基本要求云计算安全扩展要求标准应用实践

引 言

11 月 17-18 日，在杭州举办的第七届全国网络安全等级保护测评体系建设会议取得圆满成功。与往年不同，本次会议会期从一天增加到两天，邀请了多位专家就等级保护标准解读、新技术新应用测评实践指导、等级测评工作经验交流、测评业务规范化管理等方面进行了深入交流和探讨，在业内获得了良好反响，与会人士普遍评价此次会议干货满满。目前，有不少业内人士通过各个渠道向我们索取会议资料，应大家的需要，接下来我们会将专家的演讲内容陆续通过本号发出，与更多的业内人士分享。

基本要求云计算安全扩展要求标准应用实践

01

系列标准变化

对 GB/T 22239-2008 进行修订的思路和方法是针对无线移动接入、云计算、大数据、物联网和工业控制系统等新技术、新应用领域形成基本要求的多个部分。

基本要求标准由原来的单一部分变更为由多个部分组成的标准，包括：安全通用要求、云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求、工业控制系统安全扩展要求、大数据安全扩展要求（待立项）。

所以说《基本要求》已经从原来的单一部分标准进化为“1+N”的多部分标准，“1”代表安全通用要求，也就是说这部分要求是所有等级保护对象都要满足的最基本的部分，是存在共性的要求，无论是传统信息系统还是云计算系统、工业控制系统、物联网系统等等，都要先依据安全通用要求中的内容实施安全保护。“N”代表专有领域。也就是说专有领域内的等级保护对象所特有的安全控制要求分别在后面的这几个分册中。为什么不直接写“1+6”呢？因为随着新技术新应用领域的不断发展，未来可能在其他领域形成专有系统，如果时机成熟，《基本要求》系列标准将继续针对这些新兴领域进行扩充，比如我们可以脑洞一下，最近火到不行的 AI，是不是有可能针对人工智能领域出一个分册呢？要知道 AI 的安全不亚于前面这些领域，我们可以脑补，没有了 AI 系统的安全基线要求，说不定“天网”真的会启动呢。

02

与安全通用要求的关系

既然本部分标准作为《基本要求》系列标准在云计算安全领域的扩展，那云计算安全扩展要求与安全通用要求之间一定存在着密不可分的关系。

举个例子，在物理位置选择这个控制点上，对应第一级，云计算安全扩展要求较安全通用要求是增加的，意味着在安全通用要求中第一级没有对物理位置选择提出要求，而在云计算安全扩展要求中提出了物理位置选择的要求。我们具体看下提了什么？在第一级物理和环境安全中有一条要求“应确保云计算基础设施位于中国境内”，而在安全通用要求的第一级要求中没有物理位置选择的控制点，也就是“基础设施在中国境内”是云计算领域特有的要求。

