



中华人民共和国国家标准

GB/T 46902—2025

网络安全技术 网络空间安全图谱要素表示要求

Cybersecurity technology—Requirements for the representation of
elements of cyberspace security knowledge graph

2025-12-31 发布

2026-07-01 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 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 概述 2

6 网络空间安全图谱要素分类与代码 2

 6.1 要素分类 2

 6.2 分类方法 3

 6.3 编码原则 3

 6.4 编码方案 3

 6.5 要素分类与代码扩展 4

7 网络空间安全图谱要素图形符号表达 4

 7.1 符号设计 4

 7.2 符号使用方法 5

 7.3 要素图形符号 6

 7.4 要素符号扩展 6

附录 A（资料性） 网络空间安全图谱构建 7

 A.1 网络空间安全图谱概念与框架 7

 A.2 网络空间安全图谱要素生成 8

 A.3 网络空间安全知识图谱构建 8

 A.4 网络空间安全图谱构建 8

附录 B（规范性） 网络空间安全图谱要素分类、代码与图形符号 10

参考文献 32

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。

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：中国科学院地理科学与资源研究所、公安部第一研究所、中国科学院软件研究所、清华大学、三六零数字安全科技集团有限公司、奇安信科技集团股份有限公司、北京启明星辰信息安全技术有限公司、中国工商银行股份有限公司、国网思极网安科技(北京)有限公司、远江盛邦安全科技集团股份有限公司、杭州中尔网络科技有限公司、北京威努特技术有限公司、北京中科安维检测技术有限公司、工业和信息化部电子第五研究所、公安部第三研究所、中国人民公安大学、北京航空航天大学、北京理工大学、北京邮电大学、国投财务有限公司、北京圣博润高新技术股份有限公司。

本文件主要起草人：郭启全、江东、郝蒙蒙、胡光俊、陈帅、董继平、李海威、张海霞、孙东红、胡振泉、安锦程、蒋发群、苏建明、李姝、权晓文、吕萍、汪长雨、王春霞、苏峻锋、丁方宇、卓君、李坤、张静、彭媛媛、刘世明、范君、潘柱廷、王斯洁、焦彬、马强、孙磊、姜帆、李新征、刘海鹰、李阳普、石凌志、卢俊、付晶莹、林刚、柴思跃、陶源、杜彦辉、杨立群、郑军、郭三川、蒋蕊、李小川。

网络安全技术

网络空间安全图谱要素表示要求

1 范围

本文件规定了网络空间安全图谱要素分类、代码与图形符号表达。

本文件适用于网络安全监管者、行业主管者、网络运营者和网络服务提供者开展网络空间安全图谱构建和可视化表达。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络空间 cyberspace

网络、服务、系统、人员、过程、组织以及驻留或穿越其中的互联数字环境。

[来源:GB/T 25069—2022,3.622]

3.2

地理空间 geographic space

地球上具有一定位置和范围的空间区域,是地表各种自然要素和人文现象分布、组合及其相互关系的载体。

3.3

网络拓扑 network topology

用传输介质互连各种设备的物理布局,即构成网络的成员间特定的物理的或逻辑的排列方式。

3.4

知识图谱 knowledge graph

以结构化形式描述的知识元素及其联系的集合。

[来源:GB/T 42131—2022,3.6]

3.5

网络空间安全知识图谱 cyberspace security knowledge graph

在网络安全领域,基于地理环境、网络环境、行为主体和业务环境 4 类要素数据,通过知识建模、获取、融合、存储、推理、更新等步骤,提取实体、属性等关键元素并建立关联关系构建的知识图谱。

3.6

网络空间安全图谱 cyberspace security map

以数字化地理空间场景为载体,以网络空间安全知识图谱为基础,通过网络空间与地理空间映射,形成的包括地理底图、物理网络地图、逻辑网络地图以及各种应用场景图形的系列地图集合。

3.7

网络空间安全图谱要素符号 symbols of cyberspace security map elements

用于表达网络空间安全图谱要素,由形状、尺寸、定位、颜色等要素构成的图形符号。

3.8

依比例尺符号 scale-based symbols

地物依比例尺缩小后,其长度和宽度依比例尺表示的地物符号。

[来源:GB/T 20257.1—2017,3.1.1]

