

# 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ー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ー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。

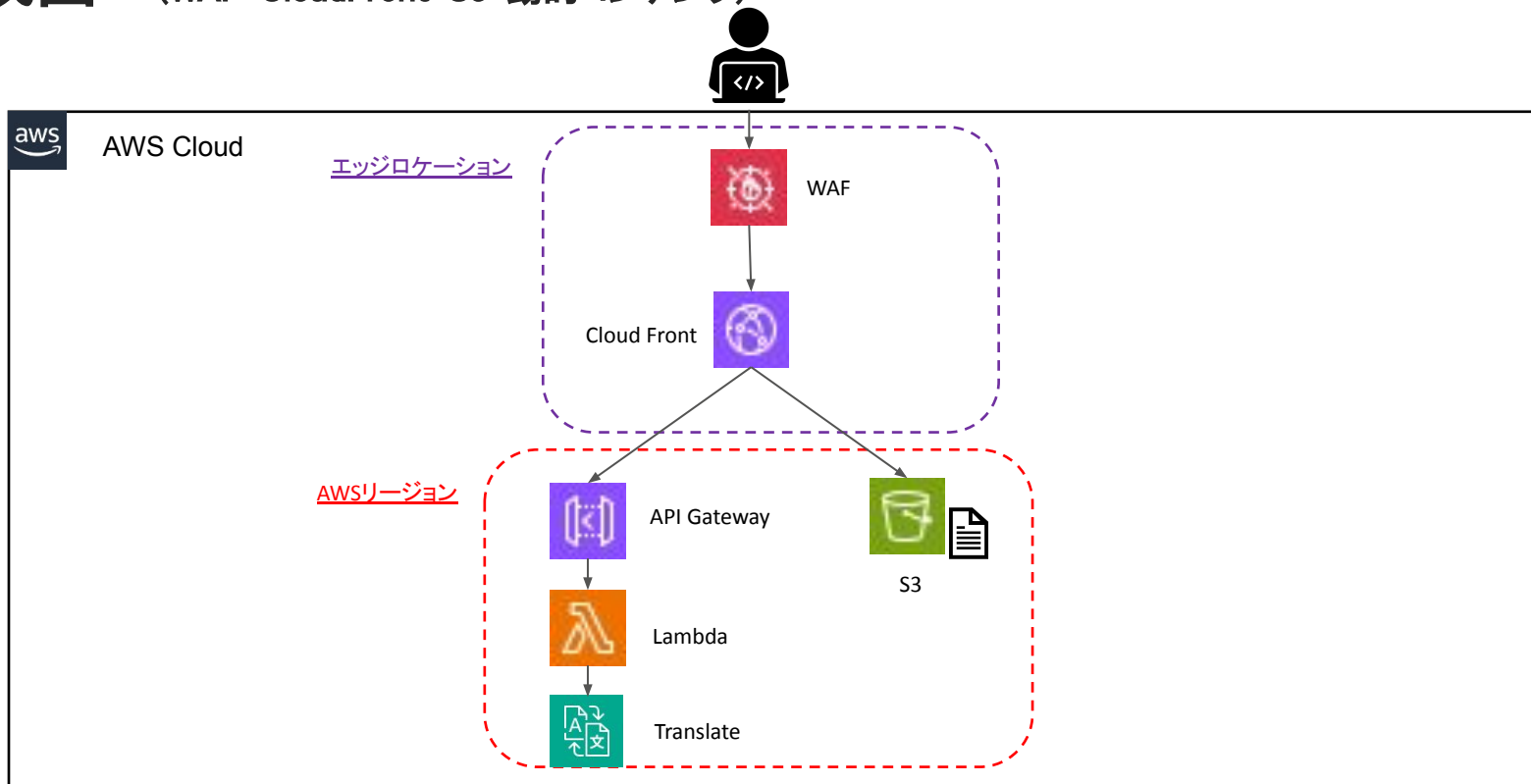
# 2: 設計

## ■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ー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)

- ① S3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

Amazon S3 > バケット > バケットを作成

バケットは S3 に保存されたデータのためのコンテナです。

## 一般的な設定

### AWS リージョン

アジアパシフィック (東京) ap-northeast-1

### バケットタイプ | 情報

#### 汎用

ほとんどのユースケースとアクセスパターンに推奨されます。汎用バケットは、複数のアベイラビリティゾーンにまたがるオブジェクトクラスを組み合わせることができます。

### バケット名 | 情報

test-bucket-85

バケット名はグローバル名前空間内で一意であることに加えて、バケット命名

### 既存のバケットから設定をコピー - オプション

次の設定のバケット設定のみがコピーされます。

バケットを選択する

## このバケットのブロックパブリックアクセス設定

パブリックアクセスは、アクセスコントロールリスト (ACL、Access Control List) を使用して、このバケットとそのオブジェクトへの公開アクセスが確実にブロックポイントにのみ適用されます。AWS では、パブリックアクセスを許可する機能することをご確認ください。このバケットやオブジェクトへの詳細

### ☒ パブリックアクセスをすべてブロック

この設定をオンにすることは、以下の 4 つの設定をすべてオンにすること

- ☒ 新しいアクセスコントロールリスト (ACL) を介して付与された S3 は、新しく追加されたバケットまたはオブジェクトに適用されたバケットでは、ACL を使用して S3 リソースへのパブリックアクセスを許可する
