# 通信计算机信息安全问题及解决对策

杨杭杭
武汉地铁桥隧管理有限公司　湖北　武汉　430060

**摘　要：**通信计算机信息安全问题日益突出，随着技术的不断进步，网络威胁也在不断演变。本文首先分析了通信计算机信息安全面临的主要问题，包括数据泄露、恶意软件等。然后，针对这些问题，提出相应的解决对策。这些对策可以有效提高通信计算机信息的安全性，保障个人和企业的合法权益。

**关键词：**通信计算机；信息安全；解决对策

## 1 通信计算机信息安全的重要性

通信计算机信息安全不仅关系到个人隐私和企业机密的保护，更直接影响到国家安全和社会稳定。第一，通信计算机信息安全对于个人隐私的保护具有重要意义。在当今社会，个人信息的收集、传输和存储都依赖于通信计算机系统。一旦个人信息泄露，可能会导致身份盗窃、网络诈骗等问题的发生，对个人造成经济损失和精神困扰。因此，保障通信计算机信息安全是维护个人隐私的必要手段。第二，通信计算机信息安全对于企业机密的保护至关重要。商业机密是企业核心竞争力的重要组成部分，关系到企业的生存和发展。一旦企业机密泄露，可能会给企业带来重大损失，甚至危及企业的生存。因此，加强通信计算机信息安全防护是保障企业健康发展的必要条件。第三，通信计算机信息安全对于国家安全和社会稳定具有重要意义。国家信息安全关乎国家安全和社会稳定。政府机关、军事部门等重要机构的信息安全防护更是重中之重。如果国家信息安全受到威胁，可能会导致国家机密泄露、社会秩序混乱等严重后果。因此，保障通信计算机信息安全是维护国家安全和社会稳定的必要保障[1]。

## 2 通信计算机信息安全问题

### 2.1 计算机病毒与恶意软件的威胁

计算机病毒是一种能够自我复制的计算机程序，通过插入恶意代码来破坏计算机系统，窃取用户信息或干扰计算机的正常运行。病毒可以通过网络、电子邮件、移动存储设备等途径传播，一旦感染，会对计算机系统造成不同程度的损害。恶意软件则是一种旨在破坏、干扰或控制计算机系统的软件。恶意软件种类繁多，包括间谍软件、广告软件、勒索软件等。这些软件通常会在用户不知情的情况下，在其电脑上安装后门、收集用户个人信息、篡改系统设置等，对用户的隐私和数据安全构成严重威胁。计算机病毒和恶意软件的不断演变和升级，使得其传播速度更快、隐蔽性更强、破坏力更大。它们不仅威胁个人用户的信息安全，也对企业的网络安全构成严重威胁。

### 2.2 网络攻击与黑客行为

网络攻击的形式多样，包括拒绝服务攻击、分布式拒绝服务攻击、缓冲区溢出攻击等。这些攻击利用各种手段，对目标系统进行干扰、破坏或控制，以达到非法目的。拒绝服务攻击通过大量无用的请求拥塞目标系统，使其无法正常响应；分布式拒绝服务攻击则通过控制多个计算机或网络僵尸，对目标系统发起攻击，使其瘫痪。黑客行为则是指黑客利用系统漏洞、恶意代码等手段，对计算机系统进行非法入侵和破坏的行为。黑客可能会盗取用户账号、密码等敏感信息，窃取商业机密、个人隐私等，甚至篡改网站内容、发动网络勒索等。网络攻击与黑客行为的频频发生，对国家安全、经济发展和民众生活造成极大的危害。攻击政府机关或军事机构可能威胁国家安全；攻击金融机构可能引发经济损失；攻击基础设施可能影响社会稳定；攻击个人用户则可能侵犯个人隐私和权益。

### 2.3 身份伪造与信息篡改

身份伪造通常是指攻击者通过非法手段获取他人的个人信息，然后利用这些信息冒充他人进行恶意活动。例如，攻击者可能会伪造他人的电子邮件地址或社交媒体账号，以实施诈骗、传播虚假信息或破坏他人声誉。在网络安全领域，身份伪造还可能涉及到假冒网络设备、IP地址等，以逃避追踪或干扰网络通信。信息篡改则是指未经授权地修改、删除或篡改数据内容，导致信息的失真或损坏。这种篡改可能发生在各种形式的数据中，包括文件、数据库、网络通信等[2]。例如，篡改电子文档的内容、在网络新闻中插入虚假信息或对关键系统的数据实施非法修改等。信息篡改的目的是为了干扰、误导或破坏正常的信息交流和服务。

