Ⅲ. SSL 방식 보안서버 구축하기

1. 소개 및 보안서버 구축 절차

가. 개요

SSL은 Secure Sockets Layer의 머리글이며, 1994년 Netscape에 의해 전세계적인 표준 보안 기술이 개발되었습니다.

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

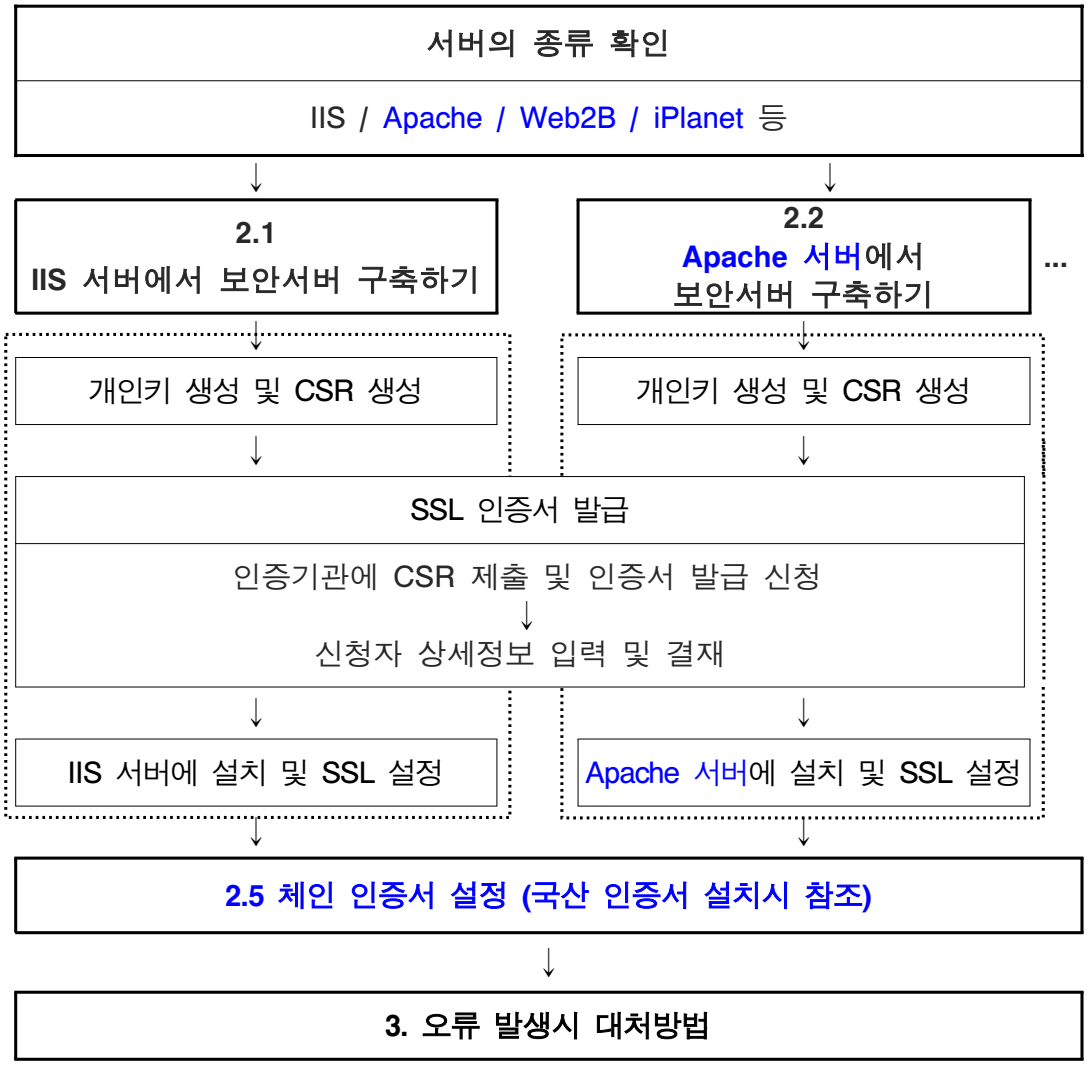
아래는 SSL 보안에 대해 그림으로 간단하게 설명해 놓은 것입니다.

<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.

나. 보안서버 구축 절차

SSL 방식의 보안서버 구축 절차는 다음과 같습니다.



<그림 3-2> SSL 방식 보안서버 구축 절차

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)이란 인증서 요청파일의 약어로서 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.

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.

