HP Operations Manager

コンセプトガイド

ソフトウェア バージョン: 9.20

UNIX および Linux オペレーティングシステム向け

ドキュメントリリース日: 2014 年 5 月 (英語版)
ソフトウェアリリース日: 2014 年 5 月

ご注意

保証について

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

Restricted Rights Legend.

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

著作権について

商標について

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

HP 9000コンピューターに搭載のHP-UX 10.20以降および11.00以降(32ビットおよび64ビット構成) はすべて、Open Group UNIX 95ブランドの製品です。

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、Oracle Corporationおよびその関連会社の登録商標です。

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

Oracleは、Oracle Corporationおよびその関連会社の登録商標です。

UNIX®は、The Open Groupの登録商標です。

1. HPOM の概要

2. HPOM の設定と保守

3. HPOM 管理対象ノードの概念

4. メッセージポリシーの設定

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

A. ポリシー本体の構文

ドキュメントの更新情報

このマニュアルの表紙には、以下の識別情報が記載されています。

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

更新状況、およびご使用のドキュメントが最新版かどうかは、次のサイトで確認できます。http://h20230.www2.hp.com/selfsolve/manuals

このサイトを利用するには、HP Passportへの登録とサインインが必要です。HP Passport ID の登録は、次の Web サイトから行なうことができます。http://h20229.www2.hp.com/passport-registration.html

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

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

サポート

HPソフトウェアサポートオンラインWebサイトを参照してください。
http://support.openview.hp.com

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

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

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

一部のサポートを除き、サポートのご利用には、HP Passportユーザーとしてご登録の上、サインインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。HP Passport IDを登録するには、次のWebサイトにアクセスしてください。
http://h20229.www2.hp.com/passport-registration.html

アクセスレベルの詳細については、次の Web サイトをご覧ください。
http://support.openview.hp.com/access_level.jsp

HP Software Solutions Now は、HPSW のソリューションと統合に関するポータルWebサイトです。このサイトでは、お客様のビジネスニーズを満たすHP製品ソリューションを検索したり、HP製品間の統合に関する詳細なリストやITILプロセスのリストを閲覧することができます。このサイトのURLはhttp://h20230.www2.hp.com/sc/solutions/index.jsp です。

HPOM ドキュメントの使用方法

HP Operations Manager (HPOM) では、製品の使い方と概念を理解し、効果的に使用できるように、マニュアルとオンライン情報を用意しています。ここでは、入手できる情報や情報の参照箇所を説明します。

電子メディアのマニュアル

HPOM のすべてのマニュアルは、次の Web サイトから Adobe Portable Document Format (PDF) ファイルとしてダウンロードできます。

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

この Web サイトにある『HPOM リリースノート』ドキュメントの最新版を定期的に調べてください。このリリースノートは 2 ～ 3 か月ごとにアップデートされ、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の情報が得られます。

HPOM 製品を限定したマニュアルも次の 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/

この例で、<management_server> は、お使いの HP Operations 管理サーバーの完全なホスト名であり、<lang> は、管理サーバーで設定されているシステム言語 (例、英語環境は C) です。

また、インストールと初期設定のプロセス終了後は、HP Operations 管理サーバーファイルシステムで、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/

- 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 Availability 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 Web サービス Perl ライブラリ:

  `/opt/OV/contrib/OprWsIncPerl/`

HPOM のマニュアルとオンライン情報

本項では、HPOM on UNIX と HPOM on Linux のマニュアルの概要、およびオンラインで利用できる情報 (すなわち、インストールと初期設定のプロセス終了後の HP Operations 管理サーバーに関する情報) について説明します。

表 1 は、最も重要な HPOM のマニュアルのリストです。対象となる読者、マニュアルの範囲と内容の簡単な説明が記載されています。

表 1　HPOM マニュアル

マニュアル名	対象者	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。このマニュアルは次の内容が記載されています。 • ソフトウェア、ハードウェアの必要条件 • ソフトウェアのインストール、削除手順 • 設定のデフォルト

表 1　　HPOM マニュアル (続き)

マニュアル名	対象者	説明
『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 の基本構造を理解できます。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 管理者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、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。
『HPOM Reporting and Database Schema』	管理者	HPOM データベースから生成されるレポートの例に加え、HPOM のデータベースの表の詳細を説明しています。
『HPOM Java GUI オペレータガイド』	管理者 オペレータ	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、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 管理 UI ヘルプ	管理者 オペレータ	HPOM 管理 UI オンラインヘルプの PDF 版です。
『HPOM リリースノート』	管理者	新機能を一覧表示されており、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。

表 1　　HPOM マニュアル (続き)

マニュアル名	対象者	説明
『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	HP Operations 管理サーバーの設定に使用する変数の一覧とその説明です。

表 2 は、利用可能な HPOM のオンライン情報のリストで、その内容の簡単な説明が記載されています。

表 2　　HPOM オンライン情報

オンライン情報	説明とアクセス方法
HPOM Java GUI のオンライン情報	Java ベースのオペレータ GUI と Service Navigator の HTML ベースのヘルプです。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。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。 • 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。 • 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。 • 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。 Java GUI のオンラインヘルプにアクセスするには次のようにします。 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**] を選択します。 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。

表 2　　HPOM オンライン情報 (続き)

オンライン情報	説明とアクセス方法
HPOM 管理 UI のオンライン情報	管理 UI の HTML ベースのヘルプです。このヘルプは、グラフィック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化します。管理 UI の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。 • HPOM for UNIX: このコンテキストでは、HPOM on UNIX と HPOM on Linux 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 : このコンテキストでは、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ブラウズが可能です。 • 管理 : このコンテキストでは、管理 UI にログインしている管理者ユーザー、管理 UI で管理しているサーバー、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 UI のオンラインヘルプにアクセスするには次のようにします。 1. 対応する Web ブラウザに次のいずれかの URL を入力して、管理 UI を起動します。 • 標準の接続 : **http://<management_server>:9662** • セキュアな接続 : **https://<management_server>:9663** この URL で、<management_server> は、お使いの HP Operations 管理サーバーの完全なホスト名です。 2. 管理者 UI にログオンします。デフォルトのユーザー名は opc_adm で、デフォルトのパスワードは OpC_adm です。 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、読みたいトピックを選択します。

表 2　　HPOM オンライン情報 (続き)

オンライン情報	説明とアクセス方法
HPOM マニュアルページ	HPOM マニュアルページはコマンドラインだけでなく、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 URL を入力してください。 • 標準の接続 : **http://<management_server>:8081/ITO_MAN** • セキュアな接続 : **https://<management_server>:8444/ITO_MAN** この URL で、<management_server> は、お使いの HP Operations 管理サーバーの完全なホスト名です。HP Operations Agent 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。

1 HPOM の概要

本章の内容

本章ではオペレータを対象として、HP Operations Manager (HPOM) の概念、機能、および構造を紹介します。

対象読者

本章は、HPOM オペレータを対象としています。

目的

本章では次の操作について説明します。

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

HPOM の概念

HP Operations Manager (HPOM) とは、あらゆる企業のシステム管理者がネットワーク、システム、アプリケーションで発生する問題の検出、解決、防止に便利に設計された分散型のクライアント / サーバーソフトウェアソリューションです。HPOM は、スケーラブルでフレキシブルなソリューションで、あらゆる IT 組織とユーザーの要件を満たすように設定できます。システム管理者は HPOM パートナーまたは他のベンダーからの管理アプリケーションを統合することによって、HPOM のアプリケーションを拡張できます。

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。

- ❏ **最大限のネットワーク**

  ネットワークコンポーネントの可用性を最大化する。

- ❏ **ダウンタイムの抑制**

  システムダウンによるエンドユーザーのロス時間を減らす。

- ❏ **作業負荷の低減**

  問題 (障害) の自動解決により、不必要なユーザーのアクションを減らす。

- ❏ **障害の予防**

  予防的なアクションにより、障害の発生件数を減らす。

- ❏ **問題解決の迅速化**

  問題解決に必要な時間を短くする。

- ❏ **コストの削減**

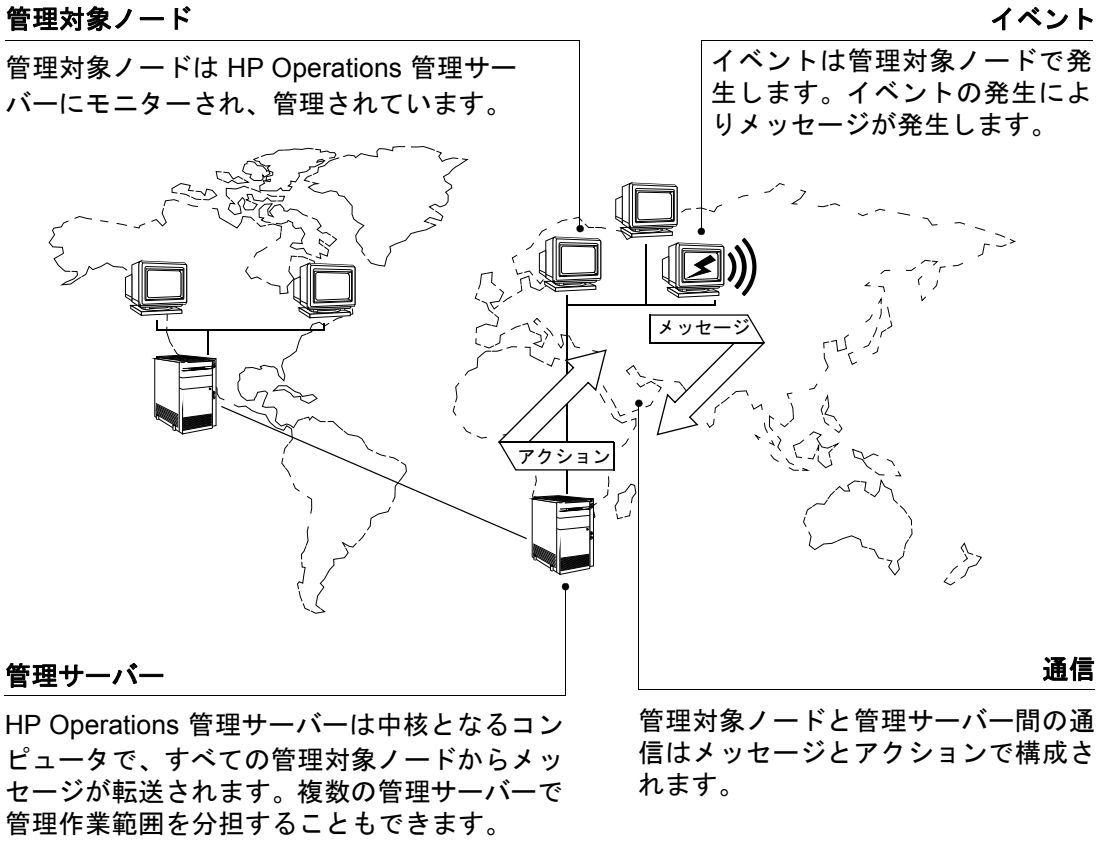
  クライアント/サーバー環境の管理コストを削減する。

クライアント/サーバーの概念

HPOM は、**管理サーバー**と**管理対象ノード**間の通信を使って管理します。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 Agent プロセス**と通信を行います。HP Operations Agent プロセスは管理対象ノードで**イベント**を収集して処理し、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。管理サーバーはこれに対応して、管理対象ノード上の問題を防止または解決するための**アクション**を起こします。

25 ページの図 1-1 は、HPOM による管理の概念を示します。

図 1-1　HPOM におけるクライアント/サーバーの概念



管理サーバー上のエージェントは、**ローカルな管理対象ノード**として管理する役割をします。

データベースは、すべてのメッセージと設定データのための集中データ保管庫として機能します。ここに記録された実行中のデータと過去の履歴データを使ってレポートを生成できます。履歴データは、同じような原因 (イベント) で起きた問題をオペレータが解決できるように指示 (instruction) を作成したり、特定の問題解決を自動化するのに便利です。データベースプロセスは管理サーバー上で実行します。

管理サーバー

管理サーバーは HPOM の中央処理機能を受け持ちます。管理サーバーには、現在の設定情報を含むソフトウェアパッケージ全体が格納されます。

管理サーバーには次の機能があります。

- **データ収集**

  管理対象ノードからデータを収集する。

- **メッセージ管理**

  メッセージの管理と分類を実行する。

- **アクション管理**

  次の処理を、特定のエージェントを呼び出し実行させる

  - アクションの開始

    管理対象ノード上でローカルな自動アクションを開始する。

  - セッションの開始

    管理対象ノード上でセッションを開始する。

- **履歴の管理**

  メッセージと実行済みアクションの履歴データベースを制御する。

- **メッセージの転送**

  他の管理サーバーや HPOM が動作しているシステムにメッセージを転送する。

- **ソフトウェアのインストール**

  管理対象ノードに HP Operations Agent ソフトウェアをインストールする。

管理サーバーは設定内容の変更を管理対象ノードに通知し、アップデートの開始も行います。

管理対象ノード

管理対象ノードとは、HPOM によって制御および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 Agent ソフトウェアは、インストールして実行すると、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すメッセージを **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

パフォーマンスに関する値を**指定した間隔でモニター**し、値が限界値を超えた場合にメッセージを生成できます。

HPOM は、**自身のプロセス**もモニターできます。

メッセージの比較

HP Operations Agent はあらかじめ設定されたポリシーの条件でメッセージを比較し、重要でないメッセージは無視しますが、予測していなかったメッセージ、または重要なメッセージを管理サーバーに転送します。重複するイベントや類似イベントを除外するように、エージェントを設定することもできます。**メッセージにフィルターをかける**ときの基準は、既存のポリシーを修正するか、新規にポリシーと条件のセットを作成して設定します。

メッセージのログ機能

すべてのメッセージは管理対象ノードのローカル**ログに記録**するか、または管理サーバー上の履歴データベースに直接保存できます。この履歴機能により、システムが無視するように設定した重要性の低いメッセージを含む、すべてのメッセージを後から確認できます。

メッセージのバッファーへの格納

管理サーバーにアクセスできない場合には、管理サーバーがメッセージを受け取れる状態に戻るまで、メッセージは**ストレージバッファー**に保存されます。

障害の修正

修復アクション (corrective action) は、メッセージに対応して管理対象ノード上でローカルに開始でき、必要に応じて停止したり再開することができます。

ノードの構成

HPOM 環境は、たとえば制御対象、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**タイプ**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るようになった場合、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可能です。

基本的な権限とユーザータイプ

ファイルやフォルダーに対する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与える権限を整理することで記述できます。

基本的な権限

ファイルやフォルダーの権限は、対象となるファイルやフォルダー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とともに ACL のすべてのデフォルトタイプにも適用されます。基本的な権限の変更や ACL の設定、また ACL の変更を実行できるのは、そのファイルやフォルダーの所有者だけです。

読み込み権

オブジェクトの内容にアクセスして検索、コピー、または表示することを許可します。

書き込み権

ファイルの場合は、ファイルの内容にアクセスして変更することを許可します。フォルダーの場合は、フォルダーにアクセスしてオブジェクトを作成したり削除したりすることを許可します。

実行権限

ファイルの場合は、ファイル (実行ファイル、スクリプト、アクション) にアクセスして実行することを許可します。フォルダーの場合は、フォルダーにアクセスしてその内容を検索したりリストにして出力したりすることを許可します。

作成したオブジェクトを、間違って上書きされないように保護しつつ、どのユーザーからも使用できるようにするには、次のようにします。

ファイルのプロパティを変更して、所有者、グループ、およびその他のユーザーに読み込み権と実行権限を与えます。書き込み権限は与えません。

基本的なユーザータイプ

ファイルやフォルダーの基本的な権限は、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ーを所有しているユーザー。ファイルやフォルダーの所有者を変更できるのは、システム管理者 (root ユーザー) だけです。

グループ　グループシステム管理者によってグループに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をすべて同じグループに所属させるということが考えられます。このグループが所有グループであり、通常は、ここにファイルやフォルダーの所有者が属しています。

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。

フォルダーを非公開にするようにする場合は、たとえば、次のようにします。フォルダーのプロパティを変更して自分自身 (所有者) に読み込み権、書き込み権、および実行権限を与え、グループとその他のユーザーにはいっさい権限を与えないようにします。このようにすれば、フォルダーの内容が見られるのは所有者と root ユーザーだけになります。

HPOM の特長

HPOM は、コンピューティング環境で発生する問題 (障害) に備え、その解決を手助けします。問題は種々のネットワークエレメント、システム、およびアプリケーションで構成される分散環境ではどこでも起こりえます。

問題の登録

HPOM は問題が発生する状況になると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。HPOM は問題が発生する状況になると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。

たとえば、未許可のユーザーが管理対象ノードへのログインを試みると、当該ノードはその問題を登録します。登録方法は、システムログファイルへのエントリの書き込み、SNMP トラップの送信、アプリケーションプログラミングインタフェース (API) による管理サーバーとのダイレクト通信のいずれかです。

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 はログファイル中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。

問題の解決

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。メッセージによって、どの程度の重要度 (severity) の問題が、どこで (どの管理対象ノードで) 発生したか、ならびに何によってメッセージが引き起こされたかを知ることができます。メッセージが到着すると、そのイベントに設定しているアクション応答の種類によって、問題が発生した管理対象ノードに対する自動アクションがただちに開始されます。または、そのメッセージにより、修復アクションを手動で開始するようにユーザーに指示する別のメッセージが生成されます。

解決方法のドキュメント化

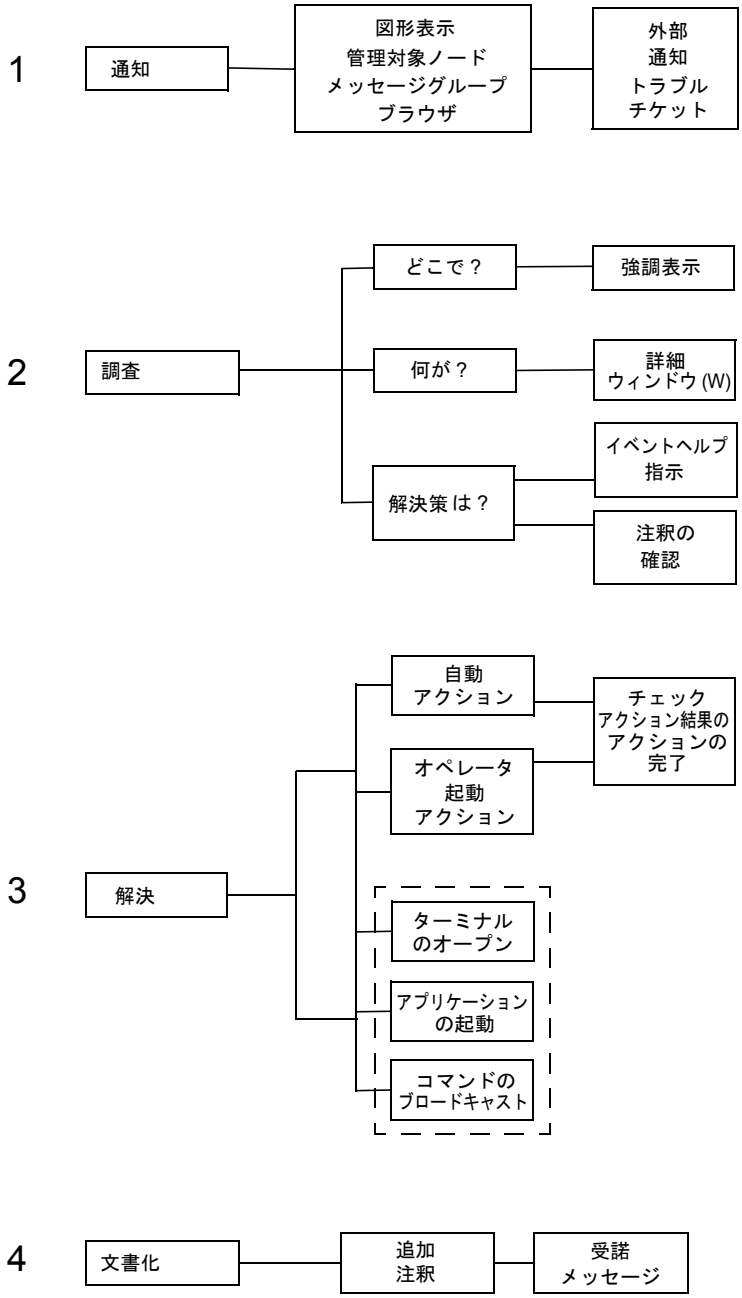
修復アクションが正常に完了後、メッセージにコメントを付け、メッセージを受諾することにより履歴データベースに移動できます。

レポートの生成

未許可のユーザーによるログインとそれに関連するアクションの状況を把握するため、データベースからレポートを生成することもできます。

32 ページの図 1-2 は、問題解決の主な要素を示しています。これらの各要素については、『HPOM Java GUI オペレータガイド』でさらに詳しく説明します。

図 1-2 問題解決の構成要素



次は、問題解決の構成要素を表す 32 ページの図 1-2 の要点です。

1. **通知**

   HP Operations Agent は、ログファイルとシステム動作をモニターします。

   問題が発生すると、HP Operations Agent 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
   - 問題の重要度に応じてノードアイコンの色を変える
   - メッセージブラウザの [重要度] フィールド (設定によってはメッセージ行全体) をカラー表示してメッセージのステータスを示す
   - メッセージとその属性 (送信時刻、アクションのステータスなど) を表示する
   - 外部への通知 (external notification) またはトラブルチケットサービスが設定されている場合には、それに転送する

   問題の重要度と影響を受けるオブジェクトを即座に把握し、問題の詳しい調査と解決に取り掛かることができます。

2. **調査**

   問題とその原因を把握します。大規模な環境においては、問題を早急に特定できることは極めて重要です。

   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**

   問題を解決するための修復アクションを開始します。

   HPOM では次のソリューションを利用できます。

   - 自動アクション

     HPOM は、エラーメッセージを受信すると、ただちに修復アクションを自動的に開始します。この修復アクションは、手動で何度でも再実行することができます。

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

  オペレータは、エラーメッセージを受信して内容を確認すると、ただちに修復アクションを手動で開始できます。開始した修復アクションは手動で停止することもできます。

- ユーザーへの指示

  エラーメッセージにはユーザーへの指示を添付できます。この指示によって、障害解決のための具体的な方法をユーザーに提示します。

- 履歴ログ

  障害の解決には、関連する障害の履歴ログも利用できます。履歴ログにはメッセージへの注釈 (annotation) も含まれます。履歴ログをたどれば、以前に同じ (または同様の) 障害が発生したときに、その解決に使用したテクニックを見つけ出すことができます。

- 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したりできます。これにより Java GUI から直接修復アクションを開始できます。

4. **文書化**

   障害処理を終了して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、システムのモニター、制御、および管理を行うことです。

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の検出

- **レポート**

  そのイベントに関するメッセージ (レポート) の作成

- **アクション**

  そのイベントに対するアクションの実行

HPOM はメッセージにより、ユーザーとコミュニケーションを行います。メッセージとは、システム内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、読み取り可能な形式にしたものです。管理対象ノードでステータスの変更やイベント、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。メッセージ生成の元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。オリジナルのメッセージ、修復アクションの結果、およびユーザーによる注釈などの関連情報はデータベースに保管されます。

イベント

イベントとは、コンピュータ環境内のオブジェクトで発生する障害またはできごとです。通常、イベントには、ステータスの変更やしきい値の超過などがあります。たとえば、用紙トレイが空になるとプリンターのステータスが変化します。また、利用可能な空きディスク領域が一定レベルを下回ると、しきい値の超過が発生します。これらのできごとはそれぞれがイベントであり、各イベントに対してメッセージを作成できます。

イベントの大部分は、修復を必要とする障害です。ただし、ユーザーのアクションを必要としないイベントもあります。ユーザーがシステムへのログオンまたはログオフを行うと、システムのステータスが変わり、イベントが発生します。このようなイベントは、通常はユーザー側のアクションは必要ありません。

イベント相関処理

イベントの発生によりメッセージが発生します。システムで発生するイベントが増えるほど、オペレータが受信するメッセージの数も増える傾向があります。“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) を使えば、“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することが可能です。このリアルタイム処理を通して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小さなストリームを作成します。この絞り込んだ情報で障害の診断と解決をより効率的に行えます。イベント相関処理は、重複するイベントや関連するイベントを除去し、互いに関連した一連のメッセージを 1 つのメッセージで置き換えます。

サポートされるエージェントと管理サーバープラットフォームは、『HPOM 管理者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は、第 4 章「メッセージポリシーの設定」(179 ページ) 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は、『HPOM 管理者リファレンスガイド』を参照してください。

メッセージ

メッセージとは、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によって、アプリケーションとシステムのログファイル (NT 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によって、管理サーバーと選択したエージェントプラットフォーム上のイベントを捕捉します。詳細は、『HPOM 管理者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)`)を使って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に対して測定された値が設定したしきい値を超えると、HPOM が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

イベントの検知後、HPOM はそのメッセージにポリシー条件を適用します。ポリシー条件はメッセージを生成するか、イベントを無視するかの判断を行うフィルターとして機能します。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。メッセージが障害を通知するものである場合は、その障害を解決するためのアクションを定義できます。

メッセージの論理リンク

複数のメッセージを論理的にリンクし、それらを相関処理したメッセージに自動アクションを設定できます。HPOM 標準のメッセージ相関処理とフィルター機能については、「メッセージの最適なフィルター処理のための方針」(225 ページ) 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の通信
- 環境内でのステータス変化のユーザー通知
- 修復アクションの開始

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 メッセージ処理のフロー

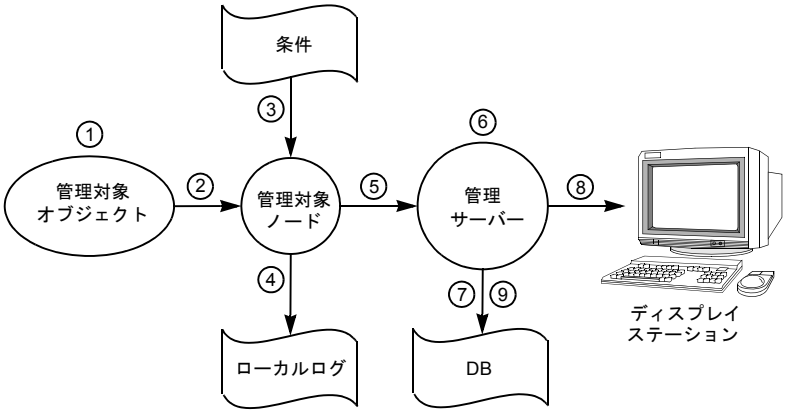


図 1-3 に示しているように、メッセージは次の手順を通じて処理されます。

1. **管理対象オブジェクトでのメッセージの生成**

   管理対象オブジェクトでイベントが発生し、その結果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ためにバックアップに失敗し、メッセージが作成されます。

2. **管理対象ノードによるメッセージの受信**

   その管理対象ノード上の HP Operations Agent がメッセージを受信します。

3. **転送または除外**

   メッセージにフィルターが適用されます。除外条件 (suppress conditions) に一致するメッセージや重複メッセージは除外されます。それ以外のメッセージが管理サーバーに転送されます。

4. **ログへの出力**

   HPOM は、メッセージをローカルのログに記録するように設定できます。

5. **管理サーバーへの転送**

   フィルターに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。ローカルなアクションが設定されている場合は、それが開始されます。

6. **管理サーバーでの処理**

   管理サーバーが、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

     他のメッセージグループに、メッセージを自動的に割り当てる (グループ替え)

   - アクション開始

     そのメッセージに対して設定されたローカルではない自動アクションを、指定されたノード上で開始する

   - 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する (HPOM がそのように設定されている場合)

   - バッファーへの格納

     ペンディングメッセージブラウザにメッセージを格納する (HPOM がそのように設定されている場合)

7. **データベースへの格納**

   アクティブなメッセージがデータベースに格納されます。

8. **表示**

   メッセージが 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格納**

   メッセージは受諾されると、アクティブなブラウザから削除されて履歴データベースに格納されます。

メッセージへのオペレータの対応方法は、『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は、第 2 章「HPOM の設定と保守」(51 ページ) 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。1 つのメッセージグループには互いに関連するさまざまなソースからメッセージが集められ、それらの管理対象オブジェクトまたはサービス (ソース) の集合したステータス情報がわかります。たとえばメッセージグループ BACKUP は、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、バックアップシステムに関するすべてのメッセージを集めるのに使います。

メッセージのフィルター処理

他のメッセージ管理操作では、重要な情報が確実に表示されるように、肯定的または否定的なフィルターを使ってメッセージを分類できます。

- **肯定的なフィルター**

  指定されたパターンに一致するメッセージをオペレータに転送する

- **否定的なフィルター**

  指定されたパターンに一致するメッセージを除外する

除外されたメッセージはローカルなログファイルに格納し、傾向分析やフィルターの妥当性チェック、および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。

不一致メッセージの分類

HPOM は、フィルターに一致しないメッセージを「非該当」として分類します。不一致メッセージは新規または未定義のソースでよく発生します。「不一致」カテゴリは、適用可能なメッセージ分類が存在しないことを示します。

非該当メッセージには、次のいずれかの処理を実行できます。

- 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処理

中央の管理システムに転送されたすべてのメッセージは、メッセージブラウザ内に同じフォーマットで表示されます。HPOM は、メッセージを重要度ごとに色分けしてカラー表示します。デフォルトでは、メッセージブラウザ内の重要度カラムだけがメッセージの重要度に応じてカラー表示されますが、メッセージブラウザ内のすべてのメッセージ行をカラー表示するように HPOM を設定することもできます。また、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可能です。

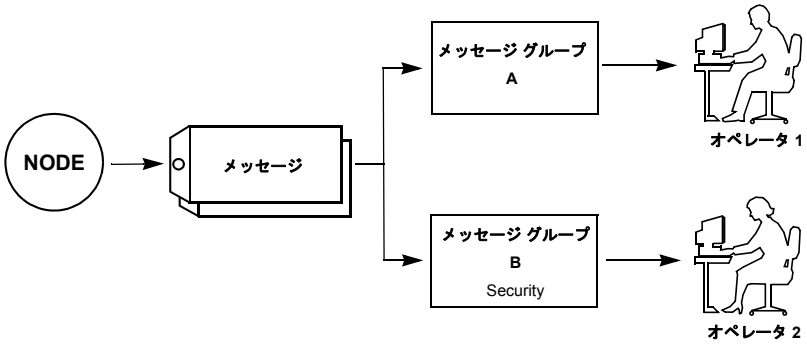
メッセージへの応答

オペレータはメッセージブラウザを、メッセージを調べ対応策を決めるための起点として使います。ここでは、あらかじめ設定された修復アクションの利用の可否、ステータスなど、関連するあらゆるメッセージ情報を調べます。これらのアクションをドキュメント化する機能もあります。

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/業務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 に示す例では、アクセスの制限を必要とする、機密性の高いメッセージを発行する 1 つのノードに対し、2 名のオペレータが共同で担当しています。セキュリティ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セキュリティを維持しています。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見ることはできません。

図 1-4　1 名のオペレータのみに送付される、セキュリティを必要とするメッセージ



アクション

アクションはメッセージに対する対応 (応答) です。メッセージ生成の元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上で毎日アプリケーションを起動するといった、日常の作業の実行にも使えます。アクション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などです。

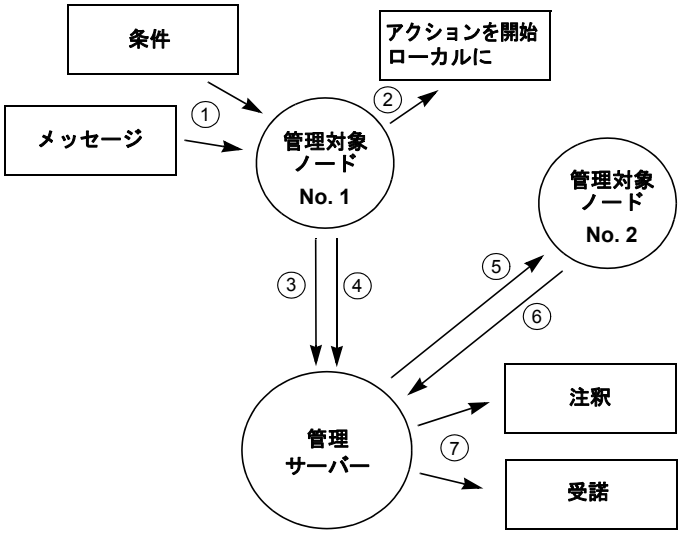
HPOM には、次の種類のアクションがあります。

- ❏ 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、あらかじめ設定され、メッセージにリンクしている障害への応答です。自動アクションにはオペレータの操作は必要なく、メッセージの受信と同時に HPOM によって開始されます。必要ならオペレータが手動で起動または停止できます。

図 1-5　自動アクションの開始



42 ページの図 1-5 に示すように、自動アクションは次のように行われます。

1. **メッセージの捕捉**

   メッセージが定義された条件に基づいて、管理対象ノードで捕捉されます。

2. **アクションの開始**

   アクションのターゲットノードがノード No.1 の場合、アクションはローカルで開始されます。

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**

   アクションのターゲットノードがノード 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**

   管理サーバーがノード No.2 にアクションを開始するよう指示を送ります。

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. **注釈の記録**

   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。また、アクションが正しく完了した後、ログへの記録を自動的に受諾 (acknowledge) することもできます。

オペレータ起動アクション

オペレータ起動アクションも自動アクションと同様、あらかじめ設定され、メッセージにリンクされた障害への応答です。このタイプのアクションは、オペレータによって開始と停止が行われます。

次の可能性が存在する場合には、管理者は自動アクションの代わりにオペレータ起動アクションを設定できます。

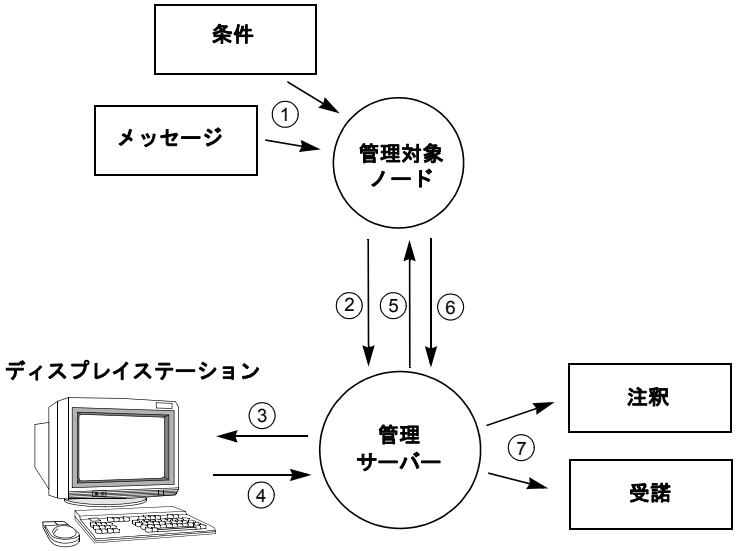
- **手動操作**

  アクションでオペレータによる手動操作が必要になる

- **前提条件**

  アクションの開始が環境条件に依存し、その条件をオペレータがまず確認しなければならない

図 1-6　オペレータ起動アクションの開始



44 ページの図 1-6 に示すように、オペレータ起動アクションは次の順序で処理されます。

1. **捕捉**

   設定された条件に基づいて、メッセージが管理対象ノードで捕捉されます。この条件には、オペレータ起動アクションまたは自動アクションを促すことができるメッセージなどがあります。

2. **転送**

   メッセージが管理サーバーに転送されます。

3. **表示**

   メッセージが担当オペレータのディスプレイステーションに送られます。メッセージにはあらかじめ設定されたオペレータ起動アクションの存在が、[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**

   オペレータがブラウザ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**

   アクションを開始するための指示が管理対象ノードに送られます。

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. **ログへの記録と受諾**

   オペレータ起動アクションの実行に関する注釈 (annotation) 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。また、アクションが正しく完了した後、自動的に受諾されるようにメッセージを設定することもできます。

アプリケーション

アプリケーションとは HPOM に統合されているスクリプトまたはプログラムです。オペレータ起動アクションや自動アクションはメッセージとダイレクトに関連付けられ、ブラウザウィンドウから開始または停止できますが、アプリケーションはオペレータの `Applications` フォルダーから使うツールです。詳細は、『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 の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とユーザープロファイルを区別します。ユーザープロファイルは、抽象的なユーザーの設定を表します。これらの抽象的なユーザー設定を使用して、実際のユーザー設定を作成できます。

ユーザーロール

HPOM で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。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。ほとんど常時 HPOM を使い、システムとオブジェクトの保守、管理、モニター、および制御を行います。

複数のオペレータ

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。各オペレータには、個々のスキルに応じて責任と権限を割り当てることができます。HPOM で管理するコンピュータ環境の規模に応じて、複数のロールを 1 名のオペレータで行うこともできます。

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。ユーザーインタフェースにアクセスする際には、HPOM 用の正しいログオン名とパスワードの入力が各オペレータと管理者に必要です。この HPOM パスワードは、Unix システムへのログオン名と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に有効です。抽象的な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、デフォルト設定を使用してユーザーを迅速にセットアップすることができます。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。詳細は「ユーザープロファイルの設定」(101 ページ) を参照してください。

管理者

HPOM 管理者 `opc_adm` には、HPOM 作業環境内での多くの作業と責任があります。

管理者は次の作業を行います。

- **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。ソフトウェアのインストール、設定、およびカスタマイズの調整全体を管理します。システムに対するこれらの調整では、オペレータ、テンプレート管理者、ノード、取り込んだメッセージなどの追加や変更を行います。

- **オペレータ作業の効率化**

  特定のイベントに対する修復アクションを対応付けたり、個々のイベントに対する指示 (instruction) を提供することによりオペレータの作業効率を高めます。

- **作業範囲の定義**

  各オペレータの担当 / 権限範囲を定義し、オペレータが割り当てられたノードを保守して必要な作業を実行するために、どのツールが必要かを判断します。

- **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作業範囲を定義します。

- **履歴の保守**

  HPOM 履歴データの保守とチェックを行います。管理者は履歴をたどることによって、自動アクションやオペレータ起動アクションを過去のデータに基づいて修正または作成できるほか、イベントに関する具体的な指示を与えたり、障害の再発状況を把握することができます。たとえば、履歴データをチェックすると、ディスクの使用量が一貫して高いノードが明らかになります。

- **ユーザーの問題の解決**

  任意のオペレータになって設定を確認します。そのオペレータがシステムを使っているときに発生する可能性があるあらゆる問題の解決を支援します。

- **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 の機能を拡張します。追加したアプリケーションは登録し、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ことを確実にします。

- **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方針を定義します。HPOM のセキュリティの詳細は、「環境のセキュリティ保護」(54 ページ) または『HPOM 管理者リファレンスガイド』を参照してください。

オペレータ

HPOM のオペレータ、`opc_op` はシステム管理機能だけを担当します。オペレータの作業環境は、管理対象ノードの集まりです。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 の各オペレータには、それぞれが担当する管理環境があります。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。作業範囲を作成することにより、HPOM は各オペレータに、その人が担当するシステムとオブジェクトの情報のみを表示します。

デフォルトの HPOM オペレータの詳細は、「ユーザーとユーザープロファイルの設定」(94 ページ) を参照してください。

2 HPOM の設定と保守

本章の内容

本章では、HP Operations Manager (HPOM) のさまざまな要素、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、オペレータなどを設定する方法を説明します。

対象読者

本章は、HPOM 管理者を対象としています。

目的

本章では HPOM 管理者向けに、次の各トピックを説明します。

- ❑ 管理者環境
- ❑ 環境のセキュリティ保護
- ❑ 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 の設定の更新
- ❑ 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用のすべての GUI と設定に加え、管理用の機能とコマンドラインツールにアクセスできます。

HPOM 管理者として、次の主要な HPOM 要素を設定できます。

- ❏ 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

環境のセキュリティ保護

環境をセキュリティで保護するには、次の各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を検討し、次にネットワークのセキュリティに関する問題を検討します。システムセキュリティの対象となるのは、HP Operations 管理サーバーと管理対象ノードを信頼できるシステムで実行するために対処する必要がある問題です。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。ネットワークセキュリティについての詳細は『HPOM 管理者リファレンスガイド』を参照してください。

- **HPOM セキュリティ**

  HPOM の設定中に対処するべきセキュリティへの影響を調べる必要があります。具体的には、アプリケーションの設定と実行や、オペレータ起動アクションなどによるセキュリティ関連の影響を調べます。HPOM ユーザーの作業ディレクトリ、ファイルアクセス、および権限の詳細は、『HPOM 管理者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

安全なシステムまたは信頼できるシステムでは、システムレベルのセキュリティを高めるために、さまざまな方法が使用されます。HPOM 環境を構築、設定する際には、これらの方法を考慮する必要があります。

セキュリティ技術

セキュリティ技術には、次のシステムレベルの要素が含まれます。

- **認証**

  厳密なパスワード/ユーザー認証

- **監査**

  ネットワーク、共有メモリ、ファイルシステムなどの監査

- **ターミナルへのアクセス**

  ターミナルへのアクセスの管理

- **ファイルへのアクセス**

  ファイルへのアクセスの管理

HPOM のセキュリティ処理

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**

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

ネットワークセキュリティの詳細、特に HPOM がどのようにプロセス間通信に関する問題に対処するかについては、『HPOM 管理者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

管理対象ノードと、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 の初期デフォルト設定に含まれる管理対象ノードは、管理サーバーだけです。この構成に別のノードを追加します。このようにして、HPOM の管理環境を構築します。(管理対象ノードの種類については、「管理対象ノードの種類」(56 ページ) を参照してください。)

HPOM 環境の構築では、コマンドラインツール `opcnode` と `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にまとめます。詳細は、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は、「管理対象ノードの編成」(57 ページ) 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。

管理対象　管理対象ノードには、すべての管理機能とモニター機能を適用できます。

監視対象　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、監視対象ノードが便利です。

メッセージ対象　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。たとえば周辺機器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るノードはメッセージ対象ノードにすることができます。

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。これは管理対象、モニター対象、またはメッセージ対象ノードの一時的な状態です。

管理対象ノードの編成

管理対象ノードを編成する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**

  ノードを論理的な作業範囲のグループにまとめます。

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作業範囲を設定し、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編成します。

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 で管理またはモニターされるすべてのノードが含まれます。また、HPOM 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。外部ノードでは HPOM ソフトウェアは動作しませんが、これらのノードが発信するイベントは受信できます。

ノード階層の詳細は「HPOM ノード階層」(58 ページ) を参照してください。

初期設定では、HPOM 登録ノードに含まれるのは、管理サーバーのみです。その他すべてのノード、外部ノード、ノードレイアウトグループは管理者が追加します。

ノードを追加するには、コマンドラインツール `opcnode` を使用します。詳細は、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。登録ノードに加えられるすべての変更は、管理者が管理します。ノードを登録ノードに追加 / 削除するタイミングも管理者が決めます。

数百台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。そ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。詳細は「ノード階層の設定」(58 ページ) を参照してください。

HPOM ノード階層

HPOM 登録ノードは、デフォルトノード階層です。**ノード階層**とは、ノードとノード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。ノード階層間の違いはこれらのノード構成だけです。

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、オペレータには作業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、ノード階層を作成するノードと他のレイアウトグループを含めることができます。レイアウトグループとノード階層は、コマンドラインツール `opclaygrp` を使って管理できます。

ノードを HPOM 登録ノードに追加するには、コマンドラインツール `opcnode` を使用できます。その他のノード階層にもノードを追加できます。ノードを追加すると、他のすべてのノード階層に同じノードが追加されます。これらの新しいノードは指定されたノードとレイアウトグループに追加され、デフォルトでその他すべての階層の最上位レベルになります。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 環境に含まれなくなります。

詳細は、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ある場合は、レイアウトグループを使用して、論理的エンティティでノードを構成できます。

レイアウトグループとは、関心のあるノード階層レベルのみを表示できる論理的に構成された階層です。レイアウトグループの概念は、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またはツリー状構造を構築できます。

レイアウトグループとノード階層の作成、変更、削除についての詳細は、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

ノード階層を作成した後、HPOM では opcnode(1m) コマンドラインツールを使用して、この親グループに含まれるすべてのノードにアクションを同時に適用できます。たとえば、一連のノードにポリシーを割り当てるには、ポリシーを割り当て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、そのグループ内のすべてのノードを含むノードグループにポリシーを自動的に割り当てます。

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、および HPOM 登録ノードには、次のアクションを適用できます。

- ❏ コマンドラインツール 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
- ❏ 選択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と停止
- ❏ ソフトウェア、設定などの配布
- ❏ ポリシーの割り当て

すべてのノードには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、および HPOM 登録ノードには、次のアクションが適用できません。

- ❏ レポートの発行
- ❏ アプリケーションの追加または変更
- ❏ [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実行するための条件

階層グループにアクションを適用する際には、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内にある場合、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**

  ノードとグループシンボルの組み合わせだけでなく、複数のグループにも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 サービスについての詳細は、「アプリケーションの追加」(87 ページ) を参照してください。

ノードの追加

ノードを HPOM 環境に追加するには、コマンドラインツール opcnode を使用します。

詳細は 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ラインツール 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) とマシンの種類を取得し、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 管理者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

コマンドラインツール 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 Agent**

  通常、内部ノードでは、HP Operations Agent 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。

- **全機能のサポート**

  内部ノードは次のような HPOM のすべての機能をサポートします。

  - ログファイルのモニター
  - HPOM メッセージの捕捉

HP Operations Agent をインストールしない場合

次のような場合には、HP Operations Agent をインストールしなくても構いません。

- ❏ セキュリティ上の問題がある
- ❏ エージェントが不要である
- ❏ プラットフォームや現バージョンの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

外部ノードを追加するには、コマンドラインツール opcnode とパターンマッチの方法を使用できます。次のような場合は、コマンドラインツール 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 アドレスがない場合(SNA、DECnet など)
- ❏ 特定のホスト名パターンや IP アドレス範囲を基準として IP ノードをグループ化する場合

コマンドラインツール opcnode を使用する場合、ノードのマシンタイプを MACH_BBC_OTHER_NON_IP に、通信タイプを COMM_UNSPEC_COMM に設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、ノードが複数回表示される場合があります。たとえば、コマンドラインツール opcnode で追加したノードが、パターンを変更しただけで再度、外部ノードのように追加されることは十分にありえます。同様に、パターンマッチで追加したノードが再度、類似したパターンで追加される可能性もあります。これが HPOM に悪影響を与えることはありませんが、ユーザーが作業を行ってノードが強調表示されたときに、メッセージのソースとして 2 つ以上のシンボルが強調表示されることがあります。

詳細は 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。

- ❏ ネームサーバーで認識される
- ❏ /etc/hosts ファイルに登録されている

注記

パターンマッチが必要なため、外部ノードは管理サーバーシステムのパフォーマンスを低下させます。

外部ノードの特徴

コマンド opcnode 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。

- ❏ **あらゆる種類のノード**

  SNA、DEC、IP など、あらゆる種類のノードが外部ノードになりえます。

- ❏ **HP Operations Agent の不在**

  外部ノードには、その上で動作する HP Operations Agent がありません。

- ❏ **一括追加**

  外部ノードは名前またはアドレスをパターンに一致させることで、一括して HPOM に追加されます。

- ❏ **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 管理者リファレンスガイド』を参照)。

  - シンボルの強調表示

    Java GUI のオブジェクトペインのノードシンボルを HPOM によって強調表示して、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すことができます。これらのノードを設定して、プロキシからメッセージを受信することもできます。

  - メッセージのフィルター処理

    Java GUI のオブジェクトペインのノードシンボルをユーザーが選択して、ビューブラウザに表示されるメッセージにフィルターを適用することができます。

- ステータスのカラー表示

  表示色を変更して、HPOM のステータス伝播で設定されたメッセージの重要度ステータスを示すことができます。

❏ 内部ノードで利用できる次の機能は、外部ノードではサポートされません。

- メッセージポリシー

  ログファイル、モニター、`opcmsg` などからのメッセージ。つまり、これらにポリシーを割り当てることができないということです。

- HPOM アプリケーションの不在

  外部ノードでは HPOM アプリケーションは動作しません。

- ブロードキャスト

  ブロードキャストは実行できません。

- スケジュールアクション

  スケジュールアクションは実行できません。

管理 UI の使用によるノードの追加

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 UI を使用します。

管理 UI では、次のノード属性が提供されます。

❏ システムリソースファイルの自動更新

HP Operations Agent コマンド `opcagt` を統合できます (HP-UX 管理対象ノードの `/etc/rc.config.d/opcagt` など)。

❏ ノードの詳細オプション

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

❏ 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。

以下を定義できます。

- セキュリティのパラメータ
- インストール方法
- バッファーファイルの上限サイズ

さまざまな種類の管理対象ノードのセキュリティの設定

管理対象ノードのタイプは、`opcnode -list_node` コマンドでリストを表示することができます。ノードの種類を変更するには、`opcnode -chg_nodetype` コマンドを使用します。

❏ **監視対象ノード**

環境内の安全なノード (オペレータによるログオンやアクションを制限するノード) は、**監視専用**ノードとして指定できます。オペレータはこのようなノードから送信されたメッセージを受信して内容を確認することはできますが、コマンドのブロードキャストやログイン、自動アクション、オペレータ起動アクションなどのアクションはいっさい実行できません。

❏ **管理対象ノード**

管理対象ノードでは、オペレータはアクションの開始/停止やログインを実行できます。管理者がノードのセキュリティを個別に確認し、オペレータアクセスの許可と、アクションやコマンドの実行の可否を決定します。

オペレータが管理対象と監視対象の 2 台のノードで同時にアクションの実行を試みると、そのアクションはアクションエージェントが存在する管理対象ノードのみに送信されます。

非管理対象ノードの管理

計画的な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、そういったメッセージが、計画的な休止とは関係ない他のメッセージ (特に緊急の注意を要するようなもの) を目立たなくしてしまうことがありえます。定期的に休止する場合は、管理者が計画休止を設定 (「計画休止の設定」(308 ページ) を参照) しておくことでメッセージを除外できます。1 回限りの計画休止のときは、管理者は管理対象ノードを一時的に**非管理対象**ノードにしておくことで分離することもできます。モニター対象や管理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。これによって、メッセージが管理サーバーへ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、そのノードを作業範囲マトリクスに含むすべてのオペレータの環境からは排除されます。このノードの属性はすべて HPOM に認識されており、このノードは登録ノードの一部のままです。

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。ノードを非管理対象にする前に使用できたメッセージが再び使用可能となり、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、オペレータに管理が任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る場合があり、そのため複数のオペレータから影響を受ける可能性があるため、ノードグループを使うと管理者の設定作業の効率はかなり低下してしまいます。

ノードグループは、設定を容易にする手段として使うこともできます。たとえば、1 つのノードグループに属するすべてのシステムに、同じポリシーグループを一括して割り当てることができます。ノードグループに後から新規ノードを追加する場合は、そのノードグループに割り当てられたポリシーが自動的に新規ノードにも割り当てられます。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。

- 同じ場所のノード

- ❏ 同様の機能を持つノード
- ❏ 同タイプのノード

グループ化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際には、担当するノードグループ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作業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 つのノードは、複数のグループに含めることができます。opcnode コマンドを使用して、特定のノードグループにどのノードが割り当てられているかを確認できます。

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

HPOM の初期設定のノードグループは、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、不明なノードは青で表示されます。メッセージブラウザが開くと、ノードの色はそのノードに関する受諾されていないメッセージの中で最も重大度が高いメッセージのステータスを反映して変わります。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て、管理対象ノードに割り当てて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の詳細は「HPOM のポリシー」(68 ページ) 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タスクについての詳細は、『HPOM 管理者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、複数のバージョンのポリシーを作成することができます。詳細は「ポリシーバージョン」(71 ページ) と「ポリシーグループ」(83 ページ) を参照してください。管理対象ノードでの複数バージョンの HPOM 設定の管理についての詳細は、『HPOM 管理者リファレンスガイド』を参照してください。

HPOM のポリシー

ポリシーとは、データ情報とメタ情報で構成される設定要素です。ポリシーは管理対象ノードに配布されます。データ情報の部分は、通常、ポリシーが配布される管理対象ノードでメッセージを生成するためのルールのセットで構成されます。データ情報の部分が完全にユーザーによって定義されるのに対して、メタ情報の部分は管理タスクに使用され、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での HP Operations Agent の設定とメッセージが作成される条件の決定に使用され、管理サーバーに送信されて、オペレータにイベントについて通知します。

