# 政府部门网络安全问题及对策探讨

骆翠萍

中共安徽省直属机关工作委员会党校　安徽合肥　230092

**摘　要：**随着信息技术的发展和互联网络的普及，各政府部门内部已经基本上实现了现代化网络办公，这在提升政府服务质量和效能的同时，也使其面临着较为严峻的网络安全问题。为确保政府信息的完整性、保密性和可用性，必须要加强网络安全管理与控制。本文就主要分析了政府部门网络安全问题的类型及风险来源，并提出有针对性防护建议，以期为政府部门的网络安全维护工作提供一定的参考。

**关键词：**政府部门；网络安全问题；对策研究

# Government Department Network Security Problems and Countermeasures

Cuiping Luo

Party School of the Working Committee of Government Offices Directly under Anhui Province Hefei, Anhui 230092

**Abstract:** With the development of information technology and the popularization of the Internet, the modern network office has been basically realized in all government departments, which not only improves the quality and efficiency of government services, but also makes them face more serious network security problems. In order to ensure the integrity, confidentiality and availability of government information, it is necessary to strengthen network security management and control. This paper mainly analyzes the types and risk sources of network security problems in government departments, and puts forward targeted protection suggestions in order to provide some reference for the network security maintenance work of government departments.

**Keywords:** Government departments; Network security issues; Countermeasure research

## 引言

根据我国互联网应急中心2021年第四季度发布的互联网安全态势报告中指出，2021年国家互联网应急中心通过自主捕获和厂商交换获得移动互联网恶意程序283万余个，同比增长11.7%[1]其中被发现有3517个互联网恶意程序是植入到政府部门的。由此可见，我国政府部门的网络安全形势非常严峻。为此政府部门必须要展开网络安全问题的专项整治行动，以确保内部网络硬件设施、软件系统的全面安全可靠。

## 1　政府部门网络安全问题

### 1.1 外力导致的安全问题

从网络安全风险的来源来看，可以分为由外力导致的安全风险问题和内力所导致的安全风险问题。首先来看外力所导致的安全风险问题主要是设备受损，这里主要指的是硬件设备的损坏。导致设备受损的风险因素包括：自然灾害、电力事故、火灾以及人为因素导致的外力破坏等。一旦政府部门的网络硬件设备遭到破坏发生损毁，不仅会使内部网络瘫痪，还会由于来不及对一些重要资料保存和备份，发生数据丢失。

### 1.2 系统操作导致的安全问题

从内部风险来源来看，系统操作所导致的安全问题是最为突出的。当前政府部门所使用的计算机操作系统 Windows 系统或者是 Unix系统，这些操作系统的开发商受到技术以及动态链等的限制，使系统本身就存在一定的缺陷，包括各种各样的安全漏洞[2]。政府部门的办公人员在使用计算机时，由于缺少相应的安全风险意识和对系统操作的基本认知，往往会忽略系统发出的各种升级和补丁安装要求，并且也存在不规范操作的情况，这些都会增加计算机安全风险，引发病毒入侵、黑客攻击等的网络安全问题。

### 1.3 非正常访问导致安全问题

在政府部门中，有关信息文件的传输有着严格的层级限制和要求，尤其是对于一些保密信息，设定有相应的访问权限。但是在实际工作的过程中，有黑客等不法分子甚至是单位中的个人对相应的系统进行非法访问和攻击，改变原有的程序设置，引发系统混乱，趁机进行机密数据的窃取或者是篡改。这就严重地破坏了政府部门的网络安全管

理秩序。

## 2 针对网络安全问题的对策

### 2.1 物理性防护策略

针对外力所导致的一类网络安全问题，政府部门要制定相应的物理性防护策略，要知道保障政府部门内部网络硬件设备的物理安全是进行网络安全防护的重要前提，因此政府部门进一步细化落实对网络设备的维护与管理工作。首先，为避免计算机硬件设备受到外力冲击发生损毁，对于存储重要资料的硬件设备可以设置专门的防护舱，防护舱具有防火、防盗、防震、防电磁干扰等的性能[3]，这样一旦遭受自然灾害等外力因素影响，可以最大限度地保护计算机系统、Web服务器、通信链路层网络设备等免受破坏。其次，政府部门要加大对计算机网络设备的维护力度，安排专门的工作人员定期对重要的硬件设施如主机、路由器等进行安全性能检查，对于存在安全隐患的硬件设备要及时加以更换。同时要做好清理工作，确保硬件设备的接口传输性能。

