ICS 35.240.50
J 07

中华人民共和国国家标准

GB/T 39403—2020

云制造服务平台安全防护管理要求

Security protection management requirements of cloud manufacturing service platform

2020-11-19 发布　　2021-06-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国机械工业联合会提出。

本标准由全国自动化系统与集成标准化技术委员会(SAC/TC 159)归口。

本标准起草单位:北京航天智造科技发展有限公司、贵州航天云网科技有限公司、航天云网数据研究院(广东)有限公司、航天云网科技发展有限责任公司、四川中英智慧质量工程技术研究院有限公司、北京电子工程总体研究所、北京机械工业自动化研究所有限公司、北京航空航天大学、北京航天紫光科技有限公司、工业云制造(四川)创新中心有限公司、清华大学、西门子(中国)有限公司。

本标准主要起草人:柴旭东、邹萍、黎晓东、于文涛、侯宝存、王琳、杨灵运、何昊、郜菁、周邯、王玫、王海丹、张霖、李云鹏、金鑫、刘刚、刘波涛、许培炎、俞坚华、刘魁。

云制造服务平台安全防护管理要求

1 范围

本标准规定了云制造服务平台安全防护体系中资源层、IAAS层、PAAS层及SAAS层安全防护管理要求。

本标准适用于云制造服务平台安全防护体系管理。

2 规范性引用文件

下列文件对于本文件的引用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 50174—2017 数据中心设计规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

云制造服务平台 cloud manufacturing service platform

支持产品全生命周期各类活动，支持各类制造资源与制造能力的感知与接入、虚拟化、服务化、搜索、发现、匹配、组合、交易、执行、调度、结算、评估等，支持用户的普适使用，支持分散的制造资源和制造能力集中管理、集中的制造资源和制造能力分散服务的支撑环境以及工具集。

[GB/T 29826—2013，定义 2.1.5]

3.2

网络安全 network security

使网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，保证系统连续、可靠、正常地运行，网络服务不中断的过程。

