保密工作中移动存储介质的管理研究

杨永辉[1]，樊金生[1]，郝喆[2]
([1]石家庄铁道学院计算机与信息工程分院，河北 石家庄，050043
[2]石家庄铁道学院后勤集团，河北 石家庄，050043)

【摘 要】随着移动存储介质的广泛使用，移动存储介质管理引发的信息泄露的安全问题越来越受到保密工作人员的关注，成为当前保密管理中的重点和难点。文章首先介绍了国内外对涉密信息安全的管理现状，接着详细分析了当前移动存储介质管理存在的问题和隐患，最后给出了解决方法和策略。

【关键词】移动存储介质；保密工作；涉密信息
【中图分类号】TP 393.08 【文献标识码】A 【文章编号】1009-8054(2008) 09-0061-03

Management of Mobile Mass Storage Devices in Secret-keeping Work

YANG Yong-hui[1], FAN Jin-sheng[1], HAO Zhe[2]
([1]College of Computer and Information Engineering, Shijiazhuang Railway Institute, Shijiazhuang Hebei 050043, China;
[2]College of Computer and Information Engineering, Shijiazhuang Railway Institute, Shijiazhuang Hebei 050043, China)

【Abstract】Mobile mass storage devices have been widely, and the infosec problem caused in the management of mobile storage devices has attracted much attention from the management personel, and thus become the focal point in and the challenge to the present secret-keeping management. This paper first gives the situation of confidential information management both home and abroad, then analyzes in detail the problems and hidden dangers in the management of mobile storage devices, and finally provides the solutions and policies for these problems and dangers.

【Keywords】mobile mass storage device; secret- keeping work; confidential informationa

0 引言

近年来，随着信息技术的飞速发展和高新技术设备的应用，移动存储介质，如U 盘、移动硬盘的出现和普及，极大方便了数据交换和存储便利性。但是，移动存储介质在给人们带来方便的同时，也给保密工作引入了极大的安全隐患，移动存储介质的安全保密问题突现出来，成为当前保密管理中的重点和难点。因此，加强移动存储介质的风险分析和管理已成为有效保障涉密信息系统安全的重要基础。

收稿日期：2007-08-15
作者简介：杨永辉，1981年生，硕士研究生，研究方向：信息与网络安全、电子商务；樊金生，1954年生，教授，硕士生导师，研究方向：信息管理系统、网络安全；郝喆，1957年生，助理工程师，研究方向：通信安全。

1 国内外涉密信息安全的管理和技术现状

11当前国内外对信息安全和保密管理法律法规制定的重视程度

从国外的情况看，据对40多个国家的调查统计，已制定信息安全专门法律的国家占40%，修订原有法律的占60%。众所周知，美国的信息化程度全球最高，在信息技术的主导权和网络话语权等方面占据先天优势，他们在信息安全技术、保密管理以及政策支持方面也走在全球的前列。美国商务部下属国家标准和技术研究所也制定了新的计算机安全准则《对联邦信息设备的推荐安全控制》，它几经修订，今年出台的是第4个修订版本，有1200多条，对计算机等信息设备的管理、操作和技术检查进行了规定，意在保障美国非国防用途信息设备的安全、完整和有效。这套准则涵盖了涉及信息安全的17个领域，重点放在风险评估、对突发和意外事故的管理、对计算机等信息设备的访问控制、对使用

者的鉴别认证等[1]。

中国历来都非常重视对于涉密移动存储介质等高新技术设备的保密管理和使用安全问题,随着电子政务系统的推广,从中央到地方各级部门都制定了一系列重要的保密管理法律法规和技术标准。从1998年起到2006年,先后下发了多个关于计算机信息系统和秘密载体的保密管理规定,国家保密局制定了《涉及国家秘密的信息系统终端安全与文件保护产品技术要求》等相关保密技术标准,各省和相关单位也都制定了本部门内的移动存储介质保密管理规定或相关办法。

