信息安全系列丛书

ISCCF

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

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

下 册

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络（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。

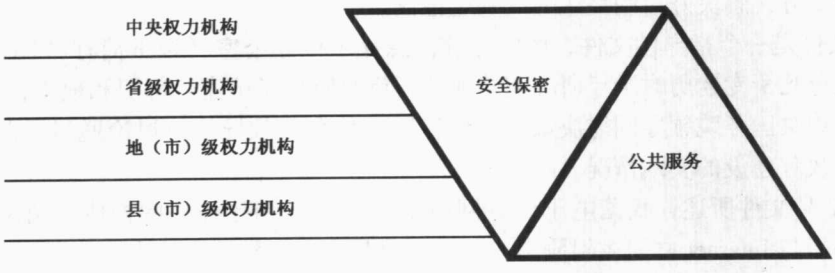

图 11 -1　电子政务中安全保密与公共服务的关系

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

单一些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）进出关口：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

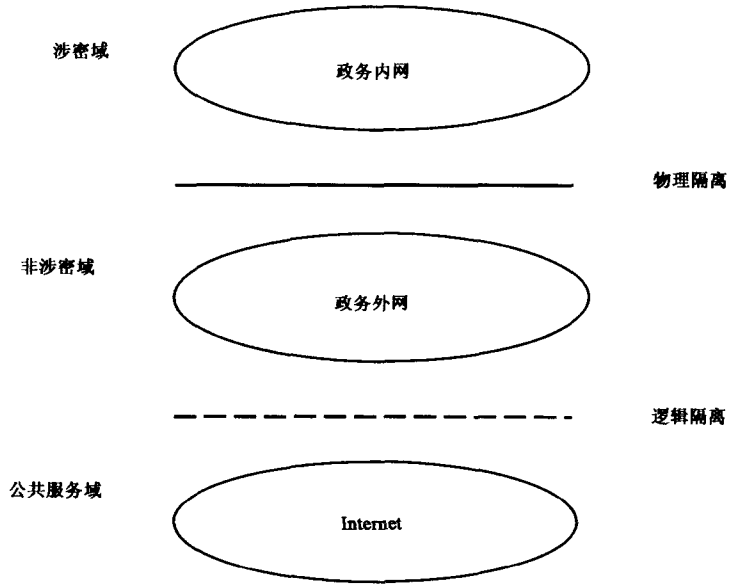

图 11－2　安全域与网络的关系

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

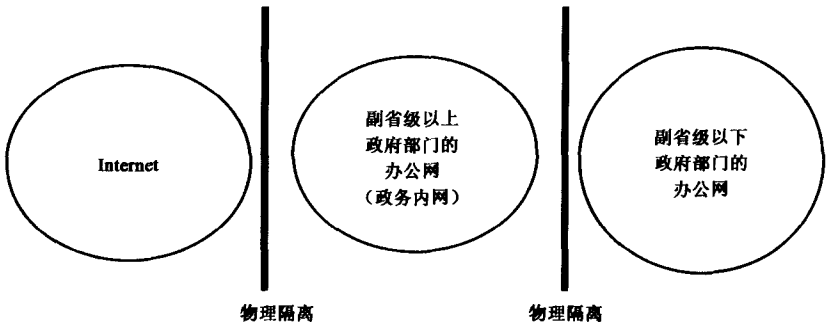

图 11－3　政务内网与 Internet、副省级以下政府部门的办公网物理隔离

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

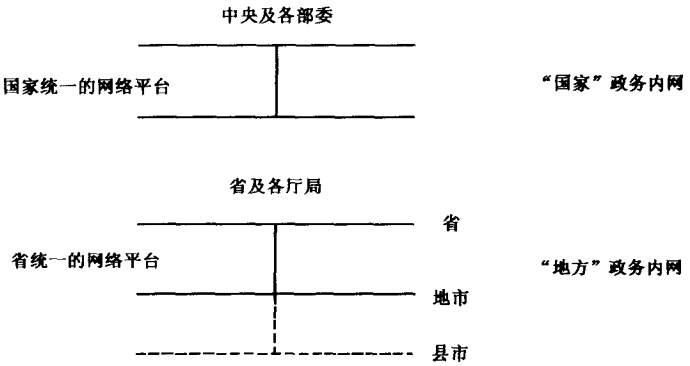

图 11－4 政务内网的划分与连接

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