- ☒ 任意のアクセスコントロールリスト (ACL) を介して付与された S3 は、バケットとオブジェクトへのパブリックアクセスを付与するすべて
- ☒ 新しいパブリックバケットポリシーまたはアクセスポイントポ S3 は、バケットとオブジェクトへのパブリックアクセスを許可する新しを変更しません。
- ☒ 任意のパブリックバケットポリシーまたはアクセスポイントポ S3 は、バケットとオブジェクトへのパブリックアクセスを付与するポリ

## test-bucket-85 | 情報

### オブジェクト

### プロパティ

### アクセス許可

### メトリク

## オブジェクト (2)



S3 URI をコピー

URL をコピー

ダウンロード

オブジェクトは、Amazon S3 に保存された基本的なエンティティです。オブジェクトにアクセスできるためには、明示的にアクセス権限を付与す

プレフィックスでオブジェクトを検索

<input type="checkbox"/>	名前	▲	タイプ
<input type="checkbox"/>	index.html		html
<input type="checkbox"/>	static/		フォルダ

# 3: 構築(実装)

## ② 翻訳コンテンツを作成のためLambdaを起動

AWS 検索 [Alt+S] アジアパシフィック (東京)

IAM EC2 VPC CloudFront S3 Lambda API Gateway CloudFormation Lightsail WAF & Shield Route 53 AWS Application Migration Service

Lambda > 関数 > 関数の作成

☒ 一から作成  
シンプルな Hello World の例で開始します。

☐ 設計図の使用  
一般的なユースケース用のサンプルコードと設定プリセットから Lambda アプリケーションを構築します。

☐ コンテナイメージ  
関数にデプロイするコンテナイメージを選択します。

### 基本的な情報

**関数名**  
関数の目的を名前として入力します。

test\_lambda\_kadai

関数名は 1 ～ 64 文字で、リージョン内で一意である必要があり、スペースを含めることはできません。有効な文字は a ～ z、A ～ Z、0 ～ 9、ハイフン (-)、およびアンダースコア (\_) です。

