



글로벌 공인 보안 자격증 CISSP의 A~Z

근래에 통신망과 시스템의 급속적인 발전으로 대부분의 사람들이 인터넷이라는 매쉬(Mesh) 형태의 거대한 네트워크에 연결되어 있다. 인터넷은 전 세계가 언제 어디서나 연결될 수 있는 글로벌 네트워크로서 많은 사람들은 인터넷을 통해 다양한 정보를 실시간으로 검색하며, 친구들과 정보를 공유하고, 인터넷 뱅킹 등 경제활동을 오프라인과 다름없이 편리하게 사용하고 있다. 하지만, 한 편으로는 이런 시스템과 네트워크의 발전으로 인해 한 번의 정보 유출에도 큰 피해가 발생하게 되었다. 이런 이유로 정보시스템 보안의 중요성이 날로 증가하고 있으며, 그와 함께 국제적으로 인정받는 국제공인 정보시스템 보안 전문가 자격증인 CISSP(Certified Information Systems Security Professional)의 수요도 급속하게 증가하게 되었다.

최근에는 CISSP가 보안 분야의 종사자가 아니어도, IT 분야 또는 정보를 취급하는 모든 사람들이 취득해야하는 필수적인 전문 자격증이 되었다. 따라서, 앞으로 6회에 걸쳐 글로벌 공인 보안 자격증인 CISSP에 대해 알아보고, CISSP를 취득하기 위해 꼭 알아야 할 사항들을 요점정리와 연습문제를 제시하여, 독자들에게 CISSP 자격증 취득의 바른 길을 안내하고자 한다.

[글로벌 공인 보안 자격증 CISSP 연재 순서]

구분	내용
1회	글로벌 공인 보안 자격증 CISSP의 A~Z
2회	정보보호와 위험관리, 보안 아키텍처 도메인
3회	통신 및 네트워크 보안, 접근통제 도메인
4회	암호학, 응용 프로그램 보안 도메인
5회	BCP, 운영 보안 도메인
6회	법규제, 물리적 보안 도메인

1. CISSP란 무엇인가?

CISSP는 보안 분야에서 가장 유명한 비영리기관인 (ISC)²⁾(International Information Systems Security Certification Consortium)³⁾에서 발급 관리하는 자격증으로서, 자격체계의 우수성을 인정받아 ISO/IEC 17024 표준을 취득하였다. CISSP는 국제적으로 공인되는 대표적인 정보보호 관련 자격이며, 전 세계적으로 100여개 이상의 국가들로부터 4만여 명이 넘는 CISSP가 배출되었다. CISSP는 2000년도에 국내에 처음으로 도입되어 현재 2,500여명이 자격을 유지하고 있다. 국가 사회의 중요한 정보시스템과 정보자산 보호를 위한 전문가에 대한 수요가 늘어나는 현 시점에서 CISSP의 중요성은 높아지고 있으며, CISSP는 날이 갈수록 지능화, 악성화, 국제화 되고 있는 사이버 범죄 억제와 IT 및 정보보호의 전문성을 갖춘 사회적, 국가적 전문가로서의 역할을 하고 있다.

