独创性（或创新性）声明

本人声明所呈交的论文是本人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢中所罗列的内容以外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得北京邮电大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

申请学位论文与资料若有不实之处，本人承担一切相关责任。

本人签名：田光　　日期：2009年6月10日

关于论文使用授权的说明

学位论文作者完全了解北京邮电大学有关保留和使用学位论文的规定，即：研究生在校攻读学位期间论文工作的知识产权单位属北京邮电大学。学校有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许学位论文被查阅和借阅；学校可以公布学位论文的全部或部分内容，可以允许采用影印、缩印或其它复制手段保存、汇编学位论文。（保密的学位论文在解密后遵守此规定）

保密论文注释：本学位论文属于保密在__年解密后适用本授权书。非保密论文注释：本学位论文不属于保密范围，适用本授权书。

本人签名：田光　　日期：2009年6月10日

导师签名：　　日期：2009年6月10日

电子政务集中运维管理系统设计与实现

摘 要

随着国务院启动了以发展中国电子货币为目的、以电子货币应用为重点的各类卡应用系统工程——金卡工程，拉开了"三金工程"的建设序幕，在神州大地展开了一场声势浩大的，围绕建设高效服务型政府为目的的电子政务建设。此同时，各级政府网站的信息内容日趋丰富，服务功能逐步增强，逐渐成为政府部门发布政务信息、提供办事服务、实现政民互动的主要渠道。目前，我国电子政务已经完成了中央各部委到省、地、县各级政府及其职能部门的网站体系架构初步建立。

在看到成绩的同时，我们应该看到，随着建设和应用的深入，各行业网络规模不断膨胀，网络应用越来越多，网络应用系统与工作流程的关系日趋紧密，各行业电子政务系统具有一个普遍的共性：跨地域的、异构的网络管理环境、设备、系统繁多。电子政务的运维的压力和挑战逐渐凸现出来，已经成为影响电子政务系统应用效果的重要因素和深入发展的主要瓶颈。

利用运维服务的支撑系统来促进运维工作地完善和提高是近几年各级电子政务运维部门都在共同探讨的方向。它涉及对分散各 IT 基础资源进行的统一监控展现、运维流程的关联、单点登录、授权管理等多方面的内容，建立集中运维管理系统的建设就是解决这些问题方案。

本文以我所在单位石景山区信息网络中心所组织的石景山区电子政务集中运维系统的建设为背景探讨了针对电子政务运维的运维服务支撑系统的设计和实现，我作为项目主管领导参与了整个建设工作的需求调研、设计以及实际部署和应用工作。本文提出了一种以 ITIL 为基础，结合电子政务实际运维特点，本着以流程为导向，对运维服务管理对象进行统一集中管理的设计方案。在技术实现上采用了目前比较先进的 Web2.0、Portal、单点登录等技术增强了系统的稳定性、安全性和易用性。解决了电子政务运维过程中运维活动角色不够明确、运维管理分散、流程不规范等问题。

关键字： 电子政务，集中运维，信息技术基础架构库

THE DESIGN AND REALIZATION OF OPERATION AND MAINTENANCE IN E-GOVERNMENT

ABSTRACT

With the purpose of constructing a highly efficient and service-oriented government in China, e-government construction was started with the 'Three Golden Project' , which has grown rapidly since the launch of the State Council's 'Golden Card Project'. Taking the application of electronic currency as its key, the Golden Card Project aims to develop China's electronic currency.

At the same time, the information on government websites at all levels is being enriched day by day and functionality is being gradually improved. As a chief information channel of the government, the websites play a very important role in releasing information, providing management services and communicating and interacting with the public. At present, the preliminary establishment of e-government website structure has been completed from central ministries to the provincial, prefectural and county governments as well as various government departments.

However, we should be aware that with the penetration of the networks,? expanded scales and closer connection with the work flow of various government division, the e-government system shares some common characteristics: cross region, heterogeneous network management environment and highly diversified equipment and systems.

The pressure and challenge of operating e-government has been manifested and become the major factor to affect its application and the main bottleneck for further development.

In recent years, e-governments at all levels have been exploring on how to improve the operation and maintenance work of their supporting systems. It involves the monitoring of the decentralization of the basic IT resources, the operation and maintenance work, single sign-ons, authorization management and etc. The establishment of a centralized operation and maintenance system can help solve many of these problems.

Based on the construction of the centralized operation and maintenance system of the Shijingshan District's e-government, which was undertaken by the Information Network Centre of the district, this article mainly discusses the design and implementation of e-government supporting system.

As the project director, I have participated in the requirement analysis of the construction, design and deploy as well as the implementation.

This paper proposes a centralized and flow-oriented solution to the operation and maintenance management of the target design, based on the ITIL, taking into consideration of the actual operation.

Technologically, we adopt the advanced Web2.0, Portal and single sign-on technologies to enhance system stability, security and user-friendliness so as to solve problems like undefined role in operation and maintenance, decentralized management and lack of standardization in work flow.

KEY WORDS: E-Government, operation and maintenance, ITIL

目 录

第一章 绪论 7

1.1 选题背景 7

1.2 本文主要工作 8

1.3 本论文的组织结构 9

第二章 运维管理及应用技术探讨研究与分析 10

2.1 电子政务系统运维 10

2.1.1 电子政务运维的背景及现状 10

2.1.2 电子政务运维存在问题及发展趋势 11

2.1.3 电子政务运维特点 12

2.2 IT 服务管理的最佳实践-ITIL 13

2.2.1 ITIL 是什么 13

2.2.2 ITIL 的实践及其发展 14

2.2.3 ITIL 的基本特点 15

2.2.4 ITIL 的核心模块 15

2.3 关键性技术研究与分析 23

2.3.1 Web2.0 技术 23

2.3.2 Portal 技术 23

2.3.3 单点登录 24

第三章 石景山区电子政务运维管理系统方案设计与分析 26

3.1 运维管理系统总体设计 26

3.1.1 系统设计原则 26

3.1.2 系统总体建设目标 27

3.1.3 系统设计思想 28

3.2 运维管理系统体系结构设计 31

3.2.1 数据存储层 33

3.2.2 业务逻辑层 40

3.2.3 业务操作层 41

3.3 运维管理系统功能模块设计 42

3.3.1 资产管理 42

3.3.2 监控管理 43

3.3.3 流程管理 45

3.4 系统安全设计 48

3.4.1 物理层.....49
3.4.2 网络层.....49
3.4.3 系统层.....50
3.4.4 应用层.....50

第四章 运维管理系统部署方案.....**52**

4.1 系统部署方案.....52
4.1.1 软件配置方案.....52
4.1.2 硬件配置建议方案.....53
4.2 角色设置和权限分配.....53
4.2.1 基于角色的权限管理模型.....53
4.2.2 石景山区电子政务系统集中运维平台的角色设置以及权限分配.....53
4.3 系统功能展示.....54
4.3.1 统一监控展现.....55
4.3.2 事件工单处理.....56

第五章 成果总结.....**57**

5.1 建设成果.....57
5.1.1 功能的满足.....58
5.1.2 促进运维机制的形成.....64
5.1.3 掌握基础数据.....64
5.1.4 提高运维服务.....64
5.2 存在的问题.....65
5.2.1 流程的适用性还需要进一步加强.....65
5.2.2 IT 服务财务管理存在着较大的困难.....66
5.2.3 对于运维外包服务商的管理.....67
5.3 个人收获.....67

第六章 结束语.....**68**

参考文献.....**69**

附录：图表索引.....**70**

致 谢.....**71**

攻读学位期间发表的学术论文目录.....**72**

第一章 绪论

1.1 选题背景

电子政务建设是我国信息化建设的重要内容，2002 年，政府决定“政府先行，加快全国电子政务建设”，并起草了指导电子政务建设的总体方案，电子政务进入大规模建设阶段。随着对电子政务应用的推广和深入，对电子政务信息系统的可用性、安全性等的要求也逐步提高。因此，近两年电子政务的 IT 服务逐渐被重视，对其中的一些流程的管理也被提上日程。其网络规模庞大，复杂。劳动和社会保障信息网络系统既要覆盖各级经办机构，又要联接各级政府，同时还要将网络向下延伸到街道、社区。

近些年来，为使运行维护工作（简称运维）能够适应形势发展的要求，跟上电子政务的建设步伐，各级政府信息化主管部门开始在运维工作上推行了“机房安全制度”、“机房管理制度”、“机房值班职责”等一系列的运行维护管理制度，取得了一定成效。但运维管理工作多是局部的、单项的，难以牵动全局、形成整体合力，各种原因导致的系统、网络故障而造成服务延误的情况时有发生。信息中心的同志常常处于“救火”的状态，处于被动的服务状态，哪里有问题就扑向哪里，缺乏科学有效的主动规划与服务流程，服务质量和业绩缺乏量化的标准，缺少相应的流程和知识积累，未能有效地从根本上解决运维工作中存在的基础台帐管理不规范、故障发现和解决滞后、设备资产底数不清、“三制”工作不实等突出问题。

2008 年，按照《北京市信息化促进条例》的要求以及电子政务发展新阶段的需要，为保证各类政务信息系统稳定运行，全面提升电子政务绩效，北京市信息办组织相关企业、协会、委办局、区县和业内专家，在研究 ITIL、ISO20000、ISO27001、GB/T14885 等国际国内相关标准的基础上，结合北京市电子政务运维工作的实际情况，编制了《北京市电子政务运维服务支撑系统规范（1.0 版）》，并于 2009 年下发北京市有关单位参照。

石景山区电子政务系统是全市电子政务系统的重要组成部分之一，从 2001 年开始大规模建设电子政务基础网络，经过 8 年的努力，石景山区的电子政务建设也已具有一定的规模，网络覆盖全区 64 个党政机关、10 多家医疗机构、127 个社区、各类事业单位及驻区国有企业，全部实现光纤接入，完全实现了区街居

三级宽带网络连通。区域平台运行的各种应用系统多达40余个，设备总数超过300台。如门户网站、办公自动化、城市管理系统、电子邮件系统等，有力保障石景山区政府电子政务全面实现系统化的战略目标，是保障石景山区政务网络稳定高效运行的核心力量。石景山区信息网络中心是负责石景山区电子政务运维的主要单位，承担着区域电子政务网络平台及重要信息系统的运维工作，在实际的工作中也面临着以下一些问题和困难：

缺乏统一的集中监控与管理平台

信息系统日常运行管理条块分割，网络、应用、安全、基础环境等基本上是各管一摊，缺乏一个统一的、主动的集中运行监控平台，既浪费了人力资源，也难以做到快速发现故障。

缺乏对运行维护工作的规范性管理

运行管理手段比较落后，只有一些基本的手工管理流程，而且只能以文件的形式对流程进行规范，这些流程没有相应的技术设施予以保证。

缺乏量化运行质量的工具，无法对下级单位进行有效监管

缺乏一套能与实际工作相结合的运行质量考核工具，无法对运维人员的工作及下级单位的考核做到实时和量化。

综上所述，如何设计并实现一个电子政务集中域内管理系统，不仅架设简单、容易使用扩展，而且可以在统一系统中集中展现各监控信息，实现对报警事件的及时发现集中处理。同时，通过对于运维流程的电子自动化，实现对运维工作的全程监督和管理，已达到提高运维工作的效率和质量，从而构建良好健康的电子政务系统运行基础平台，促进电子政务的应用，有力支撑政府政务的开展，是个值得研究的课题。

1.2 本文主要工作

虽然在电子政务运维工作中，部分监控及防御设备也设计了各自管理运维平台，在一定程度上解决了部分运维工作的电子化，但是大部分系统之间存在着不兼容的问题，没有实现集中展现、统一管理。同时，在运维流程方面也只是单个的文档方式，流程并没有电子化，运维的质量和效率不能满足新形势下电子政务应用的需求。电子政务的不断深化应用使得对信息系统稳定运行的需求越来越高，国内也开始引入ITIL等国际标准，并结合我国电子政务运维工作的实际情况来探讨运维服务支撑体系的标准。但是目前来说，在国内的电子政务运维工作中对于这些标准的实践工作还刚起步。

本文的主要工作，即针对目前电子政务运维工作中面临的问题及弥补目前使用的各种运维系统的不足，朝着集中化、自动化的方向来架构系统，提供便利的

用户界面以及日后的功能扩展，参照 ITIL 国际标准的相关内容及北京市电子政务运维服务支撑系统规范，并结合石景山区电子政务运维的实际情况来建构一套方便实用基于 B/S 的电子政务集中运维管理平台，开展实践活动。

通过集中运维平台可以将主机系统、网络系统、数据库系统、应用系统、安全系统及其他系统运行状况统一展现，并将所有报警统一显示，避免需登录多个运维系统管理界面查询报警信息的现状。在运维处理流程方面，以现有的运维流程为基础，结合 ITIL 标准流程，从事件管理、问题管理、变更管理、配置管理等方面通过系统实现流程自动化、信息电子化、文档管理规范化，进一步提高运维效率和管理水平。

1.3 本论文的组织结构

本人结合所在单位电子政务系统集中运维管理平台建设项目，对基于 ITIL 的集中运维管理平台建设进行了研究。本文的组织结构如下：

第二章讨论了对电子政务运维工作的现状和存在的问题进行简要的分析并对系统应用的关键技术进行了探讨。

第三章对系统设计的思想和体系结构进行了详细的阐述，并对功能模块的设计进行了介绍。

第四章结合石景山区电子政务运维的实际，对系统的实现和部署情况进行了描述。

第五章对研究的成果进行了总结，并对于过程中存在的困难和还存在的问题进行了说明，同时总结了本人在此次课题研究过程中的收获。

第六章对论文的工作进行了总结并展望电子政务系统的集中运维管理工作的发展方向。

第二章　运维管理及应用技术探讨研究与分析

2.1　电子政务系统运维

电子政务系统运维除了具有一般IT系统运维的特点以外，由于其服务的对象和建设的历史等原因形成了一些特有的现状和问题，例如环境复杂、部分系统受公众关注大等。同时，由于政府部门自身组织机构设置情况的不同在运维模式上又分为自运维模式或者混合运维模式等。因此，对于它的管理应该有其一定的特殊性。

2.1.1　电子政务运维的背景及现状

随着电子政务的提出和不断推广建设，电子政务网络系统建设也发生取得了瞩目的成绩，信息化建设已经处在一个比较高的水平：

网络应用系统与外界交互信息多，其外联系统多，与众多的服务渠道、外部系统关联。如为各级政府提供经济调控、城市管理以及市场监管等的宏观决策信息，为公众、企业以及政府部门之间提供政务公开信息以及办事渠道，与民政、社保、流动人口管理等办事机构交换大量人口信息，以及城市管理部门每日交换的庞大城市管理信息等等具有特别的重要性、特殊性和安全性；

“三分建设、七分管理、十二分数据”，其运行维护质量与工作水平将直接关系到电子政务信息资源库以及各个应用系统能否发挥效益和电子政务网络平台能否安全、高效运行；直接关系到政府是否能实现职能转变，促进经济发展；直接关系到民心的稳定、社会的安定、国家的兴衰。

我国电子政务建设大体经历了三个重要的发展阶段，从80年代起步，到目前为止，投资建设的大量信息系统已经进入应用维护阶段，电子政务发展正处在由建设向运维转型的时期。

目前，我国部分关键电子政务系统已经实行集中运维。例如，国家重点“金字”工程普遍实行了全国和省级的数据和应用集中，运维工作逐渐从分布式的技术支持向集中式、专业化的技术支持。

从覆盖范围来说，运维工作覆盖了终端设备、网络、系统及业务应用。据ITGov的调研，主机、数据库、存储备份、网络设备等多数都是由原生产商负责，且多以国外厂商为主。应用系统软件、网络运维多数采用“谁建设，谁运维”的方式。

应用服务与安全服务所占比例较小。

电子政务建设一方面取得了令人瞩目的成就和有益经验，另一方面还存在着许多亟待解决的问题。在电子政务工程建设中，普遍偏重硬件资源的投入，软件和维护投入在整体投入中的比例还是比较低的。一些网络资源的当前利用率不足10%，个别项目的存储资源无法满足业务增长需求。电子政务应用方面，主要侧重于内部事务处理和自我服务，支撑政府决策和面向公众服务的信息化能力亟待提高，系统保护和IT部门的管理水平还有待加强。

电子政务管理中IT治理和服务管理系统的建设情况还比较低。应围绕项目的需求符合度、公众满意度和投入产出效益等方面开展电子政务的绩效评价工作，从根本上改变电子政务工程建设后期矫正和约束机制严重不足的状况。

鉴于上面的不足，国家发展改革委与财政部将建立电子政务项目和部门信息化建设项目审批信息通报机制，有效避免项目建设资金的重复投入。财政部、国家发展改革委将会同有关部门抓紧制定电子政务项目运行维护资金的测算依据、定额标准和使用程序，以确保运行维护资金有效和规范使用，ITIL的广泛推广和使用将有效的提高维护工作的方方面面。

2.1.2　电子政务运维存在问题及发展趋势

随着电子政务运维工作重要性的日益凸显，但是大量政府单位在运行维护方面依旧主要存在以下问题：

- 对运维工作的定位不准

目前，我国电子政务工作依旧存在“重建设、轻维护、重技术、轻管理”等现象，很多领导对运维工作重视程度依旧不够。同时运维的概念模糊，依旧存在建设与运维的边界划分不清晰，运维与升级改造的关系不明确等。

- 运维管理“经验主义”依旧盛行

很多政府单位在运维工作中，普遍采用经验法则，日常工作中常处于“救活”状态，非常被动的处理各种故障；对运维外包商的管理缺乏有效的手段。针对运维中面临的日益凸显的风险，各政府单位急需建立运维管理体系，使运维工作更加科学化、规范化和专业化。

- 缺乏有效的运维工具

由于对运维工作的错误认识，在电子政务的运维过程中，缺乏有效的运维工具也是目前存在的一个重要问题。大多数运维单位都没有运维工具，有一部分单位利用了分散的工具或者开源的简单工具，但是在功能上和性能上都有很大的局限性。

