ALog

業種別事例集

AMIYA

Ver. 1_7

CONTENTS

掲載日：2020/11/04

資料をメールで受け取る ≫

品川区

ALog EVAで庁内ネットワークのログ監視体制を整備

品川区

品川区様では、庁内ネットワーク機器300台の統合的なログ管理を目的に、『ALog EVA』をご導入頂きました。
導入経緯や導入後の本音について、企画部情報推進課情報セキュリティ担当 係長 吉田 昇 氏、竹内 美和 氏にお話を伺いました。

ログの統合管理とレポーティングが自動化の第一歩

—— ALog導入の経緯を教えてください。

庁内ネットワークで通信が遅い/できないといった障害が起こったとき、原因特定から解決までの一貫体制の構築が目的でした。以前は個別のネットワーク機器内にしかログを保存しておらず、障害発生から解決まで時間を要してしまったり、ログが消えてしまい解決できないといったことがありました。現在は、庁内ネットワークのリプレイスを機に、ルーター、L3/L2SW、HUB、無線アクセスポイントの300台を対象にALogでログを統合管理しています。運用については、富士通さんにお願いしています。

品川区企画部情報推進課情報セキュリティ担当
係長 吉田 昇 氏(後列中央左)、竹内 美和 氏(後列左)、渡部 哲史 氏(後列中央右)

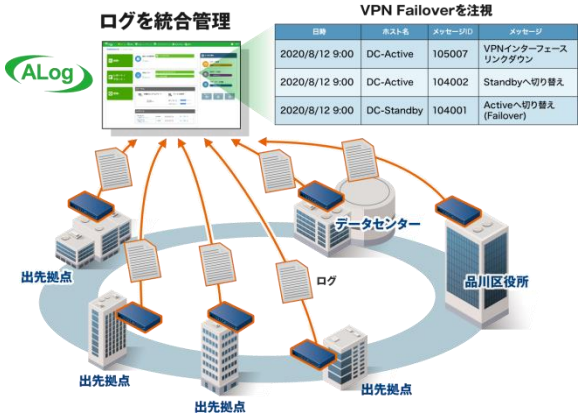
富士通ネットワークソリューションズ株式会社
塩田 洋史 氏(後列右)、廣江 直輝 氏(前列左)、山岸 博之(前列中央左)
富士通株式会社
松岡 知宏 氏(前列中央右)、峯 悠祐 氏(前列右)

—— 今回、ログ管理ツールに求められた要件を教えてください。

今回の要件は収集したログを自動でデータベース化し、高速検索できること。ログを自動でアーカイブし6年間の長期保管ができることでした。大きな要件としてはこの２つでしたが、日々利用するツールではないため、インシデント時にマニュアルを見ることなく調査ができることも重要な点でした。

—— ALogの活用方法と導入後の効果について教えてください。

庁内ネットワーク機器300台のsyslogをALogに収集しています。特に注視しているログは、VPNトンネルインターフェースのアップダウンに関するログです。出先拠点を含む複数拠点でVPNを構築しており、VPNがダウンしてしまうと業務への影響が出てしまうからです。現に移行期間中ではあったのですが、冗長構成のセンター側VPNルーターが頻繁にフェイルオーバーする事象が発生しました。冗長構成のため通信には影響はなかったのですが、インターフェース以外のログも含めて調査することで原因の特定と解決ができました。その際、センター側のVPNルーターだけでなく、拠点側のVPNルーターのログも確認が必要だったので、ALogの検索機能が大いに役立ちました。



—今後の展望について教えてください。

現在はインシデントが起こったら、ログを確認して対応することがメインの利用方法ですが、今後はインシデントが起こる前の予兆を察知するためにALogのアラート、レポート機能を活用していきたいです。さらに、ネットワーク機器以外のシステムのログも収集しておくことを検討したいです。何かあったときに、ログがないと対応の幅が狭まりますので。

ALogでネットワーク負荷の原因を特定！ 大量ダウンロード者を突き止め、再発防止へ

帝京平成大学

帝京平成大学様は、医療からグローバルまで、都内と千葉の4箇所のキャンパスに 1万人超の学生をかかえる都市型大学です。
この度、総合情報技術センター係長の江上栄司氏に、ALogの導入の背景、導入効果などについてお話を伺いました。

ネットワークのトラフィック量を把握するためにALogを導入

―― 導入の経緯を教えてください。

学生や教員によるWi-Fi利用が進んだこともあり、快適な学内ネットワークを提供する重要性が高まっていました。そのためには**ネットワークのトラフィック量など、通信実態を正確に把握することが重要と考え、ログ管理製品の選定を行いました。**
将来、校内キャンパスが新設されることを考えれば、取り込むログの種類が増加する事も予想されます。非常に高価な製品で要件を満たす事も考えましたが、将来の可能性だけで多くの投資はできません。従って、「運用のしやすさ」「将来の拡張性」「価格」の3点を軸に、様々な製品と比較検討しました。
その結果、「ALog ConVerter」と「ALog EVA」の2つが最適という判断に至りました。

ネットワーク負荷の原因も特定できた

―― ネットワーク遅延のボトルネックを突き止めたそうですね？

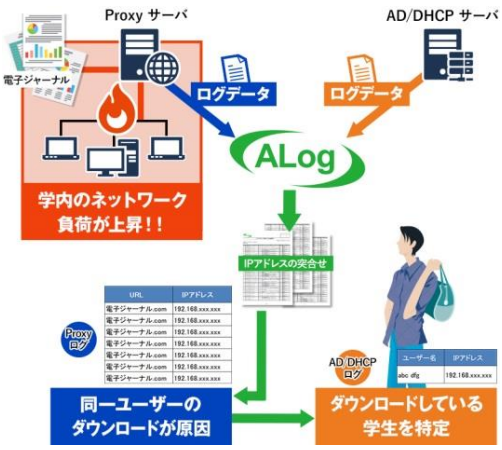
本学では様々な電子ジャーナル（学生向けのオンライン情報誌）を利用できるのですが、**ある特定の電子ジャーナルの大量ダウンロードが学内ネットワークに負荷あたえネットワーク遅延の一因になっていること**を、ALogのProxyログを確認することで、特定することができました。
更に、**ProxyのURL / IPアドレスのログ、Active Directory（AD）のログ、DHCPのIPアドレスのログなどから大量ダウンロードする学生を突き止め、本人に直接注意喚起をする事も可能となりました。**

インタビューに応じていただいた
総合情報技術センター 係長 江上栄司氏

SIEMとしての活用も見据える

―― ALogに期待する事を教えてください。

将来的にはファイルサーバやセキュリティゲートウェイのログも一元管理し、SIEM（Security Information and Event Management）としてALogの利用の幅を広げたいと考えています。
例えば、教員が個人所有するPCを業務で使用させるBYODです。作業の効率化は望めますが、マルウェア感染による情報流出などのリスクがあります。
ALogを使えば、仮にマルウェア感染されたとしても、ADサーバのログを使って、不正な管理者の作成を見つけ出したり、UTMのログを使って、外部への不審なC&Cアクセスを見つけ出したりと、ログデータからトータルに追跡でき、迅速な対処を実現できます。
セキュリティツールは、総合情報技術センターのメンバーが誰でも使いこなせることが大事なので、ALogのような使いやすいGUIは重宝します。ALogの登場で、内部、外部攻撃の両面から対策ができるので、今後の重要性はますます高くなると考えています。



帝京平成大学

設立年月日： 1986年12月
事業内容： 大学、大学院の運営
所在地： 〒170-8445 東京都豊島区東池袋2-51-419
URL： https://www.thu.ac.jp/

掲載日：2019/10/16

膨大化するファイルサーバをシンプルに管理・運用！ムダを削ぎ落とした抜群の費用対効果Resource Athlete

株式会社東京リーガルマインド

「資格の総合スクール」として、1979年の創業以来、長年に渡り社会人の学びをサポートしてきた東京リーガルマインド社（LEC）。同社はファイルサーバのリプレイスを機にResource Athleteを導入し、その運用改善に成功されました。従来抱えていた課題と、導入後の効率的なサーバ管理について、システム部で基盤運用を担当される高野隆一氏に伺いました。

肥大化と管理の煩雑さが課題に――管理ツールには費用対効果も重要

―― Resource Athleteを導入される前、ファイルサーバ管理にはどのような課題があったのでしょうか。

データ容量の増加とアクセス権管理の煩雑さが課題になっていました。全社規模で利用しているファイルサーバはフォルダ数・ファイル数ともに膨大です。特に、広告部門などでは重いビジュアルデータを大量に扱っています。最近は想定を上回るペースでデータが増えており、容量が逼迫していました。だからといって無尽蔵にディスクを増設するわけにはいきません。やはりスリム化は避けては通れず、サーバに付属されていた簡易的な管理ツールで、不要なファイルや大容量のフォルダをなんとか洗い出していました。

また、フォルダのアクセス権も、自作のExcel台帳での管理です。頻繁な部署移動や、有期的なプロジェクトが多く、正しくアクセス権が付与されているか棚卸をするのも一苦労でした。

いずれも長年運用する中で作られてきた独自ルールで管理をしていましたが、ファイルの増大に伴い運用負荷が増大してきました。この負荷を軽減できないか、自動化できるツールはないかと模索していた時に、見つけたのがResource Athleteです。

―― Resource Athleteを選ばれた理由をお聞かせください。

ALogシリーズの実績による安心感はもちろんですが、一番は費用対効果です。他製品もいくつか検討しましたが、「多機能で非常に高額」というものばかり。その点Resource Athleteは、「必要な機能がきちんと揃っていて、無駄なく、かつ手ごろな価格」です。費用と機能のバランスが非常に優れていると感じました。

操作が簡単だった点も魅力的でした。画面がわかりやすいので、直感だけでスイスイ使えます。サーバ管理の経験がある方なら、Resource Athleteはほぼマニュアルなしで理解できると思います。

