广西计划系统纵向网安全体系研究与实践
Discussion on the Portrait Safety System of Guangxi Project Division

胡安韩
Hu Anhan

(广西经济信息中心　南宁　530022)
(Guangxi Economic Information Centre, Nanning, 530022)

摘要　广西计划系统纵向网安全体系的建设必须遵循整体性、实用性、动态化、长远安全预期、经济性和技术与管理相结合等原则，通过完成物理安全、网络安全、病毒防范以及安全管理等部分工作，初步形成了系统的安全体系结构。在此基础上，数字证书认证中心和网络安全检测和监控系统的建立，使网络安全体系更加完善。

关键词　计划系统纵向网　安全体系　原则
中图法分类号　TP393.08

Abstract　The principles of integration, practicability, development, long-term safety forecast, economy, combination of technique and management must be followed in the establishment of the Portrait Safety System of Guangxi Project Division. At the moment, the portrait safety system has been built up basically by the accomplishment of parts of physic safety, network safety, anti-virus and safety management, and will be improved by the establishment of the certification authority of digital certificates and network safety detection system.

Key words　portrait safety system of project division, safety system, principles

1　概述

当今，黑客威胁已屡见不鲜，计算机网络犯罪所造成的经济损失令人吃惊。据有关资料介绍，仅在美国每年因计算机犯罪所造成的直接经济损失就达 150 亿美元，在全球平均每二十秒就发生一次网上入侵事件。

据我国公安部提供的资料，1998 年中国共破获电脑黑客案件近百起，利用计算机网络进

2002-06-26 收稿。

行的各类违法行为在中国以每年 30%的速度递增。因此，网络和信息的安全已成为信息化建设中不可缺少的重要环节。没有安全，网络和信息系统建设就失去了意义。

广西计划系统纵向网是国家计划系统纵向网的组成部分，与国家计委及各省、自治区、直辖市、计划单列市、副省级城市的计委相联，是计委系统内部信息应用、共享与交换的平台，主要传输内部级、秘密级和机密级的数据、话音和视频信息，平台结构如图 1 所示。由于，广西计划系统纵向网的安全保密涉及国家的根本利益，面对当前计算机网络的种种安全威胁，必须采取有力措施来保证安全，纵向网的安全体系设计必须使网络能够抵御敌对势力和不法分子采取的各种攻击，保证各种信息在传输、存储过程中的安全保密，确保系统资源和信息访问的安全。

