目录

[三级等保安全设计思路 2](#_Toc419381078)

[1、 保护对象框架 2](#_Toc419381079)

[2、 整体保障框架 2](#_Toc419381080)

[3 、安全措施框架 3](#_Toc419381081)

[4、 安全区域划分 4](#_Toc419381082)

[5、 安全措施选择 5](#_Toc419381083)

[6、需求分析 6](#_Toc419381084)

[6.1、 系统现状 6](#_Toc419381085)

[6.2、 现有措施 6](#_Toc419381086)

[6.3 具体需求 6](#_Toc419381087)

[6.3.1 等级保护技术需求 6](#_Toc419381088)

[6.3.2 等级保护管理需求 7](#_Toc419381089)

[7、安全策略 7](#_Toc419381090)

[7.1 总体安全策略 7](#_Toc419381091)

[7.2 具体安全策略 8](#_Toc419381092)

[8、 安全解决方案 8](#_Toc419381093)

[8.1 安全技术体系 8](#_Toc419381094)

[8.1.1 安全防护系统 8](#_Toc419381095)

[8.2 安全管理体系 8](#_Toc419381096)

[9、安全服务 8](#_Toc419381097)

[9.1 风险评估服务 9](#_Toc419381098)

[9.2 管理监控服务 9](#_Toc419381099)

[9.3 管理咨询服务 9](#_Toc419381100)

[9.4 安全培训服务 9](#_Toc419381101)

[9.5 安全集成服务 9](#_Toc419381102)

[10、 方案总结 10](#_Toc419381103)

[11、产品选型 11](#_Toc419381104)

# 三级等保安全设计思路

# 1、 保护对象框架

  保护对象是对信息系统从安全角度抽象后的描述方法，是信息系统内具有相似安全保护需求的一组信息资产的组合。

依据信息系统的功能特性、安全价值以及面临威胁的相似性，信息系统保护对象可分为计算区域、区域边界、网络基础设施、安全措施四类。具体内容略。

建立了各层的保护对象之后，应按照保护对象所属信息系统或子系统的安全等级，对每一个保护对象明确保护要求、部署适用的保护措施。

保护对象框架的示意图如下：

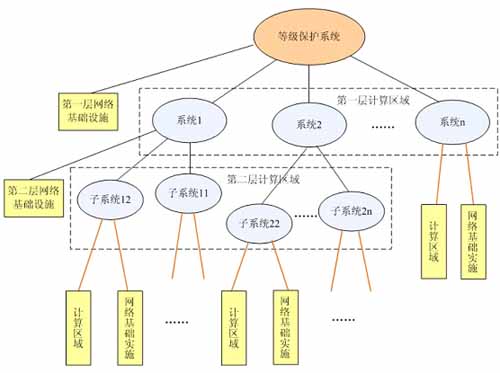


图1. 保护对象框架的示意图

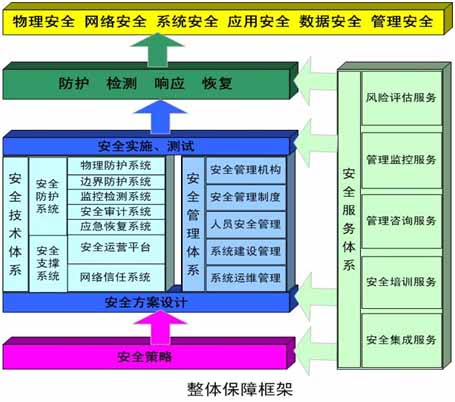
# 2、 整体保障框架

就安全保障技术而言，在体系框架层次进行有效的组织，理清保护范围、保护等级和安全措施的关系，建立合理的整体框架结构，是对制定具体等级保护方案的重要指导。  
 根据中办发[2003]27号文件，“坚持积极防御、综合防范的方针，全面提高提高信息安全防护能力”是国家信息保障工作的总体要求之一。“积极防御、综合防范” 是指导等级保护整体保障的战略方针。

信息安全保障涉及技术和管理两个相互紧密关联的要素。信息安全不仅仅取决于信息安全技术，技术只是一个基础，安全管理是使安全技术有效发挥作用，从而达到安全保障目标的重要保证。

