Neusoft

安全运维服务白皮书

沈阳东软系统集成工程有限公司

2011 年 12 月

文档名称	NSS-WP-06-安全运维服务白皮书
基本说明	介绍东软安全服务团队提供的安全运维服务。
文档编号	NSS-SOP-06
扩散范围	对安全运维服务有需求的组织

地　　址：北京市海淀区东北旺西路 8 号中关村软件园 6 号楼

邮　　编：100029

电　　话：(86 10) 5651 7887

传　　真：(86 10)8282 6052

目 录

1 安全运维服务概述

安全运维服务是为保持企事业单位信息系统在安全运行的过程中所发生的一切与安全相关的管理与维护行为。计算机系统、网络、应用系统等是不断演变的实体，当前的安全不能保证后续永久的安全。

企事业单位投入巨资构建基础设施，部署安全产品，如防火墙、IDS、IPS及防病毒系统等，并实施安全策略，但可能由于防病毒系统或入侵防御系统在后续过程中未能得到持续的升级更新，将公司的信息系统重新置于不安全或危险的境地。

因此，需要对企事业单位的信息系统进行持续的日常的安全监控、补丁升级、系统风险评估等维护服务，以保证信息系统在安全健康的环境下正常运行。

2 东软安全运维服务介绍

安全运维服务是东软安全服务体系的成熟产品，主要以响应服务和驻场服务为主，主要包括：安全监控服务、安全检查服务、安全通告及预警服务、安全加固服务、应急响应服务、补丁管理服务、安全评估服务、项目上线评测服务以及安全培训等服务。

东软通过提供以上一系列的服务，协助用户做好信息系统的安全运行与维护，为用户的核心业务提供一个持续的、安全的、健康的信息系统运行环境。

3 东软安全运维服务特点

1. 自主安全运维服务平台：东软拥有自主研发的 SOC 安全运维服务平台，通过部署东软专业的 SOC 安全运维服务平台，可以为用户提供集中的、便利的、专业的安全监控、安全审计、安全通告的服务。

2. 标准化服务流程：东软以 ITIL 最佳实践为基础，制定标准化的运维服务流程，为高效的，高质量的安全运维服务提供保障。

3. 可定制服务内容：东软根据安全服务需求，将安全运维服务模块化，可以根据用户的信息系统环境现状及用户的维护能力提供定制化的服务内容。

4 东软安全运维服务内容

4.1 安全监控服务

安全监控服务是指通过实时监控客户的安全设备、安全系统的运行状态，统计、分析安全事件，帮助客户发现并解决信息系统中存在的安全威胁，为客户更新安全策略提供参考依据。

4.1.1 服务内容

1. 安全设备运行监控：

   实时监控用户防火墙、入侵检测系统、入侵防御系统等安全设备的运行状况，及时发现安全问题，分析日志信息，进行预警通告，提供安全事件的溯源依据。

2. 防病毒系统监控：

   实施监控客户防病毒系统，及时进行病毒分析、预警，并提供病毒处理解决方案及升级方法。

3. 安全系统运行情况记录、分析、统计：

   通过对安全系统的运行情况进行记录、分析，帮助安全管理人员形成分析报告。

4. 用户其他系统：根据用户实际需求，协助用户完成其他系统的安全监控。

4.1.2 成果输出

1. 《信息系统安全监控报告》
2. 《病毒处理解决方案》

3. 《防病毒补丁升级方法》

4.2 安全检查服务

安全检查服务是指配合客户完成对信息安全管理及安全技术进行检查，以及时发现用户信息系统安全管理落实及安全技术实施中存在的不足及风险，检查内容主要包括：

4.2.1 服务内容

1. 安全管理制度及执行情况
2. 防病毒系统的版本及升级情况
3. 终端用户的安全合规情况
4. 安全设备的系统性能情况
5. 系统开放服务及安全策略检查

4.2.2 成果输出

《安全检查服务报告》

4.3 安全预警通告服务

4.3.1 服务内容

信息安全通告预警服务是指通过及时通告最新的信息安全发展动态，为客户提供第一时间的安全预警，使得客户提前部署信息安全防护，防患于未然。（东软的预警服务频次为每年期不少于 12 次）。

