



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 发布
国家标准化管理委员会

目 次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 1

5 行为分类 2

 5.1 概述 2

 5.2 终端行为 2

 5.3 网络行为 3

 5.4 其他行为 3

6 行为信息格式 3

 6.1 概述 3

 6.2 数据字段类型 3

 6.3 行为通用信息 4

 6.4 行为专有信息 4

附录 A（规范性） 网络安全产品行为信息分类代码 17

 A.1 编码方法 17

 A.2 分类代码表 17

参考文献 19

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)

FTP:文件传送协议(File Transfer Protocol)
GID:用户组标识符(User Group Identifier)
Http:超文本传输协议(Hyper Text Transfer Protocol)
Https:安全超文本传输协议(Hyper Text Transfer Protocol over Transport Layer Security)
ID:标识符(Identifier)
IMAP:邮件访问协议(Internet Mail Access Protocol)
IP:网际协议(Internet Protocol)
IPsec:IP 安全协议(Internet Protocol Security)
IPv4:网际协议版本 4(Internet Protocol version4)
IPv6:网际协议版本 6(Internet Protocol version 6)
MAC:媒体访问控制(Media Access Control)
OSPF:开放式最短路径优先(Open Shortest Path First)
POP3:邮局协议版本 3(Post Office Protocol version3)
RIP:路由信息协议(Routing Information Protocol)
SMTP:简单邮件传输协议(Simple Mail Transfer Protocol)
SSL:安全套接层(Secure Sockets Layer)
TCP:传输控制协议(Transmission Control Protocol)
TTL:生存时间(Time To Live)
UDP:用户数据报协议(User Datagram Protocol)
UID:用户标识符(User Identifier)
URL:统一资源定位系统(Uniform Resource Locator)
VPN:虚拟专用网(Virtual Private Network)
WebDav:基于 Web 的分布式创作与版本控制(Web Distributed Authoring and Versioning)

5 行为分类

5.1 概述

参照 GB/T 44886.1—2024,将行为分为终端行为、网络行为和其他行为 3 类,每个类别分别包括若干子类。

5.2 终端行为

终端行为包括基础命令执行行为和有助于支撑网络安全产品进行行为分析的特定子类终端行为。

- a) 基础命令执行行为:是用户和/或实体在安全域内终端上执行操作系统命令的所有行为。
- b) 特定子类终端行为:是指用户和/或实体在安全域内终端上执行的特定操作,包括终端账号行为、进程操作行为、文件操作行为、软件操作行为、外设操作行为、终端重要操作系统文件修改操作行为、驱动操作行为、系统服务操作行为、其他终端行为 9 个子类,具体如下:
 - 1) 终端账号行为:用户和/或实体通过用户名和口令或电子钥匙等凭证进行身份验证并获取系统或服务访问权限或对用户名、口令、权限等进行修改的行为;
 - 2) 进程操作行为:用户和/或实体对进程进行启动、中止、查看等相关操作的行为,以及进程网络访问行为;
 - 3) 文件操作行为:用户和/或实体对文件进行创建、修改、删除、权限修改等操作的行為;
 - 4) 软件操作行为:用户和/或实体安装、卸载、更新软件等相关操作;
 - 5) 外设操作行为:用户和/或实体对终端外接设备进行插入、拔出、数据写入、数据外传等操作

作的行为；

- 6) 终端重要操作系统文件修改行为:用户和/或实体对注册表项或值进行的创建、删除、修改等操作的行为；
- 7) 驱动操作行为:用户和/或实体对操作系统加载、卸载驱动文件等操作的行为；
- 8) 系统服务操作行为:用户和/或实体对操作系统服务的安装、启动、停止、配置修改(如服务依赖项、启动类型)等操作行为；
- 9) 用户和/或实体在安全域内终端上执行的其他子类行为。