3.3

平台安全 platform security

保护整个云制造服务平台环境及基础设施、应用程序、数据和信息的策略和实践，防止未经授权的使用/访问、分布式拒绝服务攻击(DDoS)、恶意软件等威胁的过程。

3.4

应用安全 application security

在应用程序中通过查找、修复和预防安全漏洞并开发、添加和测试安全功能，以防止应用程序受到未经授权访问和篡改等威胁，从而使应用程序更加安全的过程。

3.5

数据安全 data security

在数据全生命周期中对数据进行保护，从而防止对数据的未授权访问及数据的损害的过程。

3.6

基础设施即服务 infrastructure as a service；IAAS

提供给消费者的服务是对所有计算基础设施的利用，包括处理CPU、内存、存储、网络和其他基本

的计算资源，用户能够部署和运行任意软件，包括操作系统和应用程序。

3.7

平台即服务　platform as a service；PAAS

提供给消费者的服务是将客户使用供应商提供的开发语言和工具开发的或采购的应用程序部署到供应商的云计算基础设施上去。

注：开发语言和工具有 Java、Python、.Net 等。

3.8

软件即服务　software as a service；SAAS

提供给客户的服务是运营商运行在云计算基础设施上的应用程序，用户可以在各种设备上通过客户端界面访问。

注：消费者不需要管理或控制任何云计算基础设施，包括网络、服务器、操作系统、存储等。

4　缩略语

下列缩略语适用于本文件。

ACL：访问控制列表（Access Control List）

CPU：中央处理器（Central Processing Unit）

DDN：数字数据网（Digital Data Network）

DDoS：分布式拒绝服务（Distributed Denial of Service ）

ECA：事件-条件-动作（Event-Condition-Action）

FTP：文件传输协议（File Transfer Protocol）

IP：网际协议（Internet Protocol）

IPS：入侵防御系统（Intrusion Prevention System）

IDS：入侵检测系统（Intrusion Detection System）

NAT：网络地址转换（Network Address Translation）

SDN：软件定义网络（Software-Defined Networks）

SQL：结构化查询语言（Structured Query Language）

SSL：安全套接字层（Secure Sockets Layer）

TLS：传输层安全（Transport Layer Security）

URL：统一资源定位符（Uniform Resource Locator）

5　总体概述

云制造服务平台安全防护管理体系由资源层安全管理要求与云平台层安全防护管理要求构成，其中云平台层安全管理要求包括 IAAS 层、PAAS 层及 SAAS 层安全防护管理要求。资源层安全管理要求具体包括设备接入控制安全、设备安全、边界防护安全、网络传输安全管理要求，平台 IAAS 层安全防护管理要求包括网络安全、主机安全、虚拟化安全、物理环境安全管理要求，平台 PAAS 层安全防护管理要求包括工业数据接入及管理安全、统一运行环境安全、工业模型及算法安全管理要求，平台 SAAS 层安全防护管理要求具体包括应用漏洞及异常检测、应用逻辑安全、应用安全审计、后台系统安全管理要求。总体架构如图 1 所示。

图 1　云制造服务平台安全防护管理体系架构

6　资源层安全防护要求

6.1　设备接入控制安全要求

设备在接入平台网关时应进行认证，未通过认证的设备应阻止其接入。

6.2　设备安全要求

6.2.1　设备安全检测

应对设备定期进行安全检测，检查其运行状况，并进行漏洞扫描和安全补丁升级。

6.2.2　设备监控告警

应通过传感器或视频监控等方式对设备进行远程监控和告警，实现设备状态监测和预防性维护。

6.3 边界防护安全要求

边界防护安全要求如下：

a） 应对未认证设备接入的行为进行告警；

b） 边界网关应只开放与接入相关的服务端口；

c） 应对数据源地址、目的地址、源端口、目的端口和协议等进行检查；

d） 应对设备发起的攻击行为(DDoS 等)进行检测。

6.4 网络传输安全要求

6.4.1 网络接入安全

规范网络接入安全要求，应使用网络接入控制系统并对其配置合理有效的监控与审计策略，从而对网络的接入行为进行控制管理。

6.4.2 网络数据传输加密要求

规范数据传输加密要求，应为云制造服务平台的维护管理提供数据加密通道。

7 云平台层安全防护要求

7.1 IAAS 层安全防护要求

7.1.1 网络安全

7.1.1.1 安全域

根据平台服务的类型、功能及租户的不同，平台将网络区域划分成不同的子网、网段或安全组，通过技术手段进行隔离。

把相同安全等级、相同安全需求的计算机，放置于同一网段内，在网段的边界处进行访问控制；或者使用虚拟安全域进行管理，即归入一个逻辑组内，对这个组配置访问控制策略。

根据面临的风险，划分安全域，在安全域之间部署防火墙，在每个安全域内部署入侵检测系统(IDS)。

7.1.1.2 黑白名单

平台通过设置黑白名单进行访问控制，根据租户身份或其所属的预先定义的策略组，确定其访问平台资源的请求是否能通过。

平台配置白名单，则只有租户身份或其所属的预先定义的策略组位于白名单内时才可访问。

平台若配置黑名单，则拒绝所有来源于黑名单内租户的网络访问。

7.1.1.3 边界防火墙

平台采用防火墙技术进行网络边界安全控制。

在网络边界上建立相应的网络通信监控系统来隔离内部和外部网络，以阻挡来自外部的网络入侵，可以是软件、硬件或者云防火墙。

进出网络的数据都经过边界防火墙，边界防火墙通过日志对其进行记录，从而方便提供网络使用的详细统计信息。边界防火墙要能够设定报警和通知机制，当发生可疑事件时，提供网络是否受到威胁的信息。

