



2016 杭州·云栖大会
THE COMPUTING CONFERENCE




SANGFOR
深信服科技

云栖社区
yq.aliyun.com

面向关键信息基础设施的等级保护

——云计算等级保护标准介绍

2016
The Computing Conference

主办单位： 杭州

 Alibaba Group
阿里巴巴集团

战略合作伙伴：

署名：任卫红

单位：公安部信息等级保护评估中心



扫码观看大会视频

目录

content

关键信息基础设施等级保护需求

云计算定级对象和定级

云计算等级保护基本要求标准介绍



一、关键信息基础设施等级保护需求



等级保护制度的主要内容

- 定级：将信息系统（包括网络）按照重要性和遭受损坏后的影响程度分成五个安全保护等级；
- 备案：等级确定后，第二级（含）以上信息系统到公安机关备案，公安机关审核后颁发备案证明；
- 建设整改：备案单位根据信息系统安全等级，按照国家政策、标准开展安全建设整改；
- 测评：备案单位选择符合国家规定条件的测评机构开展等级测评；
- 检查：公安机关定期开展监督、检查、指导。



等级保护对象与关键信息基础设施

《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）：要重点保护**基础信息网络**和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧**建立信息安全等级保护制度**。



《网络安全法》(草案二次审议稿)

第二十条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

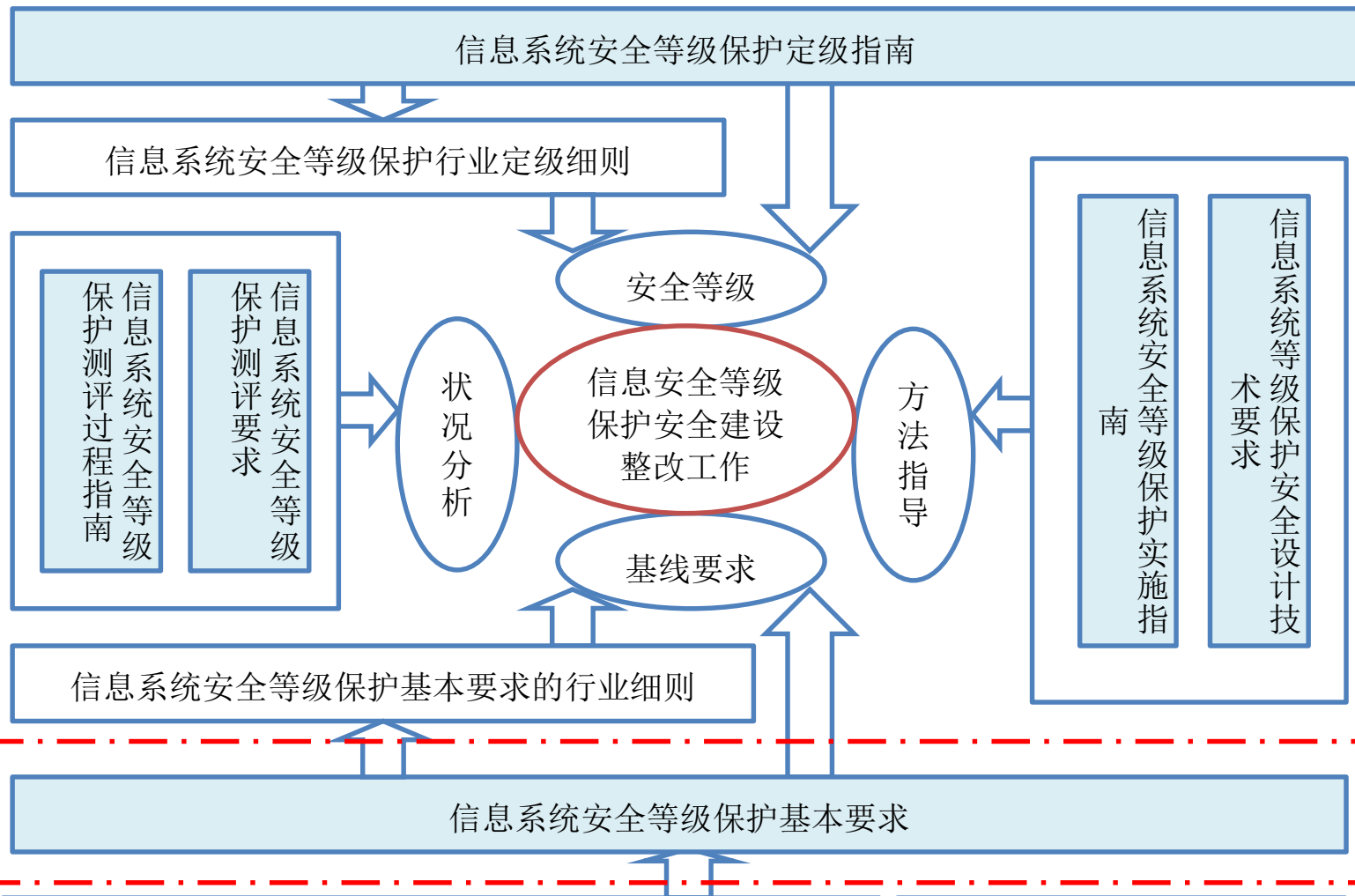
第二十九条 国家对一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。