5.3 网络行为

网络行为包括基础网络会话行为和有助于支撑网络安全产品进行行为分析的特定网络应用行为。

- a) 基础网络会话行为是指用户和/或实体在网络环境中,主动发起或被动建立的所有网络会话行为。
- b) 网络应用行为是指用户和/或实体在网络环境中,主动发起或被动建立的特定网络会话行为,包括邮件收发行为、网站访问行为、文件传输行为、远程登录行为、域名解析行为、路由信息交换行为、其他网络行为 7 个子类,具体如下:
 - 1) 邮件收发行为:用户和/或实体通过电子邮件发送和接收消息的网络行为；
 - 2) 网站访问行为:用户和/或实体访问特定网站的网络行为；
 - 3) 文件传输行为:用户和/或实体在网络上传输文件的网络行为；
 - 4) 远程登录行为:用户和/或实体通过远程访问协议登录到终端的网络行为；
 - 5) 域名解析行为:用户和/或实体通过域名解析服务获取 IP 地址的网络行为；
 - 6) 路由信息交换行为:用户和/或实体通过动态路由协议(如 BGP/OSPF/RIP)交换路由表信息,以维护网络拓扑结构和优化数据包转发路径的行为；
 - 7) 其他网络行为:用户和/或实体在网络环境中,主动发起或被动建立的其他子类会话行为。

5.4 其他行为

其他行为是指不能归为终端行为和网络行为两个基本分类的行为,目前包括数据库操作行为这一特定子类行为,即用户和/或实体对数据库进行操作的行为。

6 行为信息格式

6.1 概述

行为信息由通用信息和专有信息组成。通用信息用于描述各类行为的共性信息。专有信息用于描述不同类别行为的信息,包括行为分类基础信息和行为子类扩展信息。

示例 1: 以终端行为中的基础命令执行行为为例,其描述格式为:行为通用信息格式(见表 2)+终端行为基础信息格式(见表 3)。

示例 2: 以终端行为中的终端登录行为为例,其描述格式为:行为通用信息格式(见表 2)+终端行为基础信息格式(见表 3)+终端账号行为扩展信息格式(见表 4)。

示例 3: 以网络行为中的基础网络会话行为为例,其描述格式为:行为通用信息格式(见表 2)+网络行为基础信息格式(见表 13)。

示例 4: 以网络行为中的邮件收发行为为例,其描述格式为:行为通用信息格式(见表 2)+网络行为基础信息格式(见表 13)+邮件收发行为扩展信息格式(见表 14)。

6.2 数据字段类型

行为信息数据字段类型应符合表 1 的规定。

表 1 行为信息数据字段类型

字段类型	说明
字符型(string)	一种以字母、数字、汉字和其他字符形式表达的数据类型
整型(int)	一种用任意整数表达的数据元值的类型
日期时间型(datetime)	通过 YYYYMMDDhhmmss 的形式表达的值的类型,符合 GB/T 7408.1 的规定

6.3 行为通用信息

行为通用信息格式应符合表 2 的规定。

表 2 行为通用信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	行为类型	behaviorType	行为类型代码,符合附录 A 的规定	整型	是
2	产品标识	productID	记录行为的网络安全产品标识	整型	是
3	产品类型	productType	网络安全产品类型与代码,符合 GB/T 25066 的规定	整型	是
4	产品地址	productIP	网络安全产品 IP 地址	字符型	是
5	行为源	behaviorSource	产生行为的用户和/或实体	字符型	否

6.4 行为专有信息

6.4.1 终端行为

终端行为基础信息格式应符合表 3 的规定,其扩展信息格式应分别符合表 4~表 12 的规定。

表 3 终端行为基础信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	终端地址	hostIP	动作发生的终端 IP 地址	字符型	是
2	执行命令内容	commandContent	终端账号所执行的操作系统命令内容	字符型	是
3	终端账号名称	devAccountName	执行命令的终端账号名称	字符型	否
4	行为类型	behaviorType	终端行为的类型: 1——终端账号行为,2——进程操作行为, 3——文件操作行为,4——软件操作行为, 5——外设操作行为,6——终端重要操作系统文件修改操作行为,7——驱动操作行为,8——系统服务操作行为,9——其他终端行为	整型	是
5	行为时间	behaviorTime	终端行为发生的时间	日期时间型	是