ポリシーは、1 つの**ポリシーヘッダー**、1 つ以上の**ポリシー本体**という 2 つ以上のファイルで構成されます。ポリシーヘッダーとは名前、タイプ、バージョンなどの属性を含む XML ファイルです。

注記

コロン文字 (`:`) は、`opcpolicy` の使用法の構文でポリシーの識別に使用されるため、ポリシー名に含めることはできません。使用法についての詳細は、opcpolicy (1m) のマニュアルページを参照してください。

ポリシー本体には、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、または UUID で識別されます。**ポリシータイプ**とは、ポリシー本体が順守する必要のあるルールを決定するポリシー属性です。同じタイプのすべてのポリシーは、管理対象ノードの同じ HP Operations Agent プロセスによって使用されます。HPOM で事前定義されたポリシータイプの他に、ユーザーによってカスタムポリシータイプも作成できます。

ポリシーコンテナは、同じ名前とタイプでバージョンが異なるポリシーのセットを示します。ポリシーコンテナのすべてのポリシーバージョンは一意です。一部の操作はポリシーコンテナで実行できます。これは、操作がコンテナの各ポリシーで実行されるということです。各コンテナには、コンテナ内のすべてのポリシーによって共有される一意の ID があります。コンテナは、名前、タイプ、または ID で識別されます。

ポリシー タイプ

HPOM では、複数の異なるポリシータイプが利用できます。各タイプのポリシーで異なるモニタリングタスクまたは設定タスクが実行できます。このため、ポリシータイプとは何がポリシーで管理できるかを定義する一連の設定情報になります。すべてのポリシーは 1 つのポリシータイプに所属します。

次のポリシータイプにより、モニタリングタスクまたは設定タスクが実行できます。

- ❏ 設定ファイルポリシータイプ[12]
- ❏ イベント相関処理ポリシータイプ
- ❏ イベント相関処理コンポーザーポリシータイプ[1]
- ❏ フレキシブル管理ポリシータイプ[13]
- ❏ ログファイルエントリポリシータイプ
- ❏ 測定しきい値ポリシータイプ

---

1. このポリシータイプについては、付録 A で説明されているポリシー本体の文法は使用できません。
2. 詳細は「配布後のエージェントでの設定ファイルポリシーを使用したコールバックの実行」(82 ページ) を参照してください。設定ファイルポリシー、その構文とキーワードについての詳細は、『HPOM 管理者リファレンスガイド』も参照してください。
3. このポリシータイプの構文については、opcmom のマニュアルページを参照してください。フレキシブル管理の設定についての詳細は、『HPOM 管理者リファレンスガイド』も参照してください。

- ノード情報ポリシータイプ[1]
- オープンメッセージインタフェースポリシータイプ
- リモートアクションセキュリティポリシータイプ[12]
- SNMP インターセプタポリシータイプ
- 定期タスクポリシータイプ
- サービス自動検出ポリシータイプ[1]
- サービス/プロセスモニターポリシータイプ
- SiteScope ポリシータイプ[1]
- サブエージェントポリシータイプ[13]
- Windows イベントログポリシータイプ
- Windows 管理インタフェースポリシータイプ

ポリシータイプとポリシーは管理 UI を使用して管理できます。すべてのポリシータイプは、HPOM 管理 UI オンラインヘルプで説明されています。

HPOM ではポリシーエディターを使用して、必要に合わせて新しいポリシーの作成や既存のポリシーの変更が可能です。ポリシータイプごとに異なるポリシーエディターがあります。ポリシーエディターの詳細は、『HPOM 管理者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タイプの編集についての詳細は、付録 A「ポリシー本体の構文」(355 ページ) を参照してください。

複数のポリシータイプ 管理対象ノードで同じポリシータイプにマップされている管理サーバーで複数のタイプのポリシーを使用できます。このため、ポリシータイプの登録中、管理対象ノードでポリシーを分類するタイプを指定できます。

---

1. このポリシータイプについては、付録 A で説明されているポリシー本体の文法は使用できません。
2. リモートアクションの承認についての詳細は、『HPOM 管理者リファレンスガイド』を参照してください。
3. 詳細は「サブエージェントポリシー」(84 ページ) を参照してください。

このタイプが指定されていないと、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。この場合、管理対象ノードに対応するコンシューマーがなくてもポリシーは配布されますが、後で無視されます。

表 2-1 管理サーバーと管理対象ノードのポリシータイプの例

管理サーバー	管理対象ノード
ログファイルエントリ `Windows` イベントログ	`le`
測定しきい値 サービス / プロセスモニター	モニター

ポリシーバージョン

管理サーバー上に複数バージョンのポリシーが保存されていることによりポリシーとポリシーグループを使用する操作の柔軟性が強化され、Unix、Linux、Windows プラットフォーム上の HPOM 間の相互運用を簡略化できます。また、以下も確実にします。

- SPI とカスタマ設定移行関連の問題の簡略化

  サーバー上で複数の SPI バージョンを使用することで、ポリシーやポリシーグループを名前変更する必要なく、異なるノードのグループに配布できます。

- 設定データの容易な管理

  ポリシーのバージョニングによって、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) のバージョンを判断できます。たとえば、異なるサブエージェントバージョンの管理、管理対象ノードへの割り当てや配布が簡略化されます。詳細は、「HPOM でのサブエージェントの管理」(84 ページ) と『HPOM 管理者リファレンスガイド』を参照してください。

  異なるプラットフォーム (Unix、Linux、Windows) 向けの HPOM では、調整されたポリシーのバージョニング機能が使用されます。これにより、単一の SPI ポリシーセットを両方のプラットフォームの HPOM に配布して、相互のデータ交換も簡略化できます。データ交換の注意点については、「ポリシーデータ交換モデル」(74 ページ) を参照してください。

すべてのポリシーにバージョン番号があります。バージョン番号は、`major.minor` (1.0 など) という形式で、2 つの数字 (両方で最大 4 桁) で構成されます。

メジャー番号は連続するリリースの番号を示し、特定の目的 (SPI のリリースの追跡など) のために予約もできます。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。各リリースで最初のマイナー番号は 0 である必要があります。

注記

メジャー番号では、監視対象アプリケーションのバージョンとの整合性を図る場合があります。たとえば、3 桁で構成してアプリケーションの今後のリリースに予約できます。これは、メジャーバージョン 450 をアプリケーションバージョン 4.5 に、メジャーバージョン 460 をアプリケーションバージョン 4.6 に、などのように予約できるということです。

新しく作成され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 で配布されるすべてのデフォルトポリシーのバージョンは 9.0 になります。

ポリシーの内容が変更されると、ポリシーバージョン番号のマイナー部分の桁は、1.0 から 1.1 などのように自動的に上がります。新しいバージョンがすでに存在する場合は、1.2 などのように次に利用可能な値が選択されます。バージョン間の競合を克服する方法については、「ポリシーバージョン間の競合の管理」(73 ページ) を参照してください。

注記

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

設定に合わせてポリシーバージョンを置換するには、コマンドラインツール `opcpolicy` を使用します。ポリシーの内容を変更せずに、ポリシーバージョン番号を変更することもできます。

これは、一緒にリリースされたポリシーバージョンを調整する場合に特に便利です。使用法についての詳細は、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を作成すると、内容が変更されていなくても、新しいポリシーが作成されることになります。新しいポリシーには新しいバージョン UUID が付きますが、コンテナ ID は前と同じです。その一方で、ポリシー名を変更するとデータベースに新しいバージョン UUID と新しいコンテナ ID を持つ新しいオブジェクトが作成されます。

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。新しいポリシーバージョンを管理対象ノードに配布する場合、バージョン番号にかかわらず、新しいポリシーバージョンで既存のバージョンが置換されます。これは、両方のバージョンでポリシーの識別に管理対象ノードで使用される、同じコンテナ UUID が使用されているからです。

注記

稼働環境でポリシーはポリシーグループに割り当てられ、ノードとノードグループに配布される必要があります。ポリシーバージョンは、割り当てられたポリシーグループのバージョンに対応する必要があります。

管理対象ノードで HPOM 設定の複数バージョンを処理する方法 (ポリシーに加えて、ポリシーグループやインストルメンテーションデータを含む) については、『HPOM 管理者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 割り当てようとするポリシーのバージョン番号がすでにデータベースに存在すると、ポリシーバージョンが競合します。バージョン間の競合の管理には次のモードを使用できます。

- ❏ 上書きモード

  データベースの競合するバージョンが置換されます。

- ❏ 新しいバージョンモード

  - バージョン間の競合の場合は、アップロードされるバージョンに対してマイナー部分の桁が自動的に上がります。新しいバージョンがすでに存在する場合は、最初に使用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。
  - 競合するバージョンがない場合は、現在のバージョンでポリシーがアップロードされます。

❏ エラーモード

バージョン間の競合の場合は、エラーが返され、アップロードがキャンセルされます。

ポリシーの 1 つのバージョンが (たとえば、ノードグループやポリシーグループの割り当てによって) 間接的に割り当てられた同じポリシーの別のバージョンと同時に、直接的に管理対象ノードに割り当てられると、割り当てられたポリシーのどのバージョンを実際に管理対象ノードに配布する必要があるのかが不明確になることがあります。

HPOM では、グループなどで間接的に行われた割り当てより、直接的な割り当ての優先度がより高いと見なされます。言い換えれば、直接的に割り当てられたポリシーバージョンと間接的に割り当てられたポリシーバージョンの間で競合が生じた場合、管理対象ノードへの直接割り当てがより重要と見なされ、間接割り当てによって指定されたバージョンの方が新しくても、間接割り当てが上書きされます。

たとえば、ポリシーバージョン 1.3 が管理対象ノード AA に直接的に割り当てられ、管理対象ノード AA が所属するノードグループに同じポリシーのバージョン 1.6 が割り当てられている場合、ノードグループによって間接的に割り当てられたバージョンの方が新しくても、ポリシー配布ではそのポリシーのバージョン 1.3 がバージョン 1.6 より優先されます。

注記

両方のバージョンが間接的に割り当てられている場合 (たとえば、2 つの異なるノードグループまたはポリシーグループなど)、HPOM はポリシーの異なるバージョンを優先順位付けできません。予想外の配布結果を避けるには、同じポリシーを異なるノードグループやポリシーグループに割り当てるのは避けてください。

ポリシー割り当ての自動化やバージョンの競合の管理についての詳細は、『HPOM 管理者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 for Unix、HPOM for Linux、HPOM for Windows は、ポリシーとポリシーグループに関して、共通のデータ交換モデルを共有しています。以下に注意してください。

❏ 管理サーバーでは、ポリシーが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

❏ 同じ名前とタイプのすべてのポリシーには、コンテナ UUID という共通の ID があります。同じコンテナ UUID を共有するポリシーには異なるバージョン番号とポリシー ID という対応する個別の ID があります。

❏ チェックサムを使用して、ポリシーを比較できます。ポリシーヘッダーに保存されたチェックサムフィールドは、設定のダウンロードとアップロードの間に認識されます。チェックサムには次の 2 種類があります。

- ポリシーヘッダーチェックサム

  禁止されたポリシーの変更を検出するために使用します (ライセンス違反)。

- ポリシーデータファイルチェックサム

  コンテンツの比較をより迅速に行うために使用します。

❏ ポリシータイプは、UUID と構文のバージョンも含むエージェントに既知の文字列です (例: `monitor`、`le`、`trapi` など)。

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できます。ポリシーを変更すると、新しいポリシーバージョンになります。これは、既存の割り当ては変更されたポリシーバージョンではなく、古いポリシーバージョンをポイントすることを意味します。このため、割り当てを更新する必要があります。割り当ての更新は、自動的に行うことができます。割り当てモードは次のようになります。

❏ `FIX`

デフォルトモードです。ポリシーは変更後に配布されますが、新しいポリシーバージョンが作成されても、ポリシー割り当ては変わりません。

❏ `LATEST`

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は、新たに最新のポリシーバージョンが生成され次第、自動的に更新されます。これは「policy to policy group assignment (ポリシーグループへのポリシーの割り当て)」オブジェクトのプロパティである `LATEST` フラグを設定することで有効化されます。

このモードは、テスト環境と開発環境についてのみお勧めします。

❑ 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。メジャーバージョン番号は変わりません。たとえば、既存の 1.0 バージョンからの更新に MINOR_TO_LATEST フラグを設定すると、結果は最新の 1.x バージョンになります。

このモードは、稼働環境にお勧めします。

コマンドラインツール opcpolicy、opcnode を使用して、割り当てモードを指定できます。使用法についての詳細は、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 モードと MINOR_TO_LATEST モードを使用する場合、これらのモードでは上記の基準に適合する新しいバージョンが作成されたときに、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、ポリシー割り当ては変わりません (手動で変更されない限り)。

HPOM のポリシー割り当てタスクについての詳細は、『HPOM 管理者リファレンスガイド』を参照してください。

ポリシー割り当ての競合の管理

管理対象ノードに直接的に割り当てられたポリシーのバージョンと、たとえば、元の管理対象ノードが所属する複数のノードグループまたはポリシーグループに対する割り当てによって、同じポリシーに間接的に割り当てられたその他のバージョンとの間に相違がある場合、競合が生じる可能性があります。バージョンが競合する場合、HPOM では直接的に割り当てられたポリシーの優先度がより高いと見なされます。

注記

両方のバージョンが間接的に割り当てられている場合 (たとえば、2 つの異なるノードグループまたはポリシーグループなど)、HPOM はポリシーの異なるバージョンを優先順位付けできません。予想外の配布結果を避けるには、同じポリシーを異なるノードグループやポリシーグループに割り当てるのは避けてください。

ポリシー割り当てとの関連でのポリシーバージョン間の競合についての詳細は、『HPOM 管理者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も含めることができます。カテゴリはポリシーと HP Operations Agent がポリシーで参照されるリソースを正常に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のリンクを定義します。

カテゴリの割り当てについての詳細は、『HPOM 管理者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とは、特定のタイプのポリシーのライフサイクルであらかじめ定められた瞬間に実行される実行可能ファイルです。

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。詳細は、このセクションで後述します。

コールバックの定義に使用できる変数は多数あります。表 2-2 は、これらの変数と代入される値を示しています。

表 2-2 変数と代入される値

変数	代入される値
FILENAME	ポリシー本体の内容のダンプ先となる一時ファイルのフルパス
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	ポリシータイプの名前
AGENT_TYPE	HPOM エージェントが認識したポリシーの種類
MGMT_SV	ポリシーが使用されている管理サーバーの完全修飾ドメイン名
ENCODING	ポリシー本体の内容のエンコーディング
OPTION_X	編集コールバックによってエディターに渡された引数。X は渡された引数の数を表すため、最初の引数の名前は OPTION_1、2 番目の引数の名前は OPTION_2 のようになります。

表 2-2 変数と代入される値 (続き)

変数	代入される値
NODENAME	ポリシーが配布された管理対象ノードの完全修飾ドメイン名。この変数は配布コールバックまたはクリーンアップコールバックで使用できます。
NODE_TYPE	ポリシーが配布される管理対象ノードのオペレーティングシステムの種類。この変数は配布コールバックまたはクリーンアップコールバックで使用できます。

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、実行時の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。コールバック呼び出し文字列に変数が存在しない場合、コールバックが実行される前に、$FILENAME の値が文字列に自動的に追加されます。

管理者特権で実行されるコールバックが、未許可のユーザーによって登録されるリスクを削減するには、コールバックの実行可能ファイルに対する次のセキュリティレベルを利用できます。

❏ **STRICT** (デフォルト)

- HPOM を root ユーザーとして実行する場合

  次の条件のいずれかが満たされた場合、コールバックは登録、変更または実行されません。

  — 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- ビット、read- ビットまたは 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- ビット、read- ビットまたは execute-by-others ビットが設定されている

- HPOM を非 root ユーザーとして実行する場合

  次の条件のいずれかが満たされた場合、コールバックは登録、変更または実行されません。

  — グループの所有者が、opcgrp でない

— ファイルまたはディレクトリに `write-` ビット、`read-` ビットまたは `execute-by-others` ビットが設定されている

❏ **RELAXED**

- HPOM を root ユーザーとして実行する場合

  次の条件が満たされた場合、コールバックは登録、変更または実行されません。

  — 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

  このレベルを有効にすると、すべてのユーザーがディレクトリを表示して実行可能ファイルを実行できますが、`root` のみが書き込み権を持ちます。

- HPOM を非 root ユーザーとして実行する場合

  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場合、コールバックは登録、変更、または実行されません。

❏ **NONE**

コールバック、またはコールバックが配置されるディレクトリにチェックは行われません。

注記

セキュリティレベルは HPOM 変数 `OPC_POLICY_CALLBACK_SECURITY` を使用して設定されます。

次の場合、各コールバックスクリプトまたはバイナリは、`stat()` を使用し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

リストされた条件のいずれかが満たされた場合、メッセージブラウザ (実行前に検出された場合)、または変更か登録が試行されたターミナルのいずれかにエラーがレポートされます。その後でエラーは監査され、HPOM データベースのログに記録されます。

すべてのコールバックについて、以下の要件が適用されます。

❏ 失敗すると、0 とは異なる値が返されます。

❏ 成功すると、値 0 が返されます。

編集コールバック

編集コールバックは実行可能ファイルで、エディターが呼び出される前に実行されます。一時ポリシーデータファイルのフルパスは、コマンドライン引数としてコールバックに渡されます。

チェックコールバック

チェックコールバックは実行可能ファイルで、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ます。チェックコールバックは、`opcpolicy_add()` API が適切な引数で呼び出されるか、`opcpolicy` が `check=yes` コマンドラインオプションで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常に終了すると、ポリシーが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実行可能ファイルで、配布の前にポリシーの本体を含む一時ファイルで実行されます。この実行可能ファイルは、配布時に利用可能な情報 (ノード名、またはノードタイプなど) によってポリシーの内容を変更するために使用します。

配布コールバックでポリシー本体を変更するときに、すべての変更はコールバック実行可能ファイルに名前を渡されている一時ファイルで実行される必要があります。処理でファイルのコピーが必要な場合、コールバックでは変更されたファイルの名前を元のファイル名に戻す必要があり、そうしないとすべての変更が失われます。

配布コールバックの実行が失敗した場合、ポリシー配布は HPOM 変数 `OPC_DEPLOY_IF_CALLBACK_FAILS` の値でコントロールされます。変数のデフォルト値は `TRUE` です。これはポリシーが任意のイベントで配布されることを意味します。最終的な警告メッセージは `system.txt` ファイルにログが記録され、メッセージブラウザにも記録される場合があります。

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実行可能ファイルで、ポリシーが管理対象ノードに配布された後に実行されます。

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マークされたままですが、その問題に関する情報が記載されたメッセージがアクティブなメッセージブラウザに送信されます。

配布後のエージェントでの設定ファイルポリシーを使用したコールバックの実行

設定ファイルポリシータイプを使用すると、設定ファイルポリシーの配布後にエージェントでコールバックを実行して、OV Composer ファクトストアの読み込みなどの一部の後処理を実行できます。

設定ファイルポリシー、その構文とキーワードについての詳細、およびエージェントでコールバックの実行を有効化する方法についての詳細は、『HPOM 管理者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、ツリー状構造で構成されます。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、世界全域で一意の UUID を持ちます。これらのグループ間を任意にリンクすることはできません。

注記

ポリシーグループ名に、スラッシュ文字 (/) やバックスラッシュ文字 (\) は使用できません。

管理対象ノードにポリシーグループの複数バージョンを配置できます。ポリシーグループの複数バージョンの管理についての詳細は、『HPOM 管理者リファレンスガイド』を参照してください。

デフォルトのポリシーグループ

デフォルトのポリシーグループは、HP Operations 管理サーバーで提供されます。ポリシーグループのリストを取得するには、次のコマンドを実行します。

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

次のデフォルトのポリシーグループは、HP Operations 管理サーバーで提供されます。

- ❏ 相関処理コンポーザー
- ❏ 例
- ❏ 例/ECS
- ❏ 例/Unix
- ❏ 例/Windows
- ❏ 管理サーバー
- ❏ SNMP
- ❏ SiteScope 統合/<SiteScope ポリシーグループ>

HPOM でのサブエージェントの管理

サブエージェントはHPOM の一部ではない製品ですが、部分的に HP Operations 管理サーバーから管理できます。一部のサブエージェントは、OV コントロールデーモンでコントロールできます。

HPOM でのサブエージェントの管理には、『HPOM 管理者リファレンスガイド』で概要が説明されているタスクが含まれます。

HPOM では、サブエージェント配布と配布解除のメカニズムが提供されていますが、実際のサブエージェント設定の詳細は、サブエージェントソフトウェアパッケージとともに提供されるマニュアルに記載されています。

サブエージェントポリシー

サブエージェントポリシーとは、サブエージェントという特殊なポリシータイプによ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。サブエージェントタイプポリシーのポリシー本体には、管理対象ノードでのサブエージェントインストールとアンインストールに関す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サプライヤーによって提供されます。内容についての詳細は、サブエージェントソフトウェアパッケージに同梱されているマニュアルを参照してください。

サブエージェントタイプのポリシーは、管理対象ノードには配布されず、他のタイプのポリシーとは異なり、ノードインベントリにも存在しません。

HP Operations 管理サーバーへのサブエージェントソフトウェアパッケージインストール中に、サブエージェントポリシーはサーバーに登録されます。ポリシーとポリシーが所属するポリシーグループは、その後 HPOM リポジトリに読み込まれます。

エージェント設定の配布中に、BBC 配布マネージャ (`opcbbcdist`) がポリシーの内容を確認し、サブエージェントポリシー本体に記載された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についての詳細は、『HPOM 管理者リファレンスガイド』を参照してください。

サブエージェントタイプのポリシーは、HPOM ポリシー管理のためのルールに適合しています。

アップグレードの注意点

HPOM 9.xx 管理サーバーには、同じサブエージェントの複数バージョンをインストールできます。ただし、管理対象ノードにインストールできるのはサブエージェントの 1 つのバージョンのみです。

サブエージェントパッケージの新しいバージョンを管理サーバーにインストールすることで、サブエージェントポリシーの新しいバージョンも配布されるため、どの管理対象ノードにどのバージョンをインストールするかをより簡単に決定できます。管理対象ノードでのサブエージェントのアップグレードは、サブエージェントポリシーの新しいバージョンの割り当てと、サブエージェントの配布によって実行されます。

注記

管理サーバーに新しいサブエージェントのバージョンをインストールすることは、自動的にすべての管理対象ノードが一緒にアップグレードされることは意味しません。目的のサブエージェントポリシーのバージョンをノードに手動で割り当てて、インストールを起動する必要があります。

アップグレードプロセスについての詳細は、サブエージェントソフトウェアパッケージに同梱されてい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は、メッセージを効果的に分類するための手段です。同じ機能または同じタスクに属するメッセージは 1 つのグループにまとめることができます。たとえば、メッセージグループ「バックアップ」には、データのバックアップと保管に関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や、バックアップ処理または保管処理に使われるハードウェアから送信されたすべてのメッセージなど) を含めることができます。作成されたメッセージグループはオペレータに割り当てられます。オペレータが表示、管理できるのは、自身に割り当てられているメッセージグループのみです。

管理者として、メッセージグループを追加、確認、削除できます。

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については、『HPOM 管理者リファレンスガイド』を参照してください。)`OpC` と `Misc` 以外のデフォルトメッセージグループは、必要に応じて削除できます。また、既存のグループの定義を変更したり、新規グループを追加することも可能です。

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調べることによって、環境内の各機能の状況をおおまかに把握できます。そのためには、登録メッセージグループを設定した後で、そこからオペレータに割り当てるグループを選択します。

アプリケーションの構成

アプリケーションとは、オペレータがシステムとネットワークサービスを保守および制御するために使うプログラム、コマンド、スクリプト、ユーティリティ、サービスのことです。たとえば、バックアッププログラムもプロセスステータスコマンド ps もアプリケーションとして組み込むことができます。標準アプリケーションやカスタムアプリケーション、および HPOM に組み込み済みのアプリケーションを統合できます。

HPOM に統合されたアプリケーションとアプリケーショングループは、opcappl コマンドラインツールを使用して管理できます。このツールについての詳細は、opcappl(1m) のマニュアルページを参照してください。HPOM では、デフォルトで複数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。詳細は『HPOM 管理者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

複数のアプリケーションを階層的にアプリケーショングループにまとめることができます。たとえば、複数のエントリポイントを持つアプリケーションは分けて使えるので、オペレータは各エントリポイントにそれぞれ別のアプリケーションとしてアクセスできます。また、複数のアプリケーションをまとめて論理グループを作成することもできます。

登録アプリケーションを階層化する際には、複数のアプリケーショングループを相互にネストします。

opcappl コマンドで -assign_app_to_grp オプションまたは -assign_grp_to_grp オプションを使用して、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ことができます。

アプリケーションの追加

アプリケーションを登録アプリケーションに追加するには、次のいずれかのアクションを使います。

❑ **HPOM アプリケーションの追加**

opcappl コマンドで -add_app オプションを使用して、HPOM アプリケーションを追加できます。アプリケーション名、アプリケーション呼び出し、ユーザー名、パスワードを指定する必要があります。ターゲットノードのリスト、ラベル、その他のパラメータを指定することもできます。その例を次に示します。

```
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 のメッセージブラウザで起動できるアプリケーションは、「オペレータが選択したターゲットノード上で実行」のタイプに属するアプリケーションに限定されます。

❏ **内部アプリケーションの追加**

`opcappl` コマンドで `-add_app_inter` オプションを使用して、ブロードキャストタイプの内部アプリケーションを追加できます。アプリケーションの一般情報とアプリケーションタイプを定義します。オペレータの名前とは異なるユーザー名を指定することもできます。ユーザー名を変更することもできます (アプリケーションの起動に root ユーザーが必要な場合など)。

注記

`opcappl` コマンドで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。

HPOM 登録ツールでアプリケーション (ツール) を作成する場合は、アプリケーションの各表示がアプリケーション自体にどう影響するかを熟知している必要があります。以下の 3 つの表示のいずれかを選択できます。

❏ ウィンドウ（出力のみ）

❏ ウィンドウ（入力/出力）

❏ ウィンドウなし

詳細は、『HPOM 管理者リファレンスガイド』を参照してください。

アプリケーション起動のカスタマイズ

Java GUI または `opcappl` コマンドで `-chg_app` オプションを使用して、起動される前に、あらかじめ設定されたアプリケーションの起動属性を変更できます。

HPOM 管理者がアプリケーションの起動属性を定義します。以後、オペレータは Java GUI からアプリケーションを直接起動できます。

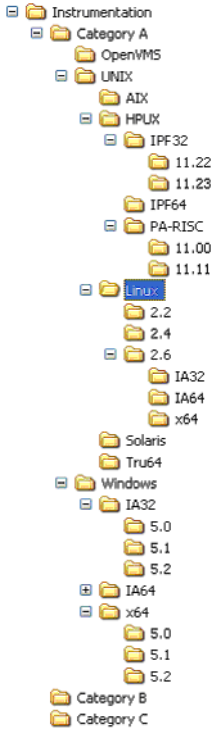
カスタマイズできる起動属性は次のとおりです。

❏ 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には、次の手順に従ってください。

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て、[次へ] をクリックします。
4. ツール実行に必要な追加情報を指定します。
   - 追加パラメータ

アプリケーション呼び出しでノード名がオプションとして受け入れられる場合は、[追加パラメータ] フィールドでノードを指定できます。たとえば、`-nodes` オプションを使用するアプリケーション呼び出しでは、オプションと引数 `-nodes $OPC_NODES` を使用できます。変数 `$OPC_NODES` はノードのリストを展開表示します。利用できる変数は、『HPOM 管理者リファレンスガイド』に記載されている一覧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。パスワードはアスタリスク(*) 文字列として表示されます。ユーザー名とパスワードを変更し、別のユーザーとしてアプリケーションを実行することもできます。

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対して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 にはデフォルトのユーザー名として `spooladm` が設定されています。

`opcappl(1)` コマンドラインツールについての詳細は、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 Agent など、多くの HP Operations Manager 製品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と、使用がロックされる可能性があります。

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とはテンポラリライセンスで、製品を 60 日間制限なしで評価目的に使用できます。このライセンスは HP Operations Manager のインストール中にインストールされ、初期化されます。このライセンスは、60 日の評価期間後に有効期限が切れます。製品の使用を継続するには、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。

- **恒久的なライセンス**

  本番ライセンスとは、通常の製品使用のためのライセンスです。すべての製品コンポーネントについて利用可能です。

  非本番ライセンスとは、バックアップシステムなど、特殊な目的のための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 のライセンスステータスは、1 日 1 回チェックされます。ライセンス取得済みオブジェクトのいずれかのライセンスステータスが OK ではなかったり、利用可能なライセンスの数が危険域に達すると、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。ライセンスステータスは、ライセンス管理ツールを使用して、いつでも確認できます。

ターゲットコネクタ数

必要とされるターゲットコネクタライセンス数を判断するため、データベースでメッセージが見つかったノードの数は 1 日 1 回カウントされます。HP Operations Agent がインストールされているノードには、ターゲットコネクタライセンスが必要ないため、カウントされません。

[today-31 days 00:00hrs] と [today 00:00hrs] の間の履歴データの値を使用して 30 日間の平均が計算されます。30 日間の平均はライセンスレポートに表示され、インストールされたターゲットコネクタライセンスの確認に使用されます。複数の値が保存されている日がある場合は、その日の平均値が 30 日の平均の計算に使用されます。

`opcremsyschk -list` コマンドを使用して、計算に使用された過去 30 日間の値を確認できます。

ライセンス通知

HPOM ライセンス供与済みコンポーネントのライセンスステータスには、「ライセンス取得済み」と「ライセンス未取得」の 2 つがあり、ライセンス違反通知 (警告) レベルには、注意域、重要警戒域、危険域の 3 つがあります。ライセンス違反通知レベルは、ライセンスタイプ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 - 注意域通知: 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、注意域通知が HPOM メッセージブラウザに送信され、電子メールがライセンス管理者に送信されます。

  レベル 2 - 重要警戒域通知: 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、重要警戒域通知が HPOM メッセージブラウザに送信され、電子メールがライセンス管理者に送信されます。

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

- **恒久的なライセンス**

  ライセンスがインストールされておらず、ライセンスが使用されていないと、ライセンスステータスは正常域と見なされます。

  レベル 1 - 注意域通知: 使用されているライセンスの数がインストールされているライセンスの数の 90% より大きく、100% より小さい場合、注意域通知が HPOM メッセージブラウザに送信され、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 - 重要警戒域通知: 使用されているライセンスの数がインストールされているライセンスの数の 100% より大きく、110% より小さい場合、重要警戒域通知が HPOM メッセージブラウザに送信され、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 - 危険域通知: 使用されているライセンスの数がインストールされているライセンスの数の 110% より大きい場合、危険域通知が HPOM メッセージブラウザに送信され、ライセンス管理者に電子メールが送信されます。使用されているライセンスの数がインストールされているライセンスの数の 110% より大きいとライセンスはロックされます。

小規模環境のサポート

小規模の HPOM 環境を少数の管理対象ノードでより適切にサポートするには、危険域のライセンスしきい値 (レベル 3) を 5 以上に設定する必要があります。

たとえば、HP Operations Agent ライセンスが 20 の HP Operations サーバーで、危険域通知レベル (レベル 3) は 22 ではなく 25 に設定するのが効率的です。こうすることで、不必要な制限が回避され、ライセンスがロックされる前に、追加システムをセットアップする柔軟性がユーザーに提供されます。

ライセンスの可用性

1 つ以上のライセンス取得済み製品コンポーネントについて、ライセンスがなかったり、ライセンスの数が不十分だという状況が発生する可能性があります。

- 利用可能な HP Operations 管理サーバーライセンスがないと、サーバープロセスは開始できません。不足しているライセンスはライセンスレポート、またはライセンスステータスの概要で報告されます。
- 利用可能な HP Operations Agent ライセンスがないと、新しいノードを HP Operations Manager データリポジトリに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、またはデータリポジトリから削除できます。不足しているライセンスはライセンスレポート、またはライセンスステータスの概要で報告されます。
- ターゲットコネクタライセンスの数が不足していると、不足しているライセンスはレポートされますが、実行が強制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の設定を完了すると、ユーザーの設定を開始できます。

その例を次に示します。

ユーザーのタイプ	作業の概要
オペレータ	管理対象ノードとオブジェクトの監視と保守

HPOM で設定できるユーザーの作業範囲についての詳細は、第 1 章「HPOM の概要」を参照してください。

設定した各ユーザーをデータベースに直接追加し、`opccfguser` コマンドラインツールを使用してオペレータを設定できます。

詳細は、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、コマンドラインツール `opccfguser` を使用します。ユーザー名を指定して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場合は、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 の管理者は、オペレータに広範囲な機能と強力なツールを提供することができます。オペレータは、環境中のシステムへのアクセス、すべてまたは特定のシステムで実行されるコマンドやスクリプトを発行したり、重要な修復アクションを実行できます。オペレータは、コンピューター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。このためには、オペレータコマンドとネットワークプラットフォームに関する基本的な知識を持ち、複数のタスクの中で優先順位を決定できなければなりません。

オペレータの作業範囲

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。オペレータにツールを指定する場合、オペレータにはそのツールを使うのに必要な経験と技術がなければなりません。また、管理対象のシステムに関する知識があり、環境内での担当者を知り、使用可能なアプリケーション、コマンド、およびスクリプトを理解でき、トラブルシューティングの手続きを使え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	アクションの起動と停止、受諾と受諾解除、メッセージの所有と所有解除、およびメッセージ属性の変更に関する属性。
作業範囲	割り当てられたノード上の、割り当てられたメッセージグループに属する全イベントの作業範囲。
アプリケーション	オペレータが利用可能な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を定義する、設定済みの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 のユーザーと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の詳細は、『HPOM 管理者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 環境に新規オペレータを追加するには、ユーザープロファイルという抽象的なユーザーを設定して、これらのユーザープロファイルをオペレータに割り当てる方法があります。または、既存ユーザーの設定をコピーして名前を変更します。新規オペレータの設定にこの方法を選んだ場合、そのオペレータに対して保存されたブラウザ設定も他のオペレータの設定データと共にコピーされることに留意してください。

デフォルトのオペレータプロファイル

HPOM にはデフォルトのオペレータプロファイル、opc_opが用意されており、既定の組織または環境の必要性を正確に反映する新しいオペレータプロファイルを作成するための基礎として使うことができます。

opc_op オペレータは、システム管理機能を制御します。opc_op オペレータは主にシステム環境内で作業し、アクセスできるのは一部のツール (プロセス、ディスク容量、印刷状況など) に限られています。デフォルトでは、opc_op にはすべての権限が与えられており、すべてのデフォルトメッセージグループが作業範囲です。

注記

opc_op オペレータは、ネットワーク動作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についての詳細は、「メッセージグループとノードグループの割り当て」(97 ページ) 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

オペレータに対するメッセージグループとノードグループの指定は 1 つの手順で行います。ノードグループをオペレータに指定すると、そのグループ内のノードが自動的にオペレータの作業範囲になります。ノードグループを選択してからオペレータが担当するメッセージグループを指定するか、メッセージグループを選択してからノードグループを指定します。

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、コマンドラインツール `opccfguser` を使用します。たとえば、「john」というユーザーに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に対する作業範囲を割り当てるには、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。

オペレータへのグループ割り当ての基準

オペレータにグループを割り当てる際の基準は次のとおりです。

ジョブ機能　オペレータにメッセージグループ「バックアップ」を割り当て、バックアップタスクを実行するノードが属する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 つの建物や施設内にあるすべてのノードグループ、および関連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 システムおよび関連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は、多数のメッセージを生成する場合が多く、注意が必要です。そのようなノードを1 人のオペレータに多数割り当てると、管理対象ノードの管理がきわめて困難になってしまいます。

オペレータの作業範囲の多重定義

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、オペレータの作業範囲を層に分けて定義できます。たとえば、各場所のノードグループをそれぞれ別のオペレータに割り当て、接続ネットワークのメッセージグループをその他のオペレータに割り当てます。同一の管理対象ノードグループやメッセージグループを複数のオペレータで管理するように設定することもできます。

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オペレータの作業範囲が決定される際にすでに決められています。オペレータに管理対象ノードの階層を割り当てるには、登録ノード階層内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［マップ選択の取込み］をクリックします。ノード階層の詳細は「HPOM ノード階層」(58 ページ) を参照してください。

ツールのオペレータへの割り当て

管理者はオペレータがその仕事の実行に必要なすべてのツールを持っていることを確認します。オペレータの仕事とは、割り当てられたノードの集まりのメッセージグループを管理することであり、オペレータが効率的にノードを管理できるように、必要なツールを決定しなければなりません。オペレータには、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などのすべてのツールを割り当てることができます。

オペレータが担当する管理対象ノードとサービスは、オペレータごとに異なります。それぞれのオペレータが互いに異なる作業を行うこともありうるため、各オペレータに割り当てられているノードグループやメッセージグループを調べる必要があります。

オペレータのツールセットの定義

オペレータ用のツールセットを定義する際には、ノードグループやメッセージグループに関して次の事柄を考慮します。

- ❏ どのようなサービスが提供されているか?
- ❏ 接続されている周辺装置は何か?
- ❏ どのようなシステムとインテリジェントデバイスが含まれるか?
- ❏ どのようなアプリケーションが動作しているか?

- ノードが特定の機能専用かどうか?

オペレータが適切なツールを持っているかどうかの検証

適切なツールを用意したかどうかを確認するには、次の質問で判断します。

- **アクセス**

  オペレータが管理対象のシステムにアクセスできるか?

- **アクション**

  自動アクションとオペレータ起動アクションが、各管理対象オブジェクトで発生する可能性のある危険域状態または注意域状態に対して十分に対応できるか?

- **権限**

  オペレータは管理対象ノード群ですべてのアプリケーションを実行できる権限を持っているか?

- **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うスクリプトと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アプリケーショングループの割り当て

アプリケーションとアプリケーショングループをオペレータ、オペレータのリスト、またはすべてのオペレータに割り当てるには、コマンドラインツール `opccfguser` を使用します。アプリケーションのリストをコマンドライン文字列で指定するか、割り当てるすべてのアプリケーションを指定したファイルを参照します。詳細は、opccfguser(1m) のマニュアルページを参照してください。

たとえば、`system_groups.txt` ファイルにリストされたアプリケーショングループをオペレータ `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の設定完了後、環境内にオペレータを容易かつ速やかに設定できます。必要な作業は、設定するオペレータに対応するプロファイルを指定するだけです。ユーザープロファイル設定の詳細は、「ユーザープロファイルの設定」(101 ページ) 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、コマンドラインツール `opccfguser` を使用します。その例を次に示します。

```
opccfguser -assign <profile name> -all
```

詳細は、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合計数を確認するには、直接、またはユーザープロファイルから、そのオペレータのレポートを生成します。詳細は「レポートの生成」(122 ページ) を参照してください。

ユーザープロファイルの設定

複雑な環境でも、ユーザープロファイルを使えばユーザー管理が容易になります。デフォルトの設定を使って抽象ユーザー群の階層セットを作成し、設定している実際のオペレータにそれを適用します。

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には、データベースの設定と保守を行うためのアプリケーションから構成されるアプリケーショングループが含まれます。これに加えて、データベースが動作する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すれば、HPOM 環境内のデータベースサーバー群を担当する新規のオペレータを簡単に設定できます。必要な権限を持つオペレータを追加し、データベース管理者にデータベースノード階層とユーザープロファイルを割り当てるだけです。新規オペレータの作業範囲やアプリケーションを拡張する必要がある場合 (ユーザープロファイルに含まれない作業範囲またはアプリケーションを追加する場合) には、それらを個別に割り当てます。

ユーザープロファイルは管理 UI を使用して設定できます。`opccfguser` コマンドを使用して、ユーザープロファイルをリスト表示、割り当て、割り当て解除することもできます。詳細は、opccfguser(1m) のマニュアルページを参照してください。

非 root での運用

非 root ユーザーは、root ユーザーと比較して使用できる権限が制限されたユーザーです。

非 root ユーザーとして操作するために満たす必要がある要件については、「非 root 操作の要件」(102 ページ) を参照してください。

注記

非 root ユーザーとして実行しているときに HP Operations 管理サーバーをホストするシステムを再起動すると、HPOM プロセスは `opc_op` ユーザーによって起動されます。

HPOM が非 root 操作モードの場合、`opcuiwww` プロセスは `opc_op` ユーザーによって常に起動されます。

非 root ユーザーの制限の範囲については、「非 root ユーザーの制限」(103 ページ) を参照してください。

重要

HPOM を非 root ユーザーとして実行すると、HP Operations Agent は非 root 混在モードで再設定されます。HP Operations Agent サイドの非 root 操作に関する要件と制限については、HP Operations Agent のドキュメントを参照してください。

非 root 操作の要件

HPOM を非 root ユーザーとして実行できるようにするには、次の要件を満たす必要があります。

- ❏ ポリシーを使ってログファイルをモニターできるようにするには、そのログファイルを読み込む権限が必要です。
- ❏ 自動コマンド、オペレータ起動コマンド、ツール、定期タスクを使用してプログラムを起動できるようにするには、そのプログラムを起動する権限が必要です。
- ❏ HPOM を非 root ユーザーとして管理するには、一次 UNIX グループを `opcgrp` に設定し、umask を `002` に設定する必要があります。

注記

非ユーザー操作に切り替えると、非 root ユーザーとしてしか動作できません。プロセスを root ユーザーで起動するには、`opcsv` コマンドを使用します。使用方法についての詳細は、opcsv マニュアルページを参照してください。

非 root ユーザーの制限

非 root 操作には次の制限が適用されます。

- RHEL 5.x では非 root 操作はサポートされていません。
- 一部の Smart Plug-in では、非 root ユーザーとして実行する場合に追加の設定または追加のユーザー権限が必要になる場合があります。詳細は、それぞれの Smart Plug-in に付属のドキュメントを参照してください。
- 管理サーバー上でローカルに実行されている HP Operations Agent のアップグレードは、root ユーザーでのみ行うことができます。
- `opcdbinit` および `opcdbsetup` コマンドは、root ユーザーしか使用できません。使用方法についての詳細は、これらのコマンドの該当するマニュアルページを参照してください。
- バックアップと復元スクリプト (`opcbackup_offline`、`opcrestore_offline`、`opcbackup_online`、`opcrestore_online`) は、非 root 操作モードで実行するように設定されている HPOM では使用できません。

非 root ユーザー設定

HPOM インストール/設定中、またはアップグレードプロセスでは、非 root ユーザーによって HPOM を実行するように設定できます。

詳細は『HP Operations Manager 管理サーバーインストールガイド』を参照してください。

非 root ユーザー特権とケーパビリティ

非 root ユーザーとして HPOM を実行すると、root ユーザーと比較して使用できる権限が制限されます。

ただし、通常 root ユーザーしか使用できない機能の一部が、特定の特権 (HP-UX および Solaris) またはケーパビリティ (Linux) を要求センダプロセス (`/opt/OV/bin/OpC/ovoareqsdr`) および `/opt/OV/bin/OpC/utils/opckilluiwww` バイナリに割り当てることで、非 root 操作に対しても有効になります。

次のケースがこれに該当します。

- ❏ HP-UX
  - `netrawaccess` 特権が要求センダに割り当てられます。これにより、要求センダプロセスは定期ポーリングを行うために ICMP パケットを送信できます。
  - 所有者特権は `/opt/OV/bin/OpC/utils/opckilluiwww` バイナリに割り当てられます。

    これにより、HP Operations 管理サーバープロセスが停止した場合に Java GUI を停止できます。
- ❏ Linux
  - ❏ `cap_net_raw` ケーパビリティが要求センダに割り当てられます。これにより、要求センダプロセスは定期ポーリングを行うために ICMP パケットを送信できます。
  - ❏ `cap_kill` ケーパビリティは `/opt/OV/bin/OpC/utils/opckilluiwww` バイナリに割り当てられます。

    これにより、HP Operations 管理サーバープロセスが停止した場合に Java GUI を停止できます。
- ❏ Solaris

  `setuid` ビットは `ovoareqsdr` バイナリに設定されます。バイナリの所有者は root であるため、このプロセスは root ユーザーとして起動されます。

  ただし、要求センダは特権対応のアプリケーションであるため、その特権を要求されたものだけに制限します。

  次のケースがこれに該当します。

  - ❏ 有効な特権: `basic`、`net_icmpaccess`
  - ❏ 継承可能な特権: `basic`、`proc_owner`

HPOM の設定の更新

本項では、HPOM のインストール後に行う設定の変更を説明します。HPOM ソフトウェアのインストールの詳細は、『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

最初のソフトウェアインストールと設定は、常に管理サーバー上で行います。最初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。設定の変更 (ノード、モニタープログラム、ポリシーの追加など) は管理サーバーで実行し、変更を行うたびに管理対象ノードに変更内容を配布します。

設定の部分的な配付

HPOM 管理者は、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、新しいノードを追加したり、特定の管理対象ノードの設定を更新する際には、そのノードに管理サーバーからソフトウェアを配布します。

配布するソフトウェアは次のとおりです。

- **エージェントソフトウェア**

  管理対象ノード用の HPOM ソフトウェア (アクションエージェント、メッセージエージェント、およびモニターエージェントなど) をすべて含みます。必要な配布は 1 回だけですが、管理対象ノードを新たに設定に追加するたびに、エージェントソフトウェアを新しいノードに配布しなければなりません。また、新しいバージョンのエージェントソフトウェアをインストールする場合も、このソフトウェア構成要素を選択する必要があります。

- **ノード設定**

  次の各項目が含まれています。

  - ポリシー

    設定されたメッセージとモニターソース、および MoM 設定ポリシー。ポリシーはそれが使われる管理対象ノードに配布します。

- アクション

  自動アクションや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、またはアプリケーション。アクションはそれが開始されるそれぞれの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う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、それを起動するノード上に配置します。

- 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、あるいはJava GUI で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、またはアプリケーションは、それを起動する管理対象ノードに配布します。

ソフトウェア配布の準備

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。このファイルは他の管理対象ノードに後で配布できるように保存されます。

注記

ファイルが配布前に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たか、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 は設定の変更された部分のみを更新します。

管理対象ノードへの設定の配布

管理サーバーから管理対象ノードへ設定をインストールまたは更新するには、次の手順を実行します。

1. インストールまたは更新される設定を定義します。
2. ポリシーをノードに割り当てます。
3. 設定のインストールまたは更新の方法を定義します。

設定のインストールや更新には、`opcragt -distrib` オプションを使用します。設定内の配布する部分を指定します。`-force` オプションを使用すれば、設定全体を置き換えることができます (例: **`opcragt -distrib -force`**)。

注記

エージェントソフトウェアは、`inst.sh` コマンドを使えば、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。さらに、`opcragt` コマンドを使えば、ポリシーやアクション、モニター、またはコマンドを手動で管理対象ノードに配布できます。どちらのコマンドも非対話モードで実行できるため、インストールや更新は夜間や週末など、任意の時間に実行されるようにスケジュール設定できます。詳細は 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 Agent ソフトウェアの手動インストールについての詳細は、HP Operations Agent のドキュメントを参照してください。

強制アップデート

`force` オプションを選択せずに標準のインストールや更新を実行すると、設定に含まれる新しい情報だけが転送されます。デフォルトでは、変更されていない情報は転送されず、それによりネットワークの負荷が減少し、転送時間が短縮されます。`force` オプションを使うと、HPOM は指定されたすべての設定のインストールまたは更新を、選択された管理対象ノードで実行します。

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、それを必要としてい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再配布します。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に変更を行ったときは、ポリシーのインストールまたは更新が必要になります。

たとえば、管理対象ノード上のプロセス数をチェックするモニタースクリプトを作成したとします。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または更新します。ポリシー本体の構文についての詳細は、付録 A「ポリシー本体の構文」(355 ページ) 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をインストールまたは更新する処理が必要になることもあります。詳細は「しきい値モニターからのメッセージ」(257 ページ) を参照してください。

新規メッセージソースポリシーの定義が完了し、ポリシーをポリシーグループに含め、そのポリシーまたはポリシーグループを管理対象ノードに割り当てた後、それ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 は次の各ポリシーを管理対象ノードにインストールします。

- ❏ 対象のノードに割り当てられている全ポリシー
- ❏ 対象のノードに割り当てられているポリシーグループ内の全ポリシー
- ❏ 対象のノードを含むノードグループに割り当てられている全ポリシー
- ❏ 対象のノードを含むノードグループに割り当てられているポリシーグループ内の全ポリシー

注記

ポリシーまたはポリシーグループを削除または変更したり、特定のノードに対するポリシーの割り当てを解除した場合、それらの変更を反映するには、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。

変更中のポリシーはロックされており、管理対象ノードには配布されません。HPOM 管理者は、管理対象ノードへのポリシーの割り当てを確認し、配布すべきポリシーをチェックするために、配布レポート (ノード設定レポート) を生成できます。詳細は「レポートの生成」(122 ページ) 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 <node name>
```

ポリシーとノードの重複する組み合わせの自動回避

HPOM は配布を開始する前に、各ポリシーが管理対象ノードに一度だけインストールまたは更新されること、およびポリシーとノードの無効な組み合わせが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属したり、複数のノードに割り当てられる場合があるため、同じポリシーが同じノードに 2 回割り当てられる可能性があります。また、ポリシーとノードの組み合わせが無効な場合もあります。たとえば、特定プラットフォーム用のポリシーが、他のプラットフォームで稼動しているノードに割り当てられる場合などです。

1 つの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 は重複した割り当てを無視し、ポリシーの配布を一度だけ行います。

配布のヒント

本項では、HPOM のソフトウェア、設定、およびポリシーを、より迅速かつ容易に配布するためのヒントを説明します。

更新が必要なノードのみを更新

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、コマンドラインツール `opcragt` を使用します。このツールを `-distrib` オプション付きで使用すれば、1 個のノード、ノードグループ、または全ノードのいずれに対しても更新を適用できます。例: ノードグループに更新を適用する場合

```
opcragt -distrib -nodegrp <group>
```

`<group>` には、ノードグループの名前を指定します。

詳細は、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には、モニター、アクション、およびコマンドを各クラスタクライアントに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数多く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方法は次のとおりです。

- ❑ **ノード数を最小限に抑える**

  `OPC_MAX_DIST_REQS` 構成変数を使用して、同時に新しい設定データを受信する管理対象ノードの数を最小限に抑えます。

- ❑ **優先度を下げる**

  `nice(1)` コマンドを使って、管理サーバー上の `opcbbcdist` プロセスの優先度を下げます。

- **カテゴリベースの配布方法、または選択的配布機能を使用する**

  `opcbbcdist` のカテゴリベースの配布方法、または選択的配布機能を選択して、特定のノードで必要とされない特定の設定ファイルの配布を回避します。

  カテゴリベースの配布方法、または選択的配布機能についての詳細は、『HPOM 管理者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

管理対象ノードにポリシーを手動で配布することが望ましい場合もあります。たとえば、夜の間に配布が行われるようにスケジュールする場合、またはセキュリティ基準でネットワーク経由でのポリシーの転送が許可されていない場合です。HPOM は次の種類の手動配布をサポートします。

- **ネットワーク経由**

  `opcragt` コマンドラインツールを `-distrib` オプション付きで実行して、ポリシーやアクション、コマンド、およびモニターを管理対象ノードに配布します。詳細はマニュアルページの opcragt(1m) を参照してください。

- **その他の媒体**

  ネットワーク経由での設定の配布が望ましくない場合には、コマンドラインツール `opctmpldwn` を使えば、ポリシーを暗号化してダウンロードできます。ダウンロードした設定を管理対象ノードまで移動する方法は任意です。詳細は、マニュアルページ opctmpldwn(1m) を参照してください。

オペレータ設定を伴わない配布

新しいオペレータを追加する際には、そのオペレータの作業範囲にな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。追加したオペレータが特殊なログオンやアプリケーション起動のカスタマイズ、またはブロードキャストコマンドを実行できる場合、これらの機能をオペレータが使うたびに、対応するオペレータ設定情報が管理対象ノードによって検証されます。この情報は、ソフトウェアや設定と共に配布することはありません。

設定変更の同期

HPOM のデータ同期機能では、HP Operations サーバーコンポーネント内 (GUI、HP Operations 管理サーバープロセス、API など) の設定データの自動更新が提供されています。

設定の更新には、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、グループ替えが含まれます。

設定変更は、ポリシーの更新など、1 つの設定オブジェクトで実行できる簡単な操作です。または、1 つの種類の設定オブジェクトが別の種類の設定オブジェクトに割り当てられたり、割り当て解除される場合、たとえば、ノードをノードグループに割り当てるのは、複雑な操作になります。HPOM では、オンラインの設定更新が使用できますが、これは設定変更がサーバープロセスと GUI の再起動なしで適用されることを意味します。

