防泄密
从入门到精通

V1.1

深圳市大成天下信息技术有限公司

UNNOO Information Tech., Inc.

二〇一一年七月

目录

一. 文档修订记录及说明 3
修订记录 3
文档说明 3
公司简介 3
二. 为什么要做防泄密项目 4
2.1 泄密带给企业的影响 4
2.1.1 您不知道的数字 4
2.1.2 泄密实例 5
2.2 需要做防泄密吗？ 5
2.2.1 他们都担心什么？ 5
2.2.2 泄密的常规渠道 6
2.3 防泄密对企业的价值 6
2.3.1 维护企业形象 6
2.3.2 提高企业竞争力 6
2.3.3 打造高效率的数据管理平台 7
三. 防泄密项目的准备工作 7
3.1 确定原始需求 7
3.1.1 什么是“原始需求” 7
3.1.2 一些可能的“原始需求” 7
3.2 制订工作清单与工作目标 9
3.2.1 制订工作清单 9
3.2.2 确定项目目标 9
3.3 产品选型要素 10
3.3.1 了解防泄密产品的技术原理与分类 10
3.3.2 产品选型核心要素 11
四. 怎么做防泄密项目 13
4.1 项目人员的选择 13
4.1.1 项目人员选择的标准 13
4.1.2 项目人员的职责 14
4.2 需求调研 14
4.2.1 需求调研的目的 14
4.2.2 调研注意事项 15
4.3 项目里程碑 15
4.4 防泄密项目的重难点 16

一. 文档修订记录及说明

修订记录

时间	版本	说明	修改人
2011-06-29	V1.0	初稿	大成天下铁卷团队
2011-07-07	V1.1	正式发布	大成天下铁卷团队

文档说明

本文档由深圳市大成天下信息技术有限公司铁卷团队制作。

公司简介

深圳市大成天下信息技术有限公司（简称大成天下）成立于 2005 年 2 月，公司总部设于中国深圳南山科技园，面向全国乃至全球用户提供高效、实用、稳定的桌面与内容安全产品。

