

# コスト超過を回避せよ

コストインシデントは対岸の火事じゃない！

2021年10月7日  
株式会社オープトーン  
観光ビッグデータ事業部  
根本賢一郎

# アジェンダ

- 自己紹介
- 要件
- 作業内容とインシデント
- 原因と対策

# 自己紹介

- 株式会社オープントーン
  - 観光ビッグデータ事業部
    - 根本賢一郎
      - Javaのアプリケーションエンジニア
      - メールシステムインフラエンジニア
      - クラウドエンジニア

# 要件

- DBインスタンス (EC2) のボリューム縮小によるコスト削減

	現環境	新環境
インスタンスタイプ	r4.xlarge	r4.xlarge
ボリュームタイプ	io1	io1
IOPS	15,000	15,000
ボリュームサイズ	3,000GiB	1,500GiB

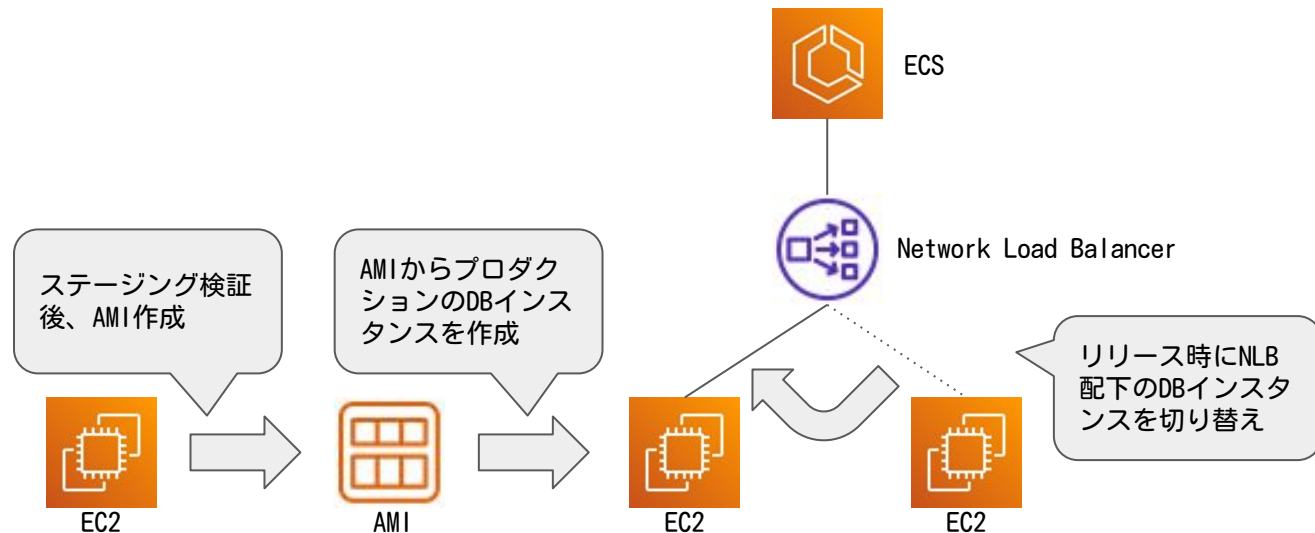


インスタンスコスト	1 インスタンス x 0.32 USD x 730 1 か月あたりの時間数 = 233.60 USD	1 インスタンス x 0.32 USD x 730 1 か月あたりの時間数 = 233.60 USD
EBS ストレージコスト	3,000 GB x 0.142 USD x 1 インスタンス = 426.00 USD	1,500 GB x 0.142 USD x 1 インスタンス = 213.00 USD
EBS IOPSコスト	15,000 IOPS x 0.074 USD x 1 インスタンス = 1,110.00 USD	15,000 IOPS x 0.074 USD x 1 インスタンス = 1,110.00 USD
Total	<b>1,769.60 USD</b>	<b>1,556.60 USD</b>

↓ 213.00 USD

# 作業内容

- ボリュームサイズを変更しステージングで検証
- 検証済みインスタンスのスナップショット（AMI）を作成
- AMIからプロダクションのインスタンスを構築



# 作業内容

- ステージングとプロダクションの差分

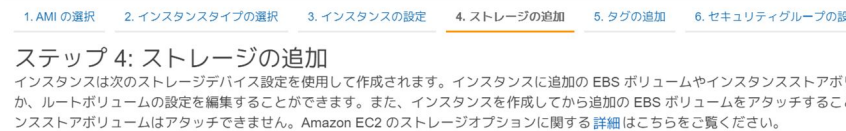
	ステージング	プロダクション
インスタンスタイプ	t2.large	r4.xlarge
ボリュームタイプ	gp3	io1
ボリュームサイズ	1,500GiB	1,500GiB

