北京市重点学科：『网络治理』交叉学科成果

安全软件市场监管

李欲晓 崔聪聪 杨晓波 田松林 ◎著

ANQUAN RUANJIAN SHICHANG JIANGUAN

北京邮电大学出版社
www.buptpress.com

北京市重点学科："网络治理"交叉学科成果

安全软件市场监管

李欲晓　崔聪聪　杨晓波　田松林　著

北京邮电大学出版社
www. buptpress. com

内 容 简 介

本书从网络、信息与软件安全的“看门人”安全软件着手，系统分析了安全软件对保障网络、信息与软件安全的重要性。通过梳理安全软件发展的现状及其存在的问题，提出应完善《反不正当竞争法》，强化安全软件企业的信息披露义务，完善市场准入和退出制度，强化行业自律，以维护公平有序的竞争秩序，从而强化安全软件保障网络、信息与软件安全的功能。

本书可供网络与信息安全的从业者、互联网监管机构工作人员参考使用，并可作为信息安全、通信工程、计算机网络、信息系统工程等专业的本科高年级或研究生的参考用书。

图书在版编目（CIP）数据

安全软件市场监管 / 李欲晓等著. -- 北京 : 北京邮电大学出版社，2014.12
ISBN 978-7-5635-4131-7

Ⅰ. ①安… Ⅱ. ①李… Ⅲ. ①软件开发－安全技术－市场监管 Ⅳ. ①TP311.52
中国版本图书馆 CIP 数据核字（2014）第 199690 号

书　　名：安全软件市场监管
著作责任者：李欲晓　崔聪聪　杨晓波　田松林　著
责 任 编 辑：何芯逸
出 版 发 行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号（邮编：100876）
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京鑫丰华彩印有限公司
开　　本：720 mm×1 000 mm　1/16
印　　张：10
字　　数：194
版　　次：2014 年 12 月第 1 版　2014 年 12 月第 1 次印刷

ISBN 978-7-5635-4131-7　　定　价：29.80 元

前　言

互联网，这个曾被认为是中国管制最少、准入门槛最低的行业，在自由的环境下旺盛了近20年：截至2014年6月底，中国网民数量达到6.32亿，互联网普及率为46.9%。中国也成为全球互联网竞争最为激烈的市场之一。随着互联网市场进入“混业经营”时代（企业由从事单一业务转向多元化经营电子商务、搜索、网络游戏、IM、安全等业务），传统企业尤其是各类传统互联网服务企业都面临新的竞争对手、竞争格局和竞争方式。新领域、无序竞争、监管缺失、公众关注等这些因素导致网络服务业的竞争往往趋向于成为社会热点，而网络本身的广泛覆盖和深入渗透更使得市场行为经常成为公众利益与企业价值冲突的平台。在冲突的过程中，网络用户往往成为企业之间不正当竞争的受害者。

安全软件市场竞争秩序混乱，网络用户的权益无法获得有效保障，一方面与网络企业的强势有关，另一方面是由于现有相关立法的滞后以及监管制度的不健全。传统的反不正当竞争法、反垄断法、消费者保护法、侵权责任法等在网络时代遭遇了前所未有的挑战。立法的滞后已无法对相关市场行为的合法性予以准确定性，尤其是涉及滥用市场支配地位等不正当竞争或垄断行为的判断，再加上有效市场监管的缺失以及低违法成本，使得企业在经营过程中的不当行为很难受到约束。因此，网络社会不仅需要保护网络用户合法权益的规则，也需要规范网络企业公平竞争的规则，更需要规范网络监管机构履行职责的规则。

尊重和维护网络用户的合法权益，公平竞争，也就相当于给了互联网行业一个重新建立规则、塑造新商业文明的机会。以此为契机，引发我们思考中国的互联网立法，订出相关互联网企业行为规范，从根本上解决互联网企业竞争的乱象，引导中国互联网企业走上良性循环。在这样的背景下，我们完成了《安全软件市场监管》一书，期冀供工业和信息化部、公安部以及其他行业主管机关在监管安全软件市场时参考，并能为我国完善安全软件行业监管立法提供理论支撑。本书各章撰写者如下：第1章，李欲晓、杨晓波；第2章，崔聪聪；第3章，李欲晓、杨晓波；第4章，田松林；第5章，崔聪聪、田松林。

