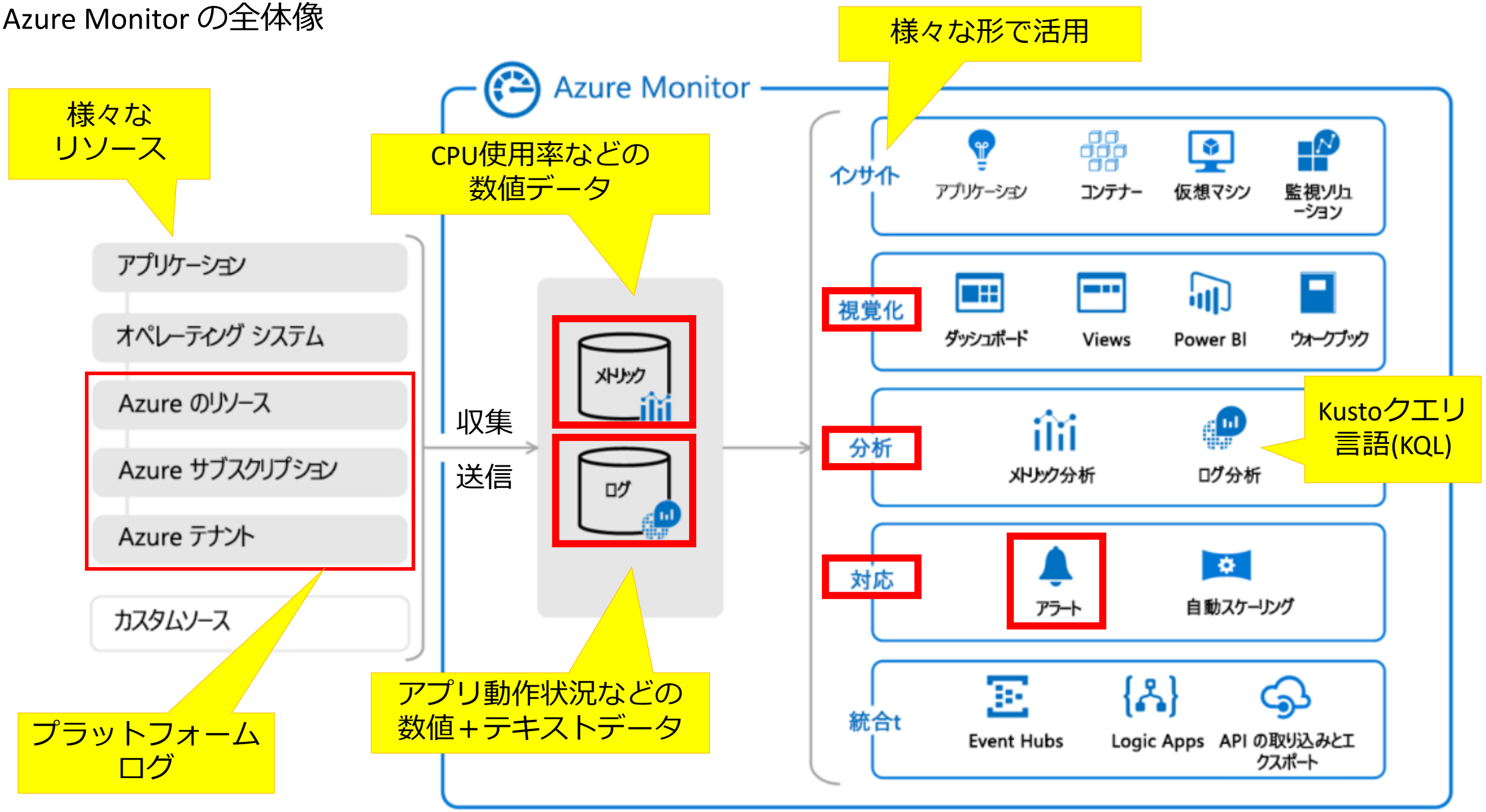
Azure Monitor の全体像



主な機能

- **メトリックの監視および視覚化**メトリックは、システムの正常性、操作、およびパフォーマンスを理解するのに役立つ Azure リソースから利用できる数値です。
- **ログのクエリと分析**ログは、アクティビティ ログ、診断ログ、および監視ソリューションからのテレメトリです。分析クエリは、トラブルシューティングと視覚化に役立ちます。
- **アラートとアクションの設定**アラートは重大な状態を通知し、メトリックまたはログからのトリガーに基づいて自動修正アクションを実行する場合があります。

