Configuration & Secret Management入門

AWS Black Belt Online Seminar

Amazon Web Services Japan K.K.
Solutions Architect
成尾 文秀

2021-September

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

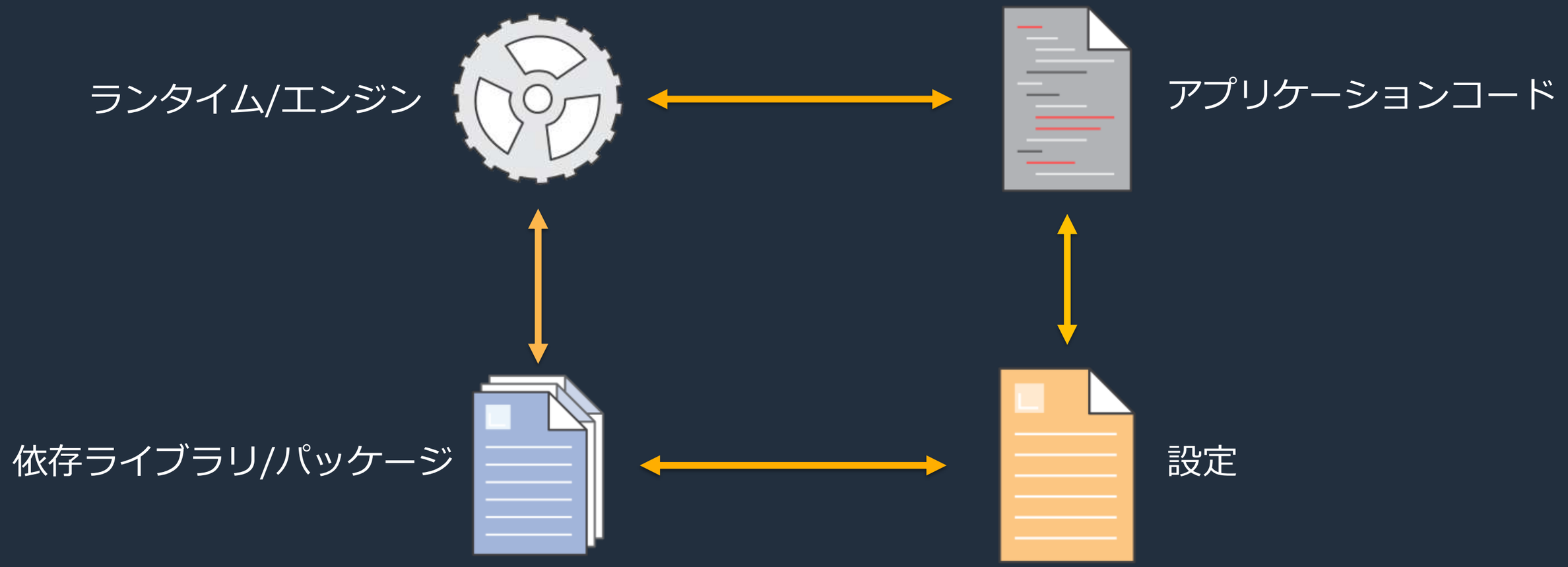
このセッションで扱うこと・学べること

- コンテナにおいてConfiguration (設定) をどのように扱うか
- AWSサービスを利用した変数の取り扱い

aws

環境変数 – アプリケーション

- アプリケーションを構成するコンポーネント



aws

環境変数 – 設定（アプリケーション）

- 設定
  - アプリケーションが稼働する上で必要となる動作環境ごとに異なる情報
  - 変更頻度が高い情報

- 設定例
  - RDBの接続先
  - 外部APIのエンドポイント
  - デバッグフラグ
  - 同時処理数、タイムアウト秒数

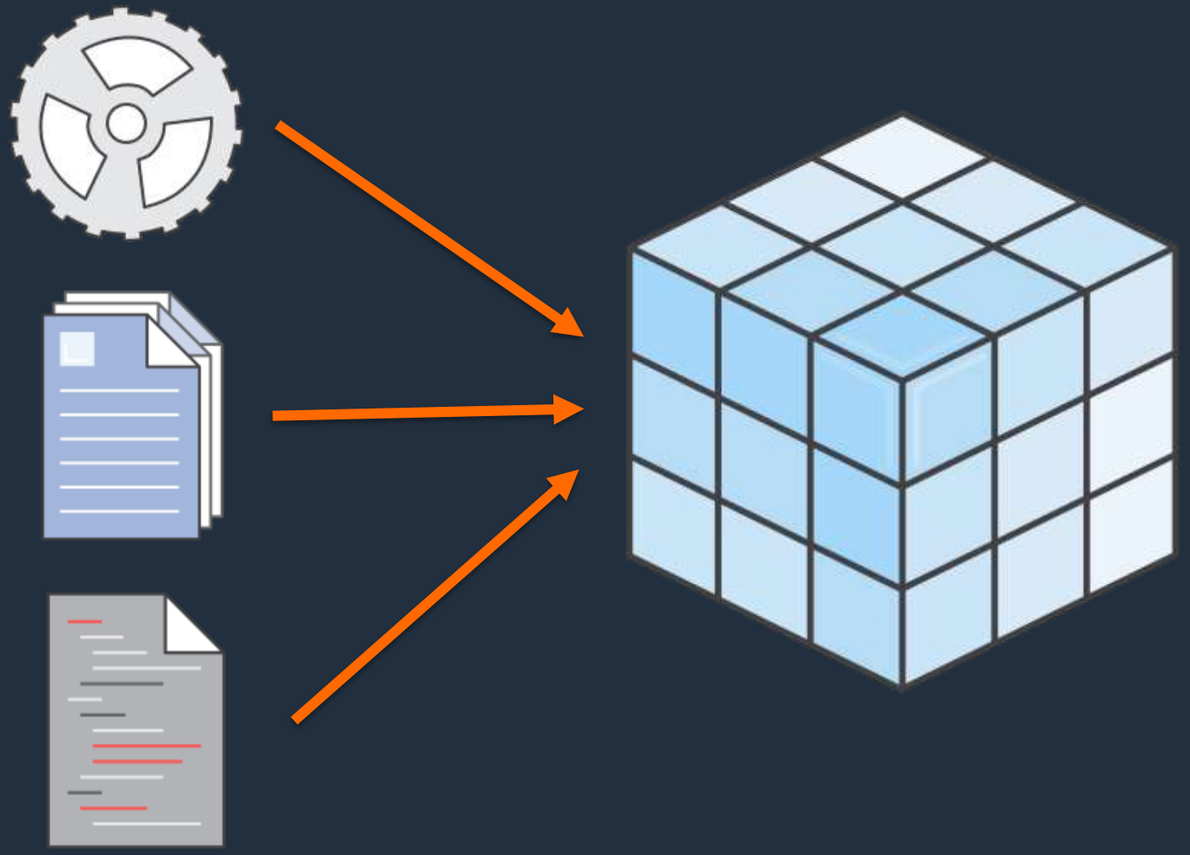
設定

- 設定をソースコードに含めた場合の影響
  - 変更の都度ビルド、テスト、デプロイ必要
  - ソースコード、コンテナイメージの流出といったセキュリティリスク

aws

環境変数 – コンテナ

- コンテナ



環境変数 – 設定（コンテナ）

- コンテナにおける設定
  - 環境変数として外部から渡す

- 読み込み例
  - 起動時にまとめて取得
  - アプリケーションから必要な時に都度取得

- AWSサービス
  - AWS Systems Manager - Parameter Store
  - AWS Secrets Manager
  - Amazon S3

aws

環境変数 – Parameter Store

Amazon ECS

- Amazon ECSでのParameter Store利用方法
  - タスク定義内のコンテナ定義 (containerDefinitions) の secrets で指定

```
"secrets": [{
  "name": "environment_variable_name",
  "valueFrom": "arn:aws:ssm:region:aws_account_id:parameter/parameter_name"
}]
```