03

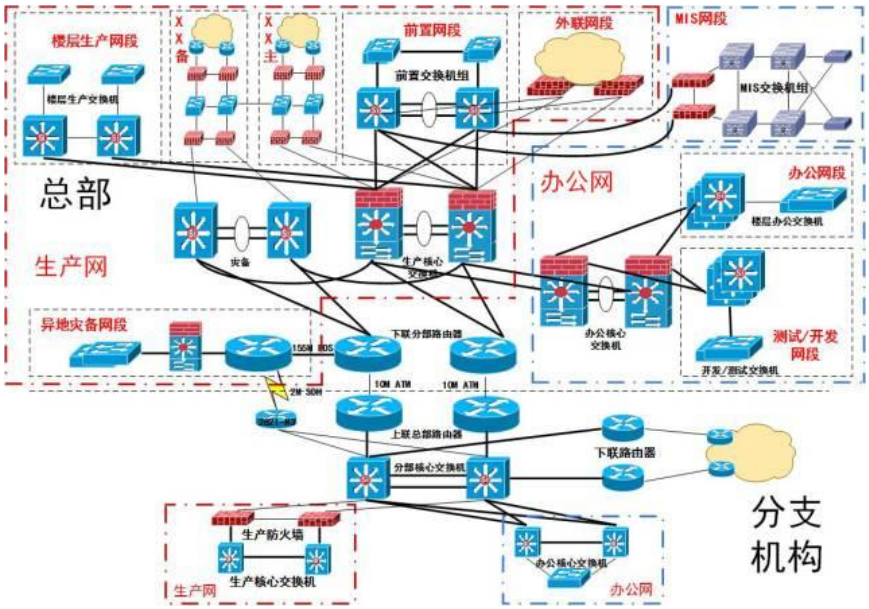
云计算系统测评实践

（一）系统边界划分

我们在做等级测评时，首先面对的问题是如何合理对云计算系统进行准确划分，只有合理的对云计算系统准确划分、找出系统的边界，才能通过测评判断业务应用系统的安全防护措施是否与系统重要性等级向匹配。因此我们依然要从业务应用的角度出发来寻找系统边界。

云计算系统边界划分方法与传统信息系统边界划分存在不同，在介绍云计算系统边界划分方法之前，我们先来看看传统信息系统的边界划分方法是怎样的。

这里我们举一个例子。

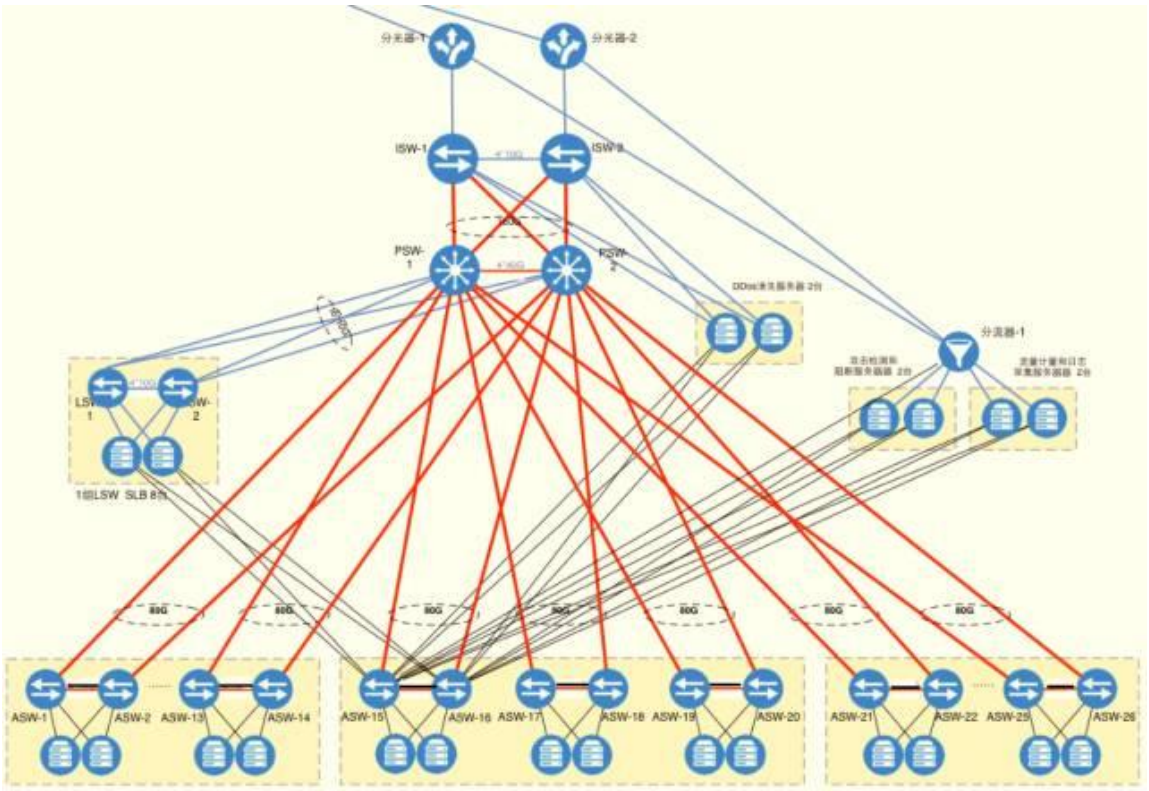


这是一个典型的传统信息系统的网络拓扑图，有总部有分支机构，有生产网有办公网，还有外联区域和办公区域。应该说作为传统业务架构，这样的网络拓扑能够很好的适应业务需要。业务到哪里网络就铺设到哪里。这样的网络架构还有一个特点，就是网络访问控制功

