Confidential（秘密情報）

動画コンテンツシステム

インフラ構築手順書

第1.1版　2024年11月1日

株式会社ドットライフ

改定履歴

|  |  |  |  |
| --- | --- | --- | --- |
| 版数 | 日付 | 改定内容 | 項番・ページなど |
| 1.0 | 2024年11月1日 | 初版作成 |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目次

内容

[1. 業務要件 3](#_Toc193356483)

[1-1. システム化の背景と目的 3](#_Toc193356484)

[1-2. システムの全体像 今回構築するシステムの全体構成図は以下である。 3](#_Toc193356485)

[1-3. システム化の範囲 3](#_Toc193356486)

[2. 機能・非機能要件 3](#_Toc193356487)

[2-1. 機能要件 4](#_Toc193356488)

[2-2. 非機能要件 5](#_Toc193356489)

[3. インフラ設計 6](#_Toc193356490)

[3-1. アーキテクチャ 6](#_Toc193356491)

[3-2. テクノロジースタック 6](#_Toc193356492)

[3-3. ソーステクノロジスタック 6](#_Toc193356493)

[4. インフラ構築手順(APP or LP) 7](#_Toc193356494)

[4-1. 前提条件 7](#_Toc193356495)

[4-2. 作業完了条件 7](#_Toc193356496)

[4-3. 作業者 7](#_Toc193356497)

[4-4. 作業場所 7](#_Toc193356498)

[4-5. 作業端末 7](#_Toc193356499)

[4-6. 制約事項・備考 7](#_Toc193356500)

[4-7. 作業実績 7](#_Toc193356501)

[4-8. 手順 8](#_Toc193356502)

[4-8-1. VPC 8](#_Toc193356503)

[4-8-2. EC2 8](#_Toc193356504)

[4-8-3. RDS 9](#_Toc193356505)

[4-8-4. ALB 9](#_Toc193356506)

[4-8-5. S3 9](#_Toc193356507)

[4-8-6. CloudFront 10](#_Toc193356508)

