CCAI–R–P42:2023

网络信息安全工程师 人员能力验证规则

Network Information Security Engineer: Rules for Personal Proficiency Testing

国家市场监督管理总局认证认可技术研究中心

2023年12月19日发布 2023年12月19日实施

目 录

前 言

网络信息安全工程师人员能力验证(Network Information Security Engineer Personal Proficiency Testing)是指遵照信息安全管理体系和标准工作，防范黑客入侵并进行分析和防范，通过运用各种安全产品和技术，设置防火墙、防病毒、IDS、PKI、攻防技术等，进行安全制度建设与安全技术规划、日常维护管理、信息安全检查与审计系统账号管理与系统日志检查等工作的人员进行能力验证。

为提高网络信息安全领域从业人员的理论知识与实际工作水平，国家市场监督管理总局认证认可技术研究中心(以下简称“认研中心”、英文简称“CCAI”)决定开展网络信息安全工程师人员能力验证工作。为规范认研中心人员能力验证工作，依据《国家市场监督管理总局认证认可技术研究中心合格评定技术体系文件管理办法（试行）》《国家市场监督管理总局认证认可技术研究中心人员能力验证管理办法》等文件，组织制定《网络信息安全工程师 人员能力验证规则》。

1.本规则是认研中心开展网络信息安全工程师人员能力验证的基本依据，内容包括概况、基本要求、验证要求、验证规则、考核内容比重。

2.本规则以现阶段网络信息安全领域从业人员所需理论知识与实践水平为目标，在充分考虑经济发展、规范企业行为和提高企业竞争力的基础上，对网络信息安全领域从业人员的工作范围、岗位职责和知识水平做了明确规定。

3.本规则参考了《合格评定 能力验证的通用要求》(ISO/IEC 17043)、《利用实验室间比对进行能力验证的统计方法》(ISO 13528)中的全部或部分条款，既保证了规则体系的规范化，又对行业从业人员的水平及行业从业人员现状进行动态分析，促进行业良性发展，同时也使其具有根据行业发展进行调整的灵活性和实用性，符合人员能力验证的需求。

4.网络信息安全工程师人员能力验证考核不属于职业资格类考

试,通过考试仅表明学员掌握了一定的网络信息安全专业理论知识和实际工作水平的能力。

网络信息安全工程师 人员能力验证规则

1 范围

本规则是认研中心网络信息安全工程师人员能力验证组织者和参加者双方都应当遵循的程序规则。

从事网络安全运维等相关职业的专业技术人员；已经从事IT行业的人员，希望转向网络安全领域或者提升自己在网络安全方面的专业能力的人员；企事业单位的IT人员或管理人员，需要了解网络安全的基本知识和技术，以保护公司的信息系统和数据安全；政府机构和军队的IT人员，需要具备网络安全技术，以保护国家的信息系统和网络安全；对网络安全领域感兴趣的计算机科学、网络工程、信息安全等专业的学生；希望通过系统学习和实践提升网络安全技术能力以及有志于从事网络信息安全领域工作的人员，均可申请参加认研中心网络信息安全工程师人员能力验证。

2 引用文件

本规则参考并修改引用了下列文件中的全部或部分条款。所引用的文件不注明其发布日期，请各相关方注意使用这些文件的有效版本（包括其修订案）。

2.1 《合格评定能力验证的通用要求》(ISO/IEC 17043)

2.2 《利用实验室间比对进行能力验证的统计方法》（ISO 13528）

3 术语和定义

人员能力验证：是指按照相关规定或标准，根据考核验证规则，采取专业知识学习、能力素质考核、结果分析比对及验证等方式，对人员的专业能力进行验证的合格评定过程。

原始分：参加考核人员答题得到的分数，最高为100分。

平均分：所有考核人员原始分的算术平均值，最高分为100分。

中等分：反映考核项目中等水平的分数，最高为100分。

标准差：反映原始分的分散性。

标准分：利用稳健统计方法，转化得到每位参加考核人员的分数，分值在-100至100之间。

百分比排名：比此原始分小的数据个数除以与此原始分进行比较的数据个数总数。

4 人员能力验证组织要求

4.1 学习时长

参加人员能力验证应满足相应的专业学习时长要求，不得少于36学时，并提供相关证明。

4.2 考核时间

网络信息安全工程师人员能力验证测验实行统一大纲、统一命题、统一组织的考试制度，原则上每年举行4次考试，分别安排在3月份、6月份、9月份、12月份的第四个周末，考试时间为120分钟。

