ICS 35.030
CCS L80

团 体 标 准

T/COSOCC 010—2024

信息安全技术 面向服务架构类应用安全要求

Information security technology — Security requirements for service-oriented architecture application

2024－04－10 发布　　2024－04－10 实施

中国基本建设优化研究会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由中国基本建设优化研究会提出并归口。

本文件起草单位：北京启明星辰信息安全技术有限公司、蓝象标准（北京）科技有限公司、广电计量检测集团股份有限公司、北京国泰网信科技有限公司、北京网藤科技有限公司、北京边界无限科技有限公司、福建金瑞信息技术有限公司、北京通州网络安全产业园运营管理有限公司、广东盈世计算机科技有限公司、北京轩宇信息技术有限公司、中科可控信息产业有限公司、嵩嘉标准化技术服务（北京）有限公司。

本文件主要起草人：李雪晴、乔华阳、于莉莉、李欣、原树生、韩群、邓明聪、边梦娜、王梓晴、郑竹萌、毛峰、赵敬宇、王向章、张德保、王新亮、姜冰、张红艳、邱天、段小莉。

信息安全技术　面向服务架构类应用安全要求

1　范围

本文件规定了面向服务架构方法的应用安全要求和安全应用管理要求。

本文件适用于指导用户对面向服务架构的应用系统进行安全管理和安全运行保障。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。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/T 25069　信息安全技术　术语

3　术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

应用　application

可运行于服务端的测试或线上环境，以及客户端的软件和数据的集合，包括应用软件包、应用数据及运行环境配置。

3.2

应用安全　application security

消减现有应用的编码、配置、架构、数据、内容风险，并持续保障其安全性处于高安全水平的方法论，实施过程、技术手段、管理措施的集合。

3.3

安全策略　security policy

为保护某一系统及其信息的机密性、完整性、可用性，而对信息系统所选择并施加的管理、操作和技术等方面的控制。

3.4

基线　baseline

经过正式评审并通过的规约，作为后续管理操作的基础。只有通过正式的变更规程方可对其进行变更。

3.5

环境感知　environment awareness

采集终端物理硬件、网络、操作系统、应用程序的安全要素，分析终端可信状态的过程。

3.6

授权策略　authorization policy

对主体访问客体进行权限分配，分配后的访问权限即为授权策略。授权策略为规则和关系的表达，在给定主体、目的（任务）、客体和环境属性的情况下，根据授权策略确定访问请求是否被允许。

3.7

审计　audit

记录和审查主体操作客体活动的过程，记录的内容包括操作时间、动作、主体、客体。审计的目的主要在于及时发现、反馈、终止违规访问应用、数据的行为，威慑和警示潜在攻击者或非法操作者。

3.8

任务　task

任务是一项原子服务，可以属于某一项工作，也可以单独存在，通常是为了完成某一个工作的服务。

3.9

面向服务架构 service-oriented architecture

面向服务架构是软件设计和软件架构的一种模式，它将应用程序的不同功能单元通过定义良好的接口和协议进行组合。这些应用程序单元被称为服务，这些服务是独立的、可重复的。

4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

CPU： 中央处理器（Central Processing Unit）

DDoS：分布式拒绝服务攻击（Distribution Denial of Service）

SSL：安全套接层协议（Secure Sockets Layer）

URL：统一资源定位符（Uniform Resource Locator）

VPN：虚拟专用网络（Virtual Private Network）

Web：全球广域网或万维网（World Wide Web）

5 概述

本文件针对面向服务架构方法设计的应用系统，给出了在其运行过程中应具备的安全技术要求包括技术要求和安全应用管理要求，其中应用安全要求包括：应用运营安全防护、动态访问控制以及密码服务；安全应用管理要求包括安全防护能力配置、应用访问控制和运行维护。

