## 系统总体安全设计

系统安全已成为IT工程师和安全设计师的挑战，直到最近几年，整个IT系统常常围绕单一对象或单一利益共同体展开设计，这些通常由独立的物理系统支持，并且每个系统都有属于自己的数据库和独立应用。目前，新标准是在更成熟的通讯环境、更智能的操作系统、各种标准整合的协议支持下，使IT工程师设计和维护广泛的组织框架下，交互式的企业解决方案。

应用安全包含用来防止应用安全政策的意外情况或者是由于设计、开发或使用过程中的缺陷导致的潜在问题（弱点）。对于一般的应用、安全和控制过程的开发是基于COTS（Checkout Test Set）功能的，它由Windows操作系统、ArcGIS、关系型数据库管理系统（RDBMS）和HTTP协议提供。

Windows访问控制列表（Access Control List，ACL）通过命令系统提供完全访问控制，即通过分配许可给角色，再分配角色给用户来实现访问控制。

对于完全访问控制列表（ACL）的文件系统访问控制接口（Access Control Entries，ACE），可定义为分组权限的特定系统对象定义，如应用、程序或者文件。这些特权或许可决定特定的访问权限，比如用户是否对某一对象进行读、写、执行或删除等操作。

ArcGIS为客户端或者网络应用提供的控制可通过ArcGIS即开即用软件、自定义应用增强（利用ArcObject）实现，或者通过ArcGIS网络客户来实现。以下应用控制可在ArcGIS企业环境中得以实现：

自定义控制扩展可用来实现诸如一致性管理和访问控制等技术。ArcGIS自定义控制扩展基于ArcObjects开发接口开发。ArcGIS使用户能限制ArcGIS客户端操作功能（如编辑、删除、保存、打印等），或者根据用户身份控制其访问各种数据。

GML是XML的一种应用，实现对地理信息的建模、传输和存储。ArcObjects利用GML和RDBMS的存储功能，为ArcGIS多用户地理数据库环境下的审核控制提供框架和方法。GIS工作流活动的详细历史记录在GML结构中，并存储在RDBMS中。另外，为了记录是谁执行了编辑操作，将附加评论和记录，以提供一个可跟踪的、备有证明文件的、活动的日志，包括前一编辑、后一编辑及合法编辑的历史记录。

整合的操作系统和单点登录(single sign-on，SSO)是两个安全体系，它们可通过ArcObjects进行重复利用，以便利用在集中位置管理的用户名和密码鉴别和连接ArcGIS产品。这个位置可能是一个加密文件、RDBMS数据表、轻量目录访问协议（Lightweight Directory Access Protocol，LDAP）服务器，或者是一个RDBMS数据表和LDAP服务器的连接器。主要目的是使用户免除不得不继续鉴别它们身份的烦恼。这些技术取决于用户通过身份认证进入桌面工作空间（整合操作系统身份认证）或者团体单点登录体系。

本地身份认证由ArcSDE和RDBMS来完成。ArcGIS与系统组件之间强有力的身份认证控制可通过由已经获取本地身份认证的用户向下游系统用户进行授权来实现。ArcSDE利用直接连接体系支持通过本地Windows身份认证，使ArcGIS客户端连接到RDBMS。直连结构允许ArcGIS客户端重复利用RDBMS连通性功能。运用使用两层ArcSDE体系结构并带有RDBMS 加密套接字协议层（Security Socket Layer，SSL），本地身份认证在可信赖的操作系统和RDBMS之间提供一个加密的通信渠道。

SSL是利用公钥加密技术覆盖整个网络的通信协议。它在客户端和服务器端建立了一个安全的通信渠道。RDBMS的加密功能将明码通信报文转换成在互联网领域传输的加密文本。每一个RDBMS与客户端产生的新会话都会创建一个新的公钥，以保证更强的安全保护。利用ArcSDE直连结构，通过将ArcSDE的功能从服务器端转移到客户端就免除了使用ArcSDE应用层的麻烦。通过将ArcSDE的功能从服务器端转移到客户端（动态链接库），客户端应用可利用RDBMS的客户端软件激活直接与RDBMS的通信。这给客户端应用提供重复利用由RDBMS提供的网络加密控制的性能。

IPSec是一组保证在ArcGIS客户端和RDBMS服务器在IP层面上进行数据包交换安全的协议。IPSec使用两组协议为IP通信提供安全控制：其一是认证报头（Authentication Header，AH），其二是压缩安全负载（Encapsulation Security Payload，ESP）。AH提供无连接的完整性、数据发起验证。ESP还可另外提供加密。

ArcGIS用户可以使用入侵侦察功能：基于网络的入侵侦察分析在网络上流动的数据包或者是在特定主机上基于主机的入侵监视。

要素层安全的执行与ArcSDE是并行的，它允许土地管理部门在要素层进行权限分配，以限制在空间Geodatabase对象的范围内访问数据。RDBMS要素层安全通过给一个表附加一个列用以给每个行分配安全级别来实现。根据这一列的值，RDBMS可通过已制定好的策略来决定是否发出请求的用户有权使用相关信息。如果安全级别相符，RDBMS允许访问数据，否则拒绝访问。

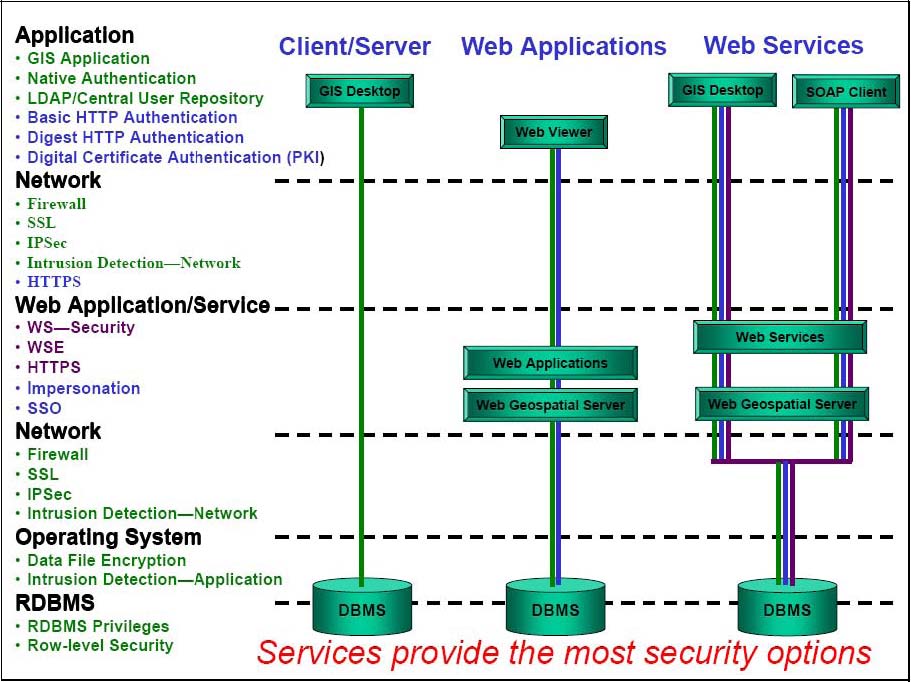
数据加密文件被用于ArcSDE直连结构，即使用附加在RDBMS中与ArcGIS产品协调工作的数据加密，这些产品作为数据仓库、自定义AO开发和自定义非基于ESRI技术应用等身份来访问RDBMS。自定义非基于ESRI技术应用是通过ArcSDE C和Java APIs来访问无版本数据。

RDBMS特权，RDBMS同时给用户和角色分配选择、更新、插入和删除（SELECT, UPDATE, INSERT and DELETE）权限。ArcSDE命令行和ArcCatalog相互利用RDBMS权限分配功能并为管理员提供分配权限的接口。

HTTP身份认证是一种安全机制，它使用HTTP身份认证方式来核实用户身份。与ArcGIS Web应用相整合的HTTP身份认证的标准方式是基础的、分类的、形式的和客户端的证书形式。基础的身份认证包括保护HTTP资源，要求客户端提供用户名和密码才能访问相应的资源。分类式身份认证也包括通过客户端提供用户名和密码来保护HTTP资源，同时分类机制通过客户端为服务器提供密码。基于形式的身份认证与基础的身份认证基本相同，不同之处是应用程序使用标准的HTML形式提供身份认证接口。客户端身份认证是最安全的身份认证方式，因为它通过有组织的公钥基础设施环境为客户端和服务器端提供和认证数字证书。

