

北京市电子政务 IT运维服务支撑系统规范

第二部分 IT运维服务支撑系统技术要求 (V1.0)

北京信息化协会

二〇〇八年十月

目录

1	总则	1
2	参考标准	1
3	术语、定义和缩略语	1
3.1	术语和定义	1
3.1.1	IT运维服务	1
3.1.2	IT运维服务支撑系统	1
3.2	缩略语	2
4	IT 运维服务涉及的管理对象	2
5	IT 运维服务管理和支撑能力要求	3
5.1	IT运维服务管理和支撑能力分类	3
5.2	IT运维服务管理和支撑能力等级划分	4
5.3	IT运维服务管理和支撑能力组合	7
6	IT 运维服务支撑系统功能需求	8
6.1	资产管理	8
6.1.1	静态资产信息管理	9
6.1.2	动态资产信息管理	10
6.2	监控管理	10
6.2.1	视图管理	10
6.2.2	配置管理	11
6.2.3	故障管理	11
6.2.4	性能管理	12
6.3	安全管理	12
6.3.1	通信及操作管理	13
6.3.2	访问控制	13
6.3.3	信息安全事件管理	13
6.3.4	风险评估和等级保护	13
6.4	流程管理	13
6.4.1	服务台	14
6.4.2	配置管理	14
6.4.3	变更管理	15
6.4.4	事件管理	15
6.4.5	问题管理	16
6.4.6	发布管理	16
6.4.7	服务级别管理	17
6.4.8	知识管理	17
6.4.9	财务管理	17
6.4.10	供应商管理	18
6.4.11	辅助流程	18
6.5	综合管理	19

6.5.1	统计分析	19
6.5.2	决策支持	20
6.6	外包管理	20
6.6.1	结果控制管理	20
6.6.2	过程控制管理	20
7	IT 运维服务支撑系统结构	20
7.1	各类支撑系统的功能结构	21
7.2	系统部署	24
8	IT 运维服务支撑系统技术指标要求	27
8.1	系统容量	27
8.2	系统可靠性	27
8.3	实时性	27
8.4	系统存储能力	28
8.5	系统安全性	28
8.6	系统扩展性	28
8.7	系统易用性	29
8.8	系统可维护性要求	29
9	IT 运维服务支撑系统管理接口要求	29

前言

本部分是北京市电子政务 IT 运维服务支撑系统系列规范的第二部分，本系列规范目前包括：

- (1)第一部分 IT 运维服务支撑系统应用需求；
- (2)第二部分 IT 运维服务支撑系统技术要求；
- (3)第三部分 IT 运维服务支撑系统测试方法。

本部分参照国际标准化组织和国家相关标准，并结合北京市电子政务 IT 运维的实际情况而制定。

本部分由北京信息化协会提出并归口。

1 总则

本部分规定了 IT 运维服务涉及的管理对象和所需的管理支撑能力，以及支撑 IT 运维服务的系统应该具备的管理功能、系统结构、技术指标和相关接口等技术要求。

本部分适用于 IT 运维服务支撑系统的规划、设计和实现。

2 参考标准

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

- (1) ISO/IEC 20000-1:2005 信息技术—服务管理—第 1 部分：规范
- (2) ISO/IEC 20000-2:2005 信息技术—服务管理—第 2 部分：实施指南
- (3) ISO/IEC 27001:2005 信息技术 安全技术 信息安全管理体系要求
- (4) GB/T XXXX (200X) 信息安全技术 信息系统安全等级保护定级指南
- (5) GB/T XXXX (200X) 信息安全技术 信息系统安全等级保护基本要求
- (6) GB/T XXXX (200X) 信息安全技术 信息系统安全等级保护实施指南

(7) 北京市信息化工作办公室 北京市电子政务 IT 运维服务支撑系统规范 第一部分 IT 运维服务支撑系统应用需求 :2008

3 术语、定义和缩略语

3.1 术语和定义

3.1.1 IT 运维服务

参见本系列规范的第一部分。

3.1.2 IT 运维服务支撑系统

参见本系列规范的第一部分。

3.2 缩略语

ISO	International Organization for Standardization	国际标准化组织
IT	Information Technology	信息技术
OA	Office Automation	办公自动化
SLA	Service Level Agreement	服务级别协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SMI	Structure of Management Information	管理信息结构
WMI	Windows Management Instrumentation	视窗管理规范

4 IT 运维服务涉及的管理对象

IT运维服务涉及的管理对象包括 IT基础设施、基于 IT基础设施之上运行的 IT应用系统、使用各类 IT 应用系统的 IT用户、供应商以及 IT运维服务管理涉及到的相关人员，管理对象的分类和详细内容如表 1 所示。

表 1 IT运维服务涉及的管理对象

管理对象类别	管理对象
IT基础设施	网络类：交换机、路由器、通信链路、其他网络设备组件、网络软件等； 主机系统类：小型机、服务器、主机系统设备组件、主机系统软件、数据库系统、中间件等； 存储、备份系统类：存储设备、备份设备、备份软件等； 终端系统类：台式机、笔记本、打印机、扫描仪、其他办公设备、终端设备系统软件和应用软件等； 安全系统类：安全设备、安全管理软件等； 机房环境类：机房专用精密空调、机房专用不间断电源、机房环境设备组件等。
IT应用系统	OA及内部办公系统； 政府网站； 电子政务核心应用：面向企业和组织的应用系统、面向公众的应用系统、城市管理类应用系统。
IT用户	单位内部用户； 单位外部用户。
IT供应商	包括 IT基础设施供应商、IT应用系统供应商、IT运维服务供应商等。

