ICS 35.040
L 80

中华人民共和国国家标准

GB/T 21028—2007

信息安全技术　服务器安全技术要求

Information security technology-
Security techniques requirement for server

2007-06-29 发布　　2007-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　　言

（略）

引　　言

本标准为设计、生产、制造、选配和使用所需要的安全等级的服务器提出了通用的安全技术要求，主要从服务器安全保护等级划分的角度来说明其技术要求，即为实现 GB 17859-1999 的要求对服务器通用安全技术进行了规范。

服务器是信息系统的主要组成部分，是由硬件系统和软件系统两大部分组成的，为网络环境中的客户端计算机提供特定的应用服务的计算机系统。服务器安全就是要对在服务器中存储、传输、处理和发布的数据信息进行安全保护，使其免遭由于人为的和自然的原因所带来的泄露、破坏和不可用的情况。服务器是以硬件系统和操作系统为基础，分别由数据库管理系统提供数据存储功能，以及由应用系统提供应用服务接口功能。因此，硬件系统和操作系统的安全便构成了服务器安全的基础。服务器安全从服务器组成的角度来看，硬件系统、操作系统、数据库管理系统、应用系统的安全保护构成了服务器安全。服务器的安全既要考虑服务器的安全运行保护，也要考虑对服务器中所存储、传输、处理和发布的数据信息的保护。由于攻击和威胁既可能是针对服务器运行的，也可能是针对服务器中所存储、传输、处理和发布的数据信息的保密性、完整性和可用性的，所以对服务器的安全保护的功能要求，需要从系统安全运行和信息安全保护两方面综合进行考虑。本标准依据 GB/T 20271-2006 关于信息系统安全保证要素的要求，从服务器的 SSOS 自身安全保护、SSOS 的设计和实现以及 SSOS 的安全管理等方面，对服务器的安全保证要求进行更加具体的描述。

本标准按照 GB 17859-1999，分五个等级对服务器的安全功能和安全保证提出详细技术要求。其中，第四章对服务器安全功能基本要求进行简要说明，第五章从安全功能要求和安全保证要求两个方面，按硬件系统、操作系统、数据库管理系统、应用系统和运行安全五个层次对服务器安全功能的分等级要求进行了详细说明。在此基础上，本标准的第五章对服务器安全功能分等级要求分别从安全功能要求和安全保证要求两方面进行了详细说明。在第五章的描述中除了引用以前各章的内容外，还引用了 GB/T 20271-2006 中关于安全保证技术要求的内容。为清晰表示每一个安全等级比较低一级安全等级的安全技术要求的增加和增强，在第 4 章的描述中，每一级新增部分用**“宋体加粗”**表示。

信息安全技术　服务器安全技术要求

1　范围

本标准依据 GB 17859-1999 的五个安全保护等级的划分，规定了服务器所需要的安全技术要求，以及每一个安全保护等级的不同安全技术要求。

本标准适用于按 GB 17859-1999 的五个安全保护等级的要求所进行的等级化服务器的设计、实现、选购和使用。按 GB 17859-1999 的五个安全保护等级的要求对服务器安全进行的测试、管理可参照使用。

2　规范性引用文件

下列文件中的有关条款通过在本标准的引用而成为本标准的条款。凡是注日期的引用文件，其后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859-1999　计算机信息系统安全保护等级划分准则

GB/T 20271-2006　信息安全技术　信息系统通用安全技术要求

GB/T 20272-2006　信息安全技术　操作系统安全技术要求

GB/T 20273-2006　信息安全技术　数据库管理系统安全技术要求

GB/T 20520-2006　信息安全技术　公钥基础设施　时间戳规范

3　术语、定义和缩略语

3.1　术语和定义

GB 17859-1999、GB/T 20271-2006、GB/T 20272-2006 、GB/T 20273-2006 和 GB/T 20520-2006 确立的以及下列术语和定义适用于本标准。

3.1.1

服务器　server

服务器是信息系统的主要组成部分，是信息系统中为客户端计算机提供特定应用服务的计算机系统，由硬件系统（如处理器、存储设备、网络连接设备等）和软件系统（如操作系统、数据库管理系统、应用系统等）组成。

3.1.2

服务器安全性　server security

服务器所存储、传输、处理的信息的保密性、完整性和可用性的表征。

3.1.3

服务器安全子系统(SSOS)　security subsystem of server

服务器中安全保护装置的总称，包括硬件、固件、软件和负责执行安全策略的组合体。它建立了一个基本的服务器安全保护环境，并提供服务器安全要求的附加用户服务。

3.1.4

安全要素　security element

本标准中各安全保护等级的安全技术要求所包含的安全内容的组成成份。

3.1.5

安全功能策略（SFP） security function policy

为实现 SSOS 安全要素要求的功能所采用的安全策略。

3.1.6

安全功能 security function

为实现 SSOS 安全要素的内容，正确实施相应安全功能策略所提供的功能。

3.1.7

SSOS 安全策略(SSP) SSOS security policy

对 SSOS 中的资源进行管理、保护和分配的一组规则。一个 SSOS 中可以有一个或多个安全策略。

3.1.8

SSOS 安全功能(SSF) SSOS security function

正确实施 SSOS 安全策略的全部硬件、固件、软件所提供的功能。每一个安全策略的实现，组成一个 SSOS 安全功能模块。一个 SSOS 的所有安全功能模块共同组成该 SSOS 的安全功能。

3.1.9

SSF 控制范围（SSC） SSF scope of control

SSOS 的操作所涉及的主体和客体的范围。

3.1.10

网络接口部件（NIC） network interface component

是服务器的重要组成部分，是服务器对网络提供支持的接口。

3.2 缩略语

SSOS 服务器安全子系统 security subsystem of server

SSF SSOS 安全功能 SSOS security function

SFP 安全功能策略 security function policy

SSC SSF 控制范围 SSF scope of control

SSP SSOS 安全策略 SSOS security policy

4 服务器安全功能要求

4.1 设备安全

4.1.1 设备标签

根据不同安全等级对服务器设备标签的不同要求，设备标签分为：

a) 设备标记：服务器设备应提供在显著位置设置标签（如编号、用途、负责人等）的功能，以方便查找和明确责任；

b) 部件标记：服务器关键部件（包括硬盘、主板、内存、处理器、网卡等）应在其上设置标签，以防止随意更换或取走。

4.1.2 设备可靠运行支持

根据不同安全等级对设备可靠运行支持的不同要求，可靠运行支持分为：

a) 基本运行支持：服务器硬件配置应满足软件系统基本运行的要求，关键部件应有数据校验能力；

b) 安全可用支持：服务器硬件配置应满足安全可用的要求，关键部件均安全可用；

c) 不间断运行支持：为满足服务器不间断运行要求，关键部件应具有容错、冗余或热插拔等安全功能，服务器应按照业务连续性要求提供双机互备的能力。

4.1.3 设备工作状态监控

构成服务器的关键部件，包括电源、风扇、机箱、磁盘控制等应具备可管理接口，通过该接口或

其它措施收集硬件的运行状态，如处理器工作温度、风扇转速、系统核心电压等，并对其进行实时监控，当所监测数值超过预先设定的故障阈值时，提供报警、状态恢复等处理。

4.1.4 设备电磁防护

应根据电磁防护强度与服务器安全保护等级相匹配的原则，按国家有关部门的规定分等级实施。

4.2 运行安全

4.2.1 安全监控

4.2.1.1 主机安全监控

根据不同安全等级对服务器主机安全监控的不同要求，主机安全监控分为：

a) 提供服务器硬件、软件运行状态的远程监控功能；

b) 对命令执行、进程调用、文件使用等进行实时监控，在必要时应提供监控数据分析功能。

4.2.1.2 网络安全监控

服务器应在其网络接口部件处对进出的网络数据流进行实时监控。根据不同安全等级对网络安全监控的不同要求，网络安全监控应：

a) 不依赖于服务器操作系统，且不因服务器出现非断电异常情况而不可用；

b) 对进出服务器的网络数据流，按既定的安全策略和规则进行检测；

c) 支持用户自定义网络安全监控的安全策略和规则；

d) 具有对网络应用行为分类监控的功能，并根据安全策略提供报警和阻断的能力；

e) 提供集中管理功能，以便接收网络安全监控集中管理平台下发的安全策略和规则，以及向网络安全监控集中管理平台提供审计数据源。

4.2.2 安全审计

4.2.2.1 安全审计的响应

安全审计 SSF 应按以下要求响应审计事件：

a） 审计日志记录：当检测到有安全侵害事件时，将审计数据记入审计日志；

b） 实时报警生成：当检测到有安全侵害事件时，生成实时报警信息，并根据报警开关的设置有选择地报警；

c） 违例进程终止：当检测到有安全侵害事件时，将违例进程终止；

d） 服务取消：当检测到有安全侵害事件时，取消当前的服务；

e） 用户账号断开与失效：当检测到有安全侵害事件时，将当前的用户账号断开，并使其失效。

4.2.2.2 安全审计数据产生

安全审计 SSF 应按以下要求产生审计数据：

a） 为下述可审计事件产生审计记录：

——审计功能的开启和关闭；

——使用身份鉴别机制；

——将客体引入用户地址空间（例如：打开文件、程序初始化）；

——删除客体；

——系统管理员、系统安全员、审计员和一般操作员所实施的操作；

——其他与系统安全有关的事件或专门定义的可审计事件；

b） 对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息；

c） 对于身份鉴别事件，审计记录应包含请求的来源（例如：末端标识符）；

d） 对于客体被引入用户地址空间的事件及删除客体事件，审计记录应包含客体名及客体的安全级。

4.2.2.3 安全审计分析

根据不同安全等级对安全审计分析的不同要求，安全审计分析分为：

a） 潜在侵害分析：用一系列规则监控审计事件，并根据这些规则指出对 SSP 的潜在侵害。这些规则包括：

——由已定义的可审计事件的子集所指示的潜在安全攻击的积累或组合；

——任何其它的规则；

b） 基于异常检测的描述：维护用户所具有的质疑等级——历史使用情况，以表明该用户的现行活动与已建立的使用模式的一致性程度。当用户的质疑等级超过阈值条件时，能指出将要发生对安全性的威胁；

c） 简单攻击探测：能检测到对 SSF 的实施有重大威胁的签名事件的出现。为此，SSF 应维护指出对 SSF 侵害的签名事件的内部表示，并将检测到的系统行为记录与签名事件进行比较，当发现两者匹配时，指出一个对 SSF 的攻击即将到来；

d） 复杂攻击探测：在上述简单攻击探测的基础上，能检测到多步入侵情况，并根据已知的事件序列模拟出完整的入侵情况，指出发现对 SSF 的潜在侵害的签名事件或事件序列的时间。

