TC260-PG-2023XX

网络安全标准实践指南

—网络安全产品互联互通 资产信息格式

（征求意见稿 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

本《实践指南》版权属于信安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国信息安全标准化技术委员会秘书处”。

技术支持单位

本《实践指南》得到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、北京神州绿盟科技有限公司、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、沈阳东软系统集成工程有限公司、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资产信息的描述格式，适用于网络安全产品互联互通的设计、开发、应用和测试。

目 录

1 范围 2
2 术语和定义 2
3 缩略语 2
4 概述 3
5 资产信息格式 4
5.1 资产通用信息格式 4
5.2 资产扩展信息格式 5
附录 A （规范性） 设备代码 8
附录 B （资料性） 资产信息格式示例 11
参考文献 14

1 范围

本实践指南规定了网络安全产品互联互通资产信息的描述格式。

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 cybersecurity 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

资产信息 asset information

实现网络安全产品互联互通时所使用的资产的相关信息，资产包括但不限于设备、操作系统、数据库、中间件、应用软件、业务系统等，资产信息主要涉及资产名称、位置、网络、运行状态等。

3 缩略语

下列缩略语适用于本实践指南。

IPv4：互联网协议第4版（Internet Protocol Version 4）

IPv6：互联网协议第6版（Internet Protocol Version 6）

4 概述

资产信息由资产通用信息和资产扩展信息组成，见图1。

a) 资产通用信息：包括基本信息、位置信息、网络信息等；

b) 资产扩展信息：包括设备类扩展信息、操作系统类扩展信息、数据库类扩展信息、中间件类扩展信息、应用软件类扩展信息、业务系统类扩展信息等。

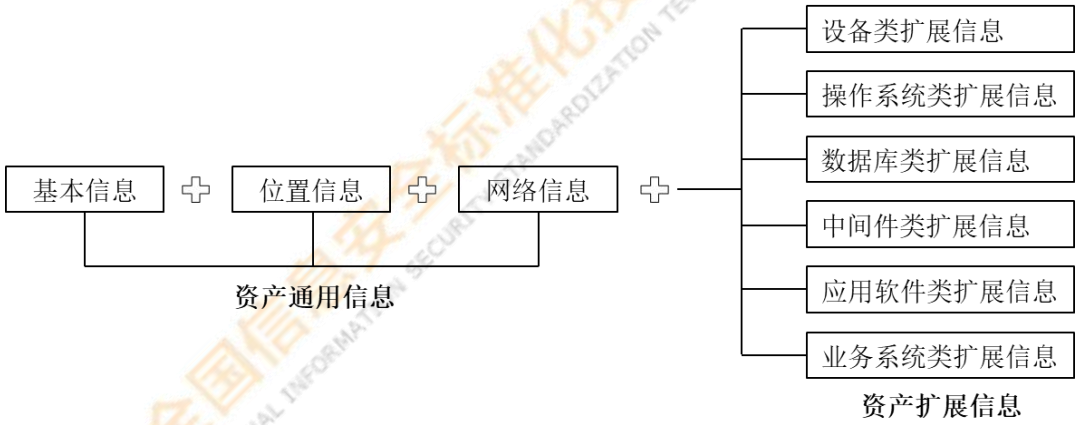

图 1　资产信息组成

资产信息格式的字段类型取值见表1。

表 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。

5　资产信息格式

5.1　资产通用信息格式

5.1.1　资产基本信息

表 2　资产基本信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	资产标识	assetId	资产管理部门分配的资产标识信息。	字符型	是
2	资产名称	assetName	资产的名称	字符型	是
3	资产类别	assetType	1-设备，2-业务系统，3-操作系统，4-数据库，5-中间件，6-应用软件，7-其它类型资产	整型	是
4	资产描述	assetDescription	资产的描述说明信息	字符型	否
5	更新时间	updateTime	资产最新更新信息的时间	日期时间型	否
6	管理部门（单位）名称	assetDepartmentName	资产管理部门（单位）的名称	字符型	否
7	资产责任人姓名	assetPersonName	资产责任人的姓名	字符型	否
8	责任人电话	assetPersonPhone	资产责任人的电话号码	字符型	否
9	重要性	assetValueSignificance	根据资产所承载或保护的业务的重要程度，结合风险评估结果进行赋值，1-非常重要，2-重要，3-一般	整型	否
10	资产所属安全域	securityDomain	资产划分到的安全域	字符型	否
11	资产所属资产组	assetGroup	资产划分到的资产组	字符型	否
12	资产运行状态	assetOperationalStatus	资产的运行状态，1-可用，2-不可用	整型	是

5.1.2 资产位置信息

表 3 资产位置信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	所处国家	assetLocationCountry	资产当前所处位置的国家名称	字符型	是
2	所处省份	assetLocationProvince	资产当前所处省份位置	字符型	是
3	所处城市	assetLocationCity	资产当前所处地市位置	字符型	是
4	所处区县	assetLocationDistrict	资产当前所处区县位置	字符型	否

