第二章　电子商务安全管理

- 安全原则的制定
- 安全协调机制的运营
- 安全管理制度的确保
- 安全法律法规的保障

第一节 安全原则与组织

一、制定安全原则的组织

- 国际原则化组织（ISO）
  - ISO7498 开放系统互连（OSI）基本参照模型，提供下列安全服务：
    - 验证服务，涉及对等实体验证和数据源验证。
    - 访问控制服务
    - 数据保密服务
    - 数据完整性服务
    - 不可否定服务
  - ISO7498-2提供如下安全机制
    - 加密机制、数字署名机制、访问控制机制、数据完整性机制、验证机制、通信业务填充机制、路由控制机制、公证机制。
  - ISO7498-2还提供如下安全机制，支持不同安全级别
    - 可信功能、安全标识、事件检测、安全审计跟踪、安全恢复

- 国际电报和电话征询委员会（CCITT现ITU）
  - X·400 报文处理系统（MHS）要求安全服务功能
    - 报文源鉴别、探询源鉴别、报告源鉴别服务、投递证明服务、提交证明服务、安全访问管理、内容完整性服务、内容机密性服务、报文流机密性服务、报文序列完整性服务、数据源的不可否定服务、投递的不可否定服务、提交的不可否定服务、报文安全标号服务。
  - X·400补充了密钥管理服务功能。
  - X·509提供了应用实体、人员、终端之间进行通信时的相互验证功能，给出了在目录中存储验证信息的条件，定义了使用验证信息进行验证的措施。
  - X·800对模型、访问控制、认证、保密、完整、不可否定、安全审计等提出了提议。
- 国际信息处理联合会第十一技术委员会（IFIP TC 11）

- 电器和电子工程师学会（IEEE）
  - 802.1　高层接口
  - 802.2　逻辑链路控制
  - 802.3　CSMA/CD网
  - 802.4　令牌总线网
  - 802.5　令牌环网
  - 802.6　城域网
  - 802.7　宽带技术征询组
  - 802.8　光纤技术征询组
  - 802.9　数据和话间综合网络
  - P 1363　公开密钥密码

- 美国国标局（NBS）与美国商业部国家技术原则研究所（NIST）
  - NIST的工作涉及：
    - 访问控制和认证技术
    - 评价和保障
    - 密码
    - 电子商务
    - 一般计算机安全
    - 网络安全
    - 风险管理
    - 电讯
    - 联邦信息处理原则
- 美国国标协会（ANSI）
  - ANSI是美国国标的出版机构。

二、因特网原则与组织

– 因特网体系

- 因特网是一种无政府的社会，它的正常运作靠在严格的技术原则下组员间的高度合作来维持。
- 因特网协会（ISOC）：为因特网原则的设置提供支持。
- 因特网体系构造工作委员会（IAB）：协调因特网的设计、工程与管理工作。
- 因特网工程任务组（IETF）：是IAB下属工作机构，负责因特网原则规范的开发。由个人技术工作者合作完毕任务。其主席由IAB任命。
- 因特网工作指导组（IESG）：是IETF的工作指导机构。由技术教授构成，负责有关因特网原则的最终决策。
- 因特网研究工作组（IRTF）：由团队组员构成，负责设定需优先研究的项目。涉及协议、应用、体系构造以及各类技术。其主席由IAB任命。

- 因特网原则的制定过程
  - 提议阶段：被提议的原则应该是比较稳定的，已经处理了设计上的问题，相信能被人们很好地了解，而且已经受到了因特网社会的仔细关注，引起了因特网社会的爱好，被以为是有价值的。一种规范作为提议原则的时间至少是6个月。
  - 草案阶段：当某个规范至少被应用于两个独立的互操作的实施项目中，而且取得了一定运作经验的阶段。草案原则不论在语义上还是作为开发某个实施项目的基础上，都必须能为人们很好地了解，而且相当稳定。一种规范作为草案原则的时间至少是4个月。
  - 正式原则阶段：一种规范进入了技术成熟的高级阶段，一般人们相信，由该规范制定的协议或服务能给因特网社会带来极大的益处。
  - 任何人都能够直接跟踪因特网原则的开发制定过程，并经过电子邮件提出自己的提议。
  - 处于原则制定过程中的规范公布在因特网祈求评议（RFC）中，如：RFC 791——IP 协议、RFC 793——TCP协议、RFC 822——SMTP协议、RFC 2068——HTTP协议等。
- 万维网联盟W3C：Web应用领域原则。HTML、XML

