信息技术应用创新人才
考试评价大纲

信息安全工程师

工业和信息化部教育与考试中心

二〇二一年

说　明

为推动信息技术应用创新（以下简称“信创”）产业发展，培养高质量信创技术技能人才，工业和信息化部教育与考试中心组织有关专家编制了《信息技术应用创新人才评价考试大纲——信息安全工程师》（以下简称《考评大纲》），作为考评命题依据。

一、本《考评大纲》以信创产业人才需求、从业人员能力提要求为依据，坚持统一部署、系统推进的原则，对考评目标、考评要求、考评科目和考评范围作了规范、明确的说明。

二、本《考评大纲》的主要编制单位有四川省信创集约化保障中心、四川师范大学、成都信息工程大学、四川轻化工大学。主要编制人员有：黄洪、李同、石睿、江宇波、陈超、李俊强等。

三、本《考试大纲》的审定工作得到了国家工业信息安全发展研究中心、北京航空航天大学、北京电子科技学院、四川大学、电子科技大学、成都信息工程大学、四川轻化工大学、北京鸿腾智能科技有限公司、奇安信科技集团股份有限公司、龙芯中科技术有限公司、天津飞腾信息技术有限公司、麒麟软件有限公司、统信软件技术有限公司、武汉达梦数据库股份有限公司、北京优炫软件股份有限公司、成都中科大旗软件股份有限公司等单位的大力支持。主要审定人员有：胡彬、李博、蒋华、胡勇、佘堃、李飞、赵卓宁、吴亚东、石睿、王力、刘兴凤、严波、任云、郑瑶瑶、谷天宇、邱宗雄、夏思、张木梁、张成光、李春红、潘剑英、王泽江、李武鸿、姚明、赵宁、蒋琳、孙灏淼、康琬悦、鲍思丛等（排名不分先后）。在此对有关单位和专家一并表示感谢。

信息安全工程师
信息技术应用创新人才考试评价大纲
（试行版）

一、评价概况

1. 目标

通过本考试的合格人员能够根据业务需求，掌握网络信息安全的基础知识；熟悉网络信息安全的国家政策、法律法规、标准规范和产业发展动态；掌握信创的网络设备、安全设备、操作系统、数据库管理系统、中间件、应用软件等方面的知识体系；熟悉信创相关技术、产品的特点，能够根据信息安全相关法律法规及业务安全保障要求，配置、管理和维护常见的设备及系统；能够对信创体系下的信息系统进行网络安全风险评估和监测，给出整改建议；能够对网络信息安全事件开展应急响应相关工作。

2. 要求

（1）了解信息安全的国家政策、法律法规、标准规范等；

（2）熟悉网络信息安全的基本知识、常见的网络信息安全技术原理及应用；

（3）了解密码技术的发展简史与发展趋势，掌握国内主流密码体制和产品特点，以及密码应用的主要安全问题；

（4）了解常见的网络安全威胁的原理，以及典型场景下的网络安全威胁；

（5）熟悉网络安全保障的概念、模型；

（6）理解身份认证、访问控制、病毒防治、入侵检测、安全审计、态势感知和安全漏洞管理等保障支撑技术的原理；

（7）掌握信创产品的特点、应用场景；

（8）掌握网络信息安全风险评估工作机制，了解物理环境、网络通信、操作系统、数据库、中间件、应用系统、安全管理等领域的安全风险，能够提出信创体系下的信息安全解决方案；

