ISSN 1002-4956
CN11-2034/T

实 验 技 术 与 管 理
Experimental Technology and Management

第 25卷 第 8期 2008年 8月
Vol. 25 No. 8 Aug. 2008

特约专栏—高校信息化运维服务体系建设的研究与实践

编者按：最近 10多年，中国高校信息化建设得到快速发展。建设起步早的高校，其信息化工作已从以建设为主的阶段向建设与运行并重的阶段转型，部分高校从整体上开始进入深化信息技术（IT）应用和加强 IT运维服务管理为主要特征的“运维服务”阶段，取得了丰硕成果，为促进高校的现代化管理、提高教学质量和科研水平、实现学校的整体发展目标作出了卓越贡献。

为了及时总结和推广“高校信息化运维服务体系建设”的经验，本刊“特约专栏”邀请清华大学、复旦大学、中山大学从事信息化工作的工程技术人员撰写了 8篇论文，包括两个主题：（1）高校信息化运维体系的理论探讨，涵盖其定位、目标、任务和结构；（2）信息化运维服务体系建设的技术研究，涉及信息安全、信息系统运行环境规划、设计、优化和服务等内容。

上述论文反映了作者所在学校信息化运维服务系统建设和研究的最新成果，具有较高的学术水平和实际参考价值，本“特约专栏”分两期于 2008年第 7、第 8期刊出，以飨读者。

数字校园信息安全保障体系的设计与实现

吴海燕，戚 丽，沈立强

（清华大学 计算机与信息管理中心，北京 100084）

摘 要：完善的信息安全体系是数字校园可持续发展的有力保障，该文对信息集成阶段数字校园的信息安全风险进行了分析，提出了将数字校园划分为若干安全域和根据各安全域的安全需求部署安全技术、进行安全防护、实施整体安全管理的数字校园信息安全保障体系设计方法，构建了数字校园整体安全体系。在此思路的指导下，清华大学实现了以数据中心为核心，将安全技术、管理、服务辐射到关键职能部门的信息安全保障体系中。该文最后对清华大学的实践工作进行了介绍。

关键词：信息安全；数字校园；信息集成

中图分类号：TP393.08 文献标识码：B 文章编号：1002-4956(2008)08-0001-06

Design and implementation of information security system in e-campus

WU Hai-yan, QI Li, SHEN Li-qiang

(Computer and Information Management Center, Tsinghua University, Beijing 100084, China)

Abstract: Sound information security system is the powerful guarantee for e-campus's sustainable development. This paper performs security risk analysis on the e-campus information integration stage. The e-campus will be divided into several security domains, and security technology will be deployed accordingly. Under the guidance of this thought, Tsinghua University built its information security system. The practice of work is introduced finally.

Key words: information security; e-campus; information integrity

1 数字校园信息安全概述

“数字校园”是以网络为基础，利用先进的信息化手段和工具，实现从环境（包括实验室、教室、设备等）、资源（如公文、图书、讲义、课件等）、到活动（包括教学、科研、管理、服务、办公等）的全部数字化，在传统校园的基础上构建一个数字空间，以拓展现实校园的时间和空间维度，从而提升传统校园的效率，扩展传统校园的功能，最终实现教育过程的全面信息化，达到提高教育水平和效率的目的[1]。

中国高校数字校园，或者说高校信息化经过

收稿日期：2008-04-01

作者简介：吴海燕（1974—），女，黑龙江省大庆市人，博士，高级工程师，主要从事教育信息化方向、信息安全方向的研究。

10多年的发展，目前已经进入全面、快速的发展阶段。纵观高校信息化 10多年的发展，其建设过程是有阶段性的，不同的阶段关注点不同[2]，部分高校已经经历了系统集成和应用集成阶段，正在进入信息集成阶段，而有些高校还正处于系统集成或者应用集成阶段。在信息化的不同阶段，信息化建设和网络 (信息) 安全的关注重点都是不同的。在系统集成阶段，信息化的重点是网络基础设施和独立信息应用的建设，网络 (信息) 安全的重点是保障校园网络的可用。在应用集成和信息集成阶段，关注的是信息资产的安全，也就是数字校园关键数据、关键部门应用的安全。

本文首先对信息集成阶段数字校园的信息安全风险和安全目标进行了分析，据此提出了以数据中心为核心，将安全技术、管理、服务辐射到关键职能部门的数字校园信息安全保障体系的构建方法上，最后介绍了清华大学的实践。

