

# HP Operations Smart Plug-ins for Infrastructure

HP Operations Manager for Windows®、HP-UX、Linux、Solaris 向け

ソフトウェア バージョン: 1.60

---

## コンセプト ガイド

ドキュメント リリース日: 2010 年 5 月

ソフトウェア リリース日: 2010 年 5 月



## ご注意

### 保証について

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。ここでの記載で追加保証を意図するものは一切ありません。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 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・ソフトウェア、コンピュータ・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

© Copyright 2009-2010 Hewlett-Packard Development Company, L.P.

### 商標について

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。

Adobe®, Acrobat®, PostScript® は、Adobe Systems Incorporated の商標です。

## ドキュメントの更新情報

このガイドの表紙には、以下の識別情報が記載されています。

- ソフトウェアのバージョン番号は、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。

最新の更新のチェック、またはご使用のドキュメントが最新版かどうかの確認には、次のサイトをご利用ください。

**<http://h20230.www2.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>**

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、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

次の 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。

**[www.hp.com/go/hpsoftwaresupport](http://www.hp.com/go/hpsoftwaresupport)**

HP ソフトウェアが提供する製品、サービス、サポートに関する詳細情報をご覧ください。

HP ソフトウェア サポート オンラインでは、セルフソルブ機能を提供しています。お客様の業務の管理に必要な対話型の技術支援ツールに、素早く効率的にアクセスいただけます。HP ソフトウェアサポート Web サイトのサポート範囲は、次のとおりです。

- 関心のある技術情報の検索
- サポート ケースとエンハンスメント要求の登録とトラッキング
- 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

一部を除き、サポートのご利用には、HP パスポートユーザーとしてご登録の上、ログ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、以下の Web サイトにアクセスしてください。

**<http://h20229.www2.hp.com/passport-registration.html>**

アクセス レベルに関する詳細は、以下の Web サイトを参照してください。

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**

# 目次

<b>1 はじめに</b> .....	7
インフラストラクチャ管理とは .....	7
システム インフラストラクチャの管理.....	8
仮想インフラストラクチャの管理 .....	8
クラスタ インフラストラクチャの管理.....	8
HP Operations Smart Plug-ins for Infrastructure .....	9
<b>2 インフラストラクチャ SPI のアーキテクチャ</b> .....	11
Smart Plug-in for Systems Infrastructure .....	12
Smart Plug-in for Virtualization Infrastructure .....	12
Smart Plug-in for Cluster Infrastructure .....	12
HP Operations Manager i .....	13
インフラストラクチャ SPI によるアラートと補助情報の表示方法.....	14
監視対象要素 .....	14
容量監視 .....	14
パフォーマンス監視 .....	14
可用性監視 .....	15
セキュリティ .....	15
<b>3 キー コンセプト</b> .....	17
しきい値の設定 .....	17
スクリプトのパラメータを使用したしきい値のカスタマイズ .....	17
Threshold Overrides (しきい値の無効化)を使用したしきい値のカスタマイズ .....	18
Adaptive Thresholds (適応しきい値).....	20
カットオフしきい値 .....	21
リモート監視 .....	23
<b>4 インフラストラクチャ SPI エキスパートとの対話</b> .....	27



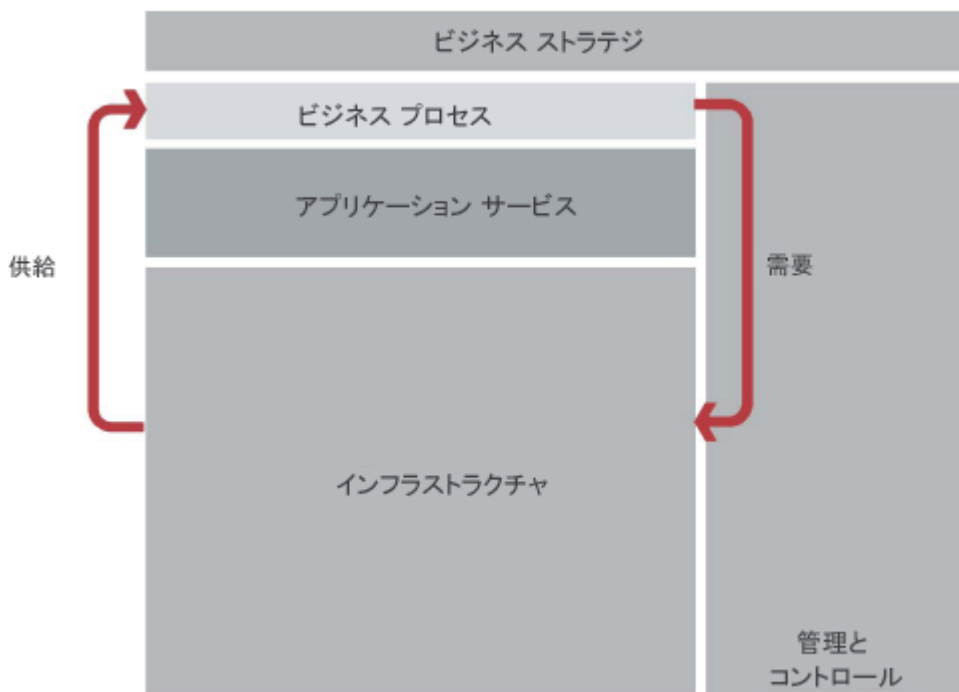
# 1 はじめに

この章では、インフラストラクチャ管理の概要、および HP Operations Smart Plug-ins for Infrastructure (インフラストラクチャ SPI) を効果的に使用して企業全体のインフラストラクチャを管理する方法について説明します。インフラストラクチャのリソースとプロセスの管理、アプリケーションの監視、およびシステムの監視に役立つ概念について紹介します。

## インフラストラクチャ管理とは

企業のインフラストラクチャへの依存度が高まるにつれ、IT インフラストラクチャを管理する方法や手段を見つけ出すことが現実的に必須となっています。インフラストラクチャ管理は、ビジネス クリティカルなシステムの維持と最適化に役立つだけでなく、複雑で分散化された IT インフラストラクチャ設定でのリソースの可用性を確保します。

図1 インフラストラクチャ管理の論理的な表現



インフラストラクチャ管理では、分散したオペレーティング システム、アプリケーションやストレージ サーバー、クラスター、および仮想マシンの使用方法を監視、分析、および最適化できます。インフラストラクチャ リソースの使用率を予測し、クリティカルなビジネスの可用性に影響が出る前に、IT インフラストラクチャの問題を回避または解決できます。また、最適なシステムのパフォーマンスとセットアップ全体の可用性を確保できます。

グローバルな組織内の各種のインフラストラクチャ環境を管理するには、クリティカルな情報のフローを調整して、問題をすばやく解決し、ダウンタイムを減らしコストを削減する必要があります。

## システム インフラストラクチャの管理

システム インフラストラクチャは、企業にとって欠かせない基盤またはベース インフラストラクチャです。CPU、オペレーティング システム、ディスク メモリ、ネットワーク リソースなどがこの中に含まれ、継続的に監視して基となる物理システムの可用性、パフォーマンス、セキュリティ、およびスムーズな動作を保証する必要があります。

システム ダウンタイムは、顧客へのサービスの品質に影響を与えます。たとえば、中央の Web サーバーで CPU ボトルネックが発生すると、クライアント アプリケーションを通じてサーバーにアクセスしている顧客への応答が遅くなる可能性があります。これは、製品とサービスに対する顧客満足度に直接影響します。このようなシナリオは、システム インフラストラクチャを継続的に監視することによって回避できます。

