22〉 https 호출시 80 포트 모니터링 결과

〈그림 6-22〉를 보면, 웹 브라우저에서 https를 통해서 호출한 index.html의 내용은 암호화되어 통신이 이루어지기 때문에 80 포트를 모니터링 하였을 경우에 그 내용이 보이지 않지만, index.html 안에 있는 프레임을 통해서 http로 호출한 topmenu.htm과 main.htm은 https 통신을 통해서 index.html을 호출했지만, 평문으로 통신이 되는 것을 확인할 수 있습니다.

〈그림 6-13〉, 〈그림 6-14〉의 소스를 같은 방법으로 테스트 해보면, http로 호출된 웹페이지는 암호화 통신이 이루어지지 않고 있는 것을 알 수 있습니다.

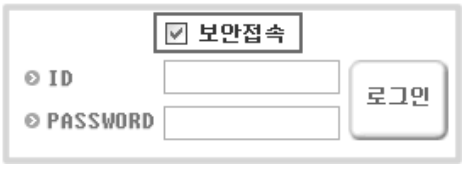
이와 같이 프레임을 이용하면, 필요에 따라서 한 페이지에서 암호화가 제공되는 부분과 암호화가 제공되지 않는 부분이 공존할 수 있도록 구성할 수 있지만, 앞서서도 이미 언급했듯이 아무리 웹 브라우저에서 https를 이용해서 호출을 했어도 프레임으로 불러오는 페이지가 http 주소를 가지고 있을 경우에는 암호화가 되지 않고 정보의 노출이 발생할 수 있으므로, 프레임이 사용되는 페이지를 암호화를 위해서 https로 호출하고자 할 때에는 꼭 확인을 해보시기 바랍니다.

1.4 체크박스를 이용한 선별적 암호화하기

웹페이지 전체를 암호화하지 않고 선별적으로 암호화하는 경우, 정보입력시 보안접속을 체크함으로써 프로토콜을 호출하는 방법이 있습니다. 그러나 http 통신과 https 통신이 혼용되는 경우, 통신과정상의 취약점으로 인해 해킹의 공격대상이 될 수 있으므로 보안접속을 기본으로 사용할 것을 권고합니다. 또한 보안접속을 통하여 암호화하는 것을 이용자에게 알리고자 하는 목적으로 사용한다면 체크박스 해제를 선택하지 못하도록 조치할 것을 권고합니다. 다음은 로그인 박스에서 선별적으로 암호화된 통신을 하기 위한 HTML 소스코드의 예입니다.

보안접속 체크박스 적용 전

보안접속 체크박스 적용 후



*** 소스 코드**

```
<script language="JavaScript">
< !--
function checkLoginForm1() {
var f = document.forms["LoginForm1"];
//아이디 입력 검사
if( f.memberID.value=="" ){
alert("아이디를 입력하세요");
f.memberID.focus();
return false;
}
//비밀번호 입력 검사
if( f.memberPW.value=="" ){
alert("비밀번호를 입력하세요");
f.memberPW.focus();
return false;
}
//액션
f.action =
"http://login.your-domain.com/login1.html;
```

*** 소스 코드**

```
<script language="JavaScript">
<!--
function checkLoginForm2() {
var f = document.forms["LoginForm2"];
//아이디 입력 검사
if( f.memberID.value=="" ){
alert("아이디를 입력하세요");
f.memberID.focus();
return false;
}
//비밀번호 입력 검사
if( f.memberPW.value=="" ){
alert("비밀번호를 입력하세요");
f.memberPW.focus();
return false;
}
//액션
if ( f.SSL_Login.checked ) {
//보안접속 체크 판별
//보안접속을 체크했을 때의 액션
f.action =
"https://login.your-domain.com/login1.html
";
} else {
//보안접속을 체크하지 않았을 때의 액션
```

```
return true;
}
//-->
</ /script>
<  form  name="LoginForm1"  method="POST"
onSubmit="return checkLoginForm1();">
< table>
<tr>
<td>아이디</td>
<td><input type="text" name="memberID"></td>
<td> </td>

</tr>
<tr>
<td>비밀번호</td>
<td><input                    type="password"
name="memberPW"></td>
<td><input type="submit" name="Submit" value=" 로
그인 "></td>
</tr>
</ /table>
</ /form>
```

```
f.action                                    =
"http://login.your-domain.com/login1.html"
;
}
return true;
}
//-->
</script>
<form name="LoginForm2" method="POST"
onSubmit="return checkLoginForm2();">
<table>
<tr>
<td>아이디</td>
<td><input                    type="text"
name="memberID"></td>
<td><input  type="checkbox"  value=1
checkedname="SSL_Login" >보안접속</td>
</tr>
<tr>
<td>비밀번호</td>
<td><input                    type="password"
name="memberPW"></td>
<td><input  type="submit"  name="Submit"
value=" 로그인 "></td>
</tr>
</table>
</form>

※ SSL을 이용한 암호화된 폼 전송을 하려면,
  action URL에서 'http' 대신 'https'를
  적어 주면 됩니다.
```

〈그림 6-23〉 로그인시 보안접속 체크박스를 이용하기 위한 HTML 소스코드

2. 보안서버 적용 확인하기

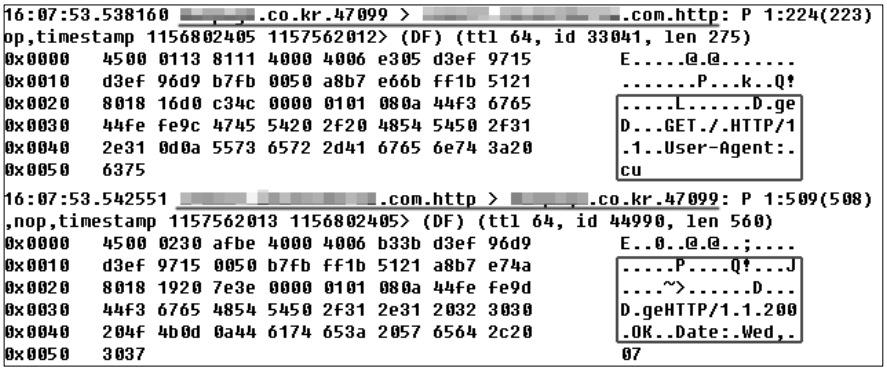
2.1 보안서버 적용 확인 방법

앞에서 암호화 통신을 위해서 보안 프로토콜을 적용하는 방법을 알아보았습니다. 본 절에서는 앞서 적용한 보안 프로토콜이 제대로 적용이 되었는지 확인하는 방법에 대해서 알아보겠습니다.