随着电子政务运维工作的逐步成熟，中国电子政务运维管理必然从粗放管理

走向科学管理，从“重建设、轻维护、重技术、轻管理”走向“建设与维护并重，技术与管理并重”。

➢ 对运维工作的认识日趋成熟

在电子政务大规模建设阶段，大家对于系统的运维工作都采取了忽略的态度。相比于建设工作来说，运维工作很难体现出成绩，难以得到领导的重视，再加上各系统的应用程度都没有达到一定的广度和深度，运维的作用也没有充分体现出来。另外，很对人认为配置一些管理软件就可以做好运维工作了，但是经过几年的工作实践，大家逐步认识到电子政务运维工作不只是技术问题，更是管理问题。认识上的提高，对于运维工作水平的提高起到了很好的促进作用。

➢ 逐步建立完善的运维体系

电子政务运维工作的最初并没有对运维体系完整的认识，只是简单地从监控系统、工作流系统等系统建设开始，在组织模式和制度规范上开展的工作较少。随着工作的开展和深入，逐步认识到运维工作的开展需要在集组织、技术、管理等多方面组成的体系下进行。《2006-2020 年信息化发展战略》中就明确提出了未来电子政务行动计划要建立运行、维护管理制度，从国家层面规划了电子政务运维管理方向。ITGov（中国 IT 治理研究中心）在基于对大量电子政务实践的基础上提出了涵盖管理目标、组织管理模式、制度管理体系、技术支撑体系等内容的 IT 运维管理体系四层架构模型。

➢ 运维工作日趋规范

运维工作水平提高，必须有科学的理论、方法来进行指导，并逐步成为行业的标准。国际上已经出台了 ITIL、ISO27001 等相关的标准，并在全球范围内进行推广，在国外也有了较好的实践。北京市信息办于 2009 年初也下发了《北京市电子政务运维服务支撑系统规范（1.0 版）》，对电子政务运维服务支撑系统应用需求以及支撑系统技术要求进行规范，使得电子政务运维工作能够科学的快速发展。

2.1.3 电子政务运维特点

总体来说，电子政务集中运维主要有以下几个特点：

网络规模庞大，复杂。电子政务网络系统既要覆盖政府各类业务部门，又要联接各级政府，同时还要将网络向下延伸到街道、社区。

环境复杂。电子政务网络系统应用和网络层面上必须覆盖以上所有的业务机构和相关部门，形成了多系统、多数据库、多应用平台、多厂商网络及系统设备，多业务应用等复杂的管理环境。

运维人员缺乏。电子政务系统大多涉及政府政务，很长一段时间运维工作都是由政府员工来承担。由于政府人事制度的特殊性，运维人员在数量和技术水平

上都有很大的不足，同时很多政府部门缺少专门的信息化部门，这就给运维工作带来了很大的困难，需要有一定的创新。

2.2 IT 服务管理的最佳实践-ITIL

随着中国政府信息化建设的深入推进，信息系统的规模不断扩大，日常工作对 IT 系统的依赖性越来越大，同时 IT 系统日趋复杂、系统维护要求越来越高。ITIL 作为运维 IT 管理的新理论、方法和工具，正在发挥着越来越重要的作用。ITIL 作为管理 IT 的一种方法和理念，从初期有人提出它的概念到成为行业标准在世界范围内得以广泛应用，以 ITIL 作为规范的 IT 服务管理也成为一个受到重视的领域。

2.2.1 ITIL 是什么

ITIL，全称 Information Technology Infrastructure Library，通常被译为"信息技术基础架构库"。它是英国中央计算机和电信局 CCTA（现在已并入英国商务部）于 80 年代中期开始开发的一套针对 IT 行业的服务管理标准库。在它的 2.0 版中，ITIL 主要包括六个模块，即业务管理、服务管理、IT 基础架构管理、IT 服务管理规划与实施、应用管理和安全管理，如图 2-1。其中服务管理是其最核心的模块，该模块包括"服务提供"和"服务支持"两个流程组。

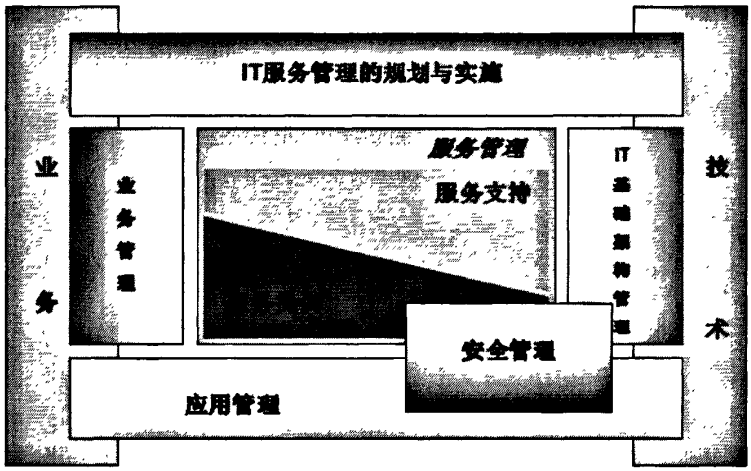

图 2-1 ITIL 整体架构

ITIL 产生的背景是，当时英国政府为了提高政府部门 IT 服务的质量，启动一个项目来邀请国内外知名 IT 厂商和专家共同开发一套规范化的、可进行财务计量的 IT 资源使用方法。这种方法应该是独立于厂商的并且可适用于不同规模、不同技术和业务需求的组织。这个项目的最终成果就是现在被广泛认可的 ITIL。

ITIL 虽然最初是为英国政府部门开发的，但它很快在英国企业中得到广泛的

应用。在20世纪90年代初期，ITIL被介绍到欧洲的许多其它国家并在这些国家得到应用。到90年代中期ITIL已经成为欧洲IT管理领域事实上的标准。90年代后期ITIL又被引入美国、南非和澳大利亚等国。90年代末，ITIL也被有关公司引入中国。

2.2.2 ITIL的实践及其发展

自20世纪80年代中期英国商务部提出信息技术基础架构库（ITIL）以来，ITIL作为IT服务管理事实上的国际标准已经得到了全球几乎所有IT巨头的全力支持。IBM、惠普、微软、CA、BMC、ASG等著名跨国公司作为ITIL的积极倡导者，基于ITIL分别推出了实施IT服务管理的软件和实施方案。ITIL在欧洲、北美、澳洲已得到广泛应用，全球1万多家在各行业处于领先地位的著名企业给我们带来了众多实施ITIL的成功案例，通过实施ITIL大大改进了企业IT服务的质量，促进了IT与业务的融合。

荷兰政府首先在该国所有政府部门采用该标准，并取得了巨大的效益；之后英国政府和澳大利亚国防部也相继宣布采纳该标准；宝洁公司（Procter & Gamble）于1997年起采用ITIL模式后，4年内共节约预算资金达5亿美元，使运营成本削减8%，技术人员减少20%；

近年来，ITIL在全球的发展更是异常迅猛。比如说在美国，2001年第一次举办itSMF年会的时候只有200人参加，到第二年就有800人参加，2003年的第三次年会甚至有超过1600人参加！

ITIL在国外特别是欧美地区可以说是呈现出一种“热火朝天”的景象，那么其在国内的发展状况又是如何的呢？

ITIL最早是1999年被引入中国的。在被引入的前3年，由于了解它的单位不多，这方面的成功案例也相当有限，所以在国内处于一种不愠不火的状态。但是从2002年开始，ITIL在国内开始受到越来越多的关注。特别是在2003年，ITIL在国内的发展历程中出现了多个第一：翰纬IT管理研究咨询中心出版了第一本中文ITIL专著、《中国计算机用户》周刊创办了中国第一个IT服务管理专栏、第一个面向ITIL的门户网站“ITSM资讯网”，也在翰纬IT管理研究咨询中心和ITSM PORTAL International的合作下正式创办。20世纪90年代，ITIL由ITIL V1逐渐扩充成为一个由31卷图书构成的庞大的方法论知识体系。

为了使ITIL得到更好地推广，也为了消除各卷书之间的重复和冲突，英国商务部（OGC）将原有的31卷图书进行了整合，形成了《服务支持》（Service Support）和《服务交付》（Service Delivery）两本指南。从2000年开始，OGC又组织有关力量对这两本指南进行全面修订，同时对ITIL进行了较大的扩充和完善，最终逐

渐形成了 ITIL V2 的完整知识体系，2000 年 11 月，BSI（英国标准协会）基于 ITIL 发布了第一版 BS15000 服务管理标准，而后又于 2002 年 11 月对其进行了更新。项目管理者联盟文章，深入探讨。2005 年 5 月 17 日，国际标准组织（ISO）以”快速通道”的方式通过了将 BS15000 接纳为国际标准的决议。同年 12 月 15 日，国际上第一个 IT 服务管理标准 ISO/IEC20000 正式发布， 该标准的颁布意味着 IT 服务管理（ITSM）在国际范围内的标准化进程又向前迈进了一大步。 2007 年 5 月 30 日，OGC 在全球发布了 ITIL 最新版本---ITIL V3。

2.2.3 ITIL 的基本特点

- 公共框架

ITIL 由世界范围内的有关专家共同开发，它也可由世界上任何组织免费使用以及利用 ITIL 开展有关业务。

- 最佳实践框架

ITIL 是根据实践而不是基于理论开发的：OGC 收集和分析各种组织解决服务管理问题方面的信息，找出那些对本部门和在英国政府部门中的客户有益的做法，最后形成了 ITIL。

- 事实上的国际标准

虽然 ITIL 当初只是为英国政府开发的，但是在 20 世纪 90 年代初期，它很快就在欧洲其它国家和地区流行起来。目前，ITIL 已经成为世界 IT 服务管理领域事实上的标准。

- 质量管理方法和标准

ITIL 内含着质量管理的思想。组织在运用 ITIL 提供的流程和最佳实践进行内部的 IT 服务管理时，不仅可以提供用户满意的服务从而改善了客户体验，还可以确保这个过程符合成本效益原则。

2.2.4 ITIL 的核心模块

ITIL 的核心模块是“服务管理”，这个模块一共包括了 10 个流程和一项职能，这些流程和职能又被归结为两大流程组，即“服务提供”流程组和“服务支持”流程组。其中服务支持流程组归纳了与 IT 管理相关的一项管理职能及 5 个运营级流程，即事件管理、问题管理、配置管理、变更管理和发布管理，图 2-2 显示了各流程之间的关系；服务提供流程组归纳了与 IT 管理相关的 5 个战术级流程，即服务级别管理、IT 服务财务管理、能力管理、IT 服务持续性管理和可用性管理。下面对这些流程进行简要的介绍。

服务台

服务台：服务台是IT部门和IT服务用户之间的单一联系点。它通过提供一个集中和专职的服务联系点促进了组织业务流程与服务管理基础架构集成。服务台的主要目标是协调客户（用户）和IT部门之间的联系，为IT服务运作提供支持，从而提高客户的满意度。

服务台的定义：

报告事件和请求提供用户支持的中心，它主要关注运作层次的用户支持。

服务台的目标：

在用户、IT服务和第三方间的中心联络点

在服务级别和业务优先级规定的范围内减少对业务的影响

使服务更易恢复正常

生成供交流和分析的报告

为组织提供价值

服务台的职责：

服务呼叫的接收、记录、跟踪和优先级排序

所有已注册呼叫的监控和状态跟踪

呼叫服务的升级处理

呼叫及服务台质量报告

一线支持

将请求状态和进展及时通知给客户

协调第二线和第三方支持小组

获得用户认可后结束突发事件

客户满意度的衡量：

电话应答是否迅速

在线解决率

是否按时解决

是否礼貌

是否得到相关建议

服务台的分类：

呼叫中心（Call Center）：处理并记录下大量的电话事务，然后交给其它部门处理；

帮助台(Help Desk)：管理、协调并尽快解决突发事件；

服务台(Service Desk)：允许将业务流程集成到服务管理基础架构里。　　不

仅能处理突发事件，还可提供与其它流程的接口。

主要活动：

负责对新事件进行记录、分派、提交。

通过查询知识库，尝试解决事件。

查询浏览自己提交事件的处理状态。

向知识库提交解决方案。

事件处理结束后关闭事件。

填写用户反馈意见。

服务台是工具而不是流程，可以根据实际情况将服务台放入事件管理流程。

事件管理流程

事件管理：事件管理负责记录、归类和安排专家处理事件并监督整个处理过程直至事件得到解决和终止。事件管理的目的是在尽可能最小地影响客户和用户业务的情况下使 IT 系统恢复到服务级别协议所定义的服务级别。

所谓事件，是指 IT 运行维护范围内的所有与 IT 基础架构和应用相关的故障报告。这个流程是为了使业务部门和最终用户尽快回到正常工作状态而设计的。

它是事件驱动的，所关心的是对事件的响应速度和和尽快恢复业务运作。

事件管理流程包含下述主要步骤：

➢ 事件提交和记录

该步骤是事件管理流程的起点。所有用户报告的事件请求必须由此步骤开始。此步骤的目的是在错误发生时快速准确地发现错误，以协助事件的诊断和解决并通知相关人员。在此步骤中将会收集创建事件记录所需的信息。该步骤的关键是信息的准确性和完整性。

事件的来源是：事件的请求者可以通过电话、传真、电子邮件、Web 系统，将事件的信息告诉服务台，由服务台将事件信息记录。服务台查看服务台中该事件是否已被记录下来，如果没有，则记录该事件。

➢ 事件分配

对于事件，需要确立该事件的严重程度和分类。若没有现成的解决方案或临时措施来恢复服务，该事件将分配给合适的支持人员对此进行分析和解决。

在本服务台系统中，事件的分类和在线支持由服务台完成。

当服务台接收到请求人请求的事件后，可以对事件进行分类，并通过查询知识库尝试解决事件。

如果服务台可以解决事件，流程进入“解决和恢复”阶段。

如果服务台无法解决事件，可以将事件故障分派给事件分析员。

服务台可以按照事件的类型，将事件分别分派给规划指导科、信息中心、通信网络科的事件分析员。

➢ 调查和诊断

若在线无法解决的问题，必须进行更加深入的诊断以找到恢复服务的方法，必要时将可能使用多名技术员以寻求解决措施。当接单的事件分析员不能处理时，可以将工单转派给部门内部其他人员。

事件的调查和诊断主要由事件分析员和事件经理完成。

当事件分析员接收到由服务台分配的事件时，

事件分析员可以调查诊断事件，并对事件进行解决，然后进入“事件关闭”阶段；

若未找到解决措施且需要向事件经理申请对事件请求重新分配；

如果事件分析员未找到解决措施并且认为该事件故障可能隐含着问题，事件分析员可以查询问题工单，如果存在和当前事件的症状相同的问题工单，可将该事件工单关联到问题工单。如果不存在，事件分析员可以据此创建问题工单，并将其自动分配给问题处理组。

➢ 事件关闭

当服务台向用户确认事件解决，填写用户反馈意见后，此时可以关闭该事件，并在必要时更新知识库。最后该事件得以关闭。

如果用户对此解决方案不满意，则服务台将当前事件关闭，并由服务台根据该事件的事件信息新建一张事件工单。

➢ 事件监控

在步骤页面可以通过工作日志来监控事件的处理情况。

服务台的事件在下列关键的控制点上得到监控：

事件产生的时间点：指事件故障发生的时间点。

事件到达的时间点：指事件工单的创建时间点。

事件分配的时间点：指事件工单分配给当前处理人员的时间点。

事件解决的时间点：指事件工单被解决的时间点。

事件花费的时间：指当前事件处理人员处理事件工单花费的时间。

事件花费的全部时间：指所有事件处理人员处理事件工单花费的时间。

服务水平协议配置

事件优先级的修改主要是制定故障需要的解决时间。

当同时处理若干事件时，必须设定优先级。优先级是根据错误对用户和正常业务带来的影响的严重程度来确定的。服务台通过与用户进行协商，并根据服务

级别协议(SLA)确定事件的优先级。

影响度—— 影响度指就所影响的用户或业务数量而言，事件偏离正常服务级别的程度。

紧急度—— 紧急度指解决故障时，对用户或业务来说可接受的耽搁时间。

优先级—— 主要基于紧急度和影响度来决定。

事件管理带来的收益

减小突发事件对业务的影响

最优化资源进行事件支持，合理分工

服务分轻重缓急，保障系统有效运行

加强管理层的有形监控和及时反馈

及时有效的沟通，提升用户满意度

建立知识库，进行知识积累

提供管理信息和决策支持依据

问题管理流程

问题管理：问题管理是指通过调查和分析 IT 基础架构的薄弱环节、查明事件产生的潜在原因，并制定解决事件的方案和防止事件再次发生的措施，将由于问题和事件对业务产生的负面影响减小到最低的服务管理流程。与事件管理强调事件恢复的速度不同，问题管理强调的是找出事件产生的根源，从而制定恰当的解决方案或防止其再次发生的预防措施。

问题管理的主要活动

接受升级事件：当事件满足升级条件时，问题管理流程接受该事件；

分析事件：定期分析事件，找出潜在问题；

生成问题记录：问题记录在 Service Desk 中生成并把所有相关事件与此记录关联起来；

分派：问题记录将根据问题内容分派给适当的技术小组；

根本原因分析：被分派的小组人员将调查问题以期找出其原因，制定解决方案或变通方法或提出预防性措施以消除产生原因或在重发时使其影响力最小化；

更新已知错误：这是流程中的关键一步，记录必须被更新以反映它是已知错误状态,并且把任何变通方法、避免或最小化负面影响的动作行为也记录下来；

提出变更请求：对问题的解决方案进行评估，通过变更请求（RFC）进行测试和实施。根据 RFC 对业务的影响和成本进行评估并决定继续进行与否。 并非所有问题需要解决，例如，如果一个新的应用系统将要实施，那么老应用系统里的一个错误可能不需要解决；