# 1. 業務要件

## 1-1. システム化の背景と目的

　現行のサービスは、Gigaスクール構想やDX化に伴う急速なコンテンツ拡充に対応できないことが課題となっている。

また、講師ごとに異なるスキルや経験に対応するカスタマイズ機能や、学習進捗の可視化機能の不足も指摘されている。

これを解決するため、クライアント企業は新たな動画コンテンツ配信システムの開発を決定した。

## 1-2. システムの全体像 今回構築するシステムの全体構成図は以下である。

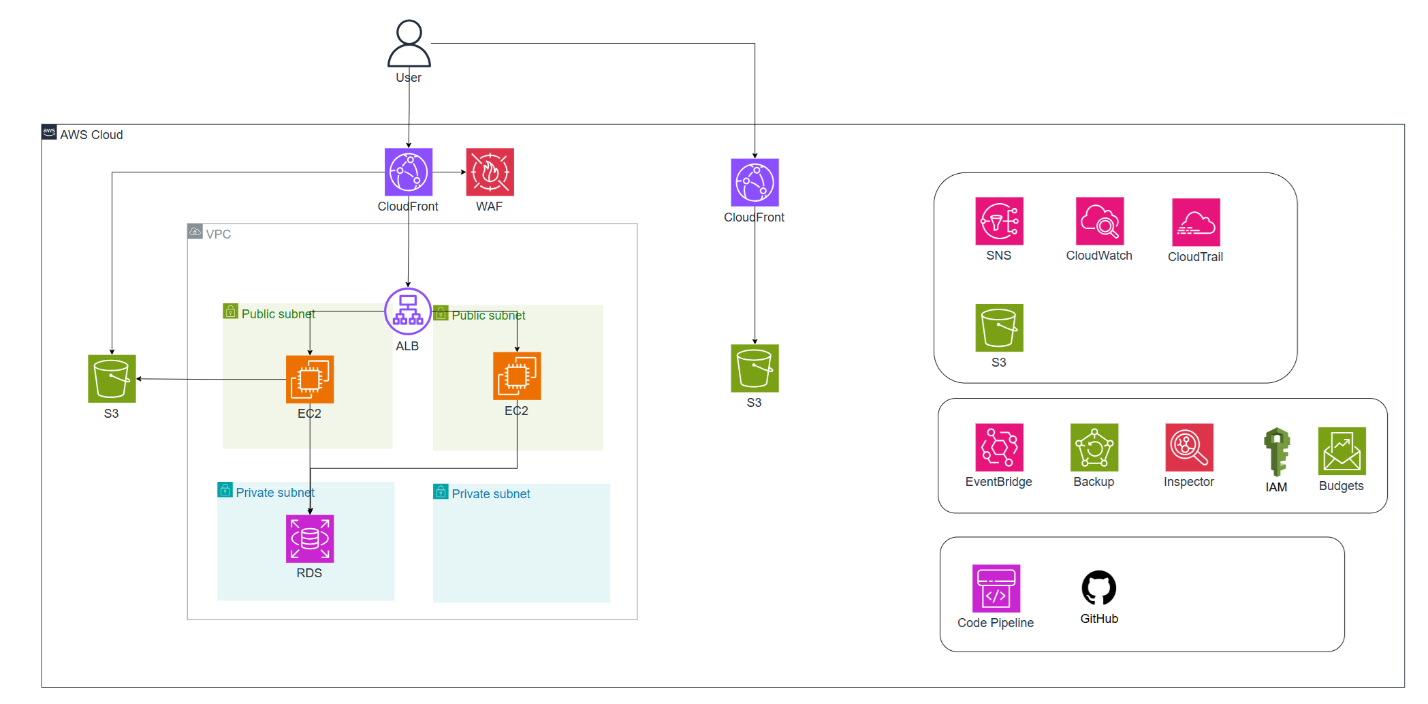


Fig.1 全体構成図

## 1-3. システム化の範囲

本システムの開発範囲は、動画コンテンツ全体のインフラ基盤を開発する。

# 2. 機能・非機能要件

動画コンテンツシステム新規開発プロジェクトの機能要件と非機能要件である。

## 2-1. 機能要件

1. 環境

* 開発環境のみ構築
* 開発環境内の構成
  + App（動画プラットフォーム用システム）
  + LP（動画プラットフォーム用の静的サイト）

2. サーバー（App）

* EC2 (Amazon Linux 2023)
* Javaバージョン: JDK 17
* フレームワーク: Spring Boot
* 必要なソフトウェア
  + Git
  + Maven
  + Gradle
  + Timezone 設定
  + PostgreSQL client
* IPアドレスを固定

3. データベース

* Amazon RDS (PostgreSQL 16)
* 初期データベース名: movie
* Timezone 設定

4. ストレージ

* S3 バケット
  + App: 動画保存用
  + LP: 静的ホスティング用（静的Webサイト）

5. 負荷分散

* ALB による負荷分散
* パスベースルーティング
  + /contents/\* → S3 へリダイレクト
  + その他のパス → ALB へ

6. 監視

* Appサービスの監視
  + エラー発生時にメール通知
  + 監視結果をダッシュボード化

7. CI/CD

* LP に対する CI/CD 環境の構築

8. IAM管理

* 開発メンバー以外の IAM 設定
  + 経理部門: コスト関連のサービスのみ許可
  + 経営管理部門: 管理者権限 (Admin)
  + IT部門: Cost と IAM 以外の権限

9. 監査

* ISO27001取得予定に対応
* AWSユーザー操作ログを S3 に保存

## 2-2. 非機能要件

1. 可用性

* App / LP の可用性を99.9%以上
* 負荷分散を実施
* EC2 / RDS の AZ 冗長化
  + テスト時以外は EC2 を停止し、RDS は Single-AZ でコスト削減
* 動画コンテンツのキャッシュ化
* メンテナンスページの作成と切り替え機能

2. セキュリティ

* ストレージの暗号化
* 脆弱性診断
  + EC2 → AWS Inspector
  + LP → OWASP ZAP

3. バックアップ

* EC2 / RDS のバックアップを 7 世代保存
* メンテナンスタイム: 0時 ~ 4時
  + 0時 ~ 2時は別システム連携があるため要考慮

4. コスト管理

* EC2 は平日日中のみ起動
* ランニングコストを 7 万円 / 月 以下に抑える
* コストが 7 万円 / 月 を超えた場合は通知

5. ドメイン

* ドメイン関連はヒアリング中のため、保留

6. AWS リソースの運用ルール

* 命名規則の設定・運用
* タグの命名規則の設定・運用

7. 監視

* 一般的な監視項目の設定
* 監視結果をメール通知
* 監視ダッシュボードの作成
* メールアドレスは未定のため保留

# 3. インフラ設計

## 3-1. アーキテクチャ

AWSシステム構成図はFig.1に掲載しているため省略

## 3-2. テクノロジースタック

テクノロジースタックは以下である。

* インフラ: AWS（EC2, RDS, S3, ALB）
* アプリケーション: Java 17 + Spring Boot
* CI/CD: AWS CodePipeline
* 監視・運用: CloudWatch, Inspector, OWASP ZAP
* セキュリティ: IAM, S3暗号化
* コスト管理: スケジューリング、予算超過通知

