ICS 35.040
L 80

GA

中华人民共和国公共安全行业标准

GA/T 1349—2017

信息安全技术
网络安全等级保护专用知识库接口规范

Information security technology—
Knowledge library interface specification for cybersecurity classified protection

2017-11-20 发布　　2017-11-20 实施

中华人民共和国公安部　　发 布

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局、公安部第三研究所提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部第三研究所、北京随方信息科技有限公司、中关村信息安全测评联盟。

本标准主要起草人：陶源、郭倬明、罗峥、李末岩、张宇翔、袁静、吴伟湘、王伟、沈昱、刘静、马思远、于春兰、郑国刚、宋文超、桑宇晨、王传宁、刘廷政、杨晓妹。

信息安全技术
网络安全等级保护专用知识库接口规范

1 范围

本标准规定了网络安全等级保护专用知识库的接口，使知识库中封装的网络安全等级保护相关标准、作业指导书、分析模型和规则库可以由测评工具调用，使测评工具采集和分析数据可以按照知识库内置的知识、模型和规则进行自动化分析。

本标准适用于为进行网络安全等级保护工作的自动化分析工具提供规范接口，有利于提高网络安全等级保护工作的规范化。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 25069—2010 信息安全技术 术语

GB/T 28448—2012 信息安全技术 信息系统安全等级保护测评要求

GA/T 1389—2017 信息安全技术 网络安全等级保护定级指南

3 术语和定义

GB 17859—1999、GB/T 22239—2008、GB/T 25069—2010、GB/T 28448—2012 和 GA/T 1389—2017 界定的以及下列术语和定义适用于本文件。

3.1

安全状况量化分析 quantitative analysis of security situation

依据等级保护的标准和分析模型，对提供的数据进行分析，给出分析对象(包括信息系统组件、信息系统等)安全防护状况合规的量化信息。

3.2

安全状况仿真规则 simulation rule of security situation

为了获取被测信息系统或被测信息系统组件的安全状况，而构建仿真环境的规则，包括某些网络设备、性能和配置等信息。

3.3

信息系统组件 component of information system

信息系统的组成部件，包括网络设备、安全设备、主机系统、网站应用服务、数据库系统等。