ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20945—2013
代替 GB/T 20945—2007

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

Information security technology—Technical requirements, testing and evaluation approaches for information system security audit product

2013-12-31 发布　　2014-07-15 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 20945—2007《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》,本标准与 GB/T 20945—2007 的主要差异如下:

——修改了“审计事件生成”功能(见 2007 版的 5.1.1);

——修改了“统计分析”功能;

——删除了“联动”(见 2007 版的 5.1.4.3)功能;

——删除了“缺省策略”和“策略模板”和“策略定制”功能(见 2007 版的 5.1.7.2、5.1.7.3 和 5.1.7.4);

——删除了“升级”功能;

——删除了“监管要求”功能(见 2007 版的 5.6);

——增加了“数据备份与恢复”功能;

——删除了“性能要求”(见 2007 版的第 7 章)。

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。

本文件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。

本标准起草单位:公安部计算机信息系统安全产品质量监督检验中心、深信服科技有限公司、蓝盾信息安全技术股份有限公司、厦门市美亚柏科信息股份有限公司。

本标准主要起草人:王志佳、沈亮、顾健、顾玮、邹春明、顾建新、赵云、胡维娜。

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

1　范围

本标准规定了信息系统安全审计产品的技术要求和测试评价方法，技术要求包括安全功能要求、自身安全功能要求和安全保证要求，并提出了信息系统安全审计产品的分级要求。

本标准适用于信息系统安全审计产品的设计、开发、测试和评价。

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 25069—2010　信息安全技术　术语

3　术语和定义

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

3.1

事件　incident

试图改变目标状态，并造成或可能造成损害的行为的发生。

3.2

安全审计　security audit

对事件进行记录和分析，并针对特定事件采取相应比较的动作。

3.3

信息系统安全审计产品　information system security audit product

对信息系统的事件进行记录和分析，并针对特定事件采取相应比较动作的产品。

3.4

审计记录　audit recordation

审计产品记录审计目标事件得到的信息。

3.5

审计日志　audit log

审计产品记录自身事件得到的信息。

3.6

审计中心　audit center

审计产品中记录、分析、处理审计代理发送的事件的功能部件。

3.7

审计代理　audit agent

审计产品中采集事件并发送给审计中心的功能部件。