目　录

第1章　安全软件界定及其发展趋势

1.1　安全软件的概念

明确监管对象是进行监管的前提。安全软件作为一个新兴的概念，目前国内外并没有一个较为权威的定义。因此，在界定安全软件基础上，划分出被监管主体的范围就显得格外必要。

百度百科上的定义是："安全软件，是指一种可以对病毒、木马等一切已知的对计算机有危害的程序代码进行清除的程序工具。安全软件也是辅助管理计算机安全的软件程序。安全软件主要以预防为主，防治结合。它可以分为：①杀毒软件，又称反病毒软件，是用于消除计算机病毒、特洛伊木马和恶意软件的一类软件。杀毒软件通常集成监控识别、病毒扫描和清除、自动升级等功能，有的杀毒软件还带有数据恢复等功能，是计算机防御系统（包含杀毒软件、防火墙、特洛伊木马和其他恶意软件的查杀程序、入侵预防系统等）的重要组成部分。例如，目前的360杀毒、卡巴斯基安全部队、小红伞、瑞星杀毒、金山毒霸、诺顿等。②辅助性安全软件，主要用于清理垃圾、修复漏洞、防木马等。系统工具可以尽可能地减少计算机执行的进程，更改工作模式，删除不必要的中断让机器运行更有效，优化文件位置使数据读写更快，空出更多的系统资源供用户支配以及减少不必要的系统加载项及自启动项。例如，360安全卫士、金山卫士、瑞星安全助手等。③反流氓软件，主要用于清理流氓软件，保护系统安全。例如，超级兔子、恶意软件清理助手、Windows清理助手等。④加密软件，主要是通过对数据文件进行加密，防止外泄，从而确保信息资产的安全。"①

维基百科上的定义是："安全软件，是指任何用于保护计算机系统或网络安全的计算机程序或程序组。安全软件的类型包括：①杀毒软件；②反密码窃取软件；③加密软件；④防火墙；⑤入侵检测系统；⑥间谍软件移除工具；⑦沙箱（sand-

① 百度百科：安全软件，资料来源：http://baike.baidu.com/view/541009.htm，2013年3月18日访问，以及其他网络资料。

box)[①];⑧其他任何具有安全功能的可操作的系统。"[②]

中国互联网信息中心(CNNIC)在其报告中将安全软件定义为:包括杀毒软件、防火墙软件、查杀木马插件等安全辅助软件等各种类型安全软件的集合。[③] 还有相关安全软件厂商指出,所谓(互联网)安全软件,是指保障互联网用户个人隐私或商业信息在网络上传输时的机密性、完整性和真实性的软件。[④] 更有国外学者采用更简洁的概括认为,安全软件即是保障个人计算机和网络系统安全而设计的计算机软件。[⑤]

上述定义,或以概括,或以列举的形式对安全软件进行了阐释,但可以看出,其核心均指向维护"计算机安全"与"网络安全"的软件或程序。然何为"维护安全"?狭义上可以理解为查杀病毒、木马等威胁;广义上却能广阔延伸,如对系统垃圾进行清理,提供安全下载通道,对系统进行优化等。在界定安全软件时应采用狭义还是广义?此外,上述定义未明确此类软件或程序的功能是否具有专一性。网络安全市场上能够提供安全功能的并非局限于专门提供安全服务软件,其他类型软件也可以通过添加安全组件或模块的形式来实现安全防护功能,如腾讯旧版本的QQ软件附带的盗号木马查杀功能(QQ医生)。这种附带安全功能的软件是否属于安全软件?再者,随着云计算技术的逐渐成熟,在线安全查杀服务[⑥]也随之产生。如金山、瑞星、江民都提供该类服务。[⑦] 在线查杀仅需安装相应的控件,通过互联网和浏览器就能够进行,本质上不能算作软件。那么提供这种服务的厂商是否也属于监管的对象?同时,受各种网络安全"疑难杂症"、安全需求复杂多样等因素的影响,人工安全服务模式兴起,严格意义上该类服务不属于软件,是否将其排除在安全软件监管的范围?最后,平板电脑、智能手机等新终端形式的普及使安全软件的概念早已不局限在"计算机软件"上。故前述的各种概念均无法准确地界定安全软件,也无法明确监管的主体范围。