管理負荷は大幅に軽減システムでできることは極力自動化し、効率化を

―― Resource Athleteの導入により変化した点を教えてください。

ファイルサーバ全体が見える化されたことは大きな成果です。具体的には、「どのフォルダを、どの部署が、どれだけ使用しているのか」のデータ容量や、「どのフォルダに誰がアクセスできるか」のアクセス権が、一目瞭然になりましたね。

以前の管理ツールでは、手動で収集したデータをより見やすい体裁に加工し、異常なものを目視で確認する必要がありました。その点Resource Athleteなら、自動的にレポート出力してくれますから。急な容量の変化があればアラートが上がり、そのレポートを持って関係部署に問い合わせるといったこともできます。大幅に作業効率がアップしましたね。
システム部の仕事はファイルサーバの管理だけではありませんから、自動化できるものは極力自動化して効率化したい、そんなニーズにぴったり合致しました。

――今後、ファイルサーバをどのように運用されていかれますか。将来の展望をお聞かせください。

Resource Athleteの機能を活用して、長期的に使われないファイルや重複ファイルなどリスト化し、それを元に関係部署に確認を取るなどして、さらなるスリム化を目指したいですね。Resource Athleteをベースに、しっかりとした運用ルール作りを進めていきたいと思っています。

インタビューに応じていただいた
システム部 インフラ整備課 基盤運用担当 高野隆一氏

株式会社東京リーガルマインド

本社： 〒164-0001 東京都中野区中野4-11-10 アーバンネット中野ビル
設立： 1979年1月
事業内容： 各種国家資格・公務員試験受験指導、LEC会計大学院の開設・運営など
URL： http://www.lec-jp.com/

監査対応にはやっぱりALog 「ALog EVA」で情報システム管理者の監査も

株式会社トランザクション・メディア・ネットワークス

電子マネーやクレジットカードなど決済サービスのインフラを提供する株式会社トランザクション・メディア・ネットワークス様。
「ALog EVA」の導入背景と効果についてお話を伺いました。

端末ではなく要所を押さえるログ管理

―― ALog導入の経緯を教えてください。

PCI DSSやPマーク、内部監査などの様々な監査に対応するためです。検討の結果、重要データへのアクセス状況を把握するためには、ツールのインストールの有無に影響されるPCログより、**データそのものに視線を向けてサーバやプリンタといった要所を押さえるログ管理が有効**と考えました。（村上氏）

ログ管理ツールといえば、ALog

―― ALog以外に、検討されたログ製品はありますか？

サーバサイドのログ取得となると、比較対象となる製品は他にありませんでした。以前前職で、ISO 27001の取得を目的にログ管理ツールの選定したことがありましたが、その時も**監査対応にはサーバログに強いALogシリーズ**という結果になりました。
こうした経験を踏まえ、私からもALogを推薦しました。（村上氏）

アーキテクチャ企画部社内情報システムグループ
マイクロソフト認定システムエンジニア 村上仁孝氏（左）
芳原憧氏（右）

ALog EVAをSIEMツールとして活用

―― 実際にALogの導入してみていかがでしょうか。

これまではファイルサーバ、Active Directory、Webアクセス、プリンタなど、複数の多種多様なログデータを、担当者が数日かけてまとめていました。統合ログ管理製品である**ALog EVAを導入してからは、それら複数のログは自動で取得／管理ができるため、手作業がほぼなくなりました。**（芳原氏）

ALogが自動出力するレポートは、グラフなど視覚的にわかりやすく、統計／集計データを簡単に確認できます。具体的な問題点を発見しやすく、現場へそのまま提供することも出来るようになりました。
また、**ALog EVAはSIEMツールとしてセキュリティのインシデントやシステム管理者の操作ログも検索分析できます。**今後は、内部監査の担当者に直接ALog EVAの管理画面を見てもらい、**情報システム管理者の監査**もしてもらおうと考えています。
（村上氏）

ログで働き方改革も！

―― 今回、勤怠管理ツールWorkTimeも一緒にご導入いただきましたが、勤怠について気がかりなことがあったのですか？

勤務実態についてですね。社員が自分で入力する「タイムシート」と「実際の業務状況」に乖離が生じていないかを確認することがコンプライアンス上、重要だと考えていました。
今回、ALogのオプションであるWorkTimeを導入し、**Windows認証ログオンのログに加え、PCのロックやスリープのログも収集できたことで、サービス残業者の発見など、より精密な勤怠データをまとめることが出来ました。**
また副次的な成果として、「ログの取得」を社内へアナウンスする事で、サービス残業への抑止効果にもつながりました。（村上氏）

株式会社トランザクション・メディア・ネットワークス

設立年月日： 2008年3月
事業内容： 電子決済に関連する決済インフラの提供
所在地： 〒103-0027 東京都中央区日本橋2-11-2 太陽生命日本橋ビル18階
URL： https://www.tm-nets.com/

“LINE”に相応しい高いセキュリティ水準を ALogシリーズがアシスト

ALog ConVerter for Windows / Resource Athlete

LINEヤフー株式会社

日本国内で圧倒的シェアを誇るおなじみのコミュニケーションアプリ「LINE」を展開するLINEヤフー株式会社様。インターネットサービスの会社として高いセキュリティ水準を掲げている同社の運用業務効率化のために、この度ALogシリーズをご採用いただきました。

複雑なイベントログを読み解く苦労が一気に解消

-- LINEヤフー社ではALog導入以前はOSのイベントログを専門チームが読み解かれていたとのこと。社内システムの運用に携わる青柳氏は、以前の状況を次のように話して下さいました。

「当社はインターネットサービスの会社ですから、セキュリティ水準は高く維持すべきだと考えています。社内外の不正アクセスに備え、ファイルサーバや認証基盤のイベントログの分析を、セキュリティ対策の一環として長年行なってきました。
しかしOSのイベントログは膨大な量がありますし、メッセージの内容も複雑ですので、セキュリティチームが大変な労力を伴ってログを読み解いていました」

--ファイルサーバの更改を機に、業務効率化のためALogを導入して約3ヶ月。青柳氏も効果を実感しておられるとのこと。

「複雑なイベントログが、ALog ConVerterによってひと目でわかるファイルアクセスログに変換され、従来のログを読み解く苦労が一気に解消されました。
セキュリティチームだけでなく、社内システム部門でもログを分析することができるようになったので、オペミスのチェックや原因特定において効率化が図れています。以前はサーバとクライアント、双方の膨大なログを読み解いて原因を究明する、という大変な作業でしたので…。
検索やレポートのGUIが分かり易いのもいいですね。マニュアルを見なくても使えています。いずれはユーザー部門に展開して、さらにコンプライアンス向上を図っていきたいと考えていますので、GUIが分かり易いのは有り難いです」

LINEヤフー株式会社

設立： 2000年9月4日
所在地： 東京都新宿区新宿四丁目1番6号
JR新宿ミライナタワー 15F～23F
資本金： 77,316百万円 （2016年9月末時点）
社員数： 1,328名 （ LINEヤフー株式会社単体、2016年10月1日時点）
事業内容： ・インターネットサービス
・キャラクター事業
URL： https://linecorp.com/

ファイルサーバの運用業務をALogシリーズで時短

-- LINEヤフー社はシリーズ製品Resource Athleteも同時に導入されています。こちらも社内システム部門の業務の一助となっている様子。

「ファイルサーバのアクセス権周りの棚卸しのために導入しました。こちらも業務効率化が主な目的です。アクセス権リストをツールなしに作成するのはやはり労力が大きいので、自動でリスト化できるResource Athleteへの期待値は高いです。
棚卸しだけでなく、古いファイルをピックアップしてアーカイブしたりと言った、ファイルサーバの肥大化防止にも活用したいです」

--さらにコストメリットにおいても、LINEヤフー社の要件を満たすものだったとお教え下さいました。

「実は他社製品も候補に挙がっていましたが、高性能でコストパフォーマンスの良いALogシリーズを選びました。我々の業務が大幅に効率化され、かつコンプライアンス向上にもつながり、ALogシリーズは当社の要件を満たす製品だったと感じています。
まだ導入してまもなく、やっと運用が落ち着いたばかりなので、これからどんどん活用していきたいと思います」

-- ALogシリーズに始終お褒めの言葉を下さった青柳氏。
今後もLINEヤフー社のご期待に応えられるよう、機能改善・拡張に取り組んでまいります。

社内システム室　社内システムチーム　青柳 幸子 氏（写真左）
ブラウン&コニーと写真を撮りたい！ という網屋営業マン（写真右）のリクエストに快く応じてくださいました。

データセンターから提供するクラウド型ログ管理サービス

ALog ConVerter for Windows Advanced edition

KDDI株式会社

KDDI様は、従来の広域イーサネットやIP-VPN型サービスとは異なる「広域仮想スイッチ」という新型ネットワーク「KDDI Wide Area Virtual Switch」を使ったデータセンターサービスを2013年2月に開始されました。**そのオプションとなるファイルサーバサービスに「ALog ConVerter for Windows」をご採用頂いています。**

クラウドサービスでも活躍する ALog ConVerter

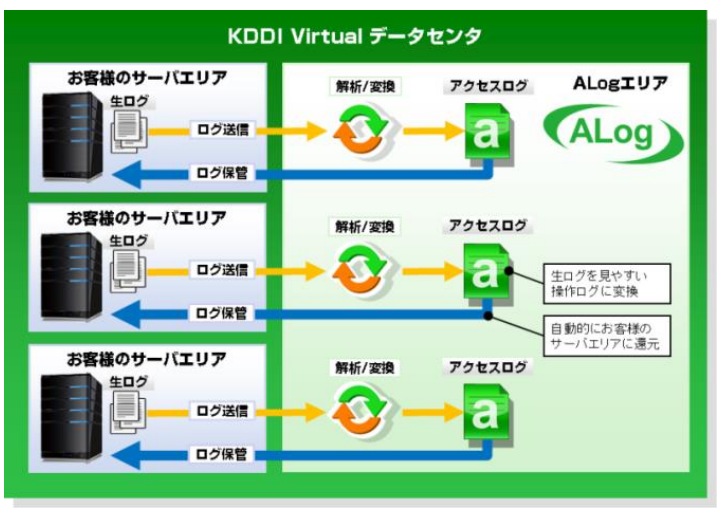
-- ALogをご選択いただいた背景や評価の決め手は？

「ファイルサーバサービスを提供するにあたり、ファイルアクセスログの取得がお客様からの要望として多くありました。とはいえ、Windows Serverの標準機能のイベントログでは、不要なログが多いため、ディスクの使用量が増加してしまいます。

