**意见汇总处理表**

标准项目名称：《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》

承办人：张振峰 共 14 页

标准项目负责起草单位：公安部第三研究所 电 话：18611127109 2016 年 9 月 28日填写

| 序号 | 标准章条编号 | 意见内容 | 提出单位 | 处理意见 | 备注 |
| --- | --- | --- | --- | --- | --- |
|  | 全文 | 因22239.2是22239的一部分，文本中“本标准”应改为“本部分” | 国家信息中心 | 采纳 |  |
|  | 8.2.2.3 | 建议在术语和定义中给出“社会化云服务”的定义 | 国家信息中心 | 未采纳。与中网办发文【2015】14号及31168保持一致 |  |
|  | 引言 | 建议加入一句话，说明使用时需与22239.1同时使用 | 国家信息中心 | 采纳 |  |
|  | 全文 | 建议在术语和定义中给出“云租户”的定义；建议根据不同的部署模式和商业模式分开写标准内容。 | 中科院信工所 | 采纳 |  |
|  | 全文 | 私有云和公有云的适用条款应该有描述。不同的部署模式应如何使用标准，要考虑商业模式。 | 中科院信工所 | 未采纳。私有云和公有云的威胁场景不适合在在本标准区分，只有极个别条款会区分公有云和私有云。私有云也有多租户的概念。 |  |
|  | 全文 | 建议本部分名称改为“指南” | 中软信息系统工程公司 | 未采纳。本部分作为22239的一部分，名称需保持一致 |  |
|  | 全文 | 建议加入SLA相关的条款 | 中国信息安全认证中心 | 采纳 |  |
|  | 6.2.1.1、7.2.1.1、8.2.1.1 | 条款中不涉及审批内容，建议标题去掉“审批” | 国家信息技术安全研究中心 | 采纳 |  |
|  | 6.1.1、7.1.1、8.1.1 | 建议细化明确对于云租户的数据和云平台管理运行数据处境的要求 | IBM | 采纳 |  |
|  | 2规范性引用文件 | 应包括 GB/T 32400-2015 云计算概览与词汇 和 GB/T 32399-2015 云计算参考架构 | IBM | 未采纳。概念上保持一致，不直接引用非安全标准 |  |
|  | 3术语和定义 | 应参照 GB/T 32400-2015 云计算概览与词汇 和 GB/T 32399-2015 云计算参考架构 | IBM | 部分采纳。保持一致性，但主要术语和定义以31167和31168为准 |  |
|  | 4.1云计算平台构成 | IaaS, PaaS, SaaS 是NIST的老提法。这些术语已在GB/T 32400-2015 云计算概览与词汇中被规范。云能力类型有3个基础设施（Infrastructure），平台（Platform）和应用（Application）。7个云服务类别除了IaaS，PaaS，SaaS还有DaaS, NaaS, CaaS等。 在GB/T 32400-2015 云计算概览与词汇中，描述了7个云服务类别与3个云能力类型之间的关系。 | IBM | 部分采纳。与GB/T31167保持一致 |  |
|  | 6.1.1.1，7.1.1.1，8.1.1.1物理位置选择 | 除了党政及涉及国家安全部门的云计算机房须位于中国境内外，用于纯商用云计算的机房不一定要求必须位于中国境内。 | IBM | 未采纳。1.与31168把持一致。  2等保二级以上的系统涉及社会秩序、公众利益，不是纯商业问题。 |  |
|  | 附录C不同交付模式的安全管理责任主体 | 和4.1相同，IaaS, PaaS, SaaS 是NIST的老提法。这些术语已在GB/T 32400-2015 云计算概览与词汇中被规范。云能力类型有3个基础设施（Infrastructure），平台（Platform）和应用（Application）。7个云服务类别除了IaaS，PaaS，SaaS还有DaaS, NaaS, CaaS etc. 在GB/T 32400-2015 云计算概览与词汇中，描述了7个云服务类别与3个云能力类型之间的关系。 | IBM | 部分采纳。与GB/T31167保持一致 |  |
