運用手順書

AWS三層構成システム 運用手順書

ALB・EC2・RDS の監視・起動停止・障害一次対応

項目	内容
文書名	AWS三層構成システム 運用手順書
バージョン	1.0
作成日	2026-11-06
作成者	Nami
対象システム	AWS三層構成 Webアプリケーション（Work 01・Work 02 と同じ環境）
対象リージョン	アジアパシフィック（東京）ap-northeast-1
資料の区分	自主制作サンプル（ポートフォリオ用）
関連資料	Work 01「AWS三層構成アーキテクチャ図」・構成説明資料、Work 02「AWSパラメータシート」

この資料について

- 実際の業務案件で作成・使用したものではなく、ポートフォリオのために作った**自主制作のサンプル**です。
- **AWSアカウントへの構築や、この手順での動作確認は行っていません。** 操作の手順と画面の名前は、AWS公式ドキュメント（2026-11-06 時点）で確認した内容に基づいています。AWSの画面は変わることがあるため、実際に使うときは最新の画面と公式ドキュメントを確認してください。
- リソース名・CIDR・ポート番号などは Work 01・Work 02 の値に合わせています。インスタンスIDやAWSアカウントIDなど、実環境がないと決まらない値は記載していません。

文書の目的

この手順書は、AWS三層構成のWebシステムを**初めて運用する担当者**が、次の作業を安全に行えるようにするためのものです。

- 作業前の確認（アカウント・リージョン・権限・承認）
- EC2の起動と停止
- CloudWatchでの監視の確認
- アラームが発生したときの一次対応
- RDSの状態確認
- 障害時の情報の記録とエスカレーション

一次対応の範囲は「状況の確認・記録・報告」です。設定の変更や再起動などの操作は、原因と影響を確認し、**承認を得てから**行います。

値の表記

表記	意味
設計上の仮値	Work 01・Work 02 に記載がなく、説明のために仮に決めた値。実際に使う前に見直す
要確認	実環境や要件が決まらないと確定できない値。推測で値を入れていない
太字の **禁止**	この手順書の範囲では行ってはいけない操作
「」で囲んだ太字	画面のメニュー・ボタン・タブの名前。日本語表示のコンソールを想定し、AWS公式ドキュメント（英語）の名前から対応させたもの。英語の名前は「付録B」に記載。表示が異なる場合は、画面右上の設定で言語を英語に切り替えて確認する

改訂履歴

版	日付	内容	作成者	承認者
1.0	2026-11-06	初版作成（自主制作サンプル）	Nami	（記入欄）

目次

01. システム概要 4

02. 運用前の確認事項 7

03. EC2の起動・停止手順 9

04. CloudWatchの監視確認手順 12

05. アラーム発生時の一次対応 15

06. RDSの状態確認 18

07. 作業前後チェックリスト 21

08. 障害対応・エスカレーション 23

09. 運用上の注意事項・制約 26

付録A. 用語集 28

付録B. 画面の名前の対応（日本語表示／英語表示） 29

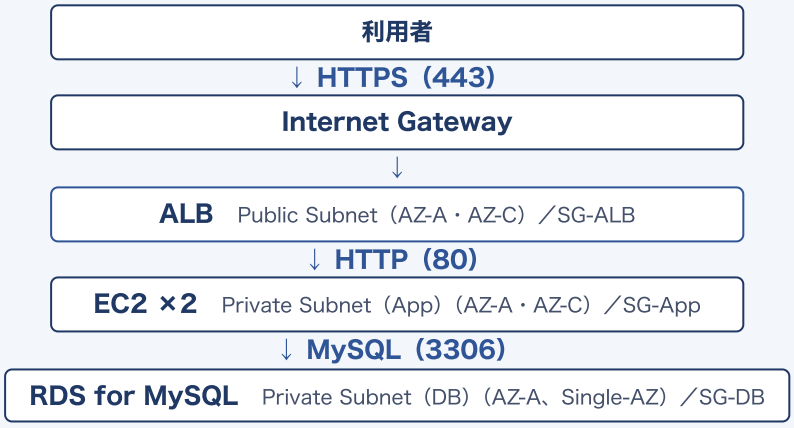
00. 表紙・文書管理（表紙、文書の目的、値の表記、改訂履歴）は1〜2ページに記載しています。

01. システム概要

1-1. 三層構成の概要

1つのVPCに2つのAvailability Zone（AZ）を使い、Webシステムを3つの層に分けています。インターネットから直接アクセスできるのは**ALBだけ**です。

層	AWSサービス	役割	配置場所
Web層	Application Load Balancer（ALB）	利用者からのHTTPS（443）を受け付け、正常なEC2に振り分ける	Public Subnet（AZ-A・AZ-C）
アプリケーション層	Amazon EC2（2台）	Webアプリケーションを動かすサーバー。ALBからHTTP（80）で通信を受ける	Private Subnet（App）（AZ-A・AZ-C に1台ずつ）
データベース層	Amazon RDS for MySQL	データを保存する。EC2からMySQL（3306）で接続される	Private Subnet（DB）（AZ-A、Single-AZ）



1-2. 運用対象のリソース

名前はすべて Work 02 の命名規則による **設計上の仮値** です。

種類	名前	主な設定
VPC	sample-3tier-vpc	10.0.0.0/16
EC2 #1	sample-3tier-web-a	ap-northeast-1a、sample-3tier-subnet-app-a（10.0.10.0/24）、SG-App、パブリックIPなし
EC2 #2	sample-3tier-web-c	ap-northeast-1c、sample-3tier-subnet-app-c（10.0.11.0/24）、SG-App、パブリックIPなし
RDS	sample-3tier-db	MySQL、ap-northeast-1a、sample-3tier-subnet-db-a（10.0.20.0/24）、SG-DB、Single-AZ、パブリックアクセスなし
EC2 Instance Connect Endpoint	sample-3tier-eice	sample-3tier-subnet-app-a、SG-EICE
Gateway VPC Endpoint（S3）	sample-3tier-vpce-s3	sample-3tier-rt-app に関連付け
ALB・ターゲットグループ	**要確認**	名前・リスナー・ヘルスチェックの設定は Work 02 の対象外

> **補足**　インスタンスID（i-で始まる値）やエンドポイント名は、実環境で作成したときに決まります。作業時は、名前とあわせてIDも作業記録に書き残してください。

1-3. VPCとサブネットの構成

AWSでは、ルートテーブルに **Internet Gateway への経路（0.0.0.0/0）があるサブネット**を Public Subnet、ないサブネットを Private Subnet と呼びます。

