TC260-PG-20234A

网络安全标准实践指南

—网络安全产品互联互通 告警信息格式

（v1.0-202311）

全国信息安全标准化技术委员会秘书处

2023 年 11 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国信息安全标准化技术委员会（以下简称“信安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

声　明

技术支持单位

本《实践指南》得到国家信息中心、中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、中国科学院信息工程研究所、沈阳东软系统集成工程有限公司、北京天融信网络安全技术有限公司、深信服科技股份有限公司、杭州安恒信息技术股份有限公司、北京神州绿盟科技有限公司、安天科技集团股份有限公司、亚信科技（成都）有限公司、北京升鑫网络科技有限公司等单位的技术支持。

摘　要

近年来，《网络安全法》《关键信息基础设施安全保护条例》《党委（党组）网络安全工作责任制实施办法》等法律法规、政策文件陆续出台，建立健全统一高效的网络安全风险监测、情报共享、研判处置机制，形成跨部门、跨行业高效联动的网络安全防护体系，已经成为现代化网络安全保障体系和保障能力建设的关注重点。网络安全产品互联互通是高效共享网络安全信息、有效整合网络安全能力的重要基础。

网络安全产品互联互通包括网络安全产品的互联互通功能和互联互通信息。其中互联互通信息的类型主要分为6类，包括资产信息、脆弱性信息、威胁信息、行为信息、告警信息和事件信息。

本实践指南规范了网络安全产品互联互通告警信息的描述格式，从不同网络安全产品告警信息有效互通和整合的角度出发，将网络安全产品告警信息类型分为恶意程序告警、网络攻击告警、数据安全告警、异常行为告警和其他告警5类，并细分为21个子类，规范了各类告警信息的通用信息和专有信息格式，并给出对应的字段表，包括字段名称、字段说明、字段类型以及是否必填等字段。

目　录

1 范围

本实践指南规定了网络安全产品互联互通时告警信息的描述格式。

本实践指南适用于网络安全产品互联互通的设计、开发、应用和测试。

2 术语和定义

2.1 网络安全产品互联互通 cyber security product interconnect

通过统一的网络安全信息描述和功能接口定义，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。

2.2 告警信息 alarm information

网络安全产品依据设定的规则或模型，对采集到的网络安全信息自动进行规则匹配、归并、分析等活动后产生的警示信息。

3 缩略语

APT：高级持续性威胁（Advanced Persistent Threat）

CPU：中央处理器（Central Processing Unit）

IP：网际互连协议（Internet Protocol）

MD5：信息摘要算法 5（Message-Digest Algorithm5）

SHA-1：安全散列算法 1（Secure Hash Algorithm 1）

SYN：同步序列编号（Synchronize Sequence Numbers）

UDP：用户数据报协议（User Datagram Protocol）

URL：统一资源定位符（Uniform Resource Locator）

4 告警分类

4.1 概述

本实践指南参考 GB/T 20986-2023 中规定的网络安全事件分类，将网络安全产品互联互通告警分为恶意程序告警、网络攻击告警、数据安全告警、异常行为告警和其他告警 5 类，每个类别分别包括若干子类。

本实践指南将告警信息分为重要告警信息和一般告警信息两级。

4.2 恶意程序告警

恶意程序告警包括计算机病毒告警、网络蠕虫告警、特洛伊木马告警、僵尸网络告警、恶意代码内嵌网页告警、勒索软件告警和挖矿软件告警 7 个子类，具体如下：

a) 计算机病毒告警：发现攻击者传播或利用恶意程序，影响计算机使用，破坏计算机功能，毁坏或窃取数据，发出警示；

b) 网络蠕虫告警：发现攻击者利用网络缺陷，通过网络自动复制并传播网络蠕虫，发出警示；

c) 特洛伊木马告警：发现攻击者传播或利用具有远程控制功能的恶意程序，实现非法窃取或截获数据，发出警示；

d) 僵尸网络告警：发现攻击者利用僵尸工具程序形成僵尸网络，

发出警示；

e) 恶意代码内嵌网页告警：发现受害对象在访问被嵌入恶意代码而受到污损的网页时，该恶意代码在访问该网页的计算机系统中安装恶意软件，发出警示；

f) 勒索软件告警：发现攻击者采取加密或屏蔽用户操作等方式劫持用户对系统或数据的访问权，并籍此向用户索取赎金，发出警示；

g) 挖矿软件告警：发现攻击者以获得数字加密货币为目的，控制他人的计算机并植入挖矿软件以完成大量运算，发出警示。

4.3 网络攻击告警

网络攻击告警包括网络扫描探测告警、网络钓鱼告警、漏洞利用告警、后门利用告警、凭据攻击告警、拒绝服务告警、网页篡改告警、失陷主机告警和 APT 告警 9 个子类，具体如下：

