计算机网络信息安全与防护策略研究

温翠玲　王金嵩　　主编

天津出版传媒集团
天津科学技术出版社

图书在版编目（CIP）数据

计算机网络信息安全与防护策略研究 / 温翠玲，王金嵩主编. --天津 : 天津科学技术出版社，2019.3

ISBN 978-7-5576-6261-5

Ⅰ. ①计… Ⅱ. ①温… ②王… Ⅲ. ①计算机网络－信息安全－研究 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2019)第065597号

计算机网络信息安全与防护策略研究

JISUANJI WANGLUO XINXI ANQUAN YU FANGHU CELUE YANJIU

责任编辑：王　冬

责任印制：兰　毅

出　　版：天津出版传媒集团
天津科学技术出版社

地　　址：天津市西康路35号

邮　　编：300051

电　　话：（022）23332397

网　　址：www.tjkjcbs.com.cn

发　　行：新华书店经销

印　　刷：天津印艺通制版印刷有限责任公司

开本 787×1092　1/16　印张 12.875　字数 260 000

2019年3月第1版第1次印刷

定价：50.00元

前　言

信息已成为社会发展的重要战略资源、决策资源，信息化水平已成为衡量一个国家现代化程度和综合国力的重要指标，抢占信息资源已经成为国际竞争的重要内容。

在信息化社会中，计算机和通信网络已经广泛应用于各个领域。以此为基础建立的各种信息系统，给人们的生活、工作带来了巨大变化。然而人们在享受网络信息所带来的利益的同时，也面临着信息安全的严峻考验，信息安全的重要性有目共睹。以因特网为代表的全球性信息化浪潮日益高涨，信息网络技术的应用正日益普及和广泛，应用层次正在深入，应用领域从传统的、小型业务系统逐渐向大型、关键业务系统扩展。伴随网络的普及，安全日益成为影响信息系统性能的重要问题，而因特网所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求。

本书共分七章，其中作者温翠玲（唐山市第一职业中等专业学校）负责编写第一、二、三、六章，共计 14 万字；作者王金嵩（辽宁经济职业技术学院）负责编写第四、五、七章，共计 12 万字。

由于计算机信息安全技术涉及内容广，而且技术本身的发展也十分迅速，难以在本书十分全面地反映出来，再加上作者水平有限，书中难免存在一些疏漏和不妥之处，恳请读者谅解，也希望广大读者批评指正。

编者

目　录

第一章　绪论 …… 1
　第一节　信息安全基本概念 …… 1
　第二节　信息安全体系结构框架 …… 7
　第三节　网络信息安全发展趋势 …… 14
第二章　攻防技术试验 …… 21
　第一节　信息搜集 …… 21
　第二节　嗅探技术 …… 28
　第三节　ICMP 重定向攻击 …… 34
　第四节　后门技术 …… 40
　第五节　缓冲区溢出攻击 …… 46
　第六节　拒绝服务攻击 …… 52
第三章　数据库安全 …… 59
　第一节　数据库的安全问题 …… 59
　第二节　推理泄露问题 …… 65
　第三节　数据库的多级安全问题 …… 70
第四章　IPS 入侵防御系统 …… 76
　第一节　安全威胁发展趋势 …… 76
　第二节　应用层安全威胁分析 …… 84
　第三节　IPS 的产生背景和技术演进 …… 89
　第四节　IPS 主要功能和防护原理 …… 95
　第五节　IPS 工作模式和主要应用场景 …… 102
第五章　网络安全技术 …… 111
　第一节　网络安全基础 …… 111
　第二节　防火墙技术 …… 116

第三节　VPN 技术 …… 122
第四节　网络入侵检测 …… 126
第五节　计算机病毒及其防治 …… 131
第六章　局域网安全技术探究 …… 137
第一节　局域网安全风险与特征 …… 137
第二节　局域网安全措施与管理 …… 145
第三节　网络监听与协议分析 …… 152
第四节　VLAN 安全技术与应用 …… 159
第五节　无线局域网安全技术 …… 164
第六节　企业局域网安全解决方案 …… 168
第七章　计算机网络信息安全与防护策略研究 …… 175
第一节　计算机网络信息安全中数据加密技术的研究 …… 175
第二节　大数据时代下计算机网络信息安全问题研究 …… 180
第三节　计算机网络信息安全分析与管理 …… 186
第四节　计算机网络信息安全及防护策略研究 …… 193
参考文献 …… 199

