



2024年3月19日

AWS障害切り分け手法の基本



自己紹介

□大吉 祐史 (Yuji Oyoshi)

□株式会社スタイルズ

- ▶ AWSを主とした監視運用サービス担当
サブリーダー



本日、お話しする内容

□対象

- ▶ AWSではどのような障害切り分け手法があるのかを知りたい方
- ▶ AWSでの障害切り分けポイントを知りたい方

□ゴール

- ▶ AWS障害切り分けの考え方を知る
- ▶ AWS障害切り分けの基本的な手法を知る

※AWS障害検知、および障害通知に関する詳細は過去のウェビナー

- ・「**CloudWatchによるAWSシステム監視の基本**」
- ・「**AWSシステム障害通知の基本**」

を参照してください。

障害切り分けとは

障害切り分けとは

障害切り分けとは

- 障害が発生した際、何が原因なのかがわからなければ復旧、エスカレーション等の対処ができない
 - ハードウェア障害
 - ソフトウェア障害
 - 人為的ミス

障害切り分けの目的

- どこで障害が発生しているのかを明らかにすること
- 障害の影響範囲の特定

障害切り分けの手法

- AWSコンソールでの確認
- AWSサポートへの確認



切り分けのポイント

障害がどこで発生しているのか

- AWS設備の問題か
- ユーザー側の問題か
- インフラの問題か、アプリケーションの問題か
- インターネットや回線の問題か



影響範囲の確認も重要

- 一部のサーバなのかシステム全体への影響なのか
- 大きな範囲の特定から絞り込む

AWS管理とユーザ管理の範囲

- マネージドサービス（RDSなど）とアンマネージドサービス（EC2など）では、管理対象の範囲が異なる



切り分けでやるべきこと

□ システム障害発生時に実施すべき確認手段と確認内容

確認手段

確認内容

① AWSコンソールでの確認

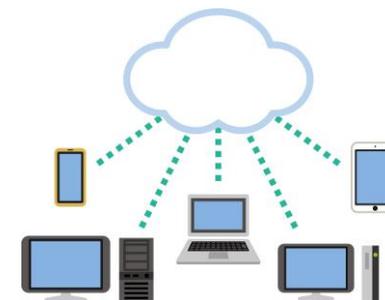
➡ AWSコンソール上で障害有無を確認
➤ ユーザ側の問題か、AWSシステム側の問題かを切り分ける

