第3章 云计算安全管理方法及相关模型

3.1 云计算安全标准化工作概况

为了保障云计算环境的安全，不仅要采取相应的技术防护措施、完善管理方案，还需要有相关的云计算安全标准为安全保障工作提供制度环境，引领云计算安全工作的开展。目前，国内外云计算安全相关标准化组织形成了众多的云计算安全标准，这些云计算安全标准为云计算提供了安全管理保障，促进了云计算安全快速发展。

3.1.1 国际云计算安全标准概况

目前，许多国家政府及标准组织都加入到了云计算安全标准的制定工作中，云计算安全标准工作已经在全球范围内全面启动。其中，比较有代表性的国际标准组织包括云安全联盟（CSA）、美国国家标准与技术研究院（NIST）、国际标准化组织（International Organization for Standardization，ISO）以及国际电信联盟远程通信标准化组织（International Telecommunication Union-Telecommunication Standardization Sector，ITU-T）、欧洲网络与信息安全局（European Network and Information Security Agency，ENISA）等。这些国际标准组织对云计算安全标准进行了长期、深入的研究，从基础类到技术类、服务类、管理类的术语和参考框架，均出台了一系列云计算及云计算安全标准，在云计算的云服务、安全及云际接口等方面均有很多成果。下面对其中几个国际标准组织进行简单介绍。

1. CSA

CSA 是 2009 年 4 月在 RSA 大会上宣布成立的一个非营利性组织，其组织成员包括 100 多家来自全球的 IT 企业，并与 ITU、ENISA、ISO 等标准组织及机构合作，建立了定期的技术交流机制，交流在云安全方面的经验和前沿技术，致力于在云计算环境下推广云安全的最佳实践方案。CSA 自建立以来已经发布了一系列研究报告，这些报告从技术、操作、数据等多个方面提出了保证云安全需要考虑的问题以及相应的解决方案。业界最为熟知的《云计算关键领域安全指南》就是 CSA 发布的，该指南在 2017 年 7 月更新到了第 4 版，从架构、治理和运行 3 个部分、14 个关键领域对云安全进行了深入阐述。另外，CSA 在云安全威胁、云安全控制矩阵、云安全度量等方面也有重要的研究成果。CSA 在云安全最佳实践与标准制定方面有着巨大的影响力，对云计算安全行业规范的形成起到

了一定的作用。

2. NIST

NIST 直属美国商务部，主要从事物理、生物、工程、测量技术以及测量方法等方面的基础和应用研究，并提供标准、标准参考数据以及相关服务。2010 年 12 月，美国联邦首席信息官(CIO)发布《联邦信息技术管理改革 25 点实施计划》(*25 Point Implementation Plan to Reform Federal Information Technology Management*)，其中确立以“云优先”策略为核心的美国联邦 IT 改革方向，并于 2011 年 2 月发布了《联邦云计算战略》(*Federal Cloud Computing Strategy*)，其中提出了美国联邦 IT 向云计算迁移的框架和政策举措。为了积极响应、落实和配合美国联邦云计算战略，NIST 于 2010 年 11 月牵头启动了云计算计划，为美国政府安全、高效地使用云计算提供标准支撑服务，并成立了云计算目标商务用例工作组(Cloud Computing Target Business Use Cases Working Group)、云计算参考架构和分类工作组(Cloud Computing Reference Architecture and Taxonomy Working Group)、云计算标准路线图工作组(Cloud Computing Standards Roadmap Working Group)、云计算应用的标准推进工作组(Cloud Computing Standards Acceleration to Jumpstart the Adoption of Cloud Working Group)、云计算安全工作组(Cloud Computing Security Working Group)这 5 个云计算工作组，制定并发布了多项云计算标准和指南，加快了美国联邦政府安全采购云服务进程，在业界产生了巨大影响。其中，由 NIST 提出的云计算定义、3 种云服务模式(SaaS、PaaS、IaaS)、4 种部署模型(私有云、公有云、社区云和混合云)以及五大基础特征(按需自助服务、宽带网络访问、资源池、快速伸缩能力以及可被测量的服务)被认为是云计算的权威性描述。

NIST 云计算安全工作组自成立以来，在为美国政府安全采用云服务提供标准方面做出了很大贡献，其输出成果如下：

(1) SP500-299，《NIST 云计算安全参考架构——草案》(*NIST Cloud Computing Security Reference Architecture—Draft*)。

(2)《美国政府采用云计算的安全需求挑战》白皮书(“*Challenging Security Requirements for US Government Cloud Computing Adoption*”White Paper)。

(3) SP800-173，《云适应的风险管理框架：应用风险管理框架到基于云的联邦信息系统指南》(*Cloud-Adapted Risk Management Framework: Guide for Applying the Risk Management Framework to Cloud-Based Federal Information Systems*)。

(4) SP800-174，《用于基于云的信息联邦系统的安全和隐私控制》(*Security and Privacy Controls for Cloud-Based Information Federal Systems*)。

3. ISO/IEC

ISO 成立于 1946 年，是一个全球性的非政府组织，其总部设在瑞士日内瓦，成员包括 162 个国家和地区，参与者包括各成员的标准机构和主要公司，中国也是 ISO 的正式成员。ISO 是世界上最大的非政府性标准化专门机构，它通过 2856 个技术机构开展技术活动，其中技术委员会有 611 个，工作组有 2022 个，特别工作组有 38 个。ISO 是国际标准化领域中十分重要的组织，它负责绝大部分领域的标准化活动，其中包括军工、船舶、石油

等垄断行业。ISO 的宗旨是“在世界上促进标准化及其相关活动的开展，以便于商品和服务的国际交换，在智力、科学、技术和经济领域开展合作”。

IEC(International Electrotechnical Commission，国际电工委员会)于 1906 年成立，是世界上成立最早的国际性电工标准化机构，负责电气工程和电子工程领域的国际标准化工作。

ISO 和 IEC 这两大国际标准组织于 1987 年联合组建了信息技术第一联合技术委员会(JTC1)。ISO/IEC JTC1/SC27 是其中专门从事信息安全标准化的分技术委员会，它是信息安全领域中最具代表性的国际标准组织。SC27 下设有多个工作组，其工作范围覆盖了信息安全管理和技术领域，包括信息安全管理体系、密码与安全机制、安全评估准则、安全控制以及服务身份管理与隐私保护技术等。SC27 于 2010 年 10 月启动了“云计算安全与隐私”项目，确定了云计算安全与隐私的基本架构，明确了信息安全管理、身份管理和隐私技术以及安全技术这 3 个领域的标准研制方案。

4. ITU-T

ITU-T 创建于 1993 年，总部设在瑞士日内瓦，它是在国际电信联盟(ITU)管理下专门制定远程通信相关国际标准的组织。ITU-T 中与云计算相关的工作组包括云计算焦点组(Focus Group on Cloud Computing，FG Cloud)、ITU-T SG13 研究组以及 ITU-T SG17 研究组。

