ICS 35.040
L 80

ISEAA

团　　体　　标　　准

T/ISEAA 001—2020

网络安全等级保护测评高风险判定指引

High risk assessment guidelines for classified protection evaluation of cyber security

2020-11-05 发布　　2020-12-01 实施

中关村信息安全测评联盟　　发 布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》给出的规则起草。

本文件由中关村信息安全测评联盟提出并归口。

本文件起草单位：上海市信息安全测评认证中心、国家网络与信息系统安全产品质量监督检验中心、江苏金盾检测技术有限公司、江苏骏安信息测评认证有限公司、山东新潮信息技术有限公司、合肥天帷信息安全技术有限公司、深圳市网安计算机安全检测技术有限公司、杭州安信检测技术有限公司、成都安美勤信息技术股份有限公司、甘肃安信信息安全技术有限公司、教育信息安全等级保护测评中心、辽宁浪潮创新信息技术有限公司、银行卡检测中心、安徽祥盾信息科技有限公司。

本文件主要起草人：金铭彦、罗峥、张笑笑、刘静、徐御、陈清明、陆臻、陈妍、吴晓艳、何欣峰、许晓晨、张杰、武建双、牛建红、倪祥焕、何志鹏、严维兵、王永琦、范仲伟、武斌、杨凌珺、盛璐禕。

引　言

等级保护测评是推动和贯彻网络安全等级保护工作的重要环节之一。为了更好地提升全国等级保护测评机构的能力，规范测评机构对网络安全风险严重程度的判定规则，中关村信息安全测评联盟组织编写本等级保护测评行业指引性文件，旨在促进安全风险判定更加标准化、规范化，从而更好地规范等级保护测评活动，提升等级保护测评工作质量。

本文件依据 GB/T 22239—2019《信息安全技术　网络安全等级保护基本要求》中第二级及以上安全通用要求及云计算安全扩展要求中的基本原则，对测评过程中发现的安全性问题如何进行高风险判定给出指引。

本文件仅考虑一般系统场景，无法涵盖所有行业及特殊场景，实际测评活动中应根据安全问题所处的环境、面临的威胁、已采取的措施，并结合本文件内容做出客观、科学、合理的判定。

网络安全等级保护测评高风险判定指引

1 范围

本文件适用于网络安全等级保护测评、安全检查等活动。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 2887—2011 计算机场地通用规范

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 25069—2010 信息安全技术 术语

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

3 术语和定义

GB 17859—1999、GB/T 25069—2010、GB/T 31168—2014 和 GB/T 22239—2019 界定的以及下列术语和定义适用于本文件。

3.1

高可用性系统

可用性大于或等于 99.9%，年度停机时间小于或等于 8.8 h 的系统，例如，银行、证券、非银行支付机构、互联网金融等交易类系统，提供公共服务的民生类系统，工业控制类系统，云计算平台等。

3.2

关键网络设备

部署在关键网络节点的重要网络设备，包括但不限于核心交换机、核心路由器等，一旦该设备遭受攻击或出现故障将影响整个系统网络。

3.3

不可控网络环境

互联网、公共网络环境、开放性办公网络等缺少网络安全管控措施，可能存在恶意攻击、数据窃听等安全隐患的网络环境。

3.4

可被利用的高危漏洞

可被攻击者用于进行网络攻击从而导致严重后果的漏洞，包括但不限于缓冲区溢出、权限提升、远程代码执行、严重逻辑缺陷、任意文件上传等。