g

更新履歴

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版 | 更新日 | 更新項目 | 更新者 | 備考 |
| (会社名/氏名) |
| 1.0 | 2021/06/16 | 新規作成 | サン・エム・システム  若林 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目次

[1 はじめに 6](#_Toc76481367)

[2 システム構成 7](#_Toc76481368)

[2.1 システム構成図 7](#_Toc76481369)

[2.2 サービス構成 8](#_Toc76481370)

[2.2.1 サービス一覧 8](#_Toc76481371)

[2.2.2 リソースグループ 10](#_Toc76481372)

[2.2.3 サービス管理方式 10](#_Toc76481373)

[2.3 サーバー構成 11](#_Toc76481374)

[2.3.1 Webサーバー(Lambda) 11](#_Toc76481375)

[2.3.2 データベース(DynamoDB) 12](#_Toc76481376)

[2.3.3 ストレージ(S3) 14](#_Toc76481377)

[2.3.4 認証基盤(Cognito) 17](#_Toc76481378)

[2.4 ソフトウェア構成 20](#_Toc76481379)

[2.5 ネットワーク構成 20](#_Toc76481380)

[2.5.1 AWSリージョン 21](#_Toc76481381)

[2.5.2 VPC 21](#_Toc76481382)

[2.5.3 サブネット 21](#_Toc76481383)

[2.5.4 ネットワークACL 21](#_Toc76481384)

[2.5.5 セキュリティグループ 21](#_Toc76481385)

[2.5.6 名前解決 21](#_Toc76481386)

[2.5.7 ルートテーブル 22](#_Toc76481387)

[3 可用性 23](#_Toc76481388)

[3.1 耐障害性 23](#_Toc76481389)

[3.2 災害対策 24](#_Toc76481390)

[4 拡張性 25](#_Toc76481391)

[4.1 拡張性設計 25](#_Toc76481392)

[5 保守性 26](#_Toc76481393)

[5.1 障害発生時フロー 26](#_Toc76481394)

[5.2 バックアップ・リストア 27](#_Toc76481395)

[5.2.1 バックアップ 27](#_Toc76481396)

[5.2.2 リストア 27](#_Toc76481397)

[5.3 ジョブ管理 28](#_Toc76481398)

[5.3.1 ジョブ一覧 28](#_Toc76481399)

[5.3.2 ジョブ監視 29](#_Toc76481400)

[5.4 URL監視 30](#_Toc76481401)

[5.5 リソース監視 30](#_Toc76481402)

[5.5.1 リソース監視方式 30](#_Toc76481403)

[5.5.2 CloudWatchメトリクス保存期間 30](#_Toc76481404)

[5.5.3 リソース監視状況確認方法 31](#_Toc76481405)

[5.5.4 リソース監視項目 31](#_Toc76481406)

[5.5.5 しきい値監視 51](#_Toc76481407)

[5.6 ログ管理 52](#_Toc76481408)

[5.6.1 ログ一覧 52](#_Toc76481409)

[5.6.2 ログ保存期間 54](#_Toc76481410)

[5.6.3 ログ監視 54](#_Toc76481411)

[5.7 時刻同期 54](#_Toc76481412)

[5.8 ソフトウェアのアップデート 55](#_Toc76481413)

[6 セキュリティ 56](#_Toc76481414)

[6.1 ユーザー管理 56](#_Toc76481415)

[6.2 ロール管理 57](#_Toc76481416)

[6.3 暗号化方針 57](#_Toc76481417)

[6.3.1 データベース(DynamoDB) 57](#_Toc76481418)

[6.3.2 ストレージ(S3) 57](#_Toc76481419)

[6.3.3 認証基盤(Cognito) 58](#_Toc76481420)

[6.3.4 バックアップデータ 58](#_Toc76481421)

[6.4 Webアクセス 58](#_Toc76481422)

[6.4.1 ACM 58](#_Toc76481423)

[6.4.1 AWS WAF 59](#_Toc76481424)

[6.4.2 CloudFront 61](#_Toc76481425)

[6.4.3 API Gateway 65](#_Toc76481426)

[6.5 ウィルス対策 67](#_Toc76481427)

# はじめに

本書はまなび+(以下、本システム)のインフラ構成、機能の実現方法、及び運用方式について記載する。

なお、本システムについてはパブリッククラウドサービスであるAmazon Web Services(以下、AWS)を利用して構築する。

本システムは同時アクセス数の増加に対して迅速な対応を可能とするため、サーバレス構成を採用する。

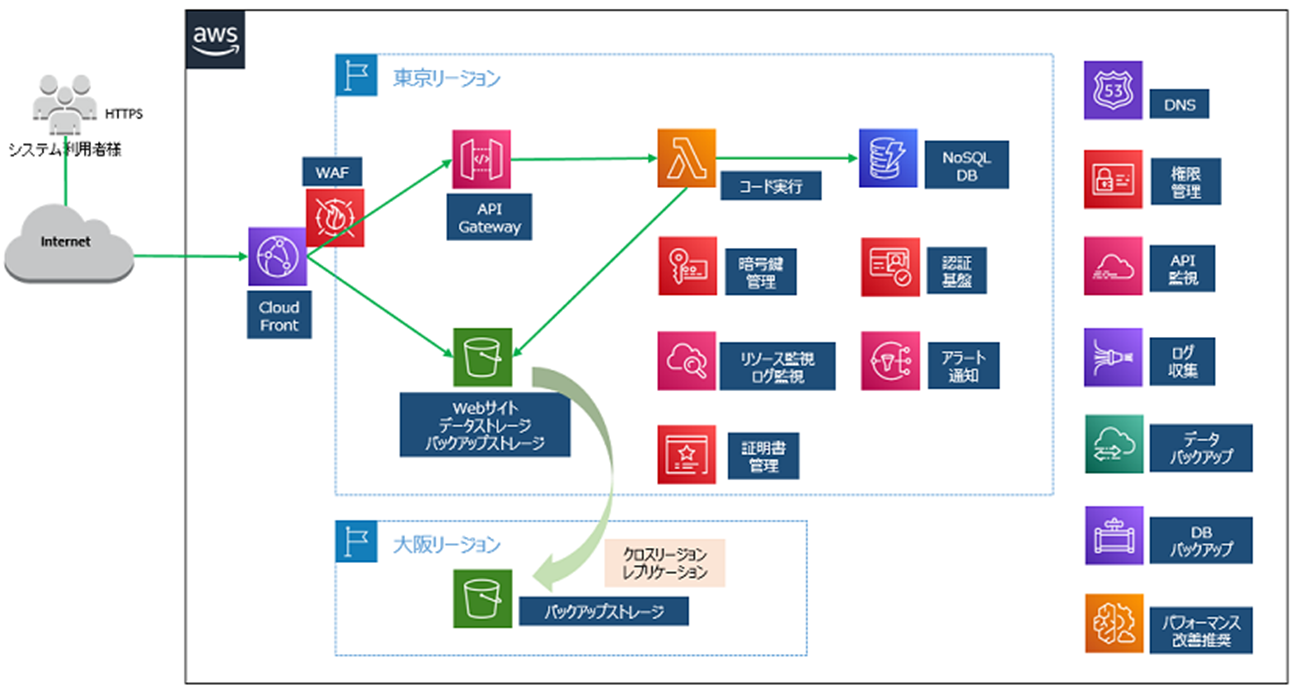
サーバレス構成とすることで、以下4点の利点を享受することができる。



# システム構成

## システム構成図

以下に本システムのシステム構成図を示す。



## サービス構成

本システムで使用するサービスについて記載する。

### サービス一覧

以下に本システムで使用するサービス一覧とその概要を記載する。

|  |  |  |  |
| --- | --- | --- | --- |
|  | システム構成図内表記 | |  |
| サービス | アイコン | 説明 | 概要 |
| ACM |  | 証明書管理 | SSL証明書のプロビジョニング、管理、デプロイを簡単にする。AWS Certificate Manager を使用すれば、SSL証明書の購入、アップロード、更新という時間のかかるプロセスを手動で行う必要がなくなる。 |
| API Gateway |  | 同左 | API の作成、公開、保守、モニタリング、保護を行います。API は、アプリケーションがバックエンドサービスからのデータ、ビジネスロジック、機能にアクセスするための「フロントドア」として機能する。 |
| AWS Compute Optimizer |  | パフォーマンス改善推奨 | 使用率データに基づいて、Amazon EC2 インスタンス、Amazon EBS ボリューム、AWS Lambda 関数の 3 種類の AWS リソースに関する最適な構成を推奨する。 |
| AWS WAF |  | WAF | 可用性、セキュリティ侵害、リソースの過剰消費といった一般的なWebの脆弱性からWebアプリケーションまたはAPIを保護するWebアプリケーションファイアウォール。 |
| CloudFront |  | 同左 | 低レイテンシーの高速転送により世界中の視聴者に安全に配信する高速コンテンツ配信ネットワーク (CDN) サービス。 |
| CloudTrail |  | API監視 | AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を行うためのサービス。CloudTrail を使用すると、AWS インフラストラクチャ全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できる。 |
| CloudWatch |  | リソース監視  ログ監視 | ログ、メトリクス、およびイベントという形式でモニタリングデータと運用データを収集し、AWSのサーバーで実行されるAWSのリソース、アプリケーション、およびサービスの統合されたビューをユーザーに提供。 |
| Cognito |  | 認証基盤 | ウェブアプリケーションおよびモバイルアプリに素早く簡単にユーザーのサインアップ/サインインおよびアクセスコントロールの機能を提供する。 |
| Data Pipeline |  | DBバックアップ | AWSのさまざまなコンピューティングサービスやストレージサービスに対して信頼性の高いデータ処理やデータ移動を行うことを支援するサービス。 |
| DataSync |  | データバックアップ | AWS ストレージサービス間でのデータの移動を簡素化、自動化、および高速化するオンラインデータ転送サービス。 |
| DynamoDB |  | NoSQL DB | 規模に関係なく数ミリ秒台のパフォーマンスを実現する、key-value およびドキュメントデータベース。完全マネージド型マルチマスターで耐久性があるデータベースで、セキュリティ、バックアップおよび復元と、インターネット規模のアプリケーション用のメモリ内キャッシュが組み込まれている。 |
| IAM |  | 権限管理 | AWS のサービスやリソースへのアクセスを安全に管理する。IAM を使用すると、AWS のユーザーとグループを作成および管理し、アクセス権を使用して AWS リソースへのアクセスを許可および拒否が可能となる。 |
| Kinesis Data Firehose |  | ログ収集 | ストリーミングデータをデータレイクやデータストア、分析サービスに確実にロードする最も簡単な方法を提供する。 |
| KMS |  | 暗号鍵管理 | 暗号化キーを簡単に作成して管理し、幅広い AWS のサービスやアプリケーションでの使用を制御できるようになる。セキュアで弾力性の高いサービスで、キーを保護するために FIPS 140-2 の検証済みまたは検証段階のハードウェアセキュリティモジュールを使用する。 |
| Lambda |  | コード実行 | サーバーのプロビジョニングや管理をすることなく、コードを実行。コードは他の AWS サービスから自動的にトリガーするよう設定することも、ウェブやモバイルアプリケーションから直接呼び出すよう設定することも可能。 |
| Route53 |  | DNS | 可用性と拡張性に優れたクラウドのDNSサービス。ドメイン登録、DNSルーティング、ヘルスチェックの3つの主要な機能を任意の組み合わせで実行可能。 |
| S3 |  | Webサイト  データストレージ  バックアップストレージ | 拡張性と耐久性を兼ね揃えたクラウドストレージ。 |
| SNS |  | アラート通知 | フルマネージド型メッセージングサービス。SMS やモバイルプッシュ、電子メールを介してユーザーと直接通信が可能。 |

### リソースグループ

本システムではすべてのサービスに共通して以下のリソースグループを指定する。

リソースグループを設定することにより、AWSマネジメントコンソールで関連するサービス一覧を表示することや、リソースグループ別に利用費を確認することが可能となる。

|  |  |  |
| --- | --- | --- |
|  | 本番環境 | 検証環境 |
| グループ名 | Manabi Plus | |
| グループタイプ | タグベース | |
| リソースタイプ | サポートされるすべてのリソースタイプ | |
| タグキー | Project | |
| オプションのタグ値 | Manabi Plus | |
| タグキー | Environment | |
| オプションのタグ値 | Production | Staging |

### サービス管理方式

本システムではすべてのサービスをCloudFormationで管理する

CloudFormationではコードでインフラ環境を管理するInfrastructure as Codeを実現することにより、AWSリソースのコレクションをモデリングし、迅速に一貫してプロビジョニングし、ライフサイクル全体で管理することが容易となる。

サービス定義はYAML 形式のテキストファイルである AWS CloudFormation テンプレートに記載する。テンプレートは最大51,200バイトの制約があるため、制約を超えるテンプレートを作成する必要がある場合にはネストされたスタックを使用して制約を回避する。

## サーバー構成

以下に本システムのサーバー構成を示す。

本番環境と検証環境を個別に管理するため、でサーバーを分離する。

各種サーバーは必要最小限のサービスから必要最小限の処理のみアクセスを許可する。

### Webサーバー(Lambda)

本システムではWebサーバーとしてLambdaサービスを利用する。

以下にLambdaの定義を示す。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| コード名 | 本番用関数名 | ランタイム | ハンドラー | アクセスするサービス | メモリ(MB) | タイムアウト(秒) | 本番用環境変数 |
| 検証用関数名 | 検証用環境変数 |
| code.zip | codeprod | Python3.8 | Index.handler | DynamoDB / S3 | 128 | 30 | key1:value1 |
|  | codestg |  |  |  |  |  | key1:value2 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

各種設定項目の説明を以下に示す。

|  |  |
| --- | --- |
| 設定項目 | 説明 |
| コード名 | Lambdaが実行するコード。S3に格納する。 |
| 関数名 | 関数の名前 |
| ランタイム | 関数を実行するLambdaランタイム |
| ハンドラー | 関数の呼び出し時にランタイムで実行されるメソッド。 |
| アクセスするサービス | 他のサービスにアクセスするロール |
| メモリ | 関数で実行時に使用できるメモリの量。  デフォルト128MB（128MB-10240MB） |
| タイムアウト | Lambda で関数が停止するまでに許可される実行時間。  デフォルト3秒（1秒-900秒） |
| 環境変数 | Lambda で実行環境に設定するキーと値のペア |