2 数字校园信息安全风险分析

信息安全 (information security) 是指确保具有重要意义的信息的保密性、完整性和可用性，以及真实性、责任性、不可否认性和可靠性。信息安全的成功解决方法是正确地建立、实施和维护一个信息安全体系。风险分析 (risk assessment), 有时也称为风险评估，是组织使用适当的风险评估工具，对信息和信息处理设施的威胁 (threat)、影响 (impact) 和薄弱点 (vulnerability) 及其发生的可能性的评估，也就是确认信息安全风险及其大小的过程。风险分析是信息安全体系的基础，它为信息安全管理的后续工作提供方向和意见，后续工作的优先等级和关注程度都是由信息安全风险决定的，而且安全控制的效果也必须通过对剩余风险的评估来衡量。

为了明确被保护的信息资产，相关部门应该列出与信息安全有关的资产清单，对每一项资产进行确认和适当的评估。信息资产是数字校园信息安全保障体系保护的对象，在分析数字校园信息安全风险之前，我们首先对信息资产在数字校园的分布情况和数字校园的信息流做一个简要的分析。高校信息化建设进入应用集成、信息集成阶段后，数据中心成为了一个必要的信息枢纽，是高校信息资源的集散地。数字校园的信息资产分布情况如表 1所示。

表 1 数字校园信息资产分布表

信息资产	所在区域
教学、科研、人力资源、学生、财务、设备资产、校友、后勤数据	数据中心
部分管理、办公信息	职能部门
实验数据、部分科研信息	院系
图书资料	图书馆
学生学习信息、个人资料	学生宿舍区

我们进一步对数字校园的信息流进行了分析，如图 1所示。数据中心是数字校园的信息核心，与数字校园的其他部分都有信息交互，例如，与财务专网交换财务数据，与 IC卡专网交换资金、卡务、人事基本信息，而高校的师生则会在院系、教室、宿舍访问在数据中心运行的信息系统和计算资源，校职能部门的管理和服务人员除了要在办公地点访问信息系统外，还需要通过应用对信息进行管理。

