MylogStar

RUNEXY®
Run in the Next!

セキュリティ

導入事例
CASE STUDY

VMware Horizon 環境でも操作ログを確実に取得して統合ログ管理による証跡の一元管理を実現

ダイレクト型損害保険のプライスリーダーとして知られるSBI損害保険株式会社。同社は、IT統制に関する監査への対応とマルウェア対策の強化を目指し、VDI環境においてさまざまな操作ログを確実に収集できるラネクシーのクライアント操作ログ管理ソフトウェア「MylogStar」を導入。統合ログ管理システム「Logstorage」と併用することで、監査対応が可能な環境を整備し、セキュリティを強化するとともに、収集したログを労務管理に活用している。今後は、ユーザー操作ログを分析することで、業務改善や効率化を図っていく方針だ。

SBI GROUP SBI損保

所在地：東京都港区六本木1-6-1 泉ガーデンタワー
設立：2006年6月1日（SBI損保設立準備株式会社として設立）
資本の額：409億円（うち資本金205億円、資本準備金204億円）
従業員数：744名（2020年10月1日現在）
事業内容：損害保険業
URL：https://www.sbisonpo.co.jp/

導入製品・ソリューション

MylogStar

課題
金融業界におけるIT 統制に関する監査への対応と、巧妙化するマルウェア対策の強化を目指し、VMware Horizon環境でも確実に操作ログを収集・分析できる仕組みが必要だった。

解決
MylogStarおよびLogstorageの導入により、各種操作ログの確実な取得と一元管理を実現。監査対応やセキュリティ強化のみならず、労務管理にもログを活用できるようになった。

ログ管理製品でIT統制に関する監査への対応とマルウェア対策の強化を目指す

新しい保険の在り方として、「ダイレクト型損害保険」という新ジャンルにチャレンジしてきたSBI損害保険株式会社（以下「SBI損保」）。同社は「新しい時代に、新しい保険を」という企業理念のもと、最先端の商品と最高水準のサービスを提供することを目指しているが、この点について経営戦略本部 情報システム部 運用管理課の課長 竹野圭輔氏は「現在、コーポレートスローガンとして『プライスリーダーからゲームチェンジャーへ』を掲げており、保険料満足度の追求だけではなく、商品ラインアップの充実、サービスの質の向上を強く推進しています」と説明する。

さらに同社では、SBIグループの経営理念のひとつ「金融イノベーターたれ」を実践すべく、デジタルトランスフォーメーションDXを推進している。グループ共通の基本理念である「顧客中心主義」に基づき、「カスタマーエクペリエンス（CX）の拡充」を実現すべく、さまざまな取り組みを行っている。

さて同社は2019年、ログ管理製品の導入を検討することになった。その主な目的は2つで、金融業界におけるIT統制に関する監査への対応と、セキュリティ対策、中でもランサムウェアなど巧妙化するマルウェア対策の強化である。それまで同社はEDRを導入していなかったため、もしマルウェアに侵入されても、どのようなふるまいをするのか適切に把握する手段がなかった。そこで監視対象となるシステムのログを、常時かつ確実に取得できる仕組みが必要だったのである。

「どのような悪さをされたのかわからないというのは、システムのセキュリティを担う立場からしても不安です。それまで特に被害を受けたことはありませんでしたが、攻撃が日々巧妙化している現状、早急な対策が必要でした」（竹野氏）

操作ログの取得に特化した機能とVDI環境への対応を評価

SBI損保では、ログ管理製品に加えてクライアント管理製品やIT資産管理製品など、複数の候補をピックアップし慎重に比較。これらの中からラネクシーのクライアント操作ログ管理ソフトウェア「MylogStar」と統合ログ管理システム「Logstorage」を販売店であるアシストの提案で採用を決定した。

MylogStarは、取得できるログの種類が豊富で、かつ精度の高い操作ログを確実に取得できる。よって、ログから異常を検知し、状況を把握して迅速に対策を打つことが可能だ。竹野氏とともに今回の導入プロジェクトを主導したアシスタントマネージャー　加藤亮平氏は「他の候補は端末管理やIT資産管理の機能がメインだったのですが、当社ではクライアント環境をVDIに移行することが決まっていたため、そうした機能は不要でした。一方、MylogStarは操作ログの取得に特化しており、VDI環境（VMware Horizon）にも対応している点を高く評価しました」と当時を振り返る。

なおLogstorageは、IT統制の観点から特権IDのアクティビティなどアクセス制御を管理することを目的に導入している。システム開発者・運用者など特権IDを持つメンバーは、本番環境にアクセス申請をすることでログイン可能だが、Logstorageはこうしたアクセス申請とサーバへのログイン記録をマッチングすることができるため、申請のないアクセスを検知することができる。

