监控网络安全信息技术的发展与应用

张海德
国网新源集团有限公司丰满培训中心　吉林吉林　132000

摘　要：互联网世界，网络将全国各地的人和物品联系起来，实现了万物互联，缔造了一个无边界、广阔的虚拟网络世界。以各类电子设备为载体，利用光缆将各类各台电子设备联系在一起，从而实现了信息数据的跨区域、跨时空流通。在互联网技术高速发展的时代背景下，网络的开放性特征进一步显现，同时网络的弊端也越发明显，各种依托于先进网络技术而进行的网络攻击、网络侵略容易带来严重的信息数据泄露问题和巨额的数据资产损失。因此，提高网络安全水平，促进监控网络安全信息技术的创新发展，将其应用于网络信息安全管理具有较强的紧迫性。本文首先介绍了监控网络安全信息系统分析的组成和相关功能，而后指出了监控网络安全信息技术发展的主要趋势，提出监控网络安全技术的具体应用层面和应用路径。

关键词：监控网络；网络信息安全；发展趋势；应用策略

引言：

网络信息安全是互联网时代，信息技术快速发展的背景下所需要考虑的重点内容，网络信息安全技术的发展得到了众多关注，在网络信息安全技术领域，各类先进的防护和预警技术被广泛应用，各种网络信息安全管理方式也正在不断发展。但是即使如此，在网络信息安全监控和防护管理中仍然存在着诸多实践性问题，管理者过度依赖监控网络安全信息技术本身而忽略了外部管理与风险监控导致网络安全技术的使用效果大打折扣，网络信息安全也得不到完美保障。在传统的安防模式下，大多采用专网或局域网的形式构架，因此风险较小，但是近些年网络监控需求的膨胀给网络安全增加了新的风险，需要对监控网络安全问题进行针对性分析，保障监控网络安全，促进网络信息安全防护控制体系的优化升级。

一、网络安全信息系统分析

网络安全信息系统涵盖多功能子系统和硬软件设施，包含了多个方面的因素，是一个以计算机系统为载体，网络传输为渠道以及后端软件为支持和其他应用服务、管理安全等为辅助的安全信息系统：

1.计算机系统

计算机系统运行的稳定性和安全性是监控网络物理安全的决定性因素，是整个监控网络系统得以安全运行的前提。计算机系统属于弱电工程，容易受到雷暴、风雪等恶劣天气的影响，导致计算机系统局部或者是全域瘫痪[1]。因此，在计算机系统设计时，需要提升其防雷防电的物理安全性能，以防范和控制各种物理安全风险。计算机系统中的监控网络安全信息防控管理功能，是依赖硬件设施为主，软件设施为辅的防护系统实现的，主要包括：（1）UPS备份电源，避免因为雷暴天气引发断电或者是短路等电源故障，影响监控网络系统运行和计算机系统的安全；（2）恢复出厂默认，因为人为操作失误导致计算机系统被还原或者是需要还原的情况下，可以选择恢复出厂默认；（3）防电磁干扰，避免对监控网络及相应设备产生干扰，影响计算机接收和处理监控信息；（4）计算机报警系统，预警到物理风险后及时开启报警和安全保护。

2.网络传输

网络系统的运行还需要畅通的网络传输通道支持，而网络传输这一环节也是产生网络信息安全问题的主要环节。在网络信息系统的网络传输环节，计算机和监控设备之间需要搭建起通畅和不间断的通信桥梁和通道，实现远程监控系统和计算机系统的联动与实时通信。而在网络系统与WEB服务器、EMAIL服务器等通信时，较为容易受到网络侵略，影响网络系统的安全。基于此，在网络传输通信渠道设计和外界通信服务器防护上，需要做好安全防护工作，必要时将DNS、WEB等公开服务器和其他网络隔离开来，阻断外部攻击，避免信息外泄。

3.后端软件

后端软件是网络安全信息系统的核心，是网络信息安全防控应用的基础。在网络安全信息系统的后端软件设计时，可以考虑采用LINUX核心平台构架，构建起网

作者简介：张海德，（1993年9月），男，汉，吉林省长春市，大学本科，初级职称，研究方向：信息网络。

络安全信息防控平台和应用服务层，采用分立设计理念来设计服务器功能，使用多级复用冗余技术来支持操作层和应用层，从而实现网络安全信息系统在海量信息数据和超大规模平台基础上的顺利稳定运行[2]。在数据储存方面，选择分布式网络储存方式，比如区块链技术以及iSCSI技术等，通过分布式记账和网络存储来实现数据信息分区存放和储存，保障数据安全、完整，适应爆炸式和超大内存的信息数据储存要求，实现储存模块的无限延展。

