ICS 35.020
CCS L70

YD

中华人民共和国通信行业标准

YD/T 2387—202X
代替 YD/T 2387-2011

网络安全监测系统技术要求

Technical requirements for network security monitor system

（报批稿）

[点击此处添加本稿完成日期]

[××××]-[××]-[××]发布　　[××××]-[××]-[××]实施

中华人民共和国工业和信息化部　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YD/T 2387-2011《网络安全监控系统技术要求》，与YD/T 2387-2011相比，除结构调整和编辑性改动之外，主要技术变化如下：

——更改了功能架构，将“功能架构”改为“系统结构”（见图 1，2011 年版的图 1）；

——更改了对术语“安全事件”的相关描述（见 3.1，2011 年版的 3.3）

——增加了对术语“告警”的相关描述（见 3.4）

——增加了对术语“响应”的相关描述（见 3.5）

——增加了网络安全监测系统整体功能要求（见 5）

——删除了与用户维度相关的网络态势展示技术要求（见 2011 年版的 6.3.1）

——增加了事件分析与事故响应技术要求相关内容（见 7.3）

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。

本文件由中国通信标准化协会提出并归口。

本文件牵头起草单位：国防科技大学计算机学院、广州大学网络空间先进技术研究院、国家计算机网络应急技术处理协调中心。

本文件参与起草单位：中国信息通信研究院、鹏城实验室、湖南星汉数智科技有限公司、西北工业大学、山东中创软件商用中间件股份有限公司、中国科学院计算技术所、湖南蚁坊软件有限公司、四川亿览态势科技有限公司、恒安嘉新（北京）科技有限公司、北京天融信网络安全技术有限公司、西安邮电大学、上海数据分析与处理技术研究所。

本文件主要起草人：贾　焰、杨　行、李树栋、韩伟红、周　斌、李爱平、张伟哲、王震、江　荣、亓玉璐、赵晓娟、张勇、朱　争、刘海天、谢浩程、钟浩成、于　晗、崔婷婷、陈晓光、王龑。

本文件于2011年首次发布，本次为第一次修订。