SSCP®

Systems Security Certified Practitioner

An (ISC)² Certification

认证 考试大纲

生效日期：2021 年 11 月

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

关于 SSCP

系统安全认证从业者 (SSCP®) 是针对在 IT 运营方面具备熟练技术并掌握实践安全知识的从业者的理想认证。该认证旨在认可从业者遵照信息安全政策和程序实施、监控和管理 IT 基础架构的能力，以确保数据的保密性、完整性和可用性。

SSCP 的公共知识体系（CBK®）中包含的广泛议题确保了信息安全领域中所有原理的相关性。通过认证的考生展示出在以下七大知识领域的能力：

- 安全运营与管理
- 访问控制
- 风险识别、监控和分析
- 事故响应和恢复
- 密码学
- 网络与通信安全
- 系统和应用安全

经验要求

考生必须在 SSCP CBK 的七个领域中的一个或多个领域拥有至少一年的工作经验的累积。如果考生拥有网络安全专业学位（学士或硕士），可获得一年的工作经验减免。

没有满足 SSCP 所需工作经验的考生，如果能够通过 SSCP 考试则可以成为 (ISC)² 的准会员（即 Associate）。(ISC)² 的准会员可以用接下来的两年时间积累所需的一年工作经验。欲了解更多关于 SSCP 工作经验要求以及如何计算兼职工作和实习经验的信息，请访问 www.isc2.org/Certifications/SSCP/experience-requirements。

认证

SSCP 认证符合 ANSI/ISO/IEC 17024 标准的严格要求。

工作任务分析 (JTA)

(ISC)² 有义务保持其会员所持 SSCP 认证的相关性。定期进行工作任务分析（JTA）是一个系统而关键的过程，用以确定从事 SSCP 所定义的专业领域的安全专业人士所执行的任务。JTA 的分析结果会用来更新考试的内容。确保了考生的测试题目与目前从业的信息安全专业人士的角色和职责密切相关。

SSCP 考试信息

考试时长	4 小时
考题数量	150
考题类型	多选择项
及格分数	1000 分中得到 700 分
考试语言	英语、日语、中文、韩语、德语和西班牙语
考试中心	Pearson VUE 考试中心

SSCP 考试的权重

领域	权重
1.安全运营与管理	16%
2.访问控制	15%
3.风险识别、监控和分析	15%
4.事故响应和恢复	14%
5.密码学	9%
6.网络与通信安全	16%
7.系统和应用安全	15%
总计:	**100%**

领域 1:
安全运营与管理

1.1 遵守道德规范

» (ISC)² 道德规范
» 组织道德规范

1.2 了解安全概念

» 机密性
» 完整性
» 可用性
» 可追责性
» 隐私保护
» 不可抵赖性
» 最小特权
» 职责分离 (SoD)

1.3 识别并实施安全控制

» 技术控制（例如，会话超时、密码老化）
» 物理控制（例如，诱捕陷阱、摄像头、锁）
» 管理控制（例如，安全政策、标准、程序、基线）
» 评估合规性
» 定期审计和审查

1.4 记录并维护功能性安全控制

» 威慑性控制
» 预防性控制
» 检测性控制
» 纠正性控制
» 补偿性控制

1.5 参与资产管理生命周期（硬件、软件、数据）

» 流程、规划、设计和启动
» 开发/获取
» 库存和许可
» 实施/评估
» 操作/维护
» 归档和保留要求
» 处置和销毁

1.6 参与变更管理生命周期

» 变更管理（例如，角色、职责、流程）
» 安全影响分析
» 配置管理 (CM)

1.7 参与实施安全意识和培训（例如，社会工程/网络钓鱼）

1.8 与物理安全运营协作（例如，数据中心评估、标记）

领域 2: 访问控制

2.1 实施和维护身份认证方法

» 单/多因子认证 (MFA)
» 单点登录 (SSO)（例如，活动目录联合服务 (ADFS)、OpenID 连接）
» 设备身份认证
» 联合访问（例如，开放授权 2 (OAuth2)、安全断言标记语言 (SAML)）

