**机房监管控运维可视化管理平台技术需求书**

**2019年03月**

目录

[1 概述 3](#_Toc2239841)

[1.1 目标 3](#_Toc2239842)

[1.2 建设内容： 3](#_Toc2239843)

[2 技术要求 6](#_Toc2239844)

[2.1 外网监控系统 6](#_Toc2239845)

[2.1.1 功能与参数要求 6](#_Toc2239846)

[2.1.2 网络监控可视化展示 6](#_Toc2239847)

[2.1.3 系统监控可视化展示 7](#_Toc2239848)

[2.1.4 用户体验监控 9](#_Toc2239849)

[2.1.5 管理平台 10](#_Toc2239850)

[2.1.6 基本功能模块 10](#_Toc2239851)

[2.1.7 基线管理 11](#_Toc2239852)

[2.2 机房动力环境监控系统 11](#_Toc2239853)

[2.2.1 动力环境监控系统功能参数 11](#_Toc2239854)

[2.2.2 动力环境监控指标 16](#_Toc2239855)

[2.2.3 统一告警管理 20](#_Toc2239856)

[2.2.4 运维数据分析 21](#_Toc2239857)

[2.2.5 移动告警管理 22](#_Toc2239858)

[2.3 内网监控系统 22](#_Toc2239859)

[2.3.1 功能与参数 22](#_Toc2239860)

[2.3.2 产品系统要求 22](#_Toc2239861)

[2.3.3 系统性能要求 22](#_Toc2239862)

[2.3.4 集中设备运行监控 22](#_Toc2239863)

[2.3.5 拓扑管理 24](#_Toc2239864)

[2.3.6 资产管理 24](#_Toc2239865)

[2.3.7 日志管理 25](#_Toc2239866)

[2.3.8 事件分析模式 25](#_Toc2239867)

[2.3.9 事件全文检索 26](#_Toc2239868)

[2.3.10 事件关联分析 26](#_Toc2239869)

[2.3.11 安全事件管理 27](#_Toc2239870)

[2.3.12 系统综合管理 28](#_Toc2239871)

[2.4 大屏展示系统 28](#_Toc2239872)

[2.4.1 系统设计说明 28](#_Toc2239873)

[2.4.2 可视化展示效果 29](#_Toc2239874)

[2.4.3 展示系统 30](#_Toc2239875)

[2.4.4 拼接处理器 30](#_Toc2239876)

[2.4.5 展示控制系统 31](#_Toc2239877)

[2.4.6 环境清理 31](#_Toc2239878)

[2.5 服务要求 31](#_Toc2239879)

[2.5.1 产品服务 31](#_Toc2239880)

[2.5.2 其他服务 31](#_Toc2239881)

概述

## 目标

建设机房监管控运维可视化管理平台，按照国家有关规定对网络系统、主机服务器、数据库、应用、安全、机房环境等内容进行监控、存储，可视化展示，根据工作需要形成日志，图表等内容，帮助运维人员提升运维工作效率和服务质量，改变被动管理、分散运维的现状，更好的保障信息系统整体安全高效稳定运行。作为机房安全管理和应急管理的重要支撑，确保发生重要安全事件时能第一时间进行故障定位和故障解除，满足“集中监控、集中维护、集中管理”的维护管理目标要求。

## 建设内容：

1、在外网部署一套监管控运维管理平台，并在IT运维管理系统中增加实时显示应用系统（中国机构编制网、事业单位登记管理系统、党政机关网站资格审核系统及互联网网络运维监控信息）的用户体验数据，比如用户实时访问量、网络带宽等功能。所有功能通过大屏进行可视化展示。同时，可以根据需要，将外网的IT运维管理系统、安防监控系统、动力环境监控、门禁等集成在一起，统一管理。

外网目前共有服务器100台、网络设备100台、另有应用系统、数据库、中间件和终端150个节点，总共约350个节点。未来可扩容到600节点

2、在涉密网A部署一套安全管理平台网络监控系统，实现对网络设备、服务器、终端、应用系统、中间件和数据库的监测，产品要有综合展示、资产管理、自动发现拓扑、日志采集过滤合并传输存储、安全事件分析、事件查询、全文检索、行为分析、安全事件可视化、集中运行监控等功能。产品需要有国家保密局涉密信息系统安全保密测评中心出具《涉密信息系统产品检测证书》，还要获得公安部信息安全产品检测中心出具的产品检测报告，并且该产品检验报告必须符合公安部《信息安全技术安全管理平台产品检验规范》，需出具相关证明材料，同时产品须获得公安部的《计算机信息系统安全专用产品销售许可证》。并通过国家保密局测评。

涉密网A目前共有服务器50台、网络设备10台、机房交换机10台、弱电间交换机30台、房间交换机50台、共有150个点，另有应用系统、数据库、中间件和终端若干，总共约250个节点。未来扩容到500节点。

3、将B401、B408进行整体规划后建设成为大屏展示区，用于展示涉密内网、非涉密内网、电子政务内网和互联网的实时监控情况。B401、B408房间配置2x2和2x3拼接屏及相关系统，六块分屏分别显示涉密网A、办公专网、涉密网B、视频监控、环境监控等监控信息。可以根据用户需求，拼接大屏显示系统既可满足支持每块屏单独显示一个画面、也可将实时的监控图像及PC等视频信号输出全屏显示。

4、产品配置清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 商品名称 | 描述 | 数量 | 单位 |
| 1 | 外网监控系统 | 大屏综合可视化展示、网络监控可视化展示、系统监控可视化展示、用户体验监控、机房动力环境监控可视化展示、统一告警管理、运维数据分析、管理平台、基线管理等功能（详见技术要求部分） | 1 | 套 |
| 2 | 动力环境监控系统 | 监测配电参数、配电开关、UPS、精密空调、漏水、温湿度、视频、安防、门禁、消防等参数与状态，当机房发生报警后能以手机短信、电话语音、声光、多媒体语音的方式及时通知管理员。（详见技术要求部分） | 1 | 套 |
| 3 | 内网监控系统 | 在涉密内网部署一套安全管理平台网络监控系统，实现对网络设备、服务器、终端、应用系统、中间件和数据库的监测，产品要有综合展示、资产管理、自动发现拓扑、日志采集过滤合并传输存储、安全事件分析、事件查询、全文检索、行为分析、安全事件可视化、集中运行监控等功能。产品需要有国家保密局涉密信息系统安全保密测评中心出具《涉密信息系统产品检测证书》，并获得公安部信息安全产品检测中心出具的产品检测报告。（详见技术要求部分） | 1 | 套 |
| 4 | 无缝拼接大屏 | 10块55寸高亮超窄边拼接液晶屏，分别布放在410、408室，分辨率不低于1920\*1080，物理拼缝≤1.7mm，亮度≥600cd/㎡，对比度≥4000:1，图像显示清晰度不低于950TVL，亮度鉴别等级不低于11级，点距≤0.53mm，选用液晶显示单元应具有多种接口，输入接口：VGA×1，DVI×1，BNC×1，YPbPr×1，HDMI×1，USB×1支持多种控制方式。（详见技术要求部分） | 10 | 台 |
| 5 | 拼接处理器：≤5U机箱+4路DVI输入（支持转VGA或HDMI）+8路HDMI输出+单主控板+单电源（详见技术要求部分） | 1 | 套 |
| 6 | 展示控制系统：能运行在国产cpu平台，支持龙芯、飞腾、兆芯。 | 1 | 套 |
| 7 | B401、B408设备原有设备迁移，房间装修，配置工作台。（详见技术要求部分） | 2 | 套 |

