随着计算机技术的飞速发展，网络规模和设备数量迅速扩大，许多企事业单位的IT系统变得越来越复杂。不同背景的操作人员的行为可能给系统安全带来较大风险，主要表现在以下几个方面。首先就是多个用户使用同一个账户，这种情况主要出现在同一工作组中，由于工作需要，同时系统管理账号唯一，因此只能多用户共享同一账号。如果发生安全事故，不仅难以定位账号的实际使用者和责任人，而且无法对账号的使用范围进行有效控制，存在较大安全风险和隐患。其次就是一个用户使用多个账号。目前，一个操作人员使用多个账号是较为普遍的情况，用户需要记忆多套口令同时在多套主机系统、网络设备之间切换，降低工作效率，增加工作复杂度。缺少统一的权限管理平台，权限管理日趋繁重和无序；而且操作人员的权限大多是粗放管理，无法基于最小权限分配原则的用户权限管理，难以实现更细粒度的命令级权限控制，系统安全性无法充分保证。最重要的就是无法制定统一的访问审计策略，审计粒度粗。各网络设备、主机系统、数据库是分别单独审计记录访问行为，由于没有统一审计策略，并且各系统自身审计日志内容深浅不一，难以及时通过系统自身审计发现违规操作行为和追查取证。为了解决这些问题，远程会话管理系统就随之产生。远程会话管理系统具有单点登录、账号管理、身份认证、访问控制、操作审计等主要功能。其中单点登录和账号管理功能可以对所有设备的账号进行统一管理，让使用者无需记忆众多系统密码，即可实现自动登录目标设备，便捷安全。身份认证提高了账号的安全性；访问控制根据操作人员的类型给予不同的操作权限，防止非法、越权访问事件的发生。操作审计功能可以记录操作人员进行的各种操作，对违规行为进行事件控制。通过远程会话管理系统，提高了系统的可操作性，可以对违规行为进行精确定位从而降低了操作人员的行为给系统带来的风险。