HP Operations Manager

コンセプトガイド

ソフトウェアバージョン : **9.10**

UNIX および **Linux** オペレーティングシステム向け

製造パート番号 : なし

2011 年 **6** 月 **17** 日

ご注意

保証について

当社は、本書に関して特定目的の市場性と適合性に対する保証を含む一切の保証をいたしかねます。当社は、本書の記載事項の誤り、またはマテリアルの提供、性能、使用により発生した直接損害、間接損害、特別損害、付随的損害または結果損害については責任を負いかねますのでご了承ください。

当社製品に適用される特殊保証条件のコピーは、地域の販売およびサービスオフィスにお問い合わせください。

Restricted Rights Legend.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

著作権について

商標について

Adobe® は、Adobe Systems Incorporated の登録商標です。

Intel®、Itanium®、Pentium® はアメリカ合衆国およびその他の国におけるインテルコーポレーションの登録商標です。

Java は、オラクルおよびその系列会社の登録商標です。

Microsoft®、Windows® は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Oracle® は、米国オラクルおよびその系列会社の登録商標です。

UNIX® は、The Open Group の登録商標です。

目次

1. HPOM の概要

2. HPOM の設定と保守

目次

3. HPOM 管理対象ノードの概念

目次

出版履歴

マニュアルの出版日付と部品番号は、マニュアルの版数を示します。出版日付は、最新版が出版されるたびに変更されます。小規模の改訂は増刷の際に対応し、出版日付は変更しません。大規模な改訂を行う際には、マニュアルの部品番号を変更します。

誤りの訂正や製品の変更のため、次の改訂の前にマニュアルのアップデート版を出すことがあります。常に最新版を確実に入手できるようにするには、適切な製品のサポートサービスにご加入ください。詳細は、当社の営業担当にお問い合わせください。

初版	2010 年 8 月
第 2 版	2011 年 6 月

はじめに

HP Operations Manager (HPOM) は、分散マルチベンダーシステム向けの一元操作型障害管理製品です。本書は、HPOM を理解し、効率的に使用していただくためのものです。

機能

HPOM には、次の機能があります。

- **メッセージ管理**

  メッセージ処理を集約、簡略化、自動化するための一元的なメッセージ管理機能

- **モニター**

  障害を予防的に解決するための一元的なモニター機能

- **障害管理**

  障害を通知、解決、トラッキングするための一元型の障害管理機能

- **制御**

  効率的な管理のための一元的な制御機能

対象読者

本書は次の 2 つのタイプのユーザーを対象としています。

- **管理者**

  HPOM のプランニング、設定、および保守を担当する管理者の方

- **オペレータ**

  日常の作業に HPOM を使用されるオペレータの方

構成

本書は次のような構成になっています。

第 1 章 すべてのユーザーが対象です。HPOM の概念、機能、構造を簡単に説明します。

第 2 章 オペレータが対象です。オペレータ環境と、障害解決のためのテクニックについて説明します。

第 3 章 管理者が対象です。HPOM の各要素 (管理対象ノード、ノードグループ、メッセージグループ、アプリケーション、オペレータなど) の設定方法について説明します。

第 4 章 管理者が対象です。メッセージポリシーを実装し、設定を配布する方法について説明します。

第 5 章 管理者が対象です。大規模な分散環境における HPOM の設定方法と管理方法について説明します。また、フレキシブル管理と manager-of-manager (MoM) 通信の基本的な概念についても説明します。

付録 管理者が対象です。デフォルトポリシータイプのポリシー本文の構文について説明します。

用語集 すべてのユーザーが対象です。HPOM で使用される用語の定義を示します。

表記規則

本書では、次の印刷表記法が使用されています。

表 1　　印刷表記法

字体	説明	例
Italic	書名およびマニュアルページ名	詳細は、『*HPOM システム管理リファレンスガイド*』および *opc(1m)* マニュアルページを参照してください。
	強調	次の手順を実行する*必要があります*。
	コマンド入力時に使用する変数 (かぎかっこ)	プロンプトで、**rlogin *<username>*** を入力します。
	関数で使用するパラメータ	*oper_name* パラメータは整数値を返します。
コンピュータ文字	コンピュータディスプレイの項目	次のシステムメッセージが表示されます。 `Are you sure you want to remove current group?`
	コマンド名	`grep` コマンドを使用して、...
	関数名	`opc_connect()` 関数を使用して接続します ...
	ファイルおよびディレクトリ名	`itooprc` ファイルを編集します ... `/opt/OV/bin/OpC/`
	プロセス名	`opcmona` が実行中かどうかをチェックします。
コンピュータ文字、太字	入力するテキスト	プロンプトで、**`ls -l`** と入力します。

表 1　　印刷表記法 (続き)

字体	説明	例
キーキャップ	キーボードのキー	**Return** を押します。
	メニュー名の後にコロン (:) が記載されていることがあります。これは、ユーザーがそのメニューを選択した後、メニュー項目を選択することを示しています。項目の後に矢印 (->) がある場合は、階層化されたメニューがその後続くことを示します。	メニューバーから [**アクション**]: [**フィルター処理**] -> [**すべてのアクティブメッセージ**] の順に選択します。
	ユーザーインタフェースのボタン	[**OK**] をクリックします。

ドキュメントの使用方法

HP Operations Manager (HPOM) では、製品を効果的に使用し、その使い方と概念を理解できるように、マニュアルとオンラインヘルプを用意しています。本項では、入手できる情報や情報の参照個所を説明します。

電子メディアのマニュアル

HPOM のすべてのマニュアルは、HPOM 製品 DVD のドキュメントディレクトリに Adobe Portable Document Format (PDF) の形式で入っています。

次の Web サイトからも HPOM 製品のすべてのマニュアルをダウンロードできます。ログイン認証が必要です。

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

この Web サイトにある『*HPOM ソフトウェアリリースノート*』(OVO ソフトウェアリリースノート) の最新版を定期的に確認してください。このリリースノートは 2 ～ 3 ヶ月ごとに更新され、サポート対象として追加された OS バージョンや最新のパッチなど、最新の情報が記載されます。

さらに製品を限定したマニュアルも、次の HPOM Web サーバーディレクトリから入手できます。

- 標準の接続

  http://*<management_server>*:8081/ITO_DOC/<lang>/manuals/

- セキュアな接続

  https://*<management_server>*:8444/ITO_DOC/<lang>/manuals/

<management_server>	HPOM 管理サーバーの完全修飾ホスト名
<lang>	管理サーバーで設定されているシステム言語 (英語環境は C など)

また、インストールの終了後は、HP Operations 管理サーバーファイルシステムの次の場所から、選択した製品マニュアルを利用できます。

- HP Operations Manager:

  /opt/OV/www/htdocs/ito_doc/<*lang*>/manuals

- HPOM 管理 UI

  /opt/OV/OMU/adminUI/jre/db/docs/pdf/

- Hotfix 配布ツール

  /opt/OV/contrib/OpC/Hotfix_deployment_tool/

- HP Event Correlation Services (ECS):

  /opt/OV/doc/ecs/<*lang*>/

- HP OVprotect ツール

  /opt/OV/contrib/OpC/OvProtect/

- HP SiteScope

  /opt/OV/nonOV/tomcat/b/www/webapps/topaz/amdocs/eng/pdfs/

- HP Business Avalability Center (BAC)

  /opt/OV/install/OpC/

- Tomcat

  /opt/OV/nonOV/tomcat/b/www/webapps/docs/architecture/startup/
  /opt/OV/nonOV/tomcat/b/www/webapps/docs/architecture/requestProcess/

- Incident WebServices Perl ライブラリ

  /opt/OV/contrib/OprWsIncPerl/

HPOM Java GUI オンラインヘルプ は、ソフトウェアのインストールの完了後、HP Operations 管理サーバーのファイルシステム上の次の場所から利用できます。

/opt/OV/www/htdocs/ito_op/help/<*lang*>/ovo/html/

HPOM マニュアル

ここでは、UNIX 上の HPOM および Linux 上の HPOM の最も重要なマニュアルの概要を説明します。追加のドキュメントについては、17 ページの「電子メディアのマニュアル」のドキュメントを参照してください。
19 ページの表 2 はマニュアルのリストです。対象となる読者、簡単な説明およびマニュアルの範囲と内容が記載されています。

表 2　　HPOM マニュアル

マニュアル名	対象読者	説明
HPOM 管理サーバーインストールガイド	管理者	管理サーバーに HPOM ソフトウェアをインストールし、初期設定を行う方法を説明します。このマニュアルには、次の内容が記載されています。 • ソフトウェアとハードウェアの要件 • ソフトウェアのインストールと削除の手順 • デフォルト値を用いた設定
HPOM コンセプトガイド	管理者 オペレータ	HPOM を理解するために使用者を 2 つのタイプに分けて説明しています。オペレータの場合には、HPOM の基本構造を理解します。管理者の場合には、現在の環境で HPOM のセットアップと設定ができるようになります。
HPOM システム管理リファレンスガイド	管理者	HPOM を管理対象ノードにインストールし、HPOM の管理とトラブルシューティングの方法を説明します。 また、HP Operations Service Navigator のインストール、構成、保守、トラブルシューティングの担当者向けの情報を提供しています。サービス管理の背景にある概念の概要も記述しています。
HPOM Reporting and Database Schema	管理者	HPOM のデータベースの表の詳細と、HPOM データベースから生成されるレポートの例を説明しています。

表 2　　HPOM マニュアル (続き)

マニュアル名	対象読者	説明
HPOM Java GUI オペレータガイド	管理者 オペレータ	HPOM の Java ベースのオペレータ GUI と Service Navigator の詳細を説明しています。このマニュアルには、HPOM オペレータ向けに、一般的な HPOM および Service Navigator の概念と作業の詳細を説明しています。また、リファレンスおよびトラブルシューティングの情報もあります。
HPOM ソフトウェアリリースノート	管理者	新機能が一覧で示されています。次の作業に便利です。 • ソフトウェアの新旧バージョンの機能比較 • システムとソフトウェアの互換性 • 既知の問題の解決法
HPOM Firewall Concepts and Configuration Guide	管理者	HPOM ファイアウォールの概念を説明し、セキュアな環境の設定手順を解説します。
HPOM Web Services Integration Guide	管理者	HPOM Web サービスの統合について説明します。
HPOM Server Configuration Variables	管理者	HPOM 管理サーバーの設定に使用する変数のリストとその説明です。

HPOM オンライン情報

インストールと初期設定が終了したら、次の情報を HPOM 管理サーバーからオンラインで利用できます。

表 3　　HPOM オンライン情報

オンライン情報	説明
HPOM Java GUI オンラインヘルプ	HPOM の Java ベースのオペレータ GUI と Service Navigator の HTML ベースのヘルプシステムです。このヘルプシステムには、一般的な HPOM および Service Navigator の概念と、HPOM オペレータの作業についての詳細な情報、リファレンス、およびトラブルシューティングの情報もあります。
HPOM のマニュアルページ	HPOM マニュアルページはコマンド行だけでなく、HTML 形式でも利用できます。HTML 形式の HPOM マニュアルページにアクセスするには、Web ブラウザに次のいずれかのアドレス (URL) を入力してください。 • 標準の接続 **http://<*HPOM_management_server*>:8081/ITO_MAN** • セキュアな接続 **https://<*HPOM_management_server*>:8444/ITO_MAN** これらの URL で、*<HPOM_management_server>* は HPOM 管理サーバーの完全修飾ホスト名です。HPOM エージェント用のマニュアルページは、各管理対象ノードにインストールされています。

HPOM 管理 UI のドキュメント

インストールと初期設定が終了したら、次の情報を HPOM 管理サーバーからオンラインで利用できます。

表 4　　HPOM 管理 UI のドキュメント

オンライン情報	説明
HPOM 管理 UI のオンラインヘルプ	HPOM 管理者 GUI のオンラインヘルプは、管理者用グラフィカルユーザーインタフェースに表示されている個々のページ、メニュー、オプションの状況に合わせた情報を提供します。メニューおよびメニューオプションは、作業中のデータコンテキストに応じて変わります。対応する Web ブラウザに次の URL を入力して、HPOM 管理者用ユーザーインタフェースを起動します。 • 標準の接続 **http://<*HPOM_management_server*>:9662** • セキュアな接続 **https://<*HPOM_management_server*>:9663**
HPOM 管理 UI インストールガイド	本書では、管理 UI のインストール、基本設定、トラブルシューティングについて説明します。
HPOM Administration UI Administration and Configuration Guide	本書では、管理 UI の設計、設定、保守、トラブルシューティングについて説明します。
HPOM Administration UI User Guide	本書では、管理 UI ソフトウェアの使用方法について説明します。
HPOM Administration UI Performance and Scalability Guide	本書では、管理 UI を実行する環境の設計と設定に関する情報と推薦事項を説明します。
HPOM 管理 UI リリースノート	本書では、管理 UI の新しい機能を示し、インストールのヒントと製品の既知の問題に関する情報と回避策を提供します。

HPOM オンラインヘルプ

ここでは、HP Operations Manager (HPOM) 管理者および HPOM オペレータを対象とした、Java グラフィカルユーザーインタフェース (GUI) のオンラインドキュメントについて説明します。

HPOM 管理者 GUI のオンラインヘルプ

HPOM 管理者 GUI のオンラインヘルプは、グラフィカルユーザーインタフェースに表示されている個々のページ、メニュー、オプションの状況に合わせた情報を提供します。メニューおよびメニューオプションは、作業中のデータコンテキストに応じて変わります。HPOM 管理 UI オンラインヘルプは、次のデータコンテキストに関する情報を提供します。

- UNIX 用 HPOM

  UNIX 用 HP Operations Manager データコンテキストで作業する際の、ユーザーインタフェースを説明します。UNIX 用 HPOM データコンテキストでは、UNIX 用 HPOM に関連するすべてのオブジェクト (ノード、ポリシー、カテゴリ、アプリケーション、ユーザー、メッセージグループなど) を管理します。

- サーバー

  *サーバー*データコンテキストで作業する際の、ユーザーインタフェースを説明します。データサーバーコンテキストでは、ローカルまたは現在選択しているサーバー上で、新しいジョブの追加、作業の管理、ログファイルの詳細の参照を実行できます。

- 管理

  管理データコンテキストで作業する際の、ユーザーインタフェースを説明します。*管理*データコンテキストでは、HPOM 管理 UI にログインしている管理者ユーザー、HPOM 管理 UI で管理しているサーバー、HPOM 管理 UI で使用するライセンスの設定および管理を行います。

管理 GUI オンラインヘルプへのアクセス

HPOM 管理者 GUI (管理 UI) のオンラインヘルプにアクセスするには、以下の手順に従ってください。

1. 対応する Web ブラウザに次の URL を入力して、HPOM 管理者用ユーザーインタフェースを起動します。

   - 標準の接続

     `http://localhost:9662`

   - セキュアな接続

     `https://localhost:9663`

2. HPOM 管理者 UI にログインします。デフォルトのユーザー名およびパスワードは次のようになります。

   ユーザー名　　**`opc_adm`**

   パスワード　　**`OpC_adm`**

3. 開いた Web ブラウザで、タイトルバーのヘルプアイコンをクリックします。

4. ヘルプを必要とする専門領域 (UNIX 用 HPOM、サーバー、管理など) に対応するリンクを選択します。

5. HPOM 管理 UI で現在表示されているページのコンテキストに応じたヘルプを表示するには、ページ上部右側にあるヘルプアイコンをクリックします。

Java GUI と Service Navigator のオンラインヘルプ

Java GUI のオンラインヘルプには HP Service Navigator (Service Navigator) に関する情報が掲載されており、オペレータが HPOM 製品に慣れ親しんだり、使用したりするために役立ちます。

HPOM Java GUI のオンラインヘルプには、次のような情報があります。

- ❏ 作業

  大切な手順を完了するための操作を手順ごとに説明します。

- ❏ 概念

  主要な概念と製品の基本的な特徴と機能を紹介します。

- ❏ トラブルシューティング

  製品の使用中に発生する共通の問題に対するヒント、こつ、解決策です。

- ❏ 索引

  必要な情報に迅速かつ簡単にアクセスできるトピックリストです。

Java GUI オンラインヘルプへのアクセス

Java GUI のオンラインヘルプにアクセスするには、以下の手順に従ってください。

1. 使用するブラウザを HPOM に設定します。
2. Java GUI を起動し、Java GUI メニューバーで [**ヘルプ**]、[**目次**] の順に選択します。
3. 起動した Web ブラウザで、読みたいトピックを選択します。

1 HPOM の概要

概要

本章ではオペレータを対象として、HP Operations Manager (HPOM) の背景と機能、および構成を紹介します。

対象読者

本章は、HPOM オペレータを対象としています。

本章の内容

本章で説明する内容は次のとおりです。

- ❏ HPOM の概念
- ❏ HPOM の特徴
- ❏ HPOM の機能
- ❏ HPOM ユーザー

HPOM の概念

HP Operations Manager (HPOM) はシステム管理者のための分散型クライアント - サーバーソフトウェアで、あらゆる企業のネットワーク、システム、およびアプリケーションで発生した問題 (障害) の検出、解決、および防止を支援するツールです。HPOM は拡張性に富む柔軟なソリューションで、種々の情報テクノロジー (IT) 部門のニーズにこたえます。さらに、HPOM のパートナー企業や他の企業で開発された管理アプリケーションを統合して、HPOM を拡張できます。

HPOM がもたらすメリット

HPOM は、次に挙げる点で優れた効果を発揮します。

- **ネットワークの最大化**

  ネットワークコンポーネントの可用性を最大化します。

- **ダウンタイムの短縮**

  システムダウンタイムによって生じるエンドユーザーの時間のロスを軽減します。

- **作業負荷の軽減**

  障害を自動的に解決することで不要なユーザーアクションを削減します。

- **障害の防止**

  予防的アクションによって障害の件数を削減します。

- **遅延の短縮**

  障害の解決に必要な時間を短縮します。

- **コストの削減**

  クライアント - サーバー環境の管理コストを削減します。

クライアント - サーバーの概念

HPOM における管理の概念は、**管理サーバー**と**管理対象ノード**の間で行われる通信に基づいています。中央の管理サーバーで実行されるプロセスは、管理領域中の管理対象ノードで実行される **HP Operations エージェントプロセス**と通信を行います。HP Operations エージェントプロセスは管理対象ノードで**イベント**を収集、処理し、必要な情報を **HPOM メッセージ**として管理サーバーに送信します。これに対して管理サーバーは**アクション**で応じ、管理対象ノード上の障害を防止または修復します。

31 ページの図 1-1 は HPOM における管理の概念を示しています。

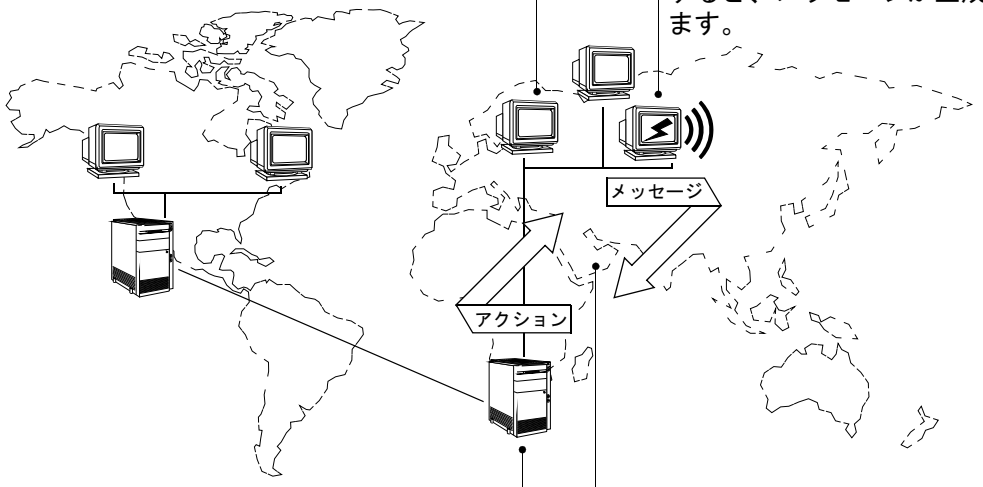
図 1-1　　HPOM におけるクライアント - サーバーの概念

管理対象ノード

管理対象ノードは HP Operations 管理サーバーによってモニター / 制御されています。

イベント

イベントは管理対象ノードで生じる事象です。イベントが発生すると、メッセージが生成されます。



管理サーバー

HP Operations 管理サーバーは中核となるコンピュータです。すべての管理対象ノードは管理サーバーにメッセージを転送します。同じ管理担当範囲を複数の管理サーバーに共有させることもできます。

通信

管理対象ノードと管理サーバーの間では、メッセージとアクションがやりとりされます。

管理サーバー上のエージェントは、**ローカル管理対象ノード**としても機能します。

データベースは、すべてのメッセージと設定データの一元的なデータリポジトリとして機能します。この実行時データと履歴データを使ってレポートを生成できます。履歴データを利用することで、同じようなイベントによって生じる障害をオペレータが解決する際に参照する指示や、特定の障害解決プロセスを自動化するための指示を作成することもできます。データベースプロセスは管理サーバー上で実行されます。

管理サーバー

管理サーバーは HPOM の一元処理機能を受け持ちます。ソフトウェアパッケージは、完全かつ最新の設定も含めて全体が管理サーバーに格納されます。

管理サーバーによって実行される処理は次のとおりです。

- ❑ **データの収集**

  管理対象ノードからデータを収集します。

- ❑ **メッセージの管理**

  メッセージを管理 / グループ化します。

- ❑ **アクションの管理**

  指定されているエージェントを呼び出して次の処理を実行します。

  - *アクションの開始*

    管理対象ノード上でローカル自動アクションを開始します。

  - *セッションの開始*

    管理対象ノード上でセッション (仮想コンソールを開くなど) を開始します。

- ❑ **履歴の管理**

  メッセージおよび実行されたアクションを格納した履歴データベースを制御します。

- ❑ **メッセージの転送**

  他の管理サーバーや HPOM が実行されているシステムにメッセージを転送します。

- ❑ **ソフトウェアのインストール**

  管理対象ノードに HP Operations エージェントソフトウェアをインストールします。

設定が変更された場合も、管理サーバーはそれを管理対象ノードに通知し、更新を開始します。

管理対象ノード

管理対象ノードとは、HPOM によって制御 / モニターされるコンピュータです。HPOM は、エージェントソフトウェアのインストールと実行を通じてこれらのノードを管理します。

メッセージの捕捉

HP Operations エージェントソフトウェアをインストールして実行すると、エージェントはログファイルと SNMP トラップを読み取ります。また、管理対象ノード上のアプリケーションが出力するメッセージを **HPOM メッセージインターセプタ**で捕捉するように設定できます。

パフォーマンスのモニター

パフォーマンス値を**調節可能な間隔でモニターし**、パフォーマンスが制限値から外れたときにメッセージを生成できます。

HPOM は **HPOM 自体のプロセス**もモニターできます。

メッセージの比較

HP Operations エージェントは、あらかじめ設定されているポリシーの条件とすべてのメッセージを比較します。重要でないメッセージは無視されますが、予測されていなかったメッセージや重要なメッセージは管理サーバーに転送されます。また、重複するイベントや類似したイベントを除外するように設定することもできます。**メッセージのフィルタリング**ポリシーを指定するには、既存のポリシーを修正するか、ポリシーと条件の独自のセットを設定します。

メッセージのロギング

すべてのメッセージは、管理対象ノード上のローカル**ログに記録**するか、管理サーバー上の履歴データベースに直接書き込むことができます。この履歴機能により、システムの設定によって重要でないと判断されたメッセージも含め、すべてのメッセージを調べることができます。

メッセージのバッファリング

管理サーバーに到達できなかったメッセージは、管理サーバーがそれを受信するまで**ストレージバッファ**で維持されます。

障害の修復

管理対象ノードでは、メッセージに応じて**修復アクション**をローカルに開始し、必要に応じて停止、再開できます。

ノードの設定

HPOM 環境は、制御対象、モニター対象、メッセージ対象、非管理対象など、さまざまな**種類**の管理対象ノードで構成できます。ノードがネットワークに属すようになった時点、または手動で追加された場合に認識されるように、IP アドレスの範囲を設定することもできます。

基本的な権限とユーザータイプ

ファイルやフォルダのデフォルトのセキュリティ設定は、各ユーザーグループに付与する権限を整理することで表現できます。

基本的な権限

ファイルやフォルダに対する権限は、対象となるファイルやフォルダにどのようにアクセスしたり変更したりできるかを示すものです。この権限は、基本的なユーザータイプだけでなく、アクセス制御リスト (ACL) のすべてのデフォルトタイプにも適用されます。基本的な権限を変更したり、ACL を設定 / 変更したりできるのは、そのファイルやフォルダの所有者のみです。

読み取り権限

オブジェクトにアクセスして内容を検索、コピー、表示できます。

書き込み権限

ファイルについては、ファイルにアクセスして内容を変更できます。フォルダについては、フォルダにアクセスしてオブジェクトを作成 / 削除できます。

実行権限

ファイルについては、ファイル (実行ファイル、スクリプト、アクションなど) にアクセスして実行できます。フォルダについては、フォルダにアクセスしてその内容を検索 / リスト表示できます。

作成したオブジェクトが誤って上書きされないように保護しつつ、どのユーザーも使用できるようにするには、次のように設定します。

ファイルのプロパティを変更し、所有者、グループ、およびその他のユーザーに読み取り権限と実行権限を付与します。書き込み権限は付与しません。

基本的なユーザータイプ

ファイルやフォルダに対する基本的な権限は、次の 3 タイプのユーザーに分けて適用されます。

所有者 ファイルやフォルダを所有しているユーザー。ファイルやフォルダの所有者を変更できるのは、システム管理者 (root ユーザー) のみです。

グループ システム管理者によってグループとしてまとめられた複数のユーザー。たとえば、ある部署のメンバーが同じグループに属しているとします。このグループが所有グループであり、通常は、ファイルやフォルダの所有者をここに所属させます。

その他 そのシステムにおける、所有者や所有グループ以外のすべてのユーザー。

たとえば、あるフォルダを非公開にするには、フォルダのプロパティを変更し、自分自身 (所有者) に読み取り、書き込み、実行権限を割り当て、グループやその他のユーザーには権限を一切付与しないようにします。自分自身にこれらの権限を割り当てると、自分と root ユーザー以外はフォルダの内容を表示できなくなります。

HPOM の特徴

HPOM は、コンピューティング環境で生じる問題 (障害) を予防的に解決する上で役立ちます。ネットワーク要素、システム、アプリケーションから構成される、異機種の混在する分散環境では、問題はどこで発生してもおかしくありません。

障害の登録

障害が発生しそうになると、HPOM は事前にその旨を通知し、発生を回避するために必要なリソースを提供します。同様に、障害が実際に発生した場合も HPOM はそれを直ちに通知し、解決に必要なリソースを提供します。

たとえば、未許可ユーザーが管理対象ノードへのログオンを試みると、ノードはいずれかの方法でその問題を登録します。このとき、ノードはシステムログファイルにエントリを書き込む、SMNP トラップを送信する、またはアプリケーションプログラミングインタフェース (API) を利用して管理サーバーと直接通信することができます。

この例では、未許可ユーザーのログオンにより、ログファイルにエントリが書き込まれます。HPOM はこのログファイルを読み取り、あらかじめ設定されている条件に基づいて、メッセージを生成するかどうかを判断します。メッセージを生成する場合、HPOM はログファイル内のエントリを使って内容のあるメッセージを作成し、属性 (追加情報) をメッセージに付加し、完成したメッセージを管理サーバーに送ります。

障害の解決

管理サーバーでは、メッセージはブラウザに表示されます。メッセージには、障害の重要度、障害が発生した場所 (該当管理対象ノード)、メッセージが生成された原因が記載されています。該当イベントに設定されている応答アクションの種類によっては、メッセージが着信すると管理対象ノード上で直ちに自動アクションが実行されます。また、着信したメッセージによって、手動による修復アクションの開始をユーザーに指示する別のメッセージが生成される場合もあります。

解決方法のドキュメント化

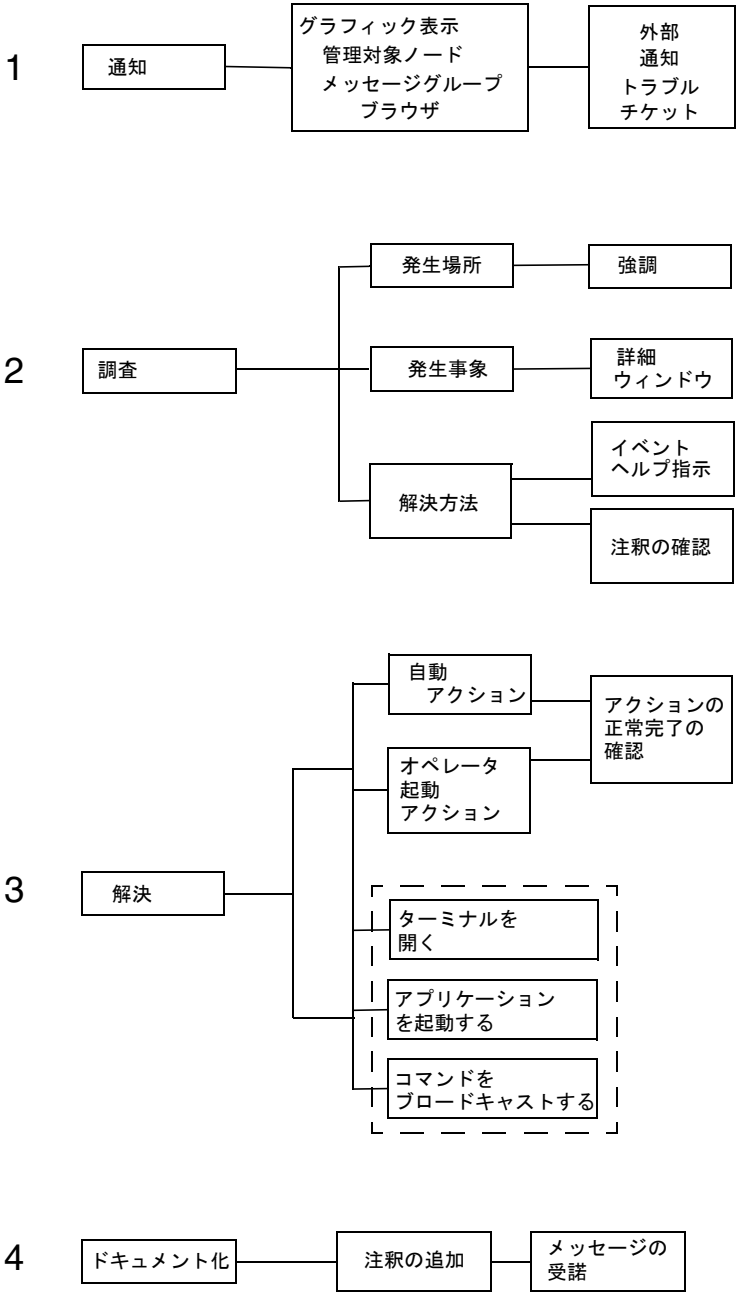
アクションが正しく完了した後で、ユーザーはメッセージに注釈コメントを付加し、それを受諾することで注釈付きメッセージを履歴データベースに保存できます。

レポートの生成

未許可ユーザーのログオンと、それに関連するアクションについての情報を見つけやすくするために、データベースに記録されている情報からレポートを生成することもできます。

38 ページの図 1-2 は障害解決の主な要素を示しています。各要素の詳細は、『*HPOM Java GUI オペレータガイド*』で説明されています。

図 1-2　　障害解決の要素


1
通知
グラフィック表示
管理対象ノード
メッセージグループ
ブラウザ
外部
通知
トラブル
チケット
2
調査
発生場所
強調
発生事象
詳細
ウィンドウ
解決方法
イベント
ヘルプ指示
注釈の確認
3
解決
自動
アクション
アクションの
正常完了の
確認
オペレータ
起動
アクション
ターミナルを
開く
アプリケーション
を起動する
コマンドを
ブロードキャストする
4
ドキュメント化
注釈の追加
メッセージの
受諾

次に、障害解決の要素を説明した 38 ページの図 1-2 の主要事項について説明します。

1. **通知**

   HP Operations エージェントはログファイルとシステムアクティビティをモニターします。

   障害が発生すると、HP Operations エージェントは次のいずれかの方法で通知します。

   - 管理サーバーにメッセージを送信する。
   - 障害の重要度に応じてノードアイコンの色を変更する。
   - メッセージのステータスに応じてメッセージブラウザの [重要度] フィールドの色を変更する、または (設定されている場合は) メッセージ行全体の色を変更する。
   - メッセージと属性 (送信日時、アクションのステータスなど) を表示する。
   - 外部通知サービスまたはトラブルチケットサービスにメッセージを転送する (設定されている場合)。

   障害の重要度と影響を受けるオブジェクトを一目で確認できます。その上で障害の詳細を確認し、それを解決できます。

2. **調査**

   障害とその原因について理解します。大規模な環境では、障害を迅速に特定できるかどうかが重要です。

   HPOM では、HPOM システムとネットワーク管理画面の高速リンクによって、環境内で発生した障害を効率的に特定できます。

3. **解決**

   障害を解決するための修復アクションを開始します。

   HPOM では次の解決方法を利用できます。

   - *自動アクション*

     エラーメッセージを受信すると、HPOM は自動的に修復アクションを開始します。自動アクションは、必要に応じて何度でも手動で再実行できます。

注記

自動アクションでサービス ID を使用するには、変数 *<$MSG_SERVICE>* を使用します。

- *オペレータ起動アクション*

  エラーメッセージを受信してそれを確認したオペレータは、手動による修復アクションを直ちに開始できます。この修復アクションは、手動で停止することもできます。

- *ユーザー指示*

  ユーザーに送信するエラーメッセージには、障害を解決するための具体的な指示を添付できます。指示には、障害の解決方法を具体的に記載する必要があります。

- *履歴ログ*

  関連する問題の履歴ログ (メッセージの注釈を含みます) を精査し、類似した問題や、過去に発生した同じ問題をどのように解決したかを調べることもできます。

- *Java GUI コンソール*

  Java GUI コンソールでは、さまざまな種類のアプリケーションを起動したり、複数のシステムにコマンドをブロードキャストできます。また、影響を受けたシステム上で仮想コンソールや物理コンソールを直接開き、Java GUI コンソール自体から修復アクションを実行できます。

4. **ドキュメント化**

   障害処理が終了したら、解決方法をドキュメント化します。ドキュメント化しておけば、必要になったときに効率的に参照できます。

HPOM の機能

HPOM の主な目的は、異機種の混在する分散環境でシステムをモニター、制御、管理することです。

HPOM は、次のタスクを通じてこれらのことを行います。

- **イベント**

  環境内で発生したイベントを通知します。

- **レポート**

  イベントを説明するメッセージまたはレポートを生成します。

- **アクション**

  イベントに対処するためのアクションを実行します。

HPOM はユーザーとのコミュニケーションにメッセージを利用します。メッセージとは、システム内に存在する特定の管理対象ノードのシステムステータス、システムイベント、または障害に関する情報を構造化し、判読可能な形式で表現したものです。管理対象ノードでステータスの変化、イベント、または障害が発生すると、HPOM はメッセージを送信して通知します。メッセージ生成の原因となったイベントが障害の場合、HPOM は障害を修復するためのアクションを開始できます。元のメッセージ、修復アクションの結果、その他の関連情報 (ユーザーが付加する注釈など) はデータベースに記録されます。

イベント

イベントとは、コンピューティング環境内のオブジェクトで発生した特定の障害または事象を意味します。一般に、イベントはステータスの変化またはしきい値違反を表します。たとえば、用紙トレイが空になると、プリンタのステータスは変化します。同様に、使用できるディスク容量が特定レベルを下回った場合はしきい値違反となります。このような事象は、いずれもイベントです。これらのイベントごとにメッセージを作成できます。

イベントの多くは修復が必要な障害です。ただしユーザーアクションを必要としないイベントもあります。たとえば、ユーザーがシステムにログオン / ログオフすると、システムのステータスが変化し、イベントが発生します。しかし、このようなイベントに対してはユーザーの対応は必要ありません。

イベントの相関処理

イベントが生じるとメッセージが生成されます。システムで発生するイベントが多いほど、ユーザーに送信されるメッセージも多くなります。イベントの大量発生 (イベントストーム) は管理サーバーに過剰な負荷をかけ、担当するオペレータが対応しきれなくなる場合があります。

イベント相関処理 (EC) を行うことで、「イベントストリーム」と呼ばれるイベントグループをリアルタイムで処理できます。このリアルタイム処理はイベントストリーム間の関係を識別し、より有用で管理しやすい情報のみで小さなストリームを作成します。この情報を利用することで、障害をより効率的に診断 / 解決できます。イベント相関処理では、重複するイベントや関連するイベントが排除され、一連の関連メッセージは 1 つのメッセージに置き換えられます。

サポートされるエージェントおよび管理サーバープラットフォームについては、『*HPOM システム管理リファレンスガイド*』を参照してください。HPOM のイベント相関処理の仕組みについては 181 ページの第 4 章「メッセージポリシーの導入」で詳しく説明します。HPOM でイベント相関処理を設定する方法については、『*HPOM システム管理リファレンスガイド*』を参照してください。

メッセージ

メッセージは、イベントに起因する構造化された情報のまとまりです。HPOM はイベントを検知し、メッセージを作成してイベントを通知します。

メッセージの捕捉

HPOM は、次のようなさまざまなソースからのメッセージを捕捉します。

- ❑ **ログファイル**

  ログファイルエンキャプスレータは、アプリケーションとシステムのログファイル (イベントログなど) からメッセージ情報を抽出します。

- ❑ **SNMP イベント**

  SNMP イベントインターセプタは、管理サーバー上および指定したエージェントプラットフォーム上のイベントを取り込みます。詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

- **HPOM メッセージ**

  メッセージインタフェースとして機能する HPOM のコマンドや API (`opcmsg(1|3)`) を使うことで、メッセージを明示的に生成できます。

- **モニター対象オブジェクト**

  モニター対象オブジェクトにはしきい値レベルを設定できます。モニター対象オブジェクトの測定値が指定のしきい値から外れると、HPOM はメッセージを生成します。

- **ユーザーアプリケーション**

  ログファイルにメッセージを出力するすべてのアプリケーションは、HPOM API を使うか SNMP トラップを送信して HPOM に情報を提供できます。

メッセージへのポリシー条件の適用

HPOM は、検出されたイベントに対してポリシー条件を適用します。ポリシー条件はフィルターのように機能し、メッセージを生成するか、イベントを無視するかを判定します。メッセージを生成する場合、HPOM ではユーザーが理解できるフォーマットへの変更など、メッセージの構成に大幅な変更を加えることができます。障害を通知するメッセージでは、その障害を解決するためのアクションを定義できます。

メッセージの論理的な関連付け

メッセージは、相関出力に添付される 1 つまたは複数のメッセージおよび自動アクションと論理的に関連付けることができます。HPOM が内蔵する標準のメッセージ相関処理とフィルターケーパビリティについては、228 ページの「メッセージの最適なフィルタリングのための方針」を参照してください。

メッセージの処理

HPOM はメッセージを使って次のことを行います。

- イベントに関する情報を伝える。
- 環境内のステータスの変化をユーザーに通知する。
- 修復アクションを開始する。

図 1-3 は HPOM がどのようにメッセージを処理するかを示しています。

図 1-3　メッセージの処理フロー

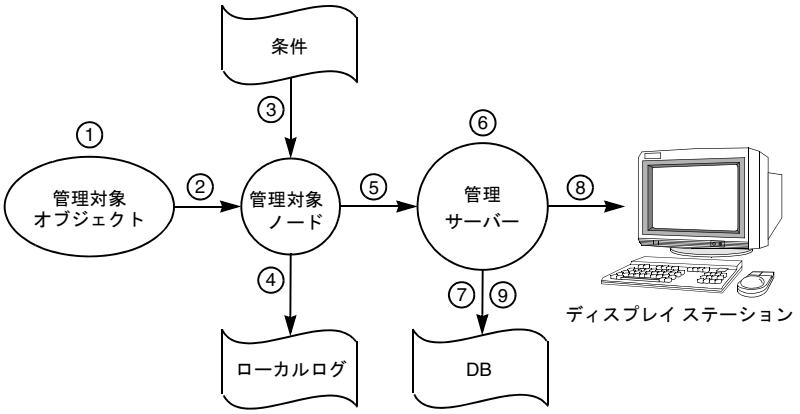


図 1-3 に示されるように、メッセージは次のように処理されます。

1. **管理対象オブジェクトでの生成**

   管理対象オブジェクトでイベントが発生すると、メッセージが生成されます。たとえば、テープが正しくロードされていないことが原因でバックアップに失敗すると、メッセージが生成されます。

2. **管理対象ノードでの受信**

   管理対象ノード上の HP Operations エージェントがメッセージを受信します。

3. **転送または除外**

   メッセージはフィルターと比較されます。除外条件と一致するメッセージ、および重複するメッセージは除外されます。その他のメッセージは転送されます。

4. **ログへの記録**

   HPOM を適切に設定しておくことで、メッセージをローカルログに記録できます。

5. **管理サーバーへの転送**

   フィルターと一致するメッセージは HPOM メッセージフォーマットに変換され、管理サーバーに転送されます。設定されている場合は、ローカルアクションが開始されます。

6. **管理サーバーによる処理**

   管理サーバーは、次のいずれかの方法でメッセージを処理します。

   - *グループ替え*

     メッセージを自動的に別のメッセージグループに割り当てます (グループ替え)。

   - *アクションの開始*

     メッセージに設定されている非ローカルアクションを指定のノードで自動的に開始します。

   - *転送*

     外部通知インタフェースとトラブルチケットサービスにメッセージを転送します (HPOM がそのように設定されている場合)。

   - *バッファリング*

     ペンディングメッセージブラウザにメッセージをバッファします (HPOM がそのように設定されている場合)。

7. **データベースへの保存**

   アクティブメッセージはデータベースに記録されます。

8. **表示**

   メッセージは 1 つまたは複数の HPOM ディスプレイステーションの [メッセージブラウザ] ウィンドウに表示されます。

9. **履歴データベースへの保存**

   受諾されたメッセージはアクティブブラウザから削除され、履歴データベースに記録されます。

オペレータがメッセージにどのように対応するかについては、『*HPOM Java GUI オペレータガイド*』を参照してください。

管理者によるメッセージとアクションの設定については 57 ページの第 2 章「HPOM の設定と保守」を参照してください。

メッセージの管理

HPOM のメッセージ管理機能は、メッセージを論理的に関連したグループにまとめます。関連するさまざまなソースからのメッセージがグループ化されるので、管理対象オブジェクト / サービスのクラスに関するステータス情報が提供されます。たとえば、BACKUP というメッセージグループを用意して、バックアップアプリケーションやテープドライブなどのソースからの、システムのバックアップに関連するすべてのメッセージをグループ化できます。

メッセージのフィルタリング

重要な情報が明確に表示されるように、メッセージを分類およびフィルタリング (肯定 / 否定) することもできます。

- ❏ **肯定的フィルター**

  指定のパターンと一致するメッセージをオペレータに転送します。

- ❏ **否定的フィルター**

  別の指定パターンと一致するメッセージを除外します。

除外されたメッセージはローカルログファイルに保存できます。ログファイルは、傾向の分析、フィルター適用性の確認、管理対象オブジェクトのステータスパターンのトラッキングに利用できます。

非該当メッセージの分類

HPOM は、フィルターと一致しないメッセージを「非該当」として分類します。多くの場合、非該当メッセージは新規または未定義のソースで発生します。非該当カテゴリは、関連メッセージの分類が不可能であることを意味します。

非該当メッセージに対しては、次の 3 種類の対応方法があります。

- ❏ ローカルログに記録する。
- ❏ 管理サーバーに転送する。
- ❏ 無視する。

メッセージのフォーマット

一元管理システムに転送されるすべてのメッセージは、メッセージブラウザで同じフォーマットを使用します。HPOM は、メッセージを重要度ごとに色分けして表示します。デフォルトでは、メッセージブラウザの [**重要度**] 列のみが重要度に応じて色分け表示されます。また、HPOM の設定を変更し、メッセージブラウザの各メッセージ行全体を色分け表示することもできます。さらに、ポケットベルや自動呼出しシステムなど、外部の通知サービスを起動するように設定することもできます。

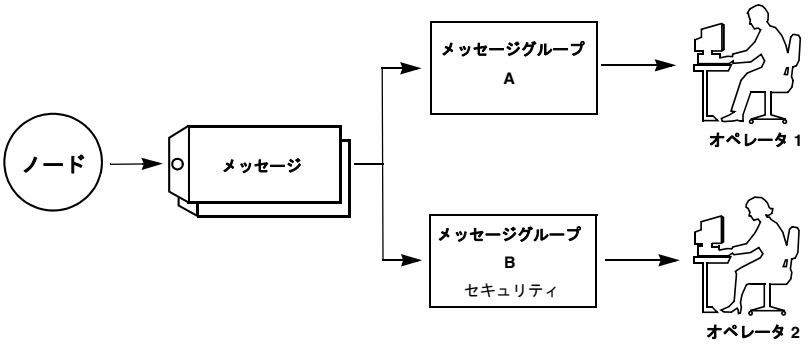
メッセージへの対応

オペレータは、まず、メッセージブラウザを使用して各メッセージを確認し、それに対応します。メッセージブラウザでは、あらかじめ設定されている修復アクションの可用性やステータスなど、メッセージに関連するすべての情報を確認できます。これらの情報や、その他のアクションをドキュメント化するためのサービスも表示されます。

メッセージグループの定義

HPOM の管理者は、機密性の高いアプリケーション / 機能からのメッセージを、1 つのメッセージグループに割り当てることができます。図 1-4 の例では、アクセス制限が必要な機密メッセージを出力する 1 つのノードの管理担当範囲を 2 人のオペレータが共有しています。ネットワークのセキュリティは、アクセス制限が必要なメッセージを *Security* というメッセージグループに割り当て、さらにこのグループをセキュリティ権限のあるオペレータに割り当てることによって維持されています。もう 1 名のオペレータはセキュリティ権限を持たないため、*Security* グループのメッセージを表示できません。

図 1-4　　1 名のオペレータのみに送信される機密メッセージ



アクション

アクションは、メッセージへの対応です。メッセージ生成の原因となったイベントが障害の場合、HPOM は障害を修復するためのアクションを開始できます。

アクションは、同一ノードでの毎日のアプリケーションの起動など、日常の作業にも使用されます。アクションには、シェルスクリプト、プログラム、コマンド、アプリケーション起動、および必要とされるその他の応答などがあります。

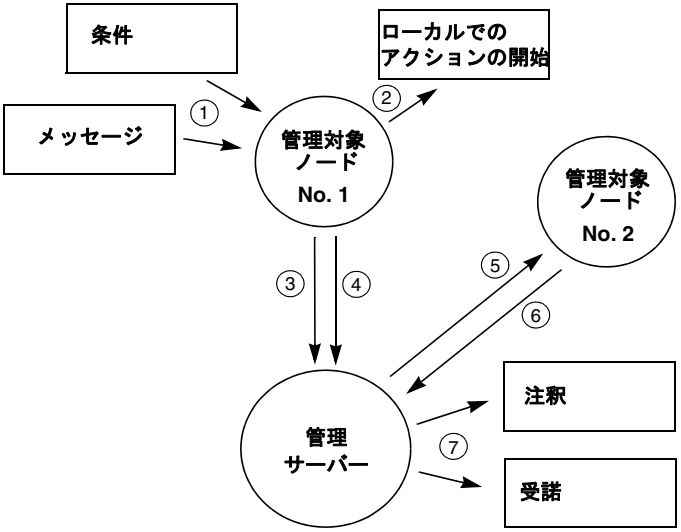
HPOM には次の種類のアクションがあります。

- ❏ 自動アクション
- ❏ オペレータ起動アクション
- ❏ アプリケーション

自動アクション

自動アクションは、メッセージと関連付けてあらかじめ設定されている、障害への対応です。自動アクションにはオペレータの操作は必要なく、メッセージが着信すると HPOM によって直ちに開始されます。オペレータは必要に応じて自動アクションを手動で停止、再開できます。

図 1-5　自動アクションの開始



49 ページの図 1-5 に示されるように、自動アクションは次のように実行されます。

1. **メッセージの捕捉**

   定義されている条件に応じて管理対象ノードでメッセージが捕捉されます。

2. **アクションの開始**

   アクションの対象となるノードが*ノード No.1* の場合、アクションはローカルに開始されます。

3. **結果の通知**

   ノード No.1 がアクションの結果を管理サーバーに通知します。

4. **管理サーバーへの通知**

   アクションの対象ノードが*ノード No.2* の場合、*ノード No.1* は管理サーバーに通知します。

5. **アクションの開始**

   管理サーバーがアクション開始の指示を*ノード No.2* に送信します。

6. **結果の通知**

   ノード No.2 がアクションの結果を管理サーバーに通知します。

7. **注釈のロギング**

   メッセージの設定によっては、自動アクションの実行結果は管理サーバーに送信され、そこで注釈としてログに記録されます。アクションが正しく完了した後で、ロギングを自動的に受諾することもできます。

オペレータ起動アクション

自動アクションと同様に、オペレータ起動アクションは、メッセージと関連付けてあらかじめ設定されている、障害への対応です。これらのアクションは、オペレータによって開始 / 停止されます。

管理者がメッセージに対して自動アクションではなく、オペレータ起動アクションを選択するのには、次のような理由があります。

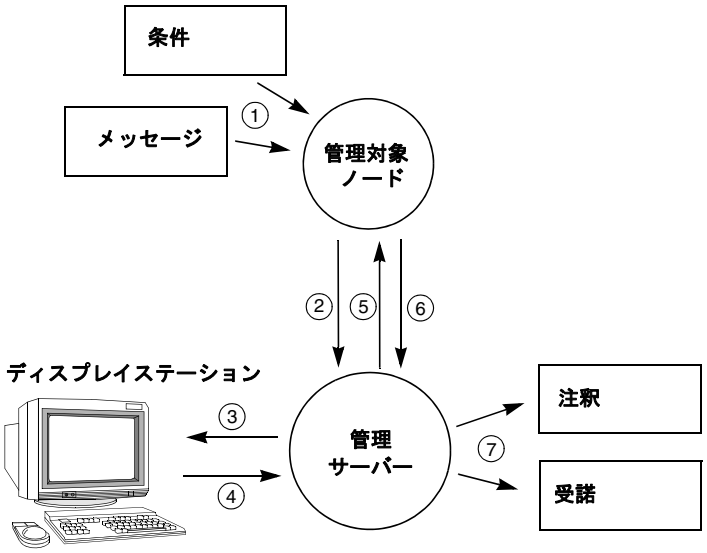
- ❑ **手動操作**

  アクションの実行時にオペレータが手動操作を実行しなければならない可能性がある。

- ❑ **前提条件**

  アクションを開始するかどうかが環境内の条件によって異なり、オペレータが最初にそれを確認する必要がある。

図 1-6　　オペレータ起動アクションの開始



51 ページの図 1-6 に示されるように、オペレータ起動アクションは次のように実行されます。

1. **捕捉**

   設定されている条件に応じて管理対象ノードでメッセージが捕捉されます。たとえば、メッセージによってオペレータ起動アクションまたは自動アクションが開始される場合があります。

2. **転送**

   管理サーバーにメッセージが転送されます。

3. **表示**

   担当オペレータのディスプレイステーションにメッセージが送信されます。そのメッセージにオペレータ起動アクションがあらかじめ設定されていることが [メッセージブラウザ] ウィンドウのメッセージ属性によって示されます。

4. **アクション**

   オペレータはメッセージブラウザ上のボタンをクリックしてアクションを開始します。

5. **指示**

   アクション開始の指示が管理対象ノードに送信されます。

6. **通知**

   管理対象ノードがアクションの結果を管理サーバーに通知します。

7. **ロギングと受諾**

   オペレータ起動アクションの実行に関する注釈は、設定によっては管理サーバーに送信され、そこでログに記録されます。アクションが正しく完了すると、メッセージは自動的に受諾されます (メッセージがそのように設定されている場合)。

アプリケーション

アプリケーションは、HPOM に統合されているスクリプトまたはプログラムです。メッセージと直接関連付けられ、ブラウザウィンドウから開始 / 停止できるオペレータ起動アクションや自動アクションとは異なり、アプリケーションはオペレータの `Applications` フォルダに用意されているツールです。詳細については、『*HPOM Java GUI オペレータガイド*』を参照してください。

HPOM ユーザー

HPOM ユーザーの概念では、HPOM 管理者や HPOM オペレータのような実際のユーザーはユーザープロファイルによって区別されます。ユーザープロファイルは抽象ユーザーの設定を表します。実際のユーザー設定には、これらの抽象ユーザー設定が使用されます。

ユーザーロール

HPOM の主なユーザーロールは次のとおりです。

- **HPOM 管理者**

  無制限の権限を持つユーザーです。主に、HPOM ソフトウェアのインストールと設定、および初期の運用方針と手順の設定を担当します。

- **オペレータ**

  権限を持たないユーザーです。日常的に HPOM を使用し、システムとオブジェクトの保守、管理、モニター、制御を行います。

複数オペレータ

HPOM では、組織の規則や要件に応じて、複数のオペレータが 1 つの管理システムで作業できます。オペレータには、各自の知識や技能に応じて特定の担当範囲とケーパビリティが割り当てられます。HPOM で管理するコンピューティング環境の規模によっては、前述の 2 つのロールを 1 名のオペレータが担うこともできます。

アクセス制限

HPOM ユーザーインタフェースへのアクセスは制限されています。どのオペレータ / 管理者も、カスタマイズされた HPOM ユーザーインタフェースにアクセスするには正しいログオン名とパスワードを指定する必要があります。この HPOM パスワードは、オペレーティングシステムへのログオン名 / パスワードとは別のものです。

ユーザープロファイル

ユーザープロファイルは、HPOM ユーザーが多数存在する大規模で動的な環境で便利です。抽象ユーザーのプロファイルを設定し、そのプロファイルを実際の HPOM ユーザーにデフォルトのプロファイルとして割り当てることができます。プロファイルを使用することで、ユーザーにデフォルト設定を迅速に割り当てることができます。必要に応じていくつものプロファイルを作成し、ユーザープロファイル階層として整理しておくことができます。詳細については 108 ページの「ユーザープロファイルの設定」を参照してください。

管理者

HPOM 管理者 (`opc_adm`) は HPOM 作業環境内で多くの作業を行い、責任を負います。

管理者が行うことは次のとおりです。

- **ユーザー環境のカスタマイズ**

  各ユーザーのカスタム環境を定義します。インストール、設定、カスタマイズのすべてが適合するように管理します。オペレータ、ノード、取り込むメッセージなどは、システムとの適合に応じて追加 / 変更されます。

- **オペレータ効率の最大化**

  特定のイベントと修復アクションを一致させ、その他のイベントの個々の指示を提供します。

- **担当範囲の委譲**

  担当範囲とケーパビリティのセットを定義し、割り当てられたノードの管理と必要作業の実行にオペレータが使用するツールを決定します。

- **ガイドラインの作成**

  メッセージポリシーを導入するためのガイドラインを作成します。管理者はポリシーまたはポリシーグループの担当範囲を定義します。

- **履歴の維持**

  HPOM 履歴データの保守とチェックを行います。この履歴のトラッキングにより、管理者は自動 / オペレータ起動アクションを適切に修正 / 作成し、具体的なイベント対応指示を作成し、繰り返される障害を特定できます。たとえば、履歴データをチェックすることで、ディスク容量の使用率が常に高いノードを見つけることができます。

- **ユーザーの問題の解決**

  任意のオペレータとして操作することでそのオペレータの設定を確認し、システムでそのオペレータが遭遇している問題の解決を手助けします。

- **HPOM の拡張**

  アプリケーションやモニター対象オブジェクトを新たに統合して HPOM の機能を拡張し、サービスの提供形態や呼び出し方法の一貫性が損なわれないように、追加したアプリケーションを登録します。

- **HPOM の保守**

  ソフトウェアの保守を行い、管理手順とセキュリティポリシーを定義します。HPOM のセキュリティの詳細については 60 ページの「環境の保護」または『*HPOM システム管理リファレンスガイド*』を参照してください。

オペレータ

HPOM オペレータ (opc_op) はシステム管理機能を制御します。オペレータの作業環境は、管理対象ノードの集合から構成されます。アプリケーションの起動など、オペレータの日々の作業の基盤となるのはこれらのノードです。オペレータが障害の解決に利用する情報もノードから提供されます。

HPOM オペレータには、各自の管理対象環境のカスタムビューが提供されます。たとえば、あるオペレータは施設内のすべてのノードを担当します。別のオペレータは別の施設の一部のノードを担当します。環境が作業ベースで構成されるため、HPOM オペレータには各自が制御するシステムとオブジェクトからの情報のみが表示されます。

デフォルトの HPOM オペレータの詳細については 102 ページの「ユーザーとユーザープロファイルの設定」を参照してください。

2 HPOM の設定と保守

概要

本章では、管理対象ノードやノードグループ、メッセージグループ、アプリケーション、オペレータなど、HP Operations Manager (HPOM) のさまざまな要素を設定する方法について説明します。

対象読者

本章は、HPOM *管理者*を対象としています。

本章の内容

本章では、HPOM 管理者向けに次の各トピックについて説明します。

- ❏ 管理者環境
- ❏ 環境の保護
- ❏ 管理対象ノードの構成
- ❏ HPOM でのポリシーの管理
- ❏ HPOM でのサブエージェントの管理
- ❏ メッセージグループの構成
- ❏ アプリケーションの構成
- ❏ HPOM ライセンス
- ❏ ユーザーとユーザープロファイルの設定
- ❏ HPOM 設定の更新
- ❏ データのバックアップと復元
- ❏ メッセージの所有権
- ❏ レポートの生成

管理者環境

HPOM 管理者環境は、HPOM オペレータ環境の上位セットです。管理者は、オペレータが利用できるすべての GUI と設定にアクセスできるだけでなく、それ以外の管理ケーパビリティやコマンド行ツールも利用できます。

HPOM 管理者が設定する主な HPOM 要素は次のとおりです。

- ❏ 登録ノード階層
- ❏ 登録ノードグループ
- ❏ 登録メッセージグループ
- ❏ 登録アプリケーション
- ❏ 登録ユーザー
- ❏ 登録ユーザープロファイル
- ❏ メッセージソースポリシー

HPOM には管理者用の Web ベースの GUI も用意されています。これは、以前の Motif ベースの UI に代わるものです。Configuration Value Pack Light (CVPL) ソフトウェアが導入されました。CVPL のユーザードキュメントは次の場所の HP Operations Manager for UNIX ディレクトリでダウンロードできます。

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

環境の保護

環境を保護するには、次の項目を調べる必要があります。

- ❑ **システムのセキュリティ**

  全体的なセキュリティを改善するには、まず、システムのセキュリティに注目し、その上でネットワークのセキュリティに関連する問題を調査します。システムのセキュリティでは、HP Operations 管理サーバーおよび管理対象ノードを信頼されたシステムで実行するために解決しなければならない問題が対象となります。システムレベルのセキュリティポリシーの詳細については、該当するオペレーティングシステムの製品ドキュメントを参照してください。

- ❑ **ネットワークのセキュリティ**

  ネットワークのセキュリティでは、管理サーバーと管理対象ノードの間でやり取りされるデータの保護などが対象となります。HPOM では、接続の当事者を確実に認証することで、このデータを保護します。ネットワークのセキュリティの詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

- ❑ **HPOM のセキュリティ**

  HPOM 自体の設定時に生じたセキュリティへの影響を調べる必要があります。アプリケーションの設定 / 実行やオペレータ起動アクションなどについて、セキュリティに関連する事項を確認してください。HPOM ユーザーの作業ディレクトリ、ファイルアクセス、権限の詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

システムのセキュリティ

安全な、または信頼されたシステムは、さまざまな方法により、セキュリティをシステムレベルで改善しています。HPOM 環境を構築、設定する際は、これらのセキュリティ技法を勘案する必要があります。

セキュリティ技法

セキュリティ技法には次のシステムレベルコンポーネントが含まれます。

- **認証**

  パスワードとユーザー認証の厳密な制御

- **監査**

  ネットワーキング、共有メモリ、ファイルシステムなどの監査

- **ターミナルアクセス**

  ターミナルへのアクセスの制御

- **ファイルアクセス**

  ファイルへのアクセスの管理

HPOM のセキュリティを保護する方法

HPOM は、次の方法によりネットワークレベルでデータを保護します。

- **認証**

  接続の当事者の識別情報を検証します。

- **監査**

  正当なソースによって生成された後にメッセージが変更されていないことを検証します。

ネットワークのセキュリティの詳細、特にプロセス間通信に関連する問題に HPOM がどのように対処するかについては、『*HPOM システム管理リファレンスガイド*』を参照してください。

管理対象ノードの構成

管理対象ノードは、HPOM によってモニター / 制御されるシステムです。環境は、さまざまな種類の管理対象ノードから構成できます。

管理対象ノードの構築

HPOM の初期のデフォルト設定では、管理サーバーが唯一の管理対象ノードです。この構成に別のノードを追加します。HPOM の管理環境はこのように構築されます (各種管理対象ノードの詳細については 62 ページの「管理対象ノードの種類」を参照してください)。

HPOM 環境の構築では、コマンド行ツール `opcnode` および `opclaygrp` を使ってノードを整理し、レイアウトグループやノードグループとしてまとめます。詳細については *opcnode (1m)* と *opclaygrp (1m)* のマニュアルページを参照してください。管理対象ノードグループの詳細については 63 ページの「管理対象ノードの構成」を参照してください。

管理対象ノードの種類

管理対象ノードには、完全なシステムとインテリジェントデバイスがあります。

制御対象
制御対象ノードには、すべての管理 / モニター用ケーパビリティを適用できます。

モニター対象
管理情報が収集され、管理サーバーに転送されますが、修復アクション / 操作を開始することはできません。セキュリティのためにノードへのアクセスを制限する場合は、モニター対象ノードが便利です。

メッセージ許容
エージェント / サブエージェントソフトウェアはロードされませんが、メッセージは HPOM で受理されます。たとえば、周辺装置などのインテリジェントネットワークデバイスや、リモートネットワークに属すノードはメッセージ許容ノードである可能性があります。

非管理対象
エージェント / サブエージェントプロセスは開始されません。これらのノードからのメッセージは無視されます。これは、制御対象、モニター対象、またはメッセージ許容ノードの一時的な状態です。

管理対象ノードの構成

管理対象ノードの構成には主に次のグループを使います。

- ❏ **HPOM 登録ノード**

  HPOM 管理環境内のすべてのノードが含まれます。

- ❏ **HPOM 登録ノード階層**

  デフォルトの HPOM ノード階層としての登録ノードが含まれます。

- ❏ **HPOM 登録ノードグループ**

  ノードを論理的な担当範囲グループに整理します。

注記

HPOM ユーザーの設定では、ノードグループを使ってオペレータの担当範囲を設定し、ノード階層を使ってオペレータの**管理対象ノード**グループを構成します。

HPOM 登録ノード

HPOM 登録ノードは HPOM のデフォルト**ノード階層**です。このデフォルト階層には、HPOM で管理 / モニターされるすべてのノードが含まれます。また、HPOM の外部ノードの集合を表すシンボルは、HPOM 登録ノードの一部である場合があります。これらのノードでは HPOM ソフトウェアは実行されませんが、これらのノードからのイベントは受理されます。

ノード階層の詳細については 64 ページの「HPOM ノード階層」を参照してください。

初期状態の HPOM 登録ノードに含まれるのは、管理サーバーのみです。ここにその他のノード、外部ノード、ノードレイアウトグループを追加します。

ノードを追加するには、コマンド行ツール opcnode を使用します。詳細については *opcnode(1m)* のマニュアルページを参照してください。

HPOM 登録ノードは静的なマップです。ここに加えられるすべての変更を制御します。また、登録ノードを追加 / 削除するタイミングも決定する必要があります。

数百のノードを管理している環境では、ノードやその名前の判読が難しくなることがあります。このような事態を避けるため、**ノードレイアウトグループ**を使って、登録ノードをいくつかの階層に分けます。詳細については 65 ページの「ノード階層の設定」を参照してください。

HPOM ノード階層

HPOM 登録ノードはデフォルトのノード階層です。**ノード階層**とは、ノードとレイアウトグループの階層構造を視覚的に表したものです。各ノード階層には HPOM 環境に設定されているすべての管理対象ノードが含まれます。階層間の違いはノード構成のみです。

ノード階層は HPOM オペレータに割り当てられ、各オペレータの [管理対象ノード] ウィンドウに表示されます。ただし、各ノード階層には HPOM 環境に設定されているすべてのノードが含まれますが、オペレータには担当範囲の管理対象ノードしか表示されません。

レイアウトグループを使用してノードをグループ化し、階層として整理することができます。レイアウトグループにはノードと別のレイアウトグループを含めることができ、それによってノード階層を形成できます。レイアウトグループとノード階層はコマンド行ツール `opclaygrp` を使って管理できます。

HPOM 登録ノードにノードを追加するには、コマンド行ツール `opcnode` を使用します。ノードは任意の別のノード階層にも追加できます。追加した各ノードは、他のすべてのノード階層にも追加されます。これらの新規ノードは指定のノードおよびレイアウトグループに追加され、デフォルトでは、他のすべての階層の最上位レベルに追加されます。同じように、1 つのノード階層からノードを削除すると、そのノードは他のすべてのノード階層からも削除され、HPOM 環境に存在しなくなります。

詳細については *opclaygrp(1m)* と *opcnode(1m)* のマニュアルページを参照してください。

ノード階層の設定

登録ノード階層に多数のノードが含まれる場合は、レイアウトグループを使ってノードを論理エンティティとして構成できます。

レイアウトグループを使用することで、関心のあるノード階層レベルのみが表示されるように、ノードを論理的に構造化できます。レイアウトグループの基本は、フラットなファイルやディレクトリの集合から UNIX ファイルツリーディレクトリを作成するのに似ています。レイアウトグループを移動して別のグループにネスト化することで、フラットな構造ではなく、階層やツリー構造としてノードを整理できます。

レイアウトグループの作成、変更、削除、およびノード階層の詳細については *opclaygrp(1m)* のマニュアルページを参照してください。

階層内のすべてのノードへのアクションの適用

ノード階層を作成すると、HPOM の**コマンド行ツール** `opcnode(1m)` を使用できるようになります。このツールは、親グループに含まれるすべてのノードに同時にアクションを適用します。たとえば、一連のノードにポリシーを割り当てるには、対象となるノードの親ノードグループと、割り当てるポリシーを指定します。

```
opcnode -assign_pol pol_name=< ポリシー名 > \
pol_type=< ポリシータイプ > version=< ポリシーバージョン > \
group_name=< ノードグループ名 >
```

HPOM は、そのノードグループに含まれるすべてのノードにポリシーを割り当てます。

すべてのノードに適用できるアクション

管理対象ノード、HPOM ノード階層、HPOM 登録ノードに適用できるアクションは次のとおりです。

- ❏ コマンド行ツール opcnode によるノードグループの変更
- ❏ [**カスタマイズ** / **起動**] による HPOM アプリケーションの起動
- ❏ 指定したノードシンボルのメッセージの表示
- ❏ エージェントサービスの開始 / 停止
- ❏ ソフトウェアや設定などの配布
- ❏ ポリシーの割り当て

すべてのノードに適用できないアクション

管理対象ノード、HPOM 登録ノード階層、HPOM 登録ノードに*適用できない*アクションは次のとおりです。

- ❏ レポートの発行
- ❏ アプリケーションの追加 / 変更
- ❏ [**カスタマイズ** / **起動**] によるアプリケーションの起動

すべてのノードにアクションを適用するための条件

階層グループにアクションを適用する場合は、次の条件を考慮する必要があります。

- ❏ **複数の親グループ**

  同じノードが複数の親グループに属す場合、HPOM はこのノードの 1 つのインスタンスのみを認識し、一度だけアクションを適用します。

- ❏ **グループ**

  ノードの組み合わせやノードグループを含め、複数のグループにアクションを適用できます。

- ❏ **HPOM アプリケーション**

  HPOM アプリケーションには、LAN カード、デバイス、ファイルシステムなど、ノード以外の HPOM オブジェクトを含めることができます。HPOM アプリケーションは他のアプリケーションと同様に機能し、同じ HPOM ファイルアクションリストを受け取ります。

  HPOM アプリケーションと HPOM サービスの詳細については 96 ページの「アプリケーションの追加」を参照してください。

ノードの追加

HPOM 環境にノードを追加するには、コマンド行ツール opcnode を使用します。

詳細については *opcnode (1m)* のマニュアルページを参照してください。

内部ノードの追加

原則として、IP ノードの追加にはコマンド行ツール opcnode を使用します。

注記

ホスト名を入力すると、HPOM はノードの特徴をできるだけ多く取得しようとします。HPOM は MIB (SNMP 経由) とマシンタイプを取得し、対応する IP アドレスを決定します。複数のアドレスを持つノードの追加については、『*HPOM システム管理リファレンスガイド*』を参照してください。

内部ノードの特徴

コマンド行ツール opcnode を使って追加したノードには、次のような特徴があります。

- **IP ノード**

  内部ノードは IP ノードです。

- **HP Operations エージェント**

  通常、内部ノードでは HP Operations エージェントが実行されています。

- **個別の追加**

  内部ノードはホスト名と一意の IP アドレスによって HPOM に個別に追加されます。

- **無制限の機能**

  内部ノードは HPOM のすべての機能をサポートします。次に例を示します。

  - ログファイルのモニター
  - HPOM メッセージの捕捉

HP Operations エージェントをインストールしない理由

次のような理由がある場合は HP Operations エージェントをインストールしなくても構いません。

- ❏ セキュリティ上の懸念
- ❏ エージェントが不要
- ❏ プラットフォームやオペレーティングシステムが HPOM に対応していない

外部ノードの追加

外部ノードの追加には、コマンド行ツール opcnode とパターンマッチングを利用できます。次のような場合は、コマンド行ツール opcnode を使って機能制限付きのノードをインストールします。

- ❏ ノードに IP アドレスがない (SNA、DECnet)
- ❏ 特定のホスト名パターンまたは IP アドレス範囲を持つ特定の IP ノードセットをグループ化する

コマンド行ツール opcnode では、ノードのマシンタイプを MACH_BBC_OTHER_NON_IP に指定し、通信タイプを COMM_UNSPEC_COMM に指定する必要があります。

例 :

```
opcnode -add_node node_name=computer.company.com
net_type=NETWORK_OTHER mach_type=MACH_BBC_OTHER_NON_IP
group_name=external ccomm_type=COMM_UNSPEC_COMM
```

外部ノードの追加には 2 つの方法があるため、ノードが複数回追加されることも考えられます。たとえば、コマンド行ツール opcnode を使って追加したノードでも、パターンを変更すれば簡単に外部ノードとして再追加できます。同様に、パターンマッチングで追加したノードも、類似したパターンマッチングで再追加できます。HPOM では、これは問題となりません。ただし、ユーザーが作業を行ってノードが強調表示されるときに、メッセージのソースとして複数のシンボルが強調表示される可能性があります。

詳細については *opcnode (1m)* のマニュアルページを参照してください。

外部ノードを追加するための条件

HPOM 環境に追加する外部ノードは、次のいずれかの条件を満たす必要があります。

- ❏ ネームサーバーによって認識されている
- ❏ /etc/hosts ファイルに指定されている

注記

外部ノードを追加すると、パターンマッチングアクティビティが必要となるために管理サーバーシステムのパフォーマンスが低下します。

外部ノードの特徴

opcnode コマンドを使って追加した外部ノードには、次のような特徴があります。

- ❏ **すべてのノードタイプ**

  外部ノードはタイプを問いません (SNA、DEC、IP など)。

- ❏ **HP Operations エージェントなし**

  外部ノードでは HP Operations エージェントは実行されません。

- ❏ **一括追加**

  名前またはアドレスをパターンマッチングさせることで、複数の外部ノードを一括して HPOM に追加できます。

- ❏ **機能の制限**

  外部ノードが提供する機能は次のとおりです。

  - *トラップの捕捉*

    HP Operations 管理サーバーでトラップを捕捉できます (『*HPOM システム管理リファレンスガイド*』を参照)。

  - *シンボルの強調表示*

    HPOM は Java GUI オブジェクトペイン上のノードシンボルを強調表示させ、**メッセージブラウザ**に表示されるメッセージのソースを示します。これらのノードは、プロキシからメッセージを受信するように設定することもできます。

- *メッセージのフィルタリング*

  Java GUI オブジェクトペイン上のノードシンボルを選択することで、[**ブラウザ表示**] に送信されるメッセージをユーザーがフィルタリングできます。

- *ステータスの色分け*

  表示色を変更して、HPOM のステータス伝播に設定されているメッセージ重要度ステータスを示すことができます。

❏ 外部ノードでは、内部ノードで利用できる一部の機能を利用できません。

- *メッセージポリシーなし*

  ログファイル、モニター、opcmsg などからのメッセージがありません。つまり、ポリシーを割り当てることができません。

- *HPOM アプリケーションなし*

  HPOM アプリケーションを実行できません。

- *ブロードキャストなし*

  ブロードキャストを実行できません。

- *スケジュールアクションなし*

  スケジュールアクションを実行できません。

- *ターミナル接続なし*

  仮想 / 物理ターミナル接続を実行できません。

管理者 GUI からのノードの追加

ノードを追加するときに、ノード属性を完全に指定しなければならない場合は、管理者 GUI (CVPL) を使用する必要があります。次の場所の HP Operations Manager for UNIX ディレクトリでダウンロードできる CVPL のユーザードキュメントを参照してください。

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

管理者 GUI では次のノード属性を指定できます。

- ❏ *システムリソースファイルの自動更新*

  HP Operations エージェントコマンド `opcagt` (たとえば、HP-UX 管理対象ノードでは `/etc/rc.config.d/opcagt`) を統合できます。

- ❏ *高度なノードオプション*

  - 仮想ターミナルエミュレータ
  - 物理ターミナル
  - キャラクタフォーマット
  - メッセージストリームインタフェース出力
  - 情報のロギング

- ❏ *通信オプション*

  HTTP/SSL は新しい HPOM ノードでのデフォルトの通信タイプです。

  次の各項目を設定できます。

  - セキュリティパラメータ
  - インストール方法
  - バッファファイルサイズの制限

タイプが異なる管理対象ノードのセキュリティ設定

管理対象ノードのタイプは、`opcnode -list_node` コマンドでリスト表示できます。ノードタイプを変更するには、`opcnode -chg_nodetype` コマンドを使用します。

- ❏ **モニター対象ノード**

  環境内の安全なノード (オペレータのログオンまたはアクションの開始が制限されているノード) は**モニター対象専用**ノードとして指定できます。オペレータはノードからのメッセージを受信し、内容を確認することはできますが、すべてのアクション (コメントのブロードキャスト、ログオン、自動 / オペレータ起動アクション) は禁じられます。

- **制御対象ノード**

  制御対象ノードに対しては、オペレータはアクションを開始 / 停止したり、ログオンを実行できます。管理者は各ノードのセキュリティ設定を個別に見直し、オペレータによるアクセスを許可したり、アクション / コマンドの実行可能性を定義します。