（9）掌握安全咨询、安全运维、应急响应、安全取证等工作的关键流程和技术；

（10）掌握网络信息安全相关领域的专业术语，熟练阅读和正确理解网络信息安全相关领域的文献资料；

（11）了解云计算、物联网、工业控制等领域的安全技术。

3.科目设置

（1）科目 1：信息安全基础知识和技术，满分 100 分，考试时间不少于 60 分钟；

（2）科目 2：信息安全工程与综合应用，满分 100 分，考试时间不少于 90 分钟；

（3）科目 1 和科目 2 成绩均达 60 分（含）以上者，视为通过。

二、 评价范围

科目 1：信息安全基础知识和技术

1.信息安全概述

1.1 信息安全基础

1.1.1 信息安全相关概念

1.1.1.2 信息、信息安全的概念

1.1.1.3 通信安全、网络空间安全的概念

1.1.2 信息安全的发展过程

1.1.2.1 通信保密到信息保障的发展历程

1.1.2.2 信息安全的前沿技术

4.2.5.1 网络安全审计的概念

4.2.5.2 网络安全审计的要素

4.2.5.3 网络安全审计的主要技术

4.2.6 态势感知技术概述

4.2.6.1 态势感知的概念

4.2.6.2 态势感知的基本原理

4.2.7 安全漏洞管理技术概述

4.2.7.1 漏洞的基本概念

4.2.7.2 常见的网络安全漏洞平台

4.2.7.3 网络安全漏洞的分类与管理

4.2.7.4 网络安全漏洞扫描技术的应用

4.2.7.5 网络安全漏洞的处置方式

4.2.8 其他网络安全保障技术

4.2.8.1 信息隐藏技术

4.2.8.2 反垃圾邮件技术

5.网络通信安全

5.1 网络通信安全概述

5.2 网络协议安全概述

5.3 通信设备安全

5.3.1 信创主流通信设备种类、功能

5.3.2 信创主流通信设备的安全配置、管理

5.4 信创安全设备

5.4.1 信创主流安全设备的产品、功能

5.4.2 信创主流安全设备的配置、管理

6.区域边界安全

6.1 区域边界安全概述

6.2 区域边界安全防护设备

6.2.1 信创主流边界访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计等产品及其功能

6.2.2 信创主流边界访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计设备等配置及其管理

7.计算环境安全

7.1 计算机物理与环境安全

7.1.1 机房选址与建筑要求

7.1.2 机房设备布置要求

7.1.3 机房灾害防护、监控

7.2 设备安全

7.2.1 服务器安全

7.2.1.1 服务器的安全风险

7.2.1.2 服务器的安全解决方案

7.2.2 终端安全

7.2.2.1 终端的安全风险

7.2.2.2 终端的安全解决方案

7.2.3 智能设备安全

7.2.3.1 智能设备的安全风险

7.2.3.2 智能设备的安全解决方案

7.2.4 存储介质安全

7.2.4.1 存储介质的结构与分类

7.2.4.2 存储介质的风险与防护

7.3 操作系统安全

7.3.1 操作系统安全概述

7.3.1.1 操作系统的安全需求

7.3.1.2 操作系统的安全模型

7.3.1.3 操作系统的安全机制

7.3.2 信创主流操作系统安全分析与防护

7.3.2.1 信创主流操作系统安全性分析

7.3.2.2 信创主流操作系统的安全增强技术

7.3.3 其他操作系统安全分析与防护

7.3.3.1 其他操作系统概况

7.3.3.2 其他操作系统安全分析

7.3.3.3 其他操作系统安全增强技术

7.4 中间件安全

7.4.1 中间件概述

7.4.1.1 中间件的概念

7.4.1.2 中间件面临的安全威胁

7.4.1.3 中间件的安全解决方案

8.1 信息安全管理概述

8.2 信息安全管理体系

9. 信息安全服务

9.1 信息安全风险评估

9.1.1 信息安全风险评估概述

9.1.2 信息安全风险评估流程

9.1.3 风险的处置方法

9.2 网络安全等级测评

9.2.1 网络安全等级测评概述

9.2.2 网络安全等级测评流程

9.2.3 网络安全问题的整改方法

9.3 网络安全应急响应

9.3.1 网络安全应急响应概述

9.3.2 网络安全应急事件发现

9.3.3 网络安全应急事件处置

9.4 计算机取证

9.4.1 计算机取证的基本概念

9.4.2 计算机取证的主要技术

9.4.3 电子证据的法律有效性

科目 2：信息安全工程与综合应用

1. 信息安全需求分析

1.1 合规性要求

4.1 信息安全事件的分类分级方法

4.2 信息安全事件的处置方法

4.3 应急响应及演练的方案

5. 典型系统的安全工程

5.1 WEB应用安全

5.2 云平台安全

5.3 工控系统安全

5.4 物联网系统安全