a) 网络扫描探测告警：发现攻击者利用网络扫描软件获取有关网络配置、端口、服务和脆弱性等信息，发出警示；

b) 网络钓鱼告警：发现攻击者利用欺诈性网络技术诱使用户泄露重要数据或个人信息，发出警示；

c) 漏洞利用告警：发现攻击者通过挖掘并利用网络配置缺陷、通信协议缺陷或应用程序缺陷等漏洞对网络实施攻击，发出警示；

d) 后门利用告警：发现攻击者恶意利用软件或硬件系统设计过程中未经严格验证所留下的接口、功能模块、程序等，非法获取网络管理权限，发出警示；

e) 凭据攻击告警：发现攻击者破解口令，解析登录口令或凭据等，发出警示；

f) 拒绝服务告警：发现攻击者通过非正常使用网络资源（诸如CPU、内存、磁盘空间或网络带宽）影响或破坏网络可用性，发出警示；

g) 网页篡改告警：发现攻击者通过恶意破坏或更改网页内容影响网站声誉或破坏网页及网站可用性，发出警示；

h) 失陷主机告警：发现攻击者获得某主机的控制权后，能以该主机为跳板继续攻击组织内网其他主机，发出警示；

i) APT 告警：发现攻击者通过对特定对象展开持续有效的攻击活动，发出警示。

4.4 数据安全告警

数据安全告警包括数据篡改告警、数据泄露告警 2 个子类，具体如下：

a) 数据篡改告警：发现未经授权接触或修改数据的行为，发出警示；

b) 数据泄漏告警：发现敏感数据或个人信息泄露的行为，发出警示。

4.5 异常行为告警

异常行为告警包括访问异常告警和流量异常告警 2 个子类，具体

如下：

a) 访问异常告警：发现用户访问行为偏离正常基线，发出警示；

b) 流量异常告警：发现网络流量偏离正常基线，发出警示。

4.6 其他告警

其他告警是指不能归为以上 4 个分类的网络安全告警。

5 告警信息格式

5.1 概述

告警信息由通用信息和专有信息组成，通用信息是描述各类告警的共性信息，专有信息是描述不同类别告警的信息，包括告警分类基础信息和告警子类扩展信息。

示例 1：以恶意程序告警中的计算机病毒告警为例，其描述格式为：告警通用部分（表 2）+恶意程序告警基础信息格式（表 3）+计算机病毒告警扩展信息格式（表 4）。附录 A 中给出了对应的告警信息格式示例。

示例 2：以数据安全告警中的数据篡改告警为例，其描述格式为：告警通用部分（表 2）+数据安全告警扩展信息格式（见表 21）。

5.2 字段类型取值

告警信息字段类型的取值见表 1。

表 1 告警信息字段类型的取值

字段类型	说明
字符型（string）	以字符包括字母、数字、汉字和其他字符形式表达的数据元值的类型。
整型（numeric）	用任意实数表达的数据元值的类型。
日期时间型（datetime）	通过 YYYYMMDDhh24mmss 的形式表达的值的类型。

5.3 告警通用信息

告警通用信息格式见表 2。

表 2 告警通用信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	告警时间	alarmTime	告警发生时间	日期时间型	是
2	告警等级	alarmGrade	1-低危 2-中危 3-高危	整型	是
3	告警名称	alarmName	告警信息名称	字符型	是
4	告警描述	alarmDesc	对告警的详细描述、说明	字符型	是
5	告警类型	alarmType	1-恶意程序告警，2-网络攻击告警，3-数据安全告警，4-异常行为告警，5-其他告警	整型	是
6	告警子类	alarmSubType	告警子类，见附录 B	字符型	是

