ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 36635—2018

# 信息安全技术　网络安全监测基本要求与实施指南

**Information security technology—Basic requirements and implementation guide of network security monitoring**

2018-09-17 发布　　2019-04-01 实施

国家市场监督管理总局
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。

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这些专利的责任。

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。

本标准起草单位:国家信息中心、国家信息技术安全研究中心、北京启明星辰信息技术股份有限公司、北京天融信科技股份有限公司、东软集团股份有限公司、亚信科技(成都)有限公司。

本标准主要起草人:周民、罗海宁、任飞、焦迪、李森、曹虎、蔡景怡、曾辉、张锐卿、吴大明、肖彪、刘增益、郑伟。

# 信息安全技术　网络安全监测<br>基本要求与实施指南

## 1　范围

本标准规定了网络安全监测的基本要求，给出了网络安全监测框架和实施指南。

本标准适用于系统或网络安全监测的实施，网络安全监测产品的设计开发，网络安全监测服务的提供等。

## 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/Z 20986—2007　信息安全技术　信息安全事件分类分级指南

GB/T 25069—2010　信息安全技术　术语

GB/T 28458—2012　信息安全技术　安全漏洞标识与描述规范

GB/T 31509—2015　信息安全技术　信息安全风险评估实施指南

## 3　术语和定义

GB/T 28458—2012 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

**网络安全监测　network security monitoring**

通过对网络和安全设备日志、系统运行数据等信息进行实时采集，以关联分析等方式对监测对象进行风险识别、威胁发现、安全事件实时告警及可视化展示。

3.2

**信息安全事件　information security incident**

由单个或一系列意外或有害的信息安全事态所组成的，极有可能危害业务运行和威胁信息安全。

[GB/T 25069—2010，定义 2.1.53]

3.3

**安全漏洞　vulnerability**

计算机信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷。这些缺陷以不同形式存在于计算机信息系统的各个层次和环节之中，一旦被恶意主体所利用，就会对计算机信息系统的安全造成损害，从而影响计算机信息系统的正常运行。

[GB/T 28458—2012，定义 3.2]

3.4

**风险管理　risk management**

识别、控制、消除或最小化可能影响系统资源的不确定因素的过程。

[GB/T 25069—2010，定义 2.3.39]