Elasticスタックを使ってお客様の目線でセキュリティ監査の仕組みを実現

前向きで継続的な監査のみならず、セキュリティチームの地位向上から内部不正の抑止効果まで

企業名
フューチャーアーキテクト

場所
Tokyo Japan

区分
コンサルティング

製品
Elasticスタック

使用事例
セキュリティ分析

1	10	1
日	**種類以上**	**台**
サポートの平均レスポンスタイム	監査のためのログ	クラスタの数

創業以来、ベンチャー気質を強く持ち続けている技術志向の会社

ITを活かした経営を実現するためのコンサルティングサービスを提供するフューチャーアーキテクトは、創業以来、ベンチャー気質を強く持ち続けています。技術革新を積極的に取り入れ、既存のプロダクトでの対応が難しければ「無いものは作る」という文化があります。また、取り組んだことのない分野にチャレンジすることも非常に大切にしています。

自社運用を選び、セキュリティ監査にElasticスタックを採用

同社はElasticスタック（Elasticsearch、Logstash、Kibana）をある金融機関様向けのシステムに採用しました。顧客のマイナンバーを管理するためのシステムで、「当社のコンサルタントがお客様と同じ目線に立ってプロジェクトを進めました」（フューチャーアーキテクトの日比野 恒Technology Innovation Groupスペシャリスト）。具体的にはLogstashでログを収集してElasticsearchに蓄積し、Kibanaで作成したダッシュボードでデータを見る、という方式を選択しています。

2015年4月に立ち上がったプロジェクトでしたが、マイナンバー法が施行される2016年1月までにシステムを完成させる必要がありました。非常にタイトなスケジュールである一方で、当然ながら金融機関に求められる高いセキュリティレベルの実現も必須でした。

他の金融機関の多くは、マイナンバーを管理するためにクラウドサービスなどを利用したアウトソーシングを選択していました。しかし「我々は厳格な運用のための管理体制についてお客様と慎重に検討を重ね、アウトソーシングではなく独自のシステムを構築し、自社で管理することを決めました」（日比野氏）。自営のシステムにすればマイナンバーの利用拡充に伴う法整備や法改正などに自ら迅速に対応でき、将来的には顧客の重要な情報のすべてをセキュアに管理するための基盤としても利用できる、との考えによる判断でした。

セキュリティ監査にElasticスタックの採用を決定した理由は、技術力に自信がある我々にとってはオープンソースであることが魅力的だったことです。高品質なのに無料で、ログの量に応じて課金される懸念もありませんでした。

プロジェクトではまず金融庁のガイドラインを読み解き、どのようなシステム要件に落とし込むかを考えました。組織体制・業務・システムを全体視点で捉え、求められる対策を「人・組織」「物理」「技術」の軸で整理しました。内部不正への対策は、業務担当者やシステム管理担当者など各々の権限を適切に分離することでより一層強化し、不正利用、不正アクセス、改ざん、ウィルス、盗聴、情報漏えい、サービス妨害などのセキュリティ脅威に対しては多軸的かつ多面的な対策を講じました。

短期間でのプロジェクト成功は、Elastic社のサポートのおかげ

オープンソースソフトウェアであり自由に手を入れることができるという点がElasticスタックを選択した最大の理由でしたし、当初は我々とお客様だけで作業を完結しようと考えていたため、Elastic社からサポートを受けられる有償のサブスクリプションを購入するつもりはありませんでした。しかし、限られたスケジュールでより付加価値の高い仕組みをつくりプロジェクトを完遂するためにはサブスクリプションのサポートがあった方が良いと判断し、契約することにしました。

Elastic社のサポートは、どんな内容にもいつでもすぐに対応してくれた印象があります。製品に関して少しでも気になる点から、設定方法、推奨構成などかなり多岐に渡る内容を質問させてもらったのですが、質問に対して平均1日以内で回答していただいていたように感じています。

「例えば、いろいろなフォーマットのログデータをKibanaのダッシュボードに分かりやすくシンプルに表示するにはどうしたらいいか」など、かなり込み入った内容であっても概ね翌日には回答していただけたので、短期間で問題を解決できました。

