国家信息安全水平考试

知识体系大纲

（安全运营专项）

NISP 专项证书管理中心

2020 年 12 月 30 日

目 录

一、概述

信息安全作为我国信息化建设健康发展的重要因素，关系到贯彻落实科学发展观、全面建设小康社会、构建社会主义和谐社会和建设创新型社会等国家战略举措的实施，是国家安全的重要组成部分。我国信息安全保障体系建设，需要完善信息安全立法，做好信息安全顶层设计，强化信息基础设施建设，特别地，需要加强信息安全人才培养与管理。在信息系统安全保障工作中，人是最核心、也是最活跃的因素，人员的信息安全意识、知识与技能已经成为保障信息系统安全稳定运行的重要基本要素之一，近年来，我国网络安全人才培养取得一定进展，但专业人才缺口仍然较大。

为培养更多优秀的实践型网络安全人才，中国信息安全测评中心推出了国家信息安全水平考试（National Information Security Test Program，简称 NISP）。NISP 考试采用理论与实践相结合的教学模式，是评定考生掌握信息安全知识、技能和本领的全国性信息安全水平考试体系。NISP 水平考试分通用证书和专项证书，通用证书分为一级和二级，分别定位于不同层次的目标群体。专项证书面向特定技术领域的人才培养。

NISP 一级主要面向各行业信息系统使用人员及高校非信息安全专业学生，普及信息安全知识，增强信息安全意识，提高安全防范技能，为今后工作中能安全的使用信息系统。

NISP 二级主要面向从事信息安全相关行业人员及高校信息安全相关专业学生，构建信息安全知识框架，帮助学员形成信息安全保障的总体概念，为国家信息安全保障工作的顺利实施打下坚实的理论基础。

NISP 三级（专项）主要面向有志于从事信息安全相关行业的从业人员，在理解信息安全基础知识基础上，掌握信息系统安全运营知识、渗透测试、信息系统审计、数据隐私保护、工业控制系统安全等特定信息安全领域的知识和技能，为国家培养跨领域的信息安全专项人才。

