ICS 35.040
L 80

中华人民共和国国家标准

GB/T 34990—2017

信息安全技术　信息系统安全管理平台技术要求和测试评价方法

Information security technology—Technical requirements and testing evaluation approaches of information system security management platform products

2017-11-01 发布　　2018-05-01 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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 2
4　安全管理平台概述 …… 3
4.1　安全管理平台基本原理 …… 3
4.2　安全管理平台管理对象 …… 4
4.3　安全管理平台使用环境 …… 5
4.4　安全管理平台安全等级 …… 5
5　功能要求 …… 6
5.1　功能构成 …… 6
5.2　基础功能 …… 7
5.2.1　安全策略及安全责任管理功能要求 …… 7
5.2.2　系统部件管理功能要求 …… 9
5.2.3　安全机制管理功能要求 …… 12
5.2.4　审计机制管理功能要求 …… 14
5.2.5　平台功能数据管理功能要求 …… 17
5.2.6　平台系统接口功能要求 …… 19
5.2.7　平台级联功能要求 …… 21
5.3　扩展功能 …… 23
5.3.1　物理安全管理 …… 23
5.3.2　安全风险管理 …… 24
5.3.3　其他扩展功能 …… 25
6　安全要求及保障要求 …… 25
6.1　安全要求 …… 25
6.1.1　身份鉴别 …… 25
6.1.2　抗抵赖 …… 27
6.1.3　访问控制 …… 27
6.1.4　安全审计 …… 28
6.1.5　完整性保护 …… 29
6.1.6　保密性保护 …… 30
6.1.7　入侵及恶意代码防范 …… 31
6.1.8　软件容错及资源控制 …… 32
6.1.9　可信路径 …… 32
6.1.10　密码支持 …… 32
6.2　保障要求 …… 33

6.2.1 配置与设备选型 …… 33
6.2.2 交付与运行 …… 34
6.2.3 开发 …… 34
6.2.4 指导性文档 …… 36
6.2.5 测试 …… 37
6.2.6 脆弱性评定 …… 37
6.2.7 生命周期支持 …… 38
7 测试评价方法 …… 39
7.1 测试评价范围 …… 39
7.2 平台功能测试 …… 40
7.2.1 安全策略及安全责任管理功能测试 …… 40
7.2.2 系统部件管理功能测试 …… 42
7.2.3 安全机制管理功能测试 …… 44
7.2.4 审计机制管理功能测试 …… 47
7.2.5 数据管理功能测试 …… 50
7.2.6 接口管理功能测试 …… 52
7.2.7 级联功能测试 …… 53
附录 A（资料性附录） 安全管理平台技术要求安全等级划分 …… 56
附录 B（资料性附录） 平台对各类管理对象的控制过程说明 …… 59
附录 C（资料性附录） 安全管理平台在云计算中的应用 …… 63
附录 D（资料性附录） 信息系统安全机制参考 …… 65
参考文献 …… 69

前　言

本标准按照 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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:公安部第一研究所、北京中科网威信息技术有限公司、北京江南天安科技有限公司、公安部计算机信息系统安全产品质量监督检验中心、浙江远望电子有限公司、中国电信股份有限公司北京研究院、北京凝思科技有限公司、北京启明星辰信息技术股份有限公司、北京赛博兴安科技有限公司、北京华热科技发展有限公司、北京初志科技有限公司、北京聆云信息技术有限公司。

本标准主要起草人:胡志昂、陈冠直、景乾元、殷国强、张翔、苏智睿、张笑笑、傅如毅、刘兵、明旭、胡托任、王磊、李大鹏、李清玉。

引　言

本标准中，安全管理平台是能够满足国家信息安全管理需要，体现组织管理层意志，以信息安全策略和管理责任为主线，以信息系统的系统部件管理、安全机制管理、审计机制管理为主要手段，以信息安全管理对象识别、安全策略设置、安全机制监控、安全事件处置为主要工作过程，实现信息安全管理和信息安全技术有机结合的安全管理中心的关键技术支撑性产品。安全管理平台适用于不同安全保护等级的信息系统，更有益于关键信息基础设施的安全集中管理。

本标准依据国家信息安全等级保护要求，提出了统一管理安全机制的平台，规定了安全管理平台的技术要求和测试评价方法。本标准的第4章安全管理平台概述，明确了基本原理、管理对象、使用环境和安全等级。第5章安全管理平台的功能要求，阐述了功能构成、基础功能、扩展功能；其中基础功能，包括安全策略及安全责任管理功能要求、系统部件管理功能要求、安全机制管理功能要求、审计机制管理功能要求、平台功能数据管理功能要求、平台系统接口功能要求、平台级联功能要求；扩展功能，包括物理安全管理、安全风险管理和其他扩展功能要求。第6章安全管理平台的安全要求及保障要求，阐述了平台自身的安全要求、保障要求。第7章安全管理平台的测试评价方法，阐述了测试评价范围、平台功能测试。本标准的附录均为资料性附录，其中，附录A阐述了安全管理平台技术要求安全等级划分，附录B阐述了平台对各类管理对象的控制过程说明，附录C阐述了安全管理平台在云计算中的应用，附录D阐述了信息系统安全机制参考。

信息安全技术　信息系统安全管理平台
技术要求和测试评价方法

1　范围

本标准规定了安全管理平台的基于信息安全策略和管理责任的系统管理、安全管理、审计管理等功能，以及对象识别、策略设置、安全监控、事件处置等过程的平台功能要求，平台自身的安全要求、保障要求，以及测试评价方法。

本标准适用于安全管理平台的规划、设计、开发和检测评估，以及在信息系统安全管理中心中的应用。

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 18018　信息安全技术　路由器安全技术要求

GB/T 20269—2006　信息安全技术　信息系统安全管理要求

GB/T 20270　信息安全技术　网络基础安全技术要求

GB/T 20272　信息安全技术　操作系统安全技术要求

GB/T 20273　信息安全技术　数据库管理系统安全技术要求

GB/T 20275　信息安全技术　网络入侵检测系统技术要求和测试评价方法

GB/T 20279　信息安全技术　网络和终端隔离产品安全技术要求

GB/T 20281　信息安全技术　防火墙安全技术要求和测试评价方法

GB/T 20945　信息安全技术　信息系统安全审计产品技术要求和测试评价方法

GB/T 20984—2007　信息安全技术　信息安全风险评估规范

GB/T 21028　信息安全技术　服务器安全技术要求

GB/T 21050　信息安全技术　网络交换机安全技术要求(评估保证级 3)

GB/T 21052　信息安全技术　信息系统物理安全技术要求

GB/T 22081　信息技术　安全技术　信息安全管理实用规则

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 24363　信息安全技术　信息安全应急响应计划规范

GB/T 25055　信息安全技术　公钥基础设施安全支撑平台技术框架

GB/T 25069—2010　信息安全技术　术语

GB/T 25070—2010　信息安全技术　信息系统等级保护安全设计技术要求

GB/T 28451　信息安全技术　网络型入侵防御产品技术要求和测试评价方法

GB/T 28452—2012　信息安全技术　应用软件系统通用安全技术要求

GB/T 28453—2012　信息安全技术　信息系统安全管理评估要求

GB/T 29240　信息安全技术　终端计算机通用安全技术要求与测试评价方法

GB/T 29244　信息安全技术　办公设备基本安全要求