### 2.2 访问控制策略

针对非正常访问导致的一类网络安全问题，政府部门要实施相应的访问控制策略，这也是保证政府内部信息资源不被破坏，提升网络安全性能的关键与核心。那么具体要如何进行访问控制呢？主要采取以下几种方式：一是入网访问控制。也就是明确规定政府部门哪些办公人员能够登录服务器，并且控制入网访问的时间和具体的工作站。二是网络权限控制。这主要是针对网络非法操作的一项控制措施，通过网络权限控制，使非法操作人员无法获取网络权限进行联网操作。三是密码控制。对于政府部门关键的软件系统和数据库，要定期更换密码指令，设置密码输入错误上限，一旦达到这个上限系统会自动以图形或文字或声音的形式发出安全警报[4]。四是属性访问控制。对政府部门所使用的文件、目录等指定相应的访问属性和加密格式，一旦脱离专用的网络设备和解码器，确保其无法被打开和使用。

### 2.3 防火墙控制策略

为有效应对病毒、黑客等对政府部门计算机网络的入侵和恶意程序的植入，政府部门还要采取有效的防火墙控制策略。防火墙其实就是位于两个网络之间执行控制策略的一个系统，通过设置专业防火墙，建立起相应的阻隔屏障，对入侵的数据程序进行实时监测，并限制外部非法用户访问内部网络资源。并且计算机使用人员要根据防火墙做好静态的病毒查杀、隔离和过滤。

### 2.4 网络安全管理策略

针对系统操作不规范所导致的一类网络安全问题，政府部门要建立完善的网络安全管理策略。与上述技术措施不同的是，网络安全管理策略侧重于对政府部门办公人员的规范化管理和教育。首先，政府部门要加大网络安全宣传力度，增强工作人员的网络安全风险防范意识。同时通过开设专题讲座以及制定培训课程等的方式，使政府办公人员能够了解一些基本的系统操作常识，按规定统一进行系统升级和补丁安装，最大限度地防范系统安全漏洞。其次政府部门要建立健全内部网络安全管理制度，包括计算机操作使用规程、主机房出入制度、网络系统维护制度以及网络安全应急管理制度等，将相关责任具体到岗位和个人，确保各项制度举措的有效落实。

### 2.5 信息数据安全防范策略

前面提到了一些比较有针对性的网络安全防范与控制策略，这里我们还要特别强调关于政府信息数据的安全防范。随着数字型政府建设的深入推进，政府部门的信息化、数据化程度越来越高，要实现对各类信息数据的安全有效管理，就需要政府部门建立起完善的数据协同与防护机制。首先，政府部门要基于大数据技术的应用来分析网络安全态势，通过数据采集和模型分析做到网络风险的可视化、可测量、自动化，提升政府部门的风险感知预警能力。同时政府部门要建立相应的业务监测预警体系，利用大数据平台对部门业务场景进行智能化分析和学习，建立相应的安全风险识别数据库，从而对政府在资金交易、业务办理等过程中存在网络安全风险进行主动地识别。其次政府部门要加强对敏感数据的安全保护。政府部门要积极推进数据的分级和分类管理，建立起完善的分级分类管理体系，将数字型政府建设过程中产生的各类信息数据进行汇总和分析，根据信息数据的敏感性和涉密程度进行分类，按照不同的标准进行数据库的创建、存储。针对敏感性较高的数据要综合运用多种手段防范数据的泄漏、篡改和非授权访问，同时加强政府网络安全部门对数据外泄溯源追踪能力。最后就是要求政府部门着力打造网络安全的运营协同机制，强化网络安全部门与其他各部门之间的联系，打造系统开发、系统运维的协同工作机制，建立内部的共享情报与处置平台，在网络安全预警、将指标监测、网络安全事件应急处置等方面优化流程，形成部门有机联动与协调，提升网络安全防护质量与水平。

**结语**：

综上，政府部门要加大对网络安全问题的重视程度，分门别类的制定网络安全防控策略，实现技术防范和管理防范举措之间的有机结合，切实打造安全可靠的政府网络办公环境。

**参考文献**：

[1]魏若璇,任瑜珏.政府部门网络安全问题及对策研究[J].信息通信技术,2022,16(06):42-46.

[2]陈彦达,丁韦娜,王伟楠.中国政府部门网络安全保护研究[J].全球科技经济瞭望,2020,35(10):46-55.

[3]罗静怡.政府部门计算机网络安全中数据加密技术的运用研究[J].通讯世界,2018(04):46-47.

[4].政府部门如何做好网络信息安全检查工作[J].中国信息化,2014(Z3):107-112.