### データベース(DynamoDB)

本システムではデータベースとしてDynamoDBサービスを利用する。

本書では非機能要件のみを記載する。テーブル定義についてはテーブル定義書を参照する。

暗号化方針については6.3暗号化方針を参照する。

ポイントインタイムリカバリについては検証環境のバックアップは不要であるため本番環境のみ有効とし、検証環境は無効とする。

#### 本番環境

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | プロビジョニング  されたキャパシティ | | 読み込みキャパシティ  自動拡張 | | | 書き込みキャパシティ  自動拡張 | | | ポイント |  |
| テーブル名 | RCU | WCU | ターゲット使用率(%) | Min RCU | Max RCU | ターゲット使用率(%) | Min WCU | Max WCU | インタイム  リカバリ | タグ  (key:value) |
| schools | 5 | 5 | 70 | 5 | 40000 | 70 | 5 | 40000 | 有効化 |  |
| users |  |  |  |  |  |  |  |  |  |  |
| textbooks |  |  |  |  |  |  |  |  |  |  |
| licenses\_schools |  |  |  |  |  |  |  |  |  |  |
| app\_properties |  |  |  |  |  |  |  |  |  |  |
| login\_id\_seq |  |  |  |  |  |  |  |  |  |  |

#### 検証環境

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | プロビジョニング  されたキャパシティ | | 読み込みキャパシティ  自動拡張 | | | 書き込みキャパシティ  自動拡張 | | | ポイント |  |
| テーブル名 | RCU | WCU | ターゲット使用率(%) | Min RCU | Max RCU | ターゲット使用率(%) | Min WCU | Max WCU | インタイム  リカバリ | タグ  (key:value) |
| schools | 5 | 5 | 70 | 5 | 40000 | 70 | 5 | 40000 | 無効化 |  |
| users |  |  |  |  |  |  |  |  |  |  |
| textbooks |  |  |  |  |  |  |  |  |  |  |
| licenses\_schools |  |  |  |  |  |  |  |  |  |  |
| app\_properties |  |  |  |  |  |  |  |  |  |  |
| login\_id\_seq |  |  |  |  |  |  |  |  |  |  |

各種設定項目の説明を以下に示す。

|  |  |  |
| --- | --- | --- |
| 設定項目 | | 説明 |
| テーブル名 | | テーブルの名前 |
| プロビジョニングされたキャパシティ | |  |
|  | RCU (読み込みキャパシティーユニット) | アプリケーションに必要と予想される読み込みのキャパシティ |
|  | WCU (書き込みキャパシティーユニット) | アプリケーションに必要と予想される書き込みのキャパシティ |
| 読み込みキャパシティの自動拡張 | |  |
|  | ターゲット使用率 | 読み込みキャパシティーユニットの範囲 (上限と下限) と、その範囲内の目標使用率を定義することでテーブルおよびグローバルセカンダリインデックス用のスループットキャパシティーが自動的に管理される。 |
|  | Min RCU(RCUの下限値) |
|  | Max RCU(RCUの上限値) |
| 書き込みキャパシティの自動拡張 | |  |
|  | ターゲット使用率 | 書き込みキャパシティーユニットの範囲 (上限と下限) と、その範囲内の目標使用率を定義することでテーブルおよびグローバルセカンダリインデックス用のスループットキャパシティーが自動的に管理される。 |
|  | Min WCU(WCUの下限値) |
|  | Max WCU(WCUの上限値) |
| ポイントインタイムリカバリ | | テーブルの増分バックアップを維持し、過去35日間の任意の時点にテーブルを復元可能とする。 |
| 暗号化 | | DynamoDBのサーバー側暗号化設定を選択し、保管時のデータを保護する。  デフォルト：デフォルトの暗号化タイプ。キーは DynamoDB によって所有される。 |

### ストレージ(S3)

本システムではストレージとしてS3サービスを利用する。

以下にS3の定義を示す。

#### Webサイト

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 設定値 | 備考 |
| バケット名 | | 本番環境：prod-manabiplus-web  検証環境：stg-manabiplus-web |  |
| アクセス設定 | | パブリックアクセスをすべてブロック |  |
| バケットポリシー | |  |  |
|  | プリンシパル | Webサイト用CloudFrontディストリビューション | Webサイト用CloudFrontからのみアクセス可とする。 |
|  | 許可アクション | 読取りのみ可能 |  |
| 暗号化 | | 別途記載 | 6.3暗号化方針を参照 |
| サーバーアクセスのログ記録 | | 有効 |  |
|  | ターゲットバケット | S3(ログストレージ) |  |
|  | プレフィックス | webacclog/ |  |
| 静的ウェブサイトホスティング | | 無効 | Webサイト用CloudFrontからのみアクセス可とする。 |

#### データストレージ

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 設定値 | 備考 |
| バケット名 | | 本番環境：prod-manabiplus-data  検証環境：stg-manabiplus-data |  |
| アクセス設定 | | パブリックアクセスをすべてブロック |  |
| バケットポリシー | |  |  |
|  | プリンシパル | Lambda(Webサーバー用)  Lambda(ウィルス対策用) |  |
|  | 許可アクション | 読み書き可能 |  |
| バケットポリシー | |  |  |
|  | プリンシパル | すべて |  |
|  | 拒否アクション | 読み取り  タグ付け |  |
|  | 条件 | ウィルス感染ファイル |  |
| バケットポリシー | |  |  |
|  | プリンシパル | Lambda(ウィルス対策用)以外 |  |
|  | 拒否アクション | 読み取り |  |
|  | 条件 | ウィルス未判定ファイル |  |
| バケットポリシー | |  |  |
|  | プリンシパル | すべて | HTTPS通信のみ許可 |
|  | 拒否アクション | S3に関する全てのアクション |  |
|  | 条件 | 暗号化されていない通信 |  |
| 暗号化 | | 別途記載 | 6.3暗号化方針を参照 |
| サーバーアクセスのログ記録 | | 有効 |  |
|  | ターゲットバケット | S3(ログストレージ) |  |
|  | プレフィックス | dataacclog/ |  |

#### アプリケーションストレージ

バケットポリシーの設定は不要

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 設定値 | 備考 |
| バケット名 | | 本番環境：prod-manabiplus-app  検証環境：stg-manabiplus-app |  |
| アクセス設定 | | パブリックアクセスをすべてブロック |  |
| バケットポリシー | |  |  |
|  | プリンシパル | Lambda(ウィルス対策用) |  |
|  | 許可アクション | 読み書き可能 | ウィルス定義ファイルを読み書きする。 |
| 暗号化 | | 別途記載 | 6.3暗号化方針を参照 |
| サーバーアクセスのログ記録 | | 有効 |  |
|  | ターゲットバケット | S3(ログストレージ) |  |
|  | プレフィックス | appacclog/ |  |

#### バックアップストレージ

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 設定値 | 備考 |
| バケット名 | | 本番環境：prod-manabiplus-backup  検証環境：stg-manabiplus-backup  大阪リージョン：dr-manabiplus-backup |  |
| アクセス設定 | | パブリックアクセスをすべてブロック |  |
| バージョニング | | 本番環境、大阪リージョン：有効  検証環境：無効 | 本番環境 - 大阪リージョン間でクロスリージョンレプリケーションを設定するため。 |
| 暗号化 | | 別途記載 | 6.3暗号化方針を参照 |
| サーバーアクセスのログ記録 | | 有効 |  |
|  | ターゲットバケット | S3(ログストレージ) |  |
|  | プレフィックス | bkacclog/ |  |
| レプリケーションルール | | 本番環境 - 大阪リージョン間で有効 |  |

#### ログストレージ

|  |  |  |
| --- | --- | --- |
| 項目 | 設定値 | 備考 |
| バケット名 | 本番環境：prod-manabiplus-log  検証環境：stg-manabiplus-log |  |
| アクセス設定 | パブリックアクセスをすべてブロック |  |
| バケットポリシー | 設定不要 | AWS WAF / CloudFront / S3 が同一アカウントで動作するため、許可設定不要 |
| 暗号化 | 別途記載 | 6.3暗号化方針を参照 |
| ライフサイクルルール | 保存期間を25ヶ月(761日)とする。 | オブジェクトの現行バージョンの有効期限を761日とし、有効期限が切れたオブジェクトを完全に削除する。 |

#### CloudTrailログストレージ

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 設定値 | 備考 |
| バケット名 | | 本番環境：prod-manabiplus-cloudtrail  検証環境：stg-manabiplus-cloudtrail |  |
| アクセス設定 | | パブリックアクセスをすべてブロック |  |
| バケットポリシー | |  |  |
|  | プリンシパル | CloudTrail | CloudTrail設定時に自動的に設定される。 |
|  | 許可アクション | 読み書き可能 |  |
| 暗号化 | | 別途記載 | 6.3暗号化方針を参照 |
| サーバーアクセスのログ記録 | | 有効 |  |
|  | ターゲットバケット | S3(ログストレージ) |  |
|  | プレフィックス | ctacclog/ |  |
| ライフサイクルルール | | 保存期間を25ヶ月(761日)とする。 | オブジェクトの現行バージョンの有効期限を761日とし、有効期限が切れたオブジェクトを完全に削除する。 |

### 認証基盤(Cognito)

本システムでは、認証基盤としてCognitoを利用する。

以下にCognitoの定義を示す。

#### ユーザープール

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 項目 | | | | 設定値 | 備考 |
| ユーザープール名 | | | | 本番環境：  検証環境： |  |
| 属性 | | | |  |  |
|  | サインインオプション | | |  |  |
|  |  | ユーザー名 | | 有効 | ユーザー名、E メールアドレスおよび電話番号の何れかを選択 |
|  |  |  | 検証済みの E メールアドレスでのサインインも許可 | 無効 | ユーザーは、ユーザー名を使用するか、オプションで複数の選択肢を使用してサインアップおよびサインインできる。 |
|  |  |  | 検証済みの電話番号でのサインインも許可 | 無効 |
|  |  |  | 任意のユーザー名 (ユーザーが変更できるユーザー名) でのサインインも許可 | 無効 |
|  |  | E メールアドレスおよび電話番号 | | 無効 | ユーザー名、E メールアドレスおよび電話番号の何れかを選択 |
|  |  |  | E メールアドレスを許可 | 無効 | ユーザーは、E メールアドレスまたは電話番号を「ユーザー名」として使用してサインアップおよびサインインできる。 |
|  |  |  | 電話番号を許可 | 無効 |
|  |  |  | E メールアドレスと電話番号の両方を許可 (ユーザーは 1 つを選択できます) | 無効 |
|  | (推奨) ユーザー名入力で大文字と小文字を区別しないことを有効にする | | |  | 有効にすると、ユーザーは「username」または「Username」のいずれでもサインイン可能となる。 |
|  | 標準属性 | | |  | 以下標準属性のうち、サインアップに必須とする属性を選択する。  address / nickname / birthdate / phone number / email / picture / family name / preferred username / gender / profile / given name / zoneinfo / locale / updated at / middle name / website / name |
| ポリシー | | | |  |  |
|  | パスワードの強度 | | |  |  |
|  |  | 最小長 | | 8 | 最小文字数 |
|  |  | 必須文字種別 | | 数字 / 特殊文字 / 大文字 / 小文字 | 以下から必須とする文字種別を選択する。  数字 / 特殊文字 / 大文字 / 小文字 |
|  | 自己サインアップ | | | 管理者のみ | 以下からユーザーの作成を許可する対象を選択する。  管理者のみ / ユーザー |
|  | 有効期限 (日数) | | | 7 | 管理者が設定した一時パスワードが使用されないまま有効期限になるまでの期間 |
| MFA、確認 | | | |  |  |
|  | 多要素認証 (MFA) | | | オフ | 以下からMFAの設定を選択する。  オフ / 省略可能 / 必須 |
|  | アカウント回復方法 | | | 使用可能な場合は E メール、それ以外の場合は電話。ただし、MFA にも使用している場合、電話でパスワードをリセットすることは許可しません | 以下からユーザーがパスワードを忘れた場合のアカウント回復方法を選択する。  ・使用可能な場合は Eメール、それ以外の場合は電話。ただし、MFA にも使用している場合、電話でパスワードをリセットすることは許可しません  ・使用可能な場合は電話、それ以外の場合は E メール。ただし、MFA にも使用している場合は、電話でパスワードをリセットすることは許可しません  ・Eメールのみ  ・電話のみ。ただし、MFA にも使用している場合は、電話でパスワードをリセットすることは許可しません  ・(非推奨) 使用可能な場合は電話、それ以外の場合は Eメール。MFA にも使用している場合は、電話でパスワードをリセットすることができます  ・なし – ユーザーは管理者に連絡してパスワードをリセットする必要があります |
|  | 属性の確認 | | |  | 以下からユーザーの検証方法を選択する。  Eメール / 電話番号 / Eメールまたは電話番号 / 検証なし |
|  | SMSメッセージ送信ロール | | | (SMSメッセージ送信ロール) | Amazon Cognito に対して SMS メッセージの送信を許可する。 |
| メッセージのカスタマイズ | | | |  |  |
|  | Eメールアドレスカスタマイズ | | |  |  |
|  |  | SESリージョン | | 米国東部(バージニア) | SES の検証済み ID から E メールを送信できる。 |
|  |  | FROM EメールアドレスARN | | デフォルト |
|  |  | FROM Eメールアドレス | |  |
|  |  | REPLY-TO Eメールアドレス | |  |
|  | SESでEメールを送信する | | | いいえ | 毎日の E メールの制限を上げる必要がある場合は [はい] を選択し、それ以外の場合は [いいえ] を選択する。 |
|  | Eメール検証メッセージのカスタマイズ | | |  |  |
|  |  | 検証タイプ | | コード | コードまたはクリック可能リンクを選択して、E メールアドレスを選択する。 |
|  |  | Eメールの件名 | | 検証コード |
|  |  | Eメールのメッセージ | | 検証コードは {####} です。 |
|  | ユーザー招待メッセージのカスタマイズ | | |  |  |
|  |  | SMSメッセージ | | ユーザー名は {username}、仮パスワードは {####} です。 | メッセージはカスタマイズし、HTML タグを含めることができるが、「{username}」および「{####}」プレースホルダーを含める必要がある。このプレースホルダーはそれぞれユーザー名および仮パスワードで置き換えられる。 |
|  |  | Eメールの件名 | | 仮パスワード |
|  |  | Eメールのメッセージ | | ユーザー名は {username}、仮パスワードは {####} です。 |
| デバイスの記憶 | | | | いいえ |  |

#### IDプール

|  |  |  |
| --- | --- | --- |
| 項目 | 設定値 | 備考 |
| IDプール名 | 本番環境：  検証環境： |  |
| 認証されていないID | 無効 | 認証されていない ID に対するアクセスの有効/無効を選択する。このオプションを有効にすると、インターネットアクセスが可能なユーザー全員に AWS 認証情報を付与することができる。 |
| 認証フローの設定 | 無効 | Cognito では、拡張された認証フローの使用を推奨しています。ただし、基本的なフローを使用する場合は、ここで有効にすることができます |
| 認証プロバイダー |  | 以下から、Cognitoの認証方法を選択する。  ・Cognito  ・Amazon  ・Apple  ・Facebook  ・Google+  ・Twitter / Digits  ・OpenID  ・SAML  ・カスタム |