FG Cloud 是由 ITU-T 于 2010 年成立的，旨在从电信角度为云计算提供云安全与云管理等支持，该工作组随后发布了多份云计算技术报告，其中包括《云安全》(该报告的完整英文名称为 *Focus Group on Cloud Computing Technical Report Part 5: Cloud security*)和《云计算标准制定组织综述》(该报告的完整英文名称为 *Focus Group on Cloud Computing Technical Report Part 6: Overview of SDOs involved in Cloud Computing*)。《云安全》报告确定了 ITU-T 与相关标准组织需要合作开展的云安全研究领域，该报告还计划对包括欧洲网络与信息安全局(ENISA)、ITU-T 等标准组织所开展的云安全工作进行评价，并在此基础上总结云服务用户与云服务供应商所面临的安全威胁与存在的安全需求。《云计算标准制定组织综述》对包括分布式管理任务组(Distributed Management Task Force，DMTF)、美国国家标准与技术研究院(NIST)、云安全联盟(CSA)等在内的标准组织已开展的活动及取得的成功进行了综述和举例分析，综述表明各标准组织制定的云计算标准架构各不相同，都是出于各自的目的，无法覆盖云计算标准化的全部。同时，该报告建议 ITU-T 需要与其他标准组织进行互补的标准化工作，避免重复工作，以提高效率，进而在功能架构、跨云安全和管理、服务水平协议等研究领域发挥引领作用。FG Cloud 下设两个工作组，分别是：WG1，即云计算效益和需求(Cloud Computing Benefits and Requirements)工作组；WG2，即云计算标准发展差距分析和线路图(Gap Analysis and Roadmap on Cloud Computing Standards Development)工作组。

FG Cloud 于 2011 年 12 月结束了工作，ITU-T 与云计算相关的后续工作就转移到了 SG13 和 SG17 研究组进行。SG13 研究组的研究内容是包括云计算、手机和下一代网络的未来网络，云计算是其中重要部分。SG13 研究组下设 Q17、Q18 以及 Q19 小组，这些

小组制定了详细描述云计算生态系统需求和功能架构的标准，涵盖云间、云内计算和支持XaaS(Anything as a Service，一切皆服务)的技术。云计算依赖于各种电信和信息技术基础设施资源的相互作用，因此SG13研究组制定了针对不同云服务商域服务和技术的一致性端到端、多重云管理和检测的标准，并发布了多份云计算建议书。SG17研究组则开展了多个与云计算安全相关的课题研究，发布的云计算标准包括《云计算安全框架》(*Security Framework for Cloud Computing V2.0*)以及《信息技术　安全技术　基于ISO/IEC 27002云服务的信息安全控制实施规程》(*Information Technology—Security Techniques—Code of Practice for Information Security Controls based on ISO/IEC 27002 for Cloud Services*)等。

5. ENISA

ENISA是欧盟及其成员国的网络和信息安全中心，它旨在帮助欧盟成员国实现相关的欧盟法规，提升欧洲关键信息基础设施和网络的弹性，从而提高欧盟的网络和信息安全。

ENISA早在2009年就启动了云计算安全相关研究工作，在云安全标准化方面主要关注云计算中的风险评估和风险管理等领域，并先后发布了《云计算：优势、风险及信息安全建议》(*Cloud Computing：Benefits，Risks，and Recommendation for Information Security*)和《云计算：信息安全保障框架》(*Cloud Computing：Information Assurance Framework*)两个报告。其中，《云计算：优势、风险及信息安全建议》定义了云所面对的风险类型、云中的资产类型、云的脆弱性类型、影响资产风险等级等；《云计算：信息安全保障框架》旨在对采购云服务的风险进行评估、对不同云服务提供商提供的云服务进行比较，帮助云服务提供商减轻安全保障负担，等等。2011年，ENISA发布了报告《政府云的安全和弹性》(*Security & Resilience in Government Clouds*)，为政府提供了决策指南。2012年4月，ENISA发布了报告《云合同安全服务水平检测指南》(*A Guide to Monitoring of Security Service Levels in Cloud Contracts*)，该指南是一套持续监测云服务提供商安全服务水平协议运行情况的指南，可以实时核查用户数据的安全性。

2012年，ENISA发布了名为“释放欧洲云计算潜力”(Unleashing the Potential of Cloud Computing in Europe)的云计算计划，该计划的内容包括：对云服务进行标准化和认证，提供安全、公平的服务合同及服务水平协议，建立欧盟云计算合作关系，以推动云计算发展。在该计划的推动下，ENISA于2014年推出了“云认证计划初步框架”(Cloud Certification Schemes Metaframework，CCSM)，该框架归纳整理了欧盟11个成员国的29个云计算相关国家法律法规以及相关指南，最终概括了安全职责、风险管理、供应链安全、信息安全策略等29个云安全目标，并将这29个云安全目标与欧盟现有的云安全认证计划中的云安全目标的达成情况进行了对照。用户利用CCSM中的对照表，可以了解某个通过某项认证计划的云服务的云安全目标具体满足达成，明确哪些安全目标已经达成，哪些未被验证，从而可以根据自身的安全需求对云服务进行选择和购买。

3.1.2　国内云计算安全标准概况

从总体上来看，我国对云计算及云计算安全方面的研究起步较晚，在云计算产业化及

标准化方面还与国外有着明显的差距。近几年，国内各标准组织和相关机构开始大力投入到云计算及其安全标准制定工作中，中国通信标准化协会（China Communications Standards Association，CCSA）在云安全标准制定方面有着较为突出的成果。同时，全国信息技术标准化技术委员会、全国信息安全标准化技术委员会以及公安部也陆续开展了云计算安全相关标准的制定工作。经过多年的技术研究积累以及市场的开拓发展，云计算在国内正迎来高速发展的黄金时期，云计算安全技术作为云计算的核心保障，在标准和规范方面也进入了一个密集开发的阶段。目前，云计算安全和标准化是我国云计算面临的关键问题。下面对几个国内相关标准组织及其工作进行介绍。

1. 全国信息技术标准化技术委员会

全国信息技术标准化技术委员会成立于 1983 年，原名全国计算机与信息处理标准化技术委员会，主要负责 ISO/IEC JTC1（信息技术第一联合技术委员会）的国际归口工作。全国信息技术标准化技术委员会下设 22 个分技术委员会和 18 个直属组，是在国家标准化管理委员会与工业和信息化部共同领导下成立的从事全国信息技术领域标准化工作的技术组织。

2009 年 4 月，工业和信息化部软件服务业司联合全国信息技术标准化技术委员会在北京成立了信息技术服务标准（Information Technology Service Standards，ITSS）工作组。该工作组的任务主要是：根据我国信息技术服务业发展现状和趋势，研究和提出信息技术咨询设计、信息技术运维、信息技术服务管控等方面的标准需求，进一步建立信息技术服务标准体系以及制定信息技术服务领域的相关标准。ITSS 工作组下设云服务专业组，该组从云服务的分类、服务交付、服务运营、服务安全等方面开展研究工作，推动云服务的标准化进程。