HPOM 設定はデータベース、設定ファイル、構成変数に保存されます。`opccfgupld` ツールで設定が変更されるたびに、データベースの変更がアップロードされます。`ovconfchg` ツールが使用されるたびに、サーバープロセスで使用される大多数の構成変数の内容が更新されます。構成変数についての詳細は、『HPOM 管理者リファレンスガイド』を参照してください。

次の HPOM 設定ファイルは、`ovconfchg` ツールが使用されるときに再ロードされます。

- 運用停止ポリシー
- メッセージ転送ポリシー
- MSI conf. ファイル
- 内部名前解決 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 は、内部 (サーバープロセス、Java GUI) および外部 (API クライアント) の設定コンシューマーに対して設定変更の登録機能を提供します。Java GUI とサーバープロセスはデフォルトで設定変更に登録されます。`opcif_*` API を使用して、設定変更通知に登録できます。

再設定後の GUI の同期

HPOM 設定の更新が実行されると、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 設定オブジェクトで関連する変更が実行されます。

HPOM には、設定更新中にサーバーと Java GUI を同期させる機能があります。ほとんどの設定変更が自動的に Java GUI に反映されるため、再起動する必要はありません。関連する設定の変更点を GUI 上ですぐに確認することができます。

たとえば、ノード階層が変更されたり、アプリケーションがアプリケーショングループに追加された場合、同期させる機能によって、GUI を再起動したり、ログオフしてログインし直したりせずに、これらの変更を確認できます。

ただし、大規模な設定変更 (`opccfgupld` を使用した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や割り当て解除など) の場合は、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。自動サービス再ロードオプションを無効にしたフィルター定義の更新やサービスの変更にも再ロードが必要です。Java GUI からログアウトする必要はありません。

注記

設定ストリームインタフェース (CSI) に接続されている場合、同期イベントは外部ユーザー (設定 API のユーザーなど) に転送されます。

設定更新ツール `opccfgupld` が実行されている場合、Java GUI への新しいログインはブロックされ、「`opccfgupld` の実行中はログインできません」、というエラーメッセージが表示されます。

最新コンテンツへの自動アクセス

HPOM 管理者 GUI セッションを初めて開く直前に、新しいウィンドウに HPOM データベースから直接最新データが読み込まれます。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通り終了しますが、メニューの [クローズ] オプションや [終了] オプションとは異なり、終了の確認はありません。[セッションの再起動] オプションは開いているウィンドウをすべて閉じ、[設定の保存/ホームセッション] で保存された最新の設定 (ノード、メッセージ、およびアプリケーション各グループの内容と設定を含む) を使って HPOM セッションを再開します。ただし、セッションの終了前に設定と詳細を保存していない場合には、[アプリケーションの出力] ウィンドウや [レポートの出力] ウィンドウなどのウィンドウは開かず、開いたウィンドウの位置もセッション終了時とは異なる場合があります。このシステムの動作は、ログアウトして再ログインする場合と同様です。

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って変更されているデータはロックされ、他のアプリケーションやユーザーが並行して変更できないようになっています。変更後、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、更新された設定データを確認して使用できるようになります。

HPOM では、設定データの変更後にコンポーネントを同期するため、ロックを使った**トランザクション**の概念が使われます。このトランザクションの概念では、ユーザートランザクションの開始、コミット、およびロールバックを実行する API 関数がサポートされています。

データのバックアップと復元

本項では、HP Operations 管理サーバーでデータをバックアップおよび復元する方法を説明します。

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**

  手動のオフラインバックアップ。自動バックアップに必要なリソースが得られない場合、`opcbackup_offline` スクリプトと `opcrestore_offline` スクリプトを使って、オフラインで完全なバックアップを行えます。

- **opcbackup_online**

  自動バックアップ。`opcbackup_online` を使って自動バックアップを行う場合、バックアップ開始時までに完了できなかったタスクはアイドル状態となり、バックアップ完了と共に再開されます。

バックアップ方法の比較

バックアップを計画および実行する際には、HPOM の設定が管理対象ノードだけでなく、管理サーバーも含んでいることに留意すべきです。したがって、管理サーバー上で復元された設定が管理対象ノード上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不正な割り当てなどに関するエラーが発生することがあります。

表 2-3 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 2-3 バックアップ方法の比較

バックアップ方法	バックアップの種類	利点	短所
opcbackup_offline	オフライン	• オンにする必要がないため、 — システム全体のパフォーマンスが高い — ディスク消費が抑制される • バイナリデータもバックアップする (フルモード使用時) • オフラインで完全なバックアップが実行される	• すべての Java GUI インスタンスを閉じる必要がある • HP Operations サーバープロセスを含むすべての HP Software サービスが停止する • 復元は前回のフルバックアップ時の状態のみ
opcbackup_online	自動	• HPOM オペレータ用 Java GUI、トラブルチケット、および通知サービスは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復元が可能 — 指定時刻まで復元 — 損傷した表の個別復元 • HP Software プロセスはバックアップ中もすべて動作する	• バックアップスクリプトにより、一部の HP Software サービスが一時的に停止する • アーカイブログまたは WAL を有効にする必要があるため、 — システム全体のパフォーマンスが低下する — より多くのディスク領域を消費する • バイナリファイルや一時ファイル (キューなど) はバックアップされない

データの復元

HPOM データベースの復元

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 でバックアップされたデータは、opcrestore_offline で復元します。同様に、opcbackup_online でバックアップされたデータには opcrestore_online を使います。

opcrestore_online スクリプトを使用すると、Oracle または PostgreSQL データベース全体をバックアップ時の状態に復元できます。

Oracle データベースを使用する場合、データベースを最新の状態に復元することもできます (ロールフォワードはオフライン REDO ログに基づいて実行されます)。

さらに、Oracle アーカイブログモードを使えば、さらに柔軟な復元処理が可能です。たとえば、Oracle アーカイブログモードでは次の処理を行うことができます。

- **ファイルの個別復元**

  破損した Oracle データファイルをバックアップから個別に取り込み、オフライン REDO ログを使用して復元できます。

- **指定時刻の状態への復元**

  オフライン REDO ログを使用して、特定の時点における Oracle データを復元できます。

注記

アーカイブログモードとは 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。データファイルへの変更は REDO ログファイルに保存されます。これらの REDO ログファイルはその後アーカイブされます。

詳細は、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

本項では、問題解決のために実行する操作に対して所有権が与える影響を説明します。

管理者は、HPOM でサポートされているいずれかの所有権モードを選択して、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の詳細は、『HPOM 管理者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

メッセージのマーキングと所有は、システム環境とその保守における自身の役割を理解するために欠かせない概念です。

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を払っていることを示します。所有権通知モード。

- **所有**

  特定のメッセージに応じて関連するアクションを実行することをユーザーが望んでいるか、または実行が強制されることを示します。前者はオプション、後者は強制の所有権モードであり、どちらが該当するかは環境設定に左右されます。

所有権表示モード

HPOM には、次の**所有権表示モード**があります。

- **ステータスの伝達なし** (デフォルト)

  メッセージが所有またはマーキングされると、メッセージの重要度を示す色が変わり、Java GUI メッセージブラウザの所有状態カラムにフラグが表示されます。メッセージブラウザの所有状態カラーバーは、所有メッセージの新しい数を反映するようになります。所有またはマーキングされたメッセージのステータスは、オブジェクトペイン、オペレータのメッセージグループおよびノードグループ、管理者の登録メッセージグループのステータス伝達の目的については無視されます。

- **ステータス伝達**

  メッセージが所有されているかどうかによらず、メッセージのステータスが他のサブマップウィンドウ内の関連するシンボルのステータスを決定します。したがって、危険域メッセージに関連する管理対象ノードは、そのメッセージが所有された後も、危険域の重要度を示す色 (デフォルトでは赤) で表示されます。この表示モードでメッセージの所有状態を確認する手段は、[メッセージブラウザ] の所有状態カラムのみです。

たとえば、ステータス伝達なしの表示モードで特定の管理対象メッセージに関連する唯一の危険域メッセージを所有すると、その管理対象メッセージは危険域の重要度を示す色 (デフォルトでは赤) では表示されなくなり、[メッセージブラウザ] ウィンドウで自身に関連付けられている非所有メッセージのうち、所有されたメッセージに次ぐ重要度の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の詳細は『HPOM 管理者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 (Optional)**

ユーザーにメッセージを所有する明示的な権限があります。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/書き込み権を持ちます。このモードで所有されたメッセージが [メッセージブラウザ] に表示されても、所有者 (および HPOM 管理者) 以外のユーザーには限定的な操作しか許可されません。

このモードでは、次の各操作はメッセージの所有者のみに許可されます。

- 当該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/終了
- 当該メッセージに関連する自動アクションおよびオペレータ起動アクションの終了/再開
- 当該メッセージの受諾
- 当該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。

このモードでは次のことを実行すると、オペレータは自動的にメッセージを所有します。

- メッセージに関連するオペレータ起動アクションの起動/停止
- 当該メッセージに関連する自動アクションおよびオペレータ起動アクションの終了/再開
- メッセージの受諾解除

❏ **通知**

所有権の代わりにメッセージのマーキングとマーク解除の概念が使用されます。メッセージの**マーキング**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。マーキングは通知のみを意図しており、オプションや強制の所有権モードのようにメッセージへの操作を制限したり、変更することはありません。オペレータがマーク解除できるのは、自身がマーキングしたメッセージだけです。管理者はすべてのマーキングメッセージをマーク解除できます。

レポートの生成

HPOM は、強力なレポート作成ツールと、ネットワークの基本的な構成要素からサービスの利用可能状況まで広範な情報を提供するレポートを備え、複雑で包括的なレポートを作成するというニーズに応えます。レポートは自動化され、さまざまなフォーマットで表示できます。一般に、レポートの範囲と可能な設定はユーザーのタイプによって異なります。たとえば、HPOM 管理者は他の HPOM ユーザーに比べ、より多くのレポート機能を利用できます。

レポートツール

レポートの作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 をベースにした HPOM で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

- **データベースへのアクセス**

  作成したスクリプトによるデータベースへの直接アクセス

『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、レポートを定義および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 環境内で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 で作成できるレポートは 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起動したアクションの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に関するレポートも生成できます。

- **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履歴メッセージを対象としたレポートを生成する場合、メッセージバッファーに大量のメッセージが格納されていると、レポートの生成に数分かかることがあります。

生成するレポートの種類とレポート出力メディアを選択します。ユーザーのスコープや作業範囲に従って、ユーザーのレポートの選択は異なります。

メッセージ、エラー、設定の各レポート

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**

  レポートは 1 つのメッセージに対しても、[ブラウザ] ウィンドウに表示されたすべてのメッセージに対しても生成できます。詳細は、『HPOM 管理者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含みます。

  これらのメッセージは、次のファイルに出力されます。

  `/var/opt/OV/log/System.txt` (テキスト形式)

  `/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、アクションなどに関する設定情報を含みます。

利用可能なレポートの詳細と、それらが対象とする範囲の簡単な説明は『HPOM 管理者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 を使用すると、HPOM 環境内の特定時点または特定の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 の管理環境を対象として、あらかじめ設定されたサービスレポートを生成します。このレポートには、メッセージのスループット、障害の通知に要した時間、傾向、および設定の概要を示す情報が含まれます。

たとえば、HP Reporter に付属している HPOM サービスレポートを使えば、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
- 自動アクションと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

これらのレポートの内容の詳細とレポート対象範囲については『HPOM 管理者リファレンスガイド』および HP Reporter のマニュアルを参照してください。

サービスレポートを特定の時間にスケジュールできるほか、取り込まれた情報を 3 通りの形式 (グラフ、ダイアグラム、統計表) で表すことができます。さらに、Web サーバーを適切に設定して稼動させれば、レポートを自動的に更新して Web 上で公開することも可能です。HP Reporter の詳細は、同製品のマニュアルを参照してください。Web サーバーをインストールし、HPOM 用に設定する方法は、『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

管理者とオペレータは、HPOM 環境内でさまざまな種類の内部レポートを作成できます。レポートのフォーマットには、簡略形式と詳細形式があります。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) タイプです。PGM レポートはプログラム、スクリプト、もしくは INT (内部) タイプレポート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。PGM レポートタイプは、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、他のプログラムやスクリプトも PGM レポートを利用します。

内部レポートのフォーマット

オペレータ用に生成される簡略形式の内部レポートには、次の情報が含まれます。

- ❏ レポートの生成日時と種類
- ❏ メッセージの全属性 (メッセージテキストを含む)
- ❏ オリジナルのメッセージテキスト

独自レポートの定義

HPOM のレポート機能により、HPOM アプリケーション、サードパーティー製ツール、または自分で作成したスクリプトでデータベースから直接抽出した情報の独自レポートをデザイン、生成できます。

HPOM 管理者は、標準以外のレポートを自身で定義することも可能です。詳細は、『HPOM 管理者リファレンスガイド』と『HPOM Reporting and Database Schema』を参照してください。

新しいレポートの設定は、新しいスクリプトまたはプログラムの作成、または新しい SQL ファイルの作成によって行われます。その場合、既存のテキスト形式のファイルを編集して、新しいレポートに統合します。これらの設定ファイルは、管理者向けのレポートとオペレータ向けのレポートを定義します。HPOM のスケジュールアクションポリシーにレポートの出力時間を設定し、HPOM のツールを使って抽出した情報を表示できます。

HPOM の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、およびコンテンツの利用方法については、『HPOM Reporting and Database Schema』を参照してください。

独自レポートの組み込み

管理者は自身で定義したレポートを HPOM に組み込むことができます。独自レポートの作成と組み込みの詳細は、『HPOM 管理者リファレンスガイド』と『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

本章の内容

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、以下のとおりです。

HPOM 管理対象ノードについての詳細は、『HPOM 管理者リファレンスガイド』および HP Operations Agent のドキュメントを参照してください。

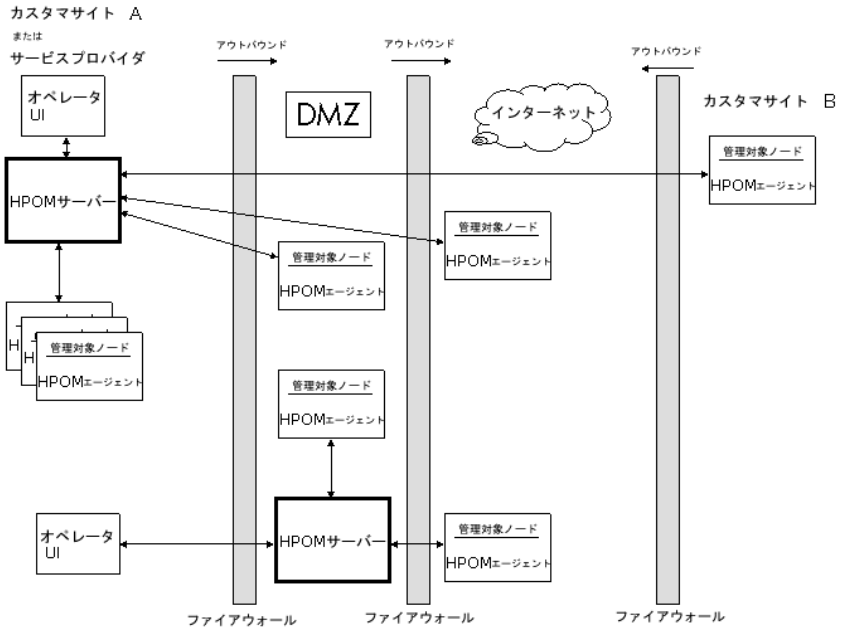
HTTPS エージェントの概要

HTTPS エージェントソフトウェアは、HP Operations 管理サーバーと管理対象ノードの間にセキュアな通信を提供します。

図 3-1 は、HP Operations Manager によって管理される一般的な環境を示しています。

HTTPS エージェントを使用するメリットについては、後の章で説明します。

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。

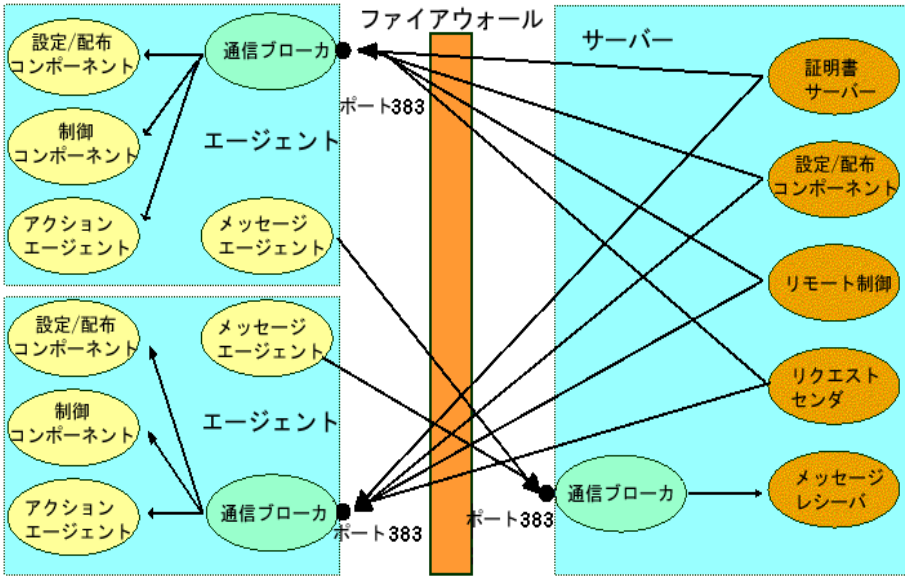
- HTTPS ベースのオープンな通信方法を使用する、設定可能な単一ポートのセキュアな通信とファイアウォールの組み合わせによるシンプルな管理。外部アクセスを専用の HTTP プロキシに制限し、HTTP プロキシの多重化によりポート使用率を削減します。

- SSL/PKI 暗号化およびサーバー / クライアント証明書による認証を使用する、追加の設定を必要としないセキュアなインターネット通信。
- 現代のあらゆる環境で利用でき、すべての IT 管理者によく知られている標準的な 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セキュリティに使用される XML と SOAP に基づく HPOM メッセージフォーマット。
- IP の非依存性/動的 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。
- 追加投資の必要がない (トレーニング、追加のソフトウェア)。
- HP Operations 標準のコントロールと配布メカニズム。
- HP Operations 標準のログ機能。
- HP Operations 標準のトレース機能。

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作業範囲

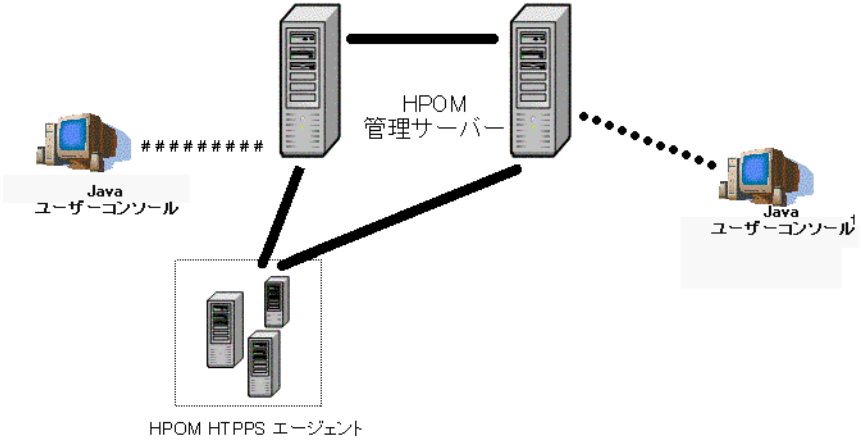


HPOM における HTTPS 通信

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、異なるシステム間でアプリケーションのデータ交換を可能にします。

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



HTTPS 通信
•••••••• ソケット通信 + OV 拡張セキュリティによる SSL
ソケット通信
+++++++ OV 拡張セキュリティによる共通鍵暗号

1. HPOM Java GUI との通信には、ソケット通信が使用されます。
OVAS がインストールされている場合、SSL による ソケット通信が使用されます。

メリット

HTTPS 通信には、次のような主なメリットがあります。

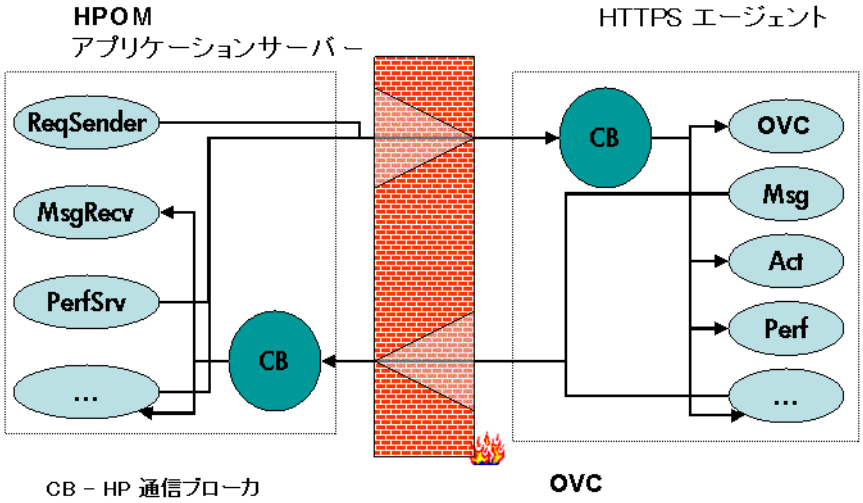
- ファイアウォールとの親和性
- 安全性
- オープン性
- 拡張性

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でセキュリティで保護され、管理が簡単な方法を求めています。このような企業の多くは、HTTP、HTTP プロキシ、ファイアウォールについてよく知っていて、使い慣れています。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でき、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 通信を使用したファイアウォールの通過を示しています。

図 3-4 HTTPS 通信を使用した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。

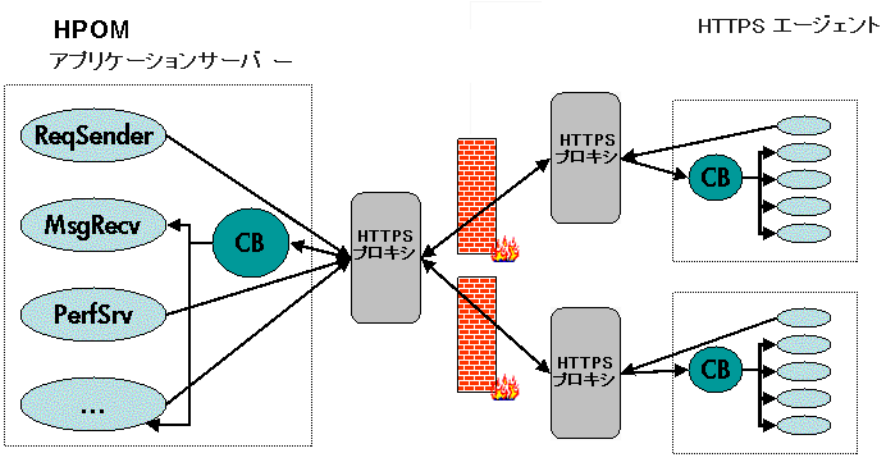
さらに次のような特徴があります。

- 受信するすべてのリモートメッセージ / リクエストは通信ブローカを経由するため、ノードへのポートエントリが 1 つになります。
- 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。

- メッセージ、ファイルまたはオブジェクトの送信時にファイアウォールを横断したり、リモートシステムに到達したりできるように、1 つ以上の標準 HTTP プロキシを設定します。

図 3-5 は、標準 HTTPS プロキシを使用したファイアウォールの横断を示しています。

図 3-5　外部 HTTPS プロキシを使用したファイアウォールの通過



HTTPS 通信とプロキシで作業するには、以下の作業が必要です。

- HTTP プロキシサーバーの設定
- SSL 暗号化の実装
- サーバー証明書によるサーバー側認証の確立
- クライアント証明書によるクライアント側認証の確立

HP Operations でこの作業を行う方法については、以下の項で説明します。

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 HTTP、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 エージェントのコンテンツフィルタリングはサポートされていません。

HTTP プロキシは現代のネットワークで広く使われています。プライベートネットワークとインターネットを安全に橋渡しするために非常に便利です。HTTP を使用することによって、HP Operations を後から導入しても現在のインフラストラクチャを活用できます。

拡張性

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、使用する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、消費するリソースを最小限に抑えながら、多数の同時接続を処理できます。設定した最大接続数を超過すると、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表示することもできます。

通信 (ブローカ) アーキテクチャ

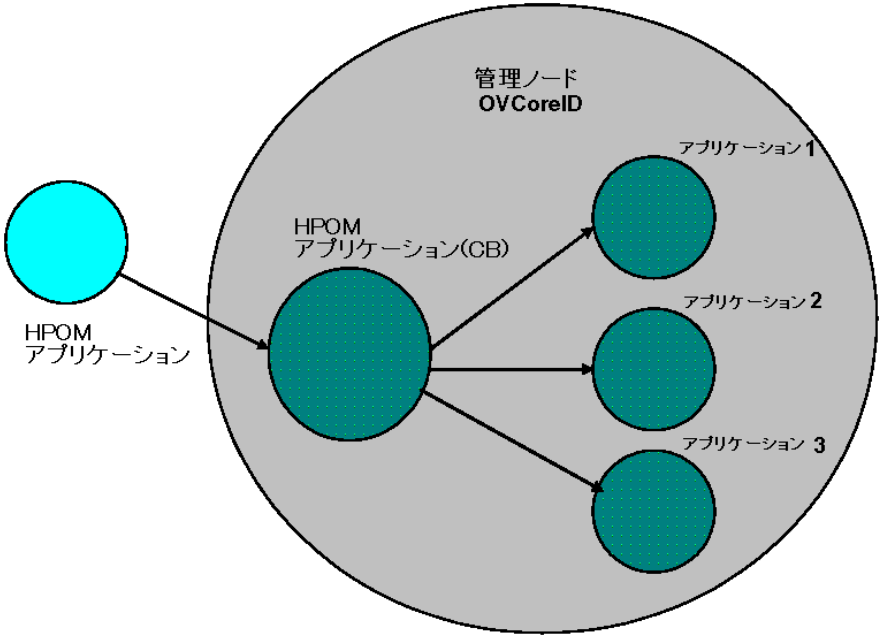
通信ブローカは、ローカルの管理対象ノードでプロキシとして機能し、その管理対象ノード上のすべてのアプリケーションについて、管理対象ノードへの一元的なエントリポイントを提供します。データを受信するアプリケーションは、通信ブローカにアドレスを登録します。登録により、ポート番号、プロトコル、バインドアドレス、およびアプリケーションがデータの受信に使用するベースパスが定義されます。他のローカルまたはリモートのアプリケーションは、通信ブローカにアプリケーションの場所を照会するか、通信ブローカをプロキシとして使用して、登録されたアプリケーションに要求を転送します。通信ブローカは、標準の HP Operations 設定ファイルから設定データをロードします。

通信ブローカには、以下の特徴があります。

- 通信ブローカは、管理対象ノードに単一ポートのソリューションを提供します。この管理対象ノードのすべての登録済みサーバーに対する要求は、通信ブローカを介して転送できます。通信ブローカは、HTTP プロキシが HTTP 要求を転送するのと同じ方法で、要求を登録済みサーバーに透過的に転送します。通信ブローカへのデフォルトポートは 383 ですが変更可能です。
- UNIX システムでセキュリティを高めるために、通信ブローカの起動時に `chroot` を使用できます。`chroot` は、指定したパスをルートディレクトリとして機能させて通信ブローカプロセスに表示されるファイルシステムの一部を制限することで、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 ユーザーとして通信ブローカを実行できます。
- 通信ブローカは、UNIX システムの root ユーザーのみが実行してポートを開いてから、その他すべての操作を非 root ユーザーに切り替えるように設定できます。
- 通信ブローカは、次の操作に対応しています。
  - UNIX システムでデーモンとして起動する
  - Windows システムに Windows サービスとしてインストールする
- 通信ブローカの制御コマンドは、対象をローカル管理対象ノードに制限できます。
- 通信ブローカは、ネットワーク経由のデータ通信に対し、SSL 暗号化を適用します。

- 通信ブローカは、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 通信ブローカのアーキテクチャ



通信ブローカは、受信データを管理対象ノードで受け入れるために最低 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、ポートは OVCoreID と関連付けられます。通信ブローカは、可用性の高い管理対象ノードに対して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 を関連付けできます。SSL を有効にすると、ポートには X509 証明書が設定されます。これらの証明書を使用すると、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。

通信ブローカに登録されている現在の管理対象ノード上のすべてのアプリケーションは、通信ブローカによって開かれたすべてのアクティブな受信ポートに自動的に登録されます。

デフォルトの名前空間 bbc.cb に関連付けられたポートは、通信ブローカの起動時に自動的にアクティブになります。その他のポートは、起動後に動的にアクティブまたは非アクティブにできます。詳細は、通信ブローカのコマンドライン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

本項では、次の HPOM セキュリティの概念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」(140 ページ)
- 「リモートアクション」(144 ページ)
- 「ロールとアクセス権」(145 ページ)

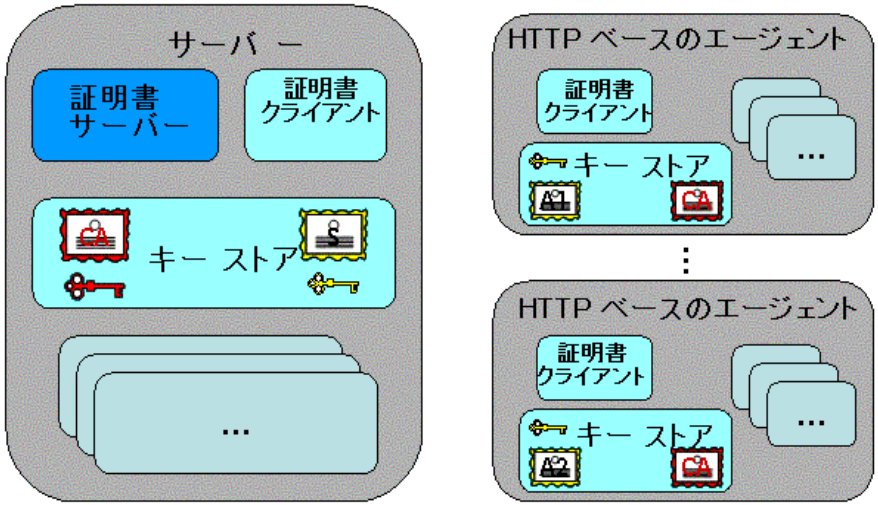
HTTPS ベースのセキュリティコンポーネント

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、有効な業界標準の X509 証明書が必要です。Secure Socket Layer (SSL) プロトコルを使用して管理対象環境で管理対象ノードを識別するには、1024 ビットキー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の「SSL ハンドシェーク」は、着信側の管理対象ノードによって提示された証明書を発行した認証局が、受信側の管理対象ノードの信頼できる認証局である場合のみ成功します。証明書の作成と管理を担当する主な通信セキュリティ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。

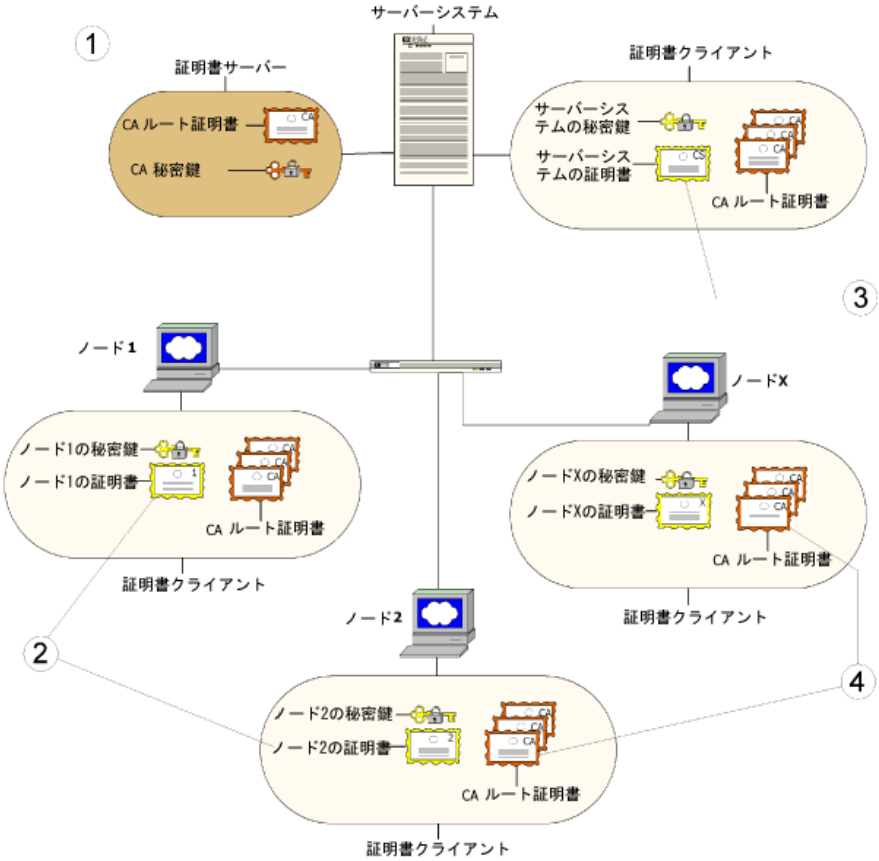
図 3-7 認証された通信のコンポーネント



`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` は、インストール中に値を割り当てられます。

図 3-8 は、認証された通信のための環境を示しています。

図 3-8 認証された通信のための環境



1. サーバーシステムは、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証明書サーバーによって署名された、認証局の秘密キー付きの証明書があります。
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、信頼できるルート証明書のリストがあり、これには少なくとも 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、信頼できる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 管理サーバーで管理されている場合、信頼できる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

証明書には次の 2 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を含む自己署名証明書です。ルート証明書に所属する秘密キーは、証明書サーバーシステムに保存され、未許可のアクセスから保護されます。認証局はルート証明書を使用してすべての証明書にデジタル署名します。

管理対象環境のすべての HTTPS 管理対象ノードは、証明書サーバーから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た対応する秘密キー、その環境で有効なルート証明書を受信します。この受信は、管理対象ノードで実行されてい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についての詳細は、HP Operations Agent 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し、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キーを保存する。
- 証明書リクエストを承諾または拒否する。
- 新しい証明書と対応する秘密キーを作成する、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。

- 信頼できる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

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において中心的な役割を担います。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ト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ト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。このルート証明書と対応する秘密キーは、認証局が動作できる一定のレベルで保護されたファイルシステムで作成され、保存されます。認証局は、初期化が正常に行われた後にルート証明書を使用して、承諾された証明書要求の署名を担当します。

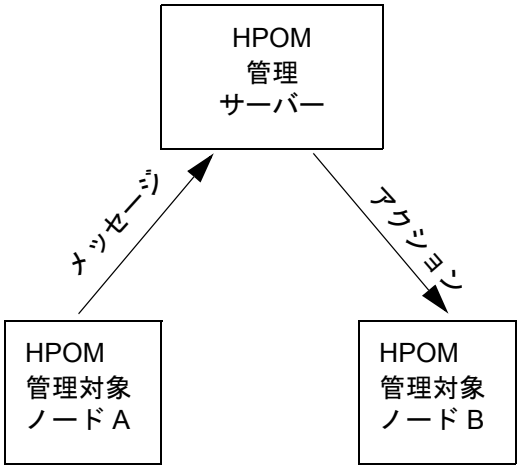
リモートアクション

リモートアクションは、管理対象ノード A によって送信された HPOM メッセージに添付され、管理対象ノード B で実行するように設定された自動アクションまたはオペレータ起動アクションです。このようなアクションの実行は、`remactconf.xml` ファイルを使用して制御できます。このファイルは次の場所にあります。

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

図 3-9 は、管理対象ノード A が HP Operations 管理サーバーにメッセージを送信し、管理対象ノード B でアクションを実行する方法を示しています。

図 3-9 リモートアクションの例



サービスプロバイダーの 1 つの HP Operations 管理サーバーで複数のカスタマの環境を管理できる必要がありますが、それと同時に、あるカスタマのセグメントにあるシステムが他のカスタマのセグメントでアクションを起動できないようにする必要があります。このため、HP Operations 管理サーバー上で、HP Operations 管理サーバーがアクションを実行できる対象のシステムを設定し、あるカスタマの管理対象ノードに設計されたリモートアクションが別のカスタマの管理対象ノードで実行されないようにすることができます。

リモートアクションの承認のための管理サーバーの設定およびリモートアクションの誤用を防止するセキュリティメカニズムについての詳細は、『HPOM 管理者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。以下で説明するあらかじめ設定された各

HPOM ロールには、デフォルトのアクセス権が設定されています。これらのアクセス権を変更する方法については、『HPOM 管理者リファレンスガイド』と HP Operations Agent 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 管理サーバーには、あらかじめ設定された HPOM ロールを割り当てることができます。管理サーバーとロールとの間のマッピングは、`sec.core.auth` 名前空間に定義され、MoM 環境では、担当マネージャのポリシーに定義されます。

HPOM 環境には、あらかじめ設定された次のロールが含まれます。

- **ローカルユーザーロール**

  `root` などの適切なシステム権限が付与されている場合、ローカルユーザーにはすべての権限があります。

- **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` と `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。担当マネージャポリシーで、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で、使用可能な設定サーバーの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、アクション実行権限以外の権限はありません。担当マネージャポリシーで、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、「ロールについて」(146 ページ) で説明されている HP Operations 管理サーバーロールにマップされます。

設定の自動配布の回避とリモートアクセスの拒否についての詳細は、『HPOM 管理者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の詳細は、『HPOM 管理者リファレンスガイド』および HP Operations Agent のドキュメントを参照してください。

承認のマッピング 次の表は、HPOM 管理サーバーの各ロールのデフォルトアクセス権を示しています。

表 3-1 承認のマッピング

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>		
コントロール (ctrl)	起動	1	可能	可能	不可
	停止	2	可能	可能	可能
	ステータス	4	可能	可能	不可
	通知	8	可能	可能	不可
	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	可能	可能	不可
	ポリシーの削除	2	可能	可能	不可
	ポリシーの有効化	4	可能	可能	不可
	ポリシーの無効化	8	可能	可能	不可
	ポリシーのリスト	16	可能	可能	可能
	ポリシーヘッダーの更新	32	可能	可能	不可
	設定の読み取り	64	可能	可能	可能
	設定の書き込み	128	可能	可能	不可
	ポリシーへの署名	256	可能	可能	不可
	デフォルト値 :	**511**	**511**	**511**	**80**

表 3-1 承認のマッピング (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	可能	可能	不可
	ファイルまたはディレクトリの削除	2	可能	可能	不可
	ファイルの取得	4	可能	可能	不可
	ファイルの実行	8	可能	可能	不可
	パッケージの配布	16	可能	可能	不可
	パッケージの削除	32	可能	可能	不可
	パッケージのアップロード	64	可能	可能	不可
	パッケージのダウンロード	128	可能	可能	不可
	インベントリの取得	256	可能	可能	可能
	インベントリの変更	512	可能	可能	不可
	ノード情報の取得	1024	可能	可能	可能
	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	可能	可能	可能
	デフォルト値 :	**1**	**1**	**1**	**1**

HTTPS ノードの管理

HP Operations 管理サーバーは HTTPS ノードで次の機能を実行できます。

- HTTPS エージェントのリモート制御
- リモートおよび手動による HTTPS エージェントのインストール
- リモートおよび手動によるパッチのインストールとエージェントのアップグレード
- リモートおよび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同時サポート
- 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による HTTPS ノードのサポート

次のセクションでは、HTTPS ノードに関するこれらの概念の一部について説明します。

- 「HTTPS ノードへの設定の配布」(150 ページ)
- 「HTTPS ノードのリモート制御」(154 ページ)

HTTPS ノードの管理についての詳細は、HP Operations Agent 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

以下の項では、HTTPS エージェントに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て、管理対象ノードに割り当てて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、複数のバージョンのポリシーを作成し、ツリー状構造で管理できます。ポリシーにはカテゴリの割り当ても含めることができます。**カテゴリ**を使用すると、関連するインストルメンテーションファイルを統合して、管理対象ノードに配布しやすくなります。

ポリシーとポリシータイプの詳細は、「HPOM のポリシー」(68 ページ) を参照してください。

ポリシーに関連する管理タスク、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の詳細は、『HPOM 管理者リファレンスガイド』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可能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ない限り、インストルメンテーションディレクトリは作成されず、ディレクトリアクション、コマンド、モニターが使用されます。

通常、アクション、コマンド、モニター、実行可能ファイルは HPOM ポリシーで参照されます。ポリシーでこれらの実行可能ファイルがフルパスで参照されていなければ、バイナリの新しい場所も HPOM 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のように、ユーティリティのパス変数に追加されるため、この変更は透過的になります。

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、それ以外の場所には権限 `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複数バージョンの配布と複数バージョンの管理についての詳細は、『HPOM 管理者リファレンスガイド』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、権限のない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 管理サーバーに手動でインストールするための準備には、`opctmpldwn` ツールを使用します。出力データは、管理対象ノード専用の管理サーバーシステムのディレクトリに保存されます。

opctmpldwn は、次のように HTTPS ノードを処理します。

- nodeinfo データと mgrconf データはポリシーと見なされるため、上述のディレクトリに保存されます。
- ポリシーは、ノード固有のキーを使用して暗号化されます。

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ーです。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 設定を HTTPS ノードで使用される 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

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

を使用して、配布する必要のある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 が受け入れる要求は、他の HP Operations 管理サーバーコンポーネントからの deploy configuration types xyz to node abc 形式の要求だけです。これらの要求は、設定 API または opcragt -update と opcragt -distrib によって発行できます。

opcbbcdist には、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、手動で再試行を起動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あり、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 つの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、opcbbcdist が HP Operations サーバーのシャットダウンによって停止し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。よりセキュアな HP Operations 管理サーバーが管理対象ノードを起動します。

デメリットは、新しい設定が配布されているときに、システムにアクセスできない場合、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。

- 保留中の各ノードで 1 時間に 1 回以上
- サーバーが再起動されたとき
- opcragt -update、opcragt -distrib によって、またはコマンドに関連付けられた API を直接呼び出して設定のプッシュが明示的に起動されたとき

保留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、配布が保留中になっ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または追加されたデータのみが配布されます。これにより、転送されるデータの量が最小限に抑えられ、インターセプタなどのサブエージェントへの再設定要求の数を減らすことができます。必要に応じて、完全な設定を管理対象ノードに再配布できます。

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、`opcbbcdist` は、ノードに必要なポリシーの削除とインストールタスクを計算して実行します。インストルメンテーション配布では、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。`opcragt -purge` コマンドラインコマンドとオプションが適用されている場合をのぞき、インストルメンテーションデータは管理対象ノードから削除されません。

HTTPS ノードのリモート制御

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。操作には、開始、停止、ステータスの取得、一次マネージャの切り替え、構成変数の取得と設定、設定の配布が含まれます。HTTPS ノードには、`opcagt` という名前の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。次の形式のエイリアスを指定できます。

<alias> <maps_to>

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 管理対象ノードの `-id 1` を `-id EA` に変換するには、以下のコマンドを入力します。

opcragt -status -id 1 <node_list>

定期ポーリング

1 つ以上の管理対象ノードに対する HPOM 定期ポーリングを有効または無効にするには、opchbp ツールを使用します。エージェントがアライブパケットを送信する必要がある場合も、このツールを使用して定期ポーリングのタイプを設定して定義します。

すべての管理対象ノードの定期ポーリングステータスを確認するには、以下のコマンドを実行します。

```
/opt/OV/bin/OpC/opchbp -status
```

定期ポーリングは、外部ノードを除き、HPOM 登録ノードのすべての管理対象ノードで実行できます。HP Operations 管理サーバーは HP Operations Agent がインストールされているこれらの管理対象ノードに対して、定期ポーリングを実行します。

管理対象ノードシステムがシャットダウンしている場合、HPOM が完全に停止している場合 (コントロールエージェントを含む)、または管理対象ノードで HPOM ソフトウェアを手動でアップグレードしている場合は、定期ポーリングを無効にすると便利です。

定期ポーリングを有効にすると、HPOM はコントロールエージェントが応答しない (つまり、到達できない) というメッセージを生成し、次の警告メッセージは自動的に除外されます。コントロールエージェントを再度実行すると、メッセージは HPOM によって自動的に受諾されます。

opchbp ツールおよびオプションについての詳細は、opchbp のマニュアルページを参照してください。

証明書の作成と配布

暗号化対応の Secure Socket Layer (SSL) プロトコルを使用した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、証明書を使用して識別されます。2 つの管理対象ノードの間の「SSL ハンドシェーク」は、着信側の管理対象ノードによって提示された証明書を発行した認証局が、受信側の管理対象ノードの信頼できる認証局である場合のみ成功します。

証明書は自動的に、または手動でインストールできます。証明書のインストールは、HPOM メッセージでモニターされます。証明書要求が自動的に承諾されると、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。証明書要求が自動的に承諾されない場合は、要求が拒否された理由と、問題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。

証明書は `ovcm` および `opccsa` コマンドラインユーティリティで管理されます。証明書要求を承諾、拒否、リスト表示、削除したり、証明書要求と登録ノード内の対応するノードをマッピングしたりできます。

証明書の使用方法についての詳細は、『HPOM 管理者リファレンスガイド』ガイドおよび HP Operations Agent 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 などの最新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体として表現されます。これらのリソースはリソースグループを形成し、このリソースグループが、クラスタ環境で動作するアプリケーションを表します。この複合体の中で、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のモデリングには、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語が使用されます。

高可用性に関連する一般的な用語

HA (高可用性)

高可用性とは、リソースを冗長化して業務上重要なシステムをダウンタイムから保護する環境を表す一般的な用語です。高可用性を実現するためにクラスタシステムが使用されることがよくあります。

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。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 パッケージに所属するホスト名と IP アドレスが割り当てられます。HPOM 仮想ノードには、`HARG` 名属性があります。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、機能は `ovconfd` プロセスにあります。

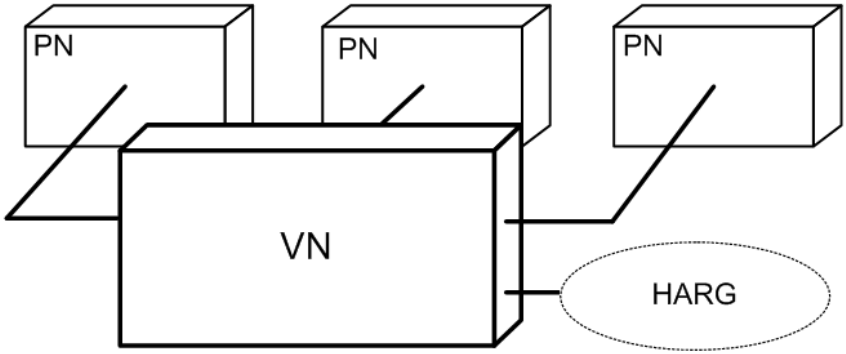
HARG 名 (高可用性リソースグループ名)

HARG 名とは、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 の HARG 名は、クラスタ内の HA リソースグループの名前と一致する必要があります。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 3-10 仮想ノード

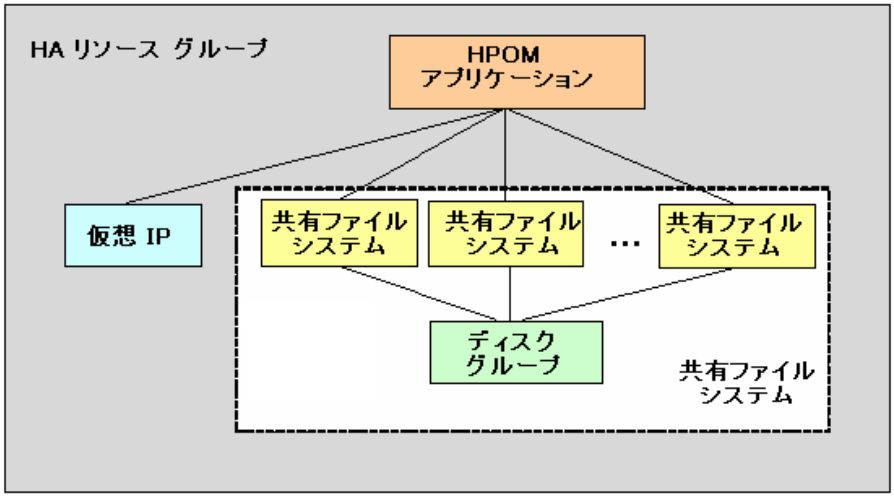


HA リソースグループ名による管理ノードのリンクには次のようなメリットがあります。

- 仮想ノードに割り当てられたポリシーなどによって HA リソースグループの範囲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を適切に関連付け、クラスタを正確に管理できます。

図 3-11 **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 CIAw 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の詳細は、『HPOM 管理者リファレンスガイド』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された範囲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次の 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
- Web プロキシなど、アプリケーションレベルで機能するプロキシサーバー

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使用には、セキュリティ上の大きなメリットがあります。以下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、特定のタイプのファイル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。

プロキシの使用には、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、以前に比べ高性能コンピュータの価格が低下しているため、これが実用上の問題になることはありません。
- 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。

イントラネット内のクライアントがインターネットへ要求を送信しようとすると、実際にはプロキシがその要求を受信します。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。要求が、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要求を目的のアドレスに転送します。応答を受信すると、プロセスが反転します。着信する要求が安全と見なされる限り、要求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要求の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、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次の 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。

- **デュアルホームまたは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要求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の詳細は、『HPOM 管理者リファレンスガイド』を参照してください。

HPOM のトレース

本項では、次のHPOM のトレースの概念について説明します。

HPOM のトレース

HPOM では、問題の原因を調査する上で役立つ、問題のトレース機能が提供されています。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問題が発生した時間と場所を特定する上で役立ちます。

HPOM では次のトレースメカニズムを使用できます。

- 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役に立ちます。

  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についての詳細は、「HP スタイルのトレースの概要」(165 ページ) 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 エージェントと HP Operations 管理サーバーの問題解決にも使用できます。設定は `ovconfchg` コマンドを使用して行います。詳細は『HPOM 管理者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の概要

HP トレース機能では、アプリケーション、コンポーネント、カテゴリ、属性という要素の階層を実装しています。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	n.a.	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	n.a.	Info、Warn、Error、Developer、Verbose

HP 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 のトレース GUI を使用して、リモートトレースを設定する。詳細は HP Operations Agent 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を使用して、手動トレースを設定する。詳細は『HPOM 管理者リファレンスガイド』を参照してください。

HPOM トレースが有効化されたアプリケーション

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 つのグループに分かれています。

- サーバープロセス
- エージェントプロセス
- XPL トレースが実装された下位のレベルの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事前設定の手順はありません。トレース機能は、XPL トレースを HPOM コードベースに追加するか、コア機能を基盤コンポーネントから導入して、対応するライブラリとリンクすることで実現できます。XPL トレースが HPOM コードベースに追加された場合、既存のトレースは XPL トレースに変換されています。基盤コンポーネントから機能を追加した場合、これらの基盤コンポーネントに組み込まれている XPL トレースが HPOM に取り込まれます。

表 3-3 HPOM トレースが管理サーバーと管理対象ノードで有効化されたアプリケーション

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 トレースが管理サーバーで有効化されたアプリケーション

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 トレースが管理対象ノードで有効化されたアプリケーション

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

以下の項では、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 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 3-6 は、サーバープロセスとエージェントプロセスに定義されたトレースコンポーネントを示しています。

表 3-6 HPOM サーバーコンポーネントとエージェントコンポーネント

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 3-7 は、製品に組み込まれている共有コンポーネント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	
制御コンポーネント	
ctrl.action	ctrl.ovc
ctrl.autoshutdown	ctrl.process
ctrl.component	ctrl.rpcclient

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	
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ー	
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	
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

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	
xpl.log	xpl.thread.mutex
xpl.msg	
組み込み Performance Agent	
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 トレース領域は、HP BTO Software カテゴリによって指定されます。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` コンポーネントと `opc` コンポーネントに定義されるトレースカテゴリを示しています。

表 3-8 HPOM opc と 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 固有のトレースカテゴリ	
actn	アクション
agtid	AgentID を使用した IP の非依存性
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	メモリ割り当ての問題
memory	残りのメモリ割り当て
misc	その他
mon	モニター
msg	メッセージフロー