我国关键信息基础设施

我国关键信息基础设施是指关系国家核心利益、
人民群**关键信息基础设施的安全保护等级**一旦遭
到破坏、丧失功能或数据泄露，可能严重危害国家安
全、国计民生和公共利益的**网络基础设施、重要业务**
不低于第三级。系统和生产控制系统以及重要数据资源。





关键信息基础设施保护发展需求

面对关键信息基础设施，等级保护《基本要求》需要创新发展：

- ◆ 适应新型的系统形态和网络架构
- ◆ 面对新技术新应用的扩展
- ◆ 使基本指标具有动态、可扩展性
- ◆ 从合规测评到CIIP安全状态评价



新技术应用的等级保护标准

《网络安全等级保护基本要求》

- ◆ 第1部分：安全通用要求
- ◆ 第2部分：云计算安全扩展要求
- ◆ 第3部分：移动互联安全扩展要求
- ◆ 第4部分：物联网安全扩展要求
- ◆ 第5部分：工业控制安全扩展要求
- ◆ 第6部分：大数据安全扩展要求



二、云计算等级保护对象和定级



定级对象的演变

➤ 定级对象

➤ 信息系统



➤ 业务处理类对象

➤ 信息系统、工业控制系统、
物联网系统等

➤ 基础服务类对象

➤ 网络、云服务平台、大数
据分析平台等

➤ 数据资源类对象

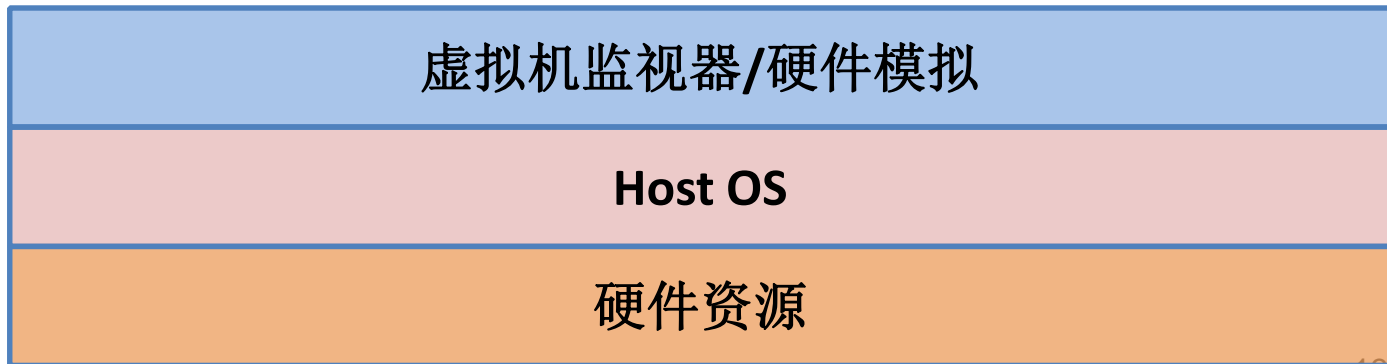


云计算相关定级对象

系统
定级
对象

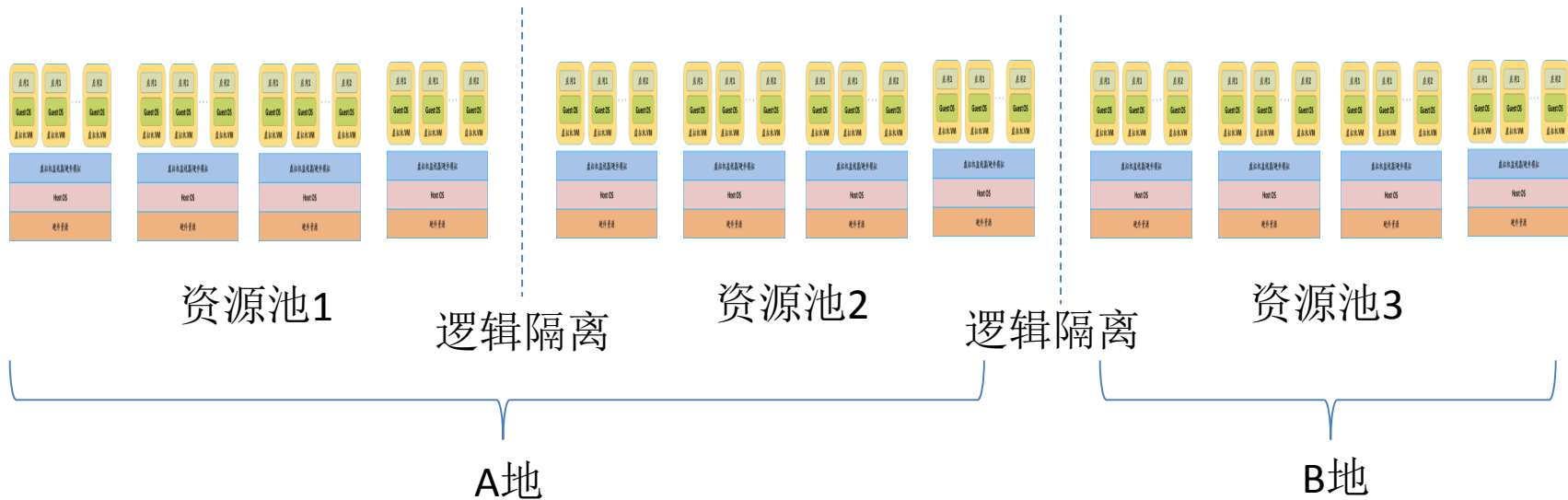


平台
定级
对象



云平台定级对象

业务管理平台



运行管理平台



云计算相关定级对象

- 云平台定级对象的设备位置与管控中心位置物理分离，是另一种跨地域部署系统类型。建议按大集中分布式部署系统定级备案。