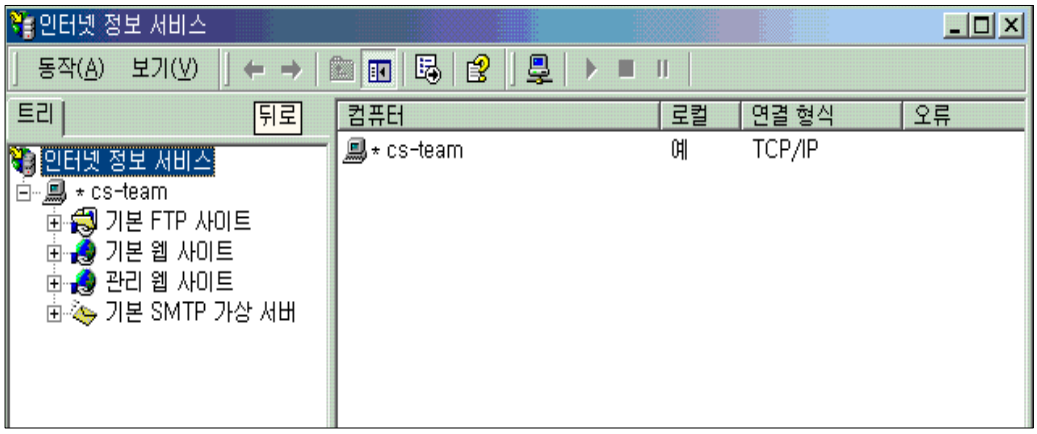
2. 설치 과정

2.1 IIS 서버에서 보안서버 구축하기

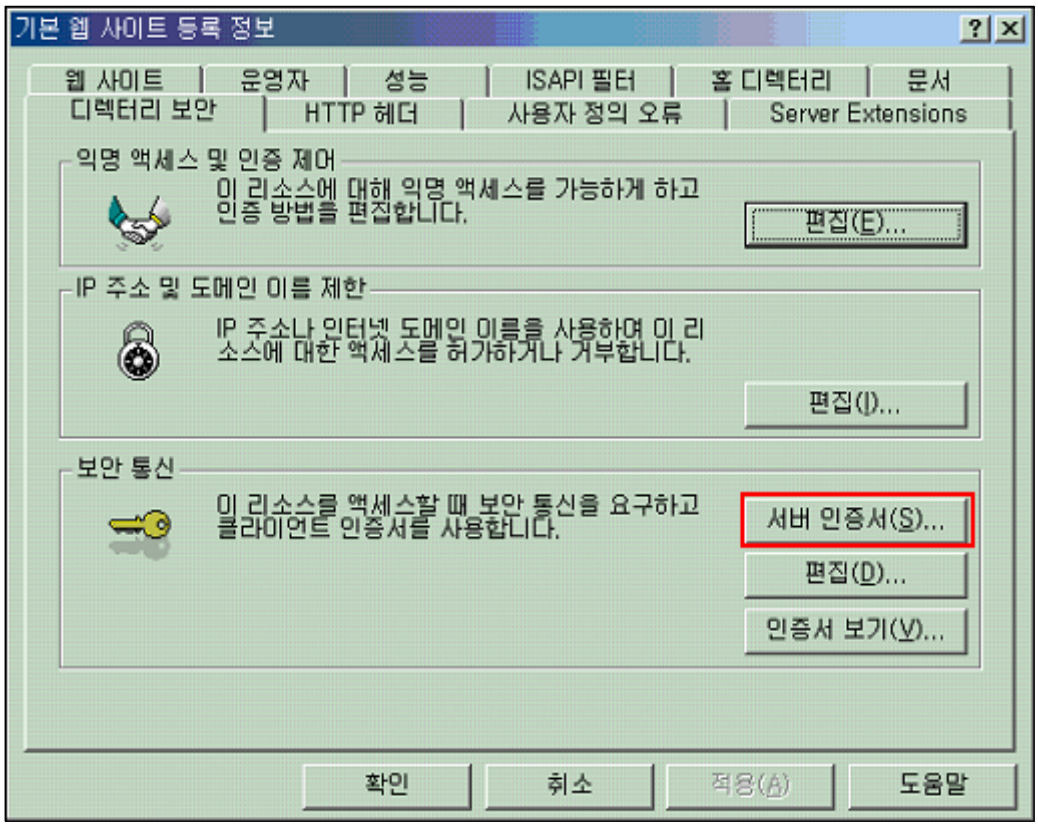
가. 개인키 생성 및 CSR 생성 방법

① 웹사이트 속성 선택

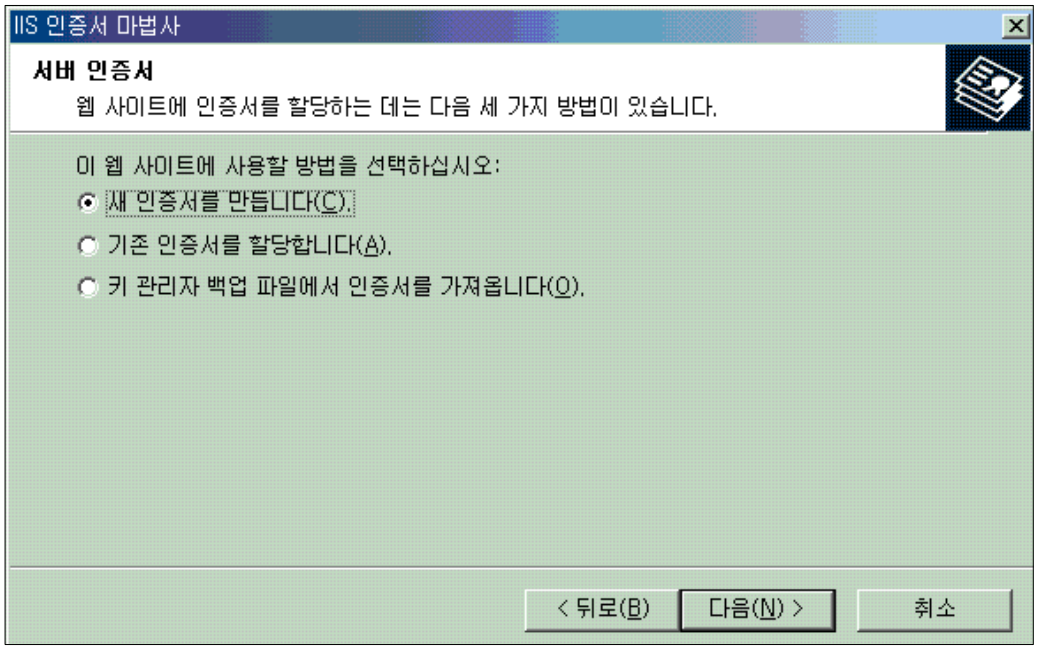
시작→프로그램→관리도구→인터넷 서비스 관리자→웹사이트→속성



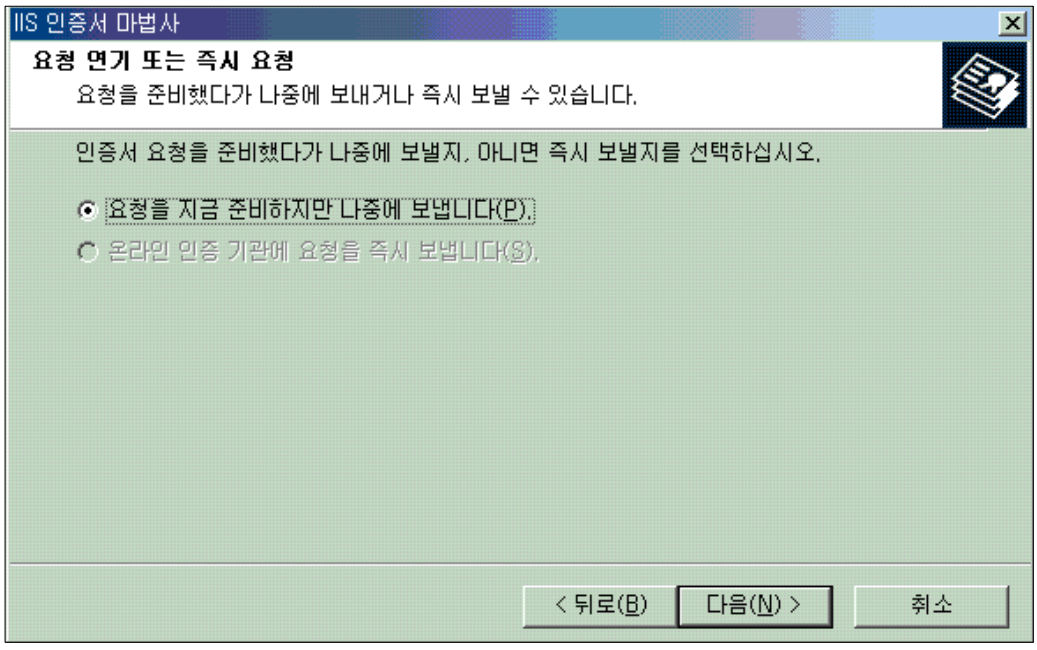
