网络安全等级保护设计方案（三级）-技术体系设计

XXX科技有限公司

20XX年 XX月 XX日

目　录

一 安全计算环境

依据《网络安全等级保护安全设计技术要求》中的第三级系统“通用安全计算环境设计技术要求”，同时参照《网络安全等级保护基本要求》等标准要求，对等级保护对象涉及到的安全计算环境进行设计，设计内容包括用户身份鉴别、自主访问控制、标记和强制访问控制、系统安全审计、用户数据完整性保护、用户数据保密性保护、数据备份恢复、客体安全重用、可信验证、配置可信检查、入侵检测和恶意代码防范、个人信息保护等方面。

1.1 用户身份鉴别

身份鉴别在整个等级保护对象中处于基础的、关键的地位。网络安全最基本和关键的保护就是要从身份鉴别入手来提高和控制整个系统的安全。身份鉴别除了必要的技术手段保证外，与之配套的管理制度规范也是必不可少的。

等级保护对象设计将加强终端登录、应用系统等身份鉴别管理，通过身份鉴别系统对用户的账户、密码、证书进行统一管理，防止非法用户随意接入访问应用服务器数据资源。所有等级保护对象内终端将增设开机 CMOS 密码，加强 CMOS 修改权限的保护，防止通过改变系统启动设置等参数、非授权使用终端。具体设计如下：

1） 用户身份标识

在应用系统身份鉴别及跟踪方面，可以在等级保护对象应用系统层面设定标识，并与应用环境如数据库存储、操作系统以及网络传输进行更深入的绑定，使更深层次的审计成为可能。

由应用系统统一生成唯一的用户身份标识符，无论在系统生命周期还是在应用过程中，该标识符是唯一的，并贯穿于业务系统应用始终。该身份标识符存放在数据库特殊位置，并进行保护。在数据库列表不被非授权地访问、修改或删除；用户如果要以特权用户访问该资源，必须要有两种或以上身份验证的方法。用户标识符应与安全审计相关联，保证系统发生安全事件时的可核查性。

登录失败处理

当用户身份鉴别尝试失败次数达到5次后,应采取以下措施:对于本地登录,将进行登录锁定，同时形成业务系统和数据库审计事件并告警。对于应用程序,禁止使用该程序或延长一定时间后再允许尝试。

重新鉴别

用户身份鉴别成功登陆系统后,如果当其空闲操作的时间超过规定值（通常为10分钟以内）后，在该用户需要执行其他操作之前，将对该用户重新进行身份鉴别。

远程管理传输

远程管理的设置是为了方便管理员随时随地进行管理操作,当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。为此，需要对鉴别信息进行加密处理，而网络传输过程中最经常使用的是SSL加密。SSL加密用以保障在网络传输数据的安全,利用数据加密技术,确保数据在网络上的传输过程中不会被截取及窃听。

双因子认证

在等级保护对象中，服务器、用户终端、应用程序以及网络和安全设备的本地登录、远程登录均进行用户身份鉴别。身份鉴别方式采用USB Key智能密码钥匙+ PIN 码的相结合的双因子认证方式。

对于普通用户，通过 PKI 公钥基础设施和终端安全登录与文件保护系统的部署,实现以数字证书为核心的双因子认证技术（如:采用存有数字证书的USB Key智能密码钥匙+PIN码的方式），包括对用户登录终端时的身份鉴别以及用户访问应用系统时的身份鉴别,防止非法用户随意登录终端并访问应用服务器数据资源。此外，当用户需要访问核心资源时，需要对用户身份进行二次鉴别。