安全保障不是单个环节、单一层面上问题的解决，必须是全方位地、多层次地从技术、管理等方面进行全面的安全设计和建设，积极防御、综合防范”战略要求信息系统整体保障综合采用覆盖安全保障各个环节的防护、检测、响应和恢复等多种安全措施和手段，对系统进行动态的、综合的保护，在攻击者成功地破坏了某个保护措施的情况下，其它保护措施仍然能够有效地对系统进行保护，以抵御不断出现的安全威胁与风险，保证系统长期稳定可靠的运行。

整体保障框架的建设应在国家和地方、行业相关的安全政策、法规、标准、要求的指导下，制订可具体操作的安全策略，并在充分利用信息安全基础设施的基础上，构建信息系统的安全技术体系、安全管理体系，形成集防护、检测、响应、恢复于一体的安全保障体系，从而实现物理安全、网络安全、系统安全、数据安全、应用安全和管理安全，以满足信息系统全方位的安全保护需求。同时，由于安全的动态性，还需要建立安全风险评估机制，在安全风险评估的基础上，调整和完善安全策略，改进安全措施，以适应新的安全需求，满足安全等级保护的要求，保证长期、稳定、可靠运行。  
整体保障框架的示意图如下：

  
   
图2. 整体保障框架的示意图

# 3 、安全措施框架

  安全措施框架是按照结构化原理描述的安全措施的组合。本方案的安全措施框架是依据“积极防御、综合防范”的方针，以及“管理与技术并重”的原则进行设计的。

安全措施框架包括安全技术措施、安全管理措施两大部分。安全技术措施包括安全防护系统（物理防护、边界防护、监控检测、安全审计和应急恢复等子系统）和安全支撑系统（安全运营平台、网络管理系统和网络信任系统）。

安全技术措施、安全管理措施各部分之间的关系是人（安全机构和人员），按照规则（安全管理制度），使用技术工具（安全技术）进行操作（系统建设和系统运维）。

安全措施框架示意图如下：

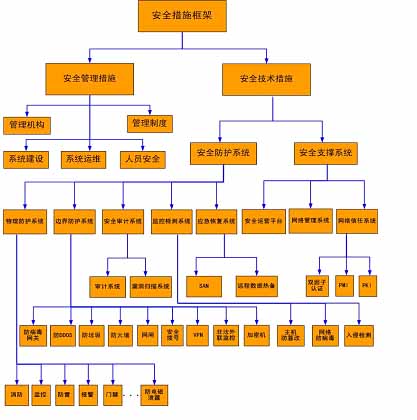


图3. 安全措施框架示意图

# 4、 安全区域划分

不同的信息系统的业务特性、安全需求和等级、使用的对象、面对的威胁和风险各不相同。如何保证系统的安全性是一个巨大的挑战，对信息系统划分安全区域，进行层次化、有重点的保护是有保证系统和信息安全的有效手段。

按数据分类分区域分等级保护，就是按数据分类进行分级，按数据分布进行区域划分，根据区域中数据的分类确定该区域的安全风险等级。目的是把一个大规模复杂系统的安全问题，分解为更小区域的安全保护问题。这是实现大规模复杂信息的系统安全等级保护的有效方法。

随着安全区域方法的发展，发现力图用一种大一统的方法和结构去描述一个复杂的网络环境是非常困难的，即使描述出来其可操作性也值得怀疑。因此，……提出了“同构性简化的方法”，其基本思路是认为一个复杂的网络应当是由一些相通的网络结构元所组成，这些网络结构元进行拼接、递归等方式构造出一个大的网络。可以说，结构性简化好像将网络分析成一种单一大分子组成的系统，而同构性简化就是将网络看成一个由几种小分子组成的系统。“3+1同构性简化”的安全域方法就是一个非常典型的例子，此方法是用一种3+1小分子构造来分析venus customer的网络系统。（注：除了3+1构造之外，还存在其他形式的构造。）具体来说信息系统按照其维护的数据类可以分为安全服务域、安全接入域、安全互联域以及安全管理域四类。在此基础上确定不同区域的信息系统安全保护等级。同一区域内的资产实施统一的保护，如进出信息保护机制，访问控制，物理安全特性等。