能与硬件的紧耦合。因此，我们在寻找系统边界时很容易的把负责网络访问控制功能的硬件作为系统的边界。

但是到了云时代，为了适应业务快速发展变化的需要，传统的网络架构已经无法适应，而云计算系统的技术特点恰好满足企业业务应用快速发展的需要，因此越来越多的系统转移到云上。

下面我们再来看看一个典型的云计算系统架构。

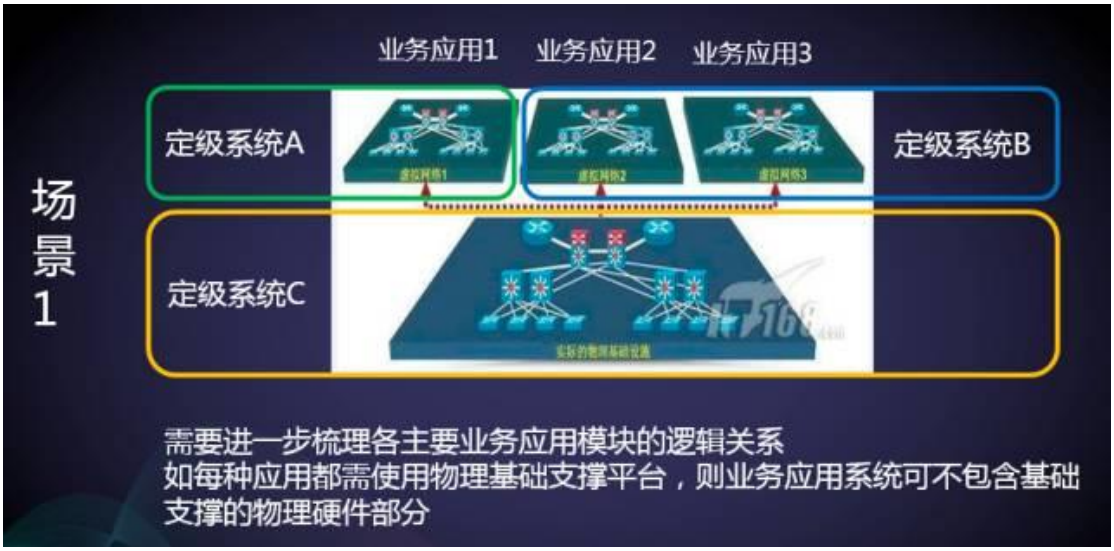


这是一个典型云计算系统架构，基本上是一个二层架构，路由器下面接交换机，交换机下面接的全部是通用服务器。相当一部分网络访问控制功能是由软件和策略实现的，不再完全依赖网络访问控制硬件设备。在这样的架构中，应用系统可以快速的部署、快速迭代和快速调整。但是网络访问控制功能和硬件呈现松耦合状态，我们再用传统信息系统划分找物理边界的方法已经无法实现。