4.2.2.4 安全审计查阅

根据不同安全等级对安全审计查阅的不同要求，安全审计查阅分为：

a） 基本审计查阅：提供从审计记录中读取信息的能力，即为授权用户提供获得和解释审计信息的能力。当用户是人时，必须以人类可懂的方式表示信息；当用户是外部 IT 实体时，必须以电子方式无歧义地表示审计信息；

b） 有限审计查阅：在基本审计查阅的基础上，应禁止具有读访问权限以外的用户读取审计信息；

c） 可选审计查阅：在有限审计查阅的基础上，应具有根据准则来选择要查阅的审计数据的功能，并根据某种逻辑关系的标准提供对审计数据进行搜索、分类、排序的能力。

4.2.2.5 安全审计事件选择

应根据以下属性选择可审计事件：

a） 客体身份、用户身份、主体身份、主机身份、事件类型；

b） 作为审计选择性依据的附加属性。

4.2.2.6 安全审计事件存储

根据不同安全等级对安全审计事件存储的不同要求，安全审计事件存储分为：

a） 受保护的审计踪迹存储：审计踪迹的存储受到应有的保护，能检测或防止对审计记录的修改；

b） 审计数据的可用性确保：在意外情况出现时，能检测或防止对审计记录的修改，以及在发生审计存储已满、存储失败或存储受到攻击时，确保审计记录不被破坏；

c） 审计数据可能丢失情况下的措施：当审计跟踪超过预定的门限时，应采取相应的措施，进行审计数据可能丢失情况的处理；

d） 防止审计数据丢失：在审计踪迹存储记满时，应采取相应的防止审计数据丢失的措施，可选择“忽略可审计事件”、“阻止除具有特殊权限外的其他用户产生可审计事件”、“覆盖已存储的最老的审计记录”和“一旦审计存储失败所采取的其它行动”等措施，防止审计数据丢失。

4.2.3 恶意代码防护

根据不同安全等级对恶意代码防护的不同要求，恶意代码防护分为：

a) 主机软件防护：应在服务器中设置防恶意代码软件，对所有进入服务器的恶意代码采取相应的防范措施，防止恶意代码侵袭；

b) 整体防护：主机软件防护应与防恶意代码集中管理平台协调一致，及时发现和清除进入系统

内部的恶意代码。

4.2.4 备份与故障恢复

为了实现服务器安全运行，需要在正常运行时定期地或按某种条件进行适当备份，并在发生故障时进行相应恢复的功能，根据不同安全等级对备份与故障恢复的不同要求，服务器的备份与恢复功能分为：

a) 用户自我信息备份与恢复：应提供用户有选择地对操作系统、数据库系统和应用系统中重要信息进行备份的功能；当由于某种原因引起系统故障时，应能提供用户按自我信息备份所保留的备份信息进行恢复的功能；

b) 增量信息备份与恢复：提供定时对操作系统、数据库系统和应用系统中新增信息进行备份的功能；当由于某种原因引起系统中的某些信息丢失或破坏时，提供用户按增量信息备份所保留的信息进行信息恢复的功能；

c) 局部系统备份与恢复：应提供定期对操作系统、数据库系统和应用系统中的某些重要的局部系统的运行状态进行备份的功能；当由于某种原因引起系统某一局部发生故障时，应提供用户按局部系统备份所保留的运行状态进行局部系统恢复的功能；

d) 全系统备份与恢复：应提供对重要的服务器的全系统运行状态进行备份的功能；当由于某种原因引起服务器全系统发生故障时，应对用户按全系统备份所保留的运行状态进行全系统恢复提供支持；

e) 紧耦合集群结构：对关键服务器采用多服务器紧耦合集群结构，确保其中某一个服务器发生故障中断运行时，业务应用系统能在其余的服务器上不间断运行；

f) 异地备份与恢复：对关键的服务器，应根据业务连续性的不同要求，设置异地备份与恢复功能，确保服务器因灾难性故障中断运行时，业务应用系统能在要求的时间范围内恢复运行。

4.2.5 可信技术支持

通过在服务器上设置基于密码的可信技术支持模块，为在服务器上建立从系统引导、加载直到应用服务的可信任链，确保各种运行程序的真实性，并对服务器用户的身份鉴别、连接设备的鉴别，以及运用密码机制实现数据的保密性、完整性保护等安全功能提供支持。

4.2.6 可信时间戳

服务器应为其运行提供可靠的时钟和时钟同步系统，并按 GB/T20520-2006 的要求提供可信时间戳服务。

4.3 数据安全

4.3.1 身份鉴别

4.3.1.1 用户标识与鉴别

4.3.1.1.1 用户标识

根据不同安全等级对用户标识与鉴别的不同要求，用户标识分为：

a） 基本标识：应在 SSF 实施所要求的动作之前，先对提出该动作要求的用户进行标识；

b） 唯一性标识：应确保所标识用户在信息系统生存周期内的唯一性，并将用户标识与安全审计相关联；

c） 标识信息管理：应对用户标识信息进行管理、维护，确保其不被非授权地访问、修改或删除。

4.3.1.1.2 用户鉴别

根据不同安全等级对用户标识与鉴别的不同要求，用户鉴别分为：

a） 基本鉴别：应在 SSF 实施所要求的动作之前，先对提出该动作要求的用户成功地进行鉴别；

b） 不可伪造鉴别：应检测并防止使用伪造或复制的鉴别信息；一方面，要求 SSF 应检测或防止由任何别的用户伪造的鉴别数据，另一方面，要求 SSF 应检测或防止当前用户从任何其它用户处复制的鉴别数据的使用；

c） 一次性使用鉴别：应提供一次性使用鉴别数据的鉴别机制，即 SSF 应防止与已标识过的鉴别机制有关的鉴别数据的重用；

d） 多机制鉴别：应提供不同的鉴别机制，用于鉴别特定事件的用户身份，并根据不同安全等级所描述的多种鉴别机制如何提供鉴别的规则，来鉴别任何用户所声称的身份；

e） 重新鉴别：应有能力规定需要重新鉴别用户的事件，即在需要重新鉴别的条件成立时，对用户进行重新鉴别。例如，终端用户操作超时被断开后，重新连接时需要进行重鉴别；

f） 鉴别信息管理：应对用户鉴别信息进行管理、维护，确保其不被非授权的访问、修改或删除。

4.3.1.1.3 鉴别失败处理

SSF 应为不成功的鉴别尝试（包括尝试次数和时间的阈值）定义一个值，并明确规定达到该值时所应采取的动作。鉴别失败的处理应包括检测出现相关的不成功鉴别尝试的次数与所规定的数目相同的情况，并进行预先定义的处理。

4.3.1.2 用户-主体绑定

在 SSOS 安全功能控制范围之内，对一个已标识和鉴别的用户，应通过用户-主体绑定将该用户与为其服务的主体（如进程）相关联，从而将该用户的身份与该用户的所有可审计行为相关联，以实现用户行为的可查性。

4.3.2 自主访问控制

4.3.2.1 访问控制策略

SSF 应按确定的自主访问控制安全策略进行设计，实现对策略控制下的主体对客体操作的控制。可以有多个自主访问控制安全策略，但它们必须独立命名，且不能相互冲突。常用的自主访问控制策略包括：访问控制表访问控制、目录表访问控制等。

4.3.2.2 访问控制功能

SSF 应实现采用一条命名的访问控制策略的特定功能，说明策略的使用和特征，以及该策略的控制范围。

无论采用何种自主访问控制策略，SSF 应有能力提供：

——在安全属性或命名的安全属性组的客体上，执行访问控制 SFP；

——在基于安全属性的允许主体对客体访问的规则的基础上，允许主体对客体的访问；

——在基于安全属性的拒绝主体对客体访问的规则的基础上，拒绝主体对客体的访问。

4.3.2.3 访问控制范围

根据不同安全等级对自主访问控制的不同要求，自主访问控制的覆盖范围分为：

a） 子集访问控制：要求每个确定的自主访问控制，SSF 应覆盖由安全系统所定义的主体、客体及其之间的操作；

b） 完全访问控制：要求每个确定的自主访问控制，SSF 应覆盖信息系统中所有的主体、客体及其之间的操作，即要求 SSF 应确保 SSC 内的任意一个主体和任意一个客体之间的所有操作将至少被一个确定的访问控制 SFP 覆盖。