メトリックの監視と視覚化

メトリックは、システムの正常性、運用、パフォーマンスを理解するのに役立つ Azure リソースから利用できる数値です。

メトリックの探索

ログのクエリと分析

ログは、アクティビティログ、診断ログ、および監視ソリューションからのテレメトリです。分析クエリは、トラブルシューティングと可視化に役立ちます。

ログの検索

アラートとアクションの設定

アラートは重大な状態を通知し、メトリックまたはログからのトリガーに基づいて修正された自動アクションを実行する可能性があります。

アラートの作成

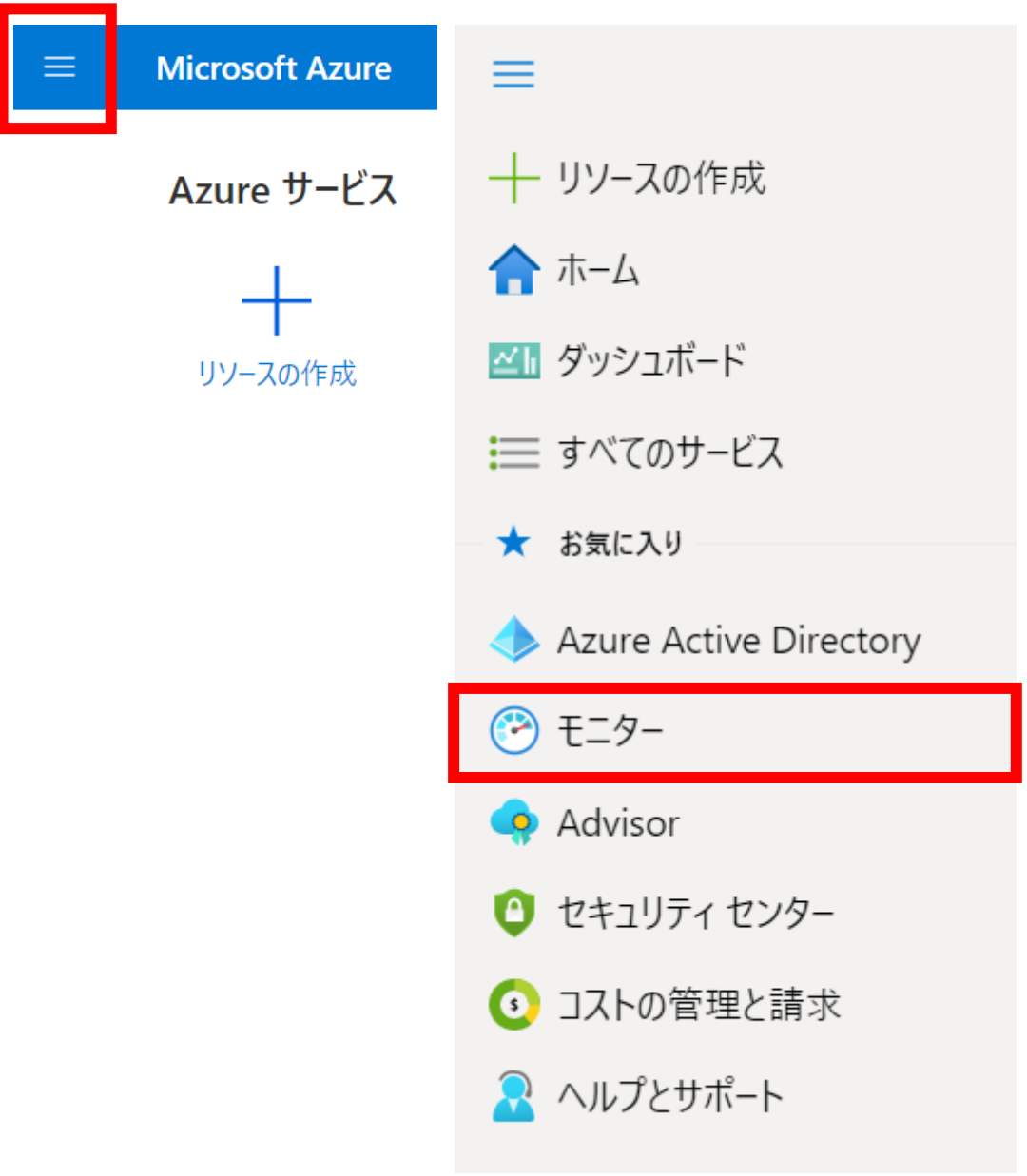
「メトリック」と「ログ」

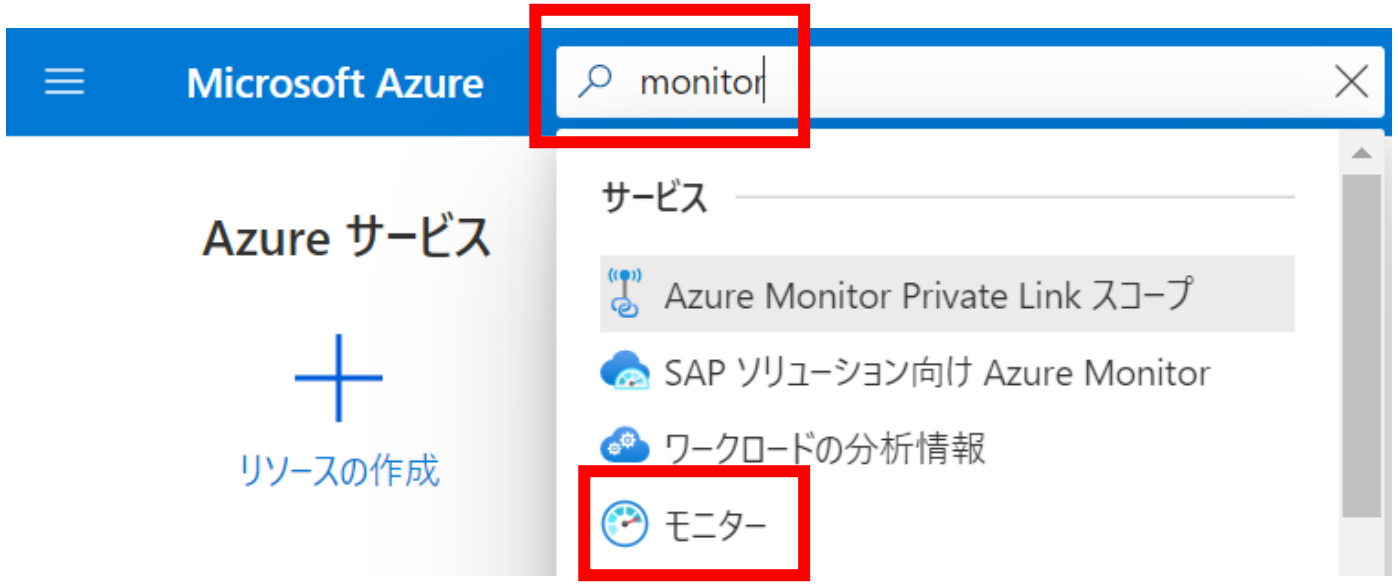
