**中国科学院肿瘤与**

**基础医学研究所（筹）**

**招标文件**

**招标项目：肿基所杀毒软件系统**

**招标人：中国科学院肿瘤与基础医学研究所**

**2020年4月**

# 第一章 招标公告

## 1.1、招标编号：ZJS-XX2020-001

## 1.2、招标项目概况及投标人要求：

|  |  |  |
| --- | --- | --- |
| 项号 | 内容 | 说明与要求 |
| 1 | 杀毒软件系统 | 中科院肿基所内、外网杀毒软件系统（300个客户端许可、50个服务器端许可,2个中心） |
| 2 | 采购内容 | 杀毒软件 |
| 3 | 实施地点 | 杭州经济技术开发区福城路150号 |
| 4 | 招标单位联系人及电话 | 联系人：吴老师 赵老师 电话：0571-88122296 |
| 5 | 踏勘现场 | 自行踏勘 |
| 6 | 投标有效期 | 为： 10 日历天（从投标截止之日算起） |
| 7 | 投标文件份数 |  1 份正本， 4 份副本 |
| 8 | 评标标准及方法 | 院内公开招（议）标 |
| 9 | 预算 | 6万 |

## 1.3、标书发售时间及地点：

1.报名截止日期：2020年4月24日14:00之前必须通过邮件报名登记。邮箱地址：zhaoqf@zjcc.org.cn，报名信息至少包含：企业名称、联系人、联系电话、营业执照等。未报名登记的,或在要求提交响应文件的截止时间后送达的响应文件，采购人有权拒收。

2．开标时间：2020年4月24日14：00

3．开标地点：浙江省肿瘤医院门诊楼（8号楼）6楼会议室

## 1.4投标人资格要求：

（一）基本条件

（1）具有独立承担民事责任的能力；

（2）具有良好的商业信誉和健全的财务会计制度；

（3）具有履行合同所必需的设备和专业技术能力；

（4）有依法缴纳税收和社会保障资金的良好记录；

（5）参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（6）法律、行政法规规定的其他条件。

（二）特定条件：

（1）根据《浙江省财政厅关于规范政府采购供应商资格设定及资格审查的通知》（浙财采监[2013]24号）第6条规定接受金融、保险、通讯等特定行业的全国性企业所设立的区域性分支机构，以及个体工商户、个人独资企业、合伙企业，且已经依法办理了工商、税务和社保登记手续，并且获得总机构授权或能够提供房产权证或其他有效财产证明材料，证明其具备实际承担责任的能力和法定的缔结合同能力；

（2）投标人未被列入失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单，信用信息以信用中国网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）公布为准；