サブネット	AZ	CIDR	種類	置くもの	ルートテーブル
sample-3tier-subnet-public-a	1a	10.0.0.0/24	Public	ALB	sample-3tier-rt-public
sample-3tier-subnet-public-c	1c	10.0.1.0/24	Public	ALB	sample-3tier-rt-public
sample-3tier-subnet-app-a	1a	10.0.10.0/24	Private	EC2 #1、EC2 Instance Connect Endpoint	sample-3tier-rt-app
sample-3tier-subnet-app-c	1c	10.0.11.0/24	Private	EC2 #2	sample-3tier-rt-app
sample-3tier-subnet-db-a	1a	10.0.20.0/24	Private	RDS	sample-3tier-rt-db
sample-3tier-subnet-db-c	1c	10.0.21.0/24	Private	なし（DBサブネットグループ用）	sample-3tier-rt-db

ルートテーブル	宛先	ターゲット
sample-3tier-rt-public	10.0.0.0/16	local
sample-3tier-rt-public	0.0.0.0/0	Internet Gateway
sample-3tier-rt-app	10.0.0.0/16	local
sample-3tier-rt-app	S3のプレフィックスリスト	Gateway VPC Endpoint（S3）
sample-3tier-rt-db	10.0.0.0/16	local

1-4. Security Group（通信の許可）

SG	付けるリソース	受信（Inbound）	送信（Outbound）
SG-ALB	ALB	443/TCP ← 0.0.0.0/0	80/TCP → SG-App
SG-App	EC2	80/TCP ← SG-ALB 22/TCP ← SG-EICE	3306/TCP → SG-DB 443/TCP → S3のプレフィックスリスト
SG-DB	RDS	3306/TCP ← SG-App	ルールなし
SG-EICE	EC2 Instance Connect Endpoint	ルールなし	22/TCP → SG-App

インターネット（0.0.0.0/0）からの受信を許可しているのは、**SG-ALB の443番だけ**です。

1-5. CloudWatchの監視対象

Amazon CloudWatch は、AWSのリソースの状態を数値（メトリクス）で記録・表示するサービスです。次のメトリクスは、エージェントを入れなくても各サービスから自動で送られます。

対象	名前空間	主なメトリクス	データの間隔
EC2	AWS/EC2	CPUUtilization（CPU使用率）、StatusCheckFailed（ステータスチェックの失敗）、NetworkIn / NetworkOut	基本モニタリング：5分ごと（ステータスチェックは1分ごと）。追加料金なし
RDS	AWS/RDS	CPUUtilization、DatabaseConnections（接続数）、FreeStorageSpace（空きストレージ）、FreeableMemory（空きメモリ）、ReadIOPS / WriteIOPS	1分ごと。追加料金なし
ALB	AWS/ApplicationELB	HealthyHostCount / UnHealthyHostCount（正常・異常なターゲットの数）など	ALBの設定は 要確認

> **注意**　EC2の**メモリ使用率やディスク使用率**は、標準のメトリクスにはありません。取得するには CloudWatch エージェントが必要ですが、この構成は NAT Gateway も CloudWatch 用のVPCエンドポイントもないため、EC2からCloudWatchへデータを送れません（「09.」参照）。この手順書では、EC2にログインして OS のコマンドで確認します。

CloudWatchアラーム（しきい値を超えたら状態が変わる仕組み）と、その通知先（メールなど）は、Work 01・Work 02 では**設定していません**。この手順書のしきい値はすべて 設計上の仮値 で、通知の方法は 要確認 です。

1-6. 2つのVPCエンドポイントの役割

エンドポイント	役割	使う場面
EC2 Instance Connect Endpoint（sample-3tier-eice）	パブリックIPを持たないEC2に、管理者がSSH（22）で接続するための入口。踏み台サーバーが不要	OSの状態確認、ログの確認
Gateway VPC Endpoint（S3）（sample-3tier-vpce-s3）	EC2がインターネットを通らずに Amazon S3 へ接続するための経路	Amazon Linux 2023 のパッケージ更新（dnf）

EC2 Instance Connect Endpoint は1つのVPCに1つまでで、AZ-A に置いています。AZ-C の EC2 にもここから接続します。同時に接続できるのは20まで、1回の接続は最大1時間です。

1-7. Work 01 の構成図との対応

構成図の表示	この手順書での名前	主に扱う章
① HTTPS（443）	利用者 → ALB	04（ALB のメトリクス）、08
② Internet Gateway	sample-3tier-igw	09
③ HTTP（80）	ALB → EC2（sample-3tier-web-a / -c）	03、04、05
④ MySQL（3306）	EC2 → RDS（sample-3tier-db）	06
EC2 Instance Connect Endpoint	sample-3tier-eice	03、05、08
Gateway VPC Endpoint（S3）	sample-3tier-vpce-s3	09

02. 運用前の確認事項

作業を始める前に、**毎回**次の確認を行います。1つでも確認できない場合は作業を始めず、作業責任者に相談します。

2-1. 作業承認・作業記録の確認

1. 作業申請書（またはチケット）があり、**承認済み**であることを確認します。
2. 作業の内容・対象リソース・作業時間・作業者・承認者が書かれていることを確認します。
3. 作業記録（「07.」のチェックリスト・作業記録）を用意し、作業開始の時刻を記入します。
4. 申請にない作業は行いません。必要になった場合は、いったん作業を止めて承認者に相談します。

2-2. AWSマネジメントコンソールへのログイン確認

1. 組織で決められた方法（IAMユーザー、IAM Identity Center など）でサインインします。**ルートユーザーでは作業しません。**
2. 多要素認証（MFA）でサインインしたことを確認します。
3. 画面右上のアカウント名をクリックし、表示されたアカウントが、作業申請書に書かれた**対象アカウント**と一致することを確認します。

> **禁止**　AWSアカウントID、パスワード、アクセスキー、MFAのコードを、作業記録・チャット・メールに書かないでください。作業記録には、アカウントの別名など、組織で決めた識別名だけを書きます。

2-3. 対象リージョンの確認

1. 画面右上のリージョン表示が「**アジアパシフィック（東京）ap-northeast-1**」であることを確認します。
2. 違う場合は、リージョンの一覧から東京を選びます。