データプラットフォームの監視

Azure Monitor によって収集されたすべてのデータは、メトリックとログの 2 つの基本的な種類のいずれかです。

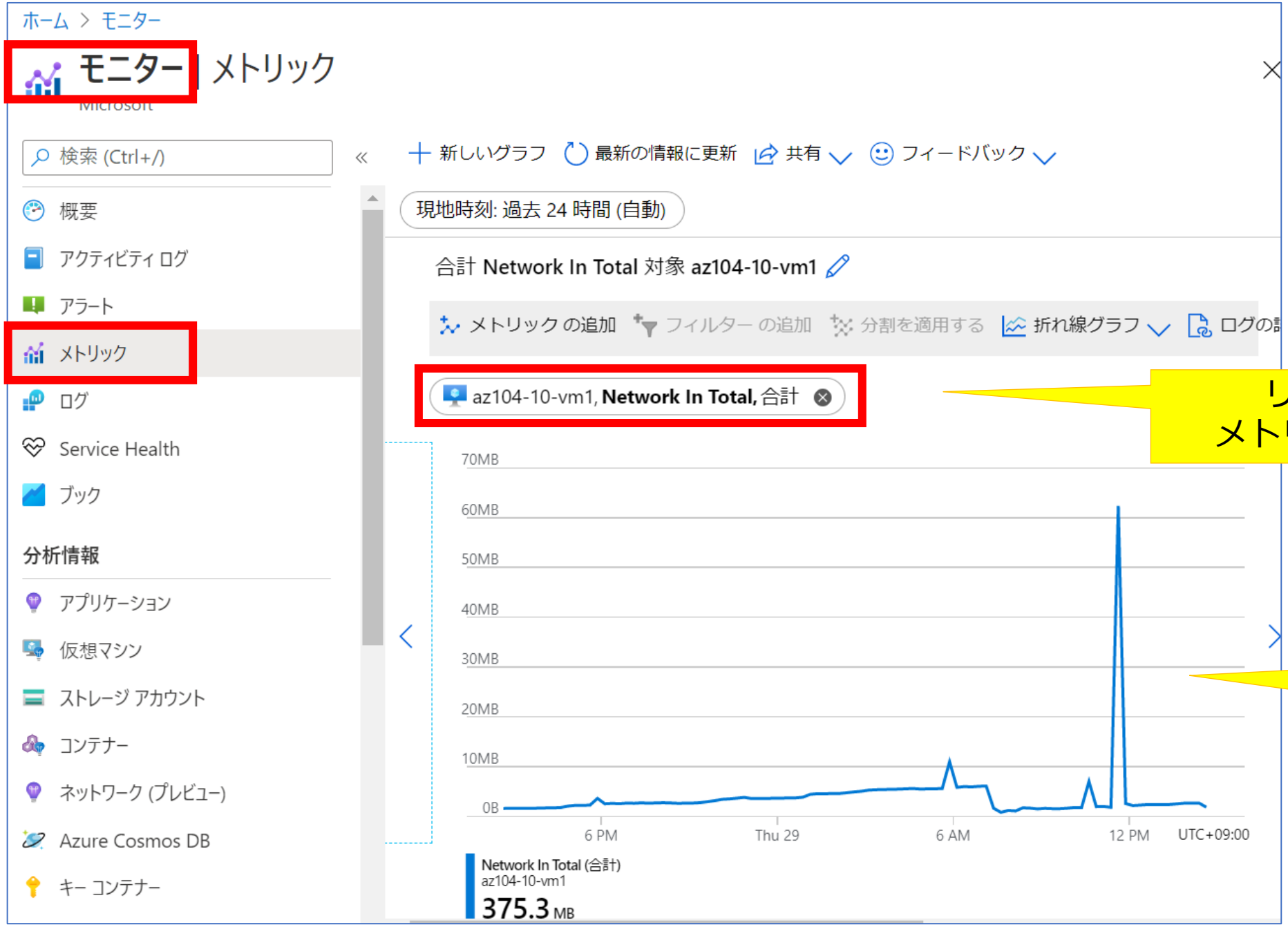
- **メトリック** は、特定の時点におけるシステムの一部の側面を記述する数値です。軽量であり、ほぼリアルタイムのシナリオをサポートできます。
- **ログ** には、種類ごとに異なるプロパティ セットを持つレコードに編成されたさまざまな種類のデータが含まれます。イベントやトレースなどの製品利用統計情報は、すべてを分析用に組み合わせることができるようにするために、パフォーマンス データとともにログとして格納されます。