第一章　绪论

第一节　信息安全基本概念

1 计算机信息系统受到的威胁

由于计算机信息系统是以计算机和数据通信网络为基础的应用管理系统，因而它是一个开放式的互联网络系统，如果不采取安全保密措施，与网络系统连接的任何终端用户都可以进入和访问网络中的资源。目前，计算机信息系统已经在各行各业，包括金融、贸易、商业、企业各个行业部门，甚至日常生活领域中得到广泛的应用。它在给人们带来极大方便的同时，也为那些不法分子利用计算机信息系统进行经济犯罪提供了可能。据不完全统计，全世界每年因被利用计算机系统进行犯罪所造成的经济损失高达上千亿美元。在我国，利用计算机管理和决策信息系统从事经济活动起步较晚，但各种计算机犯罪活动已时有报道，并直接影响了计算机信息系统的普及使用。

归纳起来，计算机信息系统所面临的威胁分为以下几类：

1.1 自然灾害

主要是指火灾、水灾、风暴、地震等破坏，以及环境(温度、湿度、振动、冲击、污染)的影响。目前，我们不少计算机房并没有防震、防火、防水、避雷、防电磁泄漏或干扰等措施，接地系统也疏于考虑，抵御自然灾害和意外事故的能力较差。日常工作中因断电而设备损坏、数据丢失的现象时有发生。

1.2 人为或偶然事故

这可能是由于工作人员的失误操作使得系统出错，使得信息遭到严重破坏或被别人偷窥到机密信息，或者环境因素的忽然变化造成信息丢失或破坏。

1.3 计算机犯罪

计算机犯罪是利用暴力和非暴力形式，故意泄漏或破坏系统中的机密信

息,以及危害系统实体和信息安全的不法行为。《中华人民共和国刑法》对计算机犯罪做了明确定义,即利用计算机技术知识进行犯罪活动并将计算机信息系统作为犯罪对象。

利用计算机犯罪的人,通常利用窃取口令等手段,非法侵入计算机信息系统,利用计算机传播反动和色情等有害信息,或实施贪污、盗窃、诈骗和金融犯罪等活动,甚至恶意破坏计算机系统。

对计算机信息系统来说,以下三个方面常常被人为的犯罪活动攻击。

1)通信过程中的威胁。计算机信息系统的用户在进行使息通信的过程中,常常受到两方面的攻击:一是主动攻击,攻击者通过网络线路将虚假信息或计算机病毒输入到信息系统内部,破坏信息的真实性与完整性,造成系统无法正常运行,严重的甚至使系统处于瘫痪;二是被动攻击,攻击者非法窃取通信线路中的信息,使信息机密性遇到破坏、信息泄漏而无法察觉,给用户带来巨大的损失。

2)存储过程中的威胁。存储于计算机系统中的信息。易于受到与通信线路同样的威胁。非法用户在获取系统访问控制权后,浏览存储介质上的机密数据或专利软件,并且对有价值的信息进行统计分析,推断出所需的数据,这样就使信息的保密性、真实性、完整性道到破坏。

3)加工处理中的威胁。计算机信息系统一般都具有对信息进行加工分桥的处理功能。而信息在进行处理过程中,通常都是以原码出现,加密保护对处理中的信息不起作用。因此,在此期间有意攻击和意外操作都极易使系统遭受破坏,造成损失。

1.4 计算机病毒

计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据,影响计算机使用,并能自我复制的一组计算机指令或者程序代码。

“计算机病毒”这个称呼十分形象,它像一个灰色的幽灵无处不存、无时不在。它将自己附在其他程序上,在这些程序运行时进入系统中扩散。一台计算机感染病毒后,轻则系统工作效率下降,部分文件丢失,重则造成系统死机或毁坏,全部数据丢失。1999 年 4 月 26 日 CIH 病毒在全球造成的危害,足以显露计算机病毒的可怕。

据一份市场调查报告表明,我国约有的 90%的网络用户曾遭到过病毒的侵袭,并且其中大部分用户因此受到损失。病毒危害的泛滥,揭示了计算机系统本身和人们的意识在安全方面的薄弱。

1.5 信息战的严重威胁

所谓信息战,就是为了国家的军事战略而采取行动,取得信息优势,干扰敌方的信息和信息系统,同时保卫自己的信息和信息系统。这种对抗形式的目标,不是集中打击敌方的人员或战斗技术装备,而是集中打击敌方的计算机信息系统,使其神经中枢似的指挥系统瘫痪。

