# 计算机通信网络安全与防护策略的相关思考

吴　美[1]　徐善河[2]
1. 防城港市公安局　广西　防城港　538000
2. 中国移动通信集团广西有限公司防城港分公司　广西　防城港　538000

**摘　要：**伴随着时代的进步，计算机市场在大家国家持续发展的愈来愈健全。恰好是计算机的融进使我们国家社会经济发展获得了更高提高，促使大家国家的每一个领域基本都渗入着计算机的应用，而现阶段面临计算机的快速发展，也存在着了诸多难题，造成计算机在使用之中，存有网络安全里的缺乏，也是我们大家一起存在的困难，为了加强计算机通讯网络安全的稳定性，应对于此事执行合理的举措。

**关键词：**计算机；通信网络；安全防护；防护对策

## 引言

在信息技术发展趋势之中，计算机互联网的发展通常是大家根据计算机来传送信息或贮存关键材料，这为大家在日常生活中带来了很大的便捷，计算机信息互联网的融进，既拯救了在日常生活中工作人员沟通，又为机关事业单位带来了便捷。而此时存有安全问题，通常是一些企业或事业单位，这种所在单位都是会通过互联网来传送一些极为重要的材料，许多材料都是不能泄漏的，而在这个过程中，在计算机快速发展的脚步中，也存有网络黑客在不断前进，这是比较容易对计算机信息互联网产生不良影响的一点[1]。为了加强计算机通信系统的提高，防止在探索中出现的风险性，要加强应用系统的监管，防止存有信息里的伤害。

## 1 计算机通信网络安全的概念和特征阐述

### 1.1 计算机通信网络安全的概念

确保客户本人信息和关键信息不会被泄漏、毁坏及其监听和盗取便是时下很受关心的计算机通讯网络安全，它能确保互联网安全运行且维持信息完好性和安全性，同时还可以保证硬件配置的安全性，确保不容易发生意外情况。

### 1.2 计算机通信网络安全的特征

#### 1.2.1 隐蔽性较强

网络安全的隐蔽性特别强，在开始发生病毒感染之际难以被人检测出，只会在系统漏洞不断发展，危害持续扩大的情形下才能被设备与用户检测出，长此以往，网络安全问题更明显，所引发的关心越来越高。目前，60%的网络安全难题全是爆发后才受到关注的，因此，它隐蔽性和潜伏性也比较强，很容易导致本人信息泄漏，造成重大的网络安全安全事故。

#### 1.2.2 专业性非常强

当出现网络安全问题的时候，外行人员难以对它进行精确分辨并妥善处理，即便在时下，仍然有许多人应对病毒感染、进攻等无计可施，只能靠专业人员。可以这么说，网络安全的专业能力特别强，对人员的技术专业专业素质也非常高。

#### 1.2.3 扩散性和影响力比较大

绝大多数的网络安全难题产生的时候都是毫无预警的，等发现后状况几乎都较为严重了，因此，网络安全难题可在极短时间迅速蔓延从而产生极大知名度和杀伤力，例如木马程序不仅能够根据自我繁殖开展蔓延，在互联网信息互换之时也能开展散播蔓延，让接触到的全部互联网都陷入偏瘫，没法正常运转[2]。

#### 1.2.4 破坏性非常大

从计算机自身安全隐患去分析，电脑病毒根据程序流程拷贝，导致客户电脑卡死、内容丢失，影响到正常运转，其杀伤力较强，危害时长都比较长期。

## 2 计算机通信网络安全与防护的重要意义

由于网络技术的迅猛发展计算机网络信息安全直接影响互联网技术发展网络安全防护成为了计算机通信网络技术性不可或缺的一部分网络信息安全直接影响计算机客户的公民基本权利在大众的生活学习中，公司的管理具体内容也涉及很多确立的工作任务。员工的管理与工作统计分析务必借助计算机服务平台。通讯系统最主要的是利用互联网服务平台存放与分析很多的信息，为顾客处理获取有关信息，并利用其来开辟较好的分享安全通道。计算机互联网的保护技术以及安全生产技术主要指在计算机系统内，信息源必须要在网络空间中快速地解决、传送和存放。计算机通信网络的保护与安全通常是确保计算机通信网络的安全与正常运转。不同类型的系统软件有着不同的系统漏洞，计算机通信网络肯定

会安全性，安全隐患问题[3]。

## 3 我国计算机通信网络安全的现状

### 3.1 自身问题

通讯系统是软件程序员依据现阶段社会发展发展的需求和计算机互联网服务合同的内容是拓展计算机作用而开发的形式。比较严重限定我们的生活与工作。但是由于计算机专业技能比较有限，针对R ampd工作员，控制系统设计上存在很多系统漏洞，为一些不法分子盗取系统中数据和信息带来了便捷，导致了很严重的安全生产事故。比如，Web软件系统受互联网技术应用愈来愈国际化危害，web APP系统的易损性特别大。其设计师和管理人员还在不断完善和优化，但依然没有很切实解决自身的问题，在怎么使用的过程当中，客户资料被不法分子故意盗取，引起了网络信息安全安全事故。

