DOI:10.12361/2705-0866-05-02-116827

# 基于大数据时代的计算机网络安全防范措施研究

祁元超　朱圣智　邱小满
武汉东湖学院，中国·湖北 武汉 430212

【摘　要】如今，随着我国计算机技术的显着提高，越来越多的企业将大数据技术用于日常管理，但由于计算机网络的特点，相关员工在数据传输管理过程中容易受到网络安全的威胁，导致数据泄露，严重影响企业运营，因此相关员工需要在大数据时代的背景下，提高计算机网络的整体安全性和可靠性。在此基础上，探讨大数据时代的计算机网络保护措施，以供参考。

【关键词】大数据时代；计算机网络安全；防范措施

# Research on Computer Network Security Precautions Based on Big Data Era

**Yuanchao Qi, Shengzhi Zhu, Xiaoman Qiu**
*Wuhan East Lake University,Wuhan,Hubei,China 430212*

[Abstract] Today, with the significant improvement of China's computer technology, more and more enterprises use big data technology for daily management. However, due to the characteristics of computer networks, relevant employees are vulnerable to network security threats in the process of data transmission and management, resulting in data leakage, and seriously affecting enterprise operations. Therefore, relevant employees need to improve the overall security and reliability of computer networks in the context of the big data era. On this basis, the computer network protection measures in the era of big data are discussed for reference.

[Keywords] Big data era; Computer network security; Preventive measures

## 引言

计算机网络技术是人们进入到21世纪的一种标志性技术，经过长时间的快速发展，我国的计算机水平也逐渐提升，大大推动着国内信息技术的发展进步。人们的生活以及生产当中融入了越来越多各式各样的信息手段，给予了人们生活极大的便利，能够对工业生存的效率进行显著的提高，计算机网络技术的到来也进一步推动了社会当中的压迫变革。但是在如今大发展大进步的时代背景之下，计算机网络安全也备受瞩目，信息安全问题非常严峻，越来越多的信息输送到了大数据当中，任何人都可以比较轻易查询到个人的因素，对用户的隐私性造成严重的影响。

## 1　落实计算机网络安全防范措施的重要性

在大数据时代环境下，加强计算机网络安全防范管理具有较大的现实意义。新时期，企业以及相关单位在经营运作过程中实现了网络化、信息化的管理运作模式，在财务管理、档案资料管理方面均应用了高质量、高效率的信息化、智能化管理手段，而在此过程中衍生出的信息安全问题也需要得到重视。各行各业结合大数据技术提高了工作的便捷性，在此过程中，加强信息安全管理、维护网络安全对于提高社会生产效率具有较大的作用，无论是个人还是企业，在日常经营运作、生活工作中均会产生大量的数据资料，而要想维护信息安全，就必须做好相关资料数据定向化的安全处理。在大数据时代，数据资料成为企业内部核心生产要素，涉及企业商业机密、战略发展规划，只有保障计算机网络安全，才能确保企业高效稳定地经营发展。总之，在当今数字经济环境下，企业以及相关机构部门需要加大网络安全管控力度，结合新思路、新思想，对现有的网络安全管理工作流程进行革新优化，运用新技术提高网络安全管控水平。

## 2　大数据时代计算机网络安全问题

### 2.1 不法分子恶意攻击

在网络环境中，不仅有许多普通用户，而且还有许多非法用户。这些非法利用各种网络技术入侵网络环境，从而窃取用户的数据和数据。信息安全的另一个安全风险是被动网络攻击，它不会危及用户网络的安全。但是，安装各种病毒会导致网络瘫痪，一旦这些病毒被激活，大量用户数据就会发送到错误的分子。当今信息时代，非法恶意攻击对网络安全构成严重威胁，许多用户遭受了巨大的经济损失。

### 2.2 用户信息容易泄露

如今，我们正处于一个数据量巨大的时代，其中有多种信息资源可用，计算机网络生成大量数据，这些数据更加复杂，而且由于独特的网络特性，例如开放性、外部入侵者更容易使系统更容易感染病毒，并使用户更容易在计算机网络上收集数据。

### 2.3 非法用户接入

由于无线网络设置过于简单，非法用户很容易进入到无线网络系统中，影响无线网络正常运行。用户在购买并安装无线网络后，没有意识到安全防护问题，容易让他人一起分享网络带

宽，影响用户带宽，使网络传输速度降低。如果非法用户在接入无线网络后下载带有病毒的软件，会造成计算机病毒侵入。另外非法用户为了可以达到加大带宽的目的，会修改路由器设置，影响合法用户网络的正常接入。非法用户在进入无线网络系统中也会盗取合法用户的隐私信息进行违法活动等，给合法用户带来一定的安全威胁。

## 3 大数据时代的计算机网络安全防范措施

### 3.1 专业防火墙技术

防火墙技术可以归纳到传统信息安全技术处理范围内，此技术经过长期研究和发展，已变得越来越成熟，目前已经成为计算机大数据信息安全处理技术中的重要技术之一。专业防火墙技术通常都会应用在网络内部环境中，最常见的防火墙有过滤防火墙和应用级防火墙。其中，应用级防火墙可以为计算机运行提供一个安全可靠的环境，对整个运行系统实施全方位监管，能够及时发现各种不利因素对计算机系统的入侵情况，一旦发现病毒入侵，应用级防火墙可以及时切断病毒传输途径，进而将病毒隔绝在计算机系统外。过滤防火墙技术将计算机系统自身的特点和功能整合在了一起，通过二者共同配合完成对计算机系统全方位检测，能够对发现的病毒彻底查杀，将病毒消除在源头，维持良好的计算机系统运行环境。通过应用专业防火墙技术，能将病毒和重要信息相互隔离，使计算机大数据信息安全得到充分保护，避免了数据丢失问题，保证了信息数据的安全性。

