国家云计算安全等级保护测评标准解读

（来源：国家信息中心网站 作者：禄凯 高亚楠 章恒）

引言

云计算作为广泛应用的新技术，越来越深入的影响着社会生活的各个领域。全国各地政务云、金融云、教育云等建设的如火如荼，越来越多的云计算系统承担着重要的基础性服务。

在高速发展的同时，安全隐患和威胁也如影随形，如：不安全接口、服务中断、越权、滥用与误操作、共享技术漏洞和信息残留等问题时刻影响着云计算的健康发展。云计算信息系统应具备什么样的安全防护措施，如何通过等级保护测评工作去检查和验证安全措施的合规性和有效性，已经成为云计算系统建设者、运营者、监管者以及使用者所关心的重要问题。

等级保护工作作为国家网络安全法明确的重要制度，已在我国信息系统安全保驾护航中发挥着重要作用。为应对新技术、新应用发展所带来的安全问题，公安部网络安全保卫局组织开展了大规模的等级保护系列标准的修订。云计算等级保护系列标准作为安全通用要求之后的第二分册，标准编制开始至今，受到相关各方的高度广泛关注，收到了很多宝贵意见和建议。

由国家信息中心负责牵头编制的《网络安全等级保护测评要求 第 2 部分：云计算安全扩展要求》（以下简称“云计算测评要求”）作为云计算安全等级保护测评的实施依据备受瞩目。此文解读标准，希望作为云计算等级保护测评工作的实践指引，给大家提供指导和帮助，相关技术研讨和培训也将后续开展。

《网络安全等级保护测评要求 第 2 部分：云计算安全扩展要求》解读

根据全国信息安全标准化技术委员会2013年10月确定的国家标准制修订计划，本次研编云计算等保系列标准包括三个：《信息安全技术网络安全等级保护基本要求 第2部分：云计算安全扩展要求》（以下简称“云计算基本要求”）、《信息安全技术 网络安全等级保护测评要求第2部分：云计算安全扩展要求》、《信息安全技术 网络安全等级保护设计技术要求 第2部分：云计算安全扩展要求》（以下简称“云计算设计要求”）。

第二分册作为第一分册安全通用要求的扩展和补充，主要用以应对云计算技术所带来的威胁与风险，在测评实施中要以安全通用要求为基础，同时参考定级指南等相关标准，共同完成云计算安全等级保护的测评工作。

要点一：系统定级与管理职责划分

云计算服务带来了“云主机”等虚拟计算资源，将传统IT环境中信息系统运营、使用单位的单一安全责任转变为云租户和云服务商双方“各自分担”的安全责任，使得云计算环境下定级工作相对比较复杂。

云计算系统的定级对象在原有定级对象基础上进行了扩展，原有定级对象主要是信息系统和相关基础网络，而云计算将定级对象扩展为云服务商的云平台和云租户的应用系统。

云计算系统定级时，云服务商的云平台和云租户的应用系统应分别定级，云平台等级应不低于应用系统的安全保护等级。对于公有云，定级流程为云平台先定级测评，再提供云服务。对于私有云，定级流程为云平台先定级测评，再将已定级应用系统向云平台迁移。

云计算系统定级的重点在于定级对象管理职责的划分，职责的划分根据不同云计算服务模式采取不同划分方式。

（一） 对于 IaaS 基础设施服务模式，云服务商的职责范围包括虚拟机监视器和硬件，云租户的职责范围包括操作系统、中间件和应用等。

（二） 对于 PaaS 平台即服务的服务模式，云服务商的职责范围包括硬件、虚拟机监视器、操作系统和中间件，云租户的职责范围为应用。

（三）对于 SaaS 软件服务模式，云服务商的职责范围包括硬件、虚拟机监视器、操作系统、中间件和应用，云租户的职责范围包括部分应用职责及用户使用职责。

云计算服务模式以及角色的不同决定着定级对象的管理职责不同，从而决定着定级的系统范围的不同。

要点二：云计算系统保护对象的扩展

由于虚拟化等新技术的应用，IaaS/PaaS/SaaS 按需服务模式的引入，相对于传统信息系统，云计算系统的保护对象有所增加。云计算系统的保护对象与传统信息系统保护对象对照如下表所示，其中加黑的对象为云计算系统所特有的保护对象：

层面	云计算系统保护对象	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、综合网管系统、**虚拟化网络结构、虚拟网络设备、虚拟安全设备、虚拟机监视器、云管理平台**	网络设备、安全设备、网络结构、综合网管系统
设备和计算安全	主机、数据库管理系统、终端、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、网络策略控制器**	主机、数据库管理系统、终端、中间件、网络设备、安全设备

应用和数据安全	应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息、**云应用开发平台、云计算服务对外接口、云管理平台、镜像文件、快照、数据存储设备、数据库服务器**	应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息等
安全管理机构和人员	信息安全主管，相关文档	信息安全主管、相关文档
安全建设管理	系统建设负责人、**服务水平协议、云计算平台、供应商资质**、相关文档、**相关资质、相关检测报告**	系统建设负责人、记录表单类文档
安全运维管理	安全管理员、相关文档、**运维设备、云计算平台、第三方审计结果**	系统管理员、网络管理员、数据库管理员、安全管理员、运维负责人、相关文档