**ランタイム** [情報](#)  
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

Python 3.13

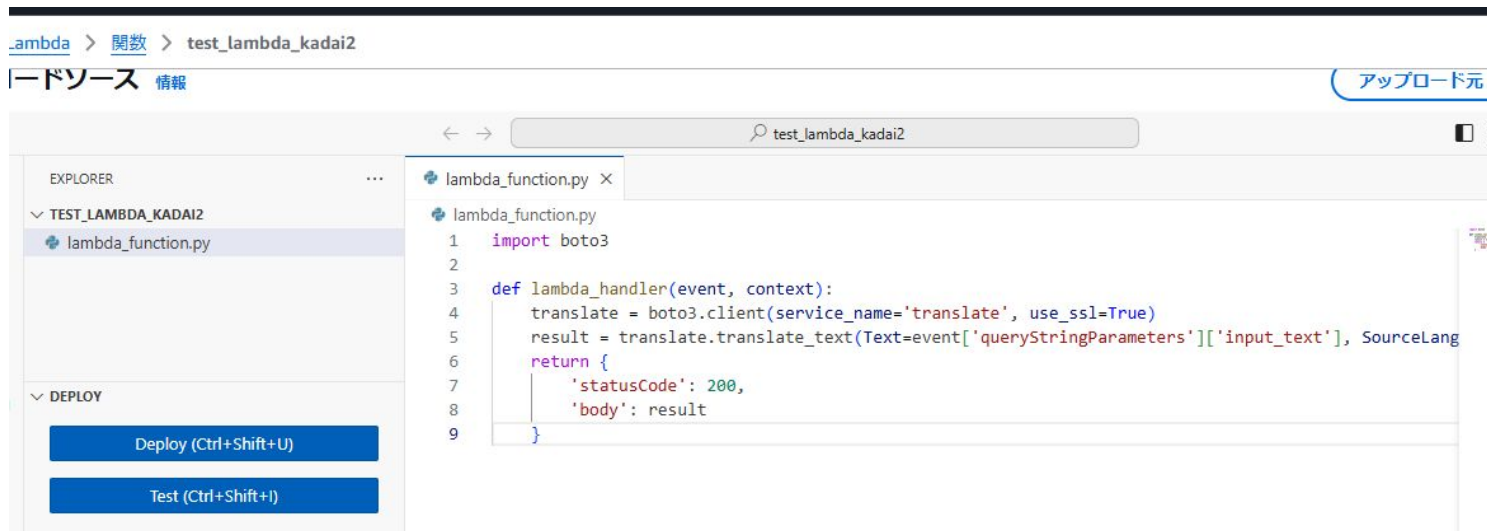
**アーキテクチャ** [情報](#)  
関数コードに必要な命令セットアーキテクチャを選択します。

☒ x86\_64

☐ arm64

# 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

≡ [IAM](#) > [ロール](#) > [test\\_lambda\\_kadai2-role-lr3cqjni](#) > 許可を追加

ポリシーを test\_lambda\_kadai2-role-lr3cqjni にアタッチ

▶ 現在の許可ポリシー (1)

その他の許可ポリシー (1/1090)

🔍 Transla



ポリシー名



[TranslateFullAccess](#)



[TranslateReadOnly](#)

# 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

API Gateway > API > リソース - translational-api (bi1vxiyabl)

### メソッドタイプ

GET

### 統合タイプ

- ☒ Lambda 関数  
API を Lambda 関数と統合します。



- ☐ AWS のサービス  
AWS のサービスと統合します。



- ☒ Lambda プロキシ統合  
リクエストを構造化されたイベントとして Lambda 関数に送信

### REST API を作成 情報

#### API の詳細

- ☒ 新しい API  
新しい REST API を作成します。
- ☐ API をインポート  
OpenAPI 定義から API をインポートします。

#### API 名

translational-api

#### 説明 - オプション

#### ☒ Lambda プロキシ統合

リクエストを構造化されたイベントとして Lambda 関数に送信します。

#### lambda 関数

lambda 関数の名前またはエイリアスを指定します。別のアカウントからの ARN を指定することもできます。

ap-northeast-1

arn:aws:lambda:ap-northeast-1:584791980123:function:test\_lambda\_kadaiz

- ☒ Lambda 関数を呼び出すための許可を API Gateway に付与します。オフにするには、関数のリソースポリシーを自分自  
る呼び出しロールを指定します。

#### 統合のタイムアウト | 情報

デフォルトでは、50 ~ 29,000 ミリ秒のインテグレーションタイムアウトを入力できます。サービスクォータを使用して、統合タイムアウトを 29  
29000

# 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

The screenshot shows the 'Method Request' configuration for an API Gateway method. At the top, the ID '29000' is displayed. Below it is a section for 'Method Request Parameters' with a dropdown menu set to 'URL Query String Parameters'. Under this dropdown, there is a table with one row: 'input\_text' in the 'Name' column and '必須' (Required) in the 'Required' column. A checkbox is present next to the 'Required' label. Below the table is a button labeled 'クエリ文字列を追加' (Add Query String). At the bottom of the visible section is a button labeled 'HTTP リクエストヘッダー' (HTTP Request Headers).

