### 信息系统信息安全保护等级第三级建设思路

根据国家网络安全保护法以及国标《信息安全技术网络安全等级保护基本要求》（GBT22239-2019）的要求，结合业务安全需求特点，遵循适度安全为核心，重点保护保障关键业务，以技术、管理、服务并重、标准化和成熟性为原则，从多个层面进行建设，构建以安全管理体系和安全技术体系为支撑的信息安全体系，使指挥信息系统在网络安全、主机安全、数据安全、应用安全、管理安全各个层面应达到信息安全技术网络安全等级保护基本要求，为信息系统业务的运行提供网络安全保障。

#### 信息系统安全等级定级

根据国家标准《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》有关要求，结合系统实际情况，来确定系统主要业务信息安全保护等级。

| 系统服务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 |

系统属于为国计民生、经济建设等提供服务的信息系统，根据其服务范围等。业务信息遭到破坏后，所侵害的客体是公民、法人和其他组织的合法权益，同时也侵害社会秩序和公共利益但不损害国家安全。客观方面表现得侵害结果为：

1. 可以对公民、法人和其他组织的合法权益造成侵害（影响正常工作的开展，导致业务能力下降，造成不良影响，引起法律纠纷等）；
2. 可以对社会秩序公共利益造成侵害（造成社会不良影响，引起公共利益的损害等）。

根据《定级指南》的要求，出现上述两个侵害客体时，优先考虑社会秩序和公共利益。上述结果的程度表现为：对社会秩序和公共利益造成严重损害，即会出现较大范围的社会不良影响和较大程度的公共利益的损害等。由于侵害的客体有两个，侵害的程度也有两个，则业务信息安全保护等级应为第三级。

| 系统服务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 |

信息系统的安全保护等级由业务信息安全等级和系统服务安全务安等级的较高者决定。所以，系统安全保护等级应为第三级。

##### 对应国家三级等级保护的措施

| 三级等级保护的主要技术要求 | 方案采取的措施 |
| --- | --- |
| 网络结构安全：应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段； | IPS技术、防火墙技术，实现重要网段和其他网段的逻辑隔离。MPLS VPN/设备冗余/vlan 技术隔离/带宽保障（ACG），需下一代防火墙、下一代防火墙的IPS 功能模块和下一代防火墙的 ACG 功能模块 |
| 网络访问控制 | 防火墙技术. 核心交换机MPLS VPN/vlan 技术隔离，需下一代防火墙和核心交换机 |
| 网络安全审计 | 网络安全审计系统(ACG/iMC)，需下一代防火墙的ACG 功能模块和网络安全管理平台（也可以直接由安全设备自身的管理页面和配置、告警信息来实现但工作量大，实时性差） |
| 网络边界完整性检查 | 网络管理平台和安全准入系统（本方案不涉及）实现，或者通过人工实现 |
| 网络入侵防范 | IPS 入侵保护系统，需下一代防火墙的 IPS 功能模块 |
| 网络恶意代码防范 | 防病毒网关（IPS 及网络/主机病毒防范）需下一代防火墙的 IPS 功能模块和防病毒功能模块 |
| 网络设备防护 | 通过运维审计系统来实现 |
| 主机身份鉴别 | 需部署 CA 系统，安全准入系统 |
| 主机安全审计 | 可通过部署网络安全管理平台来实现统一的安全审计，也可以直接由安全设备自身的管理页面和配置、告警信息来实现（后者工作量大，实时性差）。 |
| 主机访问控制 | 防火墙结合主机操作系统本身技术可以实现。需下一代防火墙 |
| 主机入侵防范 | 入侵保护系统结合运控系统技术；主机文件系统备份及集群技术。需部署漏洞扫描系统 |
| 主机恶意代码防范 | 防病毒/网页防篡改，部署与网关处不同品牌防病毒软件 |
| 主机资源控制 | 运控系统、防火墙、主机操作系统结合技术实现。 |
| Web应用安全 | 部署 web 应用防火墙 |
| 应用身份鉴别 | 需部署 CA 系统，安全准入系统 |
| 应用访问控制 | 应用用户权限控制，可结合下一代防火墙实现 |
| 资源控制 | 部署的应用系统应具备此功能 |
| 应用完整性、保密性、抗抵赖性 | （推荐使用加密机） |
| 数据安全及备份恢复 | （推荐使用 CA 系统） |
| 应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地； |  |
| 应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。 |  |