3.9

半依比例尺符号 semi-scale symbols

地物依比例尺缩小后,其长度依比例尺而宽度不能依比例尺表示的地物符号。

[来源:GB/T 20257.1—2017,3.1.2]

3.10

不依比例尺符号 non-scale symbols

地物依比例尺缩小后,其长度和宽度均不依比例尺表示的地物符号。

[来源:GB/T 20257.1—2017,3.1.3]

3.11

空间数据 spatial data

用来表示空间实体的位置、形状、大小和分布特征诸方面信息的数据。

注:用于描述所有呈二维、三维和多维分布的关于区域的现象。

[来源:GB/T 14911—2008,2.62]

3.12

图层 layer

具有相同空间特征和属性的对象及其属性的图形集合。



4 缩略语

下列缩略语适用于本文件。

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

IP:网际互连协议(Internet Protocol)

MAC:媒体访问控制(Media Access Control)

VPC:虚拟私有云(Virtual Private Cloud)

VPN:虚拟专用网络(Virtual Private Network)

5 概述

围绕人和组织、地理空间、网络空间(简称“人-地-网”)涉及的对象,将网络空间划分为地理环境层、网络环境层、行为主体层和业务环境层,这四个层为一级层。每个一级层包含若干二级要素,以此类推。利用图层将上述要素进行可视化表达,构建网络空间安全图谱。网络空间安全图谱构建见附录 A。

6 网络空间安全图谱要素分类与代码

6.1 要素分类

根据网络空间安全图谱的结构和特点,并结合网络安全业务需求,将网络空间安全图谱要素划分为

地理环境要素、网络环境要素、行为主体要素和业务环境要素 4 类。

- a) 地理环境要素: 各类网络空间要素依附的载体, 强调网络空间要素的地理属性, 包括基础地理信息和公共地理信息, 如网络基础设施和网络行为主体的地理位置、空间分布和区域特性。
- b) 网络环境要素: 各类网络空间要素形成的节点和链路, 分为物理环境和逻辑环境, 包含各种网络设备、网络应用、IP 地址、协议端口等。
- c) 行为主体要素: 在网络空间实施行为的各类角色, 包括网络安全监管者、行业主管者、网络运营者、网络使用者和网络服务提供者, 主要关注网络行为主体(实体角色或虚拟角色)的交互行为及其社会关系。
- d) 业务环境要素: 业务部门重点关注的业务对象(如保护目标、攻击者)和安全业务(如监测预警、情报信息)。

地理环境、网络环境、行为主体和业务环境 4 类要素之间相互联系、相互影响, 共同构成网络空间要素体系。

6.2 分类方法

网络空间安全图谱要素分类采用线分类法, 按照要素从属关系进行区分和归类, 建立 4 级分类体系, 依次为门类、大类、中类、小类。

- a) 门类的层级最高, 是第一层级; 大类是第二层级; 中类是第三层级; 小类是第四层级; 相同层级要素之间构成并列关系, 不同层级要素之间构成隶属关系; 同层级要素互不重复, 互不交叉。
- b) 门类共划分 4 类, 包括: 地理环境要素、网络环境要素、行为主体要素和业务环境要素。
- c) 大类共划分 11 类, 包括: 基础地理信息、公共地理信息; 物理环境、逻辑环境; 网络安全监管者、行业主管者、网络运营者、网络使用者、网络服务提供者; 业务对象、安全业务。

6.3 编码原则

在对网络空间安全图谱要素进行分类编码时, 遵循以下原则:

- a) 完备性: 网络空间安全图谱要素编码体系全面覆盖地理环境、网络环境、行为主体和业务环境中的各类要素;
- b) 唯一性: 在网络空间安全图谱要素编码体系中, 每个要素实例具有唯一的代码, 确保每个要素可被准确地标识和区分;
- c) 系统性: 各要素之间的编码类型和结构基本统一、协调一致, 以便建立一个完整的编码体系;
- d) 可扩展性: 要素编码结构考虑网络空间安全业务需求的变化和发展, 预留适当的后备容量, 能容纳未来可能出现的新要素。

6.4 编码方案

6.4.1 编码结构

参考 GB/T 7027—2002 中的编码方法, 将网络空间安全图谱要素进行区分和归类, 建立分类代码体系。网络空间安全图谱要素代码由 1 位大写英文字母和 7 位数字组成, 编码结构采用“-”作为间隔符。其结构如图 1 所示。