## ステージを作成

### ステージの詳細

ステージ名

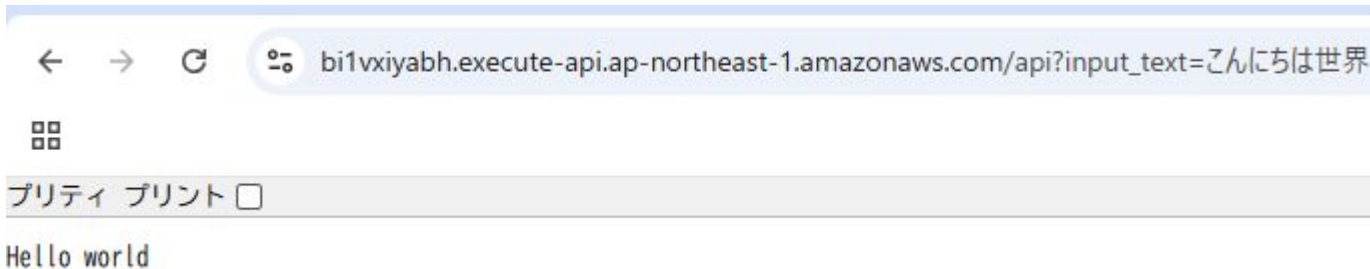
api

ステージの説明 - オプション

デプロイ

# 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)

- ④ CloudFront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

## ディストリビューションを作成

### オリジン

#### Origin domain

Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

test-bucket-85.s3.ap-northeast-1.amazonaws.com

Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or

#### Origin path - optional

Enter a URL path to append to the origin domain name for origin request

Enter the origin path

#### 名前

このオリジンの名前を入力します。

test-bucket-85.s3.ap-northeast-1.amazonaws.com

test-bucket-85.s3.ap-northeast-1.amazonaws.com

### オリジンアクセス | 情報

☐ Public

Bucket must allow public access.

☒ Origin access control settings (recommended)

Bucket can restrict access to only CloudFront.

☐ Legacy access identities

Use a CloudFront origin access identity (OAI) to access the S3 bucket

### Origin access control

Select an existing origin access control (recommended) or create a new

test-bucket-85.s3.ap-northeast-1.amazonaws.com

## キャッシュキーとオリジンリクエスト

キャッシュキーとオリジンリクエストを制御するには、キャッシュ

☒ Cache policy and origin request policy (recommended)

☐ Legacy cache settings

### キャッシュポリシー

既存のキャッシュポリシーを選択するか、新しいキャッシュポリシー

CachingOptimized

Policy with caching enabled. Supports Gzip and Brotli compression

[Create cache policy](#) [ポリシーを表示](#)

### オリジンリクエストポリシー - オプション

既存のオリジンリクエストポリシーを選択するか、新しいオリジン

オリジンポリシーを選択

[Create origin request policy](#)

# 3: 構築(実装)

## ④ CloudFront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

### ディストリビューションを作成

#### オリジン

##### Origin domain

Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

test-bucket-85.s3.ap-northeast-1.amazonaws.com

Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or

##### Origin path - optional

Enter a URL path to append to the origin domain name for origin request

Enter the origin path

##### 名前

このオリジンの名前を入力します。

test-bucket-85.s3.ap-northeast-1.amazonaws.com

test-bucket-85.s3.ap-northeast-1.amazonaws.com

#### オリジンアクセス | 情報

##### ☐ Public

Bucket must allow public access.

##### ☒ Origin access control settings (recommended)

Bucket can restrict access to only CloudFront.