制御対象ノードとモニター対象ノードの両方に対してオペレータが同時にアクションを開始しようとすると、アクションエージェントが常駐する制御対象ノードのみにアクションが送信されます。

非管理対象ノードの管理

計画休止によって生成されたメッセージなど、一部のメッセージについてはオペレータは注意を払う必要はありませんが、これらのメッセージにより、休止とは関係のない、直ちに注意しなければならない別のメッセージが判別しにくくなってしまう可能性があります。定期的に休止する場合は、管理者が計画休止を設定しておくことで (323 ページの「休止のスケジューリング」を参照) メッセージを除外できます。単発的な計画休止では、管理者は対象ノードを一時的に**非管理対象**ノードにすることで、そのノードを分離することもできます。モニター対象 / 制御対象ノードを非管理対象にすると、コントロールエージェント以外のすべての HPOM プロセスが停止します。これにより、管理サーバーにメッセージが送信されなくなります。オペレータは、管理対象環境に残るその他の管理対象ノードからのメッセージの処理を継続できます。

非管理対象ノードも HPOM の一部ですが、そのノードが担当範囲マトリックスに含まれるすべてのオペレータの環境からは排除されます。HPOM はすべてのノード属性を認識しており、ノードは登録ノードの一部のまま残ります。

非管理対象ノードを管理対象環境に戻す条件が整ったら (たとえば、計画休止作業が完了したら)、管理者はノードを管理対象に戻すことができます。ノードを管理対象から外す前に使用できたメッセージが再び使用可能になり、新しいメッセージが管理サーバーで再び受け付けられます。

ノードグループの設定

ノードグループとは、HPOM 管理者によって設定され、管理がオペレータに委譲されたシステムやインテリジェントデバイスの論理グループです。1 つのシステムは複数のノードグループに属す場合があり、複数のオペレータからの影響を受ける可能性があるため、ノードグループを使用すると管理者の設定作業の効率が大幅に低下します。

ノードグループは、設定プロセスの簡略化にも利用できます。たとえば、特定のノードグループのすべてのシステムに同じポリシーグループを割り当てることができます。その後、ノードグループに新しいノードを追加すると、ノードグループに割り当てられているポリシーが自動的に新規ノードに割り当てられます。1 つのグループに含まれるすべてのノードは、通常は同じ特徴を持ちます。

たとえば、次の共通の特徴を持つすべてのノードはグループ化できます。

- ❏ 場所が同じ
- ❏ 機能が似ている
- ❏ タイプが似ている

グループに適用するポリシーは、環境の要件に応じて自由に選択できます。

注記

オペレータを設定するときは、ノードグループの担当範囲をオペレータに割り当てます。環境内のノードを論理的な担当範囲カテゴリごとにグループ化し、それぞれを個々のオペレータに割り当てます。1 つのノードが複数のグループに属すことがあります。どのノードがどのノードグループに割り当てられているかは opcnode コマンドで確認できます。

opcnode -list_ass_nodes group_name=<*ノードグループ名*>

HPOM の初期段階のデフォルトノードグループは hp_ux (または solaris) と net_devices です。

ノードのステータスの確認

ブラウザウィンドウが開いていない状態では、認識されているすべてのノードは緑、認識不能ノードは青で表示されます。**メッセージブラウザ**が開いた状態では、ノードの色はそのノードに関連する、重要度が最も高い、受諾されていないメッセージのステータスに応じて変化します。メッセージの所有権がステータスの伝播に及ぼす影響については、『*HPOM Java GUI オペレータガイド*』を参照してください。

HPOM でのポリシーの管理

HPOM ポリシーは、ポリシーをデータベースに登録し、管理対象ノードに割り当て、管理対象ノードに配布できるように管理されます。

ポリシーの概念については 75 ページの「HPOM ポリシー」を参照してください。

ポリシーの追加、ポリシーとポリシータイプの登録など、ポリシーに関連する管理作業については、『*HPOM システム管理リファレンスガイド*』を参照してください。

HPOM 9.xx 管理サーバーでは、ポリシーに複数のバージョンを持たせることができます。詳細については 77 ページの「ポリシーバージョン」、および 89 ページの「ポリシーグループ」を参照してください。管理対象ノード上の複数のバージョンの HPOM 設定の管理については、『*HPOM システム管理リファレンスガイド*』を参照してください。

HPOM ポリシー

ポリシーは、データ情報とメタ情報から成る設定要素です。ポリシーは管理対象ノードに配布されます。通常、データ情報の部分は、ポリシーが配布されている管理対象ノードでメッセージの生成に適用されるルールセットから構成されます。データ情報の部分はすべてユーザーによって定義されますが、メタ情報の部分は管理作業に使用され、HPOM 製品によって管理されます。ポリシーは管理対象ノード上の HP Operations エージェントの設定に使用され、オペレータにイベントを通知するためにメッセージを生成して管理サーバーに送信する条件を決定します。

ポリシーは**ポリシーヘッダー**ファイルと 1 つまたは複数の**ポリシー本文**ファイルから構成されます。ポリシーヘッダーは、名前、タイプ、バージョンなどの属性が記録された XML ファイルです。

注記

`opcpolicy` コマンドの構文ではポリシーの指定にコロン (`:`) が使用されるため、ポリシー名にコロンを使用することはできません。このコマンドの詳しい使用方法については *opcpolicy (1m)* のマニュアルページを参照してください。

ポリシー本文には実際のエージェント設定が含まれます。ポリシーは、名前、バージョン、タイプの組み合わせ、または UUID によって識別されます。**ポリシータイプ**は、ポリシー本文が従うルールを決定するポリシー属性です。同一タイプのすべてのポリシーは、管理対象ノード上の同じ HP Operations エージェントプロセスによって使用されます。HPOM にあらかじめ定義されているポリシータイプ以外に、ユーザーが独自のポリシータイプを作成できます。

ポリシーコンテナは、名前とタイプが同じで、バージョンが異なるポリシーのセットです。ポリシーコンテナに含まれるすべてのポリシーのバージョンは異なります。ポリシーコンテナを対象にいくつかの操作を実行できます。この場合、コンテナ内の各ポリシーに対して操作が実行されます。各コンテナは一意の ID を持ち、コンテナ内のすべてのポリシーがこれを共有します。コンテナは、名前とタイプの組み合わせ、またはコンテナ ID によって識別されます。

ポリシータイプ

管理サーバー上の複数のポリシータイプを、管理対象ノード上の同一ポリシータイプにマッピングできます。このため、管理対象ノード上でポリシーが分類されるタイプをポリシータイプの登録時に指定できます。

タイプを指定しない場合は、管理サーバーに登録されているポリシータイプ名が代わりに使用されます。このとき、管理対象ノード上に対応するコンシューマが存在しなければ、ポリシーを配布しても結局は無視されることになります。

表 2-1　管理サーバーと管理対象ノード上のポリシータイプの例

管理サーバー	管理対象ノード
Logfile Entry Windows Event Log	le
Measurement Threshold Service/Process Monitoring	monitor

ポリシーバージョン

HPOM 9.xx では、管理サーバーに複数のバージョンのポリシーを持たせることができます。HPOM 9.xx 管理サーバーでは複数バージョンのポリシーを利用できるので、ポリシーとポリシーグループを対象とした操作の柔軟性が向上し、UNIX、Linux、Windows の各プラットフォームの HPOM 間の相互運用性を簡略化できます。また、次のようなメリットもあります。

- *SPI およびカスタム設定の移行に関連する問題が簡略化される*

  HPOM 8.xx では、SPI パッチの適用時に SPI テンプレートが上書きされないように、テンプレート名を変更する必要がありました。サーバーで複数の SPI バージョンを利用できるようになったことで、ポリシー / ポリシーグループの名前を変更せずに異なるノードグループに配布できます。これにより、移行計画に柔軟なアプローチをとることができます。移行の詳細については 81 ページの「HPOM 8.xx テンプレートから HPOM 9.xx ポリシーへの移行」を参照してください。

- *設定データの管理が容易になる*

  ポリシーのバージョニングにより、管理サーバーと管理対象ノードに存在する設定要素 (ポリシーなど) のバージョンを特定できます。たとえば、異なるサブエージェントバージョンの管理や、管理対象ノードへのサブエージェントの割り当て / 配布の管理が容易になります。詳細については 92 ページの「HPOM でのサブエージェントの管理」、および『*HPOM システム管理リファレンスガイド*』を参照してください。

  各種プラットフォーム (UNIX、Linux、Windows) の HPOM は、整合的なポリシーバージョニング機能を採用しています。これにより、プラットフォームが異なる HPOM に単一セットの SPI ポリシーを配布することができ、両者の間でのデータ交換が簡略されます。データ交換の注意点については 81 ページの「ポリシーデータ交換モデル」を参照してください。

すべてのポリシーにはバージョン番号があります。バージョン番号は、**メジャー．マイナー**という形式の 2 つの番号 (どちらも最大 4 桁) から構成されます (たとえば、1.0)。

メジャー番号は連続的なリリースの回数を表し、特定の目的 (たとえば、SPI リリースのトラッキング) のために予約しておくこともできます。マイナー番号はパッチの適用とカスタマイズに使用されます。各リリースの初期マイナー番号は 0 にする必要があります。

注記

メジャー番号は、モニター対象アプリケーションのバージョンと揃えることができます。たとえば、アプリケーションの今後のリリース用に 3 桁のメジャー番号を予約しておくことができます。つまり、アプリケーションバージョン 4.5 用にメジャーバージョン 450、アプリケーションバージョン 4.6 用にメジャーバージョン 460 のように予約するということです。

新たに作成したすべてのポリシーのバージョンは 1.0 に設定され、HPOM 9.xx にあらかじめ設定されているすべてのデフォルトポリシーのバージョンは 9.0 です。

ポリシーの内容に変更を加えると、ポリシーのマイナーバージョン番号が自動的に増加し、たとえば、1.0 は 1.1 になります。その新しいバージョンがすでに存在する場合は、次に繰り上げ可能な値 (たとえば、1.2) が選択されます。バージョン間の競合を避ける方法については 79 ページの「ポリシーバージョン間の競合の管理」を参照してください。

注記

ポリシーヘッダーを変更しても (ポリシーの説明の変更など)、新しいポリシーバージョンは作成されません。

コマンド行ツール `opcpolicy` を使用することで、ポリシーバージョンを自由に変更できます。ポリシーのバージョン番号は、ポリシーの内容を変更せずに変更することもできます。

これは、同時にリリースされたポリシーのバージョンを揃えるときに特に便利です。このコマンドの詳しい使用方法については *opcpolicy (1m)* のマニュアルページを参照してください。

注記

新しいバージョン番号が作成されると、内容が変更されていない場合でも新しいポリシーが作成されます。新しいポリシーには新しいバージョン UUID が割り当てられますが、コンテナ ID は変わりません。ポリシー名を変更した場合は、新しい UUID と新しいコンテナ ID を持つ新しいオブジェクトがデータベースに作成されます。

管理対象ノードにインストールできるのは、各ポリシーの 1 つのバージョンのみです。管理対象ノードに新しいポリシーバージョンを配布すると、バージョン番号に関係なく、既存のポリシーバージョンは新しいバージョンに置き換えられます。これは、どちらのバージョンも同じコンテナ UUID を使用しており、管理対象ノードではポリシーの識別にこの ID が使用されるためです。

注記

稼働環境ではポリシーをポリシーグループに割り当て、それをノードとノードグループに配布する必要があります。ポリシーバージョンは、割り当て先のポリシーグループの番号と対応している必要があります。

管理対象ノードで複数バージョンの HPOM 設定 (ポリシー以外にポリシーグループとインストルメンテーションデータを含みます) を扱う方法については、『*HPOM システム管理リファレンスガイド*』を参照してください。

ポリシーバージョン間の競合の管理 割り当てるポリシーのバージョン番号がデータベースにすでに存在する場合、ポリシーバージョンの競合が生じます。バージョン間の競合を管理するために、次のモードが用意されています。

- ❏ *上書きモード*

  データベース内の競合バージョンは置き換えられます。

- ❏ *新規バージョンモード*

  - バージョン間で競合が生じた場合、アップロードされるバージョンのマイナー番号が自動的に繰り上げられます。その新しいバージョンがすでに存在する場合は、次に繰り上げ可能な値が選択されます。ユーザーにはバージョン番号と UUID が通知されます。
  - 競合バージョンが存在しない場合は、ポリシーは現在のバージョンのままアップロードされます。

- ❏ *エラーモード*

  バージョン間で競合が生じた場合はエラーが返され、アップロードはキャンセルされます。

ポリシーの 1 つのバージョンが管理対象ノードに直接割り当てられ、同時に同じポリシーの別のバージョンが間接的に割り当てられている (たとえば、ノードグループ / ポリシーグループへの割り当てを通じて割り当てられている) 場合、管理対象ノードに実際に配布されているポリシーのバージョンが不明瞭になることがあります。

HPOM では、グループなどを通じた間接的な割り当てよりも直接割り当てのほうが優先されます。直接割り当てと間接割り当てによって生じたポリシーバージョン間の競合では、管理対象ノードへの直接割り当てのほうが重要と見なされ、間接的に割り当てられたバージョンのほうが新しい場合でも、間接的な割り当ては上書きされます。

たとえば、管理対象ノード AA にバージョン 1.3 のポリシーが直接割り当てられ、管理対象ノード AA が属すノードグループに同じポリシーのバージョン 1.6 が割り当てられる場合、ノードグループを通じて間接的に割り当てられるバージョン 1.6 のほうが新しいにも関わらず、ポリシーの配布ではバージョン 1.6 に優先してバージョン 1.3 のポリシーが配布されます。

注記

複数のバージョンがすべて間接的に割り当てられている (たとえば、2 つのノードグループ / ポリシーグループを通じて割り当てられている) 場合、HPOM はポリシーのバージョンに優先順位を付けることができません。予期せぬ配布結果が生じないように、異なるノードグループ / ポリシーグループに同じポリシーの異なるバージョンを割り当てないようにしてください。

ポリシー割り当ての自動化とバージョン競合の管理の詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

ポリシーデータ交換モデル

HPOM 9.xx for UNIX/Linux と HPOM 8.xx for Windows は、ポリシー / ポリシーグループのデータ交換に同じモデルを採用しています。次の点に注意してください。

- ❏ 管理サーバーでは、ポリシーは次のいずれかの方法で識別されます。
  - UUID
  - 名前、バージョン、タイプの組み合わせ
- ❏ 名前とタイプが同じすべてのポリシーは、コンテナ UUID という共通 ID を持ちます。同じコンテナ UUID を持つポリシーは、異なるバージョン番号と、ポリシー ID という個別 ID を持ちます。
- ❏ 2 つのポリシーをチェックサムで比較できます。設定のダウンロード / アップロード時は、ポリシーヘッダー内のチェックサムフィールドが評価されます。チェックサムには 2 つの種類があります。
  - *ポリシーヘッダーチェックサム*

    禁じられているポリシー変更 (ライセンス違反) の検出に使用されます。
  - *ポリシーデータファイルチェックサム*

    内容の迅速な比較に使用されます。
- ❏ ポリシータイプはエージェントが認識する文字列で (`monitor`、`le`、`trapi` など)、ここにも UUID と構文バージョンが含まれます。

HPOM 8.xx テンプレートから HPOM 9.xx ポリシーへの移行

HPOM 9.xx では、テンプレートはポリシーに移行されました。HPOM 8.xx の設定を HPOM 9.xx にアップロードすると、変換が自動的に行われます。

HPOM 8.xx テンプレートを HPOM 9.xx の設定にアップロードするときに、新たに作成されるポリシーにはバージョンが割り当てられます。

テンプレートからポリシーへの移行には、テンプレートグループからポリシーグループへの変換も含まれます。これは、`opccfgupld` ユーティリティで実行できます。アップロード / ダウンロードに使用されるディレクトリ構造の違いに注意してください。

- *HPOM 8.xx*

  < ***アップロードパス*** >/TEMPLATES/*

  (< ***アップロードパス*** >/TEMPLATES/TEMPLGROUPS も含まれます)

- *HPOM 9.xx*

  < ***アップロードパス*** >/POLICIES

  および

  < ***アップロードパス*** >/POLGROUPS

このコマンドの詳しい使用方法については *opccfgupld (1m)* のマニュアルページを参照してください。

新たに作成したすべてのポリシーのバージョンは 1.0 に設定され、HPOM 9.xx にあらかじめ設定されているすべてのデフォルトポリシーのバージョンは 9.0 です。それ以降の HPOM 8.xx テンプレートのアップロードでは、一致するバージョン 1.0 のポリシーが上書きされます。

ただし、HPOM の標準のポリシーチェックサム比較では、これらのバージョン 1.0 のポリシーは同一と見なされ、アップロードがスキップされる可能性があります。同一バージョンの 2 つのポリシーが実際には異なる場合、opccfgupld の -replace [-< ***サブエンティティ*** >] オプションを使用すると、データベース内のポリシーはアップロードするポリシーに置き換えられます。

注記

HPOM 9.xx では、HPOM 8.xx のモニターテンプレートは測定しきい値ポリシーに変換されます。

HPOM 8.xx と HPOM 9.xx の混在環境での移行

HPOM 8.xx と HPOM 9.xx が混在する環境では、HPOM 9.xx サーバーからの設定のダウンロードと、それに続く HPOM 8.xx サーバーへのアップロードはサポートされません。廃止するまですべてのテンプレートを HPOM 8.xx サーバーで維持するか、HPOM 9.xx サーバーで特定のポリシーをサポートする場合は、HPOM 8.xx サーバーでの対応するテンプレートの使用を中止することをお勧めします。

ただし、HPOM 8.xx サーバーからの複数回のダウンロードと HPOM 9.xx サーバーへのアップロードはサポートされます。たとえば、テスト用に HPOM 9.xx サーバーを設定するときは、HPOM 9.xx サーバーを稼働状態にする前に、アクティブな HPOM 8.xx サーバーからの設定データを使って更新を行う必要があります。一部のアプリケーションを HPOM 8.xx サーバーからモニターし続けなければならない場合でも、設定データを一括で HPOM 9.xx サーバーに取り込むことができます。

ポリシー割り当ての更新

ポリシーは、ノード、ノードグループ、ポリシーグループに割り当てることができます。HPOM 8.xx のテンプレートと HPOM 9.xx のポリシーの基本的な違いは、ポリシーに変更を加えた場合に HPOM 9.xx ではポリシーの新規バージョンが作成され、HPOM 8.xx では既存のテンプレートが上書きされることです。これは、既存の割り当てが変更後のバージョンではなく、古いバージョンのポリシーをポイントし続けるということも意味します。したがって割り当ての更新が必要になります。割り当ての更新は自動的に実行できます。HPOM 9.xx には次の割り当てモードが導入されました。

- `FIX`

  これはデフォルトモードです。変更後のポリシーを配布しても、ポリシーの新規バージョンの作成に関係なく、ポリシー割り当ては変更されません。

- `LATEST`

  最新バージョンのポリシーが作成されると、ポリシーグループ、ノード、ノードグループへのポリシーの割り当てが自動的に更新されます。このモードは、「policy to policy group assignment (ポリシーグループへのポリシーの割り当て)」オブジェクトの `LATEST` フラグを設定することで有効化できます。

  このモードをお勧めできるのはテスト環境と開発環境のみです。

- ❏ MINOR_TO_LATEST

  ポリシー割り当ては自動的に最新バージョンに更新されます。ただし、メジャーバージョン番号は変更されません。たとえば、MINOR_TO_LATEST フラグを設定して既存のバージョン 1.0 から更新すると、最新のバージョン 1.x に更新されます。

  稼働環境ではこのモードをお勧めします。

割り当てモードはコマンド行ツール opcpolicy および opcnode を使って指定できます。これらのコマンドの詳しい使用方法については *opcpolicy (1m)* と *opcnode* のマニュアルページを参照してください。

注記

LATEST または MINOR_TO_LATEST モードを使用する場合は、上記条件を満たす新規バージョンが作成された場合に既存のポリシー割り当てが自動的に更新されることに注意してください。FIX モードでは、手動で変更しない限りポリシー割り当ては変更されません。

表 2-2 は、HPOM for Windows バージョン 8.xx、HPOM for UNIX バージョン 8.xx、for UNIX バージョン 9.xx (および HPOM on Linux 9.01) で実行できるポリシー関連タスク / 操作を示しています。この比較は、割り当て作業の範囲の概要を明確にし、各製品間の相互運用性を高める上で役立ちます。HPOM の相互運用性については、『*HPOM システム管理リファレンスガイド*』を参照してください。

表 2-2　HPOM for Windows/UNIX でのポリシーの管理

	HPOM 8.xx for Windows ポリシー		HPOM 8.xx for UNIX テンプレート		HPOM 9.xx for UNIX/Linux ポリシー	
	新規	既存	新規	既存	新規	既存
作成	✔		✔		✔	
配布	✔	✔	✔	✔	✔	✔
割り当て			✔		✔	
割り当ての更新						✔

表 2-2　　HPOM for Windows/UNIX でのポリシーの管理 (続き)

変更	新規バージョンの作成		✔				4
	上書き				4		4

ポリシー割り当ての競合の管理

管理対象ノードに直接割り当てられているポリシーのバージョンと、間接的に割り当てられている同一ポリシーのバージョン (たとえば、元の管理対象ノードが属す 1 つまたは複数のノードグループ / ポリシーグループへの割り当てを通じた割り当て) に違いがある場合は競合が生じます。バージョンの競合が生じた場合、HPOM では直接割り当てられているポリシーが優先されます。

注記

複数のバージョンがすべて間接的に割り当てられている (たとえば、2 つのノードグループ / ポリシーグループを通じて割り当てられている) 場合、HPOM はポリシーのバージョンに優先順位を付けることができません。予期せぬ配布結果が生じないように、異なるノードグループ / ポリシーグループに同じポリシーの異なるバージョンを割り当てないようにしてください。

ポリシー割り当てでのポリシーバージョンの競合の詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

ポリシーへのカテゴリの割り当て

ポリシーにはカテゴリの割り当てを含めることもできます。カテゴリは、HP Operations エージェントがポリシーで参照されるリソースを正しくモニターするために必要なスクリプトやバイナリなどの関連インストルメンテーションとポリシーの間のリンクを定義します。

カテゴリ割り当ての詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

ポリシータイプコールバック

ポリシータイプコールバックは、特定タイプのポリシーのライフサイクル中に、指定の時点で実行される実行ファイルです。

コールバックには、編集、チェック、配布、クリーンアップの 4 種類があります。ここでは、それぞれについて詳しく説明します。

コールバックの定義用に多数の変数が用意されています。表 2-3 は変数とそれぞれの代入値を示しています。

表 2-3　変数とその代入値

変数	代入値
FILENAME	ポリシー本文の内容のダンプ先となる一時ファイルの完全パス。
POLICY	ポリシー名。
VERSION	ポリシーバージョン。
UUID	ポリシー ID。
SYNTAX	ポリシー構文バージョン。
TYPE	ポリシータイプ名。
AGENT_TYPE	HPOM エージェントが認識するポリシータイプ。
MGMT_SV	ポリシーが存在する管理サーバーの完全修飾ドメイン名。
ENCODING	ポリシー本文のコンテンツエンコーディング。
OPTION_X	編集コールバックによってエディタに渡される引数。X は渡される引数の番号を表し、最初の引数は OPTION_1、2 番目の引数は OPTION_2 のように指定される。
NODENAME	ポリシーの配布先となる管理対象ノードの完全修飾ドメイン名。この変数は配布 / クリーンアップコールバックで使用できる。

表 2-3 変数とその代入値 (続き)

変数	代入値
NODE_TYPE	ポリシーの配布先となる管理対象ノードの OS タイプ。この変数は配布 / クリーンアップコールバックで使用できる。

変数への値の代入はコールバックの実行前に行われます。これにより、実行時値をパラメータとしてコールバックに渡すことができます。コールバックの呼び出し文字列に変数が指定されていないときは、コールバックの実行前に $FILENAME が自動的に文字列に追加されます。

管理者権限で実行されるコールバックが未許可ユーザーによって登録されるリスクを軽減するために、コールバック実行ファイルの次のセキュリティレベルは変数となっています。

- **STRICT** (デフォルト)

  次のいずれかの条件に該当する場合、コールバックは登録、変更、実行 *されません*。

  - ファイルまたはディレクトリの所有者が root *ではない*
  - ファイルまたはディレクトリに write-、read-、または execute-by-group ビットが設定されている
  - ファイルまたはディレクトリに write-、read-、または execute-by-others ビットが設定されている

  コールバック実行ファイルと、実行ファイルが存在するディレクトリへのアクセスは、root ユーザーに限定されています。

- **RELAXED**

  次の条件に該当する場合、コールバックは登録、変更、実行 *されません*。

  - ファイルまたはディレクトリに write-by-group ビットが設定されている
  - ファイルまたはディレクトリに write-by-others ビットが設定されている

  このレベルが有効な場合は誰もがディレクトリの内容を表示し、実行ファイルを実行できますが、書き込み権限を持つのは root ユーザーのみです。

- **NONE**

  コールバック、またはコールバックが存在するディレクトリに対するチェックは行われません。

注記

セキュリティレベルの設定には HPOM 変数 `OPC_POLICY_CALLBACK_SECURITY` を使用します。

各コールバックスクリプト / バイナリのモードは、次のタイミングで `stat()` を使ってチェックされます。

- 登録時、データベースへの書き込み前
- 変更時、データベースへの書き込み前
- 実行前

いずれかの条件が満たされると、メッセージブラウザ (実行前に検出された場合)、または修正 / 登録を試みたターミナルにエラーが返されます。エラーは監査の対象となり、HPOM データベースにロギングされます。

すべてのコールバックには次の要件が適用されます。

- 失敗した場合は 0 以外の値を返す
- 成功した場合は 0 を返す

編集コールバック

編集コールバックは、エディタの起動前に実行される実行ファイルです。コールバックには一時ポリシーデータファイルの完全パスがコマンド行引数として渡されます。

チェックコールバック

チェックコールバックは、ポリシーがデータベースにアップロードされる前に実行される実行ファイルです。チェックコールバックは、適切な引数が指定された `opcpolicy_add()` API が呼び出される、またはコマンド行オプション `check=yes` が指定された `opcpolicy` が呼び出されると実行されます。

チェックコールバックが正しく完了すると、ポリシーはデータベースにアップロードされます。

配布コールバック

配布コールバックは、配布前にポリシー本文の内容が格納された一時ファイルに対して実行される実行ファイルです。この実行ファイルは、配布時に得られる情報 (ノード名、ノードタイプなど) に応じてポリシーの内容を変更する場合に使用されます。

ポリシー本文の内容が配布コールバックによって変更される場合は、コールバック実行ファイルに名前が渡される一時ファイル内ですべての変更を行う必要があります。ファイルのコピーが必要になる処理では、変更後のファイル名をコールバック側で元のファイル名に戻す必要があります。元のファイル名に戻さない場合、すべての変更は失われます。

配布コールバックの実行が失敗したときは、ポリシーの配布は HPOM 変数 `OPC_DEPLOY_IF_CALLBACK_FAILS` の値によって制御されます。この変数のデフォルト値は `TRUE` です。この場合、何があってもポリシーは配布されます。警告メッセージが出力された場合は `system.txt` ファイルにロギングされ、場合によってはメッセージブラウザにも出力されます。

クリーンアップコールバック

クリーンアップコールバックは、ポリシーが管理対象ノードに配布された後に実行される実行ファイルです。

クリーンアップコールバックが失敗しても、管理対象ノードへのポリシーの配布は成功として扱われ、失敗に関する情報を伝えるメッセージがアクティブメッセージブラウザに送信されます。

配布後の ConfigFile ポリシーによるエージェントに対するコールバックの実行

ポリシータイプ ConfigFile を使用することで、ConfigFile ポリシーの配布後にエージェントに対してコールバックを実行し、OV Composer ファクトストアのロードなどの後処理を実行できます。

エージェントに対するコールバックの実行を有効にする方法については、『*HPOM システム管理リファレンスガイド*』を参照してください。

ポリシーグループ

ポリシーグループ階層はツリー状の構造として構成されます。各ポリシーグループはツリー内の一意のパスで参照され、世界規模で唯一となる UUID を持ちます。これらのグループ間を任意にリンクさせることはできません。

注記

ポリシーグループ名にはスラッシュ (/) または円記号 (¥) を含める必要があります。HPOM 8.xx から HPOM 9.xx への移行では、テンプレート名に含まれるスラッシュと円記号はアンダースコア (_) に変換されます。たとえば、`SPI for SAP R/3` というテンプレートグループ名は `SPI for SAP R_3` に変更されます。

管理対象ノードにはポリシーグループの複数のバージョンが存在する場合があります。これらのバージョンのポリシーグループの管理については、『*HPOM システム管理リファレンスガイド*』を参照してください。

デフォルトポリシーグループ

HP Operations 管理サーバーにはデフォルトのポリシーグループが用意されています。ポリシーグループをリスト表示するには、次のコマンドを実行します。

```
# /opt/OV/bin/OpC/utils/opcpolicy -list_groups
```

HP Operations 管理サーバーのデフォルトポリシーグループは次のとおりです。

- ❏ Correlation Composer
- ❏ Examples
- ❏ Examples/ECS
- ❏ Examples/Unix
- ❏ Examples/Windows
- ❏ Management Server
- ❏ SNMP
- ❏ SiteScope Integration/<*SiteScope ポリシーグループ*>

HPOM 8.xx テンプレートグループから HPOM 9.xx ポリシーグループ構造への移行

HPOM 9.xx では、テンプレートグループはポリシーグループに移行されました。HPOM 8.xx の設定を HPOM 9.xx にアップロードすると、変換が自動的に行われます。

HPOM 8.xx テンプレートグループの構造から HPOM 9.xx ポリシーグループのツリー状構造への移行プロセスでは、次の点に注意してください。

- ❏ 別のテンプレートグループに属していないすべてのテンプレートグループは、ポリシーグループのツリー状構造のルート要素 (レベル 1) に移行されます。残りのテンプレートグループは、移行前のテンプレート構造内でのメンバーシップステータスに応じてレベル 2、レベル 3 のようにルートの下の要素としてグループ化されます。
- ❏ 構造に追加されるすべての要素には新しい UUID が割り当てられます。
- ❏ 複数の親グループに属す要素の名前、ポリシーグループ割り当て、ノード / ノードグループ割り当ては複製されます。

例 1、2 は移行に関する上記注意点を説明しています。

例 2-1　移行後のポリシーグループ構造

ポリシーグループ GA、GB、GC があり、GC は GA、GB に属し、GC にはポリシー P が割り当てられると仮定します。

移行により、GA、GB はルート要素として設定されます。GA、GB のすべてのメンバーはポリシーグループのツリー状構造に追加され、GA/GC、GB/GC というツリーが作成されます。どちらのグループにもポリシー P が割り当てられ、それぞれに異なる UUID が割り当てられます。

例 2-2　ノード / ノードグループ割り当ての複製

ポリシーグループ GA、GB はノードグループ X に割り当てられ、ポリシーグループ GC はノードグループ Y に直接割り当てられると仮定します。

移行により、Y に対する GC のすべての割り当ては GA/GC、GB/GC ツリーを通じて複製されます。これ以後は、1 つのグループのポリシー割り当てを更新しても別のグループには反映されないため、混乱を避けるため、これらのグループの同期を維持することが極めて重要になります。

HPOM でのサブエージェントの管理

サブエージェントは HPOM に含まれる製品ではありませんが、HP Operations 管理サーバーから部分的に管理できます。一部のサブエージェントは OV Control デーモンによって制御されます。

HPOM でのサブエージェントの管理には、『*HPOM システム管理リファレンスガイド*』に示される作業が含まれます。

HPOM にはサブエージェントを配布 / 配布解除するメカニズムが用意されていますが、サブエージェントの実際の設定の詳細については、サブエージェントソフトウェアパッケージに付属するマニュアルを参照してください。

サブエージェントポリシー

サブエージェントポリシーは、`Subagent` という特別なポリシータイプを使ってサブエージェントの管理を容易にするポリシーです。`Subagent` タイプのポリシーの本文には、管理対象ノードへのサブエージェントのインストール / アンインストールに適用されるルールが含まれます。これらのポリシーは、サブエージェントソフトウェアのベンダーから提供されます。ポリシーの内容についてはサブエージェントソフトウェアパッケージに付属するマニュアルを参照してください。

その他のタイプのポリシーとは異なり、`Subagent` タイプのポリシーは管理対象ノードに配布されず、ノードインベントリにも含まれません。

サブエージェントソフトウェアパッケージを HP Operations 管理サーバーにインストールすると、サブエージェントポリシーはサーバーに登録されます。その後、ポリシーとポリシーが属すポリシーグループは HPOM リポジトリにロードされます。

エージェント設定の配布時に、BBC 配布マネージャ (`opcbbcdist`) はポリシーの内容をチェックし、サブエージェントポリシーの本文に指定されているサブエージェントインストール手順を実行します。インストールプロセスの詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

`Subagent` タイプのポリシーは、HPOM 管理ポリシーのルールに準拠しています。管理ポリシーの詳細については、『*HPOM コンセプトガイド*』を参照してください。

アップグレードに関する注意点

HPOM 9.xx 管理サーバーには同一サブエージェントの複数のバージョンをインストールできます。管理対象ノードにインストールできるサブエージェントのバージョンは 1 つのみです。

管理サーバーにサブエージェントパッケージの新規バージョンをインストールすると、サブエージェントポリシーの新しいバージョンも登録されるので、どの管理対象ノードにどのバージョンがインストールされているかを簡単に特定できます。管理対象ノード上のサブエージェントをアップグレードするには、サブエージェントポリシーの新しいバージョンを割り当て、サブエージェントを配布します。

注記

管理サーバーにサブエージェントの新規バージョンをインストールしても、それに伴ってすべての管理対象ノードがアップグレードされるわけではありません。目的のサブエージェントポリシーバージョンを手動でノードに割り当て、インストールを開始する必要があります。

アップグレードプロセスの詳細についてはサブエージェントソフトウェアパッケージに付属するマニュアルを参照してください。

メッセージグループの構成

メッセージグループを利用することで、メッセージを簡単に分類できます。同じ機能や作業に関連するメッセージを 1 つのグループにまとめることができます。たとえば、バックアップやデータの保存に関連するすべてのメッセージ (ネットワークバックアッププログラムからのメッセージ、バックアップや保存操作に使用されるハードウェアからのメッセージなど) を Backup というメッセージグループにまとめることができます。メッセージグループはオペレータに割り当てられます。オペレータは、自分に割り当てられているグループのみを確認 / 管理します。

管理者は、メッセージグループを追加、確認、削除できます。これらの作業は管理者 GUI (CVPL) で実行されます。次の場所の HP Operations Manager for UNIX ディレクトリでダウンロードできる CVPL のユーザードキュメントを参照してください。

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

メッセージグループの追加

環境にメッセージグループを追加する前に、そのグループが HPOM のデフォルトメッセージグループと競合せず、かつ重複していないことを確認してください (デフォルトメッセージグループのリストは『*HPOM システム管理リファレンスガイド*』に記載されています)。OpC と Misc 以外のデフォルトメッセージグループは削除できます。また、既存グループの説明を変更したり、新しいグループを追加することもできます。

メッセージグループの確認

オペレータはメッセージグループのステータスを確認することで、環境内の各機能の概要を理解できます。登録メッセージグループを設定した上で、どのグループをどのオペレータに割り当てるかを決めてください。

アプリケーションの構成

アプリケーションは、オペレータがシステムとネットワークサービスの保守 / 制御に利用するプログラム、コマンド、スクリプト、ユーティリティ、またはサービスです。たとえば、バックアッププログラムとプロセスステータスコマンド ps は、どちらもアプリケーションとして統合できます。標準アプリケーションやカスタムアプリケーション、HPOM に組み込まれているアプリケーションも統合できます。

HPOM に統合されているアプリケーションとアプリケーショングループの管理には、コマンド行ツール opcappl を使用します。このツールの詳細については *opcappl(1m)* のマニュアルページを参照してください。HPOM にはデフォルトのアプリケーションとアプリケーショングループが用意されています。詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

アプリケーションのグループ化

アプリケーションをアプリケーショングループにまとめて階層構造を作成できます。たとえば、オペレータが各エントリポイントに個別のアプリケーションとしてアクセスできるように、アプリケーショングループを複数のエントリポイントに分割できます。その他のアプリケーションは論理グループに整理できます。

階層構造の登録アプリケーションを作成するには、アプリケーショングループを相互にネストさせます。

アプリケーションまたはアプリケーショングループをオペレータに割り当てるには、-assign_app_to_grp または -assign_grp_to_grp オプションを指定した opcappl コマンドを使用します。

アプリケーションの追加

アプリケーションは、次のいずれかの方法で登録アプリケーションに追加できます。

❑ **HPOM アプリケーションの追加**

HPOM アプリケーションを追加するには、-add_app オプションを指定した opcappl コマンドを使用します。アプリケーション名、アプリケーションコール、ユーザー名、パスワードを指定する必要があります。また、ターゲットノードのリスト、ラベル、その他のパラメータも指定する必要があります。次に例を示します。

```
opcappl -add_app app_name=APP_X app_call=testCall
user_name=John passwd=xyz
```

注記

Java ベースのオペレータ GUI でメッセージブラウザから開始できるのは、タイプが Start on Target Node(s) selected by Operator のアプリケーションのみです。

❑ **内部アプリケーションの追加**

タイプがブロードキャスト、仮想ターミナル、物理ターミナルの内部アプリケーションを追加するには、-add_app_inter オプションを指定した opcappl コマンドを使用します。アプリケーションの概要情報とアプリケーションタイプを定義します。オペレータ以外のユーザー名を指定することもできます。root ユーザーでなければアプリケーションを起動できない場合など、ユーザー名の変更が必要になる場合もあります。

注記

opcappl コマンドに指定するアプリケーション名は一意である必要があります。

アプリケーションの起動のカスタマイズ

あらかじめ設定されているアプリケーションの起動属性は、Java GUI、または -chg_app オプションを指定した opcappl コマンドを使ってアプリケーションの起動前に変更できます。

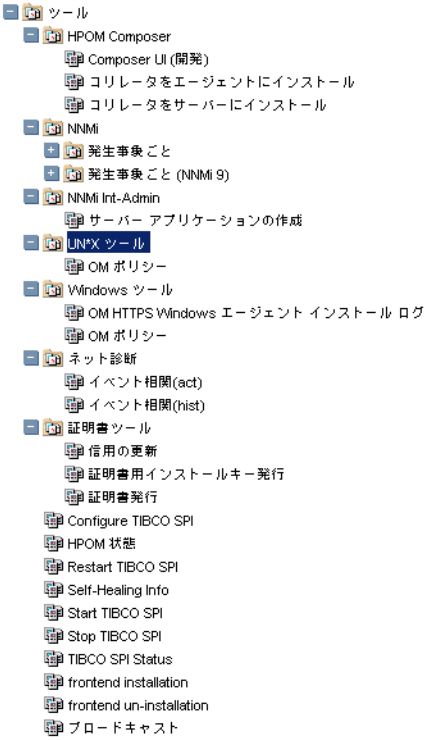
アプリケーションの起動属性は HPOM 管理者が定義します。これにより、オペレータが Java GUI からアプリケーションを直接起動できるようになります。

カスタマイズできる起動属性は次のとおりです。

- ❏ アプリケーションのターゲットノード
- ❏ アプリケーション呼び出しのパラメータ
- ❏ アプリケーションを実行するユーザー

アプリケーショングループまたは個々のアプリケーションの起動属性をカスタマイズする手順は次のとおりです。

1. Java GUI で［**アクション**］を右クリックし、［**カスタマイズ / 起動**］を選択します。［**ツール起動 – カスタマイズ ウィザード**］が表示されます。



2. [**カスタマイズ ウィザード**] でカスタマイズするツール (アプリケーション) を選択し、[**次へ**] をクリックします。
3. ツールを実行するターゲットノードのリストを指定し、[**次へ**] をクリックします。
4. ツールの実行に必要な追加情報を指定します。
   - *追加パラメータ*

     アプリケーションコールがオプションとしてノード名を受け付ける場合は、[**追加パラメータ**] フィールドにノードを指定できます。たとえば、-nodes オプションを指定したアプリケーション呼び出しでは、このオプションと引数 -nodes $OPC_NODES を使用できます。変数 $OPC_NODES はノードリストに展開されます。利用できる変数については、『*HPOM システム管理リファレンスガイド*』を参照してください。
   - *ユーザー名とパスワード*

     ターゲットノード用にあらかじめ設定されているユーザー名とパスワードが表示されます。パスワードは連続するアスタリスク (*) で表示されます。ユーザー名とパスワードを変更することで、別のユーザーとしてアプリケーションを実行できます。

注記

HPOM 管理者は、ノードへのログオンとアプリケーションの起動に適用されるデフォルトのユーザー名とパスワードを指定します。たとえば、HP OpenSpool のデフォルトユーザー名は spooladm です。

コマンド行ツール opcappl(1) の詳細については *opcappl(1)* のマニュアルページを参照してください。

HPOM ライセンス

HP Operations 管理サーバーや HP Operations エージェントなど、HP Operations Manager 製品の多くのコンポーネントにはライセンスが必要です。HPOM コンポーネントのライセンスがインストールされていない場合、そのコンポーネントはロックされ、使用できません。

ライセンスの種類

- **インスタントオンライセンス**

  インスタントオンライセンスは、評価のために製品を制限なしで 60 日間使用できる一時ライセンスです。これは HP Operations Manager のインストール時にインストールされ、初期化されます。60 日間の評価期間が経過すると有効期限が切れるため、製品を使い続けるには、新しい製品ライセンスパスワードをインストールする必要があります。

- **恒久ライセンス**

  運用ライセンスは製品の通常使用のためのライセンスです。これはすべての製品コンポーネントで利用できます。

  非運用ライセンスは、バックアップシステムなどの特別な目的で使用されるライセンスまたはライセンスパスワードです。

ライセンスの検証

HPOM ライセンスのステータスは 1 日に 1 度チェックされます。ライセンス対象オブジェクトのいずれかのライセンスのステータスが OK でない、または使用可能ライセンスの数が危機的なレベルに達すると、内部 HPOM メッセージが生成され、ライセンス管理者に電子メールが送信されます。ライセンスのステータスはライセンス管理ツールを使っていつでも確認できます。

Target Connector の数

必要な Target Connector ライセンスの数を確認するために、1 日に 1 度、データベースにメッセージが記録されているノードの数がチェックされます。HP Operations エージェントがインストールされているノードには Target Connector ライセンスは必要ないため、カウント対象に含まれません。

「*今日 - 31 日の 0 時 0 分*」～「*今日の 0 時 0 分*」の範囲の履歴データ値に基づいて 30 日間の平均が計算されます。これはライセンスレポートに表示され、インストールされている Target Connector ライセンスのチェックに使用されます。特定の日に複数の値が記録されている場合、30 日間の平均の計算にはその日の平均値が使用されます。

過去 30 日間に計算された値は、`opcremsyschk -list` コマンドを使って確認できます。

ライセンスの通知

HPOM ライセンシングコンポーネントのライセンスステータスには「ライセンス済み」と「未ライセンス」の 2 種類があり、ライセンス違反通知 (警告) レベルには「*警告*」、「*重大*」、「*危険*」の 3 種類があります。ライセンス違反通知レベルはライセンスの種類によって若干異なります。

- ❏ **インスタントオンライセンス**

  レベル 1 - 警告通知 : インスタントオンライセンスの有効期限が切れる 6 ～ 14 日前には、HPOM メッセージブラウザに警告通知が送信され、ライセンス管理者に電子メールが送信されます。

  レベル 2 - 重大通知 : インスタントオンライセンスの有効期限が切れる 0 ～ 5 日前には、HPOM メッセージブラウザに重大通知が送信され、ライセンス管理者に電子メールが送信されます。

  レベル 3 - 危険通知 : インスタントオンライセンスの有効期限が切れると、HPOM メッセージブラウザに危険通知が送信され、ライセンス管理者に電子メールが送信されます。ライセンスはロックされます。

- ❏ **恒久ライセンス**

  ライセンスがインストールされておらず、使用されていない場合、ライセンスのステータスは「*通常*」と見なされます。

レベル 1 - 警告通知 : 使用しているライセンスの数がインストール済みライセンスの数の 90% を超えて 100% 未満に達すると、HPOM メッセージブラウザに警告通知が送信され、ライセンス管理者に電子メールが送信されます。

レベル 2 - 重大通知 : 使用しているライセンスの数がインストール済みライセンスの数の 100% を超えて 110% 未満に達すると、HPOM メッセージブラウザに重大通知が送信され、ライセンス管理者に電子メールが送信されます。

レベル 3 - 危険通知 : 使用しているライセンスの数がインストール済みライセンスの数の 110% を超えると、HPOM メッセージブラウザに危険通知が送信され、ライセンス管理者に電子メールが送信されます。使用しているライセンスの数がインストール済みライセンスの数の 110% を超えると、ライセンスはロックされます。

小規模環境のサポート

管理対象ノードが少ない小規模な HPOM 環境に柔軟に対応できるように、危険ライセンスしきい値 (レベル 3) は 5 以上に設定してください。

たとえば、HP Operations エージェントライセンスの数が 20 の HP Operations サーバーでは、危険通知レベル (レベル 3) を 22 ではなく 25 に設定します。これにより、不要な制限が解消され、ライセンスがロックされる前に追加システムを設定する柔軟性が得られます。

ライセンスの利用可能性

1 つまたは複数のライセンス対象製品コンポーネントに必要なライセンスがなかったり、数が不足することもあります。

- 利用できる HP Operations 管理サーバーライセンスがない場合は、サーバープロセスを開始できません。ライセンスの欠如はライセンスレポートまたはライセンスステータス概要に示されます。
- 利用できる HP Operations エージェントライセンスがない場合は、HP Operations Manager データリポジトリに新しいノードを追加して設定することができません。すでに設定されているノードは使用 / 変更することができ、データリポジトリから削除することもできます。ライセンスの欠如はライセンスレポートまたはライセンスステータス概要に示されます。
- Target Connector ライセンスの数が不足した場合、ライセンスの欠如はレポートされますが、規制が適用されることはありません。

ユーザーとユーザープロファイルの設定

HPOM 環境に含めるすべての操作設定が完了すると、各種ユーザーを設定できるようになります。

次に例を示します。

ユーザータイプ	作業の概要
オペレータ	管理対象ノードおよびオブジェクトをモニター / 管理します。

HPOM で設定できるユーザーの担当範囲については第 1 章「HPOM の概要」を参照してください。

コマンド行ツール opccfguser を使用することで、設定する各ユーザーをデータベースに直接追加してオペレータを設定できます。

詳細については *opccfguser(1m)* のマニュアルページを参照してください。

ユーザーの追加

新規ユーザーを追加するには、コマンド行ツール opccfguser を使用します。ユーザー名を指定し、パスワードを割り当てる必要があります。たとえば、「John」というユーザーを追加するには次のコマンドを実行します。

```
opccfguser -add_user john -password secret -label John
-real_name John Doe
```

詳細については *opccfguser(1m)* のマニュアルページを参照してください。

オペレータの追加

HPOM では、オペレータは広範なケーパビリティと強力なツールを利用できます。オペレータは環境全体のシステムにアクセスし、すべてまたは指定のシステムに対してコマンドやスクリプトを実行したり、重要な修復アクションを実行したりできます。オペレータは、コンピューティング環境全体で提供される継続的なサービスに対する責任も負っています。この責任を果たすために、オペレータはオペレータコマンドとネットワークプラットフォームを理解し、複数の作業に優先順位を設定できることが求められます。

オペレータの責任

HPOM はオペレータの効率を高めながら、その負荷を軽減します。オペレータには、割り当てられるツールに見合った経験とスキルが必要です。自分が管理するシステムに関する知識を持ち、環境内の責任者を認識し、自分が使用するアプリケーション、コマンド、スクリプトを理解し、トラブルシューティング手順を遂行できなければなりません。

オペレータの設定

オペレータの設定では、次の各項目を定義する必要があります。

ケーパビリティ	アクションの開始 / 停止、受諾 / 受諾解除、メッセージの所有 / 所有解除、メッセージ属性の変更を行う権限
担当範囲	割り当てられているノード上の、割り当てられているメッセージグループに属すすべてのイベントに対する責任
アプリケーション	オペレータが利用できるアプリケーションとツール
プロファイル	HPOM の抽象ユーザーの設定が定義された、あらかじめ設定されているユーザープロファイル
ノード階層	オペレータの管理対象ノードの階層レイアウト

オペレータの追加に必要なユーザー名とパスワードは、UNIX/Linux のユーザー名 / パスワードとは関係ありません。HPOM ユーザーのファイル権限と環境設定については、『*HPOM システム管理リファレンスガイド*』を参照してください。

オペレータプロファイルの設定

HPOM 環境への新規オペレータの追加には、ユーザープロファイルと呼ばれる抽象ユーザーを設定し、設定するユーザーにそのユーザープロファイルを割り当てる方法があります。また、既存ユーザーの設定をコピーして名前を変更する方法もあります。この方法で新規オペレータを設定する場合は、すべてのオペレータ設定データと共に特定のオペレータが保存したブラウザ設定もコピーされることに注意してください。

デフォルトオペレータプロファイル

HPOM には opc_op というデフォルトオペレータプロファイルが用意されています。デフォルトオペレータプロファイルは、特定の組織または環境のニーズをより正確に反映させたオペレータプロファイルを新規作成する場合のベースとして利用できます。

オペレータ opc_op はシステム管理機能を制御します。オペレータ opc_op は主にシステム環境で作業を行い、制限された一部のツール (Processes、Disk Space、Print Status など) にアクセスできます。デフォルトでは、オペレータ opc_op にはすべてのケーパビリティが付与され、すべてのデフォルトメッセージグループを担当します。

注記

オペレータ opc_op はネットワークアクティビティの管理には関与しません。

HPOM オペレータのデフォルト環境の詳細については 104 ページの「メッセージグループとノードグループの割り当て」を参照してください。

メッセージグループとノードグループの割り当て

オペレータには、メッセージグループとノードグループを簡単に割り当てることができます。オペレータにノードグループを割り当てると、そのグループのノードがオペレータの担当範囲となります。ノードグループを選択した上で、オペレータが担当するメッセージグループを割り当てることができます。反対に、メッセージグループを選択してからノードグループを割り当てることもできます。

メッセージグループとノードグループをオペレータに割り当てるには、コマンド行ツール opccfguser を使用します。たとえば、「john」というユーザーの担当範囲としてすべてのノードグループとすべてのメッセージグループを割り当てるには、次のコマンドを実行します。

```
opccfguser -assign_respons_user -user john -node_group -all
-msg_group -all
```

詳細については *opccfguser(1m)* のマニュアルページを参照してください。

オペレータにグループを割り当てる際のガイドライン

オペレータにグループを割り当てるときは、次のガイドラインに従ってください。

ジョブ機能 オペレータにメッセージグループ Backup を割り当て、バックアップ作業を実行するノードが属すすべてのノードグループを設定できます。

地理的な場所 1 つの建物または施設のすべてのノードグループと、それに対応するメッセージグループを割り当てることができます。

ノードタイプ すべての IBM システムと、それに対応するメッセージグループを割り当てることができます。

注記

複数のユーザーに複数のサービスを提供する複雑なノードでは、一層の注意が必要です。通常、これらのノードは多数のメッセージを生成します。1 人のオペレータに複雑なノードを割り当て過ぎて、1 人では管理し切れない管理対象ノードセットにしないように注意してください。

オペレータ担当範囲の各層の定義

環境に複数の場所が含まれる、または環境がグローバルネットワーク環境である場合は、オペレータ担当範囲の層を定義すると便利です。たとえば、各場所のノードグループをそれぞれ異なるオペレータに割り当て、さらに接続ネットワークのメッセージグループを別のオペレータに割り当てることができます。同じ管理対象ノードグループやメッセージグループの管理を複数のオペレータに割り当てることもできます。

オペレータの管理対象ノード階層の割り当て

オペレータの管理対象ノード階層では、オペレータがアクセスできるノードはそのオペレータの担当範囲が確定した時点ですでに決定しています。オペレータに管理対象ノード階層を割り当てるには、[**登録ノード階層**] でノード階層を選択し、[ユーザーの追加 / 変更] ウィンドウの [**マップ選択の取り込み**] をクリックします。ノード階層の詳細については 64 ページの「HPOM ノード階層」を参照してください。

オペレータへのツールの割り当て

管理者は、ジョブの実行に必要なすべてのツールをオペレータに割り当てる必要があります。オペレータの仕事は、割り当てられたノードセットのメッセージグループを管理することです。オペレータが効率的にノードを管理できるように、割り当てるツールを決定する必要があります。コマンド、スクリプト、アプリケーション、ブロードキャスト機能、システムへのアクセスは、いずれもツールとしてオペレータに割り当てることができます。

各オペレータは、異なる組み合わせの管理対象ノードとサービスを担当します。各オペレータが実行するタスクは異なる場合があります。各オペレータに割り当てられているノードとメッセージグループを確認してください。

オペレータのツールセットの定義

オペレータのツールセットを定義するときは、ノードグループとメッセージグループについて次の点を考慮してください。

- ❏ どのサービスが提供されるか
- ❏ どの周辺装置と接続するか
- ❏ どのシステムおよびインテリジェントデバイスが含まれるか
- ❏ どのアプリケーションが実行されるか
- ❏ ノードの機能は 1 つの特定機能か

オペレータに適切なツールが割り当てられているかどうかの検証

次の点を確認することで、適切なツールが割り当てられているかどうかを検証できます。

- ❏ **アクセス**

  オペレータは制御対象システムにアクセスできるか

- ❏ **アクション**

  各管理対象オブジェクトで生じる可能性がある危機的 / 警告的状況に対応するための自動 / オペレータ起動アクションは十分に備わっているか

- ❏ **権限**

  管理対象ノードの集合に含まれるすべてのアプリケーションの起動に必要な権限がオペレータに付与されているか

❑ スクリプト

トラブルシューティングや修復アクションに使用されるスクリプトやコマンドにオペレータがアクセスできるか

ユーザーへのアプリケーションとグループの割り当て

指定した 1 人のオペレータ、複数のオペレータ、またはすべてのオペレータにアプリケーションとアプリケーショングループを割り当てるには、コマンド行ツール opccfguser を使用します。コマンド行文字列には複数のアプリケーションを指定できますが、割り当てるすべてのアプリケーションをファイルに指定し、それを参照させることもできます。詳細については *opccfguser(1m)* のマニュアルページを参照してください。

たとえば、ファイル system_groups.txt に指定されているアプリケーションセットをオペレータ opc_op に割り当てるには、次のコマンドを実行します。

```
opccfguser -assign_appgrp_user opc_op -appgrp -file
system_groups.txt
```

ユーザープロファイルの割り当て

ユーザープロファイルを設定すると、環境内のオペレータを迅速かつ簡単に設定できます。プロファイルを選択し、設定するオペレータに割り当てるだけで完了します。ユーザープロファイルの設定については 108 ページの「ユーザープロファイルの設定」を参照してください。

ユーザープロファイルの割り当てにはコマンド行ツール opccfguser を使用します。次に例を示します。

opccfguser -assign < *プロファイル名* > -all

詳細については *opccfguser(1m)* のマニュアルページを参照してください。

ヒント

オペレータに割り当てたノードグループとメッセージグループの総数を確認するには、直接、またはユーザープロファイルを使用して、そのオペレータのレポートを生成します。詳細については 125 ページの「レポートの生成」を参照してください。

ユーザープロファイルの設定

ユーザープロファイルを利用することで、複雑な環境でのユーザーの管理を簡略化できます。デフォルト設定が適用された抽象ユーザーの階層セットを作成し、実際に設定するオペレータにその設定を割り当てることができます。

注記

HPOM にはデフォルトのユーザープロファイルはありません。

たとえば、データベース管理者のユーザープロファイルであれば、データベースの設定と管理に使用するアプリケーションを含むアプリケーショングループを割り当てます。データベースが搭載されたすべての管理対象ノードを含むデータベースノード階層を設定しておけば、HPOM 環境のデータベースサーバーを担当する新規オペレータも簡単に設定できます。オペレータに適切なケーパビリティを付与し、データベースノード階層とデータベース管理者用のユーザープロファイルを割り当てるだけです。新規オペレータに追加の担当範囲やアプリケーション (ユーザープロファイルによって割り当てられていない担当範囲やアプリケーション) が必要になったときは、個別に割り当てます。

ユーザープロファイルは管理者 GUI (CVPL) から設定できます。次の場所の HP Operations Manager for UNIX ディレクトリでダウンロードできる CVPL のユーザードキュメントを参照してください。

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

ユーザープロファイルのリスト表示、割り当て、割り当て解除には `opccfguser` コマンドを使用します。詳細については *opccfguser(1m)* のマニュアルページを参照してください。

HPOM 設定の更新

ここでは、HPOM のインストール後に行う設定変更について説明します。HPOM ソフトウェアのインストールについては、『*HPOM 管理サーバーインストールガイド*』を参照してください。

設定の配布

管理サーバーでは、ソフトウェアの初回インストールと設定を常に行う必要があります。初期のデフォルト設定では、管理サーバーが唯一の管理対象ノードです。設定を変更するときは (ノード / モニタープログラム / ポリシーの追加など)、管理サーバーで変更を行い、そのたびに管理対象ノードに変更を配布する必要があります。

設定の部分的な配布

HPOM では、設定のどの部分を管理対象ノードに配布するか、およびどの HPOM ノードに設定データの受信を許可するかを決定できます。たとえば、新規ノードを追加する、または管理対象ノードの設定を更新するときは、管理サーバーからソフトウェアを配布します。

このソフトウェアに含まれる内容は次のとおりです。

❑ **エージェントソフトウェア**

管理対象ノード用のすべての HPOM ソフトウェアを含みます (アクションエージェント、メッセージエージェント、モニターエージェントなど)。必要な配布は一度だけですが、構成に新しい管理対象ノードを追加するたびに、新規ノードにエージェントソフトウェアを配布する必要があります。また、エージェントソフトウェアの新規バージョンをインストールする場合もこのソフトウェアコンポーネントを選択する必要があります。

❑ **ノード設定**

次を含みます。

- *ポリシー*

  設定されているメッセージ / モニターソース、および MoM 設定ポリシー。ポリシーは、そのポリシーが適用される管理対象ノードに配布します。

- *アクション*

  自動 / オペレータ起動アクション、またはスケジュールアクションの開始時に起動されるスクリプト、プログラム、アプリケーション。アクションは、そのアクションが開始される各管理対象ノードに配布します。

- *モニター*

  モニターエージェントがモニター対象オブジェクトのチェックに使用するスクリプトとプログラム。これらのスクリプトとプログラムは、それが起動されるノードに配置します。

- *コマンド*

  [ブロードキャストコマンド] ウィンドウで起動されるスクリプト、プログラム、アプリケーション、または Java GUI から起動されるその他のアプリケーション。これらのスクリプト、プログラム、アプリケーションは、それが起動される管理対象ノードに配布します。

ソフトウェアの配布準備

配布の準備として、HPOM はポリシーを HPOM データベースからローカルファイルにダウンロードします。ダウンロードの頻度を最低限に抑えるため、HPOM は配布後にポリシーファイルを管理サーバーに保存します。ファイルは保存されるので、後から別の管理対象ノードに配布できます。

注記

配布前にファイルがダウンロードされるのは、データベース内のポリシーが変更されている場合、またはローカルファイルが存在しない場合のみです。

ネットワークの負荷を減らしてパフォーマンスを向上させるため、HPOM は設定の変更部分のみを更新します。

管理対象ノードに設定を配布するには

管理サーバーから管理対象ノードに設定をインストール / 更新する手順は次のとおりです。

1. インストール / 更新する設定を定義します。
2. ノードにポリシーを割り当てます。
3. 設定をインストール / 更新する方法を定義します。

   設定のインストール / 更新には `opcragt -distrib` オプションを使用します。設定の中で、配布の対象となる部分を指定します。設定全体を置き換える場合は `-force` オプションを使用します (たとえば、**`opcragt -distrib -force`**)。

注記

`inst.sh` コマンドを使用することで、エージェントソフトウェアを手動で管理対象ノードにインストールすることもできます。その上で、`opcragt` コマンドを使ってポリシー、アクション、モニター、コマンドを管理対象ノードに手動で配布できます。どちらのコマンドも非対話的モードで実行できるので、スケジュールを設定してインストール / 更新を任意のタイミングで (たとえば、夜間や週末に) 実行できます。詳細については *inst.sh(1m)* と *opcragt(1m)* のマニュアルページを参照してください。HP Operations エージェントソフトウェアの手動インストールについては、『*HPOM HTTPS エージェントコンセプトと設定ガイド*』を参照してください。

強制的な更新

`-force` オプションを選択せずに標準のインストール / 更新を実行すると、設定に含まれる新しい情報のみが転送されます。デフォルトでは、未変更の情報は転送されません。これにより、ネットワークの負荷と転送時間が軽減 / 短縮されます。`-force` オプションを指定すると、HPOM は指定されたすべての設定を指定の管理対象ノードでインストール / 更新します。

注意

`-force` オプションは、できるだけ使用しないでください。HPOM のパフォーマンス向上を図ることができなくなります。

管理対象ノードへのポリシーの配布

ポリシーは、それを必要とする管理対象ノードのみに配布します。管理サーバーでポリシー定義を維持し、変更はそこで行います。変更した定義は必要に応じて配布し直します。メッセージグループや重要度レベルなど、メッセージポリシーの属性を変更するたびにポリシーをインストール / 更新する必要があります。

たとえば、管理対象ノード上のプロセス数を調べるモニタースクリプトを作成したと仮定します。管理対象ノードにポリシーを割り当てたら、モニターする管理対象ノードに対して管理サーバーからポリシーをインストール / 更新します。ポリシー本文の構文については 369 ページの付録 A「ポリシー本文の構文」を参照してください。

注記

この例では、管理対象ノードにモニタースクリプトもインストール (または更新) しなければならない場合があります。詳細については 262 ページの「しきい値モニターからのメッセージ」を参照してください。

新しいメッセージソースポリシーを定義し、そのポリシーをポリシーグループに割り当て、そのポリシーグループ (またはポリシー) を管理対象ノードに割り当てたら、そのポリシーを管理対象ノードに配布します。

HPOM によってインストールされるポリシー

HPOM がノードにインストールするポリシーは次のとおりです。

- ❏ ノードに割り当てられるすべてのポリシー
- ❏ ノードに割り当てられるポリシーグループに属すすべてのポリシー
- ❏ ノードが属すノードグループに割り当てられるすべてのポリシー
- ❏ ノードが属すノードグループに割り当てられるポリシーグループに属すすべてのポリシー

注記

ポリシーまたはポリシーグループを削除 / 変更する、または特定のノードのポリシー割り当てを解除するときは、変更が反映されるように、影響を受ける管理対象ノードに新しい設定を配布し直す必要があります。

変更中のポリシーはロックされ、管理対象ノードに配布されません。HPOM 管理者は**ノード設定レポート**という配布レポートを生成して管理対象ノードへのポリシー割り当てを検証し、どのポリシーの配布が必要であるかを確認できます。詳細については 125 ページの「レポートの生成」を参照してください。

配布レポートの生成には次のコマンドを使用します。

```
/opt/OV/bin/OpC/call_sqlplus.sh node_conf <ノード名>
```

ポリシー - ノードの組み合わせの重複の自動回避

ポリシーを配布する前に、HPOM はそのポリシーが管理対象ノードに一度だけインストール / 更新されていること、およびポリシーとノードの組み合わせが無効でないことを確認します。ポリシーは複数のポリシーグループに含めることができ、複数のノードに割り当てることができます。このため、同じノードにポリシーが複数回割り当てられる可能性があります。また、ノードへの一部のポリシーの割り当ては、それ自体が無効である場合があります (たとえば、異なるプラットフォームで稼働するノードへのプラットフォーム固有ポリシーの割り当て)。

あるポリシーが管理対象ノードに複数回割り当てられる場合、HPOM は重複割り当てを無視してポリシーを一度だけ配布します。

配布のヒント

ここでは、HPOM のソフトウェア、設定、ポリシーを迅速かつ簡単に配布するためのヒントを示します。

更新を必要とするノードのみの更新

HPOM での配布を円滑化する最も容易な手段の 1 つは、更新するノードを、更新が必要なノードだけに限定することです。

ノードの更新にはコマンド行ツール `opcragt` を使用します。`-distrib` オプションを指定してこのツールを使用することで、単一ノード、ノードグループ、またはすべてのノードに更新を適用できます。ノードグループに更新を適用する例を示します。

`opcragt -distrib -nodegrp <`*グループ*`>`

この <*グループ*> にはノードグループの名前を指定します。

詳細については *opcragt(1m)* のマニュアルページを参照してください。

注記

UNIX クラスタに配布する場合は、*すべて*のクラスタクライアントにモニター、アクション、コマンドを配布する必要があります。

配布時のノード数の削減と重要度の引き下げ

新しい設定データを多数のノードに同時に配布すると、**メッセージブラウザ**など、一部の HPOM サービスのパフォーマンスが低下することがあります。

この問題を回避するには次のように対応します。

- ❑ **ノード数を最小化する**

  設定変数 `OPC_MAX_DIST_REQS` を使用して、新しい設定データを一度に受信する管理対象ノードの数を最小化します。

- ❑ **重要度を引き下げる**

  `nice(1)` コマンドを使用して、管理サーバー上の `opcbbcdist` プロセスの重要度を引き下げます。

❑ **カテゴリベースの配布を行う、または選択的配布機能を利用する**

カテゴリベースの配布を行うか、opcbbcdist の選択的配布機能を利用して、特定のノードで必要とされない特定の設定ファイルが配布されないようにします。

カテゴリベースの配布と選択的配布機能の詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

ポリシーの手動配布

ポリシーを管理対象ノードに手動で配布したほうが良い場合もあります。たとえば、配布を夜間に実行するようにスケジューリングした場合や、ネットワーク経由でのポリシーの配布が組織のセキュリティ基準にそぐわない場合などです。HPOM は次のような手動配布に対応しています。

❑ **ネットワーク経由**

ポリシー、アクション、コマンド、モニターを管理対象ノードに配布するには、-distrib オプションを指定したコマンド行ツール opcragt を使用します。詳細については *opcragt(1m)* のマニュアルページを参照してください。

❑ **その他のトランスポートメディア**

ネットワーク経由での設定の配布が望ましくない場合は、コマンド行ツール opctmpldwn を使用し、ポリシーを暗号化してダウンロードできます。ダウンロードした (暗号化された) 設定を管理対象ノードに転送する方法については、その上で決定できます。詳細については *opctmpldwn(1m)* のマニュアルページを参照してください。

オペレータ設定なしでの配布

新しいオペレータを追加する際は、そのオペレータが担当する管理対象ノードとメッセージグループのセットを定義します。このオペレータ設定は管理サーバーに保存され、管理対象ノードには配布されません。新しいオペレータに特別なログオン、カスタマイズされたアプリケーション起動、またはコマンドのブロードキャストのケーパビリティがある場合、そのオペレータがこれらのケーパビリティを使用するたびに管理対象ノードはこの情報を検証します。ソフトウェアや設定と共にこの情報を配布することはありません。

設定変更の同期

HPOM のデータ同期機能により、GUI、HP Operations 管理サーバープロセス、API などの HP Operations サーバーコンポーネントの設定データは自動的に更新されます。

設定の更新では、設定オブジェクト (ノード、ノードグループ、アプリケーション、アプリケーショングループ、ポリシー、ポリシーグループ、メッセージグループ、ユーザープロファイル) の追加、削除、割り当て、割り当て解除、グループ替えなどの変更が行われます。

たとえば、1 つのポリシーを更新する場合など、設定オブジェクトの数が 1 つであれば設定変更は単純な操作で実行できます。一方、ノードをノードグループに割り当てる場合など、あるタイプの設定オブジェクトを別のタイプの設定オブジェクトに割り当てる (または割り当て解除する) 場合は複雑な操作になることがあります。HPOM にはオンライン設定更新機能があり、サーバープロセスと GUI を再起動せずに設定変更を適用できます。

HPOM の設定は Oracle データベース、設定ファイル、設定変数に格納されます。`opccfgupld` を使って設定を変更するたびに、変更がデータベースにアップロードされます。また、`ovconfchg` を使用するたびに、サーバープロセスで使用されるほとんどの設定変数の内容が更新されます。設定変数の詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

`ovconfchg` ツールを使用した場合に再ロードされる HPOM 設定ファイルは次のとおりです。

- 休止ポリシー
- メッセージ転送ポリシー
- MSI conf. ファイル
- 内部名解決 conf. ファイル

設定ストリームインタフェース (CSI) は、設定変更を同期させるための、メッセージストリームインタフェース (MSI) の拡張です。CSI では、内部設定コンシューマ (サーバープロセス、Java GUI) と外部設定コンシューマ (API クライアント) に設定変更を登録できます。Java GUI とサーバープロセスには、設定変更はデフォルトで登録されます。設定変更通知の登録は、`opcif_*` API を使って行うことができます。

設定変更後の GUI の同期

HPOM の設定を更新すると、それに応じてノード、ノードグループ、アプリケーション、メッセージグループなどの Java GUI 設定オブジェクトも変更されます。

HPOM には、設定更新時にサーバーと Java GUI を同期させるメカニズムが用意されています。ほとんどの設定変更は Java GUI に自動的に反映され、再起動の必要はありません。関連する設定変更は GUI で直ちに確認できます。

たとえば、ノード階層を変更したり、アプリケーショングループにアプリケーションを追加した場合、同期メカニズムにより、GUI を再起動したり、ログオフ / 再ログオンせずに変更を確認できます。

ただし、大規模な設定変更 (`opccfgupld` による設定のアップロード、ユーザーへのプロファイルの割り当て / 割り当て解除など) を行った場合は、HP Operations 管理サーバーから新しい設定を再ロードする必要があります。また、フィルター定義を更新したり、**自動サービス再ロード**オプションを無効にしてサービスを変更した場合も再ロードが必要です。Java GUI をログアウトする必要はありません。

注記

外部ユーザー (設定 API のユーザーなど) が設定ストリームインタフェースに接続している場合は、これらのユーザーに同期イベントが転送されます。

設定更新ツール `opccfgupld` を実行している場合、Java GUI への新規ログオンはブロックされ、次のエラーメッセージが表示されます : `Can't login while opccfgupld is running.` (opccfgupld の実行中はログインできません)。

最新コンテンツへの自動アクセス

HPOM 管理者 GUI セッションで初めてウィンドウを開く場合、その直前に HPOM データベースから最新のデータがウィンドウに直接ロードされます。これにより、ユーザーとアプリケーションの両方が、単一の変更済みオブジェクトの最新の内容にアクセスできます。

セッションの手動再起動

[**セッションの再起動**] オプションを選択すると、現在のセッションは通常どおりに終了します。しかし、メニューオプションの [**閉じる**] や [**終了**] とは異なり、[**セッションの再起動**] はセッションの終了をユーザーに確認しません。[**セッションの再起動**] オプションは開いているすべてのウィンドウを閉じ、[**設定の保存 / ホームセッション**] に最後に保存した設定で (ノード / メッセージ / アプリケーショングループの内容と設定を含みます) HPOM セッションを再開します。ただし、[アプリケーションの出力] や [レポートの出力] などのウィンドウは開かれません。また、終了したセッションとは異なる位置にウィンドウが表示されたり、異なる形状設定で表示される場合があります (ただし、終了するセッションで設定と詳細を保存した場合を除きます)。このシステム動作は、ログアウト / 再ログインを実行した場合と同じです。

トランザクション時のコンポーネントの自動ロック

HPOM の設定データは複数のプロセスが並行して操作できるため、必然的に設定データとその変更の管理が求められます。HPOM では、アプリケーションによるデータの変更中は、そのデータはロックされます。データがロックされることで、別のアプリケーションやユーザーによる同時変更が防止されます。変更が完了すると、サーバープロセスとユーザーインタフェースの両方が自動的に同期され、更新後の設定データを確認、使用できるようになります。

HPOM では、設定データが変更された後のコンポーネントの同期に**トランザクション**の概念とロックを採用しています。トランザクションの概念は、ユーザートランザクションを開始、コミット、ロールバックする API 関数をサポートしています。

データのバックアップと復元

ここでは、HP Operations 管理サーバーのデータをバックアップ / 復元する方法について説明します。

データのバックアップ

HPOM には、管理サーバー上のデータをバックアップするために次の 2 つのスクリプトが用意されています。

- **opcbackup_offline**

  手動オフラインバックアップ。リソースがない、または自動バックアップの必要がない場合は、`opcbackup_offline` および `opcrestore_offline` スクリプトを使用してオフラインで完全バックアップを行います。

- **opcbackup_online**

  自動オンラインバックアップ。自動バックアップを実行する場合は `opcbackup_online` を使用します。バックアップが開始されるまでに完了できなかった作業はアイドル状態で維持され、バックアップが完了すると再開されます。

バックアップ方法の比較

バックアップを計画 / 実行する際は、HPOM の設定が管理対象ノードだけでなく、管理サーバーにも及んでいることに注意してください。管理サーバーで復元された設定が管理対象ノードの現在の設定と一致しない場合、指示の欠落やポリシーの誤った割り当てに関連するエラーが生じる可能性があります。

表 2-4 は、手動 (オフライン) バックアップと自動バックアップの長所と短所を示しています。

表 2-4　バックアップ方法の比較

バックアップ方法	バックアップタイプ	長所	短所
opcbackup_offline	オフライン	• アーカイブログモードを有効にする*必要がない* — システム全体のパフォーマンスの向上 — 必要ディスク容量が少ない • バックアップ対象にバイナリも含まれる (*フル*モードが有効な場合) • オフラインで完全バックアップを実行する	• すべての HPOM GUI を終了する必要がある • HP Operations サーバープロセスを含むすべての HP Software サービスが停止される • 最後の完全バックアップの時点の状態までにしか復元できない
opcbackup_online	自動	• HPOM オペレータ用の Java GUI、トラブルチケット、通知サービスがバックアップ中も完全に機能する • 次のような Oracle データベースの部分的復元が可能 — 指定日時まで — 損傷した個々のテーブル • バックアップ中もすべての HP Software プロセスが稼働する	• バックアップスクリプトにより、一部の HP Software サービスが一時停止される • アーカイブログモードを有効にする必要がある — システム全体のパフォーマンスの低下 — 必要ディスク容量が多い • バックアップ対象にバイナリや一時ファイル (キューなど) が含まれない

データの復元

バックアップされたデータから復元を行うには、バックアップに使ったツールに対応する復元ツールを使用する必要があります。たとえば、opcbackup_offline でバックアップしたデータの復元には opcrestore_offline を使用します。同様に、opcbackup_online でバックアップしたデータの復元には opcbackup_online を使用します。

opcrestore_online スクリプトを使用することで、Oracle データベース全体を前回のバックアップ時の状態、または最新の状態 (オフラインの REDO ログに基づくロールフォワード復旧) に復元できます。ただし、Oracle のアーカイブログモードにはより多くの選択肢があります。