7.1.2 主机安全

7.1.2.1 系统加固

根据安全评估结果，平台制定相应的系统加固方案以消除与降低安全隐患。针对不同目标系统，平台可通过打补丁、修改安全配置、增加安全机制等方法，加强安全性。

尽可能避免安全风险的发生，平台应将周期性的评估和加固工作相结合。

7.1.2.2 安全镜像

镜像服务应保证安全的应用镜像托管能力，精确的镜像安全扫描功能，稳定的内外镜像构建服务，便捷的镜像授权功能，进行镜像全生命周期管理。

平台采用容器化部署，容器是基于镜像构建的。镜像安全直接决定了容器安全。

平台安全镜像构建包括代码编译、文件提取、打包镜像。应将编译和打包分离，以产生安全、精巧、不含源代码的生产级别镜像。

平台应对虚拟机镜像文件进行完整性校验，确保不被篡改。

7.1.2.3 快照

快照在主机备份时广泛采用，通常都是基于卷，在块(block)级别进行处理。

平台应提供多种快照方式。可包括：

a) 即写即拷快照(指针型快照)，占用空间小，对系统性能影响较小，但如果没有备份而原数据盘损坏，数据就无法恢复了；

b) 分割镜像快照(镜像型快照)，即主机当时数据的全镜像，要占用到相等容量的空间，会对系统性能造成一定负荷，但即使原数据损坏也不会有太大影响。

7.1.2.4 主机审计

安全审计应符合以下要求：

a) 审计范围应覆盖到服务器上的每个用户；

b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等重要的安全相关事件；

c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

d) 保护审计记录，避免其在有效期内受到非授权的访问、篡改覆盖或删除等；

e) 应支持按用户需求提供与其相关的审计信息及分析报告；

f) 应能够根据记录数据进行分析，并生成审计报表；

g) 应保护审计进程，避免受到未预期的中断；

h) 应能汇聚服务范围内的审计数据，支持第三方。

7.1.3 虚拟化安全

7.1.3.1 虚拟防火墙

将一台物理防火墙在逻辑上划分成多个虚拟的防火墙，从用户的角度来说每个虚拟防火墙系统都可以被看成是一台完全独立的防火墙设备，拥有独立的系统资源、管理员、安全策略、用户认证数据库等。应做到：

a) 实现防火墙的二层、三层(路由+NAT)转发、ACL 控制、安全检测功能；

b) 每个虚拟防火墙系统之间相互独立，不可直接相互通信；

c) 支持许可(License)控制的虚拟防火墙个数的扩展。

7.1.3.2 虚拟 IPS

虚拟 IPS 应监控虚拟系统网络流量。

平台应在虚拟设备中部署 IDS 和 IPS,提供虚拟机之间、虚拟和物理网络之间的流量监控。

7.1.3.3 虚拟主机隔离

虚拟化平台主机应隔离:

a) 应保证每个虚拟机能获得相对独立的物理资源,并能屏蔽虚拟资源故障,确保某个虚拟机崩溃后不影响虚拟机监控器及其他虚拟机;

b) 应保证不同虚拟机之间的 CPU 指令隔离;

c) 应保证不同虚拟机之间的内存隔离,内存被释放或再分配给其他虚拟机前得到完全释放;

d) 应保证虚拟机只能访问分配给该虚拟机的存储空间(包括内存空间和磁盘空间)。

7.1.4 物理环境安全要求

7.1.4.1 机房位置

机房位置发生自然灾害的概率和频率(洪水、飓风、龙卷风等)较低。机房环境除满足计算机设备对温度、湿度和空气洁净度、供电电源的质量(电压、频率和稳定性等)、接地地线、电磁场和震动等条件的技术要求外,还应满足在机房中工作的人员对照明度、空气的新鲜度和流动速度、噪声的要求。

机房位置选择应符合 GB 50174—2017 中 4.1 的要求。

7.1.4.2 防火

应配置火灾报警装置,在机房内、基本工作房间内、活动地板下、吊顶里、主要空调管道中易燃物附近部位应设置烟、温感探测器。

应配置卤代烷 1211 或 1301 灭火器。

7.1.4.3 接地

机房接地形式为机房专用直流逻辑地,设一组新的接地极,接地电阻小于 1 Ω。

机房配电系统的交流工作地、安全保护地采用建筑物本体综合接地(其电阻小于 4 Ω)。

7.1.4.4 防雷电

建筑物的进户线传导直击雷的概率较低。中心机房内设备主要需要进行直接雷击引起的电阻耦合方式(地电位反击)的防护,以及附近高层建筑落雷时造成的电感性、电容性耦合干扰的防护。具体应满足以下要求:

a) 等电位接地的处理。接地是避雷技术最重要的环节,而且小型机以上的计算机系统对接地要求也很高,其接地电阻通常要求小于 1 Ω 以下。但对于避雷技术来说,地阻小于 4 Ω 即可。应将避雷接地、电器安全接地、交流地、直流接地统一为一个接地装置,避免不同的地之间产生反击。

