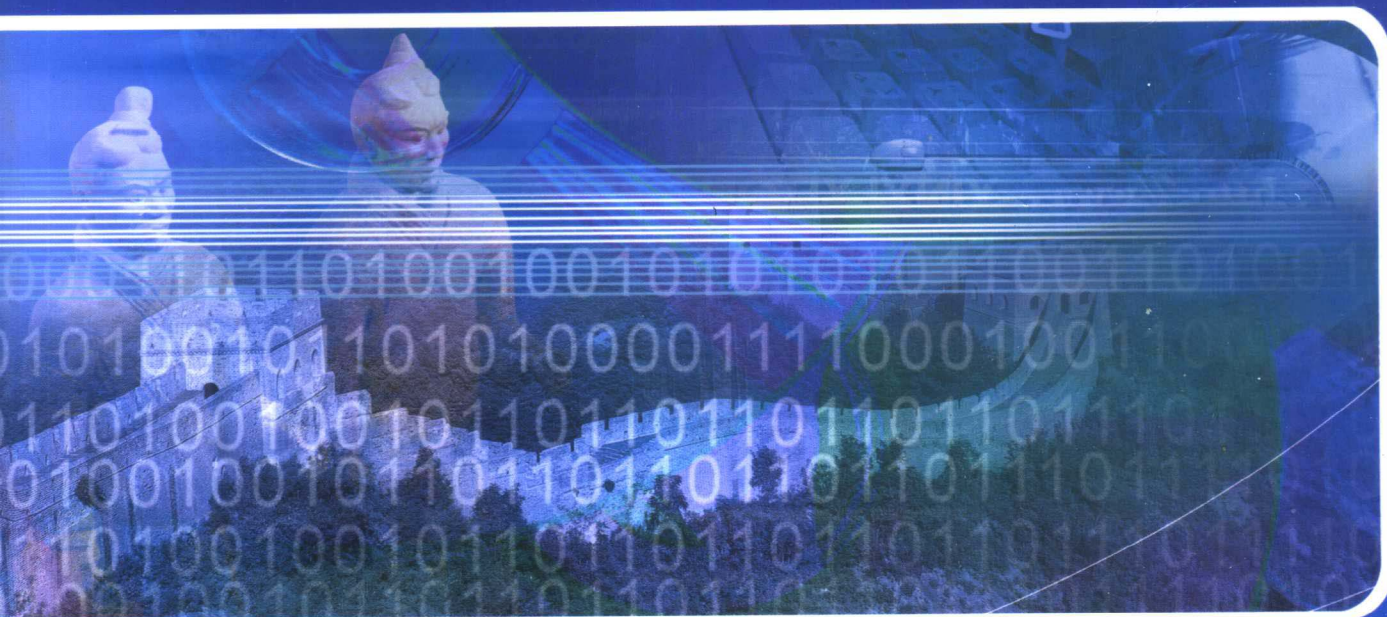


信息安全系列丛书



信息安全保密教程

XINXI ANQUAN BAOMI JIAOCHENG 下册

主编 赵战生 杜虹 吕述望

中国计算机学会信息保密专业委员会 组织策划

中国科学技术大学出版社
北京中电电子出版社

TP309

64

:2

信息安全系列丛书

信息安全保密教程

(下册)

主编 赵战生 杜虹 吕述望
中国计算机学会信息保密专业委员会 组织策划

中国科学技术大学出版社
北京中电电子出版社

总 目 录

上 册

序	(I)
总序	(III)
前言	(VII)
第 1 章 信息化与信息安全保密	(1)
1.1 信息化发展是先进生产力发展的必然	(1)
1.1.1 三次生产力革命	(1)
1.1.2 我国信息化发展历程概要	(3)
1.1.3 我国信息化发展对国民经济的深刻影响	(6)
1.2 电子政务是党政机关和各行各业信息化发展的历史重任	(7)
1.2.1 什么是电子政务	(7)
1.2.2 各国电子政务的发展	(7)
1.2.3 我国电子政务的发展	(9)
1.3 信息化的发展凸显了信息安全问题	(11)
1.3.1 生产力的成熟需要一个发展过程	(11)
1.3.2 黑客现象与信息犯罪	(12)
1.3.3 情报战与信息战	(15)
1.3.4 我国面临的严峻形势	(22)
第 2 章 信息安全保障框架	(28)
2.1 信息安全的基本概念	(28)
2.1.1 信息安全认识的发展阶段	(28)
2.1.2 信息安全的基本属性	(30)
2.1.3 信息和系统的生存状态和信息安全的生命周期	(32)
2.1.4 信息安全保障能力来源与构成	(33)
2.1.5 信息安全保障的工作环节	(34)
2.1.6 保密与信息安全	(38)
2.2 信息安全保障技术框架	(44)
2.2.1 ISO 开放式系统互连的安全体系结构	(45)
2.2.2 信息保障技术框架 (IATF)	(50)
第 3 章 信息安全保密管理	(70)
3.1 安全保密管理概述	(70)
3.1.1 安全保密管理概念	(70)
3.1.2 组织机构安全保密管理	(72)
3.2 信息安全管理的管理机构、职责及机制	(75)
3.2.1 国际信息安全管理的管理政策和机制	(75)
3.2.2 我国信息安全保密管理的管理政策和机制	(94)
3.3 涉密信息系统信息安全保密管理	(96)