信息系统可以划分为以下四个大的安全域（3+1同构法）：

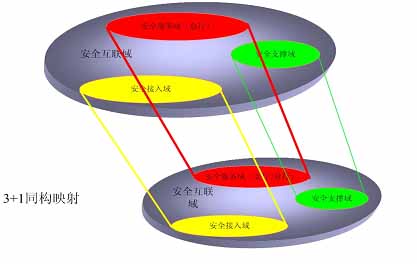
**安全接入域：**由访问同类数据的用户终端构成安全接入域，安全接入域的划分应以用户所能访问的安全服务域中的数据类和用户计算机所处的物理位置来确定。安全接入域的安全等级与其所能访问的安全服务域的安全等级有关。当一个安全接入域中的终端能访问多个安全服务域时，该安全接入域的安全等级应与这些安全服务域的最高安全等级相同。安全接入域应有明确的边界，以便于进行保护。

**安全互联域：**连接传输共同数据的安全服务域和安全接入域组成的互联基础设施构成了安全互联域。主要包括其他域之间的互连设备，域间的边界、域与外界的接口都在此域。安全互联域的安全等级的确定与网络所连接的安全接入域和安全服务域的安全等级有关。

**安全服务域：**在局域范围内存储，传输、处理同类数据，具有相同安全等级保护的单一计算机（主机/服务器）或多个计算机组成了安全服务域，不同数据在计算机的上分布情况，是确定安全服务域的基本依据。根据数据分布，可以有以下安全服务域：单一计算机单一安全级别服务域，多计算机单一安全级别服务域，单一计算机多安全级别综合服务域，多计算机多安全级别综合服务域。

**安全管理域：**安全系统的监控管理平台都放置在这个区域，为整个IT架构提供集中的安全服务，进行集中的安全管理和监控以及响应。具体来说可能包括如下内容：病毒监控中心、认证中心、安全运营中心等。

安全区域3+1同构示意图如下：

  
   
图4. 安全区域3+1同构示意图

# 5、 安全措施选择

  27号文件指出，实行信息安全等级保护时“要重视信息安全风险评估工作，对网络与信息系统安全的潜在威胁、薄弱环节、防护措施等进行分析评估，综合考虑网络与信息系统的重要性、涉密程度和面临的信息安全风险等因素，进行相应等级的安全建设和管理”。由此可见，信息系统等级保护可视为一个有参照系的风险管理过程。等级保护是以等级化的保护对象、不同安全要求对应的等级化的安全措施为参照，以风险管理过程为主线，建立并实施等级保护体系的过程。

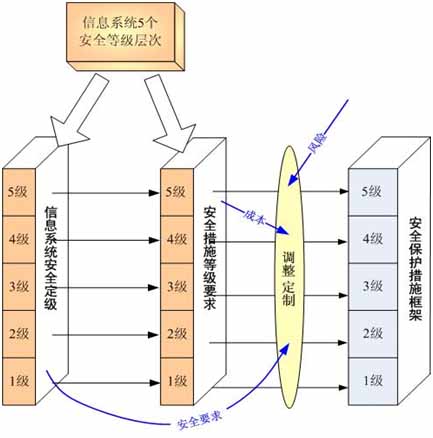
安全措施的选择首先应依据我国信息系统安全等级划分的要求，设计五个等级的安全措施等级要求（安全措施等级要求是针对五个等级信息系统的基本要求）。不同等级的信息系统在相应级别安全措施等级要求的基础上，进行安全措施的调整、定制和增强，并按照一定的划分方法组成相应的安全措施框架，得到适用于该系统的安全措施。安全措施的调整主要依据综合平衡系统安全要求、系统所面临风险和实施安全保护措施的成本来进行。信息系统安全措施选择的原理图如下：  
 

