ICS 35.240
CCS L 70

DB36

江 西 省 地 方 标 准

DB36/T 1892—2023

电子政务外网安全监测平台技术规范

Technical specifications forE-government extranet security monitoring platform

2023-12-11 发布　　2024-06-01 实施

江西省市场监督管理局　　发布

目　　次

前　言

本文件按照GB/T1.1-2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规则起草。

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。

本文件由江西省发展和改革委员会提出并归口。

本文件起草单位：江西省信息中心。

本文件主要起草人：杜军龙、钱军、何黎明、周剑涛、温小雨、刘嘉、涂烨、刘浪、龙映辉、张茜、王博琼、袁小乐、赖敬坤、王祯浩、潘志安、潘伟华、涂琳、谢冬、饶荣、严时晗。

电子政务外网安全监测平台技术规范

1 范围

本文件规定了电子政务外网安全监测平台的通用技术要求、扩展技术要求、数据共享以及平台级联要求。

本文件适用于电子政务外网安全监测平台的设计、建设和运维。

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/Z 20986 信息安全技术 信息安全事件分类分级指南

GB/T 36635信息安全技术 网络安全监测基本要求与实施指南

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 18336 信息技术 安全技术 信息技术安全性评估准则

GB/T 42583 信息安全技术 政务网络安全监测平台技术规范

DB36/T 979 电子政务外网安全接入平台技术规范

DB36/T 1093 电子政务外网网络接入规范

DB36/T 1099 电子政务云平台安全规范

DB36/T 1179 政务数据共享技术规范

DB36/T 1712 政务区块链平台技术规范

DB36/T 1713 公共数据分类分级指南

3 术语和定义

GB/T 25069《信息安全 术语》中规定内容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

由单个或一系列意外或有害的信息安全事态所组成的，极有可能危害业务运行和威胁信息安全。

[来源：GB/T 25069-2010，2.1.53]

3.2

电子政务外网安全监测平台 E-government extranetsecurity monitoring platform

以预防信息安全事件为核心，通过对网络流量、安全设备日志、威胁情报等数据信息进行实时采集、监测和分析，实现网络风险识别、威胁发现、安全事件预判和实时告警及可视化展示的系统。

3.3

政务城域网 government metropolitan area network

同城各政务部门间实现互联互通的政务网络。

[来源：GB/T 42583-2023，3.2]

3.4

政务广域网 government wide area network

连接不同地区政务局域网或政务城域网，实现远程通信的政务网络。

[来源：GB/T 42583-2023，3.3]

3.5

管理网 managementnetwork

承载安全统一运维、预警通告、安全数据传输等业务的基础网络。

3.6

探针 probe

从被观察的信息系统中，通过感知、监测等收集事态数据的一种部件或代理。

[来源：GB/T 25069-2010，2.2.1.27]

3.7

数据总线 databus

实现平台中数据采集探针、存储、分析、展示与应用等各模块之间，以及第三方平台之间数据共享和交换的功能模块。

[来源：GB/T 42583-2023，3.8]

3.8

威胁情报 threatintelligence

一种基于证据的知识，用于描述网络威胁信息、研判安全态势，支持安全事件响应和处置决策。包括事件情报、漏洞情报。

3.9

专项监测 special monitoring

云平台安全监测、移动应用安全监测、终端安全监测、数据安全监测等。

3.10

电子政务共享数据统一交换平台 E-government shared data exchange platform

电子政务共享数据统一交换平台（简称：交换平台）为异构、同构系统提供多种数据共享与交换模式，通过在线、实时、定时数据采集和数据交换，实现跨部门、跨地域、跨业务、多层级、多业务应用域的数据交换。

[来源：DB36/T 1179—2019，3.15]

