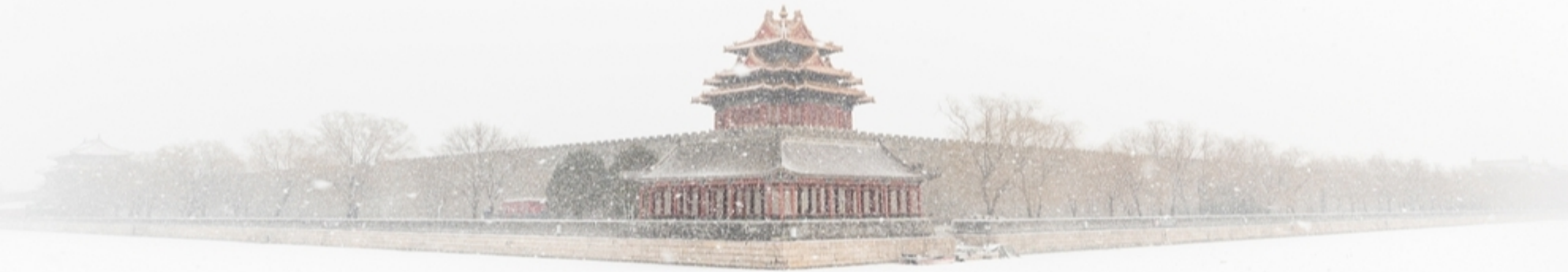
互联网安全技术与防御策略

制作人：
时　间：

目录



01

第1章 互联网安全技术基础

简介

01 **定义与重要性**

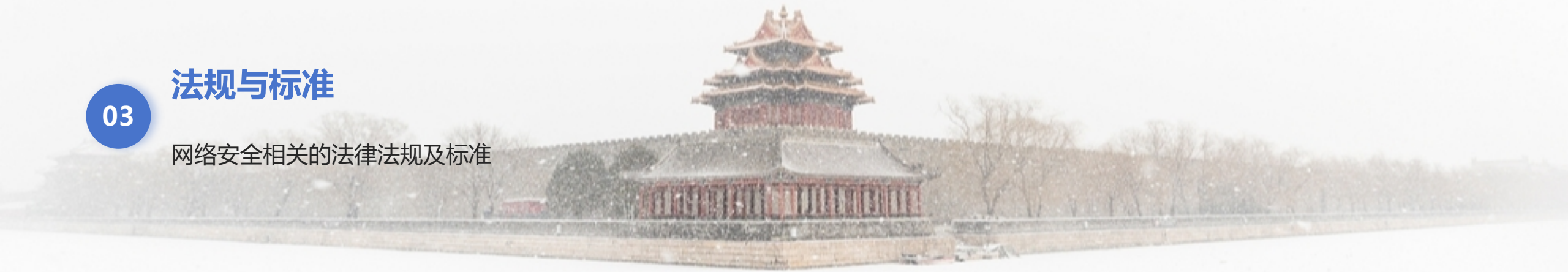
网络安全的含义及其重要性

02 **网络安全现状**

当前网络安全面临的挑战与问题

03 **法规与标准**

网络安全相关的法律法规及标准



网络安全体系

防火墙与入侵检测

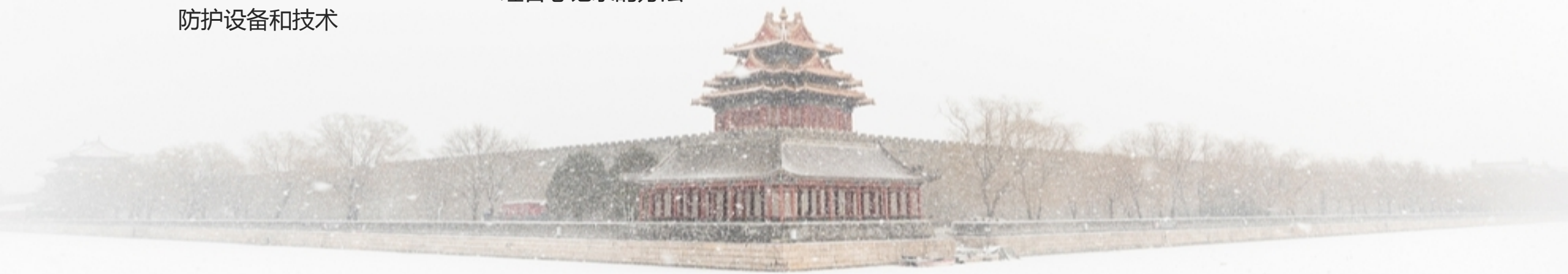
网络安全体系中的防护设备和技术

网络审计与日志管理

监控网络活动和管理日志记录的方法

数据加密与身份验证

保护数据安全和确认用户身份的技术



常见威胁与攻击

黑客攻击手段

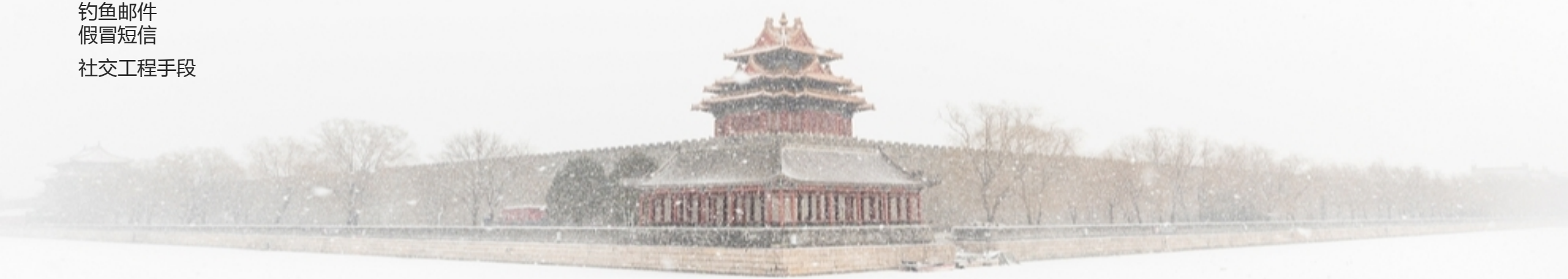
钓鱼攻击
DDoS攻击
SQL注入

病毒与蠕虫防范

防病毒软件
实时保护机制
邮件过滤