2.4 敏感数据泄露与隐私侵犯

敏感数据泄露通常是由于系统漏洞、人为错误或恶意攻击等原因引起的。一旦敏感数据落入不法分子之手，可能会被用于身份盗窃、网络诈骗、金融欺诈等违法犯罪行为，给个人和社会带来巨大的危害。例如，在医疗领域，患者的隐私信息泄露可能会导致个人隐私被侵犯；在金融领域，客户的敏感信息泄露可能引发财务损失和信用风险。隐私侵犯则是指未经用户同意或未明确告知用户的情况下，对用户的个人信息进行收集、使用或披露的行为。随着互联网和移动互联网的普及，用户的隐私信息变得越来越容易被收集和使用。一些应用程序和服务在收集用户信息时并未得到用户的明确同意，或未清晰地告知用户其信息使用目的和范围，这导致用户的隐私权被侵犯。

## 3 通信计算机信息安全解决对策

3.1 网络安全策略

面对通信计算机信息安全问题，采取有效的解决对策是至关重要的。首先，制定全面的网络安全策略是必要的。明确规定安全目标和要求，确定安全控制措施和操作规程，以确保网络的安全稳定运行。安全策略应涵盖物理安全、网络安全、数据安全和应用安全等方面，确保从多个层面保护信息资产的安全。其次，加强网络访问控制是保障网络安全的重要措施。实施严格的访问控制策略，可以限制对敏感资源的访问，防止未经授权的访问和恶意攻击。访问控制应包括用户身份验证、权限管理和日志审计等方面，确保只有合法的用户能够访问所需的资源。数据加密也是保障数据传输和存储安全的有效手段。通过加密技术，可以确保数据在传输过程中不被窃取或篡改，保证数据的完整性和机密性。建立完善的安全审计机制也是必要的。定期对网络系统和应用程序进行安全审计，可以及时发现潜在的安全隐患和漏洞，采取相应的措施进行修复和改进。审计结果还可以用于评估网络安全的状况和改进的方向。

3.2 数据保护方案

数据保护方案旨在确保数据的机密性、完整性和可用性，防止数据泄露、篡改或损坏。（1）数据加密是实现数据保护的基础手段。通过加密算法对敏感数据进行加密处理，可以确保数据在传输和存储过程中的机密性。加密算法应具备足够的强度和安全性，以抵抗各种攻击和破解尝试。定期更新和替换密钥，以降低密钥泄露的风险。（2）数据备份和恢复是保障数据完整性和可用性的关键措施。定期对数据进行备份，可以在数据损坏或丢失时进行恢复，减少数据丢失的风险。备份策略应根据数据的价值和重要性制定，同时考虑备份数据的存储位置和存储介质的安全性[3]。（3）数据脱敏也是保护敏感数据的有效方法。通过对敏感数据进行脱敏处理，可以去除或掩盖敏感信息，降低数据泄露的风险。脱敏方法包括删除、替换、模糊化等，应根据数据的类型和用途选择合适的方法。（4）数据访问控制也是保障数据安全的重要手段。通过实施严格的访问控制策略，可以限制对敏感数据的访问权限，防止未经授权的访问和恶意攻击。访问控制应包括用户身份验证、权限管理和日志审计等方面，确保只有合法的用户能够访问所需的敏感数据。

3.3 身份认证措施

通过实施有效的身份认证措施，可以降低未经授权访问、数据泄露等安全风险。除了传统的用户名和密码认证外，引入其他验证因素，如动态令牌、指纹识别、面部识别等，可以增加攻击者冒充的难度。这样即使密码被破解，攻击者仍需要其他验证因素才能成功登录。要求用户设置足够长且难以猜测的密码，并定期更换密码。同时，限制密码的重试次数，以防止暴力破解攻击。对于高敏感数据的访问，可以采用双因素身份认证或动态令牌等方法来提高安全性。通过单点登录，用户只需在可信的应用程序或设备上进行一次身份验证，就可以访问其他关联的应用程序或服务。这样可以减少重复验证的步骤，提高用户体验和系统的安全性。为了保护企业网络中的敏感信息和关键数据，可以将数据进行分级存储和访问控制。不同的数据级别设置不同的权限和认证级别。员工访问敏感数据时需要经过更高级别的身份验证或审批。这有助于减少非授权访问的风险和保护企业机密信息的保密性。随着移动设备的普及，越来越多的应用程序和数据在移动设备上存储和处理。

