ICS 35.240
A 90

GA

# 中华人民共和国公共安全行业标准

GA/T 1717.3—2020

# 信息安全技术　网络安全事件通报预警 第3部分：数据分类编码与标记标签体系技术规范

**Information security technology —Notification and warning of cyber security incident—Part3：Technical specifications for data classification coding and label system**

2020-03-24 发布　　2020-08-01 实施

中华人民共和国公安部　发布

# 目　　次

# 前　言

GA/T 1717《信息安全技术　网络安全事件通报预警》分为三个部分：

——第1部分：术语；

——第2部分：通报预警流程规范；

——第3部分：数据分类编码与标记标签系统技术规范。

本部分为GA/T 1717的第3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由公安部网络安全保卫局提出。

本部分由公安部信息系统安全标准化技术委员会归口。

本部分起草单位：公安部网络安全保卫局、中国科学院软件研究所、公安部第三研究所。

本部分主要起草人：黄小苏、张秀东、吴辰苗、任彬、张海霞、黄克振、刘玉岭、贾文卓、陶源。

# 信息安全技术　网络安全事件通报预警 第3部分:数据分类编码与标记标签体系技术规范

## 1　范围

GA/T 1717的本部分规定了网络安全事件通报预警工作中网络安全数据的分类方法、编码方法和标记标签体系。

本部分适用于网络安全职能部门开展网络安全监测分析、通报预警、应急处置工作。

## 2　规范性引用文件

下列文件对于本文件的引用是必不可少的。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/T 4754　国民经济行业分类

GB 11714　全国组织机构代码编制规则

GB/T 25069　信息安全技术　术语

GB 32100　法人和其他组织统一社会信用代码编码规则

GA/T 1717.1　信息安全技术　网络安全事件通报预警　第1部分:术语

## 3　术语和定义

GB/T 25069和GA/T 1717.1界定的以及下列术语和定义适用于本文件。

3.1

**网络安全数据分类　cyber security data classification**

根据网络安全数据的属性或特征,将其按照一定的原则和方法进行区分和归类,并建立起一定的分类体系和排列顺序,以便更好地管理和使用数据的过程。

3.2

**网络安全数据编码　cyber security data coding**

在分类的基础上,给网络安全数据赋予具有一定规律性、计算机容易识别与处理的符号。

3.3

**事权单位　responsible organization**

提供网络安全数据并从业务上对数据内容负责的单位。

3.4

**数据标记标签　datalabel**

网络安全数据自身属性内含的,或经由一定分析计算标记的,用于对数据或数据所描述对象进行概括性、抽象性描述的具有一定动态性和时效性的文本型数据。

## 4　制定原则

网络安全数据分类方法制定原则如下:

a） 稳定性。应以数据最稳定的特征和属性为依据；
b） 唯一性。保证每一个网络安全数据编码对象仅有唯一的编码；
c） 可扩性。应留有足够的备用码和标记标签，支持必要的修订和补充。

## 5 网络安全数据分类方法

### 5.1 网络安全数据要素分类

网络安全数据要素分类见表1。

**表1 网络安全数据要素分类**

| 代码 | 名称 | 说明 |
|---|---|---|
| 1 | 人 | 以人为主体进行描述的网络安全数据要素，包括个人和组织，其中组织指按照一定宗旨和系统建立起来的在网络空间内进行活动的团体 |
| 2 | 物 | 以物为主体进行描述的网络安全数据要素，包括特定情况下针对不同情况涵盖不同的内容，包括资产、威胁、脆弱性、风险等 |
| 3 | 地 | 以地点为主体进行描述的网络安全数据要素，如国家、地区、省、市、县 |
| 4 | 事 | 以网络安全事件为主体进行描述的网络安全数据要素 |

### 5.2 网络安全数据类别分类

网络安全数据类别分类见表2。

**表2 网络安全数据类别分类**

| 代码 | 名称 | 说明 |
|---|---|---|
| 1 | 基本信息 | 对主体和主体行为的基本要素进行描述，包括ID信息、日志信息 |
| 2 | 关系信息 | 对主体在网络安全活动中与主体主要关系进行描述 |
| 3 | 活动信息 | 对主体参与的各种网络安全活动进行描述 |
| 4 | 图片影像信息 | 与主体有关的以图片、音频或影像的格式存储的网络安全数据 |
| 5 | 文档资料信息 | 与主体相关的文字档案信息 |