4.3.2.4 访问控制粒度

根据不同安全等级对访问控制的不同要求，自主访问控制的粒度分为：

a） 粗粒度：主体为用户/用户组级，客体为文件、数据库表级；

b） 中粒度：主体为用户级，客体为文件、数据库表级和/或记录、字段级；

c） 细粒度：主体为用户级，客体为文件、数据库表级和/或记录、字段/元素级。

4.3.3 标记

4.3.3.1 主体标记

应为实施强制访问控制的主体指定敏感标记，这些敏感标记是实施强制访问控制的依据。如：等

级分类和非等级类别组合的敏感标记是实施多级安全模型的基础。

4.3.3.2 客体标记

应为实施强制访问控制的客体指定敏感标记，这些敏感标记是实施强制访问控制的依据。如：等级分类和非等级类别组合的敏感标记是实施多级安全模型的基础。

4.3.3.3 标记的输出

当数据从 SSC 之内向其控制范围之外输出时，根据需要可以保留或不保留数据的敏感标记。根据不同安全等级对标记输出的不同要求，标记的输出分为：

a） 不带敏感标记的用户数据输出：在 SFP 的控制下输出用户数据到 SSC 之外时，不带有与数据相关的敏感标记；

b） 带有敏感标记的用户数据输出：在 SFP 的控制下输出用户数据到 SSC 之外时，应带有与数据相关的敏感标记，并确保敏感标记与所输出的数据相关联。

4.3.3.4 标记的输入

当数据从 SSF 控制范围之外向其控制范围之内输入时，应有相应的敏感标记，以便输入的数据能受到保护。根据不同安全等级对标记输入的不同要求，标记的输入分为：

a） 不带敏感标记的用户数据输入：SSF 应做到：

——在 SFP 控制下从 SSC 之外输入用户数据时，应执行访问控制 SFP；

——略去任何与从 SSC 之外输入的数据相关的敏感标记；

——执行附加的输入控制规则，为输入数据设置敏感标记；

b） 带有敏感标记的用户数据输入：SSF 应做到：

——在 SFP 控制下从 SSC 之外输入用户数据时，应执行访问控制 SFP；

——SSF 应使用与输入的数据相关的敏感标记；

——SSF 应在敏感标记和接收的用户数据之间提供确切的联系；

——SSF 应确保对输入的用户数据的敏感标记的解释与原敏感标记的解释是一致的。

4.3.4 强制访问控制

4.3.4.1 访问控制策略

强制访问控制策略应包括策略控制下的主体、客体，及由策略覆盖的被控制的主体与客体间的操作。可以有多个访问控制安全策略，但它们必须独立命名，且不能相互冲突。当前常见的强制访问控制策略有：

a） 多级安全模型：基本思想是，在对主、客体进行标记的基础上，SSOS 控制范围内的所有主体对客体的直接或间接的访问应满足：

——向下读原则：仅当主体标记中的等级分类高于或等于客体标记中的等级分类，且主体标记中的非等级类别包含了客体标记中的全部非等级类别，主体才能读该客体；

——向上写原则：仅当主体标记中的等级分类低于或等于客体标记中的等级分类，且主体标记中的非等级类别包含于客体标记中的非等级类别，主体才能写该客体；

b） 基于角色的访问控制（BRAC）：基本思想是，按角色进行权限的分配和管理；通过对主体进行角色授予，使主体获得相应角色的权限；通过撤消主体的角色授予，取消主体所获得的相应角色权限。在基于角色的访问控制中，标记信息是对主体的授权信息；

c） 特权用户管理：基本思想是，针对特权用户权限过于集中所带来的安全隐患，对特权用户按最小授权原则进行管理。实现特权用户的权限分离；仅授予特权用户为完成自身任务所需要的最小权限。

4.3.4.2 访问控制功能

SSF 应明确指出采用一条命名的强制访问控制策略所实现的特定功能。SSF 应有能力提供：

——在标记或命名的标记组的客体上，执行访问控制 SFP；

——按受控主体和受控客体之间的允许访问规则，决定允许受控主体对受控客体执行受控操作；

——按受控主体和受控客体之间的拒绝访问规则，决定拒绝受控主体对受控客体执行受控操作。

4.3.4.3 访问控制范围

根据不同安全等级对强制访问控制范围的不同要求，强制访问控制的覆盖范围分为：

a) 子集访问控制：对每个确定的强制访问控制，SSF 应覆盖信息系统中由安全功能所定义的主体、客体及其之间的操作；

b) 完全访问控制：对每个确定的强制访问控制，SSF 应覆盖信息系统中所有的主体、客体及其之间的操作，即要求 SSF 应确保 SSC 内的任意一个主体和任意一个客体之间的操作将至少被一个确定的访问控制 SFP 覆盖。

4.3.4.4 访问控制粒度

根据不同安全等级对强制访问控制粒度的不同要求，强制访问控制的粒度分为：

a） 中粒度：主体为用户级，客体为文件、数据库表级和/或记录、字段级；

b） 细粒度：主体为用户级，客体为文件、数据库表级和/或记录、字段和/或元素级。

4.3.4.5 访问控制环境

强制访问控制应考虑以下不同的系统运行环境：

a） 单一安全域环境：在单一安全域环境实施的强制访问控制应在该环境中维持统一的标记信息和访问规则；当被控客体输出到安全域以外时，应将其标记信息同时输出；

b） 多安全域环境：在多安全域环境实施统一安全策略的强制访问控制时，应在这些安全域中维持统一的标记信息和访问规则；当被控制客体在这些安全域之间移动时，应将其标记信息一起移动。

4.3.5 数据完整性

4.3.5.1 存储数据的完整性

应对存储在 SSC 内的用户数据进行完整性保护。根据不同安全等级对用户数据完整性保护的不同要求，存储数据的完整性分为：

a） 完整性检测：SSF 应对存储在 SSC 内的用户数据在读取操作时进行完整性检测，以发现数据完整性被破坏的情况；

b） 完整性检测和恢复：SSF 应对存储在 SSC 内的用户数据在读取操作时进行完整性检测，并在检测到完整性错误时，采取必要的恢复措施。

4.3.5.2 传输数据的完整性

当用户数据在 SSF 和 SSF 间传输时应提供完整性保护。根据不同安全等级对用户数据完整性保护的不同要求，传输数据的完整性分为：

a） 完整性检测：SSF 应对经网络传输的用户数据在传输过程中进行完整性检测，及时发现以某种方式传送或接收的用户数据被篡改、删除、插入等情况发生；

b） 完整性检测和恢复：SSF 应对经网络传输的用户数据在传输过程中进行完整性检测，及时发现以某种方式传送或接收的用户数据被篡改、删除、插入等情况发生，并在检测到完整性错误时，采取必要的恢复措施。

4.3.5.3 处理数据的完整性

对信息系统中处理中的数据，应通过“回退”进行完整性保护，即 SSF 应执行数据处理完整性 SFP，以允许对所定义的操作序列进行回退。

4.3.6 数据保密性

4.3.6.1 存储数据保密性保护

对存储在 SSC 内的用户数据，应根据不同数据类型的不同保密性要求，进行不同程度的保密性保

护，确保除具有访问权限的合法用户外，其余任何用户不能获得该数据。

4.3.6.2 传输数据保密性保护

对在不同 SSF 之间或不同 SSF 上的用户之间传输的用户数据，应根据不同数据类型的不同保密性要求，进行不同程度的保密性保护，确保数据在传输过程中不被泄漏和窃取。

4.3.6.3 客体安全重用

在对资源进行动态管理的系统中，客体资源（寄存器、内存、磁盘等记录介质）中的剩余信息不应引起信息的泄漏。根据不同安全等级对用户数据保密性保护的不同要求，客体安全重用分为：

a） 子集信息保护：由 SSOS 安全控制范围之内的某个子集的客体资源，在将其释放后再分配给某一用户或代表该用户运行的进程时，应不会泄漏该客体中的原有信息；

b） 完全信息保护：由 SSOS 安全控制范围之内的所有客体资源，在将其释放后再分配给某一用户或代表该用户运行的进程时，应不会泄漏该客体中的原有信息；

c） 特殊信息保护：在完全信息保护的基础上，对于某些需要特别保护的信息，应采用专门的方法对客体资源中的残留信息做彻底清除，如对剩磁的清除等。

4.3.7 数据流控制

在以数据流方式实现数据流动的信息系统中，应采用数据流控制机制实现对数据流动的安全控制，以防止具有高等级安全的数据信息向低等级的区域流动。

4.3.8 可信路径

用户与 SSF 间的可信路径应：

a） 提供真实的端点标识，并保护通信数据免遭修改和泄漏；

b） 利用可信路径的通信可以由 SSF 自身、本地用户或远程用户发起；

c） 对原发用户的鉴别或需要可信路径的其它服务均使用可信路径。

5 服务器安全分等级要求

5.1 第一级：用户自主保护级

5.1.1 安全功能要求

5.1.1.1 硬件系统

5.1.1.1.1 设备标记

按 4.1.1 中设备标记的要求，设计和实现服务器设备标记的安全功能，设备标记一般采用标签。

5.1.1.1.2 设备可靠运行支持

按 4.1.2 中基本运行支持的要求，设计和实现服务器设备可靠运行支持的安全功能，服务器硬件最低配制应满足软件系统运行的要求，关键部件（包括 CPU、内存等）应具有数据校验功能。

5.1.1.1.3 设备电磁防护

按 4.1.4 的要求，设计和实现服务器设备电磁防护功能，防止电磁信息泄露，以及屏蔽外界电磁干扰。

5.1.1.2 操作系统

按 GB/T 20272-2006 4.1.1 的要求，从以下方面来设计、实现或选购用户自主保护级服务器所需要的操作系统：

a) 身份鉴别：根据 4.3.1 的描述，确保登录操作系统的用户身份的唯一性和真实性；

b) 自主访问控制：根据 4.3.2 的描述，对操作系统的访问进行控制，允许合法操作，拒绝非法操作；

c) 数据完整性：根据 4.3.5 的描述，确保操作系统内部传输数据的完整性。

5.1.1.3 数据库管理系统

按 GB/T 20273-2006 5.1.1 的要求，从以下方面来设计、实现或选购用户自主保护级服务器所需要

的数据库管理系统：

a） 身份鉴别：根据 4.3.1 的描述，确保登录数据库管理系统的用户身份的唯一性和真实性；

b） 自主访问控制：根据 4.3.2 的描述，对数据库管理系统的访问进行控制，允许合法操作，拒绝非法操作；

c） 数据完整性：根据 4.3.5 的描述，对数据库管理系统内部传输的用户数据应提供保证用户数据完整性的功能。

5.1.1.4 应用系统

5.1.1.4.1 身份鉴别

根据 4.3.1 的描述，按 GB/T 20271-20066.1.3.1 的要求，从以下方面设计和实现应用系统的身份鉴别功能：

a） 身份标识：凡需进入应用系统的管理用户，应先进行标识（建立账号）；应用系统管理用户标识一般使用用户名和用户标识符（UID）；

b） 身份鉴别：采用口令进行鉴别，并在每次用户登录应用系统时进行鉴别；口令应是不可见的，并在存储时有安全保护；对注册到应用系统的用户，应通过用户-主体绑定功能将用户与为其服务的主体相关联。