图5. 安全措施选择的原理图

# 6、需求分析

## 6.1、 系统现状

## 6.2、 现有措施

目前，信息系统已经采取了下述的安全措施：

1、在物理层面上，

2、在网络层面上，

3、在系统层面上，

4、在应用层面上，

5、在管理层面上，

## 6.3 具体需求

### 6.3.1 等级保护技术需求

  要保证信息系统的安全可靠，必须全面了解信息系统可能面临的所有安全威胁和风险。威胁是指可能对信息系统资产或所在组织造成损害事故的潜在原因；威胁虽然有各种各样的存在形式，但其结果是一致的，都将导致对信息或资源的破坏，影响信息系统的正常运行，破坏提供服务的有效性、可靠性和权威性。

任何可能对信息系统造成危害的因素，都是对系统的安全威胁。威胁不仅来来自人为的破坏，也来自自然环境，包括各种人员、机构出于各自目的的攻击行为，系统自身的安全缺陷以及自然灾难等。信息系统可能面临的威胁的主要来源有：

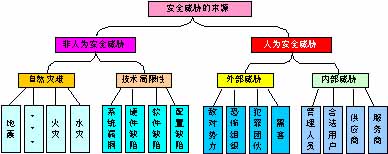


图6. 威胁的主要来源视图

威胁发生的可能性与信息系统资产的吸引力、资产转化为报酬的容易程度、威胁的技术含量、薄弱点被利用的难易程度等因素密切相关。

被动攻击威胁与风险：网络通信数据被监听、口令等敏感信息被截获等。

主动攻击威胁与风险：扫描目标主机、拒绝服务攻击、利用协议、软件、系统故障、漏洞插入或执行恶意代码（如：特洛依木马、病毒、后门等）、越权访问、篡改数据、伪装、重放所截获的数据等。

邻近攻击威胁与风险：毁坏设备和线路、窃取存储介质、偷窥口令等。

分发攻击威胁与风险：在设备制造、安装、维护过程中，在设备上设置隐藏的的后门或攻击途径。

内部攻击威胁与风险：恶意修改数据和安全机制配置参数、恶意建立未授权连接、恶意的物理损坏和破坏、无意的数据损坏和破坏。

### 6.3.2 等级保护管理需求

安全是不能仅仅靠技术来保证，单纯的技术都无法实现绝对的安全，必须要有相应的组织管理体制配合、支撑，才能确保信息系统安全、稳定运行。管理安全是整体安全中重要的组成部分。信息系统安全管理虽然得到了一定的落实，但由于人员编制有限，安全的专业性、复杂性、不可预计性等，在管理机构、管理制度、人员安全、系统建设、系统运维等安全管理方面存在一些安全隐患：

——管理机构方面:

——管理制度方面:

——人员安全方面:

——系统建设方面:

——系统运维方面:

# 7、安全策略

## 7.1 总体安全策略

 —— 遵循国家、地方、行业相关法规和标准；

 ——贯彻等级保护和分域保护的原则；

 ——管理与技术并重，互为支撑，互为补充，相互协同，形成有效的综合防范体系；

 ——充分依托已有的信息安全基础设施，加快、加强信息安全保障体系建设。

 ——第三级安全的信息系统具备对信息和系统进行基于安全策略强制的安全保护能力。

 ——在技术策略方面：

 ——在管理策略方面:

## 7.2 具体安全策略

1、安全域内部策略

2 、安全域边界策略

3 、安全域互联策略

# 8、 安全解决方案

  不同的安全等级要求具有不同的基本安全保护能力，实现基本安全保护能力将通过选用合适的安全措施或安全控制来保证，可以使用的安全措施或安全控制表现为安全基本要求，依据实现方式的不同，信息系统等级保护的安全基本要求分为技术要求和管理要求两大类。

技术类安全要求通常与信息系统提供的技术安全机制有关，主要是通过在信息系统中部署软硬件并正确的配置其安全功能来实现；管理类安全要求通常与信息系统中各种角色参与的活动有关，主要是通过控制各种角色的活动，从政策、制度、规范、流程以及记录等方面做出规定来实现。

根据威胁分析、安全策略中提出的基本要求和安全目标，在整体保障框架的指导下，本节将就具体的安全技术措施和安全管理措施来设计安全解决方案，以满足相应等级的基本安全保护能力。