社会工程学攻击示例

钓鱼邮件
假冒短信
社交工程手段



安全策略与实践

制定网络安全策略和应对措施是保护网络安全的关键。通过风险评估和安全培训，提高员工的安全意识，建立应急响应和恢复计划，可以有效应对各种安全威胁。

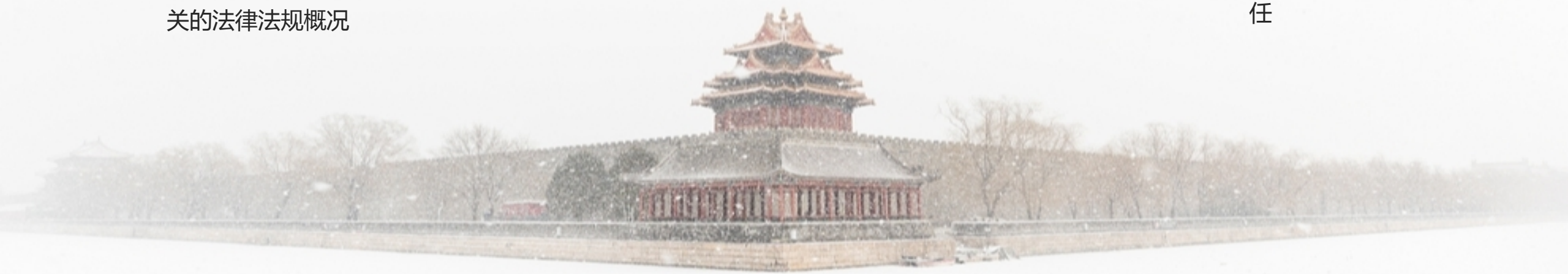
网络安全法规与案例

国内外法规概述

国内外网络安全相关的法律法规概况

案例分析与法律责任

网络安全事件案例分析和相关法律责任



未来趋势与挑战

01 **新技术影响**

新技术对网络安全的影响和应用

02 **隐私保护与数据安全**

用户隐私保护和数据安全的重要性

03 **法规更新与应对策略**

法律法规更新对企业安全策略的影响

02

第2章 网络安全架构

云安全

云安全是指在云计算环境下保护数据、应用程序和服务的安全性。云服务安全特性包括加密通信、身份认证和访问控制。在云环境下的安全挑战包括数据隐私、合规性和服务可用性。针对这些挑战，云安全解决方案主要包括数据加密、安全审计和网络隔离等措施。