信息技术从根本上改变了进行战争的方法,信息武器已经成为继原子武器、生物武器、化学武器之后的第四类战略武器。

在海湾战争中,信息武器首次进入实战。伊拉克的指挥系统吃尽了美国的大亏;仅仅是在购买的智能打印机中,被塞进一片带有病毒的集成电路芯片,加上其他的因素,最终导致系统崩溃,指挥失灵,几十万伊军被几万联合国维和部队俘虏。美国的维和部队还利用国际卫星组织的全球计算机网络,为其建立军事目的的全球数据电视系统服务。

所以,未来国与国之间的对抗首先将是信息技术的较量。网络信息安全,应该成为国家安全的前提。

2 计算机信息系统受到的攻击

2.1 威胁和攻击的对象

按被威胁和攻击的对象来划分,可分为两类:一类是对计算机信息系统实体的威胁和攻击;另一类是对信息的威胁和攻击。计算机犯罪和计算机病毒则包括了对计算机系统实体和信息两个方面的威胁和攻击。

(1)对实体的威胁和攻击

对实体的威胁和攻击主要指对计算机及其外部设备和网络的威胁及攻击,如各种自然灾害与人为的破坏、设备故障、场地和环境因意的影响、电磁场的干扰或电磁泄漏、战争的破坏、各种媒体的被盗和散失等。

信息系统实体受到威胁和攻击,不仅会造成国家财产的重大损失,而且会使信息系统的机密信息严重泄露和破坏。因此,对信息系统实体的保护是防止对信息威胁和攻击的首要一步,也是防止对信息威胁和攻击的天然屏蔽。

(2)对信息的威胁和攻击

对信息的威胁和攻击的后果主要有两种:一种是信息的泄露,另一种是信息的破坏。所谓信息泄露,就是被人偶然或故意地获得(侦收、窃取或分析破译)目标系统中的信息,特别是敏感信息,造成泄漏事件。信息破坏是指由于偶然事故或人为破坏,使得系统的信息被修改、删除、添加、伪造成非法复制,造成大量信息的破坏、失真或泄密,使信息的正确性、完整性和可用性受到破坏。

2.2 被动攻击和主动攻击

按攻击的方式分,可分为被动攻击和主动攻击两类。

(1)被动攻击

被动攻击是指一切窃密的攻击。它是在不干扰系统正常工作的情况下,进行截获、窃取系统信息,以便破译分析;利用观察信息、控制信息的内容来获得目标系统的设置、身份;通过研究机密信息助长度和传递的频度获得信息的性质。被动攻击不容易被用户察觉出来,因此它的攻击持续性和危害性都很大。

(2)主动攻击

主动攻击是指篡改信息的攻击。它不仅是窃密,而且威胁到信息的完整性和可靠性。它以各种各样的方式,有选择地修改、删除、添加、伪造和复制信息内容,造成信息破坏。

2.3 对信息系统攻击的主要手段

信息系统在运行过程中，往往受到上述各种威胁和攻击，非法者对信息系统的破坏主要采取如下手段。

1)冒充。这是最常见的破坏方式。信息系统的非法用户伪装成合法的用户，对系统进行非法的访问，冒充授权者发送和接收信息，造成信息的泄露与丢失。

2)篡改。网络中的信息在没有监控的情况下都可能被篡改，即将信息的标签、内容、属性、接收者和始发者进行修改，以取代原信息，造成信息失真。

3)窃收。信息盗窃可以有多种途径：在通信线路中，通过电磁辐射侦截线路中的信息；在信息存储和信息处理过程中，通过冒充、非法访问，达到窃取信息的目的，等等。

4)重放。将窃取的信息重新修改或排序后，在适当的时机重放出来，从而造成信息的重复和混乱。

5)推断。这也是在窃取基础之上的一种破坏活动，它的目的不是窃取原信息，而是将窃取到的信息进行统计分析，了解信息流大小的变化、信息交换的频繁程度，再结合其他方面的信息，推断出有价值的内容。