### 系统安全策略

当今的商业系统运行很容易受到各种信息安全的威胁。这些威胁产生于友好的或非友好的来源，也可能是国内的用户，也可能是国外的用户。这些威胁可能源于有意也可能源于无意，但不论那种情况，他们都会导致资源损失，都会危及到关键信息，甚至是使服务瘫痪。下图提供了C/S模式、WEB模式和Web服务模式下可用的安全选项。



图–1与ArcGIS安全体系结构

#### 客户/服务器体系结构

桌面或者是网络操作系统都根据预定义的系统访问权限要求用户身份认证和密码。网络包括防火墙，以约束和监视通信内容、建立信息流访问标准的不同层次。数据包通过加密（Secure Sockets Layer，SSL）以拒绝没有通过身份认证的信息访问，即使在传输过程中数据被捕获或丢失。在限制数据流的服务器（IPSec）和各种信息源之间建立特殊内容交换标准。监视通信活动可鉴别克服安全保护的企图。硬盘上的数据就会避免删除或不恰当的访问而得以保全。数据库环境提供了访问控制（权限）和连续级别（row-level）安全。综合所有这些安全技术，能为所有的信息流提供安全保护。

#### Web应用体系

标准的防火墙、SSL、IPSec、入侵侦察、数据文件加密及RDBMS安全策略同样支持网络操作。另外，还可以通过保护和控制HTTP通信来实现。基础或形式身份认证以及数字证书（PKI）的应用促进了安全通信的发展，并支持受限制的用户访问发布的网络应用。安全HTTP协议（HTTPS）加密数据传输，以支持高水平通信安全保护。网络应用能假定用户访问数据的权限、假定通过数据库访问用户身份认证的选择权。

#### 网络服务体系

当配置一个企业级面向服务架构，有最好的安全控制策略。由网络应用体系提供的保护支持面向服务架构（SOA），同时附加的选择权可用来增强访问控制。客户端应用程序包括附加的安全要素，确保恰当的使用和控制。附加的网络服务安全（Web Services Security，WS-Security）解决方案可用来支持用户身份认证，约束访问网络服务。网络服务扩展（Web Services Extensions， WSE）是特殊的网络安全机制，通过网络服务器技术支持。安全HTTP通信加密数据传输，提高通信安全。

### 选择正确的安全解决方案

安全解决方案对于每一个客户端都是唯一的，正确的安全解决方案取决于企业的任务和控制的选择，关键是实施合理恰当的安全控制。维持和支持当前安全任务评估、建立安全指导方针和安全控制、执行正在进行的安全审查以确保目标实现。

下图提供标准风险评价框架的列表，可用来开发和支持安全风险管理规划。这是由值得信任的行业专家提供的，包括Gartner的简单企业风险管理框架，微软为其中心客户提供的风险评价向导、国家标准与技术学会提供的安全认证和国家政府认定合格的基线。安全与价格同行。了解特定的安全风险并应用恰当的安全控制可降低总体费用，提供最可操作的解决方案。

# 安全体系建设方案 （yang）

## 安全现状分析

基础地理数据及数据服务平台项目将充分利用四川省现有的安全保障体系进行安全保障体系建设。

### 应用安全现状

目前的应用系统安全主要采取了以下措施：

**1、身份认证、访问控制：**大都基于操作系统或数据库管理系统的帐号和口令，大多数应用系统也是采用基于帐号和口令的身份认证技术，并通过对帐号授权进行访问控制。

**2、数据安全保护：**采用访问控制限制不同用户对信息的访问、使用和处理，实现对信息的安全保护。

**3、通用应用软件安全：**目前，对通用应用软件的安全主要从行政管理和安全配置两个方面保障，如对邮件帐号的统一管理等。

**4、安全审计：**基本上还是使用系统原有的审计功能，如操作系统日志、数据库管理日志、访问日志等。各日志的产生、使用、分析相互独立。

在应用方面还存在以下问题：

**部分应用系统审计功能不完善。**

**部分应用系统开发为采用安全编程方式，存在SQL注入漏洞。**

### 终端安全现状

主要采用的措施有：

**部署桌面安全审计系统，对桌面的行为进行审计和管理，并控制移动存储介质的使用。**

**安装统一的防病毒桌面终端，开启系统自带防火墙。**

**主要的问题有：**

**部分桌面终端的口令强度较弱或者没有设置口令。**

**部分桌面终端开启了较多的无关服务或者端口。**

**存在移动存储介质内外网混用情况。**

### 系统安全现状

基础地理数据及数据服务平台安全保障体系对操作系统和数据库管理系统的安全防范比较重视，各级系统操作人员也较重视系统安全，对系统按要求进行安全配置，及时了解系统安全漏洞的通告，并及时对系统进行升级，修补漏洞，在一定程度上降低了系统安全的风险。

### 网络安全现状

基础地理数据及数据服务平台安全保障体系的网络安全设计上主要采取了以下技术措施：

**1、隔离和访问控制**

在内部网络中，采用了虚拟子网（VLAN）技术，在一定程度上防范了不同行政部门间的非法访问。

在节点局域网与广域网的接入点布置防火墙，实现粗粒度的访问控制。

**2、信息传输加密**

在局域网节点尚无线路上传输数据的安全措施。

**3、网络安全评估和防范**

部分单位采购了网络漏洞扫描产品，发现安全漏洞及时采取措施，防范攻击者利用漏洞或后门。

**4、病毒防范**

各级局域网安装有病毒防护软件，通过安装不同的网络版和单机版病毒防护软件，及时进行升级和病毒代码库更新，降低了病毒的危害程度。

但在网络层面还存在部分不足之处：

网络架构方面：各个VLAN之间没有设定访问控制策略，可能造成各区域之间可以实现互访；部分区县局域网互联网服务区内网络架构比较简单，服务器未采用标准的三层架构部署，由于该区域内服务器的系统补丁和病毒库到互联网升级，造成WEB服务器和管理主机可直接访问互联网。

网络边界方面：网络边界，包括横向外联区域都部署了防火墙进行逻辑隔离，但都是单点部署，易造成单点故障；边界部署的防火墙虽然设定了访问控制策略，但访问控制策略粒度较粗；管理配置防火墙和IDS的主机可访问互联网。

### 物理安全现状

各机构对物理安全比较重视，在组织、管理、技术等多个层面采取了有效措施。在技术上主要有：

根据防灾的要求建设机房，为机房配备了消防器材，开辟了消防通道，防止灾害带来的安全事故。

设置了门禁和防盗监控装置，建立屏蔽室，按标准进行网络布线等，防止设备、信息的被盗和信息的泄露。

配置了UPS，对一些数据库服务器、网络线路等重要设备进行了冗余备份，提高了设备和系统的可靠性和可用性。

## 安全威胁与风险分析

根据对安全现状的缝隙，本方案将从基础地理数据及数据服务平台项目建设安全的角度出发，对项目中需要考虑的安全威胁与潜在安全风险进行分析，得出基于本项目的安全需求，并在后面的章节中对具体的安全方案设计内容进行阐述。

### 安全威胁分析

安全威胁是一种对系统、组织及其资产构成潜在破坏能力的可能性因素或者事件。可以说威胁是不可避免的，我们所采取的一切有效安全措施，皆是为了降低各种情况造成的威胁。

威胁可能源于对计算机系统直接或间接的攻击，例如非授权的泄露、篡改、删除等，在保密性、完整性或可用性等方面造成损害。威胁也可能源于偶发的、或蓄意的事件。一般来说，威胁总是要利用网络、系统、应用或数据的弱点才可能成功地对资产造成伤害。

在充分了解系统安全现状的前提下，对安全威胁进行了分类。下面将针对本项目重点考虑的八个方面威胁来源来确定所面临的安全威胁：

表 ‑1安全威胁来源

|  |  |
| --- | --- |
| 威胁来源 | 安全威胁描述 |
| 恶意代码和病毒 | 具有自我复制、自我传播能力，对计算机系统构成破坏的程序代码。 |
| 越权或滥用 | 通过采用一些措施，超越自己的权限访问了本来无权访问的资源；或者滥用自己的职权，做出破坏信息系统的行为。 |
| 黑客攻击技术 | 利用黑客工具和技术，例如侦察、密码猜测攻击、缓冲区溢出攻击、安装后门、嗅探、伪造和欺骗、拒绝服务攻击等手段对计算机系统进行攻击和入侵。 |
| 非授权访问 | 非授权用户登录系统，访问未授权信息。 |
| 假冒 | 用户身份被假冒，比如应急身份被假冒，发送假的应急信息。 |
| 泄密 | 保密泄漏，保密信息泄漏给他人比如：企业保密信息的泄漏将给企业带来巨大损失，更重要的是有损于政府形象，使用户在使用门户时有所顾虑，不利于执行上级的指导精神。 |
| 篡改 | 非法修改信息，破坏信息的完整性，比如：所提交的应急资源信息在网络传输过程中出现数据被截留、篡改。 |
| 抵赖 | 不承认收到的信息和所作的操作和交易，比如：一旦出现指挥命令下发出错，应急处置单位可能对行为进行抵赖、不承认。 |