3.11

前置节点 front node

江西省各级政务部门接入交换平台的前置机及相关软件，对接部门共享资源，实现政务部门间政务信息资源的共享交换。

3.12

节点 node

用于连接不同网络设备或程序。

3.13

政务区块链 blockchain for governmental affairs

利用区块链技术，通过透明和可信规则，实现政务数据跨部门、跨区域共同维护和使用，促进业务协同办理，提高政务服务效率。

[来源：DB36/T 1712-2022，3.3]

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

GIS：地理信息系统（Geographic Information System）

JSON：JS对象简谱（JavaScript Object Notation）

SMTP：简单邮件传输协议（Simple Mail Transfer Protocol）

VPC：虚拟私有云（VirtualPrivateCloud）

DNS：域名系统（DomainNameSystem）

DGA：域名生成算法（DomainGenerateAlgorithm）

URL：统一资源定位系统（Uniform Resource Locator）

IP：互联网协议（Internet Protocol）

IPv6：互联网协议第六版（Internet Protocol Version 6）

IT：信息产业（Information Technology）

HTTP：超文本传输协议（HyperText Transfer Protocol）

HTTPS：超文本传输安全协议（HyperText Transfer Protocol Secure）

5 监测范围

电子政务外网安全监测平台监测范围包括本地区/本部门政务网络，以及与之连接的政务广域网、政务城域网与政务云，与政务部门或政务网络运营者管理的网络边界范围保持一致。当电子政务外网边界或结构发生变化时，应及时调整监测范围和电子政务外网安全监测平台设备的部署。监测范围如图 1 所示。

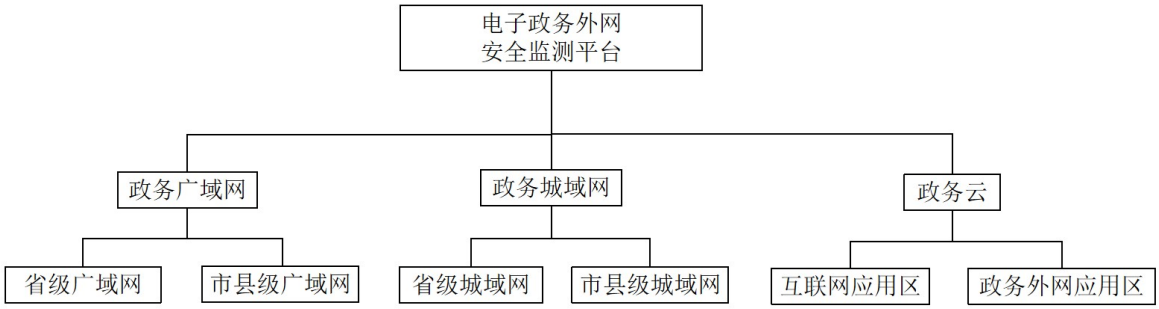

图 1 监测范围

6 部署架构

电子政务外网安全监测平台采用省市两级部署，通过级联系统对接。级联系统为省市两级电子政务外网安全监测平台对接的系统，为打通各节点之间的数据互联互通提供支撑，实现数据上报、下发、共享、预警通报、协同处置及数据展示查询功能。级联系统部署在省市两级电子政务外网安全监测平台。

省级电子政务外网安全监测平台通过省级平台级联系统向市级电子政务外网安全监测平台下发安全事件、预警通报、威胁情报及通报处置等，提供远程知识库、威胁情报库、漏洞库、通知通告的查询；市级电子政务外网安全监测平台通过市级平台级联系统向省级电子政务外网安全监测平台上报系统运行状态、安全事件、威胁情报，反馈处置结果。原则上，县级单位不部署电子政务外网安全监测平台，通过部署多元数据采集点上传数据至市级电子政务外网安全监测平台形成市县联动。电子政务外网安全监测平台部署架构如图 2 所示。

