防水墙在内网信息安全管理中的应用

李红艳　刘东苏　由振荣
（西安电子科技大学经济管理学院　西安 710071）

[摘要]：传统意义上的网络安全防范主要考虑防止外部攻击，而忽视了内网的敏感信息泄露问题，本文在分析内网安全管理现状的基础上，介绍了防水墙的结构部署、基本功能，并结合实际应用探讨了如何利用防水墙技术保证内网安全,并对具体应用结果给予相应的评价。

[关键词]：防水墙，内网，信息安全管理

1 引言

传统意义上，网络安全防范主要考虑的是防止外部攻击，因此，一般的网络系统都通过部署防火墙、入侵检测系统、数据加密、访问控制、防病毒软件、虚拟专网等安全机制与技术手段为内部网络构筑较强的安全壁垒，以减少对内部信息安全的威胁。但就一个信息系统的安全管理而言，对外防御只是其中的一个方面，内部网络的信息泄露也是一个不容忽视的问题。据美国CSI/FBI Computer Crime and Security Survey的数据表明，在计算机安全事件中，由信息泄露造成的经济损失连续几年排在前四位[1]，内网信息安全正日益受到关注。如果管理不善，内部人员可以很轻易将计算机中的机密信息通过网络、存储介质和打印等方式泄露出去，造成不可估量的损失。

目前，学术界也开始关注对内部网安全问题的研究，但绝大多数文献讨论的是计算机安全的普适问题，或是某个安全服务子域的问题。国内外市场上信息安全方面的产品种类繁多，如防火墙、入侵检测系统、漏洞扫描、防毒软件、防电磁辐射泄露、门禁通道系统、加密硬盘和保密机箱等，但大部分产品都是针对防御外部攻击的。防水墙的应用正好能够提供有效的技术手段实现内部安全监管。

2 内网信息安全状况

2.1 内网发展状况

1996年BARBERA等人提出了企业内部网(Intranet)[2]的概念，利用Intranet技术构建仅限企业内部人员信息交流的专用网络。BARBERA同时还指出，企业内部网的安全隐患主要来自内部。内网安全是近年来渐渐兴起的网络信息安全研究与应用领域。通过身份认证、访问控制、操作审计等技术手段约束、限制、监控企业内部人员对计算机网络的使用，使得内部信息交换可控，从而保障内网使用安全。

一般的内网系统都承载了一定的重要信息，按照国家相关保密制度的要求和自身的网络安全体系现状，整个网络按照重要程度划分不同的网段，在不同级别的网段之间设置防火墙，并配置一定的访问控制策略。有的涉密单位为了保障对外的绝对安全，整个网络总体上与Internet是物理隔绝，这在一定程度上排除了外部攻击的可能性，因此网络安全主要体现在内部网络信息安全上。

2.2 内网安全隐患分析

内网安全隐患主要来源于“可信的”内部人员之间无限制的信息共享与传递，

根据统计，各种计算机网络、存储数据遭受的攻击和破坏，80％是内部人员所为[3]。内网安全从目的上更关注内部的保密性、可追究性，更关注内部人员的安全问题，所以内网安全管理更注重对安全时间的可追踪性和可审计性。其不安全因素和数据泄漏途径归纳如表1所示。

表 1 内网系统信息泄露途径和方式

内网系统信息泄露途径	信息泄露方式
计算机网络化造成的信息泄露	·对文件或文件夹不当共享造成信息泄露 ·内部人员在应用互联网服务，如电子邮件、MSN、FTP 时将本单位内部敏感信息传送到外部或被窃取造成泄密。 ·内部人员对本单位网络攻击并恶意窃取单位内部信息
计算机外设接口造成的信息泄露	·开放的 USB、1394 口，串口、并口、PCMCIA 接口、红外、软盘控制器、DVD/CD-ROM 驱动器等造成的信息泄漏。
计算机存储介质、媒体造成的信息泄露	·移动硬盘、U 盘、光盘等存储介质使用监管不严造成的信息泄露。
计算机打印机、显示器造成的信息泄露	·屏幕拷贝、屏幕照相、打印机直接打印进行信息窃取。
其它途径泄密	·由工作人员无意造成的泄密：如将一台发生故障的计算机送修前既不做消磁处理，造成敏感数据的泄密。

针对内网安全方面存在的问题，许多防范工作都仅仅停留在内外网物理断开或采用一定的行管保密措施，如：将涉密信息进行密级标识；禁止使用涉密计算机连接国际互联网或连接移动存储设备；禁止在非涉密计算机上处理涉密信息；涉密计算机配备各种安全机制等。这些制度对信息系统的安全管理十分必要，但不能从技术上和本质上解决内部失泄密的问题，也不利于工作的开展。因此，为了保障内部信息的安全，除了依靠必要的行政管理措施，还必须依靠技术手段加强内部网络的监管。防水墙的应用很好地解决了内网安全方面存在的问题。