### 本项目主要考虑的安全风险

对于基础地理数据及数据服务平台项目需要考虑的安全风险，将从物理层、网络层、主机层、数据层、桌面层和应用层的风险分析展开，重点描述本项目在应用和数据层面需要考虑的安全风险：

#### GIS平台层面风险分析

由于对现有GIS 平台的安全分析尚不够深入，现有GIS 平台安全漏洞暴露较少。尽管如此，GIS 平台自身的安全性也远非完全无懈可击。经分析，GIS 平台层的隐患主要有三：一是 GIS 平台自身的漏洞；二是GIS 与其他系统交互时所产生的漏洞；三是服务器系统设置差错，扩大普通用户使用权限，使用弱口令且长时间不进行更换，系统成分（包括用户）缺少健全的识别过程等；在管理制度上，系统管理人员缺少安全意识；在系统安全受到威胁时，缺乏完善的安全管理方法、步骤和安全对策（如事故通报、风险评估、改正安全缺陷等）；安全事故后缺乏损失评估、相应的补救恢复措施等。专门针对GIS 的病毒攻击。

#### 管理层面风险分析

GIS 作为操作系统、数据库平台之上的应用系统，操作人员众多，故其安全隐患比较严重，包括两个方面：在安全技术上，系统软硬件环境的配置、使用不当，数据库访问策略（分组、角色权限设置等）的隐患，WWW 服务器系统设置差错，扩大普通用户使用权限，使用弱口令且长时间不进行更换，系统成分（包括用户）缺少健全的识别过程等；在管理制度上，系统管理人员缺少安全意识；在系统安全受到威胁时，缺乏完善的安全管理方法、步骤和安全对策（如事故通报、风险评估、改正安全缺陷等）；安全事故后缺乏损失评估、相应的补救恢复措施等。

#### 应用层面风险分析

软件设施的脆弱性。软件设施的脆弱性主要表现在缺乏安全机制设计；如，访问控制大都采用帐号/口令机制。口令很容易被猜译或在传输中被截获。数据的保密性、完整性基本上依赖于系统帐号/口令的访问控制机制，对数据的保护都很弱。一旦口令被攻破，很容易造成数据的泄漏和破坏。软件代码没有安全保护措施，很容易被篡改、替换。

网络通信协议的安全缺陷。信息系统采用的TCP/IP协议以及Finger、FTP、Telnet、POP3、SMTP、DNS等应用服务协议都存在着许多安全缺陷，涉及到鉴别、访问控制、完整性、保密性等多方面内容，这些缺陷都是攻击者利用的目标。

应用系统中要特别注意web网站所带来的风险，一般的站点都存在SQL注入的漏洞。根据统计外部攻击事件占安全事件25%左右，而SQL注入攻击的事件就占外部攻击事件的80%左右。比如一名黑客通过Internet互联网利用SQL注入就可以得到这台web主站服务器的完全控制权限（比如可以添加、删除和修改主页上的任何新闻内容），进而利用这台服务器为跳板进入网络，进而对网络内的所有机器发动恶意攻击。

#### 数据层面风险分析

由于本项目会产生很多敏感数据，如果数据传输过程中无传输加密措施，就容易造成重要数据的泄漏。这包括：

各种移动存储媒体（如软盘、移动硬盘、USB盘、光盘等）在应用后得不到及时的管理，容易造成保密信息的外泄。

非法用户在利用身份窃取或假冒骗取系统的信任之后进行业务网数据盗取。应用系统中的敏感信息，一旦被窃取有可能带来极大的风险。

以非法手段窃得对数据的使用权，删除、修改或重发某些重要信息，以取得有益于攻击者的响应；恶意添加，修改数据，以干扰用户的正常使用。

#### 终端风险分析

对于本项目的终端用户来说，主要的安全风险有：

病毒传播：终端用户是病毒传播的主要来源之一，由于使用U盘、手机存储卡等移动介质或者自有笔记本电脑的私自介入将外来病毒带入。

浏览非法网站，使用BT或者迅雷下载数据，占用带宽、植入木马。

冒用别人身份进行非法访问，或者攻击内部网络等。

私自接入网络或者非法外联等。

擅自使用不安全的移动存储介质，造成信息外泄等。

#### 主机（系统）层面风险分析

特定的 GIS 总是构建于一定的操作系统之上（GIS 开发大都使用了操作系统所提供的应用程序接口），故其安全同操作系统健壮程度息息相关。没有操作系统层面的安全，而奢谈 GIS 的系统安全无疑是镜花水月。GIS 在操作系统层的安全隐患是操作系统自身的安全架构和操作系统中的核心应用程序。

主机（系统）层的安全风险主要从操作系统和数据库的安全风险进行分析：

操作系统的安全风险分析：操作系统面临的安全风险主要来自两个方面，一方面来自操作系统本身的脆弱性，另一方面来自对系统的使用、配置和管理上的安全风险。这些问题导致系统出现安全漏洞，使得黑客利用操作系统的一些BUG、后门取得对系统的非法操作权限。

数据库的安全风险分析：业务系统运行在数据库平台上，如果数据库安全无法保证，其上的应用系统也会被非法访问或破坏。数据库管理系统主要存在着脆弱的帐号设置，缺乏审计跟踪等方面的问题。空间数据库是存储、保护空间信息的一道重要屏障，但目前国内所使用的数据库产品均存在着一定的安全隐患；加上大多数系统管理员对数据库不熟悉而数据库管理员又对安全问题关心甚少， 使得空间数据库的安全隐患问题更加严峻。

#### 网络层面风险分析

网络与GIS 的融合给GIS 开发、安全带来的挑战是多方面的，信息网络的全球性、开放性、共享性和发展的动态性，使得Web方面的 GIS 应用快速拓展， 从传统的文件型地理数据传输、局域网登录等发展到网络地图信息服务、虚拟地理环境、网格计算等，基于Internet 的GIS 应用已具备跨应用协同能力，处于在线状态势必在安全上面对更多的挑战。现有的 GIS 应用系统网络服务大多构建在TCP/IP 协议（传输控制协议／网际协议）的基础上，而作为 Internet 的基石，TCP/IP 与UDP（用户数据报文协议）在制订时并没有着重考虑到通信路径的安全性，其安全体系结构比较薄弱：其中 TCP/IP 的大多数底层协议为广播方式，网上任何机器均有可能窃听到传输信息；且协议规则中只保证了信息无差错地传输，缺乏通信协议的基本安全机制，没有加密和身份认证等功能，在发送信息时常包含源地址、目标地址和端口号等信息；位于其上的应用服务如文件传输服务（FTP）、电子邮件服务（SMTP）等，大多也只提供简单的口令防护；其他如远程登录应用服务（Telnet）协议更是完全以明文方式进行数据传输。黑客即使不知道用户口令，只要在一个或多个节点安装“嗅探”（sniff）程序，即可轻而易举地侵入到系统中。

网络层是网络入侵者进攻信息系统的渠道和通路，许多安全问题都集中体现在网络的安全层面。

对基础地理数据及数据服务平台项目说，网络层的安全风险主要体现在：

（1）网络边界接入风险。网络边界的接入风险主要有各种非法入侵、对信息的侦听和截获、流量分析等，导致系统的破坏和敏感信息的泄漏。

（2）网络节点间数据传输风险。

#### 物理层面风险分析

物理层面是指整个网络中存在的所有的信息机房、通信线路、网络设备、安全设备等，这些设备面临着地震、水灾、火灾等环境事故以及人为操作失误或错误和各种计算机犯罪行为导致的破坏过程。这些事故一旦出现，就会使整个网络的正常运营遭到威胁，影响系统正常业务的开展，给应急管理带来业务上、声誉上乃至经济上的严重损失。