技术要求

## 外网监控系统

外网监控系统不仅能够对IT基础设施进行全面监控管理，同时更能协助运维人员建立完整的、以业务系统为核心的IT综合管理平台。它以CMDB（配置管理数据库）为核心，以网络、服务器、应用的监控为基础，以权限管理和日志记录为安全准绳，从而使IT管理从日常的运营监控、统计分析、发现问题、解决问题向流程化管理转型。

通过机房监管控运维可视化管理平台建设，应能帮助用户实现整体提升运维工作效率和服务质量，改变被动管理、分散运维的现状，更好的保障信息系统整体安全高效稳定运行。

机房监管控运维可视化管理平台具备如下功能：

可视化管理平台提供从网络系统、主机服务器、数据库、应用、安全、动力环境等几方面的运行状况的集中展示管理平台，可视化管理平台提供当前运行一览视图、业务一览视图、业务监测视图、网络监测视图、机房展现视图等多种监测视图来查看当前系统的整体运行情况。

### 功能与参数要求

实时方便查看整体信息平台运行状态。例如，可将网络、服务器、业务应用、机房环境等信息，在同一界面全屏显示，投放到大屏幕上。

●计有服务器100台、网络设备100台、另有应用系统、数据库、中间件和终端150个节点，总共约350个节点。

### 网络监控可视化展示

需要针对网络设备、链路、端口、流量使用情况等进行监控，实现网络拓扑的自动发现，并且自动监控网络资源的运行状态，有问题及时报警，并构建基于网络拓扑结构的运行可视化展示，直观展示网络的运行状态与水平。

网络监控视图支持自动生成，并可按需调整布局结构，支持多层级视图设置，设置视图钻取。

1）网络设备管理

●支持多厂商的网络设备，包括华为、H3C、迈普、Foundry、Juniper、锐捷、神州数码、DLink、联想、天融信、绿盟、启明、深信服等主流厂商的网络设备、安全设备等。能够自动识别设备，并且也可以手动添加未知设备。系统应支持SNMP V1/V2C/V3版本。主要包括以下功能：基础信息管理：包括设备品牌、型号、OS版本、硬件信息等；

●设备面板管理：支持对主流厂商全系列网络设备的背板图，实现设备的真实面板管理。并可直接在背板图上查看和操作端口。系统同时提供设备面板设计工具，支持个性化设备面板设计。

●提供设备网管信息查询，可查询端口列表、设备部件表、ARP表、TCP/UDP表、转发表、CDP表、STP、VPN表等。

2）网络拓扑管理

●系统可以通过SNMP、ICMP、NetBIOS、ARP、Traceroute、Telnet等多种手段自动发现、识别各种设备。并能通过多种拓扑算法自动生成准确的物理拓扑、网络拓扑和子网拓扑，同时提供可视化管理工具，可以根据实际环境和需要自定义拓扑图。网络拓扑发现采用多种策略主动发现拓扑，支持种子发现、网段发现模式。网络拓扑监控可呈现网络拓扑、物理拓扑、VLAN拓扑等，可以灵活的建立拓扑子图。网络拓扑支持对链路的自定义，可以在拓扑图上直接操作，指定链路两端设备与端口、双工类型，链路名称增加和删除链路，同时支持链路的隐藏功能；网络拓扑提供集成化的操作入口，提供快速的模糊搜索工具，提供设备和链路快速监测入口，提供TraceRoute、Ping、Telnet、SSH、Remote Ping、MIB浏览器等快速排障工具。

### 系统监控可视化展示

需要针对服务器硬件、操作系统、数据库、中间件等各类资源进行自动监控，主动发现资源运行过程中的隐患，并构建直观的业务应用运行展示视图。通过业务应用视图展示，实现IT资源和业务系统的关联，能够以业务应用为中心，显示业务应用的逻辑关系，包括相关的服务器、中间件、数据库、网络设备等。

支持在业务应用视图上直接显示相关资源的运行状态和报警信息，当应用系统服务发生故障时，能快速确定业务影响范围，定位问题的所在的资源位置及相关信息，便于管理员快速准确查找定位故障根源，完成故障恢复处置。

1）服务器和存储监控

●支持对IBM、HP、DELL、浪潮、曙光、联想等品牌主流型号的PC服务器和存储实现硬件监控，监控指标包括：电压、温度、风扇转速、电源状态、运行状态等。

系统能够管理和监测Windows、Linux、IBM AIX、HP-UX、SUN Solaris、SCO Unix等不同操作系统的服务器的运行状态和性能数据。

支持通过CLI、WMI、代理Agent方式监控服务器，Linux/Unix系统的CLI监控方式应当同时支持SSH及Telnet两种方式；

监控指标包括：具备CPU利用率监控，显示系统、用户、空闲时间的百分比；监控磁盘空间使用率；磁盘IO读写性能；磁盘的目录和文件大小监控；支持进程运行情况，对关键进程的CPU/内存的占用情况进行监控；监控服务器网卡的运行状态和网络传输情况。

支持自定义的监控能力，提供可配置、脚本化的监控采集扩展，同时支持远程监控脚本和代理监控脚本的扩展，可完成对自定义的文件检查、命令巡检等监控。

2）数据库、中间件监控

●支持各种平台上的Oracle、MS SQL Server、MySQL、Sybase、DB2等数据库系统，能够连续地监控数据库引擎的关键参数。

●支持包括Websphere WAS、WebLogic、WebSphere MQ、Tomcat、TongWeb等中间件监测管理。

3）基础服务监控

支持标准应用管理包括Apache、IIS、SMTP、DNS、FTP等的监控。

4) 虚拟机监控

●支持对Vmware、XenServer、Hyper-V、KVM的深度监控：

* 监控虚拟服务器配置、磁盘、网络、性能等指标，对可用性进行自动评估；
* 对虚拟服务器上部署的虚拟机进行监测；
* 在统一控制台即可监控虚拟机的所有物理和虚拟组件；
* 保证虚拟服务器以及其中的虚拟机正常运行；
* 在影响到最终用户前，及时发现和排除问题；
* 采用无代理监控模式，易于配置和管理实现。

### 用户体验监控

用户体验监测要求实现对业务系统的应用前端（WEB\APP）的运行性能、故障、用户操作体验、及用户行为的监控分析，为应用前端性能优化、故障处理、用户体验优化、应用评估提供数据支撑。

监控数据方式应当采用对应用尽量小的方式，应采用轻量级的插件，不应对应用业务逻辑进行改造。系统应具有良好的水平扩展能力，能够支持未来增加被监控业务系统的性能要求。

1）应用总体分析

●系统应当支持前端应用运行分析，展示应用总体访问情况，支持按访问用户数、操作数、错误数进行排序，方便领导和管理人员了解某项应用系统的访问分布情况，对应用的关心程度和使用情况等进行全面的分析,掌握热点应用、僵尸应用。

支持分析应用的界面性能、运行错误、用户轨迹、访问热力图等，并提供性能、错误、用户访问等主题数据看板，展示数据变化趋势。

用户访问热图支持展示用户访问业务系统的所关注页面区域，了解热点页面与热点操作。

2）前端性能分析

系统应支持运营商、地域、浏览器、操作系统、访问页面/操作等多维度性能分析

系统应支持监测页面各组件（包括Html文档、JS文件、CSS、Ajax资源、图片、字体等）加载性能：包括卸载、重定向、应用缓存、DNS、TCP、请求、响应、组件加载、渲染等全过程耗时情况。支持监测Ajax请求的请求、回应、回调耗时，并支持请求错误码采集。

