# 第四章 信息系统安全审计

# 本章提纲

§1 概述

§2 安全审计系统的体系结构

§3 安全审计的一般流程

§4 安全审计的分析方法

§5 安全审计的数据源

§6 信息安全审计与标准

§7 计算机取证（安全审计的应用）

# §1 概述：信息系统安全审计

§1.1 概念

§1.2 功能

§1.3 分类

# §1.1 概念

## 安全审计的定义

指根据一定的安全策略，通过记录和分析历史操作事件及数据，发现能够改进系统性能和系统安全的地方。

- 对系统安全的审核、稽查与计算
- 记录--》评价审查--》发现隐患，追查原因--》响应处理
- 不存在绝对安全的系统，所以需要安全审计，其作为安全措施之一

- 信息安全审计

☆ 揭示信息安全风险的最佳手段

☆ 改进信息安全现状的有效途径

☆ 满足信息安全合规要求的有力武器

# §1.1 概念

## 安全审计的功能

### 1）取证

- 利用审计工具监视、记录系统的活动情况
- 对于已发生的系统破坏行为提供追究证据

### 2）威慑

- 审计追踪 + 责任追求机制
- 外部入侵、内部作恶

# §1.1 概念

## 安全审计的功能

### 3）发现系统漏洞

- 为系统管理员提供系统使用日志
- 及时发现系统入侵行为和潜在系统漏洞

### 4）发现系统运行异常

- 提供系统运行日志
- 输出安全性分析报告
- 及时发现系统异常行为，采取措施

# §1.1 概念

## 安全审计的分类

### 1）按审计对象分类

- 针对主机的审计

  -- 对系统资源进行事前控制和事后取证，形成日志文件

- 针对网络的审计

  -- 审计网络的信息内容和协议分析

