Architecture Proposal

AWS Infrastructure Proposal

医療AIプラットフォーム

リージョン
ap-northeast-1 (Tokyo)

環境構成
Prod / Staging / Dev

設計原則
High Availability (99.9%)
Security First

プロジェクト概要・目的

プロジェクト目的

- 医療データ（PHI）を安全に扱うAI推論・運用基盤の構築
- MLOpsライフサイクルを加速する高可用かつスケーラブルな環境の提供
- 3省2ガイドラインに準拠したセキュアなインフラの実装

設計原則

AWS Well-Architected
セキュリティ・信頼性・運用上の優秀性などを網羅

高可用性 99.9%以上
Multi-AZ構成による冗長化と自動復旧

セキュリティファースト
ゼロトラスト視点での暗号化・IAM最小権限・監査

環境構成

Production VPC: 10.0.0.0/16

本番運用環境。Multi-AZ冗長化、高スペックインスタンス配置。

Staging VPC: 10.1.0.0/16

検証環境。本番相当の構成でデプロイ前テストを実施。

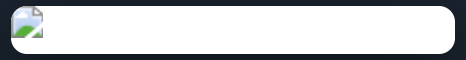
Development VPC: 10.2.0.0/16

開発環境。コストを最適化（NAT削減、インスタンス小型化）。

システム全体構成図

Medical AI Platform Architecture

Generated by GenSpark AI



Edge & Security

CloudFrontによる高速配信とWAFによる境界防御。SSL/TLS終端を行い、安全な通信経路を確立。

Load Balancing

Application Load Balancer (ALB) がトラフィックを分散。Public Subnetに配置し、EKSへの入り口として機能。

Compute (EKS Fargate)

サーバーレスなKubernetes環境。API、推論、Workerの各Podを分離し、スケーラビリティを確保。

Data Persistence

Aurora MySQL (Multi-AZ) による堅牢なRDBと、MLモデル保存用のS3バケット。KMS暗号化を適用。

Container Registry

Amazon ECRでDockerイメージを管理。脆弱性スキャンとバージョニングにより安全性を担保。

Observability

CloudWatchによる統合監視。コンテナログ(api/audit)とメトリクスを可視化し、運用をサポート。

ネットワーク設計 (VPC)

Network Architecture & Subnets

VPC CIDR 設計

Production	10.0.0.0/16
Staging	10.1.0.0/16
Development	10.2.0.0/16

サブネット構成 (本番 3AZ)

Public Subnets (ALB, NAT)

10.0.1.0/24	AZ-1a
10.0.2.0/24	AZ-1c
10.0.3.0/24	AZ-1d

Private Subnets (EKS, Aurora)

10.0.11.0/24	AZ-1a
10.0.12.0/24	AZ-1c

アプリケーション層 (EKS + Fargate)

