

电子政务外网 安全大数据和运维保障 平台接入规范 第 1 部分：安全大数据平台

E-government network—Access specification of secure big data and operation and
maintenance support platform—
Part 1: Secure big data platform

2022 – 07 – 19 发布

2022 – 08 – 19 实施

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 安全大数据平台数据交互参考模型 2

 5.1 参考模型 2

 5.2 数据采集与共享报送要求 3

 5.3 数据交互内容 3

 5.4 报送频率要求 3

6 数据接口规范 3

 6.1 接口类型 3

 6.2 接口协议 3

 6.3 接口消息格式 4

 6.4 安全要求 4

附录 A（规范性） 接口身份认证要求 5

 A.1 身份认证方式 5

 A.2 身份认证令牌刷新 5

 A.3 设区市平台节点注册 5

附录 B（规范性） 交互数据规范 7

 B.1 运行状态 7

 B.2 风险隐患 7

 B.3 漏洞情报 7

 B.4 告警数据 8

 B.5 告警清除数据 9

 B.6 安全事件 9

 B.7 安全报表 10

 B.8 案例数据 10

 B.9 预警通报数据 10

 B.10 案例知识库 11

 B.11 文件传输 12

附录 C（规范性） 分类及编码规范 14

 C.1 安全事件类型 14

C.2 接口返回状态编码表	14
C.3 行政区划编码表	15
参考文献	16

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。

DB32/T 4318《电子政务外网 安全大数据和运维保障平台接入规范》分为2个部分：

——第1部分：安全大数据平台；

——第2部分：运维保障。

本部分为《电子政务外网 安全大数据和运维保障平台接入要求》的第1部分。

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。

本文件由江苏省政务服务管理办公室提出并归口。

本文件起草单位：江苏省大数据管理中心。

本文件主要起草人：赵明、忻超、黄敏、夏国光、王光鑫、吴欣、边伟成、赵靖雯、张泊远、曹银美、王子文、付勍、刘晓红、张培勇。

电子政务外网 安全大数据和运维保障平台接入规范

第1部分：安全大数据平台

1 范围

本文件规定了江苏省电子政务外网安全大数据平台（以下简称“省平台”）与设区市电子政务外网安全大数据平台（以下简称“设区市平台”）的数据交互接口相关的接口协议、数据报送内容、数据报送格式和安全要求。

本文件适用于指导省平台和设区市平台的接口与数据对接。

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 25069 信息安全技术术语

GB/T 36635 信息安全技术网络安全监测基本要求与实施指南

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

信息安全事件 information security incident

与可能危害组织资产或损害其运行相关的、单个或多个被识别的信息安全事态。

[来源：GB/T 25069-2022，3.684]

3.2

脆弱性 vulnerability

可能被一个或多个威胁利用的资产或控制的弱点。

[来源：GB/T 25069-2022，3.19]

3.3

威胁 threat

可能对系统或组织造成危害的不期望事件的潜在因素。

[来源：GB/T 25069-2022，3.628]

3.4

网络安全监测 security monitoring

以信息安全事件为核心，通过对网络和安全设备日志、系统运行数据等信息的实时采集，以关联分析等方式，实现对监测对象进行风险识别、威胁发现、安全事件实时报警及可视化展现。

[来源：GB/T 36635—2018，3.1 有修改]

4 缩略语

下列缩略语适用于本文件。

API：应用编程接口（Application Programming Interface）

JSON：JS对象简谱（Java Script Object Notation）

5 安全大数据平台数据交互参考模型

5.1 参考模型

省平台与设区市平台通过安全数据接口进行数据对接，设区市平台应遵照本规范规定的接口和字段内容向省平台报送数据，实现全省政务外网的统一安全管理。省平台与设区市平台间对接的参考模型见图1。

