PCI DSS要件に対応、柔軟性に優れたログ管理システムとして採用 Splunk EnterpriseとSplunk On-Callがインシデント対応の効率化を実現

概要

会員カードの発行や管理、運用サポート、リアルな店舗とオンラインの顧客情報の一元化、クレジットカードやポイントカードをはじめとした支払い情報と顧客情報の連携など、ペイメントとマーケティングに特化したソリューションを提供しているベスカ株式会社。2007年に起業し、プリペイドカードやポイントカードのサービス基盤をASPにて提供しており、マルチ決済プラットフォーム「Ark」や顧客囲い込みを目指すペイメント＆マーケティングプラットフォーム「Seeds」などが主なサービスとなっています。クレジットカード決済のトランザクションは月間で1千万件を超えるまでに広がっており、同社が提供しているVerifone社製のマルチ決済端末は数万台規模にまで拡大。キャッシュレス化の大きな流れを受けて、順調に事業を拡大し続けています。

そんな同社では、クレジット決済サービスを事業展開するにあたり、カード業界におけるセキュリティ基準であるPCI DSS要件を満たすために必要なログ管理システムとしてSplunk Enterpriseを導入しています。また、業務システムおよびクラウド環境の監視システムから寄せられた各種アラートを集約管理し、事前に設定されたエスカレーションポリシーに応じて適切な担当者に通知を行う仕組みとしてSplunk On-Callを活用。IT運用における効率的なログ解析を可能にしながら、アラート情報を最適な形でフィルタリングすることで業務負担を大幅に軽減することに成功しています。

既存環境ではログ解析などが柔軟に実施できず、パフォーマンスも厳しい状況に

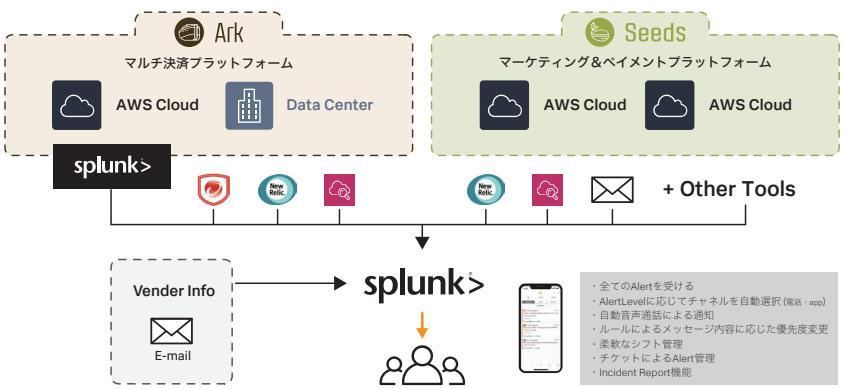
同社では、マルチ決済プラットフォーム「Ark」を運用するため、会員データの安全な取り扱いを目的に策定されたクレジットカード業界のセキュリティ基準であるPCI DSS認定を取得しています。このPCI DSSでは、会員データへのアクセスの追跡と監視、および不正アクセスの早期発見と追跡可能性を満たすためのログ管理に関連する要件が定められており、適切なログ管理を行うための環境整備が必要不可欠です。そこで同社では、以前から国産のログ管理システムを導入、運用してきました。このシステムを選択したのは、当初は単なるログの収集および管理が可能なものとして、コストを重視して選択したとオペレーション部 部長 松澤 新氏は当時を振り返ります。

しかし、PCI DSS要件に沿ったログ管理以外の活用も検討を続けていくなかで、新たな課題が顕在化してきたのです。「確かにPCI DSSの要件は満たせますが、ツールに依存した形でログを取り込む必要があり、例えばオペレーションに直結したログを解析しようとしても、相関的に見ていくことが困難でした。トランザクションの増加でパフォーマンスも落ちてくるなか、各サーバにログインしてシェルスクリプトなどを駆使したほうが迅速にログ解析しやすい状況だったのです」と松澤氏は当時を振り返ります。

また、ビジネスが広がる過程でペイメント＆マーケティングプラットフォームである「Seeds」についても課題が顕在化していました。「オンプレミスやAWS上の基盤など複数システムから毎月多くのアラート通知があり、運用負荷が増大していました。オンプレミスで稼働する一部のシステムは監視業務を外部委託していたものの、クラウド基盤については複数のツールを駆使し、自前で監視を行っていました。それぞれ部分最適化された環境で、少人数で運用するには限界を迎えていたのです」と課題を吐露します。