IT 运维部门和人员	IT运维部门和人员； IT运维管理部门和人员； IT运维服务供应商和人员。
------------	---

5 IT 运维服务管理和支撑能力要求

5.1 IT运维服务管理和支撑能力分类

IT运维服务管理和支撑能力体现在 6 个维度，他们分别是：资产管理能力、监控管理能力、安全管理能力、流程管理能力、综合管理能力以及外包管理能力，如图 1所示。

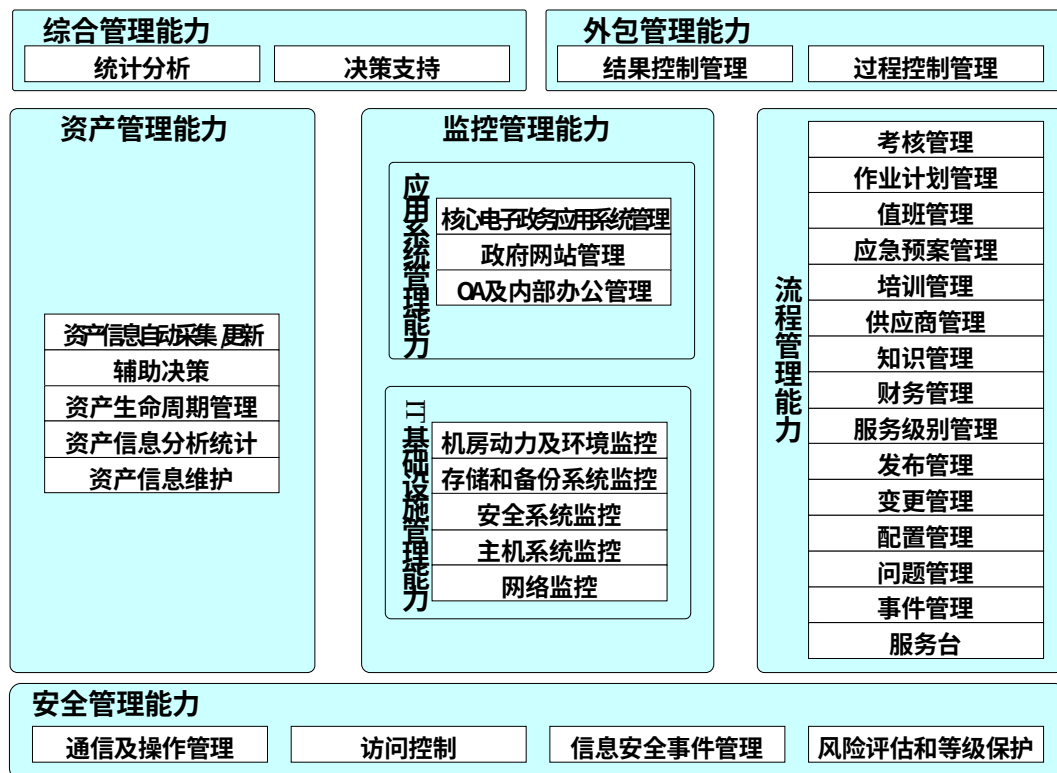


图 1 IT运维服务管理和支撑能力

其中，资产管理能力支持对各类 IT基础设施和应用系统的类型、归属、费用、使用情况等资产相关信息的维护和统计工作，实现 IT资产生命周期管理，支持对 IT资源投资和维护的辅助决策。

监控管理能力支持对 IT基础设施和应用系统的监控，对资源进行直观呈现和调度、对告警进行实时处理、对故障进行预警，具体能力包括视图管理、配置管理、故障管理和性能管理等。

安全管理能力支持通过权限控制、访问和操作日志、通信和操作管理等方法，实现信息安全事件管理、风险评估和等级保护。

流程管理能力支持采用各类电子化手段将 IT 运维服务支撑系统、IT 运维部门和人员、IT 用户等角色有机联系在一起，保证整个 IT 运维活动规范、有序、闭环地执行。流程管理包括服务台能力以及配置管理、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、财务管理、供应商管理、值班管理、作业计划管理、考核管理、应急预案管理和培训管理等各管理流程。

综合管理能力支持在资产管理、监控管理、安全管理、流程管理和外包管理等能力的基础上，实现 IT 整体运维信息统计分析，并对管理决策提供支持。

外包管理能力对外包 IT 运维服务的质量、效果和过程实施控制。

5.2 IT 运维服务管理和支撑能力等级划分

5.1 节规定了 IT 运维服务单位或者部门可以具备的 IT 运维服务管理和支撑能力的全集，在本单位或者部门运维服务管理和支撑能力的实际提升过程中，根据不同阶段所具备的运维服务管理和支撑能力的不同，可以在 6 个维度上分别评估或界定其达到的运维服务管理和支撑能力成熟度等级。

结合北京市各政务部门的实际情况，建议分别对其具备的资产管理、监控管理、安全管理、流程管理、综合管理、外包管理等 IT 运维服务管理和支撑能力按照如下等级进行划分：