表 3-8 HPOM opc と 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 (文字セットの変換など)
ntprf	NT パフォーマンスのトレース
pdh	パフォーマンスデータヘルパー
perf	パフォーマンス
pstate	ポリシーとソースの状態変化
sec	セキュリティ
srvc	サービス
wmi	LE テンプレートから WMI テンプレートへの変換
一般的な XPL トレースカテゴリ	
Trace	一般トレース
Proc	プロシージャトレース
Operation	オペレーショントレース
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、企業のネットワーク化されたシステムを外部の攻撃から保護するために使用します。ファイアウォールは通常、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。

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 HTTP プロキシを使用した接続

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接続するとします。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。同様に、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 プロキシを使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接続するとします。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超える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通信ブローカポートです。

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接続

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接続するとします。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可能性があります。HTTP プロキシはファイアウォールの外側にあるため、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 プロキシには異なる設定が必要です。

インターネット上の HP 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 HTTP プロキシを使用しない接続

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、HTTP プロキシを使用せずに、プライベートイントラネット上のアプリケーションに接続するとします。ファイアウォールは、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超える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通信ブローカポートです。ターゲットサーバーが通信ブローカに登録されている場合、ターゲットポートの番号は常に通信ブローカ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単になり、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。ファイアウォールによる HPOM の設定についての詳細は、HPOM のファイアウォール設定を参照してください。

HTTPS ベース通信の設定

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。通信ブローカ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

通信に使用されるパラメータは bbc.ini(4) ファイルに記述されます。このファイルについては HP Operations Agent のドキュメントで説明されています。

通信ブローカは、名前空間 bbc.cb を使用します。すべての管理対象ノードの通信ブローカ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、通信ブローカごとに異なるポート番号を割り当てられます。この設定は、名前空間 bbc.cb に定義されている SERVER_PORT パラメータより優先されます。

注記

名前空間とは、次のような一意の 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、ネットワーク内の通信ブローカ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=<host>:<port> または NAME=<domain>:<port>

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、*.domainname 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、この名前は該当の名前空間内で一意である必要があります。以下はエントリの例です。

- 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` で実行される通信ブローカのポート番号は `1383` になります。

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設定

本章の内容

本章では、メッセージポリシーを設定し、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。

目的

本章では HPOM 管理者向けに、次の各トピックを説明します。

- ❏ 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ー処理
- ❏ メッセージの最適なフィルター処理のための方針
- ❏ メッセージの記録
- ❏ 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 内部エラーメッセージのフィルター処理
- ❏ HPOM 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
- ❏ メッセージ選択条件に基づくカスタムメッセージ属性の設定

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が削減されます。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。メッセージソースに関する情報の追加と変更は、管理サーバーで行います。いったん追加や変更を行った後、その情報を必要とする管理対象ノードのみに配布します。

アクションの一元化

管理サーバーでは、すべてのシステムの自動アクションとオペレータ起動アクションを開始できます。したがって、リモートサイトでのオペレータの操作量は最小限になり、完全に不要になる場合さえあります。

障害の早期検出

オペレータは、環境内のノードのアクティビティを HPOM を使って監視することにより、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。

生産性の向上

単純な反復タスクを HPOM に任せ、指示を通じてオペレータによる複雑な作業の実行を支援し、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って、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。

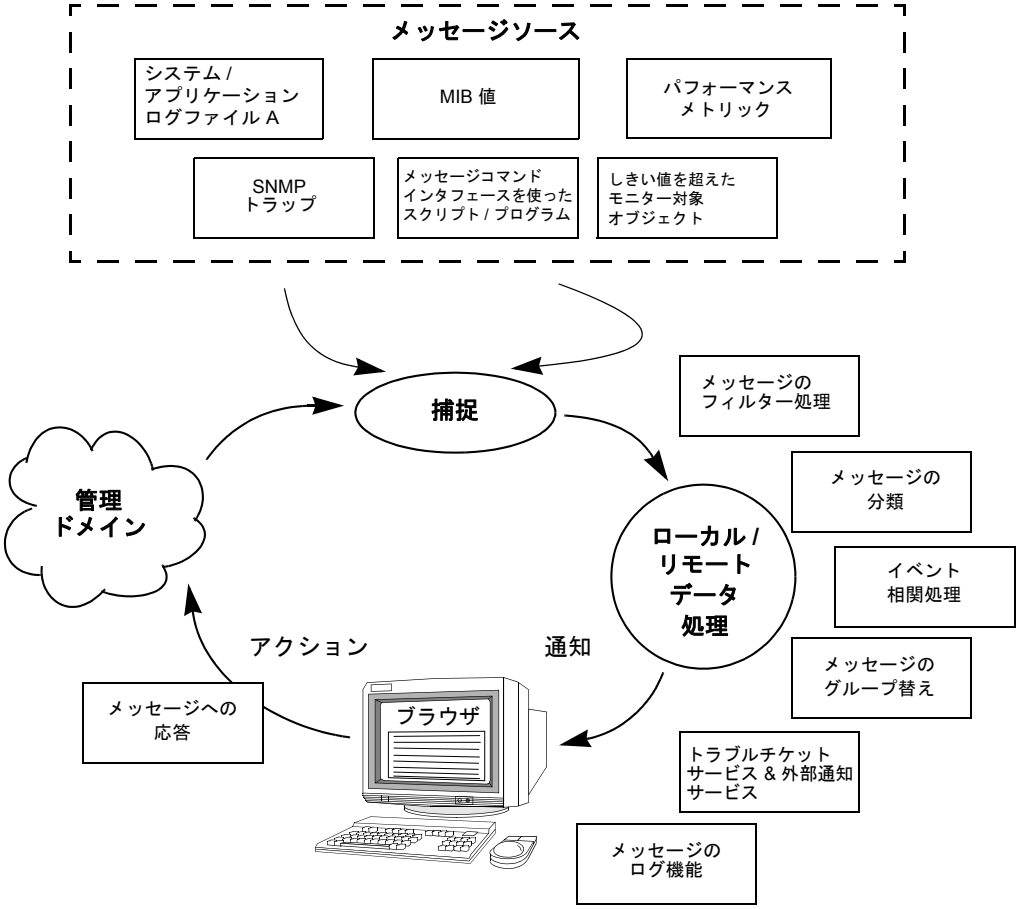
ポリシーの配布

ポリシーを使えば、環境内のあらゆるソースから同じ種類の情報を収集できます。情報の収集元となる管理対象ノードにポリシーを配布します。

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　関連するメッセージのブラウザでの統合



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によって、収集やモニターの対象となるメッセージと値を指定します。さらに、スケジュールをもとに定期的に実行するアクション、メッセージの除外または取り込みの基準となるフィルター (条件)、および捕捉後のログ出力のオプションも、メッセージソースポリシーで指定します。

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種類**

メッセージを収集するソースを定義し、すべてのメッセージにデフォルトの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`)
- イベント相関処理コンポーザー (`EC`)
- スケジュールアクション (`Schedule`)

❑ **メッセージ条件**

一連の属性に一致するメッセージを絞り込んで HPOM に取り込みます。メッセージ条件では、受信したメッセージへの応答も定義します。

❑ **除外条件**

一連の属性に完全に一致するメッセージを HPOM から除外します。

❑ **オプション**

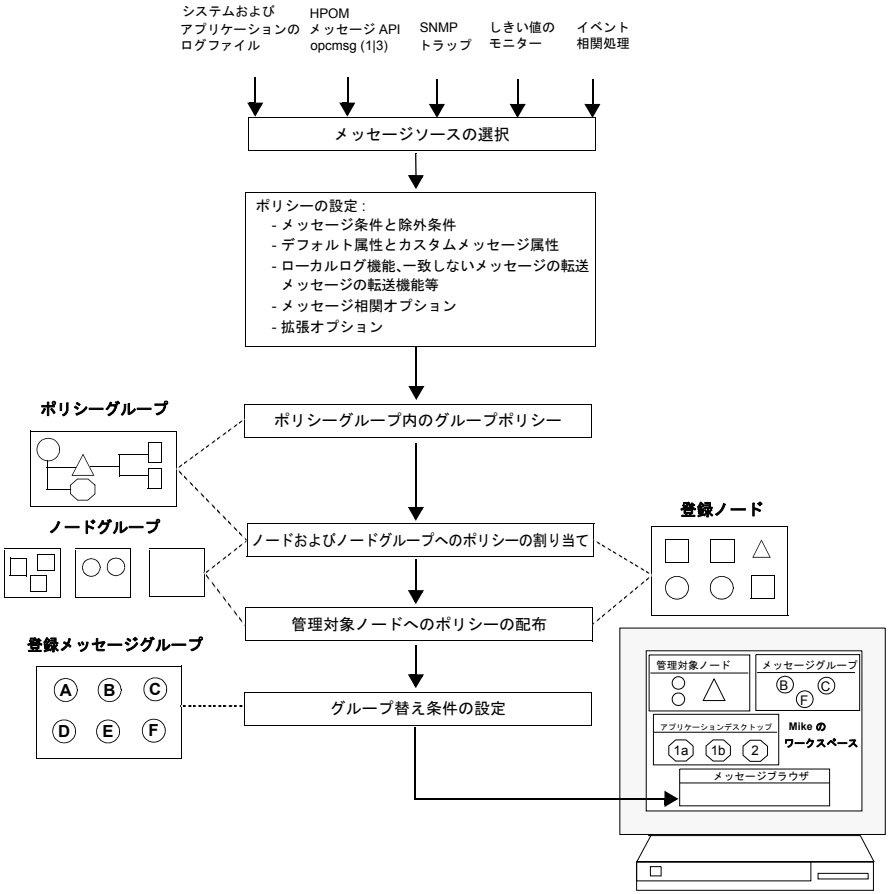
メッセージのデフォルトのログ処理を指定し、不一致メッセージの転送オプションを設定します。

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えば、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。メッセージソースポリシーでは、メッセージを Java GUI メッセージブラウザに転送するかどうか、メッセージをどの属性と一緒に表示するか、および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。それぞれのポリシーごとに条件を設定し、詳細なオプションを指定します。

メッセージソースポリシーの設定についての詳細は、『HPOM 管理者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の条件を定義しないで、ポリシー本体に `FORWARDUNMATCHED` キーワードが含まれていると、HPOM はそのメッセージソースから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することができます。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について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、定義済みポリシーを変更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

ポリシーグループとは、複数のポリシーや、他の複数のポリシーグループの集まりです。管理者は、ポリシーをグループ化することによって、設定作業や管理作業を効率化できます。

たとえば、次の特徴を持つポリシーをグループ化できます。

- ❏ 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利点

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。

- **ポリシー全体の把握**

  ポリシーグループを使えば、さまざまなポリシーを意味のある単位に分けることができます。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は 1 つのグループにまとめられます。このグループ化によって、ポリシーリストに表示されるポリシーの数が減り、利用可能なポリシーの全容を把握しやすくなります。

- **明確な階層化**

  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。ポリシーグループを階層化すると、ポリシーの構成が整理され、オペレータが同じ種類のポリシーを編集する作業も効率化されます。

- **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、すべての必要なグループを割り当てることができます。その結果、必要なポリシーがすべて確実に選択されます。

ポリシーグループの一覧表示

ポリシーグループは、`opcpolicy -list_groups` コマンドを使用して一覧表示できます。ポリシーグループを使用する操作には、ポリシーグループの作成 / 削除、ポリシーのグループへの割り当て、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一覧表示などがあります。詳細レベルを上げたり、`level` パラメータに別の値を指定することにより、より多くの情報を表示できます。詳細は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、ポリシーグループにポリシーを割り当てたり、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したがって、組織のニーズを正確に反映したポリシーグループを、柔軟に形成することが可能です。HPOM では、同じポリシーが同じ管理対象ノードに繰り返し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。サポートされている各エージェントプラットフォーム向けに HPOM が用意しているデフォルトのポリシーグループの一覧については、HP Operations Agent のドキュメントを参照してください。

あるグループが別のグループのメンバーである場合、こ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こと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

メッセージを別のメッセージグループに再編成するために、グループ替え条件を設定できます。また、HPOM Event Correlation Services (ECS) をインストールしている環境では、イベント相関処理ポリシーを設定することによって、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、コマンドラインツール `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、コマンドラインツール opcnode を使用して管理対象ノードとノードグループに割り当てることができます。ポリシーグループをノードに割り当てる手順は、ポリシーを単独で割り当てる手順と同じです。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。これにより、新しい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、ポリシーグループをノードグループに割り当てる場合は、次のコマンドを使用して行うことができます。

```
opcnode -assign_pol_group pol_group=<policy_group_name>
group_name=<node_group_name>
```

<policy_group_name> には割り当てるポリシーグループの名前、<node_group_name> には割り当て先のノードグループの名前をそれぞれ指定します。

詳細はopcnode (1M) マニュアルページを参照してください。

注記

HPOM は、ポリシーの割り当てと配布を個別に行います。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 はそのポリシーだけを再配布します。1 つのポリシーが複数のポリシーグループに属し、同じ管理対象ノードに複数回割り当てられている場合も、そのポリシーが当該ノードに配布されて処理されるのは一度だけです。変更中のポリシーはロックされ、配布されません。ポリシーのステータスと管理対象ノードへの割り当て状況は、レポートを生成して確認できます。利用可能なレポートについての詳細は、『HPOM 管理者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、「HPOM の設定の更新」(105 ページ) を参照してください。

注記

ポリシーを削除したり、特定のノードに対するポリシーの割り当てを削除した場合には、その影響を受ける各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。配布しないと変更は反映されません。

コマンドラインツール `opcpolicy` を使えば、管理対象ノード上の任意のポリシーを一時的に無効化することができます。詳細はopcpolicy (1M) 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確認です。

確認するメッセージソース

次の各メッセージソースを評価します。

- ❏ アプリケーションとシステムのログファイル
- ❏ 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
- ❏ モニター対象の 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

次の基準でメッセージを評価します。

- ❏ イベントがエンドユーザーに及ぼす影響
- ❏ 重要度のレベル
- ❏ 発生頻度
- ❏ 判読性の観点からみたファイル形式 (バイナリファイルまたはプレーンテキスト形式)
- ❏ 言語と文字セット
- ❏ ネットワークの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。このようなメッセージの他に、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すメッセージがあります。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。ほとんどのメッセージには、その一部として重要度が含まれています。この重要度が、実際の環境における当該メッセージの重要度を正しく反映しているかどうかを調べます。オブジェクトが危険域の重要度のメッセージを生成した場合でも、そのメッセージで表される実際の状況が、常に危険域に該当するとは限りません。

メッセージカタログの利用

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には、発生可能な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

メッセージとは、運用環境内の**オブジェクト**のステータスに関する情報をまとめたものです。オブジェクトには、オペレーティングシステムやアプリケーション、あるいは周辺機器など、運用環境を構成するあらゆる要素が該当します。

メッセージステータスの作成

メッセージは、イベントや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属性は、管理者が指定できます。

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、Java GUI オペレータの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。収集間隔を定義するときは、短くしすぎないようにしてください。収集間隔が短すぎると、システムに不要な負荷を与える可能性があります。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使ってもかまいません。

メッセージの捕捉

HPOM は次のソースからメッセージを捕捉します。

- **ログファイル**

  アプリケーションとシステムのログファイル

- **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、`opcmsg(3)` アプリケーションプログラミングインタフェース (API) または `opcmsg(1)` コマンドラインインタフェースを通じてメッセージを送信します。`opcmsg(3)` や `opcmsg(1)` でメッセージを送信する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

    アプリケーションやシステムの多くの値は、期待値と比較できます。

  - 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使って、特定の値 (表のサイズやロックの件数など) をモニターします。これらの値は期待値と比較します。

  - プロセス

    スクリプトを使って、重要なプロセス (デーモンなど) が動作しているかどうかを調べます。プロセスの値や動作中のプロセス数などをチェックします。

  - ファイルとファイルシステム

    重要なファイルやファイルシステムが存在するかどうかをチェックし、それらのサイズを確認します。スクリプトは、ディスクの使用状況 (使用中のディスク容量や、あらかじめ定義された上限までの空き容量) を返します。

  - パフォーマンスメトリック

    このコンポーネントが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

    管理情報ベース (MIB) の動的な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、現在の値を設定済みのしきい値と比較します。

- **スケジュールアクションのメッセージ**

  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ル設定して実行します。HPOM は、スケジュール設定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設定については、『HPOM 管理者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ー処理する**条件**を設定できます。

195 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. メッセージソースのテンプレートの適用

メッセージソースのテンプレート:	Logfile Su (11.x HP-UX)
メッセージのデフォルト: 属性:	重要度: 正常域
	ノード:
	アプリケーション: /usr/bin/su(1) Switch User
	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. メッセージ一致条件の適用

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> から <to> へのユーザー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するメッセージ

```
正常域...12/10/09 16:21:55 system_1.bb /usr/bin/su セキュリティ peter からroot へのユーザー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 からroot へのユーザー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設定

メッセージソースポリシーは、次のデフォルト設定をメッセージに割り当てます。

- **メッセージ属性**

  メッセージ属性とはメッセージの特徴を表す情報であり、HPOM 管理者はこの情報を使って、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、重要度、メッセージの生成元ノード、イベントに関連するアプリケーションやオブジェクト、メッセージが属する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、これらのデフォルト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とは 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ー処理を実行できます。

  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、`opccmachg` コマンドラインツールを使用します。使用方法についての詳細は、opccmachg(1m) 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`)、スケジュール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についての詳細は、HP Operations Agent のドキュメント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れば、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) の選択、さらに 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れば、Java GUI メッセージブラウザに同じメッセージが繰り返し表示される事態を回避できます。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。

重複するメッセージの除外では、以下の内容を指定できます。

- 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、付録 A「ポリシー本体の構文」(355 ページ) 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によって適用されるフィールドセパレータと、大文字小文字チェックの有無を指定できます。大文字小文字を区別するチェックを定義するには、キーワード `ICASE`、フィールドセパレータを定義するには、キーワード `SEPARATORS` を使用します。詳細については、付録 A「ポリシー本体の構文」(355 ページ) 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への出力オプション

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 メッセージを転送する方法を選択できます。

デフォルト値を定義する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 に転送し、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。ポリシー本体の構文の詳細については、付録 A「ポリシー本体の構文」(355 ページ) を参照してください。

複数のポリシーの設定

HPOM では、管理者が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。管理対象ノードでイベントが発生すると、そのノードに割り当てられたすべてのポリシーを使って、同時にフィルター処理が行われます。条件が適用されると、メッセージはそのポリシーに指定されたオプションに従って処理されます。したがって、HPOM がメッセージをフィルター処理する方法を理解しておくと、ブラウザが不要なメッセージで一杯になったり、重要なメッセージを失うことを回避できます。

複数のポリシーの並行処理

HPOM は、1 つのノードに割り当てられた同じ種類の複数のポリシーを並行して処理することができます。この処理では、どのポリシーにも優先順位は設定されていません。各ポリシーは独立に処理されます。除外条件に一致するメッセージや不一致除外条件に該当するメッセージは、そのポリシー内での処理に対してのみ除外されます。ただし、メッセージは別のポリシー内のメッセージ条件に一致し、担当オペレータに HPOM メッセージが作成されることがあります。複数ポリシー設定でパフォーマンスを向上させるための詳細については、「パフォーマンスの最適化」(225 ページ) を参照してください。

200 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ー処理**

  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ー処理されます。

- **デフォルト設定の適用**

  ポリシーによってメッセージにデフォルト設定が適用されます。

- **メッセージ条件のチェック**

  メッセージが条件リストと比較されます。最初に該当した条件によって、その後の処理が決定されます。

- **メッセージの転送**

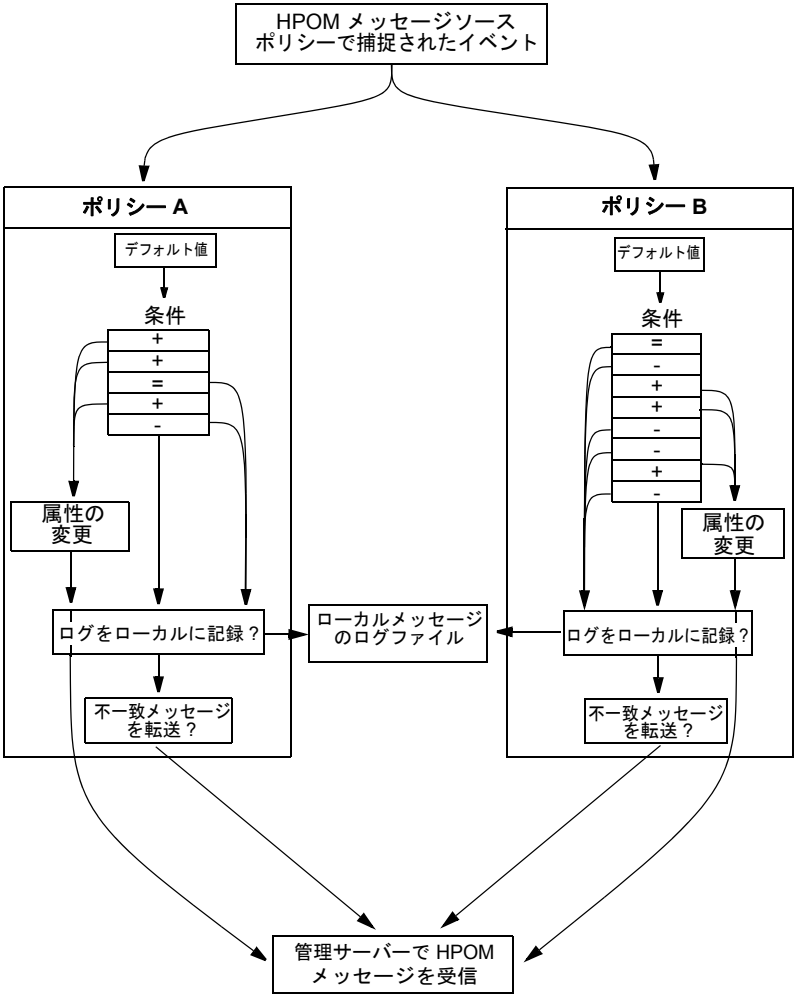
  メッセージがどの条件にも一致せず、ポリシーで [一致しないメッセージを転送] 属性が設定されている場合、そのメッセージ (ポリシーのデフォルト値が含まれる) は転送されます。

- **メッセージのログ機能**

  不一致メッセージに対して、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れば、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 複数のポリシーによるメッセージのフィルター処理



一致しないメッセージの転送

複数のポリシーで FORWARDUNMATCHED キーワードを使用すると、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、複数のメッセージの処理方法が異なります。

- **アプリケーション固有のポリシー**

  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。

次に挙げる種類のポリシーでは、1 つのイベントから複数のメッセージが生成されることはありません。

- ログファイルエントリポリシー
- 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、一致しない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に一致する場合は、別のポリシーで [一致しないメッセージを転送] が設定されていても、メッセージは除外されます。一致しないものを除外する条件では、そのポリシーのメッセージだけが除外されますが、他のポリシーの条件に一致しない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 ポリシーと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。

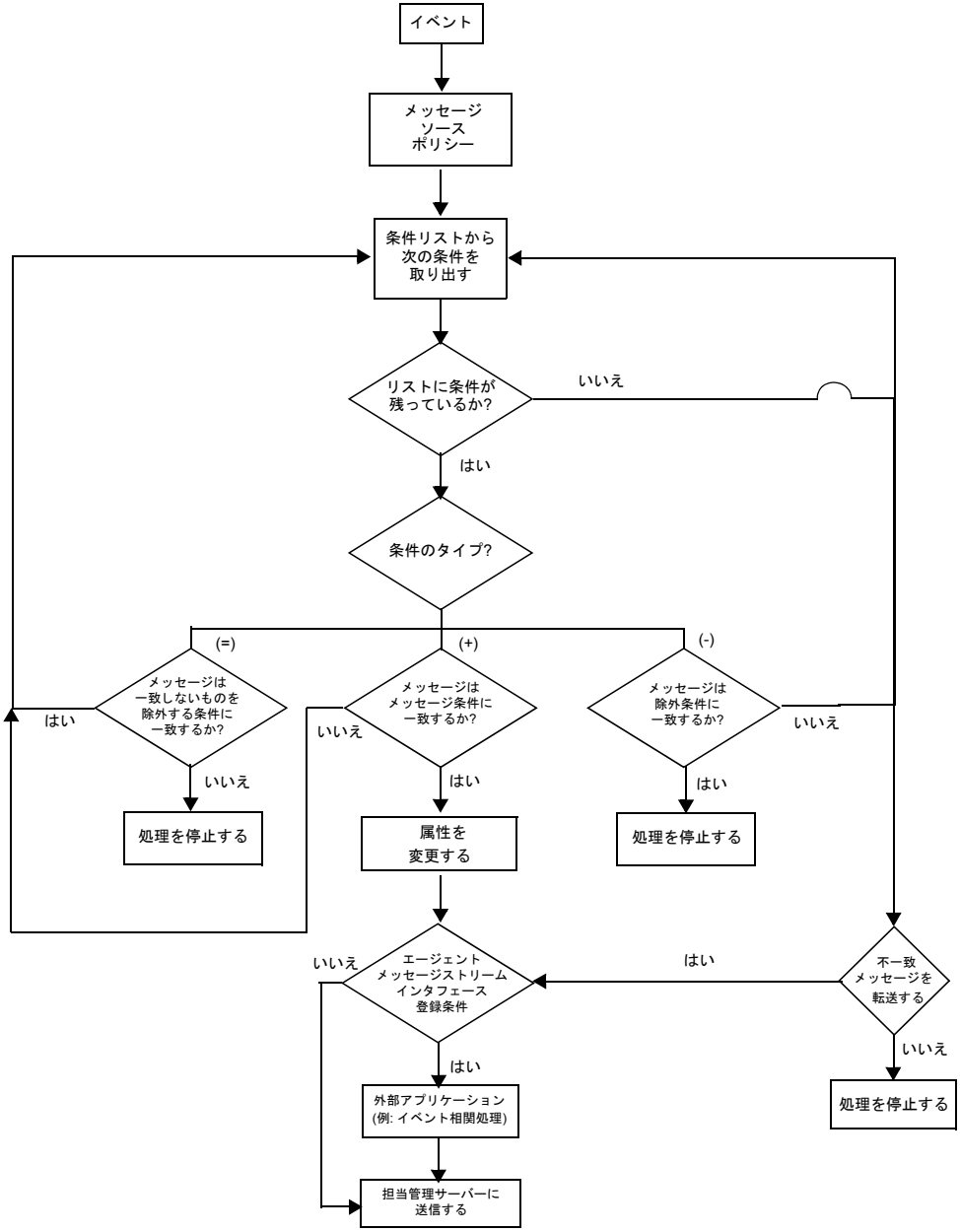
条件によるメッセージのフィルター処理

メッセージ処理メカニズムは、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ー処理

図 4-5 は、エージェント上でメッセージが条件と照らし合わせて処理される過程と、条件に一致するメッセージと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ー処理」と呼ばれます。

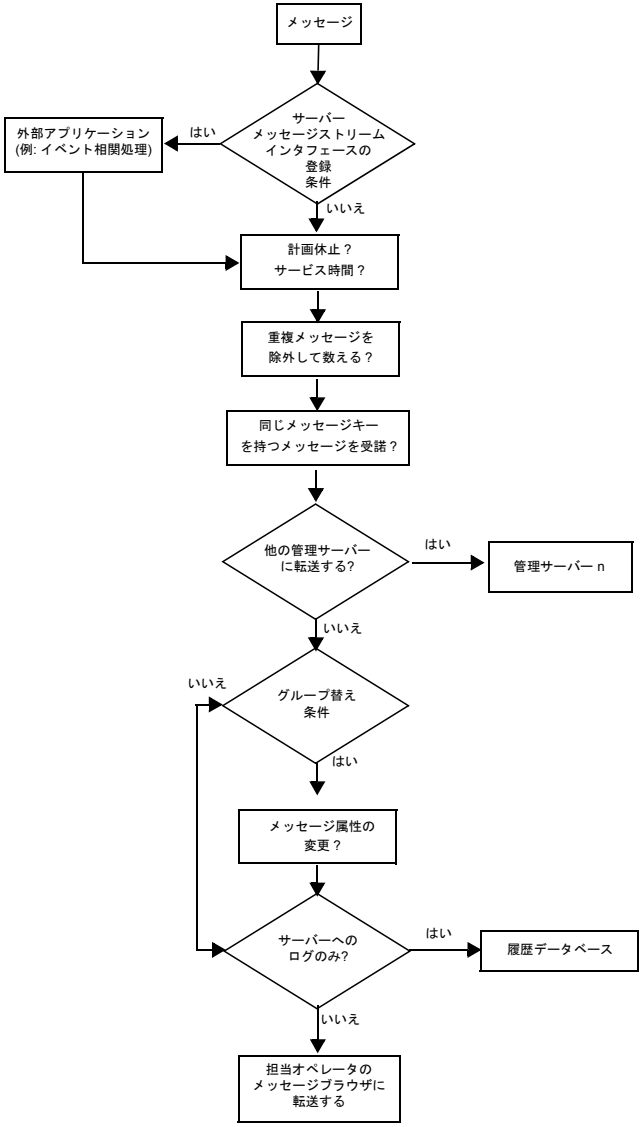
図 4-5　HPOM エージェントによるメッセージのフィルター処理の過程



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　HPOM 管理サーバーによるメッセージのフィルター処理の過程



メ ッ セージ条件の設定

メッセージ条件を設定する際は、付録 A「ポリシー本体の構文」(355 ページ) に記載されるポリシー本体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. **一致条件の定義**

   メッセージ条件または除外条件と呼ばれる照合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をテストし、正しく機能することを確認します。

3. **メッセージ相関オプションの設定**

   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メッセージ相関オプションを設定し、同じメッセージが Java GUI メッセージブラウザに何度も繰り返して表示されないようにします。

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に一致するたびに、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**

   メッセージが条件に一致するたびに 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**

   外部通知サービスやトラブルチケットサービスへ出力されるように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。これらの属性の値は、メッセージソースで生成され、パターンマッチの対象になった文字列と必ずしも一致させる必要はありません。

8. **カスタムメッセージ属性の定義**

   より適切なメッセージ情報をオペレータに提供するため、Java GUI メッセージブラウザに表示するメッセージのカスタム属性を定義します。

9. **指示の記述**

   Java GUI メッセージブラウザに表示するメッセージに添付する説明を作成します。

メッセージ条件の設定の詳細については、付録 A「ポリシー本体の構文」(355 ページ) および『HPOM 管理者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いっさい設定しない場合、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、イベントに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、または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、ポリシー本体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 HPOM 内にフィルタリングする場合でも、あるいは HPOM 内から除外する場合でも、メッセージ条件、除外条件、および不一致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

次の条件を、管理対象ノード上のイベントに適用できます。

- **メッセージ条件**

  メッセージ条件として設定されたすべての属性に該当するメッセージを 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。

- **除外条件**

  除外条件のすべての属性に一致するメッセージを HPOM から除外します。除外されたメッセージは、それ以上処理されません。

  除外条件は、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。

❏ **不一致除外条件**

不一致除外条件の属性に一致しないメッセージを HPOM から除外します。除外されたメッセージは、それ以上処理されません。

不一致除外条件のすべての属性に一致するメッセージは、条件リストの残りの条件で処理されます。

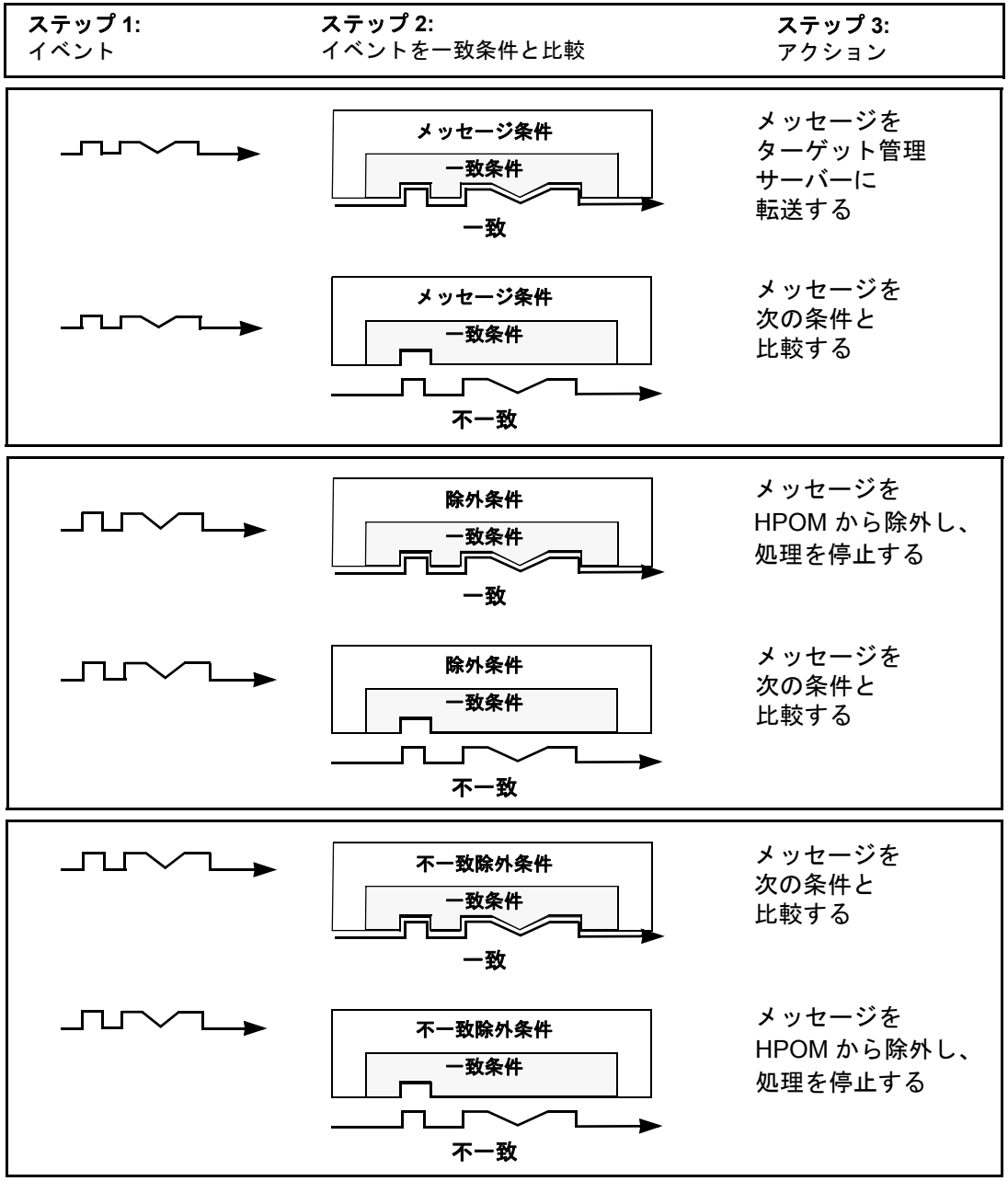
不一致除外条件は、ポリシーに該当しないすべてのメッセージを条件レベルで除外し、ポリシーの条件リストで処理されるメッセージの数を減らすことによって、HPOM のパフォーマンスを向上させます。

`FORWARDUNMATCHED` キーワードがポリシー本体で使用されている場合、サーバーに転送される不一致メッセージのセットは、ポリシーに直接関連するメッセージだけに限定されます。

着信メッセージと一致条件との比較

208 ページの図 4-7 は、着信メッセージが指定した一致条件、除外条件、および不一致除外条件と、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の詳細については、「条件によるメッセージのフィルター処理」(202 ページ) 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ー処理



注記

SUPP_UNM_CONDITIONS キーワードと FORWARDUNMATCHED キーワードはどちらも不一致メッセージの処理に関連していますが、前者は条件レベル、後者はポリシーレベルでそれぞれメッセージをフィルター処理します。

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して抽出し、変数に割り当てます。その変数をパラメータとして使用し、新しいメッセージテキストを作成または他の属性を設定します。これらのパラメータは、自動アクションコマンドとオペレータ起動アクションコマンドにも使用できます。HPOM と SNMP 変数のリストについては、『HPOM 管理者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、パターンマッチで実行するのは、メッセージ内の特定文字列の検索だけです。ただし、さまざまな演算子を利用して、検索の精度を高めることもできます。たとえば、ポリシー本体の MSGCONDITIONS ブロックに、TEXT キーワードと一緒に ERROR と入力すると、メッセージテキスト内のいずれかの位置に文字列「ERROR」を含むメッセージのみが条件に一致します。

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。演算子使用する場合は、演算子を山かっこ(< >) で囲み、角かっこ([ ]) でサブパターンを区切ります。

除外条件に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、一致する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、203 ページの図 4-5 を参照してください。

大文字と小文字を区別しないパターンマッチ

ポリシー本体で ICASE キーワードを使用した場合、大文字と小文字のあらゆる組み合わせの「warning」と一致させることができます。ポリシー本体の構文についての詳細は、付録 A「ポリシー本体の構文」(355 ページ) を参照してください。

パターンマッチ条件の例

HPOM のパターンマッチ言語で使用できるさまざまな条件の例を以下に示します。

- Error

  メッセージテキスト内のどこかにキーワード Error を含むあらゆるメッセージを識別します。この条件は、デフォルトでは大文字と小文字が区別されます。

- panic

  大文字と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どこかに panic、Panic、または PANIC を含むすべてのメッセージに一致します。

- logon|logoff

  OR 演算子 (|) の使用例。キーワード logon または logoff を含むあらゆるメッセージが識別されます。

- ^getty:<*.msg> errno<*><#.errnum>$

  次のようなメッセージに一致します。

  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」が、**msg** 変数に割り当てられます。数字の 6 は **errnum** 変数に割り当てられます。位置指定記号 ($) は、数字 6 が行末にある場合のみ一致することを指定しています。

- ^errno[|=]<#.errnum> <*.errtext>

  次のようなメッセージに一致します。

  errno 6 - no such device or address

  errno=12 not enough core.

OR 演算子の直前にスペースがあることに注意してください。角かっこの中の式は、このスペースまたは等号 (=) と一致します。<#.**errnum**> と <*.**errtext**> の間のスペースは区切り記号です。このスペースは、ここで示された変数への割り当てに厳密には必要ありませんが、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。パターンの真ん中にあるコロン (:) は、**uid** へ渡す文字列を先行する文字列から区切ります。パターン末尾のコロンは、**uid** へ渡す文字列を、入力パターン内で後続するグループ ID から区切ります。このコロンは、パフォーマンスを向上させるためだけでなく、文字列の論理的な区切りとして必要です。

- ^Warning:<*.text>on node<@.node>$

  「Warning: too many users on node hpbbx」などのメッセージを識別します。too many users を変数 **text** へ割り当て、hpbbx を変数 **node** へ割り当てます。

パターンマッチ式の詳細

ここでは、HPOM のパターンマッチ言語で使用できる式の詳細を示します。

- **通常の文字**

  通常の文字は、それ自体を表す式です。サポートされてい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には、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。

  [ ] < > | ^ $

  キャレット (^) およびドル記号 ($) が位置指定記号として使用されていない場合 (先頭または末尾の文字でない場合) には、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 (^ および $)**

  キャレット (^) をパターンの先頭文字として使用する場合は、行の先頭にある式にのみ一致します。たとえば、^ab は、行「abcde」内の文字列 ab には一致しますが、行 xabcde 内の文字列 (ab) には一致しません。

ドル記号 ($) をパターンの末尾文字として使用する場合は、行の最後にある式だけに一致します。たとえば、de$ は、行 abcde 内の文字列 de には一致しますが、行 abcdex 内の文字列 (de) には一致しません。

- **複数の文字に一致する式**

任意の数の文字から構成される文字列に一致させるには、次の式をいくつか組み合わせたパターンを使います。

<*>	0 個以上の任意の文字 (セパレータ文字を含む) 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 桁以上の数字と一致します。
<n#>	n 桁の数字と一致します。
<_>	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。
<@>	セパレータ文字を含まない文字列に一致します。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できます。

セパレータ文字は、条件ごとに設定できます。デフォルトでは、セパレータは空白とタブ文字です。

- **角かっこ ([ ])**

角かっこ ([および]) は、式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にも、無意味な角かっこの使用は避けてください。

たとえば、次のパターンは文字列 abcdefgh と等価であり、角かっこはすべて不要です。

```
ab[cd[ef]gh]
```

角かっこは通常、**OR 演算子**や **NOT 演算子**、あるいは変数に文字列を割り当てる**サブパターン**を含む式で使います。

- **OR 演算子 (|)**

特殊文字の縦線 (|) で分けられている 2 つの式は、どちらかの式に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 と文字列 cd の両方に一致します。

```
[ab|c]d
```

- **NOT 演算子 (!)**

NOT **演算子** (!) を使用する場合は必ず角かっこで区切ります。

たとえば、次のパターンは、文字列「WARNING」を含まないすべてのテキストに一致します。

```
<![WARNING]>
```

NOT 演算子は、次の例のように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>
```

このパターンを使えば、user1、user2、および root 以外のユーザーを対象に「ユーザー切換」メッセージを生成できます。

たとえば、上記のパターンは次の文字列に一致します。

```
SU 03/25 08:14 + ttyp2 user11-root
```

一方、次の行は、user2 というエントリを含んでいるため、上のパターンに一致しません。

```
SU 09/25 08:14 + ttyp2 user2-root
```

NOT 演算子を含むサブパターンと一致するものがない場合、**NOT 演算子**は <*> のように機能します。つまり、0 個以上の任意の文字と一致することになります。したがって、UNIX システムの正規表現 [!123] と、HPOM の対応するパターンマッチ式 <![1|2|3]> は同じではありません。HPOM の式が 1、2、3 を除く任意の 1 文字以上の文字列に一致するのに対して、UNIX システムの正規表現は、1、2、3 を除く任意の 1 文字に一致します。

- **マスク演算子 (\)**

円記号 (\) は、次の特殊文字の機能をマスクするために使います。

```
[ ] < > | ^ $
```

特殊文字の直前に円記号 (\) を付けると、特殊文字自体と一致する式になります。

キャレット (^) とドル記号 ($) は、それぞれパターンの先頭と末尾に置かれた場合のみ特殊な意味を持ちます。したがって、パターンの内部 (パターンの先頭や末尾以外) で使用するときには、マスクする必要はありません。

このルールの唯一の例外はタブ文字です。タブ文字をパターン文字列で指定するには、`\t` と入力します。

OR 演算子 (|) は、次に挙げる一致条件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

比較演算子

この種の演算子で複雑な式を作成する場合の基本パターンは次のとおりです。

```
<number--operator--[sub-pattern]--operator--number>
```

サブパターンには単純な数値演算子 (`<#>`、`<2#>` など) を指定できます。単純な演算子には、区切りのための角かっこを付ける必要はありません。次のように、角かっこを含む複雑なサブパターンを指定することもできます。

```
<120 -gt [<#>1] -gt 20>
```

また、次のように、演算子を 1 つだけ使用してパターンを作成することもできます。

```
Error <<#> -eq 1004>
```

比較演算子には次の 6 種類があります。

`-le`	以下
`-lt`	小なり
`-ge`	以上
`-gt`	大なり
`-eq`	等価
`-ne`	不等

以下 (-le) 演算子

使用例:

```
<<#> -le 45>
```

このパターンは、45 より小さいか等しい数値を含むすべてのメッセージに一致します。次に、一致するメッセージの例を示します。

```
ATTENTION: Error 40 has occurred
```

パターン内の数字 45 は実際の数値であり、文字列ではありません。4545 などの 45 よりも大きい数字は、たとえ 45 の組み合わせを含んでいてもマッチしません。

小なり (-lt) 演算子

使用例:

```
 <15 -lt <2#> -le 87>
```

このパターンは、最初の 2 桁が 16 ～ 87 の範囲にある数値を含むメッセージに一致します。次に、一致するメッセージの例を示します。

`Error Message 3299` は一致します。
文字列 `Error Message 9932` 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、文字列「`ERROR_`」の直後に 57 より小さいか等しい数値が続くテキストと一致します。次に、一致するメッセージの例を示します。

```
ERROR_34: processing stopped
```

文字列「34」が変数 `err` に代入されます。

位置指定記号のキャレット (^) 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 の範囲にあって最後の 1 桁が 1 であるすべての数値に一致します。たとえば、21、31、41、... 101、.... 111 などを含むメッセージが、このパターンに一致します。

使用例2:

```
Temperature <*> <@.plant>: <<#> -gt 100> F$
```

このパターンは、「Actual Temperature in Building A: 128 F」のような文字列に一致します。文字「A」が変数 plant に代入されます。位置指定記号 ($) 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、開区間とも呼ばれます。「以上」演算子を使用した場合は、閉区間となります

等価 (-eq) 演算子

使用例:

```
Error <<#> -eq 1004>
```

このパターンは、「`Error`」の直後に数値 `1004` が続く文字列を含むメッセージに一致します。たとえば、次のようなメッセージがこのパターンに一致します。

```
Warning: Error 1004 has occurred
```

一方、`Error 10041` は、このパターンには一致しません。

不等 (-ne) 演算子

使用例:

```
WARNING <<#> -ne 107>
```

このパターンは、「`WARNING`」の直後に空白文字があって、それ以降に 107 以外の 1 桁以上の数値が続く文字列を含むメッセージに一致します。たとえば、次のようなメッセージが一致します。

```
Application Enterprise (94/12/45 14:03): WARNING 3877
```

パターンマッチ式への記号の挿入

メッセージテキストのパターンマッチ式を作成するときには、マウスの左右のボタンを使って記号を式に挿入できます。

式の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。

この方法は、変数名の挿入には使用できません。変数名は、それぞれ個別に式に入力する必要があります。

パターンマッチ式の変数とパラメータ

一致する文字列は、すべて変数に割り当てることができます。文字列を割り当てた変数は、メッセージのフォーマットの変更や、アクション呼び出しのパラメータとして使うことができます。パラメータを指定するには、角かっこで閉じる直前に .パラメータ名 を追加します。パターン ^errno: <#.number> - <*.error_text> は、次のようなメッセージと一致します。

```
errno: 125 - device does not exist
```

number には 125、**error_text** には device does not exist がそれぞれ割り当てられます。

変数名に含めることができるのは、アルファベットと数字、および下線 (_) とハイフン (-) だけです。次の構文規則が適用されます。

```
(Letter | '_'){ Letter | Digit | '_' | '-' }
```

この構文で、Letter はアルファベットのすべての文字、Digit はすべての数字に該当します。

HPOM による変数への文字列割り当ての規則

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** へ a を、**var2** へ bcdef を割り当てることができますし、同様に、var1 へ空の文字列、**var2** へすべての入力文字列を割り当てることもできます。

パターンマッチアルゴリズムは、常に入力行とパターン定義 (二者択一正規表現を含む) の両方を左から右へ調べます。<*> などの式には、できるだけ少ない文字を割り当てます。一方、<#>、<@>、<_> などの式には、できるだけ多くの文字を割り当てます。したがって、上記の変数 var1 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>
```

この場合、各変数には値が次のように割り当てられます。

- **errnumber**: 100
- **errtext**: big bug

パフォーマンスのため、また、パターンを読みやすくするために、連続する 2 つの式の間には区切りとなるサブ文字列を指定できます。上記の例では、<#> と <*> の区切りとして、コロン (:) が使われています。

abc123 と **<@.word><#.num>** の照合では、<#> と <@> の両方が数字を受け入れ、左側の式にできるだけ多くの文字が割り当てられるため、**word** に abc12、**num** に 3 がそれぞれ割り当てられます。

位置指定記号が指定されていないパターンは、入力行のどの位置のサブ文字列にも一致します。たとえば、this is number<#.num> というパターンは次のパターンと同じように処理されます。

```
<*>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方法には、単独の演算子 (* や # など) 以外にも、複数の演算子を組み合わせた複雑なサブパターンを作成する方法があります。サブパターンの構文は<[sub-pattern].var> です。

次に例を示します。

```
<[<@>file.tmp].fname>
```

この例では、file と tmp の間のドット (.) は通常のドット文字と一致します。一方、「]」と「fname」の間のドット (.) は、構文的に必要な要素です。このパターンは Logfile.tmp のような文字列と一致し、一致する文字列全体が fname に割り当てられます。

他のサブパターンの例を次に示します。

```
<[Error|Warning].sev>
```

```
<[Error[<#.n><*.msg>]].complete>
```

最初の例では、Error または Warning を含むあらゆる行が、変数 sev に割り当てられます。2 番目の例では、Error を含む行のエラー番号が変数 n、エラー番号に続く文字列が msg に割り当てられます。最終的に、数字とテキストの両方が complete に割り当てられます。

複数行メッセージに一致するメッセージポリシー条件の設定

opcmsg コマンドを使用して送信された複数行メッセージに一致するメッセージポリシー条件を設定するには、”</>” パターンまたは n 個の改行に完全一致する “<n/>” パターン (たとえば、1 つの改行に完全一致するには ”<1/>”) を使用します。

メッセージブラウザに複数行メッセージを表示するように [属性の設定 : メッセージ テキスト] フィールドを設定するには、“\n” を使用します。その例を次に示します。

メッセージテキストフィールド (条件):

```
^First line:<*.text1><1/>Second line:<*.text2>$
```

メッセージテキストフィールド (属性の設定):

```
Message with two lines: \n First line:<text1>\n
Second line: <text2>
```

コマンドラインから複数行メッセージを送信するには、メッセージテキスト名を引用符で囲んで指定し、行の最後に **ENTER** キーを押します。その例を次に示します。

```
# opcmsg a=a o=o msg_t="First line: Hi
Second line: there"
```

前のポリシー条件が有効な場合は、メッセージブラウザに次のメッセージテキストが表示されます。

```
Message with two lines:
  First line: Hi
  Second line: there
```

一致したメッセージの表示

メッセージ条件に一致したメッセージには、ブラウザに表示する前に特定の属性を設定できます。

メッセージ属性の設定

値を設定できる属性は次のとおりです。

- ❏ 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
- ❏ メッセージの種類
- ❏ メッセージキー
- ❏ サービス名

条件レベルで設定された属性は、ポリシーのデフォルトで定義された同じ属性より優先します。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、「メッセージ属性の設定」(220 ページ) に示されるデフォルトのメッセージ属性のほかに、「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だけであり、ログファイル、HPOM インタフェース、およびしきい値モニターの各ポリシーでのみ利用可能です。

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、`opccmachg` コマンドラインツールを使用します。詳細については、opccmachg(1m) 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設定する場合、属性の名前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、Java GUI ブ ラウザに 4 つカラムが追加されて表示されます。

- ❏ Customer
- ❏ Device
- ❏ SLA
- ❏ Source

値には、次のいずれか 1 つ、またはいくつかを組み合わせて指定できます。

- ❏ ハードコードされたテキスト
- ❏ HPOM のパターンマッチで返された変数

  詳細については、「メッセージのパターンマッチ」(209 ページ) を参照してください。
- ❏ HPOM であらかじめ定義されている変数

  詳細については、『HPOM 管理者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が表示されるのは、Java GUI のブラウザウィンドウとメッセージプロパティウィンドウ内だけです。

カスタムメッセージ属性が、エージェントや管理サーバーの両方またはいずれか一方のメッセージストリームインタフェース (MSI) に渡されるように設定することも可能です。また、トラブルチケットシステムや通知サービスの両方またはいずれか一方に出力することも可能です。

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。指示には、通常、自動アクションを記述したり、オペレータがオペレータ起動アクションを実行するための詳細な情報を提供したり、障害解決のための別の手動による手順を記述します。

メッセージに指示を追加するには、次のいずれかの方法を使います。

❏ **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。テキストによる簡単な指示には、データベースに格納できるという利点があります。

この方法には次の利点があります。

- 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。この方法には、さまざまな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利点があります。

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、HPOM の特殊な変数によって外部アプリケーションを呼び出したり、Java GUI が動作しているクライアント上で Web ブラウザを開くことができます。詳細については、『HPOM 管理者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使ってメッセージに応答します。一部の応答は、オペレータの操作を介さずに実行されます。

応答

次の応答の種類から選択できます。

- **管理サーバーのログにのみメッセージを記録**

  このオプションを選択すると、メッセージ条件に一致するメッセージが管理サーバーのログに記録され、履歴データベースに格納されます。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

  メッセージを管理サーバーのログのみに記録する場合、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、メッセージが着信した時点で即座に起動されます。アクションを起動す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、またはその他の応答) をアクションごとに定義する必要があります。オペレータは実行中の自動アクションを停止したり、必要に応じて再起動することができます。

  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。自動受諾で自動アクションを設定すると、メッセージが Java GUI メッセージブラウザに表示されないことがあります。

- **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、**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、オペレータはオペレータ起動アクションを停止したり、必要に応じて再起動することができます。管理者は、オペレータ起動アクションのノードとコマンドを定義できます。また、注釈作成と受諾を自動的に行うかも指定できます。

