# 第一章 投标邀请

**项目概况**

QDF-V2016业务处理与综合服务平台互联网服务云托管项目招标项目的潜在投标人应在北京市海淀区海淀大街8号中钢国际广场16层**（以汇款形式支付标书款、电子邮件送达招标文件的方式发售。纸质招标文件和标书款发票的获取事宜详询采购代理机构项目联系人，如有不便，敬请谅解）**获取招标文件，并于2021年\_\_月\_\_日09点30分（北京时间）前递交投标文件。

## 一、项目基本情况

1.项目编号：2141STC31960

2.项目名称：QDF-V2016业务处理与综合服务平台互联网服务云托管项目

3.项目预算金额：225.4万元

4.采购需求：

| 包号 | 采购内容 | 最高限价 | 服务周期 | 服务地点 | 主要技术参数及招标数量 |
| --- | --- | --- | --- | --- | --- |
| 01 | QDF-V2016业务处理与综合服务平台互联网服务云托管 | 225.4万元 | 合同签订后2年 | 北京市东城区，招标人指定地点 | 拟选定一家服务商，在不中断现有业务的前提下完成QDF-V2016业务处理与综合服务平台互联网系统迁移工作以及互联网系统和业务处理系统安全的实时互联互通。具体要求详见招标文件第四章“采购需求书” |

5.合同履行期限：合同签订后2年。

6.本项目不接受联合体投标

## 二、申请人的资格要求（须同时满足）

1.申请人须为在中华人民共和国境内注册、响应招标、参加投标竞争的法人、其他组织或者自然人，满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求：

本项目01包不专门面向中小企业预留采购份额。

3.本项目的特定资格要求：

①申请人须具备有效期内的《增值电信业务经营许可证》；

②申请人须为中华人民共和国国家互联网信息办公室网站公布的《通过云计算服务安全评估的云平台》名单中的云服务商；

③申请人提供的云计算服务平台必须为中华人民共和国国家互联网信息办公室网站公布的《通过云计算服务安全评估的云平台》名单中的云平台且通过信息系统安全等级保护三级备案；

④本项目不接受联合体投标；

⑤本项目不接受进口产品投标；

⑥本项目不接受分公司、分所等分支机构参加投标；

⑦对于政府购买服务项目，公益一类事业单位、使用事业编制且由财政拨款保障的群团组织，不得作为承接主体；

⑧法律、行政法规、招标文件关于“合格投标人（申请人）”的其他条件。

## 三、获取招标文件

1.时间：2021年\_\_月\_\_日至2021年\_\_月\_\_日，每天上午9:00至12:00，下午13:00至17:00（北京时间，法定节假日除外）。

2.地点：为减少人员聚集，疫情期间我公司招标文件暂停现场发售，以电子邮件送达采购文件的方式发售。非常时期如有不便，敬请谅解。

3.方式：购买时请同时提供：

①申请人法定代表人授权书或单位介绍信。法定代表人（或单位负责人）本人前来购买时可提供法定代表人（或单位负责人）身份证明文件；

②购买人个人有效身份证件复印件；

③为便于及时通知有关项目信息并开具发票，请提供《申请人联系信息表》及《申请人开票信息表》签字件，请申请人自行前往中钢招标有限责任公司官网“帮助中心”栏目下载，下载地址为：http://tendering.sinosteel.com/）；

④标书款以汇款方式交纳。提供标书款的汇款单复印件，汇款单附言处须注明本项目“项目编号/包号”。

说明：申请人请以汇款方式邮件购买。将以上①～④项材料以及③项word格式电子版一并发送至“获取招标文件指定邮箱”。由于邮件众多，为保证购买人能及时获取招标文件，请在招标文件获取时间期限内、邮件发送后，主动与采购代理机构项目联系人确认是否收到以上资料。申请人为自然人时无需提供以上第①项材料。[“获取招标文件指定邮箱”为：panbh@sstc20.com](mailto:)。

售价：人民币500元/包。

## 四、提交投标文件截止时间、开标时间和地点

1.投标截止时间、开标时间：2021年\_\_月\_\_日09点30分（北京时间）。

2.开标地点：北京市海淀大街8号中钢国际广场16层会议室。

## 五、公告期限

本项目招标公告的期限为自本公告发布之日起5个工作日。

## 六、其他补充事宜

1.本项目的招标公告仅在中国政府采购网（www.ccgp.gov.cn）上发布。

2.本项目评标方法和标准：综合评分法，总分100分。

3.本项目需要落实的政府采购政策：节约能源、保护环境、促进中小企业及监狱企业发展、促进残疾人就业、使用信用记录结果、支持脱贫攻坚，政府采购政策具体落实情况详见招标文件。

4.标书款汇款银行信息

开户银行：中国民生银行股份有限公司北京大兴新城支行

银行账号：9576 0328 0000 0083

## 七、对本次招标提出询问，请按以下方式联系

1.采购人信息

名 称：外交部机关及驻外机构服务中心集中采购中心

地 址：北京市东城区干面胡同57号

联系方式：010-85179163

2.采购代理机构信息

名 称：中钢招标有限责任公司

地 址：北京市海淀区海淀大街8号中钢国际广场16层

联系方式：010-62688251

3.项目联系方式

项目联系人：潘炳衡、杨俏、张贺、孔伟

电 话：010-62688230、8226、8211、8251、

邮 箱：panbh[@sstc20.com](mailto:____@sstc20.com)

中钢招标有限责任公司

2021年\_\_月\_\_日

# 第三章 合同草案条款

（本章节所提供的文本为合同草案，具体签订合同以实际为准）

合同编号：

**QDF-V2016业务处理与综合服务平台互联网服务系统托管服务项目合同书**

甲方（买方）：北京千代福信息技术有限公司

乙方（卖方）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

签订日期：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

甲方与乙方就QDF-V2016业务处理与综合服务平台互联网服务系统托管服务项目相关事宜进行友好协商，根据《中华人民共和国民法典》的规定，按下述条款签订本合同。

**一、定义**

1.本合同下列术语解释：

1.1“合同”系指买卖双方所达成的协议，包括所有的附件、附录和构成合同的其他文件。

1.2“合同价”系指根据合同约定，卖方在完全履行合同义务后买方应付给卖方的价格。

1.3“甲方”系指北京千代福信息技术有限公司。

1.4“乙方”系指\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。

**二、合同内容及期限**

2.甲方购买乙方提供的以下服务：包括\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_租用服务在内的互联网服务系统托管服务，详见附件一：产品采购清单、附件二：投标文件。

2.1服务项目要求：

（1）乙方须服从甲方整体建设要求；

（2）乙方所提供的云计算服务平台需要根据《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文〔2014〕14号）要求，通过相关安全评估；

（3）乙方承诺项目经理及产品经理、技术经理等不经甲方同意不能无故更换，但因人员离职、疾病等原因导致的除外；

2.2提供服务地点：\_\_\_\_\_\_\_\_\_\_\_\_。

2.3本合同项目下的服务期限：自2021年\_\_\_\_月\_\_\_\_日起至\_\_\_\_年\_\_\_\_月\_\_\_\_日止。

**三、合同价款**

3.1本合同服务费总金额为：人民币\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（大写）圆整（￥\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_元）

3.2服务支出包括：\_\_\_\_\_\_公有云租用服务，详见附件一：产品采购清单。

3.3若甲方需对本项目进行扩容，乙方承诺并保证对于扩容单价至少维持本投标文件中承诺的折扣，并力争提供更优惠的折扣。

**四、支付和结算方式**

4.1双方因本合同发生的一切费用均以人民币结算及支付。项目费用为固定价格，合同内不作调整，如需调整，由双方达成相关补充协议。

4.2双方的帐户名称、开户银行及帐号以本合同提供的为准。

4.3付款方式：分期付款。

4.4第一次付款：自本合同生效后，乙方提交发票，甲方在履行完必要的手续后（不超过30个日历日），向乙方支付合同金额的60%，即人民币\_\_\_\_\_\_元（人民币大写：\_\_\_\_\_\_圆整）。（在未支付第一笔款项之前，不影响甲乙双方合同执行的效力。）

4.5第二次付款：项目验收完成后，乙方提交发票，甲方在履行完必要的手续后（不超过30个日历日），向乙方支付合同金额的40%，即共计人民币￥\_\_\_\_\_\_元（人民币大写：\_\_\_\_\_\_圆整）。

