|  |  |
| --- | --- |
| ICS | 35.020 |
| CCS | L 04 |

|  |
| --- |
| 2201 |

长春市地方标准

DB XX/T XXXX—XXXX

电子政务外网运行监测能力规范

Specification for monitoring capability of e-government external network operation

XXXX - XX - XX发布

XXXX - XX - XX实施

长春市市场监督管理局  发布

目次

[前言 II](#_Toc175467528)

[1 范围 1](#_Toc175467529)

[2 规范性引用文件 1](#_Toc175467530)

[3 术语和定义 1](#_Toc175467531)

[4 缩略语 1](#_Toc175467532)

[5 长春市电子政务外网运行监测框架、监测项与监测权重 1](#_Toc175467533)

[5.1 长春市电子政务外网运行监测框架 1](#_Toc175467534)

[5.2 长春市电子政务外网监测项 2](#_Toc175467535)

[5.3 长春市电子政务外网监测权重 3](#_Toc175467536)

[6 电子政务外网运行监测能力要求 3](#_Toc175467537)

[6.1 监测对象、内容与数据获取方式 3](#_Toc175467538)

[6.1.1 资产监测 3](#_Toc175467539)

[6.1.2 可用性监测 3](#_Toc175467540)

[6.1.3 事件监测 4](#_Toc175467541)

[6.1.4 隐患监测 4](#_Toc175467542)

[6.2 安全管理 4](#_Toc175467543)

[6.3 监测手段 5](#_Toc175467544)

[6.3.1 扫描监测 5](#_Toc175467545)

[6.3.2 日志监测 5](#_Toc175467546)

[6.3.3 流量监测 5](#_Toc175467547)

[6.3.4 级联监测 5](#_Toc175467548)

[7 评估方法 5](#_Toc175467549)

[附录A（资料性） 长春市电子政务外网运行监测能力分值 6](#_Toc175467550)

