国家信息中心
State Information Center

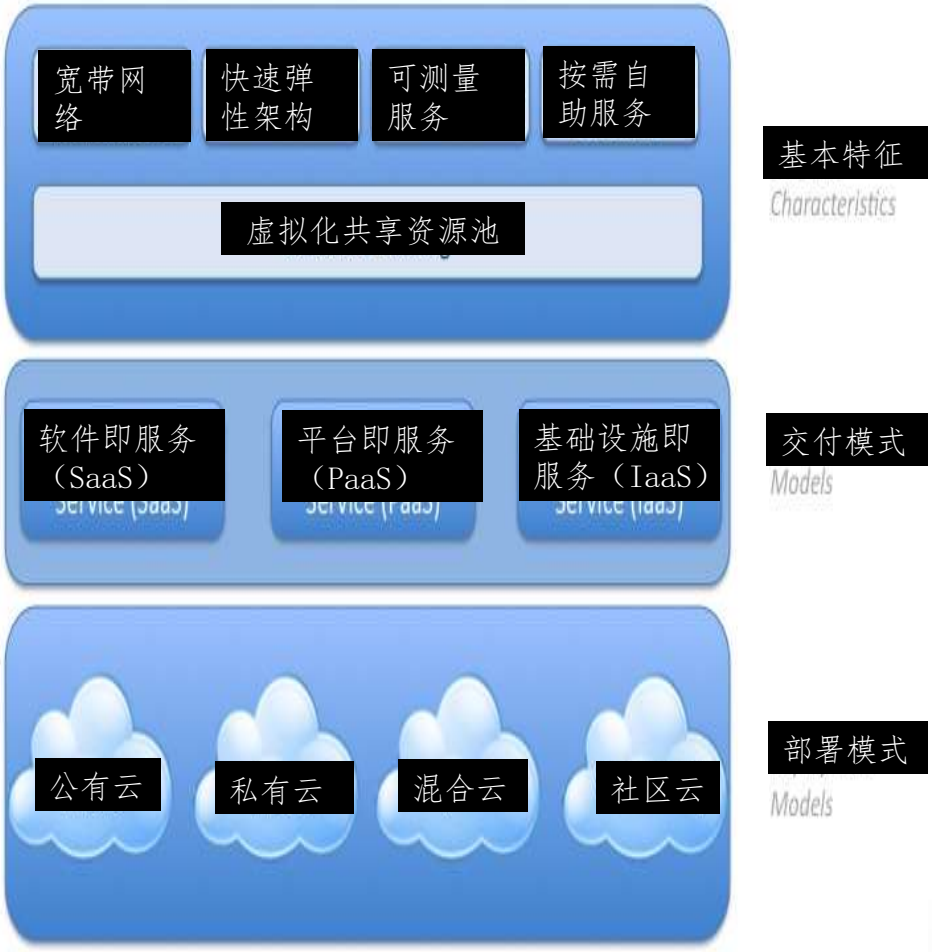
# 构建云计算环境的安全检查与评估指标体系

国家信息中心 章恒

2014年11月5日

# 云计算

美国国家标准技术研究院（NIST）对于云计算的定义




1. 安全现状
2. 规划、标准、要求
3. 指标体系的构建
5. 安全工作思考

## 安全事件

| 序号 | 时间 | 公司 | 服务项目 | 严重程度 | 持续时间 | 原因 | 后果 |
|---|---|---|---|---|---|---|---|
| 6 | 2013年1月 | Dropbox | 在线存储服务 | 高 | 16小时 | 未声明 | 在线存储服务中断 |
| 7 | 2013年1月 | 亚马逊 | Amazon.com主页出故障 | 高 | 49分钟 | 内部问题 | 主页无法正常显示，错失近500万美元的收入 |

北京时间9月1日早间消息，周日晚间，包括美国众多女星裸照在内的许多明星照片开始在美国网站和Twitter上流传。

俄罗斯Elcomsoft公司已开发出一款工具，在无需用户Apple ID帐号的情况下即可收集iCloud上的备份文件。这一工具能帮助司法部门分析被搜查的计算机。

号称“***高可靠、弹性、冗余***”的云服务实际上并不可靠!