编码结构组成说明如下。

- a) 第一位表示门类, 采用一位大写字母标识: A 为地理环境要素, B 为网络环境要素, C 为行为主体要素, D 为业务环境要素。
- b) 第二、三位表示大类, 用两位数字 00~99 表示。
- c) 第四、五位表示中类, 用两位数字 00~99 表示, 其他类用 99 表示。

d) 第六至八位表示小类,用三位数字 000~999 表示,其他类用 999 表示。

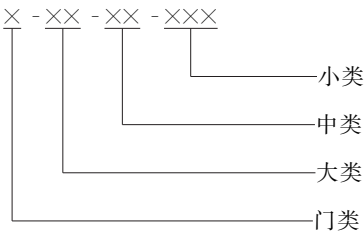


图 1 网络空间安全图谱要素编码结构

6.4.2 要素代码

网络空间安全图谱要素门类、大类代码应符合表 1 规定。有关门类、大类、中类和小类的详细分类、代码应符合附录 B 的要求。

表 1 网络空间安全图谱要素门类、大类代码表

序号	要素门类	要素大类	要素大类代码
1	地理环境要素(A)	基础地理信息	A-01
		公共地理信息	A-02
2	网络环境要素(B)	物理环境	B-01
		逻辑环境	B-02
3	行为主体要素(C)	网络监管者	C-01
		行业主管者	C-02
		网络运营者	C-03
		网络使用者	C-04
		网络服务提供者	C-05
4	业务环境要素(D)	业务对象	D-01
		安全业务	D-02

6.5 要素分类与代码扩展

当附录 B 提供的要素类型不能满足分类需要时,按以下原则扩展。

- a) 门类、大类不重新定义和扩展;中类、小类可根据需要进行扩展,但码位不扩展。
- b) 要素的中类、小类在同级别上进行扩展,扩展的中类和小类归入相应的大类和中类,同时在相关数据中说明。
- c) 扩展类型与代码符合 6.1、6.2、6.3、6.4 的规定。

7 网络空间安全图谱要素图形符号表达

7.1 符号设计

7.1.1 符号集合

依据网络空间安全图谱要素分类,网络空间安全图谱要素符号集合相应地划分为地理环境要素符

号集合、网络环境要素符号集合、行为主体要素符号集合和业务环境要素符号集合。

7.1.2 符号构成

7.1.2.1 符号的构成原则

符号的构成原则如下。

- a) 通用性原则：聚焦于网络空间安全图谱业务应用，对共性的网络资产、行为主体、案(事)件、单位、场所等进行图形符号设计时，突出其通用性。
- b) 系统性原则：反映同一类别网络空间安全图谱要素的特点，同一类符号的组合、延伸和扩展具有一致性和规律性。
- c) 准确性原则：符号的含义语义清晰、避免歧义。
- d) 简易性原则：力求以最简单的图形表达其含义。

7.1.2.2 符号的构成方法

符号的构成方法如下。

- a) 对大类、中类要素建立基础图形，基础图形宜采用象形、写意、几何等方法进行设计。
- b) 与中类关联性强的子类，在基础图形的基础上，叠加相应的文字或图形，组合成对应的符号。
组合方法如下：
基础图形 + [图形] 或 [文字] = 符号
- c) 其他子类要素按照大类、中类要素的符号设计方法进行设计。

7.2 符号使用方法

7.2.1 符号大小

符号大小的使用方法如下。

- a) 根据符号的不同类型、级别和地图比例尺大小合理确定符号大小。
- b) 在同一比例尺的地图上，同一性质(同类同级)的符号大小宜相同；不同性质的符号大小宜相称，如地图上级别高的符号要比级别低的符号大，代表实际对象大的符号通常要比代表实际对象小的符号大。

7.2.2 符号定位

符号定位的使用方法如下。

- a) 依比例尺的剖面状态符号，以其轮廓线定位。
- b) 半依比例尺的线状态符号，以其主线或中心线定位。
- c) 不依比例尺的点状态符号，定位点在其几何图形中心，基本规则为：
 - 1) 符号本身或其主体为规则几何体的，定位点在其几何重心；
 - 2) 符号主体为直线图形的，定位点在直线末端端点或其尾部交点；
 - 3) 符号下部为直角图形的，定位点在其直角顶点；
 - 4) 底部宽大的符号，定位点在图形底边的中点。