3.3.1 信息安全保密管理的组织机构	(96)
3.3.2 管理的职责	(96)
3.3.3 管理的过程	(98)
3.3.4 管理的内容	(98)
第4章 信息安全保密法律、法规和标准	(106)
4.1 信息安全法律、法规	(106)
4.1.1 国际信息安全法律法规现状	(106)
4.1.2 中国信息安全法律法规现状	(108)
4.1.3 现有重要法律法规介绍	(111)
4.2 保密法律、法规	(118)
4.2.1 保密法	(118)
4.2.2 保密法实施办法	(122)
4.2.3 计算机信息系统国际联网保密管理规定	(125)
4.2.4 涉密信息系统审批办法	(126)
4.2.5 涉密信息系统集成资质管理办法	(126)
4.3 信息安全标准	(127)
4.3.1 国际信息安全标准现状	(128)
4.3.2 中国信息安全标准现状	(132)
4.3.3 国家信息安全标准	(133)
4.4 保密标准	(135)
4.4.1 保密标准工作概况	(135)
4.4.2 保密标准体系框架	(135)
4.4.3 管理类保密标准	(135)
4.4.4 产品类保密标准	(136)
第5章 信息安全等级保护与风险评估	(137)
5.1 国家信息安全等级保护制度	(137)
5.1.1 国外情况	(137)
5.1.2 国内信息安全等级保护工作的历史回顾	(140)
5.1.3 国家信息安全等级保护制度	(141)
5.1.4 国家信息安全等级保护的标准体系	(146)
5.2 涉密信息系统分级保护	(147)
5.2.1 涉密信息系统安全保密防护的现状	(147)
5.2.2 涉密信息系统分级保护的指导思想和基本原则	(147)
5.2.3 涉密信息系统分级保护的有关标准	(148)
5.3 信息系统安全风险评估	(148)
5.3.1 基本概念	(148)
5.3.2 国内外信息系统安全风险评估现状	(149)
5.3.3 作用和意义	(154)
5.3.4 工作流程	(155)
5.3.5 理论、工具和模式	(155)
5.4 涉密信息系统安全风险评估	(157)

5.4.1	作用和意义	(157)
5.4.2	测评方式	(158)
5.4.3	测评标准	(159)
5.4.4	测评结果的判定	(159)
5.4.5	测评与审批的关系	(161)
5.5	信息安全产品的测评认证	(161)
5.5.1	国外情况	(161)
5.5.2	国内情况	(163)
5.6	涉密信息安全产品的测评认证	(165)
5.6.1	作用和意义	(165)
5.6.2	测评机构	(165)
5.6.3	检测标准	(165)
5.6.4	工作流程	(166)
第6章	应急处理	(169)
6.1	应急响应概述	(169)
6.1.1	应急响应背景	(169)
6.1.2	信息安全与应急响应的关系	(170)
6.1.3	我国的应急响应体系现状	(170)
6.1.4	应急响应的国际组织结构	(171)
6.1.5	应急响应相关术语	(172)
6.2	应急响应策略	(173)
6.2.1	策略制定	(173)
6.2.2	策略更新	(173)
6.2.3	事件的分类及处理优先级	(174)
6.3	应急处理的准备工作	(174)
6.3.1	使安全事件的数量和严重性减至最小	(174)
6.3.2	组建核心计算机安全事件响应小组	(176)
6.3.3	制定应急响应计划	(176)
6.4	应急处理的流程和方法	(178)
6.4.1	识别事件	(178)
6.4.2	作出初步评估	(178)
6.4.3	通报发生的事件	(179)
6.4.4	控制损失并将风险减至最小	(179)
6.4.5	确定破坏的严重程度	(180)
6.4.6	保护证据	(181)
6.4.7	通知外部机构	(181)
6.4.8	恢复系统	(182)
6.4.9	编辑和整理事件记录资料	(182)
6.4.10	评估事件的破坏和代价	(182)
6.4.11	检查响应过程并更新策略	(183)
6.5	应急响应团队的组建	(183)