3）页面错误分析

应支持按照浏览器、操作系统、运营商、地域等角度分析JS错误的分布情况，并提供排名显示哪些浏览器版本、或操作系统版本错误发生最频繁。

应支持识别发生前端错误的用户列表，了解其所在的区域、使用的浏览器类型及版本、运营商、分辨率、终端类型等信息，并支持记录用户应用访问的操作路径。同时支持定位页面发生的代码位置。

4）用户访问分析

应按照着陆页、操作系统、运营商、地域等角度分析会话的分布情况，并提供排名显示哪些浏览器版本、或操作系统版本使用的用户最多。

应支持某个用户最近1个月的应用访问趋势，并提供对用户操作行为的分析，掌握用户应用操作过程路径，记录每一个操作会话时间、操作数、平均响应时间等。

5）监测可视化配置

●应支持通过可视化界面设置监测数据采集点，需提供浏览模式与标记模式，支持页面上的菜单、按钮、图片、超链接等可操作的元素设置采集点，应用不需要做任何开发。

### 管理平台

提供全文检索、用户权限管理、个人桌面等功能。

●支持用户身份认证、授权检查等功能，具备完整的权限管理功能，实现面向组用户组织架构（部门）、角色的单独授权，授权范围包括功能模块、IT资源、展现视图、统计报表、告警列表等。支持三员管理，包括管理员、安全员、审计员。

针对不同的登录用户，提供个人桌面，定位不同用户各自关注的工作内容。系统支持根据用户个性要求进行换肤的能力。

### 基本功能模块

* 管理对象授权（License）：总数量600个，根据节点数进行授权。
* 网络设备管理授权:对各类网络设备、安全设备实现监控管理的授权
* 主机设备管理授权:对 Windows、IBM AIX、SUN Solaris、HP -UNIX、Linux、CentOS、Novell Suse、FreeBSD操作系统实现监控管理的授权
* 数据库管理授权:对Mysql、SQL Server、SybaseIQ、Informix、Oracle、DB2、Sybase数据库实现监控管理的授权
* 中间件管理授权:对Apache、Tomcat、weblogic、MQ中间件实现监控管理的授权

### 基线管理

支持性能指标基线管理，除了人工设定的标准静态阈值，系统还可以根据资源的运行周期规律（如周、月等），根据历史数据生成自动基线，并支持人工调整基线，设定基线的容忍度，对超过基线的情况，自动发送阈值事件到统一事件平台。

可按照业务划分不同的指标采集方案和策略，可自定义等级设备，按照设备赋予的等级自动匹配相应采集方案和告警策略。对不同等级设备的不同风险阈值可自定义设定。

## 机房动力环境监控系统

### 动力环境监控系统功能参数

对于机房动力环境系统，应能支持各种智能设备的快速监测，同时通过SNMP、数据库接口等其他接口方式可以实现客户化的扩展监控。

●系统采用“分散采集、集中管理”的方式进行设计，监测配电参数、配电开关1套、UPS2套、精密空调7套、漏水4套、温湿度31个、视频四十五套、安防4套、门禁6套等参数与状态，当机房发生报警后能以手机短信、电话语音、声光、多媒体语音的方式及时通知管理员。

1. 系统架构要求

●系统要求实现"本地采集+集中监控"的分布式结构，单点故障不影响其他设备链路的正常运行与监控。

要求现场数据采集采用嵌入式服务器，可以实现本地存储与控制，自带来电自启动功能。

●集中管理服务器要求实现双机冗余热备。系统要求能实现当主机故障时备机即时启动，确保监控数据的实时监控不间断、服务配置的不间断等。

●架构设计具有WEB访问能力，无需安装任何软件，实现WEB访问。

1. 稳定性要求

系统的软硬件均需采用成熟的设备，能够7×24×365不间断地连续工作，平均无故障时间(MTBF)大于20万小时，平均修复时间(MTTR)小于2小时。

●要求系统具有非常高的稳定性，排除硬件设备的故障外，系统的误报率要求低于0.1%。

1. 安全性要求

机房动力环境监控系统要求提供完善的操作权限管理功能，口令验证及权限验证。

●操作管理分权限管理。要求系统支持用户管理和组管理。每个用户组可以设定组成员特定的权限，包括允许查看的内容、允许控制的设备等。使得每个用户无论在服务器端还是在WEB端访问系统都是具有独立权限的，避免无权限人员对系统误操作和信息泄漏。

所有操作要有详细记录，并存入历史数据库。每个远程用户的登录，其登录时间、主机IP及用户名均应完整记录，其所进行的操作：修改系统配置、控制设备运行等，也应完整记录，系统管理员可以随时检查每个用户所作的操作。

1. 扩展性要求

要求支持标准的SNMP服务、OPC服务接口，以便将来与楼控或其他系统接口。

要求系统提供完备的二次开发平台，开发人员可以嵌入各种windows控件，可以用标准的脚本语言对功能进行任意扩充。

监控管理系统应具备较强的扩展能力，可以建成最小的基本系统，也可以建成较全面的大系统。并允许对多个机房的集中监控，满足系统扩容的需要。

●应支持在线编辑系统，可在不停止运行的情况下配置系统、修改界面等。

●可扩展三维可视化功能，不外加服务器和系统，与动环系统同一平台，模拟机房实际场景，实现漫游监控，提供自动巡航、全方位无障碍穿透查看等更加直观有效的监控效果。

1. 集成度要求

●在同一平台上将动力环境、门禁、数字视频等整体集成，远程浏览器访问界面应与监控主机完全一致，以提高系统可靠性、可管理性、易用性、安全性。

报表、报警设置等截面要求为统一窗口界面，不得外挂窗口和程序。

1. 人机交互要求

●界面以图形界面为主，主界面地图必须为3D视角地图，图形化+菜单化操作方式，保持美观、直观、易用。

要求系统必须为中文操作及编辑系统，简单易学易用。

所有报警以文字+电子地图形式弹出，具有明显提示。

监控界面支持放大缩小，便于管理查看。

要求动画界面仿真设备运行。

●要求具有多界面同时在单一显示器或多显示器显示的功能，例如单一显示器可分4个界面同时显示4个子系统的状态、参数，且4个界面均可独立操作或设置某一界面为主操作界面，其他界面的内容根据主操作界面的操作而改变；软件功能需具有单显示器最多16界面同时显示、多显示器任意数量界面扩展的功能，多界面显示时不得存在机器速度变慢、系统运行变慢的问题。

1. ●报警管理要求

提供电话语音报警、短信报警、声光报警、多媒体语音等多种报警方式；

报警可以根据重要级别将同时发生的报警排序处理。

要求系统有报警输出记录，自动记录报警的发出事件、内容、种类、是否发送成功等。

定时自动推送功能：应支持管理人员在系统上自定义时间，设定系统自动发送短信、邮件的方式报告机房运行情况。

远程控制功能：应支持自定义短信控制命令，用户可通过短信命令查询机房运行情况、控制设备动作（包括门禁开关门、启停空调等），支持单一命令批处理功能。

系统具有排班报警管理功能，可根据值班状况选择报警发送对象，非值班时间将不收到报警。

报警需具有分组功能，管理该组设备的人群才收到相应报警，避免报警信息发给不相干人员造成职责不清。

报警需具有分级功能，不同级别的人员收到不同级别的告警。级别可以在特定情况下自动提升，例如事件报警发生后，未在规定时间内完成处理，使报警恢复，要求自动提升级别，使更高层级的管理人员关注，避免引起事故。

