Intranet Security

# Intranet 的安全性

〔美〕John Vacca 著
史宗海 等译

**在安全受到破坏和灾难发生前阻止它们!**

- 最新Intranet的安全性问题
- 实现安全性的实用策略
- 灾难恢复程序

電子工業出版社
Publishing House of Electronics Industry
URL:http://www.phei.com.cn

Intranet Security

# Intranet的安全性

〔美〕 John Vacca 著

史宗海 等译

電子工業出版社

Publishing House of Electronics Industry

## 内 容 提 要

人类已步入信息社会，网络安全是当前所面临的极其严峻的问题之一。从加密学的角度，本书详细分析了Intranet系统及其安全管理的各种工具和措施；系统地剖析了对Intranet安全构成威胁的各个方面；讨论了Intranet上如何防灾和灾后如何恢复以及Intranet安全性开发、实现和管理的高级策略；探讨了未来Intranet面临的威胁及其防止方案。本书对于所有关心Intranet安全性的各类组织和专业人员不失为一本好书。




**图书在版编目（CIP）数据**

Intranet的安全性/（美）维卡（Vacca，J.）著；史宗海等译. - 北京：电子工业出版社，2000.1
书名原文：Intranet Security
ISBN 7-5053-5332-2

Ⅰ. Ⅰ… Ⅱ. ①维… ②史… Ⅲ.局部网络，Intranet-网络安全 Ⅳ. TP393.18

中国版本图书馆CIP数据核字（1999）第74362号

JS479/23

书　　名：**Intranet的安全性**
著 作 者：〔美〕John Vacca
译　　者：史宗海　等
责任编辑：吕向英
印 刷 者：北京天竺颖华印刷厂
装 订 者：三河金马印装有限公司
出版发行：电子工业出版社　URL:http://www.phei.com.cn
　　北京市海淀区万寿路173信箱　邮编：100036
　　北京市海淀区翠微东里甲2号　邮编：100036
经　　销：各地新华书店
开　　本：787×1092 1/16　印张：19.875　字数：500 千字
版　　次：2000年1月第1版　2000年1月第1次印刷
书　　号：ISBN 7-5053-5332-2
　　TP·2659
定　　价：32.00元

版权贸易合同登记号　图字：01-1999-0935

# 致　谢

如果没有各方人士直接或间接的鼎力相助，本书不可能出版发行，趁此机会在这里感谢所有对本书作出过贡献的朋友。

首先，要对提供了方便的组织和个人致谢。他们允许使用其信息和研究资料，这对编著本书非常必要。还有一些人士和组织，他们的工作为后来者指明了道路。

要感谢我的代理，他的帮助和支持贯穿本计划的始终。

要感谢执行编辑Jenifer Niles和董事长David Pallai，在我编写过程中他们进行了耐心的帮助，并通过他们超常和艰苦的工作使得本书得以出版。要特别感谢技术编辑和好友Michael Erbschloe，他保证了本书的技术准确性。最后要感谢Eric Wiznowski在CD-ROM方面的工作、从事QEP设计的Reuben Kantor、从事桌面服务和出版的Doug Porter，他们进行了布局和页面设计、Kathy Mills进行了富有经验的编辑，以及所有Charles River Media的工作人员，他们为本书的出版作出了有益的贡献。

要多谢Dennis Pleticha，在网络方面专门知识和经验，如同他的友谊一样，不可或缺。

要特别感谢我的妻子，Bee Vacca，她的恩爱和鼓励，贯穿了整个编写本书的全过程。

最后要特别感谢Greg Robertson，没有他的帮助，本书难以出版。

祝诸位青春常驻，真理永存。

# 序　言

科学技术发展的历史，很久以来就与军事领域结下了不解之缘。第二次世界大战期间，美军需要快速计算弹道发射表的技术。当时，作为PX计划，军方与Pennsylvania大学Moore电机系签订合同，建造完成这一计算任务的机器。其结果是第一台电子数字计算机ENIAC（Electronic Numerical Integrator and Computer）的诞生，描述计算机发展史的任一著作，都会讲到ENIAC。对这一军事问题所投入的资金和人力孕育并开创了计算机工业。