6.5.1 什么是应急响应团队?	(183)
6.5.2 为什么要组建应急响应团队?	(183)
6.5.3 组建应急响应团队的问题	(183)
6.5.4 应急响应团队的组成	(185)
6.5.5 规章制度	(187)
6.6 应急响应实例	(188)
6.6.1 大规模蠕虫事件处理	(188)
6.6.2 口令蠕虫事件	(188)
6.6.3 DDOS 事件处理	(189)
6.7 备份与存储安全	(189)
6.7.1 系统的备份	(189)
6.7.2 数据备份	(191)
第7章 信息系统安全工程	(196)
7.1 信息安全工程方法的发展	(196)
7.2 信息系统安全工程概述	(197)
7.2.1 信息系统安全工程基础——系统工程	(199)
7.2.2 系统安全工程	(202)
7.3 系统安全工程能力成熟度模型 (SSE - CMM)	(205)
7.3.1 SSE - CMM 简介	(205)
7.3.2 SSE - CMM 的系统安全工程过程	(207)
7.3.3 SSE - CMM 的主要概念	(209)
7.3.4 SSE - CMM 的体系结构	(210)
7.4 信息系统安全工程的生命周期模型	(215)
7.4.1 系统生命期内的 ISSE 流程	(215)
7.4.2 ISSE 管理过程	(217)
7.5 信息系统安全工程方法	(219)
7.5.1 安全规划与控制	(219)
7.5.2 安全需求的定义	(220)
7.5.3 安全设计支持	(220)
7.5.4 安全运行分析	(220)
7.5.5 生命周期安全支持	(222)
7.5.6 安全风险管理的	(222)
7.6 涉密信息系统安全工程	(222)
7.6.1 涉密信息系统安全保密工程概述	(223)
7.6.2 涉密信息系统资源及服务	(223)
7.6.3 涉密信息系统的安全风险分析	(226)
7.6.4 涉密信息系统的安全需求分析	(230)
7.6.5 涉密信息系统的安全规划与设计	(231)
7.6.6 现行涉密信息系统安全保密管理介绍	(233)
第8章 人的意识、培训和教育	(235)
8.1 信息安全道德规范	(235)

8.1.1 信息空间的道德规范	(235)
8.1.2 道德规范的历史和文化基础	(237)
8.2 信息安全意识	(238)
8.3 信息安全保障的培训	(241)
8.3.1 CISSP 培训课程	(243)
8.3.2 CIW 认证	(246)
8.3.3 Security + 考试	(248)
8.3.4 ISEC - 《国家信息安全教育认证培训》证书	(248)
8.4 信息安全保障教育	(255)
8.5 人员能力的成熟度	(257)
8.5.1 什么是人员能力成熟度模型	(258)
8.5.2 人员能力成熟度模型的体系结构	(258)
8.5.3 人员能力成熟度模型的利用	(263)
第9章 密码技术	(265)
9.1 密码技术概论	(265)
9.1.1 基本概念	(265)
9.1.2 密码体制分类	(266)
9.1.3 密码攻击概述	(266)
9.1.4 保密通讯系统	(267)
9.2 流密码	(268)
9.2.1 流密码基本概念	(268)
9.2.2 线性反馈移位寄存器、B - M 算法和线性复杂度	(271)
9.2.3 流密码的构造方法	(274)
9.3 分组密码	(276)
9.3.1 分组密码概述	(276)
9.3.2 DES 算法	(278)
9.3.3 IDEA 算法	(284)
9.3.4 线性密码分析与差分密码分析	(286)
9.3.5 分组密码运行模式	(287)
9.4 公钥密码	(289)
9.4.1 公钥密码概述	(289)
9.4.2 RSA 算法	(290)
9.4.3 椭圆曲线密码	(292)
9.5 杂凑函数	(295)
9.5.1 杂凑函数的定义	(295)
9.5.2 杂凑函数的攻击方法	(296)
9.5.3 MD5 算法	(297)
9.5.4 安全杂凑算法 (SHA)	(299)
9.5.5 杂凑函数的构造	(301)
9.6 数字签名与认证	(302)
9.6.1 数字签名的基本概念	(302)