柔軟なログの取り込みが魅力なSplunk、業務効率化に大きく貢献するSplunk On-Callに注目

新たな環境を模索するなかで出会ったのがSplunk Enterpriseでした。「セキュリティ製品としてSplunkを認識していましたが、柔軟にログ解析することでオペレーションをはじめとしたIT運用に活用できることをセミナーにて知ったのです」と松澤氏は出会いを語ります。実際には、オープンソースのElasticsearchなども試してみたことはあったものの、メンバー含めて一番分かりやすかったと評価されたのがSplunkだったのです。



vesca

業種

- IT業界

活用事例

- 決済システムの監査ログ管理、アラート通知の効率的なエスカレーション

課題

- ツールに依存した形でしかログが取り込めず、オペレーションに直結したログ解析が困難
- 複数のログを横断的に見ていくことができない
- ビジネス拡大に応じてパフォーマンスが劣化、直接サーバを確認した方が迅速な状況に
- 複数の監視ツールから寄せられるアラート通知に対応する工数が大幅に増大

導入効果

- 少数精鋭での運用に最適なオペレーションの効率化を実現
- 工数削減で新しいことを学ぶ機会の創出を可能に
- アラート通知を絞り込むことで心理的な負担軽減に貢献
- インシデントの管理工数を86%、対応工数を99%低減することに成功
- 外部委託の範囲を削減するなど、監視業務のコスト低減に寄与
- 顧客サポートのサービスレベル向上に貢献

データソース

- PCI DSSに沿ったセキュリティ監査ログ
- 各種アプリケーションログ
- Amazon CloudWatchで取得できるログやメトリクス情報
- AWS CloudTrail
- Active Directory関連ログ
- ファイアウォールログ
- ロードバランサの通信ログ

ご利用製品

- Splunk Enterprise
- Splunk On-Call

ベスカ株式会社
オペレーション部
部長
松澤 新氏

特にSplunkが魅力的だったのはSPLの存在です。「障害解析に向けて様々な付加情報をログとともに吐き出していますが、SPLを使うことで分散している数百ものログを一括で把握できるだけでなく、何かエラーが出てもサーチ文を事前に用意しておくことで、すぐに原因が特定できます。SQLライクなサーチ言語だからこそ、メンバー含めて有意義な活用が可能だと考えたのです」と松澤氏は評価します。

また、スキーマ定義せずともログを取り込んで必要なデータが柔軟に検索できる点も大きな魅力の1つだと語ります。「非構造化データを自ら構造化していくことができるため、後からでもツールから必要な情報が検索できるのはとても助かります。まさに、かゆいところに手が届くツールだと評価したのです」と松澤氏。当初から課題を持っていたパフォーマンスについても、導入企業の実例やフリーのワークショップへの参加を通じて、必要なパフォーマンスが十分得られることを確認したのです。

同時に、負担が増大していたSeeds運用についても、サービスレベルの異なる複数システムから寄せられる膨大なアラート通知を集約し、本来対応すべきものだけに絞って必要なメンバーに知らせる仕組みを検討。「問題管理などは別のツールで行っていたため、条件に基づいて通知をうまくエスカレーションしてくれるシンプルな仕組みを探していました」。そこで出会ったのが、Splunkが提供するSplunk On-Callでした。「電話やSlackなどで通知を受け取るといったバラバラの運用を統合できる高い仕組みが構築できると考えたのです」と松澤氏。実は運用コスト削減も話題になっていたタイミングだったため、Splunk On-Callにてインシデント情報を集約し、ポリシーに応じてエスカレーションしてくれる仕組みに切り替えることで、監視業務のアウトソーシング範囲が縮小できると考えたのです。

PCI DSS関連のログ管理をはじめ、ログ分析からアラート内容の振り分けを柔軟に実施

現在は、Arkが稼働するAWS上の各種システムから寄せられるログをSplunk Enterpriseにて収集し、PCI DSS要件に必要な認証系のログやAuditログなどをダッシュボード上から確認できるようにしています。また、サーバやネットワーク機器など稼働監視に必要な各種ログを集めたうえで、解析に必要なキーを事前にセットし、何かあれば全てのログが横串で確認できる環境を整えています。さらに、Splunk DB Connect機能を利用して、RDBの情報をSplunkのログと照らし合わせたうえで経営へのレポートを作成するといった運用も自動化しています。

Ark関連のログを収集しているSplunk EnterpriseやSeeds関連のシステムから寄せられる各種アラートは全てSplunk On-Callに集約されており、アラートレベルに応じて通知チャネルを自動的に選択、担当者に最適な方法で通知が行われています。アラートへの対応状況はコメントを付けたうえでPDF化し、他部署やマネジメント層へのレポートとしても活用。Splunk On-Callのシフト管理機能を利用し、例えば松澤氏に来たアラートをアプリケーション開発チームのメンバーに割り振るといった柔軟な処理も行われています。「担当者が病欠などで急遽対応が難しい場合でも、シフトを変更することで担当者変更も容易になっています」と松澤氏。