経営戦略本部　情報システム部 運用管理課
課長　**竹野 圭輔 氏**

経営戦略本部　情報システム部 運用管理課
アシスタントマネージャー　**岡寺 雄太 氏**

経営戦略本部　情報システム部 運用管理課
アシスタントマネージャー　**加藤 亮平 氏**

すぐれたログ収集力を活かし
マルウェアのふるまい把握や労務管理に活用

同じログ管理製品であるMylogStarとLogstorageの使い分けについてSBI損保では、操作ログの取得をMylogStarで実施。LogstorageはMylogStarが集めたログを他のログと合わせて蓄積し一元管理。証跡など必要なときに対象を高速検索するのに使用している。

両製品の導入効果は、さまざまな点で発揮されているようだ。竹野氏は「以前はユーザーがメールの添付ファイルを開いたり、URLをクリックしてしまったりしても私たちは把握できませんでした。本人が開いていない、クリックしていないと言えば、それを確認する手段がなかったのです。しかしMylogStarであれば、こうした操作ログを確実に取得できます。また、EメールやWebアクセスの通信パケットを記録しているため、マルウェアが外部と通信を行った際も、すぐに把握可能です」とそのメリットを語る。

また、MylogStarの操作性の良さを評価するのが、アシスタントマネージャーの岡寺雄太氏だ。「MylogStarはとても使いやすいですね。事前にラネクシーからレクチャーを受けましたが、すぐに慣れることができました。また、導入前はVDI環境でのパフォーマンスへの影響を心配していたのですが、ラネクシーがうまくチューニングしてくれたことで、業務に影響するようなことは全くありませんでした。追加でインストールしたソフトについても、しっかりと対応いただいています」

加えて、VDI環境においてCPUの利用率が跳ね上がったときなどに、その原因が分析できるようになったという。

「例えば、画像系や地図などのWebページを操作すると影響することがわかりました。これもログを分析することで得られた新たな知見です」（岡寺氏）

このほか、テレワークの労務管理にも収集したログを活用しているという。

「昨今のコロナ禍において、当社ではコールセンターなどを除き、多くの社員がテレワークを行っていますが、従来の仕組みでは的確な労務管理は困難でした。しかし今ではクライアントの操作ログがすべて把握できるようになったことで、アクティブな時間がわかるようになりました。従業員の勤務状況の把握のため、人事からレポートの提供を求められた場合でも、ログイン・ログオフ時間以外のわかりやすい指標を提出できるようになりました」（竹野氏）

今後はユーザーの操作ログを分析することで
業務改善や効率化にも役立てる

今後、SBI損保がMylogStarおよびLogstorageをどう活用していくかについて、竹野氏は次のように展望を語る。

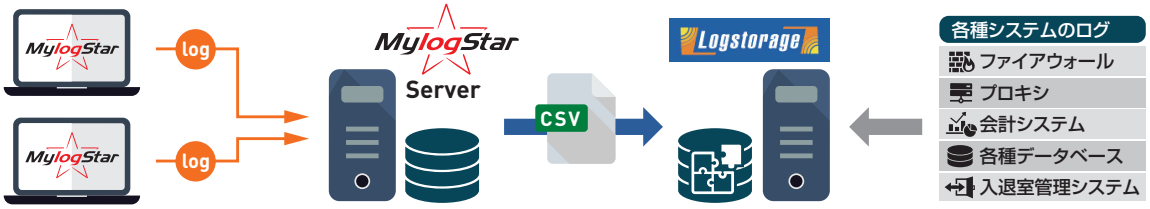
「現在はセキュリティ対策や監査対応のためにログを貯めていますが、今後は多くのユーザーの操作ログを分析することで、業務改善や効率化に役立てていきたいと考えています。そのためにも、複数のログデータの串刺し表示の活用も積極的に行っていきたいと思います」

また同社では、基幹系も含めてシステムのクラウド環境への移行を進めていく予定だ。

「クラウド環境に移行してもログ管理は重要と考えています。よってクラウド環境においてもMylogStarやLogstorageを活用した操作ログの取得、管理を徹底していきたいと思います。その上でアシストには、セキュリティ対策も含めたトータル的なインフラサポートを期待したいですね」（竹野氏）

MylogStar＋Logstorage　連携

「MylogStar」が収集したPC操作ログを「Logstorage」に取り込むことで、他のさまざまなログも含めた横断検索・分析、監査レポートの出力を可能にします。連携パックをご用意しておりますので、ログフォーマット定義やレポートテンプレート等もご利用できます。



ライセンス形態・価格、体験版のダウンロードなど詳細はこちら

https://www.mylogstar.net/

RUNEXY®
Run in the Next!

株式会社 ラネクシー
https://www.runexy.co.jp/

〒160-0023 東京都新宿区西新宿8丁目1番2号 PMO西新宿3階
TEL:03-6261-4711　E-Mail:mls_sales@runexy.co.jp

お問合せ