ICS 35.030
CCS L80

团 体 标 准

T/COSOCC 017—2024

信息安全技术 关键信息基础设施安全监测预警产品技术要求

Information security technology--Technical requirements for critical information infrastructure security monitoring and warning products

2024－05－31 发布　　2024－05－31 实施

中国基本建设优化研究会　　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。

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。

本文件由中国基本建设优化研究会提出并归口。

本文件起草单位：公安部第一研究所、北京北信源软件股份有限公司、安芯网盾（北京）科技有限公司、网络通信与安全紫金山实验室、联通数字科技有限公司、北京浩瀚深度信息技术股份有限公司、重庆梦之想科技有限责任公司、北京网藤科技有限公司、北京边界无限科技有限公司、北京马赫谷科技有限公司、北京万里红科技有限公司、福建金瑞信息技术有限公司、广西南宁英福泰科信息科技有限公司、北京赛博昆仑科技有限公司、湖南省封匠网安信息技术有限公司、中科信安（深圳）信息技术有限公司、湖北省楚天云有限公司、杭州领信数科信息技术有限公司、杭州中电安科现代科技有限公司、上海交通大学、北京华成航泰科技发展有限公司、麒麟软件有限公司、北京滴普科技有限公司、江苏蓝创智能科技股份有限公司、拓尔思天行网安信息技术有限责任公司、广东盈世计算机科技有限公司、浙江飞图影像科技有限公司、牙木科技股份有限公司、成都开元精创信息技术有限公司、北京通州网络安全产业园运营管理有限公司、广州天懋信息系统股份有限公司、北京中超伟业信息安全技术股份有限公司、维纳尔（北京）环保科技服务有限公司、中移（杭州）信息技术有限公司、蓝象标准（北京）科技有限公司、嵩嘉标准化技术服务（北京）有限公司。

本文件主要起草人：王奕钧、杨华、姚纪卫、蔡翰智、张建荣、张增波、孟涛、庞韶敏、朱东民、王智明、李斌、陈佩文、涂卫华、江海昇、魏杰、张昇鹏、郑文彬、邓庭波、杨旭东、张晓枫、张晓婷、武方、李建华、霍进彦、张大朋、李畅、黄青蓝、许芬、郝家雨、伍华樑、李文军、范子全、边梦娜、邹凯、罗远哲、张立明、历伟、张风雷、陈维、吴晗、乔华阳、熊凡凡、姜冰、张红艳、邱天、张德保、段小莉。

引　　言

为落实《中华人民共和国网络安全法》、《关键信息基础设施安全保护条例》关于保护关键信息基础设施运行安全的要求，在国家网络安全等级保护制度以及GB/T 39204《信息安全技术 关键信息基础设施安全保护要求》的基础上，本文件借鉴我国相关部门以及网络安全企业在开展安全监测预警工作的成熟经验，并吸纳国内外在关键信息基础设施监测、保护和预警方面的举措，结合我国实际情况，满足关键信息基础设施的安全诉求，提升关键信息基础设施的安全保护能力，提出关键信息基础设施安全监测预警产品技术要求，采取必要措施保护我国关键信息基础设施业务的正常运行和不受破坏。

信息安全技术 关键信息基础设施安全监测预警产品技术要求

1 范围

本文件规定了关键信息基础设施安全监测预警产品的功能要求、安全要求和保障要求。

本文件适用于关键信息基础设施产品提供者进行产品的设计和研发,可以用于第一方测评(自评价)或第二方测评(甲方评价),以及指导产品测评,也可供产品使用者参考。

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 20986 信息安全技术 网络安全事件分类分级指南

GB/T 25069 信息安全技术 术语

GB/T 31509 信息安全技术 信息安全风险评估实施指南

GB/T 36633 信息安全技术 网络用户身份鉴别技术指南

GB/T 39204 信息安全技术 关键信息基础设施安全保护要求

3 术语和定义

GB/T 20986、GB/T 25069、GB/T 39204界定的以及下列术语和定义适用于本文件。

3.1

关键信息基础设施 critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域,以及其他一旦遭到破坏、丧失功能或者数据泄露,可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

