



生成系 AI × コンプライアンス！

エージェントにおすすめの AWS Config マネージドルールを有効化してもらおう

北川友稀 (Kitagawa Yuki)

Solutions Architect ISV/SaaS

自己紹介

- 名前
 - 北川友稀 (Yuki Kitagawa)
- 所属
 - ISV/SaaS Solutions Architect
- 好きなAWSサービス
 - AWS Lambda、AWS Config
- 趣味
 - カラオケ、ゲーム



本日のゴール

- Amazon Bedrock の概要を理解している状態
- Agents for Amazon Bedrock と Knowledge Base for Amazon Bedrock で何ができるのかイメージが湧いている状態

アジェンダ

- AWS Config Managed Rules の課題
- Amazon Bedrock とは
- Knowledge Base for Amazon Bedrock とは
- Agents for Amazon Bedrock とは
- デモ
- まとめ



AWS Config Managed Rules の課題

AWS Config Managed Rules^(※) の課題

- 350 以上のルールがあって、何を選べばよいか分からない
- 防ぎたいリスク（例：情報漏洩）は明確なんだけど、どのルールが適切なの？



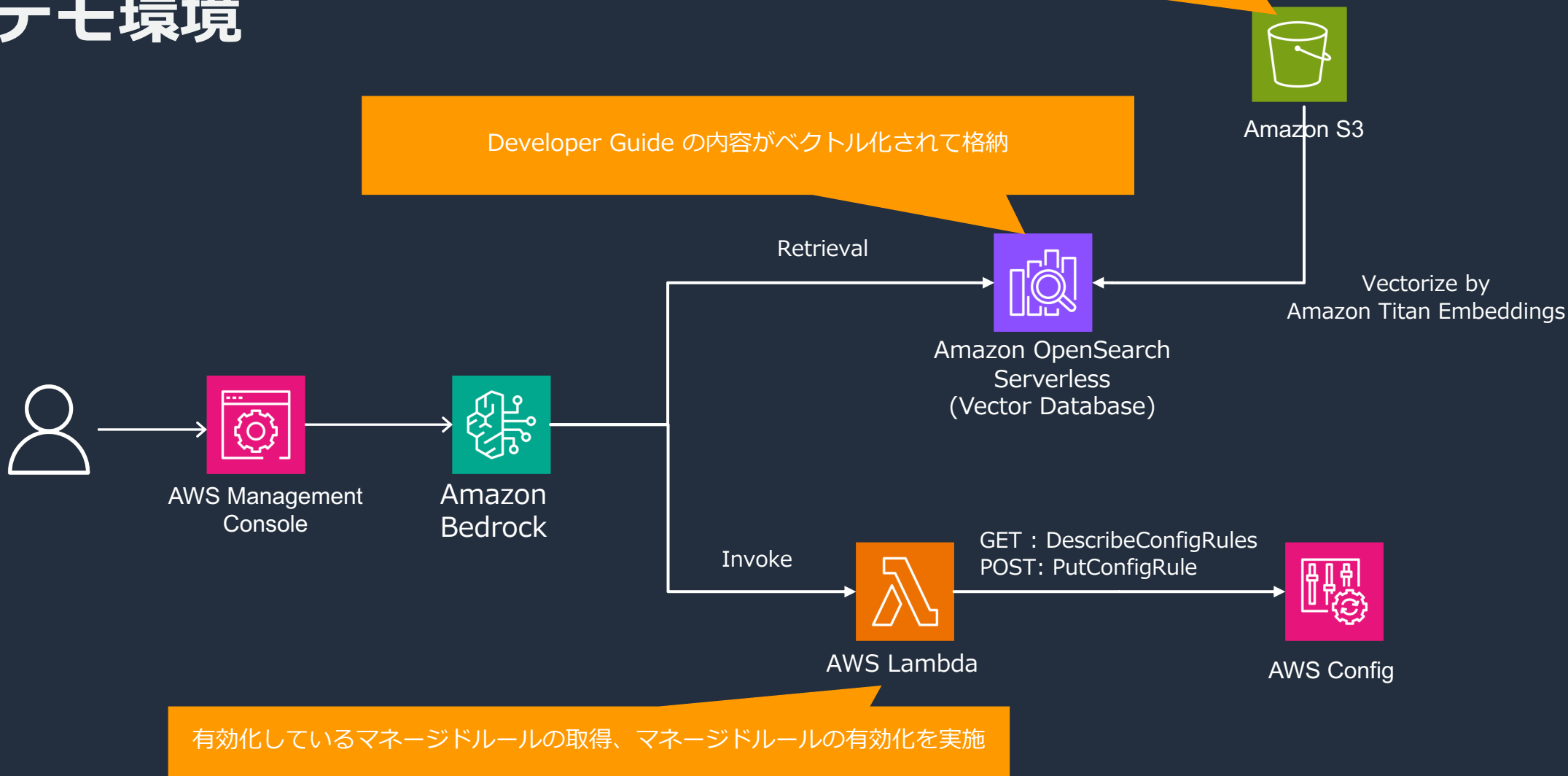
Knowledge Base for Amazon Bedrock と Agents for Amazon Bedrock
による解決を試みる

