Google Cloud

Visional における CCoE 組織と セキュリティガードレール整備の取り組み

藤原和也
ビジョナル株式会社 グループ IT 室
CCoE エンジニア

Agenda

藤原 和也 (Kazuya Fujiwara)

CCoE エンジニア

受託開発でのWeb サービス開発、ゲーム会社でのゲームサーバ開発、デジタルコンテンツ企業でのオンプレミス環境のサーバエンジニア、クラウドを使ったアーキテクチャ設計、横断SRE などを経て、2019 年に株式会社ビズリーチに入社。横断観点からVisional 全体のクラウドの効果的な利用を促進するためのプラットフォームやプロセス開発に従事している。

Visional の事業と
クラウド利用状況

Visional グループ概要

- 設立
  - 2020年2月（ビジョナル株式会社設立）
- 創業
  - 2009年4月（株式会社ビズリーチ創業）
- 代表者
  - ビジョナル株式会社
    代表取締役社長　南 壮一郎

VISIONAL

グループミッション

新しい可能性を、次々と。

私たちは、インターネットの力で、時代がもたらす様々な課題を、
次々と新しい可能性（ビジョン）に変え、世の中の革新を支えていく。
「社会にインパクトを与え続ける」その志や事業のもとに
仲間が集まり、新しい仕組みやムーブメントを生み出すことで、
本気で実現したい未来へと加速させる。

Visional グループの事業

- 「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
- 事業承継 M&A、物流 DX、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

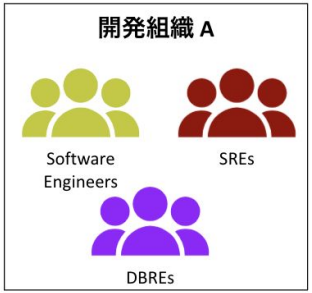
Visional におけるクラウド活用のステージ

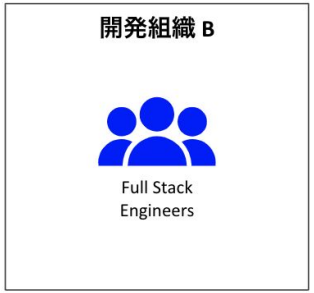
- フルクラウドでサービス運営
  - クラウドはデフォルトの選択肢
  - オンプレミス環境は保有していない
- クラウド利用状況
  - Amazon Web Services アカウント 100 以上
  - Google Cloud プロジェクト 75 以上 (アクティブなもの)
  - コストベースでは 95 % が Amazon Web Services で稼働

Visional プロダクト組織の特徴

全ての事業が自律的にクラウドを運用している

- 技術の選定 (どのクラウド、SaaS を使うのか等々) を含めそれぞれの事業部が意思決定を行っている
  - 自分たちで最適な決断を行う事により
    - 事業の自律性を尊重
    - ビジネスのアジリティを損なわない
- 組織の形も事業によって様々
  - 役割が明確に分かれて存在する組織もあれば、フルスタックなメンバが柔軟に対応する組織も





クラウドの利用状況

- 各事業のサービスはほとんどが Amazon Web Services で Web サービスを提供
  - もっとも主要な事業である Bizreach は Amazon Web Services でサービスを展開してきた
    - 社内のエンジニアにも AWS のノウハウが蓄積していく
    - 新たなプロダクトの立ち上げも AWS が選定されることが多い
  - CCoE としても、AWS に関する施策を重点的に進めてきた
    - セキュリティに関する施策
      - セキュリティ系サービスの利用など
    - コスト最適化に関する施策
      - 事前購入など
- Google Cloud もデータ分析の領域で使われてきた
- 最近になり Google Cloud をメインで使ってサービスを提供する事例が出てきている

Visional の
Cloud Center of Excellence

A CCOE is a centralized governance function for the organization and acts in a consultative role for central IT, business-unit IT and cloud service consumers in the business. A CCOE is key to driving cloud-enabled IT transformation.

Gartner: Set Up Your Organization for Cloud Adoption Success

Cloud Center of Excellence

“ 特にエンタープライズ企業において、クラウドによってより推進されるテクノロジーの運用を進化させるため、ベストプラクティスやフレームワーク、ガバナンスを作成・伝導・制度化するための専門の人材を集めたチーム ”

参照：Google Cloud Japan が CCoE（Cloud Center of Excellence）研究分科会を発足

簡単にいえば

企業内でクラウドを推進していくための仕組みやベストプラクティスを整え広めていく専門チーム

Visional の Cloud Center of Excellence の成り立ち

2018年

プラットフォーム基盤推進室が立ち上がる。プロダクトの**非機能要件改善**を目的とする

2019年

AWS について、横断的なプラットフォームとして**ガードレールの整備**を開始

2020年

活動の主体はほぼクラウドになり、**CCoE というあり方**への指向性が生まれる

2021年

改めて CCoE の組織として再始動

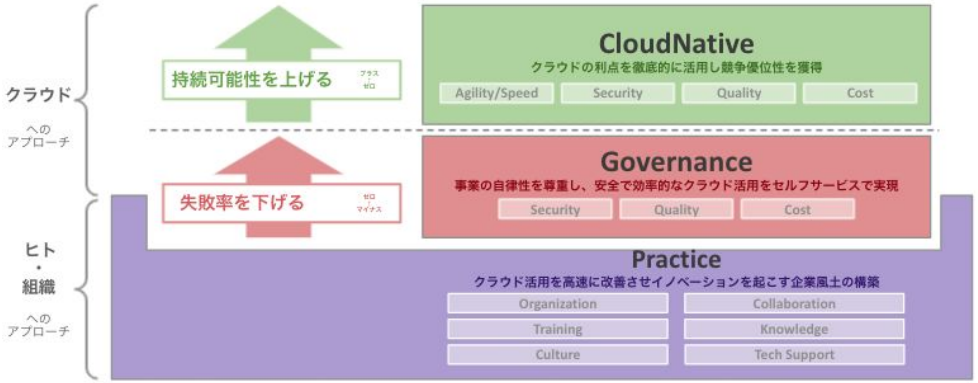
ガバナンスを主軸として、**Google Cloud のガードレール構築**にも着手