2009 年 12 月，工业和信息化部软件服务业司、国家标准化管理委员会共同领导成立了全国信息技术标准化技术委员会 SOA 标准工作组。该工作组主要开展我国 SOA（Service-Orient Architecture，面向服务的体系结构）、云计算、中间件等领域的标准制定、修订及应用推广工作。为开展 SOA 与云计算结合的相关技术标准研究工作，SOA 标准工作组成立了云计算研究专题组。该专题组自 2010 年起开始对云计算互操作和可移植、数据中心和设备等技术标准进行研制，具体内容涉及术语和参考模型、弹性计算接口标准、虚拟化资源管理及标准化、云计算管理接口规范等。此外，该专题组还发布了《中国 SOA 最佳应用及云计算融合实践》等与云计算相关的研究报告。

2012 年 9 月，全国信息技术标准化技术委员会成立了云计算标准工作组，该工作组主要负责对云计算领域的基础、技术、产品、安全等国家标准进行制定和修订，旨在发挥政府、企业、高校、科研机构、用户以及中介组织等的作用，协调和调动各方面的资源，推动国内云计算的标准化工作进程，推动我国云计算领域的技术创新和产业发展。该工作组围绕云存储和数据管理、平台即服务、数据中心、云服务及安全、弹性计算等开展多项国家标准研制，构建由框架、关键技术、服务获取与安全管理 4 部分构成的云计算标准体系框架。同时，该工作组还担任联合编辑、联合召集人等职务，同步推动云计算国际标准化工作，向 ISO/IEC JTC1/SC38 提交多篇国际标准贡献物。该工作组已发布的云计算标准包括《信

息技术云计算参考架构》(GB/T 32399—2015)、《弹性计算应用接口》(GB/T 31915—2015)等。另外,云计算标准工作组还承担国家发展和改革委员会、财政部及工业和信息化部联合支持的云计算示范工程“云计算公共技术服务平台”项目,建设云计算公共服务平台,开展云计算标准符合性和兼容性测试,为云计算产品厂商提供云计算测试服务。

2. 中国通信标准化协会

中国通信标准化协会(CCSA)于2002年12月18日在北京正式成立。该协会是由国内企事业单位自愿联合组织,并经业务主管部门批准,经国家社团登记管理机关登记,开展通信技术领域标准化活动的非营利性法人社会团体。该协会的最终目标是支撑我国的通信产业,让通信标准研究工作更好地开展,为世界通信作出贡献。

CCSA由会员大会、理事会、专家咨询委员会、技术管理委员会、若干技术工作委员会及分会、秘书处构成,目前已经有300多个企业和研究组织加盟CCSA。其主要任务是把通信运营企业、研究单位、大学、制造企业等关心标准的企事业单位组织起来,按照公平、公正、公开的原则制定标准,进行标准的协调、把关,把高技术、高水平、高质量的标准推荐给政府,并把具有我国自主知识产权的标准推向世界。CCSA的技术工作委员会下设了若干个工作组,各工作组又下设若干个子工作组和项目组。

目前,CCSA已经发布了多个专门针对云计算安全的标准。例如,在2014年10月发布的《云运维管理接口技术要求》中规定了云运维支撑系统与云资源管理平台、云服务支撑系统之间的接口,包括接口功能、协议和信息模型,以支持云运营支撑系统实现云资源运维管理、云服务保障管理、云服务开通管理、特定云服务运维管理以及云合作运维管理等。再如,2015年4月CCSA发布的《云计算基础设施即服务(IaaS)功能要求》中规定了云计算IaaS服务种类和服务模式、功能架构和功能需求、接口和安全要求以及关键业务流程。另外,CCSA还开展了多个云计算标准项目的研究,例如《2014B49:基于公众网络的高速视频云应用平台的研究》《2012-2244T-YD:云计算平台即服务(PaaS)功能要求与架构》《2013B17:具有快速响应需求的交互式云应用》等。此外,CCSA还针对政务云开展了《基于云计算的电子政务公共平台安全服务安全要求》《基于云计算的电子政务公共平台技术功能和性能评测技术要求》《基于云计算的电子政务公开平台总体顶层设计导则》《基于云计算的电子政务公共平台总体服务建设实施规范》等多个标准的课题研究,主要包括总体类、技术类、服务类、安全类以及管理类五大系列标准。

3. 全国信息安全标准化技术委员会

全国信息安全标准化技术委员会成立于2002年4月,是信息安全技术专业领域从事信息安全标准化工作的技术工作组织。全国信息安全标准化技术委员会以专家为主体组成,其下分设了WG1(信息安全标准体系与协调工作组)、WG2(涉密信息系统安全保密标准工作组)、WG3(密码技术标准工作组)等多个工作组。全国信息安全标准化技术委员会负责组织开展与国内信息安全有关的标准化技术工作,其工作范围覆盖了安全技术、安全服务、安全评估、安全管理、安全机制等领域。随着新技术和新应用的兴起及快速发展,其工作重心逐渐向应用和服务安全标准转移,在云计算、物联网、移动互联网、智慧城市、工业控制系统等领域都已经开展了国家标准化工作,并形成了阶段性的标准化工作成

果。目前，全国信息安全标准化技术委员会承担了多项云计算安全相关项目，其下设的工作组开展了《云计算安全参考架构》《信息安全技术 云计算数据中心安全建设指南》《信息安全技术 公有云安全指南》《云计算安全及标准研究报告》等多个专门针对云计算安全的标准的课题研究。

4. 公安部信息安全等级保护评估中心

公安部于 1997 年建立了公安部信息安全等级保护评估中心，该中心是公安部承担或参与国家标准、行业标准的制定、修订和标准验证的机构，不仅承担标准方面的工作，还包括以下工作：对国内生产和销售的计算机信息系统安全产品、在国内销售的国外计算机信息系统安全产品进行质量监督检测，主要内容包括产品质量检测、鉴定检验、监督抽查检验、委托检测以及仲裁检测；对国内的网络信息安全系统进行安全及风险评估等。目前，公安部信息安全等级保护评估中心已经牵头起草了多项云计算安全的相关标准，其宗旨是加强网络信息系统安全专用产品的管理，保证安全专用产品的安全功能，维护网络信息系统的安全。

3.2 云计算安全管理工作

近几年，作为第三次 IT 浪潮代表的云计算技术在全球范围内掀起了一股热潮，各国政府及 IT 公司纷纷投入到云计算技术的研发和应用中来。云计算的发展改变了人类的生活、生产以及商业模式，例如，企业只需要申请账号并按需付费，就可以使用云服务，不再需要自建数据中心等。云计算不断地发展和普及，随之而来的还有全新的网络威胁、数据泄露等风险。各国产业界和学术界的科研工作者都加紧开展对云安全管理的深入研究，多数云服务提供商也部署了安全管理措施来保障云平台的安全性，例如 Google 公司在云安全方面实现了可信云安全的接入服务管理、可信云安全产品管理、可信云安全企业自管理等。作为国际上具有代表性的信息安全管理体系标准，信息安全体系标准 ISO/IEC 27001 已经获得世界各国政府、证券、银行、保险公司、网络公司以及许多跨国公司的广泛认可。CSA 提出的云控制矩阵(Cloud Controls Matrix，CCM)在 ISO/IEC 27001 的基础上结合云计算的特点，制定了云计算安全管理的要求，CCM 还提供了基本的安全原则以及多个域的控制措施，指导云服务提供商和云客户评估云服务提供商提供的整个云计算的安全风险，现已成为业界公认的安全标准和法规。通过云计算安全管理体系的建立、运行和改进，可以进一步规范企业的云计算安全管理工作，确保企业云服务的安全。