因为保存的信息资产的不同和信息流的差异，数字校园不同部分所面临的安全风险是不同的，下面分别对其进行分析。

2 1 数据中心的安全风险分析

数据中心是数字校园信息资产和信息流的核心，是包括物理设备、计算机网络、系统软件、应用软件、数据库等的复杂系统，面临的安全风险是多层面的，主要包括以下 5个方面。

(1) 物理层安全风险。物理安全是信息系统安全的前提。校园数据中心物理层的安全风险主要包括：

① 地震、水灾、火灾等自然灾害和事故造成整个系统破坏；

② 电源故障造成的设备损坏以至操作系统引导失败或数据库信息丢失；

③ 数据中心设备因被盗或自身老化损坏等造成的数据丢失。

(2) 网络层安全风险。网络是信息传输的通道，校园数据中心网络层的安全风险主要包括：

① 数据中心网络与校园网络没有建立有效的防护措施，导致数据中心网络受到来自外部网络的攻击；

② 网络链路安全风险，数据在校园网传输时没有进行足够强度的加密导致数据被窃听、甚至篡改；

③ 计算机病毒的威胁，计算机病毒是威胁计算机安全的一个重大因素，现在的计算机病毒形式多样，不仅可以破坏本机数据和系统软件，还可以

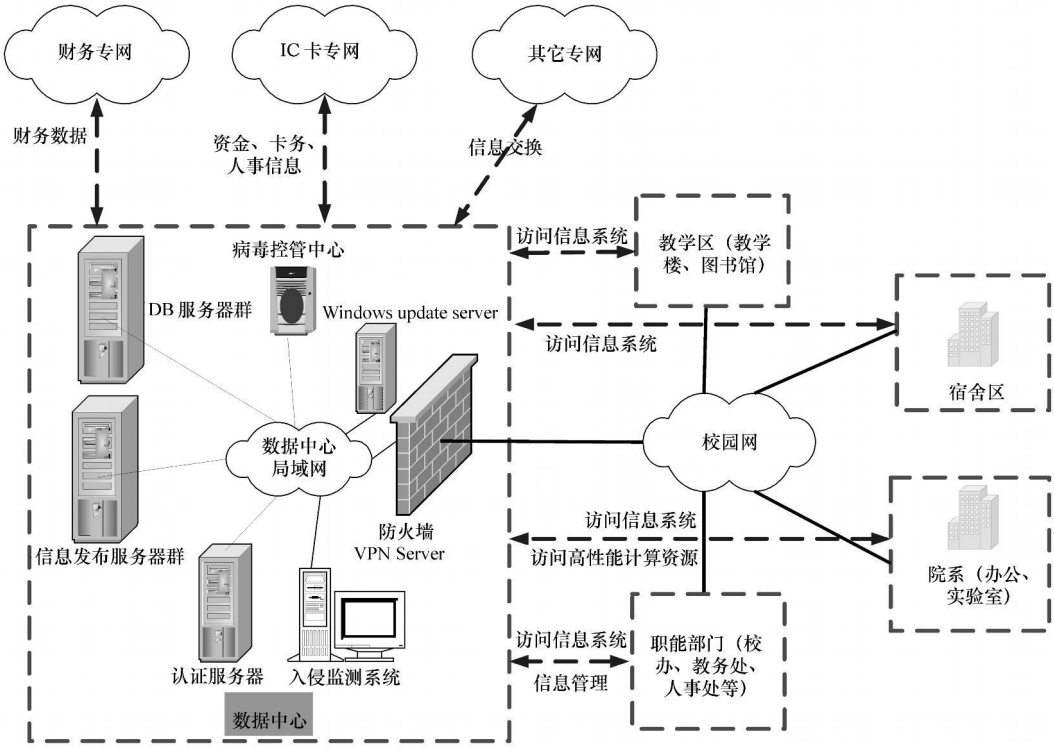

图 1 数字校园的信息流分析

通过网络进行传播，不仅可以通过后门控制被感染主机，还可以通过被感染主机发起网络攻击，进行DoS/DDoS攻击，后果是破坏范围广，需要恢复的时间长；

④ 网络设备的自身安全性也是网络安全的重要组成部分，大量路由器和交换机自身就有着众多安全漏洞。

（3）系统层安全风险。系统层安全风险指的是信息系统运行平台的安全风险，包括操作系统、系统软件等。目前的操作系统或系统软件无论是Windows还是Unix系统以及其他厂商开发的系统软件（如apache），本身都存在安全漏洞，如果没有进行合理的安全配置，如修补安全漏洞、关闭一些不常用的服务端口等，那么入侵者就有可能利用这些漏洞侵入系统。

（4）应用层安全风险。数据中心担负着数字校园和教学、科研、人事、设备等信息系统的运行工作，其业务及相关数据量庞大。目前数字校园的信息应用80%以上是Web应用，Web应用最大的优点是可以在任何地方进行操作，而不用安装任何专门的软件。信息技术从来就是一把双刃剑，Web应用的普及也为数字校园引入了更多的应用层安全风险，常见的Web应用风险包括未验证输入[3]、不完善的访问控制、不完善的认证和会话管理、跨站点脚本攻击（XSS）、缓冲区溢出、命令注入错误、错误处理机制、不安全存储、拒绝服务等。

（5）数据层安全风险。数据中心存储的数据从存储形式上来说，包括文件数据和数据库数据。数据层面的安全风险包括数据库管理系统的安全风险、缺乏统一的数据备份与容灾策略带来的数据安全风险等。

2.2 关键职能部门和院系的安全风险分析

职能部门和院系一般没有服务器，主要的信息资产都存放在办公用机上，主要面临的安全风险是因为黑客入侵、病毒破坏而造成的信息泄漏和丢失。此外，因为职能部门往往担负着信息管理的职责，因此我们可以将职能部门的工作人员的办公用计算机看作是数据中心的延伸，如果办公计算机被黑客入侵，或者被木马、病毒破坏，将直接威胁数据中心的信息安全。

2.3 教学区、宿舍区安全风险分析

教学区和宿舍区以学生的个人PC为主，主要的安全风险是因为病毒泛滥而造成的网络故障。

3 数字校园整体安全保障体系的构建

通过对应用（信息）集成阶段数字校园面临

的信息安全风险的分析，我们得出了此阶段数字校园信息安全保障体系的建设目标：针对数字校园的信息安全风险，在物理安全、网络安全、系统安全、数据安全、应用安全、终端安全等不同层次上采取可靠的安全防范措施，建立行之有效的信息安全管理制度和流程，形成一套完整的安全保障体系，实现严密、多渠道的安全控制，保证信息系统的安全稳定运行，保证数据安全，提高用户对信息系统的信赖度。