② AWSサポートへの確認

➡ AWS環境側で障害が発生していないかを確認
➤ AWSシステム側の問題が疑われる場合に確認する

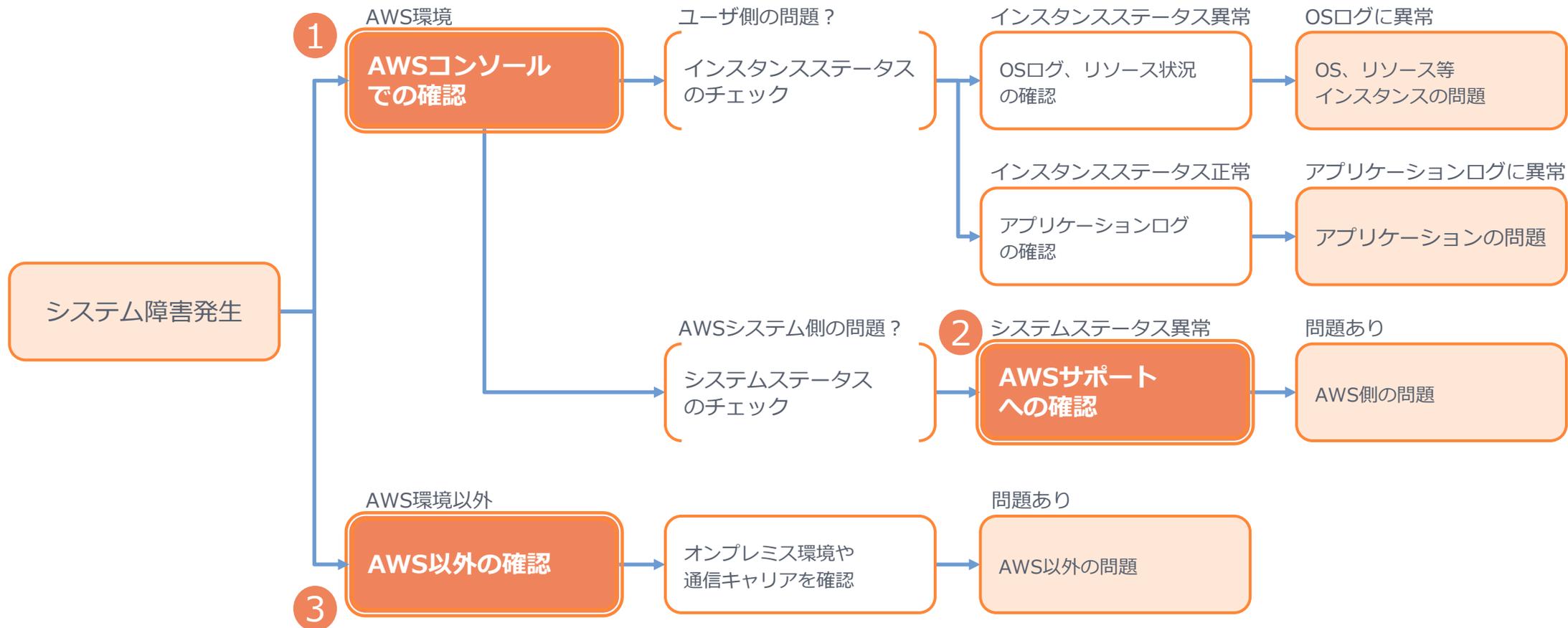
③ AWS以外での確認

➡ AWSへの経路で問題が発生していないかを確認
➤ ハイブリッドの場合はオンプレミス環境の問題等を確認する



切り分けの基本的な順序

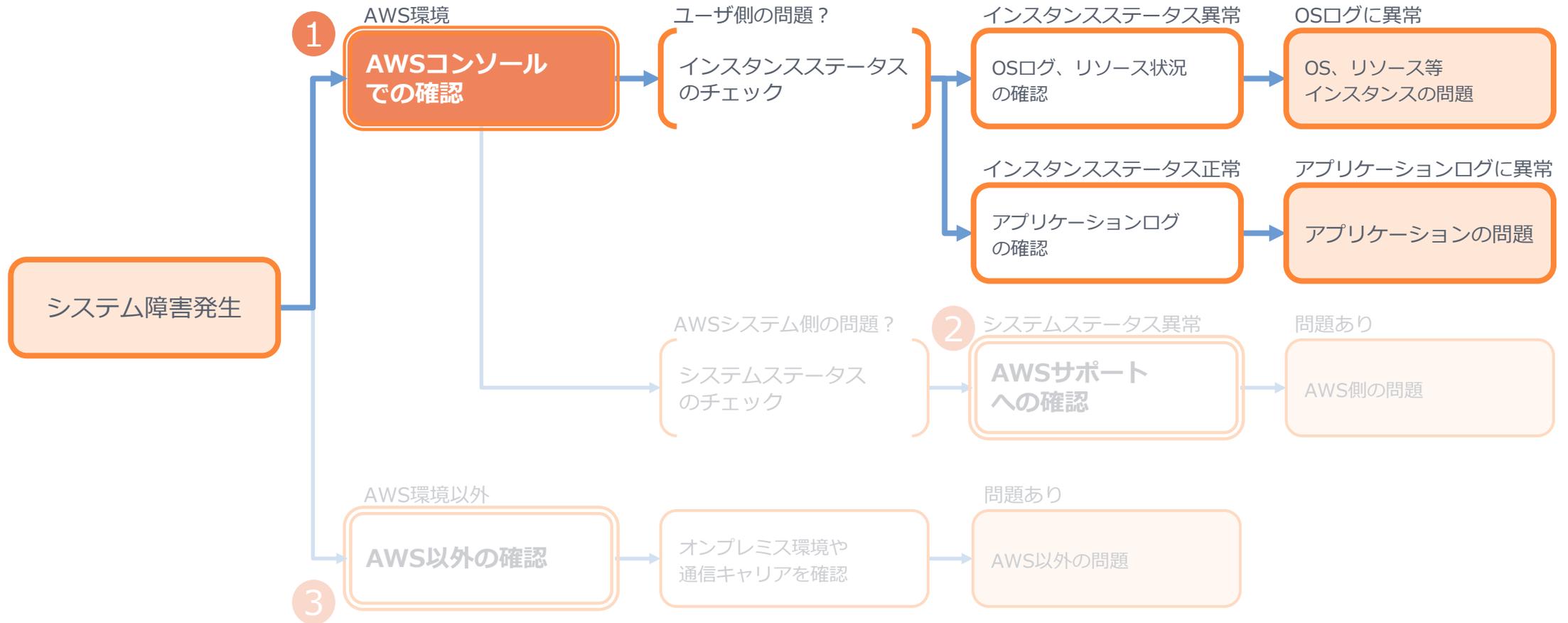
□ 大きな範囲から絞り込み、原因特定までのスピードアップ、効率化を図る



AWSコンソールでの確認

AWSコンソールでの確認

□ ユーザ環境調査のためAWSコンソールによる確認を行うケース



AWSコンソールでのユーザ側環境の確認（EC2 の場合）

- インスタンスステータスのチェックでは、個々のインスタンスのソフトウェアとネットワークの設定をモニタリング

インスタンス: i-0fdb640f331e0ea84 (Utest)

詳細 | セキュリティ | ネットワーキング | ストレージ | **ステータスチェック** | モニタリング | タグ

ステータスチェック 情報
ステータスチェックは、i-0fdb640f331e0ea84 (Utest) によるアプリケーションの実行を妨げる可能性のある問題を検出します。