云计算在安全管理方面仍然面临着很多挑战。例如，在管理权方面，云计算环境下用户将他们的应用系统和数据都迁移到了云端，交由云服务提供商管理，在这种云计算数据管理权与所有权相分离的情况下，是否应该给云服务提供商提供一些具有高级权限的管理是一个值得考虑的问题；在监管方面，云计算环境具有高度虚拟化、动态性、复杂性、海量数据等特性，这些特性给云计算的安全监管带来了巨大挑战；在审计取证方面，云计算环境具有大数据量、边界模糊、复用资源环境等特征，因此云服务提供商的安全审计工作面临着很大的挑战，取证工作难度很大，同时云计算的安全运维比起传统信息系统所面临

的运维管理更具有难度和挑战性。

在云计算安全管理方面有几个重要的领域，分别是云计算风险管理、云计算安全基线管理以及云计算应急响应管理。这几个领域对于保证云计算中心的安全性以及可持续性有着很重要的意义。下面分别对其进行介绍。

1. 云计算风险管理

基于云计算的风险管理是建立云计算安全管理体系的前提，同时也是确定用户安全需求最主要的途径之一，它主要是围绕云计算的风险开展评估、处理以及控制活动，是云计算管理的重要内容。

云计算中的风险管理需要对云计算中的风险进行辨别，评估风险出现的概率以及产生的影响，然后建立一个规划来管理风险。云服务提供商在对云计算进行安全管理时，要根据云计算信息系统的重要性以及面临的风险大小等因素来综合平衡风险成本，确定云计算安全体系中的各种安全风险等级，选择合适的云安全解决方案，避免出现“过保护”和“欠保护”的现象。

在云计算环境下，进行风险管理的主要目标就是预防风险，通过对云计算进行风险评估，云服务提供商可以系统、全面地掌握当前云计算的安全状况，找出潜在的安全风险，并对其进行合理分析，判断风险的严重性和影响程度，从而更好地确定自身在云计算安全建设方面的需求。同时，云服务提供商也可以依据风险评估内容与结果来确定最终对信息资产的保护措施以及控制方式，根据自身的弱点、各种资产面临的安全威胁等确定具体的安全需求。

2. 云计算安全基线管理

为保证信息系统的稳定运行，管理人员需要在云计算业务系统的整个生命周期的各个环节对网上的设备以及系统安全配置进行定期检查，其遵守的最低安全标准就是安全基线。安全基线是信息系统所需满足的最基本的安全要求。针对云计算信息系统建立安全基线是保障云计算信息系统安全运行的必要步骤，云计算信息系统网络结构复杂，服务器种类繁多，运维人员容易发生误操作或采用初始系统设置而忽略对安全控制的要求，从而给信息系统造成极大的影响。建立安全基线可以防止上述状况的发生。

安全基线模型以业务系统为核心，分为业务层、功能架构层以及业务实现层。其中，业务层主要根据不同业务系统的特性定义不同安全防护要求；功能架构层将业务系统分解为对应的应用系统、网络设备、数据库、安全设备等不同设备和系统模块，这些模块将业务层定义的安全防护要求细化为该层不同模块所应该具备的要求，例如将安全防护要求细化成为 Windows 安全基线、路由器安全基线等可执行和实现的要求；业务实现层根据业务系统的特性，将功能架构层的各个模块进一步分解，例如，将网络设备模块分解为路由器、交换机等系统模块。

以上介绍了安全基线模型的构成。下面结合实例分析安全基线模型如何应用于云计算中心。

云计算中心需要通过互联网的接口为互联网用户提供服务，而这些互联网的接口会受到互联网中各种蠕虫的攻击威胁。因此，云计算安全基线模型在业务层定义了需要防

范蠕虫攻击的要求；在功能架构层将蠕虫攻击的防护要求细化为操作系统、网络设备、网络架构以及安全设备等模块所对应的安全防护要求；在业务实现层针对各种不同的安全威胁以及功能架构层中的不同模块制定可执行和实现的要求，例如，针对不同类型的蠕虫病毒威胁，在 Windows、Linux 等不同操作系统里定义不同的具体防范要求。

云计算信息系统中的安全基线设计范围广泛，整个过程贯穿于信息系统的全部生命周期，是一个很复杂的系统工程，因此需要结合信息系统的风险评估报告做好安全基线建立、落实以及管理过程的规划，考虑好如何规划及动态覆盖到云计算环境中业务和操作的各种安全行为。

3. 云计算应急响应管理

应急响应指的是云计算信息系统在受到攻击时如何在安全策略的指导下及时发现问题并迅速响应，这是保障云计算信息系统安全的重点。P2DR（Policy，Protection，Detection，Response）模型是目前国内外信息系统中应用最广泛的动态安全模型，该模型是以安全策略为中心的动态自适应网络安全模型。根据 P2DR 模型构筑的网络安全体系能够在统一安全策略（Policy）的控制和指导下，综合运用防火墙、身份认证等防护（Protection）工具，并利用漏洞评估、入侵检测系统等检测（Detection）工具来了解和判断网络系统的安全状态，通过适当的响应（Response）措施来降低网络系统面临的安全风险。防护、检测和响应组成了一个完整的动态安全循环，如图 3-1 所示。

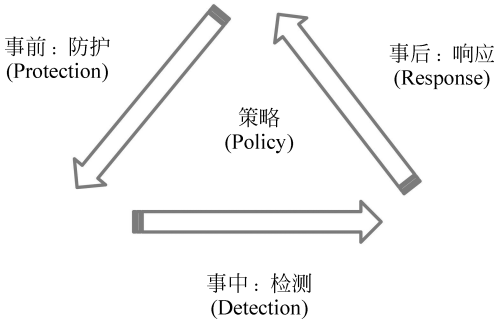

图 3-1　动态安全循环

结合 P2DR 模型，可以将云计算安全事件处理分为事前、事中以及事后 3 个阶段：

（1）事前。明确边界并划分安全区域，将要保护的资源与攻击者隔离开，做好安全保护工作。

（2）事中。应进行动态监控，在边界内要注意用户的异常行为，在边界外要观察攻击者的动向，抓住非法入侵系统的攻击者、

（3）事后。应该取证以追究责任人，通过追查入侵者进入的途径，找出系统防护体系以及监控体系的漏洞，避免让入侵者再次进入。

以上分析的是云计算安全管理的 3 个重要领域，由此可见，云计算安全管理体系的建立是一项系统工程。一般而言，整个云计算安全管理实施的周期分为 4 个阶段，分别是准备阶段、风险评估阶段、云计算安全管理系统文件建立阶段以及云计算安全管理体系运行和完善阶段：

(1) 准备阶段。该阶段的主要任务是建立云计算安全组织机构,进行云计算安全相关培训,识别云计算安全现状与标准之间的差距,并制订详细的实施计划,明确云安全管理工作实施不同阶段的工作职责和工作任务。