9.6.2	数字签名标准	(302)
9.6.3	其他签名方案	(303)
9.6.4	认证协议	(304)
9.6.5	身份识别	(306)
9.7	随机数	(308)
9.7.1	随机数概述	(308)
9.7.2	随机数发生器	(308)
9.7.3	随机数发生器安全性评估	(309)
9.8	密钥管理	(310)
9.8.1	密钥的种类与生成	(310)
9.8.2	密钥的分发	(311)
9.8.3	密钥的保护	(313)
9.8.4	密钥托管	(314)
9.9	VPN 技术	(315)
9.9.1	VPN 概述	(315)
9.9.2	VPN 涉及的关键技术	(316)
9.9.3	VPN 组网方式	(316)
9.9.4	VPN 安全性分析	(317)
第 10 章	身份鉴别与访问控制	(318)
10.1	标识与鉴别	(318)
10.1.1	用户标识	(318)
10.1.2	用户鉴别	(319)
10.2	鉴别机制	(322)
10.2.1	基于口令的鉴别	(322)
10.2.2	基于令牌的鉴别机制	(327)
10.2.3	基于生物特征的鉴别机制	(333)
10.2.4	鉴别协议	(335)
10.2.5	可信第三方认证	(337)
10.2.6	PKI	(341)
10.2.7	单点登录 (SSO)	(350)
10.3	访问控制	(353)
10.3.1	定义	(354)
10.3.2	模型	(365)
下 册		
第 11 章	边界保护	(373)
11.1	边界保护的范畴	(373)
11.1.1	边界与边界保护	(373)
11.1.2	我国电子政务中安全域的划分	(373)
11.2	防火墙	(377)
11.2.1	防火墙的基本知识	(377)
11.2.2	防火墙体系结构	(381)
11.2.3	防火墙关键技术	(384)

11.2.4 防火墙的选择	(391)
11.2.5 防火墙的发展趋势	(393)
11.3 物理隔离	(399)
11.3.1 提出背景	(399)
11.3.2 物理隔离解决方案	(399)
11.4 安全隔离与信息交换	(402)
11.4.1 国外相关技术发展现状	(402)
11.4.2 安全隔离与信息交换的需求	(404)
11.4.3 安全隔离与信息交换系统	(405)
11.4.4 安全隔离与文件单向传输系统	(409)
11.4.5 安全隔离与信息交换技术发展与应用趋势	(410)
11.5 非法外联和非法接入监控	(412)
11.5.1 非法外联与非法接入的界定	(412)
11.5.2 非法外联与非法接入的监控	(412)
11.5.3 对要求物理隔离的网络的非法外联监控	(412)
11.6 其他安全网关	(413)
11.6.1 病毒网关	(413)
11.6.2 垃圾邮件过滤网关	(414)
11.6.3 保密网关	(417)
第12章 防病毒	(420)
12.1 计算机病毒概述	(420)
12.1.1 计算机病毒的历史	(420)
12.1.2 计算机病毒的定义	(421)
12.1.3 计算机病毒的破坏行为	(421)
12.1.4 计算机病毒的特征	(422)
12.1.5 计算机病毒的传播途径	(423)
12.1.6 计算机病毒的分类	(424)
12.1.7 计算机病毒感染征兆	(426)
12.1.8 计算机病毒的危害	(430)
12.2 病毒检测技术	(432)
12.2.1 计算机病毒扫描技术	(432)
12.2.2 消毒方法	(437)
12.3 防病毒系统	(437)
12.3.1 单机工作站	(437)
12.3.2 文件服务器	(438)
12.3.3 邮件服务器	(438)
12.3.4 防火墙网关	(438)
12.3.5 企业	(438)
12.4 典型病毒分析	(445)
12.4.1 首例破坏硬件文件型病毒—CIH	(445)
12.4.2 首例病毒与蠕虫结合的“病毒”—Sircam	(446)

12.4.3	首例蠕虫与黑客相结合的“病毒”—Code red II	(448)
12.4.4	VBScript 病毒—VBS/Redlof 蠕虫	(450)
12.4.5	“秋天的童话”病毒	(451)
12.4.6	“诺维格”(Novarg/Mydoom)	(453)
12.4.7	冲击波 (mblander) 蠕虫	(455)
12.4.8	振荡波病毒	(456)
第 13 章	入侵检测	(459)
13.1	入侵检测出现的意义	(459)
13.1.1	数字化攻击的严重性	(459)
13.1.2	黑客攻击日益猖獗	(460)
13.1.3	传统信息安全技术的发展形势	(461)
13.2	入侵检测系统概述	(463)
13.2.1	入侵检测相关术语	(463)
13.2.2	IDS 在网络安全体系中的角色和作用	(463)
13.2.3	IDS 系统的分类	(464)
13.2.4	IDS 的优势和局限	(465)
13.2.5	入侵检测系统的发展历程	(469)
13.3	入侵检测技术	(469)
13.3.1	异常检测技术	(470)
13.3.2	误用检测技术	(472)
13.3.3	商业入侵检测系统的实用技术	(474)
13.4	IDS 的主要性能和功能指标	(477)
13.4.1	系统结构	(477)
13.4.2	事件数量	(478)
13.4.3	处理带宽	(479)
13.4.4	通讯安全	(479)
13.4.5	事件响应	(480)
13.4.6	自身安全	(482)
13.4.7	终端安全	(483)
13.4.8	事件库更新	(485)
13.4.9	易用性	(485)
13.4.10	日志分析	(486)
13.4.11	资源占用率	(486)
13.4.12	抗打击能力	(486)
13.5	IDS 发展趋势	(487)
13.5.1	HIDS 和 NIDS 技术进一步融合	(487)
13.5.2	IDS 厂商与 OS 提供商的进一步合作	(487)
13.5.3	不同厂商产品的互操作的标准化	(487)
13.5.4	入侵追踪、起诉的支持	(487)
13.5.5	数据源的可欺骗性	(487)
第 14 章	漏洞扫描	(489)

