

# 安全周报

中国信息安全博士网

第四期

二〇一〇年四月二十六日

weekly.secdactor.com

- 学术会议
- 政府之声
- 病毒播报
- 产业动态
- 技术前沿
- 黑客攻防
- 海外来风

# 浪潮SSR成为

“中华人民共和国第十一届运动会唯一指定服务器操作系统安全加固系统产品”



**浪潮** 主机安全的领导厂商

**浪潮SSR** (Server System Reinforcement) 服务器安全加固系统是基于对信息安全等级保护制度及相关标准的深入理解,以构建安全的计算环境为基础,以强制访问控制为主线,结合当前信息安全产业的发展现状而推出的专门针对服务器操作系统的整体安全解决方案。SSR采用先进的ROST技术理论,在操作系统内核层对服务器操作系统进行加固,同时根据信息安全管理中的“三权分立”原则,实现对用户和进程的最小授权,防止对系统文件和重要数据的误操作,从根本上免疫目前针对操作系统的各类攻击行为,彻底防范病毒、蠕虫、黑客攻击等对操作系统和数据库的破坏。这一独到的服务器系统安全解决方案填补了国内在此领域的长期空白,浪潮信息安全被赞誉为“服务器安全专家”,开辟了信息安全产业发展的新方向。

## 浪潮SSR产品系列

SSR企业版:企业核心主机操作系统免遭受非法攻击的“智能屏障”

SSR网络版:可信服务器安全运维中心

SSR专用版:为您的主机系统量身订做的“安全胃甲”

## 主要功能

从根本上免疫针对服务器操作系统的攻击

符合国家信息安全等级化保护三级标准

有效防止内、外网针对服务器系统的攻击

保障业务的连续性、稳定性、安全性及可靠性

有效解决了安全体系中系统层的安全问题

从根本上防范冲击波、震荡波等蠕虫类病毒



**inspur 浪潮**

中华人民共和国第十一届运动会  
IT产品与服务合作伙伴

## 浪潮信息安全事业部

北京办事处:北京市海淀区阜成路73号裕惠大厦1002室 邮编:100142  
电话:010-68451517 (总机) 传真:68451517-6688  
成都办事处:成都市一环路南一段22号红瓦大厦930 邮编:610041  
电话:028-85243518 传真:028-85214223  
杭州办事处:杭州文三路478号华星时代广场A楼1507 邮编:310012  
电话:0571-88907770 传真:0571-88907772  
南京办事处:南京市中山北路45号华美达怡华酒店7层 邮编:210008  
传真:025-83308166  
安徽办事处:合肥市长江中路436号金城大厦1301室 邮编:230061

广州办事处:广州市天河北路898号信源大厦17层 邮编:510898  
电话:020-38182808-8208 传真:020-38182825  
上海办事处:延安西路129号华侨大厦23楼 邮编:200050  
传真:021-62485588-9075  
太原办事处:太原市平阳路东巷56号7号楼5单元201室 邮编:030012  
济南总部:济南市山大路224号1号楼1层东厅 邮编:250013  
技术支持热线:0531-85105399 0531-88932888 (总机) 转5399  
售后服务热线:0531-85105398 0531-88932888 (总机) 转5398  
E-mail: Security@inspur.com

## 目录

|                                          |    |
|------------------------------------------|----|
| 学术会议.....                                | 4  |
| 高端容错计算成云计算关键 专家吁推进自主发展.....              | 4  |
| 第十一届中国信息安全大会隆重召开.....                    | 5  |
| 政府之声.....                                | 6  |
| 工业和信息化部抗震救灾工作快报.....                     | 6  |
| 国家集成电路公共服务联盟在无锡宣布成立.....                 | 7  |
| 工信部发布《移动电话机定制管理规定》.....                  | 8  |
| 江苏实战演练世博期间网络安全突发事件.....                  | 10 |
| 病毒播报.....                                | 11 |
| 病毒预报 （2010.4.19-2010.4.25）.....          | 11 |
| 被 Rootkit 感染的 XP 系统无法安装最新补丁.....         | 12 |
| 4 月 19 日病毒预警：谨防“埃卡”和“毒蝙蝠”.....           | 13 |
| 手机 QQ 疯狂爆发“72ub 有惊喜”病毒.....              | 14 |
| 产业动态.....                                | 15 |
| 赛门铁克发布 2011 测试版安全软件将占用更少内存.....          | 15 |
| 首个云存储标准发布.....                           | 16 |
| 专家视角：从 RSA 看网络应用安全发展趋势.....              | 17 |
| 微软首宗针对中国大企业盗版案宣判：获赔 217 万.....           | 19 |
| PGP 创始人加入苹果参与系统安全.....                   | 20 |
| 技术前沿.....                                | 21 |
| 影响校网稳定 苹果 iPad 遭封杀.....                  | 21 |
| 恰当的安全控制是虚拟化成功关键.....                     | 21 |
| 国家安全：“谷歌地球”泄露了什么？.....                   | 22 |
| 签名服务器在国库横向联网系统中的应用.....                  | 24 |
| 黑客攻防.....                                | 27 |
| 阿里巴巴速卖通平台遭攻击.....                        | 27 |
| Palm WebOS 系统存在多个安全漏洞.....               | 28 |
| Mozilla 将针对恶意 Java 插件进行屏蔽.....           | 28 |
| 黑客组织破解育碧 DRM 称育碧应多关注游戏.....              | 29 |
| 海外来风.....                                | 29 |
| Four Tips for Securing Social Media..... | 29 |

## 学术会议

### 高端容错计算成云计算关键 专家吁推进自主发展

文章来源：新浪科技

4 月 20 日消息，由 863 计划“高端容错计算机”重大项目总体技术专家组主办的“高端容错计算机发展战略论坛”日前在京举行。来自工信部、科技部、铁道部等部委的官员，来自建设银行、农业银行、中石油、中石化、上交所等用户的主要技术负责人，以及各大科研机构、知名厂商共 200 多人参加论坛。

高端容错计算机是国家信息化建设的重大装备，也是 IT 产业发展的核心技术，国际主流 IT 厂商通过占据高端计算机产业链的制高点，进而向操作系统、中间件、数据库、企业级应用、信息服务等细分领域辐射，形成对整个 IT 产业的控制权。而且在“云计算+物联网”的未来信息化模式下，高端容错计算机的核心地位更加突出。

国家 863 计划“高端容错计算机”课题总体组组长左德承教授在论坛主题演讲中指出，云计算将促使小系统逐渐被整合为大系统、巨系统，物联网则带来后台处理对象和数据跨数量级的增加，随着下一代信息化模式的成熟和深入，社会的计算平台会逐渐向高端容错计算机集中。

随着网络和信息技术的飞速发展，信息安全已经与政治安全、经济安全、国防安全、文化安全共同成为国家安全的重要组成部分。正因为如此，各国纷纷将信息技术和信息安全的自主可控能力与维护国家安全的能力紧密联系在一起。有专家指出，云计算时代的国家信息安全，很大程度上取决于云计算产业和技术是否自主可控，而高端容错计算机作为未来云时代的核心计算设备，应予以重点发展。

当前中国高端容错计算机市场面临良好的发展形式，由于 3G 的大规模建设、网上银行的快速发展、证券业的繁荣等因素的强力推动，中国高端计算机市场保持了年均 15% 以上增长速度，论坛上，中国建设银行总行、中国农业银行总行、联通总公司、上海证券交易所等典型行业客户分别就金融业务创新支持、3G 条件下的 BSS 业务支撑系统、可扩展高性能容灾证券交易系统等核心信息化系统的建设提出了对高端容错计算机的需求。

当前，全球开放、标准化的 IT 产业和技术分工模式已比较成熟，中国计算机产业应该利用当前有利的产业环境，抓住发展机遇，突破核心技术，建立自主可控的高端容错计算机产业。与会技术专家从产业生态和市场的角度提出了推动高端容错自主发展的建议，一方面，自主高端容错计算机

的应用，有赖于自主操作系统、中间件和应用软件的配套支持，打造软硬一体的自主生态环境至关重要；另一方面，建立厂商与用户共赢的产业链关系，通过“先示范后试用”、“先试点后推广”逐步打开市场。

除了有利的市场、产业环境外，中国高端计算机产业的发展也有很好的政策支持和导向，科技部高技术研究中心主任赵玉海说，2010 年是我国成功应对全球金融危机、经济回升向好的一年，加快转变经济发展方式，推进产业结构调整，是当前主要的挑战。我们要大力推进国家创新体系建设，坚持以企业为主体、市场为导向，产学研用相结合的技术创新模式，以免在新一轮技术变革中丧失发展的大好机会。

#### 名词解释：

高端容错计算机，是指具有高可靠性和强大信息处理能力的大型服务器系统。它通常含有 8 颗-64 颗处理器，可靠性高达 99.999%，每年的宕机时间不超过 5 分钟，高端容错计算机广泛应用于银行的储蓄业务系统、汇兑结算系统、银联信用卡交易结算系统，证券的交易系统和证券报价系统，电信领域的网管系统，电力行业的调度系统，民航领域的空管系统和机场出港系统，等等，这些系统的承载平台一旦出现停顿，会对社会生活造成严重破坏。

## 第十一届中国信息安全大会隆重召开

2010 年 4 月 21 日，一年一度的信息安全界的盛事，“第十一届中国信息安全大会”隆重召开。本次会议由中国电子信息产业发展研究院主办、中国计算机报承办，并得到了中国计算机学会计算机安全专业委员会、公安部第一研究所、中国信息安全测评中心、中国信息安全认证中心、国家计算机病毒应急处理中心的大力支持和指导，同时还获得了中国信息主管网、网易科技频道、中国计算机行业网和 51CTO、IT168 等网络媒体的特别支持。