(1) 资产管理能力成熟度等级划分

在覆盖所有 IT 资产管理信息的前提下，依据所实现的 IT 资产管理能力的不同，资产管理能力成熟度划分为 2 个等级，具体如表 2 所示。

表 2 资产管理能力等级划分

等级分类	等级 1	等级 2
支撑能力		
静态资产信息管理	√	√
动态资产信息管理		√

各等级具备的能力和提升方式如下：

等级 1，实现静态资产信息的维护、资产信息的分析统计、资产生命周期管

理并支持辅助决策；

等级 2，在等级 1 的基础上实现资产信息的自动采集和更新。

(2) 监控管理能力成熟度等级划分

依据监控管理的主动性和实时性程度的不同，监控管理能力成熟度划分为 2 个等级，具体如表 3 所示。

表 3 监控管理能力等级划分

等级分类 \ 支撑能力	等级 1	等级 2
被动监控、定期巡检	√	√
主动监控、实时监视		√

各等级具备的能力和提升方式如下：

等级 1，实现基于事件触发的 IT 基础设施和应用系统的监控，对 IT 资源进行定期巡检；

等级 2，借助监控工具实施对 IT 基础设施和应用系统的实时、主动监控。

(3) 安全管理能力成熟度等级划分

依据安全管理内容范围的不同，安全管理能力成熟度划分为 2 个等级，具体如表 4 所示。

表 4 安全管理能力等级划分

等级分类 \ 支撑能力	等级 1	等级 2
人员、资产安全管理	√	√
网络、系统行为安全管理		√

各等级具备的能力和提升方式如下：

等级 1，实现人员和资产的安全管理，包括对环境、介质、资产、备份 / 恢复等安全制度的建立和执行；

等级 2，在等级 1 的基础上，实现网络和系统行为的安全管理，包括信息系统的安全防护，安全状态监控、分析和报告，安全事件管理等。

(4) 流程管理能力成熟度等级划分

依据流程管理的规范化程度以及信息化支持程度的不同，流程管理能力成熟度划分为 2 个等级，具体如表 5 所示。

表 5 流程管理能力等级划分

等级分类 \ 支撑能力	等级 1	等级 2
流程规范化	√	√
流程信息化		√

各等级具备的能力和提升方式如下：

等级 1：基于规范的流程开展 IT 运维活动，但流程尚未信息化；

等级 2：可以通过信息化手段对 IT 运维的业务流程提供支持。

(5) 综合管理能力成熟度等级划分

依据其实现的综合管理能力范围的不同，综合管理能力成熟度划分为 2 个等级，具体如表 6 所示。

表 6 综合管理能力等级划分

等级分类 \ 支撑能力	等级 1	等级 2
统计分析	√	√
决策支持		√

各等级具备的能力和提升方式如下：

等级 1：实现统计分析能力；

等级 2：在等级 1 的基础上实现决策支持的能力。

(6) 外包管理能力成熟度等级划分

依据对服务外包控制程度的不同，外包管理能力成熟度划分为 2 个等级，具体如表 7 所示。

各等级具备的能力和提升方式如下：

等级 1：实现对外包服务质量和效果的控制；

等级 2：在等级 1 的基础上实现对外包服务提供过程的控制。

表 7 外包管理能力等级划分

等级分类	等级 1	等级 2
管理能力		
结果控制管理	√	√
过程控制管理		√

5.3 IT运维服务管理和支撑能力组合

对于本单位 IT运维服务管理和支撑能力的评价，可以通过对 5.2节中定义的 6个维度的不同等级进行界定。不同维度、不同等级的 IT运维服务管理和支撑能力可以灵活组合以适应不同政务部门的不同应用场景。表 8 列出了 IT运维的几种典型的场景，以及在这些场景下，相应的 IT运维服务管理和支撑能力的组合：

(1)场景 1具备静态资产信息管理能力，对 IT资源实施被动监控和定期巡检，实现对人员和资产的安全管理，基于规范的流程开展 IT运维活动，但流程尚未信息化，具备统计分析的能力；

(2)场景 2具备静态资产信息管理能力，对 IT资源实施被动监控和定期巡检，实现对人员和资产的安全管理，基于规范的流程开展 IT运维活动，但流程尚未信息化，具备统计分析的能力，可实现对外包的结果控制管理；

(3)场景 3具备静态资产信息管理能力，对 IT资源实施被动监控和定期巡检，实现对人员和资产的安全管理，可通过信息化手段对 IT运维的业务流程提供支持，具备统计分析的能力，并可实现对外包的结果控制管理；

(4)场景 4具备静态资产信息管理能力，对 IT资源实施被动监控和定期巡检，实现对人员和资产的安全管理，可通过信息化手段对 IT运维的业务流程提供支持，具备统计分析和决策支持的能力，可实现对外包的结果和过程控制管理；

(5)场景 5具备静态和动态资产信息管理能力，对 IT资源实施主动监控和实时监视，实现对人员和资产的安全管理，以及对网络和系统行为的安全管理，可通过信息化手段对 IT运维的业务流程提供支持，具备统计分析和决策支持的能力，可实现对服务外包的结果和过程的控制管理。

在其管理和支撑能力提升过程中，各政务部门可从上述五个场景中选取之

一作为其基线场景，并可根据实际需求，在该基线场景的基础上增、减相应的能力。此外，除了上述典型场景对应的能力组合方式外，各政务部门也可根据实际需求灵活采取其他组合方式。

表 8 IT 运维的典型场景和相应的能力组合

IT 运维的典型场景 管理和支撑能力		场景 1	场景 2	场景 3	场景 4	场景 5
资产管理	静态资产信息管理	√	√	√	√	√
	动态资产信息管理					√
监控管理	被动监控、定期巡检	√	√	√	√	√
	主动监控、实时监视					√
安全管理	人员、资产安全管理	√	√	√	√	√
	网络、系统行为安全管理					√
流程管理	流程规范化	√	√	√	√	√
	流程信息化			√	√	√
综合管理	统计分析	√	√	√	√	√
	决策支持				√	√
外包管理	结果控制管理		√	√	√	√
	过程控制管理				√	√

6 IT 运维服务支撑系统功能需求

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

6.1 资产管理

资产管理功能应实现对网络设备、服务器、PC、打印机、各种配件（显示器、显卡、网卡、硬盘）、软件、备品备件等 IT 资产信息的维护、统计以及资产生命周期管理。根据资产信息获取方式的不同，资产管理可划分为静态资产信息管理和动态资产信息管理。

6.1.1 静态资产信息管理

6.1.1.1 资产信息维护

系统应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。功能要求如下：

- 资产信息获取与更新：系统应支持多种形式的导入；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：系统应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；
- 资产信息导出与打印：系统应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。

6.1.1.2 资产信息分析统计

系统应实现 IT 资产信息的统计分析功能，具体包括：

- 系统应支持 IT 资产信息的统计分析，并以表格、饼图、直方图或趋势线等方式进行显示，并提供保存和打印功能；
- 系统应实现各类 IT 资产的利用率计算功能，以反映资产的使用情况，辅助用户合理使用资产；应实现基于资产生命周期状态的统计功能；
- 系统应支持将资产信息的分析统计结果向信息化管理部门和财务部门汇总和同步。