# 安全现状

## 1、国外云服务安全事件已处于高发态势，且出现较多造成重大影响的事件，而我国云服务安全事件数量少、危害轻。

■2013年，国外三大云服务商亚马逊、微软、谷歌均出现至少两次以上的大规模服务中断事故。同年，苹果的iCloud服务发生多次故障。

■差异原因：国内外云服务规模和所处阶段不同。我国云服务市场规模甚至不及亚马逊一家企业的1/3，我国云服务发展水平较发达国家落后3～5年。

## 2、在我国，针对云服务的DDoS攻击还较普遍，国外则较少。

■ 原因：一方面主要跟我国相关法律法规还不太健全有关系，国外DDoS攻击就很少，因攻击者将承担很大的法律责任。

■另一方面，国外云服务面临的黑客攻击已不再是常规的DDoS攻击，而是水平更高的攻击方式，造成的后果也更严重。

## 3、国外云服务网络安全问题大部分也是传统问题，这与我国的情况是一致的

■ 国外：云服务安全事件有50%是传统网络攻击造成的，其次是软件漏洞和配置错误。

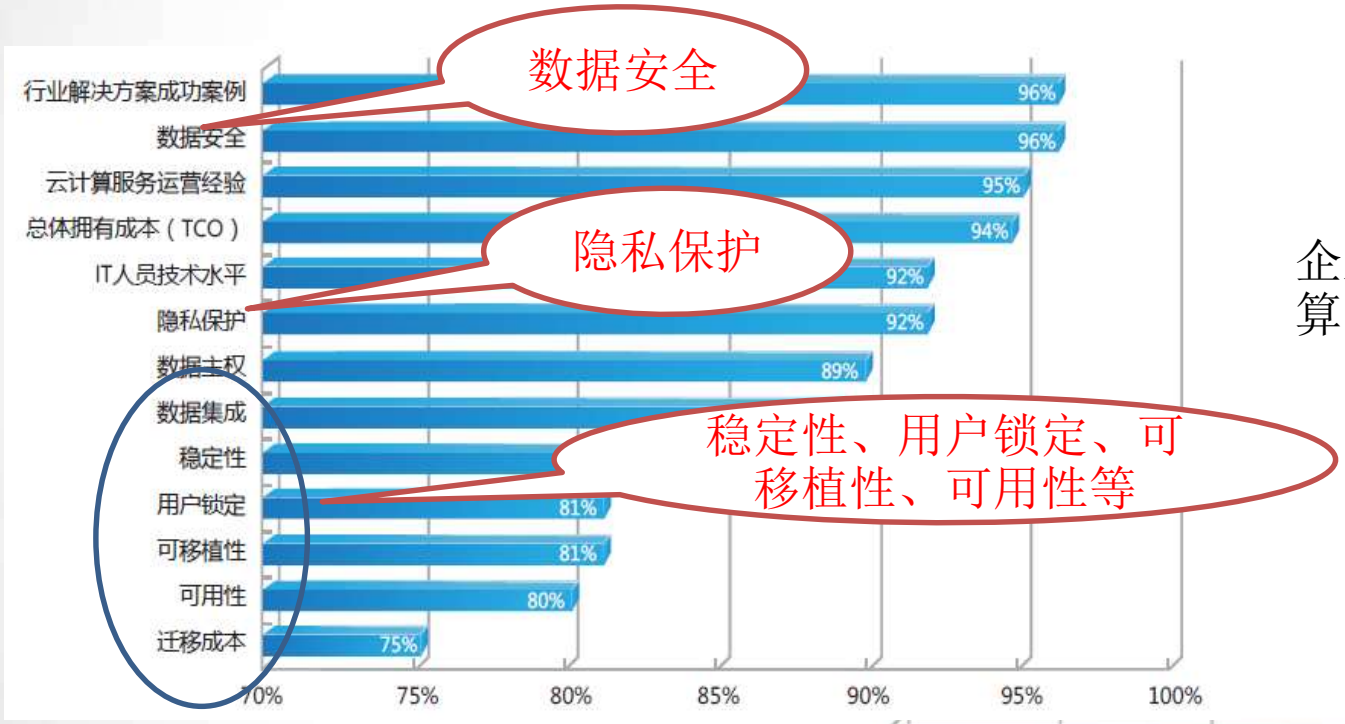
■ 国内：而据调查统计数据显示，国内典型云服务企业所发生的19次安全事件中有10次属于传统网络攻击造成的，占比达53%。

## 4、从国内外情况看，都是SaaS服务出现的安全问题最多，PaaS最少

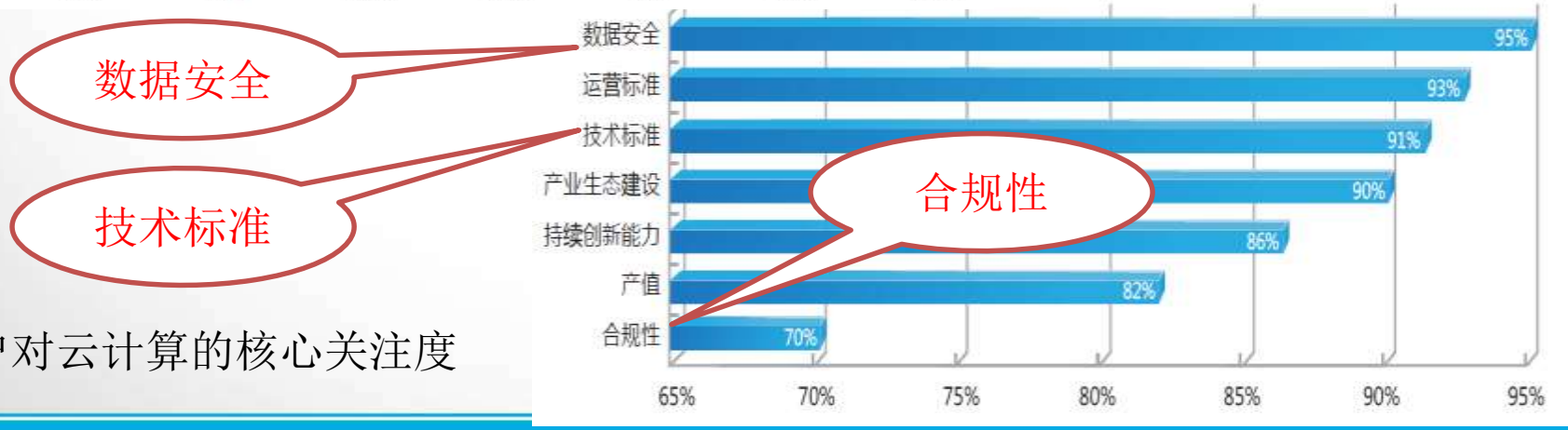
■ SaaS：国外公开报道的业界重大云安全事件中，有44%来源于SaaS服务。调查数据显示，我国SaaS服务企业暴露的安全问题占比超过50%。

■ PaaS：目前，提供PaaS服务的厂商不多，但PaaS市场热度正不断提高，未来PaaS将爆发出更多问题。

# 安全现状　　安全问题成为制约云计算产业发展的主要因素




企业用户对云计算的核心关注度




政府用户对云计算的核心关注度

# 安全现状

目前我国云服务规模较小，运行时间短，未经历大规模用户及服务环境的安全考验；
用户和服务商之间未建立起信任关系，信任问题是阻碍我国云服务发展的最核心问题；
云服务核心技术仍无法摆脱受制于人的境地，不掌握核心技术就是最大的安全隐患