2. CISSP를 취득해야 하는 이유는 무엇인가?

2-1. 취업 준비생

최근 취업 대란이라는 말이 새삼스럽지 않은 말이 되고 있다. 대학을 졸업하고도 취업을 하지 못하는 사람들을 주변에서 쉽게 찾을 수 있을 것이다. 과연, 대학을 졸업한 사람들을 모두 수용할 수 있는 일자리가 있는가? 아마도 일자리는 한정되어 있고, 실제 졸업생은 많다 보니 취업 재수생들이 증가할 것이다. 결국 취업을 위해서는 경쟁이 불가피한 구조이다. 과연, 4년간의 대학 생활 동안 다른 사람들과 똑같은 교육을 받고 비슷한 학점을 받은 사람들이 경쟁이 가능할까? 결국 차별화 요소를 가진 자가 바늘구멍 같은 취업의 문을 뚫을 수 있을 것이다. 영어, 인턴 경험 등 다양한 차별화 요소가 있겠지만, 자격증도 이러한 차별화 요소에서 가장 큰 항목으로 대우 받고 있다. 따라서, 학생들은 자기와 동일한 스펙 동일한 수준의 학생들과 경쟁하기 위해서는 자신만의 특화된 요소로 자격증이 필요할 것이다. 특히, 향후 유망 직종으로 분류되는 보안 분야의 국제 공인 자격증인 CISSP는 IT 자격증 중에서도 으뜸이라 할 수 있겠다.

2-2. 이직 준비생

취업에 성공하여 현재 직장에 다니고 있는 사람들은 직장생활에 익숙해지면, 자신의 미래에 대한 고민에 빠질 것이다. 또한, 자신의 능력을 한 단계 높이기 위해 새로운 길을 찾고자 할 것이다. 자신의 미래를 준비하고 새로운 능력을 한 단계 높이는 방법으로 가장 일반적으로 찾는 방법은 무엇인가? 보통 새로운 직장으로 이직을 준비할 것이다. 그렇다면, 다른 직장으로 이직을 위해서는 어떤 것을 준비해야 되는가? 보안 분야는 다양한 직종에서 필요로 하고 있다. 따라서, 보안 분야의 경험과 지식을 갖추고 있다면, 다른 분야의 경력보다 새로운 직종으로 이직할 가능성이 높다고 하겠다. 그럼, 이직시 보안 분야의 경험과 지식에 대한 공식적인 증명은 무엇이 있을까? 바로, 국제 공인 보안 자격증인 CISSP가 가장 최적의 증명이라고 할 수 있겠다.

1) 1989년에 창립된 비영리기관으로 정보보호 전문가 교육 및 CISSP 자격증 발급 주관 컨소시엄.

2-3. 보안 업계 종사자

보안 업계 종사자들은 보안 경력과 관련지식으로 자신의 보안 분야에서의 역량을 키울 것이다. 보통 보안 업계 종사자들은 자신에게 특화된 분야만을 깊이 있게 학습하는 경향이 있다. 하지만, 보안은 IT 개발과 달리, 한 분야에 대한 전문 지식이 중요한 것이 아니라, 전반적인 분야에 대한 지식을 가지고 있어야 한다. 보안은 한 부분이라도 취약할 경우 전체 보안 수준이 낮아지는 특성을 가지고 있으므로, 보안 전문가는 보안 전 분야에 대한 지식을 가지고 있어야 한다. 즉, 보안의 숲을 봐야 하는 것이다. 그렇다면, 보안의 숲을 볼 수 있는 가장 적절한 방법은 무엇인가? CISSP에서 제공하는 10개의 Domain에서 보안의 모든 분야를 다루고 있기 때문에 CISSP의 충분한 학습은 전반적인 보안 분야에 대한 지식을 체계적으로 쌓을 수 있는 최적의 방안이다.

2-4. 기업체(회사)

기업체들은 항상 성장기회가 있는 새로운 시장을 찾고자 한다. 최근의 보안 시장은 IT 분야에서 성장가능성이 높은 분야로서, 많은 기업들이 보안 시장에 대한 참여를 노리고 있다. 최근에는 국가기관들도 보안인력 채용을 위해 많은 투자를 하고 있다. 국내에서는 정보보호 업체로 지정 받기 위해서는 5인 이상의 CISSP 자격증 소지자가 의무이므로, CISSP 수요는 더욱 증가하고 있다. 또한, (ISC)²는 전 세계 전문가들이 연구한 최고의 실무 자료를 CBK(Common Body of Knowledge)를 통해 제공하고 있으므로, 글로벌 시장에 참여하고자 하는 기업체들은 이러한 글로벌 전문 수준의 콘텐츠를 이해하고 있는 CISSP를 절실히 필요로 하고 있다.