公司网址：www.unnoo.com 防泄密博客：http://blog.unnoo.com/ http://www.fangxiemi.org

咨询热线 400-1122-918 客户专线 0755-86158255

渠道专线 0755-86158858 华东专线 021-61094645

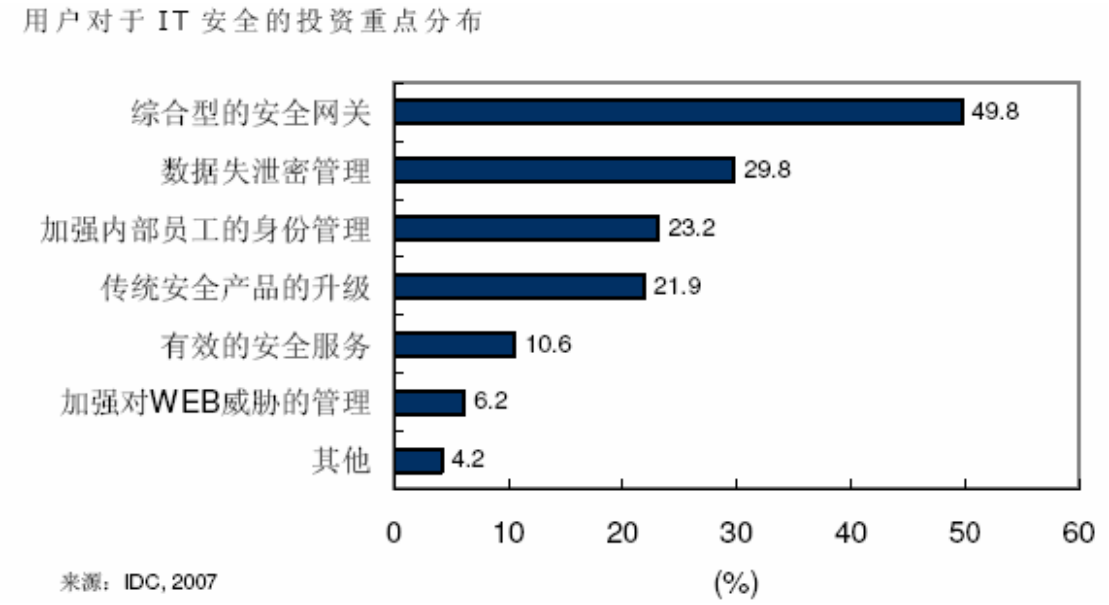
二. 为什么要做防泄密项目

2.1 泄密带给企业的影响

近些年来，企业泄密案件不断增加，各种数据泄漏事件日益增多。

泄密事件的出现，不仅给企业带来了严重的直接经济损失，而且间接地在品牌和公众形象等等诸多方面也造成了不可估量的侵害。

因此，企业领导对 IT 安全的投资已经从传统的防病毒、防火墙等安全产品慢慢转移到数据防泄密管理上。下图是 IDC 对用户投资重点调研比较：



《中国 IT 市场分析与预测 2007-2011》中，IDC 对用户投资重点调研显示：“29.8%的用户会考虑投资数据防泄密管理”。

2.1.1 您不知道的数字

- 每 400 封邮件中就有 1 封包含机密信息 ；
- 每 50 份通过网络传输的文件中就有 1 份包含机密数据；
- 50%的 USB 盘中包含机密信息 ；
- 80%的公司在丢失笔记本电脑后会发生泄密事件；
- 在美国平均每次数据泄密事件导致的财务损失高达 630 万美金(Ponemon Institute, 2007)；
- 数据泄漏导致客户流失的比例正在以每年 11%的速率上升；

- 据 FBI 和 CSI 对 484 家公司进行了网络安全专项调查，调查结果显示：超过 85%的安全威胁来自公司内部。在损失金额上，由于内部人员泄密导致了 6056.5 万美元的损失，是黑客造成损失的 16 倍，是病毒造成损失的 12 倍。

2.1.2 泄密实例

- 2007 年 6 月，国内一大型台资设备制造代工企业状告另一家大型企业，使用“挖墙角”的方式获得其企业机密数据，遂索赔人民币 50 亿元；
- 2008 年 06 月南方都市报报道：国内某市的孕产妇信息库也已发生泄露，累计每年泄露的孕产妇个人信息达 10 万余例；
- 2008 年 4 月 26 日，香港汇丰银行观塘分行在装修期间服务器被人偷走，遗失有近 16 万客户资料；
- 2008 年 6 月 19 日，汇丰遗失一盒载有 2.5 万段电话对话、涉及 1.5 万名客户的录音带事件；
- 2009 年由“力拓案”引发的席卷全国保密审计大检查再次给各单位、企业敲响了警钟，知识产权保护工作已经刻不容缓；
- 2010 年 7 月香港八达通公司承认，曾将 200 多万客户资料转售给其它公司，非法获利 4400 万港元；
- 2011 年索尼两次泄密事件使得索尼数据遭窃案受影响的用户可能超过 1 亿人，成为迄今规模最大的用户数据外泄案。

2.2 需要做防泄密吗？

2.2.1 他们都担心什么？

高层领导的担心

上级部门对数据保密的要求

数据泄密导致信任危机和法律诉讼

机密数据泄密降低企业竞争力

中层管理的担心

客户对公司的信息保密要求

公众对越来越多的个人隐私被盗用的不满

机密数据泄密使业务拓展受阻，甚至“培养”竞争对手

机密数据泄密会严重影响在客户面前的声誉

IT 部门的担心

数据泄密风险和威胁越来越大

业务部门对数据泄密事件抱怨越来越多

新技术使数据防泄密难度越来越大

2.2.2 泄密的常规渠道

泄密常规渠道分为以下几种情况：

- 内部人员离职拷贝带走资料泄密
- 内部人员无意泄密和恶意泄密
- 外部竞争对手窃密
- 黑客和间谍窃密
- 内部文档权限失控失密
- 存储设备丢失和维修失密
- 厂商合作交流泄密

为了保护重要的电子文档，企业需要一种有效的防泄密解决方案，随时控制潜在的信息泄密风险。

2.3 防泄密对企业的价值

2.3.1 维护企业形象

企业的一些重要文件被提前泄密，损失的并不仅局限于金钱，影响最大的还是企业在公众面前的形象。例如上市企业的收购计划被提前泄密，知情的投行机构会做空股票，利用杠杆效应在某些市场获得巨额利润，牺牲股民利益，从而损害了企业的公信力。