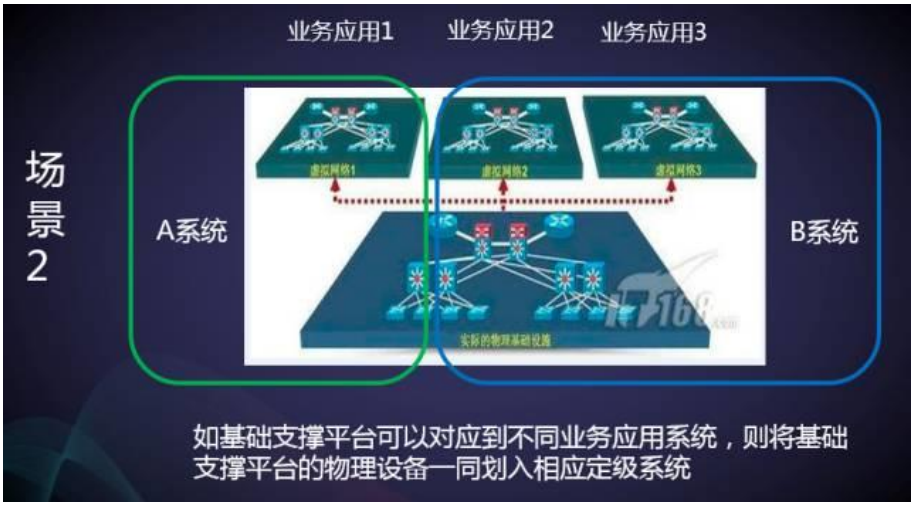
面对这样的云计算系统，如果依然用传统从物理设备的划分上找系统边界就容易忽略系统定级划分的“初心”，这个“初心”是对系统的业务信息和服务的重要性等级的确定。如果仅仅从物理设备的划分上找系统边界，我们无法将云计算系统与其承载的业务应用的信息和服务的重要性等级相对应。

因此，在这样的架构下寻找系统边界，我们依然要“不忘初心”。也就是说我们要从业务应用出发，搞清楚云计算系统承载了多少个业务应用、这些业务应用使用哪些系统模块，系统模块彼此间依赖关系是什么、有没有多个业务应用公共用的模块，再往下看这些模块有没有相对独立硬件资源池。只有这样层层向下，抽丝剥茧，才能最终确定系统边界。

云计算系统边界划分有两种基本场景。



在场景 1 中，存在业务应用不独占硬件物理资源或硬件物理资源上运行的基础服务系统是所有业务应用公用的情况，这时定级系统的边界应划在虚拟边界处，这个虚拟边界就是运行业务应用所用到的最底层独占虚拟资源，通常是虚拟机。在这个场景中有 3 个业务应用，通过对业务应用的梳理，业务应用 1 单独成为一个定级系统，业务应用 2 和业务应用 3 组成另一个定级系统。这两个定级系统公用底层服务，因此我们把底层服务连同硬件一起作为一个定级系统。当这个场景提供的是一种云计算服务时，定级系统 C 就是云计算平台了，定级系统 A 和定级系统 B 就是云平台上承载的业务应用系统。



在场景 2 中，我们依然从业务应用梳理，找到与业务应用对应的系统模块，进一步梳理发现这些业务模块存在相对独立的底层服务和硬件资源，因此我们可以将整个系统边界划分到硬件物理设备，就像切蛋糕一样可以一刀切到底，从而确定出两个定级系统。如果这个场景对应的是对外提供服务的云计算系统，那么定级系统 A 就是一个使用了云计算技术的应用系统，而顶级系统 B 是另一个使用了云计算技术的应用系统。同理，我们依然可以在定级系统 B 上嵌套场景 1 的情况，那么定级系统 B 这个云计算平台有可能也会承载多个业务应用系统，这里就不重复赘述了。

