SSCP®

Systems Security Certified Practitioner

An (ISC)² Certification

자격증 **시험 개요**

발효일: 2021년 11월

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

SSCP 정보

Systems Security Certified Practitioner (SSCP®)는 운영 IT 역할에서 입증된 기술과 실용적인 실무 보안 지식을 갖춘 사람들에게 이상적인 인증입니다. 본 인증을 통해 데이터 기밀성, 무결성 및 가용성을 보장하는 정보 보안 정책 및 절차에 따라 IT 인프라를 구현, 모니터링 및 관리하는 실무자의 능력을 확인합니다.

SSCP 공통 지식 체계(CBK®)에 포함된 광범위한 주제는 정보 보안 분야의 모든 분야에 대한 관련성을 보장합니다. 합격자는 다음 7개 도메인에 관한 능력을 입증합니다.

- 보안 운영 및 관리
- 액세스 통제
- 위험 식별, 모니터링 및 분석
- 사고 대응 및 복구
- 암호화
- 네트워크 및 통신 보안
- 시스템 및 어플리케이션 보안

경력 요구 사항

응시자는 SSCP CBK의 7개 영역 중 하나 이상에서 합계 최소 1년의 업무 경험이 있어야 합니다. 사이버 보안 프로그램에서 학위(학사 또는 석사)를 받은 후보자에게는 1년의 업무 경력이 부여됩니다.

SSCP가 되는데 필요한 경험이 없는 응시자는 SSCP 시험을 성공적으로 통과하여 (ISC)²의 준회원이 될 수 있습니다. (ISC)²의 준회원은 1년의 필수 경력을 쌓기 위해 2년의 기간이 주어집니다. SSCP 경력 요구 사항과 파트 타임 및 인턴십을 지원하는 방법에 대한 자세한 사항은 **www.isc2.org/Certifications/SSCP/experience-requirements**에서 확인하십시오.

인증

SSCP는 ANSI/ISO/IEC 표준 17024의요구 사항을 엄격히 준수합니다.

직무 과 분석(JTA)

(ISC)²는 회원들을 위해 SSCP의 관련성 유지할 의무가 있습니다. 직무 분석(JTA)은 SSCP가 정의한 직무에 종사하는 보안 전문가의 수행 과제를 결정하는 체계적이며 정기적으로 수행되는 중요한 프로세스입니다. JTA의 결과는 시험을 업데이트하는 데 사용됩니다. 이 과정을 통해 응시자는 오늘날의 현업 정보 보안 전문가의 역할 및 책임과 관련된 주제 분야에서 테스트를 거치게 됩니다.

SSCP 시험 정보

시험 시간	4시간
문항 수	150
문항 형식	다지선다형
합격 점수	700점 이상(총점 1000점)
시험 가능 언어	영어, 일본어, 중국어, 한국어, 독일어, 스페인어
테스트 센터	Pearson VUE 테스트 센터

SSCP 출제 비중

도메인	비율
1. 보안 운영 및 관리	16%
2. 액세스 통제	15%
3. 위험 식별, 모니터링 및 분석	15%
4. 사고 대응 및 복구	14%
5. 암호학	9%
6. 네트워크 및 통신 보안	16%
7. 시스템 및 어플리케이션 보안	15%
	총: 100%

도메인 1: 보안 운영 및 관리

1.1 윤리강령 준수

» (ISC)² 윤리 강령
» 조직 윤리 강령

1.2 보안 개념 이해

» 기밀성
» 무결성
» 가용성
» 책임 추적성
» 개인 정보 보호
» 부인 방지
» 최소 권한
» 직무 분리(SoD)

1.3 보안 통제 식별 및 구현

» 기 술 통제(예: 세션 시간 초과, 암호 에이징)
» 물리적 제어(예: 맨트랩, 카메라, 자물쇠)
» 관리 제어(예: 보안 정책, 표준, 절차, 기준선)
» 규정 준수 평가
» 정기 감사 및 검토