防泄密项目顺利应用能维护企业在公众心目中值得依赖的形象。

2.3.2 提高企业竞争力

具有核心技术的企业，如果核心技术数据被泄密，企业在行业市场上的技术优势势荡然无存，导致业务无法顺利开展，削弱业务获胜机会，最直接的后果就是客户减少，利润严重下降。

防泄密项目能帮助企业管理好核心技术数据安全，提升企业竞争力。

2.3.3 打造高效率的数据管理平台

防泄密项目是一个理顺企业数据管理流程的过程，通过建立合理的数据管理制度，打造一个高效率的数据管理平台。帮助企业基层员工合理利用数据，创造价值；使企业管理层对数据管理了如指掌。

三. 防泄密项目的准备工作

3.1 确定原始需求

3.1.1 什么是“原始需求”

这里的“原始需求”，指的是激发企业/单位采购防泄密产品的原因。通过了解原始需求，可以逐步推导并找到真正适应企业/单位现状，能够满足需求的产品。

要确定原始需求，我们需要分别与管理者（提出防泄密需求的领导）和使用者（需要使用防泄密产品的部门与用户）沟通，找到下面这些问题的答案：

1) 为什么计划上防泄密系统？
2) 企业/单位的机密数据是什么？在谁那里？流转流程怎样？
3) 谁可能窃取这些机密数据？
4) 他们可能通过哪些渠道泄密/窃取？

找出这些问题的答案，并且就这些信息与防泄密厂商沟通，你的防泄密项目就有了一个良好的开端。

3.1.2 一些可能的“原始需求”

1) 为什么计划上防泄密系统？

a) 曾经发生过泄密事件；
b) 企业处于“商业泄密事件”高发行业，资料保密关乎生死；
c) 合规性需求（比如企业要上市，比如军工企业要通过保密局的保密检查，比如央企要满足中央企业商业秘密保护暂行规定等）；