云计算系统保护对象除包含传统信息系统保护对象外，还包含云计算系统特有保护对象。在进行云计算系统等级保护测评时，针对不同保护对象实施不同测评内容，既要对云计算系统特有保护对象依据云安全测评要求进行测评，也要对云计算系统选取安全通用要求相关指标进行测评。

要点三：与其他标准间关系

云计算等级测评参照通用测评要求的修订思路进行了修订，技术框架同样调整为单项测评和整体测评。同时依据 GB/T22239.1 标准的文本架构，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全策略和管理制度、安全管理机构和人员、安全建设管理、安全运维管理等八个层面开展测评实施工作。同时，与其他测评要求统一编码，与通用测评要求的级差变化情况保持一致。

本标准与云计算基本要求一一对应，标准单项测评内容与云计算基本要求中条款相对应，针对云计算基本要求中每一条款，云测评要求给出具体测评对象，测评实施和结果判定。本标准与云计算设计要求相融合，结合云计算设计要求中技术实现细节，并结合实际测评情况给出云计算测评的具体实施内容。

另外，本标准同样适用于云计算系统建设时作为参考。在术语定义、云计算服务模式等方面，云计算基本要求、云计算测评要求和云计算设计要求保持了思想的一致性。

要点四：如何编制作业指导书

本标准应与通用测评要求配合使用，对使用云计算相关技术的平台及应用系统，应根据实际情况，对应通用测评要求和云计算测评要求，抽取相关测评要求，并按照这些测评要求编制测评指导书。

对于云计算系统中特有的保护对象：云管理平台、虚拟机监视器、虚拟网络设备和虚拟安全设备为例抽取测评项方式如下：

对于云管理平台，应从通用测评要求的应用和数据层面抽取测评项，并从云计算测评要求的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全层面抽取测评项。

对于虚拟机监视器，应从通用测评要求的设备和计算安全层面抽取测评项，并从云计算测评要求的网络和通信安全、设备和计算安全层面抽取测评项。

对于虚拟网络设备和虚拟安全设备，应从通用测评要求的网络和通信安全层面抽取测评项，并从云计算测评要求的网络和通信安全、设备和计算安全层面抽取测评项。

要点五：具体测评指标选取

云计算测评要求主要针对云计算技术和管理中的特殊性提出要求，相对于传统信息系统，测评单元和测评项均有所新增，云计算系

统的测评单元与传统信息系统测评单元对照如下表所示，其中加黑的测评单元为云计算系统所特有的测评单元：

层面	云计算系统测评单元	传统信息系统测评单元
物理和环境安全	物理位置的选择	物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护
网络和通信安全	网络架构、访问控制、入侵防范、安全审计	网络架构、通信传输、边界防护、访问控制、入侵防范、恶意代码防范、安全审计、集中管控
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**	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
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、剩余信息保护	身份鉴别、访问控制、安全审计、软件容错、资源控制、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护
安全策略和管理制度	N/A	安全策略、管理制度、制定和发布、评审和修订
安全管理机构和人员	授权和审批、人员录用	岗位设置、人员配备、授权和审批、沟通和合作、审核和检查、人员录用、人员离岗、安全意识教育和培训、外部人员访问管理
安全建设管理	安全方案设计、测试验收、**云服务商选择、供应链管理**	定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试

		验收、系统交付、等级测评、服务供应商选择
安全运维管理	环境管理、**监控和审计管理**	环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理

云计算测评工作的开展首先要明确测评对象是云服务商还是云租户，对于同一条测评实施内容，针对云服务商与云租户具有不同的含义，部分条款仅适用于云服务商，而部分条款仅适用于云租户。

例如测评实施中：“应检查云服务商的网络边界设备或虚拟化网络边界设备，查看安全保障机制、访问控制规则或访问控制策略等”仅适用于云服务商，而不适用于云租户。

其次，应明确测评的云计算系统的服务模式，根据云计算系统的服务模式进行职责划分。明确测评对象和服务模式后，云计算测评要求的条款就可以进行相应剪裁以适用于不同的云计算系统。根据裁剪后的结果形成作业指导书，从而指导云计算测评工作的实施。

要点六：测试手段与工具

云计算系统的安全测评对测评手段、测评工具提出了新的要求，除主机扫描、数据库扫描、应用扫描、流量分析等一些传统测试工具外，根据实际情况，需要配置专用测试工具，如：针对虚拟化漏洞的安全扫描工具、云计算系统安全审计工具、云端移动 APP 应用的安全检测工具等。另外，测试人员也应具备相应的能力，如：针对虚拟化、云平台的安全渗透测试能力等。以上可以通过购买相应测试工具，选派人员参加网络攻防培训来解决。