通告内容主要包括：

1. 系统漏洞安全通告（Windows、AIX、SUSELinux、RedhatLinux、Netware 等）
2. 应用漏洞安全通告（Oracle、MSSQL、Sybase、Weblogic、Apache、IIS、Citrix、VMware、Novell 等）
3. 设备漏洞安全通告（Cisco、华为、Nokia、Checkpoint、天融信等）
4. 病毒安全预警通告（最新流行、严重病毒发展趋势及应对措施）
5. 其它安全威胁通告（最新严重的安全威胁分析及预防措施）
6. 漏洞预警
7. 病毒预警
8. 机构信息系统应用安全预警

4.3.2 成果输出

1. 《系统安全漏洞通告》
2. 《病毒预警通告》
3. 《其他预警通告》

4.4 安全加固服务

参考国内国际权威的系统安全配置标准，并结合客户的实际业务需要，对重点服务器的操作系统和应用服务进行适度安全配置加固和系统安全优化。

4.4.1 服务内容

1. 关闭系统中不用的服务，以免产生安全薄弱点
2. 对设备的管理应当采用安全的 SSH,HTTPS 代替不安全的 Telnet 及 HTTP 管理方式
3. 对于 Unix 服务器，应当正确配置 Syslog 使其记录相关的安全事件，对于 Windows 服务器，应当开启敏感事件及对重要资源的访问审核

4. 制定用户安全策略，包括制定用户登录超时锁定、口令复杂度及生存周期策略、账号锁定策略等
5. 限制管理员权限使用，仅当进行需采用特权的管理操作时方可切换至超级用户，一般的日常维护操作应当使用普通权限用户执行
6. 对于数据库系统，应当加强对敏感存储过程的管理，尤其是能执行操作系统命令的存储过程

4.4.2 成果输出

1.《服务器系统安全加固报告》
2.《数据库安全加固报告》
3.《信息安全体系规划报告》

4.5 应急响应服务

当客户信息系统发生安全事件时，东软可以快速及时的为客户提供全方位的技术支持，帮助客户在最短时间内控制安全事件对系统造成的影响，确定安全事件的故障源及问题的原因，并提供解决方案

4.5.1 服务形式

- 东软技术中心在线支持
- 东软知识库资源共享
- 东软工程师现场支持

4.5.2 快速响应服务级别

服务形式	*服务级别*
远程响应服务	5*8 （每周 5 天，每天 8 小时响应）

	7*24（每周 7 天，每天 24 小时响应）
现场服务	5*8*4（每周 5 天，每天 8 小时响应，4 小时到客户现场） 7*24*4（每周 7 天，每天 24 小时响应，4 小时到客户现场）

4.5.3 成果输出

《应急响应服务报告》

4.6 安全评估服务

安全评估服务主要是指在驻场运维服务过程中，根据客户的实际情况，对客户指定的重要信息系统实施安全风险评估服务，帮助客户发现信息系统中潜在的安全风险，并给出整改建议，将风险控制在可接受范围内。

4.6.1 服务内容

1. 信息资产安全需求评估

帮助客户识别和统计信息系统关键资产，并参照 CIA 属性对各资产的机密性、完整性、可用性进行需求分析，帮助用户制定各资产的安全防护等级。

2. 机房状况安全评估

参照机房环境安全建设的有关国家及行业标准，评估现有机房环境的安全状况，指导未来机房安全改造建设。

3. 网络架构安全评估

评估网络架构设计的合理性和安全性，包括安全域划分、Vlan 控制、路由设计、网络访问控制、安全审计措施等，对于网络架构中可能存在的各种安全隐患给出相应的安全改造技术建议。