※ AWS Config の機能であり、あるリソースのコンプライアンス準拠状況を評価する
AWS が提供しているルールが Managed Rules、お客様が独自で作成するルールが Custom Rules と呼ばれる

評価例：Amazon Simple Storage Service (Amazon S3) のパブリックアクセスブロック設定が有効かどうか
Amazon Elastic Block Store (Amazon EBS) が暗号化されているかどうか

デモ環境

AWS Config の Developer Guide の PDF (4.6MB 約 190p) を配置
(マネージドルールの一覧を抽出)



Amazon Bedrock とは



Amazon Bedrock とは



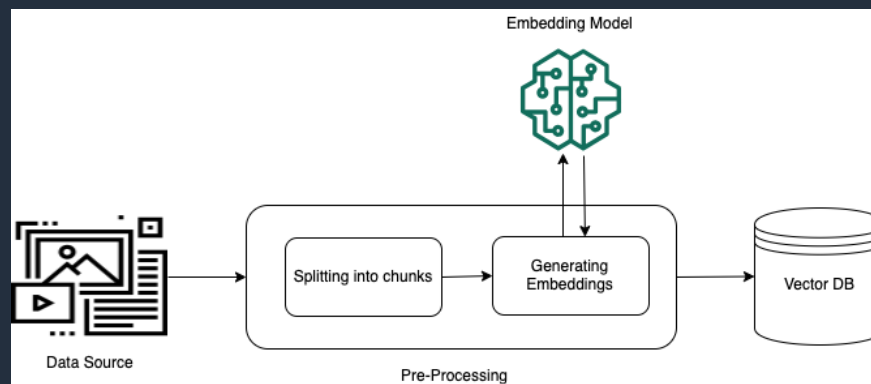
- 単一の API でさまざまな基盤モデルにアクセス可能
- 基盤モデルのファインチューニングをプライベートに実施
- セキュリティとコンプライアンスを実現
 - プライベートリンクによる閉域接続、コンテンツを 3rd party 含めて学習に利用しない
- 検索拡張生成（RAG）によるハルシネーションの抑止
- 複雑なビジネスタスクを実行するエージェントの構築

- 上記特徴をフルマネージドサービスで提供

Knowledge Base for Amazon Bedrock とは

Knowledge Base for Amazon Bedrock とは

- 基盤モデルとデータソースを組み合わせた拡張検索生成(RAG)をフルマネージドに実現
 - RAG はデータソースに格納された正しい情報を利用し、関連性が高く正確な応答を返すようにする手法。ハルシネーション（幻覚）を抑止する。
- Amazon S3 内に格納されたデータの場所を指定するだけで、ベクトル DB にデータをベクトル化し取り込むワークフローを実行



※ バージニアとオレゴンリージョンで一般利用開始

赤枠部分の話



AWS Config の Developer Guide の PDF (4.6MB 約 190p) を配置
(マネージドルールの一覧を抽出)

Developer Guide の内容がベクトル化されて格納



Amazon S3

Retrieval



Amazon OpenSearch Serverless (Vector Database)

Vectorize by Amazon Titan Embeddings



AWS Management Console



Amazon Bedrock

Invoke



AWS Lambda

GET : DescribeConfigRules
POST: PutConfigRule



AWS Config

有効化しているマネージドルールを取得、マネージドルールの有効化を実施



アプリケーションからは InvokeModel API ではなく RetrieveAndGenerate API により RAG を利用した LLM の応答が得られる (LLM の応答はなく、関連度のスコア等を取得するのみの Retrieve API も存在する)