2) 企业/单位的机密数据是什么？

a) 设计图纸（机械制造、广告设计、服装鞋帽等行业）；

b) 办公文档（律师、投资银行、金融证券、政府部门等行业及每家企业的财务、研发）；

c) 源代码（开发类企业，游戏、手机等开发目前尤其重视）；

d) 客户信息，可能包括文档和数据库（金融、运营商甚至大量互联网企业）；

e) 全部数据（有的老板认为，除了我认为可以外发的资料外，全部都是秘密）；

3) 机密数据在谁那里？

a) 管理层（包括市场、销售、研发副总等手里的企业管理数据）；

b) 研发人员（源代码、设计图等）；

c) 财务人员（财务数据、工资表等）；

d) 外协厂商（部份数据、图纸必须发给第三方）；

4) 机密文件流转流程怎样？

5) 谁可能窃取这些机密数据？

a) 3 里提到的所有人员；

b) 网络黑客；

c) 商业间谍；

6) 他们可能通过哪些渠道泄密/窃取？

a) 被动泄密/窃取

i. 硬件遗失（笔记本、硬盘、U 盘等丢失）；

ii. 硬件换代时更换未消密；

iii. 病毒、木马、黑客攻击；

iv. 错误的网络共享（如共享文件夹、BT/电驴共享等）；

b) 主动泄密/窃取

i. QQ、MSN 等即时通讯工具在线传输发走；

ii. 邮件（PDM/PLM/OA 邮件、公司邮箱、WEB 邮箱发走）；

iii. U 盘、移动硬盘拷走；

iv. 将文件资料打印带走；

v. 照像或手抄然后 OCR；

vi. 通过笔记本电脑、手机的无线（蓝牙、红外）传输带走；

vii. 通过 FTP、SCP 等各种网络协议传输后带走；

viii. 拆硬盘带走数据；

ix. QQ 截图、各种截图工具截图后发走；

x. 屏幕录像工具录走；

xi. 将源代码打包到资源文件中编译带走，执行特殊参数后释放；

xii. 通过数据库管理工具导出数据库的 sql 带走；

3.2 制订工作清单与工作目标

3.2.1 制订工作清单

要在企业/单位开展一个防泄密项目，可能需要做好下列工作：

- 明确取得领导/管理者授权；
- 极小范围（与管理者，用户部门主管）沟通他们对防泄密项目的期望；
- 了解项目预算（管理者愿意花多少钱来解决泄密问题）；
- 整理书面的《防泄密项目需求书》；
- 找到 2-4 家防泄密产品提供商，进行产品选型工作，包括：
  - 分别讨论，最终确定项目目标；
  - 了解各家产品信息，并多方了解包括口碑、成功案例、售后服务等信息；
  - 软件测试；
- 进入商务流程（可能是招标，可能是议价，视企业情况，项目金额大小而定）；

基本上这是采购前需要完成的工作内容，看似简单，实际上也需要付出大量精力——前期工作准备得越充分，防泄密项目成功的机率就越大。

3.2.2 确定项目目标

有一个经验是：“不要指望一个产品能解决所有问题。”放到防泄密产品选型上，这个道理同样适用。

有些问题适合用防泄密软件解决，有些问题适合通过防火墙、打印控制、应用虚拟化等产品解决，还有些问题可能需要还有些问题可能需要通过管理手段配合。这时候建议你填写下面的表单：

泄密渠道	危害	发生机率	防范措施	实施前风险情况	实施后残留风险

QQ、MSN 传输	高	极高	1、铁卷加密 2、锐眼监控	1、从公司内网流量监控观察，大量数据通过 QQ 外发（每天 6-10G 数据流量）； 2、所有人都能上 QQ，无法截获内容；	1、主要泄密风险消除； 2、数据被外发有日志；
U 盘拷贝	高	极高	1、铁卷加密 2、锐眼监控	不知道有哪些数据被拷走	1、主要泄密风险消除； 2、数据被外发有日志；
拆硬盘	高	中	1、铁卷加密 2、摄像头监控	高，完全缺乏监控与了解	基本消除风险，残留问题是摄像头监控数据过多，可能无法即时发现

这份表单可以与防泄密厂商的人员一起“填空”，通过这样的表格，可以对目前存在的风险、上安全措施后解决的问题、残留的问题都罗列出来，一目了然。

3.3 产品选型要素

3.3.1 了解防泄密产品的技术原理与分类

防泄密产品目前的分类大概包括以下几种：

实现方式		技术原理	代表产品
设备管控		通过禁用设备或网络协议来防止数据外泄	中软防水墙
加密	文件手动加密	用户自行给文件加上密码，防被动泄密	WinRAR
	文件透明加密	文件的加解密过程全自动，防主动泄密	大成天下铁卷
	磁盘加密	对整个磁盘加密或创建单个加密盘，防被动泄密	TrueCrypt、PGPDisk
数字权限管理（DRM）		给文档、人员赋予不同的权限，管理精细但复杂	微软 RMS
数据鉴别、审计与阻断		鉴别核心数据，审计对核心数据的使用情况，并阻断泄密行为	赛门铁克 DLP、大成天下锐眼
桌面虚拟化		应用与数据集中存储在服务器	Citrix，大成天下远驭
格式转换			Adobe PDF，大成天下密信

对不同各类的防泄密产品，大成天下做了简单的对比如下：

实现方式		优点	缺点
设备管控		效果直接，实施简单	1、做到 90%容易，做到 99%较难 2、浪费了部份 IT 投资 3、容易引起员工反弹
加密	文件手动加密	简单易行	无法防主动泄密
	文件透明加密	效果直接，防护全面	1、稳定性（自身稳定、与杀毒兼容） 2、与应用软件关联紧密，需要升级 3、难以保护源代码
	磁盘加密	简单易行	1、无法防主动泄密 2、稳定性
数字权限管理（DRM）		与流程、业务整合，符合管理者思维	1、不符合使用习惯（手动设置权限） 2、业务流程真的准备好了吗？ 3、业务系统真的适合吗？ 4、大量文档，大量权限，海量“交集”
数据鉴别、审计与阻断		分析与审计为主，业务干扰小	1、阻断不力（涉及网络环境改造） 2、无法处理加密数据（加密文档、加密流量）
桌面虚拟化		集中管理，业务复杂度降低	1、改变使用习惯与流程 2、可能存在性能瓶颈