② 등록정보 화면에서 디렉토리 보안을 클릭한 후 서버 인증서를 클릭합니다.



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

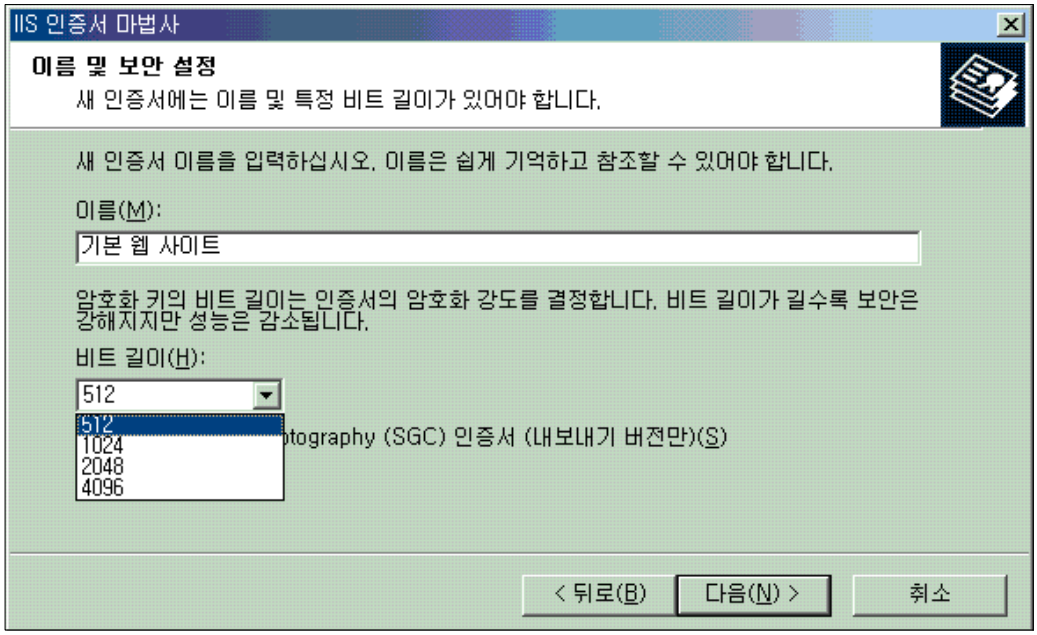


④ '요청을 준비하지만 나중에 보냅니다'를 선택합니다.



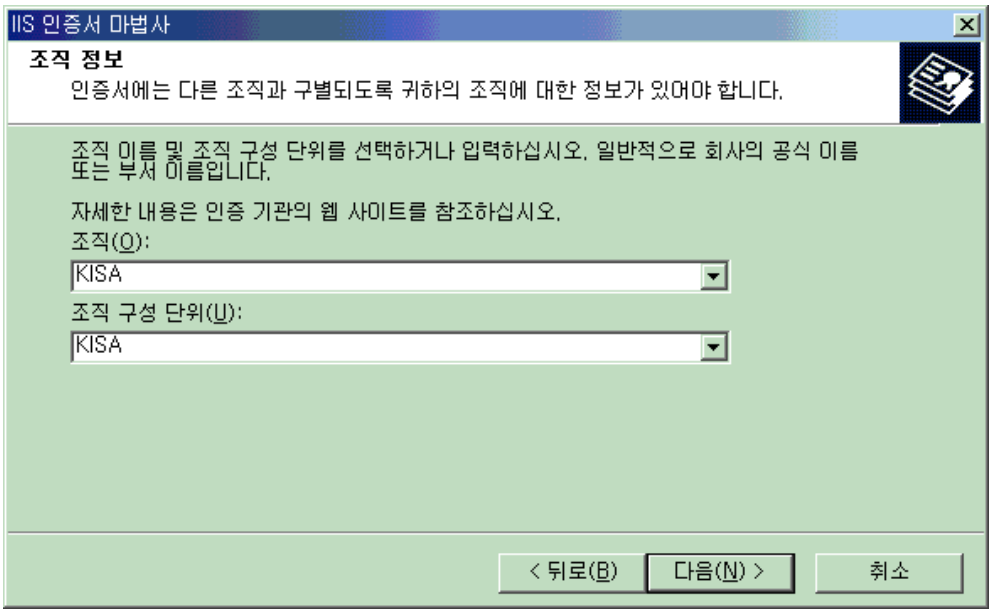
⑤ 인증서를 만들 이름을 입력하시기 바랍니다.

