[全面·系统·实用]

本书全方位、立体化地对企业及个人在电子办公过程中可能发生或潜藏的办公安全问题及解决途径，做了独到的分析和阐释，有理论、有实践、有分析、有前瞻，是一本不可多得的，对电子办公安全方面极具指导意义的工具书。

电子办公安全手册

贺荣芳 主编

办公安全必备全书

DIANZIBANGONG ANQUANSHOUCE

石油工业出版社

[全面·系统·实用]

本书全方位、立体化地对企业及个人在电子办公过程中可能发生或潜藏的办公安全问题及解决途径，做了独到的分析和阐释，有理论、有实践、有分析、有前瞻，是一本不可多得的，对电子办公安全方面极具指导意义的工具书。

电子办公安全手册

贺荣芳 主编

办公安全必备全书

DIANZIBANGONG ANQUANSHOUCE

石油工业出版社

内 容 提 要

本书对电子办公安全进行了全方位的讲述，包括计算机硬件和软件的安全，数据存取和传输过程中的安全。介绍了如何对计算机进行加密管理，电脑病毒的防治及防火墙的设置等。

本书可供企事业办公人员使用。

图书在版编目(CIP)数据

电子办公安全手册 / 贺荣芳主编.
北京：石油工业出版社，2006.6
ISBN 7-5021-5508-2
Ⅰ.电…
Ⅱ.贺…
Ⅲ.电子计算机-安全技术-技术手册
Ⅳ.TP309-62
中国版本图书馆 CIP 数据核字(2006)第 039036 号

出版发行：石油工业出版社
（北京安定门外安华里 2 区 1 号　100011）
网　　址：www.petropub.cn
总　　机：（010）64262233　　发行部：（010）64210392
经　　销：全国新华书店
印　　刷：石油工业出版社印刷厂

2006 年 6 月第 1 版　2006 年 6 月第 1 次印刷
787×1092 毫米　开本：1/16　印张：24.25
字数：458 千字　印数：1—1700 册

定价：56.00 元
（如出现印装质量问题，我社发行部负责调换）

编委会名单

主编：贺荣芳

编委：孙先锋　陈安家　沈　钢
田景惠　苏志良　李悦谦
段彦修　刘福顺　肖宗伟
王喜亮　霍　健　谢　茂
李光华　姜新生　王长江
李鸿学　张恩怀　吴红峰
党　军　刘俊山　王录震

序

伴随着计算机网络的飞速发展，电子化办公已成为企业及个人日常办公活动的主要形式，是其他传统办公手段不可比拟和取代的。也正是在这种前提条件下，由电子办公所引起的各种网络安全威胁也在不断出现，给个人、单位和社会造成了巨大的损失。由此，电子办公安全管理已引起了各界越来越多的关注。

电子办公安全防范体系不是仅仅依靠使用几种技术先进的安全设备就可以实现的，更重要的是正确合理地进行网络结构的设计、规划和组织，制定严密完善的安全技术规范、管理制度及防范措施，配备高水平的有高度工作责任心的安全技术人才队伍，并对电子办公用户加强网络安全知识教育，从而提高全员电子办公安全意识。

电子办公安全防范体系是先进技术与严格管理的有机结合。先进的技术和设备为电子办公的安全提供了知识和物质保证，严格的管理用规章制度和操作规程来加以约束。随着网络自动化应用的不断推广和深化，电子办公安全问题也将越来越严峻，只有充分利用先进的安全技术和有效的安全管理手段，坚持技术保障和管理措施两手同时抓，才能建立起一套行之有效的电子办公安全防护体系，从而保证企业及个人电子办公设施的各种运用系统安全运行，使电子办公真正成为企业发展和个人事业进步的推进器。

