某大型公司网络建设方案

航天一院通信站

2019-03

# 需求分析

## 1.1背景概述

信息化是企业文化的窗口，信息化管理创新是企业发展的必由之路，信息化管理模式带来了企业管理模式的转变。近年来，随着公司信息化建设的快速发展，信息化平台原有的基础设施、网络架构、安全技术、服务保障等能力亟需进一步提升与整合，以满足未来发展需求，提供更加稳定、可靠、安全的服务。当前公司信息化平台面临的挑战如下：

#### 网络安全技术防护能力有待提升

面对日趋复杂的网络安全环境和国家对网络安全的高度重视，公司对各信息化系统的安全提出了更高要求。公司目前安全防护设备陈旧，策略简单，没有形成体系化、等级化的有效技术防护体系，对新型网络攻击不能有效发现，对业务系统的防护能力明显不足；

#### 网络安全管理能力有待提升

缺乏有效的网络安全管理体系，工作无计划，在遇到突发事件时没有快速有效的应对机制；员工网络安全意识淡薄，随意使用移动存储设备，随意安装软件，随意存储发送敏感数据等；员工的上网行为没有有效的监控管理。

#### 网络运维管理能力有待提升

1. 缺乏有效的运维管理系统，运维人员不能统一查看和管理各系统的运行状态，事前预警机制不健全，出现故障后，处于被动救火的工作状态；
2. 运维人员和外部协作人员可以随意登录各系统，没有有效的监管和审计手段；
3. 各部门的软硬件资产混乱，没有进行统一有效的资产管理。

#### 数据存储、传输的安全性、可靠性有待提升

1、 数据存储设备陈旧，公司目前的备份系统为单一磁带机方式，效率和可靠性比较差且并未做到异地备份（热备份）；

2、 关键部门的数据没有防护措施，可以任意复制和发送，安全性缺乏保障；

3、 与分支机构数据传输未加密，一旦发生数据泄露，将后造成泄密事件；

#### 存在信息孤岛问题，各系统数据无法流通

存在信息孤岛，各信息系统间数据不能流通，需人工进行数据的导出、分析，效率低下，准确性差，严重影响了精确控制和辅助决策。

#### 基础设施自然更替带来的风险与成本

承载着各种应用业务的服务器、存储设备等，其服务的可靠周期一般为5年，超过5年即因老化而进入故障多发期，而大多数设备原厂商对销售3年以上的产品已经停止生产，因此一旦设备出现故障，则面临着维修困难或者无法更换合适配件，设备停用的风险较大，进而影响业务的稳定运行。

目前为了保障业务系统的可靠性，需要增加硬件投入，实现两台或多台设备冗余备份。基础设施的冗余机制与迭代更新，大大增加建设和维护的成本。

#### 基础资源的低利用率与高耗能

业务系统运行在独立的x86物理服务器上，为了满足突发峰值访问和后续业务的扩展，一般服务器和存储等硬件配置性能都要大大高于预估平均值，由于用户访问存在忙闲不均的情况，导致基础资源的利用率较低，利用不充分，大多资源处于闲置状态。

基础设施数量多、利用率低，电力成本居高不下，导致高能耗低功效。

#### 基础资源无法满足业务快速上线的需求

随着业务的快速推广，业务系统上线要求愈发紧急迫切，但受预算、固定资产申请、合同审批等影响，很难达到快速提供基础资源的需求，直接或间接影响业务测试、部署和上线的时间。

综上各点所述，随着信息应用系统的逐步开发和推广，现有信息化平台无论是规模还是架构都难以更好的支持业务的增长和后续新业务系统的部署实施，信息化平台在架构支撑和能力设计上都需要进一步提升。

## 1.2建设目标与任务

着眼信息化的长远发展，对于上述提出的挑战，建议参照国家等级保护要求，建设统一的信息安全技术和管理体系，提高信息系统的安全防护等级和能力。纵观信息化发展趋势，云计算、超融合、分布式集群等新的技术、架构、体系都给信息应用系统带来巨大的发展空间，建议建设以云计算为核心的信息化整体架构。