1.1 适用范围

本大纲从我国国情和企事业单位信息系统安全运营人才的需求出发，结合我国网络基础设施和重要信息系统安全保障的实际需求，兼顾知识体系的全面性、实用性和实践性。

本大纲明确 NISP 安全运营专项能力（NISP-SO）应当掌握的知识要点，是 NISP-SO 课程教材编制、讲师授课、学员学习以及考试命题的重要依据。

1.2 框架结构

NISP 课程使用组件模块化的结构，包括知识域和知识子域两个层次。

知识域：是属于同一技术领域的知识内容构成的相对独立的知识集合；

知识子域：是构成知识域的基本模块，对知识域进一步分解细化形成的完整的知识组件。每个知识子域由一至多个具体知识要点构成。

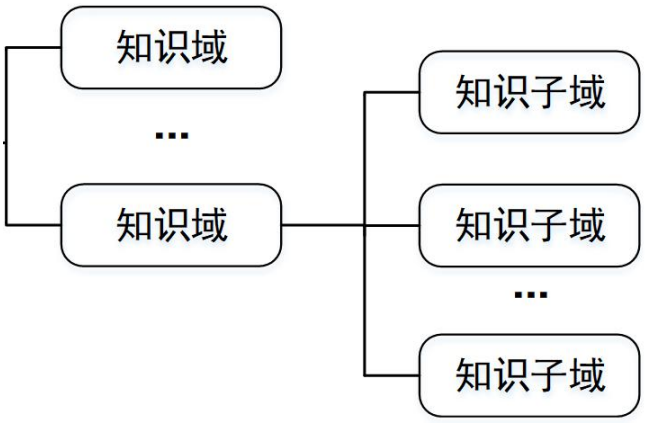

图 1：知识体系组件模块结构

本大纲规定了知识子域中每一个知识要点的内容和深度要求，分为“了解”、“理解”和“掌握”三类。

了解：是最低深度要求，学员需要正确认识该知识要点的基本概念和原理；

理解：是中等深度要求，学员需要在正确认识该知识要点的基本概念和原理的基础上，深入理解其内容，并可以进一步的判断和推理；

掌握：是最高深度要求，学员需要正确认识该知识点的概念、原理，并在深入理解的基础上灵活运用。

1.3 知识体系构成及考试

NISP 安全运营专项知识体系包括综合理论、专项基础和专项能力三个模块。

综合理论模块为所有 NISP 专项课程通用，采用 NISP 二级课程体系。

专项基础模块划分为八个知识域，是安全运营能力的基础，在培训时可根据学员基础水平安排适当课程。该模块中的知识在理论考试中均可能作为考点。

专项能力模块包括六个知识域，在理论考试和实操考试中会将此模块中的知识点作为考点。

图 2 NISP-SO （安全运营专项）知识体系结构

NISP 安全运营专项考试题型为选择题与实操题,总分共 100 分，其中理论题（单项选择题）40 分，实操题 60 分，得到 70 分以上（含 70 分）为通过。