关闭：一旦找出问题根本原因,并实施了解决方案,并确认已解决了问题,问题记录可以关闭；

事后回顾：问题必须进行回顾以发现流程和服务得以改进的机会或总结预防性措施。包括改进事件监测、找出技能差距和文档资料改进等. 这对于回顾解决方案的成功与否也很关键。

问题管理流程和事件管理流程应相互独立，但具有紧密关系：

必须确定问题根源；

问题解决方案的执行必须符合业务需求；

事件管理和问题管理具有不同目的,必须分开独立管理；

问题管理流程需要和事件管理和知识数据库建立接口。

问题管理资源应分配给对业务或 IT 支持人员影响最大的问题或事件：

问题必须进行影响度和优先级分类；

问题必须被分配给最合适的资源；

对影响度最大的问题必须优先分配资源；

必须有问题升级管理流程。

配置管理流程

配置管理：配置管理是识别和确认系统的配置项，记录和报告配置项状态和变更请求，检验配置项的正确性和完整性等活动构成的过程，其目的是提供 IT 基础架构的逻辑模型,支持其它服务管理流程特别是变更管理和发布管理的运作。

配置管理流程的主要活动

配置管理策略的规划

配置项的识别和维护 ：输入和更新 CMDB 数据. 登入新的 CI 或已有 CI 的变更，指明 IT 环境中各 CI 之间的关系；

录入和控制 ：加强 CI 变更的相应授权，在 CI 的整个生命周期内跟踪 CI 的状态历史(如以前，当前，计划状态等)，确保只有被认可的和被标识的配置项才能接受和记录。配置项的状态报告应当定期地反映配置项的版本和变动历史；

审计和确认 ：定期审核全部或部分 CMDB 数据,确认和物理环境的一致性,从而确保配置信息的完整性；

回顾和改进 ：定期回顾流程和审核结果,找出改进机会,包括流程和 CMDB

变更管理流程

变更管理：变更管理是指为在最短的中断时间内完成基础架构或服务的任一方面的变更而对其进行控制的服务管理流程。变更管理的目标是确保在变更实施

过程中使用标准的方法和步骤，尽快地实施变更，以将由变更所导致的业务中断对业务的影响减小到最低。

变更管理流程的主要活动

批准 RFC　变更经理确定对该 RFC 有批准权的经理参加 CAB，必要时参与评估。评估后该经理根据判断决定是否批准 RFC；

检查变更计划 / 测试结果，并批准实施 变更经理确定合适人员主管该变更并参与 CAB， 称为变更主管。变更请求得到评估和批准后，变更主管安排相应资源进行变更的构建 / 开发，然后需要对将要实施到生产环境的变更进行测试，并制定实施计划，随后提交测试结果和计划给变更经理以获得实施。变更经理必需要确保测试结果和计划都有文档记录和得到签署，并确认变更对生产环境没有影响或影响可以得到控制。这一步骤为变更流程的关键质量检查点；

规划 RFC　RFC 一旦获得批准，它必须根据资源和其他情况进行规　划，确定实施日期，分配相应资源，并通知请求人；

协调变更实施 一切就绪后，可以实施变更；

更新变更状态 在整个变更过程中，变更的状态从登记，评估，回顾到最后关闭是不同的。变更经理负责更新预先定义好的变更状态；

回顾和关闭 实施变更后，变更经理负责从技术和流程角度去回顾变更，该回顾在预先定义好的时间段针对变更单独进行，除确保 RFC 得到了预期效果外，也寻找流程的改进机会，如资源计划和实际使用的一致性。确定是否满足了变更目的，有没有副面影响，否则需制定后续行动计划。随后，变更经理负责利用预先定义好的结束状态关闭 RFC；

总结汇报 向管理层提供流程报表，向客户提供变更的相关执行信息。定期向相关小组 / 部门根据流程衡量标准汇报很重要，只有如此，才可以基于现有环境的最新信息，作出进一步的改进建议；

变更会议 变更经理负责定期或不定期召开变更会议，以在 IT 内部以及与客户就变更管理有一个好的沟通。在会上，可以传递如，最近变更规划（ＦＳＣ），将要实施变更的信息，也包括对变更流程的反馈和建议等；

变更流程回顾 建议定期回顾变更管理流程以提高效率和效能，在实施变更流程不久之后，可以进行第一次回顾，以确保流程得到正确实施并起到预期目的，发现的问题必须追根溯源并尽快解决。之后，可以定期举行正式的回顾——如每三个月。

发布管理流程

发布管理：发布管理是指对经过测试后导入实际应用的新增或修改后的配置

项进行分发和宣传的管理流程。发布管理以前又称为软件控制与分发，它由变更管理流程控制。

发布管理流程的主要活动

发布规划

发布的准备

培训

生产环境的测试

用户接受测试 （User Acceptance Test）

系统推广

服务提供管理流程

服务级别管理：服务级别管理是为签订服务级别协议（SLAs）而进行的计划、草拟、协商、监控和报告以及签订服务级别协议后对服务绩效的评价等一系列活动所组成的一个服务管理流程。服务级别管理旨在确保组织所需的IT服务质量在成本合理的范围内得以维持并逐渐提高。

IT服务财务管理：IT服务财务管理是负责预算和核算IT服务提供方提供IT服务所需的成本，并向客户收取相应服务费用的管理流程，它包括IT投资预算、IT服务成本核算和服务计费三个子流程，其目标是通过量化服务成本减少成本超支的风险、减少不必要的浪费、合理引导客户的行为，从而最终保证所提供的IT服务符合成本效益的原则。IT服务财务管理流程产生的预算和核算信息可以为服务级别管理、能力管理、IT服务持续性管理和变更管理等管理流程提供决策依据。

IT服务持续性管理：IT服务持续性管理是指确保发生灾难后有足够的技术、财务和管理资源来确保IT服务持续性的管理流程。IT服务持续性管理关注的焦点是在发生服务故障后仍然能够提供预定级别的IT服务，从而支持组织的业务持续运作的能力。

能力管理：能力管理是指在成本和业务需求的双重约束下，通过配置合理的服务能力使组织的IT资源发挥最大效能的服务管理流程。能力管理流程包括业务能力管理、服务能力管理和资源能力管理三个子流程。

可用性管理：可用性管理是通过分析用户和业务方的可用性需求并据以优化和设计IT基础架构的可用性，从而确保以合理的成本满足不断增长的可用性需求的管理流程。可用性管理是一个前瞻性的管理流程，它通过对业务和用户可用性需求的定位，使得IT服务的设计建立在真实需求的基础上，从而避免IT服务运作中采用了过度的可用性级别，节约了IT服务的运作成本。

2.3 关键性技术研究与分析

系统中为了满足一些功能的实现以及使用的人性化等采用一些目前比较流行的技术，下面就其中几点关键性技术做一些介绍。

2.3.1 Web2.0 技术

Web2.0，是相对 Web1.0(2003 年以前的互联网模式)的新的一类互联网应用的统称，是一次从核心内容到外部应用的革命。由 Web1.0 单纯通过网络浏览器浏览 html 网页模式向内容更丰富、联系性更强、工具性更强的 Web2.0 互联网模式的发展已经成为互联网新的发展趋势。

Web1.0 到 Web2.0 的转变，具体的说，从模式上是单纯的“读”向“写”，由被动地接收互联网信息向主动创造互联网信息的转变。从基本构成单元上，是由“网页”向“发表/记录的信息”发展;从工具上，是由互联网浏览器向各类浏览器、RSS 阅读器等内容发展;运行机制上，由 “Client Server”向“Web Services”转变。

目前，有很多网站设置的交互式的栏目采用的就是 Web2.0 技术，Web2.0 以用户为主，以简便随意方式，通过 blog/podcasting 方式把新内容往网上搬很好地实现了客户端和服务器的内容上的交流。Web2.0 以人为核心线索，提供更方便用户织网的工具，鼓励提供内容。

集中运维管理系统除了要实现监控信息的统一集中展现以外，还需要通过一些工作流程来实现对 IT 资源的管理和维护，这就需要有客户端和服务器端的交流，Web2.0 技术很好地实现了这一功能，使得动态的运维得以实现。

2.3.2 Portal 技术

Portal 是一种 web 应用，通常用来提供个性化、聚集各个信息源的内容，并作为信息系统表现层的宿主。聚集是指将来自各个信息源的内容集成到一个 web 页面里的活动。

Portal 的功能可以分为三个主要方面：

Portlet 容器：

所有的 Portlet 都部署在 Portlet 容器里，Portlet 容器控制 Portlet 的生命周期并为其提供必要的资源和环境信息。Portlet 容器负责初始化和销毁 Portlets，向 Portlets 传送用户请求并合成响应。

内容聚集：

Portlet 规范中规定 Portal 的主要工作之一是聚集由各种 Portlet 应用生成的内容。

公共服务：

Portlet 服务器的一个强项是它所提供的一套公共服务。这些服务并不是 Portlet 规范所要求的。在大部分实现中都有望找到的几个公共服务有：

单次登录：只需登录 portal 服务器一次就可以访问所有其它的应用，这意味着你无需再分别登录每一个应用。

个性化：个性化服务的基本实现使用户能从两方面个性化她的页面：第一，用户可以根据她的自身喜好决定标题条的颜色和控制图标。第二，用户可以决定在她的页面上有哪些 Portlets。

在石景山区电子政务集中运维管理系统在服务台界面和个人桌面的页面展示中使用了 Portal 技术，用户可以根据自己的需求在大量信息中选择自己所关注的内容展现在同一界面上，并且可以通过拖拽窗口来进行布局的调整。例如，如果我是一个网络管理员，我就可以将网络监控的一些信息显示添加到我的个人桌面窗口中集中显示。这样增加了系统的人性化设置，在个人桌面这个界面中体现得比较好。

2.3.3 单点登录

单点登录（Single Sign On），简称 SSO，就是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统。单点登录系统的目的就是为目前所有的运维监控系统（集中运维管理系统、网络监控系统、服务器监控系统等）提供集中统一的身份认证，实现“一点登录、多点漫游”的目标，方便用户使用。

单点登录系统可以实现以下功能：

统一授权：平台为用户统一颁发数字证书和私钥并存储在 USB-KEY 中，作为用户访问平台及各应用系统的凭据，并对用户访问应用系统的权限进行授权。

身份认证：用户在访问平台及各应用系统时，都使用相同的凭据（即包含用户证书和私钥的 USB-KEY 及其硬件保护口令 PIN），并利用数字签名技术在平台进行身份认证，证明其身份的真实性。

单点登录（SSO）：用户在通过平台认证后，可直接访问已授权的各应用系统，实现不同应用系统的身份认证共享，从而达到多应用系统的单点登录。

数据共享：认证平台存储了用户的基本信息和证书信息，所有应用系统均可以充分利用这些信息，减少用户信息的重复录入。

安全通道：平台提供两种安全通道：一种是应用层安全通道，一种是网络层安全通道。它们为内网应用之间或外网应用之间提供安全的传输通道，保证其中

传输的数据的安全性。

在石景山区电子政务集中运维管理系统中由于使用SSO技术，可以把网络监控系统、应用监控系统等其他监控系统的页面直接展现在运维管理系统中，使得维护人员无需登录多个系统就可以访问所需的信息。

第三章　石景山区电子政务运维管理系统方案设计与分析

3.1　运维管理系统总体设计

针对石景山区电子政务运维管理系统的建设需求和技术规范，在对石景山区电子政务系统现有网络、服务器、应用、安全、存储、环境等基础架构充分理解的基础上，将整个业务系统作为管理和保障的核心。设计一套真正符合石景山电子政务系统的实际网络IT环境，从集中完善的全面监控和规范化运行管理出发的技术方案。整个设计围绕“集中统一”的思路展开，区别与以往的分散的单一功能的运维管理系统。同时，参考ITIL中的流程的规范和标准，结合实际情况围绕IT资产管理进行流程的梳理。

在经过学习和考察，以及和相关公司讨论的基础上，我带领项目组成员对石景山区电子政务运维管理平台的总体架构进行了设计，并在目前国内比较成熟产品的基础上结合实际需求进行了系统的功能以及展现形式进行了设计。

3.1.1　系统设计原则

管理完整性

支持异构网络包括我中心目前使用的各种网络及安全设备（Cisco，华为，联想，北大青鸟，天融信，绿盟等等）；

易用性

全中文界面，界面友好，操作简便易用。

语言通俗易懂，易于理解。

开放性

可根据用户的需求进行定制和二次开发。

可以与设备厂商的专用管理系统的接口及部分功能集成。

稳定可靠性

系统应考虑硬件和软件的容错、数据存储的备份/恢复等系统可靠性措施。

服务器应采用相应的机制，以保证服务器故障不影响或少影响现有被管系统的正常运行。

系统具有自检功能，能监测系统各功能模块的运行情况，随时发现系统自身的问题。

运行稳定，资源占用低，客户端大小不高于 15M，系统内存占用不超过 10M，不会影响现有网络和系统的正常运行。

可用性

系统设备能支持 7x24 小时连续不间断工作。

系统数据采集不能影响被管系统的稳定性，也不能明显影响被管系统的性能。

扩展性

功能扩展性：硬件系统采用模块结构，以保证系统功能、处理器及储存容量的扩展。硬件配置的升级不应引起应用软件的修改和开发。

架构扩展性：可分布式部署到多台服务器上。

自身可管理性

系统自身管理是指对系统自身的配置、运行状况、备份、服务流程和系统安全等进行管理。通过系统的自身管理，保证系统能够安全可靠地运行。

安全性

数据备份与恢复

提供对系统数据的备份与恢复功能。数据定期进行增量备份，也可以手动备份所有数据。能够清除较早的数据；

提供数据备份接口，能够实现通过第三方备份软件实现数据备份工作。

自身运行状态管理

提供对管理系统自身所有后台服务器模块的运行状态监视，在发生故障时及时告警，设置一定的恢复策略。

权限管理

系统可以为不同角色的用户定制不同的管理权限，通过设定不同的权限，来保证本系统的数据安全性。用户可以通过分组进行管理，组内用户的权限一致。能够定义用户对不同的监控视图有不可见、浏览（读）、操作权限（写）等。

提供操作日志管理。用于记录用户对系统各功能进行操作的信息，提供对日志记录的查询、转存、删除和打印操作。日志的查询条件可以为：用户名，登录来源 IP 地址，操作时间、功能模块。用户操作的信息需要打印的记录可打印输出。

3.1.2 系统总体建设目标

系统将按照高起点、高标准、高质量的要求，采用基于 ITIL 理念的先进 IT 监控技术实施系统管理、应用管理、网络管理，对电子政务的系统运行环境进行信息采集、管理和监控，并在此基础上构建一个平台化、智能化、集成化、高可靠性的集中网络运行管理平台，用于石景山区信息化工作办公室的日常运行管理。平台具有计算机网络、重要网络设备、骨干网链路、业务应用、安全设备等的监

控报警功能，将管理、监控有机地结合起来，提升整个信息中心的IT管理水平。

系统的建设要实现如下目标：

建立在统一平台架构下，实现对石景山区电子政务系统的网络及主机系统监控管理、安全运行管理、工单流程管理和配套运行服务体系的目标。面向业务运行维护管理需要的IT管理体系，提高网络设备管理质量；

保持IT系统可靠性和可用性，保证系统、设备24小时不间断为区政府办公业务资源信息系统提供可靠服务，在此前提下提高IT设备的利用率；

在复杂的异构环境中统一管理，轻松维护复杂的异构环境并使之有效运行；

把系统管理人员从管理设备的复杂负担中解放出来，系统能实现自动的监控和告警；

总结和统计出对网络管理、安全管理、应用管理性能监控中有用的信息，为管理者提供更全面、更直接、更专业的管理信息，为制订相关决策提供依据，提高网络安全、网络故障的应急相应速度；

构建可靠的安全运行管理平台，实现对安全系统和设备的监控管理，基于安全事件的收集、分析、预警、响应和故障过程管理，实现与运维工单管理的无缝结合，实现对全网安全风险的分析和计算、展现。提供配套的系统运维管理策略、制度和规范。

建立与管理体系相适应的管理辅助工具，包括网络管理、系统管理、安全管理、流程管理等，从而最大限度的屏蔽IT技术的复杂性，实现自动管理，降低对人的依赖；

将错综复杂的系统信息，各类系统事件按照IT服务管理的需求进行过滤整理，帮助系统维护人员更专注于对重要事件的管理和响应；

通过项目实施，梳理、归纳IT系统管理工作规范，制定信息中心IT服务管理标准并进行推广。实现对整体运维工作的监督、追踪、考核和评价管理。

3.1.3 系统设计思想

随着系统规模的不断扩大，业务应用的持续增加，电子政务 IT基础设施的架构越来越复杂，单纯凭某个工具或某个人，已经不能胜任如此大的工作量和满足业务紧迫性的要求，必须有一整套借助先进方法论的IT系统运维管理的解决方案。

全方位的IT系统与运维管理：运维管理系统平台是管理一个单位的信息系统及其相关组件的一整套原理和工具，不仅是管理软件产品本身，而且还包括管理流程(Process)、管理规范 (Policy)、 办公业务(Business), 和将管理流程、管理规范及办公业务贯彻到软件产品中去的实施方法。通过石景山区电子政务集中运维

管理系统的建设，将做到信息网络故障早发现、早解决，确保计算机系统、网络和应用的连续、可靠、安全运行，降低发生故障的可能性，提高石景山区电子政务系统的IT系统运维管理水平和服务保障能力。

满足IT系统基础设施、维护管理人员、领导决策者、业务系统的使用者等多角度的管理需求：

面向基础设施的管理

全面管理系统资源

提供对网络、主机、操作系统、存储设备、数据库、中间件及应用软件、安全设备等IT资源的全面管理；包括纵向资源的配置与拓扑管理，可以生成详细的资产统计报告，以便准确掌握资产情况；能使用多种方式表现系统拓扑视图。

