Google Cloud

# 実践！Cloud Run セキュリティ

Google Cloud
アプリケーション モダナイゼーション スペシャリスト
内間 和季

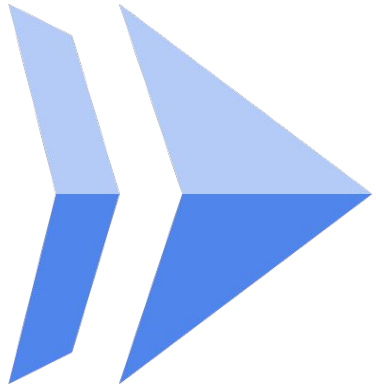
Table of Contents

01

# Cloud Run を運用する前に知っておきたいこと

# Cloud Run とは

- フルマネージドなコンテナ実行環境
- 数秒でデプロイ
- HTTPS に対応、カスタム ドメインも可
- 言語やライブラリ依存なし
- ポータブル
- クラスタ管理など不要



# Cloud Run の特徴

## 高速なデプロイ

ステートレスなコンテナ

**高速に 0 to N スケール**

数秒でデプロイし URL を付与

## サーバーレス・ネイティブ

管理するサーバーはなし
コードに集中

**言語やライブラリの制約なし**

きっちり使った分だけお支払い

## 高いポータビリティ

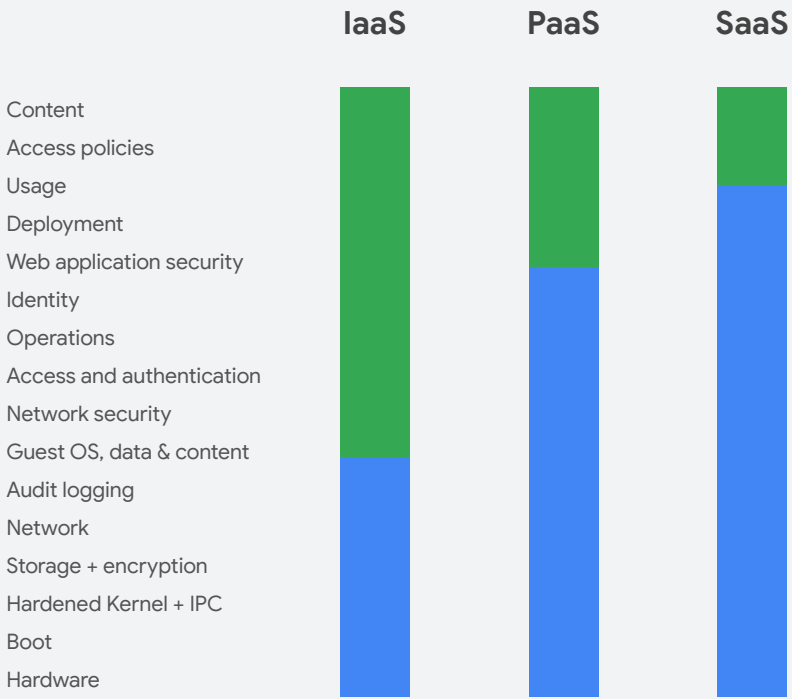
どこでも同じ Developer Experience
マネージドでも GKE のクラスタ上でも

**Knative API の一貫性**

ロックインの排除

# Google Cloud における責任共有モデル

- インフラ面のセキュリティは Google の　責任範囲
- サーバーレス プロダクトの利用において、**アクセス コントロール**や**アプリケーション自体のセキュリティ**は**利用者側の責任範囲**
- 利用者側でもセキュリティの観点で考慮すべきポイントが存在する

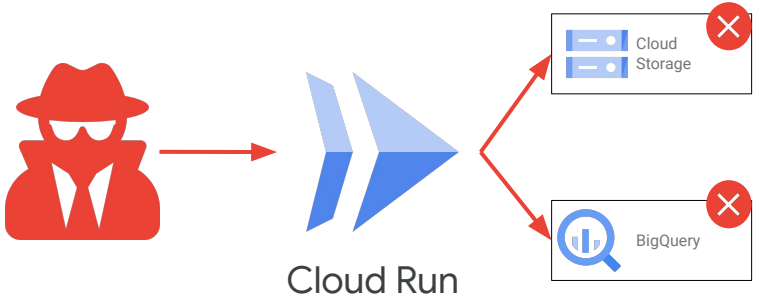


# 何も考えずにデフォルト構成のままデプロイしてしまうと...

- 内部向けサービスを **意図せず外部に公開**
- **脆弱性のあるコンテナ** のデプロイ
- 認証機構やセキュリティ機能の **バイパス**
- Cloud Run に強い権限を持たせてしまい、　　他 Google Cloud リソースを **誤って操作**

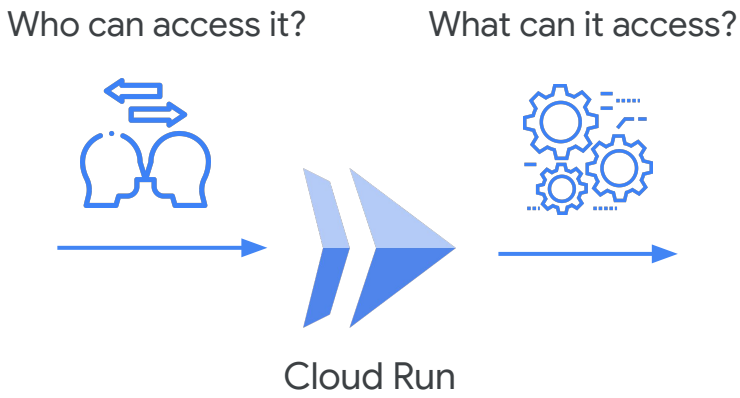
してしまう**可能性がある**..

そのため、本番運用の前に Cloud Run の基本的な仕様や　周辺サービスについて知っておく必要がある



# Cloud Run の基本的なアクセス制御機能

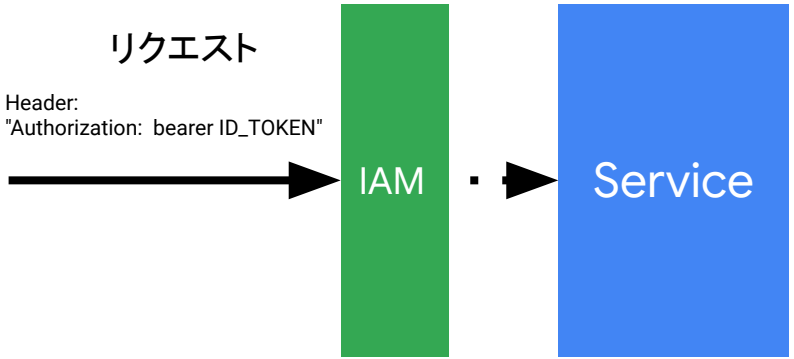
- **IAM によるアクセス制御**
  - **誰が** Cloud Run サービスにアクセスできるか
- **サービス個別のサービスアカウント**
  - 各 Cloud Run サービスが**何に**アクセスできるか
- **Ingress 設定**
  - **どの経路**で Cloud Run サービスにアクセスさせるか
- **Egress 設定**
  - **どの経路**で Cloud Run サービスから他の　サービスにアクセスさせるか



# IAM によるアクセス制御

Cloud Run では IAM によるアクセス制御をサポート

サービスデプロイ時に「認証が必要」を選択することで、
**roles/run.invoker** が付与されたユーザーのみアクセスを許可するよう設定可能

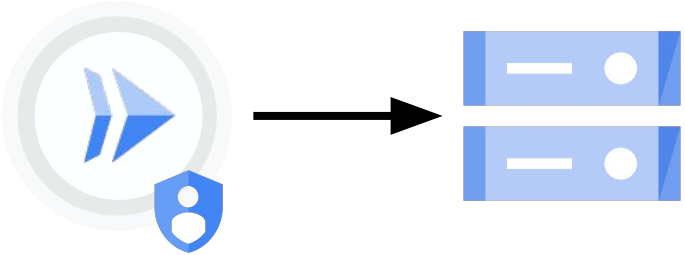



# サービス個別のサービスアカウント

Cloud Run の**サービス単位でサービスアカウントを設定** 可能

他の Google Cloud サービスへのアクセス制御で活用

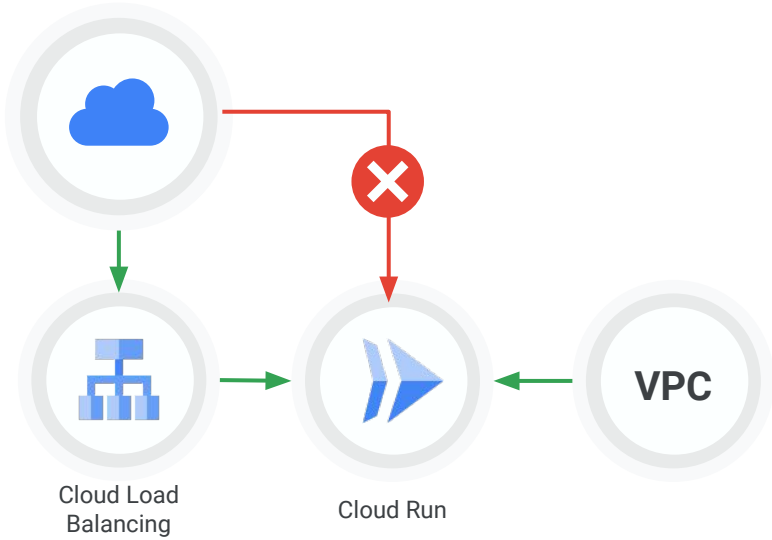
デフォルトのサービスアカウントとして Compute Engine のデフォルト サービスアカウントが設定されている