本文件凡涉及采用密码技术解决保密性、完整性、真实性、不可否认性的需求遵循密码相关国家标准和行业标准。

6 应用安全要求

6.1 应用运营安全防护

6.1.1 应用安全识别

6.1.1.1 资产发现

资产发现应符合下列要求：

a) 支持对无法准确识别的设备类型由管理人员自定义设定设备特征；

b) 支持自动搜集终端上报的外设信息，包括但不限于以通用串行总线（USB）、串口、并口、红外、蓝牙、无线、高清多媒体接口（HDMI）等方式接入的外设，并根据内置识别库对设备自动识别和分类；

c) 支持终端客户端自动识别硬件信息，包括：CPU、主板、内存、硬盘、网卡、显示器等；

d) 支持终端客户端自动识别操作系统信息，包括：类型、版本号、账号、安装时间等；

e) 支持终端客户端自动识别应用软件信息，包括：名称、类型、版本号、厂商、安装时间等；

f) 支持终端用户自助进行资产登记，包括：单位、设备类型、设备用途、使用人、联系方式、邮箱、物理位置、资产编号等信息；

g) 支持被动监听网络流量，并识别存活设备类型及其属性信息；

h) 支持发现设备的动态资产信息，包括不限于服务端口信息、进程信息；

i) 支持对设备的 CPU、内存条、显卡、驱动、硬盘、主板、网卡等进行监控，变动后告警；

j) 支持对应用所属业务系统识别；

k) 支持对应用内部所使用组件库、接口、识别。

6.1.1.2 漏洞扫描

漏洞扫描应符合下列要求：

a) 支持对操作系统等对象的安全扫描；

b) 支持及时更新漏洞的补丁信息和修补建议，支持对扫描出的漏洞信息进行标注并出漏洞风险

级；

c） 支持扫描和识别终端操作系统开放的端口以及服务存在的安全漏洞，并提供安全修复建议；
d） 支持扫描和识别终端办公软件中可能存在的安全漏洞，并提供安全修复建议；
e） 支持设置定时任务进行自动化扫描；
f） 支持生成扫描报告和报告导出功能，支持将扫描结果以报表的形式导出；
g） 支持设置详细的扫描参数，包括端口、弱口令、服务等相关设置项；
h） 支持一键修复漏洞功能，并给出修复漏洞的风险提示；
i） 支持系统预设多种扫描策略，可由用户根据需要自定义扫描策略，如实现对操作系统、主流数据库、主流应用服务的自定义扫描。

6.1.1.3 基线核查

基线核查应符合下列要求：

a） 身份鉴别：核查内容包括账户登录和口令管理，如是否启动身份验证机制，限制连续登录失败次数、连续多次登录失败后锁定账户、配置口令复杂度等；
b） 访问控制：核查内容包括账户管理和权限分配，如是否分配登录用户的账户和权限、重命名或者删除默认管理员账户，删除多余账户，删除共享账户等；
c） 安全审计：核查内容包括账户行为审计和资源访问审计，如是否配置了用户的安全审计、用户行为审计、安全审计等并对安全审计记录进行保护；
d） 剩余信息保护：核查内容包括临时文件、历史文件和虚拟文件管理，如清除虚拟内存页面文件、清除临时文件等；
e） 入侵防范：核查内容包括对组件的保护功能开启、应用程序的更新升级，如限制应用程序的下载和安装、保持操作系统补丁的及时更新、关闭高危端口、禁用不需要的服务、网络访问限制等；
f） 恶意代码防范：核查内容包括防恶意代码软件的安装、升级和病毒查杀管理，如是否开启防恶意代码软件的实时保护功能、保障防恶意代码软件版本最新、病毒库最新；
g） 资源控制：核查内容包括服务、端口、协议等资源管理和数据的加密保护，如是否禁用共享、文本传输协议（FTP）和 Telnet（远程登陆系统）等网络连接、禁止介质自动运行等；
h） 办公软件安全：核查内容包括 office 软件、WPS 软件的安全配置，如是否禁止 ActiveX 控件（对一系列策略性面向对象程序技术和工具的称呼）的使用、禁止所有未经验证的加载项、限用未数字签名的宏等；
i） 浏览器安全：核查内容包括对浏览器的安全设置检测，如是否禁止运行 java（一门面向对象的编程语言）小程序脚本、限制下载和安装未签名的 ActiveX 控件。

6.1.2 应用安全防护

6.1.2.1 访问控制

访问控制应符合下列要求：

a） 应用访问控制：对用户可访问的应用系统进行授权，并在用户访问应用服务时，对用户进行认证、鉴权，实现应用粒度的访问控制；
b） 在应用服务访问数据服务的过程中，验证应用服务身份，鉴别访问请求权限，实现对数据粒度的访问控制；
c） 运维访问控制：在运维访问过程中，对运维人员的运维账号进行访问控制，防止越权操作所采取的访问控制措施。