12计算机安全保密是国内外相关机构和企业的研究热点,相关技术得到了迅速发展和广泛应用

针对移动存储介质容易丢失、数据信息容易被非授权获取等特点,国内外相关设备厂商采用安全芯片、防盗报警、指纹识别、智能卡识别、数据加密等安全技术,相继推出了各类加密移动存储介质。此外,国内的安全厂商也开发出一些移动存储介质鉴别的安全产品,如基于UKey的终端安全与文件保护系统、移动存储介质安全管理系统等[2]。

2 移动存储介质管理当前存在的问题和隐患

移动存储介质因其通用性强、存储量大、体积小、易携带等特点而得到广泛使用,越来越多的秘密数据和档案资料被存储在移动存储介质里或通过移动存储介质传递资料,大量的秘密文件和资料变为磁性介质和光学介质,存储在无保护的介质里,泄密隐患相当大。目前,移动存储介质管理还存在不少薄弱环节和问题。

2.1对涉密移动存储介质的管理不规范,存在违规使用现象

保密法规定各单位对于保存秘密信息的移动存储介质应该进行申报登记,并按其所涉及的秘密等级粘贴单位保密部门统一制作的密级标识。而有些单位没有针对移动存储介质制定专门的管理制度,或制定的规章不具体、可操作性差,以至于使日常管理无章可循或管理松懈。此外,秘密信息和非秘密信息放在同一介质上,明密不分,磁盘不标密级,不按有关规定管理秘密信息的介质,容易造成泄密。由于疏忽,一些涉密人员存在使用非涉密介质接入涉密计算机或涉密介质接入非涉密计算机的问题。

22对涉密移动存储介质未采取加密和控制技术

有些单位的涉密存储介质的数据直接采用明文保存,如果设备丢失或被不法分子控制,非法持有者可轻而易举获取涉密文件,给国家利益和安全造成重大损失。

23涉密移动存储介质维修和报废环节管理放松

计算机出故障时,存有秘密信息的移动存储介质不经处理或无人监督就带出修理,或修理时没有懂技术的人员在场监督,容易造成泄密。有些单位在设备出现故障后,抱着有病乱投医的心态,在没有资质的维修点维修,这样不但存在数据被二次破坏、无法恢复的风险,而且还会有涉密数据被窃的危险。

此外,有些人认为,把磁盘上的文件或涉密信息删除就安全了,所以许多单位没有把报废的移动存储介质纳入保密管理之中。处理废旧移动存储介质时,由于磁盘经消磁十余次后,仍有办法恢复原来记录的信息,存有秘密信息的磁盘很可能被利用磁盘剩磁提取原记录的信息。这很容易发生在对磁盘的报废时,或存储过秘密信息的磁盘,用户认为已经清除了信息,而给其他人使用。这样增加了保密数据被窃的可能性,造成不可估量的损失。

3 解决移动存储介质管理问题的对策

由于使用移动存储介质而引起的安全问题给保密工作带来了很大困扰,这些问题随着信息化建设的深入也会越发突出和严重。文中就如何建立有效的管理机制和手段来解决存在的问题,提出以下对策。

31加强日常监督和管理,制定和健全相关法规

根据国家有关保密规定,涉密移动存储介质应由单位统一发放,并建立严格的登记、使用、销毁等技术措施和管理制度;与非密载体严格区分,不能既处理涉密信息,又上互联网;要严格控制携带移动存储介质外出,带出工作区要经过单位批准;移动存储介质要定期回收,在挪用、捐赠或不再使用时要统一对介质内的数据进行彻底销毁;同时,应对移动介质的日常使用进行监督检查,以利于各项规章制度的严格执行。

各单位应把移动存储介质管理作为内控建设的重要方面,根据国家有关法律法规,制定适合本单位的移动存储介质管理规定。同时严格执行相关规定,把移动存储介质管理工作纳入到单位、部门和个人年度目标考核,对造成泄密事故的个人和部门追究责任。此外,对涉密移动存储设备从购买到报废进行全程监管,严格把守采购关、检查关、使用关、维护关和报废关等各个环节,从制度上防止泄密事件的可能发生。