数字校园的不同部分在信息资产价值、安全风险等方面有着较大的差异，为满足各部分（包括业务系统、网络系统、用户等）各自的安全需求，我们提出了如下信息安全体系构建思路：划分安全域和建立安全域之间的联系，实施整体安全管理。

3.1 数字校园安全域

安全域是指同一系统内根据信息的性质、使用主体、安全目标和策略等元素的不同来划分的不同逻辑子网或网络，每一个逻辑区域有相同的安全保护需求，具有相同的安全访问控制和边界控制策略，区域间具有相互信任关系，而且相同的网络安全域共享同样的安全策略。通过对数字校园的信息资产和信息流的分析，我们将数字校园划分为4个安全域，分别是安全网络域、安全计算域、安全信任域和安全用户域。

（1）安全网络域：支撑数字校园的网络设备和网络拓扑，是所有安全域的承载子域。防护重点是保障网络性能和进行各子域的安全隔离与边界防护。对数字校园来说，安全网络域是指高校的校园网络。

（2）安全计算域：数字校园的核心业务服务器、数据库，是数字校园最核心的安全域。防护重点是防病毒攻击、防黑客篡改和防误操作导致数据丢失。建成校园数据中心后，高校有80%以上的信息资产集中在数据中心。数据中心集中了数字校园的硬件资源、数据资源，成为了数字校园信息流运转的中心，安全计算域在数字校园安全域划分中也是安全级别最高的域。

（3）安全信任域：需要访问安全计算域的特权客户端和维护终端，是安全计算域的信任子域。防护重点是加强审计、限制权限，严格遵守配置标准。在数字校园中，安全信任域是指分布在校内的各职能部门。

（4）安全用户域：需要访问信息系统的用户，是安全域的风险子域，重点是防病毒。包括学生宿舍、院系等。

需要说明的是，各高校可以根据自身的实际情况进行进一步的划分，例如我们将院系和学生宿舍都划入了安全用户域，但实际上院系的安全级别要高于学生宿舍，可以进一步将安全用户域拆分为两个安全子域。

上述划分的安全域之间的联系如表2和图2所示。图2清楚地显示出各安全域之间的关系。

表2 数字校园的安全域划分

安全域名称	说明	数字校园对应部分	防护重点	与其他安全域的联系
安全网络域	支撑数字校园的网络设备和网络拓扑，是所有安全域的承载子域	校园网	保障网络性能和进行各子域的安全隔离与边界防护	是所有安全域的支撑域
安全计算域	数字校园的核心业务服务器、数据库，是数字校园最核心的安全域	数据中心	防病毒攻击、防黑客篡改和防误操作导致数据丢失	为安全信任域和用户域提供信息服务、高性能计算服务，与安全信任域交换关键业务信息（如教务信息、人事信息等）
安全信任域	需要访问安全计算域的特权客户端和维护终端，是安全计算域的信任子域	职能部门	加强审计、限制权限，严格遵守配置标准	访问安全计算域的信息与计算资源，与安全计算域交换业务信息
安全用户域	需要访问信息系统的用户，是安全域的风险子域	院系、学生宿舍	防病毒	访问安全计算域的信息与计算资源

图2显示了安全计算域在数字校园安全体系中的核心地位：安全计算域（数据中心），是数字校园信息安全防范体系保障的重点，是高校信息安全投资应该重点覆盖的部分。

3.2 数字校园整体安全保障体系

在上文中我们分析了数字校园的信息资产，进行了定性的安全风险分析和安全域的划分，并讨论了安全域之间的联系。结果显示出安全计算域应是

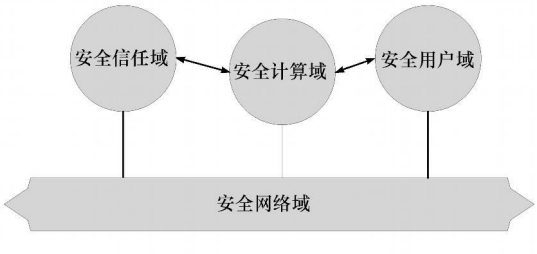

图 2 安全域联系图

数字校园信息安全体系的核心，据此构建了数字校园信息安全体系如图 3所示。

安全计算域 （一般为数据中心 ）是数字校园的核心，应建立包括物理安全、网络安全、数据安全、应用安全在内的多层面的安全技术措施。安全信任域由校关键职能部门，如校办、教务处、人事处、财务处等组成，一般没有服务器，主要的信息资产都存放在办公用机上，但需要运行 C/S的客户端程序，在信息系统还不够完善的时候，还需要

