# Azure VM上Webアプリの監視ベストプラクティス（Azure Monitor & Log Analytics）

## 概要

Azure VM上で稼働するWebアプリケーションの包括的な監視を実現するには、**Azure Monitor**と**Log Analytics Workspace**を組み合わせたソリューションが有効です。Azure Monitorはメトリックやログを統合的に収集・分析・アラートできるプラットフォームであり、Log Analytics Workspaceはそのデータを蓄積しクエリや分析を行う基盤です。ここでは、VMとその上のWebアプリに対する監視構成のベストプラクティスを、データ収集の方法からアラート通知・外部連携まで詳述します。短時間で把握できるよう、ポイントごとに見出しを設け、箇条書きやコードブロックで具体例を示します。

## 監視アーキテクチャの全体像

*Azure Monitorを用いたエンタープライズ監視アーキテクチャの概略図。各種リソースから収集されたログ・メトリックがLog Analyticsワークスペースに集約され、Azure Monitorで分析・アラートが行われる。また、アラートからITSMツール等へのチケット発行（外部連携）も可能*[*[1][2]*](https://learn.microsoft.com/en-us/azure/azure-monitor/fundamentals/enterprise-monitoring-architecture#:~:text=,created%20in%20the%20ITSM%20system)

上図のように、本シナリオではAzure VM上のエージェントがログとメトリックを収集し、**Log Analytics Workspace**に送信します。Azure Monitorはこのデータを基に分析・可視化を行い、必要に応じて**アラート**を発報します。アラートは**アクショングループ**を介して通知され、メール/SMSはもちろん、WebhookやAzure Functions経由で外部の監視サービス（Monitoring & Event Management as a Serviceなど）へ連携することが可能です[[3]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/best-practices-alerts#:~:text=match%20at%20L173%20%E3%82%B0%E3%83%AB%E3%83%BC%E3%83%97%E3%81%8C%E4%BD%BF%E7%94%A8%E3%81%95%E3%82%8C%E3%82%8B%E5%A0%B4%E5%90%88%E3%81%AF%E3%80%81%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E9%80%9A%E7%9F%A5%E3%83%9A%E3%82%A4%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AB%E5%90%AB%E3%82%81%E3%82%8B%E7%8B%AC%E8%87%AA%E3%81%AE%E3%83%97%E3%83%AD%E3%83%91%E3%83%86%E3%82%A3%E3%82%92%E8%BF%BD%E5%8A%A0%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20%E3%81%93%E3%82%8C%E3%82%89%E3%81%AE%E3%83%97%E3%83%AD%E3%83%91%E3%83%86%E3%82%A3%E3%81%AF%E3%80%81Webhook%E3%80%81Azure,Apps%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%99%E3%82%8B%E3%81%A8%E3%80%81%E7%B5%B1%E5%90%88%E3%81%AE%E3%81%9F%E3%82%81%E3%81%AB%E3%83%AF%E3%83%BC%E3%82%AF%E3%83%95%E3%83%AD%E3%83%BC%E3%82%92%E3%83%93%E3%83%AB%E3%83%89%E3%81%8A%E3%82%88%E3%81%B3%E3%82%AB%E3%82%B9%E3%82%BF%E3%83%9E%E3%82%A4%E3%82%BA%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20Logic%20Apps%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E9%80%9A%E7%9F%A5%E3%82%92%E3%82%AB%E3%82%B9%E3%82%BF%E3%83%9E%E3%82%A4%E3%82%BA%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)。

主要コンポーネントは以下の通りです：

* **Azure Monitor エージェント (AMA)**：VM上にインストールするエージェント。旧来のLog Analyticsエージェント(MMA/OMS)に代わり、**Azure Monitor Agentに移行**することでデータ収集ルールごとの柔軟な設定やフィルタリングが可能になります[[4]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E8%A9%B3%E7%B4%B0%E3%81%AA%E3%83%87%E3%83%BC%E3%82%BF%20%E3%83%95%E3%82%A3%E3%83%AB%E3%82%BF%E3%83%BC%E5%87%A6%E7%90%86%E3%81%AE%E3%81%9F%E3%82%81%E3%80%81Log%20Analytics%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%8B%E3%82%89%20Azure,Log%20Analytics%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AB%E3%82%88%E3%82%8B%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86%E3%81%AE%E6%A7%8B%E6%88%90%E3%81%AF%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9%E3%81%A7%E8%A1%8C%E3%82%8F%E3%82%8C%E3%82%8B%E3%81%9F%E3%82%81%E3%80%81%E3%81%99%E3%81%B9%E3%81%A6%E3%81%AE%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%8C%E5%90%8C%E3%81%98%E6%A7%8B%E6%88%90%E3%82%92%E5%8F%97%E3%81%91%E5%8F%96%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82%20Azure%20Monitor)。AMAはWindows/Linux両方で**マルチホーム**（複数Workspaceへの送信）も可能で、収集データに対し**変換 (transformation)**で不要データをフィルタする機能も持ちます[[5]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=match%20at%20L127%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%A7%E4%BD%BF%E7%94%A8%E3%81%95%E3%82%8C%E3%82%8B%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86%E3%83%AB%E3%83%BC%E3%83%AB%E3%81%AF%E3%80%81%E3%81%95%E3%81%BE%E3%81%96%E3%81%BE%E3%81%AA%20VM,%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E5%8F%8E%E9%9B%86%E3%81%95%E3%82%8C%E3%82%8B%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E3%83%95%E3%82%A3%E3%83%AB%E3%82%BF%E3%83%BC%E5%87%A6%E7%90%86%E3%81%99%E3%82%8B%E3%81%93%E3%81%A8%E3%82%82%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20%E4%B8%8D%E8%A6%81%E3%81%AA%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%8B%E3%82%89%E5%8F%96%E3%82%8A%E9%99%A4%E3%81%8F%E3%81%9F%E3%82%81%E3%81%AB%E3%83%95%E3%82%A3%E3%83%AB%E3%82%BF%E3%83%BC%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E3%82%84%E5%88%86%E6%9E%90%E3%81%AB%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%AA%E3%81%84%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E3%83%95%E3%82%A3%E3%83%AB%E3%82%BF%E3%83%BC%E5%87%A6%E7%90%86%E3%81%97%E3%81%A6%E3%80%81%E3%83%87%E3%83%BC%E3%82%BF%20%E3%82%A4%E3%83%B3%E3%82%B8%E3%82%A7%E3%82%B9%E3%83%88%20%E3%82%B3%E3%82%B9%E3%83%88%E3%82%92%E5%89%8A%E6%B8%9B%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)。
* **データ収集ルール (DCR)**：Azure Monitor Agentで収集するデータの内容や送信先を定義するAzureリソースです。DCRにより収集するイベントログやパフォーマンスカウンター、カスタムログファイルのパス、送信先Workspaceやテーブル名などを指定します[[6]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Azure%20Monitor%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%8B%E3%82%89%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86%E3%81%AF%E3%80%81Azure%20%E3%82%B5%E3%83%96%E3%82%B9%E3%82%AF%E3%83%AA%E3%83%97%E3%82%B7%E3%83%A7%E3%83%B3%E3%81%AB%E6%A0%BC%E7%B4%8D%E3%81%95%E3%82%8C%E3%80%81%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AB%E9%96%A2%E9%80%A3%E4%BB%98%E3%81%91%E3%82%89%E3%82%8C%E3%81%A6%E3%81%84%E3%82%8B%201,DCR%29%20%E3%81%AB%E3%82%88%E3%81%A3%E3%81%A6%E5%AE%9A%E7%BE%A9%E3%81%95%E3%82%8C%E3%81%BE%E3%81%99%E3%80%82)。1つのVMに複数DCRを適用したり、1つのDCRを複数VMに適用できる柔軟性があり、異なる役割のVMごとに収集設定を変える戦略も可能です[[6]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Azure%20Monitor%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%8B%E3%82%89%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86%E3%81%AF%E3%80%81Azure%20%E3%82%B5%E3%83%96%E3%82%B9%E3%82%AF%E3%83%AA%E3%83%97%E3%82%B7%E3%83%A7%E3%83%B3%E3%81%AB%E6%A0%BC%E7%B4%8D%E3%81%95%E3%82%8C%E3%80%81%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AB%E9%96%A2%E9%80%A3%E4%BB%98%E3%81%91%E3%82%89%E3%82%8C%E3%81%A6%E3%81%84%E3%82%8B%201,DCR%29%20%E3%81%AB%E3%82%88%E3%81%A3%E3%81%A6%E5%AE%9A%E7%BE%A9%E3%81%95%E3%82%8C%E3%81%BE%E3%81%99%E3%80%82)。
* **Log Analytics ワークスペース**：エージェントが送信したログ・メトリックデータが格納されるデータストアです。後述する各種ログ（イベントログ、カスタムログ、パフォーマンスログなど）はWorkspace内のテーブル（例えばPerfテーブルやカスタムログのテーブル）に蓄積され、**Kusto Query Language (KQL)** で分析・検索ができます。

**メモ：VM Insights** – Azure Monitorの**VMインサイト**機能を有効化すると、上記エージェント(AMA)とDCRのデプロイが簡略化できます。VMインサイトは代表的なパフォーマンスカウンター（CPU、メモリ、ディスクなど）やプロセス情報、接続マップ等を収集するプリセットDCRを自動作成し、標準のワークブックやパフォーマンスチャートも提供します[[7]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine#:~:text=,and%20dependencies%20with%20other%20services)。迅速に監視を開始したい場合はVMインサイトの利用も検討できます（後から独自DCRを追加して収集項目を拡張可能）。

## データ収集の設定（エージェントとDCR）

まず、Azure VM上にAzure Monitorエージェント (AMA) をインストールし、収集すべきデータと送信先を定義した**データ収集ルール(DCR)** を作成します。構成のポイントは次のとおりです。