> **注意**　リージョンが違うと、対象のリソースが一覧に表示されません。「リソースが消えた」と判断する前に、まずリージョンを確認してください。

2-4. 作業者のIAM権限の確認

1. 作業に必要な画面（EC2、CloudWatch、RDS）を開き、エラーにならずに表示できることを確認します。
2. 権限が足りないと「You are not authorized」などのメッセージが表示されます。その場合は自分で権限を変えず、管理者に依頼します。
3. 参照だけの作業（監視の確認、状態の確認）は、**参照権限だけ**で行うのが原則です。

作業	必要な権限の例	権限の内容
監視の確認・状態の確認	EC2・RDS・CloudWatch の参照	要確認（組織のIAMポリシーで決める）
EC2の起動・停止	対象EC2の起動・停止	要確認
EC2へのSSH接続	EC2 Instance Connect Endpoint の利用	要確認（接続できる人をIAMで絞る）

2-5. 対象リソースの確認方法

1. EC2の画面で、左のメニューから「**インスタンス**」を選びます。
2. 検索欄に名前（例：sample-3tier-web-a）を入力し、対象を絞り込みます。
3. 次の項目が、この手順書（「1-2.」）と一致することを確認します。

確認する項目	期待する値（EC2 #1 の場合）
名前	sample-3tier-web-a
アベイラビリティーゾーン	ap-northeast-1a
VPC	sample-3tier-vpc（10.0.0.0/16）
サブネット	sample-3tier-subnet-app-a（10.0.10.0/24）
セキュリティグループ	SG-App
パブリック IPv4 アドレス	なし（空欄）

4. インスタンスIDを作業記録に書き写します。以降の作業では、名前と**インスタンスID**の両方で対象を確かめます。

2-6. 本番環境と検証環境の取り違え防止

確認すること	方法
アカウント	画面右上のアカウント名が、申請書の対象アカウントと同じか
リージョン	ap-northeast-1 か
リソース名	名前の先頭が、対象環境の命名規則（この資料では sample-3tier-）と同じか
ID	インスタンスIDなどが、事前に記録したIDと同じか
環境を表すタグ	タグのキーと値は**要確認**（Work 01・Work 02 では未定義）

> **注意**　複数のブラウザタブで別の環境を開いたまま作業しないでください。作業する環境のタブだけを開き、操作の直前に画面右上のアカウントとリージョンをもう一度見ます。

03. EC2の起動・停止手順

3-1. 作業の前提

- EC2は2台（sample-3tier-web-a、sample-3tier-web-c）あり、ALBが両方に振り分けています。
- **1台ずつ**作業します。2台を同時に停止すると、Webサービスが止まります。
- 停止・起動は、承認された作業申請に基づいて行います。

3-2. 対象インスタンスの確認

1. 「02.」の確認（承認・アカウント・リージョン・権限）が終わっていることを確認します。
2. EC2の画面で「**インスタンス**」を開き、対象のインスタンスを選びます。
3. 名前・インスタンスID・AZ が、作業申請書と一致することを確認します。

3-3. 停止前の確認事項

No	確認すること	確認する場所	期待する状態
1	停止の承認があるか	作業申請書	承認済み
2	対象が正しいか	インスタンスの「詳細」タブ	名前・ID・AZ が申請どおり
3	**もう1台のEC2が正常か**	ALBのターゲットグループの「ターゲット」タブ	もう1台が healthy（ターゲットグループ名は 要確認 ）
4	もう1台のEC2のステータスチェック	インスタンスの「ステータスとアラーム」タブ	すべてのチェックに合格
5	利用者への影響	作業申請書	停止中は1台で処理することを関係者が了承している
6	停止前の状態の記録	作業記録	状態（running）、ステータスチェック、CPU使用率を記録した

補足　ALBから外すときは、ターゲットグループで対象のEC2を「登録解除」してから停止すると、処理中の通信を待ってから外せます（登録解除の待ち時間は既定で300秒）。登録解除は設定の変更にあたるため、行う場合は作業申請に含めてください。ターゲットグループの設定は 要確認 です。

3-4. EC2の停止方法

1. EC2の画面で「**インスタンス**」を開き、対象のインスタンスにチェックを入れます。
2. 名前とインスタンスIDを、もう一度作業記録と照らし合わせます。
3. 画面上部の「**インスタンスの状態**」から「**インスタンスを停止**」を選びます。
4. 確認の画面で、対象のインスタンスが正しいことを確認し、「**停止**」を選びます。
5. 操作した時刻を作業記録に書きます。

禁止　確認画面の「**OSのシャットダウンをスキップ**」（Skip OS shutdown）は選ばないでください。OSを正しく終了せずに止めるため、データが壊れるおそれがあります。

禁止　「インスタンスを終了」（Terminate）は選ばないでください。**終了するとインスタンスは削除され、元に戻せません。**「停止」と「終了」を取り違えないよう注意してください。

3-5. 停止後の状態確認

1. 「インスタンスの状態」が「**停止中**（stopping）」から「**停止済み**（stopped）」に変わるまで待ちます。数分かかることがあります。
2. ALBのターゲットグループで、停止したEC2の状態が「unused」（停止中のため使われていない）になっていることを確認します。
3. もう1台のEC2が healthy のままであることを確認します。
4. Webサイトが表示できることを確認します（確認するURLは **要確認** ）。
5. 停止が完了した時刻と、確認の結果を作業記録に書きます。

停止したときに失われるもの	残るもの
メモリ（RAM）の内容	EBSボリュームとそのデータ
インスタンスストアのデータ（この構成の仮のインスタンスタイプ t3.micro にはない）	プライベートIPアドレス、ネットワークインターフェイス

補足　停止中は、EC2の利用料金はかかりませんが、**EBSボリュームの保存料金はかかります。**

3-6. 起動前の確認事項

No	確認すること	期待する状態
1	起動の承認があるか	承認済み
2	対象が正しいか	名前・ID・AZ が申請どおり
3	現在の状態	停止済み（stopped）
4	停止した理由が解消しているか	停止の原因（作業・障害など）が完了・解消している

3-7. EC2の起動方法

1. EC2の画面で「**インスタンス**」を開き、対象のインスタンスにチェックを入れます。
2. 名前とインスタンスIDを作業記録と照らし合わせます。
3. 「**インスタンスの状態**」から「**インスタンスを開始**」を選びます。
4. 操作した時刻を作業記録に書きます。