概括来本项目面临的物理层面风险如下：

环境安全风险。一些单位没有根据应用系统和设备的安全级别设置相应的安全区域并对安全区域进行相应的安全保护。

设备安全风险。主要存在设备可用性的安全风险，如有些计算机主机、外部设备、网络设备及其它辅助设备等缺乏有效的故障报警、诊断机制。

介质安全风险。介质由于霉变、电磁干扰、物理损伤等原因很可能会导致部分甚至全部数据的损坏。介质老化造成数据丢失和数据交换可靠性的降低。

就单机架构的GIS 而言，其硬件层安全隐患主要包括设备的稳定性、可用性；就B/S 架构的GIS 而言，还需要考虑到地理信息在网络传输中的硬件因素（如通信线路、网桥、交换机、路由器等）。就后者而言，从信息传输通道上讲，Internet／Intranet一般是以没有安全保障的公用电信网络作为硬件基础， 其物理上的脆弱性是显而易见的。此外，由于地理信息在网络上的传输是以数据包的形式进行，其稳定性取决于具体的网络流量状况，且通过哪些中间节点亦难以事先控制。因此，对于B/S 架构的GIS 而言，任何中间节点均可能拦截、读取，甚至破坏和篡改封包的信息。

## 安全需求分析

### GIS层平台安全需求

GIS平台安全需求：

（1）减少GIS 平台自身的漏洞。

（2）减少GIS 与其他系统交互时所产生的漏洞。

（3）加强抵御专门针对GIS 的病毒攻击。

### 管理层安全需求

GIS 管理安全策略如下：

（1） 建立完善的GIS安全管理策略。

（2） 树立 GIS 安全意识。

（3） 建立安全分工和全审核制度

### 应用层安全需求

基础地理数据及数据服务平台项目的应用安全需求主要包括身份认证、访问控制、安全审计及日志、密码技术及应用、web应用的防护五个部分。这些安全需求有些需要应用系统本身来实现，有些需要依靠应用系统之外的安全技术。

**用户身份认证**

这里的用户是一个比较宽泛的概念，不仅包括使用信息系统的系统使用者（人），还包括访问或者使用信息系统的其他系统或者主机、服务器等（系统、计算机）。

用户身份认证一般发生于用户登录系统时或者不同电子政务系统之间传递数据时的情况。在用户登录电子政务系统时，需要对登录用户持有的数字证书进行认证，以保证只有合法持有有效数字证书的用户才能够登录电子政务系统，同时还需要进行安全审计和记录系统安全日志。

**访问控制**

基础地理数据及数据服务平台项目中，需要指定各个应用层次中的每一个用户所能够访问的业务资源和系统资源，也即访问控制和权限分配策略。这里的权限不但包括用户能否访问的业务范围、业务数据、数据的访问方式、操作类型等，还包括电子政务系统相关的系统资源，包括打印机、邮件系统等。

在基础地理数据及数据服务平台项目需要建立统一的权限管理系统PMI，PMI系统主要分为授权管理中心（又称AA中心）和资源管理中心（又称RM中心）两部分。不仅能够解决面向单独业务系统的权限管理机制带来的权限定义和划分不统一、各访问控制点安全策略不一致、管理操作冗余、管理复杂等问题，还能够提高授权的可管理性，降低授权管理的复杂度和管理成本，提高整个系统的安全性和可用性。

**安全审计及日志**

用户登录到基础地理数据及数据服务平台项目要用完整的日志记录，日志记录需要包括谁、在什么时间、访问了什么资源、做了什么事情。审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。

**密码技术及应用**

根据安全级别的划分，需要采用包括数据加密与解密、数据摘要及验证、数字签名及验证、时间戳加盖及验证等在内的安全技术，保证系统的保密性、完整性和不可否认性。

**Web应用的防护需求**

基础地理数据及数据服务平台项目中要特别注意web应用所带来的风险，一般的网络应用都存在SQL注入和跨站攻击的漏洞。根据统计SQL注入攻击的事件就占安全事件的16%左右。

### 数据层安全需求

数据是基础地理数据及数据服务平台项目应用系统的核心部分，必须对其进行保护，使其免受内部威胁和外部威胁的侵害。安全体系结构的设计目标是为了保护信息的保密性、完整性和可用性。

保密性：基础地理数据及数据服务平台项目中有大量需要保护，不想向非授权用户公开的信息，如：领导有关个人信息或应急业务保密信息。保密性可以确保只有授权用户才可以访问这些信息，其具体的实现方法是在数据处理的每个阶段上强制执行必要的安全性级别，以防止信息的未授权公开。在数据处理的各个阶段（驻留在系统中时、在传输过程中驻留在网络间层上时，以及到达目的地后）都应该维护数据保密的一致性级别。

完整性：基础地理数据及数据服务平台项目中对敏感数据必须进行保护，以使其免受未授权修改、意外修改或是无意识修改的信息，如热点敏感信息、经济敏感数据和重点监控数据。数据完整性保护的实现方法是对信息的准确性和完全性以及数据的处理方法进行保护，以使其免受未授权修改的破坏。

可用性：基础地理数据及数据服务平台项目中会提供一些特定服务或具有一些特定信息，这些服务或信息都必须及时提供才能满足关键任务的要求或避免造成实际损失。这种服务或信息的示例有：应急服务信息、各种预案等。可用性可以确保授权个人能够及时可靠地访问应急有关数据和资源。

**1、数据访问控制与传输安全**

数据访问控制与传输安全成为基础地理数据及数据服务平台项目数据安全层面最为关注的问题之一。数据访问控制首先是对用户身份进行强身份验证，其次提供对高权限用户的限制、制定行列的安全以及制定数据分类访问等；数据传输安全通过网络加密的方式避免数据的被篡改和盗窃。

**2、数据备份与恢复安全需求**

随着基础地理数据及数据服务平台项目的开展，产生了许多重要而敏感的数据信息。这些数据构成了基础地理数据及数据服务平台最重要的信息资产。因此，必须建立相应的备份和灾难后快速恢复机制，以保障重要业务的连续性，对于数据备份与恢复的安全需求如下：

确定关键业务、应用系统及关键地点；

确定关键业务的可容忍恢复时间及恢复程度；

尽量缩短业务操作和资源遭受严重性破坏的时间；

降低灾难恢复任务的复杂性；

降低直接损失；

建立紧急事故恢复能力。

### 终端安全需求

基础地理数据及数据服务平台项目建成后，将会形成庞大的客户端群体，包括各个区县、市直部门及各个乡镇。客户端的安全直接关系到整个基础地理数据及数据服务平台 的安全。

客户端的安全需求如下：利用安全技术和桌面管理系统加强对办公终端的安全防护和监管力度，实现终端自身安全防护能力的提升、终端访问行为的监控和终端资产的管理，防止终端成为信息安全防护体系的“短板”。具体需求包括：

计算机准入控制

计算机的非法外连管理

USB设备管理

实名制管理

补丁管理

系统日常维护管理

身份认证系统

桌面防病毒系统

### 系统层安全需求

针对基础地理数据及数据服务平台项目，其系统安全的需求主要是从操作系统安全和数据库安全两个层面来分析。

操作系统的安全是基础地理数据及数据服务平台安全的基础。各种操作系统之上的应用要想获得运行的高可靠性和信息的完整性、保密性和可用性，必须依赖于操作系统提供的系统软件基础，任何脱离操作系统的应用软件的安全性都是不可能的。

基础地理数据及数据服务平台中许多关键的业务系统都运行在数据库平台上，如果数据库安全无法保证，其上的应用系统也会被非法访问或破坏。

依据系统风险，通过完善的系统安全机制以避免数据库管理系统存在的风险。

### 网络层安全需求

基础地理数据及数据服务平台信息化很大程度上依赖网络系统保障，网络安全主要分为传输网络安全和业务网络安全两类。对于基础地理数据及数据服务平台项目相关的传输网络，网络安全主要是保证综合业务管理系统、预案管理系统、应急处置系统等各个系统之间的数据传输网络以及公共网络服务的安全可靠运行。对于基础地理数据及数据服务平台项目的业务网络，网络安全主要包括控制拨号用户接入、设置防火墙、防范病毒、控制与公网互连、防范黑客入侵以及就网络安全进行严格监控和规范管理等以保护业务网络资源和应用服务。