（3）单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得同时参加同一合同项下的投标；

（4）为项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得参加该项目的投标；

（5）本项目不接受联合体；

## 1.5 联系方式：

1.地址：杭州市拱墅区半山东路1号

2.联系方式：

 联系人：吴老师 赵老师 联系电话：88122296

3.同级采购监督电话：

联系人：章老师 联系电话：88122523

#  商务技术要求

## 2.1 技术要求

|  |  |
| --- | --- |
| **指标项** | **性能指标及要求** |
| 配置要求 | 本次配置300个客户端许可、50个服务器端许可；两个管理中心，分别部署在肿基所内、外网，不少于三年原厂病毒库免费升级服务。 |
| 控制中心安装环境支持 | 操作系统支持Windows Server 2008 R2/2012/2012 R2/2016的64位版本（简体中文版）；支持CentOS 7、Redhat 7等Linux系统（要求Docker版本务必大于1.8.2）；支持在虚拟机上安装控制中心; |
| Windows客户端安装环境支持 | 操作系统：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10 |
| 服务器客户端安装环境支持 | 操作系统:Windows Server 2003\_SP2/Windows Server 2008/Windows Server 2012SUSE Linux/Red Hat Linux/CentOS/Ubuntu |
| 国产系统支持 | 中标麒麟/Deepin/银河麒麟/普华桌面操作系统 |
| 系统管理功能要求 | 控制中心：采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能； |
| 客户端提供控制中心管理所需的相关数据信息，通讯可选择非明文方式；客户端执行最终的病毒查杀等安全操作； |
| 产品支持终端保护密码，设置密码后，终端退出或卸载杀毒、或安装控制中心，都需要输入正确的密码方可执行；要求客户端程序具备自保功能，避免被恶意篡改 |
| 支持网页访问部署、离线安装包部署、域推送等部署方式，可自定义部署通知邮件及部署通知公告； |
| 支持自定义默认分组的终端默认功能模块,包括产品功能模块及实用工具等； |
| 支持加密的控制中心远程访问，支持管理账户并发、密码有效期、鉴别失败锁定等设置； |
| 支持设置日志上报的带宽限制； |
| 支持根据分组、计算机名称、IP地址、操作系统、在线状态等条件的组合筛选出符合条件的终端进行管理； |
| 支持控制中心迁移、数据备份、数据恢复；支持多升级服务器； |
| 资产管理支持 | 按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息；可监控CPU温度、硬盘温度和主板温度 |
| 支持终端软、硬件变更审计，资产清单报表； |
| 支持统计指定分组或全网的终端扫描数、终端管理软件安装数、未安装终端数及安装率 |
| 支持自动发现设备的IP-MAC地址的绑定（提供产品界面截图） |
| 支持插件清理，按插件显示展示全网存在的插件和涉及的终端，可清理指定或全部插件、加入信任；按终端显示展示全网每个终端存在的插件，可清理插件（提供产品界面截图） |
| 支持正版软件的正版序列号的读取功能，确保软件正版化。（提供功能截图，并加盖公司公章） |
| 日志报表 | 展示全网终端健康状态、报警信息；可方便的查看不健康、亚健康终端列表；展示全网终端病毒库日期比例，可方便的查看全网终端病毒库的情况 |
| 展示指定时间段内指定终端修复漏洞，病毒查杀，木马查杀的情况 |
| 要求支持邮件报警，可以设定多种触发条件，满足条件后自动发送邮件到相关人。邮件触发条件至少包括：一定时间内的病毒数量阈值、一定时间内的未知文件数量阈值、重点关注的终端发现病毒、病毒库超期等 |
| 提供系统升级、热备、管理员操作、管理员远程等系统日志； |
| 设备联动支持 | 支持与旁路威胁检测系统设备、NGFW、上网行为管理、VPN产品联动，达到网关边界联动防御效果（提供产品界面截图） |
| 病毒、恶意代码、木马防护 | 内存防护 | 支持内存实时监控查毒，能够自动隔离感染而暂时无法修复的文件； |
| 启动防护 | 支持抢先加载防毒，在系统未加载前启动文件监控，通常情况下不必重启到安全模式也能清除病毒； |
| 注册表、引导区防护 | 支持文件、引导区、内存、注册表、服务、进程、进出文件、目录、压缩文件、网页等恶意代码、恶意样本查杀 |
| 电子邮件防护 | 支持电子邮件内文件检测，可清除隐藏于电子邮件计算机病毒和恶性程序； |
| 网页安全防护 | 能够对网页提供安全防护，发现网页中的危险行为实时阻断；能够对网页挂马进行拦截，能够自动拦截网页中的钓鱼、欺诈信息； |
| 网络安全防护 | 拦截下载器自动下载木马程序、恶意推广程序、盗号木马；拦截黑客远程控制本机； |
| 嵌入式防御 | 支持用户添加嵌入杀毒的应用程序；支持FlashGet、NetAnts、WinZip、WellGet、WinRAR等工具的嵌入式杀毒功能； |