## ▪专利数量

目前检索到的明确涉及云安全架构、云安全系统、云安全管理及云资源安全共享等与云服务安全明显相关的专利已达18000多件。

## 专利地域分布

美国在云服务安全领域的技术优势明显，已成垄断地位，该领域的专利申请量占比高达97%；其他国家在该领域的申请占比低。

## ▪专利企业布局

(1)传统IT领域的巨头企业微软、IBM和思科成为云服务安全领域的主要专利权人；
(2)浪潮、中兴通讯等国内企业成为我国云服务安全领域主要专利申请人。

# 国内外云安全战略规划

- 目前，世界各国政府和ICT企业还停留在发布云计算战略阶段，云安全战略规划很少涉及。

2012年3月，**新西兰政府发布全球首个云计算安全战略**（云计算保护行动），重点关注跨境云计算服务的保护措施，值得我国参考。

2012年9月，欧盟启动云计算战略规划，其中涉及云安全的有：支持在欧盟范围内开展“可信赖云服务供应商”的认证计划，为云计算SLA制定“安全和公平”模式下的合同条款。

2011年2月，美国《联邦云计算战略》指出在管理云服务时要主动监视和定期评估，确保一个安全可信的环境，并作出了战略部署，包括推动联邦风险和授权管理项目FedRAMP，成为美国联邦政府机构在采购云服务时的参考基准。

**国家科技部**2012年9月发布的《中国云科技发展“十二五”专项规划》即对云安全作出规划部署：支持身份认证、加密与隔离的硬件安全技术，研发相应安全防护产品与软件，突破运行监控与安全保障等重大关键技术。掌握云计算环境下用户身份管理技术以及云计算应用服务的安全防护和风险评估技术。

**相关主管部门：**发布的云计算发展指导意见：建设完善云计算安全保障体系。加强云计算环境下网络与信息安全监测，完善安全事件预警、态势感知和处置机制，强化云计算容灾备份和恢复能力。

# 国外相关标准

## 国际云安全标准机构和组织

- ISO/IEC 第一联合技术委员会(ISO/IEC JTC1)
- 美国国家标准技术研究所（NIST）
- 欧洲网络与信息安全管理局（ENISA ）
- 云安全联盟（CSA）
- 国际电信联盟--电信标准化部(ITU-T)
- 区域标准组织（美国）CIO委员会
- 开放式组织联盟（TheOpenGroup）
- 结构化信息标准促进组织（OASIS）
- 分布式管理任务组（DMTF）

已制定

- **ISO/IEC JTC1：**《开放虚拟机格式》、《云计算安全与隐私管理系统》、 ISO/IEC 27017 《基于ISO/IEC 27002的云计算服务的信息安全控制措施实用规则》、 ISO/IEC 27018 《公共云计算服务的数据保护控制措施实用规则》、 ISO/IEC 27036-4 《供应商关系的信息安全—第四部分：云服务安全指南》、 ISO/IEC 27009 《ISO/IEC 27001在特定行业/服务的认可的第三方认证中的使用和应用》
- **NIST ：**《云计算参考体系架构》、《完全虚拟化技术安全指南》、《云计算安全障碍与缓和措施》、《公共云计算中安全与隐私》、《通用云计算环境》、《美国政府云计算安全评估与授权的建议》（FedRAMP）
- **ENISA：**《云计算——信息安全保障框架》、《云计算——信息安全的好处，风险和建议》、《政府云的安全和弹性》
- **CSA：** 《云计算面临的严重威胁》、《关键领域的云计算安全指南》、《身份隐私与接入安全》
- **ITU-T ：**《云安全、威胁与需求》、《电信领域云计算安全指南》
- **CIO委员会：**《美国政府云计算风险评估方法》
- **TheOpenGroup：**《云安全和SOA参考架构》
- **OASIS：**《身份在云中的使用》
- **DMTF：**《云管理体系结构》

# 国内相关标准

## 中国通信标准化协会（CCSA）

中国通信标准化协会 China Communications Standards Association

- 2011年9月，在网络与信息安全技术工作委员会（TC8）的安全基础工作组（WG4）下成立了云计算安全子工作组，专门负责云计算安全方面的标准研发工作，目前该工作组已召开了三次会议，组织制定了多项云计算安全方面的标准和研究报告。
- **正在制定的标准有：**

- **在云计算的总体架构方面**，有《云安全标准体系研究》、《公有云安全基线要求》、《云计算安全威胁和需求》等；
- **在访问控制方面**，有《云计算身份识别与访问管理应用场景及技术要求》、《云计算的可信技术研究》等；
- **在云中隐私和数据保护方面**，有《公有云数据安全要求》、《公有云中隐私保护措施》等；
- **在行业云方面**，有《基于云计算的电子政务公共平台安全》、《基于云计算的居民健康服务平台安全框架》等；
- **在基于云计算的IDC方面**，有《基于云计算的互联网数据中心信息安全技术要求》和《基于云计算的互联网数据中心信息安全管理要求》；
- **在云计算应用安全方面**，有《云计算应用安全运营技术要求》等。

## 全国信息安全标准化委员会（TC260）

全国信息安全标准化技术委员会 HTTP://WWW.TC260.ORG.CN

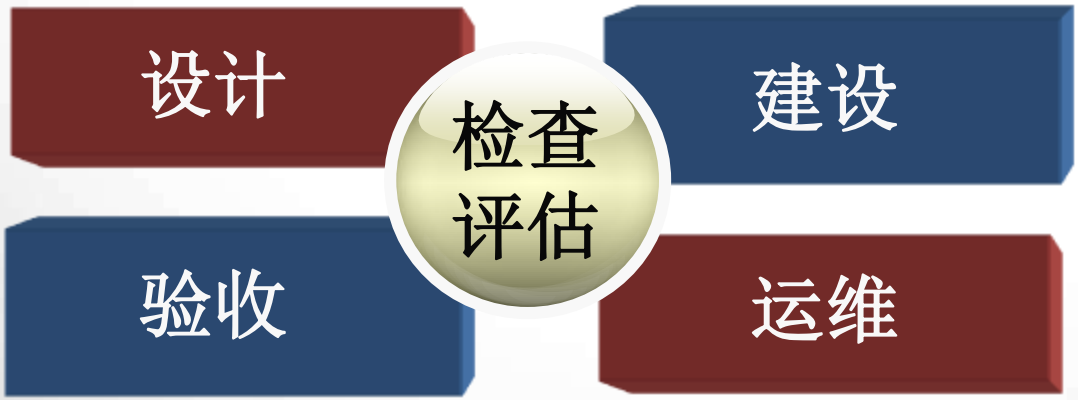
- 在信安标委内部立了专门对云计算及安全进行研究的课题，包括：《政府部门云计算服务提供商安全基本要求》、《政府部门云计算服务安全指南》和《政府部门云计算服务安全能力要求》等。