表 2 告警通用信息格式（续）

序号	信息项	字段名称	字段说明	字段类型	是否必填
7	产品类型	devType	网络安全产品类型，见附录 C	字符型	是
8	产品地址	devIp	网络安全产品 IP 地址	字符型	是
9	受害对象 IP	victimIP	受害对象的 IP 地址，支持 ipv4、ipv6 格式	字符型	是
10	受害对象端口	victimPort	受害对象的端口	字符型	是

11	是否加密	encryption	告警所采集的网络安全信息是否加密，1-非加密，2-加密	整型	否
12	产品型号	devID	网络安全产品硬件型号	字符型	否
13	产品版本	devVer	网络安全产品软件版本	字符型	否
14	产品厂商	devVenodor	网络安全产品厂家名称	字符型	否
15	告警所属网络	alarmArea	告警所属的网络区域，如互联网、内网等	字符型	否
16	源 IP	sourceIP	对受害对象发起攻击或访问的 IP 地址，支持 ipv4、ipv6 格式	字符型	否
17	源端口	sourcePort	对受害对象发起攻击或访问的的端口	字符型	否
18	协议	protocol	承载的传输层协议或应用层协议	字符型	否
19	状态	state	攻击是否成功的状态，1-失败,2-成功,3-尝试，4-未知	字符型	否

5.4 告警专有信息

5.4.1 恶意程序告警

恶意程序告警基础信息格式见表3,扩展信息格式见表4至表10。

表 3 恶意程序告警基础信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	恶意程序名称	programName	恶意程序的名称	字符型	是
2	文件地址	filePath	恶意程序文件在计算机中的存放位置	字符型	是
3	MD5 值	fileMd5	恶意程序 MD5 值	字符型	是
4	家族	family	恶意程序所在家族	字符型	否
5	SHA-1 值	fileSha1	恶意程序 sha1 值	字符型	否
6	SHA-256 值	fileSha256	恶意程序 sha256 值	字符型	否
7	SM3 值	fileSM3	恶意程序 SM3 值	字符型	否
8	黑客组织	organization	恶意程序相关黑客或组织	字符型	否

表 4 计算机病毒告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	进程名	process	计算机病毒执行进程名称	字符型	是
2	文件地址	filePath	病毒文件在计算机中的存放位置	字符型	是

表 5 网络蠕虫告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	进程名	process	蠕虫执行进程名称	字符型	是
2	文件地址	filePath	蠕虫文件在计算机中的存放位置	字符型	是

表 6 特洛伊木马告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	进程名	process	木马执行进程名称	字符型	是
2	文件地址	filePath	木马文件在计算机中的存放位置	字符型	是
3	回联域名	backConnDomain	木马回联的域名	字符型	否
4	回联邮箱	backConnEmail	木马回联的邮箱	字符型	否
5	回联 IP	backConnIp	木马回联的 IP	字符型	否

表 7 僵尸网络告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	失陷 IP 地址	controlIP	僵尸网络的相关 IP，支持 ipv4、ipv6 格式	字符型	是
2	失陷域名	controlDomain	用于指挥和控制的的域名	字符型	否

表 8 恶意代码内嵌网页告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	域名信息	whois	域名信息	字符型	是
2	挂马源 URL	orgURL	实际挂马的网页链接	字符型	是
3	挂马源 IP 地址	orgIp	实际挂马网站的对应 IP 地址，支持 ipv4、ipv6 格式	字符型	否
4	挂马源所属国家	orgCountry	实际挂马网站的所属国家	字符型	否
5	挂马源所属省	orgProvince	实际挂马网站的所属省	字符型	否
6	挂马源所属市	orgCity	实际挂马网站的所属市	字符型	否
7	挂马源所属县	orgCounty	实际挂马网站的所属县	字符型	否

表 9 勒索软件告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	进程名	process	勒索软件执行进程名称	字符型	是
2	文件地址	filePath	勒索软件在计算机中的存放位置	字符型	是
3	加密算法	algorithm	勒索软件使用的加密算法	字符型	否

表 10 挖矿软件告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	进程名	process	挖矿软件执行进程名称	字符型	是
2	文件地址	filePath	挖矿软件在计算机中的存放位置	字符型	是
3	矿池地址	miningPoollIp	矿池 IP 地址	字符型	否
4	子域名列表	subdomainList	子域名列表	字符型	否

