# 大数据时代如何加强计算机网络信息安全管理

党　正
大唐山西电力工程有限公司 山西 太原 030003

**【摘　要】**在大数据时代，计算机网络的普及和信息的流动性大大促进了社会的发展和进步。然而，随之而来的是信息安全的威胁和风险也日益增加。计算机网络信息安全管理成为了摆在我们面前的重要课题。如何加强计算机网络信息安全管理已经成为了一个迫切需要解决的问题。只有加强信息安全管理，才能保障网络信息的安全性和可靠性，推动数字经济的发展。因此，本文将探讨大数据时代下加强计算机网络信息安全管理的意义和方法，以期为信息安全管理者提供一些有益的思路和建议。

**【关键词】**大数据时代；计算机；网络信息

## 引言

近年来，伴随我国信息化技术水平的不断提高，我国也进入了大数据时代，大数据技术为人们的生活和工作带来的极大的便利，同时也在一定程度上对信息安全带来了一定的风险，这就对计算机网络信息安全管理工作提出了更高的要求。由于大数据中蕴含大量的个人信息，如果安全防护工作不到位，则会导致个人信息泄露，进而引发一系列的信息安全问题。只有通过强化网络环境管理，并结合先进的信息安全防护技术，才能有效将网络信息安全风险降到最低。

## 1.大数据时代的网络信息安全特征

大数据技术的应用有效提升了工作的效率和生活的便捷性，但是，大数据系统中蕴含海量信息，这些信息中会涉及人们工作和生活的各方面内容，例如个人手机中的照片、录像、录音甚至的网络银行支付密码等。随着信息时代的不断发展，一部分人开始发现网络个人信息的巨大价值，并通过不法手段获取以换取高额经济利益。如果这些个人信息落入不法分子手中将会给信息所有者造成严重的影响，甚至会莫名地背负罪名。但是，目前的互联网具有开放性特点，每个人都是一个小型的信息库，同时由于一些人对于网络安全防护的意识不强，给了一些不法分子可乘之机，同时也增加了网络信息安全管理工作的难度。因此，需要社会各界加强网络信息安全防护的宣传和管理，进而实现净化网络环境提升信息安全性的发展目标。

## 2.大数据时代网络信息安全控制的重要性

在当前的互联网中，包含大量的终端用户，同时由于用户的组成结构十分复杂，网络安全检查对于用户身份的合法性检查效率和准确性也会受到较大的影响，这就导致了网络安全漏洞的形成，同时，这也是造成网络信息泄露的主要原因。如果用户被黑客持续攻击，将会导致计算机系统处于无法正常运行的状态，其中的数据信息也会被黑客窃取。通过采用多种的网络信息安全控制手段，可以为计算机系统设置多道防护层，并在从访问到信息读取和处理环节都能做到安全防护，一旦发现异常则会及时对数据信息进行保护，并扫描系统存在的漏洞，进而实现保护网络信息安全，防止数据信息泄漏的目的。

## 3.大数据时代计算机网络信息安全管理优化策略研究

### 3.1.强化身份认证与访问控制

在大数据时代，加强身份认证与访问控制是一项重要的优化策略，可以通过采用更安全且先进的身份认证技术和访问控制机制，如双因素认证、生物特征识别等来加强用户身份验证，并限制其访问权限。首先，采用双因素认证可以提高用户身份验证的安全性。传统的用户名和密码认证方式容易受到猜测、破解和恶意攻击的威胁。而双因素认证结合了两个或多个不同的验证要素，如密码、指纹、面部识别等，使攻击者更难以突破多重验证，从而有效防止未经授权的用户访问敏感信息和系统资源。其次，生物特征识别作为一种先进的身份认证技术，可以使用个人独特的生物特征进行身份验证，如指纹、虹膜、面部等。这种技术基于每个人身体本身所具备的特征，不易伪造或盗用，因此能够更可靠地验证用户的身份，防止冒名顶替和未授权访问。此外，通过设立访问控制策略，可以限制用户访问敏感信息和系统资源的权限。根据用户的角色和需求，采用细粒度的访问控制机制，确保用户只能访问其合法权限之内的数据和资源。这种访问控制策略有效减少了内部和外部威胁对敏感信息的访问风险。

### 3.2.数据加密与隐私保护

在大数据时代，数据加密与隐私保护是保护敏感信息和隐私的重要手段之一。为了保证数据的安全性，在

数据传输和存储过程中采用加密技术是必不可少的。首先，可以采用对称加密和非对称加密的组合方式来加密数据。对称加密使用相同的密钥进行数据的加密和解密，速度较快，但密钥的安全性需要保证。非对称加密使用公钥和私钥进行数据的加密和解密，提供了更高的安全性，但处理速度较慢。通过结合两种加密方式的优势，可以同时兼顾速度和安全性，确保数据在传输过程中的保密性。其次，安全的密钥管理机制对于数据加密的重要性不可忽视。密钥是加密和解密的关键，必须妥善管理，防止密钥的泄露和不当使用。采用安全的密钥管理机制，如密钥分发、更新和存储的安全控制，可以保证密钥的机密性和完整性，提高数据加密的安全性。此外，隐私保护也是数据加密的核心目标之一。隐私保护包括对敏感数据的脱敏处理、匿名化处理和数据授权访问控制等。通过脱敏处理，可以将敏感数据进行替换或删除，使攻击者无法直接获取到原始敏感数据。匿名化处理则是通过消除数据中的个体身份信息，使得数据无法与特定个体相关联。数据授权访问控制则是针对不同的用户和角色，设立不同的访问权限，确保数据仅在合法授权的范围内被访问和使用。通过采用对称加密和非对称加密的组合方式，以及安全的密钥管理机制，可以保证数据在传输和存储过程中的安全性。同时，隐私保护的措施如脱敏处理、匿名化处理和数据授权访问控制等也能有效保护数据的隐私，确保数据仅在合法授权的范围内被访问和使用。这样的数据加密与隐私保护机制将在大数据时代中发挥重要作用，提高数据安全和隐私保护水平。

## 4.结束语

在目前的网络环境中，还存在着各类的网络攻击及病毒植入行为，这将导致计算机系统的数据安全性受到威胁。因此，相关单位需要进一步提升对于网络信息安全防护的重视程度，并采取科学的方式进行处理，通过采取制度建设、技术防护、安全监测等多种路径实现对计算机系统的全面防护，将网络中潜在的安全风险排除，进而有效保证网络信息的安全性。

## 【参考文献】

[1]胡中尧.大数据时代背景下计算机网络信息安全与防护[J].通讯世界，2019,26(01):39-40.

[2]廖兰芳，李耀鹏.大数据时代计算机网络信息安全与防护方法[J].电子测试，2019(09):130-131.