基于涉密计算机网络安全保密的解决方法略谈

陈希锋
（华南农业大学珠江学院，广东 广州 510920）

摘 要：基于国家安全的考虑，涉密计算机的网络安全至关重要。本文从涉密计算机保密方案的设计和解决方案展开了介绍。并在保密方案的建设上，提出了一定的建议。

关键词：国家安全；计算机网络安全；保密
【DOI】10.12231/j.issn.1000-8772.2020.30.196

1 前言

随着科技进步和互联网的发展，对涉密计算机的网络安全方面也提出了更高的要求。这一切的出发点都是为了国家安全，国家机密安全关乎人民最根本的利益。涉密计算机保密方案设计是计算机安全的基础和前提，方案制定的合理可以有效提高保证涉密计算机的网络安全。那么，该如何设计涉密计算机的保密方案以及需要考虑哪些方面的因素呢？

2 涉密计算机保密方案的设计

一般而言，国家出于对安全的考虑，涉及到国家秘密的信息采集、存储和传输处理到的计算机，这样的计算机统称为涉密计算机。涉密计算机在国家信息安全方面处于非常重要的地位。因此涉密计算机的安全保密极为重要，它关乎国家安全，更关乎人民利益。它主要有三个部分组成，基于终端安全设计、服务器的安全设计和无线移动平台的安全设计。在使用国家涉密计算机时，需要对使用人进行安全的验证，待身份核实后才可以登录计算机进行操作。根据国际惯例和行业操作规范，涉密计算机在保密设计时，需要通常考虑以下几个方面。

第一，服务器的安全。涉密计算机的使用首先需要对相应的操作人员进行身份信息的验证。通信端口与服务器之间的连接和加密是服务器安全的首要前提。同时还要兼顾到管理权的控制，比如利用USB密码令牌来控制计算机的进入[1]。

第二，客户端的安全。涉密计算机在进行文件传输时，要特别注意传输过程中的保护行为，避免发生信息泄漏而影响网络安全。文件的传输保护主要包括注册表，文件传输的过程和接入监控内容。客户端的安全还需要从USB接口、硬盘和I/O端口进行加密操作，从而实现双性的保护进而提高安全保护的程度。

第三，管理安全。生命计算机的管理者主要通过USB令牌来实现信息的认证行为，进而实现对计算机的管理。当外来人员几次未能通过验证时，系统发生预警并提示给相关主管部门，对该设备进行锁定，待故障排除时才能再次登录。

3 涉密计算机网络安全设计方案所遇到的困难

随着科技的进步，在现今“大数据时代”背景下，人们生活发生着翻天铺地的变化，同时，传统的计算机网络安全保密方式已无法满足当代网络安全发展和需求。因此在制定方案时要考虑的因素也较多，比如相关工作人员要求和客户的需求，保密系统设计要进行科学合理制定，对相关工作人员的技术要求较高。涉密系统在进行网络升级时，无论是新建的系统还是原有的系统，都要对其安全部分进行全面的设计，这无形中增加了相关人员的工作复杂度和难度。

4 涉密计算机网络安全保密的解决方案

针对涉密计算机保密方案以及需要考虑的问题，涉密计算机的安全保密的主要防护方法，由以下几个方面构成，这些的方法都是尽最大限度的来保证计算机的网络信息安全。

（1）明确划分涉密系统和非涉密系统。划分涉密系统和非涉密系统，这是涉密计算机开展工作的前提和基础。在设计时要把两者直接设定一个非常明确的界限，这样就便于对他们进行针对性的管理。如果非涉密系统遭遇侵害时，由于界限的存在，可以有效保护涉密区域，不受安全威胁或受到较小的安全威胁。涉密系统在工作中，不可连接到国际互联网中，必须采取与非涉密系统之间物理分层的方式，进行分层管理区分管理[2]。出于安全级别的考虑，对涉密系统要着重管理，而对非涉密系统则采取一些基本的管理就可以。在单位中对涉密系统的管理费要大于非涉密系统的管理费用，因此，保密费用的支出要合理进行划分。在涉密系统保护过程当中，要兼顾保密信息的全面性，避免定密不规范的情形出现，要结合实际情况，选择最优的保密措施，以提高涉密计算机系统安全性。

（2）不断完善物防方面措施。采用物防手段可对计算机网络安全提供巨大的帮助。它的主要手段是采用先进的物理防护的方法，对机房涉密中心及核心设备进行科学的管理。采用这种基础性的涉密管理方式可以大大地降低了管理的成本，提高了资源利用的效率。在进行物防方面管理时，要结合实际情况制定科学有效的物防管理措施和方法，提高物防管理的效率。

（3）加强涉密管理。涉密计算机在管理时，由于面临着不断更新的数据及网络安全方面的攻击，因此技术手段往往存在一定的滞后性，这就导致了系统可能存在一定的安全隐患。为了解决这样的隐患，可以通过采用更加有效的管理方法来解决。一般而言，涉密计算机安全性占比比重中，安全系统的保密管理占70%，技术的占比是30%。因此保密管理的占比更高，也应该得到更多的关注和投入。当保密系统设计完成后，要注意管理方面的工作的重要性，采用管理方法和技术方法相并行的方式，从而提高涉密网络系统的安全性[3]。

（4）加强安全域的划分。安全策略域和保护主客体是涉密系统内部的安全域的组成部分。安全域在划分过程当中要重点关注局域网和逻辑子网等网络结构划分，注意信息密级和重要性的划分，力求安全域划分与实际需求相一致。

关于涉密计算机的网络安全方案有很多，每一种方案都是在不同的角度对涉密计算的网络安全，提出了解决方法。计算机网络安全的保护设计同时也受到了经费的限制等。因此，制定一个科学有效同时又兼顾自身成本的保密方案至关重要。

5 结束语

本文主要根据涉密计算机网络安全的重要性，提出了涉密计算机保密方案的设计以及相关注意事项。随着科技的社会发展以及“大数据时代”的到来，涉密设计方案也面临着一定的难度和困难。本人针对于涉密计算机所遇到的困难，提出了相应的网络计算机安全保密的解决方案，包括划分涉密系统和非涉密系统，完善物防方面，加强生命管理和加强安全区域的划分。涉密计算机网络安全保密工作离不开技术手段和管理手段，只有采取这两种方式结合的形式，才能有效降低被外来入侵的风险。

参考文献

[1]李玲.涉密计算机网络安全保密方案[J].科技与创新，2018(12)：119-120.
[2]张帆.基于涉密计算机网络安全保密的解决方法研究[J].信息系统工程，2017(03)：72.
[3]邓林.涉密计算机网络保密方案设计与实现[J].中国管理信息化，2017，20(01)：176-177.