**発行日　2022/2/24**

**版数　第1.0版**

**テンプレート仕様書**

改訂履歴

|  |  |  |  |
| --- | --- | --- | --- |
| **版数** | **担当者** | **日付** | **改訂内容** |
| 1.0 | NID 篠宮 | 2022/2/24 | 新規作成 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

内容

[1 はじめに 4](#_Toc96595785)

[1.1 本資料の目的 4](#_Toc96595786)

[1.2 本資料の対象者 4](#_Toc96595787)

[1.3 本資料の範囲 4](#_Toc96595788)

[2 CloudFormationテンプレート仕様 5](#_Toc96595789)

[2.1 共通仕様 5](#_Toc96595790)

[2.1.1 テンプレート分割 5](#_Toc96595791)

[2.1.2 セクション 5](#_Toc96595792)

[2.1.3 組み込み関数 6](#_Toc96595793)

[2.1.4 論理ID 6](#_Toc96595794)

[2.1.5 エクスポート名 6](#_Toc96595795)

[2.2 各テンプレート仕様 7](#_Toc96595796)

# はじめに

## 本資料の目的

本資料は、営業・融資サポートシステムにおけるCloudFormationテンプレートの仕様書である。本書の記述に従い、以降の工程作業を行うことを目的とする。

## 本資料の対象者

本資料は、営業・融資サポートシステム開発の関係者すべてを対象とする。

## 本資料の範囲

本資料に記載される設計内容については、営業・融資サポートシステムにおけるCloudFormationテンプレートすべてを範囲としている。

# CloudFormationテンプレート仕様

## 共通仕様

テンプレートは横浜銀行(本番・研修・開発)、東日本銀行(本番・研修・開発)の各環境ごとに全体・ネットワーク・DBサーバ・Web/APサーバ・バッチサーバの各テンプレートを用意する。

各テンプレートで共通する仕様を以降に記載する。

### テンプレート分割

各環境ごとに用意するテンプレートは上述の通り、テンプレートの保守性・拡張性を考慮し1つのテンプレートではなく5つのテンプレートに分割する。

テンプレートの名前となっている、全体・ネットワーク・DBサーバ・Web/APサーバ・バッチサーバの分割単位のどこにリソースが含まれるかを考慮してテンプレートの分割を行う。

各テンプレートに含まれるリソースは別紙「IaC詳細設計\_対応リソース一覧」を参照する。

後述するExportセクションとImportValue関数を組み合わせることで各テンプレート間(スタック間)での値の参照を実現する。

### セクション

CloudFormationテンプレートには、形式バージョン・説明・メタデータ・パラメータ・ルール・マッピング・条件・トランスフォーム・リソース・出力のセクションが存在する。

営業・融資サポートシステムのCloudFormationテンプレートでは、形式バージョン・説明・トランスフォーム・リソース・出力セクションを使用する。

各セクションで記載する内容は以下とする。

|  |  |
| --- | --- |
| セクション | 内容 |
| 形式バージョン | テンプレート記載時の最新の形式バージョンを指定する。 |
| 説明 | 拡張子を除いたテンプレート名を記載する。 |
| トランスフォーム | DBサーバテンプレートにのみ使用する。  Secrets Managerのローテーション関数にAWSが用意するLambdaファンクションを使用するために「AWS::SecretsManager」を記載する。 |
| リソース | 各テンプレートで対応するリソースを記載する。  対応するリソース一覧は別紙「IaC詳細設計\_対応リソース一覧」を参照する。  リソースのプロパティについては各環境の別紙「AWSパラメータシート」を参照する。 |
| 出力 | 各テンプレート間での値の参照を実現するために、テンプレートに含まれる一部リソースの出力を記載する。  記載対象のリソース及び出力内容については後述する。 |

### 組み込み関数

営業・融資サポートシステムのCloudFormationテンプレートでは、保守性の低下が懸念される複雑な記法を極力避け、必要不可欠な組み込み関数以外は使用しないこととする。

使用する組み込み関数は、「ImportValue」と「Ref」のみとする。

### 論理ID

リソースセクション及び出力セクションで定義する論理IDの命名規則について以下に記載する。

リソースセクションでの論理IDについては、AWSリソースタイプ識別子の「data-type-name」+2桁の連番とする。

AWSリソースタイプ識別子は「service-provider::service-name::data-type-name」で表されるものであり、例としてEC2インスタンス(AWSリソースタイプ識別子「AWS::EC2::Instance」)の論理IDは「Instance01」となる。

出力セクションでの論理IDについては、エクスポート対象リソースの論理ID＋Outputとする。

### エクスポート名

出力セクションにてエクスポートする値の命名規則を以下に記載する。

エクスポートする値の名前は、スタック名＋出力セクションの論理IDとする。

## 各テンプレート仕様

各テンプレートにおけるインポート対象とエクスポート対象を以降に記載する。

なお、各テンプレートでリソースセクション内の記載も差異が生じるが、2.1.2 セクションに記載の通り別紙参照とする。

|  |  |  |
| --- | --- | --- |
| テンプレート | インポート | エクスポート |
| 全体テンプレート | 対象無し | ・フローログ用IAMロールArn  ・Web/APサーバ用IAMインスタンスプロファイルArn  ・バッチサーバ用IAMインスタンスプロファイルArn  ・AWS Backup用IAMロールArn  ・S3アクセスログ用S3バケットArn  ・SNSトピックArn |
| ネットワークテンプレート | ・フローログ用IAMロールArn  ・S3アクセスログ用S3バケットArn | ・ALB用サブネットID  ・Web/APサーバ用サブネットID  ・バッチサーバ用サブネットID  ・Aurora用サブネットID  ・Redis用サブネットID  ・ALB用セキュリティグループID  ・Web/APサーバ用セキュリティグループID  ・バッチサーバ用セキュリティグループID  ・Aurora用セキュリティグループID  ・Redis用セキュリティグループID  ・Lambda用セキュリティグループID |
| DBサーバテンプレート | ・AWS Backup用IAMロールArn  ・S3アクセスログ用S3バケットArn  ・SNSトピックArn  ・Aurora用サブネットID  ・Redis用サブネットID  ・Aurora用セキュリティグループID  ・Redis用セキュリティグループID  ・Lambda用セキュリティグループID | 対象無し |

|  |  |  |
| --- | --- | --- |
| テンプレート | インポート | エクスポート |
| Web/APサーバテンプレート | ・Web/APサーバ用IAMインスタンスプロファイルArn  ・AWS Backup用IAMロールArn  ・S3アクセスログ用S3バケットArn  ・SNSトピックArn  ・ALB用サブネットID  ・Web/APサーバ用サブネットID  ・ALB用セキュリティグループID  ・Web/APサーバセキュリティグループID | 対象無し |
| バッチサーバテンプレート | ・バッチサーバ用IAMインスタンスプロファイルArn  ・AWS Backup用IAMロールArn  ・S3アクセスログ用S3バケットArn  ・SNSトピックArn  ・バッチサーバ用サブネットID  ・バッチサーバ用セキュリティグループID | 対象無し |

以上