



中华人民共和国国家标准

GB/T 31168—2023

代替 GB/T 31168—2014

信息安全技术 云计算服务安全能力要求

Information security technology—
Security capability requirements for cloud computing services

2023-05-23 发布

2023-12-01 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	V
引言	VI
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 云计算安全要求的表达与实现	3
5.1 云计算安全措施的实施责任	3
5.2 云计算安全措施的作用范围	4
5.3 安全要求的分类	4
5.4 安全要求的表述形式	5
5.5 安全要求的调整	6
5.6 安全计划	7
6 系统开发与供应链安全	7
6.1 资源分配	7
6.2 系统生命周期	8
6.3 采购过程	8
6.4 系统文档	9
6.5 关键性分析	9
6.6 外部服务	10
6.7 开发商安全体系架构	10
6.8 开发过程、标准和工具	11
6.9 开发过程配置管理	11
6.10 开发商安全测试和评估	12
6.11 开发商提供的培训	13
6.12 组件真实性	14
6.13 不被支持的系统组件	14
6.14 供应链保护	14
7 系统与通信保护	16
7.1 边界保护	16
7.2 传输的保密性和完整性保护	17
7.3 网络中断	17
7.4 可信路径	17

7.5	密码使用和管理	18
7.6	设备接入保护	18
7.7	移动代码	18
7.8	会话认证	19
7.9	恶意代码防护	19
7.10	内存防护	20
7.11	系统虚拟化安全性	20
7.12	网络虚拟化安全性	21
7.13	存储虚拟化安全性	21
7.14	安全管理功能的通信保护	22
8	访问控制	22
8.1	用户标识与鉴别	22
8.2	标识符管理	22
8.3	鉴别凭证管理	23
8.4	鉴别凭证反馈	24
8.5	密码模块鉴别	24
8.6	账号管理	24
8.7	访问控制的实施	25
8.8	信息流控制	26
8.9	最小特权	26
8.10	未成功的登录尝试	27
8.11	系统使用通知	27
8.12	前次访问通知	27
8.13	并发会话控制	28
8.14	会话锁定	28
8.15	未进行标识和鉴别情况下可采取的行动	28
8.16	安全属性	29
8.17	远程访问	29
8.18	无线访问	30
8.19	外部信息系统的使用	30
8.20	可供公众访问的内容	30
8.21	WEB 访问安全	31
8.22	API 访问安全	31
9	数据保护	32
9.1	通用数据安全	32
9.2	媒体访问和使用	32
9.3	剩余信息保护	33

9.4	数据使用保护	33
9.5	数据共享保护	34
9.6	数据迁移保护	34
10	配置管理	35
10.1	配置管理计划	35
10.2	基线配置	35
10.3	变更控制	35
10.4	配置参数的设置	36
10.5	最小功能原则	37
10.6	信息系统组件清单	38
11	维护管理	38
11.1	受控维护	38
11.2	维护工具	39
11.3	远程维护	39
11.4	维护人员	40
11.5	及时维护	40
11.6	缺陷修复	40
11.7	安全功能验证	41
11.8	软件和固件完整性	41
12	应急响应	42
12.1	事件处理计划	42
12.2	事件处理	42
12.3	事件报告	43
12.4	事件处理支持	43
12.5	安全警报	43
12.6	错误处理	44
12.7	应急响应计划	44
12.8	应急响应培训	45
12.9	应急演练	45
12.10	信息系统备份	46
12.11	支撑客户的业务连续性计划	46
12.12	电信服务	47
13	审计	47
13.1	可审计事件	47
13.2	审计记录内容	48
13.3	审计记录存储容量	48
13.4	审计过程失败时的响应	48

13.5	审计的审查、分析和报告	48
13.6	审计处理和报告生成	49
13.7	时间戳	50
13.8	审计信息保护	50
13.9	抗抵赖性	50
13.10	审计记录留存	51
14	风险评估与持续监控	51
14.1	风险评估	51
14.2	脆弱性扫描	51
14.3	持续监控	52
14.4	信息系统监测	53
14.5	垃圾信息监测	54
15	安全组织与人员	54
15.1	安全策略与规程	54
15.2	安全组织	54
15.3	岗位风险与职责	55
15.4	人员筛选	55
15.5	人员离职	56
15.6	人员调动	56
15.7	第三方人员安全	56
15.8	人员处罚	57
15.9	安全培训	57
16	物理与环境安全	58
16.1	物理设施与设备选址	58
16.2	物理和环境规划	58
16.3	物理环境访问授权	59
16.4	物理环境访问控制	59
16.5	输出设备访问控制	60
16.6	物理访问监控	60
16.7	访客访问记录	60
16.8	设备运送和移除	61
附录 A (资料性)	安全能力要求汇总	62
附录 B (资料性)	本文件的实现情况描述	68
参考文献		70

