



# 猎隼涉密计算机安全保密检查 软件网络版



中国信息防泄漏领航企业



# 目 录

产品概述 .....	1
产品功能 .....	2
产品优势 .....	3
关于鼎普 .....	4

## 产品概述

涉密计算机信息系统的安全保密检查始终围绕非授权网络连接、越权处理涉密文件、内外网介质交叉使用、运行健康等方面开展，以往的检查手段是以 U 盘或者光盘为载体对单独的涉密计算机逐一开始检测，这种检测手段虽能有效完成深度性的检测，但针对大规模涉密网络安全检查的需要却缺乏时效性，同时给检查人员在操作性上造成极大的不便。

猎隼涉密计算机安全保密检查软件是鼎普科技自主研发力量在国内首款推出的保密检查工具。该系统已实现由单机检查向网络化检查的升级，解决了由于被检计算机的数量庞大、位置分散而导致检查效率下降、检查效果降低的问题。该系统提供的报表分析功能可以对大批量检查数据进行综合统计，满足了大规模涉密计算机安全检查和网络化统计分析平台的需求，提高了保密技检工作的广度和深度。

猎隼涉密计算机安全保密检查软件网络版，采用 C/S、B/S 相结合的模式，由客户端软件、服务器管理端、服务器 Key 三个部分组成，如下图所示。客户端软件与服务器采用 C/S 架构，运行安全，检查彻底；

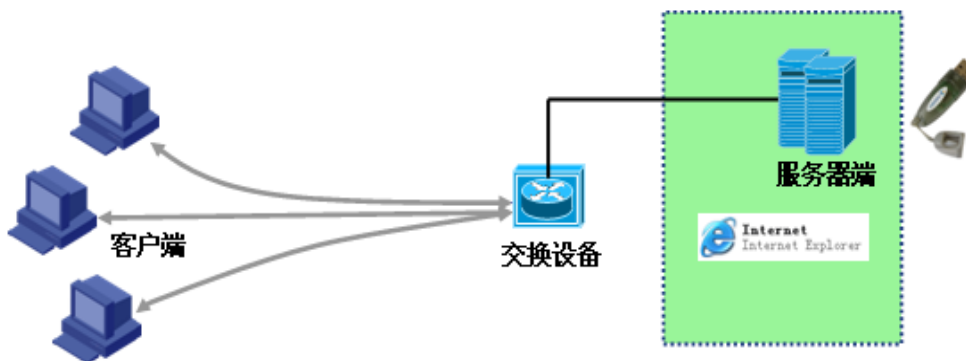


图 1-产品逻辑结构图

本系统适用于保密检查单位对涉密单位进行安全保密检查，也适用军工、政府等敏感单位进行保密自查，通过对该系统部署，能对涉密单位大规模网络进行快速、高效检查，整个检查过程采取静默方式，对于终端用户透明，最大程度上不影响终端用户操作行为习惯。

系统安装：服务器直接安装在专用硬件平台或专用笔记本上。客户端安装有两种方式，一是在终端主机上直接运行安装客户端软件，二是通过浏览

器连接服务器自动运行安装；卸载则通过服务器端完成。

日常保密检查：服务器接入单位网络，管理员与服务器采用 B/S 架构，管理员打开 IE 浏览器输入服务器地址后，在弹出的管理员登陆界面输入正确的用户名和密码，即可登录服务器进行保密检查，系统的管理简便，范围不受限。如下图所示：



图 2-服务器登录界面



图 3-服务器管理界面

## 产品功能

序号	功能分类	功能项
1	终端管理	1、用户基本信息设置； 2、终端检查策略管理

		3、检查任务执行
2	策略管理	1、新建检查策略； 2、设置及查看检查策略 3、删除检查策略； 4、设置检查任务
3	服务器管理	1、系统备份； 2、修改管理员账号密码 3、客户端卸载设置； 4、恢复出厂设置 5、报表阈值设置
4	终端安全 健康检查	1、违规上网信息检查； 2、文件操作痕迹检查 3、涉密信息检查； 4、USB 设备使用痕迹检查 5、共享目录检查； 6、屏幕保护检查 7、多操作系统安装检查； 8、无线互联设备检查 9、终端进程及服务检查； 10、杀毒软件安装检查 11、病毒查杀记录及病毒统计信息检查 12、应用软件安装检查； 13、安全策略设置检查 14、终端网络端口检查； 15、驱动及补丁安装检查 16、网络工具安装； 17、网站账号记录 18、电子邮件安装； 19、终端日志信息检查 20、终端基本信息检查
5	报表管理	1、查看终端检查记录； 2、生成及下载检查报表