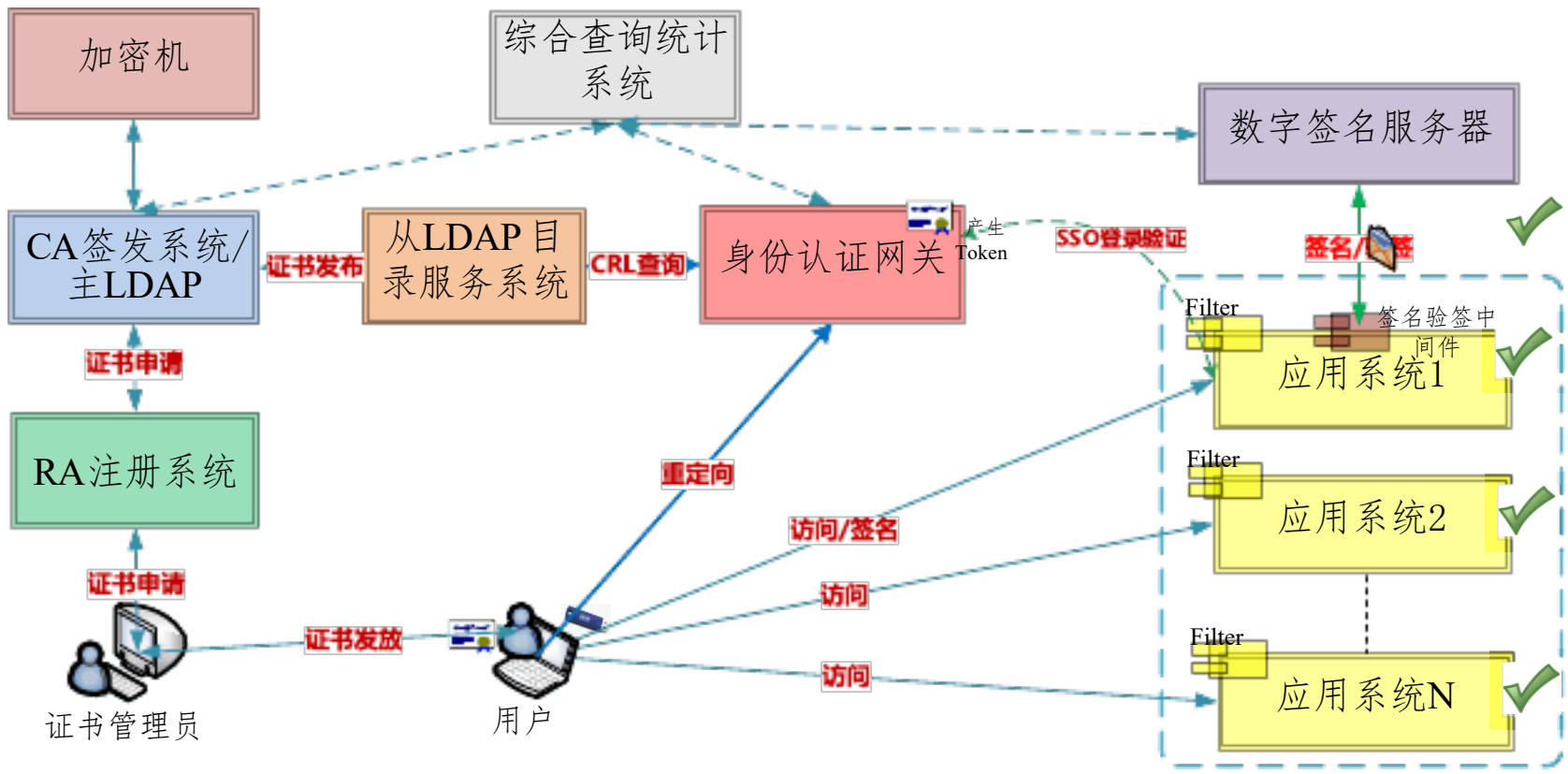
对于管理员用户，通过部署运维审计系统，并将运维审计系统与PKI/CA公钥基础设施进行集成，全部设备的维护操作都要通过运维审计系统进行。管理员用户登录运维审计系统,也采用以数字证书为核心的双因子认证技术实现身份鉴别。

采用USB Key智能密码钥匙+PIN码口令相结合的方式进行身份鉴别时，应满足如下要求:

口令长度设置不少于10位;

口令采用大小写字母、数字、特殊字符中两者以上组合设置，同时定期进行更换。

PKI/CA 系统逻辑设计



PKI/CA 系统逻辑框架设计图

PKI/CA 系统逻辑框架如上图所示，主要由证书发放、登录应用系统、数字签名三部分组成。其中：

2） 证书发放

证书管理员登录 RA 系统，录入用户信息，并审核用户注册请求；

证书注册信息传入 CA 签发系统；

CA 签发系统进行数字证书的签发；

CA 签发系统将证书发布到 LDAP 目录服务系统中；

证书经 RA 传回管理员桌面，管理员为用户制作证书，并发给用户使用。

3） 用户登录应用系统

用户登录业务系统，业务系统通过安装在系统上的 FILTER 过滤器来判断用户是否已经认证过，如果没有，则重定向用户登录网关登录页面；

用户按照网关页面插入 USB KEY，并输入 PIN 保护密码，然后提交认证请求到身份认证网关；

身份认证网关判断证书的真实有效，并从目录服务中查询 CRL 证书黑名单，判断证书是否已经被吊销；

如果证书验证全部通过，身份认证网关检查用户权限，然后显示用户可登录系统列表，根据授权策略为用户签发单点登录 TOKEN，用户凭借 TOKEN 单点登录到各业务系统中。

4） 数字签名流程

用户提交敏感操作/敏感数据，客户端签名软件将调用 USB KEY 接口对敏感操作/敏感数据产生数字签名；

数字签名传入应用系统，应用系统调用签名中间件接口，将签名信息传入签名服务器完成数字签名验证，签名服务器返回验证结果；

应用系统根据验证结果完成后续业务逻辑操作；

数字签名服务器除了能够满足用户签名外，还可以提供系统间身份认证及交互数据的数字签名功能，满足系统间的强身份认证及数据完整有效，实现抗抵赖功能。

1.2 自主访问控制

自主访问控制是一种常用的访问控制方式，它基于对主体或主体属性的主体组的识别来限制对客体的访问，这种控制是自主的。自主是指主体能够自主地（可间接地）将访问权限或访问权的某个子集授予其它主体。