|  | 6.1.2.4， 7.1.2.4访问控制  8.1.2.3边界防护 | 在通用要求的网络和通信安全部分的6.1.2.5，7.1.2.5，8.1.2.5均提到应在关键网络节点处监视、检测、防止或限制从外部或内部发起的网络攻击行为。  关键网络节点在物理网络中可以从物理上与其它节点区隔，但在云环境的虚拟网络中这种区隔及防护手段将失效  在云计算安全扩展要求中6.1.2.4，7.1.2.4，8.1.2.3中仅提到应能检测并阻断云租户对外的攻击行为，并能记录攻击类型、攻击时间、攻击流量；  需要针对云计算虚拟网络特点检测、防止或限制从外部或内部发起的网络攻击行为。建议增加对云计算虚拟网络的检测。 | IBM | 采纳。其中关键网络节点包括互联网边界、关键第三方边界和虚拟网络的关键节点 |  |
|  | 6.1.2.5 | 建议增加：  6.1.2.5 应在跨网段通讯节点处监视网络攻击行为，其中包括软件定义网络上的虚拟网段以及网络节点。跨网段通讯包括横跨私有网段的通讯以及不同云租户间的通讯。 | IBM | 未采纳。网络和通信安全中，“网络结构”中的e条和入侵防范的a条已满足这样的需求 |  |
|  | 7.1.2.5 安全审计  8.1.2.4 安全审计 | 建议增加：  d) 如果以上a)、b)、c)项在虚拟网络上，包含软件定义的网络，则应在跨私有网段通讯节点实行相同的监测及监控。 | IBM | 未采纳。在入侵防范和网络结构中已经包含。 |  |
|  | 8.1.2.3　入侵防范 | 建议增加：  c) 在虚拟网络上，包含软件定义的网络，应保证跨越私有网段的访问和数据流通过边界防护设备提供的受控接口进行通信。跨私有网段的通讯包含云租戶內部的通信，以及來自互联网的连接。 | IBM | 未采纳。安全通用要求已经涵盖此内容，对四级虚拟网络也要落实安全通用要求。 |  |
|  | 6、7、8章 | 按照31167、31168和22239.2中定义，IAAS的云计算中，网络安全都由运营商来承担。这个在实施中存在问题，较为难以贯彻。  1、 网络防火墙作为网络边界访问控制和安全路径保证的设备，配置比较复杂，较难实现自动化的由租户提要求，运营商实现方式，标准化接口难以实现。  2、 现有一些政务云项目中，很多情况是租户网络边界的访问控制功能由租户自行配制，由租户自行选购产品。与标准中的责任划分不同。  建议调整如下：  1、 建议强制租户虚拟边界防护要求，测评要求。  2、 能够将云服务商和用户在网络安全部分责任再分离，并基于不同责任做要求。 | 山石网科 | 部分采纳。1.关于边界的防护要求已有相关条款，有关测评的要求不在本标准考虑范围。2.责任划分在附录中给出参考。 |  |
|  | 7.1.2.2 | b和e项，建议可以只定义要求能力，而不规定实现方式，现在“设备”一词类似限制为硬件实现方式。  建议b、e条修改要求描述。建议修改为：  b) 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；  e) 应在不同等级的网络区域边界部署访问控制机制，并设置访问控制规则。 | 微软 | 采纳 |  |
|  | 7.1.2.3 | b条是针对用户的条目，并不是针对云服务商的条目。云服务商是没有权限访问用户VM或者数据的。  建议重新考虑是否包含b条的要求，或者修改要求描述。建议修改为：  针对云环境下的物理机等属于云服务商控制的设备远程执行特权命令进行限制，采取严格的保护措施并进行审计。 | 微软 | 未采纳。与管理员的管理范围和权限职责划分有关，并不特质某一设备和软件产品。云租户和云服务商执行特权命令均存在被审计需求。 |  |