3 防水墙及其在内网信息安全管理中的应用

“防水墙”(Water Wall)是相对于“防火墙”(Firewall)的一个概念，它处于内部网络中，可随时监控内部主机的安全状况，是一个用来加强信息系统内部安全的工具[4]。在信息安全体系的安全管理、组织与技术中，其着重点是用技术手段强化内部信息的安全管理，防止内部信息向外扩散。防水墙技术是利用密码学、操作系统核心技术、访问控制、审计跟踪等技术手段，对敏感信息的存储、传播和处理过程实施安全限制保护，使之不被非法或违规的窥探、外传、破坏、拷贝、删除，并完整记录信息处理过程日志，最大限度地防止机密信息外泄的内网数据保护技术[5]。它与防火墙、入侵检测系统、防病毒软件等一同构筑内网数据安全屏障。

3.1 防水墙系统组成结构

防水墙是内网的监控系统。从内部安全体系架构和网络管理层面上, 实现了内部安全的统一。完整的防水墙系统(Water Box，见图1虚线框内)由三部分组成：防水墙服务器(Water Box Server)、防水墙控制台(Water Box Console)和防水墙客户端(Water Box Watcher)。

(1) 防水墙服务器：包括服务器端软件和支持数据库，是防水墙系统的核心部分。通过安全认证机制，建立与多个客户端(受控制的个人计算机)系统的连接，实

现对多个客户端系统的配置、策略制定、资产管理、操作审计等功能。

(2) 防水墙控制台：是系统管理员、操作员、审计员等和防水墙系统交互控制的界面，实现系统管理、参数配置、策略管理和系统审计等功能。控制台采用分权分级的授权模式，严格限制对敏感信息的访问权限，保证系统信息安全。

(3) 防水墙客户端：安装于受监控主机上的检测软件，强制执行来自服务器的安全策略，根据安全策略检测客户端用户的行为。客户端软件采用了严密措施，防止本地用户自行卸载、关闭监控程序。

防水墙显著特点在于：提供集中式的管理、分布式的防护，能够将所管辖系统的全部个人桌面系统纳入管理范畴，不遗漏可能的泄密途径，周密监管、保护网络资源，并可动态获取更新和审计[6]。

3.2 防水墙系统在网络中的部署

防水墙系统是一套软件系统，其部署无需改变当前内网的拓扑结构，防水墙客户端安装在用户终端，防水墙服务器与防水墙控制器部署在防火墙后的第一道防线上(部署结构见图1)。管理员通过管理工作站来管理防水墙服务器，定制实施相关的安全策略，并强制分发到各客户端。防水墙服务器通过位于各部门的客户端工作站来实现对整个内部网络的用户、数据和设备等的管理和监控。

