

网络信息安全周报

【2017】第 1 期

党委宣传部 信息网络中心 编

2017 年 3 月 2 日

本期要目

- 网络安全信息与动态（2017 年 2 月 13 日—2 月 19 日）
- 我国将依法启动网络安全审查
- 《信息产业发展指南》解读：云计算
- 小知识：关键信息基础设施的概念

网络安全信息与动态（2017 年 2 月 13 日—2 月 19 日）

根据国家互联网应急中心最新公告数据：

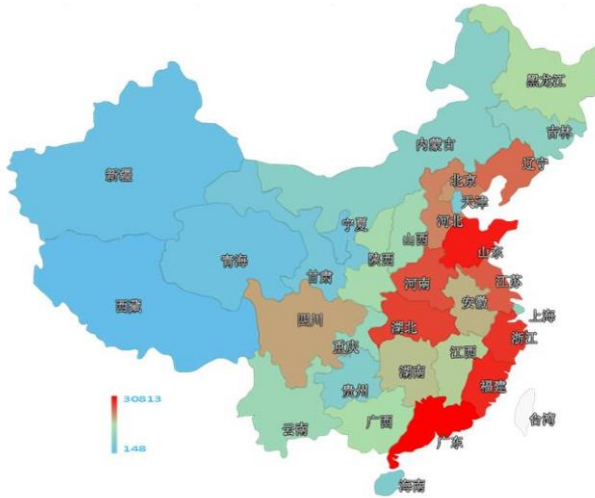
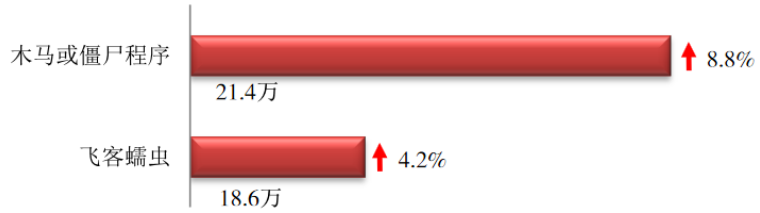
本周网络安全基本态势



— 表示数量与上周相同 ↑ 表示数量较上周环比增加 ↓ 表示数量较上周环比减少

本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 40.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 21.4 万以及境内感染飞客（conficker）蠕虫的主机约 18.6 万。



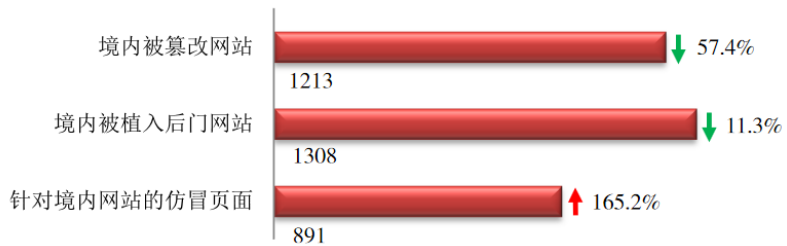
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、山东省和福建省。

TOP3



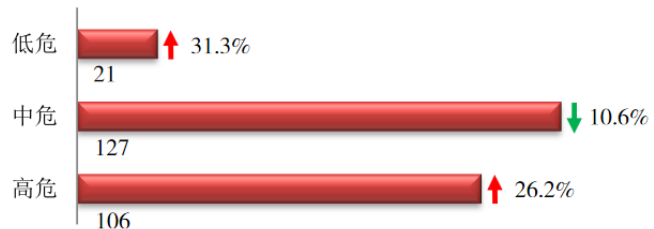
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1213 个；境内被植入后门的网站数量为 1308 个；针对境内网站的仿冒页面数量为 891。



本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 254 个，信息安全漏洞威胁整体评价级别为中。



我国将依法启动网络安全审查

2017-02-13 来源：中国信息产业网-人民邮电报 作者：天雨

2月4日，国家互联网信息办公室在其官网公开《网络产品和服务安全审查办法（征求意见稿）》（以下简称意见稿），明确将成立网络安全审查委员会，负责审议网络安全审查的重要政策，统一组织网络安全审查工作。专家表示，**网络安全审查针对的是“可能影响国家安全的，关键信息基础设施运营者采购的网络产品和服务”**。关键信息基础设施运营者采购的网络产品和服务是否影响国家安全，由关键信息基础设施保护工作部门确定。

意见稿开篇明确指出，网络产品和服务的安全审查法律依据来自《中华人民共和国国家安全法》《中华人民共和国网络安全法》。审查对象也是“关系国家安全和公共利益的信息系统使用的重要网络产品和服务”。审查机构由国家互联网信息办公室会同有关部门成立网络安全审查委员会，负责审议网络安全审查的重要政策，统一组织网络安全审查工作，协调网络安全审查相关重要问题。