### 3.2 黑客攻击

现阶段，使用计算机互联网时，网络黑客攻击是安全风险之一。尤其是在经济快速发展的当下，行业竞争的压力巨大，不法分子为了能自身利益，盗取其他企业的商业机密，随后卖给其他公司以获得一定的收益。网络黑客使用计算机互联网时之所以能攻击他人，是由于所使用的防护系统存有系统漏洞或不会受到保护。往往出现这样的情况，是由于企业没有清晰清晰地意识到自己在网上网络信息安全保护的功效，简单用保护系统软件保护核心内容，导致了不法分子能够进入的系统漏洞，严重威胁了正常运转，还给个人带来了巨大损失。由此分析出，在使用计算机网络技术时，要注重其安全系统的强化和优化[4]。

### 3.3 技术人员专业能力弱，难以胜任维护工作

现阶段，互联网技术性已经成为院校和高校的关键课程内容，能够为企业及社会发展运输更多计算机类优秀人才。但不一样水准的学生们接纳能力不一样，技术人员的职业素养不一样，在保护网络安全等方面的效果也是不一样。此外，因为一部分技术人员不遵照靠谱步骤，妥善处置，乃至留下一些插口便捷，给网络安全埋下安全隐患，引起了一系列网络安全难题。

除此之外，市场中比较常见的电脑病毒的攻击和适应能力也远远高于过去。但是由于技术人员技术专业能力不够，没法在第一时间合理清除和处理病毒感染，非常容易导致用户信息的泄漏和损失，关键信息被盗取。

### 3.4 未建立完整的网络安全体系

到现在为止，我国的网络安全不够，非传统安全难题层出不穷。最明显的难题之一是绝大多数技术人员的专业素养不太高，企业安全生产技术人员配备不合理，难以实现网络安全管理工作的统一管理。比如，在防火墙运用环节中，一些管理人员专业技能不太高，不能及时开展防火墙日常维护和升级，防火墙已经“严厉打击”新型病毒。此外，防火墙过度简单登陆密码也会增加被破译风险，可能会导致网络安全风险性。遇到这样的情况，各单位早已执行了很多的网络安全预防措施，但是由于公司技术人员中间沟通不立即，欠缺统一的技术性检测标准，造成网络安全预防措施实行落后。此外，因为各种公司对通信系统的安全应急、预测预警、安全防范、财务审计鉴别等重视程度不够，通讯网络安全都还没融进各个阶段，网络安全管理体系不健全，无法充分发挥。

## 4 计算机通信网络安全与防护策略

### 4.1 增强计算机网络安全防护意识

从计算机通信网络管理方法层面来说，计算机通讯网址软件后台管理人员要提高自已的网络通讯安全防范意识，深刻认识到计算机通信网络安全防范措施，搞好安全性安全教育培训，提高计算机通信网络智能管理系统相关人员的安全防范意识和意识，把握最新计算机通信网络安全防范技术以及水平，产品研发运用安全性能更高网站或软件登录系统软件，紧密监管计算机通信网络里的不安全的趋势，保证计算机通信网络的安全性与平稳。与此同时，充分考虑计算机通信网络环境里工作人员要素极为繁杂，计算机通讯设备维护保养及升级一般由互联网工作员进行，要高度重视计算机通信网络人员的内控管理，防止工作员获得客户的信息及个人隐私信息开展非法获利。

从计算机通信网络客户的层面来说，还需要提高计算机通信网络客户的安全防范意识，规定计算机通信网络客户把握比较常见的互联网通信防御措施和流程，掌握简单账号登录、密钥管理方式等相关信息，根据账号登录设置私人的弱密码，有效控制计算机通信网络信息的安全性；根据密钥管理方式防御力违法黑客攻击，使特殊账号登录计算机的相关管理权限[5]。

### 4.2 增强网络安全技术人员的意识

为了能有效控制计算机通信网络的安全性，应该注意提高相关技术人员的安全防范意识。因而，对职工和相关互联网技术人员给出了不同类型的规定：做为企业的日常工作员，在日常工作上务必提高自已的安全防范意识，积极主动接纳企业相关安全防范意识培训学习。唯有如此，才能保障当遇到相关安全隐患时，能够采取有力措施，保证计算机通信网络的安全性。可是，做为技术经理，务必接纳更明确的规定，应对网络安全重大