表 4 终端账号行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	账号名称	accountName	登录终端的账号名称	字符型	是
2	登录方式	logType	登录的不同方式： 1——远程登录,2——本地账号登录, 3——本地电子钥匙登录,4——其他	整型	是
3	登录源地址	logSrcIP	登录行为关联的源终端地址	字符型	是
4	登录结果	logResult	登录的结果:1——成功,2——用户名错误,3——口令错误,4——其他	整型	是
5	账号变更类型	AccChangeType	账号变更的类型:1——账号增加,2——账号删除,3——账号信息修改,4——账号口令修改,5——登录方式变更,6——账号权限变更,7——用户组权限变更,8——用户组信息增加,9——用户组信息删除,10——用户组信息修改	整型	否
6	用户名	accUname	变更后的用户名(新增账号时为新建用户名;删除或修改账号时为操作对象用户名)	字符型	否
7	用户 ID	accUid	变更后的用户 ID(新增账号时为分配的新 UID;修改账号时为更新后的 UID。)	整型	否
8	用户组名	accGname	变更后的主用户组名(新增用户组时为新建组名;删除或修改用户组时为操作对象组名)	字符型	否
9	用户组 ID	accGid	变更后的用户组 GID(新增用户组时为分配的新 GID;修改用户组时为更新后的 GID)	整型	否
10	用户根目录	accHome	变更后的用户根目录路径,例如/home/newuser(新增或修改根目录时记录)	字符型	否
11	用户 Shell	accShell	变更后的默认 Shell 路径(如 /bin/bash)	字符型	否
12	Sudoshell	sudoShell	用户被授权的 sudo 可执行命令路径(如 /usr/bin/sudo)	字符型	否
13	Sudo 用户	sudoUname	被授予 Sudo 权限的用户名,记录被添加到 sudoers 文件中的用户或用户组	字符型	否
14	变更前 GID	preGid	变更前的用户组 ID(仅当用户组 GID 发生修改时记录旧值)	整型	否
15	变更前组名	preGname	变更前组名(仅当用户组名发生修改时记录旧值)	字符型	否
16	变更前用户根目录	preHome	变更前用户根目录	字符型	否

表 4 终端账号行为扩展信息格式（续）

序号	信息项	字段名称	字段说明	字段类型	是否必填
17	变更前登录 Shell	preloginShell	变更前的默认登录 Shell 路径	字符型	否
18	变更前 Sudo shell	presudoShell	变更前的 Sudo 命令路径 （记录权限调整前的命令路径）	字符型	否
19	变更前 Sudo 用户	presudoUname	变更前的 Sudo 授权用户 （记录权限调整前的授权用户或用户组）	字符型	否
20	变更前 UID	preUid	变更前的用户 UID （仅当用户 UID 发生修改时记录旧值）	整型	否
21	变更前用户名	preUname	变更前的用户名 （仅当用户名发生修改时记录旧值）	字符型	否
22	终端账号扩展信息	extAccountInfo	终端账号相关的扩展信息	字符型	否

表 5 进程操作行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	进程操作类型	processActionType	进程操作的类型： 1——启动,2——中止, 3——暂停,4——恢复	整型	是
2	进程号	processID	进程关联的 ID 号	整型	是
3	进程名称	processName	进程的名称	字符型	是
4	进程关联端口	processPort	进程关联的端口号	字符型	否
5	进程路径	processPath	进程路径信息	字符型	是
6	父进程路径	processParentPath	父进程路径信息	字符型	是
7	进程用户名	processUname	进程所属用户名称	字符型	是
8	进程优先级	processPriority	进程优先级	整型	否
9	进程网络连接状态	processConnectionStatus	进程网络的连接状态： 0——未知,1——连接,2——未连接	整型	是
10	进程网络连接协议	processConnectionProtocol	进程网络连接的协议名称,如: TCP、UDP	字符型	否
11	进程网络连接类型	processConnectionType	进程网络的连接类型： 1——in,0——out	整型	否
12	进程网络连接 IP	processDstIP	进程外接的 IP	字符型	否

表 5 进程操作行为扩展信息格式 (续)