战时，同样重要的问题是保密，这里蕴含了另一科技历史。二战期间，人们使用密码的艺术，表现出了加密学方面的高超水平。密码已经使用了若干世纪，在本世纪中叶其技巧和自动化程度，达到了新的水平。二战中，一个精选的天才小组，包括技术专家、音乐家、数学家和国际象棋大师，共同努力，破译了轴心国的密码。在这些天才中有数学家Alan Turing，他后来成为早期计算机科学的奠基人。Turing和位于英国Bletchley Park智能中心的加密专家在破译德国Enigma机器密码方面，取得了很大成绩，德国人就是用这种机器产生的密码与盟军作战。需要提及的是：人们的这些贡献，使战争缩短了不止一年，成千上万的生命因而免遭涂炭。

因而，诞生了电子加密学——使用机器保护编码信息。虽然这些工作者没有被公开誉为英雄，但政府已注意到了这一领域的巨大潜力。

当计算机市场蒸蒸日上，ENIAC的后代繁衍滋长，加密学领域却仍然保持相对的冷淡状态。为何大量的资金投入机器的制作，以改善数据处理和发送速率，而在安全方面则投入较少？幸而，美国政府做了一些秘密的技术，如雷达和全球定位系统，将保密技术广泛地推向了市场。经过半个世纪的历程，加密学正走上自己独立发展的道路。

数据安全并不限于保护军事人员的记录不丢失给德国人或俄国人。公司也有责任保护其雇员的记录不被公开。对PC制造商的竞争对手来说，每月芯片的订单是至关重要的。设计文件、财务报告与合同草稿都是个人和组织要保密的大量信息。

具有讽刺意义的是对我们信息安全造成最大威胁的是来自我们的军事盟友。出于经济利益，一些外国政府竟容忍工业间谍活动。日本、法国和以色列的工业无不得益于从桌上计算机的苦心搜集以及从公司计算机网络上汲取资料。

在谴责外来者之前，须知最常见的威胁是来自内部。心怀不满的工作者和近期辞退的雇员，往往就是盗窃和破坏公司关键信息的人。某些雇员往往能得到公司中未成文的保密和敏感信息。他们给人的印象似乎有权得到任何信息。以一个投资银行为例。如果没有严格的数据安全制度，一个零售代理商能在银行举行的初始信息发布会上，获取内部信息，从而危及银行安全规则。

除去这些危险之外，处理数据愈快，累积的数量愈大，每年发往各处的数据也愈多。我们可能在旅馆房间阅读电子邮件，邀请顾客到我们的FTP站点。我们给商业伙伴的信息可能要发往不同的国家，这些国家的政府可能对版权法和知识产权保护持有不同看法。面对这些风险，我们怎能继续冒失地投资技术，而对数据的安全性不闻不问呢？

我们对于数据安全的重要性的认识还远远不够。我们生活在互相连结的网络世界之中，对数据安全的淡漠是不能容忍的，必须严肃的对待。此外，存在于数字王国中的数据也必须是安全的。

数字数据是脆弱的。网络的网格还将继续伸延，要在全世界创建更加紧密的数据通道。这样，数据将更加互相混合。读者的信息包可能就排列在竞争对手的后面。Internet和Intranet的界限将会模糊。在某些情况下，来自经济方面的压力将迫使公司依赖公用网络，而逻辑安全就是唯一的选择了。

在数据安全方面的投资，需对数据从不同的角度进行考虑。对软件和硬件的购买比较简单，即这些软件和硬件必须存在，否则生意就不成立。工厂不会生产，订单不会拿到，钞票也不会付出。对安全方面投资的回报则并不明显。只要系统在运行，好像什么事情也没发生。