① 패킷 캡쳐를 통한 확인

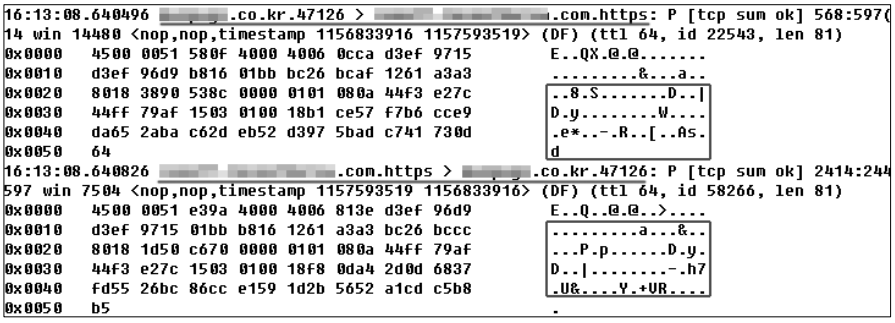
일단 제대로 암호화가 되어지고 있는지 패킷을 캡쳐하여 확인하는 방법입니다.

〈그림 6-24〉는 일반적인 http를 통한 평문 통신의 경우를 캡쳐한 것입니다. 네모상자를 확인하면 header의 내용이 평문으로 보이는 것을 확인할 수 있습니다.



〈그림 6-24〉 평문 통신 패킷 확인 결과

〈그림 6-25〉를 보면 https에 접속 요청을 한 것을 확인할 수가 있으며, 네모상자를 확인하면 동일 구간이지만 header의 내용이 암호화 되어 내용을 알아볼 수 없게 되었음을 알 수 있습니다. 즉, 암호화 통신이 정상적으로 이루어진다는 것을 의미합니다.



〈그림 6-25〉 암호화된 통신 패킷 확인 결과

② 웹페이지에서 확인

직접 패킷을 캡쳐해서 확인하는 방법 외에도, 웹페이지에서 간단히 암호화가 되어지고 있는지를 확인하는 방법이 있습니다.

SSL이 적용된 웹사이트에 https 프로토콜로 접속을 했을 경우에, 〈그림 6-26〉과 같이 브라우저 하단에 자물쇠 모양의 표시가 나타나는 것을 확인할 수 있을 것입니다. 현재 사이트와의 통신이 암호화되어 진행되고 있다는 것을 보여주는 것입니다. 웹사이트 구성방법에 따라 자물쇠 이미지가 보이지 않을 수 있으며, 구축 방법에 따라 모양은 다르게 나타날 수 있습니다.

〈그림 6-26〉 암호화 통신이 이루어지고 있음을 보여주는 자물쇠 이미지

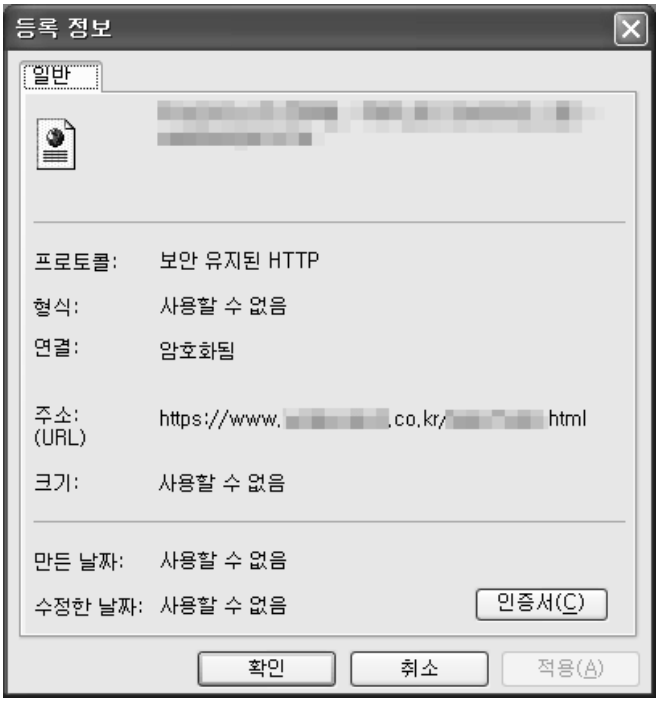
③ 호출시 포트번호 확인

https를 이용하여 접속하시면 일반적으로 443번 포트로 연결이 되어 SSL 인증서버를 통한 통신을 하게 됩니다.

서버에 여러 개의 인증서버를 설치할 경우 상황에 따라 443번 포트가 아닌 여러 가지 포트를 이용해서 접속을 하는 상황이 발생할 수 있습니다. 이런 경우 설치를 대행하는 업체나 호스팅업체에서 임의의 포트를 지정하거나 사용할 포트를 지정받아 SSL 인증서를 설치한 뒤 작업완료 통보와 함께 사용된 포트번호를 알려주게 됩니다.

④ 웹페이지 속성보기를 통한 확인

암호화를 적용한 웹페이지가 정상적으로 암호화되고 있는지는 웹페이지에서 오른쪽 마우스를 클릭하고 속성을 선택한 후 웹페이지 등록 정보를 통하여 확인할 수가 있습니다. 현재 페이지가 보안이 되고 있다면 〈그림 6-27〉와 같은 웹페이지 속성을 확인할 수 있습니다.



〈그림 6-27〉 보안이 적용된 웹페이지 등록정보

2.2 인증서의 암호화 상태 확인 방법

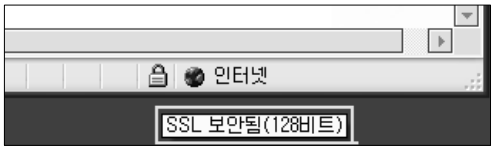
접속한 웹페이지가 암호화되고 있다는 것을 확인한 후, 다음과 같은 단계를 걸쳐서 설치된 인증서의 암호화 상태를 확인할 수 있습니다.

① 웹페이지 접속

인증서가 설치된 웹페이지에 접속하십시오.

〈그림 6-28〉 보안이 적용된 웹페이지 접속

브라우저 하단에 있는 자물쇠 아이콘에 마우스를 올리면 암호화 방식에 대한 확인이 가능합니다.



〈그림 6-29〉 자물쇠 이미지를 통한 암호화 방식 확인

② 인증서 기본 정보 확인

설치된 인증서의 정보를 확인하려면 자물쇠 아이콘을 더블클릭하거나 브라우저에서 마우스 오른쪽 버튼을 클릭하시면 등록정보 창이 열리게 됩니다.

