(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102609637 A
(43)申请公布日 2012.07.25

(21)申请号 201110428820.7

(22)申请日 2011.12.20

(71)申请人 北京友维科软件科技有限公司
地址 100102 北京市朝阳区望京园 601 号悠乐汇 E 座 1102 室

(72)发明人 林艳

(51)Int.Cl.
G06F 21/00(2006.01)
G06F 11/30(2006.01)

权利要求书 2 页 说明书 6 页

(54)发明名称

数据泄露审计防护系统

(57)摘要

本发明公开了一种数据泄露审计防护系统，以内部网络的形式在用户终端与服务器上分别安装客户端系统和管理端系统，利用客户端系统随时监控各用户终端程序和文件使用情况，生成目标文件或程序的操作运行记录和截屏记录，并汇总在服务器的操作运行历史记录数据库和截屏历史记录数据库中，从而在管理端系统中最终形成目标操作过程的文字和视频跟踪记录，灵活再现了数据泄露的全部过程，使文件泄露和责任追踪有据可查，防泄密效果明显，防护过程安全、可靠，特别适于在企业、事业、机关等单位内部安装使用。

CN 102609637 A

1. 一种数据泄露审计防护系统，其特征在于，包括基于内部网络的客户端系统和管理端系统，客户端系统以加密方式安装在用户终端上，管理端系统安装在管理服务器上；

a、管理端系统首先建立用户终端 ID，为每个用户终端 ID 制定保安政策级别并发送到对应用户终端的客户端系统中；

b、客户端系统依据保安政策级别对用户终端进行监控，随时触发客户端系统中的相关手段，针对相应文件制作文件操作运行记录、程序操作运行记录及运行过程的截屏记录，并实时传送到管理端系统中；

所述监控的内容包括经应用程序发生的文件生成、读取、保存、更名、复制、移动、删除中的一种或几种组合，特定文件的制作、打印、编码、图像处理中的一种或几种组合，以及通过编码程序、网盘、移动存储器、网络浏览器、MSN、邮箱程序、网络通讯程序发生的文件传送的一种或几种组合；

c、管理端系统接收文件操作运行记录、程序操作运行记录及截屏记录，建立操作运行历史记录数据库和截屏历史记录数据库，并随时对各客户端系统运行情况进行监控和管理；

d、管理端系统利用操作运行历史记录数据库搜索并创建目标文件操作运行跟踪记录，和 / 或根据截屏历史记录数据库搜索并建立截屏跟踪图像，通过视频编辑后生成视频，完成用户终端目标运行过程的文字和 / 或视频追踪。

2. 根据权利要求 1 所述的数据泄露审计防护系统，其特征在于，所述相关手段包括文件代理手段、应用程序代理手段、网络代理手段、打印代理手段、屏幕拦截代理手段和通讯代理手段；

所述文件代理手段依据应用程序发生的文件生成、读取、保存、更名、复制、移动、删除中的一种或几种组合，制作包括用户终端 ID、操作发生起点、文件名、文件的源路径及目标路径、目标文件名、操作方式、引发文件操作的程序名、程序路径、文件备份在内的文件操作运行记录，并保存到指定目录中；

所述应用程序代理手段依据特定文件制作、编码、图像处理中的一种或几种组合，以及通过编码程序、网盘、移动存储器、网络浏览器、MSN、邮箱程序发生的文件传送的一种或几种组合，通过文件代理手段读取文件名称、源路径和保存路径，制作包括用户终端 ID、操作发生起点、文件名、文件的源路径及目标路径、目标文件名、引发事件程序名及路径，以及文件数据备份在内的应用程序操作运行记录，并保存在指定目录里；

所述网络代理手段依据用户终端向网络传送的网络通讯程序文件信息，包括 terminal 服务、telnet 服务或 FTP 服务，制作包括用户终端 ID、操作发生起点、文件名、文件的源路径、文件目标路径、目标文件名、引发的流程及其路径，以及文件数据备份在内的通讯程序操作运行记录，并保存到指定目录中；

