云计算开源产业联盟
OpenSource Cloud Alliance for industRy,OSCAR

云 计 算 安 全 白 皮 书

（2018年）

云计算开源产业联盟

OpenSource Cloud Alliance for industry，OSCAR

2018年8月

版权声明

前　言

随着云计算的发展，云计算在应用过程中的安全问题也逐渐显露，这些安全问题已经成为制约云计算发展的关键因素之一。目前全球云计算安全服务市场保持强劲增长，我国的云计算安全市场也处于高速增长阶段，各组织也分别针对云计算安全问题出台相应政策、制定相关标准，云计算安全的重要性逐渐引起人们的关注。

本白皮书重点介绍了云计算安全的市场发展情况、安全风险、安全现状、政策环境和发展建议。白皮书首先梳理了国际、国内云计算安全市场的发展状况及热点，总结了当前云计算安全行业面临的主要风险，然后从当前的云计算用户数据安全、云计算安全行业服务能力、业务安全风控能力、安全责任和云计算安全人才等多个角度分别分析了云计算安全的发展现状，最后给出了云计算安全产业面临的政策环境及发展建议。

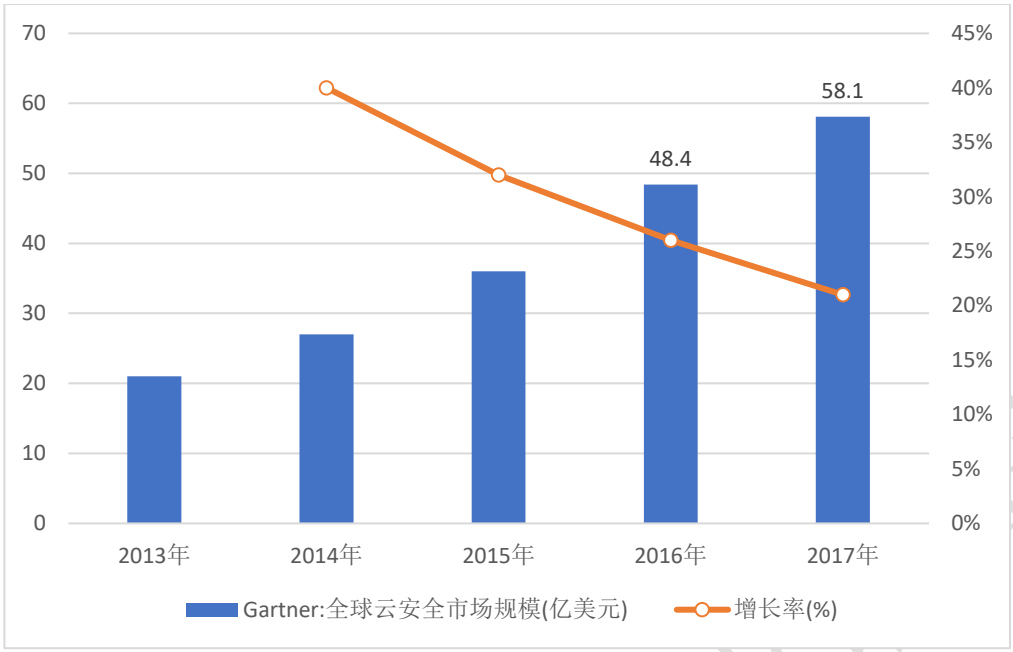
目 录

一. 云计算安全市场发展状况及分析

1.1、 全球云计算安全市场规模及发展趋势

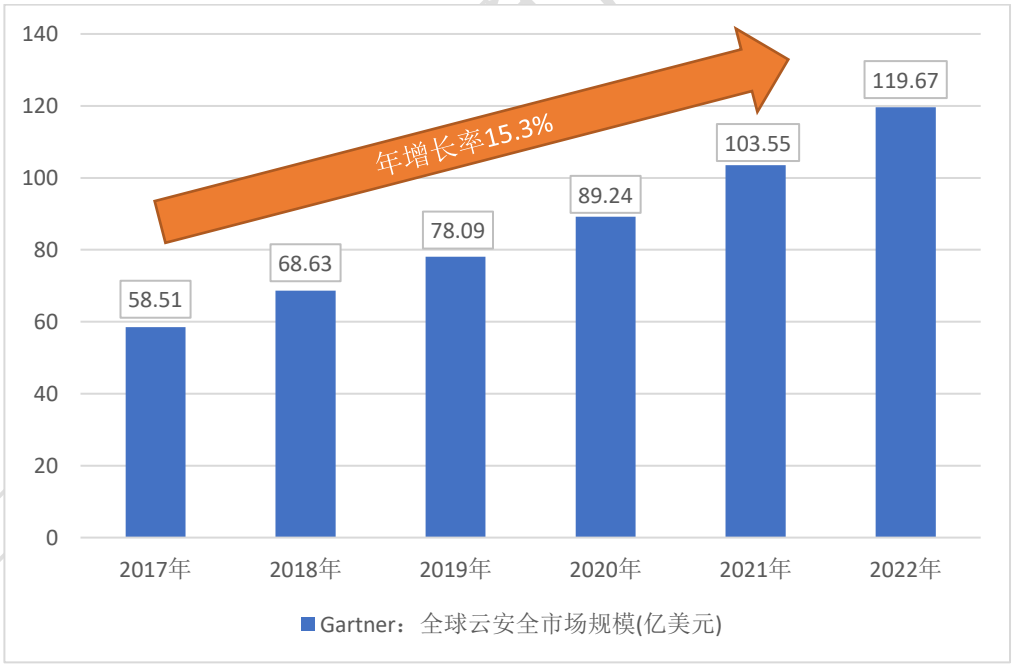
云计算不断发展，其采用的分布式计算和虚拟化技术带给云计算用户便捷的资源使用、低廉的运营成本是无所能及的，然而相应的安全性问题也随之进入了大家的视角。2017 年，知名云计算安全服务商 Cloudflare 被曝出泄露云计算用户 Https 网络会话中的加密数据长达数月，受影响的网站预计至少 200 万之多，其中涉及 Uber、1password、FastMail 等多家知名公司；2017 年，亚马逊 S3 云存储上的数据库配置错误，导致三台服务器下的数据可公开下载，造成严重的数据泄露；2017 年 1 月，IBM 云服务出现宕机事故，导致云计算用户无法管理自身的应用程序，添加或删除支持工作负载的云资源等等，这些安全问题给云计算用户、云计算服务商、甚至国家带来巨大的损失，云计算安全的重要性也随之不断上升。

众多企业业务纷纷上云，云计算安全需求迫切，潜在空间巨大，正在诞生新的市场蓝海。近几年，嗅觉敏锐的国际巨头纷纷开始收购布局云计算安全产业，2018 年初 McAfee 收购云计算安全公司 Skyhigh Network，使其扩大了产品组合，超越了传统的端点保护能力，将为 IaaS，PaaS 和 SaaS 服务提供全程安全保护。Gartner 发布的最新预测中也提出，云计算安全服务市场的增速将高于信息安全市场的总体增速，全球云计算安全服务将保持续持强劲增长势头，在 2017 年已达到 59 亿美元，相比 2016 年增长 21%，到 2022 年，云计算安全服务市场将达到 120 亿美元。