5.1.1.4.2 自主访问控制

根据 4.3.2 的描述，按 GB/T 20271-2006 6.1.3.2 的要求，从以下方面设计和实现应用系统的自主访问控制功能：

a） 允许命名用户以用户和/或用户组的身份规定并控制对客体的共享，并阻止非授权用户对客体的共享；

b） 自主访问控制的粒度应是粗粒度。

5.1.1.4.3 数据完整性

根据 4.3.5 的描述，按 GB/T 20271-20066.1.3.3 的要求，从以下方面设计和实现应用系统的数据完整性功能：

a） 对应用系统内部进行的数据传输，如进程间的通信，应提供保证数据完整性的功能。

5.1.1.5 运行安全

5.1.1.5.1 恶意代码防护

按 4.2.3 中主机软件防护的要求，设计和实现恶意代码防护功能。

5.1.1.5.2 备份与故障恢复

按 4.2.4 中用户自我信息备份与恢复的要求，设计和实现服务器备份与故障恢复的功能。

5.1.2 安全保证要求

5.1.2.1 SSOS 自身安全保护

a) SSF 物理安全保护：按 GB/T 20271-2006 6.1.4.1 的要求，实现服务器用户自主保护级 SSF 的物理安全保护；

b) SSF 运行安全保护：按 GB/T 20271-2006 6.1.4.2 的要求，实现服务器用户自主保护级 SSF 的运行安全保护；

c) SSF 数据安全保护：按 GB/T 20271-2006 6.1.4.3 的要求，实现服务器用户自主保护级 SSF 的数据按保护；

d) 资源利用：按 GB/T 20271-2006 6.1.4.4 的要求，实现服务器用户自主保护级的资源利用；

e) SSOS 访问控制：按 GB/T 20271-2006 6.1.4.5 的要求，实现服务器用户自主保护级的 SSOS 访问控制。

5.1.2.2 SSOS 设计和实现

a) 配置管理：按 GB/T 20271-2006 6.1.5.1 的要求，实现服务器用户自主保护级的配置管理；

b) 分发和操作：按 GB/T 20271-2006 6.1.5.2 的要求，实现服务器用户自主保护级的分发和操作；

c) 开发：按 GB/T 20271-2006 6.1.5.3 的要求，实现服务器用户自主保护级的开发；

d) 指导性文档：按 GB/T 20271-2006 6.1.5.4 的要求，实现服务器用户自主保护级的指导性文档；

e) 生命周期支持：按 GB/T 20271-2006 6.1.5.5 的要求，实现服务器用户自主保护级的生命周期支持；

f) 测试：按 GB/T 20271-2006 6.1.5.6 的要求，实现服务器用户自主保护级的测试。

5.1.2.3 SSOS 安全管理

按 GB/T 20271-2006 6.1.6 的要求，实现服务器用户自主保护级的 SSOS 安全管理。

5.2 第二级：系统审计保护级

5.2.1 安全功能要求

5.2.1.1 硬件系统

5.2.1.1.1 设备标记

按 4.1.1 中设备标记**和部件标记**的要求，设计和实现服务器设备标记的安全功能，标记一般采用标签的形式，**安全标记应采取保护措施（如加盖公章）**。

5.2.1.1.2 设备可靠运行支持

按 4.1.2 中基本运行支持**和安全可用支持**的要求，设计和实现服务器设备可靠运行支持的安全功能，服务器硬件最低配制应满足软件系统运行的要求；**关键部件（包括硬盘、主板、内存、处理器、网卡等）应与其标记配合，保证其安全性，以防止更换和取走；机箱面板应提供保护措施，如加锁保护。**

5.2.1.1.3 设备电磁防护

按 4.1.4 的要求，设计和实现服务器设备电磁防护功能，防止电磁信息泄露，以及屏蔽外界电磁干扰。

5.2.1.2 操作系统

按 **GB/T 20272-2006 4.2.1** 的要求，从以下方面来设计、实现或选购**系统审计保护级**服务器所需要的操作系统：

a) 身份鉴别：根据 4.3.1 的描述，确保登录操作系统的用户身份的唯一性和真实性；

b) 自主访问控制：根据 4.3.2 的描述，对操作系统的访问进行控制，允许合法操作，拒绝非法操作；

c) 安全审计：根据 4.2.2 的描述，提供操作系统安全审计功能；

d) 数据完整性：根据 4.3.5 的描述，对操作系统内部**存储、处理**和传输的用户数据应提供保证用户数据完整性的功能；

e) 数据保密性：根据 4.3.6 的描述，设计和实现操作系统的用户数据保密性保护功能。

5.2.1.3 数据库管理系统

按 **GB/T 20273-2006 5.2.1** 的要求，从以下方面来设计、实现或选购**系统审计保护级**服务器所需要的数据库管理系统：

a) 身份鉴别：根据 4.3.1 的描述，确保登录数据库管理系统的用户身份的唯一性和真实性；

b) 自主访问控制：根据 4.3.2 的描述，对数据库管理系统的访问进行控制，允许合法操作，拒绝非法操作；

c) 安全审计：根据 4.2.2 的描述，提供数据库管理系统安全审计功能；

d) 数据完整性：根据 4.3.5 的描述，对数据库管理系统内部**存储、处理和**传输的用户数据应提供保证用户数据完整性的功能；

e) 数据保密性：根据 4.3.6 的描述，设计和实现数据库管理系统的用户数据保密性保护功能。

5.2.1.4 应用系统

5.2.1.4.1 身份鉴别

根据 4.3.1 的描述，**按 GB/T 20271-2006 6.2.3.1 的要求，**从以下方面设计和实现应用系统的身份鉴别功能：

a) 身份标识：凡需进入应用系统的用户，应先进行标识（建立账号）；应用系统用户标识一般使用用户名和用户标识符（UID）；**并在应用系统的整个生存周期实现用户的唯一性标识，以及用户名或别名、UID 等之间的一致性；**

b) 身份鉴别：**采用强化管理的口令鉴别/基于令牌的动态口令鉴别等机制进行身份鉴别，并**在每次用户登录应用系统时进行鉴别；**鉴别信息**应是不可见的，并在存储**和传输**时有安全保护。对注册到应用系统的管理用户，应通过用户-主体绑定功能将用户与为其服务的主体相关联。

5.2.1.4.2 自主访问控制

根据 4.3.2 的描述，按 **GB/T 20271-2006 6.2.3.2** 的要求，从以下方面设计和实现应用系统的自主访问控制功能：

a) 允许命名用户以**用户的身份**规定并控制对客体的共享，并阻止非授权用户对客体的共享；

b) **用存取控制表访问控制等访问控制表访问控制确定主体对客体的访问权限；**

c) 自主访问控制的粒度应是**中粒度；**

d) **自主访问控制应与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。**

5.2.1.4.3 安全审计

根据 4.2.2 的描述，按 GB/T 20271-2006 6.2.2.3 的要求，从以下方面设计和实现应用系统的安全审计功能：

a) 安全审计功能的设计应与用户标识与鉴别、自主访问控制等安全功能的设计紧密结合；

b) 提供审计日志，潜在侵害分析，基本审计查阅和有限审计查阅，安全审计事件选择，以及受保护的审计踪迹存储等功能；

c) 能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问；

d) 能够创建并维护一个对受保护客体访问的审计跟踪，保护审计记录不被未授权的访问、修改和破坏。

5.2.1.4.4 数据完整性

根据 4.3.5 的描述，按 **GB/T 20271-2006 6.2.3.3** 的要求，从以下方面设计和实现应用系统的数据完整性功能：

a) **在对服务进行访问操作时，检查字符串形式提交给应用系统中的用户数据是否出现完整性错误；**

b) 对应用系统内部进行的数据传输，如进程间的通信，应提供保证数据完整性的功能；

c) **对应用系统中处理的用户数据，应按回退的要求设计相应的数据库管理系统安全功能模块，进行异常情况的事务回退，以确保数据的完整性。**

5.2.1.4.5 数据保密性

根据 4.3.6 的描述，按 GB/T 20271-2006 6.2.3.4 的要求，设计和实现应用系统的用户数据保密性保护功能。

5.2.1.5 运行安全

5.2.1.5.1 恶意代码防护

按 4.2.3 中主机软件防护的要求，设计和实现恶意代码防护功能。

5.2.1.5.2 备份与故障恢复

按 4.2.4 中用户自我信息备份与恢复、**增量信息备份与恢复、局部系统备份与恢复**的要求，设计

和实现服务器备份与故障恢复的功能。

5.2.2 安全保证要求

5.2.2.1 SSOS 自身安全保护

a) SSF 物理安全保护：宜按 **GB/T 20271-2006 6.2.4.1** 的要求，实现服务器系统审计保护级 SSF 的物理安全保护；
b) SSF 运行安全保护：宜按 **GB/T 20271-2006 6.2.4.2** 的要求，实现服务器系统审计保护级 SSF 的运行安全保护；
c) SSF 数据安全保护：宜按 **GB/T 20271-2006 6.2.4.3** 的要求，实现服务器系统审计保护级 SSF 的数据按保护；
d) 资源利用：宜按 **GB/T 20271-2006 6.2.4.4** 的要求，实现服务器系统审计保护级的资源利用；
e) SSOS 访问控制：宜按 **GB/T 20271-2006 6.2.4.5** 的要求，实现服务器系统审计保护级的 SSOS 访问控制。

5.2.2.2 SSOS 设计和实现

a) 配置管理：宜按 **GB/T 20271-2006 6.2.5.1** 的要求，实现服务器系统审计保护级的配置管理；
b) 分发和操作：宜按 **GB/T 20271-2006 6.2.5.2** 的要求，实现服务器系统审计保护级的分发和操作；
c) 开发：宜按 **GB/T 20271-2006 6.2.5.3** 的要求，实现服务器系统审计保护级的开发；
d) 指导性文档：宜按 **GB/T 20271-2006 6.2.5.4** 的要求，实现服务器系统审计保护级的指导性文档；
e) 生命周期支持：宜按 **GB/T 20271-2006 6.2.5.5** 的要求，实现服务器系统审计保护级的生命周期支持；
f) 测试：宜按 **GB/T 20271-2006 6.2.5.6** 的要求，实现服务器系统审计保护级的测试。

