Google Cloud ホワイトペーパー
2020 年 8 月

Google Cloud セキュリティ基盤ガイド

Google Cloud

I. セキュリティ基盤ブループリント

免責条項: このドキュメントの内容は、2020 年 8 月時点のものです。このホワイトペーパーは、執筆された時点での現状を取り上げています。Google は継続的にユーザーデータの保護の強化を進めており、今後、Google Cloud のプロダクトとサービス、セキュリティ ポリシー、システムは変更される可能性があります。

はじめに

さまざまな企業でクラウドの導入が進んでいます。多くの企業は、パブリック クラウド インフラストラクチャの使用を検討する段階を終え、実際にパブリック クラウド経由で本番環境サービスを顧客に提供し始めています。パブリック クラウドにおけるセキュリティは、お客様とクラウド プロバイダがセキュリティに関する責任を分担するという点で、お客様が所有するインフラストラクチャのセキュリティとは異なる部分があります。図 1.1 は、クラウドのワークロードに対するセキュリティの責任分担を示しています。

図 1.1 セキュリティの責任分担

Google Cloud のプロダクトとサービスは、従来の Platform as a Service（PaaS）から、Infrastructure as a Service（IaaS）、Software as a Service（SaaS）までさまざまです。Google Cloud で提供されるサービスの種類は日々増加しているため、**まず信頼性と安全性の高い基礎を確立してから**、サービス固有のセキュリティ ガイドの内容に進むことが重要になっています。図 1.1 に示すように、お客様とクラウド プロバイダの間の責任の境目は、選択したサービスによって変化します。セキュリティに関する責任分担の一部として、パブリック クラウド プロバイダは最初に堅牢で安全な基盤をお客様に提供する必要があります。その次に、プロバイダは、お客様が責任分担モデルの分担範囲を理解し、責任を果たすことができるように支援します。

最初からセキュリティを考慮する

クラウド セキュリティは、次のような理由でオンプレミス セキュリティと異なります。

- インフラストラクチャ内、プロダクト、サービスの間でセキュリティの基本原理、可視性、制御ポイントが異なる。
- 新しいクラウドネイティブな開発手法（コンテナ化、DevSecOps など）。
- 新しいクラウド プロダクトやサービスの種類、内容の加速的な増加と利用方法の多様化。
- 組織がシステムをデプロイ、管理、運用する方法といった文化の変化。

クラウド デプロイメントをセットアップする際に、お客様は多くの「決めておくべきこと」があります。お客様がビジネス インパクトと価値を顧客に迅速に提供できるようにするために、デフォルト設定がセキュアであるワークロードを、簡単、迅速、効率的にデプロイするための支援が必要です。しかし、従来とは異なるクラウド移行の新たな課題に対処するための必要な新しいスキルを習得する時間はないかもしれません。そこで、安全な基礎から始め、お客様それぞれのニーズに合わせてカスタマイズするための推奨事項を整理したガイドがあると便利です。

セキュリティ ブループリントは、そういったお客様のために作成されました。これを利用すれば、Google Cloud を基盤としてより迅速かつ効率的、安全に構築し、Google Cloud のセキュリティ階層に新しい重要なレイヤを追加できます。現時点では、合計で 4 つの主要なレイヤがあります。まず基盤である Google Cloud のコア インフラストラクチャを見ていきます。残る 3 つのレイヤは、「Google Cloud プロダクトとサービス」、「セキュリティ基盤のブループリント」、「セキュリティ体制、ワークロード、アプリケーションのブループリント」です。各レイヤはその前のレイヤを基にしています。

Google Cloud のコア インフラストラクチャ

Google にはグローバル規模の技術インフラストラクチャがあり、これは Google の情報処理ライフサイクル全体でセキュリティを確保できるように設計されています。このインフラストラクチャにより、サービスの安全なデプロイ、エンドユーザーのプライバシー保護を備えたデータの安全な格納、サービス間での安全な通信、インターネット経由の顧客との安全な非公開通信、管理者による安全な操作が可能になります。Google Cloud サービスはこのインフラストラクチャを基に構築され、BeyondProd ホワイトペーパーに記載されたクラウドネイティブなセキュリティ原則に従って一貫性のある形で運用されています。

Google プロダクトとサービス

Google Cloud プロダクトは、BeyondProd ペーパーで概説されている手法と原則に基づき、セキュリティを考慮して設計されています。組み込みのセキュリティ機能により、アクセス制御、セグメンテーション、データ保護が可能になります。さらに Google Cloud で構築された固有のセキュリティ サービスは、お客様のポリシー要件を満たすだけでなく、重要なアセットを Google のサービスや機能で保護するために役立ちます。

セキュリティ基盤ブループリント

セキュリティ基盤ブループリントは、推奨事項を整理し、ガイドとそれに付随する自動化スクリプトを提供することで、お客様がはじめから Google Cloud デプロイメントをセキュアな形で始められるように支援することを目的としています。このセキュリティ基盤ブループリントの内容は次のとおりです。

- Google Cloud の組織構造
- 認証と認可
- リソース階層とデプロイメント
- ネットワーキング（セグメンテーションとセキュリティ）
- ロギング
- 発見的コントロール
- 請求のセットアップ

セキュリティ体制、ワークロード、およびアプリケーションのブループリント

強固なセキュリティ基盤に加え、セキュリティ体制、ワークロード、アプリケーションに関する追加のブループリントを示します。これは推奨事項を整理したガイドに沿ってお客様がワークロードとアプリケーションを設計、構築、運用できるように支援します。GKE 上の PCI のブループリントおよび Healthcare Data Protection Toolkit などの例を示します。

図 1.2 に、Google Cloud を使用し、セキュリティ ブループリントで提供されるガイドとテンプレートに従うことで利用できる構築の基礎としてのセキュリティ レイヤを示します。

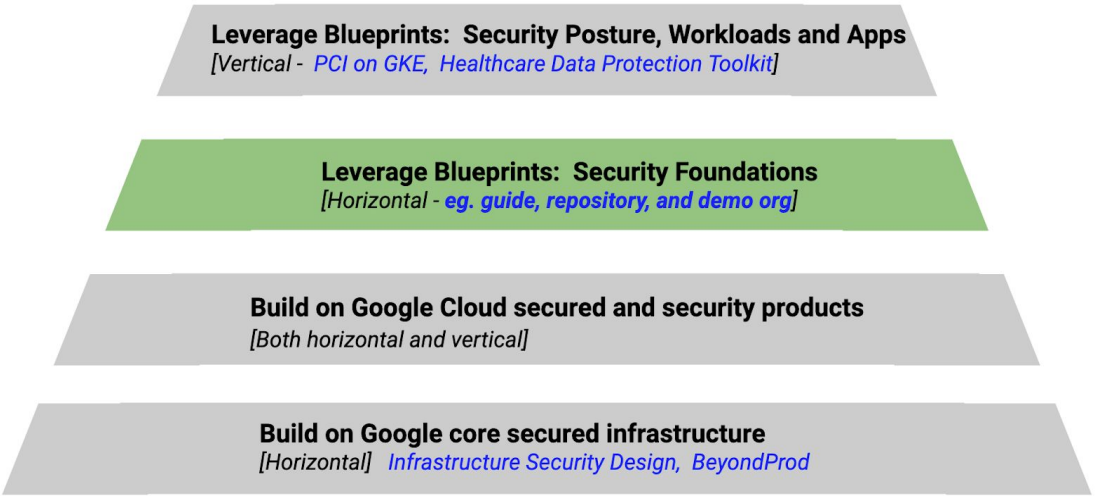


図 **1.2** Google Cloud のセキュリティ階層

セキュリティ基盤ブループリントから始める

このガイドでは推奨されるセキュリティ基盤ブループリントを示し、Google Cloud 利用環境を構成およびデプロイする方法を説明します。このドキュメントでは、考慮すべき重要なトピックを強調して、設計し始める際に参考となるリファレンスとなります。各トピックでは、Google がなぜそれぞれのアプローチを選んだかについての背景を解説しています。このセキュリティ基盤ブループリントでは、手順ガイドに加えて Terraform 自動化リポジトリを提供し、Google 組織の例をデモ用にご紹介します。これによりお客様はブループリントに従って構成された環境を実際に使用しながら学習できます。

このドキュメントこのドキュメントは以下のトピックを扱います。

- はじめに（このセクション）
- 基盤のセキュリティ モデル
- 基盤の設計
- 推奨組織構造を表すサンプル example.com
- リソースのデプロイ
- 認証と認可
- ネットワーキング
- シークレットの管理
- ロギング
- 発見的コントロール
- セキュリティに関する一般的なガイダンス

II. 手順ガイド

1. はじめに

このセクションでは、Google Cloud デプロイメント用のセキュアな基盤を構築するためのガイドを示し、このようなアーキテクチャの例として example.com という組織を見ていきます。図 2.1 に示されているように、ワークロードをクラウドで安全に実行するために推奨される基礎を提供することで、example.com のセキュリティを実現できます。example.com 組織のスクリプト、コード、その他のデプロイメント アーティファクトは terraform-example-foundation GitHub リポジトリにあります。

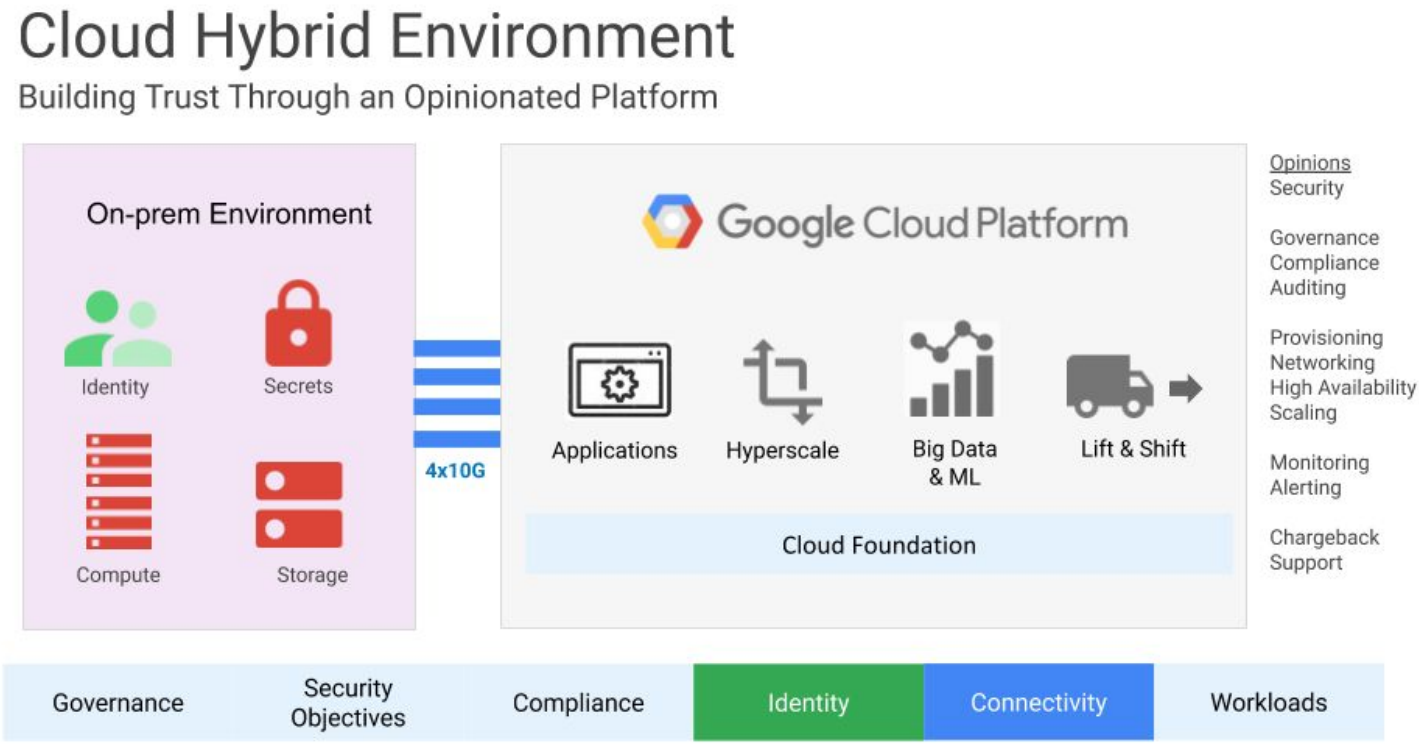


図 **2.1** Google Cloud 推奨セキュリティ基盤

2. Google Cloud 基盤セキュリティ モデル

Google Cloud の基盤におけるセキュリティは、予防的コントロールと発見的コントロールの組み合わせによって実現されています。予防的コントロールには、ポリシーとアーキテクチャによって実現されます。ポリシーは、組織を脅威から保護するプログラムによる一連の制約です。アーキテクチャとは、インフラストラクチャ構造によって組織を保護する方法です。

発見的コントロールとは、組織内の異常な行動や悪意のある行動を検出するためのモニタリング機能です。図 2.2 では、example.com リファレンス アーキテクチャが、セキュリティ モデルにおけるこの 3 つの柱の組み合わせによって形成されていることを示します。

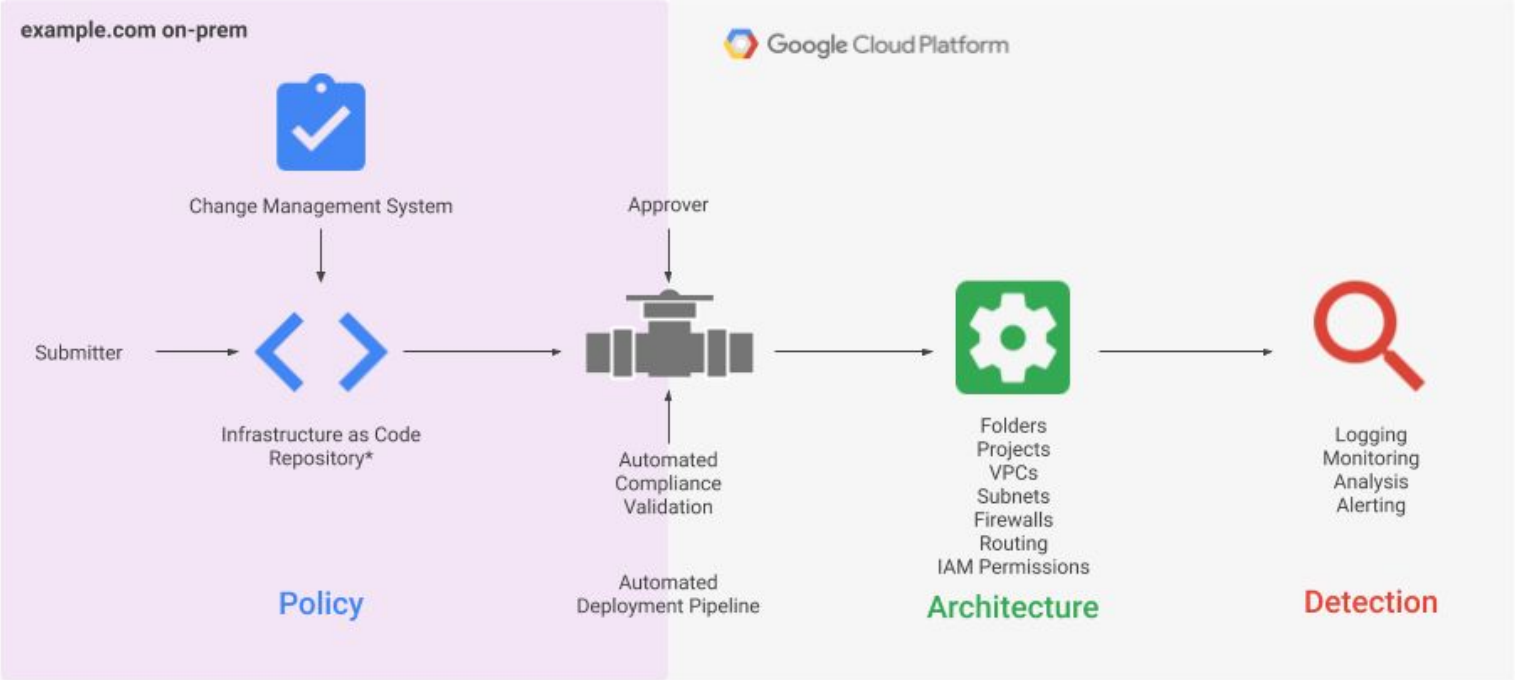


図 **2.2** example.com セキュリティ モデル

セクション 5 で詳しく述べるデプロイメントのベスト プラクティスを実装するには、Google Cloud インフラストラクチャを Terraform モジュールとして体系化し、モジュールをソースコードと同様の管理し、ポリシー検証および承認ステージ付きの自動化パイプライン経由でこれらのモジュールをデプロイします。セクション 6 ～セクション 9 で詳しく述べるアーキテクチャ構造には、Google Cloud 組織のフォルダ構造とプロジェクト構造、接続、ネットワーキング構造、ファイアウォール、アイデンティティ管理が含まれます。セクション 10 で詳しく述べる発見的コントロールは、セキュリティ体制を管理する目的で脆弱性、不適切な構成、悪意のある行動を検出する Google Cloud のプラットフォーム機能です。またセクション 10 ではセキュリティ分析に関する Google Cloud 固有の機能を活用する方法や、Google Cloud 機能とサードパーティ SIEM ツールを統合する方法を見ていきます。

3. Google Cloud の基盤の設計

3.1) アーキテクチャに関する主要な決定

このドキュメントで示す example.com リファレンス アーキテクチャは、アーキテクチャに関するいくつかの決定事項に基づいて作成されています。これらの前提を変更する必要がある場合は、example.com アーキテクチャも変更する必要があります。次の表（表 2.1）に、アーキテクチャに関する決定事項の一覧を示します。

決定領域	決定
組織構造	example.com のすべての環境とサービスを 1 つの組織に含めることで、あらゆるリソースとポリシーを 1 か所で管理します。
	フォルダ階層は単一レイヤで、ブートストラップ（boostrap）、共通（common）、本番環境（production）、非本番環境（non-production）、開発（development）の各フォルダからなり、これによってポリシー、権限、アクセス権の分離が可能になります。
	Google Cloud 組織ポリシーを使用して、すべてのプロジェクトに一貫して適用されるリソース構成制約を定義し、これによって組織のセキュリティ体制を強化します。
リソースのデプロイ	自動化され、標準化されたレビュー、承認、ロールバックを可能にするデプロイ パイプラインを介して基盤のリソースがデプロイされます。
	Infrastructure as Code（IaC）ツールとして Terraform が使用されます。
	Terraform モジュールのソース リポジトリとしてオンプレミス Git リポジトリが使用されます。
	デプロイ パイプラインは、オンプレミス環境から開始されます。
	リソースをデプロイするにはパイプライン内の承認ステージが必要です。
	ワークロードは個別のパイプラインとアクセス パターンによってデプロイされます。
認証と認可	Google Cloud は example.com のオンプレミス Active Directory アイデンティティ管理システムとフェデレーションします。
	ユーザーはシングル サインオン（SSO）を使用して Google Cloud にログインします。
	Google Cloud 環境への昇格アクセスを与えるファイアコール プロセスが使用されます。
	グループを使用して Cloud IAM 権限を割り当てます。
ネットワーキング	Dedicated Interconnect 接続を使用してオンプレミス環境と Google Cloud を接続する構成により、99.99% の SLA を得ます。

	プライマリ ネットワーキング トポロジとして共有 VPC を使用することで、ファイアウォール ルールと接続の一括管理を可能にします。
	VPC Service Controls を使用することで、機密性の高いデータを保管するサービスでは境界保護を提供し、サービスレベルのセグメンテーションを可能にします。
	クラウドおよびオンプレミスからの Google Cloud APIs へのアクセスには 限定公開 IP アドレスが使用されます。
	Google Cloud 用のアドレス割り振りは連続した /16 分の RFC 1918 スペースです。
	Google Cloud では Cloud DNS が使用され、オンプレミス DNS サーバーとの通信には DNS 転送が使用されます。
	タグベースのファイアウォール ルールを使用してネットワーク トラフィック フローを制御します。
シークレットの管理	Google Secret Manager を使用してシークレットを保存します。
	個々の Secret Manager インスタンスを使用して、組織レベルおよびフォルダレベルのシークレットを保存します。
ロギング	組織レベルのログシンクを使用して、ログを集約します。
	ログは Cloud Storage、BigQuery、および SIEM に Cloud Pub/Sub 経由で送られます。
発見的コントロール	エンタープライズ SIEM プロダクトが Google Cloud Logging と統合されます。
	Security Command Center Premium を有効にすることで、不適切なインフラストラクチャ構成、脆弱性、アクティブな脅威行動を検出し、これらの情報をエンタープライズ SIEM ツールと共有します。
	BigQuery 内のログを使用して、Security Command Center Premium による異常な行動の検出を強化します。
請求	しきい値を 50%、75%、90%、95% に設定した請求アラートをプロジェクトごとに使用します。

表 2.1 アーキテクチャに関する主要な決定

3.2) 事前作業

このドキュメントで示すリファレンス アーキテクチャは、次の事前作業が完了しているという前提に基づいています。

- ❏ Cloud Identity のセットアップが完了していること。
- ❏ Google Cloud ドメインの所有権が証明済みであること。
- ❏ 請求先アカウントが設定済みであること。
- ❏ 競合するアカウントが解決済みであること。
- ❏ Dedicated Interconnect 接続のセットアップが完了していること。