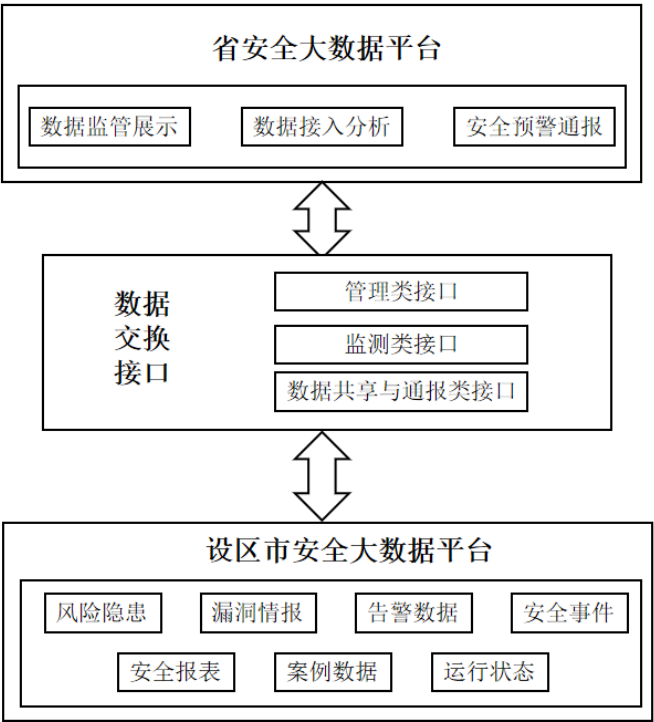


图1 省平台与设区市平台交互参考模型

省平台和设区市平台之间通过管理类、监测类、数据共享与通报类三类接口实现接入互通。其中，管理类接口用于实现省平台对设区市平台的接入管理；监测类接口用于实现监测类数据的上报，设区市平台按照数据报送要求向省平台进行上报；数据共享与通报接口用于实现省平台向设区市平台的数据共享与通报下发。

5.2 数据采集与共享报送要求

省平台与设区市平台应实现安全监测功能，应具备综合审计能力、本级的边界检测数据采集能力、安全行为和数据采集汇聚能力、数据分析呈现能力、态势感知和事件溯源分析能力、安全数据共享报送能力，具体要求如下：

- a) 安全大数据平台应具备综合审计能力，综合审计并实时采集本级对象应包括：终端、网络、服务器、数据库、中间件、应用系统等安全操作行为；
- b) 安全大数据平台应具备采集本级的边界检测数据，本级协议接口采集对象应包括：IDS、堡垒机、IPS、WAF、漏洞扫描、防火墙、防毒墙、网闸、抗 DDOS 等；
- c) 安全大数据平台能够对安全行为和数据进行采集汇聚，并运用数据挖掘分析技术对各种安全行为进行态势感知和事件溯源分析。

5.3 数据交互内容

设区市平台向省平台报送风险隐患、漏洞情报、告警数据、安全事件、安全报表、案例数据、运行状态数据，保证上报省平台数据的准确性和实时性。

省平台向设区市平台下发预警通报数据，共享案例知识库数据。

5.4 报送频率要求

报送数据的频率要求包括：

- a) 运行状态数据每天应最少报送一次，报送方式为全量报送；
- b) 风险隐患数据每天应最少报送一次，报送方式为全量报送；
- c) 漏洞情报数据及案例数据每天应最少报送一次，报送方式为增量报送；
- d) 告警数据及安全事件数据应实时报送，告警数据包括告警的产生和清除，报送方式为增量报送；
- e) 安全报表数据每周应最少报送一次，报送方式为增量报送。

6 数据接口规范

6.1 接口类型

交互接口包括管理类接口、监测类接口、数据共享与通报接口三类接口。管理类接口包括身份认证接口（见附录A）和运行状态上报接口（交互数据规范见附录B.1）。监测类接口包括风险隐患接口、漏洞情报、告警数据、安全事件、安全报表、案例数据六个数据报送接口（交互数据规范见附录B.2-B.8）；数据共享与通报接口包括预警通报下发、案例知识库获取、文件传输接口（交互数据规范见附录B.9-B.11）。

6.2 接口协议

接口协议的要求包括：

接口应按RESTful API标准对外提供服务，通过HTTPS协议加密数据，请求和响应的数据采用标准JSON格式来封装；

接口函数应包含两类：

- a) 同步调用函数，即函数的返回值就是结果，调用方应提供满足标准的回调函数，此类函数用于实现平台之间的接入认证；
- b) 异步调用函数，利用安全消息通道，实现异步数据上报，设区市平台上报时将数据放到省平台消息通道中，省平台下发时将数据放入本级消息通道，设区市平台到省平台消息通道获取数据，此类函数实现平台之间的数据传递。

6.3 接口消息格式

接口消息格式定义包括接口URL、接口描述、参数列表及接口返回信息。参数与返回值的具体JSON格式由接口提供者根据具体业务的实际情况制定，格式应层次简单、结构清晰。

6.4 安全要求

接口安全要求包括：

- a) 平台对接前需要经过安全身份认证，身份认证加密采用非对称加密算法，安全身份认证机制包括身份认证（见附录 A.1）及身份认证令牌定期刷新机制（见附录 A.2），同时设区市平台需注册节点信息（见附录 A.3）；
- b) 数据传输要经过可靠加密处理，加密处理方式可采用数据传输前安全数据加密或者网络传输通道SSL加密等方式，数据传输过程中应防止数据丢失、泄露、篡改；
- c) 涉及密码算法的相关内容，应按国家有关法规实施；涉及采用密码技术解决保密性、完整性、真实性、不可否认性需求的应遵循密码相关国家标准和行业标准。