数据来源：Gartner

图 1 全球云计算安全市场规模增长情况（单位：亿美元，%）

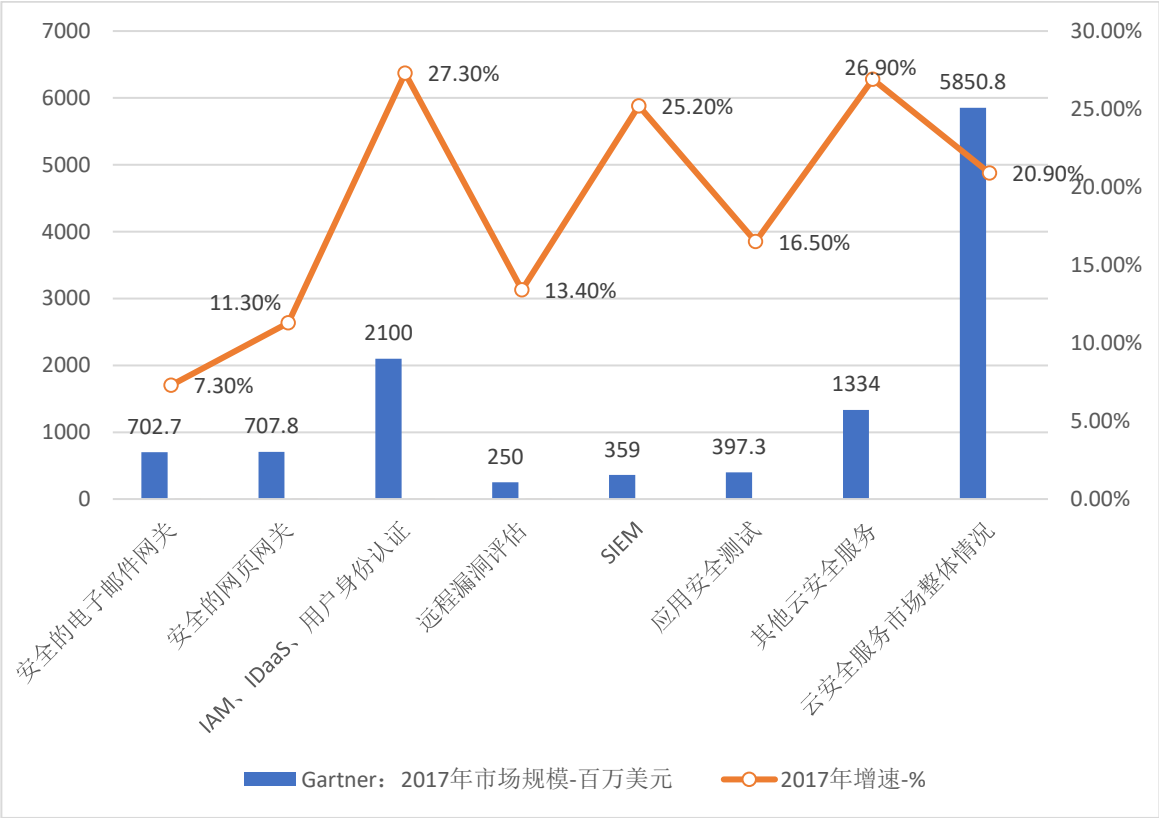


数据来源：Gartner

图 2 全球云计算安全前景预测（单位：亿美元）

Gartner 分析，电子邮件安全、web 安全以及身份识别与访问管理

（IAM）仍然是企业上云的三大优先考虑事项，这些优先事项的主流实现方法（包括 SIEM、IAM 技术以及新兴技术与服务）是云计算安全服务市场增长的主要组成部分。威胁情报、基于云的恶意软件沙箱、基于云的数据加密、端点保护管理等新兴服务，将是云计算安全服务市场增长最快的部分之一。



数据来源：Gartner

图 3 2017 年全球云计算安全细分领域市场规模及增速对比（单位：百万美元，%）

表 1 全球云计算安全服务市场细分预测

细分市场	2016 年	2017 年	2018 年	2019 年	2020 年
安全电子邮件网关	654.9	702.7	752.3	811.5	873.2
安全 web 网关	635.9	707.8	786.0	873.2	970.8
IAM、IDaas、云计算用户认证	1,650.0	2,100.0	2,550.0	3,000.0	3,421.8

远程漏洞评估	220.5	250.0	280.0	310.0	340.0
SIEM	286.8	359.0	430.0	512.1	606.7
应用安全性测试	341.0	397.3	455.5	514.0	571.1
其他云计算安全服务	1,051.0	1,334.0	1,609.0	1,788.0	2,140.0
市场总计	**4,840.1**	**5,850.8**	**6,862.9**	**7,808.8**	**8,923.6**

数据来源：Gartner

1.2、 我国云计算安全市场规模及发展趋势

我国云计算安全市场的发展，受国家政策和市场经济的共同影响。随着《网络安全法》的落地执行，网络运营商的安全责任更加明确，安全需求也更加明确。国内很多云计算服务商已经意识到了云计算安全的重要性，提供了相应的云计算安全服务，首先以 BAT 为代表的互联网企业推出云计算安全防御措施，并着手建立新的云计算安全生态圈，其次一些专业的云计算安全解决方案提供商提供安全咨询、安全运维等服务。另一方面，云计算安全市场的收购与结盟正变得愈加频繁，众多大型IT公司都在不遗余力地发展其云计算安全业务，借助资本市场的相互渗透，完善自身的技术、市场和产品。例如国内各大传统IT安全解决方案提供商纷纷并购云计算安全领域初创公司，加速在云计算安全领域的布局。

据 IDC 的预测，2014-2019 年我国信息安全市场年均复合增长率为 16.6%，预计 2019 年将会达到 48.22 亿美元。未来 3-5 年，信息安全的整体增长，将会有相当一部分来自于迅猛增长的云计算安全。中投顾问发布的《2017-2021 年网络安全产业投资分析及前景预测报告》中的数据指出，中国云计算安全处于初步发展阶段，规模尚小，但可见空间已有 50 亿元，未来发展空间将会更大。

对于云计算安全市场本身而言，其蕴含的巨大潜力已达成业内共识。随着我国行业云、政务云的逐步落地，云计算产业开始爆发式增长，对云计算安全的重视程度也不断提升，针对云环境的虚拟化安全产品具有广阔发展前景。中国云计算安全的市场规模会随云计算市场规模的快速增长而

逐渐崛起。国内云计算安全市场将保持高增长，云计算安全方面投入将数倍增加，未来将看到更多针对云计算管理平台、企业 SaaS 应用等方面的 APT 攻击，这也会更加促进云计算服务商将更多地研究云计算安全防护技术。云计算安全未来具有广泛的市场空间，但要实现快速发展，仍需解决目前云计算安全市场存在的诸多问题，云计算安全市场将呈现以下趋势：