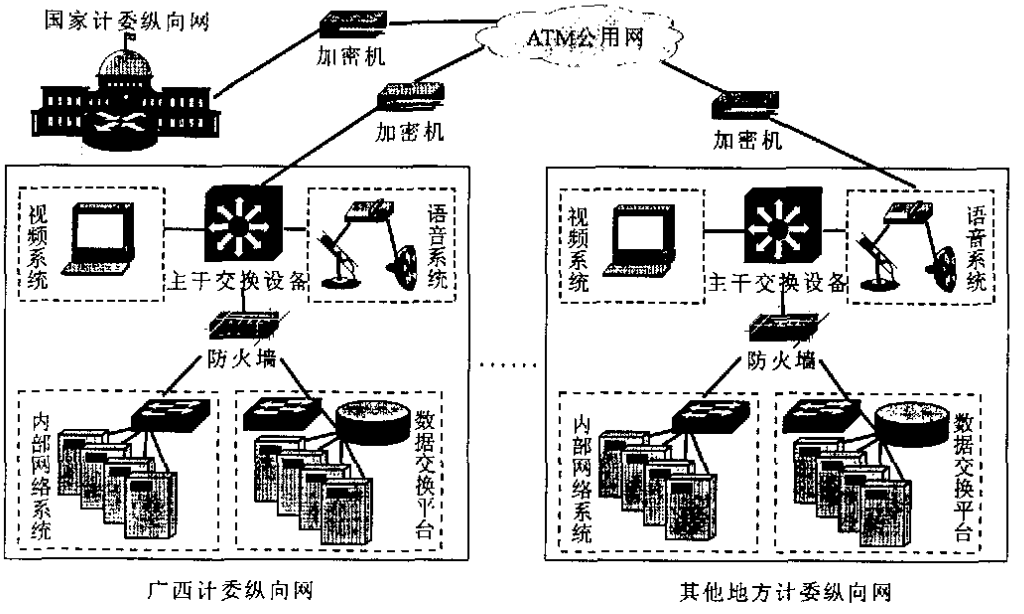

图 1　国家计划系统纵向网平台结构图

2　广西计划系统纵向网安全体系建设原则

对广西计划系统纵向网安全体系的建设，除了遵照国家有关的法律法规外，从工程技术的角度，必须遵守如下原则。

2.1　整体性原则

依据安全模型理论，综合运用保护、检测、响应和恢复四个方面的技术建立一套全方位的信息保障体系，不是孤立地解决单个问题。

2.2　实用性原则

既要安全保密，又不影响系统的正常运行和合法用户的操作。

2.3　动态化原则

安全是一个动态的过程，进攻和防守的关系不断变换。因此，要根据实际情况，不断更新安全保密体系。

2.4　长远安全预期原则

整个安全系统的建设要有总体和长远打算，要考虑到科学技术的发展，攻防技术的进步，

使系统在整个生命周期内的安全得到支持。

2.5 经济性原则

安全体系要尽量经济合理，整个计划系统联合共建，避免重复投资，尽量减小安全体系的规模和复杂性，使之具有很好的可操作性。

2.6 技术与管理相结合的原则

任何系统都包含有人的因素。因此，系统的安全解决方案，必须在考虑技术解决方案的同时还要考虑管理、法律法规方面的问题，将技术与管理相结合。

3 广西计划系统纵向网安全体系建设

广西计划系统纵向网安全体系建设，主要完成了物理安全、网络安全、病毒防范以及安全管理等几部分工作，初步形成了系统的安全体系结构。

3.1 物理安全

广西计划系统纵向网由网络连接设备、网络线路、计算机硬件平台和应用平台等要素构成，保证这些要素的物理安全是建设整个系统安全体系的基础。

为了保证广西计划系统纵向网的物理安全，我们采取了两项措施，其一是按照国家安全保密部门的规定，广西计划系统纵向网作为内部网建设，与连接因特网的广西互联网（外网）完全隔离，具有独立的网络布线系统和网络连接设备，并且严格控制了网络布线工程的设计和施工质量，保证系统物理链路的可靠运行，防止非法的物理接入。其二是使机房结构达到国家安全保密部门的要求，提供良好的温度、湿度等设备运行环境，保证所有物理设备的安全可靠，对关键设备（如加密机）采用了电磁屏蔽措施，防止电磁泄露。

3.2 网络安全

计算机网络的安全性主要包括网络服务的可用性、网络信息的保密性和网络信息的完整性。由于现有的网络安全产品从不同角度保证网络信息的安全，广西计划系统纵向网主要采用防火墙、加密机和物理隔离等来保证网络安全，网络安全结构如图2所示。

3.2.1 防火墙

防火墙是网络安全防范策略的第一个执行层，使用防火墙一方面保护服务器不受来自外部的攻击，另一方面也防止内部非授权用户从内部其他网段对服务器的攻击。广西计划系统纵向网采用了北京天融信公司的NGFW2000硬件防火墙，对进出网络的数据信息进行包过滤和访问控制。

3.2.2 加密机

加密的主要目的是防止信息的非授权泄露。广西计划系统纵向网采用2M的ATM接入方式接入国家计委中心接点，在ASX－200BX交换机与ATM公用网相连的线路上加入了信息产业部30所生产的PWL324 ATM密码机，在国家计委中心接点除配置密码机外，还配置了密钥分发管理中心，负责全国计划系统纵向网各个节点的密钥分发和管理。广西计划系统纵向网通过加密机实现与全国计划系统各接点之间信息传输的加解密，保证网络信息的安全。

3.2.3 物理隔离

广西计划系统纵向网具有独立的网络布线系统和网络连接设备，与连接因特网的广西互联网络已实现物理隔离。为了使客户端能在被隔离的2个网上进行工作，我们在客户端每一台计算机上安装了2个硬盘和1块隔离卡，对客户端也进行了物理隔离。我们在每台计算机上的

2 个硬盘中，分别安装相互独立的操作系统和各种软件，它们分别被称为“内网硬盘”和“外网硬盘”，当用户选择上内网时，计算机从内网硬盘起动，而外网硬盘不工作，此时，计算机与内网连接，而与外网断开；当用户选择上外网时，计算机从外网硬盘起动，而内网硬盘不工作，此时，计算机与外网连接，而与内网断开。由于内外网切换时需要清空内存数据，因此，在内外网切换时计算机重新起动[1]。这样，通过客户端的物理隔离，既方便了用户上内外网，又达到了保证网络安全的目的。