## 3-3. ソーステクノロジスタック

ソーステクノロジスタックは以下である。

* 言語: Java 17
* フレームワーク: Spring Boot
* ビルドツール: Maven, Gradle
* データベースクライアント: PostgreSQL Client
* バージョン管理: Git
* Java 11
* Spring 2.7.15

# 4. インフラ構築手順(APP or LP)

## 4-1. 前提条件

* 作業者のAWSアカウントが発行されていること
* 適切なロールが適用されていること

## 4-2. 作業完了条件

* 全てのリソースの作成が完了していること
* アプリケーションが正しく動くこと

## 4-3. 作業者

* 〇〇 〇〇 (xxxxx@dotlife.co.jp)

## 4-4. 作業場所

* 〒153-0063 東京都目黒区目黒1-4-16

## 4-5. 作業端末

* Macbook Pro, 2020

## 4-6. 制約事項・備考

* 特になし

## 4-7. 作業実績

 VPC

* 10.0.0.0/24

 EC2（Amazon Linux 2023）

* 固定IPアドレス設定
* JDK 17、Spring Boot、Git、Maven、Gradle、PostgreSQL Clientのセットアップ
* タイムゾーン設定

 RDS（PostgreSQL 16）

* 初期データベース（movie）の作成
* タイムゾーン設定
* シングルAZでの構築（テスト以外の時間は停止）

 S3バケット

* 動画保存用S3（動画コンテンツ格納用）

 ALB

* EC2へ転送、HTTPS終端

 CloudFront

* オリジン: ALB（アプリケーション用ロードバランサ）、S3
* /contents/\* → S3、それ以外はALBへ転送
* プロトコル: HTTPS のみ許可（HTTP → HTTPS リダイレクト）

## 4-8. 手順

### 4-8-1. VPC

1. AWS マネジメントコンソール にログイン
2. VPC サービス を開く
3. 左メニューの 「VPC を作成」 をクリック
4. VPCなどを選択



1. 設定の入力（詳細な設定はパラメータシートを参照）
2. 「VPCを作成」をクリック

正常性確認

* VPCなど必要なネットワーク設定ができていること

### 4-8-2. EC2

1. AWS マネジメントコンソール にログイン
2. EC2 サービス を開く
3. 「インスタンスの作成」ボタンをクリック
4. 設定の入力（詳細な設定はパラメータシートを参照）
5. 「起動」ボタンを押す
6. SSHにログインし、内部設定を実施（詳細な設定はパラメータシートを参照）

正常性確認

* EC2のステータスチェックが2/2であること
* EC2にSSHログイン可能であること
* 必要なソフトウェアがインストールされていること

### 4-8-3. RDS

1. AWS マネジメントコンソール にログイン
2. RDS サービス を開く
3. 「データベースの作成」ボタンをクリック
4. 設定の入力（詳細な設定はパラメータシートを参照）
5. 「データベースの作成」ボタンをクリック
6. 作成完了まで待機（15分程度）

正常性確認

* RDSが正常に起動していること
* EC2からRDSへログインできること

### 4-8-4. ALB

1. AWS マネジメントコンソール にログイン
2. EC2 サービス を開く
3. 左メニューの 「ロードバランサー」 を開き、「ロードバランサーを作成」ボタンをクリック
4. 設定の入力（詳細な設定はパラメータシートを参照）

正常性確認

* TGがhealthyであること
* ALBのDNS名でEC2の内容が表示されていること

### 4-8-5. S3

1. AWS マネジメントコンソール にログイン
2. S3 サービス を開く
3. 「バケットを作成」ボタンをクリック
4. 設定の入力（詳細な設定はパラメータシートを参照）
5. 「バケットを作成」ボタンをクリック

正常性確認

* バケットが正しく作成されていること

### 4-8-6. CloudFront

1. AWS マネジメントコンソール にログイン
2. CloudFront サービス を開く
3. 「ディストリビューションを作成」ボタンをクリック
4. 設定の入力（詳細な設定はパラメータシートを参照）
5. 「ディストリビューションを作成」ボタンをクリック

正常性確認

* ディストリビューション名にてEC2の表示内容が確認できること

以上