# §1.1 概念

## 安全审计的分类

### 2）按审计工作方式分类

- 集中式安全审计

  -- 采用集中地方法收集、分析数据源

  -- 所有数据交由中央处理机进行审计处理

- 分布式安全审计

  -- 对分布式网络的安全审计

  -- 采用分布式计算的方法，对数据源进行安全审计

# 本章提纲

§1 概述

§2 安全审计系统的体系结构

§3 安全审计的一般流程

§4 安全审计的分析方法

§5 安全审计的数据源

§6 信息安全审计与标准

§7 计算机取证（安全审计的应用）

# §2 安全审计系统的体系结构

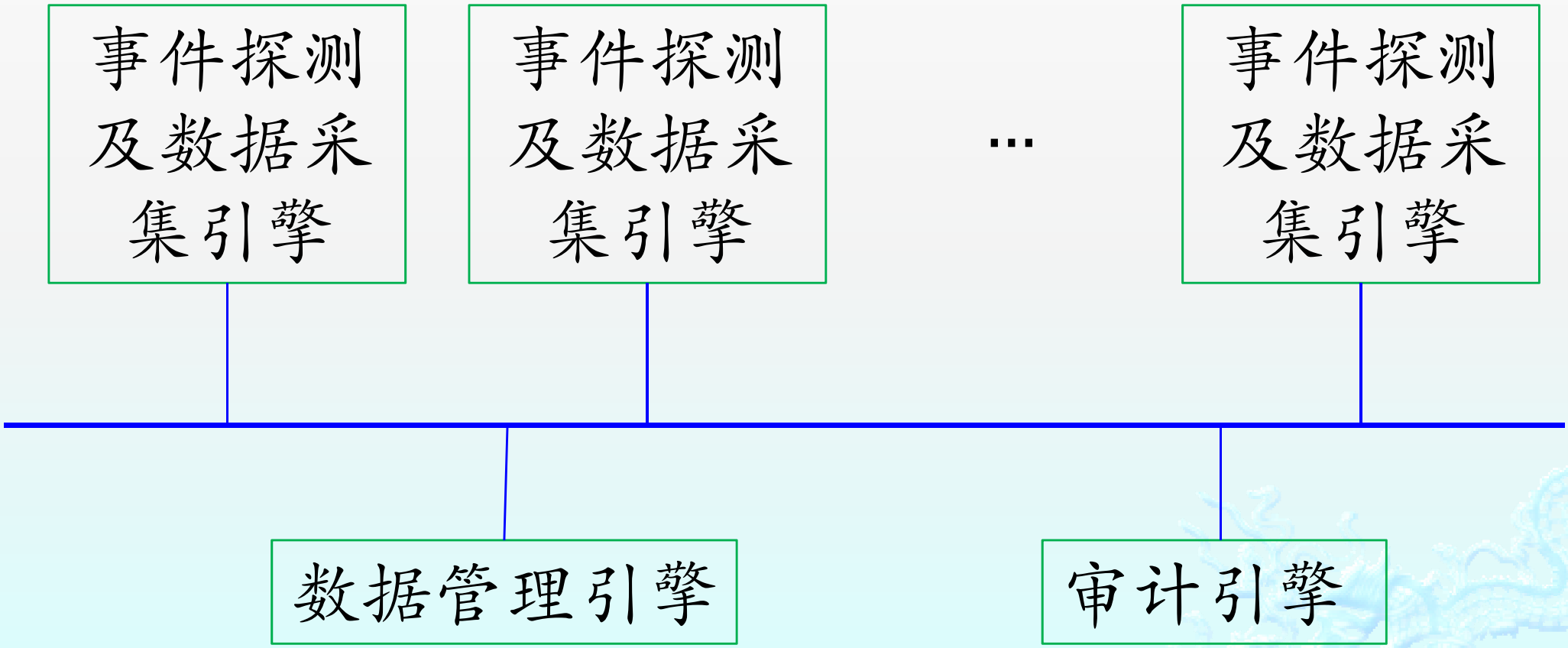
§2.1 一般组成

§2.2 集中式结构

§2.3 分布式结构

# §2.1 安全审计系统的一般组成

- 安全审计系统组成



# §2.1 安全审计系统的一般组成

- 事件探测及数据采集引擎
  - 侦听主机及网络上的信息流
  - 监视主机运行情况
  - 监听、检测并实时分析网络数据包
  - 分析结果送至数据管理中心保存

# §2.1 安全审计系统的一般组成

- 数据管理引擎
  - 数据库管理

    -- 设置数据库连接信息，管理采集和输出数据
  - 引擎管理

    -- 设置事件探测及数据采集引擎信息
  - 配置管理

    -- 对审计对象进行客户化自定义，协议审计，设定异常端口审计

# §2.1 安全审计系统的一般组成

- 审计引擎
  - 审计控制台
    - -- 实时显示网络审计信息
    - -- 可查询审计信息历史数据，回放审计事件
  - 用户管理
    - -- 可设定用户权限
    - -- 对授权用户的操作进行审计记录