针对基础地理数据及数据服务平台项目，网络层的安全需求主要解决以下几个方面的问题：

1、各级局域网应具有防止非法入侵的能力和鉴别通信对象的能力。

2、解决面向基础地理数据及数据服务平台项目的网络边界安全防护，根据基础地理数据及数据服务平台项目工程的网络特点，合理地配置防火墙、网络级入侵检测系统等网络边界防护设备，防止非法入侵，确保网络安全。

3、解决面向基础地理数据及数据服务平台项目的网络传输安全。由于数据交换网络化操作的不断增加，网上的通讯业务也随之大量增加，视网络结构设计分别选用网络传输加密方式或通过PKI（公钥基础设施）基础平台和安全应用支撑平台，来保证各类减灾救灾应急数据在网络传输过程中的安全。

### 物理层安全需求

物理安全是整个基础地理数据及数据服务平台安全的前提，用于保证计算机网络设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误和各种计算机犯罪行为导致的破坏。

针对基础地理数据及数据服务平台项目，物理层的安全需求将主要解决设备安全和媒体安全两个层面的安全问题。

设备安全则主要包括存储、传输或系统运行所用设备的防盗、防毁、防磁、防止线路截获、抗电磁干扰及电源保护等；

媒体安全则包括存储媒体本身的安全以及媒体中存储数据安全。

## 安全策略与措施

对加强地理信息系统安全的对策

（一 ）加大测绘法律法规宣传教育力度。加强地理信息管理制度建设，结合∀测绘法#和国家版图意识教育，加大宣传力度，深入开展测绘、保密等相关法律∃进机关、进乡村、进社区、进学校、进企业、进单位%，大力开展警示教育， 使从事地理信息生产、出版和服务的企事业树立依法测绘、依法经营、依法保密的意识，自觉遵守相关法律法规。

（二）重视地理信息系统安全管理工作。充分

认识地理信息系统安全管理工作的重要性和紧迫性，切实加强领导，建立健全机房安全、系统运行、人员管理、权限管理、数据备份等系统网络安全管理制度，落实定期数据备份责任制，提高安全防范水平。

（三）采取措施提高信息系统安全水平。采取适当有效的技术措施提高信息系统的安全防范水平。一是信息系统内外网应物理隔离，内网采用硬件防火墙将本单位与外单位或服务器端与客户端隔离，防止来自外部的非法入侵。二是要对不同系统应用架设备用的服务器， 确保不因某一系统应用出问题而影响全局的应用。三是数据库服务器存储可采用 RA ID1或 RA ID5阵列策略，防止因单个硬盘故障而导致系统崩溃以及数据丢失。四是通过磁带机、移动硬盘、DVD光盘等介质，做好定期异地数据备份。五是一旦发现地理信息系统有被攻击迹象或者已受到入侵破坏的，应当迅速采取措施予以修复，并及时向公安机关报告处理。

（四）严格规范获取、 提供和使用涉密地理信息行为。依法持有涉密地理信息的单位要强化安全保密措施，建立严格的登记管理制度，加强涉密计算机和存储介质管理，明确涉密岗位责任，防范他人非法获取涉密地理信息。需要对外提供涉密地理信息的，应按照法定审批程序进行。同时，在互联网上需要使用重要地理信息数据的，应当使用依法公布的重要地理信息数据。利用涉密测绘成果开发生产的。

基于现代信息安全理论，遵循国家标准，采用目前国内外先进的信息安全技术，根据安全体系框架以及基础地理数据及数据服务平台项目的安全定级，为基础地理数据及数据服务平台项目配置的安全策略如下：

强化保护措施，全面保障系统的保密性、完整性和可用性，增强防御能力，有效抵御来自互联网的各类非法入侵和攻击行为，运行管理符合国家信息安全相关法规、标准。

下面对采用的安全技术策略和对应的技术措施进行描述：

表 ‑1采用的安全技术策略和对应的技术措施

|  |  |  |
| --- | --- | --- |
| 安全技术策略 | | 技术措施 |
| 物理安全保护策略 | 设备安全 | 存储、传输或系统运行所用设备的防盗、防毁、防磁、防止线路截获、抗电磁干扰及电源保护 |
| 媒体安全 | 存储媒体本身的安全以及媒体中存储数据安全 |
| 网络安全策略 | 严格控制对内网、外网、外联网服务区的访问 | 采用防火墙作为边界隔离措施，实现不同网络边界的访问控制 |
| 恶意代码防范 | 采用病毒防治系统对网络与系统进行全方位保护 |
| 防止内部网络敏感信息泄露及传播 | 利用网络完全审计设备进行防护，通过日志服务存储和审计日志信息 |
| 防止非法内联、非法外连 | 利用非法外联监控和非法内接监控设备进行网络边界完整性检查 |
| 入侵防范 | 采用入侵检测设备进行防范 |
| 网络设备安全防范 | 采用两种或两种以上组合的鉴别技术进行身份鉴别 |
| 主机系统安全策略 | 主机系统资源访问控制 | 通过监控管理软件对主机的资源使用情况监视 |
| 防止非法帐号登录 | 对操作系统和数据库系统用户进行身份鉴别 |
| 对主机系统的访问控制 | 建立标记规则，并依据最小原则授权用户权限 |
| 对主机系统的入侵防范 | 部署入侵检测模块或防火墙设备 |
| 防止计算机病毒入侵主机 | 采用防病毒系统 |
| 对操作系统和数据的日志进行分析，查找非法调用 | 采用主机与数据库综合审计系统 |
| 应用安全策略 | 加强应用系统自身的强壮性 | 开发时对安全需求进行分析、采用安全架构设计 |
| 防止非法用户进入核心应用系 | 采用基于ＰＫＩ/KMI的统一身份认证体系及密码技术 |
| 防止进入系统的用户不受限制地访问系统中的对象 | 对已进入系统用户的各种访问操作进行访问控制；采用统一的权限管理机制管理用户授权 |
| Web安全防护 | 1、对SQL注入和跨站攻击进行实时监控  2、部署Web应用防火墙  3、安装网站防篡改软件 |
| 数据传输安全 | 根据业务单位的需要，采用加密机、VPN或者专线传输数据 |
| 防止数据丢失、错误和非法篡改 | 采用数据备份与恢复体系和相关技术 |
| 终端安全策略 | 对终端进行控制 | 采用内网管理系统的准入控制模块 |
| 防止计算机病毒进行对终端入侵 | 安装防病毒客户端 |
| 计算机非法外连管理 | 内网计算机杜绝私接设备访问互联网 |
| USB设备管理 | 对USB操作进行记录和审计，对违规情况采取报警或断网处理 |
| 实名制管理 | 绑定计算机及使用人，对违规计算机采取报警或断网处理 |
| 补丁管理 | 实现自动化分发系统安全补丁，提高整个网络安全 |
| 系统日常维护管理 | 采取统一运行及维护管理 |
| 身份认证 | 采用统一的基于PKI/KMI基础设施实现身份认证 |

## 安全方案设计

### GIS平台层安全设计

GIS 安全技术策略可以从以下几个方面加以考虑：

（1）设置用户名/口令体系：

用户名/口令体系是最基本的 GIS 安全防范技术，通过用户身份鉴别，可以防止大部分非法用户侵入和非授权用户对系统的访问。行之有效的用户名/口令策略包括：口令定期轮换；限制不必要的用户；经常性地测试账号；检查系统账户，删除不再使用的账户等。就 GIS 而言，可在四个层次上使用：开机口令、网络用户名/口令、GIS 应用系统用户名 /口令以及空间数据库管理系统用户名/口令。

（2）权限控制：

权限控制往往与用户名/口令体系相配套，且与GIS 管理的层次和权限相适应，以限定不同用户能够使用的系统功能和资源。可按照权限最小化原则，结合组织管理结构，制定GIS用户权限分配表现授权用户对授权对象的访问权限的定义、分配、回收和控制，及时发现系统安全薄弱环节。

（3）防火墙及防毒措施：

就连接到网络的GIS 而言（无论是否提供GIS网络服务），往往很容易受到恶意攻击和病毒的侵扰。防火墙是一种结合软硬件的访问控制技术，用于加强两个或多个网络间的边界防卫能力，通过用户定义的规则来判断数据包的合法性， 从而决定接受、丢弃或拒绝。其强大威力在于可以通过报告、监控、报警和登录到网络逻辑链路等方式把对网络和主机的冲击减少到最低限度。