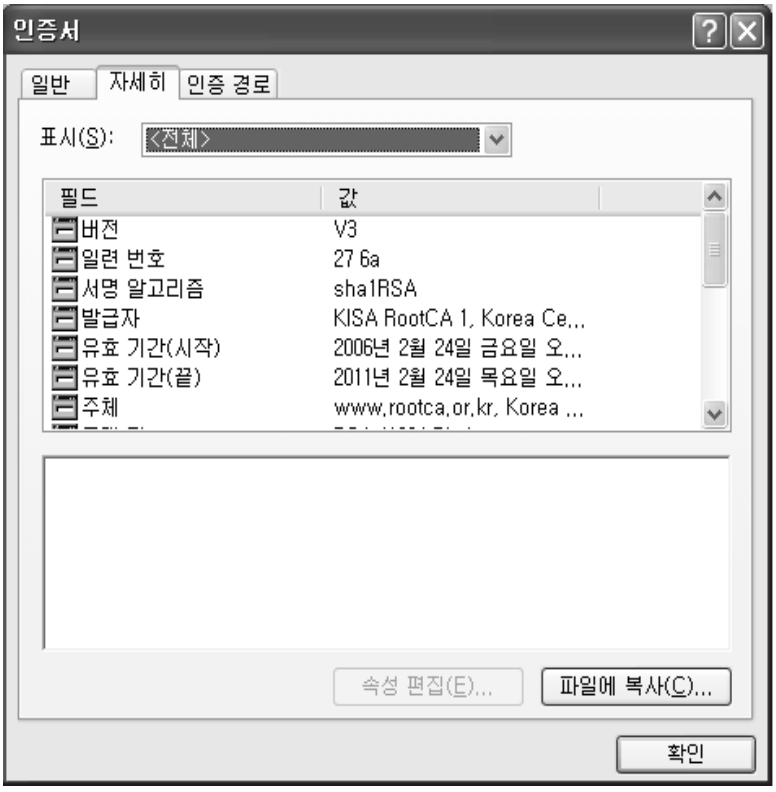
등록정보 창 하단에 인증서 버튼을 선택하여 인증서 창을 열면 설치된 인증서에 대한 정보를 확인할 수 있습니다.

〈그림 6-30〉 보안이 적용된 웹페이지의 등록정보 중 인증서 버튼

〈그림 6-31〉 보안이 적용된 웹페이지의 인증서 기본 정보 확인

③ 인증서 상세 정보 확인

발급 대상, 발급자 정보, 발급된 인증서의 유효기간 등 기본적인 인증서 정보를 확인하실 수 있고, 보다 자세한 인증서 관련 정보를 확인하고자 한다면 '자세히' 탭을 선택하면 됩니다.

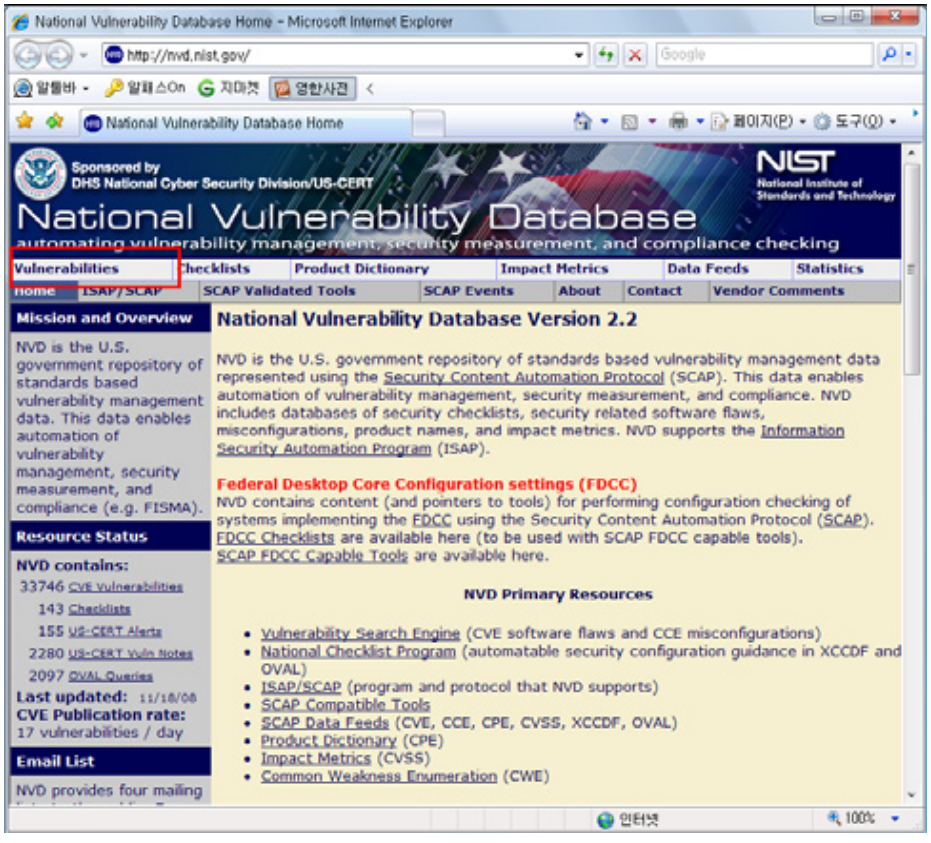


〈그림 6-32〉 보안이 적용된 웹페이지의 인증서 상세정보 확인

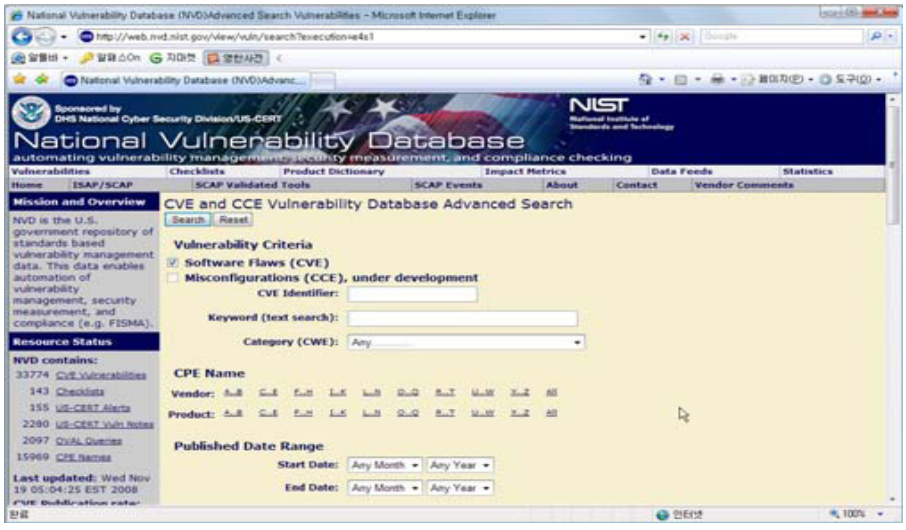
3. 보안서버의 보안 취약성 해결 방안

3.1 보안서버의 알려진 취약성 확인 방법

① http://nvd.nist.gov 는 운영체제, 보안제품 등 각 소프트웨어의 취약성을 데이터베이스 형식으로 발표하는 사이트입니다.