Oracle のアーカイブログモードを使用すれば、たとえば、次の処理を実行できます。

- **単一ファイルの取得**

  1 つの破損したデータファイルをバックアップから取り出し、オフラインの REDO ログに基づいて復元します。

- **指定日時までの復元**

  バックアップとオフラインの REDO ログを使用して、指定した日時までのデータを復元できます。

注記

アーカイブログモードは Oracle の用語の 1 つであり、データが定期的に自動保存される状態を意味します。データファイルに加えられるすべての変更は **REDO ログファイル**に保存されます。その後、これらの REDO ログファイルはアーカイブされます。詳細については Oracle のマニュアルを参照してください。

メッセージの所有権

ここでは、障害解決のために実行される操作に対する所有権の影響について説明します。

管理者は、HPOM でサポートされるいずれかの所有権モードを選択することで所有権ポリシーを決定します。所有権モードの設定については、『*HPOM システム管理リファレンスガイド*』を参照してください。

メッセージのマーキングと所有

システム環境とその管理に対する責任を理解するには、メッセージのマーキングと所有の概念を理解することが重要です。

HPOM では、マーキングと所有は次のように定義されます。

- **マーキング**

  ユーザーがメッセージに注意していることを示します。情報所有権モードです。

- **所有**

  環境の設定に応じて、ユーザーがそのメッセージの管理を引き受け、メッセージに関連付けられているアクションを実行したいと考えている (オプション所有権モード)、または実行するように強制されている (強制所有権モード) ことを示します。

所有権表示モード

HPOM には、次に示す**所有権表示モード**があります。

- **ステータス伝播なし** (デフォルト)

  メッセージが所有 / マークされると、所有メッセージの新しい数を反映してメッセージ変更の重要度を示す色、Java GUI **メッセージブラウザ**の所有状態カラムに表示されるフラグ、**メッセージブラウザ**の所有状態カラーバーの表示が変更されます。**オブジェクトペイン** (オペレータのメッセージグループとノードグループ、および管理者の登録メッセージグループ) では、ステータスの伝播については、所有 / マークされたメッセージのステータスは無視されます。

- **ステータス伝播**

  メッセージが所有されているかどうかに関わらず、他のサブマップウィンドウ内の関連シンボルのステータスは、すべてのメッセージのステータスに基づいて決定されます。1 つの危険メッセージが関連付けられている管理対象ノードは、メッセージが所有された後もそのメッセージを危険と見なし、該当する重要度レベルの色 (デフォルトでは赤) で示します。この表示モードでは、メッセージが所有されていることを示すのは、**メッセージブラウザ**の所有状態カラムのフラグだけです。

たとえば、特定の管理対象ノードに関連する、重要度が危険の唯一のメッセージをユーザーが所有すると、その危険メッセージが関連付けられている管理対象ノードはそのメッセージを危険と見なさなくなり、重要度レベルの色 (デフォルトでは赤) で示さなくなります。**メッセージブラウザ**には、同じ管理対象ノードに関連する、次に重要度レベルが高い未所有メッセージのステータスが反映されます。

所有権表示モードの変更方法については、『*HPOM システム管理リファレンスガイド*』を参照してください。

所有権モード

HPOM には、次に示すデフォルトのメッセージ**所有権モード**があります。

❑ **オプション**

ユーザーには、メッセージの所有者になることができる明確な権限があります。メッセージの所有者は、そのメッセージに対する排他的な読み取り - 書き込みアクセス権を持ちます。HPOM 管理者を除き、**メッセージブラウザ**にこのメッセージが表示されるすべてのユーザーには、このメッセージに対するアクセスは制限されます。

このモードでは、次の処理の実行は所有者のみに許可されます。

- メッセージに関連するオペレータ起動アクションの開始 / 停止
- メッセージに関連する自動 / オペレータ起動アクションの停止 / 再開
- メッセージの受諾
- メッセージの受諾解除

❑ **強制** (デフォルトモード)

オペレータは、未所有メッセージの所有者になることを明示的に選択することで、またはメッセージに対して操作を実行して自動的にメッセージの所有者となります。

このモードでは、以下の処理の実行を試みると、オペレータは自動的にメッセージの所有者となります。

- メッセージに関連するオペレータ起動アクションの開始 / 停止
- メッセージに関連する自動 / オペレータ起動アクションの停止 / 再開
- メッセージの受諾解除

❑ **情報**

このモードでは、所有権はメッセージのマーキングとマーク解除の概念に置き換えられます。**マーキング**されたメッセージは、オペレータがそのメッセージに注意を払っていることを示します。メッセージのマーキングは、情報用途のみを目的としています。オプションモードや強制モードとは異なり、メッセージに対する操作が制限 / 変更されることはありません。オペレータは、自分でマーキングしたメッセージのみをマーク解除できます。管理者は、マーキングされたすべてのメッセージのマークを解除できます。

レポートの生成

HPOM は、強力なレポート生成ツールと、低水準のネットワーク要素からサービスの可用性に至る広範な情報通知レポートを備えており、より複雑で包括的なレポートに対する一般的なニーズに応えます。レポート生成は自動化されており、さまざまなフォーマットでレポートを表示できます。一般論として、作成できるレポートの範囲と設定の幅はユーザータイプによって異なります。たとえば、HPOM 管理者は他の HPOM ユーザーと比較して、より多くの種類のレポートを作成できます。

レポート生成ツール

レポートの作成と生成に利用できるツールは次のとおりです。

- **SQL ベースのレポート**

  SQL をベースとした、HPOM であらかじめ定義されている内部レポート

- **HPOM 独自のレポート**

  HP Reporter による HPOM 独自のレポート

- **データベースアクセス**

  自己作成スクリプトによる直接データベースアクセス

『*HPOM Reporting and Database Schema*』には、HPOM 管理者が外部のレポート作成ツールを使って HPOM データベースにアクセスし、レポートを定義 / 作成するために必要な情報が記載されています。

HPOM レポート

HPOM で作成できるレポートは、管理者用レポートとオペレータ用レポートに大別されます。管理者とオペレータは、どちらも HPOM 環境のさまざまな種類の内部レポートを作成できます。

管理者用レポートとオペレータ用レポート

HPOM で作成されるレポートは 2 種類に大別できます。

- **管理者用レポート**

  HPOM の作業環境のあらゆる側面に関するレポート。たとえば、HPOM 管理者はアクションの成功率を調査するため、すべてまたは一部のオペレータが実行したアクションに関するレポートを生成できます。また、ノードやノードグループの設定などを示すレポートも作成できます。

- **オペレータ用レポート**

  すべてのオペレータ指示とメッセージ注釈が含まれます。すべてのアクティブメッセージまたはすべての履歴メッセージに関するレポートを生成する場合、メッセージバッファに多数のメッセージが含まれていると、レポート出力の生成に数分間かかる場合があります。

生成するレポートのタイプとレポート出力のメディアを選択できます。ユーザーが選択できるレポートは、そのユーザーの担当範囲によって異なります。

メッセージ、エラー、設定、監査レポート

具体的には次のレポートタイプから選択できます。

- **メッセージレポート**

  ブラウザウィンドウに表示される単一メッセージまたはすべてのメッセージに関するレポートを生成できます。詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

- **HPOM エラーレポート**

  HP Operations 管理サーバーのエラーメッセージを対象とします。

  これらのメッセージは次のファイルに書き込まれます。

  `/var/opt/OV/log/System.txt` (テキスト)

  `/var/opt/OV/log/System.bin` (バイナリ)

注記

HTTPS エージェントと管理サーバーは同じ場所を使用します。

- **設定レポート** (管理者のみ)

  ノード、ノードグループ、ポリシー、オペレータ、アクションなどの設定情報を対象とします。

利用できるレポートのリストと、それぞれが対象とする範囲の簡単な説明については、『*HPOM システム管理リファレンスガイド*』を参照してください。

サービスレポート

HP Reporter を使用することで、HPOM 環境内の特定時点または特定期間内におけるサービスのステータスの概要を知ることができます。HP Reporter は、HPOM の管理環境についてあらかじめ設定されているサービスレポートを生成します。これらのレポートには、メッセージスループット、障害応答時間、傾向、設定上の問題の概要が示されます。

たとえば、HP Reporter に付属する HPOM サービスレポートを使用して、次の各項目に関するグラフ形式および統計表形式のレポートを作成できます。

- HPOM 管理環境の全般的な状況
- HPOM オペレータとその作業負荷
- 自動 / オペレータ起動アクションのステータス
- HPOM 管理環境に存在する設定上の問題
- HPOM のさまざまな動作領域の傾向分析

各レポートの詳しい内容と対象範囲については、『*HPOM システム管理リファレンスガイド*』および HP Reporter のドキュメントを参照してください。

サービスレポートはスケジュールを設定して生成できるほか、取り込んだ情報を 3 つの形式 (グラフ、ダイアグラム、統計表) で表示できます。また、Web サーバーが稼働しており、それを適切に設定した場合は、レポートを自動的に更新して Web 上にパブリッシュできます。HP Reporter の詳細については同製品のドキュメントを参照してください。Web サーバーをインストールして HPOM 用に設定する方法については、『*HPOM 管理サーバーインストールガイド*』を参照してください。

レポートの生成

HPOM 環境では、管理者とオペレータはさまざまな種類の内部レポートを作成できます。このとき、レポートの形式として簡易と詳細を選択できます。作成結果はプリンタまたはファイルに出力するか、オンラインで表示できます。

PGM レポートと INT レポートの作成

すべてのレポートは PGM (プログラム) というタイプを持ちます。PGM レポートは、プログラム / スクリプトまたは INT (内部) タイプを使って作成できます。INT レポートはサーバーの内部機能によって生成され、対象は一部のメッセージに限定されています。レポートタイプ PGM は、SQL スクリプトによって生成される Oracle SQL*Plus レポートで使用されます。また、レポートタイプ PGM はその他のプログラム / スクリプトでも使用されます。

内部レポートの形式

オペレータ向けの、短文形式の内部レポートには次の情報が含まれます。

- ❏ レポートの日付、時刻、タイプ
- ❏ メッセージテキストを含むすべてのメッセージ属性
- ❏ 元のメッセージテキスト

独自レポートの定義

HPOM のレポート機能を利用することで、HPOM アプリケーション、サードパーティ製ツール、または自分で作成したスクリプトを使ってデータベースから直接抽出した情報に関するカスタムレポートを設計、生成できます。

より詳しいレポートを作成できるかどうかは、HPOM 環境に設定されている監査レベルによって異なります。HPOM では、管理者は追加のレポートを定義できます。詳細については、『*HPOM システム管理リファレンスガイド*』および『*HPOM Reporting and Database Schema*』を参照してください。

新規レポートの設定は、新しいスクリプト / プログラムを作成するか、新しい SQL*Plus ファイルを作成することで行います。その上で既存のテキストファイルを編集し、新しいレポートを統合します。これらの設定ファイルは、どのレポートが管理者用で、どのレポートがオペレータ用であるかを定義します。HPOM のスケジュールアクションポリシーに任意のレポート出力日時を設定し、HPOM のツールを使って抽出した情報を表示できます。

HPOM データベースの仕組みとデータベースへのアクセス方法、および格納されている情報の利用方法については、『*HPOM Reporting and Database Schema*』を参照してください。

独自レポートの統合

独自に定義したレポートを統合できます。独自に定義したレポートの作成と統合の詳細については、『*HPOM システム管理リファレンスガイド*』および『*HPOM Reporting and Database Schema*』を参照してください。

3 HPOM 管理対象ノードの概念

概要

本章では、HPOM 管理対象ノードの概念について説明します。本章で説明するトピックは次のとおりです。

HPOM 管理対象ノードの詳細については、『*HPOM システム管理リファレンスガイド*』および HP Operations エージェントのドキュメントを参照してください。

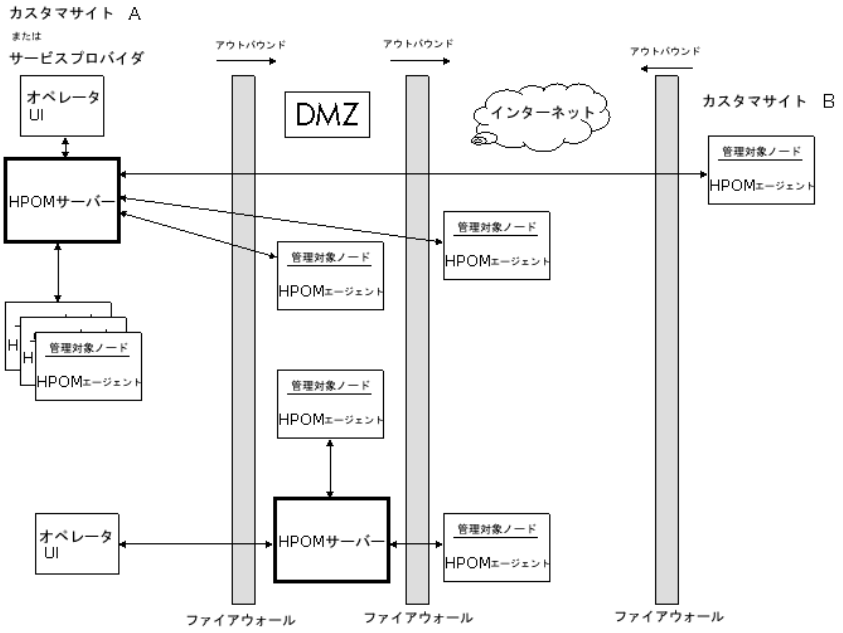
HTTPS エージェントの概要

HTTPS エージェントソフトウェアは、HP Operations 管理サーバーとその管理対象ノードの間に安全性の高い通信を提供します。

図 3-1 は HP Operations Manager による一般的な管理環境を示しています。

HTTPS エージェントを利用するメリットについては後述します。

図 3-1　HPOM による一般的な管理環境



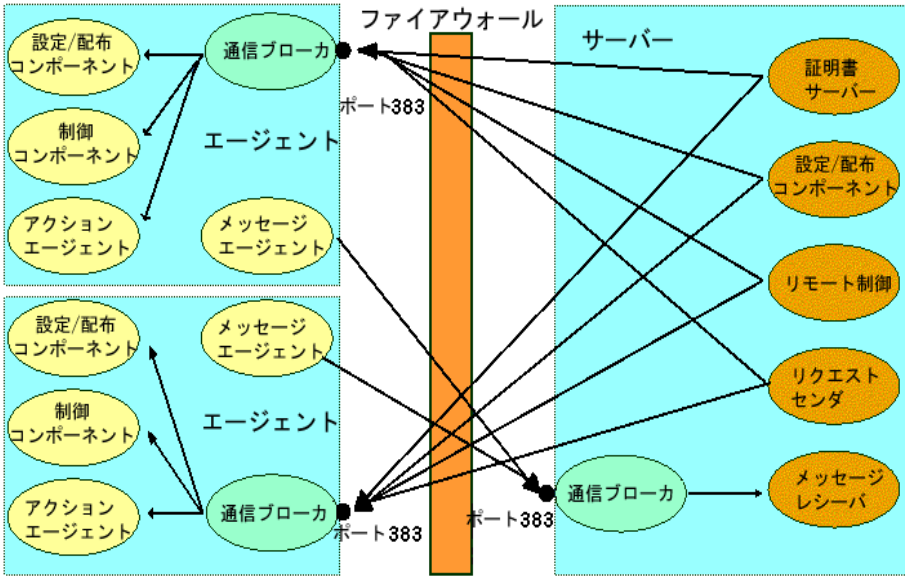
HTTPS ベースの通信の主なメリットは次のとおりです。

- HTTPS ベースのオープンな通信技法を使用する、設定可能、単一ポートのセキュアな通信とファイアウォールの組み合わせによるシンプルな管理。外部アクセスを専用の HTTP プロキシに制限し、多重 HTTP プロキシによりポート使用率を削減します。
- SSL/PKI 暗号化、および認証にサーバー / クライアント証明書を使用する、導入後直ちに利用できるインターネットセキュア通信。
- 今日のあらゆる環境で利用でき、すべての IT 管理者にとってなじみ深い標準的な Web テクノロジ (HTTP、SOAP、プロキシ、SSL など) に基づく通信。
- HTTPS エージェントから HP Operations 管理サーバーへのメッセージのセキュリティ保護に利用される XML および SOAP をベースとした HPOM メッセージフォーマット。
- IP 非依存 / ダイナミック IP (DHCP)。管理対象ノードを一意の `OvCoreID` で識別することができ、IP アドレスに依存する必要がありません。
- 追加投資 (トレーニング、追加ソフトウェアなど) が不要。
- HP Operations の標準の制御 / 配布メカニズム。
- HP Operations の標準のロギングケーパビリティ。
- HP Operations の標準のトラッキングケーパビリティ。

HP Operations HTTPS エージェントのアーキテクチャ

次の図は HPOM における HTTPS 通信のアーキテクチャを示しています。

図 3-2 HTTPS エージェントのコンポーネントと担当範囲

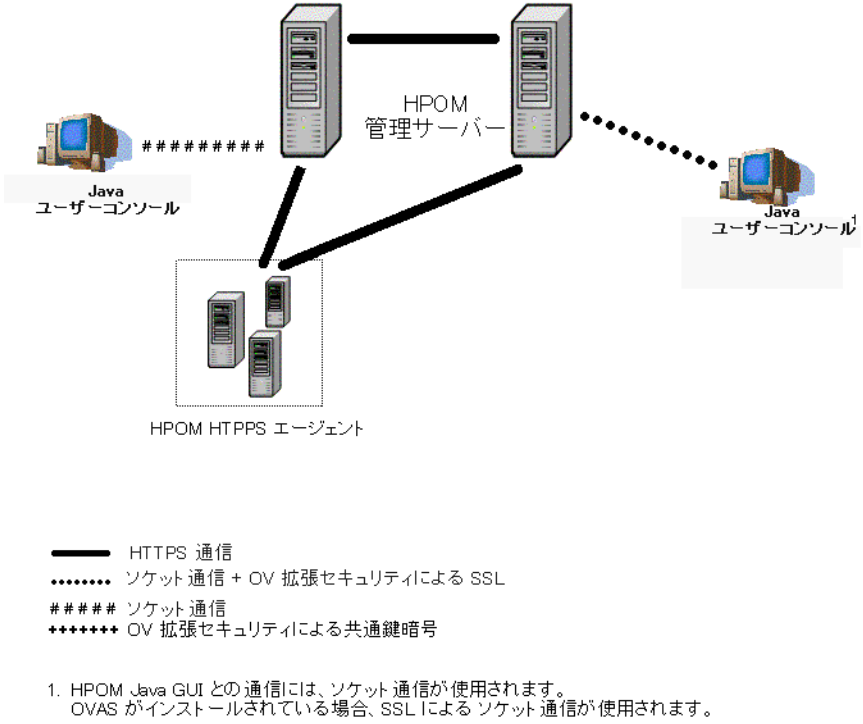


HPOM における HTTPS 通信

HTTPS 1.1 ベースの通信は HP BTO Software 製品が採用している最新の通信テクノロジであり、アプリケーションは異機種混在システム間でデータを交換できます。

HTTPS 通信を採用している HP BTO Software 製品は相互に通信できるだけでなく、業界のその他の標準的製品とも簡単に通信できます。また、現在では、ネットワーク上の既存の製品と通信し、環境内のファイアウォールおよび HTTP プロキシと簡単に統合できる新製品もより簡単に作成できます。図 3-3 は HTTPS 通信の例を示しています。

図 3-3　HP Operations Manager における通信の概要



メリット

HTTPS 通信の主なメリットは次のとおりです。

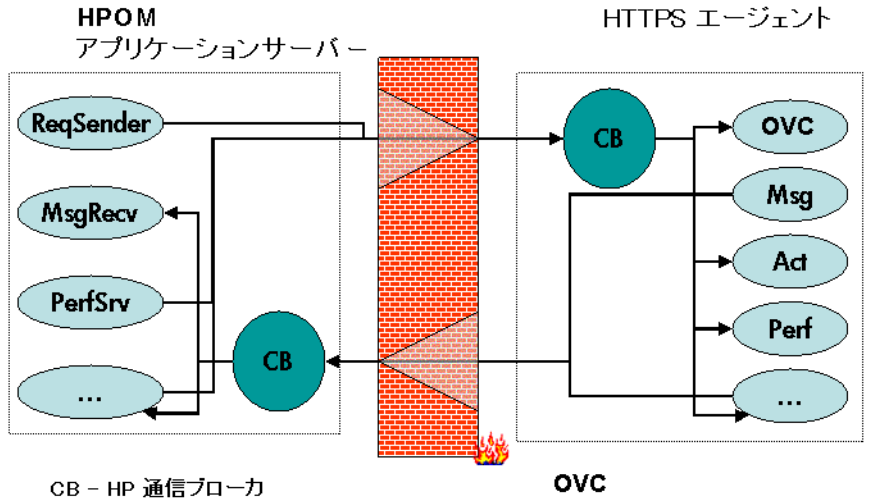
- ファイアウォールとの親和性
- 安全性
- オープン性
- スケーラビリティ

ファイアウォールとの親和性

多くの企業は、ファイアウォールを通過するための安全、セキュア、かつ管理が簡単な方法を求めています。ほとんどの企業にとって、HTTP、HTTP プロキシ、ファイアウォールは見慣れたものであり、違和感はありません。これらの企業の IT 環境は、HTTP プロキシとファイアウォールを経由して通信を行えるようにすでに設定されています。すでにほとんどの IT インフラストラクチャの一部として利用されているテクノロジに注目することは、新たなトレーニングを必要とすることなく効果と効率を高める上で役立ちます。最終的にはサポートとメンテナンスのコストを削減するのと同時に、大幅な手間をかけずに安全性の高い環境を構築できます。

図 3-4 は HTTPS 通信におけるファイアウォールの通過を示しています。

図 3-4　HTTPS 通信におけるファイアウォールの通過



安全性

HP Operations の HTTPS 通信は、信頼性の高いネットワーキングのための業界標準である TCP/IP プロトコルをベースとしています。Secure Socket Layer (SSL) プロトコルを使用する HTTPS 通信は、データにアクセスするユーザーを認証によって検証し、データ交換のセキュリティを暗号化によって保護します。インターネットやプライベートイントラネットを通じてやり取りされる業務上のトランザクションは増え続けており、セキュリティと認証の役割は特に重要性を増しています。

HP Operations の HTTPS 通信は、確立された業界標準を採用することで、この目標を達成しています。データの整合性とプライバシーは、HTTP プロトコルと SSL 暗号化の組み合わせ、および認証によって確保されます。非 SSL 接続でもデータがクリアテキスト形式で伝送されることがないように、データはデフォルトで圧縮されます。

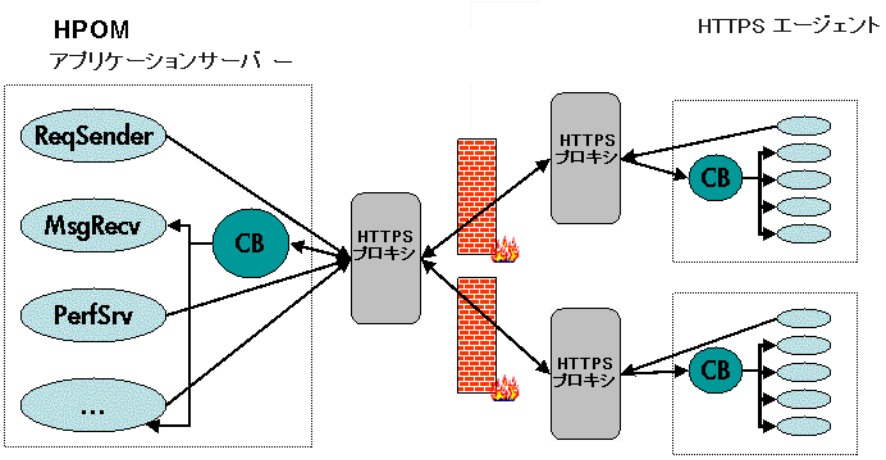
さらに次のような特徴があります。

- 受信するすべてのリモートメッセージ / リクエストは Communication Broker を経由するため、ノードへの単一のポートエントリが提供されます。

- ファイアウォールを設定する際は、限定されたバインドポート範囲を利用できます。
- ファイアウォールを通過する、またはメッセージ、ファイル、オブジェクトの送信時にリモートシステムに到達できるように、1 つまたは複数の標準 HTTP プロキシを設定します。

図 3-5 は標準の HTTPS プロキシを利用したファイアウォールの通過を示しています。

図 3-5　外部 HTTPS プロキシを利用したファイアウォールの通過



HTTPS 通信およびプロキシを使用するには、次の処理が必要です。

- HTTP プロキシサーバーを設定します。
- SSL 暗号化を実装します。
- サーバー証明書によってサーバー側の認証を確立します。
- クライアント証明書によってクライアント側の認証を確立します。

HP Operations でこの処理を行う方法については後述します。

オープン性

HP Operations の HTTPS 通信は、業界標準の HTTP 1.1 プロトコルと SSL ソケットをベースに構築されています。HP Operations は、ユーザーが既存の HTTP インフラストラクチャを最大限に活用できるように、HTTP、SSL、SOAP などのオープン標準に準拠しています。

注記

HPOM エージェント用のコンテンツフィルタリングはサポートされません。

HTTP プロキシは、今日のネットワークでは広く利用されています。これは、プライベートネットワークからインターネットへの安全な橋渡しに役立ちます。HTTP の採用により、HP Operations を追加投入しても既存のインフラストラクチャを活用できます。

スケーラビリティ

HP Operations の HTTPS 通信は、環境の規模や送受信されるメッセージの数に関係なく優れた性能が得られるように設計されています。HP Operations の HTTPS 通信は、稼働環境に合わせて設定できます。大規模なアプリケーションは、最小限のリソースで多数の同時接続に対応できます。設定されている最大接続数を超過した場合は、ログファイルにエントリが作成され、それに基づいて警告メッセージを出力することもできます。

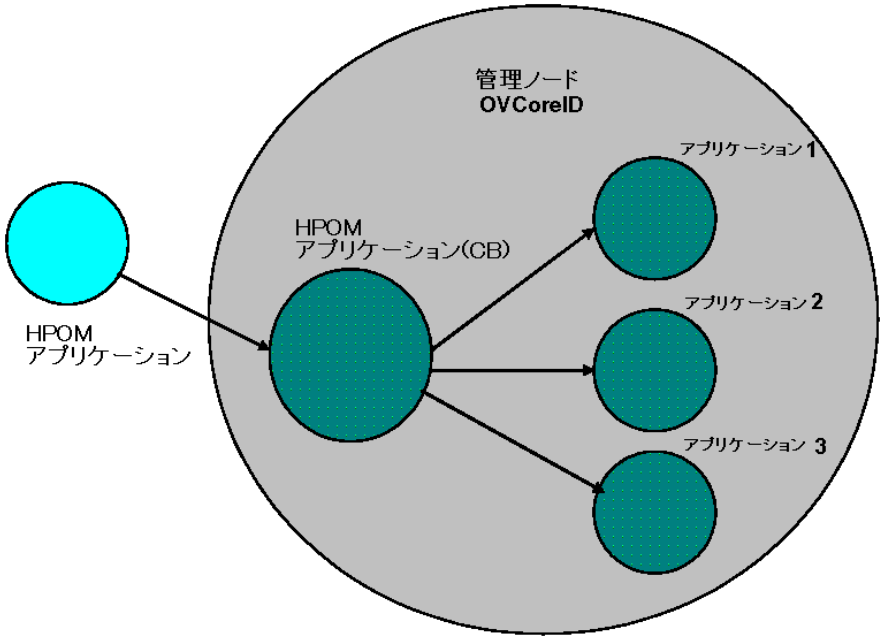
Communication Broker のアーキテクチャ

Communication Broker は管理対象ノード上でプロキシのように機能し、その管理対象ノード上のすべてのアプリケーションに対し、管理対象ノードへの一元的なエントリポイントを提供します。データの受信を必要とするアプリケーションは、Communication Broker にアドレスを登録します。登録により、ポート番号、プロトコル、バインドアドレス、およびアプリケーションがデータの受信に使用するベースパスが定義されます。ローカル / リモートのその他のアプリケーションは、登録済みアプリケーションの場所を Communication Broker にクエリするか、Communication Broker をプロキシとして利用し、これらのアプリケーションにリクエストを転送します。Communication Broker は、HP Operations の標準設定ファイルから設定データをロードします。

Communication Broker の特徴は次のとおりです。

- Communication Broker は管理対象ノードの単一ポートソリューションを提供します。管理対象ノード上のすべての登録済みサーバーへのリクエストは、Communication Broker 経由で送信できます。Communication Broker は、HTTP プロキシが HTTP リクエストを転送するのと同じ要領で、リクエストを登録済みサーバーに透過的に転送します。Communication Broker のデフォルトポートは 383 ですが、これは変更可能です。
- Communication Broker の起動に `chroot` を利用し、UNIX システムのセキュリティを向上させることができます。`chroot` は、指定されたパスをルートディレクトリとして機能させることで、ファイルシステム上で Communication Broker プロセスが認識する部分を制限し、結果としてハッカーへの露出を低下させます。
- ポート番号が 1025 以上の場合、UNIX システムの非 root ユーザーとして Communication Broker を実行できます。
- Communication Broker は、UNIX システムの root ユーザーのみが実行してポートを開き、その上でその他すべての操作用に非 root ユーザーに切り替えるように設定できます。
- Communication Broker は次の操作に対応しています。
  - UNIX システムのデーモンとして起動する
  - Windows システムの Windows サービスとしてインストールする
- Communication Broker の制御コマンドは、対象をローカル管理対象ノードのみに制限できます。
- ネットワーク経由のデータ通信に対し、Communication Broker は SSL 暗号化を適用します。
- Communication Broker は、送信者と受信者の保証された識別情報を通じて SSL 認証を適用します。

図 3-6　　Communication Broker のアーキテクチャ



Communication Broker は、管理対象ノードへの着信データの受け付け用に最低でも 1 つのポートを設定します。管理対象ノードを識別するために、ポートには OVCoreID が割り当てられます。Communication Broker は、高可用性管理対象ノード用に複数のポートを開くように設定できます。各ポートには異なる ID を割り当てることができます。SSL が有効な場合、ポートには X509 証明書が設定されます。この証明書により、接続側のアプリケーションはメッセージの送信者と受信者の両方の識別情報を検証できます。

Communication Broker に登録されている、管理対象ノード上のすべてのアプリケーションは、Communication Broker によって開かれたすべてのアクティブ着信ポートを利用できるように自動的に登録されます。

Communication Broker を起動すると、デフォルトの名前空間 (`bbc.cb`) に関連付けられているポートが自動的にアクティブ化されます。その他のポートは起動後に動的にアクティブ化 / 非アクティブ化できます。詳細については Communication Broker のコマンド行インタフェースパラメータを参照してください。

セキュリティの概念

ここでは、HPOM のセキュリティの概念に関する次のトピックについて説明します。

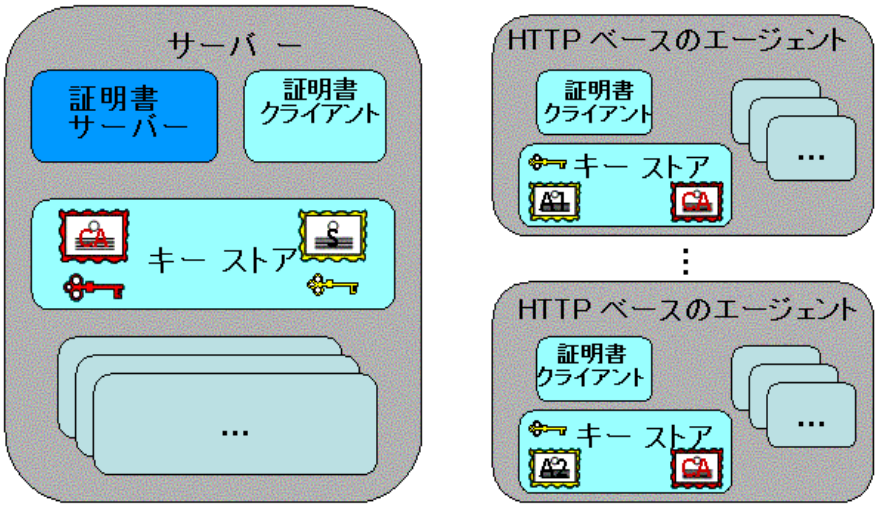
HTTPS ベースのセキュリティコンポーネント

管理対象ノードが HP Operations 管理サーバーと通信するには、HP 証明書サーバーによって発行された、業界標準の有効な X509 証明書が必要です。Secure Socket Layer (SSL) プロトコルを使用している管理対象環境内の管理対象ノードを識別するには、1024 ビット鍵によって署名された証明書が必要です。2 つの管理対象ノードの間で「SSL ハンドシェーク」が成立するのは、着信側管理対象ノードが提示する証明書の発行元認証局が、受信側管理対象ノードで信頼される認証局である場合のみです。証明書の作成と管理を担当する通信セキュリティのメインコンポーネントは次のとおりです。

- HP 証明書サーバー
- HP キーストア
- HP 証明書クライアント

図 3-7 はこれらのコンポーネントを示しています。

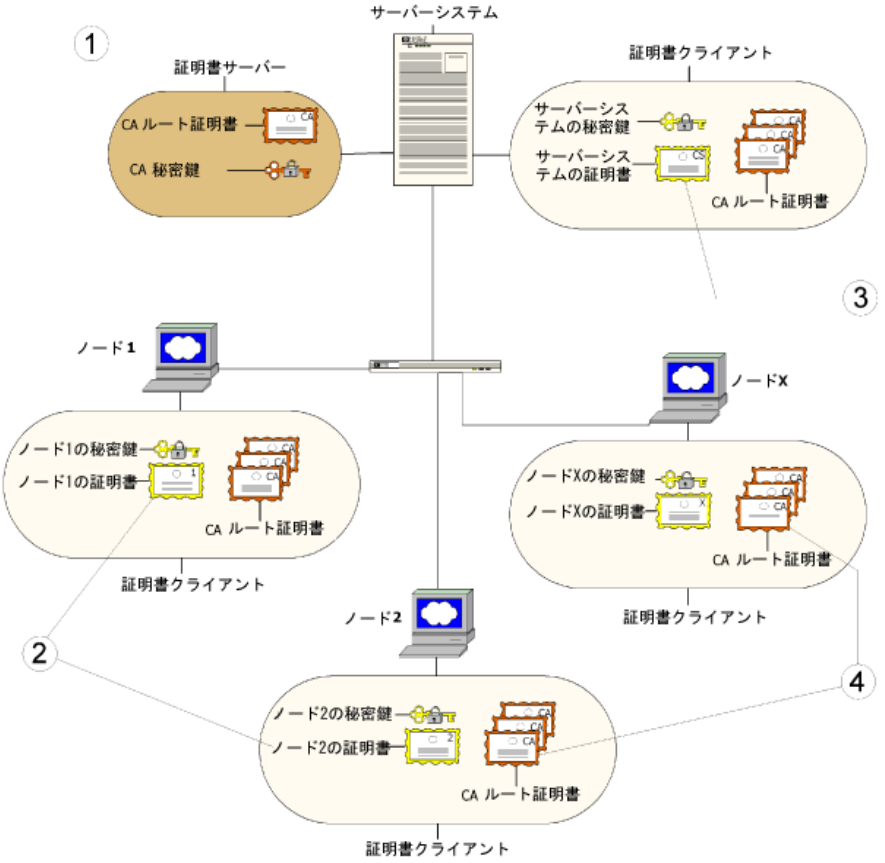
図 3-7　認証通信に使用されるコンポーネント



`OvCoreId` は、各 HP Operations システム (管理対象ノードまたはサーバー) の一意の ID として使用されます。この ID は、対応する管理対象ノード証明書に含まれます。`OvCoreId` の値はインストール時に割り当てられます。

図 3-8 は認証通信の環境を示しています。

図 3-8　認証通信の環境



1. サーバーシステムが、必要とされる認証局 (CA) 機能を持つ証明書サーバーをホスティングします。
2. すべてのシステムには、証明書サーバーが認証局の秘密鍵を使って署名した証明書が設定されます。
3. 識別情報を示すため、サーバーシステムにも証明書が必要です。
4. すべてのシステムには、信頼されたルート証明書のリストがあり、ここには少なくとも 1 つの証明書が含まれている必要があります。信頼されたルート (CA) 証明書は、通信相手の識別情報の検証に使用されま

す。通信相手は、提示した証明書が、信頼された証明書のリストを使って検証可能な場合にのみ信頼されます。

証明書クライアントが複数の HP Operations 管理サーバーによって管理されている場合は、信頼されたルート証明書のリストが必要です。たとえば、管理対象ノードが同時に複数の HP Operations 管理サーバーによって管理されている場合がこれに該当します。

証明書

証明書には 2 つの種類があります。

- ルート証明書
- 管理対象ノード証明書

ルート証明書は、証明書サーバーの認証局の識別情報が記録された自己署名証明書です。ルート証明書に属す秘密鍵は証明書サーバーシステムに格納され、未許可アクセスから保護されます。認証局は、認証局のルート証明書を使ってすべての証明書に電子署名します。

管理対象環境内のすべての HTTPS 管理対象ノードは、証明書サーバーによって発行された管理対象ノード証明書、ファイルシステムに保存されている対応秘密鍵、その環境で有効なルート証明書を受け取ります。これは、管理対象ノードで稼働する証明書クライアントによって確実に実行されます。証明書クライアントの詳細については HP Operations エージェントのドキュメントを参照してください。

HP 証明書サーバー

証明書サーバーの役割は次のとおりです。

- 自己署名ルート証明書を作成 / インストールする。
- 自己署名ルート証明書をファイルシステムからインポートする。
- ルート証明書の秘密鍵を保存する。
- 証明書リクエストを承諾 / 拒否する。
- 新しい証明書と対応秘密鍵を作成する、または証明書の手動インストール用にインストールキーを作成する。
- 信頼されたルート証明書をクライアントが自動的に取得できるようにサービスを提供する。

認証局 (CA)

注記

すべての HP Operations 管理サーバーは自動的に認証局として設定されます。すべてのエージェントの sec.cm.client:CERTIFICATE_SERVER のデフォルト設定は、そのエージェント自体の HP Operations 管理サーバーです。

認証局は証明書サーバーの一部であり、証明書管理の信頼性の中心です。この認証局が署名した証明書は有効な証明書と見なされ、信頼されます。認証局は、安全性の高い場所でホスティングする必要があります。デフォルトでは、HP Operations 管理サーバーをホスティングするシステムにインストールされます。

認証局自体が信頼の根源であるため、認証局の動作には自己署名のルート証明書が使用されます。認証局が動作できるように、このルート証明書と対応秘密鍵は一定の保護レベルの下にファイルシステムで作成 / 保存されます。正しく初期化された認証局はルート証明書を使用して、承諾された証明書リクエストへの署名を担当します。

リモートアクションの認証

セキュリティの観点から言えば、リモートアクションは HPOM 管理対象環境では特別なケースであるといえます。偽のリモートアクションを管理サーバーに送信し、環境内の指定のリモートシステムでそのアクションを実行できるようなことがあってはなりません。特に、どの管理対象システムもセキュアなシステムと見なすことができないため、これは微妙な問題です。未許可ユーザーであっても管理対象ノードにルートアクセス可能であると考えられます。

さらに、サービスプロバイダの 1 つの HP Operations 管理サーバーが複数の顧客の環境の管理に対応する必要があり、ある顧客セグメントに配置されたシステムが別の顧客セグメントでアクションを開始できないようにする必要があります。

HPOM は、アクション文字列 (具体的なコマンドなど) が悪意のあるユーザーによって改ざんされないことを保証します。HP Operations 管理サーバーでは、次の項目を設定できます。

- HP Operations 管理サーバーがどのシステムでアクションを実行できるか
- HTTPS エージェントからの「署名されたアクション」のみを受け付けるようにするかどうか

メッセージの送信側システム以外のシステムを対象とするアクションが指定された HPOM メッセージ内のアクションリクエストはリモートアクションであり、セキュアに対応する必要があります。これらのリモートアクションは、後述する追加のセキュリティチェックの対象となります。リモートアクションは、これらのセキュリティチェックを通過できた場合にのみ実行されます。

次の一般ルールが適用されます。

- リモートアクションは、管理対象ノード A が送信した HPOM メッセージに定義され、管理対象ノード B で実行するように設定されている自動アクションまたはオペレータ起動アクションとして定義されます。このようなアクションの実行は、次のファイルを使って制御できます。

  `/etc/opt/OV/share/conf/OpC/mgmt_sv/remactconf.xml`

- リモートアクションが含まれるメッセージを HPOM 管理サーバーが受信すると、メッセージは常にリモートアクション設定ファイル (remactconf.xml) に指定されているルールに基づいて処理されます。この設定ファイルが変更されている場合は、処理前に再ロードされます。
- リモートアクション設定ファイルが存在しない、空である、判読不能である、またはルールが指定されていない場合は、すべてのリモートアクションが無効化されます。
- リモートアクションを含むメッセージは、設定ファイルに指定されているのと同じ順序でルールと比較されます。最初の一致で結果が確定します。`deny` 句はメッセージ内のリモートアクションを無効化し、メッセージに適切な注釈を追加します。それ以外の場合は、実際のメッセージは通常どおりに処理されます。`allow` 句はメッセージを変更せずにそのまま残します。
- メッセージがどのルールとも一致しない場合は、リモートアクションは `deny` ルールと一致した場合と同様に無効化されます。

- ルールは、すべてのルール要素と AND 論理で一致した場合に一致と見なされます。<target> タグが指定されていない場合など、考えられるルール要素が省略されている場合は、適切なすべてのメッセージ値と一致します。ただし、これは <certified> タグには適用されません。このタグが指定されていない場合は、デフォルト値の true が適用されます。
- リモートアクション設定ファイルに構文エラーやその他の論理エラー (存在しないノードグループなど) が含まれる場合、解析はそこで停止し、残るすべてのルールは無視されます 。
- trust セクションはサポートされません。
- certified タグのデフォルト値は true です。これは、認定された送信元からメッセージが送信され、メッセージ証明書が検証されたことを意味します。<certified>true</certified> 句を含むルールは、HTTPS ノードからのメッセージと一致します。

リモートアクションを認証するためのサーバー設定の詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

ロールとアクセス権

一般に、ロールは特定の作業を実行するための権限を付与します。たとえば、HPOM 環境では、アクションの実行、ファイルの配布、設定の変更などを行うための権限があります。次に説明する、あらかじめ設定されている HPOM ロールには、それぞれにアクセス権のデフォルトセットが割り当てられています。これらの権限を変更する方法については、『*HPOM システム管理リファレンスガイド*』および HP Operations エージェントのドキュメントを参照してください。

ロールについて

HP Operations 管理サーバーは、あらかじめ設定された HPOM ロールを引き継ぐことができます。管理サーバーとロールのマッピングは sec.core.auth 名前空間に定義され、MoM 環境では、該当するマネージャのポリシーに定義されます。

HPOM 環境には、あらかじめ次のロールが設定されています。

- **ローカルユーザーロール**

  ローカルユーザーロールは、適切なシステム権限 (たとえば、root) が付与されれば、すべての権限を持ちます。

- **初期または承認済みマネージャロール**

  このマネージャはすべての権限を持ち、インストール時に設定されます。このロールはセキュリティ名前空間 sec.core.auth の MANAGER および MANAGER_ID の設定によって定義されます。初期マネージャの数は 1 つに制限されています。

- **二次マネージャロール** (MoM 環境のみ)

  二次マネージャは、アクションの実行や設定の配布など、すべての権限を持ちます。該当するマネージャのポリシーには、複数の二次マネージャを定義できます。初期マネージャと二次マネージャは、設定サーバーの候補グループを構成します。

- **アクション許容マネージャロール** (MoM 環境のみ)

  アクション許容マネージャには、アクションの実行権限以外の権限はありません。該当するマネージャのポリシーには、複数のアクション許容マネージャを定義できます。

アクセス権について

アクセス権は、たとえば、アクションの実行、ファイルの配布、設定の変更などを行うための権限です。権限は、149 ページの「ロールについて」で説明した HP Operations 管理サーバーのロールにマッピングされます。

設定の無人配布の回避およびリモートアクセスの拒否については、『*HPOM システム管理リファレンスガイド*』を参照してください。

アクセス権の制限については、『*HPOM システム管理リファレンスガイド*』および HP Operations エージェントのドキュメントを参照してください。

認証のマッピング

次の表は、HPOM 管理サーバーの各ロールの個別のデフォルトアクセス権を示しています。

表 3-1　認証のマッピング

コンポーネント	権限	値	初期マネージャ	二次マネージャ	アクション許容マネージャ
<comp_name>		*<dec_value>*	*<HPOM_mgr_role>*		
制御 (ctrl)	起動	1	あり	あり	なし
	停止	2	あり	あり	あり
	ステータス	4	あり	あり	なし
	通知	8	あり	あり	なし
	デフォルト値：	**15**	**15**	**15**	**2**
設定 (conf)	ポリシーのインストール	1	あり	あり	なし
	ポリシーの削除	2	あり	あり	なし
	ポリシーの有効化	4	あり	あり	なし
	ポリシーの無効化	8	あり	あり	なし
	ポリシーのリスト表示	16	あり	あり	あり
	ポリシーヘッダーの更新	32	あり	あり	なし
	設定内容の読み取り	64	あり	あり	あり
	設定内容の書き込み	128	あり	あり	なし
	ポリシーへの署名	256	あり	あり	なし
	デフォルト値：	**511**	**511**	**511**	**80**

表 3-1　　認証のマッピング (続き)

コンポーネント	権限	値	初期マネージャ	二次マネージャ	アクション許容マネージャ
<comp_name>		*<dec_value>*	*<HPOM_mgr_role>*		
配布 (depl)	ファイルの配布	1	あり	あり	なし
	ファイルまたはディレクトリの削除	2	あり	あり	なし
	ファイルの取得	4	あり	あり	なし
	ファイルの実行	8	あり	あり	なし
	パッケージの配布	16	あり	あり	なし
	パッケージの削除	32	あり	あり	なし
	パッケージのアップロード	64	あり	あり	なし
	パッケージのダウンロード	128	あり	あり	なし
	インベントリの取得	256	あり	あり	あり
	インベントリの変更	512	あり	あり	なし
	ノード情報の取得	1024	あり	あり	あり
	デフォルト値 :	**2047**	**2047**	**2047**	**1280**
アクションエージェント (eaagt.actr)	アクションの実行	1	あり	あり	あり
	デフォルト値 :	**1**	**1**	**1**	**1**

HTTPS ノードの管理

HTTPS ノードに対して HP Operations 管理サーバーが実行できる機能は次のとおりです。

- HTTPS エージェントのリモート制御
- HTTPS エージェントのリモート / 手動インストール
- リモート / 手動パッチインストールおよびエージェントのアップグレード
- リモート / 手動による設定の配布
- HTTPS エージェントの複数の設定サーバーの並行サポート
- 定期ポーリング
- HTTPS ノードのセキュリティ管理
- HP Operations 管理サーバー API およびユーティリティを利用した HTTPS ノードのサポート

次に、これらの HTTPS ノードの概念の一部について説明します。

- 154 ページの「HTTPS ノードへの設定の配布」
- 158 ページの「HTTPS ノードのリモート制御」

HTTPS ノードの管理の詳細については HP Operations エージェントのドキュメントを参照してください。

HTTPS ノードへの設定の配布

次に、HTTPS エージェントで導入された設定管理の概念について説明します。

ポリシーの管理

HPOM ポリシーは、汎用ポリシーをデータベースに登録し、管理対象ノードに割り当て、管理対象ノードに配布できるように管理されます。HPOM 9.xx 管理サーバーでは、ポリシーに複数のバージョンを持たせ、ツリー状の構造に構成できます。ポリシーにはカテゴリの割り当てを含めることもできます。**カテゴリ**は、関連するインストルメンテーションファイルをまとめ、管理対象ノードに配布しやすくします。

ポリシーとポリシータイプについては 75 ページの「HPOM ポリシー」を参照してください。

ポリシーに関連する管理作業、複数バージョンの管理、管理対象ノードへの HPOM 設定の配布については、『*HPOM システム管理リファレンスガイド*』を参照してください。

インストルメンテーションの管理

HP Operations 管理サーバーの実行ファイルのディレクトリは次の場所にあります。

```
/var/opt/OV/share/databases/OpC/mgd_node/
```

インストルメンテーションデータのカテゴリが作成された場合を除き、インストルメンテーションディレクトリは作成されず、アクション、コマンド、モニターのディレクトリが使用されます。

通常、アクション、コマンド、モニターの実行ファイルは HPOM ポリシーで参照されます。バイナリの新しい場所は、HPOM のアクションエージェント、モニターエージェント、ログファイルエンキャプスレータなどのユーティリティのパス変数にも追加されるため、これらの実行ファイルがポリシー内で完全パスによって参照されていない限り、この変更についてユーザーが気にする必要はありません。

HP Operations 管理サーバーのモニターディレクトリからのファイルは権限 744 でエージェントにインストールされ、それ以外はすべて権限 755 でインストールされます。

設定管理プロセスは、実行中の実行可能ファイルも更新できます。それぞれのタスクを完了できるように、実行中の実行可能ファイルのスクリプトおよびバイナリの名前は変更されます。これらのプログラムのそれ以後の実行には、新たにインストールされたファイルが使用されます。

インストルメンテーションデータの配布と複数バージョンの管理については、『*HPOM システム管理リファレンスガイド*』を参照してください。

ポリシーとインストルメンテーションの手動インストール

エージェントは設定データを安全な形式で受信する必要があるため、ポリシーデータを管理対象ノードに直接コピーすることはできません。これは、未許可ユーザーが管理対象ノードで設定データを不正に操作できないようにするためです。

ポリシーを HP Operations 管理対象ノードに手動インストールする準備には `opctmpldwn` ツールを使用します。出力データは、管理サーバーシステム上の管理対象ノード専用ディレクトリに保存されます。

`opctmpldwn` は HTTPS ノードを次のように処理します。

- `nodeinfo` と `mgrconf` のデータはポリシーと見なされるため、前述のディレクトリに保存されます。
- ポリシーは、ノード固有の鍵を使って暗号化されます。

HTTPS エージェント配布マネージャ

`opcbbcdist` は、HP Operations 管理サーバーと HTTPS エージェントの間の設定管理アダプタです。主な機能は次のとおりです。

- テンプレートをポリシーに変換する
- 既存のアクション、コマンド、モニターからインストルメンテーションを作成する
- ECS テンプレートをポリシーと関連サーキットに変換する
- `nodeinfo` の設定を HTTPS で使用される XPL 形式に切り替える

`opcbbcdist` は、次の内部ファイルシステムインタフェースを使用します。

`/var/opt/OV/share/tmp/OpC/distrib`

これにより、配布すべきデータに関する情報を取得します。次の 4 つの設定カテゴリは区別されます。

- ポリシー / テンプレート
- インストルメンテーションアクション / コマンド / モニター
- nodeinfo
- mgrconf

opcbbcdist が他の HP Operations 管理サーバーコンポーネントから受け付けるリクエストは、deploy configuration types xyz to node abc (設定タイプ xyz をノード abc に配布) という形式のリクエストのみです。これらのリクエストは、設定 API、または opcragt -update および opcragt -distrib によって発行されます。

opcbbcdist には自動再試行メカニズムが用意されています。このメカニズムは、ノードに到達できず、そのノードの新しいデータが存在する場合に起動されます。opcragt -update を呼び出して手動で再試行を開始することもできます。opcbbcdist が特定ノードのタスクを完了すると、設定データが正しく配布されたことを示すメッセージがブラウザに表示されます。タスクが完了しなかった場合は、**ノード到達不能**などのメッセージが表示されます。

opcbbcdist は、先にインストルメンテーションデータを転送し、次にポリシーを転送します。これは、ポリシーで実行可能ファイルが参照されていた場合の同期の問題を回避するためです。また、opcbbcdist のトランザクションモデルはシンプルです。特定の設定タイプのすべてのデータが正しく配布された場合にのみ次のカテゴリを処理します。1 つの設定タイプの配布は 1 トランザクションと見なされます。失敗したトランザクションはロールバックされ、後で再試行されます。このスキーマは、HP Operations サーバーのシャットダウンにより opcbbcdist が停止された場合にも適用されます。

設定のプッシュ

HTTPS ノードへのすべての設定配布タスクは HP Operations 管理サーバーによって開始されます。HP Operations サーバーは設定データをエージェントにプッシュします。この際の通信は送信のみです。管理対象ノードは、より安全な HP Operations 管理サーバーによって起動されます。

デメリットは、新しい設定を配布してもシステムに到達できない場合、管理対象ノードを古いデータで実行しなければならないことです。HP Operations 管理サーバーはすべてのノードをポーリングし、存在するのに配布できていない設定を確認する必要があります。HP Operations 管理サーバーは、この処理を次のタイミングで実行します。

- ペンディング中の各ノードで 1 時間に 1 回以上
- サーバーの再起動時
- `opcragt -update` または `opcragt -distrib` を使って、またはコマンドに関連する API を直接呼び出して設定が明示的にプッシュされたとき

ペンディング中の配布のチェックは、`dist_mon.sh` というモニターによって行われます。次の設定転送ディレクトリに

`/var/opt/OV/share/tmp/OpC/distrib`

30 分以上経過したデータが含まれている場合、配布がペンディングされている管理対象ノードを示すメッセージが表示されます。

差分配布

HPOM のデフォルトの配布プロセスは差分配布です。このプロセスでは、設定が最後に転送されてから変更 / 追加されたデータのみが配布されます。これにより、転送するデータの容量が最小化され、インターセプタなどのサブエージェントへの再設定リクエストの数を減らすことができます。必要に応じて設定全体を管理対象ノードに再配布することもできます。

差分配布モードでは、HP Operations 管理サーバーは管理対象ノードのポリシーインベントリと、前回のインストルメンテーション配布のタイムスタンプを要求します。ポリシーインベントリはポリシー割り当てリストと比較され、ノードに必要なポリシーの削除 / インストール作業が `opcbbcdist` によって計算 / 実行されます。インストルメンテーションの配布では、前回の配布のタイムスタンプと、管理サーバーのインストルメンテーションディレクトリ内のタイムスタンプが比較されます。HP Operations 管理サーバー側のファイルの中で、管理対象ノード側の対応するファイルより新しいすべてのファイルが配布されます。オプションを指定したコマンド行コマンド `opcragt -purge` を実行する場合を除き、管理対象ノードからインストルメンテーションデータが削除されることはありません。

HTTPS ノードのリモート制御

HP Operations 管理サーバーからエージェントを制御するには、opcragt ユーティリティを使用します。これらの操作には、起動、停止、ステータスの取得、一次マネージャの切り替え、設定変数の取得 / 設定、設定の配布が含まれます。HTTPS ノードには opcagt というラッパーがあります。このユーティリティを使用することで、オペレータのデスクトップからアプリケーションを起動してリモート制御作業を実行できます。これにより、すべての管理対象ノードに共通するアクション定義を設定できます。

HTTPS ノードでは、サブエージェントは名前で識別されます。このため、次の形式のエイリアスを指定できます。

< エイリアス >< マップ先 >

指定先は次の設定ファイルです。

/etc/opt/OV/share/conf/OpC/mgmt_sv/subagt_aliases

あらかじめ、1 EA と 12 CODA の 2 つのエントリが定義されています。HTTPS 管理対象ノード用に -id 1 を -id EA に変換するには、次のコマンドを実行します。

opcragt -status -id 1 *< ノードリスト >*

証明書の作成と配布

暗号化を伴う Secure Socket Layer (SSL) プロトコルによるネットワーク通信には、証明書が必要です。サーバーとクライアントの認証が有効になります。管理対象環境の管理対象ノードは、証明書によって識別されます。2 つの管理対象ノードの間で「SSL ハンドシェーク」が成立するのは、着信側管理対象ノードが提示する証明書の発行元認証局が、受信側管理対象ノードで信頼される認証局である場合のみです。

証明書のインストールは自動 / 手動で行うことができます。証明書のインストールのモニターには HPOM メッセージが使用されます。証明書リクエストが自動的に承諾された場合は、証明書が正しく配布されたことを示す通知メッセージがメッセージブラウザに送信されます。証明書リクエストが自動的に承諾されない場合は、リクエストが拒否された理由と、障害を解決するために管理者が実行しなければならない手順を示すメッセージがメッセージブラウザに表示されます。

証明書の管理には、コマンド行ユーティリティ `ovcm` および `opccsa` を使用します。証明書リクエストを承諾、拒否、リスト表示、削除したり、証明書リクエストと登録ノード中の対応ノードをマッピングできます。

証明書の操作方法については、『*HPOM システム管理リファレンスガイド*』および HP Operations エージェントのドキュメントを参照してください。

HPOM の仮想ノード

クラスタは、1 つのユニットとしてユーザーにアプリケーション、システムリソース、データを提供する複数のシステム (ノード) です。Veritas Cluster、Sun Cluster、TruCluster などの最近のクラスタ環境では、アプリケーションはリソースの複合物として表されます。これらのリソースはリソースグループを形成し、リソースグループはクラスタ環境で実行されるアプリケーションを表します。この複合物の中で、各リソースには特別な機能があります。

クラスタ環境で実行されるアプリケーションをモデリングする共通のメカニズムがあります。

用語

HPOM では、高可用性に関連する次の用語と略号が使用されます。

高可用性に関する一般用語

HA (高可用性)

高可用性は、リソースの冗長構成によってダウンタイムから保護される、ビジネスクリティカルな環境の特徴を表す一般用語です。多くの場合、クラスタシステムは高可用性を実現するために使用されます。

HA クラスタ (高可用性クラスタ)

高可用性クラスタは、HP ServiceGuard (HP/SG)、Veritas Cluster、Sun Cluster などのクラスタ管理アプリケーションによってグループ化されたハードウェアリソースです。高可用性を保証するために、複数のコンピュータ、冗長ネットワーク接続、ミラー化されたストレージデバイスなど、冗長構成されたリソースが使用されます。

HA パッケージ | HA リソースグループ | クラスタパッケージ | HARG

これらの用語はいずれも「クラスタの世界」で定義され、アプリケーションインスタンスにリンク可能なリソースを表します。これはクラスタ上で実行され、1 つのクラスタノードから別のクラスタノードに切り替えることができます。通常、クラスタパッケージは仮想ノードという「ネットワークの世界」の要素にもリンクされます。

仮想ノード

仮想ノードは、HA クラスタで実行されるアプリケーションパッケージをネットワーク側から表現した用語です。通常、仮想ノードはホスト名と IP アドレスを持ち、名前解決システムによって認識され、通常のシステムと同様にアドレスを指定できます。

物理ノード | クラスタノード

クラスタハードウェアに属し、HARG のホストになることができる単一システムです。クラスタは複数の物理ノードから構成されます。

スイッチオーバー

負荷分散などの理由による、あるクラスタノードから別のクラスタノードへのクラスタパッケージの制御された切り替え。

フェイルオーバー

アプリケーションエラーなどの理由による、あるクラスタノードから別のクラスタノードへのクラスタパッケージの計画外の切り替え。

HPOM で使用されるクラスタ関連の用語

HPOM 仮想ノード

HPOM 仮想ノードは、HPOM データベース内の HA パッケージを表現するための概念です。仮想ノードには、HA パッケージに属すホスト名と IP アドレスが割り当てられます。HPOM 仮想ノードには HARG Name 属性があります。通常、この属性の値は HA リソースグループ名です。HPOM 仮想ノードは、クラスタ上で HA リソースグループを実行できる物理ノードから構成されます。

ClAw (クラスタ認識)

ClAw (クラスタ認識) は、クラスタパッケージの起動 / 終了イベントをモニターするための HPOM の機能です。ClAw ソフトウェアはローカルノードの起動 / 停止イベントしかモニターしないため、モニターするクラスタの各物理ノードに ClAw モジュールをインストールする必要があります。ClAw モジュールは HPOM HTTPS エージェントの一部であり、その機能は ovconfd プロセスに含まれます。

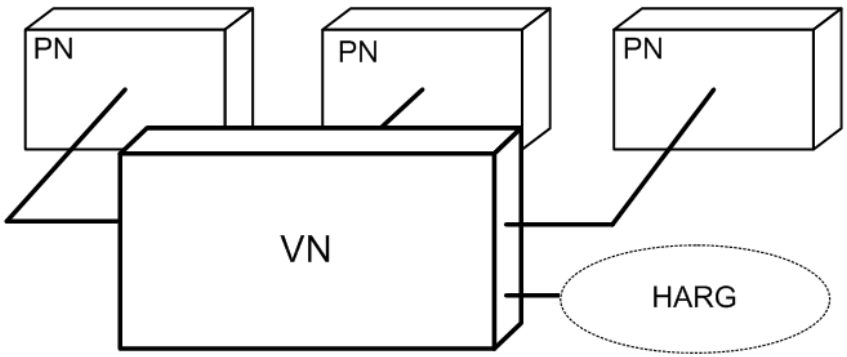
HARG Name (高可用性リソースグループ名)

HARG Name は、HPOM データベース内の HPOM 仮想ノードに割り当てることができる文字列属性です。HPOM では、HARG 名はクラスタ内の HA リソースグループの名前と同じである必要があります。この名前は、HPOM の世界 (HPOM データベース) とクラスタの世界を結ぶリンクです。

仮想ノードの概念

HPOM 仮想ノードは、共通の HA **リソースグループ**名によってリンクされた物理ノードのグループと見なすことができます。仮想ノード内でパッケージ自体が切り替わると、これらの物理ノード上のエージェントの ClAw (クラスタ認識) 拡張によって物理ノード上のポリシーを切り替えることができます。

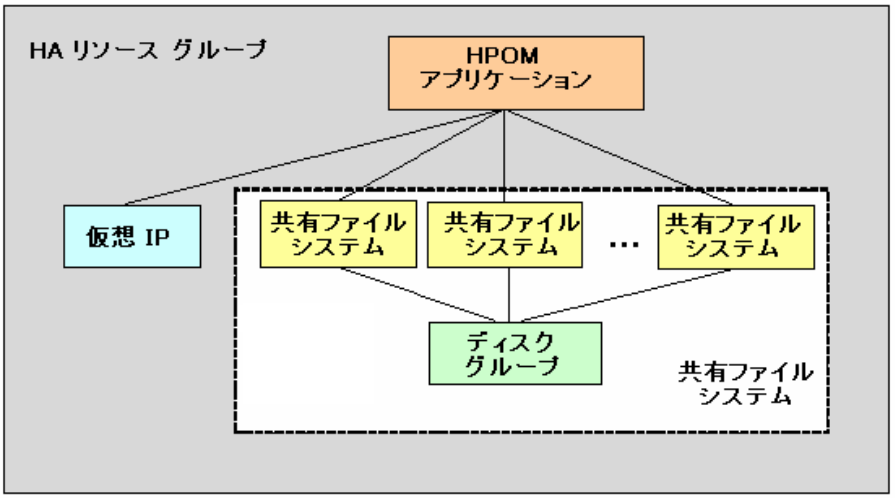
図 3-9 **仮想ノード**



HA **リソースグループ**名による管理ノードのリンクには次のようなメリットがあります。

- 仮想ノードに割り当てられているポリシーなどによって HA **リソースグループ**の範囲内で検出されたイベントは、その名前を発生元ノードの名前として受信できます。
- 管理ステーションの GUI で正しいフィルタリングと強調表示を実行できます。
- サービス名とメッセージキーの適切な相関処理を実行できるので、クラスタを本来の意味で管理できます。

図 3-10　　HA リソースグループ



注記　　この機能を利用できるのは HTTPS ノードのみです。

仮想ノードと関連付けることができる HA リソースグループ名は 1 つだけです。

HA リソースグループ名は複数の仮想ノードに割り当てることができますが、これらの仮想ノードは共通物理ノードを共有できません。これは、両方の仮想ノードに割り当てられたポリシーが同じ HARG 名を 2 回受信し、エージェントの ClAw が仮想ノードを区別できなくなるためです。

仮想ノードの操作方法については、『*HPOM システム管理リファレンスガイド*』を参照してください。

HPOM のプロキシ

ネットワークゲートウェイサーバーにあるファイアウォールプログラムとその関連ポリシーは、プライベートネットワークのリソースを外部ユーザーから保護するためのゲートウェイです。通常、イントラネットユーザーはインターネットの承認済み部分にアクセスすることができ、組織の内部リソースに対する外部からのアクセスはファイアウォールによって制御されます。

ファイアウォールには 2 つの基本カテゴリがあります。

- ネットワークレベルで機能する IP パケットフィルター
- アプリケーションレベルで機能する Web プロキシなどのプロキシサーバー

プロキシは、インターネットデータパケットのヘッダーと内容を調べ、データの送信先システムを保護する上で必要な措置を講じるソフトウェアアプリケーションです。プロキシをセキュリティポリシーと組み合わせることで、容認不可能な情報を削除したり、リクエスト自体を完全に破棄できます。

アプリケーションプロキシの利用には、セキュリティ上の大きなメリットがあります。次に主なものを挙げます。

- プロキシがアプリケーションレベルでパケットを調べるため、詳細なセキュリティ制御とアクセス制御が可能です。たとえば、`.exe` ファイルなどの特定タイプのファイルの転送を制限できます。
- プロキシは、ファイアウォールに対する「サービス拒否」攻撃を防御できます。

プロキシの利用には、よく取り上げられる 2 つのデメリットがあります。

- プロキシは、大量のコンピューティングリソースを必要とします。ただし、高性能のコンピュータの価格が比較的低下しているため、実用上は問題なくなりました。
- プロキシは特定のアプリケーションプログラム用に作成されており、プロキシを簡単に利用できないプログラムが存在する可能性があります。

プロキシサーバーは、内部ネットワークへのアクセスを許可する前にすべての情報を停止して検査します。このため、プロキシを使用した場合は、内部ネットワークと「外界」の間に直接的な通信は存在しなくなります。ユーザーが外部に情報を送信するには、プロキシの認証を受ける必要があります。

イントラネット上のクライアントがインターネットへリクエストを送信しようとすると、実際にはプロキシがそのリクエストを受信します。プロキシは、Network Address Translation (NAT) によってパケットのソース IP アドレスをプロキシサーバーの IP アドレスに変更します。これにより、内部ネットワークユーザーの識別情報は外部に見えなくなります。リクエストが、設定されているポリシーの要件を満たす場合、プロキシサーバーはそのリクエストを目的のアドレスに転送します。リクエストが受信されると、プロセスは反転します。着信するリクエストが安全と見なされる限り、リクエストはネットワーク上の対象クライアントに転送されます。応答のソースアドレスは変更されませんが、送信先アドレスはファイアウォール内のリクエスト送信元コンピュータのアドレスに戻されます。どのネットワークシステムに対しても、直接的で無制御なルートが存在しなくなるため、これによってネットワークのセキュリティが大きく向上します。

プロキシサーバーには 2 つの基本タイプがあります。

- **シングルホームホスト**

  プロキシサーバーのネットワークカードとアドレスは 1 つだけで、プロキシサーバーへのリクエストの転送と、ネットワークへのその他すべての情報のブロックは、インターネットルーターによって行われます。

- **デュアルホーム / マルチホームホスト**

  プロキシサーバーが複数のネットワークカードと関連付けられます。内部ネットワークからのリクエストはいずれかのネットワークカードに送信されます。インターネットからの情報は別のネットワークカードで受信されます。ネットワークカード間のルーティングは設定されないため、着信する情報と送信する情報の間に直接的なつながりはありません。何をどこに送信するかは、プロキシサーバーによって決定されます。

HPOM でのプロキシの設定と、HPOM 管理サーバーでのプロキシの設定については、『*HPOM システム管理リファレンスガイド*』を参照してください。

HPOM のトレース

ここでは、HPOM のトレースに関する次のトピックについて説明します。

HPOM のトレース

障害の原因調査に利用できるように、HPOM には障害トレース機能が用意されています。トレースログファイルは、プロセス / プログラムの異常終了、パフォーマンスの大幅な低下、予期せぬ結果の表示などの障害が、いつどこで発生したかを特定する上で役立ちます。

HPOM で利用できるトレースメカニズムは次のとおりです。

- HP のトレース機能は、最新の HP BTO Software 製品をトレースするためのメカニズムであり、今後リリースされるすべての製品に搭載されます。HP のトレース機能は、HTTPS エージェントや HP Operations 管理サーバーに関連する障害を解決する際に利用できます。

  トレース機能を利用することで、独自形式によるリモートアクセスが可能になります。SSL 暗号化は使用されません。デフォルトの通信ポートは 5053 です。

  HP スタイルのトレース機能の詳細については 168 ページの「HP スタイルのトレース機能の概要」を参照してください。
- 設定内容を利用する HPOM スタイルのトレース機能は、HTTPS エージェントや HP Operations 管理サーバーの障害解決にも利用できます。設定内容は `ovconfchg` コマンドで設定されます。詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

HP スタイルのトレース機能の概要

HP のトレース機能は、**アプリケーション**、**コンポーネント**、**カテゴリ**、**属性**の各要素の階層を採用しています。トレース GUI (またはトレース設定ファイル) でこれらの要素の組み合わせを指定することで、関心のある領域をトレースできます。

表 3-2 は、これらの要素と HPOM のコンポーネント、プロセス、領域の関連性を示しています。

表 3-2　トレース機能の用語

名前	HPOM スタイルでの名前	例
アプリケーション	プロセス OPC_TRC_PROCS および OPC_DBG_PROCS	opcmsga、ovpolicy
コンポーネント	該当なし	opc、eaagt
サブコンポーネント	トレース領域 OPC_TRACE_AREA	actn、msg、init、debug
カテゴリ	OPC_TRACE TRUE	Trace
属性	該当なし	Info、Warn、Error、Developer、Verbose

HP のトレース機能を使って HPOM をトレースする方法は 2 つあります。

- Windows トレース GUI でのリモートトレースの設定。詳細については HP Operations エージェントのドキュメントを参照してください。
- トレース設定ファイルによるトレースの手動設定。詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

トレースに対応している HPOM アプリケーション

すべての HPOM プロセスは HP のトレース機能を使用します。トレースに対応した HPOM プロセスは 3 つのグループに分けることができます。

- サーバープロセス
- エージェントプロセス
- XPL トレース機能を実装した低レベルコンポーネントにリンクされたプロセス

HPOM でトレース機能を有効にするために必要な、あらかじめ設定されている手順はありません。これを行うには、HPOM のコードベースに XPL トレーシングを追加するか、基礎コンポーネントからコア機能を組み込み、対応するライブラリにリンクさせます。HPOM のコードベースに XPL トレーシングを追加する場合、既存のトレース機能は XPL トレーシングに変換されます。基礎コンポーネントから機能を追加した場合は、これらの基礎コンポーネントに組み込まれている XPL トレーシングが HPOM に取り込まれます。

表 3-3 HPOM 管理サーバーと管理対象ノード上のトレース対応アプリケーション

プラットフォーム	アプリケーション名		
UNIX/Linux	coda	ovas	ovconfget
	codautil	ovbbccb	ovcoreid
	ctrlconfupd	ovc	ovcreg
	logdump	ovcd	ovcs
	opc_getmsg	ovcert	ovdeploy
	opc_ip_addr	ovcm	ovpolicy
	opccrpt	ovconfchg	
	opcnls	ovconfd	

表 3-4 HPOM 管理サーバー上のトレース対応アプリケーション

プラットフォーム	アプリケーション名		
UNIX/Linux	opc	opcdbck	opcsvcm
	opc_dbinit	opcdbinst	opcsw
	opc_dflt_lang	opcdbmsgmv	opcttnsm
	opc_rexec	opcdbpwd	opcuiadm
	opcactm	opcdispm	opcuiopadm
	opcagtdbcfg	opcforwm	opcuiwww
	opcagtutil	opchbp	ovoareqsdr
	opcauddwn	opchistdwn	
	opcbbcdist	opcmsgm	
	opccfgupld	opcmsgrb	
	opccsacm	opcnode	
	opccsad	opcragt	
	ovcd	opcservice	

表 3-5 HPOM 管理対象ノード上のトレース対応アプリケーション

プラットフォーム	アプリケーション名		
UNIX/Linux	opcacta	opcmon	opcmsgi
	opceca	opcmona	opctrapi
	opcecaas	opcmsg	
	opcle	opcmsga	

サーバーアプリケーションとエージェントアプリケーション

ここでは、サーバーアプリケーションとエージェントアプリケーションについて説明します。

HP BTO Software と HPOM に固有のコンポーネント

各アプリケーションには多数のコンポーネントとサブコンポーネントが定義されています。最も重要なコンポーネントは eaagt と opc です。表 3-2 は、サーバー / エージェントプロセス用に定義されているトレーシングコンポーネントを示しています。

表 3-6 HPOM サーバー用コンポーネントとエージェント用コンポーネント

HPOM コンポーネント名	コンポーネントの説明
eaagt	イベントアクションエージェント
opc	管理サーバーの制御

表 3-2 は、製品に組み込まれている共有コンポーネント用に定義されているコンポーネントを示しています。

表 3-7 HP BTO Software の共有コンポーネント

アプリケーションとコンポーネント / サブコンポーネント名	
ブラックボックス通信	
bbc.cb	bbc.http.output
bbc.fx	bbc.http.server
bbc.fx.client	bbc.messenger
bbc.fx.server	bbc.rpc
bbc.http	bbc.rpc.server
bbc.http.client	bbc.soap
bbc.http.dispatcher	

表 3-7 HP BTO Software の共有コンポーネント (続き)

アプリケーションとコンポーネント / サブコンポーネント名	
制御コンポーネント	
ctrl.action	ctrl.ovc
ctrl.autoshutdown	ctrl.process
ctrl.component	ctrl.rpcclient
ctrl.controller	ctrl.rpcserver
ctrl.main	ctrl.soap
ctrl.monitor	ctrl.xml
ctrl.monitorproxy	
設定管理コンポーネント	
conf.cluster	conf.ovconfd
conf.cluster.clioutputs	conf.ovpolicy
conf.config	conf.policy
conf.message	
証明書サーバーアダプタ	
CSA-CertRequestImpl	Csa-Main
CSA-CertReqContainer	csa.ovcmwrap
CSA-Database	Csa-RpcServer
Csa-Log	CSA-UpdateHandler
セキュリティコアコンポーネント	
sec.cm.client	sec.core.base
sec.cm.server	sec.core.ssl
sec.core.auth	

表 3-7 HP BTO Software の共有コンポーネント (続き)

アプリケーションとコンポーネント / サブコンポーネント名	
クロスプラットフォームライブラリ	
xpl.cfgfile	xpl.net
xpl.config	xpl.runtime
xpl.io	xpl.thread
xpl.log	xpl.thread.mutex
xpl.msg	
組み込みパフォーマンスエージェント	
coda	coda.mesa
coda.dataaccess	coda.mesainstances
coda.kmdatamatrix	coda_mesametricrdr
coda.localmesa	coda.mesarea
coda.logger	coda.prospector
配布コンポーネント	depl

HPOM 固有のカテゴリと XPL 標準カテゴリ

HPOM のトレース領域は HP BTO Software カテゴリによって決定します。また、HPOM プロセスと、HPOM が使用する下位レベルの HP BTO Software コンポーネントは多くの標準カテゴリを使用します。

