

NIST

**National Institute of
Standards and Technology**

Technology Administration
U.S. Department of Commerce

国家标准和技术研究所
技术局
美国商务部

计算机安全概论： NIST 手册

特别出版物 800-12

目录

第一部分 引言和概述

第一章 引言

- 1.1 目的
- 1.2 预期对象
- 1.3 本手册结构
- 1.4 重要术语
- 1.5 联邦计算机安全计划的法律基础

第二章 计算机安全的元素

- 2.1 计算机安全应该支持机构所要履行的使命
- 2.2 计算机安全是良好管理的一个不可分割组成部分
- 2.3 计算机安全应该具有良好的成本有效性
- 2.4 计算机安全的责任和职责应该得到明确阐述
- 2.5 系统所有者担负有超出本机构范围的计算机安全责任
- 2.6 计算机安全要求采用一种全面且完整的方法
- 2.7 计算机安全应该定期接受反复评估
- 2.8 计算机安全受社会因素制约

第三章 角色和责任

- 3.1 高级管理层
- 3.2 计算机安全管理者
- 3.3 项目和职能部门经理 / 应用拥有者
- 3.4 技术提供者
- 3.5 支持性部门
- 3.6 用户

第四章 常见威胁：简述

- 4.1 错误和疏忽
- 4.2 欺骗和盗窃
- 4.3 员工的破坏
- 4.4 失去物理和基础设施的支持
- 4.5 恶意黑客
- 4.6 工业间谍
- 4.7 恶意代码
- 4.8 外国政府的破坏
- 4.9 对个人隐私的威胁

第二部分 管理控制

第五章 计算机安全政策

- 5.1 方案政策
- 5.2 针对具体问题的政策
- 5.3 针对具体系统的政策
- 5.4 相互关联
- 5.5 成本因素

第六章 计算机安全方案管理

- 6.1 计算机安全方案的结构
- 6.2 中央计算机安全方案
- 6.3 行之有效的中央计算机安全方案的要素
- 6.4 系统层面计算机安全方案
- 6.5 系统层面计算机安全方案的要素
- 6.6 中央和系统层面计算机安全方案的交互作用
- 6.7 相互关联
- 6.8 成本因素

第七章 计算机安全风险管理

- 7.1 风险评估
- 7.2 降低风险
- 7.3 不确定性分析
- 7.4 相互关联
- 7.5 成本因素

第八章 计算机系统生命周期的安全和规划

- 8.1 《计算机安全法案》提出的联邦系统问题
- 8.2 将安全融入计算机系统生命周期的好处
- 8.3 计算机系统生命周期概述
- 8.4 计算机系统生命周期中的安全活动
- 8.5 相互关联
- 8.6 成本因素

第九章 保障

- 9.1 认可和保障
- 9.2 规划和保障
- 9.3 设计和实施保障
- 9.4 运行保障
- 9.5 相互关联
- 9.6 成本因素

第三部分 操作控制

第十章 人员 / 用户问题

- 10.1 人员
- 10.2 用户管理
- 10.3 合同商访问因素
- 110.4 公众访问因素
- 10.5 相互关联
- 10.6 成本因素

第十一章 意外和灾难防范

- 11.1 第一步: 确定与任务或业务相关的关键功能
- 11.2 第二步: 确定支持关键功能的资源
- 11.3 第三步: 预计潜在意外或灾难
- 11.4 第四步: 选择意外应对计划战略
- 11.5 第五步: 实施意外应对战略
- 11.6 第六步: 检验和修订
- 11.7 相互关联

11.8 成本因素

第十二章 计算机安全事件处理

12.1 事件处理能力的益处

12.2 成功的事件处理能力的特点

12.3 事件处理的技术支持

12.4 相互关联

12.5 成本因素

第十三章 意识、培训和教育

13.1 行为

13.2 可追究的责任

13.3 意识

13.4 培训

13.5 教育

13.6 实施

13.7 相互关联

13.8 成本因素

第十四章 计算机支持和运行中的安全考虑

14.1 用户支持

14.2 软件支持

14.3 配置管理

14.4 备份

14.5 媒体控制

14.6 文件

14.7 维护

14.8 相互关联

14.9 成本因素

第十五章 物理和环境安全

15.1 物理访问控制

15.2 防火安全因素

15.3 支持性公用设施故障

15.4 建筑结构损坏

15.5 管道破裂

15.6 数据窃听

15.7 移动和便携系统

15.8 实施方法

15.9 相互关联

15.10 成本因素

第四部分 技术控制

第十六章 识别和认证

16.1 基于用户知道的某物的识别和认证

16.2 基于用户拥有的某物的识别和认证

16.3 基于用户本身某物的识别和认证

16.4 识别和认证系统的实施

16.5 相互关联

16.6 成本因素

第十七章 逻辑访问控制

17.1 访问标准

17.2 政策：访问控制的推动力

17.3 技术实施机制

17.4 访问控制管理

17.5 访问控制协调

17.6 相互关联

17.7 成本因素

第十八章 审计踪迹

18.1 益处和目的

18.2 审计踪迹和日志

18.3 实施问题

18.4 相互关联

18.5 成本因素

第十九章 密码

19.1 基本加密技术

19.2 密码的使用

19.3 实施问题

19.4 相互关联

19.5 成本因素

第五部分 实例

第二十章 评估和降低一个虚构计算机系统的风险

20.1 风险评估

20.2 HGA 的计算机系统

20.3 HGA 资产面临的威胁

20.4 现行安全措施

20.5 风险评估小组报告的漏洞

20.6 有关减少被确定漏洞的建议

20.7 总结