システム インフラストラクチャを管理すると、より高い効率性と生産性を実現できます。インフラストラクチャ障害とパフォーマンス劣化の根本原因の関連付け、特定、および解決に役立ちます。ベース インフラストラクチャの傾向とパフォーマンスを分析することで、将来の要件の特定とプランニングができます。

## 仮想インフラストラクチャの管理

仮想では、コンピュータ リソースを複数の実行環境に分けることができます。物理ハードウェア レイヤーを抽象化して、IT リソースの使用率を向上させます。仮想マシンを使用すると、いくつかの使用率が低いサーバーの負荷を少数のマシンに統合して、ハードウェアの効率的な使用率を実現できます。また、環境コストの削減、およびサーバー インフラストラクチャのより簡単な管理も支援します。仮想マシンを使用すると、複数のオペレーティング システムを同時に実行できます。バージョンが異なるオペレーティング システムや、まったく異なるシステムを、ホット スタンバイ状態にできます。また、既存のオペレーティング システムを共有メモリ マルチプロセッサ上で実行させることができます。仮想マシンは論理エンティティであり、使用している物理リソースとは切り離されているため、ホスト環境でリソースを動的に割り当てることができます。

仮想インフラストラクチャの管理では、仮想インフラストラクチャを可視化および管理できる監視サービスを提供することで、リソースの使用率を最大化します。仮想インフラストラクチャを管理する利点は、管理コストの低減、異種リソースの管理の集中化、パフォーマンスの向上、および仮想システムに対する可視性の向上を伴う可用性の向上です。

## クラスタ インフラストラクチャの管理

クラスタとは、ネットワークを介してまとめられたシステムのグループで、1つのシステムに比べてシステムのパフォーマンスと可用性の向上を目的としています。ネットワーク接続されたコンピュータに配布ソフトウェアをインストールすることによって、分散システムとなり、ユーザーに単一システムのイメージが与えられます。Serviceguard (HP-UX および Linux) や Microsoft Cluster Server (MSCS) などのクラスタは、サーバーを管理して高可用性を実現するためによく使用されます。

システムのクラスタ化には、目的に応じてさまざまな方法があります。たとえば、「高可用性 (HA)」クラスタは、ビジネス クリティカルなアプリケーションとサービス専用のサービス可用性を確保するために作成されます。HA クラスタには冗長ノードがあります。特定のアプリケーションを実行しているサーバーがクラッシュすると、そのアプリケーションは、管理者の介入なしで別のシステムですぐに再起動されます。この冗長性によって、単一点障害が排除され、サービスの高可用性が得られます。クラスタのもう1つのカテゴリとして、「負荷分散」があります。負荷分散クラスタは、クラスタのメンバであるシステム間で負荷を共有し、単一の仮想コンピュータとして動作します。



クラスター インフラストラクチャの監視では、クラスター内のすべてのノードを可視化および管理できる監視サービスを提供することで、リソースの可用性とシステム パフォーマンスを最大化します。クラスター インフラストラクチャの利点は、管理の集中化、パフォーマンスの向上、およびクラスター ノードとリソースグループの可用性の向上です。

## HP Operations Smart Plug-ins for Infrastructure

HP Operations Smart Plug-ins for Infrastructure (インフラストラクチャ SPI) は、HP Operations Manager (HPOM) と統合してソフトウェア スイートを形成し、システム、高可用性クラスター (HA クラスター)、仮想インフラストラクチャを含む企業全体にわたる分散型ベース インフラストラクチャを対象とするように、HPOM の管理スコープを拡張します。インフラストラクチャ SPI には、IT インフラストラクチャの重要な要素をすばやく制御できる事前に定義された管理ポリシーが用意されています。これらのポリシーを使用すると、クロスドメイン IT インフラストラクチャ イベントと関連アプリケーションを関連付けて、それらのイベントを階層サービス マップにマップできます。マップ ビューには、インフラストラクチャ環境のリアルタイムの状態が表示されるため、オペレーティング システム、関連するソフトウェア サービス、さらには、CPU、メモリ、スワップ スペースなどの重要なハードウェア要素で報告されるアラームの根本的原因を特定するのに役立ちます。

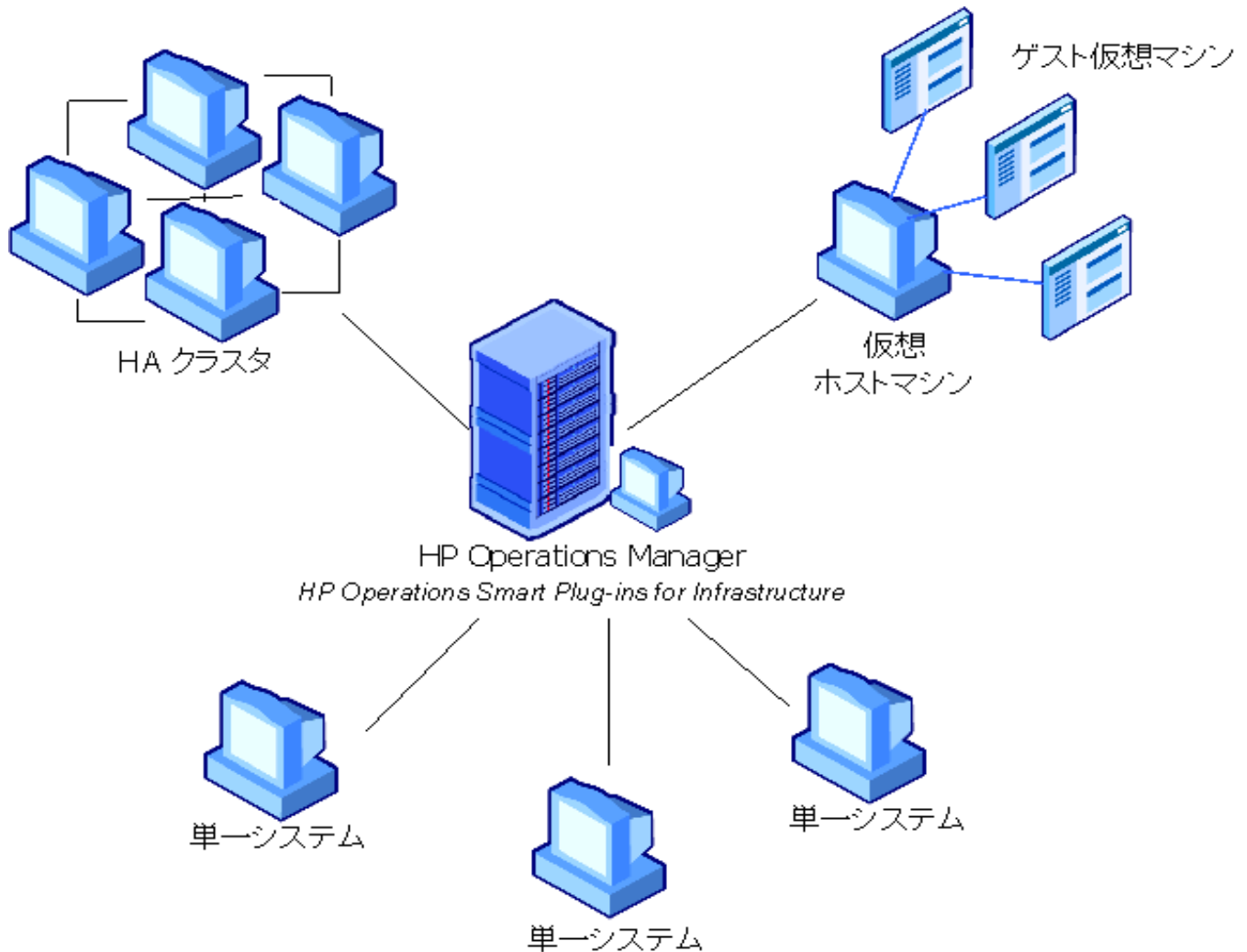
インフラストラクチャ SPI を使用すると、オペレーティング システムや関連するソフトウェアとハードウェアの機能を監視および管理できます。オペレーティング システムと関連するインフラストラクチャは、クラスター化され仮想化された環境に置くことができます。