6.1.2.2 通信加密

用户访问应用服务时，对应用访问、应用接口、控制信息传输等，应通过国密SSL安全协议进行加密，保障信息保密性。

6.1.2.3 内容防护

内容防护应符合下列要求：

a） 应用脱敏展示：支持通过安全基础设施的数据脱敏服务，对页面展示的人员敏感数据进行动态脱敏处理；
b） 应用数字水印：支持通过明水印或暗水印的方式，对擅自将应用界面显示的敏感信息进行截图等行为进行响应，包括溯源及阻断等技术措施；对于含有敏感内容的界面，应在终端屏幕自动生成水印，水印包括登录账户、登录 IP 等信息；
c） 网页防篡改：支持对网页内容的完整性进行保护，防止非授权修改；
d） 应用数据反爬：在访问终端与被保护业务系统 Web 服务器之间，应防止自动化工具攻击和数据爬虫，支持对 Web 业务进行安全防护，保护后台应用信息安全。

6.1.2.4 攻击防护

攻击防护应符合下列要求：
a） Web 攻击防护：应能够识别、防御针对 Web 应用的攻击，防范恶意用户针对 Web 应用发起的各种攻击；
b） API 攻击防护：应能够检测、识别、拦截针对 API 接口的攻击，如 API 重放、API 参数篡改等；
c） 应用层 DDoS 攻击防护：应能够利用流量清洗技术，阻断恶意发送大量合理请求、消耗目标系统服务资源的 DDoS 攻击行为，保护应用服务安全。

6.1.2.5 应用脆弱性防护

应用脆弱性防护应符合下列要求：
a） 应用代码安全审计：通过安全防护体系提供的源代码审计服务，利用数据流分析、符号执行、内存精确建模等技术，对应用源程序的语法、结构、过程、接口等进行安全审计，确定源代码的安全性；
b） 应用漏洞扫描：通过安全设备提供的漏洞扫描服务，在应用上线前和运行过程中，对应用程序的安全漏洞、编码隐患进行安全扫描检测，发现潜在的安全问题和架构缺陷；
c） 应用漏洞修复：通过安全设备提供的补丁管理服务，对已经发现的应用漏洞，通过修补程序或软件版本升级进行补丁修复。支持自动化补丁批量部署，在批量部署补丁之前应对补丁进行测试与审批，并支持定期更新补丁部署状态；
d） 应用安全基线核查：通过安全设备提供的基线核查服务，根据安全基线准则，对应用系统进行基线核查，检查应用系统的安全配置并提供整改建议，支持自动化或手动基线核查。

6.1.3 应用安全检测

6.1.3.1 基本信息检测

基本信息检测应符合下列要求：
a） 应用加固壳识别：具备应用加固壳的识别能力，防止对反编译工具的破解，降低被脱壳拿到真实代码的风险；
b） 应用签名信息检测：具备应用签名信息检测能力，能有效识别签名的真实性；
c） 应用权限信息检测：具备应用相关静态权限申请及信息检测能力；
d） 服务端应用信息检测： 具备服务端应用开发语言识别能力，组件构成。

6.1.3.2 恶意行为检测

应具有敏感词汇、敏感函数检测能力，支持敏感词、敏感函数自定义，如客户端应用程序中调用了包含敏感行为的函数服务端应用中调用了哪些敏感行为函数，包括执行命令、写入文件，以及发送短信、发送地理位置、拨打电话等。

6.1.3.3 源代码安全检测

源代码安全检测应符合下列要求：
a） 具备对 java 代码加壳、混淆、反编译检测能力；
b） 具备对动态链接库文件的加载、加固检测能力；
c） 具备日志数据泄漏检测能力；

d) 具备测试信息残留检测能力；
e) 具备 URL 硬编码检测能力；
f) 具备对硬编码中敏感数据的检测能力；
g) 具备对应用中内网测试的 URL 信息残留的检测能力；
h) 具备对启动隐藏服务检测能力；
i) 具备全局异常检测能力，检测应用是否启动全局异常捕获机制，当出现未知异常时，支持捕获异常信息并记录下来，上传到服务器，分析出现异常具体原因。

