# HP ベストプラクティス

ソフトウェアバージョン: 2.00

## エンドツーエンドのサービス監視とイベント管理

ドキュメントリリース日 : 2013年6月（英語版）

# ご注意

## 保証

HP製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載は、追加保証を提供するものではありません。ここに含まれる技術的、編集上の誤り、または欠如について、HPはいかなる責任も負いません。

ここに記載する情報は、予告なしに変更されることがあります。

## 権利の制限

機密性のあるコンピューターソフトウェアです。これらを所有、使用、または複製するには、HPからの有効な使用許諾が必要です。商用コンピューターソフトウェア、コンピューターソフトウェアに関する文書類、および商用アイテムの技術データは、FAR12.211および12.212の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

## 著作権について



## 商標について

Adobe®は、Adobe Systems Incorporated (アドビシステムズ社) の登録商標です。

Microsoft®およびWindows®は、米国におけるMicrosoft Corporationの登録商標です。

UNIX®は、The Open Groupの登録商標です。

# ドキュメントの更新情報

このマニュアルの表紙には、以下の識別情報が記載されています。

- ソフトウェアバージョンの番号は、ソフトウェアのバージョンを示します。
- ドキュメントリリース日は、ドキュメントが更新されるたびに変更されます。
- ソフトウェアリリース日は、このバージョンのソフトウェアのリリース期日を表します。

更新状況、およびご使用のドキュメントが最新版かどうかは、次のサイトで確認できます。

**http://support.openview.hp.com/selfsolve/manuals**

このサイトを利用するには、HP Passportへの登録とサインインが必要です。HP Passport IDの登録は、次のWebサイトから行なうことができます。

**http://h20229.www2.hp.com/passport-registration.html (英語サイト)**

または、HP Passport のログインページの [**New users - please register**] リンクをクリックします。

適切な製品サポートサービスをお申し込みいただいたお客様は、更新版または最新版をご入手いただけます。詳細は、HPの営業担当にお問い合わせください。

# サポート

HPソフトウェアサポートオンラインWebサイトを参照してください。

**http://support.openview.hp.com**

このサイトでは、HPのお客様窓口のほか、HPソフトウェアが提供する製品、サービス、およびサポートに関する詳細情報をご覧いただけます。

HPソフトウェアオンラインではセルフソルブ機能を提供しています。お客様のビジネスを管理するのに必要な対話型の技術サポートツールに、素早く効率的にアクセスできます。HPソフトウェアサポートのWebサイトでは、次のようなことができます。

- 関心のあるナレッジドキュメントの検索
- サポートケースの登録とエンハンスメント要求のトラッキング
- ソフトウェアパッチのダウンロード
- サポート契約の管理
- HPサポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

一部のサポートを除き、サポートのご利用には、HP Passportユーザーとしてご登録の上、サインインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。HP Passport IDを登録するには、次のWebサイトにアクセスしてください。

**http://h20229.www2.hp.com/passport-registration.html (英語サイト)**

アクセスレベルの詳細については、次のWebサイトをご覧ください。

**http://support.openview.hp.com/access_level.jsp**

# 目次

# このガイドについて

本書は、エンドツーエンドのサービス監視とイベント管理に関するベストプラクティスガイドです。本書では、ITの可用性とパフォーマンスの向上を目的に、高度なエンドツーエンドの監視ソリューションとイベント管理プロセスを実装する上で参考になるベストプラクティスを紹介します。また、使用する製品と統合ソリューションの概要も併せて説明します。各製品の詳細な内容については、各項を参照してください。

**本章の内容**



# 本ガイドの構成

本ガイドは、次のように構成されています。

**第1部: IT環境でのエンドツーエンドのサービス監視**

サービスプロバイダーとサービスコンシューマーが合意したサービスレベルを達成できるように、エンドツーエンドのサービス監視をデプロイおよび実装する方法を説明します。

**第2部: イベント管理**

イベント管理プロセスの実装に関するベストプラクティスを説明します。

# 本ガイドの対象読者

本ガイドは、エンドツーエンドのサービス監視の計画と実装に加えて、イベント管理プロセスの実施に関するガイドラインと推奨事項を紹介します。

本書は、次の方を対象に作成されています。

- カスタマー
- HP社内の現場担当者
- パートナー
- エンドツーエンドのサービス監視ソリューションの計画と実装を担当する方

本書には、他のベストプラクティスガイドと重複した内容が含まれている場合があります。

# その他のオンラインリソース

**トラブルシューティング&ナレッジベース**: HPソフトウェアサポートWebサイトのトラブルシューティングページです。セルフソルブのナレッジベースを検索できます。[**ヘルプ**] > [**トラブルシューティング&ナレッジベース**] を選択してください。WebサイトのURLは、http://support.openview.hp.com/troubleshooting.jspです。

**HPソフトウェアサポート**: HPソフトウェアサポートWebサイトにアクセスします。このサイトでは、セルフソルブのナレッジベースを参照できます。また、ユーザーディスカッションフォーラムへの投稿と検索、サポート依頼の送信、パッチと最新ドキュメントのダウンロードなども実行できます。[**ヘルプ**] > [**HPソフトウェアサポート**] を選択してください。WebサイトのURLは、http://support.openview.hp.comです。

一部を除き、サポートのご利用にはHP Passportユーザーとしてご登録の上、サインインしていただく必要があります。また、多くのサポートのご利用にはサポート契約が必要です。

アクセスレベルの詳細については、次のサイトを参照してください。
http://support.openview.hp.com/access_level.jsp

HP Passportユーザーの登録は、次のサイトを参照してください。
http://h20229.www2.hp.com/passport-registration.html (英語サイト)

**HPソフトウェアWebサイト**: HPソフトウェアWebサイトにアクセスします。このサイトには、新しいソフトウェアリリース、セミナー、見本市、カスタマーサポートなど、HPソフトウェア製品の最新情報が掲載されています。[**ヘルプ**] > [**HPソフトウェアWebサイト**] を選択してください。WebサイトのURLは、http://support.openview.hp.com/です。

**HP Software Solutions Now**: HPSW Solution and Integration Portal Webサイトにアクセスします。HP製品とITILプロセスの統合ソリューションを含めたHP製品ソリューションの中から、ニーズに合ったソリューションを選択できます。WebサイトのURLは、http://support.openview.hp.com/sc/solutions/index.jsp (英語サイト) です。

# 第I部: IT環境でのエンドツーエンドのサービス監視

# 第1章: はじめに

**本章の内容**

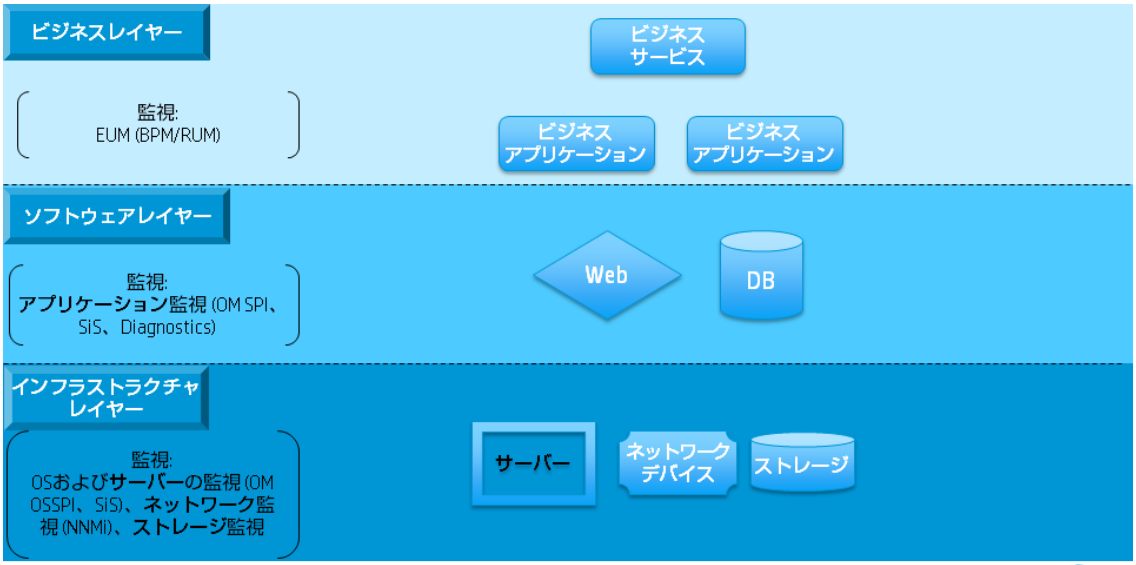


# 概要

**第1部: IT環境でのエンドツーエンドのサービス監視**では、サービスプロバイダーとサービスコンシューマーが同意したサービスレベルを達成することを目的に、エンドツーエンドのサービス監視を行うスマートソリューションの展開と実装に関するベストプラクティスを紹介します。各ユーザー環境のニーズに合わせて、ベストプラクティスで提案するソリューション全体、各種製品の組み合わせ、単体の製品を適宜活用してください。

**注:** 包括的なエンドツーエンドのサービス監視は、イベント管理プロセスで効果を発揮し、特に検出フェーズと相関フェーズで役立ちます。

次の図は、ITサービス環境の例を示しています。この環境には、現在の複雑なビジネスサービス、相互に関係する複数のインフラストラクチャとネットワークコンポーネント、さらにこのような基盤で稼働するソフトウェアが存在します。このようなサービスを提供する組織では、コンポーネントのステータスとパフォーマンスを監視および評価する機能が非常に大きなメリットをもたらします。



一般的なビジネスサービスは、図で示すように3つのレイヤーで構成されます。各レイヤーは個別に監視することができ、ステータスとパフォーマンスに関する情報を取得できます。ここでのベストプラクティスは、すべての監視を実装し、取得したデータを集約して中央コンソールに表示することです。これにより、そのデータを元にしたレポート作成、データ処理、データ分析が可能になります。

中央コンソールには、BSM OMiを使用します。OMiは、Service and Operations Bridge (SaOB) の一部として実装されます (詳細については、本書の「イベント管理」( 34ページ)を参照してください)。

- **ビジネスレイヤー:** ビジネスレイヤーでは、アプリケーション自体を監視します。この監視には、主にエンドユーザー監視 (EUM) を使用します。このレイヤーには基幹ビジネス (LOB)、ビジネスサービス、複合ビジネスアプリケーションが含まれます。たとえば、電子メールサービスはビジネスサービスであり、Microsoft Exchange Suiteはビジネスアプリケーションです。

- **ソフトウェアレイヤー:** ソフトウェアレイヤーでは、サーバーにインストールされていて、アプリケーションにサービスを提供するソフトウェアコンポーネントを監視します。ソフトウェアレイヤーには、ビジネスレイヤーをインフラストラクチャレイヤーに接続する役割があり、すべてのソフトウェアコンポーネントが含まれています。たとえば、クライアントアクセスサーバー上で稼働するIISソフトウェアはWebアプリケーションであり、Microsoft Exchangeメールボックスサーバーで稼働するMicrosoft SQLソフトウェアはデータベースです。

- **インフラストラクチャレイヤー:** インフラストラクチャレイヤーでは、ソフトウェアレイヤーが使用するインフラストラクチャを監視します。これには、サーバー、ネットワーク、その他インフラストラクチャサービスが含まれます。

  - **ネットワーク監視:** ネットワーク監視は、ネットワーキングサービスをIT環境に提供するITインフラストラクチャサービスの主要要素です。たとえば、ネットワークスイッチやルーターなどが含まれます。現在のビジネスサービスは、ほとんどの場合、稼働にネットワークインフラストラクチャが必要になります。安定した通信環境を実現するには、ネットワーク機器や設定を注意深く監視することが必要です。

各レイヤーの説明は、次の4つの項に分けて行います。

- **概要:** 監視の対象と、監視する理由を説明します。
- **ツール:** このタイプの監視に使用するツールを説明します。
- **インストールと構成:** 監視ソリューションを使用するためのアクションフローであり、ツールと監視の特定と設定を行います。
- **推奨事項:** 監視ソリューションを効果的に活用するためのベストプラクティスを紹介します。