そのため**必要なログ情報だけを保存し、理解しやすいログ管理製品を探していた**ところ、 ALogがぴったりとニーズに適していました。**お客様の中には既にオンプレミス環境でALogをご利用のお客様も多かったので、そこと連携できる**という点も大きいです。

以前からお客様に『誤ってファイルを削除してしまった際に、誰がどんな操作をしていたのか事後追跡できるようにしてほしい』と言うご意見を頂いていました。それをALogで実現できたわけです。見やすい操作ログに変換してお客様に還元できるようになりました」

■サービスイメージ図



オンプレミスとクラウドで 連携したログの管理が実現！

-- ALog を採用して良かった点はどこでしょう？

「今回ALogを採用したことで、難解なイベントログではなく、分かりやすいアクセスログをお客様に提供できるようになりました。**既にALogをご利用中のお客様が、弊社のファイルサービスで取得したログを、自社の環境で管理できる点も好評です。弊社サービスのログをお客様のALogにそのまま流し込める**という点は、他社のサービスと差別化ができ、優位性がありますね。

今後は、我々のようなクラウドサービス事業者ならではの要望も汲み取って、新しい機能を拡張して行って欲しいです。例えば、お客様ごとにALogの検索画面を使えるようになると良いと思います」

-- KDDI様という大手のクラウドサービスにALogを標準機能として組み込んで頂きまして誠にありがとう御座います。最近クラウドサービスの機能に採用されることが多いので、代表的な事例として公開出来て、大変嬉しく思っております。

今後もKDDI様のご期待に応えられるよう、より一層の機能向上と品質向上に努めます！

サービス企画本部
クラウドサービス
企画開発部　課長補佐
松本 健太郎氏

KDDI株式会社

本社： 東京都千代田区飯田橋
3丁目10番10号
ガーデンエアタワー
TEL： 03-3347-0077
代表者： 代表取締役社長 田中 孝司
設立： 1984年6月1日
資本金： 141,851百万円
従業員： 20,238人 (連結ベース)
事業内容： 電気通信事業
URL： http://www.kddi.com/

経営へのログ活用、ITの進歩に追随するログ活用

ALog ConVerter for Windows, Linux / ALog EVA

アイティ ソリューション サービス株式会社

アイティソリューションサービス株式会社（ITSS）は、セキュリティ、ネットワーク監視、ITインフラ（サーバ・ネットワーク）に関する構築、24時間のサポートサービスを手掛けるシステムインテグレーター。同社は2005年に取得したISMS認証国際規格の改訂（ISO/IEC27001：2013）を受け、情報システムのレビュー体制を従来より確実なものにするためにALogシリーズを導入した。

ログの自動解析が導入の決め手

--ISMSの運用を考えてのご導入とのことですが、ALogシリーズの選定に至ったポイントは何だったのでしょうか。

情報セキュリティ管理室
久間 司 室長

「経営層にインプットするためのログ、と考えた時に有益だと判断したのがALog ConVerterでした。我々はログ解析の専門家ではありませんから、情報システムのログを経営層にもわかる形でレポートするのは難易度が高く、これがすべて自動的に作成されるALogに魅力を感じました」（久間氏）

--差支えない範囲でログ活用の具体例を教えてください。

情報セキュリティ管理室
御子柴 晶久マネージャー

「ALog ConVerterは、消えたファイルの捜索に役立っています。ドラッグ＆ドロップで予期せずフォルダーごとどこかに行ってしまった、というミスが時々ありますが、ログを検索すればすぐに原因が特定できるので、ユーザー部門も我々も助かっています。
ALogシリーズはGUIが直感的で、様々なレポートが簡単に作成できるので、ログの有効活用が飛躍的に進みます」（御子柴氏）

発想の自由度が広がるカスタマイズ性

--ALog EVAはあらゆるログを取り込める分、ALog ConVerterより若干難易度が高いと思われますが、実際にはいかがですか？

「 ALog EVAはマッピング定義を作りこむ必要があるので、確かにALog ConVerterより手順は増えますが、難しさはそれほど感じません。基本的な設定は、組み込まれた関数を使いますので、既成のテンプレートを活用するだけです。**細かい要求があるときはC#の関数を使って定義することもできるので、簡便さも拡張性も併せ持っている**、ということですね。
カスタマイズの敷居の低さが発想の自由度を広げてくれますし、メーカーサポートも手厚く、申し分ないです」（御子柴氏）

--今後はどのような活用を計画されていますか？

「ログによる情報システムの状態の把握や追跡は、今後ますます重要になってきます。
攻撃や不正の発見に留まらず、情報システムのあらゆる情報を経営層にレポートしていけることが理想です。
例えば勤怠システムのログから残業の累計時間をまとめるなどは、働き方改革に有用です。
ログという情報の宝庫の有効活用を、もっと進化させていって頂きたいですね」（久間氏）

サイバー攻撃対策にALog EVA

--ALog EVAもご導入されていますが、主な目的は？

**ALog EVAは、我々の事業にとって非常に有用でした。
プロキシサーバのログからは、見知らぬIPアドレスへのアクセスが分かります。つまり、C&Cサーバへアクセスを繰り返していないかを検知できるようになりました。
万が一IPS/IDSで侵入をブロックできなくても、ログを見れば出口側で検出できるというわけです。**

アイティ ソリューション サービス株式会社

設立：	1999年10月1日
本社：	東京都港区芝2-3-3 芝二丁目大門ビルディング6階
資本金：	1億円
従業員：	85名（2018/1/31現在）
事業内容：	セキュリティ提案・構築・保守 ネットワーク監視提案・構築・保守 ITインフラ（サーバ・ネットワーク）に関する提案・構築・保守 サポートサービス（システムの運用管理・保守）
URL：	http://www.it-ss.co.jp/

ログ管理と言えば網屋。EMC社との技術連携も充実していて安心

ALog ConVerter for EMC

NTTコミュニケーションズ株式会社

クラウド事業の国内最大手、NTTコミュニケーションズ様は、EMCサーバをご利用のお客様に、2013年7月よりログ運用管理のため、ALogをご導入頂きました。

お客様に自信をもって勧められる、安定性のある製品

--導入背景についてお聞きしました。
「きっかけは、お客様からの『サーバ内のデータが消えているので社員の操作履歴を確認して欲しい』というお問い合わせでした。お客様の要望に迅速に対応するため、管理体制を強化する必要があると感じALogを導入しました。**ALogは以前当社のお客様に導入した経験があり、安定稼働の実績があったので、こちらのお客様にも自信をもって勧められる製品**だと感じ採用を決めました。また、費用対効果が優れている言う点も良かったです」

--実際にログ管理のサービスを提供されて、お客様の評価はいかがですか？
「これまで操作履歴の確認にはEMCサーバが出力する監査ログをそのまま利用していたのですが、ログの出力量が膨大なのですぐにディスク容量を圧迫してしまい、サーバメンテナンスの手間が課題となっていました。
ALogを導入したことによってログのデータ量が4万分の１に圧縮されるので、ログデータの肥大化を防げるようになりました。メンテナンス頻度が下がったことでサーバの可用性も高まり、お客様から高評価を得ています。
当社のお客様からいただくRFPには必ずと言っていいほどセキュリティ対策としてログ管理の要件があります。特に近年、大きな情報漏えい事件が世間を騒がせてからは、お客様も神経質になられていて、ほぼ100%ログ管理製品の導入を検討されていますので、今後も積極的にALogを提案して行きたいと思います」

『ログ管理と言えば網屋』を貫いてほしい

--導入して最も良いと感じた点は何でしょうか？
「やはりログデータが大幅に圧縮できることです。実は今までは、ディスク容量が圧迫されるたびに、マンパワーでログデータの圧縮や退避などのメンテナンスを行っていました。多い時は、週に3、4日その作業のためだけに時間を費やしていましたが、ALogは自動で監査ログを圧縮して保管してくれるので、ディスクのメンテナンスの手間が激減し、人件費は８割～９割を削減しました。ALogのおかげと言えます。
それに、 ALogのサポート対応は外資系の製品のベンダーと比較して常に丁寧・迅速で本当に素晴らしいですね！今まで困ったことは一度もないです。
EMC社との技術連携も充実しているため、安心してお任せできます。」

--最後に今後の展望や、網屋に望むことについてお聞かせください。
「昨今ファイルサーバの容量はテラバイト単位で増えており、お客様が保有するデータ量も比例して増えています。大容量データを扱う大規模ユーザー様にこそ、ALog ConVerterをご導入いただき、一元的なアクセスログ管理のサービスをご提案したいと考えています。
網屋さんは**『ログ管理と言えば網屋』という世間的な認知度もありますし、このポジションをさらに貫いていただいて、網屋さんに任せれば最先端のログ管理が実現する！という企業になって欲しいです**」

-- NTTコミュニケーションズ様やそのお客様に高い評価をいただき、大変嬉しいです。本日はありがとうございました。

クラウドサービス部
ホスティングサービス
柴田 康雄 様

NTTコミュニケーションズ株式会社

本社： 東京都千代田区内幸町1丁目1番6号
TEL： 03-3500-8111(代表)
代表者： 代表取締役社長 有馬 彰
設立： 1998年2月
資本金： 2,117億円
従業員： 26,850人（2014年3月31日現在）
事業内容： 電気通信事業等
URL： http://www.ntt.com/

