XX

等级保护（三级）建设方案

XXX 有限公司

目录

1 项目概述 1

2 等级保护建设流程 2

3 方案参照标准 4

4 信息系统定级备案 5

4.1 信息系统定级 5

4.1.1 定级结果 6

4.2 信息系统备案 7

5 系统安全需求分析 8

6 安全风险与差距分析 12

6.1 物理安全风险与差距分析 12

6.2 计算环境安全风险与差距分析 12

6.3 区域边界安全风险与差距分析 14

6.4 通信网络安全风险与差距分析 15

7 技术体系方案设计 17

7.1 方案设计目标 17

7.2 方案设计框架 17

7.3 安全域的划分 18

7.3.1 安全域划分的依据 18

7.3.2 安全域划分与说明 19

7.4 安全技术体系设计 19

7.4.1 机房与配套设备安全设计 19

7.4.2 计算环境安全设计 20

7.4.3 区域边界安全设计 28

7.4.4 通信网络安全设计 30

7.4.5 安全管理中心设计 33

8 安全管理体系设计 37

9 系统集成设计 39

9.1 软硬件产品部署图 39

9.2 安全产品部署说明 40

9.3 产品选型 43

9.2.1 选型建议 43

9.2.2 选型要求 43

1 项目概述

随着信息化的发展，YYY 的业务开展也越来越依托于网络平台，但纵观当前的安全形势，各种安全事件层出不穷，而 YYY 目前的网络中，安全设备较少，以前买的安全设备由于网络带宽升级，使用耗损等，其性能也渐渐不能满足 YYY 目前的网络安全需求，严重制约了 YYY 的信息化脚步。因此 YYY 希望加快信息化建设，以实现电子办公，执法信息网络公开化等。

通过对 YYY 信息化现状调研、分析，结合等级保护在物理安全、网络安全、主机安全、应用安全、数据安全、安全管理制度、安全管理机构、人员安全、系统建设、系统运维十个方面的要求，逐步完善信息安全组织、落实安全责任制，开展管理制度建设、技术措施建设，落实等级保护制度的各项要求，使得单位信息系统安全管理水平明显提高，安全保护能力明显增强，安全隐患和安全事故明显减少，有效保障信息化健康发展。

2等级保护建设流程

整体的安全保障体系包括技术和管理两大部分，其中技术部分根据《信息系统安全等级保护基本要求》分为物理安全、网络安全、主机安全、应用安全、数据安全五个方面进行建设；而管理部分根据《信息系统安全等级保护基本要求》则分为安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理五个方面。

整个安全保障体系各部分既有机结合，又相互支撑。之间的关系可以理解为"构建安全管理机构，制定完善的安全管理制度及安全策略，由相关人员，利用技术工手段及相关工具，进行系统建设和运行维护。"

根据等级化安全保障体系的设计思路，等级保护的设计与实施通过以下步骤进行：

1. 系统识别与定级：确定保护对象，通过分析系统所属类型、所属信息类别、服务范围以及业务对系统的依赖程度确定系统的等级。通过此步骤充分了解系统状况，包括系统业务流程和功能模块，以及确定系统的等级，为下一步安全域设计、安全保障体系框架设计、安全要求选择以及安全措施选择提供依据。

2. 安全域设计：根据第一步的结果，通过分析系统业务流程、功能模块，根据安全域划分原则设计系统安全域架构。通过安全域设计将系统分解为多个层次，为下一步安全保障体系框架设计提供基础框架。

3. 确定安全域安全要求：参照国家相关等级保护安全要求，设计不同安全域的安全要求。通过安全域适用安全等级选择方法确定系统各区域等级，明确各安全域所需采用的安全指标。

4. 评估现状：根据各等级的安全要求确定各等级的评估内容，根据国家相关风险评估方法，对系统各层次安全域进行有针对性的等级风险评估。并找出系统安全现状与等级要求的差距，形成完整准确的按需防御的安全需求。通过等级风险评估，可以明确各层次安全域相应等级的安全差距，为下一步安全技术解决方案设计和安全管理建设提供依据。

5. 安全保障体系方案设计：根据安全域框架，设计系统各个层次的安全保障体系框架以及具体方案。包括：各层次的安全保障体系框架形成系统整体的安全保障体系框架；详细安全技术设计、安全管理设计。

6. 安全建设：根据方案设计内容逐步进行安全建设，满足方案设计做要符合的安全需求，满足等级保护相应等级的基本要求，实现按需防御。

7. 持续安全运维：通过安全预警、安全监控、安全加固、安全审计、应急响应等，从事前、事中、事后三个方面进行安全运行维护，确保系统的持续安全，满足持续性按需防御的安全需求。

通过如上步骤，系统可以形成整体的等级化的安全保障体系，同时根据安全术建设和安全管理建设，保障系统整体的安全。而应该特别注意的是：等级保护不是一个项目，它应该是一个不断循环的过程，所以通过整个安全项目、安全服务的实施，来保证用户等级保护的建设能够持续的运行，能够使整个系统随着环境的变化达到持续的安全。

3 方案参照标准

- GB/T 21052-2007 信息安全等级保护 信息系统物理安全技术要求
- 信息安全技术 信息系统安全等级保护基本要求
- 信息安全技术 信息系统安全保护等级定级指南(报批中)
- 信息安全技术信息安全等级保护实施指南(报批中)
- 信息安全技术 信息系统安全等级保护测评指南
- GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求
- GB/T 20270-2006 信息安全技术 网络基础安全技术要求
- GB/T 20984-2007 信息安全技术 信息安全风险评估规范
- GB/T 20269-2006 信息安全技术 信息系统安全管理要求
- GB/T 20281-2006 信息安全技术 防火墙技术要求与测试评价方法
- GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法
- GB/T 20278-2006 信息安全技术 网络脆弱性扫描产品技术要求
- GB/T 20277-2006 信息安全技术 网络脆弱性扫描产品测试评价方法
- GB/T 20279-2006 信息安全技术 网络端设备隔离部件技术要求
- GB/T 20280-2006 信息安全技术 网络端设备隔离部件测试评价方法

等。

4信息系统定级备案

4.1 信息系统定级

确定信息系统安全保护等级的一般流程如下：

- 识别单位基本信息

  了解单位基本信息有助于判断单位的职能特点，单位所在行业及单位在行业所处的地位和所用，由此判断单位主要信息系统的宏观定位。

- 识别业务种类、流程和服务

  应重点了解定级对象信息系统中不同业务系统提供的服务在影响履行单位职能方面具体方式和程度，影响的区域范围、用户人数、业务量的具体数据以及对本单位以外机构或个人的影响等方面。这些具体数据即可以为主管部门制定定级指导意见提供参照，也可以作为主管部门审批定级结果的重要依据。

- 识别信息

  调查了解定级对象信息系统所处理的信息，了解单位对信息的三个安全属性的需求，了解不同业务数据在其保密性、完整性和可用性被破坏后在单位职能、单位资金、单位信誉、人身安全等方面可能对国家、社会、本单位造成的影响，对影响程度的描述应尽可能量化。

- 识别网络结构和边界

  调查了解定级对象信息系统所在单位的整体网络状况、安全防护和外部连接情况，目的是了解信息系统所处的单位内部网络环境和外部环境特点，以及该信息系统的网络安全保护与单位内部网络环境的安全保护的关系。识别主要的软硬件设备

- 调查了解与定级对象信息系统相关的服务器、网络、终端、存储设备以及安全设备等，设备所在网段，在系统中的功能和作用。调查设备的位置和作用主要就是发现不同信息系统在设备使用方面的共用程度。

- 识别用户类型和分布

  调查了解各系统的管理用户和一般用户，内部用户和外部用户，本地用户和远程用户等类型，了解用户或用户群的数量分布，判断系统服务中断或系统信息被破坏可能影响的范围和程度。