如果公司发现了黑客闯入系统，那是幸运的事，因为，如果不是黑客的粗心，系统的主人永远也不会知晓。首席信息主管（CIO）的真正恶梦是遇到不动声色的专业黑客，他可以随意窃取和修改信息。具有讽刺意味的是一个完善的维护良好的系统往往能帮助黑客更方便地窃取大量信息。要免遭此祸，就必须实行安全制度。严格的安全监督和管理是网络运行良好的首要问题。

个人或组织首先要确定自己数据的价值。竞争对手要花多少代价才能得到它。可以用一辆新车设计的价值、一本走俏的电影剧本的价值、或一种创新的制造工艺的价值为例，进行设想它们在新产品或新观念中所占的比重如何，以及这些新产品在市场上的价格为多少。相比之下，电子邮件的安全包或链路加密器的价格则微不足道。

或者，价值可用对信誉的损害程度来考虑。一个属于幸福100（Fortune 100）的公司不会愿意让媒体掌握它的很多刺激性的问题。一个专门诊所，不会愿意把它的知名病人的名字散播出去。即便敢冒风险的某些国会议员，也宁愿使用保密电话。数据和信息应该用市场价值和信誉的价值来衡量，并以此确定数据安全的价值。

从二战电码破译者的工作开始，到现在数据安全的方法已取得实质性的进步。直到70年代初期，在美国政府机构之外，有关数据安全技术，很少见诸文字。自70年代中期，加密学的研究和相关工程技术开始出现在IBM的T、J、Watson研究中心和Stanford大学。当时，对这方面成就的了解，仍局限于研究实验室的人员和大学数学系。直到廿年后的现在，这些加密学的基础技术，才用于硬件和软件产品的数据安全，并推向市场。

加密学是现代数据安全的核心。事实上，在数字王国中，加密学是保护数据安全的唯一手段。对数据直接进行安全保护应是默认的。对数据实施安全保护和管理应是逻辑的，而非物理的。

加密学是建立在复杂的数字和数论的基础之上，应用在很多领域，从蜂窝电话到Web浏览器。加密学推迟应用到数据安全，是对这一技术的仔细验证。廿年来，加密学家和数学家反复对加密码及其应用进行了袭击。能经受袭击并保留到现在的加密码构成了安全数据的基础。很少有其它的技术在推广之前经受了这样严格的考验。

加密技术的基础虽很复杂，但其安全特性都十分直觉。保护数据可归结为若干方法。保密性和数据完整（data integrity）可能是最显著的特性。对编码或密码的典型应用是将消息打乱，使没有密钥的人无法读取。现在用于打乱位（不是字母）的算法，同样可用于视频

信息流和文本消息。数据完整与保密相关，可防止某些人窜改消息。在一笔电子资金传送中一两位的差异，可能意味着从1,000美元到1,000,000美元不同的付款额。

与数据保密和不受触动同样重要的事情是控制哪些人可以看到它（或听到它），或者一个电子合同的领受人应该知道谁可以签字。如果要将现在由人工完成的过程自动化，那就应该有一个与人工签字等同的数字办法或光学身份证（ID），加密技术通过认证（authentication）的过程来完成这一任务，一般是进行数字签字。如果执行正确，认证就可合法地连接，并提供一个事件或交易的证明。很多政府现已立法承认数字签字的有效性。

正确实行数字安全的第一步是承认数据易损性。数据易损可用定时测试的技术来克服。对一个组织的数据的价值进行评估，可以计算出投资的回报。有了这一估计，就可执行内置安全的处理。

阅读本书，是进行Intranet安全工作的起点。数字安全技术和应用所涵盖的领域广泛。Vacca首先详细地描述了加密学和数据安全的基础。关于应用的详情，如Web浏览器、安全电子邮件、电子商务系统和Java进行了仔细讨论。

本书不仅提供了背景材料，有数章讨论了实际的技术应用。不管读者用UNIX或Windows，是一个小公司还是属Fortune 500的大公司，本书的知识都适用于读者的安全系统。除技术细节外，其它章节还讲述了风险分析和法律问题。书中还给出了对一个组织评估其数据价值的知识。