4.6甲方发票信息：

发票抬头：北京千代福信息技术有限公司

发票类型：增值税专用发票

开户银行：招商银行北京分行三里屯支行

银行账号：110906407210902

纳税人识别号（统一社会信用代码）：91110101685123117R

注册地址：北京市东城区南竹杆胡同2号1幢11层31201

**五、甲乙双方权利义务**

5.1甲方的权利和义务

5.1.1根据需要向乙方以书面形式下达工作任务。

5.1.2根据项目要求，监督乙方的服务质量。

5.1.3协调乙方在提供服务过程相关的政府部门和单位有关事宜。

5.2乙方的权利和义务：

5.2.1乙方可要求甲方按本合同的规定按时足额拨付项目经费。

5.2.2应依法独立完成的工作任务，未经甲方允许，不得以任何形式转包于其他机构。

5.2.3乙方应严格按照服务承诺完成相关工作。

5.2.4乙方对甲方提供的资料负有保密义务。

5.2.5乙方应针对甲方系统业务特点，提供完整配套的网络防护、安全检测、漏洞扫描、抵御黑客攻击和安全管家等安全服务，确保提供的网络安全服务符合信息系统安全等级保护三级备案。如乙方提供的服务不满足甲方安全防护要求，乙方应无条件按甲方要求进行整改，所涉及的相关费用由乙方自行承担。

**六、交付与验收**

6.1甲乙方项目交付进度、验收报告文档的确认：甲方授权甲方相关人员通过电子邮件（邮箱地址：jishubu@visaforchina.org）、乙方授权乙方相关人员通过电子邮件（邮箱地址：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_）对交付进度、验收文档、验收报告进行确认，前述人员的邮件确认行为代表双方的真实意思表示，对双方具有法律约束力。

6.2乙方应负责本项目下标的资源地分配和配置工作，于合同约定之日前完成上述工作，并负责制作、更新相关项目手册。

6.3乙方应书面通知甲方进行验收。甲方应在收到乙方验收申请后30日内对项目进行验收，若项目符合标的约定，甲方应出具验收报告；若项目不符合标的约定，乙方应按标的进行更改、优化。乙方应在通过验收7个工作日内，向甲方提供完整的与上述工作相关的技术文档和配置参数。

**七、知识产权和使用权**

7.1知识产权和使用权归属：

双方各自享有的商标权、著作权或者其他知识产权，均仍归各方单独享有，并不会因为双方签订或者履行本协议而转归对方享有，或者转归双方共同享有。

7.2 乙方应保证，甲方在使用乙方提供的服务或与服务配套的货物时，免受第三方提出的侵犯其专利权、商标权或工业设计权等的起诉。如果任何第三方提出侵权指控，卖方须与第三方交涉并承担由此发生的一切责任、费用和经济赔偿。

**八、履约保证金和预付款保证金**

8.履约保证金

8.1乙方在合同签订后且甲方付款前，向甲方提供相当于合同总价5%的履约保证金。

8.2乙方的履约保证金将在合同执行完成并且甲方完成支付后15个工作日内提交退款手续办理退保证金事宜。

8.3乙方以履约保函的形式向甲方提供履约保证金。

**九、违约责任**

9.1因乙方原因导致合同标的无法实现或未按规定时间提供服务的，则每延迟一天应向甲方支付合同总金额0.3‰的违约金。乙方应支付违约金的最高金额不超过合同总金额的20%。逾期超过30日的，甲方有权发出书面通知解除合同。发生合同解除时，乙方应退还甲方已支付的合同款，甲方有权要求乙方支付合同总金额20%的违约金。

9.2若乙方在合同履行过程中提出单方面中止、解除合同，则甲方有权选择要求乙方继续履行，并承担迟延履行的违约责任，或者在乙方支付合同总金额的20%的违约金，并退还全部已支付款项的情况下，选择解除合同。

9.3在符合合同约定的付款条件的情况下，甲方延迟付款，每逾期一日，乙方有权要求甲方按照应付金额的0.3‰的比例向乙方支付违约金。逾期超过30日的，乙方有权解除合同，并要求甲方支付已完成的工作对应的款项。甲方应支付违约金的最高金额不超过合同总金额的20%。

9.4如出现乙方违约情况，甲方有权将乙方根据合同约定应向甲方支付的违约金直接从甲方根据本条应向乙方支付的款项中直接扣除。

9.5在相关法律所允许的最大范围内，任何一方均不就另一方附带、间接的、偶然的损失承担责任。

**十、不可抗力**

10.1不可抗力指下列事件：战争、动乱、瘟疫、严重火灾、洪水、地震、风暴或其他自然灾害、疫情等，以及本合同各方不可预见、不可防止并不能避免或克服的一切其他因素及事件。

10.2任何一方因不可抗力不能履行本合同规定的全部或部分义务，该方应尽快通知另一方，并须在不可抗力发生后三日内以书面形式向另一方提供详细情况报告及不可抗力对履行本合同的影响程度的说明。就上述不可抗力的发生须由受到不可抗力影响的一方负责同时提供由公证机关做出的公证证明。

10.3发生不可抗力事件，任何一方均不对因不可抗力无法履行或迟延履行本合同义务而使另一方蒙受的任何损失承担责任。但遭受不可抗力影响的一方有责任尽可能及时采取适当或必要措施减少或消除不可抗力的影响。遭受不可抗力影响的一方对因未尽本项责任而造成的相关损失承担责任。

10.4合同各方应根据不可抗力对本合同履行的影响程度，协商确定是否终止本合同，或是继续履行本合同。

**十一、联系方式**

11.1合同双方发出与本合同有关的通知或回复，应以专人送递、传真或特快专递方式发出；如果以专人送递或特快专递发送，以送达至对方的住所地或通讯联络地为送达；如果以传真方式发送，发件人在收到传真报告后视为送达；如果采用电话或电子邮件的方式，则应在发送后由对方以书面方式予以确认。

11.2合同双方发出的与本合同有关的通知或回复均应发至合同条款专用部分中的通讯地址，付款或收款应使用合同条款专用部分中的帐号，一方变更通讯地址或帐号，应自变更之日起三个工作日内，将变更后的地址通知对方。变更方不履行通知义务的，应对此造成的一切后果承担法律责任。

上述发出通知、回复的费用由发出一方承担。

**十二、保密条款**

12.1任何一方对其获知的本合同及附件中其他各方的商业秘密和国家秘密负有保密义务。

12.2在下列情形下：当发布中标公告和其它公告时，当国家机关调查、审查、审计时，以及其他符合法律规定的情形下，无须事先征求甲方/乙方同意而可以披露关于采购过程、合同文本、签署情况的资料、甲方/乙方的名称及地址、采购内容的有关信息以及补充条款等，但应当在合理的必要范围内。对任何已经公布过的内容或与之内容相同的资料，以及甲方/乙方已经泄露或公开的，无须再承担保密责任。

12.3此外的其它情形下，除非法律、法规另有规定或得到本合同之其他各方的书面许可，任何一方不得向第三人泄露前款规定的商业秘密和国家秘密。保密期限自任何一方获知该商业秘密和国家秘密之日起至本条规定的秘密成为公众信息之日止。

**十三、合同的解释和法律适用**

13.1任何一方对本合同及其附件的解释均应遵循诚实信用原则,依照本合同签订时有效的中国法律、法规以及通常的理解进行。

13.2本合同标题仅供查阅方便，并非对本合同的诠释或解释；本合同中以日表述的时间期限均指自然日。

13.3对本合同的任何解释均应以书面做出。

13.4本合同及附件的订立、效力、解释、履行、争议的解决等适用本合同签订时有效的中华人民共和国法律、法规的有关规定。

**十四、合同的终止**

14.1本合同因下列原因而终止：

14.1.1本合同正常履行完毕。

14.1.2合同双方协议终止本合同的履行。

14.1.3不可抗力事件导致本合同无法履行或履行不必要。

14.1.4任何一方行使解除权，解除本合同。

14.2转移协助

（1）本合同期届满或者因乙方原因导致甲方终止合同的，乙方应采取一切必要与合理方式将处于乙方管理下的应归甲方所有的硬件、软件产品以及甲方业务数据等，及时转移并交付给甲方或者甲方指定的第三方，所需费用已经包括在本合同价款内，甲方无须为此另行向乙方付费。

（2）因甲方原因导致乙方终止合同的，乙方应采取一切必要与合理方式将处于乙方管理下的应归甲方所有的硬件、软件产品以及甲方业务数据等，及时转移并交付给甲方或者甲方指定的第三方，但甲方应当为此支付合理费用。

（3）若甲方希望乙方在本合同终止或届满时协助甲方将乙方根据本合同提供的服务转移至甲方、甲方关联公司或第三方时，应甲方合理的书面要求，乙方按照以下方式向甲方提供该转移协助：

