CREATIONLINE, INC.

お客様企業
クリエーションライン株式会社

本社所在地
東京都千代田区

業種
システム開発

製品
Elastic Stack

ユースケース
クラウドサービスの利用状況の可視化

サブスクリプション
ゴールド

クリエーションライン株式会社：クラウドサービスの利用状況を可視化 新しい働き方に合わせたゼロトラストセキュリティの一環に

システム開発を手掛けるクリエーションライン株式会社では、業務において全面的にクラウドを活用するよう決定。それに伴い、クラウドサービスの利用状況を可視化し、監査するためのシステム「HARUMAKI」を構築しました。Elastic のプロダクト、サービスを利用することで、セキュリティ監査だけでなく、業務パフォーマンスの向上などの面での活用も計画しています。

1.5
カ月
開発期間
約1.5カ月

10
種
ダッシュボード
約10種

SIEM
Elastic Stack の
SIEMソリューションを
活用

クリエーションラインについて

2006 年設立の IT プロフェッショナル企業。クラウド、OSS、アジャイル、DevOps、データ解析・機械学習等の先端技術について多くの経験および知識を有し、アジャイル開発支援サービスや、オープンソースソフトウェアのサブスクリプション提供事業を手掛ける。
https://www.creationline.com/

アジャイルや OSS、クラウドを得意とする IT 企業、コロナ禍でリモートワークに

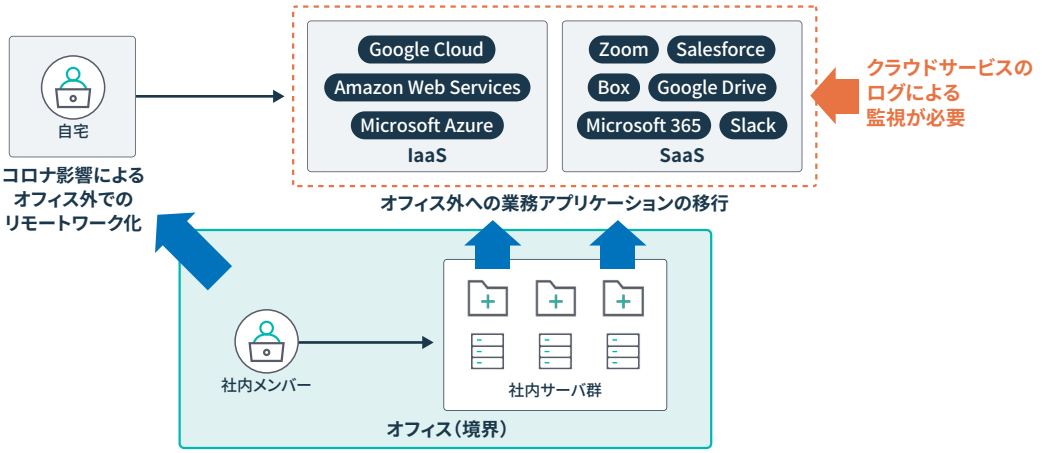
アジャイルや DevOps、CI/CD（継続的インテグレーション／継続的デプロイ）、オープンソースソフトウェア（OSS）やクラウド、そしてデータ解析・機械学習などを得意とする IT プロフェッショナル企業、クリエーションライン株式会社。2006 年に東京で設立、現在では富山市にもオフィスを構え、アジャイル開発支援サービス事業や、OSS のサブスクリプション事業などを手掛けている。前者は文字通り、アジャイル開発に取り組もうとする顧客企業に対し、そのコーチングや実開発の支援をサービスとして提供する事業。後者は言うまでもなく、OSS をエンタープライズで利用しようとする企業に対し、商用ライセンスとサポートを有償で提供する事業だ。

「当社では現在、この 2 つの事業を軸とし、社員に加え業務委託のビジネスパートナー、合わせて約 220 名のメンバーが働いています」と説明するのは、同社データ分析テクニカル エバンジェリストの日比野恒氏だ。