インフラストラクチャ SPI は、HP Operations Agent、HP Performance Agent、HP Reporter、HP Performance Manager などの他の HPOM 製品と統合されます。



## 2 インフラストラクチャ SPI のアーキテクチャ

インフラストラクチャ SPI は、インフラストラクチャの可用性とパフォーマンスの向上、容量の不足や傾向の可視化、および環境全体にわたる総運用保守コストの低減に役立ちます。これらの SPI には、単一システム、クラスタ環境、および仮想化設定でのインフラストラクチャ問題を管理するための共通の統一されたモデルが用意されています。



HP Operations Smart Plug-ins for Infrastructure は、次の 3 つの SPI から構成されるソフトウェア スイートです。

- HP Operations Smart Plug-in for Systems Infrastructure
- HP Operations Smart Plug-in for Virtualization Infrastructure
- HP Operations Smart Plug-in for Cluster Infrastructure

インフラストラクチャ固有のポリシー、たとえばクラスタ用のポリシーを簡単に見つけるには、ポリシーフォルダを使用します。HPOM for Windows コンソールの場合、**[ポリシー管理] → [ポリシー グループ] → [Infrastructure Management] → [ja] → [Cluster Infrastructure]** で、HPOM for UNIX/Linux コンソールの場合、**[Policy Bank] → [Infrastructure Management] → [ja] → [Cluster Infrastructure]** となります。

## Smart Plug-in for Systems Infrastructure

Smart Plug-in for Systems Infrastructure (システム インフラストラクチャ SPI) は、Microsoft Windows または Enterprise Linux 配布を実行している企業全体にわたる単一システムの監視に役に立ちます。この SPI は、監視対象システムのパフォーマンス、容量使用率、可用性、およびセキュリティに関するアラートを HPOM コンソールに送信します。システム インフラストラクチャ SPI の検出ポリシーは、管理ノードからハードウェア リソース、オペレーティングシステム属性、アプリケーションなどのサービス情報を収集し、この情報を HPOM の [サービス] 領域に追加します。

管理ノードが VMware vMA または Microsoft Hyper-V の場合、検出ポリシーは Virtualization Infrastructure SPI の検出機能を起動します。Virtualization Infrastructure SPI は、ホスト マシン、仮想マシン (ゲスト マシン)、およびリソース プールを検出します。

同様に、管理ノードがクラスタ ノードの場合、この検出ポリシーは Cluster Infrastructure SPI の検出機能を起動します。Cluster Infrastructure SPI は、クラスタ、クラスタ ノード、およびリソース グループを検出します。

## Smart Plug-in for Virtualization Infrastructure

Smart Plug-in for Virtualization Infrastructure は、仮想リソースのパフォーマンス、容量、および可用性の各要素を監視します。

仮想インフラストラクチャは、以下のコンポーネントから構成されます。

**ホスト マシン:** さまざまな仮想マシン間でマシン リソースの共有を可能にする物理マシンです。

**ゲスト マシン:** ホスト マシン上で実行される仮想マシンで、基礎となるハードウェアまたはオペレーティングシステムの詳細情報を要約します。

**vMA:** VMware の vSphere 管理アシスタントで、ESX/ESXi および vCenter Server の各システムを管理するための事前にパッケージ化されたソフトウェアが含まれています。

## Smart Plug-in for Cluster Infrastructure

Smart Plug-in for Cluster Infrastructure は、ネットワーク上の高可用性 (HA) クラスタ インフラストラクチャを監視するのに役に立ちます。この SPI は、クラスタ ノードのパフォーマンス、および可用性に関するアラートを HPOM コンソールに送信します。クラスタ ノードの可用性は、ダウンタイムにより影響を受ける可能性があります。ダウンタイムは、メンテナンスや定期的な操作 (アップグレード、領域管理、システム再設定など) など予期されている場合や、停電、人為的ミス、データ破損、およびソフトウェアやハードウェアのエラーなど予期されていない場合があります。

HA クラスタ インフラストラクチャは、以下のコンポーネントから構成されます。

**クラスタ サービス:** クラスタの動作、クラスタ サーバー間の通信、および障害発生時の操作を制御します。

**クラスタ ノード:** 特別にリンクされたサーバーで、クラスタ サービスを実行します。

**クラスタ リソース グループ:** クラスタ リソースのグループで、フェールオーバーの単位として管理されます。

## HP Operations Manager i

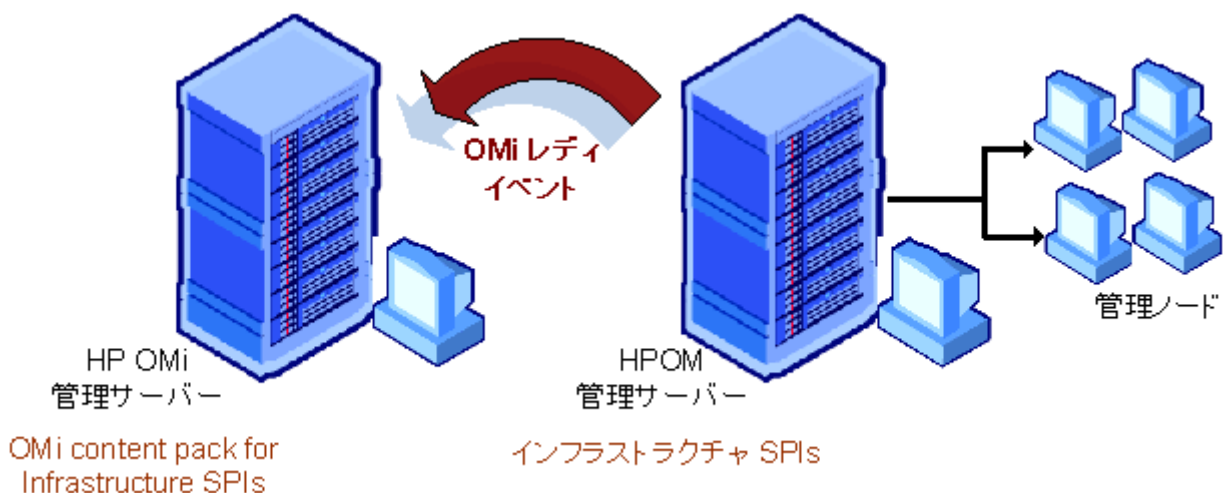
HP Operations Manager i (以降では HP OMi と呼びます) は、イベントおよびパフォーマンス マネージャで、大規模かつ複雑な環境で、運用インフラストラクチャの観点と同時にビジネス サービスの観点から、異機種ネットワークを監視します。これは、インフラストラクチャの動作状況、システム、およびアプリケーションに関する情報を収集して、特定の動作上の問題の特定と解決を支援します。

HP OMi は、以下に役立ちます。

- システムとネットワーク全体にわたるインフラストラクチャの動作状況を示す優れたビューを作成できます。
- イベントを 1 台の中央コンソールにまとめ、IT インフラストラクチャ イベントとエンド ユーザー管理イベントを関連付けることができます。
- トポロジに基づいたイベント相関を使用して、根本原因とイベントの関係を自動的に特定できます。
- IT インフラストラクチャの高度なサービスの動作状況を効率的に利用できます。