6)病毒。几千种的计算机病毒直接威胁着计算机的系统和数据文件，破坏信息系统的正常运行。

总之，对信息系统的攻击手段多种多样。我们必须学会识别这些破坏手段，以便采取技术策略和法律制约两方面的努力，确保信息系统的安全。

3 计算机信息系统的脆弱性

计算机系统本身也因为存在着一些脆弱性，抵御攻击的能力很弱，自身的一些缺陷常常容易被非授权用户不断利用。这种非法访问使系统中存储的信息的完整性受到威胁。使信息被修改或破坏而不能继续使用；而且系统中有价值的信息被非法篡改、伪造、窃取或删除而不留任何痕迹时，若计算机信息系统继续运行，还会得出截然相反的结果，造成不可估量的损失。另外，计算机还容易受到各种自然灾害和各种误操作的破坏。

从计算机信息系统自身的结构方面分析，也有一些问题是目前在短时间内无法解决的。

1)计算机操作系统的脆弱性。操作系统是计算机重要的系统软件。它控制和管理着计算机系统所有的硬件、软件资源，是计算机系统的指挥中枢。计算机操作系统的不安全是信息系统不安全的重要原因。由于操作系统地位非常重要，使得攻击者常常将之作为主要攻击目标。

2)计算机网络系统的脆弱性。计算机网络就是将分散在不同地理位置的计算机系统，通过某种介质连接起来，实现信息和资源的共享。但是由于无论是互联网本身还是 TCP/IP 协议，在形成初期都没有考虑到安全问题，因而造成了网络系统安全的“先天不足”。

3)数据库管理系统的脆弱性。数据库是相关信息的集合。计算机系统中的

信息通常以数据库的形式组织存放，攻击者通过非法访问数据库，达到篡改和破坏信息的目的。数据库管理系统安全必须与操作系统的安全进行配套，例如DBMS的安全级别为B2级，那么操作系统的安全级别同样是B2级的。数据库的安全管理还是建立在分级管理概念上的。所以，DBMS的安全也是脆弱的。

4 计算机信息安全的定义

人们对信息安全的认识，是一个由浅入深、由此及彼、由表及里的深化过程。20世纪60年代的通信保密时代，人们认为信息安全就是通信保密，采用的保障措施就是加密和基于计算机规则的访问控制。到了20世纪80年代，人们的认识加深了，大家逐步意识到数字化信息除了有保密性的需要外，还有信息的完整性、信息和信息系统的可用性需求，因此明确提出了信息安全就是要保证信息的保密性、完整性和可用性，造就进入了信息安全时代。其后由于社会管理以及电子商务、电子政务等网上应用的开展，人们又逐步认识还要关注可控性和不可否认性(真实性)。1993年6月，美国政府同加拿大及欧共体同起草通用安全评价准则(简称cc标准)并将其推进到国际标准，把所有的安全问题定义为信息系统或者安全产品的安全策略、安全功能、管理、开发、维护、检测、恢复和安全评测等概念的简称。

信息安全的概念是与时俱进的，过去是通信保密或信息安全，而今天以至于今后是信息保障。

信息安全主要涉及信息存储的安全、信息传输的安全以及对网络传输信息内容的审计三方面，它研究计算机系统和通信网络内信息的保护方法。

从广义来说，凡是涉及信息的完整性、保密性、真实性、可用性和可控性的相关技术和理论都是信息安全所要研究的领域。下面给出信息安全的一般定义：计算机信息安全是指计算机信息系统的硬件、软件、网络及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统可靠正常地运行，信息不中断。

5 计算机信息安全的特征

计算机信息安全具有以下五方面的特征。

(1)保密性

保密性是信息不被泄露给非授权的用户、实体或过程，或供其利用的特性，即防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性。

(2)完整性

完整性是信息未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和传输。

完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性

则要求信息不致受到各种原因的破坏。影响网络信息完整性的主要因素有设备故障、误码、人为攻击及计算机病毒等。

(3)真实性

真实性也称作不可否认性。在信息系统的信息交互过程中,确信参与者的真实同一性,即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息,利用递交接收证据可以防止收信方事后否认已经接收到信息。

(4)可用性

可用性是信息可被授权实体访问并按需要使用的特性,即信息服务在需要时,允许授权用户或实体使用的特性,或者是信息系统(包括网络)部分受损或需要降级使用时,仍能为授权用户提供有效服务的特性。