詳細については Google Cloud オンボーディングのドキュメントをご覧ください。

3.3) 命名規則

各種 Google Cloud リソースをカバーする標準化された命名規則を使用することをおすすめします。表 2.2 は、example.com リファレンス アーキテクチャにおける Google Cloud 内の要素の名前を作成する際の規則を示しています。表 2.3 は、名前で使用されるフィールド値についての説明です。

注: 中かっこ {} で囲まれたフィールドは任意指定です。

リソース	命名規則
フォルダ	`fldr-environment` 例: `fldr-prod`
プロジェクト	`prj-business-code-environment-code{-project-label}-unique-number` 例: `prj-acde-p-shared-base-43212`
VPC	`vpc-environment-code-vpc-type{-vpc-label}` 例: `vpc-p-shared-base`
サブネット	`sb-vpc-name-region{-subnet-label}` 例: `sb-p-shared-base-us-east1-net1`
ファイアウォール	`fw-vpc-name-priority-direction-action-src-label-dest-label-protocol-port{-firewall-label}` 例: `fw-p-shared-base-1000-i-a-all-all-tcp-80`
Cloud Router	`cr-vpc-name-region{-cloud-router-label}` 例: `cr-p-shared-base-us-east1-cr1`
ルート	`rt-vpc-name-priority-instance-tag-next-hop-{route-label}` 例: `rt-p-shared-base-1000-all-default-windows-activation`
Cloud Interconnect 接続	`ic-onprem-dc-colo` 例: `ic-dal-lga-zone1-1422`
Cloud Interconnect VLAN アタッチメント	`vl-ic-name-cr-name` 例: `vl-dal-da1-zone1-p-shared-base-us-east1-cr1`

グループ	grp-gcp-group-label 例: grp-gcp-billing-admin
ロール	rl-function{-role-label} 例: rl-compute-admin
サービス アカウント	sa-{-service-account-label} 例: sa-p-acde-shared-base-data-bkt-reader
Storage バケット	bkt-project-name{-bucket-label} 例: bkt-p-acde-shared-base-data

表 **2.2** example.com の命名規則

フィールド	説明	値
environment	Google Cloud 組織内のフォルダレベルリソースについての記述。	bootstrap、common、prod、nonprod、dev
environment-code	environment フィールドの短縮形。	b、c、p、n、d
business-code	プロジェクトをビジネス ユニットやグループに関連付けるための 4 文字のコード。	一意に識別される 4 文字のコード。ビジネス ユニットに関連のない共通プロジェクトには zzzz が使用される。
unique-number	グローバルに一意の識別子。	5 桁の整数
vpc-type	確立される VPC ネットワークの種類。	shared、service、float、nic、peer
region	リソースが配置されているリージョン。	任意の有効な Google Cloud リージョン。名前と方位に短縮形が使用されることがあります。 例: Australia（au）、North American（na）、South America（sa）、Europe（eu）、southeast（se）、northeast（ne）。
priority	Google Cloud ルートやファイアウォール ルールの優先度を指定する数値。	詳しくは、ファイアウォール優先度およびルーティング順序をご覧ください。
direction	ファイアウォールが適用される Google Cloud から見たトラフィックの方向。	i は上り（内向き）、e は下り（外向き）

action	ファイアウォール ルールに一致した場合に行われるアクション。	a は許可、d は拒否
src-label	ファイアウォールが適用されるインスタンス ソース ラベル。	all（0.0.0.0/0 を示す）、ソース IP 範囲、またはソースタグのリスト
dest-label	ファイアウォールが適用されるインスタンス宛先。	all、宛先タグのリスト、またはサービス アカウントのリスト
protocol	ファイアウォールの適用対象となるプロトコル。	all、1 つのプロトコル、または複数プロトコルの組み合わせ（tcp、udp、tcpudp など）
port	ファイアウォールが適用されるポートまたはポート範囲。	1 つのポート番号またはポート番号の範囲
instance-tag	ファイアウォールが適用されるインスタンス。	インスタンス タグ
next-hop	ルートでトラフィックが転送されるネクストホップ宛先（該当する場合）。	default、インスタンス ID、IP アドレス、VPN トンネル名、内部ロードバランサ アドレス
onprem-dc	相互接続の接続先であるデータセンターの名前。	お客様により異なる
colo	オンプレミス データセンターからの相互接続がピアリングするコロケーション施設名。	有効な Google Cloud コロケーション施設コード
function	カスタムロールに関連付けられるリソースタイプの名前。	リソースにより異なる
*name	リソースの名前（接頭辞を除く）。	リソースにより異なる
*label	リソースの説明を加えるための記述フィールド。	リソースにより異なる

表 **2.3** 命名規則のフィールド値

4. Google Cloud 組織 example.com の構造

Google Cloud 内にデプロイメントを作成する際の基礎となるのは組織です。Cloud Identity または G Suite をセットアップすることで組織が作成されます。Google Cloud 組織に備わっているリソース階層は、リソースの所有権構造を示し、ポリシーとアクセス制御の接続ポイントを提供します。

リソース階層はフォルダ、プロジェクト、リソースからなり、組織内での Google Cloud サービスの使用方法を定義します。ポリシーは継承され、階層の下位にいるリソースのオーナーはそのポリシーを変更することはできません。フォルダとプロジェクトには、デフォルトで安全な分離が組み込まれています。つまり、すべての外部ネットワークとアクセス権限はデフォルトで拒否されるため、それらを明示的に許可するか、階層の上位レベルからの継承で許可する必要があります。

フォルダ構造は組織の性質やデプロイされるワークロードの種類によって異なります。図 2.3 は、example.com リファレンス アーキテクチャを示しています。

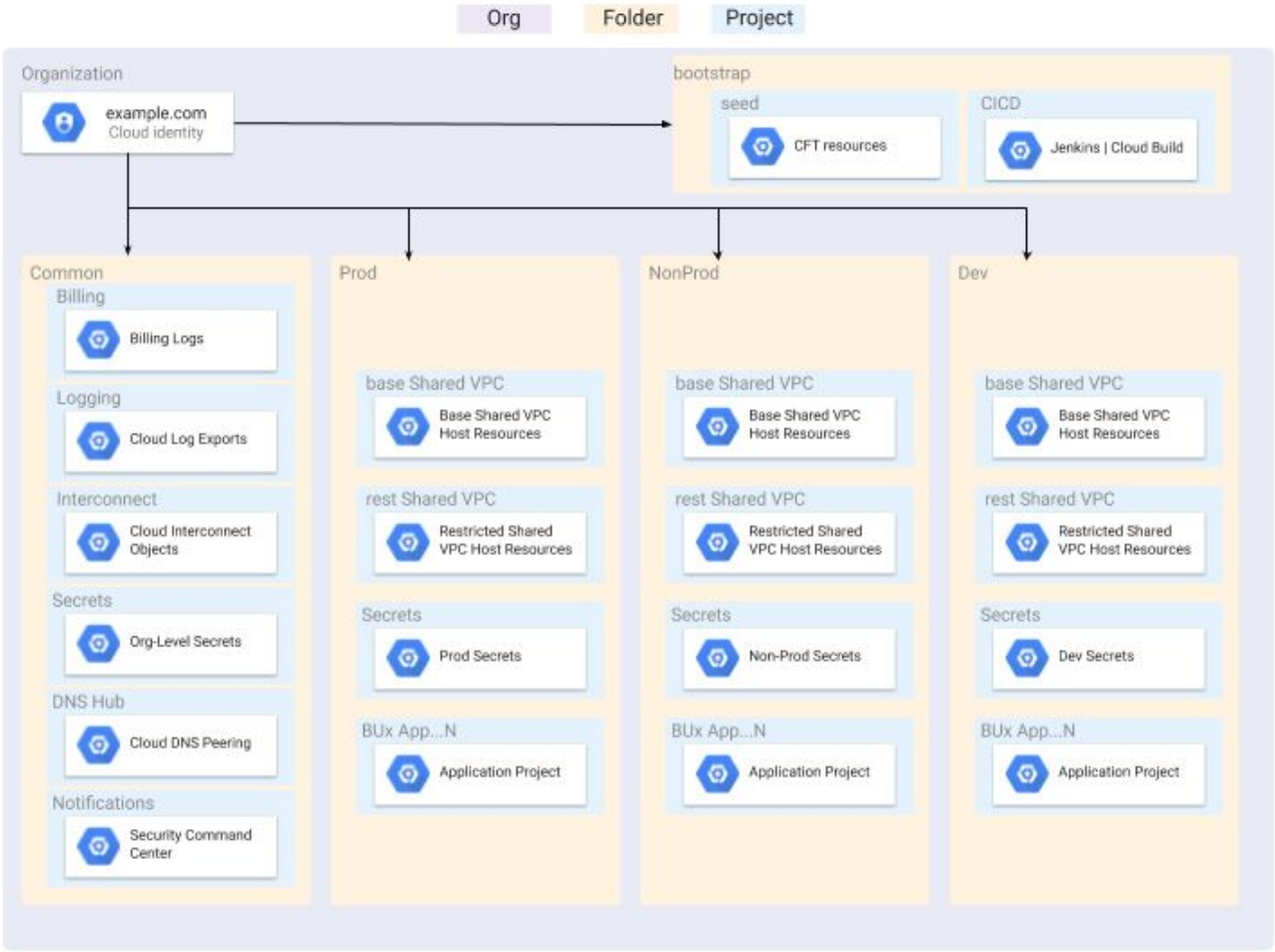


図 **2.3** example.com の組織構造

このアーキテクチャは、セクション 4.1 で説明されている 5 つのフォルダと、セクション 4.2 で詳しく述べる複数のプロジェクトで構成されています。example.com の組織構造は Terraform モジュールで体系化され、セクション 5 で説明するデプロイ パイプラインを介してデプロイされます。

注: example.com のフォルダ構造は、標準的なアプリケーション デプロイメント アーキテクチャの基本を示しています。ただし本番環境では、リソース分離、地理的な運用ニーズ、ビジネス ユニットの自律性、データ分離、アクセス制御などに関する実際のニーズに応じてデプロイ戦略を調整してください。さらに、分析などのワークロードでは、本番環境データが非本番環境で必要になる可能性もあります。このため、例とは異なる環境の分類が必要になる場合があります（分析用フォルダなど）。また、分離を強化する目的で複数の Google Cloud 組織を作成する必要が生じることもあります。

4.1) フォルダ

フォルダは、関連するプロジェクトをグループとしてまとめる手段として使用します。セキュリティ ポリシーとアクセス権限をフォルダレベルで適用できます。その場合、それらのポリシーや権限はフォルダ構造内のリソースに継承されます。

フォルダという概念は、複数のプロジェクトを論理グループにまとめることにあります。そして、一貫性のあるポリシーをフォルダ配下のプロジェクトに適用することにより、管理上のオーバーヘッドが軽減されます。表 2.4 に示すように、example.com のリファレンス アーキテクチャでは 5 つのフォルダが使用されています。このうちの 3 つ（production、non-production、development）は組織を異なる環境に分離するものです。これらのフォルダは、セクション 5 で説明するデプロイ パイプラインを介してデプロイされます。

フォルダ	説明
bootstrap	基盤コンポーネントをデプロイするのに使用される seed プロジェクトと CICD プロジェクトが含まれます。
common	組織によって使用されるクラウド リソースを持つプロジェクトが含まれます。
production	本番環境に昇格されたクラウド リソースを持つプロジェクトが含まれます。
non-production	ワークロードを本番環境に移行する前にテストするために使用できる、本番環境のレプリカが含まれます。
development	開発およびサンドボックス環境として使用されます。

表 **2.4** example.com リファレンス アーキテクチャで使用されるフォルダ

4.2) プロジェクト

Google Cloud におけるプロジェクトは、クラウド リソースを格納する構造です。各プロジェクトは、1 つ以上の親フォルダと Google Cloud 組織のポリシーを継承します。プロジェクトに必要なサービスで利用されるAPIを、各プロジェクト内で有効または無効にできます。セクション 5.3.4 で説明しているように、各プロジェクトは 1 つの請求先アカウントに関連付けられます。

4.2.1) common フォルダと bootstrap フォルダのプロジェクト

example.com アーキテクチャでは、example.com 組織全体で使用されるリソースを含む common フォルダと bootstrap フォルダに一連のプロジェクトが配置されています。表 2.5 に示すとおり、これらのプロジェクトはさまざまなエンタープライズ機能を提供し、インフラストラクチャ デプロイ パイプラインを介して作成されます。

プロジェクト	説明	詳細情報
CICD	組織の基本コンポーネントの構築に使用されるデプロイ パイプラインが含まれます。このプロジェクトへのアクセスは厳しく制限されています。	セクション 5
seed	インフラストラクチャの Terraform における状態と、状態を更新する Terraform サービス アカウントが含まれます。このプロジェクトへのアクセスは厳しく制限されています。	セクション 5
interconnect	エンタープライズのオンプレミス環境と Google Cloud の間をつなぐ Cloud Interconnect 接続が含まれます。	セクション 7
DNS hub	企業のオンプレミス DNS システムと Cloud DNS の間の通信の中心となる場所を提供します。	セクション 7
global secrets	組織レベルのシークレットが含まれます。	セクション 8
logs	ログシンクと発見的コントロールの宛先を提供します。	セクション 9
Security Command Center	Security Command Center アラート機能を管理するためのスタンドアロン プロジェクトを提供します。	セクション 10
billing	組織の請求データのエクスポートを含む BigQuery データセットが含まれます。	セクション 11

表 **2.5** common フォルダ内のプロジェクト

4.2.2) すべての環境フォルダ内にあるプロジェクト

example.com リファレンス アーキテクチャ内のそれぞれの環境フォルダ（production、non-production、development）の下には、表 2.6 に示すようなプロジェクトが共通して作成されています。これらのプロジェクトは、オンプレミス環境へのリソース接続を提供し、またワークロード固有のリソースの場合はデプロイメント環境へのリソース接続を提供します。

プロジェクト タイプ	説明
基本共有 VPC ホスト プロジェクト	VPC Service Controls を必要としない組織ワークロードをホストする共有 VPC ネットワーク用のプロジェクトを提供します。
制限付き共有 VPC ホスト プロジェクト	VPC Service Controls によって制御される境界内で実行される組織ワークロードをホストする共有 VPC ネットワーク用のプロジェクトを提供します。
シークレット	フォルダレベルのシークレットが含まれます。
アプリケーション プロジェクト	アプリケーション リソースのデプロイ場所となるプロジェクトです。セクション 7.1.1 で説明しているように、プロジェクトのデプロイ パターンには共有 VPC サービス プロジェクト パターン、フローティング プロジェクト パターン、ピアリングされたプロジェクト パターン、デュアル NIC プロジェクト パターンがあります。

表 **2.6** 環境フォルダ プロジェクト タイプ

4.3) 組織ポリシーのセットアップ

組織ポリシー サービスを使用して Google Cloud 組織にポリシーを適用できます。組織のポリシーは、ポリシーの対象となるリソースノードのすべての子リソースに継承されます。ただし子リソースでオーバーライドが明示的に設定される場合を除きます。example.com リファレンス アーキテクチャの組織ポリシー制約は Terraform モジュールで定義され、デプロイ パイプラインを介してデプロイされます。表 2.7 は、example.com 基盤の一部として設定されているポリシーのリストとその説明です。

ポリシー制約	説明	推奨される値
compute.disableNestedVirtualization	（ブール値）true の場合、すべての Compute Engine VM に関する、ハードウェア アクセラレーションによるネストされた仮想化が無効になります。	true
compute.disableSerialPortAccess	（ブール値）true の場合、Compute Engine VM へのシリアルポート アクセスが無効になります。	true
compute.disableGuestAttributesAccess	（ブール値）true の場合、Compute Engine VM のゲスト属性への Compute Engine API アクセスが無効になります。	true

compute.vmExternalIpAccess	（リスト）外部 IP アドレスの使用を許可される Compute Engine VM インスタンスのセットを定義します。	deny all=true
compute.skipDefaultNetworkCreation	（ブール値）true の場合、Google Cloud プロジェクト リソースの作成中にデフォルト ネットワークとそれに関連するリソースの作成がスキップされます。	true
compute.restrictXpnProjectLienRemoval	（ブール値）true の場合、共有 VPC プロジェクト リーエンを削除できるユーザーが制限されます。	true
sql.restrictPublicIp	（ブール値）true の場合、Cloud SQL インスタンス上のパブリック IP アドレスが制限されます。	true
iam.allowedPolicyMemberDomains	（リスト）Cloud IAM ポリシーに追加できるメンバーを定義します。許可リストまたは拒否リストでは、1 つ以上の Cloud Identity または G Suite カスタマー ID を指定する必要があります。 ドメインで制限される共有によって一部の Google Cloud サービスを使用できなくなることがあります。このような場合、Google Cloud サービスを例外として設定する必要が生じることがあります。	Cloud Identity の ID
iam.disableServiceAccountKeyCreation	（ブール値）true の場合、サービス アカウントの外部キーの作成が無効になります。	true
storage.uniformBucketLevelAccess	（ブール値）true の場合、バケットで IAM に基づく均一なバケットレベルのアクセスを使用する必要があります。	true

表 **2.7** example.com における組織ポリシー

注: 特定のアプリケーション タイプやワークロードに対応するために、組織ポリシー制約の変更が必要になることがあります。たとえば、新しいログ エクスポートの構成、一般公開されるバケットの意図的な作成、インターネット アクセス用の外部 IP アドレスの VM への付与などです。

4.4) その他のポリシー制御

Google Cloud には、前のセクションで説明した組織ポリシーの制約の他にもポリシーがあり、組織のセキュリティ体制を強化する目的でこれらのポリシーを組織に適用できます。表 2.8 は、example.com リファレンス アーキテクチャで使用されているその他のポリシー制御の一覧です。

制御	説明	管理
セッションと gcloud のタイムアウト制限	（gcloud ツールを含む）Google Cloud セッションのタイムアウトを最短 1 時間までに変更できます。	G Suite または Cloud Identity の管理コンソール
Cloud Shell の無効化	Google Cloud には、クラウド環境を操作するためのネイティブ Cloud Shell インターフェースが備わっています。このシェルを無効化できます。	管理コンソール
フィッシング耐性のあるセキュリティ キーの使用	2 要素認証（2FA）の認証要素として、フィッシング耐性のあるセキュリティ キーを有効にすると、自動化されたボット、大規模フィッシング、標的型攻撃から保護するうえで役立ちます。これらのキーは公開鍵暗号を使用してユーザーのアイデンティティを検証します。またログイン ページの URL を使用して、ユーザーが騙されてユーザー名とパスワードを入力した場合でも攻撃者がユーザーのアカウントにアクセスできないようにします。	G Suite または Cloud Identity の管理コンソール。外部システムから ID をフェデレーションする場合、ご使用の ID プロバイダで構成するか、または Cloud Identity 内で直接、既存の SSO 設定に保護レイヤを追加する必要があります。
アクセス透明性の有効化	アクセス透明性は、Google 担当者がお客様のコンテンツにアクセスする際に行うアクションを記録したログを提供します。ゴールド、プラチナ、エンタープライズ、またはプレミアのいずれかのサポート プランに加入する必要があります。	Google Cloud サポートにお問合わせください
アクセス承認の有効化	アクセス承認を使用すると、Google Cloud 上のデータや構成へのアクセスをお客様が明示的に承認しない限り、Google Cloud サポートまたはエンジニアリング担当者はデータにアクセスできなくなります。	Google Cloud Console
データ ストレージの場所の制限	リソース ロケーション制約を使用することで、Google Cloud の新しいリソースの物理的な場所を制限できます。	セクション 4.3 で詳しく述べる組織ポリシー制御と同じメカニズムです。

表 **2.8** その他の example.com ポリシー制御

注: フィッシング耐性を持たない任意の 2FA スキームとフィッシング耐性のある 2FAメカニズムは、重要な違いがあります. 後者の例には、Titan セキュリティ キーや、その他フィッシング耐性のある FIDO U2F または CTAP1 標準に準拠したキーがあります。企業は、セキュリティ キーの検証を含む 2 段階認証プロセスをアカウントに段階的に適用することで、移行が可能になります。まず、より多くの権限を持つユーザーに適用してから、必要に応じて適用範囲を広げることができます。

5. リソースのデプロイ

example.com リファレンス アーキテクチャ内のリソースは通常、2 つのカテゴリ（基盤コンポーネントとワークロード コンポーネント）のいずれかに分類されます。
企業がセキュリティ上またはコンプライアンス上のリスクにさらされるのを防ぐために、基盤リソースを厳しいセキュリティで保護、管理、監査する必要があります。基盤リソースには、階層内の組織ポリシー、フォルダ、プロジェクト、API、アイデンティティ（サービス アカウントなど）、ロール バインディング、カスタム ロール定義、共有 VPC ネットワーク、サブネット、動的ルートと静的ルート、ファイアウォール ルール、Dedicated Interconnect 接続などのリソースがあります。

Google Cloud 内のリソースのデプロイは、Google Cloud Console ウェブ ユーザー インターフェース、gcloud コマンドライン ツール、直接的な API 呼び出し、Infrastructure as Code（IaC）ツールを使用して行うことができます。企業環境の基盤となる要素を作成する際には、手動による構成を最小限に抑えて、ヒューマンエラーが発生しないようにする必要があります。example.com リファレンス アーキテクチャでは IaC に Terraform が使用され、Jenkins を使用して実装されるパイプライン経由でそれがデプロイされます。