## 8.1 安全技术体系

### 8.1.1 安全防护系统

边界防护系统

监控检测系统

安全审计系统

应急恢复系统

安全支撑系统

安全运营平台

网络管理系统

网络信任系统

## 8.2 安全管理体系

安全管理机构

安全管理制度

人员安全管理

系统建设管理

系统定级\系统备案\安全方案设计\产品采购\自行软件开发\外包软件开发\工程实施\测试验收\系统交付\安全测评。详细内容略去。

系统运维管理

# 9、安全服务

技术类的安全要求可以通过在信息系统中部署安全产品来实现，同时需要对网络设备、操作系统、应用软件的安全功能的正确配置，这需要通过安全评估和加固等安全服务来完成；管理类的安全要求需要通过管理咨询服务来完善，以实现IT运维管理标准化和规范化，提高安全管理的水平。

## 9.1 风险评估服务

安全风险评估服务可以为组织：

 ——评估和分析在网络上存在的安全技术风险；

——分析业务运作和管理方面存在的安全缺陷；

——调查信息系统的现有安全控制措施，评价组织的业务安全风险承担能力；

——评价风险的优先等级，据此为组织提出建立风险控制安全规划的建议。

具体的评估服务包括如下内容略

## 9.2 管理监控服务

  全面实时的执行对客户信息系统远程监控是M2S安全服务的主要组成部分和特点之一，通过监控来达到安全事件检测、安全事件跟踪、病毒检测、流量检测等等任务，进而通过检测的结果可以动态的调整各个安全设备的安全策略，提高系统的安全防范能力。监控服务完全是一种以人为核心的安全防范过程，通过资深的安全专家对各种安全产品与软件的日志、记录等等的实时监控与分析，发现各种潜在的危险，并提供及时的修补和防御措施建议。……的安全监控服务具有两种形式：远程监控服务和专家的现场值守服务。每一种服务都满足了客户一定层面的需求，体现了安全监控服务的灵活性以及可重组性。

## 9.3 管理咨询服务

 ……提供的主要安全管理咨询顾问服务包如下。详细内容可参考“……安全管理咨询顾问服务白皮书”。

## 9.4 安全培训服务

安全实践培训主要是从人员的角度出发来强化的安全知识以及抵御攻击行为的能力，主要包括如下方面的培训建议：

 ——基本安全知识培训：主要对常规人员提供个人计算机使用的基本安全知识，提高个人计算机系统的防范能力。

 ——主机安全管理员培训：对安全管理员进行针对于主机系统的安全培训，强化信息系统维护人员的安全技术水平。

 ——网络安全管理员培训：对安全管理员进行针对于网络系统的安全培训。

 ——安全管理知识培训：为的主要管理层人员提供，有助于从管理的角度强化信息系统的安全。

 ——产品培训：为人员能进一步认识各种安全产品而提供的基本培训。

 ——CISP培训：为培养技术全面的信息安全专家，而提供的具有国家认证资质的培训。“注册信息安全专业人员”，英文为Certified Information Security Professional (简称CISP)，根据实际岗位工作需要，CISP分为三类,分别是“注册信息安全工程师”,英文为Certified Information Security Engineer（简称CISE）; “注册信息安全管理人员”， 英文为Certified Information Security  Officer(简称CISO)，“注册信息安全审核员” 英文为Certified Information Security Auditor(简称CISA)。

## 9.5 安全集成服务

**价值**

 ——加强IT系统安全保障，提高您的客户的信任，提高竞争力；

 ——减小IT系统管理的工作量，提高效率，降低运营成本；

 ——帮助您了解IT系统面临的风险并有效地控制风险；

 ——帮助您的IT系统符合相关法律、标准与规范，减少诉讼与纷争。

**思路**

 ——……安全解决方案从三个层面来考虑客户的信息安全需求，协助客户建设基于“信息安全三观论”的信息安全保障体系；

 ——在三观论的基础上，基于信息安全三要素模型（资产、威胁与保障措施）提出了……信息安全保障总体框架功能要素模型（VIAF-FEM）。强调以IT资产与业务为核心，针对资产/业务面临的威胁从人、过程、技术三个方面设计全面的信息安全解决方案。