（3.1）乙方同意使用其当时在本合同下提供服务的现有人员来提供该等甲方要求的转移协助并且不超过本合同到期日或终止之日起计30日；

（3.2）若一方提供转移协助时需要使用乙方当时用于提供服务的资源以外的其他或额外的服务或资源，则该等转移协助的要求应视作新增服务。

14.3对本合同终止有过错的一方应赔偿另一方因合同终止而受到的损失。对合同终止双方均无过错的，则各自承担所受到的损失。

**十五、权利的保留**

15.1任何一方没有行使其权利或没有就违约方的违约行为采取任何行动，不应被视为是对其权利的放弃或对追究另一方违约责任权利的放弃。任何一方放弃针对违约方的某种权利，或放弃追究违约方的某种责任，不应视为对其他权利或追究其他责任的放弃。

15.2如果本合同部分条款依据现行有关法律、法规被确认为无效或无法履行，且该部分无效或无法履行的条款不影响本合同其他条款效力的，本合同其他条款继续有效；同时，合同双方应根据现行有关法律、法规对该部分无效或无法履行的条款进行调整，使其依法成为有效条款，并尽量符合本合同所体现的原则和精神。

**十六、争议的解决**

16.1合同双方应通过友好协商解决因解释﹑执行本合同所发生的和本合同有关的一切争议。如果经协商不能达成协议，则双方同意按照16.1.1约定处理：

16.1.1在甲方住所地有管辖权的人民法院提起诉讼；

16.1.2由贸易仲裁委员会根据其现行有效的仲裁程序进行仲裁。仲裁裁决为最终裁决对双方均具有约束力。

16.2本合同甲、乙双方一致认为，本合同仅属于甲、乙双方之间的协议，任何争议均只应当按照本合同的约定方式处理，任何情形下采购代理机构均不应当成为该等争议的当事人，无论该等仲裁或诉讼均不得针对采购代理机构提起。

16.3在争议解决期间，除了诉讼或仲裁进行过程中正在解决的那部分问题外，合同其余部分应继续履行。

**十七、合同的补充修改和变更**

17.1双方协商一致，可以对本合同进行补充、修改或变更。

17.2对本合同的补充、修改或变更必须以书面形式进行。补充、修改或变更的协议的签署及生效方式与本合同的签署及生效方式相同。

17.3招投标文件及其全部条款、双方签订的补充协议以及修改或变更的条款与本合同具有同等法律效力。

**十八、合同的生效**

18.本合同经双方法定代表人（负责人）或授权代表签字并加盖单位公章后生效。

**十九、交接**

19.甲方有权在不迟于本合同期届满或者根据本约定终止本合同前3个月通知乙方启动交接工作。

**二十、其他约定事项**

20.1本合同中的附件均为本合同不可分割的部分，与本合同具有相同的法律效力。

20.2一方当事人未经另一方事先书面同意，不得将其在合同项下的权利或义务全部或部分转让给第三人，有关分包事项或服务委托等须遵守相关法律、法规。

20.3本合同正本一式肆份，甲、乙双方各执贰份，每份正本具有同等法律效力。

甲乙双方签字盖公章：

甲方：北京千代福信息技术有限公司

地址：北京市东城区南竹杆胡同2号1幢11层31201

电话：010-85208121

开户银行及帐号：招商银行北京分行三里屯支行

法人或授权代表：（签名）

\_\_\_\_\_年\_\_\_月\_\_\_日

乙方：

地址：

电话：

开户银行及帐号：

法人或授权代表：（签名）

\_\_\_\_\_年\_\_\_月\_\_\_日

附件一：产品采购清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 服务名称 | 单位 | 数量 | 产地 | 服务期限 |
| 1 | 云服务器 | 台 | 15 | 国产 | 2年 |
| 2 | 云数据库Cassandra | 节点 | 3 | 国产 | 2年 |
| 3 | Redis数据库服务 | 套 | 1 | 国产 | 2年 |
| 4 | 文件存储（NAS） | 套 | 1 | 国产 | 2年 |
| 5 | 云日志存储服务 | 套 | 1 | 国产 | 2年 |
| 6 | 负载均衡 | 套 | 1 | 国产 | 2年 |
| 7 | 公网IP服务 | 套 | 2 | 国产 | 2年 |
| 8 | 公网及网站静、动态内容全球加速服务 | 套 | 1 | 国产 | 2年 |
| 9 | NAT网关 | 条 | 1 | 国产 | 2年 |
| 10 | SSL VPN网关 | 条 | 2 | 国产 | 2年 |
| 11 | 专线网络接入服务 | 条 | 2 | 国产 | 2年 |
| 12 | 云主机安全服务 | 台 | 15 | 国产 | 2年 |
| 13 | 云防火墙服务 | 套 | 1 | 国产 | 2年 |
| 14 | 云Web应用防火墙服务 | 套 | 1 | 国产 | 2年 |
| 15 | 云DDoS攻击防护服务 | 套 | 1 | 国产 | 2年 |
| 16 | 云堡垒机服务 | 套 | 1 | 国产 | 2年 |
| 17 | 云数据库审计Cassandra | 套 | 1 | 国产 | 2年 |
| 18 | 云数据加密服务 | 套 | 1 | 国产 | 2年 |
| 19 | 云验证码服务 | 套 | 1 | 国产 | 2年 |
| 20 | SSL证书 | 套 | 1 | 国产 | 2年 |
| 21 | 云迁移咨询及实施服务 | 套 | 1 | 国产 | 1次 |
| 22 | 云安全专家服务 | 套 | 1 | 国产 | 2年 |
| 23 | 云平台支持和运维服务 | 套 | 1 | 国产 | 2年 |

# 第四章 采购需求书

## 一、项目概述

**1.1项目背景**

QDF-V2016业务处理与综合服务平台是我公司的业务系统。该平台由互联网服务子系统（简称“互联网系统”）和专网业务处理系统（简称“业务处理系统”）两个子系统构成。

互联网系统承担着面向全球的互联网服务，主要包括信息发布等。业务处理系统承担着业务处理的职能，运行于企业广域专网。互联网子系统和业务处理系统业务上相衔接贯通，数据通过安全的方式实施互联互通。

互联网系统目前托管在第三方机房的私有化环境，因现有托管服务将于2021年12月19日到期，为保障互联网系统持续稳定、安全运行，须完成互联网系统公有云托管服务采购，并保证在业务不中断的前提下完成相关系统迁移工作以及互联网系统和业务处理系统安全的实时互联互通。

**1.2项目目标**

鉴于近年来我国云计算技术快速发展，安全性、稳定性大为提升且具有快速弹性、低成本等特点，能够满足我系统业务发展需要。在系统现有互联网机房托管服务终止前，须完成相关信息系统的迁移、初步改造工程，并达成如下目标。

（1）业务连续性：互联网系统业务工作不间断开展，相关信息系统能够安全、稳定运行，为全球用户提供7\*24小时互联网信息服务。

（2）系统对接：互联网系统平台于公有云环境搭建，此次采购的托管服务需与业务处理系统进行无缝衔接，做到资源合理复用。

（3）提升网络访问速度和用户体验：利用云厂商互联网全球加速服务，通过将访问请求动态调配接入部署于海外的网络节点，大幅提升申请人访问我门户网站动、静态内容的访问速度，提升用户体验。

（4）安全合规：互联网系统迁移完成后，须完成备案并通过国家安全等级保护三级测评。

（5）改造升级：整体基于云计算技术进行升级改造，打下坚实基础。

**1.3项目内容**

项目具体需要的技术与服务包括如下：

（1）云资源与第三方机房的互联链路，保证在公有云平台运行互联网系统与在第三方机房私有化部署内部业务处理子系统互联互通。

（2）利用云资源弹性扩展的优势，设计和部署整体支撑环境，承载千代福互联网系统。

（3）将现有互联网托管机房运行的相关系统通过成熟的技术和工程方法，完成应用从私有化环境向公有云服务的搬迁。

（4）保证系统云平台环境与原机房托管环境并轨运行一段时间后，原托管机房业务逐步退出，完全转为新环境运行。

（5）安全防护需求。针对系统业务特点，提供完整配套的网络防护、安全检测、漏洞扫描、抵御黑客攻击和安全管家等安全服务。

**1.4需求分析**

采用云上的IaaS服务形式提供高可用、多种性能实例选择、可弹性伸缩的云主机服务；PaaS中的数据库及存储服务提供系统所需的数据库及存储的支撑；依托云厂商部署于全球的优质网络接入节点，实现申请人互联网访问流量全球范围就近接入网络加速节点，大幅减少网络延迟、丢包，提升传输效率，提高互联网应用系统的访问体验；搭建第三方机房与公有云的互联专线，建立安全实时传输机制；设计云上合理网络架构以安全运行相关应用系统；按切换时间要求完成应用系统上云迁移，进行必要的试运行；建设后续持续云上运行操作规范。