# §2.2 集中式安全审计系统体系结构

- 中央处理机

  -- 承担数据管理引擎和安全审计引擎的工作

  -- 汇总、处理所收集的全部数据

- 数据采集点

  -- 承担事件检测及数据采集引擎的作用

  -- n 个

# §2.2 集中式审计的缺陷

- 不适应高度分布的网络环境
  - 中央处理器负担过大，用户增容困难
  - 数据可用性不好
  - 自适应能力差

# §2.3 分布式安全审计系统体系结构

- 两层含义
  - 对分布式网络的安全审计
  - 采用分布式计算方法对数据源进行安全审计

# §2.3 分布式审计系统的三个模块

- 主机代理模块

  -- 部署在受监视主机上，后台进程收集审计信息，传至中央管理者

  -- 承担数据采集及部分安全审计工作

- 局域网监视器代理模块

  -- 部署在受监视局域网上，收集并审计局域网上行为与通信信息，结果送至中央管理者

# §2.3 分布式审计系统的三个模块

- 中央管理者模块

  -- 承担数据管理引擎和安全审计引擎的工作

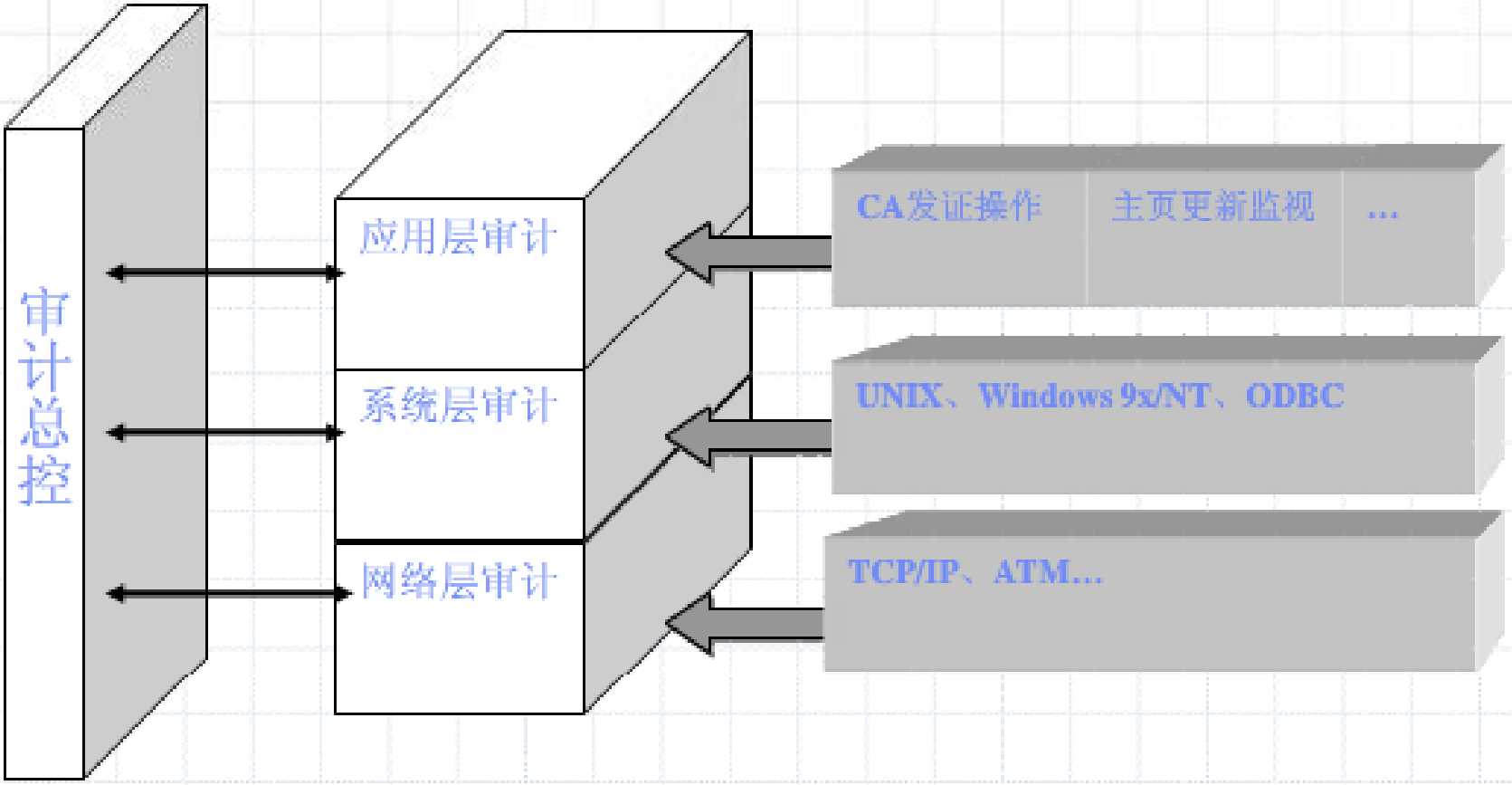
  -- 汇总、处理所收集的全部数据

  -- 接收数据和报告，控制系统通信信息

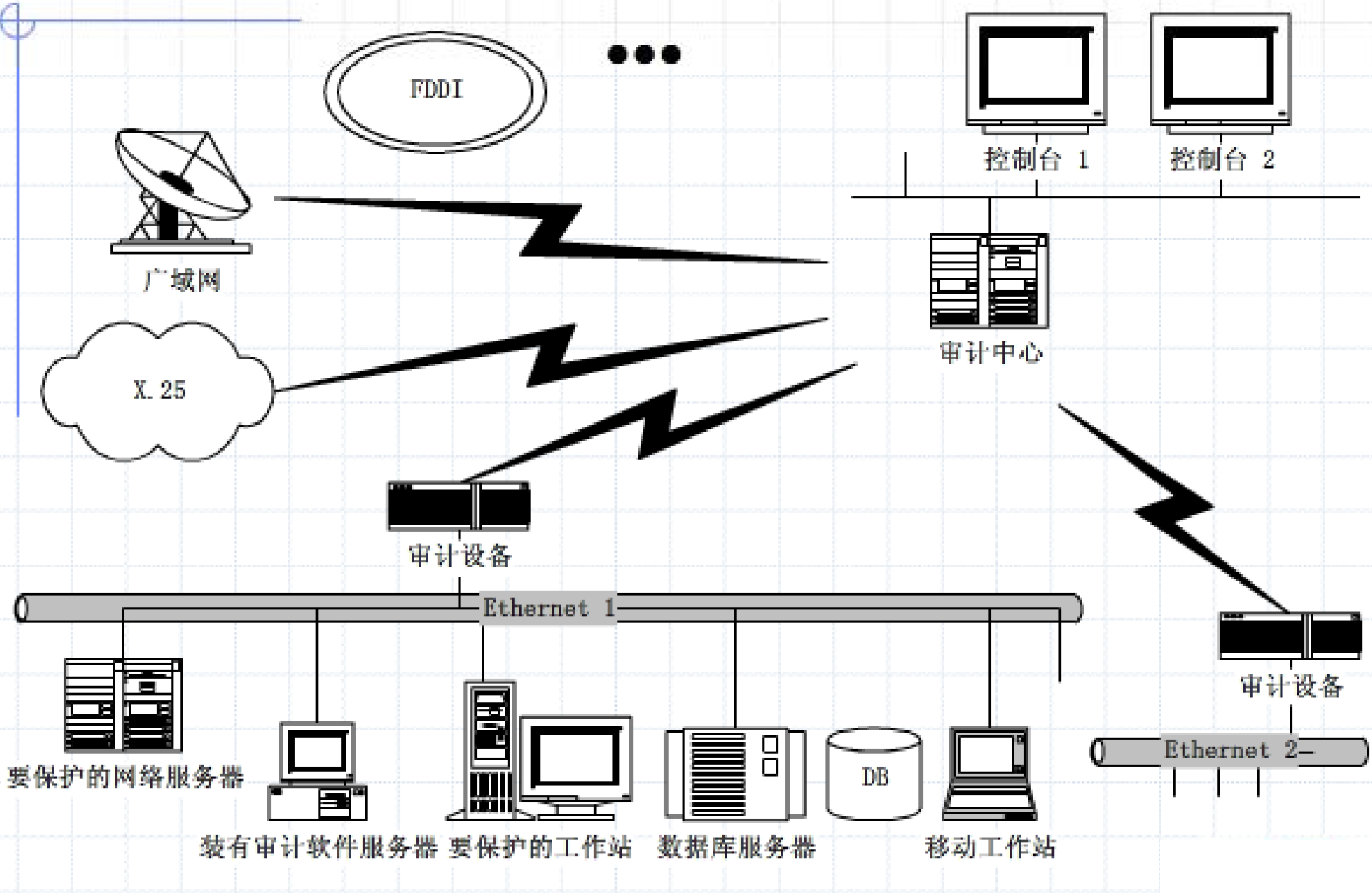
# §2.3 分布式安全审计系统体系结构

- 优点（相对于集中式结构）
  - 扩展能力强：可扩展审计单元
  - 容错能力强：解决了单点失效问题
  - 兼容性强：可同时包含基于主机和基于网络的审计
  - 适应性强：网络和主机升级或重构时，系统易修改

