浅析档案数据库的安全管理模式

摘　要：档案数据库凭借网络这一强大的信息获取和交流传输方式，得到了快速发展，但同时也对其安全管理带来了新的挑战。文章阐述了保障档案数据库信息安全的管理模式：防火墙管理模式、C/S 管理模式、人工同步安全管理模式。

关键词：档案数据库　安全管理　模式

◇ 张　威

档案数据库凭借网络这一强大的信息获取和交流传输方式，得到了快速发展，但同时也给档案数据库的安全管理模式带来了新的挑战。因此，网络环境下的档案数据库信息安全问题就显得尤为重要了。

一、防火墙管理模式

防火墙技术是近期发展起来的一种保护计算机网络安全的技术性措施，它在某个机构的网络和不安全的网络之间设置障碍，阻止对信息资源的非法访问，也可阻止专利技术从网络上被非法输出。也就是说，防火墙是一道门槛，用它来控制进、出两个方向的通信。防火墙技术是被动防卫型安全保障系统，它的特征是在网络边界上建立相应的网络通信监控系统来实现安全保障，要求所保护的网络是一个相对封闭的拓扑结构，只是在有限出口与外界联络。建立防火墙就是利用专用安全软件、硬件以及管理配置，对内部网络与外部网络之间的往来信息进行检测、控制和修改。防火墙最常采用的技术有数据包过滤（Packet filter）、应用网关（Application Gateway）和代理服务器（Proxy Server）。数据包过滤技术是根据数据包的源地址、目的地址、TCP（传输控制协议）端口令等因素或它们的组合来综合判断，只有满足逻辑条件才允许通过，选择的判断依据即为系统内部事先设置的过滤逻辑包，这一过程多在路由器上完成。防火墙系统一般由许多软件与硬件共同构成。其主要作用是在保护专用网络免受外部攻击的同时，使网络用户能够在最低风险状态下访问公共网络。档案信息系统防火墙应能为档案信息的共享、交换提供如下安全保障：保证所有档案信息的共享、交换都是授权访问，在转发所有信息流的同时能够逐项屏蔽掉可能有害的服务；能够封锁所有信息流，只对需要的服务逐项开放，以保证档案信息的共享、交换平台免遭攻击或非法入侵，保护关键系统免受外部或内部的攻击；支持私有数据加密，保证通过因特网进行的档案信息的共享、交换活动不受破坏，具备反欺骗功能，能够检测并屏蔽掉来自网络外部的非法数据包，广泛支持 WWW、HTTP、FTP 等服务。采用防火墙的访问控制原则，在网络层控制内外网之间计算机的互访、在档案专网和公网之间、在档案馆局域网和档案专网之间分别设立防火墙并建立相应的访问控制策略，以限制馆内外用户的进出访问。通过防火墙也可以将馆内局域网划分为更细的网段，如开放区、业务操作区和数据服务区等，分别实施不同安全级别的管理。

二、C/S 管理模式

在网络链接模式中，除对等网外，还有另一种形式的网络，即客户机 / 服务器网，即 C/S。在客户机 / 服务器网络中，服务器是网络的核心，而客户机是网络的基础，客户机依靠服务器获得所需要的网络资源，而服务器为客户机提供网络必须的资源。档案馆内采用 C/S 运行模式，管理方便，运行效率高，每个用户的操作权限是根据其业务需求来指定，主要包括对系统的功能操作权限和数据操作权限两大类；档案专网内的授权用户可以采用 C/S 和 B/S（浏览器 / 服务器）两种模式访问业务数据，其安全授权方式一方面通过档案馆与外网之间的防火墙访问控制策略进行限制；另一方面通过应用程序的身份认证来判断该用户是否是档案管理信息系统的合法用户，来限制其访问权限。

1.C/S 架构软件的优势。一是应用服务器运行数据负荷较轻。最简单的 C/S 体系结构的数据库应用由两部分组成，即客户应用程序和数据库服务器程序。二者可分别称为前台程序与后台程序。运行数据库服务器程序的机器，也称为应用服务器。一旦服务器程序被启动，就随时等待响应客户程序发来的请求；客户应用程序运行在用户自己的电脑上，对应于数据库服务器，可称为客户电脑，当需要对数据库中的数据进行任何操作时，客户程序就自动地寻找服务器程序，并向其发出请求，服务器程序根据预定的规则作出应答，送回结果，应用服务器运行数据负荷较轻。二是数据的储存管理功能较为透明。在数据库应用中，数据的储存管理功能，是由服务器程序和客户应用程序分别独立进行的、前台应用可以违反的规则，并且通常把那些不同的（不管是已知还是未知的）运行数据，在服务器程序中不集中实现。对于工作在前台程序上的最终用户，无须过问（通常也无法干涉）背后的过程，就可完成自己的一切工作。在 C/S 体系下，数据库不能真正成为公共、专业化的仓库，它受到独立的专门管理。

2.C/S 架构软件的劣势。Internet 上的用户分布地域较广，因此，档案馆内部采用 C/S 运行模式是非常合适的，但是 C/S 模式本身的缺点和不足也是很明显的：客户端需要安装专用的客户端软件。首先涉及到安装的工作量；其次任何一台电脑出问题，如病毒、硬件损坏，都需要进行安装或维护；再次，系统软件升级时，每一台客户机需要重新安装，其维护和升级成本非常高。这也使得 C/S 构架具有了投资大且维护成本高的劣势。采用 C/S 架构，要选择适当的数据库平台来实现数据库数据的真正“统一”，使分布于两地的数据同步完全交由数据库系统去管理，但逻辑上两地的操作者要直接访问同一个数据库才能有效实现。

三、人工同步安全管理模式

人工同步安全管理策略包括：操作系统统一升级、病毒库同步升级、日常操作严格把关，统一部署馆内计算机操作系统的升级方案、病毒库升级方案，安装防病毒软件，及时进行系统更新，采用及时备份、人工断网等基本操作规程，部署一体化安全防线。加强内部安全管理，按照密级管理原则，将保密数据服务器实行脱机操作，其数据交换主要是借助于移动 U 盘、光盘、磁带等设备进行，也可将两台独立的服务器单独联网完成数据交换。加强个人的安全防范意识，提高档案馆内所有人员的安全责任感，做到从每个人到每台机器的同步安全和统一管理才是整个信息安全管理过程中最为重要的内容。

[责编　赵晶莹]