第2章 信息安全概述

目录

2.1 信息安全的基本概念

2.1.1信息安全威胁

2.1.2信息安全定义

2.1.3信息安全属性

2.1.1信息安全威胁

内部泄密	内部泄密指由于不严谨的企业内部管理，导致内部信息被企业内部人员有意或无意被泄露。
网络窃听	网络监听工具可以监视和截获网络状态、数据流程以及网络上信息传输。
病毒感染	计算机病毒是一组计算机指令或者程序代码，它通过自我复制对计算机的功能和数据进行破坏，影响计算机的正常运转甚至导致计算机系统瘫痪。
黑客攻击	黑客攻击是通过一定的技术手段进入内部网络，通过扫描系统漏洞，利用系统中安全防护的薄弱环节或系统缺陷，攻击目标主机或窃取其中存储的敏感信息。
非授权访问	是指未经系统授权就使用网络或计算机资源，通过各种手段规避系统的访问控制机制，越权对网络设备及资源进行访问。
信息丢失	由于病毒感染或者黑客攻击导致文件删除、数据破化，从而造成关键信息丢失。

2.1.2信息安全定义

信息安全的概念

- 信息安全是指信息网络的硬件、软件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，系统连续可靠正常地运行，信息服务不中断。

- 信息安全主要包括以下五方面的内容，即需保证信息的保密性、真实性、完整性、未授权拷贝和所寄生系统的安全性。

2.1.2信息安全定义

信息安全的演变

致分为通信安全(COMSEC)，信息安全(INFOSEC)，信息保障(IA:Information Assurance)三个发展阶段，也称为:保密→保护→保障发展阶段。

- (1)通信安全(COMSEC)，本阶段开始于20世纪40年代，主要目的是保障传递的信息的安全，防止信源信宿以外的对象查看到信息。

- (2)信息安全(INFOSEC)，20世纪70年代以后，计算机软硬件技术、网络技术快速发展，这种环境下的信息安全可以归纳为对信息系统的保护，是针对信源、信宿之间的传递活动进行的。

- (3)信息保障(IA)，是世界各国信息安全发展的最新阶段。

2.1.3信息安全属性

信息安全的属性

保密性	系统中有密级要求的信息只能经过特定的方式传输给特定的对象，确保合法用户对该信息的合法访问和使用，阻止非授权的主体阅读信息。
完整性	系统保证信息在存储和传输的过程中保持不被非法存取收偷窃、篡改、删除等，以及不因意外事件的发生而使信息丢失。
可用性	授权主体在需要信息时能及时得到服务的能力。
可控性	系统对信息的传播及其内容具有可控制能力的特性，是对信息和信息系统实施安全监控管理，防止非法利用信息和信息系统。
不可否认性	在网络环境中，信息交换的双方不能否认其在交换过程中发送信息或接收信息的行为。

2.2 信息安全体系

2.2.1 信息安全体系结构

2.2.2 信息安全管理体系

2.2.3 信息安全测评认证体系

2.2.4 信息安全研究体系

2.2.1 信息安全体系结构

安全服务

ISO7498-2确定了五大类安全服务	
鉴别：	可以鉴别参与通信的对等实体和数据源。
访问控制：	能够防止未经授权而利用通过OSI可访问的资源。
数据保密性：	防止数据未经授权而泄露。
数据完整性：	用于对付主动威胁。
不可否认：	包括带数据源证明的不可否认和带递交证明的不可否认。

1.2.1信息安全体系结构

安全机制

ISO7498-2确定了八大类安全机制	
加密：	包括保密性，加密算法和密钥管理几个部分。
数字签名：	决定于两个过程：对数据单元签名和验证已签名的数据单元。
访问控制：	确定访问权，建立多个限制手段。
数据完整性：	一是数据完整性机制。二是确定单个数据单元的完整性。
鉴别交换：	这种安全机制是通过信息交换以确保实体身份的一种机制。
业务填充：	这是一种制造假的通信实例、产生欺骗性数据单元或在数据单元中产生假数据的安全机制。
路由控制：	包括路由选择，路由连接和安全策略。
公证：	保证由第三方公证人提供，公证人能够得到通信实体的信任，而且可以掌握按照某种可证实方式提供所需保证的必要的信息。

2.2.2 信息安全管理体系

网络与信息安全 = 信息安全技术 + 信息安全管理体系

1、建立信息安全管理框架

2、具体实施构架的信息安全管理

3、在信息安全管理体系基础上建立相关的文档

4、安全事件的记录、反馈

2.2.3 信息安全测评认证体系

信息安全性的度量标准

信息技术安全性评估通用准则，通常简称为通用准则(CC)，是评估信息技术产品和系统安全特性的基础准则。通用准则内容分为3部分：“简介和一般模型”；“安全功能要求”；“安全保证要求”。

国际测评认证体系的发展

1995年，CC项目组成立了代国际互认工作组。同年10月，美国的NSA和NIST、加拿大的CSE和英国的CESG签署了该协定。1998年5月德国的GISA、法国的SCSSI也签署了此协定。