（1）加快云计算安全标准工作推进，建立关于数据安全、个人隐私保护、知识产权保护、数据跨境流动等方面的国家法律法规和技术要求；

（2）云计算用户，不再满足于传统的基础安全服务，将转向能够为其提供多元化安全服务的云计算服务商，具备可信的资源、能力、安全服务的厂商将更加符合市场需求；

（3）云计算安全将带动信息安全产业的跨越式发展，在发展基础安全的同时，将更多的引入机器学习和人工智能分析技术，通过大数据分析感知安全威胁，并最终为业务安全保驾护航。

二. 十大云计算安全风险

2.1、 合规风险

云计算服务商必须符合广泛的、不断变化的法律法规要求。随着信息领域的迅速发展，各国、各行业都在加强相关的法律法规建设，云计算服务商合规清单将不断扩大。但各法规对安全的界定有所不同，涉及网络、数据、信息等方方面面，如有些法规要求特定数据不能与其它数据混杂保存在共享的服务器或数据库上；有些国家严格限制本国公民的私密数据保存于其它国家；有些银行监管部门要求客户将数据保留在本国等，因此云计算服务商需有专业的部门和人员负责合规管理工作，以确保管理合规。

相比管理合规，更为重要的是技术合规。云计算存在数据存储位置未知、数据来源难追溯、安全控制和安全责任不明确等问题，使得云计算服务商和云计算客户在面临合规性检查时存在技术不合规的风险。并且，云计算平台上最核心的就是云计算用户数据，对数据的合规收集、存储、使用、备份等如何进行技术支撑是工作重点。尤其是上级监管机构，需要对云计算平台上的云计算用户数据进行审计时，供应商如何进行配合，即如

何既能配合监管需求，又能遵守与云计算用户之间的数据保护协议。

2.2、 虚拟化安全风险

虚拟化是目前云计算服务商使用最广泛的技术之一，是将底层的硬件，包括服务器、存储与网络设备全面虚拟化，利用虚拟化带来的可扩展性有利于加强在基础设施、平台、软件层面提供多云计算用户云服务的能力，解决了资源利用率，资源提供的自动扩展等问题，其中服务器的虚拟化技术支持将单台物理服务器虚拟为多台虚拟服务器，进而大幅提高有限计算资源的利用率。虚拟化技术在提供便利的同时也带来了大量的安全风险，目前虚拟化风险是云计算需要考虑的特有安全风险之一。

- **虚拟化软件安全。**虚拟化软件直接部署于宿主机之上，提供能够创建、运行和销毁虚拟服务器的能力。虚拟化软件层是保证客户的虚拟机在云计算环境下相互隔离的重要层次，可以使客户在一台宿主机上安全地同时运行多个操作系统，所以必须严格限制任何未经授权的云计算用户访问虚拟化软件层。云计算服务商应建立必要的安全控制措施，限制对于hypervisor和其他形式的虚拟化层次的物理及逻辑访问。
- **虚拟主机的安全。**虚拟主机位于虚拟化软件之上，虚拟主机安全包括物理机选择、虚拟主机安全和日常管理三方面。虚拟主机安全现状是大多数依然采用缺省的安全基线配置，并未根据相关的计算要求进行安全加固。因此，对于不具备安全技术常识的个人或者企业来说，采用缺省安全基线配置的虚拟主机将处于较高的安全风险之中。

2.3、 数据安全风险

数据安全风险这是云计算用户目前最为关注的安全风险之一，云计算用户对自身数据在云技术环境下的中的传输、存储、应用不具备实际的控制能力，数据安全完全依赖于云计算服务商,如果服务商本身对于数据安全的控制存在疏漏则很可能导致以下数据安全风险：

- **数据传输风险。**一旦云计算下的数据传输采用明文，或者传输节点存在安全漏洞，极易发生截获数据、黑客入侵及病毒感染等各种情况。而传输数据从输出端至输入端均要通过云计算平台一系列的组件支持，硬件系统的更新、通信协议的失效等均会是数据传输受到破坏；

➢ **数据存储风险。**云计算用户将其所有数据等均存储在云端，而云端是一个庞大的系统，需要对数据统一存储、集中管理，防止数据出现零散化。因此必须要实时监控数据，确保数据正常输送与储存，确保数据的安全性。只要存储数据的相关设备发生老化或 bug，极有可能影响数据存储的安全性，导致数据不可用甚至丢失；

➢ **数据泄露风险。**数据泄露是云计算平台需要面对的问题，数据泄露可能是人为因素或者技术因素。在人为因素上，大多是暗箱操作或私自使用，具备一定谋利性质。技术因素主要是数据安全技术不高，无法有效防范黑客入侵。而黑客入侵是目前泄露信息的主要形式，他们通过边信道的时间信息，借助代码入侵一台虚拟机，通过虚拟机攻击或截获同一个服务器上其他的虚拟机，破获私有密钥，依据获取相应数据信息，导致数据泄露。

➢ **数据丢失风险。**在数据安全影响中，数据丢失属于重要原因。在输入数据、查询数据及输出数据等过程中，因疏忽大意等各种人为因素影响操作，造成操作不当而将数据清空、删除，导致数据丢失。当然也可能是非人为因素，对云系统有关设备进行破坏、损毁等各种情况，最终导致数据丢失等。这些因素丢失数据，如果没有进行备份是无法挽回。如果要重新获取数据信息，还必须要通过数据采集、数据整理、数据分析等程序，需要花费大量的人力物力。因此，数据丢失是造成风险安全的因素之一。

2.4、 API 风险

API 风险指的是接口质量不高，安全性低，第三方插件不安全而导致的安全风险。云计算服务商会公开一组客户使用的软件云计算用户界面（UI）或 API 来管理和与云服务进行交互，IT 团队使用接口和 API 去管理和调用包括云资源、管理、服务编排和镜像等云服务，在公有云中，客户通过互联网访问云平台上的资源。这些 API 能控制大量虚拟机，甚至有云计算服务商用于控制整个云系统的操作接口。

API 对一般云服务的安全性和可用性来说极为重要，安全性差的 API 会让企业面临涉及机密性、完整性、可用性和问责性的安全问题。

➢ **云服务的安全性和可用性。**从身份认证和访问控制再到加密和活动检测，均需要依赖于 API 的安全性，安全性差的 API 会对云服务造成严重

的安全威胁。

➢ **增值服务。**一些第三方组织经常基于这些接口为客户提供增值服务，这更增加了层次化的 API 复杂性，而且这种做法会要求企业将登录资料交给第三方，以便相互联系，因此其也加大了风险。

➢ **远程访问机制及 web 浏览器的使用。**这也增加了这些接口的漏洞存在并被利用的可能。

➢ **业务转移。**对大多数企业而言，业务转移到云是不可避免的，一般情况下，管理、配置和监控都是通过这些接口执行的，安全和可用性完全依赖于每个基础 API 内置的安全性。遗憾的是，云计算服务商一般只关心迁移服务，而不考虑 API 中的不安全因素。这意味着攻击者发动恶意攻击的成功率会大幅提高。