## 等保评估中心、国信中心、阿里云等

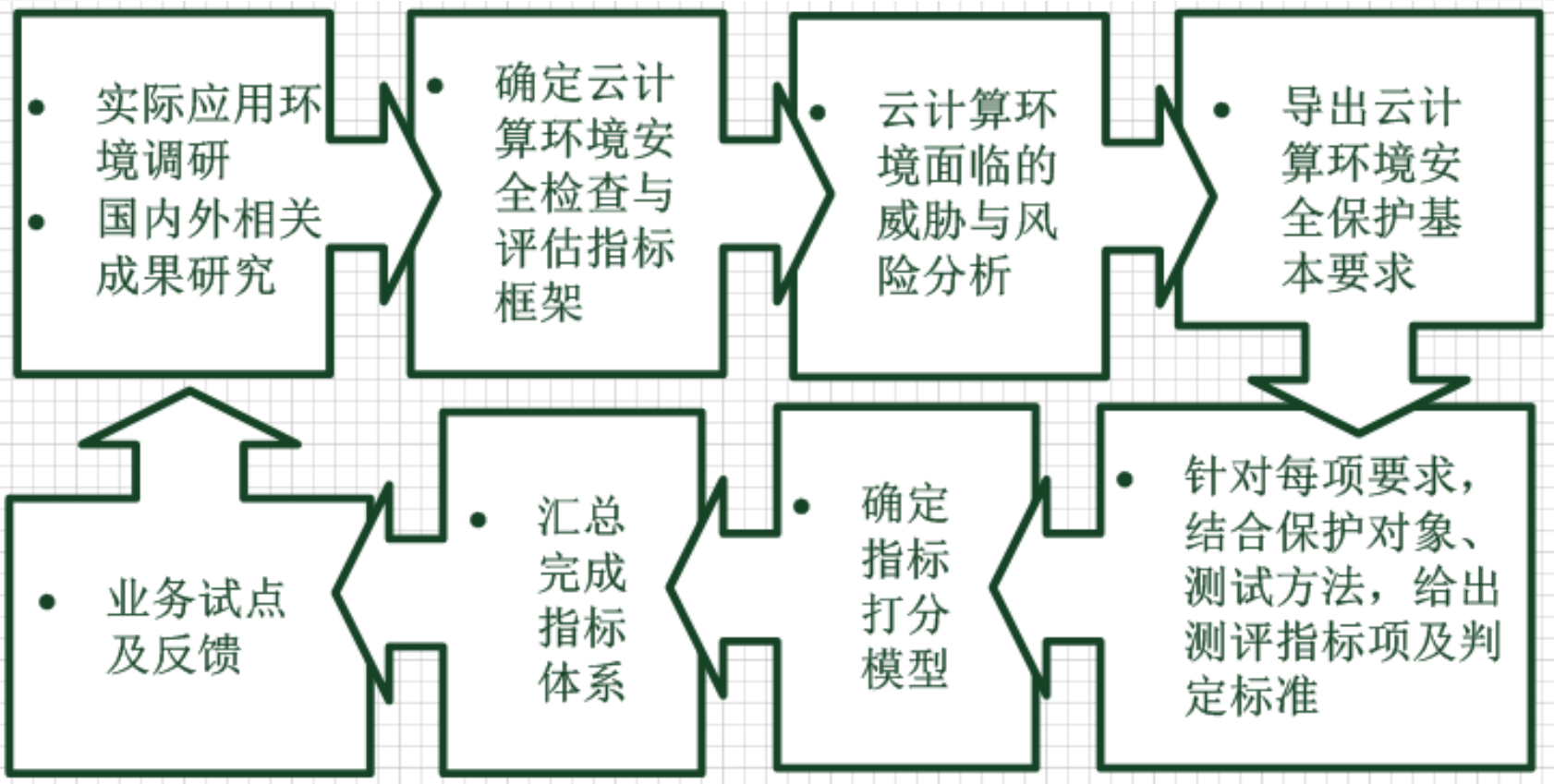
- 云计算信息系统安全等级保护基本要求》、《云计算信息系统安全等级保护测评要求》、《云计算信息系统安全等级保护设计技术指南》。

# 国家相关政策要求

- 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）
- 《关于开展信息安全风险评估工作的意见》（国信办[2006]5号）
- 《国家电子政务工程建设项目管理暂行办法》（发改委55号令）
- 《关于加强和完善国家电子政务工程建设管理的意见》（发改高技[2013]266号）



# 指标体系的构建


实际应用环境调研
国内外相关成果研究
确定云计算环境安全检查与评估指标框架
云计算环境面临的威胁与风险分析
导出云计算环境安全保护基本要求
针对每项要求，结合保护对象、测试方法，给出测评指标项及判定标准
确定指标打分模型
汇总完成指标体系
业务试点及反馈