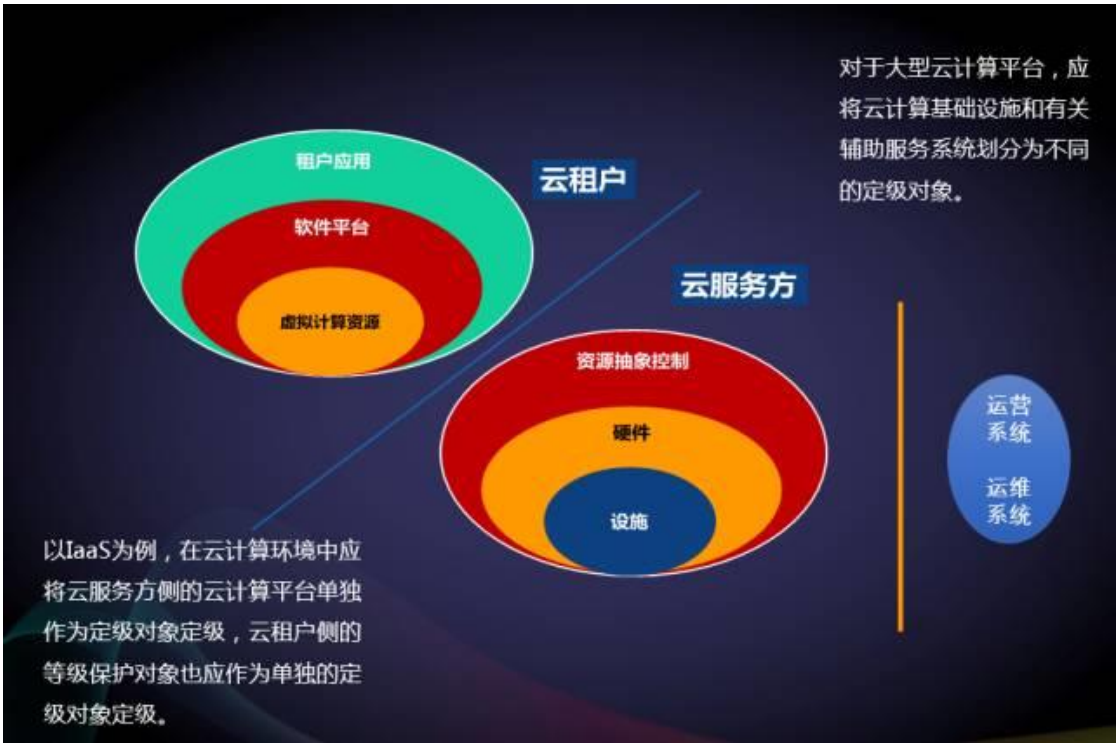
以上是云计算系统边界划分方法。云计算系统定级过程中还有几点注意：

1.应根据其承载或将要承载的等级保护对象的重要程度确定其安全保护等级，原则上应不低于其承载的等级保护对象的安全保护等级

2.国家关键信息基础设施（重要云计算平台）的安全保护等级应不低于第三级

3.在云计算环境中，应将云服务方侧的云计算平台单独作为定级对象定级，云服务客户侧的等级保护对象也应作为单独的定级对象定级

4.对于大型云计算平台，应将云计算基础设施和有关辅助服务系统划分为不同的定级对象

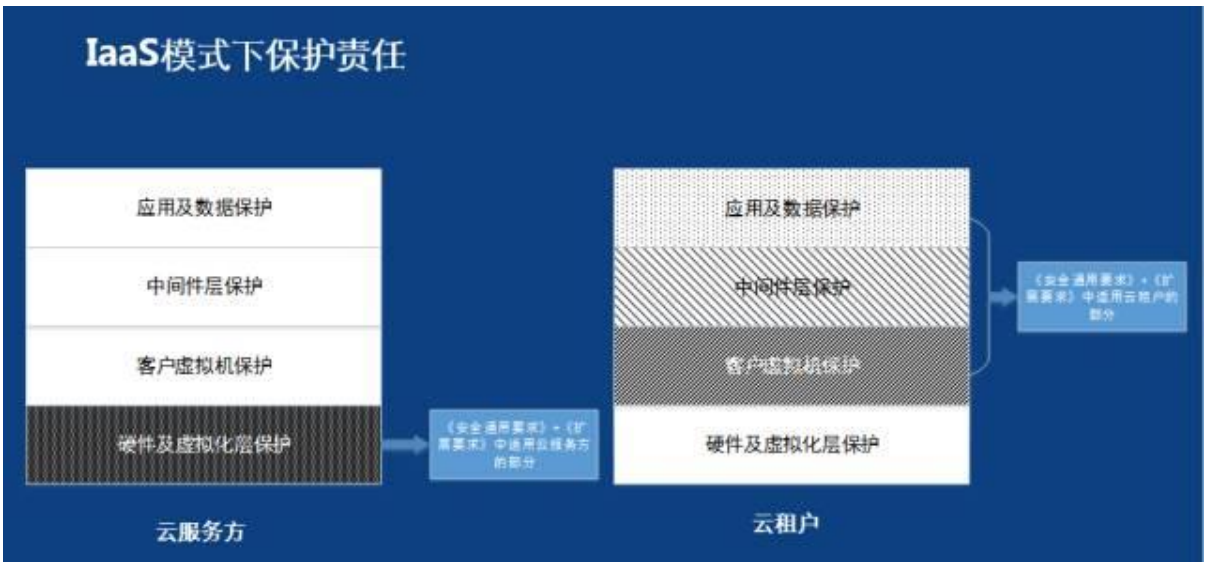


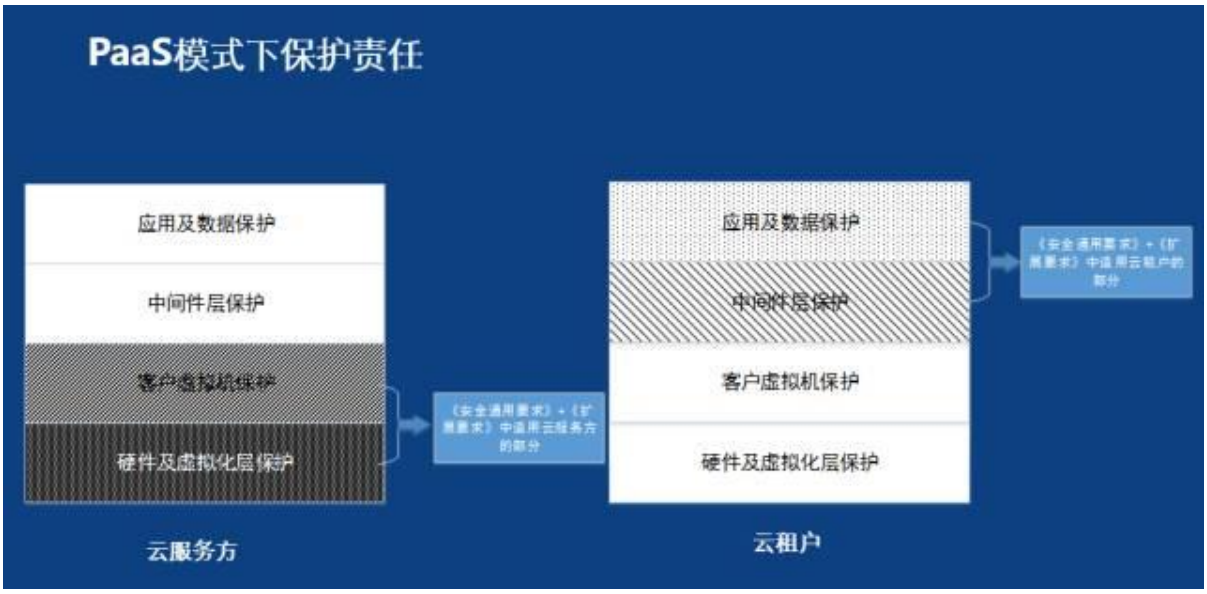
（二）测评指标与测评对象选择

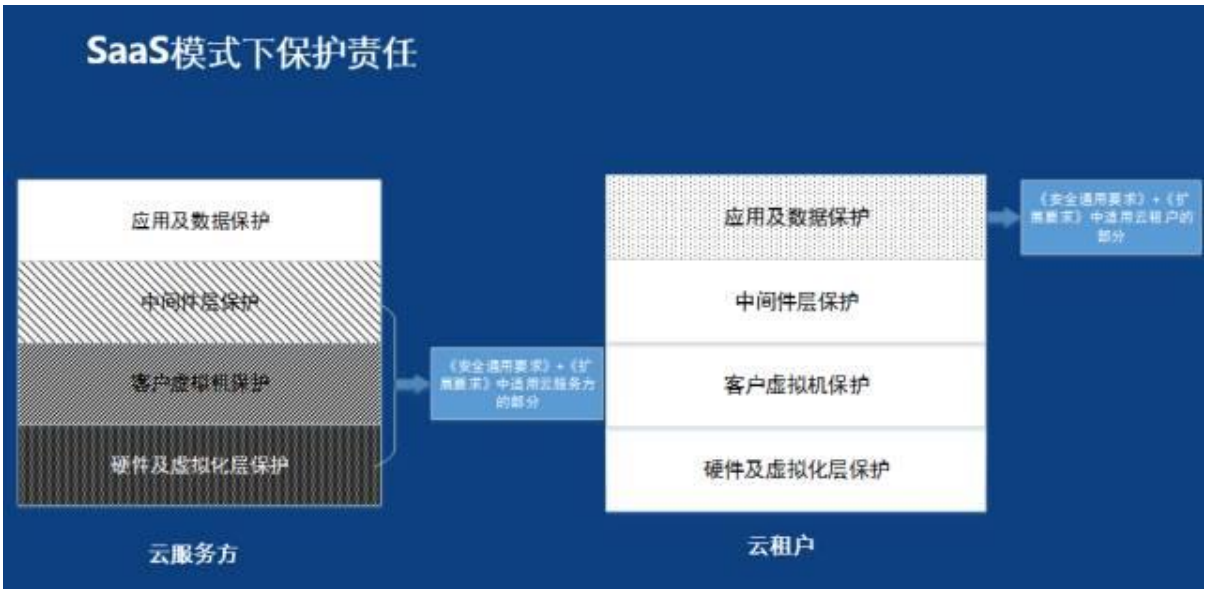