* **Azure Monitor Agentの導入**：監視対象VMにはAzure Monitorエージェントをインストールします。Azure VM上ならAzure PortalからVM拡張機能として簡単に導入可能であり、Azure Policyを使って自動展開することも推奨されます[[8]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=match%20at%20L177%20Azure%20Connected,%E3%81%AE%E3%82%BB%E3%83%83%E3%83%88%E3%81%A8%E3%80%81%E4%BD%9C%E6%88%90%E3%81%95%E3%82%8C%E3%81%9F%E6%96%B0%E3%81%97%E3%81%84%20VM%20%E3%81%AB%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%82%92%E8%87%AA%E5%8B%95%E7%9A%84%E3%81%AB%E3%83%87%E3%83%97%E3%83%AD%E3%82%A4%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20%E3%81%93%E3%82%8C%E3%81%AB%E3%82%88%E3%82%8A%E3%80%81%E7%AE%A1%E7%90%86%E8%80%85%E3%81%AB%E3%82%88%E3%82%8B%E4%BB%8B%E5%85%A5%E3%82%92%E6%9C%80%E5%B0%8F%E9%99%90%E3%81%AB%E6%8A%91%E3%81%88%E3%81%A6%E3%80%81%E3%81%99%E3%81%B9%E3%81%A6%E3%81%AE%20VM)。既存のLog Analyticsエージェント(MMA)を使用している場合はAMAへの移行を検討してください。AMAはデータ収集ルールによる細かな設定とフィルタリングを可能にし、異なるVMグループごとに適切な収集内容を割り当てられます[[4]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E8%A9%B3%E7%B4%B0%E3%81%AA%E3%83%87%E3%83%BC%E3%82%BF%20%E3%83%95%E3%82%A3%E3%83%AB%E3%82%BF%E3%83%BC%E5%87%A6%E7%90%86%E3%81%AE%E3%81%9F%E3%82%81%E3%80%81Log%20Analytics%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%8B%E3%82%89%20Azure,Log%20Analytics%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AB%E3%82%88%E3%82%8B%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86%E3%81%AE%E6%A7%8B%E6%88%90%E3%81%AF%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9%E3%81%A7%E8%A1%8C%E3%82%8F%E3%82%8C%E3%82%8B%E3%81%9F%E3%82%81%E3%80%81%E3%81%99%E3%81%B9%E3%81%A6%E3%81%AE%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%8C%E5%90%8C%E3%81%98%E6%A7%8B%E6%88%90%E3%82%92%E5%8F%97%E3%81%91%E5%8F%96%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82%20Azure%20Monitor)。
* **収集するデータの定義（DCRの内容）**：本シナリオでは「**パフォーマンスメトリック**」「**稼働状況/可用性**」「**システム/アプリケーションログ**」を主に収集します。DCRではこれらを包括的にカバーするよう設定します。
* *プラットフォームメトリック*：Azure VMについてはCPU使用率、ネットワーク送受信量、ディスクIO等の**プラットフォームメトリック**が自動収集されます。これらはAzureポータルのVM概要やメトリックチャートで確認でき、Log Analyticsへ送るには別途診断設定またはMetrics収集のDCRが必要になる場合があります。メモリ使用率など一部メトリックはプラットフォーム標準では収集されないため、次の「ゲストOSパフォーマンス」で補います。
* *ゲストOSのパフォーマンス*：Azure Monitorエージェント経由で**パフォーマンスカウンター**を収集します。代表例は**CPU**（% Processor Time）、**メモリ**（Available MBytes など）、**ディスク**（Disk Queue Length や ディスク使用率）、**ネットワーク**（Bytes sent/received）等です。VMインサイト有効時には主要カウンターが自動収集されLog AnalyticsのInsightsMetricsテーブルやPerfテーブルに送られます[[9]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%E3%83%91%E3%83%95%E3%82%A9%E3%83%BC%E3%83%9E%E3%83%B3%E3%82%B9%20%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AF%E3%80%81%E6%AC%A1%E3%81%AE%E3%83%86%E3%83%BC%E3%83%96%E3%83%AB%E3%81%AB%E9%80%81%E4%BF%A1%E3%81%95%E3%82%8C%E3%81%BE%E3%81%99%E3%80%82%20%E2%80%A2%20VM%20%E5%88%86%E6%9E%90%E6%83%85%E5%A0%B1%3A,%E2%80%A2%20%E3%81%9D%E3%81%AE%E4%BB%96%E3%81%AE%E3%83%91%E3%83%95%E3%82%A9%E3%83%BC%E3%83%9E%E3%83%B3%E3%82%B9%20%E3%83%87%E3%83%BC%E3%82%BF%3A%20%2040)。必要に応じてDCRで追加のカウンター（例えば特定プロセスのCPUやカスタムアプリケーションの独自カウンター）を収集対象に加えることも可能です[[10]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=,%E3%83%A1%E3%83%88%E3%83%AA%E3%83%83%E3%82%AF%20%E3%81%AB%E9%80%81%E4%BF%A1%E3%81%97%E3%80%81%E3%83%A1%E3%83%88%E3%83%AA%E3%83%83%E3%82%AF%20%E3%82%B9%20%E3%82%A8%E3%82%AF%E3%82%B9%E3%83%97%E3%83%AD%E3%83%BC%E3%83%A9%E3%83%BC%E3%81%A8%E3%83%A1%E3%83%88%E3%83%AA%E3%83%83%E3%82%AF%20%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E3%81%A7%E4%BD%BF%E7%94%A8%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82)。パフォーマンスデータはAzure Monitorメトリックにも送信でき、メトリックアラートにも利用できます[[11]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%E5%AE%9B%E5%85%88%20%E8%AA%AC%E6%98%8E%20%E3%83%A1%E3%83%88%E3%83%AA%E3%83%83%E3%82%AF%20%E3%83%9B%E3%82%B9%E3%83%88%20%E3%83%A1%E3%83%88%E3%83%AA%E3%83%83%E3%82%AF%E3%81%AF%E3%80%81Azure,%E3%81%BE%E3%81%9F%E3%81%AF%2038%E3%81%A7%E3%83%AD%E3%82%B0%20%E3%82%AF%E3%82%A8%E3%83%AA%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%80%81%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E3%82%A4%E3%83%99%E3%83%B3%E3%83%88%20%E3%83%87%E3%83%BC%E3%82%BF%E3%81%A8%E5%85%B1%E3%81%AB%E5%88%86%E6%9E%90%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20%E8%A4%87%E6%95%B0%E3%81%AE%E3%83%9E%E3%82%B7%E3%83%B3%E3%80%81%E3%83%AA%E3%83%BC%E3%82%B8%E3%83%A7%E3%83%B3%E3%80%81%E3%82%B5%E3%83%96%E3%82%B9%E3%82%AF%E3%83%AA%E3%83%97%E3%82%B7%E3%83%A7%E3%83%B3%E3%81%AB%E3%81%BE%E3%81%9F%E3%81%8C%E3%82%8B%E8%A4%87%E9%9B%91%E3%81%AA%E3%83%AD%E3%82%B8%E3%83%83%E3%82%AF%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E7%9B%B8%E4%BA%92%E3%81%AB%E9%96%A2%E9%80%A3%E4%BB%98%E3%81%91%E3%82%8B%E3%81%93%E3%81%A8%E3%82%82%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82)。
* *可用性・稼働状況*：VMの稼働状態や監視エージェントの健全性を確認するデータです。Azure Monitorは各VMの**稼働状態**を示す「可用性メトリック（プレビュー）」を提供しており、VMが起動中か停止中かを追跡できます[[12]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E5%8B%A7%E5%91%8A%20%E8%AA%AC%E6%98%8E%20Azure%20VM%20%E7%94%A8%E3%81%AE%E5%8F%AF%E7%94%A8%E6%80%A7%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88,%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AF%E3%80%81%E6%AF%8E%E5%88%86%20Log%20Analytics%20%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9%E3%81%AB%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%E3%82%92%E9%80%81%E4%BF%A1%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AE%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%9F%E3%83%AD%E3%82%B0%E6%A4%9C%E7%B4%A2%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88)。このメトリックはAzure VM (Azure上) に限定されますが、個別VMだけでなくリソースグループやサブスクリプション単位で一括監視するアラートルールを作成することで、新規VMも含め広範囲のVM稼働監視を簡易化できます[[12]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E5%8B%A7%E5%91%8A%20%E8%AA%AC%E6%98%8E%20Azure%20VM%20%E7%94%A8%E3%81%AE%E5%8F%AF%E7%94%A8%E6%80%A7%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88,%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AF%E3%80%81%E6%AF%8E%E5%88%86%20Log%20Analytics%20%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9%E3%81%AB%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%E3%82%92%E9%80%81%E4%BF%A1%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AE%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%9F%E3%83%AD%E3%82%B0%E6%A4%9C%E7%B4%A2%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88)。また、Azure Monitorエージェント自体は**1分ごとにLog Analyticsへハートビート(Heartbeat)** を送信しています。Log AnalyticsのHeartbeatテーブルに記録されるこの信号を監視し、一定期間ハートビートが途絶えた場合に通知することで、「VM自体がダウンしている」または「エージェントが異常停止して監視データが送られていない」状態を検知できます[[13]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AE%E6%AD%A3%E5%B8%B8%E6%80%A7%E3%82%92%E7%A2%BA%E8%AA%8D%E3%81%99%E3%82%8B%E3%81%9F%E3%82%81%E3%81%AE%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%20%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%20%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20Azure,Monitor%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%9F%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AE%E7%9B%A3%E8%A6%96%3A%20%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E3%80%8D%E3%81%AE%E6%83%85%E5%A0%B1%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%80%81%E3%82%AF%E3%83%A9%E3%82%A4%E3%82%A2%E3%83%B3%E3%83%88%20%E3%83%AF%E3%83%BC%E3%82%AF%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AE%E6%BD%9C%E5%9C%A8%E7%9A%84%E3%81%AA%E9%81%8B%E7%94%A8%E4%B8%8A%E3%81%AE%E5%95%8F%E9%A1%8C%E3%82%92%E4%BA%8B%E5%89%8D%E3%81%AB%E9%80%9A%E7%9F%A5%E3%81%99%E3%82%8B%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)。DCR上では特別な設定なしにHeartbeatは送信されますが、後述するアラート設定で活用します。
* *システムイベントログ*：**Windowsイベントログ**（例：Applicationログ、Systemログ）や**Linux Syslog**も重要な監視データです。OSや各種ミドルウェアが出力するエラー/警告イベントをキャッチすることで障害の兆候を検知できます。DCRではWindowsイベントログ（イベントログ名と必要に応じて特定のイベントIDやレベルをフィルタ）やSyslog（施設や重要度によるフィルタ）の収集を設定します。例えばWindowsなら「Application と SystemログのError/Warningレベルを収集」などと定義できます。これによりログはLog AnalyticsのEventテーブル（WindowsEvent）やSyslogテーブルに保存されます。
* *アプリケーションログ（カスタムファイルログ）*：今回のWebアプリケーションはファイルにログを書き出す形式とのことなので、これをLog Analyticsに取り込む設定を行います。Azure Monitor Agentでは**Custom Text Logs**というデータ種別で任意のテキストログファイルを収集可能です[[14]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-log-text#:~:text=Many%20applications%20and%20services%20on,Custom%20Text%20Logs%20data%20source)。DCRの設定において「**カスタム テキスト ログ**」を選び、対象ファイルパス（ワイルドカード指定可）、カスタムログの**テーブル名**、ログレコードの区切り（タイムスタンプ区切りなど）を指定します[[15]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-log-text#:~:text=Setting%20Description%20File%20pattern%20Identifies,above%20the%20file%20name%20only)[[16]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-log-text#:~:text=Table%20name%20Name%20of%20the,described%20in%20%2010%20below)。例えば、C:\Logs\MyApp\\*.log を対象にし、Log Analytics側で MyApp\_CL というカスタムテーブル（事前作成が必要）にデータを送る、といった設定が可能です。ログ内の日付書式を指定して新しいレコードの区切りを認識させることで、複数行にまたがるログエントリにも対応します[[17]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-log-text#:~:text=table%20must%20already%20exist,records%20or%20to%20format%20the)。**注意**として、収集するファイルはローカルディスク上にあり、UTF-8かASCIIで記録され、追記型である必要があります（過去ログを書き換える形式は非対応）[[18]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-log-text#:~:text=The%20file%20that%20Azure%20Monitor,must%20meet%20the%20following%20requirements)。以上の条件を満たせば、任意のアプリケーションログをAzure Monitor経由で収集し分析できます。実際にAzure Monitorでテキストログを収集するには、Log Analytics側に先にカスタムの受信テーブルを用意する必要があります[[19]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-log-text#:~:text=In%20addition%20to%20the%20prerequisites,and%20rocky8%20are%20not%20supported)。DCR作成時に指定したテーブル名（例えばMyApp\_CL）に合わせ、Log Analytics Workspace上でその名前の**カスタムログテーブル**を作成しておきます[[19]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-log-text#:~:text=In%20addition%20to%20the%20prerequisites,and%20rocky8%20are%20not%20supported)。テーブル作成後、DCRを適用するとエージェントが該当ログファイルを監視して新規行をWorkspaceに送信します。
* **データ収集ルールの管理**：環境全体で複数のVMを監視する場合、DCRの構成管理も考慮します。例えばWebサーバーVM用、DBサーバーVM用など役割に応じて別々のDCRを作成し、それぞれに適切なログ・メトリック収集設定を割り当てることができます。DCRはAzureリソースとしてAzure Resource Managerで管理できるため、IaC（ARMテンプレートやTerraform）で配置・更新することも可能です。また、Azure Policyを使えば、新規VM作成時に自動でエージェントと指定DCRを関連付けることができます[[8]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=match%20at%20L177%20Azure%20Connected,%E3%81%AE%E3%82%BB%E3%83%83%E3%83%88%E3%81%A8%E3%80%81%E4%BD%9C%E6%88%90%E3%81%95%E3%82%8C%E3%81%9F%E6%96%B0%E3%81%97%E3%81%84%20VM%20%E3%81%AB%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%82%92%E8%87%AA%E5%8B%95%E7%9A%84%E3%81%AB%E3%83%87%E3%83%97%E3%83%AD%E3%82%A4%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20%E3%81%93%E3%82%8C%E3%81%AB%E3%82%88%E3%82%8A%E3%80%81%E7%AE%A1%E7%90%86%E8%80%85%E3%81%AB%E3%82%88%E3%82%8B%E4%BB%8B%E5%85%A5%E3%82%92%E6%9C%80%E5%B0%8F%E9%99%90%E3%81%AB%E6%8A%91%E3%81%88%E3%81%A6%E3%80%81%E3%81%99%E3%81%B9%E3%81%A6%E3%81%AE%20VM)。監視漏れ防止のため、本番サブスクリプションにはエージェント未導入VMがない状態をポリシーで保証すると良いでしょう。なお、古いLog Analyticsエージェントとは異なり、Azure Monitorエージェント(AMA)ではDCRごとに収集データを**きめ細かく制御**できます。例えば開発環境VMには詳細ログを含むDCR、本番環境VMには必要最小限のDCR、というように用途別にDCRを分けられます。コストは今回は重視しない前提ですが、それでも**不要なデータは収集しない**方がパフォーマンス上も有益です（ログノイズの低減）。AMAではDCR内で**フィルター**や**変換**を適用して不要なログを除外できるため、意図しない膨大なログ（例: トレースレベルの冗長ログなど）の収集は抑制する設計が推奨されます[[20]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%E4%B8%80%E8%88%AC%E7%9A%84%E3%81%AA%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AF%E3%80%81%E6%AF%8E%E6%9C%88%201%20GB%20%E3%81%8B%E3%82%89%203,%E3%83%9C%E3%83%AA%E3%83%A5%E3%83%BC%E3%83%A0%20%E3%81%AE%20%2013%E3%81%BE%E3%81%9F%E3%81%AF%E3%83%AD%E3%82%B0%20%E3%82%AF%E3%82%A8%E3%83%AA%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%80%81%E5%90%84%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AB%E5%AF%BE%E3%81%97%E3%81%A6%E5%8F%8E%E9%9B%86%E3%81%95%E3%82%8C%E3%82%8B%E8%AA%B2%E9%87%91%E5%AF%BE%E8%B1%A1%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AE%E9%87%8F%E3%82%92%E6%B1%BA%E5%AE%9A%E3%81%97%E3%80%81%E3%81%9D%E3%82%8C%E3%81%AB%E5%BF%9C%E3%81%98%E3%81%A6%E8%AA%BF%E6%95%B4%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)[[21]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%A7%E4%BD%BF%E7%94%A8%E3%81%95%E3%82%8C%E3%82%8B%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86%E3%83%AB%E3%83%BC%E3%83%AB%E3%81%AF%E3%80%81%E3%81%95%E3%81%BE%E3%81%96%E3%81%BE%E3%81%AA%20VM%20%E3%82%BB%E3%83%83%E3%83%88%E3%81%AE%E7%89%B9%E5%AE%9A%E3%81%AE%E7%9B%A3%E8%A6%96%E8%A6%81%E4%BB%B6%E3%81%AB%E5%90%88%E3%82%8F%E3%81%9B%E3%81%A6%E8%AA%BF%E6%95%B4%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20Azure%20Monitor,%E3%82%B3%E3%82%B9%E3%83%88%E3%82%92%E5%89%8A%E6%B8%9B%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20%E3%81%95%E3%81%BE%E3%81%96%E3%81%BE%E3%81%AA%E7%9B%A3%E8%A6%96%E3%82%B7%E3%83%8A%E3%83%AA%E3%82%AA%E3%81%A7%E5%8F%8E%E9%9B%86%E3%81%99%E3%82%8B%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E3%82%AC%E3%82%A4%E3%83%80%E3%83%B3%E3%82%B9%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6%E3%81%AF%E3%80%81%E3%80%8C%20Azure%20Monitor%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%9F%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AE%E7%9B%A3%E8%A6%96)。

## 主要なメトリックの監視方法（パフォーマンス監視）

VMおよびWebアプリのパフォーマンス指標として代表的な**メトリック**には以下があります。

* **CPU使用率**：プロセッサの使用率。高負荷時にボトルネックとなりやすいため、平均値や最大値を監視します（例：閾値80%超の継続時間など）。
* **メモリ使用量**：物理メモリの消費。使用率が極端に高いとスワップやメモリ不足によるアプリケーションエラーを招くため、残容量や使用率を追跡します。
* **ディスクIOとストレージ**：ディスクの読み書き待ち時間（キュー長）やIOPS、使用容量など。ディスクキュー長が長時間増大している場合はディスクボトルネックが疑われます。またディスク容量逼迫も監視が必要です。
* **ネットワーク**：ネットワークの送受信バイトやパケット、接続エラー数など。Webアプリの場合は帯域使用量や接続数も可用性に影響するため把握します。

上記メトリックはAzure PortalのVMインサイト画面やメトリックチャートでも確認できますが、Log Analyticsで高度な分析やカスタムアラートを作成することもできます。例えば以下のような**KQLクエリ**でパフォーマンスデータを分析可能です（Log AnalyticsのPerfテーブルに格納された値を集計）。

* 各VMの平均CPU使用率を取得するクエリ:
* Perf  
  | where ObjectName == "Processor" and CounterName == "% Processor Time" and InstanceName == "\_Total"  
  | summarize AvgCPU = avg(CounterValue) by Computer
* *説明*: 全VMについて、CPU使用率 (% Processor Time カウンター) の平均値を算出します。結果は各Computer（VM名）ごとの平均CPU使用率(AvgCPU)です[[22]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%60Perf%20%5C,%5C%7C%20summarize%20AggregatedValue)。CPU使用率が特に高いVMをピックアップし、スケーリングや性能改善の検討材料にできます。
* 各VMの最大CPU使用率を取得するクエリ:
* Perf  
  | where CounterName == "% Processor Time" and InstanceName == "\_Total"  
  | summarize MaxCPU = max(CounterValue) by Computer
* *説明*: % Processor Time の最大値をVMごとに求めます。ピーク時負荷の把握に有用です[[22]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%60Perf%20%5C,%5C%7C%20summarize%20AggregatedValue)。平均値と併せて見ることで、スパイク的な負荷か継続的な高負荷かを判断できます。
* 特定VM上のCPU使用率の時間推移（1時間単位平均）:
* Perf  
  | where Computer == "MyServer1" and CounterName == "% Processor Time" and InstanceName == "\_Total"  
  | summarize AvgCPU=avg(CounterValue) by bin(TimeGenerated, 1h)
* *説明*: VMMyServer1のCPU使用率を1時間ごとの平均に集計し、時系列で出力します[[23]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%60Perf%20%5C,)。これを折れ線グラフ化すれば日内パターンやピーク時間帯を視覚化できます。
* ディスクキュー長の95パーセンタイル（VM別）:
* Perf  
  | where CounterName == "Current Disk Queue Length"  
  | summarize P95\_Queue = percentile(CounterValue, 95) by Computer
* *説明*: 各VMについてディスクの「現在のキュー長」の95%値を算出し、通常時の上限挙動を把握します[[24]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%60Perf%20%5C,1%20%E6%99%82%E9%96%93%E3%81%94%E3%81%A8)。P95が高いVMはディスクIO待ちが発生しやすいため要注意です。
* メモリ残量が少ないホストの検出（例）:  
  Windowsの場合、Memory オブジェクトの Available MBytes カウンターで空きメモリ容量が取得できます。同様にクエリで集計・フィルタして閾値以下のVMを列挙できます（LinuxならAvailable Memoryカウンター等）。

