課題演習 No.2

（WAF+CloudFront+S3+動的コンテンツ）

課題演習2（WAF+CloudFront+S3+動的コンテンツ）

目的：

ある会社では世界中のユーザーに対してweb翻訳サイトをリリース
しようと計画中です。アクセスは世界中から来るので、
遅延なく低レイテンシ―かつセキュアな配信したいと考えております。
またAWSを使用した構築環境では、webの静的サイトと動的サイト
（アプリケーション部分）の両方をサーバレスで実現したいとも考えています。
翻訳のためのアプリケーションは開発部署で作成されたものを使用し、
アプリケーションへの悪意ある攻撃に対してはセキュリティ保護を実装していきたいと考えています。

1：要件

■以下の要件でインフラを構築してください。

1. 世界中のユーザーへ低レイテンシ —な配信環境で最高のエクスペリエンスを提供できるようにしたい。

2. 1の環境へのアクセスは HTTPSになるよう、セキュアなリクエスト受信をできるようにしたい。

3. ユーザーに表示させる静的コンテンツをマネージドサービスを利用したサーバレス環境で展開したい。
   またセキュリティを考慮してオリジンページは世界に公開されないようにしたい。

4. 1で作成した環境に動的コンテンツも設定し、APIを使用したアプリケーションと連動できるようにする。
   アプリケーションは開発部署で作成されたコードを使用して動作するようにする。
   （ヒント:アプリの権限(ロール)にTranslateReadOnlyを付与する）