### 5.3 网络安全数据活动特征分类

网络安全数据活动特征分类见表3。

**表3 网络安全数据活动特征分类**

| 代码 | 名称 | 说明 |
|---|---|---|
| 1 | 网络空间基本活动 | 登录、发表观点、关注、浏览、转发等网络空间的数据记录，以及生成日志、使用工具等价值性活动 |

表 3（续）

| 代码 | 名称 | 说明 |
| --- | --- | --- |
| 2 | 网络安全活动 | 安全扫描、漏洞利用、攻击工具下载等网络安全相关的活动记录 |
| 3 | 实名活动 | 主体以实名进行的各类活动 |
| 4 | 非实名活动 | 主体以网络 ID 等未实名认证的虚拟标识进行的各类活动 |

### 5.4 网络安全数据属性分类

网络安全数据属性分类见表 4。

表 4 网络安全数据属性分类

| 代码 | 名称 | 说明 |
| --- | --- | --- |
| 1 | 基础信息 | IP 基础信息、域名基础信息等社会公共主体可以提供的数据 |
| 2 | 资源信息 | 端口服务资源信息、黑客档案资源信息、网站/设备指纹资源信息、木马特征资源信息、病毒特征资源、漏洞资源信息、钓鱼网站资源信息、违法网站资源信息等用于辅助网络安全监测分析、通报预警、应急处置的数据 |
| 3 | 业务信息 | 案(事)件信息、情报数据业务信息、通报预警业务信息、应急处置业务信息等网络安全防护、通报、预警和处置过程中产生的过程性或结果性数据 |

## 6 网络安全数据分类编码方法

### 6.1 编码方法

采用线分类法和面分类法混合编码的方法。

### 6.2 编码组成

由英文字母、阿拉伯数字和破折号组成。

### 6.3 线分类法编码规则

以线分类法构建左第 1～45 位：

a) 第 1～2 位用英文字母“CS”表示该编码为网络安全数据编码；
b) 第 3 位为破折号；
c) 第 4～21 位由阿拉伯数字和英文字母组成，表示网络安全数据的事权单位，应根据不同情况分别符合 GB 11714、GB 32100 和 GA/T 380 的规定，其中，不足 18 位时以前补零方式补齐；
d) 第 22 位为破折号；
e) 第 23～45 位由英文字母、阿拉伯数字和破折号组成，表示网络安全数据的所属目录编码，具体编码规则见 6.4 和附录 A，网络安全数据目录编码参见附录 B 中的表 B.1。

### 6.4 面分类法编码规则

以面分类法构建左起第 23～45 位：

a) 第 23～27 位由英文字母和阿拉伯数字表示网络安全数据的行业门类代码，应符合 GB/T 4754

的规定；

b） 第 28 位为破折号；

c） 第 29 位阿拉伯数字表示该网络安全数据的属性代码，应符合 5.4 的规定；

d） 第 29～ 31 位阿拉伯数字和字母表示该网络安全数据的网络安全业务代码，其中，不足 3 位时以前补零方式补齐；

e） 第 32 位阿拉伯数字表示网络安全数据的类别代码，应符合 5.2 的规定；

f） 第 33 位阿拉伯数字表示网络安全数据的要素代码，应符合 5.1 的规定；

g） 第 34 位阿拉伯数字表示网络安全数据的活动特征代码，应符合 5.3 的规定；

h） 第 35 位为破折号；

i） 第 36～45 位为预留位，可根据具体分类特征进行扩展分类。

## 7 网络安全数据标记标签

### 7.1 网络安全数据标记标签类别

网络安全数据标记标签分类包括：

a） 网络安全类目标签：

根据第 5 章所标识的数据所属多个分类所显示的标签称为网络安全类目标签。网络安全数据分类通常为多级，类目标签带有级别属性，如：使用分类树一级分类为数据打标签，标签便是一级类目标签；