**Tips:** パフォーマンスデータは**Metricsアラート**でも閾値監視できます。例えばAzure Monitorメトリックアラートを用い、あるVMのCPUが5分間平均80%を超えたらアラート、といったルールを設定可能です。静的閾値の決定が難しい場合、**動的しきい値**（Azure Monitorによる機械学習ベースのベースライン自動算出）を使用することもできます[[25]](https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/best-practices-alerts#:~:text=,with%20a%20variety%20of%20systems)。これにより通常と逸脱した振る舞いを検知しやすくなります。メトリックアラートはリアルタイム性に優れますが、対象リソース数が多い場合コスト増となる点には注意が必要です[[26]](https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/best-practices-alerts#:~:text=configuring%20log%20search%20alerts%2C%20keep,a%20large%20number%20of%20resources)（本シナリオではコスト優先度は低いですが、大規模環境ではログアラートとの併用でコスト調整が推奨されます[[27]](https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/best-practices-alerts#:~:text=Recommendation%20Benefit%20Keep%20in%20mind,Some)）。

## 可用性と健全性の監視（VMおよびアプリケーション）

**可用性 (Availability)** の監視とは、VMおよびその上のWebアプリケーションがユーザーからアクセス可能な状態を維持しているかをチェックすることです。本シナリオでは、以下の多層的なアプローチで可用性を監視する構成がベストプラクティスです。

* **仮想マシンの稼働監視**：前述の通り、Azure Monitorの**可用性メトリック**（VM稼働状態）を活用した監視が可能です[[12]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E5%8B%A7%E5%91%8A%20%E8%AA%AC%E6%98%8E%20Azure%20VM%20%E7%94%A8%E3%81%AE%E5%8F%AF%E7%94%A8%E6%80%A7%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88,%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AF%E3%80%81%E6%AF%8E%E5%88%86%20Log%20Analytics%20%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9%E3%81%AB%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%E3%82%92%E9%80%81%E4%BF%A1%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AE%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%9F%E3%83%AD%E3%82%B0%E6%A4%9C%E7%B4%A2%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88)。このメトリックに対するアラートルールを設定し、VMが停止状態になった場合に即座に通知を受けるようにします。例えば、スコープをサブスクリプション全体にした可用性メトリックのアラートルールを1つ作成すれば、そのリージョン内の全VMについて停止検知のアラートを網羅できます[[12]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E5%8B%A7%E5%91%8A%20%E8%AA%AC%E6%98%8E%20Azure%20VM%20%E7%94%A8%E3%81%AE%E5%8F%AF%E7%94%A8%E6%80%A7%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88,%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AF%E3%80%81%E6%AF%8E%E5%88%86%20Log%20Analytics%20%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9%E3%81%AB%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%E3%82%92%E9%80%81%E4%BF%A1%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AE%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%9F%E3%83%AD%E3%82%B0%E6%A4%9C%E7%B4%A2%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88)。新規VMも自動的に監視対象となるため運用負荷が軽減します。
* **エージェントのハートビート監視**：Azure Monitorエージェント(AMA)はLog Analyticsに**1分ごとにハートビート**を送っています。このHeartBeatが一定時間受信できない場合、VMがダウンしているかエージェント障害が発生していることを意味します[[13]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AE%E6%AD%A3%E5%B8%B8%E6%80%A7%E3%82%92%E7%A2%BA%E8%AA%8D%E3%81%99%E3%82%8B%E3%81%9F%E3%82%81%E3%81%AE%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%20%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%20%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20Azure,Monitor%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%9F%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AE%E7%9B%A3%E8%A6%96%3A%20%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E3%80%8D%E3%81%AE%E6%83%85%E5%A0%B1%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%80%81%E3%82%AF%E3%83%A9%E3%82%A4%E3%82%A2%E3%83%B3%E3%83%88%20%E3%83%AF%E3%83%BC%E3%82%AF%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AE%E6%BD%9C%E5%9C%A8%E7%9A%84%E3%81%AA%E9%81%8B%E7%94%A8%E4%B8%8A%E3%81%AE%E5%95%8F%E9%A1%8C%E3%82%92%E4%BA%8B%E5%89%8D%E3%81%AB%E9%80%9A%E7%9F%A5%E3%81%99%E3%82%8B%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)。Log AnalyticsのHeartbeatテーブルに対するログ検索アラートを設定し、例えば「直近5分間に指定VMからHeartbeatがない場合」にアラート発報するルールを作ります[[13]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AE%E6%AD%A3%E5%B8%B8%E6%80%A7%E3%82%92%E7%A2%BA%E8%AA%8D%E3%81%99%E3%82%8B%E3%81%9F%E3%82%81%E3%81%AE%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%20%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%20%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20Azure,Monitor%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%9F%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AE%E7%9B%A3%E8%A6%96%3A%20%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E3%80%8D%E3%81%AE%E6%83%85%E5%A0%B1%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%80%81%E3%82%AF%E3%83%A9%E3%82%A4%E3%82%A2%E3%83%B3%E3%83%88%20%E3%83%AF%E3%83%BC%E3%82%AF%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AE%E6%BD%9C%E5%9C%A8%E7%9A%84%E3%81%AA%E9%81%8B%E7%94%A8%E4%B8%8A%E3%81%AE%E5%95%8F%E9%A1%8C%E3%82%92%E4%BA%8B%E5%89%8D%E3%81%AB%E9%80%9A%E7%9F%A5%E3%81%99%E3%82%8B%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)。これにより、Azure以外の環境（オンプレや他クラウド）のVMであっても、エージェント経由で疎通監視が可能です（Azure外VMでは可用性メトリックは使えないためHeartbeat監視が有効）[[28]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E3%81%8C%E8%87%AA%E5%8B%95%E7%9A%84%E3%81%AB%E7%9B%A3%E8%A6%96%E3%81%95%E3%82%8C%E3%82%8B%E3%82%88%E3%81%86%E3%81%AB%E3%81%AA%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82%20%E3%81%93%E3%81%AE%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%81%A7%E3%81%AF%E3%80%81Azure%20Monitor%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%82%92,%E3%82%A4%E3%83%99%E3%83%B3%E3%83%88%E5%8F%8E%E9%9B%86%E3%82%92%E6%A7%8B%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20%E3%80%8C%208%20Azure%20Monitor)。HeartBeatアラートはVM停止だけでなくエージェント不調も検知できるため、監視の盲点を減らせます。
* **Webアプリケーションの外形監視**：VM自体が動作していても、Webサーバーやアプリケーションが応答しない状態になっていれば可用性に問題があります。そこで、**アプリケーションのエンドポイント監視**も導入します。方法の一つは、**Azure Application Insightsの可用性テスト**（URL Pingテスト）を利用することです。Application Insightsリソースを作成しWebアプリのURLに対するPingテストを設定すると、1分ごと等の頻度でHTTPエンドポイントの応答をチェックし、失敗時にアラートを上げることができます。この仕組みを用いれば外部から見たWebアプリの可用性（HTTP 200が返るか、応答時間は正常か等）を継続監視できます。外部の監視サービス（M&EaaS）が既に同様のチェックを行う場合はそちらに任せても良いですが、Azure側でも重要エンドポイントの監視を二重化しておくと確実です。

加えて、Azure Monitorには**接続モニター (Connection Monitor)** と呼ばれるNetwork Watcherの機能もあります。これは指定した送信元からVM上の特定ポートへの通信を定期的に試行し、成功可否やレイテンシを監視するものです[[29]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Connection%20Manager)。例えば、「社内拠点Aから当該WebサーバーVMのポート443へTCP接続できるか」を定期チェックできます。Webアプリが単純なPingに応答しなくても、特定ポートのリッスン状態を監視することでサービスダウンを検知可能です[[30]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Port%20monitoring%20verifies%20that%20a,port%20monitoring%20are%20described%20here)。もっとも、通常のWebアプリであれば可用性テスト(URL監視)の方がアプリケーションレイヤまで含めた監視となるため有用です。

* **サービスプロセス監視**：これはオプションですが、VM上で動作する特定のWindowsサービスやLinuxデーモンが停止していないかをチェックすることも信頼性向上につながります。Azure MonitorではAzure Automationの**Change Tracking & Inventory**ソリューションを有効にすることでサービスの状態変化をログとして取得できます[[31]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Monitor%20a%20service%20or%20daemon)。例えば「WWW Publishingサービス (W3SVC)」の状態変化をLog Analyticsで追跡し、停止状態が検出されたら通知するといった応用も可能です[[31]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Monitor%20a%20service%20or%20daemon)。

以上の多層的な監視により、VMそのものからアプリケーションまで可用性の穴を埋めることができます。可用性に重大な変化（例えばWebサイトがダウン）に対して即座に検知・通報し、早期復旧措置を講じられるようになります。

## ログ監視の設定（イベント & アプリケーションログ）

次に、**ログデータ**の監視についてです。Azure VM上のOSやミドルウェア、そしてWebアプリ自身が出力するログを収集・分析することで、エラーの発生やシステムの挙動を詳細に把握できます。

### システムイベントログの監視（Windows Event / Linux Syslog）

**Windowsイベントログ**（アプリケーション、システム、セキュリティなど）や**LinuxのSyslog**は、システムやソフトウェアの状態を示す基本的なログ情報です。Azure Monitorエージェントのデータ収集ルール(DCR)でWindowsイベントログやSyslogを指定しておけば、OSやアプリのエラー・警告イベントをLog Analyticsに蓄積できます。例えば、DCRで「WindowsのApplicationとSystemログの全イベント」を収集対象にすると、ログはLog AnalyticsのEventテーブルに記録されます。またLinuxの場合、「Syslogの全Facilityを収集」や「特定のSeverity以上のみ収集」等をDCRで設定可能で、SyslogはSyslogテーブルに格納されます。

これらのログはKQLで自由に検索・分析できます。いくつか例を示します。

* **Windowsイベントログからエラーイベントのみを抽出**:
* Event  
  | where EventLevelName == "Error"  
  | summarize Count = count() by Source
* *説明*: WindowsイベントログEventテーブルから、レベルが"Error"のものだけを集計し、イベントソース別の件数を数えています[[32]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=error%20%60Event%20%5C,Windows%20error%20events%20by%20source)。この結果により、どのソース（アプリケーションやサービス）でエラーが多発しているかが分かります。
* **Syslogのエラー件数をホスト別に集計**:
* Syslog  
  | where SeverityLevel == "err" // or Severity == "error"  
  | summarize ErrorCount = count() by Computer
* *説明*: SyslogテーブルからSeverityがエラーのログを抽出し、ホスト（VM）ごとの件数を集計します[[33]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Sample%20log%20queries%3A%20Syslog%20events)。多数のエラーが出ているVMを発見できます。

ログ監視では、このように**特定のエラーイベントの有無**をトリガーにアラートを上げる設定も有効です。例えば上記Windowsイベントログのクエリを用い、「特定のSourceでエラーイベントが発生した場合に即時通知」というログアラートルールを作ることができます。Azure Monitorのログ検索アラートは一定間隔でKQLクエリを実行し、結果が閾値条件に一致したときに発報します。イベントログであれば「count() > 0」で何かエラーが出たら即アラート、のように設定できます。

### アプリケーションログ（ファイルログ）の監視と分析

本システムではWebアプリがファイルに出力する**アプリケーションログ**をAzure Monitor経由で集約します。前述の通り、Azure Monitor AgentのDCRで**カスタムテキストログ**収集を設定することで、特定パスのログファイルをLog Analyticsに送信できます[[14]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-log-text#:~:text=Many%20applications%20and%20services%20on,Custom%20Text%20Logs%20data%20source)。設定後、アプリケーションログはLog Analytics上の**カスタムログテーブル**（例：MyApp\_CL）に蓄積されます。

ログが取り込まれたら、その分析にはLog Analyticsの強力なクエリエンジンを活用します。アプリケーションの動作ログからエラーや警告を検出し、頻度や内容を把握しましょう。例えば、アプリログMyApp\_CLテーブルに以下のようなフィールドがあると仮定します: 時刻、ログレベル(statusフィールド: "Info"/"Error"など)、エラーコード(codeフィールド)、メッセージ 等。KQLの例を示します。

* **アプリログ中のイベントをコード別に件数集計**:
* MyApp\_CL  
  | summarize Count = count() by code
* *説明*: カスタムログMyApp\_CLテーブル内の全レコードを対象に、codeフィールドの値ごとに件数を集計しています[[34]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%E3%82%AF%E3%82%A8%E3%83%AA%20%E8%AA%AC%E6%98%8E%20%60MyApp_CL%20%5C,%E3%82%A8%E3%83%A9%E3%83%BC%20%E3%82%A4%E3%83%99%E3%83%B3%E3%83%88%E3%81%AB%E5%AF%BE%E3%81%99%E3%82%8B%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)。これにより、どのエラーコードやイベント種別が多発しているか分かります。例えばコード500のエラーが突出して多ければ、HTTP 500エラーが頻発していることを示唆します。
* **アプリログのErrorレベル発生を監視**:
* MyApp\_CL  
  | where status == "Error"  
  | summarize ErrorCount = count() by bin(TimeGenerated, 15m)
* *説明*: 過去15分単位でstatusが"Error"のログ件数を集計しています[[34]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%E3%82%AF%E3%82%A8%E3%83%AA%20%E8%AA%AC%E6%98%8E%20%60MyApp_CL%20%5C,%E3%82%A8%E3%83%A9%E3%83%BC%20%E3%82%A4%E3%83%99%E3%83%B3%E3%83%88%E3%81%AB%E5%AF%BE%E3%81%99%E3%82%8B%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)。このクエリ結果をアラートルールに用い、ErrorCount > 0でアラート発報とすれば、「直近15分でエラーが1件でも発生したら通知」といった設定が可能です。実運用では、単発エラーで即通知がノイズになる場合はErrorCountが一定以上など条件を調整するとよいでしょう。
* **複合条件のログクエリ例**:  
  KQLはログフィールド間の相関や結合も可能です。例えば「特定のユーザーIDに関するエラーイベントのみ抽出」といったクエリも1行で書けます（適宜where句を追加）。また複数テーブルの結合により、アプリログのエラー発生時刻前後にシステムイベントログに何か記録がないか、といったクロス分析もできます。

アプリケーションログについても、重要なエラーメッセージや特定パターンを検知したら即アラートを上げるようにすると、障害対応の初動を迅速化できます。例えば「致命的エラーを表す例外ログが出力されたらアラート通知し、自動でAzure Functionsをキックしてサービスを再起動する」等、自動化を組み合わせた高度な運用も可能です。