Azure Monitor (モニター)の起動





メトリックの表示方法（Log Analytics の起動方法）



リソースと
メトリックを選択

グラフで
表示される

ログの表示方法（Log Analytics の起動方法）

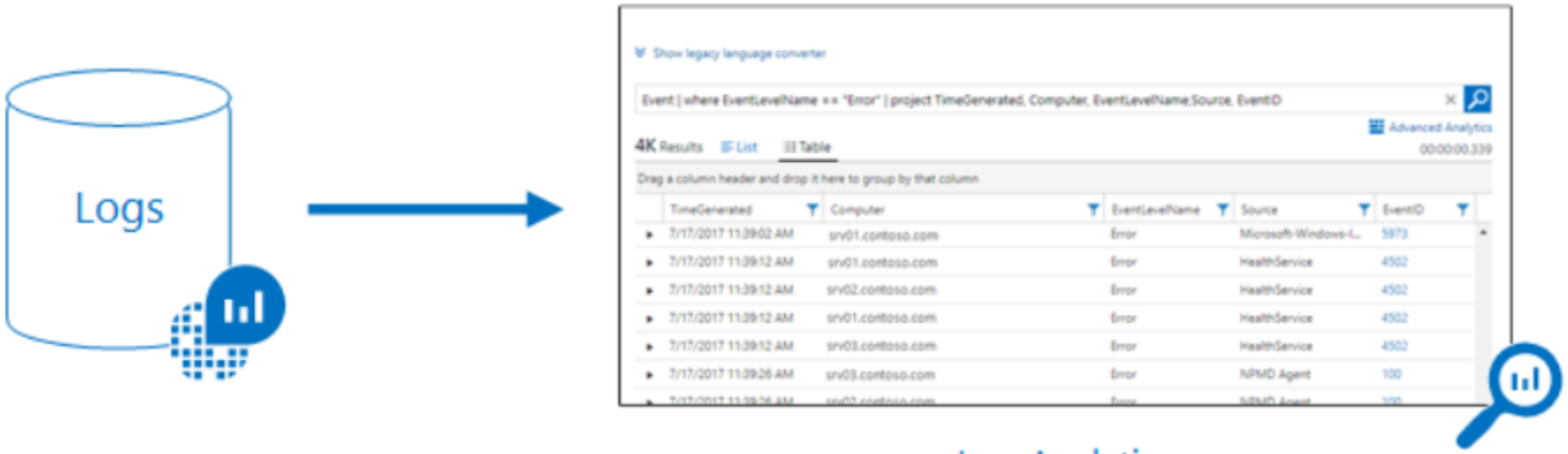
Log Analytics は、Azure portal 内の複数の場所から起動できます。 Log Analytics で使用できるデータのスコープは、起動方法によって決まります。 詳しくは、「クエリ スコープ」を参照してください。

- [Azure Monitor] メニューまたは [Log Analytics ワークスペース] メニューの [ログ] を選択します。
- Application Insights アプリケーションの [概要] ページから [ログ] を選択します。
- Azure リソースのメニューから [ログ] を選択します。

ログデータの分析: Kusto クエリ言語 (KQL)

Azure Monitor が収集したログ データは、収集されたデータをすばやく検索、統合、分析するクエリを使用して分析できます。 Azure portal で Log Analytics を使用してクエリを作成してテストした後、別のツールを使用してデータを直接分析するか、クエリを保存して視覚化またはアラート ルールで利用できます。

Azure Monitor では、Azure Data Explorer で使用される Kusto クエリ言語のバージョンを使用します。それは、単純なログ検索に適していますが、集計、結合、スマート分析などの高度な機能も備えています。 さまざまなレッスンを利用すれば、クエリ言語はすぐに覚えることができます。 既に SQL や Splunk に習熟しているユーザーには、別途ガイダンスが用意されています。



Log Analytics

Kusto クエリ

クエリは読み取り専用の要求であり、データを処理し、その処理の結果を返します。データやメタデータが修正されることはありません。 Kusto クエリでは、SQL 言語または Kusto クエリ言語を使用できます。 後者の例として、次のクエリでは、`Logs` テーブルの行のうち、`Level` 列の値が文字列 `Critical` と等しいものをカウントします。

Kusto コピー

```
Logs
| where Level == "Critical"
| count
```

https://docs.microsoft.com/ja-jp/azure/data-explorer/kusto/concepts/

History [edit]

The development of the product began in 2014 as a grassroots incubation project in the Israeli R&D center of Microsoft,[12] with the internal code name 'Kusto[9][7]' (named after Jacques Cousteau, as a reference to "exploring the ocean of data"). The project aim was to address Azure services' needs for fast and scalable log and telemetry analytics. In 2016 it became the backend big-data and analytics service for Application Insights Analytics [13] The product was announced as a Public Preview product at the Microsoft Ignite 2018 conference,[14] and was announced as a general availability product at the Microsoft Ignite conference of February 2019.[15]

この製品の開発は、マイクロソフトのイスラエルR＆Dセンターでの草の根インキュベーションプロジェクトとして2014年に開始され、内部コード名は「Kusto」（ジャック・クストーの「データの海を探索する」にちなんで名付けられました）です。 プロジェクトの目的は、高速でスケーラブルなログおよびテレメトリ分析に対するAzureサービスのニーズに対応することでした。 2016年には、Application Insights Analyticsのバックエンドビッグデータおよび分析サービスになりました。この製品は、Microsoft Ignite 2018カンファレンスでパブリックプレビュー製品として発表され、2019年2月のMicrosoftIgniteカンファレンスで一般提供製品として発表されました。

Jacques Cousteau

AC

Jacques-Yves Cousteau in 1972

https://en.wikipedia.org/wiki/Azure_Data_Explorer

https://en.wikipedia.org/wiki/Jacques_Cousteau

Azure Monitor が収集するデータ

Azure Monitor はさまざまなソースからデータを収集できます。 アプリケーションやそれが依存するオペレーティング システムやサービスから、プラットフォーム自体に至るまで、アプリケーションのさまざまな階層のデータ監視を検討することができます。 Azure Monitor は、以下のそれぞれの層からデータを収集します。

- **アプリケーション監視データ**: プラットフォームを問わず、記述したコードのパフォーマンスと機能に関するデータ。
- **ゲスト OS 監視データ**: アプリケーションが実行されているオペレーティング システムに関するデータ。 これは Azure、別のクラウド、またはオンプレミスで実行できます。
- **Azure リソース監視データ**: Azure リソースの操作に関するデータ。
- **Azure サブスクリプション監視データ**: Azure サブスクリプションの操作および管理に関するデータと、Azure 自体の正常性および操作に関するデータ。
- **Azure テナントの監視データ**: Azure Active Directory など、テナント レベルの Azure サービスの操作に関するデータ。