「特にアジャイル開発支援サービス事業においては、顧客企業のプロジェクトに深く関わる業務の都合から、当社のスタッフが開発チームの中に入り込んでいます。そのため、これまではお客様と一緒にプロジェクトルームを作るなど、物理的にも同じ場所で仕事をしていました。しかし新型コロナウイルスの流行により、そうした業務形態も変化を余儀なくされ、今ではリモートでの共同作業が中心です。当社のスタッフたちも分散して業務を行っています」

この業務形態の変化に伴い、さまざまな業務でのクラウド利用が以前より増えたという点は、他の多くの企業と同じだ。といってもクリエーションラインは、もともとクラウドの活用に積極的な会社であり、オンプレミスのサーバは少数だったという。そのためコロナ禍に

elastic



図：リモートワーク推進におけるゼロトラスト化

直面した際にも、さまざまなクラウドサービスを活用することで、比較的容易にリモートワークへ移行することができた。

「新しいモノ、新しい技術を好んで試す文化が根付いているためか、コロナ禍以前でもオンプレミス環境で使っていたサーバは多くありませんでした。業務に必要な機能は、SaaS などのクラウドサービスを利用したり、IaaS 上にインスタンスを立てて自分たちで構築したりすることがほとんどで、オフィスにあった本番環境といえるサーバは、社内で使うドキュメントを保管・共有するファイルサーバぐらいで、残りは開発サーバが少々ある程度です。そのファイルサーバも、老朽化対策などの観点からクラウドへ移行しようと考え始めていました。そこでコロナ禍を機に、各スタッフのマイドライブとして利用していた Google Drive へ一本化する形で集約、オンプレミスのサーバを廃止することにしました」（日比野氏）

全面的なクラウドサービスの活用において利用状況を監査する仕組みが必要に

ファイルサーバの移行は 2020 年 3 月末に完了し、クリエーションラインでは、その業務においてクラウドを全面的に活用するようになった。それに伴い、クラウドの利用状況をいかに監査するかという課題が新たに浮上してきた。

「スタッフは自宅などオフィス外から、クラウドの業務アプリケーションへ直接アクセスします。ファイアウォールなどのネットワークセキュリティに保護されない環境、いわゆる『ゼロトラストモデル』です。セキュリティの一環として、新たに重要なファイルの保護のためには、クラウドの利用状況を監査する仕組みが必要となります。まだ日本企業の多くは、その必要性を強く認識するまでに至っていないと思われますが、クラウドへの移行や働き方改革が進む中でニーズが高まってくることでしょう。そこで、まず自分たちで構築して、そのノウハウも得ようと考えました」と日比野氏は語る。

クラウドサービスの利用状況を監査するには、まずクラウドサービス側の監査用の API などを通じてログを取得し、必要な加工処理をした上でデータを蓄積、意味ある形に可視化するといった仕組みが必要となる。クリエーションラインでは、この一連の処理を行うシステムもクラウドで構築することにした。開発に際しては同社の得意とする CI/CD を駆使、サーバレスかつデータドリブンのアーキテクチャとし、もちろんデータはセキュアに処理するといったコンセプトを盛り込んだ。

Elastic Cloud の活用により 1.5 カ月という短期構築を実現、その後も改良を重ねる

「HARUMAKI」と名付けられたこのシステムには、概要図からも分かるように、Elastic のプロダクトが数多く用いられている。Filebeat により Google Reports API から Google Drive 監査ログを取得し、Logstash を通じて Elasticsearch に蓄積、これを Kibana で可視化し、

選定の大きなポイントは、Elastic SIEMソリューションの存在です。またFilebeatにはGoogle Workspaceモジュールもあり、開発も効率的です。監査担当者は、『感覚値でなくログというファクトから現状を正しく把握できることが刺激になった』と評価していますし、一般ユーザーも触れられる機能を追加したことで社内にElasticの良さを広める効果ももたらしました