# 实际环境及应用调研

服务 | 架构 | 方案 | 设备 | 用户 | 安全措施 | 事件

## 关心的问题

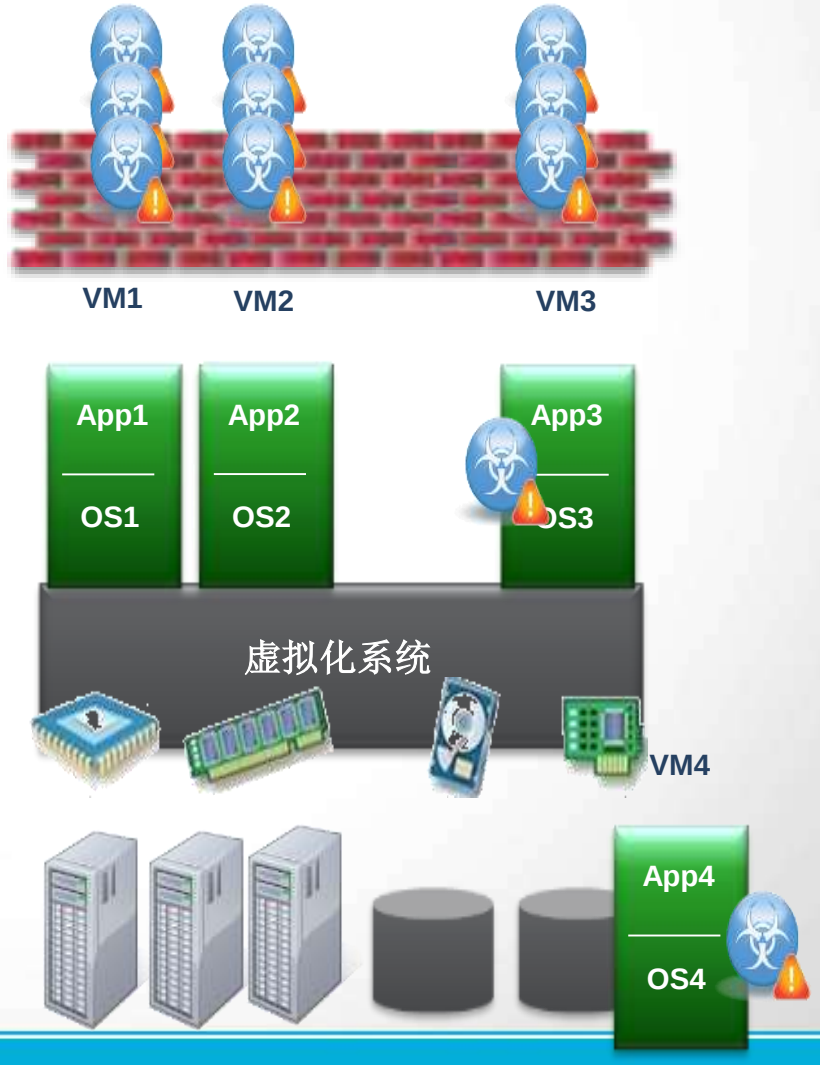
- 虚拟化厂商没有把接口完全开放，在vSwtich网间流量方面的问题：如何控制南北流量问题和东西流量问题？如何做到云平台中的所有流量的监控?
- 虚拟机在迁移情况下如何做安全防护？
- 云计算信息系统的边界划分问题，如何做好云计算信息系统的边界划分？
- 桌面云中每个虚拟机在进行文件备份时，是如何实现增量备份的？
- 传统架构的安全防护和云计算环境下的安全防护的区别？
- 如何做好传统信息系统入云前的安全检查测试，入云后的安全防护？
- 云和服务器虚拟化的区别？
- 混合云中如何做好安全防护？
- 如何做好虚拟机的安全访问控制？
- 如何做好虚拟机间的安全隔离的？
- 如何防范虚拟机的逃逸？
- 如何能防止虚拟机的内存数据不被窃取？
- 是如何来实现虚拟机加固的？

# 虚拟化安全实例

- 云计算信息系统的核心是采用**虚拟化技术**实现**资源池化**和**动态配置**；
- 虚拟化技术也是云计算信息系统诸多优势得以实现的关键因素；
- 虚拟化技术为云计算信息系统的安全增加了额外的一层安全要求；
- 云计算信息系统的安全防护需要着眼于虚拟化技术所带来的安全风险：
  - •虚拟机监视器（VMM）的安全风险
  - •虚拟资源共享风险
  - •多租户应用中的数据安全风险