物联网安全

设备安全与通信协议

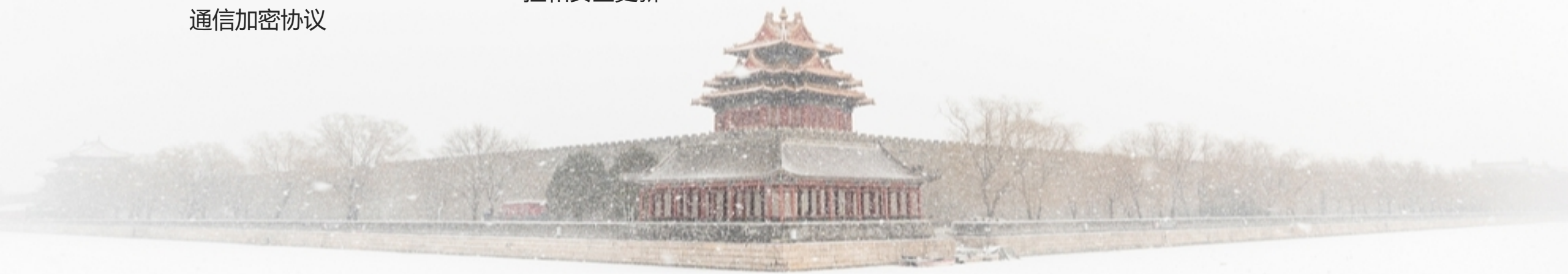
硬件和软件安全、通信加密协议

物联网安全策略

安全认证、远程监控和安全更新

物联网安全风险

设备漏洞、数据泄露风险



移动设备安全

01 **Android与iOS安全**

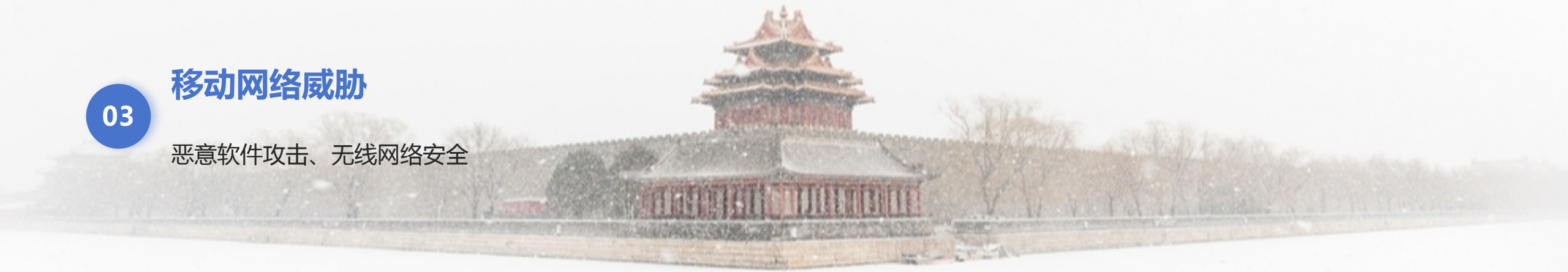
操作系统安全机制、应用权限管理

02 **应用安全与隐私保护**

应用程序漏洞、个人信息保护

03 **移动网络威胁**

恶意软件攻击、无线网络安全



网络安全法规与法规遵从

针对不同领域的法规要求

金融行业的支付安全标准

医疗行业的个人健康信息保护法规

合规实践与案例

企业信息安全管理系统建设实践

个人隐私数据合规案例分析

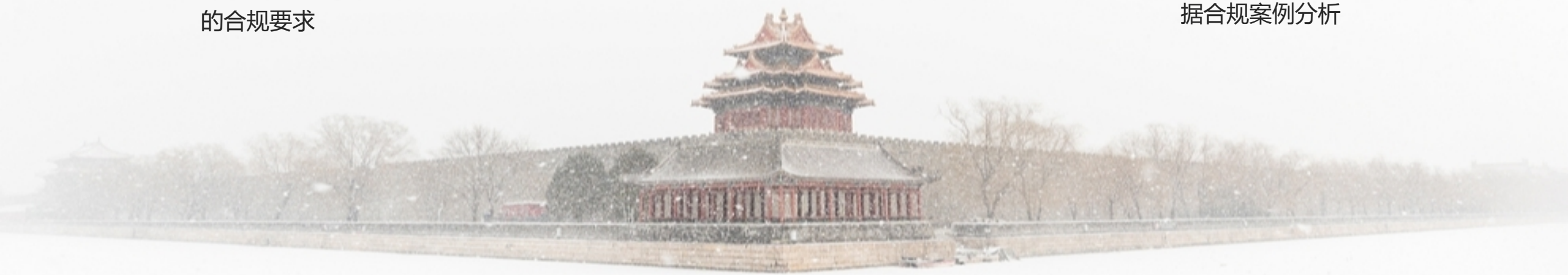
网络安全法规与法规遵从

针对不同领域的法规要求