# Ingress 設定

## Cloud Run サービスに対するアクセス経路を制御

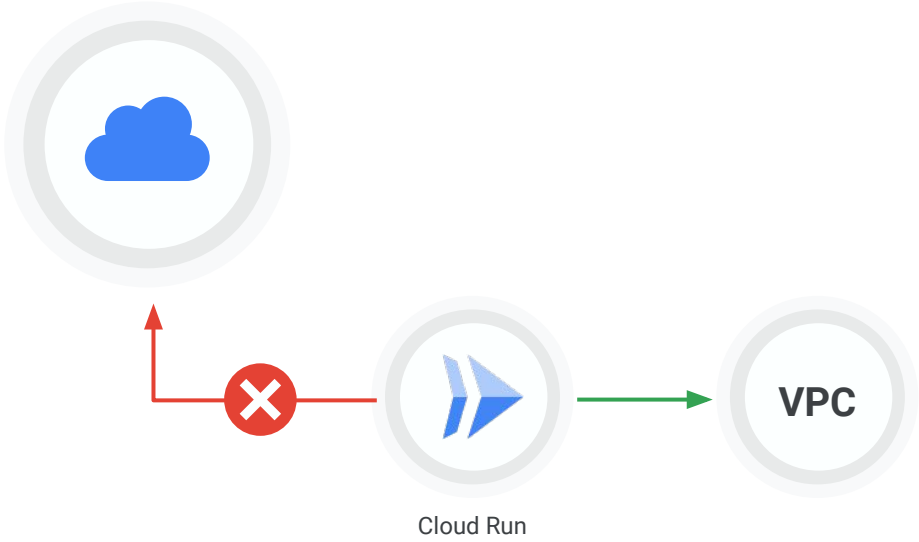
- **すべてのトラフィックを許可する**
- **内部トラフィックのみを許可する**
  - 同一プロジェクト内 VPC リソース, Eventarc, Pub/Sub, Workflows
  - Internal HTTP(S) Load Balancing
  - VPC Service Controls 境界内リソース
- **内部トラフィックと Cloud Load Balancing からのトラフィックを許可する**
  - 上記「内部トラフィック」+ External HTTP(S) Load Balancing



