海淀区云计算中心服务项目合同

项目名称：海淀区云计算中心服务项目

买方（甲方）：北京市海淀区大数据中心

卖方（乙方）：中国电信股份有限公司北京分公司

合同编号：

签订地点：北京市海淀区

目　录

合同正文

依据《中华人民共和国民法典》以及国家其他有关法律、法规的规定，甲、乙双方在遵循平等自愿、诚实信用的原则下，就乙方向甲方提供云计算中心服务事宜经协商达成一致意见，签订本合同，并共同遵守。

第一条 合同各方

甲方：北京市海淀区大数据中心

乙方：中国电信股份有限公司北京分公司

第二条 合同术语定义和解释

云计算服务：云计算服务是一种处理能力可弹性伸缩的计算服务，其管理方式比物理服务器更简单高效。云服务器帮助用户快速构建更稳定、安全的应用，降低开发运维的难度和整体 IT 成本，使用户能够更专注于核心业务创新。

海淀区云计算中心：甲方依托乙方提供的基础设施环境、资源以及服务部署专享的政务云计算中心，为海淀区政府提供政务信息化资源服务。

云服务：海淀区云计算中心提供的虚拟机、存储服务、数据库服务等业务系统云服务。

AI 算力：用于支撑人工智能算法分析和应用智能化场景需求的分析能力。

第三条 服务内容

本项目以购买服务的方式按甲方需求购买业务系统云服务和 AI 算力服务，由乙方在北京市海淀区中国电信永丰数据中心为甲方单独准备的专属政务云机房提供海淀区云计算中心服务项目的服务。乙方具体服务内容及要求如下：

3.1 专属机房服务

1）乙方在北京市海淀区中国电信永丰数据中心为甲方提供专属机房，应提供远程实时的监控系统，对专属机房的情况进行实时监控。

2）乙方为本项目提供的机房配置后备柴油发电机组及其配电线路，其容量必须满足整个机房的所有基础设施供电，其储油量应满足柴油发电机组满负荷至少运行 8 小时。

3）提供专用的门禁和 24 小时视频监控系统。

4）提供 7*24 小时热线人工值守以及响应服务。

5）提供的机房环境满足等级保护 2.0 三级要求及商用密码应用安全性评估要求。

3.2 云计算服务

1）提供的云平台为国产化平台，服务器芯片（CPU）、数据库、操作系统符合安全可靠测评要求。云平台能够适配和兼容主流的国产化芯片，同时考虑过渡阶段业务系统对非国产化资源的需求，需具备非国产化资源管理及服务能力。

2）提供的云平台产品应具备支持一云多芯的能力，能够同时支持国产化芯片服务器环境和非国产化芯片服务器运行环境。

3）提供云平台产品与中国信息安全测评中心（国家保密科技测评中心）公布的安全可靠测评结果中的至少三个品牌中央处理器（CPU）兼容性证明文件。

4）提供的云管理平台需要基于国产化服务器环境运行。

3.2.1 云主机服务

1)云主机服务应能同时支持国产化芯片服务器及非国产化芯片服务器，技术上能够支持国产化芯片服务器包括：中国信息安全测评中心（国家保密科技测评中心）公布的安全可靠测评结果中的至少三个品牌中央处理器（CPU）。

2)提供可弹性伸缩的计算服务，根据业务需要，可随时创建或释放任意多台云主机，提升运维效率。

3)支持创建、删除、启动、关闭、查看（含批量）云主机操作。

4)支持挂载/卸载磁盘、挂载/卸载网卡、配置、更改安全组操作。

5)支持用户数据注入、密码和密钥对、安全组、VNC 登陆能力。

6)支持全局镜像、私有镜像以及共享镜像三种权限维度的镜像使用模式，且支持管理员将租户的自定义镜像转换为全局镜像，可界面化进行“自定义镜像跨地域复制”，支持镜像转换，自定义镜像转换为公共镜像。

7)支持常见镜像格式的镜像导入，如 VHD、VMDK、QCOW2、QCOW、RAW 等多种格式。

8)弹性伸缩配置支持按照 CPU 利用率、内存利用率、内网出带宽、内网入带宽、外网出带宽、外网入带宽来创建触发策略。支持定时触发和伸缩组实例移除保护。

3.2.2 裸金属服务

1)提供 3 台国产化裸金属服务器，配置为 2*32 核，16*32G 内存，1 块 480GSSD 硬盘，4 块 960SSD 硬盘，1 个 HBA 卡（(支持 RAID10)，2 个万兆端口。

2)裸金属服务应能同时支持国产化芯片服务器及非国产化芯片服务器；技术上能够支持国产化芯片服务器包括：中国信息安全测评中心（国家保密科技测评中心）公布的安全可靠测评结果中的至少三个品牌中央处理器（CPU）。

3)支持对裸金属服务进行创建、开机、关机、重启、销毁、重装操作系统操作。

4)支持裸金属服务的管理、配置和查询裸金属服务器连接交换机信息。

5)支持裸金属服务器按租户进行 VPC 网络和资源隔离。

6)支持裸金属服务器和虚拟机实例在同一个 VPC 私有网络。

7)支持负载均衡服务挂载裸金属服务器，对内网或外网提供服务访问。

8)支持自动化安装监控 agent。

9)支持默认告警策略和自定义配置告警策略。

3.2.3 云数据库

1)能同时支持国产化芯片服务器及非国产化芯片服务器。

2)数据库以分布式架构进行设计，由多个不同的（物理或虚拟的）节点共同组成一个逻辑上统一的分布式数据库实例。

3)支持在相同可用区和跨可用区的部署方案下，设置主从节点的数据一致性的能力，支持选择异步、强同步和强同步可退化模式，支持强一致，避免异常情况下的数据丢失或错乱。

4)支持虚拟租户实例能力，可以在一组物理集群中，虚拟出多个相互资源隔离（如 CPU、内存、磁盘 IO 等）的数据库实例，每个实例都可为业务系统提供功能完整的数据库服务且独立管理。