不要介意标题中的“Intranet”，对读者信息的威胁不仅来自Internet。保护数据安全的最好起点是从企业内部开始，即Intranet。请记住，如果数据在内部都不安全，当它暴露于外部（不管是否自愿）时又怎能是安全的？不管朋友、顾客，或被黑客发现，存储中的数据都应是安全的。一个公司应像保护其物理资产那样保护其数据。

另外，本书讲述了破坏后的恢复工作，这是一个经常被忽视的领域。数据是脆弱的，极易受损于电子脉冲和分布的磁场。比起人为因素，自然对数据更具破坏力。对于以计算机为基础的工作来说，保护数据和破坏后的恢复计划是至关重要的。如果遭受破坏后的数据被抹掉了，那么再好的数据安全性也就没有用了。

明白了数据安全的重要性，就需要具备现代信息安全专业技巧。安全性不再是在伪装掩盖下的匕首。我们现在可以仔细地探讨这一姗姗来迟的技术，不仅解决长期存在的问题，也可在计算机上创造新的令人振奋的工作方法。对首席信息官、系统管理员、网络主管来说“Intranet的安全性”是一本非常有价值的书。

Tim Matthews, RSA Data Security, Inc.
Redwood City, CA

# 简　介

Intranet的安全性可定义如下：拒绝未经授权的物理的或电子的闯入、操作或袭击，并保证Intranet和所传信息端到端的完整性。它需要能抗拒各种类型的破坏，包括电子袭击、物理袭击、人为错误和自然灾害。

当政府、专门机构和一般公众日益依赖信息服务，以支持国家的经济活动和生活方式时，提供和传送信息服务的Intranet的可靠性和安全性也日愈重要。这些Intranet必须能抗拒天灾而不失效，在各种威胁和不利条件下也不会丧失服务能力。它必须能监视Intranet的健康运行，并在出现失效的情况下能迅速恢复运行。本书提供对一个企业资源能力的评估，以实现有效的Intranet安全策略。书中提供的合理评估，可用来测试Intranet所面临的威胁，估价其在威胁下的易损性、验证当前所用对抗措施的缺点、并研究公司应如何克服未来的问题。

本书涵盖的范围并不限于上述问题，它的很大的注意力放在主要的自然灾害，如地震、California的森林火灾、美国中西部和西北部的洪水、袭击东北部破历史记录的冬季暴风雪。与灾害恢复相关的许多待解决的问题也是本书的重点。恐怖主义者的袭击事件日益增多，如对世界贸易中心的袭击，以及最近在Oklahoma城、伦敦和英格兰的炸弹破坏事件，所有这些，本书予以同等重视，看来需对灾害开出有效的药方。

一些最平常的事件，如电网停电、水管破裂、人为错误和计算机病毒，也足以给工作带来混乱。这些事件当然不具戏剧性，但当它使用户的信息技术Intranet被迫中断时，它就不再是微不足道的“灾害”了。

并不在乎灾害有多大，但在考虑防灾计划和服务时，对灾害可能引发的事件和后果应予充分重视。本书还提供了灾害恢复计划的有关信息，告诉读者如何降低风险、减少资金投入、保证关键业务的不中断、强制检查跟踪以及实行性价比解决方案。本书还帮助读者建立灾害恢复程序，这会适合读者的工作需要。此外本书还提供了详细说明，以帮助用户实现灾害恢复计划的具体步骤，为灾害恢复组开设训练课程、编制测试和评估程序以及完成计划的定期维护。

## 本书的读者对象

考虑Intranet的安全性，本书主要对象为IT经理、系统管理员、政府计算机安全官员、Intranet管理员、和WWW开发者。关于灾害恢复，本书的对象为高级经理、应急规划者、运行经理、数据通信经理、防灾和恢复组员以及与防灾应急规划和恢复功能有关的管理者。总之，本书对所有关心Intranet安全性的各类组织和人员都很实用。

