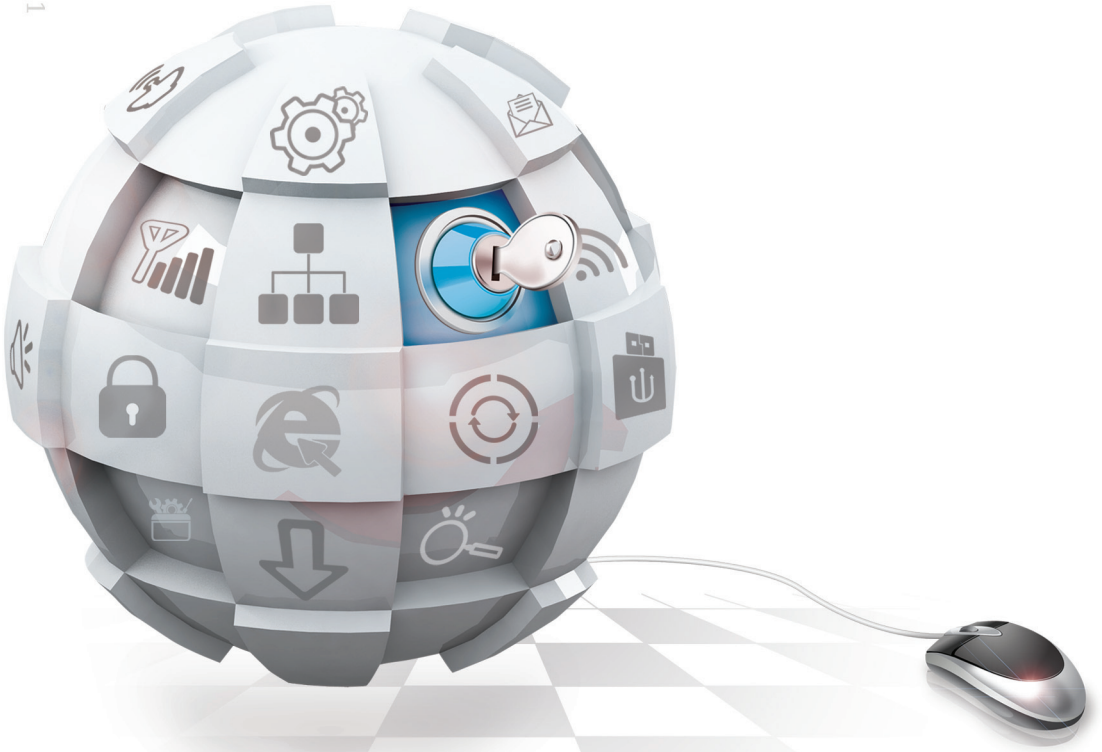
2013
보안서버 구축 가이드



미래창조과학부
Ministry of Science, ICT and Future Planning

개인정보보호협회
KOREA ONLINE PRIVACY ASSOCIATION

2013
보안서버
구축가이드

주의사항

◆ 본 가이드는 「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 개인정보보호 조치 이행을 지원하기 위하여 발간하였습니다.

◆ 본 가이드에서 안내하고 있는 제품이나 예시 등은 각 사업자에 있을 수 있는 고유한 환경을 고려하지 않았으므로 실제 환경에서 그대로 적용되지 않을 수 있습니다.

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

※ 본 가이드의 내용에 대하여 문의가 있거나 오류를 발견한 경우에는 개인정보보호협회로 문의하여 주시기 바랍니다.

– 홈페이지 주소 〈 www.opa.or.kr 〉

가이드의 구성

본 가이드는 사용자들의 이해를 돕기 위하여 다음과 같이 구성되어 있습니다.

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

보안서버 구축 방법을 선택하였다면, Ⅱ장에서 상황에 맞는 내용을 참조하시면 됩니다.

각 장에 소개되는 설치 방법과 오류 시 대처방법을 숙지한 후 보안서버 구축 전문 업체에 연락하시면 보다 자세한 안내를 받을 수 있습니다.

Ⅲ장은 보안서버 구축에 관한 FAQ를 정리한 것입니다.

웹사이트 운영자들이 자주 질문하신 내용을 정리한 것이므로 우선 궁금하신 내용이 있는지 확인한 후 추가적인 문의는 보안서버 안내 홈페이지(www.opa.or.kr – 보안서버 보급지원)를 참고 하시기 바랍니다.

목차	주요내용
Ⅰ. 보안서버(Secure Server)란	– 보안서버 정의 및 필요성 – 보안서버 관련 규정 및 종류 – 보안서버 적용확인 및 구축 전문 업체
Ⅱ. SSL 방식 보안서버 구축하기	–보안서버 소개 및 구축 절차 –수정방법 및 오류 시 대처방법
Ⅲ. 보안서버 관련 FAQ	–보안서버 구축 관련 질문과 답변

2013
보안서버 구축가이드

미래창조과학부
Ministry of Science, ICT and Future Planning

개인정보보호협회
KOREA ONLINE PRIVACY ASSOCIATION

Contents

그림 목차

I

보안서버란

I 보안서버란

1. 보안서버의 정의

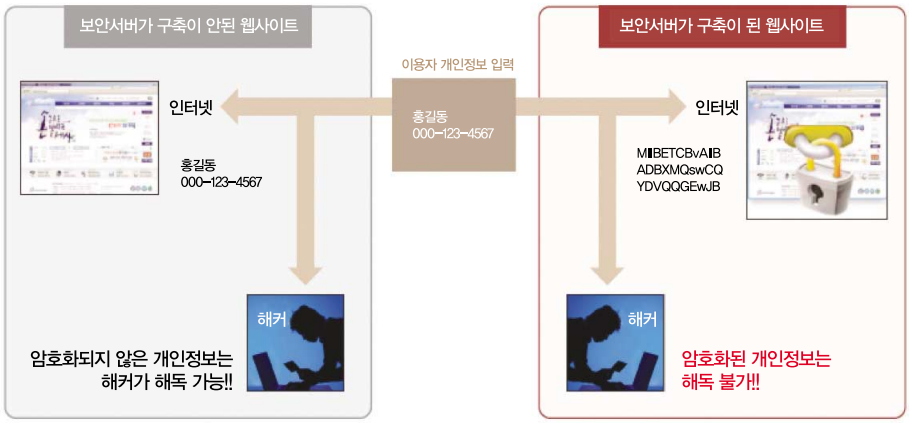
보안서버란 인터넷 상에서 개인정보를 암호화하여 송 · 수신하는 기능으로 독립적인 하드웨어를 따로 설치하는 것이 아니라 이미 사용하고 있는 웹서버에 SSL(Secure Sockets Layer)인증서나 암호화 소프트웨어를 설치하여 암호 통신을 지원하는 것을 의미합니다. SSL 인증서의 경우 해당 전자상거래 업체의 실존을 증명하는 과정을 거쳐 발급되기 때문에 웹사이트에 대한 인증 기능도 일부 가지고 있습니다.

인터넷 상에서 송수신되는 개인정보의 대표적인 예로는 로그인 시 ID, 패스워드, 회원가입 시 이름, 전화번호, 인터넷 뱅킹 이용 시 계좌번호, 계좌 패스워드 등이 있습니다. 만일 이러한 개인정보가 암호화되지 않은 채로 해킹을 통해 유출될 경우 심각한 피해를 초래할 수 있습니다. 보안서버는 이러한 위협을 방지하기 위한 방법의 하나로, 개인정보를 암호화하여 송수신함으로써 유출을 방지하며 중간에 데이터를 가로채더라도 암호화되어 있기 때문에 개인정보가 노출되지 않습니다.

그러나 보안서버의 구축 및 운영방법은 업체에 따라 많은 차이점이 있으며, 잘못된 보안서버의 구축 및 운영은 개인정보의 유출을 초래할 수 있습니다.

2. 보안서버 구축의 필요성

그림 1-1 보안서버 구축의 필요성



인터넷은 개방된 환경으로 일반적인 송 · 수신방법이 안전하지 않기 때문에 인터넷상에서 송 · 수신되는 이용자, 사업자 및 컴퓨터의 신원정보(Identity)를 확인하는 것은 어렵지 않습니다. 따라서 모든 송 · 수신 메시지는 도청자가 중간에 가로채어 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 흉내 낼 수 있습니다.

이러한 위협은 인터넷에서 전송되는 정보의 가치 및 민감도에 따라 잠재적 이득을 원하는 자에게도 동일하게 적용될 수 있습니다. 실제로 패킷을 캡처하는 프로그램을 이용하면 내가 속한 네트워크에 지나가는 대부분의 패킷 내용을 쉽게 확인할 수 있습니다.

이러한 문제점을 해결하기 위해 보안서버는 네트워크 응용 프로그램간의 통신에 대하여 프라이버시, 인증, 신뢰를 보장해주는 것을 목표로 하고 있습니다. 이를 위해 SSL 프로토콜은 어떤 TCP/IP 기반의 통신에도 유용하게 적용될 수 있으며, 특히 HTTP(hypertext transfer protocol) 통신을 보호하는 목적으로 많이 사용되고 있습니다.

보안서버 구축을 통한 송수신 구간 암호화는 통신을 안전하게 보호해 줄 뿐만 아니라, 네트워크 통신에서 다음의 장점을 제공합니다.

2.1 정보유출 방지(sniffing 방지)

사용자가 웹사이트에 접속해서 로그인 또는 전자상거래를 위해 ID, 패스워드, 신용카드 번호 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 스니핑 입니다.

스니핑 툴(sniffing tool)은 인터넷 상에서 누구나 손쉽게 구할 수 있습니다. 따라서 학교, PC방, 회사 등의 공용 네트워크에서 누군가 스니핑 툴을 이용하여 타인의 개인정보를 수집한다면, 일반적인 웹사이트의 경우 이용자의 아이디와 비밀번호 등 이용정보가 평문형태 그대로 노출되게 됩니다. 그러나 웹사이트에 보안서버가 구축된 경우에는 개인정보가 암호화되어 전송되므로 이러한 노출 위협으로부터 안심할 수 있습니다. 따라서 보안서버는 개인 정보 보호를 위한 필수적이며 기본적인 수단입니다.

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 피싱 수법이 점점 교묘해져 가고 피해자가 속출하고 있는 상황으로 사용자가 개인정보를 입력 시 해당 페이지가 신뢰할 수 있는 인증서가 설치되어 있는지 확인하는 등의 사용자의 주의가 필요합니다.

보안서버를 구축하기 위해서는 SSL 인증서를 공인인증기관으로부터 발급받아야 합니다. 발급받기 위해서는 도메인 정보 등을 제공해야 하며, 발급받은 인증서에는 도메인 정보가 포함되어 있습니다. 접속한 웹사이트에서 자물쇠 이미지를 확인하거나 개인정보 입력 시 암호화 호출(https://), 암호화 모듈 로딩 화면 등을 확인한다면 유사하게 구성된 피싱 사이트 여부를 쉽게 구별할 수 있습니다. 해커 등의 제3자가 유사사이트를 만들어 피싱을 시도 하더라도 SSL 인증서가 진위여부를 증명함으로써 피싱으로 인한 피해를 줄일 수 있는 것입니다.

2.3 기업의 신뢰도 향상

사회에 대해서도 깊은 관심과 책임감을 가져야 한다는 사회책임경영의 중요성이 나날이 커져 나가고 있습니다. 사회 책임 경영은 기업의 사회적 책임감을 의미하는 것으로 기업의 존재 기반인 사회에 대해서도 깊은 관심과 책임감을 가져야 한다는 기업경영의 화두입니다.

이에 대한 관심이 점차 높아지고 있으며, 많은 기업들이 이미 적극적으로 사회 책임 경영에 입각한 경영을 펼치고 있습니다.

보안서버의 설치는 고객에게 개인정보를 안전하게 관리하는 사회 책임 경영을 하는 기업이라는 이미지를 부각시킬 수 있습니다. 웹 사이트상 보안서버 인증마크는 개인정보보호의 신뢰성을 사용자에게 보여줄 수 있으며, 가시적인 홍보 효과 또한 얻을 수 있습니다.

3. 보안서버 관련 법률

1. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

▶ 제28조 (개인정보의 보호조치)① 정보통신서비스 제공자 등이 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 암호화 기술 등을 이용한 보안조치

▶ 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 아니하여 이용자의 개인정보를 분실 · 도난 · 누출 · 변조 또는 훼손한 자

▶ 76조(과태료) 〈개정 2012.2.17, 시행 2012.8.18〉

① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원이하의 과태료를 부과한다.

3. 제28조제1항(제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적 · 관리적 조치를 하지 아니한 자

2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

▶ 제15조(개인정보의 보호조치) ④ 법 제 28조제1항제4호에 따라 정보통신서비스 제공자 등은 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

▶ 제6조(개인정보의 암호화) ③ 정보통신서비스제공자 등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송 · 수신할 때에는 보안서버 구축 등의 조치를 통해 이를 암호화 해야 한다. 보안서버는 다음 각 호의 어느 하나의 기능을 갖추어야 한다.

1. 웹 서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송 · 수신하는 기능

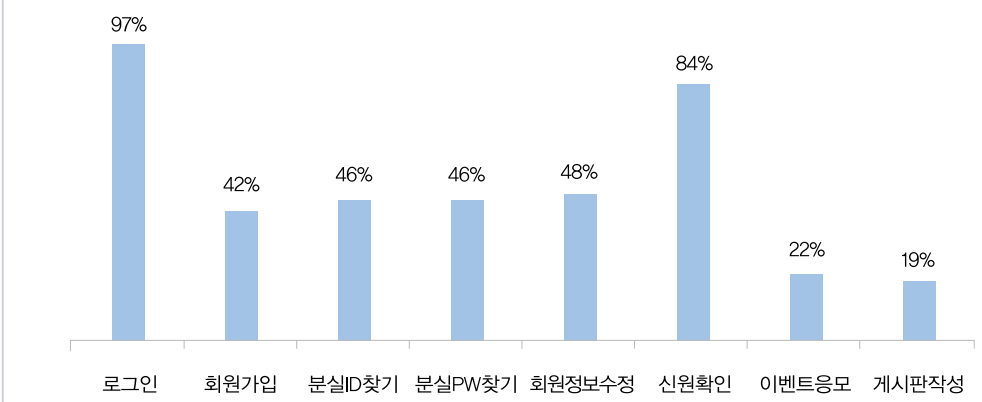
2. 웹 서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송 · 수신하는 기능

4. 보안서버 적용 범위

일반적으로 '개인정보'라 함은 생존하는 개인에 관한 정보로서 성명 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 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 SSL방식 보안서버에서 암호화 통신이 적용된 비율



위 비율은 한국인터넷진흥원에서 보안서버를 사용하는 국내 웹사이트를 대상으로 조사를 한 내용 입니다. 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.

5. 보안서버의 종류

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

5.1 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.

5.2 응용프로그램 방식

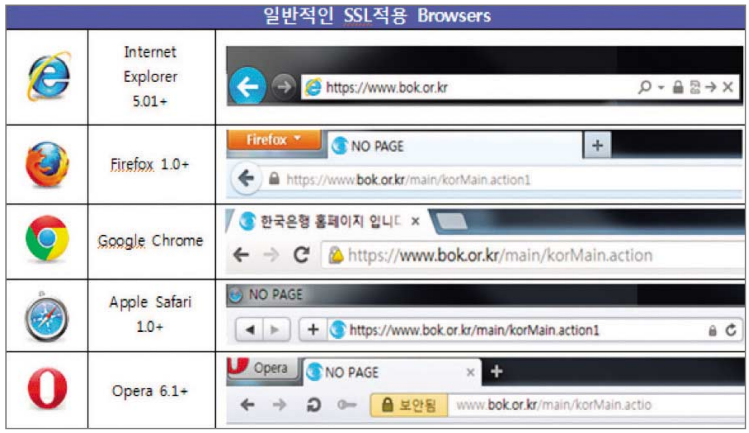
암호화 응용프로그램을 이용한 보안서버는 웹 서버에 접속하면 사용자 컴퓨터에 자동으로 보안 프로그램이 설치되고 이를 통해 개인 정보를 암호화 하여 전송합니다. 웹사이트 접속 시 초기화면이나 로그인 후 윈도우 화면 오른쪽 하단 작업표시줄 알림영역에 다음 그림과 같은 암호화 프로그램 실행여부를 확인할 수 있으며, 응용프로그램 방식의 솔루션에 따라 모양은 다르게 나타날 수 있습니다.

6. 보안서버 구축 확인 방법

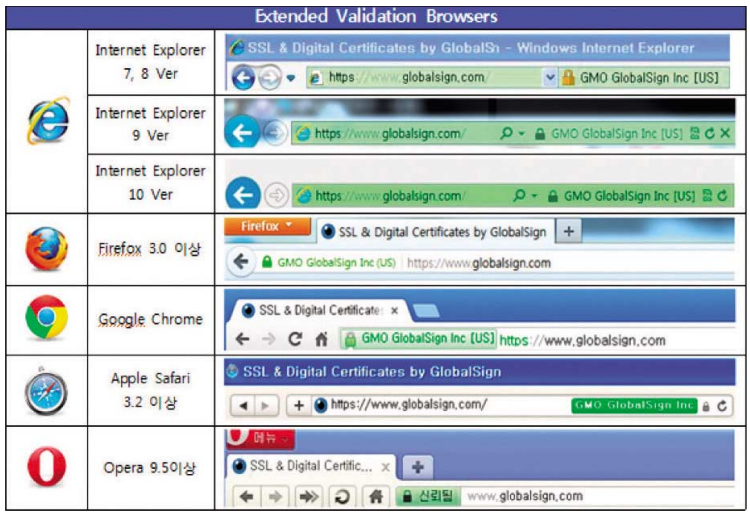
보안서버 구축 확인은 웹사이트 접속 시 SSL인증서가 설치되었는지 또는 개인정보가 암호화 되어 전송되는지 여부를 확인함으로써 알 수 있습니다. SSL인증서는 웹사이트 접속 시 브라우저 주소창에 표시된 자물쇠 및 인증서 보기 등을 통해 확인할 수 있으며, 개인정보 암호화 전송은 패킷 캡처 프로그램을 이용하여 실제 전송되는 데이터의 암호화 여부를 확인할 수 있습니다.

6.1 SSL인증서 설치 확인

1) 브라우저 주소창 표시 확인 방법(https:// 접속)



※ 인터넷 주소창의 자물쇠 표시로 인증서가 설치되어 있는지 확인할 수 있습니다.