データ分析テクニカル エバンジェリスト
日比野 恒 氏

監査できるようにした。Filebeat と Logstash は Amazon Web Services（AWS）上で稼働し、Elasticsearch と Kibana は Elastic Cloud を利用している。

「当社は Elastic のパートナーでもありますが、今回の HARUMAKI に採用した各ツールの選定はフラットに行いました。その上で Elastic Stack を選んだ最大のポイントは、SIEM ソリューションがあることです。また Filebeat には Google Workspace モジュールが用意されており、自分たちでプログラムを作るより効率的だという期待もありました。我々も過去のプロジェクトで苦労した経験がありますし、API の変更があればそのたびに修正が必要となり、運用にも負担が生じます」と、日比野氏は説明する。

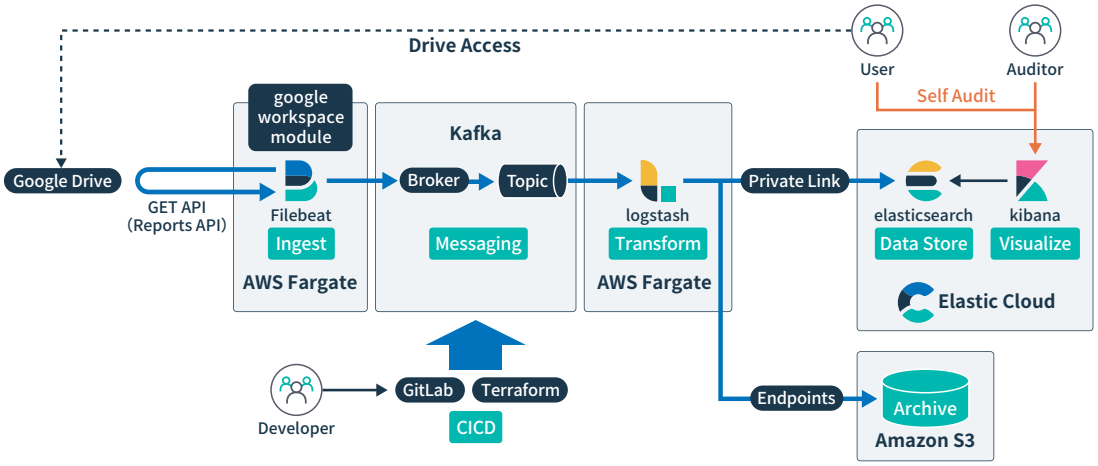
なお、Elastic Cloud と AWS の組み合わせを用いたのは、開発に着手した当時のプライベート接続の都合だ。Elastic Cloud へセキュアにデータを受け渡すため、このような組み合わせとなった。

日比野氏は、データ分析エバンジェリストという肩書きの通り、データ分析や活用のエキスパート。Elastic プロダクトに関しても数年間の活用経験があり、豊富な知識やノウハウの持ち主だ。氏を中心とした HARUMAKI の開発は、2020 年 5 月半ば頃に開始してから約 1 カ月半という短期間で、最初の稼働に漕ぎ着けた。もちろん、そのコンセプトに CI/CD が盛り込まれているだけに、その後も運用しながら継続的に開発が進められている。

「運用を開始した後にも、開発やトラブルシュートを容易にできるよう Logstash のパイプラインを見直すなどしています。平均すると、2 週に 1 度くらいの頻度でリファクタリングを行っていると思いますね」（日比野氏）

この継続的な開発を通じて、当初は想定していなかった興味深い機能も盛り込まれた。システム管理者ではない一般のユーザーも、自分自身のログに限って Kibana のダッシュボードを見ることができる、Self Audit 機能だ。

