目录

项目 4　移动存储防泄密 / 99

项目 5　电子文档安全管理 / 131

项目 6　认识数字水印 / 165

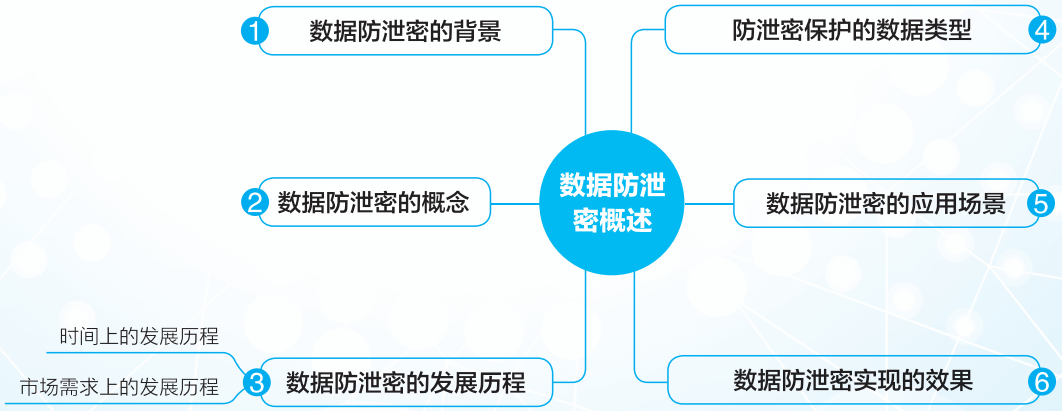
项目 7　数字水印在内控管理中的应用 / 177

项目 1 数据防泄密概述

项目目标

1. 了解数据防泄密发展的背景。
2. 了解数据防泄密保护的类型。
3. 掌握数据防泄密保护的应用场景。

知识导图



笔记

项目导入

随着信息技术的飞速发展，计算机和网络已成为日常办公、通信交流和协作互动的必备工具和途径，信息数据也成了当下最重要的交流载体，这种交流载体包罗万象并高速增长，而数据防泄密自然变就成了人们不可回避的重大问题。

【分析】

学习具体知识前，先要了解数据防泄密是如何发展的，有哪些技术手段和应用场景，即要对数据防泄密有一个基本的认识。

任务 1.1 数据防泄密的背景

随着信息技术的飞速发展，计算机和网络已成为日常办公、通信交流和协作互动的必备工具和途径。但是，信息系统在提高人们工作效率的同时，也对信息的存储、访问控制，以及信息系统中的计算机终端与服务器的访问控制提出了安全需求。目前对内外安全的解决方案，还停留在防火墙、入侵检测、网络防病毒等被动防护手段上。在过去的几年中，全球 90% 以上的计算机用户使用杀毒软件，80% 以上设有防火墙，60% 以上使用反间谍程序软件，但却有 75% 以上的用户至少遭遇过一次病毒、蠕虫或者木马的攻击，70% 以上的用户至少遭遇过一次间谍程序攻击事件。据我国国家信息安全测评中心计算机测评中心数据显示，由于内部重要机密数据通过网络泄露而造成经济损失的单位中，重要资料被黑客窃取和被内部员工泄露的比例为 1 ： 99，即互联网接入单位由于内部重要机密通过网络泄密而造成重大损失的事件中，只有 1% 是由黑客窃取造成的，而 99% 都是由于内部员工有意或者无意泄露而造成的。在这个大前提下，大家开始本书的学习。

任务 1.2 数据防泄密的概念

数据防泄密是指采取文档透明加密、数据安全隔离、内容智能识别、网络拦截等一种或多种技术，防止数据泄密的手段。数据防泄密本质上是对用户需求的一种总体、概括性的描述。与其对应的供给侧的描述，则涉及文档加密软件、DSA 数据安全隔离、DLP 数据泄露防护系统等一系列产品。

任务 1.3 数据防泄密的发展历程

子任务 1.3.1 时间上的发展历程

1. 2001 年起源——终端安全

尼姆达、求职信等标志性病毒使杀毒软件研发进入了黄金时代。孱弱的终端，使得除杀毒软件、防火墙之外的补丁漏洞管理、软件分发等产品也登上了舞台，内网安全的前身就此显现。

2. 2003 年争议——行为监管

安然会计丑闻爆发，随之而来的塞班斯法案对企业信息系统内控提出了要求，对邮件、网络等 IT 系统的审计需求，让邮件、上网监控产品开始井喷，内网安全注重“人”的风险由此开端。