##### ☐ Legacy access identities

Use a CloudFront origin access identity (OAI) to access the S3 bucket

#### Origin access control

Select an existing origin access control (recommended) or create a new

test-bucket-85.s3.ap-northeast-1.amazonaws.com

#### キャッシュキーとオリジンリクエスト

キャッシュキーとオリジンリクエストを制御するには、キャッシュ

##### ☒ Cache policy and origin request policy (recommended)

##### ☐ Legacy cache settings

#### キャッシュポリシー

既存のキャッシュポリシーを選択するか、新しいキャッシュポリシー

##### CachingOptimized

Policy with caching enabled. Supports Gzip and Brotli compression

[Create cache policy](#) [ポリシーを表示](#)

#### オリジンリクエストポリシー - オプション

既存のオリジンリクエストポリシーを選択するか、新しいオリジン

オリジンポリシーを選択

[Create origin request policy](#)

# 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

CloudFront > ディストリビューション > EFGKN4K72BADH >

### オリジンを作成

#### 設定

##### Origin domain

Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

Q bi1vxiyabh.execute-api.ap-northeast-1.amazonaws.com

Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or VPC origin

##### プロトコル | 情報

- ☐ HTTP のみ
- ☒ HTTPS のみ
- ☐ マッチビューワ

##### HTTPS port

Enter your origin's HTTPS port. The default is port 443.

443

### ビヘイビアを作成

#### 設定

##### パスパターン | 情報

Q api

##### オリジンとオリジングループ

bi1vxiyabh.execute-api.ap-northeast-1.amazonaws.com

キャッシュキーとオリジンリクエストを制御するには、キ

- ☒ Cache policy and origin request policy (recommended)
- ☐ Legacy cache settings

##### キャッシュポリシー

既存のキャッシュポリシーを選択するか、新しいキャッシュポ!

##### CachingDisabled

Policy with caching disabled

[Create cache policy](#) [ポリシーを表示](#)

##### オリジンリクエストポリシー - オプション

既存のオリジンリクエストポリシーを選択するか、新しいオリミ

input\_text2

[Create origin request policy](#) [ポリシーを表示](#)

1. フォールバックオリジン: オプション

# 3: 構築(実装)

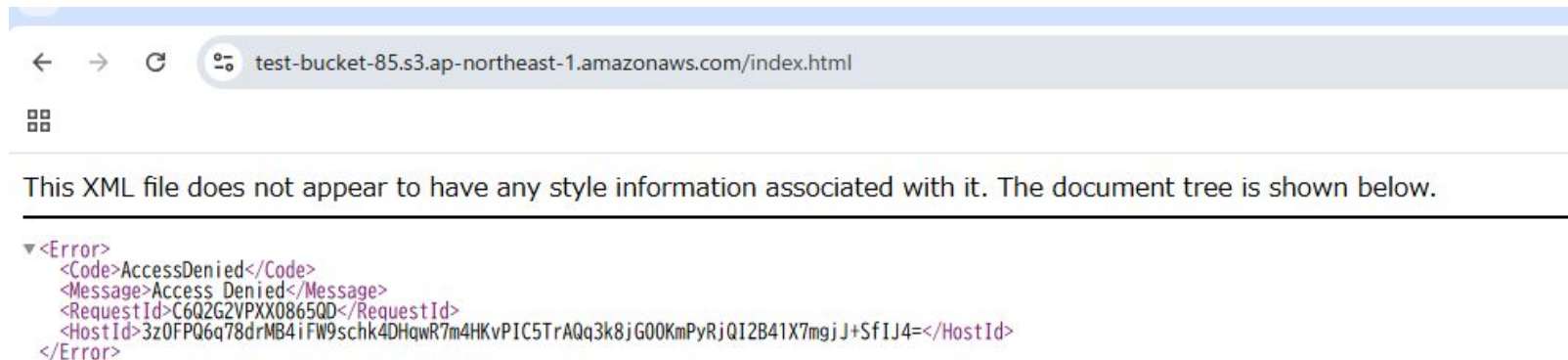
- ⑤悪意のある攻撃から保護する為に、CloudFront作成時にWAFを設定





## 4: テスト結果 (検証)

- ① S3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)

- ② CloudFront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