结合目前已有的观点和存在的问题,我们认为:安全软件即任何用于保护计算

① 对于病毒的检测,使用虚拟的环境来让可疑程序运行以发现其是否具有破坏性。

② 维基百科:Security Software,资料来源:http://en.wikipedia.org/wiki/Security_software,2012年1月10日访问。

③ CNNIC:2009年中国网民网络信息安全软件使用行为调查报告,2010年3月。

④ 参见:奇虎起诉腾讯垄断案件起诉书,资料来源:http://tech.163.com/12/0418/10/7VC8EEIK000915BF.html,2012年4月20日。

⑤ S.E.Smith:"What Is Security Software?",http://www.wisegeek.com/what-is-security-software.htm,2013年1月4日访问。

⑥ 在线查杀又具体可以分为在线查毒和在线杀毒。在线查杀是指不需要用户把整个杀毒软件安装在本地计算机,用户只需要在本地装一个很小的客户端程序或安全控件,即可通过网络调用远端服务器上的杀毒软件程序和病毒库对本地计算机进行查毒或杀毒工作。

⑦ 金山提供的http://www.pc120.com在线查杀毒服务已经下线。

机、智能移动终端和网络安全的程序和指令集合。它具有以下一项或几项功能：①对计算机、智能移动终端和网络进行安全防护；②对已存在的安全威胁进行清除和治理；③对计算机、智能移动终端进行优化、清理等安全辅助性功能。具体到安全软件行业监管的对象上，我们认为可以用功能来判断和明确。安全软件行业监管对象的共同点是：他们提供的产品或服务具有网络、终端安全防护、治理和优化等功能。提供附带安全功能软件、在线查杀应用、人工服务等的厂商，都应纳入到监管的范畴，因为其提供的都是安全服务。或可言，对安全软件行业的监管即是对安全服务提供商的监管。这与云计算环境下软件即服务模式的本质也是契合的，符合互联网发展的趋势。

根据厂商提供的产品功能和种类的差别，安全服务提供商又可以分为完全安全服务提供商和非完全安全服务提供商。完全安全服务提供商是指其提供的产品具有专一性，该厂商的经营范围全部为提供安全“防治服务”。而非完全安全服务提供商是指该厂商在提供安全服务的同时还提供其他类型的产品，或其提供的一款非安全软件具有安全功能。完全安全服务提供商和非完全安全服务提供商都是安全软件行业监管的对象。

1.2　中国安全软件发展现状

安全软件是近年兴起的概念，在此之前，安全软件主要指杀毒软件。杀毒软件的发展同计算机网络病毒的产生和传播紧密相连，由于计算机及网络从发展到广泛应用的时间并不长，因此安全软件（杀毒软件）的发展历程也并非特别复杂。

国内最早的一款杀毒软件是 1989 年诞生的 KILL 杀毒软件。[①] 1988 年，Ping-Pong 病毒通过软盘传入境内，不少计算机用户被感染。这是中国最早发现的计算机病毒。当时国内并没有专门的部门管理，刚开始只是由一些程序员等来开展民间反病毒活动。后来公安部组织人编写推出了中国第一款杀毒软件 KILL。在当时杀毒软件市场并不是很广阔的环境下，KILL 杀毒软件占据了包括政府、企业在内的绝大部分市场份额。但随着新病毒种类的不断增多，该款软件的处理能力并不能很好地满足市场需求，于是给其他新兴杀毒软件企业创造了机会。

20 世纪 90 年代中期以后，随着互联网的快速发展和广泛应用，杀毒软件的市场也随之被扩展（主要针对企业用户），KILL 杀毒软件一统天下的局面逐渐被打破。通过疯狂降价、媒体造势、诉讼等多种手段，瑞星、江民、金山毒霸等杀毒软件

① 1989 年国内首个杀毒软件 KILL 的诞生，资料来源：http://sec.chinabyte.com/438/8616938.shtml，2012 年 1 月 20 日访问。

逐渐获得更多的市场份额。[①]