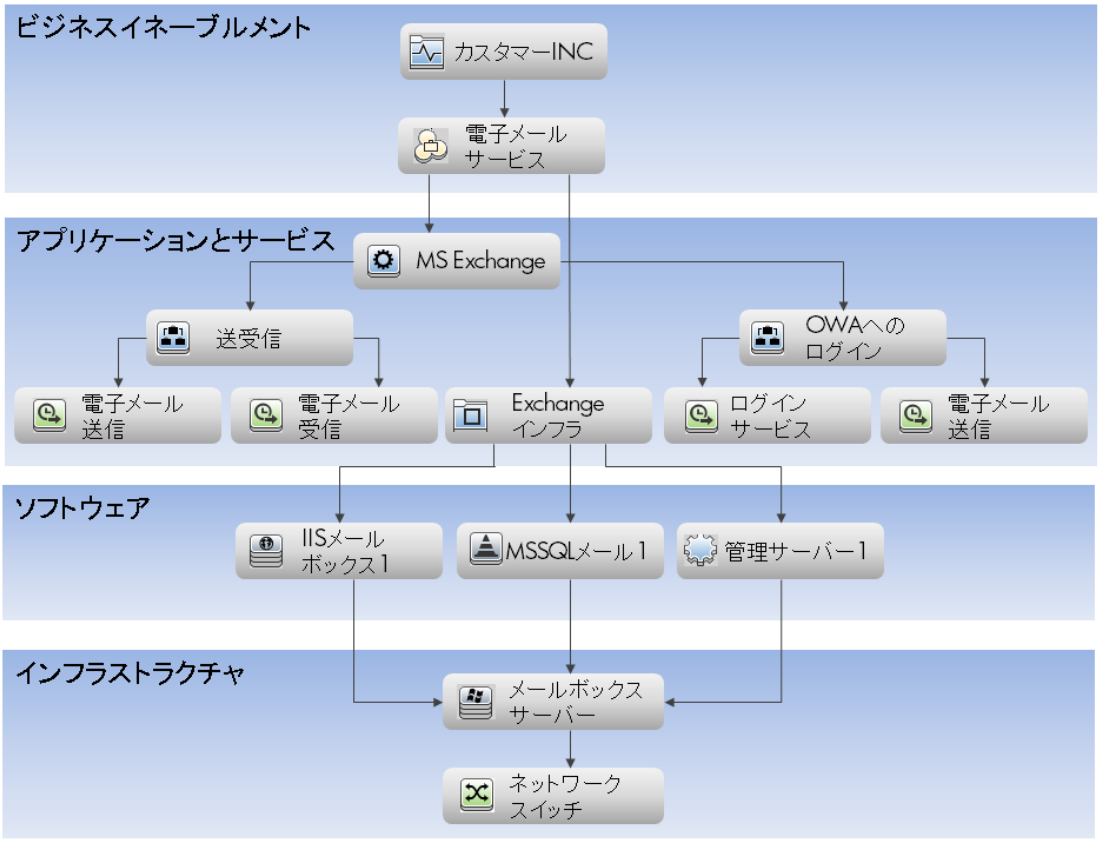
# ユースケース

IT組織は、多彩な複合サービスをビジネスに提供しています。合意したサービスレベルを達成するためには、ITはサービスの可用性とパフォーマンスを監視し、ビジネスに影響を及ぼす可能性のあるエラーを事前に特定して対処する必要があります。

実装環境を監視する方法をわかりやすく説明するために、一般的なITサービスである電子メールサービスを例として取り上げ、本ガイド全体で使用しています。エンタープライズ環境での電子メールサービスは、複数の階層と複数のコンポーネントで構成され、地理的に離れた複数のサイトで提供されます。このサービスはMicrosoft Exchange (TM) Serverを基盤とし、複数のコンポーネント [構成ア

イテム(CI)] で構成されます。本書では、電子メールサービスのさまざまな側面について考察し、各コンポーネントに適用する監視ソリューションについて説明します。

次の図は、電子メールサービス環境に存在するCIを示しています。




**構成アイテム**

| アイコン | 説明 |
|---|---|
|  | ビジネス機能 |
|  | ビジネスサービス |
|  | ビジネスアプリケーション |
|  | ビジネストランザクションフロー |
|  | ビジネストランザクション |
|  | 構成アイテム(CI)群 |

| アイコン | 説明 |
|---|---|
|  | IIS Webサーバー |
|  | SQLサーバー |
|  | 実行ソフトウェア |
|  | Windows (コンピューター) |
|  | スイッチ |

この例で使用する電子メールサービスのレイヤーは、次の4つの層で構成されています。

- **ビジネスイネーブルメントレイヤー:** ビジネス要素で構成されます。
- **アプリケーションおよびサービスレイヤー:** このレイヤーでは、エンドユーザー監視を使用してアプリケーションを監視します。電子メールサービスの例では、ユーザーが電子メールを送受信する機能や、Outlook Web Accessのグラフィカルユーザーインタフェースを監視します。アプリケーションの重要な機能が監視対象になります。
- **ソフトウェアレイヤー:** ソフトウェアレイヤーでは、サーバーにインストールされていて、アプリケーションにサービスを提供するソフトウェアコンポーネントを監視します。上記の例で監視対象となるのは、Microsoft Exchangeアプリケーション、IIS、データベースソフトウェアです。
- **インフラストラクチャレイヤー:** インフラストラクチャレイヤーでは、インフラストラクチャを監視します。これには、サーバー、ネットワーク、その他Microsoft Exchangeアプリケーションのインフラストラクチャサービスが含まれます。上記の例では、サーバーのファイルシステム、メモリ、CPU、ログファイルなど、サーバーでソフトウェアが正常稼働する条件として、安定稼働が必要になる要素を指します。また、ネットワークトラフィックも監視の対象です。上記の例では、Exchangeメールボックスサーバーに接続されているネットワークスイッチの可用性とパフォーマンスを監視します。

# 第2章: ビジネスレイヤーの監視 - EUM

**本章の内容**



## 概要

IT環境でのエンドツーエンドのサービス監視は、エンドユーザーの視点、つまりエンドユーザー監視(End-User Monitoring)を使用してビジネスレイヤーを監視します。

エンドユーザーエクスペリエンスの監視は、EUMの主な目的です。これにより、アプリケーションの最新ステータス(使用可能/使用不能)とパフォーマンス情報を取得し、発生した問題を報告するレポートを作成します。

EUM監視を行うには、まず最初に重要度の高いビジネスプロセスと、プロセス内で監視の対象となるステップのリストを作成します。たとえば、電子メールアプリケーションのEUMでは、電子メールサービスで重要度が高いプロセス(電子メールの送信、電子メールの受信、Outlook Web Accessアプリケーションのメールボックスへのログオンなど)が使用可能な状態であることと、合意したサービスレベルのパフォーマンスが達成されていることを確認します。

## ツール

**HP Business Service Management (BSM)** は、統合型管理レイヤーソリューションのポートフォリオで構成されるアプリケーションスイートであり、HP製品とアプリケーションをさまざまに組み合わせて提供されます。

BSMスイートには、2つのモジュールが含まれています。1つはサービス監視を行うモジュールであり、Application Performance Management (APM) と呼ばれます。もう1つはイベント管理を行うモジュールであり、Operations Management (OMi) と呼ばれます。モジュールの詳細については、本書の「イベント管理」(34ページ)を参照してください。

APMモジュールは、RUMとBPMという2つの製品で構成され、いずれもエンドユーザーエクスペリエンスを監視します。

- **HP Business Process Monitor (BPM):** アクティブ方式でロケーションベースの監視ソリューションを使用する総合的なユーザー監視です。ビジネスプロセスのシミュレーションをベースに一貫した方法で予測を行い、パフォーマンスと可用性の問題を未然に検出します。

  たとえば、BPM総合監視で電子メールの送受信を監視する場合、Exchangeサーバーからの受信中に処理速度の低下を検出し、電子メールサービスで発生するパフォーマンスの問題を特定することができます。

- **HP Real User Monitor (RUM):** RUMは、実ユーザーがアプリケーション内で生成したネットワークトラフィックを監視します。RUM製品は、ネットワークトラフィックをパッシブ方式でリッスンすることによ

り、すべてのロケーションで作業するすべてのユーザーを対象に、アプリケーションのパフォーマンスと可用性を監視します。

たとえば、RUMで電子メールの送受信アクションを監視する場合、全体的な電子メールサービスに問題がなくても、特定のロケーションにある支社で電子メールアカウントへのアクセス速度が低下している問題を検出できます。さらに、管理部門で発生しているネットワークの問題が、パフォーマンスに影響していることを特定できます。

BPMとRUMには、次のような特徴があります。

- **HP Business Process Monitor (BPM)**
  - 作成しておいた監視スクリプトをBPMデータコレクターで実行することによって実ユーザーをシミュレーションし、アプリケーションで事前設定したアクションを実行することによってアプリケーションを24時間365日体制で監視します。
  - 長期的なトレンドレポートを作成します。BSMの監視指標の収集機能を使用し、アプリケーションの動作を把握します。
  - ビジネスアプリケーションをプロアクティブに監視します。総合トランザクション監視を使って、ユーザーが日々実行するアクションの中で重要度の高いものを監視することにより、実際に影響が発生する前に問題を特定します。
  - レポートと指標データ収集により、パフォーマンスのベースラインを設定します。
  - 詳細な診断ツールにより、スクリプトのテスト、エンドユーザーの測定などを行います。
  - 事前設定したクリティカルなトランザクションをベースに、サービスレベルアグリーメント (SLA) を簡単に管理および定義します。

    BPMにはデフォルトで主要業績評価指標 (KPI) が用意されており、重要度の高いアクションをトランザクション内で設定できます。SLAからこのアクションを取得することにより、SLAユースケースで測定を行います。
  - 事前設定した測定と管理監視環境 (ロケーション、BPM、スクリプトの管理など) に基づいて、可用性イベントをトリガーします。各アラートには優先度が割り当てられています。

    この処理にはHP Software VuGenスクリプティングテクノロジが使用され、開発グループとオペレーショングループ間のコラボレーションを可能にします (HP Performance CenterおよびUFTと同じスクリプトとスクリプティングツールを使用します)。
- **HP Real User Monitor (RUM)**
  - パッシブ方式による監視は対象となるアプリケーションに影響を与えないので、法規制上の理由からアクティブ方式による監視が適切でないアプリケーションにもRUMを利用できます。
  - RUMは、ポートミラーリングによって実ユーザーデータを監視します。ITオペレーターは、各アプリケーション機能のパフォーマンスをエンドユーザーの視点で確認でき、監視対象がデータセンターや一部のロケーションに限定されることもありません。

- スクリプトの作成が不要なので、デプロイメントやメンテナンス用のリソースを消費しません。
- スクリプトの対象だけに限らず、アプリケーションの使用状況とパフォーマンスを完全に把握できます。BPMとは異なり、RUMは実ユーザーが実行するすべてのアクションを個々に監視します。
- ユーザーが存在する地理的ロケーションで実ユーザーのネットワークトラフィックを監視することにより、ユーザーの地理的な分散状況と、エンドユーザーエクスペリエンスへの影響を把握します。
- 重要度の高いユーザーのパフォーマンスを追跡します。この機能は特に、取引環境で威力を発揮します。
- ユーザー分析では、アプリケーションの使用方法を詳細に把握します。

複合アプリケーションやトランザクションベースの監視 (HP Diagnostics/TransactionVision) ではさらに複雑な監視を実行できますが、これについては次回のベストプラクティスガイドで取り上げる予定です。

# インストールと構成

**論理レイヤーの監視をインストールおよび構成するには、次の手順を実行します。**

- 最新版のBSMソフトウェアをインストールします。詳細については、HPソフトウェア製品マニュアルWebサイトの『HP BSMインストールガイド』を参照してください。
- BSMのインストールでは、EUMモデルを選択し、実行に必要なライセンスが取得済みであることを確認してください。
- 「推奨事項」( 18ページ)を参考に、データコレクターのデプロイメントを計画します。
- BPMとRUMの関連コンポーネント (プローブとエンジン) をインストールし、BSMに接続します。詳細については、HPソフトウェア製品マニュアルWebサイトの『Business Process Monitor Deployment Guide』または『Real User Monitor Installation and Upgrade Guide』を参照してください。
- 推奨される手順: EUM監視プロジェクト (その他の監視プロジェクトを含む) を開始するにあたり、アプリケーションオーナーと一緒に、監視対象に含めるアプリケーションをドキュメントにまとめます。

  監視対象アプリケーションでは、次の属性を定義する必要があります。

  - アプリケーションの構造 (「構成アイテム」( 13ページ)の図を参照)
  - 監視するビジネスプロセスとステップ
  - プロセスとステップに適用するしきい値
  - アラート
  - 連絡先 (アプリケーション構造全体のメンテナンスを担当するオーナーと、スクリプト作成を担当するオーナーを明確に指定)

- 反復回数 (監視の実行予定回数)
- 定期的なダウンタイム (たとえば、アプリケーションの実行時間を08:00～17:00に限定)
- 主要業績評価指標 (KPI) の設定。詳細については、HPソフトウェア製品マニュアルWebサイトに掲載されている『HP BSM ユーザ・ガイド』または『BSM アプリケーション管理ガイド』の「サービス状況」の項を参照してください。
- 監視スクリプトで指定するアプリケーション情報 (URL、ユーザー名、ビジネスプロセスステップなどのアプリケーション情報)

**注:** この情報を早めに文書にまとめておくと、実装フェーズではその文書を元に監視を作成できるので、大幅な時間の節約になります。

| App Name | Monitor | Thresholds | Alerts | Contects | Iteration times | downtimes | KPI config | App info |
|---|---|---|---|---|---|---|---|---|
| MS exchange OWA | Login to OWA | OK-5 sec,minor-8 sec,critical-15 sec,outlier-60 sec | Send email to application manager if the status is critical | John doe | Run every 5min | Every Friday at 15:00- 16:00 - do not monitor | Performance - worst status, availability - worst status | http://owa.com |
| App B | x | x | x | x | x | x | x | x |

# 推奨事項

本項では、ビジネスレイヤーでエンドツーエンドの監視を実装する際に、推奨される手順と作業を紹介します。ここで説明する内容はベストプラクティスであり、必ず行わなければならない手順ではありません。

**本項の内容**



# 監視

アプリケーションを監視する場合は一般的にBPMとRUMの両方を使用してください。この2つは相互に補完的な機能を備えているので、アプリケーションの可用性とパフォーマンスを広い視点から捉えることができます。

- デプロイメントのドキュメントを参考に、監視スクリプトを作成し、設定を行います。
- 適切なデータコレクターに監視を適用して起動すると、事前に設定しておいた実行回数に基づいて実行されます。
- 『BSM ユーザ・ガイド』のEUMの項を参考に、EUM監視で使用するアラートを作成します。
- 『BSM Platform Administration』ガイドを参考に、定期的なダウンタイムを設定して適用します (必要な場合)。ダウンタイムの間、アプリケーションの監視は行われません。