6.1.1.3 资产生命周期管理

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

6.1.1.4 辅助决策

系统应能对资产信息进行分析和计算，分析和计算的结果可作为辅助决策

的依据，包括：

- 系统应具有预警功能，如资产过保修期预警、资产报废预警等；
- 系统应支持基于规则的运维费用的计算，运维费用包括资产维护费用和相关的维护人员费用，应支持计算规则的灵活调整。

6.1.2 动态资产信息管理

动态资产信息管理在静态资产信息管理的基础上应支持资产信息的自动发现和采集，资产信息的自动同步和更新。

6.2 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。

6.2.1 视图管理

系统应以图形方式呈现 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；
- 机房平面图：提供机房内设备物理摆放位置的视图；
- 机架视图：提供设备在机架上物理摆放位置的视图；
- 设备面板图：对被管理的设备应以与设备同样的物理构成直观进行显示。对不同类型的设备应该提供模版，方便设备面板图的维护，设备面板图应同时可以显示正面面板和背面面板；
- 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。

系统应支持把视图导出为 Visio 格式和图片格式的文件。

6.2.2 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；
- 可视化监控：系统应支持提供直观的可视化管理功能，通过形象的展现方式直观展现设备工作情况；
- 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。

6.2.3 故障管理

系统应完成对 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：

- 系统应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；
- 系统应支持告警的过滤、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；
- 系统应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；

- 系统应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；
- 系统应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；
- 系统应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；
- 系统应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。

6.2.4 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；
- 性能数据可保存到数据库中，实现统计、分析和比较功能，统计、分析和比较的结果应支持图形呈现，应能生成性能趋势曲线；系统应支持同时选中多个对象，在同一坐标系中进行性能趋势对比，对比曲线应支持直接存为图片；
- 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。

6.3 安全管理

系统的安全管理功能对应于可以通过信息化手段实现的安全管理支撑能

力，安全管理应包括但不限于通信及操作管理、访问控制、信息安全事件管理以及风险评估和等级保护。在具体实施中应依据信息安全管理体系和信息系统安全等级保护的相关国家标准。安全管理功能应与流程管理中的事件管理和问题管理相关联。

6.3.1 通信及操作管理

系统应支持防范恶意代码和移动代码；支持依据既定的备份策略对信息和软件进行备份并定期测试；应能对网络进行充分的管理和控制，以防范威胁、保持使用网络的系统、应用程序和信息传输的安全；系统应支持对可移动媒体的管理；支持对通过物理媒体、电子消息以及业务信息系统交换的信息进行安全控制；系统应具有审计日志、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。

6.3.2 访问控制

系统应支持对网络访问的控制，包括远程用户的鉴别、网络设备识别、诊断和配置端口的物理和逻辑访问控制、网内隔离、网络连接控制和网络路由控制等；系统应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、授权和审计；系统应支持移动计算和远程工作管理。

6.3.3 信息安全事件管理

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；系统应能跟踪、记录安全事件及其处理过程；系统应支持对安全事件的统计分析，能够量化安全事件的类型、数量、成本，并支持统计分析结果的输出。

6.3.4 风险评估和等级保护

系统支持安全风险的评估以及评估结果的上报，支持依据评估结果生成相应的等级保护方案，等级保护的方案应可映射到环境、资产、设备、网络、系统等安全系统运维的各个方面，系统应支持等级保护方案的上报。

6.4 流程管理

系统应支持服务台功能，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、财务管理、供应商管理等标准流程，以及值班管理、作业计划管理、考核管理、应急预案管理、培训管理等辅助流程。

6.4.1 服务台

服务台是 IT 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、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。

6.4.2 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。

6.4.3 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。

6.4.4 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。

6.4.5 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。

6.4.6 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。

6.4.7 服务级别管理

服务级别管理提供 IT 部门和 IT 运维服务供应商之间关于 IT 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 IT 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 IT 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 IT 运维服务的相关各方；
- 支持生成可定制的管理报表。

6.4.8 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。

6.4.9 财务管理

财务管理完成预算编制、审核、批复和下发等功能，实现对费用支出的管理，实时监管每一笔费用的支出，并对超出预算或异常的费用及时给出预警提示，实现从预算到使用，再到考核的闭环管理。财务管理应提供如下功能：

- 费用预算制定；
- 费用申请管理；

- 费用执行管理；
- 费用考核管理。

6.4.10 供应商管理

供应商管理流程管理供应商及其所提供的服务，系统应支持以下功能：

- 供应商信息的录入、查询、增删、分类等；
- 对供应商进行定期评估，并支持对评估结果的查看；
- 对合同信息的录入、查询、增删、分类等；
- 对合同执行情况的定期评价和统计汇总。

6.4.11 辅助流程

6.4.11.1 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。

6.4.11.2 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。

6.4.11.3 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，应实现以下功能：

- 支持对工作任务、工时和工作完成情况等信息的收集；
- 综合工作任务类别、工时和任务完成情况对员工的工作量和工作绩效进行量化；
- 对任务类别、工时、任务完成情况、工作量等信息进行分析统计，如分析工时、工作量、工作任务的分布和比例等。

6.4.11.4 应急预案管理

系统应支持针对重大故障和灾难的应急预案的管理，应实现以下功能：

- 支持应急预案的制定、审批、更新、批准执行等流程；
- 支持应急预案的输入、修改、删除、查询；
- 支持应急预案操作人员的权限控制；
- 支持应急预案执行报告的发布。

6.4.11.5 培训管理

系统应支持培训管理，应实现以下功能：

- 提供基于模板的培训计划制定功能，帮助用户完成培训计划的制定；
- 对于待执行的培训计划，系统提供自动提醒功能；
- 对于已实施的培训，系统支持培训效果的测评和分析，以及分析结果的发布。