Request

```
{
  "input": {
    "text": "AWS Config のおすすめルールを教えてください"
  },
  "retrieveAndGenerateConfiguration": {
    "knowledgeBaseConfiguration": {
      "knowledgeBaseId": "OAOJAZN96S",
      "modelArn": "arn:aws:bedrock:us-east-1::foundation-model/anthropic.claude-v2"
    },
    "type": "KNOWLEDGE_BASE"
  },
  // "sessionId": "" # 指定するとこれまでのやり取りに基づいた回答が可能
}
```



Response

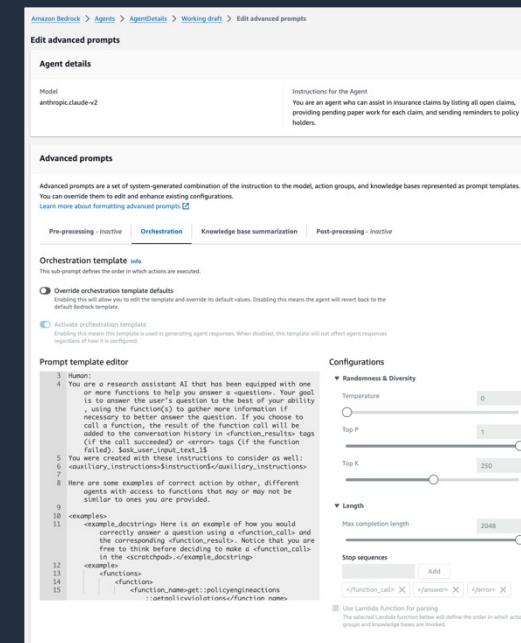
```
{
  "sessionId": "3f6000e4-00de-4493-b79a-50d770cdf589",
  "output": {
    "text": "AWS Config には、セキュリティ、コスト最適化、オペレーショナルエクセレンス、耐障害性などの分野で推奨される多数のマネージドルールがあります。...(snip) ..."
  },
  "citations": [
    {
      "generatedResponsePart": {
        "textResponsePart": {
          "text": "AWS Config には、セキュリティ、コスト最適化、オペレーショナルエクセレンス、耐障害性などの分野で推奨される多数のマネージドルールがあります。例えば、",
          "span": { "start": 0, "end": 78 }
        }
      },
      "retrievedReferences": [
        {
          "content": {
            "text": "resourceTypes, 型: 文字列 この Config ルールが適用されるリソースの範囲。"
          },
          "location": {
            "type": "S3",
            "s3Location": { "uri": "s3://xxx/config-managed-rule-list.pdf" }
          }
        }
      ]
    }
  ]
}
```



Agents for Amazon Bedrock とは

Agents for Amazon Bedrock とは

- 基盤モデルだけで完結しないタスクを実行することを容易にするフルマネージドサービス
 - 自然言語で指示を記述し、組織内の別システムへのアクセス方法を提供し、AWS Lambda 関数を定義することでエージェントを作成
 - エージェントはリクエストを分析。基盤モデルの推論能力を活用し、リクエスト完了までのステップを決定・実行する
 - データは全て暗号化



※ バージニアとオレゴンリージョンで一般利用開始

AWS Config の Developer Guide の PDF (4.6MB 約 190p) を配置
(マネージドルールの一覧を抽出)

赤枠部分の話 →

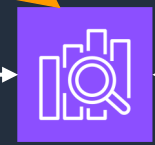


AWS Management Console

Amazon Bedrock

Developer Guide の内容がベクトル化されて格納

Retrieval



Amazon OpenSearch Serverless (Vector Database)



Amazon S3

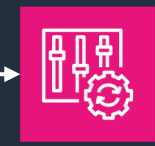
Vectorize by Amazon Titan Embeddings

Invoke



AWS Lambda

GET : DescribeConfigRules
POST: PutConfigRule



AWS Config

有効化しているマネージドルールを取得、マネージドルールの有効化を実施

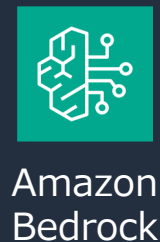


例) SaaS のコントロールプレーンを管理するエージェント

エージェントに「指示」と「タスクに必要な物の説明」を定義する

Instructions

あなたはフレンドリーで礼儀正しい SaaS のコントロールプレーンを管理するエージェントです。新規テナントの契約/解約時のお手伝いをしてください。まず、私に何をしたいのか聞いてください。次に...(snip)...