6.1.3.4 组件安全检测

组件安全检测应符合下列要求：
a) 最小化权限检测：具备对 Activity 最小化权限检测能力，检测组件导出权限是否为最小化，降低用户敏感信息泄露、被恶意代码注入等攻击的风险；
b) 漏洞检测：具备 Fragment（碎片）注入漏洞检测、WebView 系统隐藏接口未移除漏洞、WebView（网页视窗）组件克隆应用漏洞、WebView 组件远程代码执行漏洞、WebView 密码明文存储风险、WebView File（网页视窗文件）域同源策略绕过漏洞、WebView 组件忽略 SSL 证书验证错误漏洞、Intent URL Schema 攻击漏洞等多种漏洞检测能力；
c) 启用 VPN 服务检测：具备对启用 VPN 服务等检测能力，降低通过网络请求的数据被劫持，造成用户敏感信息泄露的风险；
d) 开源组件检测：具备对应用使用的开源组件进行检测和漏洞分析的能力，展示当前符合安全标准的开源组件版本，降低开源组件带来的安全风险。

6.1.3.5 网络环境检测

网络环境检测应符合下列要求：
a) 网络环境检测：支持实时检测终端所处的网络环境，支持地址检测、域名检测等多种检测方式、支持防误判检测等；
b) 违规后处理：具备网络环境违规后报警功能，具备违规后断开网络、违规后锁屏、关机等功能。

6.1.3.6 威胁检测

威胁检测应符合下列要求：
a) 具备基于签名或特征的威胁检测能力，发现各类已知威胁；
b) 具备基于威胁情报的威胁检测能力，对恶意域名、恶意 IP、恶意 URL 等进行检测和预警；
c) 支持提供终端行为，样本投递、内存活动、系统变更等数据，供大数据分析，发现终端可疑或异常行为；
d) 支持对网络流量进行检测、分析，发现流量异常、协议异常、攻击行为等网络威胁；
e) 支持检测流量中的恶意扫描、协议攻击、恶意代码、恶意文件和隐蔽通道等网络威胁；
f) 支持静态检测、动态检测等方式，识别未知恶意代码和未知高级攻击行为；
g) 具备对终端可疑进程的检测能力，包括检测隐藏进程，进程非法监听套接字，修改系统敏感文件等；
h) 具备对应用内存马注入攻击进行检测与阻断的能力；
i) 具备威胁响应能力，包括隔离、IP 封堵和断开网络连接等；
j) 支持对终端进程、终端行为（脚本执行，命令执行，文件操作，注册表操作，网络请求行为）、系统事件等进行持续检测，发现异常进程、异常行为、横向移动等威胁。

6.1.4 应用安全响应

6.1.4.1 事件抑制

事件抑制应符合下列要求：
a) 具备网络攻击抑制能力，支持网络流量过滤、阻断、限流、牵引等方式；
b) 具备主机入侵抑制能力，支持主机隔离、进程或服务终止等方式。

6.1.4.2 攻击诱捕

攻击诱捕应符合下列要求：

a） 具备网络攻击诱捕能力，支持业务仿真、攻击行为记录、样本提取、网络流量捕获等；
b） 具备攻击诱导能力，支持网络访问重定向、广播路由等方式将攻击诱导至诱捕环境；
c） 具备行为记录能力，支持记录攻击行为、攻击流量等。

6.1.4.3 响应恢复

响应恢复应符合下列要求：

a） 具备执行备份能力，支持记录备份安全策略、安全配置、基线变更及响应动作；
b） 具备执行回退能力，支持安全策略、安全配置、基线变更、回滚和回退等响应动作。

6.1.4.4 调查取证

调查取证应符合下列要求：

a） 具备取证数据转储能力，支持磁盘快照、内存空间转储等；
b） 具备取证数据提取能力，支持内存数据提取、恶意代码定位、可疑样本提取等；
c） 具备取证数据保全能力，支持基于取证结果的数字签名、统一存储、在线访问等；
d） 支持终端数据的保护和备份，支持记录安全策略、安全配置、基线变更及其他响应动作，支持恢复指定数据和配置。