32加强针对移动存储介质安全技术的研究,开发适合于用户使用的软件和硬件设备

为满足国家规定的各种保密要求,各单位仅靠传统的保密措施,显得捉襟见肘,迫切需要选用一个功能强大、运行稳定的安全软件系统和相关硬件设备。技术手段在现代化的保密工作中扮演着越来越重要的角色。

移动存储介质的安全管理也是近期研究的一个热点,众多企业纷纷投入精力进行研究和开发。通过认证和加密技术来防范移动存储介质可能引起的敏感信息泄露,可以提高存

储介质应用的安全性。一些产品已经问世，比如防水墙系统综合利用密码、身份认证、访问控制和审计跟踪等技术手段，对涉密信息、重要业务数据和技术专利等敏感信息的存储、传播和处理过程实施安全保护，最大限度地防止敏感信息的泄漏、被破坏和违规外传，并完整记录涉及敏感信息的操作日志以便事后审计和追究泄密责任。

3.3加强保密知识教育和技术培训，增强日常防范意识和技能

除了管理和技术防范措施外，还应该加强对涉密计算机操作人员进行现有法律法规的宣传和保密知识的教育工作，定期开展保密技术防范技能及保密法律法规的培训，增强日常防范措施，使相关的操作和使用人员了解移动存储介质保密管理的相关知识，加强对移动存储介质使用的敏感性，消除可能的泄密隐患。

涉密计算机操作人员还应该加强防病毒的意识。目前互联网上的病毒很多，对于需要从网上下载资料的人员，应注意涉密移动存储介质不能直接与上国际互联网或其他公共信息网的计算机相连接；用于下载国际互联网、公共信息网信息的移动存储介质不得与涉密计算机和涉密计算机信息系统相连接。如需从网上下载资料，应该用非涉密移动存储介质从上网计算机上下载资料后，通过中间机中间机指的是既不用于上网又不是涉密的计算机进行杀毒处理后，对资料进行存储并导入涉密计算机。

3.4对移动存储设备进行密级标识，对使用的过程实施安全保护和审计记录

信息是分密级的，在一个合格的安全体系中，不同密级的信息必须保存在不同的位置或不同的存储介质上，这样可以最大限度保障信息的安全。为此，需要将网络体系中所有可移动介质按其所涉及的秘密等级粘贴单位统一制作的密级标识，用以存放相应密级的数据，只有具备相关权限的人员才能对涉密信息进行访问。

在移动存储设备的使用过程中，应提供详细的审计记录，包括注册信息、使用信息和文件操作信息，记录要素包括使用人、使用计算机、使用时间和动作等，并提供丰富的审计报告。这样可以对移动存储设备的整个使用过程进行记录，以利于监督和审计。

参考文献

[1] 新华网 政府网站频遭攻击，美出台新计算机安全准则[EB/OL]. http://news.sx.xinhuanet.com/world/2005-03/01/content_2633957.htm.
[2] 动网先锋 .浅析涉密笔记本电脑和移动存储介质的风险分析及管理对策[EB/OL]. http://www.pybm.cn/news/printpage.asp?id=416.

国家保密局涉密信息系统安全保密测评中心
对郑州宇光创新技术有限公司伪造产品检测证书进行处理的公告

2008年7月，郑州宇光创新技术有限公司在向科技部科技型中小企业技术创新基金管理中心申报2008年度科技型中小企业技术创新基金的资料中，谎称其申报的“宇光IE微壳V1.0”产品已通过我中心检测，提供了伪造的《涉密信息系统产品检测证书》并加盖该公司公章。经核查，该产品并未经过我中心检测，其证书是伪造的。

郑州宇光创新技术有限公司伪造产品检测证书的行为属于严重违规行为，为加强涉密信息系统安全保密产品管理，根据国家保密局有关规定，我中心现将处理决定公告如下：

1. 两年内不受理郑州宇光创新技术有限公司的产品检测申请。

2. 将有关情况通报河南省科学技术厅和科技部科技型中小企业创业技术创新基金管理中心。

国家保密局涉密信息系统安全保密测评中心

2008年8月18日