序号	信息项	字段名称	字段说明	字段类型	是否必填
13	进程网络连接端口	processDstPort	进程外接的端口	整型	否
14	进程网络连接 URL	processConnectionURL	进程访问的 URL	字符型	否
15	进程网络连接域名	processConnectionDomian	进程访问的域名	字符型	否
16	进程扩展信息	processExtensionInfo	进程扩展信息	字符型	否

表 6 文件操作行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	文件操作类型	fileActionType	文件操作的类型： 1——创建, 2——修改内容, 3——修改权限, 4——修改属性, 5——重命名, 6——删除, 7——打开, 8——拷贝, 9——打印, 10——刻录	整型	是
2	文件名	fileName	操作目标文件名称	字符型	是
3	文件扩展名	fileNameExtensions	操作目标文件的扩展名(后缀名), 如 exe、doc、sh、bat 等	字符型	否
4	文件类型	fileType	操作目标文件的类型, 如 exe、doc、sh、bat 等	字符型	否
5	文件路径	filePath	操作目标文件在操作系统中的完整路径	字符型	否
6	文件拥有者	fileOwner	操作目标文件所属用户	字符型	否
7	文件所有组	fileGroup	操作目标文件所属用户组	字符型	否
8	文件大小	fileSize	操作目标文件大小	字符型	否
9	文件权限	filePermission	操作目标文件权限信息	字符型	否
10	进程号	processID	进程的 ID 号	整型	否
11	进程名称	processName	进程的名称	字符型	否
12	文件操作扩展信息	fileActionExtendedInfo	文件操作的扩展字段, 例如: 文件密级、文件访问范围等	字符型	否

表 7 软件操作行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	软件操作类型	softwareActionType	软件操作的类型： 1——安装,2——删除,3——更新	整型	是
2	软件名称	softwareName	操作目标软件名称	字符型	是
3	软件安装路径	softwarePath	软件操作系统中的完整路径	字符型	否
4	软件操作行为扩展信息	softwareActionExtInfo	软件操作行为的扩展信息	字符型	否

表 8 外设操作行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	终端外设操作类型	peripheralsActionType	终端外设操作的类型： 1——插入,2——拔出,3——使用中	整型	是
2	终端外设类型	peripheralsType	终端外设的类型,如:存储设备、键盘、打印机、扫描仪、鼠标等	字符型	是
3	终端操作系统名称	terminalOsType	终端的操作系统的名称	字符型	是
4	终端外设厂商名称	peripheralsVendor	终端外设所属厂商的名称	字符型	否
5	终端外设的产品序号	peripheralsProductID	终端外设的产品序号	字符型	否
6	终端外设的产品型号	peripheralsProductType	终端外设的产品型号	字符型	否
7	外设操作行为扩展信息	peripheralsExtInfo	外设操作行为的扩展信息	字符型	否

表 9 终端重要操作系统文件修改扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	操作进程名称	processName	与注册表、rc.local 等终端重要操作系统文件修改相关的进程的 名称	字符型	是
2	操作进程标识	processID	与注册表、rc.local 等终端重要操作系统文件修改相关的进程唯一标识符	整型	是
3	操作进程用户名称	processUserName	与注册表、rc.local 等终端重要操作系统文件修改相关的进程所属用户的名称	字符型	否

表 9 终端重要操作系统文件修改扩展信息格式 (续)

序号	信息项	字段名称	字段说明	字段类型	是否必填
4	终端重要操作系统文件操作对象	targetObject	与注册表、rc.local 等终端重要操作系统文件修改相关操作对象的详细信息。 如: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit、/etc/crontab、/sys/class/backlight/intel_backlight/brightness 等	字符型	是
5	操作进程路径	processPath	与终端重要操作系统文件修改相关的进程所对应的可执行文件的路径	字符型	否
6	终端重要操作系统文件操作后值	targetNewValue	与注册表、rc.local 等终端重要操作系统文件修改相关操作对象的操作后值	字符型	否
7	对象修改类型	objectModificationType	对象的修改类型及方式: 包括: 新建(create)、修改(update)、删除(delete)、新建键(createKey)、修改特定键的值(updateValue)、删除键(deleteKey)等	字符型	否
8	终端重要操作系统文件操作前值	targetOldValue	与注册表、rc.local 等终端重要操作系统文件修改相关操作对象的操作前值	字符型	否
9	终端重要操作系统文件修改扩展信息	terminalCriticalConfigModifyExtendDetails	与终端重要操作系统文件的当前变更的扩展详情信息	字符型	否

