记列表。在此基础上，安全管理员需要根据系统需求和安全状况，为主体实施授权管理，即授予用户访问客体资源的权限，生成强制访问控制列表和级别调整策略列表。除此之外，安全审计员需要通过安全管理中心中的审计子系统制定系统审计策略，实施系统的审核管理。如果定级系统需要和其他系统进行互联，则上述初始化流程需要结合跨定级系统安全管理中心制定的策略执行。

b) 计算节点启动流程

策略初始化完成后，授权用户才可以启动并使用计算节点访问定级系统中的客体资源。为了确保计算节点的系统完整性，节点子系统在启动时需要对所装载的可执行代码进行可信验证，确保其在可执行代码预期值列表中，并且程序完整性没有遭到破坏。计算节点启动后，用户便可以安全地登录系统。在此过程中，系统首先装载代表用户身份唯一标识的硬件令牌，然后获取其中的用户信息，进而验证登录用户是否是该节点上的授权用户。如果检查通过，系统将请求策略服务器下载与该用户相关的系统安全策略。下载成功后，系统可信计算基将确定执行主体的数据结构，并初始化用户工作空间。此后，该用户便可以通过启动应用访问定级系统中的客体资源。

c) 计算节点访问控制流程

用户启动应用形成执行主体后，执行主体将代表用户发出访问本地或网络资源的请求，该请求将被操作系统访问控制模块截获。访问控制模块首先依据自主访问控制策略对其执行策略符合性检查。如果自主访问控制策略符合性检查通过，则该请求允许被执行；否则，访问控制模块依据强制访问控制策略对该请求执行策略符合性检查。如果强制访问策略符合性检查通过，那么该请求允许被执行；否则，系统对其进行级别调整检查。即依照级别调整检查策略，判断发出该请求的主体是否有权访问该客体。如果通过，该请求同样允许被执行；否则，该请求被拒绝执行。

系统访问控制机制在安全决策过程中，需要根据安全审计员制定的审计策略，对用户的请求及决策结果进行审计，并且将生成的审计记录发送到审计服务器存储，供安全审计员检查和处理。

d) 跨计算节点访问控制流程

如果主体和其所请求访问的客体资源不在同一个计算节点，则该请求会被可信接入模块截获，用来判断该请求是否会破坏系统安全。在进行接入检查前，模块首先通知系统安全代理获取对方计算节点的身份，并检验其安全性。如果检验结果是不安全的，则系统拒绝该请求；否则，系统将依据强制访问控制策略，判断该主体是否允许访问相应端口。如果检查通过，该请求被放行；否则，该请求被拒绝。

e) 跨边界访问控制流程

如果主体和其所请求访问的客体资源不在同一个安全保护环境内，那么该请求将会被区域边界控制设备截获并且进行安全性检查，检查过程类似于跨计算节点访问控制流程。

B.4 第三级系统可信验证实现机制

可信验证是基于可信根，构建信任链，一级度量一级，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，可信验证实现框架如图 B.2 所示。

可信根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。可信固件内嵌在 BIOS 之中，用来验证操作系统引导程序的可信性。可信基础软件由基本信任基、可信支撑机制、可信基准库和主动监控机制组成。其中基本信任基内嵌在引导程序之中，在节点启动时从 BIOS 中接过控制权，验证操作系统内核的可信性。可信支撑机制向应用程序传递可信硬件和可信基础软件的可信支撑功能，并将可信管理信息传送给可信基础软件。可信基准库存放节点各对象的可信基准值和预定控制策略。主动监控机制实现对应用程序的行为监测，判断应用程序的可信状态，根据可信状态确定并调度安全应对措施。主动监控机制根据其功能可以分成

控制机制、度量机制和决策机制。控制机制主动截获应用程序发出的系统调用，既可以在截获点提取监测信息提交可信度量机制，也可以依据判定机制的决策，在截获点实施控制措施。度量机制依据可信基础库度量可信基础软件、安全机制和监测行为，确定其可信状态。可信判定机制依据度量结果和预设策略确定当前的安全应对措施，并调用不同的安全机制实施这些措施。