## 二、技术要求

**2.1采购产品服务一览表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务名称** | **单位** | **数量** | **产地** | **服务期限** |
| 1 | 云主机服务 | 台 | 15 | 国产 | 2年 |
| 2 | 云数据库Cassandra | 节点 | 3 | 国产 | 2年 |
| 3 | Redis数据库服务 | 套 | 1 | 国产 | 2年 |
| 4 | 文件存储（NAS） | 套 | 1 | 国产 | 2年 |
| 5 | 云日志存储服务 | 套 | 1 | 国产 | 2年 |
| 6 | 云负载均衡服务 | 套 | 1 | 国产 | 2年 |
| 7 | 公网IP服务 | 套 | 2 | 国产 | 2年 |
| 8 | 互联网加速服务 | 套 | 1 | 国产 | 2年 |
| 9 | NAT网关 | 条 | 1 | 国产 | 2年 |
| 10 | SSL VPN网关 | 条 | 1 | 国产 | 2年 |
| 11 | 专线网络接入服务 | 条 | 2 | 国产 | 2年 |
| 12 | 云主机安全服务 | 台 | 15 | 国产 | 2年 |
| 13 | 云防火墙服务 | 套 | 1 | 国产 | 2年 |
| 14 | 云Web应用防火墙服务 | 套 | 1 | 国产 | 2年 |
| 15 | 云DDoS攻击防护服务 | 套 | 1 | 国产 | 2年 |
| 16 | 云堡垒机服务 | 套 | 1 | 国产 | 2年 |
| 17 | 云数据库审计Cassandra | 套 | 1 | 国产 | 2年 |
| 18 | 云数据加密服务 | 套 | 1 | 国产 | 2年 |
| 19 | 云验证码服务 | 套 | 1 | 国产 | 2年 |
| 20 | SSL证书 | 套 | 1 | 国产 | 2年 |
| 21 | 云迁移咨询及实施服务 | 套 | 1 | 国产 | 1次 |
| 22 | 云安全专家服务 | 套 | 1 | 国产 | 2年 |
| 23 | 云平台支持和运维服务 | 套 | 1 | 国产 | 2年 |

**2.2产品详细指标要求**

注：

（1）指标按重要性分为“★”、“▲”、“#”。“★”代表实质性指标，不满足该指标项将导致投标被拒绝，“▲”代表关键指标，“#”代表一般指标。

（2）有效证明材料要求：投标人须提供包含相关指标项的证明材料，证明材料包括但不限于相关资质证书、生产厂家官方网站截图、产品白皮书、第三方机构检验报告、原厂对系统功能的承诺函、原厂商授权函或其他相关证明材料，并加盖投标人公章，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。

#### 2.2.1技术资质要求

★（1）投标人须具备有效期内的《增值电信业务经营许可证》（提供有效证明材料）

★（2）投标人提供的云平台必须为中华人民共和国国家互联网信息办公室网站公示的通过云计算服务安全评估的云平台（提供有效证明材料）

★（3）投标人提供的云平台通过信息系统安全等级保护三级备案（提供有效证明材料）

#### 2.2.2云主机服务

指标要求：

★（1）本项目提供的云主机规格为（提供有效证明材料）：

①4台CPU≥16核，内存≥32G,系统盘≥100GB SSD,数据盘≥200GB SSD，含兼容RedHat7操作系统；

②2台CPU≥16核，内存≥32G,系统盘≥150GB SSD,数据盘≥300GB SSD，含正版Windows server 2008R2（64位）操作系统；

③1台CPU≥4核，内存≥8G,系统盘≥150GB SSD,数据盘≥300GB SSD，含正版Windows server 2012R2（64位）操作系统；

④4台CPU≥8核，内存≥16G,系统盘≥150GB SSD,数据盘≥300GB SSD，含正版Windows server 2008R2（64位）操作系统；

⑤2台CPU≥8核，内存≥16G,系统盘≥100GB SSD,数据盘≥200GB SSD，云厂商提供长期支持的正版操作系统，兼容RedHat7.X操作系统；

⑥2台CPU≥8核，内存≥32G,系统盘≥100GB SSD,数据盘≥200GB SSD，云厂商提供长期支持的正版操作系统，兼容RedHat7.X操作系统；

云厂商应按以上规格要求提供云虚拟服务器资源，上述规格为云主机最低配置要求，需支持未来性能可平滑扩展。

▲（2）服务能力

①单台云主机系统盘最高可支持1024GB，最高可挂载16块弹性硬盘作为数据盘、单盘最高可达16TB；（提供有效证明材料）

②单台云主机最高可挂8个弹性网卡、单卡最高可绑定IP数30个；

③单台网络优化云主机最高包转发率（PPS）达到600W；

④单台主机内网带宽最高支持25Gbps；

⑤单台云主机创建时间小于10s，1000台云主机创建时间小于60s。

▲（3）操作系统（提供有效证明材料）

云主机提供主流的Windows、Linux等操作系统，均具备正版授权，授权费用需包含在本次投标报价中；

▲（4）快照（提供有效证明材料）

支持实例快照，可灵活配置快照时间和保存期限；

▲（5）云主机备份（提供有效证明材料）

支持全量备份和增量备份；支持针对任意快照时间点进行回滚；单云盘可保留≥4个快照，备份周期≥1个月；

#（6）监控（提供有效证明材料）

①能实现主机性能监控，包括但不限于内存利用率、内外网带宽、磁盘读写IOPS和通过宿主机采集上报的CPU使用率等；

②可实现对实例执行定期检查，监控实例的健康状态，提供监控数据收集、可视化以及实时监控告警等服务；

#（7）数据可靠性（提供有效证明材料）

云盘应采用三副本机制，对应数据存储的可靠性达99.9999999%；

▲（8）宕机重启恢复（提供有效证明材料）

在发生物理机非预期宕机或进行主动运维时，应支持自动重启恢复；

#（9）网络访问控制

支持云主机的安全域划分，可通过安全组规则配置，达到控制云主机网络访问出入流量的目的；

#（10）自定义镜像（提供有效证明材料）

①可指定用户预先配置好的镜像文件作为模板进行云主机的创建，支持自定义镜像跨地域复制；

②可导入RAW、VHD、QCOW2格式镜像，并且基于导入镜像创建云主机；

③支持镜像跨地域复制、支持跨账号共享镜像；

④支持在线、离线主机服务迁移；

#（11）管理功能（提供有效证明材料）

①支持使用密钥登录和密码登录；

②支持通过Workbench、VNC登录、远程桌面登录以及远程登录软件登录；

③支持计算能力的弹性伸缩，可根据定时、周期或监控策略，增加或减少云服务器实例；

④支持通过API或CLI管控控制云服务器；

#（12）加密（提供有效证明材料）

云盘支持加密存储，提供针对数据盘的数据加密功能，由加密数据盘创建的快照继承加密属性；加密通过云服务供应商提供的密钥管理服务来实现，客户无需构建和维护自己的密钥系统，即可实现简单高效的数据盘加解密功能；支持国密算法；

#（13）数据可销毁性

云厂商在客户要求删除数据或设备被弃置、转售前必须将其所有数据彻底删除，确保这些数据无法被复原，需提供最高级别的数据销毁，应包括但不限于数据覆写、硬盘消磁、硬盘分解等常见销毁手段；

#（14）数据可迁移性

云厂商应保证用户启用或弃用相关云服务时，用户能够自主控制数据的迁入和迁出；

#（15）数据私密性

云厂商应支持用户通过各种加密或隔离手段保证使用同一物理资源池的用户数据互不可见。不同用户的云主机至少要通过网络隔离的方式，保证同一云数据中心的用户数据互不可见，互不可访问；

#（16）数据知情权

按用户要求提供数据存储、备份的物理位置，并及时通知用户直接或间接使用了用户数据的事件以及实体信息。

#（17）可用性（提供有效证明材料）

云主机服务采用全冗余架构，无单点故障，平均可用性≥99.95%；

#（18）灵活性

支持无需关机调整实例配置；

#### 2.2.3云数据库Cassandra

指标要求：

★（1）规格（提供有效证明材料）

提供Cassandra数据库PaaS服务方案，需与原生Apache Cassandra 3.11.X社区版100%兼容，需提供≥3个节点的数据库实例，每节点最低规格配置为20C\*64G\*560G（SSD盘）；