5. アプリケーションを対象にした悪意のある攻撃から保護できる環境にしたい。
   （※実際に攻撃をして検証しなくて OKです）

6. 上記の環境で構築し、webページの閲覧とアプリケーションが動作し、翻訳コンテンツが
   問題無く動くことを確認する。

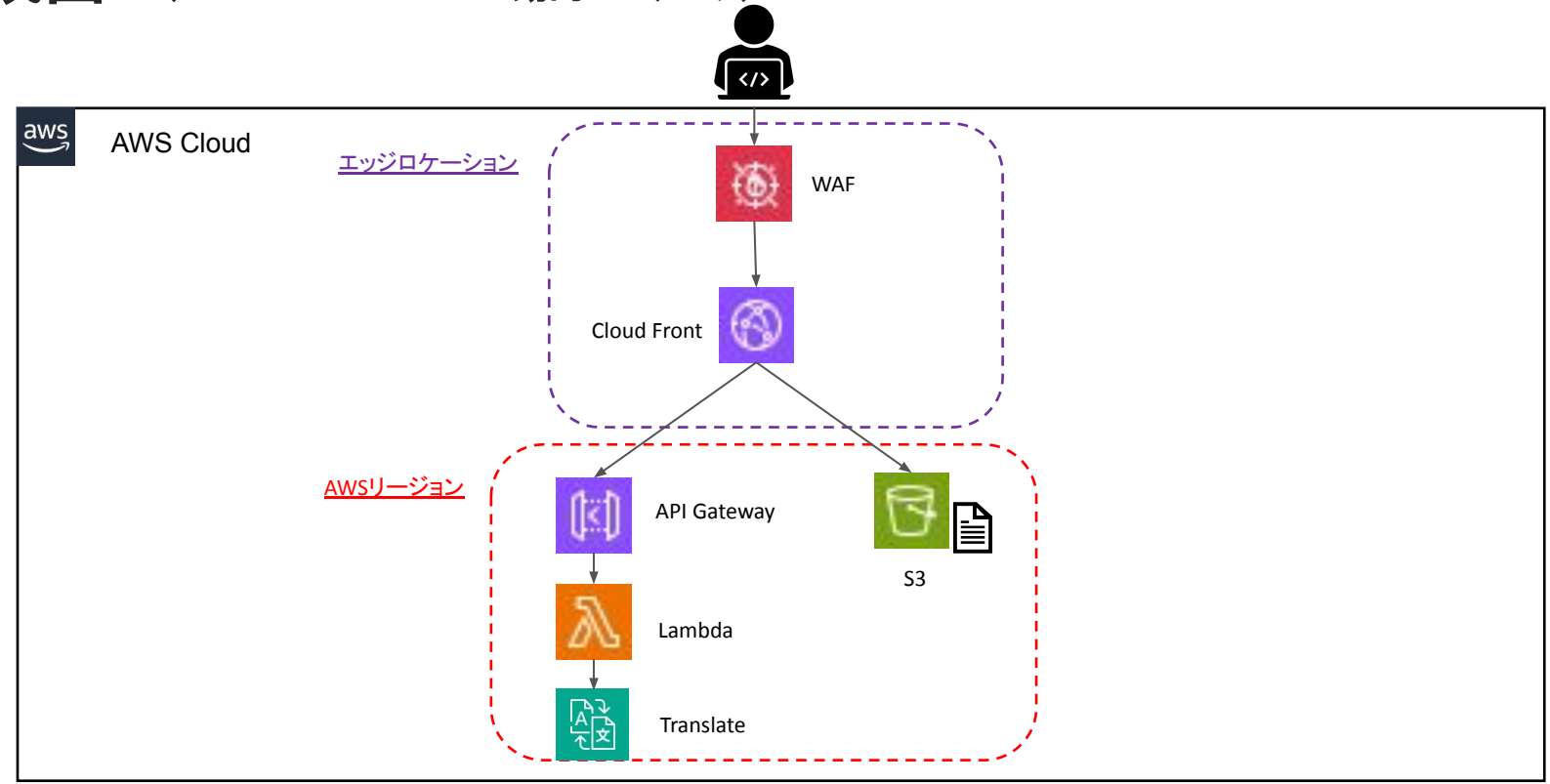
2：設計

■要件に対しての仕様(解決策)

No	要件	仕様(解決策)
1	世界中のユーザーへ低レイテンシ ―な配信環境で最高のエクスペリエンスを提供できるようにしたい。	CloudFrontの設定をして、世界中のエッジロケーションからコンテンツを配信。
2	ユーザーに表示させる静的コンテンツをマネージドサービスを利用したサーバレス環境で展開したい。またセキュリティを考慮してオリジンページは世界に公開されないようにしたい。	CloudFront経由でHTTPSリクエストのみ許可。CloudFrontのオリジンにS3バケットを配置してバケット内に静的コンテンツ格納。OACを設定して、CloudFront経由のみS3へアクセス可能にする。S3バケットはパブリックアクセス不可。
3	1で作成した環境に動的コンテンツも設定し、 APIを使用したアプリケーションと連動できるようにする。アプリケーションは開発部署で作成されたコードを使用して動作するようにする。	CloudFrontのオリジンにAPI Gatewayを構築。API Gatewayの背後にLambdaを設定。アプリのロールにTranslateReadOnlyを付与。
5	アプリケーションを対象にした悪意のある攻撃から保護できる環境にしたい。	CloudFront設定時にWAFを同時に設定。
6	上記の環境で構築し、webページの閲覧とアプリケーションが動作し、翻訳コンテンツが問題無く動くことを確認する。	Webブラウザで HTTPSアクセスし、静的コンテンツが正常に表示されるか確認。API Gatewayのエンドポイントへアプリからリクエストを送信し、期待通りのレスポンスが得られるか確認。

