国家信息安全水平考试
（一级）考试大纲

Ⅰ.考试性质与考试目标

一、 考试性质

国家信息安全水平考试项目（National Information Security Test Program，简称NISP）由教育部考试中心和中国信息安全测评中心共同设立并实施。其中，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，为国家信息安全保障工作的顺利实施奠定基础。

NISP（一级）考试从个人工作、学习和生活中面临的信息安全问题出发，结合我国网络基础设施和信息系统安全保障的实际情况，考察考生的信息安全的意识和基本技能。通过NISP（一级）知识内容的学习和相关考试，可以增强个人信息安全意识，帮助考生了解信息安全威胁和基本防护知识，掌握网络、操作系统和移动智能终端的基本安全设置方法，以及常见应用软件的安全操作方法，提高个人信息安全防护能力，同时了解信息安全管理相关知识，以具备在政府、企事业单位工作中安全使用信息系统的能力和基本信息安全素质。

NISP（一级）考试内容包含：信息安全概述、信息安全法律法规、信息安全基础技术、网络安全防护技术、操作系统安全防护技术、应用安全、移动智能终端安全防护和信息安全管理。

二、 考试目标

考生应理解信息安全相关概念，以及信息安全保障基本含义和作用。了解我国信息安全相关法律法规。提高考生的信息安全知识水平，及其对信息安全法律

法规的认识和理解。

考生应理解密码学、身份认证、访问控制和审计相关概念与作用。了解网络、操作系统、移动智能终端面临的安全威胁，掌握基本的网络、操作系统、移动智能终端的安全防护知识、技术和措施。掌握浏览器、网上金融交易、电子邮件的安全设置和操作方法，熟练使用相关工具保护数据安全。提升考生对信息安全威胁的分辨能力，及对常见安全防护技术的理解水平，培养良好的安全操作习惯，以增强其对个人信息的保护能力。

考生应了解信息安全管理的概念与作用，理解其基本方法，了解信息风险管理要素和过程，以及应急响应和灾难恢复过程。由此，提高考生对信息安全管理重要性的认识，培养其信息安全管理意识及保护组织机构信息安全的责任感。

通过对以上内容的学习，要求考生能够理解信息安全基础知识，掌握基本安全防护技术和信息安全管理知识，提高个人信息安全意识、知识和技能，具备基本信息安全素养。

Ⅱ.能力目标与实施要求

一、 能力目标

本考试要求考核识记、领会、应用、综合四种能力。

识记：要求考生知道有关名词、概念、原理、知识的含义，并能正确认识或识别。

领会：要求在识记的基础上，能把握相关基本概念、原理和方法，掌握有关概念、原理、方法的区别与联系。

应用：要求在领会的基础上，运用所掌握的基本概念、基本原理和基本方法中的少量知识点，分析和解决一般的理论问题或实际问题。

综合：要求考生在简单应用的基础上，运用学过的多个知识点，综合分析和解决比较复杂的实际问题。

下表为四个考核目标的权重：

考核目标			
识记	领会	应用	综合
45%	25%	20%	10%

二、 考核形式

考核形式			
等级	考试形式	考试总分	考试时间
一级	单项选择题	40	120 分钟
	多项选择题	10	
	材料填空题	20	
	案例题	30	

三、 学习安排

本考试每部分的建议学时如下：

知识体	组成部分	理论课时	实践课时
信息安全基础	第一部分 信息安全概述	2 课时	——
	第二部分 信息安全法律法规	1 课时	——
信息安全技术	第三部分 信息安全基础技术	2 课时	2 课时
	第四部分 网络安全防护技术	2 课时	3 课时
	第五部分 操作系统安全防护技术	3 课时	2 课时
	第六部分 应用安全	3 课时	6 课时
	第七部分 移动智能终端安全防护	1 课时	2 课时
信息安全管理	第八部分 信息安全管理	3 课时	——