[来源:GB/T 39204—2022,3.1]

3.2

网络安全事件 network security incident

由于人为原因、网络遭受攻击、网络存在漏洞隐患、软硬件缺陷或故障、不可抗力因素,对关键信息基础设施的网络和信息系统的数据和业务应用造成危害,对国家、社会、经济造成负面影响的事件。

[来源:GB/T 20986—2023,3.4,有修改]

3.3

威胁信息 threat information

基于证据的知识,用于描述现有或可能出现的威胁,从而实现对威胁的响应和预防。

注:威胁信息包括上下文、攻击机制、攻击指标、可能影响等信息。

[来源:GB/T 42453—2023,3.2]

4 缩略语

下列缩略语适用于本文件。

IP:网际互连协议(Internet Protocol)

IPS:入侵防御系统(Intrusion Prevention System)

URC:统一资源定位系统(uniform resource locator)

WAF:Web应用防火墙(Web Application Firewall)

5 概述

关键信息基础设施安全监测预警技术架构见图1。关键信息基础设施安全监测预警产品安全监测依据业务需要对关键信息基础设施网络或系统等监测预警对象进行信息监测，监测数据用户后续分析；基于风险分析关联识别以及和溯源画像技术对获取到的监测数据（数据字段格式见附录A）进行解析与研判等处理，发现和评估安全事件（网络安全事件编号编码规则见附录B和附录C）和安全风险；预警通报基于设定的预警规则进行及时准确预警，便于后续应急处置；态势展示根据应用场景调用相关数据进行多维度评估和展示，包括整体态势和专题态势；最后通过预警通报关联处置安全威胁；应用隐身保护通过可信终端对应用进行隐身保护，保障关键信息基础设施的安全运行；系统管理主要进行软硬件管理、系统升级、规则升级、系统自检、系统配置备份及回退等。监测预警产品运行环境要求见附录D。