b) 电源部分防雷设计。根据雷电流大、防雷器存在残压及设备耐冲击水平低的特性,应遵循多级保护,层层泻能的原则,选择安装避雷器,进行电源线路的过压保护。

c) 信号系统的防雷设计。机房的数据通信线路有以太网双绞线、DDN 专线、光纤线路以及电话线备份线路,对进出机房的所有通信线路进行防雷处理,才能保护机房的安全。

7.1.4.5 防潮

满足 GB 50174—2017 中环境要求中温湿度要求。

主机房的环境温度、相对湿度要求：

a) 温度：5 ℃～45 ℃；

b) 相对湿度：8%～80%；

c) 温度变化率：<5 ℃/h(不得结露)。

7.1.4.6 防盗

计算机机房应装设监控系统，实行 24 小时值班制度，出入口应安装防盗安全门，窗户应安装金属防护装置。

可监控物理环境的入口，并在入口设置门禁，门禁能够自动记录日志，管理人员能够查看、审计门禁记录。

7.1.4.7 电力安全

机房应有专用可靠的供电线路，其电源设备应提供可靠的电源，供电电源应满足下列要求：

a) 频率：(50±1)Hz；

b) 电压：380 V/220 V；

c) 变动幅度：−15%～10%；

d) 相数：三相五线制或三相四线制或单相三线制；

e) 波形失真率：≤±10%。

供电电源设备的容量应有一定的余量。

在机房出入口处或值班室，应设置应急电话和应急断电装置。

机房信息系统的各设备走线不得与空调设备、电源设备的无电磁屏蔽的走线平行。交叉时，应尽量以接近于垂直的角度交叉，并采取防延燃措施。

机房信息系统接地应采用专用地线。专用地线的引线应和大楼的钢筋网及各种金属管道绝缘。

机房信息系统应装设容量充足的 UPS。

机房应装设备用电源和自备发电机。

7.2 PAAS 层安全防护要求

7.2.1 工业数据接入及管理安全

7.2.1.1 工业数据加密

应对用户信息、订单信息等重要工业数据实施加密存储。

7.2.1.2 敏感工业数据保护

工业数据输出到平台以外时应进行脱敏处理，严格保护用户敏感信息不泄露。

7.2.1.3 工业数据备份

应提供工业数据本地备份及恢复功能，全部工业数据每周备份一次，新增工业数据应每天备份一次。

7.2.2 统一运行环境安全

7.2.2.1 登录认证

登录认证的要求应包含以下内容：

a) 对存储用户个人信息及用户服务信息的业务，应对用户实施身份认证；

b) 提供登录功能的开发环境应启用登录失败处理功能，比如采取结束会话、限制非法登录次数及自动退出等方法；

c) 提供登录功能的开发环境应启用用户身份唯一性检查功能，确保用户身份标识不重复，并启用用户认证信息复杂度功能检查，防止身份认证信息被轻易冒用；

d) 应对用户账号及口令信息实施加密存储。

7.2.2.2 访问控制

访问控制的要求应包含以下内容：

a) 应配置用户访问控制策略，严格限制默认用户的访问权限；

b) 应限制用户的访问权限，根据业务需要配置用户所需的最小权限，严格按策略要求控制用户访问业务、数据和网络资源等；

c) 用户与开发环境的通信双方中任何一方超出一定时间无响应时，另一方应自动结束会话。

7.2.2.3 服务接入安全

服务接入安全的要求应包含以下内容：

a) 应对外部组件接入接口采取安全管控措施，通过接口代码审计、黑白名单等控制措施保证接口协议操作交互符合接口规范；

b) 应监控服务接入关键接口的调用频率、调用来源等调用情况。

7.2.2.4 应用接入安全

应用接入安全的要求应包含以下内容：

a) 对应用接入的开放接口调用应采取认证措施；

b) 通过开放接口生成的业务应用和应用程序在用户下载之前应进行安全检测；

c) 应制定应用接入开放接口的管理机制及网络安全应急管理制度。

7.2.2.5 容器隔离

应采用内部 SDN 网络实现容器的网络隔离。

7.2.2.6 多租户隔离

多租户隔离应包含以下内容：

a) 系统本身元数据和基础数据的隔离(用户、角色、权限、数据字典、流程模板)；

b) 系统运行过程中产生的动态数据的隔离；

c) 业务系统所涉及的计算资源和存储资源的隔离。

7.2.2.7 日志审计

日志审计的要求如下：

a) 应对每个用户的关键操作进行审计；

b) 审计内容应包含用户的重要行为、资源使用及重要操作命令等安全相关事件；
c) 审计记录应包括事件的日期、时间、类型、描述和结果等，并按相关法律法规要求保留一定期限；
d) 应对审计记录进行安全保护，保证审计记录在有效期内不会受到非授权的访问、篡改、覆盖及删除等操作；
e) 应能按需求提供与用户相关的审计信息和审计分析报告。