2.5、 分布式拒绝服务(DDoS)风险

DDoS 攻击已经存在很多年了，但是由于云计算的兴起，他们所引发的问题再一次变得突出。云计算以宽带网络和Web方式提供服务，云服务广泛的网络访问和快速伸缩的特性促进了 DDoS 攻击的发展，然而一些新兴的平台如移动设备缺乏必要的防范措施，这也给新型的 DDoS 攻击提供了发展契机。

➢ **对云服务可用性的影响。**DDoS 攻击旨在阻止云计算用户访问其存储的数据或应用程序，通过强制目标云服务占用过多的有限系统资源，如处理器能力，内存，磁盘空间或网络带宽。在云计算时代，许多企业会需要一项或多项服务保持 7×24 小时的可用性，在这种情况下这个威胁显得尤为严重。虽然攻击者可能无法完全摧垮服务，但是可能会导致系统速度下降，并使所有合法的服务云计算用户无法正常访问云服务。

➢ **可能引起云计算用户巨大经济损失。**由于部分云平台采用了按量付费的计费模型，在遭受 DDoS 攻击的时候会产生大量额外资源（带宽、算力等）的消耗，从而会使云计算用户承受超额的经济支出。如客户在云平台的余额不足或额度不够的话，还会造成服务暂停，这会让云计算服务商失去用户。

➢ **DDoS攻击强大的扩展性。**由于云平台使用了虚拟化技术同时为多个

云计算用户提供服务，而在这种模式下针对其中一个云计算用户的 DDoS 攻击比传统服务提供模式更容易对同一云计算服务商下的其他云计算用户产生影响。

2.6、 共享技术风险

资源的虚拟池和共享是云计算的根本，共享技术的漏洞对云计算构成了重大威胁。云计算服务商经常共享基础设施、平台和应用程序，并以一种灵活扩展的方式来开展技术共享。但为了节省成本，云计算服务商是不会大幅增加现成的硬件或软件的，所以只能以牺牲安全为代价。

- **单一的漏洞或错误，会导致整个云服务被攻击。**在云计算环境下，不同的云计算用户可能共享相同的服务器、数据或应用，导致访问控制变得困难。如果极其重要的数据中心组成部分，比如虚拟机管理程序、共享平台组件或者应用程序受到攻击，那么由此可能导致整个环境遭受到损害。
- **云计算用户之间难以保证良好的隔离性。**云计算中使用硬盘分区、CPU 缓冲等机制，而为了保证可动态扩展，云计算中的计算能力、存储与网络资源在多云计算用户间共享，这些都难以保证良好的隔离性。这种风险会导致云平台中某云计算用户的恶意行为影响到同个环境下其它云计算用户的声誉，或者攻击者能对共享环境下的其它云计算用户数据进行非法操作。

2.7、 恶意内部人员

按照业界的传统认知，超过半数的安全事件源于内部人员。尽管对于大多数企业来说，存在恶意企图的内部人员都是有可能的，但是在云计算模式下被增强了，因为这种场景下，所有IT设备或数据被放到一起集中管理，企业的核心数据在云计算环境中的存储，离不开管理员的操作和审核，从基础设施即服务(IaaS)、平台即服务(PaaS)到软件即服务(SaaS)，内部人员拥有比外部人员更高的访问级别，因而得以接触到重要的系统，最终访问数据。这种访问范围的扩大，增加了恶意内部员工滥用数据和服务、甚至实施犯罪的可能性。

来自企业内部的安全威胁包括了许多方面：现任或前任员工，系统管理员，承包商或商业伙伴。恶意破坏的范围从窃取商业机密数据信息到保

护行为。而在迁移采用了云服务的情况下，一个来自企业内部的恶意人员可能会摧毁企业组织的整个基础设施或操作数据，而如果仅仅是纯粹依赖于云计算服务商的安全性，则风险是最大的。如果云计算服务商对内部人员的背景了解不清，在内部管理、安全检查、记录、监控和审核管理活动方面出现疏漏，将可能导致内部人员私自窃取云计算用户数据等内部攻击活动，从而对云计算用户的利益造成巨大的损害。

2.8、 云服务滥用风险

云计算服务由于租用成本低廉，云计算用户可廉价的购买云计算服务商提供的计算、网络、存储资源来进行生产运营。由于云计算服务商无法对使用者的目的进行有效审核，很可能导致被恶意人员利用云计算资源进行破解密钥、发起分布式拒绝服务(DDoS)攻击、发送垃圾邮件和钓鱼邮件、托管恶意内容等恶意操作。

同时，云计算服务商重点关注其云计算用户的业务是否受影响，并没有对用户的使用行为进行监控，导致即使云计算使用用户在进行恶意操作，也无法及时发现和定位。

2.9、 身份、凭证和访问管理不足

云计算服务商在对外提供服务的过程中，需要同时应对多个云计算用户的运行环境，保证不同云计算用户只能访问企业本身的数据、应用程序和存储资源。在这种情况下，云计算服务商必须要引入严格的身份认证机制。如果身份认证管理机制存在缺陷，或者身份认证管理系统存在安全漏洞，则可能导致冒充合法云计算用户、操作人员或开发人员的不法之徒获取、篡改和删除数据，或对虚拟机发起攻击等，给云计算用户带来严重损失。在这些安全机制中，经常存在以下漏洞：

（1）**由于账户锁定而拒绝服务。**攻击者在很短时间内对某个云计算用户账号进行连续失败的验证请求而导致云计算用户被锁定，即 DoS 攻击。

（2）**薄弱的凭证重置机制。**云计算服务商需提供一个机制来重置云计算用户凭证，以防凭证被忘记或丢失。攻击者可以通过该机制重新获取云计算用户密码，对云计算用户产生安全威胁。

（3）**授权检查的缺失。**最新的 Web 应用程序往往容易缺乏授权检查，导致暴露未经授权的信息。

（4）**粗粒度的访问控制。**云计算用户权限的级别过少，导致部分云计算用户权限过大，从而对系统产生威胁。

（5）**企业内部松散的身份验证，弱密码和糟糕的密钥或证书管理。**这会造成数据泄露等安全问题。例如，在美国第二大医疗保险云计算服务商 Anthem 公司数据泄露事件中，导致有超过 8000 万客户的个人信息被暴露，就是因为云计算用户平凭证被盗所致的结果。Anthem 公司没有部署多因素认证，一旦攻击者获取凭证，就很容易完成攻击。

2.10、 未知风险

云计算服务商和云计算用户之间存在很大的信息不对称性。一方面，云计算用户选择外包自己的IT计算和服务到云计算服务商，就是为了解放和优化自己的资源，所以没有必要也没有足够的资源去全面洞察“云”中的所有细节；另一方面，云计算服务商出于商业机密和安全考虑，并不情愿分享所有的关键信息，即使是和安全直接相关的。这种情形下，云计算用户必然需要处理大量的未知安全风险。

实际上，这些“Unknown Unknowns”，也就是说那些未知漏洞们，是云中真正的危险，而软件版本、安全实践、代码更新、漏洞情况、入侵企图、安全设计等都是可以帮助评估自身所面临的安全风险的重要因素。

