AI 要らずで内部不正とサイバー攻撃に対応

ログの「取りあえず保管」から「宝探しの自動化」に

2017 年 9 月 29 日キーマンズネット/TechTarget 掲載記事より

昨今のサイバー攻撃は巧妙化が進んでおり、こちらの手の内を知った上で、防御の網をかいくぐる新たな手を打ってくる。シグネチャの存在しない未知のマルウェアを用いる標的型攻撃はその一例だ。普通のメールに添付されて内部に入り込むタイプの攻撃に対し、100％の防御はあり得ない。

数年前から個人情報保護や内部犯行対策の一環として、ログ監視に取り組み始めた企業は多い。だが「内部監査対応でログは取ってはいるが、どう活用すればよいか分からず、保険的にただ保存しているだけ」という残念な状態は少なくない。しかし一方で、ログの活用がサイバー攻撃への有効策となった「成功ケース」も実は多い。成功企業と失敗企業の違いを実例を交えて探ってみよう。

～　目次　～

1. ただ残すだけでは意味がない

ログさえ残っていれば、サイバー攻撃や不正アクセスがあったときに速やかに原因を調査できる、これで問題解決だ――と思うかもしれない。だが、ただログを吐き出しているだけでは、そううまくはいかない。

IT システムは拡大の一途をたどっており、管理すべきログは膨大な量になり、機器によって出力するログのフォーマットが異なったり、ベンダーによっても差があったりする。

「時刻」や「ユーザー名」といった単純な要素を取っても、それぞれ異なる書式で出力されるため、システム内で何が起きたかを横断的に把握しようとすると、非常に面倒な突合作業をしなければならない。結局、ログは「取りあえず保険のために取っておこう」という扱いに終わってしまう。

複数の異なるサーバやネットワーク機器からログを収集し、一元的に管理できるように整理してくれる統合ログ管理ツールは以前から存在する。しかし、システム全体にまたがって、横串で横断的にログを並べても、「攻撃者を特定できた」「検知/駆除ができた」という声は聞こえてこない。なぜか？

それは、複数のログを単に並べても「あるユーザーが一連の行動をこう行った」という記録にしかならないからだ。つまり複数のログの重ね合わせでは、このユーザーが不正者だ、攻撃者だと特定できる情報は何もなく、不正を検知してくれるわけでも、サイバー攻撃を把握できるわけでもない。

本来ログとは、事後対策だけでなく『特徴的な行為を発見し、それを具体的な防衛に役立てる』という使い方にならないといけない。しかし多くの企業がそれを実践しきれていない。

ではどうすればそれを実現し、ログから「実益』を得られるようになるのか？　AI（人工知能）を搭載した高額な予兆検知システムを購入しなければそれは実現し得ないのか？　そんなことはない。実際の利用シーンの実例を見てみよう。

2. 実際にログの活用で事件を解決したケース

昨今、大きな影響を及ぼしているランサムウェアの中には、ファイルサーバに格納された重要なデータを暗号化するものもある。残念ながら、クライアント側の守りを固めるだけではこうした被害は防げない。

ある大手薬品メーカーでは、実際にあるユーザーがメールを経由してランサムウェアに感染。そのランサムウェアがファイルサーバの複数のファイルを暗号化してしまう事件があった。しかしこの会社はファイルサーバへのアクセスログを「感染したユーザー」と「ファイルの RENAME 操作」で AND 検索することで、RENAME、つまり暗号化されてしまったファイルを特定し、被害を最小限に食い止めることに成功した。

感染範囲を特定しただけでなく、さらにその後、監視レポートを自動出力して、同様の手口を自動で検知できる仕組みも構築できた。彼らは高額なシステムを構築したわけではなく、ログのパッケージソフトを使っただけだ。