  - タスク定義内のログ設定 (logConfiguration) の secretOptions で指定

```
"secretOptions": [{
  "name": "fluentd-address",
  "valueFrom": "arn:aws:ssm:region:aws_account_id:parameter:parameter_name"
}]
```

- 注意点
  - タスク起動時に環境変数として読み込む、更新した値を読む時は新しいタスクを起動
  - 大量取得がある際はスループットに注意（デフォルト：40 TPS、上限：1,000 TPS）

aws

環境変数 – Secrets Manager

Amazon ECS

- Amazon ECSでのSecrets Manager利用方法
  - タスク定義内のコンテナ定義 (containerDefinitions) の secrets で指定
  - タスク定義内のログ設定 (logConfiguration) の secretOptions で指定
  - 特定の JSON キーなど柔軟な指定が可能 (EC2 or Fargate PV 1.40以降)

```
arn:aws:secretsmanager:region:aws_account_id:secret:secret-name:json-key:version-stage:version-id
```

    - json-key：指定すると特定のKeyのみ取得、指定がないとシークレットの内容全体を取得
    - version-stage：AWSCURRENT（現在の値）AWSPREVIOUS （1つ前の値）を指定し取得
    - version-id：自動付与されるバージョンIDを指定して特定のデータを取得

- 注意点
  - タスク起動時に環境変数として読み込む、更新した値を読む時は新しいタスクを起動
  - 大量取得がある際は秒間取得上限に注意（GetSecretValue：5,000 per second 固定）

aws

環境変数 – Amazon S3

Amazon ECS

- Amazon ECSでのAmazon S3ファイルからの利用方法（EC2 起動タイプのみ）
  - タスク定義内の environment で個別にパラメータをセット
  - タスク定義内の environmentFiles の secrets で S3 を指定可能 (EC2 or Fargate PV 1.40以降)

```
"environmentFiles": [
    {
        "value": "arn:aws:s3:::s3_bucket_name/envfile_object_name.env",
        "type": "s3"
    }
```

- 注意点
  - タスク起動時に環境変数として読み込む、更新した値を読む時は新しいタスクを起動
  - タスク定義ごとに最大 10 個のファイルが指定可能

aws

環境変数 – Secrets Manager & Parameter Store

Amazon EKS

- Amazon EKSでのSecrets Manager利用方法
  - AWS Secrets and Configuration Provider (ASCP) for Kubernetes Secrets Store CSI Driver
    - 指定のmountPathにシークレットを取得して配置
    - Kubernetes Secretと同期

```
  volumeMounts:
  - name: mysecret2
    mountPath: "/mnt/secrets-store"
    readOnly: true
volumes:
  - name: mysecret2
    csi:
      driver: secrets-store.csi.k8s.io
      readOnly: true
      volumeAttributes:
        secretProviderClass: "aws-secrets"
```

```
apiVersion: secrets-store.csi.x-k8s.io/v1alpha1
kind: SecretProviderClass
metadata:
  name: aws-secrets
spec:
  provider: aws
  secretObjects:
  - data:
  - key: username
    objectName: ACSPSecrets
  secretName: ACSPEKSSecret
  type: Opaque

  parameters:
    objects: |
      array:
        - |
          objectName: "arn:aws:ssm:us-east-1:[ACCOUNT]:parameter/MyConfigValue"
          objectVersion: "1"# [オプション] オブジェクトバージョン、空の場合は最新がデフォルト
        - |
          objectName: "arn:aws:secretsmanager:us-east-1:[ACCOUNT]:secret:MySecret-00AABB"
          objectVersion: "00112233AABB00112233445566778899"
        - |
          objectName: "MyConfigValue2"
          objectType: "ssmparameter"# オブジェクトタイプ、シークレットには secretsmanager、コン
          objectVersion: "1"
        - |
          objectName: "MySecret2"
          objectType: "secretsmanager"
          objectVersion: "00112233AABB00112233445566778899"
```