本次大会以“融合安全·风险识别”为主题，继续保持着中国信息安全业内综合性、前沿性、权威性的特点，大会的话题覆盖到目前信息安全热点的相关领域话题。其中包括：等级保护、云安全、风险管理、安全法规、安全管理、安全服务、安全整体解决方案，以及信息防泄漏、数据保护、信息全生命周期管理等话题。

当前，我们面临着信息产业更新换代、迅猛发展的新形势，网络技术、计算机技术日新月异。中国信息安全产业近些年来得到了快速的发展。赛迪顾问软件与信息服务业研究中心高级分析师贾娟说，到 2012 年，中国信息安全产品市场规模将会达到 166.58 亿元，主动性安全产品将更受欢迎，同时新应用推动安全网关升级换代，安全审计应用领域也将会更加广泛。

随着网络的快速发展，网络应用类别越来越多，物联网、云计算、三网融合、移动互联网、手机支付等新兴应用给我们带来了技术层面和业务层面的全新变革。随之而来的应用复杂度和风险也

越来越高。

工业和信息化部信息安全协调司司长赵泽良在会上表示，保障国家信息安全，把握好信息化发展方向，关系到国家的根本利益。没有国家的信息安全，就没有真正意义上的经济、政治、文化和国防安全。目前，互联网发展迅速，创新活跃，应用广泛，已成为现代社会重要的信息基础设施。但网络与信息安全问题也日益突出，对国家经济安全、政治安全、社会安全、文化安全带来新的挑战。

公安部网络安全保卫局郭启全处长表示，在基础信息网络和重要信息系统的安全严重关系到国家安全、社会稳定以及人民群众切身利益的今天，信息安全问题已然成为事关全局的战略性问题。近年来，有关部门围绕信息安全保障体系建设，在信息安全等级保护、风险评估、标准制定、产品开发及打击各种网络违法犯罪活动等方面取得了积极进展。在这种情势下，将信息安全等级保护确定为提高国家信息安全保障能力、维护国家安全、社会稳定和公共利益的一项基本制度，是非常必要的。

## 政府之声

### 工业和信息化部抗震救灾工作快报

文章来源：中国信息产业网

#### 一、工业和信息化部已开展工作情况

4 月 18 日 8 时，工业和信息化部青海玉树抗震救灾指挥领导小组召开第五次会议，工业和信息化部部长李毅中刚从国外出访返京就立即参加会议，听取汇报并提出明确要求；工业和信息化部副部长苗圩传达了 17 日中央政治局常委会精神和胡锦涛总书记的重要指示。

会议要求，要按照党中央、国务院的统一部署，全力以赴投入抗震救灾工作，当前要重点做好以下工作：一是尽快全面恢复通信，保障通信机房和移动基站的油料供应，进一步提升通信质量。二是继续组织做好救灾物资保障，重点做好药品、医疗器械及其它救灾物资的储备和调运，及时保质保量地将所需物资运抵灾区。三是在做好当前工作基础上，尽早启动灾后恢复重建规划工作，重点放在通信基础设施恢复上，认真调研、科学规划。要摸清灾区工业及中小企业的受损情况，尽快制定生产恢复方案。四是组织好部机关的捐助活动。五是继续做好值班值守工作。

#### 二、当前通信恢复和应急保障基本情况

截至 18 日 7 时，青海玉树州 6 个县对外通信保持稳定。全州 45 个乡镇（镇）都有通信手段，又

有 4 个乡镇恢复了移动通信。全州 8 个通信局保持工作正常，已抢修恢复全部 14 个模块局，恢复退服基站 24 个，抢修光缆 71 皮长公里。三家基础电信运营企业共出动抢险人员 906 人，各类应急通信车辆 75 台、卫星电话 132 部、发电油机 344 台、其它应急通信装备 47 台开展抗震救灾通信保障工作。中国电信已调集 1500 部抗震救灾手机于 17 日 15 时运抵灾区。16 日 8 时至 17 日 8 时，玉树地区共有 234 部卫星移动电话提供通信服务，成为抗震救灾中确保联络的有效手段，发挥着重要作用。累计发送防震自救常识等公益短信 6203 万条。

### 三、救灾物资保障工作

协调石油供应企业全力保证灾区用油需求，截止 17 日中午 12 时中国石油累计发出运油车 112 辆，汽柴油共计 2041 吨。四川省经信委组织本省电力公司向玉树灾区派出 2 个救援队伍；协调成都铁路局运送甘孜州救灾用成品油 20 个车皮，共计 1000 吨，协调中石油四川分公司紧急调运成品油 93 吨。

### 四、有关工业企业抗震救灾情况

工业企业积极响应号召，发挥自身优势，主动投入到抗震救灾工作中。中联重科集团、柳工集团、山推股份公司等工程机械企业紧急集结 60 台中型挖掘机、25 吨汽车起重机、10 台推土机、装载机、压路机等设备随时赶赴灾区。东风雪铁龙、比亚迪、丰田及其与一汽和广汽的合资企业、广汽本田、福建戴姆勒等汽车企业积极向灾区进行捐助。

## 国家集成电路公共服务联盟在无锡宣布成立

文章来源：新浪科技

4 月 20 日，由工业和信息化部软件与集成电路促进中心(CSIP)、上海集成电路技术与产业促进中心、国家集成电路设计深圳产业化基地等 8 家单位共同发起组建的国家集成电路公共服务联盟在无锡举办成立仪式，宣布联盟正式成立。

目前，来自全国的 19 家集成电路公共服务机构加入了联盟，联盟成员单位服务的集成电路设计企业达全国总数的 90%。

该联盟于 3 月初向社会发起倡议书，得到了全国集成电路公共服务机构的积极响应。3 月底联盟挂靠单位工业和信息化部软件与集成电路促进中心代表联盟发起单位向工业和信息化部电子信息司提交了《关于发起成立国家集成电路公共服务联盟的请示》，电子信息司大力支持，很快批复了《关于同意发起成立国家集成电路公共服务联盟的复函》并给予殷切希望。《复函》中，“希望联盟加强组织建设和完善工作，力争在较短时间内达到最佳状态。”，“希望工业和信息化部软件与集成电路促进中心积极发挥作为联盟挂靠单位的作用，为联盟工作创造良好条件，重要事宜及时报告我司”。

4 月 2 日联盟在 CSIP 成功举办了筹备会议，通过了联盟章程、组成人员名单及工作任务等重大事项。

国家集成电路公共服务联盟打造的交流、沟通、合作平台，对推动集成电路产业公共服务体系建设提供了有效的模式与渠道。联盟将根据产业发展需要，提供公益性公共服务，提高企业自主创新能力和生产效率，降低企业研发成本和风险，促进集成电路产业协调、可持续发展。

## 工信部发布《移动电话机定制管理规定》

文章来源：中国信息安全博士网

中国信息安全博士网讯：日前，工业和信息化部发布了《移动电话机定制管理规定》，这是我国首次针对移动电话机定制业务发布的管理条例。规定中，对信息安全管理责任做了明确规定，规定定制方应加强对定制话机内置业务的审查，严格落实信息安全管理责任；同时还明确规定了定制方不得限制网络。

以下是《移动电话机定制管理规定》全文：

### 移动电话机定制管理规定

(工信部电管[2010]4 号)

#### 第一章 总则

第一条 为规范移动电话机定制行为，保护消费者合法权益，依据《中华人民共和国电信条例》以及有关法律法规，制定本规定。

第二条 移动电话机定制是指基础电信运营企业根据业务发展需要与移动电话机生产企业签署协议，由其生产满足特定业务要求移动电话机的行为。

第三条 基础电信运营企业（以下简称“定制方”）向移动电话机生产企业定制移动电话机，适用本规定。

第四条 工业和信息化部负责对移动电话机定制行为进行监督管理。

#### 第二章 定制要求

第五条 定制方在定制前，应制定定制规范。定制规范应符合现行国家法律法规、国家标准、通信行业标准或技术规范以及工业和信息化部的有关规定。

第六条 被定制的移动电话机（以下简称“定制话机”）应获得电信设备进网许可证、粘贴进网许可标志。

第七条 定制方与移动电话机生产企业应当明确约定双方在产品质量和售后服务等方面承担的

责任。

第八条 定制方应加强对定制话机内置业务的审查，严格落实信息安全管理责任，保护消费者合法权益。

第九条 定制方因业务发展需要，对定制话机开展与定制业务相关必要测试的，不得与进网检测重复，不得收费、发证。

第十条 定制方在定制话机上提供自营增值业务时，不得限制消费者使用其他增值业务服务商提供的增值服务。

第十一条 定制话机不得锁定网络，应允许消费者选择其他电信运营企业提供的同制式网络服务，并能实现基本的通信功能。

第十二条 定制话机应标明定制方的公司名称或品牌标识。

第十三条 定制话机可根据定制方业务需要设置相应特殊功能键，但不得影响基本操作功能键的正常使用。

第十四条 定制话机不得内置固化的 SP 代码、SP 服务链接以及 SP 客户端软件。

第十五条 定制话机应以说明书等方式履行告知义务，说明其特有的业务功能、软件和特殊功能键的使用方式和范围。

### 第三章 定制管理

第十六条 定制方应将定制规范报工业和信息化部备案。定制规范发生变更的，应于变更后 15 日内报工业和信息化部。

第十七条 定制方应于每季度第一个月 15 日前将上季度定制话机的网络制式、型号、生产企业和定制数量等信息报工业和信息化部。

每年 1 月 31 日前，将上一年度定制工作总结报工业和信息化部。

第十八条 移动电话机生产企业申请定制话机进网许可时，应提交与定制方签署的定制协议或定制方出具的定制证明。

第十九条 定制方定制已获进网许可证移动电话机，如定制话机发生技术、外型改动的，需进行检测或重新办理进网许可证。

定制话机外型改动较小，原进网许可证申请单位要求减免测试项目的，可将改动前后的照片、电路原理图、改动说明和改动后的样品等交工业和信息化部审核。经工业和信息化部同意，可以减免测试项目。