认清自身的安全现状，向云计算服务商要求最大限度的信息透明，了解它们如何配置系统，如何及时为托管的软件打补丁等。正确地处理安全的模糊性在未来依然会是一个长期的挑战。

三. 云计算安全现状分析

3.1、 云计算安全事故频发，数据安全问题日益凸显

近几年，全球云计算重大安全事故仍在不断上演，安全问题依然不容忽视。2017 年 3 月，微软 Azure 公有云存储故障导致业务受影响超过 8 小时。2017 年 6 月，亚马逊 AWS 共和党数据库中的美国 2 亿选民个人信息

被曝光。

在这些安全问题中，云计算数据安全问题日益凸显。由于脱库、撞库等攻击手段，以及内部人员管理不善引发的大面积数据泄露事件不时发生，云计算用户数据和个人信息被肆意收集、滥用导致的网络诈骗愈演愈烈。尤其是今年生效的欧盟《一般数据保护条例》（GDPR），对数据处理者的数据保护能力提出了更为严格的要求。云计算服务商如何有效保护云计算用户数据安全已成为政府、企业、个人和社会各界广泛关注的热点问题。

究其原因，主要是因为云计算与传统信息系统的云计算用户数据安全存在着本质区别：

- 传统 IT 系统数据安全问题仍然存在；
- 由于不涉及切身利益，云计算服务商在运营过程中易忽略但将长期潜在的未知安全问题；
- 云计算服务商可能为了自身利益损害云计算用户数据安全，如将云计算用户数据用来做机器学习、大数据分析，在云计算用户合同到期后未完全删除云计算用户数据，未经同意将云计算用户数据转让给第三方等。

3.2、 云计算行业安全服务能力参差不齐

在云计算的背景下，“云上的世界更安全”已成为我们对公有云计算安全形态的“普遍认识”。无论是针对传统数据中心的安全防护还是基于云计算的虚拟化安全防护，业务驱动安全的本质并没有改变，其不同之处在于虚拟化环境下，业务更为复杂，安全防护的方式也更加的多元化、复杂化。

近年来，云计算服务商对云计算安全越发重视，根据国家相关法律法规和上级监管部门要求，在网络安全、系统安全、应用安全、数据安全等基础安全方面进行了落地实施，如在管理方面制定了安全管理制度和安全运维流程，确保安全工作开展合规；在技术方面严格控制运维人员的访问权限，定期开展对宿主机、应用软件、数据库软件的安全扫描及加固，确保安全风险可控。部分云计算服务商成立了专业部门负责推动安全工作的

同步规划、同步建设、同步使用，确保其云计算平台运营安全。同时，根据云计算用户的安全需求，云计算服务商提供云抗 DDoS、云 Waf、云杀毒、云态势感知等安全服务，帮助云计算用户提升了安全防护水平。

但是，云计算服务商在安全服务能力上的表现确实参差不齐，部分云计算服务商“重发展、轻安全”的思想普遍存在，安全工作处于被动应对状态，对安全风险的把控能力不足。据中国信息通信研究院可信云评估发现：

- ✓ 一些厂商存在数据备份机制的不健全而导致云计算用户数据泄露的风险；
- ✓ 密钥管理策略的缺陷而导致云计算用户私钥泄露的风险；
- ✓ 业务安全风控能力不足而导致违规数据传播的风险等等。

因此，安全服务能力的建设应结合自身业务的发展与规划，采用同步规划、同步建设、同步运营的方式，制定配套的安全服务能力，提升防护效果。

3.3、 业务安全缺乏统一标准

安全问题对云计算用户来说是个不可逃避的话题，一旦业务的正常逻辑被滥用、被篡改，将产生与其业务目的、业务结果的不同，导致极大的危险性，并使云计算用户面临不可预估的损失和风险。因此，在“安全即服务”的今天，云计算服务商开始将其业务安全风控能力“云产品化”，这不仅为云计算用户的业务安全提供保驾护航，更成为衡量云计算服务商实力的重要因素之一。

现有云计算服务商的业务安全风控能力。目前，云计算服务商结合其云计算能力、大数据分析能力已对外提供信贷反欺诈、交易反欺诈、内容安全监控等业务安全风控能力。例如，腾讯云的直播安全解决方案可以为直播及内容服务企业提供图片、视频、直播的鉴黄服务。阿里云提供防黄牛刷单、注册链接被恶意滥刷、黑产养小号、肆意刷评论等风控能力。网易云提供防羊毛党、防好评、防刷点击等营销作弊行为。天翼云提供个人和企业信贷风控能力，通过信息采集、风险分值评估等方式对信贷风险提

供监控和预警。可以看出，业务安全风控产品可对常见的骗贷、骗保、洗钱、赌博、盗刷、套现、刷单、违规内容传播等安全事件进行实时的预警和跟踪，为云计算用户提供业务安全全程保障。

业务安全风控缺乏统一标准。经调研发现，云计算服务商的业务安全风控产品在功能、性能和自身安全上均没有统一的技术要求，云计算用户使用此类产品时面临着防护失效的风险，以至于引发连带的商业危机、甚至安全事件升级。因此，有必要加快制定相关的标准要求，进一步提升业务安全风控能力，规范行业健康发展。

3.4、 云计算服务模式下安全责任矩阵缺失

随着云计算技术的快速发展，个人和企业云计算用户纷纷上云。对云计算用户来讲，上云意味着节省搭建IT基础设施成本的同时，完全释放了对基础设施的运维，而将更多的资源和精力倾注在其主营业务上。传统IDC 模式下云计算用户对所有安全问题负责不同，到了云上，安全问题变成云服务提供商与云计算用户共同解决的问题。

云计算责任共担模式在业界已经达成共识。云计算服务商应基于云计算用户的需求，提供云主机、云存储、云数据库等服务和相应的安全策略，同时负责维护云平台的高可用，在出现风险事件时，对基础环境、主机环境、网络环境甚至是应用环境进行故障定位、处置和总结。云计算用户应基于云计算服务商提供的服务产品使用和安全说明，正确使用服务或产品，避免因为误操作、疏忽等因素造成云平台的风险，同时云计算用户应按照本公司风险管理要求，对云上信息系统进行风险评估与治理。云计算服务商和云计算用户共同分担安全责任。

共建安全责任矩阵。从安全责任来讲，普遍认为 IT 基础设施层的安全防护由云计算服务商负责，应用软件层、业务逻辑层的安全防护由云计算用户负责。但安全事件的特性是从点到面，再持续的扩散和发酵，而各个层面孤立的安全防护无法建立起有效的防护体系。只有按照安全合规的思路梳理业务流程，明确业务运营各个环节所可能面临的关键风险和防护目标，将相关的安全工作分配到对应的主责团队和配合团队，才能做到真正的责任共担、安全联动。一旦发生安全事件，也不会出现云计算服务商

和云计算用户会按照所谓的“君子协定”进行责任分担，通过一笔笔糊涂账快速降低事件的影响，而非去剖析事件发生的原因的恶性循环之中。因此，携手云计算服务商和云计算用户共同建立安全责任矩阵，通过明确责任、顶层设计、持续改进、共同分担的方式将云计算模式下的安全防护工作做得更好更有效。

