Google Cloud

Google Cloud 活用促進のためのガードレールを構築し、クラウド ネイティブな新規事業の立ち上げをサポート

即戦力人材と企業をつなぐ転職サイト『ビズリーチ®』など、HR Tech の分野で支持を集めている Visional グループ（以下、Visional）は、今、新規事業の迅速な立ち上げを実現すべく、本格的な Google Cloud 活用を加速しようとしています。しかし、そのためにはそれぞれの新規事業が無理なく自社のセキュリティ要件をクリアできるようにするための仕組み「ガードレール」の構築が不可欠でした。ここではその構築に至るまでの道程を、ホールディングカンパニーのビジョナル株式会社および、グループ会社のビジョナル・インキュベーション株式会社の皆さんに話を伺いました。

利用している Google Cloud サービス

Google Kubernetes Engine、BigQuery、Security Command Center、Identity Platform、Cloud Audit Logs、Cloud Asset Inventory など

VISIONAL

Visional

https://www.visional.inc/ja/index.html

〒150-0002
東京都渋谷区渋谷 2-15-1

「新しい可能性を、次々と。」をグループミッションとし、HR Tech 領域を中心に、産業のデジタル トランスフォーメーション（DX）を推進するさまざまな事業を展開。「ビズリーチ」をはじめとした採用プラットフォームや、人財活用プラットフォーム「HRMOS」シリーズを中心に、企業の人材活用・人材戦略（HCM）エコシステムの構築を目指す。また、事業承継 M&A、物流 Tech、サイバー セキュリティ、Sales Tech の領域においても、新規事業を次々に立ち上げている。従業員数は 1,466 名（2021 年 7月末時点・連結）

インタビュイー

Visionalグループ
ビジョナル株式会社
グループIT室 クラウドインフラグループ（CCoE）

- 長原 佑紀 氏
- 山我 晟潤 氏
- 藤原 和也 氏

ビジョナル・インキュベーション株式会社
Assured事業部 バックエンド エンジニア

- 岩松 竜也 氏
- ファン イーミン オリバー 氏

作り替えしやすい GKE を駆使して新規サービスを迅速に立ち上げ

転職サイト『ビズリーチ』など、HR Tech 領域を中心にさまざまな事業を展開する Visional は近年、これまでの枠組みに囚われないさまざまな新規事業を続々と立ち上げています。

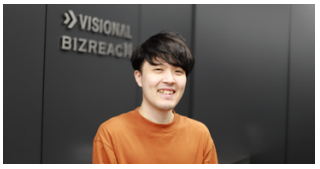
その一例と言えるのが、自社で導入を検討しているクラウド サービスのセキュリティ リスクを診断してくれるというセキュリティ評価プラットフォーム『Assured（アシュアード）』です（2021 年 1 月 β 版サービス提供開始）。そのアプリケーション基盤、データ分析基盤に Google Cloud を採用した理由について、本サービスを開発・運用するビジョナル・インキュベーション株式会社 Assured事業部 でバックエンドエンジニアを務める岩松 竜也氏に聞きました。

「Assured の立ち上げにおいては事業成長を可能な限り早めていくことを重視しました。そう考えたとき、最も有望なプラットフォームが、作り替えがしやすく、インフラを抽象化して負荷分散可能な GKE（Google Kubernetes Engine）、認証情報やユーザー権限などを柔軟に切り分けられ、マルチテナンシーなサービスと親和性の高い Identity Platform、そしてデータの蓄積と運用において大きな信頼を寄せられている BigQuery を擁する Google Cloud だったのです。」

なお、これまでも Visional ではデータ分析基盤として Google Cloud を活用していましたが、アプリケーション基盤としての利用実績はほとんどなく、社内に Google Cloud を適切に運用するためのガイドラインがありませんでした。そのため、Google Cloud の管理体制、特にセキュリティをどのように担保するかが大きな課題になったと言います。

「そこで、複数の関連部署と連携しながら手探りで責任分担や漏洩時の対応指針などを定め、ログの保存、監視、アラートといった機構を実装。認証に関しても、Identity Platform が我々のセキュリティ要件を満たすかどうかを入念にチェックするかたちで求められるセキュリティ要件をクリアしていきました。」（ビジョナル・インキュベーション株式会社 Assured事業部 バックエンド エンジニア ファン イーミン オリバー氏）