- 根据信息安全等级矩阵表，形成定级结果

业务信息安全等级矩阵表

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

系统服务安全等级矩阵表

系统服务安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

根据上述定级流程，YYY 各主要系统定级结果为：3 级

4.1.1 定级结果

根据上述定级流程，YYY 各主要系统定级结果为：

序号	系统名称	保护等级
1.	执行查看系统	**3**
2.	数字法院系统	**3**

4.2 信息系统备案

依据《信息系统安全等级保护定级指南》，确定信息系统的等级后，准备定级备案表和定级报告，协助用户单位向所在地区的公安机关办理备案手续。

第二级以上信息系统，在安全保护等级确定后 30 日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。运营使用单位或主管部门在备案时应填写《信息系统安全等级保护备案表》（以下简称《备案表》）提交有关备案材料及电子数据文件。定级工作的结果是以备案完成为标志。

受理备案的公安机关要公布备案受理地点、备案联系方式等。在受理备案时，应对提交的备案材料进行完整性审核和定级准确性审核。对符合等级保护要求的，应颁发信息系统安全等级保护备案证明。发现定级不准的，通知备案单位重新审核确定。

5 系统安全需求分析

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断，信息安全包括了保密性、完整性、可用性等特性，本方案将 YYY 公共服务平台从信息安全方面展开需求分析，使系统达到：在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难，以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭受损害后，能够较快恢复绝大部分功能。

随着信息化建设的不断推进，网络安全成为业务开展过程最重要的一环，对安全的特殊需求实际上就是要合理地解决网络开放性与安全性之间的矛盾。在确保单位信息畅通的基础上，有效阻止非法访问和攻击对系统的破坏。

安全风险特征主要取决于两个方面：一是其资产价值，二是其运行环境。安全风险主要来自网络、主机、应用和数据四个方面，从 YYY 当前网络整体安全角度出发，需要重点关注如下几个方面的安全建设：

- **终端感染木马、病毒**

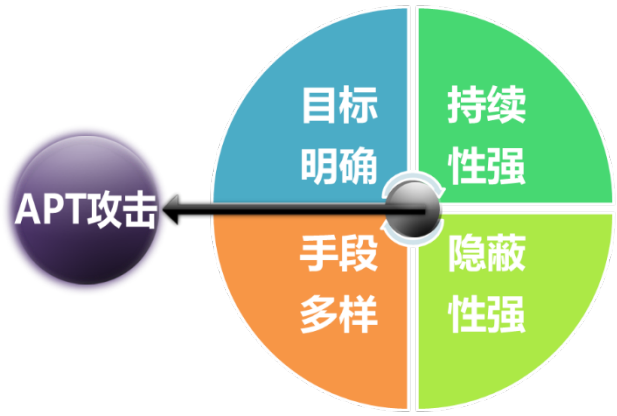
病毒、木马、蠕虫仍是局外网面临的最为迫切的安全防护需求，病毒木马蠕虫对终端的危害可能导致终端系统瘫痪、终端被控制、终端存储的信息被窃取、终端被引导访问钓鱼网站、终端成为僵尸网络甚至于终端被控制之后形成跳板攻击危害到终端具有权限访问的各类服务器。

- **终端系统漏洞**

终端感染病毒、木马、蠕虫等威胁是终端面临的主要威胁之一。而终端系统层面的漏洞被利用，会导致终端更严重的风险，比如终端被控制成为黑客攻击的跳板，或者终端成为僵尸网络的一部分，随时有可能发起针对内网的攻击。

◆ **APT 攻击不断渗透**

随着"火焰"蠕虫的爆发，高级持续性威胁（APT 攻击）受到业内的关注。APT 被称为高级持续性威胁，它是对特定目标进行长期、持续性网络入侵的攻击形式。在发动攻击之前，黑客会对攻击对象的业务流程和目标系统进行精确的情报收集，主动挖掘被攻击对象各种业务系统和应用程序的漏洞，并利用这些漏洞进入单位网络内部窃取所需的信息、产生特定的破坏。互联网出口往往是 APT 攻击切入的第一扇门，他们往往容易被黑客渗透之后对内网发起横向转移的攻击导致敏感信息被窃取、系统被控制所有行为都暴露在黑客的视野里。



◆ **系统漏洞风险问题**

黑客利用服务器操作系统漏洞、应用软件漏洞通过缓冲区溢出、恶意蠕虫、病毒等漏洞攻击，获取服务器权限、使服务器瘫痪导致服务器、存储等资源被攻

击的问题。

- **应用层攻击问题**

根据 Gartner 的统计报告显示，信息安全攻击有 75% 都是发生在 Web 应用层，针对 web 的攻击往往隐藏在大量的正常业务访问的行为中，传统的安全设备在应用层攻击防护上存在严重不足。

- **敏感信息泄漏问题**

这类安全问题主要利用 web 攻击、系统漏洞攻击等攻击手段操作后台数据库，导致数据库中储存的用户资料、身份证信息、账户信息、信用卡信息、联系方式等敏感信息被攻击者获取，从而产生巨大的经济损失。

- **带宽效率风险**

随着互联网的普及，YYY 的业务大多依托于互联网开展。但是在单位内部除了一些关键业务系统外，P2P 下载、网络炒股、游戏、视频等非关键业务应用同样共存着，形成了复杂的网络应用"脉络"。 YYY 通过租用运营商处的带宽满足业务需求，租用的带宽资源是有限的，如果不能对有限的带宽资源进行合理有效的管控，一方面用户的访问速度慢、访问体验得不到有效地满足，另一方面造成带宽资源利用率低的问题，因此 YYY 亟需一个方案解决带宽效率风险问题。

- **工作效率风险**

网络的普及改变了 YYY 的办公方式，而单位内总有部分用户在上班时间有意无意做与工作无关的网络行为，比如聊天、炒股、玩网游、看视频等，将办公室变成免费网吧，影响工作效率，从长远来看，会给 YYY 带来很大的财力损失，从而导致竞争力的下降。

- **法律风险**

目前，网络的违规违法事件越来越多，国家对于违规违法事件打击的力度越来越大，公安部 82 号令明文规定，凡是接入互联网的单位都必须具备审计的功能，记录用户的上网行为。单位职员通过组织网络，在论坛和博客发表反动、藏

独等不负责任的言论，在 QQ、MSN 等聊天过程中传播不雅信息，都属于网络的违规违法行为，一旦被公安部门查处，单位会因此而遭受法律的制裁。

- **安全快速的移动接入**

移动互联网技术的发展，使得单位办公方式多样化，部分领导出差或者员工不在办公区需要临时接入单位内网完成业务交付的需求越来越普遍。网络是信息化数据传输的载体，物联网的建设基础是互联网。目前的 WEB2.0 时代使得互联网的传输平台传输着各种各样的数据，互联网环境是一个没有太多规章制度来管理的大平台，如此一来，如果把单位内部十分重要的信息数据传输在这个互联网环境，很有可能会被黑客攻击窃取、篡改，也有可能遭到互联网中的威胁因素的侵害，影响网络办公。为了实现人们的远程办公，需要保证人员外出时可以安全访问单位内部网络进行日常操作，并确保数据的安全。因此必须在选择方法时，充分考虑多种接入方式以及各个接入方式的安全性，确保移动用户在接入内部网络时全面的安全保障。

- **业务稳定性需求**

YYY 公共服务平台业务系统承载于服务器，随着访问用户数量的增加，给单位的服务器带来越来越大的压力，如何有效的保证客户访问的速度和稳定性是目前 YYY 网络改造的重要目标。

