呼叫中心信息安全保障

胡铁君 教授
ferrie.hu@chinaanhong.cn
广州市安鸿网络科技有限公司
www.chinaanhong.cn

中国电子商会
呼叫中心与客户关系管理专业委员会
China Call Center&CRM Association

呼叫中心新的挑战

- 呼叫中心用计算机软件控制的语音和数字结合平台
  - 已经有15年的历史
- 呼叫中心的技术复杂性
  - 数字平台的ACD电话系统
  - 多种语音模式
    - 传统电话、Web交互、小总机、IVR
  - 多平台和复杂的技术结构
    - 传统交换、VoIP、SIP
    - 多媒体交换、多种数据格式
- 广泛采用IP技术引发的安全问题

呼叫中心新的挑战

- 呼叫中心安全问题至关重要
  - 任何机密的客户信息丢失，
  - 有可能要承担着巨大的法律风险
- 信息安全问题越来越多，引起世界各国的密切关注
- 经济发达国家的呼叫中心，为了降低成本，把呼叫中心业务转移到经济不发达国家，但这些国家的知识产权和保密法并不是严格的
- 呼叫中心的管理人员对信息安全问题理解水平
- 全世界没有一套完善的呼叫中心信息安全规范

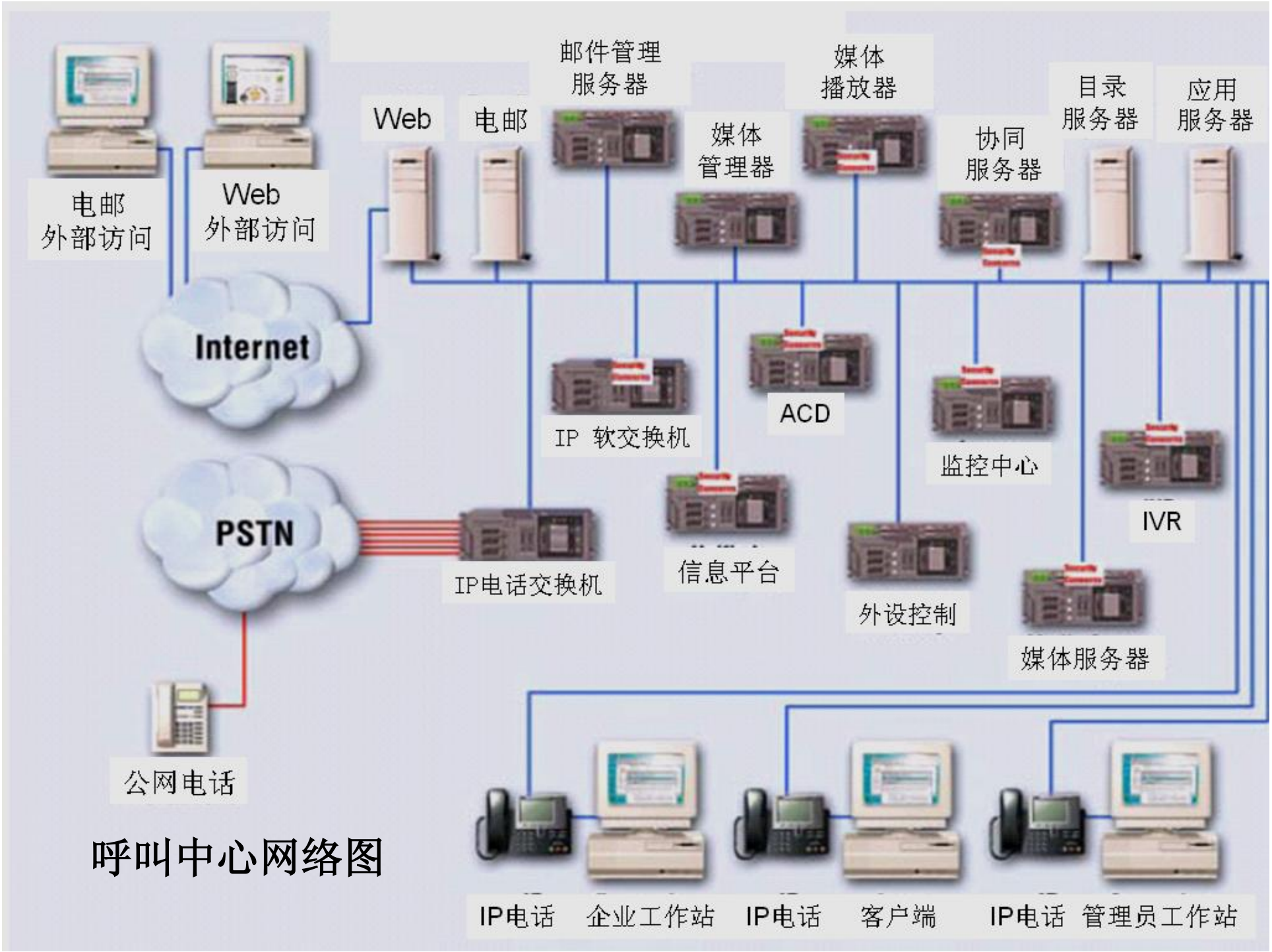
怎样确保呼叫中心的通信安全？

- 许多中心的融合数据网络上运行，受到安全威胁主要是来自数据网络
- 通信安全策略管理
  - 国际电联和国家的通信管理条例
  - 遵循信息网络安全规范
- 有关风险来源
  - 未经授权的访问黑客
  - 内部用户越权访问
  - 恶意攻击
- 解决措施
  - 监控所有信息，包括IP电话流量
  - 数据行为分析是重要的安全措施

怎样确保呼叫中心的通信安全？

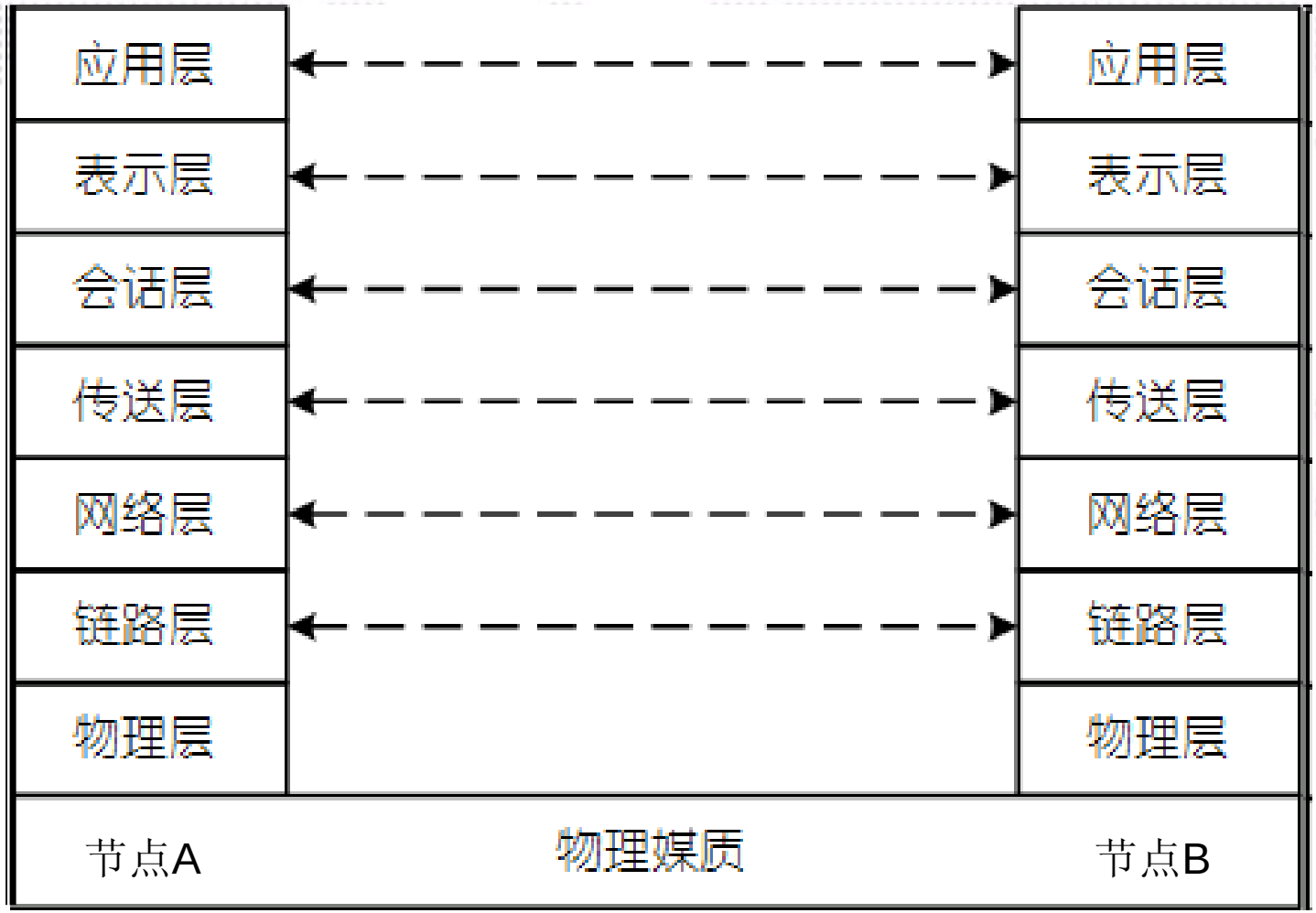
- 如何实现一个有效的安全呼叫中心
  - ü 制定信息安全政策和管理理念
  - ü 从规划、建设开始
  - ü 对已经建立的系统进行信息安全评估
    - ü 根据国家或行业协会的信息安全定义原则制定评估流程
    - ü 定出符合信息安全的系统环境
    - ü 落实确保呼叫中心的信息安全政策措施

