ICS 35.030
CCS L 80

T/CCIA

中 国 网 络 安 全 产 业 联 盟 技 术 规 范

T/CCIA XXX—XXXX

信息安全技术 网络安全产品互联互通 资产信息格式

Information security technology—Network security products interconnection - Asset information format

（征求意见稿）

2023 年 4 月 17 日

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国网络安全产业联盟　　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。

本文件由中国网络安全产业联盟提出。

本文件由中国网络安全产业联盟归口。

本文件起草单位：北京天融信网络安全技术有限公司、中国电子技术标准化研究院、国家信息中心、国家互联网应急中心、中国科学院信息工程研究所、深信服科技股份有限公司、东软集团股份有限公司、杭州安恒信息技术股份有限公司、绿盟科技集团股份有限公司、安天科技集团股份有限公司、北京升鑫网络科技有限公司

本文件主要起草人：

信息安全技术 网络安全产品互联互通 资产信息格式

1 范围

本文件规定了网络安全产品报送的资产信息结构和数据格式。

本文件适用于指导网络安全产品互联互通功能和其它互联互通信息的设计、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 25066-2022 信息安全技术 信息安全产品类别与代码
GB/T 25069-2022 信息安全技术 术语

3 术语和定义

GB/T 25069-2022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 network security product interconnect

通过统一的网络安全信息描述方式和安全功能实现，高效协同不同产品，支撑网络安全监测预警、信息共享、应急响应、态势感知等应用需求，以提升整体网络安全防护能力的一种机制。

3.2

资产信息 asset information

组织所拥有的一切可能被潜在攻击者利用的设备、业务系统、组件、域名等实体的信息。

4 缩略语

下列缩略语适用于本文件。

CPE：通用平台枚举（Common Platform Enumeration）

IP：网际互连协议（Internet Protocol）

5 资产信息数据格式

5.1 概述

资产类型可分为设备、业务系统、组件和域名。资产信息的数据格式，由资产通用信息部分和资产扩展信息部分共同组成，示意图见图1。

a) 资产通用信息：包括基本信息、责任部门信息、责任人信息、位置信息、价值信息、网络信息和其它通用信息七部分。

b) 资产扩展信息：分为设备类信息、操作系统类信息、业务系统类信息、组件类信息和域名类信息五种类型，具体资产按照其类别选择其中一种扩展信息。

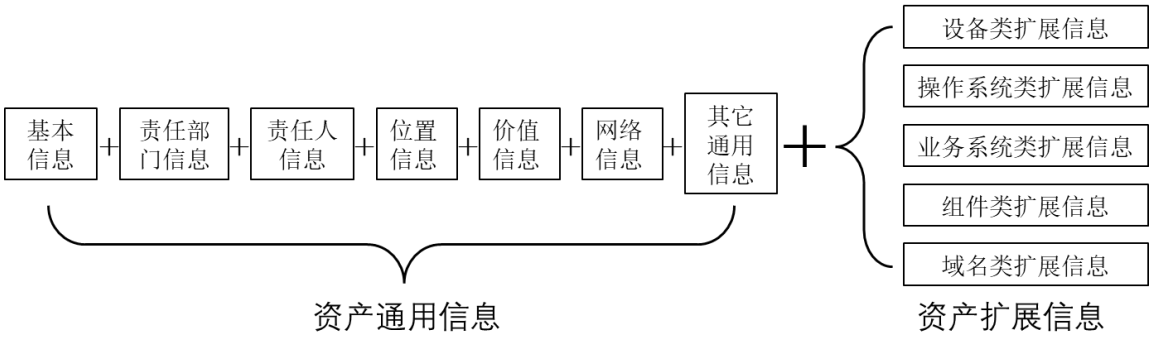

图1 资产信息组成部分示意图

本文件中使用的字段类型见附录A。

5.2 资产通用信息格式

5.2.1 资产基本信息

表1 资产基本信息格式表

序号	英文字段名称	中文字段名称	字段说明	字段类型	是否必填
1	asset_id	资产标识	资产的唯一标识	字符型	是
2	asset_name	资产名称	资产的名称	字符型	是
3	asset_description	资产描述	资产的描述说明信息	字符型	否
4	asset_type	资产类别	设备、操作系统、业务系统、组件、域名	数组型	是