3. CISSP 자격증을 취득하는 절차는 무엇인가?

CISSP 자격증 취득을 위해서는 먼저 시험에 합격해야 하고, 시험 합격 후에는 본인이 CISSP 자격을 받을 수 있는 자격이 있는지를 검증 받아야 한다. 따라서, 자격 응시 요건과 자격 인정 요건 두 가지를 만족하여야 한다.

3-1. 자격 응시 요건

- ▶ CBK 10개 정보 보호 도메인 분야에서 5년 이상의 업무 경력 필요
 - CBK의 10개 도메인에서 최소 두 개 이상의 도메인에 포함되면 응시 가능
 - 경력 인정 사항
 - 학사학위 소지자 경력 1년 인정 ⇒ 4년 이상의 근무 경력 필요
 - CISA, CIA, CISM 자격소지자 경력 1년 인정
 - 경력이 인정 사항을 충족 못하는 분은 다음 두 가지 요건을 만족할 경우 응시 가능
 - (ISC)²에 이 사실을 통보할 것(Associate로 신청)
 - 합격 후 6년 내에 경력 요건을 충족할 것 : Associates로 인정
 - 경력증명 및 CISSP 직업 윤리강령 준수의 확인.

3-2. 자격 인정 요건

- ▶ CISSP 필기시험 합격
- ▶ Endorsement Form에 맞추어서 제출
- ▶ 제출한 경력 사항에 대한 인정/Audit(무작위로 추출) Pass
- ▶ 경력보증 서류 제출(Endorsement Form을 작성하여 발송)
 - CISSP 자격자의 추천 필요.

4. 시험 응시를 위한 원서 접수 및 응시료는?

자격 응시 요건을 충족할 경우에는 원서 접수와 함께 응시료를 지불하면 된다. CISSP 시험은 미국 시험이기 때문에 시험 원서 접수 및 응시료 제출을 (ISC)²의 영문 사이트에서 처리하여 한다. 하지만, 최근에 국내에도 공인 교육기관(한국생산성본부)이 생겨, 관련된 문의사항에 대해서는 바로 문의가 가능하게 되었다. 본래, 한국생산성본부는 교육 분야에 대한 전문기관이나 국내 CISSP 수요자의 편의성을 위해 시험관련 온·오프라인 지원 등 많은 편의를 제공하고 있다. 참고로, 아시아태평양 지역의 CISSP에 대한 관리 및 지원은 홍콩 본부에서 하고 있으며, 홍콩 본부에 한국 담당자가 있어, 영어가 아닌 한국어로 편하게 업무처리가 가능하다는 점을 적극 활용하기 바란다.

4-1. 원서 접수

- ▶ 국내에서 응시 가능, 매년 4회 정기적으로 시험 실시
 - 경력이 충족되는 경우는 (ISC)² 사이트에서 경력사항 등을 입력 후 온라인 접수
 - 신용카드 결제 : 비자, 마스터 카드, 아멕스 카드 가능
- ▶ 학생이거나, 경력사항을 충족 못하는 경우는 CISSP Associate로 응시
 - 시험 합격 후 6년 내 자격충족 후 추천서와 이력서를 제출하여 자격증을 수령
 - 이 기간 동안에 매년 35\$ 비용과 20CPE 제출 필요
 - 시험을 접수하지 않으신 분은 별도로 매뉴얼을 e-mail로 전달 예정

4-2. CISSP의 시험 응시료

시험 비용	시험일 16일 전	시험일 16일 이내
	US \$549	US \$599
연기 / 취소	시험일 22일 전	시험일 22일 전 ~ 5일 전
	US \$100	US \$200

5. 시험은 어떤 형식으로 출제되며 합격기준은 무엇인가?