笔记

3. 2005 年插曲——上网行为管理

2005 年 6 月，我国宽带用户首次超过拨号上网用户；12 月，公安部颁布 82 号令，标志着上网行为监管有了正式的规章。同时，钓鱼欺诈、病毒木马也让网管头痛不已，上网行为管理作为内网安全的分支开始蓬勃发展，并形成兼重效率与安全的独立品类延续至今。

4. 2006 年蜕变——防水墙

2006 年年初，公安部颁布《信息安全等级保护管理办法（试行）》，并选择银行等严重依赖信息化的部门进行试点；7 月，塞班斯法案（Sarbanes-Oxley ACT，SOX ACT）大限，众多上市企业面临合规性要求，开始考虑和部署内部信息审计和防护产品，以防备来自网络、终端、外设等多样化的安全威胁，信息防泄漏 1.0 版本——防水墙登上舞台。

5. 2008 年核武器——加密

2008 开始的金融危机，让一大批企业倒了下去。艰难时期，IT 管理者却更加关注安全，只因机密信息关系到核心竞争力。防水墙堵漏不及，新安全威胁不断扩展，痛定思痛，号称能彻底解决安全威胁的加密产品开始全面热卖。

6. 2010 年新生——整体信息防泄密时代

索尼 PSN 泄密、富士康 iPad 图纸泄密等，频繁曝光的泄密事件，让信息防泄密逐渐成为内网安全的焦点。从终端安全到监控，从防水墙到加密，内网安全的焦点逐渐清晰，市场也更加理性。意识到这些问题的厂商和用户，开始在更深层面思考内网安全，准入控制、数据保密、操作授权、行为审计等结合的整体解决方案正当其时。

7. 2011 年延伸——多元化信息防泄密时代

随着各行业信息化建设的拓进，信息化的建设呈现“以终端为基础、应用为核心、移动办公为扩展”的整体发展模式，且“云技术、虚拟化、物联网”等新技术不断融合和加载导致信息安全规划建设日新月异，因此今后的信息安全产业链将呈现多元化特性，根据市场各行业不同的信息化应用模式和发展规划，构建完整且有针对性的信息安全解决方案才能适应客户的需求。

子任务 1.3.2　市场需求上的发展历程

1. 内网安全概念的初现

2000 年左右，中国基础网络建设已经比较完善，个人计算机（Personal Computer，PC）也已经成为一种常见的设备，基于网络的应用大量涌现，很多企事业单位已经进入网络应用的阶段，办公自动化开始普及。

网络和办公自动化的普及，为病毒等安全威胁的快速传播提供了现实基础。当时企业级防护手段还是以防火墙为代表的边界防护，一旦病毒越过防火墙，就会在内网中快速传播，由于大多数用户对计算机的认知程度不高，缺乏防护意识，加之条件有限，难以保证系统补丁、软件升级的及时性，使得企业内网毫无抵抗力。人们发现，依靠单一的防火墙、防病毒软件无法应对病毒威胁，只有将每个客户端都保护起来才能有效防止病毒入侵。随着相关需求的大量产生，市面上出现了包括控制非法接入、控制非法外连、设备加密、补丁分发等功能的内网安全产品，主要解决桌面安全防护问题，内网安全的前身就此显现。在这个阶段，内网安全产品主要还是以系统功能增强为主，管理方面的能力较弱。

笔记

2. 关注“人”的风险

2002 年，美国“安然”“世通”丑闻爆发，2004 年，美国证券市场开始实施针对上市公司财务和公司治理的塞班斯法案。该法案要求上市公司的内控管理必须切实做到保护财务数据、维护系统安全、保护客户数据免遭盗窃与破坏，以提高公司披露的准确性和可靠性。内控从此成为人们关注的焦点，随之而来的针对邮件、网络等 IT 系统的审计要求使得邮件监控、网络监控、行为审计等产品成为热潮。

塞班斯法案从法规遵从的角度对上市企业的内控提出了明确要求，但内控并非只有上市公司才需要。在 2005 年左右，众多企业发现员工会在工作时间内通过互联网访问无关信息，这不仅降低了工作效率，还使得钓鱼欺诈、病毒、木马等安全威胁轻易进入企业内网，内部泄密也变得轻而易举，传统的管理手段根本无法应对。如何对上网行为进行限制和管理成了企业信息安全建设的燃眉之急，于是“上网行为管理”也在这一时期得到了快速发展。