b） 威胁攻击属性标签：

由数据记录的具体属性字段直观显示的标签，如后门控制事件发生省、攻击者的性别、安全隐患事件的级别等。属性标签无须增加标签字段进行标识，需要时可从数据属性直接抽取；

c） 威胁攻击统计标签：

不能由数据记录的具体属性字段显示，而需要运用一定的统计分析手段处理所得的概括性、抽象性或聚类标签，如：为某攻击者描述数据所打的“青年”“中年”标签，为某钓鱼网站数据所打的影响范围标签等；

d） 关联/关系标签：

在网络要素间直接关系、间接关系以及多维度关联关系的基础上，采用一定的关联关系计算方法生成的，标示某数据网络安全威胁攻击的标签，如：利用深度学习算法为网络安全事件数据所打的准确性标签，利用关联分析算法为 IP 标记的是否恶意或者与某类事件关联度标签等；

e） 场景标签：

标示某网络威胁攻击数据所关联某项事务、某种场景、某种专项等的标签，例如：2019 两会、通报预警业务、净网行动等；

f） 组合标签：

若干子标签进行组合而标记出的网络威胁攻击的标签，如：北京市受菜刀后门影响极大的教育类网站、极大可能为某北美地区黑客组织用于实施僵尸控制的网络资源等；

g） 自定义标签：

网络威胁攻击数据使用者根据监测发现、分析研判、通报处置、追踪溯源等业务应用需要而标记出的网络威胁攻击的标签。

### 7.2 网络安全数据标记标签样例

标记标签样例参见附录 C。

# 附 录 A
（规范性附录）
分类编码规则

## A.1 分类编码规则

网络安全数据编码中的第23～45位是网络安全数据所属目录编号，包括行业门类、网络安全业务、要素、类别、活动特征和属性共六段，以面分类法构建编码，标识网络安全数据的一个分类维度，全部分类维度构建唯一的网络安全数据所属目录编号；其中，六段编码不可同时全为零。

网络安全数据编码中的第29～34位表示属性、业务、类别、要素、活动特征五个维度构成的类别编码，标识网络安全数据目录的分类，亦采用面分类法编码。根据第5章的规定，从四个维度对数据进行多维分类，构成彼此互无树型隶属关系的面，每个面都包含一组细目。将单个面中的细目与其他面的细目组合构成复合细目形态的分类对象编码。

网络安全分类编码中的第36～45位为预留编码，适用于活动特征的进一步细分。

## A.2 网络安全数据分类编码

网络安全数据编号结构为“CS—××××××××××××××××××（网络安全数据事权单位机构代码，事权单位为公安机关则按照GA/T 380填写；事权单位为非公安机关则填写18位全国组织机构代码或全国统一信用代码，前补0）-××××××—××××××—××××××××××（网络安全数据所属目录编号）”。

**示例：**

CS-121000004000123696-S9223-200532-001001000

121000004000123696：事权单位机构代码

S9223-200532-001001000：网络安全数据所属目录编号

其中，网络安全数据所属目录编号S9223—200512-001001000具体含义如下：

a) S9223表示该网络安全数据的行业门类代码，依据GB/T 4754的规定为“公共安全管理机构”；

b) 200532表示该网络安全数据的分类代码，第1位代码“2”表示网络安全数据属性分类“资源数据”；第2～4位“005”表示网络安全业务代码，具体为“通报业务”；第5位代码“3”代表网络安全数据类别“活动信息”；第6位代码“2”网络安全数据活动特征分类中的“网络安全活动”；

c) 001001000表示网络安全活动类别的具体分类，有害程序事件-僵尸控制，最后3位“000”为补全位。

## A.3 网络安全业务代码

网络安全业务代码见表A.1。

表 A.1　网络安全业务代码

| 代码 | 名称 |
| --- | --- |
| 001 | 等级保护业务 |
| 002 | CII 保护业务 |
| 003 | 监测发现业务 |
| 004 | 分析研判业务 |
| 005 | 通报业务 |
| 006 | 预警业务 |
| 007 | 应急处置业务 |
| 008 | 攻防演习业务 |
| 009 | 重大活动安保业务 |
| 010 | 情报业务 |
| 011 | 事件调查业务 |
| 012 | 案件侦查业务 |
| 013 | 互联网监管 |
| 014 | 网络安全专项 |

