信息安全系列

信息保障技术框架（3.0版）

美国国家安全局◇发布

国家973信息与网络安全体系研究课题组◇组织翻译

北京中软电子出版社

TP393.08
N147

信息保障技术框架

（3.0版）

美国国家安全局 发布
国家973信息与网络安全体系研究课题组 组织翻译

本书附盘可从本馆主页 http://lib.szu.edu.cn/
上由“馆藏检索”该书详细信息后下载，
也可到视听部复制

中软电子出版社

版权所有　翻版必纠

书　　名：信息保障技术框架(3.0 版)
总 策 划：曾传辉
作　　者：美国国家安全局　发布
责任编辑：邵祖英　高伟红
责任校对：柯　文
装帧设计：曾传辉
出版发行：北京海淀区学院南路 55 号中软大厦 B 座五层
电　　话：010 - 62147079　010 - 51527258(传真)
电子邮件：chzeng@163.net
经　　销：各地新华书店、软件连锁店
文本印刷：深圳宝峰印刷有限公司
光盘生产：华韵影视光盘有限责任公司
开本规格：787 毫米 × 1092 毫米　1/16 开本　33 印张　770 千字
版次印次：2002 年 4 月第一版　2002 年 4 月第一次印刷
印　　数：0001 - 1500 套
本 版 号：ISBN 7—900057—09—9
定　　价：180.00 元(含精装配套书、1CD)
说　　明：凡本社配套图书、光盘若有自然破损、缺页、脱页，本社负责调换。

目　　录

第一章　介　　绍

第二章　深度防御目标纵览

第三章　信息系统安全工程

第四章 技术性安全对策

此为试读,需要完整PDF请访问: www.ertongbook.com

第七章 保护计算环境

第八章　支撑性基础设施

第九章　战术环境的信息保障

第十章　对综合解决方案的观察

附　录

光盘内容

1. 信息保障技术框架英文版 2.0.1
2. 信息保障技术框架英文版 3.0
3. 保卫美国的计算机空间 - 信息系统保护国家计划(2000.1)
4. 保卫美国的计算机空间 - 信息系统保护国家计划英文版(2000.1)
5. 克林顿政府对关键基础设施保护的政策:第 63 号总统令
6. 克林顿政府对关键基础设施保护的政策:第 63 号总统令英文版

第一章　介　绍

信息保障技术框架(IATF)要解决下列问题：

- *我应怎样去定义信息保护的需求与解决方案？*
- *现有何种技术能够满足我的保护需求？*
- *什么样的机构资源能够帮我找到所需的保护？*
- *当前有哪些类型的信息保障(IA)产品与服务的市场？*
- *信息保障方法与技术的研究重点是什么？*
- *信息保障的原则是什么？*

这篇不断发展的文档的发布旨在向系统安全工程师及从事信息保障的其他人员提供对当前信息保障焦点问题和实践的建议与信息。随着时间的推移，它将反映出政策、技术、环境和信息系统使用等方面的变化情况。

1.1　目　的

本框架的目的是：

- 增强信息系统用户对信息保障技术的意识；
- 标明与国家政策相一致的信息保障所需要的技术解决方案；
- 使用“深度防御”战略的技术焦点域来定义信息保障方法；
- 定义不同条件和任务(称为“案例”)所需的安全功能与保护级别；
- 展示信息系统用户的信息保障需求；
- 强调信息保障组或信息系统安全专家在解决紧要安全问题时的重要性；
- 通过强调当前商业与政府保护技术领域所存在的某些缺陷，帮助开发能够满足信息保障需求的信息保障解决方案；
- 通过提供技术指南、权衡目前可用的解决方案(技术级而非产品级)和描述所期望的解决方案应具备的特征来指导解决信息保障问题；
- 帮助信息保障产品的购买方依据所需考虑的重要的与安全相关的特性进行决策。

1.2 预期读者

本框架适用于各种不同人员。下面分别描述这些人的不同需求并说明如何使用本文档:

