# 企业内网移动存储设备安全保密管理研究

熊 君 / 中船黄埔文冲船舶有限公司

【摘 要】移动存储设备具有使用便捷、携带方便等优点，随着在日常工作中的大量使用，给企业网络环境带来了较多安全隐患。如何防止企业人员将未授权信息拷出，如何减少移动存储设备将病毒、木马带入企业网络，已成为迫切需要解决的问题。本文通过探讨对移动存储设备的安全保密管理，提供了相应的解决方案。

【关键词】网络安全 移动存储设备 管理

## 1 引言

常见的移动存储设备主要有移动硬盘、U盘等。移动存储设备使用方便、携带方便，在日常工作中常用于数据交换。虽然相关企业规定只能在内网使用统一配发的移动存储设备，但未采取有效的技术手段进行控制，产生了不少安全隐患。急需在企业内网中加强管理手段及技术手段，控制移动存储介质的无序使用，保障企业的数据安全。

## 2 移动存储设备存在的安全隐患

经过前期调研，发现企业内网中使用移动存储设备时主要存在以下问题：

（1）大量私人移动硬盘、U盘、手机、MP3等随意接入企业内网计算机。

（2）大量病毒、木马等通过移动存储设备进入企业内网。

（3）无有效手段防止用户将未授权信息拷贝至移动存储介质中带走。

## 3 企业内网移动存储设备的管理改善措施

针对企业内网中使用移动存储设备时存在的主要问题，应从管理和技术两方面采取措施：

### 3.1管理方面

（1）标识管理

所有移动存储设备均进行编号管理，录入企业信息化设备台账，台账中记录设备编号、序列号、

责任人、使用范围等，并张贴标识，如图1。

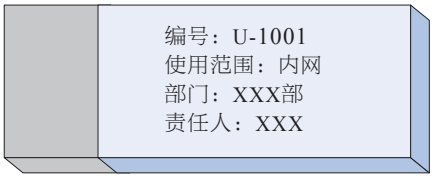


图1　标识样例

（2）移动存储设备使用范围管理

将移动存储设备分为内网专用和外部专用。企业内网计算机上只允许插接内网专用移动存储设备，禁止插接外部专用及私人移动存储设备，外部专用移动存储设备用于与外单位的信息交换。

（3）计算机使用范围管理

将计算机分为企业内网计算机和数据转换计算机。每个部门配发1~2台数据转换计算机，数据转换计算机与企业内网计算机物理隔离，可同时插接内网专用移动存储设备及外部专用移动存储设备，用于内网专用移动存储设备与外部专用移动存储设备之间的数据转换。同时，在数据转换计算机上开启防病毒系统的U盘保护功能，接入U盘时自动进行扫描，防止病毒、木马进入企业内网。

## 3.2技术方面

只采用管理手段无法有效制止用户在计算机上随意插接移动存储设备，因此，需在企业内网中部署移动存储设备管理系统从技术方面进行控制。

（1）注册移动存储设备

在企业内网部署移动存储设备管理系统后，将内网专用移动存储设备在系统中进行注册。注册后的移动存储设备中写入了标记信息及访问控制信息。标记信息用于表明该移动存储设备的所有者、所属部门等，访问控制信息用于当该移动存储设备插入计算机时，依靠访问控制信息决定是否允许在计算机上使用。已注册的内网专用移动存储设备进行了加密处理，在外部计算机上无法读取数据。

（2）配置客户端策略

所有企业内网计算机安装移动存储设备管理系统网络版客户端，数据转换机安装单机版客户端。由移动存储设备管理系统下发策略，已安装网络版客户端的计算机只可读取已注册的内网专用移动存储设备，禁止使用其他移动存储设备。单机版客户端导入移动存储设备管理策略，可读写已注册的内网专用移动存储设备及未注册的移动存储设备。