3.5、 云计算安全人才极度匮乏

2016年由中网办、发改委、教育部等六部门联合印发的《关于加强网络安全学科建设和人才培养的意见》指出：“网络空间的竞争，归根结底是人才竞争”。随着云计算应用的迅速普及，其所面临的安全威胁越来越大，对安全人才的需求也呈现出井喷趋势。

云服务的特殊性对人才能力提出更高的要求。云计算安全是一个全新的课题，云计算安全人才应摒弃传统安全重攻防轻数据，重破坏轻体系建设，重技术轻业务的安全理念，而应从云计算服务商和云计算用户的双视角出发，对云业务的不同发展阶段，选择合适的安全防护架构，即从安全责任划分、安全意识提升、平台帐号安全、网络安全、主机安全、业务安全、数据安全等不同层次进行综合的安全防护，确保安全风险可控。同时，云计算安全防护的无边界性，对云环境下运维习惯和安全技术的应用提出了挑战，云计算用户数据保护能力的有效性，云服务的特殊性等，对云计算服务商、云使用方、云计算安全服务厂商均提出了与传统安全人才能力不同的需求，传统安全人才暨需转型，提升远程安全服务能力，打破本地化，提高整体化安全水平。

云计算安全人才培养至关重要。面对云计算应用面临的安全危机，云计算安全人才培养应尽早纳入安全战略，加快云计算安全人才的培养，创新安全人才培养机制和模式，树立新的安全人才观念，通过开放合作、体系建设、提升企业责任三个维度，进一步提升安全人才的专业实力，让安全人才真正成为守护云计算产业发展的核心力量。

四. 云计算安全政策环境分析

4.1、 云计算宏观政策体系日趋完善

近几年，国内云计算产业发展、行业推广、市场监管等重要环节的宏观政策环境已经日趋完善。2015 年，国务院先后出台多项与云计算密切相关的政策文件，为云计算相关发展奠定了重要政策基础；中央网信办发布了《关于加强党政部门云计算服务网络安全管理的意见》，在政务云领域发挥重要影响；工信部于 2017 年发布《云计算发展三年行动计划（2017-2019 年）》，提出了我国云计算发展的指导思想、基本原则、发展目标、重点任务和保障措施。公安部于 2016 年发布《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》，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。

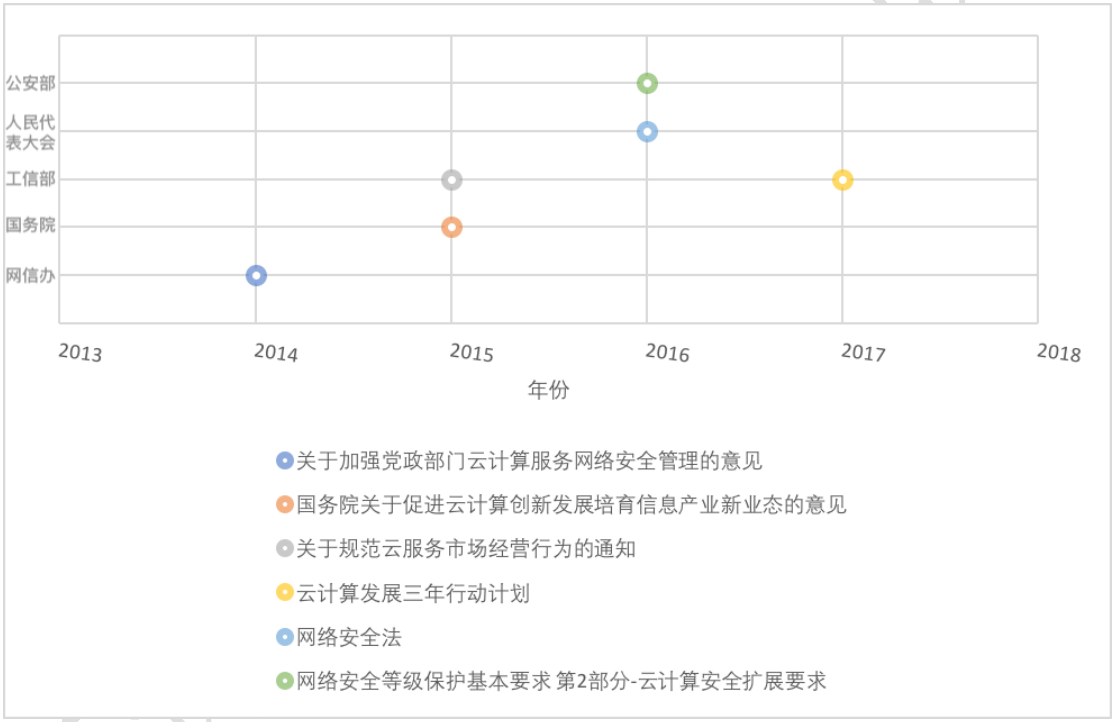


图 4 云计算政策发展

- 2014 年 12 月，《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文〔2014〕14 号）
- 2015 年 1 月，《国务院关于促进云计算创新发展培育信息产业新业态的意见》（国发〔2015〕5 号）
- 2016 年 11 月，意见征集：《关于规范云服务市场经营行为的通知》（工信部）

- 2017 年 3 月，《云计算发展三年行动计划》（工信部信软[2017]49 号）
- 2015 年 6 月，《网络安全法》（人民代表大会）
- 2016 年，《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》（GAT 1390.2-2017 公安部）

4.2、 云计算安全工作重点进一步明确

《关于加强党政部门云计算服务网络安全管理的意见》的出台是一个好的信号，表示了党政部门对云计算市场的重视和企业、政府机构信息化的趋势日益明显。有了相关的云计算标准化文件的指引，相信未来的云服务会更健康化、标准化。政府选用云计算服务商的三大核心内容是安全、可控、稳定。对于文件中提到的云计算服务安全审查机制，云计算服务商要积极主动配合该项工作，尤其在安全性和可控性两方面快速达标，为党政机关的信息安全保驾护航。

《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》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。

- **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。
- **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，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。
- **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，测试人员也应具备相应的能力。

4.3、 监管体系初步形成

《国务院关于促进云计算创新发展培育信息产业新业态的意见》提出了以下等政策措施，顺应了技术和产业发展趋势，回应了我国云计算发展面临的紧迫问题，为云计算创新发展指明了方向。