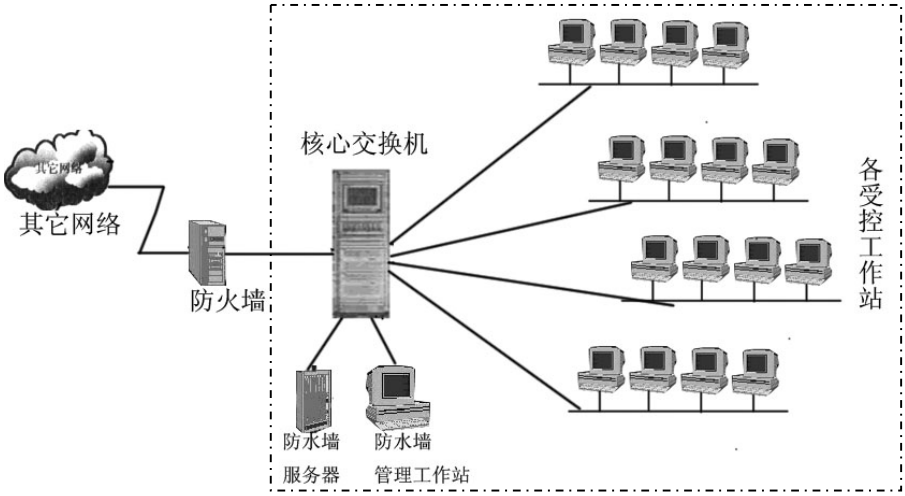

图 1　防水墙部署结构图

3.3 防水墙在内网中的应用

防水墙具备五大功能，即扩展身份认证、文件安全服务、系统资源管理、运行状况监控、失泄密防护功能[7]。利用防水墙构建的内网安全防护体系见图2。

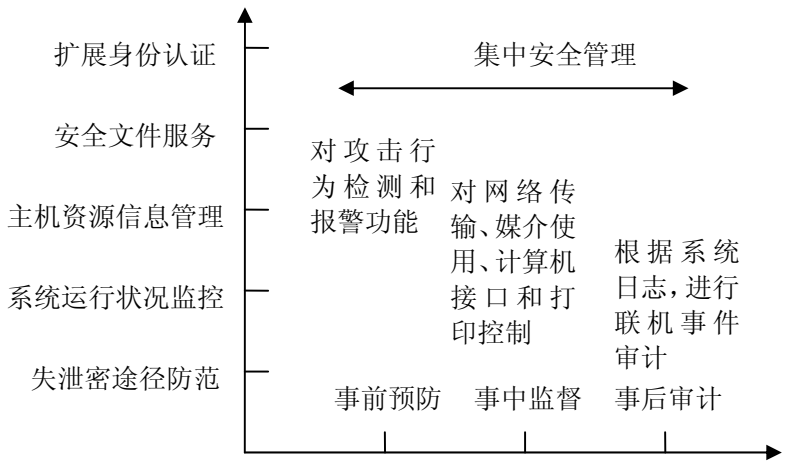

图 2 防水墙安全管理体系

由图2可见, 防水墙将所有与安全相关的内容划分为三个阶段管理，即事前预防、事中监督、事后审计。事前预防包括策略的定义、策略的有效时间和生命周期、策略的维护、策略的继承以及分级分权管理和相应得配套规章制度的建立等；事中监督包括对四种主要泄密事件类型的状况监控和运行状况的纪录；事后审计通过对防水墙系统记录的运行信息和用户操作信息进行事后审计，并提供详细分析报表。

防水墙主要有两大管理对象，一是重要的信息，一是不可靠的人。重要信息可利用加密技术和访问控制实现安全防护，防止外泄。对人员依靠监控工作状态和审计系统管理。应用防水墙构建的内网安全体系，通过统一IP绑定管理，基本杜绝了内网信息泄露问题，对前面所分析的内网信息安全方面存在的问题，均可应用防水墙系统进行解决：

(1) 针对计算机网络化造成的信息泄露，可运用防水墙所提供的“扩展身份认证”和“文件安全服务”功能，用户首先通过身份验证机制登录到防水墙客户端，防水墙身份认证系统会接管Windows 身份认证系统，通过设置安全域、授权、对文件加密实现内网用户之间文件共享互传。有效地防止了文件在传输途中可能造成的泄密，也防止了电脑丢失可能造成的泄密事件的发生。

防水墙的“运行状况监控”功能, 可以随时抓取网上的计算机界面，对内网计算机的联网、脱网和工作状况可以及时监控，并可详细记录网内的所有活动，如浏览网站、收发邮件、上传和下载文件等。可以预先对某些网络活动进行阻止, 防止通过网络传送敏感数据或浏览无关工作的网站。也杜绝了内部人员使用电子邮件、MSN、FTP等将本单位内部敏感信息传送到外部造成的泄密。

(2) 对于计算机外设接口造成的信息泄露，防水墙提供的“主机资源信息管理”功能集中管理客户机内的硬件、软件和其它资源。对计算机USB 接口、1394 接口、串口、并口、红外线等外设接口进行相应的控制，将客户端上的外设接口和软硬件信息传输到远程服务器端，服务器根据管理员事先定制的安全管理策略对各种接口以及其它硬件进行统一管理，包括禁用，卸载等。能有效防止计算机外设接口造成的信息泄露。

(3) 计算机存储介质，如移动硬盘、U盘、光盘等存储介质使用监管不严格造成的信息泄露。通过使用防水墙系统的“可信移动存储介质管理”功能，首先对移动

存储介质进行分级，并进行统一认证，使用加密存储、密级访问控制等手段，有效防止移动存储介质在计算机上跨密级使用。对于未经认证的笔记本电脑或移动硬盘、U盘等设施联网时系统将自动作无效处理。同时系统还将操作涉及的信息及过程生成日志，以便进行事后审计。

(4) 对于计算机打印机或显示器造成的信息泄露，将用户打印机放置到专门的机房内，根据需要设定不同的策略进行控制。即使是在授权状态下, 使用者的打印操作也将受到监控, 打印内容会由系统自动备案处理, 以便事后审查。同时，管理员可根据机房的视频监控系统随时监视显示器造成的信息泄露，如屏幕拷贝、屏幕拍照等。

(5) 其它途径泄密，如将一台发生故障的计算机送修前不做消磁处理，造成敏感数据的泄密，防水墙的“运行状况监控”和“安全审计”功能随时监视和备案可能造成的信息泄露。以便追究责任。

4 结束语

基于防水墙的内网安全保护系统已经在某研究所实施了近半年时间，它的应用切实有效地降低了内部敏感信息的泄露、破坏和外传风险，实现了信息安全监管和审计，从技术上有效地保护了内部网络敏感信息的安全，因此，基于防水墙的内部安全管理体系是信息网络安全体系的重要补充。

参考文献

[1] Gordon L A,Loeb M P,Lusy shyn W,et al. CSI / FBI COMPUTER CRIME AND SECURITY SURVEY[C]. 2006:15-24.

[2]BARBERAJ，RATIT D，JEAPES B.The Intranet:a new concept for corporate information handing [C].proceeding of 20th international online information meeting, London England United kingdom IEEE,1996:187-193

[3] 刘伟，余彬.内部网络的安全浅析[J].计算机与数字工程，2007(01):68-70.

[4] 陈尚义,刘胜平,赵泰.基于防水墙系统的信息安全与保密解决方案[J].信息安全与通信保密，2006(07):49-51

[5]李文剑.防水墙技术初探[J].信息安全与通信保密，2007(5):107-108.

[6]董志民.防水墙守护内网安全[J].企业管理，2007(06) :104-106.

[7]吴德.构建整体一致的内网安全体系[J].信息安全与通信保密，2008(12):28-30.