对于自主创建的文件，除了对文件做机密性、完整性保护外，还需要进行访问控制的操作。文件属主通过操作系统自带的访问控制功能实现对受保护文件的统一“读”、“写”、“执行”等操作管理。普通用户对这些文件进行访问，不能违背这些规定，否则，操作不能进行。另外，也可以通过部署统一认证及权限管理系统的访问控制功能实现文件级的访问控制。

针对等级保护对象的主机系统访问控制策略需要对服务器及终端进行安全加固，加固内容包括：限制默认账户的访问权限，重命名系统默认账户，修改帐户的默认口令，删除操作系统和数据库中过期或多余的账户，禁用无用帐户或共享帐户；根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；启用访问控制功能，依据安全策略控制用户对资源的访问。

在交换机和防火墙上设置不同网段、不同用户对服务器的访问控制权限。

关闭操作系统开启的默认共享,对于需开启的共享及共享文件夹设置不同的访问权限，对于操作系统重要文件和目录需设置权限要求。

设置不同的管理员对服务器进行管理，分为系统管理员、安全管理员、安全审计员以实现操作系统特权用户的权限分离,并对各个账户在其工作范围内设置最小权限。通过主机内核加固系统，实现服务器的内核级安全加固。

1.3 标记和强制访问控制

强制访问控制是指由系统(通过专门设置的系统安全员)对用户所创建的对象进行统一的强制性控制,按照规定的规则决定哪些用户可以对哪些对象进行什么样操作类型的访问，即使是创建者用户，在创建一个对象后，也可能无权访问该对象。等级保护对象中强制访问控制，通过以下方式实现。

1） 操作系统层面的强制访问控制安全机制

目前主流的操作系统均提供不同级别的访问控制功能,但由于国外对我国核心技术的封锁，出口商用操作系统通常采用自主访问控制机制，高等级主体如root、administrator等默认获得所有客体的访问控制权,一旦位于最高等级的超级管理员账号、密码等信息被攻击者盗取并成功利用，操作系统将无任何安全性可言,故条件允许的情况下等级保护对象可考虑使用更高安全级别的国产化中标麒麟安全操作系统。目前该操作系统通过公安部信息安全产品检测中心最高级别的权威认证，安全功能达到了第四级（结构化保护级）技术要求的强制性认证。

该操作系统基于 LSM 机制的 SELinux 安全子系统框架，以自主研发的 SXL/SXL2 安全框架为核心，将安全机制从内核延伸到应用和网络。提供三权分立机制权限集管理功能和统一的安全管理中心 SMC，支持安全管理模式切换，针对特定应用的安全策略定制；提供核心数据加密存储、双因子认证、高强度访问控制、进程级的最小权限、网络安全防护、细粒度的安全审计、安全删除、可信路径、TCM 支持等多项安全功能；提供可持续性的安全保障；兼容主流的软硬件；为用户提供全方位的操作系统和应用安全保护，防止关键数据被篡改被窃取，系统免受攻击，保障关键应用安全、可控和稳定地对外提供服务。

2） 应用系统层面的强制访问控制安全机制

应用系统层面的强制访问控制的实现，可以在需要控制的文件/数据库服务器外部部署统一认证及权限管理系统实现对用户的授权,利用基于角色的访问控制模型（RBAC）结合应用系统的安全功能开发，实现对用户功能操作的强制访问控制，等级保护对象应用系统实现对用户资源的强制访问控制。即：由安全管理员通过在统一认证及权限管理系统对所有主体（用户）进行标记，强制访问控制主体的粒度为用户级。通过应用系统对所有客体（文件、数据库中的数据）进行安全标记,客体的粒度为文件或数据库表级,将用户类别与安全标记文件对应,从用户的访问请求中取得要访问的资源和操作。通过访问控制列表，检查用户与此进行安全标记的文件是否有访问权限，实现对文件的强制访问控制。

文件在整个生存周期中，除非经安全管理中心重新定级，否则安全标记全程有效。强制访问控制，是根据安全策略来确定该用户能否对指定的受控文件进行操作。比如安全策略规定，高密级用户可以访问同密级和低密级文件；反之，低密级用户则被强制禁止访问高密级文件。当然，管理中心可以根据实际应用环境制定相应的安全策略，从而实现标识和强制访问控制目标。