5.2.2.3 SSOS 管理

按 **GB/T 20271-2006 6.2.6** 的要求，实现服务器系统审计保护级的 SSOS 安全管理。

5.3 第三级：安全标记保护级

5.3.1 安全功能要求

5.3.1.1 硬件系统

5.3.1.1.1 设备标记

应按 4.1.1 中设备标记和部件标记的要求，设计和实现服务器设备标记的安全功能，标记一般采用标签，安全标记应采取保护措施（如加盖公章）。

5.3.1.1.2 设备可靠运行支持

应按 4.1.2 中基本运行支持、安全可用支持和**不间断运行支持**的要求，设计和实现服务器设备可靠运行支持的安全功能，服务器硬件最低配制应满足软件系统运行的要求；关键部件应与其标记配合，保证其安全性，以防止更换和取走，机箱面板应提供保护措施；**不间断运行要求应满足关键部件具有容错、冗余和热插拔等安全功能。支持热插拔功能的部件应包括：硬盘、风扇、电源等；电源、硬盘应采取冗余措施，内存应具有容错功能，关键服务器应采用双机互备技术保证业务连续性要求。**

5.3.1.1.3 设备工作状态监控

应按 4.1.3 的要求，设计和实现服务器设备工作状态监控的安全功能，对监测数值超过预先设定的故障阈值时，提供报警功能。

5.3.1.1.4 设备电磁防护

应按 4.1.4 的要求，设计和实现服务器设备电磁防护功能，防止电磁信息泄露，以及屏蔽外界电磁干扰。

5.3.1.2 操作系统

应按 **GB/T 20272-2006 4.3.1** 的要求，从以下方面来设计、实现或选购**安全标记保护级**服务器所需要的操作系统：

a) 身份鉴别：根据 4.3.1 的描述，确保登录操作系统的用户身份的唯一性和真实性；

b) 自主访问控制：根据 4.3.2 的描述，对操作系统的访问进行控制，允许合法操作，拒绝非法操作；

c) **标记：根据 4.3.3 的描述，设计和实现操作系统标记功能，为主、客体设置所需要的敏感标记；**

d) **强制访问控制：根据 4.3.4 的描述，对操作系统的访问进行控制，允许合法操作，拒绝非法操作；应对操作系统实现包括系统文件、服务、驱动、注册表及进程在内的强制访问控制功能；**

e) **数据流控制：对于以数据流方式实现数据交换的操作系统， 根据 4.3.7 的描述，设计和实现操作系统的数据流控制功能；**

f) 安全审计：根据 4.2.2 描述，提供操作系统安全审计功能；

a) 数据完整性：根据 4.3.5 的描述，对操作系统内部存储、处理和传输的用户数据应提供保证用户数据完整性的功能；

g) 数据保密性：根据 4.3.6 的描述，设计和实现操作系统的用户数据保密性保护功能。

5.3.1.3 数据库管理系统

应按 **GB/T 20273-2006 5.3.1** 的要求，从以下方面来设计、实现或选购**安全标记保护级**服务器所需要的数据库管理系统：

a) 身份鉴别：根据 4.3.1 的描述，确保登录数据库管理系统的用户身份的唯一性和真实性；

b) 自主访问控制：根据 4.3.2 的描述，对数据库管理系统的访问进行控制，允许合法操作，拒绝非法操作；

c) **标记：根据 4.3.3 的描述，设计和实现数据库管理系统标记功能，为主、客体设置所需要的敏感标记；**

d) **强制访问控制：根据 4.3.4 的描述，对数据库管理系统的访问进行控制，允许合法操作，拒绝非法操作；**

e) **数据流控制：对于以数据流方式实现数据交换的数据库管理系统，根据 4.3.7 的描述，设计和实现数据库管理系统的数据流控制功能；**

f) 安全审计：根据 4.2.2 描述，提供数据库管理系统安全审计功能；

g) 数据完整性：对数据库管理系统内部存储、处理和传输的用户数据应提供保证用户数据完整性的功能；

h) 数据保密性：根据 4.3.6 的描述，设计和实现数据库管理系统的用户数据保密性保护功能。

5.3.1.4 应用系统

5.3.1.4.1 身份鉴别

应根据 4.3.1 的描述，按 **GB/T 20271-2006 6.3.3.1** 的要求，从以下方面设计和实现应用系统的身份鉴别功能：

a) 身份标识：凡需进入应用系统的管理用户，应先进行标识（建立账号）；应用系统管理用户标识一般使用用户名和用户标识符（UID）；并在应用系统的整个生存周期实现用户的唯一性标识，以及用户名或别名、UID 等之间的一致性；

b) 身份鉴别：采用强化管理的口令鉴别/基于令牌的动态口令鉴别/**生物特征鉴别/数字证书鉴别等机制**等机制进行身份鉴别，并在每次管理用户登录应用系统时进行鉴别；鉴别信息应是不可见的，**应采用加密技术对鉴别信息进行保护**；对注册到应用系统的管理用户，应通过用户-

主体绑定功能将用户与为其服务的主体相关联。

5.3.1.4.2 自主访问控制

应根据 4.3.2 的描述，按 **GB/T 20271-2006 6.3.3.3** 的要求，从以下方面设计和实现应用系统的自主访问控制功能：

a) 允许命名用户以用户的身份规定并控制对客体的共享，并阻止非授权用户对客体的共享；

b) 用存取控制表访问控制等访问控制表访问控制确定主体对客体的访问权限；

c) 自主访问控制的粒度应是中粒度；

d) 自主访问控制应与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。

5.3.1.4.3 标记

应根据 4.3.3 的描述，按 GB/T 20271-2006 6.3.3.4 的要求，从以下方面设计和实现应用系统的标记功能：

a) 应有系统用户的敏感标记，应在用户建立注册账户后由系统安全员为其设置标记；

b) 应用系统客体的敏感标记，应在数据输入到安全控制范围内时以默认方式生成或由安全员通过操作界面进行标记。

5.3.1.4.4 强制访问控制

应根据 4.3.4 的描述，按 GB/T 20271-2006 6.3.3.5 的要求，从以下方面设计和实现应用系统的强制访问控制功能：

a) 将强制访问控制的范围应限定在所定义的主体与客体，并且，强制访问控制的客体粒度应是中粒度；

b) 应将系统的常规管理、与安全有关的管理以及审计管理，分别由应用系统管理员、系统安全员和系统审计员来承担，按最小授权原则分别授予它们各自为完成自己承担任务所需的最小权限，并形成相互制约的关系。

5.3.1.4.5 数据流控制

对于以数据流方式实现数据交换应用系统， 应根据 4.3.7 的描述，按 GB/T 20271-2006 6.3.3.6 的要求，设计和实现应用系统的数据流控制功能。

5.3.1.4.6 安全审计

应根据 4.2.2 的描述，按 **GB/T 20271-2006 6.3.2.4** 的要求，从以下方面设计和实现应用系统的安全审计功能：

a) 安全审计功能的设计应与用户标识与鉴别、自主访问控制、**标记与强制访问控制**等安全功能的设计紧密结合；

b) 提供审计日志、**实时报警生成**，潜在侵害分析、**基于异常检测**，基本审计查阅、有限审计查阅和**可选审计查阅**，安全审计事件选择，以及受保护的审计踪迹存储和**审计数据的可用性确保**等功能；

c) 能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问；

d) 能够创建并维护一个对受保护客体访问的审计跟踪，保护审计记录不被未授权的访问、修改和破坏；

e) 对网络环境下运行的应用系统，应建立统一管理和控制的审计机制。

5.3.1.4.7 数据完整性

应根据 4.3.5 的描述，按 **GB/T 20271-2006 6.3.3.7** 的要求,从以下方面设计和实现应用系统的数据完整性功能：

a) 在对服务进行访问操作时，检查字符串形式提交给应用系统中的用户数据是否出现完整性错误；

b) 对应用系统内部进行的数据传输，如进程间的通信，应提供保证数据完整性的功能；

c) 对应用系统中处理的用户数据，应按回退的要求设计相应的数据库管理系统安全功能模块，进行异常情况的事务回退，以确保数据的完整性。

5.3.1.4.8 数据保密性

应根据 4.3.6 的描述，按 **GB/T 20271-2006 6.3.3.8** 的要求，设计和实现应用系统的用户数据保密性保护功能。

5.3.1.5 运行安全

5.3.1.5.1 安全监控

按 4.2.1 主机安全监控和网络安全监控的要求，设计和实现服务器安全监控的功能。

5.3.1.5.2 恶意代码防护

按 4.2.3 中主机软件防护和**整体防护**的要求，设计和实现恶意代码防护功能。

5.3.1.5.3 备份与故障恢复

按 4.2.4 中用户自我信息备份与恢复、增量信息备份与恢复、局部系统备份与恢复、**全系统备份与恢复**的要求，设计和实现服务器备份与故障恢复的功能。

5.3.1.5.4 可信时间戳

按 4.2.6 中可信时间戳的要求，设计和实现服务器可信时间戳功能。

5.3.2 安全保证要求

5.3.2.1 SSOS 自身安全保护

a) SSF 物理安全保护：应按 **GB/T 20271-2006 6.3.4.1** 的要求，实现服务器安全标记保护级 SSF 的物理安全保护；

b) SSF 运行安全保护：应按 **GB/T 20271-2006 6.3.4.2** 的要求，实现服务器安全标记保护级 SSF 的运行安全保护；

c) SSF 数据安全保护：应按 **GB/T 20271-2006 6.3.4.3** 的要求，实现服务器安全标记保护级 SSF 的数据按保护；

d) 资源利用：应按 **GB/T 20271-2006 6.3.4.4** 的要求，实现服务器安全标记保护级的资源利用；

e) SSOS 访问控制：应按 **GB/T 20271-2006 6.3.4.5** 的要求，实现服务器安全标记保护级的 SSOS 访问控制。

5.3.2.2 SSOS 设计和实现

a) 配置管理：应按 **GB/T 20271-2006 6.3.5.1** 的要求，实现服务器安全标记保护级的配置管理；

b) 分发和操作：应按 **GB/T 20271-2006 6.3.5.2** 的要求，实现服务器安全标记保护级的分发和操作；

c) 开发：应按 **GB/T 20271-2006 6.3.5.3** 的要求，实现服务器安全标记保护级的开发；

d) 指导性文档：应按 **GB/T 20271-2006 6.3.5.4** 的要求，实现服务器安全标记保护级的指导性文档；

e) 生命周期支持：应按 **GB/T 20271-2006 6.3.5.5** 条的要求，实现服务器安全标记保护级的生命周期支持；

f) 测试：应按 **GB/T 20271-2006 6.3.5.6** 的要求，实现服务器安全标记保护级的测试；

g) 脆弱性评定：应按 **GB/T 20271-2006 6.3.5.7** 的要求，实现网络安全标记保护级的脆弱性评定。

5.3.2.3 SSOS 管理

应按 **GB/T 20271-2006 6.3.6** 的要求，实现服务器安全标记保护级的 SSOS 安全管理。

5.4 第四级：结构化保护级

5.4.1 安全功能要求

5.4.1.1 硬件系统

5.4.1.1.1 设备标记

应按 4.1.1 中设备标记和部件标记的要求，设计和实现服务器设备标记的安全功能，设备标记一般采用标签；**部件标记应采用数字标签。**安全标记应采取保护措施（如加盖公章）。