二、专项基础模块

2.1 知识域：计算机及办公环境运维

2.1.1 知识子域：计算机桌面运维

熟悉计算机组成基本原理，具备设备攒机、硬件优化、故障排查、维修、升级、调优能力；

掌握 Windows 桌面操作系统安装、升级维护及常见问题解决；

了解 Windows 终端安全配置等相关要求。

了解 Linux 桌面操作系统安装、升级及常用软件安装、升级、维护及常见问题解决；

熟悉各类常见应用软件等的安装部署、调试、应用、故障诊断排查；

掌握计算机之间的网络联接及网络共享等配置。

2.1.2 知识子域：办公设备运维

熟悉打印机管理、安装、配置、共享、调试、维护等技术；

熟悉投影仪管理、安装、配置、维护等技术；

熟悉门禁系统管理、安装、配置、维护等技术。

2.1.3 知识子域：视频监控运维

熟悉视频监控设备前端、传输、控制、显示系统的常见设备；

熟悉监控设备的组网、安装，调试、配置和使用；

2.2 知识域：网络工程基础

2.2.1 知识子域：综合布线

了解综合布线系统七个子系统组网架构；

了解综合布线系统常用线缆的种类、区别，并能够制作实施；

了解综合布线系统相关标准及实施规范。

2.2.2 知识子域：计算机网络

掌握基础交换技术基础知识及相关协议（HDLC、PPP、PPPOE、ARP/RARP、STP 等）；

掌握基础路由技术基础知识及相关协议（static、ospf、bgp）；

掌握基础业务相关协议(DHCP、FTP、Telnet)；

掌握 vlan 技术及 vlan 间路由；

掌握访问控制相关技术及协议（nat、AAA）；

掌握常规 VPN 技术及协议（PPTP、L2TP、IPSec、GRE）；

掌握网络管理协议 SNMP 及相关网管软件的使用；

了解其他一些网络协议基本原理（MPLS、Segment Routing）；

掌握网络规划设计基础知识。

2.1.3 知识子域：无线网络运维

熟悉无线局域网体系结构，掌握无线局域网组网、调试及安全配置能力；

熟悉分布式无线 AP 组网及调试技术。

2.1.4 知识子域：机房基础维护

了解安防体系基础知识及信息化机房解决方案、日常维护及相关标准规范；

了解消防、电力保障等系统的日常维护、使用相关知识。

2.3 知识域：Window 系统安全基础

2.3.1 知识子域：windows 终端安全

了解 windows 终端安全安装的基本要求；

了解 Windows 终端安全配置等相关要求。

2.3.2 知识子域：windows server 安全设置

了解 windows server 安全安装的基本概念要求；

掌握 windows Server 安全策略设置；

掌握 windows 系统常用命令的使用。

2.3.3 知识子域：windows 系统服务配置

掌握 Windows server 上各类服务的部署及安全设置；

了解 Windows Server 上 VPN、远程终端等远程管理服务的部署及安全设置。

2.4 知识域：Linux 系统安全基础

2.4.1 知识子域：Linux 系统终端安全

了解 Linux 系统终端安装过程；

掌握 Linux 系统常用命令的使用；

了解 Linux 系统的日常使用及安全策略设置。

2.4.2 知识子域：Linux 系统服务安全部署

了解 Linux 系统服务器安装过程；

掌握 Linux 系统上 FTP、DNS、Openssh 等常用应用的安全部署。

2.5 知识域：网络与网络安全设备

2.5.1 知识子域：网络与网络设备

了解网络拓扑、网络结构等计算机网络基础知识；

了解路由器、交换机等网络设备的工作原理及作用；

了解 IP 地址规划、Vlan 等网络设计规划相关概念。

2.5.2 知识子域：防火墙

了解防火墙产品的基本概念、工作原理及应用场景；

了解包过滤、代理、NAT、状态检测等防火墙应用技术；

了解防火墙部署的方式及防火墙应用中的优缺点。

2.5.3 知识子域：边界安全设备

了解网闸的工作原理及应用场景；

了解 IPS、UTM 等边界安全防护设备的工作原理及应用场景；

了解防病毒网关、上网行为管理等防护设备的工作原理及应用场景。

2.5.4 知识子域：入侵检测与网络审计

了解入侵检测系统的基本概念、工作原理及应用场景；

了解入侵检测系统的数据采集、入侵检测实现原理；

了解入侵检测产品的类型、部署方式及优缺点；

了解网络审计、数据库审计等审计类产品的工作原理、部署方式及应用场景。

2.5.5 知识子域：虚拟专网（VPN）

了解虚拟专网（VPN）的概念，作用及应用场景；

了解 VPN 实现的技术原理及隧道模式、传输模式的区别；

了解 IPSec、SSL 两种不同 VPN 协议的区别。

2.6 知识域：Web 应用安全基础

2.6.1 知识子域：Web 浏览器安全

了解 Web 应用体系的结构及相关问题；

理解 Web 客户端（浏览器）常用的安全机制及安全风险；

理解浏览器端面临的网页挂马、网络钓鱼等攻击的技术原理并掌握浏览器安全设置方法。

了解 XML、HMTL 等 Web 应用中常用开发语言。

2.6.2 知识子域：HTTP 协议

理解 HTTP 协议的请求、响应工作机制；

了解 URL、请求方法（Post、get 等）、响应状态码等基本概念；

了解 cookie、session 等机制及存在的安全风险。

2.7 知识域：数据库安全基础

2.7.1 知识子域：数据库基础

了解 SQL 的基本概念并掌握 Select、update、delete 等常用的 SQL 命令的使用；

了解数据库用户、权限管理机制及安全策略；

了解存储过程、视图等数据库机制对安全的作用；

2.7.2 知识子域：数据库安全配置及管理

掌握 SQL server 安全配置、安全管理的方法与工具；