3.3.2 产品选型核心要素

如果你不太了解技术，那么建议可以重点关心以下几个项目：

- 行业成功案例；
- 产品口碑；
- 公司研发能力；

如果你希望对各种产品了解得更深入细致些，那么可以根据以下表格，对比不同厂商，看他们各自的情况如何。

提醒一句：防泄密产品选型，除了看文档，听 PPT 之外，一定要认真测试产品。前期投入细致些，产品部署的时候才能心里有数。

3.3.2.1 管理者关注点

分类	关注点	为什么要关注	检查方法
公司情况	行业成功案例	尽量少在行业中第一个当“小白鼠”	厂商主页的成功案例并电话咨询（一定要致电用户咨询，很多案例未必真实）
	产品口碑	已经使用过的用户如何评价	1、在互联网上搜索相关信息； 2、电话或邮件咨询采购过的企业； 3、要求厂商安排参观（但不光看厂商给你看的东西）；

	研发能力	技术人员的研究与开发能力	1、有多少研发人员； 2、做过什么产品，有哪些资历； 3、有什么样的行业背景；
	服务口碑	已经使用过的用户如何评价	1、看厂商的服务承诺； 2、看厂商服务人员的能力与基本素质； 3、关注厂商在当地是否有服务机构；

3.3.2.2 技术选型者关注点

分类	关注点	为什么要关注		检查方法
客户端	运行效率	企业的机器性能不一，必须能够保障在较老旧的机器上也能顺利运行		1、找高、中、低端三种性能的典型机器； 2、找 500K/5M/50M/500M 4 种典型文档/图档； 3、测试打开效率，绘制性能曲线图表。
	稳定性	客户端软件部署，很容易受到用户的抵制，如果经常与其它软件冲突，会广受批评		要求在加密情况下试用一周甚至更长时间
	安全性	不能因为引入安全软件带来更大的安全隐患		1、使用互联网上的公开破解工具进行测试； 2、请厂商说明为什么他们的安全方面有优势； 3、请厂商讲解被破解后 可能采取的补救流程；
	兼容性	操作系统兼容性	系统环境可能复杂多样	2000、xp、win7、vista 均做测试
		64 位系统兼容性	新电脑基本都是 64 位	在 64 位操作系统上安装并测试基本功能
		杀毒软件兼容性	兼容性不好很容易被误杀	装 360 或同类软件，看是否有提示或报警
		应用程序兼容性	不能引起应用崩溃等错误	要求在加密情况下试用一周甚至更长时间
	基本功能	文件加密功能	防泄密系统的基本功能	要求在加密情况下试用一周甚至更长时间
		复制粘贴保护	防泄密系统的基本防护功能，必须稳定且不易被绕过	
		截屏/录像保护		
		打印保护		
		进程保护		
	故障冗余能力	UPS 时间	服务器当机、网络中断也不能影响业务	实际测试，拨客户端、服务器网线确认
		多管理中心热备	可以快速恢复	实际测试，多机热备时拨掉一台，看能否自动切换
	便利性	离线用户认证方式	最好能有常规离线申请、硬件 KEY、文件 KEY 等灵活授权	通过实际功能测试与使用，感受这些功能的特点，并判断是否最终满足企业需求
		文件解密流程	用户可以方便地解密，可能包括需要管理员审批、自行解密、自动审批解密等方式，但均能备份供审计	
		切换个人模式	在个人模式下可以做“非涉密”工作，非涉密文档不受影响	