5)支持独享集群模式，可以在一组物理集群中，创建出一个或多个某租户（账号）独占的更小规模的物理独占的小集群。并能在这些小集群中分配实例；

6)高度兼容 MySQL/MariaDB 协议和语法。

7)支持水平拆分、分区表（二级分区）、事务能力。

8)提供高可用架构，支持多地多中心架构、防脑裂、免切机制、闪回/回档自主恢复机制等能力。

9)支持在线扩容/缩容、计算节点与存储节点均可水平线性扩容能力、自动化巡检和演练能力。

10)支持全局性能检测、sql 优化建议、实时性能检测、读写分离等能力。

11)支持防止误删机制、慢速删除、实例内置 sql 防火墙等安全能力。

12)支持数据库监控、集群健康、自定义告警能力、支持错误日志、调试日志等。

13)支持跨地域或跨集群实例的数据同步。

14)支持根据用户实际需要，自定义实例的副本数，支持最多一主五从的实例。

3.2.4 云存储

3.2.4.1 云硬盘服务

1)支持分布式存储架构，提供三副本强一致架构能力。

2)支持在线扩容、快速扩容、在线备份和回滚，支持数据随机读写、在线迁移、在线调整云硬盘类型；其中在线迁移过程中无需云主机关机或业务中断。

3)支持创建、删除、查看、挂载、卸载。

4)支持基于已有云硬盘创建云硬盘快照/备份，支持通过云硬盘快照/备份回滚源云硬盘，支持通过云硬盘快照/备份创建新云硬盘。

5)根据不同的后端存储介质（如 SATA 与 SSD 盘混合、纯 SSD 盘），云硬盘服务应具备提供多种不同性能规格的云硬盘类型的能力。

6)支持同可用区内多种 CPU 架构节点的存储池，实现一云多芯；任一种 CPU 架构的存储池均可以为不同 CPU 架构的计算节点提供块存储服务。

7)分布式存储集群支持多个独立的存储仓库，每一个仓库为独立故障域，单一存储仓库出现灾难性故障时，不能对其它存储仓库有任何影响。

8)云硬盘支持跨后端分布式存储集群的在线迁移能力，迁移过程无需云主机关机或业务中断。

3.2.4.2 对象存储服务

1)支持存储对象的复制，包括简单复制与分块复制;支持对象下载能力；支持删除对象能力，包括单个与批量删除;支持列出指定存储桶内的对象文件。

2)对象查询展现,显示对象文件的详细情况：文件名、大小、链接、ETag、访问权限、Header 头。

3)支持通过 ACL 对存储对象进行访问控制，设置对象的默认权限；支持对象客户端加密,支持 SSE-C 方式的服务端加密。

4)支持对象标签能力，对对象设置标签，根据标签对对象进行分组管理。

5)支持将存储桶归属到不同的项目资源组，实现存储桶的精细化资源管理能力，支持按项目过滤存储桶，按项目维度授权不同的账号可管理相应项目的存储桶。

6)支持防盗链，用户可以通过控制台的防盗链功能配置黑/白名单，对数据资源进行安全防护。

3.2.5 网络服务

3.2.5.1 互联网链路服务

1)提供互联网接入，互联网总带宽扩展能力大于 10Gbps，提供按需付费方式，带宽

调整步长 10Mbps，提供对应的 IP 地址服务。

2)提供2对10Gbps裸光纤接入端口,用于以裸光纤形式与海淀区政务外网进行对接。

3.2.5.2VPC 服务

1)支持通过 VPC，灵活设置网络地址空间，实现私有网络隔离，多个虚拟网络之间（同城、跨城）稳定高速对等互通。

2)提供子网、路由表、安全组、网络 ACL、对等连接能力。

3)支持有状态的虚拟化防火墙，可实现对云服务器、弹性网卡等资源的流量出方向和入方向的精细化管控。

3.2.5.3 弹性负载均衡服务

1)支持弹性负载均衡服务通过将同一区域的多台云主机虚拟成一个组，设置一个内网或外网的服务地址，将前端并发访问转发给后台多台云主机服务器，实现应用程序的流量均衡。

2)负载均衡服务还通过故障自动切换及时地消除服务的单点故障。

3)支持公网和私网负载均衡、支持四层（TCP/UDP）和七层负载均衡（HTTP/HTTPS）;

4)支持轮询/最少连接/源 IP 分发策略、支持会话保持、支持按域名和 URL 转发;

5)支持后端服务器为裸金属服务器、支持按监听器粒度监控相关指标、HTTP 重定向到 HTTPS。

6)支持跨可用区流量分发;

7)支持负载均衡器管理、监听器管理、健康检查管理。

3.2.5.4 弹性公网 IP 服务

1)弹性公网 IP 为用户提供公网带宽服务。

2)支持将弹性公网 IP 与云主机等实例绑定或解绑，为用户访问公网提供 IP 地址和公网带宽。

3)支持不同租户不同弹性公网 IP 地址池。支持白名单方式使用静态 IP 的服务。

4)支持配置上下行带宽限制。

3.2.5.5NAT 网关服务

1)NAT 网关为云主机服务提供网络地址转换服务。

2)支持 SNAT，支持多个云主机通过同一公网 IP 主动访问互联网。

3)支持 DNAT，支持绑定到 NAT 网关，NAT 网关通过与弹性公网 IP 绑定。

4)支持可以设置自定义流量告警。

5)支持设置NAT网关管理、SNAT规则管理、DNAT规则管理。

3.2.5.6VPN服务

1)支持创建、查看、删除、修改VPN网关。

2)支持创建、查看、删除、修改VPN连接。

3)新增、查看、删除监控指标和数据，并可以设置告警规则。

3.2.6云中间件

3.2.6.1云容器服务

1)支持在国产化芯片服务器及非国产化芯片服务器的部署；技术上能够支持国产化芯片服务器包括：中国信息安全测评中心（国家保密科技测评中心）公布的安全可靠测评结果中的至少三个品牌中央处理器（CPU）。