※DBインスタンス起動時に、ボリュームタイプの変更を行う。

# インシデント発生

- ストレージの追加

ボリュームタイプをio1に変更すると、ボリュームサイズからIOPS値を自動計算し、再設定する。



インスタンスコスト	1 インスタンス x 0.32 USD x 730 1 か月あたりの時間数 = 233.60 USD	1 インスタンス x 0.32 USD x 730 1 か月あたりの時間数 = 233.60 USD
EBS ストレージコスト	3,000 GB x 0.142 USD x 1 インスタンス = 426.00 USD	1,500 GB x 0.142 USD x 1 インスタンス = 213.00 USD
EBS IOPSコスト	15,000 IOPS x 0.074 USD x 1 インスタンス = 1,110.00 USD	64,000 IOPS x 0.074 USD x 1 インスタンス = 4,736.00 USD
Total	<b>1,769.60 USD</b>	<b>5,182.60 USD</b>

**↑ 3,413 USD**

# 原因

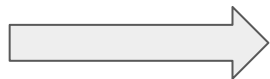
- ボリュームの設定ミス
  - リリースのシナリオ作成とレビュー実施の不備
  - バディによるリリース時のチェック体制の不備
    - レビュー・チェック体制を強化？
- インシデントの発見遅れ
  - リリースのタイミングによる発見の遅れ
    - 請求メールのチェック方法の見直し？



# 対策① ヒューマンエラーを回避

- Cfnテンプレートを利用したインスタンスの構築

Parameter  
Env  
マシンイメージID  
サブネット  
セキュリティグループ  
キーペア



CloudFormation



EC2

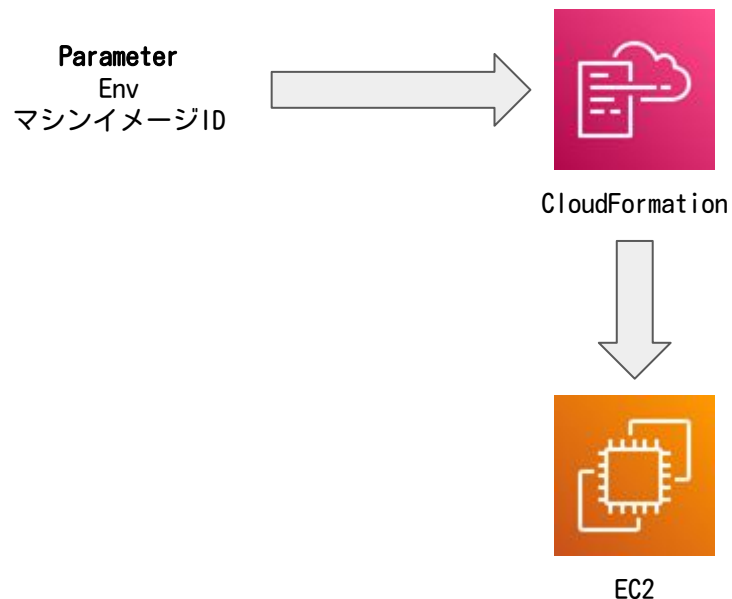
```
Mappings:
  EnvMap:
    Production:
      InstanceType: r4.xlarge
      VolumeType: io1
      Iops: 15000
    Staging:
      InstanceType: t2.large
      VolumeType: gp3
      Iops: 3000

Resources:
  Instance:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref ImageId
      InstanceType: !FindInMap [EnvMap, !Ref Env, InstanceType]
```

※テンプレート一部抜粋

# 対策① ヒューマンエラーを回避

- Cfnテンプレートを利用したインスタンスの構築（よりミス防止）

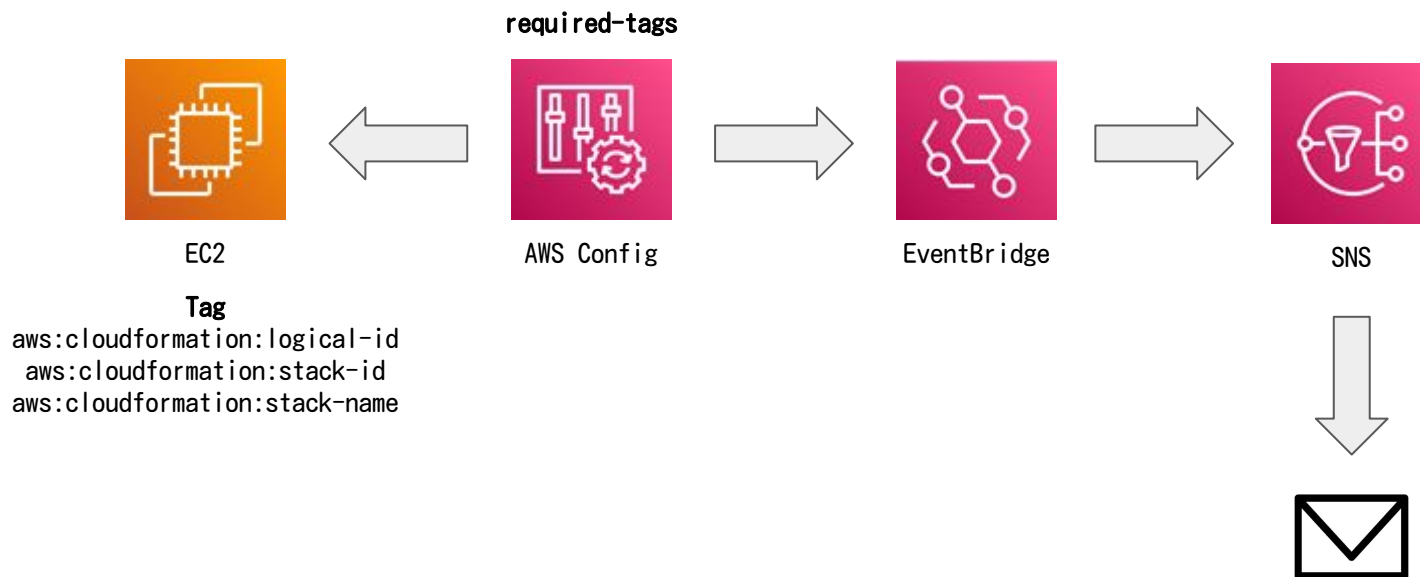


```
Mappings:
EnvMap:
  Production:
    InstanceType: r4.xlarge
    VolumeType: io1
    Iops: 15000
    SubnetId: subnet-12345678
    KeyName: key-name
    SecurityGroupIds:
      - sg-01234567
      - sg-89012345
```