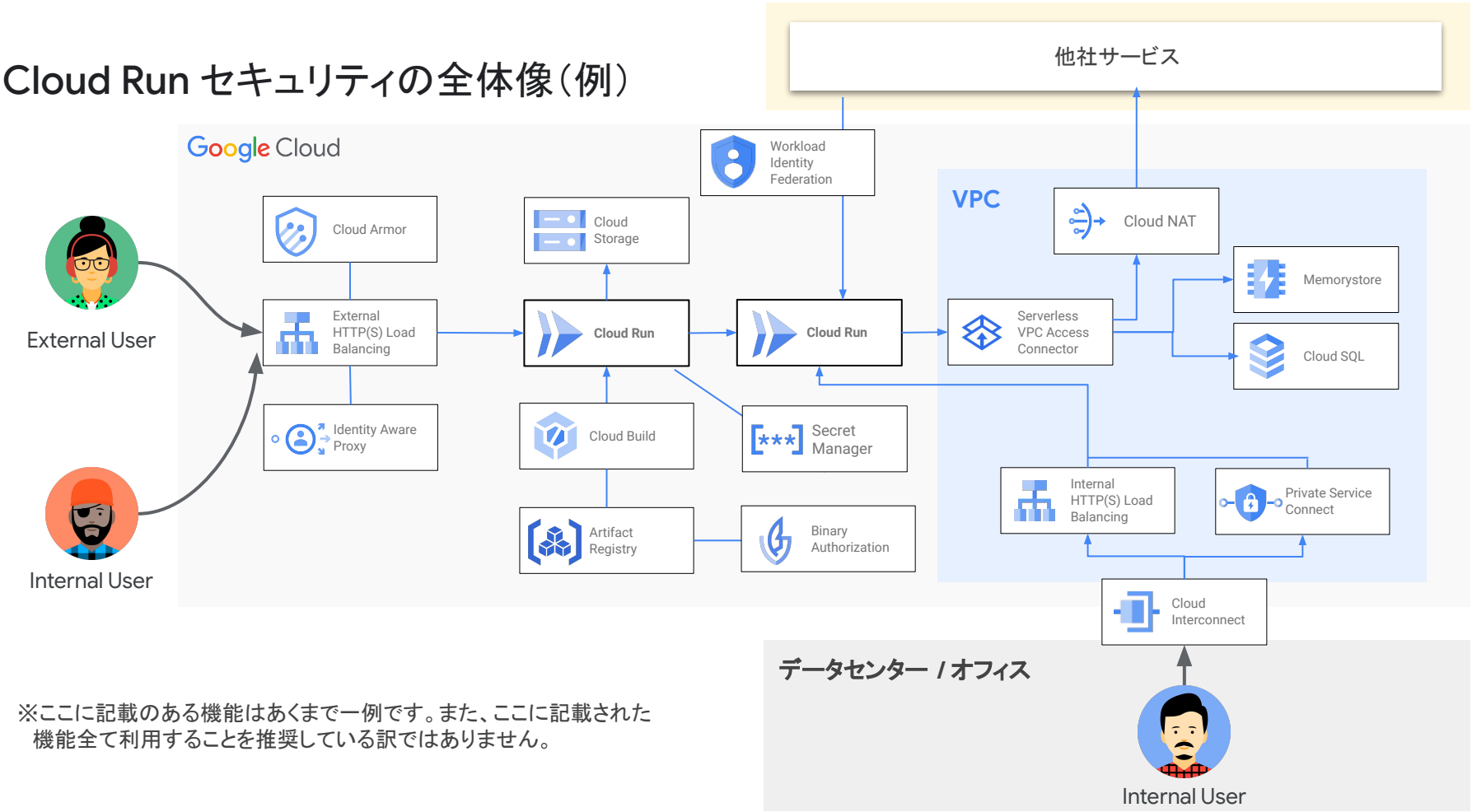

# Egress 設定

宛先 IP アドレス種別に応じて **Cloud Run から送信されるトラフィックの経路を制御**

- **プライベート IP アドレスレンジの宛先のみ** VPC コネクタ経由
- **全ての送信トラフィック** を VPC コネクタ経由

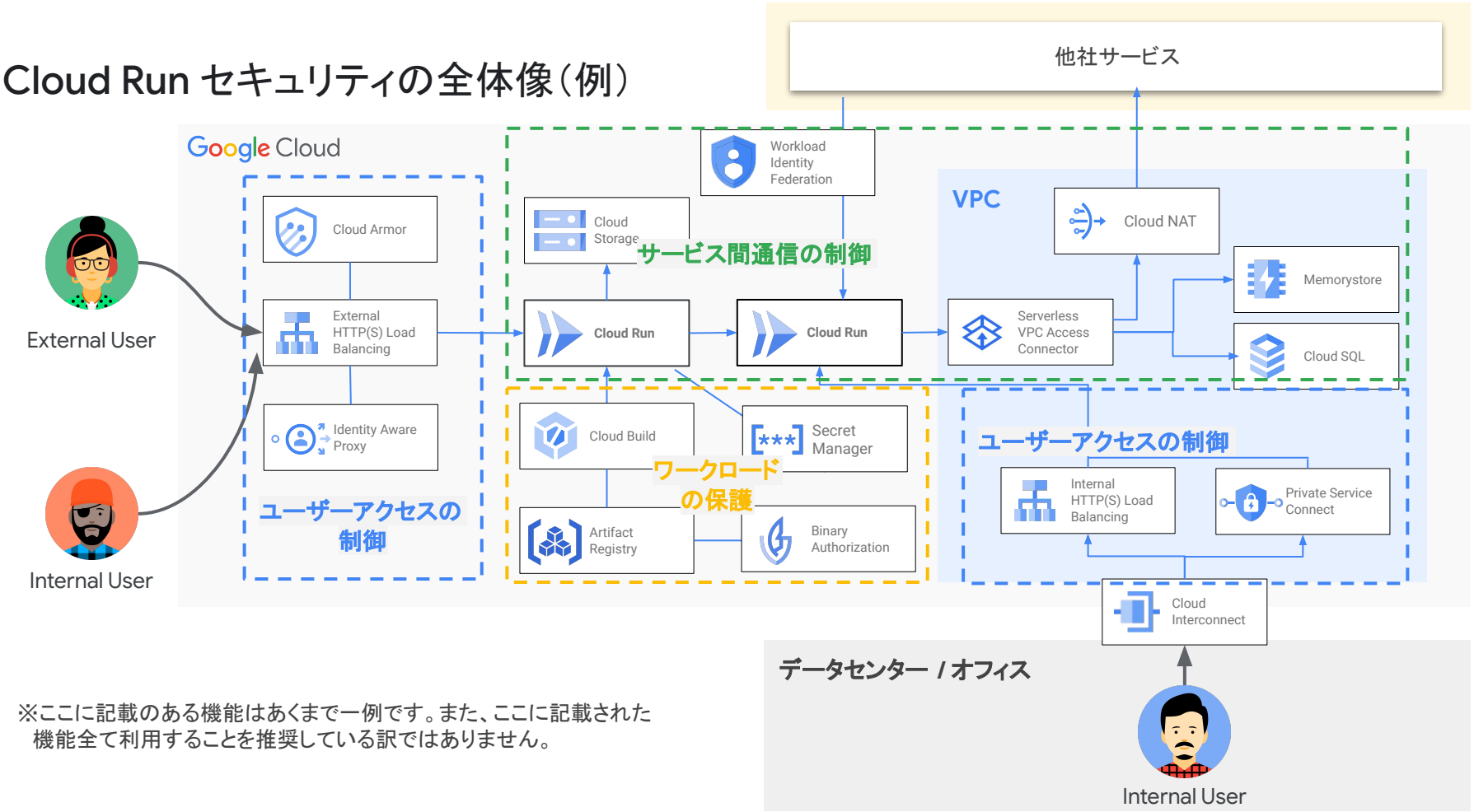



# Cloud Run セキュリティの全体像（例）




※ここに記載のある機能はあくまで一例です。また、ここに記載された機能全て利用することを推奨している訳ではありません。

# Cloud Run セキュリティの全体像（例）




※ここに記載のある機能はあくまで一例です。また、ここに記載された機能全て利用することを推奨している訳ではありません。

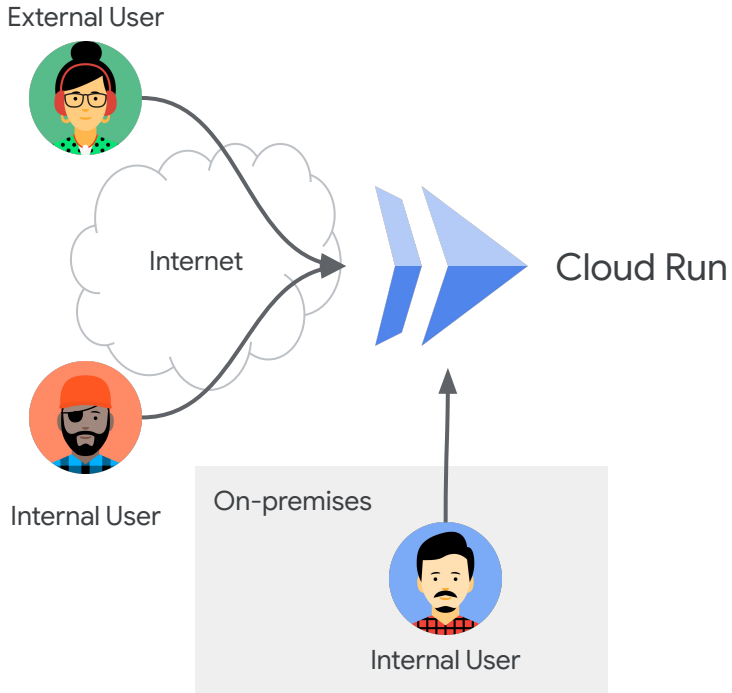
02

# ユーザーアクセスの制御

# ユーザーアクセスの種類

ユーザーアクセスの特性に応じて、ネットワーク経路やサービスへのアクセス権限を絞ることで、**攻撃の機会を少なく**することができる

- 外部ユーザーからのアクセス
  - インターネット経由
- 内部ユーザーからのアクセス
  - インターネット経由
  - 専用線 / VPN 経由

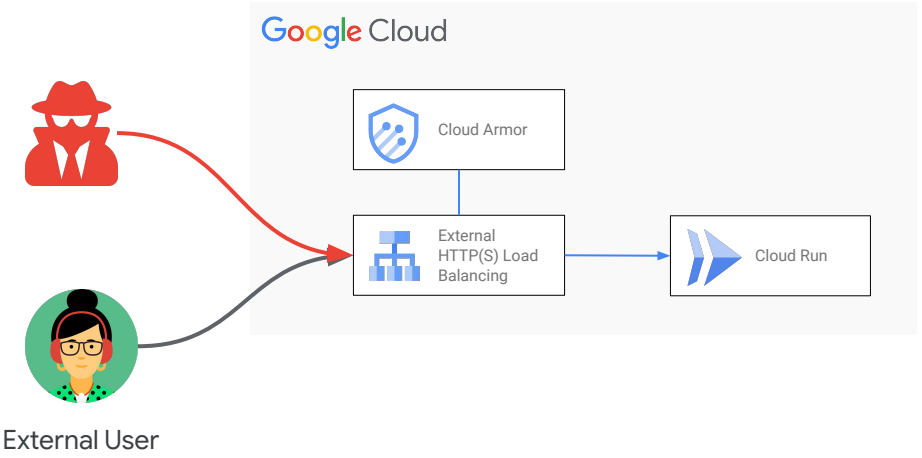


# 外部ユーザーからのアクセス

エンドユーザー向けに公開しているサービスの場合、インターネットを通じて **不特定多数（悪意のあるユーザー含む）からのアクセス** が発生する

Cloud Run では Serverless NEG により、Google Cloud Load Balancing との統合を実現

これにより、エッジでのセキュリティ保護（DDoS 対策, WAF) として **Cloud Armor** の機能を利用することが可能に




“セキュリティポリシーの概要 | Google Cloud Armor”
https://cloud.google.com/armor/docs/security-policy-overview?hl=ja

# Google Cloud Armor

## エッジ防御: DDoS & WAF

**DDoS 攻撃からのインフラ防御**
Global HTTP(S) Load Balancing にて（TCP SYN フラッド、増幅攻撃、IP フラグメント攻撃、他）

**トラフィックの許可・ブロック**
IP アドレス、地域、カスタムパラメータマッチ（L3-L7 他）

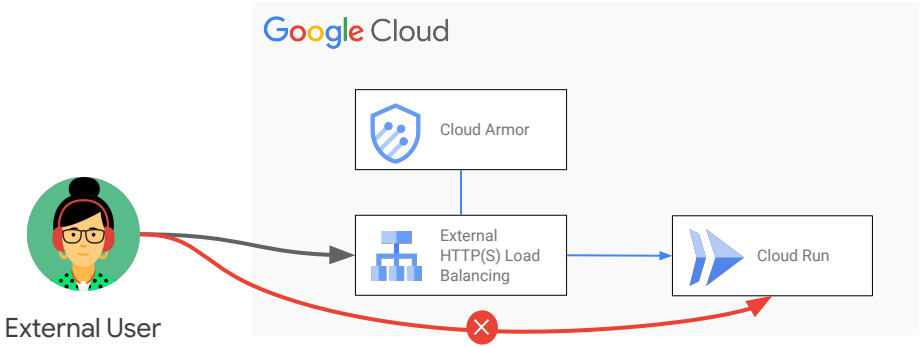
**アプリケーションレイヤ攻撃からの防御**
（SQLi、XSS 他）IAP との組み合わせ

**テレメトリ**
各種判断結果、メトリクスは Cloud Logging/Monitoring に記録

# 外部ユーザーから Cloud Run サービスへのダイレクトアクセスを防ぐ

デフォルト構成では Ingerss 設定が「すべてのトラフィックを許可する」となっており、External HTTP(S) Load Balancing (Cloud Armor) を経由せず直接 Cloud Run 上のサービスにアクセス可能

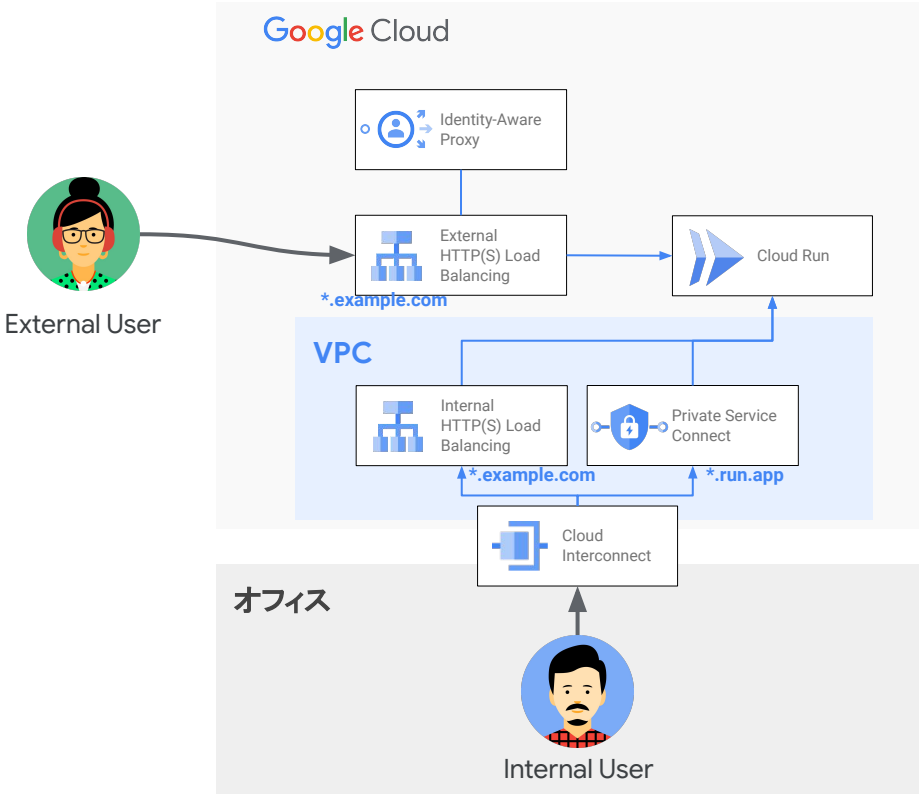
バイパスを防ぐためには Ingress 設定として **「内部トラフィックと Cloud Load Balancing からのトラフィックを許可する」**を選択する

# 内部ユーザーからのアクセス

社内システムのように、利用者が限定されるようなシステムの場合は **Identity-Aware Proxy (IAP)** 等の認証認可の仕組みを組み込むことでより安全にサービスを公開可能

また、オフィスやデータセンターから Cloud Interconnect や Cloud VPN を用いたアクセスが　可能な場合は、**Internal HTTP(S) Load Balancing** や **Private Service Connect (PSC)** を使って　プライベートな経路でのサービスアクセスを実現

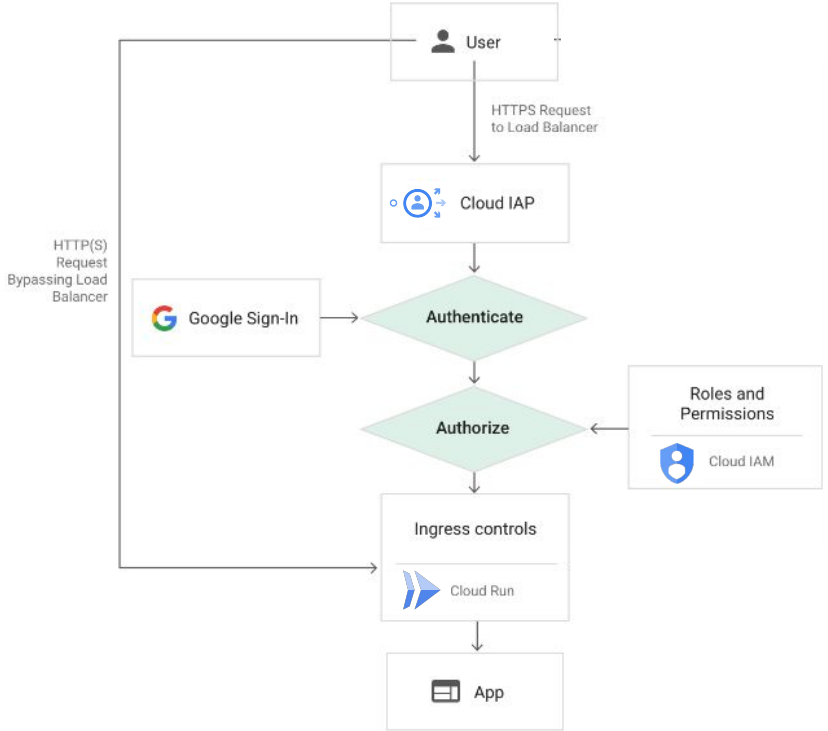


# Identity-Aware Proxy (IAP)

アプリケーションに手を加えることなく、**認証 / 認可の仕組み**を提供

Cloud Run では Serverless NEG により、Cloud Load Balancing と組み合わせることによって利用可能 (Preview)

