ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 20945—2023
代替 GB/T 20945—2013

信息安全技术
网络安全审计产品技术规范

Information security technology—
Technical specification for network security audit products

2023-05-23 发布　　2023-12-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 20945—2013《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》，与GB/T 20945—2013相比，除结构调整和编辑性改动外，主要技术变化如下：

——更改了术语和定义“事件”“安全审计”“审计记录”“产品日志”“审计中心”“审计探针”（见3.3、3.4、3.6、3.7、3.8、3.9，2013年版的3.1、3.2、3.4、3.5、3.6、3.7）；

——更改了概述（见第5章，2013年版的第5章）；

——更改了“审计内容”（见6.1.2，2013年版的6.1.1.2.1、6.2.1.2.1）；

——删除了“扩展分析接口”（见2013年版的6.2.1.2.2.5）；

——增加了“自定义事件”（见6.1.6.4）；

——增加了“产品升级”（见6.1.6.5）；

——更改了“身份标识与鉴别”（见6.2.1，2013年版的6.1.2.1、6.2.2.1）；

——增加了“用户信息安全”（见6.2.5）；

——增加了“支撑系统安全”（见6.2.9）；

——增加了“环境适应性要求”（见6.3）；

——增加了“性能要求”（见6.4）；

——更改了“安全保障要求”（见6.5，2013年版的6.1.3、6.2.3）；

——增加了规范性附录“审计产品基本级和增强级技术要求和测评方法最小集合”（见附录B）。

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专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：公安部第三研究所、北京神州绿盟科技有限公司、北京天融信网络安全技术有限公司、奇安信网神信息技术（北京）股份有限公司、启明星辰信息技术集团股份有限公司、西安交大捷普网络科技有限公司、中国科学院信息工程研究所、杭州美创科技有限公司、深信服科技股份有限公司、上海市信息安全测评认证中心、蓝盾信息安全技术股份有限公司、华信咨询设计研究院有限公司、长春吉大正元信息技术股份有限公司、中国网络安全审查技术与认证中心、公安部第一研究所、中国电力科学研究院有限公司、北京山石网科信息技术有限公司、北京市政务信息安全保障中心（北京信息安全测评中心）、北京百度网讯科技有限公司、长扬科技（北京）股份有限公司、远江盛邦（北京）网络安全科技股份有限公司。

本文件主要起草人：王志佳、沈亮、陆臻、宋好好、顾健、俞优、胡维娜、邓琦、肖颖、白霜、刘岩、张伟锋、何建锋、安高峰、韩冬旭、周杰、叶润国、徐佟海、孙小平、刘强、邹毅、申永波、赵华、杨骋昊、姚盛颖、周兆栋、贾玲、李俊佐、董平。

本文件及其所代替文件的历次版本发布情况为：

——2007年首次发布为GB/T 20945—2007，2013年第一次修订；

——本次为第二次修订。

信息安全技术
网络安全审计产品技术规范

1 范围

本文件规定了网络安全审计产品的技术要求并描述了测评方法。

本文件适用于网络安全审计产品的设计、开发、测试和评价。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第1部分：简介和一般模型

GB/T 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件

GB/T 25069—2022 信息安全技术 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 18336.1—2015、GB/T 18336.3—2015 和 GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

网络安全 network security

对网络环境下存储、传输和处理的信息的保密性、完整性和可用性的保持。

[来源：GB/T 25069—2022，3.616]

3.2

异常 abnormal

从文档、操作或监测观察到偏离以前验证过的条件、状态或行为。

注：通常异常涉及的主体可能是人、设备、应用程序、服务/进程、数据等，因识别到的异常指向的主体不同，又分为用户行为异常、设备运行异常、程序执行异常、服务运行异常、数据异常等多种。

[来源：GB/T 32422—2015，3.1，有修改]

3.3

事件 incident

试图改变目标状态，并造成或可能造成异常或损害行为的发生。

[来源：GB/T 25069—2022，3.552，有修改]

3.4

安全审计 security audit

对网络、信息系统及其组件的记录与活动的独立评审和考察，以测试系统控制的充分程度，确保对