株式会社ジャパンネット銀行

セキュリティが生命線のネット銀行を支える Splunk Enterprise の高精度な検知 & モニタリング

ジャパンネット銀行

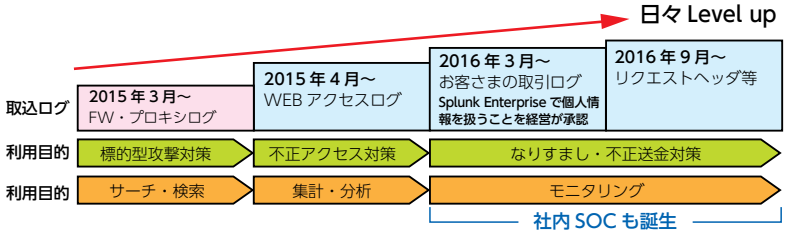
標的型攻撃、進化するサイバー犯罪、なりすましや不正送金への対策にも使えば使うほど広がる Splunk Enterprise 活用フィールド

必要な時に、自分たちの手で、しかも高速で

高度化するサイバー攻撃に連携して対抗するため、わが国の金融業界ではサイバーセキュリティ情報を広く共有するエコシステムの考え方が普及しています。そのための枠組みとして設立された金融 ISAC 等を始めとする共助団体の中で、不正に使われた IP アドレス等の情報を共有しています。

「こうして得た情報を元に私たちも自行内を調査します。しかし、これを行うにはモニタリング部門へデータ抽出の依頼が必要で、対応には多くの手間と時間がかかっていました」。そう語るのは、ジャパンネット銀行のサイバーセキュリティ対策を担う JNB-CSIRT の小澤一仁氏です。小澤氏によれば、たとえば金融 ISAC での情報共有は毎日のようにあり、とてもその全てを確認しきれない状態でした。そこで着目したのが Splunk Enterprise です。当初は標的型攻撃の検知を目的に社内 OA 環境のファイアウォールログやプロキシログを取込ませていましたが、インターネットバンキングのアクセスログを取込めば、サイバーセキュリティ対策に活用できると考えたのです。

「私たちの期待に Splunk Enterprise は見事に応えました。アクセスログを取込みさえすれば、必要な時に自分たちの手でしかも高速で検索できるのです。金融 ISAC 等で共有される情報も、一気に全ケースを確認できるようになりました」。こうして Splunk Enterprise は不正アクセス対策のためアクセスログの集計 / 分析を行うようになり、サイバーセキュリティ分野での成果を急速に蓄積しました。そして 2016 年、ジャパンネット銀行は例のない先進的な取組みに踏み切り、Splunk Enterprise 活用をさらに高度なステージへ進めます。



※取込ログの種類を増やしていくにつれ、利用目的も変化し、Splunk Enterprise の利用方法は高度化した。

Splunk Enterprise 活用で事案発生を抑え込み、不正送金被害ゼロへ

「通常、金融機関でお客様の取引情報を扱うのは業務部門に限られ、IT 部門がお客様の個人情報に触れることはありません。しかし、私たちはこの常識を打ち破ろうと考えました」。そう語るのは JNB-CSIRT を率いる二宮賢治氏です。当時は不審な動きを見つけても、インターネットバンキングのアクセスログだけではどのお客様の取引か分らず、モニタリング部門に問い合わせるしかありませんでした。そのひと手間が CSIRT の対応を決定的に遅らせていたのです。

「それまでは、お客様からご連絡をいただいて初めてなりすましログインに気がつくケースが多々ありました」（小澤氏）。こうした状況を変え、お客様を護っていくには、Splunk Enterprise にお客様の取引ログを取り込んでモニタリングし、さらなるスピードアップを図る必要がある。そう考えた二宮氏らは経営の決断を仰ぎ、承認を取り付けます。そして 2016 年 3 月、JNB-CSIRT はお客様の取引ログを Splunk Enterprise へ取込み、本格的なモニタリングを開始したのです。

業種

- ネット銀行

課題／背景

- 標的型攻撃対策のため社内 OA 環境の FW／プロキシログのサーチ・検索
- 不正アクセス対策のため Web アクセスログの素早い集計・分析
- なりすまし・不正送金対策のためお客様の取引ログ、リクエストヘッダ等の高精度なモニタリング

ソリューション

- Splunk Enterprise を用いたサイバー犯罪の検知・モニタリング体制

導入効果

- 従来は半日～ 1 日かかっていたサイバー攻撃時の分析&対応を数分に効率化
- Splunk Enterprise を含む総合的な取組みにより、不正送金被害0 件（2016年度）を達成
- Splunk Enterprise 活用により CSIRT メンバーがスキルアップし社内 SOC （セキュリティ運用センタ部門）が誕生

データソース

- 社内OA環境
  - ●ファイアウォール、
  - ●アクセスログ
  - ●次世代ファイアウォール
  - ●フィルタリングログ
  - ●プロキシ
- インターネットバンキング
  - ●アクセスログ
  - ●IP アドレスの地理情報
  - ●お客様取引ログ
  - ●レスポンスタイム
  - ●リクエストヘッダ
  - ●WAF の検知情報
  - ●レスポンスヘッダ
  - 他