**参考**: IISなどWebサーバーが出力するアクセスログもLog Analyticsに収集できます。Azure Monitor AgentにはIISログ収集の組み込み設定があり、有効化するとIISのW3Cログが自動でW3CIISLogテーブルに送信されます[[35]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Collect%20IIS%20logs)。IISログを分析すれば、リクエスト数や応答コードの内訳、特定URLへのアクセス状況などWebトラフィックの詳細を掴めます。例えば以下のクエリで特定サイト(csHost)へのアクセス数をURLパス別に集計できます[[36]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Sample%20log%20queries):

W3CIISLog   
| where csHost == "www.contoso.com"   
| summarize count() by csUriStem

Webアプリのパフォーマンスや利用状況を把握する上でもアクセスログは貴重な情報源です。コスト度外視で精度重視ならば、アプリケーションログだけでなくアクセスログも含め収集・分析すると良いでしょう。

## アラートの設計と通知（Azure Monitor アラート設定）

収集したメトリックやログに対して、**Azure Monitor アラート**を適切に設定することで、重大な状況が発生した際に自動通知・エスカレーションが可能になります。ここではアラートルールの設計指針と、通知のためのアクショングループ設定・外部サービス連携についてまとめます。

### アラートルールの設計ポイント

監視すべき事象ごとにアラートルールを用意します。先述の内容と重複しますが、典型的なアラート例を整理すると以下のようになります。

* **インフラ性能系**:
* *CPU高負荷*: CPU使用率が一定閾値を超過（例: 5分平均 > 80%）が継続。
* *メモリ逼迫*: 可用メモリがしきい値未満（例: 空きが500MB未満）になった。
* *ディスク容量不足*: ディスクドライブの空き容量が残りわずか（例: 使用率90%以上）。
* *ディスクIO異常*: ディスクキュー長やIO待ち時間が長時間高止まり。
* *ネットワーク*: ネットワークのパケットエラーが発生/増加、あるいは帯域使用率が極端に高い。
* **可用性・稼働系**:
* *VMダウン*: VMが予期せず停止した、またはAzureホスト障害で応答不能。
* *エージェント死活*: ハートビートが途絶（例: 5分以上HeartBeatなし）。
* *サービスダウン*: WebサービスのポートがLISTENしていない、特定プロセスが終了した。
* *アプリ無応答*: 外形監視のURLチェックがタイムアウト/失敗（HTTP 5xxや応答なし）。
* **アプリ・ログ系**:
* *アプリケーションエラー*: アプリのエラーログが出力された（特定の重大エラー発生）。
* *頻発する例外*: 一定期間にエラーイベントが大量発生（例: 15分にエラー50件以上）。
* *その他異常イベント*: OSイベントログでサービスクラッシュ（イベントID特定）を検知、ログイン失敗の連続検知（セキュリティ監視にも関与）等。

各アラートルールでは、**シグナルの種類**（メトリック or ログ）に応じた設定を行います。CPUやメモリなど**メトリックアラート**はリアルタイム性が高く、しきい値や動的しきい値を設定可能です。一方、複合条件やログ内容に基づく**ログ検索アラート**はKQLで柔軟な検出ロジックを記述できます[[37]](https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/best-practices-alerts#:~:text=Keep%20in%20mind%20that%20activity,mind%20that%20the%20rule%20can)。ログ検索アラートは通常1～5分おきにクエリを評価し、結果が閾値を満たせば発報します。

アラートルール設計時のベストプラクティスとして、**複数リソースを1ルールでカバー**できる場合はそうすることが推奨されます[[25]](https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/best-practices-alerts#:~:text=,with%20a%20variety%20of%20systems)。例えば前述の「VM可用性メトリック」のように、1つのルールでリソースグループ内すべてのVMの停止を検知できる場合、VMごとに個別ルールを作るより管理が容易です[[12]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E5%8B%A7%E5%91%8A%20%E8%AA%AC%E6%98%8E%20Azure%20VM%20%E7%94%A8%E3%81%AE%E5%8F%AF%E7%94%A8%E6%80%A7%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88,%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AF%E3%80%81%E6%AF%8E%E5%88%86%20Log%20Analytics%20%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9%E3%81%AB%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%E3%82%92%E9%80%81%E4%BF%A1%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AE%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%9F%E3%83%AD%E3%82%B0%E6%A4%9C%E7%B4%A2%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88)。ただし、あまりに大量のリソースを1つにまとめすぎると通知が頻発しすぎたり、1リソースの障害で全体がノイジーになる可能性もあるので、関連性・スコープを考慮してまとめます。また、**アラート抑制**や**スマート検出**機能（動的しきい値）が利用できる場合は活用し、重要な通知に集中できるよう調整します。

**FYI:** アラートルール評価頻度も調整可能ですが、ログ検索アラートは頻度を上げるとコスト増になります[[38]](https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/best-practices-alerts#:~:text=health%20alerts%20are%20free%20of,mind%20that%20the%20rule%20can)（5分間隔より1分間隔の方が評価回数が5倍に）。本ケースでは精度重視のため、必要に応じ1分評価も辞さない方針とします。ただ、全てのログアラートを高頻度にすると負荷も上がるため、**アラート処理ルール**で一括抑制や時間帯制御を行う設計も有効です。例えば深夜帯の一部アラートはサイレントにする、同一事象の重複通知をまとめる等、Azure Monitorの**アラート処理ルール**機能で調整できます。

### 通知と外部サービス連携（アクショングループ設定）

アラートルールが**発報 (Fired)** すると、対応する**アクショングループ**に定義された通知やアクションが実行されます。アクショングループはメールやSMS、Push通知、**Webhook/Function**、ITSMツール連携など様々な通知先をまとめて指定できるエンティティです[[3]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/best-practices-alerts#:~:text=match%20at%20L173%20%E3%82%B0%E3%83%AB%E3%83%BC%E3%83%97%E3%81%8C%E4%BD%BF%E7%94%A8%E3%81%95%E3%82%8C%E3%82%8B%E5%A0%B4%E5%90%88%E3%81%AF%E3%80%81%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E9%80%9A%E7%9F%A5%E3%83%9A%E3%82%A4%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AB%E5%90%AB%E3%82%81%E3%82%8B%E7%8B%AC%E8%87%AA%E3%81%AE%E3%83%97%E3%83%AD%E3%83%91%E3%83%86%E3%82%A3%E3%82%92%E8%BF%BD%E5%8A%A0%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20%E3%81%93%E3%82%8C%E3%82%89%E3%81%AE%E3%83%97%E3%83%AD%E3%83%91%E3%83%86%E3%82%A3%E3%81%AF%E3%80%81Webhook%E3%80%81Azure,Apps%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%99%E3%82%8B%E3%81%A8%E3%80%81%E7%B5%B1%E5%90%88%E3%81%AE%E3%81%9F%E3%82%81%E3%81%AB%E3%83%AF%E3%83%BC%E3%82%AF%E3%83%95%E3%83%AD%E3%83%BC%E3%82%92%E3%83%93%E3%83%AB%E3%83%89%E3%81%8A%E3%82%88%E3%81%B3%E3%82%AB%E3%82%B9%E3%82%BF%E3%83%9E%E3%82%A4%E3%82%BA%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20Logic%20Apps%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E9%80%9A%E7%9F%A5%E3%82%92%E3%82%AB%E3%82%B9%E3%82%BF%E3%83%9E%E3%82%A4%E3%82%BA%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)。本シナリオでは、外部の監視サービス（M&Eaas）への通知が要件にあるため、**WebhookあるいはAzure Functions**を用いた連携を実装します。以下、そのベストプラクティスと設定例です。

* **アクショングループの基本設定**: Azure PortalまたはCLIからアクショングループを作成します。名前と短縮名を決め、少なくとも1つのアクション（通知方法）を登録します。メール/SMS/音声通話等は個人宛の通知に便利ですが、組織の監視システム連携には**Webhook**か**Azure Function**が適しています[[3]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/best-practices-alerts#:~:text=match%20at%20L173%20%E3%82%B0%E3%83%AB%E3%83%BC%E3%83%97%E3%81%8C%E4%BD%BF%E7%94%A8%E3%81%95%E3%82%8C%E3%82%8B%E5%A0%B4%E5%90%88%E3%81%AF%E3%80%81%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E9%80%9A%E7%9F%A5%E3%83%9A%E3%82%A4%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AB%E5%90%AB%E3%82%81%E3%82%8B%E7%8B%AC%E8%87%AA%E3%81%AE%E3%83%97%E3%83%AD%E3%83%91%E3%83%86%E3%82%A3%E3%82%92%E8%BF%BD%E5%8A%A0%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20%E3%81%93%E3%82%8C%E3%82%89%E3%81%AE%E3%83%97%E3%83%AD%E3%83%91%E3%83%86%E3%82%A3%E3%81%AF%E3%80%81Webhook%E3%80%81Azure,Apps%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%99%E3%82%8B%E3%81%A8%E3%80%81%E7%B5%B1%E5%90%88%E3%81%AE%E3%81%9F%E3%82%81%E3%81%AB%E3%83%AF%E3%83%BC%E3%82%AF%E3%83%95%E3%83%AD%E3%83%BC%E3%82%92%E3%83%93%E3%83%AB%E3%83%89%E3%81%8A%E3%82%88%E3%81%B3%E3%82%AB%E3%82%B9%E3%82%BF%E3%83%9E%E3%82%A4%E3%82%BA%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20Logic%20Apps%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E9%80%9A%E7%9F%A5%E3%82%92%E3%82%AB%E3%82%B9%E3%82%BF%E3%83%9E%E3%82%A4%E3%82%BA%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)。Webhookでは汎用的なHTTP POSTを行えるため、任意の外部エンドポイントにアラート情報を送信可能です。一方Azure Functionはカスタム処理を実行できるため、Webhook受信の一種としてAzure側で中継・変換ロジックを挟む場合に有用です。
* **Webhookによる直接連携**: 外部監視サービス（例えばITSMツールやチャットOpsツール）がWebhookエンドポイントを提供している場合、アクショングループのWebhookアクションにそのURLを設定します。Azure Monitorからはアラートごとに1回、HTTP POSTリクエストが送信されます[[39]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/alerts-log-webhook#:~:text=%E3%83%AD%E3%82%B0%E6%A4%9C%E7%B4%A2%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%81%A7%20Webhook%20%E3%82%A2%E3%82%AF%E3%82%B7%E3%83%A7%E3%83%B3%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%80%811%20%E3%81%A4%E3%81%AE,%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%99%E3%82%8B%E3%82%88%E3%81%86%E3%81%AB%E3%82%A2%E3%82%AF%E3%82%B7%E3%83%A7%E3%83%B3%20%E3%82%B0%E3%83%AB%E3%83%BC%E3%83%97%E3%82%92%E6%A7%8B%E6%88%90%20%E5%A0%B4%E5%90%88%E3%81%AB%E4%BD%BF%E7%94%A8%E3%81%A7%E3%81%8D%E3%82%8B%E3%83%97%E3%83%AD%E3%83%91%E3%83%86%E3%82%A3%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6%E8%AA%AC%E6%98%8E%E3%80%82%20%E5%91%BC%E3%81%B3%E5%87%BA%E3%81%95%E3%82%8C%E3%82%8B%E3%82%B5%E3%83%BC%E3%83%93%E3%82%B9%E3%81%AF%E3%80%81Webhook%20%E3%82%92%E3%82%B5%E3%83%9D%E3%83%BC%E3%83%88%E3%81%97%E3%80%81%E5%8F%97%E4%BF%A1%E3%81%97%E3%81%9F%E3%83%9A%E3%82%A4%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AE%E4%BD%BF%E7%94%A8%E6%96%B9%E6%B3%95%E3%82%92%E6%8A%8A%E6%8F%A1%E3%81%97%E3%81%A6%E3%81%84%E3%82%8B%E5%BF%85%E8%A6%81%E3%81%8C%E3%81%82%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82)。この際、**共通アラートスキーマ**（Azure Monitorアラートの標準JSON形式）の利用が推奨されています[[40]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/alerts-log-webhook#:~:text=%E3%82%92%E3%82%B5%E3%83%9D%E3%83%BC%E3%83%88%E3%81%97%E3%80%81%E5%8F%97%E4%BF%A1%E3%81%97%E3%81%9F%E3%83%9A%E3%82%A4%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AE%E4%BD%BF%E7%94%A8%E6%96%B9%E6%B3%95%E3%82%92%E6%8A%8A%E6%8F%A1%E3%81%97%E3%81%A6%E3%81%84%E3%82%8B%E5%BF%85%E8%A6%81%E3%81%8C%E3%81%82%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82)。共通スキーマを有効にすると、メトリックアラート・ログアラート等すべての種類で統一されたフィールド構造のJSONが送られてくるため、受け手側でのパースが簡単になります[[40]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/alerts-log-webhook#:~:text=%E3%82%92%E3%82%B5%E3%83%9D%E3%83%BC%E3%83%88%E3%81%97%E3%80%81%E5%8F%97%E4%BF%A1%E3%81%97%E3%81%9F%E3%83%9A%E3%82%A4%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AE%E4%BD%BF%E7%94%A8%E6%96%B9%E6%B3%95%E3%82%92%E6%8A%8A%E6%8F%A1%E3%81%97%E3%81%A6%E3%81%84%E3%82%8B%E5%BF%85%E8%A6%81%E3%81%8C%E3%81%82%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82)。Webサービス側でこのJSONを受信・解析し、必要な情報（アラート名、深刻度、発生リソース、アラート本文など）を取り出して適切に処理します。

Webhookの設定URLには、必要に応じて認証用のキーやトークンをパラメータとして含めます。しかしURLに秘密情報を含める方式は漏洩リスクがあるため、Azure Monitorでは**Secure Webhook**という認証付きの呼び出しもサポートしています[[41]](https://ayuina.github.io/ainaba-csa-blog/azure-functions-secure-webhook/#:~:text=%E3%81%93%E3%82%8C%E3%81%8C%20%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%81%A7%E4%BF%9D%E8%AD%B7%E3%81%95%E3%82%8C%E3%81%9F%20Webhook%20,AD%20%E8%AA%8D%E8%A8%BC%E3%81%A7%E4%BF%9D%E8%AD%B7%E3%81%95%E3%82%8C%E3%81%9F%20Azure%20Functions%20%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%A6%E3%80%81%E3%82%A2%E3%82%AF%E3%82%B7%E3%83%A7%E3%83%B3%E3%82%B0%E3%83%AB%E3%83%BC%E3%83%97%E3%81%8B%E3%82%89%E5%91%BC%E3%81%B3%E5%87%BA%E3%81%9B%E3%82%8B%E3%81%8B%E8%A9%A6%E3%81%97%E3%81%A6%E3%81%BF%E3%81%BE%E3%81%97%E3%81%9F%E3%80%82)[[42]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/best-practices-alerts#:~:text=)。Secure WebhookではAzure AD認証を用いて、例えばAzure Function側をApp Service認証で保護し、アクショングループからはマネージドIDでトークン取得して呼び出す、といった構成が可能です[[41]](https://ayuina.github.io/ainaba-csa-blog/azure-functions-secure-webhook/#:~:text=%E3%81%93%E3%82%8C%E3%81%8C%20%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%81%A7%E4%BF%9D%E8%AD%B7%E3%81%95%E3%82%8C%E3%81%9F%20Webhook%20,AD%20%E8%AA%8D%E8%A8%BC%E3%81%A7%E4%BF%9D%E8%AD%B7%E3%81%95%E3%82%8C%E3%81%9F%20Azure%20Functions%20%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%A6%E3%80%81%E3%82%A2%E3%82%AF%E3%82%B7%E3%83%A7%E3%83%B3%E3%82%B0%E3%83%AB%E3%83%BC%E3%83%97%E3%81%8B%E3%82%89%E5%91%BC%E3%81%B3%E5%87%BA%E3%81%9B%E3%82%8B%E3%81%8B%E8%A9%A6%E3%81%97%E3%81%A6%E3%81%BF%E3%81%BE%E3%81%97%E3%81%9F%E3%80%82)。これは高度な構成になりますが、セキュリティ重視の場合は選択肢に入ります。Microsoftも**「Webhookアクションを使う場合は可能な限りSecure Webhookを利用して認証を強化する」**ことをベストプラクティスとして挙げています[[43]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/best-practices-alerts#:~:text=)。