이름은 인증서의 별칭이므로 쉬운 것으로 입력하여 주시기 바랍니다. 인증서 키의 길이는 1,024가 표준입니다. 비트 길이가 너무 크면 서버에서 인지하지 못할 경우도 있습니다.

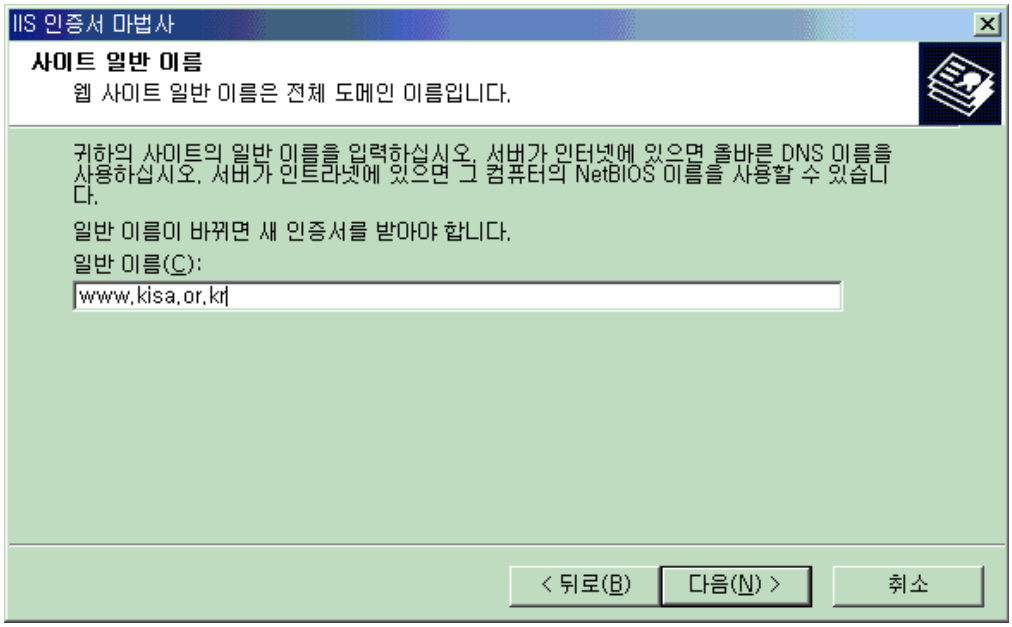


⑥ 조직 및 조직 구성 단위를 입력합니다.

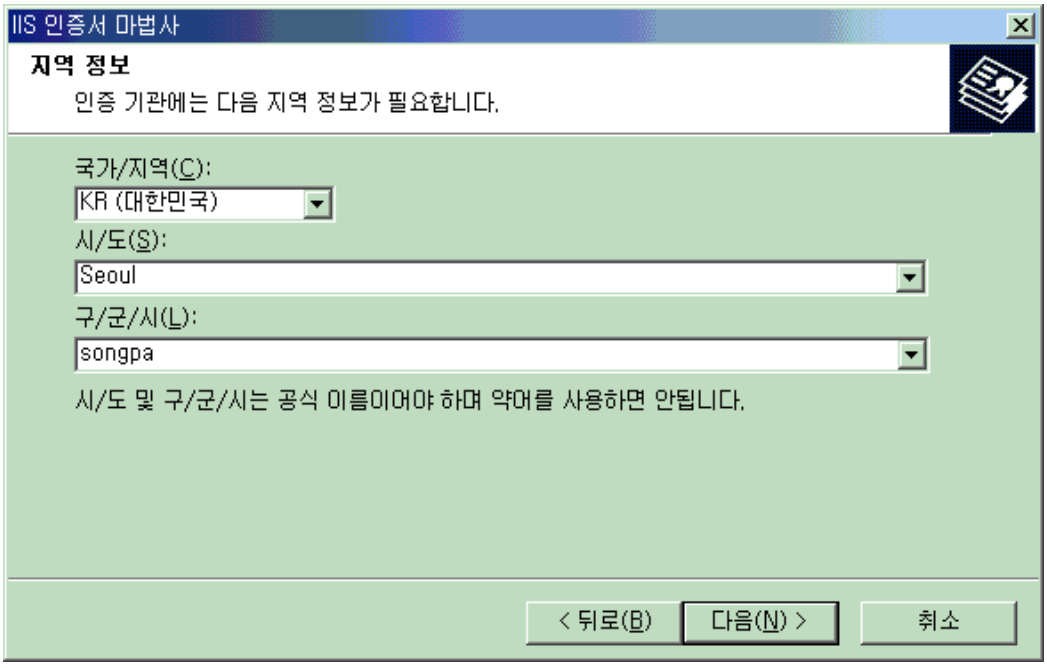
조직은 회사의 영문 전체 이름을 입력하고, 조직 구성단위는 영문 부서명을 입력합니다.(모든 내용은 영문으로 입력합니다)