所述打印代理手段通过文件代理手段读取文件名称、源路径和保存路径，制作包括用户终端 ID、操作发生起点、文件名、文件的源路径及目标路径、目标文件名、引发事件程序名及路径，以及文件数据备份在内的打印程序操作运行记录，并保存在指定目录里；

所述屏幕拦截代理手段依据文件代理手段、应用程序代理手段、打印代理手段或网络代理手段的触发，以及保安政策级别设定的周期进行用户终端屏幕拦截，生成截屏图像文件，制作包括用户终端 ID、操作发生起点、文件名、文件的源路径及目标路径、目标文件名、

操作方式、引发文件操作的程序名、程序路径、截屏信息在内的相应运行过程的截屏记录，并保存在指定目录中；

所述通讯代理手段随时将保存在指定目录中的运行记录及截屏记录传送到管理端系统中。

3. 根据权利要求 1 所述的数据泄露审计防护系统，其特征在于，所述步骤 c 中，对客户端系统的监控和管理包括监控客户端系统的完整性和运行状况，当完整性和运行处于否定状态时，通过与管理端系统的信息和数据传送，随时保持客户端系统完整和处于运行状态。

4. 根据权利要求 1 所述的数据泄露审计防护系统，其特征在于，还包括；

e、管理端系统通过数据库整理手段删除与文件泄露有直接和间接关联的时间段之外收集的所有操作运行记录和截屏记录。

数据泄露审计防护系统

技术领域

[0001] 本发明涉及一种基于内部网络的数据安全防护系统，特别涉及一种以数据追踪防护和电脑截屏为主要手段的数据泄露审计防护系统，属于网络安全控制领域。

背景技术

[0002] 随着网络的普及，网络安全成为企业、机关、事业单位关注的重点。近年来，也多有发生含保密要求的文件信息，被怀有恶意的内部相关人员向外界泄露，如：信用卡公司员工泄露客户信息；企业核心技术被复制或外泄；广告代理公司泄露艺人隐私；银行职员泄露客户账户信息等等，数据泄露随时发生在我们每个人的身边，并直接或间接影响到我们的生活，甚至给企业的生存和发展带来了严重危害。

[0003] 但现实中，随着通讯技术的高速发展，利用软盘、CD 光盘、messenger、邮箱程序、移动存储器等就可轻松收发邮件、下载或存储文件，操作过程简单、快捷，隐蔽性较高。但因工作需要，全面禁止此类应用程序的使用也不太现实，这就给管理工作带来了极大地麻烦。而重要文件一旦非法外泄，经过互联网的传播，传播速度将非常快，即使抓住和查处了泄露者，也几乎不可能全部收回或删除泄露的文件。于是，文件非法泄露的后遗症将会持续相当长时间，泄露文件的影响力也将不断发酵、扩大，危害程度不可估量。

[0004] 为了保证公司、企业、机关内部信息的安全，除了平时注重培养员工安全意识，养成良好安全习惯，自觉遵守安全规定外，建立一个基于内部网络环境的数据防护系统，对网络环境进行实时监控就变得必不可少。

发明内容

[0005] 鉴于上述现有情况，本发明旨在提供一种以保密数据追踪防护和电脑截屏为手段的、可随时跟踪记录泄密发生过程的数据泄露审计防护系统，以提高保密数据的防护能力和防护威慑力，保证企业、事业、机关单位数据资料的安全性。

[0006] 本发明是通过以下技术方案来实现的：

[0007] 一种数据泄露审计防护系统，包括基于内部网络的客户端系统和管理端系统，客户端系统以加密方式安装在用户终端上，管理端系统安装在管理服务器上．具体步骤包括：