# 附　录　B
（资料性附录）
网络安全数据目录编码样例

网络安全数据目录编码见表 B.1。

**表 B.1　网络安全数据目录编码**

| 代码 | 一级 | 二级 | 三级 | 四级 | 五级 |
|---|---|---|---|---|---|
| S9223-1000141-001001LLL | 原始数据 | 原始流量类 | 一类流量数据 | | |
| S9223-1000141-001002LLL | 原始数据 | 原始流量类 | 二类流量数据 | | |
| S9223-1000141-001003LLL | 原始数据 | 原始流量类 | 三类流量数据 | | |
| S9223-1000141-002001LLL | 原始数据 | 网络基础日志 | 安全审计日志 | | |
| S9223-1000141-002002LLL | 原始数据 | 网络基础日志 | IP 通联日志 | | |
| S9223-1000141-002003LLL | 原始数据 | 网络基础日志 | DNS 协议日志 | | |
| S9223-1000141-002004LLL | 原始数据 | 网络应用日志 | 管理端口远程连接日志 | | |
| S9223-1000141-002005LLL | 原始数据 | 网络应用日志 | SMTP 协议日志 | | |
| S9223-1000141-002006LLL | 原始数据 | 网络应用日志 | HTTPS 协议日志 | | |
| S9223-1000141-002007LLL | 原始数据 | 网络应用日志 | HTTP 协议日志 | | |
| S9223-1012141-001001LLL | 原始数据 | 案事件辅助支撑数据 | 一类辅助支撑数据 | | |
| S9223-1012141-001002LLL | 原始数据 | 案事件辅助支撑数据 | 二类辅助支撑数据 | | |
| S9223-1012141-001003LLL | 原始数据 | 案事件辅助支撑数据 | 三类辅助支撑数据 | | |
| S9223-1012141-001004LLL | 原始数据 | 案事件辅助支撑数据 | 四类辅助支撑数据 | | |

表 B.1（续）

| 代码 | 一级 | 二级 | 三级 | 四级 | 五级 |
|---|---|---|---|---|---|
| S9223-1012141-001005LLL | 原始数据 | 案事件辅助支撑数据 | 五类辅助支撑数据 | | |
| S9223-1012141-002WWWLLL | 原始数据 | 威胁告警类 | | | |
| S9223-1012143-001001LLL | 原始数据 | 案事件辅助支撑数据 | 一类支撑数据 | | |
| S9223-1012143-001002LLL | 原始数据 | 案事件辅助支撑数据 | 二类支撑数据 | | |
| S9223-1012143-001003LLL | 原始数据 | 案事件辅助支撑数据 | 三类支撑数据 | | |
| S9223—2000110-001001LLL | 资源数据 | 信息通报基础库 | 信息通报机构 | 地方通报机构 | |
| S9223—2000110-001002LLL | 资源数据 | 信息通报基础库 | 信息通报机构 | 技术支持单位 | |
| S9223—2000110-001003LLL | 资源数据 | 信息通报基础库 | 信息通报机构 | 成员单位 | |
| S9223—2000110-001004LLL | 资源数据 | 信息通报基础库 | 信息通报模版 | 威胁趋势通报模版 | |
| S9223—2000110-001005LLL | 资源数据 | 信息通报基础库 | 信息通报专家库 | 攻防技术专家 | |
| S9223—2000110-001006LLL | 资源数据 | 信息通报基础库 | 信息通报专家库 | 事件研判专家 | |
| S9223—2000110-001007LLL | 资源数据 | 信息通报基础库 | 信息通报专家库 | 数据分析专家 | |
| S9223—2000110-001008LLL | 资源数据 | 信息通报基础库 | 信息通报机构 | 其他专家 | |
| S9223—2000120-001001LLL | 资源数据 | 网络资产 | | | |
| S9223—2001110-001001LLL | 资源数据 | 等级保护基础库 | 重点保护目标 | 重点保护机构单位 | |
| S9223—2001110-001002LLL | 资源数据 | 等级保护基础库 | 重点保护对象（信息系统） | 一类支撑数据 | |
| S9223—2001110-001003LLL | 资源数据 | 等级保护基础库 | 重点保护对象（信息系统） | 二类支撑数据 | |
| S9223—2001110-001004LLL | 资源数据 | 等级保护基础库 | 重点保护对象（信息系统） | 三类支撑数据 | |
| S9223—2001110-001005LLL | 资源数据 | 等级保护基础库 | 重点保护资产 | | |

