大数据时代的计算机网络安全技术及防范探讨

刘子祺*
水利部小浪底水利枢纽管理中心，河南 450000

摘　要：在大数据时代，网络信息与数据传播方式和途径逐渐多样化，计算机网络存在的安全问题涉及范围很广，如网络病毒入侵、非法链接、网络系统漏洞等多种安全风险，严重影响人们正常使用，甚至会造成难以挽回的损失。本文对大数据时代的计算机网络安全技术及防范进行探讨。

关键词：大数据时代；计算机；网络安全；防范对策

一、大数据时代下计算机网络安全基本属性变化与问题

（一）网络安全基本属性的变化

与IT时代网络信息安全的保密性、可用性、可控性、不可否认性属性不同，大数据时代的信息安全需求有了新的变化，如某些企业可以从消费者的消费中获取用户概况和偏好，从而进行商业产品定向推送。这些都表明大数据时代下，网络信息安全属性有了新的内涵。

1. 私密性

大数据的私密性是指数据的获取需要得到授权，有选择地控制群体对数据的获取。大数据的私密性主要包括开放（完全公开，前提是必须不直接涉密而牵连国家或社会安全）、保留（部分信息需要隐瞒）、匿名（数据进行标识化）、隔绝（完全不被获取）四个形式，对大数据蕴含的信息而言，部分或局部信息的泄露会触及数据的私密性[1]。

2. 完整性

大数据的完整性是指数据必须是真实有效且全面的，大数据完整性包含内容完整性和数据完整性，比一般的数据完整性要求更为严格。大数据内容完整性主要体现在大数据整体上，除了要确保某个或某些数据的真实有效性，在信息输入和传输的过程中保证数据的一致性外，还需要在整体内涵上更加丰富，整体上反映大数据的整体特征。

3. 追溯性

大数据的追溯性主要指沿着数据供应链和交易链进行数据来源、传递路径、状况等历史信息追踪的能力。在网络安全风险日益增加的背景下，大数据完整的追溯性是保障数据安全和质量的有效机制。

4. 可控性

大数据的可控性是指可以有效机制实现对数据库活动监督管理、授权和废止，限制大数据在可控范围内活动。可控性是对大数据访问控制机制的一种体现，防止大数据平台内的任何资源未经授权使用、泄露、修改、销毁等[2]。

（二）大数据时代的计算机网络安全问题

1. 计算机系统自身漏洞频发

计算机网络处于不断更新换代中，无论是计算机，还是移动PC端都需要借助各种各样的操作系统或者软件提升自身运行能力。但是这些软件和系统不可避免存在某些漏洞。结合人工数据挖掘和漏洞自动检索数据分析，教育机构、政府机构以及事业单位行业是目前存在漏洞最多的行业。这些漏洞可以随着程序系统完善和更新而得到快速修复，但还是存在一些未被修复的漏洞，容易受一些不法分子或者恶意程序入侵，出现客户信息泄露的问题。

2. 计算机系统安全管理解决能力不足

计算机信息系统安全包括实体安全、运行安全、信息安全三个方面。其中实体安全管理主要指计算机的各接口网络设备和外部设备线路的管理；运行安全管理主要指计算机在正常使用下的系统安全管理；信息安全管理指对信息的保护，避免非法系统介入引发信息更改和泄露。目前，计算机信息系统安全管理上的最大问题主要是安全管理措施无

***通讯作者：**刘子祺，1987年2月，男，汉族，山东菏泽人，现任水利部小浪底水利枢纽管理中心副科长，工程师，硕士研究生。研究方向：水利水电工程运行管理。

法跟上硬件更新换代速度，如我国很多高校、政府等机构由于大量使用局域网系统，导致内部、外部机器严重缺乏分离管理，使其遭遇大量病毒入侵，如2017年爆发的勒索病毒就是经验教训[3]。

3. 高新软硬件设备落后

目前我国信息化的发展进程还是相对较慢，对一些核心重要的网络安全技术掌握不足，研发能力也相对薄弱。另外加上政府的限购，导致一些急需设备的高新软硬件无法及时部署到位，整体管理能力不足。

4. 大数据类专业人才缺乏，数据挖掘不及时

结合我国高校专业设置来看，只有100所高校设置了网络安全相关类的专业，这一定程度上导致人才的缺乏。人才的缺乏直接导致大数据技术创新与数据管理能力不足，无法及时分析舆情工作，引发数据泄露等问题[4]。

二、大数据时代网络安全防范技术创新分析

针对大数据时代的发展特征和现存网络安全问题，需要对现有的安全技术进行淘汰、改进或者重新开发。近年来，开发出了针对数据安全问题的技术，如区块链、智能合约等，还有一些基于区块链的审计与溯源技术也不断被创新研发出来。