2)云容器服务支持和云平台VPC网络、云负载均衡、分布式云存储、云监控、权限管理等云产品和功能模块进行无缝集成。

3)支持控制台可视化和YAML等编辑形式。支持以数据卷的形式挂载到容器目录或导入成环境变量。创建ConfigMap时支持通过文件导入的方式。

4)容器服务与路由管理，支持联动云负载均衡来提供工作负载的4层Service和7层Ingress；支持云负载均衡直连Pod模式。

5)容器集群运维支持丰富的监控指标，包括集群、节点、工作负载、Pod、容器多维度的资源监控。提供自定义监控告警指标，设定阈值及触发策略。

6)支持用户在控制台上按需对容器集群开启“集群审计”功能，开启后支持查看集群的“审计总览”、“节点操作概览”、“K8S操作对象概览”、“聚合检索”、“全局检索”，查看的维度包括操作用户数、异常访问次数、敏感操作次数、操作趋势、操作分布等。

7)权限管理支持通过账号和授权系统进行权限管理。控制台上提KubernetesRBAC的授权模式，支持对子账号进行细粒度的访问权限控制。

3.2.6.2消息中间件Kafka

1)支持在国产化芯片服务器及非国产化芯片服务器的部署；技术上能够支持国产化芯片服务器包括：中国信息安全测评中心（国家保密科技测评中心）公布的安全可靠测评结果中的至少三个品牌中央处理器（CPU）。

2)完全兼容开源KafkaAPI（0.11、2.4、2.8版本）。

3)支持数据多副本容灾，保证数据高可靠性性。

4)支持在线平滑升配，包括峰值带宽，磁盘容量，以及创建的主题（Topics）和分区（Partitions）个数，升级服务不中断。

5)支持对服务实例和主题进行实时监控和自定义告警策略，包括生产消费流量，生产消费消息个数，磁盘堆积量等。

6)支持对租户内用户进行实例和主题的安全策略配置，实现对用户的权限进行精细化的控制。

7)支持服务实例的消息保留时间配置，满足对安全性要求更高或有审计要求的数据持久化的需求。

8)提供精细化的 ACL 控制能力，支持按照用户+IP 段控制访问权限，权限配置支持到实例+主题维度，而且支持黑名单和白名单两种模式。

3.2.6.3 微服务平台

1)支持一云多芯架构，同一朵云上可基于不同芯片架构的虚拟机或容器集群运行微服务。

2)支持在国产化芯片服务器及非国产化芯片服务器的部署；技术上能够支持国产化芯片服务器包括：中国信息安全测评中心（国家保密科技测评中心）公布的安全可靠测评结果中的至少三个品牌中央处理器（CPU）。

3)微服务应用支持容器和虚拟机等多种形态，并支持对应用生命周期管理。

4)支持服务实例按需自动弹性伸缩。

5)支持将有关联的微服务间调用依赖关系进行可视化展现，支持操作行为、执行状态信息记录，便于操作回溯及审计。

6)支持任务上下游依赖、逻辑判断、手动重试和 failover 机制，支持熔断策略设置。

7)支持系统标签、自定义标签配合多种策略实现服务路由。

8)支持在容器或虚拟机环境运行 ServiceMesh。

3.2.6.4 智能网关

1)支持在国产化芯片服务器及非国产化芯片服务器的部署；技术上能够支持国产化芯片服务器包括：中国信息安全测评中心（国家保密科技测评中心）公布的安全可靠测评结果中的至少三个品牌中央处理器（CPU）。

2)提供 API 服务的完整生命周期管理功能：包括服务的创建、编辑、删除、搜索、审批发布、保存草稿、启用/禁用、冻结/解冻、查看详情等功能。

3)支持 API 服务的发布和订阅。提供查看申请服务列表、服务授权历史、对服务进

行取消授权、重新授权，查看、编辑服务订阅详情、删除服务订阅申请等相关功能。

4)提供web站点的基础管理功能：包括站点的创建、编辑、删除、搜索、审核发布、保存草稿、启用/禁用、冻结/解冻、查看详情等功能；支持OAuth，LDAP和SAML等常见的认证协议。

5)支持站点发布路径转换配置，通过对原始原始站点地址和对外发布地址转换，对原始站点地址进行保护，不暴露给访问者。

6)提供机构管理，包括机构的创建、更新、查看、删除、机构人员的新增、编辑、删除、批量导入导出。

7)提供系统管理，包括系统的创建、更新、审核发布、查看、删除以及系统下的应用列表。

3.2.7 操作系统

1)提供500台云主机配套的国产化操作系统服务，为云上运行的应用程序提供稳定、安全和高性能的执行环境操作系统。

2)提供的操作系统能够适配支持业界主流CPU架构和芯片厂商。

3)提供的操作系统能适配支持国产数据库，包括：中国信息安全测评中心（国家保密科技测评中心）公布的安全可靠测评结果中的至少三个品牌集中式数据库。

3.3 AI算力服务

平台AI算力服务部分共需提供2200路等效视频分析算力以及3台国产大模型算力训练推理物理服务器。

3.3.1 异构管理

1)提供异构AI算力资源服务，算力规模为2200路等效视频分析（包括解码、结构化分析）算力，1路视频算力在FP16精度小为2.6T算力，或者等价为INT8精度下5.2T算力。

2)AI算力实例服务内容包括：AI加速卡厂商类型、显存大小、CPU、内存大小、磁盘容量。

3)可支持管理多种异构AI芯片，包括但不限于：英伟达以及寒武纪、华为等国产AI芯片。

4)支持GPU细粒度（0.1）资源拆分和隔离调度，支持国产AI芯片单物理卡隔离和调度。

5)支持通过控制台或者SSH方式登录，部署相关AI应用和AI算法。

3.3.2 功能要求

1)异构 AI 算力调度功能：提供算力资源调度管理功能，对 AI 算力设备进行统一管理，实现算力资源的统一管理，动态调度，按需使用；

2)算力共享：实现 GPU 算力卡共享，GPU 显存共享，同时针对异构的国产 AI 芯片算力设备，通过单个物理加速卡资源调度方式，进行算力资源统一调度，实现国产 AI 算力共享；

3)算力隔离：针对 GPU 算力共享，提供算力隔离功能，针对国产 AI 芯片算力设备，通过异构物理卡算子调度部署，进行算力隔离；

4)算力虚拟：针对 GPU 高密度训练卡，提供虚拟显存功能，自动实现内存和显存的映射；

5)GPU 池化计算：支持将同一服务器上的多张 GPU 卡的显存池化为一个显存，提升训练推理时运行的显存大小，针对不同物理服务器上的 GPU 卡，可支持以 RDMA 为基础实现 GPU 远程访问，对位于不同机器的算力进行统一调度；