- **系统安全工程师**:帮助开发信息保障解决方案,使其符合特定客户的需要。将客户的需要与各IATF技术域、案例和推荐的解决方案进行比较,以便开发出一个符合该客户需要的解决方案;
- **客户**:针对涉及到为系统与网络选择具备足够信息保障特性与保障级别的大量问题与技术挑战提供答案。客户包括系统用户、管理人员以及安全官员或安全管理员。在具备相关知识的基础上,客户能够很好地与安全工程师和结构设计者一起设计出一个全面的IA解决方案;
- **科学工作者和研究人员**:关注的问题是如何满足现有技术尚无法达到的客户需求。因此,本框架强调将信息保障技术推向未来,定义政府与商业研究实体要解决的技术空白;
- **商业产品和服务供应商**:洞察客户的需求。工业行业将会获得信息保障产品和服务当前和未来市场的趋势;
- **标准化团体和工业联盟**:为制定商业产品标准而提供指导。客户基上的一个着重点是关注那些由商业标准所驱动的商业产品的使用。IATF强调了现有标准化中的空白,这将有助于人们去关注那些影响标准化团体的努力。

1.3 背景情况

1.3.1 定义信息基础设施

IATF建立在信息基础设施的概念上。信息基础设施包括通讯网络、计算机、数据库、管理、应用和消耗性电子器件。它可以建立在全球、国家或本地的级别上。全球信息基础设施不受某个机构的控制或归其所有。它的"所有权"分布于公司、院校、政府机构以及个人。Internet就是一个全球信息基础设施,也是全球通讯网络。大多数对外联络通信的机构都依靠这个全球系统,结合他们的全球网络、虚拟网络、专用网、广域网(WAN)及客户化的信息系统来处理他们的商业。

一个国家信息基础设施是一个由国家使用并实现政府或商业事务的信息基础设施联合体。典型的国家基础设施比如美国的63号总统决议令(PDD63)所定义的关键基础设施。在跨国公司发展起来之前和Internet时代到来之前,是很容易识别出国家信息基础设施的。可是,在过去这十年中全球与国家信息基础设施之间的界限已经明显地模糊起来。每个国家都需要确定是否仍有必要对这两者加以区分;如果有必要,则需要依据标准对资源进行分类,定义归属"国家"信息基础设施的部分。目前美国可能是以某项资源是否属于美国法律、法规和政策为划分标准。

此为试读,需要完整PDF请访问: www.ertongbook.com

本地信息基础设施是一个机构在实现其商业时所使用的专用资源。这些资源主要包括商业信息系统、网络技术和应用。本地信息基础设施的所有者或运行者负责在该基础设施中应用安全措施。这些所有者或运行者可以是某个机构，也可以是某个机构中的一个商业团体。

1.3.2 信息和信息基础设施分类

在机构内部，要使用系统资源进行处理的信息依据其功能被分为如下几类：管理、人事、后勤等等。一些信息可能是公用的，而另一些则是秘密的。秘密信息有许多类型；公司有不同类型的专有信息，政府有执法、秘密信息、绝密信息以及受限的敏感信息等具有不同密级的信息。如上划分的信息可用性又称“信息域”。

为完成各种任务并保护关键功能，包括政府部门与专有机构在内的所有机构都有其需要保护的公共和秘密信息。任务或商业环境决定了保护具体信息的方式与程度。被允许以公开方式发送给某个机构的信息对另一个机构而言可能具有保密性，反之亦然。联邦政府以“带密级的信息”为标题依据其专用分类标准规定了一些联邦政府专用信息的密级。一般地，这些密级按照秘密程度由低到高的次序分为以下 4 种：无密级（unclassitied）、秘密（secret）、机密（confidential）与绝密（top - secret）。在各级别中可能有用于特定团体的子级别。秘密、机密与绝密这三个密级均指的是保密信息，另一密级则包括了一些专有信息（如：敏感信息或隐私法案所规定的信息）和一些公共信息。

有几类信息被认为是专有信息，例如执法信息。如果对之保护或处理不当，可能会破坏执法效果。对于商业团体，专有信息同样如此。这些信息一旦泄露便可能威胁该团体的商业利益。隐私法案所涉及的信息包括个人资金情况、医疗状况与其它具有敏感性的信息。通过不同的机构与部门，联邦政府掌握着用于支持研究项目、工程、后勤保障以及管理与获取功能的许多敏感信息。

多数机构对于其专有信息的保护都有比公共信息保护更为严格的要求。首先，对这些信息的访问是受到控制的。例如，某机构人力资源或财务部的职员可能具有对于个人和工资数据库与服务器的完全访问权限，但他们无法访问最具敏感性的研究与开发信息。在涉密的政府领域中，这一要求通过密级划分、特殊限制与“应需可知”（need to know）的标示得以实现（图 1 - 1）。

除访问控制外，还要实施更强健的技术性安全措施。多数机构都承认向公众泄露其专有信息将会造成巨大的潜在损失。因此，他们愿意增加额外的安全保护费用。最严格的安全措施将被用于与图 1 - 1 所示顶部三角形相关的信息与信息基础设施。