性能管理与优化

即面对系统和数据库等性能进行监控，建立性能处理的基线。定期提出性能报表和趋势表，可以根据趋势分析，提出性能优化的建议，如应修改某参数，购买新硬件。

故障管理

提供一个集中管理故障和事件的中心，能够收集各种管理功能产生的故障事件（例如：网络事件、主机事件、存储备份事件、安全事件等）。完成故障事件收集、过滤、关联和处理等工作，以实现对故障的快速处理。

面向维护管理者

运维服务管理

运维服务管理基于人与流程的结合，提供方便，灵活工作流程的管理功能，使工作人员维护管理工作的自动化和信息化，其中包括帮助台、事件、问题管理以及值班管理、设备维修、工单管理等根据客户量身定制的业务管理功能。

系统监测

通过实时地动态视图显示管理系统的实际数据，一目了然地看到当前IT系统的运行状态及趋势。可以综合监控IT系统中各种资源的实时状态和性能信息等所有运行情况，帮助管理人员发现问题进行快速处理，分析和确定瓶颈所在。

知识库

为了使工程师在处理系统故障的时候，能够进行参考相关故障处理的方法，从而可以一方面降低系统管理的风险，另一方面可以让有相当技术水平的工程师也能够进行系统维护，降低系统管理对个人的依赖。知识库能够很好地存储各类系统技术方面的知识和系统描述的知识，同时也能方便进行分类和进行查询。

面向领导决策者

统一访问管理

提供基于 WEB 的统一 IT 系统访问入口，使用户能够在统一登录、统一认证的情况下，方便的实现对 IT 系统的访问和管理。

综合报表

对系统的管理信息进行汇总和相关的决策分析，并以图表的方式为管理人员提供直观的分析结果，以更全面的了解网络、主机、数据库、应用系统运行的状况，发现可能的隐患。为提高管理水平提供决策信息。利用系统生成的简洁，直观的报告，可以方便的了解系统在任一段时间内的运行状态。可以灵活生成各类事件与性能报表，提供趋势分析与决策支持功能。

绩效考核

通过运行管理平台可以实现对维护人员的考核。考核可以通过对日常维护任务的关键指标进行定义而实现。针对衡量指标，提供相应的统计报表，进行统计和查询。并能够配置关键指标（KPI）和考核分数的对应关系，自动对维护人员的考核分数进行计算。通过运行管理平台还可以对运行管理质量年的部分考核指标进行网上考核、发布。

面向业务应用者

综合业务服务

IT 服务部门和业务应用部门相互联系的接入点，记录、分解和监控提出的问题。其可以服务台的形式存在，同样具备更宽泛的角色，如接收变更请求(RFC)，并且可以支撑多种流程中的操作。它也是报告突发事件和提交服务请求的焦点，例如：服务台可能扮演用户提交请求的联系点， 基于管理流程传达实施计划，并保持将实施进程通知用户。

业务影响分析

自动分析故障对服务、业务部门和用户影响，来改善自身的服务水平，支持用户以直观方式观察系统故障是如何影响业务、服务和关键业务应用的，获取切实的经济收益。这种功能往往可以在无需人员介入的情况下对重要的事件做出及时的反应，极大的提高了为业务应用者服务的质量。

构建先进的技术架构体系：为满足系统规模不断扩大，业务不断增长，IT 基础架构不断变化和发展，要求系统管理的架构具有如下特点：良好的框架结构，能够方便、容易地增加管理功能；能够灵活的添加被管理的节点；能够全面管理所有的资源；各管理功能之间共享管理数据。

提供端到端、面向业务的管理：将 IT 管理与业务的运行联系起来，并通过所有不同的管理工具的控制台进行统一和集成，实现信息共享。

建立统一、集成的管理平台：对异构的管理对象和多种管理进行统一管理，实现对系统进行高效、准确的管理。

实现管理系统的快速开发部署：有效的利用投资，快速将投资的效果体现出来，为机构的业务运行做出贡献，系统管理技术方案具有模块化的开发、产品快速部署的能力、能够实现“开箱即用”的效果等特点。

保证管理系统的开放性：管理系统需要符合业界标准，以实现对各种资源的统一管理和与其它管理软件的集成。同时管理系统需要开放开发接口，以方便扩展管理功能。 统一 IT 运维管理需要基于开放的管理平台，遵循业界标准，并提供管理接口。

3.2 运维管理系统体系结构设计

石景山区电子政务集中运维管理系统属于石景山区电子政务运维体系的一部分，从整体来讲整个运维体系主要分为三个层次，如图 3-1。

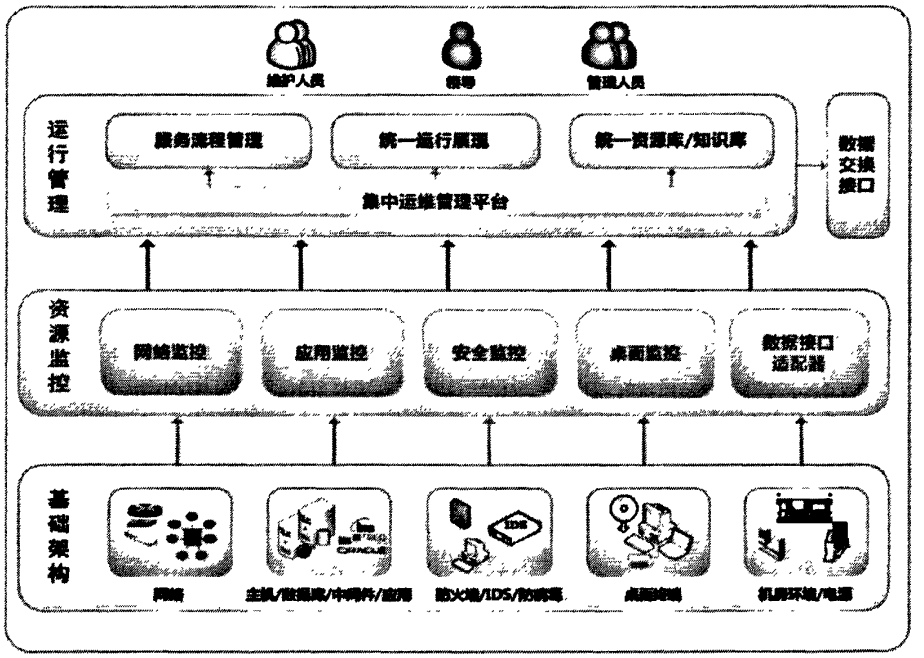

图 3-1 电子政务运维体系

最底层是基础架构层，包括电子政务系统所涉及的业务系统、物理、软件、信息资源、服务等运维工作所涉及的资产；中间层是资源监控层，主要包括网络监控、应用监控、安全监控等专项资源监控系统；最上面一层是运行管理层，对资源监控层的信息进行整理和分析，统一运行展现，形成统一的资源库，并与服务流程进行关联。

集中运维管理系统处于整个运维体系的最高层，属于运行管理层，它需要整合以往对网络、服务器与业务应用、安全设备、客户端 PC 和机房基础环境等的分

割管理，实现对 IT 系统的集中、统一、全面的监控与管理。同时通过融入 ITIL 等运维管理理念，达到了技术、功能、服务三方面的完全整合，实现 IT 服务支持过程的标准化、流程化、规范化，极大地提高了故障应急处理能力，提升了信息部门的管理效率和服务水平。

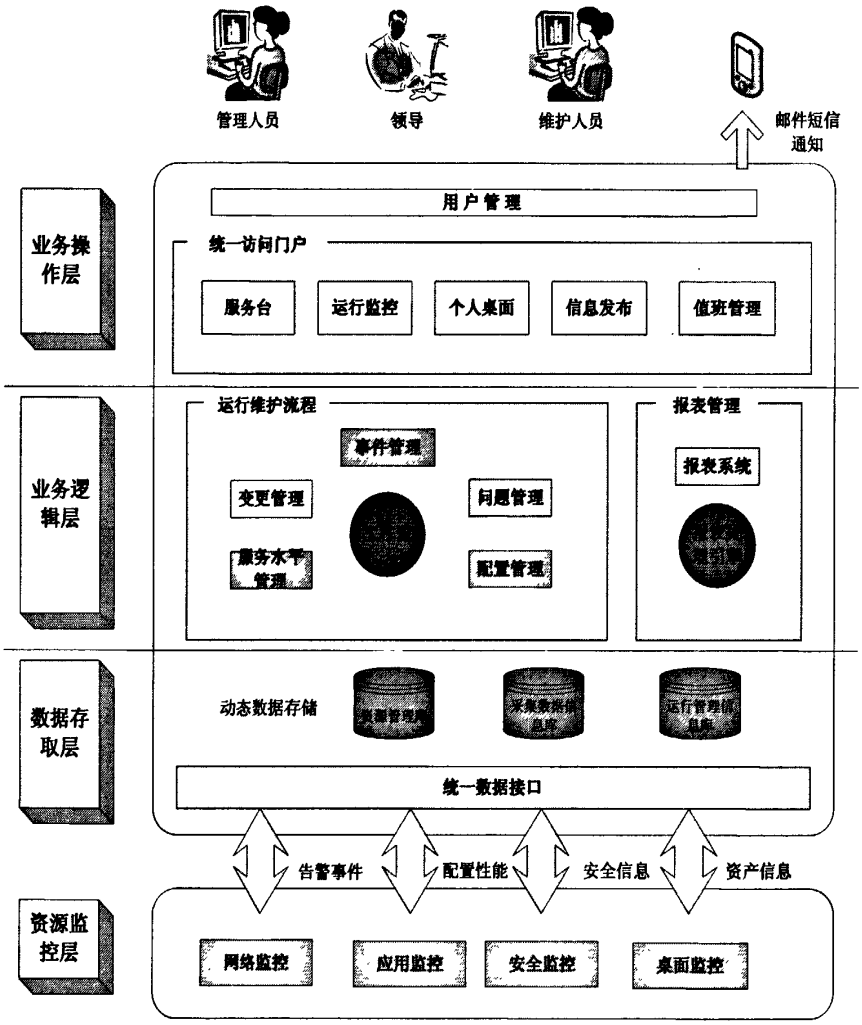

图 3-2 体系结构图

运维管理系统总体来说在保持技术的先进性、扩展性的基础上，采用层次化、模块化的设计，同时应满足和其他主流管理厂商产品的对接，通过开放的接口来持续集成。从图 3-2 可以看出系统通过数据存取层与资源监控层进行对接，通过分布式数据采集、集成接口，实现监控的数据接入，形成动态数据的存储。在数据存储，主要包括资源管理库、采集数据信息库、运行管理信息库的基础上，通过运行维护流程和报表管理等形成的业务逻辑层的模块功能将运行监控的数据统一在业务操作层展现。同时，操作员和管理员等也通过业务逻辑层将运维过程中产生的数据与数据库进行交换，保持数据库的动态更新。

3.2.1 数据存储层

数据存储层位于运维管理系统的最底层，通过统一数据接口将资源监控层获得的告警事件、配置信息、安全信息以及资产信息等数据进行提取，并形成系统的基础数据库以供在业务层展现以及使用。

统一数据接口

作为统一事件平台的入口，系统需提供统一数据汇入接口完成各类数据上报的标准化，并提供接入第三方管理系统上报数据的能力。通过统一数据接口，具有到良好的系统扩展性。统一数据接口的结构图如图 3-3：

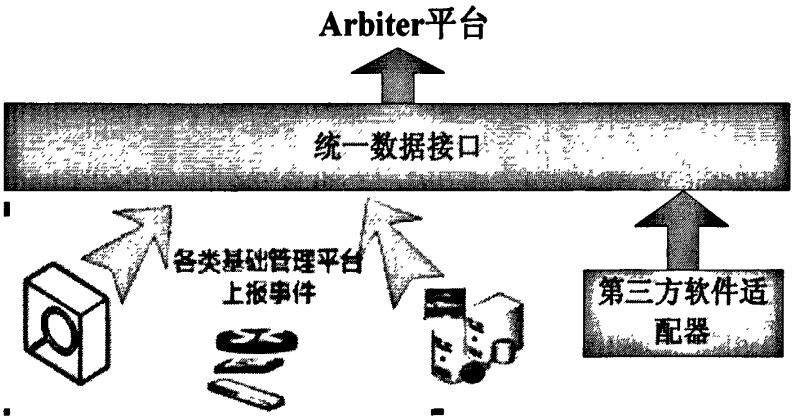

图 3-3 统一数据接口逻辑结构图

统一数据接口采用以下技术规范，并遵循以下指标：

采用在 CORBA 技术，CORBA 作为最成熟的分布式对象技术，具有性能优异，扩展性好等主动特性，被认为是下一代管理体系的最优框架。

统一数据接口支持多种语言，系统采用 IDL 接口描述，并提供地址透明的名称服务，支持分布式的数据汇总。

统一数据接口和 JAVA 平台、.Net 平台有很好的兼容性。

为了便于接入常见类型的事件，统一数据接口可以直接接入 Trap、Syslog 等常用的告警、日志格式。

统一数据接口上提供了面向 C++/JAVA 的接口封装，形成扩展管理适配器，便于提供第三方管理系统的集成。

第三方采集软件将通过统一数据接口适配器接入，一方面保护用户的现有投资，一方面补充了综合监控和管理平台的管理能力。通过第三方采集软件可以进一步扩展监测的范围和广度，挖掘监测的细粒度和深度。同时，Arbiter 核心平台内置了对国内外主流管理采集软件的集成接口，可以实现数据和事件集成，将第三方采集软件的管理对象或者数据信息进行提取，以满足用户对全网监控的一体化和扩展性要求。

经过统一数据接口，标准化的事件的相关定义如下：

故障事件等级	等级说明	英文含义
0	正常事件（恢复事件）	Clear
1	未知事件	Indeterminate
2	警告事件	Warning
3	次要时间	Minor
4	严重事件	Major
5	紧急时间	Critical

表 3-1 告警事件严重等级对应表

事件类别	事件子类
网络事件	链路通断
	端口故障
	设备故障
	流量预警事件
	性能事件
	……
安全事件	网络探测事件
	网络攻击事件
	异常流量事件
	异常协议事件
	……
系统事件	主机事件
	存储事件
	备份事件
	终端事件
	数据库事件
	中间件事件
	……
业务事件	OA 系统
	财务系统
	……

表 3-2 告警事件分类对应表

中文名称	说明
事件的序列号	产生事件消息的序列号
事件标识	事件的标识
事件源（被管对象）	事件发生源
事件初次发生时间	事件第一次发生时间
事件最后发生时间	事件最后一次发生时间
事件发生次数	事件重复发生的次数
事件变化时间	事件变化时间
事件类型	事件类型
事件级别	事件级别
活动状态	事件当前状态
事件负责人	负责事件的操作员用户名
事件标题	事件标题
事件内容	事件内容
被管对象联系人	负责被管对象的用户名
被管对象负责人联系方式	负责被管对象的用户联系方式，如电话
相关业务	被管对象支持的业务
可扩展属性	……

表 3-3 告警事件属性表

管理信息库主要由资源管理库、采集数据库、运行数据库三大逻辑信息库共同结合组成，存储的数据主要包括了配置数据、性能数据、告警数据、运维管理数据等，通过集中化的管理信息库来组织，形成运维管理系统的“数据中心”。同时，采用 Oracle 数据库作为统一的管理信息库，满足稳定性、伸缩性要求。

资源管理信息库

资源管理信息库（RDB）在网络综合管理中的举足轻重，同时资源管理信息库也可以扩展为 ITIL 中最重要、核心的配置管理库（CMDB）概念，资源管理信息库 RDB 其作为信息的组织和存储机制，为网络管理中的性能告警、ITIL 中其他的功能提供基础信息，并在整个运维管理团队得到共享，因此具有十分重要的地位。

所有为提供综合 IT 网络服务需要的人员、流程、技术实施中涉及到的所有元素，都被称为配置项或者资源项（ITEM），如软件、服务器、网络设备、链路、应用系统、服务等等；而 RDB 就是所有资源项信息的集合和存储。集中运维管

理系统对各种网络设备、服务器、应用进行采集，经过数据的加工后，保存在资源管理信息库中。

资源信息库按照资源类型进行分类，并为每一类资源单独定义属性，资源的主要信息遵循统一资源管理规范，主要包括以下内容：

- 资源基本信息：资源的内部标识、名称、类型、IP 地址、物理地址、厂商、IOS 版本等基本信息；
- 资源管理信息：资源的管理分类、用途分类、管理部门、管理人、安装位置、开始使用时间、终止使用时间、使用状态、重要级别、风险级别等；
- 资源来源信息：包括购买日期、资产价值、资产来源类型、资产来源；
- 资源属性信息：资源的附加配置属性，不同类型的资源的配置属性有所不同，例如网络设备的固件版本、设备模块组成、端口种类、服务器的操作系统类型、硬件配置、存储设备、软件资源的 Licence、服务端口、模块组成等；
- 资源状态信息：资源当前的运行状态信息，例如网络设备的端口状态，数据库运行状态等；
- 资源关联信息：提供资源的关联信息，必须提供网络节点的拓扑信息，可选提供资源的父子、安装等其他关联信息；
- 资源维护信息：包括资产编号、资产的负责人，资产的集成商，以及产品支持厂商、当前质保期、历次故障记录、历次购保记录、历次维护记录，为资产维护提供数据的支持。

系统对资源建立统一的配置模型，并提供资源明细表用于发现和监控各类资源，在库中进行统一压缩、归并，并通过数据仓库的方式抽取数据，进行挖掘和分析，资源管理库的模型如图 3-4：