下面我们再来看看在应用新标准过程中如何确定测评指标和测评对象。

首先对云计算系统进行测评时应同时使用安全通用要求部分和云计算安全扩展要求部分的相关要求。不能只是用云计算安全扩展要求。

在这个过程中根据云上系统的责任分担不同，要对安全通用要求和云计算安全扩展要求做拆分，抽取条款形成适用于云服务商和云服务客户的安全保护需求。


IaaS模式下保护责任
应用及数据保护
中间件层保护
客户虚拟机保护
硬件及虚拟化层保护
云服务方
应用及数据保护
中间件层保护
硬件及虚拟化层保护
云租户


PaaS模式下保护责任
应用及数据保护
中间件层保护
硬件及虚拟化层保护
云服务方
应用及数据保护
中间件层保护
客户虚拟机保护
硬件及虚拟化层保护
云租户


SaaS模式下保护责任
应用及数据保护
中间件层保护
客户虚拟机保护
硬件及虚拟化层保护
云服务方
应用及数据保护
中间件层保护
客户虚拟机保护
硬件及虚拟化层保护
云租户

这时我们要考虑几方面因素，首先要确定被测云计算系统是云服务商的云计算平台还是云服务客户的业务应用系统。其次还要确定被测系统使用哪种服务模式，以此来确定保护责任。再次，我们还要根据保护责任的不同选择不同的对象，这里面就包括云计算系统较传统系统引入的新的测评对象类别。

举例说明，我们现在要测一个云计算平台，这个云计算平台提供 IaaS 服务，那么根据保护责任模型，我们应该使用 IaaS 模式下的保护责任中对应云服务商的部分。这时我们就可以从标准中寻找使用 IaaS 模式下的保护责任中对应云服务商的要求条款。然后我们参考标准附录中“云服务商与云服务客户的责任划分表”中给出的参考，找到潜在的安全组件，在根据标准附录中“云计算平台及云服务客户业务应用系统与传统信息系统保护对象差异表”中云计算系统保护对象举例，确定这个提供 IaaS 服务的云服务平台的测评对象。这样，测评指标和测评对象就确定了，接下来就是编制测评方案和作业指导书。后面的测评流程与传统系统测评是一致的。