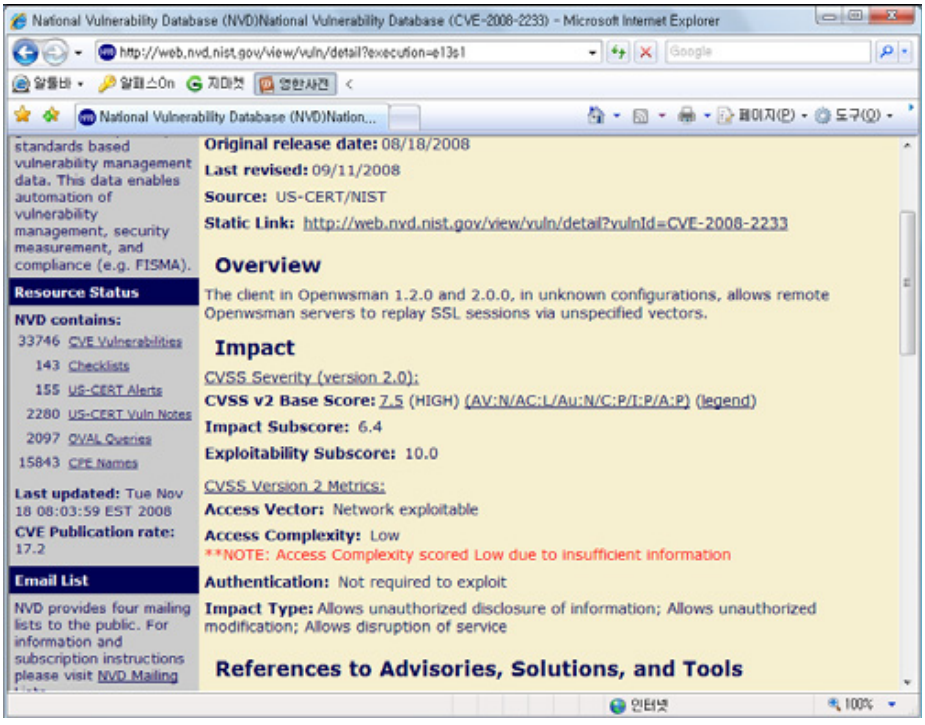


② 서버 관리자는 Advanced Search를 통하여 취약성 주제, 키워드, 보고 날짜, 해결 날짜 등과 같은 정보로 알려진 취약성들을 검색할 수 있습니다.



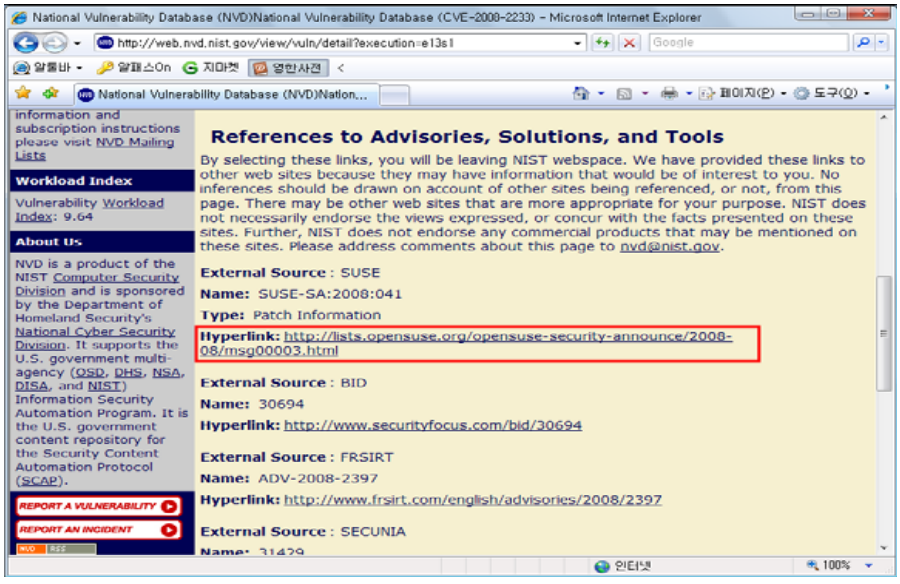
③ Advanced Search의 검색 결과는 다음 그림과 같이 보고된 날짜 별로 정렬되어 나타납니다.

④ 검색 결과에서 열람하고 싶은 취약성 링크를 클릭하면 해당 취약성의 개요와 보고 날짜 및 해결 날짜, 위험도, 해결 방법 등을 볼 수 있습니다.

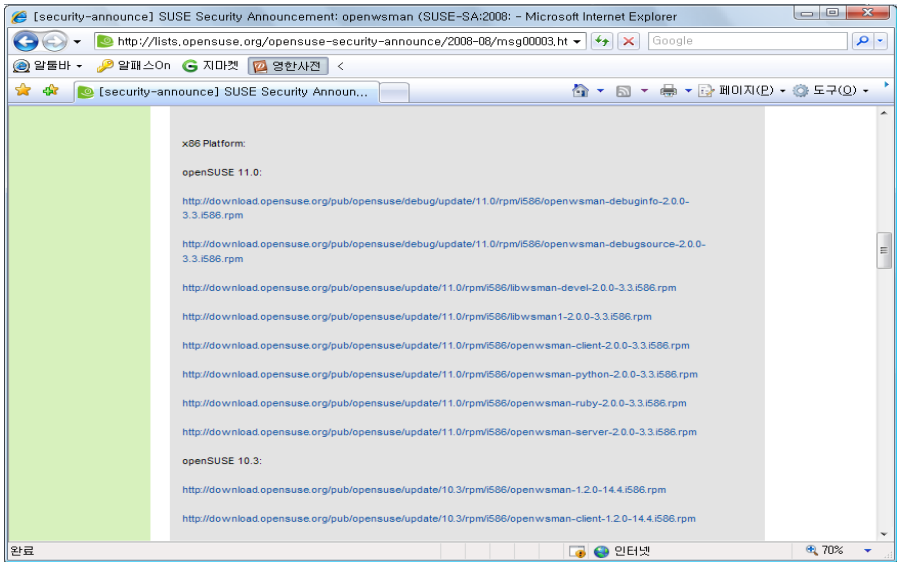


3.2 보안서버의 알려진 취약성 해결 방법

http://nvd.nist.gov에 보고된 취약성을 해결하기 위해서는 Reference to Advisories, Solution, and Tools 부분을 참고하면 됩니다. 이 부분에는 해당 취약성에 관련된 제품 개발 회사 및 보안 관련 사이트들이 링크되어 있습니다. 아래와 같이 링크를 통하여 관련 제품 개발 회사 사이트를 방문하면 해당 취약성에 대한 내용과 해결 방안 등을 볼 수 있습니다.



각 제품 개발 회사 사이트에서는 같이 다음과 같이 보안 패치 등을 제공하고 있으므로 다운로드 받아 보안서버에 적용하면 됩니다.



Ⅶ. 보안서버 관련 FAQ

1. 제도 관련
2. 구축범위 관련
3. 호스팅 관련
4. 적용 관련
5. 기타

Ⅶ. 보안서버 관련 FAQ

1. 제도 관련

1) 한국인터넷진흥원(KISA)은 어떤 기관인가요?

방송통신위원회 산하기관으로 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의해 인터넷상의 개인정보보호 업무 등을 맡고 있으며, 웹사이트 회원가입 등을 통한 개인정보 수집에 따른 실태조사 및 보호조치가 미흡한 사업자에 대한 개선권고 업무 등을 담당하고 있습니다.

2) 보안서버는 무엇이고, 구축하지 않으면 어떻게 되나요?

보안서버란, 인터넷상에서 개인정보를 암호화하여 송수신하는 기능이 구축된 웹사이트를 말하며, 하드웨어를 설치하는 것이 아니라 이미 사용하고 있는 웹서버에 인증서나 암호화 소프트웨어를 설치하여 암호통신이 가능한 것입니다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의해 개인정보를 수집하는 웹사이트에 보안서버가 구축되지 않은 경우 1천만원 이하의 벌금 등 행정조치가 있을 수 있습니다.