Terraform と Jenkins を組み合わせることで、example.com の基盤要素を一貫性のある、制御可能な方法でデプロイできます。この一貫性と制御性により、example.com の Google Cloud 環境全体での管理とポリシー制御が可能となります。example.com リファレンス パイプライン アーキテクチャは、ほとんどの企業のセキュリティ管理に適合するように設計されています。

5.1) CICD プロジェクトと seed プロジェクト

example.com 組織は Cloud Foundation Toolkit の機能を使用して、Google Cloud 内で IaC 環境を立ち上げるのに必要な基本的リソースを作成します。このプロセスにより組織のルートに bootstrap フォルダが作成され、そこに CICD プロジェクト seed Terraform プロジェクトが格納されます。

CICD プロジェクトは、Jenkins デプロイ パイプラインをホストする、組織階層内で厳密に制御されるプロジェクトです。また、これは、Jenkins エージェントの Compute Engine インスタンスの実行に使用されるサービス アカウントをホストします。Jenkins サービス アカウントは Terraform サービス アカウントになりすますことができます。Terraform サービス アカウントは seed プロジェクト内に配置され、組織内の基盤構造をデプロイする権限を持ちます。CICD プロジェクトは、スクリプト化されたプロセスを通して作成され、オンプレミス環境に（セクション 7.2 に示す接続とは別に）直接接続できます。

seed プロジェクトには、基盤インフラストラクチャの Terraform のステータス、新規インフラストラクチャを作成できる高度な権限を持つサービス アカウント、およびその状態を保護する暗号化構成が含まれています。CI / CD パイプラインが実行されると、このサービス アカウントになりすまします。互いに独立した CICD プロジェクトと Terraform seed プロジェクトが存在する理由は、対象を分離するためです。Terraform は IaC ツールとして使用され、独自の要件がありますが、その IaC のデプロイは CI / CD パイプラインによって行われます。

注: example.com リファレンス アーキテクチャではデプロイ パイプラインとして Jenkins を使用しています。Google Cloud ネイティブのサービスを使用する場合は、コード リポジトリや Cloud Build ベースのパイプラインも利用可能です。

5.2) デプロイ パイプラインのアーキテクチャ

図 2.4 は example.com のデプロイ パイプラインを示しています。example.com インフラストラクチャを定義する Terraform コードは、オンプレミス Git リポジトリに保存されます。リポジトリのメイン ブランチでコードが変更されると Webhook がトリガーされ、Webhook によって example.com 組織への Terraform コードのデプロイがトリガーされます。

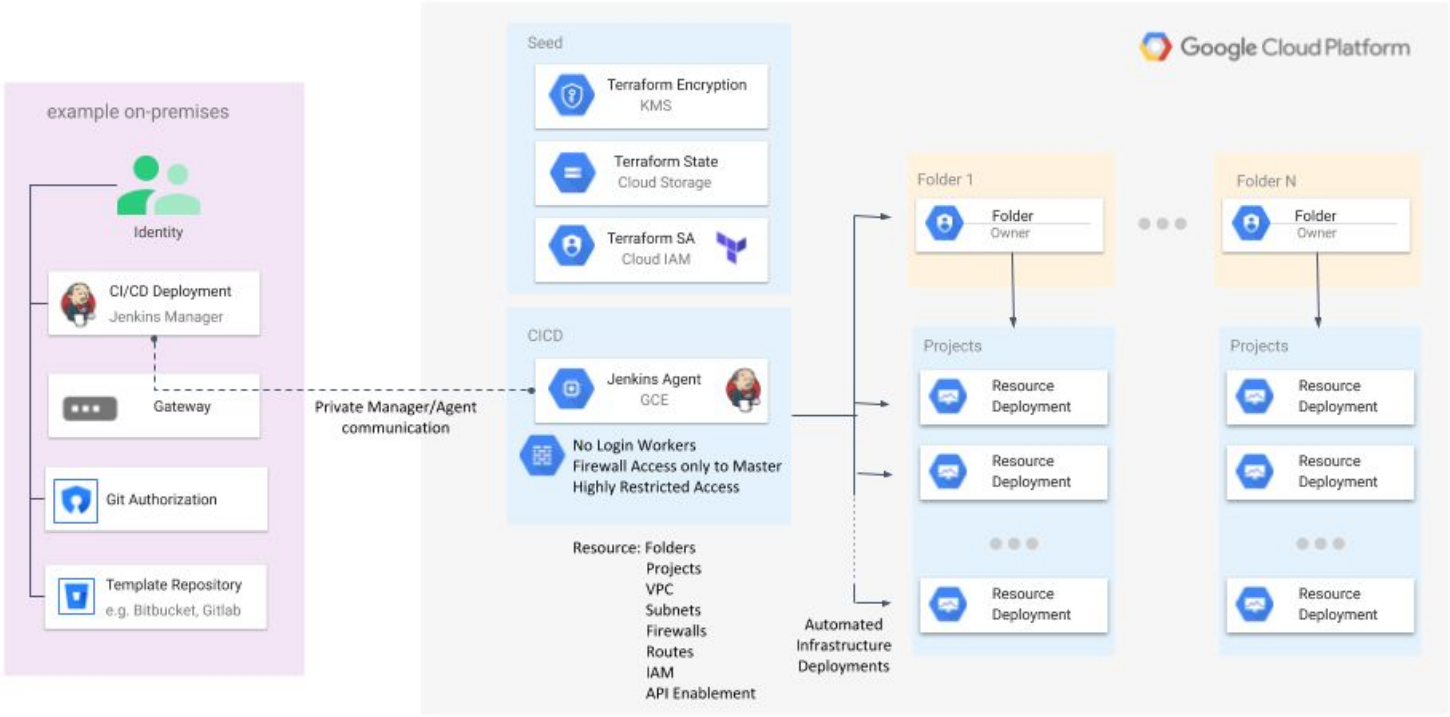


図 **2.4** example.com 基盤のデプロイ パイプライン

Jenkins パイプラインは水平分散ビルド アーキテクチャを使用して実装されます。このモデルでは、Jenkins マネージャー（マスター）が HTTP リクエストを処理してビルド環境を管理する一方で、ビルドの実行は CICD プロジェクト内の Jenkins エージェントに委任されます。

Jenkins マネージャーはオンプレミスでホストされソース コントロール管理システムと一緒に配置される一方、Jenkins エージェントは Google Cloud 環境でホストされます。Jenkins エージェントは Java と Docker がインストールされているシンプルな SSH サーバーであり、エージェントに必要な情報はマネージャーの SSH 公開鍵だけです。したがってJenkins マネージャーは SSH クライアントとして機能します。マネージャーは SSH 秘密鍵を使用してエージェントに接続し、Java 実行（JAR）ファイルをデプロイし、その実行ファイルによってパイプラインの実行をエージェントに指示できます。パイプラインで作成される一時的なコンテナ化 Terraform ワーカーは、example.com インフラストラクチャをデプロイおよび変更します。

表 2.9 は、パイプラインに統合されているセキュリティとガバナンスの制御を示しています。

制御	説明
pull リクエスト（PR）	コードがメイン ブランチに統合されるには、承認された PR を伴う必要があります。
ポリシー チェック	パイプラインによって Terraform Validator を使用した、Terraform コードに対するポリシー チェックが行われます。
デプロイ承認	コードをデプロイする際に、オプションで手動承認を行うためのステージがパイプラインに含まれています。

表 **2.9** example.com 基盤のパイプライン セキュリティ コントロール

Google Cloud でこのアーキテクチャを使用すると、クリーンなプロセスで Google Cloud APIs を認証および認可できるようになります。Jenkins エージェントで使用されるカスタム サービス アカウントは、新しいインフラストラクチャを作成する権限を持ちませんが、Terraform サービス アカウントになりすましてインフラストラクチャをデプロイします。この Terraform サービス アカウントは、組織のポリシー、フォルダ、プロジェクト、その他の基盤コンポーネントを作成するのに必要な管理ロールを持っています。これらのサービス アカウントには非常に機密性の高い権限が含まれるため、これらのエージェントの実行場所である CICD プロジェクトと seed プロジェクトへのアクセスは厳しく制限されます。

Compute Engine でエージェントを実行するとサービス アカウントの JSON版キーファイルのダウンロードが不要になります。エージェントがオンプレミスや Google Cloud 外部の他の環境で実行される場合は、ダウンロードが必要です。example.com 組織内では、Jenkins エージェントと指定されたファイアコール（セクション6.3で説明）だけが基盤コンポーネントをデプロイする権限を持っています。

注: ポリシーを Terraform モジュールやデプロイ パイプラインに直接ハードコーディングしないでください。ポリシーは Terraform Validator や Open Policy Agent などのサービスで処理するようにしてください。

5.3) プロジェクトのデプロイ

example.com 組織内のプロジェクトは、デプロイ パイプラインを介してデプロイされます。このセクションでは、プロジェクトの作成時に割り当てられるプロジェクト属性について説明します。

5.3.1) プロジェクト ラベル

プロジェクト ラベルは、請求データのエクスポートと Cloud Monitoring に含まれる Key-Value ペアです。これにより請求とリソース使用状況を詳しく分析できます。表 2.10 は、example.com デプロイメント内の各プロジェクトに追加されるプロジェクト メタデータを示しています。

ラベル	説明
`business-code`	このプロジェクトを所有しているビジネス ユニットを示す 4 文字のコード。ビジネス ユニットに明示的に関連付けられていないプロジェクトでは、abcd というコードが使用されます。
`billing-code`	チャージバック情報を提供するために使用されるコード。
`primary-contact`	プロジェクトの主たるメール連絡先。
`secondary-contact`	プロジェクトの予備メール連絡先。
`environment`	環境の種類を示す値。たとえば `nonprod`、`prod`。

表 **2.10** example.com のプロジェクト ラベル

5.3.2) IAM 権限

IAM 権限は、プロジェクトのリソースとしてプロジェクトごとに定義、作成されます。

5.3.3) Google Cloud APIs

Google Cloud APIs はプロジェクトごとに有効化されます。許可 / 拒否リストを使用して承認された API のみを有効化できるようにするために、パイプラインでポリシー チェックが実施されます。

5.3.4) 請求先アカウント

新しいプロジェクトはメインの請求先アカウントに関連付けられます。適切なビジネス ユニットへのチャージバックは、プロジェクト ラベル（セクション 11.2 を参照）を使用することで可能になります。

5.3.5) ネットワーキング

VPC ネットワーク、サブネット、ファイアウォール、ルートなどのプロジェクト ネットワーキング構造は、デプロイ パイプラインを介して有効化されます。

5.3.6) プロジェクト編集者

各プロジェクトには 2 つのプロジェクト編集者が関連付けられます。1 つは、seed プロジェクト内のデプロイ パイプラインで使用されるカスタム サービス アカウントです。もう 1 つのプロジェクト編集者は、ファイアコール アカウントです。セクション 6.3 で説明しているように、自動化が機能しない場合や緊急時にこれを使用できます。

5.4) リポジトリ構造

example.com コード リポジトリは monorepo として配布されるため、簡単にフォーク、コピー、使用できます。ただし、コードの各ステップが個別の Jenkins ジョブとリポジトリを介して実行されるようにコードが構築されています。最上位レベルのフォルダと各フォルダの内容が表 2.11 に示されています。example.com のコードは、terraform-example-foundation GitHub リポジトリにあります。

フォルダ	説明	example.com コンポーネント

0-bootstrap	後続の IaC ステージ（1〜4）のための初期プロジェクトと IAM 権限がデプロイされます。	bootstrap フォルダ
		• seed プロジェクト
		• CICD プロジェクト
		  ○ Jenkins パイプライン
		  ○ Terraform Validator

1-org	ポリシー、ログのエクスポート、IAM など、組織全体で使用するものが含まれます。	組織ポリシー 組織全体の IAM 設定 common フォルダ • 請求データのエクスポート プロジェクト • ログ エクスポート プロジェクト • interconnect プロジェクト • 組織全体のシークレット プロジェクト • DNS プロジェクト • SCC 通知プロジェクト
2-environments	新しい最上位環境のモジュール作成に使用され、必要なプロジェクトや最上位フォルダが含まれます。	dev フォルダ • 基本共有 VPC ホスト プロジェクト • 制限付きの共有 VPC ホスト プロジェクト • 環境シークレット プロジェクト • 環境モニタリング プロジェクト nonprod フォルダ • （dev フォルダと同じプロジェクト） prod フォルダ • （dev フォルダと同じプロジェクト）

3-networks	VPC ネットワークのモジュール作成と管理に使用されます。	VPC ネットワーク ファイアウォール ルール Cloud Router ルート
4-projects	さまざまなチームやビジネス ユニット用のプロジェクトの作成に使用され、アプリケーション ワークロードに焦点が置かれます。	アプリケーション プロジェクト

表 **2.11** example.com リポジトリ構造

5.5) 基盤パイプラインとワークロード

このセクションで示すパイプライン アーキテクチャは、Google Cloud 組織の基盤レイヤをデプロイするものです。このパイプラインの用途は、より上位のレベルのサービスやアプリケーションをデプロイすることではありません。さらに、図 2.5 に示すように、デプロイ パイプラインを介した Google Cloud へのアクセス パターンは、選択可能なアクセス パターンの一つにすぎません。ワークロードごとに、アクセス パターンとワークロードの制御を個別に評価する必要がある場合があります。

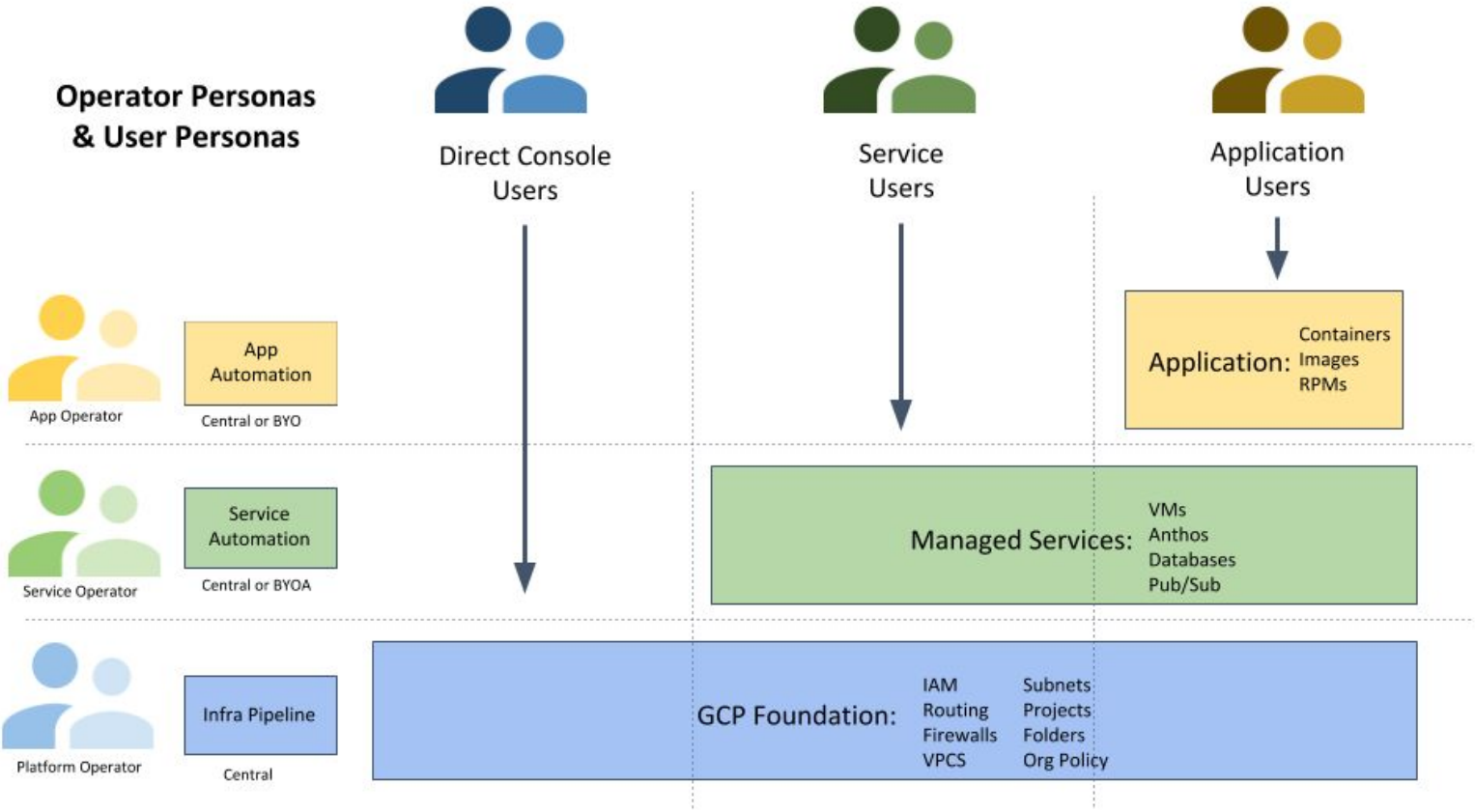


図 **2.5** example.com のアクセス パターン

6. 認証と認可

6.1) Cloud Identity、ディレクトリ プロビジョニング、シングル サインオン

Google Cloud では認証とアクセス管理に Google Cloud Identity を使用します。すべての従業員が Active Directory などの既存の ID ストアにすでにアカウントを持っている場合、各従業員の Google ID を手動で管理すると、管理の負荷が不必要に増えかねません。Cloud Identity と Active Directory の間でユーザー ID のフェデレーションを行えば、Google ID の管理を自動化して、そのライフサイクルを組織内の既存の ID 管理プロセスと関連付けることができます。

リファレンス アーキテクチャでは、図 2.6 に示すように、Google Cloud Directory Sync ツールを使用して必要なユーザーとグループが Active Directory から Cloud Identity に定期的に同期されます。これにより、Active Directory で新しいユーザーを作成すると Google Cloud でもそのユーザーを参照できるようになります。また、ユーザー アカウントが削除または停止された場合には、変更内容が Google Cloud 側に連携されるようになります。プロビジョニングは一方向に機能します。つまり、Active Directory での変更内容は Cloud
Identity に複製されますが、逆方向には複製されません。デフォルトでは、パスワードは同期されません。フェデレーションが行われている場合、認証情報を管理するシステムは Active Directory のみです。

注: 初期セットアップ中に、Directory Sync プロセスが 3-legged OAuth ワークフローでインタラクティブに認証される必要があります。従業員の管理アカウントを使用するのではなく、この同期専用のアカウントを作成することをおすすめします。これは、同期を行うアカウントが存在しなくなったり、適切な権限を失ったりした場合、同期が失敗するためです。同期用のアカウントには、Cloud Identity テナント内のグループ管理およびユーザー管理の管理者ロールが必要です。高度な権限を持つ他のアカウントの場合と同じ方法で、このアカウントへのアクセスを保護してください。Directory Sync の使用に関するその他のベスト プラクティスについては、こちらのドキュメントをご覧ください。

example.com リファレンス アーキテクチャでは、ユーザー認証にシングル サインオン（SSO）が使用されます。サインオン時に Google Cloud は Security Assertion Markup Language（SAML）プロトコルを使用して Active Directory フェデレーション サービスに認証を委任します。この委任により、Active Directory のみがユーザー認証情報を管理し、該当するポリシーや多要素認証（MFA）メカニズムが確実に実施されるようになります。サインオンが成功するには、Active Directory と Cloud Identity の両方でユーザーがプロビジョニングされる必要があります。