掲載日：2013/04/12

アクセスログ管理によるIT統制の実現と情報漏洩の抑止。追跡調査も可能に！

ALog ConVerter for Windows Advanced edition

日清紡ホールディングス株式会社

日清紡ホールディングス様は、2006年にNetApp版を導入し、新たに2012年6月に ALog ConVerter for Windows Advanced editionをご導入頂きました。

海外他社製品と比較。決め手はログの圧縮率とGUIの使い易さ。

--ご導入頂いた背景についてお聞きしました。
「6年前、統合ファイルサーバを導入する際に、内部統制の一環としてログ監視の必要性もあり、他社製品も含めログ監視ツールを検討しました。」（渡辺氏）

--決め手になったポイントをお聞きしました。
「**大量のログに困っていたところ、ALogの場合最終的にはログの容量が数千分の一になる！という言葉で決めました。**あとは、ログ監視ツールを初めて入れるので、対象サーバ側に負荷をかけずに、わかりやすい形式でアクセスログが見られるというのが条件でしたが、ALog ConVerterはエージェントレスでその条件をクリアしていたので導入を決めました。」

--導入後の使用感についてお聞きしました。
「管理画面がシンプルで使いやすい点が非常に気に入っています。選定のきっかけにもなりましたが、**一番の決め手はログサイズが非常に小さくなる点。**そのため6年前のログが今も保管出来ており、URLとアカウント/パスワードを担当者に教えるだけでどこからでも検索システムへアクセスでき、検索が行えるので運用がしやすいところです。」

不正アクセスもレポート機能を駆使して検知！

-- ALogの活用方法について
お聞かせください。
「社内から**「ファイルが無くなったので探してほしい。」といったリクエストが上がることがあります。そういった場合、削除されたのか移動されたのかが簡単に調査出来る点が良い**のと、操作をした本人は削除や移動したことに気づいていない場合があるので、どんな操作をしたのかを聞いて正しい操作方法を指導するのに役立っています。また、ALogのアクセスログ監視により「見られている」ということで情報漏洩の抑止力にもなっています。」（清家氏）

「その他には、**リモートデスクトップを踏み台とした不正アクセスを防ぐための監視としてレポート機能も利用しています。**また特権管理者が、権限を悪用して別の新規アカウントを隠れ蓑に不正を行うというケースを防ぐため、**管理者操作ログを使ってユーザーアカウントの作成履歴も監視**しています。」

--ご要望についてお聞きしました。
「検索システムが使いやすいので、マルチのログも検索システムで見られるのが理想ですね。今後そういった機能が追加されると聞いたのでリリースされるのが楽しみです。」

--次回は是非、ResourceAthleteで事例取材させて頂ける事を願っております。本日は貴重なお話をありがとうございました！

今後の展望について

--今後の展望についてお聞きしました。
今後もっと色々な業務サーバに展開したいと思っています。エージェントレスなので業務サーバには適していると思いますね。

財経･情報室
情報システムグループ
担当課長
渡辺 博信 様

財経・情報室
情報システムグループ
清家 竜二 様

日清紡ホールディングス株式会社

本社：	東京都中央区日本橋人形町二丁目31番11号
TEL：	03-5695-8833
設立：	1907年2月5日
資本金：	27,587百万円（2012年3月31日現在）
従業員：	連結22,304名（単体236名）
事業内容：	テキスタイル、ブレーキ、ペーパープロダクツ、メカトロニクス、ケミカル、エレクトロニクス、不動産
URL：	http://www.nisshinbo.co.jp/

NetAppマスターディストリビューターが自社利用NetAppにALogを採用

ALog ConVerter for NetApp

株式会社ネットワールド

国内有数のITディストリビューターであるネットワールド様は、取扱い商材の幅広さはもちろん、顧客ニーズを汲んだ的確な提案と、それを実現・サポートできる高い技術力にも定評がある。アジア初のNetApp製品のディストリビューターであるネットワールド様が、この度自社利用のNetAppにALog ConVerterを導入。その背景を、情報システム室の盛永氏、安藝氏に伺った。

NetAppのファイルアクセスならALogが一番分かりやすい

-- ズバリALogをどのように活用されていらっしゃいますか？

「重要ファイルのアクセス監視です。
ファイルアクセスログは、昨今は監査でも必ず指摘されますし、もはや当たり前になりつつあると感じています。
当社では管理の効率化のため、ファイルの重要度に応じて保存するファイルサーバを分けています。その中でも特に重要なファイルを保存しているNetAppサーバに対してのアクセスをALogで監視しています」（盛永氏）

-- NetAppのマスターディストリビューターである貴社なら、ALog以外にも様々な選択肢があったかと思いますが、ALogを選択した決め手は何でしたか？

「製品検証を担当しているチームに"NetAppのログが一番見やすいツールは？"と聞いたところ、ALogを推薦されました。
もちろんALogのようなログ製品がなくても、NetAppだけでログを見れることは見れるのですが、専門知識がないと解読が難しいのと、追跡性が弱いので…。ユーザーの操作がひと目で分かるように翻訳変換してくれるALogは、我々情シス部門にとって非常に有用です」（安藝氏）
「当社はALogの販売代理店としての多数の実績がありますし、私自身も過去にALogを販売していたことがありますので、まったく問題なくALogに決めました」（盛永氏）

エントランスにはNetApp社をはじめ、メーカー各社から贈られた表彰盾が

最新ソリューションを検証できる複合システム検証センター「GARAGE」

多機能よりも構築・運用のしやすさ

-- 他社製品との比較はされましたか？

「NetAppのログ管理ツールは統合ログ製品でいくつかありますが、ファイルアクセスの監視と言う我々の目的に対してはやや大仰です。まず管理サーバを立てるのが大変ですし、その運用にも負担がかかります。
NetAppに特化したツールでなくても、PCログ製品なら、ユーザー毎のファイルアクセスが細かく追えますが、ログが多く見きれないという課題が生まれます。
構築・運用のしやすさを重視した結果、可読性や追跡性に優れたALogが最適という結論に至りました」（盛永氏）

-- ALogを導入してみて、効果はいかがでしょう？

「月並みですが抑止力は感じています。やはり見られていると不正は犯しにくいので、ログを取っていること、監視していることはユーザーに公表していくべきと考えています。
それと、ログを取っていることを公表したせいか、消えたファイルの捜索依頼のような問い合わせも増えました。消えたと言っても、ドラッグ＆ドロップで意図しない場所にファイルを移してしまった、と言うオペミスがほとんどですね。ALogで検索するとすぐに見つかるので、情シスとしても助かっています」（安藝氏）
「今後はセキュリティだけでなく、働き方改革にもログの活用の幅を広げていきたいです。テレワークを許可する代わりにログを取るなど。ALog for NetApp以外のALogシリーズも活用していきたいです」（盛永氏）

-- セキュリティに働き方改革に、ALogを多方面で活用いただけると嬉しいです。本日はありがとうございました。

株式会社ネットワールド

設立： 1990年8月1日
本社： 東京都千代田区神田神保町2-11-15 住友商事神保町ビル
資本金： 5億85百万円
売上高： 785億（2016年12月度）
社員数： 419名（2016年12月末現在）
事業内容： IT・ソリューションズ・ディストリビューター
URL： http://www.networld.co.jp/

掲載日：2020/08/04

特権管理者こそ正当性証明を！ ALogを活用して「内部統制監査」を自動化（1/2）

明治安田アセットマネジメント株式会社

明治安田アセットマネジメント株式会社様は、明治安田生命グループの中核の資産運用会社として、高いクオリティの資産運用サービスを数多く提供されている企業です。システム全体を網羅するログの統合管理を目的に、ALog ConVerterとALog EVAを導入いただきました。導入経緯や導入後の本音について、この度、 IT推進部長 竹内正彦氏 と IT推進部次長 加藤万紀子氏にお話を伺いました。

ログの統合管理とレポーティングが自動化の第一歩

―― 主に、どのようなログを管理されていますか？

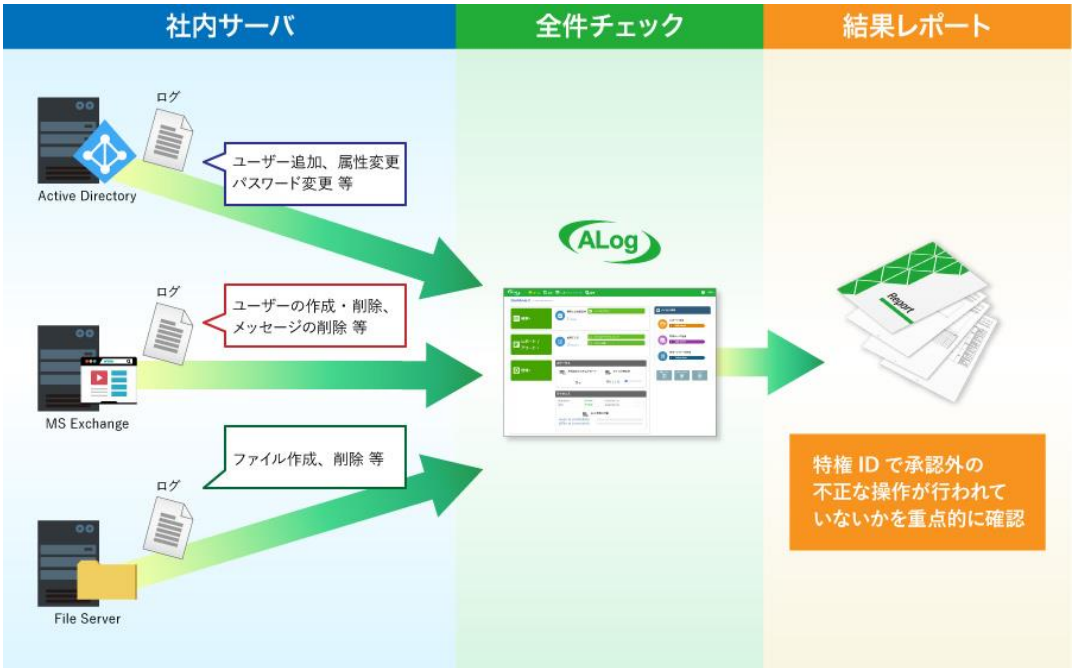
Active Directory（以下AD）、Microsoft Exchange（以下Exchange）、ファイルサーバなどのログを管理しており、一般ユーザーを含めたすべての操作ログを取得しています。特に**特権IDで承認外の不正な操作が行われていないかという点を特に重視**しています。（加藤氏）