* **Azure Functionsを用いた連携**: Azure Functionをアラート通知受信に使う方法は、実質的にはWebhookの一種ですが、Azure上でコードを動かせる点が利点です。たとえば「Azure Monitorアラートを受け取り、ペイロードを解析して外部サービスのAPI形式に整形し直し、そのAPIを呼び出す」というブリッジ処理をFunctionで実装できます。手順としては、まずHTTP TriggerのFunctionを作成し、認証レベルをAnonymousまたはFunctionキーに設定してWebhookとして呼び出せるようにします[[44]](https://ayuina.github.io/ainaba-csa-blog/azure-functions-secure-webhook/#:~:text=Azure%20AD%20%E8%AA%8D%E8%A8%BC%E3%81%99%E3%82%8B%20Azure%20Functions,App%20%E3%82%92%E4%BD%9C%E6%88%90%E3%81%99%E3%82%8B)[[45]](https://ayuina.github.io/ainaba-csa-blog/azure-functions-secure-webhook/#:~:text=%E3%81%BE%E3%81%9A%E3%81%AF%20WebHook%20%E3%82%92%E5%8F%97%E3%81%91%E3%82%8B%E3%81%9F%E3%82%81%E3%81%AE%20HttpTrigger%20%E3%81%A7%E8%B5%B7%E5%8B%95%E3%81%99%E3%82%8B,Function%20%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20%E3%81%93%E3%81%93%E3%81%AF%E6%9C%AC%E9%A1%8C%E3%81%A7%E3%81%AF%E3%81%AA%E3%81%84%E3%81%AE%E3%81%A7%E5%8B%95%E4%BD%9C%E7%A2%BA%E8%AA%8D%E3%81%8C%E5%87%BA%E6%9D%A5%E3%82%8B%E7%A8%8B%E5%BA%A6%E3%81%AE%E4%B8%8B%E8%A8%98%E3%81%AE%E6%A7%98%E3%81%AA%E3%82%B3%E3%83%BC%E3%83%89%E3%81%A7%E4%BD%9C%E3%81%A3%E3%81%A6%E3%81%8A%E3%81%91%E3%81%B0%E8%89%AF%E3%81%84%E3%81%A7%E3%81%97%E3%82%87%E3%81%86%E3%80%82)。関数内ではリクエストボディ（JSON）を受け取り、必要なフィールド（アラート名・説明・発生時刻など）を抽出します。その後、外部監視サービスのWebhookやAPIエンドポイントに対してHTTPリクエストを行います（必要なら認証ヘッダーやリクエストボディを組み立て）。最後にAzure Functionは200 OKを返して処理完了です。

以下はC# Azure Functionの擬似コード例です。

[FunctionName("AlertForwarder")]  
public static async Task<IActionResult> Run(  
 [HttpTrigger(AuthorizationLevel.Function, "post")] HttpRequest req, ILogger log)  
{  
 log.LogInformation("Received an alert from Azure Monitor.");  
 string requestBody = await new StreamReader(req.Body).ReadToEndAsync();  
 // Azure Monitor共通スキーマのJSONをデシリアライズ  
 var alert = JsonConvert.DeserializeObject<AzureAlertSchema>(requestBody);  
 // 必要な情報を抽出して外部サービス用のメッセージを構築  
 var externalMessage = BuildExternalPayload(alert);  
 // 外部サービスのWebhookにHTTP POST送信  
 string externalWebhookUrl = Environment.GetEnvironmentVariable("EXT\_WEBHOOK\_URL");  
 using(var client = new HttpClient())  
 {  
 var response = await client.PostAsync(externalWebhookUrl,   
 new StringContent(externalMessage, Encoding.UTF8, "application/json"));  
 if(!response.IsSuccessStatusCode)  
 {  
 log.LogError($"Failed to send alert to external service. Status:{response.StatusCode}");  
 }  
 }  
 return new OkObjectResult("Alert forwarded.");  
}

上記は概念実装ですが、**Azure Monitorの共通アラートスキーマ**をパースし[[40]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/alerts-log-webhook#:~:text=%E3%82%92%E3%82%B5%E3%83%9D%E3%83%BC%E3%83%88%E3%81%97%E3%80%81%E5%8F%97%E4%BF%A1%E3%81%97%E3%81%9F%E3%83%9A%E3%82%A4%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AE%E4%BD%BF%E7%94%A8%E6%96%B9%E6%B3%95%E3%82%92%E6%8A%8A%E6%8F%A1%E3%81%97%E3%81%A6%E3%81%84%E3%82%8B%E5%BF%85%E8%A6%81%E3%81%8C%E3%81%82%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82)、外部のWebhookに対してJSONメッセージをPOST送信しています。例えば外部がSlackなら、SlackのIncoming Webhook URLに対してテキストメッセージを含むJSONをPOSTするコードとなるでしょう[[46]](https://stackoverflow.com/questions/77095845/azure-function-app-to-receive-azure-monitor-alert-and-post-to-slack-webhook#:~:text=try%20,orElse)[[47]](https://stackoverflow.com/questions/77095845/azure-function-app-to-receive-azure-monitor-alert-and-post-to-slack-webhook#:~:text=String%20slackWebhookUrl%20%3D%20System.getenv%28,slackMessage)。Azure FunctionのURL（例: https://<funcapp>.azurewebsites.net/api/AlertForwarder?code=<function\_key>）をアクショングループのWebhook欄に登録すれば、以降アラート発生時にFunctionが呼び出され、外部通知が実行されます。

Azure Functionを挟むことで、Azure Monitorの生アラート情報をそのまま外部に渡さずに、フォーマット変換やフィルタリングを行える利点があります。また、Function側で失敗時リトライやログ蓄積もできるため、外部サービスが一時的にダウンしていてもFunction側で検知・再送処理する、といった柔軟な実装も可能です。

* **その他の連携オプション**: Azure Monitorには他にも**ITSMコネクタ**（ServiceNowやAzure DevOpsのチケット発行）、**Automation**（WebhookでAzure Automation Runbook実行）、**Logic Apps**（コードレスで高度なワークフロー実行）等の統合手段があります[[3]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/best-practices-alerts#:~:text=match%20at%20L173%20%E3%82%B0%E3%83%AB%E3%83%BC%E3%83%97%E3%81%8C%E4%BD%BF%E7%94%A8%E3%81%95%E3%82%8C%E3%82%8B%E5%A0%B4%E5%90%88%E3%81%AF%E3%80%81%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E9%80%9A%E7%9F%A5%E3%83%9A%E3%82%A4%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AB%E5%90%AB%E3%82%81%E3%82%8B%E7%8B%AC%E8%87%AA%E3%81%AE%E3%83%97%E3%83%AD%E3%83%91%E3%83%86%E3%82%A3%E3%82%92%E8%BF%BD%E5%8A%A0%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20%E3%81%93%E3%82%8C%E3%82%89%E3%81%AE%E3%83%97%E3%83%AD%E3%83%91%E3%83%86%E3%82%A3%E3%81%AF%E3%80%81Webhook%E3%80%81Azure,Apps%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%99%E3%82%8B%E3%81%A8%E3%80%81%E7%B5%B1%E5%90%88%E3%81%AE%E3%81%9F%E3%82%81%E3%81%AB%E3%83%AF%E3%83%BC%E3%82%AF%E3%83%95%E3%83%AD%E3%83%BC%E3%82%92%E3%83%93%E3%83%AB%E3%83%89%E3%81%8A%E3%82%88%E3%81%B3%E3%82%AB%E3%82%B9%E3%82%BF%E3%83%9E%E3%82%A4%E3%82%BA%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20Logic%20Apps%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E9%80%9A%E7%9F%A5%E3%82%92%E3%82%AB%E3%82%B9%E3%82%BF%E3%83%9E%E3%82%A4%E3%82%BA%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)。特にLogic Appsは数百種類のコネクタを通じて各種システムと連携できるので、例えば「アラート発生→ServiceNowにインシデント登録し担当者にメール、Teams通知、復旧手順をRunbook実行」など複雑なシナリオを実現できます[[3]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/best-practices-alerts#:~:text=match%20at%20L173%20%E3%82%B0%E3%83%AB%E3%83%BC%E3%83%97%E3%81%8C%E4%BD%BF%E7%94%A8%E3%81%95%E3%82%8C%E3%82%8B%E5%A0%B4%E5%90%88%E3%81%AF%E3%80%81%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E9%80%9A%E7%9F%A5%E3%83%9A%E3%82%A4%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AB%E5%90%AB%E3%82%81%E3%82%8B%E7%8B%AC%E8%87%AA%E3%81%AE%E3%83%97%E3%83%AD%E3%83%91%E3%83%86%E3%82%A3%E3%82%92%E8%BF%BD%E5%8A%A0%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20%E3%81%93%E3%82%8C%E3%82%89%E3%81%AE%E3%83%97%E3%83%AD%E3%83%91%E3%83%86%E3%82%A3%E3%81%AF%E3%80%81Webhook%E3%80%81Azure,Apps%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%99%E3%82%8B%E3%81%A8%E3%80%81%E7%B5%B1%E5%90%88%E3%81%AE%E3%81%9F%E3%82%81%E3%81%AB%E3%83%AF%E3%83%BC%E3%82%AF%E3%83%95%E3%83%AD%E3%83%BC%E3%82%92%E3%83%93%E3%83%AB%E3%83%89%E3%81%8A%E3%82%88%E3%81%B3%E3%82%AB%E3%82%B9%E3%82%BF%E3%83%9E%E3%82%A4%E3%82%BA%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20Logic%20Apps%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E9%80%9A%E7%9F%A5%E3%82%92%E3%82%AB%E3%82%B9%E3%82%BF%E3%83%9E%E3%82%A4%E3%82%BA%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)。本ケースでは要求に沿ってWebhook/Azure Functionを使った連携にフォーカスしましたが、システム全体の運用フローに応じて最適な統合方法を選択してください。

最後に、通知設定時のベストプラクティスとして**テストを必ず行う**ことを挙げておきます。Azure Monitorには「**アクショングループのテスト**」機能や「**サンプル アラートの送信**」機能があり、実際にWebhookに対してテストペイロードを送ってみることができます[[48]](https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-payload-samples#:~:text=Sample%20alert%20payloads%20,This%20helps%20validate%20the)。運用前に外部サービスが正しく受信・処理できるか確認し、必要ならペイロード内容をログ出力してデバッグすると安心です。