3) 보안서버 구축이 의무인가요? 관련 법조항이 뭔가요?

개인정보를 취급하는 영리목적의 사업자는 필수적으로 보안서버를 구축해야 합니다.

관련 법률은 이미 2005년부터 시행 중이며 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제28조(개인정보의 보호조치)와 제76조(벌금) 등에 명시되어 있습니다. 실제 법조항은 본 가이드의 Ⅰ장 내용 중 보안서버 관련 규정이나 보안서버 안내 홈페이지(www.kisa.or.kr → 보안서버 안내)를 참조하시고, 전체 법조항이 필요하신 경우는 방송통신위원회 또는 법제처 홈페이지를 참조하시기 바랍니다.

4) 정확히 언제까지 구축해야 하는 건가요?

관련법규는 2005년부터 이미 시행중이며, 매년 모니터링을 통한 사이트 점검 결과에 따라 시정명령과 과태료 부과 등 행정조치가 있을 예정이기 때문에 빠른 시일내에 구축을 완료하셔야 합니다. 구축 계획 일정과 구축결과에 대해 사무국 (http://guide.kisa.or.kr)으로 알려주시기 바랍니다.

5) 지금까지는 규제하지 않다가 왜 이제 와서 이러는 겁니까?

'05년 법개정 후 사업자들의 자율 구축을 유도하였으나 구축이 의무조항이라는 사실을 많이 인지하지 못해서 활성화가 되지 못하고 있었습니다. 금년에는 직접 사업자들을 대상으로 홍보 및 계도를 실시한 후 본격적으로 행정조치를 시행할 예정입니다.

6) 이미 구축을 완료했는데, 확인도 안하고 계도 메일을 보내는 건 정부기관의 행정처리가 너무 미흡한 것 아닙니까?

수신메일정보는 웹사이트를 통해 확인 가능한 주소로 일괄발송되었으며, 방대한 수의 온라인 사이트를 대상으로 사업을 진행하다보니 기구축 사이트가 메일이 포함된 경우가 있습니다. 이 경우 보안서버 자진등록 홈페이지(www.kisa.or.kr → 보안서버 안내 → 보안서버 자진등록)에 보안서버가 구축되었음을 신고하여 주시면 됩니다. 그리고, 계열사 및 관계사, 추후 신규 사업운영 시에 참조하시라는 의미로 받아주시면 감사하겠습니다.

2. 구축범위 관련

7) 웹사이트에서 보안서버 구축 범위는 정확하게 어디입니까?

기본적으로 보안서버가 구축되어야 할 곳은 웹페이지와 서버간에 개인정보가 전송 또는 호출되는 구간이 발생하는 곳에 암호화가 되어야 합니다. 즉, 어떠한 형식이든 개인정보를 웹페이지와 서버간에 서로 전송이 되거나 호출이 된다면 보안서버가 적용이 되어야 합니다.

통상적인 웹사이트를 기준으로 예를 들어보면 다음과 같습니다.

1. 개인정보가 입력되는 페이지(회원가입, 로그인, 게시판, 상담, 주문, 견적, 결제, 견적, 고객문의, Q&A 등)
2. 개인정보가 보여지는 화면(개인정보 확인 및 수정화면 등)
3. 개인정보가 직접적으로 보이지 않더라도 웹페이지와 서버간에 개인정보가 전송되는 경우(실명확인 등)

8) 암호화되어야 하는 개인정보의 범위는 어디까지입니까?

'개인정보'라 함은 생존하는 개인에 관한 정보로서 성명 · 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호 · 문자 · 음성 · 음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말합니다.

대표적인 예로는 로그인시 아이디/패스워드, 회원가입시 주민번호, 인터넷 뱅킹 이용시 계좌 번호/계좌 비밀번호 등이 해당됩니다. 또한 게시판 등에서 성명, 이메일, 연락처 등을 동시에 수집한다면 개인을 식별할 수 있는 정보로서 개인정보 수집행위에 해당한다고 볼 수 있습니다. 이러한 경우 해당 게시판은 보안서버 구축 대상이 될 수 있습니다.

9) 저희 사이트는 전체 계열사의 회원정보를 한 곳에서 관리하는 통합로그인 정책에 따라 운영되기 때문에 개인정보를 보유하고 있지 않습니다. 저희도 대상인가요?

직접적인 개인정보를 보유하고 있지 않더라도 회원인가 여부를 확인하거나, 로그인 기능 등 개인정보 및 인증정보가 전송되는 구간이 존재한다면 보안서버 구축 대상이 됩니다.

또한, 로그인외에 개인정보의 요구가 있는 경우는 보안서버 구축 대상이 됩니다. 예를 들어, 통합로그인 후 게시판 이용시 개인정보를 요구하는 경우 암호화를 해야 합니다.

3. 호스팅 관련

10) 웹사이트 관리를 호스팅사에 맡기고 있는데, 보안서버 구축도 호스팅 업체가 해야 하는 거 아닙니까?

보안서버 구축 의무는 원칙적으로 사이트를 통해 개인정보를 수집하는 사이트 담당자에게 귀속되나 구축과 관련된 자세한 사항은 호스팅 업체와 상의해야 합니다.

11) 웹호스팅을 받고 있는데 호스팅사가 보안서버 지원을 하지 않는다고 합니다. 어떻게 해야 하나요?

한국인터넷진흥원에 의견제출을 해 주시기 바랍니다.

12) 웹호스팅사를 변경하는 경우, 보안서버를 새로 구축해야 하나요?

웹호스팅사가 주로 사용하는 보안서버 구축 방식은 멀티도메인 SSL 인증서를 이용하는 방법입니다. 이 경우 기존에 사용하던 인증서는 폐기되며 이전하는 웹호스팅업체와 협의하여 보안서버를 구축해야 합니다. (부록 B. 참조)

단일 인증서를 사용하는 경우 다른 서버로의 이전이 가능하기 때문에 추가 구입은 하지 않아도 됩니다. 그러나 이 경우 이전하는 웹호스팅사가 보안서버 구축을 지원하는지 반드시 확인해야 하며, 서버 기종이 변경되는 경우 인증서 및 개인키의 호환이 안되는 경우가 있으니 반드시 전문 업체와 사전 협의 후 진행하시기 바랍니다.

인증서를 구입시 유효기간 동안은 웹호스팅사를 옮기더라도 사용이 가능합니다. 옮기는 웹호스팅사에 문의해서 개인키와 인증서 백업 받으셔서 설정을 요청하시기 바랍니다. 그리고 해당 웹호스팅사에서 보안서버 구축을 지원하는지 미리 확인하시기 바랍니다. 요즘 일부 웹호스팅사는 서비스 차원에서 무료로 지원해 주는 곳도 있습니다.

13) 저희는 보안서버를 기본적으로 제공해주는 호스팅사를 이용하고 있는데, 왜 보안서버가 구축되지 않았다고 하는 거죠?