4. 网络设备安全性评估

利用专业的漏洞扫描软件对网络中的关键网络设备进行安全分析，发现网络设备中存在的系统漏洞和配置安全隐患。

5. 网络流量安全性评估

利用专业网络流量检测工具监控分析网络流量的安全性和合理性，识别流量的地址分布、应用协议分布情况等。

6. 服务器漏洞检测

利用多种专业漏洞扫描工具对客户的所有服务器系统进行全面的系统脆弱性检测评估，并对扫描结果进行人工分析；检查对象包括操作系统、应用服务平台、后台数据库等。

7. 服务器人工审计

结合专家经验，并参照国内国际权威安全审计 CheckList，对重点服务器系统进行人工控制台审计评估，评估内容包括：用户账号及口令健壮性、系统安全配置、补丁更新情况、日志审核策略、受入侵迹象、可疑后门及木马清除等。

8. 应用系统安全评估

对于 C/S 和 B/S 结构开发的业务软件进行深层次的安全分析，主要针对系统的安全抗攻击能力，信息保密性与设计开发过程中的安全问题进行深度挖掘

9. 关键数据安全保障评估

分析和评估关键数据在产生、传递、使用、存储、备份等过程中的安全保障措施，对于可能导致关键数据损失的严重隐患，我方将提供有针对性的合理建议。

10. PC 终端安全性检测

利用多种专业漏洞扫描工具对关键网络区域的 PC 终端进行全面的系统脆弱

性检测评估，并对扫描结果进行人工分析；检查内容包括补丁更新情况、帐号弱口令、违规应用服务等。

11. 内网用户网络行为审计评估

监测和审计内部网络用户的上网行为、日常操作行为等，及时发现不良安全隐患和违规操作，杜绝危险事故的发生。

12. 安全防护技术措施审计

对客户已有的安全防护技术措施及相关安全设备进行人工审计评估，审计对象包括防火墙、VPN、IDS、防病毒、补丁管理等等，审计内容包括日志审计、配置审计、运行状况审计等，综合分析当前安全产品上所应用的策略是否为最佳工作状态，对于不合理的设置以及应用情况给出安全性部署建议。

13. 渗透测试

通过模拟黑客攻击的方式，分别从内网和外网对客户的网络信息系统进行抗入侵攻击能力测试，深入发现和检测安全防护措施的有效性，并模拟一旦网站系统遭受攻击后可能受到的破坏影响程度。

14. 安全管理状况评估

参照国家（主要指等级保护）及行业相关政策要求以及国内国际权威的信息安全管理体系标准，采用访谈、问卷调查、文档审计等多种方式评估客户在信息安全管理方面的现状情况，包括：安全保障组织机构及人员配备情况、安全运维管理制度及流程、应急保障体系建设等，并提供相应的改善建议。

4.6.2 成果输出

1. 《信息系统安全风险评估报告》
2. 《信息系统安全风险整改建议书》

4.7 项目上线评测服务

项目上线评测服务是指在客户新项目上线运行前对该项目进行安全测评，及时发现新项目本身存在的安全漏洞，并协助客户方指定整改方案，将风险降低到可接受程度，以最大程度的降低新项目带来的安全风险。

4.7.1 服务内容

1. 新开发应用系统上线评测
2. 新的网络及安全产品上线评测
3. 新的网络安全集成项目上线评测

4.7.2 输出成果

《项目上线安全评测报告》

4.8 安全培训服务

安全培训服务主要是指面向客户不同的对象提供相应的安全知识培训，主要包括客户 IT 管理人员，技术人员及全体员工，培训内容则从安全管理、安全技术及安全意识等不同的层次为客户提供培训，以便全方位的提升客户在信心安全方面的综合防御与治理能力。