## ソフトウェア構成

本システムのソフトウェアは全てAWSマネージドサービスを利用し、ユーザー管理によるソフトウェアは導入しない。

## ネットワーク構成

本システムのネットワーク構成を以下に示す。

### AWSリージョン

本システムの利用者は日本国内に限定される。

利用者のネットワークレイテンシを最小化するため、本システムは東京リージョンに構築する。

|  |  |
| --- | --- |
| AWSリージョン | アジアパシフィック (東京) |

### VPC

本システムはサーバレス構成であり、AWSが管理・提供するネットワーク構成で実行されるため

VPCの設計構築は不要である。

### サブネット

本システムはサーバレス構成であり、AWSが管理・提供するネットワーク構成で実行されるため

サブネットの設計構築は不要である。

### ネットワークACL

本システムはサーバレス構成であり、AWSが管理・提供するネットワーク構成で実行されるため

ネットワークACLの設計構築は不要である。

### セキュリティグループ

本システムはサーバレス構成であり、AWSが管理・提供するネットワーク構成で実行されるため

セキュリティグループの設計構築は不要である。

### 名前解決

本システムではRoute53サービスを利用し、ドメイン名解決のためのパブリックホストゾーンを作成する。

### ルートテーブル

本システムはサーバレス構成であり、AWSが管理・提供するネットワーク構成で実行されるため

ルートテーブルの設計構築は不要である。

# 可用性

## 耐障害性

本システムが利用する各種サービスはすべてAWSが管理・提供するAWSグローバルインフラストラクチャ上で実行される。

本システムは東京リージョン内の複数のアベイラビリティーゾーン(以下AZ)で稼働し、単一のAZ障害からシステムを保護する。

AWSのグローバルインフラストラクチャは、AWSリージョンとAZを中心として構成されている。AWSリージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立・隔離されたAZがある。AZは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、および拡張性が優れており、AZ間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを運用することができる。

AWSサービスはサービス別にSLAを定義している。以下に本システムが使用するサービスのSLA最低値、及びSLAが最低値の場合の週単位・月単位・年単位でシステムが停止する最大時間を示す。

|  |  |  |  |
| --- | --- | --- | --- |
| SLA最低値 | 週間停止時間 | 月間停止時間 | 年間停止時間 |
| 99.9% | 10.08分 | 43.20分 | 8.76時間 |

本システムが使用するサービスのSLAを示す。

|  |  |
| --- | --- |
| SLA | サービス |
| 100% | Route53 |
| 99.99% | DynamoDB / Kinesis Data Firehose |
| 99.95% | API Gateway / AWS WAF / Lambda / RDS |
| 99.9% | ACM / CloudFront / CloudTrail / CloudWatch / Cognito / DataSync / KMS / S3 / SNS |

## 災害対策

災害発生時にフェイルオーバーしてサービスを継続する際、及び通常運用時のデータレプリケーションのネットワークレイテンシ最小化の観点から、東京リージョンに構築する本システムの災害対策リージョンとして大阪リージョンが最適である。

しかし、2021年3月に開設された大阪リージョンは本書執筆時(2021年6月)でCognitoのサービスに対応していないため、フェイルオーバーすることができない。そのため、本システムでは災害対策を考慮しない。

大阪リージョンがCognitoのサービスに対応した後に災害対策について改めて検討することとする。

# 拡張性

## 拡張性設計

本システムでは、使用状況に応じて各種リソースを拡張する。

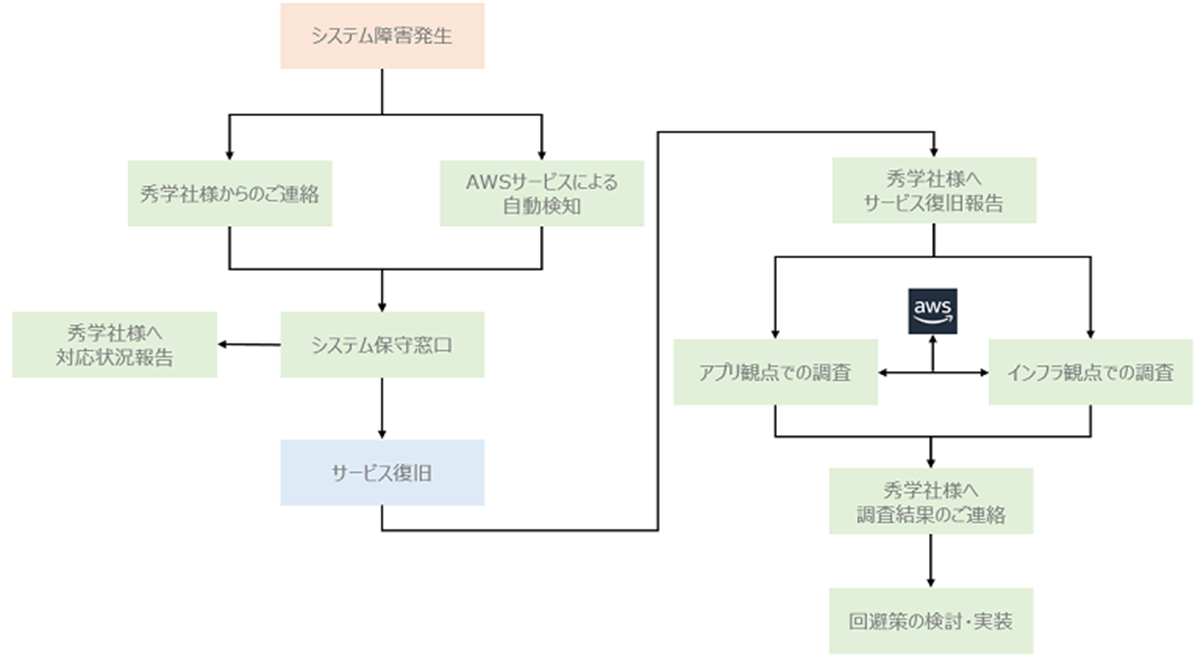
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| サーバー | 対象リソース | 拡張方式 | 拡張時サーバー停止の必要性 | 備考 |
| Webサーバー  (Lambda) | メモリ | 128 MB～10,240 MBの値を1MB単位で指定 | 不要 | 運用上、問題が発生した場合にAWS Compute Optimizerによる推奨事項を参考に拡張可否を検討する。 |
|  | CPU | メモリ割り当て容量に応じて自動調整される。(1,769 MBあたり1 vCPU) | 不要 |
| データベース | ストレージ容量 | 事実上無制限まで自動拡張 | 不要 |  |
| (DynamoDB) | スループット | 事実上無制限まで自動拡張 | 不要 | 拡張範囲は手動で設定する。 |
| ストレージ  (S3) | ストレージ容量 | 事実上無制限まで自動拡張 | 不要 |  |

# 保守性

## 障害発生時フロー

本システムにおいて障害が発生した場合はサービスを復旧することを最優先とし、サービス復旧後に原因調査及び回避策の検討を実施する。

システムに関連する全てのログはリアルタイムでCloudWatch Logs / ログストレージ / CloudTrailログストレージに格納されており、サービス復旧によりログが消失することがないため、サービス復旧後の原因調査が可能である。



## バックアップ・リストア

本システム本番環境のバックアップ・リストアの方式を示す。

検証環境については検証目的でのみ利用する環境であるため、定期でのバックアップ取得については実施しない。

### バックアップ

暗号化方針については6.3暗号化方針を参照する。

日次バックアップはバッチ処理完了後に実施する。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 対象 | 保存期間 | スケジュール | バックアップ方式 | 一次バックアップ  保存先 | 二次バックアップ  保存先 |
| データベース  (DynamoDB) | 35日間 | 連続 | 増分バックアップ | 東京リージョン内  バックアップストレージ | 二次バックアップ不可 |
| 日次 | 完全バックアップ | 大阪リージョン内  バックアップストレージ |
| データストレージ(S3) | 日次 | 増分バックアップ |
| 認証基盤(Cognito) | 認証情報をDynamoDBで管理するため、認証基盤のバックアップは不要。 | | | | |

### リストア

一次バックアップ保存先にアクセス可能な場合は一次バックアップ保存先から復旧する。

東京リージョン障害発生時等、一次バックアップ保存先にアクセス不可の場合は二次バックアップ保存先から復旧する。

復旧時間についてはS3バケット間の転送速度は保証されていないため、「クロスリージョンのバケット間転送が30MB/s程度」の実測結果を参考に試算する。

#### 一次バックアップからのリストア

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 対象 | リストア方式 | 復旧時点 | 復旧時間 | 備考 |
| データベース  (DynamoDB) | AWSマネジメントコンソールより、データベースの復元処理を実行する。 | 35日以内の任意の時点 | 1時間未満 | DynamoDBのサービス指標により、95%のテーブルリストアが1時間未満で完了している。 |
| データストレージ  (S3) | AWSマネジメントコンソールより、データストレージの復元処理を実行する。 | バックアップ取得時点 | リストアデータ量10GBあたり6分程度 |  |

#### 二次バックアップからのリストア

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 対象 | リストア方式 | 復旧時点 | 復旧時間 | 備考 |
| データベース  (DynamoDB) | Data Pipelineにより、バックアップの復元処理を実行する。 | バックアップ取得時点 | バックアップデータ量10GBあたり6分程度  + 1時間未満 | DynamoDBのサービス指標により、95%のテーブルリストアが1時間未満で完了している。 |
| データストレージ  (S3) | AWSマネジメントコンソールより、データストレージの復元処理を実行する。 | バックアップ取得時点 | 差分データ量10GBあたり6分程度 |  |

## ジョブ管理

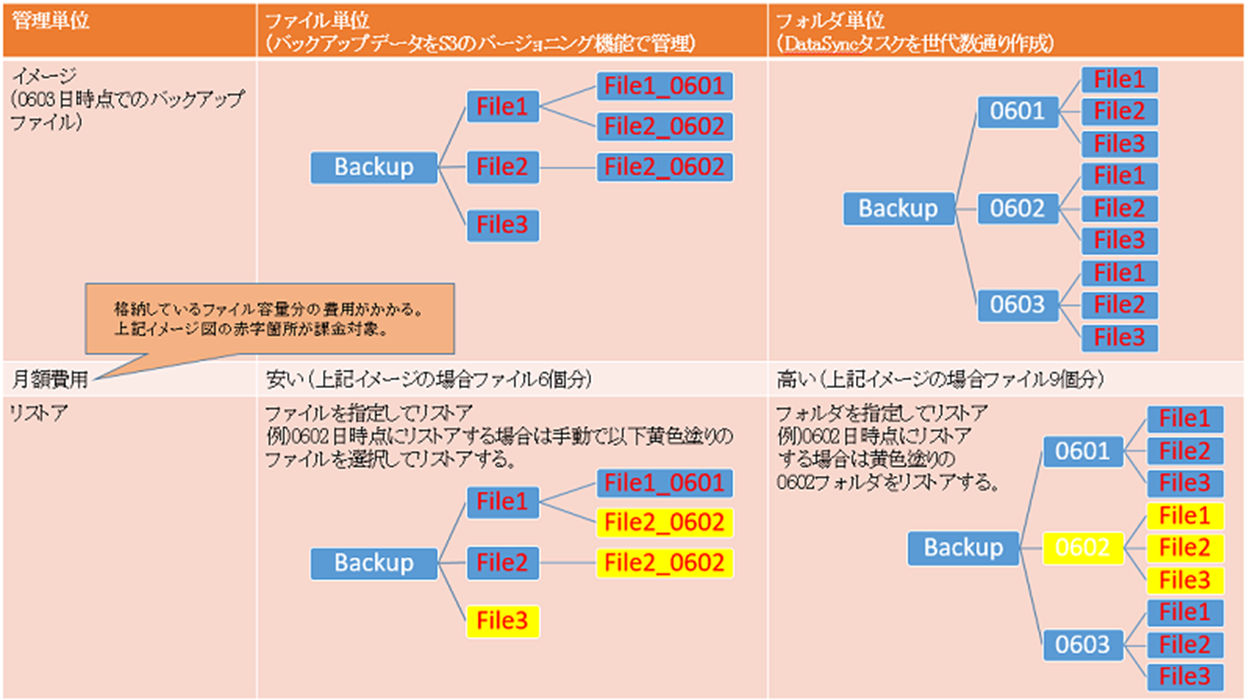
本システムのジョブ管理について記載する。

### ジョブ一覧

本システムでは以下のジョブを実行する。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 種別 | ジョブ | 内容 | 成功時 | 失敗時 |
| バックアップ | データベース(DynamoDB)の日次バックアップ | Data Pipelineによりデータベースのバックアップを取得する。 | ログ出力 | ログ出力  アラート通知 |
|  | データストレージ(S3)の日次バックアップ | DataSyncによりデータストレージを東京リージョン内バックアップストレージに同期する。  バックアップデータの世代管理方式として、ファイル単位とフォルダ単位があるが、AWS利用費が抑えられるファイル単位を採用する。  (以下表参照) | ログ出力 | ログ出力  アラート通知 |

データストレージ(S3)の日次バックアップの管理単位について



### ジョブ監視

本システムではジョブが失敗した際にメールによるアラート通知を行う。

|  |  |
| --- | --- |
| 通知先メールアドレス | 備考 |
| manaplus-alert@nichibun-g.co.jp | 秀学社様 |
| ml-shugakusha-support@sun-m.co.jp | サンエム保守窓口 |

## URL監視

本システムではCloudWatchにより本番環境のURLを監視する。

検証環境については業務影響がないためURL監視は実施しない。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | データ保持 |  |  |
| 対象 | スクリーンショット | スケジュール | タイムアウト | 障害データ | 成功データ | 監視実行データ保存先 |
| 本番環境URL | 取得しない | 10分おき | 1分 | 31日 | 31日 | ログストレージ(S3) |

本システムではURL監視が失敗した際にメールによるアラート通知を行う。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 期間 | 失敗回数 | 備考 |
| メール通知ルール | 1時間 | 2回 | 期間は右記から選択する。 (1時間 / 6時間 / 1日間) |
| 通知先メールアドレス | | | 備考 |
| manaplus-alert@nichibun-g.co.jp | | | 秀学社様 |
| ml-shugakusha-support@sun-m.co.jp | | | サンエム保守窓口 |

## リソース監視

本システムのリソース監視について記載する。

### リソース監視方式

本システムはCloudWatchサービスによりリソースを監視する。

### CloudWatchメトリクス保存期間

メトリクスの保存期間を示す。変更はできない。

|  |  |
| --- | --- |
| 期間 | 保存期間 |
| 60秒未満のデータポイント | 3時間 |
| 60秒(1分)のデータポイント | 15日間 |
| 300秒(5分)のデータポイント | 63日間 |
| 3600秒(1時間)のデータポイント | 455日間(15ヶ月) |