金山、瑞星、江民等几家主要杀毒软件长期占据着国内杀毒软件市场的前几位，直到奇虎360出现。奇虎360的出现使得国内安全软件行业的状况发生急剧改变。截至2010年1月，在短短一季中，360软件就赶超了国内其他杀毒软件，结束了瑞星连续9年占据行业第一的历史。[②] 2010年5月，腾讯电脑管家正式诞生，标志着腾讯正式进入安全软件行业，市场竞争更加激烈。

在中国安全软件市场大增的情况下，国外杀毒软件也开始进入中国市场。早在1998年，赛门铁克公司就通过合作等多种方式开始进入中国市场。2002年，国际知名杀毒软件卡巴斯基开始进驻中国。2011年3月，小红伞在中国召开产品发布会；9月，德国第一品牌、全球领先的杀毒软件巨头G Data在北京召开新品发布会，其针对中国大陆市场的产品包括G Data杀毒软件2012、G Data互联网安全套装2012、G Data全功能安全软件2012及企业终端安全防护软件，正式进军中国市场。

目前国内主流的安全软件品牌包括以下8种。

(1) 奇虎360

奇虎360公司创立于2005年9月，致力于互联网安全软件和互联网安全服务领域，其主要安全服务产品有360安全卫士、360杀毒、360手机卫士、360保险箱等。奇虎于2006年7月正式推出号称国内首款免费网络安全软件——360安全卫士，在不到两年的时间内，该款软件迅速发展为国内用户使用量第一的网络安全软件产品，覆盖国内近50%的互联网用户。根据2011年初的艾瑞数据显示，360安全卫士已覆盖了近80%的互联网用户，用户量超过3.5亿，稳居中国安全软件用户量第一；360杀毒的市场份额也超过了60%，用户量突破2亿。[③]

(2) 金山网络

金山网络是金山安全与可牛网络技术有限公司于2010年11月合并成立的独立公司，其主要安全软件产品有金山毒霸、金山卫士、网盾、可牛杀毒等。金山安全则是老牌软件公司金山软件公司的子公司，成立于2010年4月15日。金山毒霸是金山软件公司于1999年推出的一款杀毒软件，凭借出众的杀毒性能，金山毒霸曾创下国内反病毒软件市场单一品牌月销售55万套的奇迹，更以近60%的市场占

① 杀毒软件发展史和国内杀毒软件状况，资料来源：http://tech.ccidnet.com/art/3089/20060905/892767_1.html，2012年1月20日访问。

② 360杀毒颠覆瑞星九年王座，市场份额跃居行业第一，资料来源：http://bbs.360.cn/4077772/34840181.html?recommend=1，2012年1月20日访问。

③ 360安全卫士、360杀毒获天空软件"2010最佳人气奖"，资料来源：http://www.bianews.com/news/37/n-341937.html，2012年1月21日访问。

有率成为国内信息安全及反病毒领域公认的领导品牌。[①]

(3) 瑞星

北京瑞星科技股份有限公司成立于 1997 年 3 月，其前身为 1991 年成立的北京瑞星电脑科技开发部，是中国最早从事计算机病毒防治与研究的大型专业企业之一。瑞星以研究、开发、生产及销售计算机反病毒产品、网络安全产品和反“黑客”防治产品为主，拥有全部自主知识产权和多项专利技术。[②] 其主要安全软件产品有瑞星杀毒、瑞星防火墙、瑞星安全助手、瑞星加密盘、瑞星数据恢复服务等。

(4) 腾讯电脑管家

腾讯电脑管家(原名 QQ 电脑管家)是腾讯公司于 2010 年 5 月推出的安全软件产品，其前身为 2006 年 12 月诞生的 QQ 医生。该软件拥有云查杀木马、系统加速、漏洞修复、实时防护、网速保护、电脑诊所、健康小助手等多种功能，且首创了“管理＋杀毒”二合一的开创性功能。根据腾讯官方数据显示，截至 2011 年 10 月，电脑管家装机用户量已突破 2 亿。[③] 同时，腾讯还推出了腾讯手机管家，成为手机等移动终端领域主要的安全软件产品之一。[④]

(5) 江民

江民公司由中国反病毒专家王江民于 1996 年创建，其主要安全软件产品有江民杀毒系列、江民密保、江民专网安全防护系统、江民网警等。江民杀毒在质量管理方面严格执行国际标准，是中国首家通过国际第三方安全认证机构西海岸实验室(West Coast Labs)Checkmark 反病毒最高级 L2 认证的反病毒厂商。[⑤]