システムステータスのチェック
✔ システムの接続性チェックに合格しました

このインスタンスで発生している状況がチェックに反映されていない場合、または発生している問題が検出されない場合、インスタンスステータスをレポートします。

インスタンスステータスをレポート

インスタンスステータスのチェック
✔ インスタンスの接続性チェックに合格しました

インスタンスステータスのチェック

ユーザ側環境の異常

- ※ 異常の場合は以下のように表示される
- ⊗ インスタンスの接続性チェックに失敗しました

📢 インスタンスステータスチェックの失敗の原因となる問題の例

- ✓ 失敗したシステムステータスチェック
- ✓ 正しくないネットワークまたは起動設定
- ✓ メモリの枯渇
- ✓ 破損したファイルシステム
- ✓ 互換性のないカーネル

AWSコンソールでのユーザ側環境の確認（RDS の場合）

- DBインスタンスのステータスも必要に応じて確認する

The screenshot shows the 'Databases' section of the AWS console. It features a search bar 'Filter by databases' and a table with columns for 'DB identifier', 'Role', and 'Status'. The table lists five instances: database-1, database-2, database-3, database-4, and database-5, all with the role 'Instance'. The 'Status' column is highlighted with a red box, and an orange callout box with the text 'DBインスタンスのステータス' points to it. The status options shown are Stopped, Creating, Available (two instances), and Configuring-enhanced-monitoring.

DB identifier	Role	Status
database-1	Instance	Stopped
database-2	Instance	Creating
database-3	Instance	Available
database-4	Instance	Available
database-5	Instance	Configuring-enhanced-monitoring

📢 DBインスタンスのステータス異常の例

- ✓ [Failed] (失敗) ▶ DB インスタンスのデータ復旧対応が必要
- ✓ 互換性のないネットワーク ▶ DB インスタンスの IP アドレスが取得可能となるようにする対応が必要
- ✓ ストレージ不足 ▶ DB インスタンスを変更してストレージを拡張する対応が必要

AWSコンソールでログファイルを確認（EC2、RDS 共通）

- CloudWatch Logsにてログを取得している場合はログを確認する



The screenshot shows the AWS CloudWatch Logs console interface. The breadcrumb navigation at the top reads: CloudWatch > ロググループ > /var/log/messages > i-0fdb640f331e0ea84. Below this, there is a section titled "ログイベント" (Log Events) with a sub-header "下のフィルターバーを使用して、ログイベント内の用語、語句、値の検索や照合ができます。フィルターパターンの詳細" (Use the filter bar below to search and match terms, phrases, and values within log events. See details for filter patterns). To the right of this text are buttons for "アクション" (Action), "テーリングを開始" (Start Tail), and "メトリクスフィルターを作成" (Create Metric Filter). Below the text is a search bar containing the text "warning" and a clear button (X). To the right of the search bar are buttons for "クリア" (Clear), time range filters (1分, 30分, 1時間, 12時間), a "カスタム" (Custom) button with a grid icon, a "ローカルタイムゾーン" (Local Time Zone) dropdown menu, and a "表示" (Display) dropdown menu with a gear icon. Below the search bar is a table with two columns: "タイムスタンプ" (Timestamp) and "メッセージ" (Message). The table contains two log entries:

タイムスタンプ	メッセージ
2021-11-11T09:22:28.000+09:00	Nov 11 00:22:28 ip-172-31-29-134 kernel: random: 7 urandom warning(s) missed due to ratelimiting
2021-11-11T10:41:26.000+09:00	Nov 11 01:41:26 ip-172-31-29-134 kernel: random: 7 urandom warning(s) missed due to ratelimiting

※CloudWatch Logsにてログを取得していない場合は、OSログやアプリケーションログを直接確認する必要がある。

AWSコンソールでリソース状況の確認(EC2 の場合)

