# 概述

此次软件项目设计以公司的战略总目标为依托，针对实际业务需求，结合企业愿景，以建成安全办公信息监控平台为基础，最终使软件项目得以上线推广，以解决传统的非智能监控管理存在的各种弊端，为行业内受众提供便捷的监控平台。

本次平台设计着重考虑线上运行软件的大用户量、高并发、大数据、安全性、异构网络等一些核心关键问题，以数据监控为基础，结合分布式计算、数据库热备份、负载均衡等先进技术，从而保证应用服务器的高可用性、高安全性及高可扩展性。平台总体框架设计如下。

# 一、主要功能模块

XX安全办公信息监控平台主要包括7个模块。其中，文件监控管理、网络接口监控、加/解密管理、安全传输管理以及违规操作远程管理是主要的业务模块。



图1 主要功能模块

# 二、详细功能模块

## 2.1文件监控管理模块

主要包括文件获取途径监控、文件分级、文件并发操作监控、文件敏感操作监控以及操作日志（用户，访问时间）。



图2 文件监控管理模块

## 2.2网络接口监控模块

主要包括TCP常用端口监控、UDP常用端口监控、安全传输端口监控、端口异常活动监控、端口活动统计分析。实现客户端计算机物理地址和硬盘地址自动收集和绑定，服务器管理端手动控制或自动开关上网功能，对客户端网络发出数据进行镜像分析监控。对特殊文件外发可以自动阻断。



图3 网络接口监控模块

## 2.3加/解密管理模块

主要包括客户端加/解密、服务器端加/解密、密钥生成及协商、密钥管理以及加/解密日志。实现服务器端下发客户端文件操作强制加密、选择加密或不加密的管理策略。



图4 加/解密管理模块

## 2.4安全传输管理模块

主要包括安全信道建立、安全信道撤销、会话密钥生成、会话密钥管理以及信道管理日志。实现对上传文件实现先加密后建立加密信道进行传输。



图5 安全传输管理模块

## 2.5违规操作远程管理模块

主要包括违规设备记录、违规设备端口屏蔽、违规情节分级预警、文件远程操作以及违规日志记录等功能。



图6 违规操作远程管理

## 2.6系统管理模块

主要包括权限管理、系统维护以及系统日志。实现服务器端对客户端的策略下发和模块升级功能。可以通过组织架构进行权限划分，每台计算机基本信息、关键字字典库和报警信息、统计信息可以进行权限划分。



图7 系统管理模块

## 2.7 基础信息管理模块

主要包括客户端设备管理、用户信息管理、涉密关键字字典管理、软件更新日志以及设备更新日志。增加报警信息的统计、设备相关信息统计。



图8 基础信息管理模块

# 三、项目进度计划

# 四、经费划拨计划

项目总经费10万元，分三个阶段划拨：

1. 项目启动经费3万元；
2. 中期验收（2016年11月4日前后），验收客户端、服务器端通信、安全信道传输、文件加解密等模块，通过后支付经费4万元；
3. 本期系统功能模块验收并上线试运行（2016年底），支付尾款3万元。