呼叫中心面对的安全问题


电邮
外部访问
Web
外部访问
Web
电邮
邮件管理
服务器
媒体
播放器
媒体
管理器
协同
服务器
目录
服务器
应用
服务器
Internet
PSTN
IP 软交换机
ACD
监控中心
IVR
IP电话交换机
信息平台
外设控制
媒体服务器
公网电话
IP电话
企业工作站
IP电话
客户端
IP电话
管理员工作站

呼叫中心网络图

网络通信的协议


应用层
表示层
会话层
传送层
网络层
链路层
物理层
应用层
表示层
会话层
传送层
网络层
链路层
物理层
节点A
物理媒质
节点B

物理安全问题

- 呼叫中心所有看到的和摸到的通信设备，包括电源、空调、输入输出设备等等
  - 防止掉电，足够的后备UPS电源容量
  - 机房采用专业的空调设备
  - 分布式呼叫中心，可以通过IP PBX或ACD转移话务
  - 危机处理调度，人员、话务、网络路由、电源等等
  - 工作人员出入管理
  - 工作站的密码管理，使用者的身份确认
  - 公共电话远离工作区
  - 员工的电话使用管理
  - 严格控制IP电话的系统管理权限

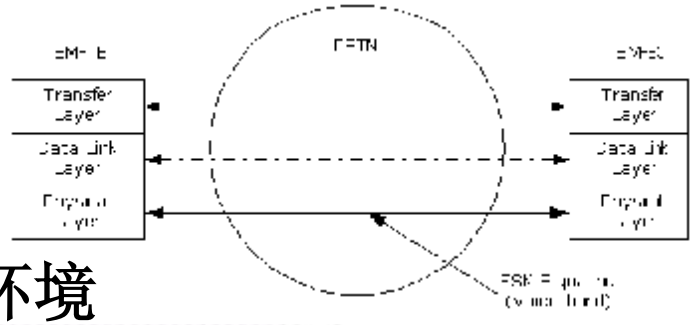
- 集中控制的呼叫中心是比较容易管理，一旦发生事故，如地震、水灾、火灾等等重大灾害，就会严重影响服务
- 分布式的呼叫中心可以防止重大灾害对服务的影响，投资巨大