- RUMは、実ユーザーのトラフィック監視に基づいて、さまざまな種類のレポートを作成し、ユーザーとネットワークの視点から有効なデータを提供します。たとえば、実際のユーザーエクスペリエンス、地理的な分散状況、ネットワークがアプリケーションの可用性とパフォーマンスに与える影響を把握できます。

- BPMは、中立的な視点からアプリケーションを総合的に監視するツールであり、アプリケーションの可用性とパフォーマンスに関するデータをリアルタイムで提供します。数個のユーザーとアクションを使ってアプリケーション内にある重要な機能の実際のステータスを取得し、トラブルシューティングに役立つ各種レポートを作成することにより、24時間365日体制での監視を可能にします。

  - 監視スクリプトに、重要なビジネスステップがトランザクションとして含まれていることを確認します。

    たとえば、電子メールの送受信を監視するスクリプトには、Exchangeサーバーへのログオン、電子メールの送信、電子メールの受信という3つのトランザクションが含まれます。このトランザクションをチェックすることにより、各アクションのステータスを明確に把握することができます。

  - 監視に使用するユーザーには**期限なしのパスワード**を割り当てます。これにより、ユーザーパスワードが期限切れになったことが原因でアラートが誤って報告される事態を回避できます。

- プロセスに関連するアプリケーション (Load Runner、サーバー、オペレーティングシステム、QTP) がすべてサポート対象バージョンであることを確認します。詳細については、サポートマトリックスを参照してください。

- BPM監視のスクリプトのメンテナンスについて、明確な手順を作成します。時間の経過に伴ってアプリケーションに変更が加えられることが多く、当初とは異なる動作になるケースが多いためです。ビジネスオーナーとアプリケーションオーナーとともに、この手順の担当者を明確に指定してください。

# デプロイメント

- 複数のデータセンターで監視を行う場合、BPM/RUMプローブのデプロイメントは、監視を実施しているデータセンター内で行う必要があります。エンタープライズカスタマーの場合、データセンターの地理的な場所にプローブを配置することをお勧めします。これにより、ユーザーエクスペリエンスの監視結果の精度が高くなり、ネットワークの問題がアプリケーションにどのような問題を与えているのか (またはネットワークに問題がない状態) を正確に特定できるようになります。また、作成されたレポートを参考に、問題が発生しやすいロケーションとその根本原因を特定し、アプリケーションの稼働状態を改善できます。

  また、HP Network Node Manager i (NNMi) ツールがある場合は、RUMとNNMi (BSM) を統合してください。この統合構成は、エンドユーザーエクスペリエンスに影響するネットワーク障害の根本原因を切り分けるときに威力を発揮します。この統合を構成する方法については、『NNMi—BSM Integration Guide version 9.22』を参照してください。

- EUM監視用にデータコレクターを配置する際には、アプリケーションを使用するユーザーが多数存在し、ネットワークやインフラストラクチャの使用など、そのエクスペリエンスが十分に反映されているロケーションを選択することをお薦めします。たとえば、BPMとRUMのデータコレクターの配置場所にお勧めなのは、多数の電子メールユーザーが存在するロケーションです。これにより、多数のユーザーのサービスとユーザーに影響を与える問題を監視できます。

BPM監視では、幅広い種類のプロトコルを監視できます。どのようなプロトコルを監視する必要があるか確認してください。

RUM監視には、汎用のTCPプロトコルトラフィックを監視し、さまざまなタイプのクライアントとサーバー間の接続に関するレポートを作成する機能があります。

# 設定

### アラート

- 無意味なアラートや大量のアラートが生成されるのを避けるため、トリガー1回で送信するアラートを1つに限定するか、特定の時間枠内で送信するアラートを1つに限定し、既知のエラーでトリガーが発生するたびにアラートを送信しないようにします (5分おきにアラート設定する場合など)。アラートの送信は、監視対象のアプリケーションの重要度が非常に高く、エラーが発生する度にエラーを確実に報告する必要のある場合や、監視の実行サイクルの時間の間隔が長い状況の場合に設定することをお勧めします。

  たとえば、ユーザーの本社から送信される電子メールをBPMで監視する場合、監視の頻度を1分に設定し、**エラーのトリガーごとに、30分に1回アラートを送信**する設定を行います。30分経過しても問題が解消されない場合には、新しいアラートを受信する必要がありますが、問題解決の担当者はエラーをすでに把握しているわけですから1分ごとにアラートを受信する必要はありません。

- BSMでは、実際のパフォーマンス指標からベースラインを計算できます。ベースラインを作成することにより、アプリケーションの通常稼働状態を把握できます。サイトの通常のパフォーマンスレベルを知ることによって、パフォーマンスに問題が発生したときに、単なる一時的な低下なのか、全体が大幅に低下しているのかを切り分けることができます。

  ベースラインを有効にすると、データサンプルから取得した実際のパフォーマンスデータに基づいて、平均応答時間と標準偏差がトランザクションとロケーションごとに計算されます。定期的に新しいサンプルが取得され、トランザクションの平均応答時間と標準偏差が更新されます。

  ベースラインに基づいてアプリケーションのトランザクションしきい値を設定する場合には、トランザクションのステータスを計算する方法として、平均トランザクション応答時間に適用する標準偏差の数を指定します。ベストプラクティスでは、デフォルト設定の使用をお勧めします。この設定では**正常稼働**のステータスに3つの標準偏差値、**問題**のステータスに4つの標準偏差値が指定されています。

# 第3章: ソフトウェアレイヤーの監視

**本章の内容**



# 概要

エンドツーエンドのサービス監視では、サーバー上で稼働するアプリケーションのソフトウェアコンポーネントの監視を行います。

サーバー上で稼働するアプリケーションコンポーネントの監視対象には、アプリケーションのサービス、プロセス、ログファイル、およびアプリケーションソフトウェアに関連するサーバー上のその他オブジェクトがあります。アプリケーション監視は、コンポーネントで発生した問題の根本原因や解決方法を特定する作業において、最初にドリルダウンする部分です。

たとえば、メールボックスアプリケーションのログファイルを監視し、ログに記録されているエラーを検索します。また、メールボックスサーバー上のデータベースや、Outlook Web Accessアプリケーションを稼働するクライアントアクセスサーバー上のIISサービスを監視することも可能です。

これ以外にも、Microsoft Exchangeアプリケーションのソフトウェアコンポーネントには、アプリケーションが正常稼働する上で重要な役割を果たすものが多数存在します。このようなコンポーネントを監視することで、すでに発生しているエラーを特定し、発生しそうなエラーの警告を事前に受信することができます。たとえば、電子メールのキューの長さが増えていることを示す警告がログファイルに記録されている場合、電子メールの送信で問題が発生する可能性があることを示しています。監視では、既存の問題の根本原因を特定することもできます。たとえば、メールボックスに接続できない場合には、関連するデータベースがダウンしていることが原因だとわかります。

# ツール

- **HP Operations Manager (HPOM)** は、インフラストラクチャコンポーネントを監視するツールです。HPOMには、監視エージェントを使って監視を行う機能と、エージェントレスのコンポーネントからメッセージを受信する機能があります。ソフトウェアの監視には、HPOMに付属のSmart Plug-in監視パッケージを使用することをお勧めします。パッケージでは監視のスクリプト、条件、ルールがまとめて定義されているので、各ソフトウェアパッケージに適した監視を実行できます。詳細については、「HP Operations Smart Plug-in」を参照してください。

  たとえば、Smart Plug-in (SPI) for Microsoft Exchangeをユーザー環境にデプロイでき、このSPIには、Exchangeサーバーを監視するパッケージが付属しています。SPI for Exchangeの詳細については、HPソフトウェア製品マニュアルWebサイトに掲載されている『SPI for the Microsoft Exchange Installation and Configuration Guide』を参照してください。

またHPOMでは、ユーザー定義の監視を使って他のアプリケーションコンポーネントを監視することができます。たとえば、ユーザー定義のログファイル監視を使用して、メールボックスサーバーのログファイルでエラーを検出します。

- **HP Diagnostics**ソフトウェアは、従来の環境、仮想環境、クラウド環境においてアプリケーショントランザクションの稼働状態を監視し、問題の特定と解決を短時間で行います。このツールを使用することでアプリケーションライフサイクル全体を通じたコラボレーションが可能になり、リリースするアプリケーションの品質をさらに高めることができます。HP Diagnosticsは、トランザクションを診断し、エンドユーザーからバックエンドにいたる詳細情報を取得します。運用移行前の環境と運用環境の両方で使用できる共通のツールセットであり、アプリケーションのボトルネックを迅速に特定して品質を向上します。

- **HP SiteScope**は、エージェントレスの監視ソリューションであり、分散したITインフラストラクチャの可用性とパフォーマンスを監視します。監視を管理し、事前定義の資格情報があるリモートサーバーにテンプレートとして配信できます。

  さらに、JDBC接続、ログファイル分析、SNMP監視などで使用するカスタム監視を設計およびデプロイできる監視機能も提供されています。

  たとえばSiteScopeでは、メールボックスサーバーで稼働するメールボックスサービスを監視できます。また、**送受信の監視**を使用して、サードパーティのメールアプリケーションから電子メールを送受信するExchangeの機能を監視することもできます。

  SiteScopeでは、Exchange監視パッケージも提供されています。

  詳細については、HPソフトウェア製品マニュアルWebサイトに掲載されているSiteScopeのドキュメントを参照してください。

# インストールと構成

**監視プロジェクトのデプロイメントと実装を計画する上で、ソフトウェアレイヤーをインストールおよび構成するには、次の手順を実行します。**

1. HP Operations Manager (HPOM) ソフトウェアの最新バージョンをインストールします。
2. HP SiteScopeソフトウェアの最新バージョンをインストールします。
3. HP Diagnosticsソフトウェアの最新バージョンをインストールします。
4. ユーザーIT環境のマッピングを行い、監視が必要なサーバーとアプリケーションをすべて特定します。この作業は、Universal Discoveryのような自動ツールを使用すると簡単になります。

   マッピングでは、次の内容を文書にまとめます。

   - アプリケーションの名前とIP
   - アプリケーションの管理者とその他の関係者

- アプリケーションサーバー
  - サーバー1: メールボックスサーバー
  - サーバー2: ハブサーバー
  - その他
- 各サーバーにインストールされているソフトウェア
  - サーバー1: MSSQL、Exchangeメールボックス、IIS
  - その他
- サーバーオペレーティングシステム(将来的に使用)
  - サーバー1: Microsoft Windows 2008R2
  - サーバー2: Linux
  - その他
- 各サーバーでのソフトウェア監視方法
  - サーバー1-MSSQL: データベースにHPOM SPI
  - サーバー1-IIS: SiS IIS監視を使用
  - その他
- 資格情報(ログファイルパス、アプリケーションパスなど)
  - サーバー1: データベースへのログオンにはユーザー名**SA**、パスワード**XYZ**を使用
  - その他
- 災害復旧/ロードバランサー(DR/LB)のデプロイメントへの参加

  監視を正しく実行するためには、サーバーがアクティブまたはパッシブのいずれの状態にあるかを把握することが重要です。詳細については、HPソフトウェア製品マニュアルWebサイトで、該当する製品と監視で提供されている監視ガイドを参照してください。
- ダウンタイムのルール(アプリケーションを非アクティブにする予定など)

5. マッピングが完了したら、各サーバー/ソフトウェアの監視にどのようなツールを使用するか検討します。

> **注:** サーバーの監視には、監視のニーズと製品の機能に基づいて、SiteScopeとHPOMの

両方を使用できます。

6. 構成とマッピングに基づいて、HPOM監視エージェントをデプロイします。
7. すべてのリモートサーバーをSiteScopeで設定します。

   詳細については、HPソフトウェア製品マニュアルWebサイトに掲載されているSiteScopeガイドを参照してください。
8. デプロイメントの規模が大きい場合は、HPOMポリシーとSiteScopeテンプレートを作成します。
9. すべての監視をデプロイします。
10. Diagnosticsのエージェントとコレクターをインストールします。
11. Diagnosticsのエージェントとコレクターのインストールが完了したら、エージェントのインストールディレクトリに格納されている各種構成ファイルを使用して、インストルメンテーションのカスタマイズとデータ収集設定を行います。構成ファイルのタイプについては、『Diagnostics バージョン 9.20 インストールおよび設定ガイド』の、特に「**Javaを監視するカスタムインストルメンテーション**」、「**.NETアプリケーション**」、「**Diagnostics サーバの詳細設定**」、「**.NETエージェント**」の各項を参照してください。

# 推奨事項

本項では、ソフトウェアレイヤーでエンドツーエンドの監視を実装する際に、推奨される手順と作業を紹介します。ここで説明する内容はベストプラクティスであり、必ず行わなければならない手順ではありません。

**本項の内容**



# 監視

アプリケーションコンポーネントの監視方法には、HPOM SPIとSiteScopeソリューションテンプレートのいずれか一方、または両方を使用する方法があり、ユーザーニーズに応じて選択できます。いずれの製品も、幅広いソフトウェアコンポーネントを事前設定したモニターを使って監視します。監視ソリューションを選択する際には、ユーザーが実行するアプリケーションに適しているかどうかを基準に判断してください。

キュー機能が必要なユースケースでは、HPOMエージェントベースの監視ソリューションが適している場合があります。HPOMエージェントは、稼働中にデータを収集してキューに格納します。

**注:** HPOMには、コンポーネントの詳細情報を取得する機能があるので、重要なソフトウェアコン

ポーネントの監視にはHPOMを使用することをお勧めします。一方、高速な監視ソリューションやエージェントレスな監視ソリューションが必要な場合、HPOMにはない監視機能が必要な場合、HPOMでは実装に非常に時間がかかる場合には、SiteScopeをお勧めします。