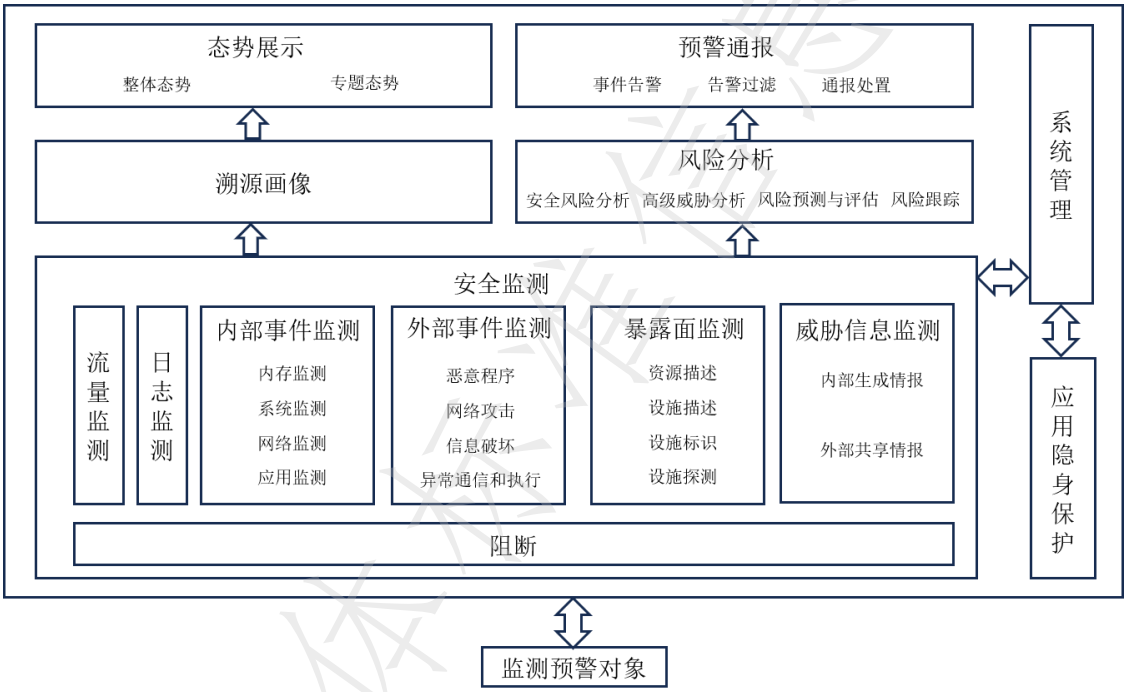

图1 关键信息基础设施安全监测预警技术架构

6 功能要求

6.1 网络部署

网络部署功能应符合以下要求：

a) 在网络边界、网络出入口等网络关键节点部署，支持串联与旁路部署方式，支持单机和分布式部署，支持 channel、trunk 等接口模式，并支持 802.1Q 等网络环境；

b) 支持管理口、镜像口、阻断口及业务口分离部署。

6.2 安全监测

6.2.1 流量监测

流量监测功能支持串联与旁路部署情况下，对流量进行实时监测，应符合以下要求：

a) 支持监测关键信息基础设施的流量报文，支持流量元数据、过程特性分析软件包（pcap）、网络监测功能（netflow）等方式的采集、存储和转发；

b) 支持监测、解析和还原指定的 IP 地址；

c) 支持对不同协议进行监测、解析的能力。

6.2.2 日志监测

日志监测功能应符合以下要求：

a) 支持监测关键信息基础设施的设备和系统日志，支持系统日志（SYSLOG）、镜像等日志采集方式，实时采集设备及系统日志；
b) 支持监测系统、安全、审计、应用程序等日志文件。

6.2.3 内部事件监测

内部事件监测功能应符合以下要求：

a) 支持监测主机内存异常行为，包括但不限于恶意程序检测等行为；
b) 支持监测系统访问行为，包括但不限于文件的读、写、重命名、删除等行为；
c) 支持监测系统入侵行为，包括环境变量劫持等篡改劫持行为，非法外联、暴力破解、隐藏进程等风险行为，异常登录、端口复用等远程控制行为；
d) 支持监测网络攻击行为，包括命令控制（C&C）通讯和数据库可用性组（DGA）域名检测，发现隐蔽通道和窃取数据行为；
e) 支持监测应用入侵行为，包括结构化查询语言（SQL）数据库注入攻击、内存马注入攻击、跨站脚本攻击（XSS）、反序列化攻击、表达式注入攻击、请求伪造、信息窃取等事件；
f) 支持监测应用服务异常行为，包括进程异常关闭、应用服务端口异常等问题。

6.2.4 外部事件监测

系统外部事件监测功能应符合以下要求：

a) 能满足识别和发现攻击行为，包括但不限于以下方式：
   1) 支持监测恶意程序事件，包括但不限于计算机病毒、蠕虫、木马等；
   2) 支持监测网络攻击事件，包括但不限于拒绝服务攻击、后门攻击、漏洞利用攻击、网络钓鱼等；
   3) 支持监测信息破坏事件，包括但不限于信息篡改、信息假冒、信息泄露、信息窃取等；
b) 能满足识别和发现异常通信和执行行为，包括不限于挖矿程序、外联程序、域名系统（DNS）隧道等。

6.2.5 暴露面监测

暴露面监测功能应符合以下要求：

a) 支持监测关键信息基础设施的设备、系统、服务、应用等指纹信息；
b) 支持监测关键信息基础设施的网络资源等信息，包括 IP、端口、协议、应用等；
c) 支持监测关键信息基础设施设备、系统、应用的安全漏洞，及时通报，闭环处置；
d) 支持监测关键信息基础设施资产的合规性，包括重要 IP 资源离线监测、禁用软件监测、禁用端口监测、禁用服务监测等。