(6) 卡巴斯基

卡巴斯基反病毒软件是国际著名的安全软件产品，其厂商卡巴斯基实验室总部设在俄罗斯莫斯科。2002 年，卡巴斯基进入中国市场，初期采取了诸如降低正版用户的使用成本等本土化政策来打开市场，但成效并不大。2006 年 7 月 27 日，卡巴斯基公司正式宣布，将为奇虎旗下的“360 安全卫士”免费提供杀毒功能。用户只需使用奇虎“360 安全卫士”，就能免费获得卡巴斯基提供的最新反病毒

① 数据来自：金山安全实验室介绍，资料来源：http://xian.qq.com/a/20100524/000421.htm，2012 年 1 月 21 日访问。

② 参见：北京瑞星科技股份有限公司，资料来源：http://labs.chinamobile.com/innobase/edition-view-272-3.html，2012 年 3 月 10 日访问。

③ 数据来自：http://guanjia.qq.com/about/history.html，2013 年 3 月 17 日访问。

④ 目前国内手机安全软件主要包括：360 手机卫士，腾讯手机管家，网秦安全，金山手机卫士，安全管家，LBE 安全大师等。

⑤ 百度百科：江民杀毒软件，资料来源：http://baike.baidu.com/view/384666.htm，2012 年 3 月 10 日访问。

KAV6.0个人版正版软件。[①] 至此，卡巴斯基在中国安全软件行业的市场份额得以飞速提升。目前卡巴斯基主要的安全软件产品有卡巴斯基安全部队、卡巴斯基反病毒软件、卡巴斯基手机安全软件等。

(7) 东方微点

东方微点公司成立于2005年，主要安全软件产品有微点主动防御软件和微点杀毒软件。微点主动防御软件开创了我国杀毒软件"主动防御"的先河，属于防病毒软件。该软件建立了动态仿真反病毒专家系统，能够自动判定新木马和病毒，并且能够自动提取新特征值并更新特征库，实现主动防御。[②]

(8) 赛门铁克

赛门铁克公司成立于1982年4月，总部在美国加利福尼亚州，现今在全球40多个国家和地区有分支机构，全球员工超过14 000人。赛门铁克是信息安全领域全球领先的解决方案提供商，为企业、个人用户和服务提供商的内容和网络安全提供丰富的软件和硬件解决方案，确保信息的安全性、可用性和完整性。1998年，赛门铁克进入中国市场。2004年，赛门铁克中国第一个研发中心在北京设立。目前赛门铁克提供的主要安全软件产品包括：赛门铁克杀毒软件、诺顿杀毒软件、诺顿系统大师、赛门铁克远程控制大师、赛门铁克邮件安全大师等。[③]

1.3 中国安全软件的发展趋势

从国内的发展现状来看，我们认为，安全软件行业具有以下4个趋势和特征。

1.3.1 免费化

如今，网络病毒、木马制造者及恶意(流氓)软件制造者、黑客等已由单纯的满足心理需求向满足经济需求转变，各种影响网络安全和信息安全的不安定因素急剧增加。互联网的普及使企业的信息数据安全、系统稳定可靠性等受到严峻考验；个人用户的个人信息、隐私等也时刻面临威胁。尤其是在2006年—2008年间，爆发了一系列重大病毒事件，机器狗病毒、熊猫烧香病毒、维京病毒等，给我国网络安全稳定带来了惨痛的教训，至今网民依然记忆犹新。根据国家计算机病毒应急处

① 参见：揭秘卡巴斯基从默默无名到大获成功，载《成都商报》(电子版)，2008年8月22日，资料来源：http://e.chengdu.cn/html/2008-08/22/content_90983.htm，2012年3月20日访问。

② 参见：微点主动防御软件，资料来源：http://www.docin.com/p-393619377.html，2012年3月20日访问。

③ 百度百科：赛门铁克，资料来源：http://baike.baidu.com/view/326323.htm?fromId=154546，2012年3月20日访问。