（一）访问控制技术

访问控制技术作为网络信息系统安全的核心，大数据时代的访问控制技术需要结合用户请求和需求，确保客户能从海量大数据中获取所需信息，并能保证在信息获取过程中请求者的权限与所获取信息私密性程度相匹配。目前传统的自主访问控制已经不能适应当今大数据时代信息需求。而强制访问控制由于具备较高的形式化推理和验证能力还可以作为大数据访问控制创新研究的理论基础，鉴于基于角色访问控制存在无法对大数据时效性等信息进行动态授权的灵活性不足，由此在角色访问控制理论上进行不断创新改进出基于属性的访问控制和基于交易的访问控制，能满足多样化、动态化的访问授权要求[5]。

（二）标识与鉴别技术

标识与鉴别技术属于身份管理技术的核心技术。为了满足大数据时代不同机构之间的数据共享需求，需要进行机构内人员身份标识与鉴别。IT时代的域内认证协议和密码分发中心由于不能支持动态机构的加入与撤销，从而不能适应大数据时代的要求。目前在公钥基础设施和优良保密协议技术之上进行改良的第三方认证、单点登录和统一身份认证技术，由于满足联邦制管理的要求和互认证性而得到不断应用，但这些技术还是不能满足大数据应用中动态属性的实时性、时效性，需要进一步进行改进[6]。

（三）数据加密技术

为了适应大数据时代系统边界模糊或消失的特征，IT时代早期使用的数据加密标准等安全性低，因此被淘汰。基于格的加密和多变量公钥密码技术是为了应对量子计算对传统密码压倒性威胁而发展起来的，是大数据时代必须考虑的技术，对网络安全保障具有重要意义。

（四）数据隐私技术

由于大数据时代的大数据蕴含价值（数据隐私），数据隐私技术成为安全核心任务所在。近年来随着大数据技术研究的深入，一些数据隐私技术也在不断研发，能为大数据处理中的不同目的和安全需求提供现实解决方案。如数据分割策略、隐私数据挖掘、全同态加密和隐私信息检索等技术[7]。

（五）入侵防范技术

在IT时代入侵防范技术主要以“堵漏洞、筑高墙、防外攻”为主。但随着大数据时代云计算和虚拟化技术的出现，推动入侵防范技术需要从全局化和智能化监控出发，不能只停留在边界层面上。全局入侵检测和防范系统是基于大数据挖掘和分析改造基础上完善的，随着该技术逐渐成熟，会成为大数据时代网络安全防御的重要技术。

（六）安全审计与灾备技术

安全审计与灾备技术与上述技术不同，属于安全事后处理技术，确保了业务的连续性，为日后安全防范提供理论技术基础。大数据时代审计和灾备技术主要以确保业务连续性为主。如针对大数据云存储和备份的安全审计上，可通过数据持有性证明技术和数据可恢复性证明技术确保大数据审计过程中信息不被泄露。另外，一些新技术正在对安全审计与灾备产生深刻影响，比如区块链审计技术由于具备不可篡改、共识一致和去中心化等优点，能提供业务全流程

的保障和持续性，能适应大数据时代下构建大范围的业务设计。

三、结束语

目前，网络已进入大数据时代，通过大数据来实现对相关信息的筛选采集和分析，数据处理能力不断提高，且技术覆盖面广。计算机网络作为大数据技术开展的基础保障，只有做好计算机网络安全维护，才能真正体验大数据时代的数据共享、传输带来的便利与经济效益，才能维护好大数据时代的健康发展。本文通过分析大数据时代下计算机网络安全防范技术分析，促使大数据和计算机网络更好为社会服务。

参考文献：

[1]梁丰.基于大数据时代计算机网络安全防范探讨[J].网络安全技术与应用, 2020(6):85-87.
[2]徐大海.大数据时代背景下计算机网络安全防范应用与运行分析[J].计算机产品与流通, 2020(6):33-34.
[3]于丹.大数据时代背景下计算机网络安全防范应用与运行[J].信息与电脑(理论版), 2019,31(22):188-189+192.
[4]吴兴博.大数据时代下企业人力资源管理模式的创新研究[J].中国商论, 2021(8):127-129.
[5]吴凌祺. 基于大数据技术的企业人力资源管理创新路径探析[J].企业改革与管理, 2021(5):127-128.
[6]高玉梅.大数据时代企业人力资源管理的思考[J].人力资源, 2021(2):4-5.
[7]魏晋童.大数据背景下企业人力资源管理模式的创新研究[J].中国商论, 2021(11):151-153.