3-8. 起動後のステータス確認

No	確認すること	確認する場所	期待する状態
1	インスタンスの状態	インスタンス一覧の「インスタンスの状態」	実行中（running）
2	ステータスチェック	一覧の「ステータスチェック」列、「ステータスとアラーム」タブ	すべてのチェックに合格（例：3/3 のチェックに合格。表示される数はインスタンスタイプによって異なる）
3	ALBのヘルスチェック	ターゲットグループの「ターゲット」タブ	initial（確認中）を経て healthy
4	パブリックIP	「詳細」タブ	なし（付与されていない）
5	CPU使用率	「モニタリング」タブ	起動直後の一時的な上昇のあと、落ち着いている
6	Webサイト	ブラウザ	表示できる（確認するURLは **要確認** ）

補足　ステータスチェックは1分ごとに行われます。起動直後は「初期化しています」と表示されることがあるため、数分待ってから確認します。ステータスチェックの結果が出るまでの時間は、インスタンスによって異なります。

3-9. 異常時の確認事項

症状	確認すること	対応
「停止中」のまま変わらない	10分程度待っても変わらないか	待っても変わらない場合はエスカレーション。強制停止は承認なしで行わない
起動できない（エラーが表示される）	エラーメッセージの内容（例：容量不足の InsufficientInstanceCapacity）	メッセージを記録してエスカレーション
ステータスチェックが失敗する	どのチェックが失敗しているか（システム／インスタンス／アタッチされたEBS）	「05.」の手順で一次対応
ALBで healthy にならない	理由の表示（例：Target.Timeout、Target.ResponseCodeMismatch）、SG-App が SG-ALB からの80番を許可しているか	EC2にログインしてWebサーバーの状態を確認（「5-5.」）し、エスカレーション
EC2にSSHできない	「5-5.」の接続の前提	「08.」の手順でエスカレーション

04. CloudWatchの監視確認手順

4-1. CloudWatchへのアクセス方法

1. AWSマネジメントコンソールにサインインし、リージョンが ap-northeast-1 であることを確認します。
2. 画面上部の検索欄に「CloudWatch」と入力し、**CloudWatch** を開きます。
3. 左のメニューの「**メトリクス**」→「**すべてのメトリクス**」を選びます。
4. 「**参照**」タブで、名前空間（EC2、RDS など）を選び、表示したいメトリクスにチェックを入れるとグラフが表示されます。

4-2. EC2のCPU使用率の確認

1. 「すべてのメトリクス」で「**EC2**」→「**インスタンス別メトリクス**」を選びます。
2. 検索欄に「CPUUtilization」と入力します。
3. 対象の2台（sample-3tier-web-a、sample-3tier-web-c のインスタンスID）の CPUUtilization にチェックを入れます。
4. 「**グラフ化したメトリクス**」タブで、統計を「平均」、期間を「5分」にします。
5. 画面右上の時間の範囲を「3時間」や「1日」に変え、普段との違いを見ます。

> **補足**　EC2のインスタンス画面で対象を選び、「**モニタリング**」タブを開いても、CPU使用率のグラフを確認できます。

4-3. EC2のステータスチェックの確認

1. EC2の画面で「**インスタンス**」を開き、「**ステータスチェック**」列を見ます。
2. 対象のインスタンスを選び、「**ステータスとアラーム**」タブを開きます。
3. 次のチェックが合格しているかを確認します。

チェックの種類	何を見ているか	失敗したときに考えられること
システムステータスチェック	インスタンスが動いているAWS側の機器（電源・ネットワーク・ホスト）	AWS側の問題。AWSの修復を待つか、承認を得て停止・起動すると多くの場合は別のホストに移る
インスタンスステータスチェック	インスタンスのOSとネットワークの設定	メモリ不足、ファイルシステムの破損、ネットワークや起動の設定の誤り。多くの場合は利用者側での対応が必要
アタッチされたEBSのステータスチェック	EBSボリュームに読み書きできるか	EBSやホストの問題

4. CloudWatchでは、メトリクス StatusCheckFailed（いずれかの失敗）、StatusCheckFailed_System、StatusCheckFailed_Instance、StatusCheckFailed_AttachedEBS で確認できます。値が **0 なら正常、1 なら失敗**です。

4-4. RDSのCPU使用率・空きストレージなどの確認

1. RDSの画面で「**データベース**」を開き、sample-3tier-db を選びます。

2. 「**モニタリング**」タブを開くと、主なメトリクスのグラフが表示されます。
3. CloudWatch で見る場合は、「すべてのメトリクス」で「**RDS**」→「**データベース別メトリクス**」を選び、DB識別子 sample-3tier-db のメトリクスにチェックを入れます。

メトリクス	内容	単位	見るポイント
CPUUtilization	CPU使用率	%	高い状態が続いていないか
DatabaseConnections	DBへの接続数	個	急に増えていないか、0になっていないか
FreeStorageSpace	空きストレージ	バイト	減り続けていないか
FreeableMemory	空きメモリ	バイト	少ない状態が続いていないか
ReadIOPS / WriteIOPS	1秒あたりの読み書きの回数	回/秒	急に増えていないか
ReadLatency / WriteLatency	読み書き1回にかかる時間	秒	普段より長くなっていないか

> **補足**　RDSの画面では MB、CloudWatch ではバイトなど、画面によって単位が違うことがあります。比べるときは単位をそろえてください。

4-5. メトリクスの確認期間と見方

確認の種類	時間の範囲	期間（1点あたりの長さ）	統計
今起きていることの確認	1時間〜3時間	EC2：5分（基本モニタリング）／RDS：1分	平均と最大
普段との比較	1日〜1週間	5分〜1時間	平均
増え方の確認（ストレージなど）	1週間〜1か月	1時間〜1日	最小（空き容量の場合）

見方のポイント：

- **平均**だけでは短い山が見えにくいため、**最大**もあわせて見ます。
- 1つの値だけで判断せず、**続いている時間**と、**同じ時間帯に他のメトリクスがどう動いたか**を見ます。
- 時刻の表示が「UTC」か「ローカル（日本時間）」かを確認します。画面右上の時間の設定で切り替えられます。作業記録には、どちらの時刻かを書きます。

4-6. 通常時と異常時の判断例

しきい値はすべて設計上の仮値です。実際の値は、普段の数値を一定期間記録してから決めます。

対象	メトリクス	通常時の目安	異常を疑う例
EC2	CPUUtilization	普段の範囲内	平均80%以上が15分（5分×3回）続く 設計上の仮値
EC2	StatusCheckFailed	0	1 が2分（1分×2回）続く 設計上の仮値
RDS	CPUUtilization	普段の範囲内	平均80%以上が15分続く 設計上の仮値
RDS	FreeStorageSpace	十分に残っている	割り当て容量（20 GiB 設計上の仮値 ）の10%（約2 GiB）を下回る 設計上の仮値
RDS	DatabaseConnections	普段の範囲内	急増、または0が続く（上限は max_connections の設定によるため 要確認 ）
RDS	FreeableMemory	普段の範囲内	少ない状態が続く（基準は 要確認 ）
ALB	UnHealthyHostCount	0	1以上 設計上の仮値

