

# 网络风险评估和网络安全应对技术

## 第一部分：网络安全与内涵

1. 网络安全定义
2. 网络安全的属性
3. 网络安全风险及其分布
4. 网络安全的作用层次
5. 网络信息安全模型
6. 网络安全的总体框架

## 第二部分：网络安全的风险

1. 网络中存在的安全威胁
2. 网络攻击发展的趋势
3. 网络攻击的一般过程
4. 信息收集的一般方法
5. 利用安全扫描工具收集信息
6. 利用网络监听工具收集信息

## 第三部分：网络安全风险的评估

1. 网络安全风险评估准则
2. 信息安全风险评估流程
3. 网络安全风险系统综合评估思想
4. 网络安全风险评估指标体系构建
5. 网络安全风险评估指标处理方法

## 6.网络安全风险评估指标权重确定方法

### 第四部分：网络安全风险管理

#### 1.风险管理概述

##### 1.1 评估准备

##### 1.2 风险识别

##### 1.3 风险确认

##### 1.4 风险控制

#### 2.生命周期各阶段的风险管理

##### 2.1 与信息系统生命周期和信息系统安全目标的关系

##### 2.2 规划阶段的信息安全风险

##### 2.3 设计阶段的信息安全风险

##### 2.4 实施阶段的信息安全风险

##### 2.5 运维阶段的信息安全风险

##### 2.6 废弃阶段的信息安全风险

#### 3.网络安全风险控制策略

##### 3.1 物理安全策略

##### 3.2 软件安全策略

##### 3.3 管理安全策略

##### 3.4 数据安全策略

### 第五部分：网络安全风险的应对

## 1 . 密码技术基础

### 1.1 密码学的发展

### 1.2 密码体制

### 1.3 古典加密方法

### 1.4 对称加密技术

### 1.5 非对称加密技术

### 1.6 混合密码体制

### 1.7 密钥类型

### 1.8 密钥的分配

### 1.9 计算机网络密钥分配方法

## 2 . 数字签名技术&CA

### 2.1 数字签名的应用和特性

### 2.2 用对称加密算法进行数字签名

### 2.3 用非对称加密算法进行数字签名

### 2.4 PKI 的基本技术和组成

### 2.5 数字证书与 X.509

### 2.6 PKI 的核心(CA)

### 2.7 SSL 网站的创建

## 第六部分:风险评估工具与评估案例分析

### 1.技术型信息安全风险评估工具

### 2.漏洞扫描工具 渗透测试工具

### 3.风险评估辅助工具

### 4.网络安全风险的模糊综合评价

#### 4.1 一级系统模糊综合评价

#### 4.2 二级系统模糊综合评价

#### 4.3 带置信因子的系统模糊综合评价

#### 4.4 基于改进模糊综合评价方法的信息系统安全风险评估

#### 4.5 需求分析与系统工具选择

#### 4.6 网络安全风险评估系统的结构设计

#### 4.7 网络安全风险评估系统的详细设计