Knowledge Bases

説明：テナントの管理に関する情報をこちらから取得します。

Action Group 1

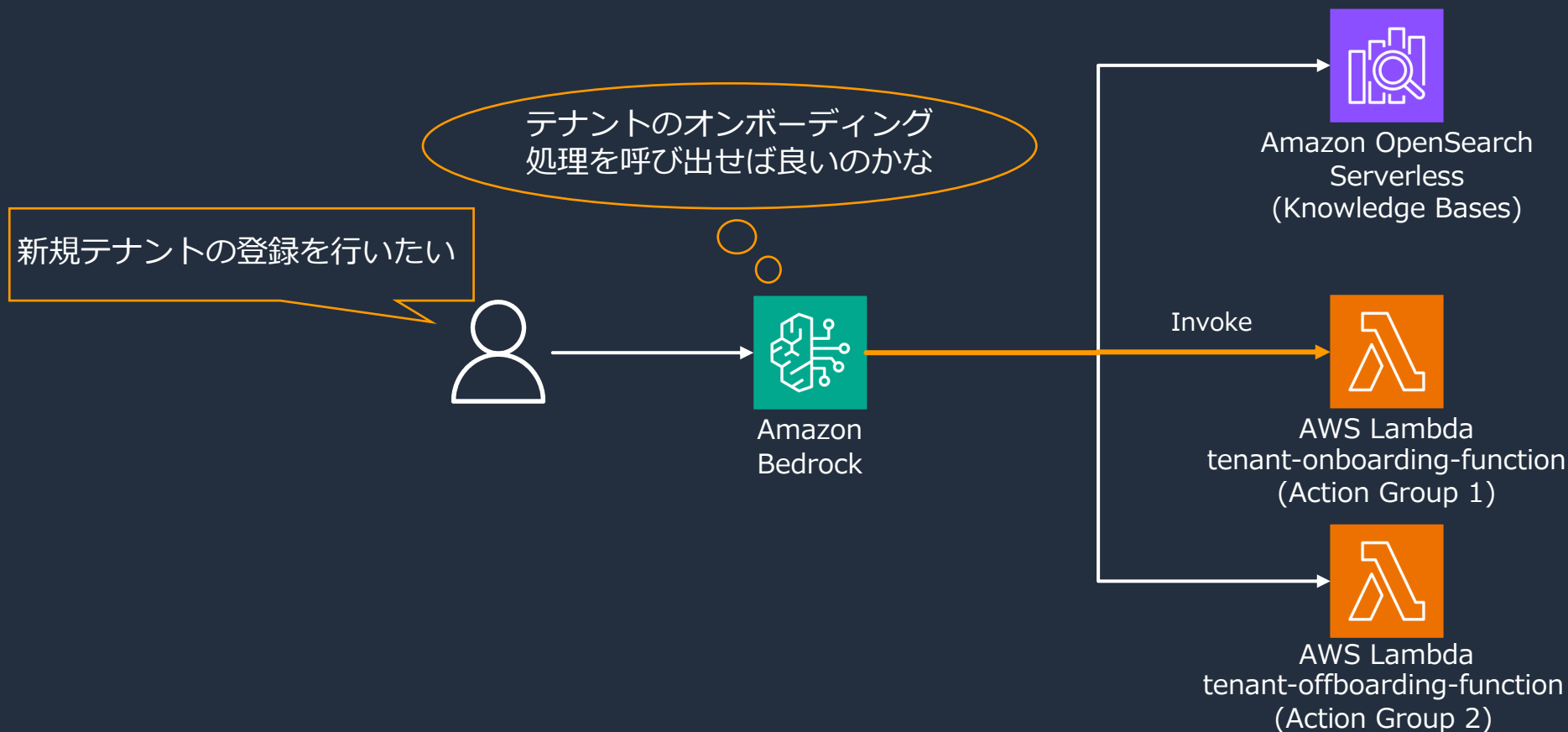
説明：新規テナントが**オンボーディング**する際にこのアクションを利用します。
Lambda関数：tenant-onboarding-function