14.1	漏洞扫描基本概念	(489)
14.1.1	漏洞的概念	(489)
14.1.2	漏洞如何出现	(490)
14.1.3	操作系统体系结构的安全隐患	(490)
14.1.4	漏洞对系统的威胁	(492)
14.1.5	漏洞扫描器	(492)
14.2	黑客攻击	(493)
14.2.1	攻击的分类	(493)
14.2.2	黑客进入系统的主要途径	(494)
14.2.3	攻击步骤	(494)
14.3	协议脆弱性分析及利用	(501)
14.3.1	NetBIOS (NetBEUI) 脆弱性分析	(501)
14.3.2	Telnet 协议脆弱性分析	(503)
14.3.3	FTP 协议脆弱性分析	(504)
14.3.4	DNS 协议脆弱性分析	(507)
14.3.5	SMTP 协议脆弱性分析	(513)
14.3.6	SNMP 协议脆弱性分析	(514)
14.3.7	Web 漏洞扫描	(514)
14.4	网络漏洞扫描技术	(516)
14.4.1	获取服务版本	(516)
14.4.2	发送扫描探测包	(517)
14.4.3	模拟客户尝试与服务器连接	(517)
14.4.4	模拟攻击	(517)
14.4.5	Web 漏洞扫描技术	(517)
14.5	扫描系统设计与实现	(519)
14.5.1	扫描器类型	(519)
14.5.2	网络漏洞扫描器的总体结构	(520)
第 15 章	物理安全	(523)
15.1	基本概念、作用、分类	(523)
15.2	环境安全	(523)
15.2.1	机房与设施安全	(523)
15.2.2	环境与人员安全	(531)
15.2.3	防其他自然灾害	(533)
15.3	设备安全	(537)
15.3.1	防盗和防毁	(537)
15.3.2	防止电磁泄漏发射	(538)
15.3.3	防电磁干扰	(538)
15.4	介质安全	(542)
15.4.1	介质的分类	(542)
15.4.2	介质的防护要求	(542)
15.4.3	介质的管理	(543)

第 16 章 电磁兼容与电磁泄漏发射	(546)
16.1 电磁兼容	(547)
16.1.1 电磁兼容基本概念	(548)
16.1.2 电磁兼容对运行安全的影响	(550)
16.2 TEMPEST 基本原理	(551)
16.2.1 电磁泄漏发射的机理与特点	(554)
16.2.2 EMI 技术与 TEMPEST 技术的联系和区别	(556)
16.2.3 电磁泄漏发射的测试与评估	(557)
16.3 电磁泄漏发射防护技术	(567)
16.3.1 低泄射技术	(567)
16.3.2 屏蔽技术	(567)
16.3.3 干扰技术	(568)
16.3.4 系统防护技术	(569)
16.4 电磁泄漏发射防护要求	(570)
16.4.1 标准与等级区分	(571)
16.4.2 测评认证体制	(572)
第 17 章 基础部件安全	(575)
17.1 操作系统安全	(575)
17.1.1 操作系统概述	(575)
17.1.2 安全操作系统及其评估标准	(576)
17.1.3 Windows2000/xp 安全	(581)
17.1.4 Linux 操作系统安全	(586)
17.1.5 国产操作系统及国产安全操作系统的发展概况	(592)
17.2 数据库安全	(593)
17.2.1 数据库系统基本概念	(593)
17.2.2 数据库安全标准与对策	(596)
17.2.3 主流 DBMS 的安全性	(600)
17.2.4 数据库安全的研究难点与发展趋势	(605)
17.2.5 数据库安全综述	(606)
17.3 终端安全	(607)
17.3.1 终端安全的现状和意义	(607)
17.3.2 可信计算平台	(609)
17.3.3 终端安全技术概述	(611)
17.3.4 LT 技术和 NGSCB 计划介绍	(613)
第 18 章 安全监控与审计	(619)
18.1 安全监控	(619)
18.1.1 基本概念、作用、分类	(619)
18.1.2 设备安全监控	(619)
18.1.3 网络端口安全监控	(621)
18.1.4 网络协议安全监控	(623)
18.1.5 安全监控基本模型	(626)