6.5 综合管理

系统应在资产管理、监控管理、安全管理、流程管理和外包管理功能的基础上，实现 IT 整体运维信息统计分析，并支持管理决策。

6.5.1 统计分析

系统应能在收集到的各种事件信息和配置信息的基础上进行综合分析，帮助运维人员进行故障问题的定位。同时，系统应支持在各类管理信息的基础上建立综合分析指标，来反映 IT 环境的总体运行趋势。

系统应支持通过界面、邮件和短信等多种方式发布分析结果。对分析结果

发布的规则可以灵活设置,能够为 IT 运维的不同角色提供不同界面和分析结果。

6.5.2 决策支持

决策支持应该包括数据、模型、推理和人机交互四个部分。系统应支持管理者就 IT 运维相关的人员、费用以及资源配置等管理关注的方面制定决策目标,通过建立、维护并运行决策模型,利用综合资产、监控、安全、流程以及外包管理的特征数据,借助知识推理功能,以人机交互方式进行半结构化或非结构化决策。

6.6 外包管理

系统的外包管理功能应面向政务部门的 IT 管理者,实现对外包的 IT 运维服务的结果控制管理和过程控制管理。

6.6.1 结果控制管理

结果控制管理应支持对外包 IT 运维服务质量和效果的控制。具体包括：

- 系统应支持对服务级别协议的查询；
- 系统应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；
- 系统应支持服务级别违例报告。

6.6.2 过程控制管理

过程控制管理应实现对 IT 运维服务提供过程的控制。具体包括：

- 系统应支持查询外包运维工作的详细情况,如事件和问题处理情况、变更执行情况等；
- 系统应支持服务级别违例相关的服务质量恢复和处理情况的查询和报告；
- 系统应支持对外包单位和外包运维人员的工作量和绩效进行查询、统计和定期报告。

7 IT 运维服务支撑系统结构

与 5.3 中可以灵活组合的 IT 运维服务管理和支撑能力相对应,支持能力信

息化实现的 IT 运维服务支撑系统功能也可灵活组合，构成不同应用场景下的各类 IT 运维服务支撑系统。来自多厂商的各类 IT 运维服务支撑系统及功能模块应能方便集成。

7.1 各类支撑系统的功能结构

IT 运维服务支撑系统的功能结构可划分为采集层、应用层、表示层、以及系统支撑管理和外部接口 5 个部分。功能结构的各个组成部分简述如下：

采集层：实现对资产、配置、告警、性能及安全信息的采集。系统应支持 SNMP、码流、xFlow、sysLog、WMI 等多种接口协议。

应用层：实现各管理功能的业务逻辑，对应于第 4 章所规定的功能需求，包括资产管理、监控管理、安全管理、流程管理、综合管理和外包管理。

表示层：实现系统用户使用系统功能时的人机交互界面，系统应支持 C/S 模式、B/S 模式，并具备仿真终端功能。

支撑管理功能：实现支撑系统各类用户信息、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。

外部接口功能：实现分级的 IT 运维服务支撑系统间以及 IT 运维服务支撑系统与其他信息化系统的互联。

实现不同 IT 运维服务支撑功能的多个模块应可灵活组合为满足北京市政务部门需要的 IT 运维服务支撑系统，与 5.3 中几种典型场景下的能力组合相对应的 IT 运维服务支撑系统功能结构如下。