6.1.5 溯源与反制

6.1.5.1 攻击反制

提供攻击反制能力支持代码注入、远程控制等。

6.1.5.2 攻击溯源

攻击溯源应符合下列要求：

a） 具备网络攻击溯源能力，包括攻击主体、攻击路径、攻击方法、攻击对象等的溯源；
b） 具备恶意代码攻击溯源能力，包括感染源、感染对象、感染途径等；
c） 具备数据泄露溯源能力，包括泄露源、泄露途径、泄露时间、泄露内容等。

6.1.5.3 响应分析

具备自动化综合分析能力通过综合分析，专业安全人员可准确定位攻击者真实身份。

6.2 动态访问控制

6.2.1 应用认证

应用认证应符合下列要求：

a） 支持根据配置确定应用的认证方式；
b） 支持根据认证方式调用对应的认证因子进行认证；
c） 支持根据各认证因子反馈的认证结果进行综合判定，根据结果签发令牌；
d） 支持持续认证；
e） 支持认证过程中的风险检测输出及处理。

6.2.2 应用权限

应用权限包括授权和鉴权应分别符合下列要求。

a） 授权
   1） 支持为用户、机构、应用等授权主体进行授权；
   2） 支持应用级、功能级、数据级和服务级授权服务。
b） 鉴权
   1） 支持应用级、功能级、数据级和服务级鉴权服务；
   2） 支持通过鉴权请求获取鉴权条件，依据鉴权条件动态返回鉴权结果；
   3） 支持为用户、机构、应用等授权主体进行鉴权；

4) 用户通过认证服务登录后，支持认证服务携带用户令牌进行应用级鉴权，支持根据用户令牌将用户所具有权限的应用系统列表返回认证。

6.2.3 应用审计

应用审计应符合下列要求：

a) 支持对用户访问敏感数据、执行关键操作行为等各类业务日志进行真实、全面的记录；
b) 具备对各类业务行为进行审计，并提供异常行为分析、发现、告警和响应的能力。

6.2.4 终端环境感知

终端环境感知应符合下列要求：

a) 具备终端信息采集、环境安全检查、关键配置检查、基线打分、补丁检查、漏洞检查、白名单防护、处置响应、威胁溯源等能力；
b) 支持环境风险分析，并向业务安全策略控制服务上报风险结果。

6.3 密码服务

密码服务技术应符合下列要求：

a) 算法支持国密标准的 SM1～SM4 等；
b) 支持安全密钥更新周期的设置。

7 安全应用管理

7.1 安全防护能力配置

应支持对安全识别、安全防护、安全检测、安全响应等服务的各种配置统一管理，包括但不限于相应服务的基本配置、管理界面、使用界面。

7.2 应用访问控制

7.2.1 认证管理

7.2.1.1 令牌管理

令牌管理应符合下列要求：

a) 令牌包括用户令牌和应用令牌
   1) 用户令牌中至少包含组织机构标识、用户标识、创建时间和过期时间，不应包含组织机构和用户的具体信息；
   2) 应用令牌至少包含应用标识、用户标识、创建时间和过期时间；
b) 支持国密算法，保证令牌信息的机密性；
c) 支持令牌防篡改，保证令牌全生命周期的完整性；
d) 具备令牌在各使用节点的验证机制；
e) 支持令牌全生命周期的管理；
f) 支持根据接收到的风险指令或自有策略判断结果，调整相应令牌状态；
g) 支持将令牌及其状态通知给需要核验令牌的相关方。

7.2.1.2 身份管理

身份管理包括用户身份管理和组织机构身份管理应分别符合下列要求。

a) 用户身份管理
   1) 用户信息包括但不限于用户唯一标识、姓名、性别、身份证号、工号、机构代码、所属单位、手机号、职务；
   2) 支持对用户信息的管理，包括但不限于增、删、改、查；
   3) 支持不同节点间用户信息的同步；
   4) 支持建立用户和组织机构关联关系；
   5) 支持登记和管理用户认证因子信息。

b） 组织机构身份管理
1） 组织机构信息包括但不限于组织机构唯一标识、组织机构名称、组织机构代码、上级组织机构名称、上级组织机构代码、单位性质、部门；
2） 支持对组织机构信息的管理，包括但不限于增、删、改、查。