- 因特网安全运作指导方针
  - RFC 1281《因特网安全运作指导方针》为人们怎样在因特网社会中努力实现一种安全的环境提供了指导。
  - 顾客有责任了解和遵守其所使用的系统（计算机系统和网络系统）的安全政策。顾客应该对自己的行为负责任。
  - 顾客有责任采用切实可行的安全机制和安全程序来保护其所拥有的数据，顾客还有责任帮助保护其所使用的系统的安全。
  - 计算机与网络服务提供商有责任维护其所营运系统的安全，还有责任将其安全政策及其变动情况告知顾客。
  - 产品经销商和系统开发商有责任提供可靠的具有一定安全控制功能的系统。
  - 顾客、服务提供商及软硬件经销商有责任为保障安全而相互合作。
  - 有关因特网安全协议方面的技术改善应该谋求在一种可连续的基础上进行，同步在因特网上的新协议和软硬件产品的设计与开发过程中，应该吸收安全技术人员参加。

三、我国的信息安全原则化工作

- 自主制定和采用了一批相应的信息安全原则。
- 因为缺乏广泛的应用经验和进一步的研究背景，水平不高，覆盖不够。
- 行业和部门参加。

第二节 安全协调机构与政策

一、国际信息安全协调机构

- 计算机应急响应小组（CERT/CC）是一种以协调Internet安全问题处理方案为目的的国际性组织。其作用是处理Internet上存在的安全问题，调查Internet的脆弱性并公布信息。
  - 提供问题的处理方案： CERT/CC经过热线了解网络安全问题，经过建立并保持受影响者与有关教授的对话来促使问题得到处理。
  - 向Internet顾客搜集脆弱性问题报告，并进行确认。建立脆弱问题数据库以确保组员在处理问题过程中尽快取得必要的信息。