附 录 A
(规范性)
接口身份认证要求

A.1 身份认证方式

接口信息说明见表A.1。

表A.1 身份认证接口说明

名称	描述
接口	/auth/token
请求方式	POST
Header: Content-type	application/json;charset=UTF-8

A.2 身份认证令牌刷新

平台身份认证令牌有效期默认为一小时，在令牌过期之前应请求新的令牌，接口信息说明见表A.2。

表A.2 身份认证令牌刷新接口说明

名称	描述
接口	/auth/refresh_token
请求方式	GET
Header: Content-type	application/json;charset=UTF-8
Header: Authentication	Bearer token

A.3 设区市平台节点注册

各地区各部门注册本级平台所属节点编码信息、IP 地址、经度，纬度等的格式，每次变更需重新注册。节点注册接口格式见表 A.3。

表A.3 设区市平台节点注册接口说明

名称	描述
URL	/api/v1/cascading/node/register
HTTP请求方式	POST
请求参数名	data
请求参数值（密文）	加密后的密文
Header: Content-type	application/json;charset=UTF-8
Header: Authentication	Bearer token

请求参数值解密之后为 JSON 格式的数据, 数据格式说明见表 A.4。

表A.4 请求参数说明

参数名	是否必须	类型	备注
center_code	是	字符	节点编码见附录C.3
center_name	否	字符	节点名称
ip	是	字符	平台IP地址
geoloc	是	字符	经度, 纬度
port	是	整数	平台端口

附 录 B
(规范性)
交互数据规范

B.1 运行状态

运行状态数据规范要求见表B.1。

表 B.1 运行状态数据

字段名称	中文名称	字段类型	是否必选	说明
memoryUsed	内存占用	字符	是	内存占用大小（带单位M,G,T）
memoryFree	内存空间	字符	是	内存空闲大小（带单位M,G,T）
memoryPercent	内存使用率	字符	是	内存使用率
cpuSpeed	CPU 速率	字符	是	CPU 速度（带单位GHZ）
cpuPercent	CPU 使用率	字符	是	CPU 使用率
diskUsed	硬盘使用量	字符	是	磁盘使用大小（带单位M,G,T）
diskTotal	硬盘总存储	字符	是	磁盘总大小（带单位M,G,T）
diskPercent	硬盘使用率	字符	是	磁盘使用率
recv	网络接收速率	字符	是	网络接收流量速率（带单位 bps,kbps,Mbps）
send	网络发出速率	字符	是	网络发送流量速率（带单位 bps,kbps,Mbps）

B.2 风险隐患

风险数据规范要求见表B.2。

表 B.2 风险数据

字段名称	中文名称	字段类型	是否必选	说明
domainName	安全域名称	字符	是	地市平台配置的安全域
riskValue	风险值	整数	是	风险值
riskLevel	风险等级	整数	是	风险等级，分为 5 级(1-5)，数字越大表示风险越高

B.3 漏洞情报

漏洞数据规范要求见表B.3。

表 B.3 漏洞数据

字段名称	中文名称	字段类型	是否必选	说明
cve	CVE ID	字符	否	示例: CVE-1999-0001
cnnvd	CNNVD ID	字符	否	示例: CNNVD-201404-530
loopholeTitle	漏洞标题	字符	是	示例: 电话信息泄露
loopholeDesc	描述	字符	是	漏洞描述
possibleAffect	漏洞可能造成的影响	字符	是	影响描述
disposalAdvice	处置建议	字符	是	处置建议
level	漏洞级别	整数	是	1-低 2-中 3-高
influenceAssetsIp	影响资产IP	字符	是	漏洞影响本地资产IP
scannerName	扫描器名称	字符	是	扫描器名称