（4）入侵检测（ IDS） ：

由于防火墙只是被动式的防御，且对网络内部人员攻击不具备防范能力。架构在防火墙之后的入侵检测系统能够实时监控成功穿过防火墙的数据包，自动检测可疑行为，分析来自网络外部入侵信号和内部的非法活动，分析攻击特征，在系统受到危害前发出警告，并对攻击做出实时的响应，并提供补救措施，以最大程度地保障系统安全。除此，在入侵检测系统中，还可配置蜜罐（ Honey- pot ），内存无用的空间信息，以吸引黑客注意力，收集攻击特征。

（5）数据加密：

CERT / CC 的研究表明，即使只经过最简单的数据加密，也可使得入侵成功率显著降低。数据加密使得网络上的敏感数据、文件与程序以密文方式存取，不易泄露或窃取，从而防止黑客对空间信息的伪造、冒充和篡改，提高了GIS 安全性。对于以非数据库形式储存的数据，可采用MD5、RSA 等加密算法，防止信息外泄。

### 管理层安全设计

管理层面的安全设计主要针对来自内部的不安全因素，如：安全机制不完善，内部人员保密意识较弱，组织机构、法律、标准、技术服务机制不健全等。确定了地理信息中心相关资料的密级范围之后，在尽量满足保密等级的情况下，管理层上要考虑四大环节：安全评估、安全策略、安全标准、安全审计，以保证涉密资料存放于一个安全环境中。具体的设计过程和内容如图1



图14.5-1管理层面安全设计图

建立安全体系的环节中安全评估必不可少，其目的，不仅在于明确潜在的危险,更重要的是为管理涉密资料提供基础和依据。作为评估直接输出，用于进行保密管理的安全整体框架应该明确。

综上具体的GIS 管理安全策略如下：

（1）确立GIS 安全目标。合理评价GIS 安全性级别，进行风险分析，明确安全需求和安全等级。在此基础上部署安全产品，进行入侵测试。

（2）树立 GIS 安全意识。从实际意义上讲，绝对安全的 GIS 是根本不存在的，只要系统还在使用，就或多或少存在着安全问题，只是程度不同而已。因此无论是领导层、管理层还是具体的执行层，都应加强风险意识，定期进行安全普查、安全业务培训，提高操作技能，以切实保障GIS 安全。（3）建立 GIS 安全管理制度。包括：机房管理制度：明确软硬件操作规程、GIS 运行规程等；责任分工制度：采用资产管理方法明确硬件设备的安全管理，结合权限控制明确 GIS 中各成员的系统。

（3）安全分工和全审核制度：对用户的行为监督管理，对 GIS 工作过程进行详尽的跟踪，记录用户活动，记录系统管理，监控和捕捉各种安全文件，维护管理审计记录和审计日志。如多次使用错误的口令试图进入系统，试图越权对某些程序或文件进行操作，审计跟踪可对这些操作时间，终端号及其他有关信息进行定位，以便发现和解决系统中出现的安全问题。（灾难恢复制度：结合责任分工制度明确GIS 安全事件后负责人员、恢复机制、方式、归档管理、硬件、软件等；）安全追踪制度：这是最为重要，也是最易被忽视的一环。管理人员（包括系统管理员 数据库管理员、系统安全员等）应及时追踪各操作系统、数据库及GIS开发商所发布的漏洞报告，及时打上各种补丁，保证GIS 的健壮性。

### 应用层安全设计

成都市CA已经实现政务数字证书的受理与发放，并建立基于数字证书技术的应用安全支撑平台，包括面向内部用户的统一认证管理系统、面向社会公众的认证服务系统、提供数据安全传输的密码服务系统和确保电子文件责任性的电子签章系统等部分，基础地理数据及数据服务平台各个应用系统将利用CA提供的可信认证、完整性保护、权限验证、责任认定等基本安全服务功能，实现各类应用系统的安全互联互通、安全信息共享、安全应用整合。

根据需要，基于CA集成来实现用户身份认证和系统安全，建立统一的身份认证系统，严格控制身份鉴别与授权和访问控制，在安全上采用多层面安全保障，以确保业务流程满足安全要求。

应用系统的安全必须以网络安全和系统安全为基础。在安全设计中应着重考虑以下几个方面：

认证与授权服务：应具有单独的登录控制模块对登录用户进行身份标识和鉴别，同时支持多种身份认证方式，如CA证书方式，用户名密码方式和多因子认证等其它认证方式。

程序资源访问控制安全：根据用户的身份和对系统的使用情况将用户分成不同的用户组；为不同的用户或用户组分配不同的系统资源（如对象、数据等）访问权限；用户只能访问到自己有权限访问的系统资源（如对象、数据等）。

功能性安全：明确各个功能的流程上的安全措施，如是否需要审核，文件上传最大限制等。

数据域安全：包括两个层次，其一是行级数据域安全，即用户可以访问哪些业务记录，一般以用户所在单位为条件进行过滤；其二是字段级数据域安全，即用户可以访问业务记录的哪些字段。

应用日志与审计：为关键的系统流程设计日志审计功能。日志中需记录用户对系统敏感资源（如保密数据或文件等）的访问情况；对过期的日志要进行备份，以便日后查阅。

#### 应用开发安全

应用开发安全主要从以下几个方面考虑：

**1、安全编程**

本项目中的所有应用系统都应正确选择程序设计语言和其它程序设计工具，从而提高最终产品的可靠性和正确性；为提高整个系统的安全性，要恰当地选择并利用这些工具帮助防止程序错误进入源编码。

严格采用软件工程的方法编制程序，对编码至少由一名未参与程序设计的程序员检查程序编码，全面了解其安全要点，他与原设计者对程序遗留问题负有同样的责任。

**2、接口安全**

应用系统接口是易受攻击的脆弱点，应从职责管理上加强，将责任实现最佳分离。基础地理数据及数据服务平台项目中涉及到的各类接口，都应尽量标准化，基于总局统一的接口标准规范定义接口，从而利于应用系统间信息的互通。

**3、数据传输的保密性**

对敏感数据以及与基础地理数据及数据服务平台交换的数据应采用加密传输技术以保证数据传输的保密性；必要时采用二次认证方式，实现对数据的保护。

**4、安全审计**

基础地理数据及数据服务平台项目的开发安全应考虑系统对安全审计的支持，审计模块至少包括以下内容：事件的日期、时间、发起者信息、类型、描述和结果等内容，审计记录的内容应当尽可能保证详细，以便事后问题的追踪和审计检查。

**5、安全测试**

在基础地理数据及数据服务平台项目核心征管系统软件与集成平台项目中，综合运用静态和动态检测技术，对软件的安全性进行全面认真的检测和评估，发现在系统设计和编码中的错误、疏忽和其它缺陷。

**6、系统开发安全管理**

建立管理体制包括建立防范组织、健全规章制度和明确职责任务三部分。管理体制是进行管理的基础，规章制度应在权限的分配过程中建立，并可根据需要参照执行。基础地理数据及数据服务平台项目应建立良好的管理体制并归档。

**7、支持外部安全控制措施的整合**

支持基于数字证书的身份认证、权限管理、传输加密、安全中间件的调转等外部控制机制的加入。

#### 身份认证

基于PKI基础设施提供应用系统的身份认证功能。通过安全基础设施，实现数字证书管理、权限管理、密钥管理、密码服务、证书查询与发布、可信时间戳服务等功能，在基础地理数据及数据服务平台项目中，形成统一的信任域和访问控制策略域，实现全系统统一的基于密码技术的身份认证和统一的细粒度访问控制，为全网提供身份认证、安全审计与责任认定、可信时间戳、加密密钥对生成、访问控制、数据保密、数据完整性保护、数据真实性保护、通信抗抵赖性保护等安全服务，提高系统整体的安全性以及安全系统的可控性与可管理性。

#### 访问控制

用户认证可以将非法用户拒绝于系统之外，但对计算机系统来说，不能因为允许一个用户进入系统后，就让他不受任何限制地访问系统中的所有程序、文件、信息等对象。从安全的角度出发，需要对已进入系统的用户的各种访问操作进行控制。同样，对进入网络中的用户也需要进行访问控制，主要体现在以下方面：

**1、防范非法用户的访问**

非法用户的访问也就是黑客或间谍的攻击行为。在没有任何防范措施的情况下，网络的安全主要是靠主机系统自身的安全，如用户名及口令字这些简单的控制。但对于用户名及口令的保护方式，对出于攻击目的人而言，他们可以通过对网络上信息的监听，得到用户名及口令，或者通过猜测获得用户及口令。因此，要采取一定的访问控制手段，防范来自非法用户的攻击，严格控制只有合法用户才能访问合法资源。