リソースログ

アクティビティログ

Azure ADログ

https://docs.microsoft.com/ja-jp/azure/azure-monitor/overview#monitoring-data-platform

Azure Monitor が収集するデータ

Azure Monitor はさまざまなソースからデータを収集できます。 アプリケーションやそれが依存するオペレーティング システムやサービスから、プラットフォーム自体に至るまで、アプリケーションのさまざまな階層のデータ監視を検討することができます。 Azure Monitor は、以下のそれぞれの層からデータを収集します。

- **アプリケーション監視データ**: プラットフォームを問わず、記述したコードのパフォーマンスと機能に関するデータ。
- **ゲスト OS 監視データ**: アプリケーションが実行されているオペレーティング システムに関するデータ。 これは Azure、別のクラウド、またはオンプレミスで実行できます。
- **Azure リソース監視データ**: Azure リソースの操作に関するデータ。
- **Azure サブスクリプション監視データ**: Azure サブスクリプションの操作および管理に関するデータと、Azure 自体の正常性および操作に関するデータ。
- **Azure テナントの監視データ**: Azure Active Directory など、テナント レベルの Azure サービスの操作に関するデータ。

この3つを
プラットフォーム
ログ と
呼ぶ

https://docs.microsoft.com/ja-jp/azure/azure-monitor/overview#monitoring-data-platform

プラットフォーム ログ（リソース ログ、アクティビティ ログ、Azure AD ログ）

ログ	レイヤー	説明
リソース ログ	Azure リソース	Azure リソース ("データ プレーン") 内で実行された操作に関する分析情報を提供します。たとえば、Key Vault からのシークレットの取得や、データベースに対する要求などです。 リソース ログの内容は、Azure サービスとリソースの種類によって異なります。 リソース ログは、以前は診断ログと呼ばれていました。
アクティビティ ログ	Azure サブスクリプション	Service Health イベントの更新に加えて、外部 ("管理プレーン") からサブスクリプションの各 Azure リソースに対する操作についての分析情報を提供します。 アクティビティ ログを使用して、サブスクリプションのリソースに対して行われるすべての書き込み操作 (PUT、POST、DELETE) について、"何を"、"誰が"、"いつ" 行ったのかを確認できます。 Azure サブスクリプションごとに 1 つのアクティビティ ログがあります。
Azure Active Directory ログ	Azure テナント	サインイン アクティビティの履歴と、特定のテナントに対して Azure Active Directory で行われた変更の監査証跡が含まれます。

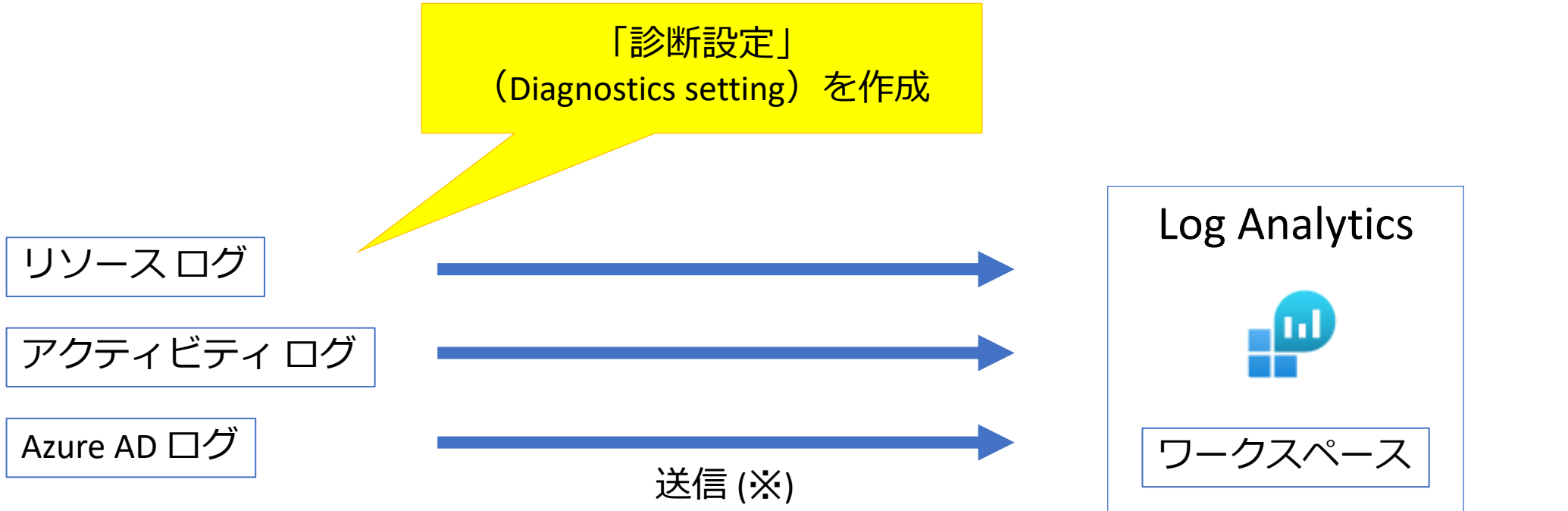
デフォルトでは保管されない

90日保管

30日保管 ※Premium P2の場合

Azure AD にレポート データが保存される期間 | Microsoft Docs
Azure リソース ログ - Azure Monitor | Microsoft Docs
https://docs.microsoft.com/ja-jp/azure/azure-monitor/platform/platform-logs-overview