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。本文件代替 GB/T 31168—2014《信息安全技术 云计算服务安全能力要求》，与 GB/T 31168—2014 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 更改了本文件的适用范围(见第1章,2014年版的第1章)；
- b) 增加了对 GB/T 32400—2015 和 GB/T 35273—2020 的规范性引用(见第3章、9.1.1)；
- c) 更改了部分术语和定义(见第3章,2014年版的第3章)；
- d) 增加了“缩略语”一章(见第4章)；
- e) 将“云服务模式”更改为“云能力类型”(见5.1)；
- f) 增加了高级要求,每类安全要求分别对应一般要求、增强要求和高级要求(见5.4)；
- g) 删除了“本文件的结构”(见2014年版的4.7)；
- h) 删除了原各类要求分别对应的策略与规程,整合至第14章的“策略与规程”(见14.1,2014年版的5.1、6.1、7.1、8.1、9.1、10.1、11.1、12.1、13.1和14.1)；
- i) 增加了“安全管理功能的通信保护”(见7.14)；
- j) 增加了“WEB访问安全”“API访问安全”(见8.21、8.22)；
- k) 增加了“数据保护”一章,提出数据安全要求,确保客户迁移数据过程中的业务连续性和数据完整性(见第9章)；
- l) 将“维护”一章的名称更改为“维护管理”(见第11章,2014年版的第9章)；
- m) 更改了“机房设计”的内容(见第16章,2014年版的第14章)。

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。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中电数据服务有限公司、四川大学、杭州安恒信息技术股份有限公司、中国科学技术大学、中国电子技术标准化研究院、中国网络安全审查技术与认证中心、国家信息技术安全研究中心、中国信息安全测评中心、中国信息通信研究院、北京信息安全测评中心、国家工业信息安全发展研究中心、中国软件评测中心、中国移动通信集团有限公司、中电长城网际系统应用有限公司、神州网信技术有限公司、深信服科技股份有限公司、宁夏西云数据科技有限公司、三六零数字安全科技集团有限公司、蚂蚁科技集团股份有限公司、合肥高维数据技术有限公司、上海市方达(北京)律师事务所、北京中测安华科技有限公司、中电和瑞科技有限公司、阿里云计算有限公司、武汉理工大学、四川发展大数据产业投资有限责任公司、南方电网数字传媒科技有限公司、上海观安信息技术股份有限公司、中科锐眼(天津)科技有限公司。

本文件主要起草人：周亚超、罗永刚、左晓栋、陈兴蜀、李世锋、张建军、闵京华、杨建军、李斌、伍扬、王惠莅、张弛、单博深、许皖秀、崔占华、王启旭、杨苗苗、张明天、刘佳良、胡华明、丁晓、史大为、卢夏、李媛、何延哲、刘俊河、王强、陈雪鸿、杨帅锋、柳彩云、胡振泉、耿贵宁、邵江宁、韦韬、郭亮、贾依真、叶润国、田辉、尹云霞、杜宇鸽、安兆彬、吴复伟、张滨、江为强、刘雨桁、杨婷、李安伦、肖广娣、程军军、王坤、张峰、邱勤、艾青松、龙毅宏、张大江、黄少青、果靖、郑珂雪、陈清明、王永基、郑赳、杨勃、王朝栋、张照龙、蒋韬、赵洪宇。

本文件及其所替代文件的历次版本发布情况为：

- 2014年首次发布 GB/T 31168—2014；
- 本次为第一次修订。

引 言

本文件与 GB/T 31167—2023《信息安全技术 云计算服务安全指南》构成了云计算服务安全管理的基础文件。GB/T 31167—2023 提出了客户采用云计算服务的安全管理基本原则,给出了采用云计算服务的生命周期各阶段的安全管理和技术措施;本文件面向云服务商,描述了提供云计算服务时应具备的安全技术能力。

参照 GB/T 31167—2023,本文件分为一般要求、增强要求和高级要求。根据云计算平台上的数据敏感度和业务重要性的不同,云服务商具备的安全能力也各不相同。

信息安全技术

云计算服务安全能力要求

1 范围

本文件规定了云服务商提供云计算服务时应具备的安全能力。

本文件适用于对云计算服务能力的建设、监督、管理和评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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—2022 信息安全技术 术语

GB/T 31167—2023 信息安全技术 云计算服务安全指南

GB/T 32400—2015 信息技术 云计算 概览与词汇

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB 50174 数据中心设计规范

3 术语和定义

GB/T 25069—2022、GB/T 31167—2023 和 GB/T 32400—2015 界定的以及下列术语和定义适用于本文件。

3.1

云计算 **cloud computing**

通过网络访问可扩展的、灵活的物理或虚拟共享资源池,并按需自助获取和管理资源的模式。

注:资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

3.2

云计算服务 **cloud computing service**

使用定义的接口,借助云计算(3.1)提供一种或多种资源的能力。

3.3

云服务商 **cloud service provider**

提供云计算服务(3.2)的参与方。

3.4

云服务客户 **cloud service customer**

为使用云计算服务而处于一定业务关系中的参与方。

注1:业务关系不一定包含经济条款。

注2:本文件中云服务客户简称客户。