ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31495.1—2015

信息安全技术　信息安全保障指标体系及评价方法　第1部分:概念和模型

Information security technology—Indicator system of information security assurance and evaluation methods—Part 1:Concepts and model

2015-05-15 发布　　2016-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 31495《信息安全技术　信息安全保障指标体系及评价方法》分为如下3部分：

——第1部分：概念和模型；

——第2部分：指标体系；

——第3部分：实施指南。

本部分为GB/T 31495的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：国家信息中心、国家新闻出版广电总局监管中心、中国信息安全测评中心、中国电信集团、中国移动通信集团、大连理工大学、国家能源局信息中心、江苏省信息中心、中国民航大学、中国电力科学研究院。

本部分主要起草人：何德全、吕欣、王宪磊、王长胜、郭艳卿、杨月圆、李守鹏、吕汉阳、杜巍、肖英、张茉楠、罗程、吴志军、杨一曼、谢东晖、程露、胡红升、孙小红、徐浩、周智、陈敏时、雷缙、樊晖、高昆仑、李鹏、李慧。

引　言

GB/T 31495 依据国家对信息安全保障工作的相关要求，提出了信息安全保障评价的概念和模型、指标体系及实施指南。

31495 由 3 部分组成。第 1 部分描述了本标准各部分通用的基础性概念，给出了信息安全保障及信息安全保障评价的概念和模型，给出了指标的测量模型；第 2 部分在第 1 部分的模型指导下给出了信息安全保障指标体系和指标测量过程；第 3 部分给出了信息安全保障评价工作实施所应遵照的要求、流程和方法。

31495 主要用于：为政府管理部门的信息安全态势判断和宏观决策提供支持；为基础信息网络和重要信息系统的管理部门及运营单位的信息安全管理工作提供支持。

信息安全技术　信息安全保障指标体系及评价方法　第1部分:概念和模型

1　范围

GB/T 31495的本部分界定了信息安全保障评价的基本概念,确立了信息安全保障评价的一般模型。

本部分适用于信息安全保障评价工作。

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/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 25069—2010中界定的以及下列术语和定义适用于本文件。

3.1

信息安全保障　information security assurance

对信息和信息系统的安全属性及功能、效率进行保障的一系列适当行为或过程。

3.2

信息安全保障评价　evaluation of information security assurance

收集信息安全保障证据,并获得信息安全保障值的过程和途径。

3.3

信息安全保障措施　measures for information security assurance

为达到信息安全目的所采用的保障手段的集合。

3.4

信息安全保障能力　capability of information security assurance

被保障实体安全防御、响应和恢复等特性的体现。

3.5

信息安全保障效果　effects of information security assurance

被保障实体的信息安全保障目标和属性的实现程度。

4　信息安全保障模型

信息安全保障模型是采用过程方法建立的。

图1说明了信息安全保障是根据利益相关方的保障需求建立保障措施,形成保障能力,以实现保障效果的过程。根据利益相关方对保障效果的反馈,可以动态调整保障措施,以更好地满足保障需求。