ゼロトラスト強化なら国産SIE「LogStare」Soliton OneGate連携で認証ログの“気づき”を自動化

目次

サイバー攻撃の手口は年々巧妙さを増しており、重要な情報の流出に関するニュースも後を絶ちません。そのため、企業や組織、個人を問わず、ネットワーク分離や認証など、さまざまな手段を用いて、外部からの侵入や情報漏えいを防ぐことが求められています。

ただし、どれだけ対策を施しても、攻撃者はあの手この手で侵入を試みます。だからこそ、仮に侵入された場合、ネットワーク内で何が起きているのか、セキュリティ対策はどう機能するのか――そういったことが気になる方もいらっしゃるのではないでしょうか。

そこで力を発揮するのが、株式会社LogStareが提供するログ収集・可視化ソリューション「LogStare」です。

国産SIEMとしてゼロトラスト強化を支える「LogStare」は、株式会社ソリトンシステムズ（以下、ソリトン）が提供する多要素認証クラウドサービス「Soliton OneGate」（以下、OneGate）との連携によって、その認証ログを受け取り、自動で分析・可視化。これにより、異常な挙動をリアルタイムで検知したり、アラート通知を自動で行ったりするなど、セキュリティ対応の迅速化と運用の効率化を実現します（図1）。

このように「LogStare」は、セキュリティ運用を支える強力な基盤となりますが、そもそも「ログ」とはどのようなもので、なぜ重要なのでしょうか。

ログとは、ITシステムやネットワーク上で発生した操作や出来事を時系列で記録する「履歴データ」のことです。「誰が・いつ・どこから・何をしたか」が明らかになるため、トラブルやインシデント発生時には“原因の可視化”や“迅速な対処”につながる、セキュリティ運用の土台ともいえる存在です。

そこで今回は、株式会社LogStare 取締役COO兼CTOの堀野友之氏に、ログ監視の重要性やその活用方法について、詳しく伺いました。

ログの蓄積と分析でできることはセキュリティ以外にも

「ログ」と一言で言っても、記録される対象や場所はさまざまです。

たとえば、誰でも閲覧可能なウェブサイトにはアクセスログが存在し、閲覧者のIPアドレスやアクセス日時、サイト内での行動履歴などが記録されます。

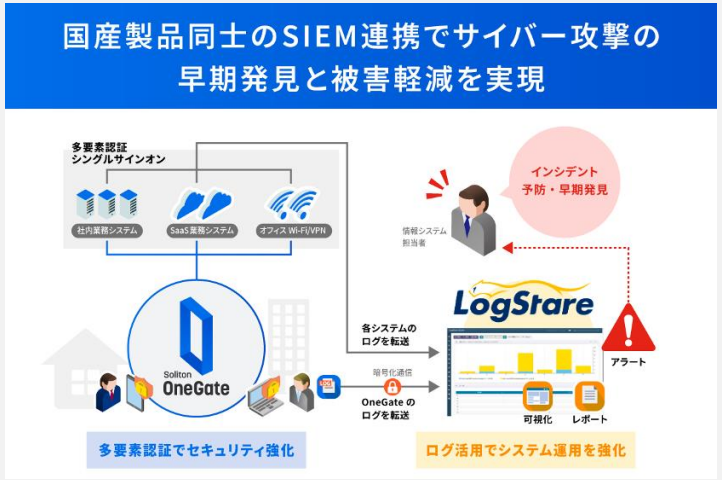
ビジネスの現場で特に重要なログのひとつが、社内ネットワークやクラウドソリューションにおける記録です。

ウェブサイトのアクセスログと同様に、誰がいつアカウント認証を試みたのか、それが成功したのか失敗したのかといった情報が記録されます。もちろん、認証ソリューションである「OneGate」においても、こうしたログは蓄積されています。

こうして見ていくと、ログは単なる記録にとどまらず、セキュリティにおいて極めて重要な役割を果たすことがわかります。たとえば、本来の就業時間とは異なる深夜に、同じユーザーが何度もアクセスを試みていたとしたら、不審な動きとして注目すべきでしょう。

