ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 44886.5—2026

网络安全技术　网络安全产品互联互通 第5部分:行为信息格式

Cybersecurity technology—Cybersecurity product interconnectivity—Part 5: Behavior information format

2026-07-02 发布　　2027-02-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件是GB/T 44886《网络安全技术　网络安全产品互联互通》的第5部分。GB/T 44886已经发布了以下部分：

——第1部分：框架；

——第2部分：资产信息格式；

——第3部分：告警信息格式；

——第4部分：威胁信息格式；

——第5部分：行为信息格式。

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。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：国家计算机网络应急技术处理协调中心、国家计算机网络应急技术处理协调中心北京分中心、北京天融信网络安全技术有限公司、启明星辰信息技术集团股份有限公司、北京升鑫网络科技有限公司、安天科技集团股份有限公司、北京神州绿盟科技有限公司、长扬科技(北京)股份有限公司、杭州安恒信息技术股份有限公司、中国电子技术标准化研究院、奇安信科技集团股份有限公司、华为技术有限公司、中国科学院信息工程研究所、中国科学院信息工程研究所、深信服科技股份有限公司、三六零数字安全科技集团有限公司、联通数字科技有限公司、北京江民新科技术有限公司、海信集团控股股份有限公司。

本文件主要起草人：崔牧凡、王文磊、陈亮、吴莉莉、刘阳、安高峰、胡月、卞建超、李林哲、张宇娜、王吉勇、田丽丹、严定宇、朱雪峰、王惠莅、张亚京、蒋发群、周莹莹、薛春晖、李奕希、李彦峰、张东举、安锦程、刘吉鹏、刘松、孙凌、郭亮、王智明、严冬、王士宁、叶晓虎、赵云霞、赵辰、李佳、刘华、杨晶。

引　言

GB/T 44886《网络安全技术　网络安全产品互联互通》是指导网络安全产品互联互通建设的基础性和通用性标准，拟由六个部分构成。

——第1部分：框架。目的在于明确网络安全产品互联互通应用场景，提出互通建设思路。

——第2部分：资产信息格式。目的在于提出网络安全产品互联互通时的资产描述。

——第3部分：告警信息格式。目的在于有效整合网络安全产品报送的告警信息，提高告警应急处置效率。

——第4部分：威胁信息格式。目的在于统一网络安全产品及各组织威胁信息共享格式。

——第5部分：行为信息格式。目的在于促进网络安全产品行为信息的分析利用。

——第6部分：功能接口。目的在于高效整合网络安全信息，促进网络安全产品功能协同。

在网络安全产品互联互通所涉及的数据中，行为信息是实现安全风险分析和安全管理的重要基础。通过流量镜像、日志采集等技术手段，获取与记录网络和终端的活动情况，形成描述实体操作的行为信息。行为信息通常包含终端行为信息和网络行为信息两类，是告警生成、事件研判的重要支撑，也是网络安全产品之间需要交换的关键数据类型。

当前，行为信息来源多样、格式各异，导致网络安全产品之间的信息理解和协同处理存在障碍。本文件旨在规范行为信息的一致表达方式，提升信息交换处理的效率。

本文件的制定有助于建立统一的网络安全产品行为信息描述规范，打通不同厂商、不同类型产品间的数据壁垒，切实提升产品的互联互通能力，使各类产品能够在统一框架下协同工作，从而推动形成更加体系化、规范化的网络安全防护能力支撑体系。

网络安全技术　网络安全产品互联互通
第5部分:行为信息格式

1　范围

本文件确立了网络安全产品互联互通的行为分类,规定了行为信息的字段类型以及行为通用信息、行为专用信息的描述格式。

本文件适用于网络安全产品互联互通功能的设计、开发、应用和测试。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 7408.1　日期和时间　信息交换表示法　第1部分:基本原则

GB/T 25066　信息安全技术　信息安全产品类别与代码

GB/T 25069　信息安全技术　术语

3　术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

网络安全产品互联互通　cybersecurity product interconnectivity

通过统一的网络安全信息描述和安全功能实现,有效共享网络安全产品感知或产生的信息,协同不同网络安全产品的功能,支撑监测预警、信息共享、应急响应、态势感知等应用,提升网络安全防护能力和网络安全事件处置效率的一种机制。

[来源:GB/T 44886.1—2024,3.2]

3.2

行为信息　behavior information

通过直接记录原始数据或采用审计日志的方式,描述安全域内终端、网络环境中的各类行为活动的信息。

注:主要包括终端行为信息和网络行为信息。

4　缩略语

下列缩略语适用于本文件。

AS:自治系统(Autonomous System)

ASN:自治系统编号(Autonomous System Number)

BGP:边界网关协议(Border Gateway Protocol)

DNS:域名系统(Domain Name System)