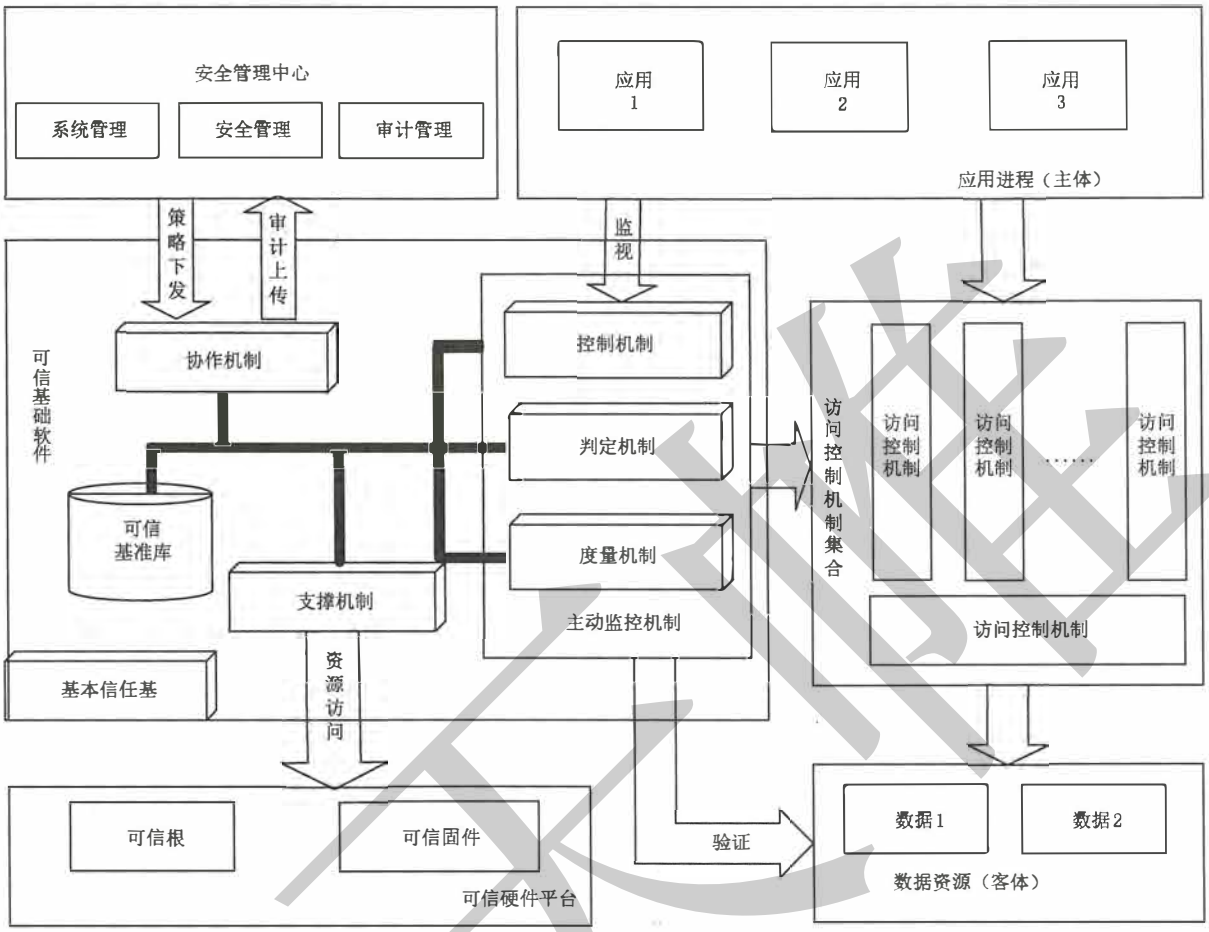

图 B.2　可信验证实现框架图

附 录 C
（资料性附录）
大数据设计技术要求

C.1 大数据等级保护安全技术设计框架

大数据等级保护安全技术体系设计，从大数据应用安全、大数据支撑环境安全、访问安全、数据传输安全及管理安全等角度出发，围绕：“一个中心、三重防护”的原则，构建大数据安全防护技术设计框架，其中一个中心指安全管理中心，三重防护包括安全计算环境、安全区域边界和安全通信网络，具体如图C.1所示。