4.3 考核方式

网络信息安全工程师人员能力验证采取线上考试，考生

信息采用计算机考试系统进行统一管理，在线完成学员信息填报、考试、电子试卷管理等工作。

考试系统应具有人脸识别等防作弊功能。

采取线上考试的形式，考生需在拥有摄像头的电脑前参加考试，监考人员与考生配比为1:500，监考中心至少不少于2名监考人员。

4.4 考核结果

网络信息安全工程师人员能力验证结果划分为优秀、良好、合格、不合格。(注：人员能力验证结果详见第6部分人员能力验证结果评价规则)。

对于考生来说，纸质证书中赋予的原始分、标准分Z和百分比排名PR为当期(或者某一时间段)考核结果。同时要提醒考生，标准分Z和百分比排名PR会根据该项目全部参加考试人员的成绩“排大队”，考生可以随时登录账号，线上关注自己的标准分Z和百分比排名PR的变化。

4.5 考核内容

网络信息安全工程师能力考核的主要内容包括《网络信息安全需求》《密码学基础》《访问控制》《互联网络安全》《操作系统安全》《数据库系统安全》《网络信息系统安全漏洞》《网络信息系统恶意代码》《网络信息安全的攻击与防护》《信息安全管理体系》《网络信息安全风险管理》十一部分内容，内容清单见附件。考核验证时，《网络信息安全需求》《密码学基础》《访问控制》《互联网络安全》《操

作系统安全》《数据库系统安全》《网络信息系统安全漏洞》《网络信息系统恶意代码》《网络信息安全的攻击与防护》《信息安全管理体系》《网络信息安全风险管理》十一部分内容占比分别为 30%、10%、5%、10%、10%、5%、5%、5%、10%、5%、5%。

5 考核申请条件

凡遵纪守法、参加专业学习时长满足要求，并符合下列条件中之一，可申请参加网络信息安全工程师能力考核:

5.1 取得计算机、网络安全类大学专科学历，并从事相关专业工作满 2 年;

5.2 取得计算机、网络安全类大学本科学历，并从事相关专业工作满 1 年;

5.3 取得计算机、网络安全类双学士学位、硕士学位或以上学位的人员;

5.4 具备其他专业大专及以上学历并从事计算机、网络安全等相关专业工作满 5 年;

5.5 有志于从事网络信息安全行业的人员。

6 验证结果评价

6.1 统计量计算

6.1.1 平均分 A

所有考核人员原始分的算术平均值，计算公式如下:

$$A = \sum^{p} x_i / p$$

x_i 为第 i 名人员的原始分，p 为参加考试人员总数。

6.1.2 中等分 M

所有参加考核人员原始分的中位值。假设 p 名参加考核人员原始分按递增顺序表示为：x_1，x_2，…，x_p。当 p 为奇数时，中位值为第(p+1) /2 位的原始分值；当 p 为偶数时，中位值为第 p/2 位和第（1+p/2）位原始分值的平均值。计算公式如下:

$$M = \begin{cases} X_{[(p+1)/2]}, & p\text{为奇数} \\ [X_{(p/2)} + X_{(1+p/2)}] / 2, & p\text{为偶数} \end{cases}$$

6.1.3 差值 D

参加考核人员原始分与中等分的差值。计算公式如下:

$$D_i = X_i - M$$

6.1.4 标准差 S

按照稳健统计方法，以标准化四分位距作为标准差。将参加考核人员的原始分按递增顺序排列，计算高四分位和低四分位原始分的差值，然后乘以系数 0.7413（因子 0.7413 是从“标准”正态分布中导出）即可得到标准化四分位距。计算公式如下:

$$S=0.7413\times(Q_3-Q_1)$$

式中，Q_1为低四分位数，该组原始分的四分之一低于 Q_1，四分之三高于 Q_1；Q_3为高四分位数，该组原始分的四分之一高于 Q_3。

6.1.5 标准分 Z

每位参加考核人员差值 D 与标准差之比。计算公式如下:

$$Z=D/S\times 50$$

标准分 Z 反映参加考核人员与中等水平间的差距。Z＞0 时，反映人员能力高于中等水平；Z＜0 时，反映人员能力低于中等水平。根据统计学原理,基于正态分布假设,D/S 在[-2,+2]的概率约为 95%。为了更加通俗易懂和直观显示，乘以系数 50 得到标准分 Z，而且，当计算 Z 值小于-100 或者大于 100 时，直接分别赋值为 Z=-100、Z=100。因此，标准分 Z 在-100 至 100 之间，Z 值越接近 100，说明参加考核人员的水平越高。

6.1.6 百分比排名 PR

某参加考核人员百分比排名为 90%，表明该人员成绩比 90%的人成绩高。

6.1.7 合格率

考核等级为合格以上的人数占参加考核总人数的比例。

6.2 人员能力评价

6.2.1 反馈给参加考核人员的指标

参加考核人员成绩单列出原始分、标准分 Z 和百分比排名 PR 三个指标值，并注明含义。其中，成绩是否合格以参加考核人员的原始分为评价基准。对于成绩合格的人员，再按标准分 Z 的大小，分级列出成绩。具体如下:

当原始分＜60 时，表明考生参加本次考核等级为“不合格”，建议考生进一步学习后，再次报名参加考核。

当 60≤原始分＜100，且标准分满足-100≤Z＜50 时，

表明考生参加本次考核等级为“合格”。

当 60≤原始分＜100，且标准分满足 50≤Z＜100 时，表明考生参加本次考核等级为“良好”。

当原始分≥60，且标准分 Z=100 时，或当原始分=100 时，表明考生参加本次考核等级为“优秀”。

当标准差 S=0，则采取原始分判断规则：原始分<60 为“不合格”；60≤原始分＜80 为“合格”；80≤原始分＜90 为“良好”；原始分≥90 为“优秀”。

对于考生来说，纸质证书中赋予的原始分、标准分 Z 和百分比排名 PR 为当期（或者某一时间段）考核结果。标准分 Z 和百分比排名 PR 会根据该项目全部参加考试人员的成绩“排大队”，考生可以随时登录账号线上关注自己标准分 Z 和百分比排名 PR 的变化。

对每一名考核“不合格”的考生，在发送成绩单的同时，应有针对性地提出改进建议和再次参加考核的方法。

6.2.2 认研中心监测指标

及时发布并动态更新每个能力验证项目参加考核的总人数、平均分、中等分、标准差、合格率、最低分、最高分等指标。此外，可以使用顺序标准分 Z 直方图直观显示参加者能力。

附录（资料性附录）

网络信息安全工程师考核内容清单

分类	考核内容	
一、网络信息安全需求	国家安全的需要	数据主权
		国家信息安全
		重大决策支持
		重大事件应对
	个人隐私和商业机密	个人隐私
		商业机密
	网络安全法	我国第一部网络安全相关的基础法律
		明确了相关责任和义务
		违法处罚更严格和多样
	国家密码法	密码的表现形式是技术、产品和服务
		不得窃取密码保护的信息
		密码实行进出口管理制度
	数据安全法	长臂管辖
		国家建立数据分类分级保护制度
	个人信息保护法	强调属地原则
		禁止侵害个人信息
	欧洲 GDPR	重视个人同意
		泄露通报
	企业合规	等保、分保、关保
		密评
二、密码学基础	古典密码学	替代密码、置换密码
		转轮机
		一次一密乱码本
		现代密码学
		公钥密码学
	密码学的应用	机密性
		完整性
		可鉴别性
三、访问控	防止未授权访问	访问控制模型

制		访问控制技术
四、互联网络安全	网络协议安全	TCP/IP 协议安全
		无线局域网协议安全
		移动通信网络安全
	网络设备安全	防火墙
		入侵检测
		其他网络设备安全
五、操作系统安全	操作系统安全概述	操作系统基本概念
		操作系统组成
		操作系统功能
		操作系统安全目标和机制
	windows 系统安全	用户组和安全
		文件系统安全
		进程及服务
		服务管理
		日志系统
	linux 系统安全	linux 安全基础
		多用户系统的用户和用户组
		保护 root 账号
		ext4 文件系统
		常见目录的用途
		文件、目录权限及命令
		linux 进程管理
		linux 日志管理
		linux 防火墙、SELinux
六、数据库系统安全	关系型数据库	数据库基本概念和主要功能
		结构化查询语言 SQL 主要功能
		数据库安全特性和安全功能
		数据库”视图“的安全功能
		数据库完整性要求和备份恢复概念
七、网络信息系统安全漏洞	安全漏洞基础知识	安全漏洞的含义
		安全漏洞产生的原因
		常见安全漏洞分类
		安全漏洞发展趋势

		安全漏洞的静态和动态挖掘方法
		安全补丁分类、修复时应注意的问题
八、网络信息系统恶意代码	恶意代码基础知识	恶意代码的发展史
		恶意代码的类型
		恶意代码的传播方式
		恶意代码的加载方式
		恶意代码的隐藏
		恶意代码的自我保护
		恶意代码检测技术
九、网络信息安全的攻击与防护	信息收集与分析	信息收集与分析的作用
		漏洞定位、定点挖掘、信息收集
		分析目标----入侵准备
		端口扫描工具
		漏洞扫描工具
	安全攻击与防护	口令攻击、字典攻击、暴力攻击
		社会工程学攻击
		IP 欺骗、DNS 欺骗原理与防范
		DDoS 原理与防范
		跨站脚本攻击的原理与防范
十、信息安全管理体系	基本概念	信息安全管理概述
		信息安全管理体系
		信息安全管理体系建立
		信息安全管理控制规范
十一、网络信息安全风险管理	基础概念	风险管理的定义
		什么是信息安全风险管理
		信息安全风险管理的目标
		安全风险术语
		风险评估
		风险处理
		监督审查