**注意：** アプリケーション監視用のSmart Plug-inは、アプリケーションのドリルダウン機能を備えた監視の複合セットです。エラー検出の効率を最大限に高め、不要なデータの検出を最小限に抑えるためには、SPIのドキュメントをよく読むことをお勧めします。

# デプロイメント

バックアップやDRPには、[**構成のダウンロード**] オプションを使用してHPOM構成を保存することをお勧めします。サーバーをバックアップする場合や別のサーバーを災害復旧 (DR) サーバーとして使用する場合は、作成した構成と監視をすべてバックアップファイルに保存することをお勧めします。

HPOMをMOM (Manager of Managers) として設定すれば、メッセージを1つのGUIに集中的にリダイレクトできます。これによって、HPOM監視環境での監視と管理がさらに効率化されます。オペレーションマネージャー全員が1つのHPOMサーバーにメッセージを転送し、相互に「会話」できる環境であれば、1つのMOMサーバーで複数のHPOMサーバーを監視する環境を管理できます。この構成は、HPOMで多数のノードを管理する大規模な環境や、HPOMサーバーが稼働する複数のデータセンターを1つのロケーションから管理する必要がある場合に適しています。

# 重要度のマッピング

監視の作成では、重要度を正しく定義することが非常に重要です。

監視イベントの重要度に応じて、NOCコンソール上のイベントを処理する順序が決まります。重要度の高いイベントの数が多すぎると、オペレーターは優先度を適切に判断できず、正しい順序で対処できなくなります。さらに、重要度に誤りがあると、重大なイベントへの対応が遅れてしまい、ビジネスに深刻な影響を及ぼしかねません。このような事態に陥らないように注意が必要です。

電子メールサービスの例で考えると、メールボックスプロセスのステータスに関するイベントには高い重要度を割り当てる必要があります。重要度を割り当てる作業では、デプロイメントタイプと、そのイベントを放置した場合に発生する影響を考慮してください。メッセージに適切な重要度を割り当てるには、ユースケースの分析も必要です。

# 第4章: インフラストラクチャレイヤーの監視

**本章の内容**



## 概要

インフラストラクチャレイヤー (サーバーとハードウェア) はソフトウェアレイヤー (サーバーやネットワークなどのインフラストラクチャサービス) が使用するレイヤーですが、これも監視が必要です。

第3章「ソフトウェアレイヤーの監視」( 21ページ) で説明したアプリケーションは、稼働のためにリソース (CPUサイクルとメモリ、ストレージリソース、ネットワークリソースなど) を使用します。

アプリケーションが十分な環境で稼働できるようには、リソースの消費状況を監視する必要があります。

たとえばメモリの場合、サーバーでメモリ不足が発生すると、Microsoft Exchangeアプリケーションなどそのサーバーにインストールされているすべてのアプリケーションが稼働を停止します。また、メールボックスデータベースで必要なディスク容量を確保できない場合にも、アプリケーションは停止します。

したがって、サーバーとインフラストラクチャサービスをサービスレベルアグリーメント (SLA) の条件どおりに稼働させることは、アプリケーションが正常稼働する上で非常に重要です。

## ツール

- **HP Operations Manager (HPOM)** は、インフラストラクチャコンポーネントを監視するツールでもあります。HPOMには、監視エージェントを使って監視を行う機能と、エージェントレスのコンポーネント (SiteScope) からメッセージを受信する機能があります。

  HPOMでは、サーバーとオペレーティングシステムの監視用にSmart Plug-in (SPI) がいくつか用意されています。

  たとえば、HPOMオペレーティングシステムSPIは、Exchangeクライアントアクセスサーバーの CPUを監視します。

  CPUの使用率が90%に達すると、Outlook Web Accessサービス経由でのメールボックスアクセスに遅延が発生することがあります。この場合、EUM監視でもOutlook Web Accessログオントランザクションでのパフォーマンス低下を検出できますが、オペレーティングシステムSPI監視を使用した方が効率的に原因を特定できます。

- **HP SiteScope**は、エージェントレスの監視ソリューションであり、分散したITインフラストラクチャの

可用性とパフォーマンスを監視します。監視を管理し、事前定義の資格情報があるリモートサーバーにテンプレートとして配信できます。

たとえば、Microsoft ExchangeメールボックスサーバーのメモリパフォーマンスをリモートのSiteScopeマシンで監視することによって、サーバーでメモリの過負荷が発生しているかどうかを確認することができます。メモリが過負荷状態になると、サーバーパフォーマンスが低下し、サーバー上で動作するアプリケーションのパフォーマンスもすべて低下します。さらに、サーバーが過負荷状態になり、ユーザーはメールボックスに接続できなくなります。

- **HP Network Node Managment i (NNMi)** は、ネットワークサービスの監視と管理を行います。ネットワーク監視の詳細については、「ネットワーク監視」(30ページ)を参照してください。
- **HP Storage Essentials (SE)** は、包括的なストレージリソース管理ソリューションです。詳細については、HP Live NetworkのStorage Essentialsを参照してください。

# インストールと構成

**インフラストラクチャレイヤーをインストールおよび構成するには、次の手順を実行します。**

- HP Operations Manager (HPOM) ソフトウェアの最新バージョンをインストールします。UNIX/Linuxサーバーで大規模な環境のインストールを行う場合には、HPOMのインストールをお勧めします。
- HP SiteScopeソフトウェアの最新バージョンをインストールし、必要な監視すべてにライセンスが用意されていることを確認し、デプロイメントを計画します。
- ソフトウェアレイヤーで作成したマッピングに基づいて、サーバーオペレーティングシステムを監視する方法を検討します。サーバーオペレーティングシステムのバージョンに適したオペレーティングシステムSPIの使用をお勧めします。
- オペレーティングシステムごとに、サポートされているHPOM監視エージェントのバージョンをデプロイします。詳細については、製品に付属するHPOMサポートマトリックスインタフェースを参照してください。
- リモートサーバーをSiteScopeで設定します。
- デプロイメントの規模が大きい場合は、HPOMポリシーとSiteScopeテンプレートを作成します。この作業では、ユーザーニーズに応じてHPOMポリシーグループを作成します。

  たとえば、サーバーに2つのタイプのオペレーティングシステムがインストールされている場合には、サーバーを2つの**ノードグループ**に分割し、監視を2つの**ポリシーグループ**に分割します。これにより、デプロイメントが簡単になります。

  また、ユーザーニーズに応じてSiteScopeでユーザーグループを使用します。たとえば、SiteScopeの用途がすべてサーバーのCPUとメモリの監視のみに限定されている場合には、監視のグループを2つ作成し、タイトルに**サーバー名**を付けたグループに監視を追加することをお勧めします。

  HPOMとSiteScopeの構成については、HPソフトウェア製品マニュアルWebサイトに掲載されてい

る製品ユーザーガイドを参照してください。

- すべての監視をデプロイします。

# 推奨事項

本項では、インフラストラクチャレイヤーでエンドツーエンドの監視を実装する際に、推奨される手順と作業を紹介します。ここで説明する内容はベストプラクティスであり、必ず行わなければならない手順ではありません。

**本項の内容**



## 監視

インフラストラクチャの監視方法には、HPOM SPIとSiteScopeソリューションテンプレートのいずれか一方、または両方を使用する方法があり、ユーザーニーズに応じて選択できます。いずれの製品も、幅広いインフラストラクチャコンポーネントを事前設定したモニターを使って監視します。監視ソリューションを選択する際には、ユーザーが実行したいユースケースに適しているかどうかを基準に判断してください。

キュー機能が必要なユースケースでは、HPOMエージェントベースの監視ソリューションが適している場合があります。HPOMエージェントは、稼働中にデータを収集してキューに格納します。

**注:** 大規模な環境では、ほとんどのインフラストラクチャコンポーネントの監視にHPOMを使用するのが一般的です。また、高速な監視ソリューションやエージェントレスな監視ソリューションが必要な場合や、HPOMにはない機能が必要な場合にはSiteScopeを使用します。

**注意:** インフラストラクチャ監視用のSmart Plug-inは、インフラストラクチャのドリルダウン機能を備えた監視の複合セットです。エラー検出の効率を最大限に高め、不要なデータの検出を最小限に抑えるためには、SPIのドキュメントをよく読むことをお勧めします。

## デプロイメント

バックアップやDRPには、[**構成のダウンロード**] オプションを使用してHPOM構成を保存することをお勧めします。サーバーをバックアップする場合や別のサーバーを災害復旧 (DR) サーバーとして使用する場合は、作成した構成と監視をすべてバックアップファイルに保存することをお勧めします。

HPOMをMOM (Manager of Managers) として設定すれば、メッセージを1つのGUIに集中的にリダイレクトできます。これによって、HPOM監視環境での監視と管理がさらに効率化されます。オペレーションマネージャー全員が1つのHPOMサーバーにメッセージを転送し、相互に「会話」できる環境であ

れば、1つのMOMサーバーで複数のHPOMサーバーを監視する環境を管理できます。この構成は、HPOMで多数のノードを管理する大規模な環境や、HPOMサーバーが稼働する複数のデータセンターを1つのロケーションから管理する必要がある場合に適しています。

# 重要度のマッピング

監視の作成では、重要度を正しく定義することが非常に重要です。

監視イベントの重要度に応じて、NOCコンソール上のイベントを処理する順序が決まります。重要度の高いイベントの数が多すぎると、オペレーターは優先度を適切に判断できず、正しい順序で対処できなくなります。さらに、重要度に誤りがあると、重大なイベントへの対応が遅れてしまい、ビジネスに深刻な影響を及ぼしかねません。このような事態に陥らないように注意が必要です。

電子メールサービスの例で考えると、メールボックスプロセスのステータスに関するイベントには高い重要度を割り当てる必要があります。重要度を割り当てる作業では、デプロイメントタイプと、そのイベントを放置した場合に発生する影響を考慮してください。メッセージに適切な重要度を割り当てるには、ユースケースの分析も必要です。

# ネットワーク監視

**本項の内容**



## 概要

ネットワークの監視は、非常に重要なインフラストラクチャITサービスの1つであり、あらゆる角度から問題を調査することができます。ネットワーク監視は、その複雑さから、インフラストラクチャレイヤーの監視ステップからは独立したステップになっています。

ネットワークデバイスの可用性とパフォーマンスを監視すると、広範囲で発生している問題の根本原因を特定して解決できるので、ネットワーク障害が引き起こす現象面への対応に時間とリソースを浪費することがなくなります。

たとえば、Microsoft Exchange環境にあるすべてのメールボックスサーバーに接続されているネットワークスイッチがダウンしたとします。ネットワークを監視していない場合、エンドユーザー監視では、**Microsoft Exchangeの電子メール送受信**の監視がクリティカルな状態であることと、トランザクションフローが使用不能状態であることが報告されるので、アプリケーションで問題が発生したように見えます。このシナリオにネットワークイベントを追加すれば、Exchangeアプリケーションで発生しているエラーの根本原因がネットワークスイッチの故障であることを簡単に切り分けることができるので、アプリケーションのダウンタイム短縮につながります。

これまで説明したように、アプリケーションが動作するには複数のリソースとサービスが必要です。ネットワークサービスは大部分のアプリケーションに不可欠なコンポーネントの1つであり、ネットワークの可用性とパフォーマンスをきめ細かく監視する必要があります。ネットワークの監視と管理には、いくつかのツールと機能が必要になります。

## ツール

- **HP Network Node Management i (NNMi)** は、あらゆる規模のネットワークの管理の効率化、ダウンタイムがビジネスに及ぼすリスクの軽減、ネットワークサービスレベルの向上など、強力な機能をネットワークオペレーションチームに提供します。NNMiは、障害、可用性、パフォーマンス、高機能ネットワークサービスの管理機能をすべて1つに凝縮したソリューションであり、物理、仮想、ハイブリッド、クラウドなどあらゆるネットワーク環境に対応します。NNMiは、HP Automated Network Management Suiteに含まれるコンポーネントの1つです。このスイートは、ネットワークの障害、可用性、パフォーマンス、変更、構成、コンプライアンス、プロセス自動化を管理する作業を包括的に自動化します。

たとえば、Microsoft Exchangeクライアントアクセスサーバーすべてを含むネットワークスイッチを監視していれば、スイッチがダウンすると、多数のExchangeサーバーが使用不能になり、電子メールサービス全体に影響が及ぶことがわかります。

また、Smart相関ルールを設定すれば、問題が発生している場所がスイッチであり、サーバーが使用不能になっているのは原因でなく現象だということを特定できるので、原因イベントが1つだけ作成されます。

- **HP Network Node Management Smart Plug-in (NNM iSPI)** は、パフォーマンスと高度なネットワークサービス向けのプラグインであり、NNMiとAutomated Network Managementソリューションでサポートできるデバイスとプロトコルを拡張することによって、幅広いネットワークデバイス、サービス、ファシリティの管理を可能にします。Smart Plug-inを使用すると、問題検出を迅速に検出して平均修復時間 (MTTR) を短縮でき、ネットワークチームの作業効率が向上します。

# インストールと構成

**インフラストラクチャサービスをインストールおよび構成するには、次の手順を実行します。**

1. NNMiソフトウェアの最新バージョンと、iSPI for Performance実行可能ファイルをインストールします。
2. NNMiのインストールは、『NNMi バージョン 9.20 インタラクティブインストールガイド ( Windows および Unix) 』を参照してください。
3. NNMiが監視対象ノードにアクセス可能であることを確認します。

   **注:** アクセス制御リスト (ACL) では、NNMiからノードへのアクセスを拒否する設定を行います。またファイアウォールでは、NNMiと監視対象ノード間の通信を拒否する設定を行います。NNMiが監視機能をすべて利用できるように、上記ではNNMiによる通信を許可してください。