5.2.2 资产责任部门信息

表2 资产责任部门信息格式表

序号	英文字段名称	中文字段名称	字段说明	字段类型	是否必填
1	assetDepartment_id	资产所属部门（单位）ID	资产所属部门（单位）的编号	字符型	是
2	assetDepartment_name	所属部门（单位）名称	资产所属部门（单位）的名称	字符型	是
3	assetDepartment_address	部门地址	资产所属部门的地址	字符型	是
4	organazition_type	统一社会信用代码	资产所属单位统一社会信用代码	字符型	否
5	assetSuperiorDepartment_iD	所属部门上级部门 id	资产所属部门的上级部门的编号	字符型	否

5.2.3 资产责任人信息

表3 资产责任人信息格式表

序号	英文字段名称	中文字段名称	字段说明	字段类型	是否必填
1	assetPerson_name	资产责任人姓名	对资产安全负直接责任的人员姓名	字符型	是
2	assetPerson_mobilephone	责任人移动电话	责任人的移动电话号码	字符型	是
3	assetPerson_fixedphone	责任人固定电话	责任人的固定电话号码	字符型	否
4	assetPerson_email	责任人邮箱	责任人的电子邮箱地址	字符型	否

5.2.4 资产位置信息

表4 资产位置信息格式表

序号	英文字段名称	中文字段名称	字段说明	字段类型	是否必填
1	assetLocation_country	资产所处国家	资产当前所处位置的国家名称	字符型	是
2	assetLocation_province	所处省份	资产当前所处省份位置	字符型	是
3	assetLocation_city	所处城市	资产当前所处地市位置	字符型	否
4	assetLocation_district	所处区县	资产当前所处区县位置	字符型	否
5	assetLocation_geographicalposition	所处的具体位置	可以定位到资产的 gps 等信息	字符型	否

5.2.5 资产价值信息

表5 资产价值信息格式表

序号	英文字段名称	中文字段名称	字段说明	字段类型	是否必填
1	significance	重要性	资产的重要等级,人工赋值[1,2,3] (1:非常重要,2:重要,3:一般)	数值型	否
2	is_critical_info_infra	是否为关键信息基础设施	(true:是,false:否)	布尔型	否
3	applicability	可用性	(true:是,false:否)	布尔型	否
4	assetValue_secretive	机密性	[1,2,3,4,5] (1:非常低,2:低,3:中,4:高,5:非常高)	数值型	否
5	assetValue_complete	完整性	[1,2,3,4,5] (1:非常低,2:低,3:中,4:高,5:非常高)	数值型	否

5.2.6 资产网络信息

表6 资产网络信息格式表

序号	英文字段名称	中文字段名称	字段说明	字段类型	是否必填
1	assetNetwork_ipv4	资产的 IPv4 地址	资产分配（或自动获取）的 IPv4 地址	字符型	否
2	assetNetwork_mac	mac 地址	资产的 MAC 地址	字符型	否
3	assetNetwork_ipv6	IPv6 地址	资产的 IPv6 地址	字符型	否
4	assetNetwork_portno	可见的端口号	资产可见的端口号	数组型	否
5	assetNetwork_protocol	使用的协议名称	资产中使用的协议名称	数组型	否

5.2.7 资产其它通用信息

表7 资产其它通用信息格式表

序号	英文字段名称	中文字段名称	字段说明	字段类型	是否必填
1	assetOther_securitydomain	资产的安全域	资产划分到的安全域	字符型	否
2	assetOther_group	所属资产组	资产划分到的资产组	字符型	否
3	source	来源	0:上报（人工添加）;1:探测（探测扫描）;2:事件发现;3:三方接入;4:其他	字符型	是
4	purchase_time	上线时间	资产购买或投入使用的时间 YYYY-MM-DDhh:mm:ss（英文半角格式）	日期时间型	否
5	update_time	更新时间	资产上次更新信息的时间	日期时间型	否