- 日比野氏

【対応チケットの抜粋】

No	チケット件名	起票日	初回回答日	クローズ日
1	I Can't Install Logstash-input-jdbc in Offline network.	2015/11/18 18:45	2015/11/19 01:38	2015/11/27 09:08
2	Windowsに導入したLogstashに関する質問	2015/11/19 10:32	2015/11/19 18:45	2015/11/20 05:27
3	Logstashの起動ユーザーについて	2015/11/25 10:13	2015/11/26 07:48	2015/11/26 14:27
4	elasticsearchの起動ユーザー	2015/11/25 12:38	2015/11/27 04:43	2015/11/27 04:43
5	kibanaの起動ユーザー	2015/11/25 12:39	2015/11/27 04:31	2015/11/27 06:25
6	elasticsearchのログの説明	2015/11/25 12:52	2015/11/26 09:53	2015/11/26 14:51
7	kibanaのログの説明	2015/11/25 12:54	2015/11/26 05:49	2015/11/26 14:18
8	dashboardのデフォルト表示設定	2015/12/01 15:18	2015/12/02 06:08	2015/12/02 15:00
9	OSパーティションサイズ変更に伴うelasticsearch不具合の可能性	2015/12/01 15:42	2015/12/02 06:15	2015/12/03 19:15
10	同一項目名のデータを抽出方法	2015/12/01 17:55	2015/12/02 06:16	2015/12/03 09:54
11	受信する大量ログ(Syslog)の抑止方法	2015/12/02 01:46	2015/12/02 06:18	2015/12/03 19:16
12	RAC構成のOracleDBへのjdbc output方法	2015/12/06 20:29	2015/12/07 06:51	2015/12/07 06:58
13	Can I change time to create a new index?	2015/12/08 04:32	2015/12/08 07:33	2015/12/11 06:00
14	My SQL lost when DB failured.	2015/12/11 03:02	2015/12/11 10:39	2015/12/14 07:18

Kibanaのダッシュボードで、セキュリティ監査を前向きかつ継続的に

この仕組みを構築する上で最も重要視したのは、ログ情報をシンプルなグラフで表示して、直感的に把握できるようにしたことです。まずは簡易的なものから作り、シンプルに仕上げていきました。

一番最初にアクセスするKibanaのダッシュボードには、必ずチェックしなくてはいけないデータを表示しています。当初は日次のデータを表示するようにしていましたが、データによっては一週間分を日にち単位で表示する方法も効果的であることが分かり、いろいろと試しながら変更を加えてみました。

WebのAPIを介してデータベースに対する参照・登録を管理する仕組みであるため、どのユーザーがどのような操作をしたのかが簡単に分かります。「APIのログが通常の値よりかなり増えている」、「通常では発生しないログが出ている」といったことをKibanaのグラフから判断できるため、ITを熟知していない担当者でもログの監視が可能です。

また、まずはシンプルに仕上げる事を目的としていたため、異常な値が出た際にアラートで知らせる、といった運用方法はあえて採りませんでした。アラート主体の運営にすると、「運用担当者はアラートが来ないから、今日は平気だと思い込み継続的に見る習慣が身につかないと思ったからです。我々は、ダッシュボードを見ることを担当者に習慣化して欲しいと考え、あえてシンプルにしました」（日比野氏）。この習慣づけが、日々の"前向きかつ継続的な監査"に繋がっていくのだと思っています。

導入した効果は意外なところでも

監査の担当者には、システム部門出身の人と、ドキュメントのチェックをしていたような総務部門出身の人がいます。後者の場合、システムに苦手意識があるケースも多く、分かりにくいシステムだと使うのが嫌になってしまうことがあります。しかしKibanaのグラフィカルなインタフェースであれば、ITを熟知していない人でも直感的に問題を把握できます。

マイナンバー対応以外にも、副次的な効果が出ています。これまでは何か事件が起きない限り動かなかった個人情報を扱う部門が、今回のシステム導入を機に、能動的に問題を察知し、問題が起きる前にシステムの利用者に注意したり、「常にチェックされている」と意識づけることで利用部門を牽制できるようになりました。これにより社内でセキュリティ部門の地位が高まり、内部不正に対する抑止の効果も見え始めました。

> 　またフューチャーアーキテクトは今後、「システムがスケールアウトしたり、マイナンバー以外の目的で使う様になった場合には積極的にElasticスタックを使っていく考えです。特にセキュリティの脅威分析など、高度なセキュリティ対策が必要になる分野では、Elasticスタックは大きな力を発揮すると考えています」
>
> - 日比野氏

お問い合わせはelastic-japan@elastic.co
までお願いします