表 3-2 は eaagt および opc コンポーネントで定義されているトレースカテゴリを示しています。

表 3-8 HPOM opc および eaagt のサブコンポーネント

サブコンポーネント名	サブコンポーネントの説明
HPOM に固有のトレースカテゴリ	
actn	アクション
agtid	AgentID を利用した IP への非依存
alive	エージェントのアライブチェック
api	設定 API
apm	クラスタ APM
audit	監査
db	データベース (dblib)
debug	デバッグ
dist	配布
fct	機能 (制御フロー)
init	初期化 (err init、conf init など)
inst	インストール
int	内部
lic	ライセンシング
memerr	メモリ割り当てに関する問題
memory	メモリ割り当てのリセット
misc	その他
mon	モニター
msg	メッセージフロー

表 3-8 HPOM opc および eaagt のサブコンポーネント (続き)

サブコンポーネント名	サブコンポーネントの説明
name	名前解決
nls	各国語サポート (文字セットの変換)
ntprf	NT パフォーマンストレース
pdh	パフォーマンスデータヘルパー
perf	パフォーマンス
pstate	ポリシー / ソースの状態変化
sec	セキュリティ
srvc	サービス
wmi	LE - テンプレート、WMI - テンプレートの変換
一般的な XPL トレースカテゴリ	
Trace	汎用トレース
Proc	プロシージャトレース
Operation	操作トレース
Init	初期化
Cleanup	クリーンアップ操作
Event	イベント
Parms	パラメータ
ResMgmt	リソース管理

ファイアウォールと HTTPS 通信

ファイアウォールは、ネットワーク接続された企業システムを外部の攻撃から保護するために使用されます。これは、通常はインターネットと企業のプライベートイントラネットを分離します。また、機密性の低い環境から信頼性の高い環境へのアクセスを制限するために、複数レベルのファイアウォールを導入することも一般的です。たとえば、研究部門と財務部門を最高のセキュリティレベルの環境に置く一方で、直販部門は外部からアクセスしやすい環境に置く必要があるかもしれません。特定の状況では、イントラネット上のシステムはファイアウォールを通過して、たとえば DMZ (非武装地帯) などに配置されているシステムなど、インターネット上のシステムにアクセスできます。また、インターネット上のシステムもファイアウォールを通過してプライベートイントラネット上のシステムにアクセスできます。いずれの状況でも、その操作を実行できるようにファイアウォールを設定しておく必要があります。HP Operations の HTTPS 通信には、ファイアウォールを通して通信できるようにファイアウォール管理者が HP Operations アプリケーションを設定するための機能が用意されています。

HTTP プロキシを利用した、イントラネットからインターネット上のアプリケーションへの接続

プライベートイントラネット上の HTTPS ベースの HP Operations アプリケーションが、ファイアウォールの外側にあるパブリックインターネット上、または非武装地帯 (DMZ) 上のアプリケーションにアクセスするとします。HP Operations アプリケーションはトランザクションを開始し、インターネット上のサーバーアプリケーションにアクセスするクライアントとして機能します。サーバーアプリケーションは、HTTP サーバーとして機能している別の HP Operations アプリケーションであったり、別の HTTP サーバーアプリケーションであったりする可能性もあります。クライアントの代表的な例としては、インターネット上の Web サーバーに接続を試みる、プライベートイントラネット上の Web ブラウザが挙げられます。ファイアウォールを越えてリクエストを転送し、インターネット上の Web サーバーにアクセスできるように、ブラウザ側で HTTP プロキシを設定する必要があります。ファイアウォール側では、HTTP プロキシがファイアウォールを通過できるように設定します。ファイアウォールは、Web ブラウザが直接ファイアウォールを通過することを許可しません。HP Operations の HTTPS 通信アプリケーションも、HTTP プロキシを使ってファイアウォールを通過できるように設定できます。

HTTP プロキシを利用しない、イントラネットからインターネット上のアプリケーションへの接続

プライベートイントラネット上の HTTPS ベースの HP Operations アプリケーションが、HTTP プロキシを使用せずにファイアウォールの外側のインターネットにアクセスするとします。ファイアウォールは、プライベートイントラネット上の HP Operations アプリケーションがファイアウォールを通過できるように設定する必要があります。これは、HTTP プロキシがファイアウォールを通過できるようにするためのファイアウォールの設定によく似ています。ファイアウォール管理者は、ファイアウォールを挟んだ通信を制限するために、ソースポートとターゲットポートを設定します。HP Operations アプリケーションは、トランザクションを開始するときにソースポートを指定する設定パラメータ `CLIENT_PORT` を送信できます。ターゲット (送信先) ポートは、イントラネット上の HTTP サーバーに接続するための URL (Uniform Resource Locator) アドレス内に定義されます。これはターゲットノード上の Communication Broker ポートです。

インターネット上の HP Operations アプリケーションからプライベートイントラネット上のアプリケーションへのアクセス

インターネット上の HTTPS ベースの HP Operations アプリケーションがプライベートイントラネット上のアプリケーションにアクセスするとします。これは、ファイアウォールの外部からファイアウォールを通過しなければならないことを意味し、ファイアウォール管理者が設定する厳密な条件の下でのみ行われます。トランザクションを開始するクライアントアプリケーションは、HTTP プロキシを使用するか、ファイアウォールを直接通過することができます。HTTP プロキシはファイアウォールの外側に配置され、ファイアウォールは、HTTP プロキシが通過できるように設定しておく必要があります。HTTP プロキシはプライベートイントラネット上のサーバーに直接アクセスするか、カスケード構成された別のプロキシを経由してアクセスします。いずれの場合も、HP Operations の HTTPS 通信クライアントアプリケーションは同じように設定されます。ただし、HTTP プロキシの設定はそれぞれで異なる必要があります。

HTTP プロキシを利用しない、インターネット上の HP Operations アプリケーションからプライベートイントラネット上のアプリケーションへのアクセス

インターネット上の HTTPS ベースの HP Operations アプリケーションがプライベートイントラネット上のアプリケーションにアクセスするとします。ファイアウォール側では、HP Operations クライアントアプリケーションがファイアウォールを通過できるように設定する必要があります。ファイアウォール管理者は、ファイアウォールを挟んだ通信を制限するために、ソースポートとターゲットポートを設定します。HP Operations アプリケーションは、トランザクションを開始するときにソースポートを指定する設定パラメータ `CLIENT_PORT` を送信できます。イントラネット上の HTTP サーバーに接続するためのターゲット (送信先) ポートは URL アドレスに定義されます。これはターゲットノード上の Communication Broker ポートです。ターゲットサーバーが Communication Broker に登録されている場合、ターゲットポートの番号は常に Communication Broker のポート番号になります。これにより、ファイアウォールの設定が簡略化され、管理者がファイアウォールに設定しなければならないターゲットポートの数を大幅に削減できます。HPOM とファイアウォールの設定の詳細については、『*HPOM Firewall Configuration*』を参照してください。

HTTPS ベースの通信の設定

HP アプリケーションのインストールは、設定パラメータを使ってカスタマイズできます。Communication Broker の設定パラメータは、次の場所にある bbc.ini ファイルに含まれます。

<OVDataDir>/conf/confpar/bbc.ini

通信のためのパラメータは *bbc.ini(4)* ファイルに指定されます。このファイルについては HP Operations エージェントのドキュメントを参照してください。

Communication Broker は名前空間 bbc.cb を使用します。すべての管理対象ノードの Communication Broker ポート番号を指定するために、追加の名前空間 bbc.cb.ports が定義されました。これにより、Communication Broker ごとに異なるポート番号を割り当てられるようになりました。この設定は、名前空間 bbc.cb に定義されている SERVER_PORT パラメータの設定に優先して適用されます。

注記

名前空間は、次の例のような一意の URL です。

www.anyco.com または abc.xyz

名前空間は、拡張マークアップ言語ドキュメントで使用される要素と属性に対し、URL 参照によって識別される名前空間を関連付けることで、それらの要素と属性を限定するシンプルな方法です。

名前空間 bbc.cb.ports 内の名前 / 値のペアは、ネットワーク内の Communication Broker のポート番号を定義します。名前 / 値のペアの構文は次のとおりです。

NAME=< **ホスト** >:< **ポート** > または NAME=< **ドメイン** >:< **ポート** >

ホスト / ポート、またはドメイン / ポートの組み合わせは、1 行に複数個を定義できます。区切り文字はカンマまたはセミコロンです。

ドメインの形式は *. **ドメイン名**です。あるドメインのすべてのエントリは、指定されたポートを使用します。エントリは、具体的であるほど優先されます。名前 / 値のペアの名前部分は無視されますが、この名前は該当名前空間内で一意である必要があります。次にエントリの例を示します。

- `HP=jago.sales.hp.com:1383, *.sales.hp.com:1384; *.hp.com:1385`
- `SUN= *.sun.com:1500`

この例では、ホスト `jago.sales.hp.com` で実行される Communication Broker のポート番号は `1383` となります。

ドメイン `sales.hp.com` のその他すべてのホストはポート番号 1384 を使用します。ドメイン `hp.com` のその他すべてのホストはポート番号 1385 を使用します。ドメイン `sun.com` のホストはポート番号 1500 を使用します。その他すべてのホストはデフォルトのポート番号 383 を使用します。

4 メッセージポリシーの導入

概要

本章では、メッセージポリシーを導入し、HP Operations Manager (HPOM) 環境内で配布する方法について説明します。

対象読者

本章は、HPOM *管理者*を対象としています。

本章の内容

本章は HPOM 管理者向けに次の各トピックについて説明します。

- ❏ メッセージの管理
- ❏ メッセージソースポリシーの管理
- ❏ メッセージソースの評価
- ❏ メッセージの収集
- ❏ メッセージの処理
- ❏ 条件によるメッセージのフィルタリング
- ❏ メッセージの最適なフィルタリングのための方針
- ❏ メッセージのロギング
- ❏ ログファイルメッセージ
- ❏ HPOM メッセージインタフェース
- ❏ しきい値モニターからのメッセージ
- ❏ SNMP トラップとイベント
- ❏ HPOM の内部エラーメッセージのフィルタリング
- ❏ HPOM でのイベント相関処理
- ❏ 計画休止
- ❏ サービス時間と計画休止の設定

メッセージの管理

HP Operations Manager (HPOM) では、メッセージソースの一元的な管理ポイントを構築できます。通常、メッセージは管理対象ノードで捕捉されるため、管理サーバーのネットワークトラフィックは削減されます。管理サーバーから特定の管理対象ノードにメッセージソースの情報を配布することで、必要な設定のみを各ノードに指定できます。管理サーバーでメッセージソースの情報に追加 / 変更を一度に加え、その情報を必要とするノードのみに配布します。

アクションの一元化

管理サーバーからすべてのシステムで自動 / オペレータ起動アクションを開始できるので、リモートサイトでのオペレータによる操作が最小化され、場合によっては皆無にすることもできます。

障害の早期検出

オペレータは HPOM を使って環境内のノードの活動状況をモニターすることにより、障害を発生の初期段階で検出し、エンドユーザーに影響を与える前に修復アクションを講じることができます。

生産性の改善

単純な反復作業を HPOM に任せ、オペレータによる複雑なタスクの実行を指示を通じて支援し、さらにオペレータのメッセージブラウザに表示されるメッセージ数を抑制することにより、オペレータの生産性を向上させることもできます。HPOM では、オペレータのスキルと作業範囲のバランスがとれるように、対応するツールセットを設定できます。

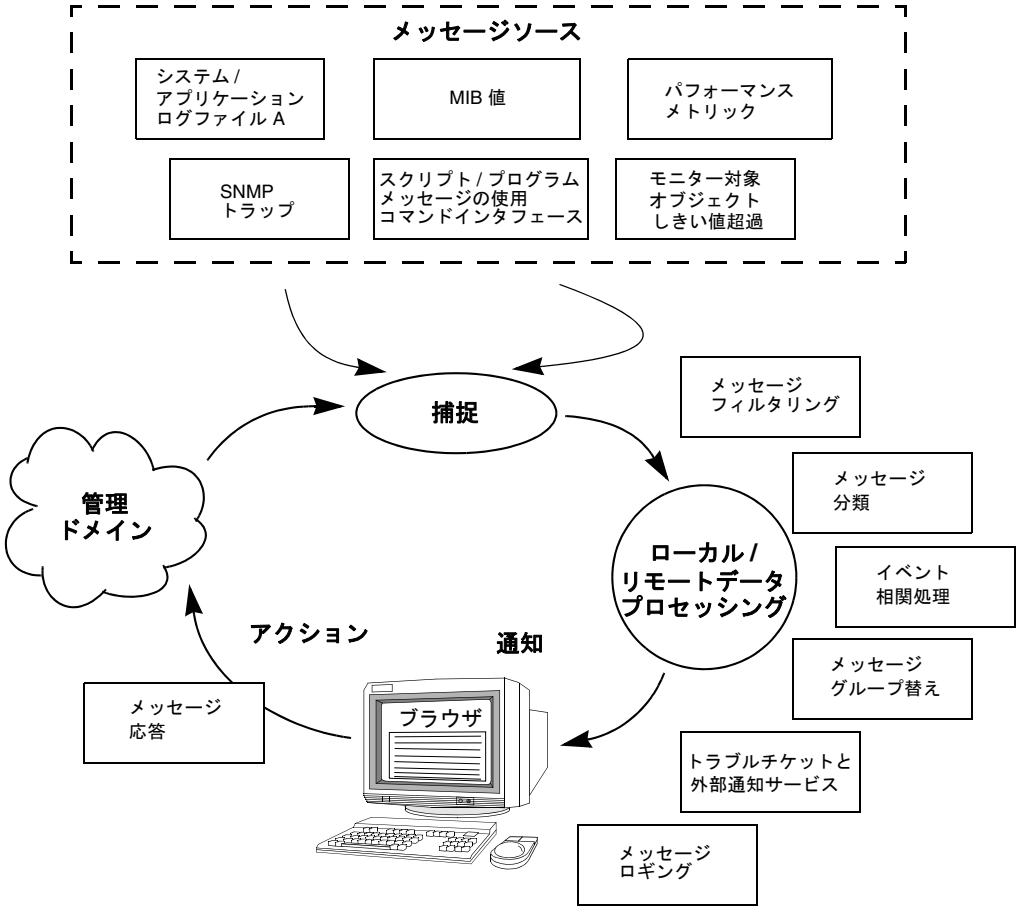
ポリシーの配布

ポリシーを利用することで、環境内のソースから同一種類の情報を収集できます。ポリシーは、情報の収集元となる管理対象ノードに配布されます。

ブラウザでのメッセージの統合

図 4-1 は、HPOM がメッセージを捕捉して処理し、表示するまでの工程を示しています。

図 4-1　　ブラウザでの関連メッセージの統合



メッセージソースポリシーの管理

メッセージの捕捉で中心的な役割を果たすのは、管理サーバーに設定される**メッセージソースポリシー**です。メッセージソースポリシーは、収集 / モニターの対象となるメッセージと値を指定します。また、定期的に実行されるアクション、メッセージを取り込む / 除外するためのフィルター (条件)、捕捉後に適用されるロギングオプションも指定します。

メッセージソースポリシーの要素

メッセージソースポリシーは次の要素から構成されます。

❑ **メッセージソースのタイプ**

メッセージの収集元となるソースを定義し、すべてのメッセージのデフォルト属性を割り当てます。

- ログファイル (Logfile)
- SNMP トラップ (Trap)
- HPOM メッセージインタフェース (opcmsg(1|3))
- しきい値モニター (Monitor)
- イベント相関処理サーキット (EC)
- スケジュールアクション (Schedule)

❑ **メッセージ条件**

属性セットと一致するメッセージのみを HPOM に取り込むためのフィルター。メッセージ条件は、受信したメッセージへの対応も定義します。

❑ **除外条件**

属性セットと完全に一致するメッセージを HPOM への取り込み対象から除外するためのフィルター。

❑ **オプション**

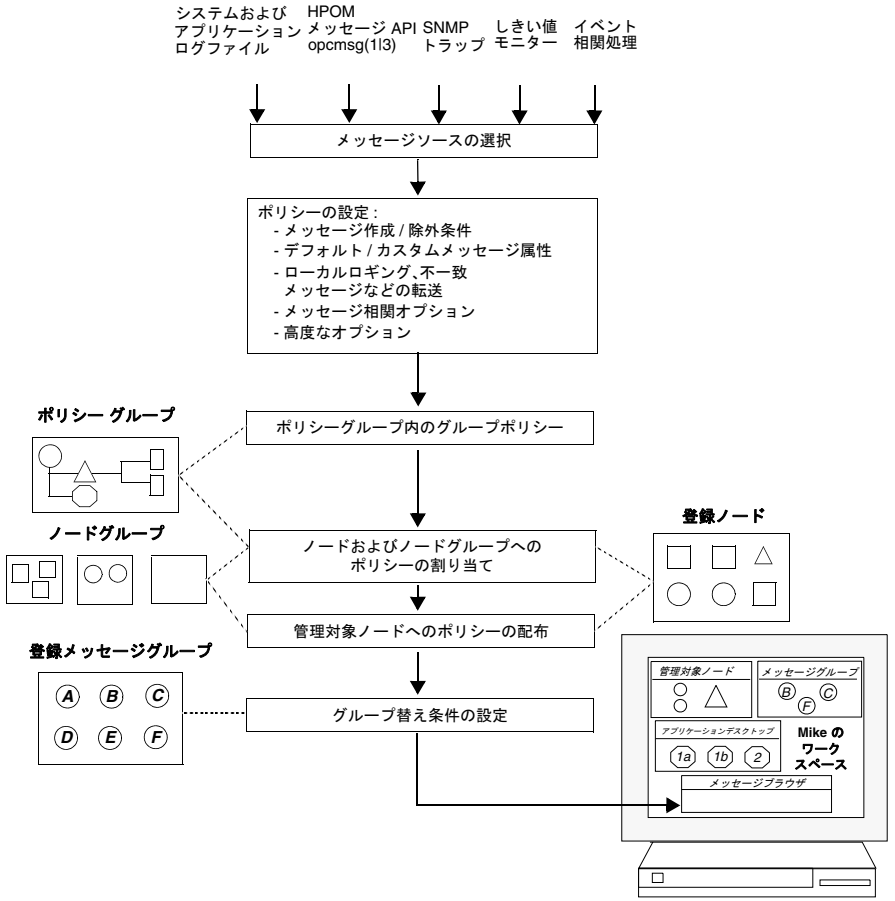
メッセージのデフォルトロギングを指定し、不一致メッセージの転送を設定するオプション。

メッセージソースポリシーの設定

メッセージソースポリシーを使用することで、さまざまな種類のメッセージソースからメッセージを収集し、HPOM に取り込むことができます。ポリシーを設定することで、Java GUI メッセージブラウザにメッセージを転送するかどうか、メッセージをどの属性で表示するか、アクションを実行するかどうかを指定できます。

図 4-2 は、メッセージソースの選択からメッセージソースポリシーのグループ替え条件の設定に至るタスクフローを示しています。

図 4-2　メッセージソースポリシーの設定



メッセージソースポリシー

管理者はポリシーを作成、編集、削除したり、ポリシーグループに割り当てることができます。ポリシーごとに条件が定義され、詳細オプションが指定されます。

メッセージソースポリシーの設定の詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

注意

メッセージソースポリシーに条件を指定せず、ポリシー本文にキーワード FORWARDUNMATCHED が含まれる場合、HPOM はそのメッセージソースからのすべてのメッセージを捕捉します。すべてのメッセージを捕捉した場合、多数の不一致メッセージがメッセージブラウザに転送されることになります。

メッセージソースのポリシーの作成

HPOM では、同じメッセージソースのポリシーを複数作成できます。あらかじめ設定されているポリシーを修正するのではなく、すべてのメッセージソースの独自のポリシーと条件を作成してください。

注意

HPOM を新しいバージョンにアップグレードすると、定義済みポリシーの修正によって作成したポリシーはすべて失われてしまいます。

ポリシーグループの構成

ポリシーグループは、ポリシーまたはその他のポリシーグループの集合です。設定と管理の作業効率を向上させるために、管理者はポリシーをグループ化できます。

たとえば、次の特徴を持つポリシーをグループ化します。

- ❑ メッセージソースが共通
- ❑ 管理対象ノードのプラットフォームが共通

ポリシーグループのメリット

ポリシーをポリシーグループにまとめることには、次のようなメリットがあります。

- **意味を持った概要**

  ポリシーグループを利用することで、ポリシーを論理単位として構成できます。たとえば、スプールサーバーに関連するすべてのポリシーを 1 つのグループにまとめることができます。このグループ化により、ポリシーリストに表示されるポリシーの数が減り、利用できるポリシーの概要を把握しやすくなります。

- **明確な階層**

  ポリシーグループをポリシーグループ階層に配置できます。この階層を利用することでポリシーの構造が改善され、編集時にオペレータが 1 つのポリシータイプに集中しやすくなります。

- **簡単な割り当て**

  管理対象ノードまたはノードグループへのポリシーの割り当てが簡単になります。特定のポリシーグループを特定タイプのノードに割り当てることができます。新しいノードを追加するときは、割り当てるポリシーを個別に集めるのではなく、すべての必要グループを割り当てることができます。これにより、必要なすべてのポリシーが確実に選択されます。

ポリシーグループのリスト表示

ポリシーグループは、`opcpolicy -list_groups` コマンドでリスト表示できます。ポリシーグループの操作には、ポリシーグループの作成 / 削除、グループへのポリシーの割り当て、グループからのポリシーの割り当て解除、すべてのポリシーグループとその内容の表示などがあります。詳細度を上げるか、`level` パラメータに別の値を指定すると、より多くの情報を表示できます。詳細については *opcpolicy (1M)* のマニュアルページを参照してください。

ポリシーグループの作成

ポリシーグループを作成 / 削除したり、グループからポリシーの割り当てを解除したりできます。ポリシーは、複数のグループに割り当てることができます。この複数割り当てケーパビリティにより、組織の詳細なニーズに見合ったポリシーグループを柔軟に作成できます。HPOM では、同じ管理対象ノードに対して同じポリシーが繰り返して配布されることはないため、システムの処理効率も維持されます。

ポリシーグループを作成するときは、グループによってポリシーの割り当てが簡略化されるようにします。たとえば、データベースサーバーをモニターするすべてのポリシーのポリシーグループを作成します。こうすることで、管理対象ノードにポリシーを割り当てるときに、ノードグループ「Database Servers」に対してポリシーグループ「Database Monitoring」を割り当てることができます。サポートされるエージェントプラットフォームごとに HPOM が提供するデフォルトのポリシーグループについては、『*HPOM HTTPS エージェントコンセプトと設定ガイド*』を参照してください。

あるグループに属す別のグループにポリシーを割り当てても、両方のグループに自動的にポリシーが割り当てられるわけではないので注意してください。たとえば、グループ /a にポリシー X を割り当てても、そのポリシーが自動的にグループ /b/a に割り当てられることはありません。

ポリシーのバージョンに関連して、ポリシーグループへのポリシーの割り当てには 3 つの種類があります。

`FIX`

指定された厳密なバージョンのポリシーがグループに割り当てられ、ノードに配布されます。

`LATEST`

配布の時点で存在する最新バージョンのポリシーがノードに配布されます。

`MINOR_TO_LATEST`

割り当てられているバージョンとメジャーバージョンが共通する、配布の時点で存在する最新バージョンのポリシーがノードに配布されます。

メッセージのグループ替え

グループ替え条件を設定することで、メッセージを別のメッセージグループに構成し直すことができます。また、HPOM Event Correlation Services (ECS) がインストールされている環境では、イベント相関処理ポリシーを設定することで、類似したメッセージをより少数の分かりやすいメッセージに絞り込むことができます。

ポリシーの割り当て

ポリシーとポリシーグループを設定したら、新しいポリシーを適用するノードまたはノードグループを決定する必要があります。ノードまたはノードグループへのポリシーの割り当てには、コマンド行ツール opcnode を使います。また、メッセージの捕捉が実行されるノードまたはノードグループにポリシーグループを割り当てることができます。これにより、新しい設定を配布できるようになります。

管理対象ノードへのポリシーの割り当て

ポリシーとポリシーグループは、コマンド行ツール opcnode を使用して管理対象ノードおよびノードグループに割り当てることができます。ノードにポリシーグループを割り当てるプロセスは、単一ポリシーを割り当てるプロセスと同じです。ノードグループ内のすべてのノードは、そのノードグループに割り当てられるポリシーとポリシーグループを継承します。この継承により、新規ノードへのポリシーの割り当てが簡略化されます。たとえば、次のコマンドを使用することで、ポリシーグループをノードグループに割り当てることができます。

opcnode -assign_pol_group pol_group=<*ポリシーグループ名*> group_name=<*ノードグループ名*>

このコマンドの <*ポリシーグループ名*> は割り当てるポリシーグループの名前、<*ノードグループ名*> は割り当て先のノードグループの名前です。

詳細については *opcnode(1M)* のマニュアルページを参照してください。

注記

HPOM では、ポリシーの割り当てと配布は個別に行われます。ポリシーグループ内のいずれか 1 つのポリシーを変更すると、HPOM はそのポリシーのみを再配布します。異なるポリシーグループの割り当てを通じて 1 つのポリシーが同じノードに複数回割り当てられる場合でも、そのポリシーが管理対象ノードに配布され、処理されるのは 1 回だけです。修正中のポリシーはロックされ、配布できません。レポートを生成することで、ポリシーのステータスと管理対象ノードへの割り当てを確認できます。利用可能なレポートの詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

割り当て済みポリシーの配布

新しいメッセージソースポリシーを定義して管理対象ノードに割り当てたら、そのポリシーを管理対象ノードに配布する必要があります。配布方法については 109 ページの「HPOM 設定の更新」を参照してください。

注記

ポリシーを削除する、または特定のノードのポリシー割り当てを解除するときは、影響を受ける管理対象ノードに新しい設定を配布する必要があります。これを行わない場合、変更は有効になりません。

管理対象ノード上のポリシーを一時的に無効にするときは、コマンド行ツール `opcpolicy` を使います。詳細については *opcpolicy(1M)* のマニュアルページを参照してください。

メッセージソースポリシーの配布

メッセージソースポリシーを定義したら、メッセージの捕捉と値のモニタリングの対象となる管理対象ノードにそれを配布します。メッセージソースポリシーの配布には、次のコマンドを使用します。

```
opcragt -distrib -policies
```

詳細については *opcragt(1M)* のマニュアルページを参照してください。

メッセージソースの評価

メッセージポリシーを導入するための最初の手順は、既存のメッセージソースの見直しです。

メッセージを探す場所

評価の対象となるメッセージソースは次のとおりです。

- ❑ アプリケーションおよびシステムログファイル
- ❑ HPOM メッセージ API `opcmsg(3)` を使用するアプリケーション
- ❑ HPOM コマンドインタフェース `opcmsg(1)` を使用するアプリケーション
- ❑ モニター対象オブジェクト
- ❑ パフォーマンスメトリック
- ❑ モニター対象 SNMP MIB 値
- ❑ SNMP トラップを送信するアプリケーション

メッセージの評価方法

メッセージを評価するための条件は次のとおりです。

- ❑ エンドユーザーに対するイベントの影響
- ❑ 重要度レベル
- ❑ 発生頻度
- ❑ 判読性の面でのファイル形式 (つまり、バイナリ形式であるか、テキスト形式であるか)
- ❑ 言語と文字セット
- ❑ ネットワークトラフィックとパフォーマンス

オペレータが注意しなければならないメッセージと、それ以外のメッセージを区別します。多くのメッセージは、システムパフォーマンスやユーザーによる日常作業の実行に影響しないため、重要ではありません。その他のメッセージは、障害が発生する可能性や、その時点で生じている障害を示しています。これらの障害メッセージは、予防的対策を講じない限り、障害が発生する、または再発生することを意味します。

メッセージの重要度の評価

各メッセージの重要度を評価します。多くのメッセージには、情報の一部として重要度レベルが含まれます。これらの重要度レベルが、環境におけるメッセージの実際の重要性を反映しているかどうかを確認してください。オブジェクトから重要度が危険域のメッセージが出力されても、そのメッセージが環境内の危険な状況を表していない可能性もあります。

メッセージカタログから始める

アプリケーションにメッセージカタログが含まれている場合は、生成される可能性があるメッセージを検討する際の手がかりとして利用できます。

メッセージの収集

メッセージは、操作環境内の**オブジェクト**のステータスに関する構造化された情報です。このオブジェクトには、オペレーティングシステムからアプリケーション、周辺デバイスを含め、操作環境で利用されるあらゆるコンポーネントが該当します。

メッセージステータスの作成

メッセージは、イベントまたはステータス変化の結果として作成されます。イベントの重要度と一般的な特徴を指定できます。

メッセージは割り当てられた重要度に応じて、HPOM で捕捉されるか、HPOM から除外されます。捕捉されたメッセージは HPOM で処理され、オペレータの Java GUI ブラウザウィンドウに表示されます。

注記

HPOM は、さまざまなメッセージソースから定期的にメッセージを収集します。この収集間隔はメッセージソースポリシーで指定します。たとえば、ログファイルエンキャプスレータや HPOM モニターエージェントに対するポーリング周期を指定できます。周期を定義するときは、短くしすぎないようにしてください。周期が短すぎると、システムに不要の過負荷が生じる場合があります。HPOM のデフォルトのメッセージソースポリシーで指定されている値をそのまま適用することもできます。

メッセージの捕捉

HPOM は次のソースからのメッセージを捕捉します。

- ❏ **ログファイル**

  アプリケーションおよびシステムログファイル。

- ❏ **HPOM に組み込まれたアプリケーション**

  HPOM に組み込まれたアプリケーションは、アプリケーションプログラミングインタフェース (API) `opcmsg (3)`、またはコマンド行ツール `opcmsg(1)` を通じてメッセージを送信します。`opcmsg(3)` または `opcmsg(1)` を使って独自のメッセージ送信プログラムを作成し、HPOM に組み込むことも可能です。

- ❏ **SNMP トラップ**

  SNMP トラップを送信するアプリケーションとネットワークデバイス。

- ❏ **しきい値モニター**

  - *アプリケーションとシステムの値*

    アプリケーションまたはシステムの値の多くは、想定値と比較できます。

  - *データベース値*

    SQL データベース言語とデータベース管理ツールを利用して特定の値 (テーブルサイズ、ロック数など) をモニターし、これらの値を想定値と比較します。

  - *プロセス*

    デーモンなどの重要プロセスが実行されているかどうかを調べるスクリプトを使用して、実行中のプロセスの数など、プロセスの値をチェックします。

  - *ファイルとファイルシステム*

    重要なファイルまたはファイルシステムの存在とサイズをチェックします。スクリプトは使用ディスク容量 (または空きディスク容量) の値を返すので、あらかじめ定義されている制限値と比較します。

- *パフォーマンスメトリック*

  組み込みパフォーマンスコンポーネントは、オペレーティングシステムからパフォーマンスカウンターとインスタンスデータを収集します。

- *SNMP MIB 値*

  動的な MIB (Management Information Base) パラメータをチェックします。これらのパラメータは、HPOM の内外にあるアプリケーションによって設定 / 更新されます。HPOM は SNMP API を使って現在の値と設定済みのしきい値を比較します。

❑ **スケジュールアクションメッセージ**

ポリシー配布などの定期的な作業は、自動アクションをスケジューリングして実行します。HPOM は、スケジューリングしたアクションが成功したかどうかをメッセージで通知するように設定できます。スケジュールアクションのポリシーの設定については、『*HPOM システム管理リファレンスガイド*』を参照してください。

メッセージの処理

メッセージソース内のメッセージを捕捉するようにポリシーを設定したら、メッセージのフィルターとなる条件を設定する必要があります。HPOM では、HPOM に取り込むメッセージ、または管理サーバーへの転送対象から除外するメッセージをフィルタリングする**条件**を設定できます。

198 ページの図 4-3 は、メッセージがポリシーフィルター、条件フィルター、グループ替え条件を通過してブラウザに到達するまでの過程を示しています。

図 4-3　　メッセージ属性の解決

1. ログファイル内のエントリ

```
SU 12/10 16:21 + ttyp2 peter-root
```

2. 適用されるメッセージソースポリシー

メッセージソースポリシー :	Logfile Su (11.x HP-UX)
メッセージのデフォルト : 属性 :	**重要度 :** normal **ノード :** **アプリケーション :** /usr/bin/su(1) **ユーザーの切り替え** **メッセージグループ : セキュリティ**

3. 条件が適用される前のメッセージ

正常域 ... 12/10/09 16:21:55 system_1.bb /usr/bin/su **セキュリティ**

4. メッセージに適用される該当条件

条件 :	su **の成功**
属性の設定 :	**重要度 : 変更なし** **ノード :** **アプリケーション :** **メッセージグループ :** **オブジェクト :** <from> **メッセージテキスト :** <from> **によるユーザー** <to> **への切り替えに成功しました** **メッセージタイプ :** succeeded_su

5. 管理サーバーに送信されるメッセージ

正常域 ... 12/10/09 16:21:55 system_1.bb /usr/bin/su **セキュリティ** peter **によるユーザー** root **への切り替えに成功しました**

6. 管理サーバーでのグループ替え (オプション)

7. メッセージブラウザに表示されるメッセージ

正常域 ... 12/10/09 16:21:55 system_1.bb /usr/bin/su **セキュリティ** peter **によるユーザー** root **への切り替えに成功しました**

ポリシーによるメッセージ処理の仕組み

メッセージソースポリシーを使用することで、メッセージ属性、メッセージ相関オプション、パターンマッチオプション、メッセージ出力オプションのデフォルト値をグローバルに設定できます。

メッセージのデフォルト値の設定

メッセージソースポリシーは、メッセージに次のデフォルト設定を割り当てます。

- **メッセージ属性**

  メッセージ属性はメッセージの特徴を表す情報であり、HPOM 管理者はこの情報に基づいて管理サーバーで受信したメッセージを分類できます。メッセージ属性には、メッセージの重要度、メッセージが生成されたノード、イベントに関連するアプリケーション / オブジェクト、メッセージのメッセージグループなどがあります。メッセージソースポリシーには、これらの属性のデフォルト値を設定できます。ただし、これらの値はメッセージ条件に設定されている値で上書きされます。HPOM はメッセージ属性を Java GUI ブラウザに表示します。

- **カスタムメッセージ属性**

  カスタムメッセージ属性は HPOM メッセージを拡張する追加情報であり、顧客名、サービスレベル契約の種類、デバイスの種類などがあります。

  HPOM はカスタムメッセージ属性を Java GUI ブラウザに表示します。オペレータは、表示されたカスタム属性に基づいて、メッセージのソートやフィルタリングを実行できます。

  メッセージにカスタムメッセージ属性を割り当てるには、コマンド行ツール `opccmachg` を使用します。詳しい使用方法については *opccmachg(1m)* のマニュアルページを参照してください。

  カスタムメッセージ属性を設定できるのは、ログファイル、HPOM インタフェース、しきい値モニターポリシー、SNMP トラップインターセプタ (`trapi`)、スケジューリングされたタスクのメッセージ条件のみです。カスタムメッセージ属性の詳細については、『*HPOM HTTPS エージェントコンセプトと設定ガイド*』を参照してください。

❑ メッセージ相関オプション

メッセージにメッセージキーを割り当て、そのメッセージキーで自動受諾するメッセージ (状態ベースのブラウザの場合) を選択し、HPOM が重複メッセージを除外する方法を指定できます。メッセージキーを割り当てることで、Java GUI メッセージブラウザに同じメッセージがあふれることを防止できます。メッセージキーと一致するメッセージを除外するには、キーワード SUPP_DUPL_IDENT を使用します。

重複メッセージを除外するには、次の方法があります。

- HPOM が重複メッセージを除外する時間の長さを指定する。指定した時間が経過すると、重複メッセージは再送信されます。
- 重複メッセージカウンターのしきい値を指定する。カウンターがしきい値を超えると、重複メッセージの送信が許可されます。

詳細については 369 ページの付録 A「ポリシー本文の構文」を参照してください。

❑ パターンマッチオプション

メッセージをスキャンするときに、ポリシーで使用されるフィールドセパレータと、大文字 / 小文字が区別されるチェックを指定できます。大文字 / 小文字が区別されるチェックを定義するときはキーワード ICASE、フィールドセパレータを定義するときは SEPARATORS を使用します。詳細については 369 ページの付録 A「ポリシー本文の構文」を参照してください。

❑ メッセージストリームインタフェースの出力オプション

HPOM から外部のメッセージストリームインタフェースにメッセージを出力するかどうかを選択し、出力する場合は、HPOM がメッセージを転送する方法を選択できます。

デフォルト値の定義には次のキーワードを使用します。

MPI_SV_COPY_MSG	MSI とサーバープロセスの両方にメッセージを送信します。
MPI_SV_DIVERT_MSG	メッセージを MSI に方向転換しますが、サーバープロセスには送信しません。
MPI_SV_NO_OUTPUT	MSI にメッセージを送信しません (デフォルト)。

これらのデフォルト属性はポリシーのレベルでグローバルに適用されますが、メッセージ条件によってオーバーライドされる場合があります。ポリシー本文の構文については 369 ページの付録 A「ポリシー本文の構文」を参照してください。

複数ポリシーの設定

HPOM では、管理者は各メッセージソースに対して、メッセージ条件と除外条件が異なる複数のポリシーを設定できます。イベントが発生すると、その管理対象ノードに割り当てられているすべてのポリシーが並行して適用され、イベントがフィルタリングされます。条件に該当する場合、メッセージはそのポリシーに指定されているオプションに基づいて直ちに処理されます。したがって、HPOM がメッセージをフィルタリングする方法を理解しておけば、ブラウザが不要なメッセージであふれたり、重要なメッセージを失うことを回避できます。

複数ポリシーの同時処理

HPOM は、1 つのノードに割り当てられている同じ種類の複数のポリシーを並行処理できます。この処理では、どのポリシーにも優先順位は割り当てられず、各ポリシーは独立したエンティティとして扱われます。あるポリシーの**除外 / 非該当除外**条件と一致するメッセージは、そのポリシーの処理のみで除外されます。ただし、メッセージが別のポリシーのメッセージ条件と一致し、担当オペレータへの HPOM メッセージが作成される可能性はあります。複数ポリシーの設定でパフォーマンスを向上させる方法については 228 ページの「パフォーマンスの最適化」を参照してください。

203 ページの図 4-4 は、複数のポリシーによるメッセージの並行処理を示しています。

- ❏ **メッセージのフィルタリング**

  イベントによって生成されたメッセージが HPOM で捕捉され、メッセージソースポリシーによってフィルタリングされます。

- ❏ **デフォルト設定の割り当て**

  ポリシーは、メッセージにデフォルト設定を割り当てます。

- ❏ **メッセージ条件のチェック**

  メッセージは、条件リストに照らしてチェックされます。それ以後の処理は、最初に一致する条件によって決定します。

- **メッセージの転送**

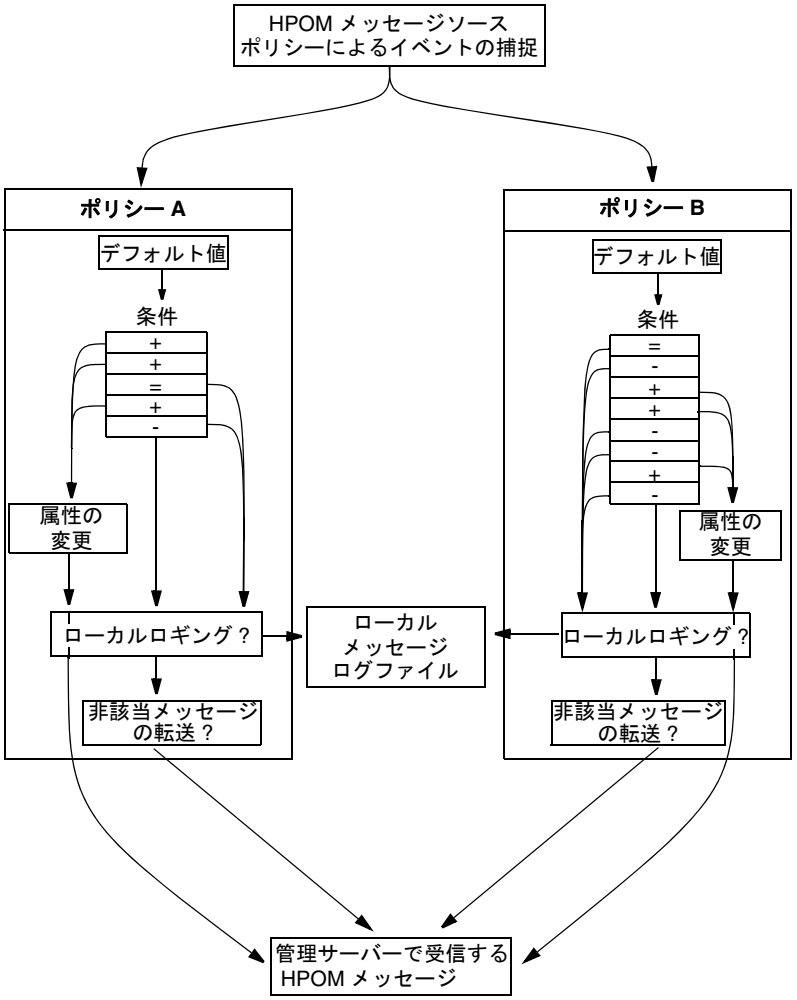
  メッセージがどの条件とも一致せず、ポリシーに非該当メッセージの転送属性が設定されている場合、そのメッセージ (ポリシーのデフォルト値を含む) は転送されます。

- **メッセージのロギング**

  不一致メッセージについて、ローカルログに出力するか、あるいはログのみを実行するように設定している場合、HPOM はその設定に従ってメッセージをログに記録します。

各ポリシーの設定が異なる場合、1 つのイベントから複数の HPOM メッセージが生成され、それぞれ独自の方法で問題に対処することがあります。

図 4-4　　複数ポリシーによるメッセージのフィルタリング



非該当メッセージの転送

複数のポリシーでキーワード FORWARDUNMATCHED を使用した場合、1 つのイベントから複数のメッセージを受信する可能性があります。キーワード FORWARDUNMATCHED が設定された各ポリシーは、ポリシーのデフォルト値を持つメッセージを作成します。

アプリケーションに固有のポリシーと汎用ポリシーでは、複数メッセージの処理方法が異なります。

- **アプリケーションに固有のポリシー**

  キーワード SUPP_UNM_CONDITIONS を使用して、関連するメッセージのみを受信します。

- **汎用ポリシー**

  キーワード FORWARDUNMATCHED を使用して、関連メッセージ以外に不一致メッセージも受信します。

1 つのイベントから複数のメッセージを生成*しない*のは、次のタイプのポリシーのみです。

- ログファイルポリシー
- SNMP トラップポリシー
- HPOM インタフェースメッセージポリシー

これらのポリシーは、不一致メッセージを管理サーバーに転送する前に、割り当てられている*すべて*のポリシーを処理します。メッセージが除外条件と一致し、非該当メッセージの転送属性が別のポリシーに設定されている場合、メッセージは除外されます。非該当除外条件によってメッセージが除外されるのは、そのポリシーにおいてのみであり、別のポリシーと一致しなかったメッセージは管理サーバーに転送されます。

独自のアプリケーション固有ポリシーの設定

あらかじめ設定されている HPOM ポリシーおよび条件を変更するときは、それぞれを別のバージョンで保存してください。

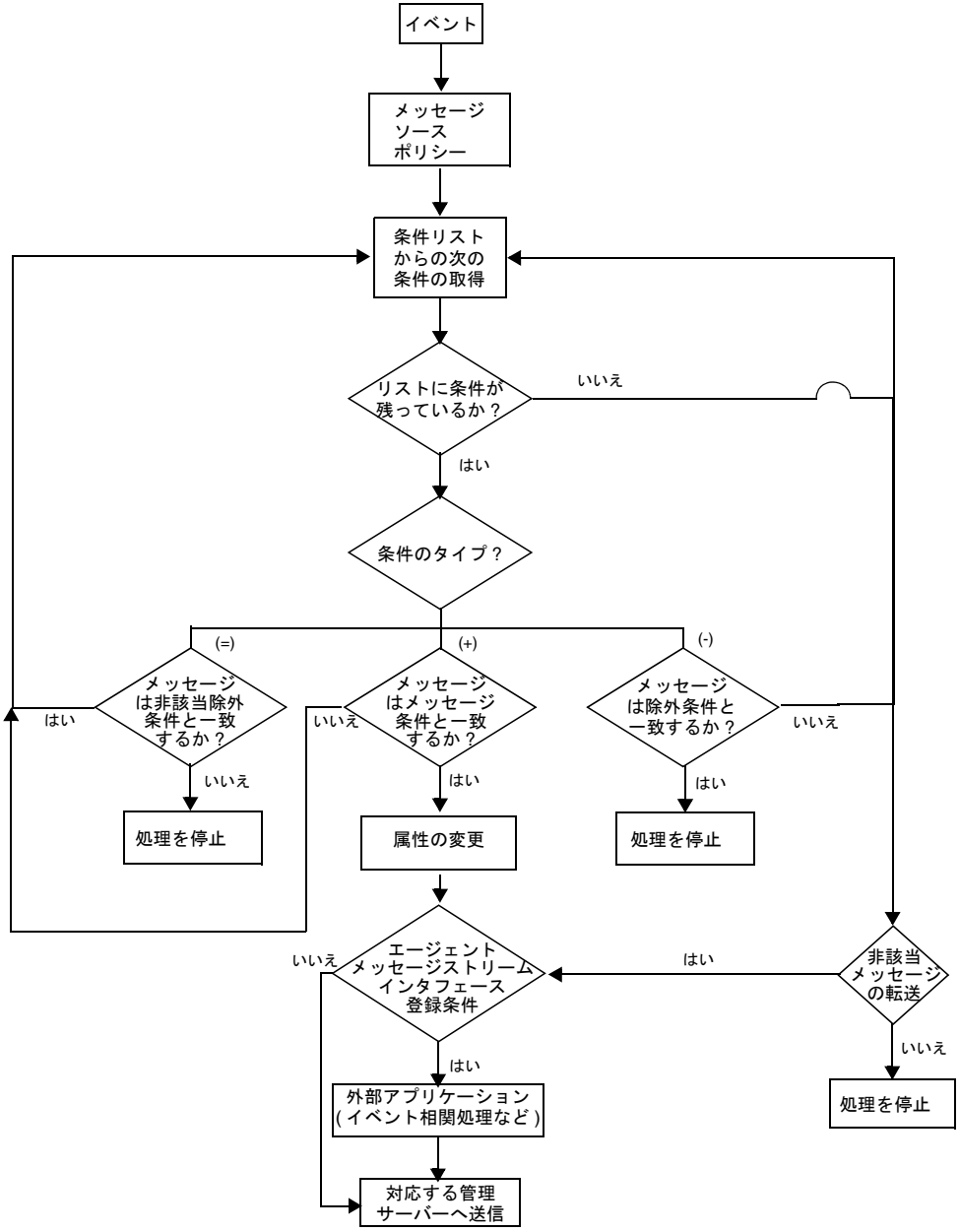
条件によるメッセージのフィルタリング

メッセージ処理のメカニズムは、HPOM の基盤ともいうべき部分です。メッセージソースからオペレータに送られるメッセージは、**条件**によって制御されます。条件はデータ量の絞り込みと、さまざまなメッセージソースで生成されたメッセージのフォーマットの共通化に役立ちます。

メッセージソースのフィルタリング

図 4-5 は、エージェント上でメッセージが条件に照らして処理される過程と、条件と一致する / 一致しないメッセージの処理方法を示しています。この一連の過程は、「メッセージソースのフィルタリング」と呼ばれます。

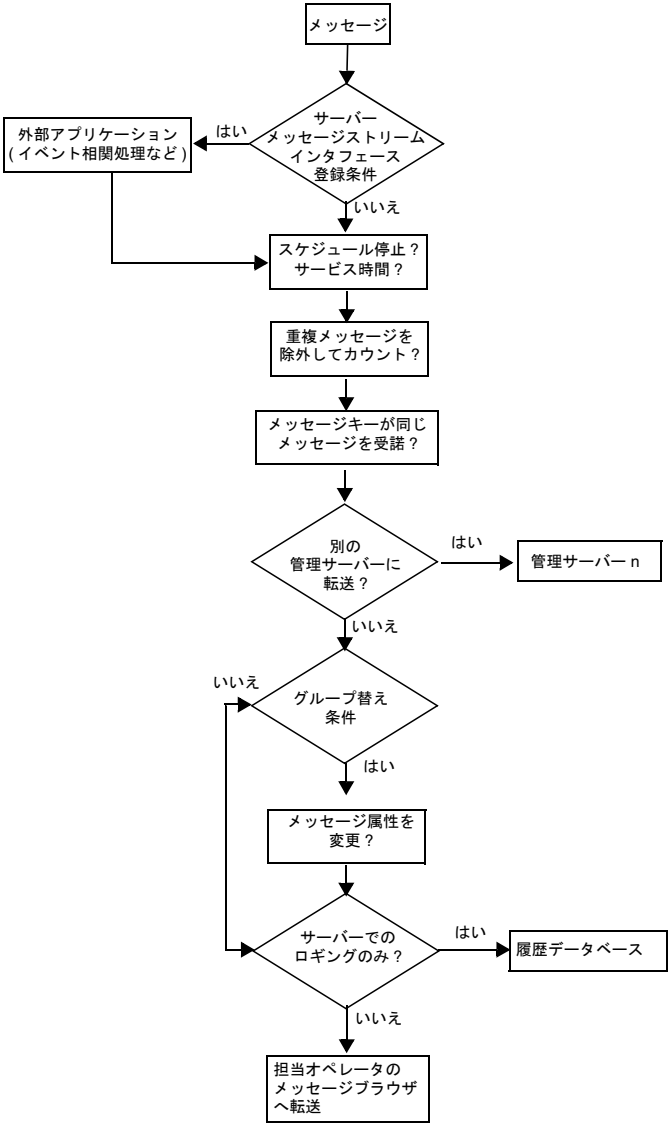
図 4-5　　エージェント上でメッセージが HPOM のフィルターを通過するフロー



管理サーバーでのメッセージの処理

図 4-6 は、メッセージが担当オペレータのブラウザに到着する前に、管理サーバー上で処理される過程を示しています。

図 4-6　サーバー上でメッセージが HPOM のフィルターを通過するフロー



メッセージ条件を設定するには

メッセージ条件を設定するときは、369 ページの付録 A「ポリシー本文の構文」で説明するポリシー本文の構文に従ってください。

メッセージ条件を設定する手順は次のとおりです。

1. **該当条件の定義**

   メッセージ条件または除外条件と呼ばれるマッチングパターンを定義します。

2. **パターンマッチのテスト**

   1 つの条件のパターンマッチが想定どおりに機能することをテストで確認します。

3. **メッセージ相関オプションの設定**

   頻繁に繰り返されるメッセージで Java GUI メッセージブラウザがあふれることがないように、特定のメッセージキーを持つメッセージを自動的に受諾するためのメッセージ相関オプションを設定します。

4. **オペレータ起動アクションの設定**

   選択したメッセージが条件と一致するたびに、管理者によって設定されたスクリプトやプログラムを特定のオペレータが実行できるようにオペレータ起動アクションを設定します。

5. **自動アクションの設定**

   メッセージが条件と一致するたびに HPOM によってスクリプトやプログラムが自動的に実行されるように自動アクションを設定します。

6. **メッセージの設定**

   外部の通知サービスまたはトラブルチケットサービスに出力されるメッセージを設定します。

7. **メッセージ属性の定義**

   Java GUI メッセージブラウザに表示するメッセージの属性を定義します。これらの属性は、メッセージソースから送られた元の一致テキストの属性と同じである必要はありません。

8. **カスタムメッセージ属性の定義**

   メッセージに関するより多くの情報をオペレータに提供するために、Java GUI メッセージブラウザに表示するメッセージの独自のメッセージ属性を定義します。

9. **指示の記述**

   メッセージに添付され、Java GUI メッセージブラウザに表示される指示を記述します。

メッセージ条件の設定については 369 ページの付録 A「ポリシー本文の構文」と『*HPOM システム管理リファレンスガイド*』を参照してください。

メッセージソースに対してフィルターを設定しない場合、不一致メッセージを管理サーバーへ転送するように指定していると、そのメッセージソースで生成されたメッセージはすべて HPOM に渡されて処理されます。

メッセージ条件と除外条件

条件は、イベントと照合できるさまざまな属性 (ノード名、アプリケーション名、メッセージキー、テキスト、オブジェクトパターンなど) から構成されます。HPOM では、受信メッセージは、ポリシー本文に表示されている順にメッセージ条件および除外条件と比較されます。

1 つのメッセージソースポリシーからのメッセージをフィルタリングして HPOM に取り込む、または除外する場合でも、メッセージ条件、除外条件、および非該当除外条件を必要に応じていくつでも設定できます。

イベントに適用できる条件

管理対象ノード上のイベントに適用できる条件は次のとおりです。

❑ **メッセージ該当条件**

メッセージ条件として設定された *すべての* 属性と一致するメッセージを HPOM に取り込んで処理します。

メッセージ条件では、**メッセージ属性**を設定し、メッセージを管理対象ノードから HP Operations 管理サーバー上のメッセージグループに転送して、そこで特定のオペレータに割り当てることができます。

- **該当除外条件**

  除外条件の *すべての* 属性と一致するメッセージを HPOM から除外します。メッセージはそれ以上処理されません。

  除外条件を適用することで、HPOM で処理するメッセージと、Java GUI メッセージブラウザに表示されるメッセージの数を削減できます。

- **非該当除外条件**

  非該当除外条件の属性と *一致しない* メッセージを HPOM から除外します。メッセージはそれ以上処理されません。

  メッセージが非該当除外条件の *すべての* 属性と一致する場合、メッセージは条件リスト内のそれ以後の条件によってさらに処理されます。

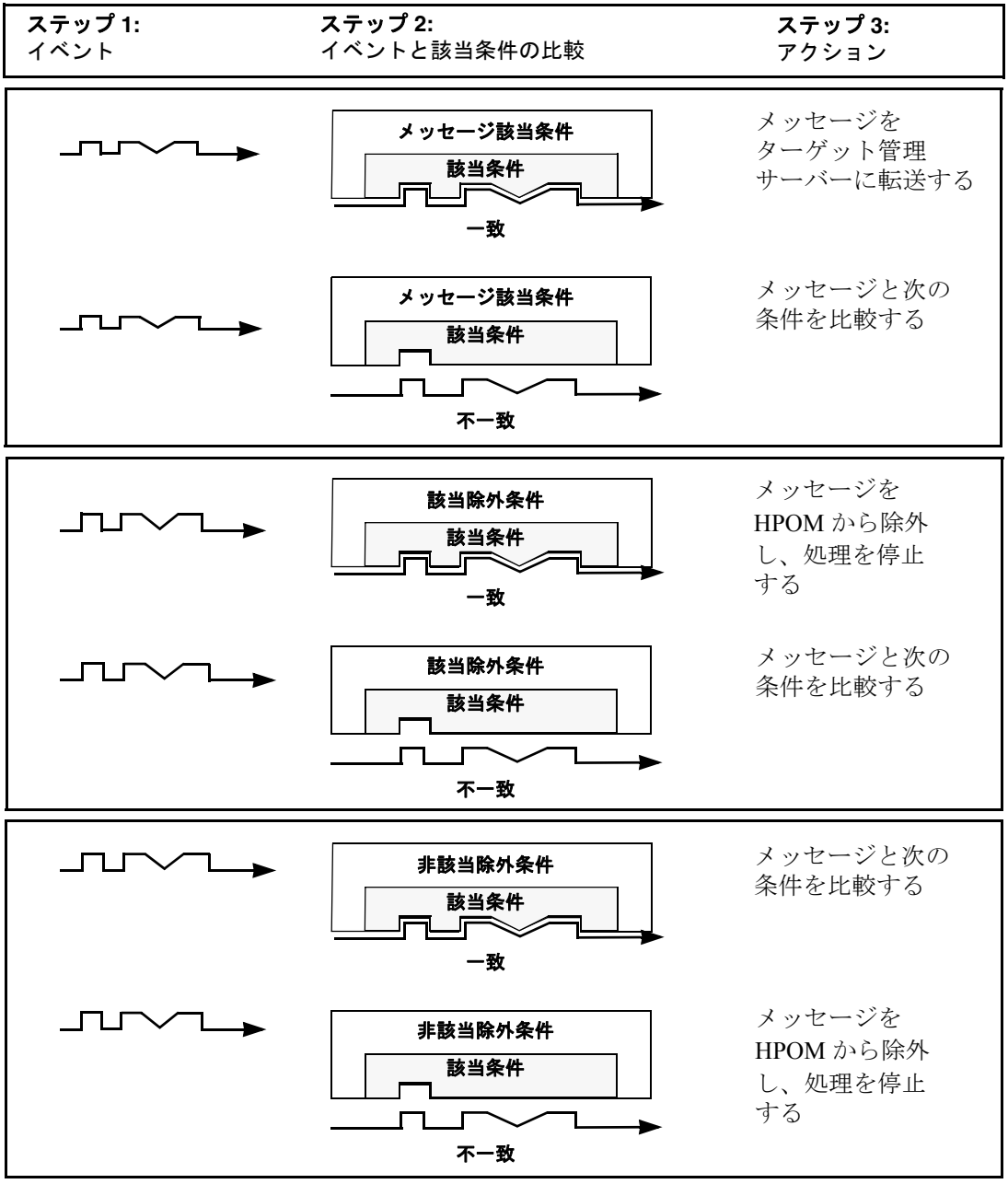
  非該当除外条件を適用することで、ポリシーに無関係なすべてのメッセージを条件レベルで除外し、ポリシーの条件リストによって処理されるメッセージの数を削減することで HPOM のパフォーマンスを向上できます。

  ポリシー本文にキーワード `FORWARDUNMATCHED` が指定されている場合、サーバーに転送される非該当メッセージはポリシーに直接関連するメッセージに限定されます。

着信メッセージと該当条件の比較

211 ページの図 4-7 は、着信メッセージが、指定した該当条件、除外条件、および非該当除外条件とどのように比較されるかを示しています。メッセージ条件の設定方法については 205 ページの「条件によるメッセージのフィルタリング」を参照してください。

図 4-7　　条件によるメッセージのフィルタリング



注記

どちらも非該当メッセージに関連しますが、キーワード SUPP_UNM_CONDITIONS はメッセージを条件レベルでフィルタリングし、キーワード FORWARDUNMATCHED はメッセージをポリシーレベルでフィルタリングします。

メッセージのパターンマッチ

HPOM は、最小限の条件入力で利用できる強力なパターンマッチ言語を備えています。メッセージの動的な部分を選択的に抽出し、変数に割り当ててパラメータとして使用することで、新しいメッセージテキストを作成したり、別の属性を設定することができます。これらのパラメータは、自動 / オペレータ起動アクションコマンドで使用することもできます。HPOM および SNMP 変数の完全なリストについては、『*HPOM システム管理リファレンスガイド*』を参照してください。

演算子を含むパターンマッチ

ほとんどの場合、パターンマッチではメッセージ内の特定文字列のスキャンのみが行われます。ただし、多数の演算子を利用することで、検索精度を向上できます。たとえば、ポリシー本文の MSGCONDITIONS ブロックでキーワード TEXT に ERROR と入力した場合、いずれかの場所に「ERROR」という文字列が含まれるメッセージのみと一致します。

同様に、特定の文字列、たとえば「WARNING」を含まないメッセージを検索する場合は、次のように入力します。

```
<![WARNING]>
```

この例では、**NOT 演算子 (!)** を使用しています。すべての演算子は開きと閉じの不等号で囲む必要があり、サブパターンの部分は角括弧で囲む必要があります。

除外条件と一致するメッセージは HPOM から除外されるため、メッセージのフォーマットを変更したり、一致メッセージ用のアクションを指定する必要はありません。HPOM でのメッセージフローについては 206 ページの図 4-5 を参照してください。

大文字 / 小文字を区別しないパターンマッチ

ポリシー本文にキーワード ICASE を指定すると、大文字と小文字をどのように組み合わせた「warning」とも一致させることができます。ポリシー本文の構文については 369 ページの付録 A「ポリシー本文の構文」を参照してください。

パターンマッチ条件の例

次に、HPOM のパターンマッチ言語で表現できる各種条件の例をいくつか示します。

- `Error`

  メッセージ内の任意の場所に Error というキーワードを持つすべてのメッセージを認識します。デフォルトでは、この条件の大文字 / 小文字は区別されます。

- `panic`

  大文字 / 小文字を区別するモードがオフの場合、この条件はメッセージテキスト内の任意の場所に panic、Panic、または PANIC というキーワードを持つすべてのメッセージと一致します。

- `logon|logoff`

  OR 演算子 (|) を使用した場合、キーワード logon または logoff を持つすべてのメッセージを認識します。

- `^getty:<*.msg> errno<*><#.errnum>$`

  次のようなメッセージと一致します。

  ```
  getty: cannot open ttyxx errno : 6

  getty: can't open ttyop3; errno 16
  ```

  最初の例では、文字列 cannot open ttyxx は変数 **msg** に割り当てられます。変数 **errnum** には 6 という値が割り当てられます。最後の記号 ($) は、6 という値が行末にある場合にのみ一致として扱うことを指定しています。

- `^errno[ |=]<#.errnum> <*.errtext>`

  次のようなメッセージと一致します。

  `errno 6 - no such device or address`

  `errno=12 not enough core.`

  OR 演算子の前の空白文字が重要です。角括弧内の表現は、空白文字または等号 (=) と一致します。<#.**errnum**> と <*.**errtext**> の間の空白文字は区切り文字として使用されています。ここに示される変数への割り当ては厳密には必須ではありませんが、この空白文字はパフォーマンスの向上に役立ちます。

- `^hugo:<*>:<*.uid>:`

  ユーザー hugo のすべての /etc/passwd エントリと一致し、変数 **uid** にユーザー ID を返します。パターンの中央にあるコロン (:) は、**uid** に渡される文字列と先行する文字列を区切るために使用されています。パターンの最後のコロンは、**uid** に渡される文字列と、入力パターン内の後続のグループ ID を区切るために使用されています。コロンは、パフォーマンスの向上だけでなく、文字列の論理的な区切りとしても必要です。

- `^Warning:<*.text>on node<@.node>$`

  「`Warning: too many users on node hpbbx`」などのメッセージを識別し、変数 **text** に `too many users` を割り当て、変数 **node** に hpbbx を割り当てます。

パターンマッチ表現の詳細

ここでは、HPOM のパターンマッチ言語で使用できる表現の詳細を示します。

- **標準文字**

  通常の文字は、それ自体を表す表現です。サポートされる文字セットの任意の文字を使用できます。ただし、次に示す特殊文字を使う場合は、特殊文字の通常の機能をマスクするために、直前に円記号 (¥) を付ける必要があります。

  `[ ] < > | ^ $`

脱字符号 (^) とドル記号 ($) は、位置指定記号として使用しない場合 (先頭または末尾の文字でない場合) は、通常の文字として解釈されるため、マスクする必要はありません。

- **位置指定記号 (^ と $)**

  脱字符号 (^) をパターンの先頭文字として使用する場合は、行の先頭にある表現のみと一致します。たとえば、^ab は、行 abcde 内の文字列 ab とは一致しますが、行 xabcde 内の文字列 ab とは一致しません。

  ドル記号 ($) をパターンの最後の文字として使用する場合は、行の最後にある表現のみと一致します。たとえば、de$ は、行 abcde 内の文字列 de とは一致しますが、行 abcdex 内の文字列 de とは一致しません。

- **複数の文字と一致する表現**

  任意の文字数の文字列と一致させるパターンには、次の表現のいずれか、またはその組み合わせが必要です。

<*>	0 個以上の任意の文字 (セパレータを含む) と一致します。
<n*>	*n* 個の任意の文字 (セパレータ文字を含む) と一致します。
<#>	1 個以上の連続する数字と一致します。
<n#>	*n* 個の連続する数字と一致します。
<_>	1 個以上の連続するセパレータと一致します。
<n_>	*n* 個の連続するセパレータと一致します。
<@>	セパレータを含まない任意の文字列と一致します。つまり、1 個以上の連続するセパレータ以外の文字と一致します。このパターンは、単語との一致に使用されます。

  セパレータ文字は、条件ごとに設定できます。デフォルトのセパレータは、空白文字とタブ文字です。

- **角括弧表現**

  角括弧 ([ ]) は、表現をグループ化するための区切り文字として使用されます。パフォーマンスを向上させるため、必要以上に角括弧を使用することは避けてください。

次のパターンでは、すべての角括弧は不要であり、文字列 abcdefgh に置き換えることができます。

```
ab[cd[ef]gh]
```

括弧で囲まれた表現は、**OR 演算子**や **NOT 演算子**と組み合わせて使用されることが多く、**サブパターン**を使って変数に文字列を割り当てる際にも使用されます。

- **OR (|) 演算子**

  特殊文字である垂直バー (|) で区切られた 2 つの表現は、いずれかの表現と一致する文字列と一致します。

  たとえば、次のパターンは文字列 abd、および文字列 cd と一致します。

  ```
  [ab|c]d
  ```

- **NOT (!) 演算子**

  NOT **演算子** (!) は、区切りの角括弧と組み合わせて使用する必要があります。

  たとえば、次のパターンは「WARNING」という文字列を含まないすべてのテキストと一致します。

  ```
  <![WARNING]>
  ```

  NOT 演算子は、複雑なサブパターンと組み合わせて使用することもできます。

  ```
  SU <*> + <@.tty> <![root|[user[1|2]]].from>-<*.to>
  ```

  このパターンは、user1、user2、または root 以外のユーザー向けのユーザー切り替えメッセージを生成できます。

  したがって、次の文字列とは一致します。

  ```
  SU 03/25 08:14 + ttyp2 user11-root
  ```

  しかし、次の行には user2 のエントリが含まれるため、一致しません。

  ```
  SU 09/25 08:14 + ttyp2 user2-root
  ```

NOT 演算子を含むサブパターンとの一致がない場合、**NOT 演算子**は <*> のように機能し、0 個以上の任意の文字と一致します。このため、UNIX システムの表現 `[!123]` と、対応する HPOM のパターンマッチ表現 `<![1|2|3]>` では機能が異なります。HPOM の表現は、1、2、3 を除く任意の 1 文字または任意の数の文字と一致します。UNIX システムの演算子は、1、2、3 を除く任意の *1* ***文字***と一致します。

- **マスク (\) 演算子**

  次の文字の特殊機能をマスクするには、円記号 (¥) を使用します。

  `[ ] < > | ^ $`

  表現の中で、直前に円記号が付けられた特殊文字は、その文字自体と一致します。

  脱字符号 (^) とドル記号 ($) は、パターンの先頭 / 末尾に置かれた場合にのみ特別な意味を持つため、パターンの内部 (先頭 / 末尾以外) で使用する場合は、マスクする必要はありません。

  この規則の唯一の例外はタブ文字です。パターン文字列では、タブ文字は `\t` と入力されます。

  OR 演算子 (|) は、該当条件の次のフィールドで使用できます。

  - ノード
  - アプリケーション
  - メッセージグループ
  - オブジェクト

数値範囲演算子

これらの演算子を使って複雑な表現を作成する際の基本パターンは次のとおりです。

< 数字 -- 演算子 --[サブパターン]-- 演算子 -- 数字 >

サブパターンには、<#> や <2#> などのシンプルな算術演算子を使用できます。このようなシンプルな演算子には、区切りの括弧は必要ありません。反対に、区切りの括弧を使った複雑なサブパターンも使用できます。

```
<120 -gt [<#>1] -gt 20>
```

1 つの演算子のみを使ってパターンを作成することもできます。

```
Error <<#> -eq 1004>
```

6 つの数値範囲演算子

-le	以下
-lt	小なり
-ge	以上
-gt	大なり
-eq	等値
-ne	不等

以下 (-le) 演算子

使用例 :

```
<<#> -le 45>
```

このパターンは、45 以下の数字を含むすべてのメッセージと一致します。たとえば、次のメッセージとは一致します。

```
ATTENTION: Error 40 has occurred
```

パターン内の 45 という数は、数値であって文字列ではありません。たとえば、4545 は 45 の組み合わせではありますが、45 より大きいので一致しません。

小なり (-lt) 演算子

使用例 :

```
 <15 -lt <2#> -le 87>
```

このパターンは、数字の最初の 2 桁が 16 ～ 87 の範囲に含まれるすべてのメッセージと一致します。たとえば、メッセージ

`Error Message 3299` とは一致します。
文字列 `Error Message 9932` とは一致しません。

以上 (-ge) 演算子

使用例 :

```
^ERROR_<57 -ge <#.err>>
```

このパターンは、直後に 57 以下の数字が続く ERROR_ という文字列から始まるすべてのテキストと一致します。たとえば、次のメッセージとは一致します。

```
ERROR_34: processing stopped
```

変数 err には文字列 34 が割り当てられます。

位置指定記号として脱字符号 (^) が使用されていることに注意してください。

大なり (-gt) 演算子

使用例 :

```
<120 -gt [<#>1] -gt 20>
```

21 ～ 119 の中で最後の桁が 1 のすべての数字と一致します。たとえば、21、31、41、... 101、111 が含まれるメッセージと一致します。

例 2:

```
Temperature <*> <@.plant>: <<#> -gt 100> F$
```

このパターンは、「Actual Temperature in Building A: 128 F」のような文字列と一致します。変数 plant には、文字 A が割り当てられます。位置指定記号としてドル記号 ($) が使用されていることに注意してください。「大なり」演算子は、オープンインターバルとも呼ばれます。「以上」演算子を使用した場合は、クローズインターバルとなります。

等値 (-eq) 演算子

使用例 :

```
Error <<#> -eq 1004>
```

このパターンは、文字列 Error と、その直後に 1004 という数字が含まれるすべてのメッセージと一致します。たとえば、次のメッセージはこのパターンと一致します。

```
Warning: Error 1004 has occurred
```

ただし、Error 10041 はこのパターンとは一致しません。

不等 (-ne) 演算子

使用例 :

```
WARNING <<#> -ne 107>
```

このパターンは、文字列 WARNING と、その直後に空白文字と 107 以外の 1 個以上の任意の数字が含まれるすべてのメッセージと一致します。たとえば、次のメッセージとは一致します。

```
Application Enterprise (94/12/45 14:03): WARNING 3877
```

パターンマッチ表現に表現記号を挿入するには

パターンマッチを操作するときは、マウスの左右のボタンを使って表現記号を挿入できます。

表現記号を挿入する手順は次のとおりです。

1. 表現に置き換えるテキストを選択します。
2. 選択したテキストを右クリックし、挿入できる記号のリストを表示します。
3. リストから記号を選択します。

この方法で変数名を指定することは *できません*。変数名は表現に個別に入力する必要があります。

パターンマッチ表現の変数とパラメータ

一致した文字列は変数に割り当てることができます。この変数を使ってメッセージを再作成したり、アクション呼び出しのパラメータとして使用することができます。パラメータを定義するには、閉じ括弧の前に . ***パラメータ名***を追加します。^errno: <#.number> - <*.error_text> というパターンは、次のメッセージと一致します。

```
errno: 125 - device does not exist
```

この場合、**number** には 125 が割り当てられ、**error_text** には device does not exist が割り当てられます。

変数名に使用できる文字は、英数字、アンダースコア (_)、ハイフン (-) のみです。次の構文ルールが適用されます。

```
(Letter | '_'){ Letter | Digit | '_' | '-' }
```

上の構文では、Letter には任意のアルファベット文字、Digit には任意の数字を指定できます。

HPOM での変数への文字列の割り当てに適用されるルール

文字列 abcdef に対して <*.**var1**><*.**var2**> というパターンを一致させる場合、入力文字列のどのサブストリングが各変数に割り当てられるのかがすぐにはわかりません。たとえば、var1 に空の文字列を割り当て、入力文字列全体を **var2** に割り当てることも、**var1** に a を割り当て、**var2** に bcdef を割り当てることも可能です。

パターンマッチのアルゴリズムは、入力行とパターン定義 (代替表現を含む) の両方を常に左から右にスキャンします。<*> のような表現には、できるだけ少ない文字が割り当てられます。反対に、<#>、<@>、<_> のような表現には、できるだけ多くの文字が割り当てられます。したがって、上の例の変数には空の文字列が割り当てられます。たとえば、
this is error 100: big bug という入力文字列と一致させるには、次のパターンを使用します。

```
error<#.errnumber>:<*.errtext>
```

この例では :

- **errnumber** には 100 が割り当てられます。
- **errtext** には big bug が割り当てられます。

パフォーマンスの向上と判読性のために、2 つの表現の間に区切りのサブストリングを指定できます。前述の例では、<#> と <*> がコロン (:) で区切られています。

abc123 に対して <@.**word**><#.**num**> を一致させる場合、<#> と <@> はどちらも数字を受け付けますが、前者により多くの文字が割り当てられるため、**word** には abc12、**num** には 3 が割り当てられます。

位置指定記号が指定されていないパターンは、入力行内の任意のサブストリングと一致します。たとえば、this is number<#.num> というパターンは、次のパターンと同様に扱われます。

```
<*>this is number<#.num><*>
```

サブパターンによる変数への文字列の割り当て

変数に文字列を割り当てるには、アスタリスク (*) や番号記号 (#) などの単一演算子を使用できる以外に、次のパターンに従って多数の演算子を使った複雑なサブパターンを作成することもできます : <[***サブパターン***].*var*>

次に例を示します。

<[<@>file.tmp].*fname*>

この例では、file と tmp の間のピリオド (.) はピリオド文字と一致し、「]」と「fname」の間のピリオドは、構文上必要な文字です。このパターンは Logfile.tmp などの文字列と一致し、fname には文字列全体が割り当てられます。

サブパターンのその他の例を示します。

<[Error|Warning].sev>

<[Error[<#.n><*.msg>]].complete>

最初の例では、変数 sev には、Error または Warning という単語が含まれるすべての行が割り当てられます。2 番目の例では、変数 n には Error という単語が含まれるすべての行のエラー番号、変数 msg にはそれ以外のテキストが割り当てられます。最後に、番号とテキストの両方が変数 complete に割り当てられます。

一致メッセージの表示

メッセージがメッセージ条件と一致した場合、それをブラウザに表示する前に特定の設定を割り当てることができます。

メッセージ設定の割り当て

次の設定に新しい値を割り当てることができます。

- ❏ 重要度レベル
- ❏ ノード
- ❏ アプリケーション
- ❏ メッセージグループ
- ❏ オブジェクト
- ❏ メッセージテキスト
- ❏ メッセージタイプ
- ❏ メッセージキー
- ❏ サービス名

条件レベルで設定される属性の値は、ポリシーのデフォルト設定によって設定される同じ属性の値に優先して適用されます。メッセージテキストの一部をパラメータとして使用して、オペレータのブラウザにメッセージを転送する前にメッセージテキストを定義し直すこともできます。

メッセージへのカスタムメッセージ属性の追加

カスタムメッセージ属性を使用することで、独自の属性をメッセージに追加できます。つまり、223 ページの「メッセージ設定の割り当て」に示されるデフォルトのメッセージ属性のほかに、顧客を表す「Customer」や、サービスレベル契約を表す「SLA」など、任意の属性を追加して HPOM メッセージを拡張できます。