시험을 응시하기 위해서는 학습보다 먼저 선행되어야 하는 것이, 이 시험의 형식 및 합격기준을 제일 먼저 확인해야 한다. 그래야, 목표를 이룰 수 있기 때문이다. 자격증은 전문지식을 얻는 것도 중요하지만, 어디까지나 시험이기 때문에 취득이 우선시 되어야 한다. 특히, 만만치 않은 시험비용을 지출해야 하는 CISSP 시험에서는 단기간에 실패하지 않고 학습하는 것이 정신적, 금전적으로 중요하다.

5-1. 문제 형식

- ▶ 객관식 사지선다형으로 250문제(시험 시간 : 6시간)
- ▶ 복수형 답은 없으며, 사지선다에서 하나만 답
- ▶ CBK 10개 도메인에서 무작위로 시험문제 출제, 분야별 구분 없음
- ▶ 사용 언어 : 응시자가 선택한 언어와 영어 함께 출제
- ▶ 시험 시간 : 오전 9시 ~ 오후 3시
- ▶ 시험 중간에 화장실 등을 감독관 통제 하에 다녀 올 수 있음.

5-2. 합격 기준

- ▶ CISSP 시험 문제점 70% 이상을 득점
 - CISSP에서 설정한 조정 1000Point 중에서 700Point 이상이면 합격
 - 합격자 발표는 시험일시 후 업무 일수로 2~4주 내에 e-mail로 결과 통보
 - 합격하면 합격 축하 내용과 Endorsement 제출 안내
 - 불합격하면 도메인별 성적표가 배송됨
- 자격 유지를 위해서는
 - CPE : 매년 최소 20CPE, 3년 내 120CPE
 - 비용 : 매년 US \$85 자격비용 납부(3년 주기로 자격 유지여부를 확인하여 갱신)

6. CISSP 시험 일정 및 시험 영역은?

CISSP는 미국에서 응시해야 하는 미국공인회계사 등과 달리 다행히, 2000년도부터 국내에서 시험을 치를 수 있으며, 한글로도 응시할 수 있다. 그러므로, 학습자들이 마음 놓고 공부에 집중할 수 있게 되었다. 총 1년에 4회 시험을 집행하며, 해당 시험일자는 (ISC)²와 동국대학교, 한국생산성본부가 협의하여 국내 사정을 고려하여 가장 적합한 일자에 시험을 집행하고 있다.

6-1. 2010년도 CISSP 시험 일정

구분	시험 일시	장소
1차	2010년 2월 27일(토)	동국대학교
2차	2010년 6월 26일(토)	동국대학교
3차	2010년 8월(토)	동국대학교
4차	2010년 12월(토)	동국대학교

6-2. 시험 영역

CISSP의 시험 영역은 우리나라 시험의 과목과 같은 의미의 도메인(Domain)으로 구분되며, 총 10개의 도메인을 치르게 되어있다. 하지만, 시험지에는 도메인별 영역 구분이 없이, 여러 도메인이 섞여서 출제된다. 시험에 출제되는 10개의 도메인은 다음과 같으며, 이 도메인은 앞으로 우리가 5회에 걸쳐서 살펴볼 내용이다.

[(ISC)² CBK Domains]

Information Security and Risk Management(정보 보호 및 위험 관리)	Access Control(접근 제어)
Cryptography(암호학)	Physical(Environmental) Security(물리적 보안)
Security Architecture and Design (보안 아키텍처 및 설계)	Business Continuity and Disaster Recovery Planning (사업 연속 계획 및 재난 복구 계획)
Telecommunications and Network Security(통신 및 네트워크 보안)	Application Security(응용 프로그램 보안)
Operations Security (운영 보안)	Legal, Regulations, Compliance and Investigations (법, 규제, 규제대응 및 수사)

6-3. (ISC)² CBK 10Domain

시험에 출제되는 10개의 Domain은 CISSP의 Bible인 CISSP CBK(Common Body of Knowledge)에 포함되어 있다. 각 도메인별 출제 내용은 다음과 같다.