プラットフォーム ログ（リソース ログ、アクティビティ ログ、Azure AD ログ）を Log Analytics ワークスペースに送信して分析する

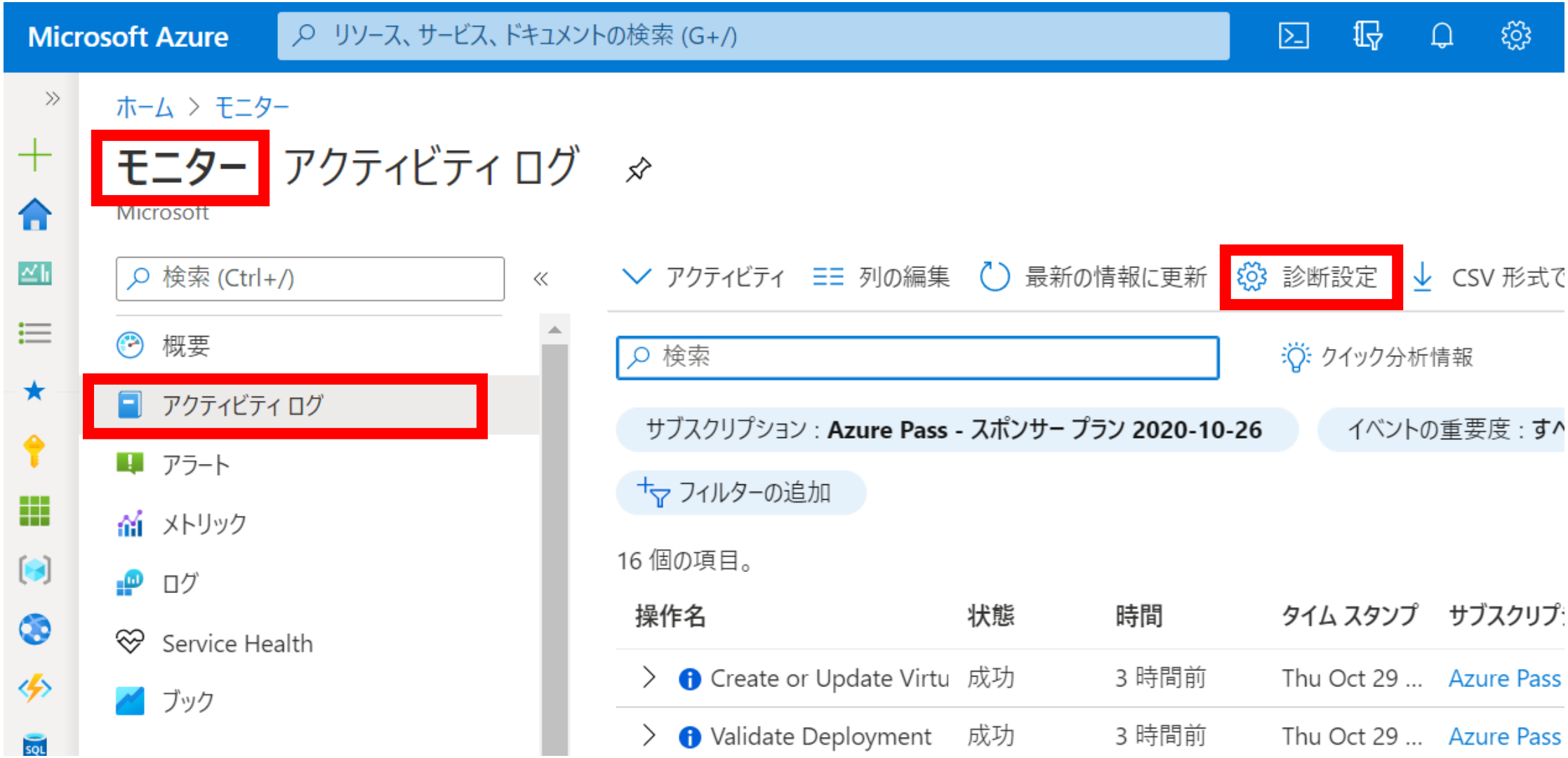


- ログの長期保存(30～720日)
- 複雑な分析

(※) Event Hub や Azure Storage にも送信可能

https://docs.microsoft.com/ja-jp/azure/azure-monitor/platform/resource-logs
https://docs.microsoft.com/ja-jp/azure/azure-monitor/platform/activity-log
https://docs.microsoft.com/ja-jp/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics

「診断設定」（Diagnostics setting）の作成 （アクティビティ ログでの例）



診断設定

最新の情報に更新　フィードバックの提供

サブスクリプション *

Azure Pass - スポンサー プラン 2020-10-26

従来のエクスペリエンスをお探しですか。ここをクリックすると [アクティビティ ログのエクスポート] ブレードが起動します

サブスクリプション のプラットフォーム ログとメトリックの選択した宛先へのストリーミング エクスポートを構成するため、診断設定を作成できます。診断設定に関する詳細情報

診断設定

名前	ストレージ アカウント	イベント ハブ
診断設定が定義されていません		

＋ 診断設定を追加する

上の [診断設定を追加する] をクリックして、次のデータのコレクションを構成してください:

- Administrative
- Security
- ServiceHealth
- Alert
- Recommendation
- Policy
- Autoscale
- ResourceHealth

診断設定

保存　破棄　削除　フィードバックの提供

診断設定では、サブスクリプション から収集するプラットフォーム ログとメトリックの両方、またはいずれかのカテゴリの一覧、またそれらをストリーミングする 1 つまたは複数の宛先を指定します。宛先の通常の利用料金が発生します。さまざまなログのカテゴリとそれらのログのコンテンツに関する詳細情報