6)算力监控：针对异构的算力资源，提供监控功能，对异构芯片算力设备的 CPU 使用率、内存使用率、显卡使用率、显存使用率、异常情况等信息进行统一监控；

7)算力注册：提供算力注册功能，对异构 AI 加速卡算力资源进行统一注册，借助 GPU 池化和异构调度，实现统一管理；

8)配额管理：对各个用户使用的资源量进行配额管理，配置的内容包括（显卡类型列表，显存大小，CPU，内存，磁盘），通过配额管理可对用户使用的资源数量进行限额，确保 AI 算力资源高效管理和使用；

9)集群管理：支持对算力硬件的导入、删除、初始化操作；支持对算力硬件进行编组管理；

10)资源监控：支持对各个 AI 应用和算法服务的资源使用情况进行监控，包括 GPU/AI 加速卡使用率、CPU 使用率、内存使用率等。

3.3.3 大模型训练推理国产算力

提供的大模型训练推理国产算力物理服务器应不低于以下配置：

1)4 路 CPU(48 核，2.6GHz)，8 颗 GPU,单台提供 FP16 算力不低于 2.5PFLOPS,FP32 算力不低于 0.65PFLOPS，单颗 GPU 显存不低于 64GB；

2)内存：1536GB（24*64GBDDR4）内存；

3)硬盘：2*480GBSATASSD，2*3.2TBNVMeSSD；

4)网卡：8*板载200GE网口，4*25GE网口；

5)支持在线运维：完成对高性能计算集群远程在线监控、异常告警通知等工作；

6)支持查看每个作业的运行资源使用情况；

7)支持各种常见的操作系统发行版（Windows各版本、Linux各版本）。

3.4多云资源管理平台

1)多云资源对接。可对业务系统云服务、AI算力服务等进行统一监控管理。

2)统一租户管理。对使用云计算中心的所有单位进行统一管理。包括对部门架构管理、部门用户管理、支持新用户注册和现有用户的导入。

3)统一权限管理。可以根据项目、角色、操作和数据范围组合定义用户权限。不同用户具有不同的平台界面视图和资源操作权限。

4)统一资源池管理。统一资源池管理主要包括管理多资源以及资源池权限管理。其中管理多资源池，按资源池一集群的关系查看每个资源池及资源池下的集群的资源情况及资源使用情况；资源池权限管理，主要是为各资源池指定管理员，管理员只能管理和查询其管理的资源池资源。

5)统一资源管理。对多个资源池所涉及的所有资源进行管理，包括资源监控管理、资源计量管理等，实现对整体资源情况的动态监控、配置以及，针对总体资源使用情况进行效能评价，提升资源的综合利用率。

6)统一监控管理。动态展示云计算中心的统一监控告警情况，主要包括：资源监控、容量监控、服务运行状态监控、实时告警、设备统计等。

7)统一运维分析管理。分析各个资源池各类资源的用户使用情况、资源容量情况，如云计算中心各业务系统的CPU、内存、存储、IP的资源使用情况分析。支持周期性生成报表，按周期统计分析各资源池资源容量情况、资源开通情况、以及资源使用率情况等，并支持将报表导出。

8)入云系统资源监测。对系统运行情况、资源使用情况、网络流量情况、系统访问情况、数据增量情况、数据共享情况进行监测，对异常情况自动发布预警信息，并对信息进行个性化定制及汇总。平台满足日常的维护工作，包括用户的增加删除、权限分配、基础数据维护等功能。

3.5资源管理及安全服务要求

3.5.1资源管理服务

乙方应提供6人专业技术团队（含驻场负责人1人、安全工程师1人）7*24小时驻

场服务，其中工作日白天 5 人值班，工作日夜间及节假日全天 1 人值守。需满足但不限于以下服务要求：

1)为区云计算中心使用单位提供云资源使用和系统部署等方面的技术指导工作。

2)配合区云计算中心使用单位完成系统向云中心国产化区迁移或部署。

3)负责区云计算中心的云计算、AI 算力、存储、网络资源、负载均衡、数据库等资源的管理及运行状况监控。

4)负责提供技术支持保障服务，操作系统、数据库等的调试配置服务。

5)定期提交用户资源使用情况报告。

6)配合开展应急演练工作。

7)负责云计算中心平台的运行安全问题，在系统遭到破坏时，及时进行恢复确保系统的正常运行。

3.5.2 安全保障服务

3.5.2.1 基础安全服务

为本项目提供高效、合理、可靠的网络链接服务、通信传输防护、访问控制、网络边界防护、访问审计等服务。

1)网络架构：应通过网络设备流量控制等技术手段保证重要业务不受网络拥堵影响，保证网络设备的业务处理能力满足业务高峰期需要及各个部分的带宽满足业务高峰期需要。

2)通信传输：对于边界接入要求具有云 VPN 功能。要求支持纯软件交付，支持虚拟化部署；控制平台及网关等组件支持多种模式部署，关键组件支持横向扩容；支持端口隐藏，默认关闭所有 TCP 端口，UDP 端口只接受不响应，网关后所有业务隐身，从网络上无法连接、扫描。

3)访问控制：在各网络边界处要求提供部署防火墙，要求能够根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级，同时安全网关要具备对进出网络的信息内容进行过滤，实现对应用层协议的命令级控制。要求提供 DDoS 防护服务能力，保证有效的拦截。

4)网络边界防护：在云网络边界要求提供部署下一代防火墙作为出口防火墙，通过出口防火墙的安全域划分提供基础安全隔离。

5)访问审计：要求提供对应用访问日志、安全设备日志、网络设备日志、服务器日志等日志记录，所有日志记录均通过日志审计系统进行集中存储和审计。

6)乙方须承诺按照等级保护 2.0 三级要求规划建设安全服务。

7)乙方需按照国标 39786《信息安全技术信息系统密码应用基本要求》中的要求，规划云平台商用密码安全产品建设，包括使用国家密码管理局认证的商用密码产品实现对云平台访问鉴别身份真实性保护、重要敏感数据传输机密性和完整性、重要敏感数据存储的机密性和完整性保护等。