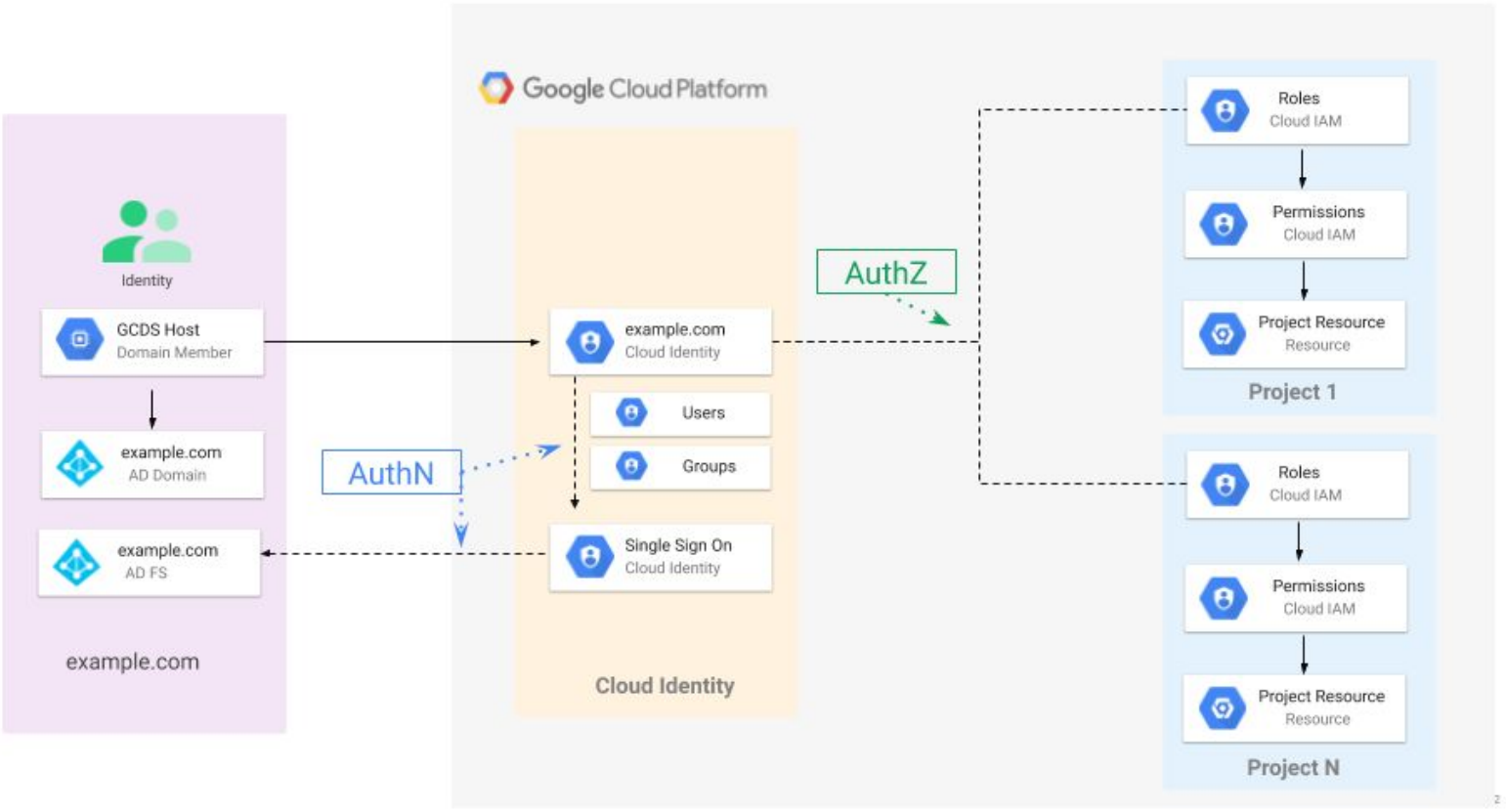


図 **2.6** example.com のアイデンティティ構造

example.com リファレンス アーキテクチャでは、ユーザー、グループ、SSO に関する信頼できる情報源としてオンプレミス Active Directory システムが使用されます。Google Cloud Directory Sync は、オンプレミスのドメイン参加ホスト（Windows または Linux）にインストールされます。（タスク スケジューラまたは cron を使用した）スケジュール済みジョブにより、ユーザーとグループが 1 時間ごとに Cloud Identity に同期されます。どのユーザーが Cloud Identity に同期されるかを制御するために、Active Directory でユーザーに属性が追加され、Directory Sync によってその属性に対するフィルタリングが行われます。example.com ドメインでは、Google Cloud 固有のグループ名の先頭には `grp-gcp-` が付き（`grp-gcp-billing-viewer` や `grp-gcp-security-reviewer` など）、フィルタを適用してこれらのグループのみが同期されます。 example.com Directory Sync フィルタを表 2.12 に示します。

フィルタの種類	フィルタルール
グループ フィルタ	`(&(objectCategory=group)(cn=grp-gcp-*))`
ユーザー フィルタ	`(&(objectCategory=user)(msDS-cloudExtensionAttribute1=googlecloud))`

表 **2.12** Google Cloud Directory Sync のユーザー フィルタとグループ フィルタ

注: Directory Sync で同期されるグループには、Cloud Identity 組織名に一致する接尾辞を持つ有効な `mail` 属性が必要です（たとえば `group@example.com`）。`mail` 属性は、メール受信用の有効な配布グループである必要はありません。ただし、Cloud Identity ではグループの一意の ID として完全なメール アドレスが使用されます。IAM ロールを割り当てるときには、この ID を使用してグループを参照します。

6.2) ユーザーとグループ

example.com のグループは、表 2.2 で示した命名規則に従います。example.com 組織では、ユーザーにロールが直接割り当てられることはありません。Cloud IAM でロールと権限を割り当てる主な方法としては、グループが使用されます。IAM ロールと権限はプロジェクトの作成中にデプロイ パイプラインを介して割り当てられ、その後、必要に応じて更新されます。

ユーザーにはオンプレミス Active Directory システムを介してグループ メンバーシップが割り当てられます。これにより、グループの作成とメンバーシップが厳密に管理されます。表 2.13 は、example.com 基盤におけるグループ設定を示しています。ワークロードごとに必要に応じて追加のグループを設定できます。

グループ	説明	ロール	対象範囲
`grp-gcp-billing-viewer@example.com`	メンバーは、プロジェクトの費用を閲覧することを許可されます。一般的に、財務チームに所属する人員がメンバーになります。	請求先アカウント閲覧者 BigQuery データ閲覧者 BigQuery ユーザー	請求先アカウント閲覧者の場合は組織 BigQuery データ閲覧者と BigQuery ユーザーの場合は請求先プロジェクト
`grp-gcp-platform-viewer@example.com`	メンバーは、Google Cloud 組織全体でリソース情報を閲覧することができます。	閲覧者	組織

grp-gcp-security-reviewer@example.com	各メンバーは、クラウド セキュリティの審査を担当するセキュリティ チームの一員です。	セキュリティ審査担当者	組織
grp-gcp-network-viewer@example.com	各メンバーはネットワーキング チームの一員で、ネットワーク構成を審査します。	Compute ネットワーク閲覧者	組織
grp-gcp-audit-viewer@example.com	各メンバーは監査チームの一員で、ロギング プロジェクトの監査ログを審査します。	ログ閲覧者 プライベート ログ閲覧者 BigQuery データ閲覧者	ロギング プロジェクト
grp-gcp-scc-admin@example.com	メンバーは Security Command Center を管理できます。	セキュリティ センター管理編集者	SCC プロジェクト
grp-gcp-secrets-admin@example.com	メンバーは、シークレットを Secrets Manager に保管する作業を担当します。	Secrets Manager 管理者	グローバル シークレット プロジェクト 本番環境シークレット プロジェクト 非本番環境プロジェクト 開発プロジェクト
grp-gcp-businesscode-environment-code-developer@example.com	特定のプロジェクト内のリソースを管理する目的でビジネス コードごと、または環境ごとにグループが作成されます。	サービス固有およびプロジェクト固有の権限	指定されたプロジェクト
grp-gcp-platform-operator@example.com	メンバーはプラットフォームの運用を担当します。必要に応じ他のグループに追加され、そのグループの権限を継承します。		

表 **2.13** example.com 内のグループ

Cloud IAM には次の 3 種類のロールがあります。

- 基本ロールには、オーナー、編集者、閲覧者の各ロールが含まれます。
- 事前定義済ロールは、特定のサービスに対しきめ細かなアクセスを提供します。事前定義ロールは Google Cloud で管理されます。
- カスタムロールは、ユーザー指定の権限リストに基づききめ細かなアクセスを提供します。

可能な限り、事前定義ロールを使用することをおすすめします。ユーザーとグループに付与された IAM 権限で許可される範囲が広すぎないことを確認するため、IAM Recommender を使用するようにしてください。Google Cloud 組織において、基本ロールは使用しないか、または少なくとも厳しく使用を制限

する必要があります。これは、これらのロールには幅広い権限が元々備わっており、最小権限の原則に反しているためです。可能な場合は常に、当初から職務分離の原則に沿って設計されている事前定義ロールを使用し、必要に応じてカスタムロールを追加してください。

注: グループとユーザーには、特権 ID を持っていない限り、セクション 5 で説明したデプロイ パイプラインによって配置された基盤コンポーネントを変更する権限を付与しないでください。

6.3) 特権 ID

特権 ID は、ファイアコール プロセスを介してアクセスされます。このプロセスは、権限昇格が必要な場合にのみ使用されるユーザーを対象とします。たとえば、自動プロセスが機能しなくなった場合や、一時的に権限を昇格させ、手動でサービスを稼働状態に戻す必要がある場合などです。

ID	説明	ロール
gcp-superadmin@example.com	Google Cloud 特権管理者権限を持っている ID。	特権管理者
gcp-orgadmin@example.com	example.com 内の組織管理者権限を持っている ID。	組織管理者
gcp-billingcreator@example.com	請求先アカウントを作成可能な ID。	請求先アカウント作成者
gcp-billingadmin@example.com	example.com 内の請求先管理者権限を持っている ID。	請求先アカウント管理者
gcp-environment-folderadmin@example.com	フォルダ管理者権限を持っている ID（フォルダごとに 1 つずつ）。	フォルダ管理者
gcp-businesscode-environment-code-editor@example.com	環境内のそのグループのプロジェクトに関するプロジェクト編集者権限を持っている ID（ビジネスコードまたは環境ごとに 1 つずつ）。	編集者

表 2.14 example.com 内の特権 ID

特権 ID は高度な権限を使用できるため、特権 ID へのアクセスには、組織内の 2 人以上のメンバーの同意が必要とするようにしてください。たとえば、1 人は特権 ID パスワードへのアクセスの管理者とし、もう 1 人は関連する MFA トークンへのアクセスの管理者とします。

注: gcp-superadmin@example.com などの特権管理者ロールを持つ Cloud Identity ユーザーは、組織の SSO 設定を迂回し、直接 Cloud Identity に認証されます。これは、SSO の構成ミスや機能停止が発生した場合に Google 管理コンソールにアクセスできるようにするためです。詳細について

は、特権管理者アカウントのベスト プラクティスのドキュメントと管理者アカウントのセキュリティに関するおすすめの方法のサポート記事をご覧ください。

7. ネットワーキング

ネットワーキングは、Google Cloud で組織を作成する場合の基本です。このセクションでは、VPC ネットワーク、プロジェクト、IP アドレス空間、DNS、ファイアウォール、および example.com オンプレミス環境への接続に関する example.com サンプル アーキテクチャの構造について説明します。

7.1) 共有 VPC 構成

共有 VPC は、ネットワーク設計の複雑さを大幅に軽減するネットワーキング構造です。共有 VPC ホスト プロジェクトは、1 つ以上の、サービス プロジェクトから利用できる、共有 VPC ネットワークで構成されます。この構成では、ネットワーク ポリシーとすべてのネットワーキング リソースの制御がホストプロジェクトの元で一元化され、管理が容易になります。サービス プロジェクト部門は、非ネットワーク リソースだけを構成して管理できるため、組織内のチームの責任分担が明確になります。

共有 VPC ネットワーク内のリソースは、内部 IP アドレスを使用し、プロジェクト境界を越えて安全かつ効率的に相互通信できます。共有ネットワーク リソース（サブネット、ルート、ファイアウォールなど）は、中央のホスト プロジェクトから管理できるため、プロジェクト全体で一貫したネットワーク ポリシーを適用できます。

図 2.7 に示すように、example.com アーキテクチャでは、基本と制限付きの 2 つの共有 VPC ネットワークを各環境のデフォルト ネットワーキング構造として使用します。プロジェクトごとに 1 つの共有 VPC が含まれています。基本 VPC ネットワークは機密データを含まないサービスのデプロイに使用され、制限付き VPC ネットワークは VPC Service Controls を使用して機密データを含むサービスへのアクセスを制限します。制限付き VPC ネットワークへのアクセスは、Access Context Manager によって制御され、アクセス ポリシーを適用することで、アクセスレベルに基づいてアクセス権を付与されます。アクセスレベルを作成することによって、制限付き VPC ネットワークに保存された機密データにアクセスする必要のあるサービスをホストするために、基本 VPC ネットワークを使用することもできます。

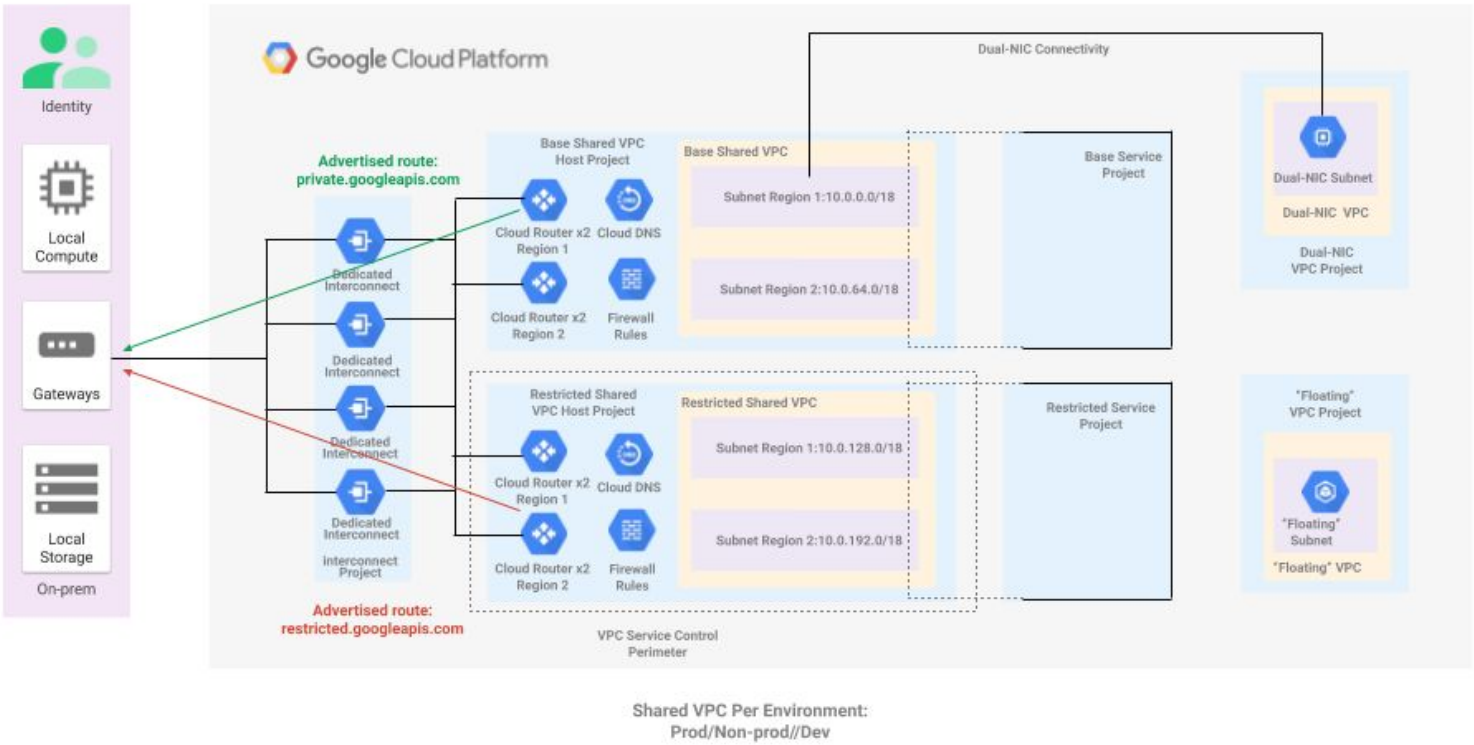


図 **2.7** example.com VPC ネットワークの構造

共有 VPC ネットワークごとに 2 つのサブネットがあります。各サブネットはそれぞれ複数のゾーンにまたがる別々のリージョンに配置されています。このインフラストラクチャは、高可用性と障害復旧ワークロード構成のためのメカニズムを提供します。セクション 7.2 で説明するように、オンプレミスリソースとの接続は、4 つの Cloud Router（リージョンごとに 2 つずつ）を使用した共有 VPC のそれぞれ 4 つの接続を介して有効にされます。表 2.16 は、example.com 設計における各サブネットの IP アドレス範囲を示しています。

注: example.com ネットワーク アーキテクチャは、VPC ネットワーク設計で採りうるアーキテクチャの一つを表しています。ご使用の VPC 設計に合わせて別のアーキテクチャを検討することもできます。

7.1.1) プロジェクト デプロイ パターン

example.com リファレンス組織には、プロジェクトのデプロイに関する 4 つのパターン（サービス プロジェクト、フローティング プロジェクト、ピアリングされた VPC プロジェクト、およびデュアル NIC 接続プロジェクト）が含まれています。

- **サービス プロジェクト**は、共有 VPC ホスト プロジェクトに接続されています。example.com において、サービス プロジェクトは、オンプレミス リソースにアクセスする必要のあるプロジェクトと、他のサービス プロジェクトとリソースを共有する必要のあるプロジェクトに対して使用されます。

- **フローティング プロジェクト**は、example.com オンプレミス環境へのプライベート ネットワーク接続がなく、Google Cloud リソースにのみアクセスが必要なプロジェクトです。オンプレミス接続がない共有 VPC ホスト プロジェクトを構成してから、オンプレミス接続のないサービス プロジェクトを含むようにフローティング プロジェクト パターンを変更できます。

- **ピアリングされた VPC プロジェクト**は、VPC ネットワーク ピアリングを使用して VPC ネットワークに接続できるため、異なる VPC ネットワーク内のワークロードが内部的に通信できます。トラフィックは Google のネットワーク内に留まり、公開インターネットを通過しません。そのため、VPC ネットワーク全体で内部 IP アドレスを使用してサービスを利用できます。ピアリングされた VPC ネットワークは、別のピアリングされた VPC ネットワーク内の静的ルートと重複するサブネット CIDR 範囲を使用できません。直接ピアリングされているネットワークだけが通信できます。これは、推移的ピアリングがサポートされていないためです。

- **デュアル NIC 接続プロジェクト**は、デュアル NIC 対応 Compute Engine インスタンスを介して基本 VPC ネットワークまたは制限付き VPC ネットワークのいずれかに接続します。この Compute Engine インスタンスは NAT として機能するため、デュアル NIC VPC ネットワーク内のリソースは、共有 VPC ネットワークを介して、または、共有 VPC ネットワーク内のリソースを使用して、オンプレミス環境と通信できます。プロジェクトをまたぐマルチ NIC 構成では、デュアル NIC Compute Engine インスタンス内の `nic0` を共有 VPC ネットワークに接続する必要があります。デュアル NIC 接続プロジェクトは、オンプレミスまたは共有 VPC ネットワークへの接続が必要な場合に使用されますが、デュアル NIC 対応 VPC ネットワークは広大な IP アドレス空間を必要とします。

注: インターネットへの下り（外向き）トラフィックが必要なワークロード向けに、Cloud NAT インスタンスをデプロイできるコードが example.com リポジトリに含まれています。インターネットからの上り（内向き）のトラフィックが必要なワークロードの場合は、Cloud Load Balancing の使用を検討する必要があります。

7.2) 企業と Google Cloud 間の接続

オンプレミス環境と Google Cloud 間の接続を確立するために、example.com リファレンス アーキテクチャでは Dedicated Interconnect を使用することでセキュリティと信頼性を最大限に高めています。

Dedicated Interconnect 接続は、企業のネットワークと Google Cloud 間を直接結ぶリンクです。プライベート接続を介して Compute Engine インスタンスや Google Cloud APIs にトラフィックをルーティングすることによって、トラフィックが公開インターネットを介してルーティングされたときに脅威になる中間者攻撃のリスクが軽減されます。

図 2.8 に示すように、example.com アーキテクチャは、2 つの異なるメトロエリアにある 4 つの Dedicated Interconnect 接続を使用して 99.99% の SLA を達成しています。この接続は 2 つのペアに分けられ、それぞれのペアが別々のオンプレミス データセンターに接続されています。すべての接続は、組織の Interconnect プロジェクトでホストされます。VLAN アタッチメントは、各 Dedicated Interconnect インスタンスを、セクション 7.1 で説明した共有 VPC 構造にアタッチされている Cloud Router に接続するために使用されます。各共有 VPC ネットワークには 4 つ（リージョンごとに 2 つ）の Cloud Router があります。動的ルーティング モードはグローバルに設定されています。これにより、すべての Cloud Router が、リージョンに関係なく、すべてのサブネットをアナウンスできます。図 2.8 は、Cloud Router の ASN と IP アドレスも示しています。

