

智华互联网站涉密信息检查监控系统介绍 V1.11

1. 引言

加强政务公开保密审查工作，是维护国家安全和利益的必然要求，也是政务信息公开健康发展的重要保障。近年来，由于门户网站泄密事件逐年呈上升趋势，保密管理部门对政府门户网站涉密信息和文件的审查和监管，已成为日常保密检查的重点工作之一。

采用传统手工检查的方式，由于工作量大、效率低下，已不能满足对大量政府门户网站涉密信息检查监管的要求。另一方面，传统的技术方式，也不能做到对互联网站信息搜索的深度挖掘，无法达到管理部门对涉密信息检查的“查全率”和“查准率”的要求。因此，管理部门迫切需要一套能够进行自动检查、自动监控政府门户网站涉密信息的软件系统，解决现有人工检查方式，工作量大、造成信息漏检、结果滞后的问题。

为此，北京智华天成科技有限公司联合核工业集团计算机应用研究所、中科院信息安全国家重点实验室博士、国家保密局系统专家，在对政府互联网门户网站检查需求充分调研的基础上，定制研发了“**智华互联网站涉密信息检查监控系统**”，协助管理部门主动检查、自动监控政府门户网站信息，发现网站上传涉密信息和文件时，主动向管理部门报警。

2. 产品概述

智华互联网站涉密信息检查监控系统，作为协助管理部门对政府门户网站涉密信息和涉密文件主动检查、自动监控的检查工具，有效的解决了传统人工方式检查时，工作量大，无法及时、全面、准确的检查、监控政府门户网站涉密信息和文件的难题，完全实现了对政府门户网站内容的主动检查和自动监控，发现疑似信息立即报警功能。

智华互联网站涉密信息检查监控系统自主研发的“智华搜索引擎”内核技术，具有深度搜索、断点续检、内嵌涉密文件检查内核、结果准确的特点。该技术从本质上解决了目前的互联网站检查软件无法做到对网站检查的实时性与同步性，以及传统搜索引擎本身的横向爬虫技术弊端，不能做到对互联网站信息搜索的深度挖掘，信息检索效率低下问题。

3. 产品特点

1. 24小时无人值守、主动检查、自动监控

该系统可以对指定的网站是否存在涉密信息进行自动检查监控，也可以通过人工模式检查指定网站，提高了整体系统的性能。同时，该系统基于无人值守、主动检查、自动监控设计原则，提高了检查速度和检查结果的有效性，提高了整体系统的性能。

2. 发现涉密文件直接向管理部门自动报警

该系统发现涉密信息或文件时，会自动向管理员报警，无需人工干涉。

3. 网站内容实时监控、网站检查断点续检

该系统对被监控的网站按照预先设定的规则和策略进行24小时实时监控，一旦发现网页中存在涉密信息，系统会即时、准确的定位抽取，并呈现在管理界面。同时，系统独有的断点续检功能，真正做到一旦发现被监控网站有新上传的网页，进行自动检查，对检查过的网页不再重复检查，大大提高了工作效率。

4. 涉密文件预警

该系统针对政府网站上传的“涉密文件”通过嵌入内核算法，能够快速而准确的定位、抽取，是智华搜索引擎的独有的创新技术。

5. 贴近用户、超强应用

系统采用C/S架构，依托先进的技术，稳定可靠，24小时无人值守，主动检查、自动监控、自动报警功能，极大方便了保密人员的工作。

4. 技术特点

- **“智华搜索引擎”内核：**智华互联网站涉密信息检查监控系统，采用自主研发的“智华搜索引擎”内核技术，改善了目前市面上大多数公司开发的门户网站检查软件，调用了百度、Google等第三方搜索引擎库来对门户网站进行检查，没有独立的搜索引擎的缺陷，避免了不能对门户网站信息检查的深度挖掘的弊端，真正实现了管理部门对门户网站涉密信息和文件检查“查全率”和“查准率”的要求。

- **“深度爬虫”技术：**智华天成自主研发的“智华搜索引擎”内核技术，继承和吸取了传统搜索引擎技术的优势，采用独有的“深度爬虫技术”，主动对网站内容进行深度检查。弥补了百度、谷歌等传统型搜索引擎，只对符合自己算法规则的网页内容进行