HP OMi では、これらを実現するために、HP Business Service Management (BSM) プラットフォームと HP Operations Manager が必要となります。HPOM は、管理環境で発生する OMi レディ イベントを、それらを評価する HP OMi に転送します。以下の図は、HPOM と HP OMi 間の通信を論理的に表現したものです。

図 2 HPOM と HP OMi 間の通信の論理的な表現



HP OMi は、content packを使用して、HP OMi 管理サーバーのインスタンス間でカスタマイズされた HP OMi 関連データを交換します。content packには、ユーザーが HP OMi を使用して IT 環境を管理できるように定義および設定した、すべて(または任意の部分)の HP OMi のルール、ツール、マッピング、割り当て、およびメニュー オプションの完全なスナップショットが含まれています。HP OMi と HP Operations Manager 間のトポロジを同期するときに、更新するコンテンツを指定できます。

Infrastructure SPIs を使用すると、HPOM でインフラストラクチャを管理し、管理ノードとしての HPOM の可用性、使用率、パフォーマンスを監視できます。Infrastructure SPIs には、HP OMi でインフラストラクチャに関連するイベントを分析できる、設定済みのcontent packが含まれています。

# インフラストラクチャ SPI によるアラートと補助情報の表示方法

インフラストラクチャ SPI は、インフラストラクチャの問題の分析、分離、および解決に役立つ情報を表示します。情報は以下のようなさまざまな形式で表示されます。

**メッセージアラート:** HPOM メッセージブラウザに表示されます。Measurement Threshold ポリシーの設定と、コレクタ/アナライザが収集した対象メトリックの値を使用して、インフラストラクチャ SPI は適切なメッセージを HPOM コンソールに転送します。転送されたメッセージには、重要度レベルが色付きで表示されます。

**説明テキスト:** 問題解決のヒントを提示します。生成されたメッセージのプロパティシートで利用できます。テキストを表示するには、メッセージを右クリックして、**[プロパティ]** を選択し、**[指示文]** タブを選択します。

**レポート:** システム、クラスタ、または仮想化リソースの全体像を提示します。レポートから、パフォーマンスと使用傾向が読み取れます。

**グラフ:** 使用傾向の確認、システム間のパフォーマンスの比較、およびメトリックの収集データの分析に役に立ちます。System Infrastructure SPI と Virtualization Infrastructure SPI には、事前設定されたグラフが何種類か付属しています。

**注釈:** HPOM メッセージの追加のメモです。インフラストラクチャ SPI のメッセージには、管理ノードで実行される自動アクションのステータスと出力を提供する注釈が含まれています。

## 監視対象要素

インフラストラクチャ SPI は、ポリシーに含まれているルールとスケジュールの指定に従って対象が定められ、収集されたインフラストラクチャ データを監視することにより、HPOM の監視機能を拡張しています。

IT リソースの使用方法が変わり、機能が進化するにつれ、ディスク容量、処理能力、メモリ、その他のパラメータも変わります。現在の要件、および時間経過に伴うそれらの変化を理解することが重要です。一定の期間にわたってこれらの要素を監視することは、IT リソースの使用率に対する影響を理解する上で役に立ちます。インフラストラクチャ管理では、現在と過去のパフォーマンスを分析して、将来のリソース容量のニーズを正確に予測します。

### 容量監視

容量監視は、要求に合ったサービスレベルとコストでパフォーマンスを提供するのに役立ちます。容量監視を行うことで、IT インフラストラクチャの容量を進化するビジネス ニーズに対応させることができます。使用率が低いリソースや高いリソースを特定するのにも役立ちます。

### パフォーマンス監視

パフォーマンス監視は、パフォーマンスの中断を予防し、サービス品質に悪影響を与える可能性があるインフラストラクチャの問題を特定するのに役立ちます。収集されたパフォーマンス データは、サーバー、オペレーティングシステム、ネットワーク デバイス、およびアプリケーションのインフラストラクチャ全体にわたってイベントを相関させ、悪化しつつあるパフォーマンス問題の根本原因を防止または特定するために使用されます。

## 可用性監視

可用性監視は、リソースの可用性を適切に確保するのに役立ちます。受け入れられないリソースの可用性レベルを特定することが重要です。IT インフラストラクチャの現在の負荷を計算し、しきい値レベルと比較して、リソースの可用性が不足しないように監視します。

## セキュリティ

セキュリティ監視は、修復手順を適切なタイミングで開始できるように、異種運用環境でのセキュリティの問題と脆弱性を特定するのに役立ちます。これはサービスの継続性と情報の安全性を確保するために必要になります。





## 3 キーコンセプト

### しきい値の設定

ほとんどのポリシーには、複数のしきい値レベルがあり、HPOM for Windows コンソールのメッセージアラートは設定されたしきい値に依存するため、各レベルに対して慎重にしきい値を設定することが重要になります。

インフラストラクチャ SPI を使用すると、ポリシーのしきい値を以下の方法で設定および変更できます。

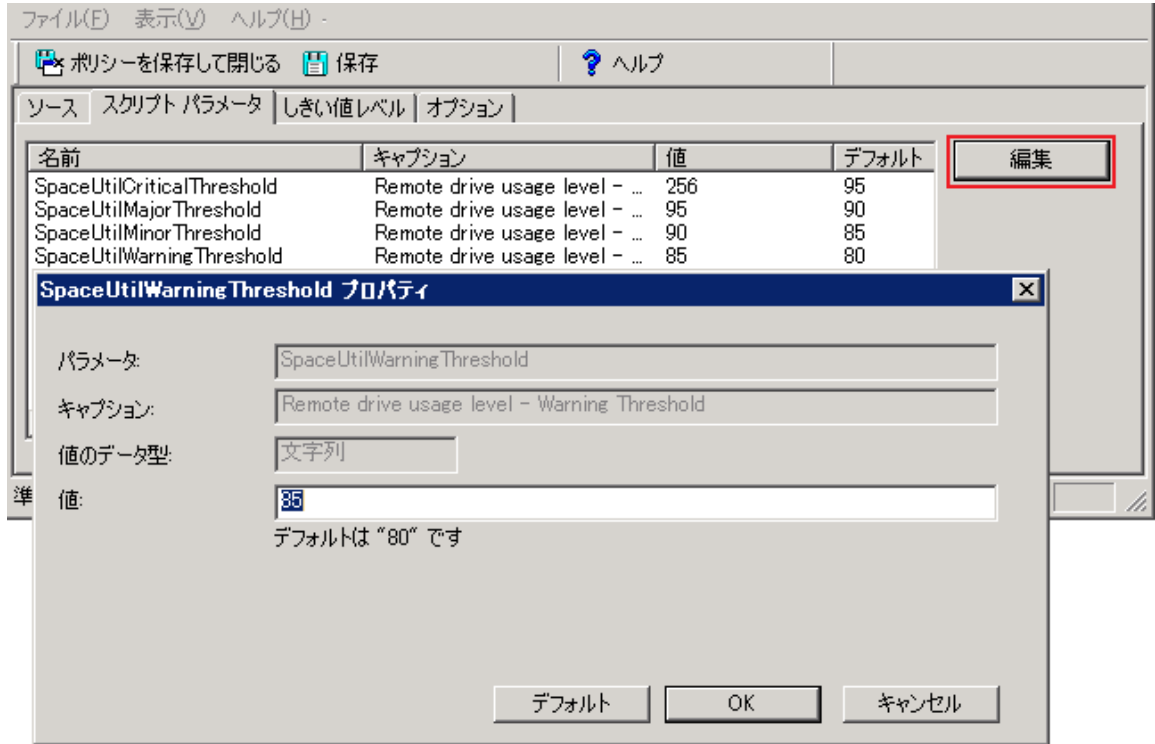
### スクリプトのパラメータを使用したしきい値のカスタマイズ

デフォルト値がユーザーの環境に合っていない場合、しきい値のタイプおよび定義済みのしきい値の限度を変更できます。ポリシーの [スクリプトパラメータ] タブには、しきい値のパラメータ名が表示されます。これらのパラメータ名には大文字と小文字の区別があります。