**2、防范合法用户的非授权访问**

合法用户的非授权访问是指合法用户在没有得到许可的情况下访问了他本不该访问的资源。一般来说，每个主机系统中，有一部分信息是可以对外开放的，而有些信息是要求保密或具有一定的隐私性。外部用户（指外部系统或网络合法用户）被允许正常访问一定的信息，但他同时通过一些手段越权访问了别人不允许他访问的信息，因此造成他人的信息泄密。所以，还得加强访问控制的机制，对服务及访问权限进行严格控制。

**3、防范假冒合法用户的非法访问**

从管理上及实际需求上是要求合法用户可正常访问被许可的资源。既然合法用户可以访问资源。那么，入侵者便会假冒合法用户的IP地址或用户名等资源进行非法访问。因此，必需从访问控制上做到防止假冒的用户访问。

#### 安全审计及日志管理

**1、安全审计**

审计是对网络上和系统中，与安全有关的重要活动进行监控、识别、记录、报警、响应的安全产品。它是能够提供更高应用层次、更高智能的安全手段。如今的网络和计算机系统虽然已经采用了一些安全防范措施，但仍然需要安全检测和审计产品，对重要的网上活动进行监视和记录，这样一旦系统瘫痪或者被入侵就能够进行侦破和取证，并能够发现安全防范系统的不足，加以改进。

安全审计系统可以对安全产品（如防火墙，IDS、AV等）、网络产品（如router、SWitch）、应用系统（如Web、 Mail）、操作系统（如Windows、 Linux、Unix）等产品和系统的日志信息统一进行收集并集中存储，同时采用先进的技术进行综合分析，检测出网络和系统中的安全隐患，以报警和直观的、可视化的方式显示出来，便于及时发现安全漏洞，采取有效措施，提高安全成效。

审计系统根据实际需要还会提供一些特殊的功能，如自学习、地址分析、服务类型分析、报文长度分析、流量分析、报文内容分析等智能分析模块。这些附加功能可以进一步满足计算机网络系统的特殊需要。

**2、日志管理**

系统要有完善的日志功能，保证操作员的每一笔操作都有据可查，记载任何进入系统的行为，包括对重要数据的修改情况，监测系统的运行，保证在数据发生问题时有据可查，避免个别人员的营私、舞弊行为。

对操作员的每一步操作都做日志记载。日志内容包括：哪个操作员、对哪个模块进行了什么操作，以及对一些重要数据表的操作前、操作后变化的记录，同时有日志查询功能，可以按用户要求对日志进行查询。

根据日志的功能，将日志分为功能日志和系统日志两类，下面将详细说明：

功能日志及实现

功能日志是指系统必须保存的，对系统中一些重要操作的记录。日志中需要记录操作人员、操作时间、操作的功能模块名称以及用户所执行的操作等等信息。记录和跟踪各种系统状态的变化，如提供对系统故意入侵行为的记录和对系统安全功能违反的记录。实现对各种安全事故的定位，如监控和捕捉各种安全事件，记录发生时间、发生地点和事件类型。同时，对于功能日志，同样要实现对日志的记录和查询功能。

对于功能日志，使用数据库来保存，并提供公共的API接口来实现日志的记录和查询功能。在每一个业务实现的时候，需要调用功能日志的API接口来添加功能日志。

系统日志及实现

系统日志主要用来记录程序的调试信息、启动和初始化状态、出错信息等；系统日志记录可以动态的记录在各种存储介质中，比如日志文件、数据库或者显示在控制台上等等。将系统日志分为三个等级，分别是DEBUG级别、INFO级别和ERROR级别。

DEBUG级别详细的记录程序的调试信息。该级别在调试程序时使用。

INFO级别详细的记录系统启动时的信息以及一些重要属性的加载信息。一般用在系统初始化和一些重要的属性初始化时使用。

ERROR级别详细的描述程序的出错信息和程序中捕获到的违例信息。用在出错和违例捕获时。

这三个级别的顺序是：ERROR > INFO > DEBUG。系统日志可以动态的调整需要记录的等级，比如：如果选择使用INFO级别，则日志文件中不会记录DEBUG级别的日志，而只记录INFO和ERROR级别的日志。

#### 权限管理

权限管理采用集中授权的工作模式，提供系统内的资源管理、用户角色定义和划分、权限分配和管理、权限认证等功能。权限管理主要是由管理员进行资源分类配置、用户角色定义及授权等操作；权限认证主要是根据用户身份对其进行权限判断，以决定该用户是否具有访问相应资源的权限。

权限管理与统一认证相结合，为基础地理数据及数据服务平台项目提供方便、简单的、可靠的授权服务，从而对内网用户进行整体的、有效的访问控制，保护系统内的资源不被非法或越权访问，防止信息泄漏。

权限管理应与统一认证相结合，由统一认证进行严格的身份认证，保证用户身份的真实性。

权限管理采用基于角色的访问控制策略，能够对用户和角色进行灵活授权。在定义角色时，可以采用职称、职务、部门等多种形式，灵活反映各种业务模式的管理需求。

#### 密码技术

密码服务应提供加解密、签名及签名验证、数字信封封装及解封等安全服务，以支持信息的保密性、完整性、真实性和不可抵赖性。客户端的密码服务由实体鉴别器提供，服务器端由加密服务器提供。密码服务系统要构建一个相对独立的可信计算环境。所有密码算法必须在经国家密码主管部门审批的密码设备上运行。

密码服务单元的密码算法采用国家密码主管部门审核批准的算法，密码算法由国家密码主管部门审核批准的专用密码设备实现，密钥运算都在密码硬件内实现。密钥加密存储在安全载体中或者密码服务系统的密码部件中，不以明文暴露在系统外。安全载体采用国家密码主管部门审核批准的安全载体。密码服务具有以下功能：

数据加解密的运算功能：提供对数据的加密和解密等运算功能，包括对称加解密，非对称加解密运算；

数据摘要和完整性验证：提供对数据进行摘要运算功能，并具有验证数据完整性功能。能够实现数字摘要算法功能，提供对数据进行摘要运算和验证摘要的功能；

数字签名和签名验证的运算功能，提供对数据的签名和签名验证等运算功能；

数字信封，提供对数据的数字信封（包括多证书的数字信封）封装和解封装等运算功能；

会话密钥生成和存储功能：提供指定长度的随机数功能，可以作为对称密钥和会话密钥；

提供对多密码算法的支持，用户根据国家密码主管部门的要求可以灵活地选择并配置合适的密码算法。

分布式计算功能，采用分布式计算技术，随着业务量的增加，灵活增加密码服务模块，实现性能动态按需平滑扩展，且不影响上层应用系统。

#### Web安全防护

对web安全防护将采用以下三种措施进行防范：

**1、利用IDS对SQL注入和跨站攻击进行实时监控，由防火墙进行阻断。**

**2、在Web服务器前部署Web应用防火墙，来防范来自应用层的风险。**

Web应用防火墙代表了一类新兴的信息安全技术，用以解决诸如防火墙一类传统设备束手无策的Web应用层安全问题。与传统防火墙不同，WAF工作在应用层，因此对Web应用防护具有先天的技术优势。基于对Web应用业务和逻辑的深刻理解，WAF对来自Web应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站站点进行有效防护。

**3、通过在重要Web服务器安装网站防篡改软件，实现对Web页面的保护。**

Web网页防篡改系统通过服务器文件访问底层驱动技术，对保护的对象（静态网页、动态执行脚本、文件夹）实时监测其属性，一旦发现更改立刻阻断非法篡改操作，阻止网页文件被修改，并实时通知管理客户端，如果发生文件篡改现象，系统也会自动从可信端进行恢复，彻底地保证了网页内容不被篡改。

#### 数据安全

**1、数据传输安全**

根据综合救灾减灾应急指挥业务特点，设计相应的数据传输策略以保证数据传输安全，主要包括：

关键业务数据传输安全：提供HTTPS的访问机制，采用SSL加速器解决访问性能；

批量数据传输安全：基于依据统一标准和规范构建数据交换平台以批量报文的方式完成机构之间的数据交换。对于异步数据传输，通过消息队列的数据恢复机制保证数据零丢失；

局域网内服务器和服务器之间的数据传输安全：采用SSH协议进行安全传输；

应急工作人员远程办公的安全访问：通过IP加密机接入业务专网。IP加密机最大的好处之一就是不需要安装客户端程序，远程用户可以随时随地从任何浏览器上安全的接入到内部网络，安全地访问应用程序，因此降低了管理员维护客户端的成本。利用IP加密机可实现：用户身份认证，防止外部人员非法接入，同时能够通过加密，保护在互联网上传输数据的安全。基于安全性的考虑，IP加密机设备部署在互联网接入区的防火墙的DMZ区。