2.2 支持互联网络信任架构

» 信任关系（例如，单向、双向、可传递、零信任）
» 互联网、内联网和外联网
» 第三方连接

2.3 参与身份管理生命周期

» 授权
» 认证
» 配置/取消配置
» 维护
» 权限
» 身份识别访问管理 (IAM) 系统

2.4 了解和应用访问控制

» 强制
» 自主
» 基于角色（例如，基于属性、主体、对象）
» 基于规则

领域 3:
风险识别、监控和分析

3.1 了解风险管理流程

» 风险可见性和报告（例如，风险登记簿、共享威胁情报/感染指标 (IOC)、通用漏洞评分系统 (CVSS)）
» 风险管理概念（例如，影响评估、威胁建模）
» 风险管理框架（例如，国际标准组织 (ISO)、国家标准与技术协会 (NIST)）
» 风险承受能力（例如，偏好）
» 风险处理（例如，接受、转移、缓解、避免、忽略）

3.2 了解法律和监管问题（例如，管辖权、限制、隐私）

3.3 参与安全评估和漏洞管理活动

» 安全测试
» 风险审查（例如，内部、供应商、架构）
» 漏洞管理生命周期

3.4 运营和监控安全平台（例如，持续监控）

» 源系统（例如，应用程序、安全设备、网络设备和主机）
» 受关注的事件（例如，异常、入侵、未经授权的更改、合规性监控）
» 日志管理
» 事件聚合和关联

3.5 分析监控结果

» 安全基线和异常
» 可视化、指标和趋势（例如，通知、仪表板、时间线）
» 事件数据分析
» 记录和交流结果（例如，升级）

领域 4:
事故响应和恢复

4.1 支持事故生命周期（例如，国家标准与技术协会 (NIST)、国际标准组织 (ISO)）

» 准备
» 检测、分析和升级
» 遏制
» 根除
» 恢复
» 经验教训/实施新对策

4.2 了解并支持取证调查

» 法律（例如，民事、刑事、行政）和道德原则
» 证据处理（例如，第一响应者、鉴别分类、保管链、现场保护）
» 分析报告

4.3 了解并支持业务连续性计划 (BCP) 和灾难恢复计划 (DRP) 活动

» 应急计划和程序（例如，信息系统应急、疫情、自然灾害、危机管理）
» 临时或备用处理策略
» 恢复计划
» 备份和冗余实施
» 测试和演练

领域 5: 密码学

5.1 了解密码学的原因和要求

» 机密性
» 完整性和真实性
» 数据敏感性（例如，个人可识别信息 (PII)、知识产权 (IP)、受保护的健康信息 (PHI)）
» 监管和行业最佳实践（例如，支付卡行业数据安全标准 (PCI-DSS)、国际标准组织 (ISO)）

5.2 应用密码学概念

» 散列
» 加盐
» 对称/非对称加密/椭圆曲线密码学 (ECC)
» 不可抵赖性（例如，数字签名/证书、信息散列验证码 (HMAC)、审计跟踪）
» 加密算法和密钥的强度（例如，高级加密标准 (AES)、RSA 密码、256位、512 位、1024 位、2048 位密钥）
» 密码攻击、密码分析和对策（例如，量子计算）

5.3 了解和实现安全协议

» 服务和协议（例如，互联网协议安全 (IPsec)、传输层安全（TLS)、安全多用途互联网邮件扩展 (S/MIME)、
» 域密钥识别邮件 (DKIM)）
» 常见用例
» 限制和漏洞

5.4 了解和支持公钥基础架构 (PKI) 系统

» 基本密钥管理概念（例如，存储、轮转、组合、生成、销毁、交换、撤销、托管）
» 信任网络 (WOT)（例如，优良保密协议 (PGP)、GNU 隐私卫士 (GPG)、区块链）

领域 6:
网络与通信安全

6.1 了解和应用网络的基本概念

» 开放系统互连 (OSI) 和传输控制协议/互联网协议 (TCP/IP) 模型
» 网络拓扑
» 网络关系（例如，点对点 (P2P)、客户端服务器）
» 传输媒介类型（例如，有线、无线）
» 软件定义网络 (SDN)（例如，软件定义广域网 (SD-WAN)、网络虚拟化、自动化）
» 常用端口和协议