(2) 风险评估阶段。确定风险评估方法,包括确定风险接受准则等,要针对各个关键业务过程识别并建立重要的云计算信息资产清单,并对识别出的关键信息资产进行风险评估,根据资产的主要威胁、脆弱性以及有关的影响程度制订风险处理计划。

(3) 云计算安全管理体系文件建立阶段。根据差距分析和风险评估结果建立公司的云计算安全管理体系文件,且需要在建立文件的时候考虑融合其他管理体系(例如 ISO/IEC 27001 等)。该体系文件一般分为 4 个层次:第一层文件包括云计算安全管理方针、云计算安全管理范围、云计算安全管理手册以及适用性申明等方面的文件,第二层文件是描述过程的程序文件,第三层文件是为组织活动提供指导的作业指导书,第四层文件是符合 CCM 条款和 ISMS(Information Security Management System,信息安全管理体系)的记录文件。

(4) 云计算安全管理体系运行和完善阶段。试运行已经建立的云计算安全管理体系,检验体系的适合性和有效性,对存在问题的部分进一步加以完善。

在整个云计算安全管理实施周期中,风险评估和体系文件建立这两个阶段最为重要,其中风险评估是云计算安全管理体系建立的基础,也是体系文件运行的依据。

3.3 云计算安全评估及相关模型

3.3.1 云计算安全评估概述

信息安全风险评估是指根据有关信息安全技术和管理标准,对信息系统及其处理、传输和存储的信息的机密性、完整性以及可用性等安全属性进行评估的过程。由于云计算中数据的处理、传输和存储都依赖于互联网和相应的云计算平台,数据的流动性对用户而言是不可见的,因此传统的信息安全风险评估方法在云计算环境下并不适用,云计算环境需要有一套相应的度量指标和评估方法。

根据评估对象的实际情况,云计算系统安全风险评估的流程一般如图 3-2 所示。在云计算环境下,由于云计算侧重于服务,更多地依赖于网络,其安全性会受到云计算平台和网络状况的影响,因此云计算安全风险评估一般是从存储、计算和网络这 3 个方面给出:存储服务一般是通过建立分布式的存储中心来实现基于网络的高效分布式存储,因此在进行安全风险评估的时候要考虑数据的安全性,包括数据的加密手段、数据存储的备份手段以及数据分散情况等;计算服务一般是通过租赁计算设备或借助统一平台来实现的,因此在对计算服务进行安全风险评估时,需要考虑租赁计算设备的运行可靠性,以及统一平台的数据加密方式、是否允许特权用户访问等安全问题;网络服务的安全风险评估则应考虑网络基础设施的运营情况,以及是否备份了多个网络接入设备,是否能满足计算和存储需要等问题。

结合传统的安全风险评估方法,针对不同云计算服务的安全评估方法可以从资产识

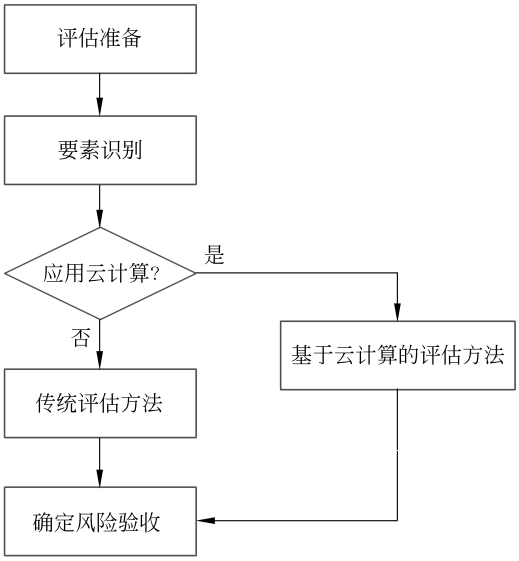

图 3-2　云信息系统安全评估流程

别、威胁识别、脆弱性识别和赋值、风险评估和分析这 4 个方面给出。下面对这几个方面进行介绍。

(1) 资产识别。包括资产分类和资产赋值。其中,资产分类是指对文档信息、软件信息、云存储设施等所有的云计算平台资源进行列表;而资产赋值指的是根据列表中各种资产在待评估的信息系统里的重要程度,采取等级评定的方法对资产进行赋值,通常将资产的机密性、完整性和可用性这 3 个属性划分为 5 个等级,分别用 5、4、3、2、1 来表示很高、高、中等、低和很低。

(2) 威胁识别。包括威胁分类和威胁赋值。其中,威胁分类指的是根据相关报道或渗透检测工具对可能存在的安全威胁进行分类;威胁赋值即根据威胁发生的频率进行赋值。

(3) 脆弱性识别和赋值。包括脆弱性识别和脆弱性赋值。其中,脆弱性识别指的是对于不同的云计算平台以及不同的基础架构,根据其规模、计算平台的可审查性、数据隔离措施、数据位置、数据恢复措施、是否允许特权用户的接入等特性来识别可能引起安全事故的脆弱性;脆弱性赋值指的是对于一个给定的脆弱性,通常用 0 和 1 来表示其不存在或存在。

(4) 风险评估和分析。即分析威胁和脆弱性的关联关系,得到安全事件发生的可能性。在进行风险评估和分析时,首先要确定哪些资产受到了影响,然后计算安全事件发生后的损失。

风险的级别是根据事件发生的可能性和造成损失的大小来评估的。事件发生的可能性指的是攻击者利用漏洞成功实施攻击的概率。每个事件发生的可能性和业务上造成的损失是由参与评估的专家小组根据经验共同给出的。

在云计算的安全风险评估中,不仅要比较和分析存储在不同位置的数据的风险,还要

比较和分析存储在自己可控范围内的数据的风险。另外，合规性也是风险评估的一个方面，例如，用户在工作中给其他人发送电子文档时必须遵守存储在云中的电子文档的安全规范。云计算的安全风险一般会随着云架构的不同而发生较大的变化，同时风险还与云服务的价格有关。

为了评价国内组织的云安全管理能力成熟度，赛宝认证中心与云安全联盟（CSA）针对我国云计算环境推出了 C-STAR 评估业务，并在信息安全工程能力成熟度模型（SSE-CMM）的基础上，结合 C-STAR 云安全管理评估自身的特点，开发了 STAR 云安全管理能力成熟度模型。下面简要介绍 SSE-CMM 信息安全工程能力成熟度模型以及 C-STAR 云安全管理能力成熟度模型。

3.3.2 SSE-CMM 模型

SSE-CMM 模型将系统安全工程划分为 3 个可以独立加以考虑的基本过程，分别是风险过程、工程过程以及保证过程，如图 3-3 所示。这 3 个过程共同实现了安全工程过程结果所要达到的安全目标。具体来说，在最简单的级别上，这 3 个过程的关系是：风险过程识别出所开发的产品或系统的危险性并对这些危险性进行优先级排序；针对风险过程得出的危险性所面临的问题，工程过程将会与其他工程一起来确定和实施解决方案；最后，保证过程将建立解决方案的可信任度并向顾客传达这种信任。