表 B.1（续）

| 代码 | 一级 | 二级 | 三级 | 四级 | 五级 |
|---|---|---|---|---|---|
| S9223—2001110-001006LLL | 资源数据 | 等级保护基础库 | 等级测评机构和人员 | | |
| S9223—2001110-001007LLL | 资源数据 | 等级保护基础库 | 等级保护专家库 | | |
| S9223—2001110-001008LLL | 资源数据 | 等级保护基础库 | 等级保护协调(领导)机构 | | |
| S9223—2001110-001009LLL | 资源数据 | 等级保护基础库 | 信息安全企业和人员 | | |
| S9223—2005341-001001LLL | 资源数据 | 网络安全事件类 | 有害程序事件 | | |
| S9223—2005341-001002LLL | 资源数据 | 网络安全事件类 | 网络攻击事件 | 仿冒钓鱼事件 | 一类相关数据 |
| S9223—2005341-001003LLL | 资源数据 | 网络安全事件类 | 网络攻击事件 | 仿冒钓鱼事件 | 二类相关数据 |
| S9223—2005341-001004LLL | 资源数据 | 网络安全事件类 | 网络攻击事件 | 后门控制事件 | 后门程序上传 |
| S9223—2005341-001005LLL | 资源数据 | 网络安全事件类 | 网络攻击事件 | 后门控制事件 | 后门回连 |
| S9223—2005341-001006LLL | 资源数据 | 网络安全事件类 | 信息破坏事件 | | |
| S9223—2005341-001007LLL | 资源数据 | 网络安全事件类 | 信息内容安全事件 | | |
| S9223—2005341-001008LLL | 资源数据 | 网络安全事件类 | 设备设施故障 | | |
| S9223—2005341-001009LLL | 资源数据 | 网络安全事件类 | 灾害性事件 | | |
| S9223—2005341-001010LLL | 资源数据 | 网络安全事件类 | 安全隐患事件 | | |
| S9223—2005341-001011LLL | 资源数据 | 网络安全事件类 | 其他 | | |
| S9223—2012111-001001LLL | 资源数据 | 案事件辅助支撑数据 | 一类支撑数据 | | |
| S9223—2012114-001001LLL | 资源数据 | 案事件辅助支撑数据 | 二类支撑数据 | | |
| S9223—2012114-001002LLL | 资源数据 | 案事件辅助支撑数据 | 三类支撑数据 | | |
| S9223—2012131-001001LLL | 资源数据 | 案事件辅助支撑数据 | 一类支撑数据 | | |