二、网络安全信息技术的发展趋势

随着互联网和衍生应用网络规模的扩大，网络安全信息技术使用范围的扩大以及安全网络系统的更新优化，使得网络安全信息技术还在持续不断地创新和发展，并且呈现出显著的特征：

1.操作的简单化

网络安全信息技术目前正在朝着操作简单化的方向发展。目前各种移动终端设备的普及使得传统的以计算机系统为载体的监控网络安全信息系统加入了新的成员，即各类移动智能设备、电子终端设备。这部分设备的操作专业性和技术性没有计算机那么强，因此不能再按照计算机专业化的操作来设计移动终端设备的部分功能操作程序，需要简化操作流程和方式，将计算机语言翻译成更好理解的语言直接呈现，从而使得非专业人士在一定的指导下也可以完成相应操作。繁琐和专业的网络安全信息系统操作简化为终端便捷操作的趋势较为明显，并且已经取得了一定成效，将原本庞大的监控网络系统变小，将网络安全信息技术从复杂变得简单成为当前网络信息安全技术发展所需要考虑的重点问题。

2.网络安全制度越发完善

庞大的网络系统和规模使得网络安全信息技术的单一化使用必然无法发挥出其应有价值和作用，因此进一步深化了对网络信息安全的制度建设和法律体系建设，除了需要运用先进的网络安全信息技术来预防、预警和控制各类网络安全风险，也需要运用严格完善的制度保障来制约各项行为[3]。因此，在网络安全信息技术不断发展的过程中，网络安全制度和行业规范也相应地实现了发展，法律约束越来越严格，制度执行更加透明，网络违法的成本显著提升，对各类网络违法行为产生了有效的抑制作用。

3.预警更加智能化

目前我国网络安全信息技术的重点和关键突破技术领域是提前智能预警领域。在各类网络系统实际运行过程中，往往各类网络安全风险预警都是发生在被攻击或者被入侵的情境下，提前地风险预警实际上不能保证。而随着网络信息安全技术的创新与发展，掌握防控先机逐渐成为可能，能够在监控网络被攻击和入侵前就预测到被攻击的可能性和动向，从而提前做出预警，使得监控网络信息安全风险的预警更加有效。

4.网络信息安全监控的远程化

网络安全信息技术本身就具有远程监控和远程操作特征，通过互联网将各地的设备和物品联系起来，将其统一集中于远程控制中心管理和调控，但是受到区域时空限制，以及为了保障网络信息安全技术的实施效果，信息安全防护和预警的距离相对更近。而随着网络信息安全技术的发展，网络信息安全监控的距离越来越远，真正实现了远程化，即使管理者不在现场或者是控制中心，也能够通过活动相应权限，访问监控网络安全信息管理平台，调试相应的设备，突破时空限制，随时随地保障监控网络的信息安全。

三、网络安全信息技术在监控中的具体应用

网络安全信息技术具有较为广泛的应用场景，能够广泛应用于各种监控安防情境中，网络安全信息技术的各类技术能够在不同的场景中发挥不同的作用。在监控网络系统中应用网络安全信息技术，还需要监控安防系统来配合网络安全信息技术的实施：

1.视频流加密技术

视频流加密技术指的是对视频进行加密处理的特殊技术，在网络监控摄像头或者是监控传感器将拍摄的视频流通过特定传输通道传输到后端系统时，不仅需要对视频流进行编码压缩处理，还应当在此环节嵌入加密技术和加密算法，设置密码和解密方式，比如数字密码、文字密码等，唯有在后端采取特定解密手法对视频流解密才可以获得正常视频信息[4]。视频流加密技术可以应用于安防领域，参考流媒体加密方式，对具有一定保密需求的视频流进行加密处理，根据视频流的保密程度和安全管理系数，考虑常规密码、分组密码、序列密码等，选择单一结构密码或者多层密码。监控网络运行主体应当按照一定规范和视频流数据储存格式加密封装视频流信息，将其上传到平台，配合智能网络监控硬件设备的解码库信息进行解密，显示最终视频图像。

2.防火墙技术

防火墙技术是保障监控网络安全最基础和最有力的技术之一，具有广泛应用场景，可以解决众多监控网络信息安全问题，如表1所示。

表1　防火墙应用场景

CIA条目	威胁种类	组合策略	策略实施设备
机密性	窃听、非法访问、窃取等	用户认证、加密	防火墙、VPN、IDS/IPS等
完整性	篡改、冒充等	数据认证、电子签名、加密	防火墙、VPN、IDS/IPS等
可用性	Dos攻击等	过滤、冗余	防火墙、带宽控制设备

