口座の不正利用未然防止に向けた効率的な分析に大きく貢献
高度な相関分析で金融犯罪対策の一翼を担うSplunk Cloud

概要

株式会社セブン&アイ・ホールディングスのグループ会社として、多くの利用者に安全かつ先進的な金融サービスを提供している株式会社セブン銀行。600を超える提携金融機関等のカードが利用できるATMを展開するATMプラットフォーム事業では、セブン&アイグループ内の店舗や施設だけでなく、交通・流通・観光の各拠点などグループ外へのATM設置も積極的に展開しており、2018年5月末現在で24,000台を超えるATMが国内に設置されています。また、同社独自の口座サービスを提供する決済口座事業では、インターネットやATMを通じた非対面取引によるサービスながら、普通預金や定期預金、ローンサービス、デビットサービス、海外送金サービスなど幅広い銀行サービスを提供しており、月に約17,000件の新規口座が開設されている状況です。

同社では、非対面での取引が中心となってビジネスを展開していることから、開業当初からセキュリティやリスクに対する意識を高く持っており、不正防止対策をはじめとした各種リスク対策への投資を積極的に行ってきました。その対策を実施するための中核組織となるのが、口座の不正利用対策の立案や口座開設謝絶、警察などへの捜査協力、セキュリティ対策などを手掛けている金融犯罪対策部であり、その組織内には恒常的な部門としてCSIRTも設置されています。この金融犯罪対策部が実施する不正防止対策に向けた基盤としてSplunk Cloudを導入、さまざまな情報ソースをもとに解析を行うことで、不正口座の発見から口座利用停止、口座開設謝絶といった不正対策が可能になっています。また、アナログ的な手法から脱却することで、金融犯罪への効率的な対応が可能な環境整備にSplunk Cloudが大きく貢献しています。

複数のログを相関的に見て判断できる行動な分析基盤が必要に

同社が恒常的に対応できる組織として金融犯罪対策部の中にCSIRTを立ち上げたのが2015年のことですが、これまでは預金取引のモニタリングやインターネットアクセスの監視といった個別のソリューションを導入し、金融犯罪の発見に努めてきたと7BK-CSIRT リーダー (企画部 次長) 安田 貴紀氏は振り返ります。「起きている事象を点でとらえることが可能な優れたソリューションではあるのですが、それだけでは監視の目をすり抜けてしまうケースも。例えば口座申込の情報は正当に見えても、一定期間の時間軸で見ると、同じマンションの階違いで毎日申し込みがある、同じ部屋で異なる氏名の人から毎月申し込みがあるなど、単一の情報だけでは不正かどうかが判断しにくい場面もあります。犯罪が高度化していく中でちょっとした“違和感”を見つけていくためには、複数のログを相関的に見て判断できるような高度な分析が必要だと考えたのです」。

アナログ的な分析手法からの脱却を目指す

従来より、個別のソリューションから得られる情報を組み合わせて分析するアプローチは行われてきましたが、口座開設件数の急増などビジネスが拡大するなかで、人手に頼らない手法が強く求められていたのです。「不正の可能性が高い、いわゆる確度の高いものは人手によるアナログな方法で発見できます。しかし、確度の低いものや作業負荷が大きなものは優先順位を下げざるを得ず、人的な力では限界を迎えていました」と安田氏は指摘します。システムから上がってくるアラートは、少しでも疑義のあるものを含めて相当の件数があることから、人海戦術では全てに対応しきれない状況となっていたのです。一方で、チェックシート上でどの閾値を超えるとリスクが高くなるのかといったノウハウが長年の運用で蓄積されていました。「これまでの知見をベースにスコアリングモデルを構築したうえでシステム展開すれば、効率的な不正発見が可能になると考えました」と安田氏。

ルール作りやデータ取り込みが柔軟な、拡張性のある仕組みを希望

個別のソリューションについても、横断的なルールが組みにくく、システムによっては限定的なルールしか作れないといった課題が顕在化していました。将来的な活用も考慮した結果、新たなデータを加えて分析しやすい、データの取り込みが柔軟な仕組みを検討することに。

セブン銀行

業種

- 金融機関

活用事例

- 銀行口座の不正利用防止やインターネットバンキングによる不正送金など金融犯罪の分析基盤として活用

課題

- 複数のログを相関的に見て判断できるような高度な分析が必要に
- 人手でのアナログな処理によって業務負担が急増していた
- ビジネスの成長や、環境変化に合わせて、人員を増やさざるを得ない状況にあった
- 個別の仕組みでは横断的または複雑なルールが作りにくく、データ取り込みなど柔軟性に欠けていた

導入効果

- 必要なソースが柔軟に追加でき、検知の精度や幅が広がる
- システムによってリアルタイムな検知が可能な基盤が整備できる
- 職人肌になりやすい分析作業が標準化できる
- 効率化によって人員を増やさずともビジネスの成長に追随できるようになる
- データ取り込みが容易になり、トライ&エラーしやすい環境が整備できる

データソース

- インターネットバンキングのアクセスログ
- 勘定系システム内の預金取引に関する情報
- 銀行口座開設時の情報
- FraudAlert (カウリス社) による不正アクセスの判定結果
- 電話番号の履歴情報
- 自社作成のリストデータ

スプランク製品

- Splunk Cloud

株式会社セブン銀行
7BK-CSIRT
リーダー (企画部 次長)
安田 貴紀氏

実はその過程で注目したのが、マーケティング的な手法でした。「さまざまな形式のデータを取り込んで、ある意味"異常値"を見つけ出すアプローチは、ロイヤルカスタマーを見つけ出すマーケティングの手法に近いと考えたのです」と安田氏。しかしデータマイニングツールなども検討してみたものの、どうしてもマーケティングに偏ってしまうなど、汎用性や柔軟性に欠ける部分があったといいます。