「最初は、システム管理者が気懸かりな箇所を見付けたとき、ダッシュボードを PDF 化して Slack で当人に伝え、確認をお願いしていました。しかし、このやり方では双方にとってコミュニケーション負担が大きく、指摘を受けたユーザーの方も自分の操作ログを自分で確認できた方が調べやすいため、Self Audit 機能のアイデアが浮上してきたのです。この機能の実装には Kibana Spaces のマルチテナントの仕組みを用いており、Google アカウントからシングルサインオンで Kibana にログインし、Elasticsearch のフィールド&ドキュメントセキュリティとロールを設定することで実現しています。これは私自身も他では見たことがないユースケースで、面白い試みだと思います」（日比野氏）



図：「HARUMAKI」のアーキテクチャ概要

セキュリティだけでなく、業務パフォーマンスの把握などアイデアが広がる

HARUMAKI の活用は、監査が可能になっただけでなく、さまざまな知見をクリエーションラインにもたらしている。

「監査担当者は、『感覚値でなくログというファクトから現状を正しく把握できることが刺激になった』と言っています。海外からの不正アクセスが疑われるケースを分析したところ、実は正当なユーザーの操作でもこのようなログを発生させるものなのだと分かったそうです。また、Self Audit 機能により、一般ユーザーも HARUMAKI に触れる機会ができ、Elastic プロダクトが使えるという感触を得た者も多いようです。実際のプロジェクトで使ってみようと考えたり、新たな活用のアイデアが出たり、いろいろな反応があります。セールスのメンバーも、自分たちが販売しているツールを実際に触って刺激を受けています」（日比野氏）

クリエーションラインでは今後、Google Drive だけでなく Slack や GitLab、Zoom などといった他のツールのログも、HARUMAKI による分析・可視化を行っていく計画だ。そして HARUMAKI の用途そのものについても、セキュリティ監査だけでなく業務パフォーマンス、仕事上のアクティビティ把握など多方面へと広げていく案が浮上している。

「複数ツールのログを相関分析し、ユーザー単位でアクティビティを分析することで、また新たな知見が得られるでしょう。クラウド上の開発環境のログなども興味深いですね。ユーザーやプロジェクト単位でクラウド利用料金を可視化する『コスト見える君』を作ろうという案もあり、マネージャたちの負担軽減にもつながるのではと期待されています」（日比野氏）

こうした社内の反応は日比野氏にとって、データ分析エバンジェリストという立場にもプラスだったと言えよう。日比野氏自身も、今回の HARUMAKI の開発を通じて Elastic プロダクトの新たな機能を知るなど、さらなるノウハウを得た。

「最近のバージョンでは、Kibana Alert and Action のように GUI で使える機能が増え、開発者ではない人でも Elastic プロダクトが使いやすくなってきました。Elastic Cloud のプライベート接続も、最近は Azure や Google にも対応し、セキュアな接続の選択肢が増えました。あとは、Logstash のマネージドサービスがあると、データエンジニアなどは大いに助かるはずです。もちろん、Elastic の本質は瞬敏な検索なので、その点は今後も保っていてほしいです。当社の情報システム部は社長直轄組織であり、また会社全体が『まずは試してみて早く体験を得ること』を大事にしているので、一緒に新しいことにチャレンジしたいという若者は大歓迎です」（日比野氏）

お問い合わせ
Email: elastic-japan@elastic.co

全文検索エンジンを提供する企業、Elastic は Elastic Stack（Elasticsearch、Kibana、Beats、Logstash の製品群）の開発元です。検索、ログ、セキュリティ、分析などのユースケースで大規模データをリアルタイムに処理するサービスを、オンプレミスと SaaS で提供しています。Elastic のコミュニティは 10 万人規模に成長しています。Elastic Stack は Cisco、eBay、Goldman Sachs、Microsoft、The Mayo Clinic、NASA、The New York Times、Wikipedia、Verizon を含む世界中の企業や組織で採用され、ミッションクリティカルなシステムを支えています。Elastic は、世界各国から社員が働く「分散型企業」として 2012 年に設立されました。詳しくは、elastic.co/jp/ をご覧ください。