3.4 恶意软件防范

防病毒软件可以对系统进行实时监控，检测和清除恶意软件。应选择具有良好信誉和及时更新病毒库的防病毒软件，并定期更新病毒库以应对新出现的威胁。及时更新系统和应用程序的补丁可以修复已知的安全漏洞，防止恶意软件利用漏洞进行攻击。应定期检查更新，并尽快应用安全补丁。安全扫描可以检测系统中的潜在安全问题，而漏洞评估则可以帮助识别系统和应用程序中的漏洞。及时发现和修复漏洞可以降低恶意软件入侵的风险。用户应了解恶意软件的常见传播途径和行为，避免打开未知来源的邮件和链接，不要随意下载和安装未经认证的应用程序。通过提高用户的安全意识，可以降低被恶意软件攻击的风险。建立防火墙、入侵检

测系统等网络安全设施可以有效地阻止恶意软件的入侵。通过监控网络流量和异常行为，可以及时发现和阻止恶意软件的传播和活动。

3.5 技术创新与研发

随着技术的不断发展和网络威胁的不断演变，要持续投入资源进行技术创新和研发，以应对新的安全挑战。企业应关注新兴的安全技术和方法，积极开展技术研发和创新，开发出更加高效、智能的安全防护产品和服务。这包括但不限于加密技术、入侵检测系统、安全漏洞扫描工具、云安全技术等。随着网络威胁的演变，现有的安全技术可能已经不足以应对新的威胁。因此，要对现有技术进行不断改进和升级，提高其防护能力。应对现有技术进行定期评估和审计，及时发现和修复潜在的安全问题。企业可以与高校、研究机构等建立合作关系，共同开展信息安全领域的研究和创新项目。通过共享资源和知识，可以加速技术创新和研发的进程，提高技术的领先优势。注重人才引进和培养，建立完善的人才激励机制，激发员工的创新精神和技术能力。提供良好的工作环境和发展机会，吸引和留住优秀的技术人才，为企业的技术创新和研发提供坚实的人才基础。

**4 通信计算机信息安全的未来技术发展趋势**

随着技术的快速进步，通信计算机信息安全的未来技术发展趋势将呈现出以下几个方向：第一，量子计算将对信息安全领域产生深远影响。随着量子计算机的不断发展，传统的加密算法可能会面临被破解的风险。因此，开发抗量子计算的安全加密算法将是未来的一个重要研究方向。利用量子力学原理实现更高效的信息加密和传输也将成为研究的热点。第二，边缘计算将在信息安全领域发挥重要作用。随着物联网和5G技术的普及，越来越多的数据将在边缘设备上生成和处理。为了确保这些数据的安全，需要发展边缘计算安全技术，包括边缘设备的身份验证、数据加密和隐私保护等方面[4]。第三，人工智能和机器学习技术将继续在信息安全领域发挥关键作用。通过训练模型来识别和防御新型威胁、自动化漏洞扫描和修复、实时监控网络流量等应用场景，人工智能和机器学习技术将进一步提高信息安全的防御能力。随着技术的不断发展，需要关注人工智能自身的安全问题，如对抗性攻击、模型窃取等。第四，区块链技术将在信息安全领域得到更广泛的应用。区块链的去中心化、可追溯和不可篡改等特点为信息安全提供了新的解决方案。第五，隐私保护技术将继续发展并受到重视。随着人们对个人隐私的关注度不断提高，隐私保护技术的研究和应用将更加广泛。这包括差分隐私、同态加密、零知识证明等技术在数据收集、存储和使用等方面的应用，确保个人隐私得到充分保护。

**结束语**

通信计算机信息安全是一个复杂而重要的领域，需要不断关注和研究。随着技术的不断进步，新的安全威胁和挑战也将不断出现。因此，不断加强技术研发和创新，提高安全防护能力只有通过不断努力和创新，才能确保通信计算机信息的安全，为个人和企业提供更加可靠和安全的网络环境。

**参考文献**

[1]李文杰.通信计算机信息安全问题及解决对策[J].中国宽带,2021(2):18.

[2]杨佳霈.通信计算机信息安全问题及解决对策[J].网络安全技术与应用,2021(1):160-161.DOI:10.3969/j.issn.1009-6833.2021.01.090.

[3]孙建中.通信计算机信息安全问题及解决对策分析[J].科技视界,2021(12):187-188.DOI:10.19694/j.cnki.issn2095-2457.2021.12.66.

[4]何应发.通信计算机信息安全问题及解决对策分析[J].信息记录材料,2020,21(1):48-49.