Ⅲ.考试内容与考核要求

知识体	组成部分	考核标准	
		要求	内容
信息安全基础	第一部分 信息安全概述	识记	信息和信息技术的概念
			信息技术的发展阶段及各阶段的主要特点
			信息安全基本属性及含义
			信息安全的特征
			信息安全保障的概念和作用
			信息系统、风险和使命的关系
			信息系统安全保障概念和关系
			信息安全保障模型
		领会	信息安全问题产生的根源
			信息系统安全保障模型中保障要素、生命周期和安全特征的内容和含义
	第二部分 信息安全法律法规	识记	国家秘密的概念和分级
			危害国家秘密的犯罪行为
			《中华人民共和国保守国家秘密法》、《中华人民共和国刑法》中保护国家秘密的条款和规定
			商业秘密和个人信息的概念
			《中华人民共和国反不正当竞争法》、《中华人民共和国合同法》、《劳动合同法》中保护商业秘密的主要条款
			《中华人民共和国宪法》、《中华人民共和国居民身份证法》、《中华人民共和国侵权责任法》中保护个人信息的主要条款
			网络违法犯罪的概念
			《关于维护互联网安全的决定》、《中华人民共和国治安管理处罚法》中打击网络违法犯罪的主要条款

			《中华人民共和国电子签名法》、《中华人民共和国保守国家秘密法》中关于信息安全管理的主要条款
信息安全技术	第三部分 信息安全基础技术	识记	明文、密文、密钥、加密和解密等密码学基本概念和术语
			对称密码体制的基本概念和典型算法
			非对称密码体制的概念和典型算法
			哈希函数的基本概念和术语
			混合加密模式的工作原理
			数字签名的概念
			身份认证的基本方法
			数字证书的作用与内容
			认证中心（CA）的功能
			公钥基础设施（PKI）的概念和组成
			访问控制基本概念及三要素
			安全审计的作用与功能
		领会	加密解密模型
			对称密码体制的优缺点
			非对称密码体制的优缺点
			哈希函数的特点
			数字签名的工作原理
			哈希函数、数字签名的应用
			访问控制常用方法
		应用	典型密码体制与数字签名的应用举例
			系统日志安全审计的操作
		综合	哈希函数的应用
		识记	TCP/IP 协议、超文本标记语、超文本传输协议、端口、域名系统、统一资源定位符等网络基础概念

	第四部分 网络安全防护技术		IPSec 的概念和功能
			SSL 的概念和功能
			VPN 的概念和特点
			防火墙的概念和主要功能
			无线局域网的概念和特点
			无线局域网的安全威胁
		领会	IPSec 的工作模式
			常见网络攻击目的和手段，包括社会工程学攻击、网络嗅探、网络钓鱼、拒绝服务攻击和远程控制攻击
			VPN 的主要应用，包括远程访问、内联网、外联网的工作方式
			无线接入点安全管理方法，包括修改管理员密码、采用加密传输、禁用 DHCP 服务等。
		综合	无线路由器的安全设置
	第五部分 操作系统安全防护技术	识记	漏洞的概念与安全威胁
			漏洞扫描的实现手段
			恶意代码和计算机病毒的概念
			恶意代码的安全威胁
			木马的特点、传播方式与危害
			端口扫描的安全威胁和隐蔽手段
			操作系统的概念与功能
			补丁程序的作用
		领会	漏洞产生的原因
			终端防护软件的功能和作用
			关闭不必要服务和端口，开启审核策略和密码策略等的安全防护策略方法
		综合	Windows 操作系统安全使用安全
			个人防火墙配置

	第六部分 应用安全	识记	网上金融交易中常见的安全防护措施
			邮件地址欺骗、垃圾邮件、邮件病毒等电子邮件安全威胁
			数据备份的概念
			账户口令的常见安全威胁
			账户口令设置的基本原则
			终端访问服务器的方式和特点
		领会	电子邮件工作流程
			垃圾邮件过滤、邮件加密和签名等电子邮件安全防护手段
			数据备份的重要性和常见手段
			数据加密和签名的重要性
		应用	数据恢复操作方法和要点
			数据加密和签名的常见手段
		综合	浏览器安全设置和安全使用方法
			电子邮件客户端安全设置和安全使用方法
	第七部分 移动智能终端安全防护	识记	移动智能终端的概念和分类
			常见的智能终端手机操作系统
			伪基站的概念和伪基站攻击威胁
			二维码的概念和二维码扫描威胁
			移动智能终端遗失的安全防范措施
			移动智能终端的加密软件
			手机病毒的概念和危害
			恶意扣费软件的安全威胁
		领会	伪基站的工作原理
			手机病毒的防范措施
			二维码扫描的安全防范措施
		应用	手机终端防护软件的设置