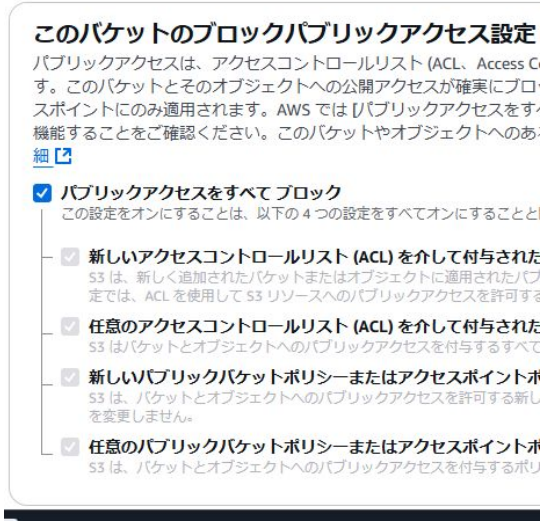
2：設計

ー構成図ー（WAF+CloudFront+S3+動的コンテンツ）



3：構築（実装）

①S3をパブリックアクセスを全てブロックしてセキュアに作成
作成したバケット内に静的コンテンツを格納
※CloudFrontのオリジンとして作成

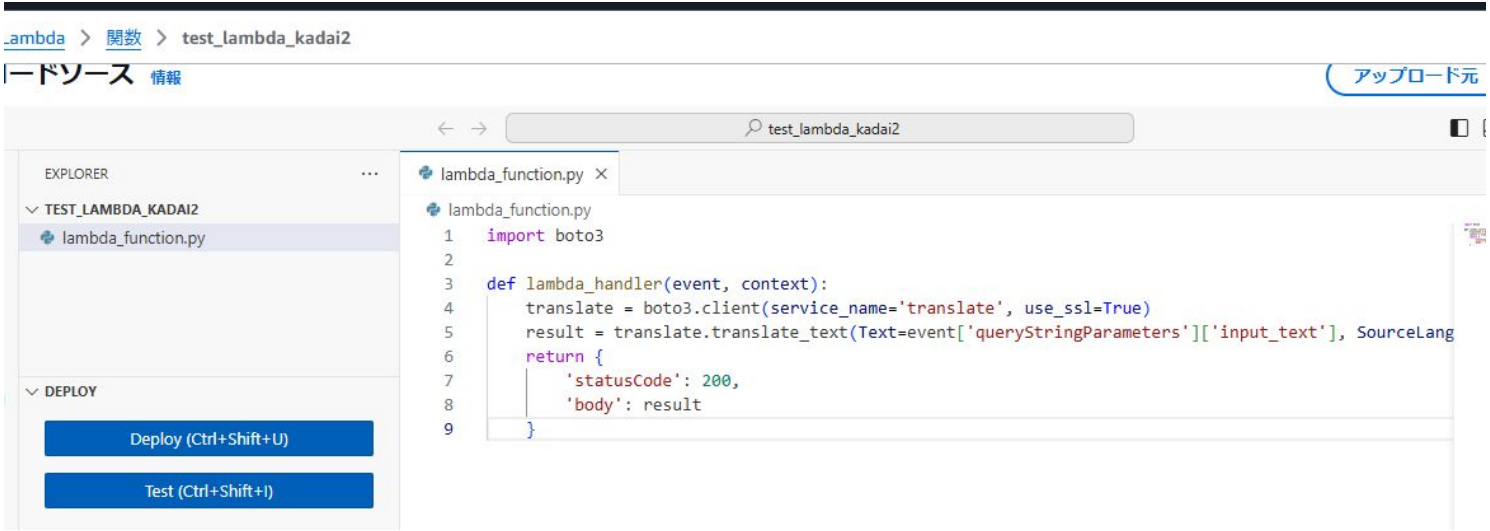


3：構築（実装）

②翻訳コンテンツを作成のためLambdaを起動

3：構築（実装）

②翻訳コンテンツ用のPythonコードをDeploy



3：構築（実装）

②作成したLambdaのIAMロールにTranslateReadOnlyのポリシーを
アタッチ

3：構築（実装）

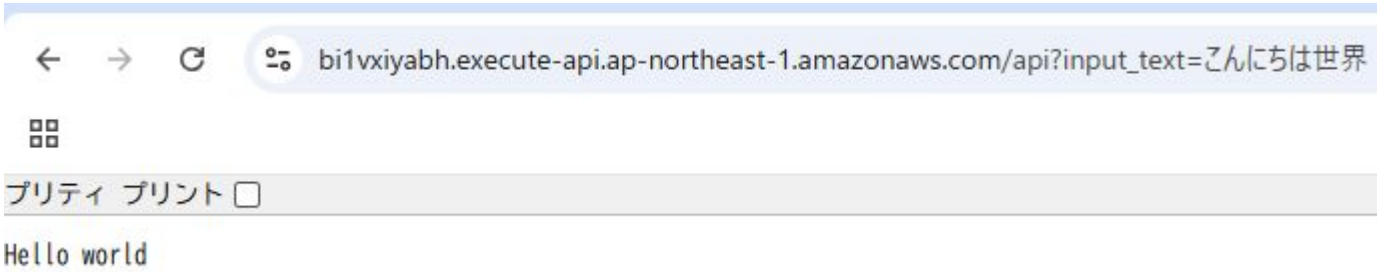
③APIGatewayをRest APIでメソッドタイプGET、Lambda関数、
プロキシ統合でアプリのLambdaを指定して作成