「最初から Google Cloud 上でどこまでセキュリティ対策や監視・権限周りの設定をすべきかの指針があればもっと開発に集中できたと思います。」と、開発当時を振り返る岩松氏。Assured の立ち上げ自体は成功したものの、Visional で今後さらに Google Cloud を活用していくためにも、Google Cloud のためのセキュリティ規定、『ガードレール』が必要だという結論に達しました。



岩松氏

オリバー氏

ガードレールと Security Command Center の連携でリスクを管理

「ガードレール」とは、企業内のクラウド プラットフォーム活用に際して厳しい制限を設けるのではなく、自由な利活用を推奨しつつ、望ましくない利用のみを制限あるいは検知できるようにするセキュリティ ソリューションのこと。開発のアジリティを損なうことなく、ガバナンス コントロールできることが特長とされています。

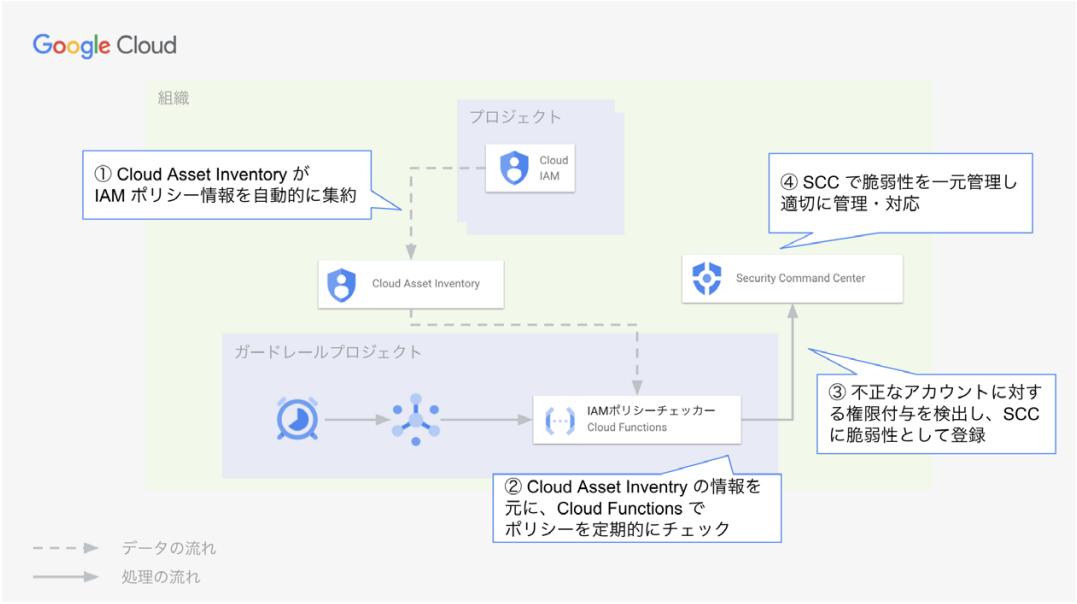
Visional では Assured での経験を踏まえ、グループ内のクラウド活用を推進する CCoE（Cloud Center of Excellence）が Google Cloud 向けのガードレール構築を主導。求められるセキュリティ要件をどのように担保していったのか、この取り組みを担当した Visional CCoE の山我 晟潤氏が次のように説明してくれました。

「ガードレールはセキュリティの基本的な考え方に基づき、予防的ガードレールと発見的ガードレールの 2 つに分類できます。予防的ガードレールとは組織として実施して欲しくない操作をあらかじめ制限しておくもの。今回の取り組みにおいては Google Cloud の組織ポリシーを使用して設定の制限を行ったほか、Cloud Audit Logs で取得したい情報を確実に取れるようにするなどしています。しかし、予防的なガードレールで対応できない場合もあります。ケース バイ ケースでリスク判断したい場合や、完全に防止しにくいリスクもあるでしょう。その場合、発見的ガードレールが有効です。発見的ガードレールはそのリスクのある設定を検出できるので、リスク管理の判断と対応が可能になります。こちらについては Cloud Audit Logs や Cloud Asset Inventory などのデータを BigQuery にエクスポートすることで検知できるようにしました。そしてこれらの情報を Security Command Center に連携させることでセキュリティ リスクを素早く可視化、脆弱性が登録されると即座にビジネス チャットなどに通知する仕組みを構築することで、いち早くリスクに対応できるようにしています。」