6 安全风险与差距分析

6.1 物理安全风险与差距分析

物理安全风险主要是指网络周边的环境和物理特性引起的网络设备和线路的不可使用，从而会造成网络系统的不可使用，甚至导致整个网络的瘫痪。它是整个网络系统安全的前提和基础，只有保证了物理层的可用性，才能使得整个网络的可用性，进而提高整个网络的抗破坏力。例如：

- 机房缺乏控制，人员随意出入带来的风险；
- 网络设备被盗、被毁坏；
- 线路老化或是有意、无意的破坏线路；
- 设备在非预测情况下发生故障、停电等；
- 自然灾害如地震、水灾、火灾、雷击等；
- 电磁干扰等。

因此，在通盘考虑安全风险时，应优先考虑物理安全风险。保证网络正常运行的前提是将物理层安全风险降到最低或是尽量考虑在非正常情况下物理层出现风险问题时的应对方案。

6.2 计算环境安全风险与差距分析

计算环境的安全主要指主机以及应用层面的安全风险与需求分析，包括：身份鉴别、访问控制、系统审计、入侵防范、恶意代码防范、软件容错、数据完整性与保密性、备份与恢复、资源合理控制、剩余信息保护、抗抵赖等方面。

- **身份鉴别**

身份鉴别包括主机和应用两个方面。

主机操作系统登录、数据库登陆以及应用系统登录均必须进行身份验证。过

于简单的标识符和口令容易被穷举攻击破解。同时非法用户可以通过网络进行窃听，从而获得管理员权限，可以对任何资源非法访问及越权操作。因此必须提高用户名/口令的复杂度，且防止被网络窃听；同时应考虑失败处理机制。

- **访问控制**

访问控制包括主机和应用两个方面。

访问控制主要为了保证用户对主机资源和应用系统资源的合法使用。非法用户可能企图假冒合法用户的身份进入系统，低权限的合法用户也可能企图执行高权限用户的操作，这些行为将给主机系统和应用系统带来了很大的安全风险。用户必须拥有合法的用户标识符，在制定好的访问控制策略下进行操作，杜绝越权非法操作。

- **系统审计**

系统审计包括主机审计和应用审计两个方面。

对于登陆主机后的操作行为则需要进行主机审计。对于服务器和重要主机需要进行严格的行为控制，对用户的行为、使用的命令等进行必要的记录审计，便于日后的分析、调查、取证，规范主机使用行为。而对于应用系统同样提出了应用审计的要求，即对应用系统的使用行为进行审计。重点审计应用层信息，和业务系统的运转流程息息相关。能够为安全事件提供足够的信息，与身份认证与访问控制联系紧密，为相关事件提供审计记录。

- **入侵防范**

主机操作系统面临着各类具有针对性的入侵威胁，常见操作系统存在着各种安全漏洞，并且现在漏洞被发现与漏洞被利用之间的时间差变得越来越短，这就使得操作系统本身的安全性给整个系统带来巨大的安全风险，因此对于主机操作系统的安装，使用、维护等提出了需求，防范针对系统的入侵行为。

- **软件容错**

软件容错的主要目的是提供足够的冗余信息和算法程序,使系统在实际运行时能够及时发现程序设计错误，采取补救措施，以提高软件可靠性，保证整个计

算机系统的正常运行。

- **数据安全**

主要指数据的完整性与保密性。数据是信息资产的直接体现。所有的措施最终无不是为了业务数据的安全。因此数据的备份十分重要，是必须考虑的问题。应采取措施保证数据在传输过程中的完整性以及保密性；保护鉴别信息的保密性

- **备份与恢复**

数据是信息资产的直接体现。所有的措施最终无不是为了业务数据的安全。因此数据的备份十分重要，是必须考虑的问题。对于关键数据应建立数据的备份机制，而对于网络的关键设备、线路均需进行冗余配置，备份与恢复是应对突发事件的必要措施。

- **资源合理控制**

资源合理控制包括主机和应用两个方面。

主机系统以及应用系统的资源是有限的，不能无限滥用。系统资源必须能够为正常用户提供资源保障。否则会出现资源耗尽、服务质量下降甚至服务中断等后果。因此对于系统资源进行控制，制定包括：登陆条件限制、超时锁定、用户可用资源阈值设置等资源控制策略。

6.3 区域边界安全风险与差距分析

区域边界的安全主要包括：边界访问控制、边界完整性检测、边界入侵防范以及边界安全审计等方面。

- **边界访问控制**

YYY 公共服务平台业务系统可划分为如下边界：互联网接入边界、对外发布边界

对于各类边界最基本的安全需求就是访问控制，对进出安全区域边界的数据信息进行控制，阻止非授权及越权访问。

- **边界完整性检测**

边界的完整性如被破坏则所有控制规则将失去效力，因此需要对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查，维护边界完整性。

- **边界入侵防范**

各类网络攻击行为既可能来自于大家公认的互联网等外部网络，在内部也同样存在。通过安全措施，要实现主动阻断针对信息系统的各种攻击，如病毒、木马、间谍软件、可疑代码、端口扫描、DoS/DDoS 等，实现对网络层以及业务系统的安全防护，保护核心信息资产的免受攻击危害。

- **边界安全审计**

在安全区域边界需要建立必要的审计机制，对进出边界的各类网络行为进行记录与审计分析，可以和主机审计、应用审计以及网络审计形成多层次的审计系统。并可通过安全管理中心集中管理。

6.4 通信网络安全风险与差距分析

通信网络的安全主要包括：网络结构安全、网络安全审计、网络设备防护、通信完整性与保密性等方面。

- **网络结构**

网络结构是否合理直接影响着是否能够有效的承载业务需要。因此网络结构需要具备一定的冗余性；带宽能够满足业务高峰时期数据交换需求；并合理的划分网段和 VLAN。

- **网络安全审计**

由于用户的计算机相关的知识水平参差不齐，一旦某些安全意识薄弱的管理用户误操作，将给信息系统带来致命的破坏。没有相应的审计记录将给事后追查带来困难。有必要进行基于网络行为的审计。从而威慑那些心存侥幸、有恶意企图的少部分用户，以利于规范正常的网络应用行为。

- **网络设备防护**

由于 YYY 公共服务平台业务系统中将会使用大量的网络设备，如交换机、防火墙、入侵检测设备等。这些设备的自身安全性也会直接关系到涉密网和各种网络应用的正常运行。如果发生网络设备被不法分子攻击，将导致设备不能正常运行。更加严重情况是设备设置被篡改，不法分子轻松获得网络设备的控制权，通过网络设备作为跳板攻击服务器，将会造成无法想象的后果。例如，交换机口令泄漏、防火墙规则被篡改、入侵检测设备失灵等都将成为威胁网络系统正常运行的风险因素。

- **通信完整性与保密性**

由于网络协议及文件格式均具有标准、开发、公开的特征，因此数据在网上存储和传输过程中，不仅仅面临信息丢失、信息重复或信息传送的自身错误，而且会遭遇信息攻击或欺诈行为，导致最终信息收发的差异性。因此，在信息传输和存储过程中，必须要确保信息内容在发送、接收及保存的一致性；并在信息遭受篡改攻击的情况下，应提供有效的察觉与发现机制，实现通信的完整性。

而数据在传输过程中，为能够抵御不良企图者采取的各种攻击，防止遭到窃取，应采用加密措施保证数据的机密性。

- **网络可信接入**

对于一个不断发展的网络而言，为方便办公，在网络设计时保留大量的接入端口，这对于随时随地快速接入到 YYY 公共服务平台业务系统网络进行办公是非常便捷的，但同时也引入了安全风险，一旦外来用户不加阻拦的接入到网络中来，就有可能破坏网络的安全边界，使得外来用户具备对网络进行破坏的条件，由此而引入诸如蠕虫扩散、文件泄密等安全问题。因此需要对非法客户端实现禁入，能监控网络，对于没有合法认证的外来机器，能够阻断其网络访问，保护好已经建立起来的安全环境。