## その他の設計上の考慮事項と推奨事項

* **監視データの蓄積と保持期間**: Log Analytics Workspaceのデータ保持期間はデフォルト31日ですが、要件に応じて延長できます（最大2年間、もしくはアーカイブでさらに長期保管）。トラブルシューティングや傾向分析のため、パフォーマンスデータは数ヶ月以上保持すると便利です。コスト許容なら長めの保持を検討してください。
* **Azure Monitorエージェントへの集約**: 以前はAzure Diagnosticsや別個のエージェントが必要だったシナリオ（例えばAzure VMの診断設定によるメトリック送信など）も、現在はAzure Monitorエージェント＋DCRに一本化されています[[49]](https://learn.microsoft.com/en-us/azure/azure-monitor/data-collection/data-collection-rule-overview#:~:text=Legacy%20method%20DCR%20method%20Description,It%20replaces%20the)。できるだけAMAに統一し、レガシー方式は廃止するのが運用負荷・信頼性の面で望ましいです[[50]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=,%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86%E3%83%AB%E3%83%BC%E3%83%AB%E3%81%AE%E6%A7%8B%E9%80%A0%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E6%88%A6%E7%95%A5%E3%82%92%E7%A2%BA%E7%AB%8B%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)。なおAzure Arc対応のハイブリッドマシンでもAMAが使えるため、オンプレVMも含め一貫した監視を行えます[[51]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=Azure%20Arc%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%80%81Azure%20%E3%81%AE%E5%A4%96%E9%83%A8%E3%81%AB%E3%81%82%E3%82%8B%20VM,for%20servers%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%99%E3%82%8B%E3%81%A8%E3%80%81Azure%20%E3%81%AE%E5%A4%96%E9%83%A8%E3%80%81%E4%BC%81%E6%A5%AD%E3%83%8D%E3%83%83%E3%83%88%E3%83%AF%E3%83%BC%E3%82%AF%E3%80%81%E3%81%BE%E3%81%9F%E3%81%AF%E4%BB%96%E3%81%AE%E3%82%AF%E3%83%A9%E3%82%A6%E3%83%89%20%E3%83%97%E3%83%AD%E3%83%90%E3%82%A4%E3%83%80%E3%83%BC%E3%81%A7%E3%83%9B%E3%82%B9%E3%83%88%E3%81%95%E3%82%8C%E3%81%A6%E3%81%84%E3%82%8B%E7%89%A9%E7%90%86%E3%82%B5%E3%83%BC%E3%83%90%E3%83%BC%E3%81%A8%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%82%92%E7%AE%A1%E7%90%86%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82)。
* **ネットワークセキュリティ**: 監視データ送信は基本的にAzure Monitorのパブリックエンドポイントに対して暗号化されて行われますが、更にセキュアにするなら**Azure Private Link**の利用が推奨されます[[52]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=,VM%20%E3%82%92%20Azure%20Monitor%20%E3%81%AB%E6%8E%A5%E7%B6%9A%E3%81%99%E3%82%8B)。Private Linkを使うと、Log Analytics Workspaceへのデータ送信を社内ネットワーク経由（ExpressRouteやSite-to-Site VPN経由）に限定できます[[52]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=,VM%20%E3%82%92%20Azure%20Monitor%20%E3%81%AB%E6%8E%A5%E7%B6%9A%E3%81%99%E3%82%8B)。金融・医療など厳格な環境ではPrivate Link接続＋送信認証(Workspaceキー管理など)を組み合わせるとよいでしょう。
* **コストモニタリング**: 本件では「コストは重視しない（精度優先）」との前提ですが、それでもAzure Monitorの費用は把握しておくべきです。Log Analyticsの課金は主にデータ量(インジェスト量と保管期間)とログクエリ実行回数により発生します[[53]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Azure%20Monitor%20%E3%81%AE%E3%82%B3%E3%82%B9%E3%83%88%E3%81%AF%E3%80%81%E5%8F%8E%E9%9B%86%E3%81%99%E3%82%8B%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AE%E9%87%8F%E3%81%AB%E3%82%88%E3%81%A3%E3%81%A6%E5%A4%89%E3%82%8F%E3%82%8B%E3%81%9F%E3%82%81%E3%80%81%E7%9B%A3%E8%A6%96%E8%A6%81%E4%BB%B6%E3%82%92%E6%BA%80%E3%81%9F%E3%81%99%E3%81%9F%E3%82%81%E3%81%AB%E5%BF%85%E8%A6%81%E3%81%A8%E3%81%99%E3%82%8B%E4%BB%A5%E4%B8%8A%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E5%8F%8E%E9%9B%86%E3%81%97%E3%81%AA%E3%81%84%E3%82%88%E3%81%86%E3%81%AB%E3%81%97%E3%81%A6%E3%81%8F%E3%81%A0%E3%81%95%E3%81%84%E3%80%82%20%E6%A7%8B%E6%88%90%E3%81%AF%E3%80%81%E4%BA%88%E7%AE%97%E3%81%A8%E3%80%81%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AE%E9%81%8B%E7%94%A8%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6%E5%BF%85%E8%A6%81%E3%81%A8%E3%81%99%E3%82%8B%E5%88%86%E6%9E%90%E6%83%85%E5%A0%B1%E3%81%AE%E9%87%8F%E3%81%AE%E3%83%90%E3%83%A9%E3%83%B3%E3%82%B9%E3%82%92%E3%81%A8%E3%81%A3%E3%81%A6%E8%A8%AD%E5%AE%9A%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)。高頻度の詳細ログ収集は大きなデータ量となるため、運用開始後は**Log Analyticsワークスペースの使用状況**を分析し、無駄なデータがないかチェックしましょう[[20]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%E4%B8%80%E8%88%AC%E7%9A%84%E3%81%AA%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AF%E3%80%81%E6%AF%8E%E6%9C%88%201%20GB%20%E3%81%8B%E3%82%89%203,%E3%83%9C%E3%83%AA%E3%83%A5%E3%83%BC%E3%83%A0%20%E3%81%AE%20%2013%E3%81%BE%E3%81%9F%E3%81%AF%E3%83%AD%E3%82%B0%20%E3%82%AF%E3%82%A8%E3%83%AA%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%80%81%E5%90%84%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AB%E5%AF%BE%E3%81%97%E3%81%A6%E5%8F%8E%E9%9B%86%E3%81%95%E3%82%8C%E3%82%8B%E8%AA%B2%E9%87%91%E5%AF%BE%E8%B1%A1%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AE%E9%87%8F%E3%82%92%E6%B1%BA%E5%AE%9A%E3%81%97%E3%80%81%E3%81%9D%E3%82%8C%E3%81%AB%E5%BF%9C%E3%81%98%E3%81%A6%E8%AA%BF%E6%95%B4%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)。Azure MonitorにはWorkspaceごとのテーブル別データ量を可視化する機能（Workspace Insights）もあります[[54]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=match%20at%20L138%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AE%E5%A0%B4%E5%90%88%E3%80%81%E3%81%BE%E3%81%9F%E3%81%AF%E5%90%8C%E6%A7%98%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86%E3%83%AB%E3%83%BC%E3%83%AB%E3%82%92%E4%BD%9C%E6%88%90%E3%81%99%E3%82%8B%E5%A0%B4%E5%90%88%E3%81%AB%E3%81%AF%E3%80%81%E5%90%84%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9%E3%81%AB%E4%B8%80%E6%84%8F%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E9%80%81%E4%BF%A1%E3%81%97%E3%81%A6%E3%81%84%E3%82%8B%E3%81%93%E3%81%A8%E3%82%92%E7%A2%BA%E8%AA%8D%E3%81%97%E3%81%A6%E3%81%8F%E3%81%A0%E3%81%95%E3%81%84%E3%80%82%20%E9%87%8D%E8%A4%87%E3%81%97%E3%81%9F%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E5%8F%8E%E9%9B%86%E3%81%97%E3%81%AA%E3%81%84%E3%82%88%E3%81%86%E3%81%AB%E5%8F%8E%E9%9B%86%E3%81%97%E3%81%9F%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E5%88%86%E6%9E%90%E3%81%99%E3%82%8B%E6%96%B9%E6%B3%95%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6%E3%81%AF%E3%80%81%E3%80%8CLog,Analytics%20%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9%E3%81%A7%E3%81%AE%E4%BD%BF%E7%94%A8%E9%87%8F%E3%82%92%E5%88%86%E6%9E%90%E3%81%99%E3%82%8B%E3%80%8D%E3%82%92%E5%8F%82%E7%85%A7%E3%81%97%E3%81%A6%E3%81%8F%E3%81%A0%E3%81%95%E3%81%84%E3%80%82%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E9%96%93%E3%81%A7%E7%A7%BB%E8%A1%8C%E3%81%99%E3%82%8B%E5%A0%B4%E5%90%88%E3%80%81%E3%81%9D%E3%82%8C%E3%81%9E%E3%82%8C%E3%81%8C%E5%9B%BA%E6%9C%89%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E5%8F%8E%E9%9B%86%E3%81%97%E3%81%A6%E3%81%84%E3%82%8B%E3%81%93%E3%81%A8%E3%82%92%E7%A2%BA%E8%AA%8D%E3%81%A7%E3%81%8D%E3%81%AA%E3%81%84%E9%99%90%E3%82%8A%E3%80%81%E4%B8%A1%E6%96%B9%E3%82%92%E4%BD%B5%E7%94%A8%E3%81%99%E3%82%8B%E3%81%AE%E3%81%A7%E3%81%AF%E3%81%AA%E3%81%8F%E3%80%81Azure%20Monitor)。エージェント側で不要データをフィルタするなど、費用対効果を考えたチューニングは継続的に行うのが理想です。
* **Application Insightsの活用**: 可能であれば、Webアプリに**Application Insights**のSDKを組み込むことも検討してください。Application InsightsはAzure Monitorの一部として提供されるアプリケーションパフォーマンス管理(APM)サービスで、リクエストの追跡や依存関係(call graph)の収集、例外発生の詳細なスタックトレース取得、カスタムイベントの計測などができます[[55]](https://learn.microsoft.com/en-us/azure/azure-monitor/fundamentals/enterprise-monitoring-architecture#:~:text=,actually%20do%20with%20your%20app)。今回、アプリログをファイル経由で収集していますが、App Insightsならより構造化されたテレメトリ（例：各HTTPリクエストの応答時間・結果、SQL呼び出しの時間、ユーザー環境情報など）が自動収集されます。監視精度を極限まで高めるなら、Log Analyticsによるインフラ監視に加えてApp Insightsによるアプリケーション監視を並用すると効果的です[[56]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine#:~:text=similar%20to%20the%20operating%20system,be%20monitored%20by%20Application%20insights)[[55]](https://learn.microsoft.com/en-us/azure/azure-monitor/fundamentals/enterprise-monitoring-architecture#:~:text=,actually%20do%20with%20your%20app)。
* **定期的なレビューとテスト**: 監視設定は一度構築したら終わりではなく、変更管理のたびに見直すことが重要です。アプリのログ仕様が変わったらDCRやクエリを更新し、閾値は適切か、アラートの頻度は適当かを定期的にレビューしましょう。また、実際のインシデント対応訓練の一環でアラートを発生させ、通知フローや外部サービス連携が期待通り機能するかシミュレーションしておくと万全です。

## まとめ

以上、Azure VM上のWebアプリケーションを対象に、Azure MonitorとLog Analytics Workspaceを用いた監視のベストプラクティスを解説しました。エージェントとDCRによるきめ細かな**データ収集**設定、CPUやメモリからアプリエラーに至るまでの**広範なメトリクス・ログ監視**、そしてAzure Monitorアラートを活用した**プロアクティブな通知・外部連携**の仕組みにより、信頼性と運用性の高い監視ソリューションを構築できます。コストよりも機能・精度を優先する方針の下、収集可能なデータは極力すべて集約し、必要なアラートは余さず定義するアプローチをとりました。ただ闇雲にデータを集めるのではなく、Microsoftのベストプラクティスに沿って適切に整理・フィルタし、**「必要な情報を、必要なときに、確実に掴める」**監視基盤を目指すことが重要です。

本ガイドが、Azureベースの監視設計・構成の一助となれば幸いです。高機能なAzure Monitorを駆使して、システムの健全性を把握・維持し、問題発生時にはいち早く検知して外部の運用フローへつなげられるよう、継続的にチューニングしながら運用してください。

**参考資料:** Azure公式ドキュメント（仮想マシン監視のベストプラクティス[[12]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E5%8B%A7%E5%91%8A%20%E8%AA%AC%E6%98%8E%20Azure%20VM%20%E7%94%A8%E3%81%AE%E5%8F%AF%E7%94%A8%E6%80%A7%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88,%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AF%E3%80%81%E6%AF%8E%E5%88%86%20Log%20Analytics%20%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9%E3%81%AB%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%E3%82%92%E9%80%81%E4%BF%A1%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AE%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%9F%E3%83%AD%E3%82%B0%E6%A4%9C%E7%B4%A2%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88)[[13]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AE%E6%AD%A3%E5%B8%B8%E6%80%A7%E3%82%92%E7%A2%BA%E8%AA%8D%E3%81%99%E3%82%8B%E3%81%9F%E3%82%81%E3%81%AE%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%20%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%20%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20Azure,Monitor%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%9F%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AE%E7%9B%A3%E8%A6%96%3A%20%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E3%80%8D%E3%81%AE%E6%83%85%E5%A0%B1%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%80%81%E3%82%AF%E3%83%A9%E3%82%A4%E3%82%A2%E3%83%B3%E3%83%88%20%E3%83%AF%E3%83%BC%E3%82%AF%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AE%E6%BD%9C%E5%9C%A8%E7%9A%84%E3%81%AA%E9%81%8B%E7%94%A8%E4%B8%8A%E3%81%AE%E5%95%8F%E9%A1%8C%E3%82%92%E4%BA%8B%E5%89%8D%E3%81%AB%E9%80%9A%E7%9F%A5%E3%81%99%E3%82%8B%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82)、データ収集の構成方法[[6]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Azure%20Monitor%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%8B%E3%82%89%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86%E3%81%AF%E3%80%81Azure%20%E3%82%B5%E3%83%96%E3%82%B9%E3%82%AF%E3%83%AA%E3%83%97%E3%82%B7%E3%83%A7%E3%83%B3%E3%81%AB%E6%A0%BC%E7%B4%8D%E3%81%95%E3%82%8C%E3%80%81%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AB%E9%96%A2%E9%80%A3%E4%BB%98%E3%81%91%E3%82%89%E3%82%8C%E3%81%A6%E3%81%84%E3%82%8B%201,DCR%29%20%E3%81%AB%E3%82%88%E3%81%A3%E3%81%A6%E5%AE%9A%E7%BE%A9%E3%81%95%E3%82%8C%E3%81%BE%E3%81%99%E3%80%82)、ログクエリ例[[22]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%60Perf%20%5C,%5C%7C%20summarize%20AggregatedValue)[[57]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%E3%81%93%E3%81%93%E3%81%A7%E4%BD%BF%E7%94%A8%E3%81%99%E3%82%8B%E5%88%97%E5%90%8D%E3%81%AF%E3%80%81%E4%BE%8B%E3%81%A8%E3%81%97%E3%81%A6%E7%A4%BA%E3%81%97%E3%81%A6%E3%81%84%E3%82%8B%E3%81%A0%E3%81%91%E3%81%A7%E3%81%99%E3%80%82%20%E3%81%BB%E3%81%A8%E3%82%93%E3%81%A9%E3%81%AE%E5%A0%B4%E5%90%88%E3%80%81%E3%81%94%E4%BD%BF%E7%94%A8%E3%81%AE%E3%83%AD%E3%82%B0%E3%81%AE%E5%88%97%E5%90%8D%E3%81%AF%E7%95%B0%E3%81%AA%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82)）、ならびに各種Azure Monitor機能ガイドライン[[43]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/best-practices-alerts#:~:text=)[[40]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/alerts-log-webhook#:~:text=%E3%82%92%E3%82%B5%E3%83%9D%E3%83%BC%E3%83%88%E3%81%97%E3%80%81%E5%8F%97%E4%BF%A1%E3%81%97%E3%81%9F%E3%83%9A%E3%82%A4%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AE%E4%BD%BF%E7%94%A8%E6%96%B9%E6%B3%95%E3%82%92%E6%8A%8A%E6%8F%A1%E3%81%97%E3%81%A6%E3%81%84%E3%82%8B%E5%BF%85%E8%A6%81%E3%81%8C%E3%81%82%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82)。これらを適宜参照し、最新のサービス更新にも注意を払いながら最適な監視を実現しましょう。

[[1]](https://learn.microsoft.com/en-us/azure/azure-monitor/fundamentals/enterprise-monitoring-architecture#:~:text=,created%20in%20the%20ITSM%20system) [[2]](https://learn.microsoft.com/en-us/azure/azure-monitor/fundamentals/enterprise-monitoring-architecture#:~:text=,created%20in%20the%20ITSM%20system) [[55]](https://learn.microsoft.com/en-us/azure/azure-monitor/fundamentals/enterprise-monitoring-architecture#:~:text=,actually%20do%20with%20your%20app) Azure Monitor enterprise monitoring architecture - Azure Monitor | Microsoft Learn

<https://learn.microsoft.com/en-us/azure/azure-monitor/fundamentals/enterprise-monitoring-architecture>

[[3]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/best-practices-alerts#:~:text=match%20at%20L173%20%E3%82%B0%E3%83%AB%E3%83%BC%E3%83%97%E3%81%8C%E4%BD%BF%E7%94%A8%E3%81%95%E3%82%8C%E3%82%8B%E5%A0%B4%E5%90%88%E3%81%AF%E3%80%81%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E9%80%9A%E7%9F%A5%E3%83%9A%E3%82%A4%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AB%E5%90%AB%E3%82%81%E3%82%8B%E7%8B%AC%E8%87%AA%E3%81%AE%E3%83%97%E3%83%AD%E3%83%91%E3%83%86%E3%82%A3%E3%82%92%E8%BF%BD%E5%8A%A0%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20%E3%81%93%E3%82%8C%E3%82%89%E3%81%AE%E3%83%97%E3%83%AD%E3%83%91%E3%83%86%E3%82%A3%E3%81%AF%E3%80%81Webhook%E3%80%81Azure,Apps%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%99%E3%82%8B%E3%81%A8%E3%80%81%E7%B5%B1%E5%90%88%E3%81%AE%E3%81%9F%E3%82%81%E3%81%AB%E3%83%AF%E3%83%BC%E3%82%AF%E3%83%95%E3%83%AD%E3%83%BC%E3%82%92%E3%83%93%E3%83%AB%E3%83%89%E3%81%8A%E3%82%88%E3%81%B3%E3%82%AB%E3%82%B9%E3%82%BF%E3%83%9E%E3%82%A4%E3%82%BA%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20Logic%20Apps%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E9%80%9A%E7%9F%A5%E3%82%92%E3%82%AB%E3%82%B9%E3%82%BF%E3%83%9E%E3%82%A4%E3%82%BA%E3%81%97%E3%81%BE%E3%81%99%E3%80%82) [[42]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/best-practices-alerts#:~:text=) [[43]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/best-practices-alerts#:~:text=) Azure Monitor アラートのベストプラクティス - Azure Monitor | Microsoft Learn