補足　EC2・RDSの仮のインスタンスタイプ（t3.micro、db.t3.micro）は「バースト可能」なタイプです。CPUクレジットの残り（CPUCreditBalance）もあわせて確認します。クレジットの設定（standard / unlimited）は 要確認 です。

05. アラーム発生時の一次対応

重要　アラームが発生しても、**すぐに再起動や設定の変更を行わない**でください。まず状況・原因・影響の範囲を確認して記録し、**承認を得てから**対応します。再起動すると、原因の調査に必要な情報（メモリの状態など）が失われることがあります。

この章は、CloudWatchアラームを設定した場合の手順です。アラームの名前・しきい値は設計上の仮値、通知の方法は要確認です。

5-1. 一次対応の流れ

順番	やること	記録すること
1	アラームの状態を確認する	アラーム名、状態、状態が変わった時刻
2	対象のリソースを特定する	リソース名、ID、AZ
3	発生時刻と続いている時間を確認する	開始時刻、今も続いているか
4	関連するメトリクスを確認する	他のメトリクスの動き
5	ログを確認する	確認したログと、気になる内容
6	影響の範囲を確認する	利用者への影響の有無
7	報告・エスカレーションする	報告した相手と時刻

5-2. アラームの状態確認

1. CloudWatch の左のメニューで「**アラーム**」→「**すべてのアラーム**」を開きます。
2. 状態が「**アラーム状態**」（ALARM）のアラームを選びます。
3. 次の内容を確認し、作業記録に書きます。

アラームの状態	意味
OK	メトリクスがしきい値の範囲内
アラーム状態（ALARM）	メトリクスがしきい値を超えている
データ不足（INSUFFICIENT_DATA）	アラームを作ったばかり、メトリクスが届いていない、または判断に必要なデータが足りない

4. アラームの詳細画面で、しきい値・期間・評価期間（何回続いたら状態を変えるか）と、「**履歴**」を確認します。

注意　「データ不足」は異常とは限りません。ただし、**EC2が停止している**とメトリクスが届かず「データ不足」になることがあります。対象の状態もあわせて確認してください。

5-3. 対象リソースの特定

1. アラームの詳細画面で、メトリクスの**ディメンション**（InstanceId、DBInstanceIdentifier など）を確認します。
2. EC2 または RDS の画面で、そのIDのリソースを開き、名前・AZ を確認します。

3. 「1-2.」の一覧と照らし合わせ、どの層（ALB／EC2／RDS）の問題かを記録します。

5-4. 発生時刻・継続時間と、関連メトリクスの確認

1. アラームの「履歴」で、状態が OK から ALARM に変わった時刻を確認します。
2. メトリクスのグラフを、発生時刻の**1時間前から現在まで**の範囲で表示します。
3. 今もしきい値を超えているか（続いているか）、一時的だったかを確認します。
4. 同じ時間帯の、次のメトリクスを確認します。

アラームの対象	あわせて見るメトリクス
EC2のCPU使用率	もう1台のEC2のCPU使用率、ALBのリクエスト数、RDSのCPU使用率・接続数
EC2のステータスチェック	どのチェックが失敗しているか、もう1台のEC2、ALBのターゲットの状態
RDSのCPU使用率	DatabaseConnections、ReadIOPS / WriteIOPS、EC2のCPU使用率
RDSの空きストレージ	減り始めた時刻、WriteIOPS

5. AWS側の障害の可能性を確認するため、AWS Health Dashboard を確認します。

5-5. ログの確認

確認するもの	確認方法	備考
EC2のコンソール出力（起動時のメッセージ）	EC2の画面で対象を選び、「**アクション**」→「**モニタリングとトラブルシューティング**」→「**システムログを取得**」	SSHで接続できないときも確認できる
EC2のOSのログ	EC2 Instance Connect Endpoint で接続し、`journalctl` で確認	Amazon Linux 2023 は既定で `/var/log/messages` がない
Webサーバー・アプリケーションのログ	EC2に接続して確認	ログの場所は**要確認**（アプリケーションによる）
RDSのログ	RDSの画面で sample-3tier-db を選び、「**ログとイベント**」タブ	最近のイベントとログファイルを確認できる
AWSの操作の記録	CloudTrail の「**イベント履歴**」	直近90日分の管理イベント（誰がいつ何を操作したか）を確認できる
ALBのアクセスログ	**要確認**	Work 01・Work 02 では設定していない

EC2への接続手順（EC2 Instance Connect Endpoint 経由）

1. EC2の画面で「**インスタンス**」を開き、対象を選んで「**接続**」を選びます。
2. 「**EC2 Instance Connect**」タブを選びます。
3. 接続タイプで「**プライベート IP を使用して接続**」を選びます。
4. 「EC2 Instance Connect Endpoint」で sample-3tier-eice のIDを選びます。
5. ユーザー名が `ec2-user`（Amazon Linux 2023 の既定）であることを確認し、「**接続**」を選びます。

接続の前提：作業者に EC2 Instance Connect Endpoint を使うIAM権限があること、SG-App が SG-EICE からの22番を許可していること、EC2が実行中であること。接続方式（一時的な鍵を送る方法か、キーペアか）は**要確認**です。

OSでの確認コマンド（参照のみ）

確認すること	コマンド
直近1時間のOSのログ	`journalctl --since "1 hour ago"`
エラー以上のログ	`journalctl -p err --since today`
メモリの使用状況	`free -h`
ディスクの使用状況	`df -h`
CPUを多く使っているプロセス	`top -b -n 1 | head -n 20`
サービスの状態	`systemctl status <サービス名>`（サービス名は 要確認 ）

> **禁止**　一次対応では、サービスの再起動、設定ファイルの変更、パッケージの更新、ファイルの削除を行わないでください。

5-6. 影響範囲の確認

確認すること	方法
Webサイトが表示できるか	ブラウザで確認（URLは 要確認 ）
ALBの正常なターゲットの数	ターゲットグループの「ターゲット」タブ、HealthyHostCount
片方のEC2だけか、両方か	2台のメトリクス・ステータスを比べる
DBに影響があるか	RDSの状態、DatabaseConnections
1つのAZに偏っているか	問題のあるリソースのAZ（1a／1c）