6.2.6 威胁信息监测

威胁信息监测功能应符合以下要求：

a) 具备监测威胁信息的能力：
   1) 支持威胁信息的内部生成，支持基于 WAF、IPS、语义检测、上下文分析等引擎至少四类，实时监测生成威胁信息数据；
   2) 支持威胁信息的外部共享，支持接入第三方威胁信息源和自定义威胁信息源的能力；
   3) 支持监测多源威胁信息，包括但不限于正向攻击威胁信息源、受控外联威胁信息源、IP 画像威胁信息源以及自定义威胁信息源等类型，应支持 ipv6 格式的威胁信息数据；
b) 具备威胁情报集成能力，整合多源威胁情报源，实时比对网络活动与已知攻击特征、恶意 IP、域名和 URL 等，提高识别精度；
c) 具备威胁信息联防联控的能力，包括旁路阻断能力，与 WAF 引擎、IPS 引擎等至少两类引擎的联动防控能力、事件与预警的共享能力。

6.2.7 阻断

阻断应符合以下要求：

a） 支持自动阻断异常访问行为和人工研判攻击阻断方式；

b） 支持阻断策略和范围配置，至少包含 IP、网段等。

6.3 应用隐身保护

应用隐身保护应符合以下要求：

a） 支持通过授权可信终端对应用进行隐身保护；

b） 具备对重要数据采取国密等算法加密和校验机制保障数据的机密性和完整性功能。

6.4 溯源画像

支持对网络安全事件的自动回溯画像，应符合以下要求：

a） 支持基础属性画像，至少包括 IP 地址、归属地、运营商、威胁等级、活跃度、经纬度等属性；

b） 支持资产属性画像，至少包含资产标签、组件标签、开放端口等属性；

c） 支持对安全事件进行跟踪管理，支持攻击轨迹溯源，能够对安全事件进行反追踪，攻击轨迹溯源时间不少于三个月，内容至少包含历史攻击单位、攻击类型、被攻击单位所属行业等属性。

6.5 风险分析

6.5.1 安全风险分析

应具备安全风险分析能力，包括网络安全事件分析、威胁分析、暴露面分析、运行状态分析、策略与配置分析等。按照GB/T 31509威胁调查要求分析威胁发生的可能性和影响程度，按照GB/T 31509中的风险分析模型和风险分析方法要求计算信息安全风险值。

6.5.2 高级威胁分析

应具备高级威胁分析能力，能识别、分析不同类别的网络攻击行为，包括但不限于攻击属性、攻击路径、建立攻击画像等高级威胁分析。

6.5.3 风险预测及评估

风险预测及评估应符合以下要求：

a） 支持对关键信息基础设施目前状态后续安全、安全运维等趋势的预测；

b） 支持对关键信息基础设施目前状态的评估。

6.5.4 风险跟踪

应支持对系统的安全风险（应用漏洞、系统漏洞、风险端口、恶意代码等）进行安全评估，实时掌握业务系统风险状况，支持业务系统变更时，自动重新进行安全评估。

6.6 态势展示

6.6.1 整体态势展示

应支持按照时间、类型、应用场景等维度对网络的整体或局部网络安全状况进行评估和展示，应展示网络安全状况变化趋势，应支持采用多种视图进行网络安全态势的展示。

6.6.2 专题态势展示

应支持资产态势、流量态势、攻击态势、运行态势、脆弱性态势、安全事件态势和异常行为态势等的展示。

6.7 预警通报

6.7.1 事件预警

事件预警应符合以下要求：

a） 支持时间预警机制，预警方式包括但不限于实时提示、邮件短信通知、声音及闪光预警等；

b) 支持基于监测和数据分析结果等进行分级别预警，预警分级应符合 GB/T 20986 中事件类别和分级方法的要求；
c) 支持以实时和统计的方式对安全预警进行展现，支持对预警进行处置派发及状态跟踪，及时自动更新预警状态；
d) 支持根据预警级别和预警流程发布预警信息，预警信息包括但不限于预警类型、预警级别、事件类型、威胁方式、涉及对象、处置动作等。