<https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/best-practices-alerts>

[[4]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E8%A9%B3%E7%B4%B0%E3%81%AA%E3%83%87%E3%83%BC%E3%82%BF%20%E3%83%95%E3%82%A3%E3%83%AB%E3%82%BF%E3%83%BC%E5%87%A6%E7%90%86%E3%81%AE%E3%81%9F%E3%82%81%E3%80%81Log%20Analytics%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%8B%E3%82%89%20Azure,Log%20Analytics%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AB%E3%82%88%E3%82%8B%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86%E3%81%AE%E6%A7%8B%E6%88%90%E3%81%AF%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9%E3%81%A7%E8%A1%8C%E3%82%8F%E3%82%8C%E3%82%8B%E3%81%9F%E3%82%81%E3%80%81%E3%81%99%E3%81%B9%E3%81%A6%E3%81%AE%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%8C%E5%90%8C%E3%81%98%E6%A7%8B%E6%88%90%E3%82%92%E5%8F%97%E3%81%91%E5%8F%96%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82%20Azure%20Monitor) [[5]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=match%20at%20L127%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%A7%E4%BD%BF%E7%94%A8%E3%81%95%E3%82%8C%E3%82%8B%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86%E3%83%AB%E3%83%BC%E3%83%AB%E3%81%AF%E3%80%81%E3%81%95%E3%81%BE%E3%81%96%E3%81%BE%E3%81%AA%20VM,%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E5%8F%8E%E9%9B%86%E3%81%95%E3%82%8C%E3%82%8B%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E3%83%95%E3%82%A3%E3%83%AB%E3%82%BF%E3%83%BC%E5%87%A6%E7%90%86%E3%81%99%E3%82%8B%E3%81%93%E3%81%A8%E3%82%82%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20%E4%B8%8D%E8%A6%81%E3%81%AA%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%8B%E3%82%89%E5%8F%96%E3%82%8A%E9%99%A4%E3%81%8F%E3%81%9F%E3%82%81%E3%81%AB%E3%83%95%E3%82%A3%E3%83%AB%E3%82%BF%E3%83%BC%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E3%82%84%E5%88%86%E6%9E%90%E3%81%AB%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%AA%E3%81%84%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E3%83%95%E3%82%A3%E3%83%AB%E3%82%BF%E3%83%BC%E5%87%A6%E7%90%86%E3%81%97%E3%81%A6%E3%80%81%E3%83%87%E3%83%BC%E3%82%BF%20%E3%82%A4%E3%83%B3%E3%82%B8%E3%82%A7%E3%82%B9%E3%83%88%20%E3%82%B3%E3%82%B9%E3%83%88%E3%82%92%E5%89%8A%E6%B8%9B%E3%81%97%E3%81%BE%E3%81%99%E3%80%82) [[8]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=match%20at%20L177%20Azure%20Connected,%E3%81%AE%E3%82%BB%E3%83%83%E3%83%88%E3%81%A8%E3%80%81%E4%BD%9C%E6%88%90%E3%81%95%E3%82%8C%E3%81%9F%E6%96%B0%E3%81%97%E3%81%84%20VM%20%E3%81%AB%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%82%92%E8%87%AA%E5%8B%95%E7%9A%84%E3%81%AB%E3%83%87%E3%83%97%E3%83%AD%E3%82%A4%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20%E3%81%93%E3%82%8C%E3%81%AB%E3%82%88%E3%82%8A%E3%80%81%E7%AE%A1%E7%90%86%E8%80%85%E3%81%AB%E3%82%88%E3%82%8B%E4%BB%8B%E5%85%A5%E3%82%92%E6%9C%80%E5%B0%8F%E9%99%90%E3%81%AB%E6%8A%91%E3%81%88%E3%81%A6%E3%80%81%E3%81%99%E3%81%B9%E3%81%A6%E3%81%AE%20VM) [[12]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E5%8B%A7%E5%91%8A%20%E8%AA%AC%E6%98%8E%20Azure%20VM%20%E7%94%A8%E3%81%AE%E5%8F%AF%E7%94%A8%E6%80%A7%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88,%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AF%E3%80%81%E6%AF%8E%E5%88%86%20Log%20Analytics%20%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9%E3%81%AB%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%E3%82%92%E9%80%81%E4%BF%A1%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AE%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%9F%E3%83%AD%E3%82%B0%E6%A4%9C%E7%B4%A2%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88) [[13]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AE%E6%AD%A3%E5%B8%B8%E6%80%A7%E3%82%92%E7%A2%BA%E8%AA%8D%E3%81%99%E3%82%8B%E3%81%9F%E3%82%81%E3%81%AE%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%20%E3%83%8F%E3%83%BC%E3%83%88%E3%83%93%E3%83%BC%E3%83%88%20%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20Azure,Monitor%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%9F%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AE%E7%9B%A3%E8%A6%96%3A%20%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E3%80%8D%E3%81%AE%E6%83%85%E5%A0%B1%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%80%81%E3%82%AF%E3%83%A9%E3%82%A4%E3%82%A2%E3%83%B3%E3%83%88%20%E3%83%AF%E3%83%BC%E3%82%AF%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AE%E6%BD%9C%E5%9C%A8%E7%9A%84%E3%81%AA%E9%81%8B%E7%94%A8%E4%B8%8A%E3%81%AE%E5%95%8F%E9%A1%8C%E3%82%92%E4%BA%8B%E5%89%8D%E3%81%AB%E9%80%9A%E7%9F%A5%E3%81%99%E3%82%8B%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82) [[21]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%A7%E4%BD%BF%E7%94%A8%E3%81%95%E3%82%8C%E3%82%8B%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86%E3%83%AB%E3%83%BC%E3%83%AB%E3%81%AF%E3%80%81%E3%81%95%E3%81%BE%E3%81%96%E3%81%BE%E3%81%AA%20VM%20%E3%82%BB%E3%83%83%E3%83%88%E3%81%AE%E7%89%B9%E5%AE%9A%E3%81%AE%E7%9B%A3%E8%A6%96%E8%A6%81%E4%BB%B6%E3%81%AB%E5%90%88%E3%82%8F%E3%81%9B%E3%81%A6%E8%AA%BF%E6%95%B4%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20Azure%20Monitor,%E3%82%B3%E3%82%B9%E3%83%88%E3%82%92%E5%89%8A%E6%B8%9B%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20%E3%81%95%E3%81%BE%E3%81%96%E3%81%BE%E3%81%AA%E7%9B%A3%E8%A6%96%E3%82%B7%E3%83%8A%E3%83%AA%E3%82%AA%E3%81%A7%E5%8F%8E%E9%9B%86%E3%81%99%E3%82%8B%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E3%82%AC%E3%82%A4%E3%83%80%E3%83%B3%E3%82%B9%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6%E3%81%AF%E3%80%81%E3%80%8C%20Azure%20Monitor%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%9F%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AE%E7%9B%A3%E8%A6%96) [[28]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=%E3%81%8C%E8%87%AA%E5%8B%95%E7%9A%84%E3%81%AB%E7%9B%A3%E8%A6%96%E3%81%95%E3%82%8C%E3%82%8B%E3%82%88%E3%81%86%E3%81%AB%E3%81%AA%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82%20%E3%81%93%E3%81%AE%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%81%A7%E3%81%AF%E3%80%81Azure%20Monitor%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%82%92,%E3%82%A4%E3%83%99%E3%83%B3%E3%83%88%E5%8F%8E%E9%9B%86%E3%82%92%E6%A7%8B%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20%E3%80%8C%208%20Azure%20Monitor) [[50]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=,%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86%E3%83%AB%E3%83%BC%E3%83%AB%E3%81%AE%E6%A7%8B%E9%80%A0%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E6%88%A6%E7%95%A5%E3%82%92%E7%A2%BA%E7%AB%8B%E3%81%97%E3%81%BE%E3%81%99%E3%80%82) [[51]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=Azure%20Arc%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%80%81Azure%20%E3%81%AE%E5%A4%96%E9%83%A8%E3%81%AB%E3%81%82%E3%82%8B%20VM,for%20servers%20%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%99%E3%82%8B%E3%81%A8%E3%80%81Azure%20%E3%81%AE%E5%A4%96%E9%83%A8%E3%80%81%E4%BC%81%E6%A5%AD%E3%83%8D%E3%83%83%E3%83%88%E3%83%AF%E3%83%BC%E3%82%AF%E3%80%81%E3%81%BE%E3%81%9F%E3%81%AF%E4%BB%96%E3%81%AE%E3%82%AF%E3%83%A9%E3%82%A6%E3%83%89%20%E3%83%97%E3%83%AD%E3%83%90%E3%82%A4%E3%83%80%E3%83%BC%E3%81%A7%E3%83%9B%E3%82%B9%E3%83%88%E3%81%95%E3%82%8C%E3%81%A6%E3%81%84%E3%82%8B%E7%89%A9%E7%90%86%E3%82%B5%E3%83%BC%E3%83%90%E3%83%BC%E3%81%A8%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%82%92%E7%AE%A1%E7%90%86%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82) [[52]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=,VM%20%E3%82%92%20Azure%20Monitor%20%E3%81%AB%E6%8E%A5%E7%B6%9A%E3%81%99%E3%82%8B) [[54]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm#:~:text=match%20at%20L138%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%AE%E5%A0%B4%E5%90%88%E3%80%81%E3%81%BE%E3%81%9F%E3%81%AF%E5%90%8C%E6%A7%98%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86%E3%83%AB%E3%83%BC%E3%83%AB%E3%82%92%E4%BD%9C%E6%88%90%E3%81%99%E3%82%8B%E5%A0%B4%E5%90%88%E3%81%AB%E3%81%AF%E3%80%81%E5%90%84%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9%E3%81%AB%E4%B8%80%E6%84%8F%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E9%80%81%E4%BF%A1%E3%81%97%E3%81%A6%E3%81%84%E3%82%8B%E3%81%93%E3%81%A8%E3%82%92%E7%A2%BA%E8%AA%8D%E3%81%97%E3%81%A6%E3%81%8F%E3%81%A0%E3%81%95%E3%81%84%E3%80%82%20%E9%87%8D%E8%A4%87%E3%81%97%E3%81%9F%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E5%8F%8E%E9%9B%86%E3%81%97%E3%81%AA%E3%81%84%E3%82%88%E3%81%86%E3%81%AB%E5%8F%8E%E9%9B%86%E3%81%97%E3%81%9F%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E5%88%86%E6%9E%90%E3%81%99%E3%82%8B%E6%96%B9%E6%B3%95%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6%E3%81%AF%E3%80%81%E3%80%8CLog,Analytics%20%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9%E3%81%A7%E3%81%AE%E4%BD%BF%E7%94%A8%E9%87%8F%E3%82%92%E5%88%86%E6%9E%90%E3%81%99%E3%82%8B%E3%80%8D%E3%82%92%E5%8F%82%E7%85%A7%E3%81%97%E3%81%A6%E3%81%8F%E3%81%A0%E3%81%95%E3%81%84%E3%80%82%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E9%96%93%E3%81%A7%E7%A7%BB%E8%A1%8C%E3%81%99%E3%82%8B%E5%A0%B4%E5%90%88%E3%80%81%E3%81%9D%E3%82%8C%E3%81%9E%E3%82%8C%E3%81%8C%E5%9B%BA%E6%9C%89%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E5%8F%8E%E9%9B%86%E3%81%97%E3%81%A6%E3%81%84%E3%82%8B%E3%81%93%E3%81%A8%E3%82%92%E7%A2%BA%E8%AA%8D%E3%81%A7%E3%81%8D%E3%81%AA%E3%81%84%E9%99%90%E3%82%8A%E3%80%81%E4%B8%A1%E6%96%B9%E3%82%92%E4%BD%B5%E7%94%A8%E3%81%99%E3%82%8B%E3%81%AE%E3%81%A7%E3%81%AF%E3%81%AA%E3%81%8F%E3%80%81Azure%20Monitor) Azure Monitor で仮想マシンを監視するベスト プラクティス - Azure Monitor | Microsoft Learn