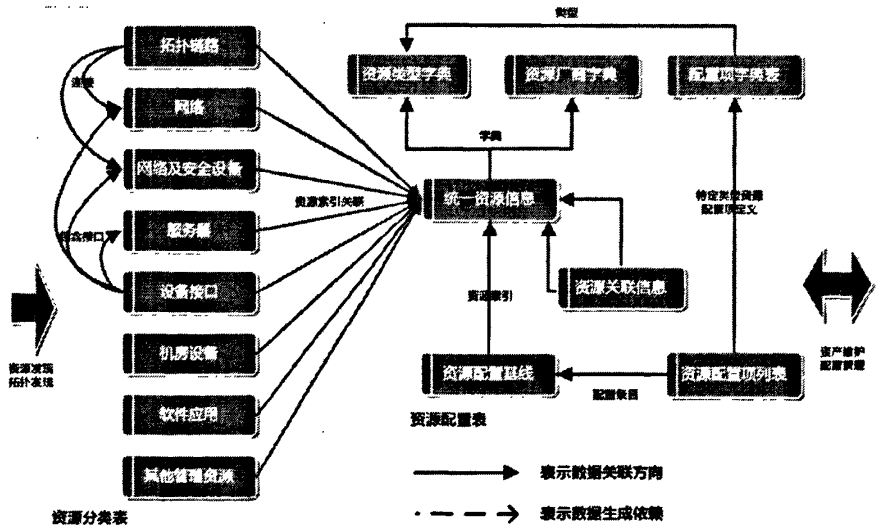

图 3-4 资源管理信息库模型

运维管理系统的资源管理信息库采用动态建模技术，主要具有以下技术特色：

➢ 资源项动态建模

资源管理库内置了动态数据字典，可以实现：

对资源项提供了多级类别结构，满足信息中心复杂的资源分类需求；通过资源项维护管理界面，用户可以扩展资源项的信息，系统提供了丰富的属性定义特征，包括：属性名、属性宿主类型，属性数据类型、属性值范围、属性可选值、属性默认值、属性校验配置等；动态字段数据存储表提供了数据存储和绑定功能，并通过组件方式封装了添加、删除、检索、修改等机制。

➢ 资源项关联关系

资源项类似于社会中的个人，和社会中的其他人和群体产生各种关系，资源管理库提供了资源项的关联能力并支持用户扩展，内置的关系包括：

关系描述	备注
具有	描述父子关系,应用系统包含了 Weblogic 中间件
安装	用于计算机安装的信息，比如服务器操作系统上安装了数据库服务
访问	描述访问关系,如计算机访问网络,政府应用的 WEB 服务器访问 DB 服务器

表 3-4 资源关系表

资源库维护功能

资源管理库中的核心数据的存储，提供数据模型字典检查、资源项数据校验、资源关联关系检查、数据备份和恢复等维护功能。

此外，资源管理库还提供配置变更的历史审计功能，可以保存每个资源项的变更历史，方便用户进行配置恢复和历史审计。

资源管理模版功能

资源管理库支持用户的 out-of-box 的使用，系统随资源管理库搭配了各类管理模板，用户按照需要选择适合自身管理特点的模板并导入，即可快速的建立起适合自己 IT 环境的资源管理库。

采集数据信息库

采集数据库的主要包括了性能数据和告警数据，是综合网管分析和报表数据的主要来源。

采集数据库采用数据仓库技术，数据仓库技术的目标是在大量数据的基础上进行及时、准确、智能化的分析，为决策提供支持。采集数据仓库中融合了 OLAP 和数据挖掘技术，数据按照不同的分类和时间纬度进行划分和重组，形成面向不同视角的统计数据，采集数据库的主要特性有：

➢ 采集数据库提供各种归并数据，按照时间间隔重组的数据包括：原始性能

数据表、小时性能数据表、天性能数据表、周性能数据表、月性能数据表、年性能数据表，能满足按照不同时间单位进行统计分析的需要。

➢ 采集数据库提供 Last 数据的缓存数据，包括最近 1 小时、最仅 1 天、最近 1 周的高速检索数据表，保证常用数据获取的高效性。

➢ 采集数据库还可以按照采集的类别进行分组存储，从而便于对相同类型的采集数据进行比较分析，并形成排名等分析报表。

采集数据库的还包含了数据采集的管理信息，通过这些管理和数据信息的结合，可以方便、快速地在此基础上定制各种报表。

采集数据库的还包含数据采集的管理信息，通过这些管理和数据信息的结合，可以方便、快速地在此基础上定制各种报表。

采集数据库的数据模型如图 3-5：

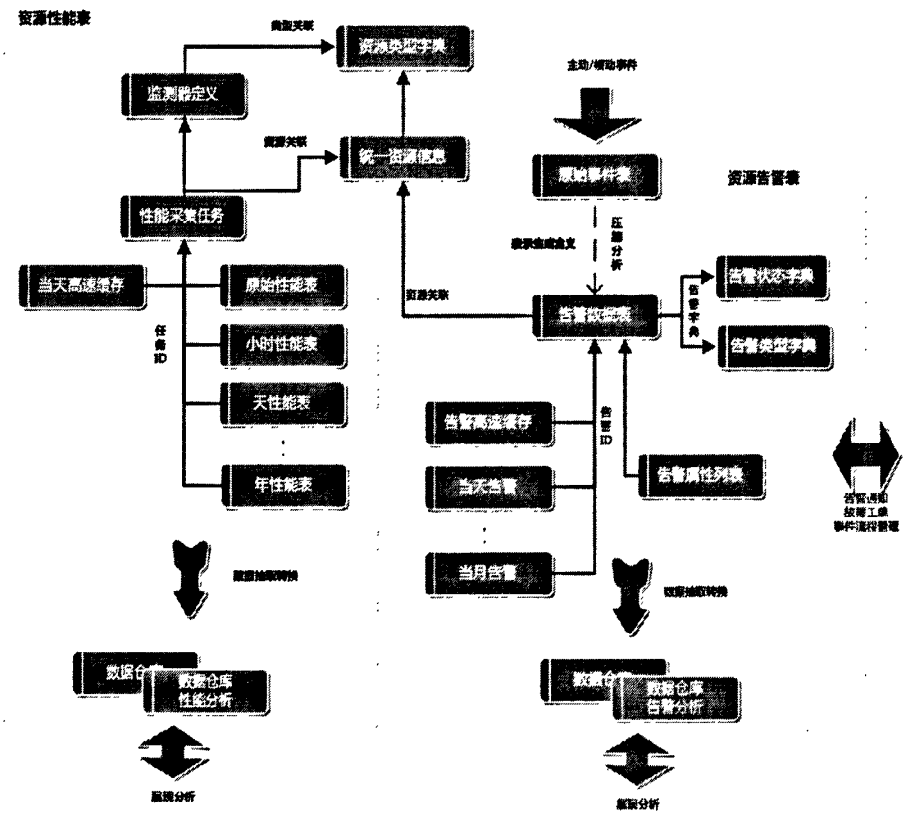

图 3-5 采集数据库模型

从上图可以看出：采集数据从逻辑上可分为两大类：

➢ 性能信息

性能数据库主要保存各类性能数据，为运行展现、统计分析提供性能数据，为评估、调整、优化运行提供数据支持和决策协助。

性能数据库满足以下技术规格：

可定义扩展：可以通过扩展性能指标字典，提供新的性能采集数据存储；

数据仓库存储：采用数据仓库的方式存储，可以在基本性能数据信息基础上，按照时间、类型等维度进行扩展，为深入分析和挖掘提供数据；

数据保存时间：原始性能数据可保存 3 个月以上，小时性能数据可保存 1 年以上，其他数据可保存 2 年以上。

➢ 事件信息

事件信息库包含以下内容：

原始事件信息：可选保存。原始事件包括来源、地址、发生事件、接收时间、事件级别、事件信息、扩展属性名、扩展属性值等基本信息；

告警事件信息：保存经过压缩、归并分析后的告警信息。告警事件属性包括：告警来源、告警标题、告警描述、告警级别、第一次事件发生事件、最后一次事件发生时间、事件数量、可信度、告警修改事件、处理状态、解决状态、负责人，扩展属性名、扩展属性值；

事件关联信息：如果保存原始事件，可以从告警事件察看到向关联的原始事件。

采集数据仓库具有自维护管理特性，维护模块会自动对入库的数据进行定时的分析和处理，确保数据的同步和准确性，不会因为数据仓库的维护增加管理人员的负担。

运行管理信息库

运行管理信息提供了集中运行监控的数据支撑，提供了运行的数据建模，支持各种运行监测的管理，并且通过运行知识库协同解决知识共享和再利用的问题。将 IT 运行管理提高过程建立在知识积累和共享的过程之上，并对行业性知识和规范提供支持。运行管理信息主要分为：

➢ 运行信息

运行信息库包含下述内容，并且可以将来实现和 IT 服务管理系统的集成和对接：

值班管理：提供多级值班安排、交接班、值班日志的数据支持；

资产维护：基于资产角度的巡检、维护、折旧等生命周期管理数据支持；

项目管理：提供项目的管理支持，并且和资产向关联；

发布管理：提供信息发布管理的数据存储支持；

运行知识

通过运行知识库协同解决知识共享和再利用的问题。将 IT 运行管理提高过程建立在知识积累和共享的过程之上，并对行业性知识和规范提供支持。

运行知识库包括以下分类：

采集知识库：为数据采集的指标和阀值提供模板和建议；

分析知识库：提供事件分析、关联、根源的知识策略；

行业知识库：提供行业信息部门标准、指标、规范性指导，以及诊断的知识信息；

信息知识库：提供各类信息的帮助知识库，例如：典型安全告警的帮助和解决知识。

3.2.2 业务逻辑层

ITIL 中的核心思想是以流程为核心，实现对 IT 资产的动态管理。集中运维平台也参照这一核心思想针对实际的运行管理环境，提出管理思想+管理流程+管理软件的融合，并且和下层实现监控功能的资源管理层有机结合，避免集中运行监测表面化，脱离实际发生的情况。

从运维组织结构的角度出发，运维维护流程模块提供了一个灵活的流程结构框架，可以把 IT 管理相关的角色映射到 IT 运维监控管理平台中。从而深刻地体现“人员－流程－技术”三者的统一。运维维护流程采用 ITIL 流程引擎，为用户提供标准的事件管理、变更管理、配置管理流程，依托灵活工作流引擎的配置功能，可以对流程进行修改和调优，并可以派生子流程，确保符合实际运维的工作需求。

报表管理模块则通过报表中心和资源管理帮助管理员更全面地了解 IT 资源情况及其运行状况和运行趋势。

运维工作流引擎

随着信息化水平的不断提高，IT 系统的规模和复杂度也越来越高，管理工作也变得日益交错和被动。信息部门内部需要保障系统运行质量，外部需要为用户提供更好的业务服务，在此趋势下，部分政府和部门开始采用业内公认的 ITIL 流程框架，以改进 IT 与业务的调和，不断提高管理和服务水平。

ITIL 作为 IT 管理的最佳建议标准，提供有关要遵循的步骤和流程的准则，并形成了 ITSM 等标准化的 ITIL 服务管理实践模型。但是在实际操作中如果一味按照 ITIL 的流程照搬，就会脱离实际用户的使用习惯和实际的管理状况，导致 ITIL 的实施好似“空中楼阁”，无法适应用户的现有管理状况，反而导致了效率的降低。

石景山区电子政务集中运维平台针对这种情况，在工作流引擎部分内置符合中国管理特色工作流引擎 COSS-WF。COSS-WF 针对国内信息部门的管理模式和工作习惯设计，并且吸收了众多国外的 ITIL 服务台产品（Remedy、HP OV ServiceDesk、CA Unicenter ServiceDesk）的工作流理念，是符合国内用户工作管理流程运维工作流引擎。COSS-WF 从电信行业吸收了“工单”的理念，符合中

国管理特点，可以有效地体现工作规范，进行流程闭环处理，跟踪处理进度、改善流程实施，提高管理服务水平。总体上说，工单管理系统就是为 IT 管理部门定制的流程管理系统。

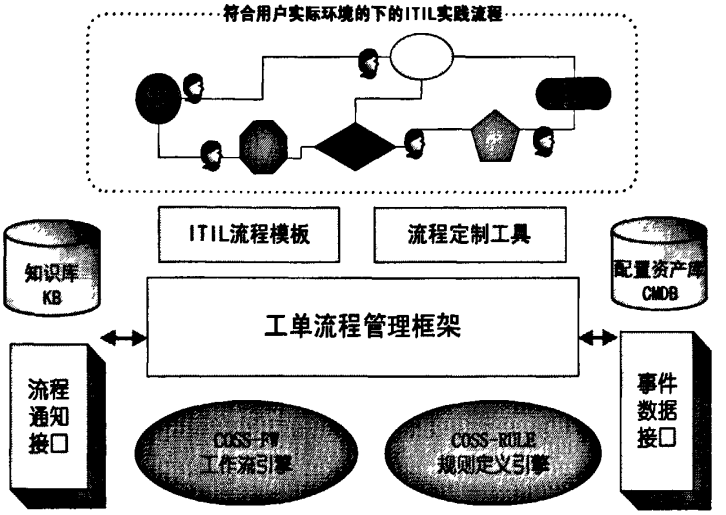

图 3-6 基于工单的 ITIL 工作流引擎

工单管理提供 ITIL 各重要管理流程的模板，同时提供工作流定制图形化工具，可以在实施阶段，根据用户自身的管理状况进行调优，提供端到端的运维流程解决方案，工单管理内置了多种流程管理动作，包括：

建立工单、派发工单、受理工单、退还工单、追回工单、转派工单、处理工单、工单升级、催办工单、回复工单、工单注释、工单评价、作废工单、关闭工单等。

3.2.3 业务操作层

业务操作层直接面对管理维护人员以及领导，集中运行展现系统衔接运行维护人员和业务逻辑层，提供集中展现和流程管理功能。

集中运行展现通过丰富、直观的展现窗口界面，呈现运行管理的整体状况；通过不同视角的视图，帮助运维人员准确评估运行性能，及早发现故障隐患。

集中运行展现的主要功能包括：拓扑展现、运行展现、告警展现等。

拓扑展现主要以图形化的方式展现综合 IT 网络管理环境，提供运行值班人员的监测入口，降低由于管理范围庞大造成的集中监测问题，拓扑展现视图包括：网络拓扑展现、业务拓扑展现。

运行展现从运行管理角度集中的展现，主要包括：运行值班视图、自定义分组视图、监测分组视图、今日一览视图、业务服务视图，并通过监控视图快速访问到各类报表和统计报告，从不同角度评估石景山区电子政务系统综合运行质量。

告警台通过集中化的故障告警管理界面，通过声、光等方式显示监测范围内的所有故障，并可以触发邮件、短信等动作通知相关人员，并在告警台快速定义告警策略，避免误报和错报。

集中展现模块具有以下技术特点和指标：

采用 JAVA J2EE 平台，提供了良好的伸缩性和扩展性。

采用 Portal 理念设计，基于标准 JAVA Portal API，符合 JSR168 规范，通过 WEB 浏览器进行访问，为用户提供了灵活定制的工作平台。

展现采用 Portal 技术，业务以展现模块划分，具备不断的增加和集成的能力，同时却不影响原有模块展现功能。

提供多种展现视图，用户可以从告警事件、业务系统、网络拓扑等不同视角全面评估 IT 运行情况，为运行人员更加有效的评估运行情况提供多角度支持。

提供导航式的展现方式，引导用户从整体运行到监测细节，从问题现象一层一层的分析到具体原因。

3.3 运维管理系统功能模块设计

为实现本单位的运维服务管理和支撑能力的信息化，必须建立与本单位运维服务管理和支撑能力相匹配的运维服务支撑系统。相应的，运维服务管理和支撑能力映射为运维服务支撑系统的功能。

3.3.1 资产管理

资产管理功能实现对各类资产信息的维护、统计以及资产全生命周期的管理，提供基于资产信息的辅助决策，并实现资产信息的共享。

系统应支持按角色设置不同的功能权限和管理范围权限，实现资产的分级管理。

系统应支持资产数据的备份和恢复。

➢ 资产信息维护

系统支持资产信息的维护，包括资产信息的获取与更新、查询、导出和打印。功能如下：

资产信息获取与更新：系统支持以多种形式将数据导入资产数据库；系统应支持资产信息的增加和删除，支持资产信息的手工录入和修改功能；

资产信息查询：系统允许用户设定单个或者多个条件的组合进行资产信息过滤查询，并以表格和图形的方式呈现；系统应允许模糊查询；

资产信息呈现：系统支持从业务系统、设备类型、地理分布、管理等级等不

同视角呈现资产信息；

资产信息导出与打印：系统支持将查询出的资产信息导出为通用格式文件进行保存，应具有将查询出的资产信息进行打印的功能。

➢ 资产生命周期管理

系统实现对 IT 资产的采购、入库、维修、借调、领用、折旧、报废、丢失、测试等生命周期各阶段的管理功能。

➢ 资产信息统计

系统应实现 IT 资产信息的统计，统计内容和功能的要求如下：

统计内容：系统应支持以下几类统计。资产数量类统计，主要统计资产的个数，用于反映资产规模情况；资产百分率类统计，主要统计处于某种状态的资产（如在用资产）占全部资产的比率；资产历史对比类统计，主要将资产历史情况和当前情况进行对比统计，反映资产的整体变化情况。

3.3.2 监控管理

监控管理包括对 IT 基础设施和应用系统的监控管理，实现 IT 基础设施和应用系统的视图管理、配置管理、故障管理和性能管理等功能。

➢ 视图管理

系统以图形方式呈现 IT 基础设施和应用系统的信息。能够动态实时显示各类资源的运行状态，方便用户直观地了解资源的分布与状态信息以及对网络中的资源进行监控。各类视图之间应能灵活进行关联。系统应支持以下视图：

网络拓扑图：以地理视图、层次图等方式显示物理、逻辑网络拓扑结构；

应用拓扑视图：呈现从用户、应用系统到 IT 基础设施间的依赖关系；

自定义视图：支持灵活的视图自定义管理功能，管理员可新增、编辑、删除拓扑图。支持用户自定义应用系统的基本信息、组成部件、依赖的基础服务、与硬件设备的关系、使用该应用系统的单位和用户信息。支持视图元素的星形、圆形、树形自动排列，并支持按照左、右、中间方式进行对齐。