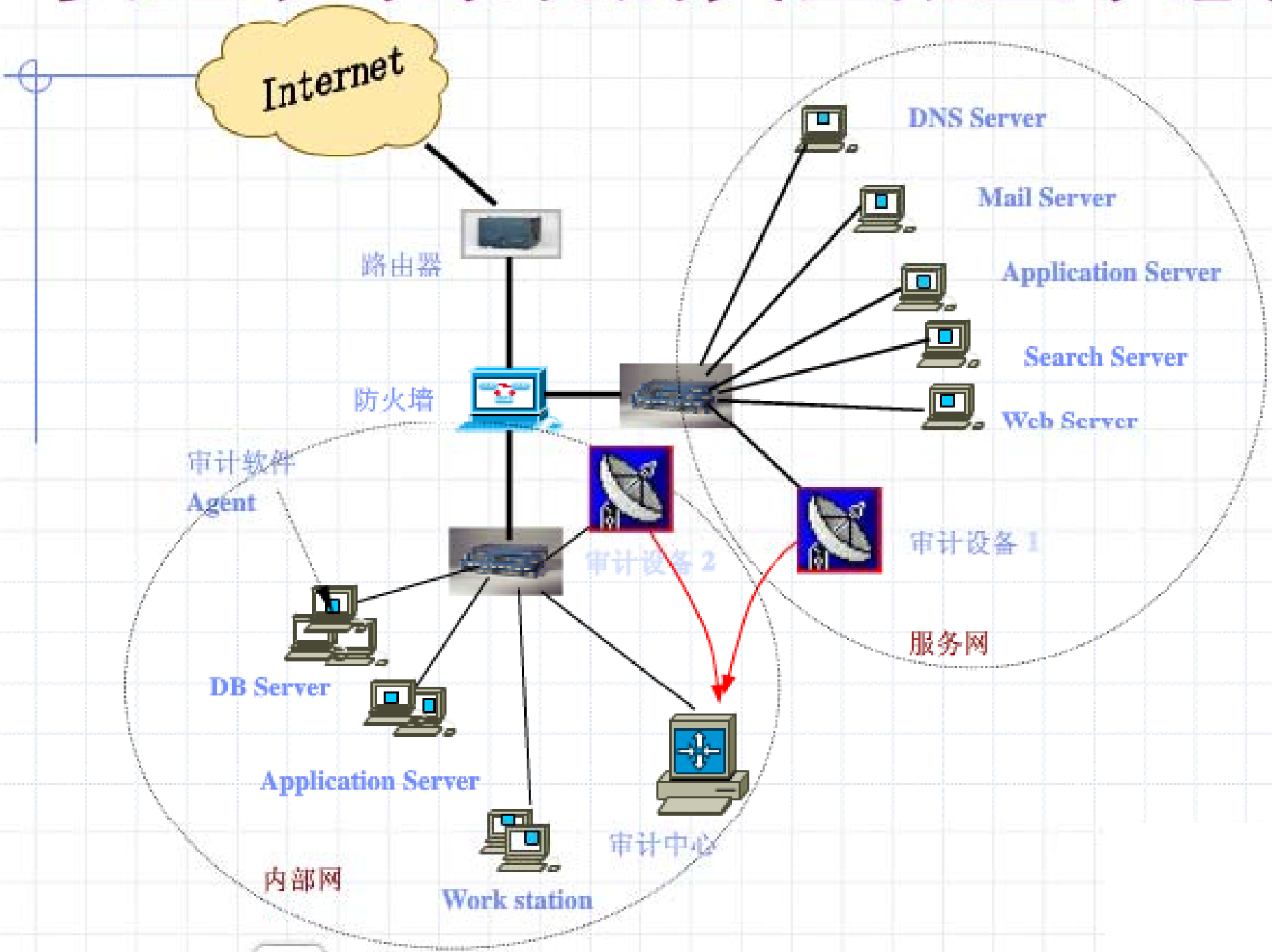
# 网络安全审计层次结构图



# 安全审计系统体系结构示意图



# 安全审计系统的典型配置示意图



# 本章提纲

§1 概述

§2 安全审计系统的体系结构

§3 安全审计的一般流程

§4 安全审计的分析方法

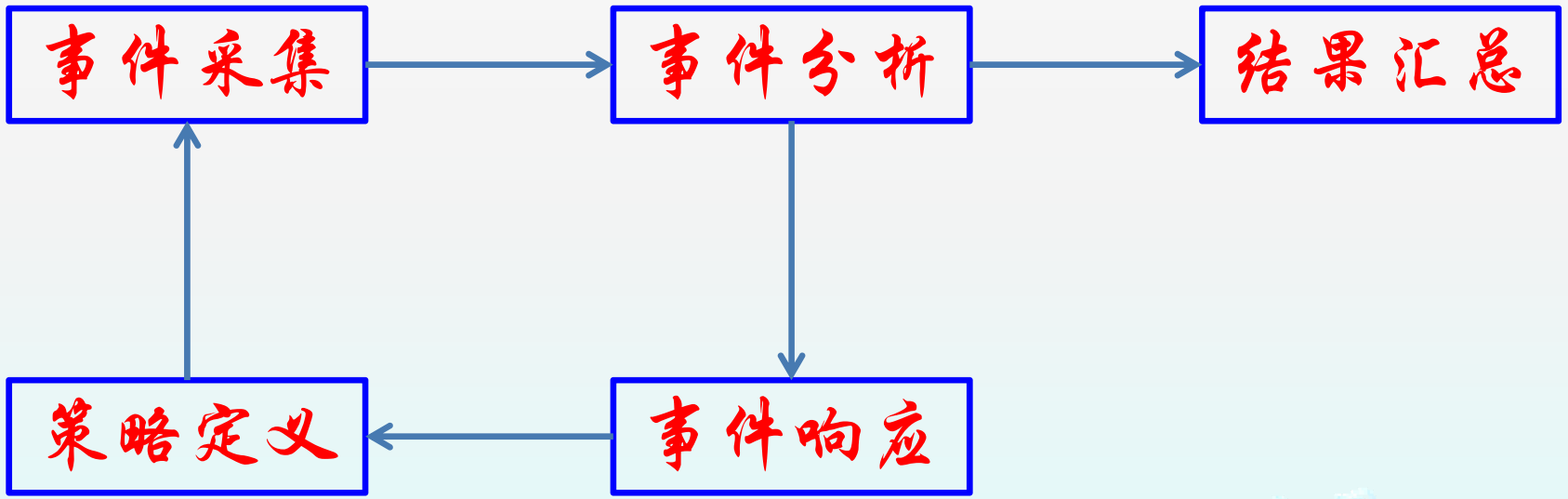
§5 安全审计的数据源

§6 信息安全审计与标准

§7 计算机取证（安全审计的应用）

# §3 安全审计的一般流程

- 安全审计流程图



# §3 安全审计的一般流程

## 1. 策略定义

-- 安全审计需在一定的审计策略下进行

-- 审计策略规定所采集信息、危险事件及其处理方法等

-- 在事件处理结束后，依据分析处理结果检查策略合理性，应需调整

# §3 安全审计的一般流程

## 2. 事件采集

-- 按照预定的审计策略对客体进行相关审计事件采集，形成的结果交由事件后续的各阶段处理

-- 将事件其他各阶段提交的设计策略分发至各审计代理，审计代理依据策略采集客体事件

# §3 安全审计的一般流程

## 3. 事件分析

- 按照预定策略进行事件辨析，决定：

  -- 忽略该事件

  -- 产生审计信息

  --产生审计信息并报警

  --产生审计信息且进行响应联动

- 将事件分析结果生产审计记录，形成审计报告

# §3 安全审计的一般流程

- 4. 事件响应：对事件分析的结果采取响应行动

  - 报警与响应
  - 生成审计记录，写入审计数据库，将各类审计分析报告发送至指定对象
  - 备份审计记录

# §3 安全审计的一般流程

- 5. 结果汇总：汇总事件分析及响应的结果

- 分类汇总各类审计报告
- 统计分析审计结果，形成分析报告
- 依据用户需求和事件分析处理结果，形成审计策略修改意见

# 本章提纲

§1 概述

§2 安全审计系统的体系结构

§3 安全审计的一般流程

§4 安全审计的分析方法

§5 安全审计的数据源

§6 信息安全审计与标准

§7 计算机取证（安全审计的应用）