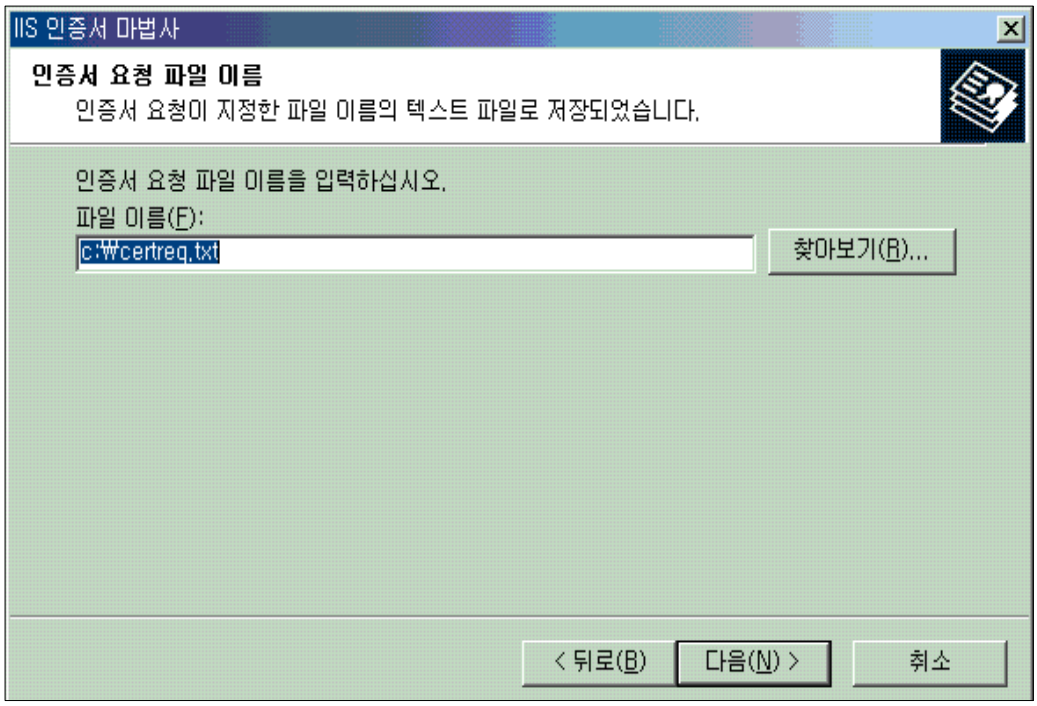
⑦ 인증받을 도메인 이름을 입력하시기 바랍니다.



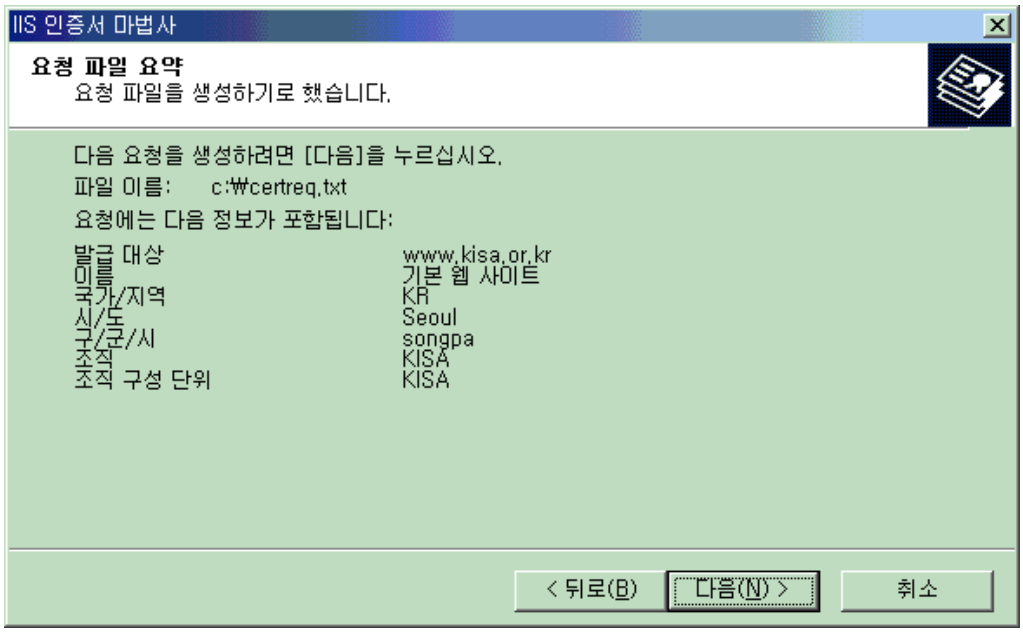
⑧ 지역 정보를 입력합니다.(모든 내용은 영문으로 입력합니다.)



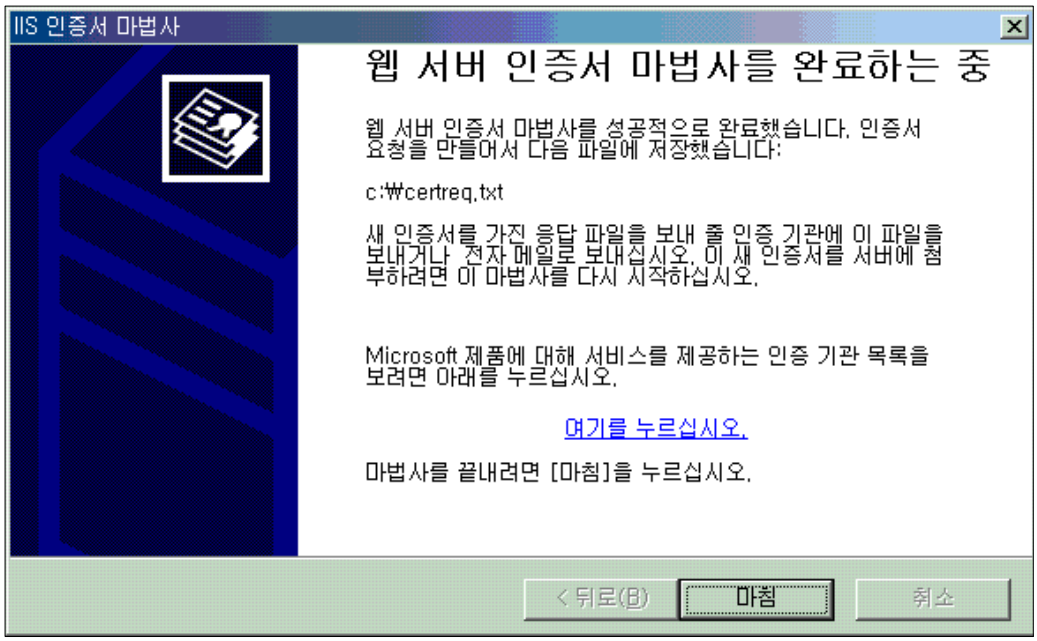
⑨ 인증서 요청파일(CSR)을 저장합니다.