将来

ガバナンス/セキュリティだけでなく、**グループ全体のクラウドネイティブ化を実現**

Visional の Cloud Center of Excellence

- Visional のクラウド戦略を推進しその戦略を事業に適用するための組織
  - 直接的な価値ではないところを CCoE は進めて、事業部の自走を助ける
- Mission「CCoE として Visional の持続可能性を上げ失敗率を下げることを推進し続ける」
  - **持続可能性を上げる** - ゼロからプラスへ クラウドの利点を徹底的に活用
  - **失敗率を下げる** - マイナスからゼロへ 事業の自律性を尊重し、安全で効率的なクラウド活用をセルフサービスで



Visional の Cloud Center of Excellenceの構成

Cloud Business Office と Cloud Platform Engineering

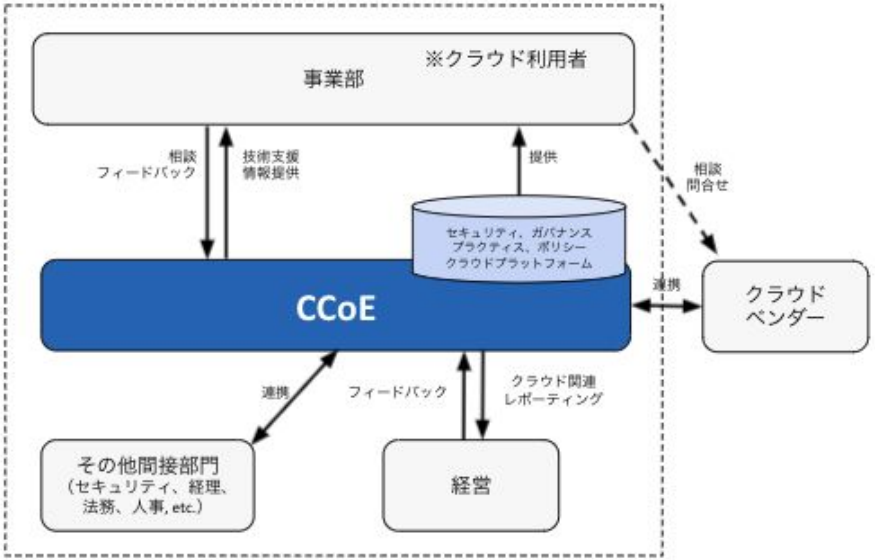
- Cloud Business Office
  - 事業や他のステークホルダー(経営、セキュリティ、財務、法務、人事等) からの要求と、CCoE が提供する基盤や Visional としてのクラウド戦略を連携させる役割
- Cloud Platform Engineering
  - ガバナンス要件の準拠と、クラウドを活用した事業・プロダクト開発の加速を両立させるために、コード化された標準や環境・基盤を提供する役割

Visional CCoE の役割

各ステークホルダーとのハブになり様々な連携を行う

- クラウド戦略計画・推進
- 事業部への技術支援・情報提供等のサービス提供
- 経営へのレポーティング
- 内部プロセス連携のための間接部門調整
- クラウド ベンダーとの連携
- ナレッジ管理
- クラウド運用ポリシーに即した組織的管理
- トレーニング

など



Visional CCoE の役割

- **ガバナンスを主軸とした施策の遂行**
  - **セキュリティ ガードレール整備**
  - コスト中央管理
    - 会社のプロセスに沿った購買/精算の集約管理・代行
    - 全社レベルでの事前購入の検討・調達
  - クラウド管理
    - アカウント・プロジェクトの払い出し・削除
    - アカウント・プロジェクトの棚卸し
- 最適なクラウド利用を目指すクラウド ネイティブを主軸とした施策の遂行
  - 将来的な注力項目

Google Cloud におけるガードレールの検討

CCoE としてのスタンス

事業のガバナンスと自由度のバランスをとった戦略遂行

Agility | Agility か Governance か、どちらか一方を選ぶのはない | ***Governance***

クラウドを活用してAgility とGovernance を両立する

クラウド利用の自由度をできるだけ損なわない

- How で縛らない
- 価値で縛る

リスクの高い箇所など、ルールを適用して管理

- “防御” はリスクの高い箇所に限り適用する
- “検知” は徹底的に取得する
- “回復” は事業部側で判断
  - ただし、その状態は正しく把握する

セキュリティガードレール

- **プロジェクトに対して硬すぎる制限を設けるのではなく、可能な限り自由を確保しつつ望ましくない領域のみ制限、または発見するソリューション**
  - 「ゲート」によるブロッカーとなる制御ではなく、「ガードレール」として利用ルールを定義し、ルールにそぐわない操作の制限と危険な設定・挙動を検出することで、**アジリティを維持しながらガバナンスコントロールを実現**することができる
- ガードレールには 2 つの種類が存在する
  - **予防的ガードレール (制限)** : 対象の操作を実施できないように制限するガードレール
  - **発見的ガードレール (検知)** : リスクがあるリソース設定を検知するガードレール
    - 発見後に自動に訂正を行う**訂正的統制**に派生も

