



流出経路の追跡と解析を容易に行える PC利用ログ収集・解析ソフトウェア「InfoTrace」

PCの操作を記録・解析して 不正行為と被害の拡大を防ぐ

企業にとって資産である重要情報の多くは、電子データとして運用されており、その操作はPCから行われている。個人情報保護法が本格施行された今日、PCで行われている操作を、常時、管理・監視して、万一漏洩した場合は速かに原因究明することが情報漏洩対策の重要なポイントになっている。しかし、多くの企業では、対策の必要性を認識していても、「何から始めたらよいかわからない」、「社員の操作ログを収集することは重要だが、全社員の膨大なログを収集後、管理者が解析するのは困難である」といった悩みを抱えているのが現状である。

このような問題を解決することを目的に開発されたのが、(株)ソリトンシステムズのPC利用ログ収集・解析ソフトウェア「InfoTrace（インフォトレース）」である

InfoTraceは、社内に保管されている情報に対して、どのPCから、誰が/いつ/どのようなアクセスをし/どのような操作を行ったか、といった一般的に「5W1H」と言われる内容を記録して、履歴を常に管理していくソフトウェアである。記録された内容から「TraceBrowser（トレースブラウザ）」と呼ばれる検索画面を使用して、どの

ような操作が行われたのか、細かい条件を設定し、検索できるとともに、クリックで簡単にトレース（追跡）する機能を実装している。また、2005年10月から出荷を開始したバージョン1.4では、オプションとしてアラート機能を搭載することができ、あらかじめ指定した操作をPC利用者が行った場合には、それを検知し、迅速に管理者に警告する。このような機能により、不正行為に対する抑止力と迅速な流出経路究明の両面で威力を発揮し、万一情報が漏洩した場合でも被害を最小限に抑えることが可能である。

管理ツールによる一元管理で 企業のPCと情報を守る

InfoTraceの特長として、「即効性」「高性能」「高セキュリティ」「コストパフォーマンス」をあげることができる。それぞれの内容は次のとおり。

【即効性】

- ・クイックインストール：特別なデータベースは不要で、インストールは約3分で完了。
- ・ユーザーへの特別な権限設定は不要：全てのユーザーの利用権限設定を行わなくても、InfoTraceをインストールすることから始められる。

【高性能】

- ・ドライバレベルでの監視：独自技術によりOSのカーネルレベルで監視。コマンドプロンプトでの操作は「ロギングできない」といった例外なく記録する。
- ・独自コピーイベントをロギング：OSのシステムコールとして存在しないコピーを独自技術により検知、ロギングする。

【高セキュリティ】

- ・ログの自動復旧：モバイルPCなどのオフライン時の操作は、一時的にローカルディスクにログを保存。そのログを利用者が悪意を持って削除しても自動復旧される。
- ・アンインストール：利用者は許可なくアンインストールできない。アンインストールするためには、サーバ本体とクライアントPCが通信をとれる環境と特別なパスワードが必要。

【コストパフォーマンス】

- ・リーズナブルに拡張が可能：1クライアントわずか3,000円。ボリュームディスカウントや100ユーザー以下を多少としたコンパクトプライスも用意。さらに、認証セキュリティシステム「Soliton SmartOnシリーズ」や統合システム管理ソフトウェア「e-Care」、アクセス制御アプライアンス

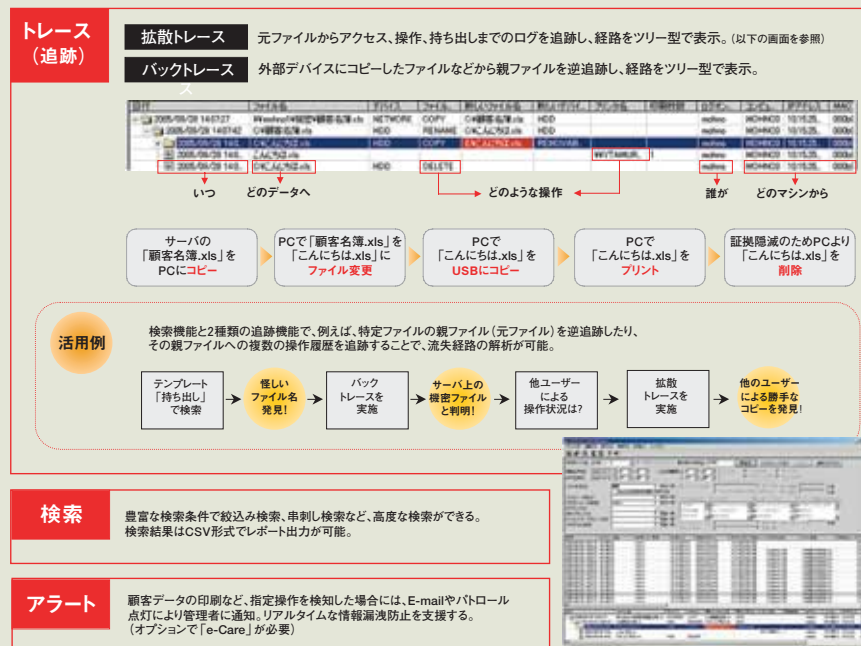


図1 InfoTraceの機能と特長

「Net' Attest」などと組み合わせ、セキュリティレベルをリーズナブルに拡張することができる。

情報漏洩の原因を迅速に究明

現在、InfoTraceは、金融機関やサービス業をはじめとした重要な顧客情報や機密データを保有する企業および団体を中心に利用が広がっている。このInfoTraceの特長を活かした利用法として、情報漏洩を未然に防ぐ対策と、情報漏洩の被害を最小限に抑える対策の2つがあげられる。それぞれの対策では、主に次のような機能が利用されている。特に後者は、事故の発生原因をシミュレーション解析して究明していくコンピュータフォレンジックに効果的である。

◆情報漏洩を未然に防ぐ対策

- ・ロギング(認証)：PCのログイン/ログオフ操作から、ネットワークおよびローカルファイル参照、削除、ファイル名変更、コピーなどのファイルアクセス情報を全て収集できる。また、アプリケーション操作やプリント出力も記録できる。
- ・アラート：顧客データの印刷や指定操作を検知した場合は、E-Mailやパトロール点灯により管理者に警告して、被害を最小限に食い止める(オプションとしてe-Careが必要)。
- ・レポート：収集した操作履歴を常時運用できるようTraceBrowserを使用せず、自動レポート出力で可能にするツールなどを無償オプションとして利用できる。

◆情報漏洩を最小限に抑える対策

- ・検索：「このファイルをアクセスした履歴」や「このユーザーが行った操作」などの様々な条件で、絞り込み検索

や串刺し検索などの高度な検索を行える。また、アプリケーション操作やプリント出力も記録できる。

- ・トレース(追跡)：元ファイルからアクセス、操作、持ち出しまでのログを追跡し、経路をツリー型で表示する「拡張トレース機能」と、持ち出しデバイスなどのファイル名から親ファイルを見つけ出し、経路をツリー型で表示する「バックトレース機能」を装備。ログは末端PCで収集するため、サーバに格納されたデータだけではなく、クライアントが独自に保持する個人情報や機密データの操作も記録、追跡することができる。

お問い合わせ先

(株)ソリトンシステムズ
 ネットワーク営業部
 TEL：03-5360-3811
 URL：http://www.soliton.co.jp/