系统统需具有防误报警功能，可对报警值设定连续报警时间和恢复稳定时间，避免空调冷凝水、温度临界浮动等特殊情况出现时频繁、大量的出现告警。

要求对机房各系统提供的监控数据进行实时报警、保存和事后分析。

系统各监控参数界面提供设备状态显示模块，包括设备的撤布防，通讯状态和故障状态等，能有效的针对设备进行检修或状态判断。

要求系统提供设备检修布撤防功能，当设备报警撤防时，可以实现正常安全检修而不对外报警，避免系统误报警。

要求提供报警后手工复位功能，某些重要数据量（如消防报警、有人非法侵入机房等）一旦发生报警以后，即便该报警已恢复，报警系统必须仍进行报警，直到管理人员点击复位按钮，确认该事件，同时系统记录该确认操作。避免火灾引起的线路烧坏、设备故障等，造成系统检测到错误的恢复信号，而造成系统报警管理盲点。

要求系统具有报警根源分析功能，只有一个报警源引起的多个报警出现，可直达报警根源，对外只发送根源报警，屏蔽其他分支报警信息。例如：停电时，不得发出大量连锁性告警，只发出停电告警。

整系统备份功能，系统要求支持本地异地备份能力，在不停止系统运行的情况下，通过只执行文件对系统整体备份，在本机或异机生产一个整体的备份文件，在系统遭到破坏时，可通过备份文件根据指引进行系统恢复。

支持在线编辑系统，可在不停止运行的情况下配置系统，进行整系统一键备份，可扩展备份计划，包括自定义定时备份时间和本地异地备份路径等。

1. 系统联动要求

●需支持自由设定联动逻辑条件，采用菜单式设置界面，在某一个状态或参数变化至设定条件时，自动进行设备的自动联动操作。

通过设定联动逻辑，可将不同监控设备或不同子系统进行联动，即可以设定一些事件触发条件，当满足这些条件的时候，系统可自动执行某个功能或者启动另外一个设备工作。例如：当报警发生时，监控系统联动视频系统，弹出对应区域的视频画面并自动录像，利于故障的溯源、倒查。

联动逻辑的设定及修改必须为菜单化的简单操作，不需重新编程，要求功能支持管理人员通过基础培训后，可自行设定、编辑联动逻辑。

1. 数据管理要求

实时数据：系统应能够监控到相关设备的实时参数，并能通过曲线趋势图进行显示。

历史数据：对预设的监控对象有关参数，系统应自动保存历史数据。任何历史数据必须有操作密码才能进行修改或删除，保证数据的可靠性、安全性。为防止病毒感染文件，造成历史数据文件的破坏，历史曲线的数据需保存在数据库中。

数据曲线选取浏览：对监控设备的任意曲线数据进行选取查看，提供基本的模糊查询功能，能实现不同的曲线根据不同的颜色同界面显示。

数据导出功能：要求提供数据点和数据表的灵活导出功能，可对各个监控设备数据点或数据表进行选取，自定义时间跨度、数据采集间隔，支持报表输出。

系统所有的数据应可以保存三年以上。

●要求具有自定义报表功能，例如设备定时巡视、巡视重要数据记录、巡视考勤、电池放电记录（所有记录均为自动报表记录）等报表，在监控系统中完整实现，并能把以上数据进行汇总，输出到excel或word文档，并在统一界面下提供远程浏览和配置功能，要求报表格式可由用户修改，报表内数据逻辑可由用户定义。

●要求系统支持数据周报、月报、年报，具有数据分析、计算功能，要求管理人员可自行编辑报表的格式、存储逻辑，报表要支持计算公式的编写，逻辑运算的设置。

●要求系统支持巡检值班报表、考勤报表、值班交接班报表，并可输出为文档。

所有报表的配置和生成都必须在监控系统程序界面中完成，不得外挂程序和使用其他工具界面，并提供友好、简洁的界面供机房管理员进行自定义更改，要求可根据在系统中绘制的样板表格自动转绘到EXCEL、WORD系统中，报表格式可由用户自己修改，报表内数据项可由用户定义。

1. 远程管理要求

●要求系统提供完整的WEB功能，授权用户可以通过浏览器（IE）访问监控系统，内容包括实时状态、历史曲线、事件查询、实时视频、录像浏览、球机控制、报警设置等所有功能，其界面应与监控站完全一致。

要求如下：

WEB页面需可以使用与监控站主机同样界面查看所有监测数据，并可自动根据监控站的更新而同步。

WEB访问端可不需增加任何软件、做任何特殊配置的前提下实现报表的检索、查阅、输出、打印，例如：巡检报表、日报、月报、数据分析报表、曲线报表等；

可实现报警的所有设置功能，短信双向查询设置功能。

支持IE5版本及以上的所有版本浏览器及第三方浏览器的访问。

### 动力环境监控指标

为满足机房监控报警的要求，机房需提供综合环境监控系统，该系统能够实时显示并存储以下信息：

1. **温湿度监控**

功能：对机房重要区域的温湿度、机柜内温度进行监测。

监控范围包括机房内各功能间、UPS间和各楼层配线间共计至少31个采样点。

其中屏蔽机房部署4个温湿度采样点，

外网机房+专网机房共6个温湿度采样点，

接入机房2个温湿度采样点，配电机房2个温湿度采样点，

机房走道2个温湿度采样点，UPS间2个温湿度采样点，

13个楼层配线间各部署1个共13个温湿度采样点，

以上共计31个温湿度采样点。

* 温湿度监控硬件应具备CE认证证书及检测报告。
* 要求监控系统对环境温湿度提供实时信息，曲线图直观反映机房温湿度变化情况，迅及、多种告警手段保障了机房环境安全。
* 实时采集温、湿度信息，并能按天、按月、按季进行统计，并能绘出时间段变化曲线图，同时提供打印功能。

1. **漏水检测**

功能：监测机房内空调四周漏水情况，漏水监测可精确到米。

参数：屏蔽机房1套，外网机房+专网机房1套，接入机房1套，配电机房1套共四套，漏水线缆长度总长度不少于30米。

* 漏水检测硬件应具备CE认证及检测报告。
* 以电子地图方式实时显示并记录漏水线缆感应到的漏水状态、漏水位置及漏水控制器的状态。

1. **门禁系统**

功能：能记录、查询所有出入门禁的信息。

根据机房的设计要求，新增门禁系统6套；机房大门、外网机房1个、专网机房1个、配电机房1个、UPS间（地下一层）1个、接入机房1个，采用指纹/密码/刷卡+出门按钮方式，门禁系统传输协议要求采用TCP/IP协议。

门禁系统应为不同的管理人员，在不同的出入口、不同的时段设定不同的进出权限；监测门的开关状态；记录进出的时间、门区及人员，分类查询进出门统计资料和报警资料，为事后分析提供依据。当设置了开门报警时，门一旦被开启，监控系统自动弹出报警画面，通过多媒体语音、电话、短信等方式报警。

门禁系统与机房监管控一体化运维可视化管理平台进行无缝集成，人员录入、权限设置、门禁资料传输等各种门禁功能都在机房监管控一体化运维可视化管理平台中统一完成，无需外挂门禁软件。在环境监控系统平台界面中实时显示人员进出记录资料，动态显示门的开关状态，并可远程控制门的开启，并与消防联动，当发生火警时自动切断每个电子锁的供电打开门禁。