(5)可控性

可控性是对信息的传播及内容具有控制能力的特性。即指授权机构可以随时控制信息的机密性。美国政府所提供的“密钥托管”“密钥恢复”等措施就是实现信息安全可控性的例子。

概括地说,计算机信息安全核心是通过计算机、网络、密码技术和安全技术,保护在信息系统及公用网络中传输、交换和存储的信息的完整性、保密性、真实性、可用性和可控性等。

6 计算机信息安全的含义

信息安全的具体含义和侧重点会随着观察者角度的变化而变化。

从用户(个人用户或者企业用户)的角度来说,他们最为关心的问题是如何保证他们的涉及个人隐私或商业利益的数据在传输、交换和存储过程中受到保密性、完整性和真实性的保护,避免其他人(特别是其竞争对手)利用窃听、冒充、篡改和抵赖等手段对其利益和隐私造成损害和侵犯,同时用户也希望他保存在某个网络信息系统中的数据不会受其他非授权用户的访问和破坏。

从网络运行和管理者的角度来说,他们最为关心的问题是如何保护和控制其他人对本地网络信息的访问和读写等操作。比如,避免出现病毒、非法存取、拒绝服务和网络资源非法占用与非法控制等现象,制止和防御网络黑客的攻击。

对安全保密部门和国家行政部门来说,他们最为关心的问题是如何对非法的、有害的或涉及国家机密的信息进行有效过滤和防堵,避免非法泄露。秘密敏感的信息被泄密后将会对社会的安定产生危害,对国家造成巨大的经济损失和政治损失。

从社会教育和意识形态角度来说,人们最为关心的问题是如何杜绝和控制网络上不健康的内容。有害的黄色内容会对社会的稳定和人类的发展造成不良影响。

在计算机信息系统中,计算机及其相关的设备、设施(含网络)统称为计算机

信息系统的“实体”。实体安全是指为了保证计算机信息系统安全可靠运行，确保计算机信息系统在对信息进行采集、处理、传输、存储过程中，不致受到人为(包括未授权使用计算机资源的人)或自然因素的危害，导致信息丢失、泄漏或破坏，而对计算机设备、设施(包括机房建筑、供电、空调等)、环境人员等采取适当的安全措施。

第二节　信息安全体系结构框架

如今世界发展步入了信息化时代，网络信息系统在国家的各个领域中得到了普遍应用，人们的生活生产充分认识到了计算机网络信息的重要性，很多企业组织发展加强了对信息的依赖。但在计算机网络信息类型增多和人们使用需求提升以及计算机网络系统自身存在的风险，计算机网络信息系统安全管理成为有关人员关注的重点。为了避免计算机使用用户信息泄露、信息资源的应用浪费、计算机信息系统软硬件故障对信息准确性的不利影响，需要有关人员构建有效的计算机网络信息安全结构体系，通过该结构体系的构建保证计算机网络信息系统运行的安全。

1 计算机网络信息系统安全概述

1.1 如何认识信息安全产业

在社会主义市场经济的条件下，按照市场规律发展信息安全产业，是国家整体信息安全体系建设的一个重要方面。从市场经济的角度认识信息安全产业，是一个重要的课题，这对领域主管部门、产业部门、从业企业都有重要的意义。

信息成为一项重要的资产，是包括信息安全产业在内的整个信息产业发展的根本原因。市场经济是以资产运营为手段、以资产增值为目的的经济形态，资产结构及资产运营管理构成了市场经济的两个基本方面。在市场经济环境下，当一种新的资产要素出现时，就会形成围绕这一资产要素的产业链条。市场经济发展到今天，信息作为资产要素的特征日益显露。以信息资产为核心要素，以信息资产运营为核心过程的信息经济，带来了市场经济的一个全新发展阶段。信息成为资产要素，是信息产业发展的根本原因，同样也是信息安全产业发展的根本原因。

安全是信息资产区别于其他资产要素的关键属性。信息的高无形价值、强时效性、低传播成本等因素决定了这一点。没有安全保障的信息资产，谈不上资产价值；没有安全管理的信息资产运营，不能实现信息资产的保值和增值。信息资产的价值与其安全状况直接相关。

安全管理是信息资产运营的关键，是信息安全产业响应的主要需求。确保资产及其运营的安全，是资产管理的普遍要求，对信息资产而言，这一点尤为重

要。信息安全产业必须解决信息资产运营中的安全管理问题。

为信息资产的安全运营提供保障是信息安全产业的核心价值所在。信息安全产业是由信息资产安全运营需求所决定的产业链条。实现信息资产的安全管理,保障信息资产的安全运营,是整个信息安全产业的核心价值所在。信息安全产业是信息产业最具投资价值的一个方向,是整个信息产业的一个制高点。