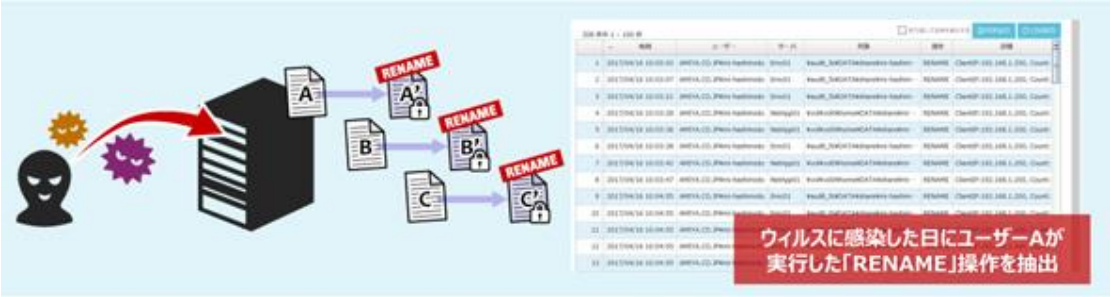

図 1　ランサムウェアを膨大な RENAME 操作で特定

また、別の企業では、あるクライアント端末が標的型攻撃によりマルウェアに感染し、重要な情報を瞬時に抜き盗られてしまったのだが、「Active Directory」のログから管理者権限を不正取得する操作を監視していたため、踏み台にされたクライアント端末を早期に突き止めることに成功した。その後、クライアント端末をネットワークから隔離。マルウェアの広範囲かつ恒常的な拡散を未然に防ぐことができたのだ。

3. リアルな不正や攻撃に対して、本当に防衛するためには？

網屋が提供する「ALog EVA」は、このようなログの有効活用を実現するツールだ。従来ファイルサーバへのファイルアクセスを記録する製品として認知のあった ALog シリーズだが、ALog EVA の登場で、ルータやスイッチ、DHCP やプロキシ、さらには業務アプリ、PC ログなど、多様なソースから、統一されたログ形式に整理して一元的に管理できるようになった。前述の具体例も、実は ALog EVA が解決した事例である。

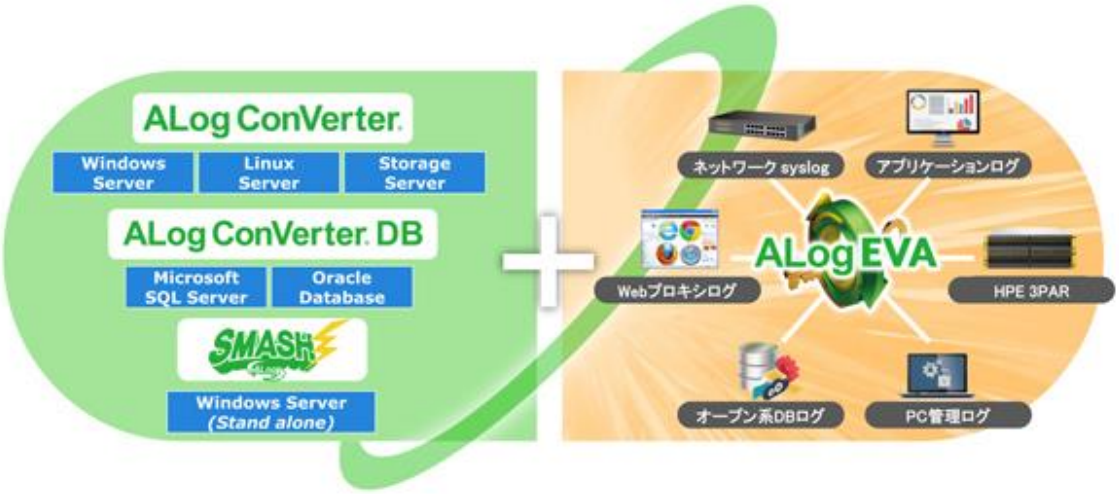

図２　ALog シリーズの守備範囲を広げる ALog EVA

なぜ具体的な不正や攻撃の防衛に成功したのか？

その答えは、ALog シリーズの開発元である網屋に、ログの収集・管理に関する長年の経験があるからだ。

同社は以前から、Windows／Linux サーバ、ストレージのログ管理ツール「ALog ConVerter」を提供してきた。「いつ、どのユーザーがドメインにログオンしたか」「いつ、どのユーザーが、ファイルサーバのどのファイルにアクセスしたか」といった、企業が本当に必要とする情報を、システムの複雑なログを分析して導き出してきた歴史が、他を圧倒するゆえんとなっている。そして、その整列されたログ群を使って、**しきい値を越えた異常な行為を特定できる**。