统一认证及权限管理系统还应实现单点登录和单点登出等相关功能。

1.4 系统安全审计

对等级保护对象的终端、服务器、数据库和应用系统均设置安全审计措施，对系统内的相关安全事件、提供审计记录，记录内容包括用户、对象、时间、操作以及结果等，并提供审计记录的查询、分类、报表、存储和事件回放功能。通过二次开发对应用系统进行相应的审计，对系统不能独立处理的安全事件提供统一的调用接口,对应用系统发生的特定的安全事件进行报警,保证系统的安全性。具体的审计措施包括：

1） 运维审计

管理人员和运维人员使用运维审计系统实现运维操作审计。审计管理员能够对管理人员和运维人员的操作进行审计。加强对相关运维事项的责任认定，运维工作质量、数量的评估与考核，满足事前预防（通过统一认证和授权运维人员只能对其有权限的设备进行运维操作）、运维事件的事中控制、操作内容事后审计的要求。

根据审计需求，对受控终端/服务器制定详尽的审计策略（包括用户登录、资源访问、进程启动等）。对已收集的审计信息，分类别提供详细的审计查询，能够对审计信息进行收集、归并、查询、备份等操作。主要通过终端管理系统或主机监控与审计产品完成。

3） 数据库审计

采用支持关系型数据库和分布式数据库审计的数据库审计系统，对数据库进行静态、动态审计，同时提供审计报表和审计事件回放，为安全审计员提供核心数据库的全方位、细粒度的保护功能。数据库审计应包括静态审计和动态审计。

4） 应用审计

应用级审计主要针对的是应用程序的活动信息，如打开和关闭数据文件，读取、编辑、删除记录或字段等特定操作，以及打印报告等。主要是通过应用系统和主机监控与审计等产品配合完成。

5） 安全审计报告

能够将安全事件主体、客体、时间、类型及结果等内容自动生成并导出定制化的报告。

用户数据完整性保护

数据完整性指传输和存储的数据没有被非法修改或删除，也就是说数据处于未受损未丢失的状态，它通常表明数据在准确性和可靠性上是可信赖的。其安全需求与数据所处的位置、类型、数量和价值有关，涉及访问控制、消息认证和数字签名等安全机制，具体安全措施包括防止对未授权数据进行修改、检测对未授权数据的修改情况并计入日志、与源认证机制相结合以及与数据所处网络协议层的相关要求相结合等。

数据完整性保障技术的目的是对数据完整性进行预防和恢复。预防是指对威胁数据完整性的各种不利因素采取预防措施，如常用的数据备份等；恢复是指在数据遭受损失或破坏后，采取有效的恢复技术，使得被破坏的数据尽快得到恢复。确保数据完整、正确性的方法包括数据校验技术、数字签名技术等。

1） 数据校验

用一种指定的算法对原始数据计算出的一个校验值。接收方用同样的算法计算一次校验值，如果和原始数据提供的校验值一样，就说明数据是完整的。

数字签名

数字签名是为了保证对信息主体的认证，以实现信息的真实性、完整性和不可抵赖性，它提供了一种保护电子文档的真实性和完整性的方法。在公钥机制下，数字签名通过一个单项函数对要传送的报文进行处理，得到用以核实报文是否发生变化的一个字母数字串，以此来判断报文的完整性。在私钥机制下，通过专属私钥加密报文，接收方只能通过对应公钥进行解密，证明该报文的真实来源，用以核实报文的不可抵赖性。

对等级保护对象的用户数据完整性防护，重点体现在数据库中的结构化数据上。对数据完整性的保护体现在两个方面。一方面，在数据的存储与操作时，在数据库管理系统中，利用对数据表的主键、外键来保障数据完整性；另一方面，在数据的传输时，应尽量利用数字签名、VPN 等加密技术，保障数据传输的完整性。

用户数据保密性保护

数据保密性是指防止信息被未经授权者访问和防止信息在传递过程中被截获并解密的功能。

数据保密性可分为动态信息保密性和静态信息保密性动态信息保密性表现为数据在传输过程中的保密性,而静态信息保密性表现为数据在存储过程中的保密性。

1） 动态数据加密

在动态数据保密性方面，通过部署 VPN、安全通信协议或其他密码技术等措施实现数据传输过程中的保密性防护，如通过 VPN 实现同城/异地备份中心的传输加密。

对鉴别信息、重要业务数据和重要个人信息进行加密传输，即确保传输的数据是加密后传输。

静态数据加密

一般通过密码加密技术实现数据存储过程中的保密性防护。对于特别重要的数据，使用数据加密系统或其他加密技术实现关键管理数据、鉴别信息以及重要业务数据存储的保密性。

对存放在关系型数据库中的原始数据，建议使用国产密码算法技术对数据的存取进行加解密操作。

数据备份恢复

数据备份恢复作为网络安全的一个重要内容，其重要性却往往被人们忽视，只要发生数据传输、存储和交换，就有可能产生数据故障，如果没有采取数据备份和灾难恢复的手段与措施，就会导致数据丢失并有可能造成无法弥补的损失。一旦发生数据故障，组织就陷入困境，数据可能被损坏而无法识别，而允许恢复时间可能只有短短几天或更少。如果系统无法顺利恢复，最终可能会导致无法想象的后果。因此组织的信息化程度越高，数据备份和恢复的措施就越重要。

