FUJITSU

splunk>

株式会社ジャパンネット銀行様

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

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、Splunk Enterpriseの活用フィールドは広がります。

導入背景

- ■標的型攻撃対策のため社内OA環境のファイアーウォール・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

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ー部門)が誕生

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一般社団法人 金融ISACなどをはじ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。

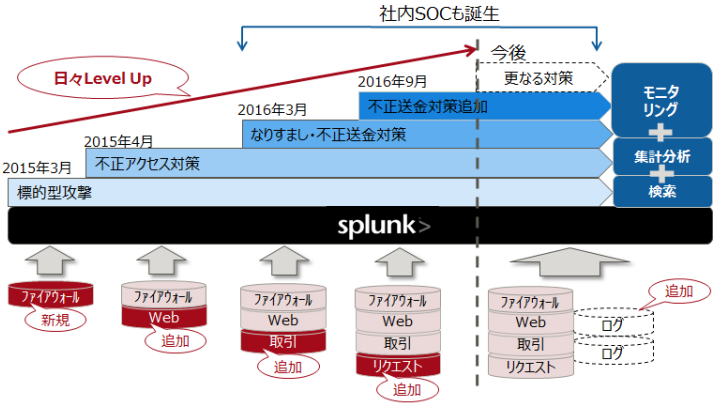
「こうして得た情報を元に私たちも自行内を調査します。しかし、これを行うにはモニタリング部門へデータ抽出の依頼が必要で、対応には多くの手間と時間がかかっていました。」そう語るのは、日本の銀行業界におけるサイバーセキュリティへの取り組みをリードする存在であるジャパンネット銀行様のサイバーセキュリティ対策を担うJNB-CSIRTの小澤一仁氏です。小澤氏によれば、例えば金融ISACでの情報共有は毎日のようにあり、とてもその全てを確認しきれない状態でした。そこで着目したのが統合ログ管理ツールのSplunk Enterpriseです。当初は標的型攻撃の検知を目的に社内OA環境のファイアーウォールログやプロキシログを取り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り込めば、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。

ジャパンネット銀行様のクリティカルなシステムを支える富士通グループにおいて、Splunk Enterpriseの導入実績の豊富な富士通SSLがシステム構築を担当しました。

「私たちの期待に、Splunk Enterpriseは見事に応えました。アクセスログを取り込みさえすれば、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。」（小澤氏）

こうしてジャパンネット銀行様はSplunk Enterpriseを活用し、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、同行は例のない先進的な取り組みに踏み切り、Splunk Enterpriseの活用をさらに高度なステージへ進めます。

[ジャパンネット銀行様の取り組み]



Splunk Enterprise 活用で事案発生を抑え込み 偽サイトの発見にも効果

「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り引きか分らず、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、お客様を守っていくには、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へ取り込み、本格的なモニタリングを開始しました。

「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、気づいていないお客様にお伝えしています。」（小澤氏）

Splunk Enterpriseが常時モニタリングし、フィッシングの兆候を検知次第、即座にCSIRTメンバーへメールを自動送信するようにしています。「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様の徹底した取り組みは、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

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

「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り組みも始まりました。例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。

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

「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。

「Splunk Enterpriseを導入してログの種類を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り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。」

日本の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、お客様の利便性向上・新たなサービスの開発にチャレンジし続けるジャパンネット銀行様を、富士通SSLは高度なセキュリティのノウハウで今後も支援していきます。

株式会社ジャパンネット銀行

【所在地】　東京都新宿区西新宿2丁目1番1号
【設立】　2000年9月19日
【代表】　代表取締役社長　小村 充広
【ホームページ】 http://www.japannetbank.co.jp/

株式会社富士通ソーシアルサイエンスラボラトリ
統合ログ管理ツール「Splunk」製品ページ

http://www.fujitsu.com/jp/group/ssl/products/network/security/network-security/log-management/splunk/

お問い合わせ先
株式会社富士通ソーシアルサイエンスラボラトリ(富士通SSL)
お問い合わせ総合窓口
〒211-0063 川崎市中原区小杉町1-403武蔵小杉タワープレイス
E-mail : ssl-info@cs.jp.fujitsu.com
当社ホームページ　http://www.fujitsu.com/jp/group/ssl/