[(ISC)² CBK Domains 상세 설명]

분야	내용	비고
정보보안과 위험관리	기업 자산(asset)의 식별, 요구되는 보호 수준을 결정하는 올바른 방법, 위협과 재정적 손실을 감소하기 위한 목표를 가지는 보안 수행을 개발하기 위한 예산의 유형에 대한 지식을 확인	
접근 통제	관리자와 매니저, 주체가 접근할 수 있는 대상, 인증(authentication)과 허가(authorization) 후의 주체의 능력의 범위, 그리고 이러한 활동에 대한 감사(auditing)와 모니터링(monitoring)을 통제하기 위해 사용하는 방법과 원리에 대한 지식을 확인	통제기법
암호학	보호 목적으로 데이터를 위장하는 방법과 기법과 다양한 암호화 기법, 접근 방식, 그리고 기술에 대한 지식을 확인	
물리적 보안	위협(threats), 위험(risks), 시설물, 하드웨어, 데이터, 매체 그리고 직원을 보호하기 위한 대책에 대한 지식을 확인	
보안 아키텍처 및 설계	안전한 응용 프로그램, 운영 시스템, 그리고 시스템을 디자인하고 구현하기 위한 개념, 원칙, 표준에 대한 지식을 확인	
사업 연속계획 및 재난 복구 계획	재난과 혼란에 직면하는 경우에 비즈니스 활동의 보존 방법과 실제 위협의 식별, 올바른 위험 평가, 그리고 대책 수행에 대한 지식을 확인	BCP/DRS
통신 및 네트워크 보안	네트워킹 구조, 장치, 프로토콜(protocols), 원격 접근 및 관리와 같은 내부, 외부, 그리고 공개 및 사설 통신 시스템에 대한 지식을 확인	
응용 프로그램 보안	운영 시스템과 응용 프로그램의 보안 구성요소, 이들의 효용성을 가장 잘 측정하고 개발하는 방법론과 소프트웨어 수명 주기(life cycles), 변경 통제(change control), 그리고 응용 프로그램 보안에 대한 지식을 확인	
운영 보안	사람, 하드웨어, 시스템에 대한 통제, 감사와 모니터링 기법과 가능한 남용 채널(abuse channels)과 그것을 감지하고 해결하는 방법에 대한 지식을 확인	
법, 규제, 대응 및 수사	컴퓨터 범죄, 법, 규정과 범죄를 조사하고, 증거를 수집하고 처리하는 절차에 대한 지식을 확인	포렌식