6.7.2 预警过滤

应具备安全、运维及管理人员定义安全策略，对关键信息基础设施中的指定事件不予预警，支持对高频度发生的相同或同类安全事件进行合并预警，避免出现预警风暴。

6.7.3 通报处置

应具备安全、运维及管理人员定义通报处置策略，对关键信息基础设施中的行为和事件定制处置方式，例如人工配置防火墙黑名单、联动安全编排自动化与响应（SOAR）通知防火墙封控拦截等策略。

6.8 系统管理

系统管理应符合以下要求：
a) 提供产品软硬件管理和配置图形化界面，支持系统及配置的备份及回退；
b) 具备独立的控制台，支持系统、补丁、规则库等在线升级，支持产品管理、自检、故障恢复等功能。

7 安全要求

7.1 身份标识与鉴别

身份标识应具有唯一性，产品应具备对用户身份的鉴别功能，用户请求执行任何操作前，对每个授权用户进行唯一的身份鉴别，身份鉴别应符合GB/T 36633中身份鉴别主要过程要求。

7.2 授权与访问控制

授权与访问控制应符合以下要求：
a) 支持区分系统管理员、安全管理员和审计管理员等角色；
b) 支持对安全角色进行维护，并将用户和角色相关联；
c) 具备对用户访问权限控制功能，保障权限的最小化原则，具备用户登录超时退出、锁定机制；
d) 支持 IP 黑白名单及访问控制策略配置，支持按照时间设定生效周期。

7.3 通信安全

通信安全应符合以下要求：
a) 各系统及子系统、组件应使用符合国家密码管理相关规定的密码算法套件；
b) 具备通信安全能力，保证传输通道的安全性，保障数据的机密性、完整性和可用性。

7.4 系统平台安全

系统平台安全应符合以下要求：
a) 具备时间同步功能，每天应至少同步一次；
b) 具备升级回滚机制；
c) 具备安全策略配置功能，应提供默认的策略，支持策略的编辑、修改和导入、导出；
d) 具备全生命周期的管理能力。

7.5 日志记录与审计

应具备日志记录与审计管理功能，具备针对检测、分析、防御等过程中产生的各类日志和数据的日志审计能力，具备对用户行为操作的日志审计能力，日志中包含具体时间、日志类别及描述等信息，用户可将日志导出，以便保存、查阅。

8 保障要求

8.1 设计与开发

开发者应为产品的不同版本提供唯一的标识。制定和实施关键信息基础设施安全监测预警产品开发流程，应提供产品安全功能的安全架构描述，提供完备的功能规格说明、产品设计文档。对设计文档、开发文档等进行配置管理，能识别产品在设计、开发环节的安全风险，采取安全措施保障产品的设计和开发安全。自行、联合或委托第三方对产品进行安全测试，对已发现的安全缺陷、漏洞进行修复，制定并实施在用户侧进行紧急修复的安全管理流程。开发者应提供测试覆盖文档、测试深度的分析文档，应测试关键信息基础设施安全监测预警产品功能，将结果文档化并提供功能测试文档。提供设计与实现之间的对应关系，并证明其一致性。

8.2 生产和交付

应建立和实施规范的产品生产和服务交付流程，采取完整性保护措施降低产品交付过程中的篡改风险，并将交付过程文档化，为用户提供操作指南等指导性文件，包含对每一种用户角色的描述，用来说明产品的安装、生成、启动等操作过程，给出风险提示和应急相应措施。