5.4.2 网络攻击告警

网络攻击告警基础信息见表 11，扩展信息见表 12 至表 20。

表 11 网络攻击告警基础信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	处置动作	action	1-阻断 2-放行 3-重定向	整型	是
2	攻击方向	direction	1-横向攻击 2-外联攻击 3-外部攻击	整型	否

表 12 网络扫描探测告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	被扫描端口列表	portList	被扫描端口列表	字符型	是
2	扫描探测类型	type	恶意攻击者对目标发起扫描探测的扫描类型	字符型	否
3	尝试频率	timesPermin	每分钟尝试次数	整型	否
4	开始时间	startTime	扫描开始时间	日期时间型	否
5	结束时间	endTime	扫描结束时间	日期时间型	否
6	返回信息	returnlnfo	扫描返回信息	字符型	否

表 13 网络钓鱼告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	钓鱼类型	type	钓鱼类型如邮件钓鱼、网站钓鱼等	字符型	是
2	域名	registrar	钓鱼网站域名	字符型	否
3	邮箱	registerEmail	钓鱼邮件邮箱	字符型	否

表 14 漏洞利用告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	漏洞名称	vulName	漏洞名称	字符型	是
2	系统研制厂商	vulOrg	存有漏洞的系统研制商	字符型	是
3	漏洞等级	vulGrade	超危、高危、中危、低危	字符型	是
4	漏洞类型	type	攻击时利用的漏洞类型	字符型	否
5	漏洞编号	vulCode	漏洞编号，支持 CNVD、CNNVD 等，格式如 CNVD-2014-0282、CNNVD-201404-530	字符型	否
6	漏洞描述	vulDescription	漏洞的描述	字符型	否
7	解决方案	solution	漏洞解决方案	字符型	否
8	漏洞发现者	vulDetector	漏洞发现的厂商或个人	字符型	否
9	参考链接	referURL	漏洞说明参考链接	字符型	否

表 15 后门利用告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	恶意程序名称	programName	后门程序的名称	字符型	是
2	文件地址	filePath	后门程序文件在计算机中的存放位置	字符型	是
3	MD5 值	fileMd5	后门程序 MD5 值	字符型	是
4	SHA-1 值	fileSha1	恶意程序 sha1 值	字符型	否
5	黑客组织	organization	后门程序相关黑客或组织	字符型	否
6	后门程序使用账号	userName	后门程序使用的账号	字符型	否

表 16 凭据攻击告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	开始时间	startTime	攻击开始时间	日期时间型	是
2	结束时间	endTime	攻击结束时间	日期时间型	是
3	凭据	credential	使用的凭据	字符型	否
4	尝试频率	timesPermin	每分钟尝试次数	整型	否

表 17 拒绝服务攻击告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	攻击类型	type	攻击类型(如 SYN 泛洪、UDP 泛洪等)	字符型	是
2	开始时间	startTime	攻击发生时间	日期时间型	是
3	结束时间	endTime	攻击结束时间	日期时间型	否
4	总包数	totalPackages	流量包总数，单位：个	整型	否
5	总字节数	totalBytes	总字节数，单位：byte	整型	否

表 17 拒绝服务攻击告警扩展信息格式（续）

序号	信息项	字段名称	字段说明	字段类型	是否必填
6	峰值包速率	peakPackagesRate	峰值包速率，单位：pps	整型	否
7	峰值字节速率	peakBytesRate	峰值字节速率，单位：Bps	整型	否
8	峰值流速率	peakFIowsRate	峰值流速率，单位：Mbps	整型	否

表 18 网页篡改告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	原网页路径	srcPath	原网页的 URL	字符型	是
2	篡改路径	disPath	篡改后的网页 URL	字符型	是
3	网页篡改类型	webDistortionType	类别如暗链、明链、其他等	字符型	否
4	关键字	keyword	篡改内容的关键字	字符型	否

表 19 失陷主机告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	失陷主机 ID	compromised_hostid	失陷主机标识，如：UUID	字符型	是
2	失陷类型	compromised_type	1-计算机病毒；2-网络蠕虫；3-特洛伊木马；4-僵尸网络；5-恶意代码；6-漏洞利用；7-后门利用；8-远程控制；9-凭据攻击；10-本地提权	整数型	是
3	外联恶意域名	extMalwareURL	失陷主机的外联 URL	字符型	否
4	外联 IP	extMalwareIP	失陷主机的外联 IP	字符型	否
5	攻击时间	attck_time	失陷判定依据的攻击行为的告警时间，格式采用 YYYY-MM-DD hh:1mm:ss，精确到秒	日期时间型	否