7 技术体系方案设计

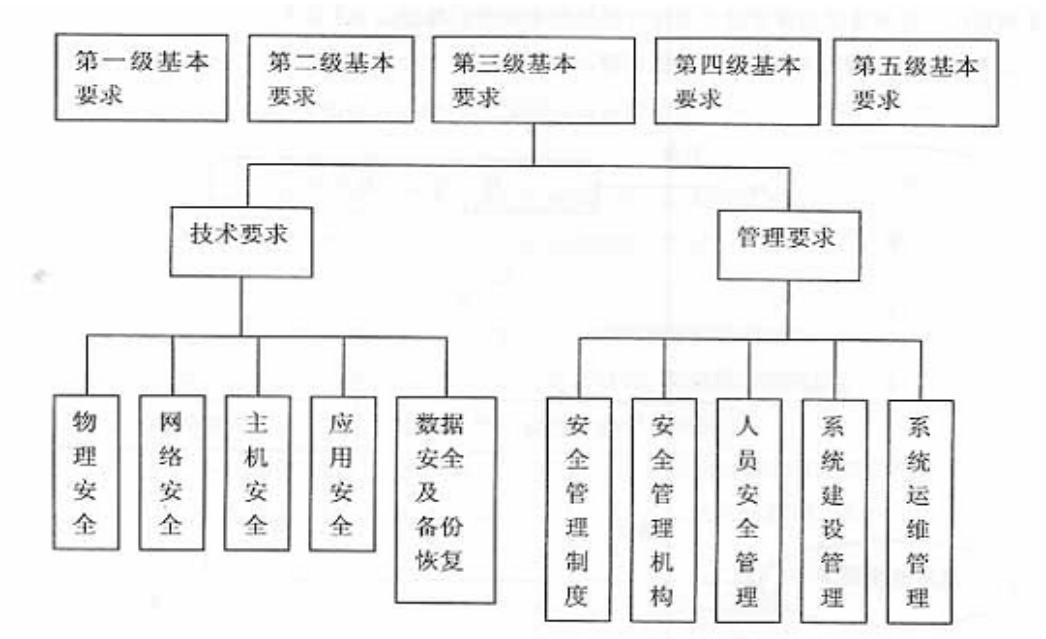
7.1 方案设计目标

三级系统安全保护环境的设计目标是：落实 GB 17859-1999 对三级系统的安全保护要求，在三级安全保护环境的基础上，通过实现基于安全策略模型和标记的强制访问控制以及增强系统的审计机制，使得系统具有在统一安全策略管控下，保护敏感资源的能力。

通过为满足物理安全、网络安全、主机安全、应用安全、数据安全五个方面基本技术要求进行技术体系建设；为满足安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理五个方面基本管理要求进行管理体系建设。使得 YYY 公共服务平台业务系统等级保护建设方案最终既可以满足等级保护的相关要求，又能够全方面为系统提供立体、纵深的安全保障防御体系，保证信息系统整体的安全保护能力。

7.2 方案设计框架

根据《信息系统安全等级保护基本要求》，分为技术和管理两大类要求，具体如下图所示：



本方案将严格根据技术与管理要求进行设计。首先应根据本级具体的基本要求设计本级系统的保护环境模型，**根据《信息系统等级保护安全设计技术要求》**，保护环境按照安全计算环境、安全区域边界、安全通信网络和安全管理中心进行设计，内容涵盖基本要求的 5 个方面。

7.3 安全域的划分

7.3.1 安全域划分的依据

对大型信息系统进行等级保护，不是对整个系统进行同一等级的保护，而是针对系统内部的不同业务区域进行不同等级的保护。因此，安全域划分是进行信息安全等级保护的首要步骤。

安全域是具有相同或相似安全要求和策略的 IT 要素的集合，是同一系统内根据信息的性质、使用主体、安全目标和策略等元素的不同来划分的不同逻辑子网或网络，每一个逻辑区域有相同的安全保护需求，具有相同的安全访问控制和边界控制策略，区域间具有相互信任关系，而且相同的网络安全域共享同样的安全策略。当然，安全域的划分不能单纯从安全角度考虑，而是应该以业务角度为主，辅以安全角度，并充分参照现有网络结构和管理现状，才能以较小的代价完成安全域划分和网络梳理，而又能保障其安全性。对信息系统安全域（保护对象）的划分应主要考虑如下方面因素：

1. 业务和功能特性

- 业务系统逻辑和应用关联性
- 业务系统对外连接：对外业务，支撑，内部管理

2. 安全特性的要求

- 安全要求相似性：可用性、保密性和完整性的要求，如有保密性要求的资产单独划区域。
- 威胁相似性：威胁来源、威胁方式和强度，如第三方接入区单独划区域。
- 资产价值相近性：重要与非重要资产分离，如核心生产区和管理终端区

分离。

3. 参照现有状况

- 现有网络结构的状况：现有网络结构、地域和机房等
- 参照现有的管理部门职权划分

7.3.2 安全域划分与说明

根据 YYY 公共服务平台业务系统的实际情况，将安全域划分为如下几个：

- 互联网接入域：互联网接入域主要为内网用户部分和业务应用部分提供互联网接入访问支撑。
- 对外发布服务域：业务人员提供业务系统的访问。

7.4 安全技术体系设计

7.4.1 机房与配套设备安全设计

机房与配套设备安全策略的目的是保护网络中计算机网络通信有一个良好的电磁兼容工作环境，并防止非法用户进入计算机控制室和各种偷窃、破坏活动的发生。

- **机房选址**

机房和办公场地选择在具有防震、防风和防雨等能力的建筑内。机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。

- **机房管理**

机房出入口安排专人值守，控制、鉴别和记录进入的人员；

需进入机房的来访人员须经过申请和审批流程，并限制和监控其活动范围。

对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；

重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

- **机房环境**

合理规划设备安装位置，应预留足够的空间作安装、维护及操作之用。房间装修必需使用阻燃材料，耐火等级符合国家相关标准规定。机房门大小应满足系统设备安装时运输需要。机房墙壁及天花板应进行表面处理，防止尘埃脱落，机房应安装防静电活动地板。

机房安装防雷和接地线，设置防雷保安器，防止感应雷，要求防雷接地和机房接地分别安装，且相隔一定的距离；机房设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。配备空调系统，以保持房间恒湿、恒温的工作环境；在机房供电线路上配置稳压器和过电压防护设备；提供短期的备用电力供应，满足关键设备在断电情况下的正常运行要求。设置冗余或并行的电力电缆线路为计算机系统供电；建立备用供电系统。铺设线缆要求电源线和通信线缆隔离铺设，避免互相干扰。对关键设备和磁介质实施电磁屏蔽。

- **设备与介质管理**

为了防止无关人员和不法分子非法接近网络并使用网络中的主机盗取信息、破坏网络和主机系统、破坏网络中的数据的完整性和可用性，必须采用有效的区域监控、防盗报警系统，阻止非法用户的各种临近攻击。此外，必须制定严格的出入管理制度和环境监控制度，以保障区域监控系统和环境监控系统的有效运行。对介质进行分类标识，存储在介质库或档案室中。利用光、电等技术设置机房防盗报警系统；对机房设置监控报警系统。

7.4.2 计算环境安全设计

7.4.2.1 身份鉴别

身份鉴别可分为主机身份鉴别和应用身份鉴别两个方面：

主机身份鉴别：

为提高主机系统安全性，保障各种应用的正常运行，对主机系统需要进行一系列的加固措施，包括：

- 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，且保证用户名的唯一性。
- 根据基本要求配置用户名/口令；口令必须具备采用 3 种以上字符、长度不少于 8 位并定期更换；
- 启用登陆失败处理功能，登陆失败后采取结束会话、限制非法登录次数和自动退出等措施。
- 远程管理时应启用 SSH 等管理方式，加密管理数据，防止被网络窃听。
- 对主机管理员登录进行双因素认证方式，采用 USB key+密码进行身份鉴别