或提供裸金属数据库支持方案，所提供的方案需包含裸金属服务器4台（3台实例加1台冷备资源），每台最低配置规格为：CPU20C、内存64G、系统盘2块SSD，每块≥600G、数据盘两块SSD，每块≥900G、网络带宽≥10Gbps,CPU不低于Intel 志强金牌6148 处理器，操作系统兼容Redhat7.X，并安装Apache Cassandra 3.11.X社区版及lucense索引；资源支持平滑扩展；

▲（2）弹性扩容（提供有效证明材料）

支持分钟级的水平弹性扩容、升降配；单集群最大节点数≥50个节点；

▲（3）数据备份（提供有效证明材料）

①支持通过灵活的备份策略生成多个备份副本数据，支持全量&增量联机备份恢复；

②支持线上恢复30天以内的数据，支持将数据导出或同步至其他可用区或线下数据中心实例；

#（4）安全加固能力（提供有效证明材料）

支持链路加密SSL/TLS；设置安全IP白名单，接入IP限制；

#（5）数据迁移（提供有效证明材料）

支持全量数据加增量数据的业务不停服的前提下完成数据库迁移工作；

#（6）监控（提供有效证明材料）

支持资源和异常问题监控配置及短信告警。

▲（7）数据库专家服务（提供有效证明材料）

提供Cassandra数据库专家技术支持服务。

#（8）可用性（提供有效证明材料）

支持7\*24\*365使用，SLA可用性≥99.95%。

#### 2.2.4Redis数据库服务

指标要求：

★（1）规格（提供有效证明材料）

提供Redis数据库服务需兼容社区Redis4.x/5.x版本，支持主从架构，内存8G；

▲（2）弹性扩容（提供有效证明材料）

支持分钟级弹性扩展，支持跨版本升级，支持无需停止业务的变配及升级；

#（3）灵活性

支持控制台一键迁移，灵活资源调配；

#（4）可用性（提供有效证明材料）

支持7\*24\*365使用，SLA可用性≥99.95%；

#### 2.2.5文件存储（NAS）

指标要求：

★（1）规格（提供有效证明材料）

支持NFSv3.0/v4.0，SMB2.1/3.0协议的共享文件挂载到云主机服务；文件存储容量≥5TB

▲（2）权限控制及访问隔离（提供有效证明材料）

支持按照客户端进行读写权限控制和访问隔离；

▲（3）数据加密（提供有效证明材料）

支持文件系统数据存储加密和传输加密；

#（4）数据备份（提供有效证明材料）

支持通过灵活的备份策略生成多个备份副本数据，在发生数据损坏时进行恢复；

#（5）服务能力（提供有效证明材料）

支持存储容量在线弹性扩展，无需中断业务。

#（6）可用性（提供有效证明材料）

支持7\*24\*365使用，SLA可用性≥99.95%。

#### 2.2.6云日志存储服务

指标要求：

★（1）规格（提供有效证明材料）

提供SaaS化的日志查询、统计、采集及存储服务，支持Log/Metric/Trace统一采集，支持云主机、负载均衡及应用的日志数据接入；存储容量≥1T；

▲（2）查询分析（提供有效证明材料）

支持关键词、SQL92等多种方式查询，支持面向文本加结构化数据实时查询分析，可提供异常巡检与智能分析服务；

#（3）可用性（提供有效证明材料）

支持7\*24\*365使用，SLA可用性≥99.95%；

#### 2.2.7云负载均衡服务

指标要求：

★（1）规格（提供有效证明材料）

提供SaaS化负载均衡服务，单集群负载均衡最大连接数≥100000，每秒新建连接数≥10000，每秒查询数≥10000；支持≥5个后端应用集群，支持按路径或端口号转发，可根据业务负载横向伸缩，弹性扩展应用系统对外的服务能力；

▲（2）支持协议（提供有效证明材料）

支持TCP、UDP、HTTP、HTTPS等协议；

#（3）会话保持

支持会话保持功能，在会话的生命周期内，可以将同一客户端的请求转发到同一台后端服务器上。

#（4）健康检查

可按照指定规则对配置的云服务器进行健康检查，自动隔离异常状态云服务器。支持流量监控&告警。

#（5）七层能力

①支持七层个性化配置。

②支持七层重定向功能（rewrite）。

③支持七层日志存储。

#（6）IPv6支持

①支持IPv6负载均衡实例。

②支持IPv6 NAT64负载均衡实例。

#（7）在线升级

支持在线平滑升级，承载能力和网络总带宽同步线性扩容。

#（8）绑定能力

支持绑定公网IP。

▲（9）安全防护（提供有效证明材料）

支持端到端https加密，支持https卸载；

#（10）流量健康和告警

支持流量监控和告警

#（11）同城容灾

支持跨多可用区容灾部署。

#（12）调度策略

支持根据不同的域名和URL进行流量调度，提升应用系统灵活性。

#（13）可用性（提供有效证明材料）

采用全冗余架构，无单点故障，支持7\*24\*365使用，SLA可用性≥99.95%。

#### 2.2.8公网IP服务

指标要求：

★（1）规格（提供有效证明材料）

云厂商提供至少2个互联网访问IP，每个IP带宽≥30Mbps；

▲（2）灵活性（提供有效证明材料）

提供访问公网和公网访问能力；可与云资源的生命周期解耦合，单独进行操作；

▲（3）扩展性（提供有效证明材料）

带宽支持分钟级升降配及扩容，最大带宽可支持≥500Mbps

#（4）可用性

支持7\*24\*365使用，SLA可用性≥99.95%（提供有效证明材料）

#### 2.2.9互联网加速服务

指标要求：

★（1）规格（提供有效证明材料）

提供云原生的、全球访问的、≥30Mbps带宽的互联网加速服务，需包括全球加速能力和相关网络接入需要的软硬件、线路；

▲（2）基本要求（提供软著或知识产权证明）

云厂商提供的互联网加速网络服务为投标方自有产品；

▲（3）基础功能（提供有效证明材料）

①支持网络服务在全球范围就近接入服务商部署的加速节点，提升用户访问网络速度，降低网络访问响应时间；

②网络加速的源站可以关联不同的后端云实例及用户自定义的源站地址；

③能够联动内容分发网络（CDN）实现回源加速；

▲（4）网络节点覆盖（提供有效证明材料）

云厂商能够提供动态加速服务的区域应包括北美、欧洲、亚洲等区域；云厂商部署于全球的网络节点应覆盖全球六大洲，全球拥有≥2000+节点；

▲（5）网络质量（提供有效证明材料）

任意海外节点到云平台主机端的响应延迟≤300ms；

#（6）协议支持

支持HTTP2.0、HTTPS协议加速；

#（7）网络安全（提供有效证明材料）

网络加速服务自带抗DDoS能力，同时也能集成DDoS和WAF等云原生安全能力，保护互联网服务免受攻击，加固对终端节点的安全访问；

#（8）可用性（提供有效证明材料）

支持7\*24\*365使用，SLA可用性≥99.95%；

#（9）扩展性（提供有效证明材料）

加速带宽支持分钟级升降配及扩容，最大带宽可支持≥500Mbps；

#### 2.2.10NAT网关

指标要求：

★（1）规格（提供有效证明材料）

提供SaaS化NAT网关服务，为部署于云内专有网络中无公网IP的云主机实例提供访问公网的代理服务；支持SNAT和DNAT功能，支持多个主机共享公网IP；最大连接数≥50,000；最大新建连接数≥5,000。

#（2）基础功能

支持同一个云区域内创建多个NAT网关；

#（3）可用性（提供有效证明材料）

支持7\*24\*365使用，SLA可用性≥99.9%

#### 2.2.11 SSL VPN网关

指标要求：

★（1）规格（提供有效证明材料）

提供SaaS化部署的SSL VPN网关服务；带宽规格≥5Mbps，SSL连接数≥5；

▲（2）基础功能（提供有效证明材料）

支持使用IKE和IPsec协议对传输数据进行加密，保证数据安全可靠；支持基于OpenVPN架构，Internet终端通过SSL-VPN拨号安全接入VPC；支持SSL VPN及国密算法；

#（3）基础功能（提供有效证明材料）

采用双机热备架构，故障时秒级切换，保证会话不中断，业务无感知；

#（4）可用性（提供有效证明材料）

支持7\*24\*365使用，SLA可用性≥99.9%；

#### 2.2.12专线网络接入服务

指标要求：

★（1）规格（提供有效证明材料）

在云服务区域和业务系统机房之间提供2条总带宽≥20Mbps的网络接入服务；

#（2）可用性（提供有效证明材料）

支持7\*24\*365使用，SLA可用性≥99.9%；

#### 2.2.13云主机安全服务

指标要求：

★（1）规格（提供有效证明材料）

提供SaaS化部署的云主机安全服务，包括云虚拟资源及数据库实例资源的木马文件检测、密码破解检测、登录行为审计、漏洞检测等主机安全防护功能；无需改变客户网络结构，即开即用