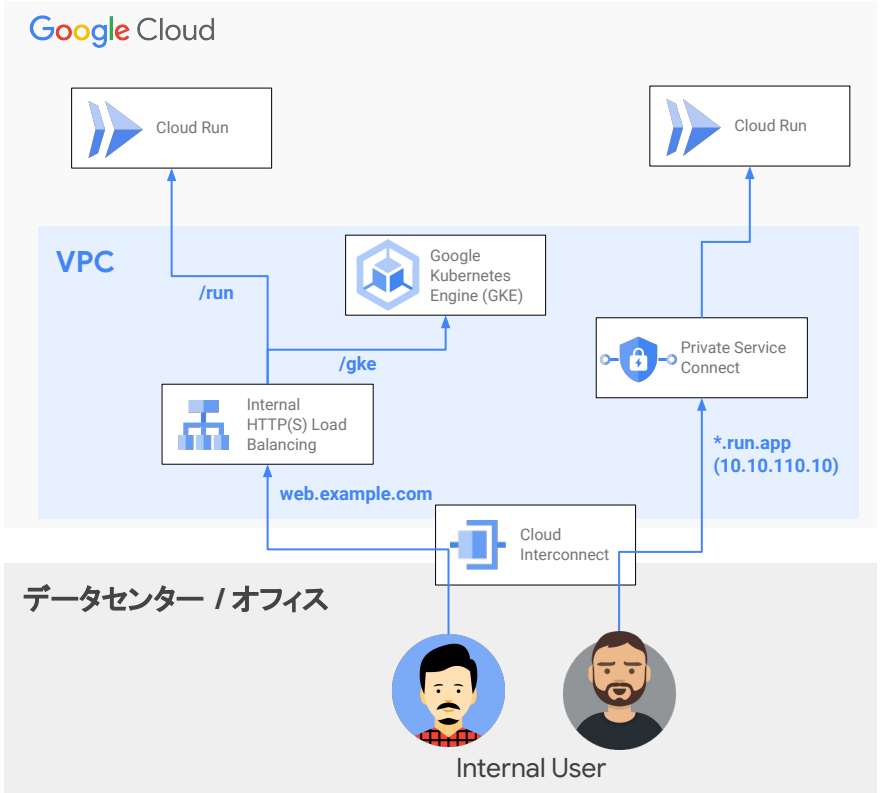
IAP を構成する場合、対象の Cloud Run サービスで公開（未認証）アクセスを許可する必要あり



# プライベートな経路でのアクセス

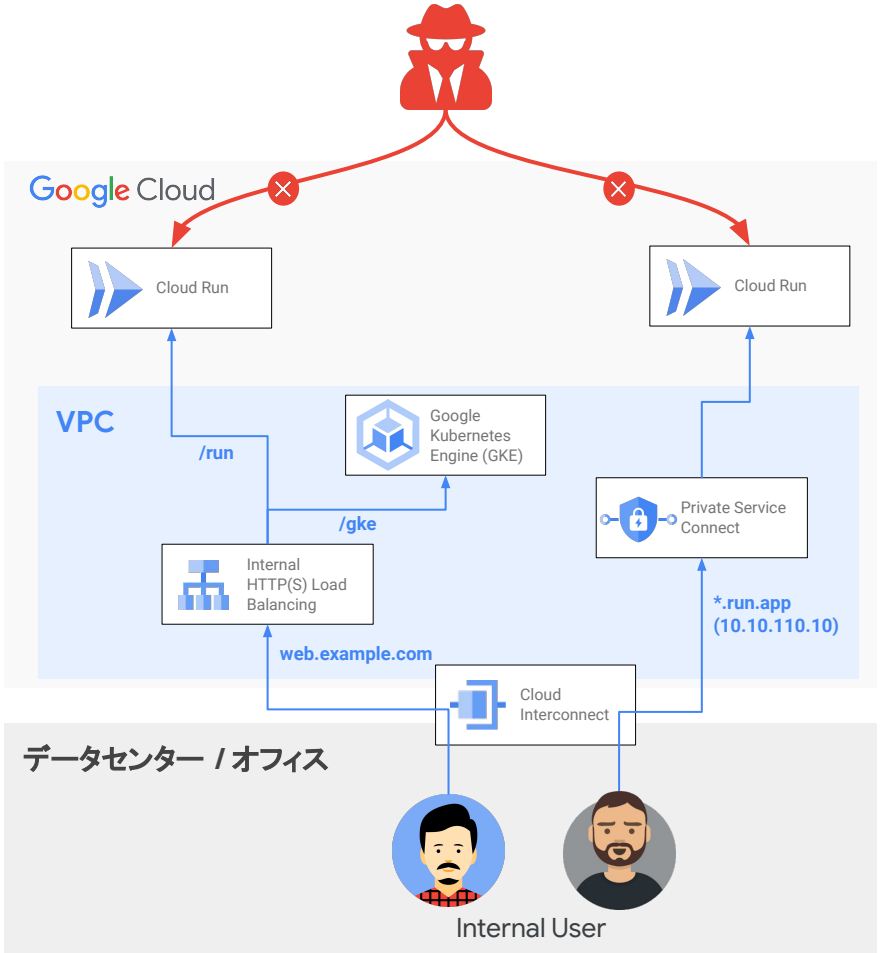
プライベートな経路で Cloud Run サービスに　アクセスさせる際の主な選択肢:

- **Internal HTTP(S) Load Balancing** Preview
  - カスタムドメインを利用したい
  - 単一 URL に複数のサービス (GKE や別の Cloud Run サービス等) を紐づけたい
- **Private Service Connect**
  - デフォルトドメイン (*.run.app) を利用する場合



# プライベートな経路でのアクセス

External HTTP(S) Load Balancing 経由時と同様に、デフォルト構成では直接 Cloud Run 上のサービスにアクセス可能となっているため、インターネット経由でのアクセスが不要な場合は Ingress 設定として**「内部トラフィックのみを許可する」**を選択することを推奨

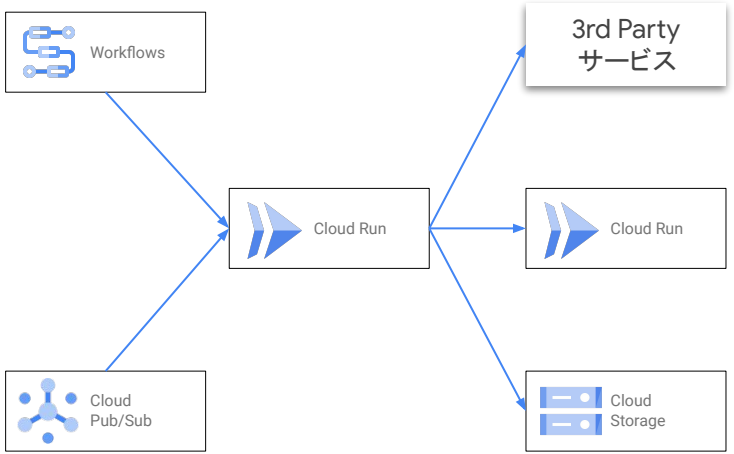
03

# サービス間通信の制御

# サービス間通信の種類

Cloud Run の通信相手となるサービスの種類によって検討ポイントが異なる

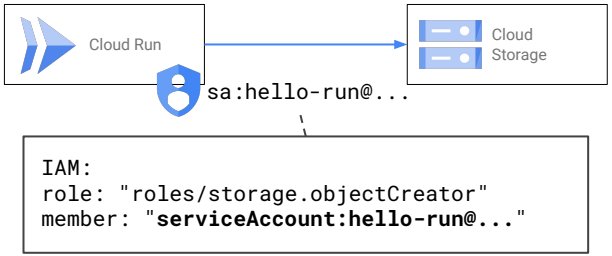
- Google Cloud サービスとの通信
  - 他 Google Cloud サービス
  - Cloud Run サービス間
- オンプレミスや 3rd Party サービスとの通信
  - 3rd Party SaaS
  - CI / CD サービス、等



# 他 Google Cloud サービスとの通信

Cloud Run サービスに設定するサービス アカウントにより、他 Google Cloud サービスへのアクセス制御を実現

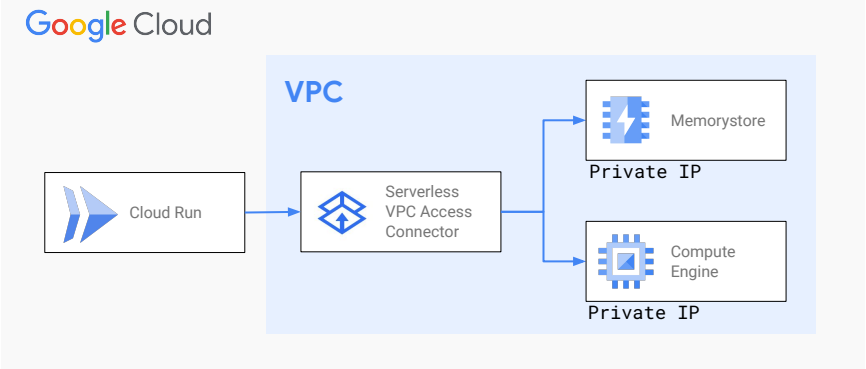
デフォルトのサービス アカウント (Compute Engine の デフォルト サービス アカウント) は強い権限を持っているため、サービス単位で**最小権限が付与されたサービス アカウントを作成・設定**することを推奨




# VPC 内リソースとの通信

プライベートな IP アドレスで公開された VPC ベースのリソース（例：Compute Engine, Memorystore 等）にアクセスしたい場合、**サーバーレス VPC　　アクセス コネクタ**を使うことで実現可能