依据访问控制、需要和保护需求对信息进行划分便产生了不同的信息类别，又称信息域。机构将实施具体的机制以进行信息划分，并在信息域之间实现有意的信息流动。

在协作环境中进行信息保护具有着挑战性。共享信息的机构需要取得对信息的敏感级别和保护信息的方法一致性意见。通常，不同机构对于信息的敏感程度有不同理解，信息共享的各方需要派代表进行协商，并在此基础上得出一个各方均满意的解决方案。这种情况经常发生在共享专有信息的公司之间、参与同一个项目的政府机构之间和两个国家之间。

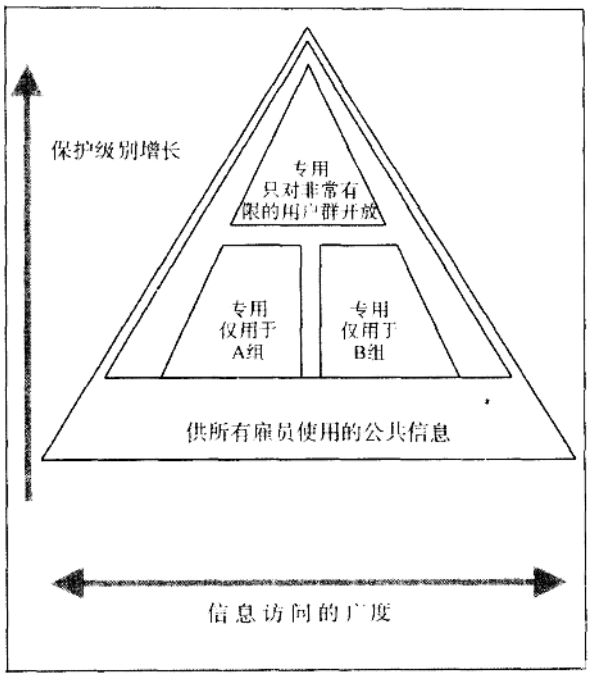

图 1-1 可用性与保护需求

1.3.3 边界和信息基础设施

在考虑信息基础设施的安全时,重要的问题在于对"边界"这一概念的理解。信息资源具有其物理和逻辑位置,而边界就位于这些位置之间。对于应该保护哪些资源使其不受外界影响的理解能够有助于确保在最恰当的地方采取保护措施并获得最好的效果。但是,在分析真实世界中的事例时,边界的识别并不容易。边界有时被定义为与一个物理位置相关的物理人、信息和信息系统。但该定义忽略了如下事实:在单一的位置上可能有许多不同的安全策略,某些策略涉及公共信息,而某些策略则涉及专有信息。

有时,"边界"被定义为受单一位置内一个策略控制的信息和信息系统的外缘。该定义没有考虑到策略超出物理边界的事实。更复杂的是,单个机器或服务器可能同时包括了公共信息和专有信息。因此,在单个机器中可能有多个边界。图 1-2 显示出这些与边界的定义相关的复杂情况。该图显示的是某个机构的设备位于两个物理位置,各设备均处理着不同级别的信息。此外,专用网也与 Internet 相连。在这种情况下,可以认为物理位置是一个边界,而逻辑边界则与不同级别的信息相关。

1.3.4 信息保障框架域

考虑到信息系统的复杂性,讨论如何保护它们是具有挑战性的,除非使用一个通用的框架。IATF 所用的框架将信息系统的信息保障技术层面分为如图 1-3 所示的四个域:

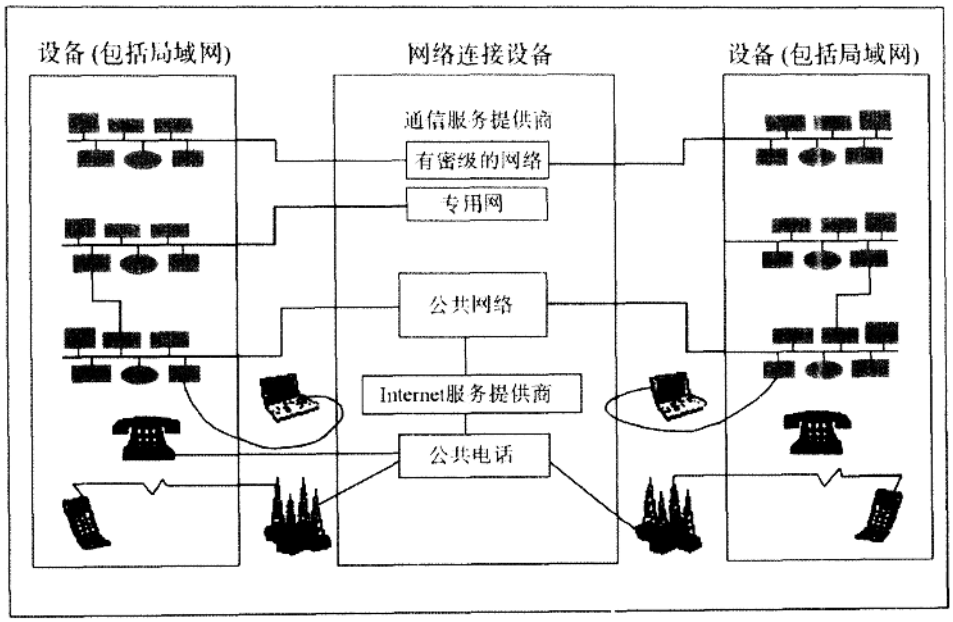

图 1-2 信息基础设施元素

- 局域计算环境;
- 飞地(enc lave)边界(局域计算环境的外缘);
- 网络和基础设施;
- 支撑性基础设施。

上述划分有助于我们重点讨论信息系统的信息保障技术层面并对其做出更清楚地展示。但是,这些层面互有重叠。针对某个信息系统实施的有效的信息保障涉及在整个信息系统的所有四个技术框架域中彼此关联的行为。下文将进一步描述这四个框架域。

局域计算环境框架域

局域用户计算环境如图 1-4 所示。它包括服务器、客户以及其上所安装的应用程序。这些应用程序能够提供包括(但不仅限于)调度(或时间管理)、打印、字处理或目录在内的一些服务。

综观计算环境范围,一个机构所使用的信息系统通常有若干类。专有机构与政府机构都曾经为满足特定的任务或商业需求而花费巨资和若干年时间进行信息系统的开发。这些系统仍在使用过程当中。许多机构都投入了大量资金使用商业现货(COTS)产品或能够满足其具体需要的客户版 COTS 信息系统组件与产品。当客户版 COTS 产品能够直接符合这些机构的使用要求时,他们将可能转而采用全面的 COTS 实现方式。