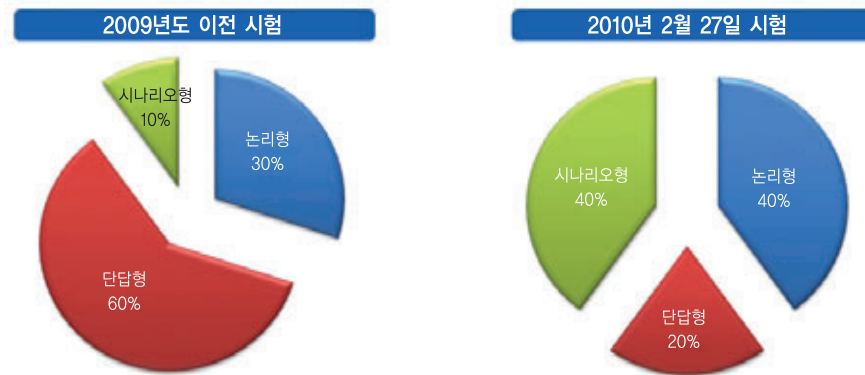
6-4. CBK 10Domain 출제 비율

CBK 10Domain이 균등하게 출제되는 것이 아니라, 시기와 중요성에 따라서 출제 비중은 다르다. (ISC)²에서는 공식자료를 제공하고 있지 않으며, 각종 커뮤니티에서 제공하는 내용들을 모아서 검토해보면 다음과 같다. 본 자료는 저자 개인적인 소견이며, (ISC)²와는 무관함을 밝힌다. CISSP는 2009년도부터 출제되는 시험의 유형이 많이 변경되었으며, 이는 국내 암기식 위주의 시험학습법을 제공하는 일부 사설 학원으로 인해 수준 부족의 CISSP 배출이라는 폐해를 막고자 (ISC)²에서 실행한 극약처방이라고 할 수 있다. 따라서, 2009년도 이전에는 암기식으로 답할 수 있는 선다형(단답형) 문제가 주를 이루었으나, 최근에는 사고와 현장 경험을 요구하는 논리형 문제와 시나리오형 문제가 다수 출제되어 난이도가 향상되었다고 할 수 있다.

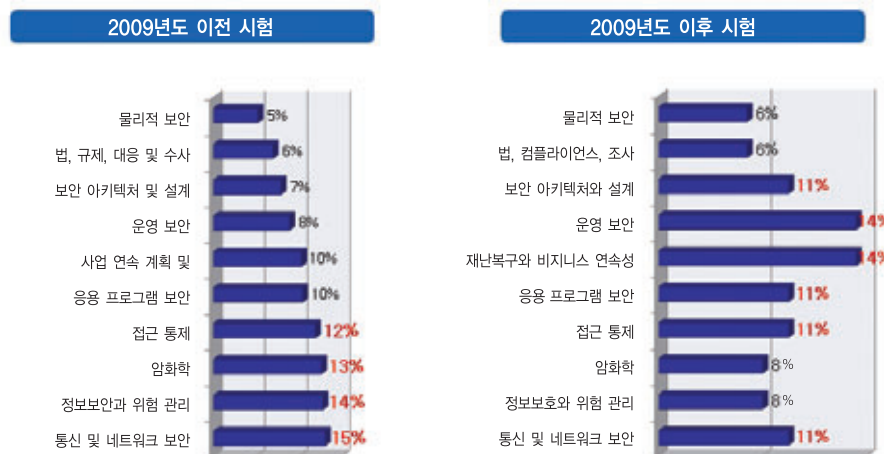
- ▶ 단답형 : 단순한 형태의 관리적, 물리적, 기술적 용어에 대한 정의를 묻는 문제
- ▶ 논리형 : 관리적, 물리적, 기술적 구성요소 중 복잡한 기능에 대해 묻는 문제로, 단답형 문제의 난이도를 높이기 위해 변형한 문제
- ▶ 시나리오형 : 상황을 설명하는 0.5~1 페이지 정도의 지문을 제시하고, 해당 지문일 때 발생할 수 있는 문제점과 최적의 방안을 묻는 문제

실제 시험에 대한 공식 발표가 없기 때문에 본 자료는 객관적인 수치라기보다는 커뮤니티에 올라온 사용자의 시험 후의 느낌을 기록한 후기위주로 작성된 것임에 다시 한 번 유의하기 바란다. 하지만, 전체적으로 본 자료에 대한 동의를 표하는 사람들이 많아, 본 자료만으로도 시험의 변화를 유추하기에는 충분할 것으로 보인다. 또한, 2009년도 이후로 CBK Domain별 출제 비율도 일부 변화가 있었던 것으로 보인다. 2009년 이전까지는 기술적 용어를 묻는 문제가 많은 비중을 차지하였으나, 2009년도 이후부터는 어떤 상황에서 정책적인 판단을 묻는 문제들이 증가하는 추세로 보인다. 이는 기존의 단순 용어 암기 위주의 문제에서 상황을 제시하고 최적의 답안을 고르도록 하는 난이도 높은 문제들이 많이 출제되기 때문이다.