应用身份鉴别：

为提高应用系统系统安全性应用系统需要进行一系列的加固措施，包括：

对登录用户进行身份标识和鉴别，且保证用户名的唯一性。

根据基本要求配置用户名/口令，必须具备一定的复杂度；口令必须具备采用 3 种以上字符、长度不少于 8 位并定期更换；

启用登陆失败处理功能，登陆失败后采取结束会话、限制非法登录次数和自动退出等措施。

应用系统如具备上述功能则需要开启使用，若不具备则需进行相应的功能开发，且使用效果要达到以上要求。

对于三级系统，要求对用户进行两种或两种以上组合的鉴别技术，因此可采用双因素认证（USBkey+密码）或者构建 PKI 体系，采用 CA 证书的方式进行身份鉴别。

7.4.2.2 访问控制

三级系统一个重要要求是实现自主访问控制和强制访问控制。自主访问控制实现：在安全策略控制范围内，使用户对自己创建的客体具有各种访问操作权限，并能将这些权限的部分或全部授予其他用户；自主访问控制主体的粒度应为用户级，客体的粒度应为文件或数据库表级；自主访问操作应包括对客体的创建、读、写、修改和删除等。 强制访问控制实现：在对安全管理员进行严格的身份鉴别和权限控制基础上，由安全管理员通过特定操作界面对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制；强制访问控制主体的粒度应为用户级，客体的粒度应为文件或数据库表级。

由此主要控制的是对应用系统的文件、数据库等资源的访问，避免越权非法使用。采用的措施主要包括：

启用访问控制功能：制定严格的访问控制安全策略，根据策略控制用户对应用系统的访问，特别是文件操作、数据库访问等，控制粒度主体为用户级、客体为文件或数据库表级。

权限控制：对于制定的访问控制规则要能清楚的覆盖资源访问相关的主体、客体及它们之间的操作。对于不同的用户授权原则是进行能够完成工作的最小化授权，避免授权范围过大，并在它们之间形成相互制约的关系。

账号管理：严格限制默认帐户的访问权限，重命名默认帐户，修改默认口令；及时删除多余的、过期的帐户，避免共享帐户的存在。

访问控制的实现主要采取两种方式：采用安全操作系统，或对操作系统进行安全增强改造，且使用效果要达到以上要求。

7.4.2.3 系统安全审计

系统审计包含主机审计和应用审计两个层面：

主机审计：

部署终端安全管理系统，启用主机审计功能，或部署主机审计系统，实现对

主机监控、审计和系统管理等功能。

监控功能包括服务监控、进程监控、硬件操作监控、文件系统监控、打印机监控、非法外联监控、计算机用户账号监控等。

审计功能包括文件操作审计、外挂设备操作审计、非法外联审计、IP 地址更改审计、服务与进程审计等。审计范围覆盖到服务器上的每个操作系统用户和数据库用户；内容包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；审计记录包括事件的日期、时间、类型、主体标识、客体标识和结果等；保护审计记录，避免受到未预期的删除、修改或覆盖等。同时，根据记录的数据进行统计分析，生成详细的审计报表，

系统管理功能包括系统用户管理、主机监控代理状态监控、安全策略管理、主机监控代理升级管理、计算机注册管理、实时报警、历史信息查询、统计与报表等。

应用审计：

应用层安全审计是对业务应用系统行为的审计，需要与应用系统紧密结合，此审计功能应与应用系统统一开发。

应用系统审计功能记录系统重要安全事件的日期、时间、发起者信息、类型、描述和结果等，并保护好审计结果，阻止非法删除、修改或覆盖审计记录。同时能够对记录数据进行统计、查询、分析及生成审计报表。

部署数据库审计系统对用户行为、用户事件及系统状态加以审计，范围覆盖到每个用户，从而把握数据库系统的整体安全。

应用系统如具备上述功能则需要开启使用，若不具备则需进行相应的功能开发，且使用效果要达到以上要求。

7.4.2.4 入侵防范

针对入侵防范主要体现在主机及网络两个层面。

针对主机的入侵防范，可以从多个角度进行处理：

- 入侵检测系统可以起到防范针对主机的入侵行为；
- 部署漏洞扫描进行系统安全性检测；
- 部署终端安全管理系统，开启补丁分发功能模块及时进行系统补丁升级；
- 操作系统的安装遵循最小安装的原则，仅安装需要的组件和应用程序，关闭多余服务等；
- 另外根据系统类型进行其它安全配置的加固处理。

7.4.2.5 主机恶意代码防范

各类恶意代码尤其是病毒、木马等是对 YYY 公共服务平台业务系统的重大危害，病毒在爆发时将使路由器、3 层交换机、防火墙等网关设备性能急速下降，并且占用整个网络带宽。

针对病毒的风险，我们建议重点是将病毒消灭或封堵在终端这个源头上，在所有终端主机和服务器上部署网络防病毒系统，加强终端主机的病毒防护能力并及时升级恶意代码软件版本以及恶意代码库。

在 YYY 安全管理安全域中，可以部署防病毒服务器，负责制定和终端主机防病毒策略，在内网建立全网统一的一级升级服务器，由管理中心升级服务器通过互联网或手工方式获得最新的病毒特征库，分发到数据中心节点的各个终端服务器。在网络边界通过防火墙进行基于通信端口、带宽、连接数量的过滤控制，可以在一定程度上避免蠕虫病毒爆发时的大流量冲击。同时，防毒系统可以为安全管理平台提供关于病毒威胁和事件的监控、审计日志，为全网的病毒防护管理提供必要的信息。

7.4.2.6 软件容错

软件容错的主要目的是提供足够的冗余信息和算法程序,使系统在实际运行时能够及时发现程序设计错误,采取补救措施,以提高软件可靠性,保证整个计算机系统的正常运行。因此在应用系统软件设计时要充分考虑软件容错设计，包括：

提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；

具备自保护功能，在故障发生时，应用系统应能够自动保存当前所有状态，确保系统能够进行恢复。

7.4.2.7 数据完整性与保密性

目前，YYY 办公中传输的信息主要是涉密类型的数据，对信息完整性校验提出了一定的需求。

在外网接入系统中，将采用消息摘要机制来确保完整性校验，其方法是：发送方使用散列函数（如 SHA、MD5 等）对要发送的信息进行摘要计算，得到信息的鉴别码，连同信息一起发送给接收方，将信息与信息摘要进行打包后插入身份鉴别标识，发送给接收方。接收方对接收到的信息后，首先确认发送方的身份信息，解包后，重新计算，将得到的鉴别码与收到的鉴别码进行比较，若二者相同，则可以判定信息未被篡改，信息完整性没有受到破坏。通过上述方法，可以满足应用系统对于信息完整性校验的需求。而对于用户数据特别是身份鉴别信息的数据保密，应用系统采用密码技术进行数据加密实现鉴别信息的存储保密性。

在传输过程中主要依靠 VPN 系统可以来保障数据包的数据完整性、保密性、可用性。目前 VPN 的组建主要采用两种方式，基于 IPSEC 协议的 VPN 以及 基于 SSL 协议的 VPN。