**Measurement Threshold タイプのポリシーのしきい値を変更するには、次の手順を実行します。**

- 1 HP Operations GUI を起動し、コンソール ツリーを使用して、**[Infrastructure Management]** ポリシー グループ/policy bankを参照します。
- 2 該当するポリシー グループ (Virtualization Infrastructure、Systems Infrastructure、または Cluster Infrastructure)、下位の該当するグループの順に展開して、変更するポリシーを見つけます。
- 3 ポリシー編集ウィンドウが表示されます。
- 4 **[スクリプトパラメータ]** タブを選択し、必要に応じて新しいしきい値を設定します。ポリシーに [スクリプトパラメータ] タブがない場合、[しきい値レベル] タブを使用してしきい値を設定できます。

図3 Measurement Threshold ポリシーのしきい値の変更例



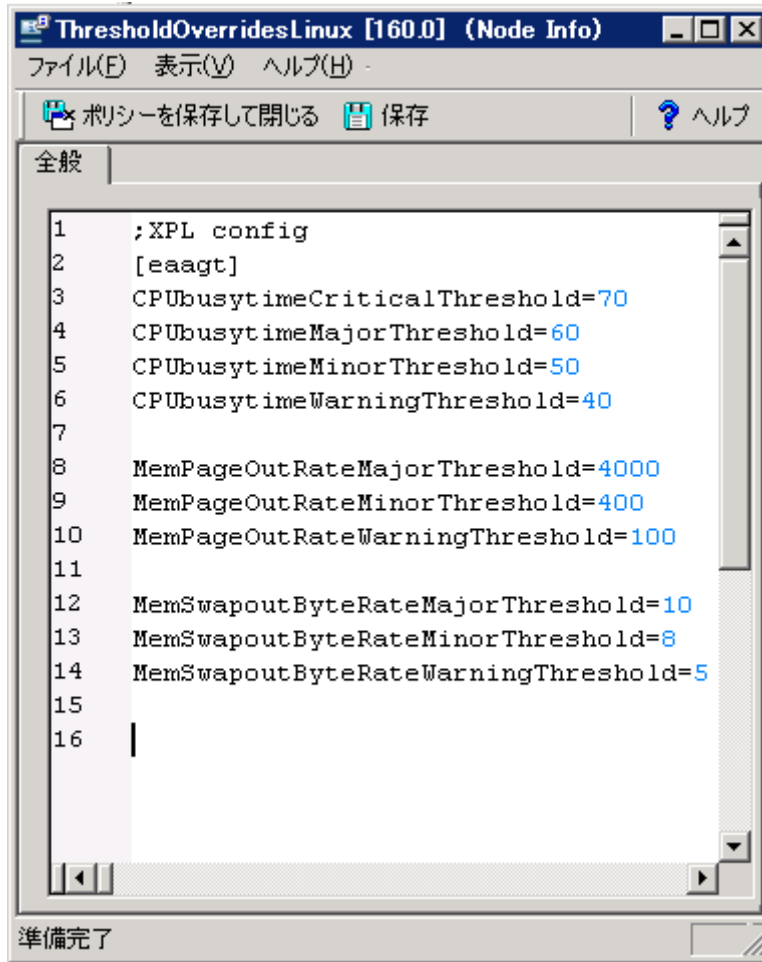
- 5 [OK] をクリックし、変更を保存します。  
ポリシーを該当する管理ノードに再配布します。

## Threshold Overrides (しきい値の無効化) を使用したしきい値のカスタマイズ

「しきい値の無効化」という概念は、一連のしきい値のターゲット管理ノードへの適用方法を制御することで、インフラストラクチャ SPI に対する柔軟性を高めます。ThresholdOverrides ポリシーを使用すると、管理ノード上の複数のポリシーのしきい値を無効にできます。

複数のポリシーのしきい値を一度に設定するには、すべてのしきい値パラメータの名前と値のリストを作成し、管理ノード上のポリシー全体のしきい値を無効にします。このしきい値パラメータのリストを使用すると、複数の管理ノード上の設定を標準化できます。ノードの値を変更する場合、リストの値を変更して、ThresholdOverrides ポリシーを特定の管理ノードに配布できます。

図 4 threshold overrides ポリシーの例



これらの手順は、特定の管理ノード上のしきい値設定を無効にするのに役立ちます。このポリシーのコピーを作成して、他の管理ノード上の別の値を設定できます。無効にするしきい値を指定したら、そのポリシーを管理ノードに配布してください。



ThresholdOverrides ポリシーは、ノード情報のタイプです。これらのポリシーによって、HPOM コンソールへのメッセージが生成および送信されることはありません。

また、XPL 設定を使用すると、ポリシー内のしきい値を直接変更することもできます。XPL 内のポリシーしきい値の設定を表示および変更するには、以下のコマンドを使用します。

- XPL 設定の名前空間を表示する場合:  
**ovconfget eaagt**
- しきい値を変更する場合:  
**ovconfchg -ns eaagt -set <しきい値名> <無効化しきい値>**

例:

```
ovconfchg -ns eaagt -set VMFSUsageCriticalThreshold 91
          -set VMFSUsageMajorThreshold 86
          -set VMFSUsageMinorThreshold 81
          -set VMFSUsageWarningThreshold 76
```

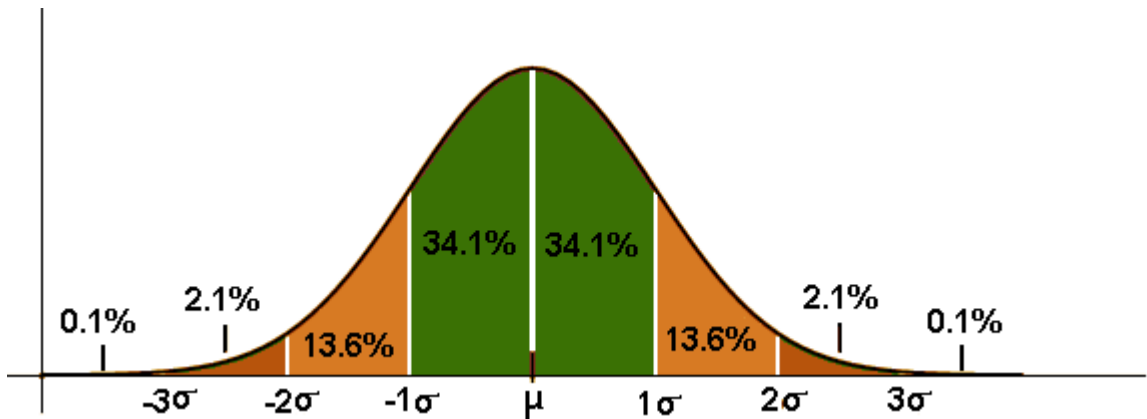
## Adaptive Thresholds (適応しきい値)

「適応しきい値」という概念は、ポリシーに指定されている固定のしきい値を使用する代わりに、インフラストラクチャリソースのパフォーマンス特性と使用パターンに関する履歴レコードを使用して、しきい値を決定するために使用されます。