数据链路安全问题

- 如何保证把数据安全的传到各设备
  - 防止非法的网络入侵
  - 访问、读取的控制
  - 工作人员名单
  - 网络的用户身份确认
  - 密码管理
  - 访问的权限
  - 网络WAN地址和工作人员的对应
  - 安置采集访问、读取记录的设备

网络层安全问题

- 主要是针对网络的结构安全
  - IP地址的管理
  - 接点管理
  - 设立防火墙隔离各种不同的应用环境
  - 防止非法的IP访问
  - 设行为监督系统
- 网络管理人员必须清楚每一个IP地址，有什么权利去访问什么服务器
- 严格定义防火墙的安全策略
  - 隔离、控制范围、TCP/IP Port控制、应用、SQL数据库访问、SIP路由
  - 拒绝非法的入侵
- 对应用系统的检验



传送安全问题

- 对通信的管理（逻辑通道的安全管理）
  - 数据包的传输
  - 防火墙不能处理
  - 在传输的数据中，没有通过加密的密码数据、访问参数等等
  - 非法入侵者可能利用网络的通信口的数据，截取入侵的方法
- 某些重要的呼叫中心应用，必须对传输数据进行加密
- 保障从用户终端到应用程序之间的数据保密

会话层安全问题

- 对于呼叫中心，重要是数据通信握手协议
  - 主要是SIP VoIP电话的通信引发
  - 入侵者可能利用SIP的通信协议获得用户的资料，如银行账户，密码
- 采用加密的手段保护会话层的安全
  - 用户利用IVR获取客户银行户口信息
    - 必须对客户与呼叫中心的数据和声音进行加密
- 对声音采用CIC 2.4 SIP加密
  - 评估从ACD分配、PBX的连接、IVR和语音邮件的话音安全性

表示层安全问题

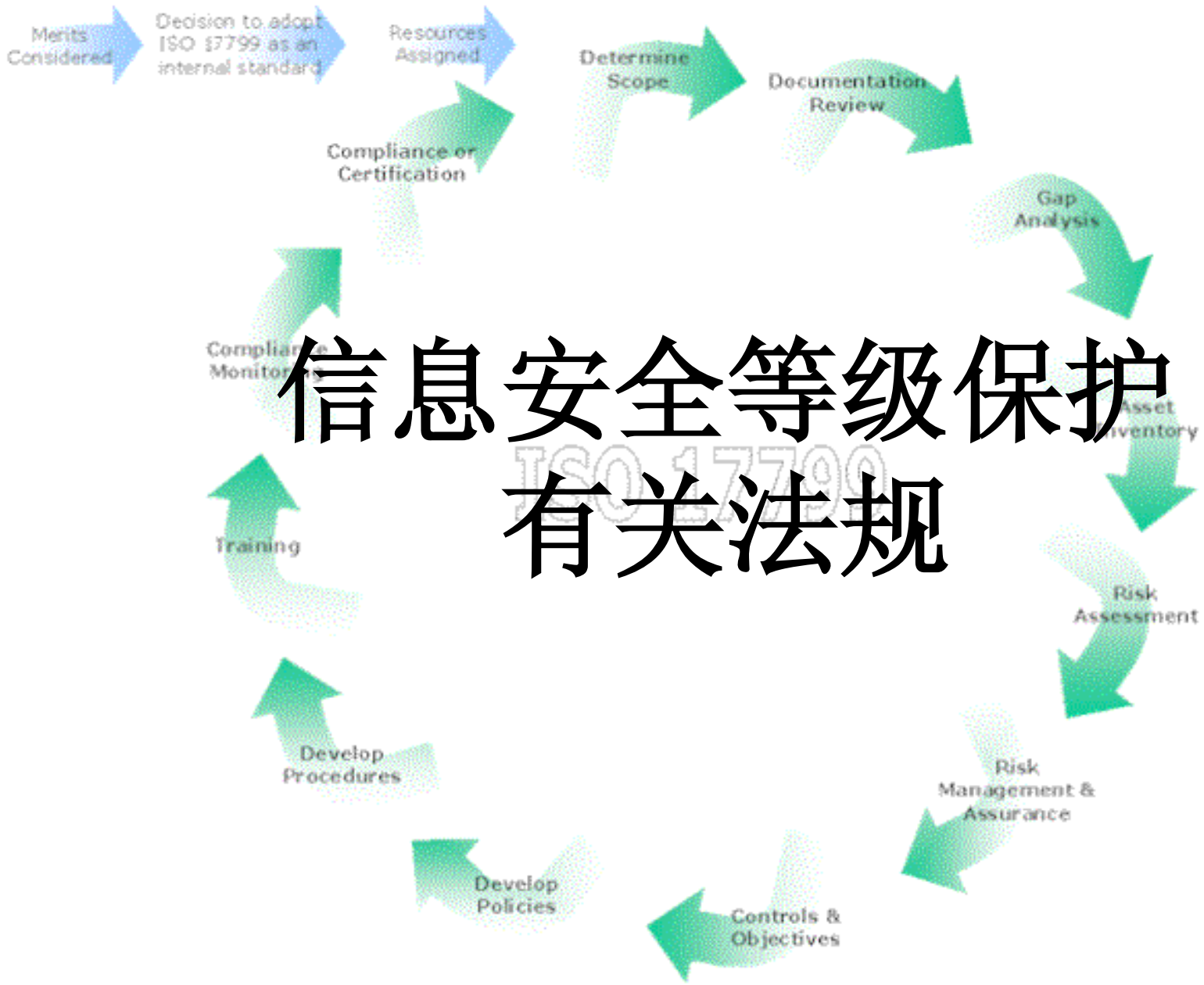
- 提供不同的系统之间的数据通信格式
  - 对于呼叫中心，主要针对系统和普通用户的管理问题
    - 系统管理员的权限
    - IT工作人员的权限
- 管理员工作日志记录
  - 任何通过管理员做的事情都要有记录
  - 跟踪所有的变更
  - 跟踪管理环境
- 用户权限管理
  - 采用许可证的管理
  - 监控所有的呼叫电话

