网络安全创新大会
Cyber Security Innovation Summit

网络安全等级保护2.0之云计算安全测评指标选取原则

陈妍

博士 副研究员
公安部第三研究所检测中心
云计算与公安大数据安全测评实验室主任

什么是网络安全等级保护？

对网络（含信息系统、数据）实施分等级保护、分等级监管，对网络中使用的网络安全产品实行按等级管理，对网络中发生的安全事件分等级响应、处置。

网络：由计算机或其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、处理的系统，包括网络设施、信息系统、数据资源等。

网络安全等级保护的意义？

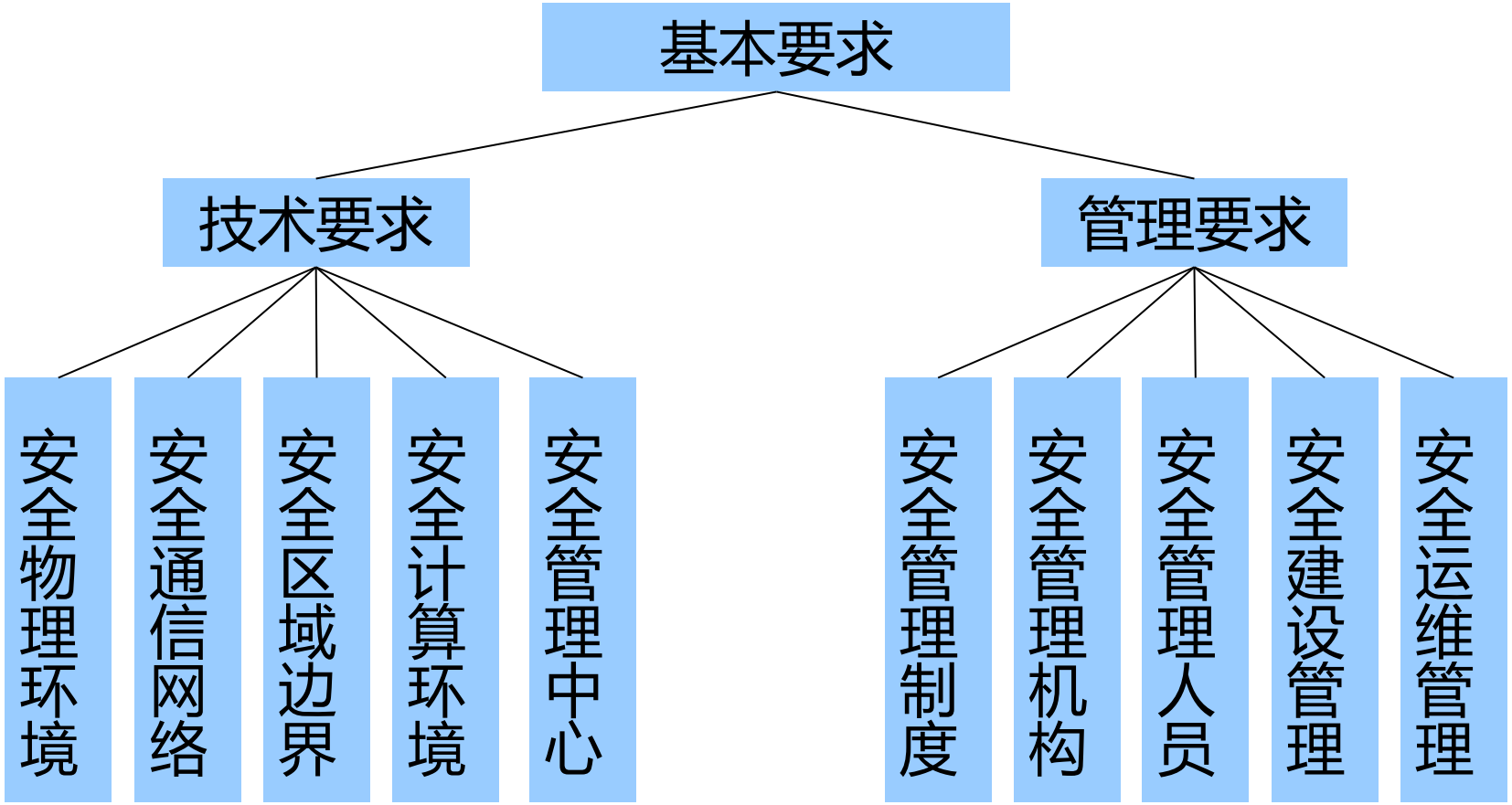
是党中央有关文件和《网络安全法》确定的网络安全基本制度。

保护关键信息基础设施、重要网络和数据免受攻击、侵入、干扰和破坏。

切实维护国家网络空间主权、国家安全和社会公共利益，保护人民群众的合法权益，保障和促进经济社会信息化健康发展。

网络安全等级保护2.0

- GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求——建设整改、等级测评、监督检查



网络安全等级保护2.0之云计算安全

8 第三级安全要求