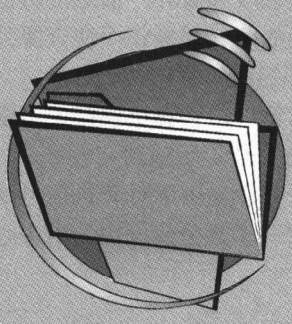
实践需要理论来做先导。目前，在电子办公安全防范方面，我国企业虽然已有所重视，但尚处于研究和探索阶段，有关这方面的专著还很少见。正是基于这种思考，本书作者从电子办公安全的概念、电子办公安全的重要性、电子办公安全的紧迫性和严峻性、电子办公安全的策略、电子办公安全设置等方面，全方位、立体化、通俗易懂地对企业及个人在电子办公过程中可能发生或潜藏的办公安全问题及解决途径，做了独

到的分析和阐释，有理论、有实践、有分析、有前瞻，可以说是一本不可多得的对电子办公安全方面极具指导意义的工具书。

当然，作者及参与本书写作的同志由于时间仓促，难免在相关理论论述和经验探讨方面出现不足之处，诚请各位专家及广大读者予以赐教！同时，也对给予这本书特别关注的领导、专家、学者深表谢意！

目　录

第一章
电子办公安全概述



第一节　电子办公安全的概念

伴随着全球信息化的蓬勃发展和深入推进，计算机网络、信息、电子办公等安全问题显得越来越突出、越来越重要、越来越紧迫，世界强国纷纷抢占网络信息、电子办公安全战略制高点。各国面临的网络信息、电子办公安全共性问题在我国信息化、电子办公发展进程中日益凸现。

网络安全是指利用网络管理、控制或用技术措施保障一个网络环境里的信息数据的保密性、完整性和可用性。具体地说，网络安全要确保计算机网络信息系统在存储、处理、传输信息数据的保密性、完整性和可用性，确保对授权合法用户的服务和限制非授权用户的服务。

网络安全包括两方面的内容，即网络的系统安全和网络的信息安全。系统安全包括系统的软件、硬件和固件的安全性，包括计算机网络信息系统的CPU操作系统、存储器、路由器等的安全；而信息安全包括信息数据的存储、处理、传输的安全，包括信息的保密性、完整性和可用性。信息保密性的目的是为了防止非授权者获取、破坏信息系统中的秘密信息；信息完整性是解决信息的精确、有效，防止信息数据被篡改和破坏；信息可用性是保证网络资源在需要时即可使用，不会因为系统的故障或误操作而使资源丢失或不能被使用，还包括具有某些不正常情况下系统的继续运行能力。

电子办公安全是指与计算机、计算机网络使用密切相关的办公领域中信息状态、信息技术体系及办公安全不受威胁与侵害。

在电子办公中，其安全实质是由于计算机信息系统作为载体和工具而引发的安全问题，它已成为当前电子办公建设中的重中之重，引起国内外政府、企业的高度重视。

第二节　电子办公安全的目的

电子办公安全就是要“保障计算机及其相关的和配套的设备、设施(网络)的安全，保障其运行环境的安全，保障信息安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行”。从这一角度看，电子办公环境下，办公安全的目的主要体现在计算机信息系统的安全，大致包括:

（1）实体安全。实体安全是指计算机设备、设施(含网络)以及其他媒体免遭自然或人为破坏。

（2）数据安全。数据安全是指防止信息被故意的或偶然的非法授权泄漏、更改、破坏或使信息被非法系统辨识、控制，即确保信息的保密性、完整性、可用性、可控性。针对计算机信息系统中信息的存在形式和运行特点，数据安全包括输入／输出数据安全、进入识别、访问控制、加密、审计跟踪、备份与恢复等方面。

（3）运行安全。运行安全包括电源、机房管理、出入控制、数据与介质管理、运行管理等方面。

（4）软件安全。软件安全包括软件开发规程、软件安全测试、软件的修改与复制等方面。

（5）人的安全。人的安全主要是指计算机使用人员的安全意识、法律意识、安全技能等。

第三节　电子办公安全威胁的严峻性

在我国，网络安全、信息安全、电子办公安全受到威胁的形势是十分严峻的。

（1）各个国家、集团正加紧准备信息战、网络战。

信息战是20世纪80年代国际军事理论界在研究新的军事变革动向过程中提出的一种新的战争形态和决战样式。90年代以来，世界大国和一批中小国家都在开展信息战的理论研究，建立信息战机构，积聚信息战力量，制定信息战战略和规章制度。