表 10 驱动操作行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	驱动操作类型	driverOperationType	驱动操作的类型: 1——加载, 2——卸载, 3——更新	整型	是
2	操作进程名称	driverProcessName	与驱动操作行为相关的进程的 名称	字符型	否
3	操作进程标识	driverProcessID	与驱动操作行为相关的进程唯一标识符	字符型	否
4	操作进程用户名	driverProcessUserName	与驱动操作行为相关的进程所属用户的名称	字符型	否
5	驱动名称	driverName	驱动的名称	字符型	是
6	文件路径	filePath	加载或卸载驱动文件的路径	字符型	是
7	是否签名	isSign	驱动文件是否有签名(是 否)	字符型	否
8	签名厂商	signName	驱动文件签名厂商名称	字符型	否

表 10 驱动操作行为扩展信息格式（续）

序号	信息项	字段名称	字段说明	字段类型	是否必填
9	签名状态	Status	签名有效性,是否为有效签名(是 否)	字符型	否
10	驱动操作行为扩展信息	driverBehaviorExtInfo	驱动操作行为的扩展信息	字符型	否
11	驱动的操作类型	driverOperationType	驱动操作的类型: 1——加载,2——卸载,3——更新	整型	是
12	操作进程名称	driverProcessName	与驱动操作行为相关的进程的名称	字符型	否

表 11 系统服务操作行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	服务名称	serviceName	系统服务的注册名称	字符型	是
2	服务描述	serviceDesc	服务的详细描述	字符型	否
3	操作进程名称	processName	操作驱动行为所对应的进程的名称	字符型	是
4	操作进程标识	processID	操作驱动行为所对应的进程的标识符	整型	是
5	操作进程用户名称	processUserName	操作驱动行为所对应的进程的所属用户名称	字符型	否
6	服务执行文件路径	commandPath	服务中可执行文件的路径	字符型	否
7	前置依赖项	startBefore	当前服务启动前应启动的依赖服务列表	字符型	否
8	后置依赖项	startAfter	依赖当前服务的其他服务列表	字符型	否
9	服务状态	serviceStatus	服务的状态: 0——停止,1——运行,2——启动中, 3——停止中,4——其他	整型	是
10	服务启动类型	serviceStartupStatus	服务启动的类型: 1——自动,2——自动延迟,3——手动, 4——禁用,5——其他	整型	是
11	服务扩展信息	serviceExtensionInfo	服务扩展信息	字符型	否

表 12 其他终端行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	其他终端行为	otherTerminalBehavior	终端行为信息类别属于其他类型时填写	字符型	是

6.4.2 网络行为

网络行为基础信息格式应符合表 13 的规定,扩展信息格式应分别符合表 14~表 22 的规定。

表 13 网络行为基础信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	网络行为类型	behaviorType	网络行为的类型: 1——邮件收发行为,2——网站访问行为,3——文件传输行为,4——远程登录行为,5——域名解析行为,6——路由交换行为,7——其他网络行为	整型	是
2	网络行为结果	behaviorResult	网络行为的结果: 1——成功,2——失败,3——未知	整型	是
3	源 IP	srcIp	网络行为发起者的 IP 地址	字符型	是
4	源端口	srcPort	网络行为发起者的端口号	整型	是
5	源端 MAC	srcMac	网络行为发起者的 MAC 地址	字符型	否
6	目的 IP	dstIP	网络行为接收者的 IP 地址	字符型	是
7	目的端口	dstPort	网络行为接收者的端口号	整型	是
8	目的端 MAC	dstMac	网络行为接收者的 MAC 地址	字符型	否
9	网络行为传输层协议	transportProtocol	传输层协议,如 TCP、UDP 等	字符型	是
10	网络行为会话开始时间	sessionStartTime	网络行为的会话开始时间	日期时间型	是
11	网络行为会话结束时间	sessionEndTime	网络行为的会话结束时间	日期时间型	是
12	网络行为应用层协议	applicationProtocol	应用层协议,如 Http/Https、Ftp、SmtP 等	字符型	否
13	网络行为 VPN 类型	behaviorVPNTYPE	网络行为的 VPN 类型: 0——不使用 VPN,1——SSL VPN, 2——IPSec VPN,3——其他类型 VPN	整型	是
14	网络行为基础信息 扩展信息	extendInfo	网络行为基础信息的扩展信息	字符型	否