18.2 安全审计	(627)
18.2.1 基本概念、作用、分类	(627)
18.2.2 网络审计	(628)
18.2.3 主机审计	(629)
18.2.4 数据库审计	(629)
18.2.5 应用审计	(630)
18.2.6 综合审计	(630)
18.2.7 分级审计	(630)
18.2.8 强审计	(630)
18.2.9 安全审计基本模型	(630)
第19章 信息隐藏技术	(632)
19.1 信息隐藏的含义与方法	(632)
19.1.1 信息隐藏的概念及其含义	(632)
19.1.2 信息隐藏技术方法简介	(634)
19.2 信息隐藏的应用领域	(650)
19.2.1 隐写术的应用领域	(650)
19.2.2 数字水印的应用领域	(651)
19.2.3 其他应用领域	(651)
19.3 信息隐藏的未来发展	(653)
19.3.1 传统的信息隐藏技术	(653)
19.3.2 信息隐藏技术的发展	(654)
第20章 其他信息安全保密技术	(658)
20.1 防窃听技术	(658)
20.1.1 电话线路(通信线路)窃听与防护	(658)
20.1.2 场所窃听与防护	(661)
20.1.3 无线(移动)通信信号接收破解与防护	(667)
20.2 防窃照技术	(673)
20.2.1 固定位置窃照技术与防护	(673)
20.2.2 手持小型窃照装置和检测防护技术	(675)
20.3 防复印技术	(678)
20.3.1 防复印纸张	(679)
20.3.2 防复印涂料	(680)
20.4 磁介质信息的可靠消除	(680)
20.4.1 软盘涉密信息的消除	(680)
20.4.2 硬盘涉密信息的消除	(680)

第 11 章 边界保护

11.1 边界保护的范畴

11.1.1 边界与边界保护

边界是地区与地区之间的界线，人们通常采取法律、巡视、构筑防护墙、设立关口等手段来保护边界。网络建立的初衷原本是要打破边界实现互通，但现实的生活使得我们不得不考虑网络世界的边界及边界保护问题。

网络的边界虽然没有一条明显的界线，但是从使用者的立场出发，通常可以分为内网和外网，而其边界就是所界定的内网与外网的连接点，通常是网关和诸如拨号、跨网连接的连接点。边界的保护就是要保护被保护的网（通常是内网）合法访问者可以通过边界访问被保护网络的合法资源，同时防止非法访问者对被保护网络的攻击、入侵、资源窃取等。目前，成熟的主要网络边界保护措施有：防火墙、物理隔离、安全隔离与信息交换、非法外连和非法接入监控、防病毒网关、保密网关。

为了大家能够更好地理解边界保护，下面先以我国电子政务安全域的划分为例来加以说明。

11.1.2 我国电子政务中安全域的划分

11.1.2.1 基本概念

一般来说，越高层权力机构的网络处理涉及国家秘密的信息机会越多，安全保密的需求越多，对公共服务的需求越少；越低层权力机构的网络处理涉及国家秘密的信息机会越少，安全保密的需求越少，对公共服务的需求越多，如图 11-1 所示，因此，网络隔离是必然之举。

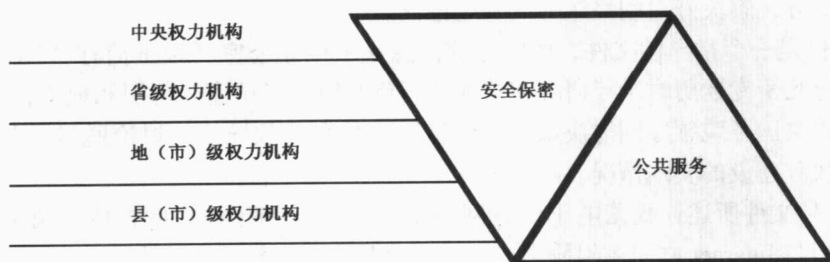


图 11-1 电子政务中安全保密与公共服务的关系

网络隔离的基本思想就是将一个庞大而复杂的网络系统的访问控制分解成一些小的、简

单一的网络系统的访问控制,从而使整个网络的访问控制易于实现、监督和测评。

这里需要明确一些基本概念:

1. 涉密网络:涉及国家秘密的计算机信息网络。
2. 物理隔离:两个网络通过各自拥有独立的传输介质系统实现的隔离。例如:各自拥有独立布线系统的局域网之间是物理隔离的,而通过防火墙等设备和公网隔离不是物理隔离;
3. 逻辑隔离:拥有相同传输介质系统的两个网络之间,通过硬件设备或软件措施实现的某种隔离。这些硬件设备如防火墙、网关等,软件措施如划分不同的网段或 VPN 等。
4. 安全隔离:由安全设备和安全线路组成的系统,用于涉密网络与外网之间、涉密网之间、安全域之间、安全圈之间的隔离。
5. 安全域:根据信息涉及国家秘密的程度进行划分的网络空间。