**分类**

 根据具体需求不同，……提供如下表所示的几种安全集成解决方案。

|  |  |
| --- | --- |
| **类型** | **满足需求** |
| 信息安全整体解决方案 | IT安全规划 |
| 信息安全管理方案 | 安全管理咨询 |
| 信息安全技术方案 | 信息安全技术保障体系 |
| 信息安全服务方案 | 特定安全服务需求 安全服务需求的组合 |
| 安全产品解决方案 | 特定安全功能需求 安全功能需求的组合 |

表1. 安全集成解决方案表

**特色**

 ——行业化：……凭借在电信、金融、政府、教育、能源等行业多年的信息安全实战经验，提供行业化的解决方案。

 ——面向业务：……从客户业务安全的角度出发解决实际安全问题，由功能需求导出面向业务的解决方案。

 ——体系完整：……凭借自身的专业安全队伍以及阵容强大的外部专家支持，基于完整的安全体系提供解决方案。

 ——理念先进：……秉承“一米宽，一公里深”的理念，及时跟踪国际先进安全理念，以此为基础开发安全的最佳实践，成功应用于客户化的解决方案中。

# 10、 方案总结

 本等级保护设计方案具有以下特点：

 1、体现了等级防护的思想。本方案根据3级信息系统的基本要求和安全目标，提出了具体的安全等级保护的设计和实施办法，明确3级信息系统的主要防护策略和防护重点。

 2、体现了框架指导的思想。本方案将安全措施、保护对象、整体保障等几个等级保护的关键部分和内容分别整理归纳为框架模型，利于在众多安全因素中理清等级保护的主线。

 3、体现了分域防护的思想。本方案根据信息系统的访问控制要求，针对不同的保护对象进行了合理的安全域划分。通过建立合理有效的边界保护策略，实现安全域之间的访问控制；在不同的安全域内实施不同级别的安全保护策略；针对不同等级的安全域之间的互联也要实现相应的保护。

 4、体现了深度防御的思想。本方案在对信息系统可能面临的安全威胁进行分析的基础上，结合安全域的划分，从物理层、网络层、系统层、应用层、数据层和管理层几个安全层面进行了整体的安全设计，在整体保障框架的指导下，综合多种有效的安全防护措施，进行多层和多重防御，实现纵深防御。

 5、体现了多角度对应的思想。本方案从威胁出发引出保护基本需求，从基本要求引出安全策略和目标，在需求分析和安全策略之间分层相互对应；在总体策略里提出各层面的总体保护要求，在具体策略里提出各层面的具体保护要求，各层相互对应；在安全解决方案的安全技术措施可以与安全策略中的基本要求和安全目标相对应。

 6、体现了动态发展的思想。本方案在满足信息系统目前基本的、必须的安全需求的基础上，要求随着应用和网络安全技术的发展，不断调整安全策略，应对不断变化的网络安全环境。

# 11、产品选型

|  |  |  |
| --- | --- | --- |
| 安全防护系统 | 安全产品 | 备注 |
| 物理防护系统 | 门禁系统 |  |
| 监控系统 |  |
| 报警系统 |  |
| 防雷击 |  |
| 防静电 |  |
| 防电磁泄露 |  |
| UPS |  |
| 防火 |  |
| 边界防护系统 | 防病毒网关 |  |
| 非法外联监控系统 |  |
| 防拒绝服务攻击系统 |  |
| 防火墙 |  |
| 安全拨号服务器 |  |
| 防垃圾邮件系统 |  |
| VPN/加密机 | SSL加密、IPSEC加密 |
| UTM |  |
| 监控检测系统 | 防间谍软件 |  |
| 网站防篡改系统 |  |
| 网络防病毒系统 |  |
| 网络入侵检测系统 |  |
| 主机入侵检测系统 |  |
| 安全审计系统 | 业务网审计系统 |  |
| 主机审计系统 |  |
| 漏洞扫描系统 |  |
| 应急恢复系统 | 备份管理软件 |  |
| 虚拟磁带库 |  |
| 磁带机/磁带库 |  |
| 光盘库 |  |
| 磁盘阵列 |  |
| 安全支撑系统 | 安全产品 | 备注 |
| 网络管理系统 | 网络管理软件 |  |
| 网络信任系统 | 动态口令系统 |  |
| 文件保密系统 |  |