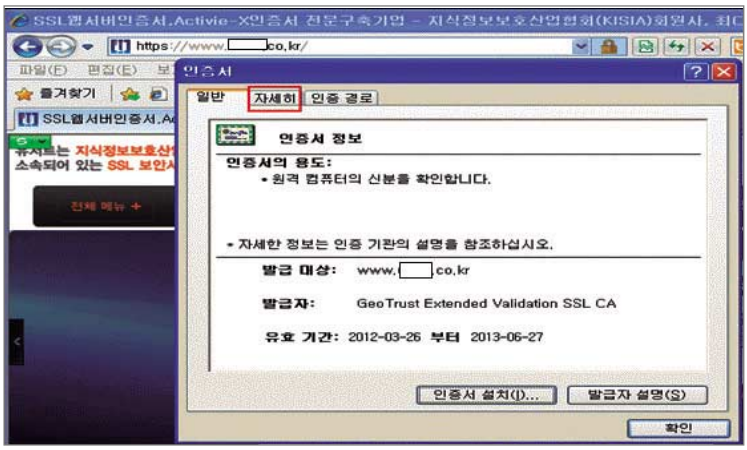
- EV(Extended Validation) 인증서는 Https 통신구간에서 주소창이 녹색으로 변하는 인증서입니다.
- IE 7.0 이상, Mozilla Firefox 3.0 이상, Google Chrome, Apple Safari 3.2 이상, IPhone 3.0 이상에서 주소창이 녹색으로 변합니다.
- IE 6.0 이하 버전은 주소창이 녹색으로 변하지 않습니다.
- 접속한 사이트를 운영하는 회사명, 주소 등을 EV SSL 인증서를 통하여 사용자들이 쉽게 확인할 수 있으며, 웹사이트의 진위 여부를 쉽게 확인 할 수 있습니다.

2) 브라우저 주소창 자물쇠 표시 및 인증서 상세보기 방법

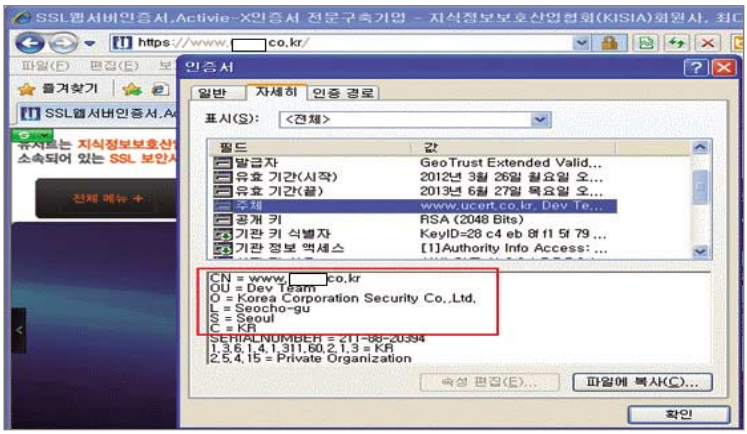
❶ 자물쇠 클릭

❷ 인증서 보기 클릭

❸ 인증서 정보확인 후 자세히 탭 클릭



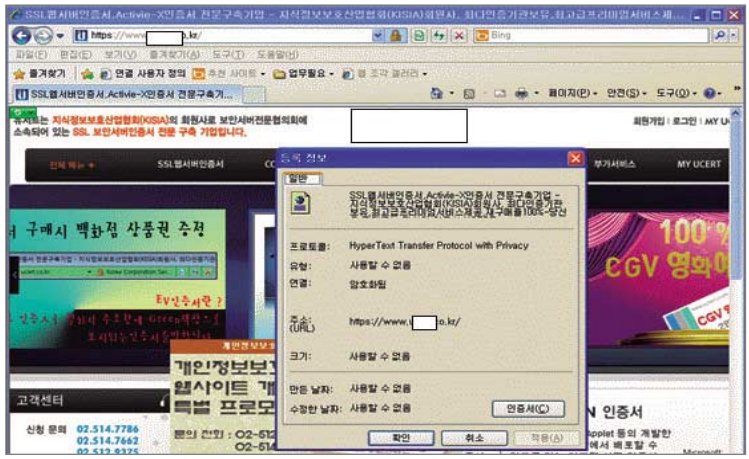
❹ 주체 클릭 후 도메인 주소 및 기업정보 확인



3) 웹페이지 속성보기를 통한 확인 방법

❶ 사이트에서 우클릭 후 속성 클릭

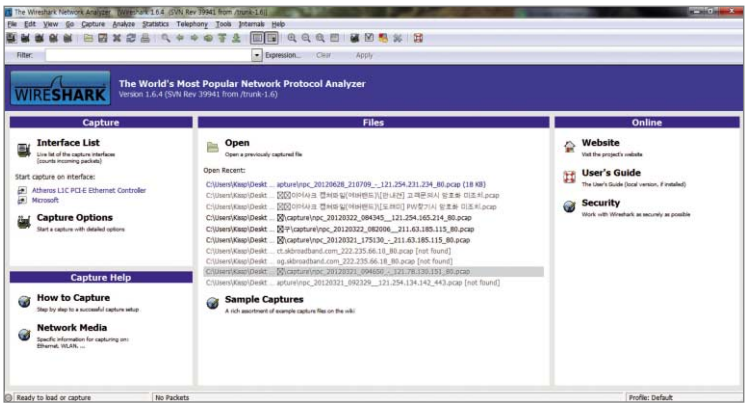
❷ 등록 정보에서 인증서 및 암호화 상태 확인



6.2 개인정보 암호화 전송 확인

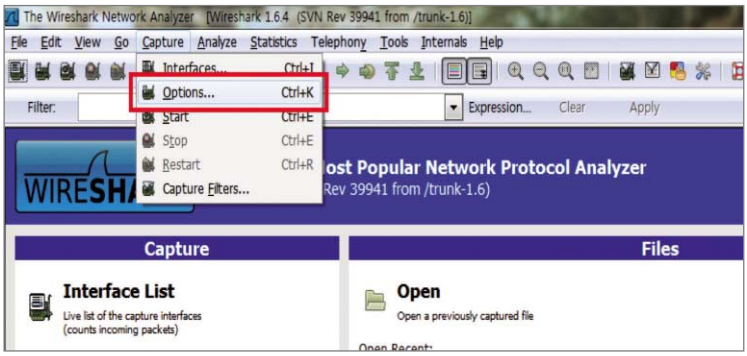
웹사이트의 개인정보가 전송되는 구간(예: 로그인, 게시판 등)을 점검함으로써 보안서버 구축 여부를 확인할 수 있습니다. 전송구간 암호화 여부는 패킷 캡처 프로그램인 와이어샤크(Wireshark)를 통해 이를 확인할 수 있으며 확인방법은 다음과 같습니다.

1) 와이어샤크 프로그램 메인화면

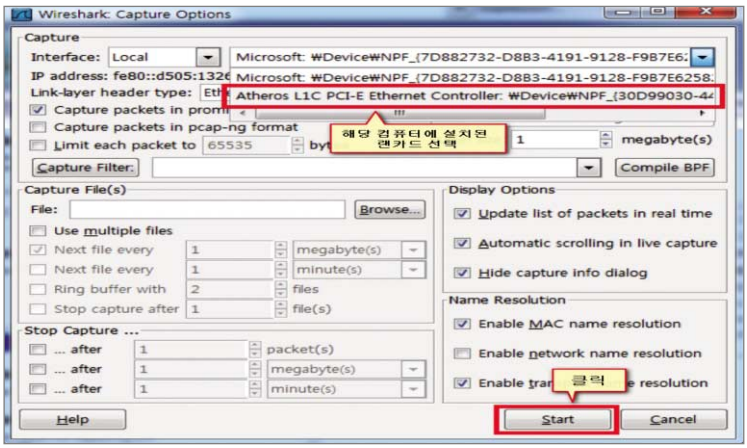


2) 환경설정 방법

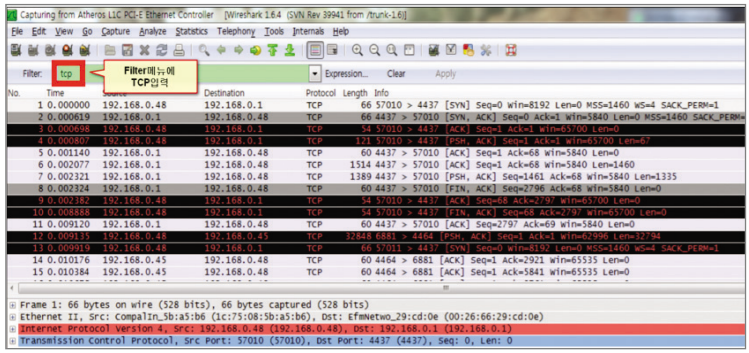
❶ 상단 메뉴에서 Capture 〉 Options 클릭



❷ Options 화면: Interface 메뉴에서 해당 랜카드(본인 컴퓨터에 설치된 랜카드) 선택 후 start버튼 클릭

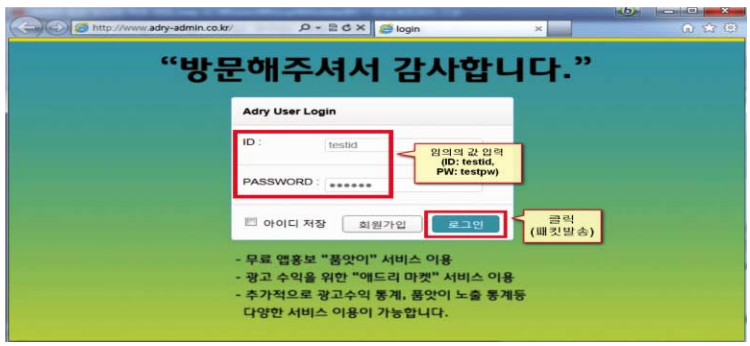


❸ 필터설정 : 패킷 분석이 시작된 후 filter메뉴에 TCP 입력



3) 점검대상 웹페이지에서 패킷 발송

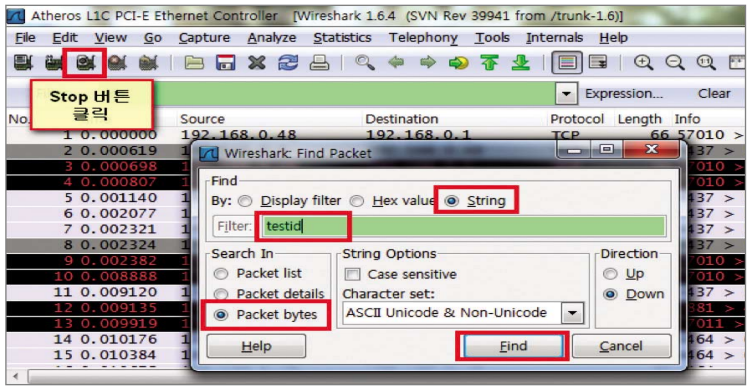
❶ 개인정보 송·수신 구간에 임의의 값(ID:testid, PW:testpw) 입력 후 로그인 버튼 클릭



4) 점검 키워드 검색

❶ 패킷분석 정지버튼을 클릭 후

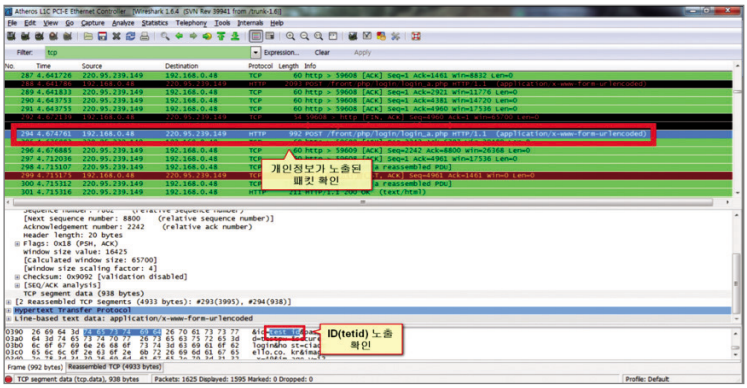
❷ 패킷검색(Ctrl + F)창을 띄워서 String, Packet byte 단위 설정 후 점검 키워드 (testid, testpw) 검색



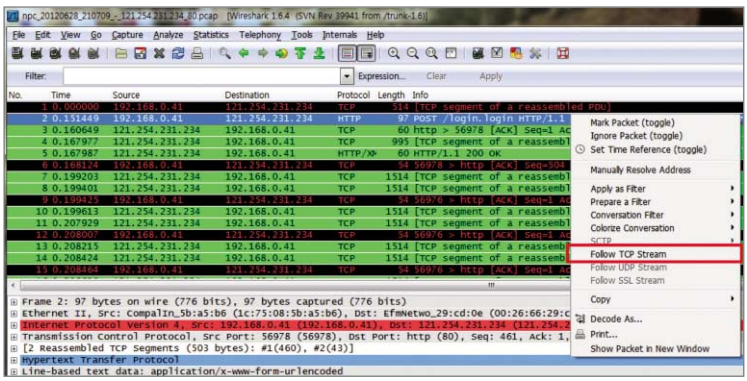
5) 점검 키워드 검출 확인

❶ 점검 키워드 가 검출된 경우 화면(ex:testid)

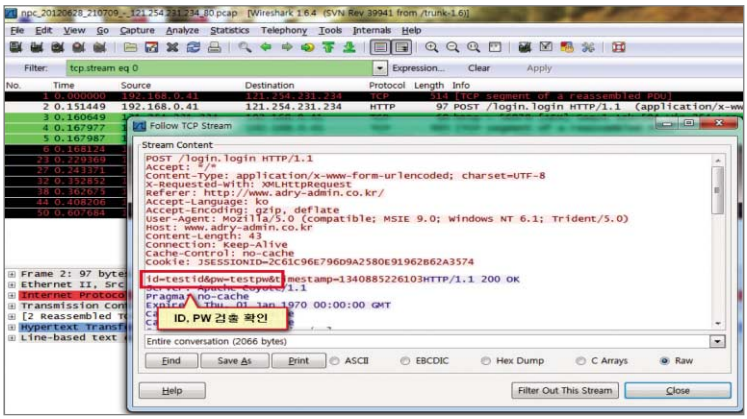
※ 점검키워드가 검출되지 않은 경우 보안서버가 정상적으로 구축된 것입니다.



❷ 검출된 패킷에 마우스 우클릭 후 Follow TCP Stream 클릭



❸ 검출된 정보 확인



7. 보안서버 구축 전문 업체

보안서버 구축 방법과 절차에 관한 보다 구체적인 내용은 다음의 「보안서버전문업체」 목록 중 선택하여 문의하면 자세한 설명을 받을 수 있습니다. 「보안서버전문업체」 외에 전문 업체를 이용하셔도 무방합니다.

SSL 방식 솔루션 공급 업체		
업체명	홈페이지	전화번호
금융결제원	www.yessign.or.kr	1577-5500
나인포유	www.certkorea.co.kr	(02) 3444-2750
애니서트	www.anycert.co.kr	070-7090-0800
아이네임즈	secure.inames.co.kr	(02) 559-1219
정보넷	sslsecurity.kr	070-7098-5732
코스콤	www.signkorea.co.kr	1577-7337
한국기업보안	www.ucert.co.kr	(02) 514-7786
한국무역정보통신	www.tradesign.co.kr	1566-2119
한국전자인증	www.crosscert.com	1588-1314
한국정보인증	www.sgssl.net	(02) 360-3065
한비로	www.comodossl.co.kr	1544-4755
응용 프로그램 방식 솔루션 공급 업체		
업체명	홈페이지	전화번호
드림시큐리티	www.dreamsecurity.com	(02) 2233-5533
소프트포럼	www.softforum.co.kr	(031) 622-6300
아이네임즈	secure.inames.co.kr	(02) 559-1219
애니서트	www.anycert.co.kr	070-7090-0800
유넷시스템	www.unetsystem.co.kr	(02) 2088-3030
이니텍	www.initech.com	(02) 6445-7000
㈜ 코리아닷컴	www.makeshop.co.kr	(02) 2026-2300
케이사인	www.ksign.com	(02) 564-0182
코스콤	www.signkorea.co.kr	1577-7337
팬타시큐리티	www.pentasecurity.com	(02) 780-7728
한국기업보안	www.ucert.co.kr	(02) 514-7786
한국정보인증	www.sgssl.net	(02) 360-3065

Ⅱ

SSL 방식 보안서버 구축하기

1 소개 및 구축 절차

2 웹서버 종류별 SSL보안서버 구축

3 웹페이지 수정 방법 및 사례

4 오류 발생 시 대처방법

5 웹사이트 운영 · 관리상의 유의사항

Ⅱ SSL 방식 보안서버 구축하기

1. 소개 및 구축 절차

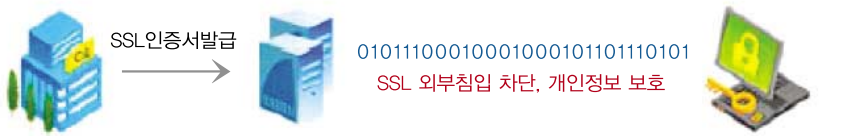
1.1 개요

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

SSL방식은 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 2-1 SSL 방식의 보안서버 개념도

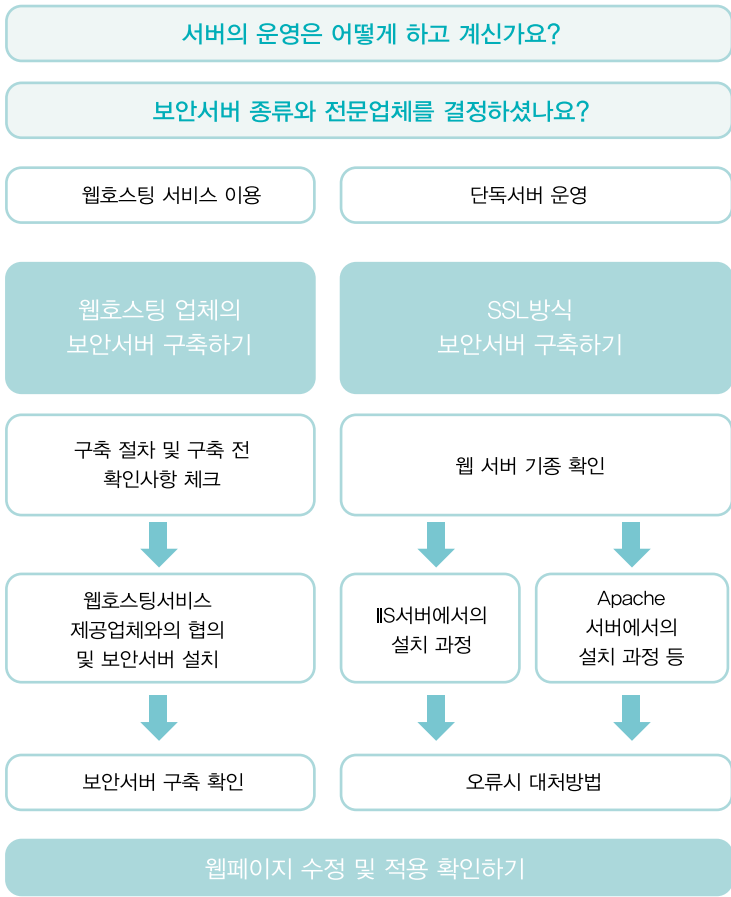


인증기관(Certification Authorities)에서 제공하는 SSL 인증서를 발급받아 웹 서버에 설치하게 되면 웹사이트 이용자들의 거래, ID/패스워드, 개인정보 등을 암호화하여 송수신할 수 있습니다.

1.2 보안서버 구축 절차

SSL 방식의 보안서버 구축 절차는 다음과 같습니다.

그림 2-2 SSL방식 보안서버 구축 절차



2. 웹서버 종류별 SSL보안서버 구축

2.1 Apache 서버에서 보안서버 구축하기

1) Apache mod_ssl 모듈 설치확인

SSL 인증서를 설치 하기 위해서 먼저 Apache에 mod_ssl 모듈이 설치가 되어 있어야 합니다. Apache 2버전 이상의 웹서버는 동적과 정적방식으로 설치를 지원하고 있고, mod_ssl 모듈이 설치되어 있지 않은 경우는 Apache 재설치를 필요로 합니다.