5.4.1.1.2 设备可靠运行支持

应按 4.1.2 中基本运行支持、安全可用支持和不间断运行支持的要求，设计和实现服务器设备可靠运行支持的安全功能，服务器硬件最低配制应满足软件系统运行的要求；关键部件应与其标记配合，保证其安全性，以防止更换和取走，机箱面板应提供保护措施；不间断运行要求应满足关键部件具有容错、冗余和热插拔等安全功能。支持热插拔功能的部件应包括：硬盘、风扇、电源、**PCI 适配器、网卡、内存、CPU 等；**电源、硬盘、**网卡**应采取冗余措施，内存应具有容错功能，关键服务器应采用双机互备技术保证业务连续性要求。

5.4.1.1.3 设备工作状态监控

应按 4.1.3 的要求，设计和实现服务器设备工作状态监控的安全功能，对监测数值超过预先设定的故障阈值时，提供报警和**状态恢复功能。**

5.1.1.1.4 设备电磁防护

应按 4.1.4 的要求，设计和实现服务器设备电磁防护功能，防止电磁信息泄露，以及屏蔽外界电磁干扰。

5.4.1.2 操作系统

应按 **GB/T 20272-2006 4.4.1** 的要求，从以下方面来设计、实现或选购**结构化保护级**服务器所需要的操作系统：

a) 身份鉴别：根据 4.3.1 的描述，确保登录操作系统的用户身份的唯一性和真实性；
b) 自主访问控制：根据 4.3.2 的描述，对操作系统的访问进行控制，允许合法操作，拒绝非法操作；
c) 标记：根据 4.3.3 的描述，设计和实现操作系统标记功能，为主、客体设置所需要的敏感标记；
d) 强制访问控制：根据 4.3.4 的描述，对操作系统的访问进行控制，允许合法操作，拒绝非法操作；应对操作系统实现包括系统文件、服务、驱动、注册表及进程在内的强制访问控制功能；
e) 数据流控制：对于以数据流方式实现数据交换的操作系统， 根据 4.3.7 的描述，设计和实现操作系统的数据流控制功能；
f) 安全审计：根据 4.2.2 描述，提供操作系统安全审计功能；
g) 数据完整性：根据 4.3.5 的描述，对操作系统内部存储、处理和传输的用户数据应提供保证用户数据完整性的功能；
h) 数据保密性：根据 4.3.6 的描述，设计和实现操作系统的用户数据保密性保护功能；
i) **可信路径：根据 4.3.8 的描述，在用户进行初始登录和/或鉴别时，应建立一条安全的信息传输通路。**

5.4.1.3 数据库管理系统

应按 **GB/T 20273-2006 5.4.1** 的要求，从以下方面来设计、实现或选购**结构化保护级**服务器所需要的数据库管理系统：

a) 身份鉴别：根据 4.3.1 的描述，确保登录数据库管理系统的用户身份的唯一性和真实性；
b) 自主访问控制：根据 4.3.2 的描述，对数据库管理系统的访问进行控制，允许合法操作，拒绝

非法操作；

c) 标记：根据 4.3.3 的描述，设计和实现数据库管理系统标记功能，为主、客体设置所需要的敏感标记；

d) 强制访问控制：根据 4.3.4 的描述，对数据库管理系统的访问进行控制，允许合法操作，拒绝非法操作；

e) 数据流控制：对于以数据流方式实现数据交换的数据库管理系统，根据 4.3.7 的描述，设计和实现数据库管理系统的数据流控制功能；

f) 安全审计：根据 4.2.2 描述，提供数据库管理系统安全审计功能；

g) 数据完整性：根据 4.3.5 的描述，对数据库管理系统内部存储、处理和传输的用户数据应提供保证用户数据完整性的功能；

h) 数据保密性：根据 4.3.6 的描述，设计和实现数据库管理系统的用户数据保密性保护功能；

i) **可信路径：根据 4.3.8 的描述，在用户进行初始登录和/或鉴别时，应建立一条安全的信息传输通路；**

j) **推理控制：应按 GB/T 20273-2006 5.4.1.10 的要求，设计和实现推理控制功能。**

5.4.1.4 应用系统

5.4.1.4.1 身份鉴别

应根据 4.3.1 的描述，按 **GB/T 20271-2006 6.4.3.1** 的要求，从以下方面设计和实现应用系统的身份鉴别功能：

a) 身份标识：凡需进入应用系统的管理用户，应先进行标识（建立账号）；应用系统管理用户标识一般使用用户名和用户标识符（UID）；并在应用系统的整个生存周期实现用户的唯一性标识，以及用户名或别名、UID 等之间的一致性；

b) 身份鉴别：采用**强化管理的口令和/或基于令牌的动态口令和/或生物特征鉴别和/或数字证书等相结合的方式，采用多鉴别机制，**实现对用户身份的真实性鉴别，并在每次用户登录应用系统时进行鉴别；鉴别信息应是不可见的，应采用加密技术对鉴别信息进行保护。对注册到应用系统的管理用户，应通过用户-主体绑定功能将用户与为其服务的主体相关联。

5.4.1.4.2 自主访问控制

应根据 4.3.2 的描述，按 **GB/T 20271-2006 6.4.3.2** 的要求，从以下方面设计和实现应用系统的自主访问控制功能：

a) 允许命名用户以用户的身份规定并控制对客体的共享，并阻止非授权用户对客体的共享；

b) 用存取控制表访问控制等访问控制表访问控制确定主体对客体的访问权限；

c) 自主访问控制的粒度应是中粒度；

d) 自主访问控制应与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。

5.4.1.4.3 标记

应根据 4.3.3 的描述，按 **GB/T 20271-2006 6.4.3.4** 的要求，从以下方面设计和实现应用系统的标记功能：

a) 应有系统用户的敏感标记，应在用户建立注册账户后由系统安全员为其设置标记；

b) 应用系统客体的敏感标记，应在数据输入到安全控制范围内时以默认方式生成或由安全员通过操作界面进行标记；

c) **将标记扩展到应用系统中的所有主体与客体。**

5.4.1.4.4 强制访问控制

应根据 4.3.4 的描述，按 **GB/T 20271-2006 6.4.3.5** 的要求，从以下方面设计和实现应用系统的强制访问控制功能：

a) **将强制访问控制扩展到数据库管理系统的所有主体与客体，**并且，强制访问控制的客体粒度应是中粒度；

b) 应将系统的常规管理、与安全有关的管理以及审计管理，分别由应用系统管理员、系统安全员和系统审计员来承担，按最小授权原则分别授予它们各自为完成自己承担任务所需的最小权限，并形成相互制约的关系。

5.4.1.4.5 数据流控制

对于以数据流方式实现数据交换应用系统， 应根据 4.3.7 的描述，按 **GB/T 20271-2006 6.4.3.6** 的要求，设计和实现应用系统的数据流控制功能。

5.4.1.4.6 安全审计

应根据 4.2.2 的描述，按 GB/T 20271-2006 6.4.2.4 的要求，从以下方面设计和实现应用系统的安全审计功能：

a) 安全审计功能的设计应与用户标识与鉴别、自主访问控制、标记与强制访问控制等安全功能的设计紧密结合；

b) 提供审计日志、实时报警生成和**违例进程终止**，潜在侵害分析、基于异常检测和**简单攻击探测**，基本审计查阅、有限审计查阅和可选审计查阅，安全审计事件选择，以及受保护的审计踪迹存储、审计数据的可用性确保和**防止审计数据丢失的措施**等功能；

c) 能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问；

d) 能够创建并维护一个对受保护客体访问的审计跟踪，保护审计记录不被未授权的访问、修改和破坏；

e) 对网络环境下运行的应用系统，应建立统一管理和控制的审计机制。

5.4.1.4.7 数据完整性

应根据 4.3.5 的描述，按 **GB/T 20271-2006 6.4.3.7** 的要求,从以下方面设计和实现应用系统的数据完整性功能：

a) 在对服务进行访问操作时，检查字符串形式提交给应用系统中的用户数据是否出现完整性错误；

b) 对应用系统内部进行的数据传输，如进程间的通信，应提供保证数据完整性的功能；

c) 对应用系统中处理的用户数据，应按回退的要求设计相应的数据库管理系统安全功能模块，进行异常情况的事务回退，以确保数据的完整性。

5.4.1.4.8 数据保密性

应根据 4.3.6 的描述，按 **GB/T 20271-2006 6.4.3.8** 的要求，设计和实现应用系统的用户数据保密性保护功能。

5.4.1.4.9 可信路径

应根据 4.3.8 的描述，按 GB/T 20271-2006 6.4.3.9 的要求，在用户进行初始登录和/或鉴别时，应建立一条安全的信息传输通路。

5.4.1.5 运行安全

5.4.1.5.1 安全监控

根据 4.2.1 主机安全监控和网络安全监控的要求，设计和实现服务器安全监控的功能。

5.4.1.5.2 恶意代码防护

根据 4.2.3 中主机软件防护和整体防护的要求，设计和实现恶意代码防护功能。

5.4.1.5.3 备份与故障恢复

根据 4.2.4 中用户自我信息备份与恢复、局部系统备份与恢复、全系统备份与恢复、**紧耦合集群结构，以及异地备份与恢复**的要求，设计和实现服务器备份与故障恢复的功能。