理中心《2007 年中国计算机病毒疫情调查技术分析报告》显示，截至 2007 年 6 月，我国计算机病毒感染率高达 91.47%。

随着不安全因素的增加，个人用户对杀毒软件、辅助性安全软件等的需求也不断增长。我国安全软件行业也由原来“三足鼎立”的局面[①]逐渐向“百家争鸣”发展。但鉴于中国现实国情，正版安全软件的费用使得个人用户市场不能完全打开。也正是在这种背景下，奇虎 360 于 2006 年 7 月 27 日正式推出国内首款永久免费的辅助性安全软件，开启了国内安全软件免费化的序幕。2008 年 7 月 17 日，奇虎 360 发布 360 杀毒，同样是永久免费。奇虎免费发布安全软件的行为使其迅速攻占大量市场。

随着安全软件行业竞争的不断激烈化，为争夺用户和市场，其他安全软件厂商不断加入到免费化阵营中来：

2008 年 7 月 24 日，瑞星全球免费发布“瑞星卡卡 6.0”，并捆绑免费期为一年的“瑞星杀毒软件 2008 版”和“瑞星个人防火墙 2008 版”。

2008 年 9 月 16 日，卡巴斯基宣布向符合要求的中国区论坛注册会员提供卡巴斯基全功能安全软件 2009 以及反病毒软件的一年激活码。

2009 年 2 月 27 日，江民科技宣布江民杀毒软件 KV2009 两年免费服务期限再延长三年。

2009 年 9 月 28 日，Windows 正版用户可在微软官网上下载免费杀毒软件 MSE(Microsoft Security Essentials)。

2010 年 11 月 10 日，金山正式宣布其金山毒霸(个人简体中文版)的杀毒功能和升级服务永久免费。

2011 年 3 月 18 日，瑞星宣布其个人安全产品全线永久免费，至此全国逾 8000 万瑞星用户都能免费享受到瑞星杀毒软件及瑞星个人防火墙、瑞星手机安全软件等涵盖计算机、互联网及移动互联网等全部信息安全领域的专业、全面的安全保护。

继个人用户领域免费化后，各大安全软件厂商逐渐转向中小企业的企业用户领域。

2011 年 6 月 15 日，奇虎 360 推出免费企业版杀毒软件[②]，根据奇虎公司公布的数据，在半年多的时间里，全国已有超过 20 万家企业、超过 500 万台计算机终端使用 360 企业版。[③]

---

① 指金山、瑞星、江民三家长期霸占着安全服务行业前三。

② 奇虎 360 企业版实施的是小于 50 点免费策略，有一定的限制条件。

③ 参见：360 企业版覆盖全行业，护航企业超 20 万家，资料来源：http://b.360.cn/news/news_21.html，2012 年 3 月 21 日访问。

2012年3月16日，金山网络发布全球首款彻底免费的企业版杀毒软件——金山毒霸企业版2012，该款安全软件的免费没有任何端点约束限制，所有用户能享受企业级而非单机版专业杀毒软件功能。

目前，我国约有1023万家中小企业，以每家企业用户10台PC计算，中小企业PC总数量将过亿。按平均每台计算机60元的年服务费计算，免费后的企业版杀毒软件将为我国中小企业用户每年节省60亿元的安全开销。①

不管是个人用户安全软件产品的免费，还是企业用户安全软件产品的免费；不管是有时间期限的免费政策，还是永久免费政策，盈利永远是企业从事一种商业行为的最终目的。各主要安全服务提供商纷纷推出免费产品和服务，是为争取市场份额，进而为其实现最终的经济利益做基础。安全服务提供商间争夺用户的激励"战争"，是互联网用户"人口红利"逐渐减少带来的必然后果。2008年—2009年，每隔半年全国网民数量可增长逾13%，而2010年，增幅回落到9%。在"蛋糕"总量增幅不大的前提下，如何从现有网民中争取到更多用户，成为市场战略的主攻方向。② 但是，也应当看，免费对于主要靠产品获利的安全服务提供商来说无疑是一场灾难。从病毒的捕获、分析，到引擎的制作，再到升级服务，这些过程都需要资金来维系，免费化的策略将使安全服务提供商的处境更加艰难。