系统应支持拓扑视图与故障、性能等功能的关联，能够在拓扑图上直观地显示被管资源的运行状态，并且支持告警的传递显示。

➢ 配置管理

系统应实现 IT 基础设施、应用、人员和供应商等各类资源信息的维护和分析统计，以及配置信息的下发等功能。具体包括：

资源信息维护：系统应支持对动态资源信息的自动采集，以及方便的静态资源信息手工录入，并支持对资源信息的更新、同步等维护手段；

资源模型编辑：系统应支持资源管理模型的编辑功能，通过模型的编辑工具，

可快速实现管理功能的调整；

配置信息下发和配置文件管理：系统应支持对可配置资源管理信息的下发控制。支持通过一个按钮即可快速批量设置整个 IT 环境的工作模式。系统应支持对网络设备配置文件的管理功能，包括配置文件上传、配置文件下载以及配置文件比较等功能；

资源信息统计分析：系统应支持对资源信息进行灵活查询与统计，报表统计的结果应能以图形（如直方图、曲线图、饼图等）或表格方式显示。

➢ 故障管理

系统完成对 IT 基础设施和应用系统的故障管理功能，包括告警信息采集、处理、显示、清除和故障定位等功能，系统应提供故障知识库功能。具体包括：

支持告警信息的实时采集，支持对 IT 基础设施和应用系统等资源的运行状态进行任务化的监视，支持设置不同的任务执行策略，完成不同监测粒度的需要；

支持告警的过滤、升级和压缩，并支持用户对告警过滤、升级和压缩条件的灵活设置；

将用户关心的告警信息以列表、视图、颜色等形式呈现给运维人员，并支持对告警显示过滤条件的灵活设置；

支持将这些事件信息通过电子邮件和短信息的方式及时告知相关运维人员，并支持信息发布规则的灵活设置，包括设置首次前转条件、间隔前转条件、延时前转条件、升级前转条件等；

提供故障根原因分析手段，能够准确定位网络故障的根原因，能够自动压缩重复告警，记录告警的重复次数；

提供自动和手动的告警清除功能，应支持灵活设置自动清除的周期和清除时保留的告警时间窗口；

记录故障发生的现象和处理的方法，为管理人员提供故障处理经验库。当故障发生时，能够方便地查看该类故障的处理经验。

➢ 性能管理

系统应完成对 IT 基础设施和应用系统的性能管理功能，包括性能数据采集、处理、统计分析和性能门限管理等功能。具体包括：

系统应支持采用任务方式对 IT 基础设施和应用系统进行性能数据采集，性能数据应反映 IT 基础设施和应用系统的运行情况和运行质量，系统应支持对性能数据采集任务进行灵活的设置；

系统应支持对不同的性能指标进行阈值设置，提供相应的阈值管理和越限告警机制，系统应支持按照对象类型和针对具体对象两种方式设置性能门限；

性能数据趋势分析应支持性能门限提醒功能。在性能趋势分析图中，应绘制

出该对象的性能门限阈值线。

3.3.3 流程管理

系统支持服务台功能，支持配置管理、变更管理、事件管理、问题管理、发布管理、服务级别管理、知识管理、等标准流程，以及值班管理、作业计划管理、考核管理等辅助流程。

➢ 服务台

服务台是运维服务提供者与用户间的单一联系点。服务台管理事件和服务请求，实现与用户的沟通。服务台应实现以下功能：

支持通过电话、电子邮件等方式向用户提供单点联系接口；

支持用户通过服务台咨询、短信或电子邮件等方式了解投诉或服务申请的处理过程；

支持对故障和服务申请的跟踪，确保所有的故障和服务申请能够以闭环方式结束；

能够提供对知识库的查询功能。

➢ 配置管理

配置管理流程负责核实 IT 基础设施和应用系统中实施的变更以及配置项之间的关系是否已经被正确记录下来，确保配置管理数据库能够准确地反映现存配置项的实际版本状态。系统应支持以下功能：

支持对配置项的登记和管理；

支持对配置项属性的记录，如序列号、版本号、购买时间等；

支持配置项间关系的建立和维护；

支持配置项及其关系的可视化呈现；

支持对配置管理数据库访问权限的控制；

支持对配置项变更的历史审计信息的记录和查询；

支持配置项的状态管理；

支持针对配置项的统计报表；

支持与事件管理、问题管理、变更管理等其他管理流程的集成。

➢ 变更管理

变更管理实现所有 IT 基础设施和应用系统的变更，变更管理应记录并对所有要求的变更进行分类，应评估变更请求的风险、影响和业务收益。其主要目标是以对服务最小的干扰实现有益的变更。系统应支持以下功能：

创建并记录变更请求：系统应支持信息的输入，并确保只有授权的人员方可提交变更请求；

审查变更请求：系统应支持对变更请求进行预处理，过滤其中完全不切实际的、不完善的或之前已经提交或拒绝的变更请求；

变更请求的归类和划分优先级：系统应支持基于变更对服务和资源可用性的影响决定变更的类别，依据变更请求的重要程度和紧急程度进行优先级划分；

系统应支持对变更请求的全程跟踪和监控，支持在变更全程控制相关人员对变更请求的读、写、修改、访问；

系统应支持将变更请求分派到合适的授权人员；

系统应支持对变更请求的审批流程，并支持对变更请求的通知和升级处理；

系统应提供可定制的管理报表，如按类型、级别对变更进行统计和分析、变更实施的成功率、失败率等等；

支持与事件管理、问题管理、配置管理等其他管理流程的集成。

➢ 事件管理

事件管理负责记录、快速处理 IT 基础设施和应用系统中的突发事件。事件管理应支持自定义事件级别、事件分类，提供方便的事件通知功能，支持对事件进行灵活的查询统计。并可以详细记录事件处理的全过程，便于跟踪了解事件的整个处理过程。事件管理应支持以下功能：

支持事件记录的创建、修改和关闭；

支持向事件记录输入描述和解决方案信息，支持创建事件记录时自动记录创建时间、创建日期和事件流水号；

支持将事件记录自动分派到相应支持组和个人；

提供对事件记录的查询功能；

支持灵活定制相关报表，可利用历史事件记录生成管理报表；

支持与问题管理、配置管理、变更管理等其他管理流程的集成。

➢ 问题管理

问题管理流程的主要目标是预防问题和事故的再次发生，并将未能解决的事件的影响降低到最小。系统应支持以下功能：

支持问题记录的创建、修改和关闭，创建问题记录时自动记录创建时间、日期；

支持对事件、问题和已知错误的区分；

支持自动分派问题记录到定义的支持组或个人；

支持对问题记录定义严重等级和影响等级；

支持对问题记录的跟踪和监控；

支持生成可定制的管理报表；

支持向问题记录输入描述和解决方案信息；

提供对问题记录的查询功能；

支持与变更管理、配置管理、事件管理等其他管理流程的集成。

➢ 发布管理

发布管理负责对硬件、软件、文档、流程等进行规划、设计、构建、配置和测试，以便为实际运行环境提供一系列的发布组件，并负责将新的或变更的组件迁移到运行环境中。其主要目标是保证运行环境的完整性被保护以及正确的组件被发布。系统应支持以下功能：

支持发布的分发和安装；

支持与配置管理、变更管理、服务级别管理等流程的集成。

➢ 服务级别管理

服务级别管理提供运维服务管理者和运维服务供应商之间关于运维服务的提供质量的约定、检查功能，其目标在于确保所有当前的及双方协议过将要交付的运维服务的提供处于协议水平。系统应支持以下功能：

服务级别协议（SLA）模板定制功能：系统应能提供统一创建、浏览、修改和删除 SLA 模板的功能；

SLA 违例通知功能：一旦发生 SLA 违例情况，系统应及时发送通知给运维服务的相关各方；

SLA 报告生成功能：系统应支持 SLA 报告自动生成功能，并支持将生成的报告自动推送给运维服务的相关各方；

支持生成可定制的管理报表。

➢ 知识管理

知识管理流程负责搜集、分析、存储和共享知识和信息，其主要目的是通过确保提供可靠和安全的知识和信息以提高管理决策的质量。知识管理应支持以下功能：

添加知识：提供支持人员提交经验和知识输入的接口或界面，支持 Word/Excel/TXT 等格式文档作为附件的输入；

支持知识库的更新；

查询知识：提供完善的查询功能，如查询关键字、知识列表等；

提供模糊匹配、智能查询、点击统计等增强功能。

辅助流程

➢ 值班管理

系统应支持对值班的管理，应实现以下功能：

值班信息的记录：值班信息应包括班次编号、值班人、记录时间、监控项是

否正常、问题及处理等。

值班信息的查询；

值班信息的统计。

➢ 作业计划管理

系统应支持对作业计划的管理，实现以下功能：

提供基于模板的作业计划制定功能，快速完成作业计划（年计划、月计划）的制定；

对于待执行的作业计划，系统提供自动提醒功能；

对于作业计划的执行情况，系统提供统计分析功能。

➢ 考核管理

系统应支持对员工工作量、工作绩效进行考核，并对考核结果进行统计分析。

3.4 系统安全设计

集中运维管理系统需要和网络中各个关键节点进行通讯，并获取参数数据，因此其安全的设计也显得至关重要。系统通过合理的管理系统软硬件系统搭配，可以保障整个系统的安全性，在软硬件的多个层面确保 IT 运维管理平台的运行、数据和信息安全。系统的安全保障措施如下：

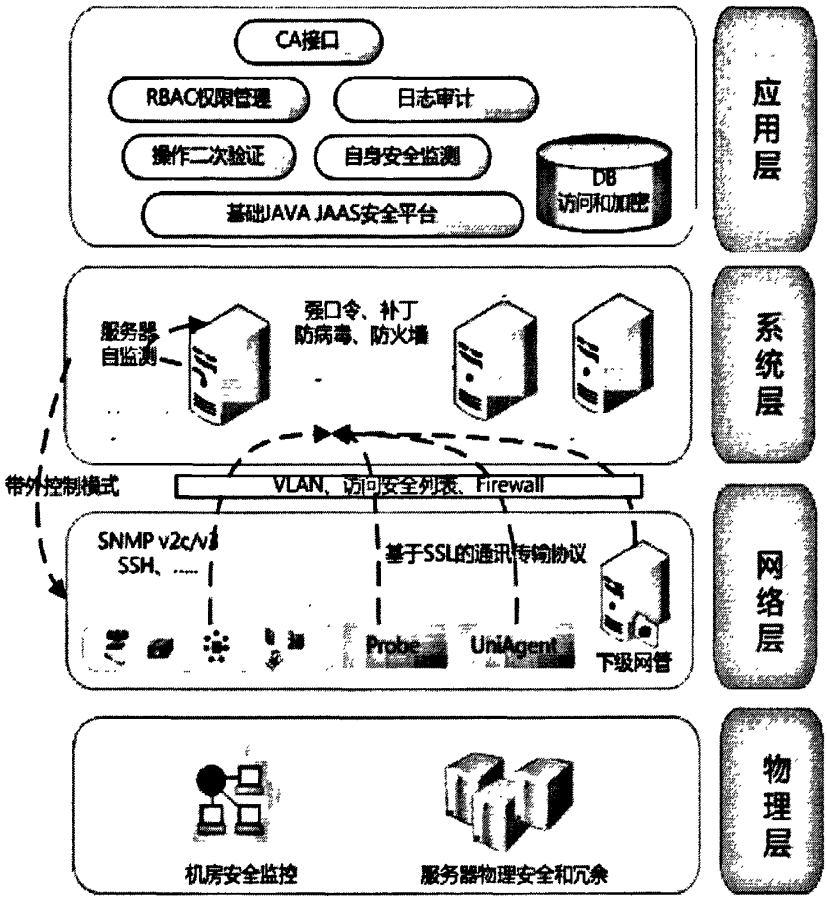

图 3-7 IT 运维管理平台安全管理示意图

如图 3-7，集中运维管理系统的安全主要体现在物理层、网络层、系统层、应用层多个方面。

3.4.1 物理层

主要针对运维管理系统各类硬件设备，要确保 IT 运维管理平台的安全运行，需要首先保障物理层的高可用性和安全性。物理层的安全性主要靠硬件设备来保障，主要建议以下措施：

IT 运维管理平台服务器部署在数据中心机房，注重数据中心机房的安全措施，通过机房定期人工例行检查和 IT 环境监控系统，确保 IT 运维管理平台服务器所在环境的安全；

将相关服务器存储纳入 San 存储，提高存储的可管理性和安全性。

3.4.2 网络层

主要针对运维管理系统和被管理各类网元之间的通讯可靠性和安全性，系统主要有以下措施来保证：

管理 VLAN 的划分和控制：将管理服务器划分到管理 VLAN 中，通过管理 VLAN 访问策略的设置，提高网络访问的安全性，从网络层防止其他 PC 直接向网管发起攻击；

系统采用单一的数据传输接口，包括系统数据交换，Agent 采集、探针管理等。

通过防火墙来保障和屏蔽运维管理系统服务器，仅仅打开系统所需的相关采集通讯和数据汇总端口；

通过统一认证和登录服务器来控制信息部门人员对资源的管理和操作，并通过登录服务器的审计日志来确保事后跟踪和追查；

运维管理系统在采集传输和数据传递中采用加密的方式，系统内部的数据信息在网络上传递时，均采用基于 SSL 的数据加密通道，确保数据的安全性，当系统进行远程采集的时候，也会采用加密访问模式，比如：主机设备的 root 口令等信息不会在网上通过 Telnet 明文传输，而是通过 SSH 远程访问 UNIX 服务器，采集各类运行指标。

3.4.3 系统层

主要针对运维管理系统所在的服务器系统，主要是针对服务器操作系统的安全运行，主要包括：

运维管理系统服务器操作系统的口令需要设置为强口令，避免弱口令造成安全隐患；服务器的补丁需要及时更新，安装防病毒软件和防火墙，服务器需要关闭不需要的服务，避免造成安全隐患；

通过统一认证和登录服务器来控制信息部门人员对资源的管理和操作，并通过登录服务器的审计日志来确保事后跟踪和追查；

通过运维管理系统对服务器的资源、进程、日志信息进行监控，确保 IT 运维管理平台系统的宿主-网管服务器操作系统的安全运行。

3.4.4 应用层

应用层的安全管理主要由运维管理系统软件进行保障，主要包括：

运维管理系统系统主体架构在 JAVA 平台基础上，JAVA 平台提供了企业级的安全特性，同时系统做了 JAVA 平台级的 JAAS 安全策略加固，具有较好防病毒、防入侵、防攻击功能，整体系统平台具有良好的安全基础。通过各种 JAVA 平台安全策略，确保系统平台的整体访问控制安全。

例如：对限制部分系统模块对网络的读写访问策略如下：

```
grant codeBase "file:${coss.home}/lib /arbitercore.jar /-" {
permission java.net.SocketPermission "ipaddress:8877", "connect";
};
```

运维管理系统数据大多保存在管理数据库中，系统可以监测 Oracle 管理数据库的访问安全，对数据库会话和 SQL 等操作进行监控，确保没有非法的数据访问和导出；

运维管理系统的管理信息库，对保存的部分敏感数据还要进行加密处理，例如访问的帐号和口令等，以保护数据的安全，以防非法进入或摄取；

统一管理信息库提供了事务原子化隔绝，确保事务完整性，系统对信息库的访问密码进行本地加密，同时提供数据备份、归档机制。

系统对关键的修改操作，需要再此输入用户密码进行；

建立完善的用户权限管理功能，采用 RBAC 的权限管理模式，并通过用户权限的分立，确保系统的相互制约和安全性；

系统支持和 CA 系统的登录结合，在密码保护的基础上进一步稳固管理员的访问安全，系统的 WEB 监控管理支持 HTTPS 方式；

系统提供完善的日志审计功能，预设专门的审计角色，对系统的登录日志、运行日志、操作日志等均保持记录和归档，确保日后追查和跟踪取证。

第四章　运维管理系统部署方案

4.1 系统部署方案

根据石景山区电子政务的网络规模、业务管理需求，我们采用了集中部署方式，整体部署方案结构如下图：

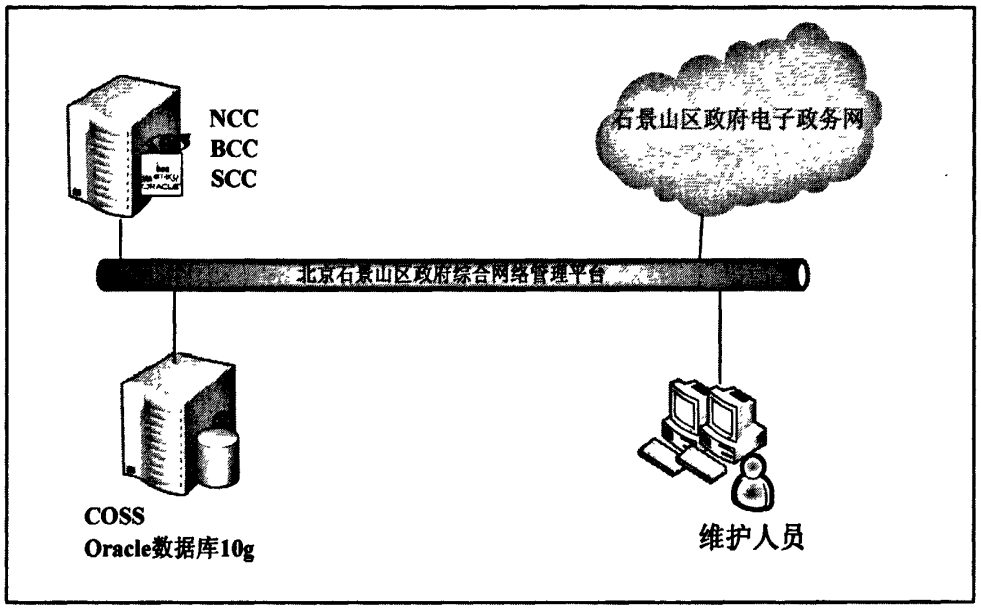

图 4-1 部署逻辑图

整体部署方案采用集中式部署，由于初期数据量较小，故将前台应用和数据库安装在统一服务器。为便于和各监控节点通信，并保证安全性的要求，将此服务器部署在网管 VLAN 中。