ガードレールの必要性

- Assured（β 版提供中）では、できるだけ早い事業成長を実現していくために、以下の要素を重視していた
  - 作り替えがしやすい環境である
  - マルチテナンシー・アーキテクチャと親和性が高い
  - 事業初期からデータ蓄積および分析が容易である
- 技術選定の結果、Google Cloud をメインで使うことに
- AWS ではガードレール施策の整備が進んでいたが、Google Cloud では存在しない
  - 同じような要件を満たすためには事業部が各所と調整しなければならなかった
- 今後の事業立ち上げ・運営を円滑にしたい
  - 今のままでは新規事業が立ち上がり、Google Cloud を使いたくても使うハードルが上がってしまう
  - Google Cloud のテクノロジを使用できないのは機会損失が大きい
  - 技術選定の柔軟性向上だけでなく、AWS 一本化のリスクを避ける上でも意義がある

ガードレールに期待すること

- AWS のガードレールでは以下が実現できていた ※
  - 発見的ガードレール
    - アカウントやワークロードに対する脅威検知
    - セキュリティリスクの高い構成設定の検知とその可視化・改善活動
  - 予防的ガードレール
    - 各アカウントで禁止したい一部の操作を、組織全体の禁止ポリシーとして権限を制限し予防
    - クラウドの監査ログ設定を統一し、一箇所に集約してログの完全性を保証
- ガードレールを実現するための仕組みとして
  - 組織のアカウントの一元管理
  - アカウントに対するベースライン設定を保証する仕組み

※ 100を超えるAWS アカウント運用におけるガードレール構築事例
https://engineering.visional.inc/blog/171/awssummit_securityguardrail/

Google Cloudではどこまでやればよい？

- AWS と同じように使ってもらうには AWS のガードレール機能で払拭されている懸念を同じように解消したい
  - プロジェクトやワークロードに対する脅威検知
    - Security Command Center Premium Tier
      - Event Threat Detection、Container Threat Detection
  - セキュリティ　リスクのある構成設定の検知とその可視化
    - Security Command Center Premium Tier
      - Security Health Analytics
  - 各プロジェクトでは禁止したい一部の操作を禁止ポリシーとして反映して予防
    - 組織のポリシー
  - クラウドの監査ログを統一し、一箇所に集約してログの完全性を保証
    - Cloud Audit Logging
- 同じようなものはできそうだけど、本当にそれで十分か？
  - 何か気にするポイントを網羅できるガイドラインが欲しい...

Google Cloud security foundations guide

- “安心して Google Cloud にワークロードをデプロイするためのセキュリティ保護を構成するためのガイド”
  - Google 独自の考え方に基づく一つの観点が示されている
  - オンプレミスと Google Cloud を併用しているハイブリッド クラウド環境での構成を例として説明されている
  - 右のような、セキュリティ基盤のアーキテクチャとしての意思決定のポイントが示されている
- ガイドが示されることにより、考慮するポイントを網羅できる安心感がある

3. Google Cloud foundation design

3.1) Key architectural decisions

The example.com reference architecture that's described in this document is based on certain architectural decisions; if you need to make changes to those assumptions, the example.com architecture also needs to be modified. Table 2.3.1 lists architectural decisions.

Decision area	Decision
Organization structure	A single organization is used for all environments and services for example.com to manage all resources and policies in one place.
	The folder hierarchy has a single layer, consisting of bootstrap, common, production, non-production, and development folders to allow for segregation of policies, privileges, and access.
	Google Cloud organization policies are used to augment the organization's security posture by allowing you to define resource configuration constraints that apply consistently across all projects.
Resource deployment	Foundation resources are deployed through a deployment pipeline to enable automated and standardized review, approval, and rollback.
	Terraform is used as the infrastructure as code (IaC) tool.
	An on-premises Git repository is used as a source repository for the Terraform modules.
	The deployment pipeline's actions are initiated from the on-premises environment.
	An approval stage in the pipeline is needed to deploy resources.
	Workloads are deployed through separate pipelines and access patterns.
Authentication and authorization	Google Cloud federates with the example.com on-premises Active Directory identity management system.
	Single sign-on (SSO) is used to allow users to log into Google Cloud.
	A firecall process is used to provide elevated access to the Google Cloud environment.
	Groups are used for assigning Cloud IAM permissions.

https://cloud.google.com/blog/ja/products/identity-security/google-cloud-security-foundations-guide

