# はじめに

## 本書の目的

本プロジェクトにおけるAWS上でのシステムアーキテクチャの基本となる考え方、設計方針を示すことを目的とする。

LION様提供の構築ガイドライン、クラウドセキュリティガイドラインに基づき、クラウドの特徴を活かしたスケーラブルで俊敏性が高く障害に強いシステム構築を行えることを第一に考える。

## 関連資料

本書の前提となる資料、情報元となる資料は以下の通り。

* [非機能要件一覧](https://docs.google.com/spreadsheets/d/1B5z5-YWOrzDnu0gY5AM-_wRCRX9LD9EZ/edit?usp=share_link&ouid=106375452255861814726&rtpof=true&sd=true)
* [構築ガイドライン](https://drive.google.com/file/d/1KaAbHae4c2WQy37im2Ujmpvk_nD-QD8-/view?usp=share_link)
* [クラウドセキュリティガイドライン](https://docs.google.com/document/d/1uHi7mWWJaxotaLL3iJ90vqa7ZCzF9PId/edit?usp=share_link&ouid=106375452255861814726&rtpof=true&sd=true)
* [POHR論理システム構成図](https://app.diagrams.net/#G122z8inmGkVqX_vwh6zkzKVSDbcr20eBX)
* [オーラル基盤\_概念モデル](https://app.diagrams.net/#G1F1moihXjpFEtD_5xQSGJ-sSz7ku2HhB_)

# 対象非機能要件

本書に関連する対象非機能要件は以下の通り。

| 大項目 | 項番 | 定義項目 | 決定メトリクス | 備考 |
| --- | --- | --- | --- | --- |
| 可用性 | A.1.2.3 | 業務継続性 | 単一障害時は業務停止を許容せず、処理を継続させる | 単一の定義をZONE・基盤の種類とする |
| 可用性 | A.1.4.1 | 大規模災害時　システム再開目標 | 再開不要 |  |
| 可用性 | A.2.4.3 | ネットワーク | ・セグメント分割用途に応じて分割 | 各ZONE毎にAWSアカウントを分ける |
| 可用性 | A.3.1.1A.3.2.1A.3.2.2A.3.3.1 | 災害対策 | なし |  |
| 運用・保守性 | C.4.1.1 | 開発用環境の設置 | 運用環境の一部に限定した開発環境を設置する |  |
| 運用・保守性 | C.4.2.1 | 試験用環境の設置 | 専用の試験用環境を設置する |  |
| 運用・保守性 | C.4.5.1 | 社外の外部システムと接続する | 社外の外部システムと接続する |  |
| セキュリティ | E.1.1.1 | 情報セキュリティに関するコンプライアンス | 順守すべき社内規程、ルール、法令、ガイドライン等有 | LION様提供のAWSクラウドセキュリティガイドライン、AWS構築ガイドライン |
| システム環境・エコロジー | F.1.1.1/F.1.2.1 | 構築/運用時の制約条件 | 制約有り(重要な制約のみ適用) | LION様提供のAWSクラウドセキュリティガイドライン、AWS構築ガイドライン |

## 対象範囲

本書の対象となるシステムは以下の通り。

* P-ZONE(生活者向けシステム)
* L-ZONE(LION様/CDH向けシステム)
* D-ZONE(歯科医院向けシステム)
* 通知配信基盤(SMS/Email/プッシュ配信)
* オーラル基盤（ver1ではP-ZONEのみとの接続）

## 外部システム

上記システムと接続する外部システムは以下の通り。

* LION基盤（P-ZONEとの接続）
* Chat SaaSサービス（P-ZONE/L-ZONEとの接続）
* 通知配信サービス（SMS、Email、FCM）　（通知配信基盤との接続）
* LIONデータ基盤　（対象システムとの接続）

# AWS アーキテクチャ共通

## AWS アカウント

本プロジェクトで使用する AWS アカウント（AWSアカウントは仮）は以下の通り。

| AWS アカウント | 対象システム | 実行環境 |
| --- | --- | --- |
| 11111111nnnn | P-ZONE | 本番、ステージング、開発、性能試験 |
| 22222222nnnn | L-ZONE | 本番、ステージング、開発、性能試験 |
| 33333333nnnn | D-ZONE | 本番、ステージング、開発、性能試験 |
| 44444444nnnn | 通知配信基盤 | 本番、ステージング、開発、性能試験 |
| 55555555nnnn | オーラル基盤 | 本番、ステージング、開発、性能試験 |

## 実行環境

本プロジェクトで使用する実行環境を以下の通り定義する。

| 実行環境 | 目的 |
| --- | --- |
| 本番 | 顧客向けサービスを提供する |
| ステージング | 開発済みアプリケーションの動作確認、パッチの事前適用や動作確認、本番環境で発生したトラブルの再現など |
| 開発 | 開発時のアプリケーション、インフラの動作確認 |
| 性能試験 | 性能テスト時のアプリケーション、インフラの動作確認 |

## CIDR

各AWSアカウントに割り当てるCIDRは以下の通り。

| AWS アカウント | CIDR |
| --- | --- |
| 11111111nnnn | 10.0.0.0/16 |
| 22222222nnnn | 10.10.0.0/16 |
| 33333333nnnn | 10.20.0.0/16 |
| 44444444nnnn | 10.30.0.0/16 |
| 55555555nnnn | 10.40.0.0/16 |

## AWS アカウント間通信

AWSアカウント間の通信はTransit Gatewayとする 下記資料では５VPC以上のフルメッシュではTransit Gatewayを推奨しているため。 [クラスメソッド資料](https://dev.classmethod.jp/articles/different-from-vpc-peering-and-transit-gateway-japanese/)

## リージョン

本プロジェクトでは東京リージョンを使用する。

## DR対応

Ver1ではDR対応は実施しない