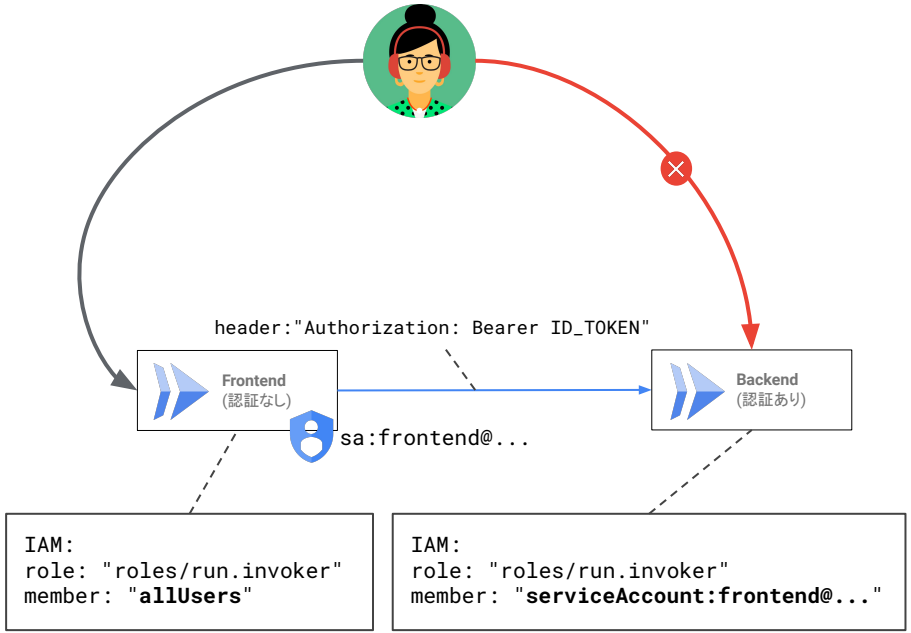
サーバーレス VPC アクセス コネクタは共有 VPC への接続もサポート



# Cloud Run サービス間の通信

バックエンドサービス等で呼び出し元を制限したいケースではサービス作成時に**「認証が必要」**を選択することで、IAM による認可を有効化

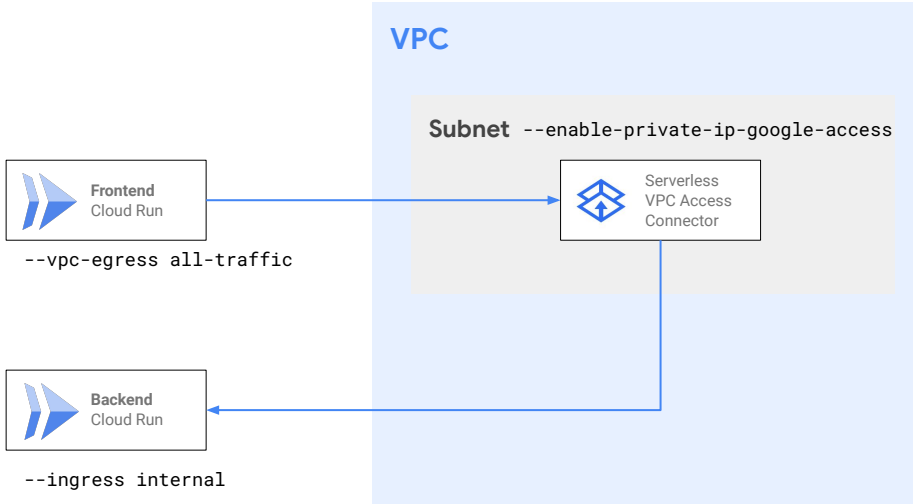
呼び出し側のサービスに **roles/run.invoker** を付与し、ヘッダにトークンを含めてアクセスする

# Cloud Run サービス間の通信

通信先の Cloud Run サービスで Ingress が**「内部トラフィックのみを許可する」**に設定されている場合は、サーバーレス VPC アクセスコネクタを　利用し VPC 経由でアクセスする必要がある

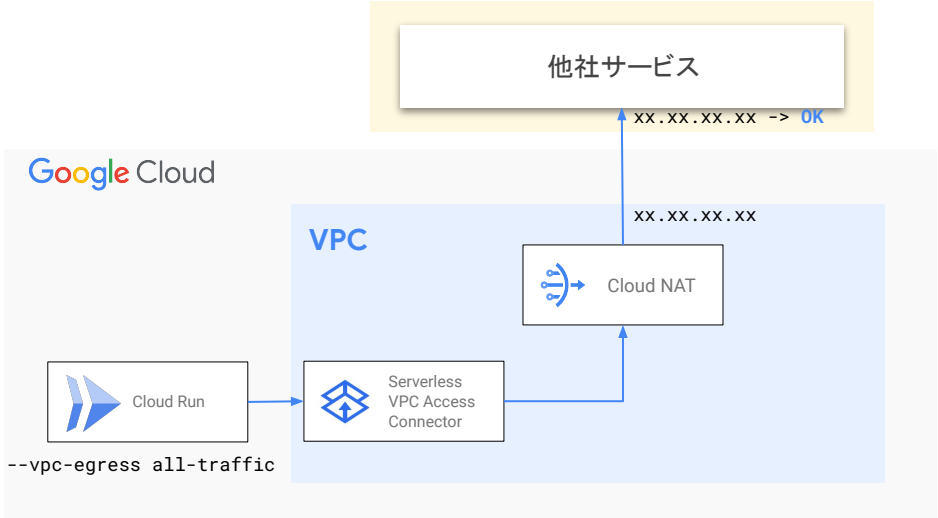
※ サーバーレス VPC アクセスコネクタが接続しているサブネット上で「限定公開の Google アクセス」を有効化する必要あり

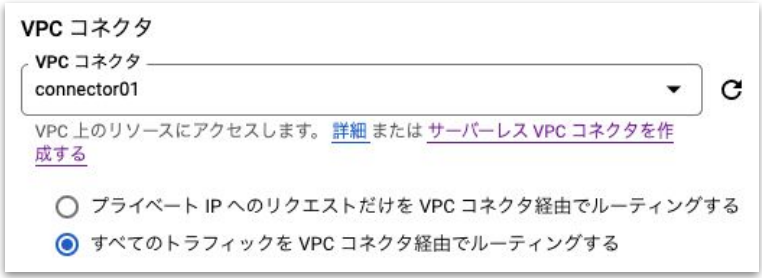


# 3rd Party サービスへの通信

3rd Party サービス側で IP アドレスベースの　アクセス制御を行なっているようなケースでは、Cloud Run から送信するトラフィックの　　IP アドレスを固定する必要がある

Egress 設定で**「すべてのトラフィックを VPC　コネクタ経由でルーティングする」**を選択し、Cloud Run からの Egress トラフィックを全て **Cloud NAT** を経由させて外部サービスへアクセスすることで Egress IP アドレスの固定を実現



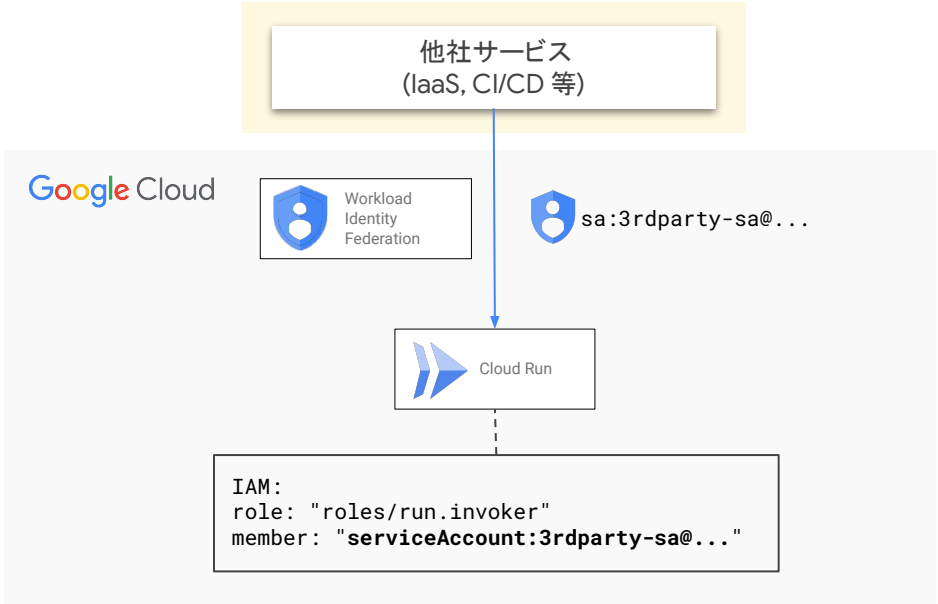



# 3rd Party サービスからのアクセス

オンプレミスや 3rd Party サービスなど Google Cloud 外部から **Workload Identity Federation** を使い Service Account Key をダウンロードせずに認証付きアクセスが可能

Workload Identity Federation は以下のプロバイダをサポート

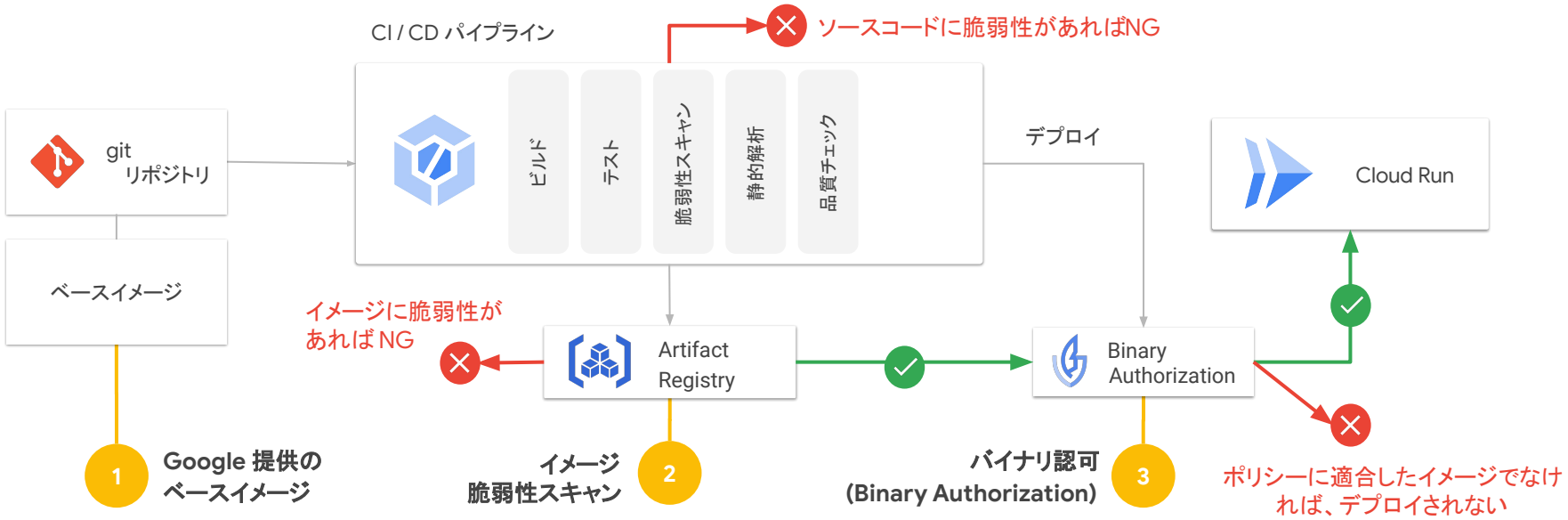
- AWS
- Azure Active Directory（AD）
- OIDC 互換 ID プロバイダ
- SAML 2.0 対応 ID プロバイダ