### リソース監視状況確認方法

本システムのリソース監視状況はAWSマネジメントコンソールのCloudWatchページで確認する。

### リソース監視項目

本システムのリソース監視項目をサービス別に記載する。

#### ACM

|  |  |
| --- | --- |
| メトリクス | 内容 |
| DaysToExpiry | 証明書の有効期限が切れるまでの日数。ACMは、証明書の有効期限が切れると、このメトリックの公開を停止する。 |

#### API Gateway

|  |  |
| --- | --- |
| メトリクス | 内容 |
| 4XXError | 指定された期間に取得されたクライアント側エラーの数。  Sum 統計は、このメトリクス、つまり、指定された期間内の 4XXError エラーの合計数を表す。Average 統計は、4XXError のエラー率、つまり、4XXError エラーの合計数をその期間のリクエストの合計数で割ったもの。分母は Count メトリクス (下記) に対応する。 |
| 5XXError | 指定された期間に取得されたサーバー側エラーの数。  Sum 統計は、このメトリクス、つまり、指定された期間内の 5XXError エラーの合計数を表す。Average 統計は、5XXError のエラー率、つまり、5XXError エラーの合計数をその期間のリクエストの合計数で割ったもの。分母は Count メトリクス (下記) に対応する。 |
| CacheHitCount | 指定された期間内に API キャッシュから配信されたリクエストの数。  Sum 統計は、このメトリクス、つまり、指定された期間内のキャッシュヒットの合計数を表す。Average 統計は、キャッシュヒット率、つまり、キャッシュヒットの合計数をその期間のリクエストの合計数で割ったもの。分母は Count メトリクス (下記) に対応する。 |
| CacheMissCount | API キャッシュが有効になっている特定の期間における、バックエンドから提供されたリクエストの数。  Sum 統計は、このメトリクス、つまり、指定された期間内のキャッシュミスの合計数を表す。Average 統計は、キャッシュミス率、つまり、キャッシュミスの合計数をその期間のリクエストの合計数で割ったもの。分母は Count メトリクス (下記) に対応する。 |
| Count | 指定された期間内の API リクエストの合計数。  SampleCount 統計は、このメトリクスを表す。 |
| IntegrationLatency | API Gateway がバックエンドにリクエストを中継してから、バックエンドからレスポンスを受け取るまでの時間。 |
| Latency | API Gateway がクライアントからリクエストを受け取ってから、クライアントにレスポンスを返すまでの時間。レイテンシーには、統合のレイテンシーおよびその他の API Gateway のオーバーヘッドが含まれる。 |

#### AWS WAF

|  |  |  |
| --- | --- | --- |
| 種別 | メトリクス | 内容 |
| Web ACL、ルールグループ、ルールメトリックス | AllowedRequests | 許可された、ウェブリクエストの数。  レポート条件 ゼロ以外の値がある。 |
|  | BlockedRequests | ブロックされたウェブリクエストの数。  レポート条件 ゼロ以外の値がある。 |
|  | CountedRequests | カウントされたウェブリクエストの数。  レポート条件 ゼロ以外の値がある。  カウントされたウェブリクエストは、少なくとも 1 つのルールに一致するリクエスト。リクエストカウントは、通常、テストに使用される。 |
|  | PassedRequests | 渡されたリクエストの数。これは、規則グループのどの規則にも一致しないで、規則グループの評価を通過する要求にのみ使用される。  レポート条件 ゼロ以外の値がある。  渡されたリクエストは、ルールグループのどのルールにも一致しないリクエスト。 |
| ラベルと AWS WAF ボットコントロールメトリックス | AllowedRequests | 許可アクション設定を持つルールによって Web リクエストに適用されたラベルの数。  レポート条件 ゼロ以外の値がある。 |
|  | BlockedRequests | ブロックアクション設定を持つルールによって Web リクエストに適用されたラベルの数。  レポート条件 ゼロ以外の値がある。 |
|  | CountedRequests | count アクション設定を持つルールによって Web リクエストに適用されるラベルの数。  レポート条件 ゼロ以外の値がある。 |
| 無料のボットの可視性指標 | SampleAllowedRequests | 許可アクションを持つサンプリングされたリクエストの割合。  レポート条件 ゼロ以外の値がある。 |
|  | SampleBlockedRequests | ブロックアクションを持つサンプリングされたリクエストの割合。  レポート条件 ゼロ以外の値がある。 |

#### CloudFront

デフォルトのメトリクスを監視対象とする。

追加のメトリクスとして以下が監視可能であるが、追加料金が必要となるためパフォーマンスに問題が生じた場合に監視の実施を検討する。

・キャッシュヒット率 / オリジンのレイテンシー / ステータスコード別のエラー率

|  |  |
| --- | --- |
| メトリクス | 内容 |
| Requests | すべての HTTP メソッド、および HTTP リクエストと HTTPS リクエストの両方について CloudFront が受信したビューワーリクエストの総数。 |
| Bytes downloaded | GET リクエスト、HEAD リクエスト、および OPTIONS リクエストに対してビューワーがダウンロードしたバイト総数 |
| Bytes uploaded | POST リクエストと PUT リクエストを使用して CloudFront でビューワーがオリジンにアップロードしたバイト総数 |
| 4xx error rate | レスポンスの HTTP ステータスコードが 4xx であるすべてのビューワーリクエストの割合 |
| 5xx error rate | レスポンスの HTTP ステータスコードが 5xx であるすべてのビューワーリクエストの割合 |
| Total error rate | レスポンスの HTTP ステータスコードが 4xx または 5xx であるすべてのビューワーリクエストの割合 |

#### Cognito

|  |  |
| --- | --- |
| メトリクス | 内容 |
| SignUpSuccesses | Amazon Cognito ユーザープールに対して成功したユーザー登録リクエストの総数を提供する。成功したユーザー登録リクエストでは値 1 を生成し、失敗したリクエストでは値 0 を生成する。スロットリングされたリクエストも失敗したリクエストと見なされるため、スロットリングされたリクエストも 0 のカウントを生成する。  成功したユーザー登録リクエストの割合を調べるには、このメトリクスの Average 統計を使用する。ユーザー登録リクエストの合計数をカウントするには、このメトリクスの Sample Count 統計を使用する。成功したユーザー登録リクエストの合計数をカウントするには、このメトリクスの Sum 統計を使用する。失敗したユーザー登録リクエストの合計数をカウントするには、CloudWatch を使用する。Math式を減算し、Sumの統計をSample Countの統計情報を使用する。  このメトリックは、各ユーザー・プール・クライアントのユーザー・プールごとに発行される。ユーザー登録が管理者によって実行された場合、メトリクスはユーザープールクライアントで管理する。  このメトリクスは、ユーザーインポートおよびユーザー移行の場合には発行されない。 |
| SignUpThrottles | Amazon Cognito ユーザープールに対してスロットリングされたユーザー登録リクエストの総数を提供する。ユーザー登録リクエストがスロットリングされるたびに、カウント 1 が発行される。  スロットリングされたユーザー登録リクエストの合計数をカウントするには、このメトリクスの Sum 統計を使用します。  このメトリックは、各クライアントのユーザー・プールごとに発行されます。スロットリングされたリクエストが管理者によって行われた場合、メトリクスはユーザープールクライアントで管理する。 |
| SignInSuccesses | Amazon Cognito ユーザープールに対して成功したユーザー認証リクエストの総数を提供する。認証トークンがユーザーに発行されると、ユーザー認証は成功したとみなされる。認証が成功すると値 1 が生成され、リクエストが失敗すると値 0 が生成される。スロットリングされたリクエストも失敗したリクエストと見なされるため、スロットリングされたリクエストも 0 のカウントを生成する。  成功したユーザー認証リクエストの割合を調べるには、このメトリクスの Average 統計を使用する。ユーザー認証リクエストの合計数をカウントするには、このメトリクスの Sample Count 統計を使用する。成功したユーザー認証リクエストの合計数をカウントするには、このメトリクスの Sum 統計を使用する。失敗したユーザー認証リクエストの合計数をカウントするには、Math式を減算し、Sumの統計をSample Countの統計情報を使用する。  このメトリックは、各クライアントのユーザー・プールごとに発行される。無効なユーザープールクライアントがリクエストで提供された場合、メトリクスの対応するユーザープールクライアント値には、固定値Invalidリクエストで送信された実際の無効な値の代わりに提供する。  Amazon Cognito トークンの更新リクエストは、このメトリクスには含まれないことに注意する。TokenRefreshSuccessesにより提供する。 |
| SignInThrottles | Amazon Cognito ユーザープールに対してスロットリングされたユーザー認証リクエストの総数を提供する。認証リクエストがスロットリングされるたびに、カウント 1 が発行される。  スロットリングされたユーザー認証リクエストの合計数をカウントするには、このメトリクスの Sum 統計を使用する。  このメトリックは、各クライアントのユーザー・プールごとに発行される。無効なユーザープールクライアントがリクエストで提供された場合、メトリクスの対応するユーザープールクライアント値には、固定値Invalidリクエストで送信された実際の無効な値の代わりに提供する。  Amazon Cognito トークンの更新リクエストは、このメトリクスには含まれない。TokenRefreshThrottlesにより提供する。 |
| TokenRefreshSuccesses | Amazon Cognito ユーザープールに対して実行された Amazon Cognito トークンの更新に成功したリクエストの合計数を提供する。Amazon Cognito トークンの更新リクエストが成功すると、値 1 が生成されます。一方、失敗したリクエストでは 0 が生成される。スロットリングされたリクエストも失敗したリクエストと見なされるため、スロットリングされたリクエストも 0 のカウントを生成する。  Amazon Cognito トークンの更新リクエストの割合を調べるには、Averageこのメトリクスの [] の統計を表示する。Amazon Cognito トークンの更新リクエストの合計数をカウントするには、Sample Countこのメトリクスの [] の統計を表示する。Amazon Cognito トークンの更新リクエストの合計数をカウントするには、Sumこのメトリクスの [] の統計を表示する。Amazon Cognito トークンの更新に失敗したリクエストの総数をカウントするには、CloudWatch を使用する。Math式を減算し、Sumの統計をSample Countの統計情報を提供する。  このメトリクスは、各ユーザープールクライアントごとに発行される。無効なユーザープールクライアントが要求内にある場合、ユーザープールクライアントの値には固定値Invalidが入る。 |
| TokenRefreshThrottles | Amazon Cognito ユーザープールに対して実行された Amazon Cognito トークン更新のスロットリングされたリクエストの合計数を提供する。Amazon Cognito トークンの更新リクエストがスロットリングされるたびに、カウント 1 が発行される。  Amazon Cognito トークンの更新のスロットリングされたリクエストの合計数をカウントするには、Sumこのメトリクスの統計を表示する。  このメトリックは、各クライアントのユーザー・プールごとに発行される。無効なユーザープールクライアントがリクエストで提供された場合、メトリクスの対応するユーザープールクライアント値には、リクエストで送信された実際の無効な値の代わりに固定値Invalidが入る。 |
| FederationSuccesses | Amazon Cognito ユーザープールに対して成功した ID フェデレーションリクエストの総数を提供する。ID フェデレーションリクエストが成功すると値 1 が生成され、失敗すると値 0 が生成される。スロットリングされたリクエストも失敗したリクエストと見なされるため、スロットリングされたリクエストも 0 のカウントを生成する。  成功した ID フェデレーションリクエストの割合を調べるには、このメトリクスの Average 統計を使用する。ID フェデレーションリクエストの合計数をカウントするには、このメトリクスの Sample Count 統計を使用する。成功した ID フェデレーションリクエストの合計数をカウントするには、このメトリクスの Sum 統計を使用する。失敗した ID フェデレーションリクエストの合計数をカウントするには、Math式を減算し、Sumの統計をSample Countの統計情報を使用する。 |
| FederationThrottles | Amazon Cognito ユーザープールに対してスロットリングされた ID フェデレーションリクエストの総数を提供する。ID フェデレーションリクエストがスロットリングされるたびに、カウント 1 が発行される。  スロットリングされた ID フェデレーションリクエストの合計数をカウントするには、このメトリクスの Sum 統計を使用する。 |
| CallCount | カテゴリに関連して顧客が発信したコールの総数を示す。このメトリックには、スロットル・コール、失敗したコール、成功したコールなど、すべてのコールが含まれる。  このメトリクスは、使用状況を表す。  カテゴリクォータは、アカウントおよびリージョンのすべてのユーザープールにわたって、各 AWS アカウントに対して適用される。  カテゴリ内のコールの合計数をカウントするには、Sumこのメトリクスの [] の統計を表示する。 |
| ThrottleCount | カテゴリに関連するスロットリングされたコールの総数を提供する。  このメトリクスは、使用状況を表す。  このメトリックは、アカウント・レベルで発行される。  カテゴリ内のコールの合計数を数えるには、Sumこのメトリクスの [] の統計を表示す。 |

#### DataSync

|  |  |
| --- | --- |
| メトリクス | 内容 |
| BytesVerifiedSource | 送信元の場所で検証されたデータの合計バイト数。 |
| BytesPreparedSource | 送信元の場所で準備されたデータの合計バイト数。 |
| FilesVerifiedSource | 送信元の場所で検証されたファイルの合計数。 |
| FilesPreparedSource | 送信元の場所で準備されたファイルの合計数。 |
| BytesVerifiedDestination | 送信先の場所で検証されたデータの合計バイト数。 |
| BytesPreparedDestination | 送信先の場所で準備されたデータの合計バイト数。 |
| FilesVerifiedDestination | 送信先の場所で検証されたファイルの合計数。 |
| FilesPreparedDestination | 送信先の場所で準備されたファイルの合計数。 |
| FilesTransferred | ネットワーク経由で転送された実際のファイル数またはメタデータ。この値は、計算され、TRANSFERRING (転送中) フェーズに継続的に更新される。これは、各ファイルが送信元の場所から読み取られるごとに定期的に更新され、ネットワーク経由で送信さる。  転送中に障害が発生した場合、この値は EstimatedFilesToTransfer 未満になることがある。場合によっては、この値は EstimatedFilesTransferred より大きくなることもある。一部の場所タイプではこの要素が実装固有であるため、正確なファイル数あるいはタスク実行のモニタリングのインジケータとしてはこれを使用しない。 |
| BytesTransferred | エージェントが送信元の場所から送信先の場所に読み込む際に、ネットワーク経由で転送された合計バイト数。 |
| BytesWritten | 送信先の場所に転送されたすべてのファイルの合計論理サイズ。 |