应用层安全问题

- 应用层的功能
  - 文件传输、远距离文件读取、虚拟终端等等
  - 呼叫中心主要针对远距离终端的管理
- 密码加密
  - 管理员、用户的密码必须加密
  - 定义密码的格式、长度、不同户的不同密码等等
- 用户登录方法
  - 应用与系统的登录绑定
  - 应用软件设立登录方法
  - 自定义DLL库解析用户的登录
  - 其他，短信确认，语音确认等等
- 远距离终端
  - VPN，用户证书

应用层安全问题

- 通过远距离终端进行维护的管理
  - 制定一套严格管理办法
  - 什么通信协议可以开放？如 FTP、SSH、SCP、HTTP、MQ、SSL、直接IP访问、SNA、SMTP、POP3、Citrix、VPN等等
- 数据库访问
  - 访问记录
  - IVR平台使用数据库很难进行加密
  - 客户的数据库与呼叫中心的数据库同步时，采用加密措施
- 有缴费功能的语音平台
  - 一般情况呼叫中心不要开放语音缴费功能
  - 采用呼叫转移，由客户的专业缴费平台完成缴费功能
  - 呼叫中心操作员不要介入



信息安全等级保护有关法规

信息安全等级保护有关法规

- 《信息安全等级保护管理办法》（公通字[2007]43号）
- 依据《信息系统安全等级保护测评要求》等技术标准，信息系统建设完成后，运营、使用单位或者其主管部门，应当选择符合规定条件的测评单位，定期对信息系统安全等级状况开展等级测评
- 2004年公安部、保密局、密码委、信息办联合发文，初步规定了信息安全等级保护工作的指导思想、原则、要求
- 2007年公安部、保密局、密码委、信息办联合发文，系统规定了信息安全等级保护制度