Apache가 설치된 경로가 /usr/local/apache 라고 가정하고 진행하겠습니다.

〈정적설치 확인〉

```
[root@#] /usr/local/apache/bin/httpd -l
Compiled-in modules:
  mod_ssl.c
    []
```

정적설치는 위와 같이 모듈이 설치되었음을 확인할 수 있습니다.

〈동적설치 확인〉

```
[root@]# /usr/local/apache/bin/httpd -l
Compiled-in modules:
  mod_so.c
    []
```

동적설치는 위와 같이 모듈이 설치되었음을 확인할 수 있습니다.

2) SSL 설정

이제부터 설명의 편의상 apache가 설치된 경로를 [$Apache_home]으로 명시하겠습니다.

Apache의 SSL 설정은 주로 [$Apache_home]/conf/extra/ httpd-ssl.conf 파일에서 이루어 집니다. 먼저 Apache 환경파일인 [$Apache_home]/conf/httpd.conf 설정에 httpd-ssl.conf 파일을 참조하도록 하겠습니다.

mod_ssl.so 모듈존재 확인

```
[root@]# ls -l /usr/local/apache/modules
mod_authn_file.so       mod_dav_fs.so       mod_imagemap.so      mod_rewrite.so
libphp5.so              mod_authz_dbm.so    mod_dbd.so           mod_include.so       mod_setenvif.so
mod_actions.so          mod_authz_default.so mod_deflate.so      mod_info.so          mod_speling.so
mod_alias.so            mod_authz_groupfile.so mod_dir.so        mod_jk.so            mod_ssl.so
mod_asis.so             mod_authz_host.so   mod_dumpio.so        mod_log_config.so    mod_status.so
mod_auth_basic.so       mod_authz_owner.so  mod_env.so           mod_log_forensic.so  mod_substitute.so
mod_auth_digest.so      mod_authz_user.so   mod_expires.so       mod_logio.so         mod_unique_id.so
mod_authn_anon.so       mod_autoindex.so    mod_ext_filter.so    mod_mime.so          mod_userdir.so
mod_authn_dbc.so        mod_cern_meta.so    mod_filter.so        mod_mime_magic.so    mod_usertrack.so
mod_authn_dbm.so        mod_cgi.so          mod_headers.so       mod_negotiation.so   mod_version.so
mod_authn_default.so    mod_dav.so          mod_ident.so         mod_reqtimeout.so    mod_vhost_alias.so
mod_ssl.so 존재 확인
```

Apache 환경파일 확인

```
[root@]# vi /usr/local/apache/conf/httpd.conf
```

내용 중 중간에 동적모듈 명시된 리스트 중 mod_ssl.so 확인

```
Dynamic Shared Object (DSO) Support

LoadModule  version_module modules/mod_version.so
LoadModule  ssl_module modules/mod_ssl.so
LoadModule  mime_module modules/mod_mime.so
```

```
[root@[$Apache_home/conf]# vi httpd.conf
```

내용 중 하단 부분으로 이동하셔서

```
# User home directories
#Include conf/extra/httpd-userdir.conf

# Real-time info on requests and configuration
#Include conf/extra/httpd-info.conf

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

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

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

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

# Secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf                    <------ # 제거함으로써 참조 선언.
```

:wq 로 저장하시고 httpd-ssl.conf 가 있는 폴더로 이동합니다.

```
[root@[$Apache_home/conf]# cd extra
[root@[$Apache_home/conf/extra]# vi httpd-ssl.conf
```

다음 httpd-ssl.conf 파일 내용을 살펴보도록 하겠습니다.

httpd-ssl.conf 내용 (// 표시는 설명입니다. 아래의 내용은 예를 든 것입니다.)

```
Listen 443   //사용하실 SSL통신포트 (기본포트 443입니다)

AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl    .crl

SSLPassPhraseDialog  "exec:/usr/local/apache2/ssl/ssl_pass.sh"  //인증서비밀번호script
위치
#SSLPassPhraseDialog  builtin                                  //수동입력시 주석제거
#SSLSessionCache          "dbm:/usr/local/apache2/logs/ssl_scache"
SSLSessionCache         "shmcb:/usr/local/apache2/logs/ssl_scache(512000)"
SSLSessionCacheTimeout  300
SSLMutex  "file:/usr/local/apache2/logs/ssl_mutex"
```

```
NameVirtualHost *:443  //주로 *자리에 서버IP를 명시합니다.

<VirtualHost *:443>      //주로 *자리에 서버IP를 명시합니다.

DocumentRoot "/home/www.test.co.kr/public_html"  //홈페이지 파일 위치
ServerName www.test.co.kr:443  // 도메인 이름
ServerAdmin  test@test.co.kr   //관리자 메일 주소
ErrorLog "/usr/local/apache2/logs/ssl_error_log"      // SSL 에러로그 파일
TransferLog "/usr/local/apache2/logs/ssl_access_log" //SSL access 로그 파일

 <Directory "/home/ www.test.co.kr/public_html">      // 디렉토리 설정
   AllowOverride FileInfo AuthConfig Limit Indexes
   Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
   <Limit GET POST OPTIONS>
       Order allow,deny
       Allow from all
   </Limit>
   <LimitExcept GET POST OPTIONS>
       Order deny,allow
       Deny from all
   </LimitExcept>
```

```
</Directory>

 SSLEngine on                    //SSL 엔진 사용
 SSLCipherSuite
 ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
 SSLCertificateFile "/usr/local/apache2/ssl/ www.uoert.co.kr .crt"  //인증서 파일 위치
 SSLCertificateKeyFile "/usr/local/apache2/ssl/ www.uoert.co.kr .key"   //키 파일 위치
 SSLCertificateChainFile "/usr/local/apache2/ssl/ www.uoert.co.kr.ca-bundle"//chain 인증서
 SSLCACertificateFile "/usr/local/apache2/ssl/ www.uoert.co.kr.root-bundle" //root인증서

 <FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
 </FilesMatch>
 <Directory "/usr/local/apache2/cgi-bin">
    SSLOptions +StdEnvVars
 </Directory>
 BrowserMatch ".*MSIE.*" \
         nokeepalive ssl-unclean-shutdown \
         downgrade-1.0 force-response-1.0
CustomLog "/usr/local/apache2/logs/ssl_request_log" \
          "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"

</VirtualHost>
:wq
```

이제 httpd-ssl.conf 파일에 명시한 대로 인증서 위치를 생성하는 작업을 하셔야 합니다.

폴더가 없다면 생성을 합니다.

[root@[$Apache_home]# mkdir-p /usr/local/apache2/ssl

받은 인증서를 ssl 폴더로 이동시킵니다. 받은 인증서가 있는 위치로 이동하신 후에 [root@~]# mv [파일] [이동위치] 형식으로 파일을 하시면 됩니다.

Ex) mv www.test.co.kr.crt /usr/local/apache2/ssl/

SSL인증서 패스워드 자동입력 shell script 제작을 해 보도록 하겠습니다.

예를 든 httpd-ssl.conf 에 파일 위치를 /usr/local/apache2/conf/ssl 으로 명시 했으므로 해당 폴더로 이동 후 생성합니다.

[root@[$Apache_home/ssl]# vi pass.sh 아래와 같이 입력 후 저장합니다.

```
#!bin/sh
echo "패스워드"
```

이제 pass.sh 파일의 퍼미션을 지정합니다.

[root@[$Apache_home/ssl]# chmod a+x pass.sh //root만 권한 준다면 chmod 700을 입력합니다.

이제 아파치를 재구동하여 SSL를 적용하는 작업이 남았습니다. 먼저 설정 문법에 오류가 있는지 체크합니다. $Apache_home/bin 폴더로 이동합니다.

```
[root@[$Apache_home/bin]#./apachectl configtest
Syntax OK
```

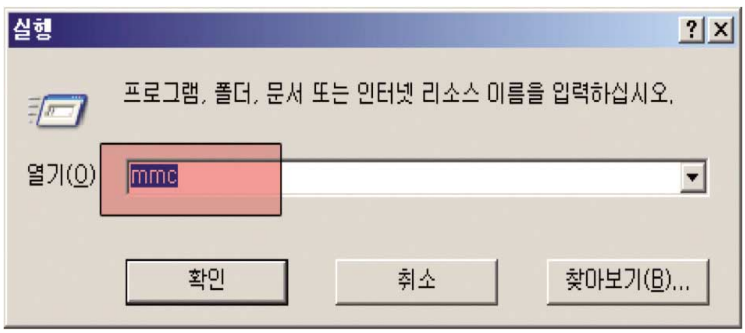
OK가 뜬다면 설정에 문제없이 설정되어 있다는 의미입니다.

2.2 IIS 5.0 서버에서 보안서버 구축하기

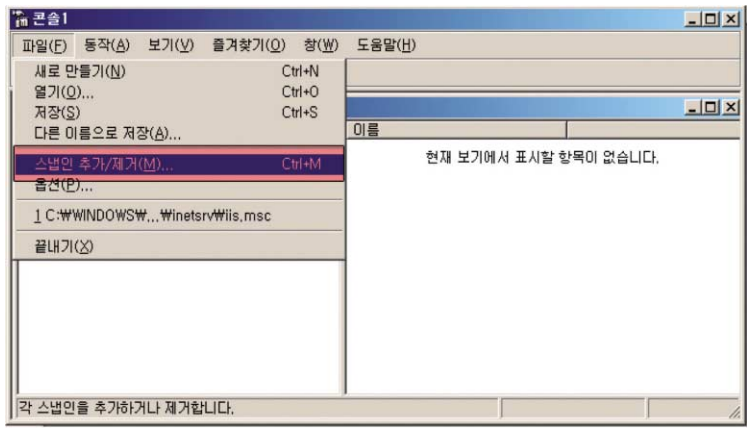
※ IIS 5.0 은 WildCard, Multi 인증서 사용은 가능하지만 중복포트를 지원하지 않습니다.

1) 스냅인 추가

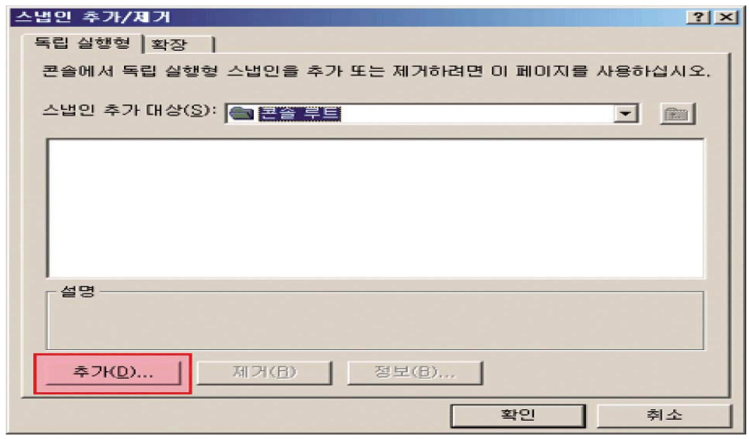
❶ 시작 → 실행 → mmc 를 입력 한 후 확인을 클릭 합니다.



❷ 파일 → 스냅인 추가/제거(M) 선택 하거나 단축키 Ctrl+M을 입력 합니다.

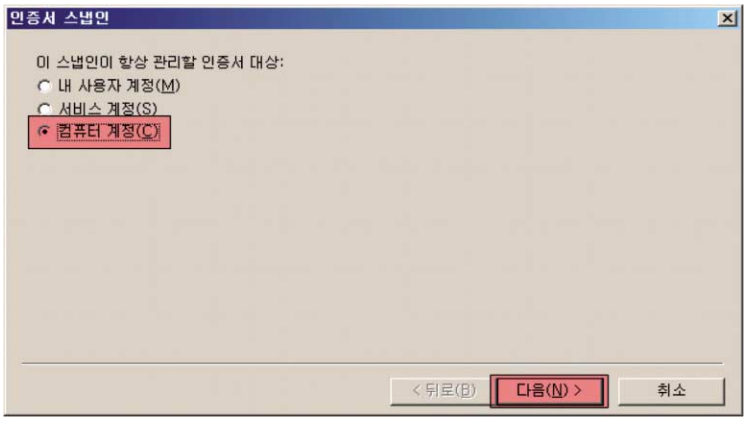


❸ 추가를 클릭 합니다.

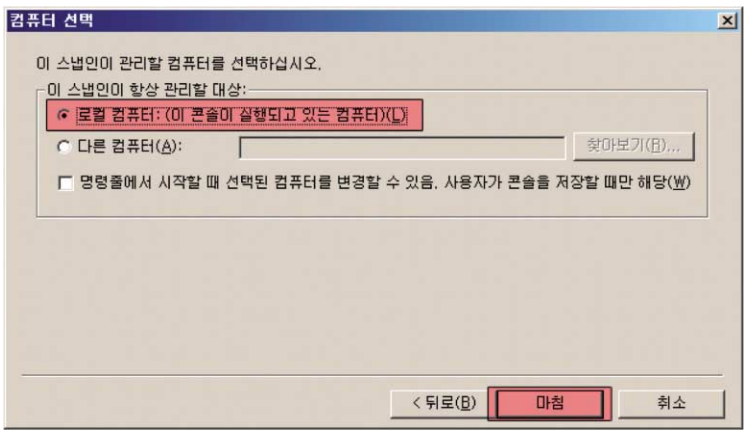


❹ 인증서 선택 후 추가를 클릭 합니다.

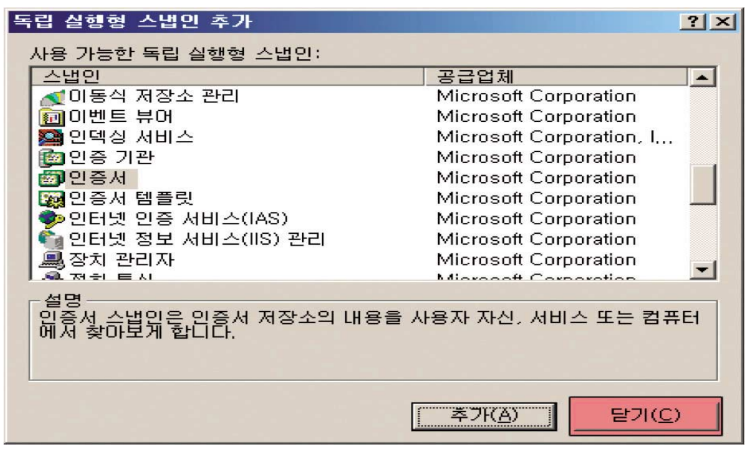
❺ 컴퓨터 계정을 선택 후 다음을 클릭 합니다.



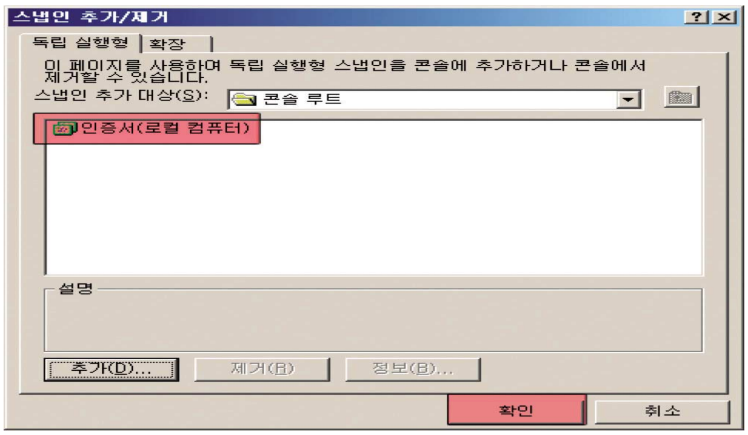
❻ 로컬 컴퓨터: (이 콘솔이 실행되고 있는 컴퓨터(L)을 선택 후 마침을 클릭 합니다.



❼ 닫기를 클릭 합니다.



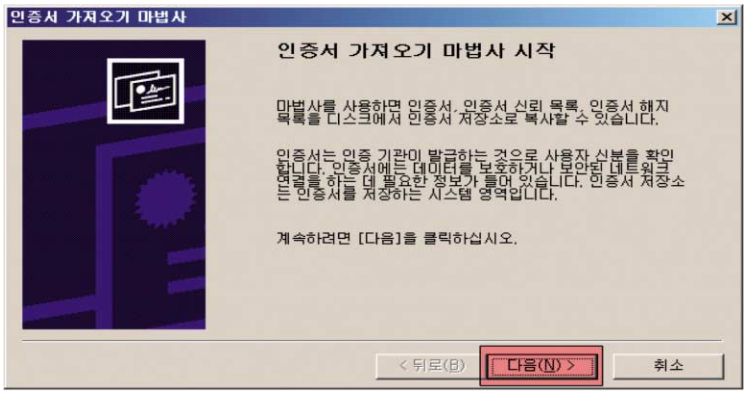
❽ 인증서(로컬 컴퓨터)가 등록 되었는지 확인 후 확인을 클릭 합니다.



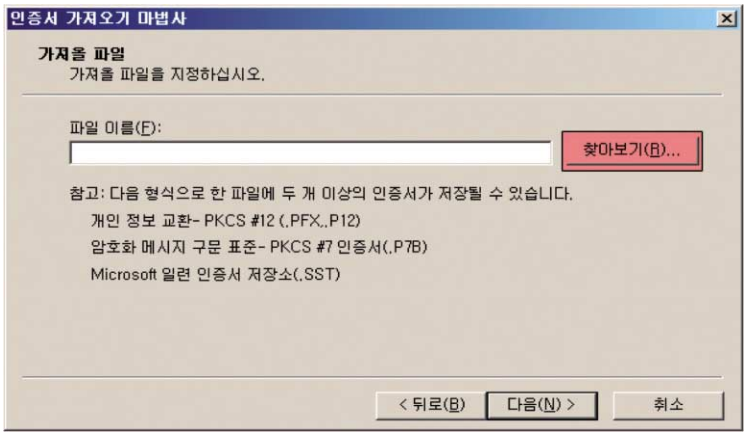
2) PFX파일 불러오기

❶ 콘솔 루트 → 인증서(로컬 컴퓨터) → 개인 → 오른쪽 마우스 클릭 → 모든 작업(K) → 가져오기(I)를 클릭 합니다.

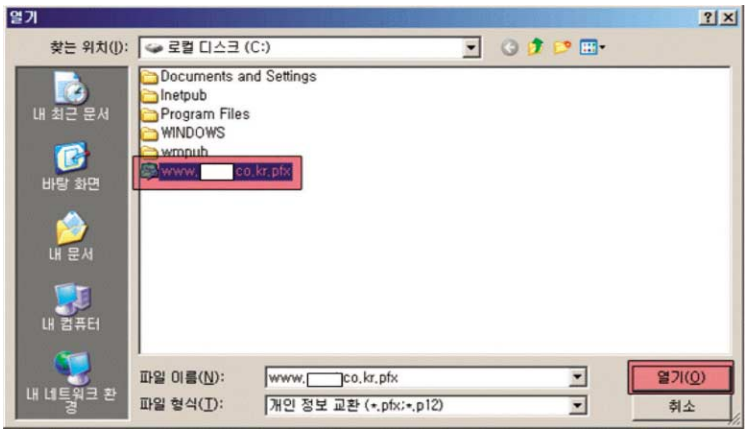
❷ 다음을 클릭 합니다.