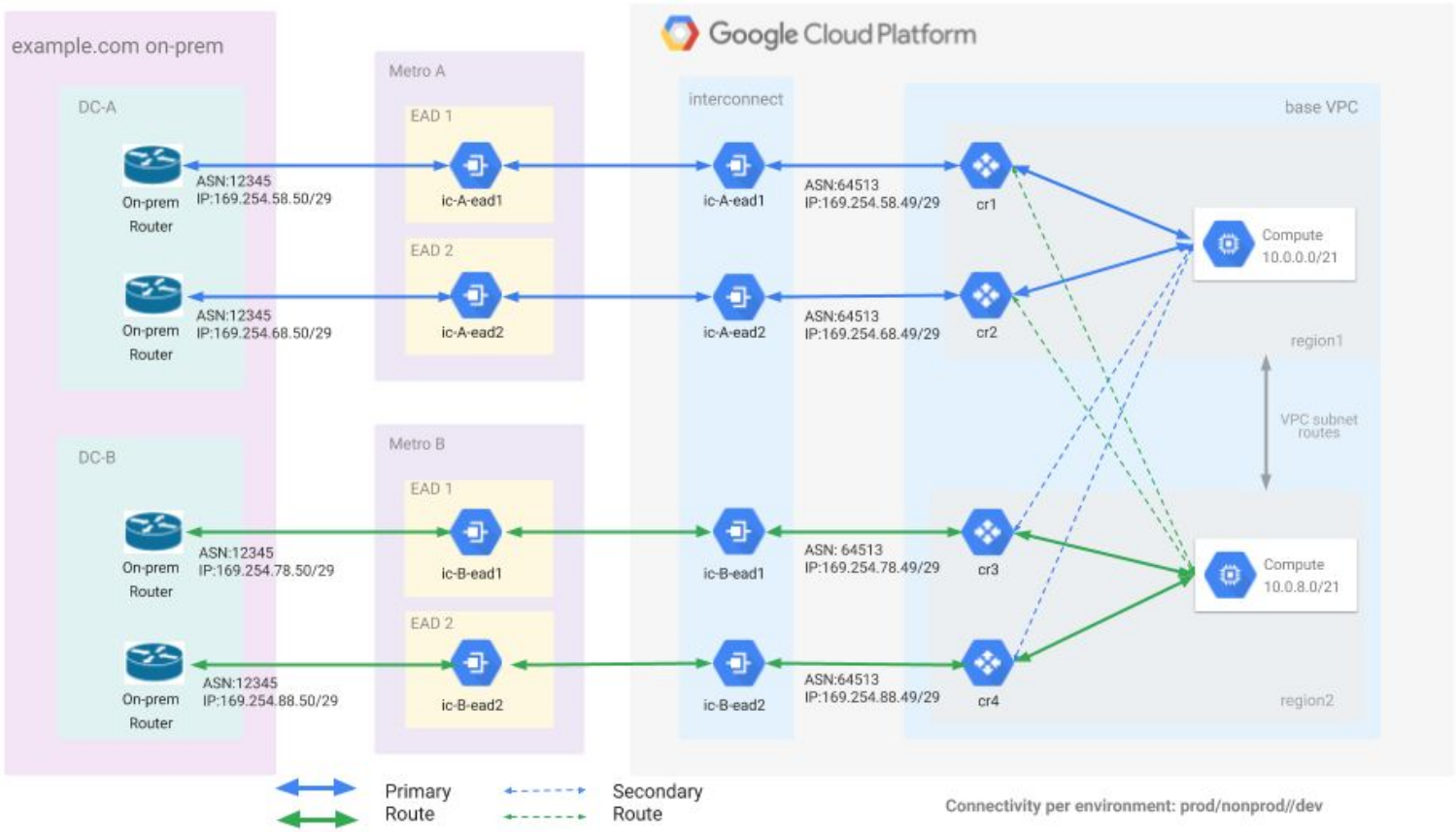


図 2.8 example.com Dedicated Interconnect 接続構造

Border Gateway Protocol（BGP）を介して受け入れるルートを指定するようにオンプレミス ルーター上のフィルタを構成する場合は、以前のステップで構成した内部 IP 空間を追加します。また、限定公開

の Google アクセス用の 199.36.153.8/30 と制限付きの限定公開の Google アクセス用の 199.36.153.4/30 も受け入れます。Google Cloud からの受信 DNS 転送クエリのために、セクション 7.4 で説明する 35.199.192.0/19 も受け入れる必要があります。これらの範囲はすべてパブリック IP アドレスですが、公開インターネット経由ではルーティングされません。

表 2.15 は、本番環境の Cloud Router、VLAN、VPC、接続、リージョン、接続拠点（POP）のマッピングを示しています。

ルーター名	POP-EAD	IC	VLAN アタッチメント	VPC	リージョン
cr-p-shared-base-region1-cr1	metroA-zone1	ic-a-ead1	vl-ic-a-ead1-p-shared-base-region1-cr1	基本	region1
cr-p-shared-base-region1-cr2	metroA-zone2	ic-a-ead2	vl-ic-a-ead2-p-shared-base-region1-cr2	基本	region1
cr-p-shared-base-region2-cr3	metroB-zone1	ic-b-ead1	vl-ic-b-ead1-p-shared-base-region2-cr3	基本	region2
cr-p-shared-base-region2-cr4	metroB-zone2	ic-b-ead2	vl-ic-b-ead2-p-shared-base-region2-cr4	基本	region2
cr-p-shared-restricted-region1-cr5	metroA-zone1	ic-a-ead1	vl-ic-a-ead1-p-shared-restricted-region1-cr5	制限付き	region1
cr-p-shared-restricted-region1-cr6	metroA-zone2	ic-a-ead2	vl-ic-a-ead2-p-shared-restricted-region1-cr6	制限付き	region1
cr-p-shared-restricted-region2-cr7	metroB-zone1	ic-b-ead1	vl-ic-b-ead1-p-shared-restricted-region2-cr7	制限付き	region2
cr-p-shared-restricted-region2-cr8	metroB-zone2	ic-b-ead2	vl-ic-b-ead2-p-restricted-region2-cr8	制限付き	region2

表 2.15 example.com 接続トポロジ

グローバル ルーティングが有効で、アドバタイズされたルートの優先度の値がデフォルトのままになっている場合は、すべての Cloud Router が BGP を使用して VPC ネットワーク内のすべてのサブネット ルートをアナウンスします。ただし、リモート リージョンからのルートには、より高いルート優先度の値（つまり、優先度が低い）が割り当てられます。これは、オンプレミス ルーティング テーブルで

は、トラフィックを送信する際に、使用されているコンピューティング リージョンにより近い接続を優先的に使用することを意味します。逆方向では、対称性を維持するために、Google Cloud は、ルートがリモート リージョンを起点にしている場合、ルートの優先度を下げます（より高いルート優先度の値が割り当てられます）。同じリージョン内の 2 つの Cloud Router 間では、BGP 経路選択がオンプレミス ルーターと BGP セッションの構成に委ねられます。

逆方向に流れるトラフィック（Google Cloud からオンプレミス ネットワークへ）も、接続とコンピューティング リソースに最も近い Cloud Router を介して送信されます。1 つのリージョン内に、MED の値が同じオンプレミス ネットワーク行きに使用可能なルートが複数存在する場合は、Google Cloud が ECMP を使用して、可能性のあるすべてのルートに下り（外向き）トラフィックを分配するため、5 タプルのハッシュに基づくアフィニティが利用されます。

注: このセクションでは、Dedicated Interconnect を使用して Google Cloud を example.com オンプレミス データセンターに接続する方法を説明しています。Google Cloud は、プライベート接続オプションとして Partner Interconnect と Cloud VPN もサポートしています。これらのサービスが接続要件を満たしているかどうかも検討してみてください。

7.3) IP 空間割り振り

Google Cloud の基盤を適切に構築するには、Google Cloud 環境用の IP アドレス範囲を割り振る必要があります。Google Cloud は、RFC-1918 空間と非 RFC-1918 空間の両方を含むさまざまな有効な IP 範囲をサポートしています。予約済みと制限付きの IP 範囲はサブネット内で使用できないので注意してください。example.com リファレンス アーキテクチャでは、プロジェクトの作成時にサブネットに IP 範囲を割り当てます。

表 2.16 は、example.com リファレンス アーキテクチャ内の共有 VPC ネットワークに割り振られる IP アドレス空間の内訳を示しています。この IP アドレス割り振りは、Google Cloud 環境で連続した /16 分の RFC 1918 IP アドレス範囲が割り当てられることを前提としています。example.com アーキテクチャを使用した 3 つの環境があるとすると、各環境には、ベース共有 VPC ネットワークと制限付き共有 VPC ネットワーク間で共有される /18 のアドレス範囲が割り振られます。各共有 VPC ネットワークは、/20 の範囲を割り振り済みのネットワーキング空間に、/20 の範囲を未割り振りの空間に割り振ります。割り振り済みの IP アドレス空間から、その範囲がさらに 2 つの /21 サブネットに分割されます。それぞれのサブネットが 1 つのリージョンに相当します。VPC ネットワーク内の未割り振りの空間は、独自の IP アドレス空間が必要なピアリングされたサービス（Cloud SQL など）で使用できます。RFC 1918 IP アドレス空間が限られている場合は、非 RFC 1918 アドレス空間を使用できます。ただし、オンプレミス ネットワーキングがこのようなトポロジをサポートしている必要があります。

VPC	リージョン	環境		
		本番	非本番	開発
基本	リージョン 1	10.0.0.0/21	10.0.64.0/21	10.0.128.0/21
	リージョン 2	10.0.8.0/21	10.0.72.0/21	10.0.136.0/21
	未割り振り	10.0.16.0/20	10.0.80.0/20	10.0.144.0/20
制限付き	リージョン 1	10.0.32.0/21	10.0.96.0/21	10.0.160.0/21
	リージョン 2	10.0.40.0/21	10.0.104.0/21	10.0.168.0/21
	未割り振り	10.0.48.0/20	10.0.112.0/20	10.0.176.0/20

表 2.16 共有 VPC の IP アドレス空間割り振り

表 2.17 は、example.com リファレンス アーキテクチャをサポートするために必要な追加の IP アドレス範囲を示しています。

プロジェクト	説明	IP 範囲
DNS ハブ	Cloud DNS がオンプレミスに接続するための独立したサブネットをサポートするための IP 空間。	172.16.0.0/24
CICD	デプロイ パイプライン用の独立したサブネットをサポートするための IP 空間。	172.16.1.0/24

表 2.17 追加の example.com IP アドレス空間割り振り

注: Google Cloud はエイリアス IP 範囲をサポートしているため、内部 IP アドレスの範囲をエイリアスとして VM のネットワーク インターフェースに割り当てることができます。これは、VM 上で複数のサービスを実行しており、サービスごとに異なる IP アドレスを割り当てる場合に便利です。エイリアス IP 範囲は GKE Pod でも使用できます。

7.4) DNS の設定

Google Cloud とオンプレミス間で DNS 情報を渡すには、Cloud DNS で 35.199.192.0/19 をオンプレミス ネットワークにアドバタイズする必要があります。複数の DNS インスタンスを処理するために、Cloud DNS はネイティブなピアリング機能を備えています。この機能を使用すれば、図 2.9 に示すように、中央のハブ DNS インスタンスを作成して、それに他の DNS インスタンスをピアリングさせることができます。Cloud DNS ピアリングは、論理的構造であり、プロジェクト間をネットワークで接続する必要はありません。

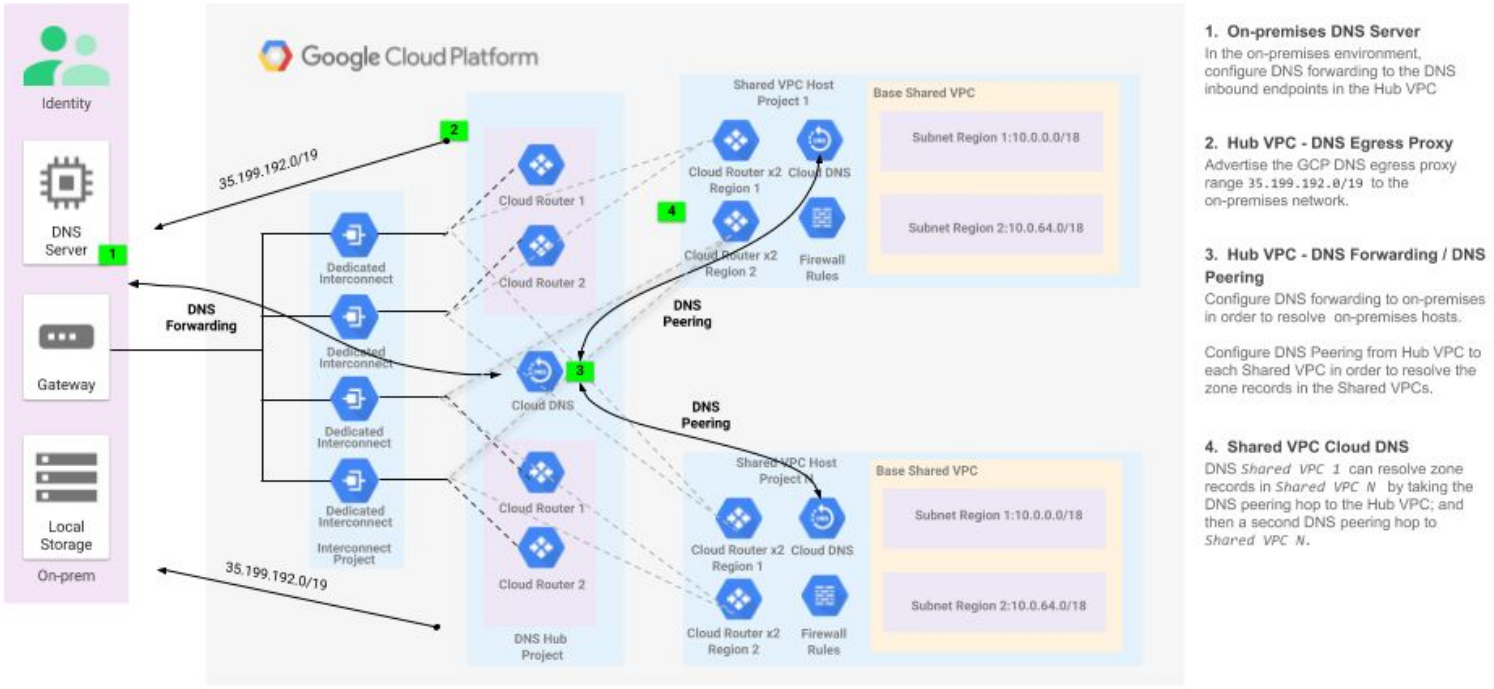


図 2.9 example.com 用の Cloud DNS の設定

DNS ハブ プロジェクト内の DNS ハブ VPC ネットワークは、DNS 構成の中央 VPC ネットワークとして使用されます。DNS ハブ プロジェクトは example.com のオンプレミス インフラストラクチャに接続する必要があります。この接続は、Dedicated Interconnect VLAN アタッチメントと、ハブ VPC ネットワークとオンプレミス間で確立された BGP セッションを介して実現されます。この VLAN アタッチメントは、本番環境、非本番環境、開発環境向けの共有 VPC ネットワークで使用される VLAN アタッチメントとは異なります。ハブ VPC ネットワークは共有 VPC ネットワークに接続されません。

DNS ハブが確立されたら、Cloud Router を介して、Google Cloud DNS の下り（外向き）プロキシ範囲 35.199.192.0/19 をオンプレミス ネットワークにアドバタイズする必要があります。オンプレミス環境では、DNS ハブ VPC ネットワーク内の DNS 受信エンドポイントへの DNS 転送を使用してエンタープライズ DNS を構成する必要があります。

DNS ハブ VPC ネットワークから各共有 VPC ネットワークへの DNS ピアリングは、共有 VPC ネットワーク内のゾーンレコードが解決されるように構成されます。Cloud DNS は、推移的 DNS ピアリングはサポートしていますが、単一の推移的ホップを介した場合に限られます。つまり、関与できる VPC ネットワークは最大 3 つです（真ん中のネットワークが推移的ホップになります）。たとえば、図 2.9 のアーキテクチャと、DNS 情報を交換する必要のある 2 つの VPC ネットワーク（共有 VPC 1 と共有 VPC 16）について考えてみましょう。共有 VPC 1 は、DNS ハブ VPC への DNS ピアリングをホップしてから、共有 VPC 16 への 2 つ目の DNS ピアリングをホップすることによって、共有 VPC 16 内のゾーンレコードを解決できます。

7.5) Dedicated Interconnect を使用したプライベート IP アドレス経由の Google Cloud APIs へのオンプレミス アクセス

example.com で、プライベート IP アドレスのみを持つオンプレミス ホストから限定公開の Google Cloud API へのアクセスを設定するために、Google Cloud は、仮想 IP アドレス（VIP）と呼ばれる 2 つの個別の /30 IP エンドポイントを用意しています。この VIP には、Dedicated Interconnect 接続を介してアクセスできます。

基本 VPC ネットワークでアクセス可能な Google Cloud APIs については、オンプレミス ホストが `private.googleapis.com` を `199.36.153.8/30` に解決することによって、これらの API にアクセスできます。`private.googleapis.com` VIP は、ほとんどの Google API へのアクセスを可能にします。これはパブリック IP アドレスですが、Google がインターネット上でアナウンスすることはありません。図 2.7 で示したように、基本 VPC ネットワークの Cloud Router は、Dedicated Interconnect 接続を介して `private.googleapis.com` ルートをオンプレミス ホストにアナウンスします。

制限付き VPC ネットワークでアクセス可能な Google Cloud APIs については、オンプレミス ホストが `restricted.googleapis.com` を `199.36.153.4/30` に解決することによって、これらの API にアクセスできます。`restricted.googleapis.com` の VIP は、サービス境界でアクセス可能な Google API へのアクセスを可能にします。これはパブリック IP アドレスですが、Google がインターネット上でアナウンスすることはありません。図 2.7 で示したように、制限付き VPC Cloud Router は、相互接続を介して restricted.googleapis.com ルートをオンプレミス ホストにアナウンスします。

Google Cloud で動作する外部 IP アドレスを持たない VM については、限定公開の Google アクセス経由での Google Cloud APIs への限定公開アクセスがプロジェクト作成時に有効になります。

> **注:** `private.googleapis.com` と `restricted.googleapis.com` の両方をサポートするためには、オンプレミスでの DNS リダイレクトが必要です。オンプレミス ワークロードが API 呼び出しをプライベート VIP または制限付き VIP のいずれかに対して行うよう、ワークロード単位で管理する必要があります。加えて、VPC Service Controls を最大限活用できるよう、クラウドベースのワークロード向けに制限付き VPC ネットワークで同じ DNS の間接参照とルーティングを設定する必要があります。

7.6) VPC ファイアウォール ルール

example.com リファレンス アーキテクチャは、VPC ファイアウォール ルールとネットワーク タグを組み合わせて、VM へのトラフィックを制限します。VPC ファイアウォール ルールは共有 VPC ネットワーク内に存在し、セクション 5 で説明したプロジェクト デプロイ パイプラインを介してデプロイされます。ネットワーク タグは Google Cloud インスタンスに追加され、トラフィックがそれらのタグに照らして評価されます。デフォルトで、example.com は、優先度が 65530 の「すべて拒否」ファイアウォール ルールを使用して、明示的に許可されていないすべてのトラフィックが拒否されるようにします。リソースから `private.googleapis.com` VIP または `restricted.googleapis.com` VIP に

アクセスするためには、トラフィックがそれらの IP アドレスに流れることを許可するファイアウォール ルールを作成する必要があります。

図 2.10 は、VPC ファイアウォールとネットワーク タグが example.com 環境でどのように機能するかを示しています。

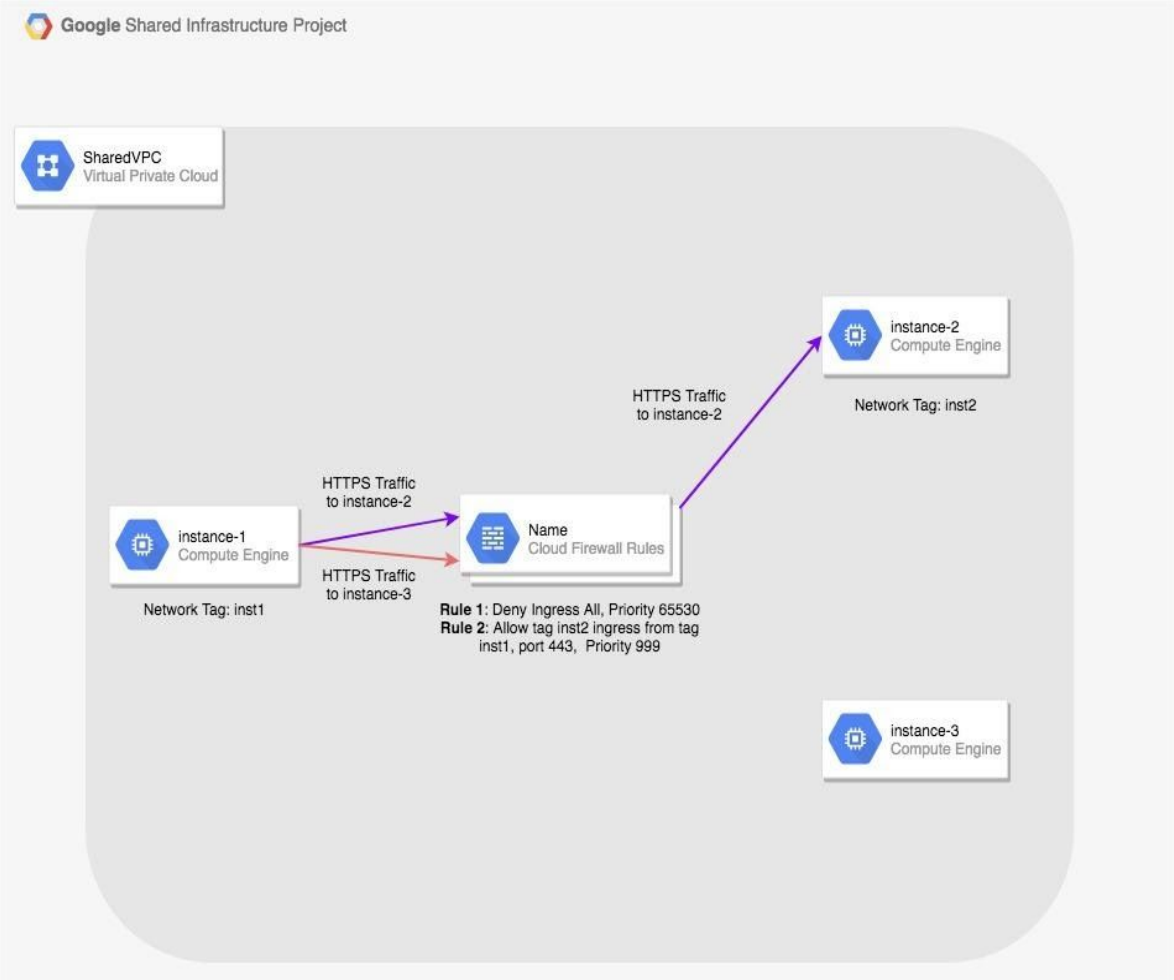


図 2.10 example.com のファイアウォール ルール

example.com のデフォルトの「すべて拒否」ファイアウォール ルール（ルール 1）はすべてのインスタンスに適用されます。より優先度が高いもう一つのファイアウォール ルール（ルール 2）では、`inst2` タグが付けられたコンピューティング インスタンスに対し、上り（内向き）トラフィックをポート 443 で許可します。つまり、`instance-2` という名前のインスタンスは、inst2 タグが付いているため、ポート 443 上で受信トラフィックを受信できます。一方、`instance-3` という名前のインスタンスは、ファイアウォール ルールと一致するタグが付けられていないため、受信トラフィックを受信できません。