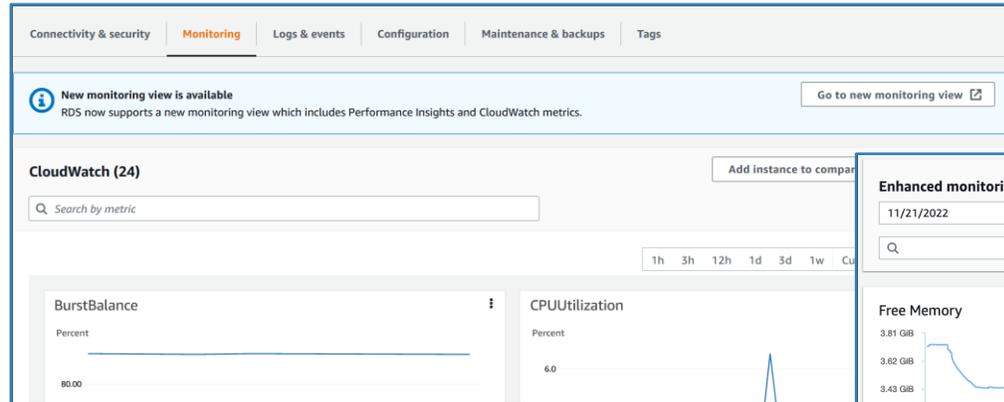
- EC2コンソールのモニタリングで異常な値が表示されていないかを確認する



モニタリング

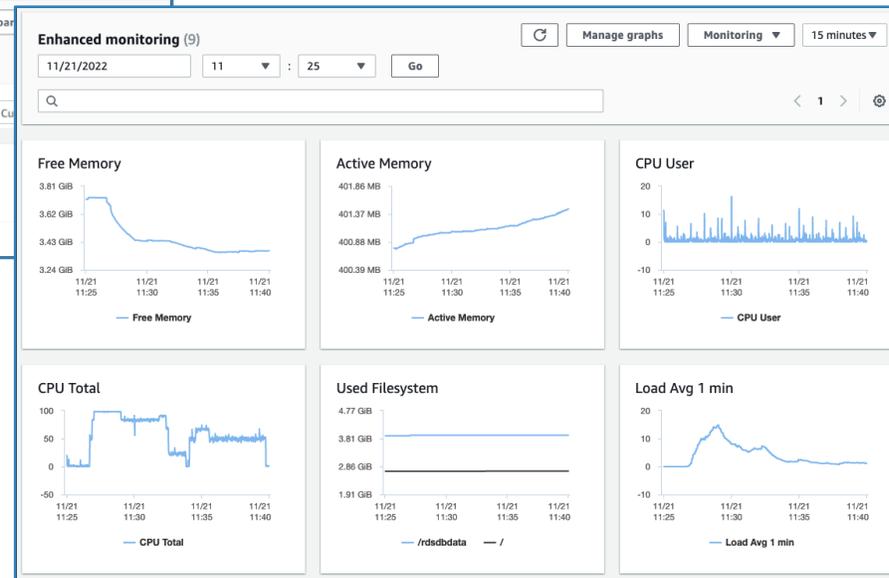
AWSコンソールでリソース状況の確認(RDS の場合)

- RDSコンソールのモニタリングで異常な値が表示されていないかを確認する



モニタリング

※デフォルトではCloudWatch メトリクスが表示される



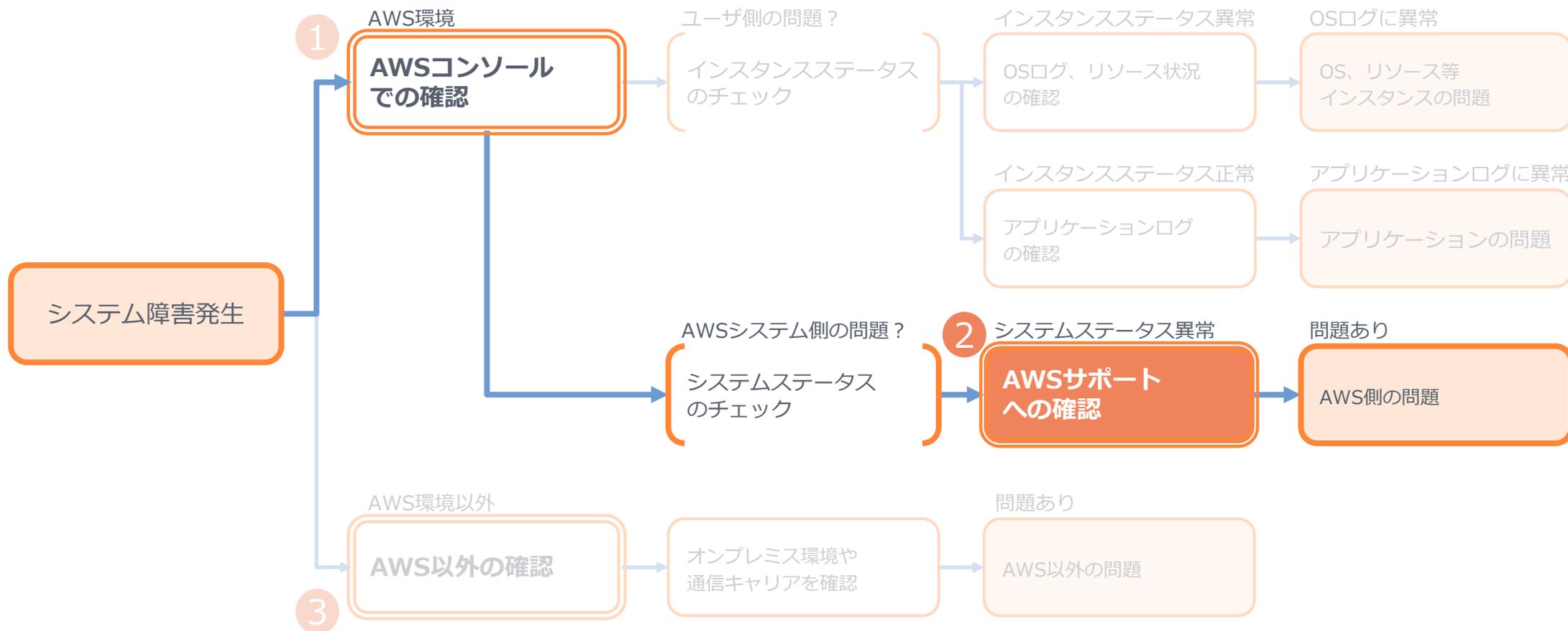
拡張モニタリング

※別途「拡張モニタリング」を有効にする必要がある

AWSサポートへの確認

AWSサポートへの確認

□ AWS環境調査のためAWSサポートに確認を行うケース



AWSコンソールでのAWSシステム側の確認（EC2 の場合）

- システムステータスのチェックでは、インスタンスが実行されているAWS システムをモニタリング

インスタンス: i-0fdb640f331e0ea84 (Utest)