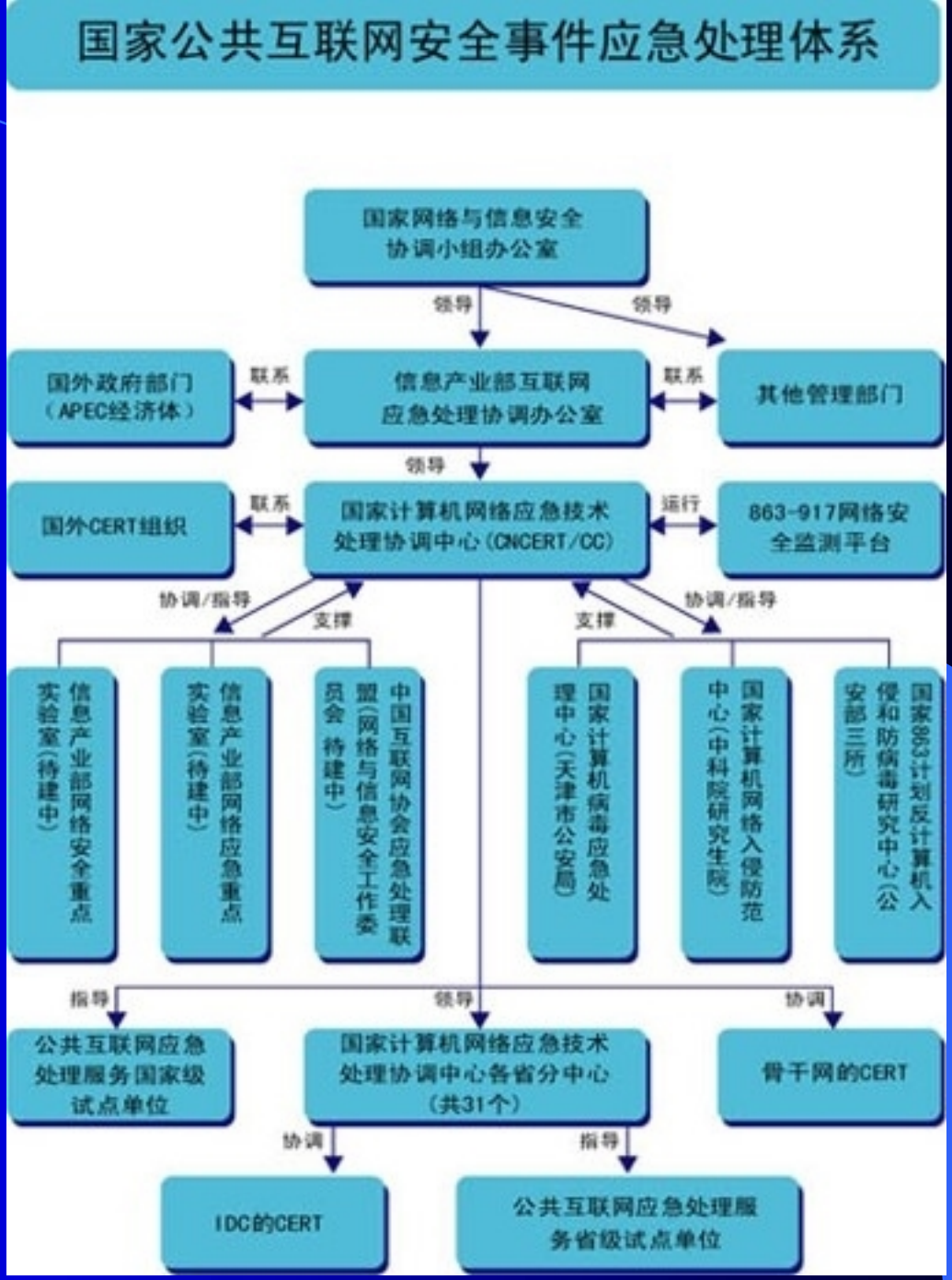
- 进行信息反馈。 CERT/CC曾将调查分析作为服务内容，以取得必要的信息。

– CERT/CC组员分为三个组
  - 运营组：负责提供针对安全问题的二十四小时在线技术帮助，进行脆弱性征询及联络销售业务等事项。
  - 教育与培训组：负责对顾客进行培训以增进网络安全性的提升。
  - 研究与发展组：负责鼓励可信系统的发展。
– 除CERT/CC外，诸多政府、商业和学术机构都组建了计算机信息安全问题小组。

二、我国的信息安全管理机构及原则

– 安全管理格局
  - 国务院信息化工作领导小组：对因特网安全中的重大问题进行管理协调。
  - 国务院信息化工作领导小组办公室：是国务院信息化工作领导小组的常设办事机构。负责组织、协调和制定有关因特网安全的政策、法规和原则。并监督落实

- 公安部、国家安全部、国家密码管理委员会、国家保密局、国务院新闻办公室等部门依其职能和权限进行管理和执法。
- 将网络类别分为：
  - 与国际上因特网连接的国际网络；
  - 与国际专业计算机信息网络连接的国际网络；
  - 经过专线与国际连网的企业内部网络。
- 将网络级别分为：
  - 因特网络、接入网络和顾客网络
- 信息安全管理的基本方针：
  - 兴利除弊、集中监控、分级管理，保障国家安全。
- 密码管理方针：
  - 统一领导、集中管理、定点研制、专控经营、满足使用
- 法律政策原则
- 机构或部门安全管理原则


国家公共互联网安全事件应急处理体系
国家网络与信息安全协调小组办公室
领导
领导
国外政府部门（APEC经济体）
联系
信息产业部互联网应急处理协调办公室
联系
其他管理部门
领导
国外CERT组织
联系
国家计算机网络应急技术处理协调中心（CNCERT/CC）
运行
863-917网络安全监测平台
协调/指导
支撑
支撑
协调/指导
信息产业部网络安全重点实验室（待建中）
信息产业部网络应急重点实验室（待建中）
中国互联网协会应急处理联盟（网络与信息安全工作委员会 待建中）
国家计算机病毒应急处理中心（天津市公安局）
国家计算机网络入侵防范中心（中科院研究生院）
国家863计划反计算机入侵和防病毒研究中心（公安部三所）
指导
领导
协调
公共互联网应急处理服务国家级试点单位
国家计算机网络应急技术处理协调中心各省分中心（共31个）
骨干网的CERT
协调
指导
IDC的CERT
公共互联网应急处理服务省级试点单位

- 机构或部门信息安全管理做到：
  - 有专门的安全管理机构
  - 有专门的安全管理人员
  - 有逐渐完善的安全管理制度
  - 有逐渐提升的安全技术措施

基本原则

- 规范原则。信息系统的规划、设计、实现、运营要有安全规范要求，要根据本机构的安全要求制定相应的安全政策。根据需要选用必要的安全功能和安全设备。不能盲目开发、自由设计、违章操作、无人管理。
- 预防原则。在信息系统的规划、设计、采购、集成、安装中应同步考虑安全政策和安全功能具有的程度。预防为主不存侥幸
- 立足国内原则。安全技术和设备首先要立足国内，未经许可，不进行消化改造直接应用国外技术和设备威胁国家安全。
- 选用成熟技术原则。采用新技术要注重其成熟度。
- 注重实效原则。投入与安全需求相适应。
- 系统化原则。分期建设，保护投资。
- 均衡防护原则。注意最单薄环节
- 分权制衡原则。要害部位分权制衡
- 应急原则。不怕一万就怕万一
- 劫难恢复原则。备份中心