# §4 安全审计的分析方法

## 1. 基于规则库的安全审计方法

- 对已知的攻击行为进行特征提取
- 以特征描述构建规则库
- 安全设计时，将收集数据与这些规则进行比较匹配，从而发现可能的网络攻击行为
- 缺陷：对易产生变种的网络攻击行为，审计效果不好

# §4 安全审计的分析方法

## 2. 基于数理统计的安全审计方法

- 为审计对象创建一个统计量的描述，如网络流量的平均值、方差等
- 统计出正常情况下特征量的数值
- 安全设计时，当发现实际值远离正常数值即认定为潜在的攻击发生
- 缺陷：统计量的阈值难设定

# §4 安全审计的分析方法

## 3. 基于日志挖掘的安全审计方法

- 利用带有学习能力的数据挖掘方法，从系统使用或网络通信的“正常”数据中发现系统的“正常”运行模式，并和常规的攻击规则库进行关联分析，以检测系统攻击行为。

- 数据挖掘是一项通用的知识发现技术，可从海量数据中提取我们感兴趣的数据信息或知识。

- 优势：检测准确率高、速度快、自适应能力强

# §4 安全审计的分析方法

## 4. 其他安全审计方法

- 借用入侵检测分析方法，只不过前者是事后监督行为，入侵检测实时性更高
- 神经网络、遗传算法

# 本章提纲

§1 概述

§2 安全审计系统的体系结构

§3 安全审计的一般流程

§4 安全审计的分析方法

§5 安全审计的数据源

§6 信息安全审计与标准

§7 计算机取证（安全审计的应用）

# §5 安全审计的数据源

## 1. 基于主机的数据源

- 操作系统的审计记录
  - ✓ 操作系统软件内含专门审计子系统
  - ✓ 安全可信的数据源
  - ✓ 提供系统内核级的事件发生情况

# §5 安全审计的数据源

## 1. 基于主机的数据源

- 系统日志
  - ✓ 分类：操作系统日志、应用程序日志
  - ✓ 与操作系统审计记录相比，安全性存在不足：保护机制不够强，易受攻击。

# §5 安全审计的数据源

## 1. 基于主机的数据源

- 应用程序日志信息
  - ✓ 不是系统级别的、非优先选用的数据源
  - ✓ 计算机网络的分布式计算架构得到发展普及，需要采用反映系统活动的较高层次的抽象信息，及特定应用程序日志作为数据源