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の中に入力します。こうすることで、オペレータは、オペレータ起動アクションを開始した場合に実行される処理の内容を正確に知ることができます。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:

- バックアップ開始前にデータベースを停止する
- プリントスプールに入る前に、サブシステムが保守モードになることをユーザーに通知する

❑ **メッセージの転送**

メッセージは、トラブルチケットシステムや外部通知サービスに転送できます。さらに、転送後に自動的に受諾するように設定することも可能です。

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には、どちらにも自動注釈と自動受諾を指定できます。

自動注釈では次の情報が記録されます。

❑ アクションの開始時刻と停止時刻

❑ 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ー処理のための方針

本項では、メッセージのフィルター処理を最適化してシステムのパフォーマンスを向上させ、オペレータのブラウザに重複メッセージや重要でないメッセージが表示されないようにするための方法を示します。

メッセージのフィルター処理

メッセージのフィルター処理は、管理対象ノードと管理サーバーの両方で実行できます。

- **管理対象ノード**

  管理対象ノードで、できるだけ多くのメッセージにフィルター処理を施せば、ネットワークトラフィックが最小限に抑えられ、管理サーバーの負荷が減ります。

- **管理サーバー**

  管理サーバーでフィルター処理を行うことで、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。除外したメッセージ数をカウントするように、管理サーバーを設定することもできます。**グループ替え条件**を指定すると、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分けをカスタマイズできます。グループ替え条件では、メッセージはフィルター処理されません。グループ替え条件の詳細については、「メッセージのグループ替え」(248 ページ) を参照してください。

パフォーマンスの最適化

条件を正しい順序で指定し、不一致除外条件を展開することで、処理性能を簡単に最適化することができます。

条件の順序の設定

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、ポリシーの先頭に不一致除外条件または除外条件を置くと (つまり、最初から不要なメッセージをフィルターによって除外しておくと)、メッセージ条件を先頭に置く場合よりも、処理要求は少なくなります。照合するメッセージが少ないと、処理量が減少してパフォーマンスが向上します。

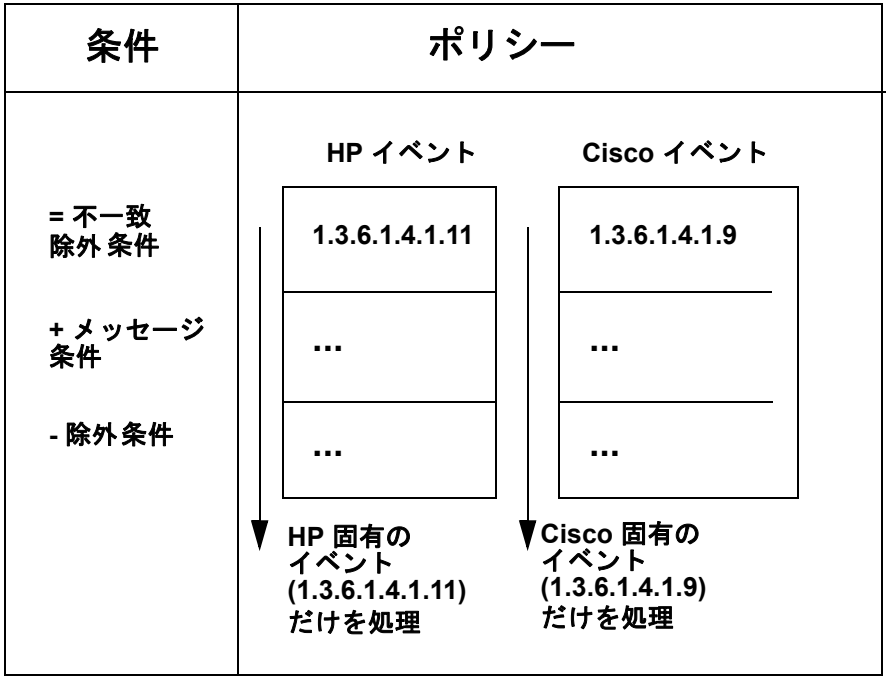
不一致除外条件の利用

不一致除外条件により、管理対象ノード上でイベントがフィルター処理されます。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。不一致除外条件では、特定のパターンに一致しないイベントが除外される一方、一致するイベントはリストの残りの条件に従って処理されます。不一致除外条件では、特定のポリシーに該当するイベントだけが HPOM によって処理されるため、管理対象ノード上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ー処理性能を向上させるには、環境内の特定企業用イベントごとにポリシーを作成し、さらに条件リストの先頭に不一致除外条件を置きます。これにより、HPOM は条件に一致しない SNMP トラップを MIB オブジェクトから除外し、作成したポリシーで想定しているトラップだけを処理するようになります。

図 4-8 では、HP の SNMP トラップ用ポリシーによって Cisco の MIB オブジェクトの SNMP トラップが除外され、HP 固有のイベントだけが処理されます。

図 4-8　企業に固有の SNMP トラップのチャネリング



メッセージ数の抑制

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がオペレータの負担にな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)。

- **類似または同一のイベント**

  一部のメッセージは、類似のイベントまたは同じイベントについて報告します (たとえば、ユーザーが root ユーザーに 3 回切り替わった場合)。

- **問題の悪化**

  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、重要かつ適切なメッセージだけをオペレータに送信す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

メッセージの置き換えは、メッセージ相関処理とイベント相関処理を通じて実行されます。

- **メッセージ相関処理**

  メッセージ相関処理は HPOM の内蔵メカニズムによって実行できますが、使用される相関処理技法は基本的なものにすぎません。相関処理を初めて使う場合は、まずメッセージ相関処理から始めて、より高度なソリューションへと段階的に移行することが推奨されます。

- **イベント相関処理**

  イベント相関処理の詳細については、「HPOM のイベント相関処理」(282 ページ) 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処理できる。イベント相関処理エンジンで処理している間に、イベントの状態が変化することがある。同じ入力イベントが、現在の状態に応じて別の出力イベントを生成することがある	• 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ない。
• 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る。

a. 管理サーバー上で除外を有効にすると、除外されたメッセージもカウントされます。

メッセージ相関

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。

HPOM はイベントやメッセージに対して、次のいずれかの方法で対応します。

- **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 (「標準的なシナリオの自動化」(232 ページ) 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 (「重複メッセージの除外」(236 ページ) を参照)。

管理サーバーで重複メッセージの除外を有効にしても、HPOM は除外されたメッセージ数もカウントします。

メッセージキー

メッセージは**メッセージキー**に基づいて相関処理されます。場合によっては、他のイベント属性やメッセージ属性が比較されることもあります。メッセージキーとは、メッセージを出力する原因となるイベントの重要な特徴を表すメッセージ属性です。

メッセージキー関連の設定には、`MSGKEY` と `MSGKEYRELATION ACK` キーワードを使用します。

効果的なメッセージキー作成のガイドライン

効果的なメッセージキーとは、メッセージの起因になったイベントを簡潔に説明するメッセージキーのことです。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 (「標準的なシナリオの自動化」(232 ページ) を参照) と重複メッセージの除外 (「重複メッセージの除外」(236 ページ) を参照) に使うことができます。

効果的なメッセージキーを作成するためのガイドラインを次に示します。

- **メッセージキーにノード名を含める**

  HPOM の変数 `$MSG_NODE_NAME` を使います。この変数により、そのコンピュータで生成されるメッセージを他のコンピュータのメッセージと区別することができます。

例

```
my_appl_down:<$MSG_NODE_NAME>
```

- **他の重要な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となるメッセージ属性をすべて指定する必要があります。通常、このような属性には、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 (しきい値のモニターポリシーの条件を定義する場合)、[条件] セクションで定義する変数などがあります。

  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 管理者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指定する必要があります。重要度の文字列そのものをメッセージキーに含める必要はありません。重要度のレベルの決定要因を含めることで、重要度を反映させる方法を使います。この要因は、メッセージ情報自体に含まれています。たとえば、しきい値のモニターポリシーの場合には、変数 <$THRESHOLD> を含めることができます。<$THRESHOLD> の個々の値は、それぞれが重要度のレベルを表します。

- **HPOM がデフォルトの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連と共にデフォルトのメッセージキーを生成するには、AUTOMATIC_MSGKEY キーワードを使用し、オプションとしてキーワードの後に文字列値を指定します。このキーワードは、既存の条件にメッセージキーを指定する場合にも利用できます。

  メッセージキー関連の詳細については、「デフォルトのメッセージキーとメッセージキー関連の生成」(233 ページ) を参照してください。

- **読みやすくする**

  コロン (:) などでメッセージキーの各構成要素を区切ります。

  例

  ```
  my_appl_down:<$MSG_NODE_NAME>
  ```

効果的なメッセージキー関連のためのガイドライン

効果的なメッセージキー関連を作成するためのガイドラインを次に示します。

- **変数の解決に注意する**

  メッセージキー関連は主に、管理対象ノードで値に解決される HPOM の変数から構成されます。メッセージキー関連には、HPOM のパターン定義も含めることができます。パターンは管理サーバーで照合されます。

- **読みやすくする**

  コロン (:) などでメッセージキー関連の各構成要素を区切ります。

  例

  ```
  my_appl_down:<$MSG_NODE_NAME>
  ```

- **メッセージキー関連を位置指定文字で囲む**

  メッセージキー関連を位置指定文字で囲みます。先頭に脱字符号 (^) を、末尾にドル記号 ($) を使います。これにより、処理性能が向上します。

  例

  ```
  ^<$NAME>:<$MSG_NODE_NAME>:<$MSG_OBJECT>:<*>$
  ```

- **パターン定義を正しい位置に指定する**

  メッセージキー関連でパターン定義を使う場合は、文字列中の正しい位置にパターン定義を指定します。これにより、処理性能が向上します。

  パターン定義を正しい位置で指定した例

  ```
  ^<$MSG_NODE_NAME>:abcdef:[pattern]$
  ```

  パターン定義を不適切な位置で指定した例

  ```
  ^[pattern]:<$MSG_NODE_NAME>:abcdef$
  ```

- **大文字/小文字の区別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 管理者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。

そのような状況の例を次に示します。

問題の解決

最初のメッセージで問題が報告されたとします。次のメッセージでは、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、実質的には、状態ベースのブラウザとなります。(しきい値のモニターにこの概念を適用する方法については、「デフォルトのメッセージキーとメッセージキー関連の生成」(233 ページ) を参照してください。)

メッセージキーによるメッセージの受諾

関連するメッセージを管理する場合、1 番目と 2 番目 (または2 番目と 3 番目) のメッセージの関係は、メッセージキーにより確立されます。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し、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体に指定されます。

受諾するメッセージと受諾されるメッセージへの注釈付け

メッセージが他のメッセージを自動受諾するときには、両方のメッセージに次のように注釈が付けられます。

- **受諾されるメッセージ**

  受諾されるメッセージには、受諾するメッセージの詳細情報を含む注釈が自動的に付けられます。この詳細情報には、受諾するメッセージのメッセージ ID、条件 ID、メッセージキー関連などが含まれます。

- **受諾するメッセージ**

  受諾するメッセージには、受諾されるメッセージの詳細情報を含む注釈が自動的に付けられます。この詳細情報には、受諾されるメッセージのメッセージキー関連、受諾したメッセージの数、受諾したメッセージのメッセージ ID と条件 ID などが含まれます。

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、および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連の生成

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、メッセージキー関連を条件ごとに生成できます。

デフォルトのメッセージキーとメッセージキー関連を条件ごとに生成するには、`AUTOMATIC_MSGKEY` キーワードを使用してください。

次のデフォルト値が生成されます。

- **メッセージキー**

  ```
  <$NAME>:<$MSG_NODE_NAME>:<$MSG_OBJECT>:<$THRESHOLD>
  ```

- **メッセージキー関連**

  ```
  ^<$NAME>:<$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 のルートディレクトリ (/) のディスク使用量が 90% を超えたことを、モニター disk_util が検出したことを示します。

メッセージキー関連により、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量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

HPOM は、モニター対象の値がしきい値を超過した後に、すべてのリセット値を下回ると、リセットメッセージを送信してモニター対象オブジェクトの最後のメッセージを自動的に受諾します。つまり、どの条件にも一致しなくなります。

リセットメッセージには、特定のモニター用の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連が含まれます。最後に送信されるメッセージは、メッセージキーを含む必要があります。メッセージキーが含まれないと、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のデフォルトの文字列は、<monitor_name>[(<instance>)]:<value> (below reset) であり、変更することはできません。

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ダイレクトに送信されます。リセットメッセージの重要度は「正常域」です。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の詳細については、「複数の条件によるしきい値のモニター」(271 ページ) 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一例を示しています。

図 4-9 HPOM のリセットメッセージ例

```
MONITOR "my_mon"
  ...
    MAXTHRESHOLD
    ...
      DESCRIPTION  "my_mon 1"
      CONDITION
          ...
          THRESHOLD 99.0000
          RESET 95.0000
          ...
      SET
          ...
          SEVERITY Critical
          ...
          MSGKEY "<$NAME>:<$MSG_NODE_NAME>:<$MSG_OBJECT>:<$THRESHOLD>"
          MSGKEYRELATION ACK "^<$NAME>:<$MSG_NODE_NAME>:<$MSG_OBJECT>:<*>$"

      DESCRIPTION  "my_mon 2"
      CONDITION
          ...
          THRESHOLD 90.0000
          RESET 85.0000
          ...
      SET
          ...
          SEVERITY Major
          ...
          MSGKEY "<$NAME>:<$MSG_NODE_NAME>:<$MSG_OBJECT>:<$THRESHOLD>"
          MSGKEYRELATION ACK "^<$NAME>:<$MSG_NODE_NAME>:<$MSG_OBJECT>:<*>$"

      DESCRIPTION  "my_mon 3"
      CONDITION
          ...
          THRESHOLD 80.0000
          RESET 75.0000
          ...
      SET
          ...
          SEVERITY Warning
          ...
          MSGKEY "<$NAME>:<$MSG_NODE_NAME>:<$MSG_OBJECT>:<$THRESHOLD>"
          MSGKEYRELATION ACK "^<$NAME>:<$MSG_NODE_NAME>:<$MSG_OBJECT>:<*>$"

      Reset Message: monitored value below lowest possible reset value (< 75%).
```

この例では、モニター my_mon に次の 3 つの条件が設定されています。

- my_mon 1

  モニター対象の値が 99% を超えると危険域メッセージを生成します。値が 95% 未満に下がると、カウンターがリセットされます。

- my_mon 2

  モニター対象の値が 90% を超えると重要警戒域メッセージを生成します。値が 85% 未満に下がると、カウンターがリセットされます。

- my_mon 3

  モニター対象の値が 80% を超えると警告メッセージを生成します。値が 75% 未満に下がると、カウンターがリセットされます。

各メッセージのメッセージキー関連により、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”で生成されるメッセージ) は、モニター対象の値が最も低いリセット値 (この場合 75%) 未満に下がると、リセットメッセージにより自動受諾されます。

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

通常、重複メッセージとは、同じイベントや類似したイベントを通知するメッセージのことをいいます。たとえば、HPOM では、ユーザーが別のユーザーに切り替わるたびにメッセージが生成されます。常に同じユーザーへ切り替わる場合はこの情報が必要ないので、このイベントを同じイベントとして宣言し、このイベントに関するメッセージをそれ以降除外できます。さらに、HPOM では、新しい重複メッセージを送信するまでのメッセージの除外頻度と除外期間を指定できます。

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、「重複メッセージの重要度とメッセージテキストの更新」(244 ページ) を参照してください。

HPOM では、管理対象ノードか管理サーバーのどちらかで重複メッセージを除外するように設定することができます。管理対象ノードでメッセージをフィルター処理(除外) すると、ネットワークトラフィックが減り、管理サーバーを別のタスクに使うことができます。

メッセージの除外は管理対象ノード上で行う方が効率的であるため、HPOM は管理対象ノードに対して多様な除外のタイプと設定を用意し、管理サーバーについては、グローバルな設定だけを用意しています。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。

除外の種類の検証

イベントが条件に一致すると、HPOM は次のいずれかの種類の除外が選択されているかどうかを検証します。

- **メッセージ条件に一致すれば除外**

  選択された条件と一致する重複メッセージがすべて除外されます。つまり、HPOM は同じ条件により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。

  そのようなメッセージがすでに存在する場合、次のイベントが指定した除外期間内に発生しているか、またはカウンターの値が設定した値に満たないとき、このイベントのメッセージは除外されます。

- **同じ入力イベントの除外**

  イベント属性が同一の重複メッセージのみが除外されます。つまり、HPOM は同じ入力イベントにより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 [条件] セクションで定義されています。2 つ以上のメッセージで次の各イベント属性が同じであれば、それらのイベントは同一と解釈されます。

  - 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)

同じメッセージがすでに存在する場合、指定した除外期間内に次のイベントが発生しているか、またはカウンターの値が設定した値に満たないとき、このイベントのメッセージは除外されます。

❑ **同じ出力メッセージの除外**

メッセージ属性が同一の重複メッセージのみが除外されます。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 [属性の設定] セクションで定義されています。複数のメッセージのメッセージキーが同じであれば、それらのメッセージは同一と見なされます。

どちらかのメッセージにメッセージキーがない場合は、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、指定した除外期間内に次のイベントが発生しているか、またはカウンターの値が設定した値に満たないとき、このイベントのメッセージは除外されます。

HP-UX の `syslog` デーモンのログファイル (`/var/adm/syslog/syslog.log`) を使って、[同じ出力メッセージの除外] オプションで重複メッセージを除外する方法を次に示します。

たとえば、この `syslog` ログファイルに次の行が含まれているとします。

```
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
```

この場合のパターンマッチテキストとしては、次のような文字列が考えられます。

```
"inetd\[<#>\] <@.service>: Connection from <@.from_node>"
```

inetd 接続メッセージで重要なのは、ローカルノード、接続した側のノード、および inetd サービスです。syslog のタイムスタンプ、PID、および接続時間は重要ではありません。

したがって、次のようなメッセージキーを使うことができます。

```
inetd_connect_from:<$MSG_NODE_NAME>:<from_node>:
<service>
```

このメッセージキーを使えば、サービス、接続先ノード、接続元ノードがすべて同じメッセージがすべて除外されます。

重複メッセージの除外では、同じ条件で生成されたメッセージだけが処理されます。異なる条件で生成された重複メッセージを除外するには、この機能を管理サーバーで有効にします。詳細については、「管理サーバーでの重複メッセージの除外」(242 ページ) を参照してください。

注記

管理対象ノードでは、しきい値のモニターポリシーに対して重複メッセージの除外を適用できません。しきい値のモニターポリシーから重複メッセージを除外する方法については、「管理サーバーでの重複メッセージの除外」(242 ページ) 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 つのタイプがあります。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	同じ条件に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。

これらのキーワードの後に続く値は、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 (キーワードの直後には数字を指定) を使用すると、定義したメッセージ数を受信するまでメッセージは除外されます。指定数に達した後にメッセージが 1 つ送信されると、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 は制限時間を指定し、その時間が経過すると、メッセージの送信が再開されます。詳細については、付録 A「ポリシー本体の構文」(355 ページ) を参照してください。

除外設定の種類

次の除外設定のどれかを選択します。

- **除外期間**

  重複イベントを無視する期間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。241 ページの図 4-10 の例では、除外期間が 30 秒に設定され、最大除外期間が 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、カウンターの値が1 ずつ増加ししきい値以上になると、重複メッセージの送信を許可します。242 ページの図 4-11 の例では、カウンターのしきい値は 2 に設定されています。カウンターの値は 30 秒後にリセットされます。

- **除外期間とカウンターの組み合わせ**

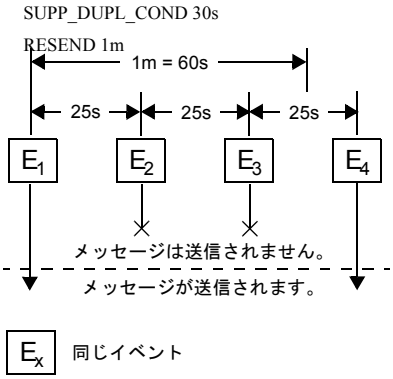
  除外期間とカウンターを併用する場合、イベントはまず除外期間で評価されます。時間によって除外されないイベントはカウンターによって評価され、その結果に従って除外されるか、または管理サーバーに送信されます。

時間に基づく除外

図 4-10 は、時間に基づく除外を示しています。

同じ入力イベントの除外では、代わりに SUPP_DUPL_IDENT キーワードを使用します。同じ出力メッセージの除外では、SUPP_DUPL_IDENT_OUTPUT_MSG キーワードを使用します。

図 4-10 時間に基づく除外

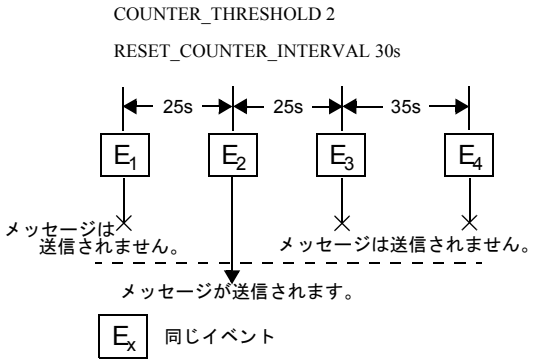


1. 最初のイベント (E_1) が条件と一致します。メッセージが送信されます。タイマーが起動されます。
2. 2 番目のイベント (E_2) が 25 秒後に発生します。このイベントは、最初のイベントから 30 秒未満で発生しているため、除外されます。
3. 条件と一致する 3 番目のイベント (E_3) は、2 番目のイベントから 30 秒未満で発生しているため、除外されます。
4. 次に条件と一致するイベント (E_4) は、3 番目のイベントから 30 秒未満で発生しています。ただし、最初のイベントから 60 秒を超えているため、新しいメッセージが送信されます。

カウンターに基づく除外

図 4-11 は、カウンターに基づく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。カウンターの値が 1 に増加します。この場合、しきい値 (2) 未満であるのでメッセージは送信されません。
2. 2 番目の該当イベント (E_2) が 25 秒後に発生します。カウンターの値が 2 に増加します。メッセージが送信されます。カウンターは、0 にリセットされます。
3. 3 番目の該当イベント(E_3)が発生します。カウンターの値が 1 に増加します。メッセージは送信されません。
4. 次の該当イベント (E_4)が 3 番目のイベントから 30 秒後以降に発生します。カウンターは 30 秒で 0 にリセットされています。したがって、カウンターの値は 1 に増加します。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。管理サーバーで重複メッセージを除外すれば、システムで大量のメッセージを処理する必要がなくなり、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送信されるメッセージを相関処理することもできます。

管理サーバーで使われる除外の方法は、管理対象ノードでの [同じ出力メッセージの除外] と同じです。受信メッセージと既存のメッセージの間でメッセージ属性が比較されます。

どちらかのメッセージにメッセージキーがない場合は、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後続のすべての重複メッセージを除外します。重複のカウントは、最初のメッセージで開始されます。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、最後に重複メッセージが着信し除外された日時が表示されます。

除外を有効にすると、除外された重複メッセージの情報が、最初のメッセージの注釈に保存されます。

注記

重複メッセージにより管理対象ノード上で起動された自動アクションは、引き続き動作します。ただし、アクションに対する応答は失われます。

管理サーバー上での重複メッセージの除外の有効化

管理サーバーでの重複メッセージの除外は、コマンド `opcsrvconfig -dms` で有効化できます。また、重複メッセージを注釈として追加するように指定することもできます。例:

```
# opcsrvconfig -dms -enable anno
```

注記 重複メッセージの除外はグローバルな設定であり、すべてのメッセージとオペレータに影響します。

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、各管理サーバーが、その直接管理する管理対象ノードからの受信メッセージのカウントを担当します。つまり、他の管理サーバーからの受信メッセージは 1 つのメッセージとしては集約されず、複数のメッセージとして、送信元の管理サーバーから受信したときにそれぞれカウントされます。

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、`ovconfchg` コマンドラインツールを使って HP Operations 管理サーバーの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

着信した重複メッセージの重要度やメッセージテキスト内容が既存メッセージと異なる場合に、既存の値ではなく新しい値を表示するように HPOM を設定することができます。

- **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
```

値を LAST_MESSAGE に設定すると、メッセージブラウザ内の該当する値が更新されます。

メッセージの記録

HPOM は次のようなタイプに分けてメッセージを処理します。

- **メッセージ条件に一致するメッセージ**

  これらのメッセージは、フィルター処理で HPOM に取り込まれます。これらのメッセージは、ローカルノードから管理サーバーに転送されて処理されます。メッセージをソースノード上で記録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。

- **除外条件に一致するメッセージ**

  これらのメッセージは、フィルター処理で HPOM から除外され、それ以上処理されません。これらのメッセージを、ソースノード上に記録するように指定することができます。

- **どの条件にも一致しないメッセージ**

  条件に一致するメッセージが存在しない場合、一致しないメッセージも HPOM に送ることができます。通常、一致しないメッセージは初めて出現するメッセージで、それに対応するフィルター条件を設定していないものです。不一致メッセージは管理対象ノードにローカルに記録するか、処理のため管理サーバーに送るかを選択できます。管理サーバーに送る場合は、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格納するかを選択できます。ブラウザに表示される場合は、Java GUI メッセージブラウザの U カラムの `X` で識別されます。

ログのオプションは、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。各メッセージタイプをどのように記録するかを指定するには、ポリシー本体で次のキーワードを使用します。

```
LOGMATCHEDMSGCOND
LOGMATCHEDSUPPRESS
LOGUNMATCHED
```

注記

イベント相関処理ポリシーのいずれかに対するログ機能をオンにすると、その他のイベント相関処理ポリシーに対して、ログ機能が自動的にオンになります。

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、フィルター処理された後に、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。オペレータの作業と作業範囲に合うように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。

メッセージの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、管理対象ノードで処理されます。これらの条件は、管理対象ノードですべての受信メッセージと照合されます。

- **グループ替え条件**

  グループ替え条件は管理サーバーのみで処理されます。管理対象ノードでのフィルター処理を通過したメッセージと照合されます。

  グループ替え条件と一致するメッセージは、管理者の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が出力するすべてのメッセージを、`Output` というメッセージグループに入れることもできます。

- **メッセージ属性**

  メッセージ条件や除外条件と同様に、グループ替え条件に定義したメッセージ属性がメッセージの実際の値の検査で使われます。

グループ替え条件の定義

グループ替え条件を定義する場合は、管理 UI を使用します。

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。

また、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

このグループ替え条件の例は、前述のメッセージ条件の例を基にしています。

前例では、HPOM 内へフィルタリングされたすべてのメッセージはメッセージグループ `FINANCE` に転送されました。

ここでは、メッセージを次の 2 つのグループに分割します。

- payroll
- accounting

これら 2 つのグループへのグループ替え条件を次に示します。

グループ替え条件 1

ノード :	`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

ノード：	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

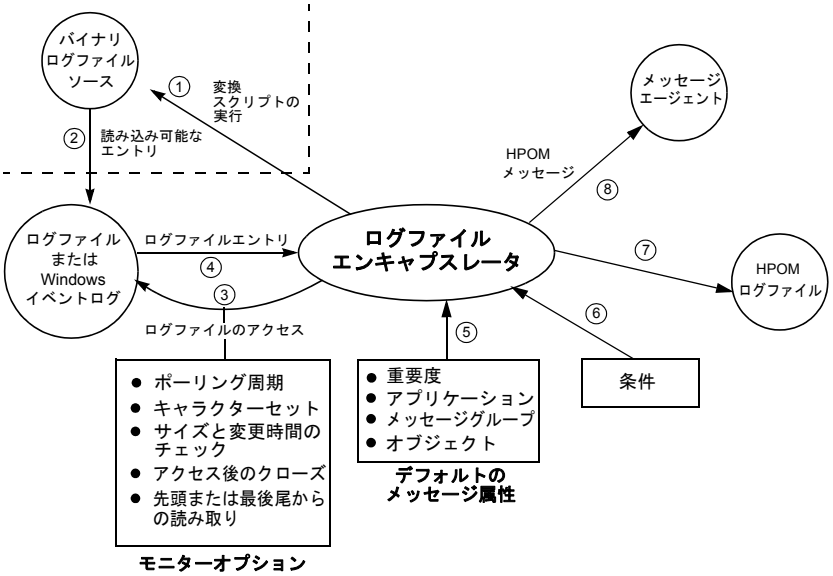
ログファイルメッセージ

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。ログファイルを作成するアプリケーションまたはサービスからメッセージを HPOM 内に取り込むことができます。アプリケーションまたはサービスに変更を加える必要はありません。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。複数のポリシーを使用して、さまざまなアプリケーションやサービスをモニターするログファイルを設定できます。

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収集してフィルター処理とフォーマット変更を施し、ブラウザウィンドウに表示する方法を示しています。

図 4-12　ログファイルエンキャプスレータ



手順 1 と手順 2 は、ログファイルがバイナリ形式の場合のみ必要です。

手順 7 は、ローカルログ機能が設定されている場合にのみ実行されます。

手順8 は、ログファイルエントリがメッセージ条件に一致した場合、または不一致の転送の条件が真である場合に適用されます。

ログファイルエントリポリシー

ログファイルエントリポリシーには、このソースからのすべてのメッセージを示すデフォルトのメッセージ属性を定義します。また、251 ページの図 4-12 に示すように、ログファイルをモニターする方法とタイミングを指示するモニターリングオプションもポリシーに指定します。

ログファイルエントリポリシーには、次の設定が含まれます。

- **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一覧表示します。

- **ログファイルのパス名と名前**

  ファイルシステム内でのログファイルの場所。UNIX で稼動している管理対象ノードでは、シェル変数を使って動的なパスを指定できます。さらに、ログファイル名を動的に検出して `stdout` に出力するコマンドまたはスクリプトの名前も指定できます。

- **モニターオプション**

  ログファイルの内容を走査する前に実行するコマンドまたはプログラム、ログファイルの別名、ポーリング周期、ログファイルで使用される文字セット、およびモニターの実行方法の詳細。

  HPOM では、ログファイルの処理を開始する位置として、次の 3 つの読み取り位置があります。

  - 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だけをモニターします。

  - 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モニターを開始するときに、初回のみログファイル全体をモニターします。次のポーリング周期では、追加されたエントリのみがモニターされます。

  - ファイルの先頭から読み取り (常時)

    ログファイルへの変更が検出されたときに、ログファイル全体を読み取ります。ログファイルエンキャプスレータは、ポーリング周期の終了後、起動時、およびログファイルエントリポリシーの配布時にはログファイルを処理しません。

HPOM は、inode (UNIX の場合) または作成日時 (Windows の場合) が変更されたログファイルを新規ファイルとして扱います。新規のログファイルは、ログファイルエンキャプスレータによってファイル全体が処理されます。

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。これはたとえば、システムログファイルの場合に起こります。

次のような場合、新規のログファイルとはみなされません。

- 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**

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。

ログファイルエントリポリシーを定義するには、ポリシー本体内で更新を行う必要があります。詳細は付録 A「ポリシー本体の構文」(355 ページ) 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

ログファイルエントリポリシーで `NODE` キーワードを使用しない場合、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 Agent がクラスタノードで実行されるクラスタ環境では、ログファイルをモニターするのに別のノードを指定できます。

NFS マウントしたファイルシステムにあるログファイルを変更する場合、または他のリモートノードのログファイルを HPOM ログファイル エンキャプスレータを実行中のシステムにコピーする場合は、別のノードを指定してください。

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を使用します。

- 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。その後、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外部ノードを設定したり、またはログファイルからのホストシステム上のディレクトリに抽出するように外部ノードを設定することができます。これは、指定されている時間間隔が経過した後、またはログファイルが変更されたときに自動的に行われます。HPOM ではこの機能がサポートされていないため、コピー操作は外部機能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て、コピーが完了すると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、またメッセージはどのイベントによって生成されたかを HPOM オペレータが認識できるように、対応するログファイルエントリポリシーを設定する必要があります。ポリシー本体の構文の詳細については、付録 A「ポリシー本体の構文」(355 ページ) 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についてのオプションも定義できます。これらのオプションは、追加する新規ポリシーのデフォルトとして使用されます。これによって既存のポリシーの動作が変化することはありません。

メッセージの条件の指定

対応するポリシーのポリシー本体を編集することで、メッセージの条件を指定できます。ポリシー本体の構文の詳細については、付録 A「ポリシー本体の構文」(355 ページ) を参照してください。

例 4-1 **ログファイルエントリポリシー本体の例**

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。ファイルは 60 秒ごとにチェックされます。ログファイルエンキャプスレータは直前のチェック終了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直前に開かれ、読み取り直後に閉じられます (キーワード CLOSE_AFTER_READ)。“missing” という単語を含むメッセージは除外され、"failure" という単語を含むメッセージの重要度は危険域に設定されます。その他のすべてのメッセージはサーバーに転送されます (これは、FORWARDUNMATCHED キーワードによって実行されます)。すべてのメッセージのアプリケーション属性は “App” に設定され、メッセージグループは “AppLog” に設定され、条件に一致しないメッセージの重要度は不明に設定されます。

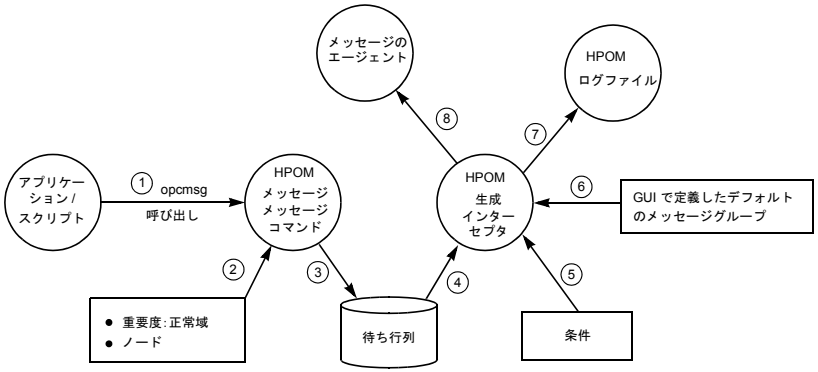
```
LOGFILE “Application log”
                  DESCRIPTION “Logfile for Application”
                  LOGPATH “/opt/App/log/logfile.txt”
                  INTERVAL “60s”
                  FROM_LAST_POS
                  CLOSE_AFTER_READ
                  SEVERITY Unknown
                  APPLICATION “App

MSGGRP “AppLog”
FORWARDUNMATCHED

SUPPRESSCONDITIONS

                  DESCRIPTION “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の `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) の `opcmsg(3)` を使えば、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することができます。

図 4-13 は、HPOM メッセージインタフェースが HPOM メッセージを捕捉して、フィルター処理とフォーマット変更を施し、ブラウザに表示する方法を示しています。

図 4-13　HPOM メッセージインタフェース



手順 7 は、ローカルログ機能が設定されている場合のみ実行されます。

手順 8 は、メッセージ条件に一致する場合のみ実行されます。

`opcmsg(1|3)` コマンド API 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についてのオプションも定義できます。これらのオプションは、追加する新規ポリシーのデフォルトとして使用されます。これによって既存のポリシーの動作が変化することはありません。

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。ただし、しきい値の超過が短時間の例外的なピークに過ぎない場合もありえます。そのような状態によるメッセージ生成を回避するため、HPOM ではしきい値の超過が特定の時間にわたって継続した場合のみ、メッセージを生成するように設定できます。

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アクションまたはオペレータ起動アクションを設定すると、即時に修復アクションを開始できます。また、既存の障害に対応するモニターや進行中の問題に対応するモニターが定義できます。これにより、予防的ツールと対応的ツールとしてモニターを使用できます。

モニター用のプログラムやユーティリティの組み込み

既存または新規のモニターリングプログラムまたはユーティリティを組み込み、上限または下限のしきい値を指定することができます。この場合 HPOM がモニターを開始するための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、定義済みのしきい値と比較します。

たとえば、UNIX の `who(1)` ユーティリティを統合すると、ログオンしているユーザーの人数を確認できます。また、`df(1M)` を統合すると、未使用のディスクブロック数を確認できます。スクリプトの結果は定義したしきい値と比較され、しきい値を超過していれば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、パフォーマンスが限界を超える前にオペレータに警告できます。このように、しきい値を予防的手段として使用すれば、障害がユーザーまで波及する前に修復アクションを開始することができます。

しきい値モニターポリシーの設定方法については、「しきい値モニターの組み込み」(267 ページ) 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、次の種類のモニターをサポートしています。

- **プログラムモニター**

  管理者が提供するモニタースクリプトとプログラムは、設定されたポーリング周期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、これらのスクリプトとプログラムが正常終了したかどうかを、戻り値を読み取ってチェックします。戻り値がゼロ以外であれば、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。

  モニター用のスクリプトやプログラムは、モニター対象オブジェクトの現在の値を収集します。この値は、`opcmon` アプリケーションプログラミングインタフェース (API) または HPOM のコマンドインタフェースを介してモニターエージェントに送られます。モニターエージェントは、この値を設定済みのしきい値と照合します。しきい値を超過している場合、モニターエージェントはメッセージを送信します。

  プログラムモニターは、Windows オブジェクトのモニターにも使用されます。詳細については、『HPOM 管理者リファレンスガイド』を参照してください。

  さらに、プログラムモニターは HPOM の組み込み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も使用されます。詳細については「パフォーマンスメトリックのモニター」(260 ページ) を参照してください。

- **MIB オブジェクトモニター**

  MIB オブジェクトは、`SNMP Get` リクエスト機能でモニターできます。モニターエージェントが戻り値を、設定済みのしきい値と照合してチェックします。

注記

デフォルトでは、コミュニティ `public` が SNMP 照会に使用されます。MIB オブジェクトが他のコミュニティに存在する場合は、MIB オブジェクトをモニターする HTTPS ベース管理対象ノード上では `ovconfchg` コマンドラインツールを使っ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コマンドおよび構文は次のとおりです。

```
ovconfchg -ns eaagt -set \
SNMP_COMMUNITY <community>
```

上記の <community> には、snmpd が設定されるコミュニティの名前を指定します。

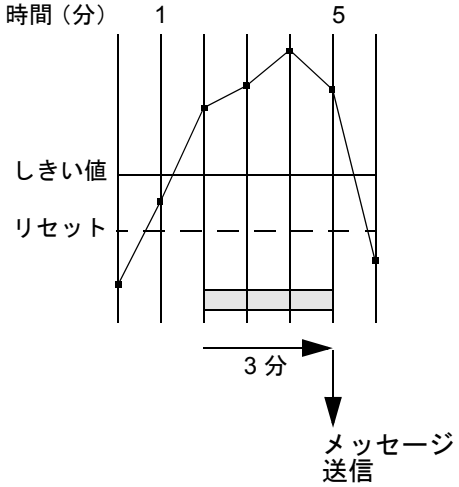
❏ **外部モニター**

外部モニターはプログラムモニターと同じですが、HPOM によって起動されることはありません。外部モニターを起動するには、opcmon 呼び出します。モニター対象の値がしきい値を最初に超過した時点でタイマーが起動されます。継続時間が指定されていない場合にはメッセージが生成されます。指定された時間内に opcmon が通知する値がすべてしきい値を超えていると、メッセージが生成されます。モニターされた値はその時間全体にわたってしきい値を超えていなくてもかまいませんが、各サンプルを収集するタイミングで超えていればメッセージが送信されます。

ポーリング周期によるプログラムや MIB オブジェクトのモニター

図 4-14 は、プログラムや MIB オブジェクトのモニターのポーリング周期が設定された後、メッセージが生成されるタイミングを示しています。モニター対象の値が最初にしきい値を超えた時点で、タイマーがカウントを開始します。モニター対象の値は各ポーリング周期で再チェックされ、しきい値を超えたままであればカウンターが上がり、設定済みの継続時間と比較されます。継続時間に到達すると、メッセージが生成されます。

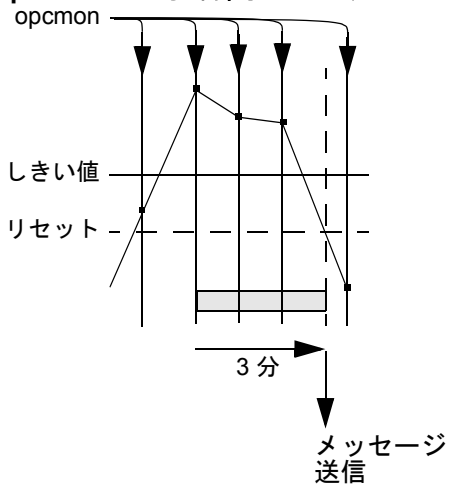
図 4-14　ポーリング周期によるプログラムや MIB のモニター



opcmon による外部オブジェクトのモニター

図 4-15 は、外部アプリケーションが 3 分間の間にしきい値に達したか、超過した後でメッセージが送信されることを示しています。

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 Agent の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。このコンポーネントが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た後、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。これらのデータを管理対象ノード上で直接抽出したり、エクスポート、表示、および収集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 Agent 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。

- **プラットフォーム共通メトリック**

  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や、CPU、ディスク、スワップ、およびメモリーの使用状況に関する情報を広く網羅した基本的なメトリックです。

- **標準メトリック**

  サポートされる各プラットフォームで利用できる追加のメトリックです。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。

- 標準の接続:

  `http://<management_server>:8081/ITO_DOC/<lang>/manuals/EmbedPerfAgent_Metrics.htm`

- セキュアな接続:

  `https://<management_server>:8444/ITO_DOC/<lang>/manuals/EmbedPerfAgent_Metrics.htm`

ここで、`<management_server>` には管理サーバーの完全修飾ホスト名、`<lang>` にはシステム言語 (たとえば、英語環境の場合 `C`) を指定します。

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` または `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>
```

この構文には次のパラメータが含まれます。

<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。

- 標準の接続:

  http://<management_server>:8081/ITO_DOC/<lang>/manuals/EmbedPerfAgent_Metrics.htm

- セキュアな接続:

  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、すべてのプラットフォーム共通メトリックと標準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最長 5 週間保存されます。この期間が経過すると、データベースの空きがなくなった時点で、もっとも古いデータ 1 週間分がロールアウトされ、データベースから削除されます。

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の詳細については、『HPOM 管理者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 Agent 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することをお勧めします。

データ収集を無効にしても、プロセス `coda` は実行を継続し、HPOM に制御された状態を維持します。その後、このプロセスは 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の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
```

データ収集を再び有効にする場合は、パラメータ `DISABLE_PROSPECTOR` を true に設定します。

モニターする変数の選択

モニターする変数の選択は、環境、現在使っているモニター、制御対象のパラメータによって変わります。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、次のような項目を確認します。

- ❑ 現在使用しているモニター
- ❑ 日 / 週 / 月ごとに使用するモニター
- ❑ 独自に作成したモニター
- ❑ 環境内のオペレーティングシステムやアプリケーションが使用しているモニター

さらに、モニター対象のパラメータも確認する必要があります。

たとえば、次のパラメータを確認します。

- ❏ モニター可能なパラメータ
- ❏ 重要なパラメータ
- ❏ しきい値が適用可能なパラメータ
- ❏ 限度を超える前に警告を発する必要のあるパラメータ

しきい値のタイプの選択

下限しきい値と上限しきい値のいずれかをモニター対象として選択できます。

- ❏ **下限しきい値**

  モニター対象の値が許容限度の下限値に達するかそれを下回ると、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) に対して下限のしきい値が使用できます。HPOM は、空きディスクブロックの数がしきい値を下回った時点でメッセージを生成します。

- ❏ **上限しきい値**

  モニター対象の値が許容限度の上限値に達するかそれを上回ると、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) に対して上限のしきい値が使用できます。HPOM は、ユーザー数が定義したしきい値を上回った時点で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のメッセージの生成ポリシーは、次の 3 つの中から選択します。

- ❏ リセットを伴うメッセージ生成
- ❏ リセットを伴わないメッセージ生成
- ❏ メッセージの継続的生成

注記

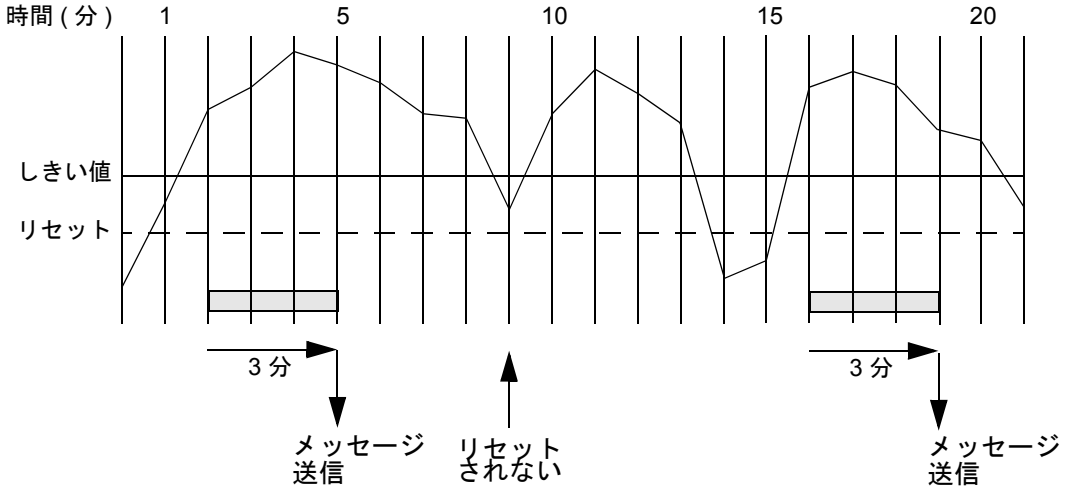
いずれの場合も、ポーリング時のモニター対象オブジェクトの値がしきい値と等しいか、しきい値の水準を超過していると、HPOM がしきい値の超過を検出します。

次の例は、これらの 3 種類の設定について違いを説明します。いずれの例でも、ポーリング周期は 1 分、継続時間は 3 分とします。

リセットを伴うメッセージ生成

図 4-16 は、リセットを伴う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超えているため、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、次にしきい値を超えた時点で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　リセットを伴うメッセージ生成

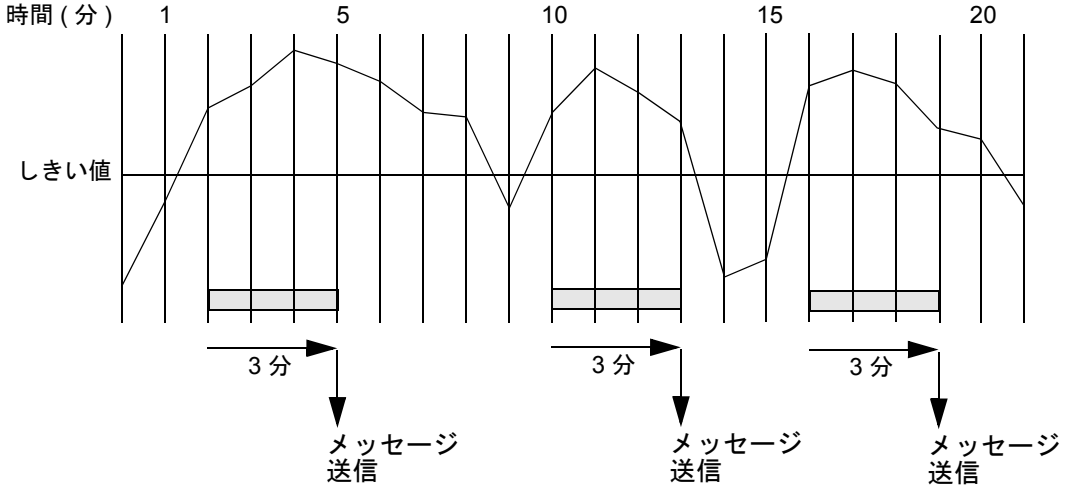


リセットを伴わないメッセージ生成

リセットを伴わないメッセージ生成とは、リセット専用の値を使わないメッセージ生成のことです。この場合、リセット値はしきい値と同じになります。

図 4-17 は、リセットを伴わない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超えているため、メッセージが送信されます。値がしきい値を下回ると、次にしきい値を超えた時点でタイマーがリセットされ、サイクルが再開されます。

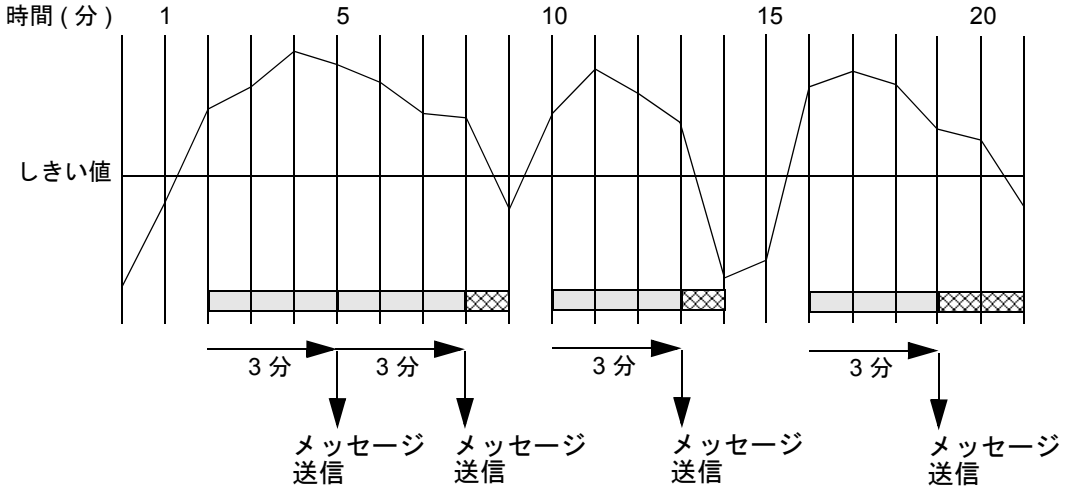
図 4-17　　リセットを伴わないメッセージ生成



メッセージの継続的生成

図 4-18 は、メッセージの継続的生成の一例を示しています。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。それから 3 分後にメッセージが送信され、ただちにタイマーがリセットされます。同様の処理が、その後も値がしきい値と同じ値になるかそれを下回るまで継続されます。モニター対象の値が再度しきい値を超えると、タイマーが起動され、サイクルが再開されます。

図 4-18　　メッセージの継続的生成



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 ではしきい値の超過が特定の時間継続した場合にのみ、メッセージが生成されるように設定できます。メッセージが生成されるためには、指定した時間の間、値が測定されるたびにしきい値を超えている必要があります。値は、ポリシーのポーリング周期の倍数で指定します。

たとえば、ポーリング周期が 2分間 (2 m) の場合、短期間のピークを 4 分間 (4m)、6 分間 (6m)、8 分間 (8m)、10 分間 (10m) のように設定します。この時間を 0 に設定するか、または指定しない場合、HP Operations によってしきい値の超過が検出されると、直ちにアラームが生成されます。

しきい値モニターの組み込み

しきい値モニターは、ログファイルを定義する場合と同じように、ポリシーを用いて定義できます。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組み込み

新しいしきい値モニターは次の手順で組み込みます。

1. **配布するしきい値モニターデータを準備します。**

   配布予定のインストルメンテーションデータは、HP Operations 管理サーバー上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、各管理サーバー上の、モニターを配布する各管理対象ノードプラットフォーム固有のディレクトリ内に、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またはスクリプトは、管理サーバー上の次の場所に配置されます。

```
/var/opt/OV/share/databases/OpC/mgd_node/customer/hp/\
ipf32/hpux1100/monitor
```

すべての配布方法、関連する管理タスク (カテゴリ管理を含めて)、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 管理者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内にモニタープログラムまたはスクリプトを (データの配布先となる各管理対象ノードプラットフォームに) 適切に配置します。このようなカテゴリがない場合は、これを作成し、ポリシーまたは管理対象ノード、あるいはその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。**

   これを行うには、`opcragt` コマンドラインユーティリティを使用します (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。**

opcpolicy コマンドラインツールを使用して、しきい値モニターポリシーをアップロードします。しきい値ポリシー本体の正しい構文の詳細については、付録 A「ポリシー本体の構文」(355 ページ) を参照してください。各ポリシーではモニターを定義します。これには、しきい値を超過したときに起動される自動アクションまたはオペレータ起動アクションが含まれます。

注記

しきい値モニターを配布する方法としてカテゴリベースの方法を選択した場合は、適切なカテゴリがポリシーに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に条件を設定します。**

ポリシー本体の 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 セクションを使用して、さらにメッセージをフィルター処理することができます。ポリシー本体の構文については、付録 A「ポリシー本体の構文」(355 ページ) を参照してください。

注記

モニターに複数の条件を設定する場合には、条件の順序に配慮してください。

しきい値の大きさに基づいて条件を並べてください。

- **上限しきい値のタイプ**

  しきい値がもっとも高い条件をリストの先頭、もっとも低い条件を末尾に配置します。

- **下限しきい値のタイプ**

  しきい値がもっとも低い条件をリストの先頭、もっとも高い条件を末尾に配置します。

条件に順序を設定すると、状態ベースのブラウザ設定で、同じモニターから前回受信したメッセージを自動受諾できます。状態ベースのブラウザについては、「状態ベースのブラウザ」(232 ページ) を参照してください。

しきい値モニターの設定

しきい値モニターポリシーは、ADVMONITOR ポリシーのポリシー本体を編集することで設定できます。ポリシー本体の構文についての詳細は、付録 A「ポリシー本体の構文」(355 ページ) を参照してください。

例 4-2 **モニターしきい値ポリシー本体の例**

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のスクリプト fs_util_mon.sh を実行しています。このスクリプトは、opcmon コマンドラインツールを呼び出して、計算結果の値を (スクリプトへのパラメータとして) extra_util という名前のモニターエージェントに渡します。

ファイルシステムの使用率が設定した使用率 (THRESHOLD) を上回る場合 (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 RESET キーワードで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、注意域に設定され、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。設定した条件に一致するもの以外、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 -k
 /extra" ANNOTATE
```