4.8.1 培训内容

序号	课程名称	可选
1.	《信息系统安全风险治理》	

2.	《信息安全技术基础》	
3.	《信息安全意识》	

注：培训内容可根据客户的实际需求进行调整。

4.8.2 成果输出

1. 《XXX 培训讲义》
2. 《XXX 培训教材》

5 安全值守服务

5.1 服务内容

安全驻场值守服务主要是根据用户的要求，在用户指定的服务范围内完成以下相关服务，包括但不限于以下服务：

1. 安全设备日常巡检：安全设备软、硬件健康性检查，安全策略检查、及安全日志分析等。
2. 安全事件技术支持，及时排查并解决安全事件，并分析、确认问题原因
3. 协助完成安全策略的核查与整改，定期检查安全策略的配置并进行优化。
4. 整理关键业务平台的安全设备的拓扑资料，保持相关资料的更新

   包括 ip 地址，网络拓扑、配置备份等资料保持最新状态。
5. 协助处理各相关部门的业务申请及故障

5.2 成果输出

1. 《安全值守日报告》
2. 《安全值守周报告》
3. 《安全值守月报告》
4. 《安全巡检报告》
5. 《安全设备管理资料》

6 东软安全运维服务形式

考虑到不同客户的信息系统的保护级别的差异，以及不同客户自身维护能力的不同，同时从降低客户服务成本的角度考虑，东软将安全运维服务形式设定为响应式服务；驻场式服务及半驻场式服务三种形式。

1. 远程响应式服务：

   响应式服务主要是指东软的服务人员被动的接受客户的服务请求，按照服务要求，在规定的时间内响应并完成服务交付。

2. 驻场式服务：

   驻场式服务是指东软将派驻安全服务顾问在客户现场全日制职守，主动的帮助客户监管信息系统中的安全风险，协助客户进行风险治理。

3. 咨询式服务：

   咨询式服务是指东软指派专人跟踪指定客户的安全服务，但不需要派驻客户服务现场，同时，东软指派的安全顾问需要定期的在客户服务现场进行安全检查，以便及时发现安全漏洞，并给出合理化整改建议。

以上几种服务形式主要根据客户对安全服务级别的要求及成本预算灵活选择。

7 东软安全运维组织架构

在为客户提供高效率、高质量运维服务的前提下，东软的安全运维组织架构简洁明了，规避了繁琐的沟通协调流程。

最前端是一线的运维服务团队，后端由行业专家及各领域专项技术专家团队组成，中间以安全运维主管为纽带，将前端一线服务与后台的二线支持承接起来，实现快速的资源调配，避免了繁琐无序的资源申请和审批，如图 6-1 所示：