信息安全等级保护有关法规

信息安全等级划分

- 计算机信息系统受到破坏后，可能对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益的，为第一级；
- 计算机信息系统受到破坏后，可能对公民、法人和其他组织的合法权益产生严重损害，或者可能对社会秩序和公共利益造成损害，但不损害国家安全的，为第二级；
- 计算机信息系统受到破坏后，可能对社会秩序和公共利益造成严重损害，或者可能对国家安全造成损害的，为第三级；
- 计算机信息系统受到破坏后，可能对社会秩序和公共利益造成特别严重损害，或者可能对国家安全造成严重损害的，为第四级；
- 计算机信息系统受到破坏后，可能对国家安全造成特别严重损害的，为第五级。

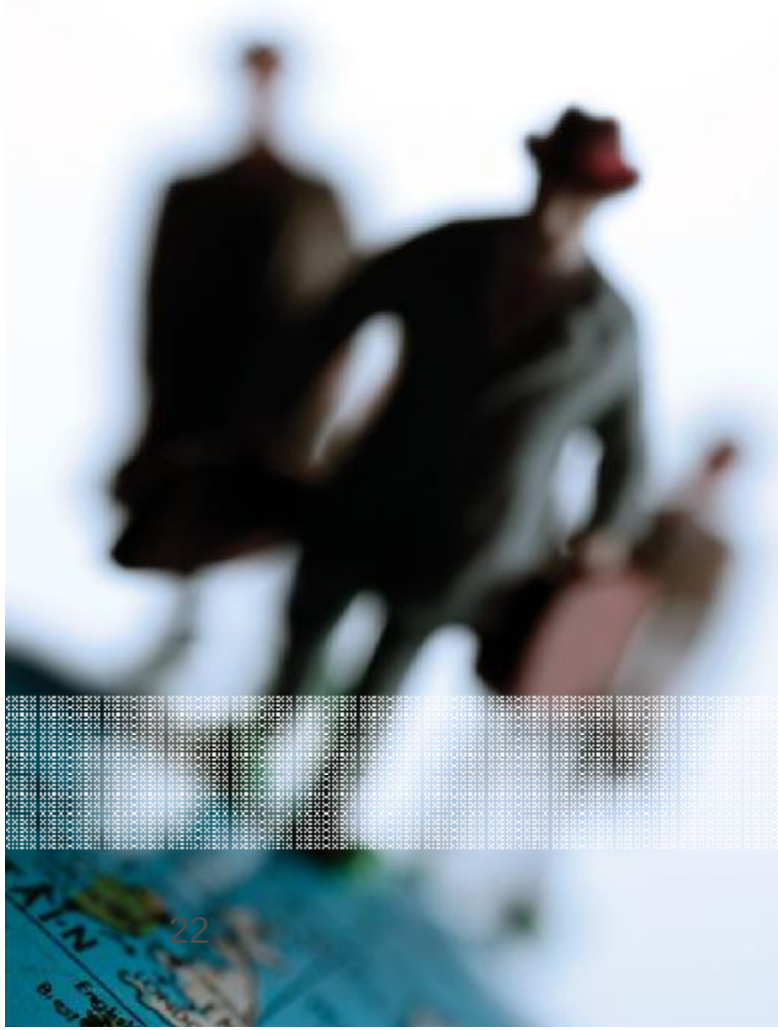
信息安全等级保护的工作

- 开展信息安全等级保护工作
  - 检查安全保护实施情况
  - 信息系统安全岗位和安全管理人员设置
  - 按照信息安全法律法规、标准规范的要求制定具体实施方案
- 制定信息安全系统定级备案制度
  - 信息系统变化及定级备案变动
  - 信息安全设施建设
  - 信息安全整改
  - 选择使用信息安全产品情况
- 聘请测评机构按规范要求开展技术测评工作

  根据测评结果开展整改情况

  自行定期开展自查情况
- 信息安全知识和技能培训

谁可以帮忙？



坚持积极防御、综合防范，探索

把握信息化与信息安全的内在规律

主动应对信息安全挑战

保障客户信息安全的服务

创造客户价值、创造社会价值

为客户及国家的信息化建设提供安全保障

“服务创造价值，进取成就客户”

www.chinaanhong.cn