一个安全域可能是一个局域网或几个局域网组成的园区网。一个安全域须有以下六个参数描述确定:

- 1) 安全域名:唯一标识该安全域的代码或名字;
- 2) 安全策略:适合于该安全域的一组安全规定;
- 3) 安全域范围:用来与其它安全域进行区分的网络边界、应用边界和人员边界;
- 4) 身份认证系统:能对本安全域合法用户进行身份识别的系统;
- 5) 进出口:进出该安全域的网络接口;
- 6) 安全域级别:该安全域的级别。

11.1.2.2 我国电子政务中安全域的划分

根据我国信息化的实际发展情况,特别是在电子政务建设中,可大致划分三个安全域(如图 11-2 所示):

1. 涉密域:涉及国家秘密的网络空间;
2. 非涉密域:不涉及国家秘密,但涉及本单位、本部门或本系统的工作秘密的网络空间;
3. 公共服务域:不涉及国家秘密,也不涉及工作秘密,但涉及个人秘密(或个人隐私)和企业敏感信息的网络空间。

11.1.2.3 安全域与网络的关系

2002 年中共中央办公厅第 17 号文件《国家信息化领导小组关于我国电子政务建设指导意见》(以下简称 17 号文件)的发布,标志着我国电子政务建设已经进入全面建设阶段。电子政务系统建设中安全保密问题突出,需要加强研究和管理^[6]。政务系统建设中需要把握好合理的网络划分,解决好对网络边界的安全控制。

17 号文件是一个指导性文件,由国务院信息化工作办公室(以下简称“国信办”)组织几十位专家分几个专题历时半年研究起草而成,反复听取了国家各部门和地方各省市的意见,关键问题由中央国务院领导同志决策,最后经国家信息化领导小组讨论通过。总体上完全符合我国电子政务建设的实际情况。

根据 17 号文件所述,我国电子政务网络由政务内网和政务外网构成,两网之间物理隔离,政务外网与 Internet 之间逻辑隔离。这一划分是中央领导同志的决策,主要考虑了安全保密问题。即信息是否涉及国家秘密目前较难划分,暂不宜完全按涉密网与非涉密网进行划分。另外,政务内网不连到地市,既有利于安全保密,也防止电子政务建设一哄而上,造成盲目建设。