从此时开始，内网安全不单单关注技术风险，也开始关注“人”的风险。行为监控和审计的出现标志着内网安全产品从单纯的“技术”走向了“管理”，但是，这一步走得并不轻松。

以现在的眼光来看，监控和审计是一种内控的必要手段。但是在当时，国人对于“隐私”的理解非常粗浅，而且企业的管理水平普遍较低，员工对于监控和审计有着非常强烈的抵触情绪。监控和审计源于美国，而此时的中国无论是企业发展水平还是员工意识都相对落后，在一些制造企业中还曾经发生过因为实施行为监控而导致大量设计人员离职的情况，许多企业最终不得不停用行为监控系统。

在这种大环境下，监控和审计的功能从台前转到了幕后，业内也开始了关于隐私的讨论。与此同时，关于内网安全中是管理重要还是技术重要的争辩也登上历史舞台。

3. 技术融合与防水墙

时间进入 2006 年，经过数年的发展，传统的网络连接控制、设备加密、补丁分发、监控、行为管理、行为审计等产品逐渐走向融合，桌面安全管理系统开始崭露头角。与传统的分散部署相比，整合后的桌面安全管理系统能够通过对网络中所有设备的统一策略制定、用户行为的统一管理、安全工具的集中审计，最大限度地减少安全隐患。同时，它还对个人桌面系统的软件资源、工作状况进行管理，有效地提高了员工工作效率。桌面安全管理系统的出现，代表着内网安全领域技术整合的开始。也在这一年，信息防泄漏 1.0 版本——能够对抗网络、终端、外设等多样化安全威胁的防火墙登上历史舞台。

融合产品的出现是内网安全发展史上的重大事件。传统的内网安全产品各自独立，企业可以选择每个具体应用上最强的软件来搭建内网安全体系。但这种方式的弱点也非常明显，不同产品互不相通，不但形成信息孤岛，还导致管理权限的交叉和重叠，从而产生更多的问题。融合产品可以将原本分散的多种功能整合成一个整体，有着更高的效率和更好的防护效果，因此一经面世就受到了众多厂商的追捧。

但是融合产品并非没有弱点。许多企业特别是制造企业，在过去的信息化建设过程中已经有了许多应用，要全部更换新系统并不现实，而且会做所有的事情并不代表能把所有事情都做好。因此，是部署分散、独立系统还是部署整体解决方案来构建企业信息安全体系是一个见仁见智的问题，时至今日，仍然是业界探讨的热点。

笔记

4. 透明加密井喷

同样是 2006 年，透明加密产品在信息安全领域刮起了一阵旋风。透明加密软件可以将企业图纸、办公文件等文档进行加密处理，整个过程对用户透明，不改变工作习惯。文档只有在授信的范围内才能打开，离开了授信范围，文档就是一堆乱码，号称“偷得走，打不开”。深陷信息安全风险的企业纷纷购买透明加密软件来保护自己的重要信息，透明加密市场出现井喷，短短半年间就出现了上百种产品，但在市场火热的背后，也埋下了隐患。

由于透明加密市场的突然火热，大量没有掌握核心技术，仅靠购买他人产品贴牌销售的厂商涌入透明加密市场。由于技术不过关，许多用户在应用过程中遇到问题，还出现了不少加密后文档损坏且无法恢复的恶性案例。经过了 2006 年的火爆之后，2007 年透明加密市场急速冷却，大量缺乏技术实力的厂商倒闭。

5. 内网安全走向成熟

2007—2008 年是内网安全领域变化较大的时期。随着移动存储介质的广泛普及，移动存储介质管理及其周边产品得到了用户的认可，主机监控审计产品也开始盛行。2008 年，美国次贷危机爆发，金融风暴席卷全球，中国也未能幸免，大量缺乏核心竞争力的企业倒闭。人心浮动之下，针对窃取企业核心信息的违法行为增多，韩国双龙汽车、现代汽车先后爆出“泄密门”事件，如何保证核心数据的安全再次成为企业关注的焦点。一些厂商将国外的数据泄漏防护（DLP）概念引入中国，根据中国企业的实际需求整合终端防护、存储磁盘、文件管理、版权管理，以及 U 盘、外设端口控制、网页信息保护、即时通信拦截等多个功能，推出了具有中国特色的 DLP 产品。国内部分知名制造企业也吸取其他厂商泄密事件的教训，迅速部署了 DLP 系统，如奇瑞、一汽集团、比亚迪、广州本田等企业都陆续实施了 DLP 数据防泄密系统。

虽然从技术角度看，DLP 系统仍然是各种传统技术的整合，但是它体现出国内厂商已经不再盯着单一的产品或技术，而是开始进行概念和整体解决方案的推广，这无疑比过去单纯的技术概念炒作要高出一个层次，也代表着内网安全厂商更加成熟。