访问控制是信息安全产业的关键技术。人和信息之间的交互管理是信息安全管理的核心,因而实现这种安全机制的访问控制技术成为关键。

1.2 计算机网络信息系统安全内涵和发展目标

计算机网络信息系统安全是指计算机信息系统结构安全,计算机信息系统有关元素的安全,以及计算机信息系统有关安全技术、安全服务以及安全管理的总和。计算机网络信息系统安全从系统应用和控制角度上看,主要是指信息的存储、处理、传输过程中体现其机密性、完整性、可用性的系统辨识、控制、策略以及过程。

计算机网络信息系统安全管理的目标是实现信息在安全环境中的运行。实现这一目标需要可靠操作技术的支持、相关的操作规范、计算机网络系统、计算机数据系统等。

1.3 计算机网络信息系统安全体系结构概述

信息安全涉及的技术面非常广,在规划、设计、评估等一系列重要环节上都需要一个安全体系框架来提供指导。信息系统安全体系结构框架是国家"等级保护制度"技术体系的重要组成部分。在计算机网络技术的不断发展下,基于经典模型的计算机网络信息安全体系结构不再适用,为了研究解决多个平台计算机网络安全服务和安全机制问题,在 1989 年有关人员提出了开放性的计算机网络信息安全全体系结构标准,确定了计算机三维框架网络安全体系结构。三维框架网络安全体系结构具体如图 1-1 所示。

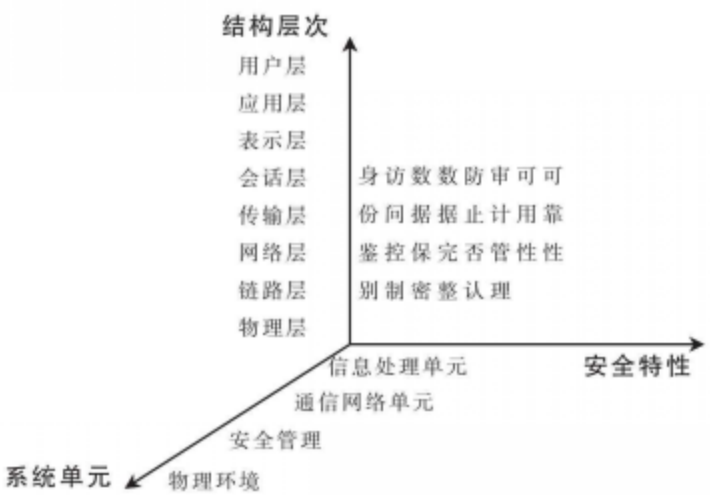

图 1-1 三维框架网络安全体系结构

这是一个通用的框架，反映信息系统安全需求和体系结构的共性，是从总体上把握信息系统安全技术体系的一个重要认识工具，具有普遍的适用性。信息系统安全体系结构框架的构成要素是安全特性、系统单元及开放系统互联参考模型结构层次。安全特性维描述了信息系统的安全服务和安全机制，包括身份鉴定、访问控制、数据保密、数据完整、防止否认、审计管理、可用性和可靠性。采取不同的安全政策或处于不同安全等级的信息系统可有不同的安全特性要求。系统单元描述了信息系统的各组成部分，还包括使用和管理信息系统的物理和行政环境。

系统单元可分为四个部分：①信息处理单元，包括端系统和中继系统；②通信网络，包括本地通信网络和远程通信网络；③安全管理，即信息系统管理中与安全有关的活动；④物理环境，即与物理环境和人员有关的安全问题。

信息处理单元主要考虑计算机系统的安全：通过物理和行政管理的安全机制提供安全的本地用户环境，保护硬件的安全；通过防干扰、防辐射、容错、检错等手段，保护软件的安全；通过用户身份鉴别、访问控制、完整性等机制，保护信息的安全。信息处理单元必须支持安全特性维要求的安全配置，支持具有不同安全策略的多个安全域。安全域是用户、信息客体以及安全策略的集合。信息处理单元支持安全域的严格分离、资源管理以及安全域间信息的受控共享和传送。

通信网络安全：为传输中的信息提供保护。通信网络系统安全涉及安全通信协议、密码机制、安全管理应用进程、安全管理信息库、分布式管理系统等内容。通信网络安全确保开放系统通信环境下的通信业务流安全。