4.1.1 软件配置方案

类别	名称	数量
操作系统	WIN2003 简体中文标准版	1 套
数据库	Oracle 10g	1 套
应用软件	集中运维管理软件	1 套

4.1.2 硬件配置建议方案

服务器	2.0GHz CPU* 2, 4 GB RAM, 146GB*3,Raid 5，	1台

4.2 角色设置和权限分配

4.2.1 基于角色的权限管理模型

建立安全高效的权限管理模型是软件系统中一个重要的环节。目前国内外研究了几种权限管理模型：基于对象的权限管理模型，基于层次的权限管理模型，基于规则的权限管理模型和基于角色的权限管理模型。总结前面三种模型，它们共同的缺点，首先是权限操作复杂，授权方式不够灵活，不能处理日益膨胀的数据信息，特别是对一些大型的结构性数据的权限管理力量薄弱；其次，在网络技术快速发展的今天，使数据不再集中在某一个地方，而上述的这些权限模型对分布式的数据安全管理束手无策。而基于角色的权限管理模型很好地解决了前面几种模型的缺点，本节将详细地论述基于角色的权限管理模型。

基于角色权限管理模型是在用户和权限之间设置了一个新的实体即角色，角色作为中间媒介把用户集合和权限集合联系起来，用户通过角色间接地访问系统资源。一个角色与权限关联可以看作是该角色拥有一组权限的集合，与用户关联又可以看作是若干具有相同身份的用户的集合。在基于角色的权限管理模型中，一个用户可以被赋予多个角色，一个角色也可以被赋予多个用户，用户和角色之间是多对多的关系。同样，一个角色也可以具有多项权限，一项权限也可以被赋予多个角色，权限和角色之间也是多对多的关系。一个登陆到系统中的用户，可以通过所拥有角色的权限来判断允许访问的数据库资源和系统资源，这是基于角色的权限管理模型的基本原理。

4.2.2 石景山区电子政务系统集中运维平台的角色设置以及权限分配

石景山区信息网络中心主要承担电子政务运维的具体工作，并将运维工作分散在各个业务部门，在进行运维平台的角色设置的时候我们结合了实际的组织架构在 ITIL 的基础上进行了调整。

由于该运维平台是基于 ITIL 的思想设计，因此初始的角色设置完全是按照 ITIL 中定义的角色来设计的。在实施过程中，根据石景山区的实际运维情况，我

们将角色进行了简化。在奥运期间为了全力做好基础保障工作，临时成立了奥运信息安全指挥中心承担了主要的运维工作，根据这个情况分配了以下几个角色：

- 超级管理员

权限模块：用户管理、监测组管理、监测配置管理、报表管理

用户：管理员

- 资产管理员

权限模块：合同管理、资产管理

用户：办公室人员

- 服务台人员

权限模块：事件管理

（工单查看、工单添加、完成工单、分发工单、回退工单、添加申告、工单监控、工单修改）；

用户：值班员

- 一线支持人员

权限模块：事件管理（工单查看、工单添加、完成工单、分发工单、回退工单、工单处理）、运行监测、统计分析

用户：指挥中心人员

- 二线支持人员

权限模块：事件管理（工单查看、工单添加、完成工单、回退工单、工单处理）、运行监测、统计分析

用户：各部门其他人员

- 事件经理

权限模块：事件管理（工单查看、工单添加、完成工单、分发工单、回退工单、工单处理）、运行监测、统计分析

用户：分管领导

奥运信息安全保障期过后，运维工作恢复常态，由各部门分散承担运维工作，我们对角色进行了调整。主要变动是由各部门负责人承担一线支持人员的工作，各部门其他人员承担二线支持人员的工作。同时，将事件经理的角色赋予各部门负责人。

4.3 系统功能展示

本部分结合使用的实际情况将系统的部分功能做一个展示。

4.3.1 统一监控展现

集中运维管理平台针对网络、操作系统、数据库、安全产品等相关监控界面进行了整合，并在同一个系统中统一展现，解决了以往监控界面分散的问题。

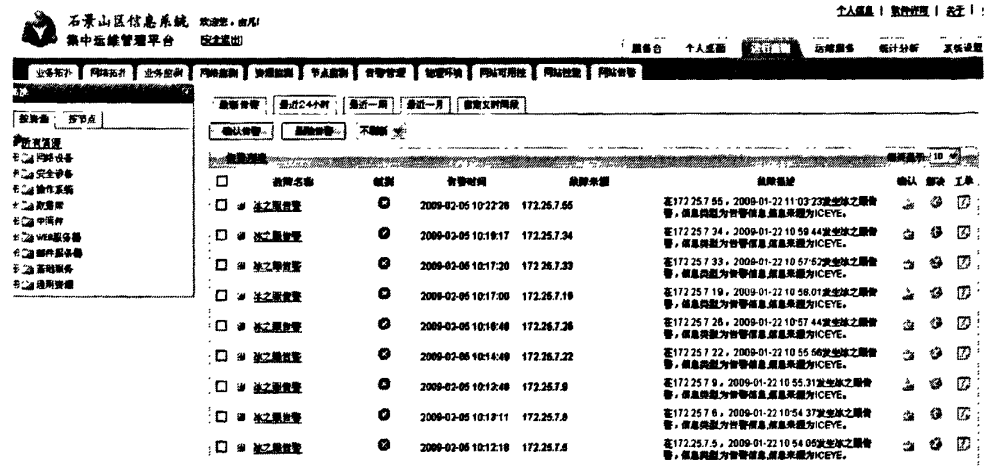

图 4-2 告警管理

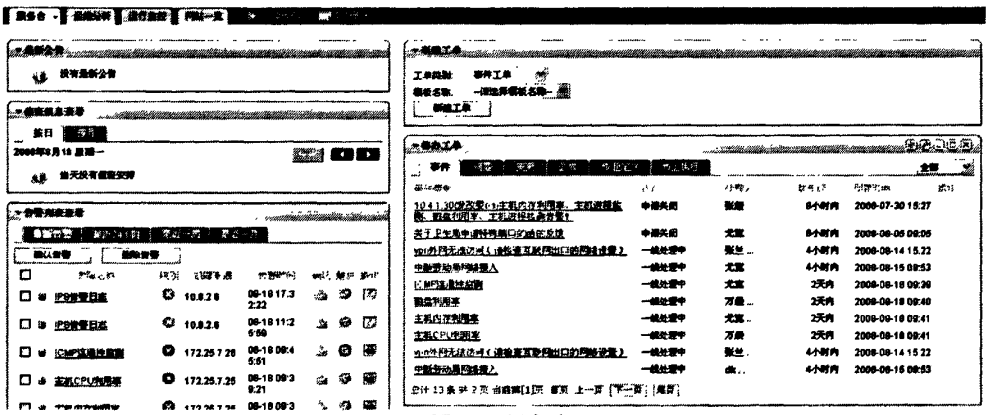

图 4-3 服务台

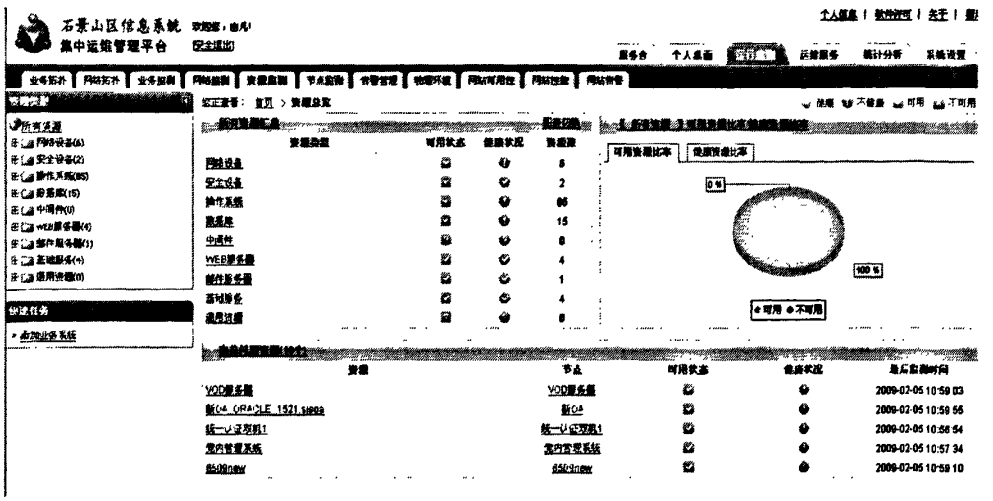

图 4-4 资源监控

4.3.2 事件工单处理

事件工单处理是运维管理流程中比较重要的内容。任何工作人员都可以发起事件工单；一线工作人员按照事件工单的分类主动处理，并将处理过程和结果记录下来；如果一线工作人员不能处理，可以将工单转至二线，由二线工作人员进行处理；工单处理完毕后由事件经理进行审核并关闭工单。

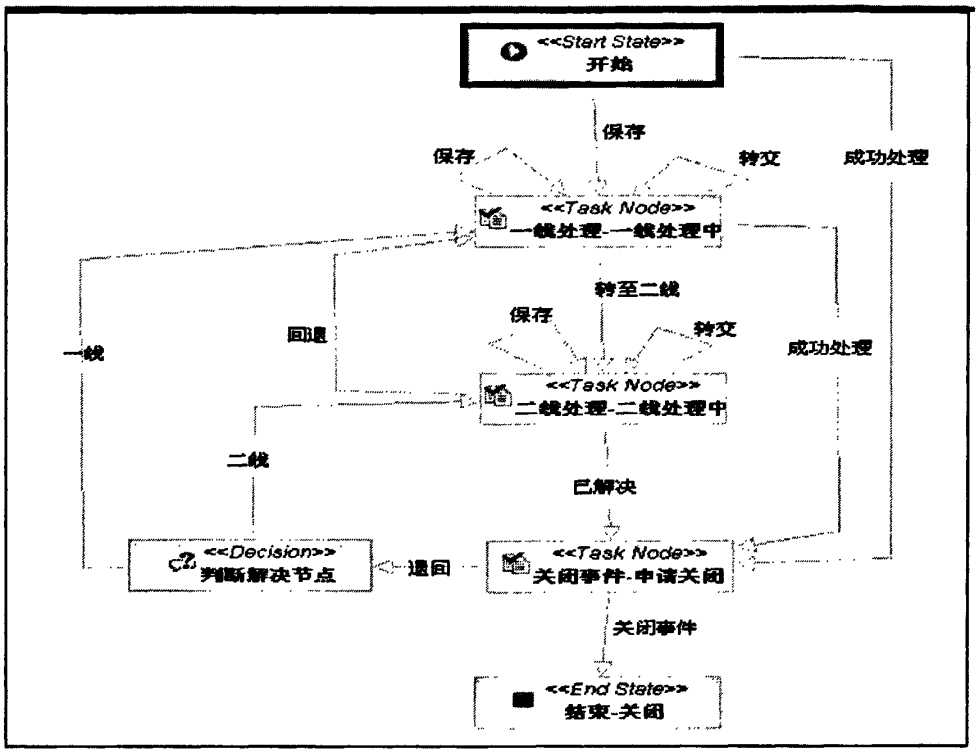

图 4-5 事件工单处理流程图

第五章 成果总结

5.1 建设成果

目前，电子政务运维模式包含自运维、完全外包运维和混合运维三种模式，石景山区采用混合运维模式，由信息化运维部门和外包单位共同提供运维服务，这种模式下的运维环境如图 5-1。

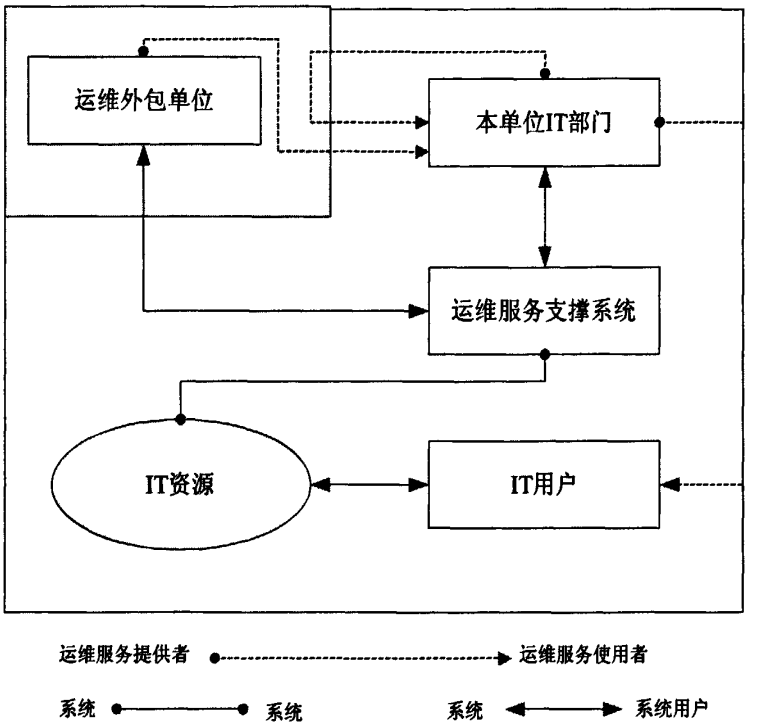

图 5-1 混合运维环境

2008 年 7 月 20 日，石景山区电子政务集中运维管理系统上线试运行，初步监控对象包含服务器 85 台、路由交换设备 234 台、数据库 16 套、web 服务 4 个，基本覆盖了核心网络所有设备和应用。同时，根据实际情况设置了服务器运维、网络运维、应用系统服务、PC 服务、网络安全运维、数据库运维、备份运维、网站运维和物理环境运维等 9 大类服务类别，初步形成了运维的工作机制的扭转，取得了较好的应用效果。

5.1.1 功能实现情况

石景山区电子政务集中运维管理系统的基于 ITIL 理念，包括了服务支持和服务提供的核心内容。同时，石景山区电子政务集中运维管理系统也覆盖了《北京市电子政务运维服务支撑系统规范》中功能需求的 80%以上的内容，具体情况见表 5-1。

资产管理	静态资产管理	85%	基本满足静态资产管理功能，包括支持资产信息手工录入、增加删除资产信息、能够进行表格和图形展现，支持模糊查找，能够根据不同类型展现设备，支持将查找到的资产信息保存成标准格式文件，支持查询结果打印。支持部分生命周期管理功能，可以根据不同部门、不同业务系统进行统计资产信息，统计结果可以保存为图表、趋线图等，并可以将统计结果导出保存为 EXCEL 等格式，可以将资产信息进行分析，提供多种第三方接口，包括数据库、web services 等接口。
	动态资产管理	10%	支持手工更新资产信息。
监控管理	视图管理	100%	支持网络拓扑图、机架导航图、设备面板图等图形展现方式，并且可以自定义视图。系统支持拓扑视图与故障的关联、性能关联，支持将视图导出为图片格式。
	配置管理	90%	支持方便的静态资源手工录入，支持资源信息的更新、同步。支持可视化的监控，支持配置信息下发和配置文件管理，报表结果可以通过曲线图、饼状图进行展现。

	故障管理	100%	支持告警信息采集、处理、显示、清除和故障定位等功能，提供故障知识库功能。能够完成不同监测颗粒度的需要。支持告警的过滤、升级和压缩。可以通过列表、视图、颜色等方式将用户关心的告警信息呈现给运维人员，支持电子邮件和短信的告警方式。
	性能管理	90%	支持性能数据采集、处理、性能分析等功能，支持通过阀值进行性能报警，支持性能趋势分析。
全管理	通信及操作管理	90%	支持审计日志、管理员和操作者日志、错误日志等日志功能，并提供对日志信息的保护、分析和呈现。
	访问控制	40%	支持对应用系统和信息的访问控制，进行统一集中的身份认证、授权
	信息安全事件管理	70%	系统应能发现并报告信息安全事件，并对安全事件做出响应。
	风险评估和等级保护	0%	不能满足
程管理	服务台	100%	支持通过电话、网络、电子邮件等方式向用户提供单点联系接口，支持对所有的故障和服务申请进行预处理，检查用户输入信息的正确性和完整性，支持用户通过服务台咨询、短信或电子邮件等方式了解投诉或服务申请的处理过程，支持对故障和服务申请的跟踪，确保所有的故障和服务申请能够以闭环方式结束，能够提供对知识库的查询功能
	配置管理	100%	支持对配置项的登记和管理，支持对配置项属性的记录，如序列号、版本号、购买时间等，支持配置项间关系的建立和维护，支持配置项及其关系的可视化呈现，支持对配置管理数据库访问权限的控制，支持对配置项变更的历史审计信息的记录和查询，支

			记录和查询，支持配置项的状态管理，支持针对配置项的统计报表，- 支持与事件管理、问题管理、变更管理等其他管理流程的集成。
	变更管理	100%	支持信息的输入，并确保只有授权的人员方可提交变更请求；支持对变更请求进行预处理，过滤其中完全不切实际的、不完善的或之前已经提交或拒绝的变更请求；变更请求的归类和划分优先级：系统应支持基于变更对服务和资源可用性的影响决定变更的类别，依据变更请求的重要程度和紧急程度进行优先级划分；支持对变更请求的全程跟踪和监控，支持在变更全程控制相关人员对变更请求的读、写、修改、访问；支持将变更请求分派到合适的授权人员；支持对变更请求的审批流程，并支持对变更请求的通知和升级处理；提供可定制的管理报表，如按类型、级别对变更进行统计和分析、变更实施的成功率、失败率等等；支持与事件管理、问题管理、配置管理等其他管理流程的集成
	事件管理	100%	支持事件记录的创建、修改和关闭；支持向事件记录输入描述和解决方案信息，支持创建事件记录时自动记录创建时间、创建日期和事件流水号；支持将事件记录自动分派到相应支持组和个人；提供对事件记录的查询功能；支持灵活定制相关报表，可利用历史事件记录生成管理报表；支持与问题管理、配置管理、变更管理等其他管理流程的集成