⑩ 신청한 내용을 다시 한 번 확인합니다.



⑪ 인증서 신청을 완료합니다.



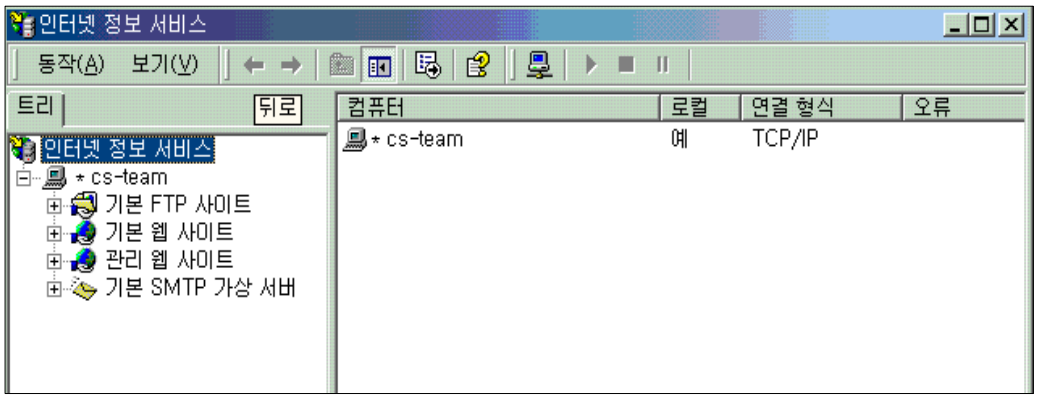
⑫ CSR 내용을 인증기관에게 메일로 송부하시던지 인증서 신청화면에 붙여 넣으신 후 인증서 신청을 진행하시면 됩니다.

자, 이제 인증기관의 발급 절차에 따라서 인증서가 발급됩니다.