美国从20世纪90年代以来，更是加紧信息战、网络战的准备：一是研究开发信息战的手段，如1990年着手研究计算机病毒战，1995年制定了计算机病毒武器计划；二是建立覆盖美国全军的信息战、网络战的机构；三是投入了几十亿美元加速网络防御手段的研究。四是建立了全国、全军计算机时间应急机制，颁布了信息战战备等级。从海湾战争、科索沃战争、阿富汗战争和伊拉克战争中可以看出，信息战已经成为美国的重要作战方式。美军信息战除了摧毁压制手段外，还广泛使用信息心理战、信息欺骗、网络控制等多种手段。

(2)因特网上的斗争日趋尖锐复杂。

近年来，我国正进入信息化建设的高潮，进入因特网的人数日渐巨大，因特网斗争日益复杂。一是将涉密计算机接通因特网等违规操作，给那些通过因特网

窃取、破坏信息的别有用心之徒提供了机会。二是敌对势力利用因特网散布有害信息、蛊惑人心、制造混乱、危害社会稳定。三是黑客组织利用因特网千方百计攻击、干扰政府和企业的主要网站，破坏信息系统的正常运行。四是非法组织和敌对势力利用因特网作为相互联络、互通信息、协调行为和发展组织的重要渠道。五是国内一些违法分子在因特网上有意无意地泄露秘密，造成了严重后果。

（3）我国涉密信息系统和网络存在的威胁。

政府机关、企业内部网络是我国信息网络的重要组成部分，按照2002年国发17号文件精神，信息网络分为内网（涉密网）、外网（非涉密网）和因特网三类，而且明确内网和外网要物理隔离。但由于主观、客观等方面的原因，涉密网络还存在不少重大的风险：一是信息系统存在大量漏洞，成为诱发安全事件的自然原因。IBM公司的专家认为，在编写软件的过程中，每1000行程序可能会出现一个漏洞，而微软操作系统是由几千万行程序组成的，自然很难不出现问题。这些漏洞为黑客和网络犯罪人员提供了兴风作浪的攻击对象。而我国绝大多数的计算机用户所使用的都是微软的操作系统。因此，造成了我国信息系统的天然不足。二是境外垄断关键的信息技术或刻意安装安全线路是造成安全隐患的另一原因。由于我国的微电子技术与发达国家存在很大差距，致使信息化所需的不少关键技术设备必须从美国等发达国家引进。这些国家为了垄断关键技术，它的高端产品或者不允许出口，或者在出口产品中安装了线门，对外声称是用于网上的远程维护。这就为窃取秘密数据埋下了通道，造成了使用者受制于人的安全风险。三是安全意识淡薄、管理不善是信息安全发生的主观原因。在许多网络发展比较落后的地方，不少网络维护使用人员缺乏必要的网络安全意识，对相关的网络信息安全管理制度也不够健全。从近几年部分单位安全检查遇到的案例来看，有的不遵守安全保密规定，将内网直接或间接地与因特网连接，有的安全设施设备的配置不合理，访问控制不够严格，有的选用非常简单的上机口令甚至是空口令等，这些问题的存在直接带来了安全威胁。

（4）随着窃密手段的高技术化，信息破坏的方法层出不穷。

除了大家比较熟悉的网络入侵攻击、计算机病毒、窃听工具等，特别要强调的是利用废旧磁媒体获取信息的问题。旧的计算机、旧的磁盘、磁带、光盘等，往往存储过涉密信息，有的技术已经可以从消过磁的介质中恢复曾经存储过的信息，情报机关就利用收集废旧物品的机会专门搜集废旧磁媒体，从中获取情报。因此对废旧磁媒体要特别加强管理。

第四节　电子办公中信息安全的特性

电子办公中信息安全包括了信息的以下几个特性:

（1）保密性。

保密性是指网络信息不被泄露给未授权的人，即信息只为授权用户使用。

（2）真实性。

真实性是指用户的身份是真实的。在电子办公系统中，如何防范冒充、伪造用户身份的不法行为，是真实性需要解决的问题。

（3）完整性。

完整性是指信息在存储或传输过程中保持不被偶然或者蓄意地添加、删除、修改、乱序、重放等破坏和丢失的特性。完整性要求信息保持原样，确保信息的正确生成、正确存储、正确传输。影响信息完整性的主要因素有：设备故障、误码、人为攻击、计算机病毒等。

（4）可靠性。

可靠性是指系统能在规定的条件和规定的时间内完成规定的功能的特性。它包括三方面：一是抗毁性，即系统在人为破坏下的可靠性。增强抗毁性可以有效地避免因各种灾害（如战争、地震）造成的大面积瘫痪事件。二是生存性，即系统在随机破坏下的可靠性。随机性破坏是指系统部件因为自然老化等造成的自然失效。三是有效性，它主要反映在办公网络信息系统部件失效的情况下，满足业务性能的可靠性。

（5）可用性。

可用性是指办公网络信息可被授权用户访问并按需求使用的特性，它是办公网络信息系统面向用户的安全性能。

（6）不可否认性。

不可否认性是指在办公网络信息系统的信息交互过程中，确信参与者的真实同一性，所有参与者都不可能否认或抵赖曾经完成的操作和承诺。数字签名技术是解决不可否认性的手段之一。

（7）可控性。

可控性是对办公网络信息的传播及内容具有控制能力的特性。对于电子办公系统而言，可控性是十分重要的特点，所有需要公开发布的信息必须通过审核后才能发布。

第五节　电子办公受到的主要威胁来源

电子办公受到的威胁有人为的，有非人为的，不仅来自于外部，也来自于内部。不仅间谍、罪犯可能对电子办公系统进行攻击，各种人员、机构出于各自的目的也可能对电子办公系统进行攻击。与传统政务不同，电子办公对信息技术有很大的依赖性，因此，信息系统自身存在的漏洞和缺陷会对电子办公业务的开展和连续运行造成安全隐患。

一、系统外部和内部的威胁

与20世纪70年代之前通信保密阶段安全威胁的来源相比，现在的计算机信息网络系统、电子办公安全威胁同样主要来自外部因素和内部原因。

1.外部因素

外部威胁一是无组织的黑客攻击，二是有组织的网络攻击。前者是个人行为，后者则发展为信息战。两者都是凭借计算机技术和通信技术侵入到计算机网络信息系统中，但黑客攻击相对独立无组织，而网络攻击是有组织的采用军事斗争手段，是信息战的一种形态。外部攻击有两种目的：一种是以刺探、破坏、干扰信息为目的，另一种是获取信息内的秘密文件，进而篡改文件命令，即以获取情报为目的。前者主要表现为各种计算机病毒，后者则是秘密地窃取情报，和前者相比，更不容易被发现，所造成的危害也就更深远一些。

2.内部原因

内部威胁行为分为违规操作和恶意报复。其中违规操作是造成外部威胁得逞的主要原因。如内部人员擅自通过实名计算机直接进入因特网，造成计算机内存储的秘密文件被窃；又如不经病毒过滤擅自从互联网上下载数据，造成计算机感染病毒；操作不当引起计算机硬件无法正常运行工作。另外，内部人员的恶意报复在企业也时有发生，如对企业不满的计算机工作人员肆意破坏计算机硬件，致使硬件系统损坏乃至瘫痪；恶意破坏数据库软件，造成数据丢失和系统故障；企业的工业间谍还通过信息系统获取工业秘密，造成企业的重大损失；银行内部的计算机员工利用计算机对银行业务的识别进行计算机犯罪等。

二、非人为和人为威胁

1.非人为的安全威胁

非人为的安全威胁分为两种：

（1）自然灾害，如地震、水灾等。电子办公系统都是在一定的地理环境下运行的，自然灾害可能对电子办公系统造成毁灭性的破坏。

（2）技术上的局限性。许多企业办公信息技术可能存在漏洞和缺陷，如系统、