ネットワーク タグをVM に対して追加または削除できるのは、オーナー、編集者、または Compute インスタンス管理者のいずれかのロールを持っているユーザーです。ネットワーク タグがより安全な方法で使用されるようにするために、example.com リファレンス アーキテクチャは、オーナー、編集者、

Compute インスタンス管理者の各ロールがセクション 6.3 で説明したファイアコール プロセス以外でユーザーまたはグループに付与されないように制限します。

Compute インスタンス管理者ロールがユーザーまたはグループに必要な場合は、`compute.instances.setTags` 権限を除く `compute.instance.admin` ロールのすべての権限を持つカスタムロールを作成できます。このカスタムロールを持つユーザーまたはグループは、VM 上でタグを追加および削除できません。タグは、ワークロード タイプに応じた異なる制御メカニズムによって追加する必要があります。

注: 基盤内で複数のワークロードを実行できるようにするには、ファイアウォール ルールを追加する必要があります。たとえば、上り（内向き）トラフィックを伴う Google Kubernetes Engine ベースのワークロードを実行するには、特定の IP 範囲から Google Kubernetes Engine にアクセスできるようにする必要があります。Firewall Insights は、ファイアウォール ルールの使用状況を可視化して、ファイアウォール ルール構成の問題を検出します。これを使用すれば、デプロイされたファイアウォール ルールを分析し、許可範囲が広すぎるファイアウォール ルールを検出できます。

8. シークレット管理

example.com リファレンス アーキテクチャは、Google Secret Manager を利用することで、API キー、パスワード、証明書などの機密データを安全に保管する方法を提供しています。シークレットへのアクセスは Cloud IAM を介して制御され、組織、フォルダ、プロジェクト、シークレットごとに個別に管理されます。Secret Manager には、次の 5 つの IAM ロールが用意されており、これによってデフォルトの職務の分離が作成されます。 Secret Manager シークレット アクセス担当者は、ペイロードを調査できます。シークレット バージョン追加担当者は、シークレットに新しいバージョンを追加できます。シークレット バージョン マネージャーは、シークレットのバージョンを作成して管理できます。Secrets Manager 閲覧者は、すべての Secret Manager リソースのメタデータを表示できます。Secrets Manager 管理者は、すべての Secret Manager リソースにアクセスして管理できます。

図 2.3 に示すように、example.com 組織には、シークレットを組織レベルと環境（フォルダ）レベルで格納するためのプロジェクトがあります。複数のシークレット リポジトリを設ける目的は、組織レベルのシークレットと環境レベルのシークレットを明確に分離することです。組織シークレットと本番環境シークレットは、セクション 6.2 で説明したように、シークレット グループごとに管理されます。シークレットの作成、アクセス ポリシーの定義、シークレットのライフサイクルの管理はシークレット グループが担当します。

9. ロギング

ロギングは、開発組織、監査組織、セキュリティ組織に重要な機能を提供するだけでなく、規制の遵守も支援します。図 2.11 に示すように、example.com 組織には Google Cloud Logging によって集約されるさまざまなロギングソースがあります。

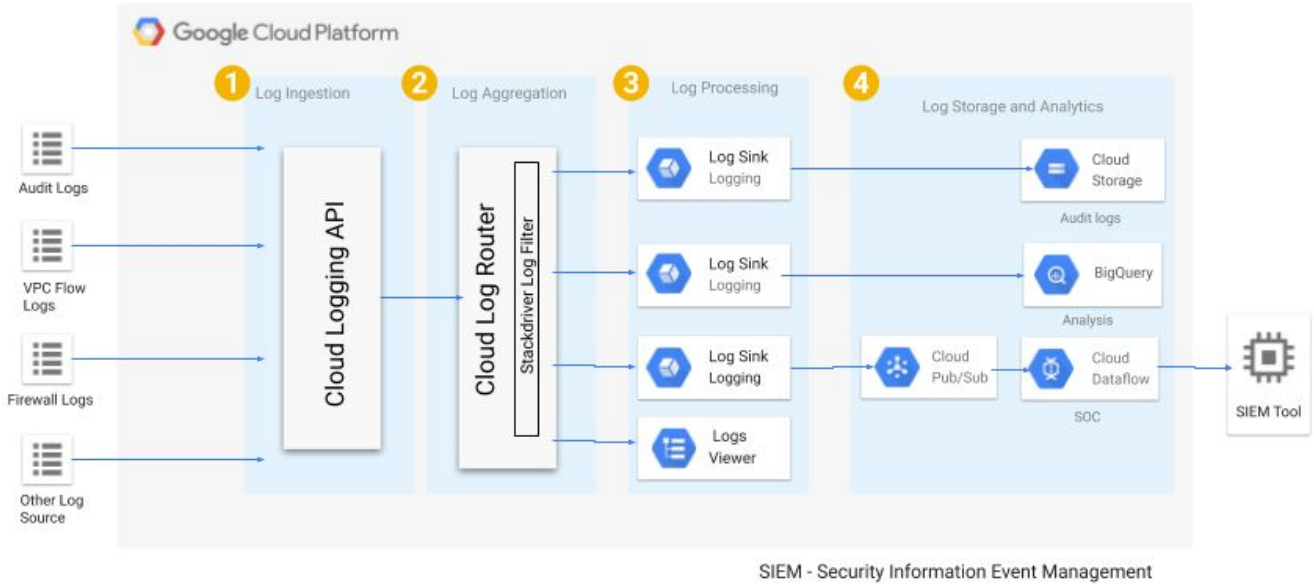


図 2.11 example.com のロギングソース

example.com リファレンス組織内では、ロギング機能を 2 つのプロジェクトに分割しています。

- Logging という名前のスタンドアロン ロギング プロジェクト。このプロジェクトには、example.com 組織によって生成されるログの収集と処理に使用される Pub/Sub トピック、Cloud Functions の関数、BigQuery インスタンスが含まれています。
- SCC という名前の SCC アラート センター プロジェクト。このプロジェクトには、Security Command Center からの通知 Pub/Sub トピックが含まれています。これはロギング プロジェクトとは異なるため、一般的なログアクセスが必要な運用チームと、特定のセキュリティ情報やイベントへのアクセスが必要なセキュリティ チーム間で職務を明確に分離できます。

Google Cloud では、ログが Cloud Logging API に送信され、Logs Router を通過します。Logs Router は、既存のルールに照らして各ログエントリをチェックし、破棄するログエントリ、Cloud Logging に取り込む（保存する）ログエントリ、ログシンクを介してエクスポートするログエントリを決定します。表 2.18 は、example.com 基盤の一部として収集されるログとログを有効化する方法を示しています。

ログソース	説明	管理
監査ログ	Google Cloud サービスは、これらのログに監査ログエントリを書き込み、Google Cloud リソースに対して「誰が、いつ、どこで、何を実行したか」という問いに答えます。	組織レベルで有効にされ、組織初期設定中にパイプラインによって構成されます。
VPC フローログ	VPC フローログは、VM インスタンス（GKE ノードとして使用されるインスタンスを含む）との間で送受信されたネットワーク フローのサンプルを記録します。	各 VPC サブネットによって有効にされ、プロジェクトの作成中にパイプラインによって構成されます。
ファイアウォール ルール ロギング	ファイアウォール ロギングは、ファイアウォール ルールがトラフィックを許可または拒否するたびにレコードを 1 つ作成します。	各ファイアウォール ルールに対して有効にされ、ファイアウォールの作成中にパイプラインによって構成されます。
G Suite 監査ロギング	G Suite は、そのログを Google Cloud Logging サービスと共有できるようにしています。G Suite は、ログインログ、管理ログ、およびグループ ログを収集します。	組織レベルで有効にされ、Cloud Identity 管理コンソールを介して構成されます。
データアクセス監査ログ	データアクセス監査ログは、リソースの構成またはメタデータを読み取る API 呼び出しと、ユーザーが提供したリソースデータの作成、変更、読み取りを行うユーザー ドリブンな API 呼び出しを記録します。	組織レベルで有効にされ、組織初期設定中にパイプラインによって構成されます。
アクセスの透明性ログ	アクセスの透明性は、Google 担当者がお客様のコンテンツにアクセスする際に行うアクションを記録したログを提供します。	組織レベルで有効にされ、Google Cloud を使用してサポートケースを作成することで構成されます。

表 2.18 example.com のログソース

シンクへのエクスポートを行うには、エクスポートするログエントリを選択するクエリを記述し、Cloud Storage、BigQuery、Pub/Sub から宛先を選択します。クエリを変更することによって一部のロギング情報を除外できます。表 2.19 は、example.com アーキテクチャで使用されるシンクについて説明しています。

シンク	説明	目的
`sk-c-logging-bq`	組織からロギング プロジェクト内の BigQuery テーブルに集計ログを送信します。	集計ログは、BigQuery で分析され、セクション 10 で説明する発見的コントロール アーキテクチャの一部として使用できます。
`sk-c-logging-bkt`	組織からロギング プロジェクト内の Cloud Storage バケットに集計ログを送信します。	集計ログは、コンプライアンス、監査、インシデント追跡の目的で使用できます。規制目的では、Cloud Storage バケットロックを適用できます。

sk-c-logging-pub	組織からロギング プロジェクト内の Pub/Sub トピックに集計ログを送信します。	セクション 10 で説明するように、集計ログは Pub/Sub から Dataflow ジョブに送信され、そこから外部 SIEM に送信されます。

表 2.19 example.com のログシンク

シンクとシンク先は、組織オブジェクトが初めて作成され、構成されたときにデプロイ パイプラインを介して作成されます。シンクが作成されると、サービス アカウント ID が返されます。このサービス アカウントは、指定された宛先に書き込む権限を持っている必要があります。この権限も設定中に構成されます。

注: 環境をモニタリングして管理するためには、ロギングとともに、SRE の概念（SLI、SLO、SLA）が必要になります。

10. 発見的コントロール

発見的コントロールは、プラットフォーム テレメトリーを使用して、クラウド環境内の構成ミス、脆弱性、潜在的な悪意のあるアクティビティを検出します。図 2.12 に示すように、example.com リファレンス アーキテクチャは、セキュリティ体制全体をサポートする幅広い発見的コントロールを備えています。

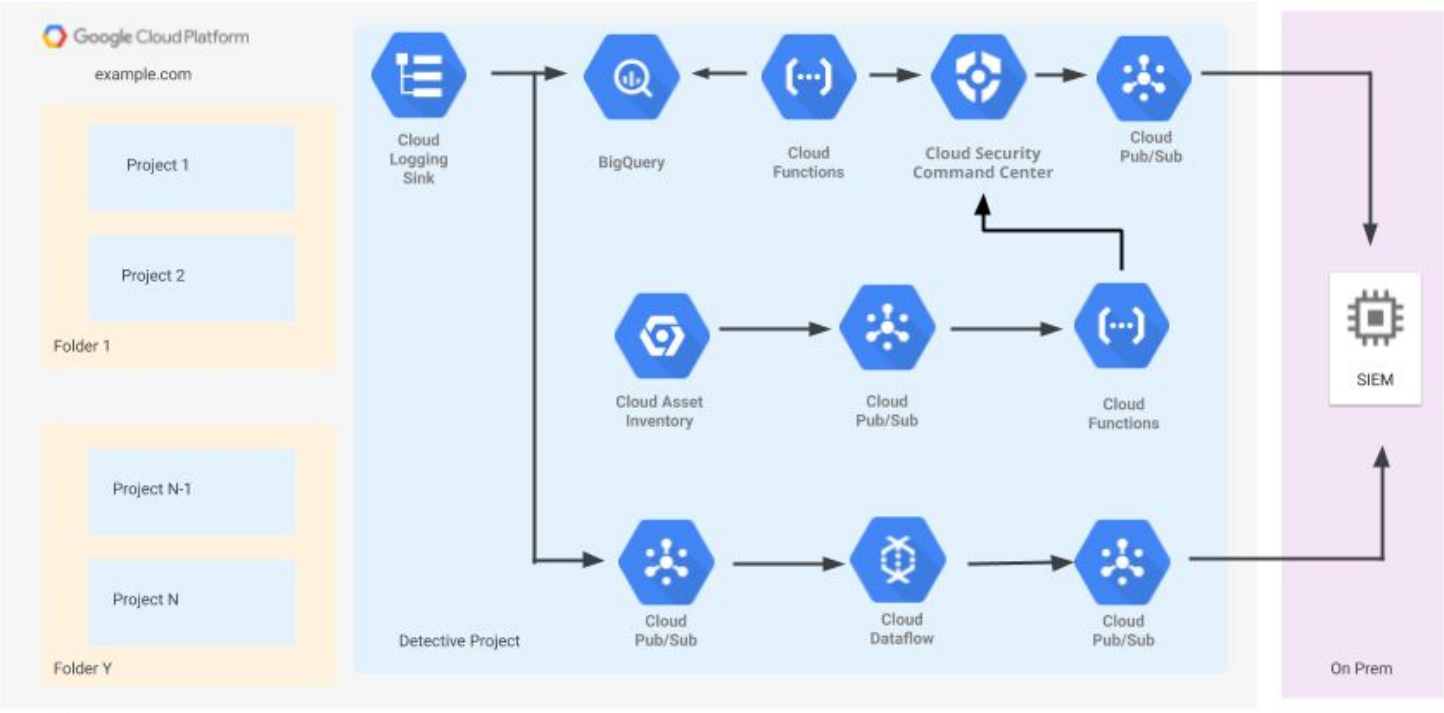


図 2.12 example.com の発見的コントロール アーキテクチャ

example.com アーキテクチャには、以下の発見的コントロールが含まれています。

- Security Command Center を介した Google セキュリティ ソース。これには、セキュリティの構成ミス情報や脆弱性の変化が含まれています（詳細については、次のセクションをご覧ください）。
- Chronicle への Google Cloud ログの接続。
- Cloud Asset Inventory からのアセット変更とポリシー遵守に関する通知。
- SIEM ツールに送信された Google Cloud Logging からのログ（G Suite 監査ログを含む）。
- サーバーレスな BigQuery ベース ツールからのカスタム知見。

加えて、サードパーティ プロバイダからの既存のイベントソースがある場合や独自のカスタムソースとカスタム知見を作成している場合は、それらの知見を Security Command Center に統合できます。

10.1) Security Command Center

Google Cloud の Security Command Center には、セキュリティの知見を集約して管理するための単一のユーザー インターフェースとデータ プラットフォームが備わっています。example.com アーキテクチャは、Security Command Center を使用して、10.1.2 セキュリティ ソース セクションで示す Google セキュリティ ソースからのネイティブな知見と BigQuery 分析ソリューションからのカスタム知見を集約します。その後で、SIEM で使用される Pub/Sub トピックに Security Command Center 通知を送信します。

10.1.1) プレミアムとスタンダード

Google Security Command Center には 2 つのバージョンがあります。

- **Security Command Center プレミアム**：セキュリティに関する厳しい要件を抱えるお客様、特に企業のお客様向けです。包括的な脆弱性と脅威の検出機能と、サードパーティ SIEM への接続および応答と修正アクションの自動化の両方を簡素化する統合オプションを提供します。Security Command Center プレミアムは有料サービスです。
- **Security Command Center スタンダード**：Security Command Center プレミアムの基本的な一部の機能をすべてのお客様に提供します。お客様が社内環境での重大な脆弱性を検出、特定、アラート生成、管理、対応できるようにすることに重点を置いています。Security Command Center スタンダードは無料でご利用いただけます。

プレミアムとスタンダードのいずれでも、一部の Security Command Center 機能を有効にでき、また Security Command Center のネイティブ検出項目の設定と構成を統一された方法で一元的に管理できます。

Security Command Center プレミアムとスタンダードの両方に組み込まれているセキュリティ ソースは、Google Cloud 組織の既存のフォルダとプロジェクト、および今後作成されるフォルダとプロジェクトに適用されるようにデフォルトで設定されています。セキュリティ上特別な状況ではない限り、このデフォルト設定を変更しないでおくことをおすすめします。

10.1.2) セキュリティ ソース

Security Command Center では、Google が提供する固有の知見、サードパーティの知見、お客様が生成する独自の知見を含む、各種セキュリティ ソースからの知見が集約されます。表 2.20 に、example.com リファレンス アーキテクチャに対して有効なセキュリティ イベントソースの一覧を示します。

セキュリティ イベント ソース	説明
Security Health Analytics	一般的な脆弱性、構成ミス、セキュアな構成からのずれを検出します。

Anomaly Detection	システムの外部からの挙動シグナルを使用して、プロジェクトと VM インスタンスでクラウドの不正使用にともなう挙動を検出する際に役立つ詳細な情報を表示します。
Event Threat Detection	さまざまなログを自動的にスキャンし、Google Cloud 環境での疑わしいアクティビティの有無を確認します。
Web Security Scanner	公開ウェブ アプリケーションをスキャンし、一般的なアプリケーション脆弱性の有無を確認します。
Container Threat Detection（**ベータ版**）	リバースシェル、疑わしいバイナリやライブラリを検出するための GKE コンテナ向けランタイム セキュリティを実現します。

表 2.20 example.com のセキュリティ イベントソース

注: Security Command Center はさまざまなサードパーティ セキュリティ ソースとも統合されています。また、お客様のアプリケーションで findings API および sources API を使用して、Security Command Center で独自の知見を生成できます。サードパーティ セキュリティ ソースや独自の知見を使用している組織では、生成される知見を Security Command Center ダッシュボードで管理できます。知見は、Security Command Center API 通知を使用して他のシステム（エンタープライズ SIEM など）と共有することもできます。

10.1.3) 基本的なセキュリティ アラートの設定

検出だけではなく、検出された脆弱性や脅威に対応し、修正するアクションを実行できることが重要です。組み込みの Security Command Center Pub/Sub トピックを利用して Security Command Center の知見を下流のアラート生成システム、サポート チケット機能、ワークフロー、SOAR システム、SIEM に接続します。Security Command Center Pub/Sub 通知は一連の通知構成により管理されます。通知構成を作成するには、gcloud ツールを使用するか、またはクライアント ライブラリと API を使用します。最初に専用の SCC Alerts プロジェクトを作成し、通知構成の変更と管理が許可されているユーザーとサービスのみに IAM アクセスを制限します。これで、プロジェクト内でイベントをパブリッシュする Pub/Sub トピックを設定できます。トピックごとに、トピックへのアクセス権を、職務上そのトピックのセキュリティ知見情報にアクセスする必要があるユーザーとサービスのみにさらに制限します。

10.1.3.1) 通知の構成

セキュリティ アラート プロジェクトを作成し、トピックを作成したら、通知構成を定義します。詳しい手順については、Security Command Center ドキュメントの検出通知の設定をご覧ください。通知構成の管理については、通知構成の作成と管理をご覧ください。通知のフィルタリングについては、通知のフィルタリングをご覧ください。

通知構成のデフォルトの割り当ては、組織あたり 500 です。これを超える割り当てが必要な場合は、Google Cloud Console を使用して Security Command Center API 割り当ての増加リクエストを送信してください（図 2.13 を参照）。

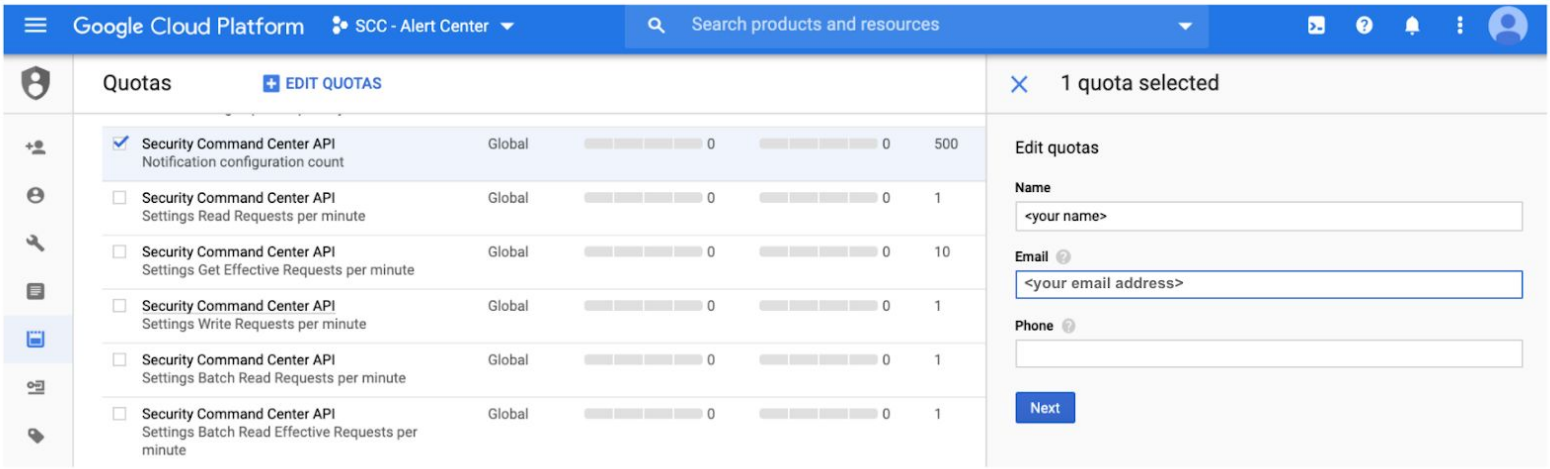


図 2.13 Cloud Console での追加の通知構成割り当てのリクエスト

最初に作成するべき通知は、Security Command Center のすべての知見を Pub/Sub トピックに送信し、その後 Pub/Sub トピックからSIEM に転送するという構成です。これを実現するために、次のロールが必要です。