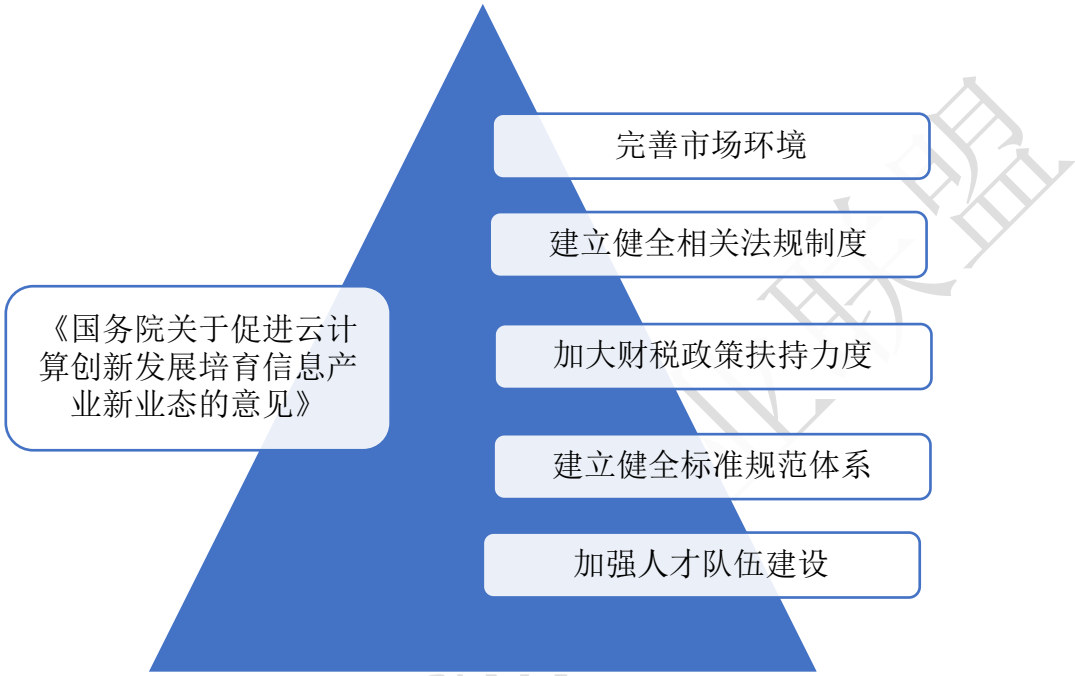


图 5 云计算政策措施

《关于规范云服务市场经营行为的通知》(以下简称《通知》)中重申了外资准入限制，明确了对 IDC 牌照持有者技术合作模式的监管，还强调服务平台必须建在境内。《通知》的各项要求，在《网络安全法》以及其他相关数据保护和个人信息保护的法律法规的基础上，强调了云计算服务商应履行的保障义务，并且细化了具体要求。对于现有的持牌运营商而言，同样需要根据上述规定，考虑更新自己的服务规则以及与云计算用户的协议相关条款，确保合规。

《通知》公开征求意见预示着中国监管机构对于云服务这个信息科技领域最重要的行业监管正式步入轨道。服务能力可信情况，主要指云服务企业通过第三方机构的服务质量可信度的评估情况。企业可通过可信云分级评估结果，或其他方式证明达到相应要求。

4.4、 协同治理体系逐渐成熟

随着越来越多的企业进入云服务领域，市场竞争日益加剧，一些不理性的竞争行为开始出现，规范发展已经成为云服务行业关注的重点，行业自律的重要性日渐凸显。2015 年 1 月 30 日，国务院在《关于促进云计算创新发展培育信息产业新业态的意见》(以下简称《意见》)中提出了“为促进我国云计算创新发展，积极培育信息产业新业态，支持第三方机构开展云计算服务质量、可信度和网络安全等评估测评工作”。

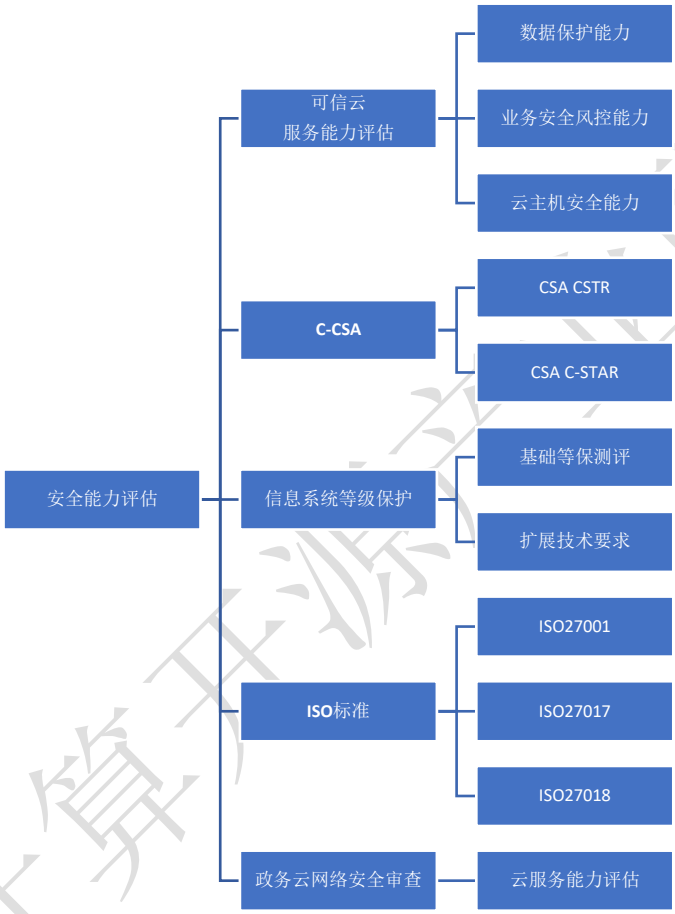


图 6 云计算协同治理体系

根据《意见》的导向，可信云服务能力评估顺应国家政策，旨在建立云计算服务的信任体系。可信云服务能力评估是由数据中心联盟组织，中国信息通信研究院测试评估的面向云计算服务的评估，是我国唯一针对云计算信任体系的权威能力评估体系。能力评估的核心目标是建立云服务商的评估体系，为用户选择安全、可信的云服务商提供支撑，并最终促进我国云计算市场健康、有序发展。

五. 云计算安全发展建议

5.1、 进一步优化云计算安全工作体系

云计算安全工作的目标是确保云计算平台能够平稳运行，能够持续稳定地为云计算用户提供优质服务。与传统安全工作不同，云计算安全工作在一定程度上，是对传统安全工作进行“云计算”的再加工，是需要不断提升云平台自身的安全规划、安全建设、安全运营能力，更是依托其在计算资源、数据资源方面的独特优势，在加强云平台自身安全防护能力，提升**安全运营能力**的同时，最大化输出**安全服务能力**，即针对云平台使用云计算用户在网络安全、信息安全、数据安全、业务安全等方面的需求提供安全服务。

云计算安全工作，是在遵守法律法规、监管要求、技术标准的同时，从云平台自身的安全保障需求和云计算用户的安全运维需求两个工作视角出发，通过服务支撑体系、技术体系和管理体系三个维度开展云计算安全工作，确保工作合规、服务合规。云计算安全工作框架如下图所示：