表 B.1（续）

| 代码 | 一级 | 二级 | 三级 | 四级 | 五级 |
|---|---|---|---|---|---|
| S9223—2012133-001001LLL | 资源数据 | 案事件辅助支撑数据 | 一类支撑数据 | | |
| S9223—2012133-001002LLL | 资源数据 | 案事件辅助支撑数据 | 二类支撑数据 | | |
| S9223—2012133-001003LLL | 资源数据 | 案事件辅助支撑数据 | 三类支撑数据 | | |
| S9223—2012134-001001LLL | 资源数据 | 案事件辅助支撑数据 | 一类支撑数据 | | |
| S9223—2012134-001002LLL | 资源数据 | 案事件辅助支撑数据 | 二类支撑数据 | | |
| S9223—2012134-001003LLL | 资源数据 | 案事件辅助支撑数据 | 三类支撑数据 | | |
| S9223—2012134-001004LLL | 资源数据 | 案事件辅助支撑数据 | 四类支撑数据 | | |
| S9223—2012213-001001LLL | 资源数据 | 案事件辅助支撑数据 | 一类支撑数据 | | |
| S9223—2012214-001001LLL | 资源数据 | 案事件辅助支撑数据 | 一类支撑数据 | | |
| S9223—2012343-001001LLL | 资源数据 | 案件库 | | | |
| S9223-3001303-001001LLL | 业务数据 | 等级保护业务 | 等级保护测评 | | |
| S9223-3001303-001002LLL | 业务数据 | 等级保护业务 | 网络安全执法检查 | | |
| S9223-3001303-001003LLL | 业务数据 | 等级保护业务 | 安全建设整改 | | |
| S9223-3003312-001001LLL | 业务数据 | 威胁态势 | 行业威胁情况 | | |
| S9223-3003312-001002LLL | 业务数据 | 威胁态势 | 重点保护目标威胁情况 | | |
| S9223-3003332-001WWWLLL | 业务数据 | 威胁态势 | 地区威胁情况 | | |
| S9223-3003342-001001LLL | 业务数据 | 威胁态势 | 热点事件分析 | | |
| S9223-3005342-001002LLL | 业务数据 | 信息通报 | 通报事件库 | 安全隐患/漏洞 | |
| S9223-3003342-001002LLL | 业务数据 | 信息通报 | 通报事件库 | 后门控制 | |

表 B.1（续）

| 代码 | 一级 | 二级 | 三级 | 四级 | 五级 |
| --- | --- | --- | --- | --- | --- |
| S9223-3005342-001003LLL | 业务数据 | 信息通报 | 通报事件库 | 网页篡改 | |
| S9223-3003342-001003LLL | 业务数据 | 信息通报 | 通报事件库 | 特定组织 | |
| S9223-3005342-001004LLL | 业务数据 | 信息通报 | 通报事件库 | 木马病毒 | |
| S9223-3003342-001004LLL | 业务数据 | 信息通报 | 通报事件库 | DDOS 攻击 | |
| S9223-3005342-001005LLL | 业务数据 | 信息通报 | 通报事件库 | 仿冒钓鱼 | |
| S9223-3003342-001005LLL | 业务数据 | 信息通报 | 通报事件库 | 暴力破解 | |
| S9223-3005342-001006LLL | 业务数据 | 信息通报 | 通报事件库 | 其他 | |
| S9223-3006000-SSSWWWLLL | 业务数据 | 信息通报 | 预警 | | |
| S9223-3007000-SSSWWWLLL | 业务数据 | 信息通报 | 处置 | | |
| S9223-3008000-SSSWWWLLL | 业务数据 | 攻防演习 | | | |
| S9223-3008000-SSSWWWLLL | 业务数据 | 网络安全大赛 | | | |
| S9223-3009110-001WWWLLL | 业务数据 | 重大活动安保 | 一类相关数据 | | |
| S9223-3009110-002WWWLLL | 业务数据 | 重大活动安保 | 二类相关数据 | | |
| S9223-3009110-003WWWLLL | 业务数据 | 重大活动安保 | 三类相关数据 | | |
| S9223-3009120-001WWWLLL | 业务数据 | 重大活动安保 | 一类相关数据 | | |
| S9223-3009120-002WWWLLL | 业务数据 | 重大活动安保 | 二类相关数据 | | |
| S9223-3009120-003WWWLLL | 业务数据 | 重大活动安保 | 三类相关数据 | | |
| S9223-3009142-001WWWLLL | 业务数据 | 重大活动安保 | 一类相关数据 | | |
| S9223-3009144-001WWWLLL | 业务数据 | 重大活动安保 | 一类相关数据 | | |