詳細 | セキュリティ | ネットワーキング | ストレージ | **ステータスチェック** | モニタリング | タグ

ステータスチェック 情報
ステータスチェックは、i-0fdb640f331e0ea84 (Utest) によるアプリケーションの実行を妨げる可能性のある問題を検出します。

システムステータスのチェック
✔ システムの接続性チェックに合格しました

インスタンスステータスのチェック
✔ インスタンスの接続性チェックに合格しました

このインスタンスで発生している状況がチェックに反映されていない場合、または発生している問題が検出されない場合、インスタンスステータスをレポートします。

インスタンスステータスをレポート

システムステータスのチェック

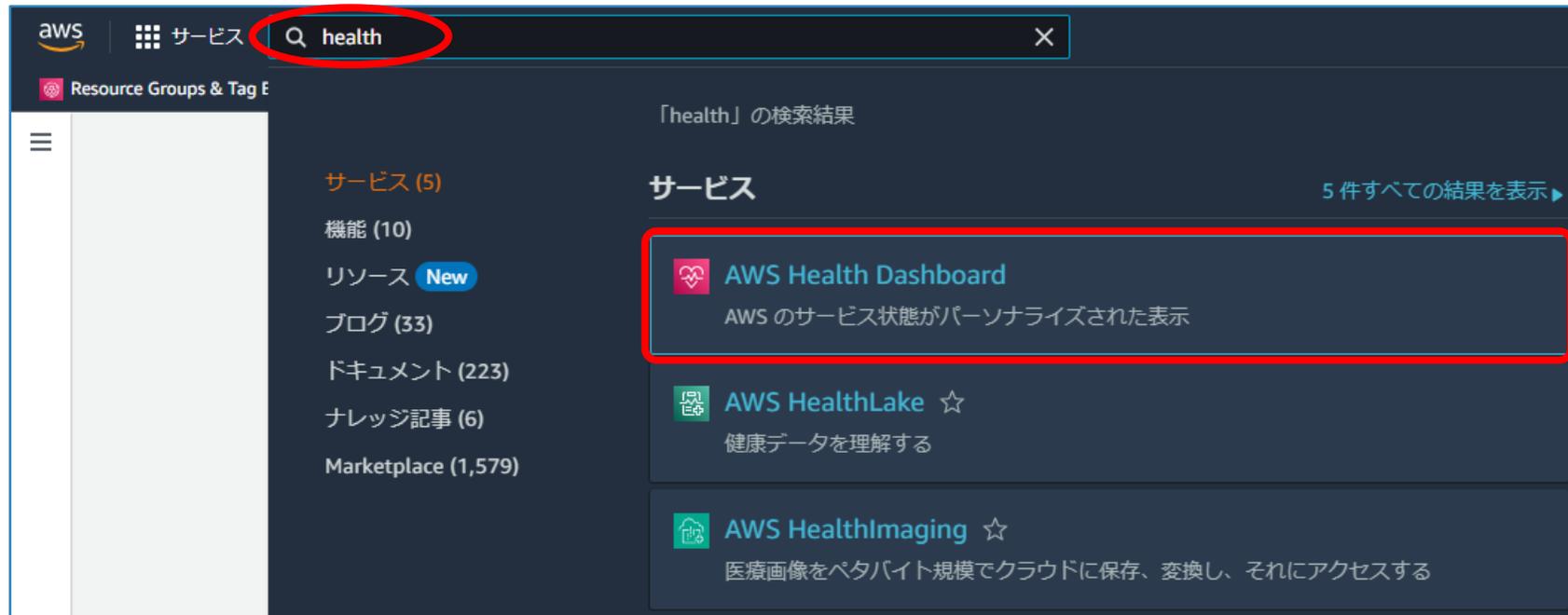
• AWSシステムの異常

📢 システムステータスチェックの失敗の原因となる問題の例

- ✓ ネットワーク接続の喪失
- ✓ システム電源の喪失
- ✓ 物理ホストのソフトウェアの問題
- ✓ ネットワーク到達可能性に影響する、物理ホスト上のハードウェアの問題

障害情報確認（マネージド・アンマネージド共通）

- AWSサービスの障害情報は **AWS Health Dashboard** で確認可能
 - ※ サービスの検索欄に「health」と入力することでサービスの選択肢に表示されるのでクリックすると別ウィンドウにAWS Health Dashboard画面が表示される



自アカウントで影響を受けているAWSサービスの確認

- AWSサービス全体のうち、自分のアカウントで影響を受けている障害情報はAWS Health Dashboard 内の **アカウントの状態** で確認することができる
- アカウントの状態 で検知した障害はSNSでメール送信可能

