文章编号:1000-582X(2010)02-0036-06

数字化企业的信息安全体系及实施方案

阎春平[1],刘　飞[1],郭　风[2]
(1.重庆大学 机械传动国家重点实验室,重庆 400044;
2.中国嘉陵工业股份有限公司(集团),重庆 400032)

摘　要:分析了数字化企业的总体框架结构、安全需求,构建了数字化企业完整的信息安全体系,包括物理安全、网络安全、支撑层系统安全、应用层系统安全、数据及资料安全;针对数字化企业数据及资料等企业内部信息安全问题,提出了一套包括身份鉴别、设备集中控制、文档权限管理、文档加密、安全审计等功能系统的综合解决方案;基于所构建的信息安全体系,提出了一种典型数字化企业的信息安全实施方案。

关键词:数字化企业;信息安全;网络安全;安全体系
中图分类号:TP393;TH166　　文献标志码:A

Information security system of digital enterprise and its implementation scheme

YAN Chun-ping[1], *LIU Fei*[1], *GUO Feng*[2]
(1. State Key Laboratory of Mechanical Transmission, Chongqing University, Chongqing 400044, P. R. China;
2. China Jialing Industry Co. Ltd. (Group), Chongqing 400032, P. R. China)

Abstract: The general framework and security demands of digital enterprises are analyzed. The information security system is constructed, which includes physical security, network security, support layer system security, application layer system security, data and documents security. Aiming at the security of internal information security such as data and documents, a comprehensive solution including identity authentication, centralized equipments control, document security management, document encryption, and security audit are put forward. Based on the above information security system, an implementation scheme for typical digital enterprise is proposed.

Key words: digital enterprise; information security; network security; security system

数字化企业是现代企业运行的一种新模式。它将信息技术、现代管理技术和制造技术相结合,并应用到企业产品生命周期全过程和企业运行管理的各个环节,实现产品设计制造、企业管理、生产控制过程以及制造装备的数字化和集成化,提升企业产品开发能力、经营管理水平和生产制造能力,从而提高企业综合竞争能力[1-3]。随着企业信息化建设的深入,企业对信息化建设的要求越来越高,建设全面集成的数字化企业成为企业信息化工作的目标[4]。

在企业信息化工作的开展中,信息安全问题是必须要考虑的首要问题之一[5-8],数字化企业是企业信息化的高级阶段,其建设同样也将面临着信息安全问题,而且更为复杂。研究数字化企业的信息安全问题,具有很大的现实意义。

收稿日期:2009-11-30
基金项目:国家自然科学基金资助项目(50975299);"十一五"国家科技支撑计划资助项目(2006BAF01A27)
作者简介:阎春平(1973-),男,重庆大学副教授,博士,研究方向为网络化制造与制造系统工程、企业信息化等,(Tel)13983229681;(E-mail)ycp@cqu.edu.cn。

国内外学者对企业信息安全问题进行了若干研究。文献[9-11]对网络化制造系统和协同制造系统中的安全问题进行了研究；文献[12]对基于应用服务提供商模式网络化制造的安全技术进行了研究；文献[13]对供应链协同系统的安全体系进行了设计与实现；文献[14]研究了一种基于采用公共密钥体系(Public Key Infrastructure，PKI)加密技术和签名技术的信息网络传输方案；文献[15]对网络环境下口令认证机制进行了研究。目前，企业信息安全研究主要集中在对单一系统、单一技术的研究方面，缺乏对数字化企业整体安全问题的系统考虑，难以满足数字化企业的信息安全需求。本文从数字化企业的总体框架结构、安全需求出发，构建数字化企业完整的信息安全体系，最后给出了一种典型数字化企业的信息安全实施方案。

1　数字化企业的信息安全需求

1.1　数字化企业的总体框架

图 1 是数字化企业的总体框架结构，包括数字化企业基础支撑系统、企业外部经营和协作层网络化系统、企业内部设计和管理层信息化系统、企业生产设备层网络化运行系统等 4 个层面。

