细数云安全之七宗罪防范各种安全漏洞思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E7_BB_86_E6_95_B0_E4_BA_91_E5_c101_644555.htm IDG集团Computerworld网站近日撰文称，安全专家表示，选择云计算的企业可能熟悉多重租赁(multi-tenancy，多个公司将其数据和业务流程托管存放在SaaS服务商的同一服务器组上)和虚拟化等概念，但这并不表示他们完全了解云计算的安全情况。云安全联盟(CSA)执行董事Jim Reavis认为，云计算其实就是将各种技术集中在一起创造出一种具有独特管理制度的应用程序。 这是计算机时代的新篇章，虽然这一切听起来很熟悉，但只要深入了解就会发现不同之处。 企业运用云计算的速度通常都让安全专家感到惊讶，安全专家Reavis认为，企业应该采取更加务实的做法，例如采用风险评估来了解真正的风险以及如何降低风险，然后再决定是否应该部署云计算技术。 云安全联盟与惠普公司共同列出了云计算的七宗罪，主要是基于对29家企业、技术供应商和咨询公司的调查结果而得出的结论。 1. 数据丢失/泄漏： 云计算中对数据的安全控制力度并不是十分理想，API访问权限控制以及密钥生成、存储和管理方面的不足都可能造成数据泄漏，并且还可能缺乏必要的数据销毁政策。 2. 共享技术漏洞： 在云计算中，简单的错误配置都可能造成严重影响，因为云计算环境中的很多虚拟服务器共享着相同的配置，因此必须为网络和服务器配置执行服务水平协议(SLA)以确保及时安装修复程序以及实施最佳做法。 3. 内奸： 云计算服务供应商对工作人员的背景调查力度可能与企业数据访问权限的控制力度有所不同，很多供

应商在这方面做得还不错，但并不够，企业需要对供应商进行评估并提出如何筛选员工的方案。 4. 帐户、服务和通信劫持：很多数据、应用程序和资源都集中在云计算中，而云计算的身份验证机制如果很薄弱的话，入侵者就可以轻松获取用户帐号并登陆客户的虚拟机，因此建议主动监控这种威胁，并采用双因素身份验证机制。 5.不安全的应用程序接口：在开发应用程序方面，企业必须将云计算看作是新的平台，而不是外包。在应用程序的生命周期中，必须部署严格的审核过程，开发者可以运用某些准则来处理身份验证、访问权限控制和加密。 6. 没有正确运用云计算：在运用技术方面，黑客可能比技术人员进步更快，黑客通常能够迅速部署新的攻击技术在云计算中自由穿行。 7.未知的风险：透明度问题一直困扰着云服务供应商，帐户用户仅使用前端界面，他们不知道他们的供应商使用的是哪种平台或者修复水平。 云服务供应商惠普公司的首席技术官Archie Reed认为，上述的云计算七宗罪虽然并不全面，但是都是非常重要的，它们能够指引大家如何正确运用云计算。 七宗罪说明了云安全状况变化非常快，安全技术人员必须了解影响他们工作的种种因素，包括政府法律和行业标准等，并且他们应该清楚这些因素是否被正确运用到风险评估方法中，评估方法是否定期修改。 毫无疑问的是，云计算确实给我们带来新的契机，但是这种新技术也意味着供应商的解决方案和技术也不断在发展。虽然企业可以信任云计算，但是并不能将所有责任都交付给云计算，企业必须对云计算中的数据或者程序进行必要的管理。 