### 3.2 做好黑客防范工作

考虑到我国大型数据技术的日益普及和黑客的日益增多，这也是对网络安全的巨大威胁。因此，必须保护相关人员免受黑客攻击。通过在确保计算机网络安全的同时收集相关数据，总体提高了计算机网络的安全性。这将基于黑客的攻击特征创建一个模型，以加快黑客检测速度。此外，员工还可以利用内部网和外部网的隔离，并改进防火墙配置，以更好地抵御黑客攻击。此外，有关人员可以利用数字认证技术有效控制接入，防止计算机网络受到非法检查，从而提高计算机网络的整体安全性。

### 3.3 提升人文保护的实施力度

网络用户必须知道网络信息有被多种因素破坏的危险，必须提高安全意识来保护网络安全信息。使用网络时，计算机用户必须加强信息安全措施，定期更改在线银行密码，不单击非法网站和信息，不使用不安全的链接，充分保护网络密码，以减少用户信息被窃取的风险。由于网络信息提供者属于数据提供者，而且网络信息的处理是主动的，因此承担一定程度的网络信息保护责任是很重要的。信息服务提供商必须时刻牢记自己的任务和责任，严格遵守网络信息安全法律法规，并有效地保护网络用户数据的安全使用。此外，网络安全司必须履行职责，并意识到在网络信息安全受到威胁的情况下，必须采取适当措施，提高信息安全的预测力，加强信息安全防护。同时，还需要履行信息监督职能，制定更加完善的信息安全监管措施并且对其进行落实，借助切实有效的措施对网络信息安全进行保障。信息安全监管人员还必须提高自身的技术处理水平，完成好网络信息安全监督管理工作。

### 3.4 建立完善的计算机网络安全管理法律法规

近年来，计算机技术的发展革新速度相对较快，但与之配套的法律法规和安全管理规定未得到及时高效的更新，不少网络不法分子借助法律漏洞、信息安全漏洞开展一系列非法经营运作活动，对计算机网络安全管理工作造成较大的威胁，在缺乏法律依据以及法律制度保障的情况下，不法分子利用信息安全漏洞、法律漏洞损害公共网络安全，严重扰乱市场运行的安全性、稳定性。当前，我国需要加大立法监督力度，规范管控现阶段计算机网络行为。同时，执法部门还需要加强对信息安全犯罪强有力的管控，对于非法窃取、销售个人信息的人员进行严厉处罚。在每轮技术创新、技术革新的背景下，我国均需要颁布与之对应的法律法规，满足计算机技术发展变革下的安全管理需求，建立生态化的网络安全法律保障体系，维护互联网健康、长远、稳定发展。此外，无论是企业，还是个人，在使用计算机的过程中都需要具备较强的计算机安全意识，严格按照相关规定和要求使用计算机与网络，避免计算机遭受恶意攻击。同时，企业在计算机安全管理工作中也需要明确安全管理事件、安全操作流程，为资产信息数据提供全方位的安全保障。

### 3.5 计算机网络安全平台大数据中心的安全设计

（1）大数据中心设计思路。基于对分步实施与多层防护原则的遵循，执行对计算机网络安全平台大数据中心的设计任务，其主要思路为通过设计外部三层安全保护，达到有效围绕大数据中心服务器的目的。（2）大数据中心安全规划。大数据中心安全规划主要由两种方式构成：①以IPS部署为基础的防御功能的实现；②以防火墙部署为基础条件的访问控制的实现。为了从真正意义上实现企业业务的持续性以及稳定性增长，将计算机安全平台运行过程中容易出现的拥堵问题发生率降低至最低水平，需要针对性地加快部署的步伐，在保证部署科学性与有效性的同时缩短部署工作所用时间。（3）大数据中心配置。通过交换机以及路由器等相关设备的汇聚接入，达到对大数据的安全配置目的。此处以防病毒数据的配置为例展开相对细化的分析，其他各项相关配置任务的实现可以基于设备登录与网关系统的支持来完成。

## 结束语

当前，在计算机网络安全风险防范工作中，企业和个人需要养成良好的习惯，构建安全防护体系，严格按照相应的法律法规、规章制度文明上网、安全上网，提高计算机安全风险防范水平。

**参考文献：**

[1]石鑫.大数据时代的计算机网络安全及防范措施探讨[J].电脑知识与技术,2020,16(03):43-44.

[2]张玉英.大数据时代的计算机网络安全及防范措施[J].电子技术与软件工程,2020(02):259-260.

[3]周鹏程,于青.大数据时代计算机网络安全防范探讨[J].信息记录材料,2020,21(01):50-52.

[4]孙志斌.大数据时代计算机网络安全及有效防范措施研究[J].数码世界,2020(01):50-51.

[5]周光前.大数据时代下计算机网络安全的防范措施[J].信息与电脑(理论版),2019,31(24):189-190+193.

[6]曾荣江.大数据时代计算机网络安全防范策略[J].无线互联科技,2019,16(24):15-16.

[7]刘旸.试谈大数据时代的计算机网络安全及防范措施[J].数字技术与应用,2019,37(12):196+198.

[8]周莹.大数据时代计算机网络安全及防范措施研究[J].黑龙江科学,2019,10(24):112-113.