8.3 运行与维护

应建立和执行针对产品在运行和维护阶段的应急响应机制和流程，并提供必要的技术支持，为产品提供持续的安全维护。

附 录 A

（资料性）

数据字段格式及说明

A.1. 数据字段的数据类型的取值说明

本文件网络安全事件分类分级和网络数据重要程度参照GB/T 20986。本文遵照此分类分级原则，根据网络安全管理工作实际需要，界定各类网络安全事件信息报送时的基本内容和格式规范。

各类数据字段的数据类型的取值说明见表A.1。

A.1. 数据类型的取值

序号	数据元值的类型	说明
1	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。
2	数值型（numeric）	用任意实数表达的数据元值的类型。
3	日期型（date）	通过YYYYMMDD的形式表达的值的类型，符合GB/T 7408。
4	日期时间型（datetime）	通过YYYYMMDDhh24mmss的形式表达的值的类型，符合GB/T 7408。
5	时间戳（timestamp）	通过YYYYMMDDhh24mmss.xxxxxxxxx的形式表达的值的类型
6	时间型(time)	通过hhmmss的形式表达的值的类型，符合GB/T 7408。
7	布尔型（boolean）	两个且只有两个表明条件的值，如on/off、true/false。
8	数组型（array）	数组是一系列类似数据的集合，数组实体包含两项：键名和值，

9	对象型（object）	对象数据类型，对象中存放实例字段的数据。如：
		{
		"object":{
		"name":"object",
		"comment":"object"
		}
		}

10	二进制型（binary）	上述无法表示的其他数据类型，比如图像、音频等。

A.2. 监测预警数据格式通用部分字段说明

监测预警数据格式通用部分字段说明见表A.2：

A.2. 监测预警数据格式通用部分字段说明

序号	字段名	键名	类型	备注
1	事件名称	incidentName	字符型	监测预警事件名称
2	事件索引编号	incidentId	字符型	编码方式按附录B “网络安全事件编号编码规则”
3	事件类型	incidentType	字符型	0:未知 1:攻击类 2:黑名单 3:外联类 4.弱密码 5.畸形TCP包检测
4	事件等级	incidentLevel	整型	1-4，依次对应特别重大事件、重大事件、较大事件、一般事件，详见GB/T 20986 信息安全技术网络安全事件分类分级指南
5	事件时间	incidentTime	日期时间型	格式采用YYYYMMDDhh24mmss，精确到秒
6	事件对象描述	incidentObject	对象型	描述事件对象详细参数
7	是否审核	verify	布尔型	是否经人工审核，0为是，1为否
8	目标URL	dstURL	字符型	预警对象的URL，多个时用英文逗号隔开，最大范围存储20个目标对象URL
9	目标域名	dstDomain	字符型	预警对象的域名，多个时用英文逗号隔开，最大范围存储20个目标对象域名
10	目标系统名称	dstName	字符型	预警对象的系统名称

序号	字段名	键名	类型	备注
11	攻击者IP地址	srcIp	字符型	攻击发起的IP地址，支持ipv4、ipv6格式，多个时用英文逗号隔开，最大范围存储20个目标对象IP
12	目标IP	dstIp	字符型	预警对象的IP地址，支持ipv4、ipv6格式，多个时用英文逗号隔开，最大范围存储20个目标对象IP
13	攻击者对象端口	srcPort	字符型	部分子类要求是多个时用英文逗号隔开，最大范围存储20个攻击发起对象端口
14	目标对象端口	dstPort	字符型	部分子类要求是多个时用英文逗号隔开，最大范围存储20个目标对象端口
15	IP的上层协议	protocolName	字符型	IP层之上的协议
16	处理动作	action	布尔型	0:监控 1:阻断
17	单位名称	uniName	字符型	被攻击单位名称
18	单位级别编码	uniLevel	字符型	预警单位级别，级别详见附录 表B.1单位级别编码表
19	单位性质编码	uniProperties	字符型	单位的性质，详见附录表B.2单位性质编码表
20	行业类型编码	industryType	字符型	单位所属行业，参照GB/T 4754-2017国民经济行业分类与代码，使用编码前3位，如A01（农业）
21	设备名称	deviceName	字符型	设备名称
22	系统版本	systemVersion	字符型	系统版本
23	补丁版本	patchVersion	字符型	补丁版本
24	规则库版本	ruleVersion	字符型	设备安全检测规则库版本
25	规则库匹配特征	ruleMatch	字符型	检测匹配的攻击特征
26	规则库匹配关键词	ruleMatchSign	字符型	检测匹配的关键词
27	目标对象所在地（国家）	dstCounty	字符型	使用正式行政区划名称，不可使用代称、简称
28	目标对象所在地（省）	dstProvince	字符型	使用正式行政区划名称，不可使用代称、简称
29	目标对象所在地（市）	dstCity	字符型	使用正式行政区划名称，不可使用代称、简称