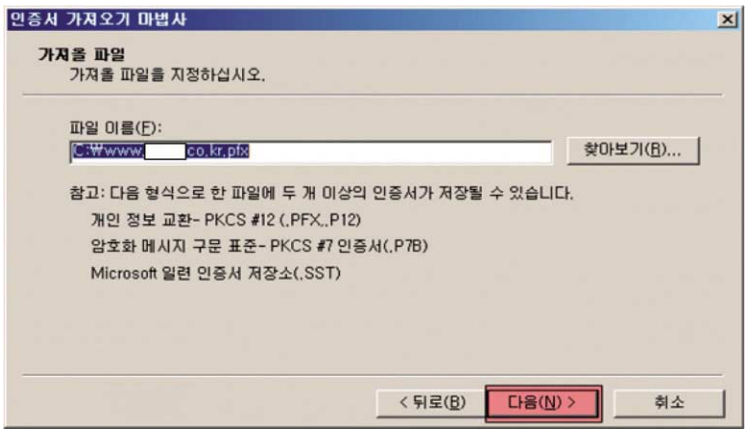
❸ 찾아보기(R)을 클릭 합니다.



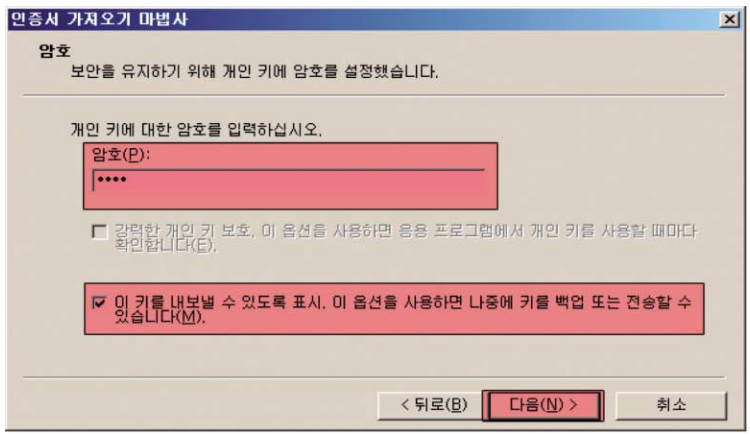
❹ 발급 받은 인증서를 선택 후 열기를 클릭 합니다.



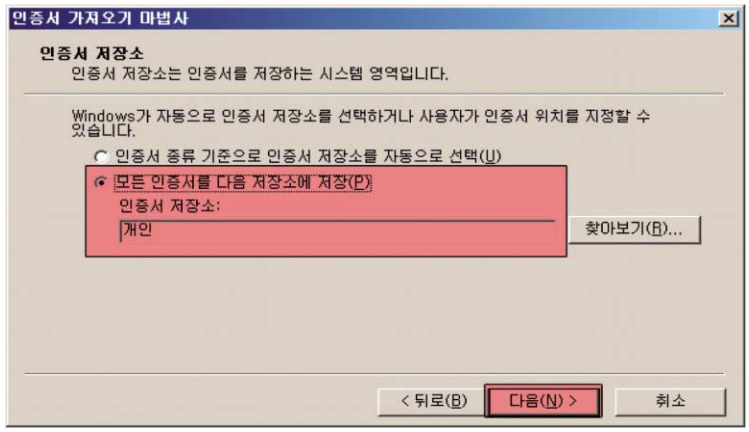
❺ 다음을 클릭 합니다.



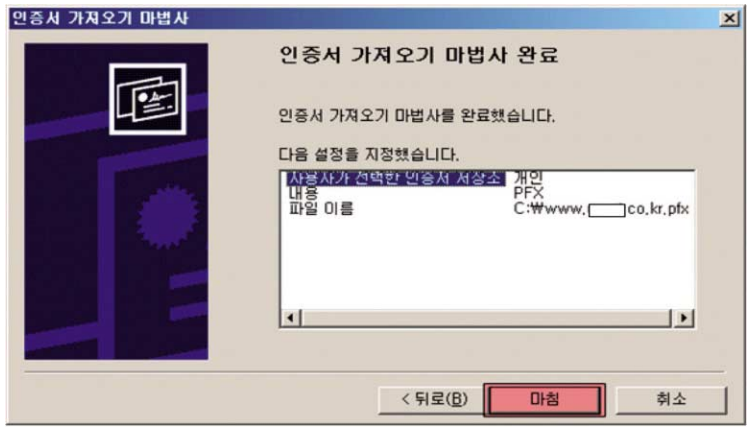
❻ 암호를 입력 후 이 키를 내보낼 수 있도록 표시를 체크 후 다음을 클릭 합니다.



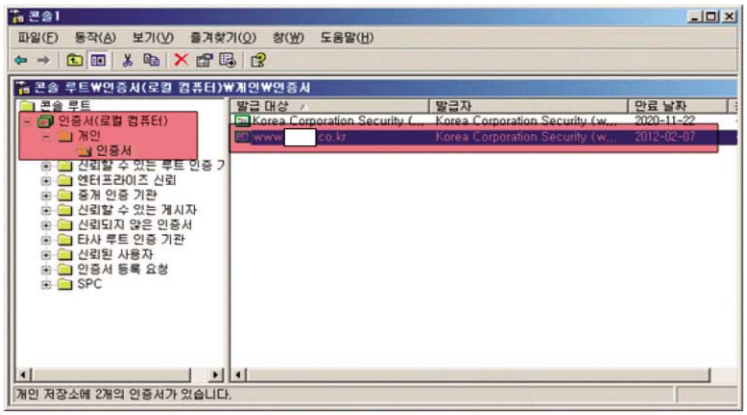
❼ 인증 저장소가 개인인지 확인 후 다음을 클릭 합니다.



❽ 마침을 클릭 합니다.

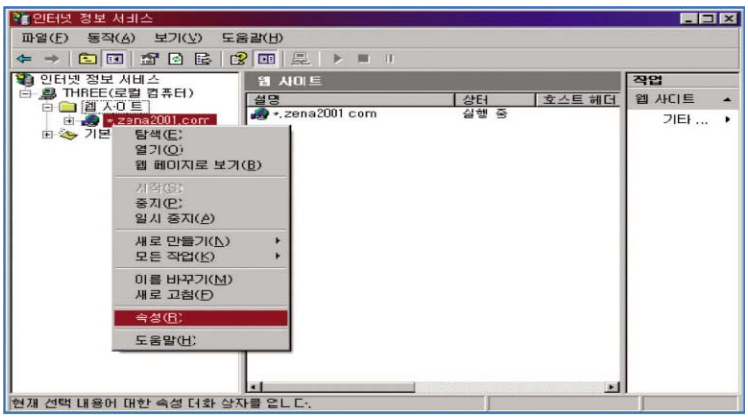


⑨ 인증서가 정상적으로 등록 되었는지 확인 합니다.

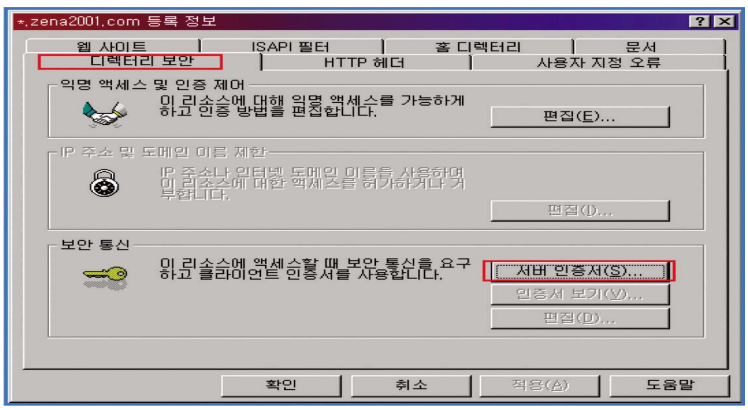


3) 인증서 설치하기

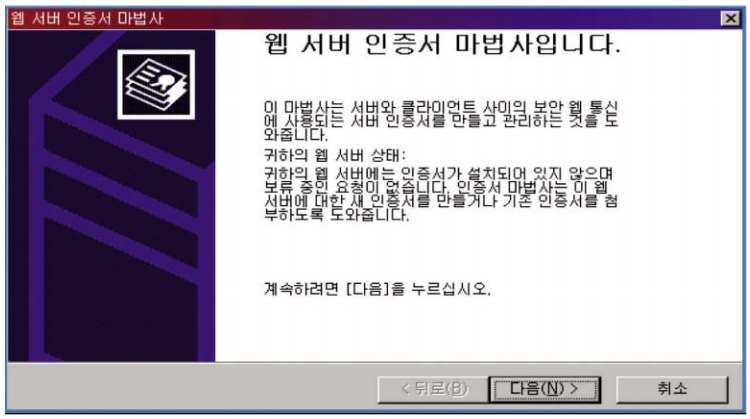
❶ IIS 5.0의 웹사이트의 속성을 클릭합니다.



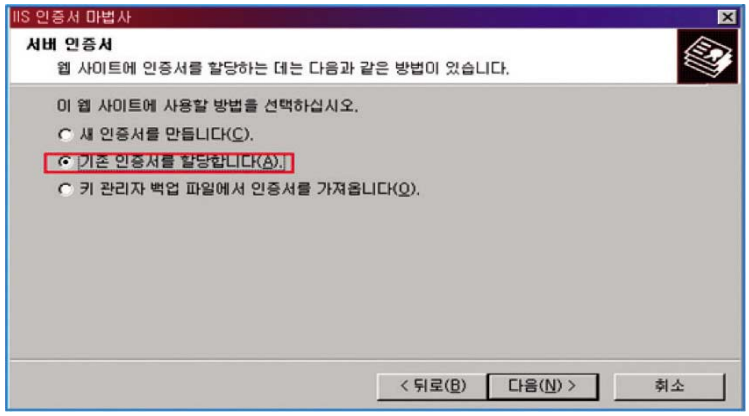
❷ 디렉터리 보안을 선택 후 서버인증서를 선택합니다.



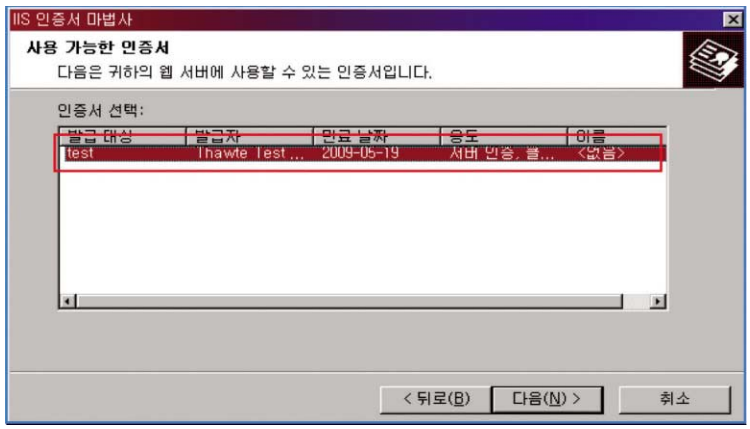
❸ 다음을 클릭합니다.



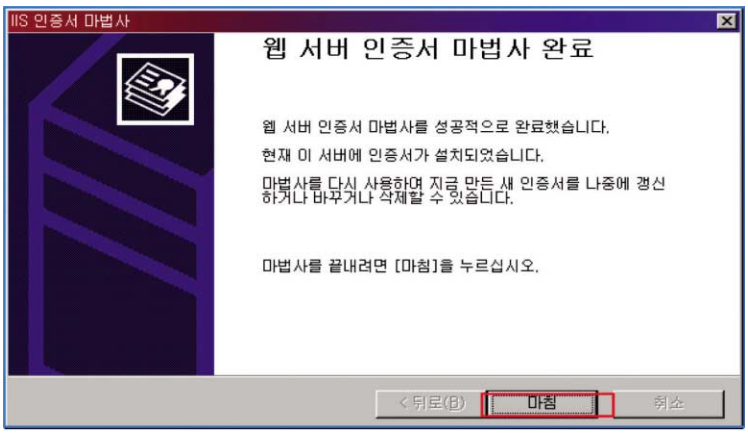
❹ 기존 인증서를 할당합니다(A)를 선택하고 다음을 선택합니다.
갱신의 경우에는 "새 인증서를 만듭니다.(C)"를 선택하고 다음을 선택합니다.



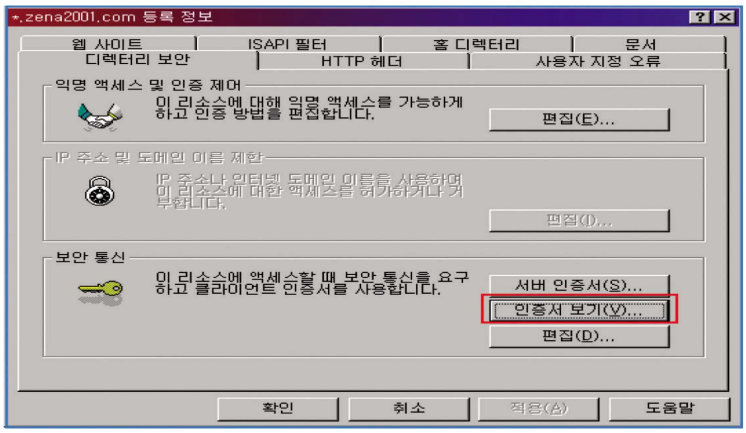
❺ 해당 웹사이트의 도메인과 만료날짜가 맞는 해당 인증서를 찾아 할당합니다.



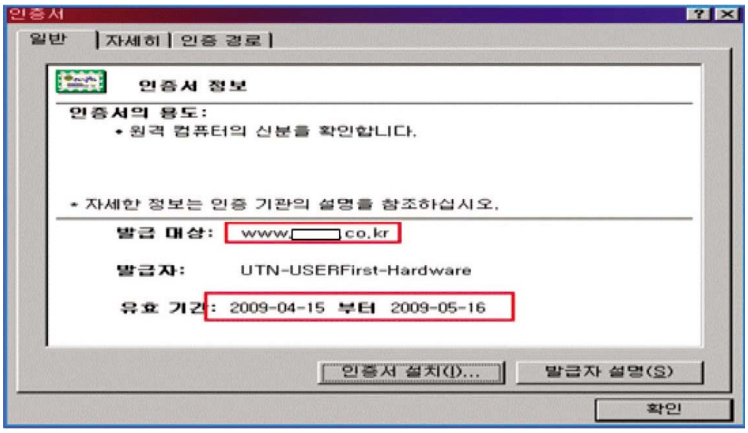
⑥ 마침을 클릭합니다



⑦ 인증서 보기를 클릭합니다.



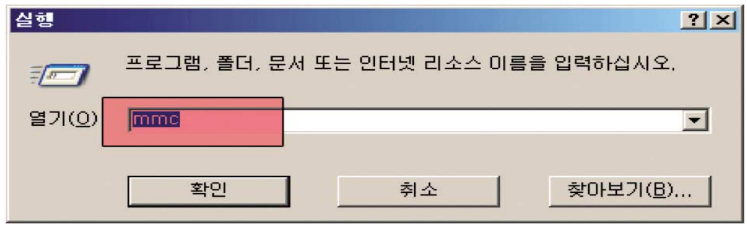
⑧ 발급대상 도메인과 인증유효기간이 맞는지 확인합니다.



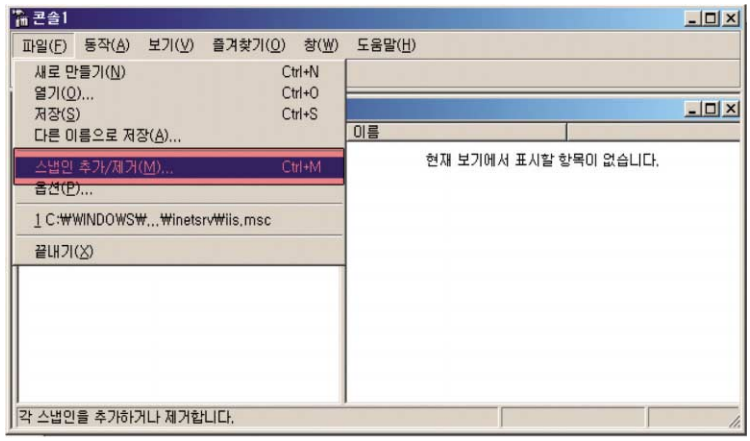
2.3 IIS 6.0 서버에서 보안서버 구축하기

1) 스냅인 추가

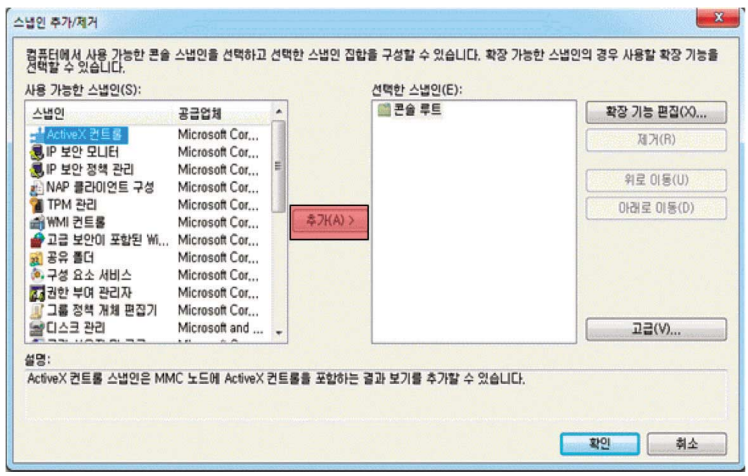
❶ 시작 → 실행 → mmc 를 입력 한 후 확인을 클릭 합니다.



❷ 파일 → 스냅인 추가/제거(M) 선택 하거나 단축키 Ctrl+M을 입력 합니다.

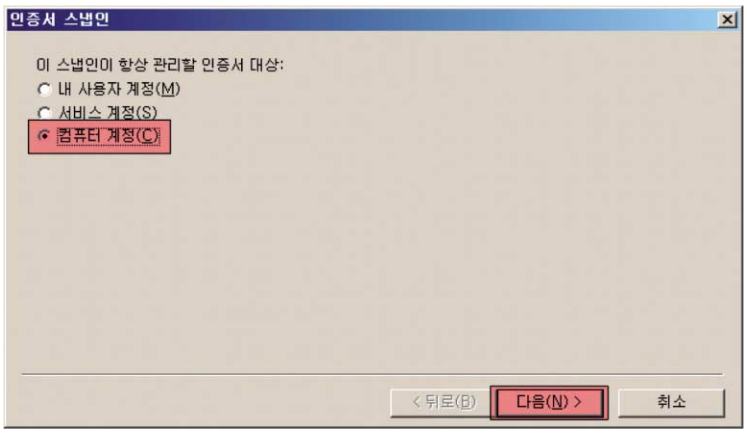


❸ 추가를 클릭 합니다.