[0008] a、管理端系统首先建立用户终端 ID，为每个用户终端 ID 制定保安政策级别并发送到对应用户终端的客户端系统中。

[0009] b、客户端系统依据保安政策级别对用户终端进行监控，随时触发客户端系统中的相关手段，针对相应文件制作文件操作运行记录、程序操作运行记录及运行过程的截屏记录，并实时传送到管理端系统中。

[0010] 所述监控的内容包括经应用程序发生的文件生成、读取、保存、更名、复制、移动、删除中的一种或几种组合，特定文件的制作、打印、编码、图像处理中的一种或几种组合，以及通过编码程序、网盘、移动存储器、网络浏览器、MSN、邮箱程序、网络通讯程序发生的文件

传送的一种或几种组合；

[0011] c、管理端系统接收文件操作运行记录、程序操作运行记录及截屏记录，建立操作运行历史记录数据库和截屏历史记录数据库，并随时对各客户端系统运行情况进行监控和管理。

[0012] 对客户端系统的监控和管理包括监控客户端系统的完整性和运行状况，当完整性和运行处于否定状态时，通过与管理端系统的信息和数据传送，随时保持客户端系统完整和处于运行状态。

[0013] d、管理端系统利用操作运行历史记录数据库搜索并创建目标文件操作运行跟踪记录，和 / 或根据截屏历史记录数据库搜索并建立截屏跟踪图像，通过视频编辑后生成视频，完成用户终端目标运行过程的文字和 / 或视频追踪。

[0014] e、管理端系统通过数据库整理手段删除与文件泄露有直接和间接关联的时间段之外收集的所有操作运行记录和截屏记录。

[0015] 所述相关手段包括文件代理手段、应用程序代理手段、网络代理手段、打印代理手段、屏幕拦截代理手段和通讯代理手段。

[0016] 所述文件代理手段依据应用程序发生的文件生成、读取、保存、更名、复制、移动、删除中的一种或几种组合，制作包括用户终端 ID、操作发生起点、文件名、文件的源路径及目标路径、目标文件名、操作方式、引发文件操作的程序名、程序路径、文件备份在内的文件操作运行记录，并保存到指定目录中。

[0017] 所述应用程序代理手段依据特定文件制作、编码、图像处理中的一种或几种组合，以及通过编码程序、网盘、移动存储器、网络浏览器、MSN、邮箱程序发生的文件传送的一种或几种组合，通过文件代理手段读取文件名称、源路径和保存路径，制作包括用户终端 ID、操作发生起点、文件名、文件的源路径及目标路径、目标文件名、引发事件程序名及路径，以及文件数据备份在内的应用程序操作运行记录，并保存在指定目录里。

[0018] 所述网络代理手段依据用户终端向网络传送的网络通讯程序文件信息，包括 terminal 服务、telnet 服务或 FTP 服务，制作包括用户终端 ID、操作发生起点、文件名、文件的源路径、文件目标路径、目标文件名、引发的流程及其路径，以及文件数据备份在内的通讯程序操作运行记录，并保存到指定目录中；

[0019] 所述打印代理手段通过文件代理手段读取文件名称、源路径和保存路径，制作包括用户终端 ID、操作发生起点、文件名、文件的源路径及目标路径、目标文件名、引发事件程序名及路径，以及文件数据备份在内的打印程序操作运行记录，并保存在指定目录里；

[0020] 所述屏幕拦截代理手段依据文件代理手段、应用程序代理手段、打印代理手段或网络代理手段的触发，以及保安政策级别设定的周期进行用户终端屏幕拦截，生成截屏图像文件，制作包括用户终端 ID、操作发生起点、文件名、文件的源路径及目标路径、目标文件名、操作方式、引发文件操作的程序名、程序路径、截屏信息在内的相应运行过程的截屏记录，并保存在指定目录中；

[0021] 所述通讯代理手段随时将保存在指定目录中的运行记录及截屏记录传送到管理端系统中。

[0022] 本发明所述的一种数据泄露审计防护系统，通过内部网络连接的方式，在用户终端与服务器上分别安装客户端系统和管理端系统，利用客户端系统随时监控各用户终端程