Terraform ブループリント スクリプト

- 安全な Google Cloud を利用するための基盤実装例
  - Google Cloud security foundations guide に従っている
  - Terraform で実装したサンプル コード
  - スクリプトを出発点にして、独自の基盤の構築を開始できる
- スクリプト
  - Google Cloud Organization を管理するためのリソース群
    - ブループリント スクリプト自体のプロビジョニング 機構
    - 組織ポリシー、DNS ハブ、ネットワーク ハブ、組織レベルのログ等の実装例
  - 環境に基づくフォルダ分け、プロジェクト作成の自動化コード例
  - 各プロジェクトへのデフォルトとしてネットワーク・CI/CD メカニズム等リソースの配備
- Terraform の google プロバイダで用意されていないリソースをコード化する手法も
  - null_resource を使った実装

https://github.com/terraform-google-modules/terraform-example-foundation

検討した・していること

- 単一の組織か複数の組織か
- フォルダ階層分け
- リソースのプロビジョニング方法
- 構成管理の方法
- コードをどこで管理するか
- ユーザの ID 管理方法
- どんな ID のアクセスを許可するか
- プロジェクトの権限をどこまで利用者に渡すか
- 組織レベルの権限をどう管理するか
- オンプレミスとの接続が必要か
- 共有 VPC を構成するべきか
- VPC Service Controls をどのように使うか
- 組織レベルでの秘密情報
- 監査ログをどのように使用するか
- 監査ログをどうやって保証するか
- Security Command Center で有効にするサービス
- 検知した際の対応をどのように行うか
- 対応してもらうためにどのような通知が効果的か

ガードレール構想
実装上の意思決定・実現したこと

ガードレール構想

- 組織管理
  - 組織構造
  - ID・認証
  - ガードレールリソースのデプロイ
  - ネットワーク
- ガードレール
  - 予防的ガードレール
    - 組織ポリシーの適用
    - （監査ログの保証・集約・保管）
  - 発見的ガードレール
    - セキュアでないリソース構成のチェック
    - （データやワークロードに対する脅威の検知）

01 組織管理

組織管理　組織構造

単一の組織配下で社内の全てのプロジェクトを管理する

- Google Cloudとしても複数組織の管理は推奨でない ※
- 組織を複数に分けると、Security Command Center の Premium Tier 利用やサポート契約上不利
- Google Workspace を利用しており、社内のプロジェクトをその組織配下に集めることはできていた。運用を煩雑にしてまで分けるメリットがない

フォルダ分けは必要になってから行う

- フォルダ分けしてポリシーを分けたり、権限を管理することはできる
    - ただし運用を確立してからでないと収拾がつかなくなる
- 現状ではプロジェクト単位の管理で問題ない状態であり、分けるメリットがない
- 全プロジェクトを組織直下に配置

※ https://cloud.google.com/resource-manager/docs/managing-multiple-orgs?hl=ja

プロジェクトの権限・管理責任

- 事業で使用しているプロジェクトの管理はそれぞれの事業で行っている
  - プロジェクトのオーナーとして権限を与え、管理責任を持ってもらう
  - ガードレールが整っていれば自由に使わせられる
- 各プロジェクト用に CI/CD を用意することもしない
  - 構成管理はそれぞれのやり方がある
  - 標準を用意しても使い勝手が悪ければ使ってもらえない

組織レベルの権限

CCoE やセキュリティ室などの管理監督を行う部署のメンバーのみ、必要に応じて最小権限を付与する。各事業のエンジニアには組織レベルの権限を付与しない

- 特に、プロジェクトを自由に作成させないように
  - 作った本人も忘れてしまうプロジェクトをこれ以上増やさない
  - 誰も知らないプロジェクトを棚卸しするコストは大きい
- 組織レベルの権限は配下のプロジェクトにも継承されるため、事業に特有の機微情報などが不要に知られてしまい、リスクが高まる恐れもある
- 費用管理の都合上、請求先アカウントを管理するメンバーを限定する