3.5.2.2 增值安全服务

为本项目提供高效、合理、可靠的 IPS 服务、威胁检测、主机安全、漏洞扫描、web 应用安全、数据安全、安全运营中心、网络入侵防护、堡垒机等服务。

1)在云出口区要求开启 IPS 能力，以阻断各类入侵攻击。IPS 应具备攻击事件检测、阻击、记录、报警功能。要求在旁路部署网络行为审计系统，实现针对网络中内容、行为的监控管理及安全事件的追查取证。

2)威胁检测：要求具备未知威胁检测能力：支持对 web 漏洞利用检测规则、入侵检测规则等多种规则的配置，可以有针对性的选择部分规则开启；支持 HTTP 解码引擎；支持 WEBAPI 接口数据泄露检测，包括手机号码、邮箱、身份证以及银行卡等数据内容，可自定义检测规则。支持区分授权/非授权 API 接口。

3)主机安全：云主机需要提供漏洞检测、木马病毒查杀、密码破解拦截等服务器安全防护功能，及时发现安全风险并提供防护解决方案。

4)漏洞扫描：提供对主机、网络设备、安全设备、服务器、应用系统等对象进行漏洞扫描。

5)web 应用安全：要求提供 web 应用防火墙服务，应通过对进出 Web 服务器的 http 流量相关内容的实时分析检测、过滤，来精确判定并阻止各种 Web 应用攻击行为，阻断对 Web 服务器的恶意访问与非法操作；要求支持 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)数据安全：要求提供采用在云数据库安装数据库代理的方式，对访问数据库的所有数据访问行为进行安全审计。完成对数据库访问行为的详细审计过程。要求支持基于样本训练的 AI 引擎，能够根据海量样本训练获取数据库危险操作的特征建模，并根据模型判断数据库语句的风险等级。

7)安全运维中心：要求提供攻防场景模型的大数据分析及可视化展示等手段，协助云计算中心建立和完善安全态势全面监控、安全威胁实时预警、安全事故紧急响应的能力；支持联动旁路阻断设备。提供统一部署安全策略，应进行安全管理平台的设计，根据要

求，应从系统管理、设备管理和系统对接等方面进行建设。

8)网络入侵防护：通过旁路部署的方式，提供网络层 ACL(访问控制)和日志审计功能，解决安全管控、云计算中心监管，ACL 控制，安全治理等问题。支持与其他第三方检测设备联动，通过拦截 API，第三方检测设备可增加 IP 黑名单规则，实现拦截。

9)堡垒机：能够建立基于唯一身份标识的全局实名制管理，支持统一账号管理策略，实现与各服务器、网络设备等无缝连接。

10)应急演练：开展云平台应急演练，制定云平台重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；提出上云业务系统应急演练的指导方案，对应急方案进行演练，确保安全和业务在出现紧急问题时及时得到处置。

11）二线支撑：提供 7*24 小时二线支撑服务，保障云平台的运行过程中，可以第一时间解决客户技术问题。

12）安全专家服务：可为平台提供高阶安全服务工作的技术支持、现场现状调研以及建议。

3.5.3 国产云迁移支撑服务

为本项目提供国产云迁移支撑服务，配合业务系统向国产化环境迁移的需求调研、技术咨询建议、性能优化、业务适配、数据库规范制定等服务。

第四条 计费方式及支付方式

4.1 计费方式

本项目为按照甲方需求以购买服务的方式向乙方购买相关服务，并根据实际购买服务结算费用。

4.1.1 甲方购买服务应按照《服务内容及价格表》（见附件 1）内约定服务内容、价格及实际使用数量进行购买，如有其他服务需求，需签订补充协议补充服务内容后再购买。

4.1.2 甲方购买服务的期限不超过本合同服务期限，如有超出合同期内的服务只计算本合同服务期内实际使用服务内容及数量，超出部分由双方签订合同另行支付。

4.2 支付方式

本项目合同金额为 20,725,752.00 元（大写：人民币贰仟零柒拾贰万伍仟柒佰伍拾贰元）。目前预计需购买的服务见《服务需求统计表》（附件 2）。该价款为包含全部相关税费的最终价款。

4.2.1 第一笔款：合同签订后或服务期开始后 6 个月内，向乙方支付合同金额的 50%，

即￥10,362,876.00元（大写：人民币壹仟零叁拾陆万贰仟捌佰柒拾陆元）。

4.2.2 尾款：服务期满一年后60个工作日内，由甲方委托第三方具备相关资质的审计单位对本合同所涉及服务费结算进行审核，甲方根据审核结果结算本合同服务期剩余服务费。

4.2.3 甲方、乙方与审计单位另行签订三方结算审核合同，进一步明确针对本合同所涉及服务费结算的审核事宜，结算审核费用由乙方承担。

4.2.4 合同执行过程中，乙方应按月提供每月实际使用费用账单（以本合同4.1计费方式条款约定计费方式计算得出）确认当月云计算中心服务费，并交由甲方确认，如出现本合同服务期服务费用超过本项目合同金额的趋势，乙方应及时提示甲方追加预算。

4.2.5 结算尾款时，如超过预算部分，甲方须于合同服务期结束后完成预算追加，并支付乙方超出部分费用。

4.2.6 甲方付款前，乙方应向甲方开具符合甲方要求的发票，否则甲方有权顺延付款而不视为违约。

因财政拨款迟延导致甲方付款延迟的，不作为甲方违约，乙方同意付款期限相应顺延。

第五条 双方的权利和义务

5.1 甲方的权利和义务

5.1.1 合同执行期间，海淀区云计算中心使用的基础IT资源所有权归乙方所有，云服务、AI算力资源使用流程由乙方根据甲方要求统一制定，云服务、AI算力资源使用权归甲方所有，云计算中心上的相关数据所有权归甲方所有。

5.1.2 甲方委托乙方利用云服务、AI算力资源为辖区内各委办局运行以智慧海淀为主的业务系统提供基础IT资源支撑和统一规范服务管理，所有经甲方批准部署在云计算中心的应用系统如涉及乙方提供的第三方软件许可使用的，甲方同意遵守相关的许可协议的约束；所有经甲方批准部署在云计算中心的应用系统，甲方负责协调相关使用单位自行解决云服务器上所需要的非乙方提供的软件版权（许可/使用权），并负责数据的完整性和保密性；甲方负责协调相关使用单位不应在云计算中心上安装、使用盗版软件，并支持乙方可以拒绝使用盗版软件的相关使用单位应用系统在云计算中心上部署。乙方侵犯第三方权利的，乙方自行处理。