安全管理：包括安全域的设置和管理、安全管理的信息库、安全管理信息通信、安全管理应用程序协议、端系统安全管理、安全服务管理与安全机制管理等。

物理环境与行政管理安全：涉及人员管理、物理环境管理和行政管理，还涉及环境安全服务配置以及系统管理员职责等。

开放系统互联参考模型结构层次：各信息系统单元需要在开放系统互联参考模型的七个不同层次上采取不同的安全服务和安全机制，以满足不同安全需求。安全网络协议使对等的协议层之间建立被保护的物理路径或逻辑路径，每一层次通过接口向上一层提供安全服务。

2 计算机网络信息安全体系结构特点

2.1 保密性和完整性特点

计算机网络信息的重要特征是保密性和完整性，能够保证计算机网络信息应用的安全。保密性主要是指保证计算机网络系统在应用的过程中机密信息不泄露给非法用户。完整性是指计算机信息网络在运营的过程中信息不能被随意篡改。

2.2 真实性和可靠性特点

真实性主要是指计算机网络信息用户身份的真实，从而避免计算机网络信

息应用中冒名顶替制造虚假信息现象的出现。可靠性是指计算机信息网络系统在规定的时间内完成指定任务。

2.3 可控性和占有性特点

可控性是指计算机网络信息全系统对网络信息传播和运行的控制能力，能够杜绝不良信息对计算机网络信息系统的影响。占有性是指经过授权的用户拥有享受网络信息服务的权利。

3 计算机网络信息安全体系存在的风险

3.1 物理安全风险

计算机网络信息物理安全风险包含物理层中可能导致计算机网络系统平台内部数据受损的物理因素，主要包括由于自然灾害带来的意外事故造成的计算机系统破坏、电源故障导致的计算机设备损坏和数据丢失、设备失窃带来的计算机数据丢失、电磁辐射带来的计算机信息数据丢失等。

3.2 网络系统安全风险

计算机信息网络系统安全风险包括计算机数据链路层和计算机网络层中能够导致计算机系统平台或者内部数据信息丢失、损坏的因素。网络系统安全风险包括网络信息传输的安全风险、网络边界的安全风险、网络出现的病毒安全风险、黑客攻击安全风险。

3.3 系统应用安全风险

计算机信息网络系统的应用安全风险包括系统应用层中能够导致系统平台和内部数据损坏的因素，包括用户的非法访问、数据存储安全问题、信息输出问题、系统安全预警机制不完善、审计跟踪问题。

4 计算机网络信息安全体系结构构建分析

4.1 计算机网络信息安全体系结构

计算机网络信息安全结构是一个动态化概念，具体结构不仅体现在保证计算机信息的完整、安全、真实、保密等，而且还需要有关操作人员在应用的过程中积极转变思维，根据不同的安全保护因素加快构建一个更科学、有效、严谨的综合性计算机网络信息安全保护屏障，具体的计算机网络信息安全体系结构模式需要包括以下几个环节。

(1)预警

预警机制在计算机网络信息安全体系结构中具有重要的意义，也是实施网络信息安全体系的重要依据，在对整个计算机网络环境、网络安全进行分析和判断之后为计算机信息系统安全保护体系提供更为精确的预测和评估。

(2)保护

保护是提升计算机网络安全性能，减少恶意入侵计算机系统的重要防御手段，主要是指经过建立一种机制来对计算机网络系统的安全设置进行检查，及时发展系统自身的漏洞并予以及时弥补。

(3)检测

检测是及时发现入侵计算机信息系统行为的重要手段,主要是指通过对计算机网络信息安全系统实施隐蔽技术,从而减少入侵者发现计算机系统防护措施并进行破坏系统的一种主动性反击行为。检测能够为计算机信息安全系统的响应提供有效的时间,在操作应用的过程中减少不必要的损失。检测能够和计算机系统的防火墙进行联动作用,从而形成一个整体性的策略,设立相应的计算机信息系统安全监控中心,及时掌握计算机信息系统的安全运行情况。

(4)响应

如果计算机网络信息安全体系结构出现入侵行为,需要有关人员对计算机网络进行冻结处理,切断黑客的入侵途径,并做出相应的防入侵措施。

(5)恢复

三维框架网络安全体系结构中的恢复是指在计算机系统遇到黑客供给和入侵威胁之后,对被攻击和损坏的数据进行恢复的过程。恢复的实现需要三维框架网络安全体系结构体系对计算机网络文件和数据信息资源进行备份处理。