序和文件使用情况，生成目标文件或程序的操作运行记录和截屏记录，并汇总在服务器的操作运行历史记录数据库和截屏历史记录数据库中，从而在管理端系统中最终形成目标操作过程的文字和视频跟踪记录，灵活再现了数据泄露的全部过程，使文件泄露和责任追踪有据可查，防泄密效果明显，同时，由于数据库在建立过程中，还对原文件内容进行了备份，避免了文件丢失或人为恶意删除带来的危害，提高了防护系统使用的可靠性和安全性。安装数据泄露审计防护系统后，可有效提高和树立操作人员的安全意识，培养防泄密习惯，保障信息安全，特别适于在企业、事业、机关等单位内部安装使用。

具体实施方式

[0023] 本发明的中心是：通过在用户终端与服务器间建立数据泄露审计防护系统，利用系统随时监控各用户终端的程序和文件使用情况，以建立操作运行历史记录数据库和截屏历史记录数据库为手段，对操作过程进行文字和视频的跟踪记录，灵活再现数据泄露过程，从而树立操作人员的安全意识，避免泄露情况发生。

[0024] 本发明所述的一种数据泄露审计防护系统，包括基于内部网络的客户端系统和管理端系统。内部网络是与类似互联网等外界局域网分离的处于内部环境中的网络。内部网络由路由器和防火墙与外界网络分离，形成一个相对独立的内部网络环境。客户端系统以加密方式安装在用户终端上，加密过程既可以是软件加密，也可以是加密狗等硬件加密，以保证客户端系统使用过程的安全性和独立性。管理端系统安装在管理服务器上，通过服务器管理分布在不同用户终端上的客户端系统，实现统一、协调、有效、实时管理。

[0025] 具体防护过程为：

[0026] 步骤一、管理端系统首先建立用户终端 ID，为每个用户终端 ID 制定保安政策级别并通过内部网络发送到对应用户终端的客户端系统中。

[0027] 用户终端 ID 作为唯一的身份识别代码，具有唯一性，是网络管理的基础。保安政策级别是基于用户终端设置的安全策略，组成了用户终端的监控对象、监控时间和监控范围，安装完客户端系统的用户终端首先接收来自管理端系统的保安政策级别，进行加密处理后，使其构成监控过程的标准和准则，全程指导监控过程顺利、有序进行。

[0028] 步骤二、客户端系统依据保安政策级别对用户终端进行监控，随时触发客户端系统中的相关手段，针对相应文件制作文件操作运行记录、程序操作运行记录及运行过程的截屏记录，并实时传送到管理端系统中。

[0029] 其中，监控的内容包括经应用程序发生的文件生成、读取、保存、更名、复制、移动、删除中的一种或几种组合，特定文件的制作、打印、编码、图像处理中的一种或几种组合，以及通过编码程序、网盘、移动存储器、网络浏览器、MSN、邮箱程序、网络通讯程序发生的文件传送的一种或几种组合。而与监控内容相对应的触发手段包括文件代理手段、应用程序代理手段、网络代理手段、打印代理手段、屏幕拦截代理手段和通讯代理手段。此类手段通过客户端系统设置在用户终端上，随时根据各自保安政策的级别进行相应触发和工作，监控用户终端的运行和使用情况。如：

[0030] 文件代理手段依据应用程序发生的文件生成、读取、保存、更名、复制、移动、删除中的一种或几种组合，制作包括用户终端 ID、操作发生起点、文件名、文件的源路径及目标路径、目标文件名、操作方式、引发文件操作的程序名、程序路径、文件备份在内的文件操作

运行记录，并保存到指定目录中。

[0031] 应用程序代理手段依据特定文件制作、编码、图像处理中的一种或几种组合，以及通过编码程序、网盘、移动存储器、网络浏览器、MSN、邮箱程序发生的文件传送的一种或几种组合，通过文件代理手段读取文件名称、源路径和保存路径，制作包括用户终端 ID、操作发生起点、文件名、文件的源路径及目标路径、目标文件名、引发事件程序名及路径，以及文件数据备份在内的应用程序操作运行记录，并保存在指定目录中。