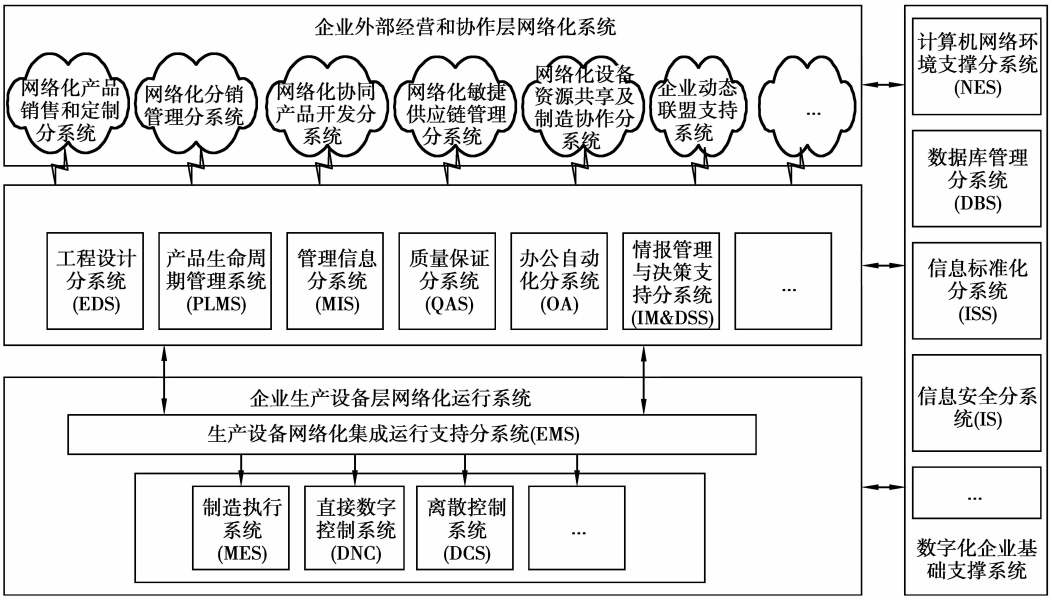

图 1　数字化企业总体框架结构

基础支撑系统是数字化企业的系统支撑层，包括计算机网络环境分系统(NES)、数据库管理分系统(DBS)、信息标准化分系统(ISS)和信息安全分系统(IS)等支撑分系统。

企业外部经营和协作层的网络化系统是数字化企业基于 Internet 的功能系统层，包括网络化产品销售和定制、网络化分销管理、网络化协同产品开发、网络化敏捷供应链管理、网络化设备资源共享及制造协作等实现企业与外部环境之间信息交互和业务协同的各功能分系统。

企业内部设计和管理层信息化系统是数字化企业基于 Intranet(企业内联网)的功能系统层，包括工程设计分系统(EDS)、管理信息分系统(MIS)、质量保证分系统(QAS)、办公自动化分系统(OA)、情报管理和决策支持分系统(IM&DSS)等企业内部信息化功能分系统。

企业生产设备层网络化运行系统是数字化企业基于车间现场总线网络或车间局域网络的底层生产设备集成运行系统层，包括基于现场总线的数控机床网络化集成生产系统和基于网络化制造多功能信息交互终端的制造装备网络化集成优化运行系统。

1.2　数字化企业的信息安全需求特点

由数字化企业的总体框架结构可以看出，相比于一般的信息化企业，数字化企业信息安全需求具有下列几个特点：

(1)信息系统覆盖面广。不仅仅涉及到企业内部设计和管理层信息化系统，而且向下延伸到了企业生产设备网络化运行系统，向上延伸到企业外部经营和协作层系统。数字化企业的这一特点使得信息安全工作覆盖面广，不仅仅要解决覆盖地域范围广、涉及人员和环节多的面向企业外部的经营和协作层系统的安全问题，也要解决企业生产现场诸如加工图纸被盗、数控程序被盗、加工状态参数信息泄露等信息安全问题。

(2)信息系统之间高度的集成化。这将带来两方面的安全难题,一方面由于系统和系统之间信息交互比较多,扩大了单一应用系统可接触的人员数及其地域范围,增加了信息安全工作的难度。另一方面,企业外部经营和协作层系统与企业内部应用系统之间存在着大量的信息交互,这将使得企业外部人员可能通过信息通道攻击企业内部应用系统及网络,带来新的安全问题。