1.4 기능적 보안 통제 문서화 및 유지 관리

» 억제 통제
» 예방 통제
» 탐지 통제
» 교정 통제
» 보완 통제

1.5 자산 관리 수명 주기 참여(하드웨어, 소프트웨어 및 데이터)

» 프로세스, 계획, 설계 및 착수
» 개발/인수
» 인벤토리 및 라이선스
» 구현/평가
» 운영/유지보수
» 아카이빙 및 보존 요구 사항
» 폐기 및 파기

1.6 변경 관리 수명 주기에 참여

» 변경 관리(예: 역할, 책임, 프로세스)
» 보안 영향 분석
» 구성 관리(CM)

1.7 보안 인식 및 교육(예: 사회 공학/피싱) 구현에 참여

1.8 물리적 보안 작업과 협력(예: 데이터 센터 평가, 배지)

도메인 2: 액세스 통제

2.1 인증 방법 구현 및 유지 관리

» 단일/다중 인증(MFA)
» 통합 인증(SSO)(예: 액티브 디렉토리 페더레이션 서비스(ADFS), OpenID Connect)
» 기기 인증
» 페더레이션 액세스(예: 공개 승인 2(OAuth2), 보안 접근제어 명령 생성 언어(SAML))

2.2 네트워크간 신뢰 아키텍처 지원

» 신뢰 관계(예: 단방향, 양방향, 전이적, 제로)
» 인터넷, 인트라넷 및 엑스트라넷
» 타사 연결

2.3 ID 관리 수명 주기에 참여

» 승인
» 증명
» 프로비저닝/디프로비저닝
» 유지 관리
» 자격
» ID 및 접근 통제(IAM) 시스템

2.4 액세스 제어 이해 및 적용

» 필수 사항
» 임의 사항
» 역할 기반(예: 속성, 주제, 객체 기반)
» 규칙 기반

도메인 3:
위험 식별, 모니터링 및 분석

3.1 위험 관리 프로세스 이해

» 위험 가시성 및 보고(예: 위험 등록, 위협 인텔리전스/침해 지표(IOC) 공유, 공통 취약점 평가 시스템(CVSS))
» 위험 관리 개념(예: 영향 평가, 위협 모델링)
» 위험 관리 프레임워크(예: 국제 표준화 기구(ISO), 국립표준기술연구소(NIST))
» 위험 내성(예: 성향)
» 위험 처리(예: 수용, 이전, 완화, 회피, 무시)

3.2 법적 및 규제 문제 이해(예: 관할권, 제한 사항, 개인 정보 보호)

3.3 보안 평가 및 취약점 관리 활동 참여

» 보안 테스트
» 위험 검토(예: 내부, 공급자, 아키텍처)
» 취약점 관리 수명 주기

3.4 보안 평가 및 취약점 관리 활동 참여

» 소스 시스템(예: 어플리케이션, 보안 어플라이언스, 네트워크 장치 및 호스트)
» 관심 이벤트(예: 이상, 침입, 무단 변경, 규정 준수 모니터링)
» 로그 관리
» 이벤트 집계 및 상관 관계

3.5 모니터링 결과 분석

» 보안 기준 및 이상
» 시각화, 메트릭 및 추세(예: 알림, 대시보드, 타임라인)
» 이벤트 데이터 분석
» 결과 문서화 및 전달(예: 에스컬레이션)

도메인 4: 사고 대응 및 복구

4.1 사고 수명 주기 지원(예: 국립표준기술연구소(NIST), 국제 표준화 기구(ISO))

» 준비
» 탐지, 분석 및 에스컬레이션
» 격리
» 근절
» 복구
» 교훈/새로운 대책의 실행

4.2 포렌식 조사 이해 및 지원

» 법적(예: 민사, 형사, 행정) 및 윤리 원칙
» 증거 처리(예: 최초 대응자, 분류, 보관 연속성, 현장 보존)
» 분석 보고

4.3 업무 연속성 계획(BCP) 및 재난 복구 계획(DRP) 활동 이해 및 지원

» 비상 대응 계획 및 절차(예: 정보 시스템 비상 사태, 전염병, 자연 재해, 위기 관리)
» 임시 또는 대체 처리 전략
» 복원 계획
» 백업 및 이중화 구현
» 테스트 및 훈련