		少量复制文字	经常会用到少量复制文字到其它文档	
服务端	可管理性	域帐号整合	对大中型企业管理便利	
		远程下发策略、升级、安装程序	方便管理员远程处理事务	
	性能	单台服务器可支撑用户数	视企业需求而定，一般在3000以上	如有环境，可请厂商提供测试方式进行实测
	稳定性	无故障运行时间	系统是否有内存泄密等问题，导致机器经常资源消耗很大	1、咨询厂商的技术人员； 2、通过压力测试拷机；
		多数据库实时同步/备份	系统热备时需要使用	实际测试，写一台数据库，看另一台的状态
	日志审计能力	通常管理者不管运维，只看报告。最好要能够记录用户操作文件的记录，包括打开、编辑、重命名、删除等各种文件操作		实际察看日志，并看日志是否易于查询、归并。咨询用户的技术人员是否有日志分析经验
其它	易用性	IT部门最后不会被某款产品“绑架”，总在解决用户对这款产品的疑问		1、请厂商培训IT人员，观察IT人员掌握程度； 2、调研、记录并分析非IT人员在未经培训的情况下，初次使用软件前半个小时的操作行为。
	产品“下线”	最终如果不使用某特定厂商的产品时，用户可以比较方便地将文档批量解密		请厂商展示“解密工具”并帮相应承诺

四. 怎么做防泄密项目

4.1 项目人员的选择

4.1.1 项目人员选择的标准

防泄密项目组项目人员的选择除了双方的项目经理重要，其它项目组成员也是项目成功的关键。防泄密项目最终的用户说到底还是业务部门，所以必须要业务部门人员参与进来才行。根据我们多年来实施防泄密项目的经验总结，项目人员选择的标准主要有以下几点：

a) 每个部门都必须要有代表参加项目组，最好部门负责人也是项目组成员；

b) 必须熟悉本部门的工作流程和性质；

c) 必须熟悉本部门内的绝大多数人员，并且经常和部门负责人打交道；

d) 要热心，能对项目方案提出意见和建议；这一点很重要，热心的项目人员可以

将即将碰到的问题提前提出来讨论，避免项目被动局面；

4.1.2 项目人员的职责

项目组的任务是将项目做好并成功验收，这个过程中大致有项目实施调研、需求评审、方案评审、项目实施、试运行和验收，每个环节的职责不同，大致内容见下表：

项目阶段	项目人员职责
实施调研	1、根据本部门的工作流程和性质选择合适的调研对象； 2、负责联络调研对象，安排调研时间；
需求评审	1、参加需求评审，关注对本部门相关内容； 2、对需求不完善的内容进行补充，对需求不正确的内容提出正确的意见；
方案评审	1、参加方案评审，关注对本部门工作的影响； 2、对方案不合理的地方要提出质疑，直到修改合理为止； 3、向本部门管理人员通报项目方案； 4、协助制订防泄密管理制度；
项目实施	1、参加项目培训，熟悉防泄密产品使用； 2、对本部门进行防泄密产品使用培训； 3、在项目实施过程中，对本部门人员提出的疑问能够解答或者传递到项目组中； 4、协调项目组与本部门人员之间的关系；
试运行	1、及时向项目组通报试运行阶段的员工使用产品情况； 2、对工作有影响或有漏洞的地方及时与项目组讨论方案修正的方法；
验收	1、根据需求文档和方案文档来评审项目是否达到预期效果；

4.2 需求调研

4.2.1 需求调研的目的

项目阶段的需求调研主要目的有如下几点：

- **项目方案的基础：**如售前阶段的需求调研相比，此时调研出来的需求更加细化，各部门有那些重要文档，那些人需要将重要文档外发，那些人有些特殊需求等等；只有把这些细微的需求都调研出来，才能设计出大多数人都满意的方案，否则后面实施阶段就会困难重重。

- **让部门管理者认识到项目的重要性：**通过调研这个过程告诉各部门，我们开始做防泄密项目了，并且告诉他防泄密会对部门产生什么影响，带来什么好处，让管理者认识到这个项目的重要性，实施阶段出了什么问题也好请管理者出来协调资源；
- **项目验收的依据：**只有把各部门的实际需求全部调研出来，才能将项目验收的标准全部细化，从而提炼出验收指标；

4.2.2 调研注意事项

- 确定调研的主题，列出所要涉及的调研要点，可以使用 MMap 作一个调研计划安排；
- 先对各部门领导进行调研，讲清这次调研的目的、方法以及你想调研的对象。只有得到领导的支持你才会将工作进行下去。
- 选择调研对象很重要，你必须选好三种调研对象：掌握信息的人、有决定权的人、有影响力的人。
- 针对不同的对象准备好不同的问题，提出的问题要针对被调研人的职位，所处的环节，能得到的信息等。
- 与被访人进行预约，告知调研的目的、提出的问题、持续时间、地点和你的联系方法，最好给被访人一天的准备时间。