表C.1　IaaS 模式下云服务方与云租户的责任划分

层面	安全要求	安全组件	责任主体
物理和环境安全	物理位置选择	数据中心及物理设施	云服务方
网络和通信安全	网络结构、访问控制、入侵防范、安全审计	物理网络及附属设备、虚拟网络管理平台	云服务方
		云租户虚拟网络安全域	云租户
设备和计算安全	身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制、镜像和快照保护	物理网络及附属设备、虚拟网络管理平台、物理宿主机及附属设备、虚拟机管理平台、镜像等	云服务方
		云租户虚拟网络设备、虚拟安全设备、虚拟机等	云租户
应用和数据安全	安全审计、资源控制、接口安全、数据完整性、数据保密性、数据备份恢复	云管理平台(含运维和运营)、镜像、快照等	云服务方
		云租户应用系统及相关软件组件、云租户应用系统配置、云租户业务相关数据等	云租户

表D.1　云计算平台及云租户业务应用系统与传统信息系统保护对象差异

层面	云计算平台及云租户业务应用系统保护对象	传统信息系统保护对象
物理和环境安全	机房及基础设施	机房及基础设施
网络和通信安全	网络结构、网络设备、安全设备、虚拟化网络结构、虚拟网络设备、虚拟安全设备	传统的网络设备、传统的安全设备、传统的网络结构
设备和计算安全	网络设备、安全设备、虚拟网络设备、虚拟安全设备、物理机、宿主机、虚拟机、虚拟机监视器、云管理平台、数据库管理系统、终端、存储	传统主机、数据库管理系统、终端
应用和数据安全	应用系统、云应用开发平台、中间件、云业务管理系统、配置文件、镜像文件、快照、业务数据、用户隐私、鉴别信息等	应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息等
安全建设管理	云计算平台接口、云服务商选择过程、SLA、供应链管理过程等	N/A

（三）云计算系统测评报告编制

云计算系统测评报告编制与传统系统大体一致，唯一需要注意的地方是如何处理云计算安全扩展要求。

根据云计算系统技术特点和试点经验，我们发现云计算系统保护措施通常是以系统整体能力体现的，某一项安全措施通常需要多个系统组件共同作用，而且这些系统组件通常以软件形式出现，贯穿整个云计算系统的各部分。因此，我们将云计算安全扩展要求作为全局要求对待，类似安全管理的要求。这些要求不落到具体某一个对象上。因此在报告结构上需要将这部分等同于全局测评，各测评项不再重复对应一个或多个测评对象。具体可参考最新版测评报告模板。

（四）报告打分

云计算系统打分方法与传统系统一样，需要注意的是，在对云服务客户业务应用系统测评时打分是不需要与云计算平台的单项得分结果共同计算，只需将云服务客户业务应用系统侧可测评项打分后带入公式计算，云服务客户业务应用系统侧不可测项做“N/A”处理。新版测评报告打分公式是支持这种处理方式的。

那么是否完全不考虑云平台的得分结果呢？也不是，我们在做云服务客户业务应用系统测评前首先就要看云计算平台是否完成等级测评，然后索要云平台测评报告结论盖章页。在我们出具云服务客户业务应用系统报告时，将云平台测评得分一并放在最终得分一栏。如：云服务客户业务应用系统测评得分为 85 分，云计算平台得分为 90 分，则云服务客户业务应用系统等级测评报告得分栏填写“（85,90）”。

来源：公安部信息安全等级保护评估中心　　张振峰

加入群聊

微信群免费共享安全行业资料、法律法规、等保相关标准、行业标准及建设方案等，为了【网络安全 Cyber Security】微信群管理，想进群的朋友先加我好友，我拉你们进群，微信二维码如下：

网络安全 CyberSecurity

欢迎扫描关注网络安全公众号，及时了解更多网络安全知识