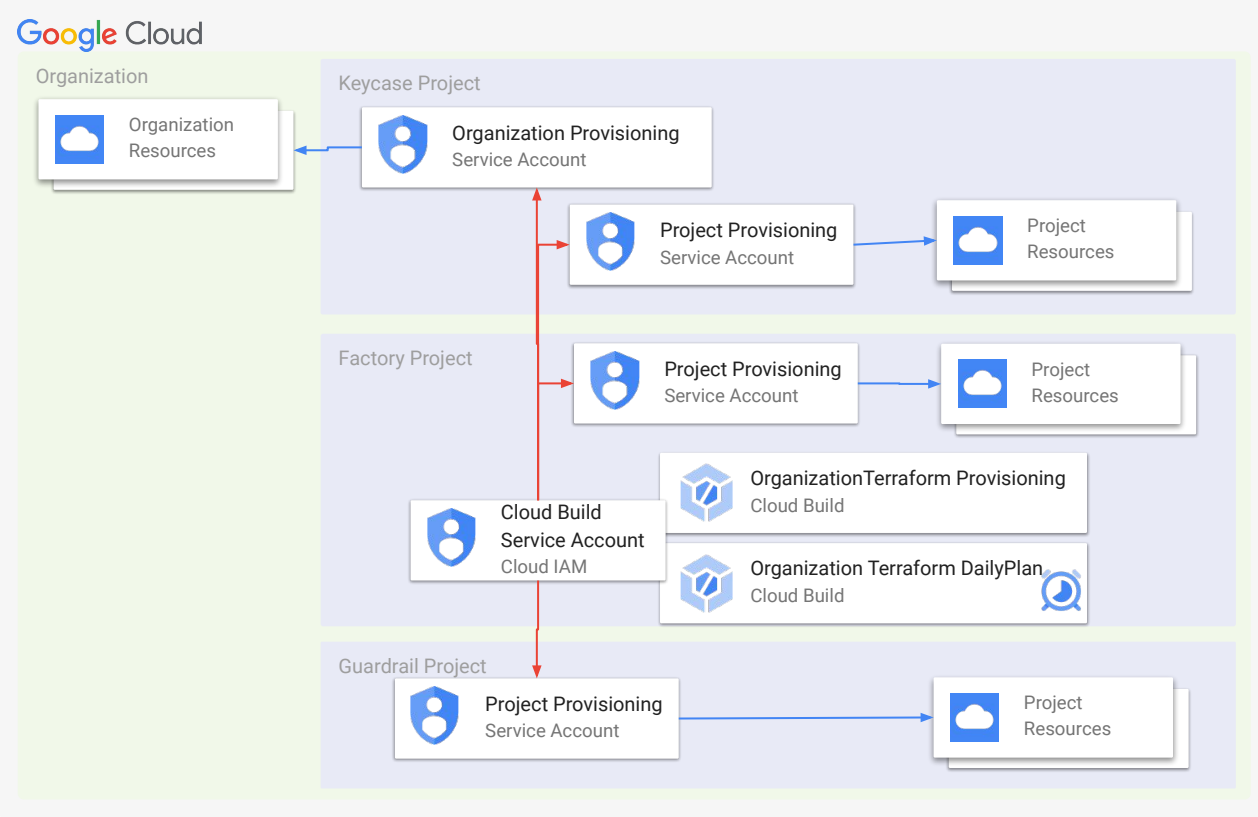
組織管理用プロジェクト

組織管理用（ガードレールも含む）のプロジェクトと組織レベルのリソースを Terraform を使用した IaC で定義し、Cloud Build によりプロビジョニングする

- 組織管理用のプロジェクトとして3プロジェクトを用意
  - keycase project
    - 特に守るべき組織上の重要なSecretおよび権限の管理
  - factory project
    - 組織管理用プロジェクトと組織に対するプロビジョニングの仕組み
  - guardrail project
    - ガードレールの各種メカニズム

プロビジョニングの仕組み

- factory project の Cloud Build でTerraform を動かし、3プロジェクトと組織への設定を行う
- factory project の DailyPlan にて、毎日構成のドリフトをチェック
- keycase project には強力な組織レベルの権限があるのでプロジェクトを分け、IAM ポリシーを厳格に管理



組織の ID・認証

- ガードレール検討前から、Active Directory と連携して社員の ID 管理がされており、同一 ID で Google Cloud に Single Sign On できるようになっていた
  - 退職者の ID が有効なままという事態は避けられていた
- 一方で組織のドメイン以外のドメインのメール アドレスに権限が付与されている事例があった
  - gmail.com のメールアドレスなど
  - 退職処理で ID を無効化しても gmail.com の ID に認証できれば引き続きアクセスできてしまう
    - 組織ドメイン外の ID の使用は禁止したい

ネットワーク

- ネットワーク アーキテクチャを**中央管理はしない**
  - サービスのネットワークについてもサービスを運営する事業が責任を持っている
  - オンプレミス環境がないため、ネットワークトポロジを管理したいという要求はなかった
- とはいえ、セキュアに利用してもらうように構成をチェックしていく
  - VPC フローログ はモニタリングや脅威検知に重要
  - 適切な設定かどうかを**発見的ガードレール**でカバー
- この辺りの意思決定は会社による。**弊社の事情では**中央管理していない
  - オンプレミス環境がある場合
    - Shared VPC を中央管理して Dedicated Interconnect を構成
  - BigQuery や Cloud Storage に対する防御をより強固にしたい場合
    - VPC SC を組織的に構成
- 今後 Hierarchical Firewall でファイアウォールルールを管理する可能性はある

02

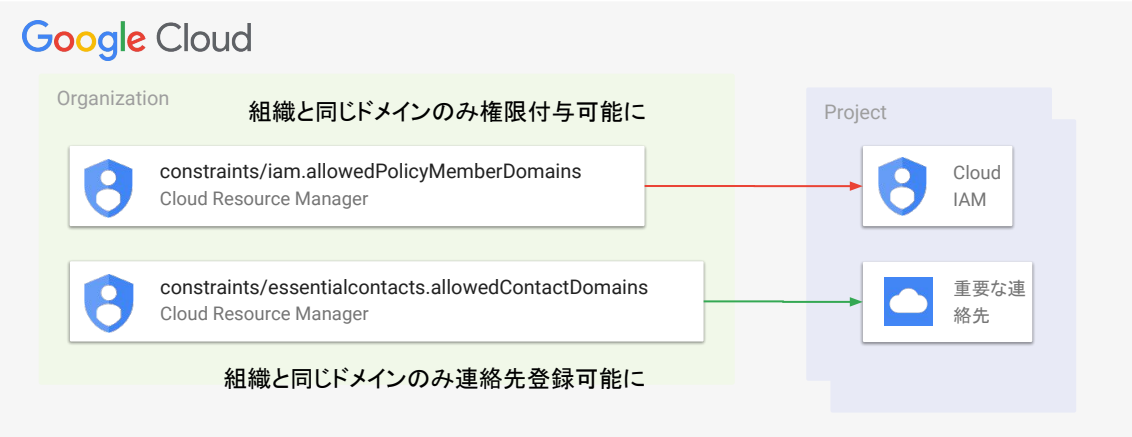
予防的ガードレール

組織のポリシーについて

- 設定できるポリシーの種類はたくさんある（60 種類以上）
- ポリシー一覧から自分たちに適したポリシーを適切に選定するのはかなり難しい
  - ポリシーの背景、設定したい状況を全て理解するのは困難
  - マイナーなサービスに関する制約もある
- ポリシーの一覧から選定するよりも、何か制限したい状況がわかった場合に組織のポリシーに制限できる機能があるかどうかを探した方が良い
  - 使えそうなポリシーがあったとしても、要求にジャストフィットするとは限らない