ALog導入以前から内部統制管理としてのログ管理は実施していましたが、サイバーセキュリティ基本法の制定などがあり、企業としてこれまで以上の内部統制とログ管理を求められるようになりました。しかし、システムが出力したままの生データをチェックするこれまでのやり方では十分に対応できないため、なんらかのシステム投資をしないといけないという判断になりました。（竹内氏）

―― ログ管理ツールは数多くありますが、その中でALogを選定された理由を教えていただけますでしょうか。

ALogは、Exchangeのログを見やすくレポーティングできた唯一の製品だったからです。これまで毎日のように生のイベントログを見てきたので、条件付けして簡単にレポートを出力させることが重要だと痛感していました。（加藤氏）

ログを溜めるだけであれば他社製品でも事足りますが、レポートを作るのに手間がかかるなど、使いこなすのにも苦労しそうでした。ALogはGUIがわかりやすく直感的なので、その点も選定理由の一つです。（竹内氏）



掲載日：2020/08/04

特権管理者こそ正当性証明を！ ALogを活用して「内部統制監査」を自動化（2/2）

明治安田アセットマネジメント株式会社

内部監査目的のログ確認時間が半分に

―― ALogではどのようなレポートを作っていますか？

特権IDによる操作ログを中心にレポートを作っています。
事前に「特に注意が必要な管理者操作」を定義したうえで、定期的にレポーティングをしています。
たとえばExchangeでは、「SET」「GET」「REMOVE」「ADD」などのイベントを抽出し、**ユーザーの作成・削除、メッセージの削除**などの管理者操作を記録しています。同様に、ADサーバからも、**ユーザーの追加やパスワードの変更、属性変更**などをレポートし、承認外の管理者操作がないか？ といった自己正当性の証明として活用しています。（加藤氏）

―― ALog導入により、ログ管理はどのように効率化されましたか？

以前までは、一部のみを抽出する「サンプリング方式」でチェックしていました。それでも、生ログは量が膨大なので、証跡のログの印刷や承認証跡と照合チェックする手間が大変でした。
加えて、「サンプリング方式では（すべてのログをチェックしていないため）不十分ではないか？」という問題意識もありましたね。（竹内氏）

ALogは一度条件を設定してしまえば、一定の品質のレポートが定期的に自動出力されます。以前は1～2件のサンプルチェックだけでも、週に3時間程度かかっていました。今はすべてのログを対象にしても、以前の半分の時間で済むので、非常に助かっています。
また、ALogは異なるシステムのログでも、時間軸をそろえてチェックすることができます。時間外の操作はないか、承認されていない操作がないかなど、システムを横断してログをチェックする必要がある際に、とても便利です。（加藤氏）

―― ログの精度やシステムの運用管理の手間はいかがですか？

実は……あまりにシンプルで使いやすく、手離れがよかったので、かえって精度が心配になり、ログを全件チェックし検証しました。結果は満点。完璧さに驚きました。
運用フェーズのトラブルもほとんどありません。ALogはSQL Serverのようなデータベースを使っていません。そのため、連携製品由来のトラブルもなく、またバッチ処理の失敗頻度が非常に少ないです。従来、ログ保管作業に関して度重なるトラブルに悩まされていたことが嘘のようです。非常に満足しています。（加藤氏）

IT推進部長　竹内正彦氏

IT推進部次長・加藤万紀子氏

明治安田アセットマネジメント株式会社

設立年月日： 1986年11月
事業内容： 投資運用業、投資助言・代理業、第二種金融商品取引業
所在地： 〒105-0001 東京都港区虎ノ門3丁目4番7号虎ノ門36森ビル
URL： https://www.myam.co.jp/

掲載日：2015/04/02

ALog+Resource Athleteで ファイルサーバの可視化を実現！

ALog ConVerter for EMC, Resource Athlete

株式会社SBI証券

SBI証券様は、SBIグループにおいて「金融サービス事業」の中核を担うオンライン総合証券です。今回はALog ConVerter for EMCとResource Athleteをご導入頂いた背景について伺いました。

導入の決め手は メイド・イン・ジャパンの信頼感

昨今のコンプライアンス対応で、ファイルサーバに格納されている重要情報や個人情報に対するログの取得が要件として挙がっており、監査でもそれを指摘されていました。
それまではログの管理やチェックがとても非効率でしたので、サーバのリプレイスにあわせて、ALogを導入しました。導入に際して海外製品も候補に**挙がっていましたが、純国産製品でシェアN0.1であること、EMCの実績が豊富であること、そして何よりエージェントレスなので、ストレージソフトウェアに対する影響を心配する必要がないという点に魅力を感じ、ALogに決めました。**

ユーザー部門でも 検索システムを活用

-- ALog を採用して良かった点はどこでしょう？
アクセスログ検索システムのインターフェイスが直観的で非常に使い易いです。 対象のファイルや操作内容を絞っての検索が簡単に出来るので、定期的なレポート出力に加え、各部門からの要望に応じてその都度必要なレポートを作成したり、意欲的な部門には検索システムのアカウントを発行して、自由にログを検索してもらったり、幅広く使っています。一番多いのは、紛失したファイルや、重要ファイルへのアクセス履歴に関するレポートです。
ファイルの操作履歴がALogで追えるようになったことで、ファイルが紛失した際の捜索や原因分析も簡単になり、システム管理部の負荷軽減にもつながっています。

同じメーカーの製品だから、 組み合わせるとさらに便利に

-- Resource Athleteの活用例も教えていただけますか？
ファイルリソースの可視化のために使っています。今までは、ファイルサーバのどの共有フォルダにどれだけのデータが入っているのかなどが全く見えていなかったので、Resource Athleteで可視化できて非常に便利になりました。
他社の製品も比較検討しましたが、ALogと同じメーカーという点でResource Athlete に決めました。まだ実践できていませんが、**ALogとResource Athleteを組み合わせて、フォルダーアクセス権の変更履歴をより詳細に把握したいと思っています。「いつ誰が変更したか」をALogで「どこをどう変更したか」をResource Athleteで確認する予定です。**
また、当社では年に一回共有フォルダーの棚卸が必要なので、今後は「共有フォルダーの一覧」「フォルダーへのアクセス権一覧」「使われていないアカウント一覧」などをレポーティングして、棚卸に活用して行きます。

--今度はぜひ棚卸のレポーティングについて詳しく取材させてください！本日は貴重なお話を有り難うございました。

システム管理部
課長代理
宗像 大 様

株式会社SBI証券

本社：東京都港区六本木1-6-1
代表者：髙村　正人
設立：1999年10月
資本金：479億3,792万円
事業内容：金融サービス事業
URL：https://www.sbisec.co.jp/

掲載日：2018/08/01

働き方改革関連法への対応
ALog WorkTimeで約2,100名の
労働時間を客観的に把握

資源に変えるチカラ、自然に還すチカラ。
21 DINS 大栄環境グループ

大栄環境株式会社

□業種

リサイクル環境事業

□従業員数

2,160人（2019年度）

□ご担当者

経営管理本部 システム部
部長 兼 システム3課長 阿部 隆義 様
次長 兼 システム1課長 高田 裕士 様
システム1課 チームリーダー 藤沢 大介 様

課題

- 社員数が多く勤怠管理の確認を手動でするのは非現実的
- PCログを取得していたが、PCを共有で利用しているため、ユーザーが特定できない
- 既存勤怠システムへの後続連携が柔軟にできない

解決

- 勤怠表を自動作成/連携
  勤怠時刻に差異があるものなどポイントのみの確認に
- ADサーバよりログを取得
  ユーザー指名やグループ情報の取得で簡単に特定
- ファイル形式を任意で選択。
  csvファイルで後続処理を簡単に。

働き方改革関連法で「客観的方法による労働時間把握」が義務化

- ALogシリーズを導入したきっかけを教えてください。

働き方改革関連法により、「客観的方法による労働時間把握」が義務化されました。これを受けて今回、労務管理の強化を図りました。その一つとして、PCログを取得し、勤怠情報と突合することで客観的に勤怠実態を把握する方法を検討しました。弊社では既にPCログを取得する資産管理ツールは利用していたのですが、こちらのツールですと、1台のPCで複数社員が作業をする際のログオン/ログオフログが取れませんでした。そこでこの問題を解決できたのがALogです。ALogはADサーバ上からログを取得するため、1台のPCからでも複数社員それぞれのログオン/ログオフログの出力が可能になりました。

ALogでPCのログオン/ログオフを取得・勤怠システムと連携

- どのようなシステムになってるのでしょうか？

ALog WorkTimeのログをCSVで出力し、後続の勤怠システムに取り込んでいます。取り込んだログと実際の勤怠データとの差異を見える化したり、差異があるものはアラートをあげたりして、その理由を記入するという運用フローになっています。ALogは、出力するCSVのフォーマットを柔軟に定義できたため、勤怠システムとの連携がスムーズにできました。

- 実際に利用されてみてどうでしょうか？

今回、大栄環境グループ全体の約2,100名の社員を対象に実施しています。約 2,100名の社員の勤怠情報とログを人力で確認するのは現実的ではありませんので、ALogで作業の自動化ができてよかったです。また、社員はログを取られていることを認識しているため、「通常時間内に、もしくは残業申請した時間内に仕事を終わらせる」という意識改革にも繋がっています。

ファイルサーバのアクセスログも視野に

- 今後の展望があれば教えてください。

今回、ALogはPCのログオン/ログオフ取得をするために導入しました。今後はセキュリティ強化という観点から、ファイルサーバのアクセスログ、その他システムログの取得・運用も検討していきたいです。

掲載日：2021/08/04

資料をメールで受け取る ≫

社会インフラ事業者としての責任
お客様情報にも「安全・安心」を第一に
(1/2)

ISG,Inc.