在场景 1 下，支撑系统应具备静态资产管理功能和统计分析功能，其对应的支撑系统功能结构如图 2

在场景 2 下，支撑系统应具备静态资产信息管理功能，统计分析功能，外包服务的结果控制管理功能，其对应的支撑系统功能结构如图 3

在场景 3 下，系统应具备静态资产信息管理功能，流程管理功能，统计分析功能，外包服务的结果控制管理功能。其对应的支撑系统功能结构如图 4

在场景 4 下，支撑系统应具备静态资产信息管理功能，流程管理功能，综

合管理功能和外包服务的结果控制和过程控制管理功能。其对应的支撑系统功能结构如图 5

在场景 5 下，支撑系统应具备资产管理功能、监控管理功能、安全管理功能、流程管理功能、综合管理功能和外包管理功能。其对应的支撑系统功能结构如图 6

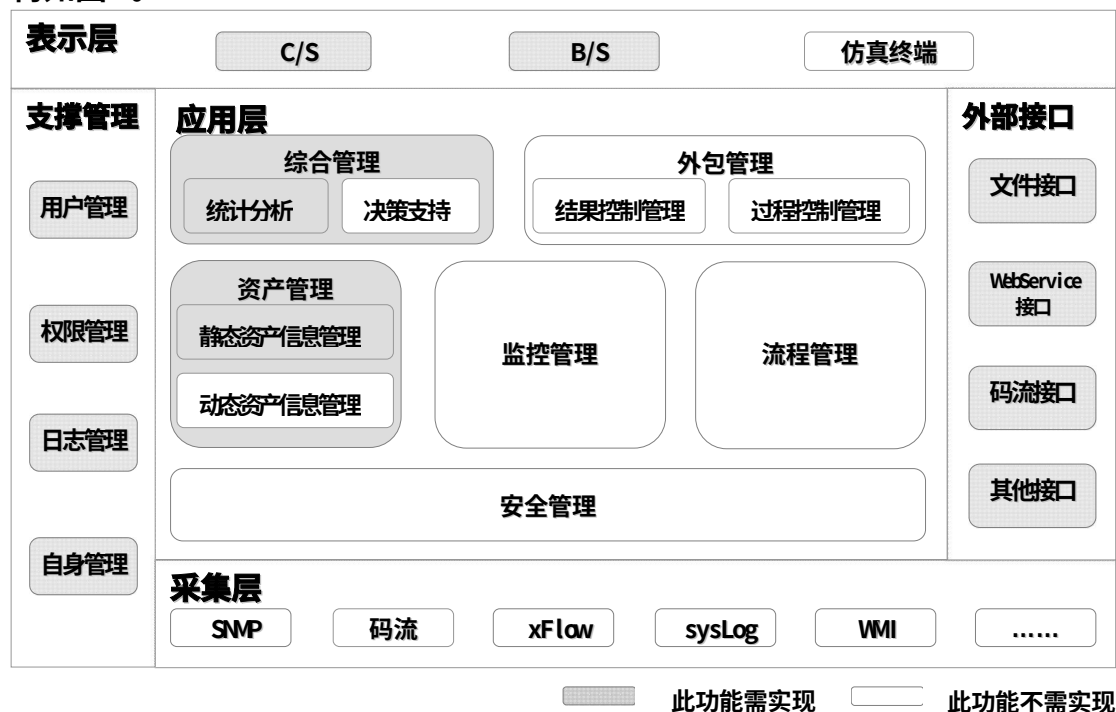


图 2 场景 1 对应的支撑系统功能结构

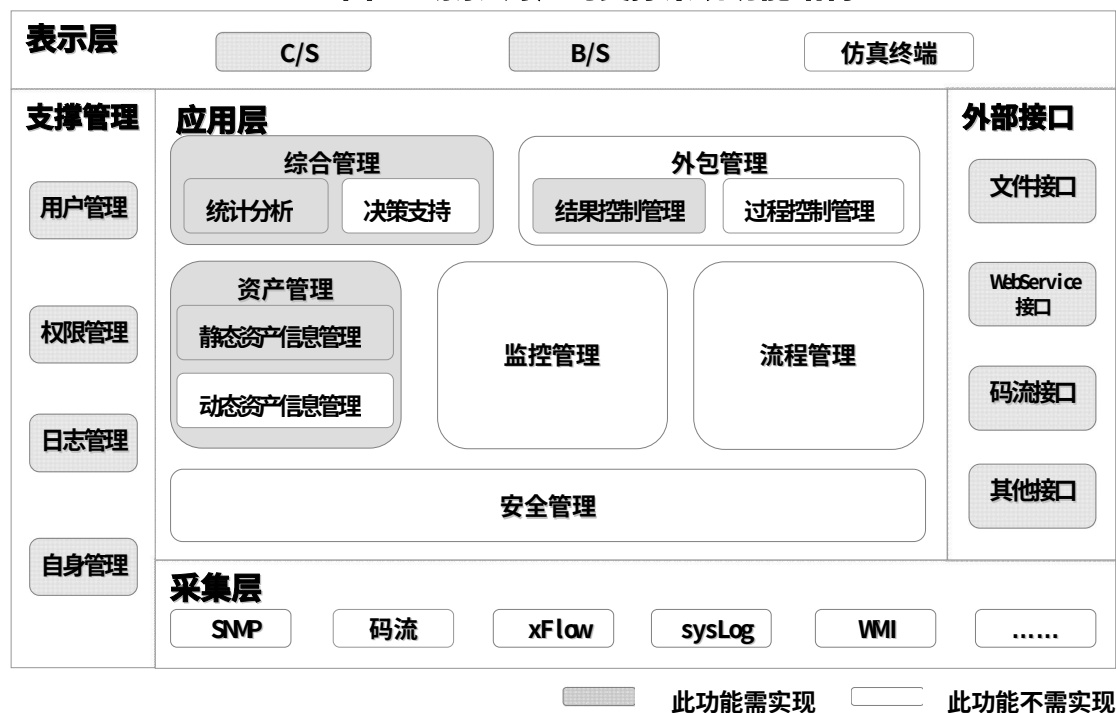


图 3 场景 2 对应的支撑系统功能结构



图 4 场景 3 对应的支撑系统功能结构

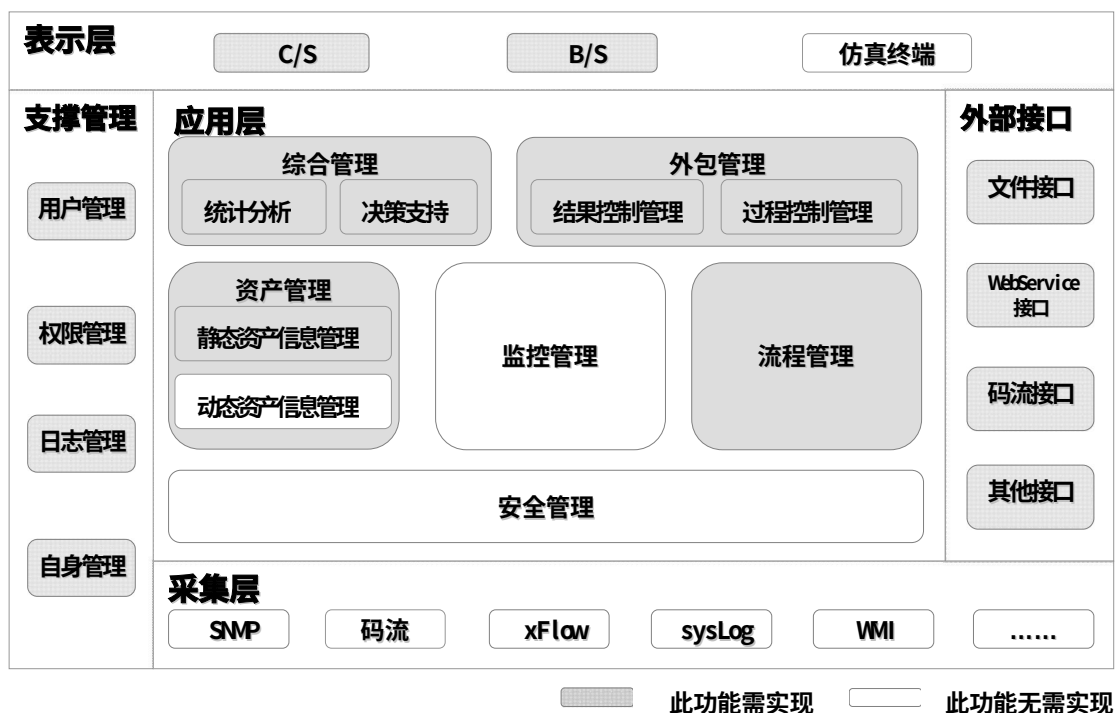