表 14 邮件收发行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	邮件协议类型	mailProtocol	邮件协议的类型: 1——SMTP,2——POP3, 3——IMAP,4——私有协议	整型	是

表 14 邮件收发行为扩展信息格式（续）

序号	信息项	字段名称	字段说明	字段类型	是否必填
2	邮件收发结果	mailResult	邮件收发的结果。 1——发送成功,2——发送失败, 3——收取成功,4——收取失败	整型	是
3	发件人邮箱	senderMail	发件人邮箱	字符型	是
4	发件人名称	senderName	发件人名称	字符型	否
5	收件人邮箱	receiverMail	收件人的邮箱,多收件人地址以“,“隔开	字符型	是
6	收件人名称	receiverName	收件人的名称,多收件人名称以“,“隔开	字符型	否
7	抄送人邮箱	ccMail	抄送人的邮箱,多收件人地址以“,“隔开	字符型	否
8	抄送人名称	ccName	抄送人的名称,多收件人名称以“,“隔开	字符型	否
9	密送人邮箱	bccMail	密送人的邮箱,多收件人地址以“,“隔开	字符型	否
10	密送人名称	bccName	密送人的名称,多收件人名称以“,“隔开	字符型	否
11	邮件主题	mailSubject	邮件主题	字符型	是
12	邮件来源真实 IP	mailOriginIP	邮件来源真实 IP	字符型	否
13	邮件附件名	attachmentsName	邮件的附件名,多附件名称以“,“隔开	字符型	否
14	邮件收发扩展信息	extEmailInfo	邮件收发相关扩展信息	字符型	否

表 15 网站访问行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	HTTP/S 请求 URL	httpRequestURL	完整的网站 URL 信息	字符型	是
2	HTTP/S 请求方式	httpRequestMode	HTTP/S 请求方式,包括 GET、POST、PUT、HEAD 等	字符型	是
3	HTTP/S 协议版本	httpRequestProtocolVersion	HTTP/S 协议版本号, 如 HTTP/1.1 等	字符型	否
4	HTTP/S 响应状态码	httpResponseStatusCode	HTTP/S 状态码(200-成功,404-未找到,500-服务器错误等)	字符型	是
5	网站访问行为扩展信息	extendInfo	网站访问行为的扩展信息	字符型	否

表 16 文件传输行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	账号	username	涉及文件传输相关协议(如 FTP、WebDav 等)的登录账号	字符型	否
2	口令	password	涉及文件传输相关协议(如 FTP、WebDav 等)的登录口令	字符型	否
3	登录信息	loginInformation	涉及文件传输相关协议的其他登录信息,如失败状态码等	字符型	否
4	传输统一资源定位符	url	文件传输协议的目标统一资源定位符(URL)	字符型	是
5	文件传输方向	fileDirection	文件传输的方向:1——接收,2——发送	整型	是
6	文件名	fileName	涉及文件传输相关协议中传输的文件名	字符型	是
7	存储路径	contentPath	文件传输协议中接受端存储文件的路径	字符型	否
8	文件哈希值	hash	涉及文件传输相关协议中传输的文件哈希值,如 SM3	字符型	否
9	文件传输扩展信息	reserved	涉及文件传输相关扩展信息,如传输端口等;扩展信息有多个时,逗号分隔	字符型	否