診断設定の名前 *

カテゴリの詳細

log

- [x] Administrative
- [x] Security
- [x] ServiceHealth
- [x] Alert
- [x] Recommendation
- [x] Policy
- [x] Autoscale
- [x] ResourceHealth

宛先の詳細

- [x] Log Analytics への送信

サブスクリプション

Azure Pass - スポンサー プラン 2020-10-26

Log Analytics ワークスペース

DefaultWorkspace-a1e4fbf9-7099-4568-960e-1c7f6e7308c1-EUS (eastus)

- [ ] ストレージ アカウントへのアーカイブ
- [ ] イベント ハブへのストリーム

収集したい
アクティビティ ログを選択

送信先の
Log Analyticsワークスペース
（事前に作成しておく）を選択

Azure Monitor アラート

リソースの選択

監視するリソースを選択します。選択できるシグナルの種類が右下に表示されます。

サブスクリプション別でフィルター * ⓘ　　リソースの種類でフィルター ⓘ　　場所でフィルター ⓘ

Azure Pass - スポンサー プラン 2020-10...　　Virtual Machines　　すべて

項目の検索とフィルター...

	リソース	リソースの種類	場所
☐	Azure Pass - スポンサー プラン 2020-10-2(	Subscription	米国東部
☐	az104-10-rg0	Resource group	米国東部
☑	az104-10-vm1	仮想マシン	米国東部

シグナル ロジックの構成

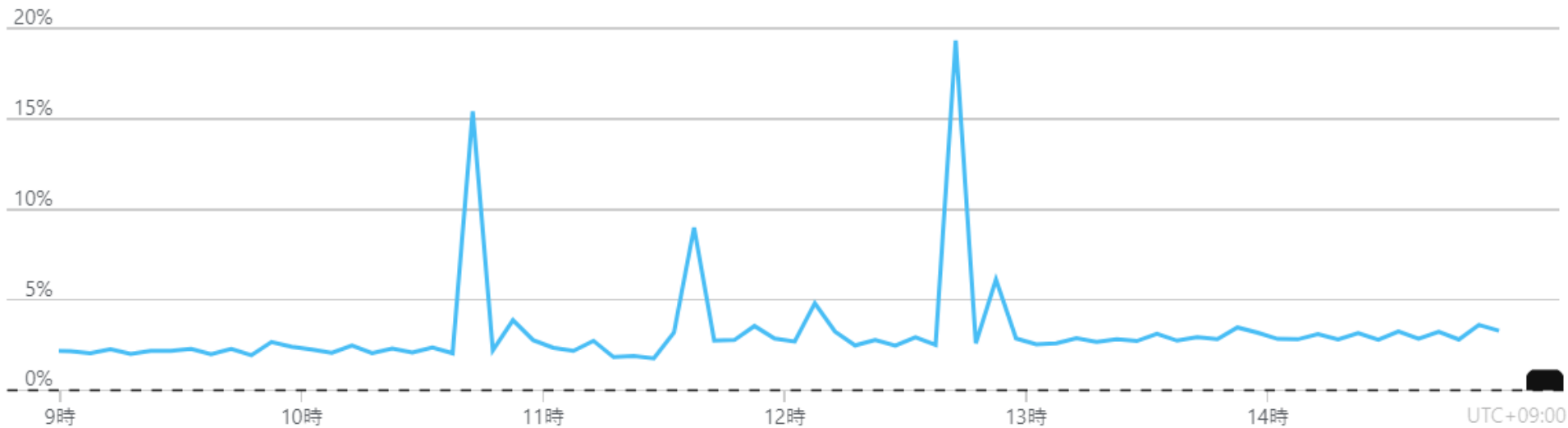
アラートをトリガーするためのロジックを定義します。グラフを使用してデータの傾向を確認します。

← シグナルの選択に戻る

Percentage CPU (プラットフォーム)
The percentage of allocated compute units that are currently in use by the Virtual Machine(s)