#### DynamoDB

|  |  |
| --- | --- |
| メトリクス | 内容 |
| AccountMaxReads | アカウントで使用できる読み込みキャパシティーユニットの最大数。この制限は、オンデマンドテーブルまたはグローバルセカンダリインデックスには適用されない。 |
| AccountMaxTableLevelReads | アカウントのテーブルまたはグローバルセカンダリインデックスで使用できる読み込みキャパシティーユニットの最大数。オンデマンドテーブルの場合、この制限は、テーブルまたはグローバルセカンダリインデックスで使用できる読み取り要求ユニットの最大上限。 |
| AccountMaxTableLevelWrites | アカウントのテーブルまたはグローバルセカンダリインデックスで使用できる書き込みキャパシティーユニットの最大数。オンデマンドテーブルの場合、この制限は、テーブルまたはグローバルセカンダリインデックスで使用できる書き込み要求ユニットの最大上限。 |
| AccountMaxWrites | アカウントで使用できる書き込みキャパシティーユニットの最大数。この制限は、オンデマンドテーブルまたはグローバルセカンダリインデックスには適用されない。 |
| AccountProvisionedReadCapacityUtilization | アカウントがプロビジョンド読み込みキャパシティ単位の割合(%)。 |
| AccountProvisionedWriteCapacityUtilization | アカウントがプロビジョンド書き込みキャパシティ単位の割合(%)。 |
| AgeOfOldestUnreplicatedRecord | Kinesis データストリームにレプリケートされていないレコードからの経過時間。 |
| ConditionalCheckFailedRequests | 条件付き書き込みの実行に失敗した回数。PutItem、UpdateItem, およびDeleteItem操作を使用すると、操作を続行する前に true と評価する必要がある論理条件を指定できる。この条件が false に評価される場合は、ConditionalCheckFailedRequestsは 1 ずつインクリメントされる。ConditionalCheckFailedRequestsは、論理条件が提供され、その条件がfalseと評価されるPartiQL UpdateおよびDeleteステートメントでも1つずつインクリメントされる。 |
| ConsumedChangeDataCaptureUnits | 消費されたチェンジ・データ・キャプチャ・ユニットの数。 |
| ConsumedReadCapacityUnits | 指定された期間に消費された読み込みキャパシティーユニットの数。プロビジョニングされたスループットの使用量を追跡できる。テーブルとそのすべてのグローバルセカンダリインデックス、または特定のグローバルセカンダリインデックスの消費された読み込みキャパシティーの合計を取得できる。詳細については、「読み込み/書き込みキャパシティーモード」を参照する。 |
| ConsumedWriteCapacityUnits | 指定された期間に消費された読み込みキャパシティーユニットの数。プロビジョニングされたスループットの使用量を追跡できる。テーブルとそのすべてのグローバルセカンダリインデックス、または特定のグローバルセカンダリインデックスの消費された読み込みキャパシティーの合計を取得できる。詳細については、「読み込み/書き込みキャパシティーモード」を参照する。 |
| MaxProvisionedTableReadCapacityUtilization | プロビジョニングされた読み取りキャパシティーユニットのうち、アカウントの最も高いプロビジョニングされた読み取りテーブルまたはグローバルセカンダリインデックスが使用している割合。 |
| MaxProvisionedTableWriteCapacityUtilization | プロビジョニングされた書き込みキャパシティーのうち、アカウントの最も高いプロビジョニングされた書き込みテーブルまたはグローバルセカンダリインデックスが使用している割合。 |
| OnlineIndexConsumedWriteCapacity | 新しいグローバルセカンダリインデックスをテーブルに追加するときに消費される書き込みキャパシティーユニットの数。インデックスの書き込みキャパシティが低すぎると、バックフィル・フェーズ中の書き込みアクティビティが抑制される可能性がある。これにより、インデックスの作成に要する時間が増える。インデックスの作成中にこの統計を監視して、インデックスの書き込みキャパシティーがプロビジョニングされていないかどうかを判断する必要がある。  インデックスの書き込み容量を調整するには、UpdateTable操作は、インデックスがまだ構築されている間でも同様。  ConsumedWriteCapacityUnitsメトリックには、インデックスの作成中に消費される書き込みスループットは含まれない。 |
| OnlineIndexPercentageProgress | 新しいグローバルセカンダリインデックスがテーブルに追加されるときの完了率。DynamoDB は、まず新しいインデックスにリソースを割り当てて、次にテーブルの属性をインデックスにバックフィルする必要がある。大きなテーブルの場合、この処理には長時間かかる場合がある。DynamoDB がインデックスを構築する際の相対的な進行状況を表示するには、この統計を監視する必要がある。 |
| OnlineIndexThrottleEvents | 新しいグローバルセカンダリインデックスをテーブルに追加するときに発生する書き込みスロットルイベントの数。これらのイベントは、着信書き込みアクティビティがインデックスのプロビジョニングされた書き込みスループットを超えているため、インデックスの作成の完了に時間がかかることを示す。  インデックスの書き込み容量を調整するには、UpdateTable操作は、インデックスがまだ構築されている間でも同様。  WriteThrottleEventsメトリックには、インデックスの作成中に発生するスロットルイベントは含まれない。 |
| PendingReplicationCount | （グローバルテーブル用）  1 つのレプリカテーブルに書き込まれていても、グローバルテーブル内の別のレプリカにはまだ書き込まれていないアイテムの更新の数 |
| ProvisionedReadCapacityUnits | テーブルまたはグローバルセカンダリインデックスのプロビジョンド読み込みキャパシティー単位の数。 |
| ProvisionedWriteCapacityUnits | テーブルまたはグローバルセカンダリインデックスのプロビジョンド書き込みキャパシティー単位の数。 |
| ReadThrottleEvents | テーブルまたはグローバルセカンダリインデックスのプロビジョニングされた読み込みキャパシティーユニットを超える DynamoDB へのリクエスト。 |
| ReplicationLatency | (グローバルテーブル用)  更新された項目が 1 つのレプリカテーブルの DynamoDB ストリームに表示され、その項目がグローバルテーブルの別のレプリカに表示されるまでの経過時間。 |
| ReturnedBytes | Amazon DynamoDB Streamによって返されるバイト数。 |
| ReturnedItemCount | Query または Scan オペレーションの結果として返された項目数。  返された項目数は、評価された項目の数と同じであるとは限らない。たとえば、リクエストされたとするScanを指定したが、100個の項目を持つテーブルにFilterExpressionの結果を絞り込み、15項目しか返さないようにする。この場合、ScanオブジェクトにScanCountの 100 とCount15が返される。 |
| ReturnedRecordsCount | Amazon DynamoDB Streamによって返されるストリームレコードの数。 |
| SuccessfulRequestLatency | 指定した期間中に成功した DynamoDB または Amazon DynamoDB ストリームへのリクエスト数とリクエストが成功するまでの経過時間。SuccessfulRequestLatencyは DynamoDB または Amazon DynamoDB ストリーム内のアクティビティのみを反映し、ネットワークレイテンシーやクライアント側のアクティビティは考慮しない。 |
| SystemErrors | 指定された期間に HTTP 500 ステータスコードを生成する DynamoDB または Amazon DynamoDB ストリームへのリクエスト数。HTTP 500 は通常、内部サービスエラーを示す。 |
| TimeToLiveDeletedItemCount | 指定した期間中に存続期間 (TTL) によって削除されたアイテムの数。このメトリックは、表のTTL削除率を監視するのに役立つ。 |
| ThrottledPutRecordCount | Kinesis データストリームの容量が不足しているため、Kinesis データストリームへの複製に失敗したレコードの数。 |
| ThrottledRequests | リソース（テーブルやインデックスなど）のプロビジョニングされたスループット制限を超える DynamoDB へのリクエスト。ThrottledRequestsリクエスト内で任意のイベントがプロビジョニングされたスループット制限を超過した場合は 1 ずつ増加する。たとえば、グローバルセカンダリインデックスを持つテーブル内の項目を更新する場合、テーブルへの書き込みと各インデックスへの書き込みという複数のイベントが発生する。これらのイベントの 1 つまたは複数がスロットルされている場合、ThrottledRequestsは 1 ずつインクリメントされる。 |
| TransactionConflict | 同じ品目に対する同時要求間のトランザクション競合が原因で、品目レベルの要求が拒否された件数。 |
| UserErrors | 指定された期間に HTTP 400 ステータスコードを生成する DynamoDB または Amazon DynamoDB ストリームへのリクエスト数。  HTTP 400 は通常、無効なパラメータの組み合わせ、存在しないテーブルの更新の試み、不正なリクエスト署名など、クライアント側のエラーを示す。  このようなイベントはすべて、UserErrorsメトリクスをサポートする。 |
| WriteThrottleEvents | テーブルまたはグローバルセカンダリインデックスのプロビジョニングされた書き込みキャパシティーユニットを超える DynamoDB へのリクエスト数。  1 つのリクエストで複数のイベントが発生する可能性がある。たとえば、PutItemリクエストを 3 つのグローバルセカンダリインデックスを持つテーブルに対して実行すると、テーブル書き込みと 3 つのインデックス書き込みという 4 つのイベントが発生します。各イベントについてWriteThrottleEventsメトリックは、そのイベントがスロットルされている場合、1 ずつ増加する。単一のPutItemリクエストで、いずれかのイベントがスロットルされている場合、ThrottledRequestsまた 1 ずつ増える。BatchWriteItemを使用する場合、ThrottledRequests全体のメトリックBatchWriteItemは、個々のPutItemまたはDeleteItemイベントが調整される。 |

#### Kinesis Data Firehose

|  |  |  |
| --- | --- | --- |
| 種別 | メトリクス | 内容 |
| Amazon S3 への配信 | DeliveryToS3.Bytes | 指定された期間に Amazon S3 に配信されたバイト数。 |
|  | DeliveryToS3.DataFreshness | Kinesis Data Firehose の最も古いレコードの経過時間。この経過時間より古いレコードは S3 バケットに配信済み。 |
|  | DeliveryToS3.Records | 指定された期間に Amazon S3 に配信されたレコード数。 |
|  | DeliveryToS3.Success | すべての Amazon S3 put コマンドの合計に対する正常に実行された Amazon S3 put コマンドの合計。 |
|  | BackupToS3.Bytes | 指定された期間に バックアップがAmazon S3 に配信されたバイト数。Kinesis Data Firehose は、バックアップが有効になっているとき (データ変換も有効になっている場合にのみ可能) に、このメトリクスを送信する。 |
|  | BackupToS3.DataFreshness | バックアップに関するKinesis Data Firehose の最も古いレコードの経過時間。この経過時間より古いレコードは Amazon S3 バケットに配信済み。Kinesis Data Firehose は、バックアップが有効になっているとき (データ変換も有効になっている場合にのみ可能) に、このメトリクスを送信する。 |
|  | BackupToS3.Records | 指定された期間にバックアップが Amazon S3 に配信されたレコードの数。Kinesis Data Firehose は、バックアップが有効になっているとき (データ変換も有効になっている場合にのみ可能) に、このメトリクスを送信する。 |
|  | BackupToS3.Success | すべての Amazon S3 バックアップの put コマンドの合計に対する、成功したバックアップの Amazon S3 put コマンドの合計。Kinesis Data Firehose は、バックアップが有効になっているとき (データ変換も有効になっている場合にのみ可能) に、このメトリクスを送信する。 |
| - | ResourceCount | アカウントで実行されている指定されたリソースの数。リソースは、メトリクスに関連付けられたディメンションによって定義される。  このメトリクスで最も役に立つ統計は MAXIMUM 。これは、1 分間の期間中に使用されるリソースの最大数を表す。 |

#### KMS

|  |  |
| --- | --- |
| メトリクス | 内容 |
| SecondsUntilKeyMaterialExpiration | インポートしたキーマテリアルの有効期限までの残りの秒数。このメトリックスは、オリジンがEXTERNALキーマテリアルの有効期限が設定された このメトリクスで最も有用な統計は Minimum で、指定した統計期間のすべてのデータポイントの最小残り時間を示す。 |

#### Lambda

|  |  |  |
| --- | --- | --- |
| 種別 | メトリクス | 内容 |
| 呼び出しメトリクス | Invocations | 関数コードが実行された回数(成功した実行や関数エラーが発生した実行を含む)。呼び出しリクエストがスロットリングされた場合、呼び出しは記録されない。それ以外の場合は、呼び出しエラーになる。これは、請求対象リクエストの数に等しくなる。 |
|  | Errors | 関数エラーが発生した呼び出しの数。関数エラーには、コードによってスローされた例外と、Lambda ランタイムによってスローされた例外が含まれる。ランタイムは、タイムアウトや設定エラーなどの問題に対してエラーを返す。エラー率を計算するには、Errors の値を Invocations の値で割る。エラーメトリクスのタイムスタンプは、エラーが発生した時点ではなく、関数が呼び出された時間を反映していることに注意する。 |
|  | DeadLetterErrors | 非同期呼び出しの場合、Lambda がイベントをデッドレターキューに送信しようとしたが、失敗した回数。デッドレターエラーは、アクセス許可エラー、リソースの設定ミス、またはサイズ制限が原因で発生する可能性がある。 |
|  | DestinationDeliveryFailures | 非同期呼び出しの場合、Lambda がイベントを送信先に送信しようとしたが、失敗した回数。配信エラーは、アクセス許可エラー、リソースの設定ミス、またはサイズ制限が原因で発生する可能性がある。 |
|  | Throttles | スロットリングされた呼び出しリクエストの数。すべての関数インスタンスがリクエストを処理していて、スケールアップできる同時実行がない場合、Lambda は TooManyRequestsException を使用して追加のリクエストを拒否する。スロットリングされたリクエストやその他の呼び出しエラーは、Invocations または Errors としてカウントされない。 |
|  | ProvisionedConcurrencyInvocations | プロビジョニングされた同時実行で関数コードが実行される回数。 |
|  | ProvisionedConcurrencySpilloverInvocations | プロビジョニングされたすべての同時実行が使用されているときに、標準同時実行で関数コードが実行される回数。 |
| パフォーマンスメトリクス | Duration | 関数コードがイベントの処理に費やす時間。呼び出しの請求期間は、最も近いミリ秒に切り上げた Duration の値。 |
|  | PostRuntimeExtensionsDuration | 関数コードの完了後、拡張のためにランタイムがコードの実行に費やした累積時間。 |
|  | IteratorAge | ストリームから読み取るイベントソースマッピングの場合、イベントの最後のレコードの所要時間。所要時間は、ストリームがレコードを受信してから、イベントソースマッピングがイベントを関数に送信するまでの時間。 |
| 同時実行メトリクス | ConcurrentExecutions | イベントを処理している関数インスタンスの数。この数値がリージョンの同時実行クォータ、または関数で設定した予約済み同時実行制限に達すると、追加の呼び出しリクエストがスロットリングされる。 |
|  | ProvisionedConcurrentExecutions | プロビジョニングされた同時実行でイベントを処理している関数インスタンスの数。プロビジョニングされた同時実行数を割り当てたエイリアスまたはバージョンの呼び出しごとに、Lambda は現在のカウントを出力する。 |
|  | ProvisionedConcurrencyUtilization | バージョンまたはエイリアスの場合、ProvisionedConcurrentExecutions の値を、割り当て済みのプロビジョニングされた同時実行の合計量で割った値。たとえば、.5 は、割り当て済みのプロビジョニングされた同時実行数の 50% が使用中であることを示す。 |
|  | UnreservedConcurrentExecutions | 同時実行が予約されていない関数によって処理されているイベントの数。 |