安全事故时，要具有配制和综合能力。使用通信网络的过程当中，为降低软件管理系统系统漏洞的概率，必须逐渐增加并增加核心数据的安全保密性难度系数。做为一家公司，招人技术人员时，考虑到其是否具备强烈的责任感至关重要。

因为数据库系统智能管理系统和电脑操作系统内容至关重要，所以需要专业技术人员予以处理，进而提升各关键单位间的交流沟通。与此同时，此方法更有助于塑造一批高端互联网技术人员，针对提升计算机通信网络安全防护具备重要意义。除此之外，技术人员还需要注意避免来源于外部网络攻击，提升技术人员学习培训，进一步增强计算机技术以及计算机通信网络安全防护技术性专业性人才的安全防范意识，避免外部网络攻击和影响。使用计算机通信网络的过程当中，不可避免也会受到外界黑客攻击，危害信息的完好性。为了能防止出现这种情况，技术人员应当不断提升自身理论知识水准，建立网络防火墙和定期开展网络安全检验来确保计算机通信网络的安全性。

4.3 建立健全防护体系，开发更安全的防护系统

只靠技术人员来维持网络安全是不够的，一定要融合互联网技术、安全工作才能保障通信网络安全性，才能保证安全防护实效性。公司在招聘管理人员时一定要考评其品德修养，并对它进行定期考核监管，对有着商业秘密信息的技术人员要加强业务培训，并提升其安全防范意识，严苛存放申请注册信息和相关数据信息，未经许可不可从企业电脑里载入相关数据信息。除此之外，提升安全防范，采用数据加密对策，严格把关新客户申请流程，然后进行实时追踪、监管。

此外，在网络设置层面，要高度重视开发作用更加全面的安全防护系统，例如时下大家常见的360电脑防火墙、金山毒霸、360等，这都是可以解决客户计算机安全防范问题可靠系统软件，公司或一个人能下载并安装。在网络安全智能管理系统层面，应采取更高效的对策提高用户实际效果，深入分析信息系统软件，确立其作用，为网络安全安全防护打牢基础。

4.4 及时更新系统

现阶段，计算机实际操作系统的刷新速率相对比较快，在这种情况下，促进病毒、黑客入侵的方法慢慢多元化。过去老旧的系统很容易被攻破，但现阶段所使用的系统在升级换代、立即补丁包里的能力以及对于风险抵御实际效果都远高于过去系统，因而使用通信系统的过程当中，相对应工作人员必须确保系统升级的次数，以此加强网络安全。此外，系统实际操作研发部还需要高度重视内部结构系统漏洞的出现，以后根据效仿黑客入侵的形式，加强其安全防范特性，提高其当面对风险性后的抵挡能力。

4.5 优化计算机杀毒能力

计算机的杀毒能力取决于计算机网络安全的前提。为了避免各种各样病毒和木马软件危害计算机的正常启动，在计算机时要组装具备测毒和杀毒能力的app。例如现阶段的360杀毒系统、诺顿杀毒软件等相关杀毒手机软件都能平稳地扫描器并且对病毒开展防护和删掉。app的杀毒能力主要来源于于对于病毒关键水平编码展开分析的专业技术，一旦发现相似的关键编码，病毒手机软件会立刻把它防护，并立即警示客户计算机得到了伤害，以预警信息——防护——客户确定的次序对病毒进行复查，既做到确保计算机安全的目的同时也减少了客户误删除关键手机软件风险。

结束语：总的来说，计算机通信系统具有一定的开放性与多元性，数据安全问题特别是在显出，变成现阶段不可忽视的关键研究内容。对于计算机通讯网络信息安全，要进一步系统地剖析危害计算机通讯网络信息安全因素，搭建计算机通讯网络安全防护管理体系，不同角度明确提出有效切实可行的计算机通讯网络安全防护对策，合理确保计算机通信系统系统数据库的安全和详细。

**参考文献**

[1]陈超.媒体融合环境下高校防范宗教势力网络渗透的长效机制研究[J].青岛远洋船员职业学院学报,2022,43(1):60-65.

[2]朱睿杰,张玉东,魏雅婷,等.基于区块链的多层卫星互联网络安全管理技术[J].天地一体化信息网络,2022,3(1):79-86.

[3]熊强,杨欣琦,李治文.网络安全漏洞信息披露中多元参与主体行为策略演化博弈分析[J].运筹与管理,2021,30(7):102-109.

[4]罗方禄,王秉,贺林豪.面向网络安全治理的网络信息内容生产者情报赋能模型研究[J].情报杂志,2021,40(3):118-124,97.

[5]张远.信息时代计算机通信技术的应用及安全防护策略[J].信息记录材料,2020,20(8):221-222.