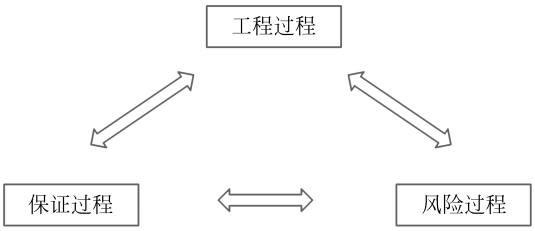

图 3-3　系统安全工程的 3 个过程

SSE-CMM 是安全工程实施的标准度量标准，它汇集了工业界常见的实施方法，其内容覆盖了以下方面：

（1）整个生命周期，包括开发、运行、维护和终止、

（2）整个组织，包括其中的管理、组织和工程活动、

（3）与其他规范并行的相互作用，包括系统、硬件、软件、测试工程、系统管理、运行和维护等。

（4）与其他机构的相互作用，包括获取、系统管理、认证、认可和评价等。

SSE-CMM 的模型包含域和能力这两个维度。其中，域维由所有定义安全工程的过程域构成；能力维则由过程管理和制度化能力构成，代表组织能力。在 SSE-CMM 模型中包含了对模型原理和体系结构的全面描述、对模型的高层描述、在该模型中的实施以及对模型属性的描述等。

SSE-CMM 包含了 5 个能力级别。其中，能力级别 1 是非正式级，该级别着重于一个组织或项目执行了包含基本实施的过程；能力级别 2 是计划和跟踪级，该级别着重于项目

层面的定义、计划和执行问题；能力级别 3 是充分定义级，该级别着重于规范化地裁剪组织层面的过程定义；能力级别 4 是量化控制级，该级别着重于与组织业务目标紧密联系在一起的测量；能力级别 5 是连续改进级，该级别从前面各级的所有管理活动中获得发展的力量，并通过加强组织文化来保持这个力量。

3.3.3　C-STAR 模型

C-STAR 云安全管理能力成熟度模型用于评价组织的云安全管理能力成熟度，该模型可以评估被评估方的云安全管理能力，并且能为被评估方的云安全管理体系的改进提供方向和指引。C-STAR 评估项目采用中立性评估模式，对云服务安全性开展缜密的第三方独立评估，并充分运用信息安全管理体系标准以及 CSA 云控制矩阵来帮助云服务提供商满足云用户对于云安全性的特定需求。

C-STAR 的评估一般从以下方面展开：应用和接口安全、电子证据及云端调查取证、业务连续性管理和操作弹性、变更控制和配置管理、人力资源、数据安全和信息生命周期管理、数据中心安全、加密和密钥管理、审计保证及合规性、治理和风险管理、基础设施和虚拟化安全、互操作性和可移植性、移动安全、安全事件管理、供应链管理、透明性及责任、身份识别和访问管理、威胁和脆弱性管理。

应用 C-STAR 模型判定某项控制措施在对应控制域中所处的能力级别的流程如下：分析各条控制措施及与之关联的管理过程中的管理、测量和制度化，判定其表现出的特征是否满足某一能力级别要求，如果满足，则可判定其处于该能力级别。

依据 GB/T 20274.3—2008《信息安全技术 信息系统安全保障评估框架》第 3 部分：管理保障以及 SSE-CMM 信息安全工程师能力成熟度模型，并且结合 C-STAR 云安全管理评估自身的特点，C-STAR 云安全管理能力成熟度可以划分为以下几个级别：

能力级别 0：未实施。该级别的云安全管理控制措施通常不能被成功执行，云安全管理控制措施的工作成果或记录无法证明云安全管理控制措施基本执行。

能力级别 1：基本执行。该级别的云安全管理控制措施基本被执行，但控制措施的执行可能未经过严格的计划和跟踪，其执行依赖于云服务提供商工作人员的个人意识，工作的质量和性能存在着不稳定性以及重复性。

能力级别 2：计划和跟踪。这一级别对云安全管理控制措施进行了良好的规划，建立了覆盖云安全管理的信息安全策略、程序和管理制度、实施手册和指南 3 层信息安全管理体系，注重组织标准管理的制度化。

能力级别 3：充分定义。该级别根据制定的涵盖云安全管理的信息安全管理体系，能够切实进行云安全管理工作，完整实施 CMM 云安全控制矩阵所涵盖的云安全管理体系。该级别的安全管理保障控制措施的实施中有充分定义的管理，注重充分定义的管理的可重复执行。另外，该级别还能够进行包括组内、组间以及与外部组的沟通协调。

能力等级 4：量化控制。该级别能够为组织标准管理保障控制措施的实施效果建立可测量的评价标准，并收集、分析执行的详细记录数据。该级别能适当测量和跟踪管理保障控制措施的实施有效性，在管理与计划间有重大差距时能采取适当的修正措施。

能力等级 5：持续改进。该级别能基于组织的业务目标建立管理有效性和效率的量

化执行目标，通过过程执行以及试验性的新概念和新技术产生的量化反馈，实现基于这些目标的持续性过程的改进。

3.4 本章小结

云计算已成为全球 IT 领域关注和投入的重点领域，其安全问题更是成为关注的焦点。为了更好地保障云计算的安全，在实施安全防护技术手段之前，首先需要做好云计算安全标准化制定、确定好如何对云计算进行安全性评估等云安全管理工作。本章从云计算安全标准化、云计算安全管理工作以及云计算安全评估 3 个层面阐述了云计算安全管理方法，结合本章的分析介绍，读者可以在理论上对云计算安全管理有一个基本的认识。

从现有的云计算安全管理相关的标准化情况来看，目前国内外云计算安全相关的标准组织很多，目前已经形成了许多云计算安全标准成果，为云计算提供了安全管理保障。本章分别从国际和国内两个方面介绍了目前已有的云安全标准组织及其安全标准成果。其中，国际的部分介绍了云安全联盟(CSA)、欧洲网络与信息安全局(ENISA)、美国国家标准与技术研究院(NIST)等具有代表性的国际和国外标准组织及其相关工作，国内部分则介绍了全国信息技术标准化技术委员会、全国信息安全标准化技术委员会、CCSA 等国内标准组织及其相关工作。

本章的云计算安全管理工作部分主要从云计算风险管理、云计算安全基线管理以及云计算应急响应管理这 3 个重要的云计算安全管理领域展开介绍，这 3 个领域对于保证云计算中心的安全性及可持续性有着重要的意义。

云计算安全评估是对安全威胁的脆弱性暴露程度进行量化，其评估结果可以帮助用户在选择云服务提供商前根据自己所能承受的风险进行权衡。本章的云计算安全评估部分先对云计算的安全评估进行总体介绍，之后对 SSE-CMM 和 C-STAR 这两个云安全评估模型进行了介绍。

3.5 思考题

(1) 列举云计算安全管理方面的几个重要领域，并简要介绍这几个领域的内容。

(2) 简述云信息系统安全评估的流程。

(3) SSE-CMM 模型将系统安全工程划分成哪 3 个过程？

第 4 章 基础设施安全

4.1 基础设施安全概述

基础设施安全是云安全运行的基础，保证了计算机和网络的安全连接。基础设施安全包括计算、网络、存储等云计算资源的安全。物理设施、用户的配置和基础设施组件的实现是云计算中所有内容的基本组成部分。