도메인 5: 암호화

5.1 암호화의 이유와 요구 사항 이해

» 기밀성
» 무결성 및 인증성
» 데이터 민감도(예: 개인 식별 정보(PII), 지적 재산(IP), 보호 의료 정보(PHI))
» 규제 및 업계 모범 사례(예: 결제 카드 산업 정보보안 표준(PCI-DSS), 국제 표준화 기구(ISO))

5.2 암호화 개념 적용

» 해싱
» 솔팅
» 대칭/비대칭 암호화/타원 곡선 암호화(ECC)
» 부인 방지(예: 디지털 서명/인증서, 해시 메시지 인증 코드(HMAC), 감사 추적)
» 암호화 알고리즘 및 키의 강점(예: 고급 암호화 표준(AES), 리베스트 셰미르 아델만(RSA), 256, 512, 1024, 2048비트 키)
» 암호 공격, 암호 분석 및 대응책(예: 양자 컴퓨팅)

5.3 보안 프로토콜 이해 및 구현

» 서비스 및 프로토콜(예: 인터넷 프로토콜 보안(IPsec), 전송 계층 보안
» (TLS), 암호화 이메일 전송(S/MIME), 도메인 키 식별 메일(DKIM))
» 일반적인 사용 사례
» 제한 사항 및 취약점

5.4 공개 키 인프라(PKI) 시스템 이해 및 지원

» 기본 키 관리 개념(예: 보관, 순환, 구성, 생성, 파기, 교환, 철회, 에스크로)
» 신뢰의 웹(WOT)(예: 개인정보 보호를 위한 이메일 암호화(PGP), GNU 프라이버시 가드(GPG), 블록체인)

도메인 6: 네트워크 및 통신 보안

6.1 네트워킹의 기본 개념을 이해와 적용

» 개방형 시스템 간 상호접속(OSI) 및 전송 제어 프로토콜/ 인터넷 프로토콜(TCP/IP) 모델
» 네트워크 토폴로지
» 네트워크 관계(예: 동등형(P2P), 클라이언트 서버)
» 전송 매체 유형(예: 유선, 무선)
» 소프트웨어 정의 네트워킹(SDN)(예: 소프트웨어 정의 광역 네트워크(SD-WAN), 네트워크 가상화, 자동화)
» 일반적으로 사용되는 포트 및 프로토콜

6.2 네트워크 공격 (예: 분산 서비스 거부(DDoS), 중간자 공격(MITM), 도메인 네임 시스템 (DNS) 포이즈닝) 및 대응책(예: 콘텐츠 전송 네트워크(CDN)) 이해

6.3 네트워크 액세스 제어 관리

» 네트워크 액세스 제어, 표준 및 프로토콜(예: 전기 전자 엔지니어 협회(IEEE) 802.1X, 원격 인증 전화 접속 사용자 서비스(RADIUS), 터미널 액세스 컨트롤러 액세스 제어 시스템 플러스(TACACS+))
» 원격 액세스 운영 및 구성(예: 씬 클라이언트, 가상 사설망(VPN))

6.4 네트워크 보안 관리

» 네트워크 장치의 논리적 및 물리적 배치(예: 인라인, 수동, 가상)
» 세분화(예: 물리적/논리적, 데이터/제어 평면, 가상 근거리 통신망(VLAN), 접근 통제 목록(ACL), 방화벽 영역, 마이크로 세분화)
» 보안 장치 관리

6.5 네트워크 기반 보안 장치 운영 및 구성

» 방화벽 및 프록시(예: 필터링 방법, 웹 어플리케이션 방화벽(WAF))
» 침입 탐지 시스템(IDS) 및 침입방지시스템(IPS)
» 라우터 및 스위치
» 트래픽 조절 장치(예: 광역망(WAN) 최적화, 로드 밸런싱)