3：構築（実装）

③APIGatewayの作成時の補足でクエリ文字列をinput_textで指定
　ステージ名をapiで作成

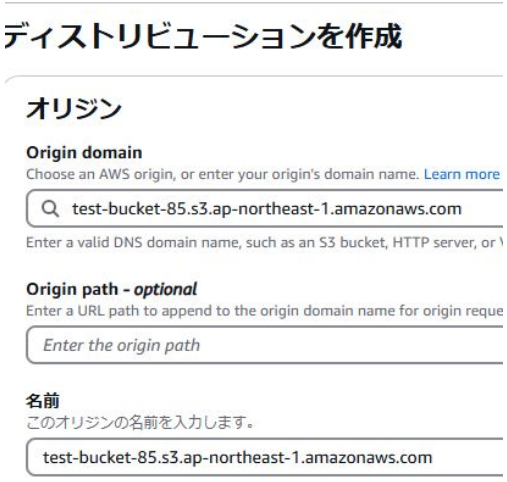
3：構築（実装）

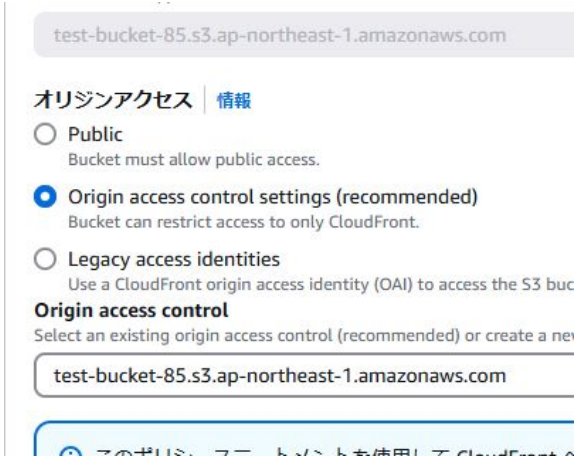
③APIGateway作成時に作成したLambdaを指定し、Lambdaのトリガーとして設定



3：構築（実装）

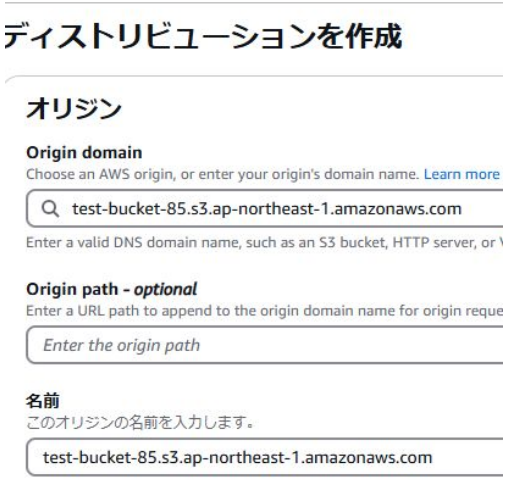
④CloudFrontのディストリビューションを作成してデフォルトで
S3バケットを指定
バケットへのアクセスをCloudFront経由のみ限定するためにOAC
を設定