金融機関にも実績が豊富な Splunk

そこで出会ったのがSplunkでした。「日本ではセキュリティソリューションという印象が強いですが、米国ではSplunkはマーケティングソリューションとして活用されている話も聞いていました。将来的にはオフィスの業務機器から得られるログを分析するといった新たな用途への展開も検討していたため、Splunkに興味を持ったのです」と安田氏は説明します。そこで複数のベンダに提案を求めたところ、結果として多くのベンダが提案してきたのがSplunkでした。「私の場合は感覚的な視点でしたが、実際のベンダからも同じ答えが出てきたことで、確度が高いと考えました。Splunkを利用している多くの金融機関があることも知っており、ノウハウの共有を含めて、我々にとって利便性が高いと判断しました」。

将来的には自前で運用していくことも想定しており、教育的な面でもSplunkを評価した安田氏。「Splunkが提供するトレーニングをはじめ、サイバーセキュリティの情報共有や分析を行う金融ISACという、我々が所属している団体内でもSplunkに関するトレーニングが開催されています。スキルアップしやすい環境が整っていた点も選択の大きなポイントです」と力説します。他にも、さまざまなベンダが提供するSplunk Appsも充実しており、自社の用途に応じて柔軟に機能拡張できる点も大きな魅力だったと安田氏。

今後も外部データの取り込みが増えてくることを想定し、拡張しやすいクラウド環境で利用できるサービスを選択、結果としてSplunk Cloudが同社の金融犯罪防止のための情報分析基盤として採用されたのです。

金融犯罪の兆候を見つけ出す基盤として活躍する Splunk Cloud

口座の不正利用や不正送金といった金融犯罪の兆候を見つけ出し、未然に防ぐための分析基盤としてSplunk Cloudが活用され、インターネットバンキングのアクセスログや預金の取引情報、口座開設情報はもちろん、不正アクセスの検知も提供するFraudAlert（カウリス社）と呼ばれるサービスなど、外部情報も含めたデータソースを活用。スコアリングしたうえでアラートにてリスクを管理者に通知し、必要に応じた対策を実施しています。分析に使うデータサイズは1日数十GB程度となっており、データは一定期間保持したうえで必要に応じて削除していく運用です。「我々独自に作成したリストもデータ投入していますが、システムごとにデータフォーマットやリストが異なっているため、口座番号などをキーに紐づけていくことで相関分析が可能になります。まさにSplunkが得意とするところ」と安田氏は評価します。

ログ自体はリアルタイムに取り込むものとバッチにて処理するものに分かれており、その場で口座の利用停止を行うといった判断が求められる分析にはリアルタイムに取得した情報が不可欠です。「犯罪を未然に防ぐためには、数秒のうちにその兆候を発見して口座を止めるといった処理が求められる場面もありますが、Splunk Cloudであれば必要なレスポンスも十分に担保されており、運用的にも十分満足しています」と安田氏は語ります。なお、各システムからSplunk Cloudにデータを自動的に転送していますが、緊急性を要する特殊な事案に対処したりログが活用できるか試してみたりするために、手作業にてアップロードできる環境も用意されている状況です。

分析作業の標準化で人手をかけずともビジネスの成長に追随できる

今回Splunk Cloudを活用したことで、職人肌になりやすい分析作業が標準化でき、効率化によって現状の人員のままでもビジネスの成長に追随できる環境が整備できると安田氏は評価します。「従来に比べて半分程度の期間で人材育成が可能になります。Splunk上のダッシュボードも非常に使いやすく、ヒットしたルール情報や過去の操作・取引履歴など、検知した口座情報が1つの画面で表現できています。必要な情報にたどり着けるようになっており、迅速な判断が可能になっています」。

データ取り込みが容易で、部品も多く用意されていることから、トライ&エラーしやすい状況にある点も大きな魅力の1つとなっています。「Splunkによって犯罪を未然に防ぐことができる機会が増え、口座の利用者から感謝される機会もより増えてくるはず。担当者のモチベーションアップにもつながってくれることを期待しています」と安田氏。以前に比べて感知レベルも向上しており、アナログでのスコアリングからシステムで自動検知できることで担当者のストレスも大きく軽減できると評価します。「これまでは監視のために画面を見続ける必要がありましたが、アラートがメールで通知されるなど、負担のない運用を構築しました」。

新たな視点や知見を得るきっかけに

特にSplunkに期待するのは、これまで気付かなかった新たな視点を養うきっかけが得られることだと安田氏。「どうしても先入観を持って分析してしまうものですが、拡張性のあるSplunkであれば、これまで対象にしていない外部情報をミックスしていくことで、これまでにない視点が得られるはず。そうなれば、マーケティングにてロイヤルカスタマーを見つけるように、金融犯罪を行う人物が特定できるようになるのではと考えています」。人手によるアナログな処理では限界があった分析も、新たな情報を容易に付加できる環境が整備できたことで、これまでにない知見を得ることができるはずと安田氏は期待を寄せています。

将来的には、リスクスコアリングによるアラート通知の環境からさらに一歩進めて、アラートのレベルによっては口座の利用停止や送金停止といった、具体的な処理まで自動化できる環境を整備していきたいと安田氏は意欲的に語ります。また、現状は金融犯罪に関連した用途が中心ですが、例えば、ハードウェアの障害予兆を検知したり、複数あるソリューションのIDを棚卸したりなど、幅広い用途への展開についても検討していきたいと語ります。「基本的にはCSIRTの動きの中で活用を広げていきますが、いずれは社内にも開放していきながら、データから新たなヒントが得られるような分野に展開していきたいですね」と今後について安田氏に語っていただきました。

20-13891-SPLK-Seven Bank-A4-103-CS-JP