# はじめに

## インフラ基本設計の目的

本プロジェクトにおける非機能要件及びLION様にて規定されたセキュリティガイドライン及びAWS構築ガイドラインを基にインフラ構築における基本的な考え方、設計方針を示すことを目的とする。

# 作成ドキュメント

クラスメソッド社作成の[クラウドデザインシート](https://github.com/YoshiiRyo1/document-templates-for-aws/tree/master/design/doc_source)を参考にインフラ基本設計に必要な下記ドキュメントを作成する。 尚、ドキュメントのフォーマットについては、Markdown形式をdocxに自動変換し作成する。（全体環境構成についてはdraw.ioで作成）

## アーキテクチャ共通

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

* 対象範囲 対象システム範囲を定める
* AWSアカウント 本プロジェクトで使用するAWSアカウントを示す
* 実行環境 本プロジェクトで使用する実行環境を定義する。
* CIDR 各AWSアカウントに割り当てるCIDRを定義する。
* AWSアカウント間通信 AWSアカウント間の通信要件を定める
* リージョン 使用するリージョンを定める
* Availability Zone AZの利用有無を定める

## システム可用性

非機能要件定義で定めた稼働率や計画停止を示す。 また、冗長構成パターンを示す。

* 稼働率
* 稼働時間
* メンテナンススケジュール
* 計画停止
* 冗長構成 AWS各種サービスの冗長構成パターンを示す

## リソース命名

* 関連資料
* 目的
* 基本ルール
* 命名規則表
* AWSリソース
* タグ

## AWS利用サービス/外部サービス

全体環境構成にて利用するAWSサービス及び外部サービスを定める。

* WEBサーバ
* APサーバ
* DBサーバ
* バッチサーバ
* ファイルサーバ
* 監視サーバ
* 踏み台サーバ
* パッチ管理サーバ
* セキュリティ対策サービス
* 外部サービス 　アプリケーションファイアウォール、DOS対策、ウィルスソフト等

## ネットワーク

ネットワーク構成を設計する上で定義が必要な下記について定める。

* ネットワーク構成方針
* CIDR
* VPC Flow Logs
* サブネット設計
* Internet Gateway
* NAT Gateway
* VPCエンドポイント
* DNSサーバ
* 踏み台サーバ
* VPCピアリング

## 全体環境構成

下記事項についてのインフラ構築の方針を定め、全体環境構成を図示する。

* 関連資料
* 使用リージョン
* マネージドサービスの利用有無
* MultiAZの利用有無
* 通信の暗号化
* アクセス制御
* データの暗号化
* 個人情報の格納先
* AWSリソース管理

## 構成管理

アプリケーションやインフラのソースコードの構成管理を定める。

* アプリケーション、インフラのソースコードの管理ツール
* ソースコード運用方法

## デプロイ・プロビジョニング

アプリケーションのデプロイ方法やIaCについて定める。

* アプリケーションのデプロイ
* インフラのコード化
* 手動パターン

## 監視

非機能要件を基に監視対象や監視ツールや監視方法を定める。

* 監視目的
* 監視対象
* 収集ツール
* 監視方法

## パッチ管理

パッチ管理として使用するツールを定める。

* OSパッチ
* RDS

## セキュリティ対策

非機能要件やAWSセキュリティガイドラインを基に下記について定める。

* セキュリティグループによるアクセスコントロール
* ネットワークACLによるアクセスコントロール
* IAMユーザー/グループ/ポリシー/ロール
* IAM ユーザーパスワードポリシー
* IAM ユーザーアクセスキー
* データ暗号化
* 通信の暗号化
* 保管データの暗号化
* ウィルス/マルウェア対策
* セキュリティを強化する AWS サービス
* Web対策

## アカウント構成

非機能要件及びAWSセキュリティガイドラインを基にAWSアカウント管理方法を定める。

* 方針
* ロール一覧
* 管制塔

## バックアップ・リストア

非機能要件を基に下記を定める。

* バックアップ対象
* バックアップ方式
* リストア方式

## ログ管理

AWS 上でログを取得・保管する方法を定める。

* 対象ログ
* 保管期間