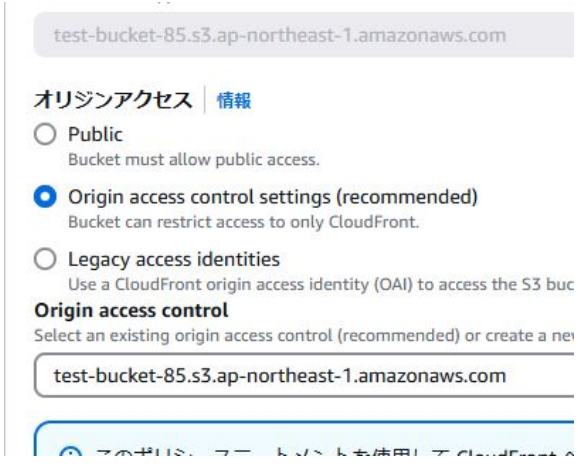




3：構築（実装）

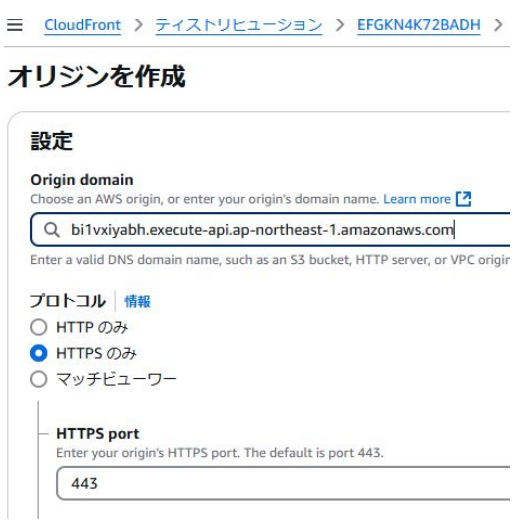
④CloudFrontのディストリビューションを作成してデフォルトで
S3バケットを指定
バケットへのアクセスをCloudFront経由のみ限定するためにOAC
を設定

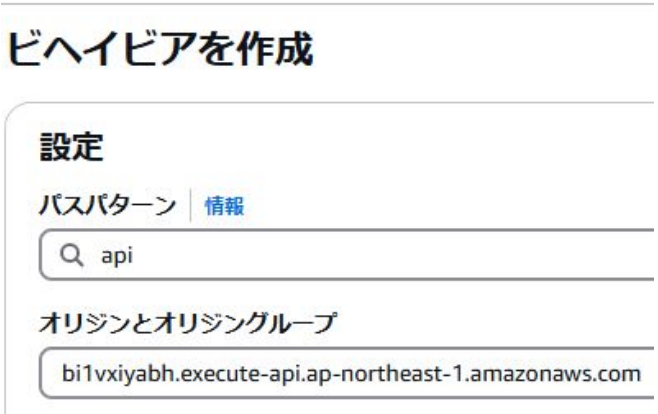




3：構築（実装）

④作成したディストリビューションからAPIGatewayもオリジンに
するためオリジンを作成
APIGatewayのビヘイビアを作成



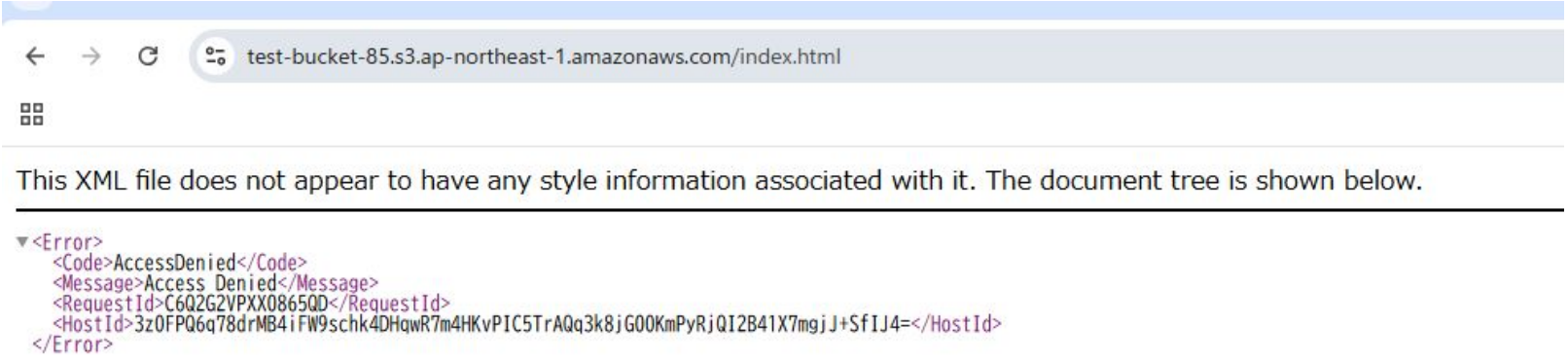


3：構築（実装）

⑤悪意のある攻撃から保護する為に、CloudFront作成時にWAFを設定

4：テスト結果（検証）

①S3バケットへの直接アクセスができないように設定されているか
確認のためバケット内のコンテンツURLをブラウザ検索
拒否されたためバケットへの制限がされているのを確認



4：テスト結果（検証）

②CloudFrontのディストリビューションドメインをブラウザから
アクセスをし、無事に翻訳機能が動作する事を確認