本次项目的总体建设目标为：

1、 参照等级保护要求构建网络安全技术及管理能力架构；

2、 打好云计算的基础，建立云平台框架，构建企业信息发布、运营服务平台；

3、 建立各信息系统间的数据流通整合体系，为决策分析提供精准的数据信息。

# 效益分析

## 2.1、经济效益

统一的网络与安全架构，整体提升网络安全与管理能力。通过各信息系统间的数据流通整合，简化工作流程，提高工作效率，提供精准决策，节约成本。

基于云计算的高弹性、高可靠性、高冗余的特点，将物理分散的各类资源池化后统筹调度和管理，灵活高效地分配资源，提高资源利用率，减少硬件投入成本，节省电力成本。

### 2.2 社会效益

安全体系和异地备份中心的建设大大增加了信息化系统的可靠性与安全性，提升能力的同时，也有助于提升企业整体形象。云计算能够快速交付虚拟化基础设施服务，提供不中断业务的设备更新，大大提高了业务上线的效率。

# 整体方案规划

**3.1 规划原则**

1. 高可用性

网络的稳定可靠是应用系统正常运行的关键，保证在网络设计中选用高可靠性 的网络产品设备，充分考虑冗余、容错和备份能力，同时合理设计网络架构，制订可靠的网络备份策略，保证网络具有故障自愈的能力，最大限度地支持系统的可靠运行。