최근 일부 호스팅사의 경우 자체 개발한 보안서버를 제공하거나, 저렴한 가격으로 제공해 주는 곳이 있습니다.

이러한 호스팅사를 이용한다고 자동적으로 보안서버가 적용되는 것이 아니라, 관리자 모드 등을 통해 보안서버 적용 설정을 해 줘야 되는 것으로 알고 있습니다.

또한, 보안서버는 로그인, 회원가입 등 개인정보가 처리되는 페이지에 모두 설정되어 있어야 하는데, 경우에 따라 적용이 누락되는 페이지가 발생하여 보안서버 미구축으로 점검 되는 경우가 있습니다.

따라서, 해당 웹호스팅사에 문의하여 보안서버를 적용하려면 어떻게 해야 되는지, 적용이 누락된 페이지가 있는지 등을 확인해 보시기 바랍니다.

4. 적용 관련

14) 개인정보의 입력값을 넘길때만 https로 호출해서 넘기는 되는 건가요? 즉, 개인정보를 입력하는 폼이 있는 페이지는 https로 안불러와도 되는지요?

서버와 클라이언트 사이에 개인정보가 전송되는 구간에서만 암호화가 이루어지면 되는 것이기 때문에 입력값을 받는 폼 페이지까지 https로 보여줄 필요는 없습니다. 개인정보 입력된 값이 넘어갈 때 https로 호출해 주시면 됩니다.

15) 보안서버 인증서만 웹사이트에 깔면 암호화 전송이 되나요?

보안인증서를 설치하게 되면 https:// 형태로 통신을 하게 됩니다. 그러나, 일반 이용자들은 보통 http:// 또는 단순히 www. 형태로 접속을 하게 됩니다. http:// 형태로 접속하게 되면 평문통신이 되어 개인정보를 암호화 전송하지 못합니다.

따라서 일반 이용자들이 http://(또는 www.) 방식으로 접속하더라도 https://로 접속될 수 있도록 귀사의 웹사이트 경로를 재설정하여야 합니다.

예: http://www.abc.co.kr, www.abc.co.kr, abc.co.kr

예와 같이 접속 방식은 다양할 수 있으므로, 어떤 방식으로 접속을 하더라도 보안서버가 적용될 수 있도록 접속경로를 수정하여 구현하면 됩니다.

경로 설정(리다이렉션) 방법에 대한 사항은 보안서버 전문 구축 업체에 문의하시거나, 또는 통합실태점검 사무국 홈페이지의 '보안서버 구축 가이드'를 참고 하시기 바랍니다.

16) 보안서버 경고창 발생은 어떻게 제거 하나요?

보안서버를 전체 사이트에 걸지 않고 개인정보가 처리되는 페이지만 각각 적용할 경우에 해당 웹페이지 내의 URL중 https로 호출하지 않는 URL이 존재하기 때문입니다.

경고창이 발생한다고 하여 암호화 전송이 되지 않는 것은 아니나, 경고창이 발생하면 이용자 입장에서 마치 암호화 되지 않는 것처럼 오인할 수 있기 때문에 가급적 경고창이 발생하지 않도록 조치 하시는 것이 신뢰성을 제고하는데 좋습니다.

경고창 발생 제거 방법은 저희 홈페이지(guide.kisa.or.kr)의 구축방법안내 -> 보안서버 구축 -> 적용방법을 참고하시기 바랍니다.

17) 보안서버 적용으로 사이트 속도가 저하되는 경우(SSL 가속기 안내)

간혹 보안서버를 웹사이트 전체에 거는 경우에 상당히 웹사이트에 부하를 주는 문제가 발생하고 있으나, 일반적으로 개인정보가 처리되는 페이지에만 적용하는 경우에는 크게 속도에 지장을 주고 있지 않은 것으로 알고 있습니다.

그러나, 혹시 이 정도의 속도에도 사이트 운영에 불편을 느끼신다면, SSL 가속기를 한번 사용해 보시기 바랍니다.

[보안서버구축가이드] 159페이지에 보시면 SSL 가속기에 대한 설명이 있습니다. 참고하여 주세요.

18) 공인된 인증기관의 인증서를 사용하지 않고 자체적으로 SSL 인증서를 발급하여 사용해도 됩니까?

자체적으로 SSL 인증서를 생성하여 설치해도 사용자의 선택에 따라 암호화는 이루어집니다.

그러나 사용자의 웹브라우저에서 보안경고창이 발생하게 되는데 익스플로러 6.0이하에서는 단순히 '신뢰할 수 없는 기관에서 발급한 인증서'라는 팝업창이 뜨지만, 익스플로러 7.0에서는 암호화 이후에도 주소창이 계속 적색으로 표시되어 사용자에게 웹사이트의 신뢰성에 대해 경고를 하게 됩니다.

또한 익스플로러 이외의 웹브라우저 사용자는 '피싱 의도가 있는 사이트'라는 더 심각한 경고문구를 접하게 됩니다.

SSL인증서의 용도가 암호화 이외에 해당 웹사이트의 실체 인증이라는 주요기능이 있으므로 가능하면 웹브라우저의 CTL(인증서 신뢰목록)에 탑재된 상용 SSL 인증서를 사용하실 것을 권고 드립니다.

시중에는 저렴한 SSL 인증서도 있고 공인인증기관에서는 국산 SSL 인증서도 발급할 수 있는 상태이므로 충분한 검토 후에 적용하시기 바랍니다.
(※국산인증서 발급기관 : 한국전자인증, 한국정보인증, 한국무역정보통신)

5. 기타

19) 보안서버를 구축하려면 누구에게 연락해야 하나요?

보안서버 구축 전문 업체와 상의하시면 되며, 'II 장 2절 보안서버 구축 전문 업체' 내용 또는 보안서버전문협의회 홈페이지 (www.kisia.or.kr/secureserver)를 참조하시기 바랍니다. 이외에 평소에 알고 있던 보안서버 구축 전문 업체를 이용하셔도 됩니다.

20) 구축 업체를 소개해 줄 수는 없습니까?

저희는 특정업체를 소개해드릴 수는 없습니다. 본 가이드 본문에 포함된 보안서버 구축 전문 업체 연락처를 참고하시거나 이외의 보안서버 구축 전문 업체를 통해 문의해 주시기 바랍니다.

21) 만약 더 이상 개인정보를 수집하지 않으면 어떻게 됩니까?

법률적용 대상이 되지 않기 때문에 보안서버 구축이 필요없으며, 운영상 불필요한 개인정보 수집은 하지 않는 것이 바람직합니다.
다만 이 경우, 기존에 수집된 개인정보를 폐기하고 수집을 중단하겠다는 내용을 명시하여 이의신청서를 사무국에 송부하여 주시기 바랍니다.

22) 사이트를 현재 운영하지 않거나 혹은 조만간 폐쇄할 예정입니다.

'사이트 폐쇄' 또는 '폐쇄 예정'임을 명시하여 이의신청서를 사무국에 송부하여 주시기 바랍니다.

23) 보안서버를 구축하려면 비용이 얼마나 드나요?