- セキュリティ センター管理者（幅広い権限を持つ）
  または
  Security Center Notification Config Editor（より特化した権限を持つ）
- Pub/Sub トピックの Pub/Sub 管理者

ロールを設定したら、以下の手順に沿って操作します。

1. Cloud Console で Cloud Shell を開くか、または Cloud SDK がインストールおよび構成されているコンピュータでターミナルを開きます。
2. Pub/Sub トピックを設定します。

```
# topic-id = siem-export
gcloud pubsub topics create topic-id
export TOPIC_ID=topic-id

# subscription-id = siem-subscription
gcloud pubsub subscriptions create subscription-id --topic topic-id
```

3. フィルタを使用して通知構成を設定します。

```
export ORGANIZATION_ID=organization-id
export PUBSUB_PROJECT=project-id
```

```
export GCLOUD_ACCOUNT=your-username@email.com
```

4. gcloud アカウントに必要なロールと権限を付与します。

```
gcloud pubsub topics add-iam-policy-binding \
    projects/$PUBSUB_PROJECT/topics/$TOPIC_ID \
    --member="user:$GCLOUD_ACCOUNT" \
    --role='roles/pubsub.admin'

gcloud organizations add-iam-policy-binding $ORGANIZATION_ID \
    --member="user:$GCLOUD_ACCOUNT" \
    --role='roles/securitycenter.notificationConfigEditor'

# The topic to which the notifications are published
PUBSUB_TOPIC="projects/project-id/topics/topic-id"

# The description for the NotificationConfig
DESCRIPTION="Notifies for active findings"

# Filters for all active findings - both vulnerabilities and threats
FILTER="state=\"ACTIVE\""

gcloud alpha scc notifications create notification-name \
    --organization "$ORGANIZATION_ID" \
    --description "$DESCRIPTION" \
    --pubsub-topic $PUBSUB_TOPIC \
    --filter $FILTER
```

クライアント ライブラリと API を使用した通知構成の設定方法を含む詳細な手順については、検出通知の設定をご覧ください。

10.1.3.2) 組織階層に合わせた通知構成

通知トピックの定義と編成を使用して、組織内の該当するチームにセキュリティ アラートを転送するように構成できます。Security Command Center では一連の通知構成を作成して保管できます。通知構成は、選択フィルタと Pub/Sub トピックの固有の組み合わせです。以下を管理することで、セキュリティに関する知見と特定の要件を一致させ、IAM アクセス ポリシーを適用します。

- 作成する通知構成の数。
- 各構成の選択フィルタ。
- 選択およびフィルタされた検出結果イベントがパブリッシュされるトピックの名前。

以降のセクションでは、通知構成とトピック パターンの 4 つの例を説明します。

10.1.3.2.1) 1 つのセキュリティ キュー

最も単純なパターンは、すべてのプロジェクトおよび知見カテゴリを対象とした選択フィルタセットと、1 つのトピックに設定されたターゲット（例: `gcp-security-alerts`）を含む 1 つの通知構成です。このパターンは、Google Cloud セキュリティの脆弱性と脅威に関するすべての知見を 1 つの一元化された Security Operations Center（SOC）に転送するお客様向けです。

10.1.3.2.2) 事業部門別

各事業部門に専用の SOC があり、インフラストラクチャ、ワークロード、アプリケーションの全体的なセキュリティの責任を各事業部門が負うアプローチを採用している場合には、複数の通知構成を作成します。次に、事業部門の SOC ごとに固有の Security Command Center 通知構成と専用トピックを設定します。通知構成の選択フィルタにより、事業部門の範囲内のすべてのプロジェクトと、すべての知見カテゴリが選択されます。この構成では、各事業部門チーム間での専用トピックの分離と IAM コントロールが可能になるので、各チームはそれぞれに関連する脆弱性と脅威のシグナルだけにアクセスでき、またそのシグナルを受信します。

10.1.3.2.3) クラウドネイティブ DevSecOps

同様に、各アプリケーション チームがチームのインフラストラクチャ、ワークロード、アプリケーションの全体的なセキュリティ上の責任を負うアプローチを採用している場合には、複数の通知構成を作成します。次に、アプリケーション チームごとに専用トピックを使用して固有の Security Command Center 通知構成を設定します。この通知構成の選択フィルタにより、アプリケーション チームの範囲内のすべてのプロジェクトとすべての知見カテゴリが選択されます。この構成では、各アプリケーション チーム間での専用トピックの分離と IAM コントロールが可能になるので、各アプリケーション チームはそれぞれに関連する脆弱性と脅威のシグナルだけにアクセスでき、またそのシグナルを受信します。

10.1.3.2.4) セキュリティに関する知見のカテゴリ分け

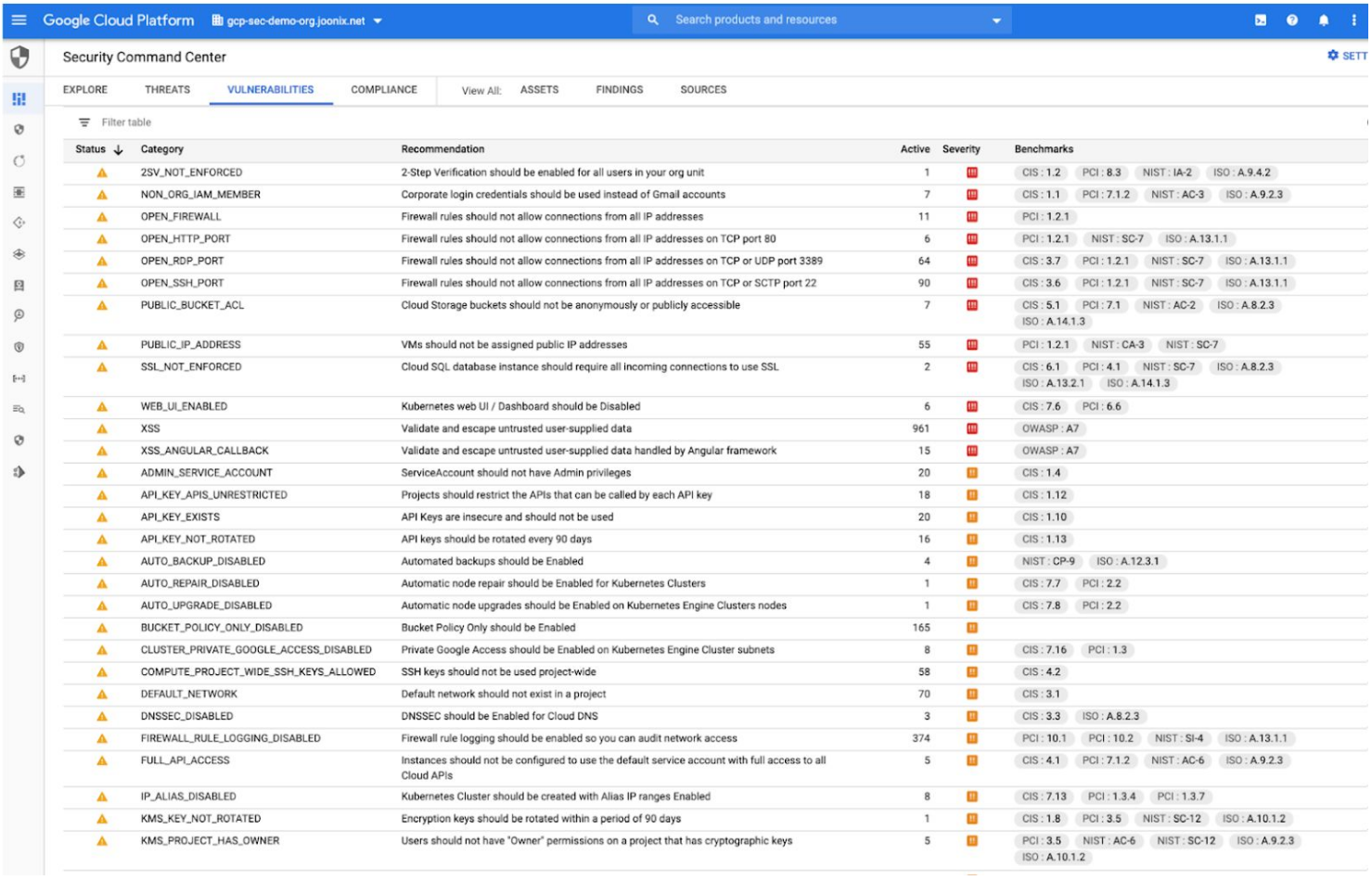
お客様社内のさまざまなチームがそれぞれ異なるタイプのセキュリティに関する知見を処理するアプローチを採用している場合は、複数の通知構成を作成します。最も一般的な例としては、脆弱性と構成ミスの対応と修正を、リアルタイムでのアクティブな脅威の対応と修正から切り離すことがあります。この場合多くのお客様は前者をクラウド セキュリティ チームに割り当て、後者を SOC に割り当てています。この例の場合、2 つのチームに対して固有の Security Command Center 通知構成と専用の Pub/Sub トピックを設定できます。構成ミスと脆弱性の通知構成に含まれる選択フィルタでは、脆弱性に関するすべての知見ソースとすべてのプロジェクトが選択されます（Security Health Analytics や Web Security Scanner など）。脅威の通知構成に含まれる選択フィルタでは、脅威に関するすべての知見ソースとすべてのプロジェクトが選択されます（例: Event Threat Detection、Container Threat Detection(ベータ版)、Abuse Anomaly Detection など）。

10.2) 脆弱性とずれの検出

構成のずれとは、事前定義の標準またはベースラインから逸脱した構成の変更を指します。時間の経過に伴ってソリューションが進化するうえである程度のずれが生じることは必然ですが、セキュリティと安定性の理由から、一部の構成詳細については違反があってはなりません。ずれの管理は、管理者が通知を受信し、必要に応じて措置をとる手動プロセスで行うことも可能です。ただし、特定の変更についてこの処理を自動化し、ポリシーに違反する変更を元に戻すことができます。

10.2.1) Security Command Center プレミアムを使用した組み込みのずれ検出機能

Security Command Center プレミアムに組み込まれている Security Health Analytics は、Security Command Center によりサポートされている組織内のすべてのリソースに対し、100 を超える構成ミスおよび脆弱性のチェックを毎日自動的に実行します。その結果の評価は Security Command Center ダッシュボードの [脆弱性] タブに表示されます。組織レベルのデータまたは特定のプロジェクトのデータを表示して確認できます。また、データをステータス、カテゴリ、推奨事項、重大度、アクティブまたは非アクティブ、コンプライアンス ベンチマークに基づいてさらに細かくフィルタできます。その後ダッシュボードの [コンプライアンス] タブで、評価結果が CIS 1.0、NIST-800-53、PCI-DSS、ISO 27001 の各ベンチマークと照合され、組織全体またはお客様が選択した一連のプロジェクト向けに要約されます。この 2 つのタブの例を図 2.14 に示します。



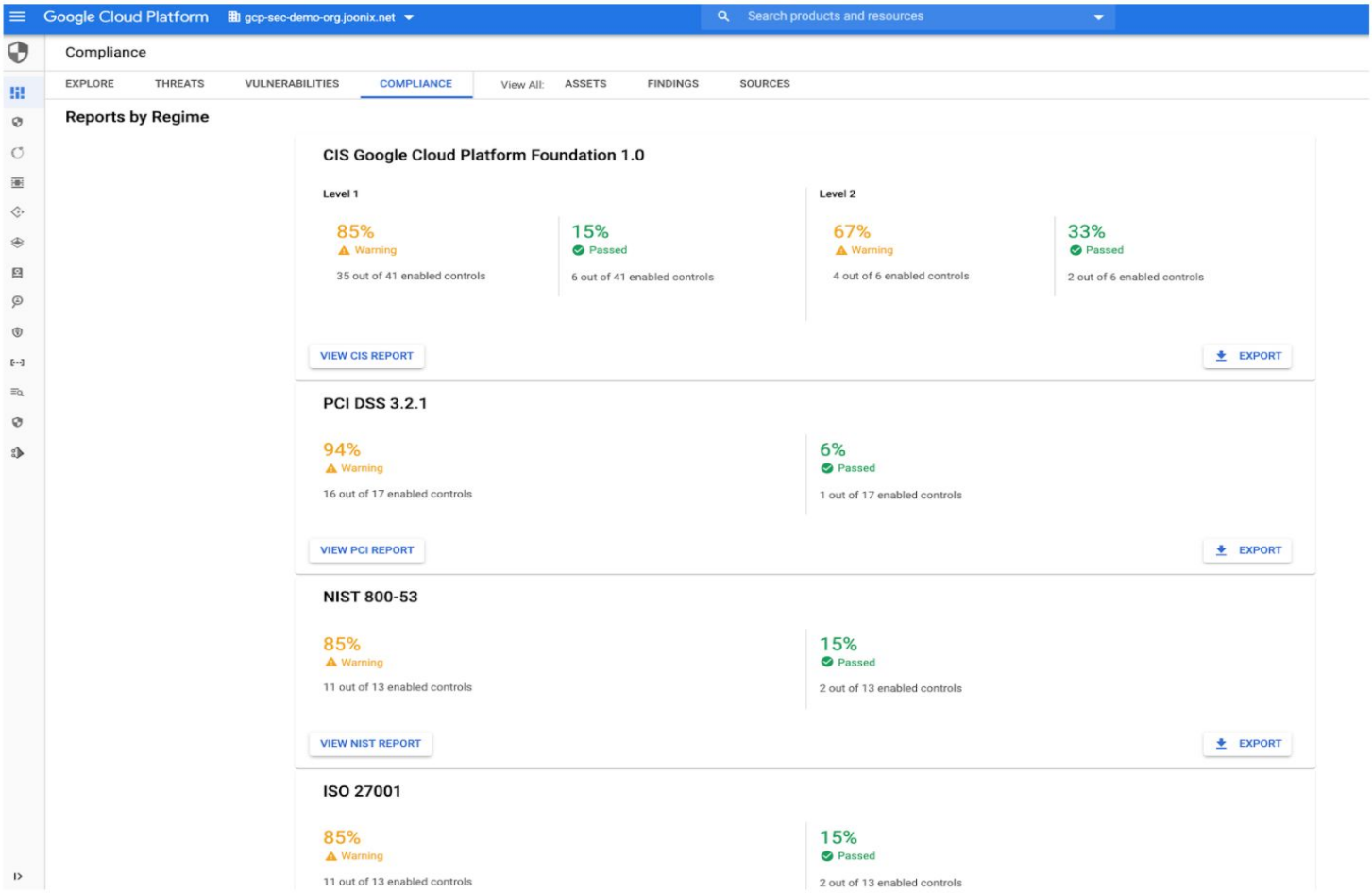


図 2.14 Security Command Center Premium の [脆弱性] タブと [コンプライアンス] タブ

Security Command Center では、Security Health Analytics の知見の変更に関するアラートを生成するように各種通知構成を設定できます。これにより、目的のリソースの構成のずれを特定できるようになります。また Security Command Center ダッシュボードの [変更済みアセット] ビューと [変更された知見] ビューを使用して、ユーザーが選択した時間範囲（過去 1 時間、前日、過去 7 日間、過去 30 日など）における変更を検出して確認できます。この 2 つのタブの例を図 2.15 に示します。

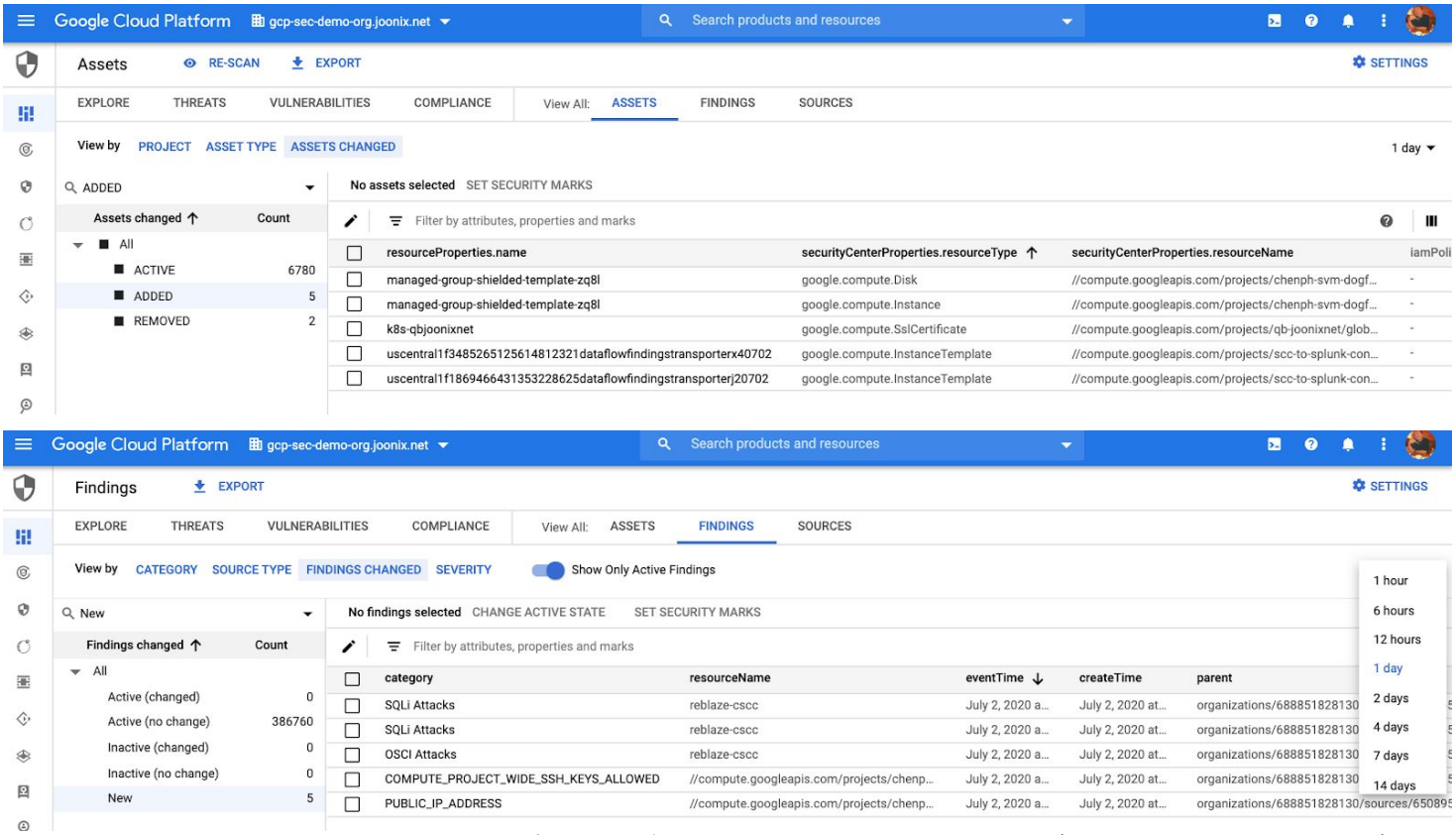


図 2.15 Security Command Center ダッシュボードの [変更済みアセット] タブと [変更された知見] タブ

ダッシュボードでは、現時点（現在時刻）を基準にした時間範囲を確認できます。基準時点を異なる時刻にする場合は、Security Command Center コマンドライン インターフェース、API またはクライアント ライブラリを使用して、独自の基準時点を設定できます。

10.2.2) マネージド ウェブ脆弱性スキャン

ウェブ アプリケーションをデプロイする場合は、Security Command Center プレミアムの組み込みマネージド ウェブ脆弱性スキャンも使用してください。現在、Web Security Scanner には OWASP 上位 10 の脆弱性のうち 4 つに対応する 13 の組み込みウェブ脆弱性検出機能があります。マネージド スキャンは週 1 回自動的に実行され、公開ウェブ エンドポイントを検出およびスキャンします。

10.3) アクティブな脅威の検出

組み込みの脆弱性および構成ミスの評価と脅威防止機能を有効にすることに加え、Security Command Center プレミアムに組み込まれているアクティブな脅威の検出機能も使用します。Security Command

Center プレミアムに組み込まれている初期セットには、Event Threat Detection と Container Threat Detection（ベータ版）が含まれています。

10.3.1) Event Threat Detection

Event Threat Detection は、Google Cloud アセットを標的とする脅威を検出する Security Command Center Premium の組み込みサービスです。プラットフォーム ログ、ネットワーク ログ、コンピューティング ログからほぼリアルタイムで脅威を検出し、またネイティブ Google 脅威インテリジェンスおよび検出アルゴリズムを活用します。知見は Security Command Center に自動的に書き込まれ、Cloud Logging にエクスポートすることもできます。Event Threat Detection は、ユーザーの知見に対して基本的な重複除去を実行します。Security Command Center プレミアムを使用するときには Event Threat Detection がデフォルトで有効になります。