# §5 安全审计的数据源

## 2. 基于网络的数据源

- 网络中传输的数据即为数据源
- 优势：采集数据时不会干扰网络正常工作及其安全性

# §5 安全审计的数据源

## 3. 其他数据源

- 来自其它安全产品
- 来自网络设备
- 来自人工方式提供的数据信息

# 本章提纲

§1 概述

§2 安全审计系统的体系结构

§3 安全审计的一般流程

§4 安全审计的分析方法

§5 安全审计的数据源

§6 信息安全审计与标准

§7 计算机取证（安全审计的应用）

# §6 信息安全审计与标准

## 涉及安全审计的相关标准

- TCSEC，美国国防部(Trusted Computer Systems Evaluation Criteria)
- CC，ISO15408
- GB17859-1999《计算机信息系统安全保护等级划分准则》
- GB/T 20945-2007《信息系统安全审计产品技术要求和测试评价方法》

# §6.1 TCSEC～安全审计

- 定义了四个级别的审计要求

- C2 – 审计的事件：用户身份鉴别、操作员/系统管理员的行为等；审计记录包含信息：事件发生事件、主体、类型等
- B1 – 增加了强制访问控制机制
- B2 – 增加了可信路径和隐蔽通道分析
- B3 – 增加了对可能将要违背系统安全政策这类事件的审计

# §6.2 CC～安全审计

- CC – 信息安全评价国际标准

  - 组织上分为：基本概念、安全功能需求、安全保证需求
  - 安全审计是一个单独的安全功能需求类
  - 安全审计类有6个族：对审计记录的选择、生成、存储、保护、分析、及相应的入侵检测响应等功能做出不同程度的要求

# §6.3 GB 17859-1999～安全审计

## 《计算机信息系统安全保护等级划分准则》

- 定义了5个等级，其中高四级有安全审计要求
- 第2级：系统审计保护级，记录事件+审计记录
- 第3级：安全标记保护级，增加对客体安全标记的记录
- 第4级：结构化保护级，增加对可能利用存储型隐蔽通道事件的审计
- 第5级：访问验证保护级，增加监视事件的发生与积累，当其超过阈值时，立即报警

# §6.4 信息系统安全审计产品技术要求

- GB/T 20945-2007《信息系统安全审计产品技术要求和测试评价方法》

- 安全审计产品分类：专用型、综合型
- 安全功能要求：审计踪迹、数据保护、安全管理、标识鉴别、产品升级、监管要求
- 自身安全要求：自身审计数据生成、审计记录独立存放、审计代理安全等
- 性能要求：稳定性、资源占用、网络影响、吞吐量
- 保证要求：产品保证方面的要求，如配置管理保证、交付与运行保证等

# 本章提纲

§1 概述

§2 安全审计系统的体系结构

§3 安全审计的一般流程

§4 安全审计的分析方法

§5 安全审计的数据源

§6 信息安全审计与标准

§7 计算机取证（安全审计的应用）

# §7.1 计算机取证的发展历史

- 各国积极开展电子证据检验鉴定工作

## 英国

- ✓ 1968年法庭审判就开始使用计算机证据，
- ✓ 2003年两起案件给公众普及了“计算机法医”概念

## 美国

- ✓ 1989年FBI成立专门从事电子证据检验的部门
- ✓ 在《联邦证据规则》（Federal Rules of Evidence）等相关法律中增加电子证据部分内容

## 法、德、新加坡、印度等

# §7.1 计算机取证的发展历史

- 各国积极开展电子证据检验鉴定工作

## 中国

- ✓ 1999年开始研究电子证据检验技术
- ✓ 2001年开展电子证据检验鉴定工作
- ✓ 起步阶段：只有一些法律法规设计一些关于计算机证据的说明；实际案例中采用的计算机证据简单

## 趋势

- ✓ 技术研究、工具软件开发、商业服务始于上世纪90年代
- ✓ 现已成为关注热点

# §7.2 计算机取证概念

- 多种定义

- 资深人士Judd Robbins
  - ✓ 计算机取证是将计算机调查和分析技术应用于对潜在的、有法律效力的证据的确定与获取

- Sensei信息技术咨询公司
  - ✓ 为对电子证据的收集、保存、分析和陈述

- 综上，我们定义：
  - ✓ 计算机取证时对计算机入侵、破坏、欺诈、攻击等犯罪行为，利用计算机软硬件技术，按照符合法律规范的方式，进行识别、保存、分析和提交数字证据的过程。取证的目的是找出入侵者，并解释入侵过程。