**2、数据备份与恢复**

建立完整的冗余和备份策略。对于重要的网络节点和设备都应当实现冗余。备份包括本地、异地、实时等方式，也要根据每天、每周、每月等要求分别设定不同的备份内容和要求。

利用异地灾难备份中心，实现异地实时备份功能。

### 终端安全设计

**1、防病毒**

桌面的病毒防范可以利用现有防病毒系统进行安全防护。整个局域网需要统一使用网络版的病毒防护系统，便于升级和管理。针对恶意软件和ARP、蠕虫等网络病毒可以采用辅助工具来完成。

安装并开启个人防火墙，防止非法入侵计算机终端。

**2、计算机准入控制**

通过安全策略的制定，利用交换机的802.1x协议，实现设备准入控制。外来计算机接入局域网之前，要访问事先设置的修复服务器，符合修复服务器设置的安全策略后方可接入局域网，否则将对外来计算机进行修复。

通过桌面管理系统的准入控制功能实现安全准入管理。

**3、计算机的非法外连的管理**

对于内网的计算机，须杜绝私接设备访问互联网的情况。对于私自访问互联网的行为，系统管理员可以及时得到报警信息，便于管理员及时处理；对于该行为，可以通过系统向该违规用户发送告警信息，让该用户主动切断互联网连接，或采取中断互联网连接的策略，使其连接过程失效；

同时利用802.1x协议，对该计算机进行断网处理，使其无法访问局域网。

**4、USB设备管理**

由于客户端数据交换主要通过网络或USB设备进行拷贝，因此需要对USB设备进行细化管理，可以自动识别、控制接入的USB设备类型，控制USB设备的读写权限、读写方向，并对USB操作进行记录和审计，提高了客户端的安全性。同时配合802.1x协议，对违规计算机进行报警或断网处理。

**5、实名制管理**

通过实名制管理，可以绑定计算机与使用人，一旦出现问题，有利于快速定位并及时解决。同时配合802.1x协议，对违规计算机进行报警或断网处理。

**6、补丁管理**

实现自动化的分发系统安全补丁，提高整个网络的系统安全。同时配合802.1x协议，对不符合要求的计算机进行报警或断网处理。

**7、系统日常维护管理**

主要实现对终端电脑的统一的运行、维护管理，提高运行维护效率。包括：软/硬件信息自动收集管理，远程在线帮助，应用软件的统一分发、部署、升级等。

### 系统层安全设计

主机（系统）层的安全设计主要从操作系统和数据库两个方面来考虑。根据等级保护三级的防护要求，主要从以下几个方面对主机的安全进行防护：

**1、身份鉴别**

对登录操作系统和数据库系统的用户进行身份标识和鉴别，杜绝默认帐号，不合规则的帐号登录访问；操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施，三次登录失败帐号会被锁定。为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。

对服务器进行远程管理需要采用安全的模式，针对系统管理员除用户名和密码外，还需要采用数字证书或者UKEY等其他身份鉴别手段。

**2、访问控制**

建立标记规则，在服务器等实体资产上粘贴属性标签，文档介质类粘贴或打印密级等标记，对于电子数据使用文件名或文件注释进行标记。建立访问控制策略，依据最小原则授予用户权限，操作系统和数据库系统要使用不同的特权用户，对用户权限分配应当定期检查。

严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；及时删除多余的、过期的帐户，避免共享帐户的存在。

**3、安全审计**

由于开启操作系统和数据库的审计功能会影响系统的性能，建议在核心交换安全域配置主机数据库综合审计系统，以便于对主机和数据库信息进行审计。

**4、入侵防范**

部署主机防火墙设备或者主机防病毒软件中的入侵检测模块，监视外来的入侵行为并记录，定期进行系统升级和安全加固。

**5、恶意代码防范**

在主机上安装防病毒产品。

**6、资源控制**

Windows系统通过本地安全策略限制登录IP，Unix系统可通过TCP Wrapper工具进行访问IP限制。使用监控管理软件对服务器的CPU、硬盘、内存、网络等资源的使用情况进行监视，设置系统资源过低报警的门限值。

数据库系统安全

由于院地理信息中心的大多数服务目标是社会各界用户，并且数据来自很多方面，所以数据库的安全至关重要。数据库的安全保密的解决措施主要有以下几点：①加固数据库安全，及时打上安全补丁；

②系统管理员为数据库使用人员分配特定的账号

和密码，对“所有者”、“组”、“其他”三项内容设置严密

的权限；

③制订完善的口令策略；

④修改系统参数，限制对权限、角色、堆栈等内容

的调用；

（3）防病毒系统

目前市场上的各类防病毒软件产品功能已经非常完善，但是在整体病毒防护上，建议采用网关级硬件防火墙，这样可以保证整体的安全性，并提供中心全部网络范围的病毒防护。芜湖市勘测院地理信息中心的具体方案是：使用网神SecGate 3600-F3硬件防火墙和McAfee杀毒软件，建立以W indows2003为控制中心的管理模式，将病毒库升级的工作交给控制中心的

McAfee防病毒中心来做。

### 网络层安全设计

利用现有网络及安全设备，保证应急指挥平台系统的网络、数据、信息安全，政务机房既有防火墙、IPSEC VPN、SSL VPN、带宽管理、防病毒、入

侵防御、内容过滤等多种安全功能，并有网络杀毒软件，及时更新病毒库，时保障网络对最新病毒的查杀。

### 物理层安全设计

这里说的物理层安全指的是物理连接方面的安全，尤其是指不同密级之间的网络连接规范和要求，保证物理结构上的安全。主要包括以下几个内容：

（1）电力中断防护由于院地理信息中心拥有大量的设备，如网络设备、服务器、输入输出设备（扫描仪、打印机）、个人电脑等。所以电力供应非常重要，应准备两种不同源的电路，重要设备均要有双电源冗余设计。

（2）恶意的物理破坏防范

采用网管设备和监控系统对机房、档案库、重要设备以及出入口进行监视保护。办公地点采用门禁系统，利用身份卡进出人员身份的识别（有条件的单位可以采用指纹识别，如武汉市勘测设计研究院基础地理信息中心），防范外部人员的随意进入。对于作业人员的个人办公电脑，完全杜绝输入功能，以免从外部感染病毒或间谍程序。原则上不允许安装光软驱，已经安装的必须屏蔽；对BIOS设置密码，限制USB等输入接口的使用；不允许随意拆机，在网线水晶头、机箱锁等关键部位粘贴易碎标签，安排专人定期检查，一旦发现问题，及时上报院领导。设置专门的输出终端，专人管理，所有输出的数据必须经过审核，在指定的终端进行输出。

（3）电磁泄露保护

对于重要的，涉密的设备进行电磁泄露保护。

（4）安全旁路问题

安全旁路问题主要是限制和管理采用物理隔离的内部网络的人员拨号行为。

（5）设计安全拓扑结构

针对地理信息中心的运行网络环境，存在涉密网络与非涉密网络间的连接，也有内、外网的连接，拓扑结构复杂。应采取物理隔离方式，实行完全网络上的隔离，对于涉密网与非涉密网之间的连接，无设备相连。原则上办公单位与数据中心的连接均用防火墙进行逻辑隔离，保证可信的数据传输及对非法访问的拒绝。院内部网络的安全拓扑结构图所示。

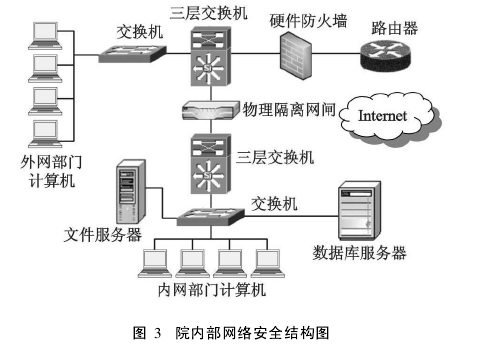


图14.5-2网络安全拓扑结构图