1. 政务内网是副省级以上政府部门的办公网,属于涉密网络,与副省级以下政府部门的

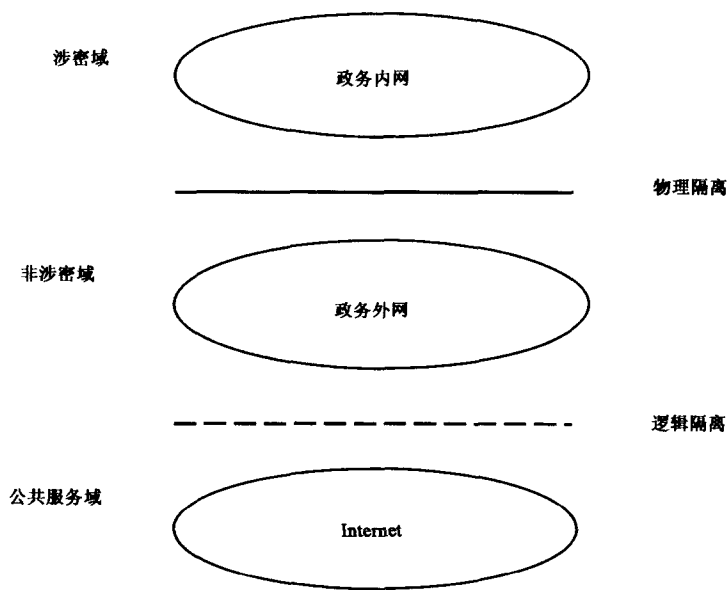


图 11-2 安全域与网络的关系

办公网物理隔离，同时也与 Internet 物理隔离，如图 11-3 所示。

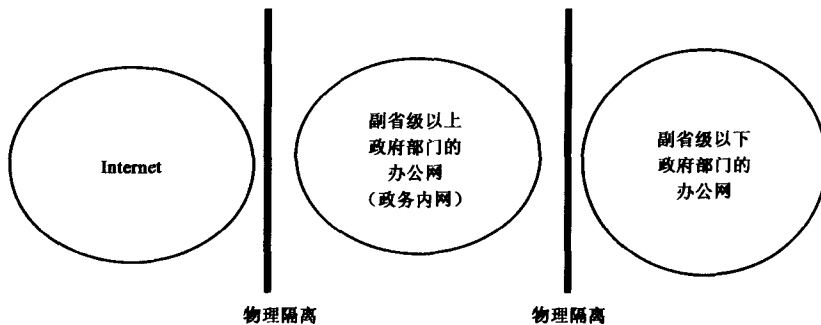


图 11-3 政务内网与 Internet、副省级以下政府部门的办公网物理隔离

2. 政务外网是非涉密网，是政府的业务专网，主要运营政府部门面向社会的专业性服务和不需要在内网运行的业务。涉及国家秘密的信息不能在政务外网上处理，属于工作秘密和敏感信息可以在政务外网处理。政务外网与政务内网物理隔离，与 Internet 逻辑隔离。

3. 这一划分方法可能存在以下两个问题：

1) 由于政务内网定义为副省级以上政务部门的办公网，是按行政级别划分的，而不是按涉密划分的，可能会造成涉密网络一定程度的扩大化。带来增加建设费用，增大保密管理难度的问题。

2) 有的信息化发展较快的省，网络已经连到地市了，有的还是经保密部门审批的，已经达到保密要求。省与地、市两级断开，不利于信息沟通。

解决问题的指导思想很明确：总的思路要符合 17 号文件精神，具体问题具体分析，解决实际问题要从实际出发，满足实际需求。

11.1.2.4 网络的定位与管理

1. 政务内网

政务内网属于涉密网络，涉密网络就是处理涉及国家秘密的网络。凡是涉及国家秘密的事项和“密”与“非密”区分不清的信息都在政务内网处理。

为确保国家秘密信息安全，内网的范围要适度，“避免内网盲目扩大化的倾向”。政务内网盲目扩大化，也难于“保障安全”。

对于涉密信息系统，《中共中央关于加强新形势下保密工作的决定》明确规定：涉及国家秘密的通信、办公自动化和计算机信息系统的建设，必须与保密设施的建设同步进行，报经地（市）级以上保密部门审批后，才能投入使用。国家保密局近几年为贯彻中共中央的决定制定了一系列的法规、标准。政务内网是涉密网，因此政务内网的建设和管理应按照国家保密局的一整套规范去要求：涉密信息系统建设、管理全过程是：资质管理→技术要求→方案设计→工程监理→安全保密测评→审批管理→日常检查。

2. 政务外网

政务外网是非涉密网，既然是非涉密网，涉及国家秘密的信息就不能上政务外网。

所谓国家秘密就是按保密法和定密办法确定为秘密、机密、绝密三级的国家秘密事项。有些属于工作秘密和敏感信息是可以在政务外网运行的。国家秘密一定要在政务内网中处理，有些信息不易分清是否是国家秘密的也放在政务内网中处理；但确属不是国家秘密的，而又有必要在政务外网运行的，不管是你部门认为是工作秘密也好，敏感信息也好，均可在政务外网运行。17号文件指出：“政务外网主要运行政府部门的面向社会的专业性服务业务和不需要在内网上运行的业务”的含义就是没有必要在内网上运行的业务都可拿到外网去。电子政务体现监管和服务的功能还靠政务外网，要充分发挥好它的作用。

政务外网尽管不处理国家秘密，但其安全保密问题也很重要。因为政务外网与互联网是逻辑隔离的，遭受攻击的风险可能更大。国信办正在组织制定相关的建设标准，准备拿出管理办法和要求。按照安全等级划分，采用“分级保护、适度安全、促进发展”的思路去做。

11.1.2.5 政务内网的划分与连接

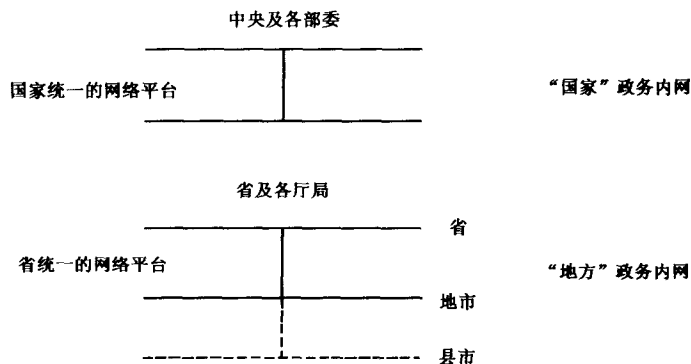


图 11-4 政务内网的划分与连接

17号文件提出“政务内网主要是副省级以上政务部门的办公网”。中央的网络连接到副省级以上的党和政府的办公厅应是明确的，但没有明确是否连到副省级以上政府的各厅、局，应理解为应该连到副省级以上政府的各厅、局。因为省级政府是由省政府办公厅和各厅局构