掌握 Mysql 安全配置、安全管理的方法与工具；

掌握 Oracle 安全配置、安全管理的方法与工具。

2.8 知识域：Web 服务软件安全

2.8.1 知识子域：IIS 服务配置及安全管理

掌握 IIS 服务网站配置的方法；

掌握 IIS 安全配置及安全管理的方法；

掌握 IIS 中 Https 的配置方法；

掌握 IIS 日志安全配置及管理相关要求。

2.8.2 知识子域：Web 服务配置及安全管理

掌握基于 Apache 配置 Web 网站的方法及安全管理要求；

掌握基于 Tomcat 配置 Web 网站及安全管理要求；

了解 Nginx、weblogic 等其他 Linux 系统常用 Web 服务软件的配置和管理要求。

三、专项能力模块

3.1 知识域：安全运营基础

3.1.1 知识子域：项目获取

掌握技术解决方案的编制；

了解招投标相关流程；

掌握投标文件编制。

3.1.2 知识子域：项目管理流程

了解项目管理流程基础知识；

了解项目管理相关工作。

3.1.3 知识子域：安全运营相关标准

理解等级保护中关于安全运维的相关管理要求；

了解我国 IT 运维国家标准的相关要求（GB/T 36626-2018）。

3. 2 知识域：IT 服务管理

3.2.1 知识子域：IT 服务管理基础

了解 IT 服务管理的概念；

了解 IT 服务管理相关标准及 ITIL V3 的结构、基本概念；

3.2.2 知识子域：服务战略

了解服务战略的目标；

了解战略制定、需求管理、服务组合管理、财务管理等工作流程。

3.2.3 知识子域：服务设计

了解服务设计的主要目标和工作；

了解服务目录管理、服务级别管理、可用性管理、容量管理、可持续性管理、安全管理、供应商管理等工作流程。

3.2.4 知识子域：服务转换

理解服务转换中变更管理的作用及流程；

理解服务转换中发布管理的作用及流程；

理解服务转换中配置管理的作用及流程；

理解服务转换中知识管理的作用及流程。

3.2.5 知识子域：服务运营

理解服务台在 IT 服务管理中的作用；

理解事件管理的作用及流程；

理解问题管理的作用及流程；

理解服务请求管理的作用及流程。

3.3 知识域：等级保护

3.2.1 知识子域：等级保护基础

了解等级保护的发展历程；

了解等级保护相关概念；

了解等级保护标准体系。

3.2.2 知识子域：等级保护定级

了解等级保护定级工作流程；

理解等级保护定级工作方法；

掌握等级保护定级报告编写。

3.2.3 知识子域：等级保护技术要求

了解等级保护通用技术要求；

掌握等级保护技术测评的方法。

3.2.4 知识子域：等级保护管理要求

了解等级保护通用管理要求；

掌握等级保护管理测评的方法。

3.2.5 知识子域：等级保护扩展要求

了解等级保护扩展管理要求；

了解等级保护扩展要求测评的方法。

3.4 知识域：操作系统安全运维

3.4.1 知识子域：Windows 安全运维

了解 Windows 服务器系统备份、还原的方法；

掌握 Windows 服务器安全基线检查；

掌握 Windows 服务器运行状态监测体系建立；

掌握服务安全、网络访问安全等策略的设置方法。

3.4.2 知识子域： Linux 安全配置与管理

了解 Linux 服务器系统备份、还原的方法；

掌握 Linux 服务器安全基线检查；

掌握 Linux 服务器运行状态监测体系建立；

掌握 Linux 系统防火墙框架 iptables、firewalld 的使用。

3.4.3 知识子域：漏洞发现及日志分析

了解漏洞扫描软件的作用并掌握漏洞扫描软件的使用；

了解 Windows、Linux 日志系统并掌握如何对日志进行备份；

了解日志分析并掌握常用日志分析软件的使用。

3.5 知识域：应用安全运维

3.5.1 知识子域：Web 浏览安全

了解 Web 应用体系的结构及相关问题；

理解 Web 客户端（浏览器）常用的安全机制及安全风险；

理解浏览器端面临的网页挂马、网络钓鱼等攻击的技术原理并掌握浏览器安全设置方法。

3.5.3 知识子域：Web 服务配置及安全管理

掌握基于 Apache 配置 Web 网站的方法及安全管理要求；

掌握基于 Tomcat 配置 Web 网站及安全管理要求；

了解 Nginx、weblogic 等其他 Linux 系统常用 Web 服务软件的配置和管理要求。

3.5.4 知识子域：远程管理安全

了解远程终端等远程管理服务、产品的使用及安全管理要求；

了解堡垒机的技术原理及在安全运维中的作用。

3.5.5 知识域：数据库安全运维

理解针对数据库的攻击方法并掌握如何构建安全的数据库防御体系。

掌握数据库漏洞扫描软件的使用；

掌握 SQL server、Mysql、Oracle 数据备份及还原方法；

掌握 SQL server、Mysql、Oracle 安全运行监测体系。

3.6 知识域：网络攻击技术基础

3.6.1 知识子域：Web 漏洞及攻击

了解 SQL 注入等注入型漏洞原理；

了解跨站脚本等跨站漏洞技术原理；

了解文件上传、访问控制漏洞等技术原理。

3.6.2 知识子域：口令攻击

了解口令嗅探、远程破解、重放攻击等针对口令的攻击方法；

理解口令远程暴力破解的原理及技术实现并掌握远程口令破解攻击的工具使用；

理解口令字典、彩虹表的概念及在口令破解中的应用；

掌握口令字典生成工具的使用及口令字典的构造方法。

3.6.3 知识子域：恶意代码

了解恶意代码的概念及类型；

理解文件传播、网络传播、漏洞传播等恶意代码的传播方式的技术原理；

了解恶意代码的自我保护机制、隐藏等机制的技术原理。

3.6.4 知识子域：系统漏洞与溢出攻击

了解系统漏洞及补丁的概念；

了解缓冲区溢出攻击的相关概念及基本原理；

了解缓冲区溢出攻击的实现及威胁。