1. 合理性

网络按照分层、模块化的思路进行设计和规划，根据业务、区域等规划因素进行模块化的区域划分，避免不合理的设计给网络带来安全隐患或造成资源浪费。

1. 最大效用

现有资源要充分利用，新增设备也要利用充分，充分挖掘设备的价值。

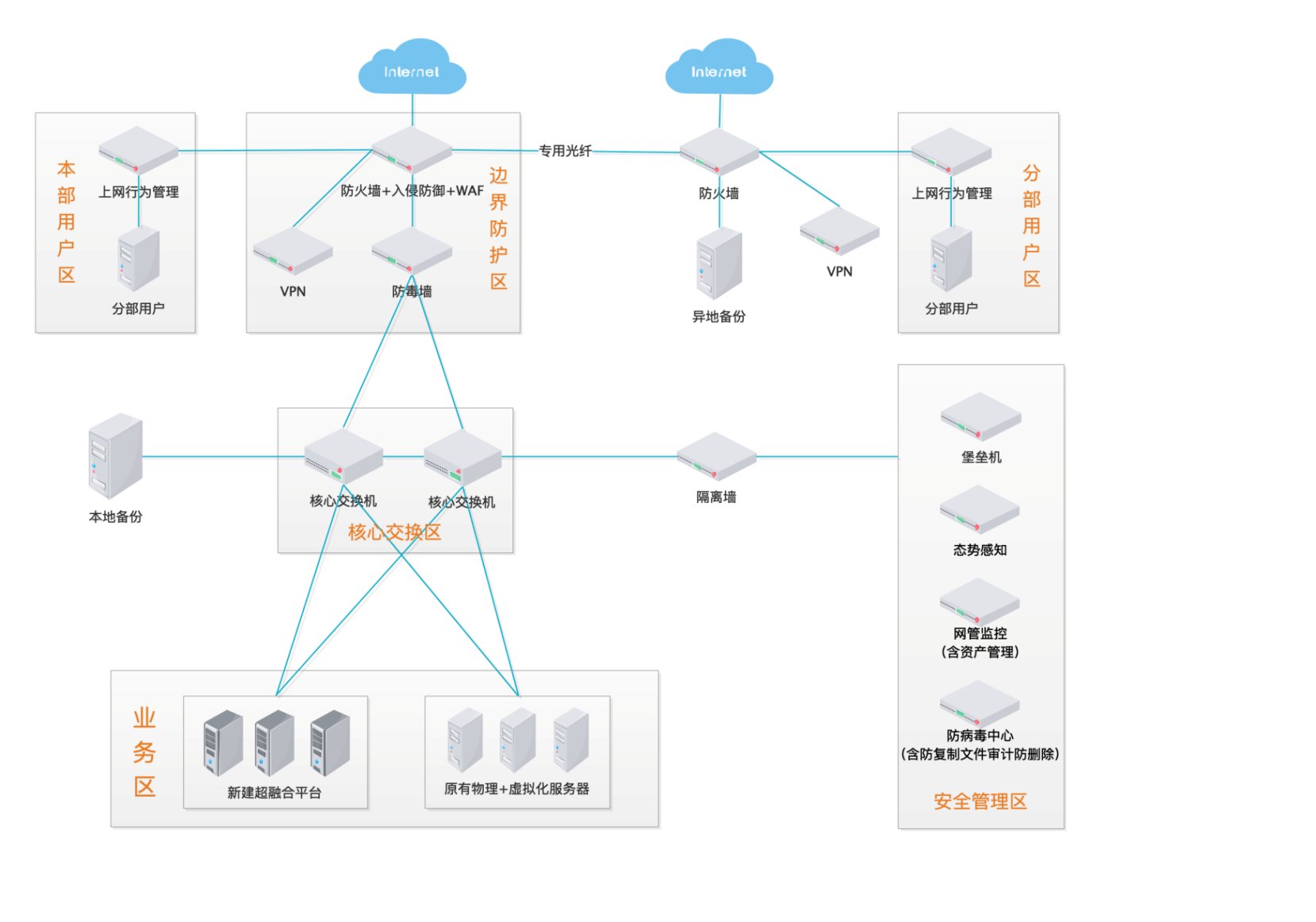
1. 可扩展性

骨干网络的性能是整个网络良好运行的基础，在设计中必须保障网络及设备的高 吞吐能力，保证各种信息（数据、语音、图象）的高质量传输，才能使网络不成为业务开展的瓶颈。

1. 安全性

制订统一的网络安全策略，整体考虑网络平台的安全性，既要考虑整体安全又要考虑具体需求。做到业务数据的安全传递和网络设备不受黑客攻击。

## 3.2整体网络与安全架构

整体网络与安全架构，包括硬件防护设备和云平台虚拟环境下安全防护产品，实现云内、云外整体防护方案。整体网络和安全架构的可靠性和稳定性都将大幅提升，有效实现了纵向的安全防护和横向各区域的隔离，统一的管理中心有利于规范化的管理维护。架构整合后，具体优势体现在：

**1、网络安全保护：**

* 安全区域划分清晰，共划分为边界防护区、核心交换区、业务区、安全管理区、本部用户区、分部用户区共6个安全区域；
* 边界防护区，部署一台“下一代防火墙”和一台“防毒墙”实现防火墙、入侵检测、 WEB防护（WAF），网页篡改、邮件安全、恶意攻击、僵尸木马、病毒检测等安全防护，实时识别网络中发生的入侵行为并进行有效拦截防护，净化网络流量，充分保障业务系统通过内、外网访问的安全；
* 旁挂态势感知安全设备，实现对全网安全状况的实时掌控，内部攻击可视化，及时发现并告警已感染或被攻击的主机，及早防范控制，减少损失；
* 部署上网行为管理系统，实现管控本部、分部内网用户网络应用和上网权限，保证本地人员的上网体验；对外发信息过滤，管控文件、邮件发送行为，对网络中的异常流量、用户异常行为及时发起告警，减少网络外发数据泄密事件和其他违法违规行为的发生。
* 病毒中心实现对业务区、内网用户区的主机病毒防护，集中管控，定制病毒查杀策略，与防毒墙形成病毒库异构，加强病毒的防范能力；
* 云平台集成的2-7层安全防护，避免云平台遭受攻击导致平台瘫痪；通过云平台内虚拟化安全防护系统实现虚机间横向流量的管控与防护，避免系统间横向病毒或攻击扩散；

**2、数据传输与存储：**

* 本部和分部，利用VPN的加密机制，保证通过专用光纤或互联网的数据加密传输；
* 部署“终端安全管理软件”对文件进行安全审计，防止关键数据被复制、发送、删除等操作，控制移动存储设备，实现数据防泄漏；
* 旁挂备份机，实现云内、云外各业务系统的操作系统、应用、数据库等全备份，在分部搭建异地灾备中心，实现备份数据异地存储；出于经济成本的考虑，建议只实现数据异地备份，达到灾后数据恢复，不建议建立异地双活灾备中心。

**3、资源池化转型：**

通过新设备的采购和利旧部分设备，结合虚拟化技术，通过构建云计算资源池、存储资源池、网络资源池、安全资源池等方式，将原有的烟囡式系统建设模式打破，通过资源池统一对外提供资源，实现基础设施建设的技术转型。包括计算资源、存储资源、网络资源、网络安全资源、数据备份恢复功能等均可以作为服务资源池的形式，实现按需提供，满足业务发展不断增长的基础设施需求。

**4、运维与审计：**

* VPN+堡垒机对运维人员和外部协作人员进行身份鉴别以及操作审计，实现细粒度访问控制、运维过程“事前预防、事中控制、事后审计”，操作“有迹可循”，全程可追踪，保障运维安全；
* 网络监控管理系统，以拓扑图的方式来直观清晰的显示设备关键属性和运行状态，实现对全网设备的监控管理，掌握各设备的运行状况，及早发现隐患，同时，实现各部门硬件资产的统一管理。