(3)数字化企业信息化程度高。一旦出现安全问题,将可能会影响整个企业的运行,使企业处于瘫痪状态。同时由于对信息的依赖程度高,使得安全问题的"水桶效应"更加明显,单点的安全问题,可能会对企业带来很大的危害。数字化企业在解决信息安全问题时应该整体规划和系统考虑。

2 数字化企业的信息安全体系

针对数字化企业的总体框架和安全需求特点,遵循安全性、可行性、效率性、可承担性的设计原则,数字化企业的信息安全体系可从物理安全、网络安全、支撑层系统安全、应用层系统安全、数据及资料安全几方面进行设计,构建了如图2所示的数字化企业信息安全模型。

在数字化企业信息安全模型中,通过采取合理的安全策略、建立专门的安全组织机构、完善安全制度来建立保障数字化企业信息安全的长效机制;通过加强定期的安全评估,发现信息系统中潜在的安全漏洞,以便及时弥补和修复;通过安全审计工作,及时发现潜在的安全事件,以便及时进行处理,同时对安全违规行为起到威慑作用,减少安全违规事件。

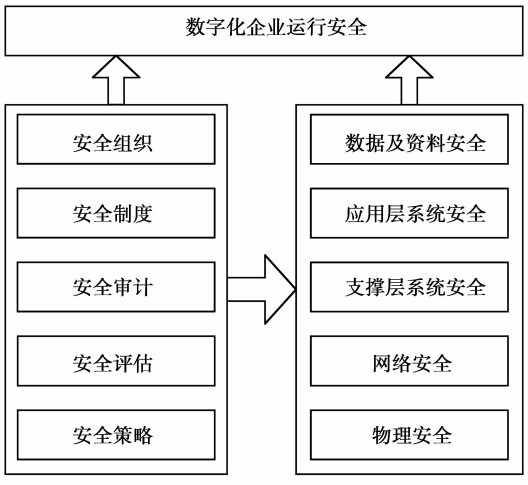

图2 数字化企业信息安全模型

数字化企业基础支撑系统中的数据库管理分系统(DBS)的安全主要通过支撑层系统安全技术解决,计算机网络环境分系统(NES)的安全主要通过物理层、网络层和支撑层系统安全技术解决。企业外部经营和协作层网络化系统、企业内部设计和管理层信息化系统、企业生产设备层网络化运行系统主要通过网络层和应用层的安全技术解决。

2.1 物理安全

物理安全的目的是保证数据库服务器、应用服务器、计算机系统、网络交换机、通讯链路以及其他物理设备的安全,在具体设计中要考虑门禁、防盗、防火、防尘、防静电、防磁、电源系统等,使得物理设备免受自然灾害、人为破坏和搭线攻击,提供切实可行的数据备份策略,制定网络数据中心的安全访问制度,防止非法进入网络数据中心。物理安全措施主要体现在机房环境要求、设备物理防范和介质安全3个方面,主要有:①建立不同安全区域标志,实施不同区域隔离;②建立出入审查和登记管理制度,保证出入得到明确授权,并且出入人员持有授权书,授权书中要明确出入的目的、操作的对象、操作步骤和操作的结果证明;③对出入标志安全的活动进行不间断实时监视记录;④建立出入安全检查制度,保证出入人员没有携带危及计算机信息系统安全的设施或物品。采用双机热备技术保证重点服务器的不间断运行,采用磁盘阵列技术对重要数据进行实时备份,采用磁带机对重要数据进行灾难备份。企业的核心交换机采用备份机制[7]。

2.2 网络安全

2.2.1 网络结构安全

通过层次设计和分区设计实现网络之间的访问控制,网络结构设计时需要对网络地址资源分配、VLAN划分、路由协议选择、QoS配置等方面进行合理规划。

2.2.2 网络安全

对网络中重要网段加以保护。通过多级防火墙隔离控制内外网络、内网不同区域的访问;通过扫描软件对重要网段内的所有提供网络服务的设备进行漏洞扫描和修补,在条件具备时扫描范围应该扩大到网络的所有设备;在企业Internet网络的入口处部署基于网络的入侵检测系统动态保护整个网络;通过网络操作系统(如Cisco IOS)的及时升级和网络设备的高可靠性认证来实现网络设备自身的安全。