The screenshot displays the AWS Health Dashboard interface. On the left, a navigation sidebar lists various categories, with 'アカウントの状態' (Account Status) highlighted by a red rectangular box. The main content area is titled 'アカウントの状態' (Account Status) and includes a sub-header 'AWS リソースに影響する重要なイベントの情報を常に把握しましょう。' (Keep up-to-date with important events that affect AWS resources). Below this, there are tabs for '未解決の問題と最近の問題 (0)', 'スケジュールされた変更 (2)', 'その他の通知 (3)', and 'イベントログ'. A green checkmark icon is followed by the text '最近の問題はありません' (No recent issues) and '1分未満前に更新' (Updated less than 1 minute ago). A section titled '未解決の問題と最近の問題 (0)' contains a message: 'AWS インフラストラクチャに影響する可能性があるイベントを表示します。過去 24 時間以内の 0 個の問題点が解決されました。' (Display events that may affect AWS infrastructure. 0 issues were resolved within the last 24 hours). Below this is a search bar with the placeholder 'フィルターを追加' (Add filter) and a pagination indicator '< 1 >'. A table header is visible with columns: 'イベント' (Event), 'リージョン/ゾーン' (Region/Zone), '開始時刻' (Start time), '最終更新日時' (Last updated), and '影響を受けるリソース' (Resources affected). The table body is empty, with the text 'イベントはありません。' (No events) centered at the bottom.

AWSサービス全体の障害情報確認

- AWSサービス全体の障害情報は **サービスの状態** で確認することができる
- リージョン、サービス単位での確認が可能

The screenshot displays the AWS Health Dashboard interface. On the left sidebar, the 'サービスの状態' (Services Status) menu item is highlighted with a red box. The main content area shows the 'サービスの状態' (Services Status) section with a message '最近の問題はありません' (No recent issues) and a table of service status history for Amazon API Gateway in different regions.

サービス	RSS	本日	28 1月	27 1月	26 1月	25 1月	24 1月	23 1月
Amazon API Gateway (Hong Kong)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon API Gateway (Hyderabad)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon API Gateway (Jakarta)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢

AWS固有の障害情報の注意点

- 全ての障害が通知されるわけではない
- 局所的な障害はAWSサポートに確認したほうが確実
- X（旧Twitter）等のSNSや DowntetectorなどAWS障害発生状況を可視化する外部サービスなどを使ってリアルタイムで影響範囲を推測することも有効



※ 画像引用元 <https://downtetector.jp/>

AWSサポートの重要性

- AWSのようなクラウドサービスではすべての情報が公開されていないためサポートに問い合わせる必要がある
 - ✔ AWSではWeb、電話、Chatでの問い合わせサポートが利用できる
 - ✔ 障害情報もすべて公開はされていないので正確な情報はサポートに確認する必要がある



AWSサポート問い合わせ時の留意点

留意事項	ポイント
連絡方法（Web、電話、Chat）の選択について	詳細な情報共有は Web が最も確実で適している
解決したい課題を明確にする	課題がクリアに伝われば結果的に解決を早められる
状況を正確に共有する	対象リソースとリージョンを明記
	事象の発生時刻（タイムゾーン付き）と継続状況
	ログ類や画面キャプチャの共有



詳細は以下のAWS公式サイトを参照

<https://aws.amazon.com/jp/premiumsupport/tech-support-guidelines/>

AWSサポートプラン

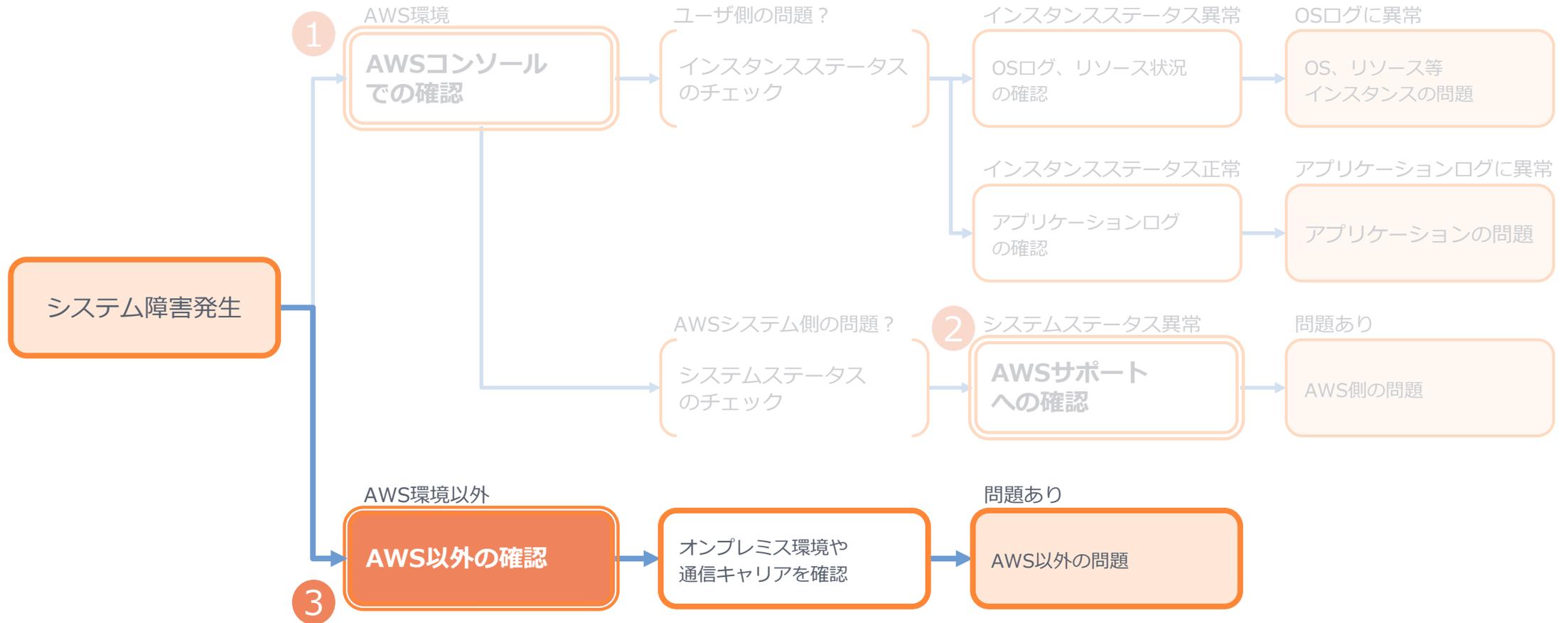
- AWSサポートプランは大きく開発者、ビジネス、エンタープライズの3種類
- 本番サービス向けはビジネス以上を推奨