金融、医疗等行业的合规要求

合规实践与案例

企业信息安全管理实践、个人隐私数据合规案例分析



03

第3章 网络安全运维与管理

安全运维流程

安全运维流程是企业网络安全的重要组成部分。日常维护与更新、漏洞管理与补丁更新、安全事件响应，是安全运维流程中的关键环节。通过建立完善的安全运维流程，可有效提升网络安全防御能力。

网络安全团队建设

角色与职责

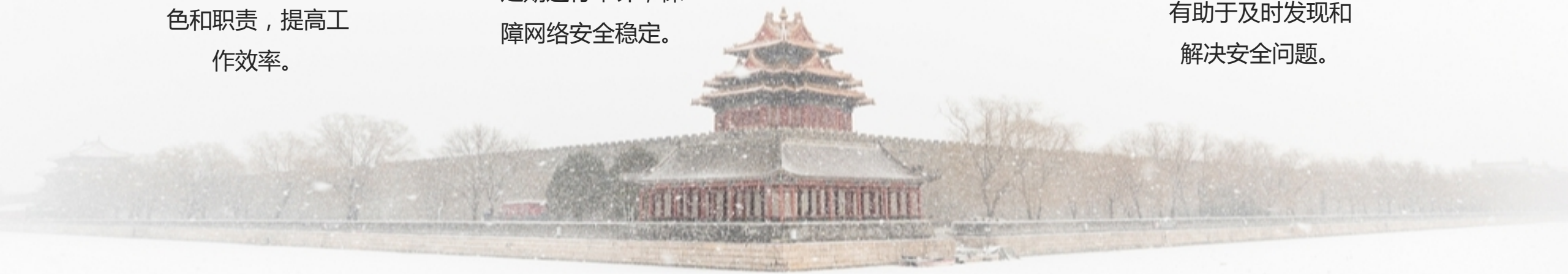
明确团队成员的角色和职责，提高工作效率。

持续改进与审计

不断改进安全措施，定期进行审计，保障网络安全稳定。

团队协作与沟通

团队成员之间的有效沟通和密切合作，有助于及时发现和解决安全问题。



网络安全审计与合规检查

网络安全审计与合规检查是确保企业网络安全的重要手段。通过内部审计方法、ISO 27001认证以及对合规挑战的应对，企业可以全面了解自身网络安全状况，并及时采取措施进行改进和应对。