5.1.3 甲方应明确要求各委办局用户对于部署在云计算中心上的业务系统申明内容责任自负，如内容中有违反政策法规的情况，由业务所有方承担全部责任。

5.1.4 甲方应按时向乙方缴纳本合同约定的费用。

5.2 乙方的权利和义务

5.2.1 乙方应按照合同约定为甲方提供服务。

5.2.2 乙方对云服务器进行日常维护和监控，以保证其正常运行。

5.2.3 乙方负责提供操作系统并提供网络环境及基础安全服务。如乙方提供的政务云服务未达到项目招标要求，无法通过测试，甲方有权利终止项目执行，并重新进行招标。

5.2.4 乙方为甲方提供每周 7 天×24 小时售后服务，并为甲方提供有效的联系方式。

5.2.5 乙方应严格遵守保密义务，除非双方另有书面约定，乙方承认甲方存放在云计算中心上的任何资料、软件、数据等的知识产权均与乙方无关，乙方无权复制、传播、转让、允许或提供他人使用这些资源。

5.2.6 如服务出现任何问题，乙方应优先协调各方资源处理解决，不推卸、推诿。

5.2.7 如果第三方机构或个人对甲方提出质疑或投诉，乙方将通知甲方，甲方有责任在规定时间内进行说明并出具证明材料，如甲方未能提供相反证据或逾期未能反馈的，乙方将采取包括但不限于立即终止服务、中止服务或删除相应信息等处理措施。因甲方未及时更新联系方式或联系方式不正确而致使未能联系到甲方的，亦视为甲方逾期未能反馈。

5.2.8 因不可抗力因素和甲方原因，造成服务的正常工作中断，乙方不承担责任。

5.2.9 乙方应积极配合甲方及其委托的第三方进行安全审查，费用审计。

5.2.10 主流 Windows 和 Linux 操作系统的 License 许可证费用由乙方承担。

5.2.11 云计算服务之间的交互而引起的网络流量属于乙方免费提供的服务范畴。

5.2.12 在未取得甲方同意的情况下，乙方不得通过任何手段收集、分析、处理、篡改云计算中心中的数据。禁止数据以任何方式渠道泄露出去。

5.2.13 乙方不得私自将未经甲方审核的系统部署在云计算中心。

第六条 交付期及验收

6.1乙方在合同签订后60个工作日内对乙方提供的云服务进行测试，测试通过即为验收合格。

6.2乙方提供的云服务未达到项目招标要求，无法通过测试，甲方有权利终止本合同，并重新进行招标。

第七条甲方数据的保存、销毁与迁移

7.1 根据法律有关规定或者行政、司法机构的要求，经甲方同意，乙方可以向第三方或者行政、司法机构提供数据审查。

7.2 除法定及甲乙另行约定外，自本服务合同期满或因任何原因导致本服务合同提前终止之日起的 60 日内，乙方应继续存储甲方的数据。超过 60 日的，乙方将不再保留甲方数据，甲方需自行承担其数据被销毁后引发的一切后果。

7.3 甲方要求删除数据或设备在弃置、转售前乙方需将其所有数据彻底删除，并无法复原。

7.4 乙方承诺甲方启用或弃用云服务时将配合甲方完成数据的迁入和迁出。

第八条 违约责任

8.1 甲乙双方任何一方不履行合同义务或者履行合同义务不符合本合同约定的，均视为违约。守约方可向违约方发出要求其履行合同义务的书面通知，违约方应在通知发出之日起 5 个工作日内采取补救措施，逾期仍未采取措施的，则守约方有权要求违约方继续履行合同义务并赔偿因此造成的损失。

8.2 甲乙双方在完成双方签署的书面确认事项后，任何一方提出变更要求，导致项目进度延迟的，不视为对方违约。

8.3 因甲乙双方任何一方的原因致使另一方遭受第三方追诉的，违约方应赔偿由此给另一方造成的损失。

8.4 因甲方的原因或与甲方具有协作关系的第三方的原因导致项目进度延迟的，乙方不承担违约责任，因此而给乙方增加工作量的，甲方应按照双方协商一致的确认结果给予补偿。

8.5 因乙方原因造成项目进度延迟的，每逾期一日，乙方应按相应阶段应付款项的万分之五支付违约金。违约金的支付并不能解除乙方继续履行合同的责任和义务。

8.6 乙方提供服务过程中可能发生的违约行为及相应应承担的违约金详见附件 3。

第九条 争议解决

9.1 因履行本合同或与本合同有关的一切争议，双方当事人应通过友好协商方式解决，若发生争议协商未成，双方约定向合同签署地有管辖权的人民法院提起诉讼。

9.2 在诉讼过程中，除各方有争议的部分外，本合同其它部分继续有效。

第十条 不可抗力

任何一方如遇有不可抗力而全部或部分不能履行本合同，应自事件发生之日起十日内，将事件情况以书面形式通知另一方，并于事件发生之日起二十日内，向另一方提交

导致引起全部或部分不能履行的证明。在取得有关机关的书面证明后，允许延期履行合同，并根据情况可部分或全部免于承担违约责任。

不可抗力、意外事件是指不能预见、不能避免并不能克服且对一方或双方当事人造成重大影响的客观事件，包括但不限于自然灾害如洪水、地震、瘟疫流行等以及社会事件如战争、动乱、政府行为、电信主干线路中断、电信部门技术调整和政府管制等。

第十一条 通知

11.1 合同要求或允许的通知或通讯，不论以何种方式传递，均自被通知一方实际收到时起生效。

11.2 上款中的“实际收到”系指通知或通讯内容到达被通知人的法定地址或住所或其指定的通讯地址范围。

11.3 一方变更通讯地址或通讯方式，应自变更之日起 10 个工作日内，将变更后的地址及联系方式通知另一方。

第十二条 保密

12.1 除以下第十二条第 12.2 款另有规定外，甲方和乙方应当各自就其或其雇员、承包商、顾问或代理人获得的关于本合同及本项目（无论是财务上、技术上或其他方面）的全部信息和文件，予以保密。