门禁管理系统应具备如下功能：

* 系统应由关系型数据库作为后台支持，可以在线管理，保证系统安全性；可提供丰富的周编程、日编程、节假日等方便用户的管理。
* 操作权限设置功能：对所有的用户可以实现分级别、组、部门进行管理，针对不同级别的操作员需要提供不同的密码，并且每个管理级别的管理员对系统操作的权限等级可由系统任意设定。
* 系统可以对内部人员进行发卡、授权，也可对临时人员制作临时卡，并可对持有该卡的人员进行跟踪、定位、限制活动区域、设置出入路线等。
* 系统支持脱机的全局联动：一旦管理PC出现问题控制器可以进行独立工作完成预制的联动工作。
* 联动功能：系统应与消防系统联动，保证在大楼火警、地震等紧急情况下，各门禁控制的房门能由房间内/外的人开启疏散。
* 接口功能：PC 数据接口，利用以太网络实现与其它集成系统交换数据。
* 加密功能：系统软件与门禁控制器之间通讯具备加密功能。
* 刷卡记录：当人员进/出门时需持卡在读卡器前进行读卡，读卡器读取信息后，将信息传送到主机，主机首先判断该信息是否合法，如合法则发出开门指令（即向电锁发送一接通信号，使门打开）；不合法则不发送开门指令并可发出警报。同时主机会将刷卡信息、日期、时间等数据保存以供查询或直接传输到电脑进行处理。
* **门禁控制器产品具备CE认证、FCC认证证书。**

1. **视频监控**

功能：应能实时监视各路视频图像，通过在电子地图上点击相应的图标即可查看该摄像机的当前画面。通过开放的体系架构，全面、丰富的产品支持，为用户提供随需应变的整体解决方案。

* 应支持灵活设置录像方式，包括24小时录像、预设时间段录像、报警预录像、移动侦测录像以及联动触发录像等多种方式。
* 应支持历史视频检索回放功能，可根据录像的类型、通道、时间等条件进行检索，回放速度可调。
* 应 支持与其它子系统的联动功能，如：门打开或发生防盗报警时联动摄像机进行录像，同时弹出相应的视频画面窗口等。

1. **精密空调监控**

功能：对机房内的精密空调的运行状态进行实时监测。

发生故障时及时告警

* 回风温度、回风湿度、回风温湿度限值、温度设定值、湿度设定值、加热器运行状态、制冷器运行状态、除湿器运行状态、压缩机高低压报警、主风扇过载报警、滤网堵塞报警等。
* 空调控制（空调的远程开机、关机；温、湿度的远程设定）。

1. **烟感监测**

功能：对机房内的消防主机状态进行监测。

* 监控机房内消防报警状态，系统检测消防主机的信号，即时显示消防系统状态。

1. **报警告警**

* 系统应具有多种方式的并行报警能力，发生事件报警时可根据级别高低进行排序告警，级别高的先报警，级别低的后报警；
* 系统应具有短信、电话、多媒体语音等多种报警方式，报警方式可由用户根据级别、重要程度、报警内容自行设定。例如将温度过高预警设定为短信告警，温度过高报警设定为电话语音报警等。
* 系统语音告警应采用真人语音方式，报警发生时系统界面可自动跟踪；特殊报警应支持人工屏蔽；报警须支持通过详细的检索查询器及报表生成工具，能直观准确的定位告警位置；应具有确认过程，可录入处理意见和结果。
* 在设备发生报警后，维护人员进行报警确认响应或设备故障排除前，系统应持续告警，同时系统应支持对本语音报警进行消音处理的操作。
* 针对测点，应可支持用户自定义报警级别，自行设置灵活的定义/屏蔽报警类型（高限报警、低限报警等）。
* 提供报警级别的详细化管理，应具备10-255个报警级别，以便管理员定义不同级别对应不同的报警方式。
* 系统应能自动对发生的报警按级别高低进行优先选择，当有不同级别的多个报警同时发生时，系统应先对级别高的进行报警提示，再依次根据级别高低对其他的报警进行提示。
* 监控系统发现报警后，事件栏将自动弹出提示报警信息，显示并打印告警信息，事件栏内显示的内容包括告警级别、站点名称、告警设备名称等数据。
* 所有报警应支持以电子地图形式弹出报警页面，报警信息须提供可视化管理窗口，发生报警时可供管理员方便的在维护窗口中进行维护。
* 系统应具备灵活的查询方式，通过条件筛选对报警事件进行查询、统计和打印，并可进行条件排序。
* 系统应支持告警的转发，可以将告警信息传递给第三方应用系统（如IT设备集中管理系统），并可无缝集成。

1. **监控记录**

* 系统应支持实时查询相关机房及设备的状态、参数，提供实时数据曲线、历史数据曲线功能，可对设备当前的参数变化进行密切的实时监测、历史数据的回滚查看等，并可实时打印；同时系统还须支持设置策略，当设备参数值达到某个标准时进行自动打印。
* 系统应支持对设备的重要参数可进行历史数据保存，可在直观的坐标图中以曲线形式显示，并可支持屏幕打印输出。
* 监控系统对历史数据曲线存储应采用二进制DAT文件格式独立存储，在数据较多时确保能够快速检索，对数据应进行加密，确保具有高可靠性，他人无法轻易进行破解和反编译行为，无法篡改。
* 应提供用户对曲线的显示精度进行时间范围调整的功能，可以细致到以秒为单位的曲线变化输出，并支持通过游标线的移动对曲线进行回滚查看。
* 所有打印出来的曲线图都应支持对打印范围的数据进行分析，显示出最高值/最小值分别为多少。
* 须提供报表功能，除提供日常报表模板外，还可根据用户要求定制各种样式报表，并可以多种格式打印输出（EXCEL，ACCESS，自定义等）。
* 系统应具备用户操作日志、系统运行状态日志、报警日志等日志。所有日志应支持根据查询条件即时生成报表，并可打印输出。
* 系统应支持对任何设备参数实现报表功能，报表中会对设备参数进行专家级数据分析，为用户的维护提供准确的数字依据。
* 系统应支持对所有历史、实时数据进行灵活定制条件查询、统计、输出和打印操作。并可对查询后显示的数据进行条件排序。

1. **电力/UPS监控**

UPS电源和配电柜是机房动力系统安全重要保障，要求从监控系统的UPS/电力监控视窗，反映电力系统的运行状态，包括：配电柜进线三相电的开关状态、相电压、线电压、相电流、频率、功率因数、有功功率、无功功率等参数及UPS整流器、逆变器、电池（电池健康检测，含电压电流等数值）、旁路、负载等各部分的运行状态与参数。