7.2.3 线型与线宽

线型与线宽的使用方法如下。

- a) 符号的线型宜根据符号的性质确定，表示实际情况或完成情况的符号，用实线标绘；表示预定或临时情况的符号，用虚线标绘。

- b) 符号的线宽宜根据符号的大小等比例变化,即符号标绘的值越大,构成符号的线就越宽。

7.2.4 文字注记

文字注记的使用方法如下。

- a) 文字注记宜从左到右直立注记。当文字注记写在符号内时,按符号方向注记。
- b) 依比例尺符号,文字注记宜写在符号内便于阅读的位置。
- c) 半依比例尺符号,文字注记宜以符号的上(右)方为第一注记位置,下(左)方为第二注记位置。
- d) 不依比例尺符号,文字注记宜以符号的右(上)方为第一注记位置,右(下)方为第二注记位置,左方为第三注记位置。
- e) 文字注记的字体宜使用字形美观、字体丰富的字库,同一类别或等级的符号注记使用同一字库的相同字体。

7.2.5 符号重叠处理

符号重叠处理的使用方法如下。

- a) 重要性高的符号压盖重要性低的符号。
- b) 不依比例尺标绘的符号压盖半依比例尺和依比例尺标绘的符号。
- c) 半依比例尺标绘的符号压盖依比例尺标绘的符号。

7.2.6 符号色彩

符号色彩不做规范性约束,宜遵照习惯性原则,并参考如下建议:

- a) 符号的颜色宜使用红色、黑色、蓝色和绿色,特殊需要时可加衬黄色和其他颜色;
- b) 表示党政机关、企事业单位及保护机构时宜使用红色。

7.3 要素图形符号

网络空间安全图谱要素图形符号应符合附录 B 的规定。

7.4 要素符号扩展

当附录 B 提供的要素图形符号不能满足需要时,按以下原则扩展:

- a) 新增符号按照 7.1 的方法进行设计,风格与已有同类别符号保持一致;
- b) 新增符号按照 6.5 的要求同步扩展要素分类及代码。

附录 A

(资料性)

网络空间安全图谱构建

A.1 网络空间安全图谱概念与框架

网络空间安全图谱是以数字化地理空间场景为载体,以网络空间安全知识图谱为基础,通过网络空间与地理空间映射,形成的包括地理底图、物理网络地图、逻辑网络地图以及各种应用场景图形的系列地图集合。其构建框架如图 A.1 所示,具体内容如下。

- a) 网络空间安全图谱要素生成:在附录 B 规定的要素分类的基础上,结合实际业务和应用场景构建网络空间安全要素指标体系,指导网络空间要素和地理空间要素的数据获取和数据集成。
- b) 网络空间安全知识图谱构建:基于知识图谱技术,分析网络空间安全数据的结构、类型、关系等,定义统一标准的本体模型,对 A.1a)中获取的多源异构数据进行关联融合,形成一张由节点和链接构成的语义网络,构建网络空间安全知识图谱,并以图数据库的形式进行存储。
- c) 网络空间安全图谱构建:按照附录 B 规定的要素图形符号,在地图上描述网络空间资源及其物质载体,并直观绘制和显示它们之间的相互联系,其丰富的属性信息可通过知识图谱的方式组织并进行可视化嵌入,最终形成多维度、多时序、多层级的网络空间安全图谱。