意见稿要求，党政部门及重点行业优先采购通过审查的网络产品和服务，不得采购审查未通过的网络产品和服务。金融、电信、能源等重点行业主管部门，根据国家网络安全审查工作要求，组织开展本行业、本领域网络产品和服务安全审查工作。对此，中国信息安全研究院副院长左晓栋表示，网络安全审查不是常态性的，法律明确的是“关键信息基础设施的运营者采购网络产品和服务，并且可能影响国家安全的”。这意味着不是天天去审查，也不是对什么都要审查，更不是要去取代日常的产品安全测评。

此前，国家网信办网络安全协调局局长赵泽良也曾表示，网络安全审查不是普世性的，不是对任何产品和服务都进行审查，只是针对关系国家安全和国计民生的产品和服务进行审查。

有关专家指出，国家网络空间治理现代化的实质是一场制度革命。其中，网络安全审查制度占有极其重要的地位。纵观世界，网络安全审查早已是国际潮流和通行做法，美英俄印等大国早已出台相关规定与办法。

征求意见稿第六条规定：网络安全审查委员会聘请相关专家组成网络安全审查专家委员会，在第三方评价基础上，对网络产品和服务的安全风险及其提供者的安全可信状况进行综合评估。对此，四川大学网络空间安全研究院特聘副研究员洪延青告诉媒体，网络安全审查工作的组织和领导工作，由网络安全审查委员会承担，该委员会由国家网信办会同有关部门成立。委员会下设网络安全审查办

公室。此外，委员会还组建网络安全审查专家委员会。网络安全审查委员会、办公室、专家委员会一道，构成了网络安全审查工作的顶层制度设计。

左晓栋认为，网络安全审查委员会将是网络安全审查的领导机构，是一个跨部门的委员会。由于网络安全审查涉及多个行业 and 多个部门，需要一个跨部门委员会在日常工作中起到协调和统筹的工作。这是网络安全审查工作中的一个关键设计。

针对网络安全审查内容的问题，征求意见稿中列出了五方面内容，主要包括：（一）产品和服务被非法控制、干扰和中断运行的风险；（二）产品及关键部件研发、交付、技术支持过程中的风险；（三）产品和服务提供者利用提供产品和服务的便利条件非法收集、存储、处理、利用用户相关信息的风险；（四）产品和服务提供者利用用户对产品和服务的依赖，实施不正当竞争或损害用户利益的风险；（五）其他可能危害国家安全和公共利益的风险。此次意见稿明确“重点审查网络产品和服务的安全性、可控性”。

专家指出，传统的安全测评更多是关注产品本身的安全性。而网络安全审查和以前的产品测评是不冲突的，重点关注产品的安全性可控性，重点检查其有没有利用提供产品的便利，从事危害用户利益的可能性。这些范围归根到底都是围绕产品的“安全和可控”。

针对具体的审查程序与办法，征求意见稿也提出明确要求，其中第八条指出：根据国家有关部门要求、全国性行业协会建议、市场反映和企业申请等，网络安全审查办公室组织第三方机构、专家对网络产品和服务进行网络安全审查，并发布或在一定范围内通报审查结果。

在启动审查阶段，意见稿规定了企业申请、主管机关和部门依职权申请、全国性行业协会建议、市场普遍反映等多种形式。

《信息产业发展指南》解读：云计算

2017-02-14 来源：工信部信软司

一、发展现状

经过“十二五”期间各方的共同努力，我国云计算产业得到快速发展，已成为推动经济增长、加速产业转型的重要力量。

（一）产业发展势头迅猛，催生新经济增长点

一是产业规模迅速扩大。据统计，2015 年我国云计算产业规模接近 1500 亿元，增速超过 30%，是全球增速最快的市场之一。其中，公有云增速达 47%，私有云增速达 26%。二是产业结构不断优化。从公有云服务的三个类别来看，SaaS 市场规模最大，SaaS、IaaS、PaaS 占比约为 52.8%、42%、5.2%。三是逐步形成了从基础软硬件到咨询、建设、迁移、交付、运维等全流程的产业链。云计算的快速发展也带动了上下游产业的迅猛发展，成为新的增长点。四是带动形成了一批产业发展的新业态、新模式。基于云计算的安全技术有效提升了计算机终端用户的安全保障水平。

