

猎鹰计算机保密检查系统介绍 V1. 12

(文档编号：110805)



文档名称	猎鹰计算机保密检查系统		版本号：V1.12
拟 制	智华产品部	审 核：李中华	批准：
发送组织		有效期：V1.13 版本发布前有效	
日期	2011 年 8 月 5 日	制作部门	产品部
修改类型	MODIFIED	修改部门	市场部

*修改类型分为 A - ADDED M - MODIFIED D - DELETE

猎鹰计算机保密检查系统介绍 V1.11

1. 引言

保密检查是保密工作管理的重要内容，是加强保密工作的重要措施。依法对各机关单位的计算机及网络进行保密检查，及各单位保密部门对本单位进行保密自查是各级保密部门和人员的职责。

为了配合2010年“新修订《保密法》”关于计算机保密安全管理规定的落实，以及目前全国保密大检查工作的进行，北京智华天成科技有限公司联合国家保密系统专家、中央部委保密主管领导、核工业集团计算机应用研究所，联合研发了一款集多项保密检查功能为一体的专业计算机保密检查工具---猎鹰计算机保密检查系统。

猎鹰计算机保密检查系统作为一款专业的计算机保密检查工具，主要用于保密局对各单位计算机及网络进行安全保密检查，以及各党政机关单位对本单位计算机及网络进行日常的安全保密自查，从而及时发现违规行为、失泄密漏洞和安全隐患，加强防护措施，做到及时有效的防止失泄密事件的发生。

2. 产品概述

猎鹰计算机保密检查系统，依据国家保密局BMB17《涉及国家秘密的信息系统分级保护技术要求》、BMB20《涉及国家秘密的信息系统分级保护测评指南》的相关标准和要求设计，在中央部委保密管理部门和各省、市、县区保密局保密的保密检查、自查中，发挥了重要作用，取得了一致的好评。

猎鹰计算机保密检查系统，实现了按保密管理部门要求检查的项目进行检查的功能并且能对已删除的上网记录、U盘使用痕迹、文件操作痕迹、文件及内容等项目，进行深度恢复和取证检查；对涉密文件和信息、内部工作文件和信息进行关键字配置的自定义轻度检查和深度恢复取证检查；在系统检查完毕后，自动生成计算机保密检查总体报告、详细报告。

检查系统共包括规检查、系统安全检查、辅助检查、深度检查、检查报告五大模块、二十七类，五十多项检查功能。

3. 技术特点

猎鹰计算机保密检查系统具有分类明晰、流程顺畅、操作简单、结果准确的特点，从功能和性能等方面来看，主要有以下几方面优势：

- 一、 **响应时间无滞后：**用户操作按钮时，各检查项响应时间快，最长响应时间在 300 毫秒之内，且数据转换和传送采用实时传送，无滞后。
- 二、 **深度检查速度快：**深度检查的扇区扫描方式，通过算法优化将扫描分析时间缩短在合理范围内，检查速度在同类型的软件中有绝对优势。
- 三、 **扇区扫描技术：**采用自主研发的扇区扫描技术可以将已删除的文件准确、快捷的恢复出来。系统不仅可以检查本地硬盘，并且对移动存储设备也可以检查。方便、准确、全面地检查取证计算机使用信息。
- 四、 **文件编码解析技术：**采用自主研发的“文件编码解析”技术，能够对包括 ANSI/ASCII、Unicode、UTF-8 等类型在内的多种类型的文件内容进行解码及恢复，方便检查人员及时准确的发现违规行为及安全隐患。
- 五、 **良好的安全性设计：**为避免在检查结果上造成误会，以及保证计算机内容的信息安全，防止泄密，本系统在检查过程中避免了写盘动作、以及不向任何介质写入数据的行为。
- 六、 **系统采用结构化设计：**系统采用结构化设计，运用数组结构，多线程控制技术，为了方便使用，系统将常规检查项目进行了整合，可以实现“一键检查”功能。
- 七、 **良好稳定的兼容性：**全面支持 Vista、Win7、winxp 等操作系统。操作简单快捷，数据取证有效，界面简洁美观，取证结果清晰。
- 八、 **操作使用方便简单：**系统不需安装，直接运行，避免了各种木马和病毒的传播和破坏，确保了系统的安全性。

4. 产品功能和性能指标

猎鹰计算机保密检查系统包括常规检查、系统安全检查、辅助检查、深度检查、检查报告五大模块、二十七类，五十多项检查功能。

常规检查：上网记录、USB 其他设备、文件操作痕迹、软件安装检查、杀毒软件检查、反取证工具检查、多操作系统检查、系统进程检查、系统服务检查、系统端口检查、网络设备检查、涉密设备、无线键鼠、涉密信息。

系统安全检查：用户身份鉴别、屏幕保护检查、安全策略检查、账户策略检查、审核策略检查、安全选项检查、共享目录检查、应用日志检查、系统日志检查、安全日志检查、系统补丁检查、当前联网检查、拨号连接检查。

辅助检查：主机信息检查、处理器和 BIOS、视频音频系统、存储系统信息、红外设备检查、蓝牙设备检查、PCMCIA 设备、1394 设备检查、MODEM 设备检查、IE 账号检查、本地站点检查、可信站点检查、受限站点检查、互联站点检查、驱动信息、开关机记录。

深度检查：上网痕迹深度检查、文件操作痕迹深度检查、USB 设备检查深度检查、涉密信息深度检查。

检查报告：总体报告、详细报告、自定义报告。

在网络安全的世界里，如果不想亡羊补牢，就要做到料敌之先！

北京智华天成科技有限公司

北京市海淀区紫竹院路 1 号人济山庄 C 栋 1905

电话：+86-10-51651800

网站：<http://www.waction.cn>