论企业内部网的安全策略

摘要

2007 年 3 月至 12 月，作者负责开发了所里的科研信息管理系统，承担系统技术选型、系统分析与设计等工作，整个系统包括科研任务计划子系统、任务管理子系统、课题文档管理子系统、资源管理子系统、信息发布子系统。

本文从单位的实际和科研信息管理系统在所里科研生产过程中重要性出发，在安全策略方面分别对加强访问安全措施、系统数据的安全、网络版防病毒软件的部署、安全管理制度的建立等方面的安全措施进行了详细论述和分析。指出在系统建设过程中，网罗安全策略的实施必须建立在对系统环境进行综合分析的基础上，要处理好应用与安全、安全与代价之间的关系，注重管理在安全方面的重要作用，合理应用现有网络安全设施，引进新的安全技术，全方位、系统化的解决各类安全问题。只有这样才能保证系统的安全性、保密性和可靠性。

正文

我所是一个国有大中型军工科研单位，每年承担了大量的国家及其他科研任务，保证科研任务的顺利圆满完成是我所的工作重心。我所对科研任务的管理一直处于半手工的管理方式，主要利用一个基于 access 数据库的单机版软件，对

科研部分业务进行管理。随着我所科研战略的调整，原有系统很难适应所里的业务发展要求。2007 年 3 月经所里研究决定由信息中心统一负责，科技处及各研究室全面支持，着手开发适合我所信息化及科研业务发展要求的科研信息管理系统。整个系统包括科研任务计划子系统、任务管理子系统、课题文档管理子系统、资源管理子系统、信息发布子系统。

我作为信息中心的技术骨干，有幸负责系统技术选型、系统分析与设计等工作。保密安全一直是我所常抓不懈的工作，再加上科研信息管理系统在我所科研管理中的重要地位，我在系统建设过程中，一直不敢放松保密安全这根弦，采取各种技术和措施，全方位保证所建系统的安全性、保密性。

一、加强访问安全措施，保证系统终端用户的合法性，监控终端用户的操作行为

随着我所科研业务的不断增加，横向合作的课题越来越多，致使同我所往来的单位和人员比较繁杂，如何保证空闲接入点的安全，是我们首先要解决的问题。同时随着互联网应用的不断普及，以及接入方式的多样性，这就为系统的保密安全性提出了更高要求。为此，我建议单位部署了非法外联监控系统，对内部网计算机非法接入互联网和外来主机接入内部网等行为进行监控，发现非法行为及时告警且切断非法的连接，从而保障内部网与外界的完全隔离，确保内部机密信息的安全。监测内部网中发生的外来主机非法接入、篡改 IP 地址、盗用 IP 地址

等不法行为，由监测控制台进行告警。运用用户信息和主机信息匹配方式实时发现接入主机的合法性，及时阻止 IP 地址的篡改和盗用行为。

非法外联监控系统的部署，保证了终端计算机的合法性，杜绝了非法接入互联网的违法行为，但是，在合法终端的用户身分认证方面无能为力，为此，我在科研信息管理系统分析过程中引入了基于角色的授权管理。通过分配和取消角色来完成用户权限的授予和取消，并且提供角色分配规则。安全管理人员根据需要定义各种角色，并设置合适的访问权限，而用户根据其责任和资历再被指派为不同的角色。这样，整个访问控制过程就分成两个部分，即访问权限与角色相关联，角色再与用户关联，从而实现了用户与访问权限的逻辑分离。

二、全面考虑，加强系统数据的安全与可靠

科研信息管理系统是我所的核心业务系统，系统的高效、稳定运行，数据的安全、可靠存储，以及故障后系统数据的快速恢复是系统必须具备的性能。只有这样才能保证我所的科研生产工作的顺利进行。在保证系统数据安全方面，首先，我对操作系统、数据库管理系统选型进行了认真分析，选择了适用于大中型企业的性能稳定的 Aix 操作系统和 DB2 数据库管理系统。放弃了对 Windows 操作系统和 SQLServer 数据库管理系统，虽然，为系统的管理与维护造成很大的不便，但是从系统层保证了科研信息管理系统的安全与稳定运行；其次，我将科研信息管理系统及数据存储在已有的 RAID 中，同时将该系统数据的备份工作加入到现有