カスタムメッセージ属性を設定できるのはメッセージ条件のみであり、それを使用できるのはログファイル、HPOM インタフェース、しきい値モニターポリシーだけです。

メッセージにカスタムメッセージ属性を割り当てるには、コマンド行ツール `opccmachg` を使用します。詳細については *opccmachg(1m)* のマニュアルページを参照してください。

カスタムメッセージ属性を作成して割り当てるときは、属性名と値を次のように指定できます。

```
# opccmachg -user opc_op -id
55d3604a-536f-71db-08c0-0a1108c90000 CUSTOMER=VIP SLA=none
Device=Device1 Source=Node1
```

次の条件と一致するメッセージは、追加の 4 つのカラムと共に Java GUI ブラウザに表示されます。

- Customer
- Device
- SLA
- Source

値には、次のいずれか、または組み合わせを含めることができます。

- ハードコードされたテキスト
- HPOM のパターンマッチメカニズムから返される変数

  詳細については 212 ページの「メッセージのパターンマッチ」を参照してください。
- あらかじめ定義されている HPOM 変数

  詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

注記

カスタムメッセージ属性は、Java GUI のブラウザとメッセージプロパティウィンドウのみに表示されます。

適切に設定した場合、カスタムメッセージ属性はエージェント上のメッセージストリームインタフェース (MSI)、管理サーバー、または両方に渡されます。カスタムメッセージ属性も、トラブルチケットシステム、通知サービス、または両方に渡されます。

メッセージへの指示の追加

メッセージには指示を追加できます。通常、これらの指示は自動アクションについて説明する、オペレータ起動アクションの実行方法の詳細を示す、または障害を解決するためのその他の手動手順について説明するために使用されます。

メッセージへの指示の追加は、次のいずれかの方法で行います。

❑ **指示の記述**

メッセージ条件の指示を記述します。これにより、条件と一致するすべてのメッセージにその指示が追加されます。テキストは、Java GUI メッセージブラウザの [メッセージのプロパティ] ウィンドウで表示できます。シンプルなテキストベースの指示を利用するメリットは、指示がデータベースに保存されることです。

この方法には次のメリットがあります。

- 指示の信頼性が高い
- 指示が高速で解決される

❑ **外部アプリケーションの呼び出しによる指示の送信**

指示テキストインタフェースを使って外部アプリケーションを呼び出し、オペレータに指示を提供します。この方法を利用するメリットは、数多くの種類のパラメータをインタフェースに渡すことができることです。テキストベースのインタフェースを設定する方法の例については、次のファイルを参照してください。

```
/opt/OV/OpC/examples/progs/oii_readme
```

この方法は柔軟性に富みます。

- *変数*

  テキストに変数を含めることができます。変数などを利用することで、指示を完全にローカライズできます。

- *メッセージ固有*

  メッセージ条件に固有の指示だけでなく、特定のメッセージに固有の指示を作成できます。

Java GUI では、Java GUI を実行しているクライアント上で外部アプリケーションを呼び出したり、Web ブラウザを起動する特別な HPOM 変数を利用できます。詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

メッセージへの応答

HPOM には、条件と一致するメッセージに応答するためのオプションがいくつか用意されています。オペレータは、メッセージブラウザでこれらのオプションを利用してメッセージに応答します。一部の応答は、オペレータが認識することなく行われます。

応答

次の応答タイプから選択できます。

- **管理サーバーのみでのメッセージのロギング**

  このオプションを選択した場合、メッセージ条件と一致するメッセージは管理サーバー上でログに記録され、履歴データベースに保存されます。これらのメッセージはそれ以上処理されませんが、オペレータは Java GUI の**履歴メッセージ**ブラウザでこれを表示できます。

  管理サーバーのみでメッセージをログに記録する場合、その他のアクションは無視されます。

- **自動アクションの定義**

  自動アクションは、メッセージを受信すると直ちに開始されます。アクションごとに、アクションの実行場所となるノードと、実行するコマンド (シェルスクリプト、プログラム、アプリケーション起動、その他の応答) を定義する必要があります。オペレータは、必要に応じて実行中の自動アクションを停止 / 再開させることができます。

  自動アクションによって注釈を提供し、成功した場合に注釈を自動的に受諾するように指定することもできます。自動アクションに自動受諾を設定すると、オペレータの Java GUI メッセージブラウザにメッセージが表示されなくなることがあります。

❑ **オペレータ起動アクションの定義**

オペレータは、Java GUI メッセージブラウザでメッセージを確認した後に、**オペレータ起動アクション**を開始できます。自動アクションの場合と同様に、オペレータは必要に応じて実行中のアクションを停止 / 再開させることができます。ノードとコマンドを定義できます。また、注釈と自動受諾も指定できます。

オペレータ起動アクションを開始した場合に具体的に何が行われるのかをオペレータが把握できるように、原則として、オペレータ起動アクションの詳細情報を指示として入力します。通常、オペレータ起動アクションではオペレータによる何らかの操作が必要です。または、何らかの前提条件を設定または確認する必要があります。

例 :

- バックアップを開始する前にデータベースを停止する
- プリントスプーリングの前に、サブシステムがメンテナンスモードに入ることをユーザーに知らせる

❑ **メッセージの転送**

メッセージをトラブルチケットシステムまたは外部の通知サービスに転送できます。さらに、メッセージの転送後の自動受諾も設定できます。

自動注釈と自動受諾の設定

自動アクションとオペレータ起動アクションのどちらにも、自動注釈と自動受諾を設定できます。

自動注釈は次の情報をログに記録します。

❑ アクションの開始時刻と終了時刻

❑ アクションの終了値

❑ `stdout` と `stderr` に書き込まれるアクション情報

アクションが失敗すると、自動的に注釈が書き込まれます。アクションの自動受諾を設定すると、アクションの処理が成功した場合にメッセージが自動的に受諾されます。自動受諾を設定しない場合は、オペレータが Java GUI ブラウザでメッセージを手動で受諾する必要があります。

メッセージの最適なフィルタリングのための方針

ここでは、システムのパフォーマンスを改善し、オペレータのブラウザに重複メッセージや不要なメッセージが表示されないようにするために、メッセージフィルターを最適化する方法について説明します。

メッセージのフィルタリング

管理対象ノードと管理サーバー上のメッセージをフィルタリングできます。

- **管理対象ノード**

  管理対象ノード上のできるだけ多くのメッセージをフィルターによって除外することで、ネットワークトラフィックを最小化し、管理サーバーの負荷を削減できます。

- **管理サーバー**

  管理サーバーでフィルタリングを行うことで、複数のノードからのメッセージを比較し、関連付けることができます。管理サーバーは、除外されたメッセージのカウンターを維持するように設定できます。**グループ替え条件**を利用することで、オペレータの Java GUI メッセージブラウザに表示されるメッセージのグループをカスタマイズできます。グループ替え条件は、メッセージの除外には使用されません。グループ替え条件の詳細については 252 ページの「メッセージのグループ替え」を参照してください。

パフォーマンスの最適化

条件を適切な順序で指定し、非該当除外条件を適用することで、処理のパフォーマンスを簡単に最適化できます。

適切な順序での条件の構成

システムで処理されるメッセージの種類と数は、ポリシー内に指定された条件の順序によって決まります。原則として、非該当除外条件または除外条件から始まるポリシーは、不要なメッセージを最初に除外するため、メッセージ条件から始まるポリシーよりも、処理は少なくて済みます。一致させるメッセージが少なくなり、処理量が減少し、パフォーマンスが向上します。

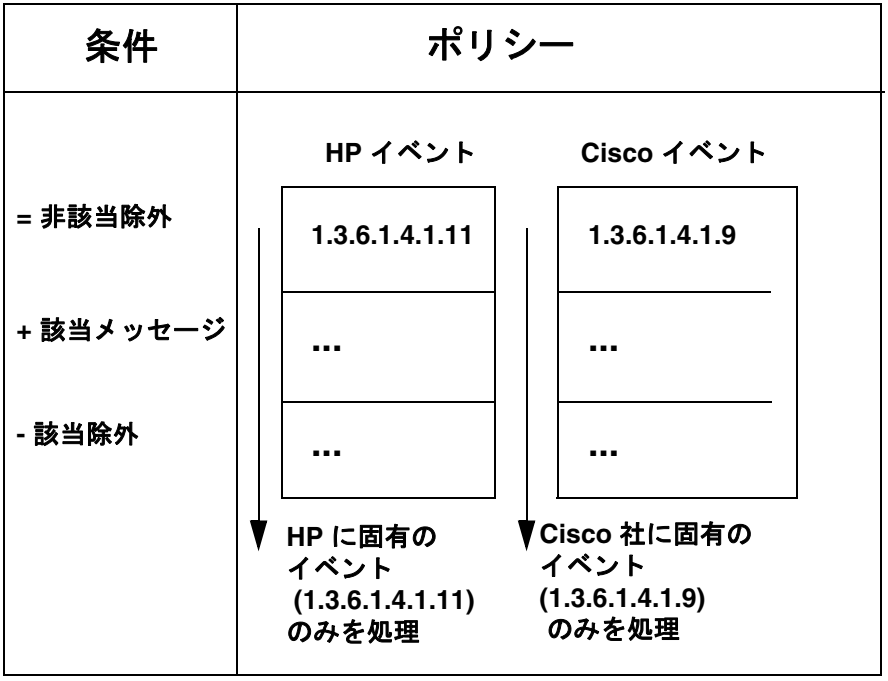
非該当除外条件の適用

非該当除外条件は、管理対象ノード上のイベントをフィルタリングします。この条件を使用することで、特定のポリシーで「意図されていない」イベントの一致処理を停止できます。非該当除外条件は、指定されたパターンと一致しないイベントを除外しますが、一致するイベントは、リストに指定されている条件によって処理されます。メッセージを除外することで、ポリシーで意図されるイベントのみが HPOM による処理の対象となるため、管理対象ノードでのパフォーマンスが向上します。

たとえば、SNMP トラップのフィルタリングのパフォーマンスを向上させるには、環境内で発生する各企業に固有のイベントごとに 1 つのポリシーを作成します。その上で、条件リストの最初に非該当除外条件を配置します。HPOM は、条件と一致しない MIB オブジェクトからの SNMP トラップを除外し、そのポリシーで意図される SNMP トラップのみを処理します。

図 4-8 では、HP に固有の SNMP を対象としたポリシーにより Cisco 社の MIB オブジェクトからの SNMP トラップが除外され、HP に固有のイベントのみが処理されます。

図 4-8 企業に固有の SNMP トラップのチャネリング



メッセージ数の削減

オペレータは、HPOM からメッセージブラウザに送信される多数のメッセージに翻弄されることがよくあります。

- **関連メッセージ**

  一部のメッセージは相互に関連しています (たとえば、アプリケーションの停止とその後の再起動)。

- **類似する、または同一のイベント**

  一部のメッセージは、類似する、または同じイベントについて報告しています (たとえば、3 回の root ユーザーへのユーザー切り替え)。

- **障害の悪化**

  一部のメッセージは、障害状況の悪化の程度を報告しています (たとえば、管理対象ノードでのディスク空き容量の低下)。

HPOM は、重要なメッセージと関連メッセージのみがオペレータに送信されるように設定できます。同じ、または類似した障害に関連するメッセージは除外したり、相関処理によってより意味のある新しいメッセージに置き換えることができます。

メッセージとイベントの相関処理

メッセージ相関処理とイベント相関処理により、メッセージを置き換えることができます。

- **メッセージ相関処理**

  メッセージ相関処理には HPOM の内蔵メカニズムが使用されますが、提供されるのは基本的な相関処理手法のみです。相関処理手法を初めて利用し、今後、より洗練されたソリューションに進んでいく場合は、このメッセージ相関処理を利用することをお勧めします。

- **イベント相関処理**

  イベント相関処理は、より洗練されたソリューションですが、特別なイベント相関処理製品 (HP ECS Designer など) を別途購入する必要があります。イベント相関処理の詳細については 290 ページの「HPOM でのイベント相関処理」を参照してください。

表 4-1 は、イベント相関処理とメッセージ相関処理の違いを示しています。

表 4-1　　イベント相関処理とメッセージ相関処理の比較

イベント相関処理	メッセージ相関処理
• HPOM により提供されるデフォルトの EC ポリシー。 • HP Event Correlation Designer などのイベント相関処理製品を購入する必要がある。	• 別製品の購入は不要。
• 設定と維持は比較的困難であるが、より複雑な条件に対応できる。	• 簡単に設定できるが、シンプルな相関処理にしか対応できない。
• イベントストリームを扱うことができる。イベント相関処理エンジンによる処理の中で、イベントの状態は変化する可能性があります。現在の状態に応じて、同じ入力イベントから異なる出力イベントが生成されることもあります。	• メッセージは静的に処理される。
• HP Event Correlation Designer の「注釈ノード」の概念により、出力イベントに異なるアクションを添付できる。	• 除外[a] または自動受諾のみに対応。
• HPOM とイベント相関処理製品の間でデータが交換される。	• すべてのデータは HPOM によって処理される。パフォーマンスは影響を受けません。
• イベント相関処理サービスがダウンすると、データが失われる可能性がある。	• すべてのデータは HPOM によって処理される。HPOM がダウンしても、データはデータベースに保存されます。

a. 管理サーバーを適切に設定することで、除外されたメッセージをカウントすることもできます。

メッセージ相関処理

メッセージ相関処理は、類似した、または同一のイベント / メッセージを HPOM が比較するメカニズムです。

イベントとメッセージに対し、HPOM は次のいずれかの方法で反応します。

- **自動受諾**

  関係が確立されたメッセージを自動的に受諾します (236 ページの「標準的なシナリオの自動化」を参照)。

- **重複メッセージの除外**

  重複するメッセージを除外します (240 ページの「重複メッセージの除外」を参照)。

管理サーバーで重複メッセージの除外を有効にすると、HPOM は除外されたメッセージのカウンターも維持します。

メッセージキー

メッセージの相関処理は、**メッセージキー**に基づいて行われます。場合によっては、その他のイベント属性またはメッセージ属性が比較されます。メッセージキーは、メッセージ生成の原因となったイベントの重要な特徴を要約したメッセージ属性です。

メッセージキーの関係の設定には、キーワード `MSGKEY` および `MSGKEYRELATION ACK` を使用します。

効果的なメッセージキーのためのガイドライン

効果的なメッセージキーは、メッセージ生成の原因となるイベントを簡潔に説明します。メッセージキーには、イベントに関する重要な情報のみを含めます。タイムスタンプや詳細情報などの不要データは含めません。効果的なメッセージキーは、状態ベースのブラウザ (236 ページの「標準的なシナリオの自動化」を参照) および重複メッセージの除外 (240 ページの「重複メッセージの除外」を参照) に使用できます。

効果的なメッセージキーを作成するには、次のガイドラインに従ってください。

- **メッセージキーにノード名を含める**

  HPOM 変数 $MSG_NODE_NAME を使用します。この変数を使用することで、あるコンピュータ上で生成されるメッセージに、別のコンピュータで生成されるメッセージとは異なるメッセージキーが割り当てられます。

  例 :

  ```
  my_appl_down:<$MSG_NODE_NAME>
  ```

- **その他の重要メッセージ属性を含める**

  メッセージキーには、メッセージの重要な側面を説明するすべてのメッセージ属性を含める必要があります。一般的には、ノード、オブジェクト、アプリケーション、重要度、サービス名、モニター名 (しきい値モニターポリシーの条件を定義する場合)、または Condition セクションに定義されている変数などの属性があります。

  例 :

  ```
  appl_status:<$MSG_APPL>:<$MSG_OBJECT>:<$MSG_NODE_NAME>
  ```

  使用できる HPOM 変数のリストについては、『*HPOM システム管理リファレンスガイド*』を参照してください。

- **メッセージの重要度を反映させる**

  重要度が異なるメッセージには、異なるメッセージキーを割り当てる必要があります。ただし、重要度を示す文字列自体をメッセージキーに含める必要はありません。重要度レベルの原因を含めることで重要度を反映させるようにしてください。この原因は、メッセージの情報自体に含まれています。たとえば、しきい値モニターポリシーでは、変数 <$THRESHOLD> を含めることができます。<$THRESHOLD> の各値は明確な重要度レベルを示します。

- **HPOM がデフォルトキーを生成できるようにする**

  ポリシー内の各条件のデフォルトのメッセージキー関係と共にデフォルトのメッセージキーを生成するには、キーワード AUTOMATIC_MSGKEY を使用し、オプションとして直後に文字列値を指定します。このキーワードは、既存の条件にもメッセージキーを割り当てることができます。

メッセージキー関係については 237 ページの「デフォルトのメッセージキーとメッセージキー関係を生成するには」を参照してください。

- **判読性を考慮する**

  メッセージキーの各要素をコロン (:) などで区切ります。

  例 :

  ```
  my_appl_down:<$MSG_NODE_NAME>
  ```

効果的なメッセージキー関係のためのガイドライン

効果的なメッセージキー関係を作成するには、次のガイドラインに従ってください。

- **変数の解決に注意する**

  メッセージキー関係は、主に管理対象ノード上で解決される HPOM 変数から構成されます。関係には、HPOM パターン定義を含めることもできます。パターンは、管理サーバー上でマッチングされます。

- **判読性を考慮する**

  メッセージキーの関係の各要素をコロン (:) などで区切ります。

  例 :

  ```
  my_appl_down:<$MSG_NODE_NAME>
  ```

- **関係を位置指定文字で囲む**

  メッセージキー関係を位置指定文字で囲みます。最初の文字には脱字符号 (^) を使用し、最後の文字にはドル記号 ($) を使用します。これにより、処理パフォーマンスが向上します。

  例 :

  ```
  ^<$NAME>:<$MSG_NODE_NAME>:<$MSG_OBJECT>:<*>$
  ```

- **パターン定義を適切な位置に指定する**

  メッセージキー関係内でパターン定義を使用するときは、関係文字列の適切な部分に配置してください。パターン定義を適切に配置することで、処理パフォーマンスが向上します。

  *適切*な位置に配置したパターン定義の例 :

  ```
  ^<$MSG_NODE_NAME>:abcdef:[ パターン ]$
  ```

*不適切*な位置に配置したパターン定義の例 :

```
^[ パターン ]:<$MSG_NODE_NAME>:abcdef$
```

❑ 大文字 / 小文字の区別のチェックとフィールドセパレータを指定する

受諾するメッセージの定義に使用できる HPOM 変数のリストについては、『*HPOM システム管理リファレンスガイド*』を参照してください。

標準的なシナリオの自動化

メッセージを自動的に受諾できると便利な場合があります。

次の例は、これについて説明しています。

障害の解決

最初のメッセージで障害が報告されたとします。2 番目のメッセージでは、障害が解決されたことが報告されるかもしれません (たとえば、パスワードが誤っていたためにユーザーがログオンに失敗したが、2 回目には正しくログオンできた場合など)。または、問題が悪化したことが報告されるかもしれません。いずれの場合も、最初のメッセージとはすでに関係なくなっています。このため、2 回目のメッセージによって最初のメッセージが受諾されると便利です。

HPOM では、このようなシナリオを自動化できます (たとえば、アプリケーションの停止とその後の再起動など)。

状態ベースのブラウザ

メッセージを自動的に受諾すると、ブラウザに表示されるメッセージは、管理対象ノードあたり最大で 1 つになります。このメッセージは、オブジェクトの現在のステータスを反映しています。メッセージブラウザは、事実上、状態ベースのブラウザとなります (しきい値モニターにこの概念を適用する方法については 237 ページの「デフォルトのメッセージキーとメッセージキー関係を生成するには」を参照)。

メッセージキーによるメッセージの受諾

関連付けられたメッセージを操作するときに、最初のメッセージと 2 番目のメッセージの間の関係は、メッセージキーによって確立されます。メッセージキーは、メッセージのメッセージキーをマッチングによって特定することでそのメッセージを受諾します。パターンは、キーワード `MSGKEYRELATIONS ACK` を使ってポリシー本文に指定されます。

受諾される側のメッセージと受諾する側のメッセージへの注釈の追加

メッセージが別のメッセージによって受諾される場合、両方のメッセージに次のように注釈を付けることができます。

- **受諾される側のメッセージ**

  *受諾される側*のメッセージには、*受諾する側*のメッセージに関する詳細情報が自動的に注釈として追加されます。*受諾する側*のメッセージの詳細情報には、メッセージ ID、条件 ID、メッセージキー関係が含まれます。

- **受諾する側のメッセージ**

  *受諾する側*のメッセージには、*受諾される側*のメッセージに関する詳細情報が注釈として追加されます。*受諾される側*のメッセージの詳細情報には、メッセージキー関係、そのメッセージが受諾したメッセージの数、メッセージ ID、条件 ID が含まれます。

これらの注釈は、トラブルシューティングに役立ちます。

注記

メッセージのステータスは、そのメッセージが受諾されるかどうかに影響しません。所有メッセージ、ペンディングメッセージ、アクションを実行中のメッセージも受諾されます。

デフォルトのメッセージキーとメッセージキー関係を生成するには

HPOM では、しきい値モニターポリシー用にデフォルトのメッセージキーと、メッセージキー関係を条件ごとに生成できます。

各条件のデフォルトのメッセージキーとメッセージキー関係を生成するには、キーワード AUTOMATIC_MSGKEY を使用します。

生成されるデフォルト値は次のとおりです。

- **メッセージキー**

  ```
  <$NAME>:<$MSG_NODE_NAME>:<$MSG_OBJECT>:<$THRESHOLD>
  ```

- **メッセージキー関係**

  ```
  ^<$NAME>:<$MSG_NODE_NAME>:<$MSG_OBJECT>:<*>$
  ```

たとえば、解決されたメッセージキーは次のようになります。

```
disk_util:managed_node.hp.com:/:90
```

このメッセージキーは、ノード managed_node.hp.com 上のルートディレクトリ (/) のディスク容量が 90% 以上使用されていることをモニター disk_util によって検出されたことを示しています。

メッセージキー関係により、モニター disk_util が生成するこれらのすべてのメッセージは自動的に受諾され、ノード managed_node.hp.com の / ディレクトリのディスク使用率がしきい値を超過した、または下回ったことがこれらのメッセージによって報告されます。

リセットメッセージの自動送信

最初にしきい値の超過が生じ、その後のモニター値がすべての該当リセット値を下回った場合 (つまり、どの条件とも一致しなくなった場合)、HPOM では、リセットメッセージの送信によってモニター対象オブジェクトの最後のメッセージも自動的に受諾されます。

リセットメッセージには、特定のモニター用に最後に送信されたメッセージを受諾するメッセージキー関係が用意されています。この最後のメッセージには、メッセージキーが含まれている必要があります。含まれていない場合、リセットメッセージは送信されません。

リセットメッセージを設定することはできません。リセットメッセージのデフォルトテキストは次のとおりです :

< **モニター名** >[(< **インスタンス** >)]:< **値** > (below reset).

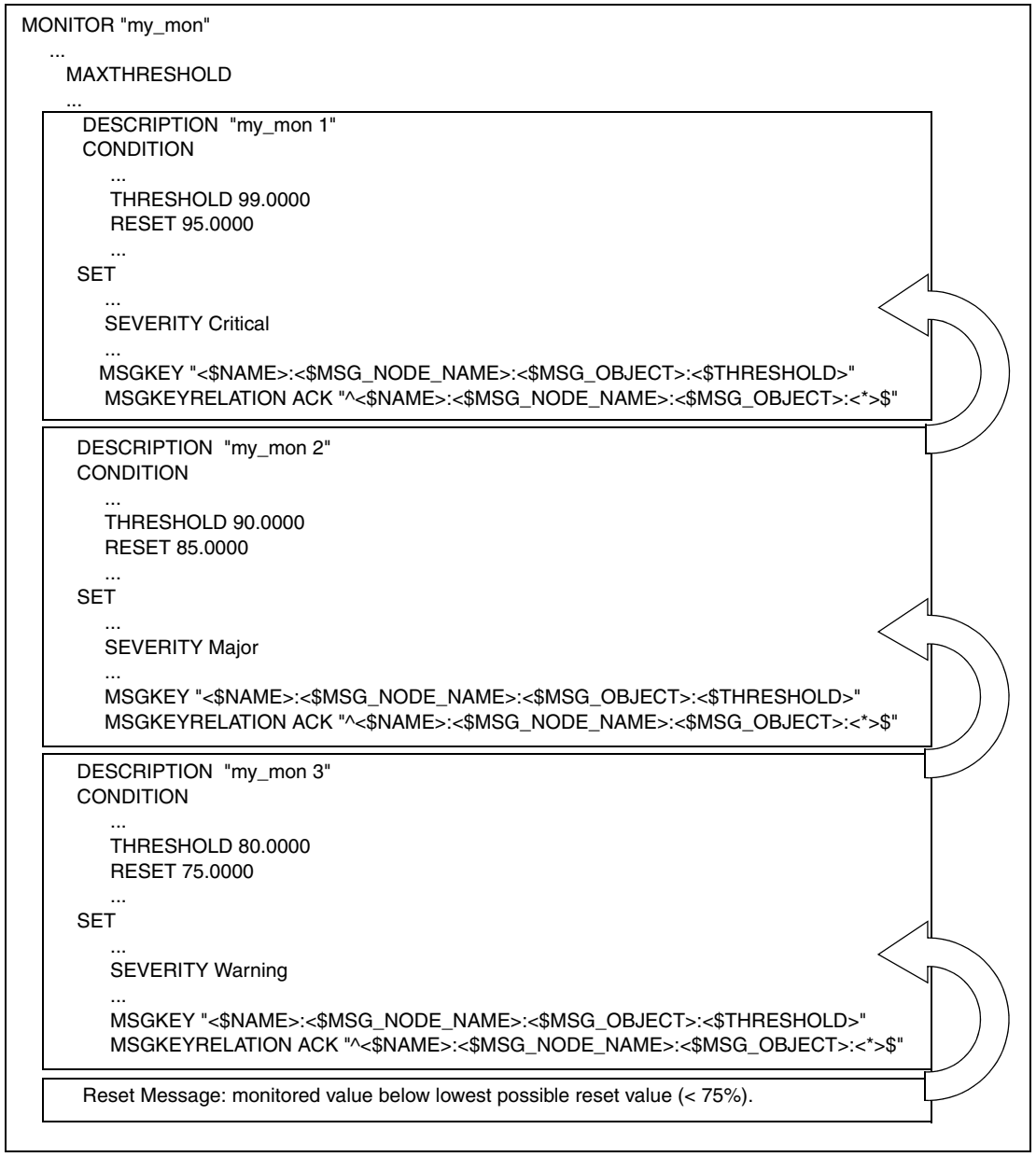
リセットメッセージはメッセージブラウザには表示されず、履歴データベースに直接送信されます。リセットメッセージの重要度は正常域に設定されます。自動 / オペレータ起動アクションは定義されません。

1 つのモニター対象オブジェクトに複数の条件が存在する場合のモニターエージェントの動作については 278 ページの「複数の条件によるしきい値モニター」を参照してください。

自動リセットメッセージの例

図 4-9 は、自動的に送信されるリセットメッセージの例を示しています。

図 4-9　　HPOM リセットメッセージの例



この例では、モニター my_mon には 3 つの条件があります。

- my_mon 1

  モニター値が 99% を超過すると危険域メッセージを生成します。値が 95% を下回ると、カウンターはリセットされます。

- my_mon 2

  モニター値が 90% を超過すると重要警戒域メッセージを生成します。値が 85% を下回ると、カウンターはリセットされます。

- my_mon 3

  モニター値が 80% を超過すると警告メッセージを生成します。値が 75% を下回ると、カウンターはリセットされます。

各メッセージのメッセージキー関係により、それ以前のメッセージは自動的に受諾されます。最後のメッセージ (「my_mon 3」によって生成されたメッセージ) は、モニター値が該当最低リセット値 (この例では 75%) を下回ると、リセットメッセージによって自動的に受諾されます。

生成される各メッセージの、解決されたメッセージキーはそれぞれ異なります。解決されたそれぞれのメッセージキーには条件に固有のしきい値が含まれ、それによってメッセージの重要度が示されます。

重複メッセージの除外

一般に、重複メッセージとは、同じ、または類似したイベントを報告するメッセージを意味します。たとえば、ユーザーが別のユーザーに切り替わるたびに HPOM はメッセージを生成します。ユーザーが常に同じユーザーに切り替わるのであれば、この情報は余分なものと見なすことができ、同一イベントとして宣言することで、これに関連するメッセージを HPOM に除外させることができます。さらに、HPOM では、重複メッセージを新たに送信するまでのメッセージの除外頻度と除外期間を設定できます。

注記

受信する重複メッセージの重要度やメッセージテキストの内容が、既存の重複メッセージから変更されている場合に、古いデータの代わりに新しい値を表示するように HPOM を設定できます。詳細については 249 ページの「重複メッセージの重要度とメッセージテキストの更新」を参照してください。

HPOM を設定し、管理対象ノードまたは管理サーバー上の重複メッセージを除外できます。管理対象ノード上のメッセージをフィルタリング (除外) すると、ネットワークトラフィックが軽減され、管理サーバーが別のタスクを実行しやすくなります。

管理対象ノード上のメッセージを除外するほうがパフォーマンス上の効果が大きいため、HPOM には管理対象ノード向けの除外タイプや設定は豊富に用意されていますが、管理サーバー向けにはグローバル設定しかありません。注釈が追加される重複メッセージの数を制限するには、設定変数 OPC_MAX_DUPL_ANNO を使用します。

除外タイプの検証

条件イベントが条件と一致すると、HPOM は、次のいずれかの除外タイプが選択されているかどうかを検証します。

❑ **条件と一致するメッセージの除外**

HPOM は、選択されている条件と一致する *すべての* 重複メッセージを除外します。つまり HPOM は、同一条件によって生成されたメッセージがすでに存在するかどうかをチェックします。

すでにメッセージが存在し、指定されている時間内に 2 回目のイベントが発生した、または設定されているカウンターの値を下回る場合は、2 回目のメッセージは除外されます。

❑ **同一入力イベントの除外**

HPOM は、*イベント属性* が等しい重複メッセージのみを除外します。つまり HPOM は、同一入力イベントによって生成されたメッセージがすでに存在するかどうかをチェックします。メッセージの入力イベントは、ポリシー条件の Condition セクションに定義されます。次のイベント属性が等しい場合、複数のメッセージは同一と見なされます。

- 重要度
- ノード
- アプリケーション
- メッセージグループ
- オブジェクト
- メッセージテキスト (元のメッセージテキスト)

すでに同一メッセージが存在し、指定されている時間内に 2 回目のイベントが発生した、または設定されているカウンターの値を下回る場合は、2 回目のメッセージは除外されます。

❑ **同一出力メッセージの除外**

HPOM は、*メッセージ属性*が等しい重複メッセージのみを除外します。つまり HPOM は、同じメッセージ属性を持つメッセージがすでに存在するかどうかをチェックします。メッセージの属性は、ポリシー条件の `Set Attributes` セクションに定義されます。メッセージキーが等しい場合、複数のメッセージは同一と見なされます。

いずれかのメッセージにメッセージキーが含まれない場合は、次のメッセージ属性が同じである必要があります。

- 重要度
- ノード
- アプリケーション
- メッセージグループ
- オブジェクト
- メッセージテキスト
- サービス名

すでに同一メッセージが存在し、指定されている時間内に 2 回目のイベントが発生した、または設定されているカウンターの値を下回る場合は、2 回目のメッセージは除外されます。

`syslog` デーモンのログファイル (HP-UX では `/var/adm/syslog/syslog.log`) は、「同一出力メッセージの除外」オプションによる重複メッセージの除外を示しています。

ログファイル `syslog` の次の行を例にとります。

```
Mar 14 14:39:01 server inetd[9900]: telnet/tcp:
Connection from node1 at Tue Mar 14 14:39:01 2009

Mar 14 12:46:02 server inetd[9005]: login/tcp: Connection
from node2 at Tue Mar 14 12:46:02 2009
```

パターンマッチテキストは次のようなものとします。

```
"inetd\[<#>\] <@.service>: Connection from <@.from_node>"
```

inetd 接続メッセージの重要な特徴は、ローカルノード、接続を行った側のノード、inetd サービスです。syslog のタイムスタンプ、PID、接続時刻は重要ではありません。

メッセージキーは次のようになります。

inetd_connect_from:<*$MSG_NODE_NAME*>:<*from_node*>:<*service*>

このメッセージキーは、同じサービスのために同じノードに接続するすべてのノードからのすべてのメッセージを除外します。

重複メッセージの除外では、同じ条件によって生成されるメッセージのみが処理されます。別の条件によって生成される重複メッセージを除外するには、管理サーバー上でこの機能を有効にします。詳細については 247 ページの「管理サーバーでの重複メッセージの除外」を参照してください。

注記

しきい値モニターポリシーでは、管理対象ノード上の重複メッセージの除外を適用 *できません*。しきい値モニターポリシーからの重複メッセージを除外する方法については 247 ページの「管理サーバーでの重複メッセージの除外」を参照してください。

重複メッセージの除外タイプ、時間間隔、およびカウンターまたはしきい値設定を指定できます。重複メッセージの除外には 3 種類あります。目的の結果を得るには次のキーワードを使用します。

SUPP_DUPL_COND	同じ条件と一致するすべてのメッセージを除外します。
SUPP_DUPL_IDENT	元のメッセージテキスト (入力) が同じすべてのメッセージを除外します。
SUPP_DUPL_IDENT_OUTPUT_MSG	出力メッセージテキストが同じすべてのメッセージを除外します。

次のキーワードの値は、メッセージが除外される時間間隔を表します。時間値の代わりにキーワード COUNTER_THRESHOLD を使って数値を指定すると、指定した数のメッセージを受信するまでメッセージは除外され、指定数に達すると、1 つのメッセージが送信され、カウンターはリセットされます。キーワード RESET_COUNTER_INTERVAL は時間間隔を設定し、その時間が経過すると、受信したメッセージの数に関係なくカウンターはリセットされます。キーワード RESEND は制限時間を設定し、その時間が経過すると、メッセージの送信は再開されます。詳細については、369 ページの付録 A「ポリシー本文の構文」でポリシー本文の構文を参照してください。

除外設定の種類

次の除外設定から選択できます。

- **時間間隔**

  重複イベントが無視される時間間隔と、メッセージの送信を再開するまでの期間を指定します。245 ページの図 4-10 の例では、除外間隔は 30 秒に設定されますが、除外期間は 60 秒に制限されています。

- **カウンター**

  重複メッセージカウンターのしきい値を指定します。HPOM は、しきい値に達する、またはしきい値を超過するまでカウンター値を繰り上げます。しきい値に達する (または超過する) と、HPOM は重複メッセージの送信を許可します。246 ページの図 4-11 の例では、カウンターしきい値は 2 に設定されています。カウンターは 30 秒後にリセットされます。

- **時間間隔とカウンターの組み合わせ**

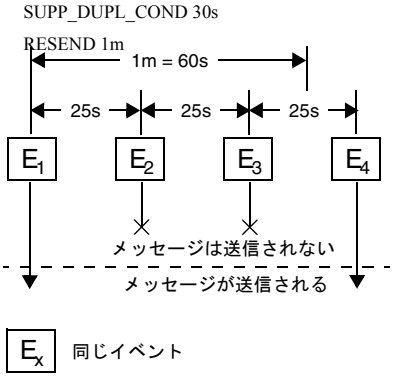
  時間間隔とカウンターを組み合わせて使用した場合、イベントはまずタイマーによって評価されます。タイマーを通過したイベントは、カウンターによって評価され、それに基づいてメッセージは除外されるか、管理サーバーに送信されます。

時間に基づく除外

図 4-10 は時間ベースの除外を示しています。

同一入力イベントの除外では、代わりにキーワード SUPP_DUPL_IDENT を使用します。同一出力メッセージの除外では、キーワード SUPP_DUPL_IDENT_OUTPUT_MSG を使用します。

図 4-10　時間に基づく除外

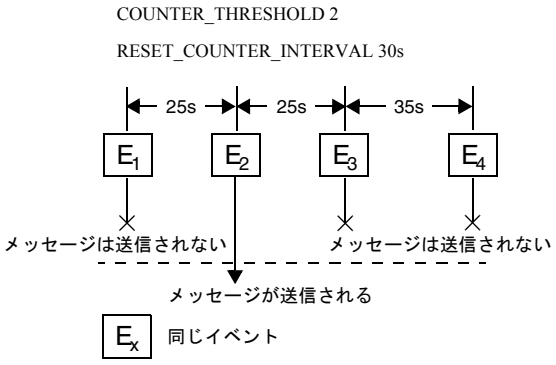


1. 最初のイベント (E_1) が条件と一致します。メッセージが送信され、タイマーが起動されます。
2. 25 秒後に 2 回目のイベント (E_2) が発生します。このイベントは、最初のイベントから *30 秒未満*で発生したため、除外されます。
3. 3 回目のイベント (E_3) も 2 回目のイベントから *30 秒未満*で発生したため、除外されます。
4. 次に条件と一致したイベント (E_4) も 3 回目のイベントから *30 秒未満*で発生しました。しかし、最初のイベントから *60 秒以上*が経過してから発生したため、新しいメッセージが送信されます。

カウンターに基づく除外

図 4-11 はカウンターベースの除外を示しています。

図 4-11　カウンターに基づく除外



1. 最初のイベント (E_1) が条件と一致します。カウンターの値は 1 になります。しきい値の 2 に達していないため、メッセージは送信されません。
2. 条件と一致する 2 回目のイベント (E_2) が 25 秒後に発生します。カウンターの値は 2 になります。メッセージが送信され、カウンターはゼロにリセットされます。
3. 条件と一致する 3 回目のイベント (E_3) が発生します。カウンターの値は 1 になります。メッセージは送信されません。
4. 次に条件と一致したイベント (E_4) は、3 回目のイベントから 30 秒以上が経過してから発生しました。30 秒の時点でカウンターはゼロにリセットされています。このため、カウンターの値は 1 になり、メッセージは送信されません。

管理サーバーでの重複メッセージの除外

重複メッセージの除外は、管理サーバーにも設定できます。管理サーバー上の重複メッセージを除外することで、多数のメッセージによる高システム負荷を大幅に削減できます。さらに、複数の管理対象ノードからのメッセージを相関処理することもできます。

管理サーバーで使用される除外方法は、管理対象ノードで使用される**同一出力メッセージの除外**と同じ方法です。HPOM は、受信メッセージのメッセージ属性と、既存メッセージのメッセージ属性を比較します。

*いずれか*のメッセージにメッセージキーが含まれない場合は、次のメッセージ属性が同じである必要があります。

- ❏ 重要度
- ❏ ノード
- ❏ アプリケーション
- ❏ メッセージグループ
- ❏ オブジェクト
- ❏ メッセージテキスト
- ❏ サービス名

同じメッセージがすでに存在する場合、HPOM はその重複メッセージと、それ以降のすべての重複メッセージを除外します。HPOM は、最初の重複メッセージでカウンターを起動します。このカウンターは、担当オペレータのブラウザウィンドウと [メッセージのプロパティ] ウィンドウに表示されます。カウンターを参照することで、障害が発生している頻度を確認できます。[メッセージのプロパティ] ウィンドウには、重複メッセージを最後に受信した (除外した) 日時も示されます。

除外を有効にすると、HPOM は除外された重複メッセージに関する情報を最初のメッセージへの注釈に保存します。

注記

管理対象ノード上で重複メッセージによって開始された自動アクションの実行は続けられます。ただし、アクションの応答は失われます。

管理サーバーでの重複メッセージ除外の有効化

管理サーバーでの重複メッセージの除外を有効にするには、opcsrvconfig -dms コマンドを使用します。重複メッセージを注釈として追加することも指定できます。次に例を示します。

```
# opcsrvconfig -dms -enable anno
```

注記

重複メッセージの除外は、すべてのメッセージとオペレータに適用されるグローバル設定です。

詳細については *opcsrvconfig(1m)* のマニュアルページを参照してください。

フレキシブル管理環境での重複メッセージの除外

フレキシブル管理環境 (MoM) では、管理を直接担当する管理対象ノードから受信したメッセージのカウントは、各管理サーバーで行われます。つまり、別の管理サーバーから受信したメッセージは 1 つのメッセージに集約されず、複数のメッセージとして表示されます。それぞれのメッセージは、送信元管理サーバーから受信した時点でカウントされます。

管理サーバーにメッセージカウントイベントを送受信させたくない場合は、コマンド行ツール ovconfchg を使って HP Operations 管理サーバーに次の変数を設定します。

- ❏ メッセージカウントイベントの送信

```
ovconfchg -ovrg <OV_resource_group> -ns opc -set \
OPC_SEND_MSG_COUNT FALSE
```

- ❏ メッセージカウントイベントの受信

```
ovconfchg -ovrg <OV_resource_group> -ns opc -set \
OPC_ACCEPT_MSG_COUNT FALSE
```

<OV_resource_group> は管理サーバーのリソースグループの名前です。デフォルトでは、どちらの変数も TRUE に設定されています。

重複メッセージの重要度とメッセージテキストの更新

受信する重複メッセージの重要度やメッセージテキストの内容が、既存のメッセージから変更されている場合に、古いデータの代わりに新しい値を表示するように HPOM を設定できます。

- **重複メッセージの重要度の更新**

  次のコマンドは、最後に受信した重複メッセージの重要度を表示するように HPOM を設定します。

  ```
  ovconfchg -ovrg server -ns opc -set
  OPC_UPDATE_DUPLICATED_SEVERITY LAST_MESSAGE
  ```

- **重複メッセージのメッセージテキストの更新**

  次のコマンドは、最後に受信した重複メッセージのメッセージテキストを表示するように HPOM を設定します。

  ```
  ovconfchg -ovrg server -ns opc -set
  OPC_UPDATE_DUPLICATED_MSGTEXT LAST_MESSAGE
  ```

LAST_MESSAGE に設定すると、メッセージブラウザ上で適切な値が変更されます。

メッセージのロギング

HPOM のメッセージ処理機能は、次の種類のメッセージ結果を生成します。

- **メッセージ条件と一致するメッセージ**

  これらのメッセージはフィルタリング後に HPOM に取り込まれます。これらのメッセージは、さらに処理するためにローカルノードから管理サーバーに転送されます。ソースノード上でこれらのメッセージをロギングするように指定することもできます。条件と一致したメッセージは、担当オペレータのブラウザウィンドウに表示されます。

- **除外条件と一致するメッセージ**

  これらのメッセージは、フィルタリング後に追加処理なしで HPOM から除外されます。ソースノード上でこれらのメッセージをロギングするように設定できます。

- **どの条件とも一致しないメッセージ**

  フィルタリングが行われない場合、条件と一致しないメッセージも HPOM に転送できます。通常、条件と一致しないメッセージは過去に送信されていないメッセージであるため、これらのメッセージのフィルタリング条件はまだ設定されていません。条件と一致しないこれらのメッセージについては、管理対象ノードにローカルにロギングするか、さらに処理するために管理サーバーに転送するかを選択できます。管理サーバーに転送する場合は、それを Java GUI メッセージブラウザに表示するか、履歴データベースに直接保存するかを選択できます。ブラウザに表示する場合、Java GUI メッセージブラウザの U カラムに x が付けられて区別されます。

ロギングオプションは、メッセージソースポリシーと、そのポリシーのメッセージ条件および除外条件を定義した後に設定できます。どの種類のメッセージをどのようにログに記録するかは、追加キーワードを使ってポリシー本文に指定します。

```
LOGMATCHEDMSGCOND
LOGMATCHEDSUPPRESS
LOGUNMATCHED
```

注記

イベント相関処理ポリシーのロギングを有効にすると、その他すべてのイベント相関処理ポリシーのロギングが自動的に有効になります。

メッセージのグループ替え

HPOM によってメッセージが統合、フィルタリングされた後に、管理サーバー上の現在のデフォルトメッセージグループを変更できます。オペレータのタスクと担当範囲に合わせてメッセージグループをカスタマイズできます。つまり、メッセージソースの条件を変更する必要はありません。また、あるグループから別のメッセージグループにメッセージを移動するときに、ポリシーを配布し直す必要もありません。

注記

グループ条件でのサービス名属性の使用の詳細については、『*Service Navigator コンセプトと設定ガイド*』を参照してください。

メッセージ条件と属性は次のように処理されます。

- **メッセージ条件と除外条件**

  メッセージ条件と除外条件は管理対象ノード上で処理され、そこですべての受信メッセージと比較されます。

- **グループ替え条件**

  グループ替え条件は、管理サーバー上でのみ処理されます。グループ替え条件は、事前に管理対象ノード上でフィルターを通過したメッセージと比較されます。

  グループ替え条件と一致するメッセージは、ポリシーに従って別のメッセージグループに転送されます。スプーリングアプリケーションからのすべてのメッセージを Output (出力) というメッセージグループにまとめることができます。

- **メッセージ属性**

  メッセージ条件 / 除外条件と同様に、グループ替え条件用に定義されるメッセージ属性は、メッセージの実際の値のチェックに使用されます。

グループ替え条件の定義

グループ替え条件を定義するときは、管理者の GUI (CVPL) を使用する必要があります。次の場所の HP Operations Manager for UNIX ディレクトリでダウンロードできる CVPL のユーザードキュメントを参照してください。
http://support.openview.hp.com/selfsolve/manuals

注記

存在しないメッセージグループにメッセージをグループ替えすると、デフォルトでは、そのメッセージグループが作成されるまで、そのメッセージグループに関連するすべてのメッセージはメッセージグループ `Misc` (その他) に属します。現在 `Misc` に割り当てられているメッセージの元のメッセージグループを確認するには、Java GUI メッセージブラウザの [メッセージのプロパティ] ウィンドウを使用します。

グループ替え条件 API を使用する方法もあります。

グループ替え条件の例

前述のメッセージ条件の例が、ここに示すグループ替え条件の例の基本となります。

フィルタリング後に HPOM に取り込まれるすべてのメッセージは、メッセージグループ `FINANCE` に転送されます。

ここでは、メッセージを 2 つのグループに分割します。

- Payroll
- Accounting

次に、この 2 つのグループ用のグループ替え条件を示します。

グループ替え条件 1

アプリケーション :	`idris4|idris5`
アプリケーション :	`FINANCE PAYROLL`
テキストパターン :	`^***PAYROLL:[ERROR|WARNING]`
新しいメッセージグループ :	`payroll`

グループ替え条件 2

アプリケーション：	idris4|idris5
アプリケーション：	FINANCE ACCOUNTING
テキストパターン：	^****ACCOUNTING:[ERROR|WARNING]
新しいメッセージグループ：	accounting

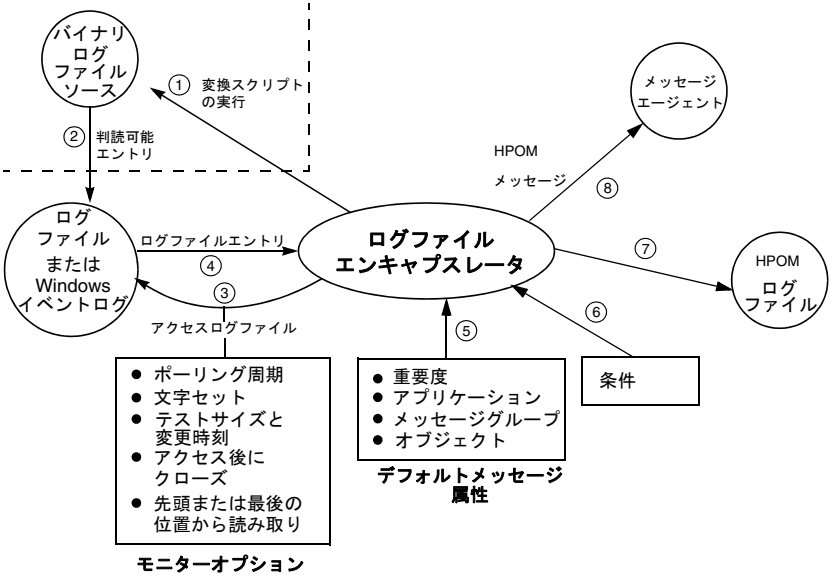
ログファイルメッセージ

アプリケーションとシステムのログファイルは、HPOM **ログファイルエンキャプスレータ**によって捕捉されます。ログファイルにエントリを書き込むアプリケーションまたはサービスからのメッセージを、アプリケーションまたはサービスに一切変更を加えずに HPOM に取り込むことができます。HPOM にはデフォルトのログファイルポリシーが用意されており、これをコピーして、固有のニーズに合わせて変更できます。複数のポリシーを作成し、各種アプリケーション / サービスのログファイルのモニターを設定できます。

ログファイルエンキャプスレータ

図 4-12 は、ログファイルエンキャプスレータがログファイルメッセージをどのように収集、フィルタリング、フォーマット変更し、Java GUI ブラウザに表示するかを示しています。

図 4-12　ログファイルエンキャプスレータ



ステップ 1、2 は、ログファイルがバイナリ形式の場合にのみ必要です。

ステップ 7 は、ローカルロギングが設定されている場合にのみ実行されます。

ステップ 8 は、ログファイルエントリがメッセージ条件と一致した場合、または非該当転送条件と一致した場合に適用されます。

ログファイルポリシー

ログファイルポリシーは、ソースからのすべてのメッセージを説明するデフォルトメッセージ属性を定義します。このポリシーには、ログファイルをいつ、どのようにモニターするかを指定するモニターオプションも含まれます (255 ページの図 4-12 を参照)。

ログファイルポリシーの設定には次の内容が含まれます。

- ❏ **ポリシーの名前と説明**

  `opcpolicy -list_pols` コマンドは、ポリシーの名前と説明を表示します。

- ❏ **ログファイルのパス名と名前**

  ファイルシステム内のログファイルの場所。UNIX 管理対象ノードでは、シェル変数を使って動的なパスを設定できます。ログファイルの名前を動的に検出し、それを `stdout` に書き込むコマンド / スクリプトの名前を指定することもできます。

- ❏ **モニターオプション**

  モニターオプションには、ログファイルをスキャンする前に実行されるコマンド / プログラム、代替ファイル名、ポーリング周期、ログファイルの文字セット、モニターの実行方法に関する詳細情報が含まれます。

  HPOM では、3 つの異なる位置からログファイルを処理できます。

  - *前回のファイル位置から読み取り*

    新たに追加されたエントリのみをモニターします。

  - *ファイルの先頭から読み取り (初回)*

    ログファイルエンキャプスレータが初めてモニターを開始するときに、ログファイル全体をモニターします。次回のポーリング周期では、新たに追加されたエントリのみがモニターの対象となります。

- *ファイルの先頭から読み取り (常に)*

  ログファイルの変更が検出されると、ログファイル全体を読み取ります。ポーリング周期の終了時、起動時、またはログファイルポリシーの配布時に、ログファイルエンキャプスレータはログファイルを処理しません。

inode (UNIX 環境) または作成時刻 (Windows 環境) が変更されると、HPOM はログファイルを新規ファイルとして扱います。ログファイルが新しい場合、ログファイルエンキャプスレータはログファイル全体を処理します。

同じ inode または作成時刻でログファイルが再表示されると、ログファイルは一度も削除されていないかのように処理されます。たとえば、システムログファイルがこれに該当します。

次の場合、ログファイルは新規ファイルとは*見なされません*。

- 既存のファイルにファイルをコピーする

  たとえば、`cp /tmp/xxx /tmp/logfile` によって既存のファイルに対してファイルをコピーしても、inode は変更されないため、ログファイルエンキャプスレータは前回の位置からファイルを読み取ります。

- 引数をファイルにエコーする

  たとえば、`echo "xxx" > /tmp/logfile` によってテキストをファイルにエコーしても、inode は変更されないため、ログファイルエンキャプスレータは前回の位置からファイルを読み取ります。

❑ **メッセージのデフォルト設定**

メッセージのデフォルト設定により、ログファイルポリシーによってフィルタリングされ、HPOM に取り込まれるメッセージにデフォルト属性を入力できます。

❑ **その他のオプション**

その他のオプションには、指示、メッセージ相関オプション、パターンマッチおよびメッセージストリームインタフェースオプションがあります。

ログファイルポリシーを定義するには、ポリシー本文内で更新を行う必要があります。詳細については 369 ページの付録 A「ポリシー本文の構文」を参照してください。

ノード上のログファイルのモニター

注記

ログファイルポリシーでキーワード NODE を使用しない場合、HPOM はログファイルエンキャプスレータが実行されているノードを使用します。HP Operations エージェントがクラスタノードで実行されているクラスタ環境では、ログファイルをモニター対象とする別のノードを指定できます。

NFS マウントファイルシステム上のログファイルを変更する場合、または別のリモートノードから HPOM ログファイルエンキャプスレータが実行されているシステムにログファイルをコピーした場合は、別のノードを指定します。

外部ノード上のログファイルのモニター

外部ノードでイベントが発生した場合、ログファイルエンキャプスレータには自動的に通知されません。外部ノードからログファイルをモニターするには、次のいずれかの方法で行います。

- ネットワークファイルシステム (NFS) を使用して、HPOM を実行しているノード上の特定のディレクトリにファイルシステムをマウントできます。その上で、その他のローカルファイルと同様に、マウントしたファイルシステム上のログファイルをモニターするようにログファイルエンキャプスレータを設定する必要があります。
- 指定したログファイルをコピーするように、またはログファイルからホストシステム上のディレクトリに抽出を行うように外部ノードを設定できます。これは、指定されている時間間隔の経過後、またはログファイルに変更が加えられるたびに自動的に行われます。HPOM はこの機能をサポートしていないため、コピー操作は外部側で実行する必要があります。ログファイルエンキャプスレータは、ファイルのローカルコピーをトラッキングし、コピーの完了後に新しいエントリを処理します。

ログファイルがどのシステムのものであるか、また、どのイベントがメッセージ生成の原因となったかを HPOM オペレータが判断できるように、対応するログファイルポリシーを設定する必要があります。ポリシー本文の構文については 369 ページの付録 A「ポリシー本文の構文」を参照してください。

メッセージポリシーの拡張オプションの定義

パターンマッチ、重複メッセージの除外、およびメッセージストリームインタフェース (MSI) へのメッセージの出力のためのオプションも定義できます。これらのオプションは、新たに追加するポリシーのデフォルト設定として使用されます。既存のポリシーの動作には影響しません。

メッセージの条件の指定

対応するポリシーの本文を編集することで、メッセージの条件を指定できます。ポリシー本文の構文については 369 ページの付録 A「ポリシー本文の構文」を参照してください。

例 4-1 ログファイルポリシーの本文の例

次の例は、アプリケーションログファイルをモニターします。ファイルのチェック間隔は 60 秒です。ログファイルエンキャプスレータは、前回のチェックの最後の位置からファイルの内容をチェックします (キーワード FROM_LAST_POS)。ファイルは読み取りの直前に開かれ、直後に閉じられます (キーワード CLOSE_AFTER_READ)。「missing」という単語が含まれるメッセージは除外され、「failure」という単語が含まれるメッセージの重要度は**危険域**に設定されます。その他すべてのメッセージはサーバーに転送されます (キーワード FORWARDUNMATCHED)。すべてのメッセージのアプリケーション属性は「App」、メッセージグループは「AppLog」に設定されます。条件と一致しなかったすべてのメッセージの重要度は**不明**に設定されます。

```
LOGFILE “Application log”
                    DESCRIPTION “Logfile for Application”
                    LOGPATH “/opt/App/log/logfile.txt”
                    INTERVAL “60s”
                    FROM_LAST_POS
                    CLOSE_AFTER_READ
                    SEVERITY Unknown
                    APPLICATION “App”

MSGGRP “AppLog”
FORWARDUNMATCHED

SUPPRESSCONDITIONS
                    DESCRIPTIN “App messages to be ignored”
                    CONDITION
                                        TEXT “<*> missing<*>”
```

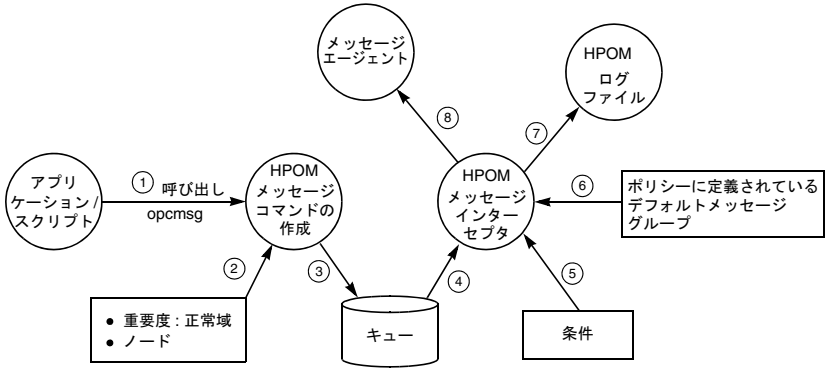
```
MSGCONDITIONS

                    DESCRIPTION “App messages to be ignored”

                    CONDITION

                                        TEXT “<*> failure<*>”

                    SET

                                        SEVERITY Critical
                                        TEXT “<$MSG_TEXT>”
```

HPOM メッセージインタフェース

HPOM メッセージインタフェースコマンド opcmsg(1) とアプリケーションプログラミングインタフェース (API) opcmsg(3) を使用することで、既存のアプリケーションから HPOM にメッセージを直接送信させることができます。

図 4-13 は、HPOM メッセージインタフェースがどのように HPOM メッセージを捕捉、フィルタリング、フォーマット変更し、ブラウザに送信するかを示しています。

図 4-13　HPOM メッセージインタフェース



ステップ 7 は、ローカルロギングが有効な場合にのみ実行されます。

ステップ 8 は、メッセージ条件と一致する場合にのみ実行されます。

コマンド API opcmsg(1|3) の詳細については、マニュアルページを参照してください。

パターンマッチ、重複メッセージの除外、およびメッセージストリームインタフェース (MSI) へのメッセージの出力のためのオプションも定義できます。これらのオプションは、新たに追加するポリシーのデフォルト設定として使用されます。既存のポリシーの動作には影響しません。

しきい値モニターからのメッセージ

HPOM では、指定したしきい値に達する、または超過するたびにメッセージを生成できます。短時間の 1 回のピークでメッセージを生成するのは好ましくない場合もあるため、HPOM では、メッセージを生成する前にモニター値がどれだけの時間しきい値を超過していなければならないかを定義できます。

注記

設定した時間 (たとえば、3 分間) は、それだけの時間にわたってモニター値がしきい値を超過することを必ずしも意味するわけではありません。メッセージは、ポーリング周期中に収集されたすべてのサンプルがしきい値を超過した場合に生成されます。

メッセージに対応した修復アクションの開始

メッセージへの応答として自動 / オペレータ起動アクションを設定しておくことで、修復アクションを直ちに開始できます。既存の障害に対応するモニターだけでなく、発生の過程にある障害に対応するモニターも定義できます。これにより、モニターを予防的ツールと対応的ツールの両方として利用できます。

モニタープログラム / ユーティリティの統合

新しい、または既存のモニタープログラム / ユーティリティを統合し、下限 / 上限しきい値を指定できます。HPOM にモニターを開始させるポーリング周期を指定します。HPOM は、モニタープログラムの結果を読み取り、定義されている制限しきい値と比較します。

たとえば、UNIX ユーティリティ `who(1)` を統合してログオンしているユーザーの人数を調べたり、`df(1M)` を統合して空きディスクブロック数を調べることができます。スクリプトの結果は定義されている制限しきい値と比較され、しきい値を超過している場合はメッセージが生成されます。

しきい値を最大許容値より低く設定することで、絶対的な制限値を実際に超過する前にオペレータに警告できます。このように、障害がユーザーに影響する前に修復アクションを開始することで、しきい値を予防的に管理できます。

しきい値モニターポリシーの設定方法については 273 ページの「しきい値モニターの統合」を参照してください。

モニターエージェントの動作

HPOM モニターエージェントは、次のモニターに対応しています。

- **プログラムモニター**

  使用するモニタースクリプト / プログラムは、設定されているポーリング周期中にモニターエージェントによって起動されます。モニターエージェントは、終了値を読み取ることでスクリプト / プログラムが正しく実行されたかどうかを確認します。終了値がゼロ以外の場合、モニターエージェントはメッセージエージェントにメッセージを送信します。

  モニタースクリプト / プログラムは、モニター対象オブジェクトの現在値を収集します。値は、アプリケーションプログラミングインタフェース (API) opcmon、または HPOM のコマンドインタフェースを通じてモニターエージェントに送信されます。モニターエージェントは、その値と設定されているしきい値を比較します。しきい値を超過している場合は、モニターエージェントはメッセージを送信します。

  Windows オブジェクトのモニターにはプログラムモニターも使用されます。詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

  さらに、組み込みのパフォーマンスコンポーネントが収集したメトリックの統合には、プログラムモニターが使用されます。詳細については 266 ページの「パフォーマンスメトリックのモニター」を参照してください。

- **MIB オブジェクトモニター**

  SNMP Get リクエスト機能を使用することで、MIB オブジェクトをモニターできます。モニターエージェントは、戻り値と設定されているしきい値を比較します。

注記

デフォルトでは、SNMP クエリにはコミュニティ public が使用されます。MIB オブジェクトが別のコミュニティに存在する場合は、MIB のモニターを行う HTTPS ベースの管理対象ノードでコマンド行ツール ovconfchg を使用して、コミュニティ名を定義する必要があります。

コミュニティ名を定義するための構文は次のとおりです。

```
ovconfchg -ns eaagt -set \
SNMP_COMMUNITY <community>
```

この <*community*> が、snmpd が設定されるコミュニティです。

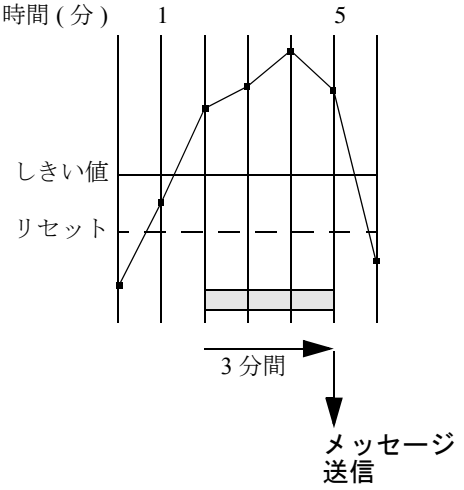
❑ **外部モニター**

外部モニターはプログラムモニターと同じですが、外部モニターは HPOM によって起動されません。外部モニターを起動するには、opcmon を呼び出します。モニター値がしきい値を初めて超過すると、タイマーが起動されます。または、期間が指定されていない場合は、メッセージが生成されます。その後、指定時間内に opcmon から報告されるすべての値が指定のしきい値を超過した場合は、メッセージが送信されます。モニター値が期間全体にわたってしきい値を超過する必要はなく、サンプルの収集時に超過している場合に超過と見なされます。

ポーリング周期によるプログラム /MIB オブジェクトのモニター

図 4-14 は、プログラム /MIB オブジェクトをモニターするためのポーリング周期を定義した後に、メッセージがどのタイミングで生成されるかを示しています。モニター値がしきい値を初めて超過すると、タイマーのカウントが開始されます。再チェックした値が引き続きしきい値を超過している場合は、そのたびにカウンターの値が繰り上げられ、指定されている時間と比較されます。指定されている時間に達すると、メッセージが生成されます。

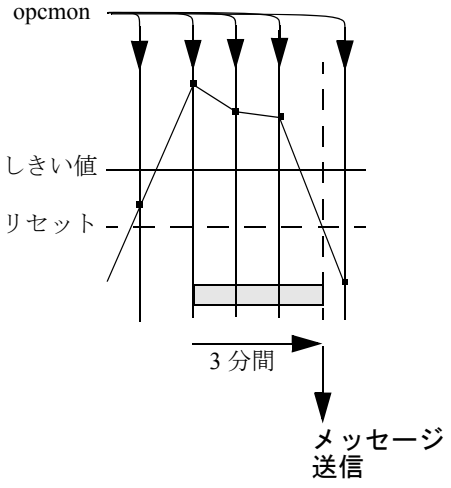
図 4-14　ポーリング周期によるプログラム /MIB オブジェクトのモニター



opcmon による外部オブジェクトのモニター

図 4-15 は、3 分間の間にしきい値に達した、または超過した外部アプリケーションを示します。しきい値に達する、または超過すると、メッセージが送信されます。

図 4-15　opcmon による外部オブジェクトのモニター



パフォーマンスメトリックのモニター

パフォーマンスメトリックは、HP Operations エージェントの一部である組み込みパフォーマンスコンポーネントによって収集されます。組み込みパフォーマンスコンポーネントは、オペレーティングシステムからパフォーマンスカウンターとインスタンスデータを収集します。

収集された値は、独自の持続性データストアに保存されます。そこから取り出された値が変換され、表示値となります。表示値は、HP Reporter や HP Performance Manager など、抽出、視覚化、分析のためのツールで利用できます。データを管理対象ノードから直接抽出、表示、集計することはできません。

HPOM では、組み込みパフォーマンスコンポーネントが収集したパフォーマンスメトリックのしきい値モニターを設定できます。

HP Operations エージェントとその組み込みパフォーマンスコンポーネントがサポートされるプラットフォームの完全なリストについては、『*HPOM 管理サーバーインストールガイド*』を参照してください。

パフォーマンスメトリック

組み込みパフォーマンスコンポーネントが提供するメトリックは次のとおりです。

- **プラットフォーム生成メトリック**

  サポートされるすべてのプラットフォームで利用できるメトリックです。これらのメトリックは、システムのグローバル設定、CPU、ディスク、スワップ、メモリ使用に関するほとんどの疑問に答えることができる基本メトリックです。

- **一般メトリック**

  サポートされる各プラットフォームで利用できる追加メトリックです。これらのメトリックはプラットフォームごとに異なりますが、ほとんどのプラットフォームで利用することができ、通常は、特定システムでのドリルダウンや診断に有用です。

組み込みパフォーマンスコンポーネントで現在利用できるメトリックの詳細については、次の Web ページを参照してください。

- 標準接続 :

  http://<*management_server*>:8081/ITO_DOC/<*lang*>/manuals/EmbedPerfAgent_Metrics.htm

- セキュア接続 :

  https://<*management_server*>:8444/ITO_DOC/<*lang*>/manuals/EmbedPerfAgent_Metrics.htm

この <*management_server*> は管理サーバーの完全修飾ホスト名、<*lang*> はシステム言語 (たとえば、英語環境であれば C) を表します。

パフォーマンスしきい値の設定

組み込みパフォーマンスコンポーネントが収集したデータにアクセスするには、しきい値モニターポリシーを使用します。モニタータイプを Program に設定し、Monitor Program or MIB ID フィールドで次の構文を使用する必要があります

OVPERF\\<*data source*>\\<*object*>\\<*metric*>

この構文では、次のパラメータが使用されています。

<*data source*>

データソースを指定します。組み込みパフォーマンスコンポーネントからのメトリックを収集する場合は、<*data source*> を CODA に設定する必要があります。

<*object*>

モニター対象となるオブジェクトクラスの名前を指定します。

パフォーマンスコンポーネントが収集するオブジェクトクラスは次のとおりです。

- グローバル (オブジェクト名 : GLOBAL)
- CPU (オブジェクト名 : CPU)
- ネットワークインタフェース (オブジェクト名 : NETIF)
- ファイルシステム (オブジェクト名 : FS)
- ディスク (オブジェクト名 : DISK)

<metric>

収集するメトリックを指定します。各オブジェクトクラスで利用できるメトリックのリストについては、次の Web ページを参照してください。

- 標準接続 :

  http://*<management_server>*:8081/ITO_DOC/*<lang>*/manuals/EmbedPerfAgent_Metrics.htm

- セキュア接続 :

  https://*<management_server>*:8444/ITO_DOC/*<lang>*/manuals/EmbedPerfAgent_Metrics.htm

```
ADVMONITOR "Outpacketrate"
DESCRIPTION "Get the global metric GBL_NET_OUT_PACKET_RATE"
INTERVAL "5m"
INSTANCEMODE  SAME
MAXTHRESHOLD
SEVERITY Warning
PROGRAM "Source"
DESCRIPTION ""
MONPROG "OVPERF\\CODA\\GLOBAL\\GBL_NET_OUT_PACKET_RATE"
```

パフォーマンスコンポーネントは、すべてのパフォーマンス生成メトリックと一般メトリックを継続的に収集します。デフォルトの収集間隔は 5 分間で、これを変更することはできません。データはデータストアで 5 週間維持されます。5 週間に収集されたデータでデータベースがいっぱいになると、週に一度、最も古いデータがロールアウトされ、削除されます。

組み込みパフォーマンスコンポーネントのトラブルシューティングについては、『*HPOM システム管理リファレンスガイド*』を参照してください。

組み込みパフォーマンスコンポーネントによるデータ収集の無効化

HP Performance エージェント が収集するメトリックは、組み込みパフォーマンスコンポーネントが収集するメトリックのスーパーセットです。このため、同じノードで OVPA を使用している場合は、組み込みパフォーマンスコンポーネントによるメトリックの収集を無効にしたほうが有利です。

データ収集を無効にしても coda プロセスは実行を続け、HPOM に制御が残ります。その後、これは OVPA のデータ通信層として機能します。

OVPA 4.5 がインストールされている HTTPS ベースの管理対象ノード上で組み込みパフォーマンスコンポーネントによるデータ収集を無効にするには、次のコマンドを実行します。

```
ovconfchg -ns coda -set DISABLE_PROSPECTOR false
```

データ収集を有効に戻す場合は、パラメータ DISABLE_PROSPECTOR を true に設定します。

モニターの対象となる変数の選択

どの変数をモニターするかは、環境、現在使用しているモニター、収集するパラメータによって異なります。既存のモニタープログラムやカスタムモニタープログラムを統合できます。また、既存のモニターを見直し、重要な環境変数を調べた上で、モニターの対象となる変数を決定することもできます。

たとえば、次の事項を確認します。

- ❏ 現在使用しているモニター
- ❏ 毎日、毎週、毎月利用しているモニター
- ❏ 自分で作成したカスタムモニター
- ❏ 環境内のオペレーティングシステムまたはアプリケーションが使用しているモニター

また、モニターしなければならないパラメータについても確認してください。

たとえば、次の事項を確認します。

- ❏ モニター可能なパラメータ
- ❏ 重要なパラメータ
- ❏ しきい値を適用できるパラメータ
- ❏ 制限値を超過する前に警告を出さなければならないパラメータ

しきい値タイプの選択

モニターの下限 / 上限しきい値を設定できます。

- ❏ **下限しきい値**

  モニター値が許容下限値に達する、またはそれを下回ると、メッセージが生成されます。たとえば、`df` モニター (空きディスクブロック) の下限しきい値を利用できます。空きディスクブロックの数が定義したしきい値を下回ると、HPOM はメッセージを生成します。

- ❏ **上限しきい値**

  モニター値が許容上限値に達する、またはそれを超過すると、メッセージが生成されます。たとえば、`who` モニター (ユーザー数) の上限しきい値を利用できます。ユーザーの数が定義したしきい値を超過すると、HPOM はメッセージを生成します。

メッセージ生成ポリシーの選択

しきい値モニターでは、次の 3 つのメッセージ生成ポリシーを利用できます。

- ❏ リセットありのメッセージ生成
- ❏ リセットなしのメッセージ生成
- ❏ 継続的なメッセージ生成

注記

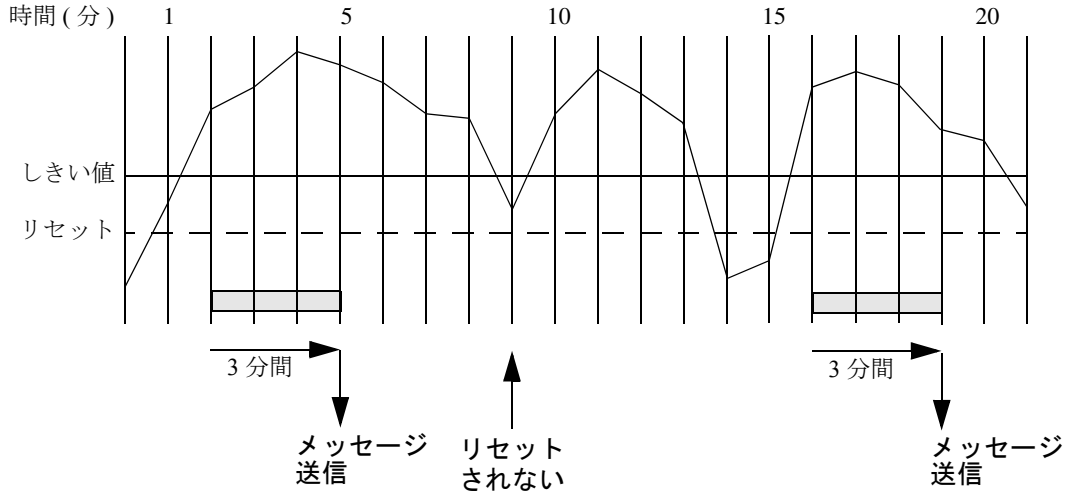
いずれを選択した場合も、ポーリング時にモニター対象オブジェクトの値がしきい値に達する、または超過する (下回る) 場合は、HPOM はしきい値違反を認識します。

次の例は、各設定の違いを表しています。すべての例において、ポーリング周期は 1 分間、指定時間は 3 分間です。

リセットありのメッセージ生成

図 4-16 は、リセットありのメッセージ生成を示しています。2 回目のポーリング (2 分) の値がしきい値を超過しているため、タイマーが起動されます。その 3 分後、値は依然としてしきい値を上回っており、メッセージが送信されます。値がリセットレベルを下回ると、次回のしきい値違反時にタイマーがリセットされ、サイクルが再開されます。

図 4-16　リセットありのメッセージ生成

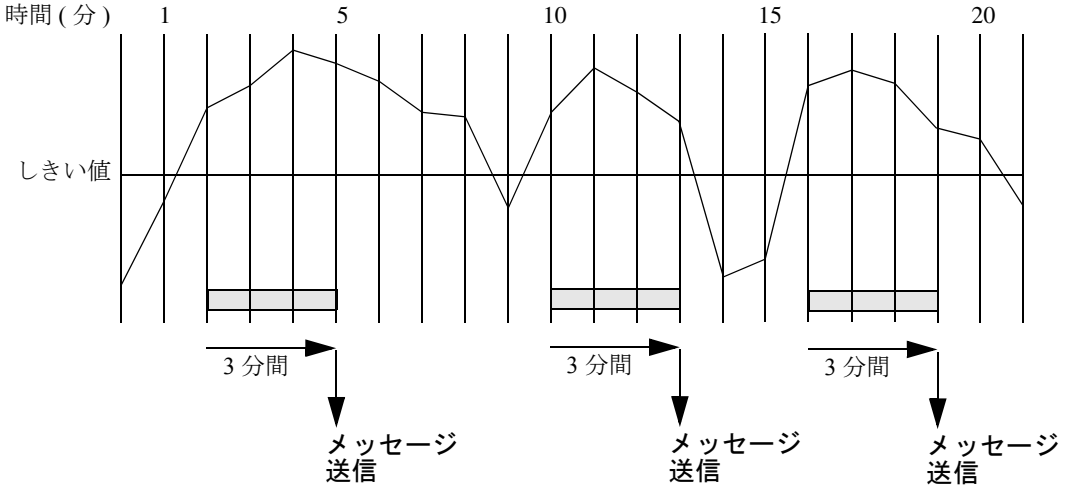


リセットなしのメッセージ生成

リセットなしのメッセージ生成では、特定のリセット値は適用されません。リセット値はしきい値と同じになります。

図 4-17 は、リセットなしのメッセージ生成を示しています。2 回目のポーリング (2 分) の値がしきい値を超過しているため、タイマーが起動されます。その 3 分後、値は依然としてしきい値に違反しており、メッセージが送信されます。値がしきい値を下回ると、次回のしきい値違反時にタイマーがリセットされ、サイクルが再開されます。