|  | 7.1.3.2 | a应该明确远程管理是云服务商管理物理机等可控设备，不是虚拟机、存储账号等信息，不要与云租户管理设备混淆。  建议a条修改要求描述。建议修改为：  当进行远程管理物理机等属于云服务商控制的设备时，防止远程管理设备同时直接连接其他网络。 | 微软 | 未采纳。与管理员的管理范围和权限职责划分有关，并不特质某一设备和软件产品。云租户和云服务商执行特权命令均存在防止远程管理设备同时直接连接其他网络。 |  |
|  | 7.1.3.6 | f和g有冲突，g公有云环境下，不存在设置优先级和资源紧张的情况，而且VM资源之间都是相互隔离的，与f 冲突。  建议g条明确适用范围是公有云还是私有云。 | 微软 | 采纳。去掉g) |  |
|  | 7.1.4.6 | a条是针对云租户的要求，不是云服务商的要求。  建议将a条删除。 | 微软 | 未采纳。本部分关注整个云计算环境下的安全，包括云服务商和云租户两方面的要求。 |  |
|  | 全文 | 标准主要是针对IaaS和PaaS提出各种安全管理要求，比如虚拟机和虚拟网络的要求，等等。但是这些在SaaS当中并不适用，也并非面向客户需要公开并给予管理能力的项目。 希望标准能够特别指出这些项目仅针对IaaS和PaaS有要求。 | 微软 | 部分采纳。责任划分在附录中给出参考。标准关注全集，在使用时可根据实际情况进行“不适用”处理。 |  |
|  | 3.4 | 建议将“云服务方 cloud service provider”改为云服务商，云服务商的叫法现在已经成为共识。 | 中国电子技术标准化研究院 | 未采纳。因为在私有云情况下，特别是四级系统采用的内部私有云，不能引入云服务商，因此本部分统一采用云服务方的说法。 |  |
|  | 6.1.2.3 a) | 应实时监视云服务远程连接；云服务是服务概念，对象应为平台。  修改建议：改为应实时监视云计算平台的远程访问。 | 中国电子技术标准化研究院 | 采纳 |  |
|  | 6.1.2.3 b) | 应对远程执行特权命令进行限制，采取严格的保护措施。  修改建议：采取严格的保护措施这句话没有意义，可删除。 | 中国电子技术标准化研究院 | 采纳 |  |
|  | 6.1.2.4 | 改为：应能监测到云租户的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。 | 中国电子技术标准化研究院 | 采纳 |  |
|  | 6.1.3.3 b) | 应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；  修改建议：这条要求建议细化为具体的做法，或者删除，不然很难理解也很难实现，原则上云服务商在用户不知情的情况下不能对云租户系统和数据有任何操作，如果是日常的运维和配置变更在不在此范围内很难界定。 | 中国电子技术标准化研究院 | 未采纳。这里对能力提出要求，具体如何实现在设计要求中给出。云计算安全很大程度上是信任问题，如何让云租户信任云服务方，而这条要求的能力就是提升云服务方操作的透明度，也在一定程度上对云服务方的操作施加压力，不能随便操作，因此还是有必要保留的。 |  |
|  | 6.1.3.4 | 建议对“宿主机”进行定义 | 中国电子技术标准化研究院 | 采纳。 |  |
|  | 6.1.3.5 b) | 建议对“虚拟机监视器”进行定义 | 中国电子技术标准化研究院 | 采纳 |  |
|  | 6.1.3.5 a) | 应提供自动保护功能，当故障发生时自动保护所有状态，保证系统能够进行恢复；  这一条看不懂，故障是什么故障？如果是云平台整体故障，是不是要求有点高？ | 中国电子技术标准化研究院 | 采纳。删除本条要求 |  |
|  | 6.1.3.5 d) | 应保证虚拟资源的业务处理能力具备冗余空间，满足业务高峰期需要；  这个概念有点问题，虚拟资源的冗余纯粹靠租户购买的资源决定，属于用户的责任范围，建议删除。 | 中国电子技术标准化研究院 | 采纳 |  |