[0032] 网络代理手段依据用户终端向网络传送的网络通讯程序文件信息，包括 terminal 服务、telnet 服务或 FTP 服务，制作包括用户终端 ID、操作发生起点、文件名、文件的源路径、文件目标路径、目标文件名、引发的流程及其路径，以及文件数据备份在内的通讯程序操作运行记录，并保存到指定目录中。

[0033] 打印代理手段通过文件代理手段读取文件名称、源路径和保存路径，制作包括用户终端 ID、操作发生起点、文件名、文件的源路径及目标路径、目标文件名、引发事件程序名及路径，以及文件数据备份在内的打印程序操作运行记录，并保存在指定目录里。

[0034] 屏幕拦截代理手段依据文件代理手段、应用程序代理手段、打印代理手段或网络代理手段的触发，以及保安政策级别设定的周期进行用户终端屏幕拦截，生成截屏图像文件，制作包括用户终端 ID、操作发生起点、文件名、文件的源路径及目标路径、目标文件名、操作方式、引发文件操作的程序名、程序路径、截屏信息在内的相应运行过程的截屏记录，并保存在指定目录中。

[0035] 通讯代理手段随时将保存在指定目录中的运行记录及截屏记录通过内部网络传送到管理端系统中，使监控内容可以实时传送、实时进行，保证监控的有效性。

[0036] 上述各手段在指定目录中的保存过程为临时存放性质，不具有真正意义的存储功能，随着通讯代理手段传送过程的完成，会自动删除用户终端上指定目录中的保存内容，以避免占用大量用户终端的使用空间，防止监控内容从用户终端外泄。在各保存内容中，用户终端 ID 是唯一识别用户终端的代码，起到身份确认的作用；操作发生起点用于快速标识操作过程的来源，构成源头历史追踪过程的脉络；文件名、文件源路径、目标文件名、目标路径和操作方式，记录了具体文件的操作过程和操作文件名称，以及文件的来源和去向，是文件操作记录中最重要的一个环节；引发文件操作或事件的程序名、程序路径，用于记录操作过程的具体程序名称和程序所在的路径，从而确定可能的操作内容和操作范围；引发的流程及其路径，是对网络操作过程中自动引发的执行动作和路径进行记录，确保网络传送中每个环节都有监控；文件备份是各手段对操作文件进行自动备份，防止文件丢失采取的一种补救措施，以进一步提高防护可靠性。

[0037] 屏幕拦截代理手段一方面可以依据文件代理手段、应用程序代理手段、打印代理手段或网络代理手段的触发进行截屏处理，记录屏幕运行情况，直观反映运行过程；另一方面还可根据保安政策级别设定的周期进行用户终端屏幕的自动拦截，按时生成重点时段的用户终端截屏图像，随机监控终端运行过程，加大监控力度，保证监控效果。

[0038] 步骤三、管理端系统接收文件操作运行记录、程序操作运行记录及截屏记录，建立操作运行历史记录数据库和截屏历史记录数据库，并随时对各客户端系统运行情况进行监控和管理。

[0039] 管理端系统安装在服务器上，通过服务器进行实时数据接收，完成数据库操作和

记录查询，以便随时监控各客户端系统。为便于查询和追踪文件泄露过程，管理端系统实时接收来自各客户端系统发送的文件操作运行记录、程序操作运行记录及截屏记录，分别创建操作运行历史记录数据库和截屏历史记录数据库，将文字记录信息和截屏图像信息分别保存在不同的数据库中，以降低数据库的大小，提高检索速度，同时，还能保持相互间的紧密联系，为后续步骤形成文字记录与截屏图像相结合的跟踪记录过程做准备。

