



中华人民共和国国家标准

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 of cloud computing services

2014-09-03 发布

2015-04-01 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	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 概述	2
4.1 云计算安全措施的实施责任	2
4.2 云计算安全措施的作用范围	3
4.3 安全要求的分类	4
4.4 安全要求的表述形式	4
4.5 安全要求的调整	5
4.6 安全计划	5
4.7 本标准的结构	6
5 系统开发与供应链安全	6
5.1 策略与规程	6
5.2 资源分配	6
5.3 系统生命周期	7
5.4 采购过程	7
5.5 系统文档	8
5.6 安全工程原则	8
5.7 关键性分析	8
5.8 外部信息系统服务及相关服务	9
5.9 开发商安全体系架构	9
5.10 开发过程、标准和工具	10
5.11 开发商配置管理	10
5.12 开发商安全测试和评估	11
5.13 开发商提供的培训	12
5.14 防篡改	12
5.15 组件真实性	12
5.16 不被支持的系统组件	13
5.17 供应链保护	13
6 系统与通信保护	14
6.1 策略与规程	14
6.2 边界保护	15
6.3 传输保密性和完整性	15
6.4 网络中断	16

6.5	可信路径	16
6.6	密码使用和管理	16
6.7	协同计算设备	16
6.8	移动代码	16
6.9	会话认证	17
6.10	移动设备的物理连接	17
6.11	恶意代码防护	17
6.12	内存防护	17
6.13	系统虚拟化安全性	18
6.14	网络虚拟化安全性	18
6.15	存储虚拟化安全性	19
7	访问控制	19
7.1	策略与规程	19
7.2	用户标识与鉴别	20
7.3	设备标识与鉴别	20
7.4	标识符管理	20
7.5	鉴别凭证管理	21
7.6	鉴别凭证反馈	21
7.7	密码模块鉴别	22
7.8	账号管理	22
7.9	访问控制的实施	22
7.10	信息流控制	23
7.11	最小特权	24
7.12	未成功的登录尝试	24
7.13	系统使用通知	24
7.14	前次访问通知	25
7.15	并发会话控制	25
7.16	会话锁定	25
7.17	未进行标识和鉴别情况下可采取的行动	25
7.18	安全属性	26
7.19	远程访问	26
7.20	无线访问	26
7.21	外部信息系统的使用	27
7.22	信息共享	27
7.23	可供公众访问的内容	27
7.24	数据挖掘保护	27
7.25	介质访问和使用	28
7.26	服务关闭和数据迁移	28
8	配置管理	28
8.1	策略与规程	28
8.2	配置管理计划	29
8.3	基线配置	29
II		

8.4	变更控制	29
8.5	配置参数的设置	30
8.6	最小功能原则	30
8.7	信息系统组件清单	31
9	维护	31
9.1	策略与规程	31
9.2	受控维护	32
9.3	维护工具	32
9.4	远程维护	32
9.5	维护人员	33
9.6	及时维护	33
9.7	缺陷修复	33
9.8	安全功能验证	34
9.9	软件、固件、信息完整性	34
10	应急响应与灾备	34
10.1	策略与规程	34
10.2	事件处理计划	35
10.3	事件处理	35
10.4	事件报告	35
10.5	事件处理支持	36
10.6	安全警报	36
10.7	错误处理	36
10.8	应急响应计划	37
10.9	应急培训	37
10.10	应急演练	37
10.11	信息系统备份	38
10.12	支撑客户的业务连续性计划	38
10.13	电信服务	38
11	审计	39
11.1	策略与规程	39
11.2	可审计事件	39
11.3	审计记录内容	39
11.4	审计记录存储容量	40
11.5	审计过程失败时的响应	40
11.6	审计的审查、分析和报告	40
11.7	审计处理和报告生成	40
11.8	时间戳	41
11.9	审计信息保护	41
11.10	不可否认性	41
11.11	审计记录留存	41
12	风险评估与持续监控	42
12.1	策略与规程	42

12.2	风险评估	42
12.3	脆弱性扫描	42
12.4	持续监控	43
12.5	信息系统监测	43
12.6	垃圾信息监测	44
13	安全组织与人员	44
13.1	策略与规程	44
13.2	安全组织	45
13.3	安全资源	45
13.4	安全规章制度	45
13.5	岗位风险与职责	46
13.6	人员筛选	46
13.7	人员离职	46
13.8	人员调动	46
13.9	访问协议	47
13.10	第三方人员安全	47
13.11	人员处罚	47
13.12	安全培训	48
14	物理与环境安全	48
14.1	策略与规程	48
14.2	物理设施与设备选址	48
14.3	物理和环境规划	49
14.4	物理环境访问授权	49
14.5	物理环境访问控制	49
14.6	通信能力防护	50
14.7	输出设备访问控制	50
14.8	物理访问监控	50
14.9	访客访问记录	50
14.10	电力设备和电缆安全保障	51
14.11	应急照明能力	51
14.12	消防能力	51
14.13	温湿度控制能力	52
14.14	防水能力	52
14.15	设备运送和移除	52
附录 A (资料性附录) 系统安全计划模版		53
参考文献		59