表 20 APT 告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	开始时间	startTime	首次发现攻击的时间	日期时间型	是
2	结束时间	endTime	攻击结束时间	日期时间型	是
3	APT 告警描述	APTMsg	APT 攻击过程描述	字符型	是
4	APT 组织名称	OrgName	APT 组织名称	字符型	否
5	APT 组织描述	OrgMsg	APT 组织描述	字符型	否

5.4.3 数据安全告警

数据安全告警的扩展信息见表 21 至表 22。

表 21 数据篡改告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	篡改类型	type	篡改类型（新建、内容修改、删除、权限变更等）	字符型	是
2	篡改路径	disPath	文档路径或者 URL	字符型	是
3	篡改时间	time	数据篡改时间	日期时间型	是
4	关键词	keyword	篡改关键字	字符型	否
5	篡改内容	distortionTitle	篡改内容说明	字符型	否

表 22 数据泄露告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	泄露内容类型	type	泄露类型	字符型	是
2	篡改路径	disPath	文档路径或者 URL	字符型	是
3	泄露时间	time	发现首次数据泄露的时间	日期时间型	是

表 22 数据泄露告警扩展信息格式（续）

序号	信息项	字段名称	字段说明	字段类型	是否必填
4	告警描述	Description	命中关键词前后文 512 字节	字符型	是
5	关键词	keyword	命中关键词，多个关键词用逗号分隔	字符型	是
6	数据泄露IP	leakIp	数据单独加密，支持 ipv4、ipv6 格式	字符型	是
7	数据泄露端口	port	数据单独加密，通用部分不再存储	字符型	是

5.4.4 异常行为告警

异常行为告警的扩展信息见表 23 至 24。

表 23 访问异常告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	访问路径	dstPath	访问路径或者 URL	字符型	是
2	请求方法	method	请求方法，包括 post 等	字符型	否
3	异常信息	abnormal_info	异常信息描述	字符型	否

表 24 流量异常告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	时间窗	cycleTime	异常流量监测时间周期，单位：秒	整型	是
2	总包数	totalPackages	流量包总数，单位：个	整型	是
3	总字节数	totalBytes	总字节数，单位：byte	整型	是
4	峰值包速率	peakPackagesRate	峰值包速率，单位：pps	整型	否
5	峰值字节速率	peakBytesRate	峰值字节速率，单位：Bps	整型	否

5.4.5 其他告警

其他告警的扩展信息见表 25。

表 25 其他告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	其他告警	other-info	其他告警信息	字符型	否

附录 A

（资料性）

告警信息格式示例

A.1 概述

本附录给出了一个网络安全产品互联互通告警信息格式描述的告警信息示例。

以恶意程序告警中的计算机病毒告警为例，其描述格式为：告警通用部分（表2）+恶意程序告警基础信息格式（表3）+计算机病毒告警扩展信息格式（表4）。

示例采用JSON作为数据交换格式。

A.2 告警信息格式示例

{
"alarmTime":"2021-12-21 12:33:24"
"alarmGrade": "1"
"alarmName": "恶意程序"
"alarmDesc": "业务平台服务器遭受XX计算机病毒攻击……"
"alarmType": "1"
"alarmSubType": "01001"
"devType": "D105"
"devIp": "1.1.1.1"

"victimIP": "2.2.2.2"

"victimPort": "1443"

"encryption": "1"

"devID": " NGFW4000-UF "

"devVer": " NGFW4000v2.0"

"devVenodor": "XXX公司"

"alarmArea": "互联网"

"sourceIP": "51.1.1.1"

"sourcePort": "443"

"protocol": "TCP"

"state": "3"

"programName":" Voluminer "

"filePath": "/etc/……"

"fileMd5": " 6512bd43d9caa6e02c990b0a82652dca"

"family": " Lockbit"

"fileSha1": " 17ba0791499db908433b80f37c5fbc89b870084b"

"fileSha256": " 4fc82b26aecb47d2868c4efbe3581732a3e7cbc
c6c2efb32062c08170a05eeb8"

"fileSM3": "d5744897e47fb6d78b726e9ff0c9fa70e0013a0d4f0
a757af8ec0b812664b828"