▲（2）漏洞检测修复（提供有效证明材料）

提供常见的黑客攻击程序检测，包括但不限于DDos木马、远控、挖矿类软件；

▲（3）病毒云查杀（提供有效证明材料）

提供常用的Web网站类脚本木马后门检测，包含ASP/PHP/JSP/Python等脚本语言；提供对二进制可执行类的病毒木马检测，包括 exe、dll、bin 等类型文件，并告警用户；

#（4）基本功能（提供有效证明材料）

①可对暴力破解行为进行告警，包括SSH、RDP等，提供爆破阻断功能。

②可实时对非白名单的IP地址登录进行告警，识别出恶意登录行为，支持白名单配置。

③针对本地提权行为实时告警，并支持白名单配置。

④针对反弹shell行为实时告警，并支持白名单配置。

⑤记录主机上执行的bash命令，实时监控被审计规则判断为危险的操作。提供默认规则配置，以及支持用户自定义规则配置。

⑥对系统级漏洞和常用组件类型的漏洞进行检测，提供修复方案，例如：Apache、Nginx、Structs、Redis等常用组件。

⑦提供常用Web类型的漏洞检测，提供修复方案，例如：phpMyAdmin、WordPress等Web类组件。

⑧漏洞预警情报服务，在爆发1day漏洞时，可及时推送检测规则。

⑨支持等保二级、三级、CIS、弱口令等基线检测，并提供修复方案。

⑩实时监控网络攻击行为，支持检测威胁类型：Webshell探测、Struts漏洞利用、代码注入攻击、命令注入攻击、机器批量控制利用等。

▲（5）管理功能（提供有效证明材料）

①支持全量日志分析包括网络、主机、云产品等；支持用户统一查询、导出安全事件日志信息；

②支持一键补丁修复功能；

③支持进行大版本、查杀引擎、病毒库、漏洞库的升级和更新，功能增强和完善优化；

#（6）自动化攻击溯源

支持自动化定位攻击源、攻击链、入侵原因，并以可视化的形式展示

#（7）性能

主机安全代理资源消耗低，不影响系统正常运行，CPU＜5%，内存＜30M。

#（8）稳定性

系统应有高可靠性、稳定性设计。在出现异常情况时，可进行降级、自杀等机制，确保业务的正常运行。

▲（9）兼容性（提供有效证明材料）

兼容Windows 、CentOS、Debian、RedHat等主流操作系统。

#（10）可用性（提供有效证明材料）

支持7\*24\*365使用，SLA可用性≥99.95%

#### 2.2.14云防火墙服务

指标要求：

★（1）规格（提供有效证明材料）

提供云原生的SaaS化防火墙服务，无需客户部署镜像资源，内置高可靠，性能可平滑扩展；

▲（2）互联网边界防御（提供有效证明材料）

支持互联网边界、VPC边界、主机边界流量管控与安全防护

▲（3）访问控制（提供有效证明材料）

支持互联网到业务和业务与业务之间流量的网络入侵行为和网络攻击行为检测能力；

▲（4）云资源隔离防御（提供有效证明材料）

支持基于虚拟机颗粒度的微隔离策略（安全组）统一管理，支持安全组高危策略检查，支持安全组配置关系与流量的可视化展示；

#（5）入侵拦截

集成IPS和虚拟补丁能力，可以对来自互联网的攻击进行实时拦截；

#（6）防火墙开关

互联网暴露面一键检测，一键开启云防火墙防护；

#（7）互联网开放端口自动发现（提供有效证明材料）

支持一键梳理云平台的互联网暴露面梳理，并可联动漏洞扫描能力，判断暴露端口和同步漏洞，并进行漏洞防护闭环；

#（8）告警中心

支持外部入侵和主机失陷的告警，对被防火墙阻断的流量进行统计分析；

#（9）流量中心

支持外部访问和主机外联流量进行统计分析；

#（10）地域位置的策略

支持基于地理位置的访问控制，可设置一键拦截海外IP的策略；

#（11）域名的策略

支持基于云主机主动外联的访问控制，支持基于域名的访问控制；

#（12）策略命中数

支持策略的命中数统计，方便管理员进行日常分析管理冗余策略；

#（13）防护模式（提供有效证明材料）

入侵防御可支持观察模式和拦截模式，拦截模式支持分级拦截，包括宽松、严格、中等模式；

#（14）威胁情报

集成云平台的威胁情报，对于恶意源IP、危险域名的访问流量，进行精准识别；

#（15）虚拟补丁

针对热门漏洞、常见漏洞、高危漏洞的热补丁防护功能，无需在业务系统中安装真实补丁；

#（16）访问控制日志

支持对全部命中防火墙访问控制策略的流量进行记录；

#（17）入侵防御日志

支持对全部命中入侵防御策略的流量进行记录，并记录入侵的payload供后续分析取证；

#（18）流量日志

支持对全部经过防火墙的流量进行记录；

#（19）操作日志

支持对防火墙的操作记录日志；

#（20）可用性（提供有效证明材料）

支持7\*24\*365使用，SLA可用性≥99.95%；

#### 2.2.15云Web应用防火墙服务

★（1）规格（提供有效证明材料）

提供SaaS化Web应用防火墙服务，至少支持1个一级域名、10个二级域名、带宽≥30Mbps；性能可平滑扩展；

▲（2）部署模式（提供有效证明材料）

无需本地部署，支持全球多节点集群容灾部署；

▲（3）协议支持（提供有效证明材料）

支持协议类型包括HTTP、HTTPS、WEBSOCKET、WEBSOCKETS，支持泛域名、支持非标端口；

#（4）防护延迟

防护节点要求采用≥30线的BGP IP链路接入；

#（5）智能检测引擎（提供有效证明材料）

支持AI+规则双检测引擎，交叉验证，精准有效捕捉各类常规Web攻击，0day攻击及其它新型未知攻击；

#（6）Web攻击防护（提供有效证明材料）

可防御SQL注入、命令注入攻击、XSS跨站脚本攻击、WebShell木马上传、文件包含、路径穿越类攻击、非法的HTTP协议请求、网页防篡改、常见Web服务器漏洞等攻击；

#（7）0day漏洞检测（提供有效证明材料）

主动检测并及时发现高危Web漏洞、0day漏洞，并生成针对漏洞的防护规则；

#（8）网页防篡改（提供有效证明材料）

支持网页防篡改功能，云端备份网站核心内容页面，保障网页内容不会因为源站安全事故而被篡改；

#（9）自定义精准防护（提供有效证明材料）

支持精细化基于IP、URL路径、Referer、UA参数的自定义防御规则，设置Web攻击防护措施，且不限制自定义防御规则数；

▲（10）反爬虫能力（提供有效证明材料）

支持对WAF发起短时间集中Web攻击的IP自动封禁；支持防目录遍历；支持对时间、访问频率、封禁时长的自定义设置；支持对常见扫描器的渗透测试拦截；支持无需用户修改代码即可接入图形或滑块验证码；

▲（11）Bot行为管理

①支持针对请求中的常见头部字段，如IP，URL、UserAgent、Referer或者参数中出现的Bot恶意特征，进行组合配置和访问控制；（提供有效证明材料）

②支持Bot行为管理，Bot策略设置，已知类型预设、自定义策略功能，并提供产品界面截图证明；

#（12）一键封禁（提供有效证明材料）

支持基于全球地理位置的区域IP封禁；

#（13）IPV6地址防护

支持IPV6的业务安全防护；

#（14）攻击报表（提供有效证明材料）

支持防护数据后台统计功能，包括攻击源IP、攻击目标、攻击URL、攻击方式等内容，统计日志可下载导出；

#（15）高级CC防护

支持针对请求路径访问频率的识别及控制；支持触发条件开启“封禁访问”或“人机识别”策略模式，支持自定义惩罚时长；

#（16）可用性（提供有效证明材料）

支持7\*24\*365使用，SLA可用性≥99.95%；

#### 2.2.16云DDoS攻击防护服务

指标要求：

★（1）规格（提供有效证明材料）

云厂商提供至少对2个公网IP、不限次数的DDoS防护能力；防火流量≥10Gbps,弹性防护≥50Gbps,业务带宽≥30bps；提供BGP高防包、BGP高防IP等多种DDoS解决方案;