在云计算中，基础设施有两个层面。第一个层面是汇集在一起用来构建云的基础资源，该层面用于构建云资源池的原始、物理和逻辑的计算、网络和存储资源，例如用于创建网络资源池的网络硬件和软件；第二个层面是由云用户管理的虚拟/抽象基础设施，该层面是指云资源池中的计算、网络和存储资源，例如由云用户定义和管理的虚拟网络。

计算、网络、存储资源等基础硬件设施的有效利用加快了云计算的发展，而虚拟化技术是云计算实现的关键技术，虚拟化技术包括计算虚拟化、网络虚拟化、存储虚拟化等，虚拟化技术提高了云计算资源的使用效率。然而，由于云计算环境与传统 IT 环境最大的区别是计算、网络和存储环境的虚拟化，所以许多传统安全防护手段无法得到有效执行，进而引起了较难控制的安全问题。因此，云计算环境中的基础设施安全是云安全的重中之重。

4.2 基础设施物理安全

强大、可靠的虚拟化和分布式计算技术推动了云计算模式的成功，其依赖于由计算、网络、存储等设备所构成的物理层。通常，云计算基础设施包括从用户桌面到云服务器的实际链路中所涉及的所有相关设备，因此，为实现全天候的可靠性，需要保障基础设施在物理层的安全。在云计算环境的物理安全中，基础设施所面临的安全问题可分为自然因素、运行威胁和人为风险这 3 个方面。接下来分别从这 3 个方面阐述物理安全风险和相应的防护措施。

4.2.1 自然因素

自然因素就是自然界中的不可抗力，例如地震、洪水等。自然因素往往难以预测，因此当设备损毁和链路发生故障时，会严重损坏云计算基础设施，同时伴随着用户数据、配置文件的丢失，应用系统在长时间内难以恢复正常运行。为增强云计算基础设施对自然因素的防御能力，可以考虑物理手段和技术手段这两方面。

1. 物理手段

在为云计算中心选址时，可以选择地理环境较好的地区，并且对建筑结构、抗震等级提出一定的要求，以减少或避免自然因素带来的损失；云计算中心还需考虑到基础设施在恶劣天气以及极端情况下的防护能力，例如是否能够有效抵御风暴，是否能够降低低温、高温、潮湿环境带来的影响；对于通信链路的防护，云计算中心可使用加固、深埋的方法来实现。

2. 技术手段

自然因素所造成的基础设施的损坏，很容易使云计算服务出现部分或完全中断的情况，从而造成较为严重的后果。因此，保证业务的连续性显得尤为重要。通过在不同地点建立多个备份和处理中心，可以有效地保证业务的连续性，一旦某个地点的设备发生故障，能够较快恢复服务的正常运行。

4.2.2 运行威胁

运行威胁指云计算基础设施在运行过程中由于直接或间接原因导致的安全问题。运行威胁会使云服务性能下降，甚至造成服务中断和数据丢失，因此，必须采取一定的防护措施来保障云基础设施，从而在物理层面保障云计算中各类资源的安全。接下来主要从能源安全和设备安全两方面考虑运行威胁的防护措施。

1. 能源安全

云计算环境中的能源安全分为能源供应安全和能源消耗安全。

对于能源供应安全问题，电力是所有电子设备运行的必备条件，而在云计算环境中，各类集群规模和业务负载对电力供应的要求各有不同。因此，为保证在意外断电情况下云计算基础设施依旧能够正常运行，云计算中心需根据不同设备的供电需求配备相应的紧急电源和不间断电源系统。其中，紧急电源包括发电机和一些必要装置，不间断电源包括蓄电池和检测设备等。虽然该措施能够有效应对意外断电的情况，但是仍需立即进行电力修复以降低临时能源耗尽所带来的损失。

对于能源消耗安全问题，由于服务器容量较大，集成度较高，云计算环境会消耗大量能源，因此设备和部件温度也会随之上升，从而引发系统性能下降甚至宕机等安全隐患。因此，需要在云计算环境中配备冷却系统，冷却系统需要具备全时、高效、稳定的制冷能力，并且能够在保持室内温湿度均衡的条件下提高能效比，优化电力利用率。除此之外，灰尘也会影响基础设施的能源利用率，因此需对云计算环境实施一定的除尘净化措施。

2. 设备安全

任何系统的运行都会造成设备的损耗，云计算中的磁盘阵列、内存、CPU 的使用寿命是有限的，一旦设备因损耗而发生故障，将会造成业务的中断。特别是云计算中的磁盘阵列长期处于高负荷运行状态，因此需要经常对其进行分布式冗余处理，从而保证数据可以完全恢复。同时，为了能及时处理紧急事件，可根据需要配备一些常用的备件。

4.2.3　人为风险

人为风险主要是指由云服务提供商内部人员或外部其他人员威胁到云计算环境安全的行为对云计算环境造成的风险。由于人为风险一般无法立即被发现，因此需要预先设定一系列防护手段。人为风险可分为员工误操作和恶意攻击。

1. 员工误操作

在云日常管理中，云服务提供商内部人员由于不熟悉操作方法而造成功能误用，进而使云服务提供商或用户数据受到损失。因此，需对员工进行相关技术培训，并建立责任人制度，让员工明白自己每一步操作产生的影响和后果。

2. 恶意攻击

恶意攻击包括物理入侵和技术入侵。物理入侵就是合法或非法人员在云计算基础设施的部署场所进行恶意操作，可使用传统的物理方法进行有效防御，例如门禁、视频监控等，也可配备安全警卫。技术入侵就是利用网络攻击手段入侵系统，从而威胁系统安全。社会工程学攻击是入侵系统成功率较高的一种方法。社会工程学是指攻击者利用人类心理骗取受害人员的信任，在取得信任后请求执行搜集用户信息、了解系统运行状况等操作，从而实现非法、越权操作，进而危害系统安全或造成数据信息泄露。因此，云计算中心需严格执行身份认证等安全策略，以保证系统安全。

4.3　基础设备虚拟化安全

4.3.1　设备虚拟化概述

虚拟化技术是云计算发展的关键。云计算中的虚拟化主要是对云计算环境中资源的逻辑表示。虚拟化为计算资源、存储资源、网络资源等其他资源提供了一个逻辑视图，简化了资源的访问和管理过程。

利用虚拟化技术可以对计算机资源进行抽象整合，它屏蔽了物理硬件的复杂性，仿真、整合或分解了现有的服务功能，同时增加或集合了新的功能。接下来主要介绍网络设备虚拟化技术。

网络设备虚拟化技术的应用可以实现网络资源灵活扩容、按需分配，从而有效提高网络系统可靠性，减少网络故障收敛时间，提高网络资源利用率，简化网络管理。支持虚拟化的网络设备有很多，例如交换机、路由器、防火墙等。常见的网络设备虚拟化技术基本上可以分为 3 类：N ∶ 1 虚拟化横向堆叠技术、N ∶ 1 虚拟化纵向堆叠技术、1 ∶ N 虚拟化。