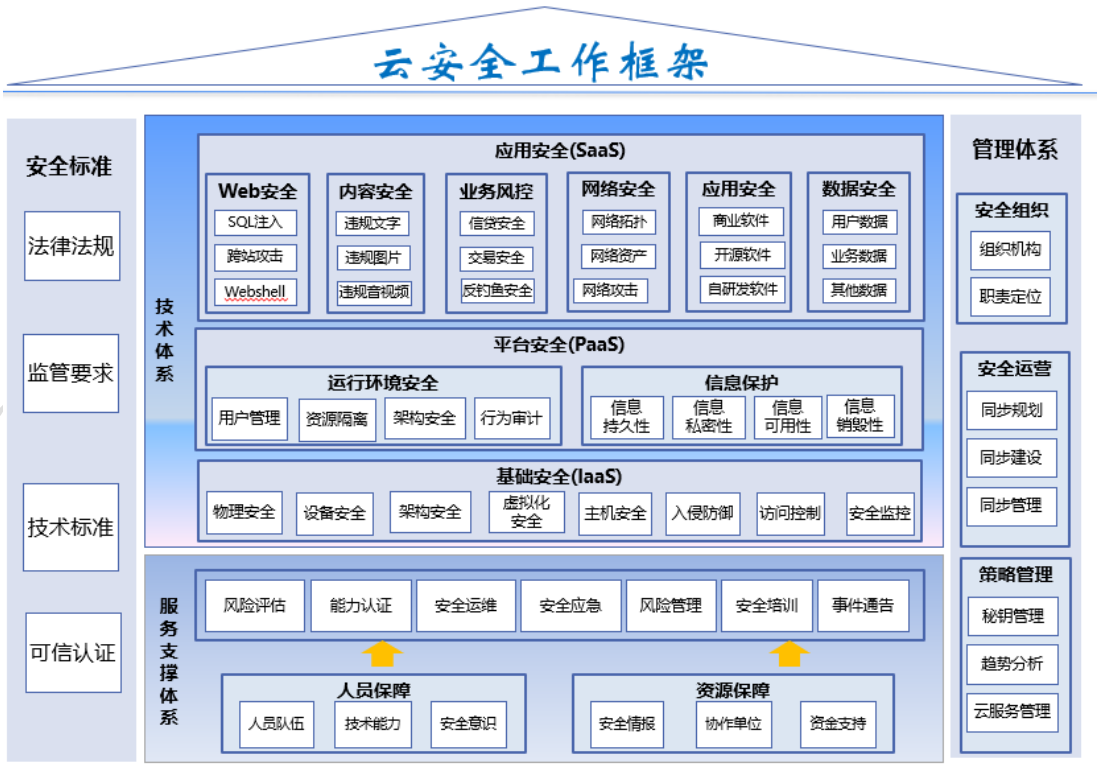


图 7 云计算安全工作框架

云计算安全工作复杂多样，各个维度相互影响、相互制约、相互促进。云计算服务商只有根据业务发展方向，针对性的建立其云计算安全工作体系，在加强安全运维的同时，同步建立服务支撑体系、技术体系和管理体系，做好重大安全事件应急响应处置，才能使得云计算安全工作高效有效。

5.2、 坚持云计算下的管理创新、技术创新、保障创新

《中华人民共和国网络安全法》中明确指出，网络运营者应履行安全保护义务，承担网络安全责任。但目前，云计算安全还处于初级阶段，在安全管理、安全技术和工作开展思路上存在很多不足，仍处于摸索前进的阶段。云计算服务商只有坚持创新，建立全方位、多维度、立体化的创新机制，才能使其适应当今云计算安全的需求，从容应对未来的挑战。

安全管理方面，结合自身业务开展模式和服务特点，制定配套的管理制度、流程和策略文档；优化督查体系，将合规管理、能力评估纳入工作常态；建立通畅的安全与业务/产品的沟通机制，充分发挥安全人员的专业能力，从安全角度观察市场、研究市场，最敏捷的将安全服务能力与市场需求进行有效的对接；

安全技术方面，规划技术发展方向，建立需重点落实的趋势分析、日志审计、攻击行为捕获等技术能力要求，为云计算用户提供可信的安全事件防护能力；指导产品、研发等部门开展 SaaS 层业务安全风控能力建设，针对影响用户业务的重大安全风险(违规内容发布、恶意钓鱼、信贷欺诈、交易欺诈等)提供安全保障能力；加大安全软服务的投入，即通过提供安全规划、安全咨询等帮助用户建立完善的云技术安全工作体制；

安全保障方面，组织建立云计算安全下的运维队伍，定期进行系统巡检、数据安全校验、应急演练等工作。同时，加强**云保险业务**在云计算行业中的深入应用，通过事前风险评估、事后定责定损的方式，转移云计算服务商面临的安全风险。

5.3、 加快国产加密算法在云数据保护中的深度应用

如何确保云计算用户数据安全是云计算安全研究的重点，加密技术作为数据安全的最后一道屏障在云计算中应用也越来越多，而国产加密算法

所具备的先天优势又给云数据安全提供了更多的保障。

在云计算环境下，云计算用户应该采取支持国产加密算法的加密手段，对于静态数据以及数据库中文件进行有效地保护。在 IaaS 环境下，云计算用户可使用云计算服务商提供的加密系统或者使用第三方加密系统对文件的加密。在 PaaS 环境下，云计算用户还可以通过云计算服务商提供的加密工具进行数据加密。同时，在数据传输方面，主要从链路层、网络层、传输层这几个关键点来实现，即采用网络传输加密技术，实现网络传输数据信息同时保证完整性，保证数据信息的机密性。

同时需要关注的是，数据变为密文时，将会丧失许多特性，从而使数据分析与检索方法失效，密文检索与处理技术目前仍然不是特别成熟，随着云计算的发展与密文处理增多的需要，这方面的安全检索与处理技术的研究将会实现突破。而且加密算法的深度应用，对密钥管理提出了更高的要求，完善现有的密钥管理策略，建立更为安全的密钥分发、管理、使用机制，确保密钥绝对安全。

5.4、 落实云计算安全服务能力的可信评估

现今大量企业应用持续向云平台迁移，鉴于云计算用户所使用的主机、存储、数据库等均由云计算厂商提供，并且云平台对用户数据的集中式存储与管理，对用户的主机、数据、业务等安全防护能力提出了更高要求，如何让云计算用户对云计算平台所提供的安全能力可信，是每个云计算服务商必须面对的问题。在安全能力评估方面：

用户数据保护能力评估：从事前防范、事中保护、事后追溯三个层面，涉及数据持久性、数据私密性、数据隐私性、数据防窃取性、数据可用性、数据访问安全性、数据传输安全性、数据迁移安全性、数据销毁安全性等数据保护的主要环节和内容要求；

主机安全防护能力评估：从主动安全防范视角出发，涉及密钥管理、登录策略、访问控制策略、口令策略、web 安全策略、敏感信息保护策略等基线和 web 安全要求。

业务安全风控能力评估：从预防黄、赌、毒、暴恐等违法违规内容肆

意传播；钓鱼网站、虚假公众号、虚假 APP 等钓鱼行为；骗贷、骗保、洗钱、盗刷、套现、恶意下单、刷单、薅羊毛等诈骗行为，进行内容安全、反钓鱼、信贷反欺诈、交易发欺诈、营销反欺诈等风控能力评估。

面对云平台防护能力的千差万别，以摸清家底、认清风险、找出不足提升能力的**可信评估**刻不容缓。