1999年10月澳大利亚和新西兰的DSD也加入了CC互认协定。证书发放机构还限于政府机构。

2000年，荷兰、西班牙、意大利、挪威、芬兰、瑞典和希腊等国也加入了该互认协定，日本、韩国、以色列等国也正在积极准备加入此协定。目前的证书发放机构已不再限于政府机构，非政府的认证机构也可以加入此协定，但必须有政府机构的参与或授权。

2.2.3 信息安全测评认证体系

组织结构

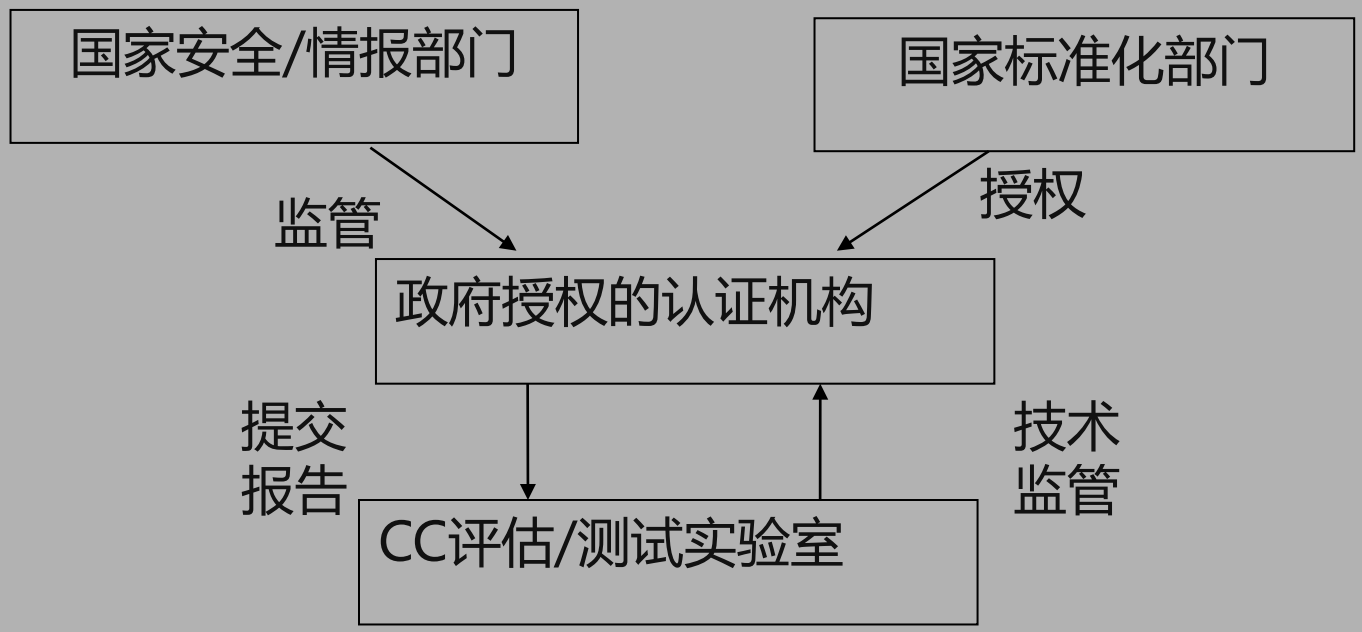

图2-1 信息安全测评认证机构

2.2.3 信息安全测评认证体系

信息安全测评认证体系

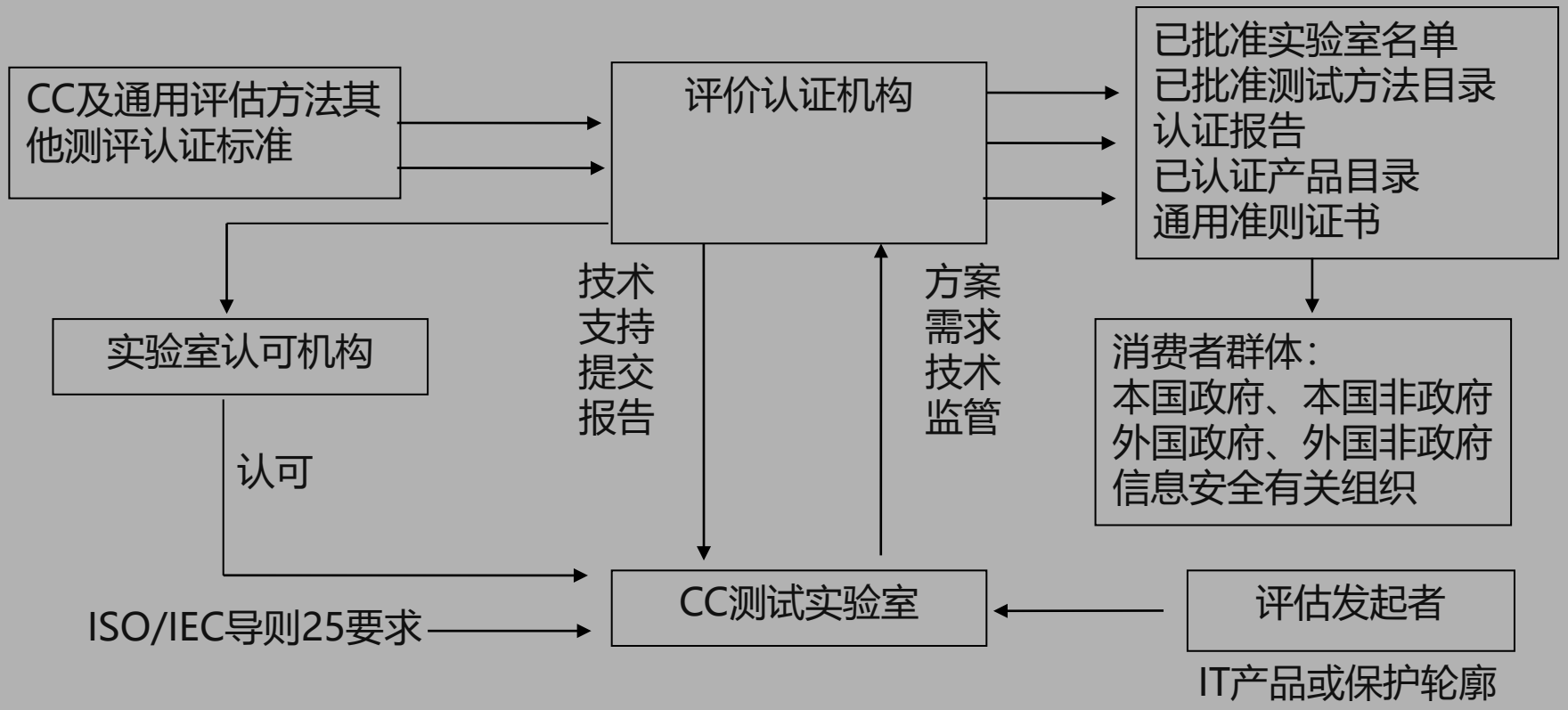

图2-2 信息安全测评认证体系

2.2.3 信息安全测评认证体系

中国信息安全测评认证体系

- 中国国家信息安全测评认证中心是经国家授权，依据国家认证的法律、法规和信息安全管理的政策，并按照国际通用准则建立的中立的技术机构。
- “中华人民共和国国家信息安全证”是国家对信息安全技术、产品或系统安全质量的最高认可。
- 中国国家信息安全测评认证中心开展以下四种认证业务：产品型号认证，产品认证，信息系统安全认证，信息安全服务认证。

2.2.4 信息安全研究体系

密码理论与技术研究

包括两部分，即基于数学的密码理论与技术和非数学的密码理论与技术。

安全协议理论与技术研究

安全协议的安全性分析方法研究和各种实用安全协议的设计与分析研究。

安全体系结构理论与技术研究

安全体系模型的建立及其形式化描述与分析，安全策略和机制的研究，检验和评估系统安全性的科学方法和准则的建立，符合这些模型、策略和准则的系统的研制。

信息对抗理论与技术研究

黑客防范体系，信息伪装理论与技术，信息分析与监控，入侵检测原理与技术，反击方法，应急响应系统，计算机病毒，人工免疫系统在反病毒和抗入侵系统中的应用等。

