

サーバーアクセスログ監査ツール

ALog ConVerter for Windows のご紹介

----- Windows サーバーのイベントログ収集と活用に最適 -----

IT システム活用の原則として、操作履歴の保管業務は決して特別な業務ではなく、むしろセキュリティの必須対策となってきました。

特に重要な情報資産を共有しているサーバーには、不正アクセスの「抑止」と、万が一に備えて「事後追跡」できるシステムが、整備されている必要があります。

今回は、Windows サーバーのイベントログ収集に最適なソリューションとして、網屋社の「ALog ConVerter for Windows」についてご紹介いたします。

ログ収集専用のソフトウェアがなぜ必要か

コンプライアンスへの対策や、セキュリティ事故が発生した場合の事後追跡を実施するために、ログが必要であることは周知のとおりです。

ただそのために、わざわざログ収集用の専用ソフトウェアが必要なのかと思われる方も、いらっしゃるのではないのでしょうか。

Windows サーバーを例に挙げますと、イベントログを出力する機能がありますので、同ログをバックアップすれば、そのまま監査ログとして利用することも可能です。

しかしログを取得するだけであれば、生ログ(イベントログ)のまま取得しても、ログ収集のソフトウェアを利用しても、変わりはありません。

ただのバックアップツールではなく、ログを活用する状況で大きな効果を期待できるのが、本当のログ収集システムであるといえます。

ログを活用するのに必要な労力

実際にログを活用する場面として、セキュリティ事故が発生した場合を想定してみましょう。

生のイベントログは、様々なシステムのログが混在していることや、1つのオペレーションでも多数のログが出力されるものがあること、またシステム側の記述で記載されているものも多く、人の目で追跡するのはなかなか簡単ではありません。

セキュリティ事故が起きた際にも、スピードが要求される中で、事故の事実確認や兆候の収集、再発防止策の策定など、その労力は関連するサーバーの数に比例して、システム担当者にかかってきます。

<図 1 参照>

【図2】

「Alge CanVerter for Windows」
アクセスログ検索システムの主な機能

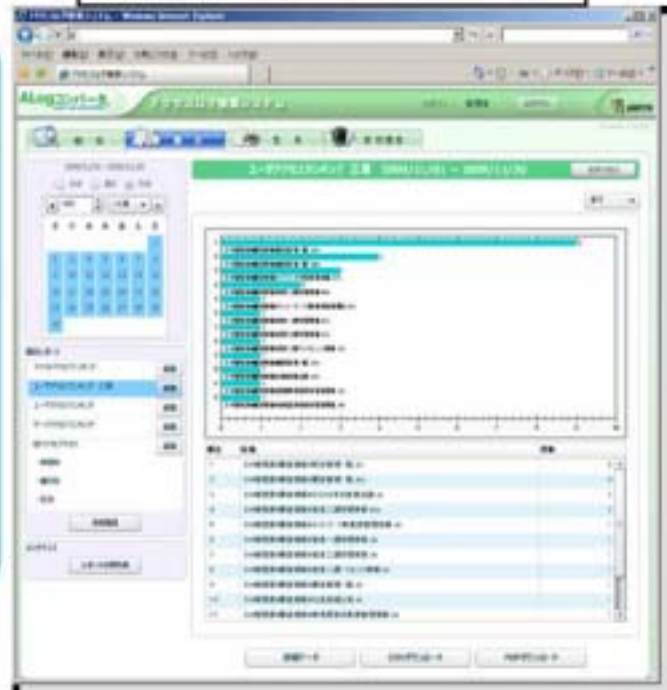
直感的に分かりやすい管理画面

<集計機能>

- ・最もファイルアクセスの多いユーザーを調べたい
- ・印刷回数が多いユーザー上位者を抽出したい

<監視機能>

- ・深夜にアクセスしている者を特定したい
- ・重要フォルダのため、全操作履歴をレポートしたい



年々増加する運用管理者の負担軽減に

IT に関連する法制も年々整備されていく中、運用管理者の負担は増加傾向にあります。弊社はそれらの法制に対応していくことはもちろんですが、その上で少しでもお客様への負担を軽減する、システムのご提案ができるよう、尽力しております。ぜひ一度ご相談ください。

(解説・IT プロフェッショナルサービス部/安藤公洋)