7.2.1.3 认证配置管理

认证配置管理应符合下列要求：
a） 应用信息包括但不限于应用唯一标识、应用名称、应用简称；
b） 支持从资源目录获取应用列表和应用识别码；
c） 支持应用关联的认证方式配置；
d） 支持根据应用关联的认证方式进行补充认证。

7.2.1.4 认证因子管理

认证因子管理应符合下列要求：
a） 认证因子包含但不限于口令、数字证书、生物特征等；
b） 认证因子信息包括但不限于认证因子名称、安全等级、启用状态、认证因子管理平台地址；
c） 支持认证因子信息的管理，包括但不限于增、删、改、查；
d） 支持认证因子的标准化接入和管理；
e） 支持组合不同的认证因子满足不同的安全级别需求。

7.2.2 权限管理

7.2.2.1 授权主体管理

授权主体管理，应符合下列要求：
a） 支持通过其他平台接收授权主体；
b） 支持自定义录入或通过其他平台接收主体环境要素；
c） 支持对主体相关环境因素进行新增、修改、删除等操作，主体相关环境要素包括但不限于场景、业务任务；
d） 支持新增、修改、删除授权主体授权类相关属性，并为相关属性赋值；
e） 支持依据各类条件查询、统计授权主体；
f） 授权主体包括但不限于：用户、组织机构、应用等。

7.2.2.2 授权客体管理

授权客体管理应符合下列要求：
a） 授权客体包括但不限于应用及其包含的资源；
b） 支持自定义录入或通过其他平台接收授权客体；
c） 支持对授权客体进行新增、修改、删除等操作；
d） 支持新增、修改、删除授权客体授权类相关属性，并为相关属性赋值；
e） 支持依据各类条件查询、统计授权客体；
f） 支持数据资源的分级分类管理。

7.2.2.3 角色管理

角色管理应符合下列要求：
a） 支持创建、删除、编辑角色，定义角色的生命周期；
b） 支持关联工作流角色生命周期的管理；
c） 支持授权主体与授权客体通过关联角色实现授权。

7.2.2.4 权限自助管理

用户可对授权客体访问权限进行申请、撤销和变更等自助管理操作，在流程流转的过程中申请人可实时查看流程审批进度。

7.2.3 终端环境感知管理

终端环境感知管理应符合下列要求：

a) 环境感知内容管理：支持自定义环境感知服务的终端环境感知项；
b) 感知策略管理：支持对环境感知内容进行管理和配置；
c) 环境感知报告管理：支持根据终端的环境感知数据，对终端环境风险进行评估，得出终端安全环境感知报告。

7.2.4 审计管理

审计管理应包含下列内容:

a) 日志标准化：支持配置管理标准化策略，保证审计信息的完整性、统一性，对采集到的不完整日志及时发出预警；
b) 日志留存时间管理：应用访问日志的保存时间不少于六个月；
c) 审计策略配置
   1) 支持审计策略配置，审计策略用于规定审计的方式，包括设定数据采集的范围、采集时间、采集方式、采集字段等；
   2) 审计策略配置功能包括策略创建、策略修改、策略删除、策略启停、策略查询等功能；
   3) 支持策略配置规则的前台展示功能。

7.3 运行维护

安全应用运行维护管理符合下列要求:

a) 应提供统一的标准化服务接口规范各子系统、组件程序的集中配置管理；
b) 应支持安全资源的注册、编排、封装等，对已有安全资源实现服务化；
c) 应支持对安全资源进行初始化配置及恢复初始化配置；
d) 宜对安全资源的接口、运行状态等系统状态进行持续监测并定期上报系统；
e) 应支持软件安全资源的生命周期管理，包括创建、变更、删除、备份、恢复等。

参 考 文 献

[1] GB/T 18794.3 信息技术 开放系统互连 开放系统安全框架 第3部分:访问控制框架
[2] GB/T 20271 信息安全技术 信息系统通用安全技术要求;
[3] GB/T 22239 信息安全技术 网络安全等级保护基本要求;
[4] GB/T 34080.4 基于云计算的电子政务公共平台安全规范 第4部分:应用安全;
[5] GM/T 0054 信息系统密码应用基本要求。