少数精鋭ながらサービスレベルの異なる複数システムのオペレーションの効率化を実現

Splunk EnterpriseおよびSplunk On-Callを導入したことで、サービスレベルの異なる複数のシステムを少数精鋭で運用できるようになっており、運用管理の工数は大幅に削減できたと松澤氏は高く評価します。「アーキテクチャも大きく様変わりしていく時代だけに、若手エンジニアには新しいことに挑戦できる機会を与えたい。運用の効率化によって新しいことを生み出すことにリソースが活用できるのは大きい」。また、これまではロールを持つ担当者全員にアラート通知が行われ、輪番制で休日出勤せざるを得ない状況でしたが、Splunk On-Callによって限られた担当者だけに絞って通知が行われ、土日もシフト制に切り替えることができるように。「Splunkで相関的なログの可視化で原因調査が容易になり、条件によって通知を絞ることも、同じ事象であればSplunk On-Callにてまとめることも可能です。余計なコールは担当者に回さずに済むなど、心理的な負担軽減に大きく役立っています」と松澤氏は評価します。

障害発生時には、以前であれば2～3人で1日ほど拘束されることもありましたが、今はSplunkにて事前に定型化しておくことで、問題個所の特定まではわずか数分程度で済むようになるなど、劇的な改善につながっています。「ある月を例に挙げると、数十万にもおよぶ膨大なアラート通知のなかで対応が必要なものが2500件ほどあり、以前であればそれらを全て確認する必要がありました。Splunkによって対応が必要なものを170件にまで絞り込むことができ、かつSplunk On-Callで絞りこんで優先順位を判断、すぐに対応する必要があるものを8件にまで落とし込むことができました。インシデントの管理工数は86%低減、そして実際の対応工数は99%低減できたことになります」と松澤氏は高く評価します。

Splunk EnterpriseとSplunk On-Callを組み合わせることで、整理された形で担当者に情報が届くだけでなく、必要な手順のリンクも張り付けて通知可能となっており、コール段階で即時オペレーションできるようになっていると松澤氏。「必要な情報にまで絞りこんで通知してくれるため、まるで自分の部下が新たにできたような感覚です」と高く評価します。結果として、緊急性の高いネットワーク機器の監視だけにアウトソーシング範囲を絞り込むことができるなど、監視業務のコスト低減にもつながっています。

障害対応が迅速になったことで、顧客サポートのサービスレベル向上にも貢献しています。「カスタマーサポート部門に対して障害原因を迅速に通知できるようになり、お客さまから問い合わせをいただいた時点で状況説明がスムーズにできるようになりました」と松澤氏は評価します。

Splunkの魅力については、SQLライクに扱えるSPLの扱いやすさはもちろん、国内でのユーザー会が充実している点も大きなポイントの1つだと松澤氏は力説します。「1つのツールながらしっかりとしたコミュニティが形成されており、有益な情報が入手しやすく、手軽に情報交換することも可能です。Splunkの方からもざっくばらんに情報が入手できるため、本当に助かっています」。

Splunk EnterpriseとSplunk On-Callの組み合わせを環境統合時にも活用していきたい

今後については、キャッシュレスの社会的な潮流や感染症の影響で非対面でのビジネスに移行しつつある現状を鑑み、ArkとSeedsのシステム統合を通じて顧客が求める最適な環境づくりをさらに推し進めていく計画です。その際には、Splunk EnterpriseとSplunk On-Callを組み合わせながら今まで以上にうまく活用していきたいと語ります。

現状は、Splunk Enterpriseでログを可視化、分析することで得られた情報を活用し、Splunk On-Callにてオペレーションの簡素化や手順の添付などによるオペレーション品質の向上を実現していますが、いずれはIT業務の自動化に向けたAIOps的な環境づくりも進めていきたいと期待を寄せています。「Splunk On-Callをハブに、Splunk Enterpriseの良さをさらに引き出していくことで、これまで我々が一次対応で行ってきたことが不要になるような環境づくりも可能なはず。他にも、クラウド監視に効果的なSignalFxやセキュリティの領域で不正アクセスなどへの対応を自動化できるSplunk Phantomなどについても興味を持っています。少数精鋭での運用をさらに高度なものにしていけるような仕組みについても学んでいきたい」と最後に語っていただきました。

20-13742-Splunk-IT-Vesca-A4-102-CS-JP