보안서버 구축 방식과 서비스 범위 등에 따라 금액의 차이가 크므로 해당 웹사이트에 적합한 보안서버 구축을 위한 자세한 내용은 전문 업체와 상의하시기 바랍니다.

24) SSL 인증서의 경우 동일한 기술을 이용하는데 인증서의 가격은 왜 차이가 납니까?

인증서의 가격은 해당 발급업체의 신뢰성, 브랜드 가치, 128비트 강제 암호화 여부, 지원되는 웹브라우저의 종류 및 설치 지원의 정도 등을 고려하여 책정되기 때문에 차이가 나게 됩니다.

25) 보안서버 관련해서 더 자세한 정보는 없나요?

한국인터넷진흥원 보안서버 안내 홈페이지(www.kisa.or.kr → 보안서버 안내) 를 참조하시기 바랍니다.

부록 | SSL 가속기 소개

1. SSL 가속기 정의

웹 브라우저 회사인 넷스케이프가 만든 SSL(Secure Socket Layer)은 널리 알려진 바와 같이 암호화와 복호화를 통해 데이터를 전달하여 안전한 통신을 가능하게 하는 기술입니다. SSL 가속기는 웹 서비스 시스템의 통신보안 및 신원확인, 부인방지 등을 위해 PKI 기반의 인증서 기반의 보안 프로토콜인 SSL을 적용하면서 비 대칭키 암호화 연산에 따른 서버시스템의 부하증가, 속도저하 문제 및 서버키 보호 문제를 해결하기 위해 출현하게 되었습니다.

2. SSL 가속기의 역할

대형 포털사이트와 같이 트래픽이 많으면서 SSL 방식의 보안서버를 운영하는 사이트가 SSL을 웹 서버에서 직접 운영하게 되면, 서버의 부하가 커지게 되고 사용자의 응답시간이 매우 느려질 수 있습니다. SSL 가속기는 SSL 연결에 따른 모든 암호화를 서버로부터 이관받아 독립된 장치에서 전담함으로써 서버의 부하를 감소시키고 웹 어플리케이션 시스템의 전체 성능을 향상시킬 수 있습니다.

또한 SSL 보안에 사용되는 서버의 암호화키를 SSL 가속기에 별도로 저장함으로써 암호화키 유출에 따른 위험성을 줄일 수 있습니다. 서버 키가 유출될 경우 SSL 보안 통신 데이터가 해킹될 수 있고 허위 사이트나 피싱 사이트에 의한 피해가 발생할 수 있습니다.

그리고 SSL 인증서를 구입하여 웹 서버 대신 웹 가속기에 설치가 가능하기 때문에 기존에 운영중인 웹 프로그램을 수정할 필요가 없다는 장점을 가지고 있습니다.

3. SSL 가속기의 종류

① 1세대 SSL 가속기 'PCI / SCSI 카드타입'

SSL 가속기의 첫 번째 세대는 서비스를 제공하는 웹 서버가 작동하는 하드웨어에 직접적으로 설치가 되는 PCI나 SCSI 타입의 카드 형태의 제품들입니다.

PCI나 SCSI 카드 타입의 SSL 가속기 제품군은 우선 SSL 핸드쉐이크 과정을 담당함으로써 CPU에 부과되던 높은 부하를 절감시켰으며 설치 구조상 실제 콘텐츠 서비스를 수행하는 웹 서버 또는 어플리케이션 서버가 작동하는 하드웨어의 슬롯에 직접 장착되기 때문에 SSL 사용시 보호되어야 할 클라이언트 브라우저로부터 웹 서버 본체까지의 엔드 투 엔드(end-to-end)의 완벽한 보안이 이루어집니다. 그러나 이러한 제품군에는 치명적인 단점이 존재하는데 하나는 가속기 설치시 반드시 시스템의 중단이 필요하다는 것이고, 또 하나는 확장성의 문제입니다. 카드 타입의 가속기는 하나의 가속기가 하나의 서버만을 감당하는 물리적인 구성의 한계 때문에 여러 가지 이유로 인해 서버의 증설이 요구되는 경우 서버 증설 숫자만큼 가속기의 추가 구매 또한 필요하기 때문입니다.

② 2세대 SSL 가속기 'SSL 오프로더'

1세대 제품의 문제점을 개선하고 나온 2세대 SSL 가속기는 네트워크 장비 타입으로 흔히 SSL 오프로더(Offloader)라고 불리는 제품군입니다. SSL 오프로더는 기존의 카드타입 가속기들과 달리 하나의 가속기가 여러 대의 웹 서버나 애플리케이션 서버를 위한 SSL 가속기능을 수행함으로 기존 1세대 제품군의 확장성 문제를 보완했습니다. 웹 서버나 애플리케이션 서버와 분리된 설치 방법으로 인해 가속기 드라이버와 서버 하드웨어 충돌 등으로 인해 발생할 수 있는 문제의 소지를 없앴습니다.

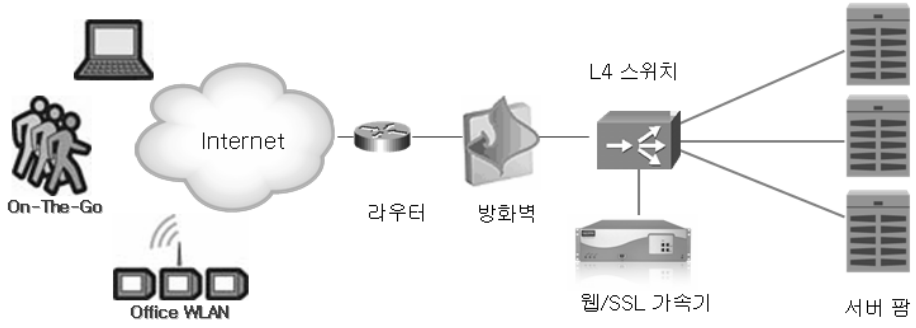
그러나 네트워크 구성상 가속기와 서버사이에 물리적인 공백 구간이 있을 수 밖에 없고 브라우저가 발생시킨 암호화 패킷은 가속기에 복호화되고 클리어 텍스트(Clear Text)로 이 구간을 통과해 서버에 전달되기 때문에 실제 클라이언트 브라우저로부터 서버까지의

엔드 투 엔드 보안이 불가능합니다. 또한 일반적인 인라인 구성(In-line Configuration)의 경우 설치시 서비스의 일시적 중단을 피할 수는 없습니다.

몇 가지 단점에도 불구하고 최근에는 단독 장비 제품형태의 2세대 제품군이 주류를 이루어 시장을 선도하고 있습니다. 또한 2세대 제품군이 가지는 단점을 보완한 장비들도 개발되고 있습니다. 특히 백엔드(Back end) SSL 기능을 통한 엔드 투 엔드 보안 제공이나 원암 구성(One-arm Configuration)을 통한 서비스 중단없는 설치기능 등을 통해 보다 효과적으로 SSL 가속기를 실제 네트워크상에 구현할 수 있는 다양한 방법들이 나오고 있습니다.