B.4 告警数据

告警数据规范要求见表 B.4。

表 B.4 告警数据

字段名称	中文名称	字段类型	是否必选	说明
sourceId	告警ID	字符	是	告警ID
alarmName	告警名称	字符	是	告警名称
alarmGrade	风险等级	字符	是	Low-低危 Medium-中危 High-高危
alarmDesc	告警描述	字符	是	告警描述
alarmTime	告警时间	字符	是	告警时间, 格式 YYYY-MM-DDHH24:MM:SS
srcIp	来源IP	字符	是	来源IP
dstIp	目的IP	字符	是	目的IP
application	所属应用系统	字符	是	应用系统名称
assetsType	资产类型	字符	是	资产类型
devName	告警设备名称	字符	是	设备名称
alarmStatus	处置状态	字符	是	falsePositives-误报 processed-处理完成 processing-处理中 unprocessed-未处理
category	告警类型	字符	是	告警类型
subCategory	告警子类型	字符	是	告警子类型
direction	数据流方向	字符	是	00-内访问内 01-内访问外 10-外访问内 11-外访问内
destPort	目的端口	整数	否	目的端口
srcPort	源端口	整数	否	来源端口
requestUrl	访问请求的相关URL	字符	否	访问请求的相关URL
appProtocol	应用协议	字符	是	应用协议

字段名称	中文名称	字段类型	是否必选	说明
alarmResults	告警结果	字符	是	UNKNOWN-无法确认是否攻击成功 FAIL-攻击失败 OK-攻击成功

B.5 告警清除数据

告警清除数据规范要求见表B.5。

表 B.5 告警清除数据

字段名称	中文名称	字段类型	是否必选	说明
alarmIds	要清除的告警ID, 逗号隔开	字符	是	取值上报告警的sourceId

B.6 安全事件

安全事件数据规范要求见表B.6。

表 B.6 安全事件数据

字段名称	中文名称	字段类型	是否必选	说明
alarmName	事件名称	字符	是	事件名称
eventType	事件类型	字符	是	附录C.1, 取值二级分类
createTime	事件发生时间	字符	是	发生时间, 格式 YYYY-MM-DDHH24:MM:SS
alarmGrade	事件等级	字符	是	Low-低危 Medium-中危 High-高危
alarmDesc	事件描述	字符	是	告警描述
alarmTime	告警时间	字符	是	告警时间, 格式 YYYY-MM-DDHH24:MM:SS
srcIp	来源IP	字符	是	多个 IP 时用 “,” 隔开
dstIp	目的IP	字符	是	多个 IP 时用 “,” 隔开
influence	事件影响评估	字符	是	影响评估
disposal	处置结果	字符	是	falsePositives-误报 processed-处理完成 processing-处理中 unprocessed-未处理
domainName	恶意域名	字符	否	有相关域名需要提供
fileHash	文件HASH	字符	否	有相关恶意文件HASH时需提供
reportUser	事件报告联系人	字符	是	联系人姓名
reportPhone	报告人员联系方式	字符	是	手机号码
threatenedAssets	受威胁资产信息	字符	是	JSON字符串
attachment	附件	字符	否	调用文件传输接口进行文件传输, 将传输 返回结果填写在此, 多个附件信息传输多 个对象, 其格式为JSON字符串

B.7 安全报表

设区市平台将本平台产生的安全报表按照报送频率要求（见5.4）上报给省平台，报表以文件方式传送。报表数据规范要求见表B.7。

表 B.7 报表数据

字段名称	中文名称	字段说明	是否必选	说明
reportName	报表名称	字符	是	报表名称
reportType	报表类型	字符	是	周报 月报
reportDesc	报告描述	字符	是	报告描述
attachment	附件	字符	是	JSON字符串
createTime	创建时间	字符	是	创建时间，格式 YYYY-MM-DDHH24:MM:SS

B.8 案例数据

设区市平台应将本地发生的案例以文档方式按照报送频率要求（见5.4）进行上报，以便省平台对典型案例进行汇总。案例数据规范要求见表B.8。

表 B.8 案例数据

字段名称	中文名称	字段说明	是否必选	说明
caseTitle	案例标题	字符	是	案例标题
createTime	创建时间	字符	是	案例创建时间，格式 YYYY-MM-DDHH24:MM:SS
content	案例内容	字符	是	案例内容
keyProperty	关键字	字符	是	案例关键字说明，用于关键字索引
createMan	案例创建人	字符	是	案例创建人姓名、单位和联系方式
attachment	附件	字符	是	调用文件传输接口进行文件传输，将传输 返回结果填写在此，多个附件信息传输多 个对象其格式为JSON字符串
reserver	保留字段	字符	否	保留字段，供系统使用

B.9 预警通报数据

预警通报数据规范要求见表B.9。

表 B.9 预警通报数据

字段名称	中文名称	字段类型	是否必选	说明
startTime	开始时间	字符	是	开始时间, 格式 YYYY-MM-DDHH24:MM:SS
noticeName	通报名称	字符	是	通报名称
noticeType	通报类型	字符	是	通报类型描述
noticeDesc	通报描述	字符	是	通报原因描述
attachment	通报附件信息	字符	否	调用文件传输接口进行文件传输, 将传输 返回结果填写在此, 预警通报附件信息, 多个附件信息传输多个对象 其格式为 JSON字符
startNodeCode	发起节点编码	字符	是	发起节点编码
targetNodeCode	数据接收节点编码	字符	是	目标节点编码
createTime	创建时间	字符	是	创建时间, 格式 YYYY-MM-DDHH24:MM:SS