（3）数据转换流程

外部数据导入到企业内网流程，如图2。

企业内网数据导入到外部移动存储设备流程，如图3。

（4）日志审计

在移动存储设备管理系统中开启日志审计功能，对插接的移动存储设备情况、导入导出的数据进行审计，可审计用户是否违规接入了未注册设备，是否导出了未授权信息。

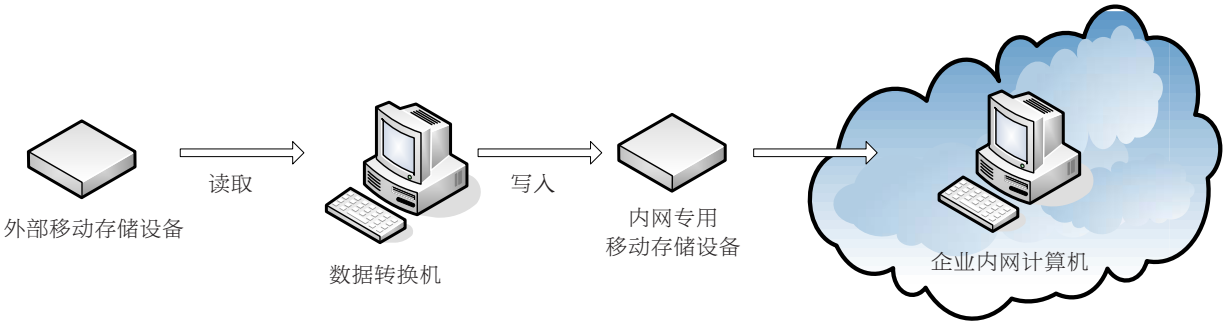


图2　外部数据导入流程图

企业内网计算机插入未注册移动存储设备记录如图4。用户导入导出数据记录如图5。

## 4 效果对比

通过管理方面和技术方面的改进，企业内网移动存储设备使用过程中的问题得到了较好改善，改进前后的对比见表1。

## 5 结语

本文通过对前期调研发现的企业内网中移动存储设备使用时存在的安全问题进行分析，提供了管理改善措施，可供对互联网使用需求较低的企业内网移动存储设备管理改善提供参考。但企业内网安全涉及的内容广而深，不仅仅是移动存储设备管理方面的问题，其他网络安全问题也会给企业带来安全保密方面的隐患。企业应根据信息安全等级保护要求，及时调整管理方法，以保障企业网络的安全。END

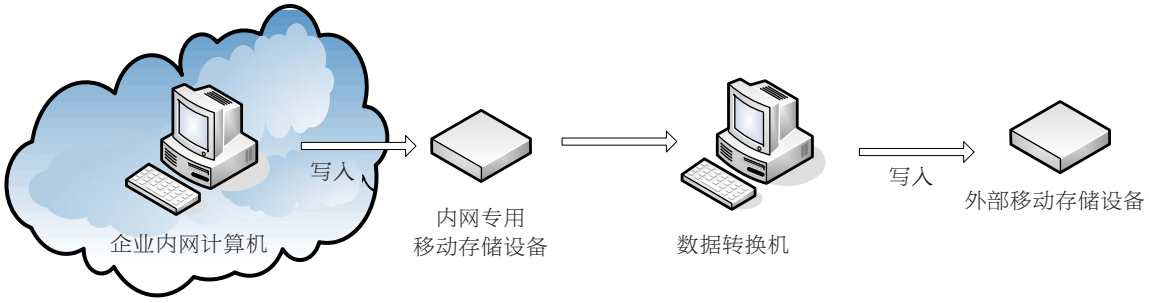


图3 内部数据导出流程图

| 事件主题 | 人员名称 | IP地址 | 主机名称 | 事件报告时间 | 设备描述 | 容量 |
|---|---|---|---|---|---|---|
| 插入【未注册介质】 | 苏 | 192.9.101 | pcw 99 | 2014-05-12 16:59:24 | SMI USB DISK USB Device | 7593M |

图4 审计记录

| 事件主题 | 人员名称 | IP地址 | 操作时间 | 源文件 | 目标文件 |
|---|---|---|---|---|---|
| 文件操作审计 | 张 | 192.9.103 | 2014-05-12 18:53:52 | 加密区1\ 介绍.doc | g:\ 介绍.doc |
| 文件操作审计 | 陈 | 192.9.103 | 2014-05-12 18:48:43 | d:\复件 新建 microsoft office power | 加密区1\复件 新建 microsoft office powe |

图5 导入导出数据记录

表1 改进前后对比表

| 事项 | 改进前 | 改进后 |
|---|---|---|
| 移动设备接入 | 随意插接 | 只能插接内部设备 |
| 病毒木马 | 极易传播 | 可防止大面积传播 |
| 信息输出 | 无法防止未授权信息输出 | 可审计输出信息 |
| 信息泄露 | 数据未加密，可随意读取 | 数据加密，未授权无法读取 |