"organization": "匿名者"

```
    "process":"123.exe "
    "filePath":  "/etc/……"
}
```

附录 B

（规范性）

网络安全产品互联互通告警信息分类代码

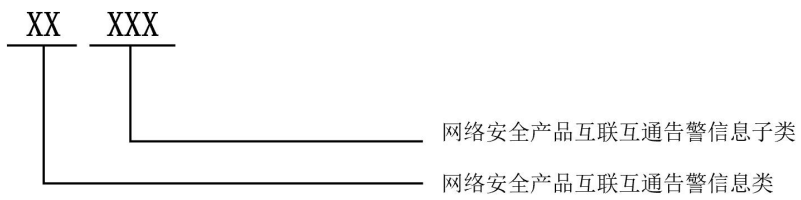
B.1 编码方法

网络安全产品互联互通告警信息分类代码(以下简称“告警代码”)是对网络安全产品互联互通告警信息类别（以下简称“告警类别”)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互联互通告警信息类(如：恶意程序告警)，用两位阿拉伯数字(01～99)表示；

b) 第二层表示网络安全产品互联互通告警信息类的子类(如：计算机病毒告警)，用三位阿拉伯数字（001～999）表示。

编码结构如图 B.1 所示。



图B.1　网络安全产品互联互通告警信息分类编码结构

B.2 分类代码表

网络安全产品互联互通告警信息的分类代码见表B.1。

表 B.1 网络安全产品互联互通告警信息分类代码表

告警信息分类	告警信息子类	英文名称	分类代码
恶意程序告警	计算机病毒告警	computer virus alarm	01001
	网络蠕虫告警	cyber worm alarm	01002
	特洛伊木马告警	trojan horse alarm	01003
	僵尸网络告警	botnet alarm	01004
	恶意代码内嵌网页告警	malicious code embedded web page alarm	01005
	勒索软件告警	ransomware alarm	01006
	挖矿软件告警	miner virus alarm	01007
网络攻击告警	网络扫描探测告警	cyber scan detection alarm	02001
	网络钓鱼告警	cyber phishing alarm	02002
	漏洞利用告警	exploitation of vulnerability alarm	02003
	后门利用告警	exploitation of backdoor alarm	02004
	凭据攻击告警	credential attack alarm	02005
	拒绝服务告警	denial of service alarm	02006
	网页篡改告警	webpage tampering alarm	02007
	失陷主机告警	lost host alarm	02008
	APT 告警	advanced persistent threat alarm	02009
数据安全告警	数据篡改告警	data tampering alarm	03001
	数据泄露告警	data breach alarm	03002
异常行为告警	访问异常告警	access exception alarm	04001
	流量异常告警	traffic anomaly alarm	04002
其他告警	其他告警子类	other alarm	99001

附录 C

（规范性）

告警相关网络安全产品类别与代码

按照GB/T 25066-2020，表C.1给出了与告警相关的网络安全产品类别与代码。

表 C.1 告警相关网络安全产品类别与代码表

网络安全产品类型编码	网络安全产品类型
B201	网络入侵检测
B202	网络活动监测与分析
B203	流量控制
B204	上网行为管理
B205	反垃圾邮件
B206	信息过滤
C101	终端隔离
C102	网络隔离
C103	网络单向导入
C201	网络入侵防御
C202	网络恶意代码防范
C203	抗拒绝服务攻击
C301	防火墙
C302	安全路由器
C303	安全交换机
C401	终端接入控制
D103	主机入侵检测
D105	主机型防火墙
D106	终端使用安全
D107	移动存储设备安全管理
D201	主机恶意代码防治
D402	WEB 应用防火墙
D403	邮件安全防护
D404	网站恢复
D501	业务流程监控
D503	网站监测
D504	应用软件安全管理
D602	数据泄露防护

表 C.1 网络安全产品类别与代码表（续）

网络安全产品类型编码	网络安全产品类型
D701	安全数据库
D702	数据库安全部件
D703	数据库防火墙
E101	安全审计
E404	漏洞挖掘
E405	态势感知
E406	高级持续威胁检测
E501	安全管理平台
X999	其它

参考文献

[1] GB/T 20986-2023 信息安全技术 网络安全事件分类分级指南

[2] GB/T 25066-2020 信息安全技术 信息安全产品类别与代码