AWSサポートプラン					
	有償サポートプラン 本番環境ではビジネス以上を推奨			テクニカルアカウント マネージャー	テクニカルアカウント マネージャー
	技術Q&A ・ Web ・ 平日8時～18時 ・ 応答時間12時間	技術Q&A ・ Web、電話、Chat ・ 年中無休 ・ 応答時間1時間	技術Q&A ・ Web、電話、Chat ・ 年中無休 ・ 応答時間1時間 ※ ビジネスクリティカル システムダウン時: 30分以内	技術Q&A ・ Web、電話、Chat ・ 年中無休 ・ 応答時間1時間 ※ ミッションクリティカル システムダウン時: 15分以内	
よくある質問	よくある質問	よくある質問	よくある質問	よくある質問	よくある質問
フォーラム	フォーラム	フォーラム	フォーラム	フォーラム	フォーラム
ベーシック	デベロッパー	ビジネス	エンタープライズ On-Ramp	エンタープライズ	
	← 開発環境		← 開発 + 本番環境		

AWS以外の確認

AWS以外の確認

□ AWS以外の確認を行うケース



AWS環境以外の確認

□ 障害発生要因の特定

確認事項

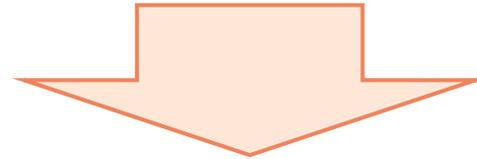
- ✓ インターネット接続回線で障害が発生していないか
- ✓ SSH接続できるか、VPN接続ができるか
- ✓ オンプレミスとのハイブリッド環境等であれば
オンプレミス側の確認
- ✓ ユーザ観点での確認はどうか
 - 特定ユーザなのかすべてのユーザなのか



システム障害への対策

システム障害への対策

- 障害発生は予測不可能であり、また不可避である
- AWS ではインフラの障害に対し要因分析および発生率の低減に努めているが、障害の発生を完全に防ぐことは困難
- このため AWS では「Design For Failure」(故障を前提とした設計)を推奨



障害監視による通知

- メトリクス
- ログ
- AWS Health イベント

障害の未然防止

- 処理の自動リトライ
- 構成の冗長化

障害後の復旧措置

- 事前のバックアップ
- 障害後のリカバリ

障害監視による通知（障害通知）

障害通知とは

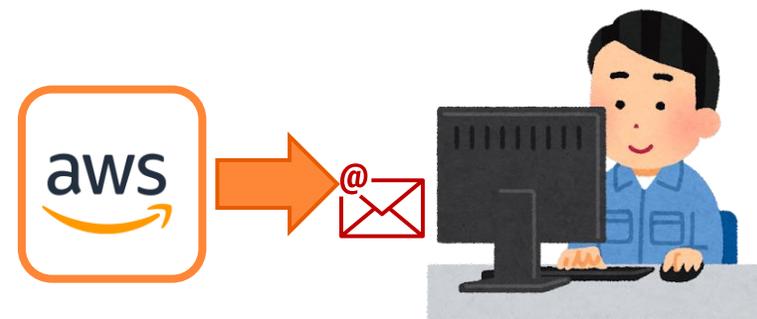
- Webサービス停止、システム停止等の**障害**が発生した場合に管理者へ**通知**すること