図 4-17　リセットなしのメッセージ生成

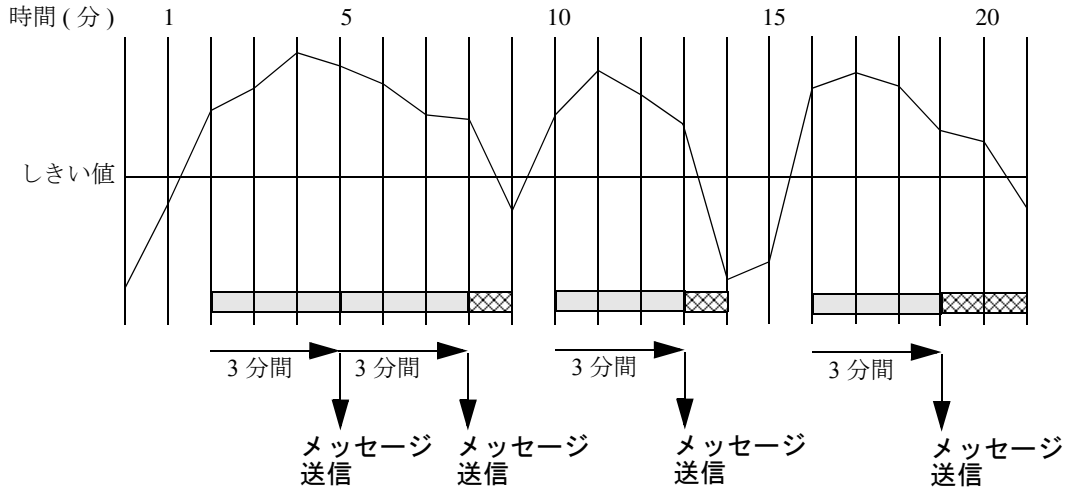


継続的なメッセージ生成

図 4-18 は、継続的なメッセージ生成の例を示しています。2 回目のポーリング (2 分) の値がしきい値を超過しているため、タイマーが起動されます。その 3 分後にメッセージが送信され、タイマーは直ちにリセットされます。

値がしきい値と同じ値になる、または下回るまで、これが繰り返されます。モニター値がしきい値を再び超過すると、タイマーが起動され、サイクルが再開されます。

図 4-18　継続的なメッセージ生成



短時間のピーク

わずかな間だけしきい値を超過しただけでメッセージを生成するのは好ましくない場合もあるため、HP Operations では、メッセージを生成する前にモニター値がしきい値を超過していなければならない最短時間を定義できます。メッセージが送信されるには、指定した最短時間中に測定される値が毎回しきい値を超過している必要があります。値は、ポリシーポーリング周期の倍数で指定してください。

たとえば、ポリシー周期が 2 分間であれば、短時間ピークの最短時間を 2 分間、4 分間、6 分間、8 分間、10 分間などに設定します。最短時間を 0 に設定する、または値を指定しない場合は、HP Operations によってしきい値違反が検出されると、直ちにアラームが生成されます。

しきい値モニターの統合

ログファイルを定義するような方法で、ポリシーを使ってしきい値モニターを定義することができます。新しいモニターを作成することも、既存のモニターを修正 / コピーすることもできます。

新しいしきい値モニターの統合

新しいしきい値モニターを統合する手順は次のとおりです。

1. **配布するしきい値モニターデータを用意します。**

   配布する予定のインストルメンテーションデータは、HP Operations 管理サーバーの次の場所にある**インストルメンテーション**ディレクトリに配置されます。

   ```
   /var/opt/OV/share/databases/OpC/mgd_node/
   ```

注記

カテゴリが作成されていない場合は、モニターディレクトリからのデータが何らかの方法で配布されます。カテゴリベースの配布方法をお勧めしますが、このディレクトリからモニターを配布することもできます。この場合、管理サーバー上の、モニターの配布先となる各管理対象ノードのプラットフォームに固有のディレクトリにモニターを配置する必要があります。たとえば、HP-UX 11i 管理対象ノード用のモニタープログラム / スクリプトは、管理サーバー上の次の場所に配置します。

```
/var/opt/OV/share/databases/OpC/mgd_node/customer/hp/\
ipf32/hpux1100/monitor
```

すべての配布方法、それに関連する管理タスク (カテゴリ管理を含む)、インストルメンテーションデータディレクトリの構造については、『*HPOM システム管理リファレンスガイド*』を参照してください。

   a. **インストルメンテーション**ディレクトリで、データに関連するカテゴリにモニタープログラム / スクリプトを適切に (データの配布先となる管理対象ノードのプラットフォームごとに) 配置します。このようなカテゴリが存在しない場合は作成し、ポリシー、管理対象ノード、または両方に割り当てることができます。

2. **しきい値モニターを管理対象ノードに配布します。**

   これを実行するには、コマンド行ユーティリティ opcragt を使用します (使用方法については *opcragt.1M* のマニュアルページを参照)。

   HPOM 管理対象ノードでは、配布されるすべてのインストルメンテーションデータ (カテゴリベースのインストルメンテーションファイル、および monitor|actions|cmds ファイル) は次のディレクトリに配置されます。

   /var/opt/OV/bin/instrumentation

3. **しきい値モニターポリシーを設定します。**

   コマンド行ツール opcpolicy を使用して、しきい値モニターポリシーをアップロードします。しきい値ポリシーの本文の構文については 369 ページの付録 A「ポリシー本文の構文」を参照してください。各ポリシーはモニター (しきい値違反が検出された場合に開始される自動 / オペレータ起動アクションを含む) を定義します。

注記

カテゴリベースの方法でしきい値モニターを配布する場合は、ポリシーに適切なカテゴリが割り当てられていることを確認してください。

4. **しきい値モニターポリシーの条件を設定します。**

   ポリシー本文の MSGCONDITIONS セクションは、条件と一致した場合に Java GUI メッセージブラウザに送信されるメッセージを生成するかどうかを決定します。SUPPRESSCONDITIONS セクションの設定でメッセージをさらにフィルタリングすることもできます。ポリシー本文の構文については 369 ページの付録 A「ポリシー本文の構文」を参照してください。

注記

モニターに複数の条件を適用する場合は、条件の順序が重要になります。

しきい値のサイズに基づいて条件を並べ替えてください。

- **上限しきい値タイプ**

  しきい値が最も大きい条件を最初に配置し、しきい値が最も小さい条件を最後に配置します。

- **下限しきい値タイプ**

  しきい値が最も小さい条件を最初に配置し、しきい値が最も大きい条件を最後に配置します。

条件を並べ替えることで、状態ベースのブラウザ設定が、同一モニターからの直前のメッセージを自動的に受諾できるようになります。状態ベースのブラウザについては 236 ページの「状態ベースのブラウザ」を参照してください。

しきい値モニターの設定

ADVMONITOR ポリシーのポリシー本文を編集することで、しきい値モニターポリシーを設定できます。ポリシー本文の構文については 369 ページの付録 A「ポリシー本文の構文」を参照してください。

例 4-2 しきい値モニターポリシーの本文の例

この例では、ユーザーはファイルシステムの使用率を計算するためのカスタムスクリプト fs_util_mon.sh を実行しています。このスクリプトは、コマンド行ツール opcmon を使用して計算結果を extra_util というモニターエージェントに渡します (スクリプトへのパラメータとして渡されます)。

ファイルシステムの使用率が指定の使用率 (THRESHOLD) を上回っている場合 (MAXTHRESHOLD)、モニターエージェントはメッセージを生成します。ただし、使用率がキーワード RESET によって設定される値を下回るまでは、メッセージは再送信されません。すべてのメッセージの重要度は**注意域**、アプリケーションフィールドは「Filesystem」、オブジェクトは「/extra」、メッセージグループは「Disks」に設定されます。設定されている条件との一致によって送信されるメッセージ以外のメッセージは管理サーバーに送信されません。

```
ADVMONITOR "extra_util"
                DESCRIPTION "Monitor /extra filesystem utilization"
                INTERVAL "5m"
                INSTANCEMODE SAME
                MAXTHRESHOLD
                SEVERITY Warning

                PROGRAM "Source"
                                DESCRIPTION "Universal FS usage
                                monitoring script"
                                MONPROG "fs_util_mon.sh /extra
                                extra_util"

                MSGCONDITIONS
                                DESCRIPTION "Monitor /extra FS util"
                                CONDITION

                                THRESHOLD 85.00
                                                RESET 80.00
                                                SETSTART

                                SEVERITY Warning
                                                APPLICATION
                                                "Filesystem"
                                                MSGGRP "Disks"
                                                OBJECT "/extra"
                                                TEXT "Filesystem
                                                /extra utilization
                                                <$VALUE> exceeds
                                                configured threshold
                                                <$THRESHOLD>"
                                                AUTOACTION "du Dk
                                                /extra" ANNOTATE
```

デフォルトしきい値モニター

HPOM にはデフォルトのしきい値モニターが用意されています。詳細については、『*HPOM HTTPS エージェントコンセプトと設定ガイド*』を参照してください。

高度なモニターのための条件を設定するには

しきい値モニターポリシーの条件を設定することで、1 つのモニター対象オブジェクトの複数のインスタンスをモニターできます。

しきい値モニターの条件を設定する手順は次のとおりです。

1. `-object` オプションを指定したコマンド行ユーティリティ `opcmon(1)` を使用して、モニター対象オブジェクトの名前をモニターエージェントに送信します。

   `-option` オプションは、モニターエージェントに追加情報を渡します。この情報は、メッセージテキストで使用したり、修復アクションで参照できます。

   HPOM は、この値と、高度なモニターポリシーの本文にキーワード `OBJECT` によって設定されているパターンを比較します。

2. 受信オブジェクトパターンの照合には、HPOM のパターンマッチ言語を使用します。

   詳細については *opcmon(1)* のマニュアルページを参照してください。

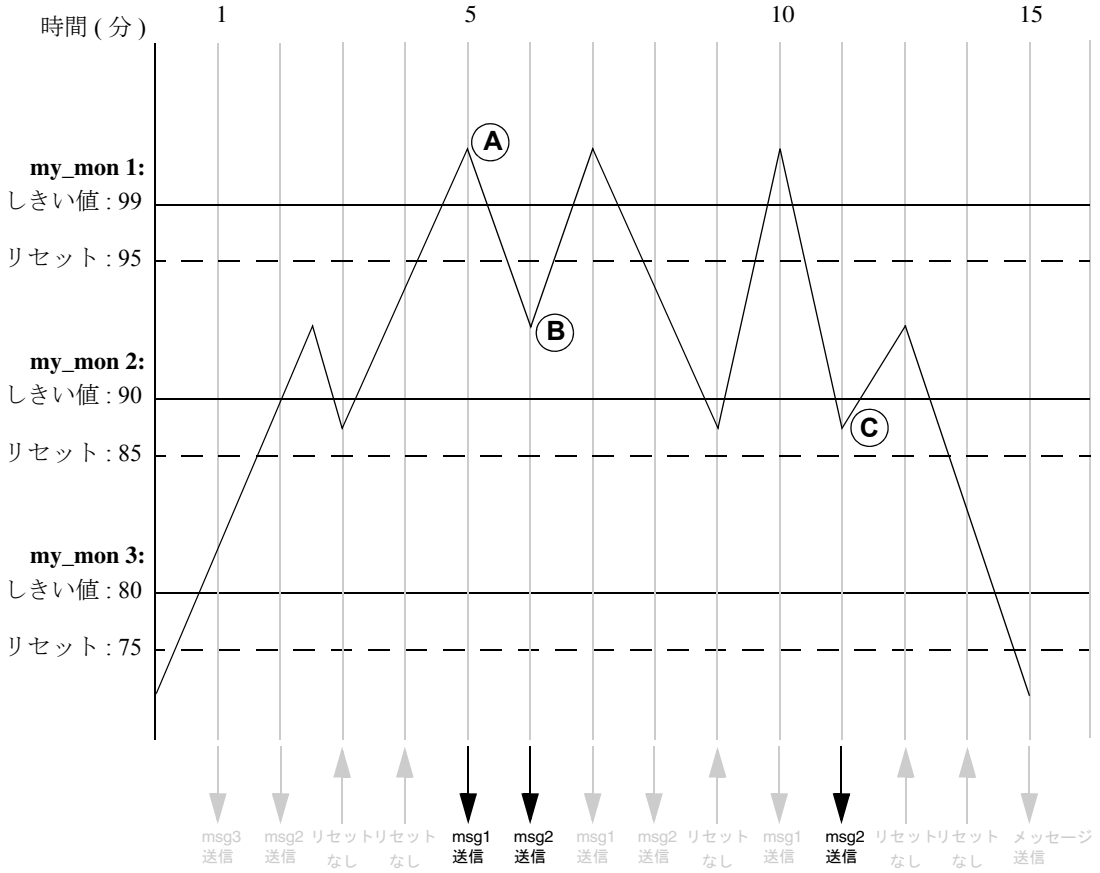
異なるファイルシステムのディスク使用率をモニターする方法を示す例については 280 ページの「しきい値モニター条件の例」を参照してください。

複数の条件によるしきい値モニター

1 つのモニター対象オブジェクトの、しきい値 / リセット値が異なる複数の条件を 1 つのポリシーに設定した場合、別の条件のモニター範囲に達するたびにメッセージが生成されます。

279 ページの図 4-19 の例を考えてください。この図は、それぞれが上限しきい値とリセット値を持つ 3 つの条件を示しています。

図 4-19　リセット値を持つ複数の条件によるメッセージの生成



5 回目のポーリング (5 分) の値が条件 my_mon 1 (しきい値 = 99) のしきい値を超過しており、メッセージが送信されます **(A)**。その 1 分後、値は条件 my_mon 1 (リセット値 = 95) のリセット値を下回ります。この値は条件 my_mon 2 (しきい値 = 90) のしきい値を超過しているため、別のメッセージが送信されます **(B)**。

つまり、値は条件のリセット値を下回っていませんが、その条件のモニター範囲に達していればメッセージが生成されます。

その 5 分後 (開始から 11 分後)、値は条件 my_mon 2 (しきい値 = 90) のしきい値を下回りますが、引き続きリセット値の 85 を上回っています。これにより、別のメッセージが生成されます **(C)**。しきい値は下回ったものの、リセット値には達しなかったため、このメッセージの元のメッセージテキストには「Reset value still exceeded (リセット値は現在も超過中)」と出力されます。このメッセージは、モニター値がしきい値を下回った場合にのみ生成されます。モニター値がしきい値を超過する場合は、リセット値も超過しており、メッセージは生成されません。

この例では、同じモニター対象オブジェクトについて多数のメッセージが生成されます。ブラウザに表示されるメッセージの数を減らすには、メッセージが自動的に受諾されるように条件を設定します。詳細については 236 ページの「状態ベースのブラウザ」を参照してください。

しきい値モニター条件の例

次の例は、しきい値モニター条件を適用し、しきい値モニターポリシー disk_util を使ってシステム /var および /file のディスク容量をモニターする方法を示しています。これらの例は、各ファイルシステムのディスク使用率を調べて報告するシェルスクリプトが事前に作成されていることを前提としています。

メッセージ条件 1

オブジェクトパターン : /var

しきい値 : 90

リセット : 85

指定時間 : 3

属性の設定 :

重要度 : **注意域**

メッセージグループ : OS

テキスト : **ファイルシステム** /var **の使用率** (<$VALUE>) **は** (<$THRESHOLD>)% **を超えています。**

メッセージ条件 2

オブジェクトパターン : ^/

しきい値 : 95

リセット : 90

指定時間 : 3

属性の設定 :

重要度 : **危険域**

メッセージグループ : OS

テキスト : **ルートファイルシステムの使用率** (<$VALUE>) **は** (<$THRESHOLD>)% **を超えています。**

SNMP トラップとイベント

HPOM イベントインターセプタ (opctrapi) は、HPOM に SNMP トラップを供給するメッセージインタフェースです。

トラップとイベントの捕捉に関するデフォルト設定

デフォルトでは、HPOM は SNMP トラップと CMIP (Common Management Information Protocol) イベントを次のように捕捉します。

- **アプリケーションから**

  HP Operations 管理サーバーで実行されている opctrapi デーモンにトラップを送信するすべてのアプリケーションから。

- **管理対象ノードで**

  トラップデーモン (ovtrapd) が実行されているすべての管理対象ノードで。

- **管理対象ノードのプラットフォームで**

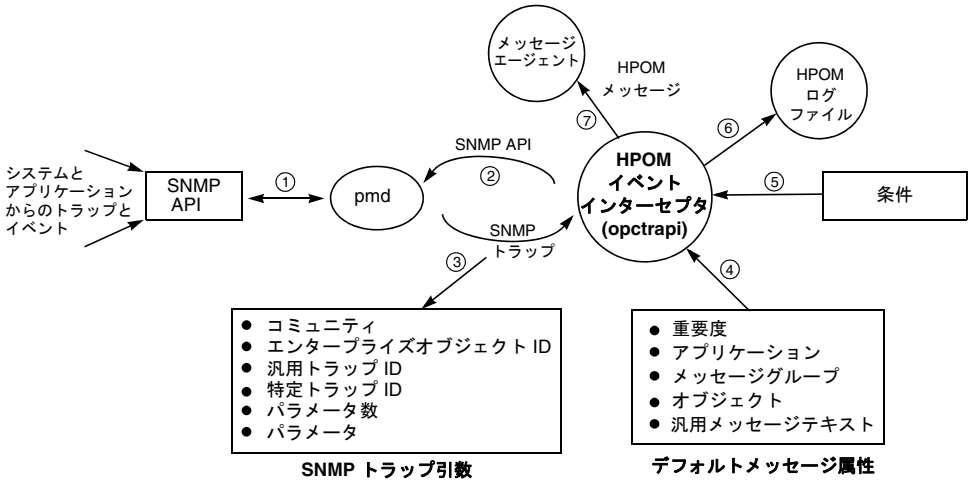
  選択している管理対象ノードプラットフォーム上の直接ポートアクセスモードで。opctrapi が対応している管理対象ノードプラットフォームのリストについては、『*HPOM システム管理リファレンスガイド*』を参照してください。

  管理対象ノード上でイベントを直接捕捉することで、メッセージをローカルに処理し、パフォーマンスを向上させることができます。たとえば、自動アクションを開始し、管理サーバーに転送する代わりにノード上またはサブネットで直接実行できます。

ブラウザウィンドウでの SNMP イベントの捕捉

図 4-20 は、HPOM イベントインターセプタがどのように SNMP イベントを収集、フィルタリング、フォーマット変更し、ブラウザウィンドウに表示するかを示しています。

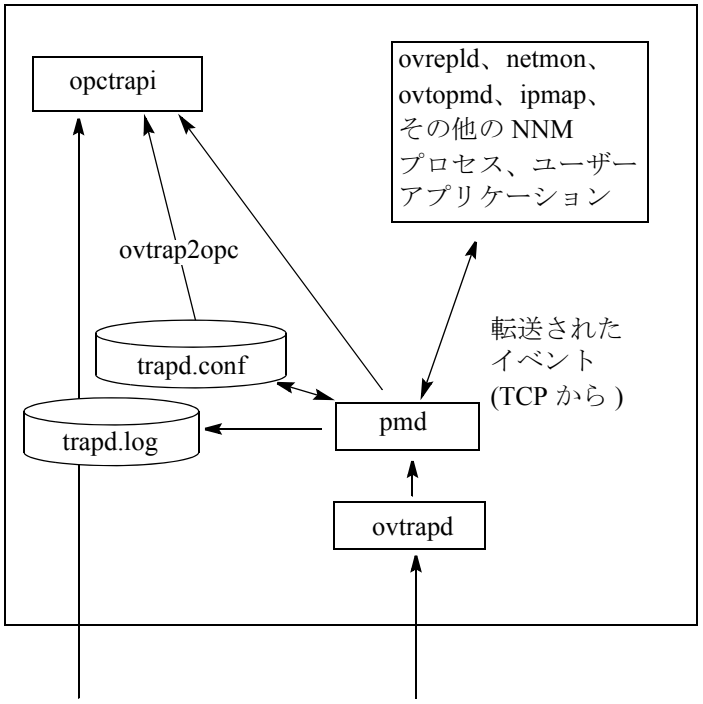
図 4-20　NNM がインストールされている場合の SNMP イベントインターセプタ



SNMP トラップと CMIP イベントの転送

図 4-21 は、opctrapi と、SNMP トラップおよび CMIP イベントを HPOM に転送する HP プロセスの関係を示しています。

図 4-21　HPOM の SNMP イベントシステム



SNMP v1 トラップと通知リクエスト (ポート 162 の UDP から)

バックグラウンドプロセス ovtrapd は、ポート 162 で SNMP トラップと CMIP イベントを受信して バッファに入れ、ポストマスタプロセス (pmd) に渡します。pmd プロセスは ovtrapd から受け取ったイベントをサブシステム (たとえば、opctrapi、または trapd.conf ファイル) にルーティングし、その上で HPOM メッセージストリームに入れます。

trapd.conf には、SNMP エージェントによって生成されたトラップと、pmd に登録されているアプリケーションによって生成されたイベントの処理方法が定義されています。これらの定義は、ovtrap2opc ユーティリティを使って HPOM メッセージや除外条件に変換できます。詳細については *ovtrap2opc(1M)* のマニュアルページを参照してください。

一部の管理対象ノードプラットフォームでは、HPOM イベントインターセプタはポート 162 に直接アクセスして SNMP トラップをキャプチャできます。詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

重複メッセージの回避

SNMP デバイスは、HP 検出プロセスによって管理サーバーにトラップを送信するように設定されますが、SNMP デバイスがトラップを複数のシステムにブロードキャストすることもあります。この場合、複数の管理対象ノードから 1 つの管理サーバーにトラップが転送されると、SNMP デバイスは重複したメッセージを生成します。

このような状況が生じないように、次のガイドラインに従ってください。

- **1 つの SNMP 送信先、または 1 つの NNM 収集ステーション**

  SNMP デバイスの SNMP 送信先を 1 つに制限します。または、管理サーバーの NNM 収集ステーションとして機能するシステムを 1 つに制限します (可能であれば、最も高速のネットワークに接続された収集ステーションを利用してください)。

  HP-UX ノード上の SNMP デバイスの送信先システムは、次のファイルに設定されます。

  `/etc/SnmpAgent.d/snmpd.conf`

  システムの設定には次の文が使用されます。

  `trap_dest:<`*ノード名*`>`

注記

NNM は、HP Operations 管理サーバーと同じシステムにはインストールできません。

- **すべての NNM 収集ステーションに HP Operations エージェント**

  すべての NNM 収集ステーションで HP Operations エージェントを (つまり、HPOM イベントインターセプタも) 実行します。

SNMP トラップポリシーの追加

SNMP トラップポリシーを追加するときは、HP Operations 管理サーバー、または HPOM イベントインターセプタがサポートされる管理対象ノードに任意の数のトラップポリシーを割り当てることができます。

SNMP ポリシーのポリシー本文を編集することで、トラップポリシーを設定できます。ポリシー本文の構文については 369 ページの付録 A「ポリシー本文の構文」を参照してください。

例 4-3 トラップインターセプタポリシーの本文の例

この例は、Cisco 社のルーターによって生成される Cisco linkDown トラップ (.1.3.6.1.4.1.9.2.0) を捕捉します。トラップが捕捉されると、重要度が**注意域**に設定されたメッセージが生成されます。エンタープライズトラップと汎用トラップが分かれていることに注意してください。変数 <$1>、<$2> はトラップの一部です (それぞれ、リンクインデックスと説明)。

```
SNMP "Sample trap interceptor template"

                DESCRIPTION "This is catches Cisco linkDown trap"

                CONDITION

                                $G 2
                                $e ".1.3.6.1.4.1.9"

                SET

                                MSGTYPE "Cisco_Link_Down"
                                SEVERITY "Warning"
                                OBJECT "<$2>"
                                TEXT "Interface <$1> down"
```

SNMP トラップ条件の例

バックアップが開始され、作業リストファイルで構文エラーが検出されると、HP Data Protector は次の SNMP トラップを出力します。

```
snmptrap idriss1 1.3.6.1.4.11.2.3.2 15.232.
117.22 58916871  6 \
1.3.6.1.4.11.2.15.2.0 Integer 1 \
1.3.2.1.4.11.2.15.3.0 OctetString doghouse.bbn.hp.com \
1.3.2.1.4.11.2.15.4.0 OctetString
”HP Data Protector:[Error](Worklist Syntax)Can’t open
worklist ‘/etc/omni/work’ Status:Critical” \
1.3.2.1.4.11.2.15.5.0 OctetString ”Critical”  \
1.3.2.1.4.11.2.15.6.0 OctetString ”dp”
```

SNMP トラップポリシーには、次の定義による条件が必要です。

ノード

doghouse

エンタープライズ ID

1.3.6.1.4.11.2.3.2

汎用トラップ ID

6

特定トラップ ID

58916871 (SNMP ステータスイベント)

変数のバインディング

アプリケーションタイプ : 1 （**エージェント**）

オブジェクト ID:

mailhouse.bbn.hp.com.omniback

イベントの説明 :

HP Data Protector:
[**エラー**] (**作業リストの構文**) **作業リスト「**/etc/omniback/work**」を開くことができません ステータス : 危険域**

トラップ固有のデータ :

危険域

属性の設定 :

重要度 :

危険域

メッセージグループ :

印刷サービス

テキスト :

`HP Data Protector` **のエラー :**
`<text>`

HPOM の内部エラーメッセージのフィルタリング

内部メッセージストリームインタフェース (MSI) から HPOM の内部エラーメッセージを抽出したり、フィルタリングすることができます。これにより、自動 / オペレータ起動アクションを添付したり、表示可能な通常の HPOM メッセージとして扱うことができます。この機能は、管理対象ノードと管理サーバーで有効にできます。HPOM のすべてのメッセージは、この機能をどこで有効にするかに応じて HP Operations 管理サーバーまたは管理対象ノード上のローカルメッセージインターセプタに戻されます。インターセプタでは、これらのメッセージはその他の HPOM メッセージと同様に読み取られ、処理されます。

管理サーバー

管理サーバーでは、コマンド行ツール ovconfchg を使用します。次のように入力します。

```
ovconfchg -ovrg <OV_resource_group> -ns opc -set \
OPC_INT_MSG_FLT TRUE
```

このコマンドの *<OV_resource_group>* は、管理サーバーリソースグループの名前です。

管理対象ノード

HTTPS ベースの管理対象ノードでは、コマンド行ツール ovconfchg を使用します。次のように入力します。

```
ovconfchg -ns eaagt -set OPC_INT_MSG_FLT TRUE
```

opcmsg (1/3) ポリシーには、HPOM の内部エラーメッセージ用に少なくとも 1 つの条件を設定してください (OpC を使用します)。その上で、ポリシー本文にキーワード SUPP_DUPL_IDENT_OUTPUT_MSG を設定します。

HPOM でのイベント相関処理

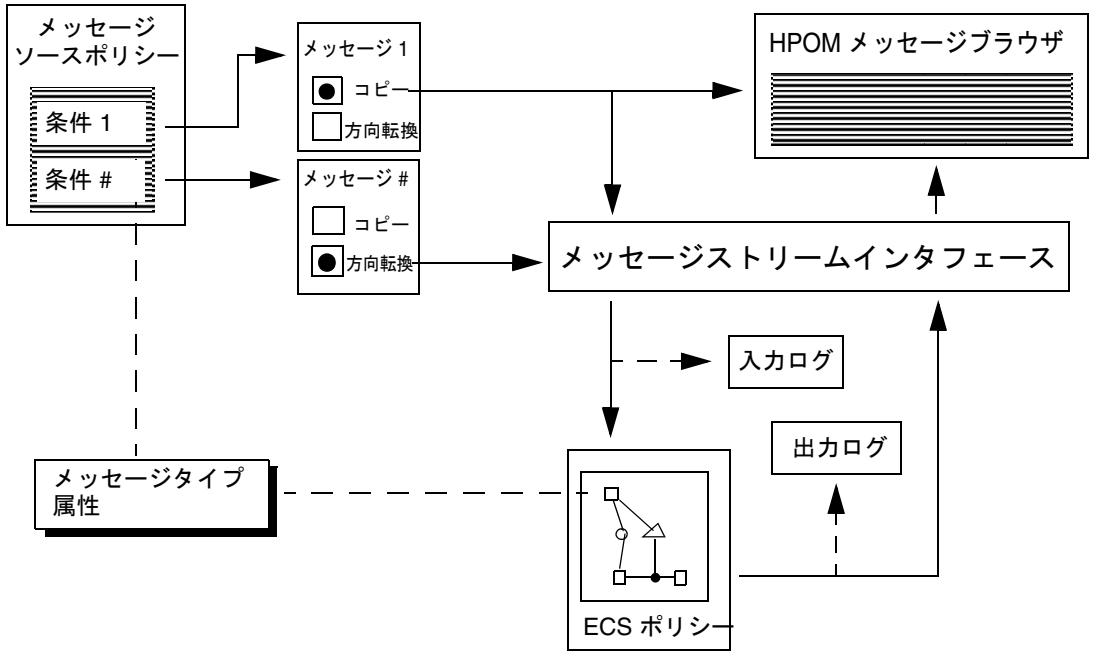
一般に、通常の HPOM メッセージソースポリシーに定義されている条件によって生成されるメッセージは HPOM イベント相関処理 (EC) ポリシーへの入力として使用されます。イベント相関処理ポリシーは、これらの HPOM メッセージを処理し、必要に応じて Java GUI メッセージブラウザに表示するメッセージを新たに生成します。

HPOM では、相関処理サーキットはポリシーと見なされ、ポリシーとして扱われます。HPOM には、相関処理ポリシーのデフォルトセットが用意されており、その他の HPOM ポリシーと同様に割り当て、配布、使用することができます。これらのデフォルトのイベント相関処理ポリシーをサンプルとして利用し、特定の環境のニーズに合わせてカスタマイズできます。ただし、ECS サーキットを修正するには、新しい ECS サーキットを作成 / 修正するための ECS Designer GUI を使用する必要があります。

イベント相関処理の仕組み

291 ページの図 4-22 は、イベント相関処理ポリシーが HPOM でどのように機能するかを示しています。HPOM メッセージソースポリシーにより、どの条件でメッセージが生成されるかを指定できます。また、生成されたメッセージをメッセージストリームインタフェース (MSI) にコピーするか、方向転換するかも指定できます。MSI の後は、生成されたメッセージをイベント相対処理ポリシーに渡して処理できます。HPOM では、メッセージを相関処理エンジンに方向転換するのではなく、コピーできます。このため、相関処理の最中に重要なメッセージに遅延が生じたり、失われることはありません。この機能は、トラブルシューティングの際に特に便利です。

図 4-22　　HPOM での論理イベント相関処理のフロー



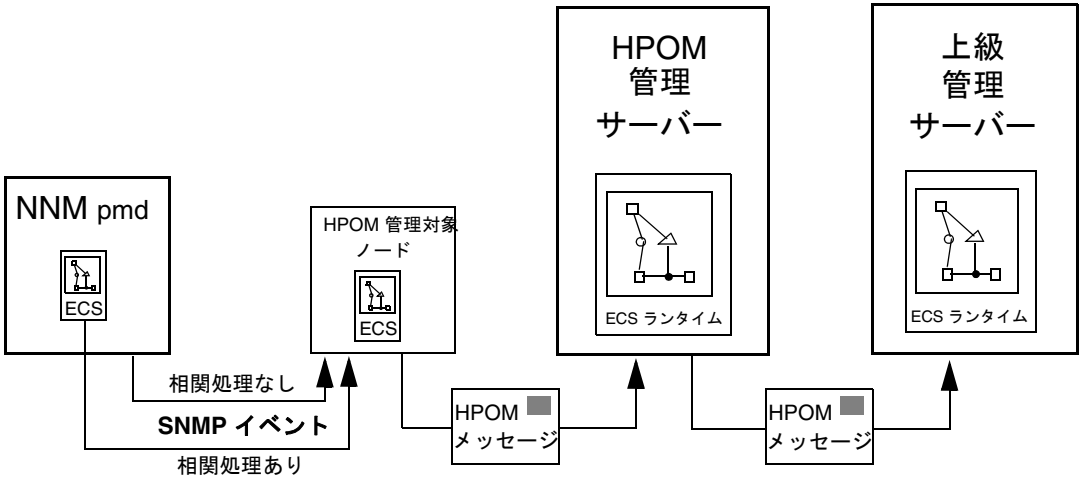
イベント相関処理ポリシーは、メッセージが送られるイベント相関処理サーキットを決定します。これは、メッセージ条件に指定されている**メッセージタイプ**属性と、イベント相関処理サーキットの**入力**ノード (ポート) の `Event-type` フィールドに指定されているメッセージ属性を照合することで行われます。

HPOM でのイベント相関処理の設定方法の詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。イベント相関処理ポリシーの作成 / 修正の詳細については、ECS Designer 製品に付属するドキュメントを参照してください。

メッセージの相関処理を行う場所

HPOM 環境内で相関処理を行う場所のメリットとデメリットを考慮することが重要です。標準的な環境では、管理対象ノード、管理サーバー、またはその両方でメッセージの相関処理を行うことができます。ただし、HPOM のフレキシブル管理構成を採用している大規模な環境では、選択肢はさらに広がります。このような環境では、管理サーバーの複数の層が階層的に構成されており、各種レベルの管理サーバー間の関係を考慮する必要があります。相関処理を NNM ドメインに設定することもできます。この場合は、HPOM イベントインターセプタが捕捉する SNMP 関連メッセージの数が大幅に減少します。相関処理の各種アプローチについては、図 4-24 を参照してください。

図 4-23　　HPOM での相関処理の設定



一般に、相関処理をできるだけ早い段階で行うほどダウンストリームの負荷が減り、メッセージブラウザに到達するメッセージも少なくなるので、パフォーマンスの面で有利です。管理サーバーまたは管理対象ノードにイベント相関処理ポリシーを割り当て、配布する前に、相関処理を行う場所を検討する必要があります。

- **管理対象ノードに到達する前**

  HPOM に到達する前に NNM の相関処理サーキットを使ってイベントの相関処理を行うことで、HPOM が捕捉するイベントの数を大幅に減らすことができます。

- **管理対象ノード上**

  管理対象ノード上でメッセージの相関処理を行うことで、管理サーバーに渡されるメッセージの数を減らすことができます。これにより、管理サーバーの負荷と、ネットワークトラフィックの使用量の両方を削減できます。

- **管理サーバー上**

  HP Operations 管理サーバー上でメッセージの相関処理を行うことで、異なる管理対象ノードから受信する、類似した、または関連するメッセージをフィルタリングできます。

- **フレキシブル管理環境内で**

  HPOM 環境内の管理対象ノードと管理サーバーの関係は、管理階層内の管理サーバー間の関係にまで拡張できます。

ソースが異なるメッセージの相関処理

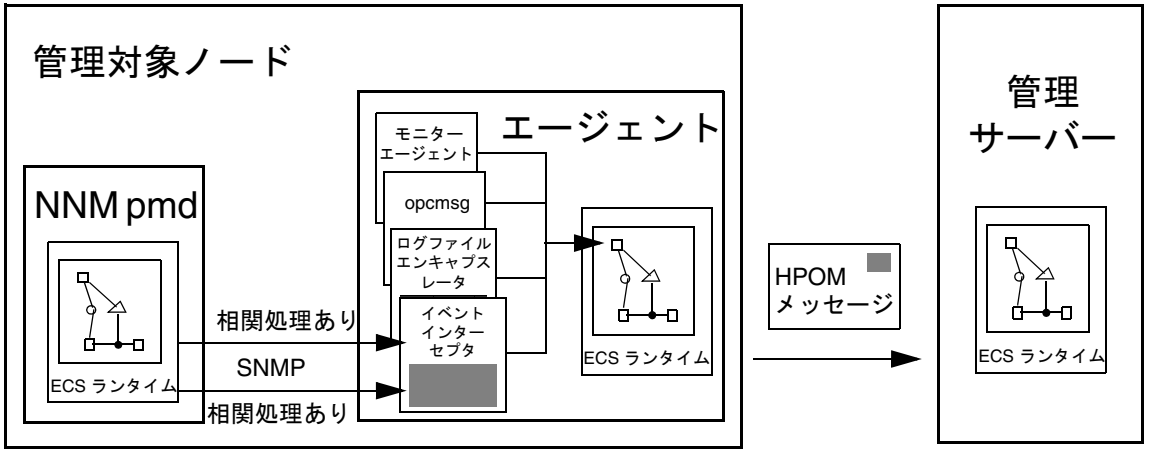
相関処理は、個々のソースに制限する必要はありません。HPOM 内の異なるソースからのメッセージを相関処理することには、数多くのメリットがあります。

次のソースからのメッセージの相関処理を行うことができます。

- SNMP トラップ
- `opcmsg`
- ログファイル
- モニターエージェント

たとえば、SNMP によって生成される、ダウン中のノードに関連するメッセージと、到達不能サーバーに関連するログファイルエントリによって生成されるメッセージを相関させることができます。

図 4-24　　ソースが異なるイベントの相関処理



HPOM イベントインターセプタ

HPOM イベントインターセプタは、NNM と HPOM を結ぶリンクです。HPOM イベントインターセプタは、NNM ポストマスターデーモン (pmd) によって生成される、相関処理された SNMP イベントと、相関処理されていない SNMP イベントの両方のストリームを捕捉し、必要に応じて HPOM メッセージを生成します。生成されたメッセージは、ログファイルなど、その他の HPOM ソースによって生成されたメッセージと共に HP Operations エージェントのイベント相関処理ポリシーによって処理されます。

HPOM に到達する前の NNM でのイベント相関処理

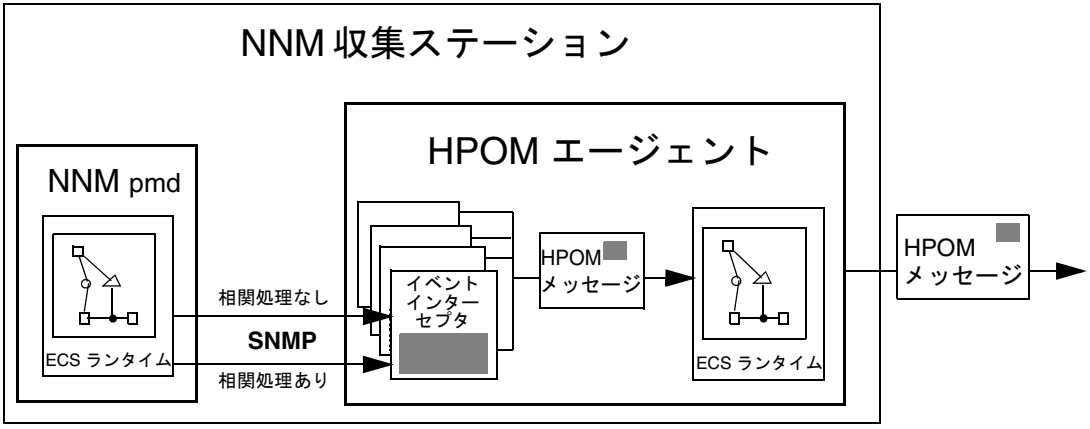
HP Operations の全体的な負荷を減らし、HPOM が相関処理を実行しやすくするには、イベントが HPOM に到達する前に NNM の相関処理サーキットを使って相関処理を行います。

たとえば、ルーターが応答しない場合に生成されるイベントの相関処理を行うように NNM のサーキットを設定できます。NNM 収集ステーション上の HPOM イベントインターセプタが相関処理済みのイベントのみを受信するようにすることで、生成される HPOM メッセージの数を大幅に削減できます。これらのメッセージは、HPOM 管理対象ノードのイベント相関処理ポリシーによってさらに処理できます。

HPOM と NNM のイベント相関処理の同期

NNM と HPOM のイベント相関処理は同期され、NNM で破棄されたイベントは HPOM でも除外されます。同様に、NNM のサーキットが受諾または削除したイベントは、自動的に HPOM によって受諾されます。さらに、相関処理された (つまり、除外された) イベントに関連付けられている各メッセージには自動注釈が追加されます。この機能は、SNMP トラップポリシー `SNMP ECS Traps` の条件に含まれています。

図 4-25　　NNM での相関処理

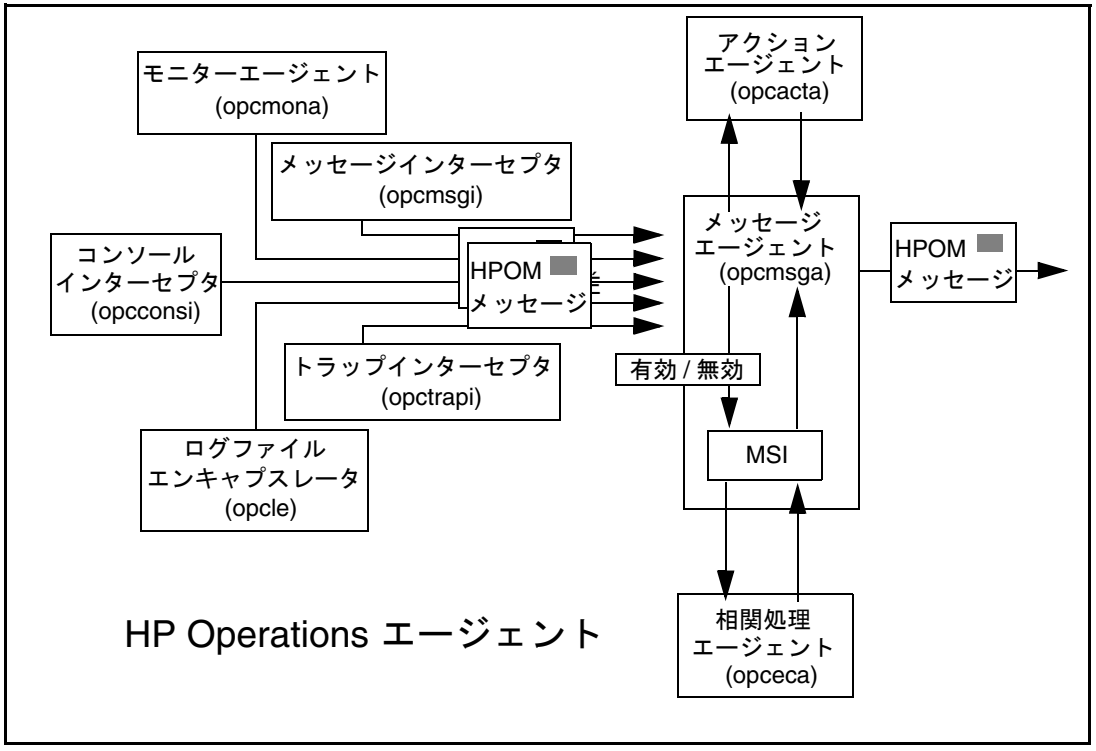


管理対象ノードでのメッセージの相関処理

HP Operations エージェントを使って管理対象ノード上でイベントの相関処理を行うことで、エージェントとサーバーの間のネットワークトラフィックを大幅に削減できます。ネットワークトラフィックは、イベント相関処理エージェントが実行されているすべての管理対象ノードで削減されます。管理サーバーの CPU の負荷が低下するため、その他の障害により効率的に対応できるようになります。

296 ページの図 4-26 は、管理対象ノードでメッセージがどのように生成、処理されるか、およびエージェント MSI へのメッセージ出力を有効 / 無効にすることで、イベント相関処理エージェント (opceca) へのメッセージのフローをどのように制御できるかを示しています。

図 4-26　　HPOM 管理対象ノード上のメッセージのフロー



opceca プロセスはエージェント MSI に接続し、HPOM エージェントメッセージストリームからのメッセージへのアクセスを有効にします。メッセージの相関処理が行われ、HPOM メッセージエージェントに戻されます。opceca によって作成 / 変更されたメッセージは、MSI:opceca というメッセージソースでメッセージブラウザに表示されます。相関処理サーキットに指定されているどのルール / 条件とも一致しなかったメッセージのメッセージソースは変更されません。

ECS の設定が管理対象ノードに存在する場合は、opc(r)agt -status コマンドを使って opceca のステータスを調べることができます。opceca プロセスは、イベント相関処理ポリシーが管理対象ノードに配布されている場合に開始されます。管理対象ノードにイベント相関処理ポリシーが存在しない場合は、opceca は停止されます。

イベント相関処理ポリシーは、その他の HPOM ポリシーと同様に管理対象ノードに割り当てられます。

注記

実行中の相関処理エンジンに相関処理サーキットをロードしようとすると (たとえば、新しい、または変更したイベント相関処理ポリシーを配布する場合)、エンジンは開いているすべてのメッセージをメッセージエージェント (opcmsga) に転送し、エンジンを停止してサーキットをロードした上で再起動します。メッセージエージェントは、転送されてきたメッセージを相対処理エンジンに戻しません。

注記

ポリシー本文にキーワード MPI_IMMEDIATE_LOCAL_ACTIONS が指定されていない場合、相関処理プロセスで破棄されたメッセージに関連付けられている自動アクションは実行されません。このオプションはデフォルトで有効です。このオプションを利用できるのは、MSI への出力が有効で、ポリシー本文にキーワード MPI_SV_DIVERT_MSG が指定されている場合のみです。

何らかの新しいアクションが必要な場合は、相関処理プロセスの実行中に新しいメッセージ、または修正した既存のメッセージにそれを指定し、関連付ける必要があります。相関処理サーキット内での自動アクションの定義については、*ECS Designer のドキュメント*を参照してください。

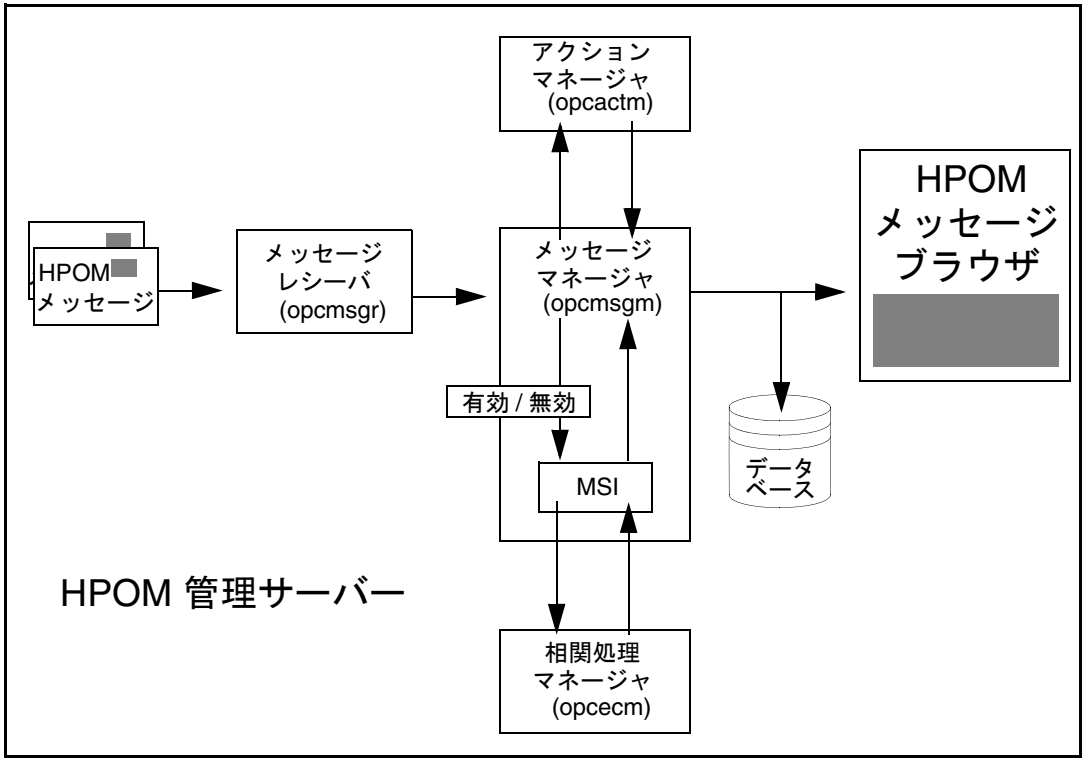
管理サーバーでのメッセージの相関処理

HP Operations 管理サーバー上でメッセージの相関処理を行うことで、同じ障害に関する異なるノードからの類似した、または同一のメッセージの数を減らすことができます。これらのメッセージは、Java GUI メッセージブラウザに表示されます。

冗長なメッセージを削減することは、クライアント - サーバーアプリケーションが分散し、プリンタ、バックアップデバイス、NFS ファイルサーバーなどのネットワークデバイスが共有されている環境で特に便利です。たとえば、データベースサーバーが一時的に使用不能になった場合に、データベースサーバーに接続できなくなった管理対象ノードからの類似したメッセージをフィルタリングできます。

図 4-27 は、管理サーバー上のメッセージのフローと、サーバー MSI へのメッセージ出力を有効 / 無効にすることで、相関処理マネージャ (opcecm) へのメッセージへのフローをどのように制御できるかを示しています。

図 4-27　　HP Operations 管理サーバー上のメッセージのフロー



opcecm プロセスはサーバー MSI に接続し、メッセージストリームからのメッセージへのアクセスを有効にします。メッセージの相関処理が行われ、HPOM メッセージエージェントに戻されます。相関処理プロセスによって作成 / 変更されたメッセージは、`MSI:opcecm` というメッセージソースでメッセージブラウザに表示されます。相関処理サーキットに指定されているどのルール / 条件とも一致しなかったメッセージのメッセージソースは変更されません。

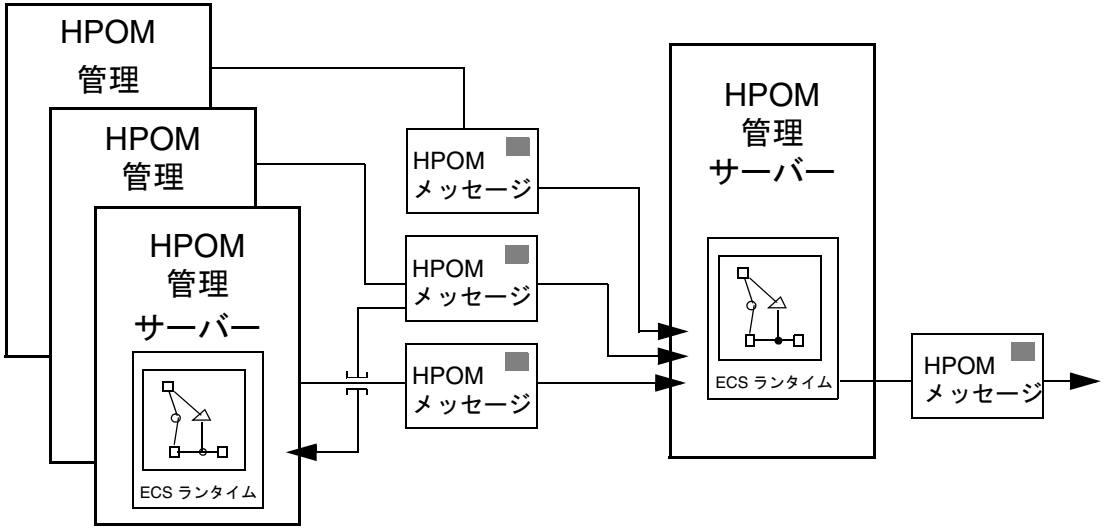
ECS の設定が管理サーバーに存在する場合は、opcsv -status コマンドを使って opcecm のステータスを調べることができます。opcecm プロセスは、イベント相関処理ポリシーが管理サーバーに配布されている場合に開始されます。管理サーバーにイベント相関処理ポリシーが存在しない場合、このプロセスは停止されます。

フレキシブル管理環境でのメッセージの相関処理

HPOM のフレキシブル管理設定機能を利用している大規模な環境では、管理階層の各種レベル間の関係を考慮しなければならないため、メッセージの相関処理は複雑になる場合があります。HPOM 環境内の管理対象ノードと管理サーバーの関係は、管理階層内の管理サーバー間の関係にまで拡張できます。その上で、管理サーバーは管理ノードから受け取ったメッセージの相関処理を行い、相関処理済みの新しいストリームを所属管理サーバーに送信します。または、相関処理されていないメッセージのストリームを次のレベルの管理サーバーに送信し、そこで相関処理を行います。

フレキシブル管理階層でのこのようなメッセージ相関処理を有効にするには、関連する各種 HP Operations 管理サーバーに管理サーバー相関処理ポリシーを割り当て、配布します。ポリシーの割り当て / 配布方法については 190 ページの「ポリシーの割り当て」を参照してください。

図 4-28　HPOM のフレキシブル管理環境での相関処理



外部データへのアクセス

相関処理サーキットが外部ソースからの情報にアクセスしなければならないことがよくあります。この外部情報には、相関処理サーキットの動作に影響するパラメータが含まれます。これにより、ECS Designer でコンパイルし直さずにサーキットの動作を変更できます。たとえば、異なるメッセージタイプに対応した過渡障害用の相関処理サーキットを作成できます。サーキットをコンパイルし直さずにメッセージタイプを追加できるように、メッセージタイプのリストを相関処理サーキットの外部で維持します。

外部情報は、相関処理上の決定を行ったり、相関処理サーキットからの情報出力を改善する場合に必要になることもあります。たとえば、エラーメッセージが検出されたときに、外部データベースをクエリしてサービスレベル契約 (SLA) に関する情報を取得できます。その上で、メッセージブラウザに表示する前にメッセージに SLA の詳細情報を追加できます。

相関処理サーキットからは、2 つの方法で外部データにアクセスできます。

- データストアとファクトストア
- 注釈メカニズム

データストアとファクトストア

ECS データストアおよびファクトストアを使用することで、相関処理の環境的側面を、イベント相関処理ポリシーにハードコードされるルールおよび基本ロジックから切り離すことができます。たとえば、1 つの HPOM 管理対象ノード用に汎用の相関処理サーキットを設定し、データストアを利用して、同じポリシーを別の管理対象ノードに適用できます。

データストアは、情報のキーと値のペアの保持に利用できます。イベント相関処理ポリシーに関連するシステム固有の情報や、外部ネットワークの詳細情報 (間隔、しきい値、その他の制約など) が変化する可能性があることがわかっている場合は、これらの情報も含まれます。たとえば、ユーザー切り替え (su コマンドを使用) をモニターするための汎用イベント相関処理ポリシーを設定し、信頼されるユーザー (システムごとに異なる可能性があります) の名前をデータストアに保存して、別の HPOM 管理対象ノードでそのポリシーを実行できます。

ファクトストアは、関係を定義するデータ構造です。これらの関係は、たとえば、企業の階層間の関係、企業間の関係、サービスとサービスプロバイダの関係などを表します。例を示します。A、B、C という 3 つのアプリケーションサーバーが同じデータベースサーバー DBserver01 に接続され、4 番目のアプリケーションサーバーは別のデータベースサーバー DBserver02 に接続されていると仮定します。ファクトストアを利用することで、これらの関係を定義できます。何らかの理由により DBserver01 が応答しなくなった場合は、ファクトストア内の情報を利用して、このデータベースサーバーからのメッセージと、DBserver01 へのアクセス不能に関するアプリケーションサーバー A、B、C からのメッセージを相関処理できます。

ファクトストアとデータストアは、管理対象ノードまたは管理サーバーに EC ポリシーが配布されるときに ECS エンジンにロードされるテキストファイルです。データストアのファイル拡張子は ds、ファクトストアのファイル拡張子は fs です。ファクトストア / データストアのファイルは EC ポリシーと共に配布されるわけではありません。EC ポリシーを配布する前に作成し、次の場所に手動でコピーする必要があります。

- 管理サーバー :
  /var/opt/OV/shared/server/datafiles/policies/ec
- 管理対象ノード (UNIX):
  /var/opt/OV/conf/eaagt
- 管理対象ノード (Windows):
  C:\Program Files\HP BTO Software\data\conf\eaagt

各相関処理サーキットがアクセスできるファクトストア / データストアファイルはそれぞれ 1 つのみです。

HPOM には、固有とグローバルの 2 種類のファクトストア / データストアがあります。グローバルファクトストア / データストアは、複数の相関処理サーキットで共有できます。固有ファクトストア / データストアにアクセスできるのは、1 つの相関処理サーキットのみです。

- *固有データストア / ファクトストア*

  各相関処理サーキットには、そのサーキットに関連付けられている ECS サーキットファイル (.eco) がコンパイルされています。コンパイルされるサーキットファイルの名前は、相関処理サーキットの作成時または変更時に自動的に生成され、*<id>*.eco (たとえば、EAAAa03015.eco) という形式になります。

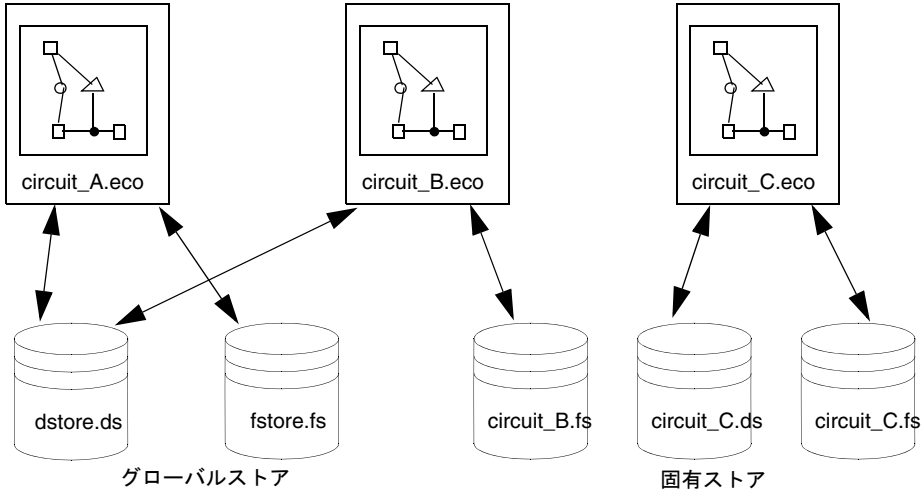
管理対象ノードまたは管理サーバーに相関処理サーキットを配布すると、コンパイルされているサーキットファイルと同じ名前で、適切な拡張子 (ファクトストアは `fs` 、データストアは `ds`) を持つファクトストア / データストアが指定のディレクトリに存在するかどうかがチェックされます。存在しない場合は、グローバルファクトストア / データストアが使用されます。

- *グローバルデータストア/ ファクトストア*

  グローバルデータストアファイル (`dstore.ds`) とグローバルファクトストアファイル (`fstore.fs`) は、複数の相関処理サーキットで共有できます。イベント相関処理ポリシーに固有ファクトストアが存在しない場合は、グローバルファクトストアがロードされます。同様に、イベント相関処理ポリシーに固有データストアが存在しない場合は、グローバルデータストアがロードされます。

303 ページの図 4-29 は、グローバルおよび固有ファクトストア / データストアにアクセスする相関処理サーキットを示しています。

図 4-29　　HPOM のデータストア / ファクトストア



データストア / ファクトストアの更新

HPOM を再起動する、または管理対象ノード / 管理サーバーに新しい、または変更された相関処理ポリシーを配布すると、ファクトストア / データストアファイルは再ロードされます。次の場所で ecsmgr ユーティリティを使用して、個々のファクトストア / データストアファイルを手動で強制的に再ロードすることもできます。

- 管理サーバー

  `/opt/OV/bin/OpC/`

- 管理対象ノード (UNIX)

  `/opt/OV/bin/OpC/utils/`

- 管理対象ノード (Windows)

  `\usr\OV\bin\OpC\install\`

ecsmgr を使用するときは、管理対象ノードと管理サーバーのどちらの ECS エンジンと通信するかを指定します。管理サーバーインスタンスは 11、管理対象ノードインスタンスは 12 です。

次の 2 つのコマンドを使用することで、イベント相関処理ポリシーを新しいファクトストア / データストアで更新できます。

- データストア

  # ecsmgr -i *<インスタンス>* -data_update *<データストア名>* \ *<ファイル名>*

  次に例を示します。

  ```
  # ecsmgr -i 12 -data_update DatabaseDown \
  /var/opt/OV/conf/eeagt/DatabaseDown.ds
  ```

- ファクトストア

  # ecsmgr -i *<インスタンス>* -fact_update *<ファクトストア名>* \ *<ファイル名>*

  次に例を示します。

  ```
  # ecsmgr -i 12 -fact_update fstore \
  /var/opt/OV/conf/eeagt/fstore.fs
  ```

注記

ecsmgr コマンドは動的なサーキットパラメータのみを更新し、静的に評価されるパラメータを変更しません。ECS の静的 / 動的なパラメータの詳細については、*ECS Designer のドキュメント*を参照してください。

ヒント

ファクトストア / データストアファイルのサイズが極端に大きい場合は、相関処理プロセスが長時間ブロックされないように、複数の小さいファイルを使って増分更新してください。

ファクトストア / データストアとそれぞれの内容の構文については、『*HP ECS Designers Reference*』を参照してください。ecsmgr ユーティリティの詳細については *ecsmgr(1M)* のマニュアルページを参照してください。

UNIX ノードへの配布の自動化

ファクトストア / データストアはイベント相関処理ポリシーと共に配布されませんが、UNIX ノードへの配布については部分的に自動化できます。

UNIX ノードへのファクトストア / データストアの配布を自動化するには、管理サーバーで次の手順を実行します。

1. ファクトストア / データストアファイルを作成し、次のディレクトリに配置します。

   /var/opt/OV/share/databases/OpC/mgd_node/customer/\
   <*arch*>/cmds

注記

HPOM のコマンドディレクトリには <*arch*> が含まれます。これは、コマンドのアーキテクチャ (hp/alpha/tru64、sun/sparc/solaris10 など) を表します。

管理対象ノードにコマンドを配布すると、ファクトストア / データストアファイルが /var/opt/OV/bin/OpC/cmds ディレクトリにインストールされます。

2. ファクトストア / データストアファイルを次のディレクトリ内の /var/opt/OV/bin/OpC/cmds から /var/opt/OV/conf/OpC/ にコピーするスクリプトを作成します。

   ```
   /var/opt/OV/share/databases/OpC/mgd_node/customer/\
   <arch>/cmds
   ```

ファクトストア / データストアを配布するときは、管理対象ノードにコマンドを配布し、HPOM のコマンドブロードキャストメカニズムを使ってスクリプトを実行します。

状況によっては、定期的に変更されるデータへのアクセスには、ファクトストア / データストアよりも ECS 注釈ノード機能を利用するほうが適しています。注釈メカニズムの詳細については 306 ページの「注釈メカニズム」を参照してください。

注釈メカニズム

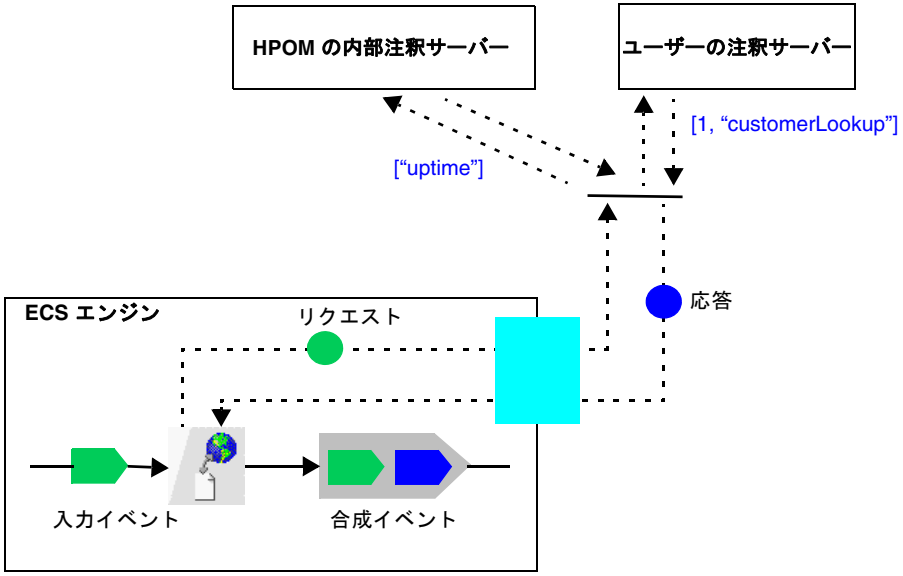
ECS 注釈ノードメカニズムを使用することで、相関処理サーキットから外部ソースの情報にアクセスできます。一般に、定期的に変更される情報へのアクセスには、ファクトストア / データストアよりも注釈ノードのほうがよく使用されます。

注釈ノードは、ECS エンジンの外部に存在する外部プロセスを呼び出します。この外部プロセスは注釈サーバーと呼ばれます。注釈サーバーは適切な処理を行い、情報を注釈ノードに返します。この情報は、相関処理上の決定を行ったり、相関処理サーキットからの情報出力を改善するために、サーキット内で利用できます。

HPOM では 2 種類の注釈サーバーを利用できます。

- 内部注釈サーバー
- ユーザー作成の注釈サーバー

図 4-30　　HPOM の注釈メカニズム



注釈サーバーへのリクエストの送信には、注釈ノードの Annotate_Spec パラメータが使用されます。デフォルトでは、リストの最初の要素が文字列であれば、HPOM の内部注釈サーバーはリクエストを捕捉し、その文字列をコマンドとして実行します。リストの最初の要素のデータタイプが文字列以外 (整数など) であれば、HPOM の内部注釈サーバーはリクエストを捕捉 *しません*。代わりに、ユーザーが作成した注釈サーバーでリクエストを利用できます。

デフォルト動作を変更し、特定の名前の注釈ノードからのリクエストのみを受信するように各注釈サーバーを設定できます。これを行うには、コマンド行ツール ovconfchg を使って次の変数を設定します。

- 管理サーバー : ECM_ANNO_NODE
- 管理対象ノード : ECA_ANNO_NODE

ECM_ANNO_NODE、ECA_ANNO_NODE、または両方の変数が設定されると、指定された名前のノードからの注釈リクエストのみが HPOM の内部注釈サーバーで処理されるようになります。変数の形式は次のとおりです。

```
ECM_ANNO_NODE <名前 1>[,<名前 2>...]
```

たとえば、内部注釈サーバーが OVOEXE という注釈ノードからの注釈リクエストを処理するように設定するには、変数を次のように設定します。

```
ECM_ANNO_NODE OVOEXE
```

注記

相関処理サーキットで同じ名前の複数の注釈ノードを使用するには、名前が競合しないように、それぞれを固有の合成ノードに配置します。合成ノードの詳細については、*HP ECS Designer のドキュメント*を参照してください。

ユーザー作成の注釈サーバーが特定の名前のノードからのリクエストを受け付けるための設定については、*ECS のドキュメント*を参照してください。

内部注釈サーバー

内部注釈サーバーは、相関処理サーキットに結果を返すコマンド / スクリプトの実行に使用されます。注釈ノードの Annotate_Spec パラメータには、実行するコマンド / スクリプトへの完全パスを指定する必要があります。また、すべてのパラメータを指定する必要があります。HPOM の内部注釈サーバーは、終了コードとコマンド / スクリプトの標準出力の両方を返します。

すべての注釈サーバーから返されるデータは、注釈ノードからの出力である合成イベントの 2 番目のサブイベントに配置されます。

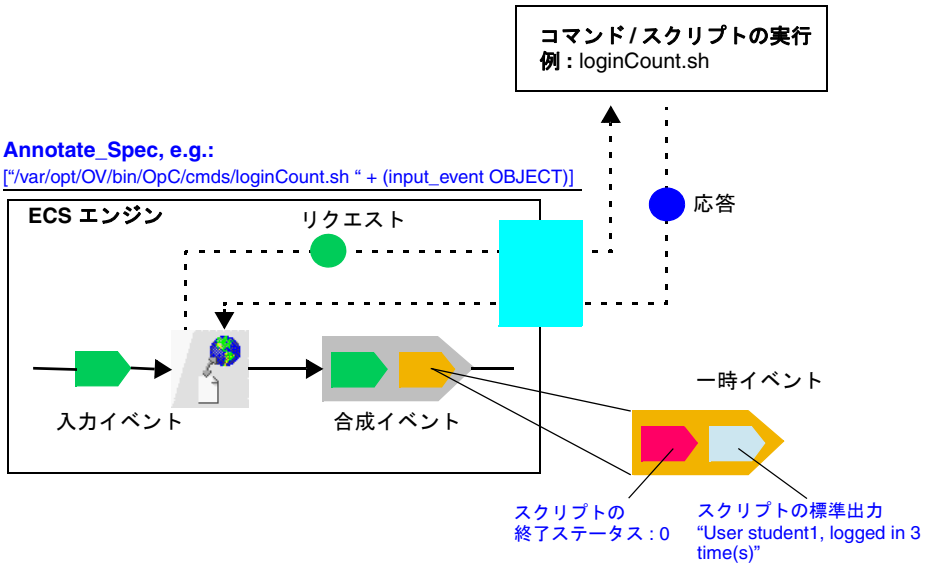
図 4-31 は、HPOM の内部注釈サーバーから返されるデータに 2 つの情報が含まれることを示しています。1 つは終了コードで、もう 1 つはコマンド / スクリプトの標準出力です。フィルターノードで終了コードを取得するには、次の文を使用します。

```
input_event 2 1
```

コマンド / スクリプトの標準出力を取得するには、次の文を使用します。

```
input_event 2 2
```

図 4-31　　HPOM の内部注釈サーバー



注釈スクリプト

HPOM の内部注釈サーバーに送信される注釈リクエストには、単一文字列のリストとして Annotation_Spec が含まれている必要があります。この文字列の値は、実行するコマンド / スクリプトの完全修飾ファイル名と、それに続くその他のパラメータです。次に例を示します。

```
["/var/opt/OV/bin/OpC/cmds/loginCount.sh student1"]
```

この例では、1 つのパラメータ student1 が指定された /var/opt/OV/bin/OpC/cmds/loginCount.sh スクリプトが実行されます。これ以外のパラメータには、スクリプト内の位置指定パラメータ ($2、$3、...) などがあります。

通常、コマンド / スクリプトに渡されるパラメータは、入力メッセージのメッセージ属性から取得されます。次に例を示します。

```
["/var/opt/OV/bin/OpC/cmds/loginCount.sh " + \
(input_event OBJECT)]
```

コマンド / スクリプトは、EC ポリシーの配布時に自動的に配布されません。スクリプトの場所はあらかじめ決められていないため、Annotation_Spec には絶対パスを指定する必要があります。

注記

スクリプトファイルを HPOM のコマンドディレクトリ (/var/opt/OV/share/databases/OpC/mgd_node/customer/<*arch*>/\cmds) に配置した場合は、スクリプトファイルは管理対象ノードの /var/opt/OV/bin/OpC/cmds ディレクトリに配布されます。

このパスは、実行されるコマンドのパスとして Annotation_Spec で使用されます。次に例を示します。

["/var/opt/OV/bin/OpC/cmds/loginCount.sh <***その他のコマンドパラメータ***>"]

目的の応答を生成するには、スクリプトは exit および echo コマンド (または同等コマンド) を使用します。

次のテキスト文字列は、ユーザー (ユーザー名は最初のパラメータ) がログオンした回数を返すスクリプトを作成する方法を示しています。

```
#!/bin/sh
# loginCount.sh script
COUNT=`who | grep $1 | wc -l`
echo "User $1, logged in $COUNT time(s)"
exit 0
```

ユーザー作成の注釈サーバー

独自のサーバープロセスの開発を希望するユーザー向けに、注釈 API が用意されています。ユーザー作成の (カスタム) 注釈サーバーは、ECS エンジンに登録され、注釈リクエストをリスンする個別のプロセスです。リクエストを受信すると、注釈サーバーはリクエストを処理し、注釈 API を使用して応答を相関処理サーキットに返します。ユーザー作成の注釈サーバーは、SLA データベースへのアクセス、ネットワークデバイス上の MIB のクエリ、別のアプリケーションからのトポロジ情報のクエリなど、さまざまな用途に利用できます。カスタム注釈サーバーの開発方法、およびユーザーの相関処理サーキットで注釈ノードを使用する方法については、*HP ECS のドキュメント*を参照してください。

ECS Designer での注釈ノードのシミュレーション

ECS Designer のシミュレーションモードを使用して、稼働環境に配布する前に相関処理サーキットをテストできます。ECS Designer から注釈サーバーに直接アクセスすることはできませんが、シミュレートされた注釈応答を作成してサーキットをテストできます。シミュレートされた注釈サーバー応答を作成する手順は次のとおりです。

1. イベントが出力されないようにサーキットを変更します。
2. ECS Designer のシミュレーションモードに切り替え、注釈ノードが含まれるサーキットを使用してサンプルイベントをいくつか実行します。イベントブラウザに注釈リクエストが表示されます。この出力は、ブラウザの下部にある **[保存]** ボタンを使って保存できます。

   リクエストの形式は次のようになっています。

   ```
   0

   20010424044754.000000Z

   ["Data sent from Anno_Spec"]

   % anno:request:

   1
   ```

3. 次の行を変更し、これらのリクエストを応答に変更します。

   ```
   % anno:request:
   ```
   を次のように変更
   ```
   %anno:response:
   ```

   リストを変更し、注釈ノードに戻されるデータを含めます。

4. 次の行に遅延値を追加して遅延を設定します。

   ```
   %anno:response:
   ```

   たとえば、応答に 2 秒間の遅延を設定するには、行を次のように変更します。

   ```
   %anno:response:2
   ```

注釈の応答はシミュレータにロードできます。

HPOM の相関処理ポリシーの例

イベント相関処理は、複数メッセージから単一メッセージへの統合、メッセージへの追加情報の注釈の追加、手動で実行している手順の自動化など、さまざまな用途に利用できます。

また、イベント相対処理によってメッセージブラウザに到達するメッセージの数を削減し、オペレータが障害の根本原因を特定しやすくすることもできます。たとえば、次のようなシステムリソース使用率制限に関連して生成されるメッセージを相関処理するポリシーを HP Operations 管理対象ノードに設定できます。

- プロセスの最大数の超過
- ディスク容量の不足
- 名前付きパイプの最大数への到達
- ノードの最大数の超過
- 設定済み共有メモリの不足
- 設定済みセマフォの不足

MIB 値を継続的にモニターすることで、プリンタなどの同一共有ネットワークデバイスに関連する障害を修復するためのアクションを実行すべきかどうかを判断することもできます。たとえば、次のような障害が対象となります。