Application Layer Architecture

Load Balancer

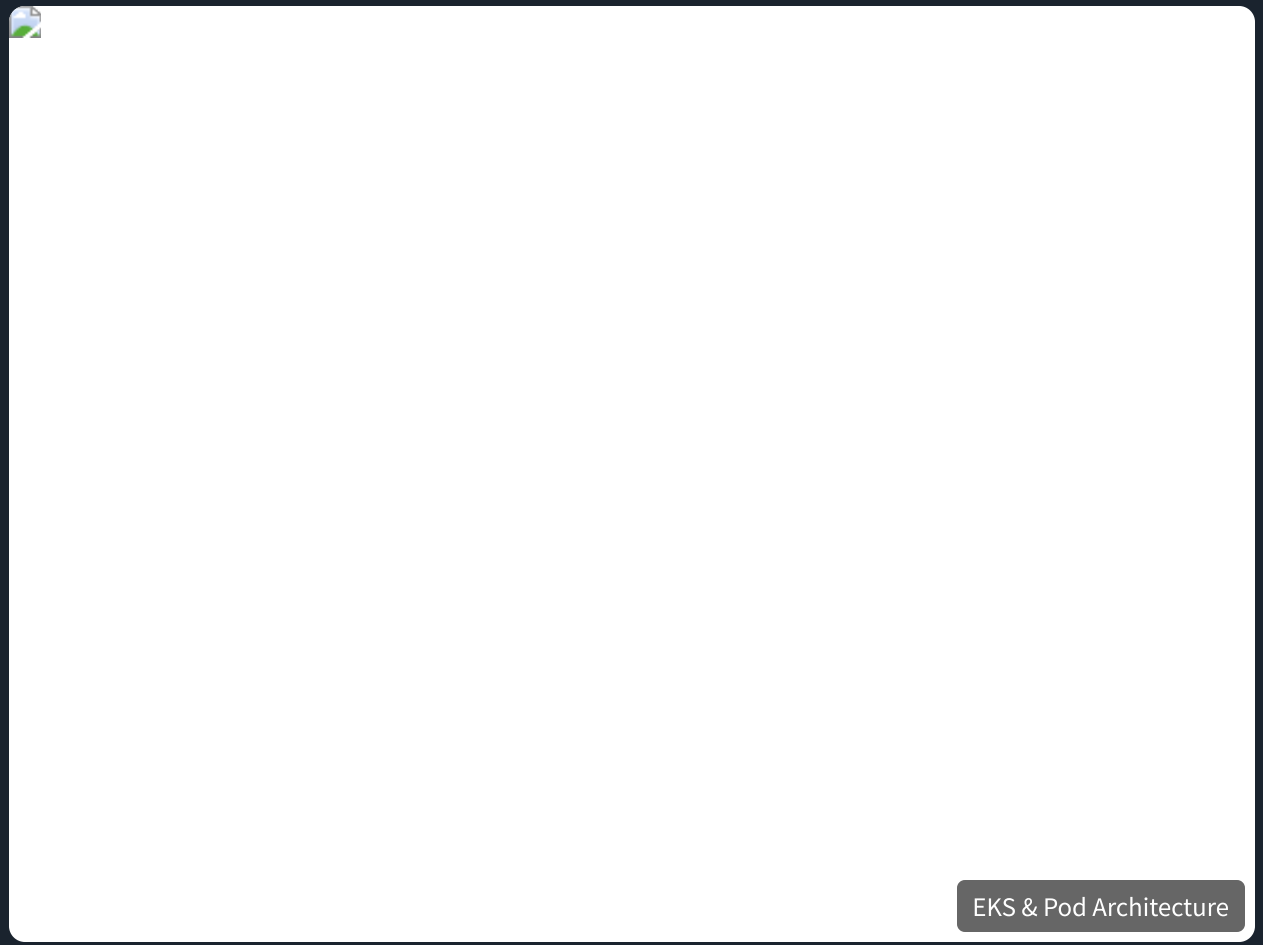
- Application Load Balancer (ALB) を採用
- Public Subnetに配置し、インターネットからのトラフィックを集約

EKS Cluster (Serverless)

- **Kubernetes 1.28** を採用
- **AWS Fargate** によるフルマネージド実行基盤（ノード管理不要）
- Fargate Profile: default, kube-system, mlops