IPSec VPN 适用于组建 site-to-site 形态的虚拟专有网络，IPSEC 协议提供的安全服务包括：

保密性——IPSec 在传输数据包之前将其加密．以保证数据的保密性。

完整性——IPSec 在目的地要验证数据包，以保证该数据包任传输过程中没有被修改或替换。完整性校验是 IPSEC VPN 重要的功能之一。

真实性——IPSec 端要验证所有受 IPSec 保护的数据包。

防重放——IPSec 防止了数据包被捕捉并重新投放到网上，即目的地会拒绝

老的或重复的数据包，它通过报文的序列号实现。

SSL VPN 适用于远程接入环境，例如：移动办公接入。它和 IPSEC VPN 适用于不同的应用场景，可配合使用。

SSL 的英文全称是“Secure Sockets Layer”，中文名为“安全套接层协议层”，它是网景（Netscape）公司提出的基于 WEB 应用的安全协议。SSL 协议指定了一种在应用程序协议（如 Http、Telenet、NMTP 和 FTP 等）和 TCP/IP 协议之间提供数据安全性分层的机制，它为 TCP/IP 连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证。

SSL 与 IPSec 安全协议一样，也可提供加密和身份验证安全方法，因此安全性上二者无明显差别。

SSL VPN 使用 SSL/HTTPS 技术作为安全传输机制。这种机制在所有的标准 Web 浏览器上都有，不用额外的软件实现。使用 SSL VPN，在移动用户和内部资源之间的连接通过应用层的 Web 连接实现，而不是像 IPSec VPN 在网络层开放的“通道”。SSL 对移动用户是理想的技术，因为：

- SSL 无需被加载到终端设备上
- SSL 无需终端用户配置
- SSL 无需被限于固定终端，只要有标准浏览器即可使用

产品部署方面，SSL VPN 只需单臂旁路方式接入。单臂旁路接入不改变原有网络结构和网路配置，不增加故障点，部署简单灵活，同时提供完整的 SSL VPN 服务。远程用户只需应用标准 IE 浏览器即可登陆网关，通过身份鉴别，在基于角色的策略控制下实现对企业内部资源的存取访问。远程移动用户只需打开标准 IE 浏览器，登陆 SSL VPN 网关，经过用户认证后即可根据分配给该用户的相应策略进行相关业务系统的访问。

7.4.2.8 备份与恢复

备份与恢复主要包含两方面内容，首先是指数据备份与恢复，另外一方面是关键网络设备、线路以及服务器等硬件设备的冗余。

数据是最重要的系统资源。数据丢失将会使系统无法连续正常工作。数据错误则将意味着不准确的事务处理。可靠的系统要求能立即访问准确信息。将综合存储战略作为计算机信息系统基础设施的一部分实施不再是一种选择，而已成为必然的趋势。

数据备份系统应该遵循稳定性、全面性、自动化、高性能、操作简单、实时性等原则。备份系统先进的特性可提供增强的性能，易于管理，广泛的设备兼容性和较高的可靠性，以保证数据完整性。广泛的选件和代理能将数据保护扩展到整个系统,并提供增强的功能，其中包括联机备份应用系统和数据文件，先进的设备和介质管理，快速、顺利的灾难恢复以及对光纤通道存储区域网（SAN）的支持等。

本地完全数据备份至少每天一次，且备份介质需要场外存放。

提供能异地数据备份功能，利用通信网络将关键数据定时批量传送至异地备用场地。

对于核心交换设备、外部接入链路以及系统服务器进行双机、双线的冗余设计，保障从网络结构、硬件配置上满足不间断系统运行的需要。

- 服务器负载均衡

应用高可用：实现多台服务器之间冗余——3 到 7 层的多种服务器健康检查

应用高性能：实现多台服务器性能叠加——4、7 层的多种负载均衡算法

应用可扩展：实现应用基于实际需求的性能调整——服务器平滑退出、平滑上线

降低服务器负载——TCP 连接复用、HTTP 缓存、SSL 卸载。

提升用户访问速度——TCP 单边加速、HTTP 缓存、压缩。

服务器状态、链路状态和用户行为可视化——各类报表功能、商业智能分析

- 链路负载均衡

（入站）解决外部用户跨运营访问造成的访问速度慢的问题——智能 DNS

（出入站）多条链路之间形成冗余，保障用户访问稳定性——链路健康状况检测

（出站）按需为内网用户选择合适的链路访问互联网,提升带宽资源利用率，减少带宽投资成本——多种链路负载算法、智能路由、DNS 透明代理

- 全局负载均衡：

实现多数据中心入站流量选路、精确为用户选择最佳（就近）站点。

7.4.3 区域边界安全设计

7.4.3.1 边界访问控制入侵防范与应用层防攻击

通过对 YYY 网络的边界风险与需求分析，在网络层进行访问控制需部署边界安全防护产品，该安全产品实现对边界的访问控制、入侵防范和恶意代码防范，因此该产品具有一下功能：

- 可以对所有流经该设备的数据包按照严格的安全规则进行过滤，将所有不安全的或不符合安全规则的数据包屏蔽，杜绝越权访问，防止各类非法攻击行为。
- 可面对越来越广泛的基于应用层内容的攻击行为，该设备还应具有能够及时识别网络中发生的入侵行为并实时报警并且进行有效拦截防护。
- 该设备还需提供完整的上网行为管理功能，可针对于内网对于外网的存取应用进行管理。可辨识多种类别如 IM / VoIP / P2P / FTP 等已知的网络应用软件，进而根据多种条件如 IP 群组、VLAN ID 等范围条件制订各种不同的管理策略，限制内网用户使用诸如：IM 软件、P2P 软件、在线游戏等互联网应用，通过技术手段规范上网行为，防止带宽滥用，阻止内网泄密。

部署边界安全防护设备时应特别注意设备性能，产品必须具备良好的体系架

构保证性能，能够灵活的进行网络部署。同时为使得达到最佳防护效果。另外，安全防护设备的防病毒库应该和桌面防病毒软件应为不同的厂家产品，两类病毒防护产品共同组成用户的立体病毒防护体系。

为能达到最好的防护效果，边界防护产品的事件库及时升级至最新版本至关重要。对于能够与互联网实现连接的网络，应对背带裤升级进行准确配置；对与不能与互联网进行连接的网络环境，需采取手动下载升级包的方式进行手动升级。

7.4.3.2 边界完整性检查

边界完整性检查核心是要对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查，维护网络边界完整性。通过部署终端安全管理系统可以实现这一目标。

终端安全管理系统其中一个重要功能模块就是非法外联控制，探测内部网中非法上互联网的计算机。非法外联监控主要解决发现和管理用户非法自行建立通路连接非授权网络的行为。通过非法外联监控的管理，可以防止用户访问非信任网络资源，并防止由于访问非信任网络资源而引入安全风险或者导致信息泄密。

- 终端非法外联行为监控

可以发现终端试图访问非授信网络资源的行为，如试图与没有通过系统授权许可的终端进行通信，自行试图通过拨号连接互联网等行为。对于发现的非法外联行为，可以记录日志并产生报警信息。

- 终端非法外联行为管理

可以禁止终端与没有通过系统授权许可的终端进行通信，禁止拨号上网行为。

7.4.3.3 边界安全审计

各安全区域边界已经部署了相应的安全设备负责进行区域边界的安全。对于流经各主要边界（重要服务器区域、外部连接边界）需要设置必要的审计机制，进行数据监视并记录各类操作，通过审计分析能够发现跨区域的安全威胁，实时

地综合分析出网络中发生的安全事件。一般可采取开启边界安全设备的审计功能模块，根据审计策略进行数据的日志记录与审计。同时审计信息要通过安全管理中心进行统一集中管理，为安全管理中心提供必要的边界安全审计数据，利于管理中心进行全局管控。边界安全审计和主机审计、应用审计、网络审计等一起构成完整的、多层次的审计系统。

7.4.4 通信网络安全设计

7.4.4.1 网络结构安全

网络结构的安全是网络安全的前提和基础，对于 YYY 网络，选用主要网络设备时需要考虑业务处理能力的高峰数据流量，要考虑冗余空间满足业务高峰期需要。网络各个部分的带宽要保证接入网络和核心网络满足业务高峰期需要。根据相应的需求，可以考虑部署广域网优化产品，优化链路质量，削减链路数据，更好的满足业务高峰期的需求。