表 17 远程登录行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	用户名	remoteLoginUsername	远程登录协议中记录的用户名	字符型	是
2	口令	remoteLoginPassword	远程登录协议中记录的口令	字符型	否
3	远程登录协议	remoteLoginPro	远程登录协议(如 Telnet、SSH、RDP 等)	字符型	否
4	远程登录路径	remoteLoginContentPath	远程登录协议连接后服务器端的当前工作目录	字符型	否
5	远程登录扩展信息	reserved	远程登录行为的扩展信息	字符型	否

表 18 域名解析行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	是否域名系统安全扩展	dnsSub	是否域名系统安全扩展	整型	否
2	访问类型	dnsType	访问类型	整型	是

表 18 域名解析行为扩展信息格式（续）

序号	信息项	字段名称	字段说明	字段类型	是否必填
3	消息 ID 标识	dnsHeader_ID	DNS 消息 ID 标识	整型	否
4	标志	flags	DNS 标志位	字符型	否
5	DNS 头部信息	dnsHeader	DNS 头部信息集合	字符型	否
6	查询类型	dnsQueryType	查询类型	整型	是
7	查询类	qClass	查询类	整型	否
8	查询内容	request	查询内容	字符型	是
9	应答资源记录集合	rr	应答资源记录集合	字符型	否
10	被查询域名	name	被查询域名（Name）	字符型	否
11	查询类型	type	查询类型（Type）	整型	否
12	类	class	类（Class）	整型	否
13	有效期	ttl	有效期（TTL）	整型	否
14	应答内容长度	rdLength	应答内容长度	整型	否
15	A 记录	addrA	A 记录是指定域名对应的 IP 地址	字符型	是
16	AAAA 记录	addrAaaa	AAAA 记录是指定域名对应的 IPv6 地址	字符型	是
17	邮件交换记录	mx	邮件交换记录	字符型	否
18	权威名称服务器	ns	权威名称服务器	字符型	否
19	真实名称记录	cname	真实名称记录	字符型	否
20	描述文本	txt	描述文本	字符型	否
21	域名解析扩展信息	reserved	域名解析行为的扩展信息	字符型	否

表 19 路由信息交换行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	路由信息交换 邻居 IP 信息	neighborInfoIP	邻居 IP，本次路由交换中对端路由器的 IP 地址（即 BGP 邻居、OSPF 邻居、RIP 邻居等），每次只填写产生路由交换行为的对应单个邻居 IPv4 或 IPv6 地址，如有必要分条填写。（例：203.0.113.1、2001:db8:1::1）	字符型	是
2	路由协议标识	protocolID	协议类型+版本（例：BGPv4/OSPFv2/RIPv1）	字符型	是

表 19 路由信息交换行为扩展信息格式（续）

序号	信息项	字段名称	字段说明	字段类型	是否必填
3	路由信息交换邻居 ASN 信息	neighborInfoASN	本次路由交换中对端邻居的自治系统编号 (ASN)标识符(例:64512)	字符型	否
4	路由交换行为类型	routeUpdate	描述本次路由交换行为在路由协议语义上的类别,路由更新类型为更新/撤销/通知(例:UPDATE、WITHDRAW、NOTIFY)	字符型	否
5	交换路由前缀	routePrefixes	这次消息中被通告或被撤销的 IP 前缀。描述的路由交换行为涉及具体路由前缀(新增、更新、撤销)时填写。(例:"203.0.113.0/24", "2001:db8:100::/48"等)	字符型	否
6	交换路径序列	asPath	路由协议的路径序列,描述当前交换路由描述的路径从哪些自治系统(AS)经过,如 BGP 路由交换行为的自治系统编号序列(AS_PATH)等。	字符型	否
7	通知协议错误代码	errorCode	协议指出的错误信息,如 BGP NOTIFICATION 消息 错误 码/错误 子 代码(例:Cease/Admin Reset)	字符型	否
8	路由交换行为扩展信息	routeSwitchBehavior ExtendDetails	与当前描述路由交换信息相关的扩展详情信息	字符型	否

表 20 其他网络行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	其他网络行为	otherNetworkBehavior	网络行为信息类别属于其他类型时填写	字符型	是

