ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20275—2013
代替 GB/T 20275—2006

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

Information security technology—Technical requirements and testing and evaluation approaches for network-based intrusion detection system

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 20275—2006《信息安全技术 入侵检测系统技术要求和测试评价方法》。

本标准与 GB/T 20275—2006 的主要差异如下：

——标准名称修改为《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》；

——删除了 GB/T 20275—2006 中对主机入侵检测系统的技术要求和测试评价方法；

——删除了 GB/T 20275—2006 中的“分析方式”(见 2006 版的 6.1.1.2.2)；

——删除了 GB/T 20275—2006 中的“窗口定义”(见 2006 版的 6.2.1.4.1)；

——增加了“最大监控流量”“最大监控并发连接数”“最大监控新建 TCP 连接速率”的性能要求；

——增加了“硬件失效处理”“双机热备”的安全功能要求和测试评价方法；

——增加了“控制台鉴别”“标识唯一性”的自身安全功能要求和测试评价方法；

——调整了 GB/T 20275—2006 中“阻断能力”“系统升级”“报告定制”和“定制响应”的级别。

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、北京启明星辰信息安全技术有限公司、公安部网络安全保卫局。

本标准主要起草人：宋好好、顾健、张笑笑、李毅、吴其聪、张艳。