的磁带库备份策略中。在保证系统数据安全的同时，增强了系统数据的故障恢复能力；第三，鉴于科研信息管理系统在所里科研生产中的重要性以及应用范围，系统的高负载性、高可用性我也必须予以考虑。为此，我在项目中使用了集群技术，利用 WebSphere 配置了群集环境，架设了两套成员系统，各集群成员具有集群中完全相同的副本，实现了工作负载管理以及 URL 和 EJB 请求故障转移。防止了系统单点故障的发生，提高了系统的运行效率和可靠性，保证了科研生产活动的正常开展。第四，结合我所的域管理模式，我们对客户端的系统设置、权限范围进行了限制，限制客户端随便安装盗版软件、对软件系统不升级的现象，保证了客户端行为的一致性。

三、部署网络版防病毒软件，保证系统平台正常运行

虽然我所园区网实现了内外网物理隔离，以及对光驱、软驱、U 口的严格管理，但是也必须留有大量的输入输出口，以方便园区网与外部环境的信息交互，方便大家工作。这也就不可避免造成将外部的病毒软件、攻击软件等带入园区网，影响系统安全。鉴于病毒在网络上来源广、传播快的特点，我建议所里采购了瑞星高级企业专用版防病毒软件（集团定制）。全网统一部署防病毒软件，加强病毒防护能力，实现病毒库文件的统一更新，统一查杀，防止系统病毒的快速传播。同时，我们可以根据近期病毒情况和单位业务特点，动态调整查杀策略。通过网络版防病毒软件的部署，我们保证了网络环境的干净，防止了病毒等不安全软件

向园区网的传播。

四、完善安全管理制度，提高职工安全意识

安全管理是三分技术七分管理，我认为这种观点对于信息系统的安全也是同样适用。在信息化建设中，安全技术不是万能的，而往往由于安全技术手段使用太多，致使信息系统运行缓慢，影响正常生产。而且，有时会出现根本没有相关安全方面的技术解决方案，由此造成的系统安全方面出现“短板效应”我们如何能防止呢，所以，我们在适当应用先进技术的同时，必须要发挥管理手段的作用。由于，考虑到科研信息管理系统在保密安全方面的重要性，在我所保密办的配合下，我们制定了“系统保密安全管理规定”，明确规定了客户端用户的规范操作，对于利用各种方法卸载安全软件、造成安全事故的行为我们严加惩罚。通过管理手段，我们避免了由于现有安全手段无法解决的安全问题的发生。

2007 年 12 月份系统通过了所里的验收，目前系统已经运行近一年时间，在我所的科研管理中发挥着重要作用，特别是系统数据的保密安全方面得到所里的一致好评。在加强访问安全措施方面，通过非法外联监控系统的部署解决了我所因地域广、网络布点散造成的安全隐患，基于角色的权限管理增加了系统权限设置的灵活性和科学性；在系统数据的安全方面，充分利用我所园区网的现有设备与安全手段，在解决科研信息管理系统安全问题的同时，为我所节省了大量资金；

通过网络版防病毒软件的部署，使我所的病毒防护由以前的单机防护转变为目前的全网统一防护，大大提高了防护能力；通过安全管理制度的制定和宣传，在规范我所职工安全应用系统的同时，也提高了大家的保密安全意识。

通过该系统安全体系的建设，增强了系统的安全性、保密性、可靠性，但是同时也为网络的安全管理工作增加了许多工作量，再加上我所原有的防火墙、入侵检测系统等，每个系统都要安排专门人进行管理与监控，每个系统问题都是单独处理，这样会造成很大的人员付出。如果下一步我们实现了各网络安全管理系统的集成，使各个安全系统能够联动相应，实现统一监控，统一管理，大将会大大提升我们网络管理与维护的工作效率。

在系统建设中，系统数据的安全离不开网络安全，网络安全是我们必须要面对和解决的重要问题。我们在对系统环境进行综合分析的基础上，处理好应用与安全、安全与代价之间的关系，注重管理在安全方面的重要作用，合理应用现有网络安全设施，引进新的安全技术，全方位、系统化的解决各类安全问题。只有这样才能保证系统的安全性、保密性和可靠性。