### 统一告警管理

故障管理实现对故障的完整的处理过程，包括格式化、过滤、压缩分析、自动消除、通知策略联动等。

●支持事件的接入标准化功能，无需经过二次开发编译，通过配置界面配置接入规则，即可接入新的告警事件，支持装载SNMP MIB来解析Trap。

支持事件过滤功能，通过配置事件过滤规则，对事件进行过滤，抛弃不需要关注的事件。

支持告警压缩功能，通过配置界面设置事件压缩规则，将重复事件进行压缩处理，并根据条件更新告警的部分信息（如最新告警时间、告警次数等）。

支持告警归并功能，可以设置告警归并规则，可对自动恢复的告警事件进行归并消除，例如：端口Up事件自动消除端口Down告警。

●支持告警升级，能够升级到指定级别，或者按照递增指定等级升级到相应告警等级；

支持告警通知规则，可配置自动向告警责任人发送告警通知，支持声音、电子邮件等多种通知方式，支持工单派发接口。

集中告警台的功能界面要求包括：告警导航、告警查看、告警处理、规则定义等几方面功能。同时可根据用户的实际需求定制事件的显示格式。

●支持告警的灵活分类，可以按照告警的导航分类看快速查看告警，分类树中显示分类下的未解决的紧急、主要、次要告警数量，并可以设定每一类的查看管理权限控制；

支持快速查看最新告警、处理中的告警和历史告警，可以通过告警快速跳转到对应的设备页面；支持人工进行告警确认和派单。

●系统支持计划停机管理，可设置停机计划的时间段及涉及停机的资源，设置完成后执行即可生效，在资源可用性报表当中可忽略计划停机时段。系统支持同时运行多个停机计划。

### 运维数据分析

报表系统提供历史数据分析，能够分析统计各类资源的历史运行数据，包括历史性能数据、历史告警数据，通过对历史数据的统计和趋势分析，帮助管理人员了解整体IT环境的运行质量，从而为运维持续优化提供数据依据。

能够提供柱状图、柄图、折线图、数据列表等多种灵活、形象的分析图表。且数据组合方式能够基于部门划分、设备、时间段、TopN等多种查询方式进行，提供多种组合条件的统计分析。

### 移动告警管理

系统具有移动告警功能，可根据要求，预设和修改告警信号发送对象。

三年内相关服务费用由中标人承担（如需移动电话号码的，由中标人办理并承担相关费用）。

## 内网监控系统

### 功能与参数

实时方便查看信息平台运行状态。例如，可将网络、服务器、业务应用、安全产品等信息，在同一界面全屏显示，投放到大屏幕上。

参数：服务器50台、网络设备10台、机房交换机10台、弱电间交换机30台、房间交换机50台、共有150个点，另有应用系统、数据库、中间件和终端若干，总共约250个节点。未来扩容到500节点。

●产品有国家保密局涉密信息系统安全保密测评中心出具的《涉密信息系统产品检测证书》

### ●产品有公安部信息安全产品检测中心出具的产品检测报告。产品系统要求

●产品要求为软件形态，支持部署在Linux64位操作系统上。系统管理设计采用B/S架构，管理员通过浏览器对管理中心进行各种操作。客户端浏览器无需安装JRE或者JAVA Web Start等任何组件即可访问管理中心；

●产品必须内置数据库，无须再单独安装数据库系统，亦无须对数据库进行专门的维护。数据库采用大数据系统架构，必须满足海量安全事件的存储与快速查询与检索，数据库存储节点支持分布式弹性扩展，实现数据库存储集群，实现存储冗余。

系统兼容性好，支持IE、Chrome与Firefox等浏览器访问管理中心。

### 系统性能要求

●作为衡量安全系统内置各种算法的检测指标，要求事件处理性能不低于每秒30000条；单节点10亿条事件简单搜索完成用时2秒；对被管控资源的监控，其并发监控任务个数不低于1000个。

### 集中设备运行监控

系统支持对各种不同厂商的安全设备、网络设备、主机的性能与可用性进行集中化实时监控；支持各主流厂商数据库、中间件、网络服务、以及以及各种应用系统的性能与可用性进行集中化实时监控；支持通过SNMP、TELNET、SSH、SSH2、ODBC、JMX、协议仿真等方式对IT资产进行性能与可用性信息的周期性采集。

* ●**网络设备监控**

支持通过SNMP协议对主流网络设备进行监控，包括但不限于路由器、交换机、负载均衡、光纤交换机等；

支持监控网络设备的基本属性，以及性能与可用性指标，包括但不限于：设备名称、IP信息、描述、节点状态、运行时间、接口信息、路由信息、网络状态、网络性能信息等。

* ●**安全设备监控**

支持通过SNMP协议对主流厂商安全设备进行监控；

支持监控安全设备的基本属性，以及性能与可用性指标，包括但不限于：设备名称、IP信息、描述、节点状态、运行时间、接口信息、网络状态信息、网络性能信息等。

* ●**主机监控**

支持主流版本的Windows、Linux、AIX、Solaris、HP-UX等主机和服务器；

支持监控主机基本属性，以及性能与可用性指标，至少包括：名称、IP、描述、节点状态、运行时间、网络接口信息、CPU利用率、内存利用率、磁盘利用率、磁盘IO、文件系统、安装软件、安装服务、运行进程、 网络连接；

支持用户自定义监控指标，例如可以对Windows、Linux、AIX、Solaris、HP-UX等主机的任意进程进行监控。

* ●**数据库监控**

支持对主流版本的MS SQL Server、Oracle、DB2、Informix、Sybase、MySQL等数据库进行监控；

支持监控数据库的基本属性，以及性能与可用性指标，至少包括：名称、版本、端口、主机名、内存信息、运行状态（例如命中率状况，数据库等待事件，Lock和latch争用情况，Shared pool的使用情况，排序使用的情况，Redo log使用情况，登录用户情况等）、事务信息、缓存信息、连接信息、锁信息、SQL统计、命中率信息、表空间信息、访问方法明细、数据库明细等。

* ●**中间件监控**

支持对主流版本的Weblogic、WebShpere、Tomcat、Apache等中间件进行监控；

支持监控中间件的基本属性，以及性能与可用性指标，至少包括：名称、版本、端口、连通性、运行状态、CPU、内存、事务、JVM Runtime、队列、Servlet会话、线程池、EJB、JDBC连接等；

* ●**应用监控**

支持各种网络服务的监控，包括并不限于：SMTP、POP3、HTTP、FTP、TELNET、SSH、DNS、DHCP、WINS、LDAP；为保证产品在实际环境的监控效果，以下各项的监控指标必须全部满足：

支持监控邮件服务（SMTP/POP3）的连通性、响应延迟；

支持监控WEB服务器（IIS和TOMCAT）的连通性、传输速率、用户访问数、会话数等；

支持对URL的连通性和响应延迟进行监控；

支持对指定网页进行监控，基于正则表达式进行网页内容检测；

支持在网页监控中进行关键字匹配告警、关键字不匹配告警、正则表达式匹配告警、正则表达式不匹配告警；

支持监控通用服务（TCP、DNS、DHCP）协议的连通性、响应时间。

* **自定义监控**

支持自定义监控类型；可以通过SNMP OID方式扩展监控指标；支持通过正则表达式建立监控指标；

* **网络故障诊断分析**

系统具备基于故障树的网络故障诊断功能，能够自动判别故障源；

系统能够可视化地展现一幅故障树，并标记出故障节点；

系统能够显示故障告警趋势图、故障告警等级分布图。

### 拓扑管理

●系统能够描绘出网络拓扑图，展示IT资产之间的逻辑拓扑连接关系，并能够自动进行多种拓扑布局；支持用户可以手工编辑资产拓扑，至少包括添加节点，添加/编辑连线，任意拖动节点，可以对拓扑图进行缩放，可以更换拓扑图背景；支持设备和链路运行监控功能，必须支持智能标记设备故障或链路故障能力，在拓扑中展示；支持网络拓扑图和网络设备列表之间进行自主切换；系统支持虚拟机房展示功能，系统能够以机架视图的形式可视化地显示设备在机架/机柜摆放位置，其支持用户可以自定义机架视图；机架视图能够实时展示设备的运行状态，如果设备发生告警，会自动加以标识。