1） 数据备份

数据备份是为了在系统出现故障时，能够确保恢复整个系统，因此需要制定详细的备份策略，明确何时进行备份、用什么备份方法、备份哪些数据等。目前采用最多的备份策略主要有以下三种。

a) 完全备份

备份全部选中的文件夹，不依据文件的存档属性来确定备份哪些文件。

在备份过程中，任何现有的标记都将被清除，每个文件都被标记为已备份。

差异备份

差异备份是相对于完全备份而言，它只备份上一次完全备份后发生变化的所有文件。差异备份过程中，只备份有标记的那些选中的文件和文件夹。它不清除标记，即备份后不标记为已备份文件。

增量备份

增量备份是针对上一次备份的，即备份上一次备份后所有发生变化的文件。增量备份过程中，只备份有标记的选中的文件和文件夹，它清除标记。

从地理位置上来看，异地备份提供了一种新的备份方式，使得备份后的数据不一定要保存在本地，也可保存在网络上的另一服务器上，这种方式是将数据在另外的地方实时产生一份可用的副本，此副本的使用不需要做数据恢复，可立即投入使用。数据异地备份的数据复制主要有如下几种实现方式：

a) 基于主机

基于主机的数据复制技术是在异地的不同主机之间，不考虑存储系统的同构问题，只要保持主机是相同的操作系统即可进行数据的复制。此外，目前也存在支持异构主机之间的数据复制软件，可以支持跨越广域网的远程实时复制。

基于存储系统

基于存储系统的数据复制技术是利用存储系统提供的数据复制软件进行数据的复制，复制的数据流在存储系统之间传递，和主机无关。

基于光纤交换机

基于光纤交换机的数据复制技术是利用光纤交换机的功能，或者利用管理软件控制光纤交换机，首先对存储系统进行虚拟化，然后管理软件对管理的虚拟存储池采用卷管理、卷复制和卷镜像等技术，来实现数据的远程复制。