- 云服务商可能的定级对象划分方法：按服务类型、按部署模式。



云计算相关定级对象

- 云服务方的云平台与云租户的应用系统应分别定级，平台等级不低于应用的安全保护等级
- 云平台先定级测评，再将已定级应用系统向云平台迁移，云上应用定级参照传统信息系统。



三、云计算等级保护基本要求标准介绍



安全威胁

- 数据丢失、被篡改或泄露
- 网络攻击
- 利用不安全接口的攻击
- 云服务中断
- 越权、滥用与误操作
- 滥用云服务
- 利用共享技术漏洞进行的攻击
- 过度依赖
- 数据残留



标准结构

- 1 范围
- 2 规范性引用文件
- 3 术语和定义
- 4 概述
- 5 第二级安全要求
- 6 第三级安全要求
- 7 第四级安全要求

附录A与GB/T 22239.1的关系，附录B、安全威胁、
附录C不同服务模式的安全管理责任主体



技术和管理要求扩展

技术要求

物理和环境安全

网络和通信安全

设备和计算安全

应用和数据安全

管理要求

安全管理机构和人员

系统安全管理

系统安全运维管理



层面	云平台保护对象	云上系统保护对象
物理和环境	机房及相关设施	
网络和通信	传统网络结构和 虚拟化网络结构 传统网络设备、安全设备 虚拟化网络设备、安全设备	虚拟化网络结构、虚拟化网络设备、虚拟化安全设备
设备和计算	传统主机、宿主机、虚拟机、主机安全软件 虚拟机监视器（Hypervisor/VMM） 云操作系统	传统主机、 虚拟机 、主机安全软件
应用和数据	中间件、 云应用开发框架	业务应用系统、业务数据、管理数据、 用户隐私数据