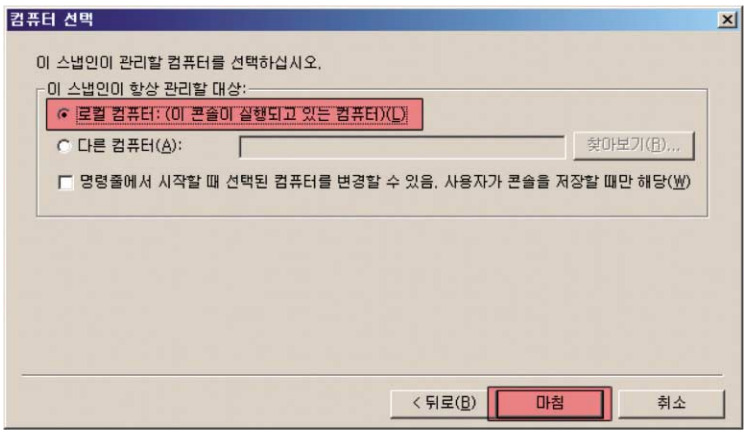


❹ 인증서 선택 후 추가를 클릭 합니다.

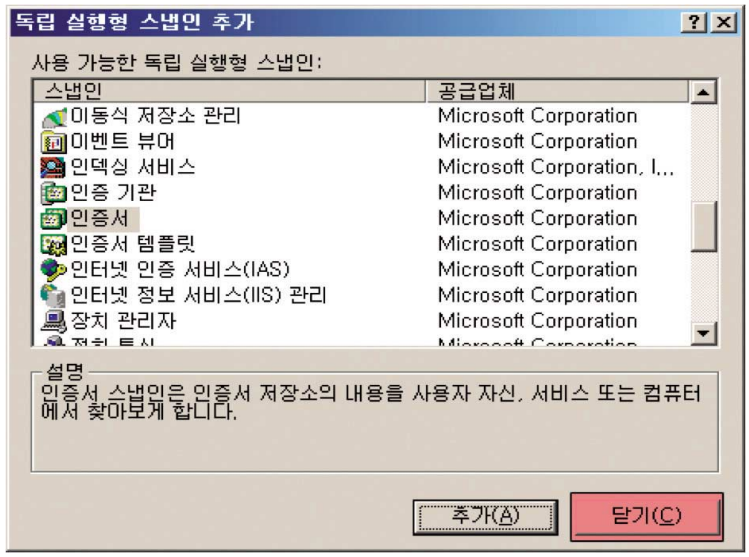
❺ 컴퓨터 계정을 선택 후 다음을 클릭 합니다.



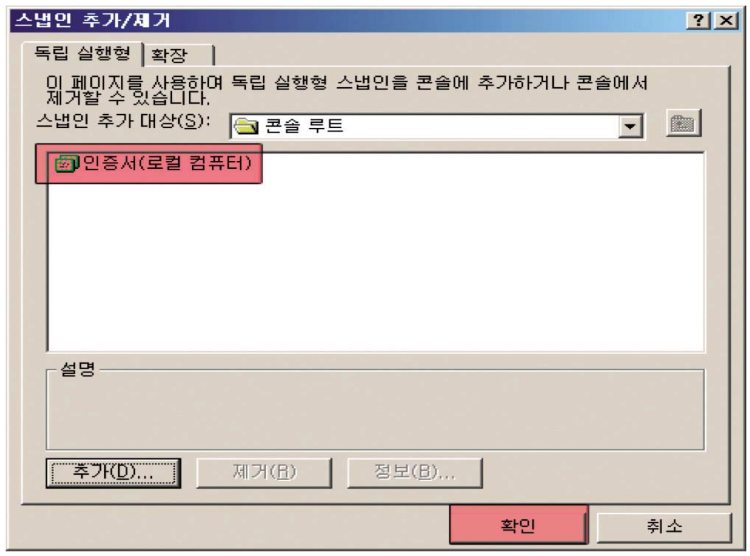
❻ 로컬 컴퓨터: (이 콘솔이 실행되고 있는 컴퓨터(L)을 선택 후 마침을 클릭 합니다.



❼ 닫기를 클릭 합니다.

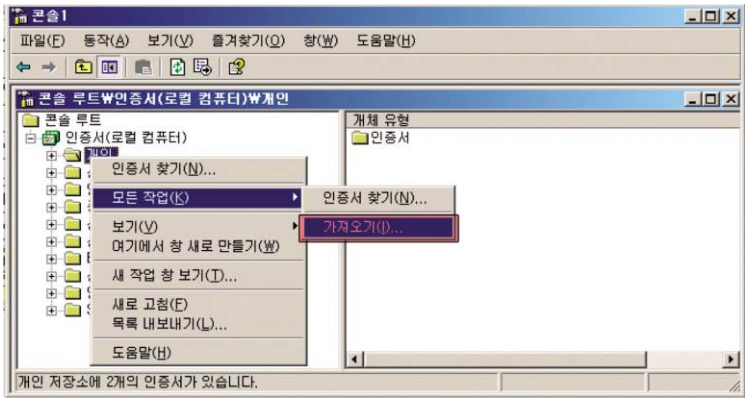


❽ 인증서(로컬 컴퓨터)가 등록 되었는지 확인 후 확인을 클릭 합니다.

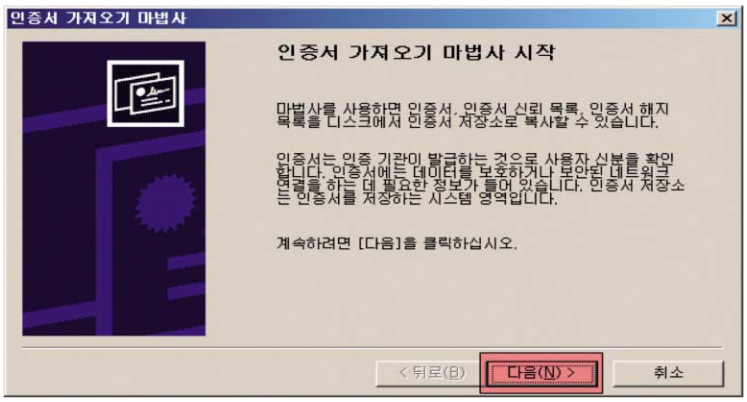


2) PFX파일 불러오기

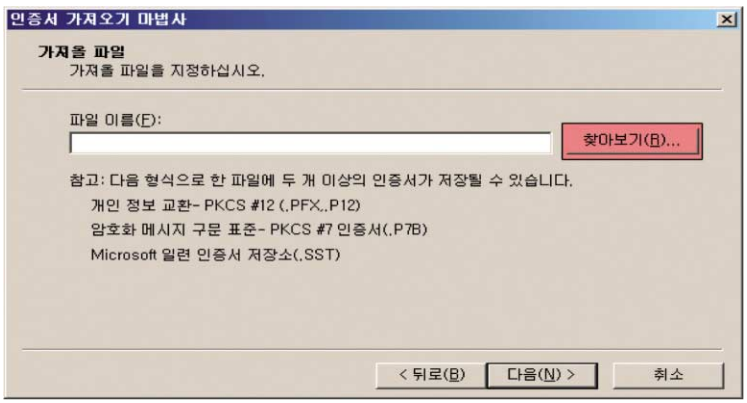
❶ 콘솔 루트 → 인증서(로컬 컴퓨터) → 개인 → 오른쪽 마우스 클릭 → 모든 작업(K) → 가져오기(I)를 클릭 합니다.



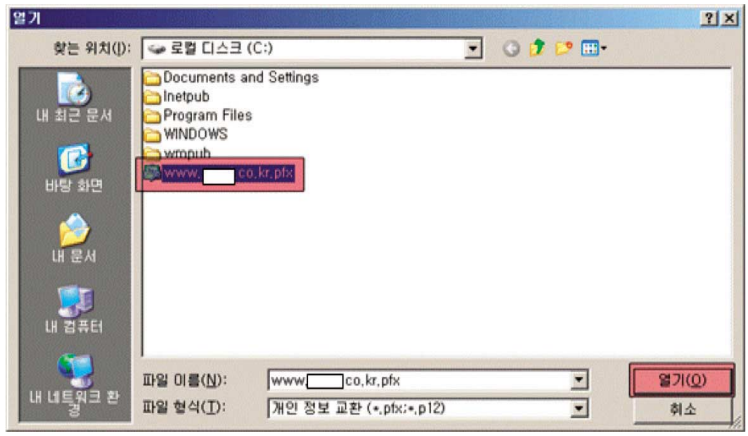
❷ 다음을 클릭 합니다.



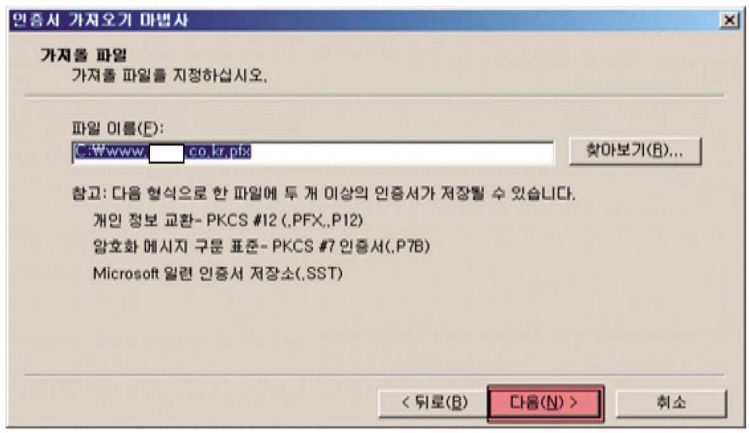
❸ 찾아보기(R)을 클릭 합니다.



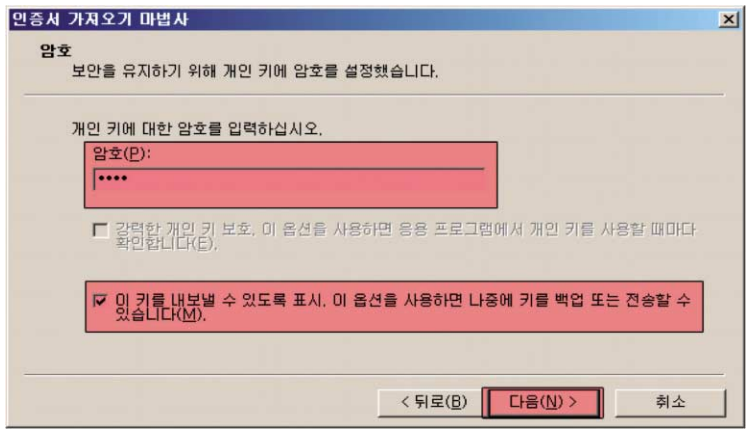
❹ 발급 받은 인증서를 선택 후 열기를 클릭 합니다.



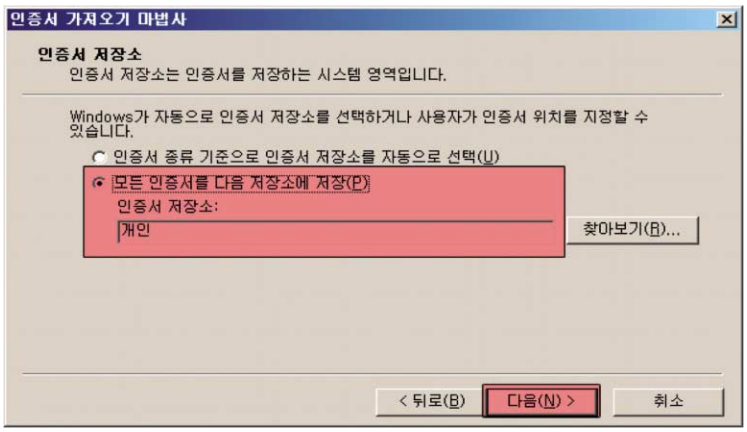
❺ 다음을 클릭 합니다.



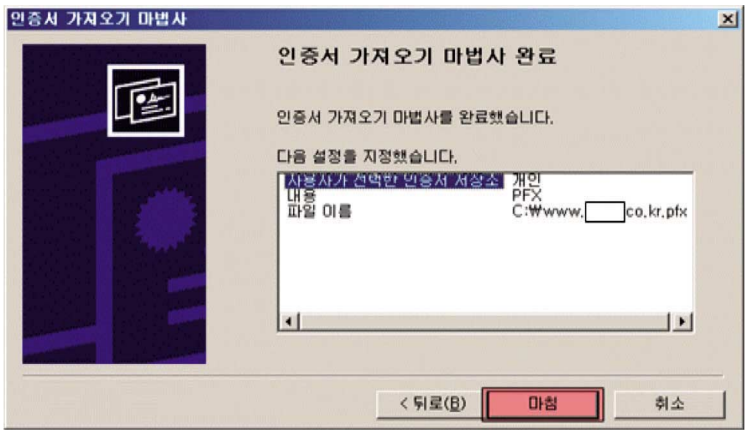
❻ 암호를 입력 후 이 키를 내보낼 수 있도록 표시를 체크 후 다음을 클릭 합니다.



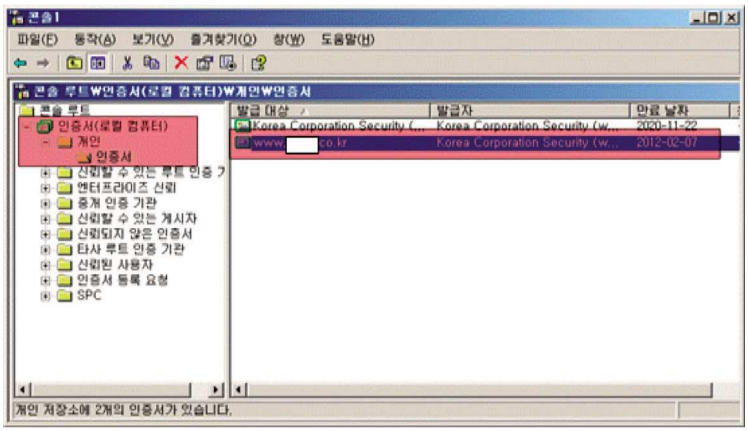
⑦ 인증 저장소가 개인인지 확인 후 다음을 클릭 합니다.



⑧ 마침을 클릭 합니다.

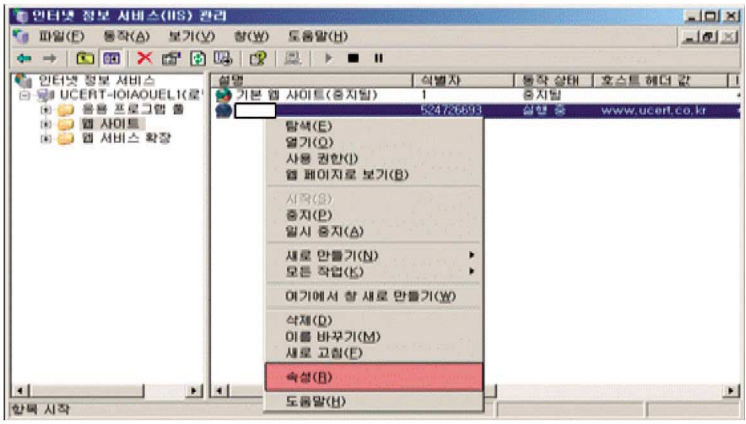


⑨ 인증서가 정상적으로 등록 되었는지 확인 합니다.

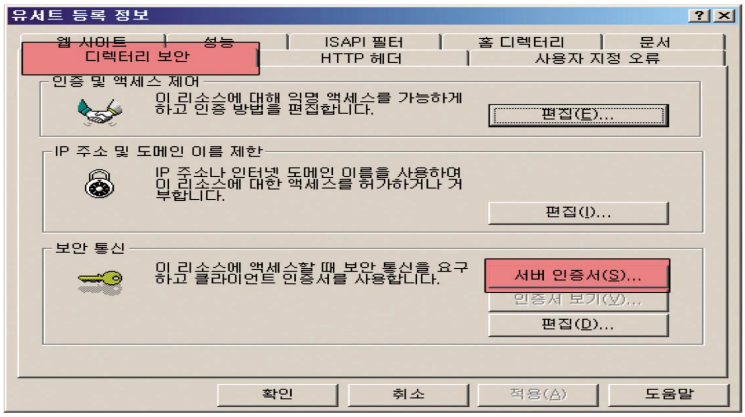


3) 인증서 설치

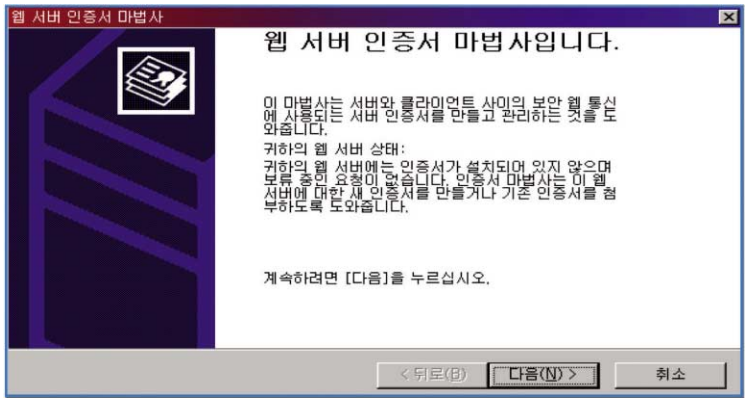
❶ IIS를 실행하여 적용 하실 사이트를 마우스 오른쪽으로 클릭 후 속성을 클릭합니다.



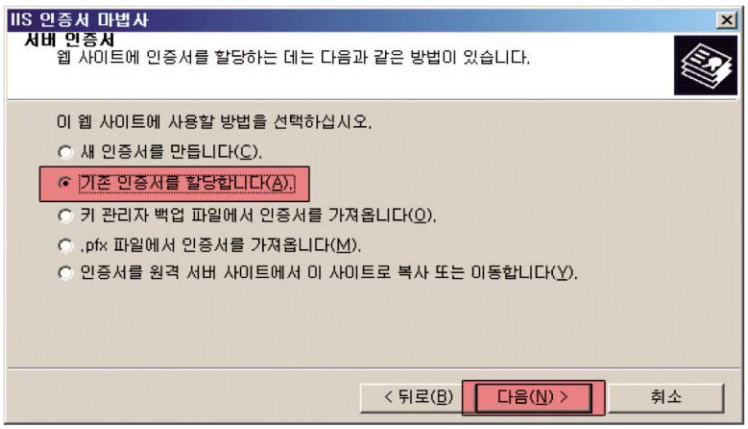
❷ 디렉터리 보안탭을 선택 후 서버 인증서(S)를 클릭 합니다.



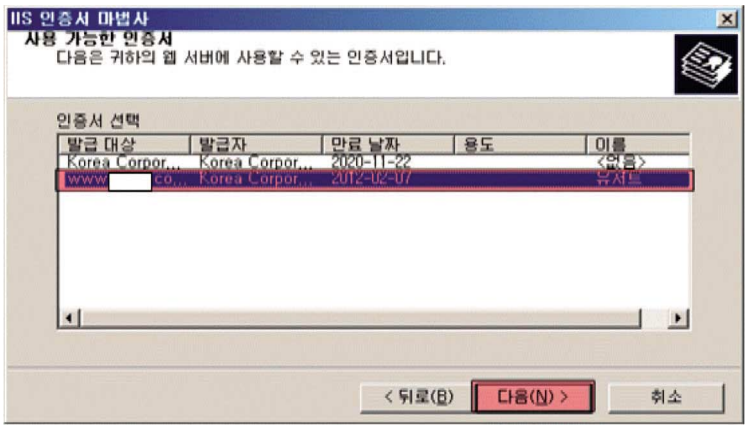
❸ 다음을 클릭합니다.