基于应用的数据复制

基于应用的数据复制技术有一定局限性，一般只能针对特定的应用使用，主要利用数据库自身提供的复制模块来完成异地数据的备份。

数据恢复

恢复是备份的逆操作，但恢复的操作比备份复杂，也容易出问题。数据恢复策略主要有如下几种：

a) 完全恢复

将备份策略指定备份的所有数据，恢复到原来的存储池。主要用于灾难、系统崩溃和系统升级等情况。

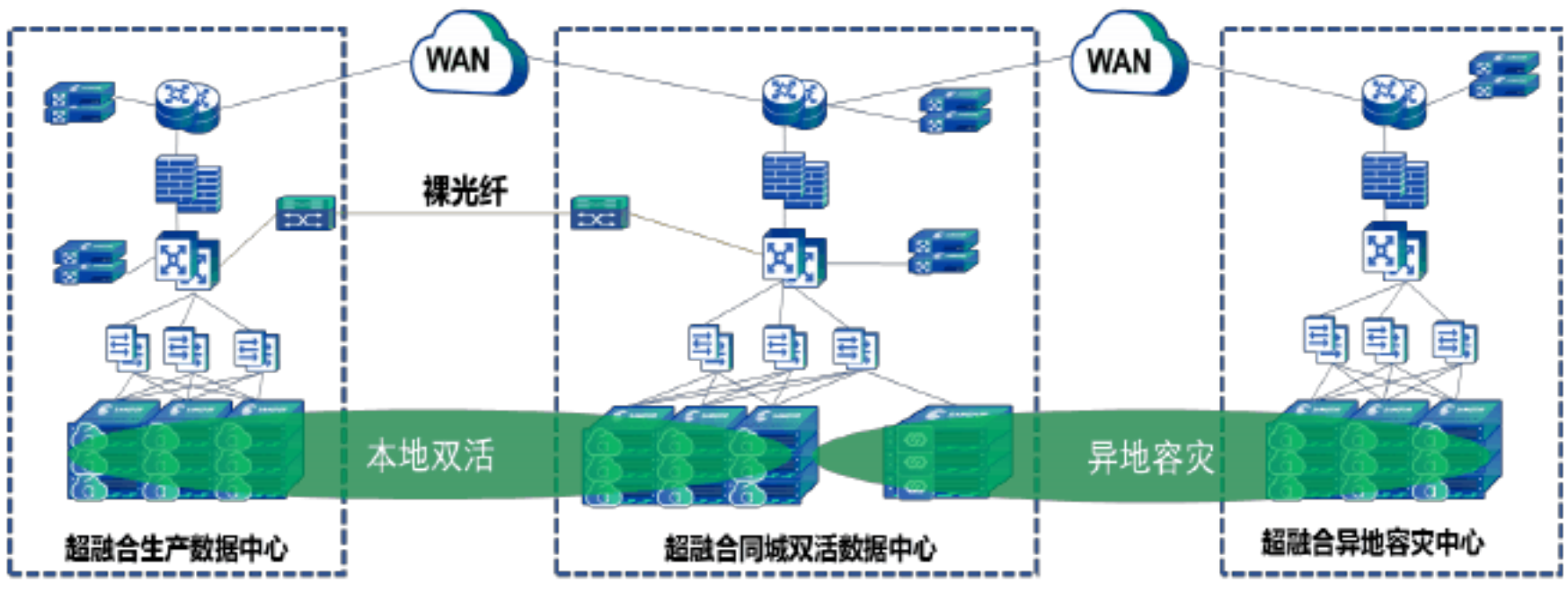
个别文件恢复

对指定的文件进行恢复。在个别文件被破坏，或想要某个文件备份时的版本等情况下，进行个别文件恢复操作。

将所备份的文件，恢复到指定的存储位置，而不是备份时的位置。重定向恢复可以是完全恢复，也可以是个别文件恢复。

重要数据处理系统热冗余

备份与恢复包括两方面内容，一方面是数据备份与恢复，另一方面是重要数据处理系统（关键网络设备、安全设备、应用服务器和数据库服务器等）热冗余，重要数据处理系统的冗余对数据备份起到重大作用，为数据的备份和恢复提供支持，保证系统的高可用性。



我司灾备解决方案可以实现本地备份、同城双活、异地容灾及两地三中心的扩展。

生产数据中心和双活中心采用分布式超融合架构，通过数据多副本的方式，实现数据副本的跨中心分布，生产中心与双活中心数据副本实现同时同时读写，实现数据 0 丢失。

生产中心或者同城双活中心的业务通过 CDP 实现数据本地备份，并同时实现备份数据的异步复制到异地容灾中心。

当生产中心和双活中心之间实现业务的高可用，利用分布式超融合架构的 HA 或者 DRS 技术实现业务的自动恢复。当生产中心和双活中心均故障时，实现业务在异地容灾中心的手动拉起。

客体安全重用是为了防止某个用户非授权获取其他用户的鉴别信息、文件、目录和数据库记录等资源，所以需要采用一定手段，保证被使用过的客体资源在重新分配前，对其原使用者的信息进行清除，包括使用恢复软件都无法恢复存储设备上曾保存过的资料，以确保信息不被泄露。等级保护对象中客体安全重用主要包括鉴别信息清除和敏感数据清除两方面内容，主要通过应用系统开发过程中通过专用代码加以实现。

1） 鉴别信息清除

设计系统时应注意，用户鉴别信息所在的存储空间被释放或重新分配给其他用户之前要完全清除。

敏感数据清除

操作系统、应用系统内文件、目录和数据库记录等资源所在存储空间被释放或重新分配给其他用户之前也需要得到完全清除。

在设计应用系统时，无论是用户鉴别信息的清空还是文件记录的清空，采取的方式是类似的，都是在用户注销退出时对存储介质上（包括硬盘和内存）的残余信息进行清理。这就要求设计人员对需要清理的地方进行适当的清理，一般可以使用一些工具或直接用代码对底层进行操作。