ポリシーに設定されている定数のしきい値は、ある状況には理想的でも、すべての状況にとって理想的ではありません。このため、インフラストラクチャパフォーマンス用の環境設定に従って、しきい値を変更する必要があります。分散システム環境は、通常、長期にわたって予測可能な傾向に従います。適応しきい値は、前の数日の使用可能なパフォーマンスデータに従って、しきい値を自動的に計算するのに役立ちます。

適応しきい値を使用するポリシーを管理ノードに配布すると、適応しきい値スクリプトによって履歴サンプルからベースラインが設定されます。サンプルデータは、HP Embedded Performance Component または HP Performance Agent から収集されます。これらのサンプルは、インフラストラクチャパフォーマンスの以前の傾向を特定するのに役立ちます。これらの傾向に基づいて、しきい値の範囲が自動的に計算されます。現在のパフォーマンスデータと適応しきい値を比較すると、現在のインフラストラクチャリソースの使用率が正常かどうか分かります。異常な動作が検出されると、アラートが生成されます。

標準偏差の計算は、サンプル集合全体から個々のサンプルを減算し、結果を平方して、各平方の総和を取ることにより行われます。総和は、(サンプル数 - 1) で除算します。標準偏差には、統計サンプル内のポイント数および最大値と比較した標準偏差と共に上昇する分散レベルを示す信頼因子があります。この信頼因子は、異常な動作の検出時にアラートが生成されるかどうかを示します。値の信頼因子が 40% 以下の場合、アラートは処理されません。これによって、不適当なデータがある場合の間違ったアラームが排除されます。



このスクリプトは、現在のデータの平均値と標準偏差レベルを比較して、現在のデータがベースラインデータの標準偏差の 1 倍または 2 倍のいずれかを上回るか下回るかを判断します。

図の  $-1\sigma$  から  $\mu$  と  $\mu$  から  $1\sigma$  で表される標準偏差の 1 倍以内のデータは、「信頼」因子のために処理されません。現在の値が標準偏差の 1 倍を超えるが、2 倍を超えない場合、ポリシーによって重要度が注意域のメッセージが生成されます。同様に、現在の値が標準偏差の 2 倍を超える場合、ポリシーによって重要度が重要警戒域のメッセージが生成されます。標準偏差の数とメッセージの重要度は、ポリシーのスキプトのパラメータを使用して設定可能です。

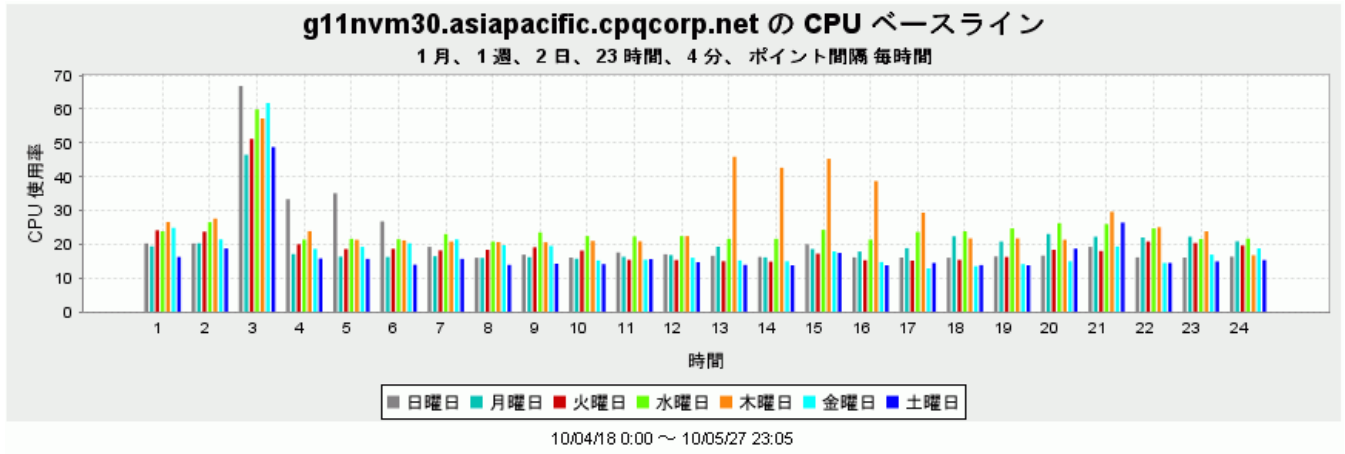
1 ヶ月超の間隔で散発的に使用されるインフラストラクチャリソースは、適応しきい値の実装に適した候補とは言えません。たとえば、四半期末処理でのみ実際によく稼動する分析サーバーがある場合、適応しきい値の計算では、ベースラインデータはあまり役に立ちません。

## カットオフしきい値

適応しきい値は、観察した値にベースラインデータと比べて有意差がある場合、アラームをトリガします。使用率が低いシステムの場合、検討中の統計用に観察される標準値は低くなります。これらの履歴データからの小さな差異でも比較的大きな偏差と見なされるため、適応しきい値によってアラームがトリガされます。

たとえば、システムの CPU 使用率が 0.5 ~ 4% の範囲で記録されていて、現在の値が 7% であるとしします。

図5 使用率が低いシステムのデータを使用した CPU 使用率グラフの例



このレベルでは、正常より高い CPU 使用率に対してアラートを受け取る必要はありません。ただし、システムの CPU 使用率が 50% である場合は、アラートを受け取る必要があります。

使用率が低いシステムに対して適応しきい値のアラームを受け取らないようにするには、パラメータにカットオフしきい値を定義できます。カットオフしきい値は、アラームを発生させるかどうかを判断するのに使用されます。

たとえば、システムの CPU 使用率が 0.5 ~ 4% の範囲で記録されていて、現在の値が 7% で、カットオフしきい値が 50% に設定されているとします。このレベルでは、CPU 使用率が記録されているデータより高くなっていますが、使用率レベルが 50% 以上に到達するまで、アラートを受け取りません。

デフォルトでは、カットオフパラメータに値は定義されていません。システム使用率の傾向に応じて、値を割り当てることができます。以下の表に、適応しきい値ポリシーに対して推奨されるカットオフ値を示します。

**表 1 adaptive threshold ポリシーに対して推奨されるカットオフ値**

ポリシー名	しきい値パラメータ名	推奨される値
SI-SwapUtilization-AT_ja_JP	SwapUtilCutOff	10
SI-PerCPUUtilization-AT_ja_JP	CPUUtilCutOff	50
SI-PerNetifInbyteBaseline-AT_ja_JP	ByNetifInByteCutOff	1000 (~ 1 KB)
SI-PerDiskUtilization-AT_ja_JP	DiskUtilCutOff	30
SI-MemoryUtilization-AT_ja_JP	MemUtilCutOff	60
SI-PerNetifOutbyteBaseline-AT_ja_JP	ByNetifOutByteCutOff	1000 (~ 1 KB)
VI-VMwareVMMemoryUsage-AT_ja_JP	MemUsageCutOff	75
VI-VMCpuEntitlementUtilizationMonitor-AT_ja_JP	CPUEntlUtilCutOff	100
VI-VMwareHostDiskUtilization-AT_ja_JP	HostDiskUtilCutOff	40
VI-VMwareNetifOutbyteBaseline-AT_ja_JP	HostNetifOutbyteCutOff	1000 × ESX/ESXi ホストで 実行中の VM の数
VI-VMwareNetifInbyteBaseline-AT	HostNetifInbyteCutOff	1000 × ESX/ESXi ホストで 実行中の VM の数

adaptive threshold ポリシーのカットオフ値を設定するには、しきい値の **Threshold Overrides** ポリシーを使用します。しきい値の無効化の詳細は、「**Threshold Overrides (しきい値の無効化)**を使用したしきい値のカスタマイズ」を参照してください。