第二十条 定制方应积极配合工业和信息化部组织的移动电话机证后监督抽查工作，必要时提供符合要求的样品。

### 第四章 监督管理

第二十一条 定制方和移动电话机生产企业在定制业务推广前应开展售后服务、维修的相关培训，防止出现因服务不到位引发的纠纷。

第二十二条 违反本规定，定制方定制未获得进网许可证的移动电话机、定制话机未粘贴进网许可标志的，由省、自治区、直辖市电信管理机构依照《中华人民共和国电信条例》的有关规定处理。

第二十三条 违反本规定，有下列行为之一的，由工业和信息化部或省、自治区、直辖市电信管理机构依照《中华人民共和国电信条例》的有关规定处理：

- （一）限制消费者使用其他增值业务服务商提供的同类增值服务的；
- （二）锁定网络，不允许消费者选择其他电信运营企业提供的同制式网络服务的。

第二十四条 违反本规定，对定制话机进行重复检测、收费、发证的，由工业和信息化部责成定制方进行整改，并视情况给予通报。

第二十五条 违反本规定，有下列行为之一的，由工业和信息化部责成定制方和移动电话机生产企业进行整改，并视情况给予通报：

- （一）未标明定制方公司名称或品牌标识的；
- （二）定制话机设置特殊功能键，影响基本操作功能键使用的；
- （三）内置固化的 SP 代码、SP 服务的链接以及 SP 客户端软件的；
- （四）未履行告知义务的；
- （五）定制话机发生技术、外型改动，未按规定报工业和信息化部审核的。

## 第五章 附则

第二十六条 本规定由工业和信息化部负责解释。

第二十七条 本规定自发布之日起施行。

# 江苏实战演练世博期间网络安全突发事件

文章来源：新华网

4月21日消息，重要网站受到黑客攻击后，相关部门立即启动应急处理机制，并在几十分钟内迅速恢复网站正常运作。为备战上海世博会，江苏省相关部门和企业21日共同举行“护城河行动”——互联网网络安全实战应急演练。

记者在演练现场看到，假设由于黑客控制了15000台电脑，对江苏省某重要金融网网站发起攻击，几分钟时间内，该网站流量从1兆迅速增加到105兆，造成网站服务器瘫痪，网页无法访问，网上银行也无法操作。这种黑客攻击方式被称为“分布式拒绝服务攻击”。

网站遭遇攻击后，相关移动运营商通过内部研判立即启动内部应急预案，并上报江苏省互联网应急办，经过江苏省通信管理局专家现场研究后，启动二级应急预案，各运营商共同行动，一方面

通过流量清洗设备过滤异常流量，一方面对发动攻击的 IP 地址进行封堵，最终使网站恢复正常。

演练还模拟了世博会期间政府门户网站遭遇网页恶意篡改的应急处理过程。

本次演练是江苏省首次组织同类应急演练，由江苏省通信管理局指导，由国家计算机网络应急技术处理协调中心江苏分中心具体实施，演练成功实现多家基础电信运营企业跨网的联动处置，并有效调度了业内应急支撑队伍的协同参与，检验了江苏省互联网网络安全应急预案的可操作性，完善了世博会互联网网络安全保障的应急准备工作。

## 病毒播报

### 病毒预报（2010.4.19-2010.4.25）

文章来源：信息安全协调司

国家计算机病毒应急处理中心通过对互联网的监测发现，近期计算机用户受到一些恶意电子邮件的威胁，其附件是病毒或是恶意后门程序。

这些恶意邮件内容通常是一些欺骗性的假信息，其中附件多数是恶意后门程序。一旦操作系统存在漏洞，附件中的恶意后门程序就会入侵感染计算机系统。恶意攻击者首先将近期的热点话题或是欺骗性信息作为邮件的内容，利用社会工程学诱使计算机用户点击包含恶意代码程序的附件，进而下载并运行邮件的附件。

这些带有病毒附件的电子邮件具有以下特征：

一、电子邮件主题为近期受关注的热点话题，具有很强的针对性。借助近期热点话题，假冒恶意电子邮件，采用社会工程学的原理诱骗计算机用户点击其中的病毒附件，进而被恶意攻击者远程控制。

二、利用第三方软件存在的漏洞进行传播。恶意攻击者利用近期曝出的第三方软件的漏洞进行传播，一旦计算机用户没有及时对软件进行修补或是忽视其软件存在的漏洞，就会给恶意攻击者造成可乘之机。

三、打开后门程序，为进一步的攻击做好准备。恶意攻击者并没有迫使受感染计算机系统直接下载恶意木马程序来盗取计算机用户系统中的私密信息，而是将附件中后门程序植入操作系统中，远程控制用户的计算机系统后，再进一步的发起攻击。

**专家提醒：**

针对以上情况，国家计算机病毒应急处理中心建议各重点企、事业单位和个人用户采取以下措施来抵御病毒邮件的入侵。

- 1、及时下载安装操作系统的漏洞补丁程序，同时也要关注热门第三方应用程序的漏洞更新，应尽可能及时升级软件到最新版本。
- 2、要及时升级计算机系统中防病毒软件和防火墙；在使用计算机系统收取电子邮件的时候，最好打开系统中防病毒软件的“邮件监控”功能，同时打开防火墙。
- 3、不要随意点击或运行通过 QQ、MSN、电子邮件发来的陌生链接地址或文件，即便是好友发来的祝贺电子贺卡、图片或链接也要在确认后再打开。
- 4、提高自己私密性数据的安全，例如银行账号密码，信箱密码，IM 通讯密码等，最好经常更换或是设置比较复杂的帐户密码。

## 被 Rootkit 感染的 XP 系统无法安装最新补丁

文章来源：赛迪网

4 月 19 日消息，据国外媒体报道，一些最新 Windows XP 安全更新将不能安装在被 Rootkit 病毒感染的计算机。Rootkit 是一种隐蔽的恶意软件，把自己隐藏在 Windows 操作系统深处避开检测。

微软称已经采取行动，因为 2 月份发布的类似的更新使那些被 Alureon rootkit 病毒感染的计算机不断地死机。如果一个系统被 Alureon rootkit 病毒感染并且终止安装，这个最新的更新能够发现这个病毒。

微软为 Windows 发布的最新的一批补丁是在 4 月 16 日发布的，其中一些补丁修复了 Win 内核中的一些安全漏洞。这是 Rootkit 病毒设法隐藏的地方。

当 Alureon 病毒出现的时候，它监视网络通讯并且收集用户名、口令和信用卡号码。它还为攻击者提供感染计算机的后门。

这个病毒第一次出现是在 2008 年，一直通过论坛、被黑的网站和假冒的按点击付费的加盟计划等途径传播。

微软为这个安全补丁发布的通知解释了哪一种异常情况会阻止 Windows XP 用户使用这个补丁。微软在声明中说，系统上的异常情况可能是计算机病毒感染造成的。这些病毒修改了某些操作系统文件，从而使被感染的计算机不兼容这个内核更新。

微软希望不使用这个补丁以避免出现 2 月份曾经发生过的事件。那次事件让许多用户努力解决让自己的计算机恢复工作的问题。微软还要避免人们因为软件更新引起系统崩溃而担心软件更新的情况。

目前还不清楚有多少人不能使用这个安全补丁。微软敦促那些被感染的用户清除这个 Rootkit 病毒。微软建议使用其恶意软件清除工具或者使用其它厂商的 Rootkit 病毒检测工具。

## 4 月 19 日病毒预警：谨防“埃卡”和“毒蝙蝠”

文章来源：比特网

### 一、今日高危病毒简介及中毒现象描述：

TrojanDropper.Ekafod.r “埃卡”变种 r 是“埃卡”家族中的最新成员之一，采用“Microsoft Visual C++ 6.0”编写，经过加壳保护处理。“埃卡”变种 r 运行后，会在被感染系统的“%SystemRoot%\system32\”和“%SystemRoot%\system32\dllcache\”文件夹下分别释放恶意 DLL 组件“eodg3.dll”、“eodgt.dll”和“tata\_1.dll”。释放完成后，原病毒程序会通过创建批处理文件“375519961057540.bat”并调用执行的方式将自身删除，以此达到消除痕迹的目的。“埃卡”变种 r 会遍历当前系统中运行的所有进程，如果发现某些指定的安全软件存在，便会尝试将其强行关闭，以此达到自我保护的目的。在被感染计算机系统的后台连接骇客指定的站点“www.f\*download.com”，获取“恶意程序下载列表”，然后下载文件中所指定的恶意程序并自动调用运行。其所下载的恶意程序可能为网络游戏盗号木马、远程控制后门或恶意广告程序(流氓软件)等，致使用户面临更多的威胁。

Trojan/BAT.lh “毒蝙蝠”变种 lh 是“毒蝙蝠”家族中的最新成员之一，采用“批处理”编写。“毒蝙蝠”变种 lh 运行后，会在被感染系统的“D:\soft\bat\v9.0\”文件夹下释放恶意文件“winnt32.exe”，并将其依次复制到“%SystemRoot%\system32\”、“%SystemRoot%\repair\”和“%SystemRoot%\”文件夹下，分别重新命名为“WinUpdate.exe”、“internet.exe”、“winu.exe”和“pat32.exe”。“毒蝙蝠”变种 lh 会在桌面上创建 Internet 快捷方式“资讯摘要”和“综合搜索”，诱导被感染系统用户进行访问，从而给骇客带来了非法的经济利益。“毒蝙蝠”变种 lh 还会在被感染计算机的后台强行篡改系统中的“hosts”文件，从而利用域名映像劫持特性来屏蔽被感染系统用户对大量常用站点的访问，由此给用户的正常网络操作造成了极大程度的干扰