- 5 分間以上の「紙詰まり」ステータス
- 5 分間以上の「要給紙」ステータス
- 2 分間以上の「プリンタドア開」ステータス

HPOM と ECS Designer の両方で、より高度な機能を利用するには、次のことができるように HPOM 相関処理ポリシーを設定します。

- 追加の、具体的な、コンテキスト関連のデータを取得する
- 古い HPOM メッセージを自動的に受諾する
- HPOM メッセージ属性を変更する

イベント相関処理のシナリオ

HPOM の相関処理のシナリオは、相関処理によってメッセージブラウザに到達する冗長メッセージの数を減らすことで、メリットをどのように得られるかを理解する上で役立ちます。フィルタリングによって除外されるメッセージの数が多いほど、メッセージブラウザに到達するメッセージの数は少なくなり、したがって、オペレータはより多くの時間を障害の調査と解決に費やすことができます。

表 4-2 は、いくつかの相関処理ポリシーの例を示しています。すべてのサンプルポリシーは、`opcpolicy -list_pols` コマンドの出力に表示されます。ECS Designer GUI がインストールされている環境では、`opcpolicy -download` コマンドを使ってポリシーをダウンロードし、ECS Designer GUI で編集してください。

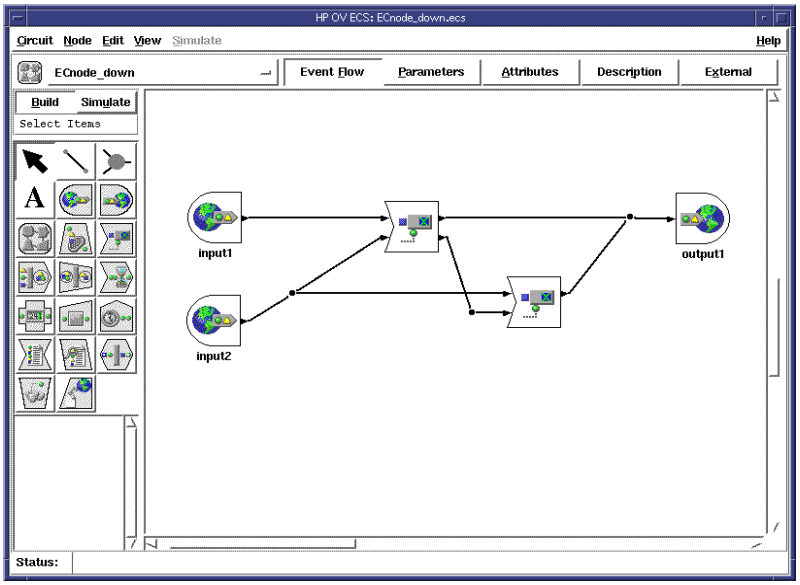
表 4-2　HPOM の相関処理ポリシーの例

ターゲットシステム	ポリシー名	説明
HP Operations 管理サーバー	一時的なノード停止 (`transient node_down`)	「ノード稼働中」メッセージが続く場合は、「ノード停止中」メッセージを除外する
	一時的なインタフェース停止 (`transient if_down`)	「インタフェース稼働中」メッセージが続く場合は、「インタフェース停止中」メッセージを除外する
HP Operations 管理対象ノード	ユーザー切り替え失敗 (`bad_su`)	「ユーザー切り替え成功」メッセージが続く場合は、「ユーザー切り替え失敗」メッセージを除外する

一時的なノード停止ポリシー

図 4-32 は、ECS Designer で開いた「一時的なノード停止」ポリシーを示しています。この相関処理ポリシーを使用することで、何らかの理由により一時的に到達できなくなったノードに関連するすべてのメッセージを相関処理プロセスで破棄できます。ただし、メッセージを破棄できるのは、指定した時間内にノードが到達可能な状態に戻る場合のみです。この条件が満たされる場合、表示されるメッセージは、ノードが到達可能な状態に復帰したことを示すメッセージのみになります。このメッセージは自動的に受諾され、履歴メッセージブラウザに送信されます。

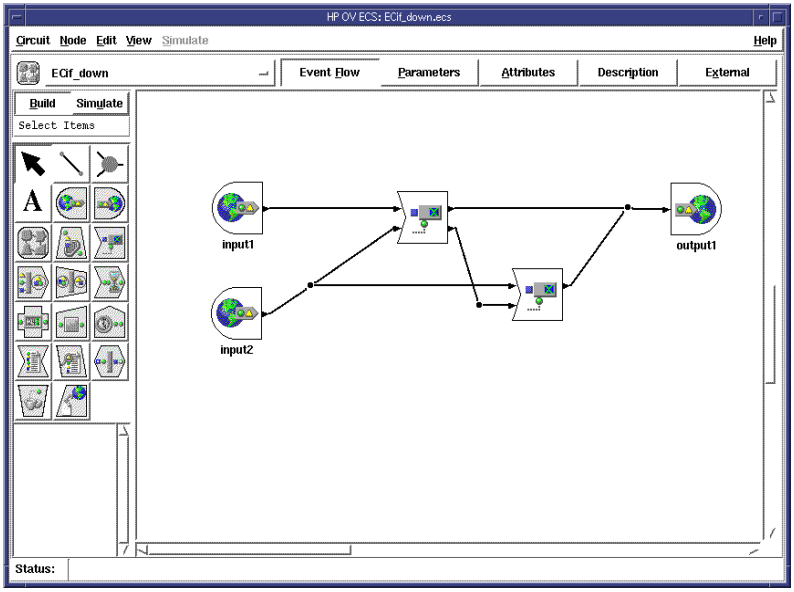
図 4-32　ノード停止の HPOM 相関処理ポリシー



一時的なインタフェース停止ポリシー

図 4-33 は、ECS Designer で開いた「一時的なインタフェース停止」ポリシーを示しています。この相関処理ポリシーを使用することで、何らかの理由により一時的に到達できなくなったインタフェースに関連するすべてのメッセージを相関処理プロセスで破棄できます。メッセージを破棄できるのは、指定した時間内に同じインタフェースが到達可能な状態に戻る場合のみです。この条件が満たされる場合、表示されるメッセージは、インタフェースが到達可能な状態に復帰したことを示すメッセージのみになります。このメッセージは自動的に受諾され、履歴メッセージブラウザに送信されます。

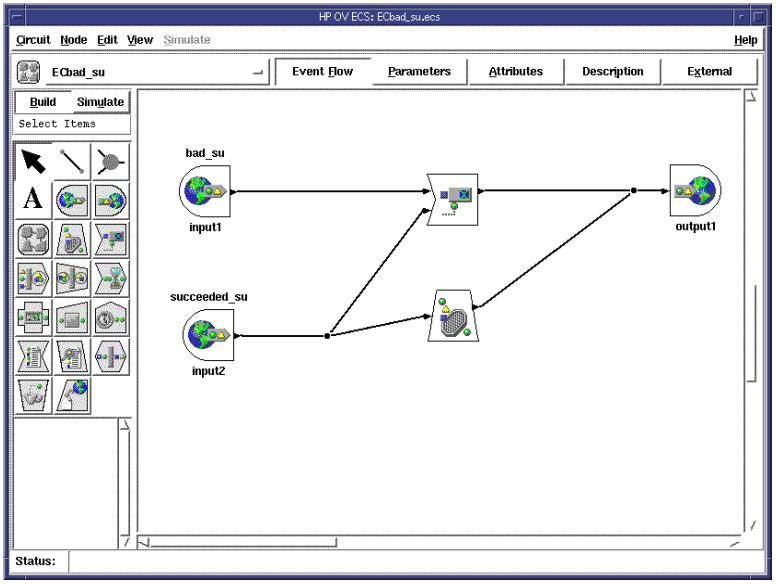
図 4-33　インタフェース停止の HPOM 相関処理ポリシー



ユーザー切り替えポリシー

図 4-34 は、ECS Designer で開いた「ユーザー切り替え」ポリシーを示しています。この相関処理ポリシーを使用することで、別のユーザーへの切り替えを試みたユーザーの切り替え失敗に関連するすべてのメッセージを相関処理プロセスで破棄できます。メッセージを破棄できるのは、指定した時間内に同じユーザーがユーザーの切り替えに 1 回以上成功する場合のみです。この条件が満たされる場合、メッセージブラウザに表示されるメッセージは、ユーザー切り替えに成功したことを示すメッセージのみになります。

図 4-34 **HPOM ユーザー切り替えの HPOM 相関処理ポリシー**



ECS Designer のリモート使用

ここでは、ECS Designer がサポートされない、または利用できない HPOM システムで ECS サーキットを使用する方法について説明します。ECS Designer がサポートされるシステムについては、次の URL を参照してください。
http://support.openview.hp.com/selfsolve/document/KM323488

ECS Designer を利用できないオペレーティングシステム (Linux など) に HPOM がインストールされている場合、これらのシステムでは ECS Designer を使って ECS 相関処理サービスを作成できません。しかし、ECS Designer がサポートされるプラットフォーム (Windows XP、Windows Vista など) で相関処理サービスを作成し、ECS Designer がサポートされない HPOM システムでそのサービスを利用することは可能です。

環境の準備

ECS Designer をリモート使用するには、サポートされるシステムに ECS Designer をインストールします。

ターゲットシステムに HP Operations 管理サーバーをインストールします。HP Operations 管理サーバーのインストールと設定については、『*HPOM 管理サーバーインストールガイド*』を参照してください。ECS Designer に関する情報については、*ECS Designer のドキュメント*を参照してください。

リモート使用のための ECS サーキットの作成

リモートシステム上の ECS Designer を使って作成された ECS サーキットを使用するには、次の手順を実行します。

1. ECS Designer がインストールされているシステムで新しい *ECS サーキット*を作成するか、既存のサーキットを修正します。

   ECS Designer を使ったサーキットの設計方法の詳細は、ECS Designer のドキュメントを参照してください。

2. 作成したサーキットをローカル保存します。
3. サーキットを設計したら、ECS Designer で検証してください。

注記

すべての ECS サーキットを検証する必要があります (構文が正しいことを確認してください)。HPOM 9.xx への設定のアップロード時に未検証の HPOM 8.xx サーキットがアップロードされると、関連するポリシー名とサーキットを示す警告が `opccfgupld` によって出力されます。

4. リモート管理 UI にログオンし、イベント相関処理ポリシータイプの新しいポリシーを作成します。その上で、このポリシーに `.ecs` ファイルと `.eco` ファイルをアップロードします。

注記

コマンド行インタフェースからのタスクの実行に関する情報は、HPOM のドキュメントに記載されています。管理 UI の使用については、次の場所の HP Operations Manager ディレクトリでダウンロードできる適切なドキュメントを参照してください。

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

既存の ECS サーキットの修正

ターゲット HP Operations 管理サーバーで使用している ECS サーキットを修正するには、次の手順を実行します。

1. ターゲット HP Operations 管理サーバーから ECS サーキットをダウンロードします。
2. ECS Designer がインストールされているシステムに ECS サーキットをアップロードします。
3. ECS Designer GUI を使って ECS サーキットを修正します。
4. 管理 UI を使用して、修正したサーキット (`.eco` ファイルと `.ecs` ファイル) をターゲット HP Operations 管理サーバー上のイベント相関処理ポリシーにアップロードします。317 ページの「リモート使用のための ECS サーキットの作成」を参照してください。

ECS サーキット名の変更

ECS サーキットの名前を変更する手順は次のとおりです。

1. 次のコマンドを実行し、EC ポリシー名のリストを取得します。

```
# opcpolicy -list_pols pol_type=Event_Correlation
```

2. 特定の EC ポリシーに対応するコンパイル済みサーキットの名前を取得するには、次のコマンドを実行してそのポリシーをダウンロードします。

   **# opcpolicy -download pol_name=<*ポリシー名*> **
   **version=<*バージョン*> pol_type=Event_Correlation **
   dir=<*ダウンロードディレクトリ*>

3. ポリシーのダウンロード先である <*ダウンロードディレクトリ*> で <*id*>_data ファイルを開き、CIRCUIT_FILE 属性を調べます。この属性の値が ECS サーキットの名前です。次に例を示します。

   ```
   CIRCUIT_FILE "85mtaliep0"
   ```

   ECS サーキット名を変更するには、CIRCUIT_FILE 属性の値を変更します。

4. 新しい名前の ECS サーキットを使用するには、次のコマンドを実行します。

   # opcpolicy -upload dir=<*ダウンロードディレクトリ*>

   opcpolicy コマンドの詳細については *opcpolicy(1M)* のマニュアルページを参照してください。

例 4-4 イベント相関処理ポリシーの操作

UNIX 管理対象ノードに配布される DatabaseDown というイベント相関処理ポリシーがあり、サーキット名は EAAAa03016 であると仮定します。イベント相関処理ポリシーは、*固有*データストア内の設定データと、*グローバル*ファクトストア内のデータベース関係にアクセスします。次の手順を実行します。

1. EC ポリシーの名前とバージョンを調べるには、次のコマンドを実行します。

   # opcpolicy -list_pols pol_type=Event_Correlation

2. DatabaseDown ポリシーのコンパイル済みサーキットの名前を調べるには、次のコマンドを実行してこのポリシーをダウンロードします。

   # opcpolicy -download pol_name=DatabaseDown \ version=1.0
   pol_type=Event_Correlation dir=/tmp/circuit

3. /tmp/circuit ディレクトリで *_data ファイルを開き、CIRCUIT_FILE 属性の値を調べます。

   CIRCUIT_FILE "EAAAa03016"

   この EAAAa03016 が ECS サーキットの名前です。

4. 次のように、ECS サーキットの名前を DatabaseDown に変更します。

   CIRCUIT_FILE "DatabaseDown"

5. 新しい名前の ECS サーキットを使用するには、次のコマンドを実行します。

   # opcpolicy -upload dir=*/tmp/circuit*

   opcpolicy コマンドの詳細については *opcpolicy(1M)* のマニュアルページを参照してください。

6. 固有データストアファイル (DatabaseDown.ds) を管理対象ノード上の次の場所にコピーします。

   /var/opt/OV/conf/eaagt/

7. グローバルデータストアファイル (fstore.fs) を管理対象ノード上の次の場所にコピーします。

   /var/opt/OV/conf/eaagt/

DatabaseDown ポリシーを配布すると、コンパイル済みサーキットファイルと同じ名前を持つデータストアファイル DatabaseDown.ds がロードされます。DatabaseDown.fs というファイルは存在しないため、グローバルファクトストアファイルである fstore.fs がロードされます。

サービス時間

サービス時間は、サービスプロバイダが HPOM から報告される障害と、指定されているサービスに関連する障害に対応するための時間帯であり、合意に基づいて定められています。サービス時間は、サービスごとに異なる場合があります。

メッセージのバッファリング

定義されているサービス時間中に受信したメッセージは、通常どおりに Java GUI メッセージブラウザに送られます。サービス時間外に受信したすべてのメッセージは、バッファリングされます。バッファリングされたメッセージは、Java GUI のペンディングメッセージブラウザで表示できます。

メッセージの自動バッファ解除

定義されている次回のサービス時間が開始されると、バッファリングされているメッセージは自動的にバッファ解除されます (つまり、Java GUI メッセージブラウザに移動されます)。バッファリングされていたメッセージは、Java GUI メッセージブラウザに移動された後は、通常どおりに操作できます。

メッセージの手動バッファ解除

バッファリングされたメッセージは、[メッセージのプロパティ] ウィンドウ、または Java GUI のペンディングメッセージブラウザから手動でバッファ解除できます。手動でバッファ解除されたメッセージは、バッファ解除操作を実行したユーザーの所有となるか、そのユーザーのマークが付けられます。

手動によるバッファ解除操作には、次の制限が適用されます。

- **バッファ時間の経過後にのみメッセージを送信**

  バッファリングされたメッセージは、メッセージのバッファ時間が経過する (つまり、メッセージを生成したサービスの次回のサービス時間が始まる)、*または*、オペレータがメッセージを開く、*いずれか*の時点でトラブルチケットおよび通知インタフェースに送信されます。

- **管理サーバーに到着した時点でのメッセージの転送**

  マネージャ間の転送が設定されている場合、バッファリングされたメッセージは、メッセージが HP Operations 管理サーバーに到達した直後に定義されている別の管理サーバーに転送されます。

注記

転送先のマネージャには、独自の休止時間とサービス時間が設定されている可能性があります。

サービス時間の定義

サービス時間の設定方法、およびサービス時間の定義に使用されるポリシーと構文規則については、『*HPOM システム管理リファレンスガイド*』を参照してください。

計画休止

HPOM では、**計画休止**を設定できます。これにより、定義した時間内に着信した、利用できなくなることが事前にわかっている (計画されている) サービス / システムに関連するメッセージを**ログに記録する**、または**除外** (削除) できます。たとえば、計画休止を利用して、保守のために一時的に利用できなくなるコンポーネントからのすべてのメッセージを除外できます。

休止のスケジューリング

計画休止は、分散した作業環境内で 1 つまたは複数のコンポーネント / サービスが利用できなくなることが事前に計画されている、または繰り返される可能性がある場合に、これらのコンポーネント / サービスに関連するメッセージをログに記録する、または削除しなければならない期間を定義します。大きな障害が発生し、特定のコンポーネントからの後続のメッセージを除外しなければならない場合は、休止を動的に定義できます。たとえば、Oracle データベースがダウンした場合は、定義した時間内に受信する Oracle に関連するすべてのメッセージを除外できます。休止のステータスは、外部アプリケーションを使って設定することもできます。

計画休止の定義

計画休止の設定方法、および計画休止の定義に使用されるポリシーと構文規則については、『*HPOM システム管理リファレンスガイド*』を参照してください。

サービス時間と計画休止の設定

HPOM 管理者は、フレキシブル管理を設定するためのポリシーに似たポリシーを使用して、管理サーバーにサービス時間と計画休止を設定できます。構文が同じなので、opcmomchk ツールを使ってチェックできます。このポリシーは /etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs に配置されます。使用するポリシーと構文の詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

注記

計画休止とサービス時間は、外部アプリケーションから設定することもできます。ただし、指定する外部アプリケーションは、計画休止とサービス時間のポリシーを作成することができ、opccfgout(1M) コマンドを使って休止を制御できる必要があります。

5 複数の管理サーバーに対応したスケーラブルなアーキテクチャ

概要

本章では、大規模な分散環境における HPOM の設定方法と管理方法について説明します。また、フレキシブル管理と manager-of-manager (MoM) 通信の基本的な概念についても説明します。

注記

本章では、「マネージャ」という用語は**管理サーバー**、「エージェント」という用語は**管理対象ノード**をそれぞれ意味します。

対象読者

本章は、HPOM 管理者を対象としています。

本章の内容

本章で説明する内容は次のとおりです。

- **サーバー間の通信**

  サーバー間通信の背景となる基本概念とサンプルアプリケーション。

- **サーバーへのメッセージ転送**

  時刻またはメッセージ属性に基づいて設定できる、管理対象ノードから別のサーバーへのメッセージ転送。

  メッセージの重要度、メッセージテキスト、カスタムメッセージ属性など、HPOM メッセージ属性の変更を別の HPOM 管理サーバーと同期させることができます。

- **管理サーバーの担当範囲の設定**

  管理サーバーが担当する HPOM 管理対象ノードの設定。これらの担当範囲により、ナレッジセンターを最大限に活用し、単一障害点のボトルネックを排除できます。

- **サーバー設定の配布**

  別の管理サーバーへのサーバー設定の配布 (たとえば、テスト環境から稼働環境への設定の移動)。

- **サーバー間でのメッセージ転送**

  管理サーバー間でのメッセージ転送。

フレキシブル管理

HPOM では、環境を階層的に構成できます。その上で、オペレータの経験、地理的な配置、時刻などの多様な条件に基づいて、管理の担当範囲を複数の管理レベルに分散させることができます。このフレキシブル管理により、テクニカルサポートをいつでも自動的に (または必要時に) 利用できる安心感が得られ、オペレータは各自が得意な業務に集中できます。

注記

日本語環境におけるフレキシブル管理については、『*HPOM システム管理リファレンスガイド*』を参照してください。

デフォルト設定

HPOM のデフォルト設定には、管理対象ノードにインストールされているエージェントとの間でやり取りを行う 1 つの管理サーバーが使用されます。このデフォルト設定では、エージェントがメッセージを送信できるのはこの管理サーバーのみとなります。ただし、HPOM の設定は、さまざまな管理対象ノード上のエージェントが別の管理サーバーにもメッセージを送信できるように簡単に変更できます。

一次マネージャ

最初の管理サーバーは、HPOM 管理対象ノードの管理で中心的な役割を果たす HP Operations サーバーであるため、**一次マネージャ**と呼ばれます。ただし、一次マネージャの機能は別のサーバーに切り替えることができます。この場合、管理対象ノードからのメッセージは新しい (通常は一時的な) 一次マネージャにリダイレクトされます。また、新しい一次マネージャは、これらの管理対象ノードで自動アクションを実行することもできます。

フレキシブル管理のメリット

HPOM のフレキシブル管理アーキテクチャには、次にようなメリットがあります。

- **ワールドワイドネットワークの管理**

  たとえば、**Follow-the-sun** 機能を使用して、世界全体に広がるネットワークをより効率的に管理できます。

- **効率の向上**

  専門技術センターのポリシーを導入することで、効率を改善できます。

- **メッセージの転送**

  管理サーバー間でメッセージを転送します。

- **拡張の管理**

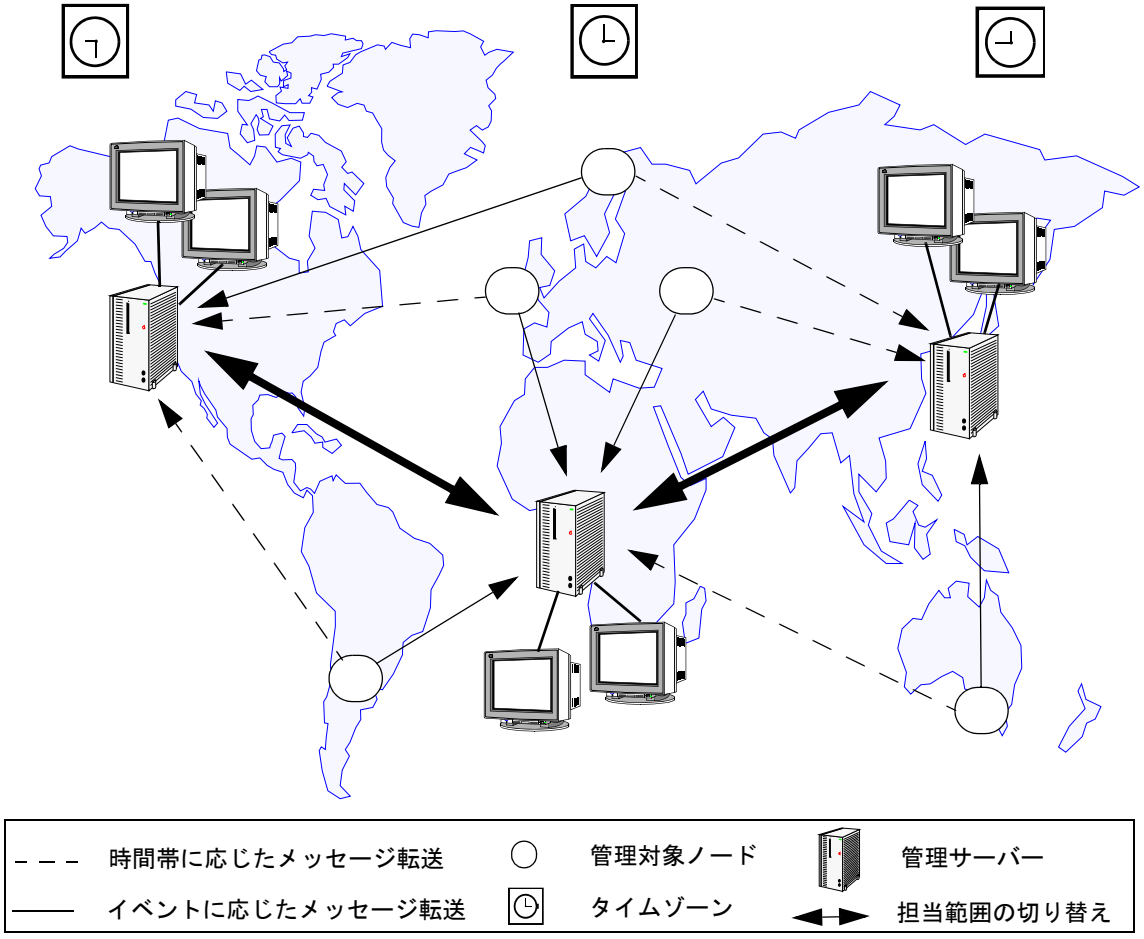
  拡張するネットワーク環境を管理し、一次サーバーが過負荷にならないようにします。

1 つの管理サーバーがすべての管理対象ノードを管理する環境にはボトルネックが生じる可能性があります。このボトルネックは、データベースのパフォーマンスに悪影響を招くことがあります。複数の管理サーバーが管理対象ノードを分散して管理することで、この障害を回避できます。管理担当範囲の分散については 337 ページの「ドメイン階層内での管理担当範囲」を参照してください。

Follow-the-sun 管理

事業拠点が複数のタイムゾーンに分散している場合、HPOM では **Follow-the-Sun** 管理を行うことで管理担当範囲をローテーションさせることができます (図 5-1 を参照)。管理対象ノードは、時間帯に応じて異なる管理サーバーに属します。このケーパビリティを利用すれば、週末や休日の業務専用の管理サーバーも設定できます。

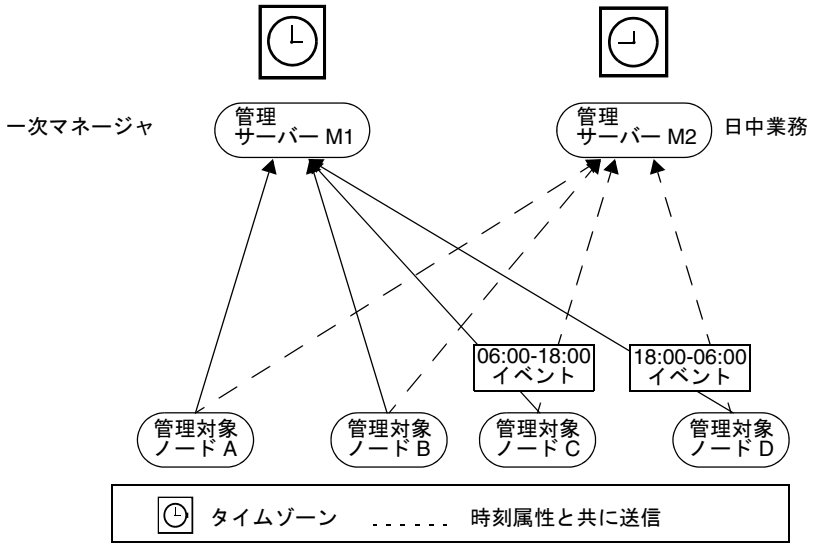
図 5-1　ワールドワイド管理ドメイン



Follow-the-Sun 管理とは、基本的にはあらかじめ設定された時間属性に応じて異なる管理サーバーにメッセージを送信することです。HPOM では、**時間ポリシー**に定義されたルールに従って異なる管理サーバーにメッセージを送信するように管理対象ノードを設定できます。

たとえば、図 5-2 は、管理対象ノード C、D が 6 時～ 18 時の間に生成したすべてのメッセージを HP Operations 管理サーバー M1 に送信し、18 時～ 6 時の間に生成されたすべてのメッセージを HP Operations 管理サーバー M2 に送信するように HPOM を設定する方法を示しています。Follow-the-sun 機能を利用して対応する地域に日中業務シフトを割り当てることで、1 日 24 時間の環境全体を制御できます。

図 5-2　時刻またはメッセージ属性に応じたメッセージ転送



たとえば、24 時間対応の一元的なサポートデスクを中央に設置する場合、HPOM を使用して、営業時間外の地域の管理対象ノードから中央の管理サーバーにメッセージを直接送信できます。Follow-the-sun ポリシーを導入するには、設定ファイル `allnodes` に 2 つのエントリを追加する必要があります。

この 2 つのエントリの形式は、たとえば、次のようになります。

```
CONDITION TIME 6am-6pm SEND TO $OPC_PRIMARY_MGR
CONDITION TIME 6pm-6am SEND TO MC
```

注記

別の管理サーバーへのメッセージの送信には、変数 `$OPC_PRIMARY_MGR` を使用します。この属性は、時間帯に応じて異なるシステムを指定できます。

Follow-the-Sun 管理のルールは、時刻に限定されません。曜日、特定の日付 (範囲)、頻度に応じて異なる管理サーバーにメッセージを送信するように設定することもできます。詳細については 343 ページの「時刻ポリシー」と *opcmom(4)* のマニュアルページを参照してください。

専門技術センター

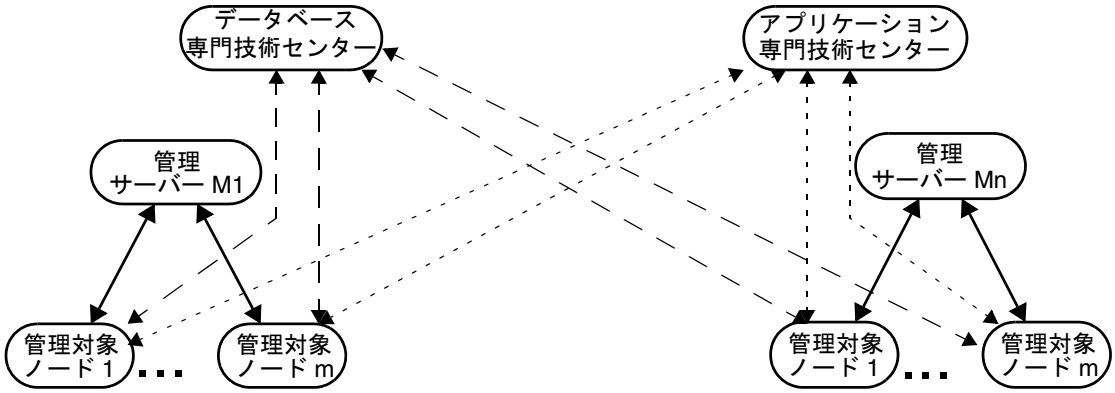
広範い地域に複数の管理サーバーが分散されている大企業では、特定分野の専門知識をローカル環境で常に利用できるとは限りません。このため、一次マネージャ以外のサーバーとの通信を行う管理対象ノードを設定しておくと便利です。ネットワーク上の他のサーバーでは、データベース管理やスプール管理など、コンピュータに関する専門知識を利用できるかもしれません。HPOM では、ネットワーク上の任意の場所にあるどの管理サーバーとも通信を行えるように、管理対象ノードを設定できます。

たとえば、オペレーティングシステムに関連するすべての障害に対応する技術センターが考えられます。これ以外に、企業全体で使用するデータベースを担当する技術センターも考えられます。管理対象ノードを適切に設定することで、オペレーティングシステムに関するメッセージを特定の技術センターに送信し、データベースの障害に関するすべてのメッセージを別の技術センターに送信できます。図 5-3 では、すべての管理対象ノードはデータベースに関連するすべてのイベントを管理サーバー M1 に送信します。

専門技術センター内の担当範囲の分散

メッセージのタイプによっては、図 5-3 に示されるような、専門技術センター指向のシンプルな階層のほうが、一元的な管理サーバーをベースとした階層よりも柔軟な環境を実現できます。

図 5-3　専門技術センター指向の環境における通信



一元的なサーバー階層とは異なり、専門技術センター指向の階層では、担当する管理対象ノードの範囲が分散されます。専門技術センター指向の階層では、管理対象ノードを担当するのは各地域のマネージャのみではありません。特定分野 (たとえば、データベース) に関するメッセージは、事前に定義されている管理サーバーに直接送信されます。この管理サーバーには、その分野に関連する、すべての管理対象ノードの問題を解決するための専門知識やスキルが蓄積されています。

専門技術センターの設定

次の概念的構文は、専門技術センターを導入する例を示しています。

```
IF MSGGRP=databases SEND TO Database Competence Center
IF MSGGRP=finance SEND TO Application Competence Center
IF MSGGRP=cad SEND TO Application Competence Center
```

注記

専門技術センターに関連する条件に時刻条件を追加することで、設定に Follow-the-sun ケーパビリティを追加できます。

バックアップサーバー

一般的なバックアップの構成では、2 つの HP Operations 管理サーバーが同じように設定されます。メインシステムは一次管理サーバーと呼ばれ、もう一方はバックアップサーバーと呼ばれます。

何らかの理由で一次マネージャが一時的にアクセス不能になった場合に、管理対象ノードからのメッセージを 1 つまたは複数の指定のバックアップ管理サーバーに転送するように HPOM を設定できます。

バックアップサーバーの設定

バックアップサーバーがこれらのメッセージに応答するには、一次マネージャで使用されている関連の設定とポリシーが必要です。つまり、一次マネージャで障害が発生する前に、関連の設定とポリシーを指定したバックアップサーバーおよびノードに配布しておく必要があります。さらに、特定のメッセージが特定のサーバーに送信されるように、各管理対象ノードに特定の時間帯と条件を設定する必要があります。

設定とポリシーの配布

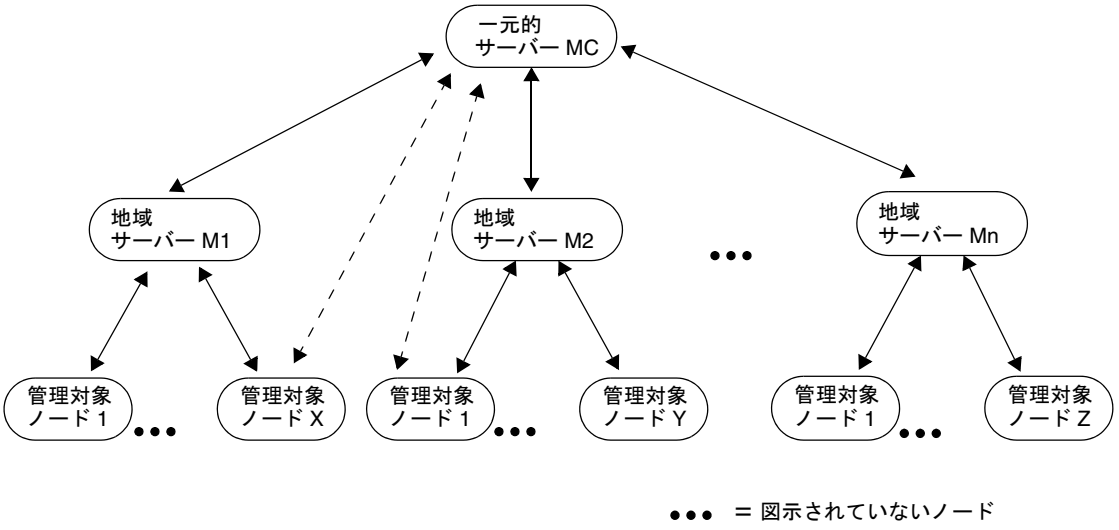
関連する設定とポリシーを、関連するすべての管理サーバーとノードに配布することで、一元的な製品開発を簡略化できます。一元的なサーバーで設定とポリシーを作成し、それを指定のサーバーおよび管理対象ノードに配布できます。

たとえば、本社でポリシーを作成し、そのポリシーを各支店の複製環境にインストールしたり、更新できます。HPOM では、このデータをファイルとしてダウンロードし、任意の数のサーバーにアップロードすることで、設定、ポリシー、ソフトウェアを配布できます。

管理階層

通常、図 5-4 に示されるような製造環境は、明確な管理階層を示します。環境の構造に手を加えることなく、マネージャ間の通信によって現行の担当範囲を利用できます。

図 5-4　一般的な製造環境と通信リンク



管理階層での管理プロファイル

図 5-4 に示される環境は、製造業では一般的です。企業は、地理的に分散した場所に複数の製造サイトを展開します。このような地理的な分散は、複製サイトの管理と比較することができます。通常、すべてのサイトには似通った管理プロファイルがあります。つまり、すべてのサイトの管理対象オブジェクト、ポリシー、エンドユーザーの担当範囲は類似しています。

管理階層内の設定比率

このような環境の規模にはばらつきがありますが、産業の種類に応じて、一般的な設定比率は次のようになります。

- ❑ 1 つの一元的管理サーバー
- ❑ 10 ～ 20 の地域管理サーバー
- ❑ HP Operations エージェントが稼働する 100 ～ 200 の管理対象ノード (サーバーおよびマルチユーザーシステム)
- ❑ SNMP イベントを送信する、最大で 5000 のその他の管理対象要素

ドメイン階層内での管理担当範囲

階層的な HPOM ドメインでは、それぞれの管理対象ノード上で HP Operations エージェントが実行され、システム自体とそのシステム上で実行されるアプリケーション (CAD、会計、データベースなど) の管理を行います。管理対象ノードは、地域管理サーバーにメッセージを送信します。特定の地域のすべての管理対象ノードの設定は同一です。

地域管理サーバー

地域管理サーバー (336 ページの図 5-4 では M1 ～ M*n*) では、HP Operations 管理サーバーソフトウェアとローカル HP Operations エージェントが実行されます。これらのサーバーは、各地域のシステムを制御します。通常、地域サイトは LAN (ローカルエリアネットワーク) 環境を管理し、高額な WAN (ワイドエリアネットワーク) トラフィックを使用しません。地域サイトを管理するオペレータは、管理対象ノードとアプリケーションを稼働させ続ける責任を負います。

一元的サーバー

一元的サーバーでは、地域管理サーバーシステムと、各システムで実行される管理アプリケーション (Data Protector、Performance など) を管理するための HP Operations 管理サーバーソフトウェアとローカル HP Operations エージェントが実行されます。

運営の面では、HPOM の一元的サイトのオペレータは、ヘルプデスクの専門技術者と比較できます。彼らは、地域レベルでは解決できない問題に対応します。管理の面では、一元的サイトは各地域サーバーの設定の作成、配布、管理を行います。アプリケーションに関する知識が一元化され、各地域の設定を均一化できるので、これは最も実用的な構成であるといえます。

管理対象サーバーの設定

一元的なサーバー環境では、管理対象ノードはすべての問題を所属している地域サーバーに報告します。地域管理サーバーは、すべてのエージェントの一次マネージャとして機能します。

アクション許容マネージャとしての一元的サーバーの設定

一元的なサーバー環境では、一元的サーバーは、すべてのエージェントの**アクション許容マネージャ**として設定されます。一元的サーバーをすべてのエージェントのアクション許容マネージャとして設定することで、一元的サーバーは分散している管理対象ノード上でアクションを実行できます。分散している管理対象ノードをこのように一元制御することで、一元的サーバーが担当範囲の切り替えを管理できるようになります。

特定地域のすべての管理対象ノードの設定は同一であるため、一元的サーバーをアクション許容マネージャとして設定することは、それほど難しいことではありません。HPOM 管理者が各地域管理サーバーで 1 つのファイルを設定するだけです。このファイルには、二次マネージャとアクション許容マネージャを指定するエントリが含まれます。

二次マネージャとしての一元的サーバーの設定

二次マネージャを指定するときは、一元的サーバーを二次マネージャとしても設定するようにしてください。これにより、一次マネージャに障害が発生した場合に、バックアップとして管理担当範囲を二次マネージャに切り替えることができます。

設定ファイルのサンプルが次のディレクトリに配置されています。

```
/etc/opt/OV/share/conf/OpC/mgmt_sv/tmpl_respmgrs
/hierarchy.agt
```

このファイルを使用するときは、必ず次のディレクトリにコピーして使用してください。

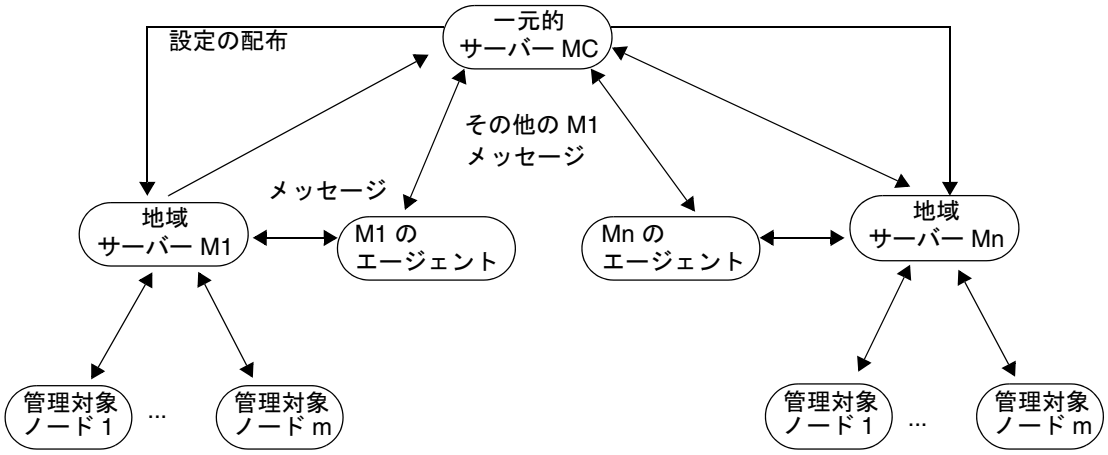
```
/etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs
```

HPOM の起動時に、ファイルはこのディレクトリから読み取られ、内容が実装されます。

一元的管理サーバーの設定

図 5-5 では、一元的管理サーバー (MC) は各地域管理サーバーシステム (M1 ～ M*n*) を管理対象ノードとして制御しています。メッセージを受け取るには、該当するすべてのノードを設定してオペレータに割り当てる必要があります。

図 5-5　一元的サーバーの設定と通信リンク



完全なマスター設定 (ノード、メッセージグループ、オペレータ、ポリシー) を一元的サーバーに保存しておくことには、いくつかのメリットがあります。HPOM の専門家を 1 か所に集めることができるので、各地域サイトの設定を一元的に作成して各サイトに配布できます。

担当マネージャの設定

HPOM では、担当マネージャ用に 1 つの設定を作成できます。設定を定義したファイルを作成し、それを一次管理サーバーの `respmgrs` ディレクトリに保存します。このファイルの名前は、環境で使用されている管理対象ノードによって決定されます。このテキストファイルは、メッセージがいつ、どこで、どのように送信されるかを定義します。

設定ファイルの作成

担当マネージャの設定ファイルには、次の項目を設定する必要があります。

- ❏ 一次および二次管理サーバー
- ❏ アクション許容管理サーバー
- ❏ 各種管理サーバーへのメッセージの送信に適用される日時ポリシー
- ❏ 各種管理サーバーへのメッセージの送信に適用されるメッセージ属性ルール

たとえば、ある環境のすべてのノードに設定が適用される場合は、すべてのノード用に 1 つの設定ファイルを作成し、`allnodes` という名前を付けます。設定が特定のノードのみに適用される場合は、そのノードの IP アドレスの 16 進表記をファイル名にします (`opc_ip_addr` コマンドで生成できます)。一部のノードの設定が共通している場合は、同一設定のノード固有ファイルへのリンクを作成できます。HPOM では、特定の設定ファイルを持たないノードには `allnodes` ファイルの設定が適用されます。

担当マネージャの設定ファイルの場所と設定手順については HPOM のオンラインヘルプ、または *opcmom(4)* のマニュアルページを参照してください。

注記

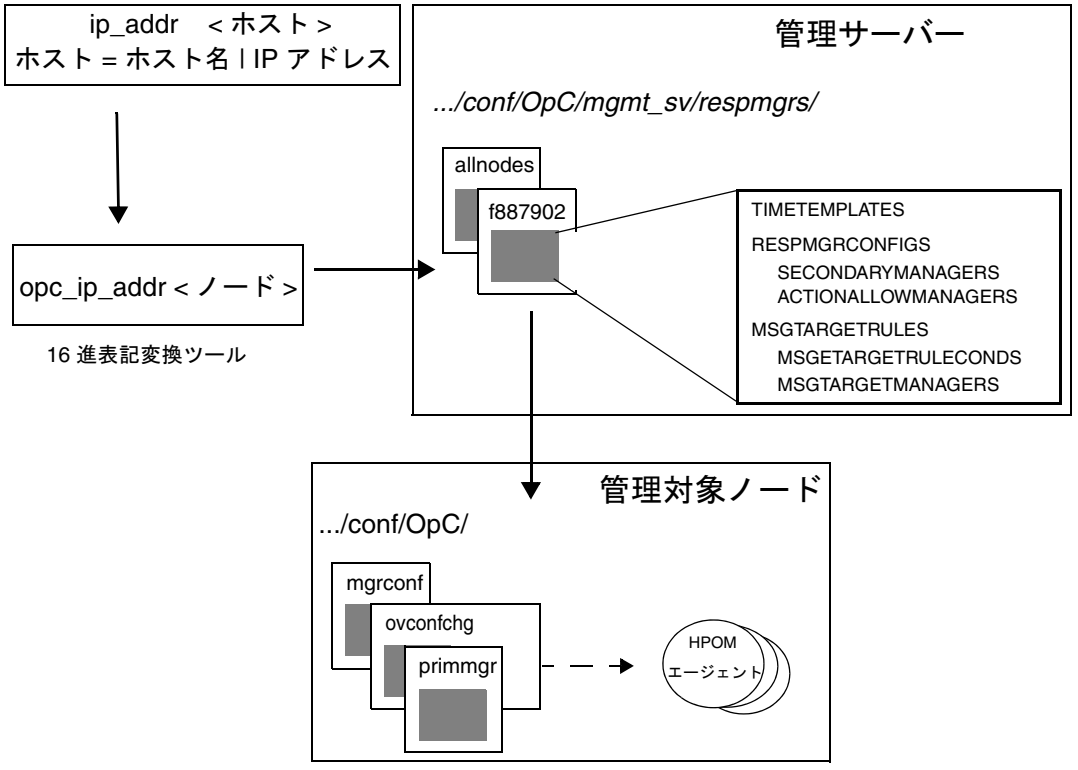
日本語環境でのフレキシブル管理の詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

設定ファイルの配布

HPOM では、管理対象ノードにポリシーを配布するときに設定が自動的に配布されます。同時に、HPOM は新しい、または更新された設定によってインテリジェントエージェントを初期化し直します。担当マネージャの設定ファイル mgrconf は管理対象ノードに配置されます。現在の一次マネージャのホスト名は primmgr ファイルに保存されます。primmgr が存在しない場合、HPOM は HTTPS ベースの管理対象ノード用の設定ツール ovconfchg を使用します。

341 ページの図 5-6 は、管理対象ノードの担当マネージャポリシーを示しています。

図 5-6　管理対象ノードの担当マネージャポリシー



メッセージターゲットルール

HPOM は、定義されている管理サーバーにメッセージを送信するかどうか、送信する場合はどのメッセージを送信するかを決定する際に、**メッセージターゲットルール**のリストを使用します。

メッセージターゲットルールの構成

メッセージターゲットルールは 3 つの部分から構成されます。

- ❏ メッセージ属性ルール
- ❏ 時刻ポリシー
- ❏ 定義されている管理サーバー

印刷グループのメッセージターゲットルールの例

印刷グループのメッセージターゲットルールの概念的な構造は次のとおりです。

メッセージグループ = “printing”

現在の時刻が *時刻ポリシー 2 に該当する .....(メッセージ) --> mgr 2*

現在の時刻が *時刻ポリシー 1 に該当する .....(メッセージ) --> mgr 1*

現在の時刻が *時刻ポリシー 3 に該当する .....(メッセージ) --> mgr 3*

この例では、ポリシー 1 の時刻条件と一致する、メッセージグループ「printing」のすべてのメッセージは HP Operations 管理サーバー 1 に転送されます。ポリシー 2 の時刻条件と一致するすべてのメッセージは HP Operations 管理サーバー 2 に転送されます。ポリシー 3 も同様に機能します。

データベースグループのメッセージターゲットルールの例

データベースグループのメッセージターゲットルールの概念的な構造は次のとおりです。

メッセージグループ = “database”

現在の時刻が *時刻ポリシー 1 に該当する .....(メッセージ) --> mgr 2*

現在の時刻が *時刻ポリシー 2 に該当する .....(メッセージ) --> mgr 3*

現在の時刻が *時刻ポリシー 3 に該当する .....(メッセージ) --> mgr 1*

この例では、ポリシー 1 の時刻条件と一致する、メッセージグループ「database」のすべてのメッセージは HP Operations 管理サーバー 2 に転送されます。ポリシー 2 の時刻条件と一致するすべてのメッセージは HP Operations 管理サーバー 3 に転送され、以下同様です。

時刻ポリシー

時刻ポリシーは、ある管理対象ノードが、特定の時刻に、どのメッセージを、どの管理サーバーに送信するかをエージェントに指定する条件 (ルール) セットです。時刻条件を作成し、それを時刻ポリシーに保存します。単純な条件を組み合わせて、たとえば、「1 月から 3 月の月、水、木曜日の午前 10 時～ 11 時 35 分」なような複雑な条件を設定できます。時刻条件には 24 時間表記を使います。したがって、午後 1 時を指定するには「13:00」と入力します。

時間間隔の設定

HPOM では、次のようにいくつかの異なる時間間隔を設定できます。

- **指定なし**

  特定の時刻、曜日、年などを指定しない場合、HPOM は条件が毎年、毎日、00:00 ～ 24:00 の範囲で満たされるものと仮定します。条件を指定した場合は、HPOM は指定されている日時の条件が継続的に適用されるものと仮定します。

  たとえば、条件として火曜日を指定すると、1 年を通じて毎週火曜日の 00:00 ～ 24:00 の範囲が毎年適用されます。

- **時間範囲**

  時間の範囲 (7:00 ～ 17:00 など) を指定します。

- **日付または期間のワイルドカード (*)**

  日付または期間をワイルドカード (*) で指定できます。たとえば、毎年の 1 月 31 日を条件として指定するには、「1/31/*」と入力します。

時刻に関係しないポリシーの設定

HPOM では、時刻に関係なく実行されるアクションの設定であっても、メッセージターゲットルールの時刻ポリシーを設定する必要があります。時刻に関係のないポリシーを設定するために、HPOM には変数 OPC_ALWAYS が用意されています。

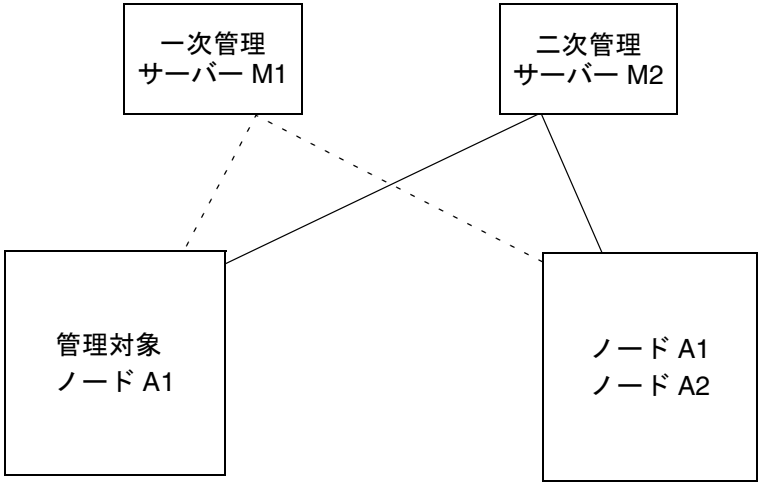
一次マネージャの指定

デフォルトでは、すべてのメッセージは、最初に HP Operations エージェントソフトウェアのインストールに使用された HP Operations 管理サーバーに集約されます。デフォルトの設定では、HP Operations 管理対象ノードの管理は 1 つの HP Operations 管理サーバーによって行われます。ただし HPOM では、ノードの管理担当範囲を複数の HP Operations 管理サーバーに分散できます。

二次マネージャへの切り替え

一次管理担当範囲を二次管理サーバーに切り替えると、それまで一次管理サーバーによって管理されていた HP Operations ノードに対する担当責任は、二次管理サーバーに引き継がれます。

図 5-7　一次管理担当範囲の切り替え



二次管理サーバーで管理担当範囲の切り替えを行うには、opcragt -primmgr コマンドを使用します。このコマンドは、管理対象ノード (ホスト名または IP アドレス) またはノードグループ名のリストをパラメータとして受け付けます。詳細については *opcragt(1m)* のマニュアルページを参照してください。

注記

OPC_PRIMARY_MGR が設定されていない、または無効な場合は、MANAGER の設定によって HP Operations 管理サーバーが指定されます。「無効」とは、OPC_PRIMARY_MGR が二次マネージャまたはアクション許容マネージャとして指定されておらず、初期マネージャとしても指定されていない状態です。

OPC_PRIMARY_MGR はメッセージ関連の設定です。これは、指定された HP Operations 管理サーバーにメッセージを送信できるように、該当マネージャのポリシーのメッセージターゲットルールで使用される変数 $OPC_PRIMARY_MGR にマッピングされます。

二次マネージャによるアクション実行の有効化

担当するノードで二次マネージャがアクションを実行できるようにするには、設定ファイルにキーワードを追加する必要があります。

または、次の行を追加して、現在の *各*一次マネージャがアクション許容マネージャになれるようにします。

```
ACTIONALLOWMANAGER $OPC_PRIMARY_MGR
```

マネージャ切り替えの反転

新しい一次管理サーバーが一次管理担当範囲を放棄しても、一次管理担当範囲が自動的に元の一次マネージャに戻るわけではありません。一次管理担当範囲の切り替えを元に戻すには、元の一次管理サーバーを二次管理サーバーおよびアクション許容マネージャとして再設定し、opcragt -primmgr を使って手動で担当範囲を切り替える必要があります。

マネージャの担当範囲の委譲

HPOM インストールマネージャの担当範囲 (定期ポーリング、ライセンスカウントなど) は、*opchbp(1m)* または *opcsw(1m)* コマンドを使って一次サーバーに委譲できます。詳細については、それぞれのマニュアルページを参照してください。

バックアップマネージャへの切り替え

一次管理担当範囲の切り替えは、システム停止時、または工場全体の電源障害時のフェイルセーフ機構として機能します。たとえば、定期的なポーリングによって二次管理サーバーが一次管理サーバーの状態をモニターするように設定できます。一次管理サーバーでシステム障害が発生すると、二次管理サーバーは HPOM 管理者に通知します。HPOM 管理者は一次管理担当責任を二次 HP Operations 管理サーバーに切り替え、障害が発生した管理サーバーで管理されていたすべての管理対象ノードの制御を二次管理サーバーに担当させます。

アクション許容マネージャの指定

管理対象ノードでアクションを実行できるのは、そのノードの `mgrconf` ファイルに**アクション許容マネージャ**として定義されている管理サーバーのみです。したがって、特定のノードに対する一次管理サーバーとしての責任を引き継いだ二次管理サーバーも、担当するノードでアクション許容マネージャとして設定されている必要があります。設定されていない場合、そのノードでアクションを実行することはできません。

デフォルトでは、管理対象ノードでアクションを実行できる HP Operations 管理サーバーは、HPOM **インストールマネージャ**のみです。より柔軟な運営を行うため、HPOM では特定の管理対象ノードグループに対してアクションを実行できるように複数の HP Operations 管理サーバーを設定できます。

注記

一次マネージャは、アクション許容マネージャとして設定されている必要があります。該当するマネージャの設定に次の行を追加してください。

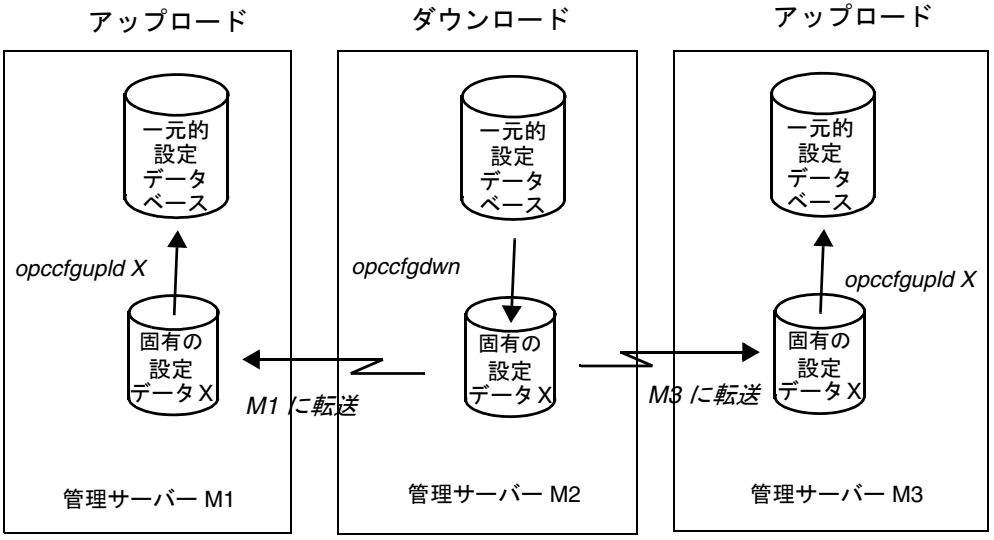
```
ACTIONALLOWMANAGER $OPC_PRIMARY_MGR
```

他のサーバーへの設定の配布

複製サイトとして機能する複数の HPOM ドメインから構成される環境では、設定を一元的に作成し、それを各種管理サーバーに配布する方法が便利です。たとえば、本社の HPOM 管理者が設定やアプリケーションを自分のサイトで定義し、他のサイトがアクセスして使用するファイルセットにそのデータをダウンロードします。

HPOM が設定ファイルを他のサーバーに配布すると、リモートサイトの管理者は、ファイルをデータベースにアップロードして使用できます。図 5-8 を参照してください。

図 5-8　設定ファイルのダウンロードとアップロード



他の管理サーバーへの設定の配布は、大きく分けて 3 つの手順で実行されます。

1. **設定の対象部分をダウンロードする**

   この情報はインデックスファイルに保存され、ダウンロードコマンド opccfgdwn の実行時に HPOM によって使用されます。設定タイプが同じであれば、ダウンロードに古い設定を再利用できます。

2. **ダウンロードしたファイルを配布する**

   ダウンロードしたファイルを別の HP Operations 管理サーバーに配布します。ローカル管理サーバーとリモート管理サーバーの間に信頼関係が確立されている場合は、次の手順で実行します。

   a. ダウンロードした設定を含む tar ファイルを作成します。

   b. コマンド行ツール ovdeploy を使って tar パッケージをリモート管理サーバーにセキュアにコピーします。次に例を示します。

   ```
   ovdeploy -upload -file config.tar -targetdir \
   /tmp -host remote.server.com
   ```

注記

管理サーバー間に信頼関係が確立されていない場合は、FTP、rcp、scp など、別の方法で行います。

3. **ファイルをデータベースにアップロードする**

   受信側の HP Operations 管理サーバーの管理者は、opccfgupld コマンドを使ってファイルをローカルデータベースにアップロードします。自動アップロードを行う場合は、**スケジュールアクション**を使ってアップロードをスケジューリングします。

注意

アップロード中に設定データ (ポリシー、オペレータなど) を変更しないでください。アップロードしているデータが破損する可能性があります。

管理者は、アップロードコマンド opccfgupld にオプション contents を指定することで、設定に含まれるデータを確認できます。その他のアップロードオプションの詳細については *opccfgupld(1m)* のマニュアルページを参照してください。

ローカル管理サーバーへの設定データのアップロード

設定データをファイルにダウンロードして他の管理サーバーへ配布したら、そのファイルをローカル管理サーバー上のデータベースにアップロードする必要があります。次のコマンドを使用して設定データをアップロードしてください。

`/opt/OV/bin/OpC/opccfgupld` < *アップロードディレクトリ* >

設定のアップロードについては 116 ページの「設定変更の同期」を参照してください。このコマンドのパラメータについては、*opccfgupld(1m)* のマニュアルページを参照してください。

注記

設定またはアプリケーションを HPOM に自動的にアップロードさせるには、`at` または `cron` を使って `opccfgupld` コマンドの実行をスケジューリングします。

管理サーバー間でのメッセージ転送

メッセージ転送は、ある HP Operations 管理サーバーから別の管理サーバーにメッセージを転送して障害の発生をそのサーバーに通知すると共に、転送されたメッセージに関連付けられているアクションをそのサーバーに実行させる機能です。関連性が考えられる別の管理サーバーにメッセージを伝えることで、柔軟性を向上させることを目的としています。さらに、HPOM ではメッセージの制御を 1 つの管理サーバーから別の管理サーバーに、または必要に応じて複数の管理サーバーに渡すことができます。ターゲット管理サーバーでは、転送されたメッセージは通常の HPOM メッセージと同様に処理されます。たとえば、設定によっては転送されたメッセージはメッセージストリームインタフェース (MSI) によって処理されます。また、トラブルチケットシステムや通知サービスに転送される場合もあります。

メッセージの転送

HPOM では、メッセージの転送は自動的に行われます。つまり、メッセージを転送するソース管理サーバーをポリシーで設定できます。ターゲット管理サーバーに転送されるメッセージは、ソース管理サーバー側の参照メッセージのコピーです。

メッセージの転送には、2 つの基本概念が適用されます。

- ❏ メッセージの制御の切り替え
- ❏ 通知メッセージの転送

メッセージの制御の切り替え

HPOM では、各メッセージは管理サーバー (`MSGCONTROLLINGMGR`) によって制御されます。メッセージの制御がソース管理サーバーから別のターゲット管理サーバーに切り替えられると、元のメッセージに関連付けられているすべてのアクションと操作がターゲット管理サーバーに渡されます。

メッセージの制御を切り替える理由

メッセージの制御を切り替えることで、通常はソース管理サーバーによって実行されるすべてのメッセージ関連アクションを、ターゲット管理サーバーが実行できるようになります。メッセージの制御は、さまざまな理由によって切り替えられます。たとえば、リソースをより均等に分散させる場合や、より広範囲の専門知識が得られるサーバーに制御を渡す場合などに行われます。

メッセージの制御の共有

制御が切り替えられたメッセージは、ソース管理サーバーの設定に応じて両方のサーバーによって制御されたり、ターゲットサーバーのみによって制御されます。

- **両方のサーバーによる制御**

  ソース管理サーバーがメッセージ制御マネージャとして定義されている場合、ターゲット管理サーバーとの間でメッセージの制御が共有されます。

- **ターゲットサーバーのみによる制御**

  ソース管理サーバーがメッセージ制御マネージャとして*定義されていない*場合、ソース管理サーバーにはメッセージの読み取り専用コピーが残されます。

制御が切り替えられたメッセージに対するユーザーの操作

管理者とオペレータは、制御が切り替えられたメッセージを通常のメッセージと同様に扱うことができます。

制御が切り替えられたメッセージに対して管理者とオペレータが実行できる操作は次のとおりです。

- 受諾
- 所有 / 所有解除
- オペレータ起動アクションの開始での使用
- 注釈付け

制御が切り替えられたメッセージに関連付けられているアクションの実行

ソース / ターゲットサーバーは、制御が切り替えられたメッセージに関連付けられているアクションを次のように実行します。

- ソース管理サーバー

  ソース管理サーバーは、制御が切り替えられたメッセージに関連付けられている自動アクションを実行します。ソース管理サーバーは、アクションステータスの変化をターゲット管理サーバーに通知することもできます。

- ターゲット管理サーバー

  一次マネージャでない場合、メッセージを生成した管理対象ノードでアクションを実行するには、ターゲット管理サーバーをアクション許容マネージャとして設定する必要があります。

通知メッセージ

通知メッセージは、HPOM がターゲット管理サーバーに転送する読み取り専用メッセージです。通知メッセージは情報目的専用であり、実行できる操作は限られています。通知メッセージを受信するターゲット管理サーバーは、必要に応じていくつでも定義できます。

通知メッセージに対するユーザーの操作

通知メッセージに対して管理者とオペレータが実行できる操作は次のとおりです。

- 受諾

  ソース管理サーバーでメッセージを受諾できます。もう一方の管理サーバー側のメッセージのコピーは受諾されません。

- 注釈付け

  メッセージに注釈を付けることができます。もう一方の管理サーバー側のメッセージのコピーにも情報が追加されます。

- 転送

  トラブルチケットおよび通知サービスにメッセージを転送できます。

注記

元のメッセージが手動で、または元のメッセージに関連付けられているアクションの正常な終了によって受諾されると、ターゲット管理サーバー上の通知メッセージは自動的に受諾されます。

通知メッセージに対して実行できない操作

通知メッセージに対して管理者とオペレータが実行 *できない* 操作は次のとおりです。

- ❏ 所有
- ❏ オペレータ起動アクションの開始

HPOM 管理者は、ソース管理サーバー上のポリシーを設定することで、通知メッセージの生成と、制御が別の管理サーバーに切り替えられるメッセージの生成を制御します。このポリシーの設定方法と、ポリシーの構文の詳細については、『*HPOM システム管理リファレンスガイド*』を参照してください。

メッセージ転送ポリシー

HPOM では、通知メッセージを生成し、メッセージ制御の切り替えを行う 1 つのメッセージ転送ポリシーを作成できます。このポリシーを、ソース管理サーバーに割り当てます。

メッセージ転送ポリシーには、次のような設定を含めます。

- ❏ **複数のターゲットサーバーへの転送**

  メッセージごとに複数のターゲット管理サーバーを指定できます。

- ❏ **メッセージ制御属性の転送**

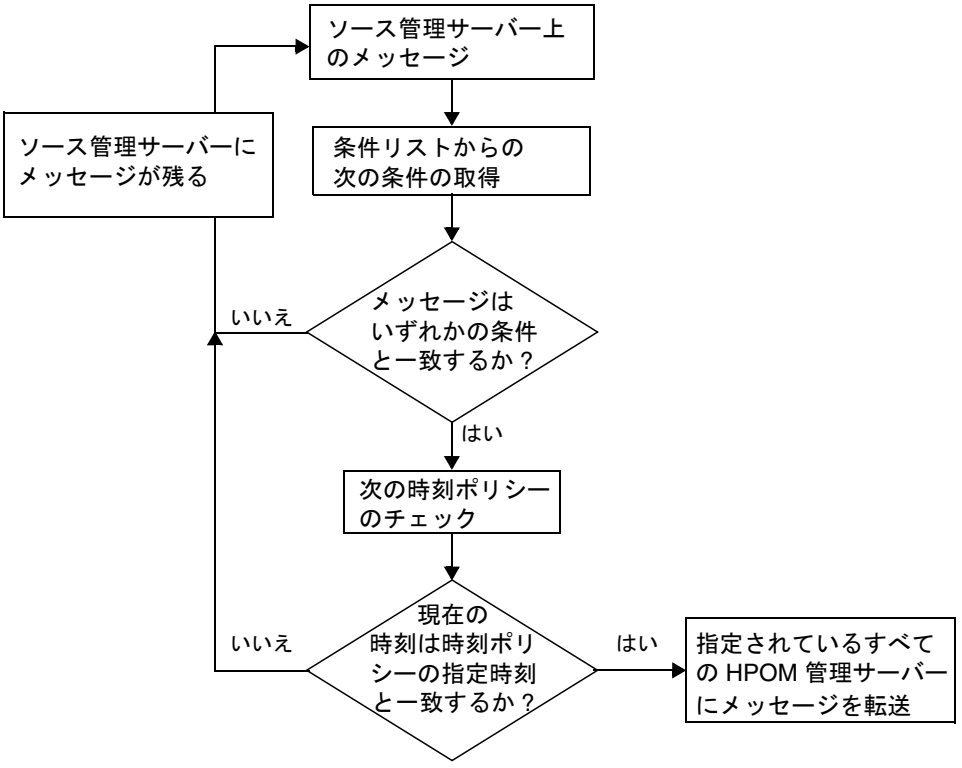
  メッセージの転送先となるターゲット管理サーバーでもメッセージの制御を切り替えることができるように、ターゲット管理サーバーに MSGCONTROLLINGMGR 属性を割り当てます。

- ❏ **直接受諾の強制**

  メッセージ条件ごとに ACKNONLOCALMGR 属性を指定し、ソース管理サーバーが通知メッセージを直接受諾するように強制できます。

ソース管理サーバーに着信するすべての新規メッセージは、転送アクションの実行前にチェックされます。354 ページの図 5-9 を参照してください。

図 5-9　　ポリシーチェックのプロセス



メッセージ配布リスト

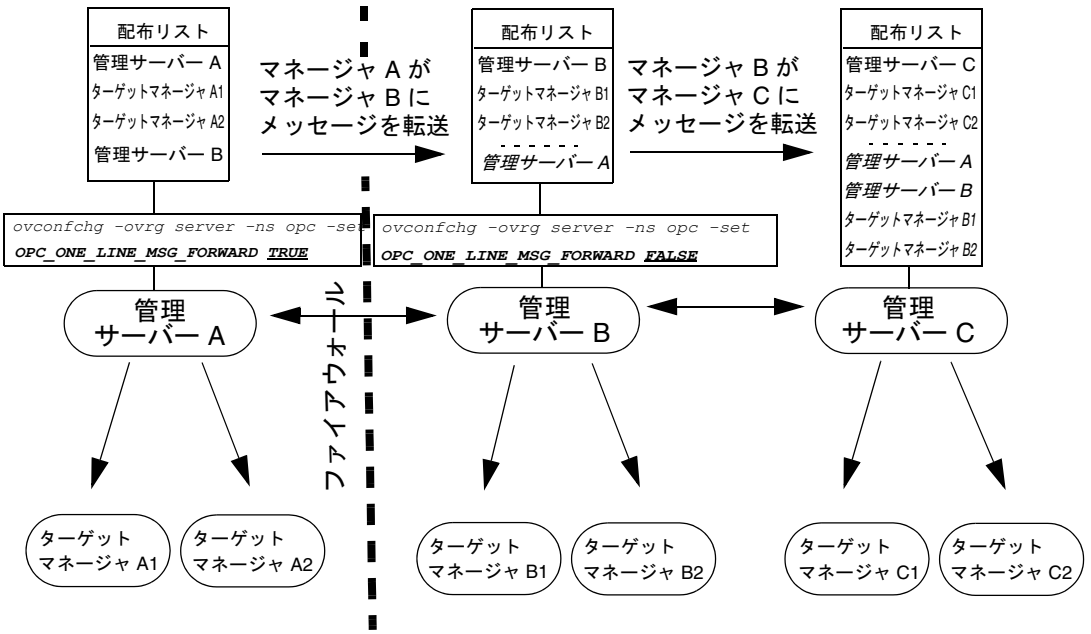
転送される各メッセージには、メッセージの送信側で認識されていた管理サーバーの配布リストが含まれます。この配布リストは、それ以後にメッセージに加えられる変更 (注釈の追加、アクションの実行など) をこれらのマネージャに通知する際に使用されます。転送されたメッセージを受信したターゲットマネージャは、メッセージに関連付けられている、そのターゲットマネージャに固有の管理サーバー配布リストにこのリストを追加します。

配布リストのサイズの制御

OPC_ONE_LINE_MSG_FORWARD パラメータを使用することで、メッセージが一連の管理サーバーに通知される間に膨張する配布リストのサイズを制御できます。

図 5-10 の例では、OPC_ONE_LINE_MSG_FORWARD の設定がデフォルトの FALSE である場合、管理サーバー B は、転送されてきたメッセージに関連付けることができる すべてのターゲットマネージャを、管理サーバー C に転送するすべてのメッセージに含めます。これらのマネージャは、サーバー C のメッセージ固有配布リストに追加され、管理サーバー C がそのメッセージに対応して何らかのタスクを実行する場合は、より大きくなった新しい配布リストが使用されます。このとき、サーバー B は必要なアクションを実行し、そのサーバー自体の配布リストと、サーバー C から受け取ったメッセージに含まれている配布リストを比較して、サーバー C から通知を受けていないターゲットのみに通知を行います。

図 5-10　大規模階層でのメッセージの転送



通常の状況であれば、このアプローチは高速であり、より効率的ですが、管理サーバー B の配布リストに指定されている 1 つまたは複数のターゲットマネージャが管理サーバー C に認識されていない (または到達できない) 場合は、メッセージ転送処理が失敗するという欠点があります。図の例では、管理サーバー B は管理サーバー A を認識しています。しかし、ファイアウォールが存在するため、管理サーバー C は管理サーバー A を*認識していません*。

ただし、管理サーバー A は管理サーバー C の配布リストに含まれているため、次のようになります。

- 管理サーバー A は変更を検知しません。
- 管理サーバー C は、管理サーバー A を起点として転送されてきたメッセージに対する変更を A に通知しようとしますが、失敗します。
- 管理サーバー B は、管理サーバー C から管理サーバー A に対して通知が行われたものと見なします。

図 5-10 で管理サーバー B の `OPC_ONE_LINE_MSG_FORWARD` の値を `FALSE` から `TRUE` に変更すると、管理サーバー B から管理サーバー C に転送されるメッセージに含まれる配布リストには、管理サーバー B 自体のみが追加されます。

管理サーバー B のみが追加されることで、転送されてくる同じメッセージに対して管理サーバー C が関連付けるリストは、図 5-10 の状態から次のように短縮されます。

- メッセージの送信者 (この場合は管理サーバー B)
- 管理サーバー C のターゲットマネージャ (ターゲットマネージャ C1、C2)

それ以後に管理サーバー C がメッセージに対応してタスクを実行する、または注釈を追加すると、その情報は管理サーバー C の配布リストに指定されている、短縮された管理サーバーリストのみに対して配布されます。管理サーバー B がメッセージの変更について管理サーバー C から通知を受け取ると、管理サーバー B は指定されているアクションを実行し、*管理サーバー B 自体*のメッセージ固有配布リストに指定されているサーバーに通知します。このアプローチの欠点は、通知を受けるサーバーのチェーンが直線的になり、結果としてチェーンが長くなって、ネットワークの設定や信頼性に応じて中断されやすくなることです。

注記

管理サーバー A と B の OPC_ONE_LINE_MSG_FORWARD を FALSE に設定すると、管理サーバー C の配布リストには、管理サーバー A と B が認識しているすべてのターゲット管理サーバーが含まれることになります。この場合、管理サーバー C のドメインでメッセージの状態に変化が生じると、管理サーバー C はリストに含まれるすべての管理サーバーへの通知を試みます。

管理サーバーとトラブルチケットシステムの接続

同じトラブルチケットシステムに複数の管理サーバーが接続する可能性があるため、複数の管理サーバーから同じトラブルチケットサーバーに同じメッセージが送信される場合があります。たとえば、あるメッセージのポリシーにトラブルチケットが指定されており、そのメッセージが別の管理サーバーに転送された場合は、このような状況が生じます。

注記

管理対象ノードからのメッセージでトラブルチケットが有効化されている場合、管理サーバーが受信すると、そのメッセージは直ちにトラブルチケットシステムに自動転送されます。ただし、HPOM ではパラメータ OPC_FORW_NOTIF_TO_TT (デフォルト設定は FALSE) および OPC_FORW_CRTL_SWITCH_TO_TT (デフォルト設定は TRUE) を使用して、メッセージの転送先となる管理サーバーでの、通知メッセージ / 制御切り替えメッセージのトラブルチケットシステムへの転送を制御できます。

転送されたメッセージの管理

メッセージ転送は、HPOM のフレキシブル管理の中核となる強力な機能です。メッセージの転送をどのように設定するかは、環境内でのメッセージのフローに直接影響します。メッセージ転送の方針を計画するときは、さまざまな事項を考慮する必要があります。