在这个阶段会出《需求说明书》，详细描述此项目的需求，通过需求评审后，再由乙方项目经理设计项目方案，再由项目组来评审方案。

4.3 项目里程碑

防泄密项目分为以下几个里程碑：

里程碑一 项目启动阶段

此阶段完成项目组建立、工作内容的确定等准备工作，以项目启动会议作为此阶段结束点。

里程碑二 需求分析阶段

此阶段对客户方进行需求调研，将客户业务需求提取、分析，通过充分调研反馈，双方评审之后形成需求规格说明书，并以此作为项目验收标准。提交主要成果为：

1. 《调研访谈记录汇总表》
2. 《项目需求分析书》

里程碑三 设计阶段

此阶段对将根据《项目需求分析书》来设计实施计划、实施方案及详细的安全保护策略和相应的数据防泄密管理制度，提交主要成果为：

1. 《安全保护策略列表》（初稿）

2. 《实施方案和计划》

3. 《防泄密管理制度建议（初稿）》

4. 《防泄密整体技术方案规划》

里程碑四 实施阶段

对既定范围的计算机安装实施。提交主要成果为：

1. 《使用者操作手册》

2. 《代理管理员操作手册》

3. 《管理员操作手册》

4. 《人员培训资料》

5. 《管理员培训资料》

里程碑五 试运行阶段

实施阶段完成后，进入项目试运行阶段，开始系统的运行维护。提交主要成果为：

1. 《项目问题跟踪记录汇总表》

2. 修正后的《安全策略保护列表》

3. 《防泄密安全系统运维手册》

4. 修正后的《防泄密管理制度建议》

里程碑六 验收阶段

完成试运行阶段之后，按照《项目需求分析书》及相关需求变更文档根据系统运行情况来组织项目的验收。提交主要成果为：

1. 《项目功能验收清单》

2. 《需求变更统计表》

3. 《项目验收报告》

里程碑七 维护阶段

项目完成验收之后，进入维护期。提交主要成果为：

《系统维护分析报告》

4.4 防泄密项目的重难点

原本计划着把项目实施过程也详细写出来，但后来仔细想想，如果我们把前面三节的功课都做好了，项目实施就没什么好写的了。项目人员的选择把谁来执行给确定了；需求调研把问题找出来了，即做那些；里程碑把计划整出来了，项目实施就按计划执行即可。绝大多数项目实施阶段出的问题都是因为前面的工作没做好。

这一节，我们来说说整个项目中的重难点，首先我来提几个问题，大家可以先想想：

1) 您公司内的最重要的文档由那个部门创建的，会流转到那些部门？
2) 如果每个部门都有重要的文档，您是选择把所有部门都保护起来还是先把整个公司中最重要的文档保护起来？
3) 如果加密的文档要外发，管理员怎样判断该不该解密外发？

上面的三个问题其实是防泄密项目中的三个重难点，这三点就是项目的范围、目标和管理制度。

防泄密项目对文档加密很简单，但加密后对各部门的影响有大有小。比如说，对制造企业的研发而言，重要的文档非常多，外发的东西相对少，而且领导也相当重视，一般企业对研发都上防泄密产品。但行政、人事等部门重要文档占部门文档的比例相对较小，外发的文档又会很多。如果这两类部门全部按同一标准一起上防泄密产品，肯定会出问题。

因此在需求调研阶段就要考虑这方面的问题，在需求说明书中确定项目的目标和范围，是分一二三期上，还是整体上（每个部门不同的标准），都要考虑清楚，方案设计时也要把这些区分开来。

至于管理制度就必须规定防泄密产品怎么用，那些文档在什么情况下可以解密，那些不能解密，都要规定清楚。而且管理制度必须是在项目实施前就要敲定执行，项目实施的过程中可以进行微调，避免出现项目实施完了，管理员还不知道那些该解密，那些不能解密，都不知道按什么标准来执行防泄密制度了。