組織のポリシーの適用

- ドメインで制限された共有 constraints/iam.allowedPolicyMemberDomains
  - 各種リソースの IAM ポリシーのプリンシパルに追加できる ID のドメインを制限する
  - ドメインと対応するGoogle Workspace 顧客 ID を指定して制限できる
- ドメインで制限された連絡先 constraints/essentialcontacts.allowedContactDomains
  - [重要な連絡先] に追加できるメールアドレスのドメインを制限する
  - ドメイン名で制限できる



組織のポリシーについて

「ドメインで制限された共有」の制約には注意点がある

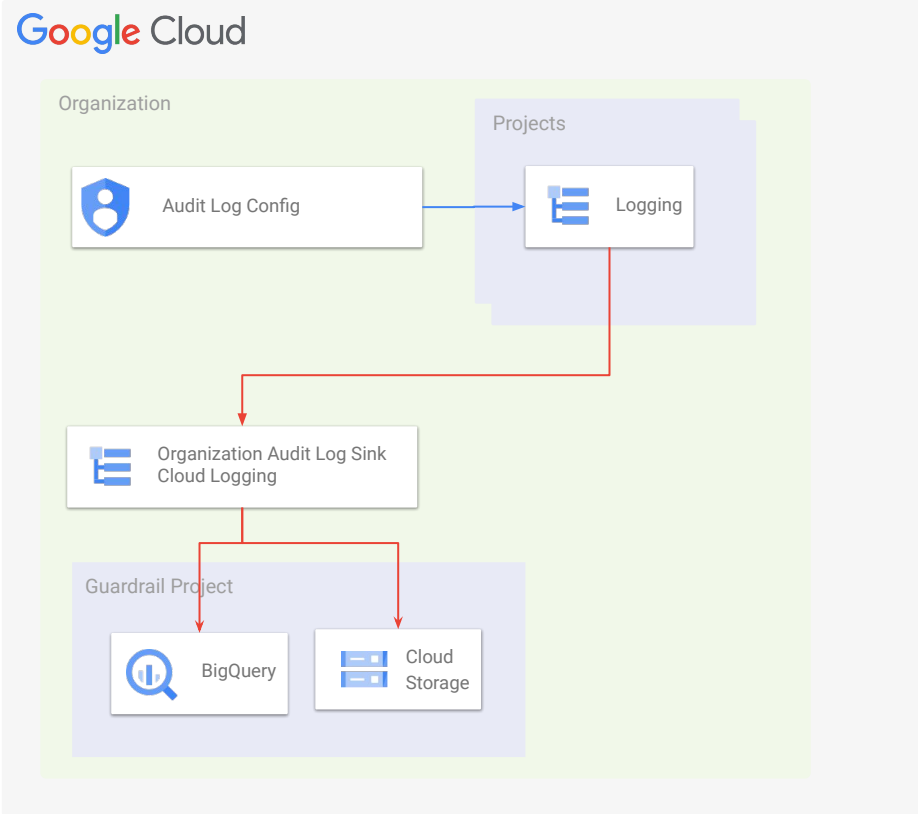
- Google が提供するサービスのサービスアカウントの登録がはじかれることがある
  - Google Analytics のデータを BigQuery にエクスポートするときなど
- 対処法は以下
  - ポリシーを外し、必要なエクスポート設定を行い、ポリシーを元に戻す
  - サービスアカウントをグループに追加し、グループに権限を持たせる
- 都度対応が必要になりガードレールの思想的には合わない...
  - 「ドメインで制限された共有」は使用しない
  - 発見的ガードレールとして実装するように**方針を変更**した

監査ログの保証・集約・保管

- Event Threat Detection (SCC Premium) で検知項目を利用するために有効にするべき監査ログを組織レベルで強制する
  - 組織レベルで設定すれば個々のプロジェクトでは無効化を制限できる
  - 全てのデータアクセス監査ログを取得設定することはしなかった
    - 各プロジェクトへのコスト負担が大きくなる
    - 変更ログと、権限周りの読み取りログがあればまずは十分
    - 集約先のストレージコストも膨らむ。取得しても見きれない
- 各プロジェクトの監査ログを一箇所に集約してログの完全性を保証
  - 完全性の確保のために Cloud Storage の機能を使ったり、BigQuery のデータセットに対する変更オペレーションを監視したりなどの追加の措置
    - 内部不正の可能性に対する対策