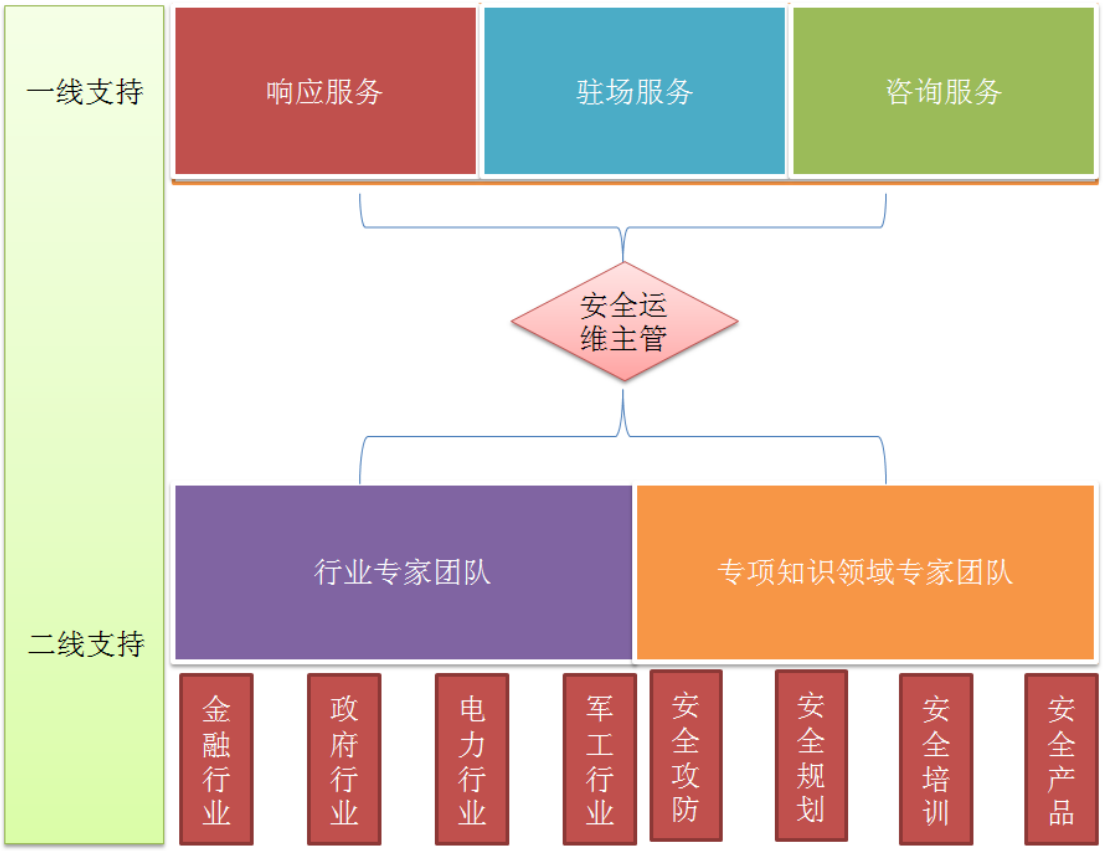
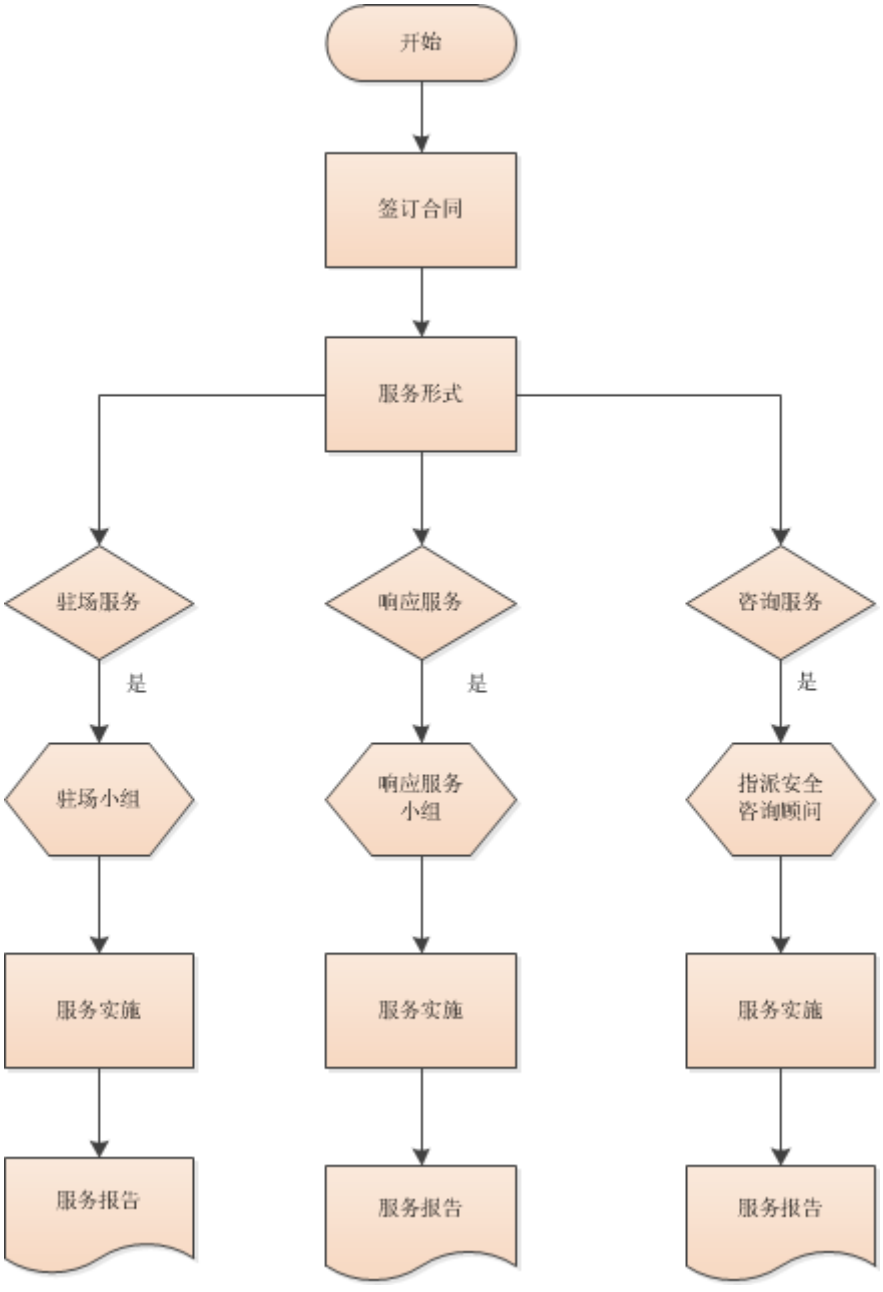