其次，需要按照业务系统服务的重要次序定义带宽分配的优先级，在网络拥堵时优先保障重要主机。根据实际需求，部署流量管理系统，实现按照业务系统服务的重要次序来分配带宽，优先保障重要主机。

最后，合理规划路由，业务终端与业务服务器之间建立安全路径；绘制与当前运行情况相符的网络拓扑结构图；根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的网段或 VLAN。保存有重要业务系统及数据的重要网段不能直接与外部系统连接，需要和其他网段隔离，单独划分区域。

7.4.4.2 网络安全审计

网络安全审计系统主要用于监视并记录网络中的各类操作，侦察系统中存在的现有和潜在的威胁，实时地综合分析出网络中发生的安全事件，包括各种外部事件和内部事件。

在 YYY 交换机处并接部署网络行为监控与审计系统，形成对全网网络数据

的流量监测并进行相应安全审计，同时和其它网络安全设备共同为集中安全管理提供监控数据用于分析及检测。

网络行为监控和审计系统将独立的网络传感器硬件组件连接到网络中的数据会聚点设备上，对网络中的数据包进行分析、匹配、统计，通过特定的协议算法，从而实现入侵检测、信息还原等网络审计功能，根据记录生成详细的审计报表。

网络行为监控和审计系统采用旁路技术，不用在目标主机中安装任何组件。同时网络审计系统可以与其它网络安全设备进行联动，将各自的监控记录送往安全管理安全域中的安全管理服务器，集中对网络异常、攻击和病毒进行分析和检测。

7.4.4.3 网络设备防护

为提高网络设备的自身安全性，保障各种网络应用的正常运行，对网络设备需要进行一系列的加固措施，包括：

- 对登录网络设备的用户进行身份鉴别，用户名必须唯一；
- 对网络设备的管理员登录地址进行限制；
- 身份鉴别信息具有不易被冒用的特点，口令设置需 3 种以上字符、长度不少于 8 位，并定期更换；
- 具有登录失败处理功能，失败后采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
- 启用 SSH 等管理方式，加密管理数据，防止被网络窃听。
- 对于鉴别手段，三级要求采用两种或两种以上组合的鉴别技术，因此需采用 USB key+密码进行身份鉴别，保证对网络设备进行管理维护的合法性。

7.4.4.4 通信完整性与保密性

信息的完整性设计包括信息传输的完整性校验以及信息存储的完整性校验。

对于信息传输和存储的完整性校验可以采用的技术包括校验码技术、消息鉴别码、密码校验函数、散列函数、数字签名等。

对于信息传输的完整性校验应由传输加密系统完成。部署 VPN 系统保证远程数据传输的数据完整性。对于信息存储的完整性校验应由应用系统和数据库系统完成。

应用层的通信保密性主要由应用系统完成。在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；并对通信过程中的敏感信息字段进行加密。

对于信息传输的通信保密性应由传输加密系统完成。部署 VPN 系统保证远程数据传输的数据机密性。

7.4.4.5 网络可信接入

为保证网络边界的完整性，不仅需要进行非法外联行为，同时对非法接入进行监控与阻断，形成网络可信接入，共同维护边界完整性。通过部署终端安全管理系统可以实现这一目标。

终端安全管理系统其中一个重要功能模块就是网络准入控制，启用网络阻断方式包括 ARP 干扰、802.1x 协议联动等。

监测内部网中发生的外来主机非法接入、篡改 IP 地址、盗用 IP 地址等不法行为，由监测控制台进行告警。运用用户信息和主机信息匹配方式实时发现接入主机的合法性，及时阻止 IP 地址的篡改和盗用行为。共同保证 YYY 网络的边界完整性。具体如下：

- 在线主机监测

可以通过监听和主动探测等方式检测系统中所有在线的主机，并判别在线主机是否是经过系统授权认证的信任主机。

- 主机授权认证

可以通过在线主机是否安装客户端代理程序，并结合客户端代理报告的主机补丁安装情况，防病毒程序安装和工作情况等信息，进行网络的授权认证，只允许通过授权认证的主机使用网络资源。

- 非法主机网络阻断

对于探测到的非法主机，系统可以主动阻止其访问任何网络资源，从而保证非法主机不对网络产生影响，无法有意或无意的对网络攻击或者试图窃密。

- 网络白名单策略管理

可生成默认的合法主机列表，根据是否安装安全管理客户端或者是否执行安全策略，来过滤合法主机列表，快速实现合法主机列表的生成。同时允许管理员设置白名单例外列表，允许例外列表的主机不安装客户端但是仍然授予网络使用权限，并根据需要授予可以和其他授权认证过的主机通信的权限或者允许和任意主机通信的权限。

- IP 和 MAC 绑定管理

可以将终端的 IP 和 MAC 地址绑定，禁止用户修改自身的 IP 和 MAC 地址，并在用户试图更改 IP 和 MAC 地址时，产生相应的报警信息。

7.4.5 安全管理中心设计

由于 YYY 网络覆盖面广，用户众多，技术人员水平不一。为了能准确了解系统的运行状态、设备的运行情况，统一部署安全策略，应进行安全管理中心的设计，根据要求，应在系统管理、审计管理和安全管理几个大方面进行建设。

在安全管理安全域中建立安全管理中心，是有效帮助管理人员实施好安全措施的重要保障，是实现业务稳定运行、长治久安的基础。通过安全管理中心的建设，真正实现安全技术层面和管理层面的结合，全面提升用户网络的信息安全保障能力。

7.4.5.1 系统管理

通过系统管理员对系统的服务器、网络设备、安全设备、应用系统进行统一的管理包括：

- 用户身份管理：统一管理系统用户身份，按照业务上分工的不同，合理地把相关人员划分为不同的类别或者组，以及不同的角色对模块的访问权限。权限设置可按角色划分，角色分为普通用户、系统管理员、安全管理员、审计管理员等。
- 系统资源配置：进行系统资源配置管理与监控，包括 CPU 负载、磁盘使用情况、服务器内存、数据库的空间、数据库日志空间、SWAP 使用情况等，通过配置采样时间，定时检测。
- 系统加载和启动：进行系统启动初始化管理，保障系统的正常加载和启动。
- 数据备份与恢复：数据的定期备份与恢复管理，识别需要定期备份的重要业务信息、系统数据及软件系统，规定备份信息的备份方式、备份频度、存储介质、保存期等；根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，定期执行备份与恢复策略。
- 恶意代码防范管理：建立恶意代码管理中心，进行防恶意代码软件的统一管理。恶意代码管理中心实现：杀毒策略统一集中配置；自动并强制进行恶意代码库升级；定制统一客户端策略并强制执行；进行集中病毒报警等。
- 系统补丁管理：集中进行补丁管理，定期统一进行系统补丁安装。注意应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装。
- 系统管理员身份认证与审计：对系统管理员进行严格的身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

7.4.5.2 审计管理

通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括：根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等；对安全审计员进行严格的身份鉴别，并只允许其通过特定的命令或界面进行安全审计操作。

具体集中审计内容包括：

- 日志监视

实时监视接收到的事件的状况，如最近日志列表、系统风险状况等；监控事件状况的同时也可以监控设备运行参数，以配合确定设备及网络的状态；日志监视支持以图形化方式实时监控日志流量、系统风险等变化趋势。

- 日志管理

日志管理实现对多种日志格式的统一管理。通过 SNMP、SYSLOG 或者其它的日志接口采集管理对象的日志信息，转换为统一的日志格式，再统一管理、分析、报警；自动完成日志数据的格式解析和分类；提供日志数据的存储、备份、恢复、删除、导入和导出操作等功能。日志管理支持分布式日志级联管理，下级管理中心的日志数据可以发送到上级管理中心进行集中管理