## 本书的结构

本书由六部分组成，包括CD-ROM中的附录、有关Intranet安全性术语和缩写词的汇编。

## 第一部分 系统和Intranet的安全管理

第一部分讨论了系统的人为方面和Intranet安全的实施和管理，以及由Intranet安全管理员所使用的有效的Intranet安全工具和方法，用以保护Intranet的信息资源。

第1章 “Intranet安全的趋势”，说明了当前安全性政策的概貌，包括了事故应急和有关计算机安全性方面的法律问题。此外本章还通过和闯入者实际斗争的经验，描述了当前检测入闯者方法的趋势。

第2章 “Intranet安全的基础”，包括有需要评估的风险和安全政策，根据这一政策对雇员的培训，和授与访问权限。本章还包含了对防火墙和防毒软件的简要讨论（这两个题目将在本书的后一部分予以更多的关注），还讲述了审查跟踪软件和简化记录过程的优点。

第3章 “设计和实现Intranet的安全政策”包括真正安全性的必要条件。在硬件和软件上如果没有有计划地实行安全措施，会留下让黑客进入的漏洞。围绕这一问题，一定要建立完整的、紧密结合的政策，从Intranet的一端贯彻到另一端。

第4章 “验证Intranet的安全管理”，讨论一般的概念，如一个企业是否需要Intranet，对硬件和软件进行安全保护的需要，以及域名服务（Domain Name Service）。此外本章还接触到了Intranet可能具有的各种设备问题，以及出现安全漏洞的可能，安全管理员要经常防止出现漏洞。

第5章 “系统和Intranet的安全管理：人为因素”，包括对系统的实现和Intranet安全得到管理层的支持；从十个简要问题中发现优秀的系统管理员；雇主应寻求什么样的系统管理员；系统管理员的职业道德。

## 第二部分 验明对Intranet安全的威胁

本书第二部分验证在Web上Intranet安全的发展方向：客户机和服务器；步骤和工具；近期在多数机构内系统和Intranet的实现。

第6章 “Intranet安全方面的步骤和工具”，研究了Intranet安全的分析综合工具；移动计算的安全问题；接收电子邮件的认证；包括闯入者的案例研究；方法和预防；电子入侵的探查和预防；黑客冒险的案例分析；使用革新的Intranet安全审计和监视技术；以及使用一次性口令系统和其它认证技术。

第7章 “实用的Intranet安全方法和工具”，研究了商业化的FTP服务，xswatch（这是一个用于系统记录检查结果的样本），还研究了配置和获得的教训。

第8章 “更有用的Intranet安全方法和工具”，讲述了为用户提供Intranet安全产品选集；实现一个高度可用的数据仓库；配置和学习课程以及简化系统管理的技术。

第9章 “Web上的Intranet安全性：客户机、服务器及其它”，包括了用于客户机和服务器上当前Intranet安全问题和技术。本章还让读者了解到运行WWW服务器（并考虑到Java和JavaScript）的安全实质。

第10章 “鉴别计算机病毒”，初步讨论利用防病毒扫描程序鉴别病毒，或者相反，一个防病毒扫描器是否会认定一个本无病毒的文件受到了感染。本章还阐明了病毒检查虚报警的损失、计算机病毒的命名和分类。

第11章　“用于Intranet的防病毒软件”，包括了Intranet管理员所研究的问题。最大的挑战是负责保护Intranet不感染病毒和其它破坏性编码，大部分病毒是来自Internet。一般的解密扫描程序是有用的，但也有失效的情况。本章还给出了一个实例，使用帮助桌面方法，来帮助雇员消除病毒。

## 第三部分　防灾与恢复

第三部分包括有防灾计划和恢复服务，在LAN环境下的防灾，灾害恢复计划的要求和灾害恢复管理。

第12章　“LAN/Intranet环境下的防灾”，讨论了灾害恢复服务的供应商，如何防灾和灾害恢复产品。本章还讨论了在不同设备上的安全问题。

## 第四部分　Intranet安全的开发、实现和管理

这一部分讨论了高级Intranet安全的选择和策略，及其开发、实现和管理。这会改变现在和将来机构的工作方式。

第13章　“保护Intranet工作站的安全”，根据一般类型的工作站，讨论了各种安全措施。本章还充分讨论了入侵Intranet的问题：多数公司和组织都不愿家丑外扬。