#### Route53

|  |  |  |
| --- | --- | --- |
| 種別 | メトリクス | 内容 |
| ヘルスチェック | ChildHealthCheckHealthyCount | Route 53 がモニタリングしているヘルスチェック間で正常なヘルスチェックの数。 |
|  | ConnectionTime | Route 53 ヘルスチェッカーがエンドポイントとの TCP 接続を確立するのにかかった平均時間。ヘルスチェックの ConnectionTime は、すべてのリージョンまたは選択した地理的リージョンについて確認できる。 |
|  | HealthCheckPercentageHealthy | Route 53 ヘルスチェッカーが選択したエンドポイントを正常であるとみなす割合。HealthCheckPercentageHealthy は、すべてのリージョンについてのみ確認できる (選択したリージョンについてのデータは表示できない)。 |
|  | HealthCheckStatus | Route53がチェックしているヘルスチェックエンドポイントのステータス。1 は正常、0 は異常を示します。HealthCheckStatus は、すべてのリージョンについてのみ確認できる (選択したリージョンについてのデータは表示できない)。 |
|  | SSLHandshakeTime | Route 53 ヘルスチェッカーが SSL ハンドシェイクを完了するまでにかかった平均時間。ヘルスチェックの SSLHandshakeTime は、すべてのリージョンまたは選択した地理的リージョンについて確認できる。 |
|  | TimeToFirstByte | Route 53 ヘルスチェッカーが HTTP または HTTPS リクエストへの応答の先頭バイトを受け取るまでにかかった平均時間。ヘルスチェックの TimeToFirstByte は、すべてのリージョンまたは選択した地理的リージョンについて確認できる。 |
| ホストゾーン | DNSQueries | ホストゾーン内のすべてのレコードについて、指定された期間に Route 53 が応答する DNS クエリの数。 |
|  | DNSSECInternalFailure | ホストゾーン内のオブジェクトが INTERNAL\_FAILURE 状態の場合、値は 1 。それ以外の場合、値は 0 。 |
|  | DNSSECKeySigningKeysNeedingAction | ACTION\_NEEDED 状態 (KMS の障害のため) を持つキー署名キー (KSKs) の数。 |
|  | DNSSECKeySigningKeyMaxNeedingActionAge | キー署名キー (KSK) が ACTION\_NEEDED 状態に設定されてから経過した時間。 |
|  | DNSSECKeySigningKeyAge | キー署名キー (KSK) が作成されてから経過した時間 (アクティブ化されてからではありません)。 |
| リゾルバーエンドポイント | InboundQueryVolume | インバウンドエンドポイント、またはIPアドレスを対象とし、EndpointId で指定されたエンドポイントを介してネットワークから VPC に転送された DNS クエリの数。 |
|  | OutboundQueryVolume | アウトバウンドエンドポイントを対象とし、EndpointId で指定されたエンドポイントを介して VPC からネットワークに転送された DNS クエリの数。 |
|  | OutboundQueryAggregateVolume | アウトバウンドエンドポイント、またはIPアドレスを対象とし、、Amazon VPC からネットワークに転送された 以下を含むDNS クエリの総数。  ・EndpointId で指定されたエンドポイントを介して VPC からネットワークに転送された DNS クエリの数。  ・現在のアカウントが他のアカウントと リゾルバー ルールを共有する場合、EndpointId によって指定されたエンドポイントを介してネットワークに転送される、他のアカウントによって作成された VPC からのクエリ。 |
| リゾルバー IP アドレス | InboundQueryVolume | インバウンドエンドポイントの IP アドレスごとに、ネットワークから、指定された IP アドレスに転送された DNS クエリの数。各 IP アドレスは、IP アドレス ID で識別されます。この値は Route 53 コンソールを使用して取得できる。該当するエンドポイントのページの [IP アドレス] セクションで、[IP アドレス ID] 列を参照する。また、ListResolverEndpointIpAddresses を使用してプログラムで値を取得することもできる。 |
|  | OutboundQueryAggregateVolume | アウトバウンドエンドポイントの IP アドレスごとに、Amazon VPC からネットワークに転送された 以下を含むDNS クエリの総数。  ・指定された IP アドレスを使用して VPC からネットワークに転送された DNS クエリの数。  ・現在のアカウントが他のアカウントと リゾルバー ルールを共有する場合、指定された IP アドレスを介してネットワークに転送される、他のアカウントによって作成された VPC からのクエリ。  各 IP アドレスは、IP アドレス ID で識別される。この値は Route 53 コンソールを使用して取得できる。該当するエンドポイントのページの [IP アドレス] セクションで、[IP アドレス ID] 列を参照する。また、ListResolverEndpointIpAddresses を使用してプログラムで値を取得することもできる。 |

#### S3

|  |  |  |
| --- | --- | --- |
| 種別 | メトリクス | 内容 |
| 日次ストレージメトリクス | BucketSizeBytes | STANDARD ストレージクラス、INTELLIGENT\_TIERING ストレージクラス、標準低頻度アクセス (STANDARD\_IA) ストレージクラス、OneZone 低頻度アクセス (ONEZONE\_IA)、低冗長化ストレージ (RRS) クラス、ディープアーカイブストレージ (S3 Glacier Deep Archive)、または Glacier (GLACIER) ストレージクラスのバケットに保存されているデータの量 (バイト単位)。この値を計算するには、バケット内のすべてのオブジェクト (最新のオブジェクトと最新でないオブジェクトの両方) のサイズを合計する。これには、バケットに対するすべての不完全なマルチパートアップロードのすべてのパートのサイズも含める。 |
|  | NumberOfObjects | すべてのストレージクラスのバケットに保存されたオブジェクトの総数。この値を計算するには、バケット内のすべてのオブジェクト (最新のオブジェクトと最新でないオブジェクトの両方) と、バケットに対するすべての不完全なマルチパートアップロードの合計パート数をカウントする。 |
| リクエストメトリクス | AllRequests | タイプに関係なく、Amazon S3 バケットに対して行われた HTTP リクエストの総数。フィルタでメトリクス設定を使用している場合、このメトリクスはフィルタの要件を満たすバケット内のオブジェクトに対する HTTP リクエストのみを返す。 |
|  | GetRequests | Amazon S3 バケット内のオブジェクトに対して行われた HTTP GET リクエストの数。これには、リストオペレーションは含まれない。 |
|  | PutRequests | Amazon S3 バケット内のオブジェクトに対して行われた HTTP PUT リクエストの数。 |
|  | DeleteRequests | Amazon S3 バケットのオブジェクトに対して行われた HTTP DELETE リクエストの数。これには、複数オブジェクトの削除リクエストも含まれる。このメトリクスは、削除されるオブジェクトの数ではなくリクエストの数を示す。 |
|  | HeadRequests | Amazon S3 バケットに対して行われた HTTP HEAD リクエストの数。 |
|  | PostRequests | Amazon S3 バケットに対して行われた HTTP POST リクエストの数。 |
|  | SelectRequests | Amazon S3 バケットのオブジェクトに対して行われた Amazon S3 の SELECT Object Content リクエストの数。 |
|  | SelectBytesScanned | Amazon S3 バケットの Amazon S3 の SELECT Object Content リクエストでスキャンされたデータのバイト数。 |
|  | SelectBytesReturned | Amazon S3 バケットの Amazon S3 の SELECT Object Content リクエストで返されたデータのバイト数。 |
|  | ListRequests | バケットの内容をリストする HTTP リクエストの数。 |
|  | BytesDownloaded | Amazon S3 バケットに対する、レスポンスに本文が含まれるリクエストに対してダウンロードしたバイト数。 |
|  | BytesUploaded | Amazon S3 バケットに対する、リクエストボディを含むアップロードしたバイト数。 |
|  | 4xxErrors | Amazon S3 バケットに対して行われた、値が 0 または 1 の HTTP 4xx クライアントエラーステータスコードリクエストの数。average 統計はエラーレートを示し、sum 統計は各期間中のそのタイプのエラー数を示す。 |
|  | 5xxErrors | Amazon S3 バケットに対して行われた、値が 0 または 1 の HTTP 5xx サーバーエラーステータスコードリクエストの数。average 統計はエラーレートを示し、sum 統計は各期間中のそのタイプのエラー数を示す。 |
|  | FirstByteLatency | Amazon S3 バケットがリクエスト全体を受信してからレスポンスの返信が開始するまでのリクエストあたりの時間。 |
|  | TotalRequestLatency | 最初のバイトが受信されてから Amazon S3 バケットに最後のバイトが送信されるまでのリクエストあたりの経過時間。これには、FirstByteLatency には含まれない、リクエストボディの受信とレスポンス本文の送信にかかった時間が含まれる。 |
| レプリケーションメトリクス | ReplicationLatency | 特定のレプリケーションルールについて、レプリケート先リージョンがレプリケート元リージョンより遅れる最大秒数。 |
|  | BytesPendingReplication | 特定のレプリケーションルールについて、レプリケーションが保留中のオブジェクトの合計バイト数。 |
|  | OperationsPendingReplication | 特定のレプリケーションルールについて、レプリケーションが保留中のオペレーションの数。 |
| Outpostsメトリクス | OutpostTotalBytes | Outpost のプロビジョニングされた合計キャパシティー (バイト単位)。 |
|  | OutpostFreeBytes | お客様のデータを保存するために Outpost で使用可能な空きバイト数。 |
|  | BucketUsedBytes | 指定されたバケットのすべてのオブジェクトの合計サイズ。 |

#### SNS

|  |  |
| --- | --- |
| メトリクス | 内容 |
| NumberOfMessagesPublished | Amazon SNS トピックに対して発行されたメッセージ数 |
| NumberOfNotificationsDelivered | Amazon SNS トピックからそのトピックにサブスクライブしているエンドポイントに正常に配信されたメッセージ数。  配信の試行が成功するには、エンドポイントのサブスクリプションでメッセージが許可されている必要がある。サブスクリプションは、メッセージを受け入れます。フィルタポリシーがないか、b.) そのフィルタポリシーには、メッセージに割り当てられた属性と一致する属性が含まれている。サブスクリプションでメッセージが拒否された場合、配信の試行はこのメトリクスに対してカウントされない。 |
| NumberOfNotificationsFailed | Amazon SNS が配信に失敗したメッセージの数。  Amazon SQS、E メール、SMS、またはモバイルプッシュエンドポイントの場合、Amazon SNS がメッセージ配信の試行を停止すると、このメトリクスが 1 増分される。HTTP または HTTPS エンドポイントの場合、失敗した配信の試行がすべて、初回試行に続く再試行を含め、このメトリクスに対してカウントされる。その他のすべてのエンドポイントの場合、メッセージが配信されないと、カウントが 1 増加する (試行回数には関係ありません)。  サブスクリプションフィルタポリシーによって拒否されたメッセージは、このメトリクスに対してカウントされない。 |
| NumberOfNotificationsFilteredOut | サブスクリプションフィルタポリシーによって拒否されたメッセージの数。メッセージの属性がポリシーの属性と一致しない場合、フィルタポリシーによってメッセージは拒否される。 |
| NumberOfNotificationsFilteredOut-InvalidAttributes | メッセージの属性が無効であるため、たとえば属性の JSON 形式が正しくないため、サブスクリプションフィルタポリシーによって拒否されたメッセージの数 |
| NumberOfNotificationsFilteredOut-NoMessageAttributes | メッセージに属性がないため、サブスクリプションフィルタポリシーによって拒否されたメッセージの数 |
| NumberOfNotificationsRedrivenToDlq | デッドレターキューに移動されたメッセージの数 |
| NumberOfNotificationsFailedToRedriveToDlq | デッドレターキューに移動できなかったメッセージの数 |
| PublishSize | 発行されたメッセージのサイズ |
| SMSMonthToDateSpentUSD | 今月の始めから今日までの SMS メッセージの送信料金。  今月の始めから今日までの料金がアカウントの毎月の SMS 使用限度に近付いたことがわかるように、このメトリクスにアラームを設定できる。Amazon SNS が、SMS メッセージを送信するとこの限度を超えるコストが発生すると判断した場合、数分以内に SMS メッセージの発行が停止される。 |
| SMSSuccessRate | 正常な SMS メッセージ配信のレート。 |

### しきい値監視

本システムはサーバレス構成であり、利用する各種サービスは自動でスケールするため、しきい値監視は行わない。

運用上、問題が発生した場合にしきい値監視の実施を検討する。

## ログ管理

本システムのログはCloudWatch Logs、S3により管理する。

### ログ一覧

本システムのログ一覧を管理方式別に示す。

#### CloudWatch Logs管理ログ

CloudWatch Logsにより以下のログを管理する。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ログ確認方法 | AWSマネジメントコンソールCloudWatchページ | | | |
| 対象サービス | 対象ログ | ロググループ | リージョン | 備考 |
| API Gateway | アクセスログ | 本番環境：/aws/apigateway/manabiplus/prod/acclog  検証環境：/aws/apigateway/manabiplus/stg/acclog | 東京 |  |
|  | 実行ログ | API-Gateway-Execution-Logs\_<文字列>/<ステージ名> |  | 自動作成される。ロググループ名変更不可。 |
| Lambda |  | /aws/lambda/<Lambda関数名> |  |
| DataSync |  | 本番環境：/aws/datasync/manabiplus/prod/synclog  検証環境：/aws/datasync/manabiplus/stg/synclog |  |  |
| Route53 | 以下の情報を含むパブリック DNS クエリログ  ・リクエストされたドメインまたはサブドメイン  ・リクエストの日付と時刻  ・DNS レコードタイプ (A や AAAA など)  ・DNS クエリに応答した Route 53 エッジロケーション  ・DNS レスポンスコード (NoError や ServFail など) | 本番環境：/aws/route53/manabiplus/prod/dnsquerylog  検証環境：/aws/route53/manabiplus/stg/dnsquerylog | バージニア北部 | ロググループは、米国東部（バージニア北部） リージョンにある必要がある。 |
| ACM  API Gateway  AWS WAF  CloudFront  CloudWatch  Cognito  Data Pipeline  DataSync  DynamoDB  Kinesis Data Firehose  KMS  Lambda  Route53  S3  SNS | 操作ログ(90日以上前のログ) | 本番環境：/aws/cloudtrail/manabiplus/prod/operationlog  本番環境：/aws/cloudtrail/manabiplus/stg/operationlog | 東京 |  |