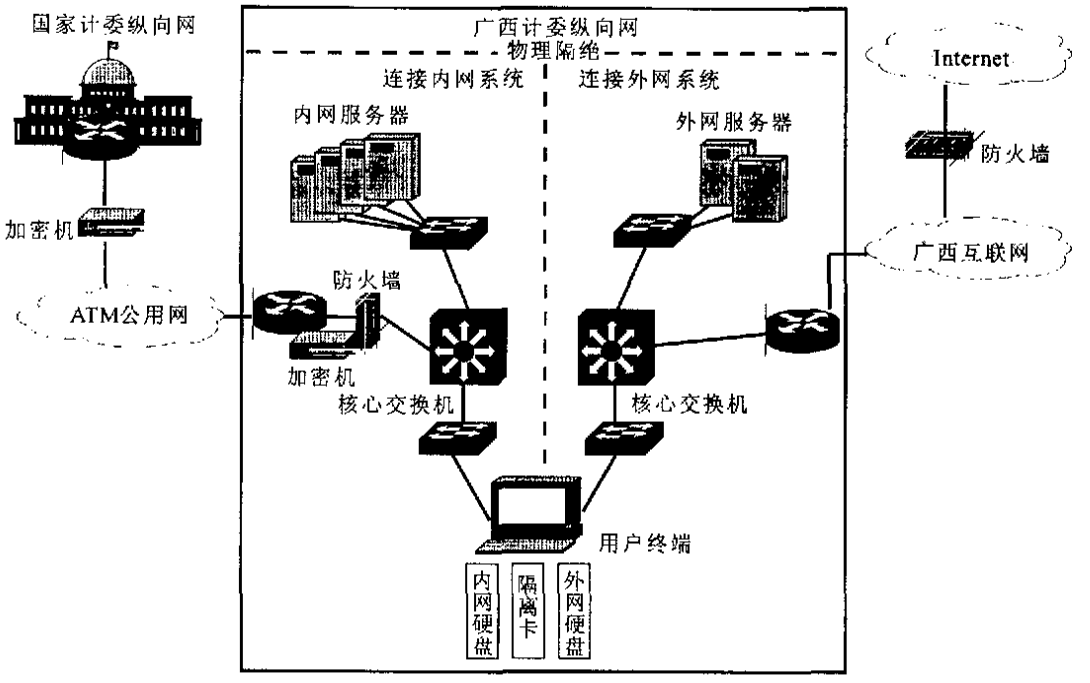

图 2　广西计委纵向网网络安全结构图

3.3　病毒防范

在网络环境下，计算机病毒有不可估量的威胁性和破坏力。网络中的所有文件服务器，会遭受大量引导型病毒、DOS 病毒、32 位 WINDOWS 病毒以及宏病毒等的攻击。同时，由于文件服务器为网络中所有工作站提供信息资源共享，因而也成为病毒理想的隐身寄居场所，进而将病毒轻而易举地扩散到网络中的所有工作站上。此外，随着电子邮件应用的日益普及，病毒入侵又增加了一个管道。在广西计划系统纵向网中，对所有可能被病毒攻击的服务器和通道中设置对应的防病毒软件，使网络免受病毒的入侵和危害。

3.4　安全管理

在网络的安全体系中，管理性和技术性是相辅相成的，在加强技术性防范的同时，必须加强网络的安全管理，因为有许多不安全因素来自组织管理不当和人员使用方面。因此，为了保证广西计划系统纵向网的安全，成立了广西计划系统纵向网安全领导小组和领导小组办公室，制定了安全管理的各种规章制度，对负责网络安全的人员进行了专门培训，初步建立起管理性和技术性是相结合的广西计划系统纵向网安全体系。

4 广西计划系统纵向网安全体系建设的完善

4.1 数字证书认证中心(CA)的建立

证书机制是目前被广泛采用的一种安全机制,使用证书机制的前提是建立CA(CERTIFICATION AUTHORITY—认证中心)以及RA(REGISTRATION AUTHORITY—注册审批机构)系统。

广西计划系统纵向网将根据国家计划系统纵向网的统一部署建立系统内的CA中心,又称为数字证书认证中心,负责为每个使用公开密钥的用户发放一个数字证书,管理用户(包括各种应用程序)的证书,把用户的公钥和用户的其它信息捆绑在一起,在网络上验证用户的身份,为网络建立起一个安全的运行环境,使相关工作人员可以在多种应用环境下方便地使用加密和数字签名技术,保证信息传输的机密性、真实性、完整性和不可否认性。

4.2 网络安全检测和监控系统的建立

信息网络的安全防护是一个多方位的复杂问题,信息网络面临的安全威胁是动态的、发展的。广西计划系统纵向网已建立的每一种安全防护技术都只能解决某一方面的问题,并且相对来说是静态的。而网络安全检测技术和安全监控技术是更注重动态安全策略的技术。

使用网络安全检测产品定期检测网络安全状况,发现安全隐患和漏洞。通过检测,建立系统安全档案,明确需要完善的功能和改正的问题,及早采取措施,增强系统的安全性。

使用安全监控产品实时监测网络活动,查找入侵活动和安全违规活动,记录安全事件,为日后的安全审计、问题查找和系统恢复提供依据,对违背安全规则的网络活动可根据安全策略实施通信阻断。

因此,广西计划系统纵向网将根据国家计划系统纵向网的统一部署建立网络安全检测和监控系统,使网络安全体系更加完善。

参考文献

1 赵 龙. 网络物理隔离解决方案探讨. 计算机安全,2001,80(10):46.

(责任编辑:黎贞崇)

(上接第115页)

4 结语

中国企业实施ERP难度虽然很大,但只要切实做好各项工作,就能达到预期目标,并与国际企业信息化发展潮流同步。

参考文献

1 Ravi Kalakota,Marcia Robinson. 电子商业. 潇湘工作室译. 北京:人民邮电出版社,2001.

2 朱春燕,马光华. 第二界ERP在中国大型研讨会文献全集. 北京:计算机世界信息服务中心,2001.

(责任编辑:邓大玉)