附 录 B

（资料性）

网络安全事件编号编码规则

网络安全事件编号编码规则见表B.1。

表B.1 网络安全事件编号编码规则

编号序号	1	2	3	4	……	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
说明	第一部分						第二部分								第三部分							
	行政区划代码						报送时间码								事件顺序码							

事件编号作为网络安全事件的唯一标识符，由32位阿拉伯数字组成，包括第1-16位上报单位行政区域代码（16位），第17-24位报送时间码（8位），第25-32位事件顺序码（8位）。

上报单位代码由上报平台统一编制配置。

报送时间码参照GB/T 7408编制，年、月、日代码之间不使用分隔符，例如20010101。

附 录 C

（资料性）

其它可枚举类型编码规则表

C.1 单位级别编码表

单位级别编码见表C.1。

C.1.单位级别编码表

序号	类型	编号
1	部委级	001
2	省级	002
3	地市级	003
4	区县级	004
5	其他	000

C.2 单位性质编码

单位性质编码见表C.2。

C.2.单位性质编码表

序号	名称	编码
1	国防机构	UP01 (unit properties)
2	党委机关	UP02
3	政府机关	UP03
4	事业单位	UP04
5	企业	UP05
6	个人	UP06
7	社会团体	UP07
8	民办非企业单位	UP08
9	基金会	UP09
10	律师执业机构	UP10
11	外国在华文化中心	UP11
12	群众性团体组织	UP12
13	司法鉴定机构	UP13
14	宗教团体	UP14
15	境外机构	UP15
16	医疗机构	UP16
17	公证机构	UP17
18	其他	UP18

附 录 D

（资料性）

运行环境要求

根据关键信息基础设施安全监测预警产品运行实际需要，列出了不同规格、性能对硬件最低配置需求，运行环境要求见表D.1。

表 D.1 运行环境要求

序号	规格	性能要求	配置要求
1	千兆	新建链接数≥15000/秒、并发连接数≥1000000	CPU≥4核、内存≥32GB、存储≥2TB
2	万兆	新建链接数≥60000/秒、并发连接数≥3000000	CPU≥14核、内存≥64GB、存储≥4TB

参 考 文 献

[1] GB/T 20984 信息安全技术 信息安全风险评估方法
[2] GB/T 28458 信息安全技术 安全漏洞标识与描述规范
[3] GB/T 36635 信息安全技术 网络安全监测基本要求与实施指南
[4] GB/T 37953 信息安全技术 工业控制网络监测安全技术及测试评价方法
[5] GB 42250 信息安全技术 网络安全专用产品安全技术要求
[6] GB/T 42453—2023 信息安全技术 网络安全态势感知通用技术要求
[7] GB/T 7408 数据元和交换格式 信息交换 日期和时间表示法
[8] 《关键信息基础设施安全保护条例》（2021年国务院令第745号）
[9] 《中华人民共和国网络安全法》