5-7. 一次対応で解決しない場合のエスカレーション

次のいずれかに当てはまる場合は、すぐに「08.」の連絡先へエスカレーションします。

- Webサイトが表示できない、または利用者に影響が出ている
- 2台のEC2が両方とも異常、または RDS が利用できない
- 発生から一定時間（ 設計上の仮値 ：30分）たっても原因が分からない
- 再起動・停止・設定変更など、**変更を伴う対応が必要**だと考えられる
- AWS側の障害が疑われる

報告では、「5-1.」で記録した内容（何が・いつから・どこで・どの程度・何を確認したか）を伝えます。対応の方針は、承認者の判断に従います。

06. RDSの状態確認

6-1. RDSインスタンスの状態確認

1. RDSの画面で、左のメニューの「**データベース**」を開きます。
2. sample-3tier-db の「**ステータス**」を確認します。

ステータス	意味	対応
利用可能（available）	正常に動いている	なし
バックアップ中（backing-up）	バックアップを作成している	終わるまで待つ
変更中（modifying）	設定の変更を反映している	申請された作業か確認する
再起動中（rebooting）	再起動している（短い停止を伴う）	申請された作業か確認する
ストレージフル（storage-full）	ストレージの空きがない	すぐにエスカレーション
停止済み（stopped）	一時的に停止している	申請された作業か確認する

3. 「**メンテナンス**」列に、予定されているメンテナンスがあるかを確認します（「6-5.」）。

6-2. Single-AZ構成であることの確認

1. sample-3tier-db を選び、詳細画面を開きます。
2. 次の項目を確認します。

タブ	項目	期待する値
設定	マルチ AZ	いいえ（Single-AZ）
接続とセキュリティ	アベイラビリティーゾーン	ap-northeast-1a
接続とセキュリティ	VPC	sample-3tier-vpc
接続とセキュリティ	サブネットグループ	sample-3tier-db-subnet-group（sample-3tier-subnet-db-a / sample-3tier-subnet-db-c）
接続とセキュリティ	VPC セキュリティグループ	SG-DB
接続とセキュリティ	パブリックアクセス	いいえ
接続とセキュリティ	ポート	3306
設定	削除保護	有効 設計上の仮値

> **注意**　この構成は Single-AZ のため、**AZ-A（ap-northeast-1a）で障害が起きるとデータベースが使えなくなります**。スタンバイがないため、自動での切り替えはありません。

6-3. CPU使用率・接続数・ストレージの確認

1. sample-3tier-db の「**モニタリング**」タブを開きます。

2. 時間の範囲を「過去 3 時間」と「過去 1 週間」に切り替えて、次の項目を確認します。

項目	メトリクス	確認すること
CPU使用率	CPUUtilization	高い状態が続いていないか（目安は「4-6.」）
接続数	DatabaseConnections	普段と比べて急に増減していないか
空きストレージ	FreeStorageSpace	減り続けていないか。このまま減るといつ不足するか
空きメモリ	FreeableMemory	少ない状態が続いていないか

6-4. バックアップ状態の確認

1. sample-3tier-db を選び、「**メンテナンスとバックアップ**」タブを開きます。
2. 次の項目を確認し、作業記録に書きます。

項目	期待する値
自動バックアップ	有効
バックアップ保持期間	7日 設計上の仮値
バックアップウィンドウ	要確認
最新の復元可能時刻	現在に近い時刻になっている

3. 左のメニューの「**自動バックアップ**」または「**スナップショット**」で、バックアップが作られていることを確認します。

> **補足**　自動バックアップは、DBインスタンスが「利用可能」のときに、バックアップウィンドウの時間帯に作られます。「ストレージフル」などの状態では作られません。

6-5. メンテナンス情報の確認

1. RDSの「データベース」一覧で、sample-3tier-db の「**メンテナンス**」列を確認します。

表示	意味
なし	予定されているメンテナンスはない
必須（required）	必ず適用される。いつまでも延期はできない
利用可能（available）	適用できるが、自動では適用されない
次のウィンドウ（next window）	次のメンテナンスウィンドウで適用される
進行中（In progress）	適用している最中

2. sample-3tier-db を選び、「**メンテナンスとバックアップ**」タブの「**保留中のメンテナンス**」で、内容と適用予定日を確認します。
3. メンテナンスウィンドウ（毎週の30分の時間帯）を確認します。設定値は 要確認 です。**表示はUTC**のため、日本時間（UTC＋9時間）に直して記録します。

> **注意**　Single-AZ の場合、OSやDBエンジンの更新など一部のメンテナンスでは、**DBが短時間使えなくなります**。メンテナンスの予定を見つけたら、適用の時期を決めるために作業責任者へ報告します。「今すぐパッチを適用」などの操作は、承認なしで行いません。

6-6. 異常時の一次対応

症状	確認すること	一次対応
ステータスが「利用可能」以外のまま	申請された作業中か、「ログとイベント」タブのイベント	作業でなければエスカレーション
アプリがDBに接続できない	RDSのステータス、SG-DB の受信3306（送信元SG-App）、接続先がエンドポイント（DNS名）か	確認結果を記録してエスカレーション
CPU使用率が高い	接続数・IOPSの増加、EC2側の負荷	記録してエスカレーション
空きストレージが少ない	減り方（いつ不足するか）	すぐにエスカレーション（容量の追加は設定の変更）
AZ-A の障害	AWS Health Dashboard	すぐにエスカレーション。復旧の方法（バックアップからの復元など）は承認者が判断する

禁止　次の操作は、通常の運用手順としては**行いません**。必要な場合は、障害対応の責任者が判断し、別の手順書と承認に基づいて行います。

- DBインスタンスの**削除**、作り直し
- スナップショットや特定時点への**復元**（復元すると**新しいDBインスタンス**が作られ、接続先も変わる）
- インスタンスクラス・ストレージ・パラメータグループなどの**変更**
- **再起動**（短時間DBが止まる）、**一時的な停止**（停止から7日たつと自動で起動する）
- Multi-AZ への変更（構成の変更にあたる）

なお、「フェイルオーバーありで再起動」は **Multi-AZ 構成でのみ**使える機能です。Single-AZ のこの構成では、切り替え先のスタンバイがありません。