04

# ワークロードの保護

# セキュアなソフトウェア サプライチェーンの例



# Google 提供のベースイメージ

- **定期的な脆弱性スキャン** が実行され、**最新のセキュリティ パッチが自動的に適用** されたベースイメージを提供
- 利用可能な OS ディストリビューション:

| OS | ソース | リポジトリのパス | Google Cloud Marketplace リスティング |
|---|---|---|---|
| CentOS 7 | GitHub | marketplace.gcr.io/google/centos7 | Google Cloud Marketplace |
| CentOS 8 | GitHub | marketplace.gcr.io/google/centos8 | Google Cloud Marketplace |
| Debian 9 "Stretch" | GitHub | marketplace.gcr.io/google/debian9 | Google Cloud Marketplace |
| Debian 10 "Buster" | GitHub | marketplace.gcr.io/google/debian10 | Google Cloud Marketplace |
| Debian 11「BullsEye」 | GitHub | marketplace.gcr.io/google/debian11 | Google Cloud Marketplace |
| Ubuntu 18.04 | GitHub | marketplace.gcr.io/google/ubuntu1804 | Google Cloud Marketplace |
| Ubuntu 20.04 | GitHub | marketplace.gcr.io/google/ubuntu2004 | Google Cloud Marketplace |

- また、distroless のような軽量イメージを利用することで **攻撃対象領域を小さくする** ことも可能
  https://github.com/GoogleContainerTools/distroless

# Container Analysis

- 以下の Common Vulnerabilities and Exposures（CVE）データを取得し、コンテナ イメージの脆弱性の重大度（5 段階）を判定
  - Debian
  - Ubuntu
  - Alpine
  - Red Hat Enterprise Linux and CentOS
  - National Vulnerability Database
  - CentOS
- **リポジトリへのイメージ Push 時**や**オンデマンド**での脆弱性スキャンをサポート
- OS パッケージだけではなく、Go や Java パッケージもスキャン対象に

# Binary Authorization

**信頼できるコンテナ イメージのみ**が Cloud Run にデプロイされることを保証する

以下の条件に当てはまるコンテナイメージのみ デプロイを許可するよう制御が可能に

- イメージに対する認証者 (Attestors) による証明書 (Attestation) が存在する
- またはイメージ名が許可リストにマッチする

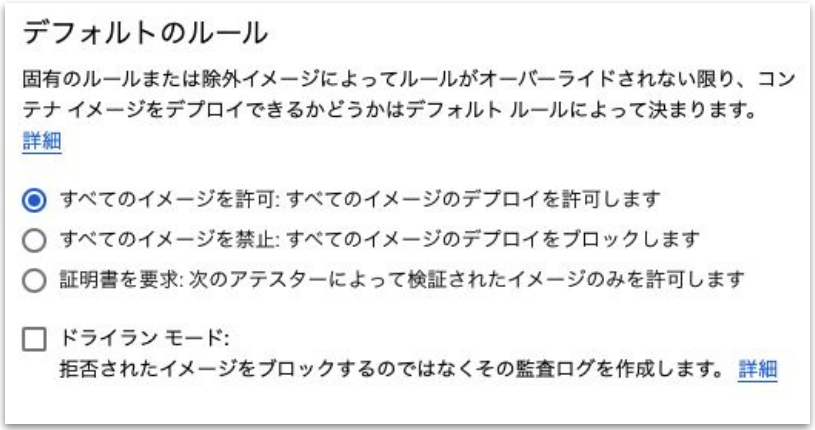
# Binary Authorization ポリシー

**デフォルトのルール**と、ルールの**除外対象**を設定

除外するイメージのパターンは複数定義可能

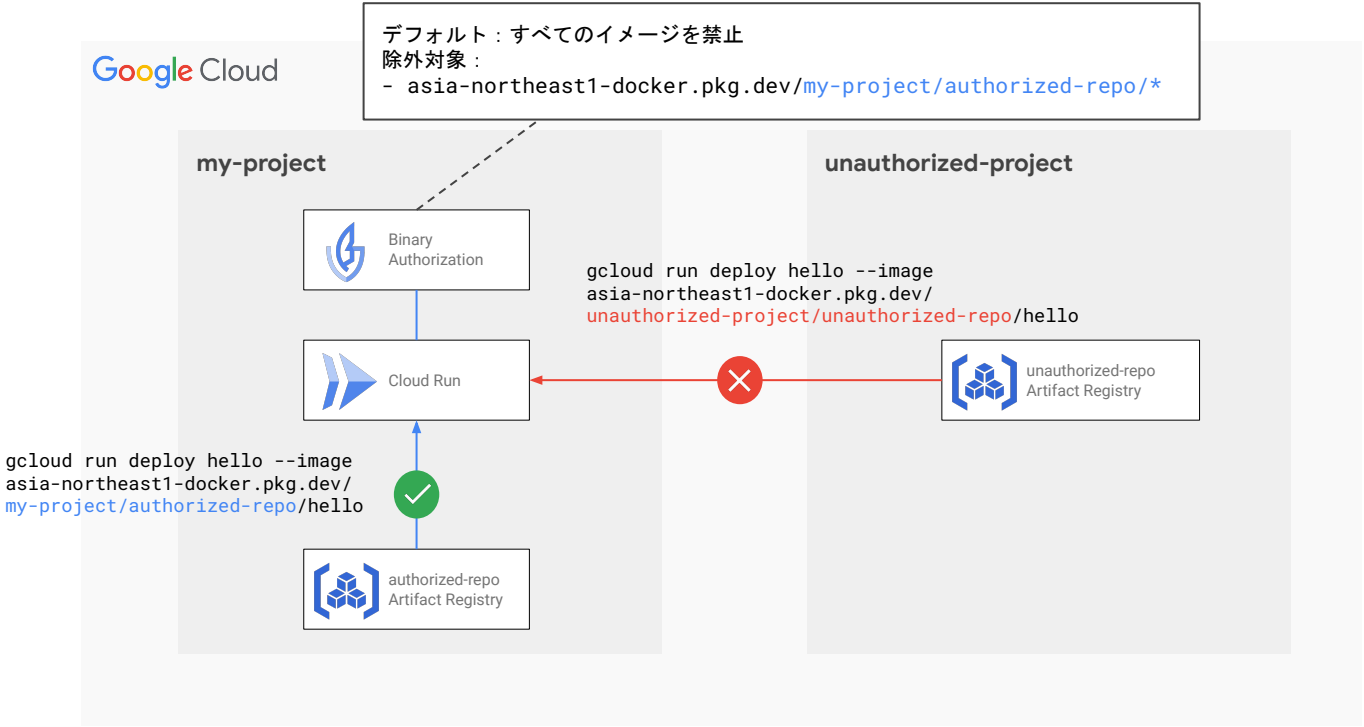
ドライランモードを設定することにより、実際の制御は　行わずに監査ログ上にポリシー適用結果を出力することも