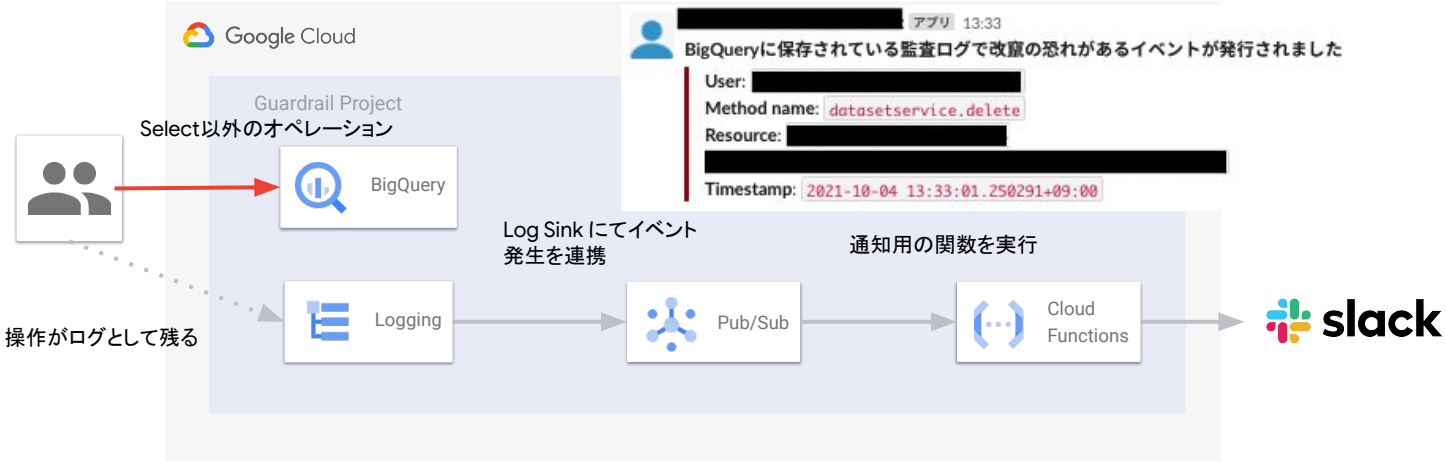
監査ログの保証・集約・保管

- Audit Log Config
  - Resource Manager
  - IAM
- Organization Audit Log Sink
  - logName:cloudaudit.googleapis.com
  - includeChildren
- Cloud Storage
  - 保持ポリシーでバケットロック（内部不正対策）
- BigQuery
  - 独自の改竄検知の仕組みを実装（内部不正・侵入時の対策）



BigQuery への変更操作に気づく

- BigQuery の監査ログから検知して Slack に通知
  - ログシンクのフィルタで対象のイベントを監視
    - 監査ログ集約データセット・テーブルに対する削除API発行
    - Select 以外のクエリ
  - Pub/Sub 経由で CloudFunction を起動し通知



03 発見的ガードレール

Security Command Center Premium Tier

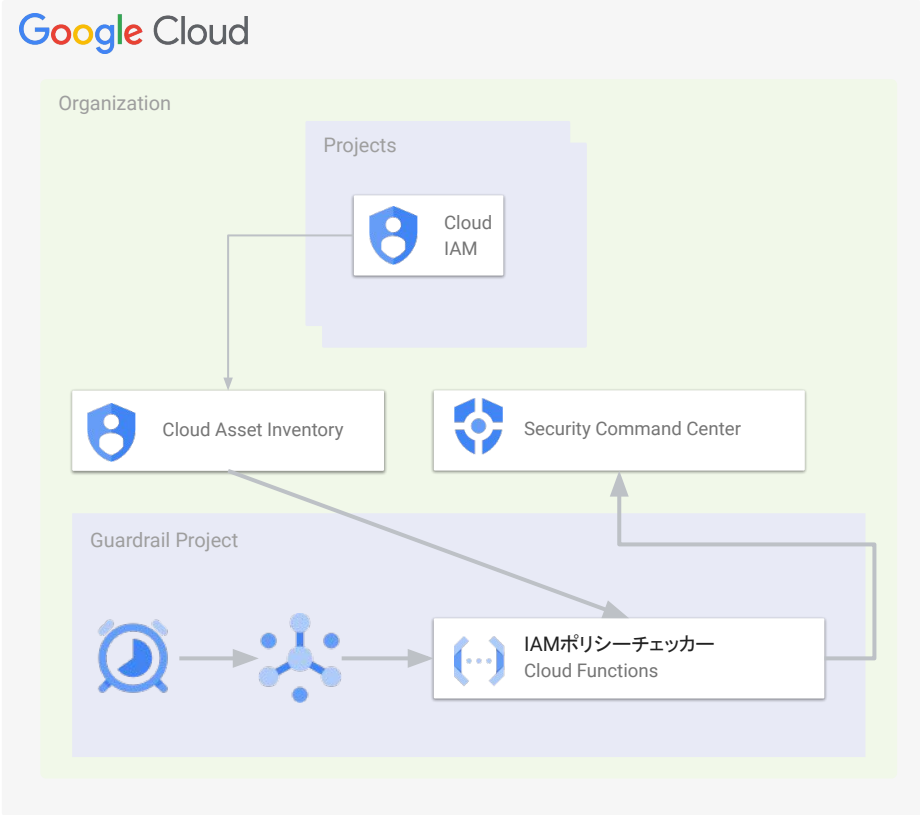
- マネージドな検知項目を多数提供してくれる
  - CIS 1.1 や PCI DSS v3.2.1 などの基準にそった検知項目
  - 自分で検知項目を実装する手間が省ける
- プロジェクト レベルでのダッシュボード閲覧権限が付与できる
  - 提供されているダッシュボードの完成度はかなり高く、別途用意する必要がない
  - 各個社間でリスク情報を制限したかった
  - ダッシュボードをプロジェクト個別に確認でき、事業部各自で改善に集中できる
- 最低利用料金が設定されている
  - スタートアップの一事業で負担するには高い
  - 事業横断的なレイヤーで契約のための意思決定が必要

セキュアでないリソース構成のチェック

- Security Health Analytics (SCC Premium)
  - マネージドなチェックルールについて、デフォルトの設定で検知データを収集した
    - 有効化が必要な一部ルールは利用していない
  - リスクを素早く洗い出すことができ、致命的な問題がないことを確認できた
- カスタムの構成チェックルール
  - Cloud Asset Inventory のリソース情報と合わせた
  - Security Command Center に独自のセキュリティソースを定義し、知見として作成
- 通知は検討中
  - 単に通知しても対応する側は難しい
  - どう言った単位で通知すると効果的なのかを考えている
- 提供してくれる検知項目のうち、どれを重視してどのように対応していくかは自分たちに合わせて考えていく