图 5 场景 4 对应的支撑系统功能结构



图 6 场景 5 对应的支撑系统功能结构

7.2 系统部署

IT 运维服务支撑系统应具有灵活的部署能力，根据被管 IT 网络的规模，IT 服务支撑系统可以采用单级系统或者多级系统。

单级系统：网络规模不大的情况下，可设置单级系统。根据系统可靠性要求、系统可扩展性要求以及数据存储和备份要求等因素，系统的各软件模块应可部署在一台或多台服务器上。为满足不同级别的管理需求，可在单级系统上部署多级用户。

多级系统：在网络规模较大的情况下，可设置多级系统。根据系统可靠性要求、系统可扩展性要求以及数据存储和备份要求等因素，每一级系统的各软件模块应可部署在一台或多台服务器上。为满足不同级别的管理需求，也可在某一级系统上部署多级用户。

图 7 为几种典型的系统部署示意图，在实际部署中可根据需要灵活选择和组合。其中，图 7a 为集中部署的单级系统，图 7b 为分布部署的单级系统，且支持多级用户的接入；图 7c 为二级系统，一级系统为分布部署，两个二级系统中一个为集中部署，另一个为分布部署。

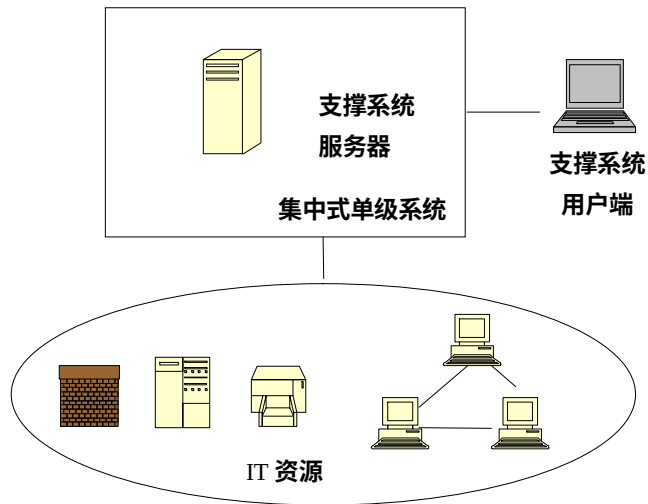
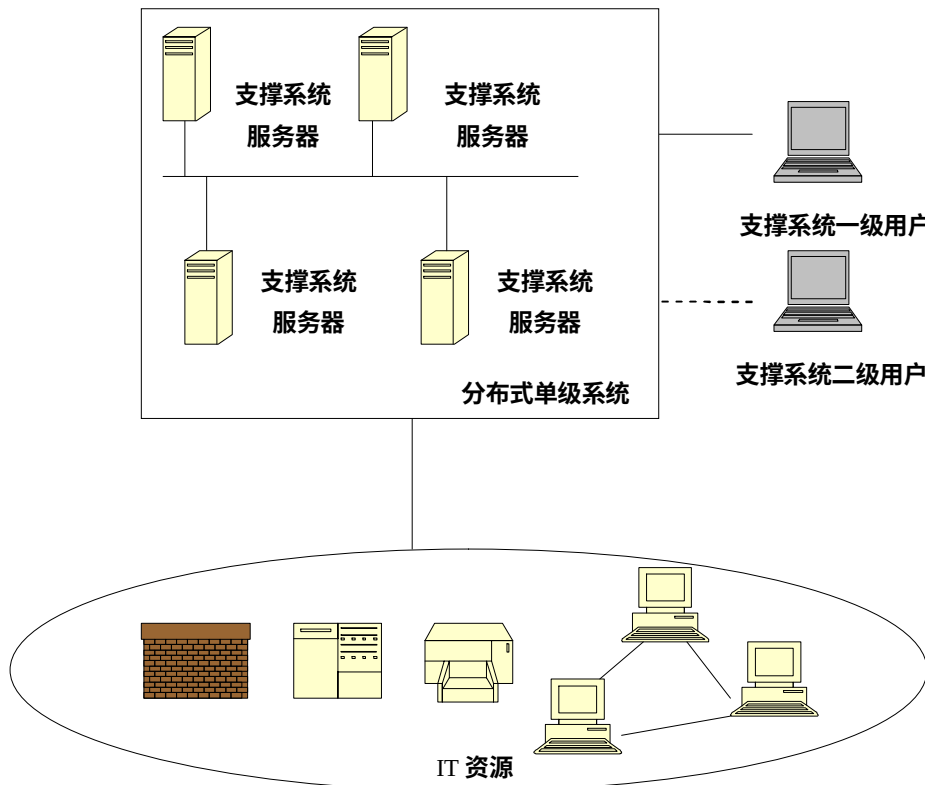