然而，安全服务产品的免费化又是个人软件产品免费化潮流下的必然趋势。随着新一代互联网技术的发展，软件产品的互联网化、消费化、服务化和云端化特征越发突出。要想在这种转变中继续获得利益，就必须转变以卖产品为本位的思路到以卖服务为本位的思路上来。③ 因此，安全服务提供商必须通过继续探寻新的盈利模式来弥补产品免费化所带来的损失，如通过提供增值服务和发布广告等来获得利润。而在这过程中，应当警惕某些安全服务提供商通过免费获得大量用户，并向这些用户推广有商业价值的其他应用软件，进而打击其他竞争对手的行为。

对于用户而言，目前免费的安全服务产品主要集中于个人用户领域，且提供的功能主要是一些基本的安全防护，部分产品的免费也有期限。对于个性化和专业化的需求，大部分安全服务提供商还是采取收费的模式。因此，对于安全防护系数要求较高的个人用户和企业用户，这种免费的福利可能难以惠及。同时，用户在选择免费安全软件或服务时也应当慎重考虑，应选择信誉和品质较高的产品或服务，

① 数据来源：企业安全软件进入免费时代，资料来源：http://www.0375.gov.cn/2012/0319/27355.html，2012年4月2日访问。

② 参见章迪思："3Q大战"后，互联网需要怎样的竞争，载《解放日报》2010年12月30日第4版。

③ 如NOD32和卡巴斯基通过提供代理服务的方式来收取代理费；360网址导航每年可为360带来近亿元的收入；360浏览器中的广告收入占了奇虎公司收入的70%；通过远程真人维护计算机收费服务等。（参见飞雪散花：免费安全软件究竟如何赚钱？，载《网友世界》2011年第10期。）

以免面临权利被侵犯的风险。

1.3.2　云安全技术逐步深入

云计算，是指用户可以通过网络按需求、以易扩展的方式获得所需资源。这种资源狭义上指各种 IT 基础设施，广义上则可延伸为各种服务。它是一种基于互联网的计算方式，是网格计算、分布式计算、并行计算、效用计算、网络存储等传统计算机网络技术发展融合的产物。这种新型的计算技术已经普遍被认为是继个人计算机、互联网之后的第三次革新浪潮，并得到了各国政府、IT 厂商的高度重视。目前，我国也已经将云计算列入国家战略性新兴产业，预示其在未来将迎来更大的空间。①

杀毒引擎和病毒库是构成杀毒软件的两大重要技术机制。简单来说，杀毒引擎就是一套判断特定文件或程序进程是否合法（是否为病毒程序）的技术机制。病毒库则指一个记录病毒特征文件的数据库。杀毒引擎和病毒库相互作用完成反病毒任务。② 早期安全软件的工作原理是，在病毒或木马出现之后，对这些恶意代码程序进行人工分析，并制作出包含病毒属性的特征码，软件厂商定期提供这些特征码供杀毒软件用户下载。用户更新了个人计算机上安全软件的病毒库后，软件就能根据特征码来对病毒和木马进行识别和清理，这种技术也被称为“病毒特征码识别技术”（见图 1-1③）。这种技术对于病毒木马查杀的准确率高、误报率低，但也存在速度慢的缺陷。从病毒木马的发现，到特征码的发布，再到用户更新本地的病毒数据库，存在一个较长的时间段，病毒查杀具有被动性的特点。于是，在这种缺陷下，“未雨绸缪”的主动防御技术出现了。主动防御技术基于虚拟机技术和病毒行为阻断技术，通过提取病毒木马的行为共性特征，如修改注册表、自我复制、不断连

---

① 我国《“十二五”国家战略性新兴产业发展规划》中提到：“把握信息技术升级换代和产业融合发展机遇，加快建设宽带、融合、安全、泛在的下一代信息网络，突破超高速光纤与无线通信、物联网、云计算、数字虚拟、先进半导体和新型显示等新一代信息技术，推进信息技术创新、新兴应用拓展和网络建设的互动结合，创新产业组织模式，提高新型装备保障水平，培育新兴服务业态，增强国际竞争能力，带动我国信息产业实现由大到强的转变。”表明云计算已被列入国家战略性新兴产业行列。