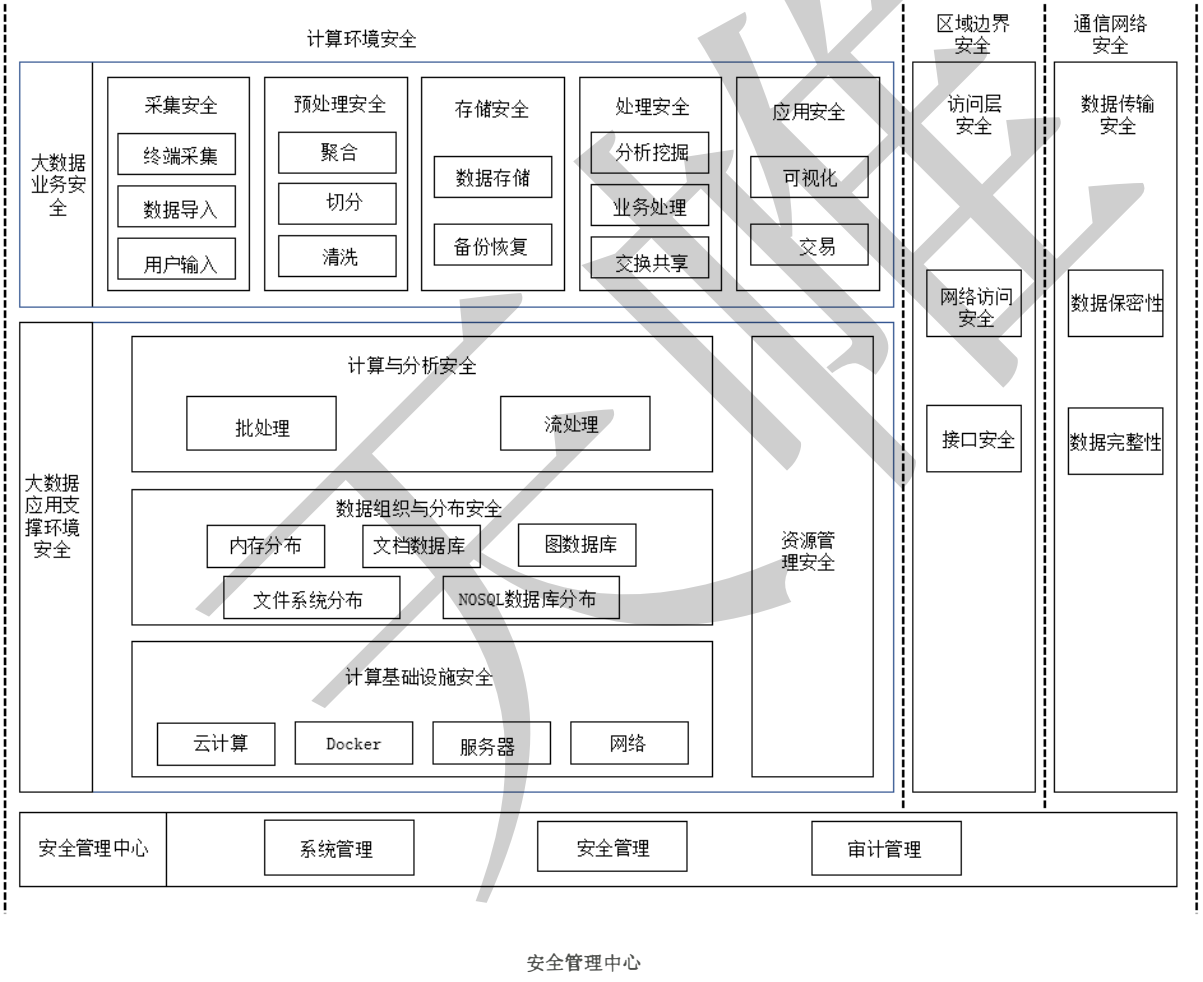

图 C.1 大数据系统等级保护安全技术设计框架

大数据业务安全：对采集、预处理、存储、处理及应用等大数据业务采用适合的安全防护技术，保障大数据应用的安全。

大数据应用支撑环境安全：对大数据应用的计算基础设施、数据组织与分布应用软件、计算与分析应用软件等各层面，采用适合的安全防护技术及监管措施，保障大数据应用支撑环境的安全。