### 二、针对以上病毒，比特网安全频道建议广大用户：

1、最好安装专业的杀毒软件进行全面监控并及时升级病毒代码库。建议用户将一些主要监控经常打开，如邮件监控、内存监控等，目的是防止目前盛行的病毒、木马、有害程序或代码等攻击用户计算机。

2、请勿随意打开邮件中的附件，尤其是来历不明的邮件。企业级用户可在通用的邮件服务器平台开启监控系统，在邮件网关处拦截病毒，确保邮件客户端的安全。

3、企业级用户应及时升级控制中心，并建议相关管理人员在适当时候进行全网查杀病毒。另外为保证企业信息安全，应关闭共享目录并为管理员帐户设置强口令，不要将管理员口令设置为空或过于简单的密码。

截至记者发稿时止，江民的病毒库已更新，并能查杀上述病毒。感谢江民科技为比特网安全频道提供病毒信息。

## 手机 QQ 疯狂爆发“72ub 有惊喜”病毒

文章来源：多彩空间 Elife9.com

近日，无数 QQ 群里大量收到用手机 QQ 自动发送的“上 [www.72ub.cn](http://www.72ub.cn) 有惊喜”的消息，零点现已确认，[www.72ub.cn](http://www.72ub.cn) 是流氓网站、病毒网、钓鱼骗人网站，大量发送不良信息的网站，若你的 QQ 收到对方 QQ 发送的上述信息，说明对方 QQ 已经被“劫持”了，零点完全确认：72U 是恶意手机病毒！这个病毒应该是 23 日 0:00 以后爆发的，而且专门针对于手机 QQ 用户。

输入 [www.72ub.com](http://www.72ub.com) 网址，是一个号称测虎年运气的网站，并会自动转向新浪的一个名叫芑倬勒:fengyun 的博客，页面上面列数了“用移动手机拨打 125906586864 参加身份验证，立马拿到二百圆话费，太棒了！”的信息。

如果你出于好奇，点击此网站，那就是大大的杯具了！这个挂马网站会自动修改你的 QQ 签名成“测你的虎年运势 [www.72ub.com](http://www.72ub.com) 我试了太准了！”，并以近似疯狂的手段向 QQ 好友或 QQ 群爆发性大量发送“上 [www.72ub.cn](http://www.72ub.cn) 有惊喜”的恶意消息。

更大的杯具是，据零点研究了一晚上，有些杀毒或清马软件官网虽然说这是病毒，但现在为止，好像没发现任何能够干死这个病毒的杀毒软件！

更更大的杯具是，零点观测了一个通宵，发现这个病毒的传播速度和强度几乎超出了历史上所有的病毒，截止现在，几乎挂满了各大门户网站的博客网页！

还是零点的研究，处理办法，似乎只有一个，重装 QQ！

据国外某网站称：此病毒主要通过低端品牌手机登陆的 QQ 传播，因为有些低端手机内置了自动发送程序，一旦用这种带有内置自动发送程序登陆 QQ 之后，即便以后你没有登陆你的 QQ，手机也会自动以你 QQ 账号发送上述垃圾信息。零点提醒您：不要用没有安全保障的低端手机上网或者登陆聊天软件，只能这样了！

以下是关于 72UB 病毒的网络投诉信息：

欺诈，误导短信，我在朋友的 QQ 个性签名上看到了龙博高通公司(10667171)的 2010 运势测试网站([www.72ub.com/](http://www.72ub.com/))，出于好奇和信任我就点播了，他们网页上面说的是测试 2010 运势每次两元，根据他们的要求我把生日姓名发过去了，结果回复过来又要问是男是女，我只好回复，结果又要证明测试人的正确信息，我又得回复，结果回过来的就几个字说要下载全文还要回复，我又回复

了，结果回过来的是给存到了缓冲区，要下载还要回复，就这样一步一步的往里带，钱越花越多，但就是不给结果，本来说的两元，我花了 10 元还没有见到测试结果。后来我发现上当后，去刷新我朋友的 QQ 资料，发现那个 2010 运势测试的个性签名又没有了，然后到网上查找相关信息，也发现很多网友被骗了，请有关部门认真查处一下！

#### 友情提示：

- 1、请查看你的 QQ 签名，判断是否中毒，如果发现你的 QQ 好友给你或 QQ 群发送此病毒信息，请及时通知好友；
- 2、如果发现在本论坛出现此信息，请及时告知管理或版主进行清除；
- 3、加强防范，及时升级杀毒软件；
- 4、据说，NOD 可以清除此病毒，未作验证；
- 5、如果哪位高人好的清除办法，请发上来共享！

## 产业动态

### 赛门铁克发布 2011 测试版安全软件将占用更少内存

文章来源：赛迪网

4 月 20 日消息，据国外媒体报道，安全软件公司赛门铁克星期一推出了 2011 诺顿互联网安全套装软件和诺顿杀毒软件的测试版并且推出了一些全新免费的安全工具。这些软件现在全部提供下载。

诺顿互联网安全 2011 是赛门铁克公司全套的互联网安全软件，包括杀毒、反间谍软件、防火墙和反垃圾邮件工具等。在过去的几年里，一些人总是说诺顿安全软件速度慢和消耗太多的内存。但是，赛门铁克称，它要在 2011 版本的安全软件中改善这些功能吸引人们安装这个软件，更快地扫描和使用更少的内存。

赛门铁克补充说，除了安全功能之外，它还提供了一种名为“System Insight 2.0”的新功能，在其它应用程序占用太多的内存和系统资源的时候提醒用户。2011 版互联网安全和杀毒软件产品的新功能还有扫描通过你的浏览器、电子邮件或者即时消息程序提供的下载。

赛门铁克 2011 版安全软件更新的功能包括“诺顿身份安全保护”和“诺顿网页安全”。前者旨在帮助创建和管理你的所有口令。后者旨在分析和评级来自谷歌、雅虎和必应等搜索引擎的搜索结果以保证网站没有恶意软件。

赛门铁克还推出了一些免费的安全工具。“Norton Safe Web Lite”是上述诺顿网页安全工具的一

个免费的版本，旨在提醒用户搜索结果中的不安全的网站。“Norton Safe Web for Facebook”是对抗针对社交网络网站的 Koobface 和其它恶意软件的工具。

赛门铁克称，免费的诺顿急救工具提供了两个单独的工具，旨在清除恶意软件。Norton Power Eraser（诺顿强力清除器）能够清除传统的安全软件也许不能删除的恶意软件。Norton Bootable Recovery Tool（诺顿可启动恢复工具）能够帮助用户创建一个急救盘，以便在系统被攻破无法使用的时候利用这个急救盘。

诺顿互联网安全 2011（下载测试版）、诺顿杀毒 2011（下载测试版）和 Norton Safe Web Lite 等软件可以从赛门铁克测试网站下载。

## 首个云存储标准发布

文章来源：全球 IP 通信联盟

网络存储行业协会（SNIA）发布了第一个云存储标准--云数据管理接口（CDMI）。

CDMI “提供了访问云存储和管理云存储数据的方式。”云存储被定义为在网络上随需提供虚拟存储的一种服务方式，也被称为数据存储即服务（DaaS）。客户可以根据实际存储容量来支付费用。

SNIA 表示任何根据固定的容量增加量来提供存储的方式都不是云存储。

CDMI 同时支持块（逻辑单元号或虚拟卷）和文件（通过通用互联网文件系统、网络文件系统或 WebDAV 访问的文件系统）存储客户端。块和文件的底层存储空间被抽象化为封装器。

不过，它也可以抽象化为简单的表存储空间以供数据库操作。这里的重点是可扩展性而不是功能。CDMI 并不基于虚拟化的关联表（RDBMS）实例。每个 RDBMS 都有自己的专有接口，而 CDMI 甚至都没有在云里面提供访问虚拟 RDBMS 的方式。

SNIA 表示：“由于该领域的创新速度很快，我们最好还是等待这种类型的云存储进一步发展，而不是马上标准化该类存储的功能接口。”

还有第四个存储抽象化，就是对象抽象化。CDMI 将对象看作是可以通过 URI（统一资源 ID）来访问的独一无二的项目。SNIA 表示数据对象被看作可以创建、搜索、更新和删除（CRUD--上述操作的首字母缩写）的独立资源。

通过对象，封装器可以封装其他封装器。

SNIA 存储行业资源域模式（SIRDM--SNIA 喜欢首字母缩写）提供了一个处理云元数据的框架。元数据能够详细表明存储中的数据是如何在云中管理的。

CDMI 是一个直接的规范，能够让大多数旧的非云存储产品访问方式演进成云存储访问。它提供了数据中心利用云存储的方式。数据中心对现有网络存储资源的访问应该可以相当轻松和透明地切

换到 CDMI 云存储资源。

SNIA 在这项标准的开发上动作很快。我们可以设想许多云存储产品将很快遵守 CDMI。

CDMI 没有提供通过可靠性和质量来衡量云存储提供商质量的方式。它不能防止像像微软系统那样的数据丢失风险。

不过，SNIA 应该要帮助客户从遵守 CDMI 的云存储提供商切换到其他提供商。SNIA 并不规定成员应该如何向客户提供服务质量。SNIA 是一个行业协会，其宗旨是促进成员间的共同协作，以便让客户可以使用不同的 SNIA 成员的产品并根据需要在这些产品间切换。

## 专家视角：从 RSA 看网络应用安全发展趋势

文章来源：比特网 作者：联想网御 王智民

信息安全，其核心在于“信息数据”的安全，而在数据处理中，应用才是关键。随着网络的快速发展，网络应用类别越来越多，应用复杂度也越来越高，人们逐渐发现，单纯解决数据的访问和传输的安全已经无法很好地保障信息安全，必须高度重视维护关键应用的安全，从数据的产生、计算和存储等多个角度来思考和解决。因此，对于“网络应用”安全的关注度也逐渐升温。在本次 RSA 大会上，技术专家、知名安全厂商谈论的焦点来看，网络应用安全呈献出以下几大发展趋势。