5.1.3 资产网络信息

表 4 资产网络信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	资产的 IPv4 地址	assetNetworkIPv4	资产的 IPv4 地址	字符型	是
2	可见的 IPv4 端口号	assetNetworkIPv4PortNo	资产可见的 IPv4 端口号	数组型	是
3	MAC 地址	assetNetworkMAC	资产的 MAC 地址	字符型	否
4	资产的 IPv6 地址	assetNetworkIPv6	资产的 IPv6 地址	字符型	否
5	可见的 IPv6 端口号	assetNetworkIPv6PortNo	资产可见的 IPv6 端口号	数组型	否
6	使用的协议名称	assetNetworkProtocol	资产中使用的协议名称	数组型	否
7	域名地址	domainAddress	域名地址	数组型	否
8	子域名列表	subdomain	子域名列表	数组型	否

5.2 资产扩展信息格式

资产扩展信息包括设备、操作系统、数据库、中间件、应用软件、业务系统等，信息格式见表5至表10。

表 5　设备类扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	设备序列号	devSerialNo	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	设备类型	devTypeId	1-网络安全产品，2-网络设备	数组型	是
3	设备代码	devCode	设备代码详见附录 A。网络安全产品代码见表 A.1，网络设备代码见表 A.2	字符型	是
4	设备型号	devModel	如防火墙产品的具体型号	字符型	否
5	是否虚拟机	isVirtualMachine	[1,0](1:是,0:否)	整型	是
6	CPU 型号	CPUModel	设备中使用的 CPU 的型号	字符型	否
7	硬盘型号	harddiskModel	设备中使用的硬盘的型号	字符型	否
8	网卡型号	NICModel	设备中使用的网卡的型号	字符型	否

表 6　操作系统类扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	名称	osName	操作系统名称	字符型	是
2	型号	osType	操作系统型号	字符型	是
3	版本	osVersion	操作系统版本号	字符型	是

表 7　数据库类扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	名称	dbName	数据库的名称	字符型	是
2	类型	dbType	数据库的类型	数组型	是
3	版本	dbVersion	数据库的版本号	字符型	是

表 8　中间件类扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	名称	middlewareName	中间件的名称	字符型	是
2	版本	middlewareVersion	中间件的版本号	字符型	是

表 9　应用软件扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	应用软件名称	softwareName	应用软件的名称	字符型	是
2	应用软件版本	softwareVersion	应用软件的版本	字符型	是
3	应用软件序列号	softwareSerialNo	应用软件的序列号	字符型	是
4	应用软件使用端口	softwarePort	应用软件使用的端口	字符型	是
5	应用软件协议	softwareProtocol	应用软件的协议	字符型	是
6	设备序列号	devSerialNo	应用软件所处的硬件设备的序列号	字符型	否
7	业务系统 ID	softwareInBusSystemId	应用软件所处的业务系统 ID	字符型	否

表 10　业务系统扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	系统名称	busSystemName	业务系统名称	字符型	是
2	版本	busSystemVersion	业务系统版本	字符型	是
3	系统包含的设备列表	systemIncludeDevList	系统包含的设备列表	数组型	否
4	系统包含的应用软件列表	systemIncludeSoftwareList	系统包含的应用软件列表	数组型	否

附 录 A

（规范性）

设备类别与代码

表A.1按照GB/T 25066-2020规定了网络安全产品的类别与代码，表A.2规定了网络设备的类别与代码。

表 A.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 A.1 网络安全产品类别与代码（续）

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
D704	安全网络存储
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
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

表A.2 网络设备类别与代码

资产类型编码	资产类型
G1	服务器
H1	路由器
I1	交换机
J1	PLC
K999	其它

附 录 B

（资料性）

资产信息格式示例

B.1 概述

本附录给出了一个采用本指南所规定的网络安全产品互联互通资产信息格式描述的资产信息示例,目的是演示本指南所规范的网络安全产品互联互通资产信息格式的使用方法。

本示例采用JSON作为数据交换格式。

B.2 资产信息格式示例


```
{
    "assetId":"ZC-D0001-SB0001",
    "assetName":"FW0001",
    "assetType":"1",
    "assetDescription":"D0001部门的防火墙设备SB0001",
    "updateTime":"2023-11-22T09:32:45Z",
    "assetDepartmentName":"D0001",
    "assetPersonName":"张三",
    "assetPersonPhone":"010-82776666",
    "assetValueSignificance":"1",
    "securityDomain":"Domain001",
```

"assetGroup":"Group001",

"assetOperationalStatus":"1",

"assetLocationCountry":"中国",

"assetLocationProvince":"河北省",

"assetLocationCity":"张家口市",

"assetLocationDistrict":"崇礼区",

"assetNetworkIPv4":"10.236.183.55",

"assetNetworkIPv4PortNo":"21,22,23,80",

"assetNetworkMAC":"0C-9A-3C-E2-29-22",

"assetNetworkIPv6":"fe80::bc1c:9f2c:64eb:c426%19",

"assetNetworkIPv6PortNo":"80,513",

"assetNetworkProtocol":"ftp, tcp, udp, telnet",

"domainAddress":"www.test.com",

"subdomain":"mail.test.com",

"devSerialNo":"SN00010001",

"devTypeId":"1",

"devCode":"C301",

"devModel":"NGFW4000-UF",

"isVirtualMachine":"0",

"CPUModel":"龙芯3A5000",

"harddiskModel":"致态TiPlus5000-2T",

```
    "NICModel":"TL-NT521"
}
```

参考文献

[1] GB/T 36328-2018 信息技术 软件资产管理 标识规范

[2] GB/T 40685-2021 信息技术服务 数据资产 管理要求

[3] GA/T 1359-2018 信息安全技术 信息资产安全管理产品要求

[4] NIST SP1800-5 IT Asset Management