区域边界安全：采用适合的网络安全防护技术，保障网络访问安全、接口安全等。

通信网络安全：对采集数据和用户数据的网络传输进行安全保护，保障数据传输过程的完整性和保密

性不受破坏。

安全管理中心:对系统管理、安全管理和审计管理实行统一管理。

C.2 第一级系统安全保护环境设计

C.2.1 大数据系统安全计算环境设计技术要求

a) 可信访问控制

应提供大数据访问可信验证机制,并对大数据的访问、处理及使用行为进行控制。

C.2.2 大数据系统安全区域边界设计技术要求

应遵守 6.3.2.1。

C.2.3 大数据系统安全通信网络设计技术要求

应遵守 6.3.3.1。

C.3 第二级系统安全保护环境设计

C.3.1 大数据系统安全计算环境设计技术 要求

a) 可信访问控制

应提供大数据访问可信验证机制,并对大数据的访问、处理及使用行为进行细粒度控制,对主体客体进行可信验证。

b) 数据保密性保护

应提供数据脱敏和去标识化等机制,确保敏感数据的安全性;应采用技术手段防止进行未授权的数据分析。

c) 剩余信息保护

应为大数据应用提供数据销毁机制,并明确销毁方式和销毁要求。

C.3.2 大数据系统安全区域边界设计技术要求

应遵守 7.3.2.1。

C.3.3 大数据系统安全通信网络设计技术要求

应遵守 7.3.3.1。

C.4 第三级系统安全保护环境设计

C.4.1 大数据系统安全计算环境设计技术要求

a) 可信访问控制

应对大数据进行分级分类,并确保在数据采集、存储、处理及使用的整个生命周期内分级分类策略的一致性;应提供大数据访问可信验证机制,并对大数据的访问、处理及使用行为进行细粒度控制,对主体客体进行可信验证。

b) 数据保密性保护

应提供数据脱敏和去标识化等机制,确保敏感数据的安全性;应采用技术手段防止进行未授权的

数据分析。

c) 剩余信息保护

应为大数据应用提供基于数据分类分级的数据销毁机制，并明确销毁方式和销毁要求。

d) 数据溯源

应采用技术手段实现敏感信息、个人信息等重要数据的数据溯源。

e) 个人信息保护

应仅采集和保护业务必须的个人信息。

C.4.2 大数据系统安全区域边界设计技术要求

a) 区域边界访问控制

应仅允许符合安全策略的设备通过受控接口接入大数据信息系统网络。

C.4.3 大数据系统安全通信网络设计技术要求

应遵守 8.3.3.1。

C.5 第四级系统安全保护环境设计

C.5.1 大数据系统安全计算环境设计技术要求

a) 可信访问控制

应对大数据进行分级分类，并确保在数据采集、存储、处理及使用的整个生命周期内分级分类策略的一致性；应提供大数据访问可信验证机制，并对大数据的访问、处理及使用行为进行细粒度控制，对主体客体进行可信验证。

b) 数据保密性保护

应提供数据脱敏和去标识化等机制，确保敏感数据的安全性；应提供数据加密保护机制，确保数据存储安全；应采用技术手段防止进行未授权的数据分析。

c) 剩余信息保护

应为大数据应用提供基于数据分类分级的数据销毁机制，并明确销毁方式和销毁要求。

d) 数据溯源

应采用技术手段实现敏感信息、个人信息等重要数据的数据溯源。

e) 个人信息保护

应仅采集和保护业务必须的个人信息。

C.5.2 大数据系统安全区域边界设计技术要求

a) 区域边界访问控制

应仅允许符合安全策略的设备通过受控接口接入大数据信息系统网络。

C.5.3 大数据系统安全通信网络设计技术要求

应遵守 9.3.3.1。

参 考 文 献

[1] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
[2] GB/T 20270—2006 信息安全技术 网络基础安全技术要求
[3] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[4] GB/T 20272—2006 信息安全技术 操作系统安全技术要求
[5] GB/T 20273—2006 信息安全技术 数据库管理系统安全技术要求
[6] GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求
[7] GB/T 21028—2007 信息安全技术 服务器安全技术要求
[8] GB/T 21052—2007 信息安全技术 信息系统物理安全技术要求
[9] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[10] GB/T 32400—2015 信息技术 云计算 概览与词汇
[11] GA/T 709—2007 信息安全技术 信息系统安全等级保护基本模型
[12] 信息安全等级保护管理办法（公通字〔2007〕43号）
[13] IEC/TS 62443-1-1 Industrial communication networks—Network and system security—Part 1-1: Terminology, concepts and models

中华人民共和国
国家标准
信息安全技术
网络安全等级保护安全设计技术要求
GB/T 25070—2019
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 3.25 字数 92 千字
2019年4月第一版 2019年4月第一次印刷
*
书号:155066·1-62417 定价 45.00 元

GB/T 25070-2019