#### CloudTrail管理ログ

CloudTrailにより以下のログを管理する。

|  |  |
| --- | --- |
| ログ確認方法 | AWSマネジメントコンソールCloudTrailページ |
| 対象サービス | 対象ログ |
| ACM  API Gateway  AWS WAF  CloudFront  CloudWatch  Cognito  Data Pipeline  DataSync  DynamoDB  Kinesis Data Firehose  KMS  Lambda  Route53  S3  SNS | 操作ログ  (90日前までのログ) |

#### ログストレージ(S3)管理ログ

S3により以下のログを管理する。

|  |  |  |  |
| --- | --- | --- | --- |
| ログ確認方法 | AWSマネジメントコンソールS3ページのS3 Selectクエリ | | |
| 対象サービス | 対象ログ | プレフィクス | 備考 |
| AWS WAF | 以下の情報を含むWebACLトラフィック情報のログ  ・リクエストを受信した時間  ・リクエストの詳細  ・リクエストが一致したルールのアクション | awswaf/ | Kinesis Data Firehoseでログ収集する。 |
| CloudFront | アクセスログ | 6.4.2CloudFront参照 |  |
| Data Pipeline | 実行ログ | datapipeline/<テーブル名> |  |
| S3 | アクセスログ | 2.3.3ストレージ(S3)参照 | バケットに対するリクエストの詳細 |

### ログ保存期間

IPAが発表した企業における情報システムのログ管理に関する実態調査によると、一般的にはログの保存期間は1年程度が妥当である。

本システムでは同時期のログを2年間まで遡って確認可能とするため、ログの保存期間を以下とする。

|  |  |  |
| --- | --- | --- |
| ログ格納先 | ログ保存期間 | 備考 |
| CloudWatch Logs | 24ヶ月 | 25ヶ月が設定できないため、24ヶ月とする。 |
| S3 | 25ヶ月 |  |

### ログ監視

本システムのログ監視については、運用上問題が発生した場合に実施を検討する。

## 時刻同期

本システムが利用する各種サービスはAWSグローバルインフラストラクチャにより時刻同期する。

## ソフトウェアのアップデート

本システムのソフトウェアはすべてAWSマネージドサービスを利用し、ソフトウェアのアップデートはAWSに一任する。

# セキュリティ

## ユーザー管理

以下のユーザーを作成する。

|  |  |  |  |
| --- | --- | --- | --- |
| ユーザー | 管理ポリシー | 権限 | 備考 |
| manabiplus-cfnuser | AmazonAPIGatewayAdministrator | API Gateway管理 |  |
| (CloudFormation管理ユーザー) | AmazonCognitoPowerUser | Cognito管理 |  |
|  | AmazonDynamoDBFullAccess | DynamoDB管理 |  |
|  | AmazonElasticMapReduceFullAccess | EMR管理 |  |
|  | AmazonEventBridgeFullAccess | EventBridge管理 |  |
|  | AmazonKinesisFirehoseFullAcces | ログ収集管理 |  |
|  | AmazonRoute53FullAccess | Route53管理 |  |
|  | AmazonS3FullAccess | S3管理 |  |
|  | AWSCertificateManagerFullAccess | ACM管理 |  |
|  | AWSCloudFormationFullAccess | CloudFormation管理 |  |
|  | AWSCloudTrail\_FullAccess | CloudTrail管理 |  |
|  | AWSDataPipeline\_FullAccess | DynamoDBバックアップ管理 |  |
|  | AWSDataSyncFullAccess | データストレージバックアップ管理 |  |
|  | AWSLambda\_FullAccess | Lambda管理 |  |
|  | AWSWAFFullAccess | AWS WAF管理 |  |
|  | CloudFrontFullAccess | CloudFront管理 |  |
|  | CloudWatchFullAccess | CloudWatch管理 |  |
|  | IAMFullAccess | 権限管理 |  |
| manabiplus-operator | AmazonS3FullAccess | ログ確認、データストレージリストア | リソースグループのタグにより対象のリソースを限定する。 |
| (運用ユーザー) | AWSCloudTrail\_FullAccess | ログ確認 |
|  | CloudWatchFullAccess |  |
|  | AWSDataPipeline\_FullAccess | DynamoDBバックアップ・リストア |
|  | AWSDataSyncFullAccess | データストレージバックアップ |
| manabiplus-developer | AmazonS3FullAccess | Lambdaコード管理 |
| (アプリケーション開発ユーザー) | AmazonAPIGatewayAdministrator | API Gateway管理 |

## ロール管理

各種サービスに以下のロールを付与する。

|  |  |  |
| --- | --- | --- |
| サービス | 権限 | 備考 |
| AWS WAF | Firehose書き込み | ログをS3に書き込むため |
| Lambda | DynamoDB接続 |  |
| (Webサーバー用) | CloudWatchLogs書き込み | ログをCloudWatch Logsに書き込むため |
| Lambda | CloudWatchLogs書き込み | ログをCloudWatch Logsに書き込む |
| (ウィルス対策用) | S3バケット一覧表示 | ウィルススキャンを実行するため |
|  | S3タグ付け | ウィルススキャン判定結果を書きこむ |
| API Gateway | CloudWatchLogs書き込み | ログをCloudWatch Logsに書き込むため |
| DataSync | S3読み書き | データバックアップ実行のため |
| Data PipeLine | EC2管理 | DynamoDBバックアップ実行のため |
|  | EMR管理 |  |
| DyanmoDB | オートスケール | DynamoDBがオートスケールするため |
|  | CloudWatchLogsFullAccess | CloudWatchLogsにログを書きこむため |
| CloudTrail | CloudWatchLogs書き込み | ログをCloudWatch Logsに書き込むため。 |
| Route53 | CloudWatchLogs書き込み | ログをCloudWatch Logsに書き込むため。 |

## 暗号化方針

本システムの暗号化方針について記載する。

### データベース(DynamoDB)

|  |  |  |
| --- | --- | --- |
| テーブル名 | 暗号化 | 備考 |
| schools | デフォルトの暗号化 | 機密データが含まれるため暗号化する。 |
| users |  |  |
| textbooks |  |  |
| licenses\_schools |  |  |
| app\_properties |  |  |
| login\_id\_seq |  |  |

### ストレージ(S3)

|  |  |  |  |
| --- | --- | --- | --- |
| ストレージ種別 | 暗号化 | 暗号化キータイプ | 備考 |
| Webサイト | 無効 | - | 機密データが含まれないため暗号化不要。 |
| データストレージ | 有効 | Amazon S3 キー (SSE-S3) | 機密データが含まれるため暗号化する。 |
| アプリケーションストレージ | 無効 | - | 機密データが含まれないため暗号化不要。 |
| バックアップストレージ | 有効 | Amazon S3 キー (SSE-S3) | 機密データが含まれるため暗号化する。 |
| ログストレージ | 有効 | Amazon S3 キー (SSE-S3) |  |
| CloudTrailログストレージ | 有効 | Amazon S3 キー (SSE-S3) |  |

### 認証基盤(Cognito)

|  |  |
| --- | --- |
| 暗号化 | 備考 |
| 有効 | 機密データが含まれるため暗号化する。  デフォルトで暗号化される。 |

### バックアップデータ

|  |  |  |
| --- | --- | --- |
| 対象 | 暗号化 | 備考 |
| データベース(DynamoDB) | 有効 | 機密データが含まれるため暗号化する。 |
| データストレージ(S3) | 有効 |  |

## Webアクセス

本システムでは以下のサービスを利用し、セキュアなWebアクセス環境を提供する。

### ACM

本システムではACMサービスにより以下のSSL証明書を発行する。

|  |  |
| --- | --- |
| 項目 | 設定値 |
| 証明書のタイプ | パブリック証明書 |
| ドメイン名 | 本番環境：manaplus-s.com  検証環境：manaplus-test.com |

ACMにより以下の特性を持つACM証明書を発行する。

|  |  |
| --- | --- |
| 特性 | 内容 |
| ドメイン検証 (DV) | ACM 証明書はドメイン検証される。 |
| 有効期間 | ACM 証明書の有効期間は 13 ヶ月 (395 日) |
| マネージド型更新とデプロイ | ACM は、ACM 証明書の更新プロセスと、更新後の証明書のプロビジョニングを管理し、証明書の設定ミス、失効、期限切れによるダウンタイムを防止する。 |
| ブラウザとアプリケーショントラスト | ACM証明書は、Google Chrome、Microsoft Internet Explorer と Microsoft Edge、そして Mozilla Firefox および Apple Safari を含むすべての主要なブラウザから信頼されている。 |
| 複数のドメイン名 | 各 ACM 証明書には、少なくとも 1 つの完全修飾ドメイン名 (FQDN) が含まれる必要があり、必要に応じて追加の名前を付け加えることができる。  (例) 「www.example.com」のACM 証明書に「example.com」 を追加 |
| ワイルドカード名 | ドメイン名にアスタリスク (\*) を使うことで、同じドメイン内の複数のサイトを保護できるワイルドカード名を含む ACM 証明書を作成することができる。 |
| アルゴリズム | 以下のパブリックキーアルゴリズムが ACM でサポートされている。  ・2048 ビット RSA (RSA\_2048)  ・4096 ビット RSA (RSA\_4096)  ・Elliptic Prime Curve 256 ビット (EC\_prime256v1)  ・Elliptic Prime Curve 384 ビット (EC\_secp384r1) |

### AWS WAF

AWS WAFを利用し、アプリケーションの可用性、セキュリティの侵害、リソースの過剰な消費などに影響を与えかねない一般的なウェブの弱点からシステムを保護する。本システムでは、絶えず変化する脅威に対して迅速な対応をとるためにAWSマネージドルールを適用する。

AWSマネージドルールでは新しい脆弱性と脅威が発生した場合、AWSによりルールグループが自動的に更新される。

検証環境ではAWSマネージドルールに一致するリクエストをカウント(監視)するのみとし、ブロックは行わない。

本番環境ではAWSマネージドルールに一致するリクエストをブロックする。

本番環境で正常なリクエストが意図せずブロックされた場合は検証環境でルールの調整と動作検証を行い、本番環境のルールを調整する。

ルールの優先順位についてはIPアドレスによるルール等、限定的な範囲に及ぶルールを優先とし、より低コストで攻撃をブロック可能とする。

|  |  |  |
| --- | --- | --- |
| 優先順位 | ルールグループ | 説明 |
| 1 | IP 評価ルールグループ | ボットトラフィック等、接続元に基づいてリクエストをブロックする。 |
| 2 | AWS WAF ボットコントロールルールグループ | 一般的なボットを分類して識別し、一般的に望ましいボットを検証し、ボットの信頼度の高い署名を検出することで、サイトに対するボットのアクティビティを管理する。 |
| 3 | ユースケース固有のルールグループ | さまざまな AWS WAF ユースケースに対して段階的な保護を提供する。 |
| 4 | ベースラインルールグループ | さまざまな一般的な脅威に対する一般的な保護を提供する |

AWSマネージドルールによるWebACLは以下の通り構成する。

|  |  |  |  |
| --- | --- | --- | --- |
| ルールグループ | ルールセット | 適用(優先順位) | 説明 |
| ベースラインルールグループ | コアルールセット | ○(5) | Webアプリケーションに一般的に適用すべきルールセット。高リスクの脆弱性や一般的な脆弱性など、幅広い脆弱性の悪用に対する保護が提供される。 |
|  | 管理者保護 | ×  サードパーティーのソフトウェアを実行しないため | 公開されている管理ページへの外部アクセスをブロックするためのルールセット。サードパーティーのソフトウェアを実行している場合や、悪意のある攻撃者がアプリケーションへの管理アクセスを得るリスクを軽減したい場合に適用する。 |
|  | 既知の不正な入力 | ○(4) | 無効であることがわかっており脆弱性の悪用または発見に関連するリクエストパターンをブロックするためのルールセット。悪意のある攻撃者が脆弱なアプリケーションを発見するリスクを軽減する。 |
| ユースケース固有のルールグループ | SQL データベース | ×  SQLデータベースを使用しないため | SQL インジェクション攻撃などの SQL データベースの悪用に関連するリクエストパターンをブロックするルールセット。これにより、不正なクエリのリモートインジェクションを防ぐことができる。アプリケーションが SQL データベースにアクセスする場合に適用する。 |
|  | Linux オペレーティングシステム | ×  LinuxOSを使用しないため | Linux 固有のローカルファイルインクルージョン (LFI) 攻撃など、Linux 固有の脆弱性の悪用に関連するリクエストパターンをブロックするルールセット。攻撃者がアクセスしてはならないファイルの内容を公開したり、コードを実行したりする攻撃を防ぐことができる。 |
|  | POSIX オペレーティングシステム | ×  POSIXOSを使用しないため | POSIX および POSIX と同等のオペレーティングシステムに固有の脆弱性の悪用 (ローカルファイルインクルージョン (LFI) 攻撃など) に関連するリクエストパターンをブロックするルールセット。攻撃者がアクセスしてはならないファイルの内容を公開したり、コードを実行したりする攻撃を防ぐことができる。 |
|  | Windows オペレーティングシステム | ×  WindowsOSを使用しないため | PowerShell コマンドのリモート実行など、Windows 固有の脆弱性の悪用に関連するリクエストパターンをブロックするルールセット。攻撃者が不正なコマンドを実行したり、悪意のあるコードを実行したりする脆弱性の悪用を防ぐことができる。 |
|  | PHP アプリケーション | ×  PHPを使用しないため | 安全でない PHP 関数のインジェクションなど、PHP プログラミング言語の使用に固有の脆弱性の悪用に関連するリクエストパターンをブロックするルールセット。 |
|  | WordPress アプリケーション | ×  WordPressを使用しないため | WordPress サイト固有の脆弱性の悪用に関連するリクエストパターンをブロックするルールセット。 |
| IP 評価ルールグループ | Amazon IP 評価リスト | ○(1) | Amazon 内部脅威インテリジェンスに基づくルールセット。ボットやその他の脅威に関連付けられている IP アドレスをブロックすることでボットを軽減し、悪意のある攻撃者が脆弱なアプリケーションを発見するリスクを軽減する。 |
|  | 匿名 IP リスト | ○(2) | VPN、プロキシ、Tor ノード、ホスティングプロバイダー (AWS を含む)など、ビューワーIDの難読化を許可するサービスからのリクエストをブロックするルールセット。アプリケーションから ID を隠そうとするビューワーをブロックし、ボットの軽減や地理的制限を回避する。 |
| AWS WAF ボットコントロールルールグループ | AWS WAF ボットコントロール | ○(3) | ボットからのリクエストをブロックして管理するルール。このルールグループを使用する場合は追加料金が必要となる。 |