## リモート監視

ネットワークトポロジでは、サーバーによって直接監視されるクライアントがあります。このような設定では、クライアントが代わりに、リモート エンティティと呼ばれる他のサーバー、ディスク、またはマシンをホストするか、対話します。サーバーは、クライアント経由で間接的にこれらのリモート エンティティと対話します。通常、これらのリモート エンティティは、プロキシ接続経由で監視されるエージェントレス ノードです。リモート エンティティとは、クラスター ノード、クラスター リソース グループ、仮想マシン、リモート ドライブなどのネットワークでアドレス可能なエンティティです。

**Infrastructure SPI** は、リモート インフラストラクチャの監視に役立ちます。これらの SPI は、管理ノード、または **SNMP/メッセージ許可ノード**として監視されるノードとして追加されます。

個々のシステムにマウントされたリモート ドライブは、**Systems Infrastructure SPI** ポリシーを介して監視されます。リモート ドライブの領域使用率監視ポリシーは、別のシステムによって提供されるファイル共有の領域使用率を監視します。

仮想環境では、HP Operations Agent を実行せずに、リモートで仮想マシンのパフォーマンスと可用性を監視できることが重要です。Virtualization Infrastructure SPI は、仮想マシンをリモートで監視します。VMware 監視の場合、Virtualization Infrastructure SPI は、vMA から ESX および ESXi の各リモート ホストを監視します。

クラスタ環境では、Cluster Infrastructure ポリシーが、クラスタのノードとリソース グループをリモートで監視します。

Systems Infrastructure SPI は、管理ノードを仮想化されたサーバーまたはクラスタ システムとして識別した場合、必要に応じて virtualization discovery ポリシーまたは cluster discovery ポリシーを起動します。アラートを適切なエンティティに割り当てられるようにするには、HP Operations Agent が実行されていないノードなどを、HPOM 登録ノード内のメッセージ許可ノードまたは SNMP ノードとして追加できます。インフラストラクチャ SPI では、HPOM 登録ノード内のノードの追加は、自動的に行われる場合と、手動で行う場合があります。ノードがインフラストラクチャ SPI によって自動的に登録ノードに追加されるのか、手動で追加する必要があるのかを確認するには、以下の表を参照してください。

**表 2 ノードが HPOM 登録ノードに自動的に追加されるシナリオ**

ノードの自動追加シナリオ	ノード タイプ
クラスタ ノード	SNMP/メッセージ許可/管理ノード
クラスタ リソース グループ	SNMP/メッセージ許可/仮想ノード/管理ノード
vMA に登録されている ESX ホスト	SNMP/メッセージ許可/管理ノード
vMA に登録されている ESXi ホスト	SNMP/メッセージ許可ノード
vMA に登録されている vCenter ホスト	SNMP/メッセージ許可/管理ノード

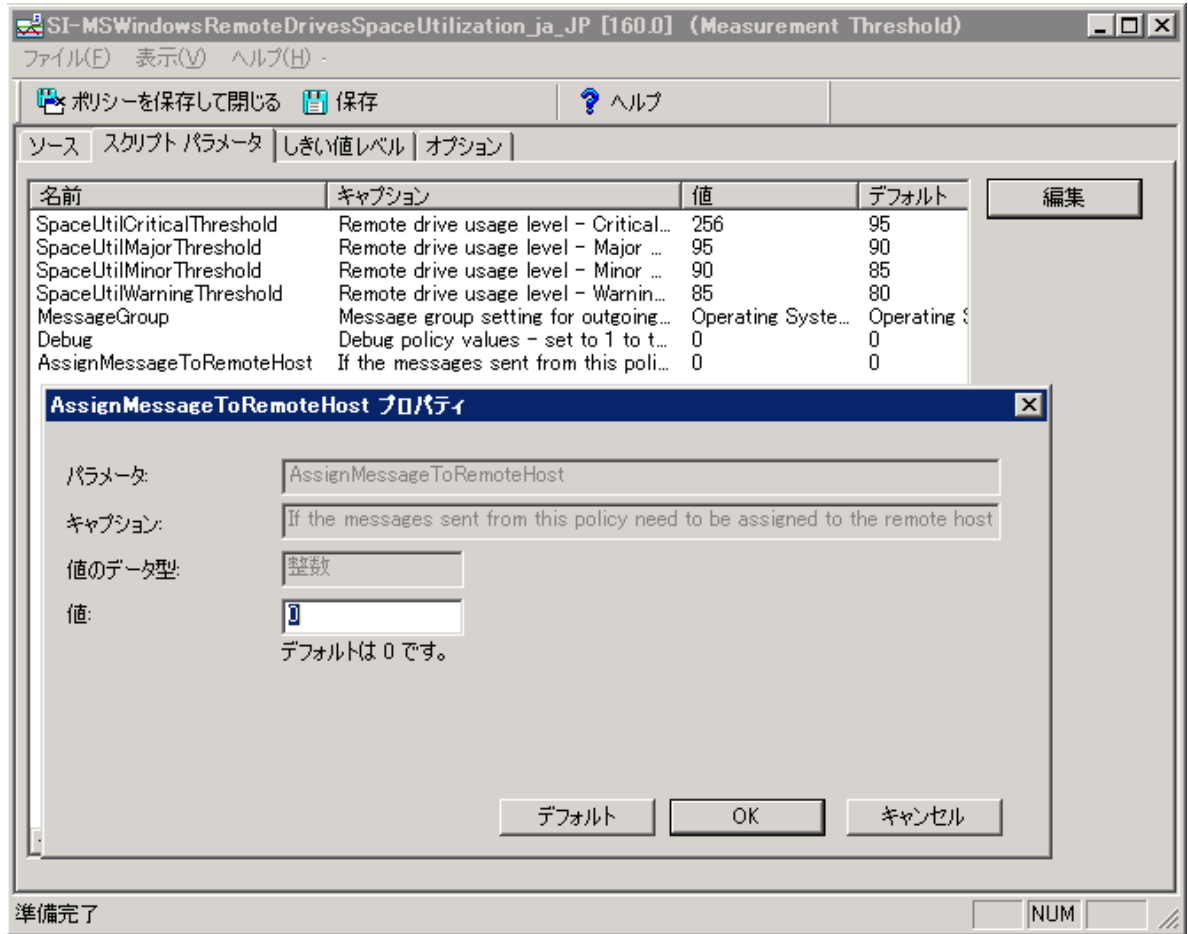
**表 3 ノードが HPOM 登録ノードに自動的に追加されないシナリオ**

ノードが自動追加されないシナリオ	ノード タイプ (追加可能なタイプ)
NFS/Samba (CIFS) 共有プロバイダ	SNMP/メッセージ許可/管理ノード
vCenter ホストで、vMA に登録されている ESX/ESXi ホストを管理しているが、vMA で登録されていない vCenter ホスト	SNMP/メッセージ許可/管理ノード
Hyper-V ゲスト仮想マシン	SNMP/メッセージ許可/管理ノード

アラートを監視の実行元のホストでなくリモート システムに割り当てられるようにするために、多くのインフラストラクチャ SPI ポリシー (リモート監視を実行可能) には、ニーズに応じて 0 または 1 に設定できる、*AssignMessageToRemoteHost* というパラメータ設定があります。



図 6 ポリシー内の AssignMessageToRemoteHost パラメータの例



値を 1 に設定すると、アラート メッセージのプライマリ ノードをリモート ホストとして表示できます。デフォルトでは、メッセージはメッセージの送信元の管理ノードに割り当てられます。