4. SNMP通信の設定を強くお勧めします。

   **注:** ICMPのみを使用してノードを監視する場合には、SNMPを使用すると監視の効率が大幅に向上します。

5. ノードの検出方法として、ルールベースの自動検出と、ノードごとの個別シーディングのいずれかを選択します。自動検出ルールは簡単に設定できるので、ノードごとのシーディングではなく自動検出ルールの使用をお勧めします。
6. NNMiサーバーにトラップを送信する設定をネットワークデバイスで行うことを強くお勧めします。詳細については、『NNMi version 9.22 Deployment Reference Guide』を参照してください。

# 推奨事項

本項では、ネットワーク監視でエンドツーエンドの監視を実装する際に、推奨される手順と作業を紹介します。ここで説明する内容はベストプラクティスであり、必ず行わなければならない手順ではありません。

**本項の内容**



## デプロイメント

NNMiには、2つのデプロイメントモデルがあります。

- 単一のNNMiステーションですべてのノードを監視するモデル

  サーバーが1つしかない環境でも、NNMiは非常に高い拡張性を発揮します。このモデルの特長は、シンプルであることです。ただし、すべてのノードとWANリンクのトラフィックを1か所から監視するので、処理が低速になる可能性があることが欠点です。

- **グローバル**なNNMiステーションと複数の**リージョナル**なNNMiステーションを使用する分散モデル

  リージョナルステーションは、グローバルステーションと通信します。リージョナルステーションはポーリングを行い、負荷が適切に分散されているかチェックします。このモデルの特長は、ローカルからリージョン (データセンターなど) にポーリングを実行できるので、DMZなどセキュアな環境に適している点です。ただし、構成が複雑でメンテナンスにも手間がかかるのが欠点です。各デプロイメントモデルの長所と短所を考慮し、ニーズに合ったアーキテクチャを選択してください。

## 検出

- サービスのマッピングと相関ルールの精度を高めるには、NNMi検出にサーバーを含めてください。
- ルールでは、自動検出の対象に含めるノードと除外するノードを指定できます。一般的に、検出対象にするノードはシステムOIDに基づいて決定します。プリンターなど、監視が不要なコンポーネントを含めないように注意してください。NNMiのデフォルト設定では、スイッチとルーターのみが検出対象になっているので、これを元に設定を変更すると簡単です。

- サーバーを検出対象にする場合には、サーバーでSNMPを有効にすることを強くお勧めします。また、一般的にLinuxサーバーでは、SNMPツリーへのアクセスを追加設定し、インタフェースとアドレスを指定する必要があります。

  SNMPの有効化と構成については、『NNMi version 9.22 Deployment Reference Guide』を参照してください。

## 監視

デフォルトで付属する監視オプションの使用をお勧めします。このオプションは、ユーザーニーズのほとんどを網羅できるように調整されています。一般的にNNMiでは、監視対象スイッチに接続するポートを除き、アクセススイッチ上のアクセスポートは監視しません。したがって、切断状態や電源オフ状態になる可能性のあるノートブックやデスクトップの監視にも対応できます。

## 設定

ほとんどの場合、インストールが完了した後は、MIBをNNMiにロードしないことをお勧めします。MIBはトラップの追加定義に使用します。たとえば、サードパーティの監視アプリケーションからSNMPトラップを受信する場合などには便利ですが、MIBをロードしてもNNMi監視には反映されないので、MIBは必要ありません。

## ドキュメント

デプロイメントの例や役立つシナリオをわかりやすく紹介したホワイトペーパーは、HPソフトウェア製品マニュアルWebサイトで入手できます。

非常に幅広いデプロイメントリファレンスが提供されています。このリファレンスは製品と一緒にインストールされ、NNMiドキュメントライブラリというオンラインヘルプメニューから参照できます。このリファレンスは、パッチごとに更新されます。

# 第II部: イベント管理

# 第5章: はじめに

**本章の内容**



# 概要

**第2部: イベント管理**では、イベント管理を実装する方法について説明し、「第1部: IT環境でのエンドツーエンドのサービス監視」で作成した監視を使用してイベント管理プロセスを実装するためのベストプラクティスを併せて紹介します。詳細については、「ユースケース」( 12ページ)を参照してください。

ITIL v3では、イベントは「Iインフラストラクチャの管理またはITサービスの提供と異常がサービスに及ぼす影響の評価において、検出可能または識別可能な状態」と定義されています。詳細については、『ITIL Service Operation Guide』を参照してください。

ITILイベント管理の目的は、構成アイテム (CI) とサービスをライフサイクルを通じて継続的に監視することにあります。イベント管理は、イベントをフィルター処理および分類することにより、必要に応じて適切なアクションを決定することを目的にします。

大規模なIT環境の管理では、効率的なイベント管理プロセスを実装することが非常に重要です。

イベント管理プロセスでは、次のような処理を行います。

- 環境内にあるCIとサービスに重大な影響を及ぼす可能性のある状態を検出します。
- サービスレベルアグリーメント (SLA) と事前設定した基準に対して、実際の運用ステータスを比較する機能を提供します。
- 相関ルールと優先度ルールを統合イベントコンソールで使用することにより、IT環境の可用性とパフォーマンスを向上します。
- インシデント管理や変更管理といったイベント管理以外のITプロセスやアクティビティに関して、情報提供やレポート作成を行います。

イベント管理プロセスの実装には、HP BSM Operations Management (OMi) モジュールを使用します。このモジュールはBSM Service and Operations Bridgeソリューションの一部として提供されます。Service and Operations Bridgeの詳細については、『HP Business Service Management BSM スタートアップ・ガイド』の第2章、「BSM の概要, Service and Operations Bridge」(12ページ)を参照してください。

BSM Service and Operations Bridgeソリューションは、サービスとイベントの管理を1つのコンソール (OMiアプリケーション)で行います。IT環境で発生したイベントの監視と管理を行うことにより、サービスが中断しても最短時間で復旧し、影響を最小限にとどめることができます。

イベントを正しく管理するには、重要なイベントから優先的に処理する必要があります。サービス中断を示すイベントが複数発生した場合、その中から原因を特定および解決する作業を効率化する

ためには、イベントの相関関係の設定、イベントの文書化、イベントがビジネスに及ぼす影響の把握が必要です。

第2部のイベント管理の章でも、代表的なITサービスである電子メールサービスを例として取り上げ、HP BSM OMiモジュールを使ってIT環境でイベント管理プロセスを実装する際のベストプラクティスを紹介します。

# イベントとは

イベントとは、ITサービスやCIの状態が変化したときに、それがITサービスやCIの管理に大きな影響を与える場合に監視ツールが生成する通知です。イベントの検出には、次に示すように、データコレクターと呼ばれるさまざまな監視ツールが使用されます。

- HP Operation Manager (HPOM)
- HP Business Service Management – エンドユーザー管理 (BSM-EUM)
- HP Network Node Manager (NNMi)
- ArcSight Logger
- サードパーティツール (Microsoft SCOMなど)

詳細については、第1部の「IT環境でのエンドツーエンドのサービス監視」( 10ページ)を参照してください。

# 第6章: イベント管理

**本章の内容**



# 概要

イベント管理とは、ライフサイクルを通じてイベントを管理するプロセスです。このプロセスでは、ITサービスを正常稼働状態にできるだけ早く復旧することを目的に、IT環境内で発生するすべてのイベントを処理します。

サービス管理を行うには、まずサービスのモデル化が必要です。モデル化では、監視対象の環境、ビジネスアプリケーション、ビジネスサービス構造といった構成アイテム (CI) のレイヤー間の関係を定義します。

サービスのモデル化は、モデルCIと、それをとりまくエンティティを関連付ける作業です。モデルの設定が完了したら、モデル内で作成したCIの関係に基づいて、トポロジビューを作成します。

サービスのモデリングを適切に行うことは、イベント管理プロセスに付加価値をもたらします。これは、CIやビジネスサービス、さらに関連するビジネスサービスに対してイベントが及ぼす影響を的確に把握できるようになるからです。

また、サービスのモデル化によって、IT環境全体を可視化でき、あるCIで発生するイベントが組織全体にどのような影響を与えるかを認識できます (ビジネスインパクト分析)。さらには、組織内のビジネスニーズに応じた優先順位の決定、イベントの相関関係の指定、ビジネスサービスに関するビジネスインパクトとSLAマトリックスの数値化が可能になります。

サービスのモデル化には、いくつかのアプローチがあります。モデル化の作業は、他のさまざまなITプロセスの構成管理プロセスの一部として実行されるので、モデル化にはUniversal CMDB (UCMDB) 製

品やHP Business Service Management (BSM) のRun-Time Service Model (RTSM) モジュールを使用します。

サービス監視とイベント管理の目的でサービスのモデル化プロセスを実装する場合は、UCMDB製品でモデルを作成することをお勧めします (サービス監視とイベント管理のニーズを考慮したモデル化が可能です)。

UCMDBでモデルを作成し、検出したインフラストラクチャCIにビジネスレイヤーのCIを関連付けて、そのモデルをBSM RTSMモデルに同期させます。さらに、監視データコレクターが収集した情報をモデルに追加します。このプロセスは、逆の手順 (RTSMでモデルを作成し、UCMDBに同期) でも実行できますが、一般的にはお勧めしません。UCMDBとRTSMのどちらでモデル化を行うかは、さまざまな要因に基づいて決定する必要があります。

モデル化に使用するモジュールは、次の原則に基づいて選択してください。

- サービスをモデル化する主な目的とニーズを検討し、それに基づいてモジュールを選択します。
- UCMDBでモデル化を行う場合には、監視のニーズを考慮してください。
- UCMDBは、**正しいデータソース**としての役割を果たす必要があるので、サービスのモデル化をRTSMで行う場合には、UCMDBへの同期が必要になります。

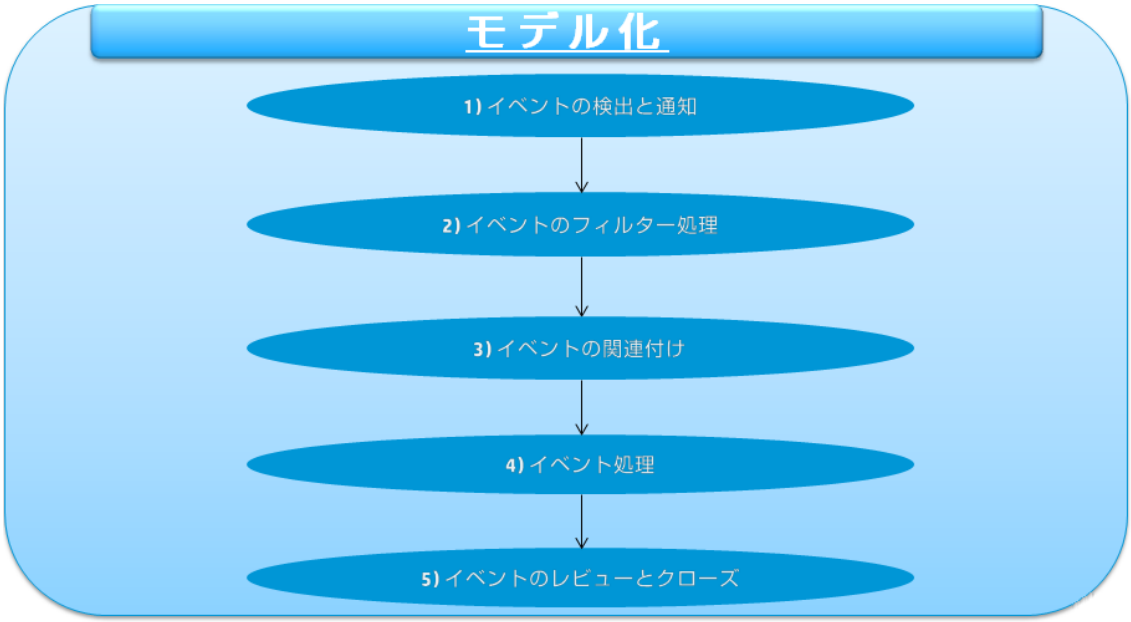
RTSMは、BSMバージョン9.00で追加されたモジュールです。Operations Management (OMi) やトポロジベースのイベント関連付け (TBEC) など、さまざまなBSMアプリケーションとサービスの基盤です。OMiとTBECの機能を最大限に活用するには、IT環境内のCIとその関係を正しく反映したサービスモデルを作成する必要があります。

RTSMでのCIとその関係に関する情報は、次のソースで参照できます。

- **CMSとUniversal Discovery (UD):** IT環境に構成管理データベース (CMDB) が実装されている場合 (HP UCMDB以外も含む)、サービスモデルをCMDBからRTSMに同期できます。トポロジはUDまたは旧バージョンのDDMaやDDMiで検出されているか、CMDBチームが手作業でモデル化しています。
- **BSMデータコレクターとスタンドアロン製品:** BSMデータコレクターは、監視および検出されたデータに基づいて、RTSMでCIとその関係を作成します。たとえば、CPUの監視をHP SiteScopeで作成すると、リモートサーバーはコンピューターCIとなり、SiteScopeはこれに基づいてトポロジをRTSMで作成します。次に、いくつか例をあげます。
  - HP Real User Monitor (RUM): ネットワークトラフィックに基づいて、コンピューターに接続するWebServer CIを作成
  - Network Node Manager i (NNMi): L2トポロジを検出し、RTSMに情報を追加
  - BSM Connector: SCOMのレポート作成トポロジとイベント
  - HP Operations Manager (HPOM): TopoSync操作を使用して、データに基づいてサービスモデルを作成