② 杀毒引擎在杀毒软件中起着核心的作用。一个完整的技术引擎一般包含如下几个行为过程：①非自身程序行为的程序行为捕获。包括来自于内存的程序运行，来自于给定文件的行为虚拟判断，来自于网络的动态的信息等等。②基于引擎机制的规则判断。这个环节代表了杀毒引擎的质量好坏，一个好的杀毒引擎能够在这个环节发现很多的病毒行为。虚拟机技术、实时监控主动防御技术都是在该阶段完成的。③杀毒引擎与病毒库的交互作用。杀毒引擎将非自身程序行为过程转化为杀毒软件可识别的行为标识符，然后与病毒库中所存储的行为信息进行比较，并作出处理。当前大多数的杀毒软件的病毒识别是在这个阶段完成的。（参见 zhangnn5：杀毒软件工作原理及现在主要杀毒技术，资料来源：http://blog.csdn.net/zhangnn5/article/details/6437371，2013 年 4 月 2 日访问）

③ 图片参考自：http://shop.micropoint.com.cn/product/index.htm，2012 年 6 月 23 日访问。

接网络等，综合这些特称来判断用户计算机上的不明程序（尚未被确认为病毒木马或安全服务提供商尚未发布病毒码特征）是否为病毒或木马，起到提前发现并阻止各种恶意行为的目的。这种技术的出现，弥补了病毒特征码识别技术反应缓慢的缺陷，但同时判断不准确甚至是误判也是困扰该技术发展的因素之一。

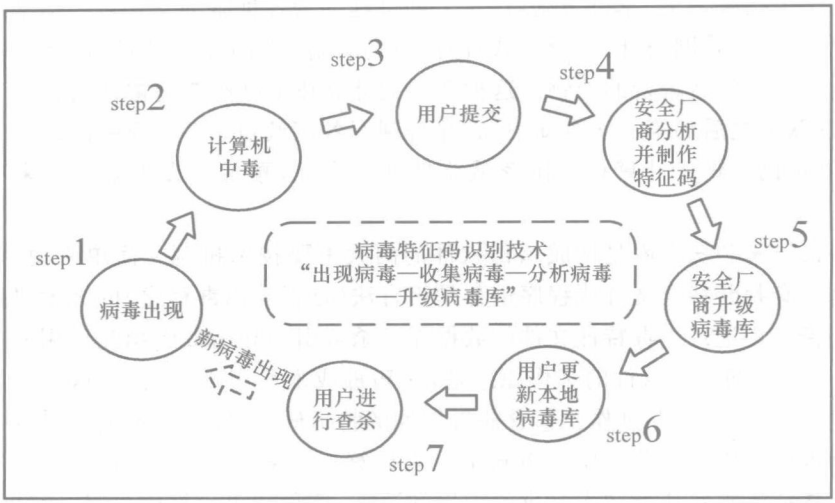

图 1-1　病毒特征码识别技术

无论是病毒特征码识别技术，还是主动防御技术，以及后来开发的虚拟机脱壳引擎技术、启发式杀毒技术等，在应对日益增长的海量病毒和木马等恶意程序代码上都无法得心应手。云计算技术的出现则为安全软件技术的发展提供了新的发展方向，基于云计算而产生的云安全技术成为各大安全服务提供商争相追捧的对象。迈克菲、卡巴斯基、赛门铁克、奇虎 360、腾讯电脑管家、金山、瑞星、趋势科技等都推出了基于云安全技术的安全服务产品。如腾讯电脑管家在 2013 年实现了云鉴定功能。QQ2013beta2 中打通了与腾讯电脑管家在恶意网址特征库上的共享通道，每一条在 QQ 聊天中传输的网址都将在云端的恶意网址数据库中进行验证，并立即返回鉴定结果到聊天窗口中。[①] 安全服务提供商通过安装在用户个人计算机上的客户端和互联网上的其他服务器，将出现的各种病毒样本进行收集，只要有用户受到攻击，病毒的样本就会迅速发送至安全服务提供商，这样恶意代码样本库就可以迅速增大，当有用户再次遇到相同的威胁时，就可以通过在线访问云端样本库的方式来进行查杀。[②] 大多数安全服务提供商的云查杀、病毒查杀的方式并没有

① 百度百科：安全软件，资料来源：http://baike.baidu.com/view/541009.htm，2013 年 4 月 1 日访问。

② 参见：趋势深度解析云安全，资料来源：http://wenku.baidu.com/view/d008d92fe2bd960590c677e2.html，2012 年 7 月 2 日访问。