防火墙可以应用于非法窃取、窃听、篡改、冒充视频流信息和Dos攻击的各个场景中。因此，监控网络运营主体应当设置防火墙，通过计算机硬件、软件的组合来形成有效的信息安全防控网关，在监控网络内部和外部之间建立起一个安全的屏障，将内部网络和外部网络隔离开来，从而避免外部网络的网络攻击影响到内部网络。通过设置防火墙和访问权限，制定访问用户和访问条件清单，决定监控网络内的哪些服务可以被哪些访问者访问，并且在内部网络和外部网络监控摄像头通讯的路由器或者服务器上设置包过滤防火墙，有效拒绝无访问许可的用户访问内部网络。

3.VPN网络

根据表1可知，VPN网络同样具有较为广阔的应用场景，也适用于解决和规避各种网络信息安全风险和问题，主要可以将其应用于企业和其他单位的监控网络、公安监控、超市联网监控等场景，在较大规模、较大范围以及和其他网络有交叉的情况下，可以利用VPN网络，将公网中传播的信息数据进行加密处理，但是不是对流通在公用信息网中的视频流信息本身进行加密，而是通过VPN网络中的“隧道技术”构建起一个虚拟局域网，设置“加密隧道”，使得视频流信息得以在加密隧道上流通，加密隧道直接连接监控网络运营主体或者是使用者，实现大区域广泛安全的视频流信息传递，避免视频流信息和其他数据信息传输传递过程中被盗取、篡改。

4.网络访问控制技术

在监控网络安全信息技术的应用过程中，还需要合理地分析监控网络的用户需求和应用场景，特别是在访问量过大的情况下，更是要关注访问者的信息和行为东西，避免有黑客入侵或者是病毒植入。因此，需要合理利用网络访问控制技术，对外来用户访问控制网络设置相应条件的限制，或者说访问其他网站时跳出安全提醒，并且限制访问，从而保障监控网络的安全性。在监控网络用户访问识别时，采取用户名识别、身份识别、密码识别、账号识别、人脸识别等方式来辨别和确认用户，赋予相应用户访问权限，并且做好记录，追踪IP地址，有效避免网络访问用户携带病毒入侵监控网络[5]。

5.数据库备份与恢复

在监控网络进行信息安全管理时，不得不考虑到人工操作失误或者是被黑客入侵而导致各类数据和信息资料丢失的情况，因此需要考虑做好信息数据的备份和恢复工作，并且给每个数据库设置备份数据库，同时实现各类数据信息奠定云端储存，保证监控网络产生的信息数据能够多次备份，长期处于安全的状态，数据丢失和被窃取后也能够通过备份信息和一键恢复功能找回相应的文件与数据。而为了保证监控网络数据库的安全性，应当针对不同影响因素展开不同的监督管理。例如，对数据库运用和管理工作人员实行监督，采取金字塔级权限设置，保证机密越高的文件和数据掌握在更少和更高职称与级别的人手中。

四、结束语

综上所述，近些年不断更新换代的网络攻击和网络侵略方式紧迫地催促着网络信息安全技术的发展，要求网络信息安全技术的安全性能更高、预警监控功能更完善、更加智能化，硬件和软件操作更简单，从而保障个人计算机和组织机构计算机的安全，有效杜绝和防范网络信息数据丢失、被窃取、被篡改等风险，建立起更加完善成熟的网络信息安全监控和管理体系。需要注意的是，在网络信息安全防范管理中，单凭先进的监控网络安全信息技术不能完美实现安全防控目标，而是需要较高的监控网络安全防范意识和配套的安全管理制度与之相配合，才能够保证监控网络安全信息技术的价值与作用得到充分发挥，才能够构建形成一个更加安全、更加开放、更加便于操作和管理的监控网络安全信息管理系统，形成安全性能更高的网络。

参考文献：

[1]邓志东.基于大数据背景的计算机信息安全及防护策略[J].电子技术与软件工程，2020（23）：246-247.

[2]马现.智能化计算机安全监控信息网络技术分析[J].信息记录材料，2021，22（02）：128-129.

[3]石兆军，周晓俊，李可等.基于多源信息融合的网络安全监控技术[J].计算机工程与设计，2020，41（12）：3361-3367.