 [摘 要] 本文对企业电子商务技术风险管理问题进行了研究，从网络安全、数据存取安全和支付安全3个方面分析了电子商务中存在的技术风险，并在此基础上提出了降低电子商务技术风险的相关安全策略及措施。 [关键词] 电子商务；技术风险；风险管理 电子商务（Electronic Commerce，EC）是指通过网络（尤其是Internet）所进行的买卖交易以及相关服务或其他的组织管理活动。交易的安全性能否得到保障是电子商务的核心问题。近几年来，我国的电子商务发展较快，但各种风险也日趋突出。一般来说，电子商务中常见的风险可分为经济风险、管理风险、制度风险、技术风险和信息风险。IT技术是实现电子商务的基础，分析研究其技术风险是保障电子商务安全的重要研究课题。 为了促进电子商务的健康发展，研究电子商务中可能存在的风险及相应的控制策略是十分必要的。本文分析了电子商务中存在的技术风险及其产生的原因，并在此基础上提出了降低电子商务技术风险的相关安全策略及措施。 1. 电子商务中存在的技术风险 由于网络的开放性、共享性和动态性，使得任何人都可以自由地接入Internet，导致以Internet为主要平台的电子商务的发展面临严峻的安全问题。其主要技术风险包括： 1.1 网络环境风险 网络服务器常遭受到黑客的袭击，个别网络中的信息系统受到攻击后无法恢复正常运行；网络软件常常被人篡改或破坏；网络中存储或传递的数据常常被未经授权者篡改、增删、复制或使用。 1.2

数据存取风险 由于数据存取不当所造成的风险。这种风险主要来自于企业内部。一是未经授权的人员进入系统的数据库修改、删除数据；二是企业工作人员操作失误，受其错误数据的影响而带来的风险，其结果必然是使企业效益受到损失，或者是使顾客利益受到损失。 1.3 网上支付风险 网上支付一直被认为是制约中国电子商务发展的最大瓶颈，许多企业和个人担心交易的安全性而不愿使用网上支付。 2.电子商务风险管理 电子商务安全的风险管理（Risk Management）是对电子商务系统的安全风险进行识别、衡量、分析，并在此基础上尽可能地以最低的成本和代价实现尽可能大的安全保障的科学管理方法。其本质就是防患于未然：事前加以消减和控制，事后积极响应和处理，为响应和处理所做的准备就是制订应急计划。 了解了电子商务存在的风险之后，需要对这些风险进行管理和控制，具体包括风险识别、风险分析、风险应对和风险监控4个过程。 2.1 风险识别 对电子商务系统的安全而言，风险识别的目标主要是对电子商务系统的网络环境风险、数据存取风险和网上支付风险进行识别。识别风险的方法有很多，主要有：试验数据和结果、专家调查法、事件树分析法。电子商务风险识别最常用的一种方法就是收集各种曾经发生过的电子商务攻击事件（不仅局限于本企业），经过分析提取出若干特征，将其存储到“ 风险 ”库，作为识别潜在风险的参考。 2.2 风险分析 风险分析的目的是确定每种风险对企业影响的大小，一般是对已经识别出来的电子商务风险进行量化估计。这里量化的概念主要指风险影响指标，风险概率以及风险值。技术安全是电子商务实现的基础，其重要性不言而喻，因此在该项目规划、计划阶段就应充

分考虑。 2.3 风险应对（风险控制） 根据风险性质和企业对风险的承受能力制订相应的防范计划，即风险应对。确定风险的应对策略后，就可编制风险应对计划。电子商务的技术风险控制主要是针对网络环境风险、数据存取风险和网上支付风险制订风险应对策略，从硬件、软件两方面加强IT基础设施建设。 2.4 风险监控 制定规划，实施保护措施，在保护措施实施的每一个阶段都要进行监控和跟踪。风险贯穿于电子商务项目的整个生命周期中，因而风险管理是个动态的、连续的过程。因此制订了风险防范计划后，还需要时刻监督风险的发展与变化情况。 3. 电子商务技术风险控制 针对电子商务中潜在的各类技术风险，笔者提出利用以下技术手段建立一套完整的风险控制体系，将电子商务的风险减少到最小。 3.1 网络安全技术 网络安全是电子商务安全的基础，一个完整的电子商务应该建立在安全的网络基础之上。网络安全技术涉及面较广，主要包括操作系统安全、防火墙技术、虚拟专用网技术（VPN）、漏洞识别与检测技术。 3.1.1 操作系统安全 操作系统的安全机制主要有：过滤保护、安全检测保护以及隔离保护。 （1） 过滤保护分析所有针对受保护对象的访问，过滤恶意攻击以及可能带来不安全因素的非法访问。 （2） 安全检测保护对所有用户的操作进行分析，阻止那些超越权限的用户操作以及可能给操作系统带来不安全因素的用户操作。 （3） 离保护在支持多进程和多线程的操作系统中，必须保证同时运行的多个进程和线程之间是相互隔离的，即各个进程和线程分别调用不同的系统资源，且每一个进程和线程都无法判断是否还有其他的进程或线程在同时运行。一般的隔离保护措施有以下4种：①物理隔离 不同的进