2.2.3 网络传输安全

采用虚拟专用网技术(Virtual Private Network, VPN)解决外部经营和协作层系统中信息传输的安全性问题,利用不可靠的公用互联网作为信息传输媒介,通过附加的安全隧道、用户认证和访问控制等技术实现与专用网络相类似的安全性能,实现对重要信息的安全传输。

2.3 支撑层系统安全

支撑层系统安全主要包括数据库管理系统和操作系统安全。数据库的安全保护，一方面需要在数据库系统的设计、实现、使用和管理等各个阶段都遵循一套完整的数据库系统安全策略；另一方面需要选择数据库评估扫描软件，通过专业的数据库评估扫描软件检测数据库系统存在的安全漏洞并进行修补，保护关键应用系统的数据。当前的各类操作系统（包括 Windows、UNIX、LINUX 等）都存在着众多的系统漏洞，而黑客通常以对系统的攻击作为对整个网络攻击的第一步。加强操作系统安全主要可采取三方面的措施，一是通过基于网络的扫描软件对重要主机系统进行定期漏洞扫描评估，发现漏洞后对系统及时进行修补；二是通过在重要的主机上（如应用服务器、WEB 服务器、数据库服务器等）安装基于主机的实时入侵检测系统防范各类攻击；三是建立基于网络的防病毒系统。

2.4 应用层系统安全

应用层系统安全一方面需要对应用系统进行检测和修补，在应用系统的权限管理中加强安全性的考虑，建立有效的身份验证（ authentication）与授权（ authorization）机制。另外一方面在数据的传输过程中要做好数据加密工作，保证数据传递的正确性和完整性。

2.5 数据及资料安全

数据及资料安全主要是指数字化企业中一些脱离于数据库管理系统和应用系统保护的数据及文档资料的安全[16]，如设计和制造过程中产生和使用的各类图纸、工艺等设计文件和数据文件、企业的商业资料等。造成企业内部敏感数据及资料泄漏的因素和途径是多方面的，其中人为的因素有：

（1）由于员工信息安全意识淡薄所造成的信息无意泄漏；

（2）员工主动或受竞争对手的指派非法获取；

（3）人员流动造成信息泄漏；

（4）不法分子出于各种目的盗窃硬件设备，如笔记本电脑、PC 机等。

信息泄漏的物理渠道主要有：

（1）输出设备：包括软盘、USB 移动设备、串并口、红外线设备等；

（2）非法登录计算机主机导致的泄密。

无论信息泄露的表现形式如何，这类安全违规事件追究到最后大部分都是由企业内部人员所造成的。因此，解决来自企业内部的信息安全问题应以人为核心。另一方面，信息泄露事件都是通过网络、计算机及软件工具进行的，由于计算机信息资料的大存储量、易复制、隐蔽性强并不留痕迹，加上计算机使用上的开放性，使公司内部员工可以轻易地复制和拥有属于公司的技术与商业秘密资料。