- 审计分析

集中审计可综合各种安全设备的安全事件，以统一的审计结果向用户提供可定制的报表，全面反映网络安全总体状况，重点突出，简单易懂。

系统支持对包过滤日志、代理日志、入侵攻击事件、病毒入侵事件等十几种日志进行统计分析并生成分析报表；支持按照设备运行状况、设备管理操作对安全设备管理信息统计分析；支持基于多种条件的统计分析，包括：对访问流量、入侵攻击、邮件过滤日志、源地址、用户对网络访问控制日志等。对于入侵攻击日志，可按照入侵攻击事件、源地址、被攻击主机进行统计分析，生成各类趋势

分析图表。

系统可以生成多种形式的审计报表，报表支持表格和多种图形表现形式；用户可以通过 IE 浏览器访问，导出审计结果。可设定定时生成日志统计报表，并自动保存以备审阅或自动通过邮件发送给指定收件人，实现对安全审计的流程化处理。

7.4.5.3 监控管理

统一监控管理将集中进行系统安全监测，并为安全计算环境、安全区域边界、安全通信网络进行统一的监控与告警。

对全网的安全设备、安全事件、安全策略、安全运维进行统一集中的监控、调度、预警和管理。集中安全管理平台针对每个安全域的设备提供灵活的策略制定和管理，实现本安全域内的信息收集和处理。同时，在安全管理安全域中部署设备管理系统服务器和控制台，通过与各事件服务器组件或安全设备通信，实现整个网络的全局监控。

管理员在安全管理安全域的控制台上，可以集中的对设备的报警策略进行指定和下发，同时，监视可处理报警信息。安全管理平台可以以拓扑图的方式来直观清晰的显示设备关键属性和运行状态。

通过部署集中安全管理平台实现：安全事件的深度感知、安全事件的关联分析、安全威胁的协同响应。通过部署集中安全管理平台，提高安全管理的效率，保障网络的安全运行

8 安全管理体系设计

安全体系管理层面设计主要是依据《信息系统安全等级保护基本要求》中的管理要求而设计。分别从以下方面进行设计：

- 安全管理制度

根据安全管理制度的基本要求制定各类管理规定、管理办法和暂行规定。从安全策略主文档中规定的安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法，是具有可操作性，且必须得到有效推行和实施的制度。

制定严格的制定与发布流程，方式，范围等，制度需要统一格式并进行有效版本控制；发布方式需要正式、有效并注明发布范围，对收发文进行登记。

信息安全领导小组负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定，定期或不定期对安全管理制度进行评审和修订，修订不足及进行改进。

- 安全管理机构

根据基本要求设置安全管理机构的组织形式和运作方式，明确岗位职责；

设置安全管理岗位，设立系统管理员、网络管理员、安全管理员等岗位，根据要求进行人员配备，配备专职安全员；成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

建立授权与审批制度；

建立内外部沟通合作渠道；

定期进行全面安全检查，特别是系统日常运行、系统漏洞和数据备份等。

- 人员安全管理

根据基本要求制定人员录用，离岗、考核、培训几个方面的规定，并严格执

行；规定外部人员访问流程，并严格执行。

- 系统建设管理

根据基本要求制定系统建设管理制度，包括：系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级评测、安全服务商选择等方面。从工程实施的前、中、后三个方面，从初始定级设计到验收评测完整的工程周期角度进行系统建设管理。

- 系统运维管理

根据基本要求进行信息系统日常运行维护管理，利用管理制度以及安全管理中心进行，包括：环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等，使系统始终处于相应等级安全状态中。

9 系统集成设计

9.1 软硬件产品部署图

系统改造前拓扑图如下：

本次系统改造新增软硬件产品后的拓扑图如下：

9.2 安全产品部署说明

外网设备			
部署产品	**数量**	**部署位置**	**部署作用**
网络审计系统			✧ 审计内网用户上网行为，可供公安部 82 号令要求 ✧ 封堵与办公无关应用，提高员工办公效率 ✧ 管理内部网络带宽，合理分配流量，保障核心业务流量
下一代防火墙			✧ 保护安全管理区设备的安全 ✧ 对业务网进行独立防护，进行访问控制、攻击防御
入侵检测			✧ 对入侵行为的检测。它通过收集和分析网络行为、安全日志、审计数据、等信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。 ✧ 积极主动地安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护
WAF			✧ WEB 应用防护，防止 web 业务被破坏、篡改 ✧ 对传输数据进行内容检测，保障数据安全，防泄密
防火墙			✧ 做安全隔离，隔离看守所与内部网络 ✧ 进行访问控制、攻击防御
隔离安全网关			✧ 隔离办公网与专网
负载均衡			✧ 服务器负载 ✧ 服务健康检查

服务器虚拟化			✧ 将服务器虚拟化后，可备份数据 ✧ 可将服务器资源最大化利用
SSL VPN			✧ 移动办公安全接入
内网设备			
下一代防火墙			✧ 保护安全管理区设备的安全 ✧ 对业务网进行独立防护，进行访问控制、攻击防御
入侵检测系统			✧ 对入侵行为的检测。它通过收集和分析网络行为、安全日志、审计数据、等信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。 ✧ 积极主动地安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护
集中管理设备			✧ 统一管理内网安全设备，可实时监控
入侵防御系统			✧ 实时监控并阻断针对数据中心核心 HIS 业务服务器的入侵行为 ✧ 边界集中进行病毒过滤，防止病毒侵入扩散，与网络防病毒组成多层次深度防御。
负载均衡			✧ 服务器负载 ✧ 服务健康检查
防火墙			✧ 做安全隔离，隔离看 3G 网络与执行查控服务器 ✧ 进行访问控制、攻击防御
服务器虚拟化			✧ 将服务器虚拟化后，可备份数据 ✧ 可将服务器资源最大化利用

堡垒机			✧ 管理网络中得所有安全设备
数据库审计系统			✧ 审计服务器里的数据库，以便责任做到追溯到人

9.3 产品选型

9.2.1 选型建议

根据国家有关法律法规，并结合 YYY 通信网络的实际要求。我们建议使用具有国内自主知识产权的产品，并且要完全符合 YYY 提出的产品资质要求：所有产品是经公安部、国家信息安全测评认证中心等国家权威测试通过，并获得安全产品销售许可证，是在国内政府机关、银行、部队、医疗卫生等系统采用较多，运行稳定的国产防火墙、上网行为管理、SSLVPN 等安全产品，在功能、性能与管理性等方面能够满足 YYY 计算机网络的需求。

9.2.2 选型要求

1、在产品选型时，需要厂家可以提供个性化的安全产品。只有这样才能保证系统的安全充分满足客户的现状，才能有针对的为用户的应用和业务提供安全保证。国内具有自主知识产权的安全产品可以随时根据用户的要求对产品进行相应的改进，使产品更加适合用户的实际需要，而不是一般的通用性产品。

2、采用可提供本地化服务的厂家的产品。可以提供本地化服务产品对用户的安全至关重要，可以及时提供应急安全响应服务，如在病毒或黑客入侵事件发生的时候，可以在第一时间进行响应，最大程度的保护用户利益。

3、在选择产品时需要保证符合相应的国际、国内标准，尤其是国内相关的安全标准。如国内的安全等级标准、漏洞标准，安全标准以及国际的 CVE、ISO13335、ISO15408、ISO17799 等标准。

4、产品在使用上应具有友好的用户界面，并且可以进行相应的客户化工作，使用户在管理、使用、维护上尽量简单、直观。

5、所选择的安全产品尽可能为同一厂家产品，以种于日常维护、升级、设备联动等。