程和线程调用的系统资源在物理上是隔离的；②暂时隔离 在特殊需要的时间段内，对某一个或某些进程或线程实施隔离，该时间段结束后解除隔离；③软件隔离 在软件层面上对各个进程的访问权限实行控制和限制，以达到隔离的效果；④加密隔离 采用加密算法对相应的对象进行加密。百考试题编辑整理 3.1.2 防火墙技术 防火墙是将专用网络与公共网络隔离开来的网络节点，由硬件和软件组成，其主要功能是通过建立网络通信的过滤机制，控制和鉴别出入站点的各种访问，进而有效地提高交易的安全性。目前的防火墙技术主要包括两种类型，第一类是包过滤技术，其运作方式是监视通过它的数据流，根据防火墙管理事先制定的系统安全政策，选择性地决定是否让这些数据通行；第二类是代理网关技术，其运作方式是所有要向服务器索取的数据，都通过代理服务器来索取。目前，防火墙技术的最新发展趋势是分布式和智能化防火墙技术。分布式防火墙是嵌入到操作系统内核中，对所有的信息流进行过滤与限制；智能化防火墙利用了统计、记忆、概率和决策等智能技术，对网络执行访问控制。 3.1.3 VPN 虚拟专用网（VPN）是依靠Internet服务提供商（ISP）和其他网络服务提供商（NSP），在公用网络中建立专用数据通信网络的技术。VPN实现技术主要有：隧道技术、虚电路技术和基于MPLS（Multi-Protocol Label Switching，多协议标签交换协议）技术。基于MPLS技术的VPN通过改善和加速数据包处理提高VPN效率，集隧道技术和路由技术优点于一身，组网具有极好的灵活性和扩展性。用户只需一条线路接入VPN网，便可以实现任何节点之间的直接通信。不过基于MPLS技术的VPN技术本身还有一个成熟的过程，但是它代

表了VPN的发展方向。（3）基于生物特征的认证方式 以人体唯一的、可靠的、稳定的生物特征（如指纹、虹膜、人脸、掌纹、耳郭、声音）为依据，利用图像处理与模式识别技术进行认证。基于密码的认证技术存在密码难以记忆，容易被黑客破译的缺点。而基于生物特征的认证方式具有很好的安全性、可靠性和有效性，正逐渐成为一种新的身份认证方式，特别是近几年来，全球生物识别技术的飞速发展为生物认证提供了广泛的技术支持。其中，基于人脸识别的认证技术已经成为当前的研究热点，主要方法有基于几何特征的人脸识别方法与基于统计的人脸识别方法，并且已有产品投入网络安全领域，如True Face Cyber Watch. 3.4 数据库安全机制 数据库安全最重要的一点就是确保只授权给有资格的用户访问数据库的权限，同时令所有未被授权的人员无法接近数据，这主要通过数据库系统的存取控制机制实现。存取控制机制主要包括两部分：（1）定义用户权限，并将用户权限登记到数据字典中。（2）合法权限检查，每当用户发出存取数据库的操作请求后，DBMS查找数据字典，根据安全规则进行合法权限检查。若用户的操作请求超出了定义的权限，系统将拒绝执行此操作。 一旦数据遭到破坏，就必须采取补救措施。建立严格的数据备份与恢复管理机制是保障数据库系统安全的有效手段。数据备份可以分为2个层次：硬件级和软件级。硬件级的备份是指用冗余的硬件来保证系统的连续运行。软件级的备份指的是将系统数据保存到其他介质上，当出现错误时可以将系统恢复到备份时的状态，这种方法可以完全防止逻辑损坏。 3.5 第三方认证CA 与采用其他交易方式相比，采用电子商务交易模式的各方还有更多的风险，这

些在电子商务中所特有的风险有：卖方在网站上对产品进行不实宣传，欺诈行为的风险；买方发出恶意订单的风险；交易一方对电子合同否认的风险；交易信息传送风险，如信息被窃、被修改等风险。这些风险的存在，需要设立第三方认证技术中心，为在网上交易各方交易资料的传递进行加密、验证和对交易过程进行监察。CA认证技术中心是一个确保信任的权威实体，它的主要职责是颁发证书，验证用户身份的真实性。任何相信CA的人，按照第三方信任原则，也都应该相信持有证明的用户。CA发放的证书有SSL和SET两种。SSL（Secure Sockets Layer） 安全协议又叫“ 安全套接层协议 ”，主要用于提高应用程序之间数据的安全系数，一般服务于银行对企业或企业对企业的电子商务。SET协议（Secure Electronic Transaction） 位于应用层，用来保证互联网上银行卡支付交易安全性，一般服务于持卡消费、网上购物等。 4. 结 论 电子商务的开展以信息技术为基础，如何解决电子商务中存在的安全问题已成为一个迫在眉睫的课题。电子商务风险是不可能完全消除的，因为它是与电子商务共生的，是电子商务的必然产物，但是，可以将风险限制在影响最小的范围之内。只有了解风险，才能规避风险。本文从安全风险管理的角度出发，分析了电子商务中可能存在的技术风险，论述了这些风险的控制策略，希望对企业开展电子商务活动起到一定的积极作用。 主要参考文献 [1] 阮新新。电子商务技术风险管理的探讨[J].经济问题探索， 2004，（4）：96-97. [2] Thomas Finne. Information Systems Risk Management： Key Concepts and Business Process [J]. Computer and Security，2000，（19）：234-242. [3] 刘伟江，王勇。电子商务风险及控制

策略[J].东北师范大学学报：哲学社会科学版，2005，（11）。[4] 朱亚殊，朱荆州。实现操作系统安全的几种策略[J].计算机与数字工程，2005，33（1）：49-52. [5] 张欣。浅析防火墙技术的发展[J].徐州工程学院学报，2005，（20）：77-79.F8F8" 