実はこれが ALog の大きな特徴の１つであり、まゆつば的な AI という自動化を使わずとも実際の不正や攻撃を防ぐ本質的なメリットだ。

4. 働き方改革もログで実現できる？

ログの一元管理ができれば、業務時間中に従業員が仕事と無関係な作業をしていないかも把握できる。働き方改革の中で生産性の向上を担保する仕組みとしても有用だ。

例えば、Web プロキシサーバのログを集約し、勤務時間中の YouTube や Facebook の閲覧状況を集計して「長時間利用 Top30 ユーザー」といったランキンググラフを作成し、労働生産性の低い社員を特定した実例もある。

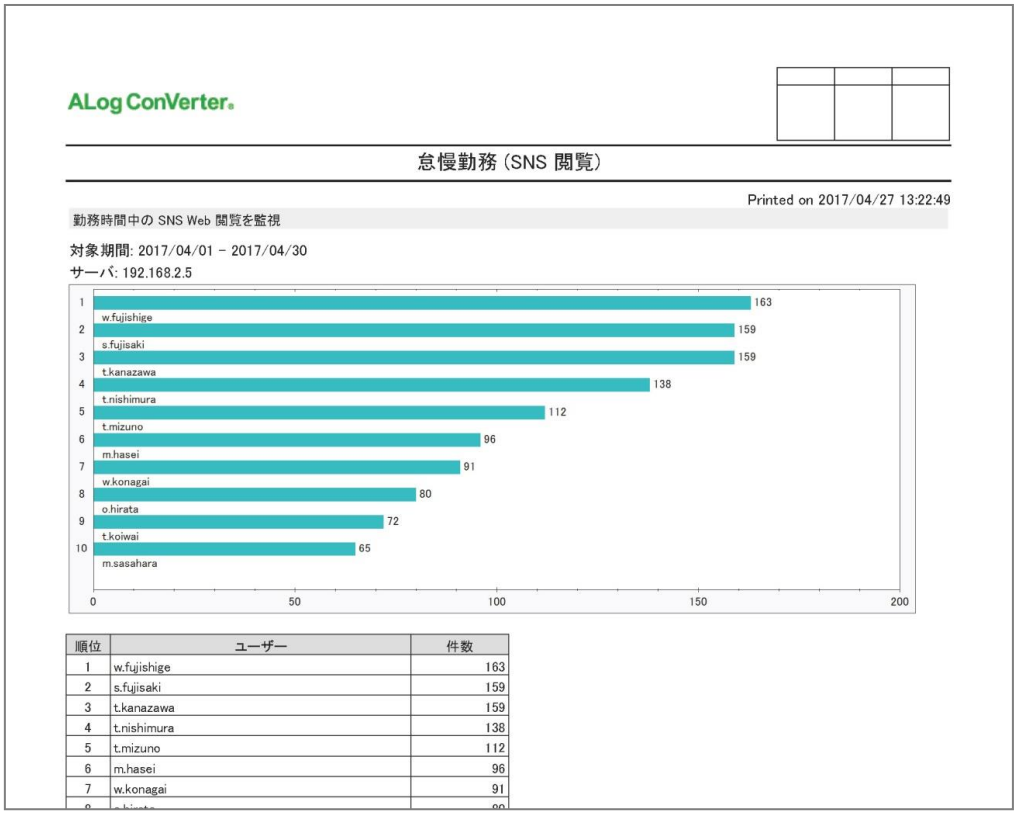

図３　１カ月間の SNS 閲覧レポート

また、働き方改革に重要な“客観的な労働時間の把握”として、従業員のオフィス入退室のログと Windows ログオン認証のログを集約して１カ月の勤怠表を作成し、**タイムカードに記録された勤務時間との差異を暴いた**ことも、実例としては多い。

このようにログの役割は、「何となく保険として取っておくもの」から、「特異な兆候を見いだして不正を特定する」や「異常値を設定し、非人間的アクセスを特定する」といった実益を伴うものへと変わりつつある。これからのログの在り方を簡単な操作で実現するログツールは、多くの企業にとって力強い味方になるだろう。