### CloudFront

本システムではCDN(コンテンツデリバリーネットワーク)としてCloudFrontを利用することにより、キャッシュ機能によるオリジンサーバー（CloudFront がコンテンツを取得する元のウェブサーバー）の負荷軽減とコンテンツ配信のパフォーマンス向上を実現する。また、CloudFront はAWS Shield によるDDoS 保護機能が有効化されており、ネットワーク層およびトランスポート層のDDoS 攻撃に対する緩和が自動的に行われる。

S3の静的Webサイト向け、及びAPI Gateway向けのCloudFrontディストリビューションを作成する。

各ディストリビューションへはACMで管理するACM証明書、及びAWS WAFで作成したWebACLを設定する。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | 設定値 | |  |  |
| 項目 | | Webサイト向け | | API Gateway向け | 備考 |
| オリジンの設定 | |  | | |  |
|  | オリジンドメイン名 | Webサイト(S3) | | API の invoke URL | CloudFront がこのオリジンのオブジェクトの取得先としている Amazon S3 バケットまたは HTTP サーバーの DNS ドメイン名。 |
|  | オリジンのパス | (空白) | | | CloudFront で AWS リソースまたはカスタムオリジンのディレクトリにコンテンツがリクエストされるようにするには、スラッシュ (/) から始まるディレクトリパスを入力する。 |
|  | オリジンシールド | 無効 | | | オリジンの前に追加されるキャッシュレイヤー。「異なる地理的リージョンにビューワーが分散している場合」のユースケースに該当しないため無効にする。 |
|  | オリジンID | (自動入力) | | | デフォルトのキャッシュ動作に加えてキャッシュ動作を作成する場合、ここで指定した ID を使用して、そのキャッシュ動作のパスパターンにリクエストが一致した場合に CloudFront がリクエストをルーティングするオリジンまたはオリジングループを識別する。 |
|  | バケットアクセスの制限 | 無効 | | | CloudFront URL のみを使用して Amazon S3 バケット内のオブジェクトにアクセスするようユーザーに要求する場合は有効化する。 |
|  | オリジンへの接続試行回数 | 3 | | | CloudFront がオリジンへの接続を試行する回数。 |
|  | オリジンへの接続タイムアウト | 10 | | | オリジンへの接続を確立しようとするときに CloudFront が待機する秒数。 |
|  | オリジンカスタムヘッダー | (空白) | | | リクエストをオリジンに転送するときに CloudFront が常にカスタムヘッダーを追加するようにする。 |
| キャッシュ動作の設定 | |  | | |  |
|  | パスパターン | デフォルト | | | パスパターン (例: images/\*.jpg) を使用して、このキャッシュ動作をどのリクエストに割り当てるかを指定する。 |
|  | ビューワープロトコルポリシー | Redirect HTTP to HTTPS | | HTTPS Only | CloudFront エッジロケーションのコンテンツへのアクセスに使用するビューワーのプロトコルポリシーを選択する。 |
|  | 許可される HTTP メソッド | GET, HEAD | | GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE | CloudFront が処理してオリジンに転送する HTTP メソッドを指定する。 |
|  | フィールドレベル暗号化の設定 | (空白) | | | 特定のデータフィールドにフィールドレベル暗号化を適用する場合は、フィールドレベル暗号化の設定を選択する。 |
|  | キャッシュされる HTTP メソッド | GET, HEAD | | | ビューワーから OPTIONS リクエストが送信されたときに、オリジンからの応答を CloudFront でキャッシュするかどうかを指定する。 |
|  | キャッシュポリシー | Managed-CachingOptimized | | | CloudFront がコンテンツをキャッシュする方法を管理する。オリジンで再検証する前にオブジェクトをキャッシュする時間の設定（TTL）、CloudFront が HTTP ヘッダー、クエリ文字列パラメータおよび Cookie のパラメータによって変わるコンテンツをキャッシュする方法、および CloudFront が圧縮されたコンテンツをキャッシュする方法を制御する |
|  | オリジンリクエストポリシー | (空白) | | | オリジンへのリクエストが行われたとき（キャッシュミスまたは再検証）に CloudFront がリクエストタイムメタデータをオリジンに送信する方法を管理する、CloudFront がオリジンに送信するヘッダー、クエリ文字列パラメータ、Cookie を設定できる。 |
|  | スムーズストリーミング | 無効 | | | Microsoft Smooth Streaming 形式のメディアファイルを配信するが、IIS サーバーがない場合は、[Yes (はい)] を選択する。 |
|  | ビューワーのアクセス制限 (署名付き URL の使用) | 無効 | | | このキャッシュ動作の PathPattern に一致するオブジェクトのリクエストで署名付き URL を使用する場合、[Yes (はい)] を選択する。 |
|  | オブジェクトを自動的に圧縮する | 無効 | | | ビューワーが圧縮コンテンツをサポートしている場合に、特定のタイプのファイルを CloudFront で自動的に圧縮するには、[Yes (はい)] を選択する。CloudFront がコンテンツを圧縮する際、ファイルが小さいためダウンロードはより高速に行われ、ウェブページは高速にレンダリングされる。 |
|  | Lambda 関数の関連付け | (空白) | | | CloudFront イベントのトリガーを Lambda 関数に追加するに |
|  | リアルタイムログ | 無効 | | | ディストリビューションに対するリクエストの情報をリアルタイムで取得する |
| ディストリビューション設定 | |  | | |  |
|  | 価格クラス | 全てのエッジロケーション | | | CloudFront サービスに支払う上限価格に対応する価格クラスを選択する。 |
|  | AWS WAF ウェブACL | (作成したWebACL) | | | AWS WAF を使用して、指定した条件に基づいてリクエストを許可したりブロックしたりする場合は、このディストリビューションに関連付けられたウェブ ACL を選択する。 |
|  | 代替ドメイン名 (CNAME) | (ドメイン名) | | | ディストリビューションを作成するときに CloudFront が割り当てるドメイン名ではなく、オブジェクトの URL に使用する 1 つ以上のドメイン名を指定する。 |
|  | SSL証明書 | カスタムSSL証明書 | | | ディストリビューションで使用する代替ドメイン名を指定した場合は、[Custom SSL Certificate (カスタム SSL 証明書)] を選択してこの代替ドメイン名を使用する許可を検証し、これを対象とする証明書選択する。 |
|  | 独自 SSL クライアントのサポート | Server Name Indication (SNI) をサポートするクライアント | | | ディストリビューションに 1 つ以上の代替ドメイン名と独自 SSL 証明書を指定した場合は、CloudFront が HTTPS リクエストを処理する方法を選択する。とんどすべての最新のウェブブラウザとクライアントは、SNI をサポートしているため、ディストリビューションに接続できる。 |
|  | セキュリティポリシー | TLSv1.2\_2019 (recommended) | | | CloudFront がビューワー (クライアント) との HTTPS 接続に使用するセキュリティポリシーを指定する。 |
|  | サポートされる HTTP バージョン | HTTP/2, HTTP/1.1, HTTP/1.0 | | | ビューワーが CloudFront と通信するときにディストリビューションでサポートする HTTP バージョンを選択する。 |
|  | デフォルトのルートオブジェクト | XXXXX  ※アプリケーション要件確定後記載 | (空白) | | ビューワーがディストリビューション内のオブジェクト (http://www.example.com/product-description.html) ではなくディストリビューションのルート URL (http://www.example.com/) をリクエストするときに、CloudFront がリクエストする、オリジンからのオブジェクト (index.html など)。 |
|  | ログ記録 | 有効 | | | CloudFront がオブジェクトに対する各リクエストの情報をログに記録し、ログファイルを Amazon S3 バケットに保存する。 |
|  | ログ用のバケット | S3(ログストレージ) | | | ログ記録を有効にした場合にCloudFront がアクセスログを保存する Amazon S3 バケット |
|  | ログのプレフィックス | cf-website/ | cf-api/ | | ログ記録を有効した場合にこのディストリビューションのアクセスログファイル名の先頭に CloudFront が追加する文字列 (ある場合) を指定する。 (例: exampleprefix/)。末尾のスラッシュ (/) はオプションだが、ログファイルの参照を容易にするためにこれを使用することが推奨される。 |
|  | Cookie のログ作成 | 無効 | | | CloudFront で Cookie をアクセスログに含めるようにするには、有効を選択する。Amazon S3 は Cookie を処理しないため、S3がオリジンである場合は無効にする。 |
|  | IPv6 を有効にする | 有効 | | | 一般的に、IPv6 ネットワークのユーザーがいてコンテンツにアクセスする場合は、IPv6 を有効にする必要がある。ただし、コンテンツへのアクセスを制限するために署名付き URL または署名付き Cookie を使用していて、コンテンツへのアクセスが可能な IP アドレスを制限する IP アドレスを含む IpAddress パラメータを使用している場合、IPv6 は有効にしない。 |
|  | コメント | (空白) | | | ディストリビューションを作成するときに、最大で 128 文字のコメントを含めることができる。 |
|  | ディストリビューションの状態 | 有効 | | | ディストリビューションがデプロイされた後にディストリビューションを有効または無効のどちらにするか指定する。 |

### API Gateway

本システムでは、API の作成、公開、保守、モニタリング、保護のためにAPI Gatewayサービスを利用する。

以下にAPI Gatewayの非機能要件関連の定義を示す。機能要件についてはAPI一覧を参照する。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 項目 | | | | | | 設定値 | 備考 |
| API | | | | | |  |  |
|  | | APIタイプ | | | | REST API |  |
|  | | API名 | | | | manabiplus-api |  |
|  | | エンドポイントタイプ | | | | エッジ最適化 | CloudFrontからのみアクセスを許可する。 |
|  | | ステージ名 | | | | 本番環境：prod-manabiplus-stage  検証環境：stg-manabiplus-stage |  |
|  | |  | キャッシュ設定 | | | 無効 | パフォーマンスに問題が生じた場合に有効化を検討する。 |
|  | |  | デフォルトのメソッドスロットリング | | | 有効 | スループット向上のため、APIに対するリクエストのレートを制限する。 |
|  | |  |  | レート | | 10000 リクエスト数/秒 | リクエストの送信数がリクエストの定常レートおよびバーストを超えると、API Gateway は制限を超えたリクエストを失敗させ、クライアントに 429 Too Many Requests エラーレスポンスを返す。 |
|  | |  |  | バースト | | 5000 リクエスト数 |
|  | |  | ウェブアプリケーションファイアウォール (WAF) ウェブACL | | | なし | 前段のCloudFrontにWAFを設定するため、API GatewayではWAFを設定しない。 |
|  | |  | クライアント証明書 | | | なし  (バックエンドポイントとしてLambda関数のみを使用するため、クライアント証明書は不要) | API Gateway を使用して SSL 証明書を生成し、バックエンドでそのパブリックキーを使用して、バックエンドシステムへの HTTP リクエストが API Gateway からのものであることを確認する。 |
|  |  | | ログ/トレース | | |  |  |
|  | |  | CloudWatch設定 | | |  |  |
|  | |  |  | CloudWatchログを有効化 | | 有効 | 実行ログを取得する。 |
|  | |  |  |  | ログレベル | エラー | 情報レベルのログは取得しない。 |
|  | |  |  |  | リクエスト/レスポンスをすべてログ | 無効 | このログは API のトラブルシューティングに役立つが、機密データが記録される可能性があるため無効を推奨。 |
|  | |  |  | 詳細 CloudWatch メトリクスを有効化 | | 有効 | API Gatewayの監視を有効化する。 |
|  | |  | カスタムアクセスのログ記録 | | |  |  |
|  | |  |  | アクセスログの有効化 | | 有効 | API Gatewayのアクセスログを取得する。 |
|  | |  |  | Access Log Destination ARN | | ClouodWatchグループ |  |
|  | |  |  | ログの形式 | | CLF |  |
|  | |  | X-Ray トレース | | | 無効 | REST API から基盤となるサービスへのユーザーリクエストの流れをトレースして分析する |
|  |  | | ステージ変数 | | |  |  |
|  | |  | 名前 | | | ステージ変数なし |  |
|  | |  | 値 | | |  |  |
| オーソライザー | | | | | | Cognito | Amazon Cognito ユーザープールまたは Lambda 関数を使用して API へのアクセスを制御する。  ※アプリケーション要件確定後記載 |
|  | | トークンのソース | | | |  |
|  | | トークンの検証 | | | |  |
| ゲートウェイのレスポンス | | | | | |  |  |
|  | | アクセスが拒否されました | | | | レスポンスのステータスコード：403 |  |
|  | | API 設定エラー | | | | レスポンスのステータスコード：500 |  |
|  | | オーソライザー設定エラー | | | | レスポンスのステータスコード：500 |  |
|  | | オーソライザーエラー | | | | レスポンスのステータスコード：500 |  |
|  | | リクエスト本文が不正です | | | | レスポンスのステータスコード：400 |  |
|  | | リクエストパラメータが不正です | | | | レスポンスのステータスコード：400 |  |
|  | | DEFAULT 4XX | | | | - |  |
|  | | DEFAULT 5XX | | | | - |  |
|  | | 期限切れのトークン | | | | レスポンスのステータスコード：403 |  |
|  | | 統合の失敗 | | | | レスポンスのステータスコード：504 |  |
|  | | 統合のタイムアウト | | | | レスポンスのステータスコード：504 |  |
|  | | 無効な API キー | | | | レスポンスのステータスコード：403 |  |
|  | | 無効な署名 | | | | レスポンスのステータスコード：403 |  |
|  | | 認証トークンが見つかりません | | | | レスポンスのステータスコード：403 |  |
|  | | クォータを超過しました | | | | レスポンスのステータスコード：429 |  |
|  | | リクエストが大きすぎます | | | | レスポンスのステータスコード：413 |  |
|  | | リソースは存在しません | | | | レスポンスのステータスコード：404 |  |
|  | | スロットル済み | | | | レスポンスのステータスコード：429 |  |
|  | | 権限がありません | | | | レスポンスのステータスコード：401 |  |
|  | | サポートされていないメディアタイプ | | | | レスポンスのステータスコード：415 |  |
|  | | WAF フィルター | | | | レスポンスのステータスコード：403 |  |
| カスタムドメイン名 | | | | | | 設定しない | エッジ最適化APIを使用するため、ドメイン名はCloudFront ディストリビューションドメイン名を使用する。 |
| VPCリンク | | | | | | 設定しない | VPC 内のプライベートリソースに接続する場合設定する。 |

## ウィルス対策

本システムではデータストレージ(S3)にファイルをアップロードする際にアンチウィルスソフト(ClamAV)によるウィルススキャンを実施し、ウィルスチェックで正常判定が出るまで、オブジェクトを読み取り不可とする。ウィルスチェックで感染判定が出た場合は、ウィルスチェック完了後もオブジェクトを読み取り不可とし、判定結果の書き換えを禁止する。なお、オブジェクトの削除は許可する。

アンチウィルスソフト(ClamAV)の定義ファイルは1日に1回更新する。