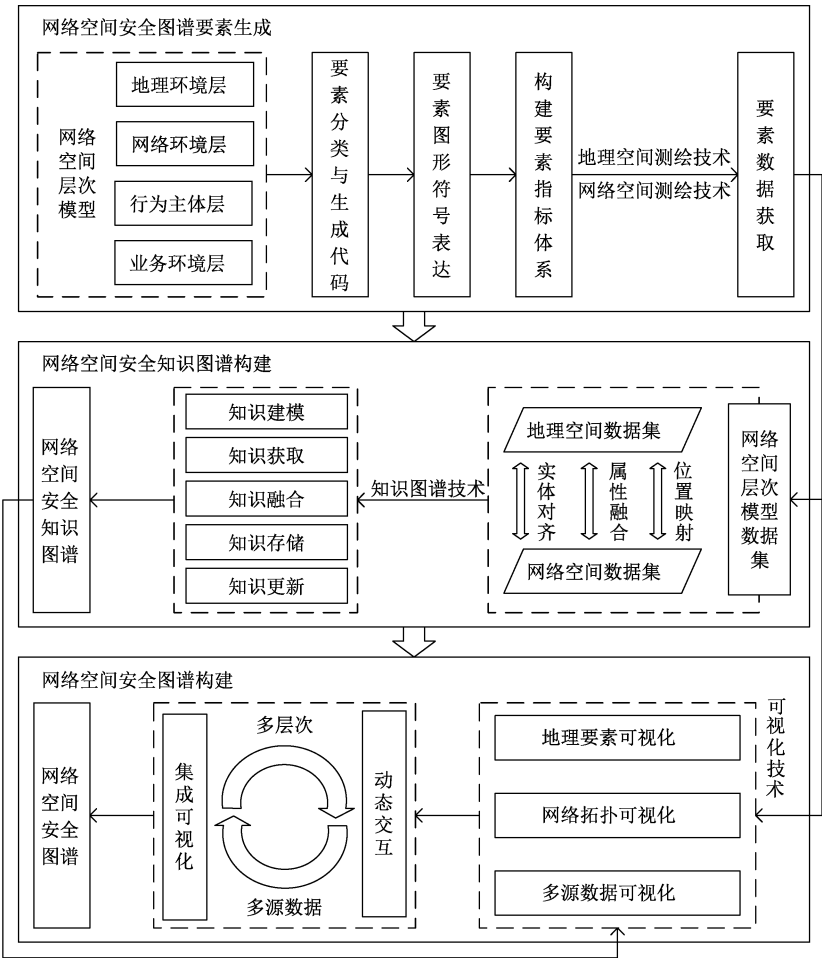


图 A.1 网络空间安全图谱构建框架

A.2 网络空间安全图谱要素生成

在网络空间安全图谱要素分类(见附录 B)的基础上,建立要素指标体系,利用地理空间测绘技术和网络空间测绘技术获取网络空间安全图谱所涉及的多源异构数据,并通过规范接口将其重新整合到统一框架下,构建地理空间数据集和网络空间数据集,为网络空间安全知识图谱构建提供数据基础。

其中,地理空间数据集涵盖具有位置信息的数据,包括地理环境层数据(如道路、建筑),网络环境层数据(如接入设备、交换设备),行为主体层数据(如网络监管者、网络使用者)和业务环境层数据(如关键信息基础设施)。这些数据以空间数据的形式存储在计算机中,是现实世界地理实体或现象在信息世界的映射,用于表达地理空间实体的位置、形状、分布、相互关系和变化规律等信息。

网络空间数据集中的数据来源于网络环境层、行为主体层和业务环境层,位置信息是连接网络空间与地理空间的纽带。其中,网络实体资源真实存在于物理空间中,具有典型的地理空间分布特征,可利用传统测绘、IP 地理定位等手段获取其地理位置,从而与地理空间进行关联。网络虚拟资源依赖于网络实体资源存在,可通过 IP 地址等信息对虚拟资源与实体资源建立关联,将网络虚拟资源映射到地理位置上。

A.3 网络空间安全知识图谱构建

面向网络空间安全防护、监测发现、通报预警、应急处置、追踪溯源、威胁情报等实际需求,基于地理环境、网络环境、行为主体和业务环境四类要素数据,通过知识建模、获取、融合、存储、推理、更新等步骤,提取实体、属性等关键知识元素并建立关联关系,构建网络空间安全领域的知识图谱。

具体而言,在获取网络空间安全图谱要素(见 A.2)后,利用命名实体识别、语义分析、实体对齐、属性融合等自然语言处理技术以及知识建模、知识获取、知识融合、知识存储、知识推理、知识更新等知识图谱技术,对地理环境要素数据(如地点、机构名称、经纬度等),网络环境要素数据(如资产、操作系统、IP 地址等),行为主体要素数据(如网络角色、人员信息等)以及业务环境要素数据(如漏洞、攻击、情报等)进行处理,建立实体之间的关系,实现各要素数据的关联和融合,构建网络空间安全知识图谱,为网络安全图谱构建提供领域知识和数据支撑。

A.4 网络空间安全图谱构建

网络空间安全图谱构建以数字化地理空间场景为本底,在网络空间安全知识图谱构建(见 A.3)的基础上,从网络空间安全知识图谱中提取网络资产、网络拓扑、网络安全事件等要素数据,将具有明确位置信息的要素展示到三维地图上,其他要素信息则以知识图谱、分析图表或统计图表等形式进行可视化。具体包括以下内容。