网络安全教育与培训

网络安全意识提升

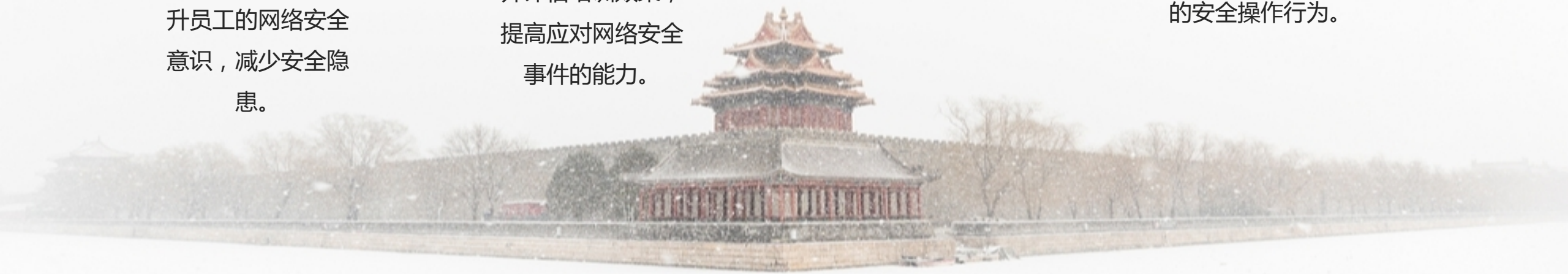
通过教育与培训提升员工的网络安全意识，减少安全隐患。

应急演练与培训效果评估

定期进行应急演练，并评估培训效果，提高应对网络安全事件的能力。

安全操作指南

制定并传达安全操作指南，规范员工的安全操作行为。



04

第4章 网络安全案例分析

重大安全事件回顾

波士顿银行数据泄露

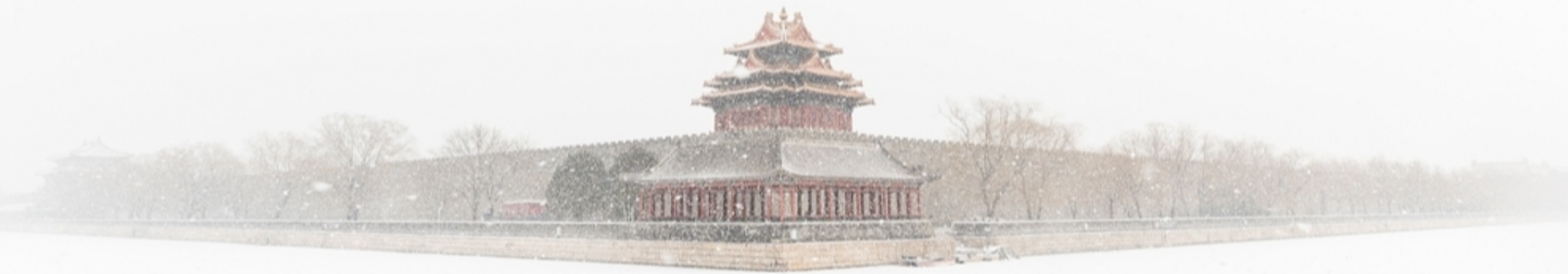
影响与教训

网络安全事件的影响与教训

应对策略

Equifax数据泄露

影响与教训



以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：
https://d.book118.com/046152221124010140