### 资产管理

●系统具有资产管理的功能，支持对被管理IT资产进行分组、分域的统一维护。

系统提供基于资产的拓扑视图，可以显示资产之间的逻辑连接关系。系统可以按列表和拓扑两种模式显示资产拓扑节点；支持随意在资产的拓扑视图和列表视图之间进行切换；

支持用户手工编辑资产拓扑，包括添加节点，添加/编辑连线，任意拖动节点，可以对拓扑图进行缩放，可以更换拓扑图背景；

在资产拓扑上选择每个资产节点，可查看每个资产的的信息，至少包含基本属性、事件信息、告警信息、漏洞信息、风险信息、关联事件、访问配置数据等，并且支持向下钻取，直接进入事件列表、关联告警列表；

支持资源自发现功能，能够自动将被发现资源添加到资源库；

支持用户对资产标签自定义，实现对资产属性的动态扩展。

### 日志管理

* ●**日志采集**

无需另外安装软件组件，管理中心即可通过 SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC等多种方式完成日志收集功能；

可灵活定制不支持的数据源采集，而无须改动代码。

* **●日志范式化**

系统必须具备日志范式化功能，实现对异构日志格式的统一化；

范式化字段至少应包括事件接收时间 、事件产生时间、事件持续时间、用户名称、源地址、源MAC地址、源端口、操作、目的地址 、目的MAC地址、目的端口、事件名称、事件摘要 、等级、原始等级、原始类型、网络协议、网络应用协议、设备地址、设备名称、设备类型等；

对日志设备类型、日志类型、日志级别等可进行重定义。

在范式化的时候能够对日志进行分类，分类需按照安全事件的类型，而不是日志的设备类型，并提供日志分类的类型清单。

* ●**日志传输和存储转发**

日志可加密压缩传输，保证数据的完整性和机密性；

日志可加密存储。支持大数据量存储；

可根据转发条件，将采集范式化后的数据转发到其他的目标地址；

支持加密压缩方式转发，定时转发。

* ●**日志过滤**

1）要支持对无用日志的自动过滤，减少垃圾数据数量；

2）可以建立日志过滤条件；

3）过滤条件可以按照所有范式化后的字段属性来定义。

* ●**日志合并**

1）要支持对无用信息的自动合并，减少垃圾数据数量；

2）可以建立日志合并规则，设定合并的时间范围。

* ●**日志源管理**

系统可以统计不同采集器和不同安全域下的设备个数并以饼图展示，统计采集器或安全域中事件量Top10以柱图展示，配以统计列表；

可以根据日志源断点时间进行配置，并生成告警。点击单个日志源设备查看该设备最近7天的事件趋势。

### 事件分析模式

●系统采用基于策略的事件分析模式，使用户从传统的“条件编辑”式的分析体验转变为“策略选取” 式的分析体验，大大提升分析效率；

系统提供交互式事件分析模式，供用户按照自己的需求通过仪表盘与系统存储的所有事件进行交互，实现按需查询，支持查询嵌套，可任意回退，查询时间缩短至秒级。系统可将用户的查询条件保存为策略，供后期快速分析使用，支持策略的导入导出；

●系统应内置不少于1000条分析策略，包括各种实时分析策略、历史分析策略、告警统计策略、工作台仪表板视图、报表报告策略等。

### 事件全文检索

系统提供输入关键字搜索，从海量事件原始信息中获取与关键字匹配或部分匹配的所有事件；

系统提供基于正则表达式的检索功能，用户可在搜索栏内输入正则表达式，系统可搜索出原始信息中与正则表达式相匹配的所有事件；

●检索完成后系统会在检索结果中，事件原始信息中以高亮方式显示检索的内容。

### 事件关联分析

* **基于规则的事件实时关联分析**

系统具有基于规则的安全事件实时关联分析的能力，能够对不同的事件进行相关性分析，发掘潜在的信息；

●系统提供基于图形化方式的关联规则编辑器；

在编辑规则条件的时候，可以针对事件属性引用规则、应用资产属性、引用资源；

●可实现统计计数关联，能够设定一段时间内的事件发生次数的阈值，还能指定重复事件的属性特征；

支持观察列表功能。管理员能够根据关联分析的结果将可疑或者需要关注的信息列入观察列表，并对观察列表中的信息进行任何关联，可以被任何规则引用

●关联分析规则具备测试功能，分析师能够更方便地对新设计的关联规则进行模拟测试，以便调校规则的作用效果。

具有多级关联的能力，即一次关联后的事件可以跟其他事件再次关联，并不断的延展下去，二次关联，三次关联，四次关联，等等，深度不限。

●根据需要结合应用场景，系统可重定义关联事件中一个或多个字段的值，比如某些原始事件触发了某一关联规则而产生新的关联事件，原本是一个自动不可干预的过程，关联事件重定义可以凭借安全专家经验，重定义及补全像事件类型、事件名称、摘要描述信息，起到修正、补正信息的作用。

关联分析规则具备灵活的时间窗口触发功能，不仅采用单位时间内发生多少此便触发的单一方式，还具备触发条件动态定义的功能。

●支持多事件关联，对不同来源的安全事件进行复杂的相关性分析。

* **基于观察列表的长期事件关联分析**

系统支持基于观察列表的事件关联分析；

可分析长期和短期事件的实时关联分析，可将关注的事件或符合条件的事件保存至观察列表中供后续规则读取并关联；

●可将关注的字段保存至观察列表中供规则读取并对事件进行实时关联。

* **基于情境的事件关联分析**

系统能够将安全事件与当前网络和业务的实际运行环境进行关联，透过更广泛的信息相关性分析，识别安全威胁；

系统应至少支持基于弱点的情境关联、基于资产的情境关联、基于网络告警的情境关联。

### 安全事件管理

* ●**事件分析**

系统允许管理员以策略的形式从各个维度实时查看安全事件；

用户可自定义事件分析条件，并可保存为策略，以树形结构进行组织，形成一个分析策略树；

可以显示一段时间的动态事件移动图，能够在图上显示每个时间切片的事件数量、等级，并能够在图上显示每秒事件数。用户点击每个时间切片，可以查看该切片内的事件；

动态事件移动图可设置动态刷新频率，根据刷新时间显示实时事件；

可以多种形式展示动态事件移动图，包括折线图、柱状图、折柱混合图、等级堆积图等，并可进行选择切换，支持以鼠标选择时间区域，并显示相应事件；

系统支持即席在线查询，支持嵌套查询，可针对查询结果任意回退，收敛事件范围；

用户点击事件任意属性字段，可以该字段为条件对事件进行统计分析；

可以对事件依据其源目的IP和端口等各类字段信息进行深入的事件追踪调查，支持无限次数的追踪调查；

对于关联事件，可以钻取出导致该关联事件的原始事件，并可查看关联规则；

可以对选中的事件源/目的IP地址进行全球地图定位，包括在线定位和离线定位；

可以对选中的事件进行事件拓扑分析，并可视化的展示一幅描述事件之间相互关系的事件拓扑图；

可以以图形化的方式展示日志属性之间的聚合关系，显示多维事件分析图；

可以对选中日志进行视网膜视图分析，以可视化方式展示日志的源IP与目的IP分布走向。

* **事件可视化**

系统具备丰富的事件可视化展示能力，具备多种展现手段，至少包括事件拓扑图、IP全球定位图、动态事件移动图、事件多维分析图、资产拓扑图，等等

* **存储管理**

●系统应提供事件维护功能，动定时备份采集上来的安全事件，也支持手动备份与恢复；管理员可设置事件存储容量告警阈值。

### 系统综合管理

* ●**告警管理**

告警动作支持告警重定义、弹出提示框、播放警示音、发送邮件、发送SNMP Trap、执行命令脚本、设备联动、发送飞鸽传书、发送Syslog、设置观察列表、引用通知等方式；