- a) 地理要素可视化:按照附录 B 规定的网络空间安全图谱要素分类、代码与图形符号,将地理要素及属性加载到地图上,实现地理要素可视化;在地理要素上图过程中,由于地图载负量有限,可采用分层分类、逐级下钻的形式进行表达与展示。
- b) 网络拓扑可视化:从网络空间安全知识图谱中抽取与地理位置有关的要素,将这些要素之间的逻辑关系转化为拓扑关系,实现网络要素之间的关系映射;在此基础上,通过网络空间和地理空间的多尺度拓扑关联,实现网络拓扑空间化;最后,按照附录 B 规定的要素分类、代码与图形符号,实现网络拓扑可视化。
- c) 多源数据可视化:对于已映射到地理空间的要素,从知识图谱中提取出与之相关的数据,作为该要素的属性或附加信息,以子图谱的形式进行可视化展示;对于其他未映射到地理空间的要素,选择合适的可视化方式(如柱状图、折线图、雷达图等)或直接使用附录 B 中的图形符号

进行展示。

- d) 多层次集成可视化:将地理要素、三维模型、网络拓扑、知识图谱、动态图表等以可视化形式进行集成,形成多层次集成可视化的网络空间安全图谱,以提供对网络空间的直观感知,为网络空间资源管理及网络安全综合防控体系建设提供支持。

附 录 B
(规范性)

网络空间安全图谱要素分类、代码与图形符号

网络空间安全图谱的要素分类、代码与图形符号应符合表 B.1 的规定。

表 B.1 网络空间安全图谱要素分类、代码与图形符号

要素门类	要素大类	要素中类	要素小类	图形符号样式
地理环境要素 A				
	基础地理信息 A-01			
		境界与政区 A-01-01		
			国家行政区界限 A-01-01-001	 (见 GB/T 24354—2023, G.2.1.2.1)
			省级行政区界限 A-01-01-002	 (见 GB/T 24354—2023, G.2.2.1)
			地级行政区界限 A-01-01-003	 (见 GB/T 24354—2023, G.2.2.3)
			县级行政区界限 A-01-01-004	 (见 GB/T 24354—2023, G.2.2.4)
			乡镇(街道)级界限 A-01-01-005	 (见 GB/T 24354—2023, G.2.2.5)
		道路交通 A-01-02		

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）


要素门类	要素大类	要素中类	要素小类	图形符号样式
			铁路 A-01-02-001	 (见 GB/T 24354—2023， A.1.1.1)
			公路 A-01-02-002	 (见 GB/T 24354—2023， A.1.2.1)
		水系 A-01-03		
			河流 A-01-03-001	 (见 GB/T 24354—2023， G.4.2.1)
			湖泊 A-01-03-002	 (见 GB/T 24354—2023， G.4.2.4)
			水库 A-01-03-003	 (见 GB/T 24354—2023， G.4.2.6)
	公共地理信息 A-02			
		餐饮住宿 A-02-01		
		体育健身 A-02-02		
		地产小区 A-02-03		

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
		购物娱乐 A-02-04		
		生活服务 A-02-05		
		医疗卫生 A-02-06		
		社会福利 A-02-07		
		旅游景点 A-02-08		
		政府机构 A-02-09		
		科研教育 A-02-10		
		交通设施 A-02-11		
		金融行业 A-02-12		
		公司企业 A-02-13		
		公共设施 A-02-14		

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
网络环境要素 B				
	物理环境 B-01			
		交换设备 B-01-01		
			路由器 B-01-01-001	
			交换机 B-01-01-002	
			无线通信技术 B-01-01-003	
			基站 B-01-01-004	
			卫星 B-01-01-005	
		接入设备 B-01-02		
			固网接入设备 B-01-02-001	
			移动接入设备 B-01-02-002	

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
			物联/工控接入设备 B-01-02-003	
		网络安全设备 B-01-03		
			防火墙 B-01-03-001	
			防病毒网关 B-01-03-02	
			漏洞扫描器 B-01-03-003	
			安全网络存储 B-01-03-004	
			公钥基础设施 B-01-03-005	
			网络安全管理平台 B-01-03-006	
			入侵检测系统 B-01-03-007	
			入侵防御系统 B-01-03-008	
			安全数据库系统 B-01-03-009	