また、Breakglass を利用することで、ポリシーに反する　緊急デプロイの許可も可能（Breakglass の利用は Audit Log に記録される）



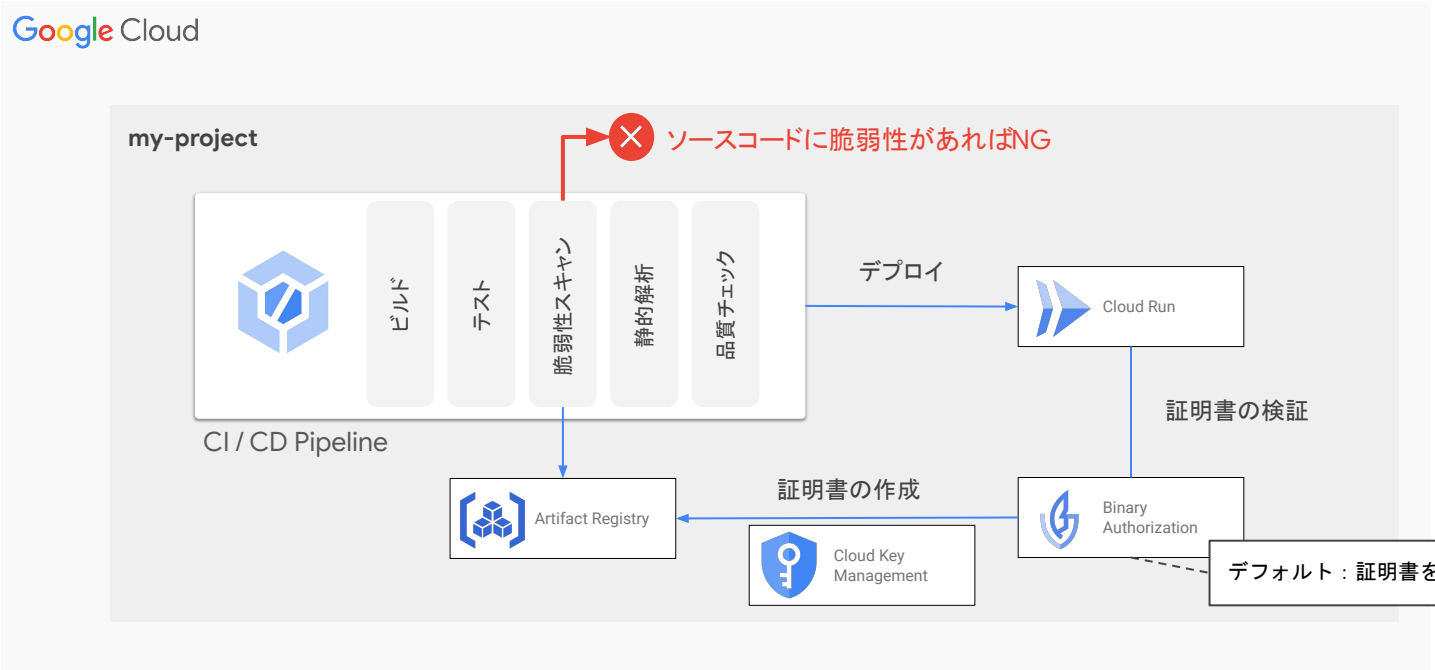
# Binary Authorization 利用例 ①

## 許可されたリポジトリ上のイメージのみデプロイを許可



# Binary Authorization 利用例 ②

脆弱性スキャンが実行されたイメージのみデプロイを許可

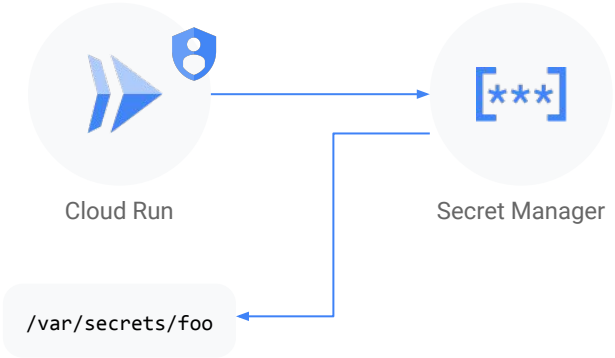


# Secret Manager

Cloud Run では **Secret Manager** をネイティブにサポートしており、機密情報を Secret Manager でセキュアに管理可能

シークレットは**ボリューム**としてマウントするか、**環境変数**に設定することができる（Jobs の場合は環境変数のみ　サポート）

シークレットに対するアクセス権限は IAM で制御



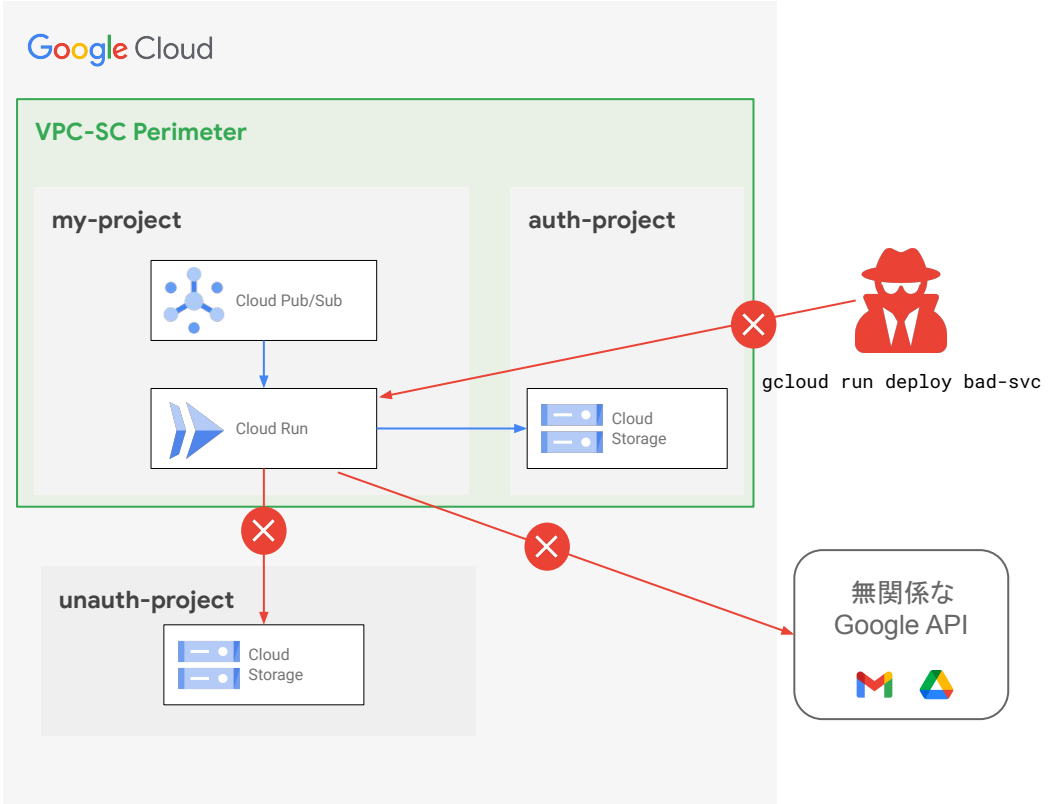
05

# より厳密に制御するために

# VPC Service Controls

Cloud Run を VPC Service Controls の境界内に含めることで、以下のようなリスクを低減

- 悪意のある内部関係者や感染コードによる**データの持ち出し**
- **盗まれた認証情報を使用**し、無許可のネットワークから Cloud Run サービスをデプロイ / 更新



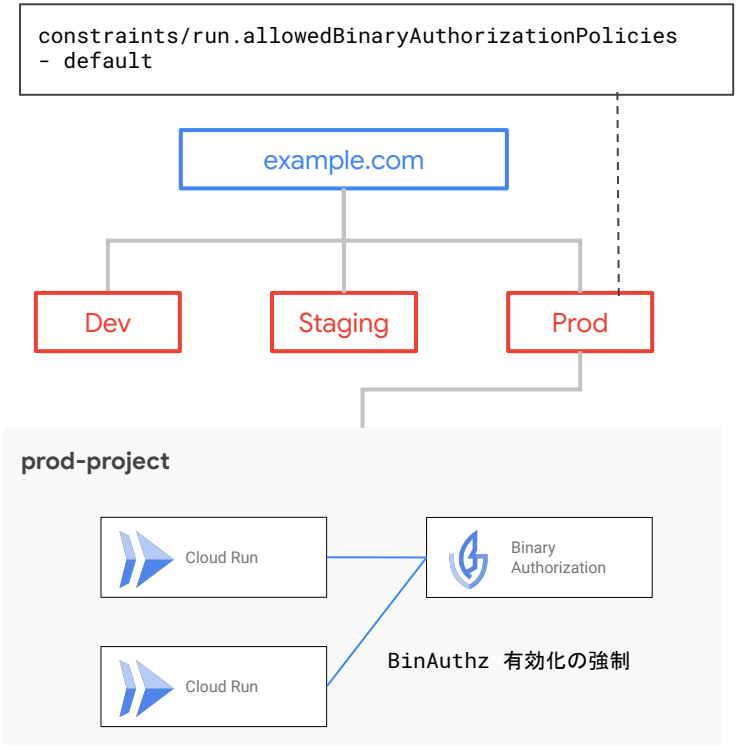
# 組織ポリシーによる強制

組織ポリシーを設定することにより、**Cloud Run の　各種設定を強制**させることが可能に

- Ingress 設定
- Egress 設定
- Binary Authorization 有効化

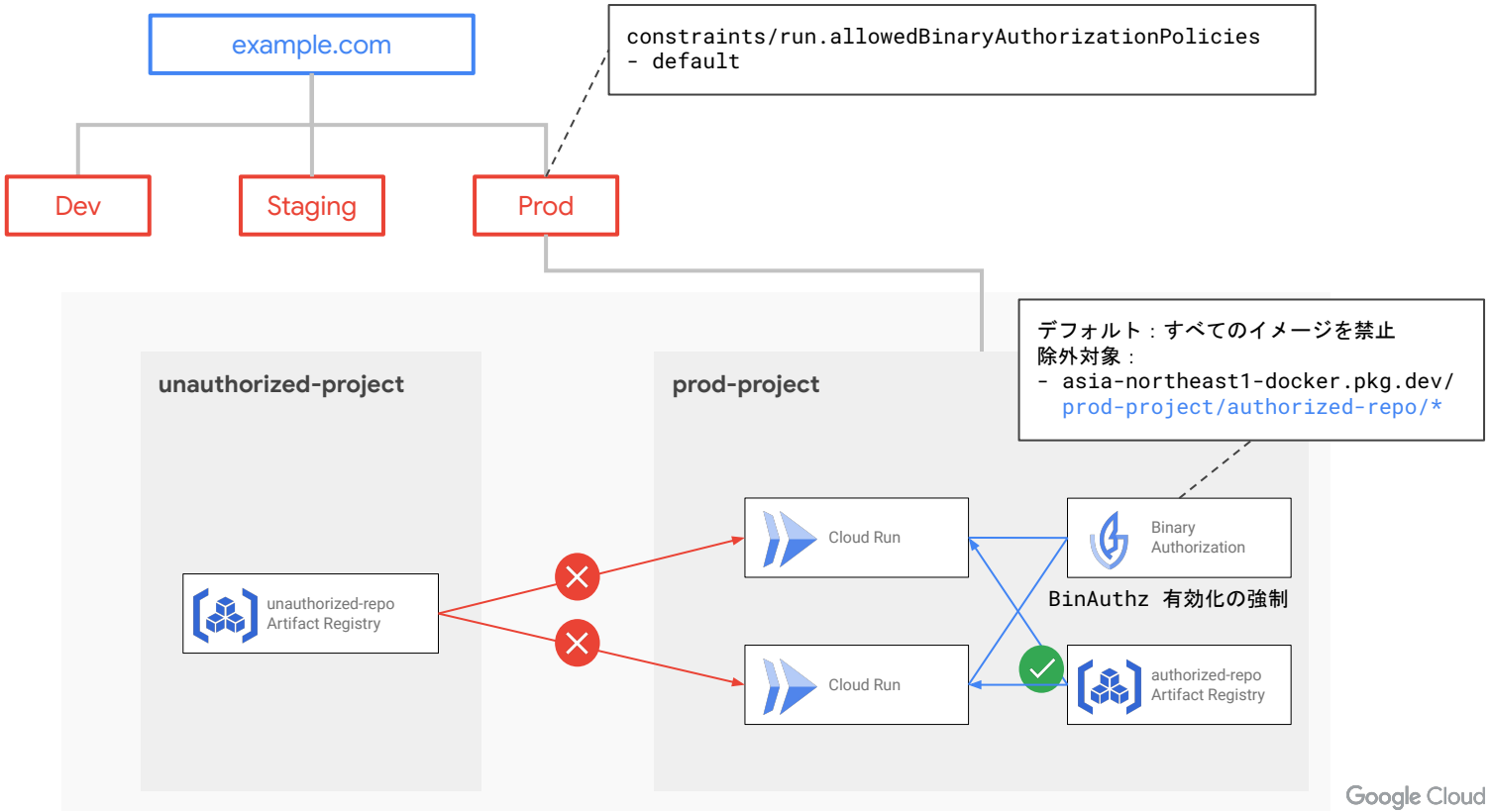
組織ポリシーは組織ノードだけでなく、特定フォルダ配下や特定プロジェクトに対しても設定可能