## 虚拟化后的状况

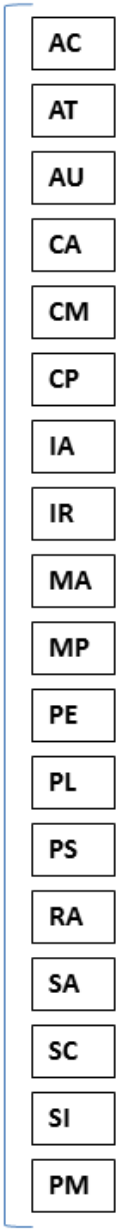
所有虚拟机共享资源
虚拟机和应用程序随时可能移动或变更

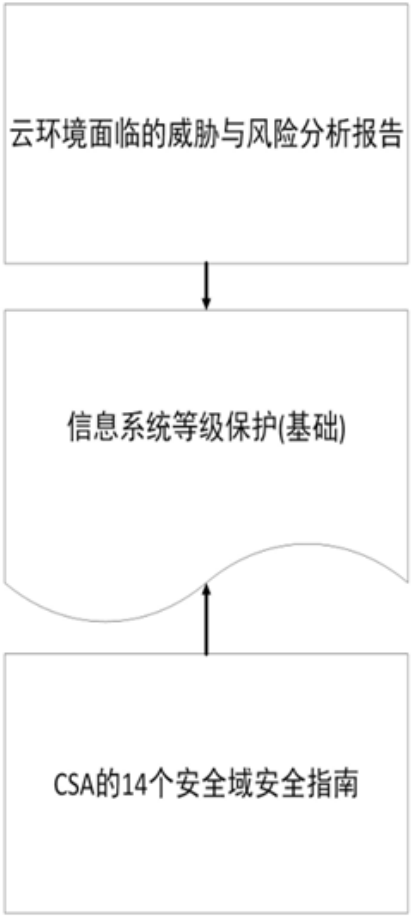


# 指标体系框架

一、二级目录参考CSA架构


三级目录参考（NIST.sp.800-53r4）



# 指标体系框架

## 三级目录参考

- **《云计算关键领域安全指南v3.0》提出三部分共14个关键域的安全指南**
  - D1：云计算体系架构
  - D2：治理与企业风险管理
  - D3：法律问题：合同与电子发现
  - D4：合规与审核
  - D5：信息管理与数据安全
  - D6：互操作性与可移植性
  - D7：传统安全、业务连续性和灾难恢复
  - D8：数据中心运行
  - D9：事故响应
  - D10：应用安全
  - D11：加密与密钥管理
  - D12：身份、授权和访问管理
  - D13：虚拟化
  - D14：安全即服务 SecaaS

# 风险分析

| 网络安全风险来源 | 风险种类 |
|---|---|
| 虚拟机与外部系统之间进行通信 | 网络攻击，如DoS攻击、网络监听等 |
| | 传统网络安全防护边界消失 |
| 虚拟机之间进行通信 | 恶意虚拟机进行网络攻击 |
| | 虚拟机共享物理网卡引起安全风险 |

| 主机安全风险来源 | 风险种类 |
|---|---|
| Hypervisor | 恶意代码通过应用程序接口（API)进行攻击 |
| | Hypervisor的访问权限被非法用户获取 |
| | Hypervisor自身存在安全漏洞 |
| 虚拟机 | 安全风险扩散 |
| | 虚拟机之间的相互攻击 |
| | 基于主机的安全策略难以部署 |
| | 资源冲突 |

| 虚拟桌面的安全风险来源 | 具体风险 |
|---|---|
| SaaS提供商 | 多租户架构下的应用隔离 |
| | 补丁管理复杂 |
| 用户 | 用户在虚拟桌面上自行安装软件 |
| | 客户端的外设端口引起数据泄露 |
| 传输链路 | 数据传输安全风险 |

- ➢ 网络安全风险来源
- • 虚拟机与外部系统之间的通信；
- • 虚拟机间相互通信；
- ➢ 主机安全风险来源
- • 虚拟机监视器（VMM)
- • 虚拟机
- ➢ 虚拟桌面的安全风险来源
- • SAAS提供商
- • 用户
- • 传输链路

| 应用安全风险来源 | 风险种类 |
|---|---|
| 应用的开发 | PaaS提供的开发环境不安全 |
| | 用户不明确PaaS提供的编程模型 |
| | PaaS提供的编程接口过于复杂 |
| 应用的部署 | 用户对应用及其运行环境的配置不当 |
| | 多租户应用无法安全隔离 |

| 数据安全风险来源 | 风险种类 |
|---|---|
| 数据存储 | 存储位置不确定 |
| | 数据难以有效隔离 |
| | 数据丢失 |
| | 数据残留 |
| 数据迁移 | 数据传输过程中的安全性难以保障 |
| | 数据安全迁移面临着很多技术难题 |
| 数据处理 | 组件失效 |
| | 处理速度过慢 |
| | 多用户并发访问 |
| | 服务器频繁增减 |

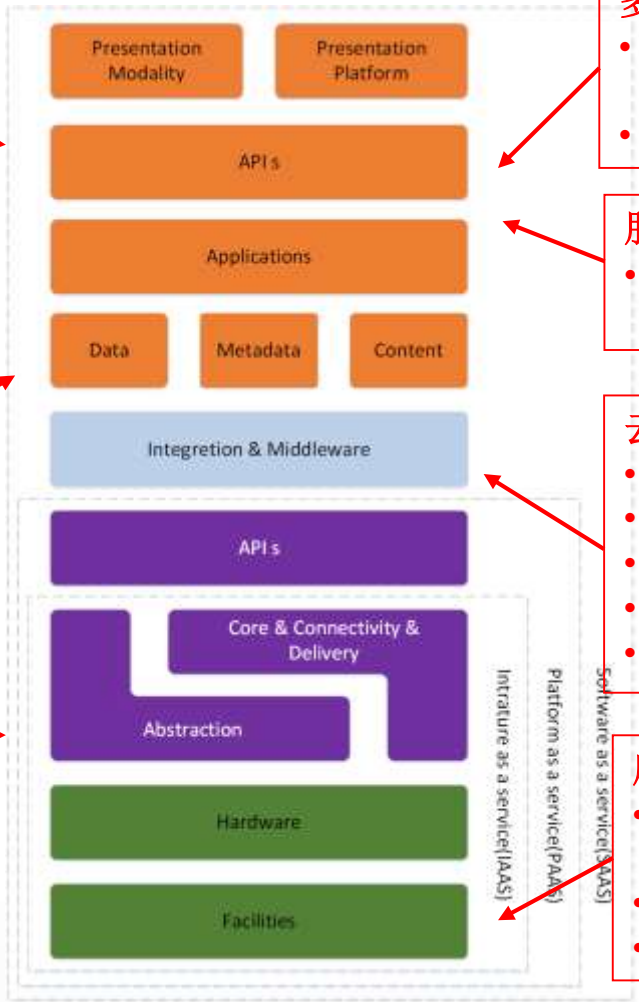
- ➢ 应用安全风险
- • 应用开发
- • 应用部署
- ➢ 数据安全风险来源
- • 数据存储
- • 数据迁移
- • 数据处理