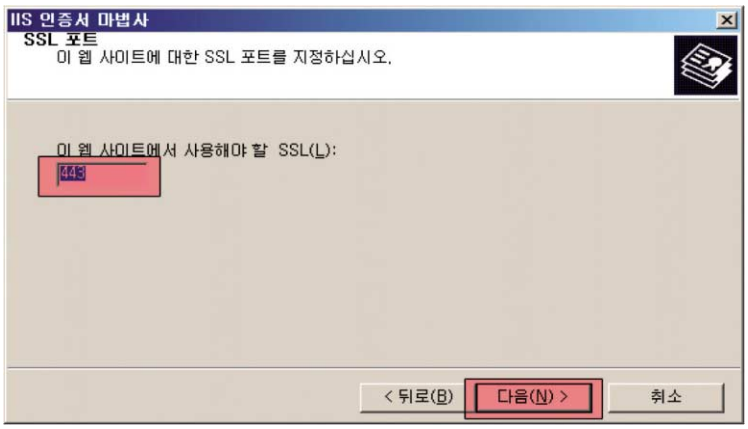
❹ 기존 인증서를 할당합니다.를 선택 후 다음을 클릭 합니다.



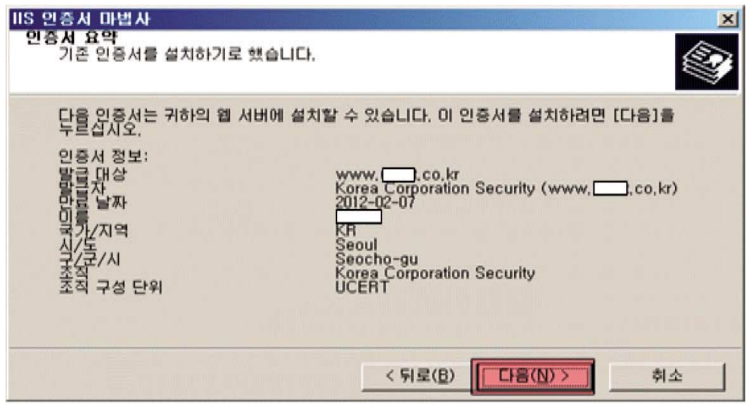
❺ 등록 하였던 인증서를 선택 후 다음을 클릭 합니다.



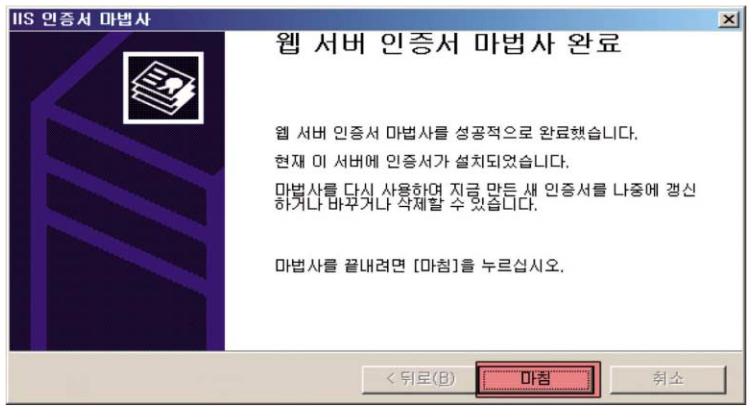
❻ SSL포트를 지정 후(기본 443) 다음을 클릭 합니다.



❼ 다음을 클릭 합니다.

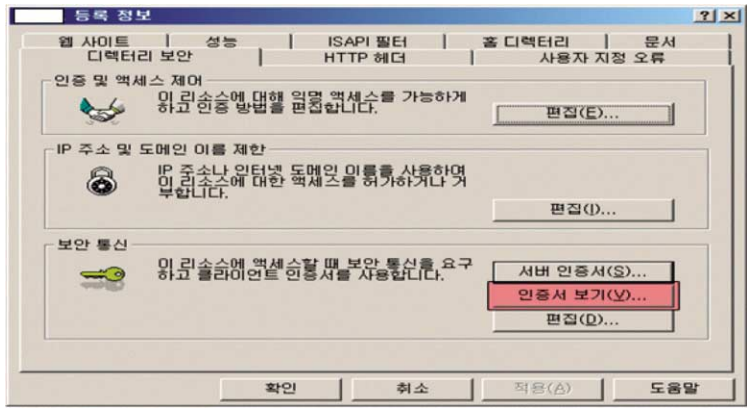


❽ 마침을 클릭 합니다.



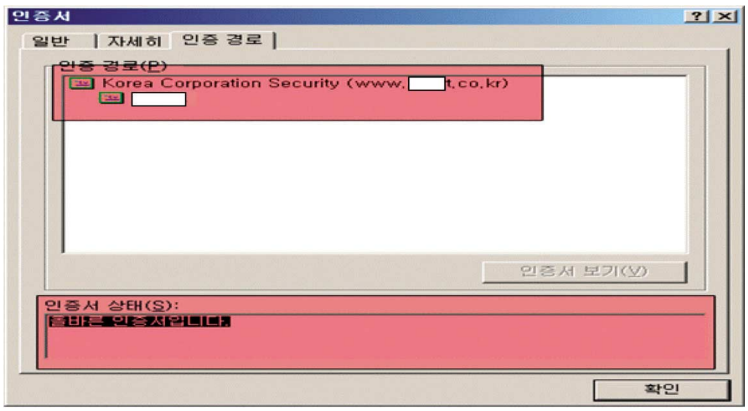
4) 인증서 확인 방법

❶ 인증서 보기(V)을 클릭 합니다.

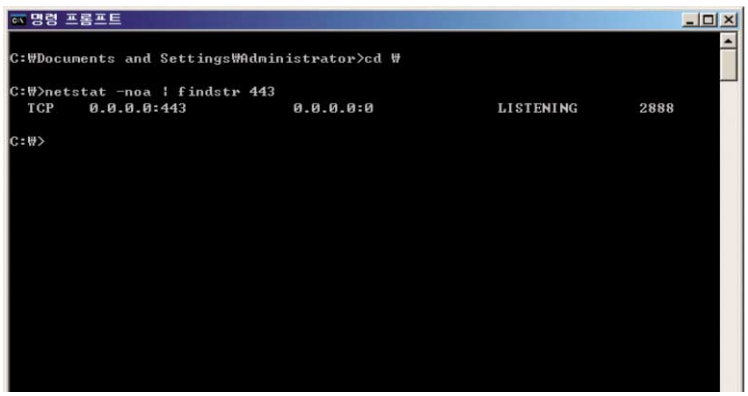


❷ 일반 탭은 발급대상/발급자 유효 기간 등을 확인 할 수 있습니다.

❸ 인증 경로 탭은 인증 경로/인증서 상태를 확인 할 수 있습니다.
("올바른 인증서입니다."일 경우 정상)



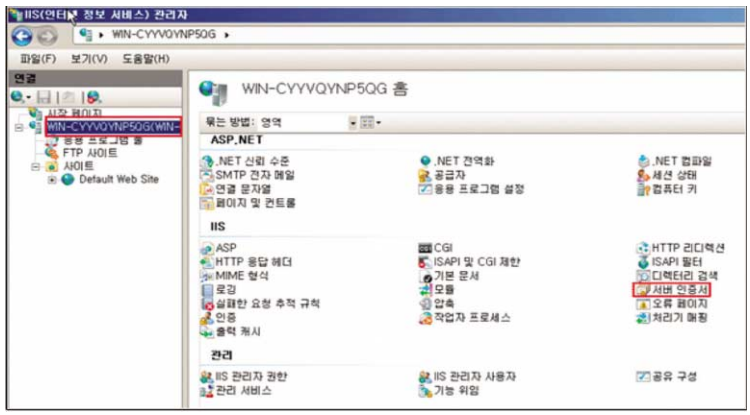
❹ 시작 → 실행 → cmd 실행 후 netstat -noa | findstr 443 으로 인증서를 설치 한 포트가 활성화 되었지는 확인 가능합니다.



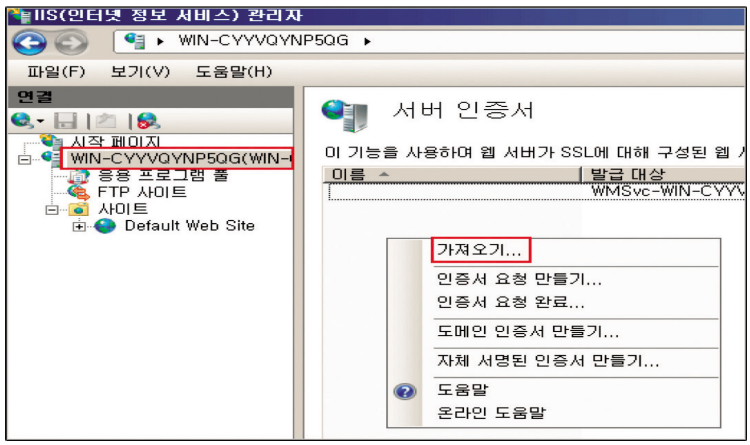
2.4 IIS 7.0 서버에서 보안서버 구축하기

1) 인증서 가져오기

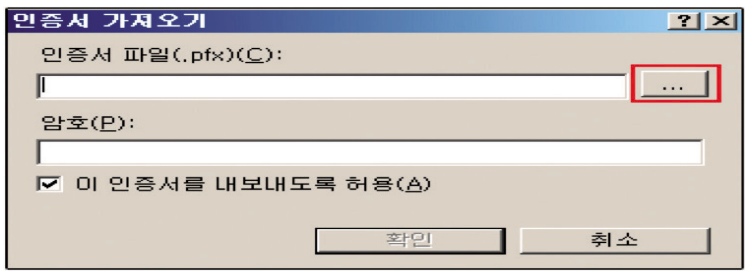
❶ [시작] 〉 [프로그램] 〉 [관리도구] 〉 [IIS(인터넷 정보 서비스)관리자]를 선택합니다.

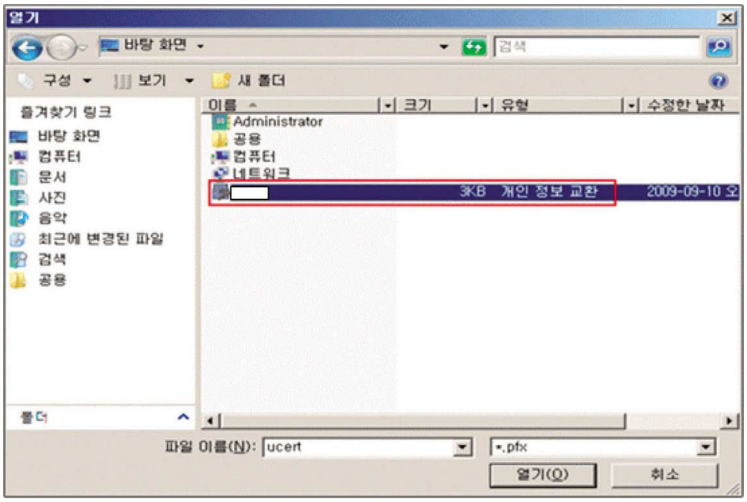


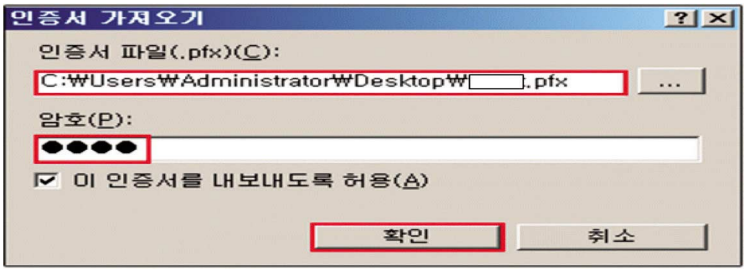
❷ 서버 인증서를 더블 클릭 〉 마우스 오른쪽 〉 가져오기를 선택합니다.



❸ 인증서 파일을 찾은 후 암호를 입력합니다.



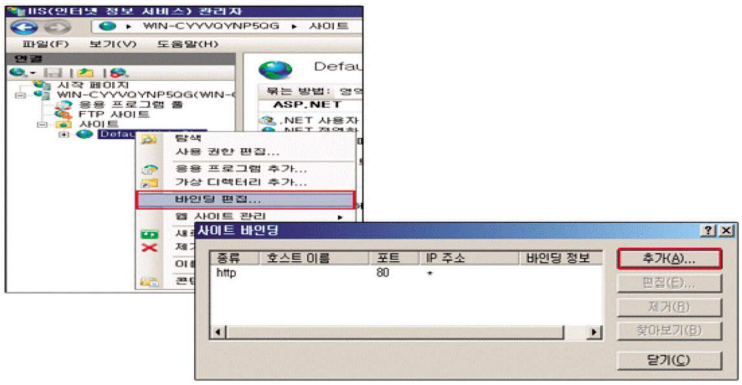




❹ 다음과 같이 인증서가 추가된 내용을 확인합니다.

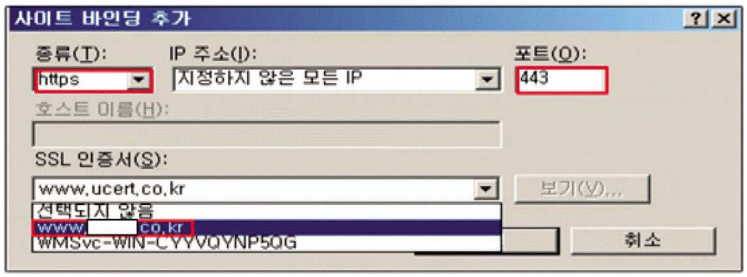
2) 인증서 설치

❶ SSL인증서를 설치 할 웹사이트 목록의 마우스 오른쪽을 클릭 하시여 바인딩 편집을 선택 합니다.

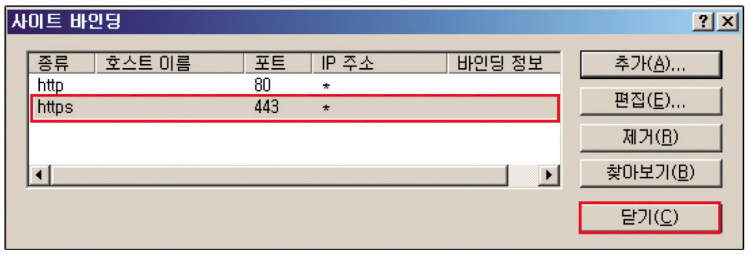


❷ 추가를 클릭하여 SSL 서비스를 클릭합니다.

– 종류: https 〉 포트번호 입력 (Default는 443입니다) 〉 SSL 인증서 항목을 확장하신 후 등록하신 인증서를 선택 합니다.



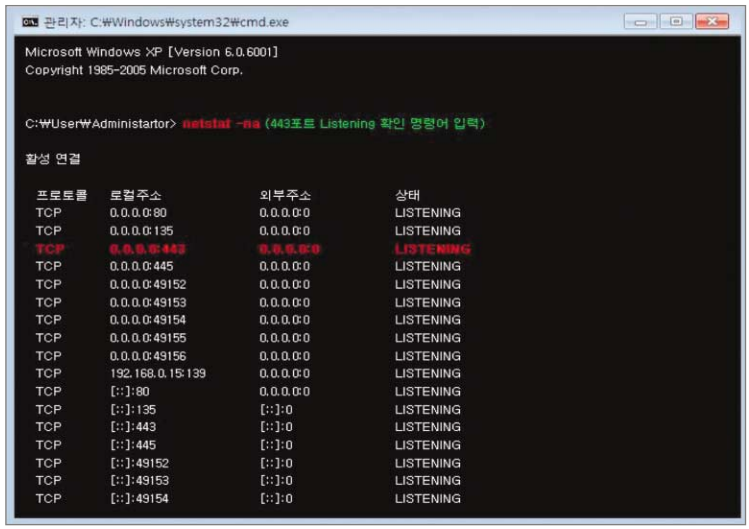
❸ 추가된 인증서를 확인하신 후 닫기를 클릭 합니다.



3) 포트 활성화 확인

❶ Netstat –na 명령어를 사용하여 443포트가 Listening되어있는지 확인합니다.

❷ 만약 활성화 상태이지만 외부에서 접속이 안 되신다면 방화벽 설정을 확인 부탁 합니다.



3. 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.

3.1 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 수정하시면 됩니다.

〈그림 2-3〉과 〈그림 2-4〉는 암호화 통신을 하기 위해 https 프로토콜을 호출하기 전과 호출한 후의 HTML 소스코드 예입니다.

●● 그림 2-3 ●● 평문 통신을 위한 HTML 소스코드

```
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 2-4 ●● https 프로토콜을 호출하기 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=
}
```

2) 리다이렉션(Redirection) 설정

앞서 설명을 하였듯이, 암호화 통신을 위해서는 https 프로토콜을 직접 호출을 해줘야 합니다. 하지만, 대부분 www.test.co.kr 또는 test.co.kr 도메인을 웹 브라우저의 주소창에 직접 입력하여 접속하는 경우가 대부분일 것입니다. 이때 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 불편할 뿐만 아니라 입력하지 않은 경우 암호화 통신이 이루어지지 않을 수 있습니다.

리다이렉션은 현재 접속한 도메인이나 혹은 웹페이지를 강제로 다른 주소나 다른 페이지로 변경해 줌으로써 사용자들의 불편함을 감소시켜주고 자연스럽게 암호화 통신을 할 수 있도록 해주는 기능입니다.

〈그림 2-5〉는 Apache 서버에서 Redirect 지시자를 써서 http://test.co.kt 또는 http://www.test.co.kr로 들어온 사용자를 강제로 https:// www.test.co.kr로 리다이렉션 시켜서 암호화 통신하는 예입니다.

그림 2-5 Apache 서버에서의 Redirection

```
<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>
```

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 2-6〉은 웹페이지의 index.html에 한줄의 소스코드를 추가함으로써 http://URL로 접속하는 사용자들을 강제로 https://URL로 리다이렉션하는 예입니다.

●● 그림 2-6 ●● HTML Tag를 이용한 Redirection

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

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

Meta tag를 이용한 방법은 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 리다이렉션 해주게 됩니다.

●● 그림 2-7 ●● Javascript를 이용한 Redirection

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

3.2 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 필요 없는 부분까지 암호화를 하여 서버의 부하를 증가시키는 것을 최대한 줄일 수 있기 때문입니다.

다음 〈그림 2-8〉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 2-8 ●● 페이지별 암호화 대상 메뉴

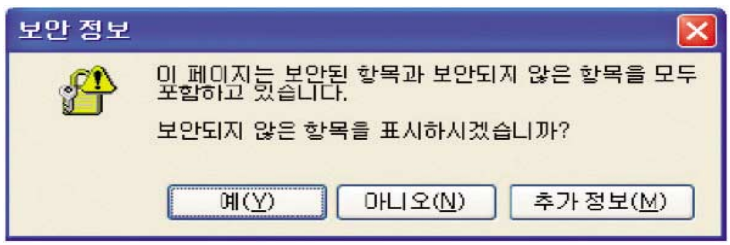
〈그림 2-9〉는 〈그림 2-8〉 메뉴 부분의 소스코드입니다. 밑줄 부분 중 첫 번째 밑줄에 해당하는 부분이 현재위치에서 메뉴를 클릭하여 이동할 때 암호화 전송을 하도록 하게끔 설정된 것이고, 두 번째 밑줄은 현재 위치에서 메뉴를 클릭하여 이동할 때 평문 전송을 하도록 설정된 것입니다.