6.6 안전한 무선 통신

» 기술(예: 셀룰러 네트워크, Wi-Fi, Bluetooth, 근거리 무선통신(NFC))
» 인증 및 암호화 프로토콜(예: 유선 동등형 정보보호(WEP), 와이파이 보호 접속(WPA), 확장 인증 프로토콜 (EAP))
» 사물 인터넷(IoT)

도메인 7: 시스템 및 어플리케이션 보안

7.1 악성 코드 및 활동 식별 및 분석

- 맬웨어(예: 루트킷, 스파이웨어, 스케어웨어, 랜섬웨어, 트로이 목마, 바이러스, 웜, 트랩도어, 백도어, 파일리스
- 맬웨어 대응책(예: 스캐너, 맬웨어 방지, 코드 서명)
- 악의적인 활동(예: 내부 위협, 데이터 도난, 분산 서비스 거부(DDoS), 봇넷, 제로 데이 익스플로잇, 웹 기반 공격, 지능형 지속 공격(APT))
- 악의적 행위 대응(예: 사용자 인식, 시스템 강화, 패치, 격리, 데이터 손실 방지(DLP))
- 사회 공학(예: 피싱, 사칭)
- 행동 분석(예: 기계 학습, 인공 지능(AI), 데이터 분석)

7.2 엔드포인트 장치 보안 구현 및 운영

- 호스트 기반 침입방지시스템(HIPS)
- 호스트 기반 방화벽
- 어플리케이션 허용 목록
- 엔드포인트 암호화(예: 전체 디스크 암호화)
- 신뢰할 수 있는 플랫폼 모듈(TPM)
- 보안 검색
- 엔드포인트 탐지 및 대응(EDR)

7.3 모바일 장치 관리(MDM)

- 프로비저닝 기술(예: 기업 소유, 개인 사용(COPE), 개인 소유 기기의 업무 활용(BYOD))
- 컨테이너화
- 암호화
- 모바일 어플리케이션 관리(MAM)

7.4 클라우드 보안 이해 및 구성

- 배포 모델(예: 퍼블릭, 프라이빗, 하이브리드, 커뮤니티)
- 서비스 모델(예: 서비스형 인프라(IaaS), 서비스형 플랫폼(PaaS) 및 서비스형 소프트웨어(SaaS))
- 가상화(예: 하이퍼바이저)
- 법률 및 규제 문제(예: 개인 정보 보호, 감시, 데이터 소유권, 관할권, eDiscovery)
- 데이터 저장, 처리 및 전송(예: 아카이빙, 복구, 복원력)
- 타사/아웃소싱 요구 사항(예: 서비스 수준 협약(SLA), 데이터 이동성, 데이터 파기, 감사)
- 공동 책임 모델

7.5 안전한 가상 환경 운영 및 유지

- 하이퍼바이저
- 가상 어플라이언스
- 컨테이너
- 연속성과 탄력성
- 공격 및 대응책
- 공유 스토리지

시험 관련 추가 정보

추가 참조 사항

응시자는 CBK와 관련된 자료를 검토하고 추가 관심이 필요한 부분을 확인함으로써 교육 및 경험을 보완할 것을 권장합니다.

추가 참조 전체 목록은 www.isc2.org/certifications/References에서 확인하십시오.

시험 정책 및 절차

(ISC)²는 SSCP 지원자가 시험에 등록하기에 앞서 시험 정책 및 절차를 검토할 것을 권장합니다. 중요한 정보에 대한 종합적인 내용은 www.isc2.org/Register-for-Exam 에서 확인하십시오.

법률 정보

(ISC)²의 법률 정책과 관련된 질문은 (ISC)2 법무팀에 legal@isc2.org로 문의하십시오.

문의사항 연락처

(ISC)² 아메리카
전화번호: +1.866.331.ISC2 (4722)
이메일: info@isc2.org

(ISC)² 아시아 태평양 전화번호: +(852) 28506951
이메일: isc2asia@isc2.org

(ISC)² 유럽, 중동, 아프리카
전화번호: +44 (0)203 300 1625
이메일: info-emea@isc2.org