4. SSL 가속기 구성 방식

SSL 가속기를 구성하는 방식은 서버 환경과 가속기의 기능 범위에 따라 다양합니다. L4스위치 기능과 웹/SSL 가속을 동시에 담당하거나 방화벽, L4/L7 SLB, 웹/SSL 가속을 동시에 처리하는 경우도 있으나, 기존 네트워크 인프라에 대한 변경을 최소화하면서 가속 기능만을 활용하고자 구성하는 방식을 소개하겠습니다.



〈그림 C-1〉 SSL 가속기 구성 방식

위 그림은 기존 L4 스위치에 접속하는 구성 방식으로 L4스위치에서는 웹 트래픽을 가속기로 Redirection되도록 처리하고, 가속기에서는 캐싱, TCP 멀티플렉싱, SSL 처리 등을 담당하게

됩니다. 웹/SSL 가속기가 장애 시에는 L4 스위치에서 자동으로 Bypass 처리하는 방식입니다.

이 외에도 L4 스위치 기능과 웹/SSL 가속을 동시에 담당하거나 방화벽, L4/L7 스위치 기능을 웹/SSL 가속을 동시에 처리하는 등 다양한 구성이 가능하므로 업체의 서버 환경과 요구사항에 따라 적합한 SSL 가속기를 구성할 수 있습니다.

※ 참고문헌

1. SSL 프로토콜에 대한 이해, 퓨쳐시스템 http://www.future.co.kr/
2. 보안서버 가속을 위한 SSL 가속기 솔루션, 어레이네트웍스 코리아
3. SSL Accelerator for Secure Web Server, 엑스비전씨큐리티시스템

《 한국인터넷진흥원(KISA) 『안내서·해설서』 시리즈 》

분류	안내서·해설서	해당팀명	발간 년월	대상	수준
인터넷 진흥	DNS 설정 안내서	시스템관리팀	'09.	IT시스템관리자	중급
	인터넷주소분쟁해결 안내서	도메인팀	연간지	일반	초급
	모바일 RFID코드 및 OID기반 RFID코드 적용 안내서	무선인터넷팀	'09.8	IT기업개발자	중급
	13.56MHz대역의 OID적용을 위한 미들웨어 개발 안내서	무선인터넷팀	'09.12	IT기업개발자	중급
	공공기관 IPv6 적용 안내서	IP팀	'08.12	IT시스템관리자	중급
인터넷 이용 활성화	본인확인제 안내서	인터넷윤리팀	'09.2	일반,업무관계자	중급
	본인확인제 만화 안내서	인터넷윤리팀	'09.	일반	초급
정보 보호 시스템 관리	BcN 정보보호 안내서	인터넷서비스보호팀	'07./ '10.1	IT시스템관리자	중급
	침해사고 분석절차 안내서	해킹대응팀	'10.1	IT시스템관리자	고급
	웹서버구축 보안점검 안내서	웹보안지원팀	'10.1	IT시스템관리자	고급
	웹어플리케이션 보안 안내서				
	홈페이지 개발보안 안내서				
	무선랜 보안 안내서	해킹대응팀	'10.1	일반	중급
	침해사고대응팀(CERT) 구축/운영 안내서	상황관제팀	'07.9	업무관계자	중급
	WebKnight를활용한 IIS 웹서버 보안 강화 안내서	웹보안지원팀	'09.6	IT시스템관리자	중급
	WebKnight 로그 분석 안내서				
	ModSecurity를 활용한 아파치 웹서버 보안 강화 안내서				
	보안서버구축 안내서	개인정보보호팀	'08.7	IT시스템관리자	중급
정보보호인증	IT보안성 평가·인증 안내서	공공서비스보호팀	'09.12	일반·업무관계자	초급
기업 정보 보호	정보보호 안전진단 해설서	기업보안관리팀	'08.4/ '10.1	업무관계자	초급
	정보보호 안전진단 업무 안내서	기업보안관리팀	'10.1	업무관계자	초급
	정보보호관리체계 안내서	기업보안관리팀	'09.12	일반	초급
신규 서비스 정보 보호	패스워드 선택 및 이용 안내서	융합보호R&D팀	'10.1	일반	초급
	암호이용 안내서	융합보호R&D팀	'07./ '10.1	일반	중급
	IPv6운영보안 안내서	융합보호R&D팀	'06.12	IT시스템관리자	중급
	IPv6보안기술 안내서	융합보호R&D팀	'05.	일반	초급
	와이브로 보안기술 안내서	융합보호R&D팀	'06.8	IT시스템관리자	중급
	암호 알고리즘 및 키 길이 이용 안내서	융합보호R&D팀	'07	IT시스템관리자	중급
	(기업 및 기관의 IT 정보자산 보호를 위한) 암호정책 수립 기준 안내서	융합보호R&D팀	'07	IT기업개발자	중급
	(정보의 안전한 저장과 관리를 위한) 보조기억매체 이용 안내서	융합보호R&D팀	'09	일반	초급
	웹사이트 회원탈퇴 기능 구현 안내서	융합보호R&D팀	'06	IT시스템관리자	중급
개인 정보	개인정보의 기술적 · 관리적 보호조치 기준 해설서	개인정보보호기획팀	'09.9	업무관계자	중급
	위치정보의 보호 및 이용 등에 관한 법률 해설서	개인정보보호기획팀	'08.12	업무관계자	중급
	위치정보보호를 위한 관리적·기술적 보호조치 권고 해설서	개인정보보호기획팀	'08./ '10.1	업무관계자	중급
	웹사이트 개발·운영을 위한 개인정보 안내서	개인정보보호기술팀	'09.11	IT기업 개발자, 관리자	중급
	I-PIN 2.0 도입 안내서	개인정보보호기술팀	'09.7	업무관계자	중급
	김대리, 개인정보보호 달인되기	이용자권익보호팀	'09.8	업무관계자	중급
	기업의 개인정보영향평가 수행을 위한 안내서	이용자권익보호팀	'09.1	업무관계자	중급
스팸	사업자를 위한 불법스팸 방지 안내서	스팸대응팀	'08.9	일반, 업무관계자	초급
인력 양성	지식정보보안 신규일자리 창출사업 세부시행 안내서	KISA아카데미팀	'09.	업무관계자	초급

○ 본 안내서·해설서는 한국인터넷 홈페이지(www.kisa.or.kr)자료실에서 내려 받으실 수 있습니다.

보안서버구축 안내서

2009년 12월 인쇄
2009년 12월 발행

발행처: **한국인터넷진흥원**

서울특별시 종로구 세종로 20
방송통신위원회
Tel: (02) 750-1114

서울특별시 송파구 가락동 79-3번지
대동빌딩 한국인터넷진흥원
Tel: (02) 405-5118

인쇄처: 한국신체장애인복지회
Tel: (02) (02) 6401-8891

<비매품>

이 책을 볼 수 있는 독자는?

IT시스템관리자 초급

IT시스템관리자 중급

IT시스템관리자 고급

한국인터넷진흥원

138-950 서울시 송파구 가락동 79-3번지 대동빌딩
Tel. 405-5118 Fax. 405-5119
www.kisa.or.kr