告警内容可以自定义，可以根据日志的实际情况将参数（即预定义变量）传递给命令行脚本；用户可自定义告警统计策略，并以树形结构进行组织，形成一棵告警统计策略树。

* **报表管理**

系统须内置资产、事件、监控、风险等报表报告；提供内置报表模板；

系统内置报表编辑器，可以自定义报表。

* ●**知识管理**

系统应能提供开放的知识管理功能，内置安全知识，同时也允许用户在系统使用过程中不断丰富和完善；系统预先建立的知识包括：案例库、漏洞库、事件分类库、字典库等；方便用户查询不同原始日志信息的错误ID号和详细描述信息。

内置交换机的事件编码知识库；内置Windows、Linux、Solaris、AIX操作系统的事件ID知识库；内置Oracle、SQL Server、MySQL、Informix、DB2数据库的事件编码知识库；能够查看系统内置的事件库中事件类型名称及其描述信息。

* **运行管理**

可以对自身运行的CPU、内存和磁盘空间的使用率设置告警阈值；

支持系统时间同步，能够指定时钟服务器，确保审计系统与用户网络环境的时间保持同步。

* ●**权限管理**

实现基于角色的权限管理，所有的用户的权限都通过角色来赋予；

系统内置三类管理员：系统管理员、安全保密管理员和审计管理员，且三权分立。

## 大屏展示系统

### 系统设计说明

此系统包括涉密网、办公专网、互联网专线接入、电子显示屏（拼接大屏）系统及指挥扩声系统等。

1. **信息点接入**

在B401每个工位各布置1个语音点2个信息点，互备方式分别接入中国机构编制网、事业单位登记管理系统、党政机关网站资格审核系统及互联网网络运维监控信息。（共2个工位）

在B408每个工位各布置1个语音点3个信息点，分别接入涉密网A、涉密网B、办公专网、视频监控和环境监控。（共4个工位）

在B3会议室监控大屏处接入2个信息点，留备后用。

1. **物理环境**

包括B401、B408以及B3会议室，其中，B401室长7.2米、宽4米、高3.3米，B408室长5.2米、宽4米，高3.3米，B3会议室长12米、宽8.5米、高2.8米。

1. **房间改造设备迁移**

B401、B408作为系统监控中心，需要达到房间整体美观整洁。把房间内的安防监控系统和动环系统主机部署到机房，重新购置指挥控制台2套，指挥控制台尺寸：600mm\*3500mm，全钢结构。

### 可视化展示效果

依托监控系统，汇聚各类资源、拓扑、业务、安全、机房监控信息，结合三维建模等技术，实现对各类信息的集中展现。

提供一张图模式直观展现。实现在3D环境下以统计图表、分析图表等形式，描述整体IT环境实况，变化信息以及动态效果加强。

系统支持建筑可视化、分楼层可视化、机房可视化、机柜可视化、设备可视化、业务可视化、容量管理可视化、告警信息可视化等相关功能的3D呈现。

系统支持自定义展示面板设计，可以灵活定义展示面板上的统计图表和分析图表卡片，支持卡片大小、位置的自由拖动调整，并支持自动面板的切屏、页面自动刷新等功能。

系统适应大屏幕呈现，支持矢量图界面元素，适应多种分辨率，支持多块拼接的大屏显示，支持大屏轮播展示。支持数据驱动的2D/3D场景及数据的自动更新，提供多种数据对接方式。

### 展示系统

●401采用4块55寸高亮超窄边拼接液晶屏，408采用6块55寸高亮超窄边拼接液晶屏；分辨率不低于1920\*1080，物理拼缝≤1.7mm，亮度≥800cd/㎡，对比度≥5000:1，图像显示清晰度不低于950TVL，亮度鉴别等级不低于11级，点距≤0.53mm，选用液晶显示单元应具有多种接口，输入接口：VGA×1，DVI×1，BNC×1，YPbPr×1，HDMI×1，USB×1支持多种控制方式。  
LCD显示单元支持U盘点播，内置MPEG、JPEG和RealMedia解码器，支持点播U盘、移动硬盘中的视频、图片、音频或文本资源。

视频：支持TS、3g2、avi、mkv、mov、mp4、mpg、tp等文件。

音频：支持mp3、wma、m4a、wav、aac等文件。

图片：支持jpg、bmp、png等文件。文本：支持txt文件。

●LCD采用双CPU+多个协处理器核的构架；双CPU负责通讯、色彩调整及模块控制等控制功能；3个DSP核+1个FPGA核负责图像数据的处理，分工明确保证系统稳定性和实时性。

●LCD显示单元通过调整γ曲线，使得实际γ曲线更为平滑且更为准确，从而提升显示设备的显示效果。

### 拼接处理器

投标产品对录像文件解码延时≤110ms。

●投标产品支持4K输出板最大分辨率为4096×2160，其它板卡支持至少8种分辨率输出1920×1080、1680×1050、1600×1200、1400×1050、1280×1024、1280×960、1280×720、1024×768。

投标产品支持手动视频切换功能，支持将选定的视频输入切换到选定的视频输出，支持视音频同步切换、异步切换，画面切换时不出现黑屏。

●投标产品具有同一输入通道的视频图像在不同输出端口显示的失步误差小于1ms。

●投标产品可通过无线终端将视音频、图片、PPT等传送到屏幕上显示。

实现如下功能：

1. 单屏显示：组合大屏的每个单元单独显示一路视频画面，每个单元的视频信号可以任意切换
2. 整屏显示：整个大屏显示一路完整的视频图像，显示的图像可以是复合视频（PAL或NTSC）、VGA、S-Video、Ypbpr/YCbCr、DVI。
3. 任意分割显示：以一个屏为单元可任意1、4、9、16路画面分割显示。
4. 图像叠加：可以将任意一个或者多个信号叠加到其他信号之上显示。
5. 任意分割显示：可以对任意重要目标细节画面进行切割放大显示。
6. 任意组合显示:可以任意几个大屏组合显示一路画面。
7. 图像半透明混合处理:可将任意一个信号叠加到其他信号（地图）之上，图像透明度可调，即可以看到实图像又不覆盖其他信号。
8. 图像漫游：将任意一个信号在整个大屏上进行随意移动。
9. 图像拉伸：可将一个信号在整个屏幕墙上随意缩放。
10. ●logo/OSD显示：在不占用视频输入的情况下，可通过网络在任意单元上以任意大小显示任意多幅静止图像，也可以是LOGO信息或地图。可在任意单元任意位置显示适量字库文本信息，文字透明度可调。
11. 网络抓屏：可通过网络将远端电脑的操作界面投射到电视墙上。

### 展示控制系统

展示控制系统能运行在国产cpu主机上，支持龙芯、飞腾、兆芯。

### 环境清理

对B401 、B408原有设备进行移除和规整后，对两个房间进行简单装修，房间墙面无明显污渍和工程痕迹，达到房间整体美观整洁。

## 服务要求

### 产品服务

本项目所采购的产品均要求原厂家三年免费维修。产品在出现质量问题时，厂家需要在24小时内解决问题。

### 其他服务

投标人承诺三年免费技术支持和服务。在系统调试完成后，须做好产品使用培训，及其他文档移交工作，在三年内产品出现故障时，需要在4小时内到场，24小时内解决问题。