网络安全与安全产品研究

网络安全整体解决方案的设计与分析，网络安全产品的研发等。

2.3信息安全发展史

2.3.1信息安全发展

2.3.2中国信息安全发展

2.3.1信息安全发展

理论与技术	70年代	80年代	90年代	21世纪
密码	公钥密码	认证码 序列密码	数字签名法 数据加密标准	非数学的密码理论与技术
安全协议		形式化分析方法	电子商务协议 IPSec协议 TLS协议	
安全体系结构	ARPANET BLP模型	TCSEC	CC for ITSEC	达到TCSEC要求100多种
信息对抗		"蠕虫事件“ Y2k问题	计算机病毒 黑客攻击技术	网络攻击 入侵检测与防范
安全产品				防火墙 安全路由器 等

2.3.2中国信息安全发展

初期

较国外存在很大差距，理论基础和自主的技术手段也需要发展和强化。

90年代信息安全

在这个阶段，一个典型的标志就是关于计算机安全的法律法规开始出现——1994年公安部颁布了“中华人民共和国计算机信息系统安全保护条例”。另一个中国安全产业起步的重要标志是，在这个时期中，许多企事业单位开始把信息安全作为系统建设中的重要内容之一来对待，加大了投入，开始建立专门的安全部门来开展信息安全工作。

21世纪的信息安全现状

（1）在密码理论与技术研究方面
RSA的快速实现和椭圆曲线公钥密码的快速实现方面都有所突破。
（2）在安全协议理论与技术研究方面
在理论研究方面和国际上已有协议的分析方面做了一些工作。
（3）在安全体系结构理论与技术研究方面
1999年10月发布了“计算机信息系统安全保护等级划分准则”。
（4）在信息对抗理论与技术研究方面
网络攻击研究刚刚起步。
（5）在网络安全与安全产品研究方面
目前国内已有一些网络安全解决方案和产品。
……我国信息安全的研究发展很快，但是很不平衡。有些方面达到了世界先进水，有些方面依然存在很大的距离。