こうしたログ環境の中で「LogStare」はどのようにセキュリティ対策を実現しているのでしょうか。

【図1】



【図2】

この点について、堀野氏に詳しく伺いました。

“まず、ログは蓄積してこそ意味があります。

「LogStare」を導入すれば、ログをきちんと蓄積し、必要なデータをいつでも取り出せるようになります。これが「LogStare」で実現できる基本的なポイントのひとつです。ただ、ここまでお話しした内容だけでは「それは当たり前のことでは？」と感じる方もいらっしゃるかもしれません。

では「LogStare」を使わずにログを記録している企業では、どのような方法でログを残しているのでしょうか。

中には、CSVファイルでログを蓄積しているケースもあるかと思います。そうした場合、記録そのものはテキストの羅列にすぎず、見やすい形に加工するには一定の手間がかかってしまいます。実際、ログを取得していても「手動での集計が面倒」「気づきにつながらない」といった悩みは少なくありません。「LogStare」を導入すれば、ログの自動整理・可視化により、“見る・気づく・対応する”までの一連の流れを効率化できます（図2）。

「LogStare」は、ユーザーがアクセスした時間や場所など、さまざまなログ情報を可視化できます。

たとえば、あるユーザーが何度もログインに失敗しているという状況があれば、メールアドレスの流出や不正アクセス試行の兆候として、いち早く気づくことができます。

また「LogStare」には、こうした不審なアクセスがあった際にアラートを発する機能も備わっており、異常の早期発見につながります。

ここまでに挙げた点は、情報システム担当者にとってセキュリティの観点から非常に重要なものばかりですが「LogStare」を導入することで得られる効果は、それだけにとどまりません。

たとえば、先ほどの“あるユーザーが何度もログインに失敗している状況”が、“就業時間外のアクセス”となっていて、それについて詳しく調べた結果、真正なユーザーによるものであれば、働き過ぎの兆候を察知できる可能性があります。

さらに、同じく真正なユーザーによる業務とは無関係なウェブサイトや、危険なサイトへのアクセス状況も把握できるため、人事的な観点や生産性向上といった側面でも、ログは有効に活用できるのです。”

LogStareによって守られた教育機関の情報

不審なアクセスや認証の異常は、気づいたときには被害がすでに拡大していることも少なくありません。しかし「LogStare」が“手遅れになる前”に、リスクを発見した事例もあります。

現代のビジネスにおいて、あらゆる企業がITネットワークを活用する中「LogStare」は情報・通信業や製造業、医療機関、金融機関など、幅広い業種で活用されています。

中でも特に高く評価されているのが、官公庁や教育機関での導入です。大学などの教育機関では、企業以上に多様な利用環境への対応が求められます。学生と教職員を合わせると膨大な数のユーザーが存在し、それぞれが場所を問わず快適にネットワークへアクセスできる環境が必要です。教育機関のネットワークには、外部からの防御を強化しながらも、ユーザーにとってはスムーズに利用できる環境が求められるのです。

そうした複雑な要件を抱える中で「LogStare」が、ユーザーと組織を守った実例について、堀野氏は語ってくれました。

“不正アクセスの兆候は、日常の中でふとしたログから見つかることもあります。ある大学で「LogStare」を使ってログを監視していたところ、特定のユーザーがさまざまな国からログインを試みており、中には成功しかけていたケースもありました。

すぐにアカウントを停止し、大学側が調査を行った結果、その学生の名前とメールアドレスがダークウェブに流出していたことが判明したのです。こうした出来事を受けて、この大学では多要素認証の導入を検討しています。

「LogStare」と「OneGate」の連携が、いかに有効かをご理解いただける事例ではないかと思います。”