1. 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。

本文件由长春市政务服务和数字化建设管理局提出并归口。

本文件起草单位：杭州安恒信息技术股份有限公司、长春市政务服务和数字化建设管理局、长春市标准研究院（长春市WTO/TBT咨询中心）。

本文件起草人：刘竞雄、柳羽辉、戚志军、李聪、邓贺、冷皓、李凌岳。

电子政务外网运行监测能力规范

* 1. 范围

本文件规范了长春市电子政务外网运行监测能力要求及相关要求。

本文件适用于指导长春市内各级政务外网运行监测体系的规划、设计、建设和管理等相关工作。

* 1. 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 25069-2022 信息安全技术 术语

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南

DB33/T 2350—2021 数字化改革 术语定义

* 1. 术语和定义

GB/T 25069-2022 界定的术语和定义适用于本文件。

* 1. 缩略语

下列缩略语适用于本文件。

IRS 一体化数字资源系统（Integrated Resources System）

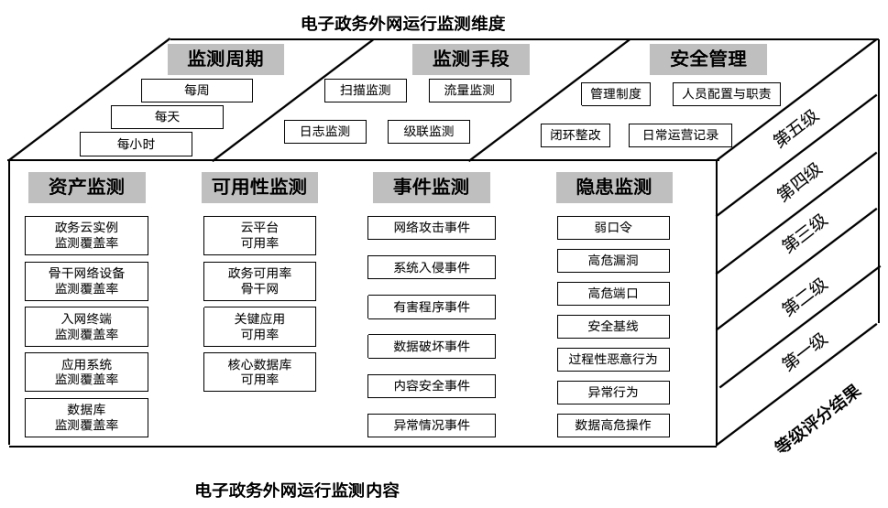
MI 监测项（Monitor Item）

MS 监测子项（Monitor SubItem）

SUM 最终分值（Sum）

* 1. 长春市电子政务外网运行监测框架、监测项与监测权重
     1. 长春市电子政务外网运行监测框架

长春市电子政务外网运行监测框架包括电子政务外网运行监测内容、电子政务外网运行监测维度、等级评估结果。长春市电子政务外网运行监测框架见图 1。



1. 长春市电子政务外网运行监测框架
   * 1. 长春市电子政务外网监测项

长春市电子政务外网监测项包括资产监测、可用性监测、事件监测、隐患监测四类。

1. 资产监测项（MI1）的子项主要包括：
   1. 政务云实例监测覆盖率（MS1）；
   2. 骨干网络设备监测覆盖率（MS2）；
   3. 入网终端监测覆盖率（MS3）；
   4. 应用系统监测覆盖率（MS4）；
   5. 数据库监测覆盖率（MS5）；
   6. 资产状态变化（MS6）。
2. 可用性监测项（MI2）的子项主要包括：
   1. 云平台可用率（MS7）；
   2. 政务云可用率（MS8）；
   3. 关键应用可用率（MS9）；
   4. 关键数据库可用率（MS10）。
3. 事件监测项（MI3）的子项主要包括：
   1. 网络攻击事件（MS11）；
   2. 系统入侵事件（MS12）；
   3. 有害程序事件（MS13）；
   4. 数据破坏事件（MS14）；
   5. 内容安全事件（MS15）；
   6. 异常情况事件（MS16）。
4. 隐患监测项（MI4）的子项主要包括：
   1. 弱口令（MS17）；
   2. 高危漏洞（MS18）；
   3. 高危端口（MS19）；
   4. 安全基线（MS20）；
   5. 过程性恶意行为（MS21）；
   6. 异常行为（MS22）；
   7. 数据高危操作（MS23）；
   8. 隐患监测周期（MS24）。
      1. 长春市电子政务外网监测权重

根据长春市电子政务外网监测项重要性设置该监测项的权重值，权重值一般为1-5的整数，权重指标见附录A。

* 1. 电子政务外网运行监测能力要求
     1. 监测对象、内容与数据获取方式
        1. 资产监测

资产监测包括以下内容：

1. 监测对象：政务云实例、骨干网络设备、入网终端、应用系统、数据库；
2. 监测内容：政务云实例监测覆盖率、骨干网络设备监测覆盖率、入网终端监测覆盖率、应用系统监测覆盖率、数据库监测覆盖率、资产状态变化监测；
3. 数据获取方式：
   1. 各级设区市、县（市、区）政务云实例总数可从IRS系统获取，可监测到的政务云实例数应从本级云平台系统中获取；
   2. 各级设区市、县（市、区）骨干网络设备总数可从IRS系统获取，可监测到的骨干网络设备应从本级云平台系统中获取；
   3. 各级设区市、县（市、区）入网终端总数可从IRS系统获取，可监测到的入网终端总数应从本级云平台系统中获取；
   4. 各级设区市、县（市、区）入网应用系统总数可从IRS系统获取，可监测到的应用系统总数应从本级云平台系统中获取；
   5. 各级设区市、县（市、区）数据库总数可从IRS系统获取，可监测到的数据库总数应从本级云平台系统中获取；
   6. 各级设区市、县（市、区）应具备政务云实例、骨干网络设备、入网终端、应用总数及数据库的资产状态变化（上线、下线、变更IP）监测能力。
      * 1. 可用性监测

可用性监测包括以下内容：

1. 监测对象：云平台、政务骨干网、关键应用、关键数据库；
2. 监测内容：云平台可用率、政务骨干网可用率、关键应用可用率、关键数据库可用率；
3. 数据获取方式：
   1. 云平台可用率可从本级的云平台系统中获取；
   2. 政务骨干网可用率可从本级网络管理系统中获取；
   3. 关键应用可用率可从本级网络管理系统中获取；
   4. 关键数据库可用率可从本级网络管理系统中获取。
      * 1. 事件监测

事件监测包括以下内容：

1. 监测对象：网络攻击事件、系统入侵事件、有害程序事件、数据破坏事件、内容安全事件、异常情况事件；
2. 监测内容：
   1. 网络攻击事件包括拒绝服务攻击事件、域名解析服务异常事件、广播欺诈事件、WIFI劫持事件、路由劫持事件5等类；
   2. 系统入侵事件包括后门入侵事件、身份仿冒事件、域名仿冒事件、高级威胁事件等4类；
   3. 有害程序事件包括计算机病毒事件、网络蠕虫事件、特洛伊木马事件、僵尸网络事件、网页内嵌恶意代码事件和综合性恶意程序事件等6类；
   4. 数据破坏事件包括数据篡改事件、数据泄漏事件、数据窃取事件、数据损毁事件等4类；
   5. 内容安全事件包括违反宪法和法律、行政法规的信息安全事件；针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的信息安全事件；组织串连、煽动集会游行的信息安全事件；其他信息内容安全事件等 4 个子类；
   6. 异常情况事件包括服务异常事件和流量异常事件。
3. 数据获取方式：
   1. 网络攻击事件可从本级网络安全监测系统中获取；
   2. 系统入侵事件可从本级网络安全监测系统中获取；
   3. 有害程序事件可从本级网络安全监测系统中获取；
   4. 数据破坏事件可从本级网络安全监测系统中获取；
   5. 内容安全事件可从本级网络安全监测系统中获取；
   6. 异常情况事件可从本级网络安全监测系统中获取。
      * 1. 隐患监测