デフォルトのしきい値モニター

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、HP Operations Agent のドキュメントを参照してください。

高度なモニターの条件の設定

しきい値モニターポリシーに条件を設定すれば、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することが可能になります。

しきい値モニターに条件を設定する手順は次のとおりです。

1. `opcmon(1)` コマンドを `-object` オプション付きで実行し、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渡します。

   `-option` はモニターエージェントに追加情報を渡すオプションです。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したりすることができます。

   HPOM は、この名前を高度なモニターポリシー本体で `OBJECT` キーワードで指定されたパターンと照合します。

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います。

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

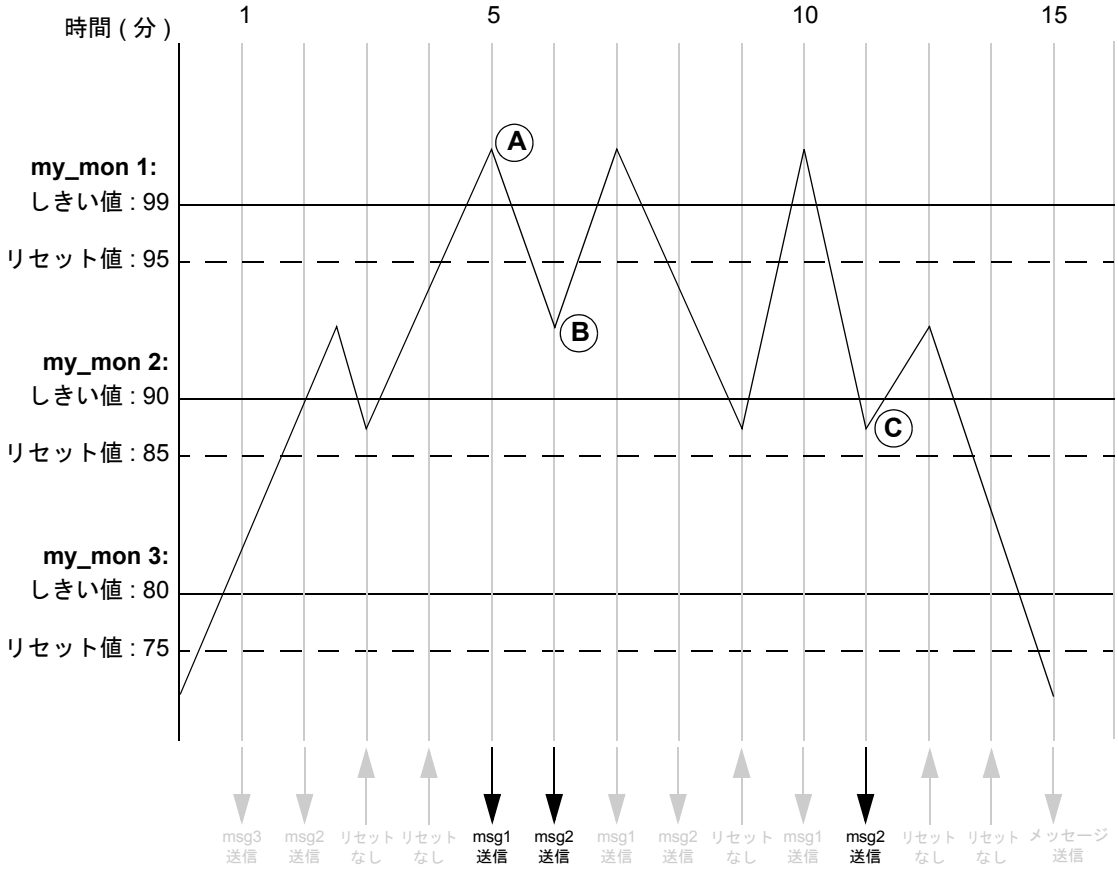
各種ファイルシステムのディスクの使用状況をモニターする方法については、「しきい値モニターの条件の例」(273 ページ) を参照してください。

複数の条件によるしきい値のモニター

1 つのポリシーの中で 1 つのモニター対象オブジェクトに対して、それぞれ異なるしきい値とリセット値を持つ条件を複数設定すると、モニター対象の値がいずれかの条件のモニター範囲に該当するたびに、メッセージが送信されるようになります。

272 ページの図 4-19 の例は、3 つの条件が設定されている場合を示しています。これらの各条件には、それぞれ異なる上限しきい値とリセット値があります。

図 4-19　条件が複数存在する場合のリセットを伴うメッセージ生成



5 回目のポーリング (5 分) で、値が条件 `my_mon 1` (しきい値 = 99) のしきい値を超過し、メッセージが送信されます **(A)**。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。値は条件 `my_mon 2` (しきい値 = 90) のしきい値を超えているため、別のメッセージが送信されます **(B)**。

つまり、値はこの条件のリセット値を下回っていなくても、条件のモニター範囲に達するとメッセージが生成されます。

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)**。このメッセージの元のメッセージテキストには、リセット値には達せず、しきい値のみを超えたために、「リセット値をまだ超えています」と示されます。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いるため、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対して多くのメッセージを受け取ります。ブラウザに表示されるメッセージ数を選らすには、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、「状態ベースのブラウザ」(232 ページ) を参照してください。

しきい値モニターの条件の例

次の例は、しきい値モニターポリシー disk_util のしきい値モニター条件を使って、/var および / ファイルシステムのディスクの空き容量をモニターする方法を示しています。この例は、各ファイルシステムのディスク使用量をチェックして通知するシェルスクリプトが、すで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

リセット値: 85

期間: 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:	/var ファイルシステムのディスク使用量 (<$VALUE>) が (<$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

リセット値: 90

期間: 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ディスク使用量 (<$VALUE>) が (<$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 トラップを送信するメッセージインタフェースです。

デフォルトでのトラップおよびイベントの捕捉

HPOM は、デフォルトでは 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 管理サーバーで動作している opctrapi デーモンにトラップを送信するあらゆるアプリケーションから捕捉。

- **管理対象ノードで**

  トラップデーモン (ovtrapd) が動作しているすべての管理対象ノード上で捕捉。

- **管理対象ノードのプラットフォームで**

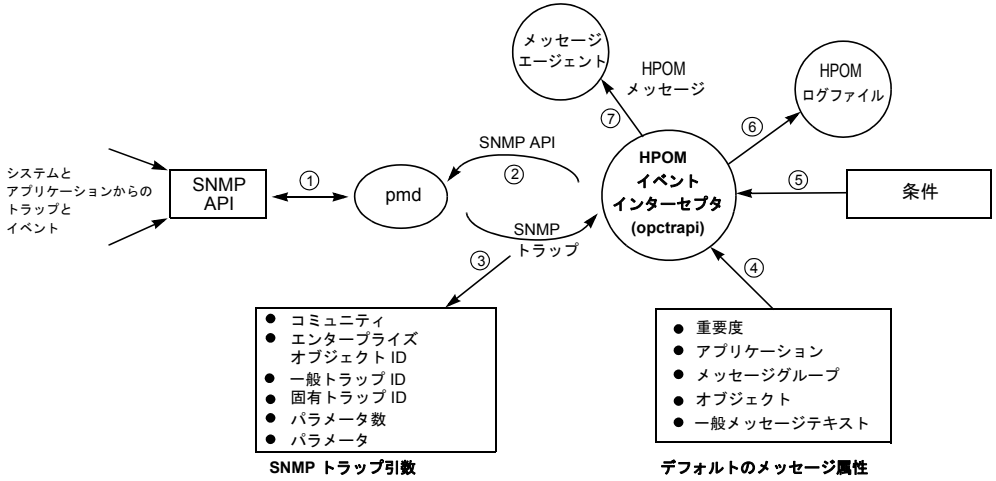
  選択された管理対象ノードプラットフォーム上のポートへのダイレクトアクセスモードで捕捉。opctrapi が対応している管理対象ノードのプラットフォームのリストについては、『HPOM 管理者リファレンスガイド』を参照してください。

  管理対象ノードで直接イベントを捕捉すれば、メッセージをローカルで処理できるため、パフォーマンスが向上します。たとえば、メッセージを管理サーバーに転送することなく、管理対象ノードやサブネット内で自動アクションを直接起動し、実行することができます。

ブラウザウィンドウ内での SNMP イベントの捕捉

図 4-20 は、HPOM のイベントインターセプタが SNMP イベントを収集し、フィルター処理とフォーマット変更を施して、ブラウザウィンドウに表示する過程を示しています。

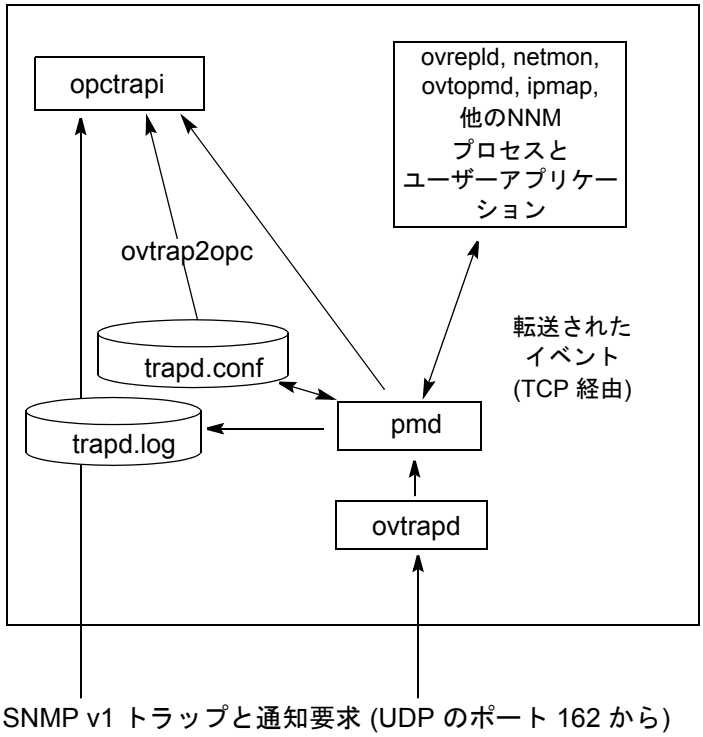
図 4-20　NNM をインストールした環境での SNMP イベントインターセプタの処理



SNMP トラップと CMIP イベントの転送

図 4-21 は、opctrapi と HPOM プロセスとの関係を示しています。SNMP トラップと CMIP イベントは、HPOM プロセスによって HPOM に転送されます。

図 4-21　HPOM 内の SNMP イベントシステム



ovtrapd バックグラウンドプロセスはポート 162 で SNMP トラップと CMIP イベントを受信します。このプロセスは受信したトラップとイベントをバッファーに格納し、Postmaster プロセス (pmd) に渡します。pmd プロセスは、ovtrapd から受信したイベントをサブシステム (opctrapi や trapd.conf ファイルなど) にルーティングし、HPOM メッセージストリームに格納します。

trapd.conf には SNMP トラップ (SNMP エージェントが生成) とイベント (pmd で登録したアプリケーションが生成) を処理するための定義が含まれています。これらの定義は ovtrap2opc ユーティリティを使って、HPOM のメッセージ条件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。

管理対象ノードのプラットフォームによっては、HPOM イベントインターセプタがポート 162 に直接アクセスして SNMP トラップを捕捉できる場合もあります。詳細については、『HPOM 管理者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。そのような場合に、複数の管理対象ノードが同じ管理サーバーにトラップを転送すると、重複するメッセージが生成されてしまいます。

この問題を回避するためのガイドラインを次に示します。

❏ **SNMP の送信先や NNM 収集ステーションを 1 つに限定する**

各 SNMP デバイスの SNMP 送信先を 1 つに限定するか、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 台に限定します (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 SNMP 送信先システムは、次のファイルで設定します。

```
/etc/SnmpAgent.d/snmpd.conf
```

設定の構文は次のとおりです。

```
trap_dest:<nodename>
```

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 収集ステーションで HP Operations Agent を動作させる**

HP Operations Agent (および HPOM イベントインターセプタ) を、すべての NNM 収集ステーションで動作させます。

SNMP トラップポリシーの追加

SNMP トラップポリシーを設定する際は、HPOM イベントインターセプタがサポートされている HP Operations 管理サーバーまたは管理対象ノードに、トラップポリシーを任意の数だけ割り当てることができます。

トラップポリシーは、SNMP ポリシーのポリシー本体を編集することで設定できます。ポリシー本体の構文の詳細については、付録 A「ポリシー本体の構文」(355 ページ) 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本体の例**

この例は、Cisco 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一般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> と <$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になります)。

```
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、ワークリストファイルに構文エラーが検出されると、HP Data Protector は次のような SNMP トラップを発行します。

```
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"
```

この場合、SNMP トラップポリシーには、次のように条件を定義する必要があります。

ノード

```
doghouse
```

エンタープライズ ID

1.3.6.1.4.11.2.3.2

一般トラップ ID

6

固有トラップ 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:
[Error](Worklist Syntax)Can't
open worklist
'/etc/omniback/work'
Status:Critical

トラップ固有のデータ:

危険域

属性設定

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:

Error in HP Data
Protector:<text>

HPOM 内部エラーメッセージのフィルター処理

HPOM の内部エラーメッセージは、フィルター処理を施して内部メッセージストリームインタフェース(MSI) から取り込んだり、除外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

管理サーバー上では、`ovconfchg` コマンドラインツールを使います。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、管理サーバーのリソースグループの名前です。

管理対象ノード

HTTPS ベース管理対象ノードでは、`ovconfchg` コマンドラインツールを使います。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 HPOM 内部エラーメッセージ用の条件を少なくとも 1 つ設定してください (メッセージグループ `OpC` を使用します)。さらに、ポリシー本体で `SUPP_DUPL_IDENT_OUTPUT_MSG` キーワードを設定します。

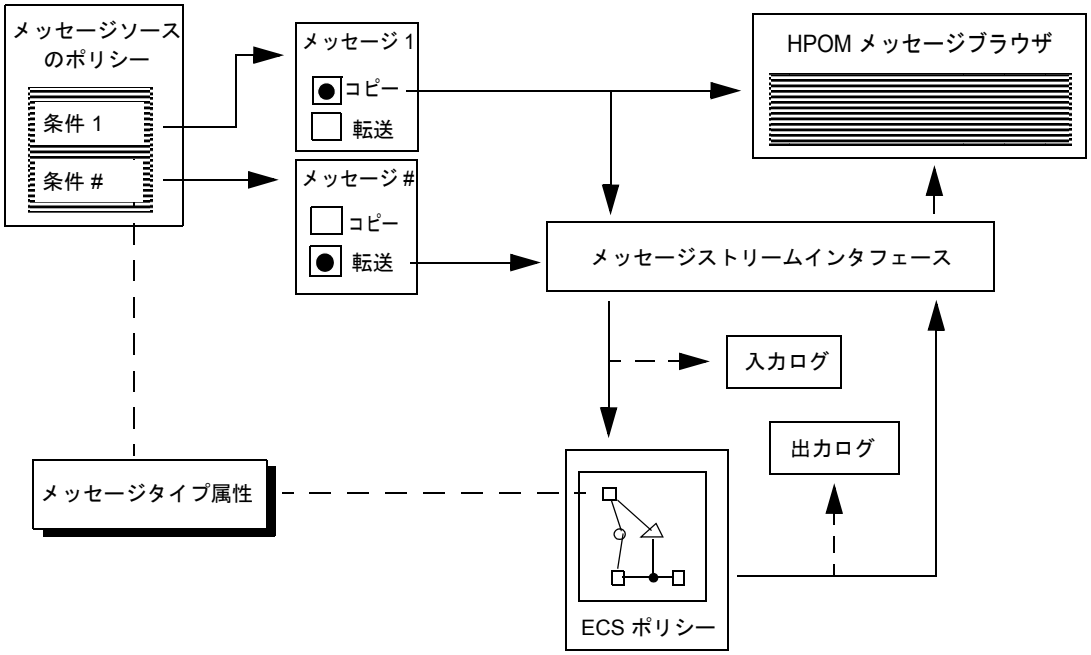
HPOM のイベント相関処理

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して表示され、処理されます。

イベント相関処理の仕組み

283 ページの図 4-22 は、イベント相関処理ポリシーが HPOM 内でどのように機能するかを示しています。HPOM のメッセージソースポリシーでは、メッセージを生成する条件を指定できます。さらに、生成されたメッセージ自体をメッセージストリームインタフェース (MSI) に転送するか、あるいはメッセージを MSI にコピーするかを選択することもできます。生成されたメッセージを MSI からイベント相関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で特に役立ちます。

図 4-22 HPOM でのイベント相関処理の論理フロー



イベント相関処理ポリシーでは、メッセージが経由するイベント相関処理サーキットが決定されます。この決定は、メッセージ条件で指定された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] フィールドで指定されたメッセージ属性との照合に基づきます。

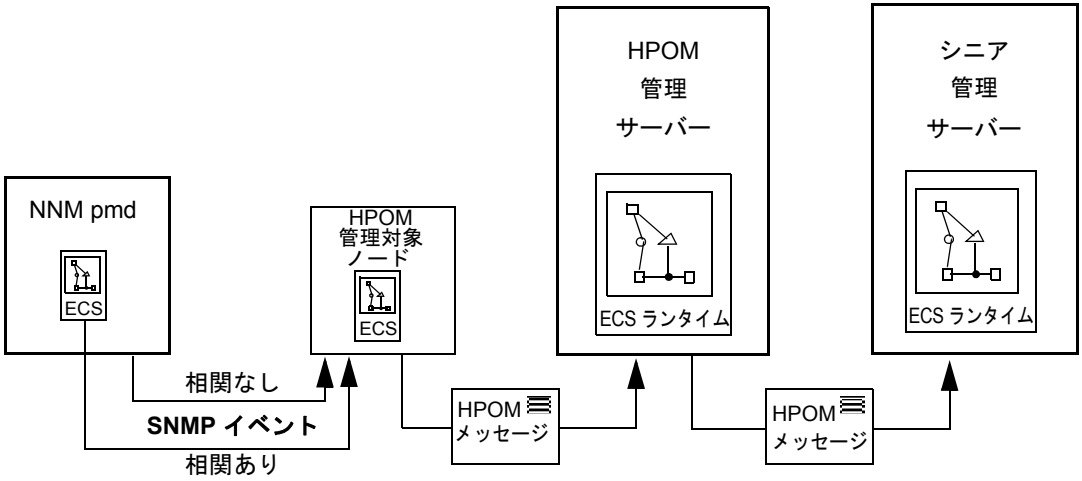
HPOM でイベント相関処理を設定する方法の詳細については、『HPOM 管理者リファレンスガイド』を参照してください。

メッセージの相関処理の実行場所

HPOM 環境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は重要になります。標準的な環境では、管理対象ノードまたは管理サーバー、あるいはその両方でメッセージを相関処理するように設定できます。しかし、HPOM フレキシブル管理設定を使用する大規模な環境では、さらに選択肢は広がります。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るため、階層サーバーの各レベル間の関係を考慮する必要があります。また、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、HPOM イベントインターセプタによって捕捉される SNMP 関連メッセージの数が大幅に削減されます。選択できる相関処理の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、早い段階で相関処理を実行すると、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数も少なくなるので有益です。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考慮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用してイベントを相関処理することで、HPOM によって捕捉されるイベント数を大幅に削減することができます。

- **管理対象ノード上**

  管理対象ノード上でメッセージを相関処理することで、管理サーバーに渡されるメッセージの数を削減できます。その結果、管理サーバー上の負荷と、ネットワークトラフィックの全体的な量が削減されます。

- **管理サーバー上**

  HP Operations 管理サーバー上でメッセージを相関処理することで、各管理対象ノードからの類似または関連するメッセージをフィルター処理できます。

- **フレキシブル管理環境内**

  HPOM 環境内での管理対象ノードと管理サーバー間の関係は、管理階層内では下位レベルと上位レベルの管理サーバー間の関係に該当します。

ソースが異なるメッセージの相関処理

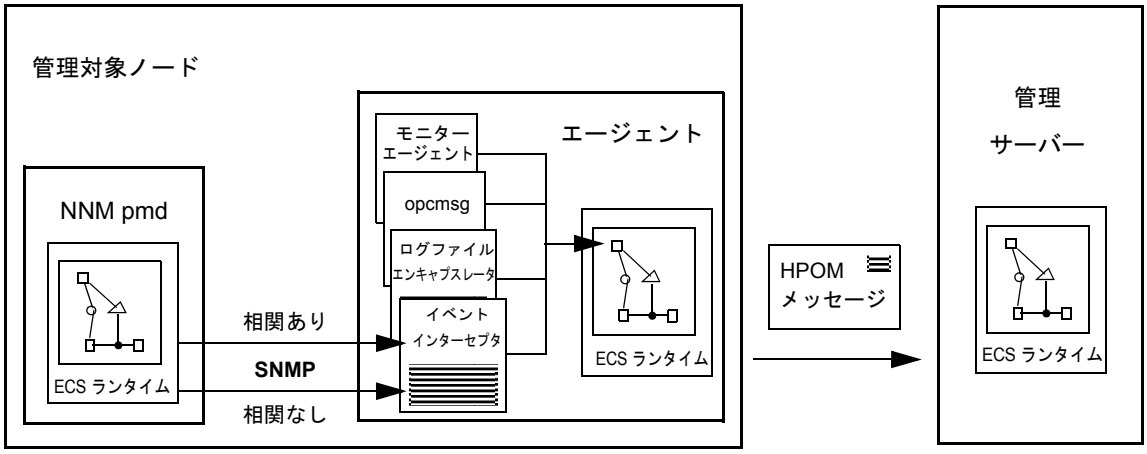
相関処理するメッセージのソースを、特定の種類に限定する必要はありません。HPOM 内の種類が異なるソースからのメッセージに対する相関処理には、いくつかの利点があります。

次のソースからのメッセージに相関処理を実行できます。

- 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 の postmaster デーモン (pmd) によって生成された SNMP イベントストリームを相関処理の有無にかかわらず捕捉し、必要に応じて HPOM メッセージを生成します。こうして得られたメッセージは、ログファイルなど他の HPOM ソースから生成されたメッセージと共に、HP Operations Agent の相関処理ポリシーで処理されます。

HPOM に到達する前の NNM でのイベント相関処理

HP Operations Agent の全体的な負荷を削減し、HPOM が相関処理を行いやすくするには、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用して相関処理を行います。

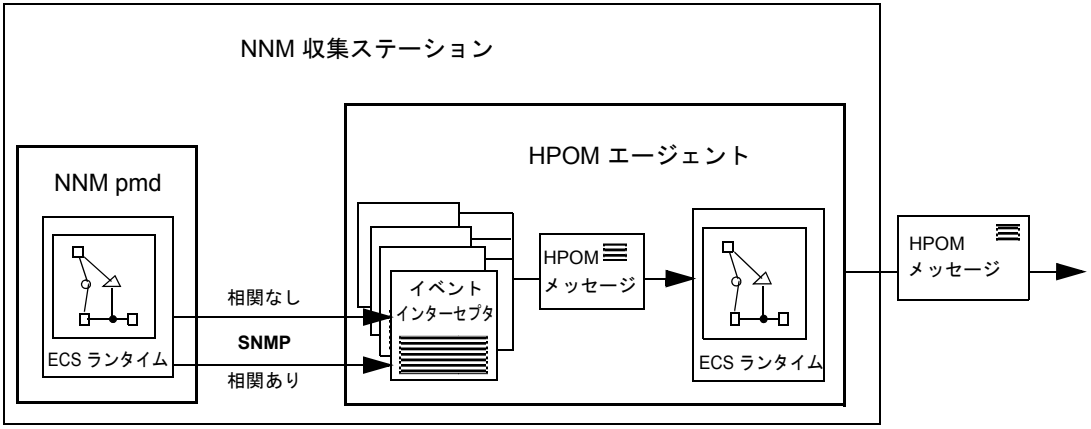
たとえば、ルーターの応答がない場合に生成されるイベントを処理するために NNM のサーキットを設定できます。NNM 収集ステーション上の HPOM イベントインターセプタが確実に相関処理されたイベントのみを受け取る

ようにすると、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 管理対象ノード上のイベント相関処理ポリシーによってさらに相関処理することもあります。

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しており、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 のサーキットで受諾または削除されたイベントは、HPOM で自動的に受諾されます。さらに、相関処理によって除外されたイベントに関連する各メッセージには自動的に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

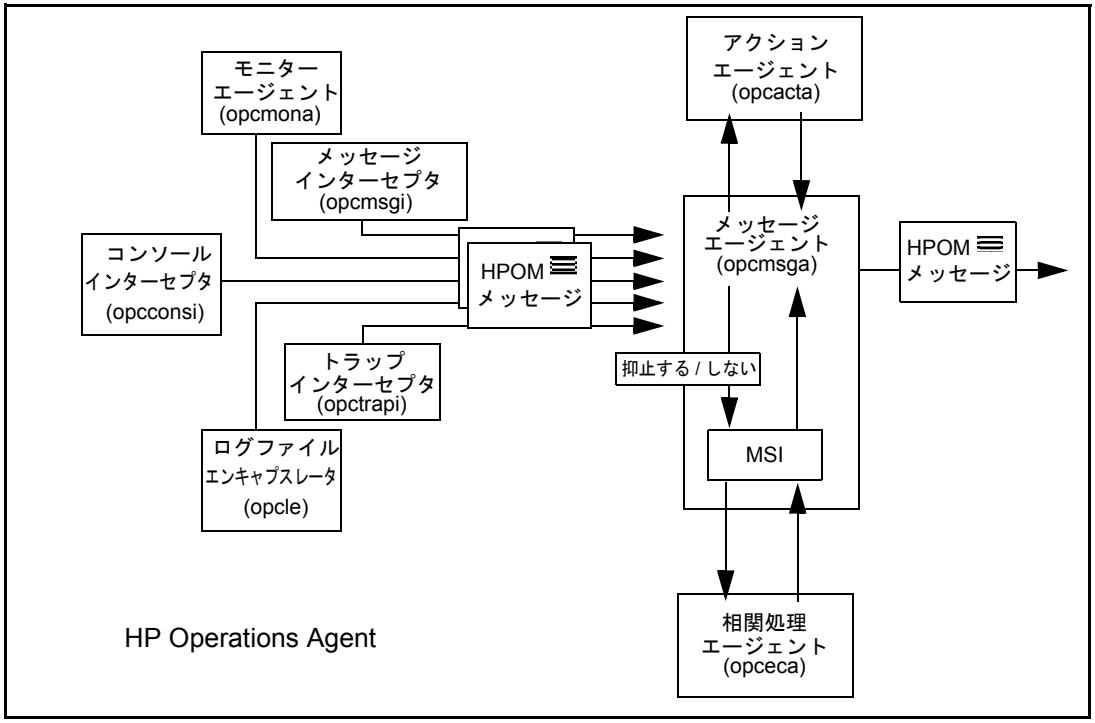


管理対象ノードでのメッセージの相関処理

HP Operations Agent を使って管理対象ノード上でイベント相関処理を行えば、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が大幅に抑制されます。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 負荷が軽減され、より効率的に他の問題に対処できるようになります。

288 ページの図 4-26 は、管理対象ノード上でどのようにメッセージが生成され、どのようにメッセージが処理されるか、およびエージェント MSI へのメッセージ出力をオン / オフすることによって、イベント相関処理エージェント (opceca) へのメッセージの流れ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フロー



opceca プロセスはエージェント MSI に接続して、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にアクセスできるようにします。メッセージは相関処理され、HPOM メッセージエージェントに送り返されます。opceca によって作成または変更されたメッセージは、メッセージソース MSI:opceca を使ってメッセージブラウザに表示されます。メッセージが相関処理サーキットに指定されたルールおよび条件に一致しない場合、メッセージの元のメッセージソースはそのまま維持されます。

ECS 設定が管理対象ノード上に存在する場合、opc(r)agt -status コマンドを使用して opceca ステータスをチェックできます。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る場合、opceca プロセスは開始されます。イベント相関処理ポリシーの設定が管理対象ノード上に存在しない場合、opceca プロセスは停止されます。

イベント相関処理ポリシーは、他の HPOM ポリシーと同じように管理対象ノードに割り当てられます。

注記

実行している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)、エンジンはすべての開いている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、相関処理サーキットをロードしてから再起動します。メッセージエージェントは、転送されたメッセージを相関処理エンジンに送り返しません。

注記

自動アクションが相関処理プロセス内で破棄されたメッセージに関連づけられており、ポリシー本体に `MPI_IMMEDIATE_LOCAL_ACTIONS` キーワードが指定されていない場合、その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に設定されており、MSI への出力が有効で、ポリシー本体に `MPI_SV_DIVERT_MSG` キーワードが指定されている場合にのみ使用できます。

新しいアクションが必要な場合、相関処理プロセスの実行中に新しいメッセージ、または変更した既存のメッセージにそのアクションを指定して、関連付ける必要があります。

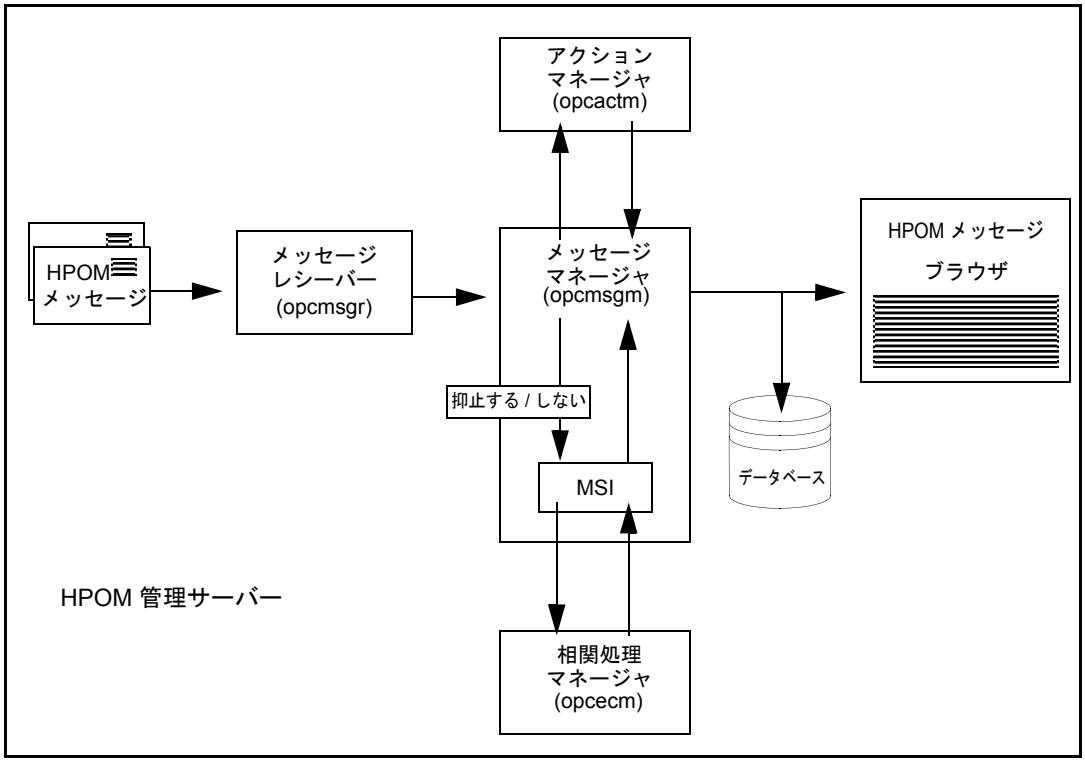
管理サーバーでのメッセージの相関処理

HP Operations 管理サーバーでメッセージの相関処理を行えば、同じ問題に関する (複数のノードから着信された) 重複メッセージや類似メッセージを除外し、Java GUI メッセージブラウザに表示されるメッセージを絞り込むことができます。

冗長なメッセージを削減することは、分散しているクライアントサーバーアプリケーションがあり、プリンターやバックアップデバイス、NFS ファイルサーバーなどの共有ネットワークデバイスを装備した環境において特に有益です。たとえば、データベースサーバーが一時的に利用できなくなった場合に、データベースサーバーとの連絡が絶たれた管理対象ノードからの類似のメッセージを除去することができます。

図 4-27 は、管理サーバー上のメッセージフローを示しています。図中に示すように、相関処理マネージャ (opcecm) へのメッセージフローは、サーバー MSI へのメッセージ出力のオン / オフを切り換えることによって制御できます。

図 4-27 HP Operations 管理サーバー上のメッセージフロー



opcecm プロセスはサーバー MSI に接続して、メッセージストリームからのメッセージにアクセスできるようにします。メッセージは相関処理され、HPOM メッセージマネージャに再度書き込まれます。相関処理プロセスによって作成または変更されたメッセージは、メッセージソース MSI:opcecm を使ってメッセージブラウザに表示されます。メッセージが相関処理サーキットに指定されたルールおよび条件に一致しない場合、メッセージの元のメッセージソースはそのまま維持されます。

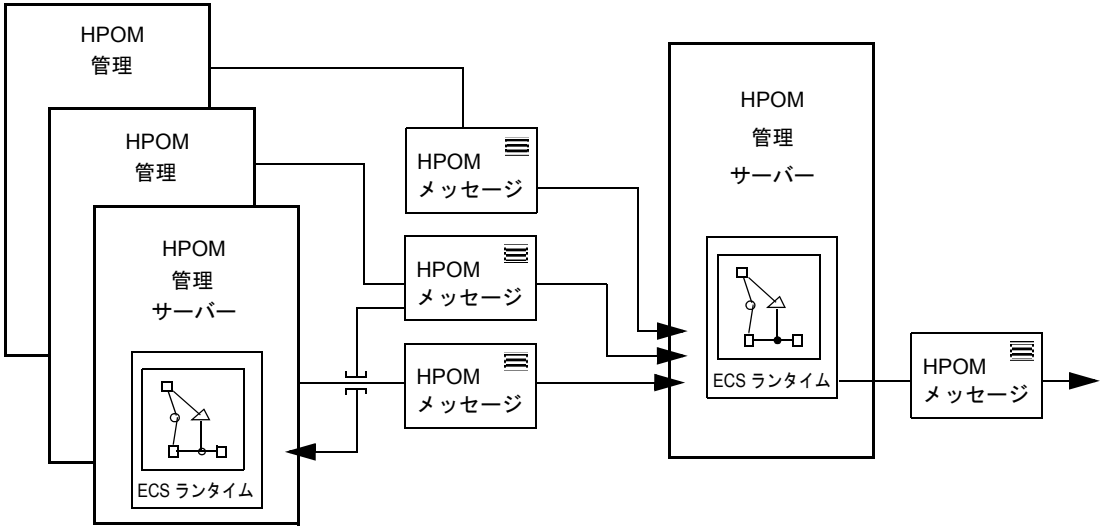
ECS 設定が管理サーバー上に存在する場合、opcsv -status コマンドを使用して opcecm ステータスをチェックできます。イベント相関処理ポリシーが管理サーバーに配布される場合、opcecm プロセスは開始され、イベント相関処理ポリシーの設定が管理サーバー上に存在しない場合、このプロセスは停止されます。

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する大規模な企業環境では、メッセージ相関処理は管理階層内のさまざまなレベル間の関係を考慮した複雑なものになります。HPOM 環境内での管理対象ノードと管理サーバー間の関係は、管理階層内では下位レベルと上位レベルの管理サーバー間の関係に該当します。したがって、管理サーバーは管理対象ノードから受信したメッセージに相関処理を行って、自身が属する上位の管理サーバーに相関処理済みのストリームを送信できるほか、相関処理を行わずに送信することもできます。後者の場合、相関処理はメッセージストリームを受信した上位の管理サーバーで実行されます。

フレキシブル管理階層においてこの種のメッセージ相関処理を行えるようにするには、管理サーバー相関処理ポリシーを HP Operations 管理サーバーに割り当て、配布します。ポリシーの割り当てと配布の方法については、「ポリシーの割り当て」(187 ページ) を参照してください。

図 4-28　　HPOM フレキシブル管理と相関処理



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を変更するパラメータが含まれます。これにより、相関処理サーキットの動作を再コンパイルせずに変更できます。たとえば、さまざまな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。相関処理サーキットを再コンパイルせずにその他の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一覧を相関処理サーキットの外部に維持できます。

相関処理の決定を支援したり、相関処理サーキットからの情報出力を改善するために、外部情報が必要になる場合もあります。たとえば、エラーメッセージを検出したときに外部データベースに対してクエリを実行して、サービスレベル契約 (SLA) 情報を取得できます。SLA に関する詳細情報は、メッセージブラウザに表示される前にメッセージに追加できます。

相関処理サーキットから外部データにアクセスするには、次の 2 つの方法があります。

- 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 のデータストアとファクトストアを使用すると、相関処理の環境的な側面を、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、ある 1 つの HPOM 管理対象ノードに対して一般的な相関処理サーキットを設定し、データストアを使用して同じポリシーをそれ以外の管理対象ノードに適用します。

データストアは、情報のキーと値のペアを保持するために使用できます。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に関する詳細情報 (間隔、しきい値、その他の制約など) が変わる可能性があることがわかっている場合、データストアには、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一般的な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る) の名前をデータストア内に保存することで各種の HPOM 管理対象ノードで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、組織内の階層、組織間またはサービスプロバイダー間の関係などを表します。たとえば、3 つのアプリケーションサーバー A、B、C が同じデータベースサーバー `DBserver01` に接続され、4 つめのアプリケーションが別のデータベースサーバー `DBserver02` に接続されているとします。これら

の関係を定義するには、ファクトストアを使用します。何らかの理由により DBserver01 が応答しない場合、ファクトストア内の情報を使用して、このデータベースサーバーからのメッセージと、DBserver01 との接続が失われたこと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。データストア用のファイルには ds の拡張子が付き、ファクトストア用のファイルには fs 拡張子が付いています。ファクトストアファイルとデータストアファイルは、EC ポリシーと共に配布されません。これらのファイルは、EC ポリシーを配布する前に手動で作成し、次の場所にコピーする必要があります。

- 管理サーバー上
  /var/opt/OV/shared/server/datafiles/policies/ec
- 管理対象ノード上 (UNIX)
  /var/opt/OV/conf/eaagt
- 管理対象ノード上 (Windows)
  C:\Program Files\HP BTO Software\data\conf\eaagt

注記

コンポーザーを使用する場合、ファクトストアファイルの作成、配布、インストールを行うには ovocomposer スクリプトを使用できます。

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ファイルと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とデータストアがあります。グローバルファクトストアとデータストアは、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とデータストアは、単一の相関処理サーキットからしかアクセスできません。

- 固有データストアとファクトストア

  各相関処理サーキットには、コンパイル済みの ECS サーキットファイル (.eco) が関連付けられています。コンパイル済みのサーキットファイル名は、相関処理サーキットが作成または変更されたときに自動的に生成され、<id>.eco という形式になります (たとえば、EAAAa03015.eco)。

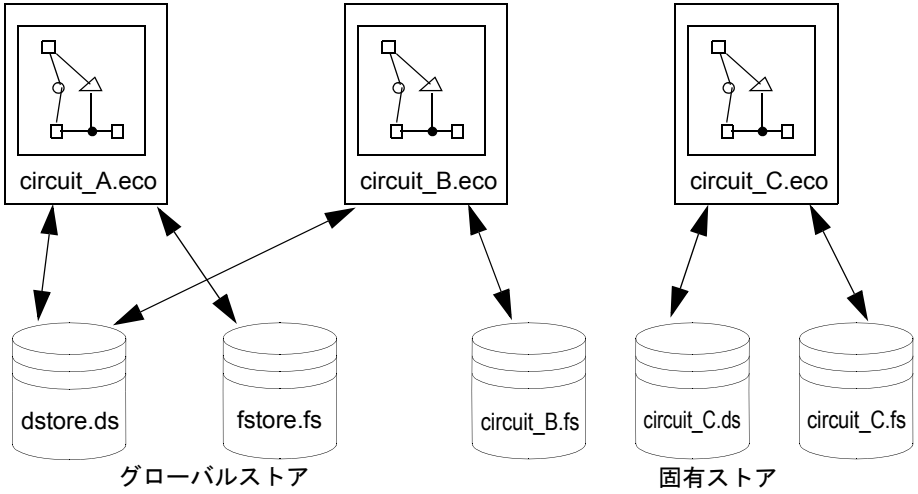
相関処理サーキットが管理対象ノードまたは管理サーバーに配布されたとき、相関処理サーキットは指定したディレクトリに、コンパイル済みのサーキットファイルと同じ名前で、適切な拡張子 (ファクトストアは fs、データストアは ds) を持つファクトストアまたはデータストアが存在することを確認します。これらのファイルが存在しない場合、グローバルファクトストアまたはデータストアが使用されます。

- グローバルデータストアとファクトストア

  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対して固有ファクトストアが存在しない場合、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対して固有データストアが存在しない場合、グローバルデータストアがロードされます。

294 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と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 のデータストアとファクトストア



ファクトストアとデータストアの更新

HPOM を再起動したり、または管理対象ノードまたは管理サーバーに新しい、または変更したイベント相関処理ポリシーを配布すると、ファクトストアおよびデータストアファイルが再ロードされます。また、次の場所から ecsmgr ユーティリティを使用して、個別にファクトストアおよび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。

- 管理サーバー上

  `/opt/OV/bin/OpC/`

- 管理対象ノード上 (UNIX)

  `/opt/OV/bin/OpC/utils/`

- 管理対象ノード上 (Windows)

  `\usr\OV\bin\OpC\install\`

`ecsmgr` を使用する場合は、管理対象ノードの ECS エンジンまたは管理サーバーの ECS エンジンのどちら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して、イベント相関処理ポリシーを新しいファクトストアまたはデータストアで更新できます。

- データストア

  ```
  # ecsmgr -i <instance> -data_update <datastore_name> \
  <filename>
  ```

  例:

  ```
  # ecsmgr -i 12 -data_update DatabaseDown \
  /var/opt/OV/conf/eeagt/DatabaseDown.ds
  ```

- ファクトストア

  ```
  # ecsmgr -i <instance> -fact_update <factstore_name> \
  <filename>
  ```

  例:

  ```
  # 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は変更しません。

ヒント

ファクトデータまたはデータストアファイル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ることがないように小さいファイルを使用して増分更新を行います。

ecsmgr ユーティリティの詳細については、ecsmgr(1M) 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

ファクトストアおよび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 ノード上への配布を部分的に自動化することができます。

UNIX ノードへのファクトストアおよびデータストアの配布を自動化するには、管理サーバー上で次の手順を実行します。

1. ファクトストアおよびデータストアファイルを次のディレクトリに作成します。

   ```
   /var/opt/OV/share/databases/OpC/mgd_node/customer/\
   <arch>/cmds
   ```

注記

HPOM 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 や 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した後、ファクトストアおよびデータストアファイルは /var/opt/OV/bin/OpC/cmds ディレクトリにインストールされます。

2. ファクトストアおよびデータストアファイルを次のディレクトリの /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
   ```

ファクトストアおよびデータストアを配布する際は、管理対象ノードにコマンドを配布し、HPOM ブロードキャストコマンドメカニズムを使用してスクリプトを実行できます。

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、ファクトストアまたはデータストアより ECS 注釈ノード機能を使用する方が適しています。注釈メカニズムについての詳細は、「注釈メカニズム」(297 ページ) を参照してください。

注釈メカニズム

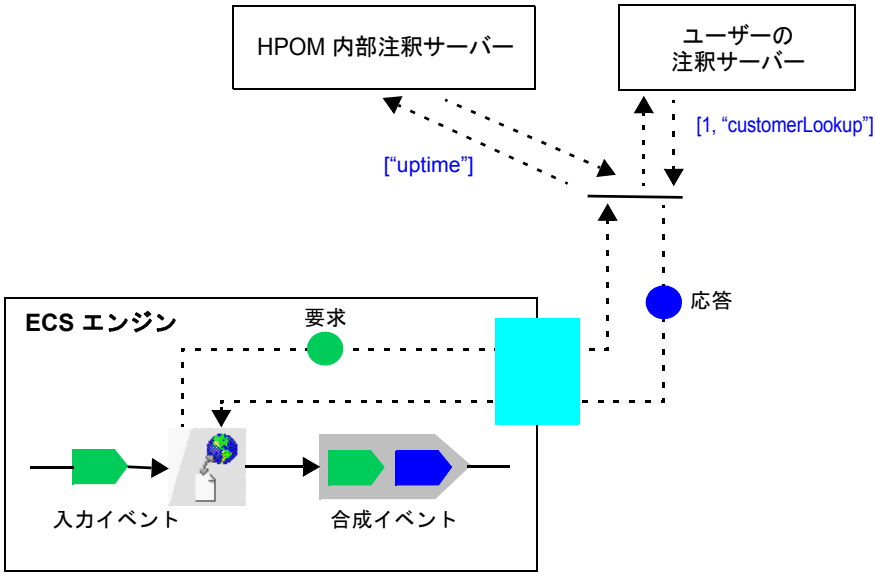
ECS 注釈ノードメカニズムを使用すると、相関処理サーキットから外部の情報ソースにアクセスできます。定期的に変更される可能性がある情報にアクセスする場合、一般的にファクトストアまたはデータストアよりむしろ注釈ノードが使用されます。

注釈ノードは、ECS エンジンの外側にある外部プロセスを呼び出します。この外部プロセスを注釈サーバーと呼びます。注釈サーバーは適切な処理を実行して、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が使用できます。

- 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



注釈サーバーへの要求の送信には、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、リストの最初の要素が文字列である場合、HPOM の内部注釈サーバーは要求を捕捉して、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が文字列以外のデータタイプ (整数など) である場合、HPOM 内部注釈サーバーは要求を捕捉しません。代わりに、ユーザー作成の注釈サーバーで要求を利用できます。

デフォルトの動作を変更して、特定の名前の注釈ノードからの要求のみを受信するように各注釈サーバーを登録できます。これを行うには、ovconfchg コマンドラインツールを使用して次の変数を設定します。

- 管理サーバー上: ECM_ANNO_NODE
- 管理対象ノード上: ECA_ANNO_NODE

ECM_ANNO_NODE、ECA_ANNO_NODE、またはその両方の変数を設定すると、HPOM 内部注釈サーバーは指定した名前のノードからの注釈ノードのみを処理します。変数の形式は次のとおりです。

```
ECM_ANNO_NODE <name1>[,<name2>...]
```

たとえば、OVOEXE という名前の注釈ノードからの注釈要求を処理するように内部注釈サーバーを設定するには、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を持つ複数の注釈ノードを使用するには、名前の競合を避けるために各注釈ノードをそれぞれを固有の合成ノードに配置します。

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またはスクリプトを実行するために使用されます。注釈ノードの Annotate_Spec パラメータには、実行するコマンドまたは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、コマンドまたは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置かれます。

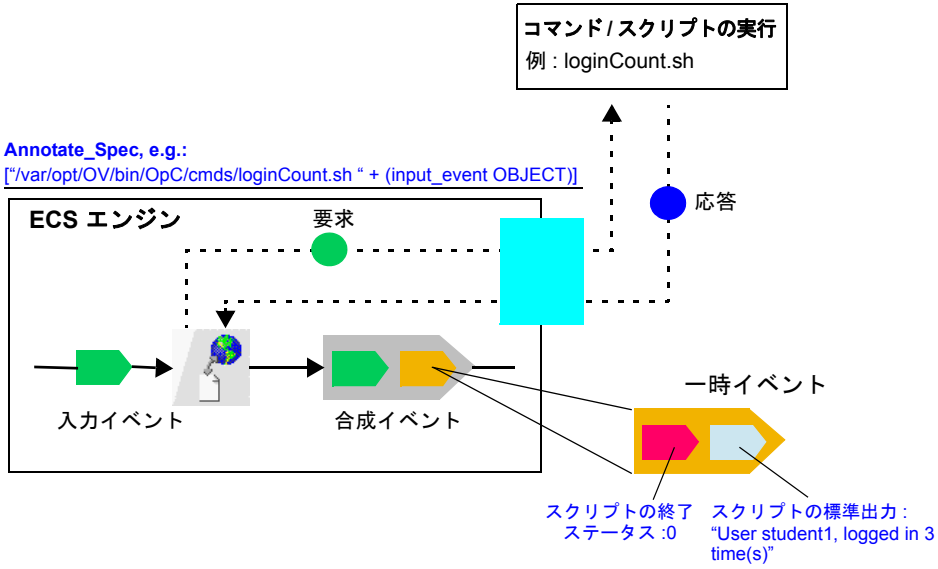
図 4-31 は、HPOM の内部注釈サーバーから返されるデータに終了コードとコマンドまたはスクリプトの標準出力の 2 つの情報が含まれていることを示しています。フィルターノードで終了コードを取得するには、次の文を使用します。

```
input_event 2 1
```

コマンドまたは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要求には、単一文字列を含めたリストとして `Annotation_Spec` が含まれている必要があります。この文字列値は、実行するスクリプトまたはコマンドの完全修飾ファイル名と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、単一パラメータ student1 を指定した /var/opt/OV/bin/OpC/cmds/loginCount.sh スクリプトを実行します。スクリプトには、これ以外にも位置指定パラメータ ($2、$3 など) を指定できます。

通常、スクリプトまたはコマンド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)]
```

スクリプトまたはコマンドは、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設定されていないため、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 コマンドディレクトリ /var/opt/OV/share/databases/OpC/mgd_node/customer/<arch>/\cmds に置く場合、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
<other_cmd_parameters>"]
```

スクリプトは、必要な応答を生成するためにexit および echo コマンド (またはこれに相当するコマンド) を使用します。

次のスクリプトは、ユーザー (ユーザー名は最初のパラメータ) がログインした回数を示すテキスト文字列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

独自の注釈サーバープロセスを開発するユーザーのために注釈 API が用意されています。ユーザー作成 (カスタム) の注釈サーバーは、ECS エンジンに登録され、注釈要求をリスンする独立したプロセスです。要求を受信する

と、注釈サーバーはその要求を処理し、注釈 API を使用して相関処理サーキットに応答を返します。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や、ネットワークデバイスの MIB に対するクエリの実行、別のアプリケーションからのトポロジ情報に対するクエリの実行など、さまざまな用途に使用できます。

ECS サーキットのインポート

本項では、HPOM システムへの ECS サーキットのインポート方法を説明します。コマンドラインツール[1] を使用して ECS ポリシーを作成し、そのポリシーに .eco (コンパイル済みの EC サーキット) と .ecs (EC ソースサーキット)[2] ファイルをアップロードするには、次の手順に従ってください。

1. HP Operations 管理サーバー上で、次のコマンドを実行してすべての ECS ポリシーを一覧表示します。

   ```
   opcpolicy -list_pols pol_type=Event_Correlation
   ```

2. 次のコマンドを実行して、ECS ポリシーを選択してダウンロードします。

   ```
   opcpolicy -download pol_name=<policy_name> \
   version=<version> pol_type=Event_Correlation \
   dir=<download_dir>
   ```

   例:

   ```
   opcpolicy -download pol_name=bad_su \
   version=0009.0000 pol_type=Event_Correlation \
   dir=/tmp/ecs_policy
   ```

   <download_dir> ディレクトリには、<id>_circuit、<id>_source、<id>_data、<id>_header.xml ファイルが保存されています。これらのファイルを使用して、自分のニーズに合わせて新しい ECS ポリシーを作成してください。

3. 次のコマンドを実行してダウンロードディレクトリ内のすべてのファイルを一覧表示します。

   ```
   ls <download_dir>
   ```

---

1. 管理 UI を使用する場合は、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、作成した ECS ポリシーの [ソース] タブで、そのポリシーに .ecs と .eco ファイルをアップロードします。
2. .ecs ファイルはオプションです。

次のような出力が表示されます。