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
			安全操作系统 B-01-03-010	
			USB 移动存储介质 管理系统 B-01-03-011	
			网络脆弱性 扫描产品 B-01-03-012	
			网络型流量控制产品 B-01-03-013	
			网络和终端隔离产品 B-01-03-014	
			网络安全审计产品 B-01-03-015	
			网站数据恢复产品 B-01-03-016	
			网络安全态势感知 产品 B-01-03-017	
			统一威胁管理产品 B-01-03-018	
			反垃圾邮件产品 B-01-03-019	
			信息过滤产品 B-01-03-020	

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
			病毒防治产品 B-01-03-021	
			抗拒绝服务攻击产品 B-01-03-022	
			负载均衡产品 B-01-03-023	
			文件加密产品 B-01-03-024	
			终端接入控制产品 B-01-03-025	
			终端安全监测产品 B-01-03-026	
			身份鉴别产品 B-01-03-027	
			安全配置检查产品 B-01-03-028	
			运维安全管理产品 B-01-03-029	
			日志分析产品 B-01-03-030	
			电子文档安全管理产品 B-01-03-031	

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
			安全基线系统 B-01-03-032	
			移动终端安全管理系统 B-01-03-033	
			诱捕蜜罐系统 B-01-03-034	
			主机安全加固系统 B-01-03-035	
			桌面终端管理系统 B-01-03-036	
			情报系统 B-01-03-037	
			边界安全集中管控 B-01-03-038	
			网络安全隔离装置 B-01-03-039	
			网络动态应用保护 B-01-03-040	
			网络攻击拦截 B-01-03-041	
			网页防篡改 B-01-03-042	

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
			威胁监测探针 B-01-03-043	
			安全编排 B-01-03-044	
			IP 封禁 B-01-03-045	
			资产准入 B-01-03-046	
			WEB 应用防护 B-01-03-047	
			物联终端安全管理 模块 B-01-03-048	
			移动 APP 加固软件 B-01-03-049	
			加密流量解析 B-01-03-050	
			高级威胁检测 B-01-03-051	
			病毒风险治理 B-01-03-052	
			域名安全监测 B-01-03-053	



表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
			违规外联监测 B-01-03-054	
			未备案网站监测 B-01-03-055	
			病毒感染分析 B-01-03-056	
			攻击溯源分析 B-01-03-057	
			全流量分析 B-01-03-058	
			物联终端行为分析 B-01-03-059	
			安全策略管理 B-01-03-060	
			供应链安全管理 B-01-03-061	
			漏洞补丁管理 B-01-03-062	
			上网行为管理 B-01-03-063	
			其他网络安全产品 B-01-03-999	

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
		数据安全产品 B-01-04		
			数据安全管理类产品 B-01-04-001	
			数据安全防护类产品 B-01-04-002	
			数据安全合规类产品 B-01-04-003	
			其他数据安全产品 B-01-04-999	
		操作系统 B-01-04		
		网络应用 B-01-05		
			网络服务 B-01-05-001	
			应用软件 B-01-05-002	
		传输介质 B-01-06		
		信息通信技术 基础设施 B-01-07		

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
			数据中心 B-01-07-001	
			云计算中心 B-01-07-002	
			边缘计算中心 B-01-07-003	
			区块链网络 B-01-07-004	
			卫星网络 B-01-07-005	
			其他 B-01-07-999	
	逻辑环境 B-02			
		逻辑链路 B-02-01		
			网络对象 B-02-01-001	
			IP 地址 B-02-01-002	
			域名 B-02-01-003	

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
			数字证书 B-02-01-004	
			协议 B-02-01-005	
			端口 B-02-01-006	
			网段 B-02-01-007	
			MAC 地址 B-02-01-008	
		虚拟网络 B-02-02		
			VPN B-02-02-001	
			VPC B-02-02-002	
			安全组 B-02-02-003	
行为主体要素 C				
	网络监管者 C-01			

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
	行业主管者 C-02			
	网络运营者 C-03			
		网络所有者 C-03-01		
		网络管理者 C-03-02		
	网络使用者 C-04			
		网络角色 C-04-01		
			网络用户账号 C-04-01-001	
			网络用户邮箱 C-04-01-002	
			网络用户认证信息 C-04-01-003	
			虚拟人/数智人 C-04-01-004	
			其他网络身份 C-04-01-999	