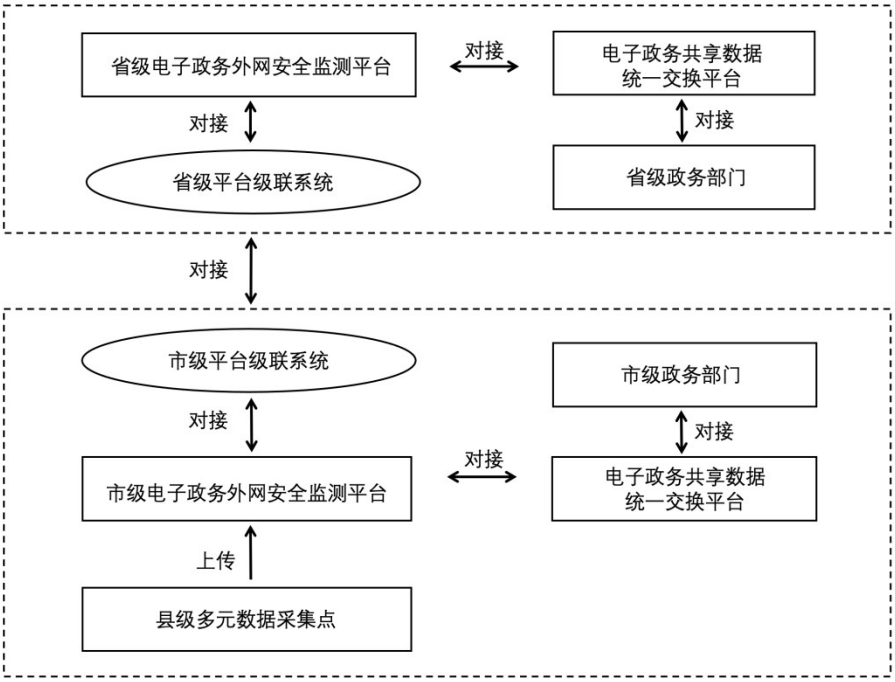

图 2 电子政务外网安全监测平台部署架构

7 通用技术要求

电子政务外网安全监测平台基于省电子政务外网建设，基本要求包括但不限于：

a）省级电子政务外网安全监测平台为省级政务部门提供监测服务，将威胁情报、案例、安全事件通告与数据安全治理结果等资源共享到市级电子政务外网安全监测平台；

b）省级电子政务外网安全监测平台应通过网络安全等级保护三级测评，市级电子政务外网安全监测平台宜按照省级标准进行建设；

c）市级电子政务外网安全监测平台为市县级政务部门提供监测服务，按要求对省级电子政务外网安全监测平台下发的安全事件进行整改，及时上报市级电子政务外网安全态势、告警信息、风险状况、案例、安全事件等内容；

d）市级电子政务外网安全监测平台应通过平台级联系统与省级电子政务外网安全监测平台进行级联对接；

e）电子政务外网安全监测平台应具备数据采集、威胁情报、数据安全治理、数据总线、数据分析、展示与应用、平台管理、数据存储等功能；

f)可集成不同厂商的各类 IT 资产，实现各类设备日志信息的实时采集与统一监测；

g)安全日志存储时间至少为 6 个月，采用密码技术保证日志记录的完整性 ;安全监测平台应支持日志检索功能；

h）采用国产自主可控安全产品，支持国密算法；

i）电子政务外网安全监测平台应满足 IPv6 功能要求。

8 扩展技术要求

电子政务外网安全监测平台扩展技术要求分为基本要求和增强要求,网络安全等级保护三级以下的

电子政务外网安全监测平台适用基本要求，网络安全等级保护三级（含）以上电子政务外网安全监测平台适用基本要求和增强要求。在本文件中，**黑体**字部分表示增强要求。

电子政务外网安全监测平台架构分为八个部分，分别为数据采集子系统、威胁情报子系统、数据安全治理子系统、数据总线子系统、数据分析子系统、展示与应用子系统、平台管理子系统和数据存储子系统，电子政务外网安全监测平台技术架构如图 3 所示。