第14章　“保护Intranet关系数据库的安全”，这是一个重要的课题，因为Intranet上的很多信息都保存在数据库。本章的部分内容讨论了防火墙，因为这是保护数据库的第一道防线。

第15章　“移动和远程站点访问Intranet的安全管理”，这是因为日益频繁地从远程访问Intranet和从家用或膝上计算机访问Intranet，增加了新的安全问题。本章还讨论了远程访问的可用选择。

第16章　“成功地建造一个Intranet安全基础”，建立基础的概念是：安全性的首要目标是保护信息。基于此，安全官员必须严格掌握特别访问授权。本章还说明保护Intranet的最好方法是侵入它，试试看。安全官员还应注意到是谁企图越过公司的防线。每一公司都应有一成文的安全应急计划。

## 第五部分　结果与未来的方向

这一部分给出了实现各种Intranet安全政策的结果，这些安全政策已在前几章讨论过。还讨论了对Intranet安全的威胁以及未来如何防止威胁的解决方案。

第17章　“盗窃秘密”，讨论了包括计算机和Intranet在内的各方面的间谍。受害者在遭受计算机间谍的打击后，往往能极大地改善其安全性。侵犯知识产权也是一个实际问题。工业界的职业道德如何？在这里，对计算机应用领域给予了充分考虑。

第18章　“2000年Intranet安全的危机”，讨论了当2000年来临时，能影响到大小计算机站点的Intranet安全问题。在1999年12月31日午夜之后，全世界的计算机会成为黑客和其它无耻之徒的攻击对象。他们会利用在2000年1月1日时计算机因分不清是2000年还是1900年而失效的机会，将时间倒回一个世纪。（美国）国会已指出了这一问题的严重性，如果商界和政府继续忽视这一问题，例行的商业运行和联邦政府为美国公众提供的服务将会遭受破坏。

第19章 “Intranet安全的发展方向和WWW”，本章讨论了认证和权标的未来技术。此外，加密和防火墙还需继续存在，这两种安全措施不会消失。

第20章 “综合、结论和建议”，讨论了当前的全球信息高速公路（GII, Global Information Infrastructure）如何满足未来的设备，以及Intranet内部的安全性和可靠性要求。本章对GII的安全性和易损性作了评估，高度重视了Intranet内部的安全性，并说明当前技术中固有的多样性以及所关心的可能领域。本章还评论了Intranet的安全问题，这能帮助GII的发展，并建议改变到现行的和推荐的美国出口政策，以便在世界范围允许个人和公司保护其电子信息、出版物和通信。本章还回顾了已建立的Intranet安全性的原则，据此可以判断美国的政策。还帮助建议政策的修改以符合这些原则。本章通过对Intranet安全性和灾害恢复有关问题的讨论，得出了必要的结论，以及将来如何避免这类问题的发生。

在本书之末，附有与安全相关术语的汇编。

## 第六部分 附录

在CD-ROM上有九个附录。这些资源都与Intranet的安全性相关。附录A给出了与Intranet安全性和灾害恢复相关的供应商名单。附录B给出了与灾害恢复相关的Web站点名单。附录C讨论了应急的方向。附录D是一个通向成功Intranet安全性的道路图。附录E描述了Cisco's FTP站点的历史和第一个FTP系统的问题——高级用户系统产品分配服务器（ACSPDS, Advanced Customer Systems Product Distribution Server）——及其最新的FTP系统，Cisco信息在线电子软件分配（CIOESD, Cisco Information Online Electronic Software Distribution）。附录F讨论了对UNIX安全性的威胁以及如何应用。附录G则将重点放在如何为公司电子工作室提供Intranet安全，在客户机/服务器的特点方面，工作室希望其位置和规模不受限制。附录H讨论了安全产品发展对政府和商业的影响。附录I讨论了Intranet安全性的法律问题。