●● 그림 2-9 ●● 페이지별 암호화 대상 메뉴의 소스코드

```
<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">
```

이렇게 페이지별로 암호화가 적용된 사이트를 방문해보면, 〈그림 2-10〉과 같은 경고창을 만나게 되는 경우가 있습니다.

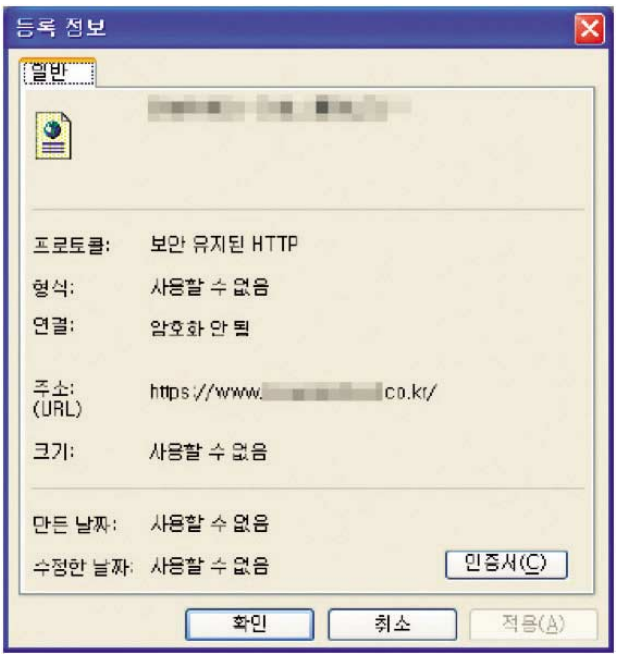
●● 그림 2-10 ●● SSL이 적용된 페이지의 경고창



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.

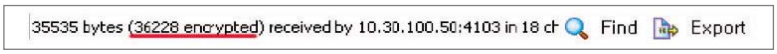
이런 경고창이 발생하는 웹페이지 속성을 보면 〈그림 2-11〉처럼 '암호화 안됨' 이라고 해서 마치 암호화가 되지 않은 평문 상태로 데이터가 전송되는 것처럼 생각되지만 웹페이지 상 전송되는 데이터를 볼 수 있는 third-parth 툴을 이용해서 확인해보면, 암호화 통신이 이루어지고 있다는 것을 알 수 있습니다.

그림 2-11 http 평문 통신 주소가 호출되는 웹페이지의 속성



〈그림 2-12〉는 third-parth 툴을 이용하여 웹페이지의 암호화 통신 여부를 확인한 화면입니다. 페이지 속성이 '암호화 안됨' 이지만 암호화 전송이 이루어지고 있음을 알 수 있습니다.

그림 2-12 웹페이지의 암호화 통신 확인



하지만 〈그림 2-10〉과 같이 경고창이 발생하게 되면, 상세한 내용을 모르고 웹사이트에 접속하는 사용자들에게 보안이 되고 있지 않다는 불신을 줄 수도 있고, 또한 계속적인 경고창으로 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

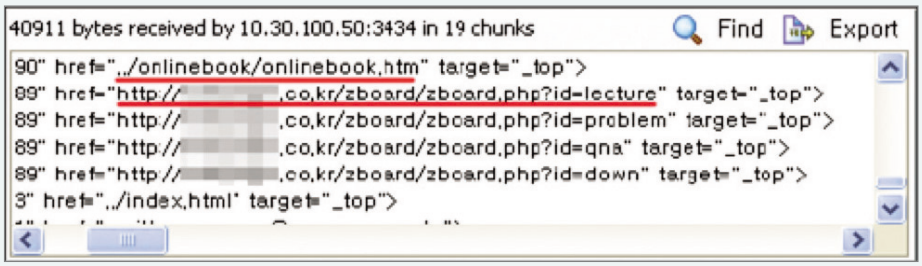
절대경로 호출과 상대경로 호출이란 무엇인가?

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 말합니다.

아래 그림에서 첫 번째 밑줄 그은 부분이 상대 경로로 호출하는 경우이고, 두 번째 밑줄 그은 부분이 절대 경로로 호출하는 경우입니다.

첫 번째의 경우에는 https 암호화 통신을 하더라도 소스코드 수정이 필요 없는 부분이고, 두 번째의 경우에는 https 암호화 통신을 할 경우 호출 URL을 http에서 https로 바꿔줘야 합니다.

만일 바꿔주지 않을 경우에는 〈그림 2-10〉과 같이 경고창이 뜨게 됩니다.



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

적용 시나리오는 〈그림 2-13〉과 같이 웹페이지(index.html)에 프레임으로 두 개의 페이지 topmenu.htm과 main.htm을 불러오는 소스코드가 있을 때 소스코드의 URL을 〈그림 2-14〉와 〈그림 2-15〉처럼 변경하고 웹 브라우저에서 http와 https로 각각 호출했을 때의 결과를 살펴보고자 합니다.

●● 그림 2-13 ●● 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="http://lab.[redacted].co.kr/test_ssl/topmenu.htm" scrol
ling="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 2-14 ●● topmenu.htm을 https로 호출하기

```
<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>
```

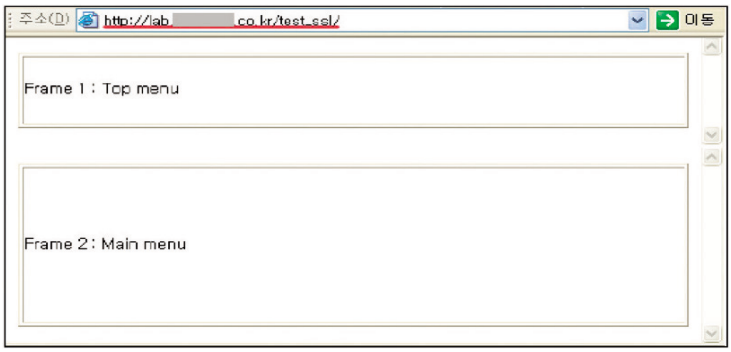
●● 그림 2-15 ●● topmenu.htm과 main.htm을 https로 호출하기

```
<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="https://lab.[redacted].co.kr/test_ssl/main.htm" scroll
ing="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>
```

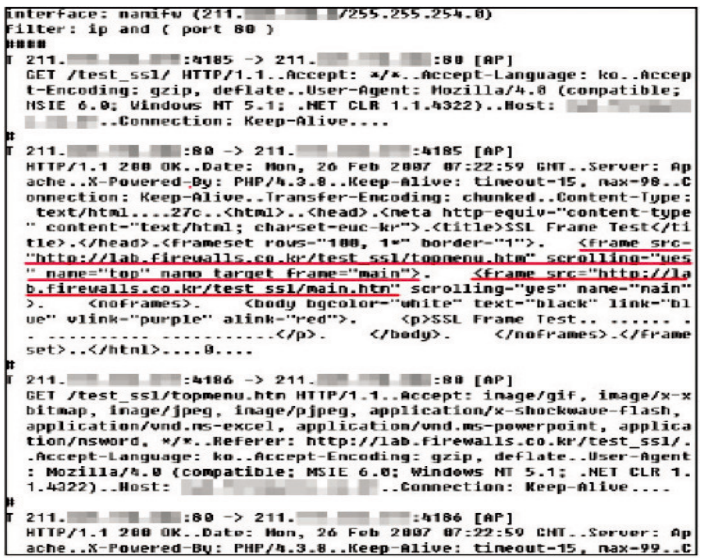
1) 비암호화 통신(http)를 이용해서 호출하기

〈그림 2-16〉은 topmenu..htm과 main.htm을 모두 〈그림 2-13〉의 소스를 이용해서 호출한 경우입니다. 이 경우에는 모든 정보가 암호화되지 않고 〈그림 2-17〉과 같이 그대로 노출됩니다.

●● 그림 2-16 ●● 비암호화된 페이지 호출하기



●● 그림 2-17 ●● Http호출 시 80 포트 모니터링 결과

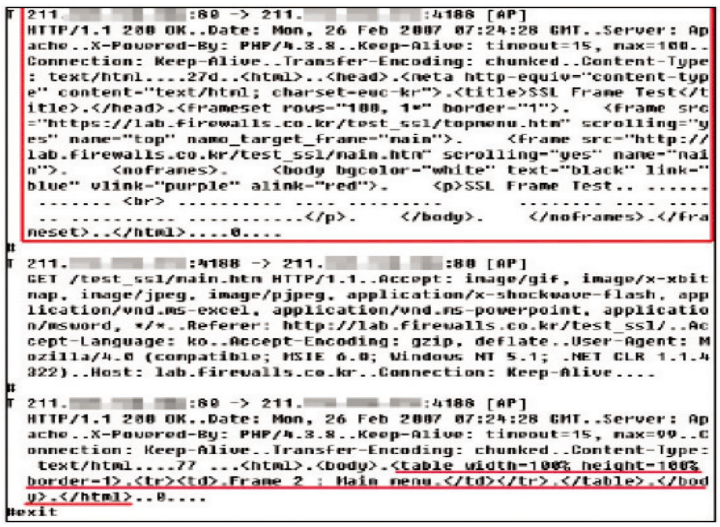


다음으로는 〈그림 2-14〉의 소스코드를 적용하여 topmenu.htm만을 https로 호출을 하는 경우입니다.

●● 그림 2-18 ●● topmenu.htm만 암호화하여 호출하기

프레임을 이용하여 호출하는 경우에는 아래 〈그림 2-19〉와 같이 암호화되지 않는 index.html (네모박스)의 내용과 main.htm의 내용만이 80포트로 텍스트 전송되는 것을 확인할 수 있습니다. topmenu.htm의 내용은 암호화 전송되기 때문에 평문 전송되는 80포트에서는 내용을 알 수 없습니다.

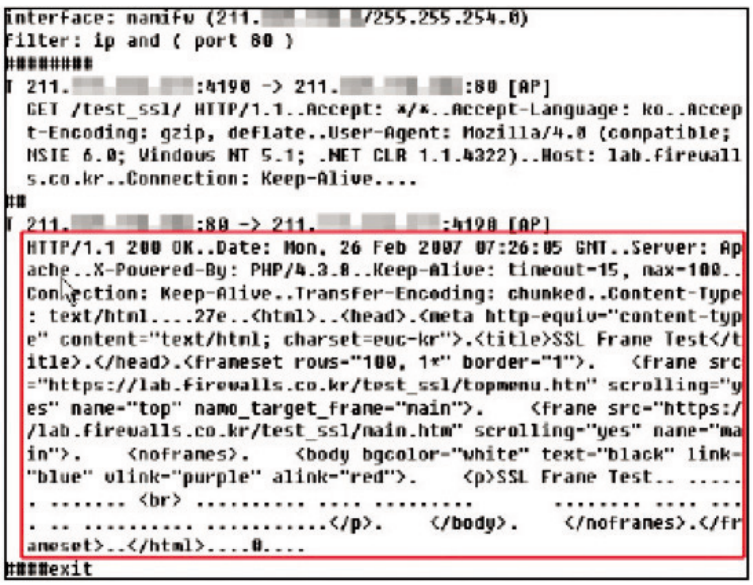
●● 그림 2-19 ●● topmenu.htm의 내용만 암호화된 모니터링 결과



마지막으로 〈그림 2-15〉와 같이, 호출하는 index.html을 제외하고 모든 프레임내의 호출 페이지를 https를 통해서 호출하게 될 경우에는 아래와 같이 index.html의 내용만 평문으로 전송이 되고, 나머지 topmenu.htm과 main.htm은 암호화 되어서 전송됩니다.

●● 그림 2-20 ●● topmenu.htm과 main.htm을 https로 호출하기

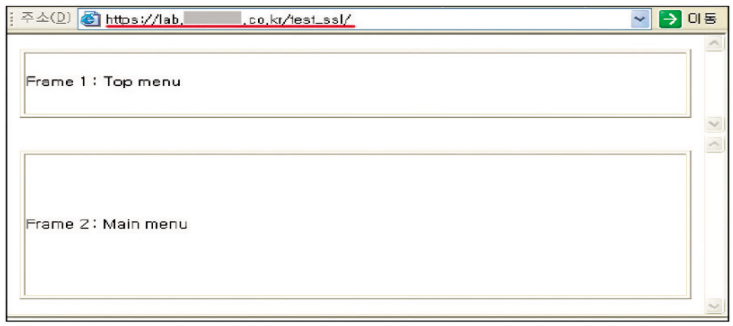
●● 그림 2-21 ●● index.html의 내용만 모니터링 된 결과



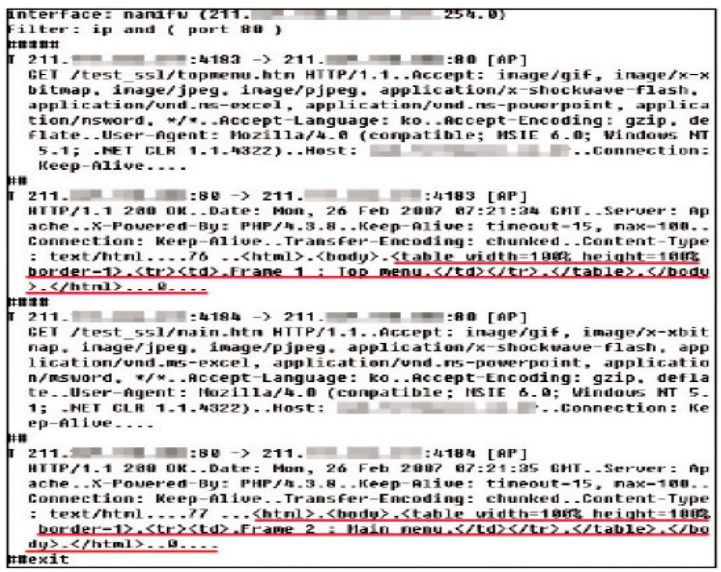
2) 암호화 통신(https)을 이용해서 호출하기

앞에서와 같은 절차를 이용해서 https를 이용해서 호출을 하게 되면, 프레임을 포함하고 있는 index.html은 URL을 https로 호출을 하게 되므로, 항상 암호화가 되어지고, topmenu.htm과 main.htm은 〈그림 2-13〉, 〈그림 2-14〉, 〈그림 2-15〉와 같이 암호화 적용 여부에 따라서, 평문 통신 또는 암호화 통신이 이루어집니다.

●● 그림 2-22 ●● https를 이용한 호출



●● 그림 2-23 ●● https 호출시 80포트 모니터링 결과



〈그림 2-23〉을 보면, 웹 브라우저에서 https를 통해서 호출한 index.html의 내용은 암호화되어 통신이 이루어지기 때문에 80포트를 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.

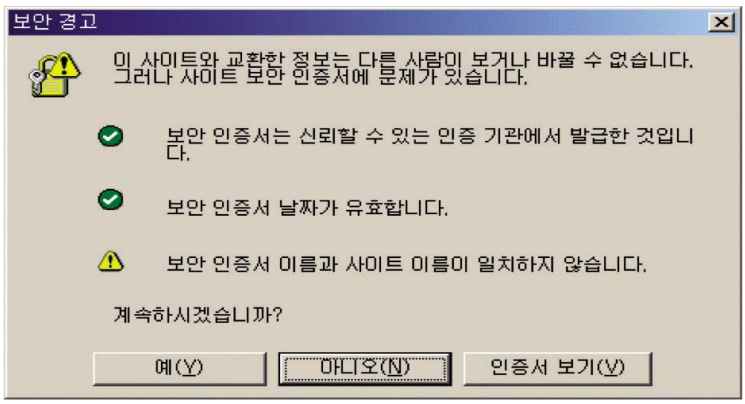
〈그림 2-14〉, 〈그림 2-15〉의 소스를 같은 방법으로 테스트 해보면, http로 호출된 웹페이지는 암호화 통신이 이루어지지 않고 있는 것을 알 수 있습니다.

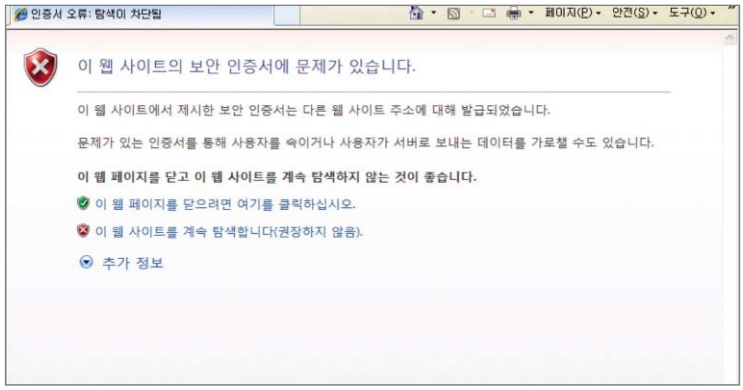
이와 같이 프레임을 이용하면, 필요에 따라서 한 페이지에서 암호화가 제공되는 부분과 암호화가 제공되지 않는 부분이 공존할 수 있도록 구성할 수 있지만, 앞서서도 이미 언급했듯이 아무리 웹 브라우저에서 https를 이용해서 호출을 했어도 프레임으로 불러오는 페이지가 http 주소를 가지고 있을 경우에는 암호화가 되지 않고 정보의 노출이 발생할 수 있으므로, 프레임이 사용되는 페이지를 암호화를 위해서 https로 호출하고자 할 때에는 꼭 확인을 해보시기 바랍니다.

4. 오류 발생 시 대처방법

4.1 인증서 관련

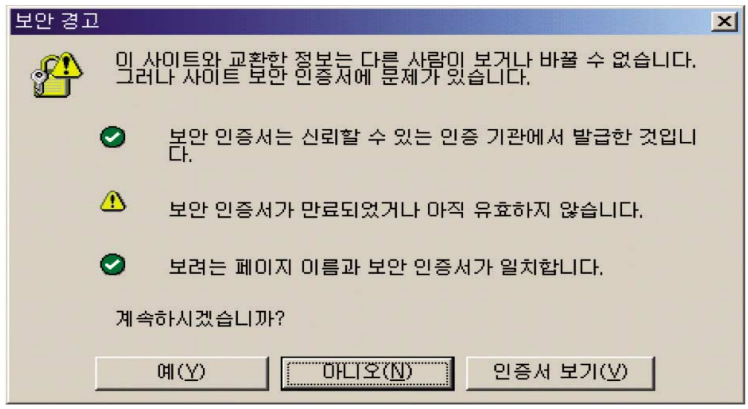
① 인증서를 발급받은 사이트 주소와 실제로 접속한 사이트 주소가 다른 경우

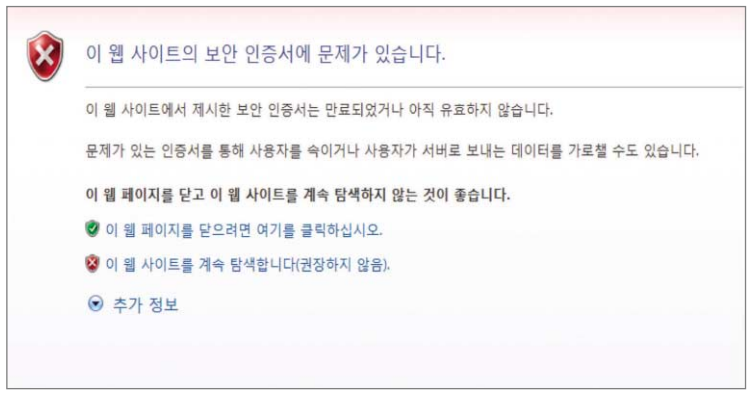




예를 들어 www.opa.or.kr로 인증서를 발급받아 설치한 후 실제 적용은 login.opa.or.kr로 설정하여 인증서를 발급받은 주소와 실제로 접속한 주소가 다른 경우에 위와 같은 경고창이 나오게 됩니다.