行检查，对不符合其规则的网页不去检查，造成对涉密文件资料、涉密信息漏检、漏报等缺陷。

● **“断点续检”功能：**智华互联网站涉密信息检查监控系统独有的“断点续检”功能，对已经检查判断过的网页不再进行重复检查，只检查最新上传、更新的网页内容。解决了重复检查带来的效率低、工作量大的问题，大大提高了工作效率。

● **“涉密文件”内核检查：**智华互联网站涉密信息检查监控系统对政府网站上传的“涉密文件”通过内核算法，能够快速而准确的定位、抽取，无需人工判断，是智华互联网站涉密信息检查监控系统独有的创新技术。

产品功能和性能指标

智华互联网站涉密信息检查监控系统功能、性能一览表			
项目	分项	功能描述/性能指标	说明
适用领域	保密局、安全局、公安局检查部门，中央部委、部队、军工、大型企业。		
主要用途	协助管理部门检查、监控门户网站上传的涉密信息、涉密文件。		
体系结构	网络版系统	C/S 架构，支持多区域、多用户授权管理。适用于国家级、省级、市级管理部门和单位，门户网站数量比较多的单位。	
	单机版系统	C/S 架构，只支持单用户。适用于区县管理部门、行业系统、单位，门户网站数量比较少的单位。	
自动监控	涉密信息监控	自动检查、监控网站上传的信息，发现涉密信息自动报警。	
	涉密文件监控	自动检查、监控网站上传的文件，发现涉密文件准确定位抽取。	
手动检查	涉密信息检查	检查人员可以采用人工方式检查涉密信息。	
	涉密文件检查	检查人员可以采用人工方式检查涉密文件。	
涉密内容报警	报警内容	显示详细的报警信息网站内容及网站地址等信息。	
	报警摘要	包含有涉密信息文件的主要内容摘要。	
	网址链接定位	实现对涉密信息所在的网址的链接定位。	
疑似信息处理	涉密信息处理	管理人员对系统抽取的涉密信息进行人工分类。	
	涉密文件处理	系统内核算法自动将符合条件的文件设定为涉密文件。	
	待判断信息处理	对于一些暂时无法判断其属性的信息，提供待判断功能。	

涉密信息取证	涉密信息取证	系统自动进行网络拍照功能，提取证据。	
	涉密文件取证	系统自动将涉密文件进行保存，并提供导出功能。	
站点管理	站点管理	对被检查监控的网站进行增加、删除、修改、查询等操作。	
	站点监控	对网站索引建立进度进行监控。	
	断点续检	可以根据需要对指定的门户网站进行断点续检。	
	区域管理	根据需要设置不同的区域管理人员的权限，管理本区域内信息。	适用于网络版
关键词管理	公共关键词管理	用于全局检查的关键词	
	区域关键词管理	设定用于某一区域内的关键词。	
	专属关键词管理	设定用于某一网站的关键词。	
	关键词关系管理	设定多个关键词之间的关系“和”与“或”。	
信息查询	信息查询功能	可按时间、内容、站点等查询。	
报表统计	总体统计	统计系统监控的所有网站信息、检查数量、报警数量等。	
	分站点统计	统计特定网站的监控信息。	
	监控内容统计	统计监控到的门户网站点的数量、网页数量等内容。	
	自定义统计	根据实际需要，人工设定要查询的内容进行自定义统计。	
	报表导出打印	将统计出的报表进行打印输出。	
用户管理功能	用户权限管理	支持多用户权限分级管理。	适用于网络版
	用户密码管理	管理授权用户的 密码。	
	用户授权管理	可为二级管理员分配操作权限。	
	用户有效期管理	可为二级管理员分配操作的有效期限。	

成功案例

● 智华搜索引擎技术应用在“中国科学技术信息研究所的“词表系统集成与服务平台”,该平台是基于搜索引擎技术的全球检索系统,“智华搜索引擎”内核已经在搜索引擎技术方面取得了优越性的性能体现。

● 智华互联网站涉密信息检查监控系统在中央部委、全国保密局、军工系统等200多个单位部署使用,产品和技术性能均取得了优越的体现,获得了用户好评和保密部门的嘉奖。

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，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，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，多线程控制技术同事，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：**猎鹰计算机保密检查系统，可以很好的支持 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>