### 趋势 1：WEB 应用安全市场成为各应用安全厂商的必争之地

如今，越来越多的企业用户已将核心业务系统转移到网络上，WEB 浏览器成为业务系统的窗口。在此背景下，如何保障企业的应用安全，尤其是 Web 应用安全成为新形势下信息安全保障的关键所在。Gartner 的一份分析报告指出：在调查的企业数据中心中，92%的 Web 应用有安全缺陷；80%存在跨站攻击；高达 62%存在 SQL 注入风险，而参数篡改和 Cookies 毒化也分别达到 60%和 37%；同时，专门针对应用层进行攻击的手段越来越多，越来越难以防范。

从技术的角度，WEB 应用的安全主要涉及两个方面：服务器端和客户端。服务器端的安全隐患主要有脚本安全、SQL 注入、“盗链”、DoS/DDoS 攻击。而客户端的安全隐患主要是 Cookie、证书、可执行代码的限制、安全选项设置不当等。

参加本次 RSA 大会的国外安全厂商中，有相当大的比重在试图提供完善的 Web 应用安全解决方案，国内安全厂商如绿盟科技、联想网御也都展示了自己在 Web 应用安全防护方面的探索和努力。可以看出，各安全厂商已经开始瞄准并不断发力此细分市场。

### 趋势 2：加强应用本身的安全是网络应用安全的关键

网络应用之所以不安全，其中很关键的一点是应用程序本身不安全，给网络攻击留下了可乘之机。

如何保障网络应用服务本身的安全也成为本次 RSA 大会讨论较多的话题。与会者从网络应用程序开发、协议标准的制定到业务逻辑等各个层次进行了探讨。在本次 RSA 展会上，记者也注意到有几家安全厂商已经将目光覆盖到应用程序开发过程中，提出了所谓的代码级方案解决方案，确保应用服务本身的安全漏洞尽量少，尽可能地消除程序的安全漏洞带来的可乘之机。

### 趋势 3：身份管理成为应用访问控制主流技术

基于身份的应用管理包括身份识别、权限控制、行为审计等多方面。网络边界正在逐渐变得模糊，移动终端越来越普及，我们面临的网络世界不再是清晰的内部与外部，身份成为网络世界的辨识要素，因此对于身份的管理就显得尤为重要。本次 RSA 大会充分印证了这一观点。相当数量的安全厂商展示了自己的身份管理解决方案，如：双因子认证、身份审计等。

传统的身份管理技术主要采用所谓的 AAA 技术，然而随着应用安全需求的发展，不再是身份的识别和权限控制那么简单，更多的是希望通过“身份”的管理来实现应用访问控制。比如当前比较流行的 P2P 应用占据了大量的网络带宽，在某些场合，事实上已经严重影响了正常的业务操作，成为企业和网络运营商头疼的问题，但又不能简单的禁止这些应用。于是如何识别这些 P2P 应用，如何给不同的身份配置不同的 P2P 应用权限，如何监控这些应用下载的数据的合法性和安全性，都成为了应用访问控制的关键。

除此之外，本届 RSA 展会上有关身份识别、权限控制、行为审计等安全类产品也备受关注。

### 趋势 4：越来越多的厂商采用多核硬件架构来解决应用安全处理性能不足的问题

要确保纷繁复杂的网络应用的安全，就不得不深入分析报文，不仅仅需要分析报文的传输层，还需要分析报文的应用协议层，应用数据内容，甚至还需要分析报文之间的关联性，这就给应用安全技术带来更大挑战。既要分析准确，又要确保报文的实时性，在一定程度上，这两者是矛盾的，单纯希望从软件角度解决此矛盾已经不再现实，必须寻求更高更强的硬件架构才能解决根本问题。

在本次 RSA 大会上可以看到，部分实力雄厚的应用安全厂商已经采用多核硬件架构来解决性能瓶颈，将应用安全的处理能力提升到以前的 5~10 倍，基本满足了当前对网络应用安全的性能要求。有的国外厂商在非常显眼的位置宣传“用多核，实现真正的 10G IPS”。事实上，国内厂商采用多核架构的高端 IPS 产品也有成功案例。记者发现此次联想网御参展的 KingGuard IPS 9202 在多项关键性能指标上已超过国外厂商。

随着信息化建设不断深入，基于网络的关键应用越来越丰富，特别是云计算已成为发展趋势。未来更多的业务将以 WEB 应用方式呈现，信息安全也必将从以边界防护为主向应用和数据安全防护为主过渡，同时加强在应用研发、部署以及维护等方面的安全管理并辅以必要的技术设备，才能跟上信息化发展的步伐，实现协调发展。

## 微软首宗针对中国大企业盗版案宣判：获赔 217 万

文章来源：新浪科技

4 月 22 日消息，上海浦东新区人民法院今天一审判决大众保险股份有限公司需向微软赔偿 217.28 万元，因其使用了盗版的微软软件。

这是微软首次在中国针对大型企业发起诉讼，也是微软在中国区知识产权案中索赔最大金额。微软表示，希望借此来推动大型企业使用正版。

### 首宗针对大企业盗版维权

大众保险于 1995 年在上海成立，由上海国际集团有限公司、上海国际集团资产管理有限公司、上海市城市建设投资开发总公司、上海大众公用事业(集团)股份有限公司等 26 家大中型企业投资创建，目前注册资本为人民币 11.46 亿元。

被告大众保险股份有限公司缺席一审判决宣判，新浪科技未能立即联系到大众保险就此事置评。

微软中国高级知识产权总监于维东透露，与大众保险就版权问题的接触始于 2007 年，但双方谈判破裂，最终，微软于去年选择了采取诉讼措施。

微软指控大众保险公司至少安装使用了 9 种盗版微软软件共计 450 套，诉请赔偿 224.957 万元，于维东说：“大众保险安装使用我们盗版的软件包括 Windows 系列、Office 系列、Windows Server 系列以及 SQL Server 系列等。”

浦东法院在此案件中发挥了重要作用。“法院进行了诉讼过程中的保全，在保全当中，又发现了很多证据，也发现了一些对我们提起诉讼有利的其他一些证据。”于维东拒绝进一步透露如何发现新证据的细节。

微软代理律师、上海市凌云永然律师事务所袁新忠在判决后通过微软新闻稿称，浦东新区法院通过“高超的办案技巧以及大量耐心细致的工作使得案件得以圆满解决”。

### 欲借此推动大企业正版化

几乎每一个企业都会使用到微软的软件产品，这其中，大型企业自然成了微软的重点关注对象。

“并不是微软跟哪一家企业过不去或者怎么样，通常都是有相当多阶段的沟通和交流。”于维东说，“目前我们碰到最大的问题，是大家都在用而没买。”

这是微软首次在中国对大型企业发起了维权行动，此前，微软曾针对一些中小型企业，如对上海大亚公司与深圳豪佳的公司发起诉讼，分别获赔 40 万与 50 万人民币。

于维东表示，中国政府着力推进正版化，是这一行动发起的背景。政府的行动方向，从 2007 年开始，已经从清理电脑市场、网络侵权等渠道层面重点转向了企业层面。

“企业盗版对软件业伤害最大，从这个意义上讲，这个案子本身有很大的意义。”于维东表示，微软希望通过此来“尽最大的力量推动企业正版化，特别是大企业的正版化。”

于维东称，微软在中国已经从“很少寻求司法救济”转为了“司法与行政救济并重”的策略。他拒绝透露微软在中国针对多少家企业采取了法律行动。

### 承诺对个人用户不采取强硬措施

这一案件的宣判选在了 4 月 26 日知识产权日到来前夕，此举被认为有利于彰显中国在打击盗版上的决心。代表商业软件企业利益的商业软件联盟(BSA)于去年 5 月援引来自 IDC 的数据称，中国的 PC 软件盗版率在 2008 年下降了 2 个百分点，达到 80%。这是继 2003 至 2007 年的 5 年间减低 10 个百分点之后的又一次降低。

由于担心强势形象引发消费者反弹情绪，微软在中国的个人用户市场的盗版，一直采取了温和策略。于维东表示，微软会采取包括价格优惠在内的多种手段来拉动正版市场，个人用户不会是微软采取强硬手段的对象，且“相当长时间都不会是”。

“在中国市场，微软在过去很长一段时间都是贯彻全球统一定价制度，但近期有很大突破，大家如果注意到的话，Windows 和 Office 针对个人用户的价格都是全世界最低的。”于维东说。

## PGP 创始人加入苹果参与系统安全

文章来源：cnBeta.com

PGP 在加密领域的大名无人不知，它的共同创始人和首席技术专家乔恩·卡拉斯近日宣布加入苹果，协助其操作系统的密钥、高度复杂程序和安全存储方面的工作。不过 PGP 技术咨询委员会将仍然存在，PGP 公司成立以来，他一直担任首席技术官和首席信息安全官。卡拉斯在安全界相当著名，它帮助过 Firefox 的安全设计，担任过 OLPC 的高级安全架构师，当然，最令他声名鹊起的自然是 PGP 的成功销售。

与他共事的同行都表示，他是一个非常有价值的成员，具有良好的人际交往能力，他的专业知识功底非常深厚，目前尚不知道它在苹果负责哪个版块，但据推测应该会加强 OS X 的存储加密，因为 OS X 至今只考虑加密用户的主目录，许多其它地方的存储文件容易被攻击。

# 技术前沿

## 影响校网稳定 苹果 iPad 遭封杀

文章来源：赛迪网

4 月 19 日据国外媒体报道，出于网络稳定性考虑，美国乔治华盛顿大学和普林斯顿大学已经封杀苹果 iPad 平板电脑。

乔治华盛顿大学表示，校园无线网络的安全特性导致 iPad、iPhone 和 iPod touch 无法接入其网络。而普林斯顿大学则称，iPad 自身故障会导致校园计算机系统崩溃，因此已经封杀了 20% 的 iPad。此外，康奈尔大学科技信息部门主任史蒂夫·舒斯特(Steve Schuster)表示，学校正监测网络和连接问题，确保 iPad 不会对其网络造成毁灭性的影响。