タグを利用し、サービス単位でより細かなポリシー　制御を実現



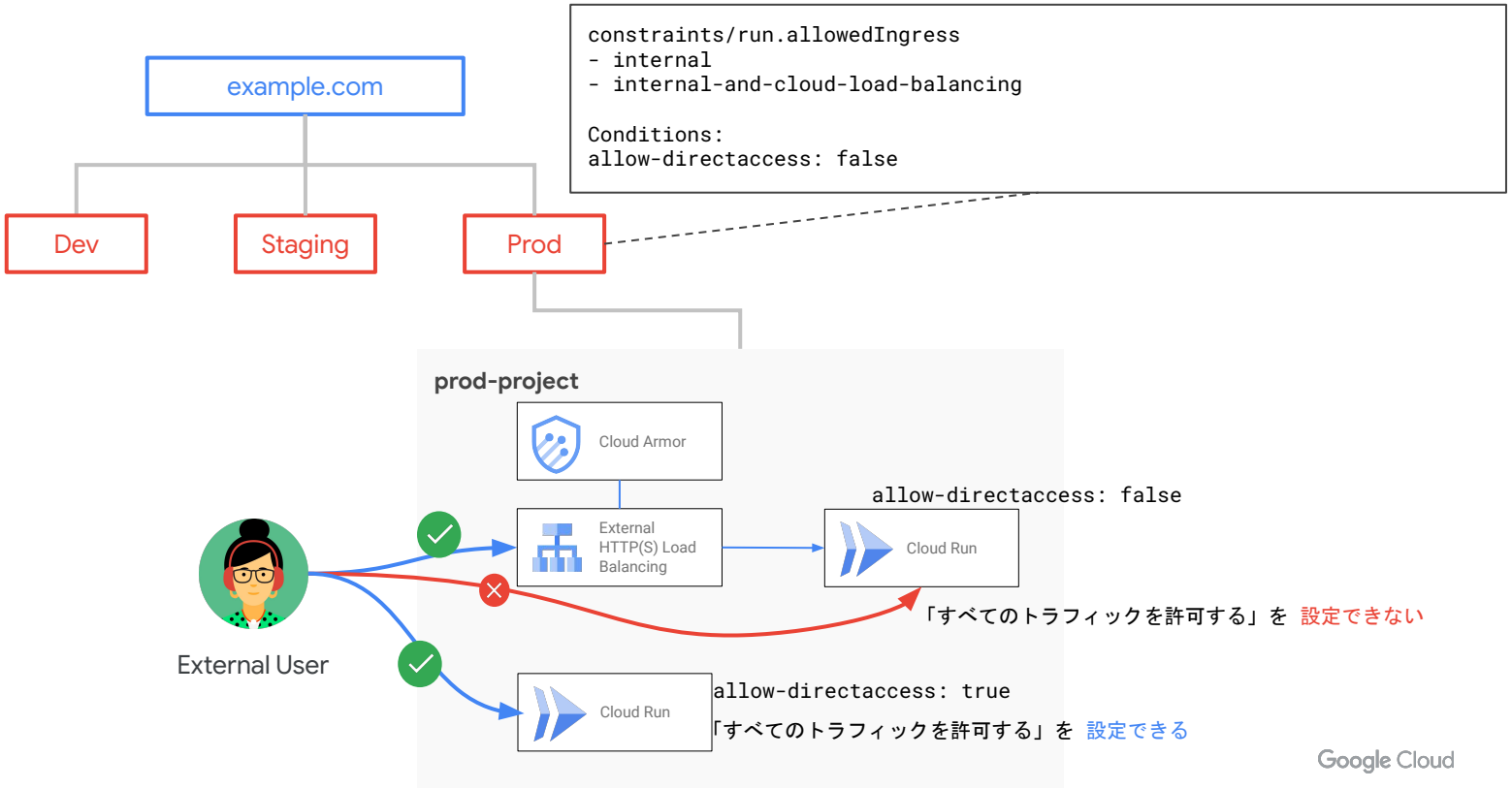
# 組織ポリシーの利用例 ①

## 本番環境のサービスでは Binary Authorization の有効化を必須にする



# 組織ポリシーの利用例 ②

## 特定のタグが付いているサービスでは Cloud Run サービスへの直アクセスを許可しない



06

# まとめ

# ユーザーアクセスの制御のまとめ

- ユーザーアクセスの特性に応じて、ネットワーク経路やサービスへのアクセス権限を絞ることで、**攻撃の機会を少なく**することができる
- 外部ユーザーからのアクセスが発生するようなケースでは **Cloud Armor** の機能を利用しアプリケーションを保護することが可能
- 社内向けアプリケーション等の場合は **Identity-aware Proxy** を利用し認証・認可の仕組みを組み込むことができる
- **Internal HTTP(S) Load Balancing** や **Private Service Connect (PSC)** を利用しプライベートな経路で Cloud Run サービスにアクセス可能
- Cloud Run サービスの前にロードバランサーを配置する場合は、Ingress 設定により Cloud Run への**ダイレクトアクセスを防ぐ** ことを推奨

# サービス間通信の制御のまとめ

- デフォルトのサービスアカウントは強い権限を持っているため、サービス単位で **最小権限が付与されたサービス アカウントを作成・設定** することを推奨
- **サーバーレス VPC アクセス コネクタ**を使うことで、プライベートな IP アドレスで公開された VPC ベースのリソースにアクセス可能
- Cloud Run サービス間の通信において、バックエンドサービス側で呼び出し元を制限したいケースでは「認証が必要」を選択することで、**匿名アクセスを防ぎ** IAM による認可を有効化できる
- Cloud Run からの Egress トラフィックを全て Cloud NAT を経由させて外部サービスへアクセスすることで **Egress IP アドレスの固定化** が可能
- オンプレミスや 3rd Party サービスなど Google Cloud 外部から **Workload Identity Federation** を使うことで Service Account Key のダウンロード不要で認証付きアクセスが可能に

# ワークロードセキュリティのまとめ

- **Google 提供のベースイメージ** など、信頼できるリポジトリで公開されているベースイメージを利用することでセキュリティリスクを抑える
- 攻撃対象領域を小さくするために、**slim や distroless 等の軽量ベースイメージ** の利用を検討する
- **Container Analysis** を有効にし、定期的にイメージの脆弱性スキャンを実行する
- **Binary Authorization** を有効にし、信頼できるコンテナ イメージのみが Cloud Run にデプロイされることを保証する
- アプリケーション内で扱う機密情報は **Secret Manager** で管理する

# より厳密に制御するために

- Cloud Run を VPC Service Controls 境界に含めることで、以下のリスクを低減可能
  - 悪意のある内部関係者や感染コードによる **データの持ち出し**
  - **盗まれた認証情報を使用**し、無許可のネットワークから Cloud Run サービスをデプロイ / 更新
- 組織ポリシーを設定することにより、Cloud Run の**各種設定を強制**させることが可能に
  - Ingress 設定
  - Egress 設定
  - Binary Authorization 有効化

# 最後に

- サーバーレスは簡単にサービスを公開できる反面、仕様を知らずに運用していると思わぬ　　セキュリティ インシデントが発生する**リスク**もある
- Cloud Run にはセキュリティ関連の機能・周辺サービスが充実しており、また **エンタープライズに求められるような柔軟な制御** も可能となっている
- Cloud Run を上手に使って「**開発生産性**」と「**セキュリティ**」を両立させていきましょう

# Tech Acceleration Program

## アプリケーション開発支援プログラム

### Prototype

開発予定アプリケーションの
プロトタイプ開発の
ご支援

### Architecture

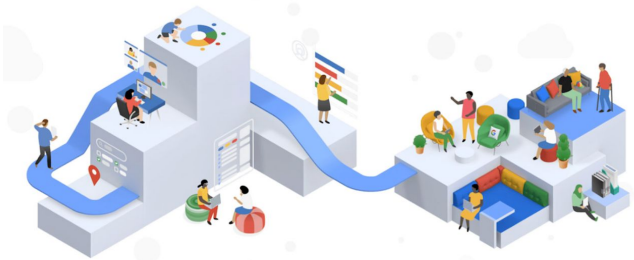
開発予定アプリケーションの
最適なアーキテクチャ設計の
ご支援

### Security

クラウド開発における
セキュリティルール策定の
ご支援

# 内製化支援パートナー

## 内製化支援で DX を加速



| ビジネスアセスメント | 組織・体制作り支援 | テーマ選定 | 技術アセスメント | 開発支援 | 活用・運用支援 |
|---|---|---|---|---|---|
| 課題発掘から開発プロセスへの繋がりをコンサル | アジャイルな開発組織構築支援 | どのようなユニットで何を開発するのか | ユーザー側の技術スキルレベルのアセスメント | PoC、Pilot 開発<br>DevOps との連携支援 ex) GitLab | 定期的な活用支援 |

| | ビジネスアセスメント | 組織・体制作り支援 | テーマ選定 | 技術アセスメント | 開発支援 | 活用・運用支援 |
|---|---|---|---|---|---|---|
| iret | ○ | ○ | ○ | ○ | ○ | ○ |
| CTC | ○ | ○ | ○ | ○ | | |
| UL Systems, Inc. | ○ | ○ | ○ | | | |
| Cloud Ace | ○ | ○ | ○ | ○ | ○ | ○ |
| CREATIONLINE, INC. | | ○ | | | ○ | |
| GI Cloud | | ○ | | | ○ | ○ |
| Sreake | | | | | ○ | ○ |
| Centillion System | | ○ | | ○ | ○ | |
| DIGITAL VORN | | | ○ | ○ | ○ | ○ |

Google Cloud パートナーが提供する内製化支援サービスにご興味のある方はこちらまで
https://goo.gle/naiseika-partners