6.4.3 其他行为

其他行为专用部分由各行为子类扩展信息构成。数据库操作行为扩展信息格式应符合表 21 的规定。其他行为扩展信息格式应符合表 22 的规定。

表 21 数据库操作行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	会话 ID	logSessionId	数据流会话 ID	字符型	是
2	数据库名称	databaseName	数据库名/实例名	字符型	是

表 21 数据库操作行为扩展信息格式（续）

序号	信息项	字段名称	字段说明	字段类型	是否必填
3	数据库类型	dbType	数据库类型	字符型	否
4	数据库 IP	dbIP	数据库服务器 IP	字符型	是
5	登录 IP	relateIP	登录用户终端 IP	字符型	否
6	来源用户名	srcUserName	数据库登录账号	字符型	是
7	客户端工具	clientTool	客户端工具	字符型	否
8	sql 语句	sql	数据库查询语句	字符型	否
9	SQL 报文	payload	SQL 报文	字符型	是
10	执行时长	CostTime	执行时长	整型	否
11	执行结果	executeResult	执行结果(数据库)	字符型	否
12	影响行数	effectRow	SQL 执行影响行数	整型	否
13	响应内容	responseMsg	服务器在响应消息中发送给客户端的实际数据内容	字符型	是
14	数据库操作行为扩展信息	dbBehaviorExtendDetails	与数据库操作行为相关的扩展详情信息	字符型	否

表 22 其他行为扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	其他行为	otherBehavior	行为信息类别属于其他类型时填写	字符型	是

附 录 A
(规范性)
网络安全产品行为信息分类代码

A.1 编码方法

网络安全产品行为信息分类代码(以下简称“行为代码”)是对网络安全产品行为信息类别(以下简称“行为类别”)的编码,采用层次编码方法,代码由 5 位等长码构成。其中:

- a) 第一层表示网络安全产品行为信息类(如:网络行为),用两位阿拉伯数字(01~99)表示;
- b) 第二层表示网络安全产品行为信息类的子类(如:文件传输应用),用三位阿拉伯数字(001~999)表示。

编码结构如图 A.1 所示。

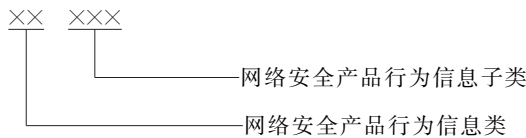


图 A.1 网络安全产品互联互通行为信息分类编码结构

A.2 分类代码表

网络安全产品行为信息分类代码应符合表 A.1 的规定。

表 A.1 网络安全产品行为信息分类代码

行为信息分类	行为信息子类	英文名称	分类代码
终端行为	基础命令执行行为	Common Command Execution Behavior	01001
	终端账号行为	Terminal Login Behavior	01002
	进程操作行为	Process Operation Behavior	01003
	文件操作行为	File Operation Behavior	01004
	软件操作行为	Software Operation Behavior	01005
	外设操作行为	Device Operation Behavior	01006
	终端重要操作系统文件修改行为	Registry Operation Behavior	01007
	驱动操作行为	Driver Operation Behavior	01008
	系统服务操作行为	System Service Operation Behavior	01009
	其他终端行为	Other Terminal Behavior	01010
网络行为	基础网络会话行为	Common Network Session Behavior	02001
	邮件收发行为	Email Communication Behavior	02002
	网站访问行为	Website Access Behavior	02003
	文件传输行为	File Transfer Behavior	02004
	远程登录行为	Remote Login Behavior	02005

表 A.1 网络安全产品行为信息分类代码（续）

行为信息分类	行为信息子类	英文名称	分类代码
网络行为	域名解析行为	Domain Name Resolution Behavior	02006
	路由信息交换行为	Route Switching Behavior	02007
	其他网络行为	Other Network Behavior	02008
其他行为	数据库操作行为子类	Database Operation Behavior	99001
	其他行为子类	Other Behavior	99002

参 考 文 献

- [1] GB/T 44886.1—2024 网络安全技术 网络安全产品互联互通 第1部分:框架
-