这类安全风险主要有以下特征：

（1）使用者易于假冒他人权利非法获取信息；

（2）通过共享行为交换信息易于被非法窃取信息，网络服务器易被攻击；

（3）内部员工有机会获取整体信息；

（4）内部员工容易将非法获取的资料通过存储介质带出公司；

（5）员工的行为难以进行审计和追踪。

笔者认为数字化企业内部信息安全解决方案应着重关注解决以下问题：

（1）员工身份的确认，使其对行为负完全责任；

（2）阻止员工非法获取信息，特别是全局的和整体的信息；

（3）阻止员工将信息非法复制转移出公司；

（4）对员工的非法信息获取渠道进行监控。

要解决以上的企业内部信息安全问题，一方面要加强技术手段，另外一方面要完善企业关于信息安全问题的相关管理制度，加强对员工安全意识的培训和安全行为的管理。

在技术实现上，提出了如图 3 所示的企业内部数据及资料安全方案。其中身份鉴别通过 SKey（硬件 USB 钥匙）结合口令加强身份认证对操作系统进行完善，同时为每一个内部员工分配一个固定唯一的 IP 地址，并在网络安全设备中将其与 MAC 地址捆绑起来，则该计算机所产生的所有行为视为该员工的行为。访问控制采用防火墙（FireWall）对服务器的网络访问进行控制，同时对重要服务器安装专门的访问控制软件，对登陆操作系统进行身份识别和审计。设备集中控制采用基于网络的设备集中控制系统对受限机器的对外复制渠道进行控制。中心控制台接管所有受限机器的系统资源，对受限机器的终端输出设备（USB、软盘、串并口、红外接口等）、网络文件共享进行监管。通过控制外设通道，切断员工将商业、技术秘密资料带出企业的途径，通过对共享文件的监控，防止员工通过网络共享方式将商业、技术秘密传递给联网的其他员工。安全审计是在每个安全系统中实施审计模块，同时建立基于网络的集中审计系统，对员工行为进行审计和追踪。信息加密采用基于 intranet 和角色的分布式权限控制系统。将信息资料根据密级及阅知范围分为不同等级，并用相应的密钥进行加密，同时在系统中设置角色，为每个角色按规定赋予阅读、创建不同等级信息资料的权限，对员工根据工作需要赋予不同的角色，这样员工就只能访问授权的信息资料，可有效防止员工越权限非法获取资料。

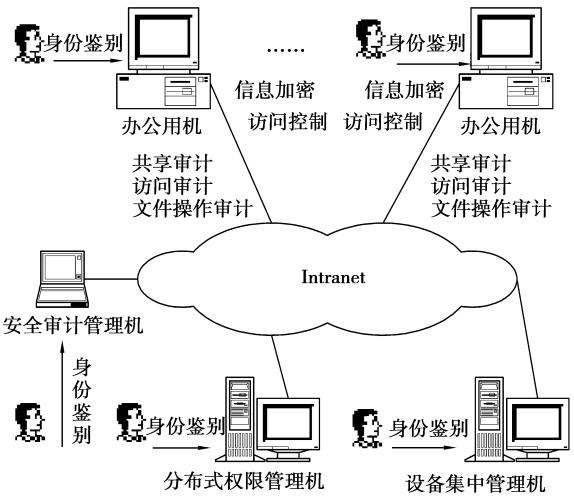

图3 企业内部数据及资料安全实现方案

3 一种典型数字化企业的信息安全实施方案

图4是一典型数字化企业的信息安全实施方案。通过双机热备、数据灾难备份、磁盘阵列等方式,减少由于硬件安全问题带来的损失;通过VPN加密信道保障企业分支机构、合作伙伴与总部之间信息传输的安全性,通过布置防火墙系统、划分VLAN,加强了网络层的安全性,通过在入口防火墙上布置入侵检测系统动态保护网络;通过布置访问控制系统、基于主机的入侵检测系统,进一步保障关键服务器的安全。