5.4.1.5.4 可信计算支持

根据 4.2.5 中可信计算支持的要求，设计和实现服务器可信计算支持功能。

5.4.1.5.5 可信时间戳

根据 4.2.6 中可信时间戳的要求，设计和实现服务器可信时间戳功能。

5.4.2 安全保证要求

5.4.2.1 SSOS 自身安全保护

a) SSF 物理安全保护：应按 **GB/T 20271-2006 6.4.4.1** 的要求，实现服务器**结构化保护级** SSF 的物理安全保护；

b) SSF 运行安全保护：应按 **GB/T 20271-2006 6.4.4.2** 的要求，实现服务器**结构化保护级** SSF 的运行安全保护；

c) SSF 数据安全保护：应按 **GB/T 20271-2006 6.4.4.3** 的要求，实现服务器**结构化保护级** SSF 的数据按保护；

d) 资源利用：应按 **GB/T 20271-2006 6.4.4.4** 的要求，实现服务器**结构化保护级**的资源利用；

e) SSOS 访问控制：应按 **GB/T 20271-2006 6.4.4.5** 的要求，实现服务器**结构化保护级**的 SSOS 访问控制。

5.4.2.2 SSOS 设计和实现

a) 配置管理：应按 **GB/T 20271-2006 6.4.5.1** 的要求，实现服务器**结构化保护级**的配置管理；

b) 分发和操作：应按 **GB/T 20271-2006 6.4.5.2** 的要求，实现服务器**结构化保护级**的分发和操作；

c) 开发：应按 **GB/T 20271-2006 6.4.5.3** 的要求，实现服务器**结构化保护级**的开发；

d) 指导性文档：应按 **GB/T 20271-2006 6.4.5.4** 的要求，实现服务器**结构化保护级**的指导性文档；

e) 生命周期支持：应按 **GB/T 20271-2006 6.4.5.5** 的要求，实现服务器**结构化保护级**的生命周期支持；

f) 测试：应按 **GB/T 20271-2006 6.4.5.6** 的要求，实现服务器**结构化保护级**的测试；

g) 脆弱性评定： 应按 **GB/T 20271-2006 6.4.5.7** 的要求，实现网络**结构化保护级**的脆弱性评定。

5.4.2.3 SSOS 管理

应按 **GB/T 20271-2006 6.4.6** 的要求，实现服务器**结构化保护级**的 SSOS 安全管理。

5.5 第五级：访问验证保护级

5.5.1 安全功能要求

5.5.1.1 硬件系统

5.5.1.1.1 设备标记

应按 4.1.1 中设备标记和部件标记的要求，设计和实现服务器设备标记的安全功能，设备标记一般采用标签；部件标记应采用数字标签。安全标记应采取保护措施（如加盖公章）。

5.5.1.1.2 设备可靠运行支持

应按 4.1.2 中基本运行支持、安全可用支持和不间断运行支持的要求，设计和实现服务器设备可靠运行支持的安全功能，服务器硬件最低配制应满足软件系统运行的要求；关键部件应与其标记配合，保证其安全性，以防止更换和取走，机箱面板应提供保护措施；不间断运行要求应满足关键部件具有容错、冗余和热插拔等安全功能。支持热插拔功能的部件应包括：硬盘、风扇、电源、PCI 适配器、网卡、内存、CPU 等；电源、硬盘、网卡应采取冗余措施，内存应具有容错功能，关键服务器应采用双机互备技术保证业务连续性要求。

5.4.1.1.3 设备工作状态监控

应按 4.1.3 的要求，设计和实现服务器设备工作状态监控的安全功能，对监测数值超过预先设定的故障阈值时，提供报警和状态恢复功能。

5.1.1.1.3 设备电磁防护

应按 4.1.4 的要求，设计和实现服务器设备电磁防护功能，防止电磁信息泄露，以及屏蔽外界电磁干扰。

5.5.1.2 操作系统

应按 **GB/T 20272-2006 4.5.1** 的要求，从以下方面来设计、实现或选购**访问验证保护级**服务器所需要的操作系统：

a) 身份鉴别：根据 4.3.1 的描述，确保登录操作系统的用户身份的唯一性和真实性；
b) 自主访问控制：根据 4.3.2 的描述，对操作系统的访问进行控制，允许合法操作，拒绝非法操作；
c) 标记：根据 4.3.3 的描述，设计和实现操作系统标记功能，为主、客体设置所需要的敏感标记；
d) 强制访问控制：根据 4.3.4 的描述，对操作系统的访问进行控制，允许合法操作，拒绝非法操作；应对操作系统实现包括系统文件、服务、驱动、注册表及进程在内的强制访问控制功能；
e) 数据流控制：对于以数据流方式实现数据交换的操作系统， 应根据 4.3.7 的描述，设计和实现操作系统的数据流控制功能；
f) 安全审计：根据 4.2.2 描述，提供操作系统安全审计功能；
g) 数据完整性：根据 4.3.5 的描述，对操作系统内部存储、处理和传输的用户数据应提供保证用户数据完整性的功能；
h) 数据保密性：根据 4.3.6 的描述，设计和实现操作系统的用户数据保密性保护功能；
i) 可信路径：根据 4.3.8 的描述，在用户进行初始登录和/或鉴别时，应建立一条安全的信息传输通路。

5.5.1.3 数据库管理系统

应按 **GB/T 20273-2006 5.5.1** 的要求，从以下方面来设计、实现或选购**访问验证保护级**服务器所需要的数据库管理系统：

a) 身份鉴别：根据 4.3.1 的描述，确保登录数据库管理系统的用户身份的唯一性和真实性；
b) 自主访问控制：根据 4.3.2 的描述，对数据库管理系统的访问进行控制，允许合法操作，拒绝非法操作；
c) 标记：根据 4.3.3 的描述，设计和实现数据库管理系统标记功能，为主、客体设置所需要的敏感标记；
d) 强制访问控制：根据 4.3.4 的描述，对数据库管理系统的访问进行控制，允许合法操作，拒绝非法操作；
e) 数据流控制：对于以数据流方式实现数据交换的数据库管理系统，根据 4.3.7 的描述，设计和实现数据库管理系统的数据流控制功能；
f) 安全审计：根据 4.2.2 描述，提供数据库管理系统安全审计功能；
g) 数据完整性：根据 4.3.5 的描述，对数据库管理系统内部存储、处理和传输的用户数据应提供保证用户数据完整性的功能；
h) 数据保密性：根据 4.3.6 的描述，设计和实现数据库管理系统的用户数据保密性保护功能；
i) 可信路径：根据 4.3.8 的描述，在用户进行初始登录和/或鉴别时，应建立一条安全的信息传输通路；

j） 推理控制：应按 **GB/T 20273-2006 5.5.1.10** 的要求，设计和实现推理控制功能。

5.5.1.4 应用系统

5.5.1.4.1 身份鉴别

应根据 4.3.1 的描述，按 **GB/T 20271-2006 6.5.3.1** 的要求，从以下方面设计和实现应用系统的身份鉴别功能：

a） 身份标识：凡需进入应用系统的管理用户，应先进行标识（建立账号）；应用系统管理用户标识一般使用用户名和用户标识符（UID）；并在应用系统的整个生存周期实现用户的唯一性标识，以及用户名或别名、UID 等之间的一致性；

b） 身份鉴别：采用强化管理的口令和/或基于令牌的动态口令和/或生物特征鉴别和/或数字证书等相结合的方式，采用多鉴别机制，实现对用户身份的真实性鉴别，并在每次用户登录应用系统时进行鉴别；鉴别信息应是不可见的，应采用加密技术对鉴别信息进行保护。对注册到应用系统的管理用户，应通过用户-主体绑定功能将用户与为其服务的主体相关联。

5.5.1.4.2 自主访问控制

应根据 4.3.2 的描述，按 **GB/T 20271-2006 6.5.3.2** 的要求，从以下方面设计和实现应用系统的自主访问控制功能：

a） 允许命名用户以用户的身份规定并控制对客体的共享，并阻止非授权用户对客体的共享；

b） 用存取控制表访问控制等访问控制表访问控制确定主体对客体的访问权限；

c） 自主访问控制的粒度应是**细粒度**；

d） 自主访问控制应与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。

5.5.1.4.3 标记

应根据 4.3.3 的描述，按 **GB/T 20271-2006 6.5.3.4** 的要求，从以下方面设计和实现应用系统的标记功能：

a） 应有系统用户的敏感标记，应在用户建立注册账户后由系统安全员为其设置标记；

b） 应用系统客体的敏感标记，应在数据输入到安全控制范围内时以默认方式生成或由安全员通过操作界面进行标记；

c） 将标记扩展到应用系统中的所有主体与客体。

5.5.1.4.4 强制访问控制

应根据 4.3.4 的描述，按 **GB/T 20271-2006 6.5.3.5** 的要求，从以下方面设计和实现应用系统的强制访问控制功能：

a） 将强制访问控制扩展到数据库管理系统的所有主体与客体，并且，强制访问控制的客体粒度应是**细粒度**；

b） 应将系统的常规管理、与安全有关的管理以及审计管理，分别由应用系统管理员、系统安全员和系统审计员来承担，按最小授权原则分别授予它们各自为完成自己承担任务所需的最小权限，并形成相互制约的关系。

5.5.1.4.5 数据流控制

对于以数据流方式实现数据交换应用系统， 应根据 4.3.7 的描述，按 **GB/T 20271-2006 6.5.3.6** 的要求，设计和实现应用系统的数据流控制功能。