5.3 资产扩展信息格式

资产扩展信息按照设备、操作系统、业务系统、组件和域名五种类型分别给出其信息格式，扩展信息格式见表8至表12。

表8 设备类扩展信息格式表

序号	字段名称	中文名称	字段说明	字段类型	是否必填
1	dev_code	设备序列号	设备的唯一识别 id;没有序列号可以用 UUID 代替;探测到的设备取值为 UUID	字符型	是
2	devIdCertificate	设备身份证书	设备的身份证书	字符型	否
3	devTypeId	类型	网络安全产品类型与代码见附录 B	数组型	是
4	devModel	型号	（如防火墙的具体型号）	字符型	否
5	devHwVersion	硬件版本	设备的硬件版本	字符型	否
6	devIsDomestic	是否国产化设备	是否是国产化设备	字符型	否
9	isVirtual	是否为虚拟机	[1,0] (1:是,0:否)	数组型	否
10	updateRecord	修改记录	设备的修改记录	字符型	否

表8 设备类扩展信息格式表（续）

序号	字段名称	中文名称	字段说明	字段类型	是否必填
11	riskValue	风险值	设备的风险值	字符型	否
12	verifyStatus	审核状态	0（未审核、未退库）1(审核中、退库中）2（审核通过、已退库）	数组型	否
13	extendColumn1	扩展字段 1	设备信息扩展字段 1	字符型	否
14	extendColumn2	扩展字段 2	设备信息扩展字段 2	字符型	否
15	extendColumn3	扩展字段 3	设备信息扩展字段 3	字符型	否

表9 操作系统类扩展信息格式表

序号	字段名称	中文名称	字段说明	字段类型	是否必填
1	osType	操作系统类型	网络安全产品类型与代码见附录 B	数组型	是
2	osName	操作系统名称	（如操作系统的具体型号）	字符型	是
3	osVersion	操作系统版本	操作系统的	字符型	否
4	osIsDomestic	是否国产化操作系统	是否国产化操作系统	字符型	否
5	extendColumn1	扩展字段 1	操作系统扩展字段 1	字符型	否
6	extendColumn2	扩展字段 2	操作系统扩展字段 2	字符型	否

表10 业务系统类扩展信息格式表

序号	英文名称	中文名称	字段说明	字段类型	是否必填
1	systemName	系统名称	业务系统或软件名称	字符型	是
2	businessType	业务类型	业务类型描述	字符型	是
3	serviceScope	服务范围	业务系统服务的范围描述	字符型	是
4	serviceObject	服务对象	业务系统服务对象的描述	字符型	是
5	isSelfConstruct	是否自建	业务系统是否自建还是采购的	整型	是
6	IsDomestic	是否国产化系统	(1:是,0:否)	整型	否
7	supplierName	供货方单位名称	供货方的单位名称	字符型	否
8	supplierFixedPhone	供货方联系电话	供货方的联系电话	字符型	否
9	supplierEmail	供货方联系邮箱	供货方的电子邮箱	字符型	否
10	isClassifyProtection	是否要进行等保测评	(1:是,0:否)	整型	否
11	CPLevel	等保等级	等保 1、2、3、4、5 级	整型	否
12	CPNo	等保系统编号	等保系统编号	字符型	否
13	CPGradingTime	等保定级时间	等保定级时间	日期时间型	否
14	extendColumn1	扩展字段 1	业务系统扩展字段 1	字符型	否
15	extendColumn2	扩展字段 2	业务系统扩展字段 2	字符型	否
16	extendColumn3	扩展字段 3	业务系统扩展字段 3	字符型	否