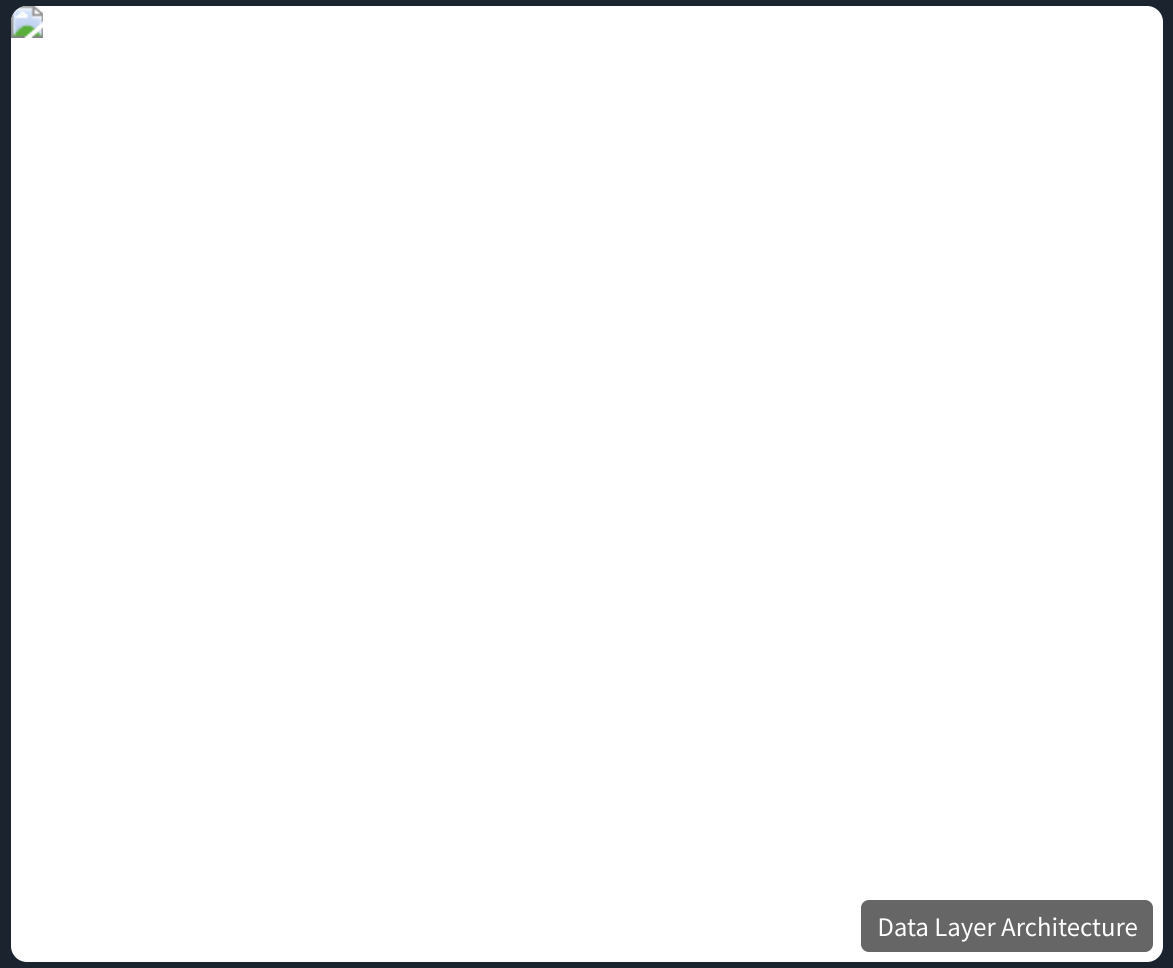
Pod 構成

API	REST/GraphQL APIリクエスト処理
Inference	MLモデルによる推論実行（CPU/GPU最適化）
Worker	非同期タスク・データ前処理



データ層（Aurora + S3 + ECR）

Data Persistence & Registry Strategy



Amazon Aurora MySQL 8.0

医療データの核となるリレーショナルデータベース

構成	Multi-AZ (Primary + Read Replica)
暗号化	KMS (At Rest) / SSL (In Transit)
バックアップ	保持期間 35日 (PITR)
インスタンス	Prod: db.r6g.large / Dev: db.t3.medium

Amazon S3

MLモデルおよび非構造化データの保存

用途	MLモデル / ログアーカイブ
アクセス制御	パブリックアクセス完全ブロック
暗号化	SSE-KMS (サーバーサイド暗号化)
保護機能	バージョニング有効

Amazon ECR

コンテナイメージのセキュアな管理

セキュリティ対策 (医療データ対応)

Security & Compliance for Healthcare

規制・基準

Governance & Standards

医療情報システムとしての適格性を担保するため、以下のガイドラインおよび基準に準拠した設計を行います。

- **3省2ガイドライン準拠**
  厚労省・総務省・経産省の医療情報ガイドライン適合
- **PHI (保護対象保健情報) 対応**
  個人情報の適切な分離とアクセス制御の実装
- **AWS Well-Architected**
  セキュリティ・ピラーに基づくベストプラクティス

暗号化

Encryption (In-transit / At-rest)

- **転送時:** 全通信をTLS 1.2+で暗号化。CloudFront/ALBで終端し、内部通信もTLS化。
- **保存時:** AWS KMS (Key Management Service) を用いてAurora/S3/ECR/EBS

アクセス制御

Identity & Access Management

- **IAM最小権限:** RBACに基づき、ユーザー・サービスごとに必要最小限の権限のみを付与。
- **IRSA (EKS):** Pod単位でIAMロールを割り当て、コンテナからのAWSリソース