5.5.1.4.6 安全审计

应根据 4.2.2 的描述，按 **GB/T 20271-2006 6.5.2.4** 的要求，从以下方面设计和实现应用系统的安全审计功能：

a） 安全审计功能的设计应与用户标识与鉴别、自主访问控制、标记与强制访问控制等安全功能

的设计紧密结合；

b) 提供审计日志、实时报警生成和违例进程终止、**服务取消和用户帐号断开与失效**，潜在侵害分析、基于异常检测和**复杂攻击探测**，基本审计查阅、有限审计查阅和可选审计查阅，安全审计事件选择，以及受保护的审计踪迹存储、审计数据的可用性确保和防止审计数据丢失的措施等功能；

c) 能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问；

d) 能够创建并维护一个对受保护客体访问的审计跟踪，保护审计记录不被未授权的访问、修改和破坏；

e) 对网络环境下运行的应用系统，应建立统一管理和控制的审计机制。

5.5.1.4.7 数据完整性

应根据 4.3.5 的描述，按 **GB/T 20271-2006 6.5.3.7** 的要求,从以下方面设计和实现应用系统的数据完整性功能：

a) 在对服务进行访问操作时，检查字符串形式提交给应用系统中的用户数据是否出现完整性错误；

b) 对应用系统内部进行的数据传输，如进程间的通信，应提供保证数据完整性的功能；

c) 对应用系统中处理的用户数据，应按回退的要求设计相应的数据库管理系统安全功能模块，进行异常情况的事务回退，以确保数据的完整性。

5.5.1.4.8 数据保密性

应根据 4.3.6 的描述，按 **GB/T 20271-2006 6.5.3.8** 的要求，设计和实现应用系统的用户数据保密性保护功能。

5.5.1.4.9 可信路径

应根据 4.3.8 的描述，按 **GB/T 20271-2006 6.5.3.9** 的要求，在用户进行初始登录和/或鉴别时，应建立一条安全的信息传输通路。

5.5.1.5 运行安全

5.5.1.5.1 安全监控

根据 4.2.1 主机安全监控和网络安全监控的要求，设计和实现服务器安全监控的功能。

5.5.1.5.2 恶意代码防护

根据 4.2.3 中主机软件防护和整体防护的要求，设计和实现恶意代码防护功能。

5.5.1.5.3 备份与故障恢复

根据 4.2.4 中用户自我信息备份与恢复、局部系统备份与恢复、全系统备份与恢复、紧耦合集群结构，以及异地备份与恢复的要求，设计和实现服务器备份与故障恢复的功能。

5.5.1.5.4 可信计算支持

根据 4.2.5 中可信计算支持的要求，设计和实现服务器可信计算支持功能。

5.5.1.5.5 可信时间戳

根据 4.2.6 中可信时间戳的要求，设计和实现服务器可信时间戳功能。

5.5.2 安全保证要求

5.5.2.1 SSOS 自身安全保护

a) SSF 物理安全保护：应按 **GB/T 20271-2006 6.5.4.1** 的要求，实现服务器访问验证保护级 SSF 的物理安全保护；

b) SSF 运行安全保护：应按 **GB/T 20271-2006 6.5.4.2** 的要求，实现服务器访问验证保护级 SSF 的运行安全保护；

c) SSF 数据安全保护：应按 **GB/T 20271-2006 6.5.4.3** 的要求，实现服务器访问验证保护级 SSF 的数据按保护；

d) 资源利用：应按 **GB/T 20271-2006 6.5.4.4** 的要求，实现服务器访问验证保护级的资源利用；

e) SSOS 访问控制：应按 **GB/T 20271-2006 6.5.4.5** 的要求，实现服务器访问验证保护级的 SSOS 访问控制。

5.5.2.2 SSOS 设计和实现

a) 配置管理：应按 **GB/T 20271-2006 6.5.5.1** 的要求，实现服务器访问验证保护级的配置管理；

b) 分发和操作：应按 **GB/T 20271-2006 6.5.5.2** 的要求，实现服务器访问验证保护级的分发和操作；

c) 开发：应按 **GB/T 20271-2006 6.5.5.**3 的要求，实现服务器访问验证保护级的开发；

d) 指导性文档：应按 **GB/T 20271-2006 6.5.5.4** 的要求，实现服务器访问验证保护级的指导性文档；

e) 生命周期支持：应按 **GB/T 20271-2006 6.5.5.5** 的要求，实现服务器访问验证保护级的生命周期支持；

f) 测试：应按 **GB/T 20271-2006 6.5.5.6** 的要求，实现服务器访问验证保护级的测试；

g) 脆弱性评定： 应按 **GB/T 20271-2006 6.5.5.7** 的要求，实现网络访问验证保护级的脆弱性评

5.5.2.3 SSOS 管理

应按 **GB/T 20271-2006 6.5.6** 的要求，实现服务器访问验证保护级的 SSOS 安全管理。

附 录 A
（资料性附录）
有关概念说明

A.1 组成与相互关系

一个安全的服务器，无论其安全保护等级达到 GB 17859-1999 所规定的哪一个级，都应从安全功能和安全保证两方面考虑其安全性。安全功能主要说明服务器所实现的安全策略和安全机制符合 GB 17859-1999 中哪一级的要求，安全保证则是通过一定的方法保证服务器所提供的安全功能确实达到了确定的功能要求。本标准描述服务器的每一安全级所应达到的安全功能要求和安全保证要求。

安全功能是指：设备安全、运行安全、数据安全。

安全保证是指： SSOS 自身保护、SSOS 设计和实现、SSOS 安全管理。

五个安全等级则是指 GB 17859-1999 所规定的等级。

A.2 服务器安全的特殊要求

服务器是在信息系统中，通过对信息数据进行处理、存储、检索等操作后向用户提供特定的应用服务和功能服务。应用服务比如像信息浏览服务、邮件服务、数据存储服务等；功能服务比如像缓存服务、负载均衡服务等。它由硬件系统和软件系统两部分组成。硬件系统包括组成服务器的硬件设备及其他配套设备。软件系统包括操作系统、数据库管理系统、应用系统等；操作系统为管理服务器硬软件资源提供支持；数据库管理系统为服务器中的信息数据按指定格式存储和访问提供支持；应用系统是为某种特定应用提供支持。

服务器安全有着广泛的含义，从服务器组成的角度，包括对服务器硬件系统的保护、操作系统的保护、数据库管理系统的保护和应用系统的保护要求。从信息保护的角度，服务器安全可概括为信息的保密性、完整性和可用性（含可控性、可操作性和抗抵赖性）。从信息系统运行的角度可以概括为系统的运行安全和运行中的信息安全。

这里应把握的基本原则是：各组成部分安全保护等级应不低于整体信息系统安全保护等级。服务器的安全性与支持其运行的服务器硬件设备密切相关。因此，支持服务器运行的硬件设备的安全保护等级应与该服务器的安全保护等级相匹配。

A.3 关于主体、客体的进一步说明

在 GB 17859-1999 中，对主体、客体已经进行了定义。为了更确切的了解主体与客体在服务器中的地位与作用，这里对其作进一步说明。

在一个服务器中，每一个实体成分都必须是主体或客体，或者既是主体又是客体。

主体是一个主动的实体，它包括用户、用户组、进程等。系统中最基本的主体应该是用户（包括一般用户和系统管理员、系统安全员、系统审计员等特殊用户）。系统中的所有事件要求，几乎全是由用户激发的。进程是系统中最活跃的实体，用户的所有事件要求都要通过进程的运行来处理。在这里，进程作为用户的客体，同时又是其访问对象的主体。服务器进程一般分为用户进程和系统进程。用户进程通常运行应用程序，实现用户所要求的运算处理；系统进程则是服务器完成对用户所要求的事件进行处理的必不可少的组成部分。

客体是一个被动的实体。在操作系统中，客体可以是按一定格式存储在一定记录介质上的数据信息（通常以文件系统格式存储数据），也可以是服务器中的进程。服务器中的进程（包括用户进程和系统进程）一般有着双重身份。当一个进程运行时，它必定为某一用户服务——直接或间接的处理该用户的事件要求。于是，该进程成为该用户的客体，或为另一进程的客体，而这另一进程则是该用户的客体。依此类推，服务器中运行的任一进程，总是直接或间接为某一用户服务。这种服务关系可以构成一个服务链。服务者是要求者的客体，要求者是服务者的主体，而最原始的主体是用户，最终的客体是一定记录介质上的数据信息。

用户进程是固定为某一用户服务的，它在运行中代表该用户对客体资源进行访问，其权限应与所代表的用户相同（通过用户-主体绑定实现）。系统进程是动态的为所有用户提供服务的，因而它的权限是

随着服务对象的变化而变化的，通过用户-主体绑定将用户的权限与为其服务的进程的权限动态地相关联。当一个系统进程与一个特定的用户相关联时，这个系统进程在运行中就代表该用户对客体资源进行访问。

A.4 关于SSOS、SSF、SSP、SFP及其相互关系

SSOS、SSF、SSP、SFP 是本标准中的重要的概念。在服务器中，SSOS（服务器安全子系统）是构成一个安全的服务器的所有安全保护装置的组合体。一个 SSOS 可以包含多个 SSF（SSOS 安全功能模块），每个 SSF 是一个或多个 SFP（安全功能策略）的实现。SSP（SSOS 安全功能策略）是这些 SFP 的总称，构成一个安全域，以防止不可信主体的干扰和篡改。实现 SSF 有两种方法，一种是设置前端过滤器，另一种是设置访问监控器。两者都是在一定硬件基础上通过软件实现确定的安全策略，并提供所要求的附加服务。在网络环境下，一个 SSOS 可能跨网络实现，构成一个物理上分散、逻辑上统一的分布式 SSOS。

A.5 关于密码技术的说明

密码技术已成为当今服务器安全保护的关键技术。在不同安全保护等级中根据所采用的不同安全策略，应选取不同配置的密码技术作为构成服务器安全保护的重要机制，或将密码技术与服务器安全技术相结合，组成统一的安全机制。SSF 可以利用密码功能来满足一些特定的安全要求。这里主要是指由密码系统提供的以下支持：标识与鉴别、抗抵赖、数据加密保护、数据的完整性保护等。各个安全保护等级的密码技术的具体配置由国家密码主管部门决定。

A.6 关于电磁防护的说明

电磁防护对于服务器设备安全来说是十分重要部分。服务器发出辐射干扰的主要部件包括电源、主板和处理器等，而阻止辐射外泄的主要屏障就是机箱。在不同安全保护等级中应根据不同安全策略，采用不同强度的电磁防护措施作为构成服务器设备安全保护的重要机制。各个安全保护等级的电磁防护的具体要求由国家有关部门决定。

参　考　文　献

[1] GB/T 18336-1：2002 信息技术　安全技术　信息技术安全性评估准则　第1部分：简介和一般模型(idt ISO/IEC 15408-1:1999)

[2] GB/T 18336-2：2002 信息技术　安全技术　信息技术安全性评估准则　第2部分：安全功能要求(idt ISO/IEC 15408-2:1999)

[3] GB/T 18336-3：2002 信息技术　安全技术　信息技术安全性评估准则　第3部分：安全保证要求(idt ISO/IEC 15408-3:1999)

[4] Trusted Computing Group. Trusted Platform Module Main Specification(Version 1.2)：Part 1 Design Principles. May 2004