1. N ∶ 1 虚拟化横向堆叠技术

横向堆叠技术通常指的是把多个同一类型的设备通过特定的链路连接起来，在逻辑上作为一个设备使用。横向堆叠的网络架构与传统的网络架构相比具有以下 4 个优势：

(1) 简化了协议配置。

使用虚拟化技术后,多个成员设备在逻辑上成为一个设备,从而简化了设备管理,管理员对虚拟的逻辑设备管理进行配置即可,并且在配置文件中取消了单一网关的使用,因此无须配置多个 IP 地址。

(2) 避免环路的出现。

虚拟化技术使多个设备在逻辑上成为一个设备,避免了逻辑环路的出现,并且不再使用生成树协议和虚拟路由冗余协议(Virtual Router Redundancy Protocol,VRRP),而是使用跨设备的链路聚合。

(3) 提高了网络资源利用率。

通过分布式跨设备链路聚合技术,使多条上行链路可以分担负载和互为备份。

(4) 提高了网络系统可靠性。

堆叠系统中的物理设备通过协议互为备份,当一个成员物理设备发生故障时,业务可以快速恢复,从而有效减少网络故障带来的损失。

横向堆叠技术的主要代表有 H3C 公司的 IRF 2.0 技术、Cisco 公司的 VSS 技术、华为公司的 CSS 技术、Juniper 公司的 Virtual Chassis 技术等。

2. *N*∶1 虚拟化纵向堆叠技术

与横向堆叠技术相比,纵向堆叠技术不是对相同角色的设备进行堆叠,而是对在逻辑上不同位置的设备进行堆叠,例如对核心层的设备和接入层的设备进行堆叠等,从而在纵向上形成一个逻辑设备。

纵向堆叠技术按照设备角色可以分为控制设备和纵向扩展设备。控制设备也称控制桥(Controlling Bridge,CB),一般情况下 CB 相当于 CPU,集中控制和管理虚拟设备,PE 在逻辑上是一块远程接口板,也被称为端口扩展器(Port Extender,PE),相当于扩展 I/O 接口,在堆叠系统中由 CB 对其进行集中控制管理。纵向堆叠技术具有以下 3 个优势:

(1) 多级可靠性。

第一级使服务器跨 PE 冗余接入,第二级使 PE 能够跨板甚至跨框聚合接入 CB,从而实现了网络冗余的多级可靠性。

(2) 可扩展性。

纵向堆叠技术的可扩展性体现在两个方面,分别是 CB 可扩展性和 PE 可扩展性。其中 CB 可扩展性指 CB 通过横向堆叠的方式扩展,PE 可扩展性指 PE 可以根据需要接入纵向堆叠系统,从而可以使用不同设备的组合进行网络设备的扩容。

(3) 保护用户投资。

PE 设备支持的交换模式是标准交换模式和纵向堆叠 PE 模式,可通过命令行或者网管程序进行切换。其中纵向堆叠 PE 模式支持即插即用。用户可根据自身网络系统建设的需要选择交换模式,从而有效地保护用户投资。

纵向堆叠技术主要有 H3C 公司私有的 IRF 3.0、Cisco 公司私有的 FEX 等。公有技术有 IEEE 802.1BR,通过使用 PE 形成一个端口数目较大的网络设备。

3.1∶N 虚拟化

1∶N 虚拟化技术将一台物理设备虚拟为多台独立的逻辑设备，并且各逻辑设备均独占硬件资源。1∶N 虚拟化技术具有以下 3 个优势：

(1) 管理平面隔离。

在管理平面，每一个逻辑设备为一个独立设备，并具有单独的配置文件，能够独立进行逻辑设备的重启和加载配置。对于网管系统，通过对每一个逻辑设备进行标记，从而实现各逻辑设备网管信息的处理。对于用户，可通过专有命令直接登录逻辑设备进行配置以及使用各种管理功能。

(2) 数据平面隔离。

每个逻辑设备数据平面独立，使用支撑自身系统运行的硬件和软件资源，包括独立的接口、CPU 等。

(3) 故障隔离。

所有逻辑设备都有独立的进程和独立的网络转发数据，因此，通过合理的资源分配，可以有独立的转发芯片资源和 CPU 资源。一旦某一逻辑设备发生故障，可以将故障控制在本逻辑设备内而不影响其他的逻辑设备，从而实现故障隔离。

1∶N 虚拟化技术主要有 H3C 公司的 MDC 技术、Cisco 公司的 VDC 技术等。

4.3.2　虚拟设备的挑战

在云计算环境中，由于物理设备无法插入，所以除了使用云服务提供商提供的设备资源之外，如果仍然需要增加设备，就必须使用虚拟设备来替代，这也给云计算的发展带来了安全挑战。

(1) 虚拟设备可能占用大量的资源，并且有可能通过增加成本来满足所需的网络性能要求。

(2) 虚拟设备在使用过程中应该支持自动缩放以匹配它们所保护的资源弹性。如果云服务提供商无法根据产品类型提供与自动缩放相兼容的弹性许可证支持，就可能导致一系列的安全问题。

(3) 虚拟设备需要考虑到在云中的操作以及实例在不同地理区域和可用区域之间的移动能力。由于云网络的变化速度快于物理网络，因此需要设计特定的工具来有效地处理这一重要差异。

(4) 在云计算环境下，为了提高弹性，云应用程序组件趋向于分布式。同时由于虚拟设备的自动缩放能力，虚拟服务器使用寿命更短、数量更多。针对这一改变就要设计相应的安全策略，一方面安全工具必须能够管理更高的虚拟设备变化率，另一方面安全工具还需要考虑到云中的 IP 地址改变速度将明显快于传统网络。云资产不太可能使用静态 IP 地址，不同云的云资产可以在短时间内共享相同的 IP 地址。必须修改告警和事件响应生命周期，以确保告警在这种动态环境中是可操作的。单个应用程序层中的资产常常位于多个子网上以提高弹性，从而使基于 IP 的安全策略更加复杂。

4.4 本章小结

基础设施安全是云安全的基础，只有在基础设施层面保障云计算资源的安全，才能为上层应用的可靠运行提供底层保障。本章首先介绍了云计算基础设施的基本概念，从而引出了基础设施安全在云计算中的重要性；其次阐述了基础设施在物理层面的安全威胁以及防护措施，包括自然因素、运行威胁和人为风险这 3 个方面；最后介绍了基础设备虚拟化安全的基本概念以及虚拟化设备所面临的挑战。

本章在介绍基础设备虚拟化安全时侧重介绍了网络设备虚拟化技术，包括设备虚拟化特点、虚拟化对象以及常见设备虚拟化技术。常见网络设备虚拟化技术分别是 N ∶ 1 虚拟化横向堆叠技术、N ∶ 1 虚拟化纵向堆叠技术和 1 ∶ N 虚拟化，并分析了虚拟设备带来的安全挑战以及应对措施。

4.5 思考题

(1)基础设施在物理层面所面临的安全问题可以分为哪 3 类？

(2) 基础设施所面临的运行威胁包括哪两个方面？分别阐述应对措施。

(3) 网络设备虚拟化技术可分为哪 3 类？分别进行阐述。

(4) 纵向堆叠技术具有哪 3 个优势？给出 3 个具有代表性的纵向堆叠技术。

(5) 简述虚拟设备带来的 4 个安全挑战。