### 3.3云平台整体技术架构

### 3.3.1架构选择

建议选择“云管平台 + 超融合架构”方案搭建云平台， 基于分布式存储架构，通过软件定义的方式实现全新的IT基础架构。通过服务器虚拟化将所有X86的计算资源池化、通过网络虚拟化构建出适合虚拟机迁移的大二层环境、通过存储虚拟化实现存储空间的融合。通过CDP（连续数据保护）备份恢复实现秒级的数据备份恢复。基于VDC（虚拟数据中心）实现多组织/多业务共享资源，按需服务。通过云管平台实现平台资源的统一管理，同时提供完整的云内安全体系建设。

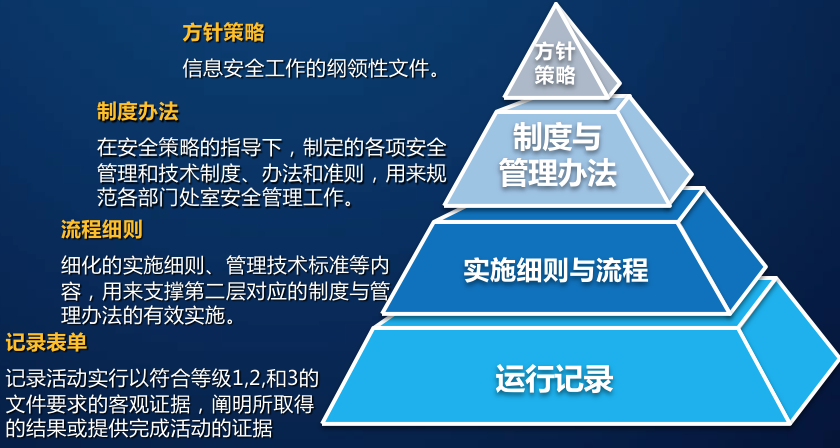


#### 3.3.2架构优势

超融合架构层以服务器虚拟化为底层架构，扩展出网络、存储、安全与桌面虚拟化，通过拓扑呈现的方式快速的构建出业务逻辑，实现虚拟资源的动态调度和灵活扩展，同时全网流量可视，配置简易直观，运维灵活便捷。

## 3.4 网络安全管理

根据信息安全管理工作的特点，制定信息安全工作的总体方针和安全策略，明确安全管理工作的总体目标、范围、原则和安全框架等。根据安全管理活动中的各类管理内容建立安全管理制度；并由管理人员或操作人员执行的日常管理操作建立操作规程，形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系，从而指导并有效地规范各级部门的信息安全管理工作。通过制定严格的制度规定与发布流程、方式、范围等，定期对安全管理制度进行评审和修订。安全的管理制度可以在很大程度上防止由于人为因素导致的安全性问题，同时，对一个信息网络系统来说，管理制度需要结合系统的特点以及系统所处环境的特殊性进行考虑。