图 7a 集中式单级系统



7b 分布式多级用户单级系统

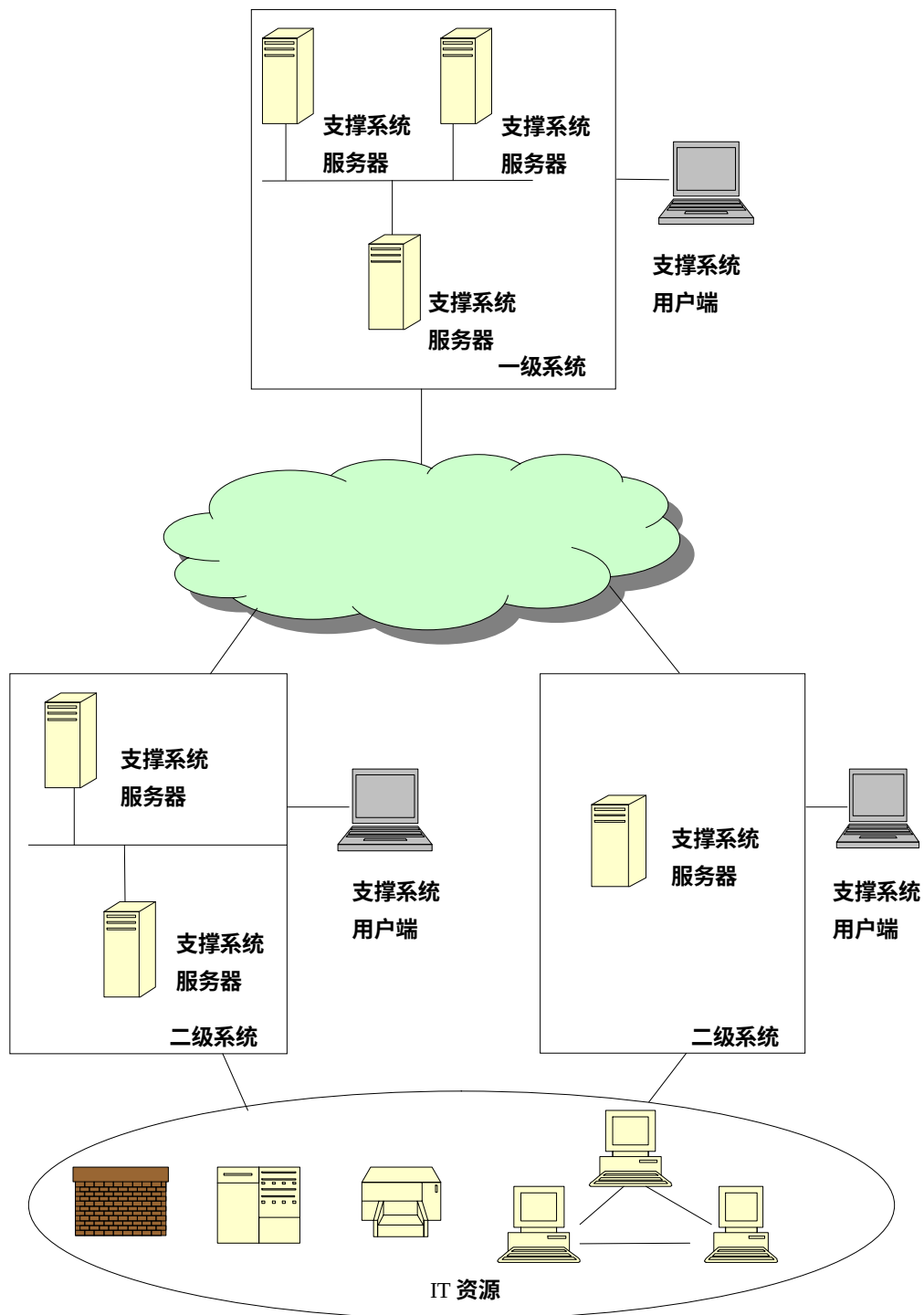


图 7c 多级系统

8 IT 运维服务支撑系统技术指标要求

8.1 系统容量

不同场景对应的支撑系统，其系统容量要求分别如下：

(1) 场景 1 对应的支撑系统

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。

(2) 场景 2 对应的支撑系统

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。

(3) 场景 3 对应的支撑系统

支撑系统软件可支持的图形终端应不少于 100 个，可支持并发操作的用户数应不少于 30 个。

(4) 场景 4 对应的支撑系统

支撑系统软件可支持的图形终端应不少于 100 个，可支持并发操作的用户数应不少于 30 个。

(5) 场景 5 对应的支撑系统

支撑系统软件可支持的图形终端应不少于 150 个，可支持并发操作的用户数应不少于 40 个。

8.2 系统可靠性

系统的退出和异常停止，应不影响其管理的 IT 基础设施和应用系统。

系统的年可用率应大于 99.9%。

8.3 实时性

设备运行正常情况下，支撑系统的告警最长响应时间（指设备上传告警到支撑系统显示告警）小于 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。

8.4 系统存储能力

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）。

8.5 系统安全性

系统应通过设置诸如防火墙等技术手段，对外部用户的访问进行控制。系统应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。

系统应提供有效的数据安全保护机制。

系统应对用户登录系统以及使用系统功能的情况进行记录。

系统应提供有效的系统病毒检测与清除的手段。

8.6 系统扩展性

系统软件应能够支持多种操作系统平台，包括主流的 UNIX、Windows 和 Linux 等。

系统软件应能够支持主流的关系型数据库。

系统应支持按照网络情况和用户需求调整软件规模，进行灵活的部署，支持单级和多级部署方式。

系统应采用分布式结构、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。

系统应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。

8.7 系统易用性

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。

系统应支持用多种方式来呈现各类管理信息。对于统计信息，应具有表格或直观图形化（如直方图、曲线图、饼图等）输出方式。

8.8 系统可维护性要求

系统应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。

9 IT 运维服务支撑系统管理接口要求

IT 运维服务支撑系统包含以下几类管理接口：

(1) IT 运维服务支撑系统与被管理资源之间的接口

本接口实现对被管 IT 资源的配置、告警、性能等数据的采集。可采用的接口技术有 SNMP/SMI、码流、xFlow、sysLog、WMI 等。接口采集的管理信息应满足政务部门的管理要求。

(2) IT 运维服务支撑系统间的接口

本接口实现分级情况下支撑系统之间的资产、配置、告警、性能等数据的交互。可采用的接口技术有 Web Service 接口、文件、码流等。

(3) IT 运维服务支撑系统与其他信息化系统间的接口

本接口实现 IT 运维服务支撑系统与其他信息化系统之间的运维信息的交互。可采用的接口技术有 Web Service 接口、文件、码流等。