# 安全措施

**云服务门户安全**
- 双向身份鉴别
- 传输加密
- 门户防DDOS攻击
- 门户防入侵
- 用户流量隔离(防流量渗入)

**数据安全**
- 数据隔离
- 数据完整性、保密性

**虚拟化安全**
- 虚拟机间的“溢出”监控与阻断
- 虚拟机流量识别
- 虚拟机迁移、操作日志审计
- 虚拟机内安全监控与用户行为审计、病毒过滤
- 虚拟化系统加固
- 虚拟机映像安全、数据安全




**多租户隔离**
- 多租户共享的情况下实现资源、环境、数据隔离
- 租户的身份认证、访问控制

**服务水平协议管理**
- 云服务内容、责任与权限、惩罚措施、服务能力监督

**云管理平台安全**
- 平台内部安全监控
- 管理行为审计
- 用户行为审计
- 云服务及接口安全
- 操作日志

**底层数据备份等**
- 多数据中心、多资源池的备份容灾
- 虚拟机备份与恢复
- 云存储备份与恢复

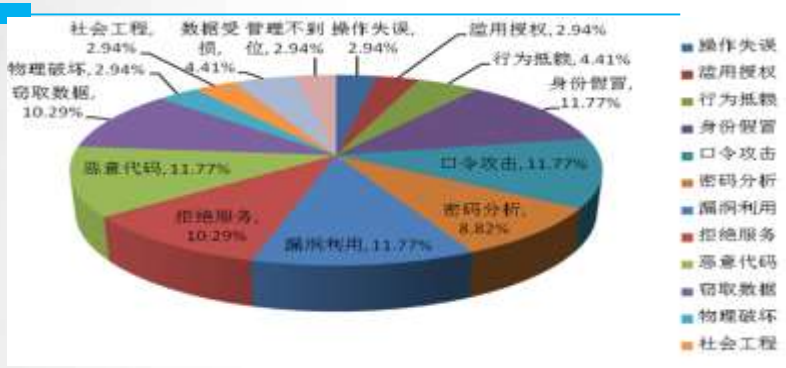
# 云计算环境安全保护基本要求的导出　　风险与指标项对照表

| 指标项（一级目录） | 指标项（二级目录） | 指标项对应的具体产品 | 指标项（三级目录） | 风险类型 | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 针对用户的技术风险 | | | | | | 针对提供商的技术风险 | | | | | |
| | | | | 身份假冒风险 | 共享风险 | 数据安全风险 | 客户端隐私风险 | 网络传输风险 | 失去控制器的风险 | 服务器端风险 | 服务中断/迁移风险 | 服务连续性风险 | 不安全的接口 | 人员管理风险 | 安 |
| 基础设施 | 物理环境 | 存储（san存储、iscsi存储、NAS存储）、服务器（小型机、X86刀片服务器、X86机架式服务器）、网络（负载均衡设备、防火墙、路由器、交换 | 访问控制 | √ | | | | | | | | | | √ | |
| | | | 安全审计 | √ | | | | | | | | | | √ | |
| | | | 物理环境的保护 | | | | | | | | | | | | |
| | 设备主机 | 小型机：IBM Power、HP Oracle sun T系列及M系列、曙光、；<br>X86机架式服务器：HP、IBM、Dell、oralce、天地超云、曙光、浪潮、联想、华为等；<br>X86刀片式服务器：HP、IBM、Dell、华为、天地超云、曙光、浪潮、联想等； | 身份鉴别 | √ | √ | √ | √ | √ | √ | | | | | √ | |
| | | | 访问控制 | √ | √ | √ | √ | √ | √ | √ | | | √ | √ | |
| | | | 系统与通信保护 | √ | √ | √ | √ | √ | √ | √ | √ | √ | | | |
| | | | 分布式处理和存储 | | | √ | √ | √ | √ | √ | | | | √ | |
| | | | 安全审计 | √ | √ | √ | √ | √ | √ | | | √ | | | |
| | | | 剩余信息保护 | | | √ | √ | | √ | √ | √ | √ | | | |
| | | | 入侵防范 | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | |
| | | | 恶意代码防范 | | | √ | √ | | √ | √ | √ | √ | | | |
| | | | 资源控制 | | | | | √ | | √ | √ | √ | √ | | |
| | | | 安全评估与授权 | √ | √ | | | √ | | √ | √ | √ | | | |
| | | | 配置管理 | √ | | | | √ | | √ | √ | √ | | √ | |
| | | | 介质保护 | | | √ | √ | √ | √ | | √ | √ | √ | | |
| | | | 风险规划 | | | | | | | | | √ | √ | √ | |
| | | | 应急计划 | | | | | | | | | √ | √ | √ | |
| | 网络 | 以太网交换机:思科、H3C、华为、锐捷、DCN、D-link、TP-link、艾泰、斐讯通信、TG-NET、优肯、Extreme、天伟通讯<br>光纤交换机：思科、博科、QLOGIC<br>防火墙：思科、H3C、锐捷、天融信、深信服、Juniper、网御星云、华为、飞塔、山石、启明星辰、DCN、网康、SONICWALL、艾泰、清华紫光、 | 访问控制 | √ | √ | √ | √ | √ | √ | √ | √ | √ | | | |
| | | | 系统与通信保护 | √ | √ | √ | √ | √ | √ | √ | √ | √ | | | |
| | | | 安全审计 | | √ | √ | √ | √ | √ | √ | √ | √ | | √ | |
| | | | 入侵防范 | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | |
| | | | 协同计算 | | √ | | | | | | | | | | |
| | | | 安全评估与授权 | √ | √ | | | √ | | √ | | √ | | | |
| | | | 配置管理 | √ | √ | | | | | √ | | √ | | √ | |
| | | | 应急计划 | | | | | | | | | √ | √ | √ | |

# 指标计算

- 所有的检查指标项均来源于相应保护对象所面临的安全风险项，因此打分的基础也是对相应风险项的赋值。
- 在总体框架下，保护对象分为3级，如：虚拟化层（1级）的主机虚拟化（2级）的访问控制模块（3级）。
- 针对每一保护对象的子类风险赋值主要从三个方面考虑：资产重要程度、对象的脆弱性以及外部威胁，其中，对象的脆弱性来源于检查的结果，资产重要程度及外部威胁来源于研究统计成果。
- 基础项赋值完成后，可以从纵向（保护对象架构）、横向（风险分类）采用分层分权计分模型，得出上层的分值。