| 移动设备病毒防护 | 要求提供U盘等移动设备接入电脑自动检测功能，全面拦截和清除在移动设备接入系统可能带来的病毒木马； |
| 局域网共享查杀 | 能够对局域网共享文件传输进行检测和查杀； |
| 浏览器防护 | 支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置（提供功能截图，并加盖公司公章） |
| 聊天安全防护 | 检测QQ、MSN、阿里旺旺等常用聊天软件传输文件的安全性，确保传输文件不中毒；检测QQ、YY、飞信等聊天软件中对方发来网址的安全性聊天软件传输某些文件会添加“.重命名”，如果文件安全，将自动去除“.重命名” |
| 输入法防护 | 要求可以拦截伪装成输入法程序的木马；要求拦截利用输入法启动的木马程序 |
| 文件传输防护 | 支持U盘等移动磁盘设备和电脑硬盘间文件传输检测；支持局域网共享文件传输检测； |
| 攻击防护 | 能够实时检测和拦截攻击行为，包括改写系统关键文件、修改注册表关键键值、感染移动存储介质、创建系统账号 |
| 云修复 | 支持扫描发现文件遭破坏或被感染时触发修复流程，修复通过公有云下载正常文件替换遭破坏的文件； |
| 定时查杀 | 要求能够自定义时间、自定义扫描频率，自定义扫描类型，对终端进行定时查毒，并且可以自定义查杀病毒后的处理方式自定义； |
| 黑白名单例外 | 支持文件、目录和数字签名自定义黑白名单的方式来管理全网终端的文件；支持手工导入MD5+SHA1的黑白名单方式，支持txt批量导入方式；文件被加入白名单，客户端不再查杀，加入黑名单，客户端不可执行此文件；（提供功能截图，并加盖公司公章）支持下发忽略白名单的病毒扫描；支持对windows/Linux/国产操作系统终端的文件黑白名单和信任区在服务端统一管理; |
| 病毒查杀统计 | 要求支持通过数字签名或者文件名的方式分别显示文件，方便管理员管理全网终端上报的文件；（提供功能截图，并加盖公司公章） |
| 支持按病毒、木马、终端等维度统计全网病毒感染状况； |
| 要求支持对网内未知文件云查询的控制，可以选择直接连接互联网云查询中心查询，也可以选择采用私有云查杀引擎完成未知文件查询； |
| 要求上报文件至少包括:文件名称、发现时间、鉴定结果、文件大小、数字签名和文件所属源计算机等信息 |
| 压缩包杀毒 | 要求支持文件解压缩病毒查杀，支持对zip、rar、7z等多种格式的压缩文件查杀能力；（提供测试样本和测试方法）可对压缩包层级设置以节省终端计算资源； |
| 备份区隔离区管理 | 可对备份区、隔离区的文件进行有效管理。能够对单个、指定的文件和全部文件，进行文件的删除、恢复等多项管理措施。 |
| 敲诈者病毒防御 | 对敲诈者病毒提供防护机制，同时可提供相关解密工具，解密工具为自主研发；（提供功能截图，并加盖公司公章） |
| 多杀毒引擎 | 要求产品具备本地多引擎查杀能力，且引擎可配置；（提供功能截图，并加盖公司公章） |
| Linux、国产操作系统、云桌面杀毒 | 支持linux、国产操作系统、云桌面产品杀毒（提供产品截图，并提供至少2个厂商认证证书） |
| 私有云引擎 | 要求产品具备公有云与本地私有云检测能力； |
| 支持部署私有云查杀引擎，增强本地隔离网查杀效果； |
| 病毒库升级管理 | 要求支持服务器端病毒库的定时更新和手动更新两种升级模式。 |
| 要求支持客户端升级时对网络带宽的保护，可以设定服务器端最大升级带宽。（提供截图，并加盖单位公章） |
| 客户端补丁分发与漏洞修复 | 要求产品具有定时修复漏洞功能，同时可以设置筛选高危漏洞、软件更新、功能性补丁等修复类型； |
| 支持漏洞修复影响文档编辑时提醒功能； |
| 支持补丁下载安装顺序设置，可以有效节省漏洞修复时间与减少CPU占用； |
| 支持自定义补丁排除名单，防止终端打补丁后造成系统或业务进程崩溃； |
| 支持设置对特定分组优先进行补丁分发，一段时间后再全网升级 |
| 终端支持智能屏蔽过期补丁、与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁（要求提供截图）； |
| 产品具备漏洞集中修复，强制修复，自动修复；具备蓝屏修复功能（要求提供截图） |
| 要求产品生产公司具备热补丁修复功能（至少需要8个以上为用户提供Windows漏洞修复的热补丁列表） |
| 要求产品生产公司具备面向微软官方级别漏洞发现能力（提供2014年至今少20个以上微软漏洞发现案例，提供微软官方确认链接） |
| 产品具备漏洞集中修复过程中的流量控制和保证带宽,补丁分发支持服务端带宽限流与客户端P2P补丁分发加速，有效节省外网带宽资源（要求提供截图） |
| 客户端平台支持 | 支持服务器、PC、虚拟化的同台管理； |
| 至少支持3个以上Linux服务器版本并且可以和Windows统一管理； |
| 支持苹果MAC OS X系统的病毒防护功能； |
| 如果未来服务器端采用虚拟化技术进行业务升级，需要提供配套的解决方案用于服务器虚拟化的安全防护； |
| 产品资质要求 | 销售许可证；软件著作权； 涉密资质（天擎恶意程序辅助检测系统）；EAL2评级认证； |
| 其它服务 | 1、安排工程师负责统一安装杀毒软件系统。2、每个季度至少一次上门巡检服务，并出具安全巡检报告。3、提供7\*24小时服务，有突发安全问题，1小时内响应，2小时内到达现场处理问题。4、每月定时提醒网络安全风险及处置办法。 |