<https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/best-practices-vm>

[[6]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Azure%20Monitor%20%E3%82%A8%E3%83%BC%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88%E3%81%8B%E3%82%89%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E5%8F%8E%E9%9B%86%E3%81%AF%E3%80%81Azure%20%E3%82%B5%E3%83%96%E3%82%B9%E3%82%AF%E3%83%AA%E3%83%97%E3%82%B7%E3%83%A7%E3%83%B3%E3%81%AB%E6%A0%BC%E7%B4%8D%E3%81%95%E3%82%8C%E3%80%81%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AB%E9%96%A2%E9%80%A3%E4%BB%98%E3%81%91%E3%82%89%E3%82%8C%E3%81%A6%E3%81%84%E3%82%8B%201,DCR%29%20%E3%81%AB%E3%82%88%E3%81%A3%E3%81%A6%E5%AE%9A%E7%BE%A9%E3%81%95%E3%82%8C%E3%81%BE%E3%81%99%E3%80%82) [[9]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%E3%83%91%E3%83%95%E3%82%A9%E3%83%BC%E3%83%9E%E3%83%B3%E3%82%B9%20%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AF%E3%80%81%E6%AC%A1%E3%81%AE%E3%83%86%E3%83%BC%E3%83%96%E3%83%AB%E3%81%AB%E9%80%81%E4%BF%A1%E3%81%95%E3%82%8C%E3%81%BE%E3%81%99%E3%80%82%20%E2%80%A2%20VM%20%E5%88%86%E6%9E%90%E6%83%85%E5%A0%B1%3A,%E2%80%A2%20%E3%81%9D%E3%81%AE%E4%BB%96%E3%81%AE%E3%83%91%E3%83%95%E3%82%A9%E3%83%BC%E3%83%9E%E3%83%B3%E3%82%B9%20%E3%83%87%E3%83%BC%E3%82%BF%3A%20%2040) [[10]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=,%E3%83%A1%E3%83%88%E3%83%AA%E3%83%83%E3%82%AF%20%E3%81%AB%E9%80%81%E4%BF%A1%E3%81%97%E3%80%81%E3%83%A1%E3%83%88%E3%83%AA%E3%83%83%E3%82%AF%20%E3%82%B9%20%E3%82%A8%E3%82%AF%E3%82%B9%E3%83%97%E3%83%AD%E3%83%BC%E3%83%A9%E3%83%BC%E3%81%A8%E3%83%A1%E3%83%88%E3%83%AA%E3%83%83%E3%82%AF%20%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E3%81%A7%E4%BD%BF%E7%94%A8%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82) [[11]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%E5%AE%9B%E5%85%88%20%E8%AA%AC%E6%98%8E%20%E3%83%A1%E3%83%88%E3%83%AA%E3%83%83%E3%82%AF%20%E3%83%9B%E3%82%B9%E3%83%88%20%E3%83%A1%E3%83%88%E3%83%AA%E3%83%83%E3%82%AF%E3%81%AF%E3%80%81Azure,%E3%81%BE%E3%81%9F%E3%81%AF%2038%E3%81%A7%E3%83%AD%E3%82%B0%20%E3%82%AF%E3%82%A8%E3%83%AA%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%80%81%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E3%82%A4%E3%83%99%E3%83%B3%E3%83%88%20%E3%83%87%E3%83%BC%E3%82%BF%E3%81%A8%E5%85%B1%E3%81%AB%E5%88%86%E6%9E%90%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82%20%E8%A4%87%E6%95%B0%E3%81%AE%E3%83%9E%E3%82%B7%E3%83%B3%E3%80%81%E3%83%AA%E3%83%BC%E3%82%B8%E3%83%A7%E3%83%B3%E3%80%81%E3%82%B5%E3%83%96%E3%82%B9%E3%82%AF%E3%83%AA%E3%83%97%E3%82%B7%E3%83%A7%E3%83%B3%E3%81%AB%E3%81%BE%E3%81%9F%E3%81%8C%E3%82%8B%E8%A4%87%E9%9B%91%E3%81%AA%E3%83%AD%E3%82%B8%E3%83%83%E3%82%AF%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E7%9B%B8%E4%BA%92%E3%81%AB%E9%96%A2%E9%80%A3%E4%BB%98%E3%81%91%E3%82%8B%E3%81%93%E3%81%A8%E3%82%82%E3%81%A7%E3%81%8D%E3%81%BE%E3%81%99%E3%80%82) [[20]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%E4%B8%80%E8%88%AC%E7%9A%84%E3%81%AA%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AF%E3%80%81%E6%AF%8E%E6%9C%88%201%20GB%20%E3%81%8B%E3%82%89%203,%E3%83%9C%E3%83%AA%E3%83%A5%E3%83%BC%E3%83%A0%20%E3%81%AE%20%2013%E3%81%BE%E3%81%9F%E3%81%AF%E3%83%AD%E3%82%B0%20%E3%82%AF%E3%82%A8%E3%83%AA%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%80%81%E5%90%84%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AB%E5%AF%BE%E3%81%97%E3%81%A6%E5%8F%8E%E9%9B%86%E3%81%95%E3%82%8C%E3%82%8B%E8%AA%B2%E9%87%91%E5%AF%BE%E8%B1%A1%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AE%E9%87%8F%E3%82%92%E6%B1%BA%E5%AE%9A%E3%81%97%E3%80%81%E3%81%9D%E3%82%8C%E3%81%AB%E5%BF%9C%E3%81%98%E3%81%A6%E8%AA%BF%E6%95%B4%E3%81%97%E3%81%BE%E3%81%99%E3%80%82) [[22]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%60Perf%20%5C,%5C%7C%20summarize%20AggregatedValue) [[23]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%60Perf%20%5C,) [[24]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%60Perf%20%5C,1%20%E6%99%82%E9%96%93%E3%81%94%E3%81%A8) [[34]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%E3%82%AF%E3%82%A8%E3%83%AA%20%E8%AA%AC%E6%98%8E%20%60MyApp_CL%20%5C,%E3%82%A8%E3%83%A9%E3%83%BC%20%E3%82%A4%E3%83%99%E3%83%B3%E3%83%88%E3%81%AB%E5%AF%BE%E3%81%99%E3%82%8B%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82) [[53]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Azure%20Monitor%20%E3%81%AE%E3%82%B3%E3%82%B9%E3%83%88%E3%81%AF%E3%80%81%E5%8F%8E%E9%9B%86%E3%81%99%E3%82%8B%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AE%E9%87%8F%E3%81%AB%E3%82%88%E3%81%A3%E3%81%A6%E5%A4%89%E3%82%8F%E3%82%8B%E3%81%9F%E3%82%81%E3%80%81%E7%9B%A3%E8%A6%96%E8%A6%81%E4%BB%B6%E3%82%92%E6%BA%80%E3%81%9F%E3%81%99%E3%81%9F%E3%82%81%E3%81%AB%E5%BF%85%E8%A6%81%E3%81%A8%E3%81%99%E3%82%8B%E4%BB%A5%E4%B8%8A%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E5%8F%8E%E9%9B%86%E3%81%97%E3%81%AA%E3%81%84%E3%82%88%E3%81%86%E3%81%AB%E3%81%97%E3%81%A6%E3%81%8F%E3%81%A0%E3%81%95%E3%81%84%E3%80%82%20%E6%A7%8B%E6%88%90%E3%81%AF%E3%80%81%E4%BA%88%E7%AE%97%E3%81%A8%E3%80%81%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%81%AE%E9%81%8B%E7%94%A8%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6%E5%BF%85%E8%A6%81%E3%81%A8%E3%81%99%E3%82%8B%E5%88%86%E6%9E%90%E6%83%85%E5%A0%B1%E3%81%AE%E9%87%8F%E3%81%AE%E3%83%90%E3%83%A9%E3%83%B3%E3%82%B9%E3%82%92%E3%81%A8%E3%81%A3%E3%81%A6%E8%A8%AD%E5%AE%9A%E3%81%97%E3%81%BE%E3%81%99%E3%80%82) [[57]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=%E3%81%93%E3%81%93%E3%81%A7%E4%BD%BF%E7%94%A8%E3%81%99%E3%82%8B%E5%88%97%E5%90%8D%E3%81%AF%E3%80%81%E4%BE%8B%E3%81%A8%E3%81%97%E3%81%A6%E7%A4%BA%E3%81%97%E3%81%A6%E3%81%84%E3%82%8B%E3%81%A0%E3%81%91%E3%81%A7%E3%81%99%E3%80%82%20%E3%81%BB%E3%81%A8%E3%82%93%E3%81%A9%E3%81%AE%E5%A0%B4%E5%90%88%E3%80%81%E3%81%94%E4%BD%BF%E7%94%A8%E3%81%AE%E3%83%AD%E3%82%B0%E3%81%AE%E5%88%97%E5%90%8D%E3%81%AF%E7%95%B0%E3%81%AA%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82) Azure Monitor で仮想マシンを監視する: データの収集 - Azure Monitor | Microsoft Learn

<https://learn.microsoft.com/ja-jp/azure/azure-monitor/vm/monitor-virtual-machine-data-collection>

[[7]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine#:~:text=,and%20dependencies%20with%20other%20services) [[56]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine#:~:text=similar%20to%20the%20operating%20system,be%20monitored%20by%20Application%20insights) Monitor virtual machines with Azure Monitor - Azure Monitor | Microsoft Learn

<https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine>

[[14]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-log-text#:~:text=Many%20applications%20and%20services%20on,Custom%20Text%20Logs%20data%20source) [[15]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-log-text#:~:text=Setting%20Description%20File%20pattern%20Identifies,above%20the%20file%20name%20only) [[16]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-log-text#:~:text=Table%20name%20Name%20of%20the,described%20in%20%2010%20below) [[17]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-log-text#:~:text=table%20must%20already%20exist,records%20or%20to%20format%20the) [[18]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-log-text#:~:text=The%20file%20that%20Azure%20Monitor,must%20meet%20the%20following%20requirements) [[19]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-log-text#:~:text=In%20addition%20to%20the%20prerequisites,and%20rocky8%20are%20not%20supported) Collect text file from virtual machine with Azure Monitor - Azure Monitor | Microsoft Learn

<https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-log-text>

[[25]](https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/best-practices-alerts#:~:text=,with%20a%20variety%20of%20systems) [[26]](https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/best-practices-alerts#:~:text=configuring%20log%20search%20alerts%2C%20keep,a%20large%20number%20of%20resources) [[27]](https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/best-practices-alerts#:~:text=Recommendation%20Benefit%20Keep%20in%20mind,Some) [[37]](https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/best-practices-alerts#:~:text=Keep%20in%20mind%20that%20activity,mind%20that%20the%20rule%20can) [[38]](https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/best-practices-alerts#:~:text=health%20alerts%20are%20free%20of,mind%20that%20the%20rule%20can) Best practices for Azure Monitor alerts - Azure Monitor | Microsoft Learn

<https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/best-practices-alerts>

[[29]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Connection%20Manager) [[30]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Port%20monitoring%20verifies%20that%20a,port%20monitoring%20are%20described%20here) [[31]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Monitor%20a%20service%20or%20daemon) [[32]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=error%20%60Event%20%5C,Windows%20error%20events%20by%20source) [[33]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Sample%20log%20queries%3A%20Syslog%20events) [[35]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Collect%20IIS%20logs) [[36]](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection#:~:text=Sample%20log%20queries) Monitor virtual machines with Azure Monitor: Collect data - Azure Monitor | Microsoft Learn

<https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection>

[[39]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/alerts-log-webhook#:~:text=%E3%83%AD%E3%82%B0%E6%A4%9C%E7%B4%A2%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%20%E3%83%AB%E3%83%BC%E3%83%AB%E3%81%A7%20Webhook%20%E3%82%A2%E3%82%AF%E3%82%B7%E3%83%A7%E3%83%B3%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%80%811%20%E3%81%A4%E3%81%AE,%E3%82%92%E4%BD%BF%E7%94%A8%E3%81%99%E3%82%8B%E3%82%88%E3%81%86%E3%81%AB%E3%82%A2%E3%82%AF%E3%82%B7%E3%83%A7%E3%83%B3%20%E3%82%B0%E3%83%AB%E3%83%BC%E3%83%97%E3%82%92%E6%A7%8B%E6%88%90%20%E5%A0%B4%E5%90%88%E3%81%AB%E4%BD%BF%E7%94%A8%E3%81%A7%E3%81%8D%E3%82%8B%E3%83%97%E3%83%AD%E3%83%91%E3%83%86%E3%82%A3%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6%E8%AA%AC%E6%98%8E%E3%80%82%20%E5%91%BC%E3%81%B3%E5%87%BA%E3%81%95%E3%82%8C%E3%82%8B%E3%82%B5%E3%83%BC%E3%83%93%E3%82%B9%E3%81%AF%E3%80%81Webhook%20%E3%82%92%E3%82%B5%E3%83%9D%E3%83%BC%E3%83%88%E3%81%97%E3%80%81%E5%8F%97%E4%BF%A1%E3%81%97%E3%81%9F%E3%83%9A%E3%82%A4%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AE%E4%BD%BF%E7%94%A8%E6%96%B9%E6%B3%95%E3%82%92%E6%8A%8A%E6%8F%A1%E3%81%97%E3%81%A6%E3%81%84%E3%82%8B%E5%BF%85%E8%A6%81%E3%81%8C%E3%81%82%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82) [[40]](https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/alerts-log-webhook#:~:text=%E3%82%92%E3%82%B5%E3%83%9D%E3%83%BC%E3%83%88%E3%81%97%E3%80%81%E5%8F%97%E4%BF%A1%E3%81%97%E3%81%9F%E3%83%9A%E3%82%A4%E3%83%AD%E3%83%BC%E3%83%89%E3%81%AE%E4%BD%BF%E7%94%A8%E6%96%B9%E6%B3%95%E3%82%92%E6%8A%8A%E6%8F%A1%E3%81%97%E3%81%A6%E3%81%84%E3%82%8B%E5%BF%85%E8%A6%81%E3%81%8C%E3%81%82%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82) Webhook アクションを使用した Azure Monitor ログ検索アラートのサンプル ペイロード - Azure Monitor | Microsoft Learn

<https://learn.microsoft.com/ja-jp/azure/azure-monitor/alerts/alerts-log-webhook>

[[41]](https://ayuina.github.io/ainaba-csa-blog/azure-functions-secure-webhook/#:~:text=%E3%81%93%E3%82%8C%E3%81%8C%20%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%81%A7%E4%BF%9D%E8%AD%B7%E3%81%95%E3%82%8C%E3%81%9F%20Webhook%20,AD%20%E8%AA%8D%E8%A8%BC%E3%81%A7%E4%BF%9D%E8%AD%B7%E3%81%95%E3%82%8C%E3%81%9F%20Azure%20Functions%20%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%A6%E3%80%81%E3%82%A2%E3%82%AF%E3%82%B7%E3%83%A7%E3%83%B3%E3%82%B0%E3%83%AB%E3%83%BC%E3%83%97%E3%81%8B%E3%82%89%E5%91%BC%E3%81%B3%E5%87%BA%E3%81%9B%E3%82%8B%E3%81%8B%E8%A9%A6%E3%81%97%E3%81%A6%E3%81%BF%E3%81%BE%E3%81%97%E3%81%9F%E3%80%82) [[44]](https://ayuina.github.io/ainaba-csa-blog/azure-functions-secure-webhook/#:~:text=Azure%20AD%20%E8%AA%8D%E8%A8%BC%E3%81%99%E3%82%8B%20Azure%20Functions,App%20%E3%82%92%E4%BD%9C%E6%88%90%E3%81%99%E3%82%8B) [[45]](https://ayuina.github.io/ainaba-csa-blog/azure-functions-secure-webhook/#:~:text=%E3%81%BE%E3%81%9A%E3%81%AF%20WebHook%20%E3%82%92%E5%8F%97%E3%81%91%E3%82%8B%E3%81%9F%E3%82%81%E3%81%AE%20HttpTrigger%20%E3%81%A7%E8%B5%B7%E5%8B%95%E3%81%99%E3%82%8B,Function%20%E3%82%92%E4%BD%9C%E6%88%90%E3%81%97%E3%81%BE%E3%81%99%E3%80%82%20%E3%81%93%E3%81%93%E3%81%AF%E6%9C%AC%E9%A1%8C%E3%81%A7%E3%81%AF%E3%81%AA%E3%81%84%E3%81%AE%E3%81%A7%E5%8B%95%E4%BD%9C%E7%A2%BA%E8%AA%8D%E3%81%8C%E5%87%BA%E6%9D%A5%E3%82%8B%E7%A8%8B%E5%BA%A6%E3%81%AE%E4%B8%8B%E8%A8%98%E3%81%AE%E6%A7%98%E3%81%AA%E3%82%B3%E3%83%BC%E3%83%89%E3%81%A7%E4%BD%9C%E3%81%A3%E3%81%A6%E3%81%8A%E3%81%91%E3%81%B0%E8%89%AF%E3%81%84%E3%81%A7%E3%81%97%E3%82%87%E3%81%86%E3%80%82) Azure Function で作る Azure Monitor アクショングループの Secure な Webhook

<https://ayuina.github.io/ainaba-csa-blog/azure-functions-secure-webhook/>

[[46]](https://stackoverflow.com/questions/77095845/azure-function-app-to-receive-azure-monitor-alert-and-post-to-slack-webhook#:~:text=try%20,orElse) [[47]](https://stackoverflow.com/questions/77095845/azure-function-app-to-receive-azure-monitor-alert-and-post-to-slack-webhook#:~:text=String%20slackWebhookUrl%20%3D%20System.getenv%28,slackMessage) java - Azure Function app to receive Azure Monitor Alert and post to Slack webhook - Stack Overflow

<https://stackoverflow.com/questions/77095845/azure-function-app-to-receive-azure-monitor-alert-and-post-to-slack-webhook>

[[48]](https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-payload-samples#:~:text=Sample%20alert%20payloads%20,This%20helps%20validate%20the) Sample alert payloads - Azure Monitor - Microsoft Learn

<https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-payload-samples>

[[49]](https://learn.microsoft.com/en-us/azure/azure-monitor/data-collection/data-collection-rule-overview#:~:text=Legacy%20method%20DCR%20method%20Description,It%20replaces%20the) Data collection rules in Azure Monitor - Azure Monitor | Microsoft Learn

<https://learn.microsoft.com/en-us/azure/azure-monitor/data-collection/data-collection-rule-overview>