```
50287ad6-e455-11dc-94db-00306ef38b73_circuit
50287ad6-e455-11dc-94db-00306ef38b73_data
50287ad6-e455-11dc-94db-00306ef38b73_header.xml
50287ad6-e455-11dc-94db-00306ef38b73_source
```

4. 必要に応じて、<name> と <description> 行を変更して、<id>_header.xml ファイルを編集します。

   次に例を示します (ダウンロードした ECS ポリシーの名前を bad_su とします)。

```
<name>bad_su</name>
<description>suppress bad_su if followed by
succeeded_su</description>
```

5. ECS、DESCRIPTION、CIRCUIT_FILE 行を変更して、<id>_data ファイルを編集します。

   次に例を示します (ダウンロードした ECS ポリシーの名前を bad_su とします)。

```
ECS "bad_su"
DESCRIPTION "suppress bad_su if followed by succeeded_su"
CIRCUIT_FILE "ECbad_su"
```

重要

ECS と DESCRIPTION の値が <id>_header.xml ファイルで使用されている <name> と <description> の値に対応していることを確認します。サーキットファイル名には任意の名前を使用できます。

6. ECS Designer がインストールされているシステムから HP Operations 管理サーバーに .ecs と .eco ファイルを転送します。

7. .ecs ファイルを <id>_source ファイルに、.eco ファイルを <id>_circuit ファイルにコピーします。

   次に例を示します。

```
cp newcircuit.ecs \
50287ad6-e455-11dc-94db-00306ef38b73_source
cp newcircuit.eco \
50287ad6-e455-11dc-94db-00306ef38b73_circuit
```

8. 次のコマンドを実行してポリシーをアップロードします。

   ```
   opcpolicy -upload file=<id>_header.xml mode=add
   ```

   次に例を示します。

   ```
   opcpolicy -upload \
   file=/tmp/ecs_policy/50287ad6-e455-11dc-94db-00306ef38b7
   3_header.xml mode=add
   ```

9. 次のコマンドを実行して、新しい ECS ポリシーが作成されたことを確認します。

   ```
   opcpolicy -list_pols pol_type=Event_Correlation
   ```

重要

管理 UI を使用する場合: ローカルの .ecs と .eco ファイルを管理 UI で参照できるように、ECS Designer と同じシステムで実行されているブラウザから管理 UI にアクセスしていることを確認します。

.ecs と .eco ファイルを管理 UI で参照する場合、ポリシーは他の残りのポリシーデータと共にデータベースに保存されます。

ECS サーキット名の変更

ECSサーキット名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て 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のサーキット名を取得するには、このポリシーをダウンロードします。これを行うには、次のコマンドを実行します。

   ```
   # opcpolicy -download pol_name=<policy_name> \
   version=<version> pol_type=Event_Correlation \
   dir=<download_dir>
   ```

3. ポリシーをダウンロードした <download dir> ディレクトリで、<id>_data ファイルを開き、CIRCUIT_FILE 属性をチェックします。この属性の値は、ECS サーキット名に対応します。

   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=<download_dir>

   opcpolicy コマンドの詳細については、opcpolicy(1M) 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 という名前のイベント相関ポリシーがあり、サーキット名は EAAAa03016 であるとします。イベント相関処理ポリシーは、固有データストアから設定データにアクセスし、グローバルファクトストアからデータベース関係にアクセスします。次の手順に従ってください。

1. 次のコマンドを実行して EC ポリシーの名前とバージョンを取得します。

   # opcpolicy -list_pols pol_type=Event_Correlation

2. DatabaseDown ポリシーのコンパイル済みのサーキット名を取得するには、このポリシーをダウンロードします。これを行うには、次のコマンドを実行します。

   **# 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 属性をチェックします。

   CIRCUIT_FILE "EAAAa03016"

   ここで、EAAAa03016 は ECS サーキット名です。

4. 次のように入力して、ECS サーキット名を 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) 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. グローバルファクトストアファイル (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、コンパイル済みのサーキットファイルと同じ名前を持つ DatabaseDown.ds データストアファイルがロードされます。DatabaseDown.fs ファイルは存在しないので、グローバルファクトストアファイル 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ーが 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ーへの格納

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 Java GUI メッセージブラウザに送られます。一方、サービス時間外に受信したメッセージは、すべてバッファーに格納されます。バッファーに格納されているメッセージは、Java GUI ペンディングメッセージブラウザで確認できます。

メッセージのバッファーからの自動取り出し

バッファーに格納されたメッセージは、次のサービス時間の開始時に自動的にバッファーから取り出され、Java GUI メッセージブラウザに移動されます。バッファーから Java GUI メッセージブラウザに移動したメッセージには、通常どおりの処理を実行できます。

メッセージのバッファーからの手動取り出し

バッファーに格納されたメッセージは、[メッセージのプロパティ] ウィンドウか、Java GUI ペンディングメッセージブラウザから、手動で取り出すことができます。手動でバッファーから取り出されたメッセージは、取り出し操作を行ったユーザーによって所有またはマーキングされます。

手動でバッファーから取り出されたメッセージには、次の制限が適用されます。

- **メッセージはバッファ時間の終了後にのみ送信される**

  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。

- **管理サーバーへの着信時に転送される**

  マネージャ間 (manager-to-manager) 転送が設定されている場合、バッファーに格納されるメッセージは HP Operations 管理サーバーへの着信時に、定義済みの他の各管理サーバーに転送されます。

注記

管理サーバーが異なれば、休止時間とサービス時間の設定も異なる場合があります。

サービス時間の設定

サービス時間の設定方法と、サービス時間の定義に使用されるポリシーおよび構文規則の詳細については、『HPOM 管理者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、サービスやシステムが特定の時間にわたって利用できなくなる場合、またはそのように計画されている場合に、**計画休止**を設定することによって、その時間内に到着した関連するメッセージを**ログ**に記録したり、**除外** (削除) することが可能です。たとえば、特定のコンポーネントが保守のため一時的に利用できなくなる場合には、計画休止を使ってそのコンポーネントに関するメッセージをすべて除外することができます。

計画休止の設定

計画休止とは、分散した作業環境内の 1 つまたは複数のコンポーネントやサービスを特定時間にわたって計画的または定期的に停止することであり、計画休止の時間内に着信する当該コンポーネントやサービスに関するメッセージは、ログに記録するか、削除する必要があります。重大な障害が発生し、特定のコンポーネントに関するメッセージを除外する必要が生じたときには、休止を動的に設定することもできます。たとえば、データベースサーバーがダウンした場合には、そのデータベースサーバーに関連するすべてのメッセージを特定の時間にわたって除外できます。計画休止のステータスを、外部アプリケーションから設定することも可能です。

計画休止の定義

計画休止の設定方法と、計画休止の定義に使用されるポリシーおよび構文規則の詳細については、『HPOM 管理者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、フレキシブル管理の設定に使われるものと同様のポリシーを使用して、管理サーバー上でサービス時間と計画休止を設定できます。同じ構文が使われるので、`opcmomchk` ツールでチェックできます。このポリシーは `/etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs` にあります。サービス時間と計画休止の設定に使用するポリシーとその構文の詳細については、『HPOM 管理者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で設定することもできます。ただし、その外部アプリケーションで、休止とサービス時間のポリシーを作成し、`opccfgout(1M)` コマンドを使用して休止を制御する必要があります。

メッセージ選択条件に基づくカスタムメッセージ属性の設定

各種のメッセージ条件に基づいてカスタムメッセージ属性 (たとえば、ノード名、IP アドレス、メッセージテキスト、重要度など) を設定できます。この設定には、各種のメッセージ条件に基づいて一致するメッセージを取り込んで処理できる `msgmodify` 設定ファイルを使用します。

メッセージ条件に基づいたカスタムメッセージ属性の設定は、メッセージ変更の一例です。メッセージ変更を有効にするには、次の手順に従ってください。

1. `tmpl_respmgrs` ディレクトリから `work_respmgrs` ディレクトリに `msgmodify` テンプレートをコピーします。

   両方のディレクトリは次の場所にあります。

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

2. お使いの環境に合わせてテンプレートを変更します。
3. `opcmomchk(1)` ツールを使用して構文をチェックします。
4. 変更したファイルを次のディレクトリにコピーします。

   `/etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs`

5. `opccfgout -update` コマンドを実行します。

`msgmodify` 設定ファイルの構文についての詳細は、msgmodify(4) マニュアルページを参照してください。

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

本章の内容

本章では大規模な分散環境での HPOM の設定方法と管理方法を説明します。さらに、フレキシブル管理と manager-of-manager (MoM) 通信の基本的な概念も説明します。

注記

本章における“「マネージャ」”という用語は、**管理サーバー**を意味し、“「エージェント」”という用語は**管理対象ノード**を意味します。

対象読者

本章は HPOM 管理者を対象としています。

目的

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**

  管理サーバー間の通信の基本となる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**

  時間やメッセージの属性に基づいて設定可能な管理対象ノードから各種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の 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。

- **管理サーバーの作業範囲の設定**

  HPOM 管理対象ノードに対する管理サーバーの作業範囲の設定。管理サーバーの作業範囲を設定することによって、ナレッジセンターを最大限に活用し、さらに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**

  他の管理サーバーへのサーバー設定の配布 (テスト環境から運用環境への設定の移動など)。

- **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の転送

フレキシブル管理

HPOM では、環境を階層的に構成することが可能であり、これにより、オペレータの経験や地理的な場所、時刻などのさまざまな条件に基づいて、複数の管理レベルに渡って管理の作業範囲を分散させることができます。このフレキシブル管理によって、技術的なサポートをいつでも必要なときに自動的に安心して利用できるため、オペレータは各自が得意な業務に専念できます。

注記

日本語環境でのフレキシブル管理についての詳細は、『HPOM 管理者リファレンスガイド』を参照してください。

デフォルトの設定

HPOM のデフォルト設定では、管理対象ノードにインストールされたエージェントとやり取りを行う 1 台の管理サーバーで構成されます。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だけです。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から他の管理サーバーにもメッセージを送信できるように、容易に変更できます。

一次マネージャ

最初の管理サーバーは、HPOM 管理対象ノードに対して主要な役割を果たす 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を別のサーバーに切り替えることができます。一次マネージャを切り替えると、管理対象ノードから出力されるメッセージの送信先も、新しい (通常、一時的な) 一次マネージャにリダイレクトされます。一次マネージャは、これらの管理対象ノードに対する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利点

HPOM のフレキシブル管理アーキテクチャを活用すると、以下を行うことができます。

- **ワールドワイドネットワークの管理**

  フォローザサン機能を使用して、全世界に広がるネットワークをより効率的に管理できるようになります。

- **効率性の向上**

  専門技術センターのポリシーを実装することで効率を向上させます。

- **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。

- **ネットワーク拡張の管理**

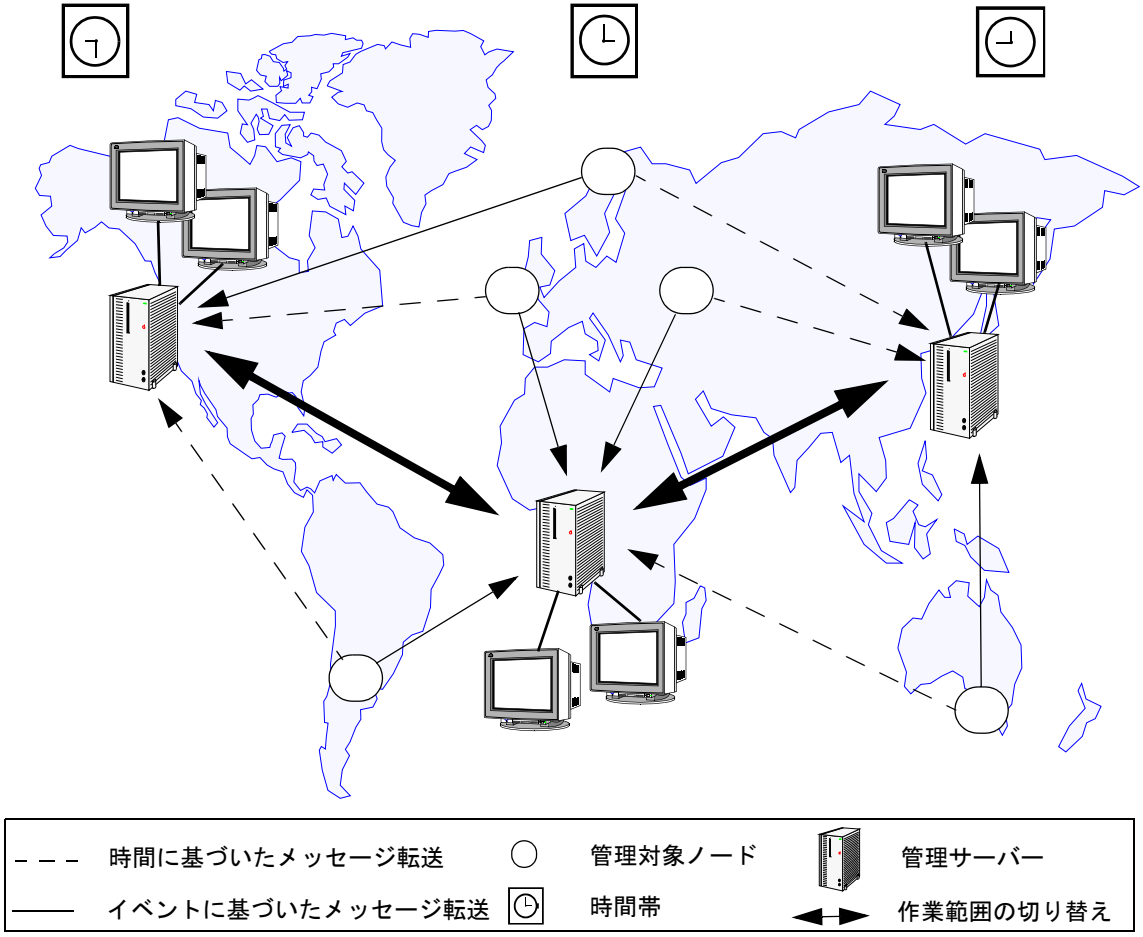
  ネットワーク環境の拡張を管理し、一次サーバーの負荷を抑制します。

すべての管理対象ノードが 1 台の管理サーバーにメッセージを送信すると、それがボトルネックになる可能性があります。このボトルネックがデータベースのパフォーマンスが悪影響を及ぼす可能性があります。管理対象ノードが複数の管理サーバーにメッセージを送信すれば、この問題の発生を回避できます。管理作業範囲の分散についての詳細は、「ドメイン階層内の管理作業範囲」(323 ページ) を参照してください。

フォローザサン管理

複数のタイムゾーンにわたって事業拠点が分散している場合、HPOM では**フォローザサン**管理を行うことにより管理作業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)。つまり、1 日の時刻の経過に応じて管理対象ノードのメッセージの送信先を、異なる地域の管理サーバーに変更させます。この機能を使用して、週末や休日用の特定の管理サーバーを設定することもできます。

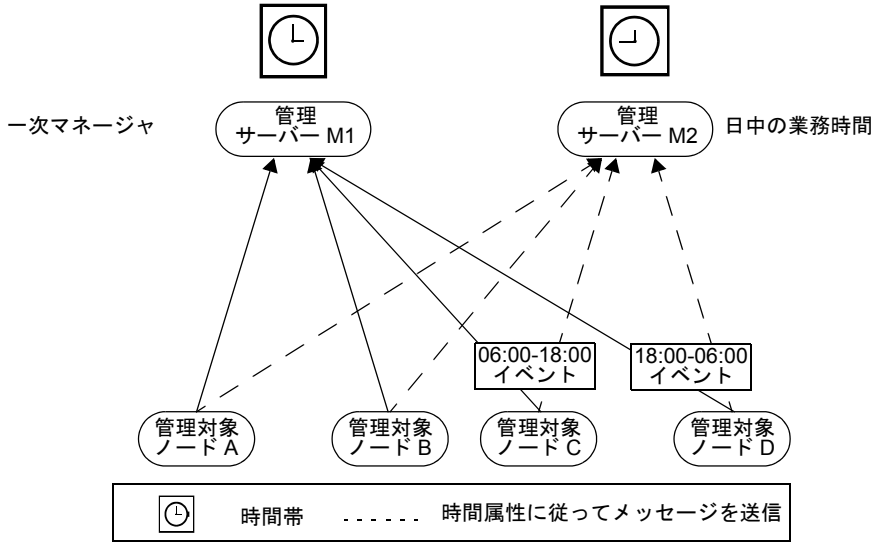
図 5-1　ワールドワイド管理ドメイン



フォローザサンの概念は、あらかじめ設定された時間属性に基づいて、異なる管理サーバーにメッセージを送信するという考え方に基づいています。HPOM では、**時間ポリシー**によって定義されたルールに従い、異なる管理サーバーにメッセージを送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 および D が、6 時から 18 時までに生成したすべてのメッセージを HP Operations 管理サーバー M1 に送信するように HPOM を設定する方法を示しています。18 時から 6 時までに生成されたメッセージは、HP Operations 管理サーバー M2 に送信されます。フォローザサン機能を使用すると、ある地域の管理サーバーが営業時間外になっても、昼間である別の地域の管理サーバーにその地域の業務をシフトすることによって、24 時間を通じて環境全体を制御できます。

図 5-2　メッセージを転送するための時間やメッセージの属性の使用



たとえば、企業で 24 時間対応のサポートデスクを中央拠点に集約していた場合、HPOM では他の地域の営業拠点が営業時間外にあるときに、その地域の管理対象ノードから中央拠点の管理サーバーに直接メッセージを送信させることができます。フォローザサンポリシーを実装する場合、`allnodes` 設定ファイルに 2 つのエントリを追加する必要があります。

これらの 2 つのエントリは、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

各種の管理サーバーにメッセージを送信するには、変数 `$OPC_PRIMARY_MGR` を使用します。この属性によって、時刻に応じて異なるシステムを指定できます。

フォローザサンの概念は、時刻に基づいたルールに限定されるものではありません。特定の曜日や日付、あるいは頻度で、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可能です。詳細は、「時間ポリシー」(330 ページ) 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

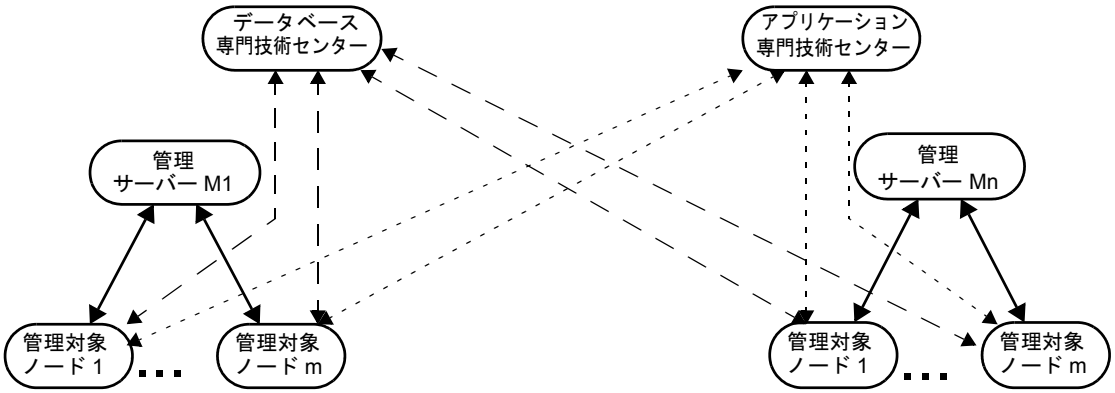
複数の管理サーバーが広範囲に分散した大企業では、特定分野の特化した知識を持つ専門家がすべての拠点にいるわけではありません。このため、一次マネージャ以外のサーバーとの通信を行う管理対象ノードを設定しておくと便利です。ネットワーク上の他のサーバーでは、データベース管理やスプール管理など、コンピュータに関する専門知識を利用できるかもしれません。HPOM では、管理対象ノードをネットワーク内のどの場所にある管理サーバーとも通信を行えるように設定できます。

たとえば、オペレーティングシステム関連のあらゆる問題を担当する専門技術センターが企業内に設置されているとします。さらに別のセンターが、会社全体で使用するデータベースを担当しているとします。この場合、オペレーティングシステムに関するメッセージは一方の専門技術センターに送り、データベースの問題に関するメッセージはもうひとつのセンターに送るよう管理対象ノードを設定できます。図 5-3 では、すべての管理対象ノードが、データベース関係のイベントをすべて管理サーバー M1 に送信します。

専門技術センターにおける役割分担

メッセージの種類によっては、図 5-3 に示すような専門技術センターに基づくシンプルな階層の方が、中央管理サーバーに基づく階層よりも柔軟な環境を構築できます。

図 5-3　専門技術センターに基づく環境での通信



中央管理サーバーの階層とは異なり、専門技術センターの階層では、管理対象ノードの作業範囲が分散しています。専門技術センターでは、地域ごとのマネージャは管理対象ノードだけを担当するわけではありません。データベースなどの特定の分野についてのメッセージは、定義済みの管理サーバーに直接送信され、この管理サーバーには、すべての管理対象ノードに関する問題を解決するための専門的な知識が蓄積されています。

専門技術センターの設定

次の概念的な構文は、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

専門技術センターの条件に時間条件を追加することにより、設定にフォローザサン機能を含めることができます。

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 台の HP Operations 管理サーバーは同じように設定されます。メインのインストールは一時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。

なんらかの理由により一次マネージャが一時的にアクセスできなくなった場合、メッセージを管理対象ノードから指定された 1 台以上のバックアップ管理サーバーに送るように、HPOM を設定できます。

バックアップサーバーの設定

これらのメッセージに応答するには、バックアップサーバーに一次マネージャで使用されている関連する設定とポリシーが必要になります。つまり、バックアップ用に指定したサーバーとノードには、一次マネージャに問題が発生する前に、関連する設定とポリシーを配布しておく必要があります。さらに、それぞれの管理対象ノードでは、特定のメッセージを特定のサーバーに送信するための時間帯と条件を設定しなければなりません。

設定とポリシーの配布

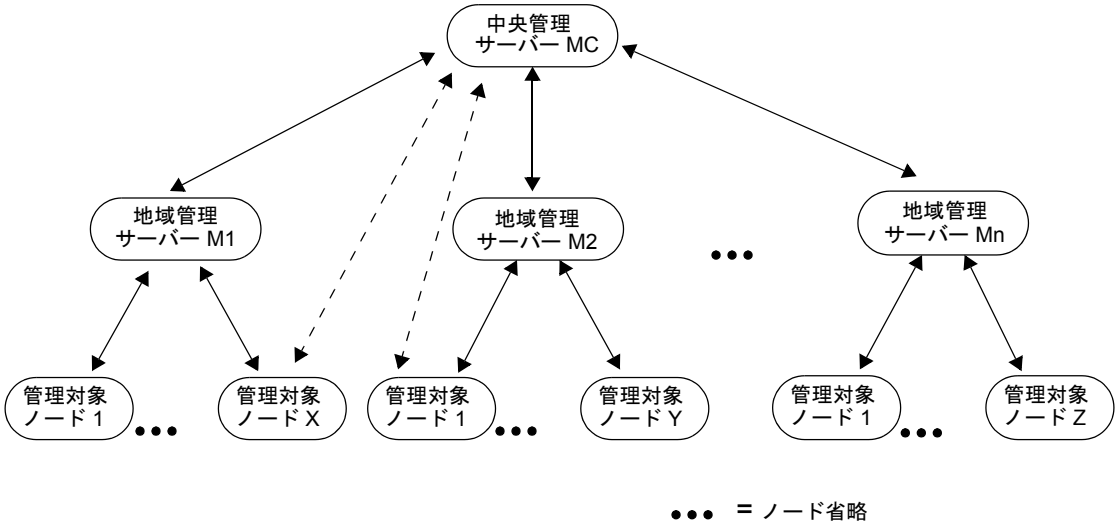
関連するすべての管理サーバーとノードに関連する設定とポリシーを配布することにより、製品開発の一元化を容易に行えます。中央のサーバー上で設定とポリシーを作成して、それを指定したサーバーと管理対象ノードに配布できます。

たとえば、本社でポリシーを作成し、そのポリシーを各支社の複製環境にインストールしたり、更新したりできます。HPOM では、このデータをファイルにダウンロードし、他のサーバーにこのファイルをアップロードすることで、設定、ポリシー、およびソフトウェアを配布できます。

管理階層

一般的に、図 5-4 に示すような製造環境では明確な管理階層が形成されています。環境を再構成することなく、マネージャ間の通信で適切な作業範囲を使用することができます。

図 5-4　一般的な製造環境と通信リンク



管理階層内の管理プロファイル

地域的に分散した場所に複数の製造サイトを持つ企業の場合、図 5-4 に示すような環境は製造業でごく一般的です。このような地理的分散は、複製されたサイト管理と比較できます。通常、すべてのサイトには類似した管理プロファイルがあります。つまり、すべてのサイトには、管理対象オブジェクト、ポリシー、エンドユーザーの作業範囲が類似して設定されています。

管理階層の設定比率

このような環境は規模において大きく異なりますが、一般的な設定比率は次のようになります。

- ❏ 中央の管理サーバー － 1 台
- ❏ 地域管理サーバー － 10 ～ 20 台
- ❏ HP Operations Agent が動作する管理対象ノード (サーバーとマルチユーザーシステム) － 100 ～ 200 台
- ❏ SNMP イベントを送信する管理対象要素 － ～ 5000

ドメイン階層内の管理作業範囲

HPOM のドメイン階層では、それぞれの管理対象ノード上で、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) を管理する HP Operations Agent が実行されます。管理対象ノードは、メッセージを地域の管理サーバーに送ります。指定した地域のすべての管理対象ノードは同じ設定になります。

地域の管理サーバー

地域の管理サーバー (322 ページの図 5-4 の M1-Mn) では HP Operations 管理サーバーソフトウェアと、HP Operations のローカルエージェントが実行されています。これらのサーバーが地域内のシステムを制御します。地域サイトでは通常、高コストな WAN (広域ネットワーク) ではなく LAN (ローカルエリアネットワーク) 環境で管理されます。この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の正常な動作を維持する役割を担当します。

中央の管理サーバー

中央の管理サーバーでは、HP Operations 管理サーバーソフトウェア、ローカルの HP Operations Agent、地域の管理サーバーシステム、これらのシステム上で実行されている管理アプリケーション (Data Protector、Performance など) が実行されます。

運営面では、中央サイトの HPOM 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。中央サイトの HPOM のオペレータは、地域レベルで解決できない問題を処理します。管理面では、中央サイトは地域のサーバーの設定を作成、配布、および維持管理する役割を担っています。アプリケーションに関するノウハウを中央に一元化し、各地域の設定をほぼ共通化できるため、もっとも合理的な設定といえます。

管理サーバーの設定

中央管理サーバーの環境では、管理対象ノードは問題をすべて地域の管理サーバーに送ります。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。

中央管理サーバーのアクション許容マネージャとしての設定

中央管理サーバーの管理環境では、中央サーバーをすべてのエージェントに対し、**アクション許容マネージャ**として設定します。中央サーバーを、すべてのエージェントに対するアクション許容マネージャとして設定することにより、中央サーバーは分散した各管理対象ノードに対してアクションを行えるようになります。その結果、分散した管理対象ノードの制御が一元化され、中央サーバーは上位転送されたメッセージを処理し、作業範囲の切り替えを管理することができます。

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、中央サーバーを最低限の作業でアクション許容マネージャとして設定できます。HPOM 管理者が各地域管理サーバー上で 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した項目が含まれます。

中央管理サーバーの二次マネージャとしての設定

二次マネージャを指定するときは、中央サーバーも二次マネージャとして設定することをお勧めします。これにより一次マネージャに障害が発生しても、管理作業範囲は二次マネージャにバックアップとして切り替えられます。

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場合は、次のディレクトリにコピーする必要があります。

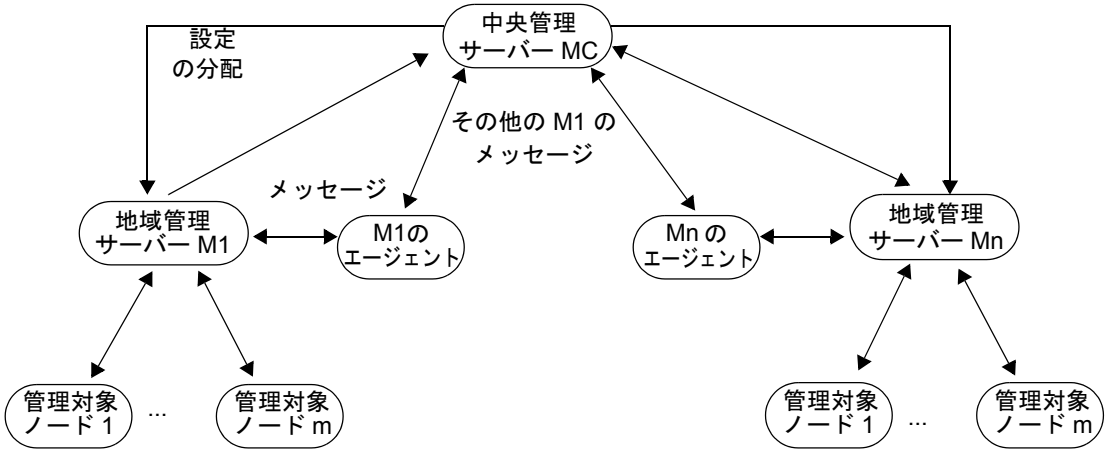
```
/etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs
```

HPOM の起動時に、ファイルがこのディレクトリから読み取られ、その内容が実装されます。

中央管理サーバーの設定

図 5-5 の中央管理サーバー (MC) は、地域管理サーバーシステム (M1 ～ Mn) を管理対象ノードとして制御します。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、それらをオペレータに割り当てる必要があります。

図 5-5　　中央管理サーバーの設定と通信リンク



マスター設定全体 (ノード、メッセージグループ、オペレータ、ポリシー) を中央管理サーバーに格納することにより、いくつかの利点が得られます。HPOM の専門技術者を 1 か所に集めることができるため、専門技術者が各地域サイトの設定を一元化し、それを各サイトに配布することができます。

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、そのファイルを一次管理サーバー上の `respmgrs` ディレクトリ内に保存します。ファイル名は、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。このテキストによってメッセージを送信するタイミング、場所、方法が定義されます。

設定ファイルの作成

担当マネージャの設定ファイルでは、以下を設定する必要があります。

- ❏ 一次管理サーバーと二次管理サーバー
- ❏ アクション許容管理サーバー
- ❏ 異なる各管理サーバーにメッセージを送信するための日時ポリシー
- ❏ 各マネージャにメッセージを送信するためのメッセージの属性規則

たとえば、環境内のすべてのノードに設定を適用する場合には、すべてのノード用に設定ファイルを 1 つ作成し、このファイルに `allnodes` という名前を付けます。設定を特定のノードのみに適用する場合は、ファイル名はそのノードの IP アドレス (16 進形式) で、`opc_ip_addr` コマンドによって生成されます。いくつかのノードの設定が共有している場合は、同じ設定を含むノード固有ファイルへのリンクを作成します。ノードに対する固有のファイルが存在しない場合、HPOM は `allnodes` ファイル内の設定を使います。

担当マネージャの設定ファイルの場所と、その作成に必要な手順は、HPOM のオンラインヘルプか、opcmom(4) のマニュアルページを参照してください。

注記

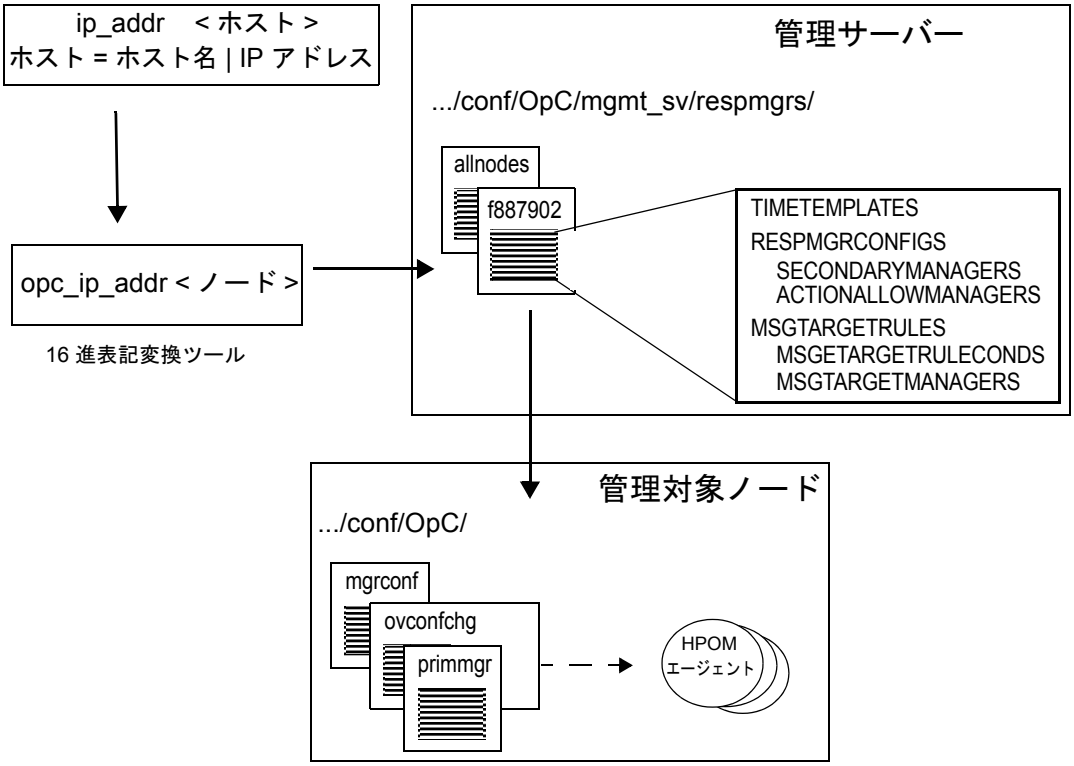
日本語環境でのフレキシブル管理の詳細は、『HPOM 管理者リファレンスガイド』を参照してください。

設定ファイルの配布

HPOM はポリシーを配布するときに、管理対象ノードに自動的に配布します。同時に、HPOM はインテリジェントエージェントを新しい、または更新された設定により初期化し直します。担当マネージャの設定ファイル `mgrconf` は、管理対象ノード上に配置されます。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。

328 ページの図 5-6 は、管理対象ノード用の担当マネージャポリシーを示しています。

図 5-6　管理対象ノード用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、**メッセージターゲットルール**のリストを使用して、定義済みの管理サーバーにメッセージを送信するかどうか、メッセージを送信する場合はどのサーバーに送信するかを決定します。

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次の 3 つの要素から構成されます。

- ❏ メッセージの属性ルール
- ❏ 時間ポリシー
- ❏ 定義済みの管理サーバー

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成は次のとおりです。

メッセージグループ = “printing”

現在の時刻が時間テンプレート 2 に該当する .....(メッセージ) --> mgr 2

現在の時刻が時間テンプレート 1 に該当する.....(メッセージ) --> mgr 1

現在の時刻が時間テンプレート 3 に該当する.....(メッセージ) --> mgr 3

この例では、ポリシー 1 の時間条件に一致する、メッセージグループ「“printing”」に属する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 の時間条件に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。時間ポリシー 3 の機能も同様です。

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時間は次のとおりです。

メッセージグループ = “database”

現在の時刻が時間テンプレート 1 に該当する.....(メッセージ) --> mgr 2

現在の時刻が時間テンプレート 2 に該当する.....(メッセージ) --> mgr 3

現在の時刻が時間テンプレート 3 に該当する.....(メッセージ) --> mgr 1

この例では、ポリシー 1 の時間条件に一致するメッセージグループ「“database”」に属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 2 の時間条件に一致するすべてのメッセージは HP Operations 管理サーバー 3 に転送されます。

時間ポリシー

時間ポリシーは、特定の管理対象ノードが、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示する条件 (またはルール) のセットです。時間条件を作成して、時間ポリシーに保存します。単純なルールを組み合わせて、複雑な条件を設定できます。たとえば“「1 月から 3 月までの月曜、水曜、木曜の午前 10 時から 11 時 35 分まで」”というルールです。時間条件には 24 時間表記を使用します。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。

- **時刻指定なし**

  特定の時刻、曜日、年などを指定しないと、HPOM は条件がその年一年を通して毎日 00:00 から 24:00 の範囲で満たされるものと仮定します。条件を指定すると、HPOM はその条件が指定した日時において継続的に適用されるものと仮定します。

  たとえば、“ 火曜日 ” を指定すると、条件は 1 年を通じて毎週火曜日の 00:00 から 24:00 の範囲が毎年適用されます。

- **時間の範囲**

  時間の範囲 (“7:00 ～ 17:00” など) を指定します。

- **日付または期間を示すワイルドカード (*)**

  日付または期間にワイルドカード (*) を指定できます (たとえば、毎年の 1 月 31 日を指定するには、「“1/31/*”」と入力します)。

時間に関係しないポリシーの設定

HPOM では、スケジュール設定したアクションが時間に関係しないときでも、メッセージターゲットルールに対して時間ポリシーの設定を必要とします。HPOM では時間に関係しないポリシーを設定するため、変数 `OPC_ALWAYS` が用意されています。

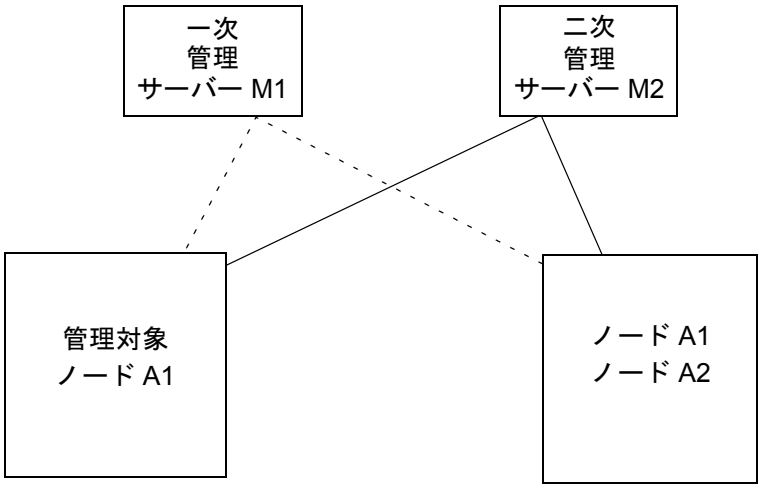
一次マネージャの指定

デフォルトでは、すべてのメッセージは最初に HP Operations Agent ソフトウェアをインストールした HP Operations 管理サーバーに集められます。デフォルトの設定では、HP Operations 管理対象ノードは 1 台の HP Operations 管理サーバーによって管理されます。ただし、HPOM では、ノードの管理作業範囲を複数の 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

一次管理作業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 ノードに対する作業範囲を二次管理サーバーに与えることになります。

図 5-7　一次管理作業範囲の切り替え



管理作業範囲の二次管理サーバーへの切り替えは、`opcragt -primmgr` コマンドを使用して起動します。このコマンドは、パラメータとして管理対象ノードのリスト、(ホスト名または IP アドレス)、またはノードグループ名を受け入れます。詳細は、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場合、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いない、あるいは初期マネージャとして指定されていない状態です。

OPC_PRIMARY_MGR はメッセージに関連する設定です。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、担当マネージャポリシーのメッセージターゲットルールで使用される $OPC_PRIMARY_MGR 変数にマッピングします。

二次マネージャによるアクション実行の許可

二次マネージャが作業範囲となるノードへの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、現在の一次マネージャを一括してアクション許容マネージャにします。

```
ACTIONALLOWMANAGER $OPC_PRIMARY_MGR
```

マネージャ切り替えの取り消し

一次管理作業範囲は、新しい一次管理サーバーが一次管理作業範囲を外れても、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。一次管理作業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とアクション許容マネージャとして設定し、opcragt -primmgr コマンドにより作業範囲を手動で切り替えます。

マネージャ作業範囲の委譲

HPOM インストールマネージャの作業範囲 (定期ポーリングやライセンスカウントなど) は、opchbp(1m) コマンドまたは opcsw(1m) コマンドを実行して一次サーバーに委譲できます。詳細は、対応する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

一次管理の作業範囲の切り替えは、システムのシャットダウンや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を使用することで一次管理サーバーの状態をモニターするように二次管理サーバーを設定できます。一次管理サーバーでシステム障害が発生すると、二次管理サーバーが HPOM 管理者に通知します。HPOM 管理者はこれに対応して一次管理の作業範囲を二次 HP Operations 管理サーバーに切り替え、このサーバーは障害が発生した管理サーバーによって管理されていた管理対象ノードをすべて制御するようになります。

アクション許容マネージャの指定

管理対象ノード上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 (または複数のノード) を担当する一次管理サーバーの機能を引き継ぐ二次管理サーバーも、担当する管理対象ノード上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。この設定を行わないと、二次管理サーバーはこれらのノードにアクションを実行できません。

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 管理サーバーのみが、HPOM **インストールマネージャ**になります。運用上の柔軟性を高めるために、HPOM では共有管理対象ノードに対してアクションを実行できるように HP Operations 管理サーバーを複数設定できます。

注記

一次マネージャ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。担当マネージャ設定に、次の行を追加します。

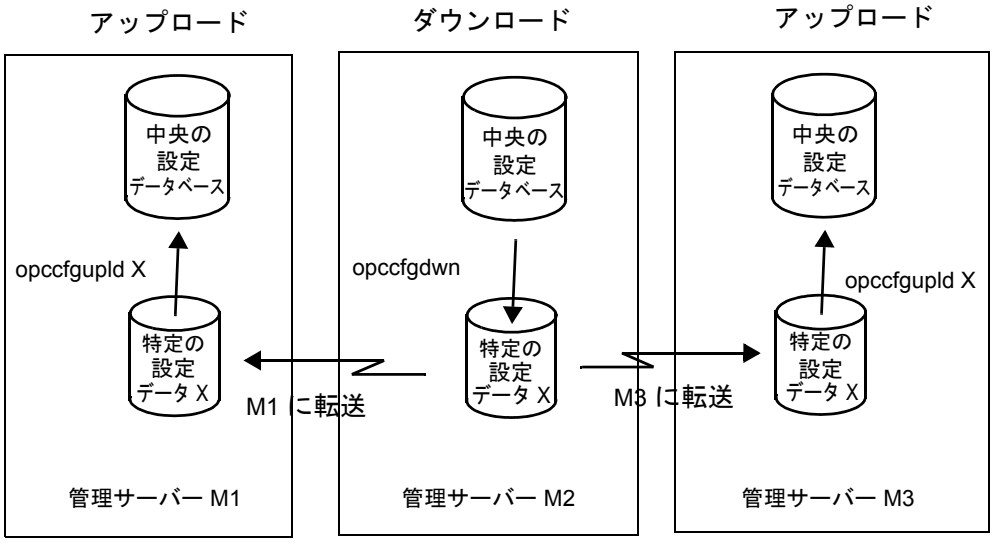
```
ACTIONALLOWMANAGER $OPC_PRIMARY_MGR
```

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、それを各種の管理サーバーに配布する方法が役に立ちます。たとえば、本社の HPOM 管理者は、設定やアプリケーションを特定のサイトで定義し、そのデータを他のサイトでアクセスして使用するファイルセットにダウンロードできます。

HPOM によって他のサーバーに設定ファイルが配布されると、図 5-8 で示すようにリモートサイトの管理者はこのファイルを自分のサイトのデータベースにアップロードして利用できます。

図 5-8　設定ファイルのダウンロードとアップロード



各管理サーバーに設定を配布する主な手順には次の 3 つがあります。

1. **設定の対象部分をダウンロードする**

   この情報は、ダウンロードコマンド `opccfgdwn` を実行したときに、HPOM によって使用されるインデックスファイルに保存されます。同一の設定タイプをダウンロードする場合は、以前の指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間に信頼関係が確立されている場合は、次の手順を実行します。

   a. ダウンロードした設定を含めた tar ファイルを作成します。

   b. `ovdeploy` コマンドラインツールを使用して tar パッケージをリモート管理サーバーに安全にコピーします。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、`FTP`、`rcp`、`scp` などの別の方法を使用します。

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` コマンドを使用してこの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、管理者はスケジュールアクションを使用してアップロードをスケジュールします。

注意

アップロード中は、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。変更すると、アップロードしたデータが壊れる場合があります。

管理者はアップロードコマンド `opccfgupld` に `contents` オプションを指定することで、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についての詳細は、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。設定データのアップロードには、次のコマンドを使用します。

