ICS 35.040
L 80

中华人民共和国国家标准

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 products**

2007-06-13 发布　　2007-12-01 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

中 华 人 民 共 和 国
国 家 标 准
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 20945—2007
*
中国标准出版社出版发行
北京西城区复兴门外三里河北街16号
邮政编码:100045
http://www.spc.net.cn
http://www.gb168.cn
电话:(010)51299090、68522006
2007年10月第一版
*
书号:155066·1-29945

目　　次

前　言

本标准的附录 A 是资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：北京中科网威信息技术有限公司、公安部计算机信息系统安全产品质量监督检验中心、上海汉邦京泰数码技术有限公司。

本标准主要起草人：肖江、叶小列、刘宝旭、王晓箴、顾健、沈亮、陆中威、王贤蔚、王鸣。

引　言

信息系统安全审计产品为评估信息系统的安全性和风险和完善安全策略制定提供审计数据和审计服务支撑，从而达到保障信息系统正常运行的目的。同时，信息系统安全审计产品对信息系统各组成要素进行事件采集，将采集数据进行自动综合和系统分析，能够提高信息系统安全管理的效率。

本标准规定了安全审计产品的基本技术要求和扩展技术要求，提出了该类产品应达到的安全目标，并给出了该类产品的基本功能、增强功能和安全保证要求。

本标准规定了安全审计产品的测评方法，包括安全审计产品测评的内容和测评功能目标，给出了产品基本功能、增强功能和安全保证要求必须达到的具体目标。

本标准的目的是规范设计者如何设计和实现安全审计产品，并为安全审计产品的测评和应用提供技术支持和指导。

本标准用以规范设计者如何设计和实现安全审计产品，并为安全审计产品的测评和应用提供技术支持和指导。

本标准规定了基本型和增强型安全审计产品的技术要求以及测评方法，给出了该类产品应达到的安全功能要求和安全保证要求的具体目标。

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技术要求(安全功能要求、自身安全要求、性能要求和保证要求)和对应的测评方法。

本标准适用于信息系统审计产品的开发、测评和应用。

2　规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包含勘误的内容)或者修订版均不适合于本标准,但鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB 17859—1999　计算机信息系统安全保护等级划分准则

GB/T 5271.8—2001　信息系统　词汇　第8部分:安全(idt ISO/IEC 2382-8:1998)

GB/T 18336(所有部分)　信息技术　安全技术　信息技术安全性评估准则(GB/T 18336—2001,idt ISO/IEC 15408:1999)

3　术语和定义及记法

GB 17859—1999、GB/T 5271.8—2001 和 GB/T 18336—2001 确立的及以下术语和定义适用于本标准。

3.1　术语和定义

3.1.1

安全审计　security audit

对信息系统的各种事件及行为实行监测、信息采集、分析并针对特定事件及行为采取相应比较动作。

3.1.2

事件辨别器　event discriminator

提供事件最初的识别并决定是否向审计记录器传送该事件消息和产生审计报警的功能部件。

3.1.3

审计记录器　audit recorder

产生审计记录并将记录保存在本地或远程系统的功能部件。

3.1.4

审计分析器　audit analyzer

检查审计记录,以确认是否需要产生审计报警及采取相应行动的功能部件,对分析结果进行数据汇总,发送至报表生成器。

3.1.5

报表生成器　report processor

根据数据分析结论,进行报告处理,生成相关报告的功能部件。