|  | 6.1.4.1 b) | 应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  修改意见类似第5条。 | 中国电子技术标准化研究院 | 未采纳。这里对能力提出要求，具体如何实现在设计要求中给出。云计算安全很大程度上是信任问题，如何让云租户信任云服务方，而这条要求的能力就是提升云服务方操作的透明度，也在一定程度上对云服务方的操作施加压力，不能随便操作，因此还是有必要保留的。 |  |
|  | 6.1.4.5 a) | 云租户应在本地保存其业务数据的备份；  修改建议：这个标准整体是针对云服务商还是云租户？是不是需要明确，目前来看绝大部分是针对云服务商。假如双方都能用，那么云服务商做合规时是不是就可以认为这条不适用？  另外，作为二级要求，数据是不断变化的，如果在本地保存备份，岂不是要保持一种混合云的架构，这个代价是不是太大了？  建议删除。 | 中国电子技术标准化研究院 | 部分采纳。改为从第三级开始要求。针对本条，对云服务商做不适用处理。 |  |
|  | 6.2.2.1 a) | 应保证云服务方对云租户业务数据和隐私信息的访问或使用必须经过云租户的授权，授权必须保留相关记录。  建议：隐私的概念是针对个人信息主体的，这里和业务数据并称不合适，建议删除隐私。 | 中国电子技术标准化研究院 | 采纳 |  |
|  | 6.2.2.2 a) | 应确保云服务商的选择符合国家的有关规定；  建议改为：应确保选择云服务商的过程符合国家有关规定。 | 中国电子技术标准化研究院 | 采纳。同时将后面供应链管理a)也做相同修改 |  |
|  | 6.2.2.2 b) | 应选择有资质的云服务商，其所提供的云平台应具备与信息系统等级相应的安全保护能力；  建议：有资质这几个字容易误解，可改为应选择安全合规的云服务商。 | 中国电子技术标准化研究院 | 采纳 |  |
|  | 6.2.2.3 b) | 云服务方应确保供应链安全事件信息或威胁信息能够及时传达到云租户。  建议统一写法，不加主语，删掉云服务方。  如果说整体只针对云租户的内容不多，是不是考虑把云租户的要求单独列出？或者给云服务商提出不适用项的建议？不然显得很乱。 | 中国电子技术标准化研究院 | 采纳 |  |
|  | 7.1.2.1 f) | 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；  这句话不通顺。首先，这一部分是网络隔离的内容，其次，要和后面的要求g)匹配。所以，可以改为：  应根据承载的业务系统安全保护等级划分不同安全级别的资源池区域，并实现资源池之间的网络隔离。 | 中国电子技术标准化研究院 | 部分采纳。为体现出不同等级对抗威胁能力的不同，在措施上高级别系统有所加强，在第三级要求实现资源池之间网络隔离，在第四级要求实现资源池之间物理隔离。 |  |
|  | 7.1.2.1 g) | 应提供开放接口，允许接入第三方安全产品，实现云租户的网络之间、安全区域之间、虚拟机之间的网络安全防护；  这个要求有点离谱，且对公有云架构具有破坏性。实现这两个字不合适。网络之间四个字没有意义。  建议改为：应提供开放接口或开放性安全服务，允许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。加强云租户虚拟机之间、安全区域之间的网络安全防护能力。 | 中国电子技术标准化研究院 | 采纳 |  |
|  | 7.1.2.2 d) | 应依据安全策略控制虚拟机间的访问；  这句话写的很怪，云服务商当主语不合适，租户当主语也很怪。  建议改为，应允许云租户设置不同虚拟机之间的访问控制策略。  另外，这一条很基本，是VPC和隔离的基本条件。建议二级要求也做到。 | 中国电子技术标准化研究院 | 采纳 |  |
|  | 7.1.2.2 e) | 应在不同等级的网络区域边界部署访问控制设备，设置访问控制规则。  部署设备还是太落后不适用于所有云平台  建议改为：应在不同安全等级的网络区域边界部署访问控制设备或提供额外的访问控制机制，以设置区域间的访问控制规则。 | 中国电子技术标准化研究院 | 采纳。与微软建议相同，统一采用“机制”一词。 |  |