信息安全管理	第八部分 信息安全管理	识记	信息安全管理的概念和内容
			信息安全风险的概念
			风险管理的概念和作用
			风险评估的概念与作用
			信息安全事件的概念与分级
			信息安全事件分级考虑的要素
			信息安全应急响应的概念和作用
			灾难恢复的概念与作用
			灾难备份的概念与作用
			本地备份与异地备份的概念
			数据级灾备和系统级灾备的概念
			完全备份和不完全备份的概念
		领会	成功实施信息安全管理的关键因素
			信息安全应急响应管理过程
			灾难备份方法

IV.题型示例及参考答案

一、单项选择题（每小题 1 分，共计 40 分）

下列各题 A)、B)、C)、D）四个选项中，只有一个选项是正确的。请按要求作答。

1.信息安全的发展经历四个历史发展阶段，信息安全的内涵和外延在不断地加深和扩大。以下关于信息安全发展阶段顺序，正确的选项是：

A）通信安全阶段、信息系统安全阶段、计算机安全阶段、信息安全保障阶段

B）计算机安全阶段、信息系统安全阶段、通信安全阶段、信息安全保障阶段

C）通信安全阶段、计算机安全阶段、信息系统安全阶段、信息安全保障阶段

D）计算机安全阶段、通信安全阶段、信息系统安全阶段、信息安全保障阶段

正确答案：C

2.网络嗅探是通过截获、分析网络中传输的数据而获取有用信息的行为，这种攻击形式破坏了以下哪一项内容：

A）网络信息的抗抵赖性

B）网络信息的保密性

C）网络服务的可用性

D）网络信息的完整性

正确答案：B

二、多项选择题（每小题 2 分，共计 10 分）

在备选答案中有两到四个答案是正确的。多选、错选、漏选均不得分。请按要求作答。

1．防火墙的基本功能包括：

A）过滤进/出网络的数据

B）管理进/出网络的访问行为

C）封堵某些禁止的业务

D）对某些网络攻击进行检测和告警

正确答案：ABCD

2．在信息安全领域，风险是指信息资产遭到损坏并给企业带来负面影响的

潜在可能性。风险的大小，与以下哪些要素有关：

A）资产

B）威胁

C）完整性

D）脆弱性

正确答案：ABD

三、材料填空题（每小题 2 分，共计 20 分）

1. 对信息安全事件进行分级管理，是有效防范和响应信息安全事件的基础之一。通常，对信息安全事件的分级主要考虑三个要素：_____、系统损失和社会影响。

正确答案：信息系统的重要程度（答系统的重要程度、系统的重要性均可）

2.木马程序一般由两部分组成，分别是服务器端和_____。

正确答案：客户端（答用户端、使用端均可）

四、案例题（案例一 15 分，案例二 15 分，共计 30 分）

小王是 A 单位信息网络中心的网管，A 单位所有新购置的计算机设备需网络中心的网管配置网络和个人防火墙以后才能使用。小王在给计算机配置网络和个人防火墙的操作过程中，遇到如下问题，请选择正确答案进行解答。

（1）打开命令行界面后，查看本机 IP 地址的命令是_____。

A. ipconfig

B. netstat

C. tracert

D. route

正确答案：A

（2）本机已经加入到局域网中，需要配置个人防火墙，以下关于防火墙配置，说法正确的是：

A. 不需要添加规则

B. 规则不需要进行通过或不通过的设定

C. 根据需要添加规则

D. 添加的规则不用设置生效或部署

正确答案：C