**注:** モデルの作成方法と、モデル化のベストプラクティスについては、『HP Business Service Management Effective Modeling for BSM—Best Practices』を参照してください。

CIサービスのモデル化は、既存のプロセスの前提条件に従い、次の5つのステップで行います。




1. 「イベントの検出と通知」(42ページ)

   イベントのライフサイクルの最初のステップです。本項では、組織内で稼働している監視ツールを使ったイベント検出について説明しています。使用する監視ツールには、HP Operations Manager、HP SiteScope、HPエンドユーザー監視 (EUM)、ArcSight Loggerに加え、Microsoft SCOMやNAGIOSなどのサードパーティツールも含まれます。

   しきい値とポリシーの違反を検出すると、監視ツールは通知を生成します。この通知がイベントです。

   第1部:「IT環境でのエンドツーエンドのサービス監視」(10ページ)のイベント検出と通知では、サービス指向のIT環境において監視ソリューションを実装するときの推奨事項とガイドラインを紹介しています。

2. 「イベントのフィルター処理」(43ページ)

   本項では、イベントのパラメーターに基づいて、イベント通知にフィルターを適用する方法について説明しています。

   イベントの中には重要度の低いものもあるので、イベントのフィルター処理が必要になります。フィルター処理によって、オペレーションブリッジの効率化 (ビジネスでの重要度の高いイベントの操作)、イベントコンソールに表示するデータの精度向上、不要なイベントや重要度の低いイベントの除外が可能です。

   本項では、OMiオペレーションブリッジコンソールにイベントを送信する前に、データコレクターでイベントパラメーターをフィルター処理および編集する方法について説明します。重要度の高いイベントを漏れなく捕捉し、適切に分類およびフィルター処理してからオペレーションブリッジコンソールに送信することができます。

3. 「イベントの関連付け」(46ページ)

   本項では、イベント管理コンソール (OMi) でイベントを関連付ける方法、推奨事項、ヒント、手法を紹介します。

   イベントの関連付けとは、イベント間の関係を特定する作業です。イベントの関連付けは、イベントが大量に発生する環境や複雑な方法で監視を行っている環境で役立ち、大量のイベントから重要なイベントだけを探し出すことができます。

   また、大量のイベントの中から問題の根本原因や現象を切り分ける作業でも役立つので、偶発的なイベントが発生しても迅速に対応し、解決することが可能になります。

4. 「イベント処理」(51ページ)

   本項では、HP BSM OMiオペレーションブリッジ (メインイベントコンソール) でのイベントに対する応答オプションを説明し、イベント処理に関する推奨事項を紹介します。

   応答について解説し、イベントに対する自動アクション、半自動アクション、ユーザーアクションを使用する方法、オペレーションブリッジコンソールにイベントが到着してから、正しい応答を選択してイベント処理が開始されるまでのフローを説明します。

   また、プロセスで行った作業について注釈を追加する方法、サービス管理アプリケーションでインシデントを作成する方法についても説明します。インシデントを通じて、イベント処理プロセスで行うすべてのアクションが管理されます。

5. 「イベントのクローズとレビュー」(53ページ)

   本項では、イベントが解決されるまでの過程を、オペレーションブリッジコンソールを使って管理する方法について説明します。

   大規模なIT組織のイベント管理では、イベントを継続して追跡し、問題が発生した場合はできるだけ迅速に解決して通常稼働状態に復旧する必要があります。

本項では、オペレーションブリッジコンソール(HP BSM OMi)とサービス管理システム(HP Service Manager)を統合することでイベントを管理する方法と、イベントの発生から解決にいたるまでイベントを効率的に管理する方法について説明します。

# イベントの検出と通知

検出と通知は、イベント管理プロセスの最初のフェーズで行われます。

イベントの検出には、監視ツールやデータ収集ツールを使用します。このツールは、アプリケーション、サーバー、ネットワークコンポーネントなどのITサービスやCIを分析し、CIステータスが異常を示す状態に変化してITサービスが中断されたことを検出すると、通知を送信します。

監視ツールとデータコレクターは1つのツール群として提供され、ステータス変更に応答する機能を備えます。

イベント管理プロセスではまず、サービス監視ツールをすべて適切にインストールおよび設定する必要があります。これによって、ITサービスが中断されると通知が生成されるので、この通知に基づいてイベントを受信し、あらゆるケースを漏れなくカバーすることで優れたイベント管理プロセスを構築できます。

たとえば、エンドツーエンドのサービス監視を行っている環境では、電子メールサービスのパフォーマンスが低下すると、OMiコンソールにこの問題に関連するイベントがいくつか報告されます。この情報を、後で行うイベント管理プロセス(相関ルールやインパクトルール)に反映することによって、サービス中断の解決作業のさらなる効率化が可能になります。

イベント検出フェーズで行うエンドツーエンドのサービス監視の実装について、ベストプラクティスとガイドラインは本ガイドの第1部「IT環境でのエンドツーエンドのサービス監視」( 10ページ)を参照してください。

# イベントのフィルター処理

**本項の内容**



## 概要

イベントのフィルター処理は、イベント管理プロセスで2番目に行うステップです。フィルター処理を行うことによって、オペレーションコンソールに報告されるイベントの数を減らし、管理対象のCIとサービスに重大な影響を及ぼすイベントを絞り込むことができます。

イベントのフィルター処理とは、データコレクターや監視ツールで使用するフィルタールールを作成する作業を指します。

フィルタールールは、OMiコンソールのゲートキーパーの役割を果たし、検出された情報をイベントとしてイベント管理コンソール(OMi)に送信するかどうか、各種条件に基づいて送信対象から除外するかどうかを判断します。

イベントフィルターは継続的なメンテナンスによって、報告されるイベントの件数が多くなりすぎないように、重要なイベントが欠落しないように、バランスを調整する必要があります。

フィルタールールは、時間の経過とともに変化するものであり、次のようにさまざまな条件を考慮する必要があります。

- **エラーの重要度:** 重要度が低いイベントは報告対象から除外する方がよい場合があります。たとえば、大規模な環境で電子メールサービスを監視し、イベントを受信する場合、**情報イベントや重要度が低い**イベント (**メールボックスへのログイン失敗**など) はビジネスに影響を与えないので、無視することができます。ただし、情報イベントや重要度の低いイベントであっても、特定のパターンが検出されたり大量に発生する場合には注意が必要です。重大な問題につながる可能性があるので、Smart相関ルールを作成し、必要に応じて捕捉することをお勧めします。詳細については、「イベントの関連付け」(46ページ)を参照してください。

  電子メールサービスの例では、**メールボックスへのログオン失敗**イベントが大量に受信された場合、メールボックスサーバーとディレクトリサービスの接続で問題が発生している可能性があります。

  **注:** IT組織に影響を及ぼさないイベントは、重要度に関係なく、管理対象から除外してください。

- **正常状態を示すイベント:** イベントがサービスの全体的なステータスに影響を与えるかどうかを検討します。

  正常状態を示すイベントとは、CIが正常稼働状態に復帰したことを示すイベントや、正常稼働状態を維持していることを示すイベントです。このようなイベントを元に、イベントをクローズできるかどうかを判断することがあるので、管理対象から除外しないことをお勧めします。ただし、このイベントはビジネスにまったく影響を与えません。たとえば、1分ごとに送信されるハートビート監視などが

その1例です。通常はこのようなイベントは管理の対象外とし、CIで問題が検出された時のみにイベントを生成することをお勧めします。電子メールサービスの例でいえば、CIがハートビートメッセージを5分間送信しない場合にイベントを送信する設定を行います。

- **イベントカテゴリ:** イベントの重要度に応じてイベントを分類します。OMiでは、イベントカテゴリ別にローカルビューフィルターを作成できます。これにより、コンソールでの管理担当としてオペレーターを割り当てることができます。たとえば、2つのビジネスサービスを監視している場合、2つのオペレーションチームがそれぞれ1つのビジネスサービスを担当できるようにフィルターを設定します。
- **サービスの稼働時間:** サービスで予定した稼働時間に合わせてイベントにフィルターを適用します。たとえば、8:00～17:00の時間帯のみに動作するサービスを監視してイベントを受信する場合、17:00～8:00の時間帯に発生したイベントを除外する設定や、重要度の低いイベントのみを無視する設定が可能です。

> **注:** この設定は、HP Operations ManagementまたはBSMのダウンタイム管理で行います。詳細については、『BSM 9.20 プラットフォーム管理ガイド』の第17章「ダウンタイム管理」を参照してください。

- **環境:** イベントの影響は、ビジネスアプリケーションの稼働環境 (開発環境、テスト環境、運用環境) で決まるので、環境を考慮する必要があります。たとえばテスト環境では、監視プロセスの機能自体を検証する場合を除き、重要度が低いイベントはすべて除外できます。
- これ以外にも、さまざまな条件があります。

イベント管理プロセスを実装するときは、適切なイベントフィルターを作成することをお勧めします。不要なイベントを除外することによって、イベントの大量発生を防ぎ、重要なイベントを見過ごすことがなくなります。

イベントフィルターにはさまざまなルールがあり、フィルターを適用する理由もさまざまです。イベントフィルターについては組織ごとに設定や意志決定プロセスが異なり、提供するサービス、使用するアプリケーション、インフラストラクチャコンポーネントも異なります。

# 設定

監視の作成フェーズは、監視の対象とその重要度を確定するフェーズであり、イベントフィルタールールのほとんどをこのフェーズで定義します。監視を作成する際には、何か問題が検出されるたびに、監視条件で指定した重要度のイベントが送信されるという点を考慮する必要があります。

ただし、イベントが大量に発生する環境では、使用できるフィルター処理方法の1つである**グループ化**を利用できます。監視の設定がすべて完了したら、大部分のイベントの共通点を特定することによって、多数のイベントに適用できる共通のフィルタールールを作成します。

たとえば、ある大規模な組織では、イベント管理メインコンソール (OMi) から電子メールサービス監視に送信されるイベントの中で、重要度の低いイベント (OMiの警告メッセージなど) をすべて自動的に除外しています。このような設定を行う理由としては、重要度の低いイベントが大量に発生すると、それに対処するリソースがない場合や、電子メールサービス監視から送信される警告メッセージはITや組織に大きな影響を与えないことを確認済みの場合があります。

イベントの送信では、正しいパラメーター(重要度、関連するCIやアプリケーションなど)を設定してから送信することが重要であり、これによってフィルター処理の効率が高まります。

フィルターには、場所を条件に指定することもできます。たとえば、HP Network Node Manager i (NNMi) で、LABデータセンター内にあるネットワークコンポーネントのイベントをすべて除外する設定を行うことができます。詳細については、NNMiドキュメントリストの「HP Network Node Manager Online Help for Administrators」、またはアプリケーションのヘルプメニューを参照してください。

監視ソリューションのデプロイメントを計画するときには、できるだけ幅広い視点から監視を行う必要があるケースもあります。ただしこの方法には、ITには直接的な影響を及ぼさないイベントが大量に生成されるという欠点もあります。また、コンソールに負荷がかかり、オペレーターが適切に応答できなくなる可能性もあります。このような事態を避けるため、監視の実装計画では、CIとサービスに影響を与える対象のみに監視を絞り込む必要があります。

重要度の低いイベント(および正常状態を示すイベント)は、サービスの中断状態が解消されたこと(自動的な復旧も含む)を示す場合や、相関ルールの作成において役立つ場合もあるので、重要度の高いイベントと同様に、不可欠な情報を提供しているということを忘れないでください。詳細については、「ストリームベースのイベント相関」(50ページ)を参照してください。

# イベントの関連付け

**本項の内容**



## 概要

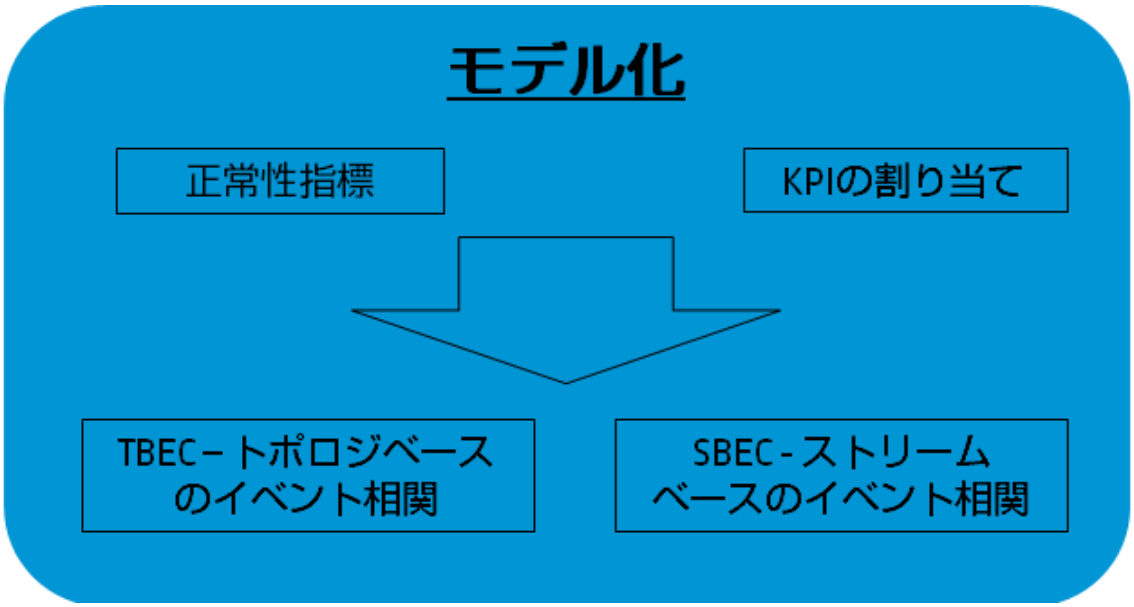
イベントの関連付けとは、複数のイベントの相関関係を特定し、この関係に基づいてイベント間のリンクを作成する機能です。