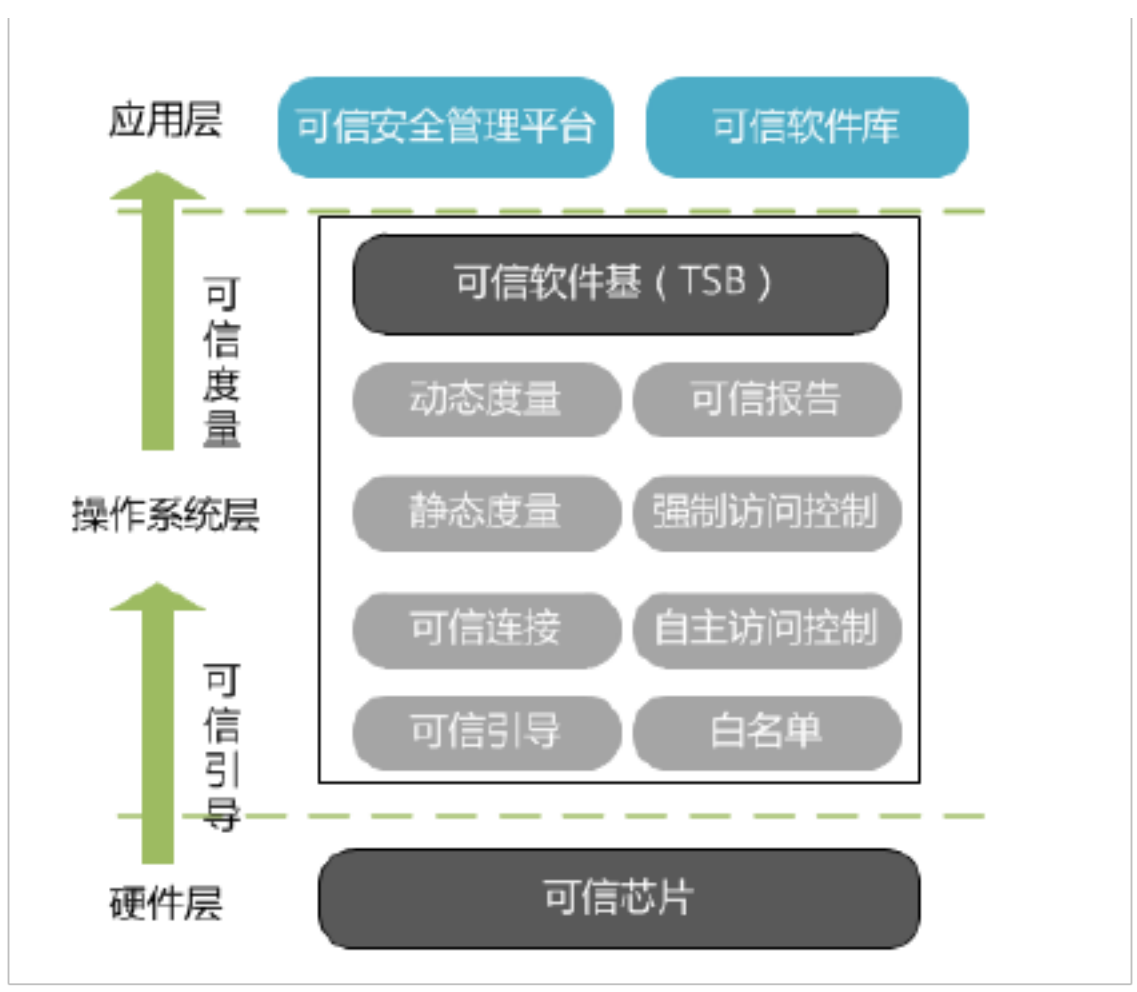
1.9 可信验证

传统的计算机体系结构过多地强调了计算功能，忽略了安全防护，可信验证技术目的就是要解决这个安全防护先天不足的问题。

可信验证的基本思想是，首先在计算机系统中构建一个可信根，可信根的可信性由物理安全、技术安全和管理安全共同确保，可信根的内部有密码算法引擎、可信裁决逻辑、可信存储寄存器等部件，可以向节点提供可信度量、可信存储、可信报告等可信功能，是节点信任链的起点；再建立一条信任链，从信任根开始到软硬件平台、到操作系统、到应用，一级度量认证一级、一级信任一级，把信任关系扩大到整个计算节点，从而确保计算节点可信的过程。

部分关键服务器设备可采用部署基于可信计算技术的操作系统免疫保护平台，提供执行程序可信度量，阻止未授权及不符合预期的执行程序运行，实现对已知/新型恶意代码的主动防御，实现计算设备的内核级系统监控、文件可信校验、动态度量、可信网络连接及可信审计等功能。

操作系统免疫保护平台由可信安全管理平台、可信终端软件、可信软件库、可信芯片组成。可信安全管理平台对所有接入终端的应用、安全软件、系统环境进行统一管理，可信终端软件是安装在终端操作系统中的安全执行软件，可信软件库为信息系统提供可信软件，可信芯片提供可信根。操作系统免疫保护平台产品架构图如下图所示：



操作系统免疫保护平台产品架构图

可信安全管理平台采用三权分立的管理模式，通过可信安全管理平台采用标准化的接口和协议，统一管理计算节点、安全组件和应用系统。可信安全管理平台可以对应用、安全软件、系统环境进行统一管理和集中体现。

可信终端软件是安装在终端操作系统中的安全执行软件，是实现系统运行过程中度量、存储、报告功能的实际执行部件，可利用可信芯片的特性，为应用和系统的运行建立可信的计算环境通过可信连接形成可信网络，并将可信计算功能的接口提供给应用和操作系统使用。

可信软件库是为终端软件提供软件安全检测、安全下载和安全使用的软件仓库。通过对业务环境中使用的软件进行收集、分析、整理，形成企业可信软件库，并生成与软件配套的白名单信息库及规则库。通过对软件的合法性检查、版本管理及规范存储，保证软件的规范管理与使用。

1.10 配置可信检查

以操作系统免疫保护平台中的可信软件库作为基准库，并且进行联动，只有通过软件库认证检查过的软件才可以使用。阻止未授权软件和恶意软件的安装使用。

可信软件库会对库中的软件进行安全分析和安全规则的制定，每一个可信软件都有一个与之匹配的安全规则，在软件使用过程中，可信终端软件会执行相应的安全规则，一旦攻击者利用应用软件的漏洞进行提权，可信终端软件会根据应用软件的安全规则进行拦截，有效弥补因为应用软件漏洞而形成的安全威胁。