[그림 2] CISSP 10Domain 출제 비율도 객관적 수치라기보다는 커뮤니티에 올라온 각종 후기들을 취합한 정성적 자료이므로, 시험 변화 유형을 파악하는데 참고하기 바란다.



[그림 1] CISSP 시험 변화



[그림 2] CISSP 10Domain 출제 비율

7. CISSP 시험은 어떻게 준비해야 되는가?

2009년 이후부터 암기식 학습을 지향하는 사설학원의 폐해로 전문 지식이 없는 일부 CISSP 자격자가 배출되고, 그러한 자격자들은 곧 활동이 없어 자격을 유지하지 못하는 상황이 벌어졌다. 이러한 문제 점을 막고자 (ISC)²에서는 시험을 변경하였다. 따라서, CISSP를 준비 하는 수험생들은 변화된 시험 경향을 분석하여 제대로 된 학습이 필 요하겠다. 필자는 이번 호를 통해 시험 경향 분석결과와 함께 학습 방법에 대해서 안내하고자 한다.

7-1. 시험 경향 분석

단편 지식 거절	· 문제와 답을 암기한 응답자는 뽑지 않겠다. · 단편적인 지식으로는 묻는 문제에 20%만 답할 수 있음
깊이 있는 학습 요구	· 토픽에 대해 정확한 이해가 있어야 풀 수 있는 문제 · 문제를 꼬고 꼬아서 출제
실무능력 보유 체크	· 지식이 구조화되어 논리적인 조치가 가능한지 확인 · 시나리오를 제시하여 실무 조치 능력을 체크
넓은 시야 요구	· 보안의 숲을 볼 수 있는지를 체크(BCP, 보안 아키텍처) · 보안 전문가로서 CISSP의 위치를 공고히 하고자 함

7-2. 시험 합격 전략

기본 지식 학습	· 개인 학습 또는 (ISC) ² 공인 교육기관을 통한 기본 지식 학습
반복적인 복습	· 충실한 교재를 이용한 개인 복습 · 매일 1시간 이상 복습(지하철, 버스 이용)
문제 풀이	· 최신 경향을 반영한 모의 문제로 구성된 핵심 문제를 이용한 학습 · 시험 1개월 전부터 문제 적응력 향상
문제 복습	· 내가 아는 것과 모르는 것에 대한 체크(틀린 문제) · 시험 3주전부터 틀린 문제의 관련 토픽을 다시 복습

시험이라는 것은 합격이 가장 중요하겠으나, 올바른 학습이 전제 되 지 않을 경우에는 합격 후에도 몇몇하지 못하고, 자신의 자격증을 100% 활용하지 못하게 된다. 따라서, 앞의 학습 전략을 적극 활용하 여 유비쿼터스와 클라우드 서비스로 대표되는 지식 총아의 시대에서 보안 전문가로 한 걸음을 내딛기 바란다.

다음 호에는 CISSP 도메인별로 주요 학습 내용과 연습 문제를 제시 하여, 앞으로 CISSP 합격으로 여러분을 안내하고자 한다.

[CISSP 참고 사이트]

(ISC)² 공식 사이트

- URL : <http://www.isc2.org/>
- 주요 활동 : CISSP 시험 신청 및 CISSP 관련 공식 정보 제공 사이트



한국 CISSP 협회

- URL : <http://www.ciisspkorea.or.kr>
- 주요 활동 : CISSP 국내 공식 Chapter로서, CISSP 시험 집행 및 Endorsement 지원



한국생산성본부

- URL : <http://www.kpc.or.kr>
- 주요 활동 : 국내 유일의 (ISC)² 공인 교육기관으로 온·오프라인 시험 접수 안내 및 공식 정보 제공



정보보호 커뮤니티 Korsec

- URL : <http://cafe.naver.com/korsec>
- 주요 활동 : (ISC)² 공인강사들이 운영하는 사이트로서, 최신 시험경향 및 학습정보, Q&A 등을 무료 제공