相互に関連のあるイベントは、次のいずれかの方法でリンクできます。

- トポロジベースのイベント相関 (TBEC)
- ストリームベースのイベント相関 (SBEC)

OMiモジュールで相関ルールを作成するには、正しい指標を作成し、イベントを割り当てます。BSMでは、イベントに次の指標を割り当てることができます。

- 正常性指標 (HI)
- 主要業績評価指標 (KPI)



**注:** モデル化の詳細については、「イベント管理」(37ページ)を参照してください。

イベントの関連付けプロセスは、次の手順で行います。

- 「正常性指標」(47ページ)
- 「主要業績評価指標」(48ページ)
- 「トポロジベースのイベント相関」(49ページ)
- 「ストリームベースのイベント相関」(50ページ)

# 正常性指標

正常性指標 (HI) は、監視対象のアプリケーションとビジネスサービスであるCIの稼働状態を示します。正しいCIの正しい指標にイベントを割り当てることにより、イベントとCIの関係を定義することができます。

正常性指標は、サービスのモデル化と組み合わせて使用することにより、相関ルールの機能性をさらに引き出すことができます。

HIには、バックログやボリュームといったビジネスに関する指標や、CPUの負荷やディスク容量といったパフォーマンスと可用性を監視する指標があります。

HIのステータスと値には、次の2つのタイプのデータソースが影響を与えます。

- イベント
- 指標

次に例を示します。

- **イベント:** データコレクター (HP SiteScopeやHP Operations Management (HPOM) など) を使用して、正常性指標 (**CPU負荷のしきい値超過**など) に影響を与えるイベントをOMiに送信します。
- **指標:** データコレクター (HP Real User Monitor (RUM) やHP Business Process Monitor (BPM) など) を使用して、指標を含むサンプル (**応答時間が6ミリ秒**など) を送信します。

  他にも例を示します。メールボックスへのログオンをBPMで監視する場合、正常性指標のステータスに影響を及ぼす指標サンプル (**応答時間が5ミリ秒**など) をOMiに送信します。BPMから最後に受信したサンプルに応じて、HIのステータスが変わります。

イベント管理の詳細については、『BSM バージョン 9.20 Operations Manager i コンセプト・ガイド』を参照してください。

**注:** BPMとRUMの指標サンプルを使用して、監視がしきい値を超えた時点でイベントを送信することをお勧めします。これにより、KPIに影響を与えるイベント以外にも問題を反映できます。

イベントがOMiに送信されると、サービス状況モデルで処理され、指標の割り当てが開始されます。

正常性指標にイベントを割り当てる方法には、次の2つがあります。

- ETIをイベントに埋め込む
- HI (ETI) マッピングルール (イベントプロパティのフィルターを使用してBSMで定義)

イベントの送信時には、可能な限り、イベントタイプインジケーター (ETI) を指定することをお勧めします。ETIには、名前と状態 (**CPU_Load:exceeded**など) が含まれています。[サービス状況] は、インジケーターリポジトリ内のHI定義に基づいて、ETI状態をサービス状況の標準的なステータス (クリティカル、メジャー、マイナーなど) に変換します。また、事前設定の監視の中には、ETIが定義されているものもあります。詳細については、『BSM バージョン 9.20 Operations Manager i コンセプト・ガイド』を参照してください。

- 既存のETIは変更しないことをお勧めします。変更すると、インパクト分析ルールに影響を与えたり、ルールに違反することがあり、事前設定されたヘルス指標に反映されなくなることもあります。
- 事前設定のETIとHIを使用しない場合には、できるだけ具体的にHIを定義してください。監視ごとにHIを作成し、監視状態の重要度ごとにHIの状態を定義することをお勧めします。

HIとETIの詳細については、HPソフトウェア製品マニュアルWebサイトにある『HP BSM ユーザ・ガイド』または『BSM アプリケーション管理ガイド』の「サービス状況」の項を参照してください。

# 主要業績評価指標

主要業績評価指標 (KPI) は、CIのパフォーマンスと可用性を高レベルで示すインジケーターであり、ルールに基づいてHIデータからCIステータスを計算します。

**注:** BSMでは、さまざまなKPIルールが事前設定されています。KPIルールを新しく作成する場合は、まず事前設定のルールを確認してください。

KPIは、HIのステータス、他のKPIのステータス、HIとKPIのステータスの組み合わせから計算できます。

たとえば、KPIの重要度を計算するルールには、割り当てられたHIの中で最も高い値を設定するルールや、すべての子KPIの平均値に設定するルールを指定することができます。

計算結果とKPIの定義に基づいて、KPIの重要度が設定されます。KPIの重要度は、正常、警告、マイナー、メジャー、クリティカルのいずれかです。[サービス状況] では、検出されたKPIのステータスが色別で表示されるので、KPIの状態が良好か低下しているかを色で確認できます。

KPIに反映するHIを限定することができます。

次に例を示します。

- 事前設定のシステムパフォーマンスKPI (コンピューターCIタイプ) には、CPU使用率、ディスク使用率、メモリ、ページングファイルなど、多数のHIが含まれています。コンピューターのシステムパフォーマンスの測定をCPUのみに絞り込みたい場合は、CPU関連のHIのみを計算するようにKPIを設定します。
- WindowsサーバーでExchangeメールボックスアプリケーションを実行している場合、**アプリケーションの可用性**KPIを作成し、アプリケーションの可用性に影響を与えるイベント (HIメールボックスサービスステータス **(UP-normal、DOWN-critical)** など) の関連HIすべてにリンクします。

**注:** KPIの設定では、正しい計算ルールを指定することが重要です。

KPIの詳細については、HPソフトウェア製品マニュアルWebサイトに掲載されている『HP BSM ユーザ・ガイド』または『BSM アプリケーション管理ガイド』の「サービス状況」の項を参照してください。

# トポロジベースのイベント相関

トポロジベースのイベント相関 (TBEC) は、トポロジに基づくルールを適用してイベントを分類し、イベント管理を行います。イベント間の依存関係を分析することによって、あるイベントが他のイベントを引き起こす原因になっているかどうかを特定できます。

どのITオペレーショングループにも、どのようなイベントが他のイベントの原因になるか、という依存関係に関する知識が蓄積されています。このような知識を元に、相関ルールを作成してください。また、RTSMトポロジビューでCI間のインパクトリンクを参照することによって、CIのあるイベントが、リンク先CIの別のイベントを引き起こす可能性を確認できます (現象イベントと原因イベントのリンク)。

たとえば、Outlook Web Access (OWA) ユーザーインタフェースCIで発生したパフォーマンスの問題と、OWAサーバーCIで発生したCPU過負荷の問題という2つのイベントが発生しているとします。Exchange Business ServiceのCIモデルに両方のCIが含まれている場合は、TBECエンジンでこの2つのイベントを関連付けます。これにより、OWAサーバーCIでCPUが過負荷状態になると、OWAユーザーインタフェースCIでパフォーマンス低下のイベントが発生します。この例では、両方のイベントに対処するのではなく、原因イベントの解決に集中できるので、リソースが無駄になることがなくアクションの競合も発生しません。

上記の例は、2つのイベントを関連付けることによっていずれか1つを集中的に対処するシンプルな例です。適切にイベントの相関関係を定義し、時間の経過とともに改良を加えていくことが大切です。平均で5～6の現象を1つのイベントに関連付けることにより、ITオペレーショングループが日々対処しなければならないイベントの数を60～70%低減することができます。このプロセスには、関連するイベントを調査するための時間と手間がかかりますが、長期的にみると優れた投資収益率 (ROI) を実現できます。

イベント相関は、データベース、ハードウェア、ネットワーク、Webアプリケーションといった技術的な領域を超えてリンクできます。このように包括的な視点を持つことによって、一見すると関連性のないイベントの相関を見つけ出すことができます。また、クロスドメインの監視を行うことで、オペレーターが担当する領域の重複を避けることができ、生産性も向上します。たとえば、データベースの問題、ネットワークの問題、ストレージの問題に関連するイベントを関連付けておくと、担当領域の異なる複数の

オペレーターが、1つの原因から発生している複数のイベントをばらばらに調査する事態や、1つの領域で行った操作が担当以外の領域で障害を引き起こすという事態を回避できます。

TBECを複合イベントの解決に活用することには、次のようなメリットがあります。

- 重要なデータを無視または除外することなく、コンソールで表示されるイベントの数を減らすことができます。これにより、関連イベントの階層内を自由にドリルダウンできます。
- 複数のドメインにわたってイベント相関を行うことにより、現象イベントを引き起こしている原因を簡単に特定できます。
- トポロジデータを変更しても、相関ルールの変更は必要ありません。
- イベントの重要度と、イベントに関連するCIがSLAでどのように規定されているかを確認し、それに基づいてイベント処理にビジネス上の優先度を割り当てます。

# ストリームベースのイベント相関

ストリームベースのイベント相関 (SBEC) では、ルールとフィルターを使用して、発生しやすいイベントやイベントの組み合わせを特定します。回避や排除が可能なイベントや、新規イベントの生成やオペレーターへの情報表示が必要なイベントを自動的に特定できるので、イベント処理プロセスが簡単になります。

次のタイプのSBECルールを設定できます。

- **反復ルール:** 同じイベントが高頻度で繰り返し発生する場合には注意が必要です。たとえば、同じノードで2時間内に再起動が11回以上発生した場合にクリティカルなイベントを生成するルールを設定できます。
- **複合ルール:** 特定の順序または同時に発生する複数のイベントであり、特別な対処が必要です。たとえば、NNMiから**interface down – interface up**イベントが短時間で報告された場合、SBECで両方を破棄する方法と、一時的な問題として**log only**イベントを新しく生成する方法を選択できます。
- **継続イベント欠落ルール:** 定期的に継続するイベントが発生していません。たとえば、定期的に発生するハートビートイベントが所定の時間内に受信されない場合などです。

# イベント処理

HP Operations Management (OMi) でイベントを受信し、設定 (フィルターや相関など) が完了すると、イベントはOMiコンソールで保留中になり、処理が行われるまで待機します。

イベントは、Operations Managerモジュールの [**イベントブラウザー**] ウィンドウ (OMiイベントブラウザー) に表示されます。BSMユーザーは、イベントブラウザーのビューを、ニーズに合わせて定義できます。

イベントブラウザーを表示するダッシュボードを定義し、BSMモジュールにリンクすれば統合できます。たとえば、ダッシュボードのページを作成し、RTSMからトポロジマップにリンクしたイベントブラウザーを追加することにより、選択したトポロジビューに関連するイベントが表示されます。これによってイベントの調査を効率化でき、各ユーザーが必要とする情報を表示するダッシュボードを作成することができます。またOMiでは、ユーザーグループ (特定のイベントに対する権限を持ったユーザー) に基づいて、フィルターの定義や事前設定されたイベントフィルターの指定が可能です。

OMiコンソールとMyBSMの使用方法については、HPソフトウェア製品マニュアルWebサイトに掲載されている『OMi コンセプト・ガイド』と『BSM ユーザ・ガイド』を参照してください。

イベントへの応答とは、イベントで提供される情報に基づいて、影響を受けるCIで実行するアクションを指します。アクションの実行方法は、スクリプトによる自動実行、オペレーターによる半自動実行、オペレーターによる手動実行 (イベントの解決手順を使用) があります。

イベントには次のように応答します。

- イベントを修正します。

  たとえば、**Windowsサービスの停止** イベントが発生した場合、Windowsを開始するアクションを実行します。このアクションは、オペレーターによる手動実行またはスクリプトによる自動実行が可能です。

  > **注:** この操作は、HP Business Service ManagementとHP Operations Orchestrationを使用して、CLIPソリューションの一部として実行できます。詳細については、『CLIP version 9.30 Solution Configuration Guides』を参照してください。

- インシデントのオープン

  たとえば、メールボックスのExchangeサーバーで重大な問題を引き起こしているイベントがある場合、インシデントを開き、Exchangeアプリケーションチームに送信します。

  インシデントを開くと、これによって変更要求や問題管理などのプロセスが開始され、イベントの原因となった問題が解決されるまでの間、インシデントはイベントにリンクされた状態になります。

  > **注:** この操作は、HP Business Service ManagementとHP Service Managerを使用して、CLIPソリューションの一部として実行できます。詳細については、『CLIP version 9.30 Solution Configuration Guides』を参照してください。

OMiイベントブラウザーに表示されたイベントでは、応答を選択し、次の3つの方法で実装できます。

- **自動アクション:** イベントが送信されると、スクリプトが自動実行され、問題が解決されます。この方法は、一般的なイベント (ファイルシステムのC:\ドライブ (一般的なオペレーティングシステムのファイルシステム) のディスク容量がいっぱい、など) の解決方法として使用しますが、ユーザーニーズに応じて他のイベントの解決にも使用できます。

  電子メールサービスの例で考えてみると、電子メールサービスで小さな問題 (Outlook Web AccessサーバーでIIS Webサービスが停止) が発生したとします。

  この場合、イベントがOMiに送信され、スクリプトの自動実行によってサーバーでサービスを開始するアクションが実行されます。

  これは一般的な問題なので、サービスを開始するアクションを自動実行が適切であり、解決にかかる時間を節約できます。自動アクションが失敗すると、イベントはOMiコンソールに表示されたままの状態になるので、他の方法で解決する必要があります。