6.2 了解网络攻击（例如，分布式拒绝服务 (DDoS)、中间人攻击 (MITM)、域名系统 (DNS) 投毒）和对策（例如，内容分发网络 (CDN)）

6.3 管理网络访问控制

» 网络访问控制、标准和协议（例如，电气与电子工程师协会 (IEEE) 802.1X、远程验证拨号用户服务 (RADIUS)、终端访问控制器访问控制系统增强版 (TACACS+)）
» 远程访问操作和配置（例如瘦客户端、虚拟专用网 (VPN)）

6.4 管理网络安全

» 网络设备的逻辑和物理位置（例如，行内、被动、虚拟）
» 分段（例如，物理/逻辑、数据/控制平面、虚拟局域网 (VLAN)、访问控制列表 (ACL)、防火墙区域、微分段）
» 安全设备管理

6.5 操作和配置基于网络的安全设备

» 防火墙和代理（例如过滤方法、Web应用防火墙 (WAF)）
» 入侵检测系统 (IDS) 和入侵防御系统 (IPS)
» 路由器和交换机
» 流量整形设备（例如，广域网 (WAN) 优化、负载平衡）

6.6 安全的无线通信

» 技术（例如，蜂窝网络、Wi-Fi、蓝牙、近场通信 (NFC)）
» 认证和加密协议（例如，有线等同隐私 (WEP)、Wi-Fi 保护访问 (WPA)、可扩展验证协议 (EAP)）
» 物联网 (IoT)

领域 7: 系统和应用安全

7.1 识别和分析恶意代码和活动

» 恶意软件（例如，Rootkit、间谍软件、恐吓软件、勒索软件、特洛伊木马、病毒、蠕虫、陷门、后门、无文件）

» 恶意软件对策（例如，扫描仪、反恶意软件、代码签名）

» 恶意活动（例如，内部威胁、数据盗窃、分布式拒绝服务 (DDoS)、僵尸网络、零日攻击、基于 Web 的攻击、高持续性威胁 (APT)）

» 恶意活动对策（例如，用户意识、系统强化、补丁、隔离、数据丢失防护 (DLP)）

» 社会工程（例如，网络钓鱼、假冒）

» 行为分析（例如，机器学习、人工智能 (AI)、数据分析）

7.2 实现和操作端点设备安全

» 基于主机的入侵防御系统 (HIPS)

» 基于主机的防火墙

» 应用白名单

» 终端加密（例如，整个磁盘加密）

» 可信赖平台模块 (TPM)

» 安全浏览

» 终端监测和响应 (EDR)

7.3 管理移动设备管理 (MDM)

» 配置技术（例如，企业拥有但个人使用 (COPE)、

» 自带设备 (BYOD)）

» 容器化

» 加密

» 移动应用管理 (MAM)

7.4 了解和配置云安全

» 部署模型（例如，公共云、私有云、混合云、社区云）

» 服务类别（例如，软件即服务 (SaaS)、基础架构即服务 (IaaS)、平台即服务 (PaaS)）

» 虚拟化（例如 Hypervisor）

» 法律和监管问题（例如，隐私、监视、数据所有权、管辖权、电子发现）

» 数据存储、处理和传输（例如归档、恢复、恢复能力）

» 第三方/外包要求（例如，服务等级协议 (SLA)、数据可移植性、数据销毁、审计）

» 责任共担模型

7.5 操作和维护安全的虚拟环境

» Hypervisor

» 虚拟设备

» 容器

» 连续性和恢复能力

» 攻击和对策

» 共享存储

附加考试信息

补充参考

鼓励考生通过审查与 CBK 相关的资源并确定可能需要额外关注的学习领域来补充其教育背景和经验。

请访问 www.isc2.org/certifications/References 查看补充参考的完整列表。

考试政策和程序

(ISC)² 建议 SSCP 考生在报名参加考试之前查看考试政策和程序。请访问 www.isc2.org/Register-for-Exam 阅读此重要信息的详解。

法律信息

如对 (ISC)² 的法律政策有任何问题, 请联系 (ISC)² 法务部 (电子邮件：legal@isc2.org。

有任何问题?

(ISC)² 美洲区

电话：+1.866.331.ISC2 (4722)
电子邮件：info@isc2.org

(ISC)² 亚太地区
电话：+852-5803-5662
电子邮件：isc2asia@isc2.org

(ISC)² 欧洲、中东及非洲地区
电话：+44 (0)203-960-7800
电子邮件：info-emea@isc2.org