**招标内容:**

本次招标实施内容包括杀毒软件系统、软件安装、病毒库升级、运行巡检等一系列杀毒软件项目实施方案，包括对杀毒软件维护，软硬件基础环境安装调试和维护，基础数据准备，人员培训，售后服务和技术支持等内容。

投标人应在投标文件中详细提供实施所列中国科学院肿瘤与基础医学研究所需要的具体实施方法以及需要研究所相关配合方案。

## 2.2 商务要求

### 2.2.1 响应及培训

1.乙方提供7×24小时热线服务，并在接到甲方的故障申告电话后立即响应；故障申告时间以甲方电话申告的时间为准，故障消除时间以乙方提供的并经甲方确认的时间为准。

2.组织实施人员培训。

### 2.2.2 质保期

1.以项目验收合格之日起免费质保期3年并提供杀毒软件免费升级。

### 2.2.3 报价

1. 报价为总价报价（包含项目达到预期使用效果所需的一切费用，不再另行付费）

### 2.2.4 付款方式及合同续签

1. 合同款项支付：安装调试完成后，系统试运行正常并验收合格后，甲方内部审核完成后15个工作日内向乙方支付合同金额的95%，付款途径根据甲方财务规定的方式支付；
2. 在项验收合格满12个月后，甲方内部审核完成后15个工作日内向乙方支付合同金额的5%。甲方如需继续向乙方购买维保服务的，可经过友好协商签订维保合同，每年维保费不超过合同价10%。

# 第三章 响应文件编制要求

1. 响应文件分报价文件、技术商务文件，一式五份，一正四副。

2. 报价文件至少应包括以下内容（均需加盖公章）：

（1）按本文件内容报价（至少包含，名称、单价、数量、总价），并有大小写，计价单位人民币元；

（2）采购到货响应周期及相应优惠条件等；

（3）供应商需要说明的其他报价说明。

3. 商务文件至少应包括以下内容：证明其为合格供应商和所提供的为合格产品的有关资格证明文件，招标文件要求提供的其他资料等（均需加盖公章）：

（1）法人授权委托书；

（2）法定代表人及受委托人的身份证复印件；

（3）企业法人营业执照；

（4）所有资质及认证文件；

（5）主要业绩证明；

（6）供应商认为需要的其他商务文件或说明。

4. 技术文件至少应包括以下内容：针对本项目的技术和服务投标方案，招标文件要求提供的其他资料等（均需加盖公章）,偏离表：

（1）项目负责人简历表；

（2）拟派本项目人员技术力量配备情况；

（3）供应商应提供的技术资料；

（4）供应商需要说明的其他文件和说明。

# 第四章 合同范本

1、参考浙江省政府采购合同，细节可以另行协商约定；

2、具体内容签订合同时另行起草；