多数机构希望使用多种应用来实现他们操作任务功能,从而促使用户去努力将持续增长的应用集成到有效的信息处理能力当中。各种应用都将对支撑性基础设施提出了要求。

在不同的计算环境中,客户方均需要能够应用于现有应用范围的信息保障解决方案。计算环境的安全强调服务器和客户,包括其上安装的应用程序、操作系统和基于主

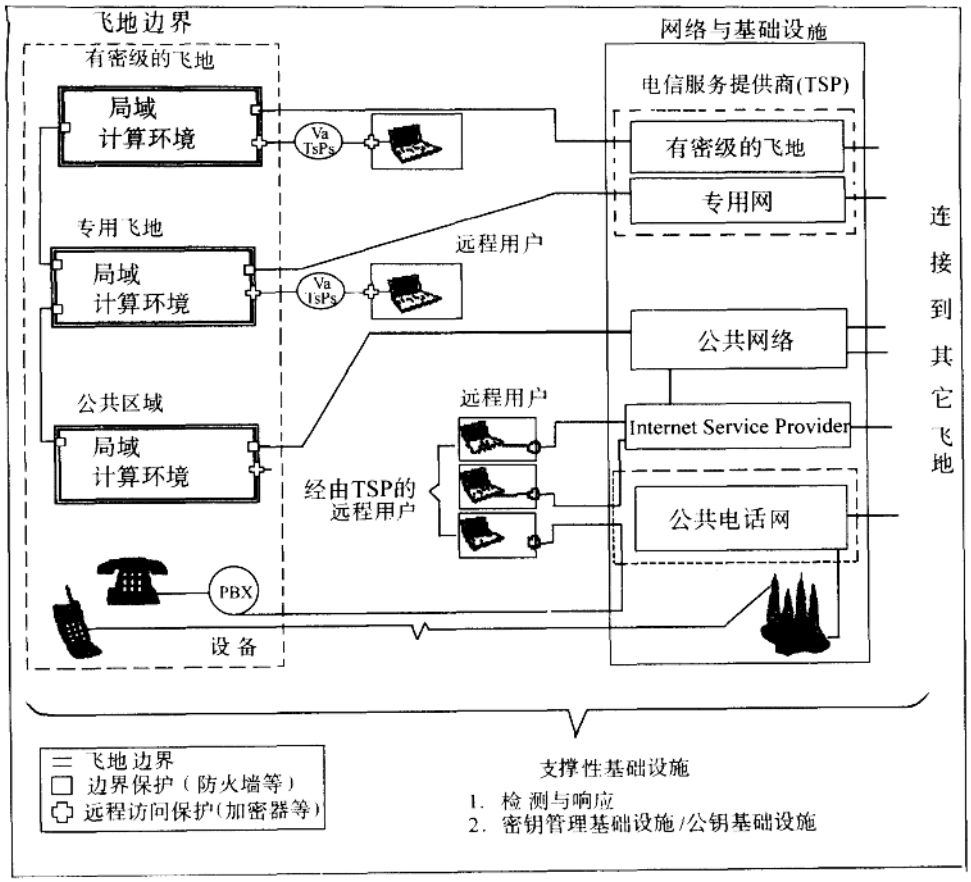

图 1-3 信息保障技术框架范围

机的监视器性能。需要信息保障解决方案的应用也包括如下各方面:

- 通信,如电子邮件;
- 操作系统;
- Web 浏览器;
- 电子商务;
- 无线访问;
- 联合计算;
- 数据库访问;

飞地边界框架域

"飞地"指的是通过局域网相互连接、采用单一安全策略并且不考虑物理位置的本地计算设备的集合。如上所述,由于安全策略独立于所处理信息的类型或级别,单一物理设备可能位于不同的飞地之内。本地和远程元素在访问某个飞地内的资源时必须满足该飞地的安全策略要求。如图 1-5 所示,单一飞地可以跨越多个不同地理位置并通过 T-1、T-3 或综合服务数字网(ISDN)等商用点到点通信线路或 Internet 等广域网方式相连。