アイエスジー株式会社

◆ 事業内容

エネルギー事業
住宅リフォーム事業
環境事業

◆ 従業員数

402名（2021年2月28日現在）

◆ ご担当者

デジタルと人の調和推進室　室長　田村様、堀様

課題	効果
■有事の際、システムから出てくる生ログを遡るのが大変	■ALog の分析変換技術で、ログを自動変換して見やすくした
■ゼロトラストをベースにしたセキュリティ対策のためにログを活用したい	■システムの異常を察知できる ALog を導入し、高セキュリティ化を図った
■情シス初心者が管理するので難しい画面は不安	■初心者でも使いやすい画面設定のおかげで運用管理を簡略化

社会インフラ事業者としての責任
お客様情報にも「安全・安心」を第一に
(2/2)

「安全・安心」を第一に。高セキュリティ化を図る

-- ALogシリーズを導入したきっかけは？

近年、サイバー攻撃が増加している中、インフラ事業者は特にターゲットにされやすい傾向にあり、更なる対策をしなければならない状況になってきました。
当社は主にインフラ事業を行っているため、常に安定稼働をし続けなければなりませんし、尚且つお客様情報の「安全・安心」も第一に考える必要があります。そこで、今流行りのゼロトラストをベースとしたセキュリティ対策の導入を進めています。例えば、クラウドを最優先としたシステム基盤の導入、シングルサインオンによる認証基盤の統合管理などです。
これらを導入していく中でシステムの異常にいち早く気付くためには、ログを有効活用することが必須なので、ログ管理ツールを導入しようという流れになりました。製品について色々調べていたのですがどこも価格が高く、且つ機能も沢山付いていて難しいイメージでした……。そんな中でも、ALogは求めていた機能が搭載されていて且つわかりやすく、コスト面についてもかなり抑えられることがわかり、導入へ至りました。

インタビューに答えてくださった堀氏

情シス初心者でも使いやすい画面設定で管理が容易

-- ログ管理ツールに求めていたポイントは？

3点ありまして、まずは、ログを変換できることです。システムから出てくる生のログだと内容がわからないので、ALogの分析変換技術で、ログをわかりやすく変換できるところが良かったです。
2点目は、データの長期保管を可能にすることです。現在利用しているクラウドシステムだと、ログの保存期間が決まっていて、期限がくると消えてしまうからです。
3点目は、webコンソール画面を直感的に操作できるところです。網屋のハンズオンセミナーに事前参加して、初心者でもマニュアルをみながら触ることができる管理画面だとわかりましたし、サポート体制がしっかりしていてよかったと思いました。

-- 実際に利用した感想は？

運用上、特権アカウントとしてログインする端末を限定しているため、それ以外の端末での特権昇格があればアラートが出るよう設定しています。
また、サイバー攻撃手法は次から次へと新しい攻撃が生み出されてますので、ログ管理は日々の運用の中でレポートとアラート設定をアップグレードしていくものだと考えています。
しかし、膨大なアラートが上がってきても毎日チェックすることは現実的ではありません。ですから、本当にチェックしなければならないアラートや、レポートが作成できるようチューニングが必要になってきます。
したがって、マニュアルを見なくても感覚的に操作できるところが大変ありがたいです。

CSIRTの設置でログ活用の重要性を実感

-- 今後の展望や網屋への要望は？

アラート設定の精度を上げて、作業の自動化、効率化を図っていきたいです。また、クラウド上のサーバログ・基幹システムのログも取得し、ログの取得対象を拡大していく予定です。
重要な情報の管理をさらに強化していきたいと考えています。
冒頭でもお話した通り、サイバー攻撃の件数が増加していることもあり、更なるセキュリティの強化が必要ということで、CSIRT（シーサート）も立ち上げました。その中でもログ活用を進めていきたいと考えています。
最後に、弊社はエネルギーを提供する企業でありますから、事業における「安全・安心」だけではなく、お客様情報においても「安全・安心」となるよう経営陣のバックアップのもと、全社的にセキュリティ対策を進めて参ります。

掲載日：2022/02/10

資料をメールで受け取る ≫

“事業継続”の観点で、セキュリティ体制を強化
【松屋】ALog＋運用サービス導入で攻撃に備える
(1/3)

MATSUYA FOODS HOLDINGS

株式会社
松屋フーズホールディングス

◆ 事業内容

飲食事業を中心とするグループ会社の経営管理

◆ 従業員数

1,580名　2021年（令和3年）3月期・連結

◆ ご担当者

ITソリューション部 IT企画グループ

グループマネージャー	佐藤 篤史 様
マネージャー	水口 直之 様
マネージャー	小髙 友裕 様

課題	効果
■攻撃 / 侵入を早期に発見、対処できる体制を整えたい	■ログから、不正や危険を検知できるようになった
■トラブル発生時、原因特定にとにかく時間がかかる	■ログの統合管理により、原因特定がスピーディーになった
■ログモニタリングを強化したいが人手もスキルも足りない	■高度なスキルを要する、ログ運用をプロに委託できた

“事業継続”の観点で、セキュリティ体制を強化 【松屋】ALog＋運用サービス導入で攻撃に備える (2/3)

事業継続のために、リスクをいかに軽減するか？侵入を前提にしたセキュリティ対策

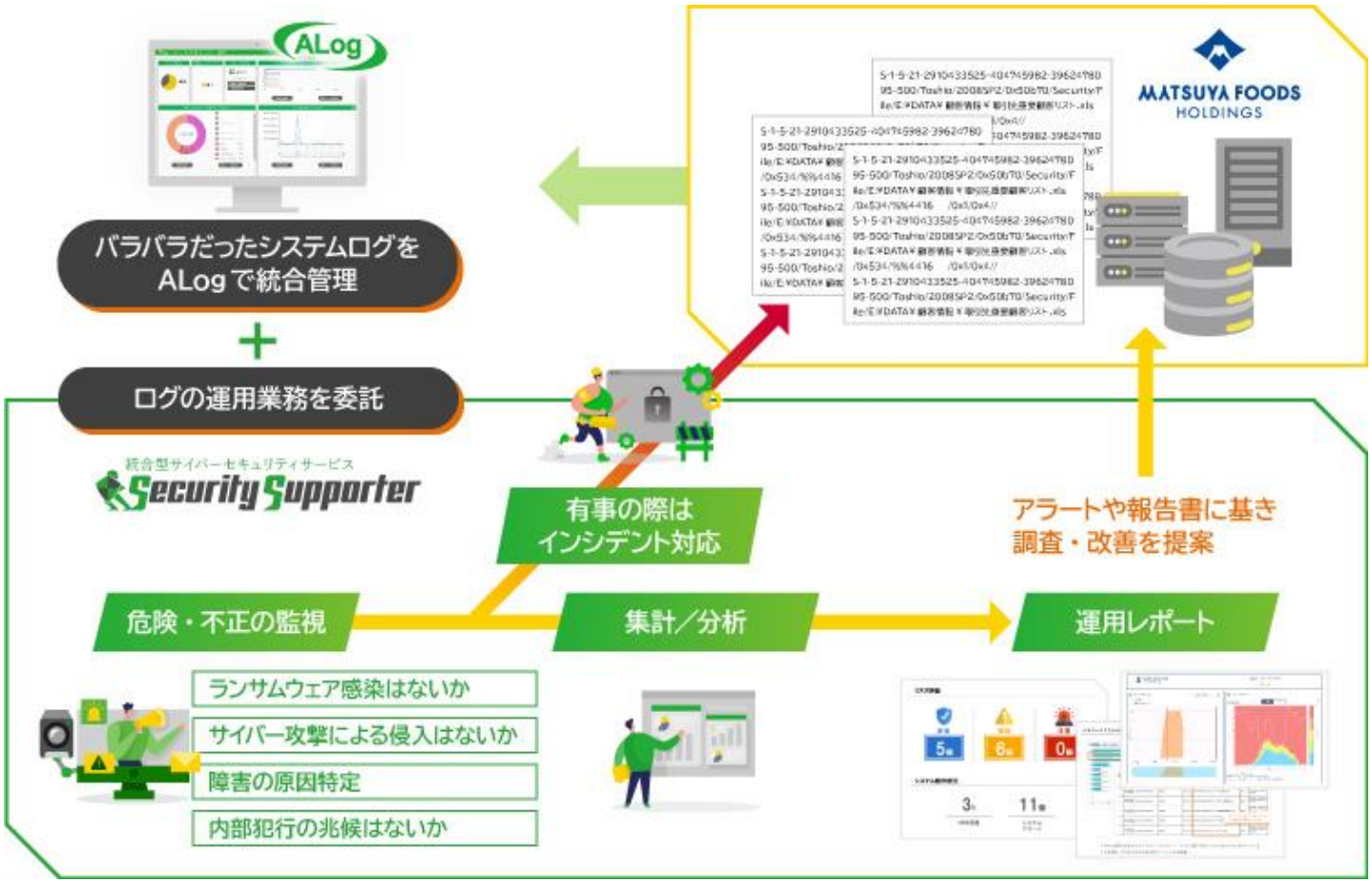
-- なぜ、セキュリティを強化？

全国各地にお店を構える当社にとって、一番のリスクは店舗システムが止まること。万が一マルウェア感染でもして、それが広まるような事態となれば、店舗営業がストップしてしまい、一大事です。そのため、これまでもアンチウイルスソフトやUTMなど、サイバー攻撃から身を守るためのセキュリティ製品は一通り導入してきました。しかし、どれだけセキュリティ対策を講じたとしても、被害を受ける可能性をゼロにすることは決してできません。侵入されることを前提にした対策作りも必要なのです。 そこで、“事業継続”という観点から、改めてセキュリティ対策について考えてみました。ポイントは2つ。一つ目は、攻撃されたとしても事業継続を脅かすような事態となる前に発見し対処できること。二つ目は、攻撃が成功し万が一被害が出てしまったとしても、ダメージを最小限にするために、迅速に原因分析し復旧出来る状態にあること。この2点を叶える為に、必要と判断したのが『ALog』と『Security Supporter』でした。

