ICS 35.040
A 90

GA

# 中华人民共和国公共安全行业标准

GA/T 1728—2020

# 信息安全技术　基于 IPv6 的高性能网络入侵检测系统产品安全技术要求

**Information security technology—Security technical requirements for IPv6-based high-performance network intrusion detection system products**

2020-05-13 发布　　2020-08-01 实施

中华人民共和国公安部　　发 布

# 目　　次

# 前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

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、公安部第三研究所、网神信息技术（北京）股份有限公司。

本标准主要起草人：宋好好、顾建新、武腾、邹春明、陆臻、沈亮、顾健、李博、杨柳。

# 信息安全技术　基于IPv6的高性能网络入侵检测系统产品安全技术要求

## 1　范围

本标准规定了基于IPv6的高性能网络入侵检测系统产品的安全功能要求、环境适应性要求、性能要求、安全保障要求及安全等级划分。

本标准适用于基于IPv6的高性能网络入侵检测系统产品的设计、开发与测试。

## 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/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—2010　信息安全技术　术语

## 3　术语和定义

GB/T 18336.3—2015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　event**

一种系统、服务或网络状态的发生或者改变的记录信息，可作为分析安全事件的基础。

3.2

**安全事件　incident**

通过对事件的分析处理，从而识别出一种系统、服务或网络状态的发生，表明一次可能的违反安全规则或某些防护措施失效，或者一种可能与安全相关但以前不为人知的情况，极有可能危害业务运行和威胁信息安全。

3.3

**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。

3.4

**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。

3.5

**探测器　sensor**

用于收集可能指示出入侵行为或者滥用信息系统资源的实时事件，并对收集到的信息进行初步分析的入侵检测系统组件。