境界防御

Network Security & WAF

- **AWS WAF:** SQLインジェクション、XSS等の攻撃をブロック (Managed Rules利用)。
- **レート制限:** 1000 req/5min の制限を設け、DDoSや過剰アクセスを緩和。

監査・ログ

Audit & Logging

- **VPC Flow Logs:** ネットワークトラフィックを全記録し、不正通信を検知可能に。
- **証跡管理:** CloudTrailおよびCloudWatch Logsにより、操作ログを

監視・運用体制

Monitoring & Operations Strategy

統合監視（Observability）

CloudWatch & Container Insights

EKSのメトリクス（CPU/メモリ）、Podログ（api/audit）、およびインフラ全体の死活監視を集約。

アラート通知連携

異常検知時はSNS経由でChat/メールへ即時通知。重大度に応じたエスカレーションフローを定義。

運用・デプロイメント

CI/CDパイプライン

GitHub Actions連携。ECRへのイメージプッシュをトリガーに、EKSへ自動デプロイ（Blue/Green検討）。

SLA & 変更管理

データ保護・復旧

AURORA BACKUP

35 Days

Point-in-Time Recovery

Auto Snapshot

Enabled

S3 ML MODELS

Versioning & Lifecycle

Cross-Region (Opt)　MFA Delete

Deploy Flow

コスト見積もり（月額・本番環境）

Estimated Monthly Cost (Production)

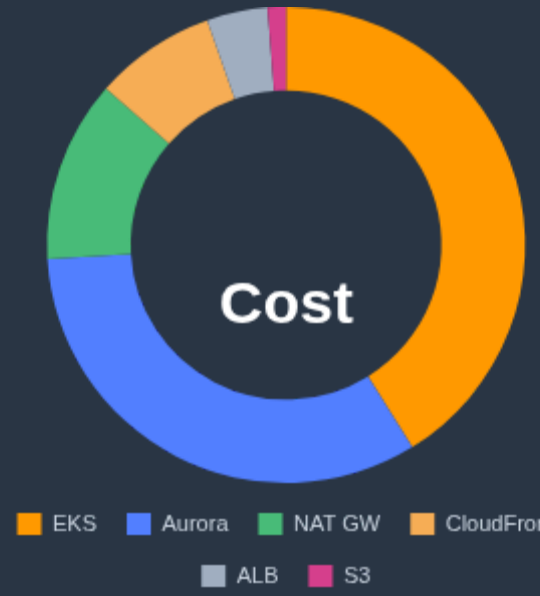
Service Category	Configuration Details	Monthly Cost
Amazon EKS (Fargate)	Cluster + Fargate vCPU/GB	$500.00
Amazon Aurora MySQL	db.r6g.large × 2 (Multi-AZ)	$400.00
NAT Gateway	3 AZs × Traffic Processing	$150.00
Amazon CloudFront	1TB Outbound Transfer	$100.00
Application Load Balancer	LCU + Hourly Charge	$50.00
Amazon S3	500GB Storage + Requests	$15.00

上記金額はAWS計算ツールに基づく概算見積もり（USD）です。実際のご請求額は、データ転送量、リクエスト数、為替レート、税金等により変動します。
リザーブドインスタンスやSavings Plansの適用により、さらにコストを削減できる可能性があります。

ESTIMATED TOTAL

$1,215 / month

(約 182,250 円 @ 150円/$)



今後のロードマップ

Implementation Roadmap & Milestones

PHASE 1 — 1-2 Weeks

設計・アセスメント

- 基本/詳細設計レビュー
- セキュリティ要件定義 (3省2ガイドライン)
- AWSアカウント/VPC環境準備

PHASE 2 — 2-4 Weeks

PoC・検証環境構築

- Staging環境でのEKSデプロイ
- ML推論負荷テスト
- CI/CDパイプライン整備

PHASE 3 — 1-2 Weeks

本番移行・ローンチ

- 本番環境 (Production) 構築
- セキュリティ監査ログ運用開始
- 切り替え・サービスイン

PHASE 4 — Ongoing

運用・最適化

- コストモニタリング・チューニング
- 定期的なセキュリティレビュー
- EKSバージョンアップ計画