（二）关键技术取得突破，核心能力建设进展显著

一是在部分关键技术指标达到国际先进水平。目前，我国云计算领军企业的单集群服务器规模已达到万台，数据处理能力达到 EB 级。在面向云计算应用的整机柜服务器和微模块数据中心方面也取得了重大创新突破。二是云计算的系统解决方案研发取得积极进展。针对不同应用场景，形成了多套成熟的云计算解决方案，并在政务、交通、医疗等领域得到广泛应用。三是在数据中心绿色节能方面取得了积极突破。云计算骨干企业综合利用各类节能技术，大幅度降低数据中心能耗，提高能源使用效率，目前新建数据中心 PUE 值低于 1.4，部分数据中心 PUE 达到 1.3 甚至 1.2。四是在开源社区、国际标准制定中扮演着重要角色。在云计算主流开源社区中，我国企业深度参与，贡献度也在不断增加。在 ISO/IEC、ITU-T、IETF 等组织中，我国在云计算相关国际标准制定中也发挥着越来越积极重要的作用。

（三）行业应用广泛深入，带动产业转型升级

云计算在各领域广泛应用，通过行业与互联网深度融合，有力助推“互联网+”战略的实施。一是成为互联网应用发展的基础设施。目前，我国大部分网站、移动应用、视频服务、游戏服务和电子商务的后台均架设在云平台上，应用服务的性能和质量也得到了有力保障。二是在政务领域的应用有力地促进了政府管理模式创新和社会治理体系建设。国家食药监局、国家气象局等部门利用云计算进行食品药品监管和气象数据分析，大幅提高了管理效率。浙江、贵州、陕西等多个省份利用云计算搭建公共服务平台，完善民生工程。三是助推传统产业加速转型升级。北京等 16 个省市积极开展工业云创新服务试点，探索创新两化融合的新模式。目前注册用户已超过 1300 多万，服务企业超过 16000 家。

（四）降低创新创业门槛，支撑“双创”快速发展

云计算的广泛深入应用大大降低了创业创新的技术门槛以及信息化成本。目前，云计算已成为我国创业创新的重要基础支撑平台，聚集了大量新应用、新业

态、新模式的开发团队，带动就业能力明显，取得了良好的经济效益。大量中、小、微企业已应用云服务，平均节省信息化成本约 40%。云计算的发展也催生了分享经济等新型经济模式，带动广大企业和个人分享资源，创造多元化的增值业务。在云计算平台支撑下，一批分享经济平台如雨后春笋般快速发展，为数以亿计的用户提供服务。

二、主要问题

一是云计算服务的市场需求尚未完全释放。出于对云计算安全性、可靠性和可迁移性的顾虑，我国行业用户对公有云还存在一定顾虑，政务、金融等重点行业采购公有云服务还面临政策、技术标准等障碍。

二是产业规模小，技术产品服务能力仍需提高。从产业规模看，我国在全球云计算市场份额占比不到 5%。目前，国内云计算产业化的总体水平与国际先进水平还有一定差距，在部分关键行业尚没有形成成熟的解决方案，产业供给能力有待提升。

三是促进云计算发展的生态体系有待完善。在制度建设方面，我国云计算标准体系和评测认证体系尚不完备，个人隐私、数据保护等法律法规有待健全，市场管理方式尚需改进，政府信息资源开放共享、业务协同等方面的机制问题亟待解决。

三、总体形势

当前云计算已从技术导入阶段进入到了产业蓬勃发展、应用迅速普及阶段。未来一段时间，我国云计算还将继续呈现出技术创新和应用推广快速发展的态势。

一是云计算产业发展面临着更大的市场机遇。一方面，随着“中国制造 2025”、“互联网+”战略的不断推进，各行业迫切需要通过构建云计算系统，满足转型需求。另一方面，云计算近年来技术和产业的不断成熟以及成功案例不断出现，使得用户对云计算的认知和采用度不断提高。

二是产业格局将加快调整。2014 年以来，云计算龙头企业纷纷通过并购、融资、合作等手段构建产业体系，增强自己的产业竞争力，拟补产业短板，与合作伙伴共同构筑强大的竞争优势。

三是开源技术将影响云计算技术变革。开源技术与云计算的结合，为云计算产业注入了新鲜血液，对于云计算技术演进产生了重大影响。目前越来越多的云计算企业开始使用开源云平台，并积极参与开源云计算社区建设。

四是混合云将成为云计算服务业态的重要方向。混合云将公有云和私有云的优点融于一体。未来，众多大型企业在信息化建设过程中需要实现在私有云和公有云之间的高效对接和无缝切换，为混合云架构的发展带来了巨大空间。

五是工业云异军突起，成为云计算的重要增长点。工业云的应用帮助企业在生产经营各环节实现智能协同，以工业云为基础的“云制造”模式推动企业内部或区域集群企业之间实现产能资源、工艺知识库和数据资源共享，将助推了制造业的转型升级。