障害通知の目的

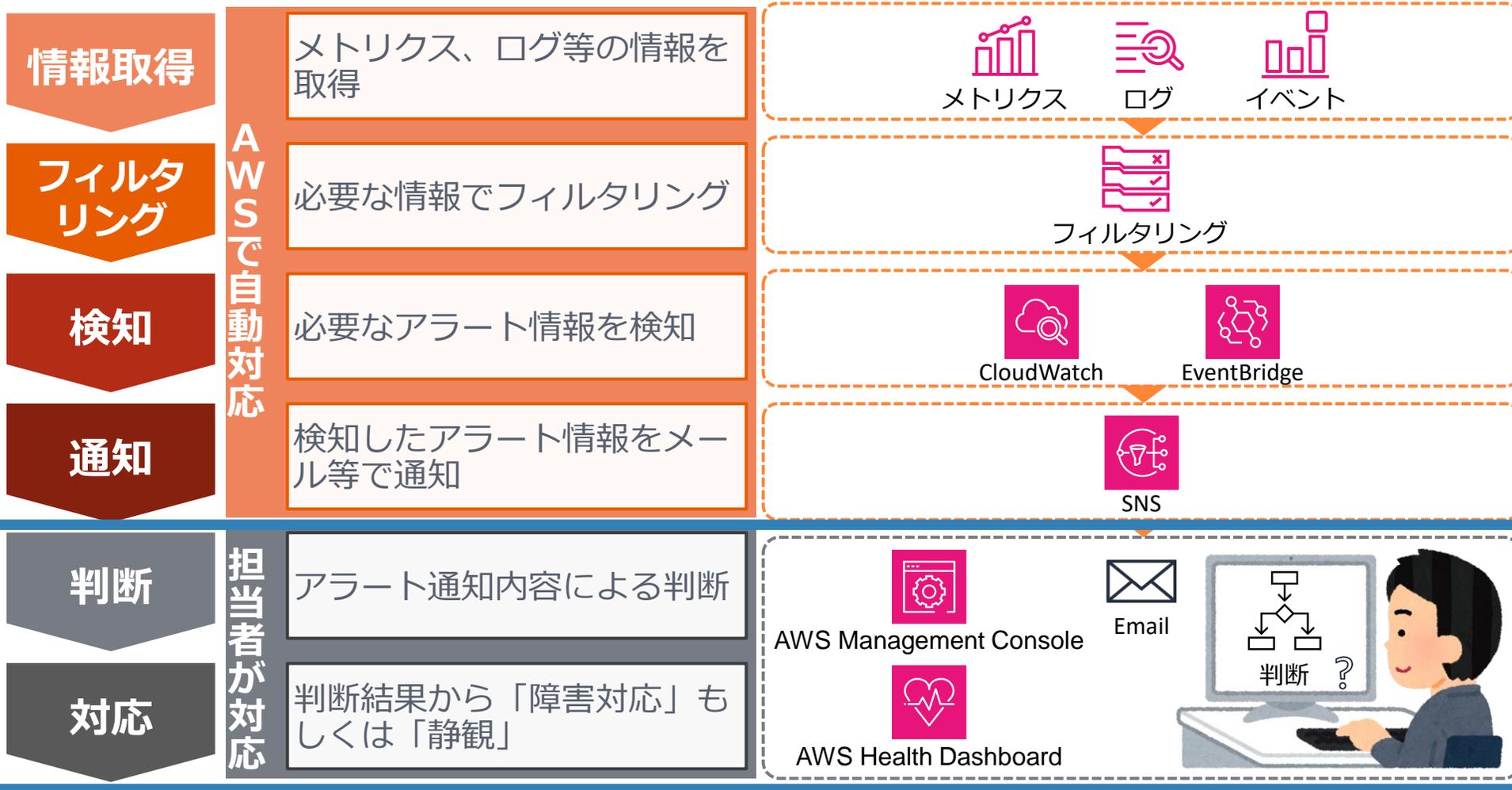
- 障害発生時にできるだけ早く気づき対処することで**サービス影響などの被害を低減**すること
- 障害に至らなくてもリソースに余裕がない場合に通知することで**障害を未然に防ぐ**こと

障害通知の手段

- 通常はメールでの通知
- SMS、チャットツール(Slack 等)、電話で通知することもある



障害対応に至るフローとAWSサービスとの対応



システム障害に備えて

- システム障害に備えて、あらかじめ情報を取りまとめて常に最新の状態を保つことが重要

要件	要素	備考
システム情報の可視化	構成図	全体の構成情報を管理
	サーバ設計書	サーバごとの設計情報
障害対応手順の確立	対応フロー	対応者の連絡先整備
	対応手順書	障害対応の手順を整備 ➤ 障害報告のためのエビデンスを考慮



まとめ

まとめ

- まずはAWS側の問題なのかユーザー側の問題なのかを判別する
 - ▶ 大きな範囲の特定から対象を絞っていく
- AWSサポートへの確認は重要
- 従来型の運用と同様ドキュメントの整備も大切
- 障害監視による通知も有用



実績豊富なエンジニア集団の技術と開発ツールで
「開発期間/コスト削減」「品質向上」を実現

株式会社スタイルズ

<https://www.stylez.co.jp>

東京都千代田区神田小川町1-2 風雲堂ビル6階

Tel:03-5244-4111

オープンソースソフトウェア推進