メッセージ転送方針の計画

メッセージ転送方針を計画する際に検討すべき事項は次のとおりです。

- ❏ **管理対象ノード**

  メッセージ転送に関わるすべての管理サーバーでは、それぞれの登録ノードですべての管理対象ノードが設定されている必要があります。

- ❏ **ターゲットマネージャ**

  制御切り替えメッセージに対応してオペレータ起動アクションを実行する場合は、メッセージの転送先ターゲットマネージャが、該当管理対象ノードでアクション許容マネージャとして定義されている必要があります。

- ❏ **メッセージの所有権**

  ある管理サーバーでメッセージを所有 / 所有解除した場合、すべてのオペレータがすべての管理サーバーに存在する場合にのみ、その他の管理サーバーのオペレータに通知されます。

  所有 / 所有解除イベントを管理サーバーに送受信させないようにするには、コマンド行ツール `ovconfchg` を使って管理サーバーに次の変数を設定します。

  - `OPC_SEND_OWN_DISOWN FALSE` (デフォルト設定は `TRUE`)
  - `OPC_ACCEPT_OWN_DISOWN FALSE` (デフォルト設定は `TRUE`)

  コマンド行ツール `ovconfchg` を使ってこれらの変数を設定する方法については *ovconfchg* のマニュアルページを参照してください。

❑ **重複メッセージ**

トラブルチケットサーバーに重複メッセージが送信されないようにするには、コマンド行ツール ovconfchg を使って管理サーバーにパラメータを設定します。詳細については 357 ページの「管理サーバーとトラブルチケットシステムの接続」、および HPOM のオンラインヘルプを参照してください。ovconfchg の使用方法については *ovconfchg* のマニュアルページを参照してください。

❑ **配布リスト**

メッセージの配布リストに不明な、または到達不可能な管理サーバーへの参照が含まれる場合、メッセージ転送処理の一部、または全体が失敗します。これらのサーバーが到達可能になるまで HPOM にメッセージをバッファリングさせるには、コマンド行ツール ovconfchg を使って変数 OPC_MSGFORW_BUFFERING (デフォルト設定は FALSE) を TRUE に設定します。ovconfchg の詳細については *ovconfchg* のマニュアルページを参照してください。

注意

メッセージのバッファリングは、管理サーバーの数が 2 つの環境のみで行ってください。配布リストに不明なサーバーへの参照が含まれる場合、メッセージはバッファリングされ続けます。詳細については 354 ページの「メッセージ配布リスト」を参照してください。

❑ **無限ループ**

メッセージ転送を実装するときは、サーバー間に無限ループが生じないように注意してください。

❑ **同一の指示**

同じメッセージのコピーが、異なる HPOM マネージャに表示されることがあります。メッセージに添付されている指示が確実に正しく表示されるには、管理サーバーでの指示インタフェースの設定を含め、同一の指示が必要です。指示を確実に同一にするには、管理サーバー A から指示をダウンロードし、それを管理サーバー B にアップロードするのも 1 つの方法です。

❑ **同期の問題**

制御の切り替えにより、一度に複数の管理サーバーが同じメッセージを担当することがあるため、次のような同期の問題が生じる可能性があります。

- *並行インスタンス*

  異なる管理サーバーのオペレータが同時に同じアクションを開始した場合、オペレータ起動アクションの複数のインスタンスが並行して生じる可能性があります。

- *早期の受諾*

  作業を行っているメッセージが、作業完了前に別の管理サーバーのオペレータによって受諾される可能性があります。

- *不要な注釈*

  自分で追加していないメッセージ注釈が追加される可能性があります。

- *転送されない注釈*

  オペレータ起動アクションの開始に関する注釈情報は、管理サーバー間で転送されません。この注釈には、アクションの開始時刻とアクション自体に関する情報が含まれます。

これらの問題を部分的にでも回避するには、メッセージに対して作業を開始する前に、そのメッセージを所有してください。

❑ **通信障害**

ソース管理サーバーとターゲット管理サーバー間で通信障害が発生すると、通信チェーン上のターゲット管理サーバーより先の各システムにも影響する可能性があります。メッセージがターゲット管理サーバーからすでにダウンロードされていたり、メッセージストリームインタフェースに出力されてしまった場合にも、同様の問題が生じることがあります。

メッセージ転送ポリシーに関する問題のトラブルシューティング

メッセージ転送ポリシーに問題や不整合が存在する場合、HPOM はエラーメッセージを生成し、ポリシーの残りの内容を無視します。また、ソース管理サーバーがターゲット管理サーバーに通知できない場合にも、HPOM はソース管理サーバーでメッセージを生成します。

原則として、HPOM は次の状況を検出するとエラーを生成します。

- ポリシーの設定が誤っている
- ネットワークに関連する問題が存在する
- リモート / ターゲット管理サーバーに到達できない
- ターゲット管理サーバーが転送メッセージを受信するように設定されていない

構成例

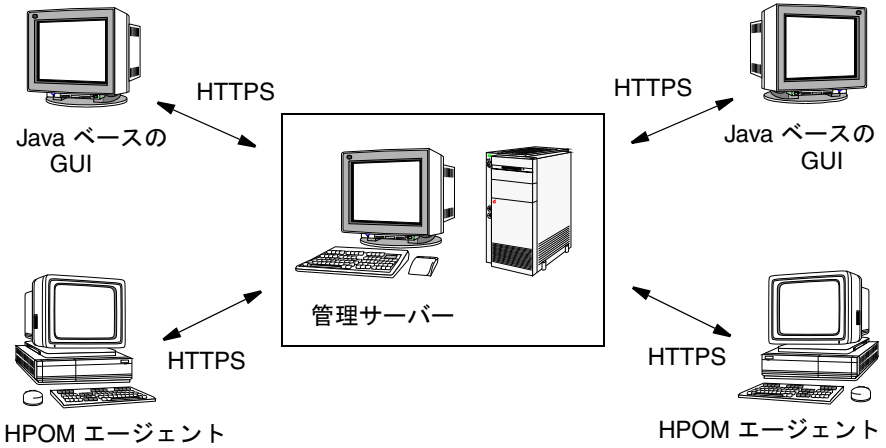
HPOM は、大規模かつ複雑な環境での運用を念頭に設計されています。HPOM のアーキテクチャは柔軟性に優れており、1 つまたは複数の管理システムを統合して、組織構成のニーズに見合った 1 つの強力な管理ソリューションを形成できます。

ここでは、いくつかの構成例を紹介します。これらの構成は、組織の特定のニーズに合わせて HPOM をスケーリングする方法を例示しています。シンプルなものから複雑なものまでさまざまな構成があるので、ニーズに適した構成を採用できます。また、複数の構成例を組み合わせて新しいソリューションを構築することもできます。

構成例 1: 単一サーバーによる複数ノードの管理

図 5-11 のシンプルな構成は、それぞれが HP Operations エージェントを実行している複数のリモートノードを管理する 1 つの HP Operations 管理サーバーを示しています。管理対象ノードと管理サーバーは、通信に HTTPS プロトコルを使用します。Java ベースのオペレータ GUI を使用して、複数のオペレータが共同で環境を管理できます。

図 5-11　単一管理サーバーによる複数ノードの管理



このシンプルなアーキテクチャは、一元的な場所から複数のリモートシステムを管理するための効率的なソリューションを提供します。

- **可変しきい値**

  SNMP MIB 変数とカスタム変数のしきい値をモニターします。

- **メッセージソース**

  各種メッセージソースを処理します。

- **ローカルイベント**

  管理対象ノード上でローカルイベントをフィルタリングします。

- **自動アクション**

  管理対象ノード上でローカル自動アクションを開始します。

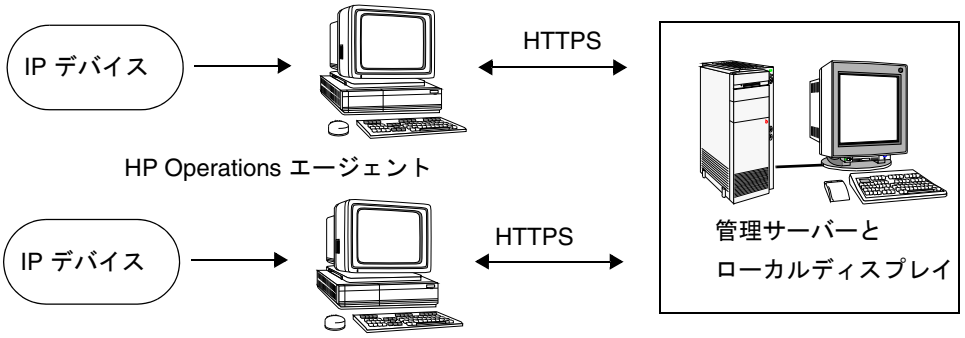
- **エージェントプラットフォーム**

  さまざまなエージェントプラットフォームに対応しています (HP-UX、Linux、AIX、Solaris、Windows など)。

構成例 2: HP Operations エージェントによる IP デバイスのモニター

図 5-12 は、HP Operations エージェントがプロキシエージェントとして機能し、リモート SNMP デバイスの SNMP しきい値をモニターする構成を示しています。この構成では、HP Operations エージェントが稼働するリモート管理対象ノードを使用して、ネットワーク上の他の SNMP 専用デバイスのしきい値をモニターできます。HP Operations エージェントはしきい値イベントをマネージャのみに転送するため、管理サーバーからの SNMP ポーリングは大幅に減少します。

図 5-12　　HP Operations エージェントによる IP デバイスのモニター



HPOM の標準機能の一部として、管理サーバーは次の処理も実行できます。

- **IP デバイスのマッピング**

  IP デバイスを自動的に検出し、マッピングします。

- **IP デバイスのポーリング**

  IP デバイスの IP ステータスをポーリングします。

- **SNMP トラップの受信**

  任意のデバイスからの SNMP トラップを受信します。

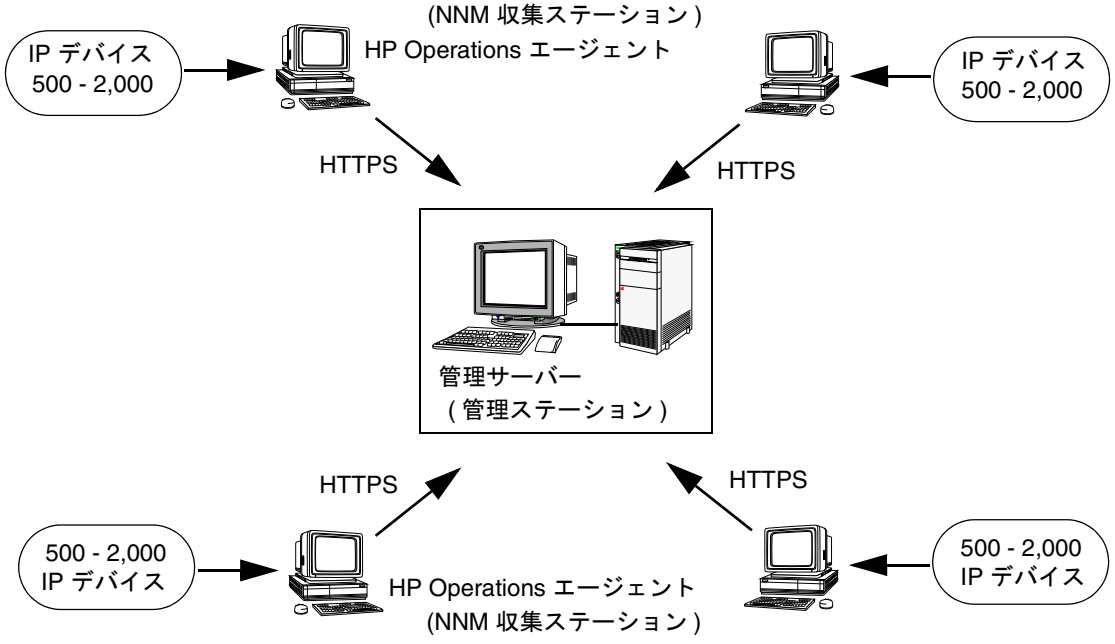
- **SNMP トレンドの収集**

  任意の SNMP デバイスから MIB 変数に基づく SNMP トレンドデータを収集します。

構成例 3: HP Operations エージェントが稼働する NNM 収集ステーション

図 5-13 は、管理対象ノードまたはデバイス以外に 1 つまたは複数の NNM 収集ステーションを一元的に管理する HP Operations 管理サーバーを示しています。各リモート NNM ステーションには、HPOM インテリジェントエージェントがインストールされます。

図 5-13　HP Operations エージェントが稼働する NNM 収集ステーション



この構成は、HP Operations 管理サーバーとリモート NNM システムの両方にメリットがあります。

一元的 HP Operations 管理サーバーのメリット

NNM 収集ステーションによって一元的 HP Operations 管理サーバーに提供されるメリットは次のとおりです

- ❑ **モニタリングの分散**

  トポロジ検出と IP ステータスモニターが分散されます。

- ❑ **収集の分散**

  SNMP データ収集が分散されます。

- ❑ **イベント転送**

  収集ステーションから管理ステーションに SNMP イベントが転送されます。

収集ステーションには、完全レベルとエントリレベルの*両方*の NNM ステーションを利用できます。

リモート NNM 収集ステーションのメリット

HP Operations 管理サーバーによってリモート NNM ステーションにもたらされるメリットは次のとおりです。

- ❑ **ステーションのモニター**

  リモート NNM 収集ステーションをモニターします。

- ❑ **ステーションの設定**

  NNM 収集ステーションのリモート設定には、次の設定が含まれます。

  - SNMP ポーリングの再試行とタイムアウト
  - データ収集としきい値
  - ロードされる MIB
  - SNMP イベントの転送設定

- ❑ **ステーションのロールの設定**

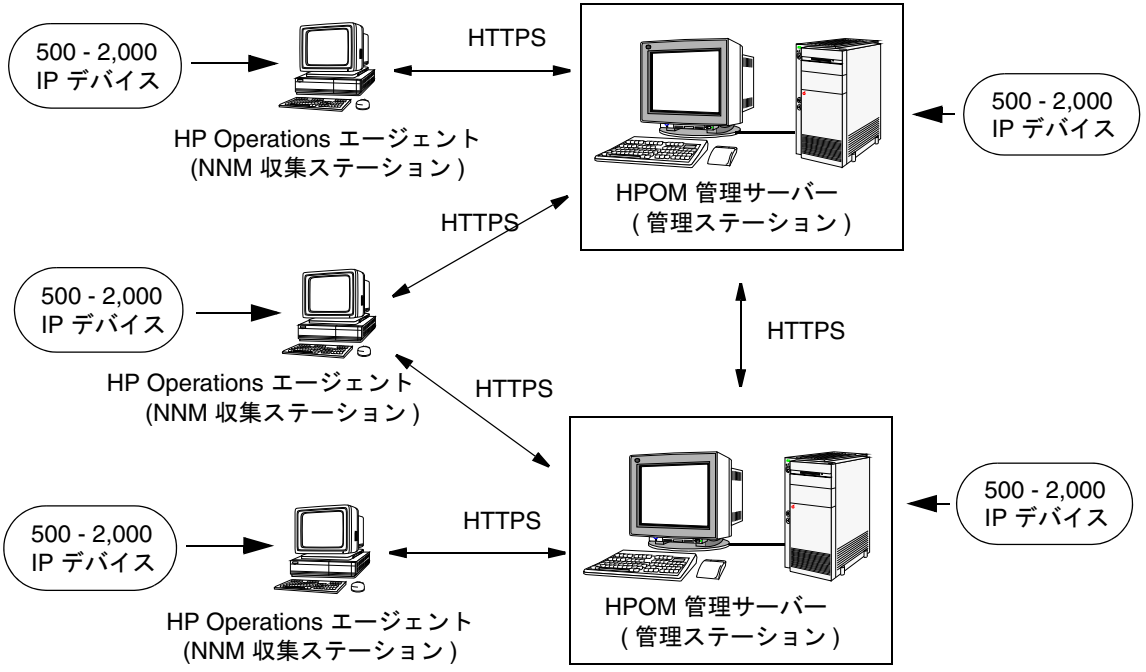
  リモート NNM 収集ステーションのロールを設定します (収集ステーションの追加、テスト、管理解除など)。

構成例 4: HP Operations エージェントが稼働する NNM 収集ステーションと複数の管理サーバー

図 5-14 の構成は、365 ページの「構成例 3: HP Operations エージェントが稼働する NNM 収集ステーション」に似ています。ただし、この構成では複数の HP Operations マネージャが並行して動作し、環境全体を管理しています。このソリューションは、構成例 3 より柔軟であり、よりスケーラブルです。

この構成は、複数の HP Operations マネージャと複数の NNM ステーションが連携して大規模なエンタープライズ環境を効率的かつ効果的に管理する例を示しています。

図 5-14　HP Operations エージェントが稼働する NNM 収集ステーションと複数の管理サーバー



複数の管理サーバーを使用することで得られるメリットは次のとおりです。

- **複数のマネージャ**

  一元的な HP Operations マネージャから複数の HP Operations マネージャを設定できます。

- **バックアップサーバー**

  障害が発生した管理サーバーから担当を引き継ぐバックアップサーバーを構成し、単一障害点を回避できます。

- **Follow-the-sun 管理**

  時刻に応じてメッセージを異なるマネージャにルーティングすることで、ピーク時に自動的にマネージャ間でタスクを委譲できます。

- **専門技術センター**

  メッセージのタイプに応じてメッセージを特定のマネージャにルーティングできます。このルーティングにより、特定の分野に関連するすべてのメッセージ (たとえば、データベースに関連するすべてのメッセージ) を受信する専門技術センターを構成できます。専門技術センターは、IT 管理に関する組織全体の情報とスキルを十分に活用する手段として効果的です。

A ポリシー本文の構文

概要

この付録では、デフォルトポリシータイプのポリシー本文の構文について説明します。デフォルトポリシータイプに含まれる内容は次のとおりです。

- オープンメッセージインタフェース (OPCMSG)
- ログファイルエントリ (LOGFILE)
- 測定しきい値 (ADVMONITOR)
- SNMP インターセプタ (SNMP)
- イベント相関処理 (ECS)
- スケジュール済みタスク (SCHED)
- サービスプロセスモニター (ADVMONITOR)
- Windows 管理インタフェース (WBEM)
- Windows イベントログ (LOGFILE)

次のポリシータイプの編集には、この付録で説明するポリシー本文の構文を利用できないので注意してください。

- サービス自動検出
- ノード情報
- 設定ファイル
- サブエージェント

ポリシー本文の構文

デフォルトポリシータイプを編集するためのポリシー本文の構文は次のとおりです。

```
file:           ε |
                SYNTAX_VERSION syntax_number |
                file logsource |
                file snmpsource |
                file csmsource |
                file monsource |
                file advmonsource |
                file schedsource |
                file ecsource |
                file wbemsource

syntax_number: 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11

logsource:      LOGFILE <文字列 (名前)> DESCRIPTION
                <文字列 (説明)> logdefopts conditions

snmpsource:     SNMP <文字列 (名前)> DESCRITPION
                <文字列 (説明)> snmpdefopts snmpconditions

csmsource:      OPCMSG <文字列 (名前)> DESCRIPTION
                <文字列 (説明)> csmdefopts conditions

monsource:      MONITOR <文字列 (名前)> DESCRIPTION
                <文字列 (説明)> mondefopts monconditions

advmonsource:   ADVMONITOR <文字列 (名前)> DESCRIPTION
                <文字列 (説明)> advmondefaults
                advmonsourcedef advmonconditions

schedsource:    SCHEDULE <文字列 (名前)> DESCRIPTION
                <文字列 (説明)> schedsetopts

ecsource:       ECS <文字列 (名前)> DESCRIPTION
                <文字列 (説明)> ecopts ecver CIRCUIT_FILE
                <文字列 (ファイル)> circuit

wbemsource:     WBEM <文字列 (名前)> DESCRIPTION
                <文字列 (説明)> wbemdefopts wbemconditions
```

ポリシー本文の構文

```
logdefopts:    ε | logdefopts logdefault | logdefopts
               logoption | logdefopts sourceoption

logdefault:    stddefault | NODE node

logoption:     LOGPATH <文字列（ログファイルへのパス）> |
               EXEFILE <文字列（実行するファイルへのパス）> |
               READFILE <文字列（ログファイルへのパスが記録されて
               いるファイルへのパス）> |
               INTERVAL <文字列（ログファイルチェックの間隔）> |
               CHSET <文字列（ログファイルの文字セット）> |
               FROM_LAST_POS |
               FIRST_FROM_BEGIN |
               NO_LOGFILE_MSG |
               CLOSE_AFTER_READ

snmpdefopts:   ε | snmpdefopts stddefault | snmpdefopts
               sourceoption

snmpconditions: ε |
               snmpconditions MSGCONDITIONS snmpmsgconds |
               snmpconditions SUPPRESSCONDITIONS
               snmpsuppressconds |
               snmpconditions SUPP_UNM_CONDITIONS
               snmpsupp_unm_conds

snmpmsgconds:  ε |
               snmpmsgconds DESCRIPTION <文字列（説明）>
               condsuppdupl condition_id CONDITION snmpconds
               SET sets

snmpsuppressconds: ε |
               snmpsuppressconds DESCRIPTION <文字列（説明）>
               condition_id CONDITION snmpconds

snmpsupp_unm_conds: ε |
               snmpsupp_unm_conds DESCRIPTION
               <文字列（説明）> condition_id CONDITION
               snmpconds
```

ポリシー本文の構文

```
snmpconds:      ε |
                snmpconds $e <文字列 (エンタープライズ)> |
                snmpconds $G <数字 (汎用トラップ)> |
                snmpconds $S <数字 (固有トラップ)> |
                snmpconds $(<数字 (変数)>) pattern |
                snmpconds NODE nodelist

csmdefopts:     ε | csmdefopts stddefault | csmdefopts
                sourceoption

mondefopts:     ε | mondefopts mondefault | mondefopts
                monoption | mondefopts sourceoption

mondefault:     stddefault | NODE node

monoption:      INTERVAL <文字列 (チェックの間隔)> |
                MONPROG <文字列 (モニター実行可能ファイルへの
                パス)> |
                MIB <文字列 (MIB 変数)> |
                MIB <文字列 (MIB 変数)> NODE node |
                EXTERNAL |
                MINTHRESHOLD |
                MAXTHRESHOLD |
                GEN_BELOW_THRESHOLD |
                GEN_BELOW_RESET |
                GEN_ALWAYS |
                AUTOMATIC_MSGKEY

monconditions: ε |
                monconditions MSGCONDITIONS monmsgconds |
                monconditions SUPPRESSCONDITIONS
                monsuppressconds |
                monconditions SUPP_UNM_CONDITIONS
                monsupp_unm_conds

monmsgconds:    ε |
                monmsgconds DESCRIPTION <文字列> condition_id
                CONDITION monconds SET sets

monsuppressconds: ε |
                monsuppressconds DESCRIPTION <文字列>
                condition_id CONDITION monconds
```

ポリシー本文の構文

```
monsupp_unm_conds: ε |
                   monsupp_unm_conds DESCRIPTION <文字列>
                   condition_id CONDITION monconds

monconds:          ε |
                   monconds THRESHOLD numval duration |
                   monconds RESET numval |
                   monconds OBJECT pattern

advmondefaults: ε | advmondefaults sourceoption |
                   advmondefaults stddefault | advmondefaults
                   NODE node | advmondefaults advmonoption

advmonoption:  INTERVAL <文字列（チェックの間隔）> |
                   INSTANCEMODE ALL | INSTANCEMODE SAME |
                   INSTANCEMODE ONCE |
                   MULTISOURCE |
                   INSTANCERULES |
                   AUTOMATIC_MSGKEY |
                   AUTOMATIC_MSGKEY <文字列（デフォルトメッセージ
                   キー）> |
                   MINTHRESHOLD |
                   MAXTHRESHOLD |
                   GEN_BELOW_THRESHOLD |
                   GEN_BELOW_RESET |
                   GEN_ALWAYS |
                   SCRIPTTYPE <文字列（スクリプトのタイプ）> |
                   DDF DATASOURCE <文字列> |
                   DDF OBJECT <文字列>
```

ポリシー本文の構文

```
advmonsourcedef: ε |
                 advmonsourcedef PROGRAM <文字列 (名前)>
                 DESCRIPTION <文字列 (説明)> advmonprog |
                 advmonsourcedef EXTERNAL <文字列 (名前)>
                 DESCRIPTION <文字列 (説明)> ddf |
                 advmonsourcedef NTPERFMON <文字列 (名前)>
                 DESCRIPTION <文字列 (説明)> advmonperfmon |
                 advmonsourcedef SNMP <文字列 (名前)>
                 DESCRIPTION <文字列 (説明)> advmonsnmp |
                 advmonsourcedef MEASUREMENT <文字列 (名前)>
                 DESCRIPTION <文字列 (説明)> advmonme |
                 advmonsourcedef CODA <文字列> DESCRIPTION
                 <文字列 (説明)> advmonme |
                 advmonsourcedef WBEM <文字列 (説明)>
                 DESCRIPTION <文字列 (説明)> advmonwbem

advmonprog:      MONPROG <文字列 (実行可能ファイルへのパス)> ddf

advmonperfmon:   OBJECT <文字列 (名前)> COUNTER <文字列>
                 INSTANCE <文字列> ddf

advmonsnmp:      MIB <文字列 (MIB 変数)> ddf

advmonme:        COLLECTION <文字列> metrics |
                 COLLECTION <文字列> GUID <文字列 (UUID)>
                 metrics |
                 DATASOURCE <文字列> COLLECTION <文字列 >
                 metrics

advmonwbem:      NAMESPACE <文字列> CLASS <文字列> ATTRIBUTE
                 <文字列> instancefilter ddf |
                 WMI_USERNAME <文字列> WMI_PASSWORD <文字列>
                 NAMESPACE <文字列> CLASS <文字列> ATTRIBUTE
                 <文字列> instancefilter ddf

instancefilter: ε | INSTANCE_FILTER <文字列>

ddf:             DDF DATASOURCE <文字列> OBJECT <文字列>
                 METRIC <文字列>

metrics:         ε |
                 metrics METRIC <文字列> metricguid
                 useforinstance
```

ポリシー本文の構文

```
metricguid:     ε | GUID <文字列 (UUID)>

useforinstance: ε | USEFORINSTANCE

advmonconditions: ε |
                advmonconditions tMSGCONDITIONS
                advmonmsgconds |
                advmonconditions tSUPPRESSCONDITIONS
                advmonsuppressconds |
                advmonconditions tSUPP_UNM_CONDITIONS
                advmonsupp_unm_conds

advmonmsgconds: ε |
                advmonmsgconds instancerule tDESCRIPTION
                <文字列 (説明)> condition_id CONDITION
                advmonconds advmonmsgsets

instancerule:   ε |
                INSTANCERULE <文字列> ID <文字列> |
                INSTANCERULE <文字列>

advmonmsgsets:  ε |
                advmonmsgsets SETSTART sets |
                advmonmsgsets SETCONT sets |
                advmonmsgsets SETEND sets

advmonsuppressconds: ε |
                advmonsuppressconds DESCRIPTION <文字列>
                condition_id CONDITION advmonconds

advmonsupp_unm_conds: ε |
                advmonsupp_unm_conds DESCRIPTION <文字列>
                condition_id CONDITION advmonconds

advmonconds:    ε |
                advmonconds THRESHOLD numval duration |
                advmonconds THRESHOLD condscript duration |
                advmonconds RESET numval |
                advmonconds RESET condscript |
                advmonconds OBJECT pattern |
                advmonconds OBJECT condscript

condscript:     SCRIPTTYPE <文字列> SCRIPT <文字列> |
                SCRIPT <文字列>
```

ポリシー本文の構文

```
duration:      ε | FOR <文字列 (条件の指定時間)>

numval:        <整数> | <浮動小数点数>

schedsetopts:  ε |
               schedsetopts DISABLED |
               schedsetopts TEMPLATE_ID <文字列 (ポリシーの
               UUID)> |
               schedsetopts VERSION <数字> |
               schedsetopts SCRIPTTYPE <文字列 (スクリプトの
               タイプ)> SCRIPT <文字列 (実際のスクリプト)> |
               schedsetopts SCHEDPROG <文字列 (実行可能ファイル
               へのパス)> |
               schedsetopts USER <文字列 (ユーザー名)> |
               schedsetopts USER <文字列 (ユーザー名)>
               PASSWORD <文字列 (パスワード)> |
               schedsetopts MONTH <文字列 (月)> |
               schedsetopts MONTHDAY <文字列 (日)> |
               schedsetopts WEEKDAY <文字列 (曜日)> |
               schedsetopts HOUR <文字列 (時間)> |
               schedsetopts MINUTE <文字列 (分)> |
               schedsetopts TIMEZONE_VALUE <文字列 (タイム
               ゾーン)> |
               schedsetopts YEAR <数字> |
               schedsetopts INTERVAL <文字列 (アクションの
               間隔)> |
               schedsetopts LOGLOCAL |
               schedsetopts SEND_OUTPUT |
               schedsetopts TIMEZONE_TYPE tz_type |
               schedsetopts BEFORE SET sets |
               schedsetopts FAILURE SET sets |
               schedsetopts SUCCESS SET sets

ecopts:        ε |
               ecopts DISABLED |
               ecopts TEMPLATE_ID <文字列 (ポリシーの UUID)> |
               ecopts VERSION <数字 (ポリシーのバージョン)> |
               ecopts ECS_LOG_INPUT |
               ecopts ECS_LOG_OUTPUT

ecver:         VERIFIED | UNVERIFIED
```

ポリシー本文の構文

```
circuit:        ε | circuit <文字列>

wbemdefopts:    ε |
                wbemdefopts wbemdefault |
                wbemdefopts wbemoption |
                wbemdefopts sourceoption

wbemdefault:    stddefault | NODE node

wbemoption:     NAMESPACE <文字列 (WBEM 名前空間)> |
                CLASS <文字列 (WBEM クラス)> |
                WITHIN <文字列 (間隔)> |
                WHERE_CLAUSE <文字列 (where 句)> |
                QUERY_LANGUAGE <文字列 (クエリ言語)> |
                QUERY <文字列 (クエリ)> |
                INSTANCE_CREATION_EVENT |
                INSTANCE_MODIFICATION_EVENT |
                INSTANCE_DELETION_EVENT |
                CLASS_CREATION_EVENT |
                CLASS_MODIFICATION_EVENT |
                CLASS_DELETION_EVENT |
                NAMESPACE_CREATION_EVENT |
                NAMESPACE_MODIFICATION_EVENT |
                NAMESPACE_DELETION_EVENT |
                INTERVAL <文字列 (間隔)>

wbemconditions: ε |
                wbemconditions MSGCONDITIONS wbemmsgconds |
                wbemconditions SUPPRESSCONDITIONS
                wbemsuppressconds |
                wbemconditions SUPP_UNM_CONDITIONS
                wbemsupp_unm_conds

wbemmsgconds:   ε |
                wbemmsgconds DESCRIPTION <文字列 (説明)>
                condsuppdupl condition_id CONDITION wbemconds
                SET sets

wbemsuppressconds: ε |
                wbemsuppressconds DESCRIPTION <文字列>
                condition_id CONDITION wbemconds
```

ポリシー本文の構文

```
wbemsupp_unm_conds: ε |
                wbemsupp_unm_conds DESCRIPTION
                <文字列（説明）> condition_id CONDITION
                wbemconds

wbemconds:      ε |
                wbemconds <文字列（条件名）> ~= pattern |
                wbemconds <文字列（条件名）> wbemop wbemval

wbemop:         == |  != | >= | > | < | <=

wbemval:        <文字列> | <数字（浮動小数点数）> |
                <数字（整数）>

condefopts:     ε |
                condefopts stddefault |
                condefopts sourceoption

conditions:     ε |
                conditions MSGCONDITIONS msgconds |
                conditions SUPPRESSCONDITIONS suppressconds |
                conditions SUPP_UNM_CONDITIONS supp_unm_conds

msgconds:       ε |
                msgconds DESCRIPTION <文字列> condsuppdupl
                condition_id CONDITION conds SET sets

suppressconds: ε |
                suppressconds DESCRIPTION <文字列>
                condition_id CONDITION conds

supp_unm_conds: ε |
                supp_unm_conds DESCRIPTION <文字列>
                condition_id CONDITION conds

condsuppdupl:  ε |
                SUPP_DUPL_COND suppdupl |
                SUPP_DUPL_IDENT suppdupl |
                SUPP_DUPL_IDENT_OUTPUT_MSG suppdupl
```

ポリシー本文の構文

```
conds:          ε |
                conds SEVERITY severities |
                conds NODE nodelist |
                conds APPLICATION <文字列> |
                conds MSGGRP <文字列> |
                conds OBJECT <文字列> |
                conds TEXT pattern

suppdupl:       <文字列> |
                <文字列> RESEND <文字列> |
                <文字列> COUNTER_THRESHOLD <数字> |
                <文字列> COUNTER_THRESHOLD <数字>
                RESET_COUNTER_INTERVAL <文字列> |
                <文字列> RESEND <文字列> COUNTER_THRESHOLD
                <数字> |
                <文字列> RESEND <文字列> COUNTER_THRESHOLD
                <数字> RESET_COUNTER_INTERVAL <文字列> |
                COUNTER_THRESHOLD <数字> |
                COUNTER_THRESHOLD <数字>
                RESET_COUNTER_INTERVAL <文字列>

stddefault:     SEVERITY severity |
                APPLICATION <文字列> |
                MSGGRP <文字列> |
                OBJECT <文字列> |
                SERVICE_NAME <文字列> |
                MSG_KEY <文字列> |
                HELPTEXT <文字列 (指示のテキスト)> |
                HELP <文字列 (指示の UUID)> |
                INSTRUCTION_TEXT_INTERFACE <文字列> |
                INSTRUCTION_PARAMETERS <文字列>
```

ポリシー本文の構文

```
sourceoption:  LOGMATCHEDMSGCOND | LOGMATCHEDSUPPRESS |
               LOGUNMATCHED | FORWARDUNMATCHED |
               UNMATCHEDLOGONLY | MPI_SV_COPY_MSG |
               MPI_SV_DIVERT_MSG | MPI_SV_NO_OUTPUT |
               MPI_AGT_COPY_MSG | MPI_AGT_DIVERT_MSG |
               MPI_AGT_NO_OUTPUT |
               MPI_IMMEDIATE_LOCAL_ACTIONS | ICASE |
               DISABLED |
               SUPP_DUPL_COND suppdupl |
               SUPP_DUPL_IDENT suppdupl |
               SUPP_DUPL_IDENT_OUTPUT_MSG suppdupl |
               SEPARATORS <文字列> |
               TEMPLATE_ID <文字列> |
               TEMPLATE_VERSION <数字>

severities:    ε | severities severity

severity:      Unknown | Normal | Warning  | Critical |
               Major | Minor

nodelist:      nodelist node | node

node:          IP <文字列 (IP アドレス)> |
               IP <文字列 (IP アドレス)> <文字列 (ノード名)> |
               OTHER <文字列 (変数その他)>

tz_type:       MGR_LOCAL | AGT_LOCAL | FIX

sets:          ε | sets set
```

ポリシー本文の構文

set: **SEVERITY** severity |
NODE node |
APPLICATION <*文字列（メッセージを関連付けるアプリケーション）*> |
MSGGRP <*文字列（メッセージグループ）*> |
OBJECT <*文字列（メッセージを関連づけるオブジェクト）*> |
MSGTYPE <*文字列（メッセージのタイプ）*> |
TEXT <*文字列（メッセージテキスト）*> |
SERVICE_NAME <*文字列（メッセージを関連付けるサービスの名前）*> |
MSGKEY <*文字列（メッセージキー）*> |
MSGKEYRELATION ACK pattern |
CUSTOM <*文字列（カスタム属性の名前）*>
<*文字列（カスタム属性の値）*> |
SERVERLOGONLY |
AUTOACTION action |
OPACTION action |
TROUBLETICKET acknowledge |
NOTIFICATION |
MPI_SV_COPY_MSG |
MPI_SV_DIVERT_MSG |
MPI_SV_NO_OUTPUT |
MPI_AGT_COPY_MSG |
MPI_AGT_DIVERT_MSG |
MPI_AGT_NO_OUTPUT |
MPI_IMMEDIATE_LOCAL_ACTIONS |
HELPTEXT <*文字列（指示メッセージのテキスト）*> |
HELP <*文字列（格納された指示メッセージの UUID)*> |
INSTRUCTION_TEXT_INTERFACE <*文字列（指示テキストインタフェースの名前）*> |
INSTRUCTION_PARAMETERS <*文字列（指示テキストインタフェースのパラメータ）*>

condition_id: ε | **CONDITION_ID** <*文字列 (UUID)*>

action: <*文字列（実行可能ファイルへのパス）*> actionnode annotate acknowledge msgsendmode signature

actionnode: ε | **ACTIONNODE** node

ポリシー本文の構文

acknowledge: ε | **ACK**

msgsendmode: ε | **SEND_MSG_AFTER_LOC_AA** msgsendok msgsendfailed

msgsendok: ε | **SEND_OK_MSG** logonly

msgsendfailed: ε | **SEND_FAILED_MSG**

logonly: ε | **LOGONLY**

signature: ε | **SIGNATURE** *<文字列（署名）>*

pattern: *<文字列>* separators icase

separators: ε | **SEPARATORS** *<文字列（セパレータ）>*

icase: ε | **ICASE**

chset: ε | **ASCII** | **ACP1250** | **ACP1251** | **ACP1252** | **ACP1253** | **ACP1254** | **ACP1255** | **ACP1256** | **ACP1257** | **ACP1258** | **NT_ANSI_JP** | **NT_OEM_JP** | **ACP874** | **NT_OEM_L1** | **NT_ANSI_LP** | **NT_OEM_US** | **NT_UNICODE** | **OEMCP437** | **OEMCP720** | **OEMCP737** | **OEMCP775** | **OEMCP850** | **OEMCP852** | **OEMCP855** | **OEMCP857** | **OEMCP860** | **OEMCP861** | **OEMCP862** | **OEMCP863** | **OEMCP864** | **OEMCP865** | **OEMCP866** | **OEMCP869** | **OEMCP932** | **ROMAN8** | **ISO8859** | **ISO88591** | **ISO885910** | **ISO885911** | **ISO885913** | **ISO885914** | **ISO885915** | **ISO88592** | **ISO88593** | **ISO88594** | **ISO88595** | **ISO88596** | **ISO88597** | **ISO88598** | **ISO88599** | **TIS620** | **UCS2** | **EBCDIC** | **SJIS** | **EUC** | **EUCJP** | **EUCKR** | **EUCTW** | **GB2312** | **BIG5** | **CCDC** | **UTF8**

ポリシー本文の構文

用語集

E

EC
メッセージ属性を参照。

F

Follow-the-sun
タイムゾーンに応じて担当範囲を複数の管理サーバーに分散させること。管理対象ノードは、管理者が定義した時刻属性に基づいて、設定されている管理サーバーにメッセージを送信します。 *フレキシブル管理も参照。*

G

GUI
Java GUI を参照。

H

HP アプリケーション
HPOM と統合されている HP アプリケーション。 *アプリケーション ; HP サービス ; HPOM アプリケーション ; HPOM 内部アプリケーションも参照。*

HP サービス
コマンド行ツール opcservice を使って HP Software から HPOM に統合されたスクリプト、プロセス、またはコマンド。アプリケーションとは異なり、サービスをシンボルから呼び出すことはできません。サービスは、自動的に、またはメニューバーから手動で呼び出されます。サービスはシンボルとして、またはグループシンボルに属す階層の一部として表されます。 *アプリケーション ; HP アプリケーション ; HPOM アプリケーション ; HPOM 内部アプリケーションも参照。*

HPOM アプリケーション
HPOM に統合されているアプリケーション。 *アプリケーション ; HP アプリケーション ; HP サービス ; HPOM 内部アプリケーションも参照。*

HPOM インストールマネージャ
HP Operations エージェントソフトウェアは、この管理サーバーから各管理対象ノードにインストールされます。デフォルトでは、この管理サーバーはエージェントの状態をモニターし、ライセンスをカウントします。 *アクション許容マネージャ ; 一次マネージャも参照。*

HPOM オペレータ
オペレータを参照。

HPOM 管理者
HPOM ソフトウェアのインストールと設定、運用方針の策定と管理、HPOM 以外のソフトウェアの維持、オペレータのワークスペースとスクリプトの設定を担当する管理者。管理者は、HPOM オペレータインタフェースのすべての機能にアクセスできます。管理者は、各オペレータの管理タスクと担当範囲に応じて完全にカスタマイズ可能な作業環境をオペレータごとに作成できます。 *opc_adm; オペレータ ; ユーザープロファイルも参照。*

HPOM 内部アプリケーション
ブロードキャストまたは仮想ターミナルタイプのアプリケーション。 *アプリケーション ; HP アプリケーション ; HP サービス ; HPOM アプリケーションも参照。*

HPOM パスワード
パスワードを参照。

HTTPS ベースの Java GUI
HTTPS プロトコルと SSL (Secure Socket Layer) 暗号化をベースとした、Java GUI と HP Operations 管理サーバーの間のセキュアな通信のためのソリューション。 *Java GUI も参照。*

J

Java GUI
Java グラフィカルユーザーインタフェース。 *オブジェクトペインも参照。*

M

manager-of-manager (MoM)
フレキシブル管理を参照。

MoM
manager-of manager。 *フレキシブル管理も参照。*

N

NNM
Network Node Manager。包括的なネットワーク管理ソリューションです。

O

opc_adm
HPOM 管理者。あらかじめ定義されている 3 種類の HPOM ユーザーの 1 つ。HPOM では、これがデフォルトの管理者です。 *opc_op; HPOM 管理者 ; ユーザー名も参照。*

OPC_NODES
オペレータの管理対象ノード、または管理者の登録ノード / 登録ノードグループで選択されているノードのリストを取得するために予約されている変数。ノードのホスト名は、HPOM アプリケーションに渡されます。

opc_op
HPOM オペレータ。あらかじめ定義されている 3 種類の HPOM ユーザーの 1 つ。オペレータは、システムの管理機能のみを制御します。オペレータがネットワークアクティビティを管理することはありません。オペレータは一部の UNIX ツール (Processes、Disk Space、Print Status など) を利用できます。 *opc_adm; オペレータ ; ユーザー名も参照。*

opcacta
アクションエージェントを参照。

opcactm
アクションマネージャを参照。

opcbbcdist
設定管理アダプタを参照。

opcctla
コントロールエージェントを参照。

opcle
ログファイルエンキャプスレータを参照。

opcmon (1|3)
アプリケーション / スクリプトがモニター値を HPOM のモニターエージェント (opcmona) に渡すときに使用されるコマンドおよび API。

opcmona
モニターエージェントを参照。

opcmsg (1|3)
アプリケーション / スクリプトが HPOM のメッセージテキストおよび属性を HPOM のメッセージインターセプタ (opcmsgi) に渡すときに使用されるコマンドおよび API。

opcmsga
メッセージエージェントを参照。

opcmsgi
メッセージインターセプタを参照。

opcmsgm
メッセージマネージャを参照。

opcuiwww
ディスプレイマネージャとの間でやり取りされるすべての通信リクエストを転送することで Java ベースのオペレータ GUI として機能するプロセス。Java ベースの各 GUI では、このようなプロセスが少なくとも 1 つ開始されます。

OV Control
「ovcd」。その他すべてのマネージャプロセスを開始 / 停止し、すべてのマネージャプロセスが稼働していることを確認する、管理サーバー上のプロセス。

ovcd
OV Control を参照。

ovoareqsdr
リクエスト送信者を参照。

S

SNMP
簡易ネットワーク管理プロトコル (Simple Network Management Protocol)。ネットワーク管理情報を拡張するために TCP/IP で実行されるプロトコル。SNMPv2C では、当初のプロトコルの機能が拡張されています。

SNMP トラップ
HPOM のメッセージソースの 1 つ。HPOM イベントインターセプタは、ネットワーク上のノードからトラップを収集してフィルタリングします。フィルタリングされたメッセージは、メッセージエージェントに転送されます。管理者は、トラップ用のポリシーを設定できます。ポリシーは、メッセージとパターンマッチのデフォルト設定、メッセージ条件、除外条件から構成されます。

あ行

アクション
メッセージソースポリシーまたは条件によって割り当てられる、メッセージに対する応答。この応答には、自動とオペレータ起動があります。 *自動アクション ; オペレータ起動アクションも参照。*

アクションエージェント
「opcacta」。管理対象ノード上でアクションを起動、制御します。アクションエージェントにはスクリプト、プログラム、アプリケーションがあります。 *エージェントも参照。*

アクション許容マネージャ
特定の管理対象ノードでアクションを実行できる、そのノードの管理サーバー。デフォルトでは、管理対象ノードでアクションを実行できる管理サーバーは、**インストールマネージャ**のみです。複数の管理サーバーが共通の管理対象ノードでアクションを実行できるように設定できます。 *HPOM インストールマネージャも参照。*

アクションマネージャ
「opcactm」。管理サーバーに常駐し、管理対象ノード上のアクションエージェントを制御します。オペレータ起動アクションまたはアプリケーションを実行する際に、ディスプレイマネージャによって呼び出されます。メッセージを生成した管理対象ノード以外のシステムで自動アクションを実行する場合は、メッセージマネージャによって呼び出されます。

アクティブメッセージブラウザ
メッセージブラウザを参照。

アプリケーション
1. シンプルなスクリプト、プロセス、またはコマンド。2. 多数のプログラムおよび設定ファイルを持つ複雑な製品。 *操作ビュー ; HP アプリケーション ; HP サービス ; HPOM アプリケーション ; HPOM 内部アプリケーションも参照。*

アプリケーションデフォルト
色やフォントなど、X ウィンドウアプリケーションデフォルトファイルにアクセスして変更できるデフォルト設定。 *opc(1) のマニュアルページも参照。*

暗号化
メッセージの傍受や改ざんを防ぐためのセキュリティオプション。このオプションを使用することで、認証された正当な関係者のみがメッセージを読むことができます。 *認証も参照。*

一次収集ステーション
オブジェクトのモニタリングに対して一次的な責任を負う収集ステーション。 *二次収集ステーションも参照。*

一次マネージャ
ある時点で HP Operations エージェントの管理を担当している管理サーバー。エージェントの起動 / 停止、新規ソフトウェアのインストール、エージェントへの設定の配布を実行できるのは、このサーバーのみです。このサーバーに関する情報は、`primmgr` ファイルに保存されます。このファイルが存在しない場合は、HPOM のインストールマネージャが HP Operations エージェントの管理担当サーバーとして機能します。HPOM は、HTTPS ベースの管理対象ノード用の設定ツール `ovconfchg` を使用してファイル名を抽出します。 *バックアップマネージャ ; HPOM インストールマネージャも参照。*

イベント
コンピューティング環境でメッセージの生成につながる事象が発生すること。通常、この事象はステータスの変化またはしきい値違反です。たとえば、用紙トレイが空になると、プリンタのステータスは変化します。

イベント相関処理
イベントストリームをリアルタイムに処理することでイベント間の関係を特定する相関処理。可能であれば、より有用で管理しやすい情報が含まれる、縮小されたストリームを新たに生成します。

イベント属性
メッセージ属性を参照。

エージェント
マネージャプログラムからリクエストを受け取り、情報の収集、処理の実行、応答の生成を行うことができるプログラム。 *アクションエージェント ; コントロールエージェント ; メッセージエージェントも参照。*

オブジェクト
HPOM によって管理されるリソースと関連機能 (ノード、アプリケーション、オペレータなど)。

オブジェクトペイン
管理対象環境内の各種要素を選択するための、Java GUI の上部にある 2 番目のペイン。
Java GUI も参照。

オペレータ
HPOM 管理者によって割り当てられた一連のノードおよびメッセージグループからのメッセージをモニターし、それに対応する HPOM ユーザー。これらのユーザーは、Java GUI メッセージブラウザおよびオブジェクトペインからタスクを実行します。あらかじめ定義されている 3 種類のオペレータの opc_op に該当します。 *opc_op; ユーザープロファイルも参照。*

オペレータ起動アクション
特定のメッセージに応じて実行される、修復または予防アクション。自動アクションとは異なり、これらのアクションはオペレータがクリック操作を行った場合にのみ開始されます。管理者はオペレータブラウザを使用できるので、管理者もこれらのアクションを開始できます。 *アクション; 自動アクションも参照。*

か行

外部ノード
HPOM ドメインの外部に存在するノード。これらのノードには、IP ノードだけでなく、あらゆる種類のノードが含まれ、通常の HPOM ノードの一部の機能のみを持ちます。これらのノードでは HP Operations エージェントは稼働していません。 *ノードグループも参照。*

仮想コンソール
仮想ターミナルを参照。

仮想ターミナル
直接物理接続ではなく、ネットワーク経由でリモートコンピュータ上で開かれるターミナルウィンドウ。HPOM では、あらかじめ設定されている、またはカスタマイズされたユーザー名 / パスワードを使ってリモートターミナルに接続できます。 *リモートログオン; 物理ターミナルも参照。*

簡易ネットワーク管理プロトコル (Simple Network Management Protocol)
SNMP を参照。

監査エントリ
データベースに書き込まれる、オペレータの操作 (アクションの実行、アプリケーションの起動、ログオン / ログオフなど) または管理者の操作 (設定など) を記したエントリ。これらのエントリのハードコピーはレポートとして印刷できます。

管理サーバー
ドメインの中心となるコンピュータシステム。ドメイン内のすべての管理対象ノードは、HPOM メッセージを管理サーバーに転送します。

管理対象ノード
HPOM によってモニターまたは制御されるコンピュータシステムまたはインテリジェントデバイス (ネットワークプリンタ、ルーターなど)。HP Operations エージェントは各ノードからの情報を収集、フィルタリング、処理し、管理サーバーに送信します。 *デフォルトターゲットノード; メッセージソース; ノード; ノードグループ; リモートノードも参照。*

起動属性
特定のアプリケーションのターゲットノード、アプリケーション呼び出し、アプリケーション呼び出しを実行するユーザー。これらの属性は、HPOM 管理者によってアプリケーションに事前に設定されます。

グラフィカルユーザーインタフェース
Java GUI を参照。

計画休止
コンピューティング環境内のサービスおよびシステムを利用できなくなる、あらかじめ予定されている期間。この期間中は、利用できないサービスおよびシステムからのメッセージは除外されるか、履歴データベースに直接移動されます。 ***ペンディングメッセージ; サービス時間; メッセージのバッファ解除も参照。***

コントロールエージェント
「opcctla」。各管理対象ノード上でその他すべてのエージェントの起動 / 停止、および管理サーバーからのリクエストの処理を担当するエージェント。起動時、またはリクエスト送信者から配布リクエストを受信した後に、このエージェントは管理サーバーから新しい設定データを収集する配布エージェントを起動します。 ***エージェントも参照。***

さ行

サービス
HP サービスを参照。

サービス時間
1. ヘルプデスクの要員が配置されている時間帯。この時間帯は、顧客とのサービスレベル契約で定義されます。2. HPOM ノードからのメッセージが HPOM オペレータに転送される時間帯。この時間帯以外に生成されたメッセージは、メッセージが転送される次の時間帯になるまでバッファリングされます。3. サービスプロバイダがサービス (電子メール、印刷、SAP R/3、アウトソーシングなど) のサポートを行う時間帯。 ***ペンディングメッセージ; ペンディングメッセージブラウザ; オブジェクトペイン; メッセージのバッファ解除も参照。***

サービスレポート
指定した時間帯または任意の時点における HPOM 環境内のサービスのステータスの概要を示すレポート。これらのレポートは、HP Service Reporter によって生成されます。

しきい値モニター
障害を初期段階で検出するためにオブジェクトのしきい値をモニターすること。オブジェクトの値が一定期間以上しきい値から外れた場合は、オペレータにメッセージを送信できます。オペレータがこのメッセージに対応することで、システムの機能やエンドユーザーの作業に影響が生じる前に障害を解決できます。 ***モニターエージェントも参照。***

時刻ポリシー
時刻に関連するルールまたは条件。これらのルールまたは条件は、メッセージを対象とした条件の一部です。HPOM は、これらのルールに基づいて、どの時間帯に、どのメッセージを、どの管理サーバーに送信するかを決定します。システム管理者は時刻条件を作成し、それをポリシーに保存します。 ***ポリシーも参照。***

指示文インタフェース
管理者が、指定のオペレータに指示を表示するように外部プログラムを定義するためのインタフェース。使用する外部プログラムによっては、管理者はメッセージごとに異なる指示を表示できます。

システムリソースファイル
opc_op ユーザーの設定ファイル (/etc/passwd、/etc/group など)、およびシステムの起動時 / シャットダウン時に実行されるファイル。これらの設定ファイルは、手動で、または自動的に変更できます。

自動アクション
着信イベント / メッセージによって起動されるアクション。オペレータは関与しません。 *メッセージの受諾 ; オペレータ起動アクションも参照。*

重要度
特定のオペレータ環境での重要性に基づいて HPOM 管理者が割り当てるレベル。ノード、ノードグループ、またはメッセージグループを表すシンボルには、最高重要度のステータスレベルが割り当てられます。 *ステータスの伝播も参照。*

受諾
メッセージの受諾を参照。

受諾解除
メッセージの受諾解除を参照。

使用ライセンス (LTU)
使用者が入手したライセンス。LTU は、ライセンスを必要とする製品コンポーネントで使用されます。

除外条件
特定のソースからの特定のメッセージをフィルタリングするために HPOM 管理者が設定する条件。これらの条件を設定することで、管理者はメッセージがメッセージブラウザに送られないようにすることができます。除外されたメッセージは、管理対象ノード上でローカルにロギングできます。 *フィルター ; メッセージ条件 ; メッセージのグループ替え条件も参照。*

所有権
メッセージの所有権を参照。

所有権表示モード
所有している、またはマークしたメッセージを取り込むか、無視するかを決定するためのモード。このモードは、メッセージのステータスを生成する際に使用されます。ステータス伝播モードとステータス伝播なしモードがあります。 *ステータスの伝播も参照。*

所有状態
メッセージの所有権 ; 所有権表示モードを参照。

ステータスの伝播
特定の管理対象ノードまたはメッセージグループのステータス (重要度によって決定されます)。この重要度レベルのステータスは、その管理対象ノードまたはメッセージグループから送信される最高重要度のメッセージのステータスを反映します。 *所有権表示モード ; 重要度も参照。*

制御対象ノード
リモートログオンなど、HPOM のすべての管理 / モニター用ケーパビリティが適用される管理対象ノード。このノードでは、アクションを実行したり、アプリケーションを起動できます。

制御の切り替え
メッセージの担当をソース管理サーバーからターゲット管理サーバーに切り替えること。担当を切り替えると、元のメッセージに関連付けられているすべてのアクションと操作はターゲット管理サーバーに渡されます。ソース管理サーバーはメッセージの読み取り専用コピーを維持します。 *メッセージ転送；通知メッセージも参照。*

セッション
HPOM にログオンしている時間。HPOM にログオンすると HPOM セッションが開始され、ログオフすると終了します。

設定管理アダプタ
「opcbbcdist」。HP Operations 管理サーバーと HTTPS エージェントの間に存在し、既存のアクション、コマンド、モニターからインストルメンテーションを作成し、nodeinfo の設定を HTTPS ノードで使用される XPL 形式に変換します。

専門技術センター
データベースやオペレーティングシステムなど、管理システムの特定の分野に関する専門知識が集約された場所。これらのセンターが階層構造として構成される場合、管理対象ノードは特定の分野に関連するメッセージを、障害を解決するための専門情報が存在する指定の管理サーバーに送信するように設定されます。 *フレキシブル管理も参照。*

操作ビュー
操作ビューには、管理対象環境内のノードとアプリケーション、およびオペレータに割り当てられているメッセージグループの階層ツリー構造が表示されます。 *アプリケーション；メッセージグループ；ノードも参照。*

た行

注釈
メッセージ注釈を参照。

通知サービス
イベントの発生をオペレータに伝えるサービス。HPOM では、このサービスには Java GUI メッセージブラウザに表示されるメッセージに設定されている色と重要度レベルが含まれます。HPOM はメッセージを外部サービス (ブザーやポケットベルなど) に転送することもできます。

通知メッセージ
HPOM によってターゲット管理サーバーに転送される読み取り専用メッセージ。このメッセージは情報を伝達するためのものですが、限定的な操作セットが関連付けられています。 *制御の切り替え；メッセージ転送も参照。*

データストアサービス
分散環境で情報の保存に使用されるあらゆる保存メカニズム (メタデータ、持続性オブジェクト情報、履歴情報、トポロジ情報を保存するデータベースなど)。

デフォルトオブジェクト
オブジェクトを参照。

デフォルトターゲットノード
アプリケーションが起動される、またはコマンドのブロードキャスト先となるノードのリスト。このリストは管理者によって定義されます。管理者が、カスタマイズされた起動権限をオペレータに付与すると、オペレータは Java GUI からこのリストを変更できます。
管理対象ノード；ノードも参照。

な行

二次収集ステーション
オブジェクトをモニターするが、そのオブジェクトの一次収集ステーションとして指定されていない収集ステーション。 *一次収集ステーションも参照。*

二次マネージャ
二次管理サーバー。一次管理サーバーの管理担当範囲を二次管理サーバーに移行することができます。二次管理サーバーに担当範囲を移行すると、二次管理サーバーが一次管理サーバーになります。 *opcragt(1m) コマンドのマニュアルページも参照。*

認証
接続に関わる当事者のアイデンティティを検証するセキュリティ機能。 *暗号化も参照。*

ノード
ネットワーク上のコンピュータシステムまたはインテリジェントデバイス (ブリッジ、ルーターなど)。 *デフォルトターゲットノード; 管理対象ノード; 操作ビューも参照。*

ノード階層
ノードとノードレイアウトグループの階層的な構造を視覚的に表現したもの。各階層には、HPOM 環境に構成されているすべての管理対象ノードが含まれます。階層間の違いは、ノードがどのように構成されているかのみです。階層は HPOM ユーザーに割り当てられ、各ユーザーが担当する管理対象ノードを表します。HPOM のデフォルト階層は登録ノードです。

ノードグループ
オペレータが管理する内部 / 外部ノードの論理グループ。この論理グループに対し、管理者は一貫性のあるポリシーセットを適用します。1 つのノードは複数のグループに属すことができます。 *外部ノード; 管理対象ノードも参照。*

は行

パスワード
HPOM 管理者 / オペレータの一意の識別情報。この識別情報は、オペレーティングシステムにアクセスするためのパスワードとは関係ありません。 *ユーザー名も参照。*

パターンマッチ
メッセージを分類するための条件。これらの条件には、イベントと照合されるテキストパターンを含めることができます。照合の一致 / 不一致に応じて、HPOM がメッセージをどのように処理するかが決定されます。 *非該当メッセージも参照。*

バックアップマネージャ
別の管理サーバーを代替する管理サーバー (障害発生時など)。この場合、代替管理サーバーが一次管理サーバーとなります。通常は、代替されるサーバーと同じように設定されています。 *一次マネージャも参照。*

非該当メッセージ
メッセージ条件 / 除外条件と一致しないメッセージ。これらのメッセージは、ローカルにロギングするか、管理サーバーに転送できます。 *パターンマッチも参照。*

非管理対象ノード
特定のオペレータの環境から一時的に除外されているノード。エージェントプロセスは開始されず、これらのノードからの着信メッセージは無視されます。

ビュー
特定のデータベースまたはシステム用にユーザーが設定する表示。たとえば、フィルターを使用して、メッセージブラウザに表示するメッセージを定義できます。フィルタリング済みアクティブメッセージブラウザには、条件と一致するメッセージが表示されます。

フィルター
ノード上、または GUI 内で情報を変更、リダイレクト、または除外する、メッセージ条件によるスクリーニング機能。管理者は、このスクリーニング機能を利用してメッセージ条件 / 除外条件を定義し、さまざまなソースからのメッセージを収集します。 *メッセージ条件 ; 除外条件も参照。*

フィルタリング済みメッセージブラウザ
選択されたメッセージが表示される Java GUI メッセージブラウザ。このブラウザを使用することで、メッセージブラウザ全体ではなく、特定のメッセージのみを表示できます。 *履歴メッセージブラウザ ; メッセージブラウザ ; ペンディングメッセージブラウザも参照。*

物理コンソール
物理ターミナルを参照。

物理ターミナル
管理対象ノードに物理的に接続されているターミナル。このターミナルは、通常はシリアルインタフェースを使って接続されます。このターミナルを使用することで、ノードがネットワーク接続を利用できない場合でも、オペレータはノードの再起動などのタスクを実行できます。HPOM では、ターミナルへの汎用インタフェースのみが提供されます。 *リモートログオン ; 仮想ターミナルも参照。*

フレキシブル管理
管理対象ノードに対する責任を多数の管理サーバーに分散させることで、受信するメッセージの時刻、場所、内容に応じて、これらの管理対象ノードから各種管理サーバーにメッセージを送信できるようにすること。 *専門技術センター ; Follow-the-sun も参照。*

ブロードキャスト
指定された 1 つまたは複数の管理対象ノードへのコマンドの同時送信。Java GUI では、オペレータはオブジェクトペインのツールツリーからこれらのコマンドを送信します。

プロセス
プログラムファイルを実行すること。HPOM では、統合されているアプリケーションとスクリプト、管理サーバープロセス、エージェントプロセス、トラブルチケットサービスなどがプロセスに該当します。

プロパティシート
タブのクリックによって表示されるオプションで作業手順を示すポップアップウィンドウ。これらの手順は任意の順序で実行できます。

ペンディングメッセージ
定義されているサービス時間以外、または計画休止中に HP Operations 管理サーバーに着信するメッセージ。定義されているバッファ解除時間が経過するまで、これらのメッセージは Java GUI のフィルタリング済みペンディングメッセージブラウザに入れられます。メッセージのバッファ解除は、手動または自動で実行されます。バッファ解除されたメッセージはメッセージブラウザに移動します。受諾されたメッセージは、フィルタリング済み履歴メッセージブラウザに移動します。 ***オブジェクトペイン; サービス時間; メッセージのバッファ解除も参照。***

ペンディングメッセージブラウザ
定義されているサービス時間外に着信したためにバッファリングされているメッセージを表示するためのブラウザ。 ***履歴メッセージブラウザ; メッセージブラウザ; ペンディングメッセージ; サービス時間; フィルタリング済みメッセージブラウザも参照。***

ポリシー
1 つのメッセージソースのメッセージ条件と属性 (メッセージとメッセージが属すグループの重要度など) から構成されるルールセット。このルールセットは、メッセージに新しいメッセージ属性を適用する際にも使用できます。ログファイル `opcsmsg(1)` および `opcsmsg(3)`、モニター対象オブジェクト、SNMP トラップのルールを定義できます。 ***メッセージソースポリシー; ポリシーグループ; 時刻ポリシーも参照。***

ポリシーグループ
共通の特徴を持つポリシーの論理グループ。グループと階層を作成することで、管理者はポリシーの管理と、管理対象ノードまたはノードグループへのポリシーの割り当てを簡略化できます。 ***ポリシーも参照。***

ま行

メッセージ
管理対象オブジェクトのステータス、管理対象オブジェクトに関連するイベント、および管理対象オブジェクトの障害に関する、構造化された判読可能な情報。オブジェクトのステータスに応じて、この情報は Java GUI のアクティブメッセージブラウザ、フィルタリング済みアクティブメッセージブラウザ、フィルタリング済み履歴メッセージブラウザ、またはフィルタリング済みペンディングメッセージブラウザに表示されます。 ***メッセージ属性も参照。***

メッセージインターセプタ
「opcmsgi」。着信メッセージを受信するプロセス。opcmsg(1) コマンドと opcmsg(3) API を使用して、メッセージを HPOM に転送できます。また、条件を設定し、指定したメッセージタイプを取り込む、または除外することもできます。

メッセージエージェント
「opcmsga」。メッセージソースからメッセージを受信し、管理サーバーにメッセージを転送する、管理対象ノード上のエージェント。 ***エージェントも参照。***

メッセージキー
特定のイベントによって生成されたメッセージを識別するためのメッセージ属性 (文字列)。この文字列は、イベントの重要な特性を要約したものです。この文字列を使用することで、メッセージによって別のメッセージを受諾できます。また、この文字列を使用して重複メッセージを特定することもできます。 ***メッセージ属性も参照。***

メッセージ許容ノード
エージェントソフトウェアを実行していないノード。これらのノードが送信したメッセージは HPOM に受理されます。

メッセージグループ
同じタスクに属す、または同じ論理接続を持つメッセージのグループ (バックアップ / 出力タスクからのメッセージ、ポリシーが共通のメッセージなど)。 *操作ビューも参照。*

メッセージ条件
さまざまなソースからメッセージを取り込むために HPOM に設定されるフィルター。これらのフィルターによりメッセージが生成され、通常はメッセージブラウザに表示されます。メッセージソースポリシーは、一連のメッセージ条件 / 除外条件から構成されます。 *フィルター ; メッセージのグループ替え条件 ; 除外条件も参照。*

メッセージ所有モード
オペレータ / 管理者がアクションを実行する際の 3 種類のモードの 1 つ。オプション、強制、情報モードがあり、デフォルトは強制モードです。 *メッセージの所有権も参照。*

メッセージストリームインタフェース
HPOM の内部メッセージフローに外部アプリケーションからアクセスするためのインタフェース。外部の読み取り - 書き込み、読み取り専用、書き込み専用アプリケーションはこのインタフェースにアクセスし、追加のメッセージ処理を行うことができます。このインタフェースは、管理サーバーとエージェントで利用できます。インタフェースの機能を利用するには、インタフェースに付属する API セットを利用します。

メッセージソース
HPOM が管理するメッセージのソース (生成場所)。HPOM は、SNMP トラップ、しきい値モニター、HPOM メッセージコマンドインタフェースと API (`opcmsg(1|3)`)、HPOM モニターコマンドインタフェースと API (`opcmon(1|3)`)、イベント相関処理サービスなど、さまざまなソースからのメッセージを管理します。各ソースから生成されるメッセージを処理するために、HPOM 管理者はメッセージのデフォルト設定、メッセージ条件、除外条件から構成されるポリシーを定義します。 *ログファイルメッセージ ; 管理対象ノードも参照。*

メッセージソースポリシー
HPOM へのメッセージの取り込みを制御するポリシー。 *ポリシーも参照。*

メッセージ属性
1. 管理サーバーが受信したメッセージを管理者が分類するために使用する特徴。2. `OPCDATA_MSG` の数値フィールド。これらのフィールドは文字列形式で参照されます (たとえば、EC ノードのイベントタイプフィールド)。 *メッセージ ; メッセージキーも参照。*

メッセージターゲットルール
特定のメッセージをどの管理サーバーに送信するべきかを示す、管理対象ノード側の条件。これらの条件は、計画休止中 / サービス時間中に抑制またはバッファリングするメッセージをメッセージ属性または時刻に基づいて決定する際にも使用されます。これらの条件は、管理対象ノードの設定ファイル `mgrconf` に定義されます。

メッセージタイプ
メッセージをサブグループにソートするためのメッセージ属性。この属性を使用することで、相関処理ルールで参照できる、メッセージの詳細な差別化が可能になります。この属性は、HPOM にイベント相関処理エンジンが接続されている場合に特に便利です。

メッセージ注釈
自動的に、またはオペレータ / 管理者によって手動でメッセージに追加されるテキスト。このテキストは、障害を解決するために実行されたアクションを説明します。テキストは、複数の行 / ページで構成できます。オペレータ / 管理者は、メッセージに複数の注釈を追加できます。

メッセージ転送
ある管理サーバーから別の管理サーバーへのメッセージのコピー。別のサーバーにメッセージをコピーした後に、管理者はイベントについてコピー先のサーバーに通知するか、メッセージの制御をコピー先のサーバーに切り替えることができます。 *制御の切り替え ; 通知メッセージも参照。*

メッセージのグループ替え条件
操作環境に定義されるメッセージ管理ポリシー内の条件。この条件を使用することで、管理サーバー上のメッセージをグループ化し直すことができます。たとえば、HP-UX のメッセージグループを組み合わせ、オペレーティングシステムメッセージの新しいグループを作成できます。 *メッセージ条件 ; 除外条件も参照。*

メッセージの重要度
重要度を参照。

メッセージの受諾
メッセージブラウザから履歴データベースへのメッセージの移動。履歴データベース内のメッセージは、Java GUI のフィルタリング済み履歴メッセージブラウザで表示できます。通常、メッセージは、生成の原因となった障害またはイベントがアクションによって解決された後に履歴データベースに移動されます。 *自動アクション ; メッセージの受諾解除も参照。*

メッセージの受諾解除
履歴データベースから Java GUI のアクティブメッセージブラウザ (受諾前にメッセージが配置されていた場所) へのメッセージの移動。メッセージはフィルタリング済み履歴メッセージブラウザには表示されなくなりますが、フィルタリング済みアクティブメッセージブラウザで表示できるようになります。受諾解除できるのは、履歴メッセージブラウザ上のメッセージのみです。 *メッセージの受諾も参照。*

メッセージの所有権
オペレータ / 管理者がメッセージに関連付けられているアクションを実行するために、そのメッセージの担当を引き受けることを示します。これは、情報モードでのメッセージへのマーク付けの概念に似ています。 *メッセージマーク ; メッセージ所有モードも参照。*

メッセージのバッファ解除
フィルタリング済みペンディングメッセージブラウザからフィルタリング済みアクティブメッセージウィンドウへのメッセージの移動。これにより、メッセージを変更できるようになります。 *ペンディングメッセージ ; オブジェクトペイン ; サービス時間も参照。*

メッセージブラウザ
管理サーバーが受信したメッセージをユーザーが表示するためのユーザーインタフェースの一部。このブラウザを使用して、ユーザーは障害を検出し、メッセージを表示 / 受諾し、障害管理アクティビティを特定します。 *履歴メッセージブラウザ; ペンディングメッセージブラウザ; フィルタリング済みメッセージブラウザも参照。*

メッセージへのマーク付け
メッセージの所有権を参照。

メッセージマーク
オペレータ / 管理者がメッセージに注意していることを示します。この概念は情報モードのみで利用されます。これは、強制モードでのメッセージの所有権の概念に似ています。*メッセージの所有権も参照。*

メッセージマネージャ
「opcmsgm」。管理サーバーで実行されるプロセス。このプロセスは、メッセージグループへの優先順位付け、注釈の追加、アクションの実行を行います。

モニターエージェント
「opcmona」。システムパラメータ (CPU の負荷、ディスク使用率、カーネルパラメータ、SNMP MIB など) を監視するプロセス。このプロセスは、あらかじめ定義されているしきい値と実際の値を比較します。しきい値から外れている場合はメッセージが生成され、メッセージエージェントに転送されます。HPOM 管理者はモニター対象オブジェクトのポーリング周期を設定できます。 *しきい値モニターも参照。*

モニター対象オブジェクト
HPOM によって定期的に読み取られるシステムパラメータ、データベースステータス、スプール情報などのオブジェクト。

モニター対象専用ノード
すべてのエージェントプロセスが開始されるが、アクションは実行されないノード。これらのノードを使用することで、厳しいセキュリティ要件を満たし、リモートログオン / アクションが制限されるシステムを構成できます。

や行

ユーザープロファイル
仮想 HPOM ユーザーの設定を定義するプロファイル。実際の HPOM ユーザーの設定は、あらかじめ設定されている 1 つまたは複数のプロファイルから取り込むことができます。*オペレータ ; HPOM 管理者も参照。*

ユーザー名
HPOM アプリケーションにとって一意の識別情報。これは、オペレーティングシステムの識別情報とは関係ありません。HPOM の GUI を使用するには、有効な HPOM ユーザーの名前とパスワードが必要です。HPOM は、HPOM の管理者 / オペレータに一意のユーザー名 `opc_adm`/`opc_op` を割り当てます。これらの名前を変更することはできません。その他のユーザー名の最大長さは 8 文字で、オペレーティングシステムのすべての制限が適用されます。 *opc_adm; opc_op; パスワードも参照。*

ら行

ライセンスキー
ライセンスキーには、ライセンス対象オブジェクトに関する情報と、そのキーのライセンス (LTU) の数が記録されています。ライセンス対象オブジェクトには、HP Operations 管理サーバーや HP Operations エージェントなどがあります。

ライセンスパスワード
ライセンス対象オブジェクトの 1 つまたは複数のライセンスに関する情報が含まれる一意の文字列。パスワードは、ライセンス (LTU) をインストールするためのライセンスパスワードリポジトリに追加されます。

リクエスト送信者
「ovoareqsdr」。管理サーバーから管理対象ノードにリクエスト (エージェントの起動 / 停止、定期ポーリングの設定など) を送信するプロセス。

リモートノード
通信リンクを使用するシステム。 *管理対象ノードも参照。*

リモートログオン
管理対象ノード以外の場所からの管理対象ノードへのアクセス。仮想ターミナルまたは物理ターミナルを開き、あらかじめ設定されている、またはカスタマイズされたユーザー名 / パスワードを入力することで、管理対象ノードにアクセスできます。 *物理ターミナル; 仮想ターミナルも参照。*

履歴メッセージブラウザ
受諾されたすべてのメッセージを表示する Java GUI ブラウザ。受諾されたメッセージを調べることで、過去に障害の解決に利用された方法を確認できます。 *メッセージブラウザ; ペンディングメッセージブラウザ; フィルタリング済みメッセージブラウザも参照。*

レポート
設定情報の要約。HPOM 管理者は、HPOM のレポートを出力したり、HPOM に含まれていないレポートを統合したりできます。

ログ専用メッセージ
管理サーバーで (設定によってはローカルに) ログに記録され、履歴データベースに送信されるメッセージ。このメッセージは履歴メッセージブラウザのみに表示されます。
log-on-management-server-only 属性は各メッセージ条件に個別に設定できます。条件でこのオプションが選択されている場合、その他のアクションを設定することはできません。

ログファイルエンキャプスレータ
「opcle」。管理対象ノードに常駐し、ログファイルポリシーを使用して、1 つまたは複数のアプリケーションログファイル / システムログファイルで管理者が指定したパターンと一致するメッセージをスキャンします。一致によってメッセージが生成される場合、そのメッセージはメッセージエージェントに転送されます。

ログファイルメッセージ
アプリケーションログファイル / サービスログファイルから生成されるメッセージ。ログファイルポリシーは管理者によって設定されます。これらのポリシーは、モニターオプション (ポーリング周期、処理ツール、文字セットなど)、およびログファイルエンキャプスレータがログファイルを読み取る方法を決定するメッセージ条件 / 除外条件から構成されます。生成されたメッセージは、ログファイルエンキャプスレータによってメッセージエージェントに転送されます。 *メッセージソースも参照。*

わ行

ワークスペース
オペレータが特定のタスク用に定義する、ワークスペースペイン上のタブ。通常のワークスペースには、メッセージブラウザ、チャート、履歴ラバランプ、アプリケーション出力、サービスグラフ、非 ActiveX ブラウザなどを表示できます。ActiveX ワークスペースに表示できるのは、ActiveX Web ブラウザのみです。 *ワークスペースペインも参照。*

ワークスペースペイン
Java GUI の上部にある 3 番目のペインで、オペレータが定義したワークスペースが表示されます。各ワークスペースには、メッセージブラウザ、アプリケーション出力ウィンドウ、グラフとチャート、Web ブラウザなどを表示できます。 *Java GUI; ワークスペースも参照。*