	问题管理	100%	支持问题记录的创建、修改和关闭，创建问题记录时自动记录创建时间、日期；支持对事件、问题和已知错误的区分；支持自动分派问题记录到定义的支持组或个人；支持对问题记录定义严重等级和影响等级；支持对问题记录的跟踪和监控；支持生成可定制的管理报表；支持向问题记录输入描述和解决方案信息；提供对问题记录的查询功能；支持与变更管理、配置管理、事件管理等其他管理流程的集成
	发布管理	100%	支持发布的分发和安装；支持与配置管理、变更管理、服务级别管理等流程的集成
	服务级别管理	100%	服务级别协议（SLA）模板定制功能：系统应能提供统一创建、浏览、修改和删除 SLA 模板的功能；SLA 违例通知功能：一旦发生 SLA 违例情况，系统应及时发送通知给运维服务的相关各方；SLA 报告生成功能：系统应支持 SLA 报告自动生成功能，并支持将生成的报告自动推送给运维服务的相关各方；支持生成可定制的管理报表
	知识管理	100%	添加知识：提供支持人员提交经验和知识输入的接口或界面，支持 Word/Excel/TXT 等格式文档作为附件的输入；支持知识库的更新；查询知识：提供完善的查询功能，如查询关键字、知识列表等；提供模糊匹配、智能查询、点击统计等增强功能
	财务管理	0%	
	供应商管理	50%	可在资产管理功能钟添加供应商信息
	辅助流程管理	60%	支持值班流程管理，并支持多种表单

			自定义流程。支持日常作业管理。
综合管理	统计分析	80%	支持统计分析功能。
	决策支持	10%	支持人机交换方式自定义流程
外包管理	结果控制管理	70%	支持基于服务级别协议中规定的内容定制并提交服务质量报告
	过程控制管理	70%	支持对工作量和绩效进行查询
系统支撑管理	用户管理	100%	添加用户、删除用户、修改用户基本信息、修改用户所属部门，并支持按照部门或管理分工设置用户归属的角色。
	权限管理	100%	支持按管理功能和管理范围进行用户权限分配
	日志管理	100%	支持日志记录、查询、日志备份等功能
	自身管理	100%	支持自身软、硬件监控管理。
运维服务支撑系统结构	各类支撑系统的功能结构	90%	支持 SNMP、码流、xFlow、sysLog、WMI、Web Service 等多种接口协议，支持各管理功能的业务逻辑，持 C/S 模式、B/S 模式，支持用户功能权限、用户登录日志和系统操作日志的管理；实现构成系统的各软件模块进程、数据库、计算机设备等的监控和管理；实现数据备份等功能，支持外部接口功能。
	系统部署	100%	支持单级或多级系统部署
运维服务支撑系统技术指标要求	系统容量	100%	保证支撑系统软件可支持的图形终端应不少于 50 个，可支持并发操作的用户数应不少于 10 个
	系统可靠性	100%	系统的退出和异常停止，不影响其管理的 IT 基础设施和应用系统。系统的年可用率大于 99.9%

实时性	100%	支撑系统的告警最长响应时间，不超过 10 秒。在网络告警风暴情况下，该响应时间不超过 30 秒。简单操作及普通数据查询操作界面响应时间小于 2 秒，大数据量报表数据查询操作界面响应时间小于 15 秒。网络设备运行正常情况下，支撑系统的性能数据处理时延小于性能数据设置的采集周期。
系统存储能力	100%	告警数据、性能数据在系统中存储 1 个月；资源数据在系统中存储 6 个月；经系统处理后的报表数据、分析数据在系统中存储 12 个月；经用户设定为重要的数据（如与分析预测相关的数据）长期保存。经系统处理后的数据可在磁带机或磁盘中长期保存（大于 2 年）
系统安全性	100%	支持灵活的用户权限分配，能够满足自运维、部分外包、全部外包等运维模式下各种角色不同权限的安全需求
系统扩展性	100%	支持多种操作系统平台，包括主流的 UNIX、Windows 和 Linux 等，支持单级和多级部署方式，采用分布式结构、模块化设计，能够支持通过增加硬件设备来提高系统的管理容量，具有平滑的扩展能力，能够方便地接入新厂家、新类型的 IT 资源。
系统易用性	100%	用户界面应简洁、友好，操作简单，提示清晰，提供系统操作在线帮助。用户界面显示应采用简体中文。 系统支持用多种方式来呈现各类管理信息。对于统计信息，具有表格或直观图形化（如直方图、曲线图、饼图等）输出方式
系统可维护性要求	100%	系统提供对自身运行情况的维护和管理，包括系统软硬件运行状态监控、系统数据库备份和还原等

表 5-1 功能完成表

5.1.2 促进运维机制的形成

通过集中运维管理系统的建设过程，使得大家的思想理念得到了进一步更新，运维工作在整个信息化工作中得到了更高的重视。同时，对于运维的组织机构以及工作流程方面我们都做了相应的探讨和尝试，在学习国外先进经验和结合工作实际的基础上初步形成以系统管理部为核心的运维管理组织机构，为下一步运维工作的完善和深层次开展打下了很好的基础。

5.1.3 掌握基础数据

通过运维管理系统的监控数据，使得 IT 基础运维数据得到了掌握，并具有很高的实效性。在系统产生数据的基础上我们定期出具总结分析报告，对于目前存在的问题和发展的趋势进行研究，为下一步的完善提高工作提供可靠依据。

例如，我们通过对主机监控数据的分析，发现目前大部分（约占 95％）服务器的计算资源利用率一般在 0.1%-10%之间。然而部分负荷重的服务器（仅占 5%左右）资源利用率达到了 80%，具体数据如表 5-2 所示：

服务器类别	CPU 利用率	内存利用率	备注
A 类（占 5%）	>10%	>60%	
B 类（占 50％）	1%-3%	<40%	
C 类（占 45％）	<1%	<10%	

注：A 类：运行负荷很重；B 类：运行负荷正常；C 类：运行负荷较轻

表 5-2 主机性能利用统计表

从以上服务器和存储的利用情况来看，由于大部分的应用采用了独立的服务器，各服务器的计算资源无法共享，导致一些业务运行资源紧张的同时另一些计算能力充足的应用服务器资源无法被共享利用，计算资源紧张的应用还需要再进行独立扩展，造成了主机设备资源的极大浪费。

在掌握了这个情况后，我们对资源的利用问题开始了调研研究，通过系统整合和主机整合来充分利用基础资源，同时减少运维的复杂度。

5.1.4 提高运维服务

运维工作流程的建立，大大提高了事件处理的效率和质量，避免小事件不及时处理升级成大问题。同时，系统提供的运维统计分析功能对工单的数量和处理

的效率为运维工作的考核打下了基础。

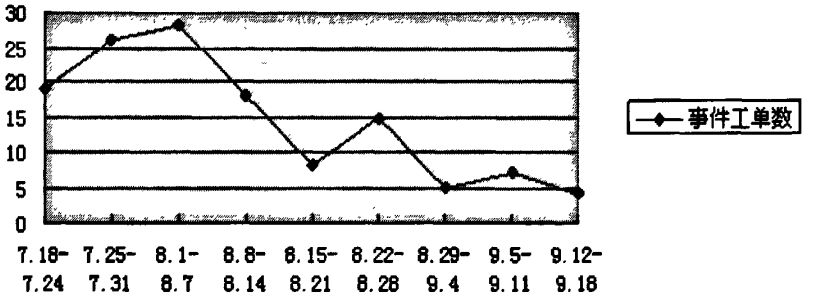

图 5-2 事件工单趋势图

图 5-2 显示了从 7 月 18 日到 9 月 18 日为止每周产生的工单数，从趋势图来看，事件工单从开始的每周 20 多个逐步减少到每周 10 个以内。这个数据可以显示出工作效率和质量的提高大大促进了 IT 服务的质量。

5.2 存在的问题

通过借助对集中运维管理系统的使用，我们的运维水平和服务质量都有了很大的提高，但同时还存在着一些问题。

5.2.1 流程的适用性还需要进一步加强

在 ITIL 标准中对于事件管理、问题管理等各部分内容都有一定的标准流程，但是在实际应用中我们发现这种标准的流程对于呼叫中心等中大型专业运维队伍比较适合，而在电子政务的运维过程中实施有一定的困难。例如，在事件管理流程中涉及服务台、事件经理、一线技术人员、二线技术人员等角色，但是在政府部门大多是按照部门分工分散运维，是不可能有这么完整并且集中的组织机构。在实际应用过程中，我们一方面逐步来优化我们的运维团队组织机构，一方面对标准流程进行修改，让流程既符合我们的实际情况，又具有一定的科学性。图 5-3 和图 5-4 分别显示了 ITIL 标准中以及实际应用中的事件管理流程。

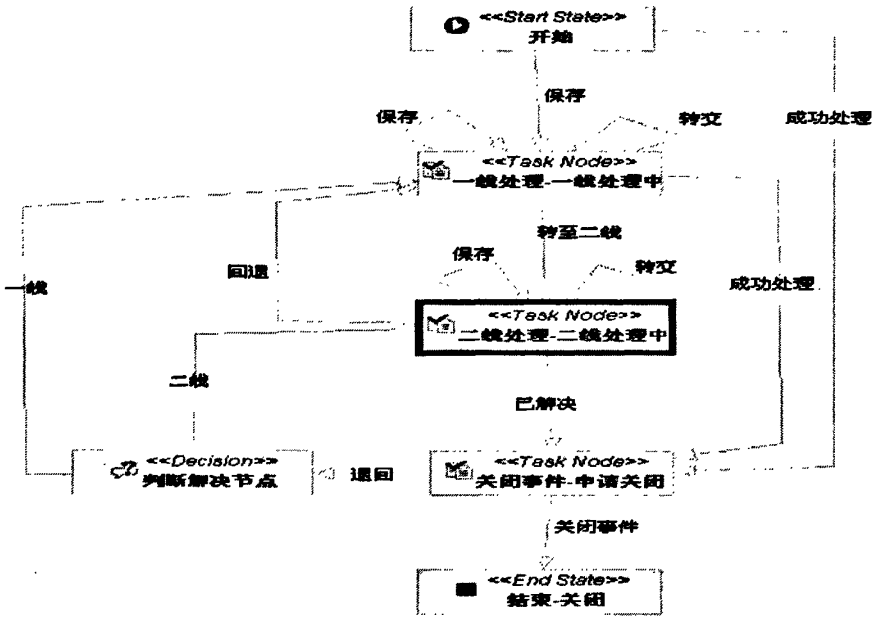

图 5-3 ITIL 标准中事件管理流程

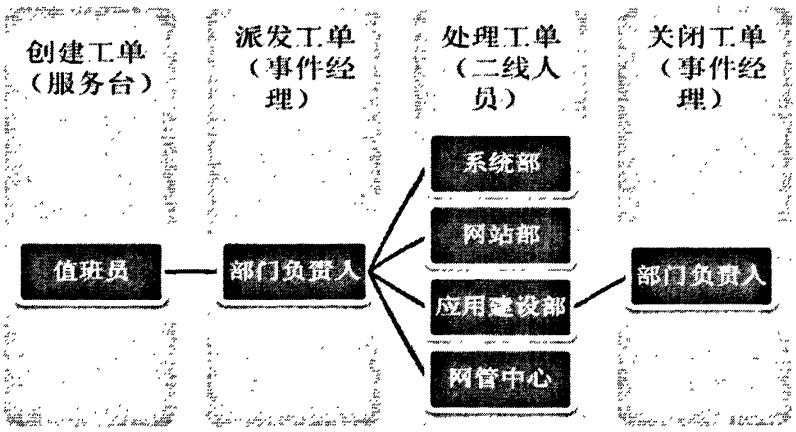

图 5-4 实际形成的事件管理流程

为了更好地和实际情况接轨，在二期的建设中流程部分增加了定制的功能，用户可以根据自身的情况去定制具体的操作流程，这就大大增强了系统的灵活性。

5.2.2 IT 服务财务管理存在着较大的困难

大部分人都将 IT 服务视为支持组织日常业务活动的一个重要贡献因素，然而却很少有人意识到这些服务是需要花费成本的，特别是在政府部门，往往忽视了对于绩效的考虑。ITIL 中提到的 IT 服务财务管理的目的就是要构建对 IT 基础设施的管理，从而促进高效和经济地使用 IT 资源。电子政务的财务管理相对于传统的财务管理在分类、计算等方面都有其特殊的地方。目前，关于电子政务系统的财务管理没有统一的标准，北京市经信委也正在和市财政局探讨相关的标准和管

理办法。

5.2.3 对于运维外包服务商的管理

由于石景山区电子政务系统运维采用的是混合模式，其中一部分运维内容由外包服务商来完成，怎么利用集中运维管理系统将他们的运维工作有机地整合到整个运维体系中来，其中的流程和标准等都有待进一步讨论。

5.3 个人收获

通过参与本次课题的研究，本人在理论基础、专业知识及撰写论文等方面的能力都有了很大的提高，主要有以下几点：

- 通过学习ITIL等国际标准以及市级规范文档的学习对于IT运维的工作有了系统的学习。目前，我主要负责本单位的运维体系的建立工作，这对于科学建立运维体系有很大的帮助。
- 通过参与对软件系统体系架构以及功能的设计进一步巩固了软件工程中涉及的对于软件工程管理的相关内容，尤其是加深了对软件设计建模内容的理解。
- 通过对软件技术实现的了解，学习了目前比较流行的一些技术，在专业技术上有了提高。
- 通过撰写论文，从论文的架构、格式、思路等方面提高了写作意识和写作能力，对于今后工作中的调研报告以及论文的撰写有很好的促进。

第六章 结束语

石景山区电子政务系统集中运维平台一期建设已经告一段落，此项目的实施完成了项目初期的目标，为石景山区电子政务系统现代化运维奠定了一个良好的开始。目前该系统将我区电子政务系统运维中物理环境监控、安全入侵监控、服务器系统监控、数据库系统监控等10多项内容的信息加以整合和集中展现，并通过工单的形式将故障事件按照既定的工作流进行处理，在奥运期间大大提高了我们的运维水平和工作效率。但是，该系统在功能上和性能上还有地方需要改进，我们也正在做进一步的需求调研，对其进行完善和修改。

在下一步的工作中，我们将以信息资产为核心，以其健康运行为目标，进一步加强平台中对监测数据的统计和分析，增强其趋势预测的内容。同时，按照信息系统的生命周期，我们还将逐步融入信息系统建设期间的部分信息，提高我们的运维服务水平。

集中运维平台的建设将是电子政务系统甚至IT服务管理的一种趋势，它不仅仅是一个信息化手段的体现，更是大家对于运维理念的一个变革。在未来我们可以看到，集中运维平台将融合价值交付、资源管理、风险管理、绩效管理等内容，服务于电子政务系统的效率、效果、规范这一相同的目标。

参考文献

[1].Jan van Bon 主编，章斌翻译 基于 ITIL 的 IT 服务管理基础篇，清华大学出版社，2007 年 8 月第 1 版.

[2]. Jan van Bon 主编，章斌翻译 基于 ITIL 的全球最佳实践，清华大学出版社，2006 年 1 月第 1 版.

[3]. 左天祖 主编，中国 IT 服务管理指南，北京大学出版社，2004 年 3 月第 1 版.

[4].Duane Merrill， Mashups：Web 应用程序新成员，2006 年 8 月 31 日 developerworks 中国.

[5].中国电子政务运维管理现状与发展趋势研究报告， ITGov 中国 IT 治理研究中心，2008 年 11 月.

[6].北京市电子政务运维服务支撑系统规范（1.0 版），北京市信息化工作办公室，2008 年 12 月.

附录：图表索引

图 2-1 ITIL 整体架构 13
图 3-1 电子政务运维体系 31
图 3-2 体系结构图 32
图 3-3 统一数据接口逻辑结构图 33
图 3-4 资源管理信息库模型 36
图 3-5 采集数据库模型 38
图 3-6 基于工单的 ITIL 工作流引擎 41
图 3-7 IT 运维管理平台安全管理示意图 49
图 4-1 部署逻辑图 52
图 4-2 告警管理 55
图 4-3 服务台 55
图 4-4 资源监控 55
图 4-5 事件工单处理流程图 56
图 5-1 混合运维环境 57
图 5-2 事件工单趋势图 65
图 5-3 ITIL 标准中事件管理流程 66
图 5-4 实际形成的事件管理流程 66

表 3-1 告警事件严重等级对应表 34
表 3-2 告警事件分类对应表 34
表 3-3 告警事件属性表 35
表 3-4 资源关系表 37
表 5-1 功能完成表 63
表 5-2 主机性能利用统计表 64

致　谢

此篇论文凝结了我在工作中的探索和学习中的总结，也蕴涵着我的老师、同事、亲人和朋友的帮助和支持。

在此，首先感谢我的导师马严教授。马严教授作为我的导师，在自己教学和科研任务繁重的情况下，特意抽出时间，认真审阅我的论文，给予了我很多非常重要的启发和引导，也给了我很多战略指导性的帮助。

同时感谢我的领导，给了我这个机会负责该项目的组织实施，并在工作遇到困难的时候给予了大力的支持。感谢我的同事，在项目的调研以及实施过程中和我一起加班加点进行研究，并在实施过程中克服困难，才保证项目在计划的时间内完成了所有工作，并取得了显著的效果。在系统使用过程中各部门同事提出了很多宝贵的改进意见，使得我们的系统得以进一步完善，并为第二期建设提供了很多参考意见。

感谢我们项目的合作伙伴广通信达公司，他们在技术实现上投入了很多人力和精力，协助我们进行工作的开展。并在运维工作这方面提供了很多技术资料，对我们进行了多次培训，使得我们的水平有了很大的提高。

再次感谢所有帮助过我的老师、同事、家人和朋友！

攻读学位期间发表的学术论文目录

[1].IPv4,走过历史的脚步，第一作者，网管员世界，第 96 页，2008 年 9 月

[2].信息安全风险评估方法的研究，第一作者，软件导刊，第 164 页，2008 年 12 月