表 B.1（续）

| 代码 | 一级 | 二级 | 三级 | 四级 | 五级 |
|---|---|---|---|---|---|
| S9223-3010110-001WWWLLL | 业务数据 | 情报信息 | 一类相关数据 | | |
| S9223-3010120-002WWWLLL | 业务数据 | 情报信息 | 二类相关数据 | | |
| S9223-3010322-003001LLL | 业务数据 | 情报信息 | 攻击活动情报信息 | 一类支撑数据 | |
| S9223-3010322-003002LLL | 业务数据 | 情报信息 | 攻击活动情报信息 | 二类支撑数据 | |
| S9223-3010322-003003LLL | 业务数据 | 情报信息 | 攻击活动情报信息 | 三类支撑数据 | |
| S9223-3010322-003004LLL | 业务数据 | 情报信息 | 攻击活动情报信息 | 四类支撑数据 | |
| S9223-3010322-003005LLL | 业务数据 | 案事件线索 | 一类线索数据 | | |
| S9223-3010322-003006LLL | 业务数据 | 案事件线索 | 二类线索数据 | | |
| S9223-3014000-SSSWWWLLL | 业务数据 | 网络安全专项 | | | |
| S9223-4001120-001WWWLLL | 知识数据 | 信息安全产品 | | | |
| S9223-4005120-002001LLL | 知识数据 | 有害程序库 | 木马 | | |
| S9223-4005120-002002LLL | 知识数据 | 有害程序库 | 病毒 | | |
| S9223-4005120-003WWWLLL | 知识数据 | 漏洞库 | | | |
| S9223-4005120-004WWWLLL | 知识数据 | 恶意 IP 库 | | | |
| S9223-4005120-005WWWLLL | 知识数据 | 恶意域名库 | | | |
| S9223-4005120-006WWWLLL | 知识数据 | 其他知识库 | | | |
| S9223-4012120-001WWWLLL | 知识数据 | 案事件辅助支撑数据 | 一类支撑数据 | | |

# 附 录 C
（资料性附录）
标记标签样例

标记标签样例参见表 C.1。

**表 C.1 标记标签样例**

| 标签类别 | 标签样例 |
| --- | --- |
| 网络安全类目标签 | 资源（一级）、原始（一级）、知识（一级）、业务（一级）；<br>原始-网络流量（二级）、资源-网络日志（二级）、资源-网络安全事件（二级）、业务-信息通报（二级）；<br>资源-网络安全事件-网络攻击事件-后门控制事件-后门回连（五级） |
| 威胁攻击属性标签 | 广东省、北京市、上海市等；男、女 |
| 威胁攻击统计标签 | 中年、青年、少年；境外、境内；华北、华东、华南等；危害高、危害低等；影响范围一般、极广等 |
| 关联/关系标签 | 事件角色关系：仿冒钓鱼受害人、网站承载 IP、后门控制端、僵尸 C&C、域名注册关系等；<br>攻击组织关系：事件发起组织、发起嫌疑人、反华势力组织、协作关系等 |
| 场景标签 | 两会、奥运会、十九大、一带一路、金砖会议等 |
| 组合标签 | 北京市反攻黑客发起对保护目标的攻击；黑客爱好者对网站控制尝试 |

## 参 考 文 献

[1] GB/T 7027—2002 信息分类和编码的基本原则与方法
[2] GB/T 20529.2—2010 企业信息分类编码导则 第2部分:分类编码体系
[3] GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南
[4] GB/T 21062.3—2007 政务信息资源交换体系 第3部分:异构数据库接口规范
[5] GB/T 22239 信息安全技术 信息系统安全等级保护基本要求
[6] GB/T 28442—2012 导航电子地图数据分类与编码
[7] GB/T 32619—2016 政务服务中心信息公开编码规范
[8] GA/T 380 全国公安机关机构代码编制规则
[9] GA/T 2000.225—2017 公安信息代码 第225部分:资源服务总线行业门类代码
[10] DB 52/T 1123—2016 政府数据 数据分类分级指南
[11] ISO/IEC 29100:2011 Information technology—Security techniques—Privacy framework
[12] ISO/IEC 29151:2017 Information technology—Security techniques—Code of practice for personally identifiable information protection

中华人民共和国公共安全
行业标准
信息安全技术 网络安全事件通报预警
第3部分：数据分类编码与
标记标签体系技术规范
GA/T 1717.3—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址：www.spc.org.cn
服务热线：400-168-0010
2020年10月第一版
*
书号：155066·2-35545



GA/T 1717.3-2020