##### 对应国家三级等级管理的措施

| 三级等级保护的主要管理要求 | 方案采取的措施 |
| --- | --- |
| 资产管理 | 网管平台或者 web 界面人工管理 |
| 监控管理 | 网管平台或者 web 界面人工管理 |
| 网络安全管理 | 管理设备软件管理，配置文件管理，漏洞扫描 |
| 恶意代码防范管理 | 下一代防火墙 |
| 密码管理 | 通过 ca 系统/加密机实现 |
| 变更管理 | 运维审计统 |
| 备份与恢复 | 制定数据的备份策略和恢复策略/备份过程应记录/建立备份及冗余设备的安装、配置、启动、操作及维护过程控制的程序，记录设备运行过程状况（备份软件） |

#### 安全环境设计

##### 防火墙安全设计

部署一台多功能安全防火墙，实现防火墙、VPN、防病毒、入侵防御等多种设备的功能，从而降低了设备成本和管理成本，能够从网络层到应用层对网络纵向边界提供全方位的安全保护。

##### IDS入侵检测安全设计

在安全网络域的核心交换机处部署IDS设备，实现内部网络区域入侵行为的报警与记录。

##### 数据库审计系统设计

数据库审计部署为旁路监听模式，使用侦听数据库协议，审计的内容包括：访问时间、访问者IP、访问对象IP、双方端口、协议、内容、数据库操作、数据库信息等。

网络审计系统能够全面详实地记录网络内流经监听出口的各种网络行为，以便进行事后的审计和分析。网络行为日志全面地记录了包括使用者、分组、访问时间、源IP地址、源端口、源MAC地址、目的IP地址、目的端口、访问类型、访问地址/标识等关键数据项。审计数据库用户登录事件，并记录用户账号信息；可实现对数据库的查询、创建、插入、删除、更新等常规数据库操作过程的审计，可还原用户操作过程；可实现数据库特权操作(如权限更改、备份与恢复等)的审计，可还原操作过程。

##### 终端安全管理系统设计

在用户办公终端上部署终端安全管理系统，主要实现内部办公终端用户接入域的主机安全防护、安全监控、外设管理、准入控制、安全审计、非法外连控制、安全检测、安全加固、安全响应和终端防泄密等。

##### 防病毒安全设计

针对病毒的风险，在各应用服务器、数据库服务器、用户终端等安装防病毒软件，有效查杀病毒、恶意脚本、木马、蠕虫等恶意代码。加强终端主机与服务器系统、网络出入口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。使网络免受病毒、特洛伊木马和其它恶意程序的侵袭，不让其有机会透过文件及数据的分享进而散布到整个网络环境，提供完整的病毒扫描防护功能。

本方案中部署网络版防病毒设备，在所有服务器及工作终端上部署防病毒客户端软件。

##### WEB应用安全防护

部署WAF系统，即WEB应用防火墙。WAF系统采用透明模式部署在业务服务域前，通过实时扫描等技术，对本区域内的基于B/S结构的工作站进行实时监测和防护；对访问该区域WEB工作站的数据进行安全检查，一旦发现攻击行为立刻中断连接保护WEB工作站的安全。

##### 堡垒机系统设计

采用物理旁路方式部署，不需改变现有网络结构，同时不需要在被管理设备上安装任何代理程序，只需确保堡垒主机和被管资源以及用户终端维护区域网络可达即可。终端维护区域用户通过http或https方式登录系统portal，经过用户身份认证后，通过资源列表单点登录至被管目标资源。