四、“十三五”时期的发展方向及重点

深入贯彻落实国务院《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）、《关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28号），认真按照创新、协调、绿色、开放、共享的发展方针，加快推动供给侧结构性改革，推动我国云计算产业发展再上新台阶，打造推动产业转型升级和经济平稳增长的新引擎，为实现制造强国、网络强国提供有力支撑。

一是加快突破核心技术环节。持续支持骨干企业联合高校、科研院所、用户单位等优势力量，强强联合、协同推进，加快突破核心技术环节，构建高水平的云计算服务平台，丰富云服务种类，不断提高技术水平和服务能力。培育云计算领域具有国际竞争力的龙头骨干企业。

二是加快推进云计算标准化工作。围绕落实《云计算综合标准化体系建设指南》，继续开展关键急需标准研制，逐步完善标准体系框架。面向各地积极开展标准化宣贯，鼓励各地积极组织产业力量参与云计算标准化工作。积极参与国际标准制定，推动提升国际标准话语权。

三是推进云计算开源软件发展。探索通过联盟的方式提升我国产业力量在云计算开源社区的话语权。加强与国际主流开源社区的对接，积极开展开源技术交流和案例推广，建立完善人才培养机制。

四是加快云计算测评体系建设。围绕云计算服务关键环节，组织第三方测评机构积极推进制定云计算服务测评指标体系，构建完善的云计算测评体系，推动开展服务能力测评，规范云计算服务市场，推动云计算企业加快提升云计算服务质量。鼓励第三方测评机构积极发展基于云计算的新型软件测试服务。

五是在现代制造业等重点领域推广云计算应用。抓好工业云服务平台试点示范。以智能制造为主攻方向，加快云计算等信息技术与现代制造业结合。继续深化各地工业云平台的试点工作，针对中小企业发展需求，支持建设一批高质量的工业云服务平台，推进制造资源、服务资源的开放共享。

六是打造云计算环境下的安全保障体系。以“整体、动态、开放、相对、共同”的安全观为指引，妥善处理安全与发展的关系。支持骨干企业研发适应云计算环境下的安全技术和产品，组织开展应用示范，增强安全技术支撑和服务能力。推动制定和完善云计算环境下信息安全的标准规范和管理政策，不断健全安全防护体系，切实保障云计算信息安全。

《信息产业发展指南》正式发布

根据《中华人民共和国国民经济和社会发展第十三个五年规划纲要》、《中国制造 2025》、《国家信息化发展战略纲要》、《国务院关于积极推进“互联网+”行动的指导意见》、《国务院关于深化制造业与互联网融合发展的指导意见》等的部署，经国务院同意，工业和信息化部、国家发展改革委正式印发了《信息产业发展指南》（工信部联规〔2016〕453号，以下简称《指南》）。

《指南》以加快建立具有全球竞争优势、安全可控的信息产业生态体系为主线，提出了到 2020 年基本建立具有国际竞争力、安全可控信息产业生态体系的发展目标。《指南》提出了增强体系化创新能力、构建协同优化的产业结构、促进信息技术深度融合应用、建设新一代信息基础设施、提升信息通信和无线电行业管理水平、强化信息产业安全保障能力、增强国际化发展能力 7 大任务，确定了集成电路、基础电子、基础软件和工业软件、关键应用软件和行业解决方案、智能硬件和应用电子、计算机与通信设备、大数据、云计算、物联网 9 个领域的发展重点，研究部署了 7 个重大工程，明确了相关保障措施。《指南》的实施期限为 2016—2020 年，是“十三五”时期引导信息产业发展的重要文件，将有力支撑制造强国和网络强国建设。

关键信息基础设施的概念

目前，国家关键信息基础设施已经被视为国家的重要战略资源，以立法形式保护关键基础设施和关键信息基础设施的安全，已经成为当今世界各国网络空间安全制度建设的核心内容和基本实践。

关键信息基础设施是指面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，且这些系统一旦发生网络安全事故，会影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失。

关键信息基础设施包括网站类，如党政机关网站、企事业单位网站、新闻网站等；平台类，如即时通信、网上购物、网上支付、搜索引擎、电子邮件、论坛、

地图、音视频等网络服务平台；生产业务类，如办公和业务系统、工业控制系统、大型数据中心、云计算平台、电视转播系统等。

《网络安全法》对保护关键信息基础设施进行了特别强调，县级(含)以上党政机关网站、重点新闻网站、日均访问量超过 100 万人次的网站，以及发生网络安全事故后可能造成 100 万人个人信息泄露的网站，都可认定为关键信息基础设施。

抄送：校领导