# §7.2 计算机取证概念

- 计算机取证遵循的原则

  - 尽早收集证据，保证其无破坏
  - 保证证据连续性
  - 全过程监督

# §7.3 计算机取证流程

- 保护目标系统
  - ✓ 冻结计算机，以避免发生更改、破坏电子证据事情
- 电子证据确定
  - ✓ 区分出有用数据，确定犯罪者留下的活动记录作为电子证据
- 电子证据收集
  - ✓ 收集系统配置信息、备份/打印原始数据、收集数据到取证设备、记录有关时间和操作步骤等
- 电子证据保护
  - ✓ 采取措施保护电子证据的完整性和真实性

# §7.3 计算机取证流程

- 电子证据分析
  - ✓ 电子证据分析并得出结果对法庭证供重要
  - ✓ 分析方法包括关键字搜索、文件日志分析、智能相关性分析等
- 归档
  - ✓ 对涉及计算机犯罪的时间、存储、系统、文件、软件、取证分析结果和评估报告等进行归档处理，形成能给法庭的呈堂证供
- 补充说明
  - ✓ 确保证据链的完整性，对各步骤的情况归档

# §7.4 计算机取证相关技术

- 电子证据监测技术
  - ✓ 监测各类系统设备及存储介质中的电子数据，分析是否有可作为证据的电子数据
  - ✓ 涉及技术包括：事件/犯罪监测、异常监测、审计日志分析
- 物理证据获取技术
  - ✓ 全部取证工作的基础
  - ✓ 保证所保存的原始证据不受任何破坏
  - ✓ 常用数据获取技术包括：对计算机系统和文件的获取技术、对数据和软件的安全搜集技术、对磁盘或存储介质的安全无损备份技术、对删除文件的恢复重建技术等等

# §7.4 计算机取证相关技术

- 电子证据收集技术
  - ✓ 遵照授权方法，使用授权软硬件设备，将已收集数据进行保全，做一些预处理，转移到取证设备
- 电子证据保全技术
  - ✓ 应对电子证据及整套的取证机制进行保护
  - ✓ 保证电子证据的真实性、完全性和安全性
  - ✓ 常用技术包括：物理隔离、加密、数字签名、访问控制等

# §7.4 计算机取证相关技术

## 电子证据处理及鉴定技术

- ✓ 电子证据处理与鉴定是指对已收集的电子证据进行过滤、模式匹配、隐藏数据挖掘等预处理，然后进行数据统计、数据挖掘等分析工作，试图对攻击者身份、攻击的时间、目标、意图、手段，及造成的后果等给出明确且符合法律规范的说明
- ✓ 涉及技术包括：关键词匹配、数据挖掘、关联规则得等等

## 电子证据提交技术

- ✓ 以法庭可接受的证据形式提交电子证据及相应的文档说明

# §7.5 计算机取证工具

- 计算机取证工具分类
  - ✓ 证据获取工具
  - ✓ 证据保全工具
  - ✓ 证据分析工具
  - ✓ 证据归档工具

# §7.5 计算机取证工具

## 证据获取工具

- ✓ 主机系统证据获取工具
- ✓ 网络证据获取工具
- ✓ 计算机取证原则之一：应在不对原始证物进行任何改动或损坏的前提下获取证据，否则证据将不被法庭接受

## 证据保全工具

- ✓ 计算机取证原则之一：需要证明所获得的证据和原有的数据时完全相同的
- ✓ 保护证物的方法与技术：证物监督链、数字签名、数字时间戳

# §7.5 计算机取证工具

## 证据分析工具

- ✓ 证据分析是计算机取证的核心和关键，发现隐藏、可疑、篡改等
- ✓ 第一步通常是分析可疑硬盘的分区表
- ✓ 分析文件系统（目录树）
- ✓ 搜索关键词，找回被删除文件
- ✓ 使用文件浏览器打开各种格式文件
- ✓ 查阅大量图片
- ✓ 快速识别反常文件

## 证据归档工具

- ✓ 整理取证分析结果供法庭作为诉讼证据
- ✓ 计算机证据要同其他证据相互印证、相互联系起来综合分析