▲（2）基本要求（提供有效证明材料）

提供的DDos攻击防护服务为厂商自有产品；

▲（3）DDoS防护（提供有效证明材料）

①支持包括但不限于SYN Flood、ACK Flood、ICMP Flood、UDP Flood、NTP Flood、SSDP Flood、DNS Flood、HTTP Flood等攻击类型；

②支持600Gbps的保底防护能力；

#（4）CC防护（提供有效证明材料）

支持CC攻击防护功能，提供不低于100万QPS的CC防护；

#（5）高级安全策略（提供有效证明材料）

支持协议禁用、端口禁用、报文特征过滤、拒绝海外流量、空连接防护功能；

#（6）CC自定义策略（提供有效证明材料）

支持自定义策略，进行限速及过滤；支持配置CC触发阈值，避免特殊时期业务受影响；

#（7）自主解封（提供有效证明材料）

支持因超过防护阈值被封堵时，自助解除封堵的功能；

#（8）黑白名单（提供有效证明材料）

支持黑白名单功能；

#（9）协议支持

支持TCP、UDP、HTTP、HTTPS等协议，支持泛域名；

#（10）转发回源

支持IP及域名两种回源方式；

#（11）安全报表

支持提供实时精准的流量报表及攻击详情信息，至少包括：网络出入库流量趋势、攻击类型、攻击IP、攻击次数、攻击峰值等信息；

#（12）告警

①当发生相关安全事件，支持主动进行告警，告警信息包括攻击开始、攻击结束、IP封堵及解除封堵；

②支持短信、邮件、微信等多种告警方式；（提供有效证明材料）

#（13）安全联动（提供有效证明材料）

支持和云平台上云Web应用防火墙进行联动，保护业务安全；

#（14）IPv6支持（提供有效证明材料）

支持IPv6业务防护；

#（15）可用性（提供有效证明材料）

支持7\*24\*365使用，SLA可用性≥99.95%；

#### 2.2.17云堡垒机服务

指标要求：

★（1）规格（提供有效证明材料）

提供SaaS化堡垒机服务，支持通过SSLVPN或千代福专线访问；

▲（2）用户管理（提供有效证明材料）

支持用户多角色划分功能，对各类角色进行细粒度的权限管理；

▲（3）访问控制（提供有效证明材料）

支持用户安全策略配置功能，如密码锁定次数、密码有效期、密码复杂度、用户登录IP范围等；支持用户登录双因素或多因素认证；

▲（4）资源管理（提供有效证明材料）

支持SSH、TELNET、FTP、SFTP、VNC、XWINDOW等协议；

#（5）设备管理

①支持对设备批量添加主机账号、修改运维IP类型和运维端口，提高主机管理效率；

②支持登录设备IP、运维协议、端口号、账号、密码、用户、用户组的权限导出；

#（6）身份认证要求（提供有效证明材料）

支持与短信网关平台进行联动，实现短信动态口令双因素认证机制；

#（7）字符审计（提供有效证明材料）

对字符命令方式的访问可以审计到所有交互内容，可以还原操作过程的命令输入和结果输出；

#（8）图形审计（提供有效证明材料）

图形资源访问时，支持键盘、剪切板、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、文件传输记录的指定位置开始回放；

#### 2.2.18云数据库审计Cassandra

指标要求：

▲（1）规格（提供有效证明材料）

提供支持云数据库中Cassandra PaaS服务的3个数据库实例或裸金属服务的4个数据库实例的数据库安全审计服务；

▲（2）数据库攻击实时动态检测（提供有效证明材料）

针对数据库所在主机、数据库本身的网络攻击行为实时检测，支持对SQL注入、数据库漏洞攻击、远程命令执行等攻击方式，对任何尝试的攻击操作都会产生告警；支持用户界面告警、邮件、短信等多种方式告警；

▲（3）数据库支持（提供有效证明材料）

支持本项目涉及数据库的安全审计；

▲（4）报表功能（提供有效证明材料）

提供告警报表、通知报表、SQL注入报表、批量数据访问行为报表；

#### 2.2.19云数据加密服务

指标要求：

★（1）规格（提供有效证明材料）

提供SaaS化数据加密服务，支持密钥托管和调用；

▲（2）基本密钥管理（提供有效证明材料）

①用户可创建、启用、禁用、删除、别名、轮转用户主密钥，支持对用户主密钥的生命周期管理；

②用户可创建、加密、解密数据密钥，支持国密算法；

#（3）一键集成加密能力（提供有效证明材料）

提供与其他云服务一键集成加密能力，包括云盘、文件存储、对象存储、数据库；

#（4）可用性（提供有效证明材料）

支持7\*24\*365使用，SLA可用性≥99.95%；

#### 2.2.20云验证码服务

★（1）规格（提供有效证明材料）

提供SaaS化网站访问验证码服务；支持滑块或图形验证、支持多语言，并发峰值≥900qps,每小时验证量≥20000次，可平滑扩展；

▲（2）基本要求（提供有效证明材料）

云验证服务为云厂商自有产品；

#（3）多平台的防控（提供有效证明材料）

支持PC端Web和移动端平台的风险防控；

#（4）风险二次验证（提供有效证明材料）

对于正常请求，一次通过；对恶意请求，直接拦截；对高风险请求，进行二次再验证；

#（5）可用性（提供有效证明材料）

支持7\*24\*365使用，SLA可用性≥99.95%；

#### 2.2.21SSL证书

★（1）证书类型（提供有效证明材料）

提供适合政府组织使用、全球各国家均承认的SSL证书；

▲（2）重新颁发

不限次数颁发证书；

▲（3）多年服务

支持多年服务；

**2.3服务要求**

注：

（1）指标按重要性分为“★”、“▲”。★代表最关键指标，不满足该指标项将导致投标被拒绝，▲代表重要指标。

（2）有效证明材料要求：投标人须提供包含相关指标项的证明材料，证明材料包括但不限于相关资质证书、生产厂家官方网站截图、产品白皮书、第三方机构检验报告、原厂对系统功能的承诺函、原厂商授权函或其他相关证明材料，并加盖投标人公章，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。

#### 2.3.1云迁移咨询及实施服务

★（1）人力资源要求（提供有效证明材料）

提供不少于30人天的云迁移咨询及实施服务；迁移咨询团队负责设计系统上云后整体架构，包括网络、应用、安全及容灾备份架构；实施服务团队负责提供互联网系统迁移到云的具体实施方案设计，保证现有数据资源、系统架构和系统进行资源整合及平滑迁移和过渡。要求方案经济可行，且投标方负责实施并完全承担相应的迁移成本；

★（2）专家支持（提供有效证明材料）

云迁移部署实施过程中，云厂商需要指派自有技术专家团队提供技术支持服务,包括云主机、网络、安全及Cassandra数据库等领域至少一名专家支持；

#### 2.3.2安全专家服务

★（1）安全产品配置指导（提供有效证明材料）

提供5\*8的安全产品配置指导及在线安全咨询服务，包含但不限于云防火墙、高防、云WAF、态势感知等

★（2）安全评估服务（提供有效证明材料）

每年进行一次云上业务安全评估，并提供一份云上业务安全书面建议方案；

▲（3）安全扫描

新业务上线前提供一次安全扫描，一次复扫；每季度进行一次全面扫描。

▲（4）安全监控与巡检

每天提供一次全面巡检，每周发送安全巡检周报

▲（5）安全事件应急

提供每年4次服务范围内业务（已完成扫描和评估）的安全入侵事件7\*24小时电话响应；

#### 2.3.3云平台支持和运维服务

★（1）监控服务（提供有效证明材料）

监控服务：提供7\*24小时的云平台监控服务。提供项目涉及的云资源监控，有监控平台的登录权限，可以通过监控平台实时查看系统的监控信息，监控内容包括CPU，内存，网络等；