[0040] 当然，在管理端系统不断接收各客户端系统发送的记录信息的时候，管理端系统还会实时对客户端系统进行监控和管理。对客户端系统的监控和管理主要包括监控客户端系统的完整性和运行状况，当客户端系统由于多种原因造成系统不完整或处于停止运行状态时，甚至被人为删除时，管理端系统首先会向客户端系统发送信息或数据，实时修补或更新客户端系统，保持客户端系统完整后，重新发送控制指令，启动客户端系统，实现客户端系统对用户终端的实时监控。

[0041] 步骤四、管理端系统利用操作运行历史记录数据库检索并创建目标文件操作运行跟踪记录，并根据截屏历史记录数据库检索并创建截屏跟踪图像，经视频编辑后生成视频，完成对用户终端目标文件操作运行过程的文字和视频追踪。

[0042] 数据库是为了更快、更有效的追踪文件历史记录而建立的。其中，操作运行历史记录数据库主要由各客户端系统生成的文件操作运行记录、应用程序操作运行记录、打印程序操作运行记录、通讯程序操作运行记录组合而成，不同的记录间可通过用户终端 ID、文件名、路径等等不同的数据库字段作为索引，建立起所要的不同阶段的不同事件的历史记录，形成目标文件操作运行跟踪记录。由于各客户端系统在监控各用户终端时，根据保安政策级别设定的周期以及随着各手段的触发随时进行截屏处理，在管理端系统中形成有截屏历史记录数据库，故，在形成目标文件操作运行跟踪记录时，还可相应地以数据库字段为索引，形成不同阶段、不同事件的截屏图像记录，利用管理端系统中的视频编辑功能，自动将各截屏图像记录转化成视频图像展示出来，使跟踪记录过程更直观、更可靠、更有效。

[0043] 当然，根据需要，管理端系统利用操作运行历史记录数据库也可只创建目标文件操作运行跟踪记录或根据截屏历史记录数据库只创建截屏跟踪图像，从而以文字或视频的方式显示追踪目标。

[0044] 步骤五、管理端系统通过数据库整理手段删除与文件泄露有直接和间接关联的时间段之外收集的所有操作运行记录和截屏记录。

[0045] 为便于管理和查询，操作运行历史记录数据库和截屏历史记录数据库需定期进行不必要记录的删除，在管理端系统中设有相应地数据库整理手段，通过数据库整理手段可以方便地对不符合保留条件的操作运行记录和截屏记录进行删除，以减少记录数，提高后期检索速度。

[0046] 实施例一

[0047] 以用户终端对‘abc.txt’的文件更换名称为‘efg.txt’为例。

[0048] 登录管理端系统，通过查询方式，在操作运行历史记录数据库中查找‘abc.txt’文件名，得到一条或多条使用记录，其中，带有目标文件名的记录就是我们要查找的，目标文件名‘efg.txt’就是文件更名后的名称。再通过目标路径记录情况，就可找到更名后文件的存放位置，从而最终找到所要查找的文件。如文件已被删除，还可通过备份文件进行文件恢复，避免文件丢失带来损失。查询过程中，还可在截屏历史记录数据库中查找原文件名为

‘abc.txt’的记录，得到一条或多条使用记录后，含有目标文件名‘efg.txt’的记录就是我们要找的记录，根据记录上记载的截屏信息，就可找到截屏图像，通过自动视频编辑后，就能以视频的方式进行更名操作时屏幕运行过程的播放。整个追踪过程简单、直观、方便。

[0049] 如果文件名称经过多次变化，在操作运行历史记录数据库中查找出来的记录，则会以起始名称→目标文件名→下一记录起始名称→下一记录目标文件名的方式为线索，将多条记录串联起来，从而形成文件被更名过程的跟踪记录，同时，再配合屏幕运行过程的视频，就可将文件泄露过程完整展现出来。同样，此方式还可适用于存储路径变换、传送地址变换、邮箱目标变换等等。