※テンプレート一部抜粋

# 対策① ヒューマンエラーを回避

- AWS ConfigによるEC2インスタンスの監視



<https://console.aws.amazon.com/cloudformation/home?region=ap-northeast-1#/stacks/create/review?stackName=aws-config-required-tags&templateURL=http://s3-ap-northeast-1.amazonaws.com/ot-nemoto.aws-cloudformation-templates/aws-config/required-tags/template.yaml>

# 対策① ヒューマンエラーを回避

- AWS ConfigによるCfnドリフト検出の監視

cloudformation-stack-drift-detection-check



CloudFormation



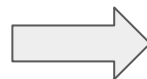
ドリフト検出



AWS Config



EventBridge



SNS



## 注意点

Cfnテンプレートのインスタンスを起動テンプレートから立ち上げる場合に、インスタンスの変更をドリフト検出出来ない。

```
Resources:          ※テンプレート一部抜粋
  Instance:
    Type: AWS::EC2::Instance
    Properties:
      LaunchTemplate:
        LaunchTemplateId: !Ref LaunchTemplate
        Version: 1
  LaunchTemplate:
    Type: AWS::EC2::LaunchTemplate
```

<https://console.aws.amazon.com/cloudformation/home?region=ap-northeast-1#/stacks/create/review?stackName=aws-config-cloudformation-stack-drift-detection-check&templateURL=https://s3-ap-northeast-1.amazonaws.com/ot-nemoto.aws-cloudformation-templates/aws-config/cloudformation-stack-drift-detection-check/template.yaml>

## 対策②障害の早期発見による軽減

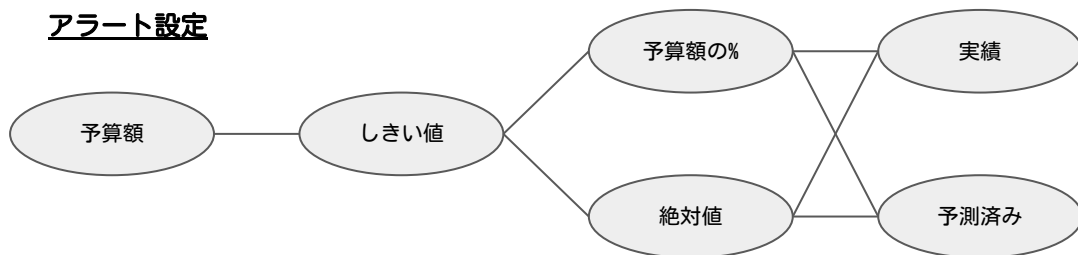
- AWS Budgetsによるコストアラートの設定



AWS Budgets



### アラート設定



\$1,000

95

予算額の%

実績



実績がしきい値 (\$950)を超えた場合にアラート

### 注意点

アラートの条件を余裕をもって設定すると、毎回アラートが出るため、オオカミ少年アラートになることを注意。

### 注意点

請求代行を利用している場合、EC2インスタンスやECSは、Savings Plansになっている可能性が高く、また独自の割引が適用されると思われる。請求代行側で提供しているアラートサービスがあれば、そちらを推奨。

# 最後に

- 正解ではない。よりいい方法は必ずある
- コスト管理に関するリスクを完全回避は不可
- 但し、個別にリスクを回避、軽減する方法・サービスは提供されている
- 所感
  - ヒューマンエラーの対応に、人をでどうにかしようとしても一次的な回避にしかならない。たぶん。自動化（人じゃないチェック）を検討しよう。
  - アラートは本当にヤバそうな時。アラートが多すぎると意味をなさなくなるので、設定内容については十分検討しよう。

ご清聴ありがとうございました。