对此，苹果发言人表示，对 iPad 在校园内所出现的问题并不是很清楚。

## 恰当的安全控制是虚拟化成功关键

文章来源：ZDnet

身份识别和接入控制是任何安全设计的基本组成部分。知道谁或者什么正在连接到你的系统以及他们有什么许可对于保护系统安全及其数据是非常重要的。采用虚拟化，需要做出一些决定以保证建立适当的控制措施：

- 物理主机上的接入控制系统如何影响虚拟主机上的接入控制系统？
- 如果这个虚拟机是可移植的并且能够在许多物理主机上运行，如何让这些接入控制措施也能够移植？
- 一个虚拟机快照能够复制到任何物理机器上并且执行吗？
- 如果一个虚拟机在多个物理机器上复制，它的账户和口令也能够复制吗？会出现不能同步或者账户锁死的情况吗？
- 应该允许一个应用程序从任何物理主机访问另一个应用程序或者数据库吗？

作为全面的威胁和风险评估的一部分，可以并且应该提出类似的其它问题。最终，要尽可能地得到许多问题的答案，从而建立一个更安全的系统和消除潜在的部署障碍。

通过使用基于 LDAP/主动目录的身份管理系统、实施一个 SSO 系统或者使用双因素令牌等手段

实现用户身份识别外部化将取消管理存储在每一个虚拟机上的单独的身份识别的需求。虽然这对于最终用户团体来说是起作用的并且是一种推荐的方法，但是，这个方法不能完全解决管理员和应用程序接入的挑战。许多(并非全部)应用程序包括对可插入的身份识别的支持;也就是说，他们能够通过安装适当的软件模块与外部身份识别存储器进行沟通。对于不支持外部身份识别并且使用基本的身份和口令的应用程序来说，这个机构要坚持维护那个具体的应用程序的用户存储器。更糟糕的是，需要与那个应用程序及其数据交流的任何计划也许都需要用户身份和口令的硬编码。在现在和遵守法规和审计要求的年代，这种做法将很快成为一种被禁止的做法。

任何接入系统的基本的身份识别都是通过使用合法的身份和口令实现的。所有的操作系统和应用程序都包括支持基本的身份识别。即使在已经为用户实现了可插入的身份识别的时候，管理员和程序仍然使用共享的身份和口令。反对使用口令的常见的观点是，口令在防御专门的攻击方面很差，因为口令很短、结构软弱以及不经常改变。这使人们认为长的、强大的、定义维护的身份和口令将会给系统提供充分的身份识别控制。口令还消除了应用双因素令牌或者生物统计身份识别方法的成本和复杂性。在物理的、虚拟的和应用程序环境中维护管理员和程序的身份和口令或者有权限的账户是机构面临的一个更大的挑战。

## 国家安全：“谷歌地球”泄露了什么？

文章来源：中国青年报

“谷歌地球”(Google Earth)是一款由谷歌公司开发并免费提供使用的虚拟地球仪软件。与传统平面地图相比，“谷歌地球”提供的地图是三维立体的，使用者不仅可以方便地“飞上天空”，俯瞰自己的居所，而且还能寻找并标注办公地、酒店以及银行等等。若支付一定费用，还可以得到分辨率相当高的局部卫星照片，其作用甚至超过某些军用侦察卫星。

“谷歌地球”——这个互联网产业催生的“新星”，引发了人们因其对国家安全存在潜在危险的争论

既然民用目标可以轻易地被发现，那么军事设施呢？事实上，在网络地图所提供的服务面前，全球大多数国家和地区的重要军事设施都已经暴露无遗，加之有许多好事者乐此不疲地上网“发现”他国原本非常神秘的军事设施，从而引起了一些国家对军事机密和国防安全的担心，也引发了人们对“谷歌地球”存在潜在安全危险的争论。

2005 年 10 月，印度指责“谷歌地球”其卫星图片把首都新德里的国会大楼、孟买的航空母舰锚地及核反应堆以及南部数个空军基地等设施“一览无余”。

更为可怕的是，2007 年，在伊拉克武装分子的据点中就曾发现过英国军事基地的照片。为此，

多国政府都曾要求谷歌删除或者模糊一些包括军事基地、核反应堆以及政府建筑在内的敏感地区的照片，很多国家甚至谴责谷歌暗中帮助恐怖分子。

2008 年，印度政府称袭击孟买的恐怖分子使用了“谷歌地球”工具来熟悉袭击目标。英国《每日电讯报》也曾披露恐怖分子企图利用“谷歌地球”袭击英军基地。在“谷歌地球”上，人们可以轻而易举地找到英国特种部队总部驻地，还可以看到英国普斯毛斯港内的航母以及护卫舰，甚至英国军情六处伦敦总部。

从传统保密角度看，谷歌确实给国家安全带来了隐患。一般而言，卫星照片的分辨率在 30 米以下就可以发现港口、基地、桥梁、公路或舰船等较大目标，而 3~7 米的分辨率就可以发现雷达、小股部队、导弹基地、指挥所等较小目标。这就是说，这些卫星照片都是有军事价值的，难怪会引起许多国家和地区军方的强烈反应。

之所以出现种种泄密问题，跟“谷歌地球”提供的诸多功能密切相关。

首先，通过“谷歌地球”，大量重要目标图片和相关涉密信息被发布，给各国的安全保密工作带来严重挑战。“谷歌地球”推出以来，印度、韩国、以色列、英国、澳大利亚等国先后反映有大量重要目标被曝光。据英国《每日邮报》报道，3 月 20 日晚，英国政府强迫谷歌从街景地图中删除一些英国最敏感的军事和安全基地照片，防止恐怖分子利用。即使是对“谷歌地球”图片发布有审查权的美国也未能幸免，已有多处重要军事目标被公之于众。

其次，“谷歌地球”软件中的实景照片图层功能也是泄密渠道。这些照片和地图，带有地理坐标信息，可实现对特定目标的多角度解读，同时也可弥补“谷歌地球”图片时效性的不足。用户可以在街景地图上查看图片共享网站上的照片，从多角度去看特定建筑、街道的情况。而街景地图是对鸟瞰式卫星图片的补充，直观地反映有关目标的情况。两者的结合，将会使相关重要目标情况被泄露的隐患更多。

从这个意义上看，“谷歌地球”泄露的秘密为恐怖分子制造恐怖活动提供了便利，各国遭受恐怖袭击的危险性增大。4 月 3 日，谷歌街景（Google View）拍摄用车在英国白金汉郡境内一小镇取景时就曾遭当地居民围追堵截，并导致警方介入。更为严重的是，任何人都能免费查找重要的军事设施。近年来，美、英、印等国安全部门都曾破获了恐怖分子利用“谷歌地球”提供的卫星图片实施恐怖活动的案件。

此外，“谷歌地球”还具有网友自动标注功能，日积月累，大量的信息被丰富到“谷歌地球”上去。这些做法实际上能帮助别有用心的情报机构完成模糊情报的判断和确认工作。

“谷歌地球”的泄密问题，引起了世界各国的高度重视。一些国家采取多种应对措施，以防止本国重要军事机密被泄露。为避免本国机密通过“谷歌地球”泄露，也想出了种种办法。

其实，恰恰是美国最早建立了针对“谷歌地球”的防护体系。美国军方要求“谷歌地球”所公布的美国图片必须经过筛选，对敏感地区要进行模糊化处理，有的地方连 15 米的分辨率都不到，一些更为关键的军事基地打上马赛克隐去。现在，用户使用“谷歌地球”搜寻美国时不难发现，在美

国地图上有不少小片的灰色“马赛克”，它们其实就是美国的敏感地带。

由于“谷歌地球”采用的是商用卫星，参数公开，卫星经过的时间和覆盖地域比较容易确定。英国军方则据此对有关军事设施进行了伪装，驻伊英军目前已着手加强许多军事设施的伪装工作好让“谷歌地球”难现当地真容。

当前，世界上许多国家都加强了对国际互联网上泄露本国军事机密情况的监察力度。一些国家安全和情报部门已加大了对“谷歌地球”的监控力度。特别是技术侦察情报部门组织专门力量，加强对“谷歌地球”及相关网站、论坛和交流系统的侦察和监视，及时发现和掌握本国军事基地、敏感目标卫星图片在网上曝光情况和相关地标文件发布情况，为其国家有关部门做好网上地理信息安全监管和防范工作提供情报支持。

面对是否需要一个“完全不受管制”的互联网，国际社会产生了很大的分歧。一些认为互联网应该完全开放，且不受国界限制的“自由派”认为，政府对于网络的审查过滤会影响到人们自由选择的权利。

实际上，世界很多成熟的民主国家都有对网络进行审查过滤的先例。撇开军事敏感内容不说，在德国，宣扬纳粹思想的内容在互联网上无法打开；在法国，否认纳粹对犹太人大屠杀的内容也受到屏蔽，其实这些都是各国政府对他们认为不良的内容进行过滤。

一些国家与谷歌的冲突表明，网络时代正对各国的安全利益制造出前所未有的麻烦。什么是秘密，又如何保密，这些对国家安全至关重要的概念随着时代在不断嬗变。

从这个意义上看，加紧制定保护本国空间地理信息安全的相关法律法规就显得尤为重要。也恰恰是美国，早就制定了严格的军事信息管理制度和相关法律，用于限制美商业卫星公司出售有损国家安全的卫星图片。而谷歌公司购买的美国敏感地区卫星图片必须经过筛选、处理，符合要求后才能公布，而且还必须是 3 年前拍摄的。