7.2.3 工业模型及算法安全

7.2.3.1 模型及算法接入安全

模型及算法接入安全的要求如下：
a) 应对使用模型及算法的用户进行认证，针对不同接入方式的模型及算法用户，应采用不同的认证方式进行认证；
b) 需要检查用户使用模型及算法的合法性及有效性。

7.2.3.2 模型及算法访问控制

模型及算法访问控制的要求如下：
a) 应对授权主体配置访问控制策略，并严格限制默认用户的访问权限；
b) 应严格限制各用户的访问权限，按安全策略要求控制用户对模型及算法的访问；
c) 应周期性检查用户操作模型及算法的情况，统一管理模型及算法使用权限；
d) 如需将收集到的信息共享给第三方应用，应对信息进行脱敏处理，严格保护用户隐私不被泄露。

7.2.3.3 模型及算法流量控制

应配置模型及算法流量控制策略，按照策略要求控制流量，保障模型及算法的高可用性。

7.2.3.4 模型及算法存储安全

模型及算法存储安全的要求如下：
a) 应禁止对模型计算法存储区域内的原始数据进行增加、修改、删除等操作，以保证原始数据的可用性及完整性；
b) 应禁止将模型及算法产生的中间过程数据与原始数据存储于同一空间，以防止数据使用的混乱，加大数据存储的管理难度；
c) 不同模型及算法之间应进行关联性隔离，防止不同模型及算法之间的事件-条件-动作规则(ECA 规则)分析，产生数据泄露。

7.3 SAAS 层安全防护要求

7.3.1 应用漏洞及异常检测

应用漏洞及异常检测的要求如下：
a) 应能检测和避免存在常见的网络漏洞(Web 漏洞)，比如 SQL 注入、跨站脚本、跨站请求伪造等；
b) 应能检测挂马、暗链等网络业务系统(Web 业务系统)入侵事件，并能进行应急处理；
c) 应能检测和避免 Web 业务系统域名、访问链路的异常、访问延迟、解析错误等情况，并能进行应急处理。

7.3.2 应用逻辑安全

7.3.2.1 用户身份认证

身份认证的要求如下：

a) 应对用户进行身份标识和认证，并保证用户身份标识的唯一性；
b) 应提供并启用用户登录口令复杂度检查功能，保证身份信息不易被冒用；
c) 应提供并启用登录失败处理功能，能采取结束会话、限制非法登录次数和自动退出等措施；
d) 应对用户的登录口令信息进行加密存储。

7.3.2.2 访问控制

访问控制的要求如下：

a) 应配置用户访问控制策略，严格限制各用户的访问权限，按安全策略要求控制用户对业务、数据、网络资源等的访问；
b) 应严格设置登录策略，按安全策略要求具备防范账户暴力破解攻击措施的能力（如限定用户连续错误输入密码次数，超过设定阈值，对用户进行锁定，并设定锁定时间，在锁定时间内被锁定的用户需通过注册时的标志信息进行密码重新设定或者凭有效证件进行设定）；
c) 当进行业务权限更改时（如密码重置、密码找回等），应设置相关策略，防止暴力破解攻击；
d) 业务订购、变更、退订流程应根据实际业务需求，应采用“认证码”或“二次短信认证”等方式加强安全性，应限定同一用户每日业务订购次数。

7.3.3 应用安全审计

应用安全审计的要求如下：

a) 应对用户在业务应用中的重要行为、关键操作、资源使用情况等重要安全事件进行审计；
b) 审计记录应包括事件的日期、时间、类型、描述和结果等，并按相关法律法规要求保留一定期限；
c) 应对审计记录进行安全保护，保证审计记录在有效期内受到非授权的访问、篡改、覆盖及删除等操作；
d) 应定期对审计日志进行人工审计；
e) 应能按需求提供与用户相关的审计信息和审计分析报告。