ログを前に、情報システム担当者が最初にすべきこととは？

企業や組織におけるネットワーク構築やセキュリティ体制には、さまざまな事情があります。中には、十分な人的リソースを割けない現場もあるでしょう。

とくに、定員が決まっている行政機関などでは、ひとりの担当者が全体のシステムを管理しなければならないケースも少なくありません。

堀野氏に話を聞くと、こういったケースでも「LogStare」でのログの監視は、決して難しくないそうです。

“「LogStare」で蓄積したログのレポートは「見る人に依存させない」ことが特長です。

どういうことかというと「LogStare」のレポートを見るために特別なスキルや知識を身につける必要がなく、誰が見ても判断しやすい内容になっているということです。例えば、ある自治体で「OneGate」のログを「LogStare」で記録・分析していたとします。運用を続けていくうちに、日本以外からのアクセスは基本的に発生しないといった傾向が見えてきます。

そして、担当者が異動し、新しい担当者に引き継ぐ際には「日本以外からのアクセスに注意」といった“見るべきポイント”を簡潔に伝えやすい。そういった継続性のある運用ができる点も「LogStare」の強みです。”

このような運用ができれば、少人数体制でシステムを維持しながらも、本来注力すべき業務に時間とリソースを割けるようになるはずです。

一方で「OneGate」ユーザーが「LogStare」を活用したいと考えたとき、まず何から始めるべきなのでしょうか。

両製品の連携が始まった今、堀野氏はその第一歩について次のように語ります。

“冒頭でも少し触れましたが、まずはログの蓄積を始めることが大切です。

当たり前のように思えるかもしれませんが、実際にはログを貯めるという意識自体がない企業も少なくありません。ログが蓄積されていなければ、そもそも分析ができませんので、まずは「ログを取る」ことから始めていただきたいですね。

また、すでにログを取得している場合は、自社でどのようなシステムやアプリケーション、デバイスを使っているかをあらためて棚卸しすることで、より効果的な分析につながると思います。”

セキュリティソリューションの運用には、並行してログを記録すると非常に効果的だとわかります。

まとめ

セキュリティ製品は“入れて終わり”ではなく、日々の運用の中でどう使いこなすかが重要です。

そういった意味で「LogStare」は単なるツールではなく、現場に「気づき」と「判断力」をもたらすパートナーとも言えます。

「LogStare」という社名や製品名から、海外企業ではと思われる方もいるかもしれませんが、東証グロース市場に上場するセキュアヴェイルのグループ企業であり、純国産のセキュリティソリューションを提供する日本企業です。

ソリトンとのパートナーシップについて、堀野氏は次のように語ります。

“ソリトンもLogStareも、ともに日本のセキュリティメーカーです。私たちは『日本のセキュリティは日本企業が守る』という意識を強く持っており、ソリトンとともに、高いレベルで使いやすいソリューションを提供していきたいと考えています。また、今後は「OneGate」以外のソリトン製品とも連携を進めていきたいですね。”

2025年3月、日本政府は国産のセキュリティソフトウェアを優先的に調達する方針を打ち出しました。国産のセキュリティ技術を強化することが、その狙いです。ソリトンとLogStareは、日本の企業・行政・社会全体を守るため、より高品質で信頼性の高いセキュリティの実現を目指して進化を続けていきます。

ゼロトラストやクラウド活用が進むいま、セキュリティ運用の鍵を握るのは「認証ログの活用」です。まずは「OneGate」との連携によって得られる「LogStare」の“気づき”を、自社の現場でもぜひ体感してみてください。

ログを味方につけることが、ゼロトラストを支える第一歩になります。

株式会社LogStare

ご購入に関するご質問、デモ依頼、お見積りなど、お気軽にお問い合わせください。

よくある質問とその回答をまとめたFAQもご活用ください。

https://www.logstare.com/contact/

ネットアテスト

「ネットアテスト」は、企業ネットワークに関わる全ての方のためのサイトです。安心・安全な環境を実現したい情報システム担当者様、確かなシステムを提案されたいインテグレータ様に向けて、運用の効率化やセキュリティ強化の方法などをお届けしていきます。

サイトはこちら