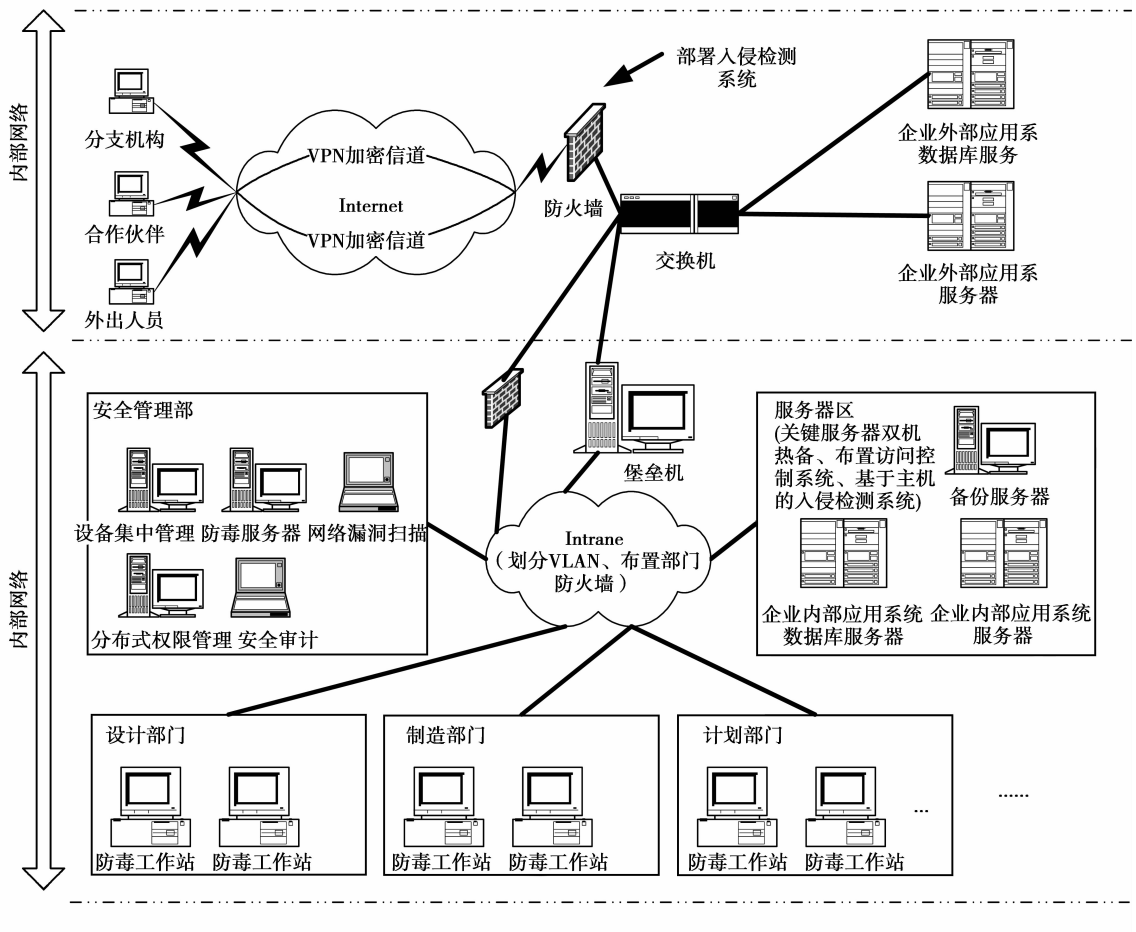

图4 典型数字化企业信息安全实施方案

企业外部的经营和协作层网络化系统覆盖地域范围广、涉及人员和环节多,潜在的安全风险大,而其与企业内部信息化系统之间又存在着大量的数据交换,为了解决这一问题,部署了安全堡垒机,堡垒机有双网卡,分别连接内外网络,外部网络通过堡垒机上布置的交换程序实现对内部关键服务器中数据的访问,在内外网络之间的防火墙中,切断了外部网络与内部关键服务器之间的路由通道,从而加强了企业内部关键服务器的安全。

4 结 语

由于信息系统覆盖面更广、集成度更高,解决数

字化企业面临的信息安全问题显得更为棘手。文中根据数字化企业的安全需求特点，系统地构建了数字化企业信息安全体系，并将多种安全方案纳入到该体系中；针对数字化企业数据及资料安全问题，提出了一套综合解决方案，该方案实现了身份鉴别、设备集中控制、文档权限管理、文档加密、安全审计，大大提高了企业内部数据及资料的安全性；提出了一种典型数字化企业的信息安全实施方案，通过设置堡垒机，在不影响内外部信息交互的情况下，保障了内部业务应用系统关键服务器的安全。

文中提出的数字化企业信息安全体系及具体解决方案已经成功应用到重庆某集团公司的信息安全项目中，有效解决了该公司信息化建设推进过程中信息安全问题，并使该公司一次性通过了军工保密资格现场认证。

参考文献：

[1] 阎春平，何小兵，刘飞，等. 数字化企业的一种描述模型及总体框架[J]. 重庆大学学报，2008，31(4)：382-386.
YAN CHUN-PING，HE XIAO-BIN，LIU FEI，et al. A descriptive model and general framework for digital enterprises [J]. Journal of Chongqing University，2008，31(4)：382-386.