8.1 安全通用要求

8.2 云计算安全扩展要求

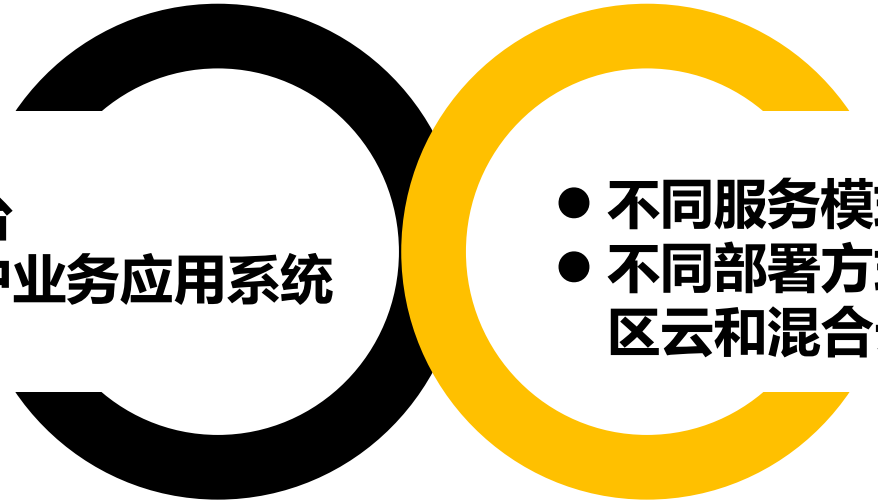
8.3 移动互联安全扩展要求

8.4 物联网安全扩展要求

8.5 工业控制系统安全扩展要求

	安全通用要求	云计算安全扩展要求
技术部分	安全物理环境	安全物理环境
	安全通信网络	安全通信网络
	安全区域边界	安全区域边界
	安全计算环境	安全计算环境
	安全管理中心	安全管理中心
管理部分	安全管理制度	——
	安全管理机构	——
	安全管理人员	——
	安全建设管理	安全建设管理
	安全运维管理	安全运维管理

网络安全等级保护2.0之云计算安全



1. 云计算平台
2. 云服务客户业务应用系统

- 不同服务模式（ IaaS、PaaS和SaaS ）
- 不同部署方式（公有云、私有云、社区云和混合云）

云安全威胁

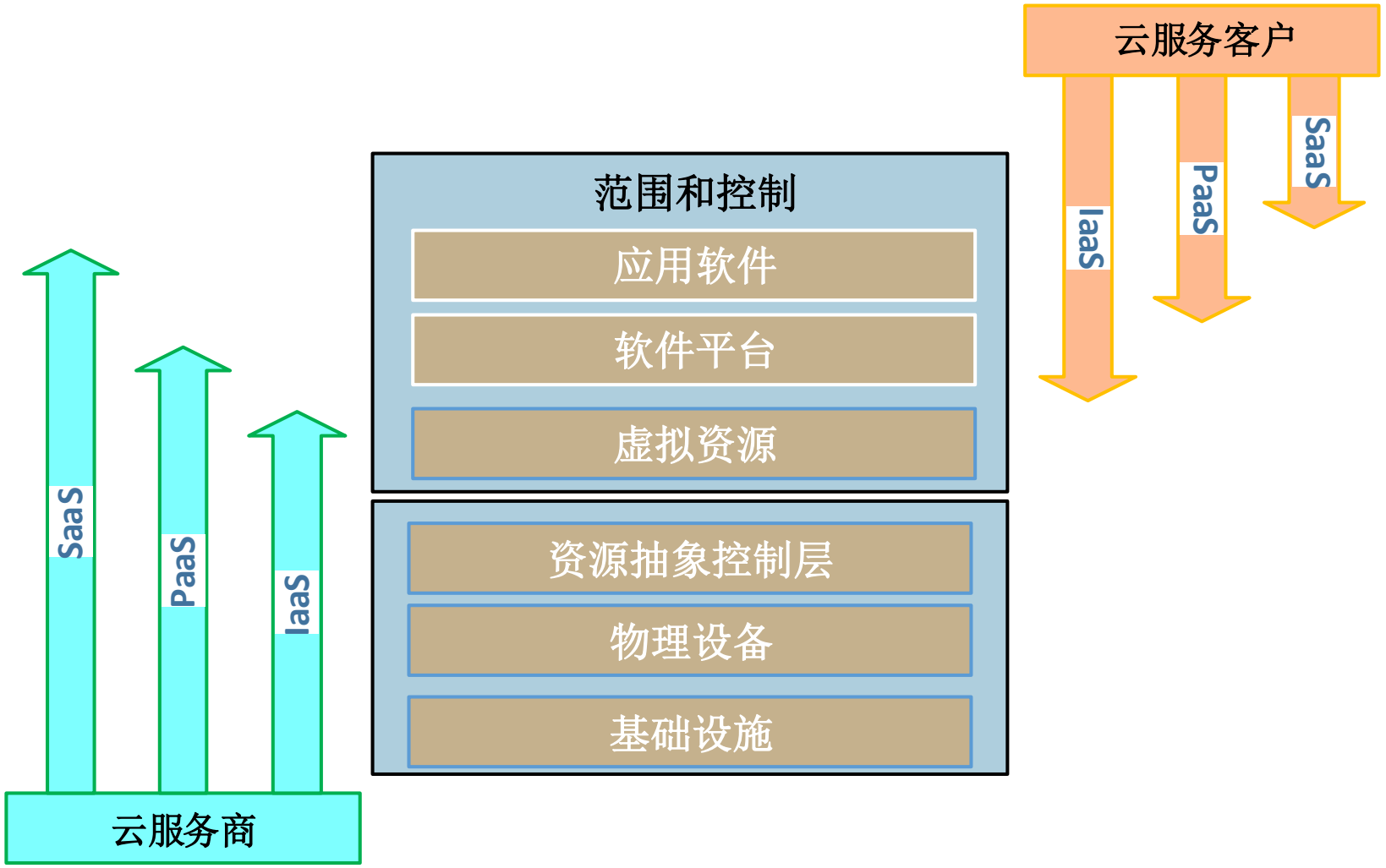
序号	Top Threats 2016
1	数据泄露
2	身份/凭据和访问管理不善
3	不安全的接口和API
4	系统漏洞
5	账号劫持
6	恶意的内部人士
7	APT（高级持续性威胁）
8	数据丢失
9	调查不足
10	滥用和恶意使用云服务
11	拒绝服务（DoS）攻击
12	共享技术的问题