## 4 インフラストラクチャ SPI エキスパートとの対話

ここでは、インフラストラクチャ SPI のシナリオを紹介します。

この例では、Newbie という最近採用された管理者が、インフラストラクチャ SPI のインストールと配布の責任者としてアサインされたとします。この新しい管理者には、インフラストラクチャ SPI や以前のバージョンの Virtualization Infrastructure SPI に関する知識がありません。彼女は、上級管理者で運用管理機能のパワーユーザーである InfraSPI エキスパートに、製品を理解するための支援を求めています。以下はこの 2 人の間で交わされた会話です。

**Newbie:** 最近、使用中のサーバーの 1 台の処理速度が遅くなり、システム上で実行されるデータベース インスタンスの応答時間が異常になることがよくあるんです。

**InfraSPI エキスパート:** CPU とメモリの使用率を監視しても、システム上のボトルネックが見つかりませんでしたか？

**Newbie:** 見つかりませんでした。

**InfraSPI エキスパート:** Systems Infrastructure SPI の CPU CPU bottleneck diagnosis (ボトルネック診断) ポリシーと memory bottleneck (メモリ ボトルネック診断) ポリシーをノードに配布してみてください。これらのポリシーが、上位 10 の CPU 占有プロセスとメモリ占有プロセスをそれぞれ報告してくれます。きっと問題の原因を特定するのに役立つはずです。

**Newbie:** やってみます。

**Newbie:** これらのポリシーを配布したところ、サーバーの処理速度が遅くなった理由が分かりました。Systems Infrastructure SPI が HPOM コンソールにアラート メッセージを送信したため、問題の根本原因をすぐに把握できました。送付されたメッセージには、CPU とメモリの使用率を占有している上位 10 のプロセスが表示されています。

**InfraSPI エキスパート:** よくやりましたね。ところで問題は何でしたか？

**Newbie:** 散発的に CPU 消費とメモリ使用率を増大させている、ログ アプリケーションが実行されていたんです。そのログ アプリケーションを修正しました。

**InfraSPI エキスパート:** なるほど。

Systems Infrastructure SPI に付属しているポリシーの詳細は、『*HP Operations Smart Plug-in for Systems Infrastructure ユーザーガイド*』を参照してください。

**Newbie:** この方法は、問題を特定するのに非常に有効でした。でも、いつもビジーまたはアイドルなシステムの場合は、どうしたらいいのでしょうか？

**InfraSPI エキスパート:** 使用率の高いシステムまたは低いシステムの場合、Systems Infrastructure SPI の CPU utilization (CPU 使用率監視) ポリシーと memory utilization monitor (メモリ使用率監視) ポリシーをノードに配布するといいですよ。これらは adaptive threshold (適応しきい値) ポリシーで、正確な結果が得られます。

**Newbie:** adaptive threshold ポリシーについては、読んだことがあります。これらのポリシーは、パフォーマンス特性や前に収集したデータのパターンから学習し、現在の使用率が正常かどうかを統計的に判断するものですね。これらのしきい値は、履歴データに基づいて自動的に計算されるんですね。

**InfraSPI エキスパート:** そのとおり。実際に問題のあるシナリオに関するアラートのみを受け取ります。auto threshold determination (自動しきい値決定) ポリシーを簡単に特定するには、SI-SwapUtilization-AT\_ja\_JP や VI-VMwareHostDiskUtilization-AT\_ja\_JP などのようにポリシー名の末尾に AT が追加されているかどうかを確認してください。

adaptive threshold (適応しきい値) の計算方法の詳細は、「[Adaptive Thresholds \(適応しきい値\)](#)」を参照してください。

**Newbie:** 分かりました。また、多くのポリシーを使用しているうちに気づいたんですが、危険域のしきい値パラメータに「65535」という妙な値が割り当てられていました。

**InfraSPI エキスパート:** この値は、危険域のしきい値パラメータをマスクで除外するために、意図的に割り当てられているんです。これで、システムは危険域のアラートメッセージを生成しなくなります。必要に応じて、危険域のしきい値レベルを手動で定義することもできます。

**Newbie:** でも、なぜ 65535 なんですか?

**InfraSPI エキスパート:** 単なる数字ですよ。マスクの場合、100 を超える任意の数字を指定できます。

**Newbie:** 分かりました。VM state monitor (VM 状態監視) ポリシーはどのように使用したらいいのでしょうか?

**InfraSPI エキスパート:** VI-StateMonitor\_ja\_JP ポリシーは、ホスト サーバーとそのサーバー上に設定されているゲスト仮想マシンの状態を報告します。このポリシーは、基本的に、仮想マシンを監視し、その状態の変化を報告します。

**Newbie:** マシンが過渡段階でハングまたは処理不能になりますが、どうしてでしょうか?

**InfraSPI エキスパート:** よく聞いてくれました。Virtualization Infrastructure SPI は、仮想マシンが起動、スナップショット、移行、保存、停止などの過渡段階で 30 分以上処理不能になると、アラートを送信します。このポリシーは、仮想マシンの実行に関する状態の移行または問題 (存在する場合) を特定するのに非常に役に立ちます。

**Newbie:** もう 1 つ、テスト用の仮想マシンで毎晩発生する計画停止についてですが、これは意図的なもので、スケジュール済み停止の VM 状態の変更に関するメッセージは不要です。これらのサーバーに関するアラートを受け取らないようにするには、どうしたらいいのでしょうか?

**InfraSPI エキスパート:** 良い質問です。毎日事前に定義された時刻に計画停止されるノード (21:00:00 にシャットダウンされ、翌朝の 05:00:00 に復元されるテスト用の仮想マシンなど) の場合、**AlertOnPlanned Outage** パラメータを true に設定すると、VI-StateMonitor\_ja\_JP ポリシーからの状態変更に関するアラートメッセージを受け取らないようにできます。この設定でポリシーを配布すると、VI-StateMonitor\_ja\_JP ポリシーでは、指定された期間、監視対象ノードに関する VM 中断アラートを生成しなくなります。virtual infrastructure の監視用に提供されるポリシーの詳細は、『*Smart Plug-in for Virtualization Infrastructure SPI ユーザーガイド*』を参照してください。

**Newbie:** サーバーの高可用性を確保したいクラスタ化された Web サーバーがあります。このサーバーをダウンさせるわけにはいきません。quorum 侵害や単一点障害状況などの危険域サービス レベル水準を監視し、アラートを発生させるのに役立つポリシーはありませんか?

**InfraSPI エキスパート:** Cluster Infrastructure SPI に CI-ClusterMonitor ポリシーが用意されています。このポリシーは、次のような条件を監視します。

- クラスタがダウンまたはオフラインになっている。
- 大半のノードがダウンしていて、クラスタ quorum が維持されていない。(n/2 + 1) 個のノードがアクティブな状態でない場合。たとえば、クラスタ内に 6 つのノードがあり、アクティブなノードが 4 未満の場合、ポリシーによってアラートが発生します。
- クラスタ全体でアクティブなノードが 1 つしかなく、単一点障害 (SPOF) とクラスタの可用性に関する潜在的なリスクがある場合。

このポリシーは上記のすべての条件に対してアラートを送信するため、クラスタの可用性水準に対する何らかの侵害があれば、必ず通知されます。cluster infrastructure の監視用に提供されるポリシーの詳細は、『*Smart Plug-in for Cluster Infrastructure SPI ユーザーガイド*』を参照してください。

**Newbie:** 役に立つ情報をありがとうございました。

## We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click on the bookmark “Comments”.

In case you do not have the email client configured, copy the information below to a web mail client, and send this email to **docfeedback@hp.com**

**Product name:**

**Document title:**

**Version number:**

**Feedback:**