7.3.4 后台系统安全

7.3.4.1 输入验证

输入验证的要求如下：

a) 应对文件路径、URL 地址等输入数据做安全验证，并尽量使用白名单验证方法；
b) 应在服务器端进行输入验证，避免客户端输入验证被绕过；
c) 关键参数应直接从服务器端提取，避免从客户端输入，防止关键参数被篡改。

7.3.4.2 后台系统身份认证

身份认证的要求如下：

a) 应采用 SSL/TLS 加密隧道确保用户密码的传输安全，禁止明文传输用户密码；
b) 应采用单向散列值在数据库中存储用户密码，降低存储的用户密码被字典攻击的风险，禁止在数据库或文件系统中明文存储用户密码；

c) 应禁止在小型文本文件(COOKIE)中保存明文用户密码;
d) 应采取技术措施避免暴力破解、恶意注册、恶意占用资源等行为;
e) 应对关键业务操作进行二次鉴权,例如修改用户认证鉴权信息(如密码、密码取回问题及答案、绑定手机号码等),避免用户身份被冒用;
f) 应避免认证错误提示泄露信息,在认证失败时,应向用户提供通用的错误提示信息(如不应区分是账号错误还是密码错误),避免这些错误提示信息被攻击者利用;
g) 应支持密码策略设置,从业务系统层面支持强制的密码策略,包括密码长度、复杂度、更换周期等,特别是业务系统的管理员密码;
h) 应支持账号锁定功能,系统应限制连续登录失败次数,在客户端多次尝试失败后,服务器端需要对用户账号进行短时锁定,且锁定策略支持配置解锁时长;
i) 应确保用户不能访问到未授权的功能和数据,未经授权的用户试图访问受限资源时,系统应予以拒绝或提示用户进行身份鉴权。

7.3.4.3 会话管理

会话管理的要求如下:

a) 应确保会话的安全创建。在用户认证成功后,应为用户创建新的会话并释放原有会话;创建的会话标识应满足随机性和长度要求,避免被攻击者猜测;会话与 IP 地址可绑定,降低会话被盗用的风险。
b) 应确保会话数据的存储安全。用户登录成功后所生成的会话数据应存储在服务器端,并确保会话数据不能被非法访问;当更新会话数据时,要对数据进行严格的输入验证,避免会话数据被非法篡改。
c) 应确保会话数据的传输安全,防止泄露会话标识。
d) 应确保会话的安全终止。当用户登录成功并成功创建会话后,应在网络应用系统(Web 应用系统)的各个页面提供用户登出功能,登出时应及时删除服务器端的会话数据;当处于登录状态的用户直接关闭浏览器时,需要提示用户执行安全登出或者自动为用户完成登出过程,从而安全地终止本次会话。
e) 应设置合理的会话超时阈值,在合理范围内尽可能减小会话超时阈值,可以降低会话被劫持和重复攻击的风险,超过会话超时阈值后立刻销毁会话,清除会话的信息。
f) 应限制会话并发连接数,限制同一用户的会话并发连接数,避免恶意用户创建多个并发的会话来消耗系统资源,影响业务的可用性。
g) 在涉及关键业务操作的网络页面(Web 页面),应为当前 Web 页面生成一次性随机令牌,作为主会话标识的补充。在执行关键业务前,应确保用户提交的一次性随机令牌与服务器端保存的一次性随机令牌匹配,以避免跨站请求伪造等攻击。

7.3.4.4 数据存储

数据存储的要求如下:

a) 对于不同类别的数据,比如日志记录和业务数据,应采取相应的隔离措施和安全保护措施;
b) 禁止在客户端本地存储用户敏感数据,如用户密码、身份信息等;
c) 应避免在代码中硬编码密码(即在代码中直接嵌入密码,会导致密码修改困难,甚至密码的泄露),可从配置文件载入密码;
d) 在配置文件中禁止明文存储数据库连接密码、FTP 服务密码、主机密码、外部系统接口认证密码等。

7.3.4.5 数据传输

应确保通信信道的安全，在客户端与网络服务器（Web 服务器）之间使用并正确配置 SSL/TLS，应使用 SSL3.0/TLS1.0 以上版本，对称加密密钥长度不少于 128 位，非对称加密密钥长度不少于 1 024 位，单向散列值位数不小于 128 位。