B.10 案例知识库

设区市平台调用知识库查询接口, 根据传递的接口参数获取相应的知识库案例内容。请求参数说明见表B.10。

表 B.10 案例知识请求参数说明

字段名称	中文名称	字段类型	是否必选	说明
titleKeyWord	标题关键字	字符	否	支持标题模糊查询
startTime	开始时间	字符	否	时间格式 YYYY-MM-DDHH24:MM:SS
endTime	结束时间	字符	否	时间格式 YYYY-MM-DDHH24:MM:SS
currentPage	当前页	字符	否	默认 1
maxResult	每次返回多少条数据	字符	否	默认 100

返回参数说明见表 B.11。

表 B.11 案例知识接口返回参数说明

字段名称	中文名称	字段说明	是否必选	说明
pages	页数	整数	是	根据关键字查询出数据的总页数
total	文档数量统计	整数	是	查询到的文档数量统计
id	标识	字符	是	案例标识
createTime	创建时间	字符	是	知识创建时间, 格式 YYYY-MM-DDHH24:MM:SS
keyProperty	关键字	字符	是	关键字

字段名称	中文名称	字段说明	是否必选	说明
content	内容	字符	是	知识详细内容
attachment	附件	字符	是	调用文件传输接口进行文件传输，将传输返回结果填写在此，附件信息
caseTitle	案例标题	字符	是	案例标题
createMan	案例创建人	字符	否	案例创建人姓名
reserver	保留字段	字符	否	保留字段，供系统使用

B.11 文件传输

附件内容通过文件传输接口进行传输，请求参数说明见表B.12。

表 B.12 文件传输请求参数说明

字段名称	中文名称	字段说明	是否必选	说明
file	校验信息	文件流	是	附件流

返回参数说明见表B.13。

表 B.13 文件传输返回参数说明

字段名称	中文名称	字段说明	是否必选	说明
code	返回编码	整数	是	返回状态码见附录C.2
msg	返回信息	字符	是	success 代表成功
docUrl	文件存储路径	字符	是	安全协同返回文件存储路径

附 录 C
(规范性)
分类及编码规范

C.1 安全事件类型

网络安全事件类型见表C.1。

表 C.1 网络安全事件类型

一级分类	二级分类
网络攻击	WEB攻击
	扫描探测
	暴力猜解
	漏洞攻击
	拒绝服务攻击
	可疑活动
	网络攻击
	其它网络攻击
恶意代码	灰色软件(恶意程序)
	蠕虫(有害程序)
	木马(有害程序)
	僵尸(有害程序)
	恶意事件(有害程序)
	病毒(有害程序)
	勒索软件
	异常信息
	可疑信息
	可疑程序
	漏洞
	弱口令
	未知威胁
	其它恶意代码

C.2 接口返回状态编码表

接口返回状态编码见表C.2。

表 C.2 接口返回状态编码表

状态码	状态码英文名称	代码描述
100	unauthorized	需要认证才能访问
99	forbidden	没有权限访问
98	too_many_requests	接口调用超过最大次数，请明天再试
97	bad_request	请求的参数不正确
96	not_found	资源不存在
95	register_node_error	无上级节点或上级节点未认证
94	encry_or_decrypt_error	加解密错误
93	internal_server_error	服务器内部错误
92	service_unavailable	服务器资源暂时不可用
200	success	成功

C.3 行政区划编码表

行政区划编码见表C.3。

表 C.3 设区市区划编码表

设区市区划代码	名称
320100	南京市
320200	无锡市
320300	徐州市
320400	常州市
320500	苏州市
320600	南通市
320700	连云港市
320800	淮安市
320900	盐城市
321000	扬州市
321100	镇江市
321200	泰州市
321300	宿迁市

参 考 文 献

- [1] GB/T 29246 信息技术 安全技术 信息安全管理体系统 概述和词汇
 - [2] GW 0203—2014 国家电子政务外网安全监测体系技术规范与实施指南
 - [3] GW 0204—2014 国家电子政务外网安全管理系统技术要求与接口规范
 - [4] DB32/T 3514.6—2019 电子政务外网建设规范第6部分：外网安全接入平台技术要求
 - [5] T/CIIA 005—2019 政务网络安全监测平台总体技术要求
-