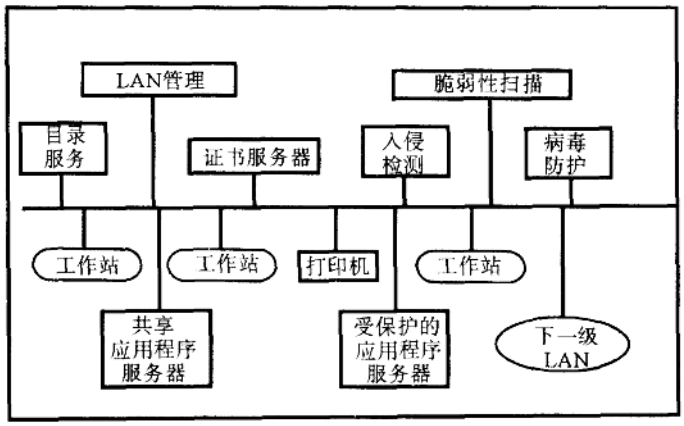

图 1－4 局域计算环境域

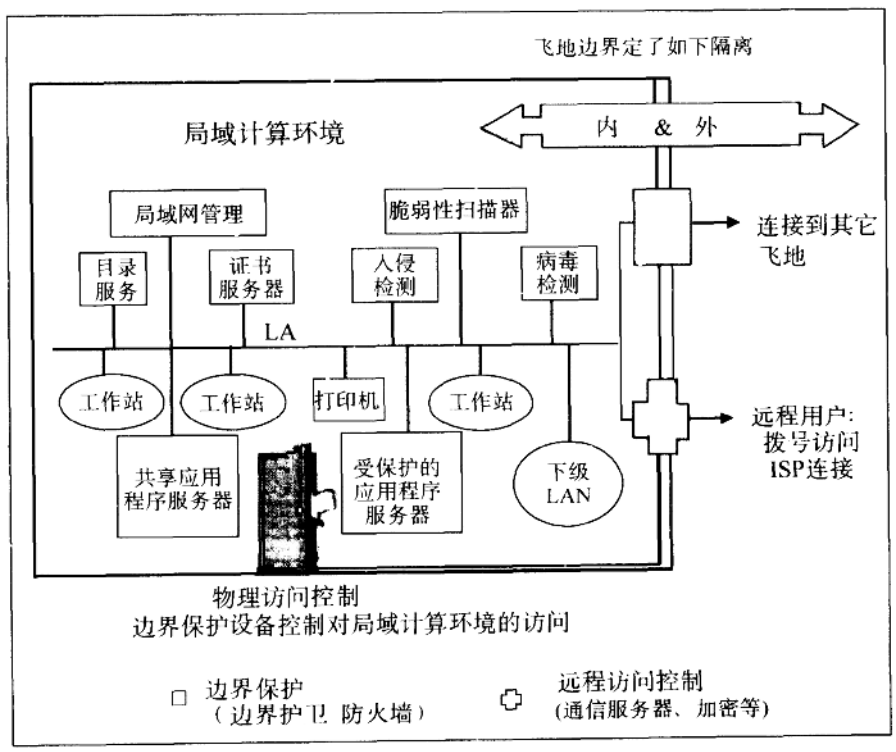

图 1－5 飞地边界框架域

飞地边界是信息进入或离开飞地或机构的点。因为许多机构都与其控制范围之外的网络相连,所以需要一个保护层来保障进入该范围的信息不影响机构操作或资源并且离开该范围的信息是经过授权的。

许多机构在其飞地边界处采用多种方式的外部网络连接。这些方式包括:

- 与外部网络(如 Internet)连接,以便与另一个飞地交换信息或访问网络上的数据;
- 与远程用户的三种连接方式:通过公共电话网拨号访问、通过直接连接方式(如电缆调制解调器)或拨号访问方式连接到 Internet 服务提供商(ISP)和通过专用线路连接到通信服务提供商(TSP)(参见图 1-3);
- 与其它不同密级的本地网络相连。

上述各类连接均需要能够同时满足操作和信息保障需求的不同类型的解决方案。在数据传输网络与其边界的安全级别相同的情况下,Internet 允许越界访问。

网络与基础设施

网络与基础设施提供了飞地互连。它们包括运行域网(OAN)、城域网(MAN)、校园域网(CAN)和局域网(LANs),涉及广泛的社会团体与本地用户。传输网络包括在网络节点(例如:路由器和网关)间传输信息的信息传输组件(例如:卫星、微波、其它无线电(RF)频谱与光纤)。如图 1-6 所示,网络基础设施的其它重要组件有网络管理、域名服务器和目录服务。

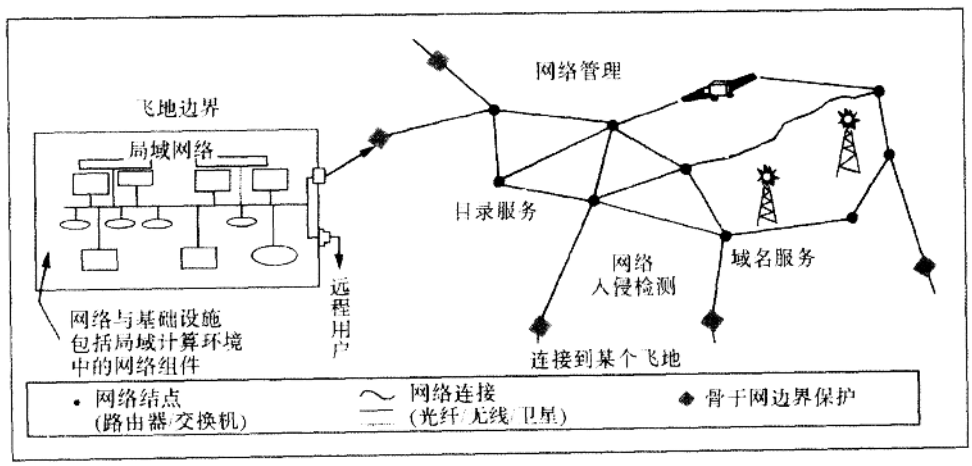

图 1-6 网络与基础设施框架域

现在政府和工业部门所使用而且仍将继续使用的典型传输网络和服务在逻辑上可以归为以下三方面:

1) 公共/商业网络和网络技术;

2) 专用网服务;

3) 归政府所有并由政府负责运行的部分。

专有机构与政府部门均使用的公共/商业网络,包括 Internet、公共交换电话网络(PSTN)和无线网络。其中,无线网络包括:蜂窝无线网络,卫星无线网络,无线局域网和寻呼网络。用户通常通过通信服务提供商获得网络访问权限。这些公共网络完全属于某个专有机构并由其负责运行。

为获得专用网服务,政府构建了联邦无线服务和 FTS 2000 等许多用于获得网络服务的网络服务契约。公共网络提供者在政府协约的基础上向用户提供网络访问权限。专

此为试读,需要完整PDF请访问: www.ertongbook.com