07. 作業前後チェックリスト

作業のたびに印刷するか、コピーして使います。チェック欄（□）に ✓ を付け、確認した内容を書きます。

7-1. 作業情報

項目	記入欄
作業名	
作業申請番号	
作業日	年　月　日
作業時間（予定）	：　～　：　（日本時間）
作業者	
確認者（ダブルチェック）	
承認者	
対象アカウント（識別名）	※アカウントIDは書かない
対象リージョン	ap-northeast-1
対象リソース（名前・ID）	

7-2. 作業前チェックリスト

No	チェック	確認項目	確認した内容・時刻
1	□	作業対象を確認した（名前・ID・AZ が申請どおり）	
2	□	作業承認を得た（承認者・承認日）	
3	□	対象アカウントとリージョン（ap-northeast-1）を確認した	
4	□	作業に必要なIAM権限があることを確認した	
5	□	変更前の状態を記録した（状態、ステータスチェック、主なメトリクス）	
6	□	CloudWatchで、作業前に異常がないことを確認した	
7	□	影響を受ける関係者に作業開始を連絡した	
8	□	中止の条件と、元に戻す手順を確認した	

7-3. 作業中の記録

時刻	作業内容	結果	作業者

7-4. 作業後チェックリスト

No	チェック	確認項目	確認した内容・時刻
1	□	作業内容を記録した（実施した操作と時刻）	
2	□	作業後のステータスを確認した（インスタンスの状態、ステータスチェック）	
3	□	ALBのターゲットが healthy であることを確認した	
4	□	RDSのステータスが「利用可能」であることを確認した	
5	□	CloudWatchに異常がないことを確認した（アラームの状態、主なメトリクス）	
6	□	Webサイトが表示できることを確認した	
7	□	変更前の状態と比べ、意図しない変化がないことを確認した	
8	□	関係者への報告を完了した（報告先・時刻）	

7-5. 完了の確認

項目	記入欄
作業結果	□ 完了　□ 中止　□ 一部完了
作業終了時刻	：　　（日本時間）
特記事項	
作業者の署名	
確認者の署名	

08. 障害対応・エスカレーション

8-1. 障害発生時の初動

1. **落ち着いて、まず記録を始めます。** 気づいた時刻と、気づいたきっかけ（アラーム、利用者からの連絡など）を「8-5.」の対応履歴に書きます。
2. 「02.」の確認（アカウント・リージョン）を行います。
3. 「05.」の手順で、状態・対象・時刻・影響を確認します。
4. 利用者に影響がある、または影響が分からない場合は、原因が分からなくても**先に第一報**を入れます（「8-4.」）。
5. 変更を伴う対応は、承認者の指示を受けてから行います。

8-2. 影響範囲の確認

確認項目	確認結果（記入欄）
Webサイトは表示できるか	□ 表示できる　□ 表示できない　□ 一部エラー
影響を受けている層	□ ALB　□ EC2 #1　□ EC2 #2　□ RDS　□ 不明
影響を受けているAZ	□ ap-northeast-1a　□ ap-northeast-1c　□ 両方　□ 不明
影響の始まり	：　　（日本時間）
今も続いているか	□ 続いている　□ 回復した（　　：　　）
AWS側の障害の情報	□ あり　□ なし（AWS Health Dashboard を確認）

8-3. ログ・メトリクスの採取

あとで原因を調べるため、**変更や再起動の前に**次の情報を保存します。保存した場所を対応履歴に書きます。

No	採取するもの	方法	済
1	アラームの詳細と履歴	CloudWatch のアラーム画面の画面キャプチャ	□
2	関連するメトリクスのグラフ（発生の1時間前から）	CloudWatch のグラフの画面キャプチャ、または「アクション」からデータをダウンロード	□
3	EC2のステータスチェックの結果	「ステータスとアラーム」タブの画面キャプチャ	□
4	EC2のコンソール出力	「システムログを取得」の内容を保存	□
5	EC2のOSのログ	`journalctl` の出力を保存（期間を指定）	□
6	ALBのターゲットの状態と理由	ターゲットグループの「ターゲット」タブの画面キャプチャ	□
7	RDSのイベントとログ	「ログとイベント」タブ	□
8	AWSの操作の記録	CloudTrail の「イベント履歴」（発生前後の時間で絞り込む）	□

> **注意**　画面キャプチャや保存したログに、パスワード・アクセスキー・個人情報が含まれていないか確認してから共有してください。保存先は**要確認**（組織で決めた場所）です。

8-4. エスカレーション先の記録欄

連絡先は、運用を始める前に記入します。

順位	役割	担当者名	連絡方法	連絡先	対応時間
1	運用担当（一次対応）				
2	運用責任者（承認者）				
3	インフラ担当（AWS）				
4	アプリケーション担当				
5	AWSサポートへの問い合わせ				

AWSサポートの契約プラン（問い合わせできる内容と回答時間）は 要確認 です。

エスカレーションの基準 設計上の仮値

重要度	状況の例	連絡先	連絡の目安
高	Webサイトが表示できない、RDSが使えない、データの消失が疑われる	順位1〜3 にすぐ連絡	気づいてすぐ
中	EC2が1台だけ異常で、もう1台で処理できている	順位1〜2	15分以内
低	一時的なアラームで、すでに回復している	順位1、運用の報告で共有	当日中

8-5. 対応履歴の記録欄

日時（日本時間）	内容（確認したこと・行ったこと）	実施者	承認者	結果

8-6. 復旧後の確認事項

No	チェック	確認項目
1	□	Webサイトが表示できる
2	□	ALBのターゲット（EC2 2台）がすべて healthy
3	□	EC2 2台のステータスチェックがすべて合格
4	□	RDSのステータスが「利用可能」
5	□	CloudWatchのアラームがすべて OK（または意図した状態）
6	□	主なメトリクスが普段の範囲に戻った
7	□	障害中に行った変更をすべて記録した（元に戻す必要があるものを含む）
8	□	関係者へ復旧を報告した
9	□	再発防止の検討（障害報告書の作成）を依頼した