[2] 潘星，王君，刘鲁. 数字化制造企业中知识管理集成框架及关键技术研究[J]. 计算机集成制造系统，2004(S1)：90-95.
PAN XING，WANG JUN，LIU LU. Research on framework of knowledge management integration and key technologies in digital manufacturing enterprise [J]. Computer Integrated Manufacturing Systems，2004(S1)：90-95.

[3] 邓崧，白庆华. 企业信息化对企业效益和内部机制的影响[J]. 同济大学学报：自然科学版，2005，33(5)：701-705.
DENG SONG，BAI QING-HUA. Study on effect s of enterprise informatization to its performance and inner mechanism[J]. Journal of Tongji University：Natural Science，2005，33(5)：701 -705.

[4] MAROPOULOS P G，ROGERS B C，CHAPMAN P et al. A novel digital enterprise technology framework for the distributed development and validation of complex products [J]. CIRP Annals-Manufacturing Technology，2003，52(1)：389-392.

[5] VON SOLMS B，VON SOLMS R. The ten deadly sins of information security management[J]. Computers and Security，2004，23(5)：371-376.

[6] SIPONEN M，WILLISON R. Information security management standards：Problems and solutions [J]. Information & Management，2009，46(5)：267-270.

[7] KARYDA M，KIOUNTOUZIS E，KOKOLAKIS S. Information systems security policies：a contextual perspective[J]. Computers and Security，2005，24(3)：246-260.

[8] VON SOLMS B，VON SOLMS R. From information security to business security [J]，Computers and Security，2005，24(4)：271-273.

[9] Cisco Systems Inc. Cisco intelligent networked manufacturing [EB/OL]. http://www.cisco.com/web/strategy/docs/manufacturing_inm_overview.pdf，2004-01-01.

[10] 董红召，刘冬旭，陈宁，等. 分形网络协同制造系统的信息安全策略[J]. 计算机集成制造系统-CIMS，2004，10(F12)：166-172]
DONG HONG-ZHAO，LIU DONG-XU，CHEN NING，et al. Fractal-agent based information security policies of web-based collaborative manufacturing system [J]. Computer Integrated Manufacturing Systems，2004，10(F12)：166-172.

[11] 段文峰，孙永国，段铁群，等. 网络化制造系统的信息安全模型研究[J]. 机械工程师，2006(1)：60-62.
DUAN WEN-FENG，SUN YONG-GUO，DUAN TIE-QUN，et，al. Study of Information Security Technology Based on the Network Manufacturing System[J]. Mechanical Engineer，2006(1)：60-62.

[12] 徐立云，李爱平. 基于应用服务提供商模式网络化制造的安全技术研究[J]. 计算机集成制造系统，2006，12(11)：1881-1885.
XU LI-YUN，LI AI-PING. Security technology of networked manufacturing based on ASP mode [J]. Computer Integrated Manufacturing Systems，2006，12(11)：1881-1886.

[13] 宋伟，刘卫宁，孙棣华. 供应链协同系统的安全体系的设计与实现[J]. 计算机集成制造系统，2006，12(2)：292-296.
SONG WEI，LIU WEI-NING，SUN DI-HUA. Security system design & its implementation for collaborative supply chain [J]. Computer Integrated Manufacturing Systems，2006，12(2)：292-296.

[14] 黄蓓，黄杰. 网络制造的信息安全策略[J]. 信息与控制，2002，31(3)：260-263.
HUANG BEI，HUANG JIE. A strategy of information security of network manufacturing[J]. Information and Control，2002，31(3)：260-263.

[15] SHIMIZU A，HORIOKA T，INAGA KI H. A password authentication method for contents communication on the Internet[J]. IEICE Transactions Communication，1998，E81- B(8)：1666-1673.

[16] SKLOVOS N，SOUROS P. Economic models and approaches in information security for computer networks [J]. International Journal of Network Security，2006，2 (1)：243-256.

（编辑　张小强）