## 产品优势

### 1 保密检查网络化

使用本系统，可以更加方便的进行终端安全检查。管理员仅需为终端或分组配置好策略，执行检查功能，所有终端即可自动进行检查。以往的单机版检查工具需要在每一台计算机上逐一进行检查，既费时，又费力。网络版检查工具可对终端进行网络化统一配置、检查，使得检查取证省时省力。

### 2 多模式算法效率高

采用了多模式匹配算法，可同时遍历扫描整个终端磁盘上的多种检测信息，如同一扇区中，既有上网信息，又有文件操作痕迹和 U 盘使用信息等。

则采用一次扫描、并行分析这种方式，可同时检测多个深度被检项目，极大缩短总体检查时间，提高检查效率。

### 3 数据逆向恢复

通过直接分析注册表文件，解决注册表读取无权限问题，即使删除的 U 盘使用记录仍可以恢复取证，揭示出违规行为；涉密文件深度返查技术：基于 Windows 下常用的 FAT、NTFS 文件系统，根据“涉密关键字检查”中检索出的关键字所在扇区号，通过数据逆向恢复技术，即使被删除文件也可以检查到并恢复，使涉密文件违规操作的检查更彻底。

### 4 报表统计归一化

网络版检查工具在检查结果查看方面比单机软件具有独特优势——数据统一存储在服务器的数据库中，检查人员需要查看某个终端或某部门终端的检查结果，只需打开网页，登录服务器，找到相对应的分类检查项数据即可浏览，并且审计报表可以集中分析后再导出，使检查结果统计上报更方便。

### 5 数据加密传输

采用数据加密传输。系统基于 C/S 架构，对网络数据进行了加密，避免了检查结果被窃取或篡改，为用户单位提供产品使用的安全保障。

### 6 终端静默运行

终端用户无法使用任务管理器、360 进程管理等违规技术手段结束正在运行的客户端程序，为检查工作的顺利开展提供了可靠的保护机制。

## 关于鼎普

北京鼎普科技股份有限公司坐落于中关村软件园，是中国信息防泄漏的领航企业。鼎普科技创建于 2003 年，经过 8 年的快速成长，已成为国内信息防泄漏产品与解决方案的专业提供商，公司拥有 200 多人的专业团队，在全国各地拥有 5 家分公司和 7 个办事处，同时在北京、上海、成都、郑州、石家庄设立了五大客服中心，为众多的军队、军工企业、政府、高校、科研院所、金融系统和大型央企等客户提供及时、便利、真诚的服务。

鼎普科技拥有国际性标准水平的安全产品研发中心，中心设有信息安全攻防实验室、信息安全检查与评估实验室及新品研发等机构。在安全产品研发中心从事计算机、网络、电子信息应用等领域的顶级科技人才，通过长期

对客户需求的理解与信息技术的研究，使鼎普科技的技术成为国内内网安全产品的标杆典范。专业从事信息安全的咨询顾问以其精湛的技术，帮助客户解决实际面临的安全问题，为客户呈现具有鼎普产品个性化、高效率的解决方案。

卓越的管理团队使鼎普科技通过了 ISO9001 质量体系认证、CMMI 三级认证、军工保密二级资格认证，获得了涉密信息系统集成资质、计算机信息系统集成资质，成为商业密码定点生产单位。取得了权威机构的各类资质认证 70 余项、专利 26 项。

作为“中国计算机学会计算机安全专业委员会”、“中国计算机学会信息保密专业委员会”和“全国信息安全标准化技术委员会”的成员企业，鼎普科技荣获了最具成长科技型 100 强企业、北京市专利试点企业、国家互联网应急服务支撑单位等多项国家级荣誉称号。为国防、国家奥运、神舟飞船等大型信息安全项目提供高品质的产品及服务，更获得了高度评价及认可。

鼎普科技旗下拥有信息防泄漏领域的领军品牌“鼎普”，同时拥有信息安全检查类第一品牌“猎隼”，秉承“更底层、更安全”的技术创新理念，与客户共同分享信息安全时代的无限精彩！