  またオペレーターは、日々のイベントアクティビティをレビューし、繰り返し実行されているアクションの中から自動化できるアクションがないかチェックすることもできます。

  発生しやすいイベントのパターンを特定し、自動スクリプトや自動応答を作成することをお勧めします。

- **半自動アクション:** 自動アクションを同じ機能ですが、手動でアクションを実行します。この方法では、発生しているイベントは一般的であっても、CIの重要度が非常に高いため、オペレーターが確認しながらアクションを実行したい場合に使用します。また、イベントの問題の詳細情報を収集したい場合にも、半自動スクリプトを使用します。

  たとえば、CPUのパフォーマンスの問題を示すイベントが発生した場合には、CPU容量のほとんどの消費するプロセスを検出するスクリプトをプロンプトから手動で実行してプロセスを終了するか、インシデントを開いてOMiから担当チームに送信します。プロセスを終了する処理にはオペレーターの判断が必要なので、自動実行できません。したがって、オペレーターがアクションを実行できる半自動スクリプトが最適です。

  詳細については、『HP CLIP version 9.30 Solution Configuration Guides』を参照してください。

  また、同じ結果を繰り返し得ることができるので、再現性のメリットもあります。**メールボックスサーバーのファイルシステムのクリーンアップ**などの複合アクションは、異なるオペレーターが実行しても必ず同じ結果を得ることができます。

- **オペレーターアクション:** OMiコンソールを使用しないで、オペレーターがイベントにアクションを実行する方法です。

  たとえば、メールボックスサーバーのデータベースで、表スペースの容量が上限を超えたことを示すイベントが発生した場合、オペレーターは手動でインシデントを開き、データベース管理者 (DBA) に連絡します。DBAは、データベースに接続し、表スペースにストレージを追加します。

上記の方法は、状況に応じて組み合わせることができます。たとえば、オペレーターがイベント処理を始める前に、半自動のスクリプトを手動で実行して問題の情報を収集しておくことができます。

# イベントのクローズとレビュー

イベントのライフサイクルの最後のステップなので、イベントクローズ手順と呼ばれます。

イベントの原因となった問題を修正するアクションが完了したら、問題が解決されていることを確認し、イベントをクローズする準備をします。

イベントのクローズには、いくつかの方法があります。

- **自動クローズ:** 正常な状態に復帰したことを示すイベントステータスを使用します。この操作は、フィルターステージまたは監視の作成時 (「IT環境でのエンドツーエンドのサービス監視」( 10ページ)を参照) に行うことができ、稼働状態が正常になった時点でイベントを送信する条件を監視に追加します。
- **半自動クローズ:** CLIPソリューション経由でインシデントがイベントにリンクしている場合、担当のチームまたは担当者がインシデントをクローズすると、イベントもクローズします。
- **手動クローズ:** オペレーターがイベントを解決 (クローズ) します。

  イベントをクローズする前に問題が解決されていることを確認し、オペレーターのアクションによってどのようなイベントが発生するのかを綿密に調べる必要があり、イベントを手動でクローズした後も問題がまだ解決していない場合は、その問題がユーザーや他のCIに及ぼす影響のみが表示されます。

**推奨事項**

- 自動クローズでは、イベントの原因となる問題がクローズされたことをチェックしてからクローズされるので、可能な限り自動クローズを使用してください。ただし、自動クローズを使用できない場合 (ログファイルの監視など、問題解決が通知されない場合) には、次の方法をお勧めします。
  - ステータスチェックで行ったアクションには、記録を残す目的で注釈を必ず付けます。
  - 問題解決を担当したチームに確認します。
  - イベントにインシデントをリンクします。CLIPソリューション経由でインシデントがイベントにリンクされている場合、インシデントをクローズするとイベントもクローズするので、イベント管理が簡単になります。
- イベントを手動でクローズする場合は、実際に操作するオペレーターにイベントを割り当てます。これにより、調査中のイベントを誤ってクローズしてしまうことがなくなります。詳細については、「イベントの管理」( 56ページ)を参照してください。

# 第7章: Detect to Correct Value Streamでのイベント管理

**本章の内容**



# 概要

HP Detect to Correct (D2C) Value Streamは、複数のHP製品と統合ソリューションを使用したクロスポートフォリオのバリューストリーム(価値の流れ)です。D2C Value Streamの基盤となるのが、サービスの監視とイベント管理です。D2Cは、監視、管理、修正など、提供中のサービスと開発中のサービスを運用する上で行う機能を統合するフレームワークであり、ITチームが提供するオペレーションとサービスをビジネスの視点から包括的に把握する機能も備えています。

D2Cはサービスモデルを基盤にすることで、さまざまなオペレーション領域 (イベント、インシデント、問題、変更、構成管理など) の相関関係を明確にし、オペレーションの要求や新しい要件をビジネスの観点から評価できるようにします。D2Cは、サービス、テクノロジ、機能の枠を超え、さまざまな手法に対応できるように設計されています。

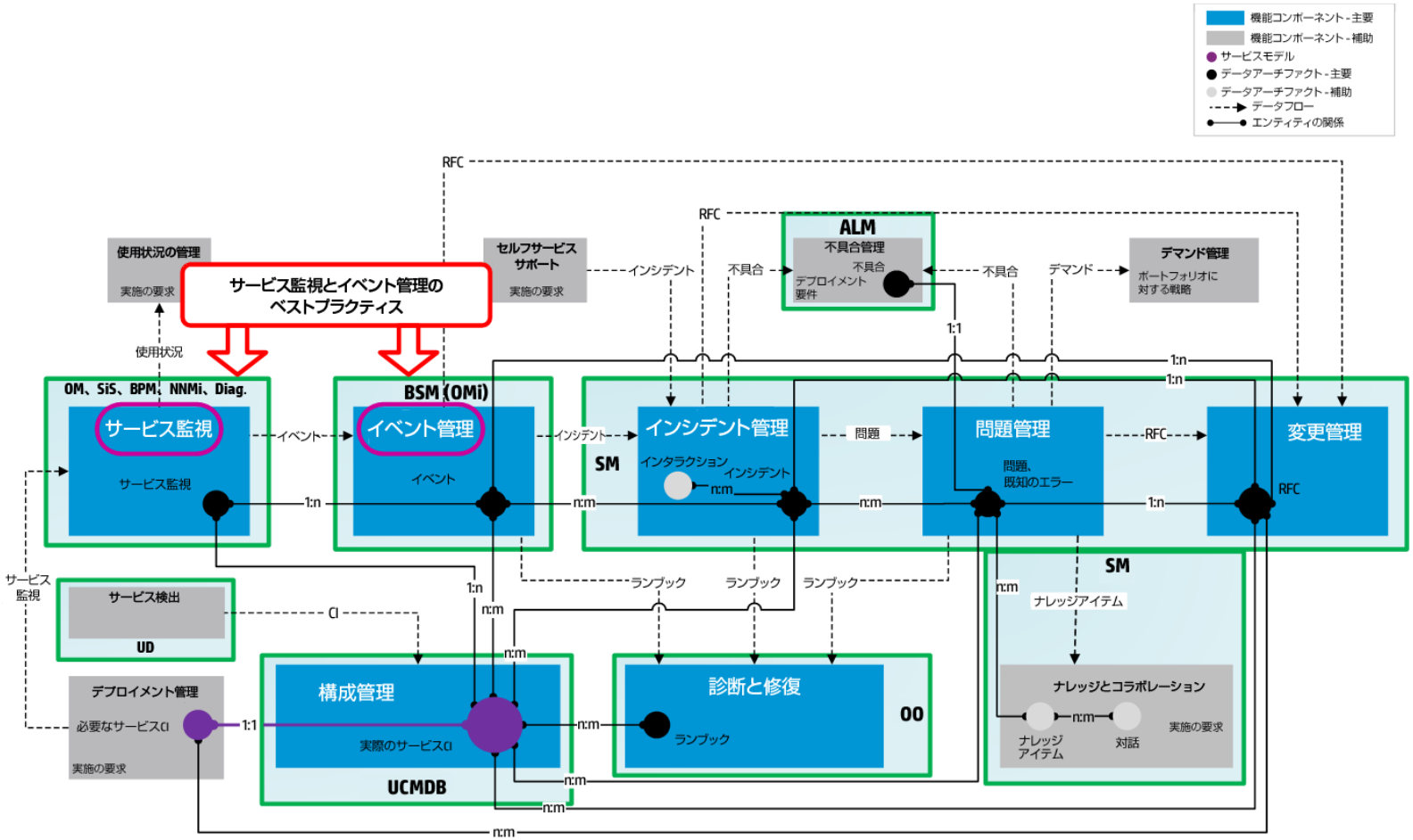
D2Cは、サービスオペレーションで行われる幅広い機能に接続し、さらに大きな成果や効率化を目指します。現在のIT環境では、主要なアーチファクト (成果物) を十分に把握できず、コラボレーションや共有を可能にするタクソノミ (分類法) が確立されていないため、ほとんどのチームは孤立した状態に陥っています。プロセス主導のアプローチでこの問題を解決しようとすると、作業が複雑になりすぎて実現不可能になるケースや、テクノロジの変化や組織的な変更に対応できず成果が得られなくなるケースもあります。これに対してサービスモデルとバリューストリームのアプローチでは、D2Cを構成する機能コンポーネントとデータ交換には一貫性があるので、テクノロジ、組織構造、プロセス、手法の変化にも十分対応できます。

D2C Value Streamの検出フェーズでは、ライフサイクル全体を通じてイベントを監視します。したがって、HPのベストプラクティスを参考に監視環境を設定することにより、D2Cが確実に効果を発揮できる実装基盤を構築してください。

**注:** Detect to Correct Value Streamの詳細については、『Detect to Correct Value Stream Concept and Configuration Guide』を参照してください。

# Detect to Correct Value Streamの図

次の図は、Detect to Correct Value Streamで使用する主なユースケースを示しています。エンドツーエンドのサービス監視およびイベント管理のベストプラクティスに含まれるプロセスと機能コンポーネントの中で、D2Cで使用するものを示しています。



# 第8章: イベントの管理

**本章の内容**



# 概要

監視が必要なイベントがすべてメインITイベントコンソール(HP BSM Operations Management (OMi))に送信されることを確認したら、イベントの管理を始めます。

イベント管理とは、イベントを解決できる最も実用的な手順を事前に設定しておき、これに従ってコンソール内のすべてのイベントを管理することによって、イベントがビジネスに与える影響を最小限に抑える作業を指します。

次に示すように、組織にはそれぞれ独自の優先順位やルールがあり、それに沿ってイベントを管理します。

- どのイベントを優先して対処するか。
- 重要なイベントが発生した場合、オペレーションチームマネージャーに報告するか。
- イベントでアクションを実行する場合に注釈を追加するか。
- どのような条件でイベントのインシデントを開くか。
- 重要度が低いイベントに対処が必要か。
- これ以外にも、さまざまなルールがあります。

上記の質問に対する答えは、イベント管理に各組織が適用するガイドラインとルールによって異なります。

どのIT組織もイベント管理ガイドラインを定める必要がありますが、一般的にはITサービスレベルアグリーメント (SLA) が使用されます。

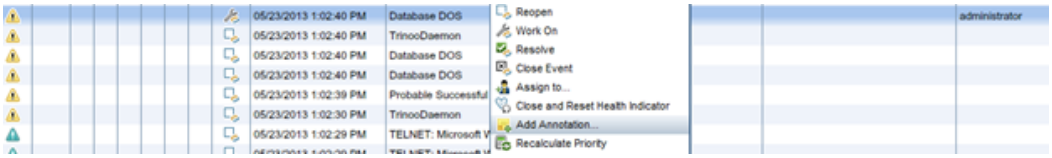
イベント管理では、次の方法をお勧めします。

1. オペレーターチームが、OMiメインコンソールを24時間365日体制で監視します。十分な数のオペレーターを配置することにより、数分以内にメッセージに応答できる体制を整えます。修正時間は、SLAの規定や1分あたりに発生するメッセージの数などに基づいて決定する必要があります。
2. OMiを正しい方法で使用します。
   - OMiを使用するオペレーターには、それぞれのユーザー名をBSMで定義し、適切なアクセス権限を割り当てます。詳細については、『BSM version 9.22 User Guide』を参照してください。
   - オペレーターは、イベント処理を開始する前に、イベントのオーナーになる必要があります。これにより、他のオペレーターはそのイベントを操作できなくなります。この操作は、**イベントの割り当て**と呼ばれます。

OMiでイベントの操作を行うには、[**Work On**] オプションをクリックしてイベントのオーナーになります。これにより、イベントが割り当てられます。


- オペレーターがシフト制で、イベントの調査が継続している場合、イベントの担当者が問題解決の過程で作業した内容を記録することが非常に重要です。

  この操作は、関連のインシデントで行うか、OMiの [**Add Annotation**] を使用します。




- イベント処理では、イベントでインシデントを開き、インシデント管理プロセスでイベントを管理します。これによって、変更要求を開く操作やインシデントを別のチームに転送する操作など、インシデント管理機能をイベントで実行できるようになります。

  OMiでインシデントを開く操作にはCLIPソリューションを使用することをお勧めします (詳細については、『HP CLIP version 9.30 Solution Guides』を参照してください)。

3. 優先度や重要度の高い順にイベントを解決してください。優先度や重要度が高いほど、イベントがビジネスに与える影響も大きくなります。また、関連イベントのグループを解決する場合は、他のイベントの原因となっているイベントを特定し、それを先に解決します。原因イベントを解決することによって、他の関連イベントをすべてクローズすることができます。イベント管理の詳細については、『BSM バージョン 9.20 Operations Manager i コンセプト・ガイド』を参照してください。