aws

このセッションで扱ったこと

- コンテナにおいてConfiguration (設定) をどのように扱うか
- AWSサービスを利用した変数の取り扱い

aws

Link

- Systems Manager パラメータストアを使用した機密データの指定 - Amazon ECS
  https://docs.aws.amazon.com/ja_jp/AmazonECS/latest/userguide/specifying-sensitive-data-parameters.html
- Parameter Store のスループットを引き上げる - AWS Systems Manager
  https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/parameter-store-throughput.html
- Secrets Manager を使用した機密データの指定 - Amazon Elastic Container Service
  https://docs.aws.amazon.com/ja_jp/AmazonECS/latest/developerguide/specifying-sensitive-data-secrets.html
- AWS Secrets Manager のクォータ - AWS Secrets Manager
  https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/reference_limits.html
- 環境変数の指定 - Amazon Elastic Container Service
  https://docs.aws.amazon.com/ja_jp/AmazonECS/latest/developerguide/taskdef-envfiles.html
- Using Secrets Manager secrets in Amazon Elastic Kubernetes Service
  https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/integrating_csi_driver.html
- AWS Secrets & Configuration Provider を Kubernetes Secrets Store CSI Driver で使用する方法 | Amazon Web Services ブログ
  https://aws.amazon.com/jp/blogs/news/how-to-use-aws-secrets-configuration-provider-with-kubernetes-secrets-store-csi-driver/

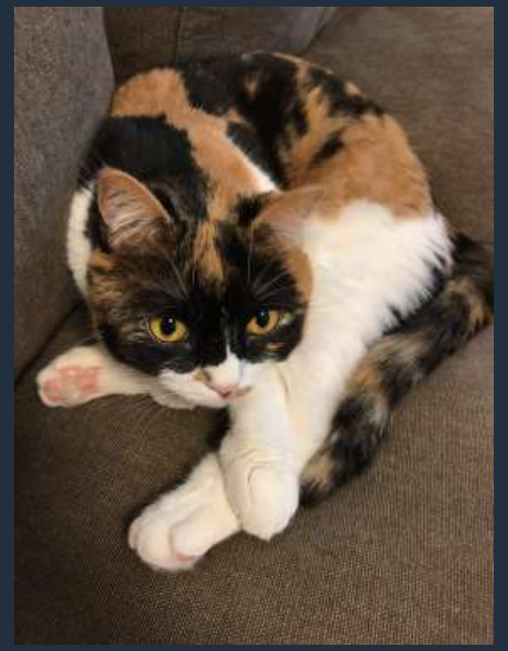
aws

本セッションの担当： 成尾 文秀

- 所属：
  アマゾン ウェブ サービスジャパン株式会社
  ソリューションアーキテクト

- 好きなAWSサービス：
  - Amazon ECS, Amazon EKS, Amazon S3

- 趣味：
  - ねこ、旅行



aws

AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分け、アマゾン ウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

- AWSの技術担当者が、AWSの各サービスについてテーマごとに動画を公開します
- お好きな時間、お好きな場所でご受講いただけるオンデマンド形式です
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます

aws

内容についての注意点

- 本資料では2021年6月時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(http://aws.amazon.com)にてご確認ください。

- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。

- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます。

- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

本資料に関するお問い合わせ・ご感想

- 技術的な内容に関しましては、有料のAWSサポート窓口へお問い合わせください
- https://aws.amazon.com/jp/premiumsupport/

- 料金面でのお問い合わせに関しましては、カスタマーサポート窓口へお問い合わせください（マネジメントコンソールへのログインが必要です）
- https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service

- 具体的な案件に対する構成相談は、後述する個別技術相談会をご活用ください

ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

AWS の日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

AWS のハンズオン資料の場所「AWS ハンズオン」で検索

https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/

AWS Well-Architected 個別技術相談会

毎週”W-A個別技術相談会”を実施中

- **AWSのソリューションアーキテクト(SA)に対策などを相談することも可能**
- **申込みはイベント告知サイトから**

(https://aws.amazon.com/jp/about-aws/events/)

AWS イベント で[検索]

ご視聴ありがとうございました