## 3.5建立信息系统流通整合平台

通过与大型信息系统软件公司合作开发，实现各信息系统的接口对接，形成数据流通与分析平台，为精准决策提供数据支撑。

## 3.6实施规划

根据整体布局设计，按照分期分步、平滑迁移的原则，信息应用系统实施规划如下：

* **一期：**建立整体网络安全防护体系，建立超融合企业云区（包括云安全产品），建立本、异地数据备份系统；
* **二期：**建立信息系统流通整合平台。

# 产品选择与价格清单

## 4.1一期产品选型与价格清单

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 某大型公司设备清单 | | | | | | | | |
| **业务区域** | **序号** | | **设备名称** | **型号** | **数量** | **单位** | **单价** | **总价** |
| 边界 防护 区 | 1 | | 防火墙+入侵防御+WAF | AF-2000-H642 | 1 | 台 | ￥382,000 | ￥382,000 |
| 2 | | VPN设备 | VPN-1000-A400 | 2 | 台 | ￥22,700 | ￥45,400 |
| 3 | | 防毒墙 | AF-2000-H642 | 1 | 台 | ￥458,400 | ￥458,400 |
|  | | | | | | | | |
| 核心交换区 | 4 | 交换机 | | RS3300-52T-4F | 2 | 台 | ￥4,800 | ￥9,600 |
|  | | | | | | | | |
| 本部用户区 | 5 | 上网行为 | | AC-1000-E600 | 1 | 台 | ￥146,800 | ￥146,800 |
| 6 | 本地备份机 | | 科力锐 | 1 | 套 | ￥790,000 | ￥790,000 |
|  | | | | | | | | |
| 业 务 区 | 7 | 超融合服务器 | | aServer-2200 | 3 | 台 | ￥71,150 | ￥213,450 |
| 8 | 超融合--交换机 | | RS3300-28T-4F | 2 | 台 | ￥3,600 | ￥7,200 |
| 9 | 超融合软件 | | 网络虚拟化 | 6 | 套 | ￥5,880 | ￥35,280 |
|  | 存储虚拟化 | 6 | 套 | ￥14,602 | ￥87,612 |
|  | 服务器虚拟化 | 6 | 套 | ￥8,722 | ￥52,332 |
|  | 深信服云计算管理软件 | 6 | 套 | ￥3,332 | ￥19,992 |
| 10 | vAF | 1 | 套 | ￥10,682 | ￥10,682 |
| 11 | vAD | 1 | 套 | ￥32,379 | ￥32,379 |
|  | | | | | | | | |
| 分部用户区 | 12 | 上网行为管理设备 | | AC-1000-E600 | 1 | 台 | ￥146,800 | ￥146,800 |
| 13 | 防火墙 | | AF-1000-FA40 | 1 | 台 | ￥158,000 | ￥158,000 |
| 14 | 异地备份机 | | 科力锐 | 1 | 套 | ￥790,000 | ￥790,000 |
|  | | | | | | | | |
| 安全管理区 | 15 | 防火墙 | | AF-1000-FA40 | 1 | 台 | ￥148,044 | ￥148,044 |
| 16 | 堡垒机 | | OSM-1000-A600 | 1 | 台 | ￥65,000 | ￥65,000 |
| 17 | 态势感知 | | SIP-1000-A600 | 1 | 台 | ￥215,492 | ￥215,492 |
| 18 | STA-100-B420 | 1 | 台 | ￥52,822 | ￥52,822 |
| 19 | 防病毒中心 | | 深信服终端检测响应平台软件V3.0 | 1 | 套 | ￥100 | ￥100 |
| 20 | 深信服端点安全软件V3.0 | 100 | 套 | ￥1,764 | ￥176,400 |
| 21 | 北信源终端管理 | | 北信源数据泄露防护系统V1.0 | 100 | 点 | ￥643 | ￥64,300 |
| **总计（一年服务）：** | | | | | | | | **￥4,108,085** |
| **税金、利润、管理费** | | | | | | | | **￥821,617** |
| **合计** | | | | | | | | **￥4,929,702** |

# 4.2 二期系统整合预估

**4.2.1 现状和问题**

各部门在自行建立应用系统，依据自己的思路，解决各自管理上的问题。各个系统间数据不能互相流通和共享，传输数据使用手工进行，及时性和准确性都无法保证，也就谈不到精确控制，辅助决策。

**主要问题表现如下:**

**A**.有七个信息化产品在公司各部门进行运转。

**B**.各个系统模块应用情况各不相同，核心数据编码不同。

**C**.各系统模块的编码规则及标准不同。

**D**.各模块的信息传递是以上--业务的系统结果为基础进行手工录。

**E**.各模块得到的信息滞后时间较长。

**F.**最终财务结果输出准确性无法验证。

**G**.边制造边生产及变更信息的传递有待提升。

**4.2.2 建设目标**

信息化平台的建设属于推动公司战略发展目标的必要条件，同时也是公司发展智能制造和物联网理念的有效协同工具。建立统一信息化管理平台的核心目标：项目业务财务一体化，实现“两个标准化”即:数据标准化和流程标准化。完成“三个集成”，即:集成研发、集成业主计划、集成主数据。

**4.2.3 建设任务**

建立公司级的管理信息系统，支持大量原始数据的查询、汇总,借助计算机的运算能力及系统对客户订单、在库物料、产品构成的管理能力，实现依据客户订单，按照产品结构清单展开并计算物料需求计划，实现减少库存，优化库存的管理目标。

在公司中形成以计算机为核心的闭环管理系统，使公司的人、财、物、供、产、销全面结合、全面受控、实时反馈、动态协调、以销定产、以产求供，降低成本。

**根据已知信息，初步预估报价350万。**

* + - 1. **这文档是投标的么**
      2. **文档主要讲解安全，集成信息，企业信息发布、运营服务平台三点。**
      3. **具体处理业务未知**