10.3.2) Container Threat Detection（ベータ版）

Container Threat Detection は、Google Kubernetes Engine（GKE）コンテナを標的とする脅威を検出する Security Command Center プレミアムの組み込みサービスです。リバースシェル実行、不審なバイナリの実行、不審なライブラリのリンクをほぼリアルタイムで検出します。Container Threat Detection は、脅威の検出時にコンテナとその基盤となる物理ノードを結びつけます。

Container Threat Detection を使用するには、GKE 環境で最新の Container-Optimized OS イメージを実行している必要があります。Container Threat Detection は、データと、コンテナ識別のための追加情報を送信するために、すべてのノードで daemonset コンテナを自動的にデプロイして管理します。知見は Security Command Center と Cloud Logging に自動的に書き込まれます。

10.4) カスタム ポリシーの遵守状況のリアルタイム モニタリング

カスタム ポリシーの遵守状況をリアルタイムでモニタリングするために、example.com アーキテクチャでは Cloud Asset Inventory のリアルタイム通知が使用されています。Cloud Asset Inventory は、特定のアセット名またはアセットタイプの構成が変更されるたびに Pub/Sub メッセージを送信できます。このメッセージは、Cloud Functions の関数による変更の確認をトリガーします。その変更がポリシー違反である場合、Cloud Functions の関数によって、変更の取り消しや管理者への通知などのアクションが実行されます。

example.com でモニタリングされるポリシーの一つに、Gmail アカウントに example.com プロジェクトへの権限を付与するかどうかがあります。Cloud Functions の関数を使用して、作成または変更される IAM ポリシーにメンバーとして Gmail アドレスが含まれているかどうかがチェックされます。Cloud Functions の関数は、ポリシー違反を検出すると変更を元に戻し、カスタム知見を Security Command Center に送信します。図 2.16 にこの構成を示します。

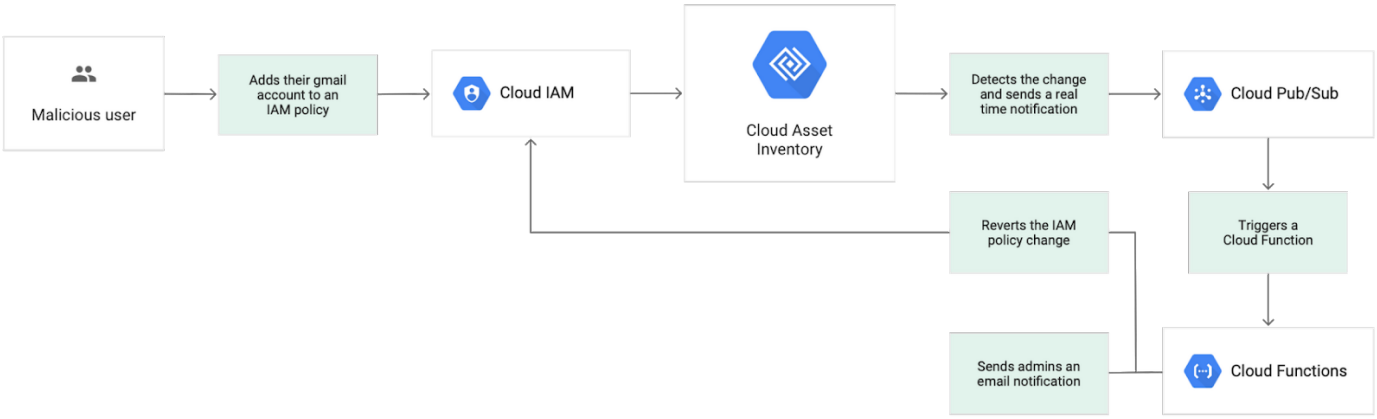


図 2.16 IAM ポリシー変更を自動的に戻して通知を送信する

また Cloud Asset Inventory は、詳しい分析のために構成メタデータを BigQuery テーブルにエクスポートすることも可能にします。データが BigQuery に読み込まれることにより、SQL クエリを使用して構成の内容を詳しく調べ、レポートを作成することができるようになります。リスト 2.1 に、Gmail アカウントにアクセス権を付与する IAM ポリシーを検出する例を示します。

```
SELECT name, asset_type, bindings.role
FROM `PROJECT_ID.DATASET_ID.TABLE_NAME`
JOIN UNNEST(iam_policy.bindings) AS bindings
JOIN UNNEST(bindings.members) AS members
WHERE members like "%@gmail.com"
```

リスト 2.1 @gmail.com のメンバーを持つ IAM バインディングを識別する SQL クエリ

10.5) Chronicle との統合

Cloud Logging と Security Command Center のイベントを Chronicle にエクスポートすることができます。Chronicle は、セキュリティ脅威の検出と調査のためのプラットフォームです。Chronicle は Google インフラストラクチャを基に構築されているので、Google の大規模環境を利用して、発生する可能性のある脅威の調査と選別にかかる時間を削減できます。これは、複数のセキュリティ ソースと脅威フィードからのデータを相互に関連付けて、イベントと検出からなる 1 つのタイムラインベースの集約ビューを示します。Chronicle の検出ルールを使用することも、リアルタイム検索とカスタム ルールを使用して独自の検出を作成することもできます。

10.6) SIEM ソリューションの統合

エンタープライズ SIEM プロダクトは、セキュリティ イベント全体をまとめたり可視化したりする際には便利ですが、クラウド規模のロギングを処理する場合には非効率となる可能性があります。Security Command Center と Cloud Logging はいずれも、構成可能な組み込み Pub/Sub イベント ストリームを出力します。したがって、各自のニーズに応じて最適なオプションを選ぶことができます。

図 2.12 に示したように、example.com リファレンス アーキテクチャには、SIEM ツールが Pub/Sub サブスクリプションを使用して Google Cloud のログを取り込む仕組みがあります。必要なすべてのログを 1 つの未加工ログ Pub/Sub トピックにまとめるため、Cloud Logging のログシンクが使用されます。Dataflow ジョブは未加工ログトピックをサブスクライブし、ログを集約してから、SIEM がサブスクライブできる処理済みログ Pub/Sub トピックにこれらのログを取り込みます。

注: 各種エンタープライズ SIEM ツールをGoogle Cloud に統合する方法はツールとログソースに応じてさまざまです。利用できるその他の統合方法には次のようなものがあります。

- Security Command Center ネイティブ Pub/Sub トピックからの直接取り込み。
- Pub/Sub ログシンクからの直接取り込み（管理可能なボリュームの場合）。
- Cloud Storage またはファイル サーバーからのフラット ファイルの取り込み。
- Pub/Sub イベントを SIEM への API 呼び出しに変換する Cloud Functions の関数。
- Google API を使用した Google Cloud からのログの取得。

10.6.1) Splunk との統合

Cloud Logging イベントと Security Command Center イベントの両方を Splunk に直接エクスポートできます。またこれらのイベントでは統合のために Splunk Add-on for GCP が使用されます。Cloud Logging では、Splunk へのロギング エクスポートを設定できます。Security Command Center では、通知構成を設定できます。いずれの場合でも Pub/Sub イベント ストリームの設定後に、承認済みの Pub/Sub Splunk Dataflow テンプレートを使用して統合を完了することができます。

10.7) BigQuery を使用したセキュリティ データの分析

エンタープライズ SIEM へのエクスポートが非効率な場合は、BigQuery、Pub/Sub、Cloud Functions、Security Command Center などのクラウドネイティブ ツールからなる独自のセキュリティ分析ソリューションを構築できます。このソリューションは大量のログ処理にも対応できます。セキュリティ イベントを特定し、これらのイベントを未加工ログではなく知見としてエンタープライズ SIEM に転送できます。

10.7.1) 独自の分析ソリューションの構築

example.com リファレンス アーキテクチャには、BigQuery ベースのソリューションによってモニタリングされるクラウド固有のセキュリティ イベントがあります。このようなセキュリティ イベントのログが集約され、Security Command Center にカスタム知見として表示されるとともに、通知 Pub/Sub トピックによりエンタープライズ SIEM ツールに転送されます。この BigQuery ベースのアーキテクチャでは、データアクセス ログや VPC フローログなどの大容量のログソースを処理できます。詳しくは、図 2.17 をご覧ください。

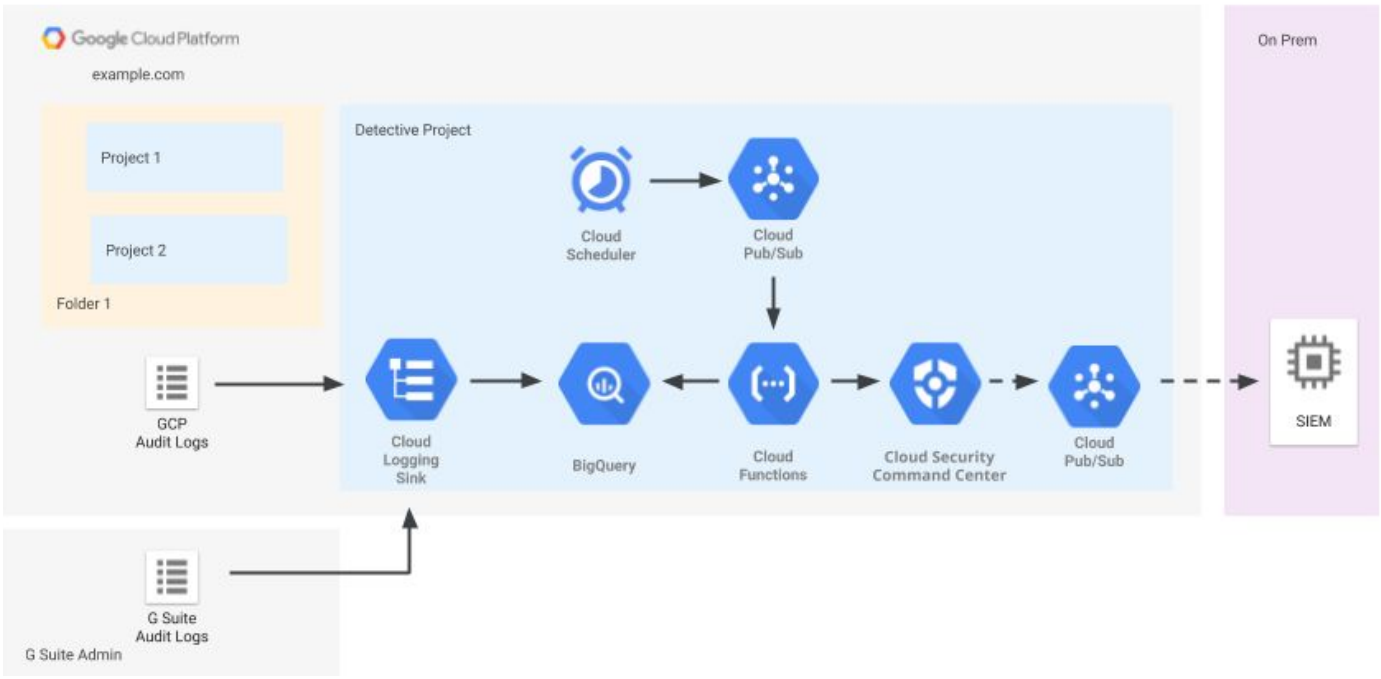


図 2.17 BigQuery ベースのアーキテクチャ

BigQuery ベースのソリューションの仕組みは次のとおりです。

1. Cloud Logging のログが、ログシンクを使用して BigQuery の未加工データセットに保存されます。コスト管理のため、このデータセットが定期的に有効期限切れになるように構成できます。
2. モニタリング対象のセキュリティ イベントを表すビューが BigQuery データセットに追加されます。ビューは保存済みのクエリに似ています。この場合、モニタリング対象のセキュリティ イベントのインシデントごとに 1 つのエントリが生成されます。モニタリング対象のユースケースについてはセクション 10.7.2 をご覧ください。
3. Cloud Scheduler がイベントをスケジュール設定 Pub/Sub トピックに 15 分間隔でプッシュします。Cloud Functions の関数が、すべてのスケジュール設定イベントでトリガーされるように構成されます。この関数は、見逃したイベントがないかを確認するために、過去 20 分間の新しいイベントを検出するクエリをビューに対して実行します。イベントが検出されると、検出されたイベントがカスタム知見として Security Command Center API にプッシュされます。
4. Security Command Center の通知機能が、すべての新しい知見（カスタム知見と Google またはサードパーティのセキュリティ ソースを含む）を Pub/Sub 知見トピックにプッシュします。
5. エンタープライズ SIEM はセキュリティ イベントを受信するためにこの知見トピックをサブスクライブします。

10.7.2) アラート生成ユースケースの例

アラート生成ユースケースは、BigQuery にビューとして保存される SQL クエリとして実装されます。BigQuery ベースのアーキテクチャを使用してアラートが生成される特定の条件の一覧を以下に示します。

- 高いレベルの特権アカウント ログイン（特権管理者、組織管理者など）からのログインが発生する。

- 許可されていないドメインのユーザーに対し Cloud IAM 権限が付与される。
- ロギング設定が変更される。
- 予期される範囲外の IP アドレスを含む VPC フローログが検出される。
- 重要な暗号鍵に対する権限が変更される。
- 未承認の Google サービスが使用される。

これらのユースケースを拡張するには、クエリを作成して BigQuery データセットにビューとして保存します。これにより、他のユースケースのビューの新しい結果があるかどうかを確認するため、定期的にクエリが実行されます。たとえば、次のクエリ（リスト 2.2）ではロギング設定が変更されたケースが特定されます。

```
SELECT
  receiveTimestamp,
  timestamp AS eventTimestamp,
  protopayload_auditlog.requestMetadata.callerIp,
  protopayload_auditlog.authenticationInfo.principalEmail,
  protopayload_auditlog.resourceName,
  protopayload_auditlog.methodName
FROM
  `${project}.${dataset}.cloudaudit_googleapis_com_activity_*`
WHERE
  protopayload_auditlog.serviceName = "logging.googleapis.com"
```

リスト 2.2 ロギング設定の変更を検出する SQL クエリ

11. 請求

Google Cloud の使用量をモニタリングし、想定外の消費についてアラートを生成することで、請求機能を管理とセキュリティを強化するメカニズムとして使用できます。Google Cloud の課金はプロジェクトと請求先アカウントを関連付けることによって処理されます。セクション 5 で説明したように、example.com リファレンス アーキテクチャでは、プロジェクトの作成時にすべてのプロジェクトが関連付けられる 1 つの請求先アカウントを使用しています。表 2.13 に、example.com の請求先アカウントのロールに関連付けられているグループとロールを示します。

11.1) 請求額アラート

プロジェクト レベルまたは組織レベルで予算を設定できます。予算は、支出額が一定となるように固定の金額として設定するか、または変動する費用に対応できるように、前月の支出額に対するパーセンテージとして設定できます。請求額アラートは組織内の異なるスコープに適用できます。example.com では、プロジェクトの作成時に予算とそれに関連する請求額アラートが作成されます。請求額アラートはまた、組織レベルの予算アラートを生成するために example.com 請求先アカウントにも適用されます。

example.com リファレンス アーキテクチャには、プロジェクトまたは組織の支出が予算しきい値の 50%、75%、90%、95% に達した時点でトリガーされる請求額アラートがあります。請求額アラートはデフォルトで請求先管理者と請求先ユーザーのメール アカウントに送信されます。example.com では、これらに対応するのはサービス アカウントとファイアコール アカウントであるため、サービス アカウントとファイアコール アカウントへのメールを転送する必要があります。予算消費に対する請求額アラートの上限に達しても、使用は停止されないので注意してください。このアラートは単なる通知です。

注: 請求額アラートのデフォルトの受信者以外にもアラートを送信する必要がある場合は、Cloud Console から追加の受信者を構成できます。

11.2) 請求データのエクスポートとチャージバック

Cloud Console の充実したコスト管理ツールを使用して、コストとその予測をさまざまなフォーマットで表示できます。example.com モデルでは、請求プロジェクトですべての請求レコードを BigQuery データセットにエクスポートすることで、このようなコスト管理ツールを補完しています。Cloud Console でエクスポートを有効にする必要があります。エクスポートされる請求レコードには、プロジェクトの作成時にプロジェクトに割り当てられたプロジェクト ラベル メタデータが含まれています（表 2.10 を参照）。各プロジェクトには、チャージバックに使用できる請求コードと連絡先が関連付けられています。リスト 2.3 に示すエクスポートされたデータセットに対する単純な SQL クエリを使用して、example.com 内の各ビジネス ユニットの請求情報を取得できます。

```
#standardSQL
SELECT
   (SELECT value from UNNEST(labels) where key = 'business-code') AS bu,
   service.description AS description,
   SUM(cost) AS charges,
   SUM((SELECT SUM(amount) FROM UNNEST(credits))) AS credits
FROM `PROJECT_ID.DATASET_ID.TABLE_NAME`
GROUP BY bu, description
ORDER BY bu ASC, description ASC
```

リスト 2.3 ビジネス ユニットとサービス別に請求額をまとめるクエリの例

12. セキュリティに関する一般的なガイダンス

Compute Engine サービス アカウントに自動的に割り当てられるデフォルトのロールは編集者であり、これは非常に幅広い権限を持つロールです。デフォルトのサービス アカウントではなく、ユースケースに合わせて権限が厳しく制限された、プロジェクト用の新しいサービス アカウントを作成してください。新しいサービス アカウントが該当する用途に適していることを確認したら、デフォルトの Compute Engine サービス アカウントを無効にします。デフォルトの Compute Engine サービス アカウントは、Cloud Console のプロジェクト レベルの Cloud IAM セクションで確認できます。サービス アカウント名の形式は次のとおりです。

```
project-number-compute@developer.gserviceaccount.com
```

同様に、App Engine サービスを使用している場合は、各自のユースケースに合わせて権限が厳しく制限された新しいサービス アカウントを作成し、デフォルトのフローをオーバーライドしてください。新しいサービス アカウントが各自の用途に適していることを確認したら、自動的に作成された App Engine のデフォルト サービス アカウントを無効にします。デフォルトの App Engine サービス アカウントは、Cloud Console のプロジェクト レベルの [Cloud IAM] セクションで確認できます。サービス アカウント名の形式は次のとおりです。

```
your-project-id@appspot.gserviceaccount.com
```

各 Kubernetes Engine ノードには Cloud IAM サービス アカウントが関連付けられています。デフォルトでは、ノードに Compute Engine のデフォルトのサービス アカウントが付与されています。これは Cloud Console の [Cloud IAM] セクションで確認できます。前述したように、このアカウントにはデフォルトで幅広いアクセス権が付与されており、さまざまな用途に役立ちますが、Kubernetes Engine クラスタの実行には権限が過剰です。Kubernetes Engine クラスタの実行には、最小限の権限のみを持つサービス アカウントを作成して使用することを検討してください。Kubernetes Engine クラスタの強化について詳しくは、クラスタのセキュリティ強化に関する資料と、コンテナ セキュリティ ブログシリーズをご覧ください。

13. 次のバージョンでの更新

具体的なビジネス シナリオで必要となるセキュリティ コントロールは、非常に多様になると考えられます。このセキュリティ基盤ブループリントの初版では、そのすべてには対応していません。今後の更新では、ネットワーク セキュリティにおける可視性と制御の強化、データ セキュリティ、暗号化オプションとデータ分類、クラウドネイティブ セキュリティ アプリケーションの開発、アプリケーション セキュリティなどに関するトピックが含まれる予定です。

III.まとめ

このガイドは、Google Cloud 資産の構成およびデプロイに関して Google が推奨する手順のガイダンスです。主な決定事項と注目すべき領域について説明し、そのそれぞれについて、考慮すべき背景と、各決定を行うにあたってのメリットとデメリット、決め手となる事柄を示しました。本資料で行った選択は、各企業の要件やビジネスのコンテキストと合致しているとは限りません。本資料の内容を取り入れ、必要に応じて修正してご利用ください。

新しいプロダクトの機能、お客様からのフィードバック、セキュリティ環境のニーズと変化を反映して常に最新の内容を維持するために、今後もこのブループリントを更新します。

BeyondProd ペーパーで説明している Google の中核的なセキュリティ原則は、自動化され、標準化されたシンプルな変更のロールアウトです。これは、自動化を使用して例外の発生を抑制し、人間によるアクションの必要性を最小限に抑えることを重視しています。そのため、このガイドで扱う手順のほとんどを自動化する際に使用できるスクリプトを集めた Terraform リポジトリを含めました。これらのスクリプトをエンドツーエンドで実行することで、Google が推奨する基盤ブループリントのすべてをデプロイできます。各スクリプトは、個別に修正を加えて使用し、ブループリントの中でお客様のユースケースに最も適した部分を利用することもできます。

最後に、Terraform 自動化のリポジトリを使用したデモ用 Google 組織全体へのアクセス権をご用意しています。これにより、構成が完了し運用されている状態のセキュリティ基盤を把握していただけます。

デモ用組織への閲覧者アクセス権が必要な場合は、Google Cloud セールスチームにご連絡ください。

サポートに関する質問は、security-foundations-blueprint-support@google.com にお問い合わせください。

アドバイスの提供および実装の支援について、Google Cloud は業界屈指のサイバー事業を持つ Deloitte と連携し、クラウド セキュリティ導入を支援するためのエンドツーエンドのアーキテクチャ、設計、デプロイ サービスを提供しています。