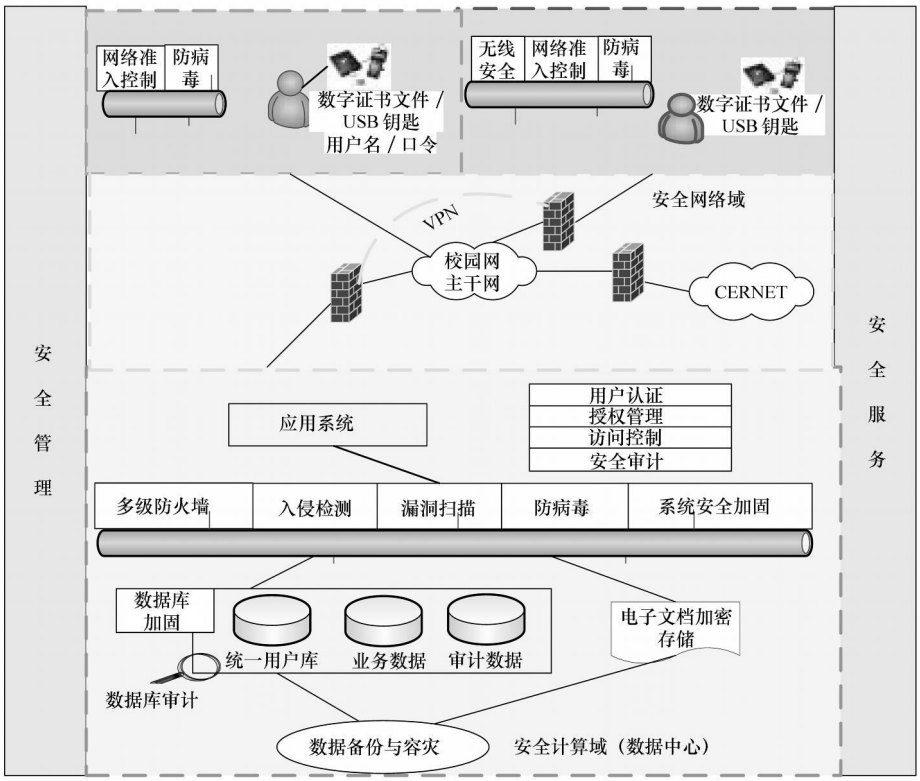

图 3 数字校园信息安全保障体系

直接访问计算域的数据库等资源。因此安全信任域需要考虑两个方面的安全问题，一是终端安全，二是信任域与计算域之间的通信链路的安全，解决方法是建立 VPN通道，防止数据被非法窃听。安全网络域是数字校园的承载体，由网络线路和网络设备组成。需要采用的安全措施包括采用门禁等物理措施保障通信线路和网络设备的物理安全，保证数据传输安全性、完整性、可获性。对网络设备进行安全配置，并在校园网出口架设防火墙等确保校园网和教育网之间的通信安全，使其能最大限度地提供可靠、通畅、便捷的网络通道。安全用户域由学生宿舍、院系网络组成，应建立网络准入控制、网络防病毒、 W indow s补丁自动升级等安全措施保证此域的安全。信息安全管理和服务是安全体系的重要组成部分。实践一再告诉人们仅有安全技术防范，而无严格的安全管理体系相配套，是难以保障网络系统安全的。必须制订一系列安全管理制度，对安全技术和安全设施进行管理。实现安全管理必须遵循可操作、全局性、动态性、管理与技术的有机结合、责权分明、分权制约及安全管理的制度化等原则。数字校园最终用户的安全意识是信息系统是否安全的决定因素，因此对用户的安全培训和安全服务是整个安全体系中重要的、不可或缺的一部分。特别是在目前病毒泛滥的大环境下，必需通过定期培训、及时发放病毒警告通知、敦促大家打补丁等方法，增强所有教职员工的安全意识、提高他