图 6-1

8 东软安全运维服务流程



9 东软安全运维服务能力

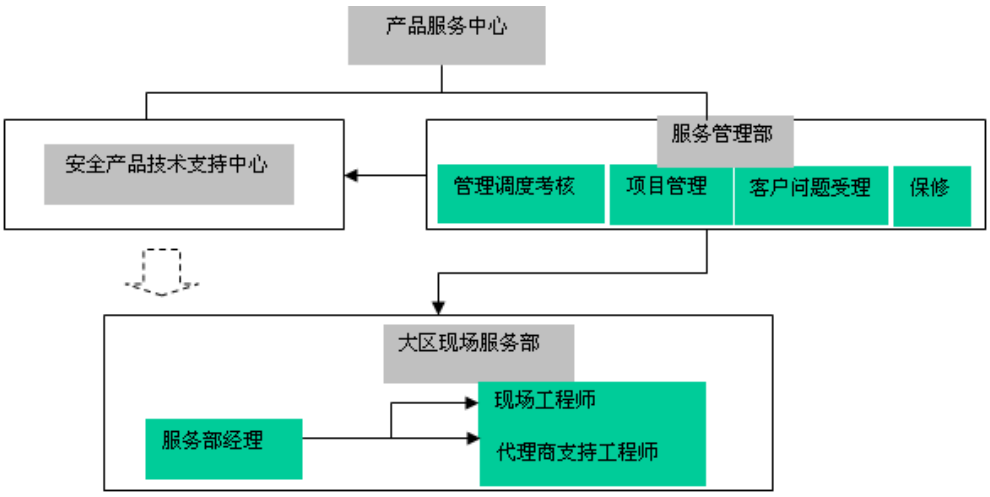
东软承接过多项大型系统集成项目和安全服务项目，具有强大技术力量和丰富的售后服务经验。东软在网络安全领域有 10 多年的研发生产历程，在网络安全技术方面积累了丰富的经验，并且，拥有累计投资 4000 万的高水平的网络安全产品应用测试实验室，这为项目的技术支持、售后维护服务提供强有力的保障。