株式会社ジャパンネット銀行 会社概要

設立日：2000年9月19日

代表者：代表取締役社長　小村 充広

所在地：東京都新宿区西新宿2丁目1番1号

2000 年 9 月に設立。戦後初となる銀行法第四条による営業の免許を取得し、「日本初のインターネット専業銀行」として同年 10 月に営業を開始。インターネット・ IT 革命を背景とした消費者志向型の新たなスタイルの銀行の誕生は、日本の金融史に新たな 1 ページを記した。ジャパンネット銀行は、銀行界のベンチャー的存在として、従来の銀行にないスピード感・創造性を発揮し、お客さまの利便性向上・新たなサービスの開発にチャレンジを続ける。

「私たちにとってもチャレンジでしたが、この時から Splunk Enterprise の活用法がステップアップした実感があります。実際、なりすましログインやフィッシングサイトも、今では私たちが先んじて Splunk Enterprise で発見し、気づいてないお客様にお伝えしています」（小澤氏）。

サイバーセキュリティ対策のもう一つの柱であるワンタイムパスワードトークンの全顧客配布の効果も相まって、ジャパンネット銀行では 2016 年度以降の不正送金被害件数を0件と完全に抑え込んだのです。フィッシングも同様で、Splunk Enterprise が常時モニタリングし、兆候を検知次第即座に CSIRT メンバーへメールを自動送信するようになりました。「おかげで偽サイトなども、その完成前に発見できるようになりました。そうやって摘発した偽サイトは、今年度すでに 20 サイトを超えています」（小澤氏）。

そして、こうしたジャパンネット銀行の徹底した取組みは、さらに予想外の効果も生み出しています。

次は不正口座利用対策や機械学習の活用へ

「最近、ジャパンネット銀行はサイバー犯罪のターゲットから外されつつある、と感じるのです。実際、当社のようにきちんと対策を取っている所を狙うこと自体コストがかかり、犯罪者にとっては割が合いません。もっと弱い所を狙おうと考えるのです」（小澤氏）。それだけに業界の注目も集まっており、最近は Splunk Enterprise を導入したいと JNB-CSIRT を訪れる企業も増えています。「そうした要望には可能な限り応え、ノウハウも積極的に公開しています。情報やノウハウを提供し合うことで、皆が助かるのですから当然です」（二宮氏）。

こうして、サイバーセキュリティ対策用途の Splunk Enterprise 活用に大きな成果を上げた JNB-CSIRT では、すでに次のステージを目指す取組みも始まりました。たとえば金融犯罪の検知など、不正口座対策に Splunk Enterprise の活用を拡大しようという試みです。「不正な入出金などを Splunk Enterprise でモニタリングし、不正な口座の開設を防ごうと考えています。それを専門とする部隊も社内にいるのですが、Splunk Enterprise を使った方が速いしより多彩な観点から抽出できるので、そちらへも 展開していこうというわけです」（小澤氏）。さらにその先には、より高度な技術への挑戦も始まっています。

「機械学習を用いた不正送金検知にトライしたいのです。機械学習による予測でサイバー犯罪を先回りして検知できないか、と」。小澤氏によれば、それに必要な Splunk Enterprise のバージョンアップもすでに完了しているそうです。また、二宮氏は Splunk Enterprise が人材育成にまで効果を発揮していると語ります。

セキュリティ対策をリードするネット銀行の 2 つの核

日本初のインターネット専業銀行として生まれたジャパンネット銀行は、いまやわが国銀行業界のサイバーセキュリティに関わる取組みをリードする存在となっています。もちろん同行が、ここまでサイバーセキュリティの取組みに力を注いでいるのには理由があります。

「ジャパンネット銀行はネット銀行なので、基本ネットの窓口が全てです。もし Web での取引に問題が発生すれば、ほとんどの業務ができなくなります。当然、サイバーセキュリティ対策を徹底する必要があり、他行に比較優位で取り組む経営ポリシーの1つとしています」（二宮氏）。たとえば現在最も有効なサイバーセキュリティ施策とされるワンタイムパスワードトークンについても、同行がいち早く全顧客への無償配布と必須化を行い、メガバンクなど各行がこれに追随しています。同様に Splunk Enterprise の活用も広がっていく可能性が高いでしょう。

「もしこれから導入するのなら、とにかくどんどんデータを投入することをお勧めします。データを入れて常に検索できる状態に持って行く、そしてなるべく多様なデータを入れて、積極的に試行錯誤することが重要です。試行錯誤を怖れずチャレンジすることでフィールドが広がり、高度化していく。 それが Splunk Enterprise なのです」（小澤氏）。

Splunk Enterprise を導入してログの種類も増やし、レポートも作るようになったことで、私たち自身もより多様な観点を獲得できた実感があります。つまり、CSIRTとしてスキルアップできたわけで、Splunk Enterpriseの効果はメンバー育成にも役立っているといえるでしょう。

今後はその活用を、不正口座の開設防止の取組みや、機械学習による不正送金の検知等にも広げていきたいですね。

株式会社ジャパンネット銀行
IT統括部 部付部長
二宮 賢治 氏

株式会社ジャパンネット銀行
IT 統括部　部付部長
二宮 賢治 氏

株式会社ジャパンネット銀行
IT 統括部
サイバーセキュリティ対策室 室長代理
小澤 一仁 氏

splunk> www.splunk.com/ja_jp

Splunk Services Japan
〒 100-6334 東京都 千代田区丸の内 2-4-1 丸の内ビルディング 34F
TEL：03-6206-3780