们的安全技能。

4 清华大学的实践

清华大学在教育信息化建设方面经过近 20年的艰苦努力，取得了较大的进展，尤其在国家启动“211工程”之后，取得了一批可喜成果。学校教学、科研、管理等工作的正常运行越来越依赖于网络信息平台，因此，如何建立安全、稳定、高效的信息系统运行环境成为重要的课题。在清华大学“十五”211工程经费的支持下，对本文第三部分的数字校园信息安全体系构建方法进行了实践。

将清华大学数字校园划分为 4个安全域：数据中心是安全级别最高的安全计算域；职能部门属于安全信任域；校园网为数字校园的承载体，属于安全网络域；学生宿舍、院系属于安全用户域。

（1）在安全计算域（数据中心）建立了网络、系统、数据、应用各层面的安全防护措施，建立了清华大学异地数据容灾备份体系，保证了数字校园核心信息资产和信息应用的安全。

（2）在安全网络域（校园网）部署用户入网身份认证系统、计算机补丁管理和安全漏洞扫描系统、分布式入侵检测系统、分布式的网络准入控制系统、集中管理的病毒防护系统、网络不良信息监测和内容审计系统，基本实现了校园网的“可信、可知、可控和可查”。

（3）安全信任域（职能部门）是安全计算域的外延，通过在二者之间架设 VPN通道，保证了数据传输安全，通过防火墙、桌面安全措施的部署保证了安全信任域内的信息安全。

（4）在安全管理与服务方面，我们一方面严抓数据中心内部的安全管理制度与流程，进行安全角色划分。另一方面不断探索如何为职能部门与全校师生提供更好的安全服务。我们在 2003年底就开始在一些职能部门进行了成功的试点工作，效果显著。目前数据中心向职能部门提供网络安全方案规划、实施、安全培训、安全咨询、安全报告等多项安全服务。

5 结束语

信息安全是一个多层次、多因素、综合的动态过程，是一场“道”与“魔”的永恒斗争。随着信息技术的发展与高校信息化建设的深入，会不断暴露新的问题，推动我们对安全体系进行完善。当前阶段，信息安全的主要问题已经从网络安全问题、系统安全问题转向应用安全和数据安全问题。据调查，目前超过 90%的 Web应用存在某种类型的安全漏洞，有超过 75%的攻击是通过 HTTP/S协议进行的[4]，而且实际发生的 Web攻击数量有明显的上升趋势。在此形式下，我们必须积极进行应用安全和数据安全的研究，以有效保障数字校园关键应用和关键业务数据的安全。

参考文献（References）：

[1] 蒋东兴，陈怀楚. 大学资源计划理论探讨与实践 [J]. 教育信息化，2005（9）：4-7.

[2] OWASP. OWASP Top 10 Project [EB/OL]. [2007]. http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

[3] Watchfire公司. Watchfire white paper, Web Application Security: Automated Scanning or Manual [Z]. 2006.

[4] CNCERT. 2006年上半年网络安全报告 [EB/OL]. [2007-01-31]. http://www.cert.org.cn/articles/docs/common/20070131163191.shtml.

[5] 吴海燕，蒋东兴. 入侵防御系统研究 [J]. 计算机工程与设计，2007，28（24）：5844-5846.

[6] 吴海燕，戚丽. 校园数据中心高可用运行环境建设研究 [J]. 中国教育信息化，2007（5）：16-18.

[7] 蒋东兴，陈怀楚，沈培华，等. 清华大学数字校园建设发展与规划 [J]. 实验技术与管理，2002，19（增1）：14-20.

◦名词解释◦

因特网≠互联网（Internet≠internet）

因特网是通过产业、教育、政府和科研部门的自治网络将用户连接起来的世界范围的网络。因特网采用网际协议（IP）进行网络互联和路由选择，采用传输控制协议（TCP）实现端对端控制，其主要业务包括电子邮件、文件传输协议（FTP）、远程登录、万维网和电子公告板等。

互联网指两个或多个相互连接的局域网组成的互连网，即它们位于同一座建筑物里和属于同一个机构所有，是互联网络（internetwork）的同义词。

《实验技术与管理》编辑部 编录