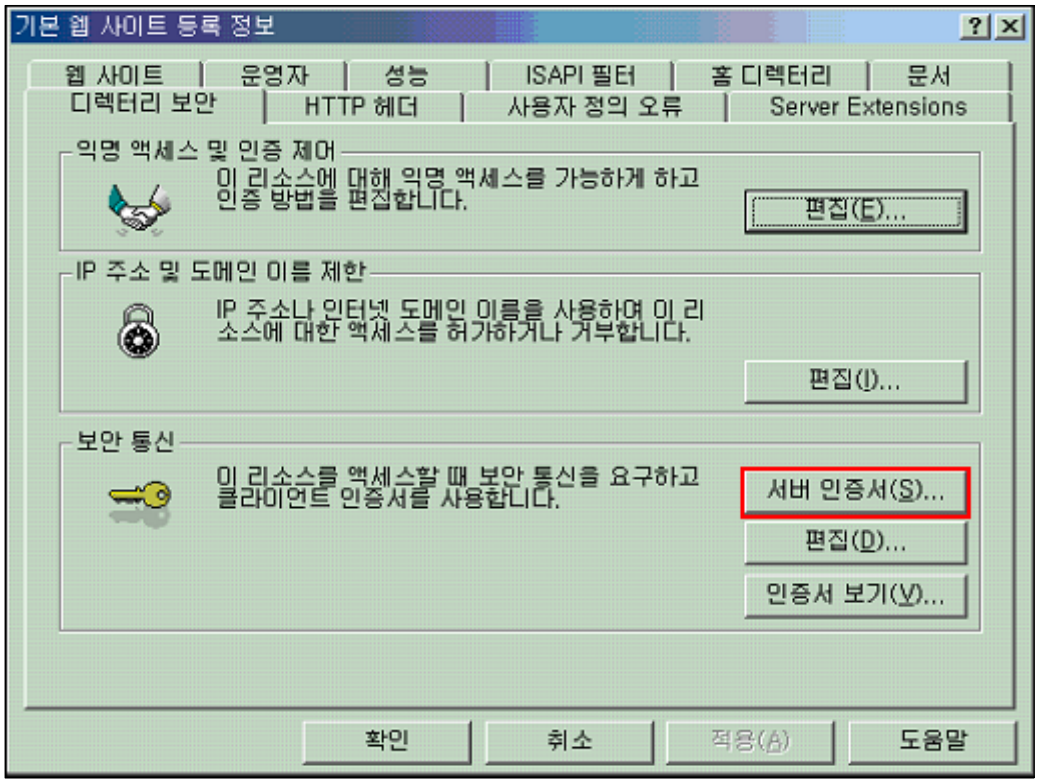
나. SSL 설정

① 웹사이트 속성 선택

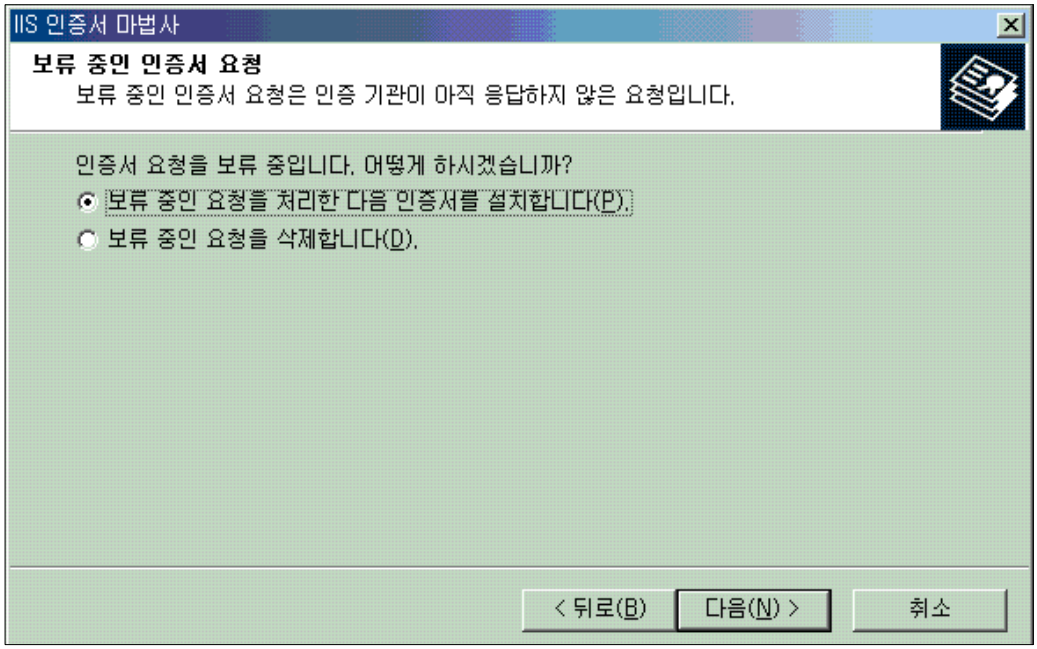
시작→프로그램→관리도구→인터넷 서비스 관리자→웹사이트→속성



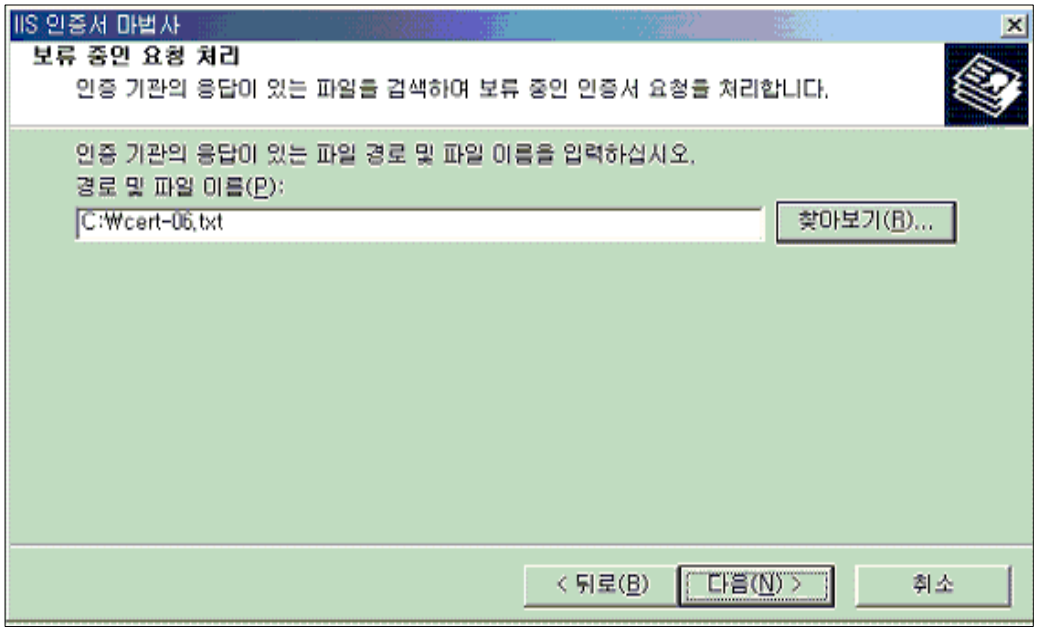
② 등록정보 화면에서 디렉토리 보안을 클릭한 후 서버 인증서를 클릭합니다.



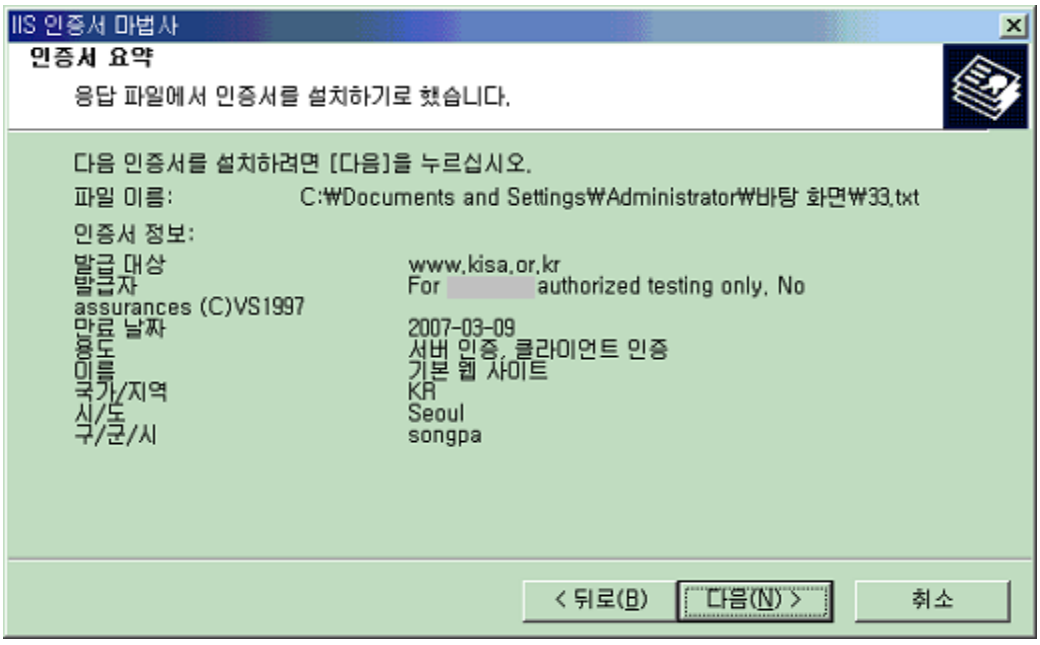
③ 보류중인 요청을 처리합니다.