针对云租户的安全要求

– IaaS服务

- 通用要求：除物理与环境安全外的所有要求。
- 扩展要求：网络和通信安全、设备和计算安全、应用和数据安全、系统安全管理。

– PaaS、SaaS服务

- 通用要求：应用和数据安全，部分安全管理要求
- 扩展要求：应用和数据安全



针对云租户的安全要求

— 网络和通信安全

- 在虚拟化网络边界、不同等级的网络区域边界部署访问控制机制，设置访问控制规则。
- 允许云租户设置不同虚拟机之间的访问控制策略；
- 远程管理时，管理终端和云计算平台边界设备之间应建立双向身份验证机制
- 根据云服务方和云租户的职责划分，收集各自控制部分的审计数据，实现各自控制部分的集中审计



针对云租户的安全要求

— 设备和通信安全

- 远程管理时，防止远程管理设备同时直接连接其他网络。
- 能够检测恶意代码感染及在虚拟机间蔓延的情况，并提出告警
- 针对重要业务系统采用加固的操作系统镜像；
- 集中审计

— 应用和数据安全

- 对应用系统的运行状况进行监测，并在发现异常时进行告警
- 云租户应在本地保存其业务数据的备份；



针对云服务商的扩展要求

- 定级对象需满足通用要求和云计算扩展要求；
- 云计算虚拟对象需要满足通用要求中的部分要求；
- 一般信息系统对象需要满足扩展要求的部分要求；
- 云平台既需要具备相应等级自身保护能力，也需要具备提供云上应用相应等级的保护能力。



物理位置

- 应确保用于业务运行和数据处理及存储的物理设备位于中国境内。



平台安全

- 基础设施的组件自身安全应遵循《基本要求》；
- 登录Hypervisor、云管理平台等的管理用户进行相应等级身份鉴别；
- 进行远程管理时，管理终端和云平台边界设备之间应建立双向身份验证机制；
- 网络策略控制器和网络设备之间双向认证、数据加密传输



资源隔离

- 应根据承载的业务系统安全保护等级划分资源池，并实现资源池之间的隔离；应保证虚拟机仅能迁移至相同安全保护等级的资源池；
- 应保证分配给虚拟机的内存空间仅供其独占访问；
- 应保证云计算平台管理流量与云租户业务流量分离；
- 应保证虚拟机所使用的内存和存储空间回收时完全清除。



访问控制

- 依据访问控制策略实现虚拟机之间访问
- 实现云平台管理用户权限分离机制，为网络管理员、系统管理员建立不同账户并分配相应的权限
- 确保只有在云租户授权下，云服务方或第三方才具有云租户数据的管理权限
- 云计算平台应提供开放接口或开放性安全服务，允许云租户接入第三方安全产品或在云平台选择第三方安全服务。



数据安全

- 应提供查询云租户数据及备份存储位置的方式
- 应保证云租户业务及数据能移植到其他云平台或者迁移到本地信息系统
- 提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改
- 对虚拟机快照中的敏感信息进行加密保护
- 提供虚拟机迁移过程中的完整性保护和信息防泄漏



审计与监控

- 能识别、监控虚拟机之间、虚拟机与物理机之间、虚拟机与宿主机之间的流量
- 保证云服务方对云租户系统和数据的操作可被云租户审计
- 根据云服务方和云租户的职责划分，实现各自控制部分的集中审计
- 应为安全审计数据的汇集提供接口，可供第三方审计



云租户：管理要求

- 应根据业务系统的安全保护等级选择能够提供相应安全等级保护能力的云服务商；
- 应以书面方式约定云服务的各项服务内容和具体技术指标；
- 应以书面方式约定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。



云服务商：管理要求

- 签订服务水平协议SLA和签订隐私保护协议，并可向第三方提供相关证明
- 供应链管理：文档提供、风险分析、措施描述、持续监控等
- 监控管理：对通信线路、物理资源、主机、网络设备、虚拟资源、云管理平台和应用软件的运行状况、网络流量、用户行为等进行监测和报警



2016 The
Computing
Conference
THANKS



SANGFOR
深信服科技