|  | 7.1.2.4 b） | 应对散播到互联网的有害信息进行实时监测和告警。  这条太离谱，原则上IaaS平台，云服务商不能监测租户业务数据流，最多也就给用户提供类似的功能模块便于租户自行筛选有害信息。  建议删除，或改为：应向云租户提供互联网发布内容监测功能，便于云租户对其发布内容中的有害信息进行实时监测和告警。 | 中国电子技术标准化研究院 | 采纳 |  |
|  | 7.1.3.4 d) | d) 应保证虚拟机仅能迁移至相同安全等级的资源池。  建议改为：应保证虚拟机仅能迁移至不低于自身所承载业务系统安全等级的资源池。 | 中国电子技术标准化研究院 | 未采纳。如果能迁移到更高等级资源池，就破坏了另一个原则，即“分等级划分资源池”。 |  |
|  | 7.1.4.5 d) | d) 应采用加解密技术保证网络策略控制器和网络设备（或设备代理）之间网络通信的保密性。  不通顺，建议改为：应对网络策略控制器和网络设备（或设备代理）之间网络通信进行加密。 | 中国电子技术标准化研究院 | 采纳 |  |
|  | 7.1.4.6 d) | d) 应保证云租户业务及数据能移植到其他云计算平台或者迁移到本地信息系统。  写法不科学，建议改为：为云租户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。 | 中国电子技术标准化研究院 | 采纳 |  |
|  | 7.2.2.1 | 云计算平台应开放接口，允许接入第三方安全产品，支持异构方式对云租户的网络、主机、应用、数据层的安全措施进行实施。  建议改为：云计算平台应提供开放接口或开放性安全服务，允许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，支持异构方式对云租户的网络、主机、应用、数据层的安全措施进行实施。 | 中国电子技术标准化研究院 | 采纳 |  |
|  | 7.1.4.5 c) | c) 提供或支持云租户部署密钥管理解决方案，确保仅云租户能对其数据进行解密；  目前该句写法和同一条中的b)的意思基本重合。  建议改为：支持云租户部署密钥管理解决方案，确保云租户自行实现数据的加解密过程； | 中国电子技术标准化研究院 | 采纳。同时删除原b）条 |  |
|  | 7.2.2.3 g) | g) 应与云服务商的可接触到云租户数据的员工签订保密协议，并进行背景调查；  做背景调查的应该是云服务商而不是租户。这种写法有点歧义，租户做不了也没有可实施性。  建议改为：应对可能接触到云租户数据的员工进行背景调查，并签署保密协议。 | 中国电子技术标准化研究院 | 采纳 |  |
|  | 7.2.2.3 h) | 建议对“第三方”进行定义。 | 中国电子技术标准化研究院 | 部分采纳。单独对“第三方”不好定义，因为这是在特定语境下的第三方，别的条款也有第三方，但是不是同一类第三方。本条所指第三方是云租户以外的政府监管部门、行业主管部门、行业协会和独立机构等。如果对其定义不能用“等”，因此会带来穷举问题。具体可在未来的标准解读中细化。 |  |
|  | 附录 C.1 | 云服务的三种交付模式  国际通用说法为service model  建议改为“服务模式” | 中国电子技术标准化研究院 | 采纳 |  |
|  | 8 | 四级的要求和三级要求太相似，所谓的告警和阻断，从技术上来讲一般不会区别实施。而且，盲目阻断本身带来的弊端很多，影响可用性，建议统一改为告警后及时处理，或直接阻断异常行为。  另外，四级的系统是否能够部署在云平台是否还需要再做考虑？ | 中国电子技术标准化研究院 | 采纳。  另讨论：我们认为，从应对威胁的角度看，四级系统如果上云，则宜采用本组织机构自建的内部私有云，并由本组织机构运营管理，也就是避免使用社会化云服务。能否上云可能更多的是行政监管的要求，不宜写入技术要求。从另一个角度看，如果某行业有特殊需求，可针对本行业制定相应的管理规定或标准，而作为国家基线要求，可能不宜直接限制四级系统上云。 |  |