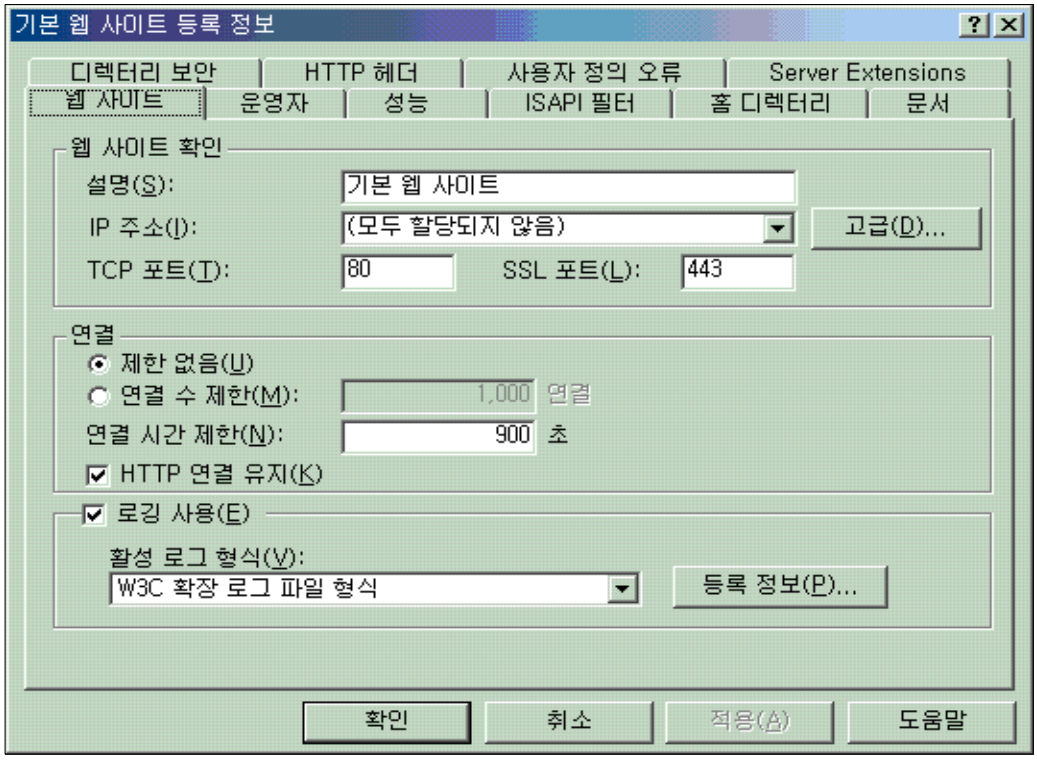
④ 보류 중인 요청 처리-메일을 통하여 받은 인증서(-----begin 부터 end-----까지)를 저장한 파일을 선택합니다. 인증서 파일을 선택한 후 다음 버튼을 누릅니다.



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

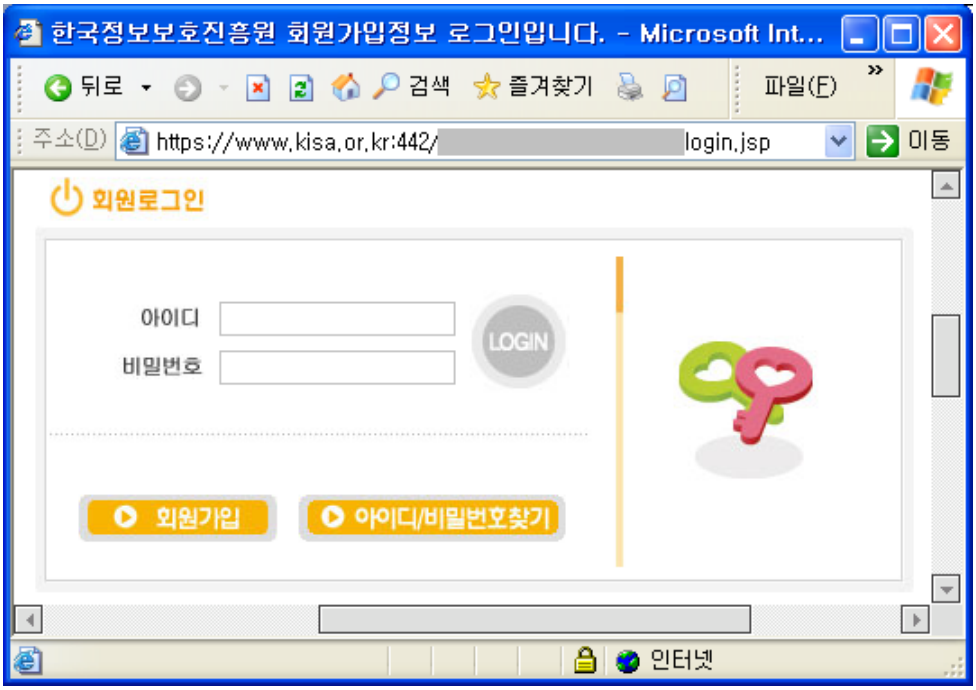


⑥ 인증서 설치 후의 설정 - 기본 웹 사이트의 등록정보에서 웹사이트 탭을 선택합니다. 웹 사이트 확인 섹션에서 고급 버튼을 클릭해서 SSL 포트에 443을 설정해줍니다.(기본적으로 443을 사용하지만, 사이트 운영자가 1~65535 범위내에서 임의로 포트번호를 설정할 수 있습니다)



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. VI장으로 이동하셔서 실제 웹페이지를 어떻게 수정해야 하는지 알아보겠습니다.

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.