ICS 35.040
L 80

# 中华人民共和国国家标准

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

**Information security technology—
Techniques requirements and testing and evaluation approaches for
intrusion detection system**

2006-05-31 发布　　2006-12-01 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

# 目　　次

# 前　言

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：启明星辰信息技术有限公司、公安部公共信息网络安全监察局。

本标准主要起草人：陈洪波、刘恒、严立。

# 信息安全技术
# 入侵检测系统技术要求和测试评价方法

## 1 范围

本标准规定了入侵检测系统的技术要求和测试评价方法，技术要求包括产品功能要求、产品安全要求、产品保证要求，并提出了入侵检测系统的分级要求。

本标准适用于入侵检测系统的设计、开发、测试和评价。

## 2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，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 信息技术 词汇 第8部分：安全(idt ISO 2382-8：1998)

GB/T 18336.1—2001 信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型(idt ISO/IEC 15408-1：1999)

## 3 术语和定义

GB 17859—1999、GB/T 5271.8—2001 和 GB/T 18336.1—2001 确立的以及下列术语和定义适用于本标准。

3.1

**事件 incident**

信息系统中试图改变目标状态，并造成或可能造成损害的行为。

3.2

**入侵 intrusion**

任何危害或可能危害资源完整性、保密性或可用性的行为。

3.3

**入侵检测 intrusion detection**

通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

3.4

**入侵检测系统 intrusion detection system**

用于监测信息系统中可能存在的影响信息系统资产的行为的软件或软硬件组合。它通常分为主机型和网络型两种，由控制台、探测器和/或主机代理组成。

3.5

**网络型入侵检测系统 network-based intrusion detection system**

以网络上的数据包作为数据源，监听所保护网络内的所有数据包并进行分析，从而发现异常行为的入侵检测系统。