統合ログ管理＋運用業務の委託で、攻撃検知とスピーディーな原因特定・対処が可能に

-- 実際に導入してみていかがですか？

『ALog』の導入により、**インシデント発生時の原因特定が、とにかくスピーディーになりました。**システム毎にバラバラに保管されていたログが集約されたので、ここから一貫して事象を確認できるようになったためです。
また、**ALog導入に付随してログ運用業務まで委託できた事もとても大きなメリットでした。**ログ運用には、大前提として複数のシステムが出力するログの意味を理解し、かつそこから状況把握まで出来る体制を整える必要があります。
加えて今回の目的である、ログを活用した外部攻撃の検知まで実現するには、多様な攻撃手法を理解し、事前に適切なアラート/レポート設定を施す必要があります。とはいえ、当社の人員体制を鑑みるに、ここまで内製で行うのは若干ハードルが高いと感じていました。なので『Security Supporter』で、この部分をプロにお任せ出来た事は、非常に有難かったです。



“事業継続”の観点で、セキュリティ体制を強化 【松屋】ALog＋運用サービス導入で攻撃に備える (3/3)

-- 『Security Supporter』の報告レポートはどんな感じですか？

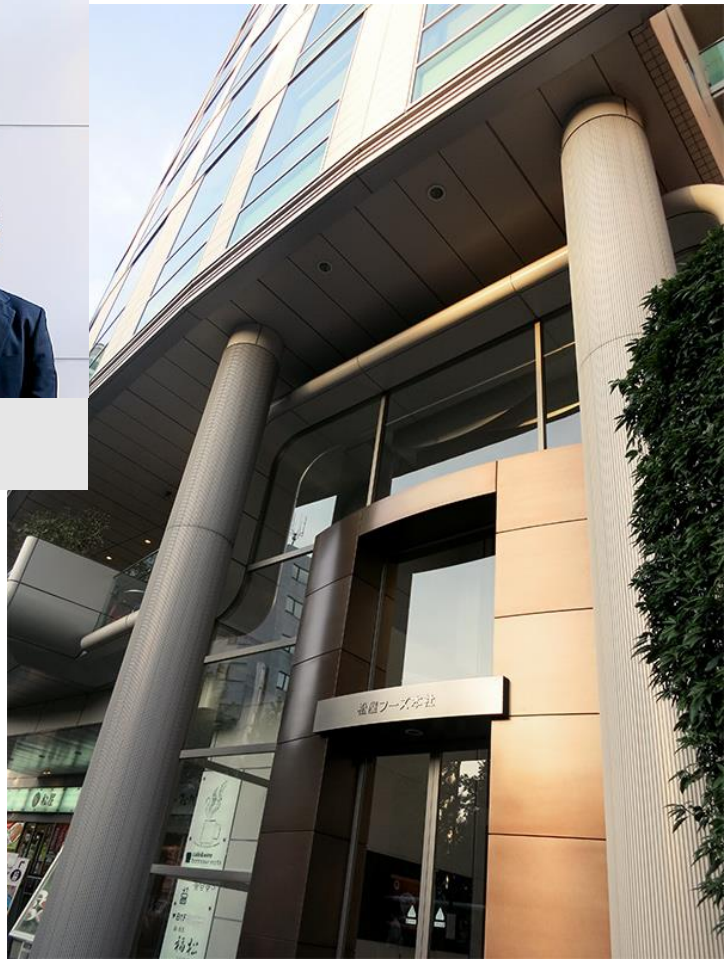
サービス契約後、すぐに大量のシステムエラーが上がっているとの報告をうけました。どうやら、過去に利用していたシステムアカウントによる認証失敗が出ていたようです。お陰様で適切な設定に修正することができました。
その他には、幸いにもこれまで、重大なインシデント発生報告がなくこれといってご紹介できるケースがないのですが…。しいて上げるとしたら、UTMからランサムウェア感染のブロックログが出ているとの報告が2件ほどあったことくらいでしょうか。きちんとブロックされていることを確認できその点では安心でしたが、ログを深堀調査し、該当端末の使用者を特定、念のため本人にヒアリングを行いました。すると、2名ともまったく自覚がなく、この感染がブロックされずに発覚も遅れていたら被害は広がっていたのだろうと、恐怖を感じました。こういう**ヒヤリハットに気付けるように**なったことも、今後の対策や社員教育の強化という観点で大きな意味があると感じています。

セキュリティインシデント発生時に、慌てない体制

-- 今後の展望やご要望は？

事業継続という観点で費用対効果を考えながらセキュリティ対策を進めていきたいです。そのため、セキュリティインシデント発生を想定した、訓練などを実施できるプログラムもあればいいなと感じます。

取材協力いただいた
小髙 様　佐藤 様　水口 様



お客様の大切な個人情報を守り、ログ情報のさらなる活用も AWSのRDBを確実に監視するALog ConVerter DB

株式会社LAVA International

全国に420店舗以上を展開するホットヨガスタジオのLAVA様は、ウェルネスの分野で目覚しい成長を続ける健康サポート企業です。2019年には1号店のオープンから15周年を迎えられました。同社では個人情報を含むAmazon Web Services（AWS）上のDBを、ALog ConVerter DBで監視されています。その詳細について、経営企画部システムグループの髙橋吾郎氏にお伺いしました。

事業の生命線は お客様情報の高度な管理

―― 多くの会員様の個人情報を預かる企業として、DBのセキュリティには苦労をされたのではないですか？

個人情報保護に対する社会の要請、また会員様からの期待は年々高まっていますからね。当社は、会員様の個人情報を数多くお預かりしています。皆様に安心して当スタジオをご利用いただくためにも、セキュリティの担保は極めて重要です。
従来は、外部からのサイバーセキュリティ対策を重点的に行っていました。しかし、セキュリティをさらに高めるには、内部対策も欠かせないという認識が強まりました。その要が個人情報の含まれたDBの監視だと考えています。当時、DBを扱っていたのはシステムグループのごく限られた社員でした。信頼できるメンバーのみによる厳重な運用で問題が生じることはなかったのですが、事業の成長にともない関係者が増加し、内部対策の必要性が浮上したのです。

―― そこでALog ConVerter DBを導入されたわけですね。選定の理由は何だったのでしょう。

まず、AWSへの対応実績があったからです。以前はオンプレミスで運用していましたが、ビジネスの継続性を考慮し、数年前からリスクのより少ないクラウド（AWS）へと移行しました。
そのため、AWSのDB監視というのは必須要件でしたね。
また、費用対効果も魅力的でした。他の資産管理ツールもいくつか検討しましたが、ネットワーク内の全端末を幅広く監視するものばかりで、必要のない機能が多く盛り込まれているため、その分費用も高価でした。
その点、ALog ConVerter DBはDBの監視に特化しており、他製品と比較しても安価です。そして、とにかく使いやすいのです。SQLサーバのログは知見がないと扱いにくいものですが、ALog ConVerter DBであれば、専門的な技術がなくともログを理解できるようになります。費用対効果は抜群ですね。

株式会社LAVA International

創業： 1990年12月
事業内容： ホットヨガスタジオLAVAの運営
所在地： 〒107-0061 東京都港区北青山1-2-3 青山ビル9階
URL： https://yoga-lava.com/

セキュリティの高度化に加え、 ログ情報のさらなる活用も視野に

―― ALog ConVerter DBを実際に導入されて、どのような効果がでていますか。

まず、セキュリティレベルが向上しましたね。「誰が、いつ、どのような操作を行っていたか」。そういった操作ログを取得しているというのは、それだけで抑止力になりますし、逆に言えば、「不正をしていない」と自己の正当性を証明することもできます。
まれに会員様より「登録情報は漏洩していないか？」と安全性についてお問い合わせをいただくことがあります。そんな時もログと照らし合わせて調査すれば、より精度の高い回答ができますね。ログは「動かぬ証拠」ですから、情報が確実に守られていることを証明できて、ご納得いただけます。

―― 今後のALog ConVerter DBの活用について展望を教えてください。

ALog ConVerter DBの機能を活かして、障害対策やパフォーマンス調査など、セキュリティ以外の用途にログ活用を広げようと考えています。システムやアプリケーションに不具合があった時、実際にどのようなSQL文が実行されていたのか、よく実行されるSQL文にはどんな傾向があるのかなどの調査ができますから。
あとは、業務の効率化を強化したいですね。例えば先ほどの問い合わせに関しても、これまではシステムグループの専門家が調査を行っていました。しかしALog ConVerter DBなら、システムの専門家でなくても利用できるため、ヘルプデスク内で問題を解決することが可能です。このように属人化の解消を視野に入れて、会社全体の業務効率化がはかれたらと考えています。

インタビューに応じていただいた
経営企画部 システムグループ システムサポートチーム
チームリーダー 髙橋吾郎氏

プライバシーマークの管理策「ログ取得及び監視」をALogで自動化 (1/3)

学習に喜びと感動を
桐原書店

株式会社桐原書店

◆ 取扱商品について

文部科学省検定教科書
学習参考書・問題集
デジタル教材
小論文添削

◆ 従業員数

124名（2020年3月31日現在）

◆ ご担当者

管理局システム部 部長　柳橋 知恵子 様
管理局 システム部 システム課 係長　古閑 大徳 様

課題	効果
■プライバシーマークの管理策「ログ取得及び監視」を達成したい	■ALog が出力するレポートで定期的に不審な操作を監視
■Windows イベントログは複雑で、実際に何が起こったのかを解析するのが大変	■ALog のログ変換エンジンで、「いつ、誰が、どのファイルに、何をしたのか？」を瞬時に把握
■管理者アカウントを悪用していないことを証明したい	■管理者による操作ログで正当性を証明