印度、韩国等国对重要敏感的“国家安全目标”的拍摄和信息发布也均有严格限制。即使这样，这些国家也承认现行法律对“谷歌地球”这样的服务软件仍缺乏制约效力，应及时修改完善。当前，对于各国政府来讲，规范互联网，制定适合本国的规章制度，完全是职责所在。当谷歌触犯这些规章制度时，受到所在国政府的“敲打”也就在所难免了。

## 签名服务器在国库横向联网系统中的应用

文章来源：中国信息安全博士网

### 1、什么是国库横向联网系统？

国库横向联网系统是以人行国库为中心，与财政、税务、海关、商业银行等部门进行信息的横

向联网，利用电子信息和网络数据交换方式代替传统的手工单据及票据交换方式，电子缴税，全面实现国库收付业务的电子化、票据交换的无纸化操作，以增强国库资金管理的时效性和准确性，实现多个部门之间国库管理信息的资源共享，确保预算收入及时、准确、足额入库，保证财政资金的正常调度，直接服务于政府的预、决策。“横行联网”的核心思想是达到税款“实时代扣”，财政收入和拨款实时到帐，信息资源共享，完善纳税服务体系。

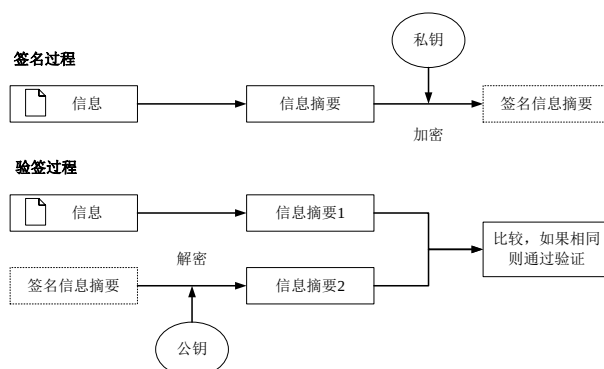
## 2、面临的主要问题是什么？

由于是多家机构参与的复合联网工程，因此存在大量的帐务、管理、统计、决策等信息相互交换。如何保证交互数据的安全性是横向联网系统建设面临的主要问题。为此由财政部、国家税务总局、中国人民银行联合起草并颁布的《财税库银税收收入电子缴库横向联网管理暂行办法》第二章基本要求第六条明确指出“电子缴库信息的传输实行全过程加密及身份确认，能够保证信息的安全性、完整性、不可篡改性和不可否认性”。

## 3、如何解决该问题？

在当前的国库横向联网信息系统中主要采用 PKI 技术，通过数字签名和签名验证来保证交互数据的安全性、完整性、不可篡改性和不可否认性。

### 数字签名原理



图表 1-1 数字签名原理

数字签名主要经过以下几个过程：

信息发送者使用单向散列函数对信息生成信息摘要；

信息发送者使用自己的私钥签名信息摘要；

信息发送者把信息本身和已签名的信息摘要一起发送出去；

信息接收者通过使用与信息发送者使用的同一个单向散列函数对接收的信息本身生成新的信息摘要，再使用信息发送者的公钥对信息摘要进行验证，以确认信息发送者的身份和信息是否被修改过。

人民银行已率先采用签名服务器完成上述技术实现，实现对缴库信息的安全保障。相较于国库横向联网系统建设初期的软件接口实现，签名服务器可提供更为可靠的签名、验证服务，优势集中

体现在：

### 1、系统压力可控

中国人民银行的国库信息处理系统将签名或验签的工作提交给签名服务器进行处理，由于签名服务器是独立的硬件设备，单独完成对数据的签名与验证签名，因此其系统的压力更可控，可以根据不同的签名或签名验证的效率选择不同档次的签名服务器。对于国库信息处理系统业务来说，待签名或签名验证的数据仅仅是通过数据接口发送给签名服务器，签名或签名验证的工作将不再占用系统主机的资源，整体的国库信息处理系统业务环境压力更加可控。

### 2、业务与安全独立

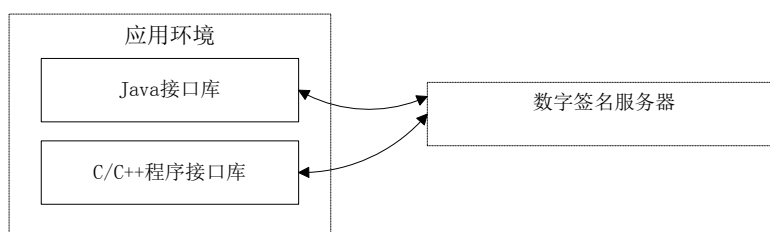
由于业务与安全部分的相对独立，在国库信息处理系统整体的业务环境中，业务系统的管理模式符合了人民银行的管理模式，一旦国库信息处理系统整体业务出现问题可以迅速的定位故障，是业务流程？还是数据发送？还是签名服务器的设备故障？

### 3、安全性高符合国家相关规定

在吉大正元硬件签名服务器实现的国库信息处理系统业务环境中，国库信息处理系统业务的签名证书将被存储到吉大正元硬件签名服务器中，签名服务器通过硬件加密卡对证书进行保存，并且不允许签名证书的私钥导出，这就保证了业务系统证书的安全性和唯一性，根本不可仿冒和伪造，大大提高了国库信息处理系统业务系统的整体安全性。同时，也满足了国家对密钥管理的相关要求。

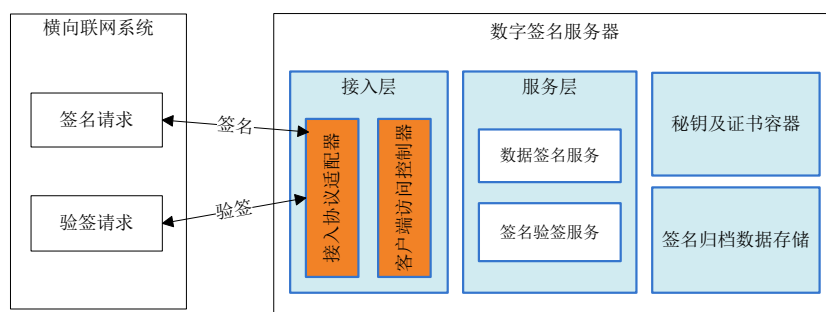
### 4、签名服务器原理

在实际的应用环境中，签名服务器为国库横向联网系统提供一套完备的客户端组件，通过对客户端组件相关函数的调用完成对缴库信息的签名、验签操作。客户端组件的形态为多种程序设计语言的程序接口库，用以满足可能面临的不同种类系统环境的需求。



图表 1-2 客户端接口库形态

签名服务器自身由接入层、服务层、密钥及证书容器、签名归档数据存储等四个核心组件构成。



图表 1-3 签名服务器系统构成

接入层位于签名服务器最前端，受理来自应用系统中的签名请求和验签请求，并返回服务处理结果。接入层包含接入协议适配器，按照特定的网络协议监听来自客户端组件的服务请求，解析协议数据和编组服务处理结果数据，将服务响应数据传输到客户端组件。

服务层提供核心签名、验签服务，该组件使用密钥及证书容器完成数据签名和验签操作。密钥及证书容器用于存放签名证书、信任证书颁发机构的证书链，该容器必须具有强安全机制予以保护。密钥对必须存在于硬件加密设备中，签名、验签过程涉及的加密、解密运算必须由硬件加密设备完成，充分保障密钥的安全性。

密钥及证书容器包含不限于一个的签名证书及密钥对，可按照客户端组件的请求使用不同的签名证书及密钥对对数据进行签名。

签名归档数据存储用于存放签名服务器运行期间所签发的数据签名及涉及事后验签所需要的特定数据，为快速定位、排查问题提供有效的数据支撑。

到目前为止，吉大正元签名服务器已经在人民银行稳定运行超过 20000 小时，富滇银行等商业银行也已陆续选用签名服务器作为国库横向联网系统中的数据安全保障。2010 年 2 月人民银行清算司发文建议：在网间结算业务中，对业务量较大的参与者，可以考虑在行内系统部署专用的硬件签名服务器，以实现快速的编签、核签处理。我们相信随着电子信息化的不断发展，签名服务器产品必然在网间数据交易中扮演越来越为重要的角色。

## 黑客攻防

### 阿里巴巴速卖通平台遭攻击

文章来源：网易科技报道

4 月 19 日，阿里巴巴公司近日上线并试运营全球小单贸易平台。该平台试运营不久后，阿里巴

巴于今日发布一则声明，声称该平台上周末遭到黑客攻击，并称其已向监管部门报案。

速卖通是阿里巴巴于近日推出的面向小企业间小单在线贸易的平台，此前尚处于试运营阶段。阿里巴巴在一份发给媒体的声明中称，这一平台网站于上个周末受到了不明身份黑客的持续恶意攻击。阿里巴巴在声明中还强调称，该平台的正式上线和进军美国将按原计划进行。

## Palm WebOS 系统存在多个安全漏洞

文章来源：比特网

4 月 19 日消息，据国外媒体报道，安全顾问公司 Intrepidus 即将在下周发表一份报告披露 Palm 公司的 WebOS 系统存在多个严重的安全漏洞。

Intrepidus 联合创始人兼首席执行官 Aaron Higbee 向 CNBC 记者 Jim Goldman 表示他对 WebOS 如此轻易被侵入感到“震惊”，并指出该系统的“架构存在问题”。

据 Goldman 的报道，Intrepidus 声称仅需向 WebOS 手机发送一条文本短信，即可实现对其控制；该公司还声称该缺陷可允许远程拨号，并轻松地取得手机上的通信录。

Higbee 向 CNBC 表示：“Palm 在推出 WebOS 系统前就已经清楚该系统存在安全漏洞，但仍将其推向市场。”