表11 组件类扩展信息格式表

序号	英文名称	中文名称	字段说明	字段类型	是否必填
1	compType	组件类型	组件类型描述	字符型	是
2	compName	组件名称	组件的名称	字符型	是
3	compVersion	组件版本	组件的版本	字符型	是
4	compCPE	cpe 通用平台	组件的 CPE 通用平台	字符型	否
5	isDomestic	是否国产	[1,0] (1:是;0:否)	整型	否
6	developmentFramework	开发框架	组件的开发框架	字符型	否
7	developmentLanguage	开发语言	组件的开发语言	字符型	否
8	compPort	组件端口	组件的端口	字符型	是
9	compProtocol	协议	组件的协议	字符型	是
10	devId	设备 ID	组件所处的设备 ID	字符型	否
11	sysId	业务系统 ID	组件所处的业务系统 ID	字符型	否
12	extendColumn1	扩展字段 1	组件扩展字段 1	字符型	否
13	extendColumn2	扩展字段 2	组件扩展字段 2	字符型	否
14	extendColumn3	扩展字段 3	组件扩展字段 3	字符型	否

表12 域名类扩展信息格式表

序号	字段名称	中文名称	字段说明	字段类型	是否必填
1	domainAddress	域名地址	域名地址	数组型	是
2	domainAddressType	域名地址类型	域名地址是中文还是英文	整型	否
3	whoisStatus	域名状态	域名状态	字符型	否
4	domainPurpose	域名用途	域名用途	字符型	否
5	domainResolutionIP	域名解析 IP	域名解析 IP	字符型	否
6	isRecord	是否已备案	0-未备案，1-已备案	整型	否
7	recordInfo	备案信息	域名的备案信息	字符型	是
8	whoisCreateTime	注册时间	域名的注册时间	日期时间	否
9	registrarName	注册服务供应商	域名的注册服务供应商	字符型	否
10	whoisDomainServer	域名服务器	域名服务器	字符型	否
11	subdomain	子域名列表	子域名列表	数组型	否
12	extendColumn1	扩展字段 1	域名扩展字段 1	字符型	否
13	extendColumn2	扩展字段 2	域名扩展字段 2	字符型	否
14	extendColumn3	扩展字段 3	域名扩展字段 3	字符型	否

附 录 A
（规范性）
资产信息字段取值类型

资产信息字段类型的取值见表A.1。

表A.1 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，符合 GB/T 7408。
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。

附 录 B
（规范性）
网络安全产品类别与代码

按照GB/T 25066-2020，网络安全产品类别与代码的取值范围见表B.1。

表B.1 网络安全产品类别与代码

资产类型编码	资产类型
B101	虚拟专用网
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	网络单向隔离
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
D102	身份鉴别（主机）
D103	主机入侵检测
D104	主机访问控制
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
D301	安全操作系统
D302	操作系统安全部件
D401	身份鉴别（应用）

表B.1 网络安全产品类别与代码（续1）

资产类型编码	资产类型
D402	WEB 应用防火墙
D403	邮件安全防护
D404	网站恢复
D405	应用安全加固
D501	业务流程监控
D502	源代码审计
D503	网站监测
D504	应用软件安全管理
D505	应用代理
D506	负载均衡
D507	数字签名
D601	数据加密
D602	数据泄露防护
D603	数据脱敏
D604	数据清除
D605	数据备份与恢复
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
E201	应急响应辅助系统
E301	密码设备
E302	公钥基础设施
E401	系统风险评估
E402	安全性检测分析
E403	配置核查
E404	漏洞挖掘
E405	态势感知
E406	高级持续威胁检测
E407	舆情分析
E501	安全管理平台

表B.1 网络安全产品类别与代码（续2）

资产类型编码	资产类型
E502	安全监控
E503	运维安全管理
E504	统一身份鉴别与授权
X999	其它

参 考 文 献

[1] GB/T 25000.1-2021 系统与软件工程 系统与软件质量要求和评价(SQuaRE) 第1部分：SQuaRE指南
[2] GB/T 31360-2015 固定资产核心元数据
[3] GB/T 33172-2016 资产管理 综述、原则和术语
[4] GB/T 36328-2018 信息技术 软件资产管理 标识规范
[5] GB/T 40685-2021 信息技术服务 数据资产 管理要求
[6] GA/T 1359-2018 信息安全技术 信息资产安全管理产品要求
[7] YD/T 3803-2020 电信网和互联网资产安全管理平台技术要求
[8] T/CCIA 001-2022 面向网络安全保险的风险评估指引
[9] NIST SP1800-5 IT Asset Management