カスタムの構成チェック ルール

- ドメイン外の IAM ポリシーのメンバーの登録を検知するルール
- Cloud Asset Inventory に各リソースの IAM ポリシー情報が集約されている
- ルールをチェックする CloudFunction を設定し、Cloud Asset Inventory から IAM 情報を取得
- ドメイン外の IAM ポリシーが見つかったらSecurity Command Center の Findings として登録
- Security Command Center を見ればマネージド・カスタム問わず検知が集約されている状態



データやワークロードに対する脅威の検知

- Event Threat Detection
  - 各種ログを取得することで 24 種類の脅威を検知
  - 監査ログの保証しているので 検知に必要な監査ログを利用できるようにしている
  - その他 VPC フロー ログやファイアウォール ルールのログも今後確認していく
    - リソース構成のチェックの方で未設定を指摘し、事業部に改善を求めていく
- Container Threat Detection
  - Kubernetes クラスタで実行中のコンテナに対する 4 種類の脅威を検知
  - 組織レベルで有効化済み
  - クラスタが Google API と通信できる必要がある
    - リソース構成のチェックの方で未設定を指摘し、事業部に改善を求めていく

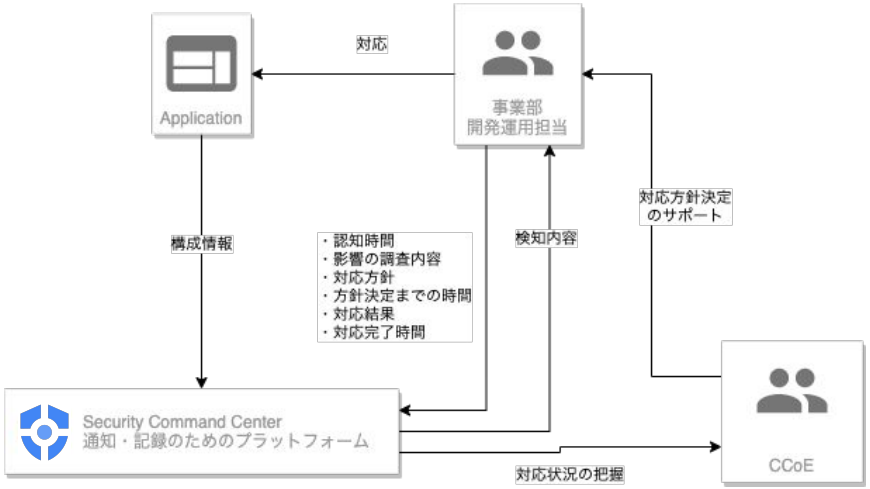
今後の展望

Security Command Center をより使いこなす

- Security Health Analytics
  - 自分たちにとって重要な検知とそうでない検知を仕分け、重要な検知をSecurity Command Center のダッシュボードで確認できるようにしたい
    - 事業部の対応コストも下がる
- カスタムの構成チェックルールを拡充
  - マネージドでルールが存在しないがチェックしたい場合・マネージドのルールとは別の評価をしたい場合
- Web Security Scanner
  - CCoE がスキャン対象のプロジェクトを把握できていない
    - プロジェクトの棚卸しを進行中
  - 今後使っていきたい

Security Command Center の検知項目への対応体制構築

- 事業部のプロダクト開発と検知項目対応のバランスをとる
  - 検知項目に対応していくためのプロセスを構築
    - 事業部側の対応の体制
    - 対応内容の評価・モニタリング
    - 検知項目の改善だけでなく運用の改善
- プロセスに基づいて対応の状況を把握できる仕組みの構築を検討中
  - Security Command Center の Findings のステータスと連動して Jira や Asana などでタスク管理など



Recommenderを使いこなす

- セキュリティだけではない、より Google Cloud を使いこなすための推奨事項が提供される
  - クラウドの最適化を通じて Cloud Native に近づけたい
  - 直近ではコスト最適化
- 不要なプロジェクト・不要なリソースを発見することによるコスト最適化
  - 放置プロジェクト Recommender
  - アイドル状態リソースの Recommender
- 全社視点でのコスト最適化
  - 確約利用割引 Recommender

まとめ

Cloud Center of Excellence

- 組織横断的にクラウドの効果的な利用を推進
- 専門チームとして仕組みやベストプラクティスを整える
- CCoE内部でも役割分けがある。エンジニアリングのスキルだけでなく、関係各所との調整のスキルも必要
- 役員や他部署からのスポンサーシップがCCoEの影響力を高める

セキュリティガードレール

- ガードレールという思想によって自由でアジリティ高い開発と守るべきところを両立
- CCoEがガードレールを敷くことによって、事業部のセキュリティ対策の負担を減らし、本質的な価値の追求をサポート
- それぞれの会社の状況に合わせてガードレールの要件は異なる

Google Cloud のセキュリティサービスの効果的な利用

- Security Command Center により検知・可視化を効率的に行える
- Google Cloud security foundations guide を軸にすることで、セキュアに Google Cloud を利用するための基盤を網羅的に検討できる

Thank you.

We're hiring! ▶
募集職種の詳細はこちら（採用サイト）
https://www.visional.inc/ja/careers.html