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
		实体角色 C-04-02		
			组织信息 C-04-02-001	
			人员信息 C-04-02-002	
	网络服务提供者 C-05			
		网络接入服务提供者 C-05-01		
		网络平台服务提供者 C-05-02		
		网络产品服务提供者 C-05-03		
		网络安全服务提供者 C-05-04		
			互联网企业 C-05-04-001	
			网络安全企业 C-05-04-002	
			网络安全研究机构 C-05-04-003	

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
			网络安全检测机构 C-05-04-004	
			网络安全咨询机构 C-05-04-005	
			网络安全管理专家 C-05-04-006	
			网络安全技术专家 C-05-04-007	
			网络安全技术服务人员 C-05-04-008	
业务环境要素 D				
	业务对象 D-01			
		保护对象 D-01-01		
			保护机构 D-01-01-001	
			保护资产 D-01-01-002	
			个人信息 D-01-01-003	

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
		关键信息基础设施 D-01-02		
			公共通信和信息服 务基础设施 D-01-02-001	
			能源基础设施 D-01-02-002	
			交通基础设施 D-01-02-003	
			水利基础设施 D-01-02-004	
			金融基础设施 D-01-02-005	
			公共服务基础设施 D-01-02-006	
			电子政务基础设施 D-01-02-007	
			国防科技工业基础 设施 D-01-02-008	
			其他重大基础设施 D-01-02-999	
		数据 D-01-03		

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
			一般数据 D-01-03-001	
			重要数据 D-01-03-002	
			核心数据 D-01-03-003	
		网络安全漏洞 D-01-04		
			超危漏洞 D-01-04-001	
			高危漏洞 D-01-04-002	
			中危漏洞 D-01-04-003	
			低危漏洞 D-01-04-004	
		攻击者 D-01-05		
			黑客 D-01-05-001	
			APT 组织 D-01-05-002	

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
			网军 D-01-05-003	
			网络恐怖分子 D-01-05-004	
			内部威胁者 D-01-05-005	
			业余爱好者 D-01-05-006	
			其他 D-01-05-999	
		攻击目标 D-01-06		
		攻击时间 D-01-07		
		攻击工具 D-01-08		
		攻击装备 D-01-09		
		攻击武器 D-01-10		
		攻击技术 D-01-11		





表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
		攻击谋略 D-01-12		
		攻击方法 D-01-13		
		攻击组织 D-01-14		
		攻击个体 D-01-15		
		攻击者位置 D-01-16		
		攻击危害程度 D-01-17		
	安全业务 D-02			
		保护 D-02-01		
			网络安全等级保护 D-02-01-001	
			关键信息基础设施 安全保护 D-02-01-002	
			数据安全保护 D-02-01-003	

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
			网络安全监测预警 D-02-01-004	
			网络安全威胁态势 D-02-01-005	
			网络安全信息通报 D-02-01-006	
			网络安全应急处置 D-02-01-007	
			网络安全检测评估 D-02-01-008	
			比武竞赛 D-02-01-009	
			技术对抗 D-02-01-010	
			供应链安全 D-02-01-011	
			网络安全审查 D-02-01-012	
			网络安全知识库 D-02-02-013	
			重大活动安保 D-02-02-014	

表 B.1 网络空间安全图谱要素分类、代码与图形符号（续）

要素门类	要素大类	要素中类	要素小类	图形符号样式
			网络安全专项 D-02-02-015	
		保卫 D-02-02		
			威胁情报 D-02-02-001	
			执法调查 D-02-02-002	



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 13923—2022 基础地理信息要素分类与代码
 - [3] GB/T 14911—2008 测绘基本术语
 - [4] GB/T 20257.1—2017 国家基本比例尺地图图式 第1部分:1:500 1:1 000 1:2 000
地形图图式
 - [5] GB/T 20986—2023 信息安全技术 网络安全事件分类分级指南
 - [6] GB/T 23707—2009 地理信息 空间模式
 - [7] GB/T 24354—2023 公共地理信息通用地图符号
 - [8] GB/T 25066—2020 信息安全技术 信息安全产品类别与代码
 - [9] GB/T 25069—2022 信息安全技术 术语
 - [10] GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南
 - [11] GB/T 42131—2022 人工智能 知识图谱技术框架
 - [12] GA/T 492—2004 城市警用地理信息图形符号
-