(6)反击

三维框架网络安全体系结构中的反击是技术性能高的一种模块,主要反击行为是标记跟踪,即对黑客进行标记,之后应用侦查系统分析黑客的入侵方式,寻找黑客的地址。

4.2 基于三维框架网络安全体系结构计算机安全统平台的构建

(1)硬件密码处理安全平台

该平台的构建面向整个计算机业务网络,具有标准规范的 API 接口,通过该接口能够让整个计算机系统网络所需的身份认证、信息资料保密、信息资料完整、密钥管理等具有相应的规范标准。

(2)网络级安全平台

该平台需要解决计算机网络信息系统互联、拨号网络用户身份认证、数据传输、信息传输通道的安全保密、网络入侵检测、系统预警系统等问题。在各个业务进行互联的时候需要应用硬件防火墙实现隔阂处理。在计算机网络层需要应用 SVPN 技术建立系统安全虚拟加密隧道,从而保证计算机系统重要信息传输的安全可靠。

(3)应用安全平台

该平台的构建需要从两个方面实现:第一,应用计算机网络自身的安全机制进行应用安全平台的构建。第二,应用通用的安全应用平台实现对计算机网络上各种应用系统信息的安全防护。

(4)安全管理平台

该平台能够根据计算机网络自身应用情况采用单独的安全管理中心、多个安全管理中心模式。该平台的主要功能是实现对计算机系统密钥管理、完善计算机系统安全设备的管理配置、加强对计算机系统运行状态的监督控制等。

(5)安全测评认证中心

安全测评认证中心是大型计算机信息网络系统必须要建立的。安全测评认证中心的主要功能是通过建立完善的网络风险评估分析系统，及时发现计算机网络中可能存在的系统安全漏洞，针对漏洞指定计算机系统安全管理方案、安全策略。

4.3 实施安全信息系统

正确把握安全信息系统的实施思路，是信息安全系统建设单位十分关心的一个问题。在《计算机信息系统安全保护等级划分准则》编制说明的编写过程中，总结并建议了下图所示的实施流程，这一流程对安全信息系统的实施过程具有普遍的指导意义。

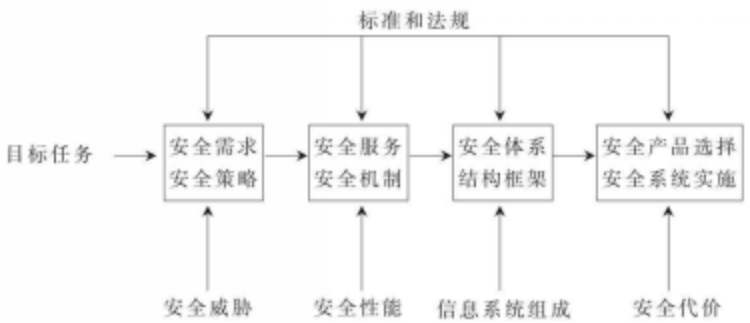

图 1-2 实施安全信息系统流程图

(1)确定安全需求与安全策略

根据用户单位的性质、目标、任务以及存在的安全威胁确定安全需求。安全策略是针对安全需求而制定的计算机信息系统保护政策。该阶段根据不同安全保护级的要求提出了一些原则的、通用的安全策略。各用户单位要规定适合自己情况的完整安全需求和安全策略。下面列举一些重要的安全需求。

1)支持多种信息安全策略。计算机信息系统能够区分各种信息类型和用户活动，使之服从不同的安全策略。当用户共享信息及在不同安全策略下操作时，确保不违反安全策略。计算机信息系统必须支持各种安全策略规定的敏感和非敏感的信息处理。

2)使用开放系统。开放系统是当今发展的主流。在开放系统环境下，必须为支持多种安全等级保护策略的分布信息系统提供安全保障，保护多个主机间分布信息处理和分布信息系统管理的安全。

3)支持不同安全保护级别。支持不同安全属性的用户使用不同安全保护级别的资源。

4)使用公共通信系统。使用公共通信系统实现连通性功能是节约通信资源的有效方法，但是必须确保公共通信系统的可用性安全服务。

(2)确定安全服务与安全机制