09. 運用上の注意事項・制約

9-1. この構成の前提と制約

No	前提・制約	運用での注意
1	**NAT Gateway は配置していない**	Private Subnet の EC2 は、**インターネット上のサイトやサービスに接続できません。**外部APIの呼び出し、Amazon Linux 以外のリポジトリ、インターネットからのファイルのダウンロードはできません
2	**RDS は Single-AZ 構成**	AZ-A の障害やメンテナンスで、DBが使えなくなることがあります。自動の切り替えはありません
3	**EC2 にパブリックIPは付与しない**	インターネットからEC2へは直接接続できません。パブリックIPを付ける・Elastic IP を関連付ける変更は行いません
4	**EC2 への管理接続は EC2 Instance Connect Endpoint を利用する想定**	踏み台サーバーは置きません。同時接続は20まで、1回の接続は最大1時間です。AZ-A の障害時は接続できないことがあります
5	**S3 Gateway Endpoint を利用する**	EC2 から S3 へは、インターネットを通らずに接続します。OSのパッケージ更新（dnf）に使います
6	**Security Group で 22番・3306番をインターネットに公開しない**	22番は SG-EICE から、3306番は SG-App からだけ許可しています。送信元を 0.0.0.0/0 にする変更は行いません
7	**本資料は実際のAWS環境にデプロイして検証したものではない**	手順はAWS公式ドキュメントに基づくサンプルです。実際に使う前に、検証環境で手順を確認してください

9-2. EC2 から使える通信と、使えない通信

NAT Gateway がないため、**「S3に接続できる」ことは「インターネットに接続できる」ことではありません。**

通信先	経路	使えるか
同じVPCの中（ALB、RDS、EC2 Instance Connect Endpoint）	local の経路	使える（SGで許可した通信のみ）
東京リージョンの Amazon S3（Amazon Linux 2023 のリポジトリを含む）	Gateway VPC Endpoint（S3）	使える（SG-App の送信443番。エンドポイントポリシーは 要確認 ）
別のリージョンの S3	なし	使えない（Gateway Endpoint は作成したリージョンの S3 だけが対象）
インターネット上のサイト・外部API	なし（0.0.0.0/0 の経路がない）	**使えない**
S3 以外のAWSサービス（CloudWatch、CloudWatch Logs、Systems Manager など）の API	なし	**使えない**（インターフェイス型のVPCエンドポイントか NAT Gateway が必要）

そのため、この構成では次のことができません。

- CloudWatch エージェントでメモリ・ディスクの使用率やログを CloudWatch に送ること
- AWS Systems Manager（Session Manager など）で EC2 を管理すること
- EC2 から AWS CLI で S3 以外のAWSサービスを操作すること

これらが必要になった場合は、構成の変更（VPCエンドポイントや NAT Gateway の追加）として設計を見直します。**費用がかかるため、運用担当の判断では追加しません。**

> **補足**　EC2 と RDS の CloudWatch メトリクス（CPU使用率、ステータスチェックなど）は、AWSが自動で集めるため、NAT Gateway がなくても確認できます。

9-3. 運用で行ってはいけない操作（まとめ）

対象	行ってはいけない操作
アカウント	ルートユーザーでの作業、認証情報の共有・記録
EC2	承認のない停止・起動・再起動、「終了」（削除）、「OSのシャットダウンをスキップ」、2台同時の停止、パブリックIPの付与
RDS	削除、作り直し、復元、設定の変更、承認のない再起動・停止、パッチの即時適用
ネットワーク	Security Group・ルートテーブルの変更、22番・3306番のインターネット公開、NAT Gateway の追加
OS	一次対応の中でのサービスの再起動、設定ファイルの変更、ファイルの削除

付録A. 用語集

用語	説明
リージョン	AWSのデータセンターがある地域。この構成は東京（ap-northeast-1）
AZ（アベイラビリティーゾーン）	リージョンの中にある、電源やネットワークが分かれたデータセンターの集まり。この構成は 1a と 1c
VPC	AWS上に作る、自分専用のネットワーク
サブネット	VPCをさらに分けた範囲。AZごとに作る
Security Group（SG）	リソースごとの仮想のファイアウォール。許可した通信だけを通す。応答の通信は自動で通る（ステートフル）
ALB	Application Load Balancer。利用者からの通信を受け、複数のEC2に振り分ける
ターゲットグループ	ALBが通信を振り分ける先（EC2）のまとまり。ヘルスチェックで正常なEC2を判断する
ヘルスチェック	ALBがEC2に定期的に通信を送り、正常に応答するかを確認する仕組み
ステータスチェック	EC2が正常に動いているかを、AWSが1分ごとに確認する仕組み
メトリクス	CPU使用率など、リソースの状態を表す数値。CloudWatch に時間ごとに記録される
アラーム	メトリクスがしきい値を超えたときに状態が変わり、通知などを行う CloudWatch の機能
Single-AZ / Multi-AZ	RDSを1つのAZだけに置くか、別のAZにスタンバイも置くか
NAT Gateway	Private Subnet のリソースがインターネットに接続するための仕組み。この構成では使っていない
VPCエンドポイント	インターネットを通らずに、VPCからAWSのサービスに接続するための仕組み
エスカレーション	自分で解決できない問題を、決められた上位の担当者に報告して判断を仰ぐこと
一次対応	障害に最初に気づいた担当者が行う、状況の確認・記録・報告
UTC	協定世界時。日本時間はUTCに9時間を足した時刻

付録B. 画面の名前の対応（日本語表示／英語表示）

AWS公式ドキュメント（英語）に記載されている名前です。日本語表示の名前は対応させたもので、実際の表示と異なる場合があります。

サービス	日本語表示（この手順書）	英語表示
EC2	インスタンス	Instances
EC2	インスタンスの状態 → インスタンスを停止／インスタンスを開始	Instance state → Stop instance / Start instance
EC2	OSのシャットダウンをスキップ	Skip OS shutdown
EC2	ステータスチェック（列）、ステータスとアラーム（タブ）	Status check, Status and alarms
EC2	アクション → モニタリングとトラブルシューティング → システムログを取得	Actions → Monitor and troubleshoot → Get system log
EC2	接続 → EC2 Instance Connect → プライベート IP を使用して接続	Connect → EC2 Instance Connect → Connect using a Private IP
CloudWatch	メトリクス → すべてのメトリクス、参照、グラフ化したメトリクス	Metrics → All metrics, Browse, Graphed metrics
CloudWatch	インスタンス別メトリクス	Per-Instance Metrics
CloudWatch	アラーム → すべてのアラーム	Alarms → All alarms
RDS	データベース	Databases
RDS	接続とセキュリティ、モニタリング、ログとイベント、設定、メンテナンスとバックアップ（タブ）	Connectivity & security, Monitoring, Logs & events, Configuration, Maintenance & backups
RDS	保留中のメンテナンス	Pending maintenance
CloudTrail	イベント履歴	Event history