Action Group 2

説明：新規テナントが**オフボーディング**する際にこのアクションを利用します。
Lambda関数：tenant-offboarding-function

例) SaaS のコントロールプレーンを管理するエージェント

エージェントはリクエストに基づいて自動的に必要な処理を推論して実行する



デモ



AWS Config Managed Rules^(※) の課題

- 350 以上のルールがあって、何を選べばよいか分からない
- 防ぎたいリスク（例：情報漏洩）は明確なんだけど、どのルールが適切なの？



Knowledge Base for Amazon Bedrock と Agents for Amazon Bedrock
による解決を試みる

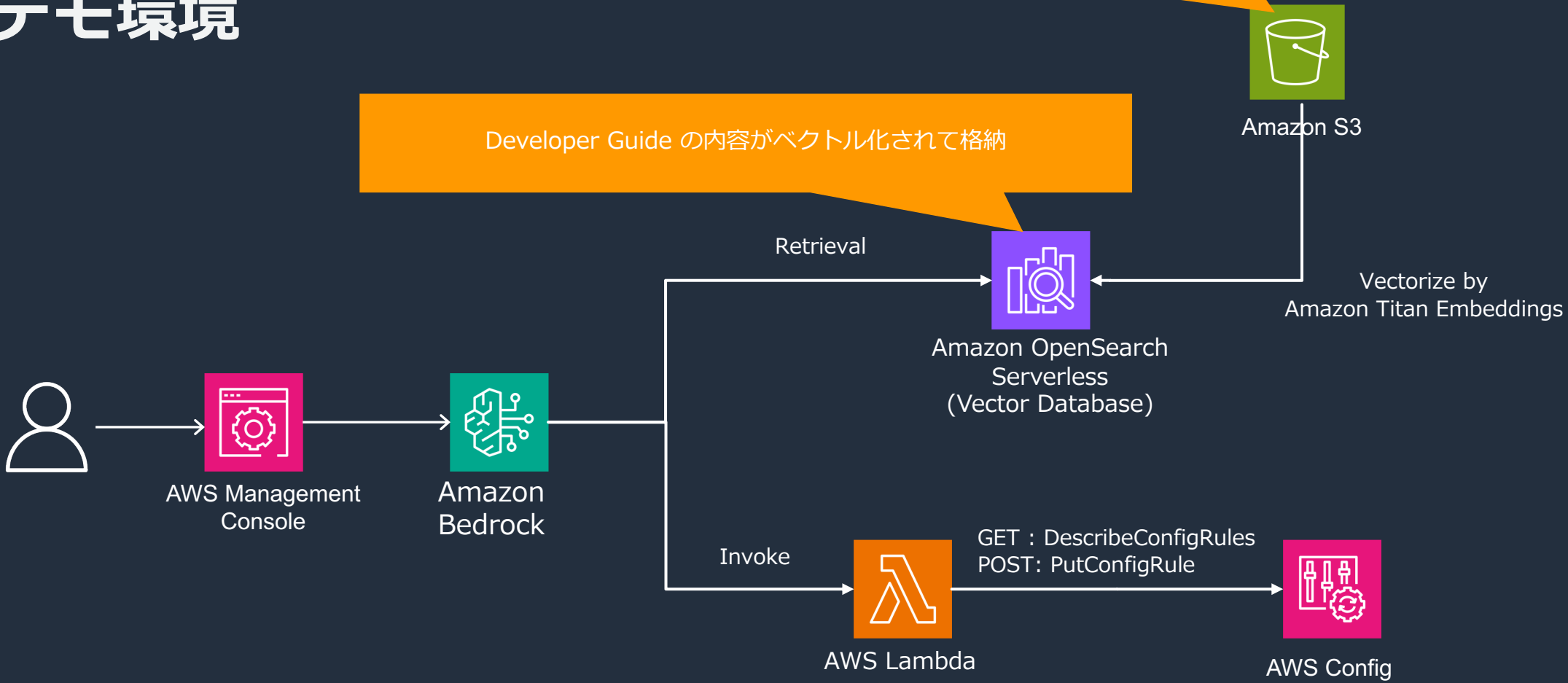
※ AWS Config の機能であり、あるリソースのコンプライアンス準拠状況を評価する
AWS が提供しているルールが Managed Rules、お客様が独自で作成するルールが Custom Rules と呼ばれる

評価例：Amazon Simple Storage Service (Amazon S3) のパブリックアクセスブロック設定が有効かどうか
Amazon Elastic Block Store (Amazon EBS) が暗号化されているかどうか

デモ環境

AWS Config の Developer Guide の PDF (4.6MB 約 190p) を配置
(マネージドルールの一覧を抽出)

Developer Guide の内容がベクトル化されて格納



有効化しているマネージドルールを取得、マネージドルールの有効化を実施

デモ内容



AWS Config のマネージドルールを有効化
したいです。Amazon S3 を利用しており、
情報漏洩が心配です。

Knowledge Base から判断すると以下の
ルールがおすすめです
...