### 副 栏

我们使用如下的副栏，以强调有关的信息，例如，详细地讨论某个项目，或帮助读者了解术语和缩写词的难点，以充分理解这一主题。副栏可补充每一章的主题。如果读者不能逐页阅读，可跳过副栏。如果读者要快速浏览有趣的信息，可仅读副栏。

## 惯例

本书使用若干惯例，以帮助查找内容和重要的事实、提示和注意事项。

引人注目的图标可提醒读者有重要信息和有关问题。

**注释：** 强调有关Intranet安全问题的特别有趣之点。

**提示：** 给读者以忠告提示——为保持安全应做之事。

**警告：** 告诉读者注意步骤，以防地雷。

**危险：** 指出对Intranet真正的或潜在的入侵。

**机密：** 提醒用户不为人知的但有潜在价值的有关Intranet安全的信息。

## 实情!

当地球上的三个人首次连通Web，随着Web的发展，连接到它上面的Intranet也在三倍地增长——这主要是由于它的普及和在声像信息方面日益增长的应用。

末日的预言已提出警告，由于按指数增长的Intranet用户连到这一全球的网上之网，Internet已达到了危险的容量水平。预言家们惧怕有一天Internet会崩溃！这一趋势使新的和当前的用户感到恐惧。

Internet可能最终崩溃的真正原因并不是其潜在的增长，而是提供适当的安全能力以保护接到它上面的Intranet。真正使用户感到不安的是企业、政府和教育机构没有能力提供安全，以保护其Intranet免遭灾害。

读完本书，作者希望关心Intranet安全和灾害恢复的用户能制订策略验证威胁。为了一个安全的 Intranet，发展并实现灾害恢复计划，不仅为自己，也为二十一世纪的下一代用户。

John R.Vacca
Jvacca @ hti.net
http://www.commerce.com/ctw

# 目　录

# 第一部分 系统和INTRANET的安全管理

询问任何一位系统和Intranet安全管理员或IT（信息技术）经理：从现在到21世纪的前期，最大的技术趋势是什么？得到的回答会很简单：Intranet安全。Intranet的安全性成了最热门的话题。自从有了电子信箱，通信技术的安全保护也提到了公司的议事日程。

要满足用户对Intranet应用的需要，公司首先必须花费时间和精力，改变他们对网络安全的想法。IT经理要从目前认为资源和平台组成基础结构的想法，改变为更开阔的观点。他们应该集中力量研制并配备一个企业Intranet安全管理基础结构。这种基础结构应包括网络、系统、数据库和应用程序的Intranet安全管理，所有这些应有商务过程的观点。

商务过程的观点还要变为实际行动。系统和Intranet安全管理员需要工具进行管理和保护IT资源。本部分讨论系统和Intranet安全管理的人为因素。还提供了简单的对商务过程观点有用的Intranet安全工具和方法，Intranet的安全管理员用这些工具和方法保护Intranet的信息资源。

## 第1章 Intranet安全的趋势

**内容摘要**

- Intranet的保护策略
- Intranet完整性
- 威胁、风险分析和安全政策
- 法律问题

公司的计算机网络已不新鲜。无论如何，当在公司范围建立起计算机系统时，商务活动会从Internet的多媒体WWW（World Wide Web）得到越来越多的信息。跨越长距接到PC的服务器，如图1.1所示，已移到Intranet。

Intranet是专用网络，与Web的结构相对应。它使用了标准的Internet语言TCP/IP（Transmission Control Protocol/Internet Protocol），这一技术为不同的计算机系统（如Macintosh，Windows或UNIX工作站）在一个组织内互相通信的另一方法。它改善了公司通信，公司雇员在PC机上使用Web浏览器就可访问数据库，数据库所在的服务器可以位于公司网络的任何地点。同一技术还可使用户在文档和其它项目上进行合作。