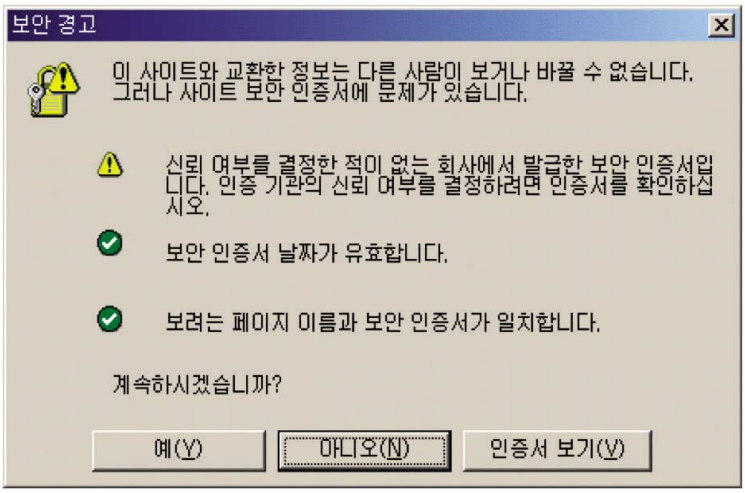
② 인증서가 유효하지 않은 경우





인증서는 저마다 고유한 유효기간을 가지고 있는데, 이 기간이 지난 인증서를 계속 설치해 두는 경우에 나오는 경고창입니다. 그러나, 일반적으로 인증서가 설치된 사이트에 접속하는 PC의 날짜가 잘못되어 있어서 생기는 경우도 많습니다.

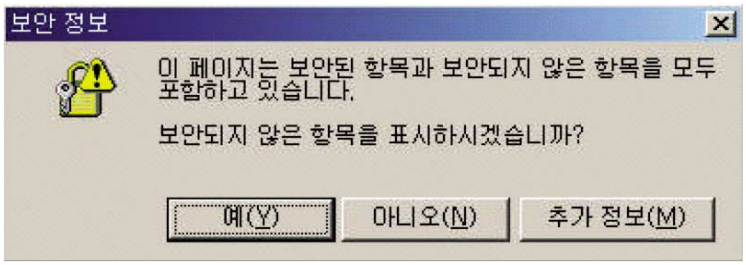
③ 브라우저가 웹 서버 인증서를 신뢰할 수 없는 경우

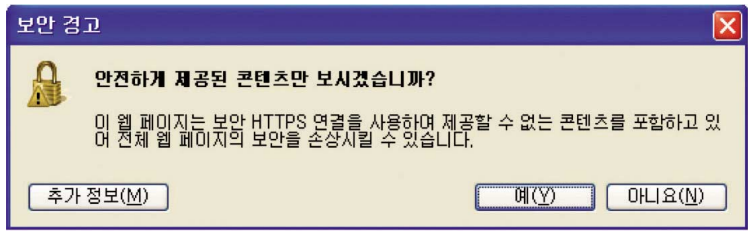


이 경우는 웹 서버 인증서를 발급한 인증기관을 웹 브라우저가 인식하지 못하는 경우로써, 브라우저에는 기본적으로 신뢰할 수 있는 인증기관 리스트가 내장되어 있는데 그 리스트에 없는, 즉 신뢰할 수 없는 인증기관에서 발급된 인증서를 설치한 경우에 발생하는 경고창 입니다. 그리고 웹 서버에서 자체적으로 만든 인증서를 설치한 경우에도 경고창은 발생합니다.

4.2 보안되지 않은 항목의 표시 · 연결 관련

① 보안된 항목 https와 보안되지 않은 항목 http를 모두 포함하는 경우

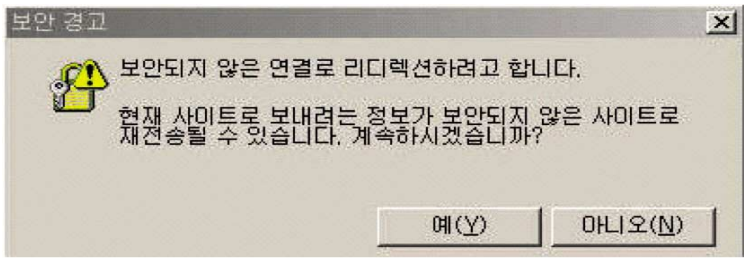




말 그대로 보안된 항목 https와 보안되지 않은 항목 http를 모두 포함하고 있어 나타나는 보안경고창입니다. https://를 이용해서 암호화 통신을 하고자 하는 페이지의 소스에 http://를 이용하여 호출하는 이미지 등이 존재할 때 보안경고창이 나타나는 것입니다.

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.test.com에서 로그인을 위해 https://www.test.com/login.jsp로 접속할 때 /login.jsp안에 http://www.test.com로 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 refresh 하게 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 리다이렉션 한 것처럼 동작되게 되어 경고가 뜨지 않습니다.

③ https로 접속할 경우 페이지를 표시할 수 없다고 확인되는 경우

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 보안장비가있다면 https를 위한 해당 포트를 모두 허용해 주어야 합니다. IIS 서버의 경우 'Netstat -na | grep 포트 번호' 명령어를 이용하여 https를 위한 포트가 활성화되어 있는지 확인할 수 있습니다.

4.3 웹서버 기종 변경 관련

① 운영 중인 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 운영 중인 웹 서버 종류를 다른 기종으로 변경하려 하는 경우

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

5. 웹사이트 운영 · 관리상의 유의사항

5.1 인증서의 유효성 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 명실된 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.

5.2 웹사이트의 신뢰성 확보

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.

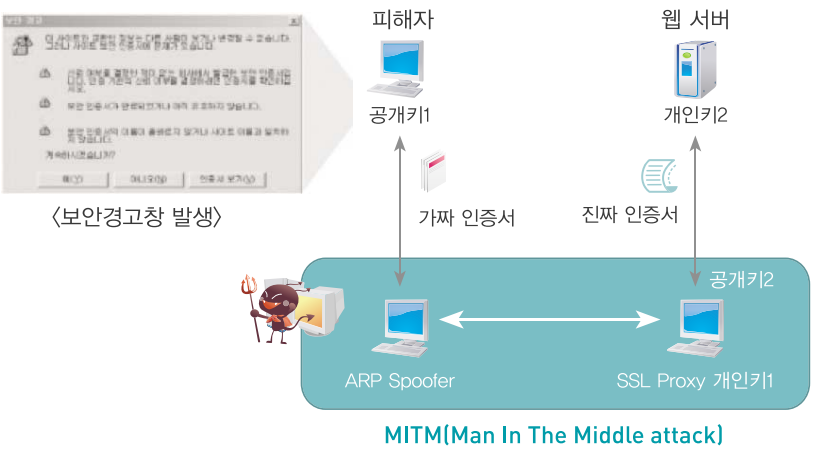
또한 보안서버 구축 가이드 및 리플렛, 안내 홈페이지를 통하여 보안경고창 발생 시 주의할 것으로 지속적으로 안내하고 있기 때문에, 이러한 안내를 받은 이용자가 위 · 변조된 사이트나 피싱 사이트 등의 불법 웹사이트로 오인하여 접속을 기피하는 현상이 발생할 수 있습니다.

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 이용 시 정보보호를 위한 기본적으로 확인하는 사항입니다.

그림 2-24 ARP 스푸핑을 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, 인증기관이 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 발급 시 다음 사항을 점검한다.
   ① 주요 웹브라우저에서 신뢰기관으로 등록된 인증기관에서 발급된 인증서인가?
   ② SSL 인증서 내 도메인 명과 웹사이트 명이 일치하는가?
   ③ SSL 인증서 내 유효기간이 정확한가?

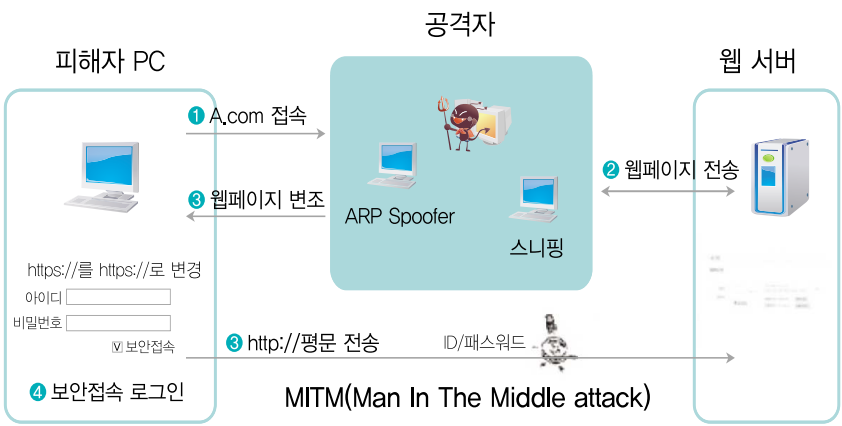
2) 보안서버 구축 후 다음 사항을 점검한다.
   ① 내 · 외부 네트워크에서 웹사이트를 접속하여 보안경고창이 발생하는지 확인한다.
   ② IE, 파이어 폭스, 사파리 등 주요 웹브라우저에서 보안경고창이 발생하는지 확인한다.

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

그림 2-25 ARP 스푸핑과 데이터 변조를 통한 MITM 공격



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

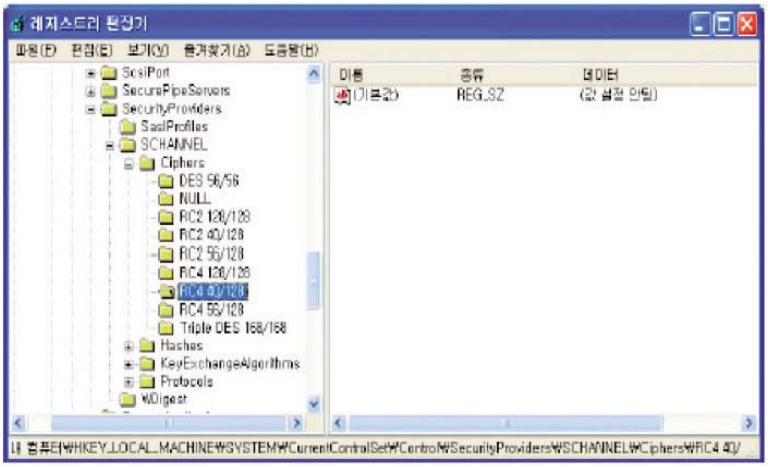
대책

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.

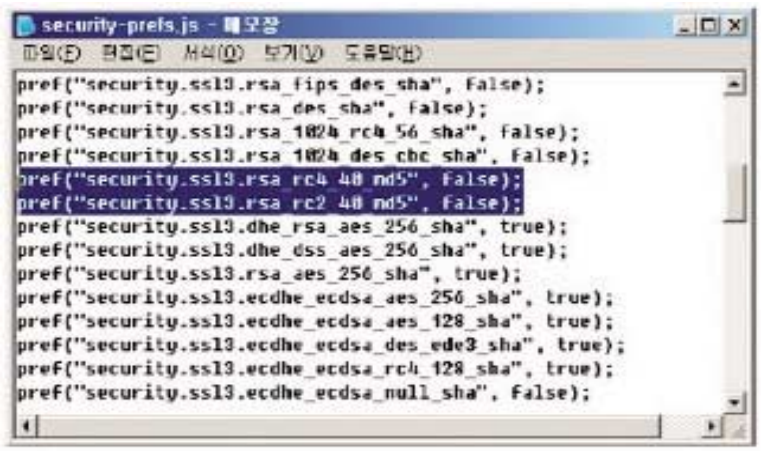
●● 그림 2-26 ●● 익스플로러의 Ciphersuite 수정



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

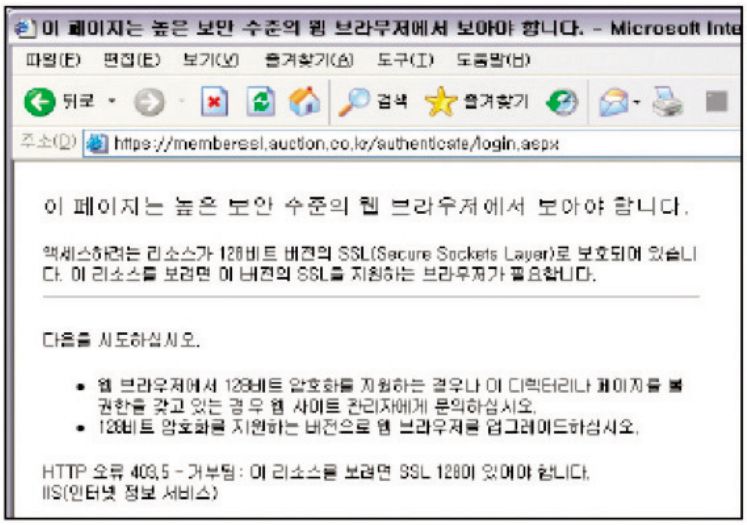
파이어폭스는 C:₩Program Files₩Mozila Firefox₩greprefs₩security-orefs.js파일을 수정하면 〈그림 2-27〉과 같이 메모장을 통해 수정이 가능합니다.

●● 그림 2-27 ●● 파이어폭스의 Ciphersuite 수정



이처럼 Ciphersuite의 수정을 통한 낮은 암호화 알고리즘의 강제사용을 막기 위해서 서버 관리자는 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 2-28〉은 높은 강도의 암호화 알고리즘을 사용할 것을 권장하는 경고메시지의 예입니다.

그림 2-28 Cipersuite 키 길이에 대한 보안 경고



Ⅲ

보안서버 관련 FAQ

Ⅲ 보안서버 관련 FAQ

1. 제도관련

1 개인정보보호협회(OPA)는 어떤 기관인가요?

미래창조과학부 업무를 위임받아 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의해 인터넷 상의 개인정보보호 업무 등을 맡고 있으며, 웹사이트 회원가입 등을 통한 개인정보 수집에 따른 미흡한 사업자에 대해 개선안내 업무 등을 하고 있습니다.

2 보안서버는 무엇이고, 구축하지 않으면 어떻게 되나요?

보안서버란, 인터넷상에서 사용자 PC와 웹 서버 사이에 송수신되는 개인정보를 암호화하여 전송되는 서버를 의미합니다.

SSL 인증서 또는 응용 프로그램은 보안서버 전문 구축업체를 통해 구입 및 설치할 수 있습니다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의해 개인정보를 수집하는 웹사이트에 보안서버가 구축되지 않은 경우 3천만원 이하의 과태료 등 행정조치가 있을 수 있습니다.

3 보안서버 구축이 의무인가요?

보안서버 구축은 현행법상 개인정보를 취급하는 영리 목적의 사업자 분들은 필수적으로 구축하셔야 하는 의무조항입니다.

관련 법률은 이미 2005년부터 시행 중이며「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제28조(개인정보의 보호조치)와 제76조(과태료) 등에 명시되어 있습니다. 실제 법조항은 본 가이드의 보안서버 관련 법률(16p)을 참조하시고, 전체 법조항이 필요하신 경우는 법제처(www.law.go.kr) 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 시일 내에 구축을 완료하셔야 합니다.

2. 구축범위 관련

5 웹사이트에서 보안서버 구축 범위는 정확하게 어디입니까?

기본적으로 보안서버가 구축되어야 할 곳은 웹페이지와 서버 간에 개인정보가 저장 또는 전송되는 구간이 발생하는 곳에 암호화가 되어야 합니다. 즉, 어떠한 형식이든 개인정보를 웹페이지와 서버 간에 서로 전송이 되거나 호출이 된다면 보안서버가 적용이 되어야 합니다.

6 암호화되어야 하는 개인정보의 범위는 어디까지입니까?

'개인정보'라 함은 생존하는 개인에 관한 정보로서 성명 · 이메일주소, 주소, 전화번호 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, 인터넷 뱅킹 이용시 계좌번호/계좌 비밀번호 등이 해당됩니다. 또한 게시판 등에서 성명, 이메일, 연락처 등을 수집한다면 개인을 식별할 수 있는 정보로서 개인정보 수집행위에 해당한다고 볼 수 있습니다. 이러한 경우 해당 게시판은 보안서버 구축 대상이 될 수 있습니다.

3. 호스팅 관련

7 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 업체 및 보안서버 구축 전문 업체에 문의하시기 바랍니다.

8 웹호스팅사를 변경하는 경우, 보안서버를 새로 구축해야 하나요?

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

인증서를 구입 시 유효기간 동안은 웹호스팅사를 옮기더라도 사용이 가능합니다. 옮기는 웹호스팅사에 문의해서 개인키와 인증서 백업 받으셔서 설정을 요청하시기 바랍니다. 그리고 해당 웹 호스팅사에서 보안서버 구축을 지원하는지 미리 확인하시기 바랍니다.

9 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. 기술 관련

10 개인정보의 입력 값을 넘길 때만 https로 호출해서 넘기면 되는 건가요?

즉, 개인정보를 입력하는 폼이 있는 페이지는 https로 안 불러와도 되는지요?

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

11 보안서버 인증서만 웹사이트에 깔면 암호화 전송이 되나요?

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

따라서 일반 이용자들이 http:// (또는 www.) 방식으로 접속하더라고 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.

12 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 익스플로러6.0 이하에서는 단순히 '신뢰할 수없는 기관에서 발급한 인증서' 라는 팝업창이 뜨지만, 익스플로러7.0에서는 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 경고 문구를 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.

13 보안서버 경고창 발생은 어떻게 제거 하나요?

보안서버를 전체 사이트에 걸지 않고 개인정보가 처리되는 페이지만 각각 적용할 경우에 해당 웹페이지내의 URL중 https로 호출하지 않은 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.

5. 기타

14 보안서버를 구축하려면 누구에게 연락해야 하나요?

보안서버 구축 전문 업체와 상의하시면 되며, 'I 장 7.보안서버 구축 전문 업체' 내용 또는 평소에 알고 있던 보안서버 구축 전문 업체를 이용하셔도 됩니다.

2013
보안서버 구축가이드

인 쇄 | 2013년 7월
발 행 | 2013년 7월

발행처 | **개인정보보호협회**

서울특별시 강남구 역삼동 824-27 지희빌딩 9층
Tel : (02) 550-9543

인쇄처 | **호정씨앤피** Tel : (02) 2277-4718

〈비매품〉

2013
보안서버 구축 가이드

미래창조과학부
Ministry of Science, ICT and Future Planning

개인정보보호협회
KOREA ONLINE PRIVACY ASSOCIATION