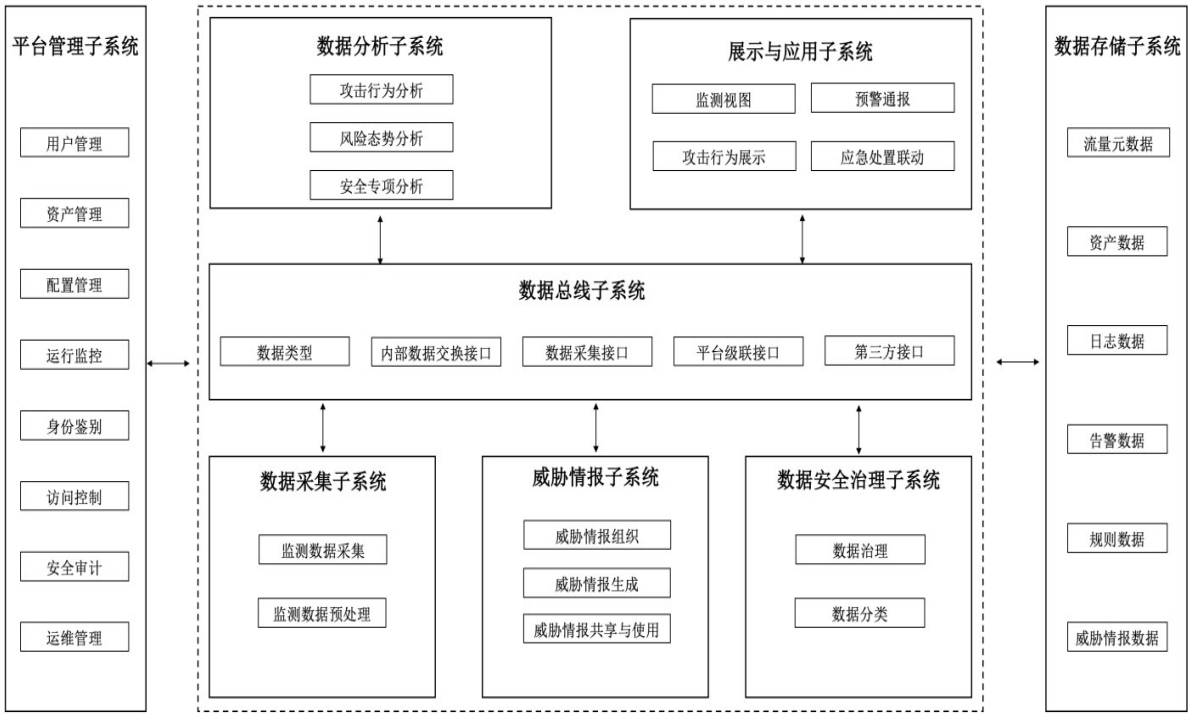

图3电子政务外网安全监测平台技术架构

8.1 数据采集子系统

8.1.1 监测数据采集

本项要求包括：

a) 采集范围。应覆盖监测范围内的通信网络、区域边界以及计算环境。采集点部署在核心交换节点、核心汇聚节点和移动接入点等关键节点；

b) 采集对象。应实时监测采集范围内各网络区域的网络流量、资产信息、威胁情报、脆弱性信息、知识数据、级联/第三方平台数据、各类安全基础资源/服务等产生的告警数据、与安全相关的审计日志，实现资产梳理；

c) 采集方式。应支持通过流量采集系统、标准协议、API 接口、手动导入、扫描、第三方导入等不同的方式采集流量、日志、资产信息、威胁情报等信息。

8.1.2 监测数据预处理

本项要求包括：

a) 应通过配置相关解析规则，过滤规则，富化规则，日志类型来达到归一化，过滤、丰富、分类日志信息的目的；

b) 应支持自定义预处理解析规则文件，可根据应用场景，通过配置选择插件，正则表达式、分隔符、JSON 等方法定义解析规则。