山我氏

藤原氏

長原氏



Cloud Asset Inventory , Security Command Center を活用した意図しない権限付与を検出するガードレールの仕組み

なお、Visional では Security Command Center のプレミアム ティアを利用。これによってプロジェクト単位での活用が可能になったほか、マネージド スキャンのおかげで「何を検出するかを考えて実装する作業を削減できた。」（山我氏）とのことです。

「今回の取り組みではガードレールの要件を決めることに最も時間を割きました。その際に参考になったのが、Google Cloud を組織的に利用する際に考慮すべきことがまとめられた『Google Cloud セキュリティ基盤のブループリント ガイド』。このガイドのサンプルが GitHub にあり、弊社も利用している Terraform で書かれていたのが非常にありがたかったです。また、Security Command Center 自体にダッシュボードが用意されていたことで、開発工数が削減できたことにも助けられました。」（山我氏）

「その他、細かいことを言うと Google Cloud では配下のプロジェクトに対して、組織レベルの設定を継承するかたちで設定を入れこんでいくことができるので、統一した設定を確立しやすいところがやりやすかったですね。」（Visional CCoE 藤原氏）

Visional における Google Cloud のためのガードレール施策は道半ばだが、ひとまずの道筋は付いた、今後はこれを全社的にアピールし、Google Cloud の利用を促進していきたいと語る山我氏と藤原氏。

「ガードレールはボディーブローのようにジワジワと効いてくる施策だと思っています。今後、新規サービスに Google Cloud を選定するという場合、Assured のときのような苦労をエンジニアにさせなくて済むはずです。サービス開発においてクラウド プラットフォームの選択肢を狭めないようにするという当初の目的は実現できたのではないでしょうか。今後は、Security Command Center で検知された検知項目について対応の要不要をきちんと見極め、事業にコミットしているメンバーと密にコミュニケーションを取りながら、よりセキュアなサービスを提供していけるようにしたいですね。」（藤原氏）

ちなみに CCoE とはもともと、プラットフォーム基盤推進室というグループ内プロダクトの信頼性や運用性、セキュリティなどといった非機能要件の改善を目的に設立された部署のメンバーにより、これからのクラウド時代に即したグループ横断的な組織として始動したもの。今回のセキュリティ ガードレールに関する取り組みは、CCoE が目指す大きな目標の第一歩だと言います。

「我々は Google Cloud を始めとするクラウド プラットフォームを徹底的に活用して信頼性、セキュリティ、アジリティ、コスト効率などを高めていくことが、プロダクトの成功、ひいてはビジネスの成功に繋がっていくと考えています。現在は、課題感が大きなガバナンスやセキュリティ部分に注力しており、ガードレールについても今後、マルチクラウド対応などさらに発展させていく予定です。その上でこれから数年かけて Visional のサービス全体をクラウド ネイティブ化していくことを目指しています。なお、こうした CCoE の活動に際しては、Google Cloud 公式ユーザー会 Jagu'e'r の CCoE 研究会に参加し、情報交換をさせていただいています。今後も Jagu'e'r で得られた知識によって我々の活動に磨きをかけるとともに、弊社の活動を発信することで世の中の CCoE の取り組みへ微力ながら貢献できればと考えています。」（Visional CCoE 長原氏）

※ 掲載の情報は、2021 年 12 月 取材時点のものです。

Google Cloud を活用することで、ビジネスの将来に注力できるようになります。インフラストラクチャの管理やサーバーのプロビジョニング、ネットワークの構成などに起因する負担を軽減することができます。つまり、イノベーターもプログラマーも、自分の本来の仕事に集中することができます。

お問い合わせはこちらから
https://goo.gl/CCZL78

Google Cloud

Google Cloud の詳細については、右記 URL もしくは QR コードからアクセスしていただくか、同ページ「お問い合わせ」よりお問い合わせください。