★（2）服务网络（提供承诺书）

投标人需提供不少于5人的服务团队支持，且保证服务团队人员可1小时内到达客户现场。

▲（3）运维方式受理时间（提供有效证明材料）

热线电话支持，7×24小时；

官网在线咨询，7×24小时；

人工服务7×15小时（早9-晚24）；

工单支持：7×24小时；

▲（4）专家会诊（提供有效证明材料）

严重问题时，需要云主机、存储、安全、网络等各领域专家进行疑难应急会诊；

响应时间：业务不可用＜10分钟；一般问题＜60分钟；一般咨询＜4小时；

★（5）故障恢复（提供有效证明材料）

因云厂商提供的资源和服务导致的严重系统宕机和严重安全问题，云厂商需承诺在6小时内提供解决方案；

★（6）数据库专家服务（提供有效证明材料）

提供7\*24小时Cassandra数据库专家服务；

▲（7）培训服务（提供有效证明材料）

提供本次云产品不少于10人天的厂商认证的工程师产品实操培训课程。涵盖本项目使用的各种云产品。

★（8）扩容单价折扣（提供有效证明材料）

投标人须承诺未来扩容单价的折扣不超过本次投标单价的折扣；

## 三、实施方案

注：

投标人须按以下要求提供相关证明材料。证明材料可以使用生产厂家官方网站截图、原厂商服务授权函或其他相关证明材料，并加盖原厂公章。

**3.1迁移能力要求**

（1）具备具备丰富从非云原生环境向云环境迁移服务实践经验和能力；

（2）具备多厂商硬件、云、系统平台、应用、中间件等云化迁移评估、集成设计、实施经验；

（3）具备多种数据库以及中间件整合迁移技术交付经验；具备跨平台迁移方案设计、性能规划方法和经验。

**3.2迁移方案要求**

（1）含根据待迁移的应用关联性来规划的迁移批次计划；

（2）业务系统云迁移场景分类详细、合理，且迁移方案科学，与本次搬迁需求符合；

（3）明确定义割接步骤、责任分工界面（包括应用厂商及买方）、割接报告模板和回退方案；

（4）明确定义风险识别、风险评估、风险等级及风险应对措施；

**3.3项目实施过程控制**

具备完善的流程，包括项目启动会议、提交项目计划、评估系统现状、涉及迁移方案、实施迁移服务、验收迁移项目；

**3.4项目实施过程安排**

（1）项目启动阶段，完成团队组建，输出项目计划；

（2）评估分析阶段，完成需求分析、信息收集，输出迁移策略；

（3）规划设计阶段，完成迁移流程规划、方案设计、应以预案，完成技术上的准备；

（4）实施迁移阶段，完成实施研讨、迁移工具部署、工具测试、迁移演练、应用软件调测和业务验证，最终完成业务割接；

（5）迁移验收阶段，完成验收方案制定、监控和实施验收；

**3.5项目验收安排**

（1）提供《业务迁移方案》，《项目迁移计划》等文档材料；

（2）业务系统完成迁移工作，运行10个自然日；

# 第五章 评标标准

| **序号** | **项目** | **评分标准** | **分值** |
| --- | --- | --- | --- |
| （一）  商务部分  （10分） | 投标人企业实力 | 投标人具有有效期内的：  ①信息系统安全管理体系认证证书（ISO27001）；  ②个人信息安全管理体系认证证书（BS10012）；  ③具有隐私信息管理体系认证证书(ISO27701)；  ④信息技术服务管理体系认证证书（ISO20000）；  ⑤云安全管理体系认证证书（ISO27017）。  以上每提供1项得2分，最高得10分。  注：投标人提供以上有效的认证证书复印件并加盖公章，否则评审时不予认可。 | 10 |
| （二）  技术部分  （80分） | 项目经理 | 根据投标人拟派项目经理实力进行评分，担任本项目的项目经理需同时满足如下条件：  ①具备本科及以上学历；  ②具备7年及以上工作经验（以毕业证书时间作为起始日期计算）；  ③具备高级信息系统项目管理师证书或PMP认证证书。  满足上述3项要求的得3分，一项不满足则该项不得分。  注：须提供项目经理身份证复印件、学历及资质证书复印件、开标前半年内任意1个月在本单位缴纳社保的证明材料，并加盖投标人公章，否则评审时不予认可，证明材料不完备不得分。 | 3 |
| 服务团队 | 根据投标人拟派本项目服务团队人员进行评分，拟派主要技术管理人员（除项目经理除外）须≥10人，拟派主要技术管理人员＜10人的此项不得分。  资质情况需满足：  ①具备高级系统架构设计师认证证书≥1人；  ②具备高级系统分析师认证证书≥1人；  ③具备高级软件架构师认证证书≥1人；  ④高级信息系统项目管理师认证证书≥1人。  以上证书每提供一项得1，最多得4分。同一技术人员具备多个证书按照一个计算，不重复计分。  ⑤具有Cassandra数据库开发经验；  提供使用Cassandra数据库项目产品的软件著作权证书及投标单位出具的工程师参与项目证明文件得1分，未提供或不满足不得分。  注：须提供拟派本项目服务团队人员身份证复印件、资质证书复印件、开标前半年内任意1个月在本单位缴纳社保的证明材料，并加盖投标人公章，否则评审时不予认可，证明材料不完备不得分。 | 5 |
| 数据与业务迁移服务 | 根据投标人提供现有系统与服务迁移到云平台的衔接、切换的服务方案，对现状了解清晰能够充分利用现有资源，在迁移过程中保证数据与服务的可靠和系统平稳过渡进行评分。服务方案内容全面，对现状了解清晰，迁移过程中保障措施合理并承诺提供服务得7分；服务方案内容满足项目要求，对现状基本了解，迁移过程中保障措施较合理并承诺提供服务得5分；服务方案内容欠缺，对现状了解不全面，迁移过程中保障措施完整得3分；服务方案内容欠缺，或未承诺提供服务得1分； | 7 |
| 项目建设进度管理服务 | 根据投标人提供针对本项目的项目建设进度提供管理服务，包括项目人员安排、时间节点、事务的安排等进行评分。服务方案内容完整，人员安排合理、时间节点科学得7分；服务方案内容较完整、人数安排较合理、时间节点较科学得5分；服务方案内容一般完整、时间安排科学得3分；服务方案内容不完整得1分； | 7 |
| 采购需求指标响应情况 | 根据投标人响应“▲”及“#”指标情况进行打分。以投标人提供的有效证明材料为审核依据（投标人须提供包含相关指标项的证明材料，证明材料包括但不限于相关资质证书、生产厂家官方网站截图、产品白皮书、第三方机构检验报告、原厂对系统功能的承诺函、原厂商授权函或其他相关证明材料，并加盖投标人公章，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理）全部指标无偏离或正偏离响应得满分，每有一项“▲”负偏离扣2分，最多扣20分。每有一项“#”负偏离扣1分，最多扣20分。负偏离指标共计超过20项按无效投标处理。 | 40 |
| 数据库服务解决方案 | 根据投标人提供的数据库解决方案符合客户需求、部署架构、安全架构、数据结构规划合理，方案完整、功能完善，数据库可扩展性强、稳定性强，易维护，能提供针对Cassandra数据库PaaS服务方向的比较全面的设计和描述等进行评分。投标人提供的数据库解决方案为提供全面的Cassandra PaaS能力，且技术方案实现功能合理，完全满足需求得6分；投标人提供的数据库解决方案为提供全面的Cassandra PaaS能力，但部分指标不满足得4分；投标人提供的数据库解决方案为提供裸金属服务器支持Cassandra数据库能力，且方案完整，裸金属服务器配置高于标准配置，功能完善得2分；投标人提供的数据库解决方案为提供裸金属服务器支持Cassandra数据库能力，且方案较完整，裸金属服务器配置符合标准配置，功能较完善得1分；投标人不能提供Cassandra PaaS能力，也无高性能裸金属服务器部署环境，只能提供IaaS服务的得0分； | 6 |
| 互联网加速服务技术 | 根据投标人的互联网加速服务技术指标进行评分。投标人提供的互联网加速服务解决方案完全满足需求，方案合理，内容全面，所覆盖得海外节点完全符合需求得6分；投标人提供的互联网加速服务解决方案较合理，基本满足要求，覆盖海外节点完全符合需求得4分；投标人提供的互联网加速服务解决方案较合理，可满足部分要求，海外节点部分符合需求得2分；投标人提供的互联网加速服务解决方案不满足要求，或无法提供网络加速服务得1分。 | 6 |
| 内外网数据安全交互技术指标 | 根据投标人的内外网数据安全交互技术指标进行评分。投标人提供的数据交互方案完全满足需求，内容全面，方案合理，安全合规，无单点故障，可以支持弹性扩展，得6分；投标人提供的数据交互方案可以满足基本数据交互需求，安全合规，得4分；投标人提供的数据交互方案基本满足基本数据交互需求，得2分；投标人提供的数据交互方案不满足需求得1分。 | 6 |
| （三）  价格部分  （10分） | 价格权重 | 价格得分的计算：  本项目价格权重为：10分  投标人报价得分的计算采用低价优先法，按如下公式进行计算：  投标人报价得分=（满足招标文件要求且响应价格最低的投标人评标价/投标人评标价）×价格权重  投标人报价为所投包次中全部产品的单价合计。  注：投标人评标价为根据《投标人须知》23.3条规定调整后的响应报价。 | 10 |
| 总分 | | (一)~(三)项得分之和，即为供应商的综合得分 | 100 |