隐患监测包括以下内容：

1. 监测对象：口令、漏洞、端口、基线配置、行为操作；
2. 监测内容：弱口令、高危漏洞、高危端口、安全基线（配置错误）、过程性恶意行为、异常行为、数据高危操作；
3. 数据获取方式：
   1. 弱口令隐患可从本级网络安全监测系统中获取；
   2. 高危漏洞隐患可从本级网络安全监测系统中获取；
   3. 高危端口隐患可从本级网络安全监测系统中获取；
   4. 安全基线（配置错误）隐患可从本级网络安全监测系统中获取；
   5. 过程性恶意行为隐患可从本级网络安全监测系统中获取；
   6. 异常行为隐患可从本级网络安全监测系统中获取；
   7. 数据高危操作隐患可从本级网络安全监测系统中获取。
      1. 安全管理

安全管理监测包括以下内容：

1. 监测对象：管理制度、机构人员、闭环整改、运营记录；
2. 监测内容：
   1. 管理制度包括电子政务外网网络安全管理制度、首席网络安全官制度及开展安全教育和培训等内容；
   2. 机构人员包括网络安全管理机构与人员配置情况、专职网络安全管理员配备情况等内容；
   3. 闭环整改包括隐患和事件整改情况；
   4. 日常运营记录包括单位每周日常运营工作周报。
3. 数据获取方式：
   1. 管理制度可从本级网络安全监测系统中获取；
   2. 机构人员可从本级网络安全监测系统中获取；
   3. 闭环整改可从本级网络安全监测系统中获取；
   4. 日常运营可从本级网络安全监测系统中获取。
      1. 监测手段
         1. 扫描监测

扫描范围应包括政务外网IP资产，包括但不限于政务云平台、骨干网络设备、入网终端、关键应用、关键数据库。

* + - 1. 日志监测

日志监测应支持Syslog、SNMP、FTP、插件代理等方式采集日志。

* + - 1. 流量监测

流量监测应支持部署流量探针，通过流量镜像的方式获取被监测的流量，包括但不限于FTP、DNS、HTTP、SSH等常用网络流量。

* + - 1. 级联监测

级联监测可通过API接口或对接第三方威胁情报平台采集、查询安全数据。

* 1. 评估方法

运行监测能力计算方法可采用以下方式：

1. 监测项得分等于监测子项积分之和乘以监测项权重，即：

MI1=C:\Users\dh\AppData\Local\Temp\ksohtml6804\wps4.png（其中i=1，2，…，n）\*R

1. 运行监测能力得分等于监测项之和，即：

SUM=C:\Users\dh\AppData\Local\Temp\ksohtml6804\wps5.png（其中i-1,2,…,n）

2. （资料性）  
   长春市电子政务外网运行监测能力分值

A.1 长春市电子政务外网运行监测能力分值

长春市电子政务外网运行监测能力分值见表A.1

* 1. 长春市电子政务外网运行监测能力分值参考表

|  |  |  |  |
| --- | --- | --- | --- |
| 一级指标监测项（MI） | 监测项权重(R) | 二级指标监测子项（MS） | 分值 |
| 资产监测（MI1） | 4 | 政务云实例监测覆盖率(MS1) | 4 |
| 骨干网络设备监测覆盖率(MS2) | 3 |
| 入网终端监测覆盖率(MS3) | 4 |
| 应用系统监测覆盖率(MS4) | 4 |
| 关键数据库监测覆盖率(MS5) | 3 |
| 资产变化状态(MS6) | 2 |
| 可用性监测（MI2） | 2 | 云平台可用率(MS7) | 2.5 |
| 政务骨干网可用率(MS8) | 2.5 |
| 关键应用可用率(MS9) | 2.5 |
| 关键数据库可用率(MS10) | 2.5 |
| 事件监测（MI3） | 3 | 网络攻击事件监测(MS11) | 3 |
| 系统入侵事件监测(MS12) | 3 |
| 有害程序事件监测(MS13) | 3 |
| 数据破坏事件监测(MS14) | 4 |
| 内容安全事件监测(MS15) | 3 |
| 异常情况事件监测(MS16) | 4 |
| 隐患监测(MI4） | 4 | 弱口令识别(MS17) | 4 |
| 高危漏洞监测(MS18) | 4 |
| 高危端口监测(MS19) | 2 |
| 安全基线（配置错误）监测(MS20) | 2 |
| 过程性恶意行为监测(MS21) | 3 |
| 异常行为监测(MS22) | 2 |
| 数据高危操作监测(MS23) | 3 |
| 安全管理(MI5） | 3 | 制度保障(MS24) | 3 |
| 机构人员落实情况(MS25) | 4 |
| 闭环整改(MS26) | 2 |
| 日常运营记录(MS27) | 3 |
| 监测手段（MI6） | 2 | 扫描监测(MS28) | 2 |
| 日志采集(MS29) | 2 |
| 流量监测(MS30) | 2 |
| 级联监测(MS31) | 2 |
| 监测周期（MI7） | 3 | 资产状态监测周期（MS32） | 2.5 |
| 可用性监测周期(MS33) | 2.5 |
| 事件监测周期（MS34） | 2.5 |
| 隐患监测周期（MS35） | 2.5 |