## Mozilla 将针对恶意 Java 插件进行屏蔽

文章来源：赛迪网

据安全博客 Brian Krebs 介绍，上周甲骨文公司发布了一个修复 Java 插件漏洞的更新，但 Mozilla 开发人员发现，这个更新没有删除旧版本的代码，使得系统仍然留下了漏洞代码，从而使得遗留代码成为新的漏洞。对此，Mozilla 不得不将屏蔽黑名单进行了修改，对这一恶意 Java 插件进行屏蔽。

而来自 Mozilla 的开发人员和管理员的论坛 Bugzilla 上的信息表明，Mozilla 目前还没有对这一漏洞发表任何消息。产生新漏洞的这一插件名叫“Java Deployment Toolkit”，该插件在 2008 年 4 月所发表的 Java 6 update 10 中就被发现存在漏洞，之前的版本为 6.0.200.2。JDT(Java Deployment Toolkit 的简称)插件以简化开发人员发布应用开发的程序，同时通过建立一个可透过网站执行程序的通道来方便开发人员对程序进行维护。但是该插件当时被发现的漏洞允许黑客在目标电脑上执行远端程序，而且用户只要点击一个网页就可能被黑客攻击。甲骨文在上周四发布了 Java 6 update 20，修补了 3

个 Java 插件的安全漏洞。但是没想到，新的问题又发生了。

据论坛 Bugzilla 透露，Mozilla 已经通过 Firefox 的更新机制对屏蔽黑名单进行了修改。用户可以免费的通过 Firefox 的更新对造成这一漏洞的插件进行屏蔽或关闭。Mozilla 表示，黑名单不会对系统软件造成误伤。

有研究报告显示，一些补丁对漏洞不能起到作用，新版本和旧版本往往在过渡期间会出现更多的错误和混乱。而且针对 Java 插件的更新补丁往往没有引起开发商的高度重视。特别是一些 Firefox 和 IE 用户，在安装各类 Java 插件的时候，往往没有得到相关的安全提示，只有在漏洞大范围的爆发时，才会有相应的通知。

## 黑客组织破解育碧 DRM 称育碧应多关注游戏

文章来源：多玩单机游戏

育碧（Ubisoft）新的 DRM 反盗版技术，这种反盗版技术要求玩家即使在玩单机版的时候也要一直连接在互联网上，否则将无法正玩游戏及保存游戏进度，这给玩家们带来很多不便和莫名的问题。上个月《刺客信条 2》公布以来，黑客组织一直尝试这各种方法对其进行破解，一直效果不佳。而今日，黑客组织称像 SKIDROW 已设法绕过了育碧的保护，《刺客信条 2》（Assassin's Creed II）PC 版已有一个完美下载版。

他们还在论坛上附上了一个公告：

“感谢你育碧，这个反盗版技术对我们是一个挑战，但只要我们想，没有什么东西能够阻止我们，下一次请你更多的关注游戏，而不是 DRM。”

## 海外来风

### Four Tips for Securing Social Media

CIO Zone By Laton McCartney

Facebook has more than 400 million users globally, and over 5 million Twitter messages are sent a day in the U.S. Any CIO or CSO who believes he or she can monitor this volume of traffic -- or at least the part of it that flows through their organizations -- and completely mitigate the risks is at best a cockeyed optimist. Still, there are tools and techniques you can use to lower the danger levels. Here are four tips.

### **Policies Are Not Enough**

Some companies such as IBM post thorough corporate policy documents regarding social media usage on their Web sites as step one in curtailing risk. Social media strategists, however, advise training sessions, workshops and the like to discuss the risk factors in bringing Facebook, Twitter and others onto the home court. There also needs to be follow-up and a means of alerting employees to any problems. Companies such as Modern Media Leadership Institute put on workshops for professionals and executives that address concerns like the legal issues involved with social media. The institute also puts out a social media management newsletter to update social media users on emerging issues and developments.

### **Enforcement Tools**

A number of vendors have come out with technologies for enforcing social networking security policies. These include traffic filtering solutions, access controls and data loss prevention (DLP) tools. Sophos, for example, offers encryption, access controls and data protection software for organizations seeking to curtail malware, phishing and spam incursions from social media.

DLP vendor Fidelis Security Systems has introduced a tool that it claims provides the first controls to understand the content and context of information posted to social network applications. This, says the company, enables the use of social networking for business purposes while preventing leaks of digital assets, intellectual property and identity.

### **Providers Add Muscle**

At the same time, some social networking sites have beefed up their own security, or are trying to. Earlier this year McAfee and Facebook entered into a partnership in which the two companies have jointly created security solutions including McAfee security software, a customer scanning and repair tool as well as educational material that Facebook will make available to its 400 million users. McAfee is offering its software on a complimentary 6-month subscription basis. Twitter has also added new security features it says can detect, intercept and prevent the spread of bad links.

### **Foosball**

With the "foosball" approach, social media users within an organization are permitted to use certain servers for social media exchanges but other servers remain off limits. The U.S. Army employs a variation of the approach, allowing users to access social media sites only through a non-classified Internet network.

## **加强社交媒体安全的四个技巧**

文章来源: CIO Zone 作者 Laton McCartney

Facebook 在全球拥有超过四亿的用户，在美国，每天有超过 500 万的 Twitter 消息被发送。任何一个 CIO 或者 CSO, 认为自己可以监控这一发送量并完全降低风险—或者至少是流过他们机构的那部分，充其量是位荒唐的乐天派！尽管如此，你还是可以使用一些工具或者技巧来降低危险程度。这里有四个小窍门。

### 政策是不够的

一些公司如 IBM 公司就在其网站上公布关于“社交媒体的使用”的周密的公司政策文件作为降低风险的第一步。然而，社交媒体战略家们建议培训课程、研讨会等诸如此类的由 Facebook、Twitter 以及其他引起的风险因素的讨论。那也需要被跟进，需要一种手段提醒员工所遇到的任何问题。像 Modern Media Leadership Institute 这样的公司，为专业人员和高管增加涉及到的像关于社交媒体的法律问题的研讨会。学院也出版“社交媒体管理实时通讯”来更新社交媒体的用户新出现的问题和进展。

### 强制工具

大量的供应商公布技术来强制社交网络安全政策。这些政策包括交换过滤解决方案、访问监控、数据泄漏防护工具。例如，Sophos 公司为组织机构提供加密技术、访问监控和数据系统保护，争取缩减从社交媒体上恶意软件、网络欺诈和垃圾邮件的入侵。

数据防护系统供应商 Fidelis Security Systems 安全系统已推出一种工具，他要求提供第一个控件来了解发往社交网络应用程序的信息的内容与环境。公司表示：这样，就能够使以商业目的使用社交网络的用户防止泄露数据资产、知识产权和身份。

供应商增加力量

与此同时，一些社交网络网站也在加强自身的安全性，或试着去这么做。今年早些时候，McAfee 和 Facebook 达成合作，两家公司共同建立的安全解决方案，包括迈克菲安全软件。Facebook 会让他的 4 亿用户能够使用客户扫描和修复工具以及培训资料，McAfee 正提供 6 个月的免费订阅，Twitter 也增添了新的安全特性，它能探测拦截并组织恶意链接的传播。

### 桌上足球

通过“桌上足球”的途径，社交媒体用户内的一个组织允许特定服务器为社交媒体交换，但其他服务器仍然禁止入内。美国陆军采用这种变化的途径，只允许用户进入未分类的社交媒体页面。



SMP-U



# 国迈移动存储设备管理系统

## 三证齐全的移动存储设备管理系统

### U盘系统核心功能：

- 杜绝U盘泄密事件
- U盘使用权限控制
- 防止U盘交叉使用
- U盘病毒主动防御
- U盘使用日志审计
- 适用于单机/网络

### ● 功能描述：

全国唯一三证齐全的U盘管理系统，通过国家保密局、解放军保密委、公安部三重权威认证。全网Internet告警中心+专用安全U盘+U盘管理系统“三合一”，对U盘、移动硬盘、手机存储、数码相机、MP3、MP4、各种CF/MD/SD卡/各类FlashDisk等移动存储介质进行分级注册，灵活控制U盘使用权限，防止信息泄密，记录使用日志，主动防御U盘病毒。杜绝因移动存储介质丢失、被盗用等造成的泄密事件。

### ■ Internet告警中心：

如涉密U盘违规外联到Internet，告警中心自动发出告警信息，并可查询到谁的U盘什么时间在哪台计算机（包括CPU、IP地址、MAC地址等）违规外联。

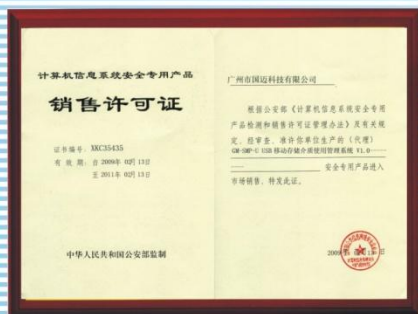
### ■ 六类专用安全U盘：

安全U盘、增强型安全U盘、单向导入U盘、单向导出U盘、双向交换U盘、外部受限使用U盘

### 权威认证：



**国家保密局认证证书**  
ISSTEC2008YT0618



**公安部认证证书**  
XKC35435



**解放军保密委认证证书**  
军密认字第0587号

**成功案例：**北京奥组委、解放军保密委、中国移动、中国边检、中国边防、某军工集团信息中心、总装某局、某卫星发射基地、中国兵器某研究所、中船舶某所、中国航天某设计院、核工业某研究院、山东公安、广东公安、河北检察院、广东省文化厅、洛阳有色金属设计院、机械工业四院、商丘电力、广东省第二人民医院、珠江医院、普利斯通、深圳电器、长丰集团、泰豪集团、汕头海关、北京大唐微电子、上海百联集团、深圳广前电力、河北建筑设计院、达尔嘉（亚洲）等。

**防信息泄密，找国迈科技，要找就找最专业的！**  
**更多信息，请登陆**[www.goldmsg.com](http://www.goldmsg.com)