对业务环境下的用户运维操作进行控制和审计的合规性管控系统。它通过对自然人身份以及资源、资源账号的集中管理建立“自然人账号——资源——资源账号”对应关系，实现自然人对资源的统一授权，同时，对授权人员的运维操作进行记录、分析、展现，以帮助内控工作事前规划预防、事中实时监控、违规行为响应、事后合规报告、事故追踪回放，加强内部业务操作行为监管、避免核心资产（服务器、网络设备、安全设备等）损失，保障业务系统的正常运营。

##### 日志审计系统安全设计

日志审计系统通过监测及采集信息系统中的系统安全事件、用户访问行为、系统运行日志、系统运行状态等各类信息，经过规范化、过滤、归并和告警分析等处理后，以统一格式的日志形式进行集中存储和管理，同时保留原始的日志信息和日志格式，以便事后分析取证用，结合丰富的日志分析综合显示功能，实现对信息系统整体安全状况的全面管理。

##### 漏洞扫描系统设计

漏洞扫描系统是一种主动检测本地或远程主机系统安全性弱点的程序，采用模仿黑客入侵的手法对目标网络中的服务器、应用系统、数据库等各种系统以及路由器、交换机、防火墙等网络设备可能存在的安全漏洞进行逐项检查，测试该系统上有没有安全漏洞存在，然后将扫描结果向系统管理员提供周密可靠的安全性分析报告，从而让管理人员从扫描出来的安全漏洞报告中了解网络中服务器提供的各种服务及这些服务呈现在网络上的安全漏洞，在系统安全防护中做到"有的放矢"，及时修补漏洞，从根本上解决网络安全问题，有效地阻止入侵事件的发生。

在应用业务及生产核心系统网络通过旁路监听方式部署漏洞扫描设备。漏洞扫描设备在网络中并不是一个实时启动的系统，只需要定期挂接到网络中，对当前网段上的重点服务器以及主要的桌面机和网络设备进行一次扫描，即可得到当前系统中存在的各种安全漏洞，针对性地对系统采取补救措施，即可在相当一段时间内保证系统的安全。

##### 云安全计算环境设计

云平台及虚拟化平台应实现虚拟机之间的CPU、内存和存储空间安全隔离，能检测到非授权管理虚拟机等情况，并进行告警;应禁止虛拟机对宿主机物理资源的直接访问，应能对异常访问进行告警;应支持不同云租户虛拟化网络之间安全隔离;应监控物理机、宿主机、虚拟机的运行状态。

同时云平台利用网络安全设备实现以下目标：

1. 用户身份鉴别；
2. 入侵防范应能检测到虚拟机对宿主机物理资源的异常访问；
3. 数据保密性保护应提供重要业务数据加密服务；
4. 数据备份与恢复；
5. 恶意代码防范物理机和宿主机应安装经过安全加固的操作系统或进行主机恶意代码防范。

##### 移动互联安全设计

业务应用应实现以下功能：

1. 用户身份鉴别应对移动终端用户实现基于口令或解锁图案、数字证书或动态口令、生物特征等方式的两种或两种以上的组合机制进行用户身份鉴别；
2. 标记和强制访问控制应确保用户或进程对移动终端系统资源的最小使用权限;应根据安全策略，控制移动终端接入访问外设，外设类型至少应包括扩展存储卡、GPS等定位设备、蓝牙、NFC等通信外设，并记录日志；
3. 应用管控应具有软件白名单功能，能根据白名单控制应用软件安装、运行;应提供应用程序签名认证机制，拒绝未经过认证签名的应用软件安装和执行；
4. 数据保密性保护应采取加密、混淆等措施，对移动应用程序进行保密性保护，防止被反编译;应实现对扩展存储设备的加密功能，确保数据存储的安全。