# 指标计算




$$风险值 = R(V,T,A) = R\big(F(V,A),L(V,T)\big)$$

脆弱性指数 + 威胁修正指数 + 资产 = 风险指数

风险指数 + 风险指数归一化 + 指标打分 = 指标最后得分

$$F_n = \sqrt{脆弱性指数V \times 威胁修正指数T}$$

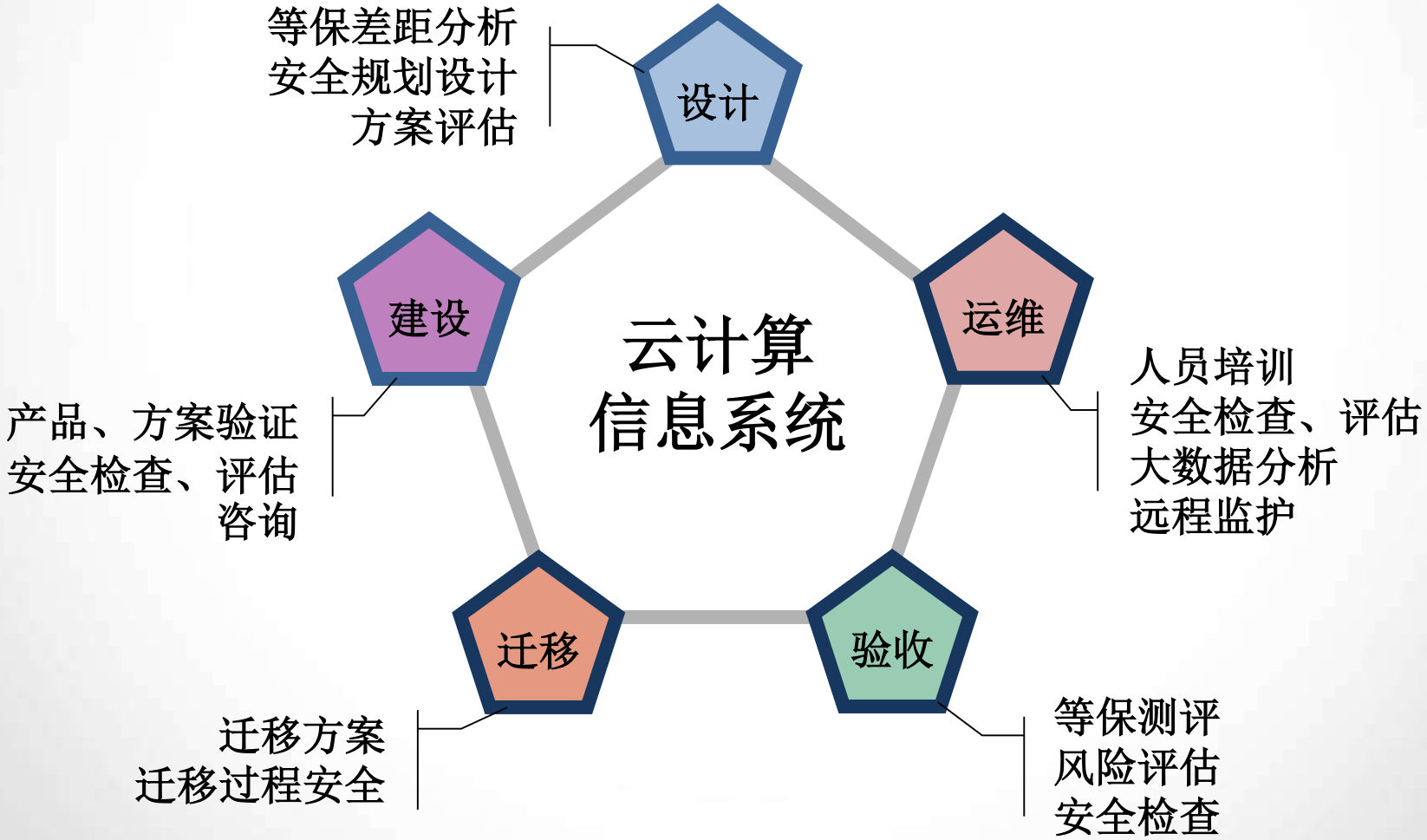
$$L_n = \sqrt{脆弱性指数V \times 资产价值A}$$

$$R_n = F_n \times L_n$$

$$RW_n = {R_n}\Big/{\sum_1^N R_i}$$

$$S_n = \left(\sum RW_i\right) \times S_n^{`}$$

# 安全工作思考


等保差距分析
安全规划设计
方案评估
设计
运维
人员培训
安全检查、评估
大数据分析
远程监护
建设
产品、方案验证
安全检查、评估
咨询
云计算
信息系统
迁移
迁移方案
迁移过程安全
验收
等保测评
风险评估
安全检查

# 安全工作思考

**试点目标**

1、摸清我国云服务存在的安全问题，特别是云计算带来的新安全问题，总结对应的解决措施；
2、为我国出台云服务安全标准奠定基础，也为后续的规划、政策、法律法规等方面提供准备；

**试点原则**

1、坚持以点带面，通过典型企业试点，归纳出整个云服务行业网络安全普遍问题和重点问题；
2、坚持同步进行，试点工作与企业运营服务同时开展，不另行搭建测试平台，不影响试点企业现有业务开展；
3、坚持分工协作和各有侧重，试点企业根据各自业务重点，着重关注各自服务领域内的相关安全问题；

**试点单位**

从30多家已开展云服务的运营商、互联网公司、安全厂商中选取5-6家典型云服务商，覆盖S/P/I三类；

国家信息中心
State Information Center

合作、发展、共赢

# 谢谢！

章恒
zhangheng@cei.gov.cn
13910271360

2014年11月5日