```
/opt/OV/bin/OpC/opccfgupld <upload_directory>
```

設定のアップロードについての詳細は「設定変更の同期」(112 ページ) 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の詳細は、opccfgupld(1m) のマニュアルページを参照してください。

注記

HPOM が設定やアプリケーションを自動的にアップロードするようにするには、`at` または `cron` を使用して `opccfgupld` コマンドの実行をスケジュールします。

管理サーバー間でのメッセージ転送

メッセージ転送は、特定の HP Operations 管理サーバーから他の管理サーバーにメッセージを転送して、問題の発生を他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するアクションを他のサーバーが実行できるようにする機能です。この機能を使用すると、他の管理サーバーに関係する可能性のあるメッセージを該当するサーバーに伝えることで、より柔軟性が高まります。さらに、HPOM ではメッセージの制御を特定の管理サーバーから他の管理サーバーに、また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。転送されたメッセージは、ターゲット管理サーバー上で通常の HPOM メッセージと同じように処理されます。たとえば、MSI が設定されている場合、転送されたメッセージは MSI で処理されるか、トラブルチケットシステムや通知サービスに転送されます。

HPOM では、メッセージの転送は自動的に行われます。つまり、管理者はポリシーを使って、メッセージを転送するソース管理サーバーを設定できます。ターゲット管理サーバーに到着した転送メッセージは、ソース側の管理サーバー上にある参照メッセージのコピーです。

メッセージの転送は、管理サーバー上にメッセージが到着したときに必ず行われます。メッセージを後から転送することはできません (つまり、オンデマンドによる転送は行われません)。GUI またはコマンドラインを使用して、通知メッセージ (メッセージブラウザのステータスカラムに `n` のマークが付いているメッセージ) を正常域メッセージに、あるいはその反対に変換することはできません。

正常域メッセージと通知メッセージ

通知メッセージとして送信するように明示的に定義しないかぎり、すべてのメッセージは正常域メッセージとして送信されます。また、メッセージ転送の設定ファイル (`/etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs/msgforw`) 内で、転送条件に `MSGCONTROLLINGMGR` または `NOTIFYMGR` キーワードを定義すると、変更する必要がなくなります。

通知メッセージは情報伝達の用途のみに使われ、実行できる操作も限られています。通知メッセージを受け取るターゲット管理サーバーの数に制限はありません。ただし、他の管理サーバーへの通知メッセージの転送は、デフォルトで無効 (つまり、`OPC_FORWARD_READONLY_MSGS` サーバー設定変数が `FALSE` に設定されている) ですので注意してください。この変数を `TRUE` に

設定すると、通知メッセージを他の管理サーバーに転送できます。サーバー設定変数についての詳細は、『HPOM Server Configuration Variables』を参照してください。

注記

HPOM for Windows では通知メッセージをサポートしていません。ただし、Operations Manager i (OMi) では通知メッセージをサポートしています。

正常域メッセージに対する操作は常に、これらのメッセージを保持している管理サーバーすべてに転送されます。その一方で、通知メッセージに対する一部の操作はローカルにのみ影響し、それ以外に転送されることはありません。表 5-1 では、各タイプのメッセージに対して実行できる操作、または実行できない操作を示しています。

表 5-1 正常域メッセージおよび通知メッセージに対する操作

操作	正常域メッセージ	通知メッセージ
受諾 / 受諾解除	✔	✔[a]
注釈の追加 / 削除 / 変更	✔	✔
所有 / 所有解除	✔	-
テキスト / 重要度の変更	✔	✔
CMA の追加 / 削除 / 変更	✔	✔
オペレータ起動アクションの開始	✔	-
自動アクションの再実行	✔	-

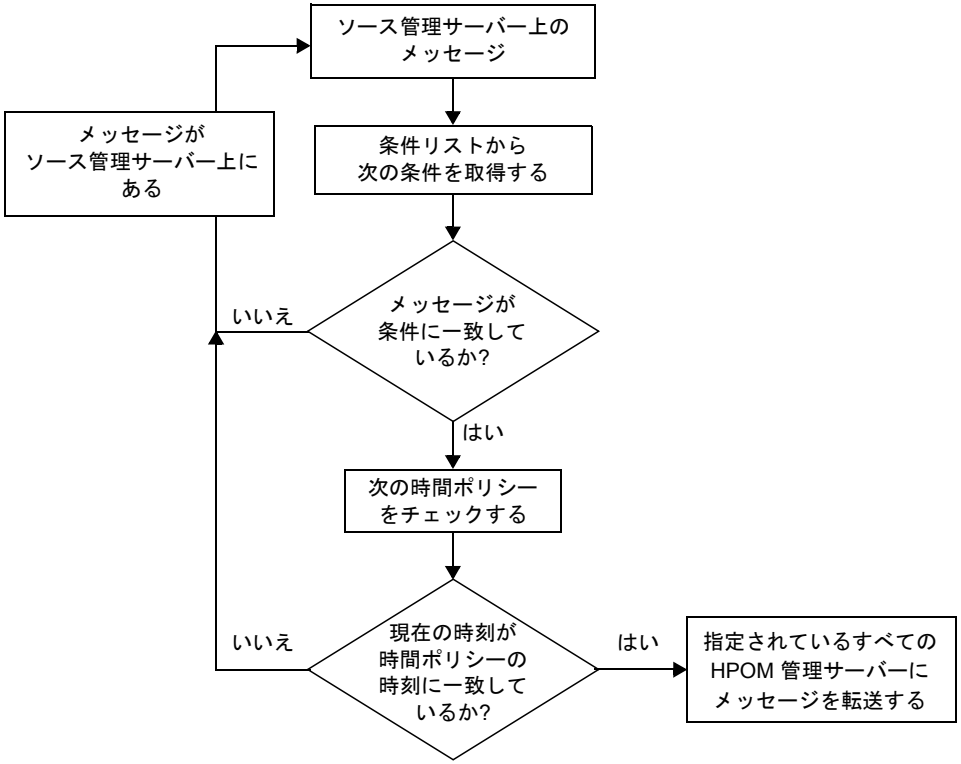
a. この操作はローカルにのみ影響します (他の管理サーバー上のメッセージコピーを受諾または受諾解除しません)。

メッセージ転送ポリシー

HPOM では、1 つのメッセージ転送ポリシーを作成して、通知メッセージの生成およびメッセージ制御の切り替えを行うことができます。ソース側の管理サーバーにこのポリシーを割り当てます。

ソース管理サーバーに到着する新規メッセージは、転送アクションが行われる前に必ずチェックされます (339 ページの図 5-9 を参照)。

図 5-9　ポリシーのチェックプロセス



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る配布先管理サーバーのリスト (配布リスト) が含まれています。この配布リストは、当該メッセージに転送後に加えられるあらゆる変更 (注釈の追加やアクションの実行など) を、リスト内の各マネージャに通知するために使われます。

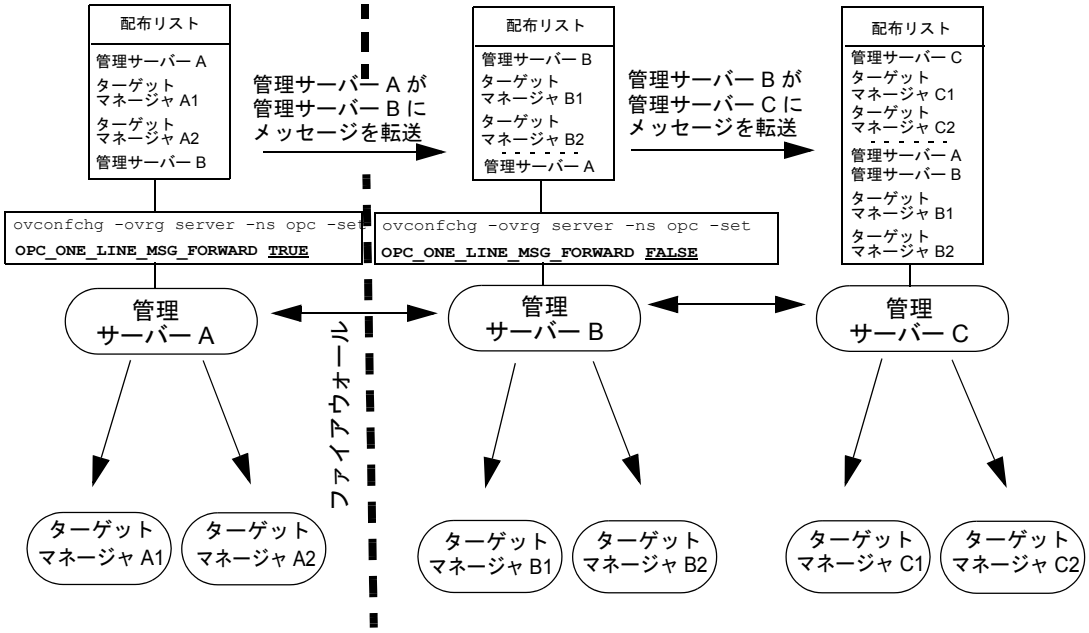
ターゲットマネージャは転送メッセージを受信すると、メッセージに関連付けられている、そのターゲットマネージャに固有の管理サーバー配布リストにこのリストを追加します。

配布リストのサイズの調整

メッセージが一連の管理サーバーに通知される間に増大する配布リストのサイズは、OPC_ONE_LINE_MSG_FORWARD パラメータで調整できます。

図 5-10 の例では、OPC_ONE_LINE_MSG_FORWARD パラメータがデフォルトの FALSE の設定のままである場合、管理サーバー B は、転送されたメッセージに関するすべてのターゲットマネージャのリストを、管理サーバー C に送る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。この場合、サーバー B は必要なアクションを実行し、そのサーバー自身の配布リストをサーバー 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と比較して、C から通知されていないターゲットのみに通知します。

図 5-10　大規模階層でのメッセージ転送



このアプローチは、通常の状況であれば高速で効率的ですが、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 A は管理サーバー B では認識されていますが、ファイアウォールが存在するため管理サーバー C では認識されていません。

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、次のような状況になります。

- ❏ 管理サーバー A は、メッセージへの変更を検知しない。
- ❏ 管理サーバー C は A から転送された元のメッセージへの変更を A に通知しようと試み、失敗する。
- ❏ 管理サーバー B は、C から A に変更が通知されたものとみなす。

管理者が 図 5-10 の管理サーバー B の `OPC_ONE_LINE_MSG_FORWARD` パラメータの値を `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 に転送される各メッセージに含まれる配布リストには、管理サーバー B 自身のみが含まれるようになります。

管理サーバー B のみが含まれることで、転送された同じメッセージに対して管理サーバー C が関連付ける配布リストは、図 5-10 に示されたものより次のように縮小されます。

- ❏ メッセージの送信元 (この場合、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 および C2)

これ以降に管理サーバー C がタスクを実行したり、またはメッセージに注釈を付けた場合、この情報は管理サーバー C の配布リストに指定された管理サーバーの縮小されたリストにのみ配布されます。管理サーバー B は (管理サーバー C から) メッセージへの変更を通知されると、指定されたアクションを実行し、管理サーバー B 自身がメッセージ固有配布リストに一覧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、結果として通知のチェーンが長くなりネットワークの設定や信頼性によっ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 で OPC_ONE_LINE_MSG_FORWARD が FALSE に設定された場合、管理サーバー C の配布リストには A と B に認識されているすべてのターゲット管理サーバーが含まれます。その結果、C のドメイン内でメッセージ状態が変化すると、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。

管理サーバーからトラブルチケットシステムへの接続

複数の管理サーバーを同じトラブルチケットシステムに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メッセージが同じトラブルチケットサーバーに対して送られることがあります。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、このメッセージが別の管理サーバーに転送された場合、このような状況になることがあります。

注記

管理対象ノードからのメッセージに対してトラブルチケットが有効になっている場合、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的に転送されます。ただし HPOM では、OPC_FORW_NOTIF_TO_TT パラメータ (デフォルトは FALSE) と OPC_FORW_CRTL_SWITCH_TO_TT パラメータ (デフォルトは TRUE) を使用して、このメッセージの転送先となる各管理サーバーでの、トラブルチケットシステムへの通知メッセージと正常域メッセージの転送を制御することができます。

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。メッセージ転送の設定は、環境での運用効率に直接影響します。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は、次の事項に留意してください。

❏ **管理対象ノード**

メッセージ転送を行うすべての管理サーバーで、登録ノードにすべての管理対象ノードを登録しておく必要があります。

- **ターゲットマネージャ**

  正常域メッセージに対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、該当する管理対象ノード上でアクション許容マネージャとして事前に定義されている必要があります。

❏ **メッセージの所有権**

ある特定の管理サーバーでメッセージを所有または所有解除すると、他の管理サーバーのオペレータには、すべてのオペレータがすべての管理サーバーにいる場合にのみ所有状態の変更が通知されます。

特定の管理サーバーで所有イベントと所有解除イベントを送受信しないようにするには、ovconfchg コマンドラインツールを使用して管理サーバーに次の変数を設定します。

- OPC_SEND_OWN_DISOWN FALSE (デフォルトは TRUE)
- OPC_ACCEPT_OWN_DISOWN FALSE (デフォルトは TRUE)

ovconfchg コマンドラインツールを使用し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**

管理サーバー上で ovconfchg コマンドラインツールを使用してパラメータを設定することによって、トラブルチケットサーバーにメッセージが重複して送信されることを防止できます。詳細は、「管理サーバーからトラブルチケットシステムへの接続」(342 ページ) と 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の詳細は、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管理サーバーまたは接続不能な管理サーバーが含まれていると、メッセージ転送の一部または全部が失敗することがあります。これらのサーバーが再度接続可能になるまで HPOM にメッセージをバッファーするには、ovconfchg コマンドラインツールを使用して、OPC_MSGFORW_BUFFERING 変数を TRUE (デフォルトは FALSE) に設定します。ovconfchg についての詳細は、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ーは、管理サーバーが 2 台のみの環境で実行してください。配布リストに不明なサーバーへの参照が含まれていると、メッセージは継続してバッファーされます。詳細は「メッセージ配布リスト」(339 ページ) 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際は、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。メッセージの指示が正しく表示されるようにするには、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。たとえば、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と、両者間の指示を同一にすることができます。

❏ **同期に関する問題**

制御切り替えを行うと、1 つのメッセージを複数の管理サーバーで同時に担当できるようになるため、次のような同期に関する問題が発生する可能性があります。

- インスタンスの並行実行

  別々の管理サーバー上のオペレータが同じアクションを同時に開始した場合、同じオペレータ起動アクションのインスタンスが平行して実行されることになります。

- 未完了のメッセージの受諾

  作業中のメッセージが、作業の終了前に他の管理サーバー上のオペレータによって受諾される場合があります。

- 不要な注釈

  自分が追加していないメッセージ注釈が追加されていることがあります。

- 転送されない注釈

  オペレータ起動アクションの開始注釈は、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間、およびアクション自体の情報が含まれます。

メッセージへの作業を開始する前に対象メッセージを所有すれば、これらの問題を部分的にでも回避することができます。

❏ **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、ターゲット管理サーバーより先の通信チェーン上にある各システムに影響が及ぶ可能性があります。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た場合にも、同様な問題が発生することがあります。

メッセージ転送ポリシー内で発生した問題のトラブルシューティング

HPOM はメッセージ転送ポリシーに問題や不整合を検出するとエラーメッセージを生成し、そのテンプレートの残りの部分を無視します。また、ソース管理サーバーがターゲット管理サーバーに接続できなかった場合も、HPOM はソース管理サーバーでエラー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。

- ❏ ポリシーが正しく設定されていない
- ❏ ネットワーク関連の問題が存在する
- ❏ リモート (またはターゲット) 管理サーバーに接続できない
- ❏ 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

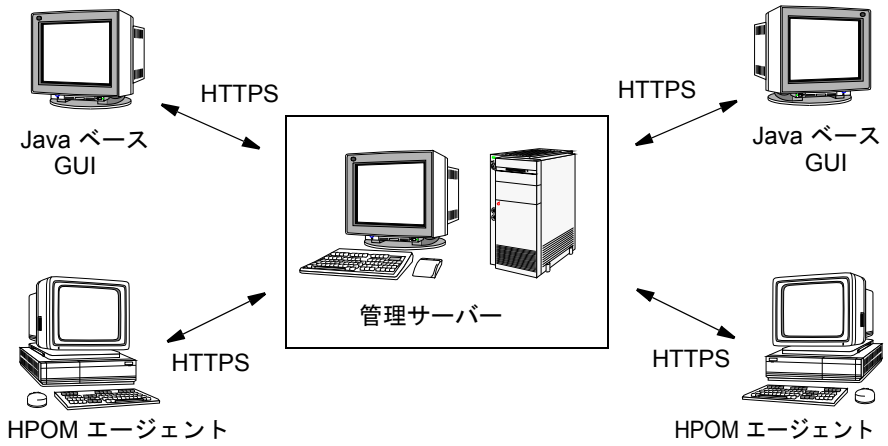
HPOM は、大規模かつ複雑な環境での運用を念頭に設計されています。HPOM のフレキシブルなアーキテクチャは、1 台または複数の管理システムを統合して、組織構成の要件に合わせた強力な 1 つの管理ソリューションを提供します。

本項では、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 を拡張する方法を例示しています。紹介する例にはシンプルな構成から複雑な構成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、いくつかの例を組み合わせて、新しい独自のソリューションを構築することもできます。

構成例 1: 単独のサーバーによる複数ノードの管理

図 5-11 に示されるシンプルな構成では、複数のリモートノードを管理する 1 台の HP Operations 管理サーバーを示しており、それぞれの管理対象ノード上では、HP Operations Agent が動作しています。管理対象ノードと管理サーバーは、HTTP プロトコルを使用して通信を行います。複数のオペレータが Java ベースのオペレータ GUI を使用して環境を共同して管理できます。

図 5-11 単独の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、次に挙げる機能を通じて、複数のリモートシステムを 1 つの場所から効率的に管理できます。

- **変数のしきい値**

  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**

  さまざまなメッセージソースを処理します。

- **ローカルイベント**

  管理対象ノードでのローカルイベントをフィルター処理します。

- **自動アクション**

  管理対象ノードでのローカルな自動アクションを起動します。

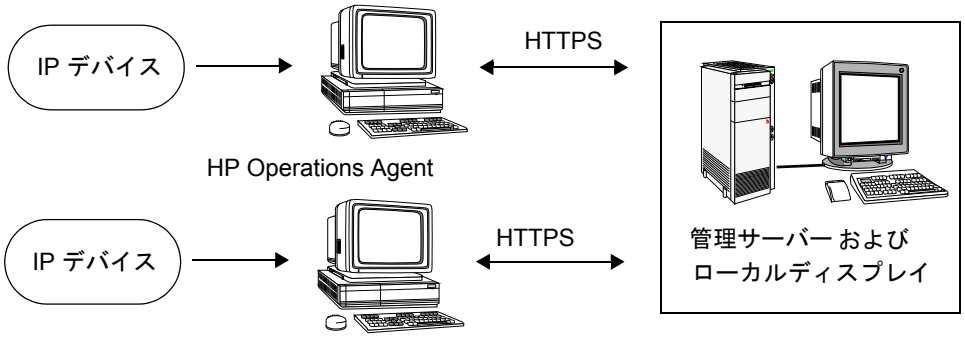
- **エージェントプラットフォーム**

  HP-UX、Linux、AIX、Solaris、Windows などのさまざまなプラットフォームに対応します。

構成例 2: HP Operations Agent による IP デバイスのモニター

図 5-12 に示す構成では、HP Operations Agent が、プロキシエージェントとして動作し、リモート SNMP デバイス上で SNMP しきい値のモニターを実行します。この構成では、HP Operations Agent が動作するリモート管理対象ノードを使用して、ネットワーク内の他の SNMP 専用デバイスのしきい値のモニターを実行できます。HP Operations Agent 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 ポーリングのトラフィックは大幅に軽減されます。

図 5-12 HP Operations Agent による IP デバイスのモニター



管理サーバーでは、HPOM 標準の機能により、次の処理も実行できます。

- **IP デバイスのマッピング**

  すべての IP デバイスを自動的に検出してマッピングします。

- **IP デバイスのポーリング**

  IP デバイスへのポーリングを行い、デバイスの IP ステータスをチェックします。

- **SNMP トラップの受信**

  あらゆるデバイスからの SNMP トラップを受信します。

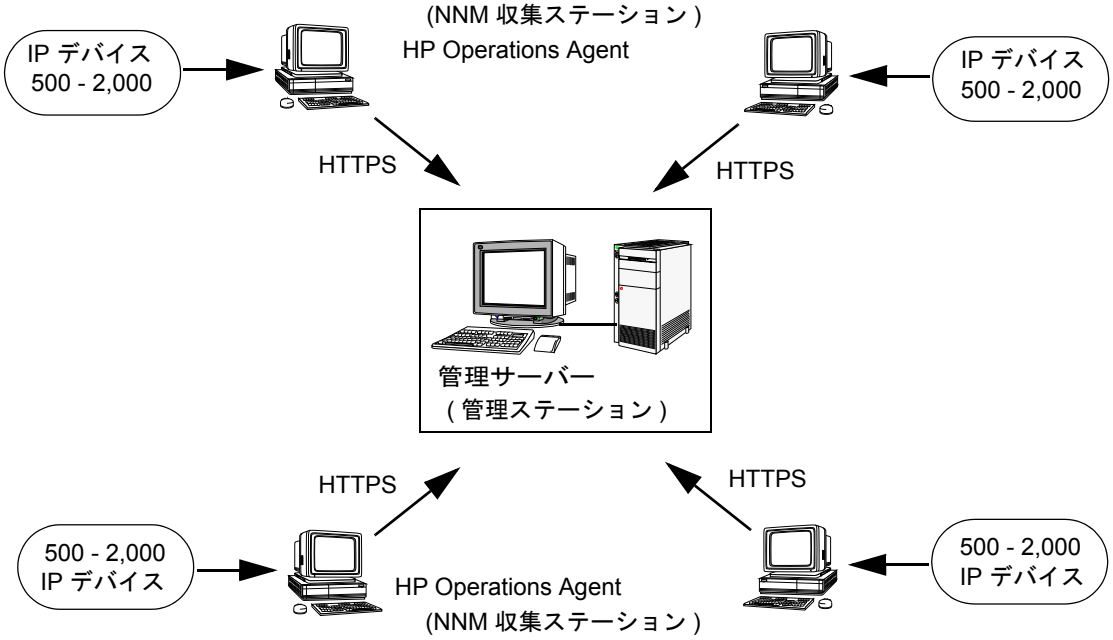
- **SNMP トレンドデータの収集**

  あらゆる SNMP デバイスから (MIB 変数に基づいて) SNMP トレンドデータを収集します。

構成例 3: HP Operations Agent が稼働する NNM 収集ステーション

図 5-13 に示す構成では、中央に位置する HP Operations 管理サーバーが管理対象ノードやデバイスに加え、1 台または複数の NNM 収集ステーションを管理しています。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 Agent が動作する 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。

中央の HP Operations 管理サーバーへのメリット

NNM 収集ステーションによって中央の HP Operations 管理サーバーに提供されるメリットには以下があります。

- **分散モニター**

  トポロジ検出と IP ステータスモニターの分散実行

- **分散収集**

  SNMP データの分散収集

- **イベント転送**

  収集ステーションから管理サーバーへの SNMP イベント転送

ハイエンド、エントリレベルのどちらの NNM ステーションも、収集ステーションとして使うことができます。

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 ステーションのメリットには以下があります。

- **ステーションのモニター**

  リモート NNM 収集ステーションのモニター

- **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。設定できる属性は次のとおりです。

  - SNMP ポーリングの再試行回数とタイムアウト
  - データ収集としきい値
  - MIB のロード
  - SNMP イベント転送の設定

- **ステーションの役割設定**

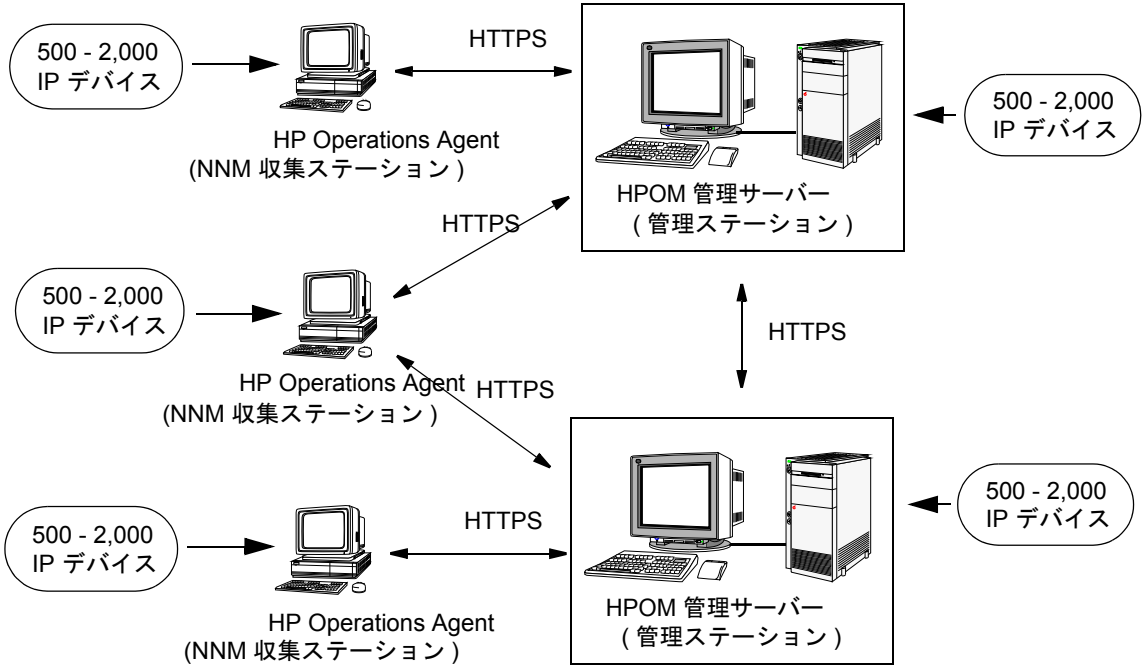
  リモート NNM 収集ステーションの役割 (収集ステーションの追加、テスト、管理解除など) を設定します。

構成例 4: HP Operations Agent が稼動する NNM 収集ステーションと複数の管理サーバー

図 5-14 で示される構成は、「構成例 3: HP Operations Agent が稼働する NNM 収集ステーション」(350 ページ) 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 に比べより高い柔軟性とスケーラビリティを提供します。

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 Agent が稼動する 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には、以下のメリットがあります。

- **複数のマネージャ**

  中央の 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**

  管理サーバーに障害が発生したときにその役割を引き継ぐバックアップサーバーを構成することで、単独の障害によるシステム全体のダウンを回避できます。

- **フォローザサン管理**

  メッセージの送信先マネージャを時刻に応じて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指定したマネージャにメッセージをルーティングできます。このルーティングによって、データベース関連のメッセージなど、特定分野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 ポリシー本体の構文

本付録の内容

付録では、デフォルトポリシータイプのポリシー本体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体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
- イベント相関処理コンポーザー
- フレキシブル管理ポリシータイプ
- リモートアクションセキュリティポリシータイプ
- SiteScope ポリシータイプ
- サブエージェントポリシータイプ

ポリシー本体の構文

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体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

logdefopts:    ε | logdefopts logdefault | logdefopts
               logoption | logdefopts sourceoption
```

ポリシー本体の構文

```
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

snmpconds:      ε |
                snmpconds $e <文字列 (エンタープライズ)> |
                snmpconds $G <数字 (一般トラップ)> |
                snmpconds $S <数字 (固有トラップ)> |
                snmpconds $(<数字 (変数)>) pattern |
                snmpconds NODE nodelist
```

ポリシー本体の構文

```
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

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
```

ポリシー本体の構文

```
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>

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 数字)> 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
```

ポリシー本体の構文

```
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

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> ID <文字> |
                INSTANCERULE <文字>

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
```

ポリシー本体の構文

```
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>

duration:      ε | FOR <文字列 (条件の指定時間)>

numval:        <integer number> | <floating number>

schedsetopts:  ε |
               schedsetopts DISABLED |
               schedsetopts TEMPLATE_ID <文字列 (テンプレートの
               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 <数字 (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
```

ポリシー本体の構文

```
ecopts:         ε |
                ecopts DISABLED |
                ecopts TEMPLATE_ID <文字列 (テンプレートの
                UUID)> |
                ecopts VERSION <数字 (テンプレートのバージョン)> |
                ecopts ECS_LOG_INPUT |
                ecopts ECS_LOG_OUTPUT

ecver:          VERIFIED | UNVERIFIED

wbemdefopts:    ε |
                wbemdefopts wbemdefault |
                wbemdefopts wbemoption |
                wbemdefopts sourceoption

circuit:        ε | circuit <文字列>

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 <間隔 (where 句)> |
                QUERY_LANGUAGE <間隔 (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
```

ポリシー本体の構文

```
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

wbemsupp_unm_conds: ε |
               wbemsupp_unm_conds DESCRIPTION <文字列
               (説明)> condition_id CONDITION
               wbemconds

wbemconds:     ε |
               wbemconds <説明 (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
```

ポリシー本体の構文

```
condsuppdupl:  ε |
               SUPP_DUPL_COND suppdupl |
               SUPP_DUPL_IDENT suppdupl |
               SUPP_DUPL_IDENT_OUTPUT_MSG suppdupl

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 instruction)> |
               INSTRUCTION_TEXT_INTERFACE <文字列> |
               INSTRUCTION_PARAMETERS <文字列>

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 |
```

ポリシー本体の構文

```
                    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 <文字列>

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

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 |
```

ポリシー本体の構文

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

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** |

ポリシー本体の構文

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

E

EC — 参照: メッセージ属性

G

GUI — 参照: Java GUI

H

HP アプリケーション HPOM に統合された HP アプリケーション。 — 参照: 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

HPOM アプリケーション HPOM プラットフォームに統合されているアプリケーション。 — 参照: 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

HPOM インストールマネージャ 管理サーバー。HP Operations Agent ソフトウェアは、ここから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ハートビートをモニターし、ライセンシングをカウントします。 — 参照: アクション許容マネージャ、一次マネージャ

HPOM 内部アプリケーション ブロードキャストタイプのアプリケーション — 参照: 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

HPOM オペレータ — 参照: オペレータ

HPOM 管理者 管理者は、HPOM ソフトウェアのインストールと設定、運用方針の設定と維持、HPOM 以外のソフトウェアの保守、および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します。管理者は、HPOM オペレータインタフェースの機能すべてにアクセスできます。各オペレータの管理作業と作業範囲に応じて、オペレータ単位で作業環境をカスタマイズできます。 — 参照: opc_adm、オペレータ、ユーザープロファイル

HP サービス `opcservice` コマンドラインツールを使用して 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。サービスの呼び出しは、自動的に行われるか、メニューバーから手動で行われます。サービスはシンボルとして表示されるか、グループシンボルの下の階層の一部として表示されます。 — 参照: 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

HPOM パスワード — 参照: パスワード

HTTPS ベースの Java GUI Java GUI と HP Operations 管理サーバーとの間に、セキュアソケットレイヤー (SSL) 暗号化方式で暗号化された HTTPS プロトコルによる安全な通信を提供するインタフェース。 — 参照: Java GUI

J

Java GUI Java グラフィックユーザーインタフェース。 — 参照: オブジェクトペイン

M

MoM — 参照: フレキシブル管理

MoM manager-of manager の略。 — 参照: フレキシブル管理

O

opc_adm HPOM 管理者。3 つの定義済 HPOM ユーザーの 1 つ。HPOM のデフォルトの管理者です。 ― 参照: opc_op、HPOM 管理者、ユーザー名

OPC_NODES 予約されている変数。オペレータ管理ノードまたは管理者登録ノード/ノードグループから選択したノードのリストを取り出すときに使用されます。取り出した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。3 つの定義済 HPOM ユーザーの 1 つ。システム管理機能だけを担当します。オペレータはネットワークアクティビティを管理しません。このオペレータは、プロセス、ディスク容量、印刷状況など、UNIX の一部の機能を利用できます。 ― 参照: opc_adm、オペレータ、ユーザー名

opcacta ― 参照: アクションエージェント

opcactm ― 参照: アクションマネージャ

opcbbcdist ― 参照: 設定管理アダプター

opcctla ― 参照: コントロールエージェント

opcle ― 参照: ログファイルエンキャプスレータ

opcmon (1|3) モニター対象の値を HPOM のモニターエージェント (opcmona) に渡すために、アプリケーションやスクリプトが使用するコマンドおよび API。

opcmona ― 参照: モニターエージェント

opcmsg (1|3) HPOM が生成したメッセージの文字列や属性を HPOM メッセージインターセプタ (opcmsgi) に渡すために、アプリケーションやスクリプトが使用するコマンドおよび API。

opcmsga ― 参照: メッセージエージェント

opcmsgi ― 参照: メッセージインターセプタ

opcmsgm ― 参照: メッセージマネージャ

opcuiwww Java ベースのオペレータ用 GUI とディスプレイマネージャとの間で、通信要求のやり取りを行うプロセス。Java ベースの GUI ごとに、少なくとも 1 つ起動する必要があります。

ovcd ― 参照: OV コントロール。

ovoareqsdr ― 参照: 要求センダ

OV コントロール “ovcd” とも呼ばれます。管理サーバー上のプロセス。他のすべてのマネージャプロセスを開始、終了し、すべてのマネージャプロセスが実行中であることを確認します。

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交換する TCP/IP の上位プロトコルです。SNMPv2C は従来の SNMP に比べ、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ー処理します。フィルター処理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、トラップ用テンプレートを設定できます。トラップ用テン

プレートは、メッセージのデフォルトとパターンマッチのデフォルト、メッセージ条件、および除外条件からなります。

あ

アクション メッセージへの応答。メッセージソースのテンプレートや条件に基づいて割り当てられます。自動的に起動されるアクションと、オペレータが起動するアクションがあります。 ― 参照: 自動アクション、オペレータ起動アクション

アクションエージェント “opcacta” とも呼ばれます。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。 ― 参照: エージェント

アクション許容マネージャ 特定の管理対象ノードに対してアクションの実行を許可されている管理サーバー。デフォルトでは、管理対象ノードに対してアクションの実行を許可されている管理サーバーは、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有の管理対象ノード上でアクションを実行するように設定することもできます。 ― 参照: HPOM インストールマネージャ

アクションマネージャ “opcactm” とも呼ばれます。管理サーバー上にあり、管理対象ノード上のアクションエージェントを制御する要素。アクションマネージャは、オペレータ起動アクションやアプリケーションを実行するためにディスプレイマネージャから呼び出されます。また、メッセージを送信した管理対象ノード以外のシステム上で自動アクションを実行する場合には、メッセージマネージャから呼び出されます。

アクティブメッセージブラウザ ― 参照: メッセージブラウザ

アプリケーション 1. 簡単なスクリプト、プロセス、またはコマンド。2. たくさんのプログラムや設定ファイルを含む複雑な製品。 ― 参照: オペレーションビュー、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

アプリケーションデフォルト 色やフォントなど、アプリケーションがデフォルトで使用する設定。アプリケーションデフォルトは、X Window アプリケーションのデフォルトファイルを編集して変更できます。 ― 参照: opc(1) のマニュアルページ

暗号化 メッセージの盗聴や、改変を防止するセキュリティオプション。正当に認証された受信者だけがメッセージを読み取れることを保証します。 ― 参照: 認証

一次収集ステーション この条件には、イベントとの比較に使う文字列パターンが入っています。 ― 参照: 二次収集ステーション

一次マネージャ 現在、HP Operations Agent の実行を管理している管理サーバー。エージェントの起動と停止、新しいソフトウェアのインストール、およびエージェントへの設定情報の配布は、このサーバーだけに許可されます。一次マネージャに関する情報は `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 Agent の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の `ovconfchg` 設定ツールを使用してファイル名を抽出します。 ― 参照: バックアップマネージャ、HPOM インストールマネージャ

イベント コンピューティング環境で発生し、メッセージ生成の原因になる事象。通常、イベントには、ステータスの変更やしきい値の

超過などがあります。たとえば、用紙トレイが空になるとプリンターのステータスが変化し、メッセージが生成されます。

イベント相関処理 イベントストリームのリアルタイム処理を通じて、イベント間の関係を認識する処理。可能な場合には、便利で管理しやすい情報で小さいストリームを新しく生成します。

イベント属性 ― 参照: メッセージ属性

エージェント マネージャプログラムから要求を受信し、情報の収集、処理の実行、および応答の生成を行うプログラム。 ― 参照: 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

オブジェクト HPOM で管理されるリソースと関連機能。ノードやアプリケーション、オペレータなど。

オブジェクトペイン Java GUI の上部にある 2 番目のペイン。管理対象環境内の別の要素へのアクセスに使用されます。 ― 参照: Java GUI

オペレーションビュー オペレーションビューでは、管理対象環境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たメッセージグループを階層ツリーで表示します。 ― 参照: アプリケーション、メッセージグループ、ノード

オペレータ起動アクション メッセージに応じて、オペレータが起動する修正アクションまたは予防アクション。自動アクションと違って、オペレータがボタンをクリックすると起動します。管理者もオペレータのブラウザを使用できるので、オペレータ起動アクションを管理者が起動することもできます。 ― 参照: アクション、自動アクション

オペレータ HPOM 管理者によって割り当てられたノードやメッセージグループから着信するメッセージをモニターし、応答する HPOM ユーザー。オペレータは、Java GUI ではメッセージブラウザとオブジェクトペインを使って作業を実行します。opc_op は 3 つの定義済オペレータの 1 つです。 ― 参照: opc_op、ユーザープロファイル

か

外部ノード HPOM ドメイン外に存在するノード。IP ノードだけでなく、さまざまな種類のノードが外部ノードになります。しかし、外部ノードは、通常の HPOM ノードの機能の一部しか持っていません。外部ノード上では、HP Operations Agent は動作しません。 ― 参照: ノードグループ

簡易ネットワーク管理プロトコル (Simple Network Management Protocol)

― 参照: SNMP

監査エントリ オペレータの活動 (たとえば、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) や、管理者の活動 (設定作業など) を定義するデータベースエントリ。

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。管理サーバーには、ドメイン内のすべての管理対象ノードから HPOM メッセージが転送されます。

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やインテリジェントデバイス (ネットワークプリンター、ルーターなど) の総称。HP Operations Agent は、各ノードから情報を収集し、フィルター処理やその他の処理を施して管理サーバーに送信します。 ― 参照: 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

起動属性 ある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出、およびそのアプリケーションのアプリケーション呼出を実行するユーザー。HPOM 管理者が、起動属性をアプリケーションにあらかじめ設定します。

グラフィックユーザーインタフェース

— 参照: Java GUI

計画休止 コンピューティング環境のサービスとシステムを利用できないように、あらかじめ計画した期間。この期間中に、利用できないサービスやシステムから着信した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。 — 参照: 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ー解除

コントロールエージェント “opcctla” とも呼ばれます。各管理対象ノード上のエージェント。他のすべてのエージェントの起動と停止、および管理サーバーから送信された要求の処理を担当します。コントロールエージェントは、起動中や、要求センダから分配要求を受信したときに分配エージェントを起動し、管理サーバーから新しい設定データを収集します。 — 参照: エージェント

コントロールの切り替え メッセージの担当サーバーを、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。オリジナルメッセージに関連付けられたアクションと操作のセットすべてを、ターゲット管理サーバーに与えます。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だけが残ります。 — 参照: メッセージの転送、通知メッセージ

さ

サービス — 参照: HP サービス

サービス時間 1. ヘルプデスクの営業時間として取り決められた時間帯。顧客とのサービスレベル契約でこの時間帯を定義します。2. HPOM ノードからのメッセージを HPOM オペレータに渡す時間帯を定義します。この時間帯の前後に生成されたメッセージはバッファーに入れられ、次の時間帯になってから転送されます。3. サービスプロバイダーがサービス (たとえば、電子メール、印刷、SAP R/3、アウトソーシング) をサポートする時間帯を定義します。 — 参照: 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ー解除

サービスレポート 指定した時間帯または任意の時点について、HPOM 環境のサービスのステータスの概要を示すレポート。HP Service Reporter が生成します。

しきい値のモニター 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。指定した期間、オブジェクトの値がしきい値を超過した場合に、オペレータへメッセージを送信できます。このメッセージによって、システムの機能やエンドユーザーの作業に影響を与える前に、障害を解決できます。 — 参照: モニターエージェント

指示文インタフェース 選択したユーザーに指示を示すときに使用する外部プログラムを、管理者が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、メッセージごとに違う指示を示すことができます。 — 参照: ヘルプ指示文テキスト

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`や`/etc/group` など)、システムの起動またはシャットダウン時に自動実行されるファイルの総称。これらの設定ファイルは手動で編集できるほか、自動的に変更される場合もあります。

自動アクション 着信したイベントや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。 ― 参照: メッセージの受諾、オペレータ起動アクション

重要度 あるオペレータ環境での重要性に従って、HPOM 管理者がメッセージに割り当てたレベル。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、該当するノード、ノードグループ、またはメッセージグループから送信される最も重要度の高いメッセージの重要度が反映されます。 ― 参照: ステータス伝達

受諾 ― 参照: メッセージの受諾

受諾解除 ― 参照: メッセージの受諾解除

使用ライセンス (LTU) 顧客が入手したライセンス。LTU は、ライセンシング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 特定のソースから着信するメッセージを選別するために、HPOM 管理者が設定する条件の 1 つ。除外条件を設定すると、条件に一致するメッセージはメッセージブラウザに渡されません。除外メッセージは、管理対象ノードのローカルログに記録できます。 ― 参照: 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

所有権 ― 参照: メッセージの所有権

所有権表示モード 所有済またはマーク済のメッセージを表示するか、または除外するかを指定するモード。メッセージステータスの生成に、このモードを使います。有効なモードは、[ステータス伝達あり] と [ステータス伝達なし] の 2 つです。 ― 参照: ステータス伝達

所有状態 ― 参照: メッセージの所有権、所有権表示モード

ステータス伝達 指定した管理対象ノードやメッセージグループのステータスを重要度レベルによって決定すること。管理対象ノードやメッセージグループから送信される最も重要度の高いメッセージのステータスを、その管理対象ノードやメッセージグループのステータスにします。 ― 参照: 所有権表示モード、重要度

制御対象ノード リモートログオンなど、HPOM の管理/モニター機能すべての対象となる管理対象ノード。このノード上で、アクションを実行したり、アプリケーションを起動したりします。

セッション HPOM にログオンしている時間。HPOM にログオンまたはログアウトすると、HPOM セッションが開始または終了します。

設定管理アダプター “opcbbcdist” とも呼ばれます。既存のアクション、コマンド、モニターからインスツ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 形式に変更する HTTPS エージェントと HP Operations 管理サーバーの間の設定管理アダプター。

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領域に関する専門情報を集めるように指定されたところ。専門技術センターが階層構造であるときは、特定の障害に関連するメッセージを、定義済の管理サーバーに送信するように管理対象ノードを設定します。送信先のサーバーには、その障害を解決するための情報があります。 ― 参照: フレキシブル管理

た

注釈 ― 参照: メッセージの注釈

通知メッセージ HPOM が管理サーバーに転送する読み取り専用メッセージ。通知を目的としていますが、限られた範囲で関連する操作を伴うこともあります。 ― 参照: コントロールの切り替え、メッセージの転送

通知サービス イベントの発生をオペレータに警告するサービス。HPOM の Java GUI メッセージブラウザに表示される情報の色や重要度レベルも、このサービスの一部です。HPOM は、ブザーやポケットベルなど、外部のサービスへもメッセージを転送できます。

データ保存サービス 分散環境での情報の保存に使う記憶メカニズムの総称。たとえば、メタデータ、固定のオブジェクト情報、履歴情報、およびトポロジ情報を格納するデータベースなどがあります。

デフォルトオブジェクト ― 参照: オブジェクト

デフォルトターゲットノード アプリケーションの起動やコマンドのブロードキャストの対象となるノードのリスト。このリストは、管理者が定義します。カスタマイズした起動権限を管理者がオペレータに割り当てた場合は、オペレータは Java GUI からリストを変更できます。 ― 参照: 管理対象ノード、ノード

な

二次収集ステーション オブジェクトをモニターする収集ステーションのうち、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ステーション。 ― 参照: 一次収集ステーション

二次マネージャ 二次管理サーバー。一次管理サーバーから二次管理サーバーへ管理作業範囲を移すことができます。二次管理サーバーへ管理作業範囲を移すと、二次管理サーバーが一次管理サーバーになります。 ― 参照: opcragt(1m) コマンドのマニュアルページ

認証 接続を確立する前に、双方の妥当性を検証するセキュリティ機能。 ― 参照: 暗号化

ノード ネットワーク上に存在するコンピュータシステムやインテリジェントデバイス (ブリッジ、ルーターなど) の総称。 ― 参照: デフォルトターゲットノード、管理対象ノード、オペレーションビュー

ノード階層 ノードとノードレイアウトグループの階層構造を視覚的に表現したもの。各ノード階層には HPOM 環境に属する管理対象ノードがすべてあります。各階層の違いはノードの構造だけです。ノード階層は HPOM ユーザーに割り当てられ、ユーザーが担当する管理対象ノードを表示します。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ノードおよび外部ノードの論理的なグループ。管理者は、この論理グループに対して一貫した方針を適用します。1 つのノードが複数のノードグループに属すこともできます。 ― 参照: 外部ノード、管理対象ノード

は

パスワード HPOM 管理者やオペレータを一意に識別する ID。オペレーティングシステムへのアクセス時に使用するパスワードとは関係ありません。 ― 参照: ユーザー名

パターンマッチ メッセージの分類に使う条件。この条件には、イベントとの比較に使う文字列パターンが入っています。比較結果によって、HPOM によるメッセージの処理方法が決まります。 ― 参照: 非該当メッセージ

バックアップマネージャ 障害の発生時などに、他の管理サーバーを代替する管理サーバー。代替の結果、バックアップマネージャ

は一次管理サーバーになります。通常、バックアップマネージャの設定は、代替対象の管理サーバーと同じです。 ー 参照: 一次マネージャ

非該当メッセージ メッセージ条件と除外条件のどちらにも該当しないメッセージ。非該当メッセージをローカルにログしたり、管理サーバーに転送したりできます。 ー 参照: パターンマッチ

非管理対象ノード オペレータの作業環境から一時的に除外されているノード。非管理対象ノードでは、エージェントプロセスは起動されません。また、非管理対象ノードから着信したメッセージは無視されます。

ビュー 特定のデータベースやシステム用に設定した表示。たとえば、メッセージブラウザでのメッセージの表示を、フィルターを使って定義できます。フィルターの条件に一致するメッセージだけが、フィルター処理済アクティブメッセージブラウザに表示されます。

フィルター ノードの情報や GUI に表示する情報を、メッセージ条件を基に変更、リダイレクト、または除外して選別する機能。管理者はメッセージ条件と除外条件を定義することによって、さまざまなソースからメッセージを選別して収集します。 ー 参照: メッセージ条件、除外条件

フィルター処理済メッセージブラウザ 選択したメッセージだけを表示するJava GUI メッセージブラウザ。メッセージブラウザ内にすべてのメッセージを表示するのではなく、特定のメッセージだけを表示できます。 ー 参照: 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

フォローザサン タイムゾーンによって複数の管理サーバーに担当を分散すること。管理対象ノードは、管理者によって定義された時間属性に従って、設定された管理サーバーにメッセージを送信します。 ー 参照: フレキシブル管理

フレキシブル管理 管理対象ノードの担当を多数の管理サーバーに分散すること。また、メッセージの受信日時、受信場所、内容に応じて、管理対象ノードがさまざまな管理サーバーへレポートできるようにすること。 ー 参照: 専門技術センター、フォローザサン

プロセス プログラムファイルの実行。HPOM で動作するプロセスには、統合されたアプリケーションやスクリプト、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あります。

ブロードキャスト 指定された 1 つ以上の管理対象ノードに、同時にコマンドを送信すること。オペレータは、Java GUI のオブジェクトペインにあるツールツリーからコマンドを送信します。

プロパティシート 作業手順を示すオプションを含むポップアップウィンドウ。このダイアログボックスのタブをクリックすると、オプションが表示されます。

ペンディングメッセージ 定義されたサービス時間外や、計画休止の期間中に HP Operations 管理サーバーに着信するメッセージ。このメッセージは、定義済のバッファー解除時刻になるまで Java GUI ペンディングメッセージブラウザに表示されます。このメッセージは、自動または手動でバッファーから解除されます。メッセージがバッファー解除されない場合は、メッセージブラ

ウザに移動します。メッセージが受諾された場合は、フィルター処理済履歴メッセージブラウザに移動します。 ― 参照: 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ー解除

ペンディングメッセージブラウザ 定義されたサービス時間外に着信したため、バッファーに格納されているメッセージを表示するブラウザ。 ― 参照: 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、フィルター処理済メッセージブラウザ

ポリシー 少なくとも 2 つのファイル、ポリシーのヘッダーと 1 つ以上のポリシー本体からなる設定要素。ポリシーのヘッダーは、名前、タイプ、バージョンなどの属性を含む XML ファイルです。ポリシー本体には、実際の属性を含まれています (たとえば、ポリシーが配布される 1 つ以上の管理対象ノードでのメッセージの生成を決定するルールのセット)。 ― 参照: ポリシーグループ

ポリシーグループ 共通の特徴を持つポリシーの論理的なグループ。管理者はポリシーグループとその階層を作成して、ポリシー管理を簡単にできます。また、管理対象ノードやノードグループへのポリシーの割り当ても簡単になります。 ― 参照: ポリシー

ま

マーキング ― 参照: メッセージの所有権

メッセージ 管理対象オブジェクトのステータス、関連するイベント、または障害を構造化した読み取り可能な情報。この情報は、対応するオブジェクトのステータスに基づいて、Java GUI アクティブメッセージブラウザ、フィルター処理済アクティブメッセージブラウザ、フィルター処理済履歴メッセージブラウザ、またはフィルター処理済ペンディングメッセージブラウザに表示されます。 ― 参照: メッセージ属性

メッセージインターセプタ “opcmsgi” とも呼ばれます。着信メッセージを受信するプロセス。メッセージを HPOM に転送するには、opcmsg(1) コマンドと opcmsg(3) API を使用します。条件を設定して、特定の種類のメッセージを統合したり、除外したりできます。

メッセージエージェント opcmsga とも呼ばれます。管理対象ノード上のエージェント。メッセージソースからメッセージを受信し、処理して管理サーバーに送信します。 ― 参照: エージェント

メッセージキー 特定のイベントによって発生したメッセージを識別するために使用するメッセージ属性 (文字列)。この文字列はイベントの重要な特性を示しています。メッセージによる他のメッセージの受諾手段として使用できます。また、この文字列を使って、重複するメッセージを識別できます。 ― 参照: メッセージ属性

メッセージグループ 同じ作業に属す、または何らかの論理的な関係を持つ複数のメッセージの集合。たとえば、バックアップ作業や出力作業からのメッセージ、共通のポリシーを持つメッセージなどです。 ― 参照: オペレーションビュー

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 に設定するフィルター。これらのフィルターはメッセージを生成し、生成されたメッセージは通常、メッセージブラウザに表示されます。メッセージソースのテンプレートは、一連のメッセージ条件と除外条件からなります。 ― 参照: フィルター、メッセージのグループ替え条件、除外条件

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。読み取り/書き込み両用、読み取り専用、または書き込み専用の外部アプリケーションは、メッセージストリームインタフェースにアクセスして、メッセージに追加処理を行います。メッセージストリームインタフェースは、管理サーバーとエージェントで利用できます。インタフェース機能にアクセスするための API のセットがあります。

メッセージ属性 1. 管理者が管理サーバーから受信したメッセージの分類に使用する属性。 2. `OPCDATA_MSG`の数値フィールド群。各フィールドの値は、たとえば、EC ノードの event-type フィールドなど、文字列形式で参照されます。 ― 参照: メッセージ、メッセージキー

メッセージソース HPOM が管理するメッセージのソース (生成源)。HPOM は、ログファイル、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その API (`opcmsg(1|3)`)、HPOM モニターコマンドインタフェースとその 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生成される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、HPOM 管理者はメッセージデフォルト、メッセージ条件、および除外条件からなるテンプレートを定義します。 ― 参照: ログファイルメッセージ、管理対象ノード

メッセージ対象ノード エージェントソフトウェアを実行しないノード。メッセージ対象ノードが送信したメッセージは、HPOM に受理されます。

メッセージタイプ メッセージ群をサブグループに分類するために使うメッセージ属性。この属性を利用すると、相関処理の規則で参照できるようにメッセージ群を細かくグループ分けできます。メッセージタイプは、HPOM に接続されているイベント相関処理エンジンがあるときは、特に便利です。

メッセージターゲット規則 管理対象ノードに対して、特定のメッセージの送信先となる管理サーバーを指示する条件。この条件では、計画休止中または稼動時間中にメッセージを除外したり、バッファーに格納したりするタイミングも、メッセージ属性や日時を基に調べます。メッセージターゲット規則は、管理対象ノード上の設定ファイル`mgrconf`で定義されています。

メッセージのグループ替え条件 オペレーティング環境用に定義されたメッセージの管理方針内の条件。この条件を使って、管理サーバー上でのメッセージグループを再編成できます。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構成できます。 ― 参照: メッセージ条件、除外条件

メッセージの重要度 ― 参照: 重要度

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にメッセージを移動すること。履歴データベースに移動したメッセージは、Java GUI フィルター処理済履歴メッセージブラウザで表示できます。メッセージは通常、その生成原因になった障害やイベントがアクションによって解決された後、履歴データベースに移動されます。 ― 参照: 自動アクション、メッセージの受諾解除

メッセージの受諾解除 履歴データベースから Java GUI アクティブメッセージブラウザにメッセージを戻すこと。メッセージが受諾前に属していたメッセージブラウザが移動先になります。受諾解除したメッセージは、フィルター処理済履歴メッセージブラウザには表示されなくなりますが、フィルター処理済ア

クティブメッセージブラウザには表示されます。受諾解除できるのは、履歴メッセージブラウザ内のメッセージだけです。 ― 参照: メッセージの受諾

メッセージの所有権 オペレータまたは管理者が、あるメッセージに関連するアクションを実行するために、そのメッセージを引き受けること。メッセージ所有の概念は、通知モードでのメッセージのマーキングに似ています。 ― 参照: メッセージのマーキング、メッセージの所有権モード

メッセージの所有権モード オペレータや管理者がアクションとのやり取りを行うときに使用するモード。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。 ― 参照: メッセージの所有権

メッセージの注釈 メッセージに付加された注釈。自動的に付加されるか、オペレータまたは管理者が付加します。障害を解決するために実行するアクションを説明するものです。複数行または複数のページにわたる注釈を付加できます。オペレータ、管理者のどちらも、1 つのメッセージに複数の注釈を付加できます。

メッセージの転送 HP Operations 管理サーバー間でメッセージを転送して問題の発生を別の管理サーバーに伝えたり、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別の管理サーバーに実行させることができます。 ― 参照: コントロールの切り替え、通知メッセージ

メッセージのバッファー解除 フィルター処理済ペンディングメッセージブラウザから、フィルター処理済アクティブメッセージブラウザにメッセージを移動すること。移動後、メッセージを編集できます。 ― 参照: 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

メッセージのマーキング オペレータまたは管理者がメッセージに注意していることを示します。マーキングは通知モード特有の概念です。強制モードでのメッセージの所有権に似ています。 ― 参照: メッセージの所有権

メッセージブラウザ ユーザーインタフェースの一部。ユーザーが管理サーバーから受信したメッセージを表示するときに使用されます。ユーザーは、障害の検出、メッセージの確認と受諾、障害管理作業の実行にこのブラウザを使用します。 ― 参照: 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、フィルター処理済メッセージブラウザ

メッセージマネージャ “opcmsgm” とも呼ばれます。管理サーバー上で実行されるプロセス。メッセージの優先順位付けと分類、メッセージへの注釈の付加、およびアクションの実行を管理します。

モニターエージェント “opcmona” とも呼ばれます。システムパラメータ (CPU の負荷、ディスクの使用率、カーネルパラメータ、SNMP MIB など) をモニターするプロセス。モニターエージェントは、パラメータの実際の値を定義済のしきい値とチェックします。パラメータ値がしきい値を超過している場合には、メッセージを生成し、メッセージエージェントに転送します。HPOM 管理者は、モニター対象オブジェクトの照会周期を調整できます。 ― 参照: しきい値のモニター

モニター対象オブジェクト HPOM によって周期的に照会されるオブジェクト。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。

モニターのみのノード エージェントプロセスはすべて起動されるが、アクションは実行されないノード。モニターのみのノードを使って、システムのセキュリティ要件を高め、リモートログオンやリモートアクションを制限するように、システムを設定できます。

や

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。1 つ以上の設定済プロファイルから、実際の HPOM ユーザーの設定を取り込むことができます。 ー 参照: オペレータ、HPOM 管理者

ユーザー名 HPOM アプリケーションがユーザーを一意に識別するための名前。オペレーティングシステムのユーザー名とは無関係です。オペレーティングシステムのユーザー名とは無関係です。HPOM の GUI には、ユーザー名とパスワードを正しく入力する必要があります。HPOM は管理者に `opc_adm`、オペレータに `opc_op` という一意のユーザー名を割り当てています。この 2 つのユーザー名は変更できません。他のユーザー名の長さは、最大で 8 文字です。ユーザー名には、オペレーティングシステムの制約がすべて適用されます。 ー 参照: opc_adm、opc_op、パスワード

要求センダ “ovoareqsdr” とも呼ばれます。管理サーバーから管理対象ノードに、エージェントの起動や停止、定期ポーリングの設定などの要求を送信するプロセス。

ら

ライセンスキー ライセンスキーには、ライセンスされるオブジェクトに関する情報と、ラインセンス (LTU) の数が含まれます。たとえば、HP Operations 管理サーバーと HP Operations Agent はライセンスされるオブジェクトです。

ライセンスパスワード ライセンスされたオブジェクトの 1 つまたは複数のライセンスに関する情報を持つ一意の文字列。ライセンス (LTU) をインストールするためのパスワードは、ライセンスパスワードリポジトリに追加されます。

リモートノード 通信リンクを使用するシステム。 ー 参照: 管理対象ノード

リモートログオン 管理対象ノードに、そのノード以外からアクセスすること。

履歴メッセージブラウザ 受諾したメッセージをすべて表示する Java GUI ブラウザ。受諾したメッセージを調べると、これまで使用された障害解決の手法を確認できます。 ー 参照: メッセージブラウザ、ペンディングメッセージブラウザ、フィルター処理済メッセージブラウザ

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 に含まれていない要素のレポートを統合したりできます。

ログのみのメッセージ 管理サーバーに記録され、履歴データベースに送信されるメッセージ (設定によっては、管理サーバーではなくローカルに記録されます)。このメッセージが表示されるのは、履歴メッセージブラウザだけです。log-on-management-server-only 属性はメッセージ条件ごとに設定できます。この属性を設定している条件には、他のアクションを設定できません。

ログファイルエンキャプスレータ opcle とも呼ばれます。管理対象ノードで動作するプロセス。1 つ以上のアプリケーションやシステムのログファイル内を、ログファイルのテンプレートを使って走査し、管理者が指定したパターンに一致するメッセージを検索します。一致の検出時にメッセージを生成する場合、そのメッセージをメッセージエージェントに転送します。

ログファイルメッセージ アプリケーションやサービスのログファイルから生成されるメッセージ。管理者はログファイルのテンプレートを設定します。テンプレートは、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)、メッセージ条件、および除外条件からなり、ログファイルエンキャプスレータによるログファイルの読み取り方法を決定します。ログファイルエンキャプスレータは、生成されたメッセージをメッセージエージェントに転送します。 ー 参照: メッセージソース

わ

ワークスペース ワークスペースペインの各タブの内容。オペレータが特定の作業用に定義します。通常のワークスペースには、メッセージブラウザ、グラフ、傾向グラフ、アプリケーション出力、サービスグラフ、および ActiveX 対応でない Web ブラウザを表示できます。ActiveX 対応の Web ブラウザを使用するには、ActiveX ワークスペースを定義します。ActiveX ワークスペースに表示できるのは、Web ブラウザだけです。 ー 参照: ワークスペースペイン

ワークスペースペイン ツールバーとペインコントロールの右下に表示されるペイン。このペインには、オペレータ定義の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、または Web ブラウザを表示できます。 ー 参照: Java GUI、ワークスペース