グラフの期間 ⓘ

直近 6 時間



Percentage CPU (平均)
az104-10-vm1
3.2164 %

アラート ロジック

しきい値 ⓘ

Static　動的

演算子 ⓘ

次の値より大きい

集計の種類 * ⓘ

平均

しきい値 * ⓘ

80

%

条件のプレビュー

percentage cpu の 平均 が80 % 次の値より大きい 場合

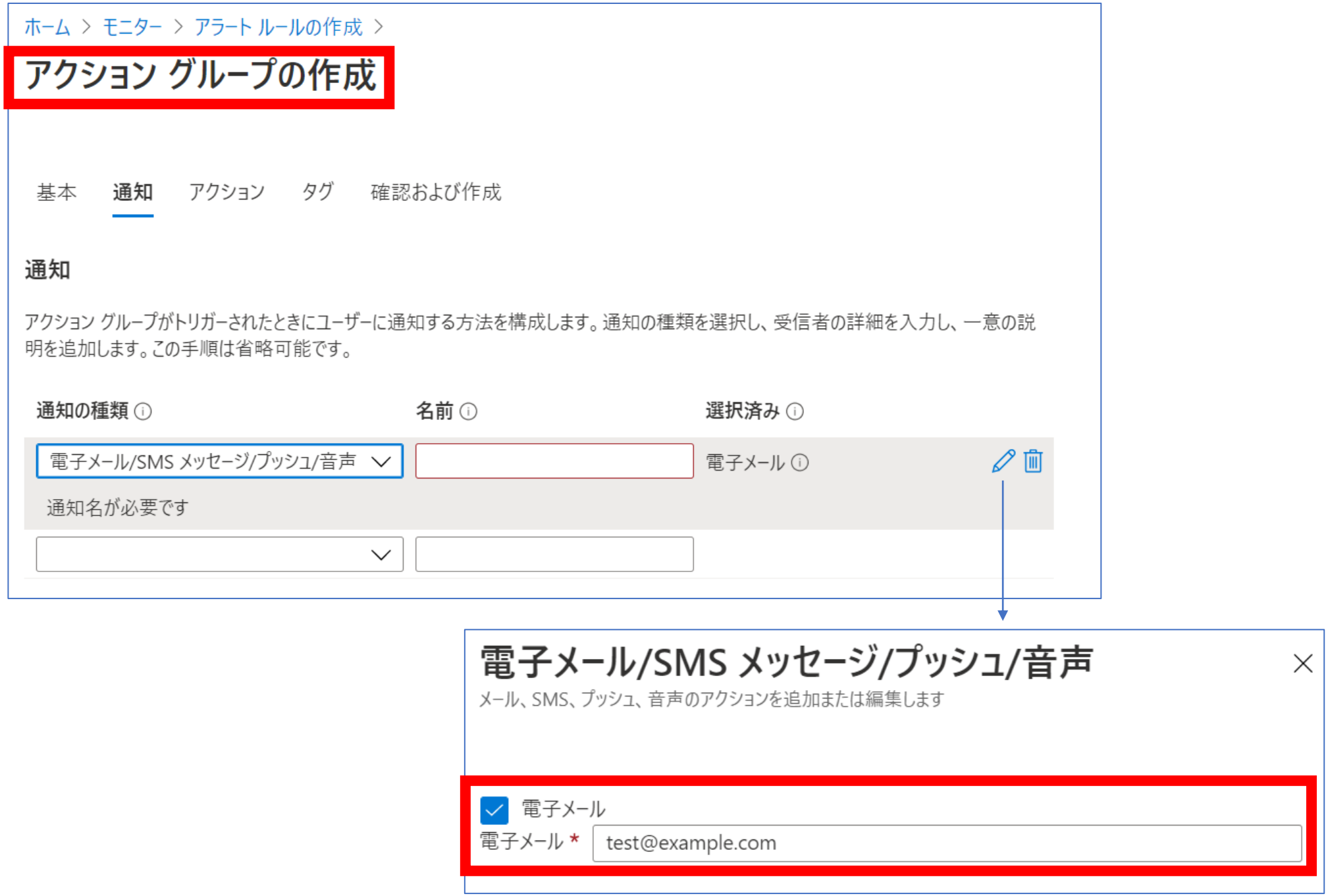
評価基準

集約粒度 (期間) * ⓘ

5 分

評価の頻度 ⓘ

1 分ごと


ホーム > モニター > アラート ルールの作成 >
アクション グループの作成
基本
通知
アクション
タグ
確認および作成
通知
アクション グループがトリガーされたときにユーザーに通知する方法を構成します。通知の種類を選択し、受信者の詳細を入力し、一意の説明を追加します。この手順は省略可能です。
通知の種類
名前
選択済み
電子メール/SMS メッセージ/プッシュ/音声
電子メール
通知名が必要です
電子メール/SMS メッセージ/プッシュ/音声
メール、SMS、プッシュ、音声のアクションを追加または編集します
電子メール
電子メール *
test@example.com

アクションの種類

- **Automation Runbook** - Automation Runbook は、システムおよびネットワークの運用プロセスをサポートするワークフローを定義、構築、調整、管理、およびレポートする機能です。Runbook ワークフローは、アプリケーション、データベース、ハードウェアなど、あらゆる種類のインフラストラクチャの要素と潜在的にインタラクトします。
- **Azure Function** – Azure Functions は、インフラストラクチャを明示的にプロビジョニングや管理をすることなく、オンデマンドでコードを実行できるサーバーレス コンピューティング サービスです。
- **電子メールの Azure Resource Manager のロール** – サブスクリプションのロールのメンバーにメールを送信します。メールは、ロールの Azure AD ユーザー メンバーにのみ送信されます。メールは Azure AD グループやサービス プリンシパルには送信されません。
- **メール/SMS/プッシュ/音声** - 任意のメール、SMS、プッシュ、または音声のアクションを指定します。
- **ITSM** – サポートされている IT Service Management (ITSM) 製品/サービスと Azure を接続します。これには ITSM 接続が必要です。
- **Logic Apps** – Logic Apps はワークフローを自動化することで、ビジネスに不可欠なアプリとサービスを接続します。
- **Webhook** – Webhook は、外部アプリケーションがシステムと通信できるようにする HTTP エンドポイントです。

アラートの状態

アラートの状態を設定して、解決プロセスの場所を指定できます。アラートルールで指定された条件が満たされると、アラートが作成されるか発生し、ステータスは「**新規**」になります。アラートを確認したとき、およびアラートを閉じたときにステータスを変更できます。すべての状態の変更は、アラートの履歴に保存されます。次のアラート状態がサポートされています。

状態	説明
新規	問題は検出されたばかりで、まだレビューされていません。
確認済み	管理者がアラートを確認し、作業を開始しました。
終了	問題は解決しました。アラートが終了した後でも、別の状態に変更すると再度開くことができます。

✓ アラート状態はモニター状態とは異なり、無関係です。アラート状態はユーザーが設定します。モニター条件はシステムによって設定されます。アラートが発生すると、アラートのモニター状態は発生済みに設定されます。アラートの発生を引き起こした基本的な条件がクリアされると、モニターの状態は解決済みに設定されます。アラートの状態は、ユーザーが変更するまで変わりません。