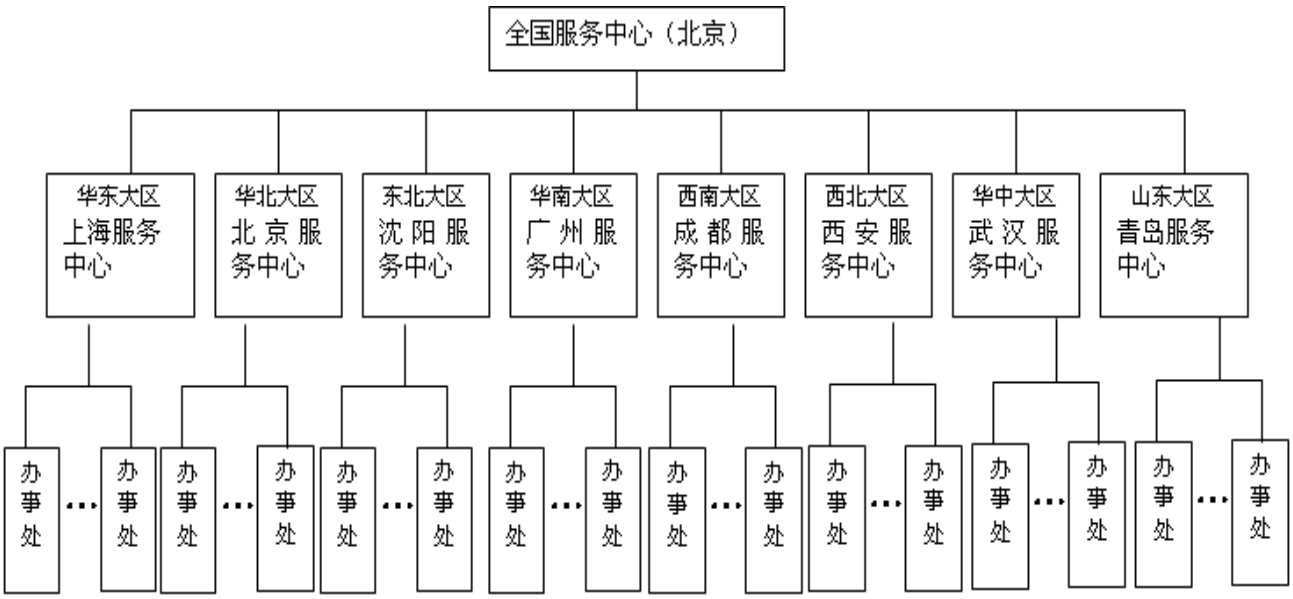
9.1.1 售后服务技术支持体系

东软拥有自己特色的客户服务体系，在北京设立产品服务中心，该中心的工程师为核心技术支持团队，由资深的网络安全工程师和网络安全咨询顾问对大区服务工程师提供技术咨询和支持。在北京、上海、广州、成都、西安、沈阳、武汉、青岛设大区服务中心，其对大区所辖区域的网络安全产品用户提供技术支持和服务，大区服务中心对大区所辖分支机构服务网点提供技术支持，分支机构服务网点的工程师作为一线工程师，直接为本地用户提供服务。全国客户服务中心和大区服务中心工程师也可以为用户直接提供服务。

各大区现场服务工程师由大区服务经理管理和调度，各大区现场服务部由产品服务中心服务管理部管理和考核。

服务组织结构图如下图所示：





9.1.2 东软本地化服务机构

为了更好地为广大客户提供本地化的开发和技术支持服务，东软在北京设立产品服务中心，在全国建立了八个大区服务中心。大区服务中心对大区所辖分支机构服务网点提供技术支持，分支机构服务网点的工程师作为一线工程师，直接为本地用户提供服务。东软的三层服务体系提供了本地化的特色服务。

东软在北京设有全国服务中心，拥有强大的技术实力，各类技术机构包括：

1) 产品服务中心，负责网络安全产品的售后服务和技术支持。

2) 网络安全实验室，负责攻防等安全技术研究。

3) 解决方案中心，负责提供网络安全整体解决方案。

4) 应急响应中心，负责为大型客户提供安全事件应急响应服务。

9.1.3 全国售后服务网点

东软在国内近 40 个主要城市设有分支机构服务网点，建立了遍布全国的三级技术服务体系，形成遍布全国的技术支持服务网络。这种统一管理的分布式技术服务体系有利于为用户提供最迅速的响应，同时也保证了服务管理的有效性和服务质量的一致性。

10 安全运维服务客户收益

1. 降低客户信息系统安全风险
2. 降低客户人员成本
3. 弥补客户安全技术知识相对单一的不足
4. 提升客户品牌价值与客户满意度