Special
“情報”＝資産”価値に応じた情報漏洩対策とは？

ソリトンシステムズ

情報漏洩対策におけるトレーサビリティを実現したPC利用ログ収集・解析ソフトウェア「InfoTrace」

情報漏洩を防ぐには、抑止力と事後の迅速な原因究明が不可欠

顧客情報をはじめとした企業にとって資産である重要情報は、電子データとして保管、運用されているケースが多く、その情報の操作はデータの出入り口であるPCから行われている。しかし、これまでの情報セキュリティシステムは、認証やアクセス制御などの「利用制限」による事前防止策が主流であった。企業の情報漏洩事件の80%が内部の犯行であると言われている今日、さらには個人情報保護法が完全施行された中、企業内の全てのPCの操作や通信の履歴をログそして記録することで、重要情報の不正利用を抑止するとともに、万一情報が漏洩した場合は速やかに原因を究明することができるソリューションが、現在の情報漏洩対策には不可欠になっている。

その一方で、このような対策の必要性を認識していても「何からはじめていいのかわからない」、また「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管理者が解析することは困難である」といった悩みを抱えている企業も数多くある。このような問題を解決するソリューションとして開発されたのが、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。

流出経路の追跡と解析を容易に行える「InfoTrace」

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／などを記録して、履歴を常に管理していくソフトウェアである。そして、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を細かい条件を設定して検索できるとともに、クリックで簡単にトレース（追跡）する機能が実装されている。

InfoTraceの構成について、㈱ソリトンシステムズ　プロダクト営業推進部の大野真理子氏は、次のように語っている。

「InfoTraceは、ログサーバ、トレースブラウザ、エージェントの3つのソフトウェアから構成されています。ログサーバは、企業内のPCから行われたあらゆる操作を記録、収集します。収集されたログは、トレースブラウザと呼ばれる専用コンソールに必要な検索条件を入力することで、重要データへのアクセス履歴や変更履歴、コピー、プリント履歴などの経路、経緯をわかりやすくレポートします。エージェント・ソフトウェアは、PCに簡単にインストールできますが、アンインストールは簡単にはできないようになっています。ログ管理体制をユーザーに告知することで、一定の抑止力が発揮され、社内のセキュリティレベルが維持されます。このログサーバ、トレースブラウザ、エージェントは、構築が容易ですので、短期に導入することができ、ログ管理体制を迅速

㈱ソリトンシステムズ
プロダクト営業推進部
大野 真理子氏

に構築、開始することができます。」

追跡／検索／アラートなどの機能で内部情報漏洩対策を強化

InfoTraceの主な機能および特長は次のとおりである。

●クイックインストール：特別なデータベースは不要、ログサーバやトレースブラウザなどの管理コンポーネントやクライアントも極めて簡単に導入可能。セキュリティに対するユーザー権限の設定などの必要がないので、迅速な対応にも有効。

●ロギング（記録）：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、名前変更、コピーなどのファイルアクセス情報を全て収集可能。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。

●トータル（集計）：ユーザー別、プリンタ別で指定した期間や条件における印刷集計を行うことができる。

●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。

●検索：豊富な検索条件で、絞込み検索や串刺し検索などの高度な検索が行える。検索結果はCSV形式でレポート出力が可能。

●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、ソリトンシステムズの統合システム管理ソフトウェア「e-Care」が必要）。

●高いセキュリティ性：PCがオフラインの時の操作は、一時的にローカルディスクに保存。しかし、故意にログを削除しても自動復旧される。

●優れたコストパフォーマンス：1クライアント僅か3,000円。ボリュームディスカウントや100ユーザー以下を対象としたコンパクトプライスもある。

この他、2005年10月に出荷を開始した新バージョンV1.4では、日本語OSと英語OSの混在環境においても使用できるよう、Windows Agent（クライアントPC）に英語OS（Windows 2000 Professional、Windows XP Professional/Home Edition）のサポートが追加された。

19万5千ライセンス／約400社に導入

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・団体を中心に導入が進んでいる。例えば白河信用金庫では、USBメディアやFDなどへのデータコピーの持ち出し監視、Webページの閲覧監視、重要なファイルサーバへのアクセス監視などに利用することで、抑止効果とセキュリティに関する意識改善に役立てている。2004年3月の発表から現在（2005年9月末現在）までの実績は、19万5千ライセンス、同入社数は約400社である。

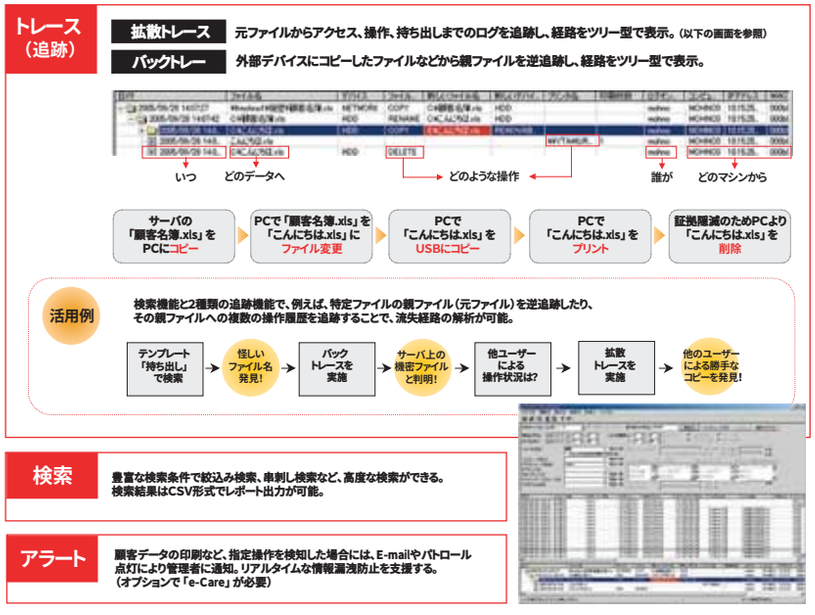

図1　InfoTraceの機能と特長

お問い合せ先
株式会社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/