プライバシーマークの管理策「ログ取得及び監視」をALogで自動化（2/3）

複雑なログをALogでわかりやすく変換

-- ALogを導入したきっかけは？

当社の主な事業は、教育出版事業です。中でもデジタル教材やオンラインの学習サービスに力を入れているのですが、サービス利用者の拡大に比例して、個人情報の取り扱いも増えてきました。お客様にサービスを安心してご利用いただくために、お預かりしている個人情報を適切に管理・運用することは、サービス提供者の責務だと考えています。当社が個人情報を適切に管理・運用していることを証明するため、プライバシーマークの取得を目指すのは当然の流れとしてありました。

プライバシーマーク取得にあたっての管理策の一つに、「ログ取得及び監視」（個人情報に係るイベントを記録し、証拠を作成する）という項目があり、これには、イベントログ取得とログ情報の保護をしていく必要がありました。
それらのログを管理するためツールを探し始めたのが、導入のきっかけです。

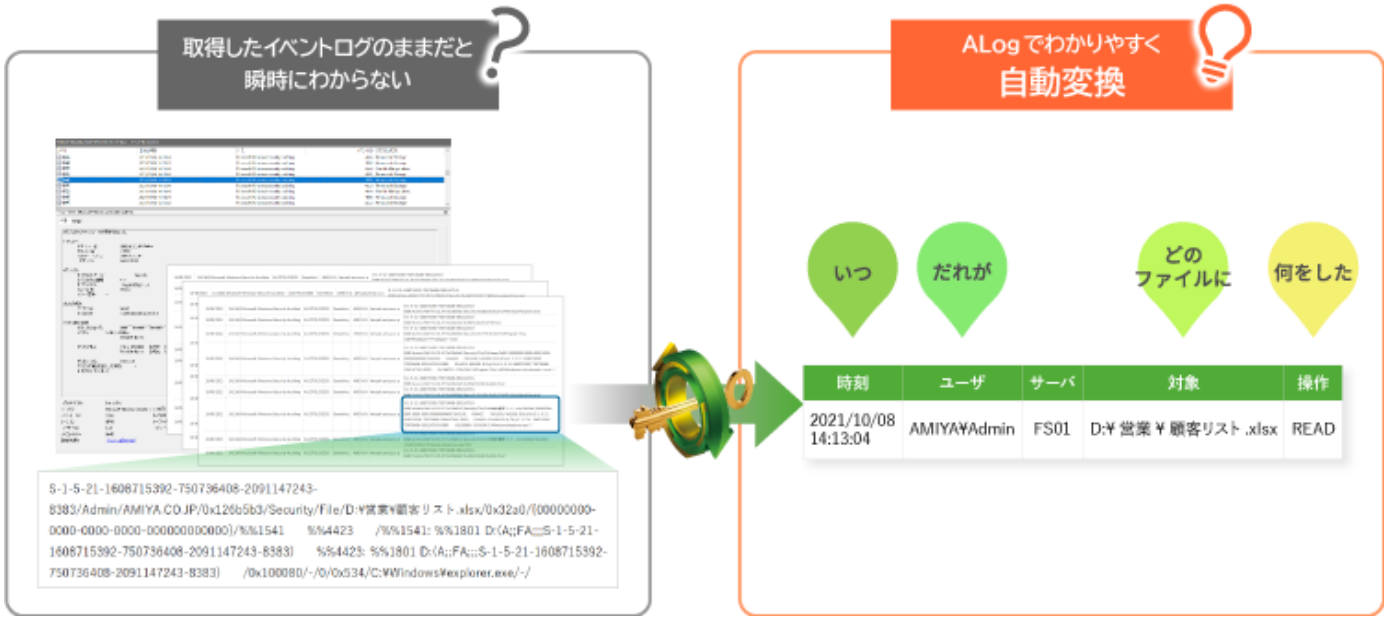
-- ALogを選んだ決め手は？

プライバシーマークの管理策「ログ取得及び監視」をクリアするためには当初、「個人情報が保管されているファイルサーバのイベントログを取得しておけばいいのだろう」と考えていました。そこで、実際にファイルを「開き」、「書き込み」「保存をする」という一連の操作を実際に行い、イベントログにどう出力されるのかを検証をしてみました。一目でわかる形でログが出ることを期待したのですが、実際には「一連の操作なのに大量のログが出力されてしまう」などかなり難解な出方で、このログからユーザー操作を速やかに把握するのは困難で、実際の運用として現実的ではないと判断しました。

ALogにはログ変換エンジンが搭載されていて、先程のイベントログを人の操作通りに変換してくれます。「いつ、誰が、どのファイルに、何をしたのか？」という形式で表示されるので、解析にかかる作業を省略することができます。

さらに、どんなに万全な体制を整えたとしても日々新たな脅威が生まれ、変化していく現在の状況では、外部からの不正アクセス等による情報流出の危険性について考えざるを得ません。また、万一そのような事態に陥ってしまった場合、どの情報が、どの段階で流出してしまったのかを特定する必要もあります。この時、状況を可能な限り早く把握することが重要と考えますが、ALogなら瞬時に実施することもできます。

これらの点に加えて、グループ運用という観点や親会社での利用実績もあることから、ALogを導入する運びとなりました。



プライバシーマークの管理策「ログ取得及び監視」をALogで自動化（3/3）

ログ取得及び監査の役目を果たすALog

-- 実際にALogを導入した後の活用方法について教えてください。

プライバシーマーク取得の要件である、「ログ取得及び監査」のワークフローにALogを盛り込んでいます。 具体的には、お預かりしている個人情報に対して、「いつ」、「誰が」、「何をしたか」の全てのアクセスを対象に、自動レポートを作成し、不審なアクセスがないかの監視をしています。

また、メンテナンスや問合せ対応時に 横断的なデータアクセスを行うような、システム管理者などの高権限を持つアカウントが悪用されず、適正に運用されていることを示すためにも役立っています。

-- 今後の展望について教えてください。

今後は、不正アクセスの予兆監視に活用したいです。例えば、「本来、顧客情報にアクセスする必要のないユーザーからのアクセス」や「普段とは違うルート（指定ツール以外のコマンド操作など）でのアクセス」、「アクセス自体の増減」など、いつもと違う動きを把握できれば、インシデントとなる前に止められるのではないかと考えています。なので、ALogを色々設定してみようと思います。効果的な使用方法があれば教えてください。

取材を受けてくださった
柳橋様・古閑様

デジタルエンタメ業界のログ調査業務を ALogが6時間から0時間に短縮 (1/2)

mixi GROUP

株式会社ミクシィ

◆ 事業内容

デジタルエンターテインメント
スポーツ
ライフスタイル

◆ 従業員数

1,168名（連結・正社員のみ）（2021年3月末現在）

◆ ご担当者

はたらく環境推進本部　社内IT室
リーダー　佐藤 隆行様
　　高柳 博紀様

課題

■今の環境ではログ調査に
“非現実的な時間” が必要と判明

■ログ管理製品は不必要な機能が多く高価

■実際の運用は IT 部門ではなく監査部門
(IT に詳しくなくても利用できる必要性あり)

効果

■圧倒的に時間短縮
(6 時間のログ調査が 0 時間に)

■求めていた機能と価格がベストマッチ

■直感的に操作できる UI だから
監査部門にもスムーズに導入

デジタルエンタメ業界のログ調査業務をALogが6時間から0時間に短縮（2/2）

-- ALogシリーズを導入したきっかけは？

情報漏洩が発生したと仮定して社内でシミュレーションしたのがきっかけです。もし標的型攻撃によりファイルが流出した場合、乗っ取られたアカウントがどのファイルにアクセスしたのかを調査し、流出したファイルを特定する必要があります。そこでファイルサーバのイベントログから特定アカウントがアクセスしたファイルをピックアップしてみたのですが、たった4時間分のログ調査に6時間かかってしまいました。当時で2億個くらいのファイルがあったと記憶してます。これが実際のサイバー攻撃だった場合、4時間分のログだけでは足りず、1週間分調査しないといけないかもしれません。これは現実的ではないなと思いました。そこで、イベントログを実際のファイルアクセス通りに整形してくれるツールを導入しようという流れになりました。

取材協力いただいた
高柳様・佐藤様

-- ログ管理ツールに求めていたポイントは？

求めていたポイントは、先ほどの通り、イベントログを実際のファイルアクセス通りに整形をしてくれるツールです。他のツールも検討したのですが、どのツールも他にたくさんの機能がついていて、セットで高いものばかりで。なので、ALogが我々にはマッチしました。

-- 実際に利用した感想は？

ALogはイベントログが自動変換され、実際のファイルアクセス通りのログが出力、保管されます。「誰がいつどのファイルにアクセスしたのか」と。そのため、イベントログを使ったシミュレーションではログ調査に6時間必要でしたが、ALogでは特定アカウント名を入力して検索するだけでそのアカウントがアクセスしたファイルが一瞬でわかります。つまり6時間が“ゼロ時間”になりました。これで、もしサイバー攻撃を受けたとしても、迅速に対応できる環境となりました。

他にも導入してみて気づいたのですが、ALogはITに詳しくない人でも操作できるようにデザインされているなと感じました。当社では、日々の運用は監査チームが行っていますが、ALogを導入し、監査担当者に1度ALogの使い方を教えてからは、今のところ使い方について質問が来てません。他のツールだと結構質問があるので、ALogはITに詳しくなくても簡単に扱えてるかなと思います。

イベントログのままだと、
4時間分のログ調査で6時間必要

ALogなら、“0”時間で調査完了

-- 今後の展望や網屋への要望は？

今、180TBぐらいのファイルがあるのですが、年々増えているのが悩みです。そこで、ALogシリーズのResource Athleteを導入して、何年も使っていない不要なファイルを可視化・削除し、ファイルサーバの容量を増やさないようにしたいです。