1.11 入侵检测和恶意代码防范

在所有主机和终端安装网络版防病毒软件，通过全面的网络病毒防护，保护全网终端及服务器，对各类病毒进行彻底查杀，构建起一道最基本的病毒防线。

在重要的业务服务上部署操作系统免疫保护平台，采用可信计算主动防御机制，提供执行程序可信度量，阻止未授权及不符合预期的执行程序运行，实现对已知/新型恶意代码的主动防御，降低操作系统完整性及可用性被破坏的风险。从管理角度出发，提供程序安装接口，仅允许通过程序安装接口对操作系统的可信软件进行完整性安装，同时可以生成采集模板，经管理员授权批准，实现程序批量安装，从而阻止未知来源的软件、插件进行安装，保证节点系统安全、有效地运行。

1.12 个人信息保护

等级保护对象中业务系统在需要采集个人信息时，应当仅采集和保存必需的用户个人信息，与业务无关的个人信息应当禁止被业务系统或其组件采集。可以

采用上网行为管理等设备的部署或应用安全配置项,通过访问控制限制对用户信息的访问和使用进行限制,实现禁止未授权访问和非法使用用户个人信息。同时,组织应当按照等级保护相关要求,制定保障个人信息安全的管理制度和流程,严格按照个人信息保护管理制度和流程进行操作,对违反个人信息保护管理制度和流程的人员进行处罚,保障用户个人隐私数据信息和利益不受到侵害。

采集的个人信息包括但不限于:姓名、性别、年龄、电话、地址等个人隐私数据,应当按照法律法规要求妥善保管,必要时采取加密措施对数据的传输和存储进行加密处理,以保障用户的个人数据不会被泄露或篡改。按照工作职能和人员的岗位职责分配业务系统账号和访问权限,保证业务系统数据库内存储的数据信息不被用户越权访问。

二 安全区域边界

依据《网络安全等级保护安全设计技术要求》中的第三级系统“通用安全区域边界设计技术要求”,同时参照《网络安全等级保护基本要求》、《网络基础安全技术要求》,对等级保护对象涉及到的安全区域边界进行设计,设计内容包括区域边界访问控制、区域边界包过滤、区域边界完整性保护、入侵防范、恶意代码防范和垃圾邮件防范、可信验证等方面。

2.1 区域边界访问控制

等级保护对象安全区域边界是网络安全域划分和明确安全控制单元的体现。区域边界访问控制的实施对象是配置了访问控制策略的网络设备或网络安全设备。访问控制策略是网络安全防范和保护的主要策略,其目的是保证网络资源不被非法使用和访问或防止合法用户的不当操作造成破坏.通过采取访问控制措施可以具有对网络、系统和应用的访问进行严格控制的能力。

针对网络边界的访问控制,建议部署防火墙系统,对所有流经防火墙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。

在不同网络安全区域之间的访问，可部署防火墙系统和 VLAN 隔离进行访问控制。在防火墙上配置安全策略，对跨越网络安全区域的访问进行控制，仅允许已知的业务访问；在核心交换机上设置访问控制列表策略，禁止终端接入用户对数据备份域、运维管理域的直接访问。重要网段及设备进行 IP 与 MAC 地址绑定。

2.2 区域边界包过滤

对业务应用的访问需求进行梳理，在区域边界防火墙上配置细粒度的访问控制策略，访问控制策略规则基本匹配项应包括源地址、目的地址、源端口、目的端口和协议等，访问控制力度为端口级。同时在设定访问控制策略时，管理员应厘清安全需求，设定逻辑清晰的、满足需要的最少访问控制策略，否则设置过多、冗余的访问控制策略，可能引起网络性能降低、或者规则混乱导致最终没有达到应有的控制效果。

为了防范新型漏洞，访问控制策略细粒度要求控制到对应用协议和应用内容的访问控制，一般通过部署下一代防火墙或其他相关安全组件，实现基于应用协议和应用内容的访问控制。通过增加对应用层协议的访问控制以及深层检测，可以有效防止攻击者在应用层发起的攻击行为，或者内部敏感信息的泄露。

2.3 区域边界安全审计

在等级保护对象中实施区域边界安全审计，可通过在网络边界和重要网络节点进行安全审计实现。

1） 网络边界安全审计

网络边界安全审计一般利用网络边界所部署安全防护设备自身的安全日志记录功能，对区域边界的行为进行记录审计和进一步的关联分析，并将网络边界设备的安全事件记录日志上传至集中的日志审计系统或安全管理中心的审计管理功能模块，进行集中审计，通常不需要在网络边界重新部署审计系统。例如，在网络边界防火墙或其他相关设备上配置安全审计策略，对用户访问业务系统的