6. 整体信息防泄密时代

2011 年，全球泄密事件仍然层出不穷。索尼 PSN 泄密、富士康 iPad 图纸泄密、达利集团配方泄密、蜀山产业园丢失财政数据 U 盘，无论是相关公司的规模、泄露信息的重要性，还是泄密事件的发生频率，2011 年都超过往年。这表明，企业核心数据的价值已被攻击者认同，他们将花费更多的成本去非法获得企业核心数据。而另一方面，许多企业防泄密意识还不够，对核心信息的价值、内网安全以及信息防泄漏的认识还不足，由于成本原因，很多企业还在建设内网安全究竟是“挣钱”还是“花钱”的问题中纠结。

但是在安全业界，厂商们已经从层出不穷的泄密事件中看到了问题所在。加密不能解决所有的问题，单纯审计也没有任何意义。只有从全局的视角出发，对安全问题进行统筹规划、统一管理，整合运用审计、权限管理、透明加密等防泄密功能，根据涉密程度的不同（如核心部门和普通部门），部署力度不一的梯度式防护，将技术、管理、审计进行有机的结合，在内部构建起立体化的整体信息防泄露体系，使得成本、效率和安全三者达到最优平衡，才能实现真正意义上的内网安全。作为内网安全领域的最新理念，融合审计、监控、加密于一体的整体信息防泄露正式登上历史舞台。

笔记

7. 移动办公时代

随着全球化信息网络进程和无线高速网络的迅速发展，移动智能终端处理能力也越来越强，移动办公必然是未来的发展趋势，越来越多的单位采用智能手机（以 iPhone、Android 系列产品为主）和平板电脑（如 iPad 和华为 MatePad 等产品）等移动智能终端来访问单位内部资源和应用，实现高效的资源共享和办公流程。

如何使用移动终端接入到内网应用系统，如何保障移动接入安全、基础网络通信安全、网络边界安全以及移动应用安全（包括移动终端基本应用和行业应用）成了移动办公应用推广的迫切问题和安全风险。因此，今后的数据安全领域将从传统终端数据 DLP 朝着终端数据安全、应用数据安全和移动安全整体解决方案的领域迈进。

任务 1.4 防泄密保护的数据类型

防泄密保护的数据类型主要有以下 3 种。

（1）文档、图纸类数据。

（2）源代码类数据。

（3）结构化数据。

通常来说，文档加密软件主要用来实现文档（包括文字、图形、图像、声音、视频数据等）、图纸类数据防泄密，DSA 数据安全隔离主要用来实现源代码类数据防泄密，内容智能识别主要用来实现结构化数据防泄密；那么所谓 DLP 数据泄露防护系统，其实质上是一个平台，可以将以上不同方案，融合在一个平台之上。从这里也可看出，目前主流厂商通常将 DLP 数据泄露防护（平台型）用于应对比较复杂型的数据防泄密需求，将其他单个产品主要用于应对简单型的数据防泄密需求，在技术上是有道理的。

另外需要重点说明的是，文档加密软件不能用于源代码防泄密，无论从技术或实践都已表明使用文档加密软件加密保护源代码数据效果不佳，容易使电脑出现卡、慢、蓝屏等现象。目前实现源代码防泄密，大多选择使用 DSA 数据安全隔离方案。

任务 1.5 数据防泄密的应用场景

数据防泄密的应用场景主要有以下 4 种。

（1）PC 终端。

（2）移动终端。

（3）服务器。

（4）网络。

终端中的数据防泄密大多会安装客户端软件，OA、KM 等应用服务器、网络中数据防泄密大多会部署数据泄露防护网关类硬件，但也有例外，如文件服务器中的数据防泄密需求。

任务 1.6 数据防泄密实现的效果

（1）加密实现的效果：非授权人员，打开加密文档显示为乱码，合法人员则可正常打开并使用加密文档。

（2）隔离实现的效果：源代码类数据不出安全区域不受任何影响，要出安全区域则必

须通过内容审核。

（3）拦截实现的效果：对事先经过策略设定的敏感内容进行智能识别、监控，在外发时予以及时拦截。

（4）告警实现的效果：对事先经过策略设定的敏感内容进行智能识别、监控，在外发时予以及时告警。

（5）预警实现的效果：对事先经过策略设定的敏感内容进行智能识别、监控，在触发相关规则时预警。

总体而言，要想全面做好数据防泄密还是需要花费大量时间和经济投入。当然在实践中，单独部署文档加密软件和 DSA 数据安全隔离的用户数量相对多一些，无论是需求，还是整个实施过程也都相对简单一些。

笔记