12.2 以上第十二条第 12.1 款不适用于：

12.2.1 已经公布的或能以其他方式公开获得的信息或文件（但不包括以违反本合同的方式公布或获得者）。

12.2.2 已经由一方以不违反任何保密义务的方式获得的信息或文件。

12.2.3 以不违反任何保密义务的方式从第三方获得的信息或文件。

12.2.4 按照法律须披露的信息或文件。

12.2.5 为按照本合同履行一方义务而披露的信息或文件。

12.3 以上第十二条第 12.1 款在本合同届满或终止后的十年内仍然有效。甲乙双方对彼此之间相互提供的信息、资料以及本合同的具体内容负有保密责任。

第十三条 服务期限及终止

13.1 本合同有效期自签订之日起，一年服务期满后止。

13.2 本合同服务期自 2025 年 1 月 25 日起至 2026 年 1 月 24 日止。

13.3 本合同服务费用按年结算，第一年服务期结束后，在不改变合同其它条款的情况下，甲方可视服务情况与乙方续签合同，续签次数不得超过两次，总服务期限不得超

过三年。

13.4 发生下列情形，服务期限提前终止：

13.4.1 双方协商一致提前终止的。

13.4.2 甲乙任何一方单方面提出终止合同，需提前三个月通知对方，双方协商解决。

13.4.3 甲方违反本合同条款的，包括但不限于未按照合同约定履行付款义务或严重违反法律规定等。

第十四条 其他事项

14.1 本合同的权利和义务非经对方书面同意，不得转让。

14.2 本合同签订前双方所作的口头或书面讨论、协商、承诺及其他事项，非经订入本合同者，不再有效。

本合同由以下文件构成，优先解释顺序如下：

（1）本合同；

（2）中标通知书；

（3）乙方投标文件；

（4）甲方招标文件。

14.3 本合同未尽事宜，双方另行协商签订补充合同，补充合同与本合同不一致之处，以补充合同为准。

14.4 对本合同内容的任何修改和补充应以书面形式做出，由双方授权代表签字盖章，并视为合同不可分割的部分，与本合同具有同等法律效力。本合同附件与本合同具有同等法律效力。

14.5 本合同正本一式壹拾叁份，具有同等法律效力。甲方执陆份，乙方执肆份，海淀区政府采购中心执壹份。

14.6 本合同经甲、乙双方授权代表签字并加盖各方公章或合同专用章之日起生效。

（以下无正文）

合同签署页

甲方	单位名称	北京市海淀区大数据中心（盖章）
	法定代表人（或授权代表）	签字（或盖章）：
	项目负责人	卢诚
	电　　话	50869097
	传　　真	/
	邮政编码	100081
	地　　址	北京市海淀区中关村南大街5号海淀科技大厦
	纳税人识别号	12110108MB09868857
乙方	单位名称	中国电信股份有限公司北京分公司（盖章）
	法定代表人（或授权代表）	签字（或盖章）：
	项目负责人	曲维浩
	电　　话	13331108258
	传　　真	59323247
	开户银行	工行阜外大街支行
	账　　号	0200049219022523842
	邮政编码	100027
	地　　址	北京市东城区朝阳门北大街21号
签署日期		2025 年 1 月 24 日

附件 1：服务内容及价格表

序号	名称	单位	单价（元/月）	备注
1	云主机（8 核16GB）	台	752	参考规格；需明确“1 核 CPU ”、“1GB 内存 ”的单价；其他规格服务需按 单价进行核算
1.1	云主机 cpu	核	22	
1.2	云主机 内存	GB	36	
2	云数据库（8 核 16G）	台	584	
2.1	云数据库 cpu	核	22	
2.2	云数据库 内存	GB	25.5	
3	云存储	TB	350	
4	裸金属服务	台	14000	
5	国产操作系统	套	40	
6	国产中间件	套	40	
7	网络服务	10M	400	
8	资源管理及安全服务	套	196122	
9	机柜服务	个	6500	
10	国产大模型算力服务	台	48340	
11	AI算力云服务	路	190	
12	多云资源管理平台	套	37500	

附件2：服务需求统计表

序号	服务名称		数量	单位	周期（月）	服务单价（元/月）	服务费小计（元/年）
1	云计算服务	云主机（8C/ 16GB）	613	台	12	752	5531712
		云数据库（4C/8G）	384	台	12	292	1345536
		云存储	484	T	12	350	2032800
		国产裸金属服务	3	台	12	14000	504000
		国产操作系统	500	套	12	40	240000
		国产中间件	500	套	12	40	240000
		网络服务	200	10M	12	400	960000
		资源管理及安全服务	1	套	12	196122	2353464
		机柜服务	4	个	12	6500	312000
2	AI算力服务	国产大模型算力服务	3	台	12	48340	1740240
		AI 算力云服务	2200	路	12	190	5016000
3	多云资源管理平台	入云系统监控、性能可用性监控、生命周期管理、资源配置管理	1	套	12	37500	450000
合计							20725752

注：

1.上述需求仅为估算需求情况，实际费用按照服务实际使用量及服务单价进行核算。

2.云主机（8核 16GB）、云数据库（4核 8GB）为参考规格，其他规格服务需按1核、 1GB单价进行核算。

附件3：乙方服务补充要求及违约行为罚处细则

第一条 乙方提供的服务补充要求

1.1 为保障上云系统的正常运行，乙方每天应进行2次云计算中心健康检查，检查内容包括但不限于云计算中心控制节点、计算节点、存储节点、数据库集群，并将检查报告通报甲方。

1.2 乙方应对检查过程中发现的云计算中心软硬件风险隐患进行修复维护；在维护操作前,乙方应向甲方提交实施方案，说明处置流程和处置人员，经甲方批准后，严格按方案实施操作，操作完成后向甲方通报结果，并记录备案。

1.3 乙方进行云计算中心系统版本迭代前，应向甲方提交风险评估报告和测试报告，确保甲方业务系统在不同版本环境下均可稳定运行。

1.4 乙方应根据甲方业务系统上云计划,提前进行云计算中心扩容所需物理服务器、网络设备、互联网带宽等资源的部署，并保证云计算中心可用资源冗余不少于现有资源的30%。