CSA《12 大云安全威胁》

序号	Top Threats 2020
1	数据泄露
2	配置错误和变更控制不足
3	云安全架构和策略缺失
4	身份、凭证、访问和密钥管理不善
5	账号劫持
6	恶意的内部人士
7	不安全的接口和API
8	控制面薄弱
9	分界面失效
10	云资源使用的可见性差
11	滥用和恶意使用云服务

CSA《云计算11大威胁报告》

安全责任共担模型


云服务客户
SaaS
PaaS
IaaS
范围和控制
应用软件
软件平台
虚拟资源
资源抽象控制层
物理设备
基础设施
SaaS
PaaS
IaaS
云服务商

指标选取原则

责任分担原则

区别于传统信息系统，云计算环境中涉及一个或多个安全责任主体，各安全责任主体应根据管理权限的范围、根据部署模式的不同划分安全责任边界。

云服务模式适用性原则

云计算环境中可能承载一种或多种云服务模式，每种云服务模式下提供了不同的云计算服务及相应的安全防护措施，在对云计算平台/系统测评时，应仅关注每种特定云服务模式下，与其提供的云服务相对应的安全防护措施有效性。

不同服务模式

安全通信网络

网络结构

a）应保证云计算平台不承载高于其安全保护等级的业务应用系统；

解读：

——云服务商：云平台应对租户公开系统等级及等保测评通过情况（综合得分、符合情况、等保报告编号及通过时间），同时在管理上对其进行要求。

——云服务客户：选择云平台应通过等保测评，且级别大于等于云服务客户系统级别。

——IaaS、PaaS、SaaS的适用性。

不同服务模式

安全通信网络

网络结构

b)应实现不同云服务客户虚拟网络之间的隔离；

解读：

——云服务商：主要是IaaS，PaaS和SaaS的网络架构一般不对客户提供网络配置的能力，其可以为不同的云服务客户进行网络隔离，也可以通过其它方式进行客户隔离。

——云服务客户：不适用。

——容器服务？

不同服务模式

安全区域边界

入侵防范

a)应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

解读：

——攻击方向：云服务客户对其他云服务客户的攻击，也包括云服务客户对平台以及对外部的攻击；东西向、南北向。

——安全通用要求—安全区域边界—入侵防范—a)应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；b)应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。

不同服务模式

安全计算环境

镜像和快照保护

b)应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；

解读：

——云服务商，对于IaaS平台来说，如为客户提供操作系统镜像，应能提供加固的镜像或提供加固服务；对于PaaS平台来说，如提供容器镜像，也应满足该项要求。

——IaaS、PaaS、SaaS的适用性。

不同部署方式

安全通信网络

网络架构

d)应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略；

解读：

——云服务商。

——IaaS、PaaS、SaaS的适用性。

——公有云、行业云、私有云。

不同部署方式

安全管理中心

集中管控

d）应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

解读：

——云服务商、云服务客户。

——IaaS、PaaS、SaaS的适用性。

——公有云、行业云、私有云。

云平台的嵌套问题

一个IaaS平台上部署了一个PaaS平台，PaaS平台上运行着一个SaaS业务应用系统：

- IaaS平台
- PaaS平台（不另外测评IaaS部分）、IaaS租户
- SaaS业务应用系统（不另外测评IaaS、PaaS部分）、PaaS租户

指标选取原则

在进行指标选取时只考虑等级测评对象作为其角色的基本属性所可能存在的安全风险。

通过这样模式解耦、场景组合的方式考虑云计算安全扩展要求的测评指标适用性，将有助于更好地满足不同服务模式、不同责任主体下的安全防护需求

网络安全创新大会
Cyber Security Innovation Summit

THANKS