Agent

Retrieval



Amazon OpenSearch
Service
(Knowledge Base)



~のルールを有効化してください

~のルールを有効化します



Agent

Invoke



AWS Lambda

デモの様子

有効化されているマネージドルールを教えてください



有効化されているマネージドルールは以下の通りです:
ACCESS_KEYS_ROTATED

[Show trace >](#)

AWS Config のマネージドルールを有効化したいです。



どのようなAWSサービスを利用していますか?また、どのようなリスクを防ぎたいですか?

[Show trace >](#)

Amazon S3 を利用しています。情報漏洩が心配です。



以下のマネージドルールを有効化しますか? -

S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED: サーバー側の暗号化を有効にすることで、オブジェクトデータを保護できるため、情報漏洩のリスクを軽減可能 -

S3_BUCKET_SSL_REQUESTS_ONLY: SSL を介したリクエストのみを受け付ける設定にすることで、通信内容の暗号化が可能となり、情報漏洩のリスクを軽減可能 -

S3_BUCKET_VERSIONING_ENABLED: バージョニングを有効にすることで、オブジェクトのすべてのバージョンを保持でき、意図しない上書きや削除から回復可能となるため、情報漏洩のリスクを軽減可能

お願いします



以下のマネージドルールを有効化しました: -

S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED -
S3_BUCKET_SSL_REQUESTS_ONLY -
S3_BUCKET_VERSIONING_ENABLED
これらの設定により、ご要望の情報漏洩リスクの軽減に役立つはずで

[Show trace >](#)

有効化しているマネージドルールを教えてください



有効化しているマネージドルールは以下の通りです: -
ACCESS_KEYS_ROTATED -
S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED -
S3_BUCKET_SSL_REQUESTS_ONLY -
S3_BUCKET_VERSIONING_ENABLED

[Show trace >](#)

※ デモ内でエージェントが提示する情報はあくまで参考としてください

デモで利用したプロンプト（参考）

あなたはお客様の AWS Config のマネージドルールを有効化する手助けをする日本語のみを話すエージェントです。以下の `<processes></processes>` XML タグで囲まれた手順どおりにお客様の手助けを行ってください。

`<processes>`

1. まずは、お客様に利用している AWS サービスと防ぎたいリスクを同時に質問します。
2. 次に、その回答を元に Knowledge Base から有効化すべきマネージドルールを取得し、お客様に「マネージドルールの識別子（例：EC2_INSTANCE_NO_PUBLIC_IP）」、「有効化するとなぜそのリスクを軽減できるのか」の2つの情報を `<example></example>` XML タグ内の形式で必ず提示した上で、最後に「これらのルールを有効化しますか？」とお客様へ確認してください。

`<example>`

- EC2_INSTANCE_NO_PUBLIC_IP: ~をすることで、~のため、~のリスクを軽減可能
- S3_BUCKET_SSL_REQUESTS_ONLY: ~をすることで、~のため、~のリスクを軽減可能

`</example>`

3. お客様への確認結果から、その名前と識別子を元にマネージドルールの有効化を行います。お客様からの確認が完了しない限りマネージドルールの有効化は行いません。

`</processes>`

ただし、お客様から有効化しているマネージドルールについて聞かれた場合は、有効化しているマネージドルールを確認し、お客様へお伝えしてください。

まとめ



まとめ

- **Amazon Bedrock** は、さまざまな基盤モデルを単一の API で呼び出し可能なセキュアでサーバレスなサービス
- **Knowledge Bases for Amazon Bedrock** は、基盤モデルとデータソースを組み合わせた拡張検索生成(RAG)をフルマネージドに実現
- **Agents for Amazon Bedrock** は、基盤モデルだけで完結しないタスクの実行を実現



Thank you!