1.5 乙方应根据国家互联网应急中心公布的威胁预警情报对云计算中心上的系统和软件进行全面的漏洞扫描与病毒查杀，发现问题应及时进行处置并通报甲方。

1.6 乙方应持续优化云计算中心安全组策略和防火墙入站规则，加强云计算中心的安全访问控制策略，形成双重保险机制。

1.7 乙方应持续升级完善云计算中心安全防护系统，加强云计算中心用户侧的安全防护功能；对涉及民生、教育、医疗、政务等重要业务系统目应进行重点防护。

1.8 乙方接到甲方故障通报后，应及时处理，做好相关信息的登记工作，定时向甲方反馈处置进度及结果；故障排除后，乙方应向甲方提交故障发生及处置过程中全部软硬件日志和故障分析报告，明确故障原因和整改措施，并严格落实整改措施，杜绝类似故障再次发生。

1.9 乙方应确保云计算中心运维人员符合岗位要求，运维人员到岗前，需经过全面系统的技术培训、安全培训、保密事项培训。

1.10 乙方应确保云计算中心运维团队稳定,运维人员变动需提前一个月通知甲方。

第二条 乙方违约惩处细则

乙方服务期内未能达到合同及附件的约定的服务标准，发生违约行为，甲方将按相应违约行为进行**惩处**。违约行为分为重大违约行为、严重违约行为和一般违约行为。

2.1 乙方重大违约行为

乙方服务期内的违约行为造成云计算中心整体故障（非不可抗拒力条件下）或重大安全事故的（根据其严重程度分为A级事件和B级事件）。乙方触发该A级事件一次及以上或一年内三次及以上B级事件违约行为，属于乙方重大违约行为，即重大安全事故（具体如下表），甲方有权解除本协议，并要求乙方赔偿甲方相应的经济损失。

一年内B级事件发生少于三次，违约金金额=当月云计算中心服务费*30%。

类别		范围	影响	影响时间	事件级别	次数
重大安全事故（乙方主责）	服务中断	云计算中心整体	因非不可抗力造成超过30%以上业务系统中断、影响人数50万以上、导致500万元以上经济损失。	2小时以上	A级	1次及以上
	重大篡改事件	应用系统	在重大或特别重大保障期间，因乙方的安全隐患原因造成的系统被恶意篡改事件。事件发生后乙方未按照应急预案进行处置，造成信息安全事件处置延误。且该事件被国家级机构或媒体通报、市级领导批示或关注的。	30分钟以上		
	数据丢失	等保三级或重要业务系统的核心业务数据	因非不可抗力造成的云计算中心超过3个业务系统丢失超过1个月以上的数据，且确认无法恢复。	——		
	恶意入侵攻击	等保三级或重要业务系统	被第三方安全机构通报云计算中心存在安全隐患，乙方未在24小时内做有效处置或应急防护措施，造成业务系统在重大或特别重大保障期间被恶意篡改或敏感信息泄露事件。	——		
	服务中断	云计算中心整体	因非不可抗力造成超过10%至30%业务系统中断、影响人数10万以上、导致100万元以上经济损失。	2小时以上	B级	一年内3次及以上
	重大篡改事件	应用系统	因乙方的安全隐患原因造成的系统被恶意篡改事件，事件发生后乙方未按照应急预案进行处置，造成信息安全事件处置延误，且该事件被	30分钟以上		

类别		范围	影响	影响时间	事件级别	次数
			市级机构或媒体通报、区领导批示或关注的。			
	数据丢失	业务系统核心业务数据	因非不可抗力造成1个业务系统丢失超过1个月以上的数据，且确认无法恢复。	——		
	恶意入侵攻击	业务系统	被第三方安全机构通报云计算中心存在安全隐患，乙方未在24小时内做有效处置或应急防护措施，造成业务系统被恶意篡改或敏感信息泄露事件。	——		

2.2 乙方严重违约行为

乙方在服务期内的违约行为对用户业务系统产生一定的经济损失，但其影响和经济损失未达到重大违约行为中规定的B级事件的。

违约金金额=业务系统云服务费/服务月数*惩处系数。

序号	问题描述	惩处系数
1	所提供的云服务器可用性低于99.95%,数据可用性低于99.999%,网 络可用性低于99.99%，出现问题并造成重大损失的	200%
2	因未做好系统和数据互备，由于政务云服务中断，而导致系统和数据无法正常应用的，但影响未达到B级及以上事故影响的	200%
3	因所提供的安全服务出现故障，导致某系统网页被篡改，造成重大影响	600%
4	因所提供的安全服务出现故障，导致某系统数据丢失，造成重大影响	600%
5	因所提供的安全服务出现故障，导致某系统被入侵，造成重大影响	600%
6	在甲方已发出整改通知后未正确处置，出现问题并造成重大事故	200%

2.3 乙方一般违约行为

乙方在服务期的违约行为对用户业务系统造成的影响未达到重大违约行为和严重违约行为的其他违约行为。

违约金金额=业务系统云服务费/服务月数*惩处系数。

序号	问题描述	惩处系数
1	所提供的云服务器可用性低于99.95%,数据可用性低于99.999%,网 络可用性低于99.99%，出现问题但未造成重大损失的	50%

2	所提供的云服务器可用性低于99.95%，或数据可用性低于99.999%，网络可用性低于99.99%，且在服务期内接到委办局投诉此类情况3次以上的	20%
3	在运维期间，甲方对乙方实施月度考核，如乙方连续3次未能通过考 核，经限期整改后仍不能达到甲方要求的	20%
4	在运维期内，如乙方未能按照用户方的扩容需求，在14个自然日内完 成云计算中心的资源扩容，且经管理单位书面通知仍未能限期满足用 户需求的	20%
5	因所提供的云服务或安全服务出现故障，造成某系统宕机2小时以上	30%
6	因所提供的云服务或安全服务出现故障，造成某系统连续宕机3次以上或累计8小时以上	60%
7	在甲方已发出整改通知后未正确处置，出现问题的，未造成重大影响	50%